# NetScaler Application Delivery Management 13.0

**Machine translated content**

## Disclaimer

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

# Contents

**Notas de la versión** 17

**Migración local de NetScaler ADM a Citrix Cloud** 18

**Preguntas frecuentes** 27

**Solución de problemas** 31

**Todos los artículos** 34

**Overview** 39

**Funciones y soluciones** 39

**Arquitectura** 42

**Cómo descubre NetScaler ADM instancias** 44

**Visión general de sondeo** 46

**Gobierno de datos** 54

**Sistema de licencias** 59

**Requisitos del sistema** 72

**Introducción** 86

**Implementar** 90

**Requisitos previos para instalar NetScaler ADM** 91

**Citrix ADM en Citrix Hypervisor** 93

**NetScaler ADM en Microsoft Hyper-V** 95

**NetScaler ADM en VMware ESXi** 102

**Citrix ADM en clúster de Kubernetes** 107

**NetScaler ADM en el servidor KVM Linux** 110

**Configurar la implementación de alta disponibilidad** 116

**Configurar la recuperación ante desastres para alta disponibilidad** 132

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Configurar agentes en prem para la implementación en varios sitios** 142

**Instalar un agente ADM como microservicio en un clúster de Kubernetes** 150

**Migrar la implementación de un solo servidor de Citrix ADM a una implementación de alta disponibilidad** 151

**Migrate from NetScaler Insight Center to NetScaler ADM** 156

**Integración de NetScaler ADM con Citrix Director** 158

**Conecte un disco adicional a NetScaler ADM** 160

**Configuración** 173

**Agregar instancias a Citrix ADM** 174

**Agregar instancias de NetScaler ADC VPX implementadas en la nube a NetScaler ADM** 184

**Administrar licencias y habilitar análisis en servidores virtuales** 186

**Configurar servidor NTP** 194

**Configurar la configuración del sistema** 195

**Integre Citrix ADM con la instancia de ServiceNow** 199

**Exportar o programar informes de exportación** 204

**Actualizaciones** 207

**Autenticación** 214

**Configurar servidores de autenticación externos en NetScaler ADM** 216

**Agregar servidor de autenticación LDAP** 216

**Agregar servidor de autenticación RADIUS** 218

**Agregar servidor de autenticación TACACS** 220

**Usuarios en NetScaler ADM** 222

**Extraer un grupo de servidores de autenticación** 223

**Habilitar servidores de autenticación externa de reserva y en cascada** 223

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Control de acceso** 225

**Control de acceso por roles** 226

**Configurar directivas de acceso** 228

**Configurar grupos** 233

**Configurar roles** 244

**Configurar usuarios** 245

**Aplicaciones** 247

**Administración de aplicaciones y panel de aplicaciones** 248

**Administración de aplicaciones** 250

**Introducción al panel de aplicaciones** 257

**Ver aplicaciones** 260

**Detalles de la aplicación** 261

**Seleccionar componentes de App Score y establecer umbrales** 267

**Detalles de aplicación para aplicaciones de microservicios** 270

**Panel de control Web Insight** 275

**Análisis de uso de aplicaciones** 279

**Solucionar problemas del panel de aplicaciones** 287

**Crear un umbral y una alerta para el análisis de aplicaciones** 295

**Análisis inteligente de aplicaciones** 297

**Configurar el análisis inteligente de aplicaciones** 297

**Indicadores de rendimiento para análisis de aplicaciones** 298

**Tiempo de respuesta** 299

**Servicios Activos** 300

**Uso medio de CPU** 301

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Uso de memoria** 302

**Solapas de servicio** 303

**Servidor inestable** 304

**Acumulación de sesiones** 306

**Reutilización baja de sesiones** 307

**Acumulación SurgeQueue** 308

**Paquetes HTTP inusualmente grandes** 309

**Tipo de persistencia incorrecto** 310

**TCP volver a ensamblar visitas de límite de cola** 311

**Tráfico en tiempo real SSL** 312

**Panel de seguridad de aplicaciones** 313

**Gráfico de servicio** 316

**Configuración del gráfico de servicio** 320

**Ver detalles en el gráfico de servicio** 323

**Configurar umbrales en el gráfico de servicio** 337

**Ver detalles del servicio** 339

**Ver detalles de ingreso para solucionar problemas** 342

**Seguimiento distribuido** 348

**Ver detalles de diagnóstico para datos parciales o nulos en el gráfico de servicio** 355

**Gráfico de servicio para aplicaciones** 358

**Vista holística de todas las aplicaciones en el gráfico de servicio** 364

**StyleBooks** 373

**Categorías de StyleBook** 375

**Importar y sincronizar StyleBooks desde el repositorio de GitHub** 385

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Usar StyleBooks predeterminados** 387

**StyleBook de firewalls de aplicaciones web** 390

**Crear perfiles WAF y BOT con StyleBook** 398

**Ocultar todos los StyleBooks predeterminados** 399

**Migrar la configuración de aplicaciones Citrix ADC con StyleBooks Configuration Builder** 401

**StyleBooks de aplicaciones empresariales** 405

**StyleBook del SSO de Google Apps** 406

**StyleBook del SSO de Office 365** 410

**StyleBook de Microsoft Skype Empresarial** 419

**StyleBook de Microsoft Exchange** 427

**StyleBook de Microsoft SharePoint** 430

**StyleBook proxy de Microsoft ADFS** 439

**StyleBook del negocio electrónico de Oracle** 457

**StyleBooks de Citrix StoreFront** 459

**Crear y utilizar StyleBooks personalizados** 462

**StyleBook para crear un servidor virtual de equilibrio de carga** 464

**StyleBook para crear una configuración básica de equilibrio de carga** 471

**Crear un StyleBook compuesto** 479

**Usar atributos de GUI en un StyleBook personalizado** 481

**Importar StyleBooks personalizados** 482

**Crear y modificar un paquete de configuración** 488

**Crear un StyleBook para cargar archivos a NetScaler ADM** 499

**Crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM** 503

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Habilitar análisis y configurar alarmas en un servidor virtual definido en un StyleBook** **509**

**Roles de instancia** **510**

**Crear un StyleBook para realizar operaciones que no sean CRUD** **518**

**Migrar el paquete de configuración de un StyleBook a otro StyleBook** **519**

**Usar API para crear configuraciones a partir de StyleBooks** **526**

**Usar API para crear configuraciones para cargar archivos de certificados y claves** **534**

**Use API para crear configuraciones para cargar cualquier tipo de archivo** **536**

**Usar API para importar StyleBooks personalizados** **537**

**Usar API para descargar StyleBooks personalizados** **538**

**Usar API para eliminar StyleBooks personalizados** **539**

**Gramática de StyleBooks** **541**

**Header** **543**

**Importar StyleBooks** **544**

**Parámetros** **545**

**Construcción Parameters-Default-sources** **558**

**Sustituciones** **561**

**Componentes** **566**

**Componentes auxiliares** **567**

**Propiedades opcionales** **569**

**Properties-default-sources construct** **570**

**Componentes anidados** **572**

**Construcción de condición** **573**

**Repetir componente fijo** **574**

**Construcción de condición de repetición** **577**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Repeticiones anidadas** 577

**Resultados** 579

**Referencia de parámetros** 580

**Referencia de principal** 581

**Referencia de componentes** 582

**Referencia de sustituciones** 583

**Referencia de variable** 583

**Operaciones** 584

**Análisis** 586

**Alarmas** 588

**Expresiones** 591

**Interpolaciones in situ** 597

**Funciones integradas** 600

**Detección de dependencias** 613

**Administración de instancias** 615

**Supervisar sitios distribuidos globalmente** 618

**Cómo crear etiquetas y asignar a instancias** 624

**Cómo buscar instancias mediante valores de etiquetas y propiedades** 627

**Administrar particiones de administración de instancias NetScaler ADC** 630

**Crear un par de alta disponibilidad de NetScaler ADC** 635

**Realizar copias de seguridad y restaurar instancias de NetScaler ADC** 639

**Forzar una conmutación por error a la instancia secundaria de NetScaler ADC** 647

**Forzar una instancia secundaria de NetScaler ADC para que permanezca secundaria** 648

**Crear grupos de instancias** 649

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Aprovisionar instancias VPX de ADC en SDX mediante ADM** 650

**Aprovisionamiento de instancias de NetScaler ADC VPX en VMware ESX** 661

**Redescubrir varias instancias de Citrix VPX** 669

**Desadministrar una instancia** 670

**Rastrear la ruta a una instancia** 671

**Asesoramiento de actualización** 672

**Asesoramiento de seguridad** 674

**Eventos** 675

**Usar panel de eventos** 676

**Establecer la edad del evento para los eventos** 677

**Programar un filtro de eventos** 679

**Establecer notificaciones de correo electrónico repetidas para eventos** 680

**Suprimir eventos** 682

**Crear reglas de eventos** 683

**Modificar la gravedad reportada de los eventos que se producen en instancias de NetScaler ADC** 698

**Ver resumen de eventos** 699

**Mostrar severidades de eventos y detalles de capturas SNMP** 701

**Ver y exportar mensajes syslog de Citrix ADC** 703

**Suprimir mensajes de syslog** 707

**Configurar los parámetros de poda para eventos de instancia** 709

**Administración de certificados SSL** 710

**Usar el panel SSL** 717

**Configurar notificaciones para la caducidad del certificado SSL** 722

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Actualizar un certificado instalado** 724

**Instalar certificados SSL en una instancia de NetScaler ADC** 724

**Crear una solicitud de firma de certificados (CSR)** 726

**Vincular y desvincular certificados SSL** 729

**Configurar una directiva de empresa** 729

**Encuesta de certificados SSL de instancias Citrix ADC** 730

**Configurar la administración de direcciones IP (IPAM)** 731

**Trabajos de configuración** 734

**Crear un trabajo de configuración** 736

**Usar grabación y reproducción para crear trabajos de configuración** 740

**Utilizar trabajos de configuración para replicar la configuración de una instancia a varias instancias** 745

**Usar variables en trabajos de configuración** 748

**Crear trabajos de configuración a partir de comandos correctivos** 754

**Replicar la configuración en ejecución y guardada de una instancia de Citrix ADC a otra** 756

**Reutilizar trabajos de configuración de ejecución** 757

**Programar trabajos creados mediante plantillas integradas** 759

**Utilizar trabajos de mantenimiento para actualizar instancias de NetScaler ADC SDX** 761

**Crear trabajos de configuración para instancias Citrix SD-WAN WANOP** 762

**Utilizar la plantilla de configuración maestra** 767

**Usar trabajos para actualizar instancias de Citrix ADC** 774

**Usar plantillas de configuración para crear plantillas de auditoría** 781

**Usar el comando SCP (put) en trabajos de configuración** 784

**Reprogramar trabajos configurados mediante plantillas integradas** 787

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Reutilizar plantillas de auditoría de configuración en trabajos de configuración** 788

**Importar y exportar plantillas de configuración** 792

**Trabajos de mantenimiento** 794

**Auditoría de configuración** 802

**Crear plantillas de auditoría** 803

**Ver informes de auditoría** 808

**Auditar los cambios de configuración en todas las instancias** 813

**Obtener consejos de configuración sobre la configuración de la red** 818

**Auditoría de configuración de sondeo de instancias NetScaler ADC** 820

**Generar diferencias de auditoría de configuración para capturas SNMP de ConfigChange** 822

**Funciones de red** 823

**Generar informes para entidades de equilibrio de carga** 823

**Exportar o programar la exportación de informes de funciones de red** 827

**Informes de red** 830

**Utilice los registros de auditoría de ADM para administrar y supervisar su infraestructura** 841

**Análisis** 844

**Requisitos de licencia** 845

**Visión general de Logstream** 847

**Inhabilitar la recopilación de datos de URL** 849

**Crear umbrales y alertas** 850

**Configurar umbrales adaptativos** 851

**Configurar la persistencia de la base de datos** 852

**Diagnósticos de autoservicio para Analytics** 853

**Información web** 857

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Solucionar problemas de Web Insight** 870

**HDX Insight** 874

**Habilitar la recopilación de datos de HDX Insight** 881

**Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto único** 893

**Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo transparente** 894

**Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto doble** 896

**Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo de usuario LAN** 901

**Crear umbrales y configurar alertas para HDX Insight** 904

**Visualización de informes y métricas de HDX Insight** 908

**Informes y métricas de vista de aplicaciones** 954

**Informes y métricas de Desktop View** 962

**Informes y métricas de visualización de usuarios** 975

**Informes y métricas de vista de instancias** 992

**Informes y métricas de vista de licencias** 999

**Solucionar problemas de HDX Insight** 1000

**Gateway Insight** 1014

**Solucionar problemas de Gateway Insight** 1034

**Security Insight** 1038

**Bot** 1050

**Ver detalles de infracciones de seguridad de la aplicación** 1057

**Insight SSL** 1058

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Información TCP** 1065

**WAN Insight** 1070

**Video Insight** 1072

**Ver la eficiencia de la red** 1075

**Compare el volumen de datos utilizado por los videos ABR optimizados y no optimizados** 1076

**Ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red** 1078

**Compare el tiempo de reproducción optimizado y no optimizado de los vídeos ABR** 1081

**Compare el consumo de ancho de banda de vídeos ABR optimizados y no optimizados** 1084

**Compare el número optimizado y no optimizado de reproducciones de videos ABR** 1086

**Ver la velocidad máxima de datos para un período de tiempo específico** 1089

**Análisis de proxy de reenvío SSL** 1092

**Paneles** 1093

**Casos de uso** 1099

**Orchestration** 1111

**OpenStack: Integración de instancias NetScaler ADC** 1113

**Requisitos previos** 1117

**Tareas previas a la configuración en NetScaler ADM y OpenStack** 1118

**Configurar LBaaS V1 mediante Horizon** 1130

**Configurar LBaaS V2 mediante la línea de comandos** 1130

**Configurar la conmutación de contenido de capa 7** 1135

**Provisioning manual de la instancia NetScaler ADC VPX en OpenStack** 1143

**Aprovisionamiento de la instancia NetScaler ADC VPX en OpenStack mediante StyleBook** 1146

**Licencia de check-in y check-out VPX y soporte de licencias agrupadas para el entorno OpenStack** 1147

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Compatibilidad con VLAN compartida para particiones de administración** **1150**

**Flujo de trabajo de licencias de prueba** **1153**

**Integración con los servicios de OpenStack Heat** **1154**

**Directivas de aislamiento de paquetes de servicio** **1160**

**Asignación flexible de dispositivos basada en directivas** **1163**

**NSX Manager: Provisioning manual de instancias de NetScaler ADC** **1168**

**NSX Manager: Provisioning automático de instancias de NetScaler ADC** **1185**

**Automatización de Citrix ADC mediante Citrix ADM en el modo híbrido ACI de Cisco** **1197**

**Requisitos previos** **1199**

**Configurar NetScaler ADC en modo híbrido mediante Cisco APIC y NetScaler ADM** **1200**

**Crear un StyleBook para una aplicación mediante NetScaler ADM** **1200**

**Importar paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC** **1201**

**Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC** **1202**

**Agregar NetScaler ADC como dispositivo en Cisco ACI mediante APIC** **1206**

**Crear e implementar un gráfico de servicio** **1210**

**Configure los parámetros L4-L7 desde NetScaler ADM con StyleBook** **1221**

**Adjuntar y desenlazar eventos de punto final de APIC** **1225**

**Informes de fallos de APIC** **1226**

**Registros generados por NetScaler ADM** **1226**

**Registros generados por el paquete de dispositivos de modo híbrido** **1231**

**Paquete de dispositivos NetScaler ADC en el modo de orquestación de nube de ACI de Cisco** **1235**

**Administrar la configuración de Kubernetes Ingress en NetScaler ADM** **1240**

**Capacidad agrupada de NetScaler ADC** **1246**

**Configurar la capacidad agrupada de Citrix ADC** **1254**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Configurar un servidor ADM solo como servidor de licencias agrupado** 1260

**Actualizar una licencia perpetua en NetScaler ADC VPX a la capacidad agrupada de NetScaler ADC** 1262

**Actualización de una licencia perpetua en NetScaler ADC MPX a la capacidad agrupada de NetScaler ADC** 1268

**Actualizar una licencia perpetua en un NetScaler ADC SDX a la capacidad agrupada de NetScaler ADC** 1276

**Capacidad agrupada de NetScaler ADC en instancias de NetScaler ADC en modo de clúster** 1278

**Supervisión de estado** 1282

**Comportamientos esperados cuando surgen problemas** 1284

**Configurar comprobaciones de caducidad para licencias de capacidad agrupadas** 1285

**Registre y desproteja las licencias de NetScaler ADC VPX y BLX** 1286

**Licencias de CPU virtual NetScaler ADC** 1295

**Administrar instancias de Citrix SD-WAN** 1301

**Agregar instancias de Citrix SD-WAN** 1305

**Ver los datos de análisis de Citrix SD-WAN para la implementación de varios saltos** 1308

**Ver informes de eventos para instancias de Citrix SD-WAN WANOP** 1310

**Ver informes de red para instancias de Citrix SD-WAN WANOP** 1310

**Respaldar instancias de Citrix SD-WAN WANOP** 1312

**Administrar instancias de HAProxy** 1317

**Agregar instancias de HAProxy a NetScaler ADM** 1317

**Panel de aplicación HAProxy** 1319

**Licencias de terceros** 1320

**Control de acceso basado en roles para instancias de HAProxy** 1322

**Supervisar instancias de HAProxy** 1322

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ver los detalles de front-ends configurados en instancias HAProxy** 1323

**Ver los detalles de back-ends configurados en instancias HAProxy** 1323

**Ver los detalles de los servidores configurados en instancias HAProxy** 1323

**Ver las instancias HAProxy con el mayor número de servidores o front-ends** 1324

**Reiniciar una instancia de HAProxy** 1324

**Realizar una copia de seguridad y restaurar una instancia de HAProxy** 1325

**Modificar el archivo de configuración HAProxy** 1326

**Administrar la configuración del sistema** 1327

**Configurar las opciones de copia de seguridad del sistema** 1333

**Configurar un servidor NTP** 1334

**Actualización de Citrix Application Delivery Management (ADM)** 1336

**Cómo restablecer la contraseña para Citrix ADM** 1336

**Configurar una NIC doble para acceder a NetScaler ADM** 1344

**Configurar el intervalo de depuración de syslog** 1346

**Configurar los parámetros de poda del sistema y de poda de eventos** 1347

**Habilitar el acceso al shell para usuarios no predeterminados** 1350

**Recuperar servidores NetScaler ADM inaccesibles** 1350

**Asignar un nombre de host a un servidor NetScaler ADM** 1356

**Copia de seguridad y restauración del servidor NetScaler ADM** 1356

**Ver información de auditoría** 1361

**Configurar la configuración de SSL** 1362

**Supervisar el uso de CPU, memoria y disco** 1363

**Configurar las opciones de notificación** 1364

**Generar un archivo de soporte técnico** 1369

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Configurar un grupo de cifrado** **1371**

**Crear destino de capturas SNMP, comunidad de administradores y usuarios** **1372**

**Configurar y ver alarmas del sistema** **1373**

**NetScaler ADM como servidor proxy API** **1375**

**Visualice problemas con Infrastructure Analytics** **1381**

**Ver detalles de instancia en Infrastructure Analytics** **1407**

**Ver los problemas de capacidad en una instancia de ADC** **1413**

**Análisis de infraestructura mejorado con nuevos indicadores** **1416**

**Preguntas frecuentes** **1419**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Notas de la versión

August 23, 2024

Las notas de la versión de Citrix Application Delivery Management (ADM) 13.0 describen las nuevas funciones, las mejoras de las funciones existentes y los problemas conocidos de una compilación. El documento de notas de la versión 13.0 incluye las siguientes secciones:

- **Novedades**: Las nuevas funciones y mejoras de las funciones existentes publicadas en una compilación.
- **Problemas conocidos**: Los problemas que existen en una compilación y sus soluciones, siempre que corresponda.
- **Problemas resueltos**: Los problemas abordados en una compilación.

Para ver el documento de notas de la versión de una compilación específica de la versión 13.0, haga clic en el enlace correspondiente de la tabla siguiente. Cuando se actualizan las notas de la versión de una compilación, también se actualizan el número de versión de las notas de la versión y la fecha de publicación. Es posible que la fecha de publicación de las notas de la versión no sea la misma que la fecha de compilación de GA.

| Notas de publicación de la versión 13.0 del software NetScaler ADM local | Fecha de publicación | Versión |
|---|---|---|
| Compilación 13.0-92.31 | 09 de julio de 2024 | 1.0 |
| Compilación 13.0-91.12 | 18 de mayo de 2023 | 1.0 |
| Compilación 13.0-90.7 | 01 de febrero de 2023 | 1.0 |
| Compilación 13.0-89.7 | 19 de diciembre de 2022 | 1.0 |
| Compilación 13.0-88.12 | 20 de octubre de 2022 | 1.0 |
| Compilación 13.0-87.9 | 06 de febrero de 2023 | 2.0 |
| Compilación 13.0-86.17 | 20 de junio de 2022 | 1.0 |
| Compilación 13.0-85.19 | 14 de junio de 2022 | 1.0 |
| Compilación 13.0-84.10 | 14 de diciembre de 2021 | 1.0 |
| Compilación 13.0-83.27 | 28 de septiembre de 2021 | 1.0 |
| Compilación 13.0-82.41 | 09 de junio de 2021 | 1.0 |
| Compilación 13.0-79.64 | 06 de abril del 2021 | 1.0 |
| Compilación 13.0-76.29 | 19 de febrero de 2021 | 1.0 |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Notas de publicación de la versión 13.0 del software NetScaler ADM local | Fecha de publicación | Versión |
|---|---|---|
| Compilación 13.0-71.40 | 20 de enero de 2021 | 2.0 |
| Compilación 13.0-67.42 | 28 de octubre de 2020 | 1.0. |
| Compilación 13.0-64.35 | 16 de octubre de 2020 | 2.0 |
| Compilación 13.0-61.48 | 18 de septiembre de 2020 | 2.0 |
| Compilación 13.0-58.30 | 10 de junio de 2020 | 1.0 |
| Compilación 13.0-52.24 | 26 de marzo de 2020 | 1.0 |
| Compilación 13.0-47.22 | 10 de diciembre de 2019 | 1.0 |
| Compilación 13.0-41.28 | 27 de septiembre de 2019 | 1.0 |

> **Nota**
>
> Estas notas de la versión no documentan las correcciones relacionadas con la seguridad. Para obtener una lista de correcciones y avisos relacionados con la seguridad, consulte el boletín de seguridad de Citrix.

## Migración local de NetScaler ADM a Citrix Cloud

August 23, 2024

Puede migrar **NetScaler ADM 13.0 64.35 local o una versión posterior** a Citrix Cloud. Si su ADM tiene 12.1 o una versión anterior, primero debe actualizar a **13.0 64.35 o una versión posterior** y, a continuación, migrar a Citrix Cloud. Para obtener más información, consulte la sección Actualización.

El servicio ADM a través de Citrix Cloud le permite obtener:

- Lanzamientos más rápidos, aproximadamente cada dos semanas con las últimas actualizaciones de funciones.
- Análisis basado en aprendizaje automático para seguridad de aplicaciones y bot, rendimiento y uso.
- Varias otras funciones que actualmente solo se admiten en el servicio ADM, como análisis de períodos de pico y lean, análisis basado en aprendizaje automático para seguridad de aplicaciones y bot, análisis de CPU de aplicaciones y muchas más.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para una migración correcta, debe:

- Asegúrese de tener conexión a Internet en ADM local para la accesibilidad de Citrix Cloud
- Configurar el agente de servicio ADM
- Obtenga el cliente y el archivo CSV secreto de Citrix Cloud
- Validar las licencias de servicio ADM
- Migrar mediante un script

Después de migrar de ADM local a un servicio ADM, si quiere volver a continuar con ADM local, puede usar el script de reversión. Para obtener más información, consulte Volver a ADM local.

### Configurar el agente de servicio ADM

Para habilitar las comunicaciones entre las instancias de NetScaler ADC y NetScaler ADM, debe configurar un agente. De forma predeterminada, los agentes de NetScaler ADM se actualizan automáticamente a la versión más reciente. También puede seleccionar una hora específica para la actualización del agente. Para obtener más información, consulte Configuración de los valores de actualización del agente.

- Si el ADM local existente (par independiente o HA) no tiene agentes locales configurados, debe configurar al menos un agente para el servicio ADM.
- Si el ADM local existente (par independiente o HA) se ha configurado con agentes locales para implementaciones multisitio, debe configurar el mismo número de agentes para el servicio ADM.

Para obtener más información sobre la configuración de un agente, consulte la sección Introducción.

### Obtenga el cliente y el archivo CSV secreto de Citrix Cloud

Después de configurar el agente, obtenga el cliente y el archivo CSV secreto de la página de Citrix Cloud:

1. Inicie sesión en citrix.cloud.com
2. Haga clic en el icono **Inicio** y seleccione **Administración de identidades y accesos**.
3. En la ficha **Acceso API**, introduzca un nombre de cliente seguro y haga clic en **Crear cliente**.
4. Se generan ID y Secret. Haga clic en **Descargar** y guarde el archivo CSV en el ADM local.

   Por ejemplo, guarde el archivo CSV en el directorio /var.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Validar las licencias de servicio ADM

Debe obtener licencias para el servicio ADM.

- Las licencias VIP en el servicio ADM deben ser superiores o iguales a las licencias VIP locales.

  > **Nota**
  >
  > Si las licencias VIP son menores, los servidores virtuales se seleccionan aleatoriamente y se produce un error en la configuración de nivel VIP para el servicio ADM.

- Si utiliza la implementación local de ADM como servidor de licencias, reasigne las licencias al servicio ADM antes de la migración. Para obtener más información, consulte Configurar un servidor ADM solo como servidor de licencias agrupado y Cómo reasignar un archivo de licencias.
- Si utiliza las licencias agrupadas en ADM local, debe obtener las licencias agrupadas para el servicio ADM y, a continuación, asignar licencias a las instancias de ADC. Para obtener más información, consulte Configurar licencias agrupadas. Las siguientes versiones admitidas de ADC permiten modificar la asignación de licencias desde ADM:
  - NetScaler ADC SDX: 13.0 74.11 o versiones posteriores.
  - NetScaler ADC VPX y MPX: 13.0 47.24 o versiones posteriores, 12.1 58.14 o versiones posteriores y 11.1 65.10 o versiones posteriores.

### Migrar mediante un script

- Con la compilación ADM 82.x, puede seleccionar la función y, a continuación, migrar.
- Para las compilaciones ADM 76.x o posteriores, los scripts de migración (`servicemigrationtool.py` y `config_collect_onprem.py`) están disponibles como parte de la compilación, disponible en `cd /mps/scripts`.
- Para compilaciones de ADM anteriores a 76.x, debe descargar los scripts de migración y copiar los scripts en ADM local.

  > Nota
  >
  > Asegúrese de que el ADM local tenga conectividad a Internet durante la migración.

1. Con un cliente SSH, inicie sesión en el ADM local.

   > Nota
   >
   > Para un par ADM HA, inicie sesión en el nodo principal.

2. Escribe **shell** y presiona **Entrar** para cambiar al modo bash.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Copie el ID de cliente y el archivo CSV secreto. Por ejemplo, copie el archivo en el directorio /var.

   Después de copiar el archivo CSV, puede validar si el archivo CSV está presente.

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```

> Nota
>
> Para un par ADM HA, copie el archivo CSV en el nodo principal.

4. Para la **versión ADM 13.0 82.xx**, ejecute los siguientes comandos para completar la migración:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

   Por ejemplo, `python servicemigrationtool.py /var/secureclient.csv`

   Después de ejecutar el script de migración, la herramienta muestra las siguientes opciones:

```
-----------------------------------------------------
Checking For Pre-requisites before we start the Migration
-----------------------------------------------------

The no.of Agents in ADM Service are :1


VIP licenses available in ADM Service are: 2

No.of Vservers Licensed in ADM on-prem are: 72


All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
vServers will be licensed randomly. Do you want to continue ? [Y|N] y


User has started rerunning the migration.Providing the all options


-------------------------------------------------------------------------------
Citrix ADM on-prem to ADM Service Configuration Migration.
The following menu enables you to select the components to migrate.
Type the number of the component that you want to migrate, and then press Enter.
For example, type 1 if you want to migrate Management and Monitoring(M&M).
-------------------------------------------------------------------------------

    1. Management and Monitoring(M&M).
    2. Analytics.
    3. Stylebooks.
    4. PooledLicensing.
    5. All.

Select an option from 1 to 5 [1]: 1
```

   Según la opción que proporcione, solo esa función se migra al servicio ADM.

   En el ejemplo, se selecciona la opción 1. La herramienta completa la migración de Administración y supervisión (M&M) y muestra el siguiente mensaje:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
1. Management and Monitoring Module Migration to ADM Service is Complete.
=====================================================================


ADCs,SDXs and SDWANOPs Addition and their SNMP,Syslog Configurations to ADM Service are Successful. Tool will now disable System Features in ADM on-prem

Device_Events : ['SUCCESS']
Device_SSL_Cert : ['SUCCESS']
Device_Syslog : ['SUCCESS']
Device_Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device_Perf_Reporting : ['SUCCESS']
Device_Config_Audit : ['SUCCESS']
Emon_Scheduler : ['SUCCESS']

Disable Status of ADM System Features: {'Device_Events': "['SUCCESS']", 'Device_SSL_Cert': "['SUCCESS']", 'Device_Syslog': "['SUCCESS']", 'Device_Backup': "['SUCCESS']", 'AgentCluster':
 "['SUCCESS']", 'Device_Perf_Reporting': "['SUCCESS']", 'Device_Config_Audit': "['SUCCESS']", 'Emon_Scheduler': "['SUCCESS']"}
1620286058


=============================================================
ADM on-prem to ADM service Migration is Successfully Completed.
=============================================================



-------------------------------------------------------------------------------
ADM On-rem to ADM Service Configuration Migration is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
-------------------------------------------------------------------------------
```

La función **de gestión y supervisión (M&M)** incluye:

- Instancias ADC, etiquetas, grupos de instancias, perfiles, aplicaciones personalizadas, trabajos de configuración, SNMP, configuraciones de syslog.
- Sitios, bloqueos de IP, informes de red, umbrales de análisis, configuración de notificaciones, configuración de eliminación de datos.
- Configura plantillas de auditoría, intervalos de sondeo, reglas de eventos y ajustes.
- Grupos, roles y directivas de RBAC

La función de **análisis** incluye:

- Configuración de Appflow por servidor virtual desde instancias de ADC.
- Configuración de Appflow por dispositivo SD-WAN.

> Nota:
>
> - La función Administración y supervisión (M&M) se migra automáticamente, incluso si selecciona cualquier otra función (2, 3 o 4).
> - Solo puede especificar una función a la vez.
> - Después de completar la migración de cualquier función, si quiere migrar cualquier otra función más adelante, la función que ya se ha migrado no se muestra en la lista. Por ejemplo, si primero completa la migración de la función de **Analytics**, la próxima vez que ejecute el script de migración, solo podrá ver las opciones **StyleBooks**, **Licencias agrupadas** y **Todo**.

5. Para la **versión de ADM 13.0 76.xx**, ejecute los siguientes comandos para completar la migración:

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Por ejemplo, `python servicemigrationtool.py /var/secureclient.csv`

6. Para ADM anterior a 13.0 76.xx versión:

   a) Descargue el script de migración desde la siguiente ubicación: `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

      The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `config_collect_onprem_27.py`.

   b) Guarde los dos scripts en ADM local. Por ejemplo, guarde en el directorio /var

   c) Ejecute los siguientes comandos para migrar:

      i. `cd /var`

      ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

      Por ejemplo, `python servicemigrationtool_27.py /var/secureclient.csv`

Después de ejecutar el script, comprueba los requisitos previos y, a continuación, procede con la migración. En primer lugar, el script comprueba la disponibilidad de la licencia. El siguiente mensaje solo se muestra si tiene una licencia de servicio ADM menor que la licencia local.

```
bash-3.2# python servicemigrationtool.py /var/baga.csv

 Trying to Get the Customer Id...


 The Customer Id: iaahfc73d8f4

 ADM Service FQDN: baga.adm.cloud.com

 The ADM on-prem IP: 10.106.150.37


 Citrix ADM Deployed with No Agents



-------------------------------------------------------
Checking For Pre-requisites before we start the Migration
-------------------------------------------------------

 The no.of Agents in ADM Service are :1


 VIP licenses available in ADM Service are: 2

 No.of Vservers Licensed in ADM on-prem are: 26


 All the vServers licensed in ADM on-prem will not be licensed in ADM Service since licenses available in service is less.
 vServers will be licensed randomly. Do you want to continue ? [Y|N]
```

Si selecciona **Y**, la migración continúa otorgando licencias al VIP aleatoriamente. Si selecciona **N**, el script detiene la migración.

Si tiene la versión de instancia ADC no compatible para el servidor de licencias agrupado, aparecerá el siguiente mensaje:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
Changing of PooledLicense Server will be effective for below SDX/ADC versions
-----------------------------------------------------------------------------
  For SDX Versions: 13.0 74.11 Onwards
  For ADC Versions: 13.0 47.24 and Onwards
                    12.1 58.14 and Onwards
                    11.1 65.10 and Onwards
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------

 The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

 The List of SDXs supported for Pooled License Server change are:
[]

 The List of ADCs not supported for Pooled License Server change are:
[]

 The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

 Migration will change the License Server to ADM Service Agent.
 Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

 Do you want to continue with rest of the migration ? [Y|N]
```

Si selecciona **Y**, el proceso de migración continúa cambiando el servidor de licencias. Si selecciona **N**, el script le preguntará si quiere continuar con el resto de la migración. El script detiene la migración si selecciona **N**.

Dependiendo de la configuración local, el tiempo aproximado para completar la migración es entre unos minutos y unas horas. Una vez completada la migración, verá el siguiente mensaje:

```
-------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
-------------------------------------------------------------------------------
```

La migración se realiza correctamente una vez que todas las instancias de ADC y SD-WAN WANOP y sus respectivas configuraciones se mueven correctamente al servicio ADM. Después de la migración correcta, NetScaler ADM local deja de procesar los siguientes eventos de instancia:

- Certificados de SSL
- Mensajes de Syslog
- Backup
- Cluster de agentes
- Informes de rendimiento
- Auditoría de configuración
- Emon programador

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Volver a ADM local

Si quiere volver a ADM local, asegúrese de que se cumplan los requisitos previos.

### Requisitos previos

Si su ADM local (antes de migrar al servicio ADM) es:

- Si se utiliza como servidor de licencias agrupadas, asegúrese de tener las licencias agrupadas necesarias en la ADM local.
- Configurado con agentes ADM locales, asegúrese de que los agentes estén disponibles en estado "ACTIVO".

### Usar el script de reversión

> Nota
>
> Después de la reversión, las mismas configuraciones (antes de la migración) en Analytics, SNMP y las licencias agrupadas vuelven a estar disponibles en ADM local. Si ha realizado algún cambio en estas configuraciones después de la migración, estos cambios no se reflejan en ADM local.

- Para compilaciones de **ADM 82.xx o posteriores**, el script de reversión está disponible como parte de la compilación y se puede acceder a él en `/mps/scripts`.
- Para compilaciones de **ADM anteriores a 79.xx**, puede actualizar a la compilación 82.x y usar el script de rollback o puede descargar el script de rollback y copiar el script en ADM local.

1. Con un cliente SSH, inicie sesión en el ADM local.
2. Escribe shell y presiona Enter para cambiar al modo bash.
3. Para la compilación ADM **13.0 82.xx**, ejecute los siguientes comandos para completar la reversión:

   a) cd /mps/guiones

   b) python rollback_to_onprem.py <`path of ClientID/Secret File in ADM on-prem VM`>

   Por ejemplo, `python rollback_to_onprem.py /var/ secureclient.csv.csv`

   La herramienta inicia la operación de reversión y un mensaje le pregunta si quiere continuar. Escriba **Y** para continuar.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
bash-3.2# python rollback_to_onprem.py /var/tmp/baga_prod.csv

The Customer Id: iaahfc73d8f4

ADM Service FQDN: baga.adm.cloud.com

The ADM on-prem IP: 10.106.150.10

-----------------------------------------------------------------------------------------------------------------------------------------------------------
On successful rollback operation,Instances will be removed from ADM Service. SNMP,Syslog,Analytics configurations and Pooled Licensing Server in Instances will point to on-prem ADM Serv
er and reports will be shown in ADM on-prem.
-----------------------------------------------------------------------------------------------------------------------------------------------------------


Do you want to proceed for roll back operation from ADM Service to ADM on-prem ? [Y|N] y

-----------------------------------------------------------------------------
```

Puede ver el siguiente mensaje después de que se complete la reversión.

```
==========================Rollback Status Check================================


Removal of ADCs,SDXs,SDWANOPs and their respective Configurations from ADM Service are Successful.


Rollback operation from ADM Service to ADM on-prem is Successful


Enabling System features in ADM on-prem Server
Device_Events : ['SUCCESS']
Device_SSL_Cert : ['SUCCESS']
Device_Syslog : ['SUCCESS']
Device_Backup : ['SUCCESS']
AgentCluster : ['SUCCESS']
Device_Perf_Reporting : ['SUCCESS']
Device_Config_Audit : ['SUCCESS']
Emon_Scheduler : ['SUCCESS']

Enable Status of ADM System Features: {'Device_Events': "['SUCCESS']", 'Device_SSL_Cert': "['SUCCESS']", 'Device_Syslog': "['SUCCESS']", 'Device_Backup': "['SUCCESS']", 'AgentCluster':
"['SUCCESS']", 'Device_Perf_Reporting': "['SUCCESS']", 'Device_Config_Audit': "['SUCCESS']", 'Emon_Scheduler': "['SUCCESS']"}

-----------------------------------------------------------------------------------------
ADM Service to ADM on-prem Rollback operation is Complete.
Note: Please look out for failures and re-trigger the Tool after taking appropriate action.
-----------------------------------------------------------------------------------------

bash-3.2#
```

4. Para la compilación ADM anterior a la versión 82.xx:

   a) Descargue el script de reversión desde la siguiente ubicación:

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   b) Para las compilaciones de ADM 79.xx y 76.xx, guarde el script `/mps/scripts` y ejecute los siguientes comandos para la reversión:

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

      Por ejemplo, `python rollback_to_onprem.py /var/ secureclient.csv`

   c) Para compilaciones de ADM anteriores a 76.xx, guarde el script en ADM local. Por ejemplo, guárdelo en la ubicación `/var` y ejecute los siguientes comandos para la reversión:

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

      Por ejemplo, `python rollback_to_onprem_27.py /var/secureclient.csv`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La herramienta inicia la operación de reversión y un mensaje le pregunta si quiere continuar. Escriba **Y** para continuar.

## Preguntas frecuentes

August 23, 2024

### Servicio ADM

#### ¿El agente de servicio ADM es opcional similar al agente de NetScaler ADM local?

No. El agente de servicio ADM es obligatorio para el servicio ADM y todas las comunicaciones entre instancias y el servicio ADM se producen a través del agente de servicio ADM. El agente ADM local es opcional; sin embargo, puede configurar el agente local solo para ahorrar el consumo de ancho de banda.

#### ¿Por qué el servicio ADM?

El servicio ADM a través de Citrix Cloud ofrece las siguientes ventajas, sin necesidad de nuevas compilaciones periódicas:

- Oferta SaaS basada en la nube con incorporación más fácil y menor coste de propiedad que el NetScaler ADM local.
- Lanzamientos más rápidos, aproximadamente cada dos semanas con las últimas actualizaciones de funciones.
- Análisis basado en aprendizaje automático para la seguridad, el rendimiento y el uso de las aplicaciones.
- Varias otras funciones que actualmente solo se admiten en el servicio ADM, como análisis de períodos pico y lean, análisis de seguridad de aplicaciones basadas en aprendizaje automático para WAF y bot, análisis de CPU de aplicaciones y muchas más.

También puede unirse al seminario web mensual del servicio NetScaler ADM para conocer las últimas funciones y soluciones del producto. Regístrese en el seminario web mediante el siguiente enlace:

`https://attendee.gotowebinar.com/register/4248811314610265355`

O bien:

`https://attendee.gotowebinar.com/register/1601431406507289611`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

#### ¿Qué ocurre después de la migración si NetScaler ADM local es un par HA?

Todas las configuraciones se mueven a Citrix Cloud. No es necesario configurar un nodo de recuperación ante desastres.

#### ¿Qué pasa si el agente cae por alguna razón?

Puede esperar una posible pérdida de datos hasta que el agente esté en funcionamiento. Sin embargo, también puede configurar agentes ADM para implementaciones multisitio para garantizar la continuidad si hay una conmutación por error del agente. Para obtener más información, consulte Configurar agentes ADM para la implementación en varios sitios.

#### ¿También se migra la copia de seguridad de instancias?

La copia de seguridad no se incluye en la migración.

#### ¿También se migran los datos históricos?

Los datos históricos no se migran. Puede exportar los datos desde el ADM local.

#### ¿También se migran las licencias locales?

No. El archivo de licencia local no se puede utilizar para el servicio ADM. Debe obtener licencias para el servicio ADM. Para obtener más información, consulte Licencias. Si utiliza licencias agrupadas en ADM local, debe obtener licencias agrupadas para el servicio ADM y, a continuación, asignar licencias a instancias.

#### ¿Qué no se migra desde NetScaler ADM local?

Las siguientes funciones no se pueden migrar al servicio ADM:

- **RBAC**: En el servicio ADM, el acceso del usuario se basa en la invitación del administrador. Los usuarios del servicio ADM deben tener una cuenta en Citrix Cloud. Como resultado, los usuarios de ADM locales no se migran.
- **Exportar programas**: Las programaciones de exportación incluyen detalles como desglose y programaciones de varias páginas. Todas estas programaciones detalladas de exportación no se migran.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Certificados/claves/CSR SSL**: El servicio ADM solo puede mostrar los certificados/claves/-claves/CSR ADC SSL. Como resultado, los certos/claves SSL cargados en NetScaler ADM local no se migrarán al servicio ADM.

**NetScaler ADM local está integrado con Citrix Director. ¿Qué pasa con la integración?**

Actualmente, la integración de Director con ADM solo se admite en ADM local.

**Después de la migración, ¿se requiere de nuevo la licencia de la instancia o habilitar el análisis?**

Debe asegurarse de que las licencias del servicio ADM sean superiores o iguales a las licencias VIP locales. Si las licencias ya son superiores a la VIP local de NetScaler ADM, los servidores virtuales se otorgan automáticamente a los servidores virtuales. De lo contrario, las licencias se asignan aleatoriamente.

## Herramienta de migración

**Después de ejecutar el script de migración, se muestran los mensajes de error. ¿Cuál puede ser el problema?**

Se muestra un archivo de registro con motivos de error. Puede realizar las acciones correctivas adecuadas y ejecutar de nuevo el script de migración. En general, antes de ejecutar el script de migración, asegúrese de:

- Configurar el agente de servicio ADM
- Obtener las licencias de servicio ADM
- Copie la ruta correcta donde ha almacenado el cliente y archivo CSV seguro

**Las instancias de ADC tienen versiones inferiores a la limitación mencionada para licencias agrupadas. ¿Qué sucede si se selecciona la opción "Y"para cambiar el servidor de licencias?**

El cambio del servidor de licencias solo se realiza para las versiones de NetScaler ADC MPX, VPX y SDX compatibles.

**¿Qué sucede si el script de migración ha fallado la configuración con respecto a las instancias WANOP de ADC/SD-WAN?**

Las instancias WANOP de ADC y SD-WAN continúan funcionando en la configuración local de ADM. Puede tomar las medidas necesarias a partir del motivo de error sugerido y volver a ejecutar el script

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

de migración.

**¿Qué sucede si algunas de las instancias WANOP de ADC o SD-WAN no se mueven al servicio ADM? ¿Ayudará la reejecución del script de migración?**

Sí. Después de volver a ejecutar el script, solo se migran las instancias fallidas. Supongamos que dos de cada cinco instancias no han podido moverse. Después de realizar acciones correctivas y volver a ejecutar el script de migración, tres instancias que se movieron correctamente anteriormente muestran el mensaje "El dispositivo ya existe". Y las otras dos instancias que fallaron anteriormente se migran correctamente.

**¿Hay un archivo de registro para comprobar el estado de la migración?**

Sí, se genera un archivo de registro en el `/var/mps/log/` directorio. ADM con python3.7 tiene el archivo de registro como `servicemigrationtool.py.log` y ADM con python 2.7 tiene el archivo de registro como `servicemigrationtool_27.py.log`.

**¿Qué sucede si la sesión termina mientras se ejecuta el script de migración?**

Puede volver a ejecutar el script de migración. En la nueva sesión, las instancias ya agregadas de la última sesión se muestran como "El dispositivo ya existe"y la migración continúa aún más.

**¿Qué ocurre si el servicio ADM tiene licencias inferiores a las de NetScaler ADM local y se inicia el script de migración?**

Después de ejecutar el script de migración, aparece una sugerencia, mencionando que las licencias son menores y se solicita que continúe o detenga. Si quiere continuar con licencias menores, los servidores virtuales se otorgan licencias aleatoriamente a partir de las licencias disponibles.

**¿Qué ocurre cuando NetScaler ADM local se migra a la cuenta Express del servicio ADM?**

El servicio ADM Express Account solo tiene dos licencias de servidor virtual, dos paquetes de configuración StyleBook y dos trabajos de configuración. Si su ADM local tiene más de estas configuraciones e inicia la migración con Express Account, el script solo puede migrar las configuraciones mencionadas aplicables a Express Account (dos licencias de servidor virtual, dos paquetes de configuración de StyleBook y dos trabajos de configuración)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**¿Qué sucede si un usuario invitado de Citrix Cloud (que no sea el usuario administrador que creó una cuenta de Citrix Cloud) intenta migrar la configuración de ADM local?**

Se recomienda que el administrador ejecute el script de migración. Un usuario invitado no tiene privilegios de administrador (AdminExceptSystem_Group). Como resultado, se produce un error en la migración de grupos, roles y directivas y se muestra el mensaje "El usuario no tiene permiso".

Como solución, el administrador (que creó la cuenta de Citrix Cloud) puede cambiar el grupo asociado con el usuario invitado como "admin_group".

### Guión de reversión

**¿Qué ocurre si el script de reversión se utiliza en el par ADM HA local?**

El par ADM HA local se restaura con todas las configuraciones que estaban disponibles antes de la migración.

**¿Qué ocurre con el nodo de recuperación ante desastres después de usar el script de reversión?**

El nodo de recuperación ante desastres también se restaura con todas las configuraciones antes de la migración

## Solución de problemas

January 30, 2024

Cuando ejecuta el script de migración por primera vez, comprueba los requisitos previos y continúa con la migración. Si se cumplen todos los requisitos previos, la migración se completa sin ningún error. Si falla algún requisito previo, el script muestra mensajes de error con motivos. Después de corregir los errores, debe volver a ejecutar el script.

> Nota
>
> Si aparece un mensaje de error que muestra "ya existe", significa que:
>
> - Es posible que haya ejecutado el script de migración durante más de una vez y algunas configuraciones ya se han migrado al servicio ADM.
> - Es posible que haya creado manualmente la misma configuración en el servicio ADM antes de ejecutar el script de migración.

Consulte algunos de los siguientes mensajes de error:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Perfil manual agregado al servicio ADM

```
==================Profiles Addition to ADM Service=====================


60.26 : FAILURE : Profile 60.26 already exists


 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

**Solución alternativa**: Si ha creado perfiles de administrador en el servicio NetScaler ADM antes de ejecutar el script de migración, asegúrese de eliminar esos perfiles y volver a ejecutar el script de migración.

### Se agregó el dispositivo NetScaler ADC al servicio ADM

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

**Solución alternativa**: en ADM local, asegúrese del estado de la instancia y vea si puede acceder a la instancia sin ningún problema. Si persiste algún problema, solucione el problema y vuelva a ejecutar el script de migración.

### Importación de plantillas personalizadas de StyleBook al servicio ADM

```
==============Stylebook custom templates Import to ADM Service=====================


neustar.citrix.adc.stylebooks_5.0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.

neustar.citrix.adc.stylebooks_5.0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}
==============Stylebook repository Addition to ADM Service=====================
```

**Solución alternativa**: este mensaje de error es un ejemplo para el StyleBook ya migrado. También puede ver este error si ha creado manualmente un StyleBook con el mismo nombre, versión y espacio de nombres, en el servicio NetScaler ADM antes de ejecutar el script de migración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Trabajos de configuración agregados al servicio ADM

```
===============Config Jobs Addition to ADM Service====================

config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

**Solución alternativa**: Este error se produce si se ha suscrito a Express Account y tiene más de dos trabajos de configuración. Debe obtener una suscripción válida para poder migrar todos los trabajos de configuración.

### Bloques IP agregados al servicio ADM

```
====================IP Blocks Addition in ADM Service=======================

ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

**Solución alternativa**: elimine el bloque IP que se crea manualmente en el servicio ADM y vuelva a ejecutar el script de migración.

### Estado de adición del informe del panel de red

```
================Network Dashboard Reports Addition to ADM Service=================

new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Solución alternativa**: Elimine el panel que se crea manualmente en el servicio ADM y vuelva a ejecutar el script de migración.

## Todos los artículos

January 30, 2024

Los «artículos prácticos» de Citrix Application Delivery Management (Citrix ADM) son artículos sencillos, relevantes y fáciles de implementar sobre las funciones de Citrix ADM. Estos artículos contienen información sobre algunas de las funciones más populares de NetScaler ADM, como la administración de instancias, la administración de aplicaciones, los StyleBooks, la administración de certificados y Analytics.

Haga clic en el nombre de una función en la tabla siguiente para ver la lista de artículos prácticos sobre esa función.

| | | Temas | |
|---|---|---|---|
| Administración de instancias | Gestión de eventos | StyleBooks | Administración de certifi |
| Administración de aplicaciones | Administración de la configuración | Autenticación | Análisis |

### Administración de instancias

Cómo supervisar sitios distribuidos globalmente

Cómo administrar las particiones de administración de las instancias de NetScaler ADC

Cómo agregar instancias a NetScaler ADM

Cómo crear grupos de instancias en NetScaler ADM

Cómo configurar sitios para Geomaps en NetScaler ADM

Cómo forzar una conmutación por error a la instancia secundaria de NetScaler ADC mediante NetScaler ADM

Cómo forzar que una instancia secundaria de NetScaler ADC permanezca secundaria mediante NetScaler ADM

Cómo hacer copias de seguridad y restaurar una instancia mediante NetScaler ADM

Cómo utilizar el panel de control de NetScaler ADM para supervisar una instancia de HAProxy

Cómo mostrar los detalles de las interfaces configuradas en las instancias de HAProxy

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cómo mostrar los detalles de los backends configurados en las instancias de HAProxy

Cómo mostrar los detalles de los servidores configurados en las instancias de HAProxy

Cómo reiniciar una instancia de HAProxy desde NetScaler ADM

Cómo hacer una copia de seguridad y restaurar una instancia de HAProxy mediante NetScaler ADM

Cómo editar el archivo de configuración de HAProxy mediante Citrix ADM

Cómo redescubrir varias instancias de NetScaler ADC VPX

Cómo sondear instancias y entidades de NetScaler ADC en NetScaler ADM

Cómo desadministrar una instancia en NetScaler ADM

Cómo rastrear la ruta a una instancia desde NetScaler ADM

## Administración de la configuración

Cómo crear un trabajo de configuración en NetScaler ADM

Cómo usar el comando SCP (put) en trabajos de configuración

Cómo actualizar instancias de NetScaler ADC SDX mediante NetScaler ADM

Cómo programar los trabajos creados mediante plantillas integradas en NetScaler ADM

Cómo reprogramar trabajos configurados mediante plantillas integradas en NetScaler ADM

Cómo reutilizar los trabajos de configuración ejecutados

Cómo actualizar instancias de NetScaler ADC con NetScaler ADM

Cómo usar variables en trabajos de configuración en NetScaler ADM

Cómo usar plantillas de configuración para crear plantillas de auditoría en NetScaler ADM

Cómo crear trabajos de configuración a partir de comandos correctivos en NetScaler ADM

Cómo replicar los comandos de configuración en ejecución y guardados de una instancia de NetScaler ADC a otra en NetScaler ADM

Cómo crear trabajos de configuración para instancias WO de Citrix SD-WAN de Citrix en NetScaler ADM

Cómo utilizar Record-and-Play para crear trabajos de configuración

Cómo utilizar trabajos de configuración para replicar la configuración de una instancia a varias instancias

Cómo utilizar la plantilla de configuración maestra en NetScaler ADM

Cómo sondear la auditoría de configuración de las instancias de NetScaler ADC

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cómo reutilizar las plantillas de auditoría de configuración en los trabajos de configuración

Cómo importar y exportar plantillas de configuración

Cómo generar una diferencia de auditoría de configuración para las trampas SNMP de ConfigChange

## Administración de certificados

Cómo configurar una directiva empresarial en NetScaler ADM

Cómo instalar certificados SSL en una instancia de NetScaler ADC desde NetScaler ADM

Cómo actualizar un certificado instalado desde NetScaler ADM

Cómo vincular y desvincular certificados SSL mediante NetScaler ADM

Cómo crear una solicitud de firma de certificados (CSR) mediante NetScaler ADM

Cómo configurar notificaciones para la caducidad de certificados SSL desde NetScaler ADM

Cómo utilizar el panel SSL en NetScaler ADM

Cómo sondear certificados SSL desde instancias NetScaler ADC

## Administración de aplicaciones

Cómo crear una definición de aplicación en Citrix ADM

## StyleBooks

Cómo ver diferentes grupos de StyleBooks

Cómo crear sus propios StyleBooks

Cómo usar StyleBooks definidos por el usuario en NetScaler ADM

Cómo usar la API para crear configuraciones a partir de StyleBooks

Cómo habilitar análisis y configurar alarmas en un servidor virtual definido en un StyleBook

Cómo crear un StyleBook para subir archivos a NetScaler ADM

Cómo usar la API para crear configuraciones para cargar cualquier tipo de archivo

Cómo crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM

Cómo usar la API para crear configuraciones para cargar archivos de certificados y claves

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cómo usar Microsoft Skype Empresarial StyleBook en empresas empresariales

Cómo utilizar Microsoft Exchange StyleBook en empresas comerciales

Cómo usar Microsoft SharePoint StyleBook en empresas empresariales

## Análisis

Cómo habilitar el análisis en las instancias

Cómo configurar umbrales adaptativos

Cómo configurar la administración de SLA

Cómo configurar el resumen de bases de datos para análisis

Cómo crear umbrales y alertas con NetScaler ADM

Cómo inhabilitar la recopilación de datos de URL para el análisis desde Citrix ADM

Cómo ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red

Cómo ver la velocidad máxima de datos para un período de tiempo determinado

Cómo ver la eficiencia de la red

## Gestión de eventos

Cómo configurar la edad de los eventos en NetScaler ADM

Cómo programar un filtro de eventos mediante NetScaler ADM

Cómo configurar notificaciones de correo electrónico repetidas para eventos de NetScaler ADM

Cómo suprimir eventos mediante NetScaler ADM

Cómo utilizar el panel de eventos para supervisar eventos

Cómo crear reglas de eventos en Citrix ADM

Cómo modificar la gravedad reportada de los eventos que ocurren en instancias de NetScaler ADC

Cómo ver el resumen de eventos en NetScaler ADM

Cómo mostrar la gravedad de los eventos y los sesgos de las trampas de SNMP en NetScaler ADM

Cómo exportar mensajes syslog mediante NetScaler ADM

Cómo suprimir los mensajes de syslog en NetScaler ADM

Cómo configurar los ajustes de poda para eventos de ejemplo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Autenticación

Cómo habilitar servidores de autenticación externos alternativos y en cascada

Cómo agregar servidores de autenticación RADIUS

Cómo agregar servidores de autenticación LDAP

Cómo agregar servidores de autenticación TACACS

Cómo extraer el grupo de servidores de autenticación en NetScaler ADM

Cómo habilitar la autenticación local de reserva

## Sistema NetScaler ADM

Cómo actualizar NetScaler ADM

Cómo restablecer la contraseña para Citrix ADM

Cómo generar un archivo de soporte técnico para NetScaler ADM

Cómo hacer copias de seguridad y restaurar su servidor NetScaler ADM en una implementación de un solo servidor

Cómo hacer una copia de seguridad y restaurar una configuración de NetScaler ADM en un par HA

Cómo habilitar el acceso a la consola para usuarios no predeterminados en NetScaler ADM

Cómo configurar el servidor NTP en NetScaler ADM

Cómo configurar la configuración de SSL para NetScaler ADM

Cómo configurar el intervalo de purga de syslog para NetScaler ADM

Cómo ver la información de auditoría de NetScaler ADM

Cómo configurar los ajustes de notificación del sistema de NetScaler ADM

Cómo supervisar el uso de la CPU, la memoria y el disco de NetScaler ADM

Cómo configurar un grupo de cifrado para NetScaler ADM

Cómo crear trampas, administradores y usuarios de SNMP en NetScaler ADM

Cómo asignar un nombre de host a un servidor NetScaler ADM

Cómo configurar los ajustes de poda del sistema para NetScaler ADM

Cómo configurar los ajustes de copia de seguridad del sistema mediante NetScaler ADM

Cómo configurar y ver alarmas del sistema en NetScaler ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Funciones de red

Cómo generar informes para entidades de equilibrio de carga

Cómo exportar o programar la exportación de informes de funciones de red

## Overview

January 30, 2024

NetScaler Application Delivery Management (ADM) es una solución de administración centralizada que simplifica las operaciones al proporcionar a los administradores visibilidad en toda la empresa y automatizar los trabajos de administración que deben ejecutarse en varias instancias. Puede administrar y supervisar los productos de red de aplicaciones Citrix que incluyen NetScaler ADC MPX, NetScaler ADC VPX, NetScaler ADC SDX, NetScaler ADC CPX, NetScaler Gateway y Citrix SD-WAN. Puede usar ADM para administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada.

ADM es un dispositivo virtual que se ejecuta en Citrix Hypervisor, VMware ESXi y Linux KVM. ADM aborda el desafío de la visibilidad de las aplicaciones mediante la recopilación de la siguiente información detallada sobre el tráfico de aplicaciones web y escritorios virtuales:

- información de nivel de sesión de usuario
- Datos de rendimiento de páginas web
- información de base de datos que fluye a través de las instancias ADC en su sitio y proporciona informes prácticos.

ADM permite a los administradores de TI solucionar problemas y supervisar de forma proactiva los problemas de los clientes en cuestión de minutos.

## Funciones y soluciones

January 30, 2024

NetScaler Application Delivery Management (ADM) ofrece las siguientes funciones:

### Gestión y análisis de aplicaciones

Análisis del rendimiento de las aplicaciones

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

App Score es el producto de un sistema de puntuación que define el rendimiento de una aplicación. Muestra si la aplicación está funcionando bien en términos de capacidad de respuesta, no es vulnerable a las amenazas y tiene todos los sistemas en funcionamiento.

### Análisis de seguridad de aplicaciones

El Panel de seguridad de aplicaciones proporciona una vista holística del estado de seguridad de sus aplicaciones. Por ejemplo, muestra métricas de seguridad clave, como infracciones de seguridad, infracciones de firmas, índices de amenazas. El panel de seguridad de aplicaciones también muestra información relacionada con los ataques, como ataques SYN, ataques de ventanas pequeñas y ataques de inundación DNS para las instancias de ADC descubiertas.

## Redes

### Instances

Le permite administrar las instancias de Citrix ADC, Citrix Gateway, Citrix SD-WAN y HAProxy.

### Grupos de instancias

Le permite agrupar sus instancias de la siguiente manera:

- Grupo estático: le permite definir un grupo de dispositivos que puede utilizar en diferentes tareas, como trabajos de configuración, etc.
- Bloqueo de IP privado: permite agrupar las instancias en función de las ubicaciones geográficas.

### Gestión de eventos

Cuando la dirección IP de una instancia ADC se agrega a ADM, ADM envía una llamada NITRO y se agrega implícitamente como destino de captura para que la instancia reciba sus capturas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia de ADC administrada.

### Administración de certificados

Citrix ADM ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una sola consola, puede establecer directivas automatizadas para garantizar el emisor correcto, la fortaleza de la clave y los algoritmos correctos, al tiempo que mantiene una estrecha ficha sobre los certificados que no se utilizan o que caducan pronto. Para comenzar a usar el panel SSL de ADM y sus funcionalidades, debe comprender qué es un certificado SSL y cómo puede usar ADM para realizar un seguimiento de sus certificados SSL.

### Administración de la configuración

NetScaler ADM le permite crear trabajos de configuración que lo ayuden a realizar tareas de configuración, como la creación de entidades, la configuración de funciones, la replicación de cambios de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

configuración, las actualizaciones del sistema y otras actividades de mantenimiento con facilidad en varias instancias. Los trabajos de configuración y las plantillas simplifican las tareas administrativas más repetitivas en una sola tarea en ADM.

### Auditoría de configuración

Permite supervisar e identificar anomalías en las configuraciones de las instancias.

- Consejos de configuración: le permite identificar una anomalía en la configuración.
- Plantilla de auditoría: permite supervisar los cambios en una configuración específica.

### Informes de red

Puede optimizar el uso de los recursos supervisando los informes de su red en ADM.

## Análisis

### Información web

Proporciona visibilidad de las aplicaciones web empresariales y permite a los administradores de TI supervisar todas las aplicaciones web que ofrece NetScaler ADC al proporcionar una supervisión integrada y en tiempo real de las aplicaciones. Web Insight proporciona información crítica, como el tiempo de respuesta del usuario y del servidor, lo que permite a las organizaciones de TI supervisar y mejorar el rendimiento de las aplicaciones.

### HDX Insight

Proporciona visibilidad de extremo a extremo del tráfico ICA que pasa por NetScaler ADC. HDX Insight permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento.

### Gateway Insight

Proporciona visibilidad sobre los errores que encuentran los usuarios al iniciar sesión, independientemente del modo de acceso. Puede ver una lista de usuarios que han iniciado sesión en un momento determinado, junto con el número de usuarios activos, el número de sesiones activas y los bytes y licencias utilizados por todos los usuarios en un momento determinado.

### Security Insight

Proporciona una solución de panel único que le ayuda a evaluar el estado de seguridad de sus aplicaciones y a tomar medidas correctivas para protegerlas.

### Insight SSL

SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y permite a los administradores de TI monitorear todas las aplicaciones web seguras que ofrece NetScaler ADC al proporcionar una supervisión histórica e integrada en tiempo real de las transacciones web seguras.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Información TCP

TCP Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión utilizadas en las instancias de ADC a fin de evitar la congestión de la red en la transmisión de datos.

### Video Insight

La función Video Insight proporciona una solución sencilla y escalable para monitorear las métricas de las técnicas de optimización de vídeo utilizadas por las instancias de NetScaler ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa.

### WAN Insight

Los análisis de WAN Insight permiten a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre el centro de datos y los dispositivos de optimización de WAN de sucursal. WAN Insight también proporciona visibilidad en clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz.

## Orchestration

### Orquestación en la nube

Permite la integración de los productos NetScaler ADC con la orquestación en la nube de OpenStack. NetScaler ADM y OpenStack implementan las API de cada uno, lo que permite la integración de la función de equilibrio de carga (LBaaS) de la instancia de NetScaler ADC con la orquestación en la nube de OpenStack.

### Orchestration

NetScaler ADM admite SDN en la red empresarial mediante la integración con controladores SDN de diferentes proveedores. ADM admite VMware NSX Manager y Cisco Application Policy Infrastructure Controller (APIC).

# Arquitectura

January 30, 2024

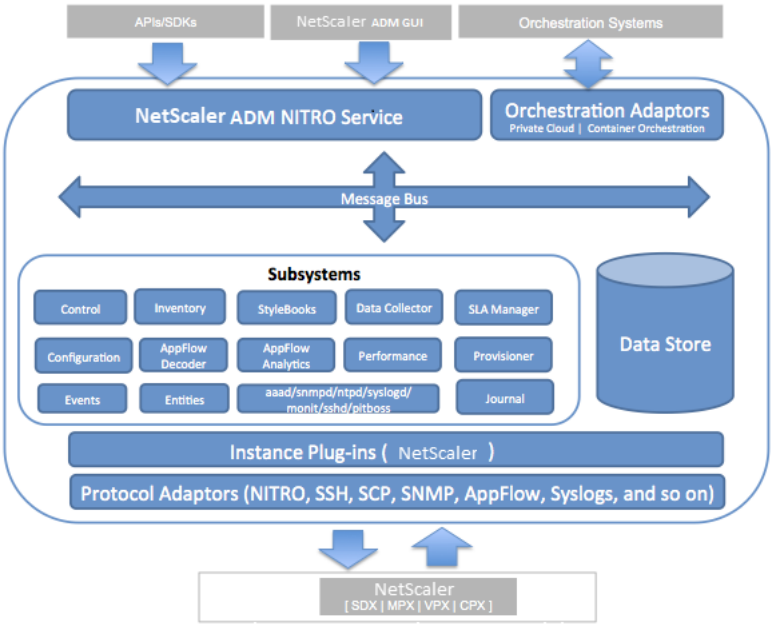
La base de datos Citrix Application Delivery Management (ADM) está integrada con el servidor y el servidor administra todos los procesos clave, como la recopilación de datos y las llamadas NITRO. En su almacén de datos, el servidor almacena un inventario de los detalles de la instancia, como el nombre del host, la versión del software, la configuración guardada y en ejecución, los detalles del certificado y las entidades configuradas en la instancia. La implementación de un solo servidor es

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

adecuada si desea procesar pequeñas cantidades de tráfico o almacenar datos durante un tiempo limitado.

Actualmente, ADM admite dos tipos de implementaciones de software: servidor único y alta disponibilidad.

La siguiente imagen muestra los diferentes subsistemas dentro de ADM y cómo ocurre la comunicación entre el servidor ADM y las instancias administradas.




El subsistema Servicio en ADM actúa como un servidor web que gestiona las solicitudes y respuestas HTTP que se envían a subsistemas dentro de ADM desde la GUI o API, mediante los puertos 80 y 443. Estas solicitudes se envían a los subsistemas a través del bus de mensajes (sistema de procesamiento de mensajes) mediante el mecanismo IPC (comunicación entre procesos). Se envía una solicitud al subsistema Control, que procesa la información o la envía al subsistema correspondiente. Cada uno de los otros subsistemas (Inventory, StyleBooks, Data Collector, Configuration, AppFlow Decoder, AppFlow Analytics, Rendimiento, Eventos, Entidades, Administrador de SLA, Aprovisionador y Diario) tiene una función específica.

Los complementos de instancia son bibliotecas compartidas que son exclusivas de cada tipo de instancia admitido por ADM. La información se transfiere entre ADM y las instancias administradas mediante llamadas NITRO o mediante el protocolo SNMP, Secure Shell (SSH) o Secure Copy (SCP). Esta información se procesa y almacena en la base de datos interna (data store).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Cómo descubre NetScaler ADM instancias

January 30, 2024

Las instancias son dispositivos Citrix o dispositivos virtuales que desea detectar, administrar y supervisar desde Citrix Application Delivery Management (ADM). Para administrar y monitorear estas instancias, debe agregarlas al servidor NetScaler ADM. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a ADM:

- Instancias de NetScaler ADC
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
  - Citrix BLX
- Instancias de NetScaler Gateway
- Instancias de Citrix SD-WAN

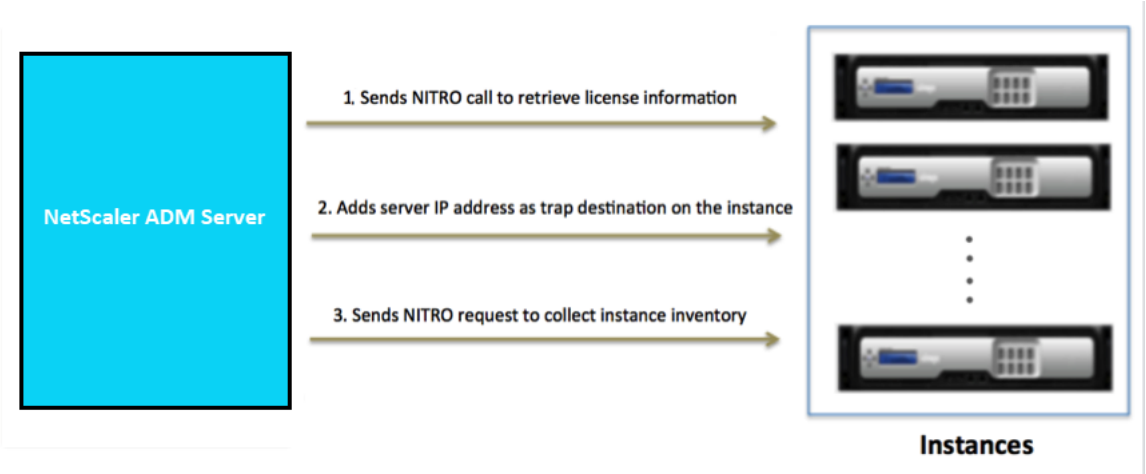
Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde.

> **Nota**
>
> NetScaler ADM utiliza la dirección IP de NetScaler ADC (NSIP) de las instancias ADC para la comunicación. ADM también puede detectar instancias ADC con una dirección IP de subred (SNIP) que tiene habilitado el acceso de administración en ella. Para obtener información sobre los puertos que deben estar abiertos entre las instancias de ADC y ADM, consulte Puertos.
>
> Si quiere agregar un par ADC HA mediante SNIP, asegúrese de habilitar el modo Configuración de red independiente (INC) en el par ADC HA. Para obtener más información sobre cómo agregar instancias, consulta Agregar instancias.
>
> Para Citrix SD-WAN WO, ADM utiliza la dirección IP de administración de las instancias para la comunicación.
>
> No puede agregar instancias de Citrix SD-WAN SE/PE en ADM. Puede configurar ADM como un recopilador AppFlow en los dispositivos Citrix SD-WAN SE/PE.

Cuando agrega una instancia al servidor ADM, el servidor se agrega implícitamente como destino de captura para la instancia y recopila el inventario de la instancia.

El siguiente diagrama describe cómo ADM descubre y agrega instancias implícitamente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Como se muestra en el diagrama, NetScaler ADM realiza implícitamente los siguientes pasos.

1. NetScaler ADM utiliza los detalles del perfil de instancia para iniciar sesión en la instancia. Mediante una llamada ADC NITRO, ADM recupera la información de licencia de la instancia. Según la información de licencia, determina si la instancia es una instancia ADC y el tipo de plataforma ADC (por ejemplo, NetScaler ADC MPX, ADC VPX, ADC SDX, ADC BLX o NetScaler Gateway). Al detectar correctamente la instancia, se agrega a la base de datos de ADM.

   Para las instancias de Citrix SD-WAN WO, ADM no detecta la instancia mediante la información de licencias. Envía una solicitud NITRO a la instancia para comprobar el tipo y la versión de la instancia.

   Este paso puede fallar si el perfil de instancia no incluye las credenciales correctas. En el caso de las instancias de ADC MPX, ADC VPX, ADC SDX, ADC BLX y NetScaler Gateway, este paso también puede fallar si las licencias no se aplican a la instancia.

   > **Nota**
   >
   > Con HTTP, puede agregar todas las instancias a ADM incluso si las licencias no están configuradas en las instancias.

2. ADM agrega su dirección IP a la lista de destinos de captura de la instancia. Esto permite que ADM reciba las trampas generadas en la instancia de ADC.

   Este paso puede fallar si el número de destinos de captura de la instancia supera el límite máximo de destinos de captura. El límite máximo de instancias es de 20.

   Para las instancias de Citrix SD-WAN WO, ADM agrega su dirección IP como administrador SNMP en la instancia.

3. ADM recopila el inventario de la instancia mediante el envío de una solicitud NITRO. Recopila detalles de instancia como el nombre del host, la versión del software, la configuración en ejecución y guardada, los detalles del certificado y las entidades configuradas en la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Este paso puede fallar debido a problemas de red o firewall.

Para aprender a agregar instancias a ADM, consulte Agregar instancias.

## Visión general de sondeo

August 23, 2024

El sondeo es un proceso en el que Citrix Application Delivery Management (ADM) recopila determinada información de las instancias de Citrix ADC. Es posible que haya configurado varias instancias de Citrix ADC para su organización en todo el mundo. Para supervisar sus instancias a través de Citrix ADM, Citrix ADM debe recopilar determinada información, como el uso de la CPU, el uso de la memoria, los certificados SSL, las funciones con licencia, los tipos de licencia, etc., de todas las instancias de ADC administradas. Los siguientes son los diferentes tipos de sondeo que se producen entre ADM y las instancias administradas:

- Sondeo de instancias
- Encuesta de inventario
- Colección de datos de rendimiento
- Encuesta de respaldo de instancias
- Encuesta de auditoría de configuración
- Sondeo de certificados SSL
- Sondeo de entidades

Citrix ADM utiliza protocolos como NITRO call, Secure Shell (SSH) y Secure Copy (SCP) para sondear la información de las instancias de Citrix ADC.

### Cómo Citrix ADM sondea las instancias y entidades administradas

De forma predeterminada, Citrix ADM sondea automáticamente a intervalos regulares. Citrix ADM también le permite configurar los intervalos de sondeo para algunos tipos de sondeo y permite realizar sondeos manualmente cuando sea necesario.

La siguiente tabla describe los detalles de los tipos de sondeo, el intervalo de sondeo, el protocolo utilizado, etc.:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo de sondeo | Intervalo de sondeos | Información encuestada | Protocolo utilizado | Configuración de intervalos de votación |
|---|---|---|---|---|
| **Sondeo de instancias** | Cada 1 minuto (por defecto) | Información estadística, como el estado, las solicitudes HTTP por segundo, el uso de la CPU, el uso de la memoria y el rendimiento. | Llamada NITRO. | No |
| **Encuesta de inventario** | Cada 60 minutos (de forma predeterminada) | Detalles del inventario, como la versión de compilación, la información del sistema, las funciones con licencia y los modos. | Llamadas NITRO y SSH | No |
| **Colección de datos de rendimiento** | Cada 5 minutos (de forma predeterminada) | Información de informes de red | Llamada NITRO | No |
| **Encuesta de respaldo de instancias** | Cada 12 horas (por defecto) | Archivo de respaldo del estado actual de las instancias de ADC administradas | Llamadas NITRO, SSH y SCP. | Sí. Desplácese a **Redes** > **Instancias** > **NetScaler ADC**. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Copia de seguridad/restauración**. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo de sondeo | Intervalo de sondeos | Información encuestada | Protocolo utilizado | Configuración de intervalos de votación |
|---|---|---|---|---|
| **Encuesta de auditoría de configuración** | Cada 10 horas (por defecto) | Cambios de configuración que se producen en las instancias de ADC (por ejemplo, configuración en ejecución o configuración guardada) | Llamada SSH, SCP y NITRO | Sí. Vaya a **Redes** > **Auditoría de configuración**. En la página Auditoría de configuración, haga clic en **Configuración** y configure el intervalo de sondeo para el sondeo de auditoría de configuración. Puede sondear las auditorías de configuración manualmente y agregar todas las auditorías de configuración de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Auditoría de configuración** y haga clic en **Sondear ahora**. La página **Encuesta ahora** le permite sondear todas las instancias o seleccionadas de la red. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo de sondeo | Intervalo de sondeos | Información encuestada | Protocolo utilizado | Configuración de intervalos de votación |
|---|---|---|---|---|
| **sondeo de certificados SSL** | Cada 24 horas (de forma predeterminada) | Certificados SSL que se instalan en las instancias de Citrix ADC. | Llamadas NITRO y SCP | Sí. Vaya a **Redes** > **Panel de SSL**. En la página Tablero SSL, haga clic en **Configuración** para configurar el intervalo de sondeo<br>Puede sondear los certificados SSL manualmente y agregar todos los certificados de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Tablero SSL** y haga clic en **Sondear ahora**. La página **Encuesta ahora** le permite sondear todas las instancias o seleccionadas de la red. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo de sondeo | Intervalo de sondeos | Información encuestada | Protocolo utilizado | Configuración de intervalos de votación |
|---|---|---|---|---|
| **Sondeo de entidades** | Cada 60 minutos (de forma predeterminada) | Todas las entidades configuradas en las instancias. Una entidad es una directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC. Para habilitar el sondeo de entidades, consulte Habilitar o inhabilitar las funciones de ADM. | NITRO llama. | Sí, pero no se puede establecer en menos de 10 minutos. Para configurar, vaya a **Redes** > **Funciones de red**. En la página Función de redes, haga clic en **Configuración** para configurar el intervalo de sondeo. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo de sondeo | Intervalo de sondeos | Información encuestada | Protocolo utilizado | Configuración de intervalos de votación |
|---|---|---|---|---|
| | | | | Puede sondear entidades manualmente y agregar todas las entidades de las instancias inmediatamente a Citrix ADM. Para ello, vaya a **Redes** > **Funciones de red** y haga clic en **Sondear ahora**. La página **Encuesta ahora** le permite sondear todas las instancias o seleccionadas de la red |

> **Nota**
>
> Además del sondeo, Citrix ADM recibe eventos generados por instancias de ADC administradas a través de capturas SNMP enviadas a las instancias. Por ejemplo, se genera un evento cuando hay un error del sistema o un cambio en la configuración.
>
> Durante la copia de seguridad de la instancia, se descargan en Citrix ADM los archivos SSL, los archivos de certificados de CA, las plantillas de ADC, la información de la base de datos, Durante una auditoría de configuración, los archivos ns.conf se descargan y almacenan en el sistema de archivos. Toda la información recopilada de las instancias administradas de Citrix ADC se almacena internamente en la base de datos.

### Diferentes formas de sondear instancias

A continuación se muestran las diferentes formas de sondeo que Citrix ADM realiza en las instancias administradas:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Sondeo global de instancias
- Sondeo manual de instancias
- Encuesta manual de entidades

### Sondeo global de instancias

Citrix ADM sondea automáticamente todas las instancias administradas en la red, dependiendo del intervalo configurado por usted. Aunque el intervalo de sondeo predeterminado es de 30 minutos, puede configurarlo en función de sus requisitos navegando a **Redes** > **Funciones de red** > **Configuración**.

### Sondeo manual de instancias

Cuando Citrix ADM administra muchas entidades, el ciclo de sondeo tarda más tiempo en generar el informe, lo que podría dar como resultado una pantalla en blanco o que el sistema siguiera mostrando datos anteriores.

En Citrix ADM, hay un período mínimo de intervalo de sondeo en el que no se realiza el sondeo automático. Si agrega una nueva instancia de Citrix ADC o si se actualiza una entidad, Citrix ADM no reconoce la nueva instancia ni las actualizaciones realizadas en una entidad hasta que se realice el siguiente sondeo. Además, no hay forma de obtener inmediatamente una lista de direcciones IP virtuales para futuras operaciones. Debe esperar a que transcurra el intervalo mínimo de sondeo. Si bien puede realizar una encuesta manual para descubrir las instancias recién agregadas, esto lleva a que se sondee toda la red Citrix ADC, lo que genera una carga pesada en la red. En lugar de sondear toda la red, Citrix ADM ahora le permite sondear solo instancias y entidades seleccionadas en un momento dado.

Citrix ADM sondea automáticamente las instancias administradas para recopilar información a determinadas horas del día. El sondeo seleccionado reduce el tiempo de actualización que requiere Citrix ADM para mostrar el estado más reciente de las entidades enlazadas a estas instancias seleccionadas.

**Para sondear instancias específicas en Citrix ADM:**

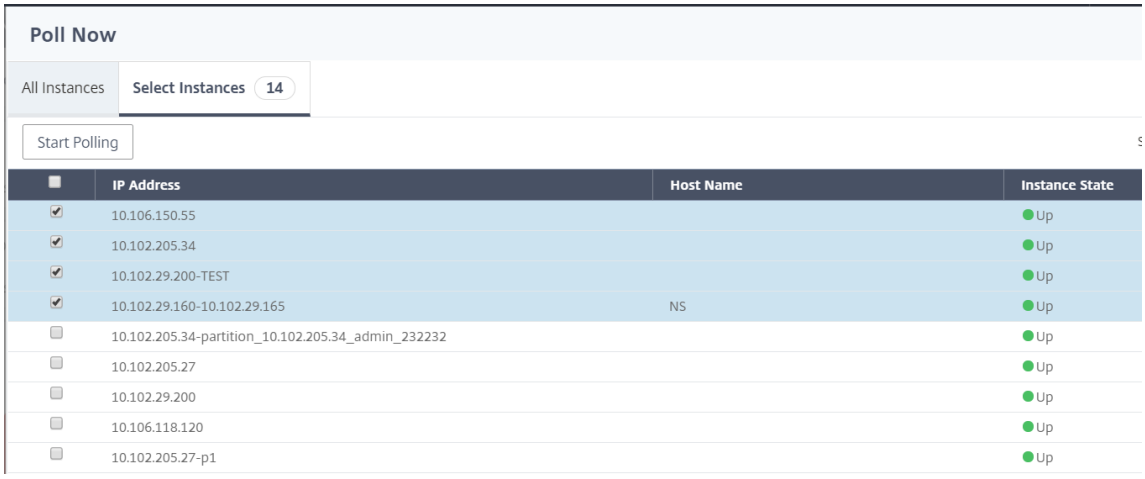
1. En Citrix ADM, vaya a **Redes** > **Funciones de red**.
2. En la página **Funciones de red**, en la esquina superior derecha, haga clic en **Sondear ahora**.
3. La página emergente **Poll Now** ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.

    a) Ficha**Todas las instancias**: haga clic en **Iniciar sondeo** para sondear todas las instancias.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) **Seleccione la ficha Instancias**: seleccione las instancias de la lista

4. Haga clic en **Iniciar sondeo**.




Citrix ADM inicia el sondeo manual y agrega todas las entidades.

## Encuesta manual de entidades

Citrix ADM también le permite sondear solo unas pocas entidades seleccionadas que están enlazadas a una instancia determinada. Por ejemplo, puede utilizar esta opción para conocer el estado más reciente de una entidad concreta en una instancia. En tal caso, no necesita sondear la instancia como un todo para conocer el estado de una entidad actualizada. Al seleccionar y sondear una entidad, Citrix ADM sondea solo esa entidad y actualiza el estado en la GUI de Citrix ADM.

Considere un ejemplo de un servidor virtual que está INACTIVO . Es posible que el estado de ese servidor virtual haya cambiado a ACTIVO antes de que se realice el siguiente sondeo automático. Para ver el estado modificado del servidor virtual, es posible que desee sondear solo ese servidor virtual para que se muestre inmediatamente el estado correcto en la GUI.

Ahora puede sondear las siguientes entidades para detectar cualquier actualización en su estado: servicios, grupos de servicios, servidores virtuales de equilibrio de carga, servidores virtuales de reducción de caché, servidores virtuales de conmutación de contenido, servidores virtuales de autenticación, servidores virtuales VPN, servidores virtuales GSLB y servidores de aplicaciones.

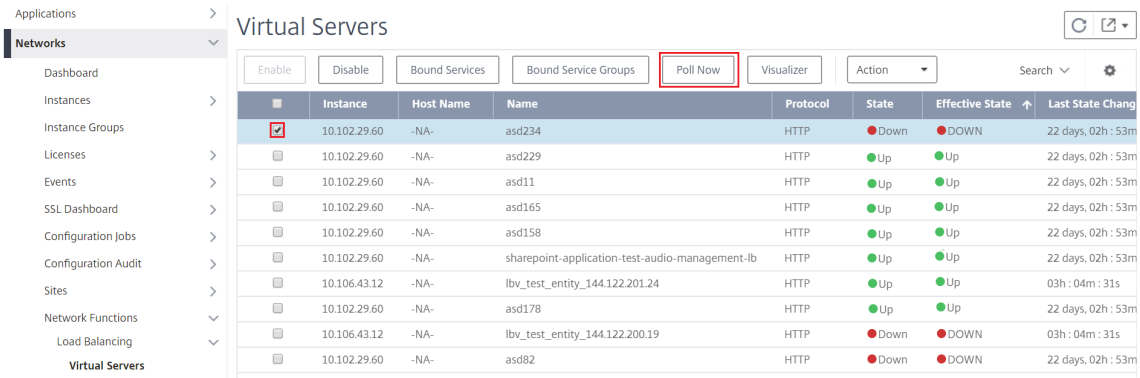
> **Nota**
>
> Si sondea un servidor virtual, solo se sondea ese servidor virtual. Las entidades asociadas, como servicios, grupos de servicios y servidores, no se sondean. Si necesita sondear todas las entidades asociadas, debe sondear manualmente las entidades o debe sondear la instancia.

**Para sondear entidades específicas en Citrix ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Por ejemplo, esta tarea le ayuda a sondear los servidores virtuales de equilibrio de carga. Del mismo modo, también puede sondear otras entidades de función de red.

1. En Citrix ADM, vaya a**Redes** > **Funciones de red** > **Equilibrio de carga** > **Servidores virtuales**.
2. Seleccione el servidor virtual que muestra el estado como DOWN y haga clic en **Sondear ahora**. El estado del servidor virtual ahora cambia a ACTIVO .




## Gobierno de datos

January 30, 2024

Citrix recopila estadísticas sobre las implementaciones de Citrix Application Delivery Management (ADM) para comprender el uso y la escala de la implementación. Las estadísticas incluyen el estado, el estado y el patrón de uso de ADM en sus instalaciones. Las estadísticas ayudan a Citrix a solucionar problemas de forma proactiva en la implementación de ADM.

- **Cree una identidad de cliente en Citrix Cloud**: Para enviar estadísticas importantes sobre el estado, el estado y otras métricas de la implementación local de ADM a la cuenta de Citrix Cloud.

  Después de crear una identidad de cliente, “Cloud Connect”establece la conexión entre ADM on-prem y el servicio ADM mediante la creación de una cuenta de Citrix Cloud. Consulte Configurar la identidad del cliente.

- **Configurar scripts de mantenimiento**: Para optimizar la base de datos. La optimización de la base de datos puede crear tablas, modificar columnas y más. La misma función “Cloud Connect”se utiliza para configurar scripts de mantenimiento. Consulte Optimización de bases de datos mediante scripts de mantenimiento

- **Programa de mejora de la experiencia de usuario del cliente (CUXIP)**: Este programa está habilitado de forma predeterminada. Recopila los datos de uso de Citrix ADM. Estos datos permiten optimizar la experiencia de ADM a través de flujos de trabajo guiados, artículos de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

búsqueda, notificaciones de productos, comentarios, encuestas, etc. Consulte Programa de mejora de la experiencia del usuario del cliente.

## Configurar la identidad del cliente

Citrix Application Delivery Management (ADM) requiere que se autentique en la GUI de ADM antes de empezar a acceder a la información. Es obligatorio que se registre en los servicios de Citrix Cloud antes de autenticarse en ADM. Proporcione las credenciales de usuario de Citrix Cloud en la GUI de ADM. Para obtener más información, consulte Inscribirse en Citrix Cloud.

Existen diferentes formas de autenticarse en Citrix ADM. En las secciones siguientes se describen los flujos de trabajo si es un usuario nuevo o un usuario existente en ADM.

### Flujo de trabajo 1: si es un usuario nuevo

1. Complete la instalación de Citrix ADM en el Hypervisor seleccionado.
2. Configure las distintas direcciones IP necesarias.
3. En un explorador web, escriba la dirección IP de Citrix ADM.
4. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.

   Se abre la página **Configurar identidad del cliente**, donde debe identificarse con sus credenciales de Citrix Cloud.

   Si no ha creado una cuenta en Citrix Cloud, haga clic en Citrix Cloud para registrarse.
5. Haga clic en **Autenticar** y proporcione la dirección de correo electrónico que ha utilizado para registrarse en Citrix Cloud.
6. Seleccione la casilla de verificación situada junto a **Acepto compartir datos** para telemetría y haga clic en **Enviar**.

### Flujo de trabajo 2: si ya es un usuario, actualice a la última versión de ADM

1. Después de actualizar Citrix ADM a la versión más reciente, en un navegador web, escriba la dirección IP del Citrix ADM.
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Se abre la página **Configurar identidad del cliente**, donde debe identificarse con sus credenciales de Citrix Cloud.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si no ha creado una cuenta en Citrix Cloud, haga clic en Citrix Cloud para registrarse.

4. Haga clic en **Autenticar** y proporcione la dirección de correo electrónico que ha utilizado para registrarse en Citrix Cloud.
5. Active la casilla de verificación situada junto a "Acepto compartir datos para telemetría"y haga clic en Enviar.

Como usuario existente, también puede configurar su identidad en ADM más adelante de una de las dos formas siguientes:

- Vaya a **Sistema > Administración del sistema** y haga clic en **Autenticación**.
- Haga clic en el símbolo de nube en la parte superior derecha de la GUI de ADM.
  Después de una autenticación correcta, X se convierte en una marca de verificación de color verde.

> **Nota**
>
> Asegúrese de que los siguientes dominios estén en la lista de permitidos:
>
> - `*.citrixnetworkapi.net`
> - `*.blob.core.windows.net`

Al cargar sus datos en Citrix ADM y utilizar las funciones de Citrix ADM, acepta y acepta que Citrix recopile, almacene, transmita, mantenga, procese y use información técnica, de usuario o relacionada sobre sus productos y servicios Citrix.

La información recibida por Citrix siempre se trata de acuerdo con la Directiva de privacidad de Citrix.com.

### Diagnóstico y recopilación de datos

Citrix ADM recopila la siguiente telemetría mediante la identidad del cliente:

- **Acciones realizadas en ADM:**
  - Acciones realizadas mediante la interfaz UI/API de Citrix ADM.
  - Acciones realizadas mediante la interfaz Citrix ADM SDK.
  - Recuento de operaciones en un solo día. Este recuento incluye cualquier solicitud que no sea GET de la API o la interfaz de usuario.
  - Recuento de actualizaciones de ADC realizadas por ADM.
- **Información de licencia de Citrix ADM**: Recuento de servidores virtuales autorizados.
- **Estadísticas clave**:
  - Recuento total de reglas del evento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - Recuento total de StyleBooks definidos por el usuario.
  - Recuento de aplicaciones gestionadas y personalizadas.
  - Recuento de agentes registrados.
  - Rendimiento general en Citrix ADC (Rx+Tx).
  - Recuento de instancias gestionadas. Este recuento también incluye las particiones de administración.
  - Recuento de administradores que utilizan Citrix ADM SaaS.

- **Geolocalización de Citrix ADM**
- **Información de implementación**: esta información incluye tipos de implementación, como agentes de alta disponibilidad, recuperación ante desastres y ADM.

#### ¿Por qué se recopilan los datos?

Los datos de telemetría recopilados ayudan a:

- Recomiende el dimensionamiento y la implementación correctos de Citrix ADM.
- Solucione problemas de forma proactiva en las implementaciones locales de ADM.

#### ¿Quién puede usar estos datos?

Citrix es el único propietario de la información recopilada. Citrix tiene acceso a la información que usted nos proporciona voluntariamente y la recopila. No vendemos ni alquilamos esta información a nadie. No compartimos su información con ningún tercero ajeno a nuestra organización, excepto cuando sea necesario para cumplir con su solicitud. Ejemplo: para enviar un pedido o resolver problemas de forma proactiva.

#### ¿Durante cuánto tiempo conservamos sus datos?

Por lo general, almacenamos datos personales y de uso hasta que el usuario utilice nuestros Servicios. O tenemos otro propósito para hacerlo. Posteriormente, los datos no se almacenan más de lo que exige o permite la ley o de lo necesario para la elaboración de informes internos y la conciliación.

Todos los datos de telemetría se almacenan durante un período no superior a 13 meses o 396 días.

### Optimización de bases de datos mediante scripts de mantenimiento

Los scripts de mantenimiento se utilizan para resolver problemas relacionados con las bases de datos en las implementaciones locales de ADM. El software ADM descarga automáticamente los scripts de mantenimiento de la base de datos desde el servicio ADM, lo que proporciona una resolución más

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

rápida para los problemas relacionados con la base de datos. Anteriormente, estos problemas se resolvieron ejecutando manualmente los scripts.

Con esta función, la implementación de ADM on-prem descarga periódicamente los scripts de mantenimiento de la base de datos desde el servicio ADM. Para hacerlo, asegúrese de configurar la identidad del cliente.

Los scripts de mantenimiento se ejecutan diariamente y semanalmente Además, los scripts pueden crear tablas o agregar o quitar columnas para mejorar el rendimiento de la base de datos.

## Programa de mejora de la experiencia del usuario del cliente

En Citrix Systems, nuestro objetivo es ofrecer a nuestros usuarios una experiencia de producto atractiva. El **Programa de mejora de la experiencia del usuario del cliente (CUXIP)** utiliza Pendo para guiar a los usuarios a través de algunas tareas comunes pero detalladas, proporcionando artículos de búsqueda, guías en la aplicación, etc. También ayudamos a nuestros usuarios a mantenerse al tanto de todos los anuncios recientes.

### ¿Qué datos de uso se recopilan a través de CUXIP?

Los datos de uso tienen que ver con las acciones de los usuarios. También denominados datos a nivel de evento, los datos de uso incluyen todo tipo de datos, desde las páginas que nuestros usuarios visitan en un sitio web hasta el número de clics en una función determinada. Los datos de uso son información valiosa sobre cómo se mueven los usuarios en nuestras aplicaciones. Estos datos permiten optimizar la experiencia de nuestros usuarios.

Los siguientes son algunos de los datos de uso que recopilamos:

- Detalles de las páginas vistas, tiempo empleado en cada página.
- El identificador de visitante es un identificador anónimo único que ayuda a identificar el número de visitantes únicos en una página.
- Estadísticas de la encuesta: puntuación, visitas, número de envíos, etc.

### ¿Cómo le ayuda CUXIP?

Usamos los datos de uso para mejorar su experiencia con ADM. Las siguientes son algunas de las formas en las que pretendemos mejorar la experiencia del usuario del cliente:

- Flujos de trabajo guiados en la aplicación y capacidad de buscar artículos relevantes.
- Participa en una encuesta desde la aplicación para ayudar a mejorar el producto.
- Mantente informado sobre los anuncios recientes y otras notificaciones.
- Publica una pregunta o comentario en el equipo del producto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

#### ¿Cómo funciona CUXIP?

El dispositivo Citrix ADM puede estar en la red interna. El navegador debe tener conectividad a Internet para disfrutar de los beneficios de la asistencia guiada de CUXIP.

#### ¿Cómo puedo inhabilitar CUXIP en mi ADM?

Para inhabilitar CUXIP, haga lo siguiente en la GUI de ADM:

1. Vaya a **Sistema > Administración del sistema**.
2. En **Configuración de CUXIP** e inhabilite CUXIP.

### Cambios en nuestra Directiva de privacidad

Es posible que actualicemos nuestra Directiva de privacidad de vez en cuando. Le notificaremos los cambios mediante la publicación de la nueva Directiva de privacidad en esta página. Le informaremos por correo electrónico o mediante un aviso destacado en nuestro Servicio antes de que el cambio entre en vigor y actualizaremos la "fecha de entrada en vigor"que aparece en la parte superior de esta Directiva de privacidad.

Se recomienda revisar esta Directiva de privacidad periódicamente para ver si hay cambios. Los cambios en esta Directiva de privacidad entran en vigor cuando se publican en la página Directiva de privacidad de Citrix.

#### Referencias

Directiva de privacidad de Citrix: https://www.citrix.com/about/legal/privacy/

## Sistema de licencias

January 30, 2024

Citrix Application Delivery Management (ADM) requiere una licencia de Citrix ADC verificada para administrar y supervisar las instancias de Citrix ADC, cuando las instancias se detectan a través del protocolo `https`.

Puede administrar y supervisar cualquier número de instancias y entidades sin licencia. Sin embargo, solo puede administrar 30 aplicaciones descubiertas en el panel de aplicaciones y ver los datos de análisis de 30 servidores virtuales sin solicitar una licencia. Más de 30 aplicaciones descubiertas o 30 servidores virtuales, debe comprar y aplicar una licencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | Función Citrix ADM | [**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales | Se requiere una licencia Citrix ADM para > 30 servidores virtuales | Requisitos de licencia de Citrix ADC |
|---|---|---|---|---|
| Análisis | Información web | No | Sí | No aplicable |
| | HDX Insight* | No | Sí | Avanzado (informes < 1 hora) Premium (informes = Ilimitado) |
| | Security Insight | No | Sí | Licencia Premium (o) Avanzada con App Firewall |
| | Insight SSL | No | Sí | No aplicable |
| | Gateway Insight | No | Sí | Avanzado (informes < 1 hora) Premium (informes = Ilimitado) |
| | Información TCP | No | Sí | No aplicable |
| | Video Insight | No | Sí | Premium (serie Citrix-T 1000, VPX-T) |
| | WAN Insight | No | No aplicable | Utilice la edición de optimización de instancias de Citrix SD-WAN (WANOP) |
| Aplicaciones | | | | |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | Función Citrix ADM | [**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales | Se requiere una licencia Citrix ADM para > 30 servidores virtuales | Requisitos de licencia de Citrix ADC |
|---|---|---|---|---|
| | Estadísticas de aplicaciones (Panel de aplicaciones, Panel de seguridad de aplicaciones) | No | Sí | La información relacionada con Citrix ADC Web App Firewall en el panel de aplicaciones y el panel de seguridad de aplicaciones necesita una licencia Premium (o) Advanced with App Firewall. |
| | StyleBooks | Sí | No | No aplicable |
| Redes | | | | |
| | Servidor de licencias | Sí | No | No aplicable |
| | Gestión de inventario: panel de infraestructura, grupos de instancias, panel de instancias y sitios | Sí | No | No aplicable |
| | Gestión de eventos y Syslog | Sí | No | No aplicable |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | Función Citrix ADM | [**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales | Se requiere una licencia Citrix ADM para > 30 servidores virtuales | Requisitos de licencia de Citrix ADC |
|---|---|---|---|---|
| | Trabajos de configuración, auditoría de configuración y consejos de configuración | Sí | No | No aplicable |
| | Informes de red (nivel de instancia) | Sí | No | No aplicable |
| | Informes de red (nivel de servidor virtual) | Sí | No | No aplicable |
| | Funciones de red (visibilidad y administración de servidores virtuales, servicios, grupos de servicios, servidores) | Sí | No | No aplicable |
| | Gestión, supervisión y panel de control de certificados SSL (nivel de instancia) | Sí | No | No aplicable |
| | Panel de certificados SSL (nivel de servidor virtual) | Sí | No | No aplicable |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | Función Citrix ADM | [**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales | Se requiere una licencia Citrix ADM para > 30 servidores virtuales | Requisitos de licencia de Citrix ADC |
|---|---|---|---|---|
| Sistema | | | | |
| | RBAC y autenticación externa (nivel de instancia) | Sí | No | No aplicable |
| | RBAC y autenticación externa | Sí | No | No aplicable |
| Orchestration | | | | |
| | Integración con OpenStack | Sí | No | No aplicable |
| | Integración con VMware NSX | Sí | No | No aplicable |
| | Integración de Cisco APIC | Sí | No | No aplicable |
| | Integración de contenedores | Sí | No | No aplicable |
| Equilibradores de carga de terceros | | | | |
| | HAProxy: visibilidad en el host/instancia/backend/servidores/frontend, configuración de descarga o carga y reinicio del dispositivo. | Sí | No | No aplicable |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | | | | |
|---|---|---|---|---|
| | Función Citrix ADM | [**LIBRE**] La licencia Citrix ADM no es necesaria independientemente del número de servidores virtuales | Se requiere una licencia Citrix ADM para > 30 servidores virtuales | Requisitos de licencia de Citrix ADC |
| | Panel de aplicaciones | No | Sí (requiere una licencia independiente) | No aplicable |

*Para la integración de Citrix Director con el soporte de Citrix ADM, Citrix Director debe tener una licencia Premium.

Las licencias para más servidores virtuales están disponibles en paquetes de servidores virtuales de 10. Puede obtener una licencia válida y agregar las licencias en los servidores Citrix ADM a través de la GUI de Citrix ADM.

## Alta disponibilidad

El servidor Citrix ADM puede contener licencias VIP, CICO y capacidad agrupada. Cuando las licencias se emiten a un servidor ADM, las licencias están enlazadas al identificador de host del servidor. Además, la asignación de licencias a un servidor ADM diferente está restringida.

Si configura un par de alta disponibilidad de ADM como servidor de licencias, los servidores principal y secundario deben tener los mismos archivos de licencia. Por lo tanto, en la implementación de alta disponibilidad de ADM, Citrix ADM admite la asignación de los mismos archivos de licencia a ambos servidores.

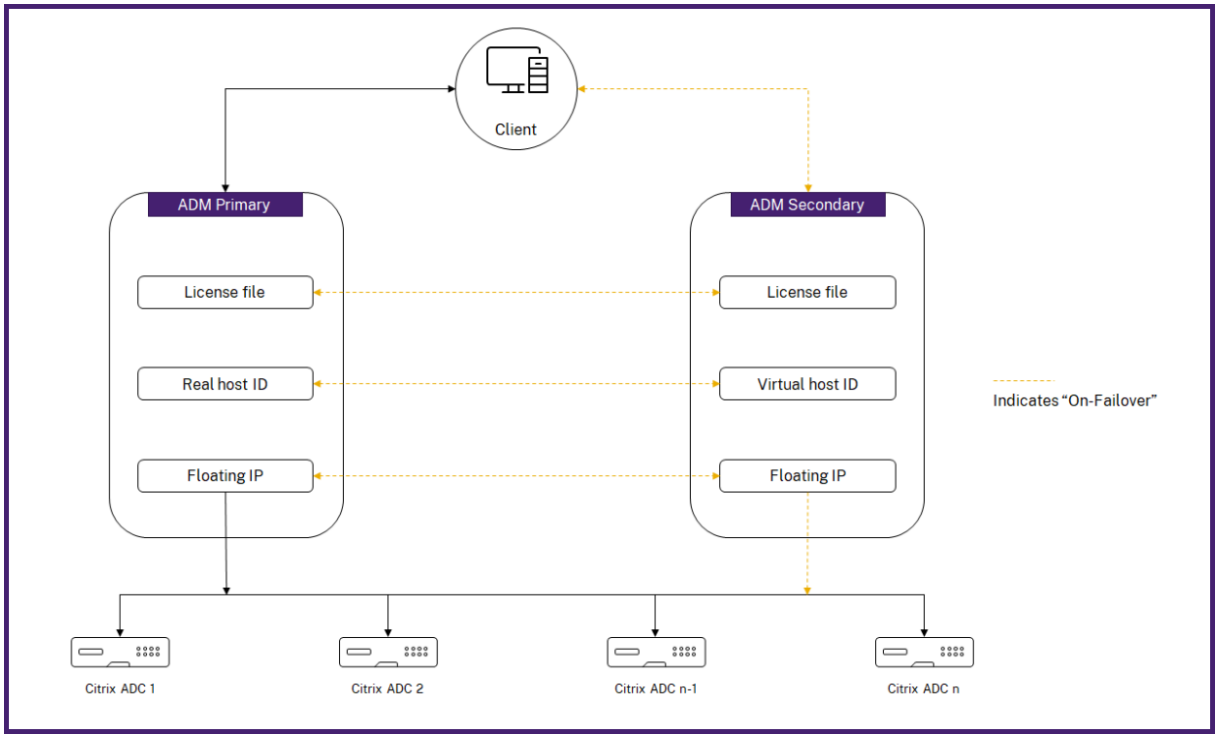
> **Nota**
>
> - Si ha instalado Citrix ADM 12.1.49.x o versiones anteriores, dispondrá de un período de gracia de 30 días para mantener las licencias en el nodo secundario. Tras el período de gracia, debe ponerse en contacto con Citrix para volver a alojar la licencia original.
> - Para 12.1.50.x o versiones posteriores, la licencia de Citrix ADM se sincroniza automáticamente con el nodo secundario.
> - Las licencias agrupadas se sincronizan automáticamente con el nodo secundario desde la versión 12.1.50.x o posterior.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**¿Cómo se sincronizan las licencias entre nodos de alta disponibilidad de ADM?**

Cada vez que se produce una conmutación por error, el servidor secundario asume la función del servidor principal. El ID de host real del servidor principal se configura como el ID de host virtual del nuevo servidor principal. Los archivos de licencia reconocen el nuevo servidor principal mediante el identificador de host virtual.

- **ID de host real** - Este ID se genera a partir de una dirección MAC del servidor ADM. Cada implementación independiente de ADM tiene un identificador de host único.
- **Identificador de host virtual**: Este identificador se genera automáticamente durante la implementación de HA. El ID de host real de un servidor primario de ADM se utiliza como ID de host virtual de un servidor secundario. Este ID se almacena en la base de datos ADM en un formato cifrado y las modificaciones de este ID están restringidas. El identificador de host virtual es preferible sobre el ID de host real.




Supongamos que el nodo-1 es el servidor principal y el Nodo-2 es el servidor secundario. El identificador de host virtual del Node-1 está sincronizado con el Node-2.

1. Los archivos de licencia disponibles en Node-1 se sincronizan con Node-2.
2. Cualquier nuevo archivo de licencia del Node-1 se sincroniza periódicamente con el Node-2.
3. ADM garantiza que el servidor de licencias se ejecuta solo en el Nodo-1 para evitar duplicar la capacidad de licencia.
4. Las instancias de Citrix ADC retiran las licencias del Node-1 mediante la dirección IP flotante.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Las licencias están bloqueadas para instancias de ADC. Para obtener licencias de un Citrix ADM HA, las instancias requieren la dirección IP del dispositivo específico. Cuando aplique licencias en un servidor principal, se encargará de las licencias y aplicará todas las licencias futuras en esa instancia. Solo puede eliminar licencias del servidor en el que haya instalado las licencias.

### Orchestration

El módulo de orquestación es independiente de la licencia y siempre está disponible.

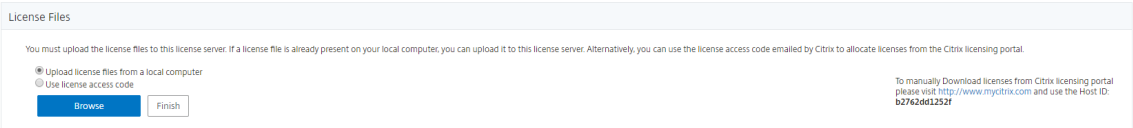
### Actualización de las licencias de servidor virtual

Puede actualizar las licencias en Citrix ADM para supervisar y administrar más servidores virtuales alojados en los dispositivos Citrix ADC.

**Para actualizar las licencias del dispositivo:**

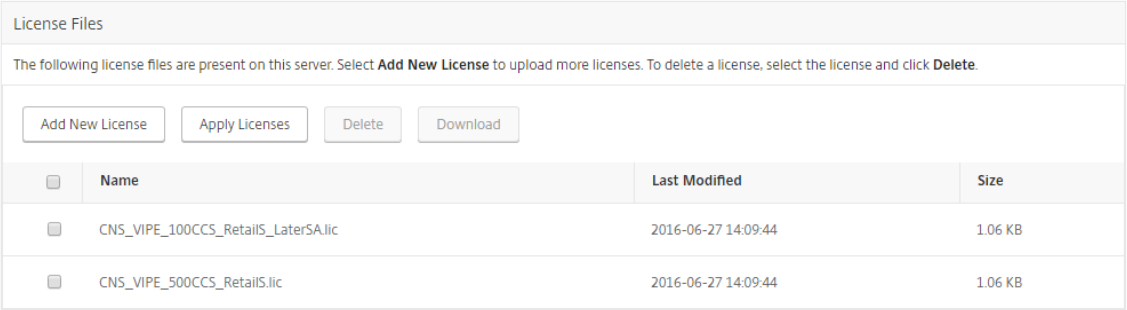
1. Inicie sesión en Citrix ADM con las credenciales de administrador.
2. Vaya a **Redes** > **Licencias** > **Configuración**.
3. En el panel de detalles, vaya a Archivos de licencias y seleccione una de las siguientes opciones:
   - **Cargue los archivos de licencia desde un equipo local**. Si ya hay una licencia en su equipo local, haga clic en**Examinar** y seleccione el archivo de licencia (.lic) que desee utilizar para asignar las licencias. Haz clic en **Finalizar** .
   - **Utilice el código de activación de licencia**. Citrix envía por correo electrónico el código de acceso de licencia de la licencia que adquirió. Introduzca el código de acceso de la licencia en el cuadro de texto y haga clic en **Obtener licencias**.

   > **Nota**
   >
   > Si selecciona esta opción, Citrix ADM debe estar conectado a Internet o un servidor proxy debe estar disponible.



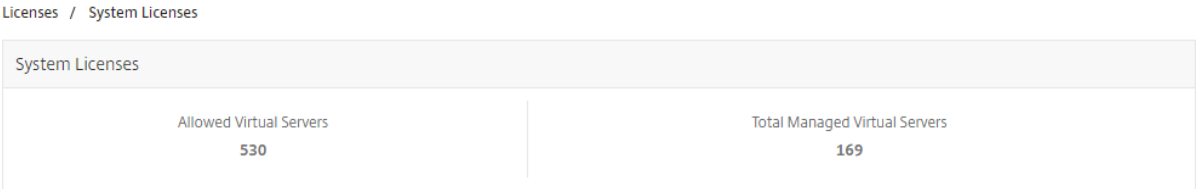

4. Puede agregar más licencias desde la página Configuración de licencias en cualquier momento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Verificación

Para comprobar las licencias instaladas en su Citrix ADM, vaya a**Sistema > Licencias y análisis**.




## Administrar servidores virtuales

Puede seleccionar los servidores virtuales o los servidores virtuales de terceros que quiere administrar y supervisar a través de Citrix ADM.

> **Puntos que tener en cuenta**
>
> - De forma predeterminada, Citrix ADM licencia automáticamente los servidores virtuales aleatoriamente después de cada ciclo de sondeo de servidores virtuales.
> - Si el número total de servidores virtuales descubiertos en su Citrix ADM es inferior al número de licencias de servidor virtual instaladas, Citrix ADM, de forma predeterminada, otorga licencias a todos los servidores virtuales.

Para seleccionar manualmente los servidores virtuales o para restringir las licencias a los servidores virtuales limitados, primero debe inhabilitar la concesión automática de licencias de los servidores virtuales y, a continuación, seleccionar los servidores virtuales que quiere administrar.

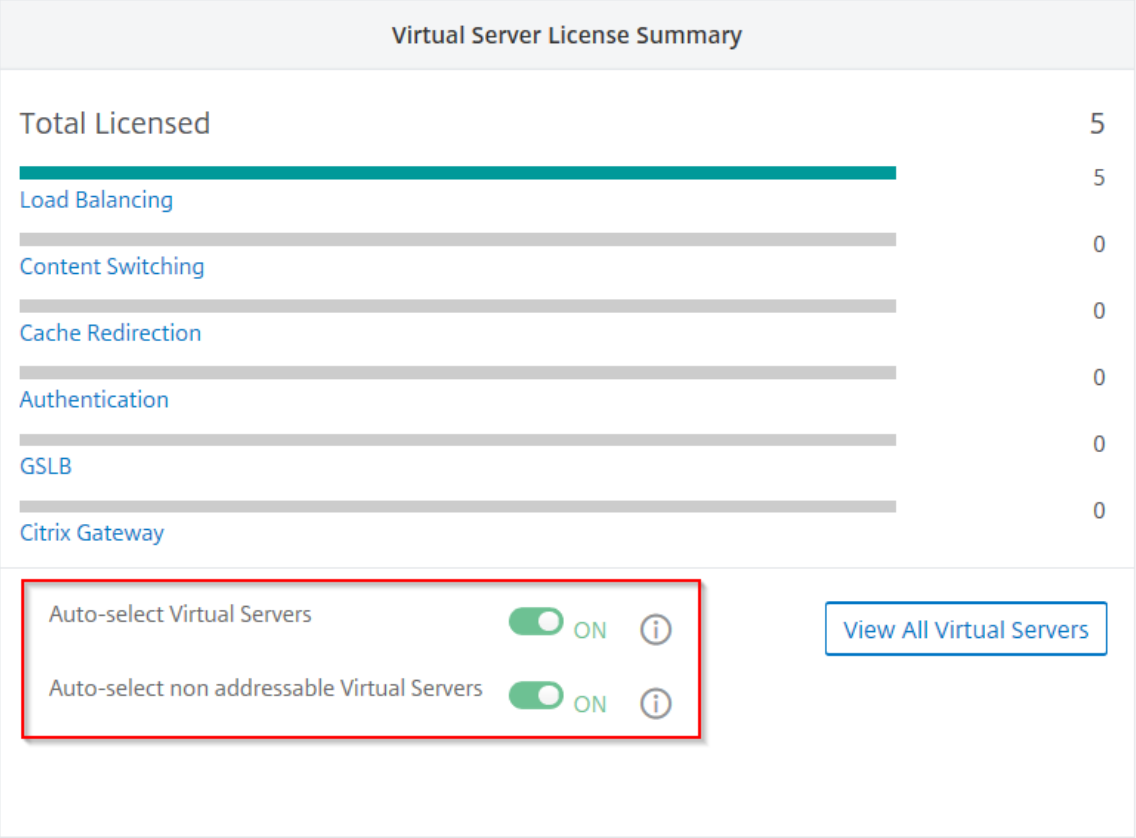
### Inhabilitar la concesión de licencias automáticas de servidores virtuales

1. Vaya a **Sistema > Licencias y análisis**.

   El panel muestra las licencias de servidor virtual disponibles, los servidores virtuales administrados junto con el tipo de servidor virtual e información sobre la caducidad de la licencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En **Asignación de licencias de servidor virtual**, inhabilite **los servidores virtuales con licencia automática** y **seleccione automáticamente los servidores virtuales no direccionables**.



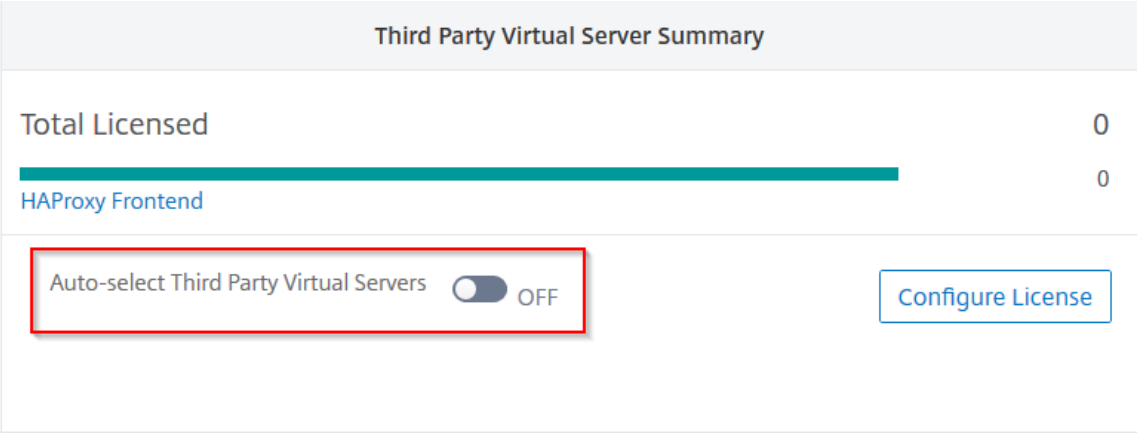

**Seleccionar servidores virtuales de terceros para la concesión de licencias**

1. Vaya a **Sistema > Licencias y análisis**.

   El panel muestra las licencias de servidor virtual disponibles, los servidores virtuales administrados junto con el tipo de servidor virtual e información sobre la caducidad de la licencia.

2. En **Resumen de servidores virtuales de terceros**, desactive la **selección automática de servidores virtuales de terceros**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Aplicar licencias de servidor virtual manualmente

Puede aplicar licencias manualmente a un servidor virtual individual.

1. En **Asignación de licencias de servidor virtual**, seleccione **Configurar licencias**.

   Aparece la página **Todos los servidores** virtuales.
2. Filtrar servidores virtuales sin licencia mediante la propiedad:`Licensed: No`.
3. Seleccione el servidor virtual que quiere licenciar.
4. Haga clic en **Licencia**.

### Configurar licencias de servidor virtual basadas en directivas

Puede configurar una directiva para aplicar la licencia a los servidores virtuales. Esta directiva controla el número de servidores virtuales que quiere conceder licencias automáticas. También aplica licencias solo a los servidores virtuales de las instancias seleccionadas.

Haga clic en **Modificar directivas** y puede especificar lo siguiente:

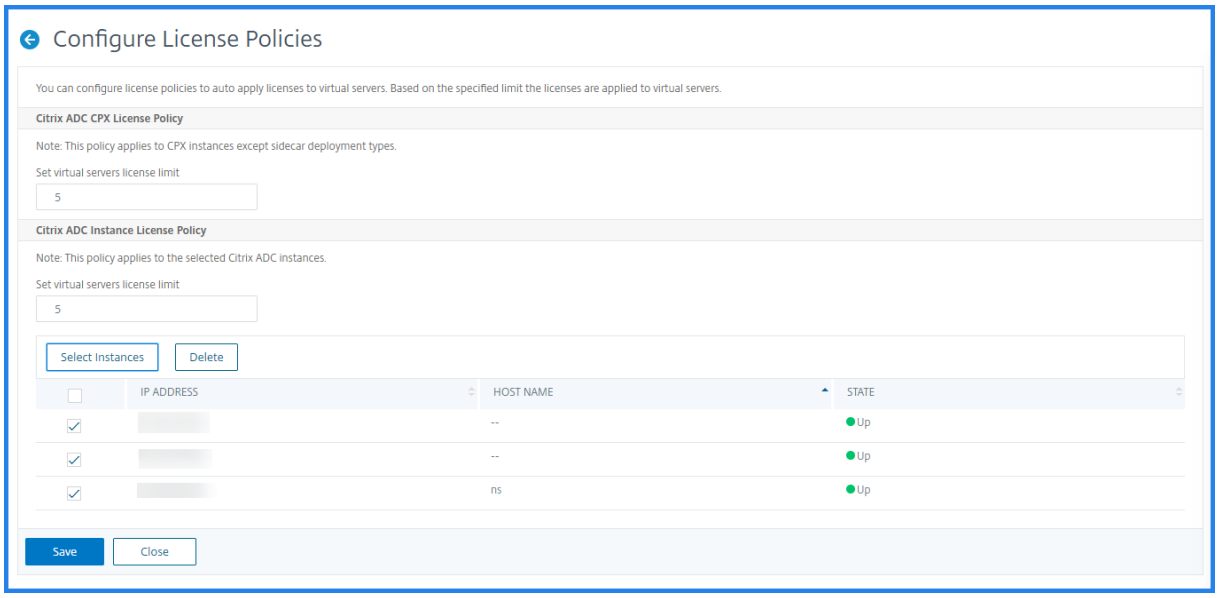
- Establezca el límite de servidores virtuales en instancias CPX por separado para aplicar licencias. ADM aplica licencia a servidores virtuales en instancias CPX hasta un límite especificado.

  > **Importante**
  >
  > Este límite se aplica a las instancias CPX, excepto a los tipos de implementación sidecar.
  >
  > Para ver las instancias CPX de los tipos de implementación de sidecar, filtre los servidores virtuales mediante la propiedad: `License Type: Freely Managed`.

- Establezca el límite de servidores virtuales en instancias ADC seleccionadas (MPX/VPX/BLX) para aplicar licencias. El ADM aplica licencias a los servidores virtuales en las instancias de ADC hasta un límite especificado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Seleccione las instancias de ADC prioritarias para aplicar las licencias de servidor virtual. Por lo tanto, ADM solo puede aplicar licencia a los servidores virtuales de instancias seleccionadas.




## Ver los servidores virtuales con licencia

Una vez aplicadas las licencias a los servidores virtuales, puede ver los servidores virtuales con licencia o los servidores virtuales de terceros en la página **Licencias y análisis**. Para ver los servidores virtuales con licencia, realice lo siguiente:

1. Vaya a **Sistema > Licencias y análisis**.
2. Haga clic en el tipo de servidor virtual en la sección **Total de licencias** del **Resumen de licencias de servidores virtuales**.

## Configurar la compatibilidad con licencias automáticas para servidores virtuales no direccionables

Citrix ADM, de forma predeterminada, no aplica licencias automáticamente a servidores virtuales no direccionables. Para obtener licencias de servidores virtuales no direccionables, debe inhabilitar la opción de licencia automática y seleccionar manualmente los servidores virtuales no direccionables. Esto aumenta su esfuerzo por seleccionar manualmente los servidores no direccionables inicialmente cuando aplica las licencias. También debe seleccionar manualmente los nuevos servidores virtuales no direccionables cada vez que se agregan a la red.

Citrix ADM proporciona una opción en Citrix ADM en **Asignación de licencias de servidor virtual**. Si habilita la opción **Seleccionar automáticamente servidores virtuales no direccionables**, aplique automáticamente licencias servidores virtuales no direccionables.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> - Citrix ADM, de forma predeterminada, sigue sin seleccionar automáticamente los servidores virtuales no direccionables para las licencias.
> - Application Analytics (App Dashboard) es la única analítica admitida actualmente en servidores virtuales con licencia no direccionables.

## Comprobaciones de caducidad de licencias de servidores virtuales

Ahora puede ver el estado de Citrix ADM y establecer alertas para la caducidad de la licencia del servidor virtual.

**Para ver el estado de las licencias:**

1. Vaya a **Redes**> **Licencias** > **Licencias de sistema.**
2. En la sección **Información de caducidad de licencia**, puede encontrar los detalles de las licencias que van a caducar:
   - **Función:**tipo de licencia que va a caducar.
   - **Recuento:** número de instancias o servidores virtuales que se ven afectados.
   - **Días hasta la fecha de caducidad:**número de días que quedan antes de la fecha de caducidad.

**Para configurar los valores de notificación de las licencias:**

1. Vaya a **Redes** > **Licencias** > **Configuración**.
2. En la sección **Configuración de notificaciones**, haga clic en el icono del lápiz y modifique los parámetros.
   - **Perfil de correo electrónico:** Perfil de correo electrónico o lista de distribución para enviar notificaciones cuando las licencias alcancen el umbral o vayan a caducar.
   - **SMS (mensaje de texto):** perfil SMS o lista de distribución para enviar notificaciones cuando las licencias alcanzan el umbral o van a caducar.
   - **Slack**: Especifique los detalles del perfil Slack.
   - **Alertas de PagerDuty**: Especifique un perfil de PagerDuty. Según la configuración de notificaciones configurada en su portal de PagerDuty, se envía una notificación cuando sus certificados están a punto de caducar.
   - **Notificarme:** defina el porcentaje de licencias agrupadas para notificar a los administradores por correo electrónico o SMS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Umbral de caducidad de licencia:** Número de días antes de que expire el número de licencias determinadas por Alert Threshold.
- **Caducidad de licencias:** Número de días restantes antes de la expiración.

## Requisitos del sistema

January 30, 2024

Antes de instalar Citrix Application Delivery Management (ADM), debe comprender los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencia y las limitaciones.

### Requisitos de Citrix ADM

| Componente | Requisito |
| --- | --- |
| RAM | 32 GB |
| CPU virtual | 8 CPUs<br>**Nota:** Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. |
| Espacio de almacenamiento | El espacio de almacenamiento predeterminado requerido es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Use la calculadora de tamaño que se menciona en la sección **Límites máximos** (página número 7) de la Guía de implementación de Citrix ADM HA. Esta guía está disponible en nuestro sitio de descargas, en **NetScaler MAS Release 12.1 > Versiones anteriores**. **Nota**: necesita una cuenta Citrix para acceder a la guía de implementación y a la calculadora de tamaño. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Componente | Requisito |
| --- | --- |
| | Si el requisito de almacenamiento Citrix ADM supera los 120 GB, debe adjuntar un disco adicional. Solo se puede agregar un disco adicional.<br>Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial.<br>Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |

> Nota
>
> Citrix ADM no es compatible con el chipset AMD.

### Requisitos para el agente de Citrix ADM on-prem

| Componente | Requisito |
| --- | --- |
| RAM | 32 GB |
| CPU virtual | 8 CPUs |
| Espacio de almacenamiento | 30 GB |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps |

> Nota
>
> El agente Citrix ADM no se admite en el chipset AMD.

### Se requiere una versión mínima de Citrix ADC para las funciones de Citrix ADM

> **Importante**
>
> La versión y compilación de Citrix ADM deben ser **iguales o superiores a** la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADM 12.1 compilación 50.39, asegúrese de haber

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> instalado Citrix ADC 12.1 compilación 50.28/50.31 o anterior.

| Función Citrix ADM | Versión del software Citrix ADC |
|---|---|
| StyleBooks | 10.5 y versiones posteriores |
| Compatibilidad con OpenStack/CloudStack | 11.0 y posteriores, si se requiere una partición |
| | 11.1 y posteriores, si se requiere una partición en una LAN virtual compartida |
| Soporte de NSX | 11.1 Compilación 47.14 y posteriores (VPX) |
| Soporte Mesos/Marathon | 10.5 y versiones posteriores |
| Copia de seguridad/Restauración | Para Citrix ADC, 10.1 y posteriores |
| | Para Citrix SDX, 11.0 y posteriores |
| Monitorización/generación de informes y configuración mediante trabajos | 10.1 y versiones posteriores |
| **Funciones de análisis** | |
| Información web | 10.5 y versiones posteriores |
| HDX Insight | 10.1 y versiones posteriores |
| Security Insight | 11.0.65.31 y posteriores |
| Gateway Insight | 11.0.65.31 y posteriores |
| Insight de caché | 10.5 y posteriores* |
| Insight SSL | 12.0 y versiones posteriores |

* Las métricas de caché integradas no se admiten en Citrix ADM con instancias de Citrix ADC que ejecutan la versión 11.0 build 66.x.

## Requisitos para la administración de instancias de Citrix SD-WAN

### Matriz de interoperabilidad de las ediciones/versiones de la plataforma Citrix SD-WAN y las funciones de Citrix ADM

| Modificación de plataforma | Citrix SD-WAN WANOP | Citrix SD-WAN SE | Citrix SD-WAN PE |
|---|---|---|---|
| **Detección** | Sí | Sí | Sí |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Modificación de plataforma | Citrix SD-WAN WANOP | Citrix SD-WAN SE | Citrix SD-WAN PE |
|---|---|---|---|
| **Configuración** | Sí | No | No |
| **Supervisión** | Sí | No | No |
| **Informes (informes de red)** | Sí | No | No |
| **Gestión de eventos** | Sí | No | No |
| **HDX Insight** | Sí | No | No |
| **WAN Insight** | Sí | No | No |
| **HDX Insight (implementación de varios saltos)** | Sí | Sí | No |

#### Clientes ligeros admitidos para instancias Citrix SD-WAN

Citrix ADM admite los siguientes clientes ligeros para supervisar las implementaciones de Citrix SD-WAN:

- Cliente ligero Dell Wyse WTOS modelo R10L Rx0L
- NComputing N400
- Dell Wyse WTOS Model CX0 C00X Xenith
- Dell Wyse WTOS Model TXO T00X Xenith2
- Dell Wyse WTOS Model CX0 C10LE
- Dell Wyse WTOS Model R00LX Rx0L HDX Thin Client
- Dell Wyse Enhanced SUSE Linux Enterprise, Model Dx0D, D50D
- Dell Wyse ZX0 Z90D7 (WES7) Thin Client

### Requisitos para el análisis de Citrix ADM

#### Versiones mínimas de Citrix Virtual Apps and Desktops requeridas para las funciones de Citrix ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Función Citrix ADM | Versión de Citrix Virtual Apps and Desktops |
|---|---|
| HDX Insight | Citrix Virtual Apps and Desktops 7.0 y posteriores |

> **Nota**
>
> La función Citrix Gateway (con la marca Access Gateway Enterprise para las versiones 9.3 y 10.x) debe estar disponible en la instancia de Citrix ADC. Citrix ADM no admite dispositivos Access Gateway Standard independientes.

Citrix ADM puede generar informes para aplicaciones que se publican en Citrix Virtual Apps o Citrix Virtual Desktops y a las que se accede a través de Citrix Receiver. Sin embargo, esta capacidad depende del sistema operativo en el que esté instalado Receiver. Actualmente, un Citrix ADC no analiza el tráfico ICA para aplicaciones o escritorios a los que se accede a través de Citrix Receiver que se ejecutan en sistemas operativos iOS o Android.

**Clientes ligeros compatibles con conocimientos de HDX**

- Clientes ligeros basados en Dell Wyse Windows
- Clientes ligeros basados en Dell Wyse Linux
- Clientes ligeros basados en Dell Wyse ThinOS
- Clientes ligeros basados en Ubuntu 10ZiG
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

**Se requiere una licencia de instancia de Citrix ADC para HDX Insight**

Los datos recopilados por Citrix ADM para HDX Insight dependen de la versión y las licencias de las instancias de Citrix ADC que se están supervisando. Los informes de HDX Insight solo se muestran en los dispositivos Citrix ADC Premium y Advanced que ejecutan la versión 10.5 y versiones posteriores.

| Licencia y duración de Citrix ADC | 5 minutos | 1 hora | 1 día | 1 semana | 1 mes |
|---|---|---|---|---|---|
| Estándar | No | No | No | No | No |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | | | | | |
|---|---|---|---|---|---|
| Avanzado | Sí | Sí | No | No | No |
| Premium | Sí | Sí | Sí | Sí | Sí |

## Hipervisores compatibles

En la siguiente tabla se enumeran los hipervisores admitidos por Citrix ADM.

| Hipervisor | Versiones |
|---|---|
| Citrix Hypervisor | 7.1 y 7.4 |
| VMware ESX | 6.0, 6.5, 6.7 y 7.0 |
| Microsoft Hyper-V | 2012 R2 y 2016 |
| KVM genérico | RHEL 7.4 y Ubuntu 16.04 |

## Sistemas operativos y versiones de receptor compatibles

En la siguiente tabla se enumeran los sistemas operativos compatibles con Citrix ADM y las versiones de Citrix Receiver que se admiten actualmente con cada sistema:

| Sistema operativo | Versión de Receiver |
|---|---|
| Windows | Edición estándar 4.0 |
| Linux | 13.0.265571 y posteriores |
| Mac | 11.8, compilación 238301 y posteriores |
| HTML5 | 1.5* |
| Aplicación Chrome | 1.5* |

* Aplicable con la versión 7.4 y posteriores de Citrix CloudBridge (Citrix SD-WAN WANOP).

## Exploradores web compatibles

En la siguiente tabla se enumeran los exploradores web compatibles con Citrix ADM:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Explorador web | Versión |
|---|---|
| Microsoft Edge | 79 y versiones posteriores |
| Google Chrome | 51 y versiones posteriores |
| Safari | 10 y versiones posteriores |
| Mozilla Firefox | 52 y versiones posteriores |

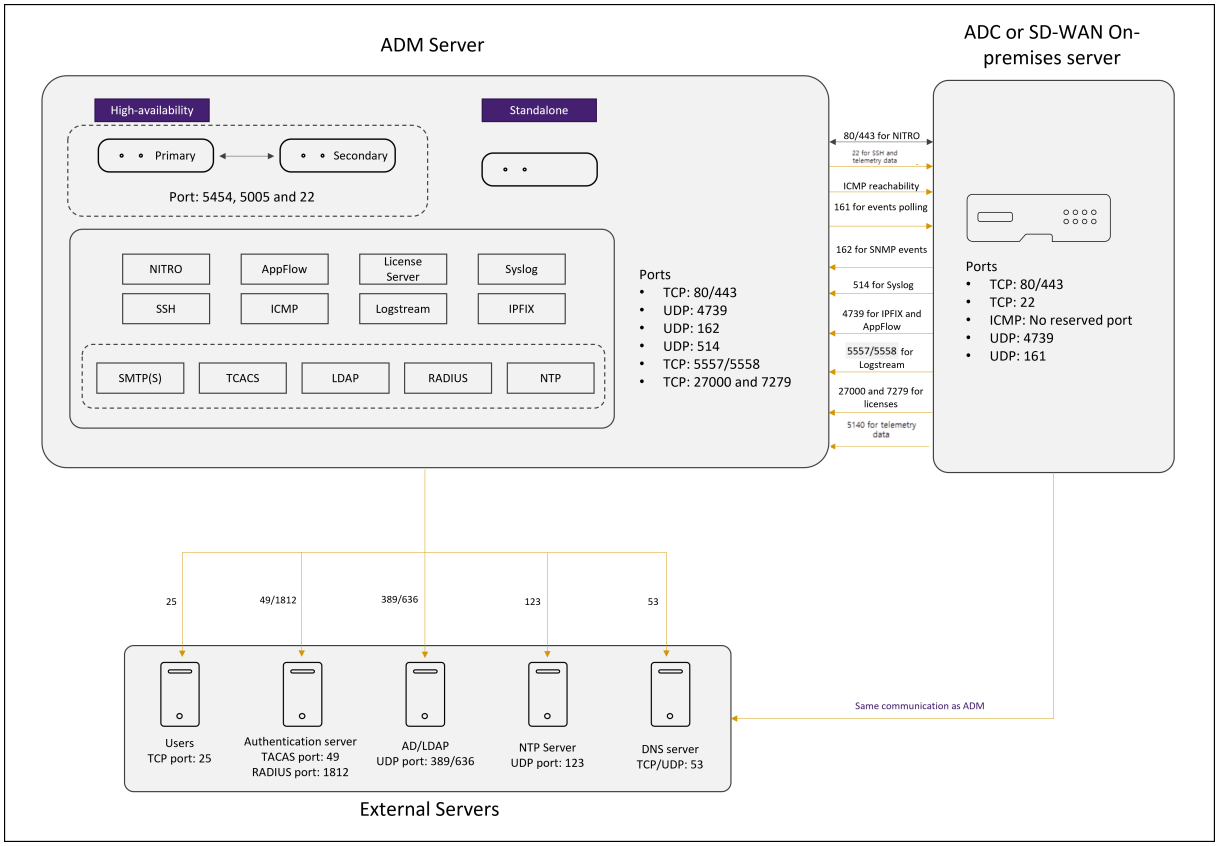
## Puertos compatibles

Citrix ADM utiliza la dirección IP de Citrix ADC (conocida como NSIP) para comunicarse con Citrix ADC. Puede utilizar el agente ADM como intermediario entre la instancia ADC y ADM o la instancia de SD-WAN y ADM. Para establecer una comunicación con estos servidores, abra los puertos necesarios.

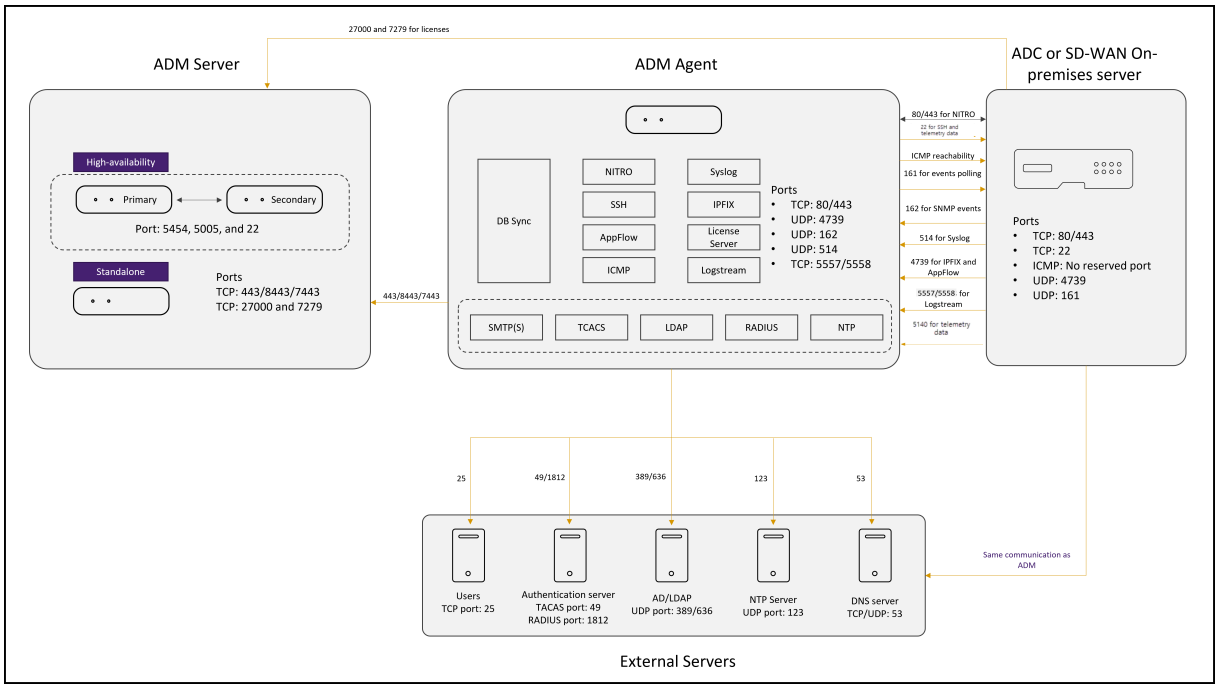
> **Nota**
>
> Si ha configurado Citrix ADC en modo Alta disponibilidad, Citrix ADM utiliza la dirección IP de subred (Management SNIP) de Citrix ADC para comunicarse con Citrix ADC. Para la comunicación mediante SNIP con Citrix ADM, los puertos requeridos siguen siendo los mismos.

**Diagrama de puertos de red para la implementación sin agentes:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Diagrama de puertos de red para la implementación que incluye el agente ADM:




Las siguientes secciones explican los puertos requeridos y su finalidad:

- Servidor ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Agente ADM
- Instancia de ADC o SD-WAN
- Servidores externos

**Puertos para el servidor ADM**

En esta tabla se explican los puertos necesarios que deben estar abiertos en el servidor ADM.

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 5454 y 22 | TCP | Puerto predeterminado para la comunicación y sincronización de bases de datos entre nodos Citrix ADM en modo de alta disponibilidad. | Nodo principal de Citrix ADM a nodo secundario de Citrix ADM |
| 443/8443/7443 | TCP | Puerto para la comunicación entre el agente Citrix ADM y Citrix ADM. | El agente Citrix ADM inicia la comunicación con Citrix ADM. A continuación, Citrix ADM y el agente interactúan entre sí. |

Si las instancias ADM y ADC no utilizan un agente para la comunicación, asegúrese de abrir los siguientes puertos en el servidor ADM:

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 80/443 | TCP | Para comunicación NITRO desde Citrix ADM a Citrix ADC o instancia de Citrix SD-WAN. | Agente de Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM agente |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 4739 | UDP | Para la comunicación de AppFlow desde Citrix ADC o Citrix SD-WAN instancia a Citrix ADM. | Agente de Citrix ADC o Citrix SD-WAN a Citrix ADM |
| 162 | UDP | Para recibir eventos SNMP desde la instancia de Citrix ADC a Citrix ADM. | Citrix ADC a agente Citrix ADM |
| 514 | UDP | Para recibir mensajes de syslog desde Citrix ADC o una instancia de Citrix SD-WAN a Citrix ADM. | Agente de Citrix ADC o Citrix SD-WAN a Citrix ADM |
| 5557/5558 | TCP | Para la comunicación logstream (para Security Insight, Web Insight y HDX Insight) desde Citrix ADC a Citrix ADM. | Citrix ADC a Citrix ADM |
| 5005 | TCP | Puerto para intercambiar latidos entre los nodos HA. | De nodo principal a nodo secundario de Citrix ADM. De nodo secundario a nodo principal de Citrix ADM. |

**Puertos para el agente ADM**

En esta tabla se explican los puertos necesarios que deben estar abiertos en el agente ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 80/443 | TCP | Para comunicación NITRO desde Citrix ADM a Citrix ADC o instancia de Citrix SD-WAN. | Agente de Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM agente |
| 4739 | UDP | Para la comunicación de AppFlow desde Citrix ADC o Citrix SD-WAN instancia a Citrix ADM. | Agente de Citrix ADC o Citrix SD-WAN a Citrix ADM |
| 162 | UDP | Para recibir eventos SNMP desde la instancia de Citrix ADC a Citrix ADM. | Citrix ADC a agente Citrix ADM |
| 514 | UDP | Para recibir mensajes de syslog desde Citrix ADC o una instancia de Citrix SD-WAN a Citrix ADM. | Agente de Citrix ADC o Citrix SD-WAN a Citrix ADM |
| 5557/5558 | TCP | Para la comunicación logstream (para Security Insight, Web Insight y HDX Insight) desde Citrix ADC a Citrix ADM. | Citrix ADC a Citrix ADM |

**Puertos para instancias ADC y SD-WAN**

En esta tabla se explican los puertos necesarios que deben estar abiertos en las instancias de Citrix ADC y SD-WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 80/443 | TCP | Para la comunicación NITRO desde Citrix ADM a Citrix ADC o Citrix SD-WAN instance.443. Para la comunicación NITRO entre servidores Citrix ADM en modo de alta disponibilidad. | Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM |
| 22 | TCP | Para la comunicación SSH desde Citrix ADM a Citrix ADC o instancia de Citrix SD-WAN. Para la sincronización entre los servidores Citrix ADM implementados en modo de alta disponibilidad. Además, este puerto es necesario para la comunicación SSH entre el agente ADM y Citrix ADC. | Citrix ADM a Citrix ADC. O bien, el agente de Citrix ADM a Citrix ADC. |
| Sin puerto reservado | ICMP | Detectar la accesibilidad de la red entre las instancias Citrix ADM y Citrix ADC, las instancias SD WAN o el servidor Citrix ADM secundario implementado en modo de alta disponibilidad. | Citrix ADM a Citrix ADC |
| 161 | UDP | Para sondear eventos de instancias de ADC. | Citrix ADM a Citrix ADC |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota:**
>
> En la implementación de alta disponibilidad de ADM, todas las comunicaciones de ADM utilizan la dirección IP del nodo principal.

**Puertos para servidores externos**

En esta tabla se explican los puertos necesarios que deben estar abiertos en servidores externos:

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 25 | TCP | Para enviar notificaciones SMTP desde Citrix ADM a los usuarios. | Citrix ADM a los usuarios. |
| 389/636 | TCP | Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo LDAP. | Servidor de autenticación externa de Citrix ADM a LDAP |
| 123 | UDP | Puerto de servidor NTP predeterminado para, sincronización con varias fuentes de tiempo. | Citrix ADM a servidor NTP |
| 1812 | RADIUS | Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo RADIUS. | Citrix ADM a servidor de autenticación externa RADIUS |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Puerto | Tipo | Detalles | Dirección de comunicación |
|---|---|---|---|
| 49 | TACACS | Puerto predeterminado para el protocolo de autenticación. Para la comunicación entre Citrix ADM y el servidor de autenticación externo TACACS. | Citrix ADM a servidor de autenticación externa TACACS |

**Limitaciones**

Desde Citrix ADM 12.1 o posterior, las siguientes funciones admiten el formato IPv6 de las direcciones IP:

1. Acceso de administración para la GUI de Citrix ADM
2. Acceso de administración para Citrix ADC
3. Registro e inventario
4. Panel de mandos de las redes
5. Tablero SSL
6. Trabajos de configuración
7. Auditoría de configuración
8. Funciones de red
9. Informes de red
10. Copia de seguridad y restauración de instancias de ADC
11. Eventos SNMP de Citrix ADC

Las siguientes funciones no admiten IPv6:

1. IP flotante de alta disponibilidad
2. Syslogs recibidos de ADC que admiten IPv6
3. StyleBooks en ADC que admiten IPv6
4. Análisis
5. Licencias agrupadas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Introducción

January 30, 2024

En este documento se explica cómo empezar a implementar y configurar NetScaler Application Delivery Management (ADM) por primera vez. Este documento está dirigido a administradores de redes y aplicaciones que administran dispositivos de red Citrix (Citrix SD-WAN WO, NetScaler Gateway, etc.) y también dispositivos de terceros, como HAProxy. Siga los pasos de este documento independientemente del tipo de dispositivo que tenga previsto administrar con NetScaler ADM.

Si ya es usuario de NetScaler ADM, se recomienda revisar las notas de la versión,los requisitos del sistemay los detalles de las licencias antes de actualizar el servidor a la última versión de NetScaler ADM.

## Paso 1: Revisar los requisitos del sistema

Antes de empezar a implementar Citrix ADM en su centro de datos, revise los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencias y las limitaciones.

- **Información sobre la licencia**. Puede administrar y supervisar cualquier número de instancias y entidades sin licencia. Sin embargo, solo puede administrar 30 aplicaciones descubiertas y ver la información de análisis de solo dos servidores virtuales sin solicitar una licencia. Para administrar más de 30 aplicaciones o para ver análisis de más de dos servidores virtuales, debe adquirir las licencias adecuadas. Obtenga más información.
- **Requisitos del sistema operativo y del receptor**. Revise esta información para asegurarse de que tiene la versión correcta del receptor para los sistemas operativos compatibles. Obtenga más información.
- **Requisitos del explorador**. Para acceder a la GUI de NetScaler ADM, debe asegurarse de que dispone del explorador necesario y de la versión correcta. Obtenga más información.
- **Puertos**. Asegúrese de que los puertos requeridos estén abiertos para que NetScaler ADM se comunique con las instancias de NetScaler ADC o SD-WAN o con las instancias de NetScaler ADC y SD-WAN. Obtenga más información.
- **Requisitos de instancia de NetScaler ADC**. Las diferentes versiones del software NetScaler ADC admiten diferentes funciones de NetScaler ADM. Revise esta información para asegurarse de que ha actualizado las instancias de NetScaler ADC a la versión correcta. Obtenga más información.
- **Requisitos de instancia Citrix SD-WAN**.Revise esta información para asegurarse de que ha actualizado las instancias de Citrix SD-WAN a la versión correcta y de que dispone de las ediciones de plataforma correctas. Obtenga más información.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Paso 2: Implementar NetScaler ADM

Para administrar y supervisar las aplicaciones y la infraestructura de red, primero debe instalar NetScaler ADM en uno de los hipervisores. Puede implementar NetScaler ADM como un único servidor o en un modo de alta disponibilidad. Si utiliza NetScaler ADC Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, monitoreo, orquestación y administración de aplicaciones, además de las funciones de análisis.

- **Despliegue**de un solo servidor .En una implementación de un solo servidor de NetScaler ADM, la base de datos se integra con el servidor y un solo servidor procesa todo el tráfico. Puede implementar NetScaler ADM con Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM. Consulte:
  - Citrix ADM con Citrix Hypervisor
  - NetScaler ADM con Microsoft Hyper-V
  - NetScaler ADM con VMware ESXi
  - NetScaler ADM con servidor KVM Linux
- **Implementación de alta disponibilidad.** Una implementación de alta disponibilidad (HA) de dos servidores NetScaler ADM proporciona operaciones ininterrumpidas. En una configuración de alta disponibilidad, ambos nodos de NetScaler ADM deben implementarse en modo activo-pasivo, en la misma subred con la misma versión y compilación de software, y deben tener las mismas configuraciones. Con la implementación de HA, la capacidad de configurar la dirección IP flotante en el nodo principal de NetScaler ADM elimina la necesidad de un equilibrador de carga de NetScaler ADC independiente. Para obtener más información, consulteConfigurar en una implementación de alta disponibilidad.

### Paso 3: Agregar instancias a NetScaler ADM

Las instancias son dispositivos Citrix o dispositivos virtuales o dispositivos de terceros que desea descubrir, administrar y supervisar desde Citrix ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias. Puede agregar las siguientes instancias a NetScaler ADM:

- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - Citrix ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HAProxy

Cuando agrega una instancia al servidor NetScaler ADM, el servidor se comunica implícitamente con las instancias y recopila un inventario de estas instancias.

Más información

### Paso 4: Habilitar el análisis en servidores virtuales

Para ver los datos de análisis del flujo de tráfico de su aplicación, debe habilitar la función de análisis en los servidores virtuales que reciben tráfico para las aplicaciones específicas.

Más información

### Paso 5: Configurar el servidor NTP en NetScaler ADM

Debe configurar un servidor de Protocolo de hora de red (NTP) en NetScaler ADM para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

Más información

### Paso 6: Configurar la configuración del sistema para un rendimiento óptimo de NetScaler ADM

Antes de empezar a usar NetScaler ADM para administrar y supervisar sus instancias y aplicaciones, se recomienda configurar algunos parámetros del sistema que garanticen un rendimiento óptimo del servidor NetScaler ADM.

- **Configure las alarmas del sistema**. Configure las alarmas del sistema para asegurarse de que conoce cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor.
- **Configure las notificaciones del sistema**. Puede enviar notificaciones a grupos de usuarios seleccionados para diversas funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en NetScaler ADM y configurar servidores de Gateway de correo electrónico y servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y texto a

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

los usuarios. Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el inicio de sesión del usuario o el reinicio del sistema.

- **Configure las opciones de poda del sistema**.Para limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).
- **Configure las opciones de copia de seguridad del sistema**. NetScaler ADM realiza automáticamente una copia de seguridad del sistema todos los días a las 00:30 horas. De forma predeterminada, guarda tres archivos de copia de seguridad. Es posible que desee conservar un mayor número de copias de seguridad del sistema.
- **Configure las opciones de copia de seguridad de instancia**. Si realiza una copia de seguridad del estado actual de una instancia de NetScaler ADC, puede usar los archivos de copia de seguridad para restaurar la estabilidad en caso de que la instancia se vuelva inestable. Hacerlo es especialmente importante antes de realizar una actualización. De forma predeterminada, se realiza una copia de seguridad cada 12 horas y se conservan tres archivos de respaldo en el sistema.
- **Configure los parámetros de poda del evento de instancia**.Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00:00 horas).
- **Configure la configuración de purga del syslog de la instancia**. Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días después de los cuales se eliminarán los siguientes datos de syslog de NetScaler ADM:
  - Datos genéricos de Syslog
  - Datos de AppFirewall
  - Datos de NetScaler Gateway.

    Más información

## A continuación

Una vez que haya implementado y configurado NetScaler ADM, puede empezar a administrar y monitorear sus instancias y aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Administración de instancias y aplicaciones de Citrix ADC.** Todas las funciones de NetScaler ADM son compatibles con las instancias de NetScaler ADC. Puede empezar a utilizar cualquiera de las funciones.

**Administración de instancias**de SD-WAN de Citrix ADC . No todas las funciones de NetScaler ADM son compatibles con las instancias WO de SD-WAN; por ejemplo, no se admite la administración de certificados o la auditoría de configuración. Para obtener información sobre qué funciones se admiten y cómo usarlas, consulte Administración de WO de Citrix SD-WAN con NetScaler ADM.

**Gestión de instancias y aplicaciones de HAProxy**. Puede supervisar los front-ends, los back-ends y los servidores configurados en una implementación de HAProxy. También puede utilizar la función Administración de aplicaciones para supervisar las estadísticas en tiempo real de los front-end supervisados por NetScaler ADM. Para obtener más información sobre las funciones compatibles con HAProxy y cómo usarlas, consulte Administración y supervisión de instancias de HAProxy mediante NetScaler ADM.

## Implementar

January 30, 2024

Antes de usar NetScaler ADM para administrar y monitorear las aplicaciones y la infraestructura de red, primero debe instalarlo en uno de los hipervisores o en un clúster de Kubernetes. Si implementa NetScaler ADM en un hipervisor, puede implementarlo como un único servidor o en modo de alta disponibilidad. El modo de alta disponibilidad no se aplica a un clúster de Kubernetes. Si utiliza NetScaler Insight Center, puede migrar a NetScaler ADM y aprovechar las funciones de administración, monitoreo, orquestación y administración de aplicaciones, además de las funciones de análisis.

- **Implementación de un solo servidor**: en el caso de un ADM independiente implementado en un hipervisor, la base de datos se integra con el servidor y un solo servidor procesa todo el tráfico. Puede implementar NetScaler ADM con Citrix Hypervisor, VMware ESXi, Microsoft Hyper-V y Linux KVM. Consulte:
  - Citrix ADM en Citrix Hypervisor
  - NetScaler ADM en Microsoft Hyper-V
  - NetScaler ADM en VMware ESXi
  - NetScaler ADM en el servidor KVM Linux
  - NetScaler ADM en el clúster de Kubernetes
- **Implementación de alta disponibilidad (HA) :**una implementación de alta disponibilidad de dos servidores Citrix ADM proporciona operaciones ininterrumpidas. En una configuración de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

HA, los dos nodos NetScaler ADM deben implementarse en modo activo-pasivo, en la misma subred con la misma versión de software y compilación, y deben tener las mismas configuraciones. Con la implementación de alta disponibilidad, la capacidad de configurar la dirección IP flotante en el nodo principal de NetScaler ADM elimina la necesidad de un equilibrador de carga independiente de NetScaler ADC. Consulte:Configurar en una implementación de alta disponibilidad.

> Nota La
>
> alta disponibilidad no es aplicable para ADM implementado en un clúster de Kubernetes.

- **Migre de NetScaler Insight Center a Citrix ADM**: puede migrar la implementación de NetScaler Insight Center a Citrix ADM sin perder la configuración, los parámetros o los datos existentes. Con NetScaler ADM no solo puede ver los distintos análisis generados por las instancias NetScaler ADC y Citrix SD-WAN, sino que también puede administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada. Consulte:Migración de NetScaler Insight Center a NetScaler ADM
- **Integre NetScaler ADM con Director: Director**se integra con NetScaler ADM para el análisis de red y la administración del rendimiento. Consulte: Integración de NetScaler ADM con Director

## Requisitos previos para instalar NetScaler ADM

January 30, 2024

Puede descargar e instalar Citrix Application Delivery Management (ADM) para las plataformas Microsoft HyperV,
VMware ESXi, Linux KVM y Citrix Hypervisor como un dispositivo virtual. Antes de instalar NetScaler ADM, debe comprender los requisitos de software, los requisitos del explorador, la información de puertos, la información de licencias y las limitaciones de todas estas plataformas.

Para conocer los requisitos de plataforma específicos y los pasos detallados para instalar Citrix ADM, consulte los siguientes temas:

- Citrix ADM con Citrix Hypervisor
- Citrix ADM con Microsoft Hyper-V
- NetScaler ADM con VMware ESXi
- NetScaler ADM con servidor KVM Linux

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Requisitos generales para Citrix ADM

| Componente | Requisito |
|---|---|
| RAM | 32 GB |
| CPU virtual | 8 CPUs |
| Espacio de almacenamiento | Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.<br>El espacio de almacenamiento predeterminado requerido es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Use la calculadora de tamaño que se menciona en la sección **Límites máximos** (página número 7) de la Guía de implementación de Citrix ADM HA. Esta guía está disponible en nuestro sitio de descargas, en **NetScaler MAS Release 12.1 > Versiones anteriores**. **Nota**: necesita una cuenta Citrix para acceder a la guía de implementación y a la calculadora de tamaño<br>Si el requisito de almacenamiento de NetScaler ADM supera los 120 GB, debe conectar un disco adicional.<br>Citrix recomienda que estime el almacenamiento y conecte un disco adicional en el momento de la implementación inicial. Solo puede agregar un disco adicional.<br>Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps |

> Nota:
>
> Citrix recomienda alojar el VHD de NetScaler ADM en un almacenamiento local. Cuando se aloja en dispositivos de almacenamiento en una SAN, es posible que NetScaler ADM no funcione como se esperaba. Por lo tanto, no se admite la implementación de ADM en SAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Citrix ADM en Citrix Hypervisor

January 30, 2024

Para instalar Citrix ADM en Citrix Hypervisor (anteriormente conocido como XenServer), primero debe descargar el archivo de imagen de Citrix ADM .xva en su equipo local. Debe utilizar Citrix XenCenter para realizar la instalación de Citrix ADM.

> **Nota:**
>
> Citrix ADM no admite XenMotion.

## Requisitos previos

Antes de instalar Citrix ADM, compruebe que se cumplen los siguientes requisitos:

- Citrix Hypervisor versión 7.1 o posterior está instalado en el hardware que cumple los requisitos mínimos.
- XenCenter se instala en una estación de trabajo de administración que cumple con los requisitos mínimos. Debe utilizar XenCenter para instalar Citrix ADM en Citrix Hypervisor.
- Ha descargado el archivo de imagen XVA de Citrix ADM.

## requisitos del sistema de XenCenter

XenCenter es una aplicación cliente de Windows. No puede ejecutarse en la misma máquina que el host de Citrix Hypervisor. En la siguiente tabla se describen los requisitos mínimos del sistema.

| Componente | Requisito |
|---|---|
| Sistema operativo | Windows 7, Windows Server 2003 o Windows 10 |
| .NET framework | Versión 2.0 o posterior |
| CPU | 750 MHz (MHz), recomendado: 1 gigahercio (GHz) o más rápido |
| RAM | 1 GB, Recomendado: 2 GB |
| NIC | NIC de 100 megabits por segundo (Mbps) o más rápido |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Instalación de Citrix Application Delivery Management

1. Importe el archivo de imagen XVA a su Citrix Hypervisor y, desde la ficha **Consola**, configure las opciones de configuración de red iniciales.

```
------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------
      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

2. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
3. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

4. Ejecute el script de implementación escribiendo el comando en el símbolo del shell: `/mps/deployment_type.py`

```
bash-3.2# deployment_type.py
------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

5. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

6. Escriba **Sí** para implementar Citrix ADM como una implementación independiente.
7. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Después de instalar Citrix ADM, puede actualizar los valores de configuración inicial más adelante.

### Verificación

Una vez instalado el servidor, puede acceder a la GUI escribiendo la dirección IP del servidor Citrix ADM en el explorador web. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración Citrix ADM.

## NetScaler ADM en Microsoft Hyper-V

January 30, 2024

Para instalar NetScaler ADM en Microsoft Hyper-V, primero debe descargar el archivo de imagen NetScaler ADM en el equipo local. Además, asegúrese de que el sistema tenga las extensiones de virtualización de hardware y compruebe que las extensiones de virtualización de la CPU estén disponibles.

### Requisitos previos

Antes de instalar el dispositivo virtual Citrix ADM, compruebe que se cumplen los siguientes requisitos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- La versión 6.2 o posterior de Microsoft Hyper-V se instala en un hardware que cumple los requisitos mínimos.
- Instale Microsoft Hyper-V Manager en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.
- Ha descargado el archivo de imagen Citrix ADM.

### Requisitos del sistema Microsoft Hyper-V

Microsoft Hyper-V es una aplicación cliente de Windows. En la siguiente tabla se describen los requisitos mínimos del sistema.

| Componente | Requisito |
|---|---|
| Sistema operativo | Windows Server 2012 R2 |
| .NET framework | Versión 2.0 o posterior |
| CPU | 750 MHz (MHz), recomendado: 1 gigahercio (GHz) o más rápido |
| RAM | 1 GB, Recomendado: 2 GB |
| NIC | NIC de 100 megabits por segundo (Mbps) o más rápido |

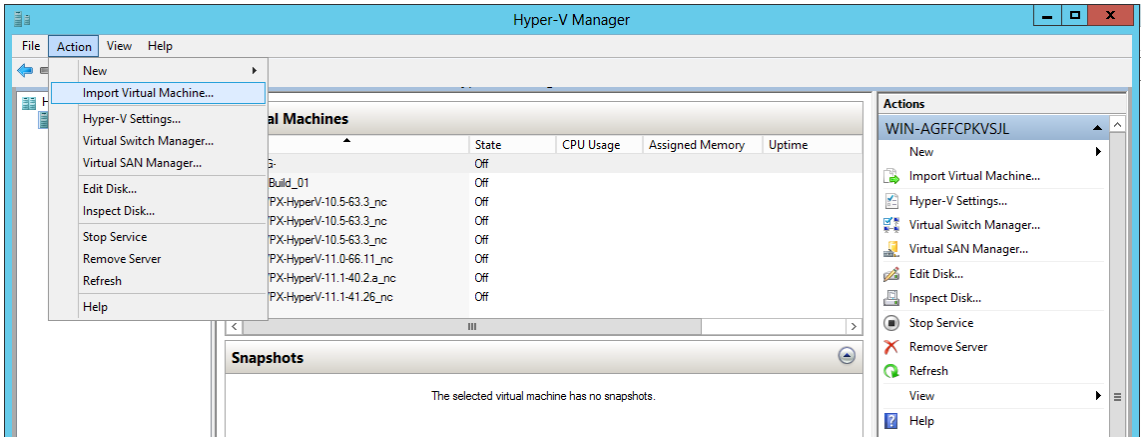
### Instalación de NetScaler Application Delivery Management

La cantidad de servidores Citrix ADM que puede instalar depende de la memoria disponible en el servidor Hyper-V.

**Para instalar NetScaler ADM:**

1. Inicie el cliente Hyper-V Manager en su estación de trabajo.
2. En el menú **Acción**, haga clic en **Importar máquina virtual**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. Importe la imagen de Hyper-V y haga lo siguiente:

   a) En el cuadro de diálogo Importar máquina virtual, en la sección **Localizar carpeta** , vaya a la carpeta en la que guardó la imagen de Citrix ADM Hyper-V, seleccione la carpeta y haga clic en **Siguiente**.

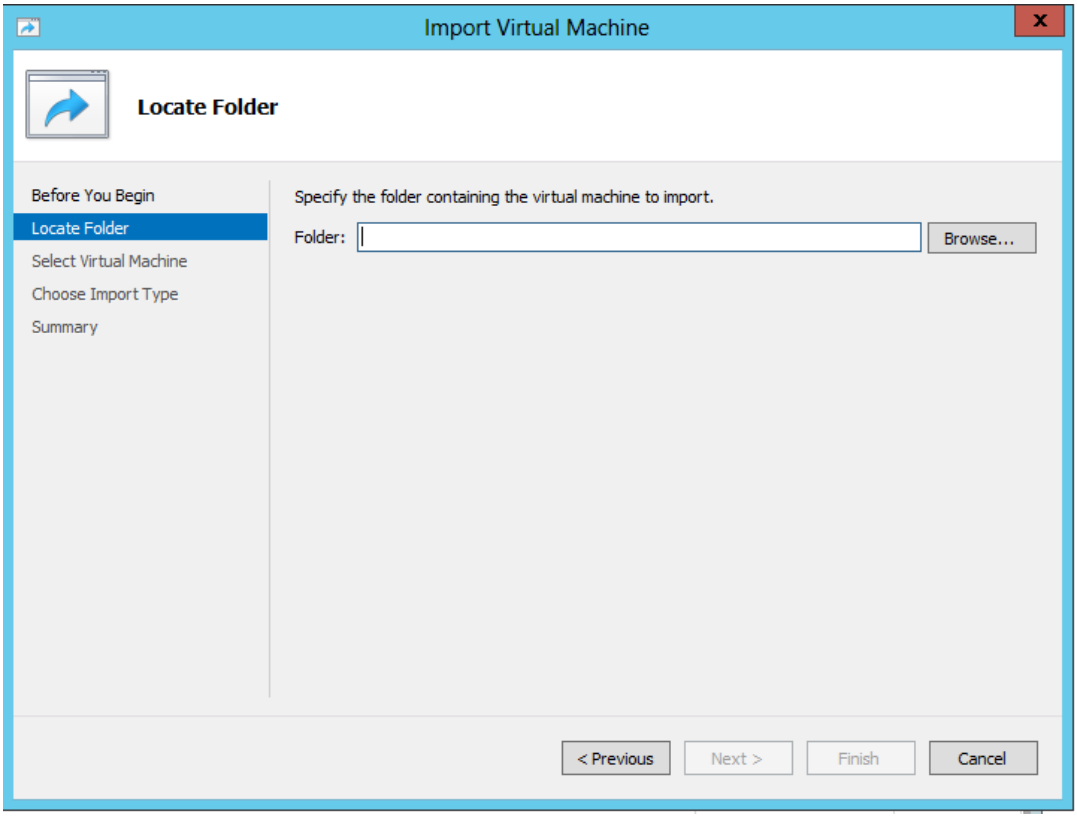
   b) En la sección Seleccionar máquina virtual, seleccione el nombre de máquina virtual correspondiente.

   c) En la sección **Elija el tipo de importación**, seleccione la opción Copiar la máquina virtual (crear un nuevo identificador único) y haga clic en Siguiente.

   d) En la sección **Elegir destino**, puede especificar las carpetas para almacenar los archivos de la máquina virtual.

   > **Nota**
   >
   > De forma predeterminada, el asistente importa los archivos de la máquina virtual a las carpetas predeterminadas de Hyper-V del host local.

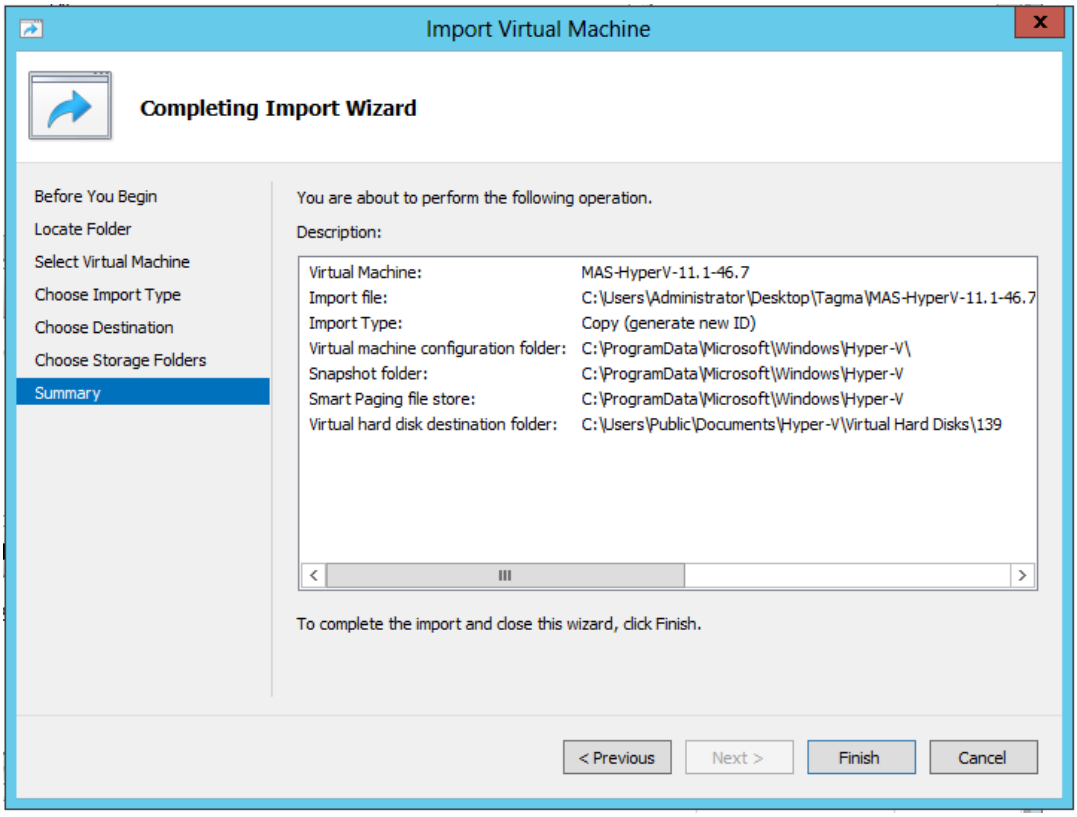
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




e) En la sección **Elegir carpetas de almacenamiento**, puede seleccionar la ubicación en la que desea almacenar los discos duros virtuales y, a continuación, hacer clic en **Siguiente**.

f) Puede comprobar los detalles de la máquina virtual en el panel de resumen y hacer clic en **Finalizar**.

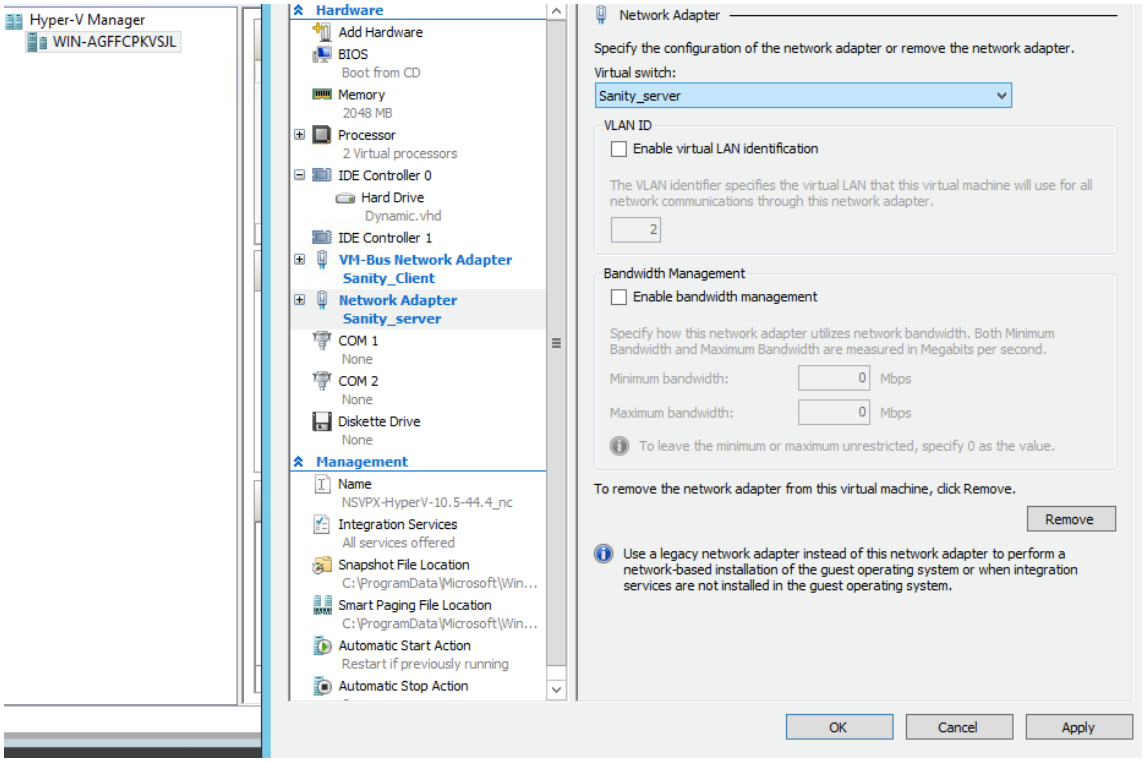
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La imagen de Citrix ADM Hyper-V aparece en el panel derecho.

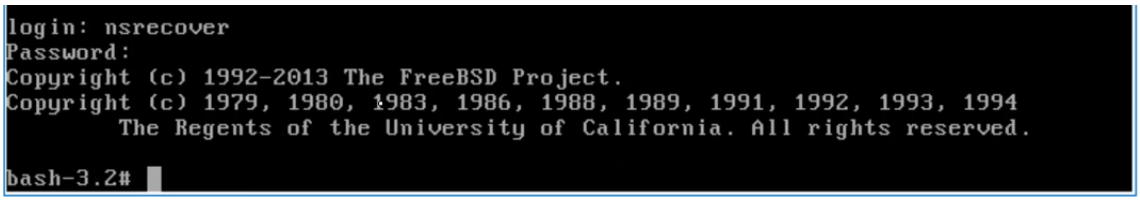
4. Haga clic con el botón secundario en la imagen de NetScaler ADM Hyper-V y, a continuación, haga clic en **Configuración**.
5. En el panel izquierdo del cuadro de diálogo que aparece, vaya a **Hardware** > **Adaptador de red VM_Bus**y, en el panel derecho, en la lista de redes, seleccione la red correspondiente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7. Haga clic con el botón derecho en la imagen de Citrix ADM Hyper-V y haga clic en **Conectar**.
8. En la ventana de la consola, haga clic en el botón **Inicio**.
9. Configure las opciones de configuración de red iniciales.

10. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.
11. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

12. Ejecute el script de implementación escribiendo el comando en la línea de comandos:

```
deployment_type.py
```

```
bash-3.2# deployment_type.py
-------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.

```
-------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. Escriba **Yes** para implementar Citrix ADM como implementación independiente.
15. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Después de instalar Citrix ADM, puede actualizar los valores de configuración inicial más adelante.

## Verificación

Una vez instalado el servidor, puede acceder a la interfaz gráfica de usuario escribiendo la dirección IP del servidor NetScaler ADM en la barra de direcciones del explorador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

El explorador muestra la utilidad de configuración Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# NetScaler ADM en VMware ESXi

January 30, 2024

Para instalar dispositivos virtuales NetScaler ADM en VMware ESXi, utilice el cliente VMware vSphere.

## Requisitos previos

Antes de comenzar a instalar un dispositivo virtual, compruebe que los siguientes requisitos:

- Instale una versión de VMware ESXi compatible (6.0, 6.5, 6.7 y 7.0).
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Descargue los archivos de configuración de NetScaler ADM.

> Nota
>
> VMotion solo es compatible con **NetScaler ADM 13.0 Build 47.22 o posterior**. Puede programar y automatizar la migración del servidor ADM implementado en un hipervisor ESXi, incluidas las configuraciones de vSphere de alta disponibilidad y vSphere DRS.

## Para instalar NetScaler ADM

> **Nota**
>
> Los pasos y las capturas de pantalla se basan en la versión 6.0 de VMware ESXi. La GUI puede diferir en otras versiones de ESXi. VMware ESXi versión 7.0.1c número de compilación 17325551 con adaptador VMXNET3 se admite en **NetScaler ADM 13.0 71.40 o posterior**. Consulte la documentación de VMware para conocer los pasos específicos de la versión.

1. Inicie el cliente de VMware vSphere en su estación de trabajo.
2. En el cuadro de texto **Dirección IP/Nombre**, escriba la dirección IP del servidor de VMware ESXi al que desea conectarse.
3. En los cuadros de texto **Nombre de usuario** y **Contraseña** , escriba las credenciales de administrador y, a continuación, haga clic **en**Iniciar sesión .
4. En el menú **Archivo**, haga clic en **Implementar plantilla OVF**.
5. En el cuadro de diálogo **Implementar plantilla de OVF**, en **Implementar desde un archivo o URL**, seleccione el archivo OVF y haga clic en **Siguiente**.

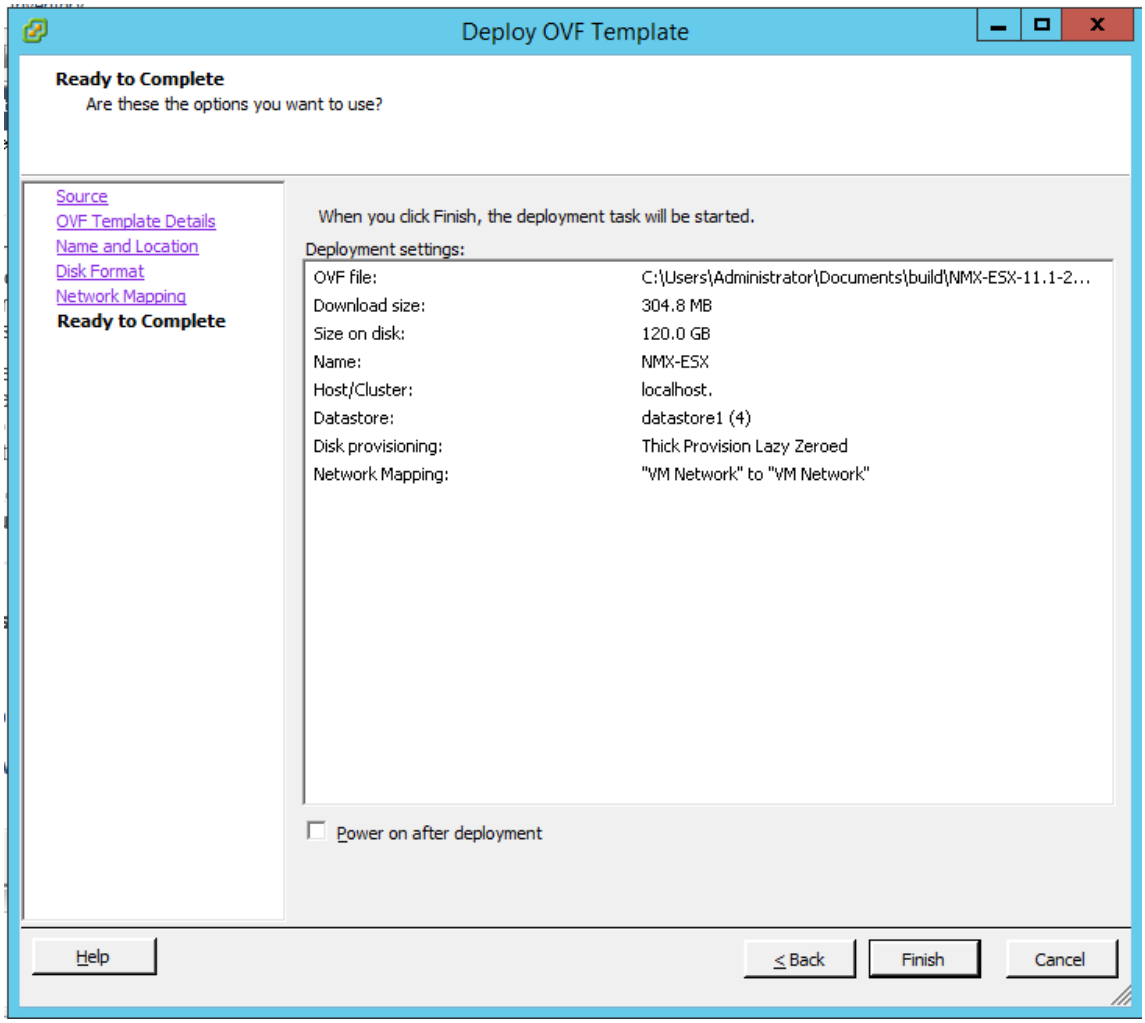
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Si aparece un mensaje de advertencia con el siguiente texto: El identificador del sistema operativo no es compatible con el host seleccionado, compruebe si el servidor VMware soporta el sistema operativo FreeBSD. Haga clic en **Sí**.

6. En la página **Detalles de plantilla de OVF**, haga clic en **Siguiente**.
7. Escriba un nombre para el dispositivo virtual NetScaler ADM y, a continuación, haga clic en **Siguiente**.
8. Especifique el formato de disco seleccionando Formato de aprovisionamiento fino o Formato de aprovisionamiento grueso.

> **Nota**
>
> Citrix recomienda seleccionar el **formato de aprovisionamiento grueso**.

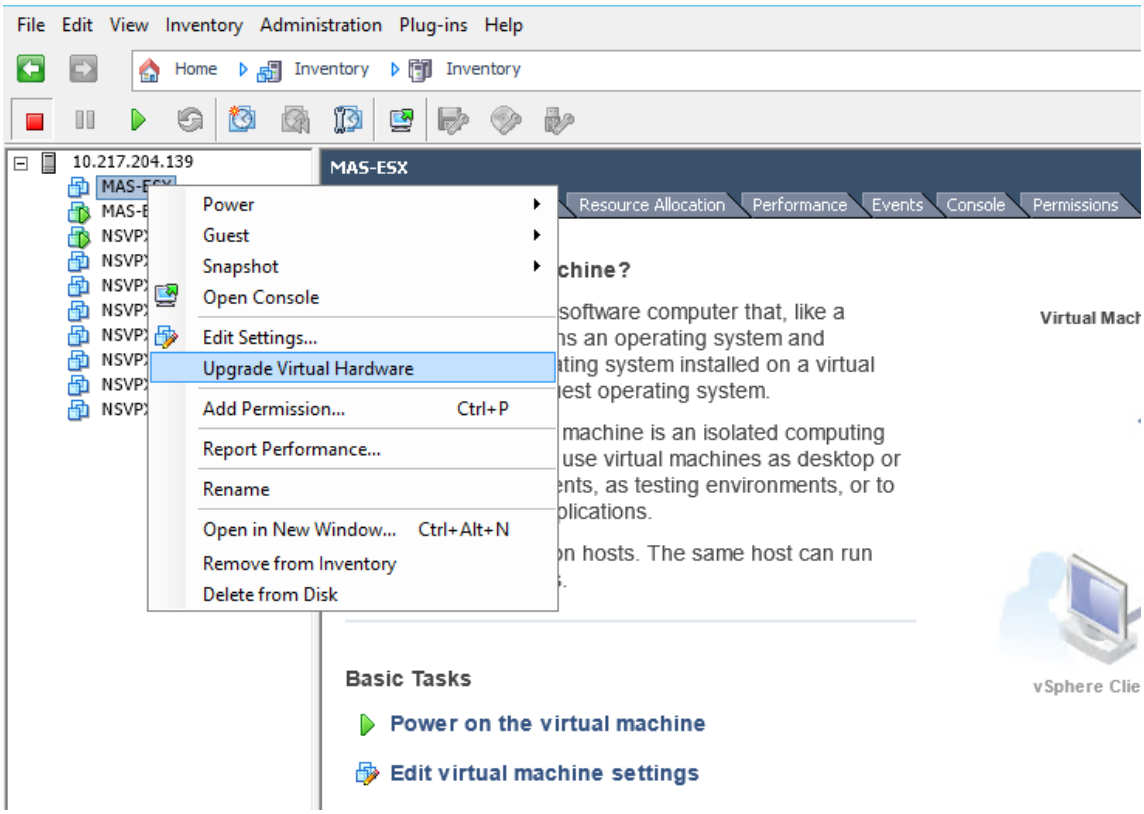
9. Haga clic en **Finalizar** para iniciar el proceso de instalación.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

10. Ya tiene todo listo para iniciar el dispositivo virtual NetScaler ADM.

11. En el panel de navegación, seleccione el dispositivo virtual que instaló. En el menú **Inventario**, haga clic con el botón derecho en la **máquina virtual** y, a continuación, haga clic en **Actualizar hardware virtual**. En el cuadro de diálogo **Confirmar máquina virtual**, haga clic en **Sí**.



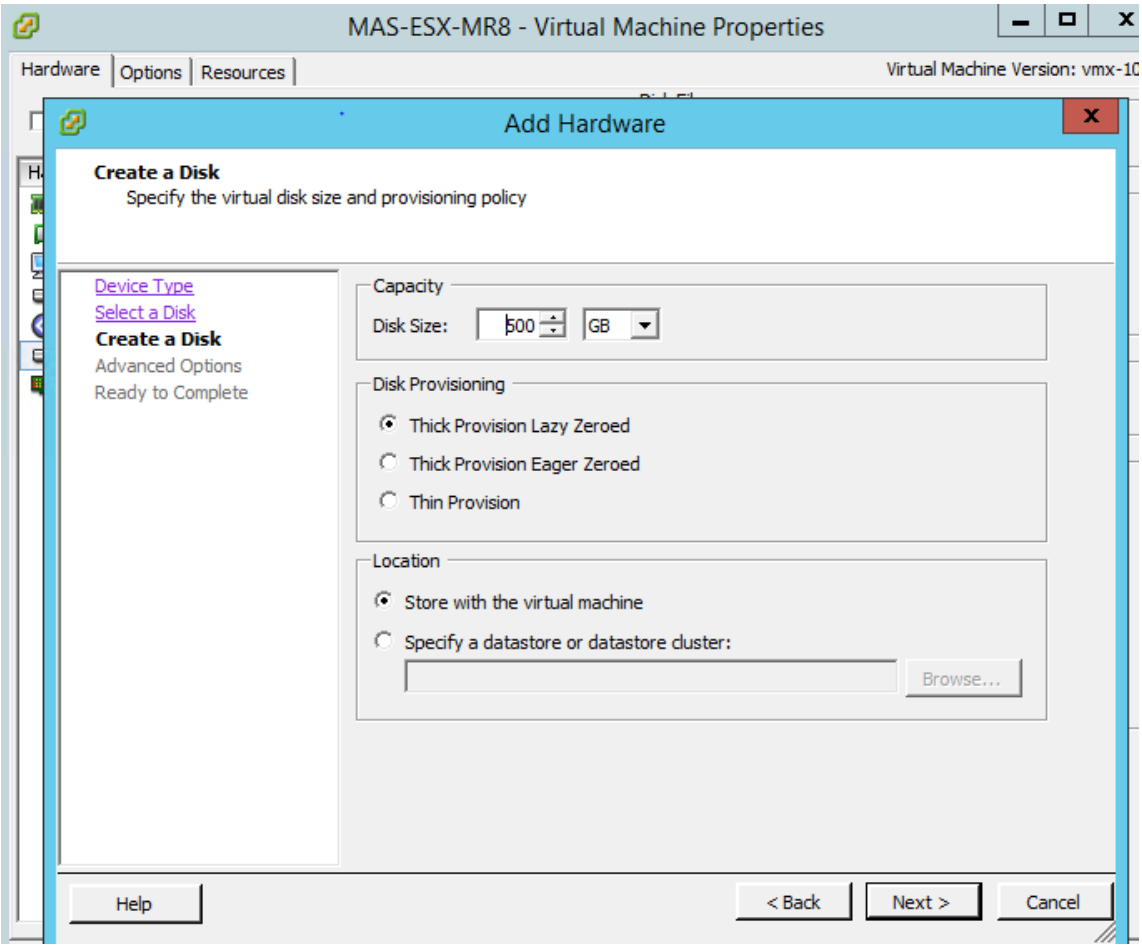

12. En el menú **Inventario**, haga clic en **Máquina virtual** y, a continuación, en **Modificar configuración**.

13. En el cuadro de diálogo **Propiedades de la máquina virtual**, en la ficha **Hardware**, haga clic en **Memoria** y, a continuación, en el panel derecho, especifique el **Tamaño de memoria** como 32 GB.

14. Haga clic en **CPU** y, a continuación, en el panel derecho, especifique las CPU como 8. Haga clic en **Aceptar**.

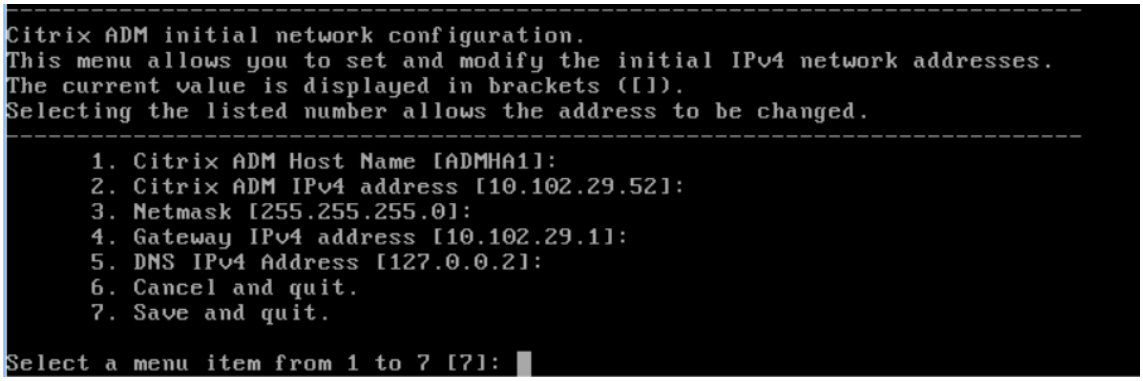
15. Agregue un disco adicional según sus necesidades.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




16. En el panel de navegación, seleccione el dispositivo virtual que instaló. En el menú **Inventario**, haga clic en **Máquina virtual**, en **Encender** y, a continuación, en **Encender**.

17. Haga clic en la ficha **Consola** para ver las opciones de Configuración de red inicial de NetScaler ADM.




18. Después de especificar las direcciones IP necesarias, guarde los valores de configuración.

19. Cuando se le solicite, inicie sesión con las credenciales nsrecover/nsroot.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
login: nsrecover
Password:
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

bash-3.2#
```

> **Nota**
>
> Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

20. Ejecute el script de implementación escribiendo el comando en la línea de comandos:

```
deployment_type.py
```

```
bash-3.2# deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

21. Seleccione el tipo de implementación como **Citrix ADM Server**. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

22. Escriba **Sí** para implementar Citrix ADM como una implementación independiente.
23. Escriba **Sí** para reiniciar el servidor de Citrix ADM.

> **Nota**
>
> Después de instalar Citrix ADM, puede actualizar los valores de configuración inicial más adelante.

## Verificación

Una vez instalado el servidor, puede acceder a la GUI escribiendo la dirección IP del servidor de NetScaler ADM en el explorador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son nsroot/nsroot.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El explorador muestra la utilidad de configuración Citrix ADM.

> **Nota**
>
> El tiempo típico de instalación de ADM es de unos 10 minutos en VMware ESXi, pero puede tardar más en algunos sistemas.

## Citrix ADM en clúster de Kubernetes

January 30, 2024

Antes de instalar dispositivos virtuales Citrix ADM en un clúster de Kubernetes, lea la sección de requisitos previos.

### Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos antes de instalar ADM.

#### Clúster de Kubernetes

- El clúster de Kubernetes debe ser de la siguiente versión o superior:
  - Versión del servidor v1.13
  - Versión de cliente v1.13

  Escriba el comando `kubectl version` para comprobar la versión.
- La aplicación Helm instalada en el clúster debe ser de la siguiente versión o superior.
  - Versión del servidor v2.12.1
  - Versión de cliente v2.12.0

  Use el comando `helm version` para comprobar la versión.
- El clúster de Kubernetes CNI (Container Network Interface) debe ser la versión de Calico v3.1.3 o superior.
- Todos los nodos subordinados del clúster deben tener instalado un cliente NFS. Esto se debe a que la aplicación ADM persiste los datos y la configuración en volúmenes montados en un servidor de archivos de red. Para instalar un cliente NFS en un subordinado basado en Ubuntu, escriba los siguientes comandos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
apt-get update
apt install nfs-common
```

- La aplicación ADM necesita 32 GB de memoria y 8 vCPU en el clúster y 120 GB de espacio en NFS.

#### Compartición de NFS

La aplicación ADM necesita volúmenes persistentes para almacenar datos como la configuración, los certificados, las imágenes y otros. Para ello, ADM requiere montajes NFS. La aplicación requiere dos carpetas de los montajes de red compartidos:

- Uno para almacenar archivos como certificados, imágenes y otros
- El otro para la base de datos

> Nota
>
> Se recomienda tener un NFS con una SSD.

Estas dos carpetas pueden ser diferentes o iguales. Ambas carpetas deben tener 777 permisos. La primera carpeta debe tener un espacio mínimo de 10 GB. El tamaño de la segunda carpeta depende de la cantidad de datos que deben ser persistentes en la base de datos. El tamaño mínimo es de 100 GB.
Para el entorno de producción, recomendamos tener una solución NFS de grado de producción.

### Dispositivo Citrix ADC

Se requiere el dispositivo Citrix ADC como dispositivo de entrada. ADC hace que los servicios de aplicaciones requeridos estén disponibles fuera del
clúster de Kubernetes. El dispositivo Citrix ADC debe estar fuera del clúster de Kubernetes y los nodos de trabajo deben ser accesibles desde el ADC. Siga estos pasos:

- Configure un SNIP en el ADC. ADC usa este SNIP para llegar a los nodos de trabajo del clúster de Kubernetes.
- Identifique una dirección IP gratuita que se utilizará como dirección IP del servidor virtual para que los servicios de aplicaciones requeridos estén disponibles fuera del clúster de Kubernetes.

#### Instalar ADM en el clúster de Kubernetes

Siga estos pasos para instalar un dispositivo ADM en un clúster de Kubernetes:

1. Vaya al sitio de descargas de Citrix y descargue el archivo de Citrix ADM Helm Chart for Kubernetes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Extraiga el tarball descargado del gráfico de Helm en el directorio /var del nodo principal del clúster de Kubernetes.
3. Abra el`values.yaml` archivo bajo el`/var/citrixadm` directorio.
4. Introduzca una contraseña para la base de datos en el campo `dbpasswd` del archivo.
5. Cambie los valores siguientes. La aplicación ADM utiliza estos valores para configurar el dispositivo Citrix ADC de modo que los servicios estén expuestos al mundo externo:
   - `ingressIP`: una IP virtual configurada en Citrix ADC para acceder a la aplicación.
   - `applicationID`: un identificador único para distinguir la configuración de ingreso del resto de la configuración en el dispositivo Citrix ADC.
   - `ingressADCIP`: la dirección IP Citrix ADC (NSIP), que se utiliza como ingreso para la aplicación ADM.
   - `ingressADCUsername`: un nombre de usuario para acceder al dispositivo Citrix ADC. Este usuario debe tener privilegios de escritura.
   - `ingressADCPassword`: Contraseña para el nombre de usuario.

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. Cambie los siguientes valores en la sección de **almacenamiento**. Estos valores especifican la persistencia requerida para almacenar los archivos requeridos por la aplicación ADM.
   - `nfsServer`: nombre de host o dirección IP del servidor NFS
   - `path`: monta la ruta de la carpeta para almacenar los archivos de la aplicación.
   - `size`: al menos 10 GB.

   > Nota
   >
   > La unidad de este valor es Gi. Por ejemplo, 10Gi, 20Gi.

7. Vaya a la sección **de almacenamiento** en`pg-datastore` y cambie los siguientes valores. Estos valores especifican la persistencia utilizada para crear una base de datos.
   - `nsfServer`: nombre de host o dirección IP del servidor NFS.
   - `size`: monte una ruta para la carpeta utilizada para el almacén de datos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- `path`: al menos 100 GB.

> Nota
>
> La unidad de este valor es Gi. Por ejemplo, 100Gi, 200Gi.

8. Vaya al directorio /var/citrix en el nodo principal y ejecute el siguiente comando para instalar una aplicación ADM:
   ```
   helm install -n citrixadm --namespace <name> ./citrixadm
   ```
   > Nota
   >
   > Este comando helm no se admite en la versión 3.x de helm.

   Este comando también instala los pods necesarios en el clúster. El argumento de espacio de nombres es opcional. Si no se proporciona un espacio de nombres, Helm instala ADM en el espacio de nombres predeterminado. Para facilitar la administración, instale ADM en un espacio de nombres independiente.

9. Abra su explorador y escriba `http://< virtual server IP address >` e inicie sesión en el ADM utilizando `nsroot/nsroot` como credenciales. Para un acceso seguro escriba `https://< virtual server IP address >`.

> Nota
>
> Durante la implementación, la aplicación ADM crea tablas en el almacén de datos, lo que puede tardar un poco. Dependiendo de los recursos asignados por Kubernetes a varios pods de la aplicación ADM, el servicio puede tardar entre 5 y 15 minutos en aparecer.

## NetScaler ADM en el servidor KVM Linux

January 30, 2024

Las plataformas de virtualización en las que se puede aprovisionar NetScaler Application Delivery Management (ADM) incluyen Linux-KVM.

Antes de instalar NetScaler ADM en Linux-KVM, asegúrese de que el sistema tiene las extensiones de virtualización de hardware y compruebe que las extensiones de virtualización de CPU están disponibles. Compruebe que `virsh` (una herramienta de línea de comandos para administrar máquinas virtuales) esté disponible en el hipervisor.

Utilice sus credenciales de administrador para iniciar sesión en el sitio web de Citrix.com, acceder a los archivos de configuración de NetScaler ADM más recientes y descargarlos en su equipo. A continuación, instale Citrix ADM en la plataforma Linux-KVM y configúrelo para la red.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Requisitos previos

Antes de instalar el dispositivo virtual Citrix ADM, compruebe que la versión 3.6.11-4 y posteriores de Linux-KVM esté instalada en un hardware que cumpla con los requisitos mínimos.

### Requisitos de hardware

| Componente | Requisito |
| --- | --- |
| CPU | Un procesador x86 de 64 bits con las funciones de virtualización de hardware incluidas en el procesador Intel VT-X. Proporcione al menos 2 núcleos de CPU para alojar Linux-KVM. **Nota** Para comprobar si la CPU es compatible con el host Linux, introduzca el siguiente comando en el símbolo del shell de host Linux: `*. egrep'^flags.\* ( vmx \| svm )' /proc/cpuinfo*` Si la configuración del BIOS para la extensión está inhabilitada, debe habilitarlos en el BIOS. No hay ninguna recomendación específica para la velocidad del procesador, pero mayor es la velocidad, mejor será el rendimiento del NetScaler ADM. |
| Memoria (RAM) | Mínimo 4 GB para el kernel Linux host. Agregue memoria adicional según lo requieran las máquinas virtuales. |
| Disco duro | Calcule el espacio para los requisitos del núcleo y la máquina virtual de Host Linux. Una sola máquina virtual Citrix ADM requiere 120 GB de espacio en disco. |

> **Nota**
>
> Los requisitos de memoria y disco duro especificados son para implementar Citrix ADM en la plataforma OpenStack, teniendo en cuenta que no hay otras máquinas virtuales ejecutándose en el host. Los requisitos de hardware para OpenStack dependen del número de máquinas virtuales que se ejecutan en él.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Requisitos de software**

Citrix recomienda núcleos más nuevos, como la versión de 64 bits del núcleo 3.6.11-4 o posterior.

**Requisitos de la red** Citrix ADM solo admite una interfaz de red paravirtualizada de VirtIO. Asegúrese de conectar esta interfaz a la red de administración del host Linux-KVM para que NetScaler ADM y Linux-KVM puedan comunicarse.

## Descargar archivos de configuración de NetScaler ADM

Para descargar los archivos de configuración de NetScaler ADM desde www.citrix.com:

1. Abra un explorador web y escriba www.citrix.com en la barra de direcciones.
2. Pase el cursor sobre la opción **Iniciar sesión y haga clic enMy Account**, escriba sus credenciales de Citrix y, a continuación, vuelva a hacer clic**en Iniciar sesión**.
3. Vaya a la sección **Descargas**.
4. En la lista de **descargas** , seleccione **Citrix Application Delivery Management** .
5. En la página **NetScaler Application Delivery Management**, seleccione la versión. Por ejemplo, seleccione la **versión 13.0**.
6. Haga clic en **Software de producto** para expandirlo y haga clic en la versión más reciente. Por ejemplo, seleccione **NetScaler MAS Release (Feature Phase) 13.0**Build 36.27.

   Se muestra la página de creación seleccionada.
7. En la lista **Jump to Download**, seleccione **NetScaler MAS image for KVM, 13.0 Build xx.xx**
8. Haga clic en **Descargar archivo**, acepte el CLUF y descargue el archivo de imagen comprimido en cualquier carpeta del equipo local.

## Instalación de NetScaler Application Delivery Management en Linux-KVM

1. Con SSH, inicie sesión en el host KVM.
2. En la línea de comandos de la CLI, copie la imagen en una carpeta del servidor mediante cualquiera de los programas de transferencia de archivos.
3. Navegue hasta el directorio donde ha guardado la imagen descargada.
4. Realice lo siguiente en la línea de comandos:

   a) Haga una lista de los archivos del directorio y verifique la presencia del archivo de imagen.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Utilice el comando tar para descomprimir el archivo de imagen de Citrix Application Delivery Management. El paquete descomprimido contiene los siguientes componentes:

i. Un archivo XML de dominio que especifica los atributos de Citrix ADM

ii. Archivo de texto que especifica la suma de comprobaciones de la imagen de disco del dominio

iii. Una imagen de disco de dominio

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
```

```
root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build#
```

iv. Cree una copia de MAS-KVM.xml como MAS1-KVM.xml, como opción de copia de seguridad. Abra el archivo MAS1-KVM.xml mediante el editor vi.

v. Modifique MAS1-KVM.xml para los siguientes atributos de red:

A. `name` - Especifique el nombre.

B. `mac` - Especifique la dirección MAC.

C. `source file`: Especifique la ruta de origen de la imagen de disco absoluta. La ruta del archivo tiene que ser absoluta.

> **Nota**
>
> El nombre de dominio y la dirección MAC deben ser únicos.

D. `mode` - Especifique el modo.

E. `model type` - Establece Virtio.

F. `source dev` - Especifique la interfaz.

```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
```

vi. Defina los atributos de VM en el archivo MAS1-KVM.xml mediante el siguiente comando: `virsh define \<FileName\>.xml`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
```

```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

vii. Inicie NetScaler ADM escribiendo el siguiente comando: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS
Domain MAS started
```

```
root@ubuntu:/home/mas-build# virsh start MAS
Domain MAS started

root@ubuntu:/home/mas-build#
```

viii. Puede conectarse a la máquina virtual NetScaler ADM mediante el siguiente comando: `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
```

```
root@ubuntu:/home/mas-build# virsh console MAS
Connected to domain MAS
Escape character is ^]
```

## Configurar NetScaler Application Delivery Management

> **Nota**
>
> En algunos servidores KVM de Linux, los huéspedes de FreeBSD no se reinician correctamente si tienen más de una CPU. Cuando se reinicia el dispositivo virtual Citrix ADM, la CLI y la GUI de Citrix ADM dejan de responder. Para obtener más información, consulte https://bugs.launchpad.net/qemu/+bug/1329956
>
> Para evitar que la CLI y la GUI de NetScaler ADM no respondan cuando se reinicia el dispositivo virtual NetScaler ADM, apague todas las máquinas virtuales del host KVM y realice lo siguiente en el host KVM:
>
> 1. Retire el módulo kvm_intel con el siguiente comando:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
rmmod kvm\\_intel
```

2. Desactive **APICv** y vuelva a cargar el módulo kvm_intel con el siguiente comando:
   `modprobe kvm\\_intel enable\\_apicv=N`
3. Inicie las máquinas virtuales en el host KVM.

Después de instalar NetScaler ADM, espere unos 10 minutos para que los servicios estén disponibles y, a continuación, inicie sesión en NetScaler ADM.

1. En la línea de comandos, utilice las credenciales de administrador del sistema predeterminadas para iniciar sesión en el sistema:
   - Nombre de usuario: `nsroot`
   - Contraseña: `nsroot`

   > **Nota**
   >
   > Después de iniciar sesión por primera vez, cambie la contraseña administrativa. A continuación, configure el MAS para que funcione en su red. Puede cambiar la contraseña desde la interfaz de usuario de NetScaler ADM. En la página principal de Citrix ADM, vaya a **Sistema** > **Administración** de usuarios > **Usuarios** . Seleccione el usuario y haga clic en **Modificar** y, a continuación, actualice la contraseña en el campo Contraseña.

2. Cuando se le solicite, escriba: *shell*
3. Escriba **networkconfig** para acceder al menú de configuración de red inicial de Citrix ADM. Configure la dirección IP de administración.
4. Para completar la configuración de red inicial de Citrix ADM, siga las instrucciones. La consola muestra las opciones de configuración de red iniciales de Citrix ADM para establecer los siguientes parámetros para Citrix ADM. El nombre del host se rellena de forma predeterminada.
   a) Introduzca **2** para actualizar la dirección IPv4 de Citrix ADM: la dirección IP de administración en la que accede a un Citrix ADM
   b) Introduzca **3** para actualizar Máscara de red: Máscara de subred asociada a la dirección IP de administración.
   c) Introduzca **4** para actualizar la dirección IPv4 de la puerta de enlace: la dirección IP de la puerta de enlace predeterminada para la subred de la dirección IP de administración de Citrix ADM
   d) Escriba **7** para guardar y salir: Guarda los cambios de configuración y sale del sistema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
--------------------------------------------------------------------------
      1. Citrix ADM Host Name [ADMHA1]:
      2. Citrix ADM IPv4 address [10.102.29.52]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

5. Ejecute el script de implementación escribiendo el comando en el símbolo del shell: `deployment_type.py`
6. En la pantalla de implementación que aparece, seleccione el tipo de implementación como **servidor NetScaler ADM**.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

7. Escriba **Sí** para implementar NetScaler ADM como implementación independiente.
8. Escriba **Sí** para reiniciar el servidor Citrix ADM.
9. Una vez reiniciado el servidor Citrix ADM, inicie sesión en Citrix ADM con las credenciales de administrador predeterminadas, nsroot/nsroot, a través de la línea de comandos o la GUI.

   Más adelante, puede acceder al Citrix ADM escribiendo la dirección IP del servidor Citrix ADM en la barra de direcciones del explorador. Las credenciales de administrador predeterminadas para iniciar sesión en el servidor son *nsroot/nsroot* .

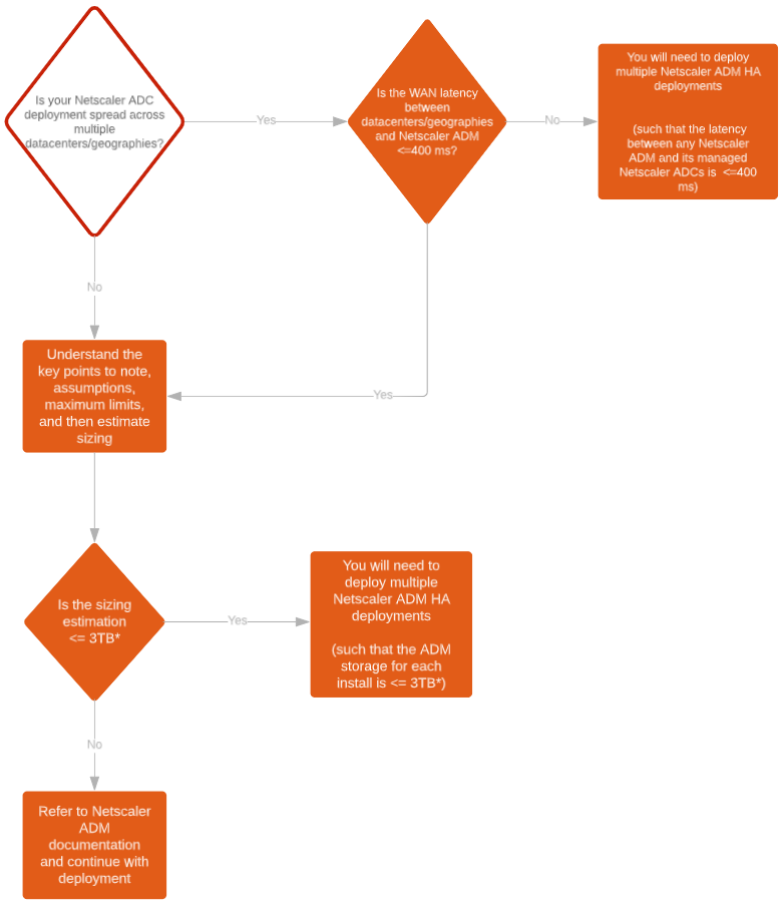
## Configurar la implementación de alta disponibilidad

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La alta disponibilidad (HA) se refiere a un sistema que siempre está disponible para el usuario sin interrumpir los servicios. La configuración de alta disponibilidad es crucial durante el tiempo de inactividad del sistema, los errores de la red o las aplicaciones, y es un requisito clave para cualquier empresa. Una implementación de alta disponibilidad de dos nodos Citrix ADM en modo activo-pasivo con las mismas configuraciones proporciona operaciones ininterrumpidas.

## Caso de implementación




> **Nota**
>
> El límite máximo de almacenamiento validado para una implementación única de Citrix ADM HA es de 3 TB. Para obtener más información, consulte la guía de implementación.
>
> **Importante**
>
> **Para acceder a Citrix ADM 12.1, compilación 48.18 o versiones posteriores, mediante HTTPS:**
>
> Si ha configurado una instancia de Citrix ADC para equilibrar la carga de Citrix ADM en modo de alta disponibilidad, primero elimine la instancia de Citrix ADC. A continuación, configure una

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> dirección IP flotante para acceder a Citrix ADM en modo de alta disponibilidad.

Las siguientes son las ventajas de la implementación de alta disponibilidad en Citrix ADM:

- Un mecanismo mejorado para monitorizar los latidos del corazón entre el nódulo primario y el secundario.
- Proporciona una replicación en streaming física de la base de datos en lugar de una replicación bidireccional lógica.
- Capacidad de configurar la dirección IP flotante en el nodo principal para eliminar la necesidad de un balanceador de cargas Citrix ADC independiente.
- Proporciona un acceso sencillo a la interfaz de usuario de Citrix ADM mediante la dirección IP flotante.
- La interfaz de usuario Citrix ADM solo se proporciona en el nodo principal. Mediante el nodo principal, puede eliminar el riesgo de acceder al nodo secundario y realizar cambios en él.
- La configuración de la dirección IP flotante permite gestionar la situación de conmutación por error y no es necesario volver a configurar las instancias.
- Proporciona la capacidad incorporada para detectar y manejar situaciones de cerebro dividido.

En la siguiente tabla se describen los términos utilizados en la implementación de alta disponibilidad.

| Términos y condiciones | Descripción |
|---|---|
| Nodo principal | Primer nodo registrado en la implementación de alta disponibilidad. |
| Nodo secundario | Segundo nodo registrado en la implementación de alta disponibilidad. |
| Latido | Mecanismo utilizado para intercambiar mensajes entre el nodo principal y el secundario en la configuración de alta disponibilidad. Los mensajes determinan el estado y el estado de la aplicación en cada nodo individual. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

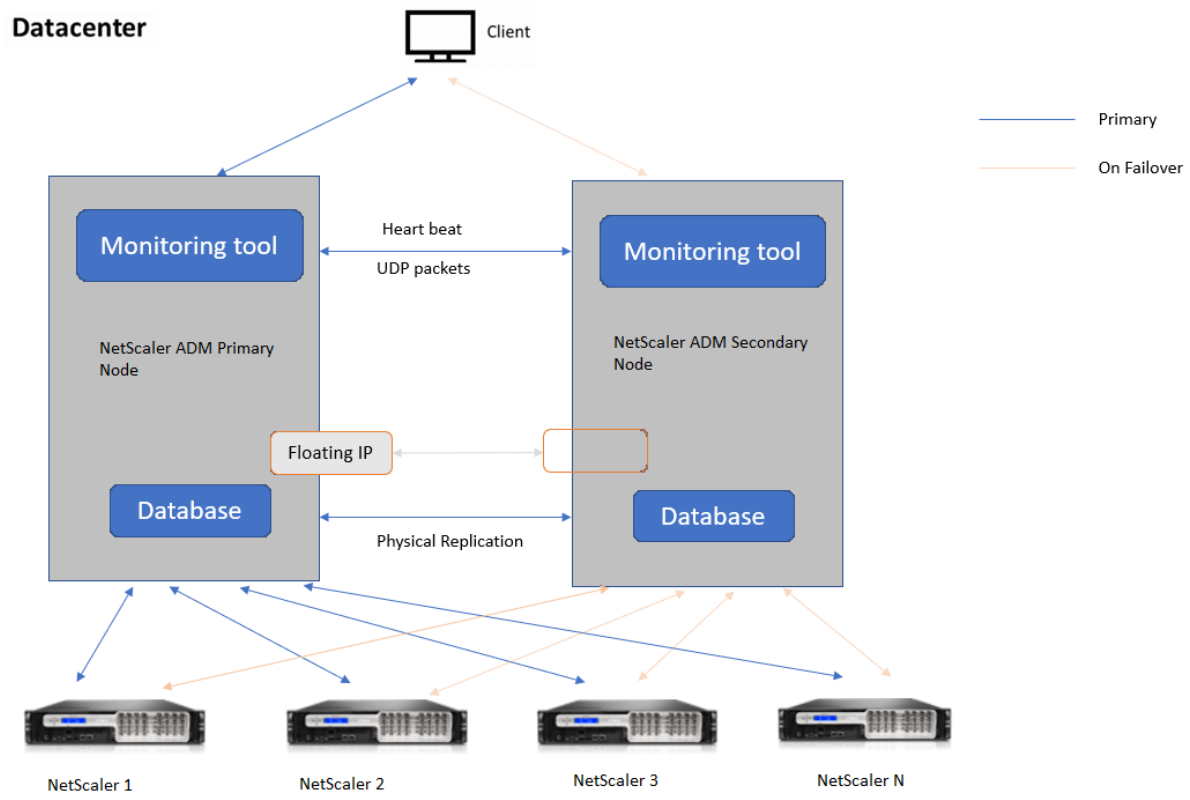
| Términos y condiciones | Descripción |
| --- | --- |
| Dirección IP flotante | Una IP flotante es una dirección IP que se puede mover instantáneamente de un nodo a otro de la misma subred. Internamente, se configura como un alias en la interfaz de red del nodo principal. Si se produce una conmutación por error, la dirección IP flotante se mueve sin problemas de la antigua principal a la nueva. Es útil en la configuración de alta disponibilidad porque permite a los clientes comunicarse con los nodos de alta disponibilidad mediante una sola dirección IP. |

> **Nota**
>
> Para obtener más información sobre los detalles de puertos y protocolos, consulte Puertos.

### Componentes de la arquitectura de alta disponibilidad

En la siguiente ilustración se muestra la arquitectura de dos nodos Citrix ADM implementados en modo de alta disponibilidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En la implementación de alta disponibilidad, un nodo Citrix ADM se configura como nodo principal (MAS 1) y el otro como nodo secundario (MAS 2). Si el nodo principal cae por algún motivo, el nodo secundario se hace cargo como el nuevo nodo principal.

## Herramienta de monitorización

La herramienta de supervisión es un proceso interno que se utiliza para supervisar, alertar y gestionar situaciones de conmutación por error. La herramienta está activa y se ejecuta en cada nodo en alta disponibilidad. Es responsable de iniciar los subsistemas, iniciar la base de datos en ambos nodos, decidir cuál es el nodo principal o el secundario en caso de que se produzca una conmutación por error, etc.

## Nodo principal

El nodo principal acepta las conexiones y administra las instancias. El nodo principal administra todos los procesos, como AppFlow, SNMP, LogStream, syslog, etc. El acceso a la interfaz de usuario de Citrix ADM está disponible en el nodo principal. La dirección IP flotante se configura en el nodo principal.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Nodo secundario

El nodo secundario escucha los mensajes de latidos del corazón enviados desde el nodo principal. La base de datos del nodo secundario solo está en modo de lectura-réplica. Ninguno de los procesos está activo en el nodo secundario y no se puede acceder a la interfaz de usuario de Citrix ADM en el nodo secundario.

### Replicación de transmisión física

Los nodos primario y secundario se sincronizan mediante el mecanismo de los latidos del corazón. Con la replicación física en streaming de la base de datos, el nodo secundario se inicia en modo de lectura-réplica. El nodo secundario escucha los mensajes de latidos del corazón recibidos del nodo principal. Si el nodo secundario no recibe ningún latido cardíaco durante un período de tiempo de 180 segundos, se considera que el nodo principal está inactivo. A continuación, el nodo secundario pasa a ser el nodo principal.

### Mensajes de latidos

Los mensajes Heartbeat son paquetes de datagramas de usuario (UDP) que se envían y reciben entre el nodo principal y el secundario. Supervisa todos los subsistemas de Citrix ADM y la base de datos para intercambiar información sobre el estado, el estado, los procesos, etc. del nodo. La información se comparte entre los nodos de alta disponibilidad cada segundo. Las notificaciones se envían como alertas al administrador si se produce una conmutación por error o una interrupción de los estados de alta disponibilidad.

### Dirección IP flotante

La dirección IP flotante está asociada al nodo principal en la configuración de alta disponibilidad. Es un alias asignado a la dirección IP del nodo principal que el cliente puede utilizar para conectarse a Citrix ADM en el nodo principal. Como la dirección IP flotante está configurada en el nodo principal, no es necesaria la reconfiguración de la instancia en caso de conmutación por error. Las instancias se vuelven a conectar a la misma dirección IP para llegar a la nueva primaria.

### Puntos clave a tener en cuenta

- En una configuración de alta disponibilidad, los dos nodos Citrix ADM se implementan en modo activo-pasivo. Deben estar en las mismas subredes con la misma versión y compilación de software, y tener las mismas configuraciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Dirección IP flotante:
  - La dirección IP flotante se configura en el nodo principal.
  - No es necesario volver a configurar las instancias si se produce una conmutación por error.
  - Puede acceder a un nodo de alta disponibilidad desde la interfaz de usuario, ya sea mediante la IP del nodo principal o la dirección IP flotante.

    > **Nota**
    >
    > Citrix recomienda utilizar la dirección IP flotante para acceder a la interfaz de usuario.

- Base de datos:
  - En una configuración de alta disponibilidad, todos los archivos de configuración se sincronizan automáticamente del nodo principal al nodo secundario en un intervalo de un minuto.
  - La sincronización de bases de datos se realiza al instante mediante la replicación física de la base de datos.
  - La base de datos del nodo secundario está en modo de lectura-réplica.

- Actualización de Citrix ADM:
  - Los procesos internos actualizan implícitamente Citrix ADM desde las versiones anteriores.

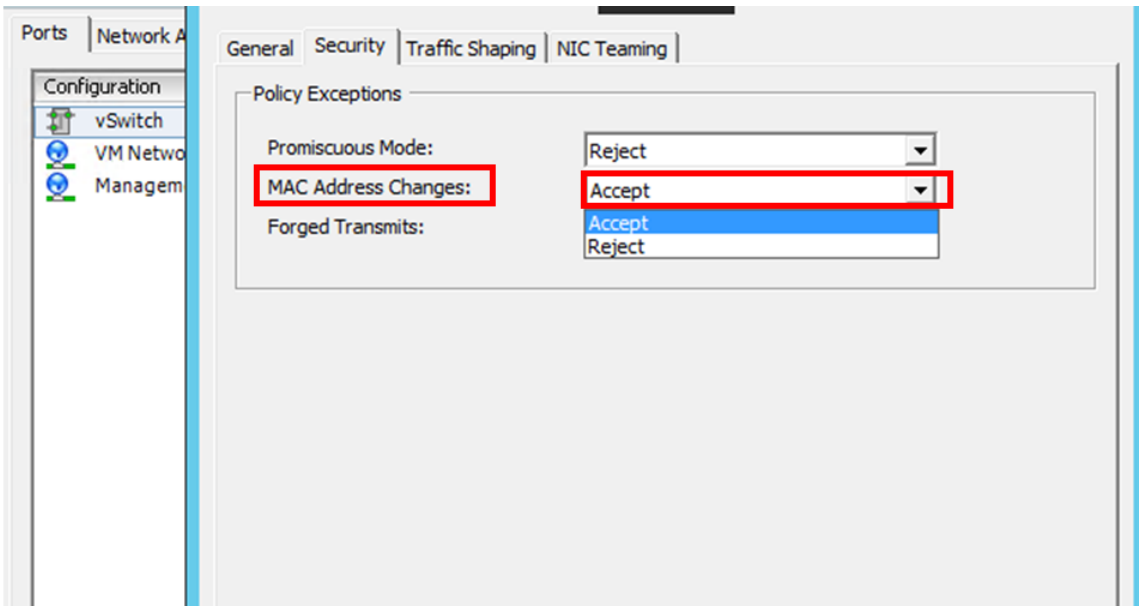
    > **Nota**
    >
    > Una vez que la actualización se haya realizado correctamente, debe configurar la dirección IP flotante.

- El puerto UDP predeterminado 5005 está disponible tanto en los nodos para enviar latidos como para recibir mensajes.

- Dirección MAC
  La configuración de la opción “Cambios de dirección MAC”de un hipervisor afecta al tráfico que recibe una máquina virtual. Permitir que los cambios de dirección MAC se habiliten en el conmutador virtual para que la dirección IP flotante se mueva sin problemas al nuevo nodo principal después de la conmutación por error.
  Por ejemplo, al implementar Citrix ADM con alta disponibilidad en VMware ESXi, asegúrese de aceptar los cambios en la dirección MAC. ESXi ahora permite que las solicitudes cambien la dirección MAC activa a otra que la dirección MAC inicial.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Para Citrix ADM implementado en la versión 6.7 de ESXI, también puede configurar la opción de **cambios de dirección MAC** en **Rechazar**. Tras la conmutación por error, el tráfico fluye al nuevo nodo principal sin problemas, independientemente de la configuración de **cambios de dirección MAC**. Por lo tanto, aceptar los cambios en la dirección MAC no es obligatorio.
>
> Si Citrix ADM está implementado en una versión de ESXI inferior a 6.7, asegúrese de que la opción **Cambios de dirección MAC** esté configurada en solo **Aceptar**.




## Requisitos previos

Antes de configurar la alta disponibilidad para los nodos Citrix ADM, tenga en cuenta los siguientes requisitos previos:

- La implementación de alta disponibilidad de Citrix ADM es compatible con la versión 12.0, compilación 51.24 de Citrix ADM.
- Descargue el archivo de imagen de Citrix Application Delivery Management (.xva) del sitio de descargas de Citrix: https://www.citrix.com/downloads/

Citrix recomienda establecer la prioridad de la CPU (en las propiedades de la máquina virtual) en el nivel más alto para mejorar el comportamiento de la programación y la latencia de la red.

En la siguiente tabla se enumeran los requisitos mínimos para los recursos informáticos virtuales:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Componente | Requisito |
| --- | --- |
| RAM | **32 GB** |
| CPU virtual | **8 CPUs** |
| Espacio de almacenamiento | Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Si sus requisitos de almacenamiento de Citrix ADM superan los 120 GB, debe conectar un disco adicional. **Nota** Solo puede agregar un disco adicional. Citrix recomienda estimar el almacenamiento y adjuntar disco adicional en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |
| **Hypervisor** | **Versiones** |
| Citrix Hypervisor | 6.2 y 6.5 |
| VMware ESXi | 5.5 y 6.0 |
| Microsoft Hyper-V | 2012 R2 |
| Linux KVM | Ubuntu y Fedora |

### Para configurar Citrix ADM en modo de alta disponibilidad

1. Registre e implemente el primer servidor (nodo principal).
2. Registre e implemente el segundo servidor (nodo secundario).
3. Implementar el nodo principal y secundario para la configuración de alta disponibilidad.

### Registrar e implementar el primer servidor (nodo principal)

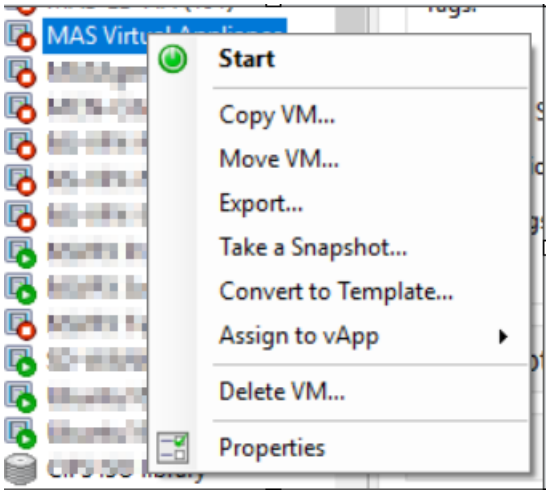
Para registrar el primer nodo:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

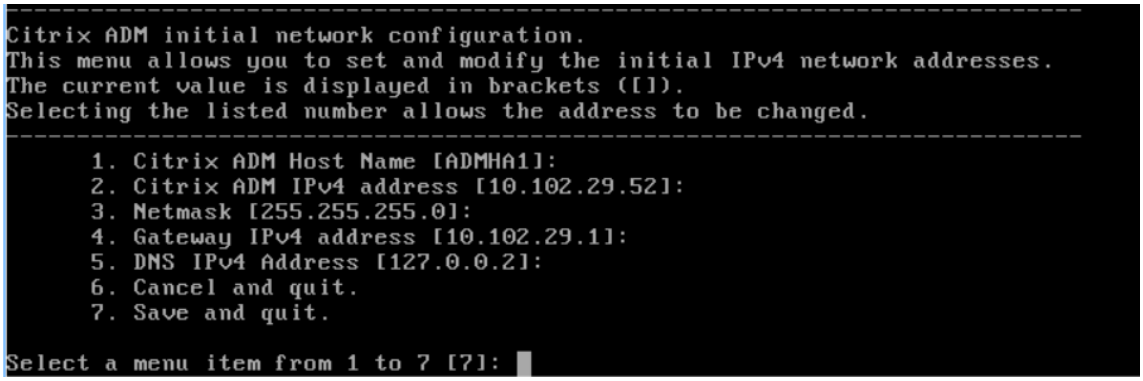
1. Utilice el archivo de imagen.xva descargado del sitio de descargas de Citrix e impórtelo al hipervisor.

   > **Nota:**
   >
   > Es posible que el archivo de imagen.xva tarde unos minutos en importarse y comenzar. Puede ver el estado en la parte inferior de la pantalla.
   >
   > 
   > 

2. Una vez que la importación se haya realizado correctamente, haga clic con el botón derecho y haga clic en **Inicio**.

3. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.

4. Una vez completada la configuración de red inicial, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot*.

   > **Nota**
   >
   > Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Para implementar el nodo principal, escriba **/mps/deployment_type.py**. Aparece el menú de configuración de implementación de Citrix ADM.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

6. Seleccione **1** para registrar el servidor Citrix ADM como nodo principal.

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

7. La consola le pide que seleccione la implementación independiente de Citrix ADM. Introduzca**No** para confirmar la implementación como alta disponibilidad.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. La consola le pide que seleccione el primer nodo del servidor. Escriba**Sí** para confirmar el nodo como el primer nodo.

```
-------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
```

9. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.

```
-------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
[yes/no]:yes
```

El sistema se reinicia y se muestra como nodo principal en la interfaz de usuario de Citrix ADM.

## Registrar e implementar el segundo servidor (nodo secundario)

1. Utilice el archivo de **imagen.xva** descargado del sitio de descargas de Citrix e impórtelo al hipervisor.
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales, como se muestra en la siguiente imagen.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Una vez completada la configuración inicial de la red, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: *nsrecover/nsroot*.

   > **Nota**
   >
   > Después de iniciar sesión, si quiere actualizar la configuración de red inicial, escriba `networkconfig`, actualice la configuración y guarde la configuración.

4. Para implementar el nodo secundario, escriba **/mps/deployment_type.py**. Aparece el menú de configuración de implementación de Citrix ADM.
5. Seleccione **1** para registrar el servidor Citrix ADM como nodo secundario.
6. La consola le pide que seleccione Citrix ADM como implementación independiente. Introduzca**No** para confirmar la implementación como alta disponibilidad.
7. La consola le pide que seleccione el primer nodo del servidor. Escriba**No** para confirmar el nodo como segundo servidor.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

8. La consola le pide que introduzca la dirección IP y la contraseña del nodo principal.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
-----------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

-----------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

9. La consola le pide que introduzca la dirección IP flotante.

```
-----------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

-----------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
    Enter Floating IP address:10.102.29.97
```

10. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.

> **Nota**
>
> - La dirección IP flotante es obligatoria para la implementación de nodos de alta disponibilidad.
> - El sistema mostrará mensajes de error si hay algún problema en la configuración.
> - El sistema se reinicia y las configuraciones tardan unos minutos en surtir efecto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Implemente el nodo principal y el secundario como un par de alta disponibilidad

Tras el registro, los nodos principales y secundarios se muestran en la interfaz de usuario de Citrix ADM. Implemente estos nodos en un par de alta disponibilidad.

> **Nota**
>
> - Antes de implementar los nodos en un par de alta disponibilidad, asegúrese de que el nodo secundario se haya completado con un reinicio, después de la configuración inicial de la red.
> - Una vez finalizada la implementación de alta disponibilidad, utilice la dirección IP flotante para acceder a la interfaz de usuario de Citrix ADM.

**Para implementar nodos como un par de alta disponibilidad:**

1. Abra un explorador web e introduzca la dirección IP del primer nodo del servidor Citrix ADM.
2. En los campos**Nombre de usuario**y**contraseña**, introduzca las credenciales de administrador.
3. Haga clic en **Comenzar** en la página de inicio.
4. Seleccione el tipo de implementación como**Dos servidores implementados en modo de alta disponibilidad**y haga clic en**Siguiente**.
5. En la página Implementación, haga clic en**Implementar**.
6. Aparece un mensaje de confirmación. Haga clic en **Sí**.

   Citrix ADM se reinicia y tarda aproximadamente 10 minutos en que la configuración surta efecto.

   > **Nota**
   >
   > Ahora puede comenzar a usar la dirección IP flotante.

7. Inicie sesión en Citrix ADM con credenciales de administrador, haga clic en **Comenzar** en la página de inicio y, si lo quiere, complete lo siguiente:

   a) Agregar instancias de Citrix ADC

   b) Configurar la identidad del cliente

   > **Nota**
   >
   > También puede hacer clic en **Omitir** para completarlo más tarde y hacer clic en **Finalizar**.

8. Navegue hasta **Sistema** > **Implementación** para validar la implementación.

   Para obtener más información, consulte las Preguntas frecuentes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Inhabilitar alta disponibilidad

Puede inhabilitar la alta disponibilidad en un par de alta disponibilidad de Citrix ADM y convertir los nodos en servidores Citrix ADM independientes.

> **Nota**
>
> Desactive la alta disponibilidad desde el nodo principal.

**Para inhabilitar la alta disponibilidad:**

1. En un explorador web, introduzca la dirección IP del nodo principal del servidor Citrix ADM.
2. En los campos **Nombre de usuario**y**Contraseña**, introduzca las credenciales del administrador.
3. En la ficha**Sistema**, vaya a**Deployment** y haga clic en**Break HA**.

   Se muestra un cuadro de diálogo. Haga clic en **Sí** para interrumpir la implementación de alta disponibilidad.

## Reimplemente la alta disponibilidad

Después de inhabilitar la alta disponibilidad en una implementación independiente, puede volver a implementarla en el modo de alta disponibilidad. Redistribuir alta disponibilidad es similar a la primera implementación de alta disponibilidad. Para obtener más información, consulte Implementar el nodo principal y el secundario como un par de alta disponibilidad.

## Casos de conmutación por error de alta disponibilidad

Se produce una conmutación por error si se da una de las siguientes condiciones:

- **Fallo de nodo**: el nodo principal deja de funcionar y no se detecta ningún latido del nodo principal durante 180 segundos.
- **Error de mantenimiento de la aplicación**: El nodo principal está activo y en ejecución, pero uno de los procesos Citrix ADM está inactivo.

## Caso de cerebro dividido

Cuando no hay comunicación entre ambos nodos debido a un tiempo de inactividad en el enlace de red, entonces:

- El nodo principal sigue funcionando como principal

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El nódulo secundario pasa a ser el primario debido a la incapacidad de recibir los latidos del corazón
- Ambos nodos ejecutarían sus instancias de bases de datos individuales

Por ejemplo, en una empresa se han implementado dos nodos Citrix ADM como principales y secundarios. Debido a un posible tiempo de inactividad del enlace de red, la comunicación entre los dos nodos de Citrix ADM se interrumpe por completo. Como no hay intercambio de latidos durante más de 180 segundos, ambos nodos se consideran el nodo principal. Ambos nodos actúan como nodos activos y ejecutan sus propias instancias de base de datos.

A partir de Citrix ADM 12.1 o una versión posterior, esta situación de cerebro dividido se gestiona sin problemas una vez restaurados el enlace de red y el latido del corazón. La sincronización de alta disponibilidad se restaura automáticamente. El tiempo de recuperación depende de los datos y de la velocidad del enlace entre los nodos.

> **Nota**
>
> Durante la afección de cerebro dividido, los cambios que se produjeron en el nodo principal antiguo se restablecen con el nuevo primario cuando se vuelve a unir a él en alta disponibilidad. Los cambios que ocurrieron en el nuevo nodo primario durante el split-brain permanecen intactos.

## Configurar la recuperación ante desastres para alta disponibilidad

January 30, 2024

El desastre es una interrupción repentina de las funciones empresariales causada por desastres naturales o eventos causados por seres humanos. Los desastres afectan a las operaciones del centro de datos, después de lo cual los recursos y los datos perdidos en el sitio del desastre deben reconstruirse y restaurarse por completo. La pérdida de datos o el tiempo de inactividad en el centro de datos es fundamental y colapsa la continuidad del negocio.

La función de recuperación ante desastres (DR) de Citrix ADM proporciona funciones completas de copia de seguridad y recuperación del sistema para Citrix ADM implementado en modo de alta disponibilidad. En el momento de la recuperación, los certificados, los archivos de configuración y una copia de seguridad completa de la base de datos están disponibles en el sitio de recuperación.

En la tabla siguiente se describen los términos que se utilizan al configurar la recuperación ante desastres en Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

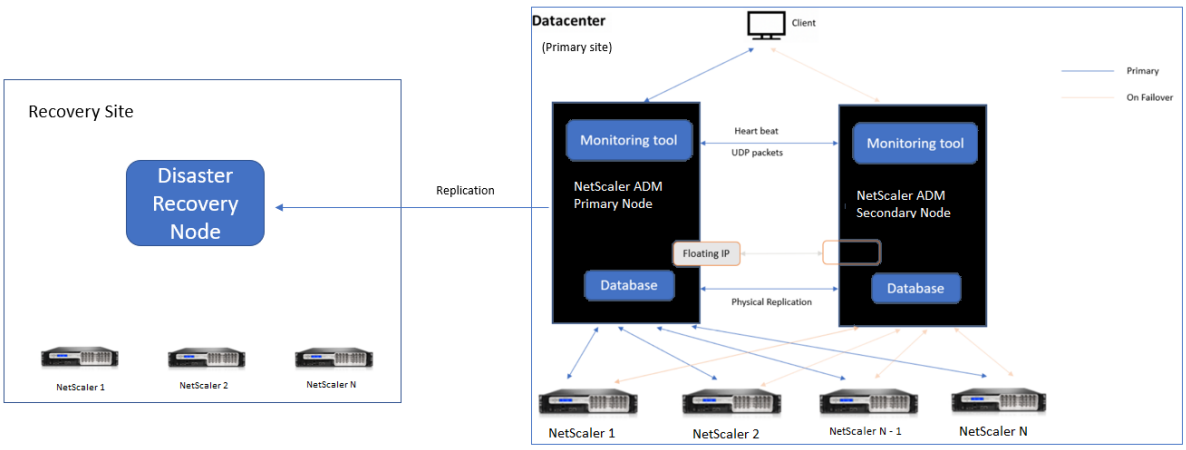
| Términos y condiciones | Descripción |
|---|---|
| Sitio principal (centro de datos A) | El sitio principal tiene nodos Citrix ADM implementados en modo de alta disponibilidad. |
| Sitio de recuperación (centro de datos B) | El sitio de recuperación tiene un nodo de recuperación ante desastres implementado en modo independiente. Este nodo está en modo de solo lectura y no estará operativo hasta que el sitio principal esté inactivo. |
| Nodo de recuperación ante desastres | El nodo de recuperación es un nodo independiente implementado en el sitio de recuperación. Este nodo se hace operativo (al nuevo primario) en caso de que se produzca un desastre en el sitio primario y no funcione. |

> Nota: El sitio principal y el sitio DR se comunican entre sí a través de los puertos 5454 y 22, y estos puertos están habilitados de forma predeterminada.
> Para obtener más información sobre los detalles de puertos y protocolos, consulte Puertos.

## Flujo de trabajo de recuperación ante desastres

La siguiente imagen muestra el flujo de trabajo de recuperación ante desastres, la configuración inicial antes del desastre y el flujo de trabajo posterior al desastre.

### Configuración inicial antes del desastre




La imagen muestra la configuración de recuperación ante desastres antes del desastre.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El sitio principal tiene nodos Citrix ADM implementados en el modo de alta disponibilidad. Para obtener más información, consulte Implementación de alta disponibilidad

El sitio de recuperación tiene un nodo de recuperación ante desastres de Citrix ADM independiente implementado de forma remota. El nodo de recuperación ante desastres está en modo de solo lectura y recibe datos del nodo principal para crear copias de seguridad de datos. También se detectan instancias de Citrix ADC en el sitio de recuperación, pero no hay tráfico que fluya a través de ellas. Durante el proceso de copia de seguridad, todos los datos, archivos y configuraciones se replican en el nodo de recuperación ante desastres desde el nodo principal.

### Requisitos previos

Antes de configurar el nodo de recuperación ante desastres, tenga en cuenta los siguientes requisitos previos:

- Para habilitar la configuración de recuperación ante desastres, el sitio principal debe tener los nodos Citrix ADM configurados en modo de alta disponibilidad.
- La implementación independiente de Citrix ADM en el sitio principal no admite la función de recuperación ante desastres.
- El par Citrix ADM HA (en el sitio principal) y el nodo independiente (en el sitio de recuperación ante desastres) deben tener la misma versión de software, compilación y configuraciones.

Citrix recomienda establecer la prioridad de la CPU (en las propiedades de la máquina virtual) en el nivel más alto para mejorar el comportamiento de la programación y la latencia de la red.

En la siguiente tabla se enumeran los requisitos mínimos para configurar el nodo de recuperación ante desastres:

| Componente | Requisito |
|---|---|
| RAM | 32 GB |
| CPU virtual | 8 CPUs |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Componente | Requisito |
| --- | --- |
| Espacio de almacenamiento | Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. El valor predeterminado es 120 GB. Los requisitos reales de almacenamiento dependen de la estimación del tamaño de Citrix ADM. Si sus requisitos de almacenamiento de Citrix ADM superan los 120 GB, debe adjuntar un disco adicional. **Nota** Solo puede agregar un disco más. Citrix recomienda estimar el almacenamiento y adjuntar más disco en el momento de la implementación inicial. Para obtener más información, consulte Cómo conectar un disco adicional a Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |
| **Hypervisor** | **Versiones** |
| Citrix Hypervisor | 6.2 y 6.5 |
| VMware ESXi | 5.5 y 6.0 |
| Microsoft Hyper-V | 2012 R2 |
| Linux KVM | Ubuntu y Fedora |

## Configuración de recuperación ante desastres por primera vez

- Implementar Citrix ADM en modo de alta disponibilidad
- Implementar y registrar el nodo de recuperación ante desastres de Citrix ADM
- Habilitar y inhabilitar la configuración de recuperación ante desastres desde la interfaz de usuario

### Implementar Citrix ADM en modo de alta disponibilidad

Para configurar la configuración de recuperación ante desastres, asegúrese de que Citrix ADM se implementa en modo de alta disponibilidad. Para obtener información sobre la implementación de Citrix ADM en alta disponibilidad, consulteImplementación de alta disponibilidad

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> - Citrix ADM implementado en modo de alta disponibilidad debe actualizarse a la versión 13.0 de Citrix ADM.
> - **La dirección IP flotante es obligatoria** para registrar el nodo de recuperación ante desastres con el nodo principal.

### Implemente y registre el nodo de recuperación ante desastres de Citrix ADM mediante la consola DR

Para registrar el nodo de recuperación ante desastres de Citrix ADM:

1. Descargue el archivo de imagen `.xva` del sitio de descargas de Citrix e impórtelo a su hipervisor.
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.

   > **Nota**
   >
   > El nodo de recuperación ante desastres puede estar en una subred diferente.

   ```
   ------------------------------------------------------------------------
   Citrix ADM initial network configuration.
   This menu allows you to set and modify the initial IPv4 network addresses.
   The current value is displayed in brackets ([]).
   Selecting the listed number allows the address to be changed.
   ------------------------------------------------------------------------
         1. Citrix ADM Host Name [DR]:
         2. Citrix ADM IPv4 address [10.102.29.53]:
         3. Netmask [255.255.255.0]:
         4. Gateway IPv4 address [10.102.29.1]:
         5. DNS IPv4 Address [127.0.0.2]:
         6. Cancel and quit.
         7. Save and quit.

   Select a menu item from 1 to 7 [7]:
   ```

3. Una vez completada la configuración de red inicial, el sistema solicita el inicio de sesión. Inicie sesión con las siguientes credenciales: `nsrecover`/`nsroot`.

   > **Importante** No cambie las credenciales del nodo DR (`nsrecover`/`nsroot`) durante el registro. Puede cambiar las credenciales del nodo DR después de registrar el nodo DR correctamente.

4. Para implementar el nodo de recuperación ante desastres, escriba **/mps/deployment_type.py** y presione Entrar. Aparece el menú de configuración de implementación de Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. Seleccione **2** para registrar el nodo de recuperación ante desastres.

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. La consola solicita la dirección IP flotante del nodo de alta disponibilidad y la contraseña.
7. Introduzca la dirección IP flotante y la contraseña para registrar el nodo de recuperación ante desastres en el nodo principal.

```
--------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    --------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

El nodo de recuperación ante desastres se ha registrado correctamente.

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
--------------------------------------------------------------------------
    Backup node Registration successful.
    --------------------------------------------------------------------
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El nodo de recuperación ante desastres no tiene una GUI.

8. Si quiere cambiar la contraseña del nodo DR, ejecute la siguiente script:

```
/mps/change_freebsd_password.sh <username> <password>
```

#### Implementar el nodo de recuperación ante desastres mediante la GUI de Citrix ADM

Una vez que el nodo de recuperación ante desastres se haya registrado correctamente mediante la consola de recuperación ante desastres, implemente el nodo de recuperación ante desastres desde la GUI de Citrix ADM. Este paso habilita la configuración de recuperación ante desastres desde el sitio principal de Citrix ADM.

1. Vaya a **Sistema > Administración del sistema > Configuración de recuperación ante desastres.**
2. En la página de **recuperación ante desastres**, seleccione **Deploy DR Node**.
3. Se muestra un cuadro de diálogo de confirmación. Haga clic en **Sí** para continuar.

> **Nota**
>
> El tiempo necesario para la copia de seguridad del sistema depende del tamaño de los datos y de la velocidad del enlace WAN.

Tras implementar correctamente el nodo DR en la GUI de Citrix ADM, puede supervisar el estado de la base de datos, la memoria, la CPU y el uso del disco del nodo DR.

Para inhabilitar la configuración de recuperación ante desastres, seleccione**Eliminar nodo DR**. Se muestra un cuadro de diálogo de confirmación. Haga clic en**Sí** para continuar.

Para volver a habilitar el nodo DR, vuelva a configurar el nodo DR para el par de alta disponibilidad:

1. Inicie sesión en el nodo DR mediante un Hypervisor o una consola SSH.
2. Configure el nodo de DR siguiendo el procedimiento disponible en Implementar y registrar el nodo de recuperación ante desastres de Citrix ADM mediante la consola de DR.
3. Implemente el nodo de recuperación ante desastres mediante la GUI de Citrix ADM.

Para obtener más información, consulte las preguntas frecuentes.

> **Importante**
>
> - Es responsabilidad del administrador detectar que se ha producido un desastre en el sitio principal.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> - El flujo de trabajo de recuperación ante desastres lo inicia manualmente el administrador después de que el sitio principal se apaga.
> - Un administrador debe iniciar manualmente el proceso ejecutando un script de recuperación en el nodo de recuperación ante desastres en el sitio de recuperación.
> - Si actualiza el par HA en el sitio primario, también debe actualizar manualmente el nodo independiente en el sitio DR.

### Flujo de trabajo después del desastre

Cuando el sitio principal deja de funcionar después de un desastre, el flujo de trabajo de recuperación ante desastres se debe iniciar de la siguiente manera:

1. El administrador identifica que un desastre ha afectado al sitio principal y que no está operativo.
2. El administrador inicia el proceso de recuperación.
3. El administrador debe ejecutar manualmente uno de los siguientes scripts de recuperación en el nodo de recuperación ante desastres según su requisito (en el sitio de recuperación):
   - Configure SNMP, Syslog y Analytics en el nodo DR:

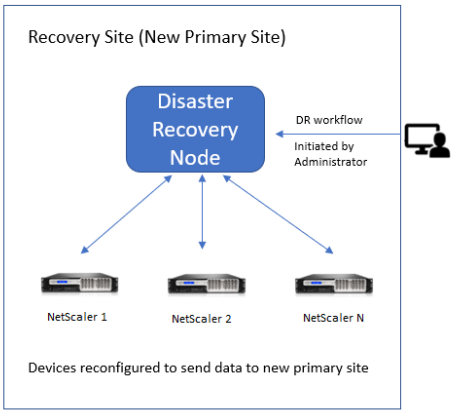
     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh
     ```

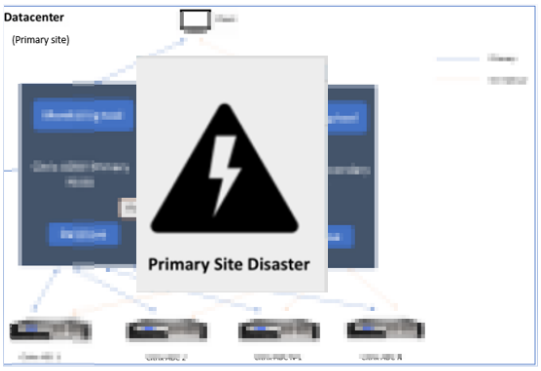
   - Configure también el nodo DR como servidor de licencias:

     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
        ls <IP-address-of-the-primary-site>
     ```

4. Internamente, las instancias Citrix ADC se reconfiguran automáticamente para enviar los datos al nodo de recuperación ante desastres que ahora se ha convertido en el nuevo sitio principal.

   La imagen siguiente muestra que el flujo de trabajo de recuperación ante desastres después de que el sitio principal se golpea con un desastre.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Nota:
>
> Después de iniciar el script en el sitio de DR, el sitio de DR ahora se convierte en el nuevo sitio principal. También puede acceder a la interfaz de usuario DR.

## Recuperación posterior a desastres

Una vez que se ha producido el desastre y el administrador inicia el script de recuperación, el sitio de recuperación ante desastres se convierte ahora en el nuevo sitio principal.

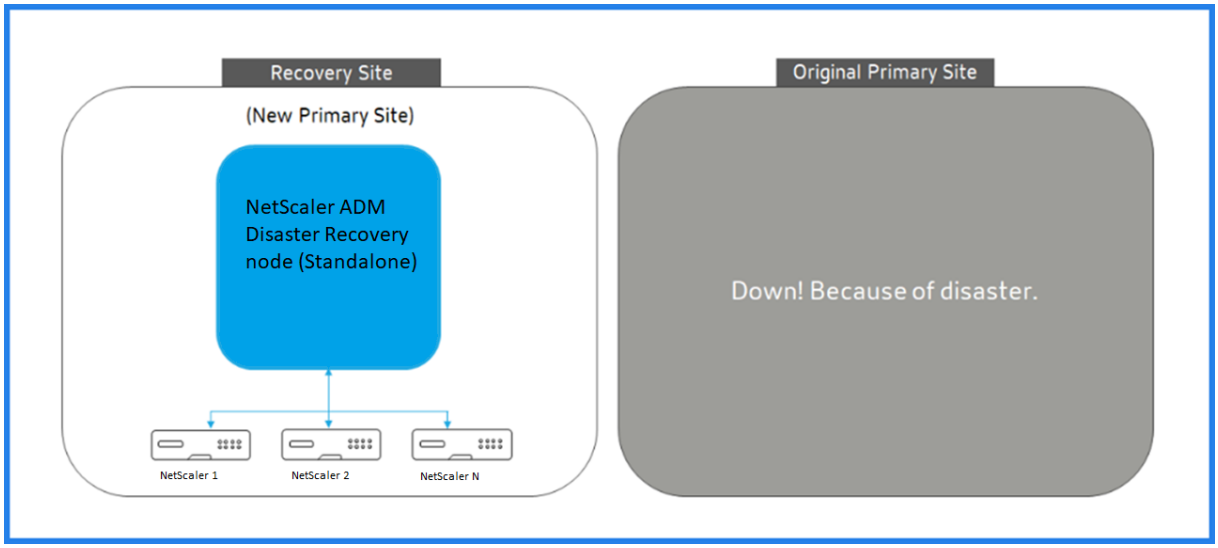
Si quiere revertir las configuraciones al sitio original más adelante, consulte Revertir configuraciones al sitio principal original.

> **Importante**
>
> - Si ha instalado Citrix ADM 12.1.49.x o versiones anteriores, dispone de un período de gracia de 30 días para ponerse en contacto con Citrix para volver a alojar la licencia original en Citrix ADM (en el sitio de recuperación ante desastres).
> - Para la versión 12.1.50.x o versiones posteriores, la licencia Citrix ADM se sincroniza automáticamente con el sitio de recuperación ante desastres (no es necesario ponerse en contacto con Citrix para obtener la licencia).
> - La licencia agrupada para el sitio de DR se admite desde la versión 12.1.50.x o versiones posteriores. Si ha aplicado licencias agrupadas para las instancias, vuelva a configurar manualmente las instancias en el sitio de recuperación ante desastres.

## Revertir las configuraciones al sitio principal original

Tras un desastre, el nodo de recuperación ante desastres (DR) configurado se convierte en el nuevo sitio principal y el tráfico del cliente fluye a través de este nodo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para obtener más información, consulte Flujo de trabajo después del desastre.

Cuando el sitio primario original esté libre de desastres y decida mover todas las operaciones al sitio primario, vuelva a configurar el sitio primario original para que coincida con las configuraciones del nodo DR.

Antes de empezar, asegúrese de que tanto el sitio principal como el sitio de DR estén activos.

Para revertir los cambios en el sitio principal original desde el sitio de DR, lleve a cabo los siguientes pasos:

1. Inicie sesión en el sitio principal original y ejecute el siguiente comando:

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
       password> -L <primary-node-password> &
   ```

   Este comando configura solo Syslog, SNMP y Analytics en el sitio principal.

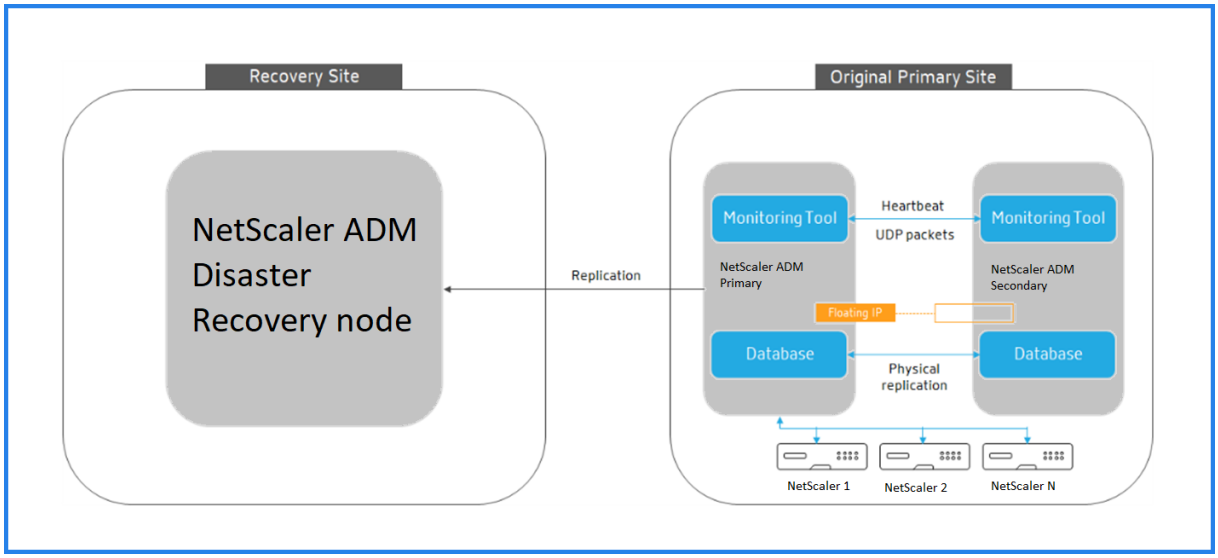
   Si quiere configurar el sitio principal como un servidor de licencias agrupado para instancias de ADC, ejecute el siguiente comando:

   ```
   nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-
       password> -L <primary-node-password>  -O yes &
   ```

   El comando -O recupera la dirección IP del sitio DR y reconfigura el sitio primario como servidor de licencias agrupado.

2. Vuelva a configurar el sitio de recuperación ante desastres. Consulte Implementar la configuración de recuperación ante desastres.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Después de revertir correctamente las configuraciones del sitio de recuperación ante desastres al sitio principal original, el tráfico del cliente fluye a través del nodo principal de Citrix ADM.

## Configurar agentes en prem para la implementación en varios sitios

January 30, 2024

En las versiones anteriores de Citrix ADM, las instancias de Citrix ADC implementadas en centros de datos remotos se pueden administrar y supervisar desde Citrix ADM que se ejecuta en un centro de datos principal. Las instancias de Citrix ADC enviaron datos directamente al dispositivo principal de Citrix ADM, lo que provocó el consumo de ancho de banda de la red WAN. Además, el procesamiento de datos de análisis utiliza recursos de CPU y memoria del dispositivo principal de Citrix ADM.

Puede tener centros de datos ubicados en todo el mundo. Los agentes desempeñan un papel vital en los siguientes casos:

- Instalar agentes en centros de datos remotos para reducir el consumo de ancho de banda WAN.
- Limitar el número de instancias que envían tráfico directamente al Citrix ADM principal para el procesamiento de datos.

> **Nota**
>
> - Se recomienda instalar agentes para instancias en el centro de datos remoto, pero no es obligatorio. Si es necesario, los usuarios pueden agregar directamente instancias de Citrix ADC a Citrix ADM principal.
> - Si ha instalado agentes para uno o más centros de datos remotos, la comunicación entre

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> los agentes y el sitio principal se realiza a través de una dirección IP flotante. Para obtener más información, consulte port.
>
> - Puede instalar agentes y aplicar licencias agrupadas a las instancias de uno o más centros de datos remotos. En este caso, la comunicación entre el sitio principal y uno o más centros de datos remotos se realiza a través de la dirección IP flotante.

Desde Citrix ADM 12.1 o posterior, las instancias se pueden configurar con agentes para que se comuniquen con el Citrix ADM principal ubicado en un centro de datos diferente.

Los agentes funcionan como intermediarios entre la instancia principal de Citrix ADM y las instancias descubiertas en diferentes centros de datos. Los siguientes son los beneficios de instalar agentes:

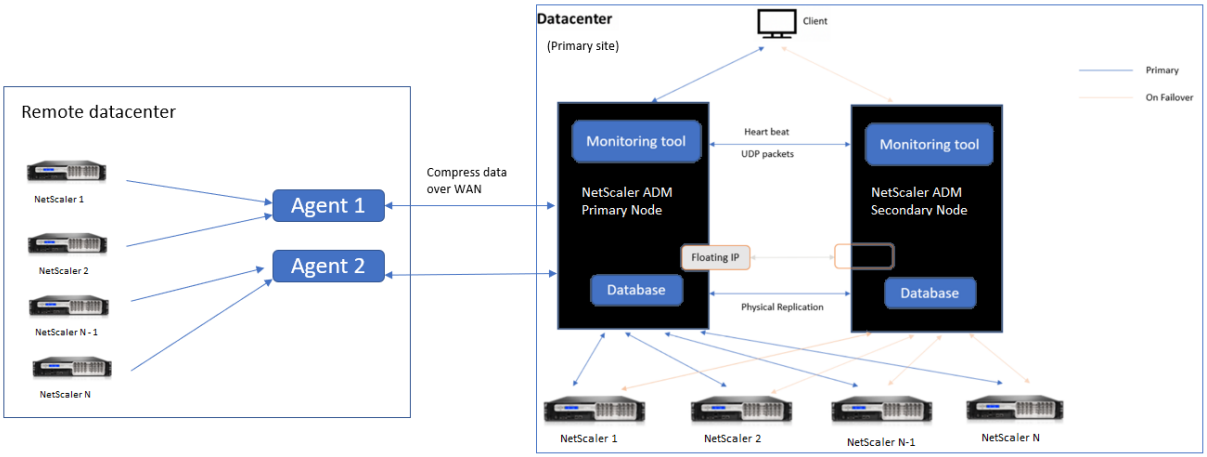
- Las instancias se configuran para agentes de modo que los datos no procesados se envíen directamente a los agentes en lugar de la instancia principal de Citrix ADM. Los agentes realizan el primer nivel de procesamiento de datos y envían los datos procesados en formato comprimido al Citrix ADM principal para su almacenamiento.
- Los agentes y las instancias se encuentran en el mismo centro de datos para que el procesamiento de datos sea más rápido.
- La agrupación en clústeres de los agentes proporciona una redistribución de instancias de Citrix ADC en caso de conmutación por error del agente. Cuando un agente de un sitio falla, el tráfico de las instancias de Citrix ADC se cambia a otro agente disponible en el mismo sitio.

  > **Nota**
  >
  > El número de agentes que se instalarán por sitio depende del tráfico que se esté procesando.

## Arquitectura

En la siguiente ilustración se muestran las instancias de Citrix ADC en dos centros de datos y la implementación de alta disponibilidad de Citrix ADM mediante una arquitectura basada en agentes multisitio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




El sitio principal tiene los nodos Citrix ADM implementados en una configuración de alta disponibilidad. Las instancias de Citrix ADC del sitio principal se registran directamente en Citrix ADM.

En el sitio secundario, los agentes se implementan y registran con el servidor Citrix ADM en el sitio principal. Estos agentes trabajan en un clúster para gestionar el flujo continuo de tráfico en caso de que se produzca una conmutación por error del agente. Las instancias de Citrix ADC del sitio secundario se registran en el servidor Citrix ADM principal a través de agentes ubicados en ese sitio. Las instancias envían datos directamente a los agentes en lugar de la instancia principal de Citrix ADM. Los agentes procesan los datos recibidos de las instancias y los envían a la instancia principal de Citrix ADM en un formato comprimido. Los agentes se comunican con el servidor de Citrix ADM a través de un canal seguro y los datos enviados por el canal se comprimen para aumentar la eficiencia del ancho de banda.

## Introducción

- Instalar el agente en un centro de datos
  - Registrar el agente
  - Adjuntar el agente a un sitio
- Agregar instancias de Citrix ADC
  - Agregar una nueva instancia
  - Actualizar una instancia existente

### Instalar el agente en un centro de datos

Puede instalar y configurar el agente para habilitar la comunicación entre la instancia principal de Citrix ADM y las instancias administradas de Citrix ADC en otro centro de datos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede instalar un agente en los siguientes hipervisores del centro de datos de su empresa:

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Servidor KVM Linux

> **Nota**
>
> Los agentes locales para la implementación en varios sitios solo se admiten con la implementación de alta disponibilidad de Citrix ADM.

Antes de comenzar a instalar el agente, asegúrese de que dispone de los recursos informáticos virtuales necesarios que el Hypervisor debe proporcionar para cada agente.

| Componente | Requisito |
|---|---|
| RAM | 32 GB |
| CPU virtual | 8 CPUs |
| Espacio de almacenamiento | 30 GB |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps |

**Puertos**

A efectos de comunicación, los siguientes puertos deben estar abiertos entre el agente y el servidor de Citrix ADM on-prem.

| Tipo | Puerto | Detalles | Dirección de comunicación |
|---|---|---|---|
| TCP | 8443, 7443, 443 | Para la comunicación entrante y saliente entre el agente y el servidor de Citrix ADM on-prem. | Agente de Citrix ADM a Citrix ADM |

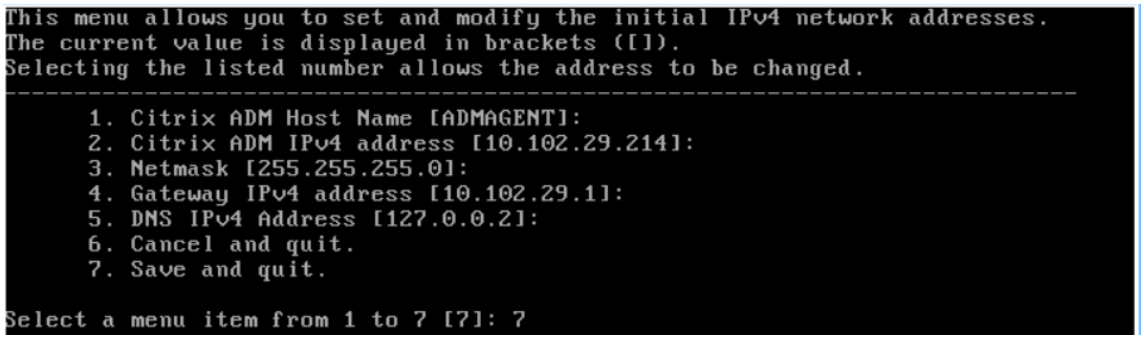
Los siguientes puertos deben estar abiertos entre el agente y las instancias de Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Tipo | Puerto | Detalles |Dirección de comunicación|
| —- | —| ——- |—-|
| TCP | 80 | Para la comunicación NITRO entre el agente y la instancia Citrix ADC o Citrix SD-WAN. |Citrix ADM a Citrix ADC y Citrix ADC a Citrix ADM|
| TCP | 22 | Para la comunicación SSH entre el agente y la instancia de Citrix ADC o Citrix SD-WAN. Para la sincronización entre los servidores Citrix ADM implementados en modo de alta disponibilidad. |Citrix ADM a Citrix ADC y agente de Citrix ADM a Citrix ADC|
| UDP | 4739 | Para la comunicación de AppFlow entre el agente y la instancia Citrix ADC o Citrix SD-WAN.|Citrix ADC o Citrix SD-WAN a Citrix ADM|
| ICMP | Sin puerto reservado | Para detectar la accesibilidad de la red entre instancias de Citrix ADM y Citrix ADC, instancias SD WAN o el servidor secundario de Citrix ADM implementado en modo de alta disponibilidad. |
| UDP | 161, 162 | Para recibir eventos SNMP de una instancia de Citrix ADC al agente. |Puerto 161 - Citrix ADM a Citrix ADC| |
| | |Puerto 162 - Citrix ADC a Citrix ADM |
| UDP | 514 | Para recibir mensajes syslog de Citrix ADC o instancia de Citrix SD-WAN al agente. |Citrix ADC o Citrix SD-WAN a Citrix ADM|
| TCP | 5557 | Para comunicación Logstream entre instancias de agente y Citrix ADC. |Citrix ADC a Citrix ADM|

**Registrar el agente**

1. Utilice el archivo de imagen del agente descargado desde el sitio de descarga de Citrix e impórtelo en el Hypervisor. <Version.no\ >El patrón de nombres del archivo de imagen del agente es el siguiente:**MASAGENT- \-**<HYPERVISOR\ >. Por ejemplo: **MASAGENT-XEN-13.0-xy.xva**
2. En la ficha **Consola**, configure Citrix ADM con las configuraciones de red iniciales.
3. Introduzca el nombre de host de Citrix ADM, la dirección IPv4 y la dirección IPv4 de la puerta de enlace. Seleccione la opción 7 para guardar y salir de la configuración.




4. Una vez que el registro se realiza correctamente, la consola le pedirá que inicie sesión. Utilice *nsrecover/nsroot* como credenciales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Para registrar el agente, escriba**/mps/register_agent_onprem.py**. Las credenciales de registro del agente Citrix ADM se muestran como se muestra en la siguiente imagen.
6. Introduzca la dirección IP flotante Citrix ADM y las credenciales de usuario.

```
bash-3.2# /mps/register_agent_onprem.py

--------------------------------------------------------------------------------
--------------------------------------
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows y
ou to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix AD
M floating IP Address.
--------------------------------------------------------------------------------
--------------------------------------
    Enter IP Address or URL:10.102.29.211
    Enter User Name:nsroot
    Enter Password:

Trying to register this agent with Citrix ADM  10.102.29.211
Dec  3 18:07:52 <auth.notice> ns date: date set by nsrecover
--------------------------------------------------------------------------
    Citrix ADM Agent Registration successful.
--------------------------------------------------------------------------
```

Una vez que el registro se realiza correctamente, el agente se reinicia para completar el proceso de instalación.

Después de reiniciar el agente, acceda a la GUI de Citrix ADM, desde el menú principal vaya a la página **Redes > Agentes** para verificar el estado del agente.El agente recién agregado se muestra en estado **Activo**.

> **Nota**
>
> Citrix ADM muestra la versión del agente y también comprueba si el agente está en la versión más reciente. El icono de descarga indica que el agente no está en la versión más reciente y debe actualizarse. Citrix recomienda actualizar la versión del agente a la versión de Citrix ADM.

### Adjuntar un agente a un sitio

1. Seleccione el agente y haga clic en **Adjuntar sitio.**
2. En la página**Adjuntar sitio**, seleccione un sitio de la lista o cree un sitio mediante el botón más (+).
3. Haz clic en **Guardar.**

> **Nota**
>
> - De forma predeterminada, todos los agentes recién registrados se agregan al centro de datos predeterminado.
> - Es importante asociar el agente con el sitio correcto. En caso de que se produzca un error en el agente, las instancias de Citrix ADC asignadas se conmutan automáticamente

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> a otros agentes en funcionamiento en el mismo sitio.

## Acciones del agente

Puede aplicar varias acciones a un agente en **Redes > Agentes > Seleccionar acciones**.

En **Seleccionar acción**, puede utilizar las siguientes funciones:

Instale un certificado nuevo: si necesita un certificado de agente diferente para cumplir con sus requisitos de seguridad, puede agregar uno.

Cambie la contraseña predeterminada: para garantizar la seguridad de su infraestructura, cambie la contraseña predeterminada de un agente.

Generar un archivo de soporte técnico: genere un archivo de soporte técnico para un agente de Citrix ADM seleccionado. Puede descargar este archivo y enviarlo al soporte técnico de Citrix para su investigación y solución de problemas.

## Agregar instancias de Citrix ADC

Las instancias son dispositivos Citrix o dispositivos virtuales que quiere descubrir, administrar y supervisar desde Citrix ADM a través de agentes. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM o agentes:

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Proxy de reenvío SSL de Citrix
- Citrix SD-WAN WO

Para obtener más información, consulte Agregar instancias a Citrix ADM.

### Adjuntar una instancia existente al agente

Si ya se ha agregado una instancia al dispositivo principal de Citrix ADM, puede adjuntarla a un agente modificando un agente.

1. Vaya a **Redes > Instancias** y seleccione el tipo de instancia. Por ejemplo, Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Haga clic en **Modificar** para modificar una instancia existente.
3. Haga clic para seleccionar el agente.
4. En la página **Agente**, seleccione el agente al que quiere asociar la instancia y, a continuación, haga clic en**Aceptar**.

> **Nota**
>
> Asegúrese de seleccionar el **sitio** al que quiere asociar la instancia.

#### Acceder a la GUI de una instancia para validar eventos

Después de agregar las instancias y configurar el agente, acceda a la GUI de una instancia para comprobar si el destino de la captura está configurado.

En Citrix ADM, vaya a**Redes > Instancias**. En**Instancias**, seleccione el tipo de instancia a la que quiere acceder (por ejemplo, Citrix ADC VPX) y, a continuación, haga clic en la dirección IP de una instancia específica.

La GUI de la instancia seleccionada se muestra en una ventana emergente.

De forma predeterminada, el agente está configurado como destino de captura en la instancia. Para confirmarlo, inicie sesión en la GUI de la instancia y compruebe los destinos de las trampas.

> **Importante**
>
> Se recomienda agregar un agente para las instancias de Citrix ADC en centros de datos remotos, pero no es obligatorio.
>
> En caso de que quiera agregar la instancia directamente al MAS principal, no seleccione**un agente** al agregar instancias.

### Conmutación por error del agente de Citrix ADM

La conmutación por error del agente puede producirse en un sitio que tiene dos o más agentes registrados. Cuando un agente pasa a estar inactivo (estado INACTIVO) en el sitio, Citrix ADM redistribuye las instancias de ADC del agente inactivo con otros agentes activos.

> **Importante**
>
> - Asegúrese de que la función de **conmutación por error del agente** esté habilitada en su cuenta. Para habilitar esta función, consulte Habilitar o inhabilitar las funciones de ADM.
> - Si un agente está ejecutando un script, asegúrese de que el script está presente en todos

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> los agentes del sitio. Por lo tanto, el agente modificado puede ejecutar el script después de la conmutación por error del agente.

Para adjuntar un sitio a un agente en la GUI de ADM, consulte Adjuntar un agente a un sitio.

Para lograr una conmutación por error del agente, seleccione agentes Citrix ADM uno por uno y adjunte al mismo sitio.

Por ejemplo, dos agentes 10.106.1xx.2x y 10.106.1xx.3x están conectados y operativos en el sitio de Bangalore. Si un agente queda inactivo, Citrix ADM lo detecta y muestra el estado como inactivo.

Cuando un agente Citrix ADM pasa a estar inactivo (estado Inactivo) en un sitio, Citrix ADM espera cinco minutos a que el agente se active (estado Activo). Si el agente permanece inactivo, Citrix ADM redistribuye automáticamente las instancias entre los agentes disponibles en el mismo sitio.

Citrix ADM desencadena la redistribución de instancias cada 30 minutos para equilibrar la carga entre los agentes activos del sitio.

## Instalar un agente ADM como microservicio en un clúster de Kubernetes

January 30, 2024

La implementación de un agente de Citrix ADM como microservicio es útil para administrar Citrix ADC CPX. Los procedimientos disponibles en este documento solo son aplicables si el clúster de Citrix ADM y Kubernetes están configurados en una red diferente. En este caso, puede configurar un agente ADM como un microservicio, donde se aloja el clúster de Kubernetes.

> Nota
>
> También puede configurar un agente local y registrarlo en la red, donde se aloja el clúster de Kubernetes.

### Introducción

1. En Citrix ADM, vaya a **Redes > Agentes**.
2. En la lista **Seleccionar acción**, seleccione la opción **Descargar microservicio del agente**.
3. En la página **Descargue Agent Microservicio**, especifique los siguientes parámetros:
   a) **ID de aplicación**: Un ID de cadena para definir el servicio para el agente en el clúster de Kubernetes y distinguir este agente de otros agentes del mismo clúster.
   b) **Contraseña**: Especifique una contraseña para que CPX utilice esta contraseña para incorporarla CPX a ADM a través del agente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

c) **Confirmar contraseña**: Especifique la misma contraseña para la confirmación.

> Nota
>
> No debe usar la contraseña predeterminada (`nsroot`).

d) Haga clic en **Descargar archivo Yaml**.

### Instalar el agente Citrix ADM en el clúster de Kubernetes

En el nodo principal de Kubernetes:

1. Guardar el archivo YAML descargado
2. Ejecute este comando:

   ```
   kubectl create -f <yaml file>
   ```

   Por ejemplo, `kubectl create -f testing.yaml`

   El agente se ha creado correctamente.

   ```
   root@[redacted]:/# kubectl create -f testing.yaml
   deployment.apps/testing created
   service/testing created
   secret/testing created
   configmap/testing created
   root@[redacted]/#
   ```

En Citrix ADM, vaya a **Redes** > **Agentes** para ver el estado del agente.

Para obtener más información sobre cómo empezar a usar el gráfico de servicio, consulte Configuración del gráfico de servicio.

## Migrar la implementación de un solo servidor de Citrix ADM a una implementación de alta disponibilidad

January 30, 2024

Puede actualizar su servidor único Citrix ADM a una implementación de alta disponibilidad de dos servidores Citrix ADM. Un par de servidores Citrix ADM de alta disponibilidad están en modo activo-pasivo y ambos servidores tienen la misma configuración. En este tipo de implementación activa-pasiva, un servidor Citrix ADM se configura como nodo principal y el otro como nodo secundario. Si por alguna razón, el nodo principal deja de funcionar, el nodo secundario toma el relevo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para migrar un servidor único de Citrix ADM a un par de alta disponibilidad, debe aprovisionar un nuevo nodo de servidor Citrix ADM, configurarlo como el segundo servidor único de Citrix ADM e implementar ambos servidores Citrix ADM como un par de alta disponibilidad.

La migración de un servidor único Citrix ADM a un modo de alta disponibilidad implica los siguientes pasos:

1. Modificación del nodo de servidor existente
2. Provisioning del segundo nodo del servidor
3. Implementación de los dos nodos en modo HA
4. Configuración del par de alta disponibilidad

### Modificar el nodo del servidor Citrix ADM existente

Para migrar Citrix ADM del modo de servidor único al modo de alta disponibilidad, debe cambiar el tipo de implementación inicial del nodo del servidor al modo de alta disponibilidad.

1. En una estación de trabajo o portátil, abra la consola del nodo del servidor Citrix ADM existente. Por ejemplo, considere que ha implementado un Citrix ADM con la dirección IP 10.106.171.17 como servidor independiente.
2. Inicie sesión en Citrix ADM. Las credenciales predeterminadas son `nsroot` y `nsroot`.
3. En el símbolo del shell `/mps/deployment_type.py`, escriba y presione **Entrar**.
4. Seleccione el tipo de implementación como servidor Citrix ADM. Si no selecciona ninguna opción, de forma predeterminada, se implementa como servidor.

```
bash-3.2# /mps/deployment_type.py
-------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
-------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. La consola de implementación le pide que seleccione la implementación del servidor (como independiente). Escriba **No** para confirmar la implementación como par de alta disponibilidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. La consola le pide que seleccione el (primer nodo del servidor). Introduzca **Sí** para confirmar que el nodo es el primer nodo del servidor.
7. La consola le pide que reinicie el servidor.
8. Escriba **Sí** para reiniciar.

```
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
 [yes/no]:yes
```

### Aprovisione el segundo nodo del servidor

Debe aprovisionar el segundo servidor del hipervisor. Utilice el mismo archivo de imagen que utilizó para instalar el primer servidor u obtenga un archivo de imagen de la misma versión en el sitio de descargas de Citrix.

1. Importe el archivo de imagen al Hypervisor y, a continuación, desde la ficha Consola, configure las opciones de configuración de red iniciales como se explica en la siguiente pantalla:

```
-----------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
-----------------------------------------------------------------------
      1. Citrix ADM Host Name [CitrixADM]:
      2. Citrix ADM IPv4 address [10.102.29.211]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

2. Tras especificar las direcciones IP necesarias, en la línea de comandos, escriba /mps/deployment_type.py y pulse enter.
3. Seleccione el tipo de implementación como **servidor Citrix ADM**.
4. La consola de implementación le pide que seleccione la implementación del servidor (como independiente). Escriba **No** para confirmar la implementación como par de alta disponibilidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
bash-3.2# /mps/deployment_type.py
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

5. A continuación, la consola le pide que seleccione el (primer nodo del servidor). Escriba **No** para confirmar el nodo como el segundo nodo del servidor.

```
--------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
--------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

6. Introduzca la dirección IP y la contraseña del primer servidor.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
-----------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

-----------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

7. Introduzca la dirección IP flotante del primer nodo.

```
-----------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no

-----------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            -------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
    Enter Floating IP address:10.102.29.97
```

8. La consola le pide que reinicie el sistema. Escriba**Sí** para reiniciar.

## Implemente los dos servidores en un modo de alta disponibilidad

Para completar el proceso de instalación de los dos nodos de servidor como un par de alta disponibilidad, debe implementar estos nodos desde la GUI del nodo de servidor Citrix ADM existente anteriormente. La comunicación interna entre los dos servidores se inicia al implementar los dos nodos de servidor.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Importante**
>
> Antes de implementar nodos de alta disponibilidad, asegúrese de cambiar la contraseña predeterminada.

1. En un explorador web, escriba la dirección IP del nodo del servidor Citrix ADM existente anteriormente.
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Sistema**, vaya a **Implementación** y haga clic en **Implementar**.
4. Aparece un mensaje de confirmación. Haga clic en **Sí**.

   > **Nota**
   >
   > Tras implementar Citrix ADM en alta disponibilidad, puede acceder al nodo principal o a la dirección IP flotante. No se puede acceder al nodo secundario desde la versión 12.1 en adelante.

5. Si bien ha introducido la IP flotante al configurar el segundo nodo del servidor, tiene la opción de actualizar el FIP en la página **Sistemas**. Haga clic en **Configuración de HA** > **Configurar una dirección IP flotante para el modo de alta disponibilidad**. Puede ver la dirección IP flotante que configuró anteriormente. Puede introducir una nueva dirección IP y hacer clic en **Aceptar**.

## Migrate from NetScaler Insight Center to NetScaler ADM

January 30, 2024

Ahora puede migrar la implementación de NetScaler Insight Center a NetScaler ADM sin perder la configuración, la configuración o los datos existentes. Con Citrix ADM, no solo puede ver los distintos análisis generados por las instancias de Citrix ADC asociadas a una aplicación, sino que también puede administrar, supervisar y solucionar problemas de toda la infraestructura global de entrega de aplicaciones desde una única consola unificada.

> **Nota**
>
> Actualmente, la migración solo se admite en las instancias independientes de NetScaler Insight Center.

### Requisitos previos

Antes de migrar el dispositivo virtual NetScaler Insight Center a Citrix ADM, compruebe que se cumplen los siguientes requisitos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Está instalado NetScaler Insight Center 11.1 Build 47.14 o posterior.
- Ha descargado el archivo de imagen de NetScaler ADM 12.0, compilación 57.24 .tgz.

> **Nota**
>
> Debe instalar NetScaler ADM 12.0 build 57.24 y, a continuación, actualizar a la versión más reciente de NetScaler ADM 13.0. Para obtener más información, consulte Actualizar.

- Ha descargado el archivo de imagen.tgz de compilación más reciente de NetScaler ADM 13.0.

## Requisitos de hardware

| Componente | Requisito |
|---|---|
| RAM | 32 GB |
| CPU virtual | 8 CPUs |
| Espacio de almacenamiento | 120 GB |
| | **Nota:** Citrix recomienda utilizar**500 GB**para obtener un mejor rendimiento. Además, Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |
| Requisitos de hipervisor | |
| Citrix Hypervisor | 6.2, 6.5 |
| VMware ESX | 5.5, 6.0 |
| Microsoft Hyper-V | 2012 R2 |
| Linux - KVM | Ubuntu, Fedora |

## Procedimiento de instalación

**Para migrar NetScaler Insight Center a NetScaler ADM**:

1. Inicie sesión en el símbolo del shell de NetScaler Insight Center.
2. Descargue NetScaler ADM 12.0 compilación 57.24 en la carpeta */var/mps/mps_images*.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Descomprima el archivo TGZ mediante el comando **tar -zxvf build-mas-12.0-57.24.tgz**.

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. Instale NetScaler ADM mediante **./installmas**.

```
bash-3.2# ./installmas
```

5. Después de instalar NetScaler ADM 12.0 build 57.24, debe actualizar a la versión más reciente de NetScaler ADM 13.0 realizando los pasos anteriores.

Tras la migración, todas las instancias de Citrix ADC que se descubrieron en el inventario de NetScaler Insight Center aparecen en la sección **Redes > Instancias** de Citrix ADM. Sin embargo, por primera vez debe sondear manualmente los servidores virtuales alojados en los dispositivos detectados.

> **Nota**
>
> En Citrix ADM, de forma predeterminada, no hay ningún coste de licencia para administrar y supervisar dos servidores virtuales creados en las instancias de Citrix ADC descubiertas. Para supervisar y administrar más de dos servidores virtuales, instale las licencias NetScaler ADM necesarias. Para obtener más información, consulteLicencias de NetScaler ADM.

## Integración de NetScaler ADM con Citrix Director

January 30, 2024

Director se integra con NetScaler ADM para el análisis de redes y la gestión del rendimiento.

- El análisis de red obtiene los informes de HDX Insight de NetScaler ADM y proporciona una vista de la red desde las aplicaciones y el escritorio. Con esta función, Director proporciona una vista analítica avanzada del tráfico ICA en su implementación.
- La función de administración del rendimiento (Performance Management) proporciona la retención del historial y los informes de tendencias. Con la retención del historial de datos frente a la evaluación en tiempo real, puede crear informes de tendencias que incluyen las tendencias de capacidad y estado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Tras integrar NetScaler ADM con Director, los informes de HDX Insight le proporcionan la siguiente información en Director:

- La ficha Red de la página Tendencias muestra los efectos de latencia y ancho de banda para las aplicaciones, los escritorios y los usuarios de toda la implementación.
- La página Detalles del usuario muestra la información de latencia y ancho de banda específica de la sesión de un usuario en particular.

## Requisitos previos

### Requisitos de hardware para la migración de HDX Insight a NetScaler ADM

| Componente | Requisito |
|---|---|
| RAM | 32 GB |
| CPU virtual | 8 |
| Espacio de almacenamiento | 500 GB. Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM. |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |

### Requisitos de software

Antes de migrar al dispositivo virtual NetScaler ADM, compruebe que se cumplen los siguientes requisitos:

- Está instalada la versión 1811 de Director
- NetScaler HDX Insight versión 10.1 o posterior está instalado
- HDX Insight y NetScaler ADM son compatibles con la versión 7.0 y posteriores de Citrix VDA
- Citrix Workspace es compatible con Citrix Virtual Apps and Desktops versión 7.0 y posterior
- Asegúrese de que MAC Citrix Receiver para Mac versión 11.8 y posteriores y Windows Citrix Receiver para Windows 14.0 y posteriores estén disponibles para mostrar métricas ICA RTT precisas
- NetScaler ADM versión 11.0 y posterior está instalado. Para obtener más información sobre cómo instalar NetScaler ADM, consulte Implementar NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Limitaciones

- La disponibilidad de esta función depende de la licencia de la organización y los permisos de administrador.
- El tiempo de ida y vuelta (RTT) de la sesión ICA muestra los datos correctamente para Citrix Receiver para Windows 3.4 o posterior y para Citrix Receiver para Mac 11.8 o posterior. Para las versiones anteriores de estos paquetes de Receiver, los datos no se muestran correctamente.
- En la vista Tendencias, los datos de inicio de sesión de la conexión HDX no se recopilan para los VDA anteriores a la versión 7. Para los VDA anteriores, los datos gráficos se muestran como 0.
- Para las implementaciones que ya tienen un disco duro externo con un espacio de almacenamiento inferior a 500 GB, no puede agregar otro disco duro.

> **Nota**
>
> - Para obtener más información sobre Director y los pasos para integrar NetScaler ADM con Director, consulte https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html.
> - Para obtener más información sobre HDX Insight, consulte http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html.

## Conecte un disco adicional a NetScaler ADM

January 30, 2024

Los requisitos de almacenamiento de NetScaler Application Delivery Management (ADM) se determinan en función de la estimación del tamaño de NetScaler ADM. De forma predeterminada, NetScaler ADM proporciona una capacidad de almacenamiento de 120 GB. Si necesita más de 120 GB para almacenar sus datos, puede conectar un disco adicional.

> **Nota**
>
> - Calcule los requisitos de almacenamiento y conecte un disco adicional al servidor en el momento de la implementación inicial de NetScaler ADM.
> - Para una implementación de un solo servidor de NetScaler ADM, solo puede conectar un disco al servidor además del disco predeterminado.
> - Para una implementación de alta disponibilidad de NetScaler ADM, debe adjuntar un disco adicional a cada nodo. El tamaño de ambos discos debe ser idéntico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> - Si anteriormente había conectado un disco externo de menor capacidad, debe quitar el disco antes de conectar un disco nuevo.
> - Puede conectar un disco adicional de capacidad superior a 2 terabytes. Si es necesario, el tamaño del disco también puede ser inferior a 2 terabytes.
> - Citrix recomienda utilizar la tecnología de unidades de estado sólido (SSD) para las implementaciones de Citrix ADM.

En este documento se explican los siguientes casos acerca de adjuntar un disco nuevo adicional, crear particiones y cambiar el tamaño de los discos adicionales:

1. Adjuntar un disco nuevo y adicional
2. Inicie la herramienta de partición de disco
3. Crear particiones en el nuevo disco adicional
4. Cambiar el tamaño del disco adicional existente
5. Eliminar particiones en el disco adicional

### Conecte un disco adicional en un NetScaler ADM independiente

Realice los siguientes pasos para conectar un disco a la máquina virtual:

1. Apague la máquina virtual NetScaler ADM.
2. En el Hypervisor, conecte un disco adicional del tamaño de disco requerido a la máquina virtual NetScaler ADM.

   El disco más grande recién conectado almacena los datos de la base de datos y los archivos de registro NetScaler ADM. El disco predeterminado existente de 120 gigabytes ahora se usa para almacenar los archivos principales, los archivos de registro del sistema operativo, etc.
3. Inicie la máquina virtual NetScaler ADM.

### Herramienta de partición de disco NetScaler ADM

NetScaler ADM ahora proporciona la **herramienta de partición de disco NetScaler ADM**, una nueva herramienta de línea de comandos. Las funcionalidades de esta herramienta se describen en detalle de la siguiente manera:

1. Con la herramienta, puede crear particiones en el disco adicional recién agregado.
2. También puede cambiar el tamaño del disco adicional existente mediante esta herramienta. Pero el disco externo existente no debe ser mayor que 2 terabytes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> - No es posible cambiar el tamaño de los discos existentes más allá de 2 terabytes sin perder datos. Esto se debe a una limitación conocida de la plataforma.
> - Para crear una capacidad de almacenamiento superior a 2 terabytes, debe eliminar las particiones existentes y crear particiones con esta nueva herramienta.

3. Con esta nueva herramienta, puede realizar cualquier acción de partición en el disco de forma explícita. La herramienta le proporciona una visibilidad y un control claros sobre el disco y los datos asociados.

> **Nota:**
>
> Solo puede usar esta herramienta en el disco adicional que haya conectado al servidor NetScaler ADM. No puede crear particiones en el disco principal (predeterminado) de 120 gigabytes con esta herramienta.

### Inicie la herramienta de partición de disco

1. Abra una conexión SSH a NetScaler ADM mediante un cliente SSH, como PuTTY.
2. Inicie sesión en Citrix ADM con las credenciales de administrador.
3. Cambie al símbolo del shell y escriba:

```
/mps/DiskPartitionTool.py
```

```
bash-3.2# /mps/DiskPartitionTool.py

-------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
-------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> **Nota**
>
> Para NetScaler ADM en la implementación de alta disponibilidad, debe iniciar la herramienta en ambos nodos y crear o cambiar el tamaño de las particiones después de conectar los discos a las máquinas virtuales respectivas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crear particiones en el nuevo disco adicional

El comando **create** se usa para crear particiones siempre que se agrega un disco secundario nuevo. También puede usar este comando para crear particiones en un disco secundario existente después de eliminar las particiones existentes mediante el comando “remove”.

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> **Nota**No
>
> hay limitación de tamaño de 2 terabytes al crear particiones con la herramienta de partición de disco. La herramienta puede crear particiones de más de 2 terabytes. Al particionar el disco, se agrega automáticamente una partición de intercambio de 32 GB de tamaño. A continuación, la partición principal utiliza todo el espacio restante en el disco.

Una vez ejecutado el comando, se crea un esquema de particiones de tabla de particiones GUID (GPT). También se crean una partición de intercambio de 32 GB y una partición de datos para utilizar el resto del espacio. A continuación, se crea un nuevo sistema de archivos en la partición principal.

> **Nota**
>
> Este proceso puede tardar unos segundos y no debe interrumpir el proceso.

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

Una vez que se completa el comando create, la máquina virtual se reinicia automáticamente para que la nueva partición se monte.

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Después del reinicio, la nueva partición se monta en /var/mps.

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0        456046  374346     72580    84%    /
devfs                1       1         0   100%    /dev
procfs               4       4         0   100%    /proc
fdescfs              1       1         0   100%    /dev/fd
/dev/da0s1a    1623950  284466   1209568    19%    /flash
/dev/da0s1e  116073918 2812298 103975708     3%    /var
/dev/da1p1   495168802   43854 455511444     0%    /var/mps
```

La partición swap agregada se muestra como espacio swap en la salida del comando “create”.

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> **Nota**
>
> La herramienta reinicia la máquina virtual después de crear la partición.

### Cambiar el tamaño de las particiones en el disco adicional existente

Puede utilizar el comando **resize** para cambiar el tamaño del disco adjunto (secundario). Puede cambiar el tamaño de un disco que tenga un esquema `master boot record` (`MBR`) o GPT. El tamaño del disco debe ser inferior a 2 terabytes hasta un máximo de 2 terabytes.

> **Nota**
>
> - El comando “cambiar tamaño”está diseñado para funcionar sin perder ningún dato existente. Sin embargo, Citrix recomienda hacer una copia de seguridad de los datos críticos de este disco en un almacenamiento externo antes de intentar cambiar el tamaño. La copia de seguridad de datos es útil en los casos en que los datos del disco pueden dañarse durante la operación de cambio de tamaño.
> - Asegúrese de aumentar el espacio en disco en incrementos de 100 GB de espacio mientras cambia el tamaño de las particiones. Este incremento incremental garantiza que no tendrá que cambiar el tamaño con más frecuencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

El comando "cambiar tamaño"comprueba todas las condiciones previas y continúa si se cumplen todas las condiciones previas y después de que haya dado su consentimiento para cambiar el tamaño. Detiene los procesos que acceden al disco, lo que incluye los subsistemas NetScaler ADM, los procesos de base de datos de PostgreSQL y el proceso de supervisión de NetScaler ADM. Una vez que se detienen los procesos, se desmonta el disco para prepararlo para el cambio de tamaño. El cambio de tamaño se realiza extendiendo la partición para que ocupe todo el espacio disponible y luego aumentando el sistema de archivos. Si existe una partición de intercambio en el disco, se elimina y se vuelve a crear al final del disco después de cambiar el tamaño. La partición swap se describe en la sección **Crear** comando del documento.

> **Nota**
>
> El proceso de "sistema de archivos en crecimiento"puede tardar algunos en completarse y tener cuidado de no interrumpir el proceso mientras está en curso. La herramienta reinicia la máquina virtual después de cambiar el tamaño de la partición.

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

Todos los pasos intermedios en el proceso de cambio de tamaño (detener aplicaciones, cambiar el tamaño del disco, el crecimiento del sistema de archivos) se muestran en la consola. Una vez completado el proceso, se ve el siguiente mensaje.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

Después de reiniciar, el aumento de tamaño se puede observar con el comando “df”. Aquí está el antes y después de aumentar el tamaño:

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

## Elimine las particiones en el disco adicional

Se puede cambiar el tamaño de una partición existente en el disco secundario hasta 2 terabytes. Esto se debe a una limitación conocida de la partición. Si quiere un disco de más de 2 terabytes, conecte un disco nuevo y particione con la herramienta de partición de disco. También puede eliminar la partición existente mediante el comando **remove** y, a continuación, crear una partición.

> **Nota**
>
> Al eliminar la partición existente, se eliminan todos los datos existentes. Por lo tanto, se debe realizar una copia de seguridad de los datos críticos en almacenamiento externo antes de utilizar este comando.

```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

La ejecución del comando “remove”le pide confirmación y, una vez confirmado, detiene todos los procesos (como los subsistemas ADM, los procesos PostgreSQL y el monitor ADM) que utilizan el disco secundario. Si existe una partición de intercambio y el intercambio está habilitado en la partición, el intercambio está inhabilitado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

Cuando escribe “y”, el comando desmonta el disco y elimina todas las particiones del disco.

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

> **Nota**
>
> La herramienta reinicia la máquina virtual después de eliminar la partición.

### Reinicie la máquina virtual

Cuando se crea o cambia el tamaño de una partición, o cuando se crea un archivo de intercambio, reinicie la máquina virtual. Los cambios solo surtirán efecto después de reiniciarse. Para este propósito, se proporciona un comando de **reinicio** en la herramienta.

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

Se le pide confirmación y, una vez confirmado, detiene todos los procesos (como subsistemas ADM, procesos PostgreSQL y monitor ADM). A continuación, se reinicia la máquina virtual.

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

```
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crear un archivo de copia de seguridad de los datos del disco

Estos son los pasos a seguir para hacer una copia de seguridad de los datos de NetScaler ADM antes de cambiar el tamaño de las particiones

> **Nota La**
>
> creación de un archivo de copia de seguridad requiere espacio en disco. Citrix recomienda asegurarse de que hay suficiente espacio libre en disco disponible (50% o más) antes de ejecutar los comandos de copia de seguridad.

1. Detenga ADM.

```
/mps/masd stop
```

2. Detenga PostgreSQL.

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
```

3. Detenga ADM Monitor.

```
/mps/scripts/stop_mas_monit.sh
```

4. Crea un tarball.

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
```

> **Nota**
>
> La operación lleva tiempo dependiendo del tamaño de los datos a los que se debe realizar una copia de seguridad.

5. Generar suma de comprobación.

```
md5 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
```

6. Copie los archivos tarball y de suma de comprobación en un servidor remoto.
7. Validar la exactitud del tarball copiado. Genere una suma de comprobación del archivo transferido y compárela con la suma de comprobación de origen.
8. Elimine el tarball de la máquina virtual ADM.

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Comandos adicionales

Además de los comandos enumerados anteriormente, también puede usar los siguientes comandos en la herramienta:

**Comando de ayuda:**

Para enumerar los comandos admitidos, escriba **help** o **?** y presione Entrar. Para obtener más ayuda en cada uno de los comandos, presione **ayuda** o **?** seguido del nombre del comando y pulse la tecla **Intro**.

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

**Comando Info:**

El comando **info** proporciona información sobre el disco secundario conectado, si el disco existe. El comando proporciona el nombre del dispositivo, el esquema de particiones, el tamaño en formato legible por humanos y la cantidad de bloques de disco. El esquema puede ser MBR o GPT. Un esquema MBR significa que el disco se particionó con una versión anterior de la versión de NetScaler ADM. La partición basada en MBR/GPT se puede cambiar de tamaño, pero no más de 2 terabytes. El esquema de partición GPT significa que el disco se particionó con NetScaler ADM 12.1 o posterior.

> **Nota**
>
> Una partición GPT puede tener más de 2 terabytes pero cuando se crea. Sin embargo, no puede cambiar el tamaño del disco a un tamaño superior a 2 terabytes después de crear un disco con un tamaño más pequeño. Esta es una limitación conocida de la plataforma.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

**Create_swapfile (comando):**

La partición de intercambio predeterminada en el disco principal de NetScaler ADM es de 4 GB y, por lo tanto, el espacio de intercambio predeterminado es de 4 GB. Para la configuración de memoria predeterminada de NetScaler ADM, que es de 2 GB, este espacio de intercambio es suficiente. Sin embargo, cuando ejecuta NetScaler ADM con una configuración de memoria más alta, debe tener más espacio de intercambio asignado en el disco.

> **Nota**
>
> La partición de intercambio suele ser una partición dedicada que se crea en una unidad de disco duro (HDD) durante la instalación del sistema operativo. Dicha partición también se denomina espacio de intercambio. La partición swap se usa para la memoria virtual que simula la memoria principal adicional.

Los discos secundarios que se agregaron en las versiones anteriores de NetScaler ADM no tienen una partición de intercambio creada de forma predeterminada. El comando "create_swapfile"está diseñado para discos secundarios creados con versiones anteriores de NetScaler ADM que no tienen una partición de intercambio. El comando comprueba lo siguiente:

- Presencia de un disco secundario
- Disco que se monta
- Tamaño del disco (al menos 500 GB)
- La existencia del archivo swap

El comando "create_swapfile"solo es útil cuando la memoria es mayor o igual a 16 GB y no cuando la memoria es baja. Por lo tanto, este comando también comprueba si hay memoria antes de continuar con la creación de archivos de intercambio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

Si se cumplen todas las condiciones y el usuario consiente en continuar, se crea un archivo de intercambio de 32 GB en el disco secundario. El proceso de creación del archivo de intercambio tarda unos minutos en completarse y tiene cuidado de no interrumpir el proceso mientras está en curso. Después de completarse correctamente, se realiza un reinicio para que el archivo de intercambio surta efecto.

```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

Después del reinicio, el aumento en el intercambio se puede observar con el comando top.

```
CPU:  1.7% user,  0.0% nice,  0.8% system,  0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user,  0.0% nice,  7.6% system,  5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

**Comando Salir:**

Para salir de la herramienta, escriba exit y presione la tecla **Intro**.

```
(dpt): exit
bash-3.2#
```

## Adjuntar discos adicionales a NetScaler ADM implementados en alta disponibilidad

Consideremos un caso en el que haya configurado un par de servidores NetScaler ADM en una configuración de alta disponibilidad sin discos secundarios. Además, consideremos que ha agregado 2 o más instancias de NetScaler ADC, comprobado y asegurado que todos los procesos se están ejecutando. Es posible que quiera agregar discos secundarios a las máquinas virtuales en esta instalación. En una configuración de alta disponibilidad, debe agregar discos adicionales a ambos nodos como se detalla en esta tarea:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Supongamos que los nombres de los nodos de NetScaler ADM son “ADM_primary”y “ADM_secondary. “
2. Primero, ejecute la herramienta de partición en ADM_secondary y, a continuación, agregue un disco secundario. La máquina virtual se reinicia después de agregar el disco.
3. Apague el ADM_secondary después de que se reinicie.
4. Ahora ejecute la herramienta de partición en ADM_primary y agregue un disco secundario. La máquina virtual se reinicia después de agregar el disco.

   Asegúrese de agregar discos de capacidad similar a ambos nodos. Por ejemplo, si agrega un disco con una capacidad de 500 GB al nodo principal, agregue también un disco de 500 GB de capacidad al nodo secundario.
5. Después de que se reinicie ADM_primary, compruebe que es el nodo principal.
6. Ahora inicie el nodo ADM_secondary. Asegúrese de que aparezca como nodo secundario y de que las bases de datos se hayan sincronizado.
7. Confirme que todos los datos aún existen.

**Para aumentar la capacidad de RAM en ambos nodos:**

1. Cierre ADM_Secondary y aumente el tamaño de RAM según sea necesario. No reinicies el nodo.
2. Cierre ADM_Primary y aumente el tamaño de RAM según sea necesario.

   Asegúrese de aumentar el tamaño de la RAM por igual en ambos nodos. Por ejemplo, si aumenta el tamaño de la RAM en el nodo principal a 16 GB, haga lo mismo en el nodo secundario también.
3. Reinicie ADM_primary.
4. Después de que se reinicie ADM_primary, compruebe que es el nodo principal.
5. Ahora inicie el nodo ADM_secondary. Después de que se reinicie, asegúrese de que aparezca como secundario y que la sincronización de la base de datos esté funcionando.
6. Ahora confirma que todos los datos siguen existiendo.

> **Nota:**
>
> Después de agregar el disco secundario, el nodo principal tarda un tiempo en aparecer. Además, todo el proceso de agregar discos secundarios a ambos nodos y aumentar la capacidad de RAM requiere que ambos nodos estén inactivos durante algún tiempo. Tenga en cuenta este tiempo de inactividad al planificar esta actividad de mantenimiento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configuración

January 30, 2024

Puede acceder a un servidor NetScaler ADM únicamente mediante la GUI. Debe acceder a la GUI para agregar instancias, administrar y supervisar sus instancias y aplicaciones, ver análisis y configurar el servidor NetScaler ADM.

Su estación de trabajo debe tener un explorador web compatible para acceder a la utilidad de configuración y al Panel de control.

Se admiten los siguientes exploradores.

| Explorador web | Versión |
|---|---|
| Internet Explorer | 11.0 y versiones posteriores |
| Google Chrome | Chrome 19 y versiones posteriores |
| Safari | Safari 5.1.1 y versiones posteriores |
| Mozilla Firefox | Firefox 3.6.25 y posterior |

**Para acceder a la GUI de NetScaler ADM:**

Inicie sesión en Citrix ADM con las credenciales de administrador.

Después de iniciar sesión en NetScaler ADM, debe hacer lo siguiente para comenzar:

- Agregue instancias a NetScaler ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias.
- Habilite el análisis en servidores virtuales. Para ver los datos de análisis del flujo de tráfico de su aplicación, debe habilitar la función de análisis en los servidores virtuales que reciben el tráfico de las aplicaciones específicas.
- Configure el servidor NTP en NetScaler ADM. Debe configurar un servidor de protocolo de hora de red (NTP) en Citrix ADM para sincronizar su reloj con el servidor NTP.
- Configure los parámetros del sistema para un rendimiento óptimo de NetScaler ADM.Antes de empezar a utilizar NetScaler ADM para administrar y supervisar sus instancias y aplicaciones, se recomienda configurar algunas opciones del sistema que garanticen un rendimiento óptimo de su servidor NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Agregar instancias a Citrix ADM

January 30, 2024

Las instancias son dispositivos Citrix o dispositivos virtuales que quiere descubrir, administrar y supervisar desde Citrix ADM. Debe agregar instancias al servidor Citrix ADM si quiere administrar y supervisar estas instancias. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM:

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix SD-WAN

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde. A continuación, debe especificar un perfil de instancia que Citrix ADM pueda usar para acceder a la instancia.

> **Nota**
>
> - Citrix ADM utiliza la dirección IP de NetScaler (NSIP) de las instancias Citrix ADC para la comunicación. Para obtener información sobre los puertos que deben estar abiertos entre las instancias de Citrix ADC y Citrix ADM, consulte Puertos.
> - Para las instancias de Citrix SD-WAN WO y Citrix SD-WAN EE, Citrix ADM utiliza la dirección IP de administración de las instancias para la comunicación.
> - Para obtener información sobre cómo Citrix ADM descubre instancias, consulte Descubrir instancias.

## Cómo crear un perfil de Citrix ADC

El perfil Citrix ADC contiene el nombre de usuario, la contraseña, los puertos de comunicación y los tipos de autenticación de las instancias que quiere agregar a Citrix ADM. Para cada tipo de instancia, está disponible un perfil predeterminado. Por ejemplo, `nsroot` es el perfil predeterminado para las instancias de Citrix ADC. El perfil predeterminado se define mediante las credenciales de administrador predeterminadas de Citrix ADC. Si ha cambiado las credenciales de administrador predeterminadas de las instancias, puede definir perfiles de instancia personalizados para esas instancias. Si

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

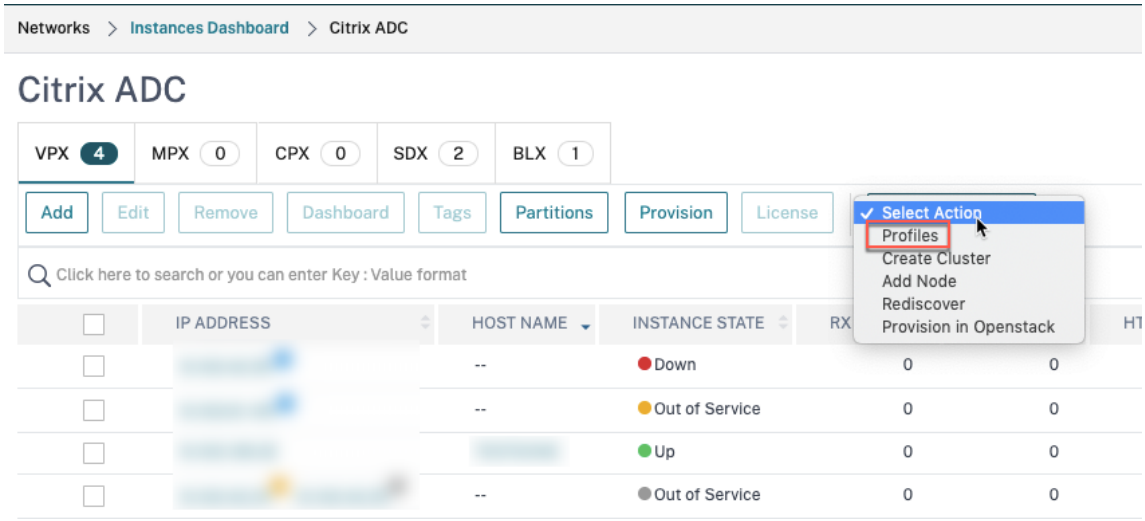
cambia las credenciales de una instancia después de detectarse la instancia, debe modificar el perfil de instancia o crear un perfil y, a continuación, volver a descubrir la instancia.

Puede crear un perfil de Citrix ADC desde la página **Instancia** o al agregar o cambiar una instancia.

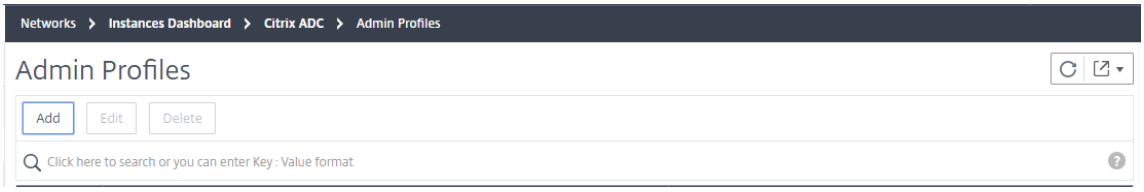
> **Nota**
>
> Asegúrese de usar la cuenta de superadministrador para crear un perfil de instancia.

**Para crear un perfil de Citrix ADC desde la página Instancia:**

1. Vaya a **Redes > Instancias**.
2. Seleccione una instancia. Por ejemplo, Citrix ADC.
3. En la página Citrix ADC, en **Seleccionar acción**, seleccione **Perfiles**.

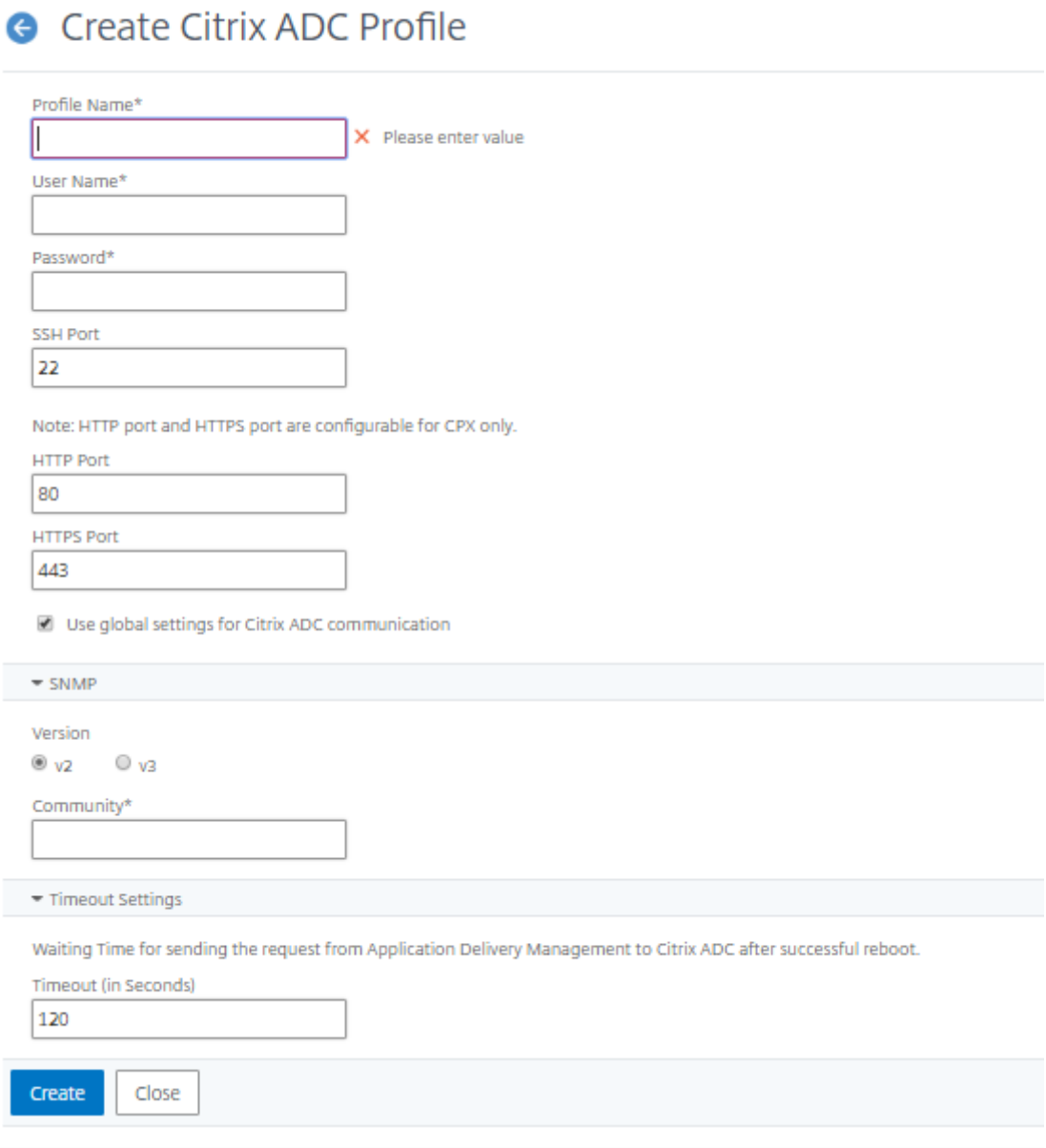



4. En la página **Perfiles de administrador**, seleccione **Agregar**.




5. En la página **Crear perfil de Citrix ADC**, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




a) **Nombre de perfil**: especifique un nombre de perfil para la instancia de Citrix ADC.

b) **Nombre de usuario**: especifique un nombre de usuario para iniciar sesión en la instancia de Citrix ADC.

c) **Contraseña**: especifique una contraseña para iniciar sesión en la instancia de Citrix ADC.

d) **Puerto SSH**: especifique el puerto para la comunicación SSH entre Citrix ADM y la instancia de Citrix ADC.

e) **Puerto HTTP**: especifique el puerto para la comunicación HTTP entre Citrix ADM y la instancia de Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El puerto HTTP predeterminado es 80. También puede especificar el puerto HTTP personalizado o no predeterminado que podría haber configurado en su instancia de Citrix ADC CPX. El puerto HTTP personalizado solo se puede utilizar para la comunicación entre Citrix ADM y Citrix ADC CPX.

f) **Puerto HTTPS**: especifique el puerto para la comunicación HTTPS entre Citrix ADM y la instancia de Citrix ADC.

> **Nota**
>
> El puerto HTTPS predeterminado es 443. También puede especificar el puerto HTTPS personalizado o no predeterminado que podría haber configurado en su instancia de Citrix ADC CPX. El puerto HTTPS personalizado solo se puede utilizar para la comunicación entre Citrix ADM y Citrix ADC CPX.

g) **Usar la configuración global para la comunicación de Citrix ADC**: Seleccione esta opción si quiere utilizar la configuración del sistema para la comunicación entre Citrix ADM y la instancia de Citrix ADC; de lo contrario, seleccione HTTP o https.

h) **Versión SNMP**: seleccione **SNMPv2 o**SNMPv3** y haga lo siguiente:

   i. Si selecciona SNMPv2, especifique el nombre de la **comunidad** para la autenticación.

   ii. Si selecciona SNMPv3, especifique el **nombre de seguridad** y el **nivel de seguridad**. Según el nivel de seguridad, seleccione **Tipo de autenticación** y **Tipo de privacidad**.

   > **Nota**
   >
   > Para Citrix ADC SDX, solo se admite **SNMPv2**.

i) **Configuración de tiempo de espera**: especifique el tiempo que debe esperar Citrix ADM antes de enviar una solicitud de conexión a la instancia de Citrix ADC tras un reinicio.

j) Seleccione **Create**.

## Agregar instancias de ADC a Citrix ADM

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde.

Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de Citrix ADC, o un intervalo de direcciones IP.

Para las instancias SD-WAN, especifique la dirección IP de cada instancia o un intervalo de direcciones IP. Tenga en cuenta que Citrix ADM solo admite las ediciones Citrix SD-WAN WO y Citrix SD-WAN PE.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

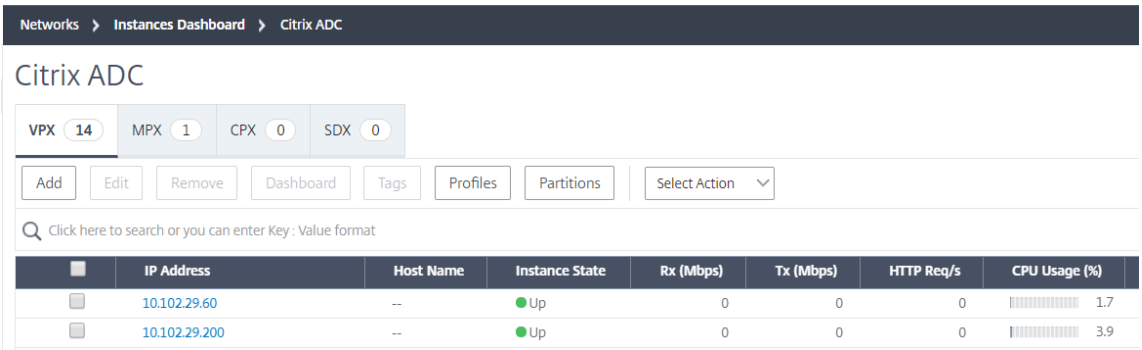
> **Nota**
>
> - Para agregar instancias de Citrix ADC configuradas en un clúster, debe especificar la dirección IP del clúster o cualquiera de los nodos individuales de la configuración del clúster. Sin embargo, en Citrix ADM, el clúster se representa únicamente mediante la dirección IP del clúster.
> - Para las instancias de Citrix ADC configuradas como un par de HA, cuando agrega una instancia, la otra instancia del par se agrega automáticamente.

Si dos servidores Citrix ADM están configurados en modo de alta disponibilidad, cuando se agrega una instancia, la fuente de tráfico es a través de la dirección IP flotante de ADM.

Cuando se agrega una instancia de datos remotos configurados con un agente local, el origen de tráfico se realiza a través del agente ADM.

**Para agregar una instancia a Citrix ADM**:

1. Inicie sesión en Citrix ADM con credenciales de administrador.
2. Vaya a**Redes**>**Instancias** > **Citrix ADC**. Seleccione el tipo de instancia que quiere agregar (por ejemplo, Citrix ADC VPX) y haga clic en**Agregar**.




3. Seleccione una de estas opciones:

   - **Escriba la dirección IP del dispositivo**: Para las instancias Citrix ADC, especifique el nombre de host o la dirección IP de cada instancia, o un rango de direcciones IP.

     Si quiere descubrir un par ADC HA mediante SNIP, asegúrese de que el modo de configuración de red independiente (INC) esté activado. Además, especifique las direcciones SNIP en el siguiente formato:

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     ```

     Por ejemplo, `10.10.10.11#10.10.10.12`

     Para las instancias SD-WAN, especifique la dirección IP de cada instancia o un intervalo de direcciones IP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Importar desde un archivo**: desde tu sistema local, sube un archivo de texto que contenga las direcciones IP de todas las instancias que quieras agregar.

4. En **Nombre de perfil**, selecciona el perfil de instancia correspondiente o crea un perfil nuevo haciendo clic en el icono +.
5. En **Sitio**, selecciona la ubicación en la que quieres agregar la instancia o crea una nueva ubicación haciendo clic en el icono **+**.
6. Haga clic en**Aceptar**para iniciar el proceso de agregar instancias a Citrix ADM.

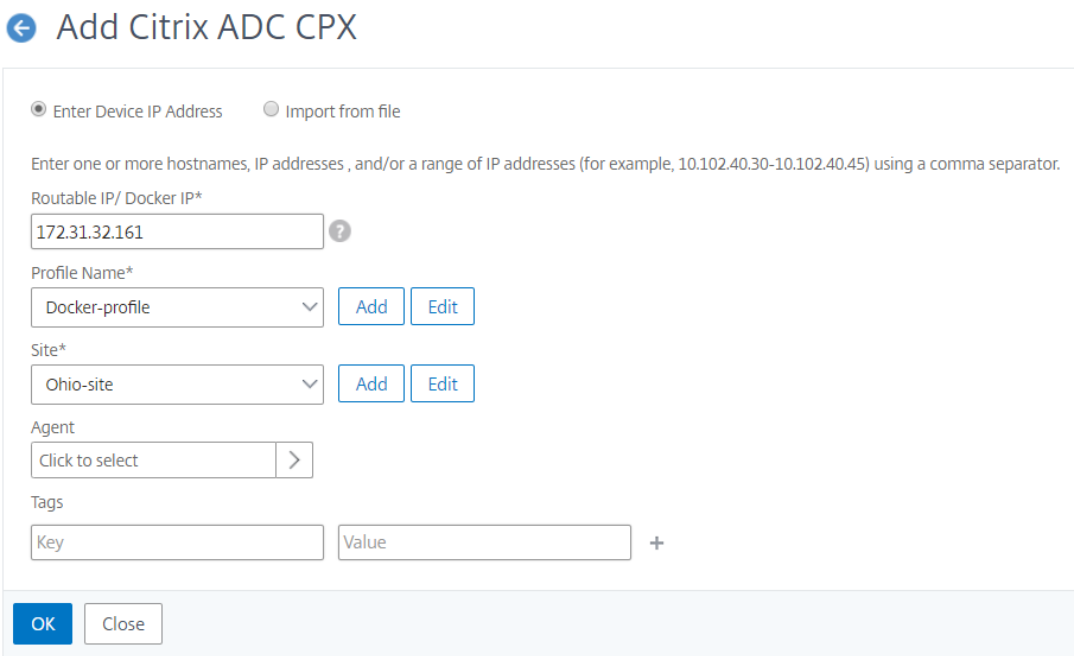
> **Nota**
>
> Si quiere volver a descubrir una instancia, vaya a **Redes** > **Instancias** > **Citrix ADC**. Seleccione el tipo de instancia (por ejemplo, VPX) y seleccione la instancia que quiere volver a descubrir y, a continuación, en la lista **Seleccionar acción**, haga clic en **Redescubrir**.

## Agregar instancias CPX de ADC a Citrix ADM

Se ha mejorado Citrix ADM para brindar soporte a las mejoras que se han realizado en las funcionalidades de CPX. La instancia CPX de Citrix ADC ahora se agrega a Citrix ADM al proporcionar una dirección IP para el CPX junto con un perfil de dispositivo. El proceso de adición de una instancia CPX ahora es similar a cómo se agregan otros tipos de ADC como VPX o MPX en ADM. Además, se ha mejorado el registro de CPX en ADM. Cuando se inicia un CPX, Citrix ADM descubre y registra automáticamente la instancia CPX. Una instancia CPX ya no se descubre a través del host Docker.

1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y haga clic en la ficha **CPX**.
2. Haga clic en **Agregar** para agregar nuevas instancias CPX en Citrix ADM.
3. Se abrirá la página **Add Citrix ADC CPX**. Introduzca los valores de los siguientes parámetros:
   a) Puede agregar instancias de CPX proporcionando la dirección IP accesible de la instancia CPX o la dirección IP del contenedor Docker donde está alojada la instancia de CPX.
   b) Seleccione el perfil de la instancia CPX.
   c) Seleccione el sitio en el que se van a implementar las instancias.
   d) Seleccione el agente.
   e) Como opción, puede introducir el par clave-valor en la instancia. Agregar par clave-valor hace que sea fácil para usted buscar la instancia más adelante.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> Para las instancias CPX de Citrix ADC, debe especificar los detalles de los puertos **HTTP, HTTPS, SSH**y **SNMP** del host al crear el perfil de instancia CPX. También puede especificar el rango de puertos que publicó el host en el campo **Puerto de inicio** y **número de puertos**.

4. Haga clic en **Aceptar**.

## Agregar una instancia independiente de Citrix ADC BLX en Citrix ADM

Una instancia independiente de Citrix ADC BLX es una instancia única que se ejecuta en el servidor host Linux dedicado.

1. Desplácese a **Redes** > **Instancias** > **NetScaler ADC**.
2. En la ficha **BLX**, haga clic en **Agregar**.
3. Seleccione la opción **Independiente** de la lista **Tipo de Instancia**.
4. En el campo **Dirección IP**, especifique la dirección IP de la instancia de BLX.
5. En el campo **Dirección IP del host**, especifique la dirección IP del servidor Linux en el que está alojada la instancia de BLX.
6. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

   Para crear un perfil, haga clic en **Agregar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Importante**
>
> Asegúrese de haber especificado el nombre de usuario host y la contraseña correctos del servidor Linux en el perfil.

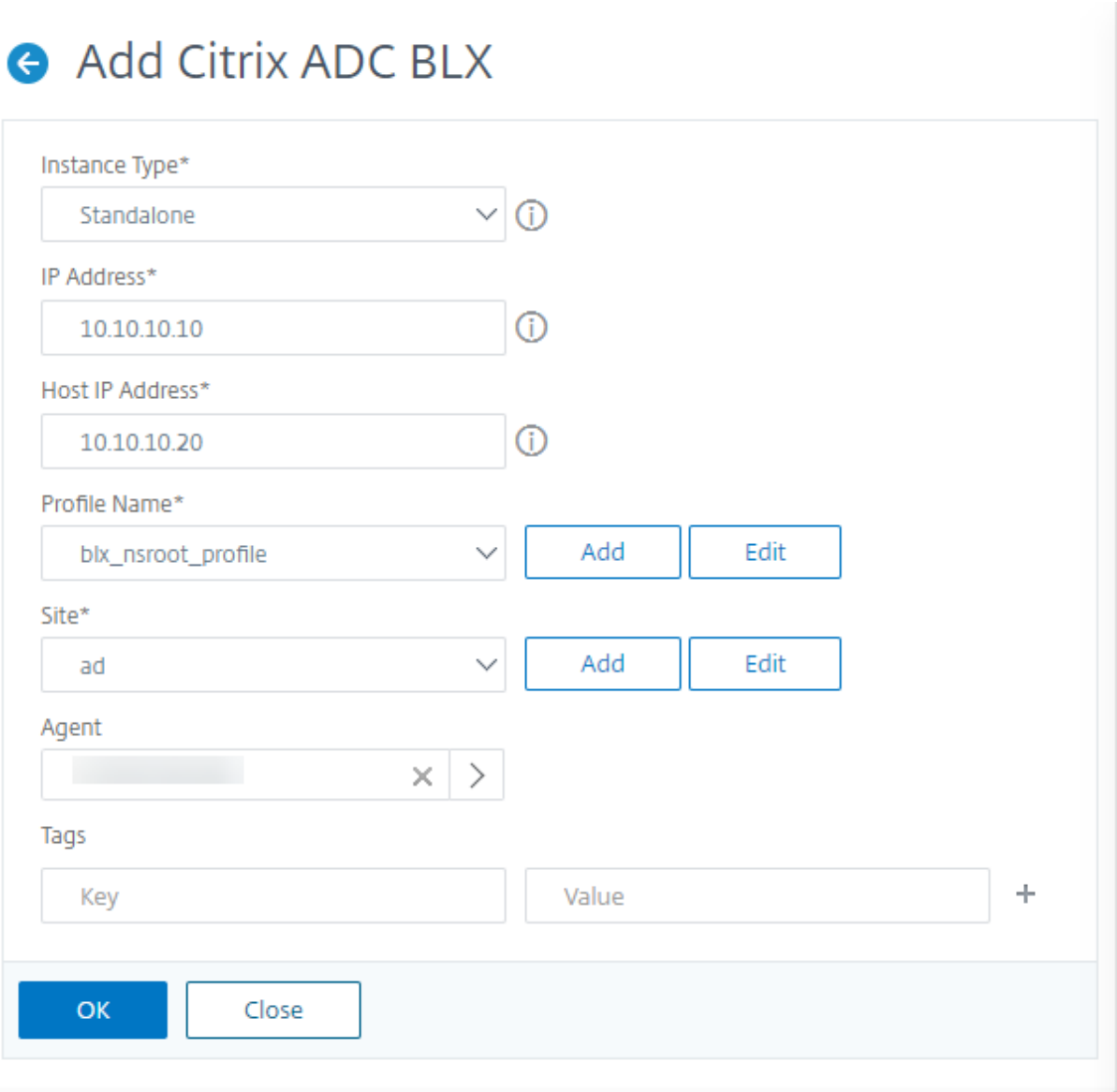
7. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

   Si quieres agregar un sitio, haga clic en **Agregar**.

8. En la lista de **agentes**, seleccione el agente Citrix ADM al que quiere asociar la instancia.

   Si solo hay un agente configurado en su Citrix ADM, ese agente se selecciona de forma predeterminada.

9. Haga clic en **Aceptar**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Agregue instancias de Citrix ADC BLX de alta disponibilidad en Citrix ADM

Las instancias de Citrix ADC BLX de alta disponibilidad que se ejecutan en diferentes servidores host Linux. Un servidor Linux no puede alojar más de una instancia de BLX.

1. En la ficha **BLX**, haga clic en **Agregar**.
2. Seleccione la opción **Alta disponibilidad** en la lista **Tipo de instancia**.
3. En el campo **Dirección IP**, especifique la dirección IP de la instancia de BLX.
4. En el campo **Dirección IP del host**, especifique la dirección IP del servidor Linux en el que está alojada la instancia de BLX.
5. En el campo **Dirección IP del mismo** nivel, especifique la dirección IP de la instancia BLX homóloga.
6. En el campo **Dirección IP del host del mismo** nivel, especifique la dirección IP del servidor Linux en el que está alojada la instancia BLX del mismo nivel.
7. En la lista **de nombres de perfil**, seleccione el perfil adecuado para una instancia de BLX o cree un perfil.

   Para crear un perfil, haga clic en **Agregar**.

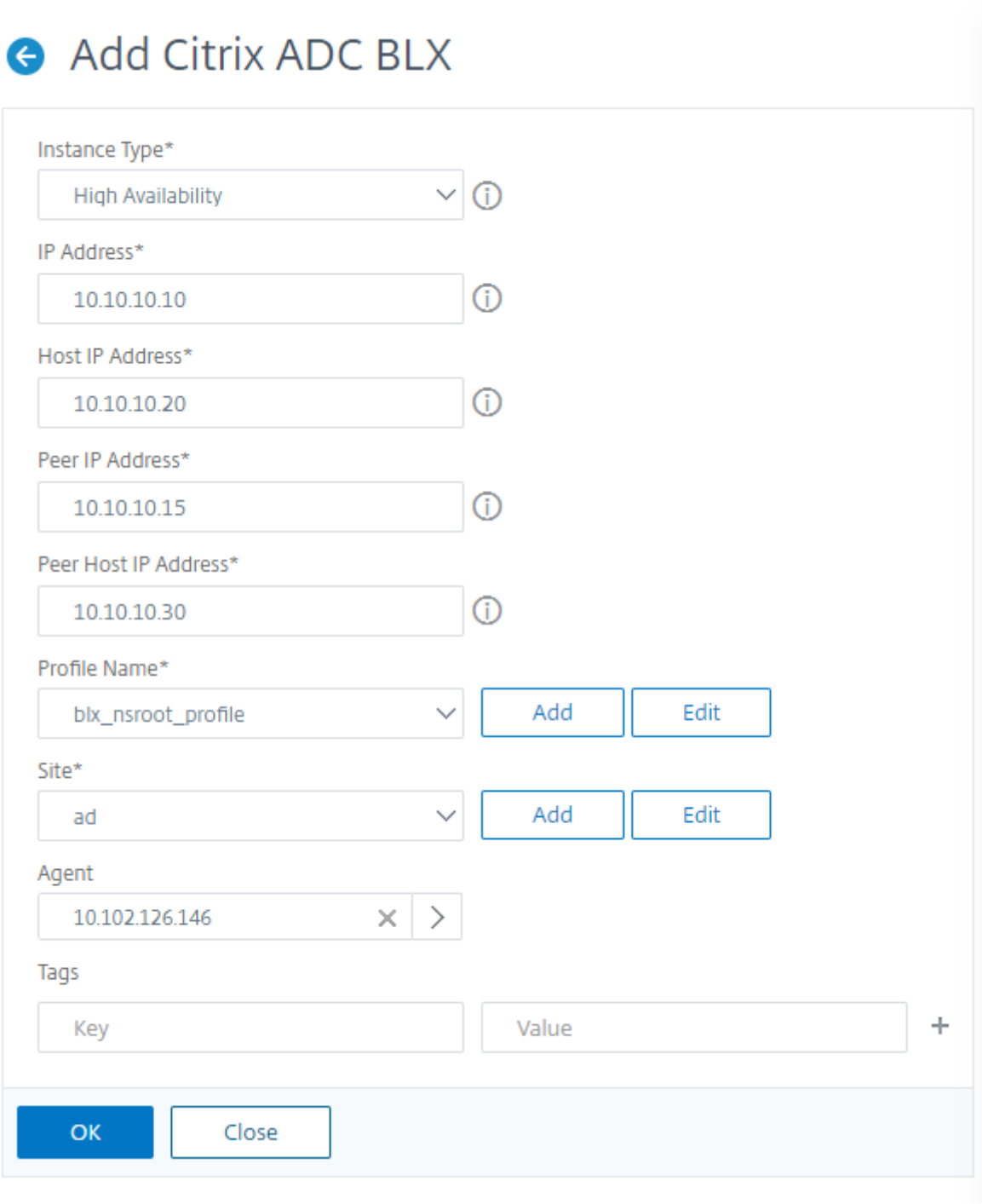
   > **Importante**
   >
   > Asegúrese de haber especificado el nombre de usuario host y la contraseña correctos del servidor Linux en el perfil.

8. En la lista de **sitios**, selecciona el sitio en el que deseas agregar una instancia.

   Si quieres agregar un sitio, haga clic en **Agregar**.
9. En la lista de **agentes**, seleccione el agente Citrix ADM al que quiere asociar la instancia.

   Si solo hay un agente configurado en su Citrix ADM, ese agente se selecciona de forma predeterminada.
10. Haga clic en **Aceptar**.

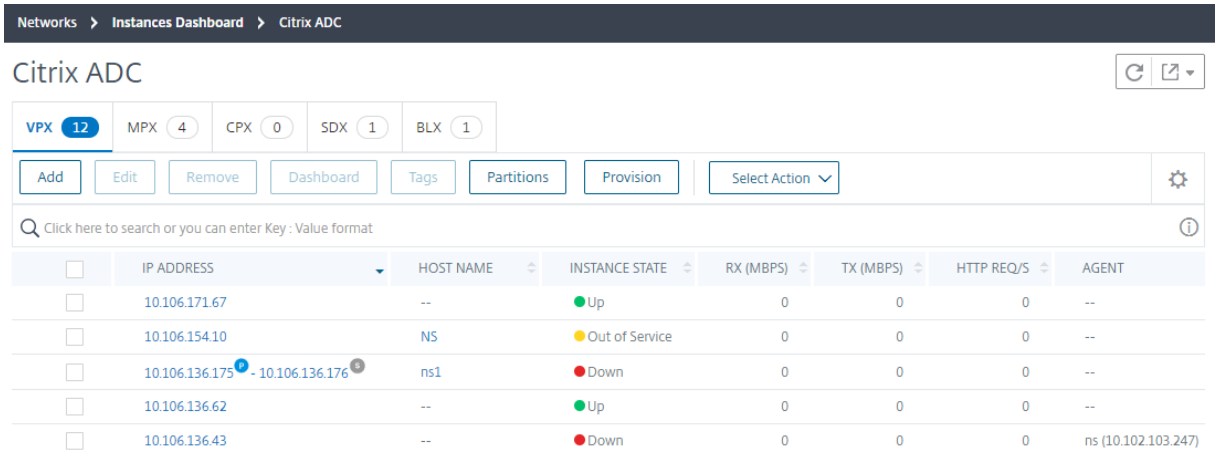
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Acceder a una GUI de instancia desde Citrix ADM

1. Vaya a **Redes > Instancias** > **Citrix ADC** .
2. Seleccione el tipo de instancia a la que quiere acceder (por ejemplo, VPX, MPX, CPX, SDX o BLX).
3. Haga clic en la dirección IP de Citrix ADC requerida o en el nombre de host.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La GUI de la instancia seleccionada aparece en una ventana emergente.

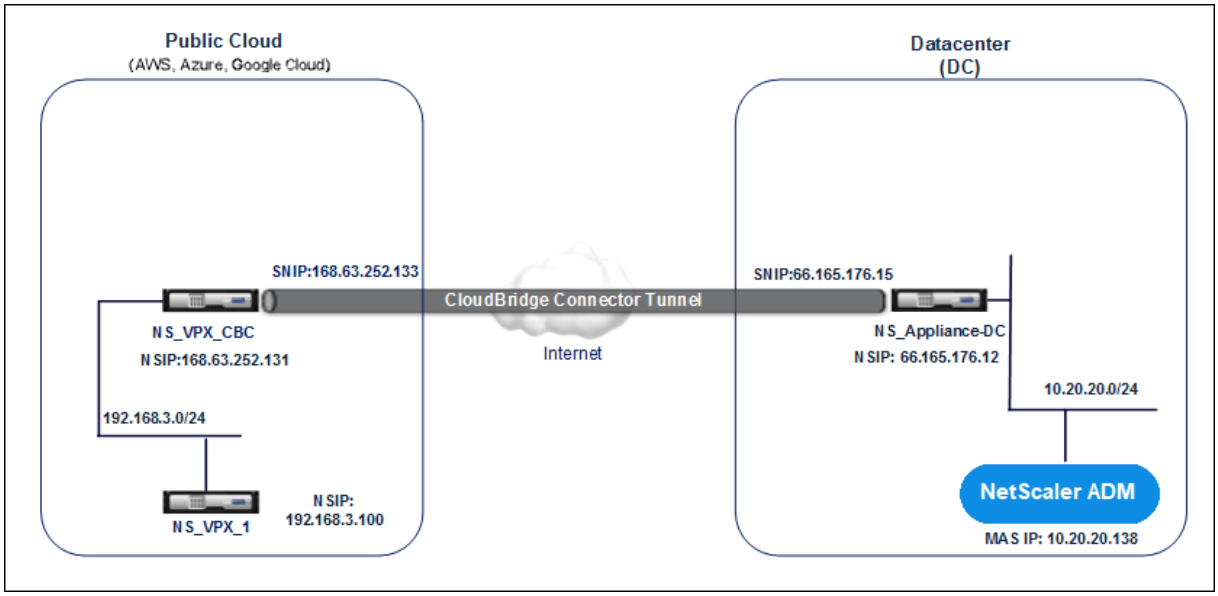
## Agregar instancias de NetScaler ADC VPX implementadas en la nube a NetScaler ADM

January 30, 2024

Puede usar Citrix ADM para administrar y supervisar las instancias de Citrix ADC VPX implementadas en una nube pública, como Amazon Web Services (AWS) o Microsoft Azure. Debe establecer conectividad de Capa 3 entre NetScaler ADM y las instancias de NetScaler ADC VPX implementadas en la nube pública. Para establecer la conectividad de capa 3, puede usar soluciones como Citrix CloudBridge Connector, Citrix SD-WAN, Direct Connect to AWS, VPN en Azure o conectores de terceros como Equinix, etc.

La siguiente topología de ejemplo utiliza la conectividad de Citrix CloudBridge Connector para la capa 3 entre NetScaler ADM y las instancias de NetScaler ADC VPX implementadas en la nube.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



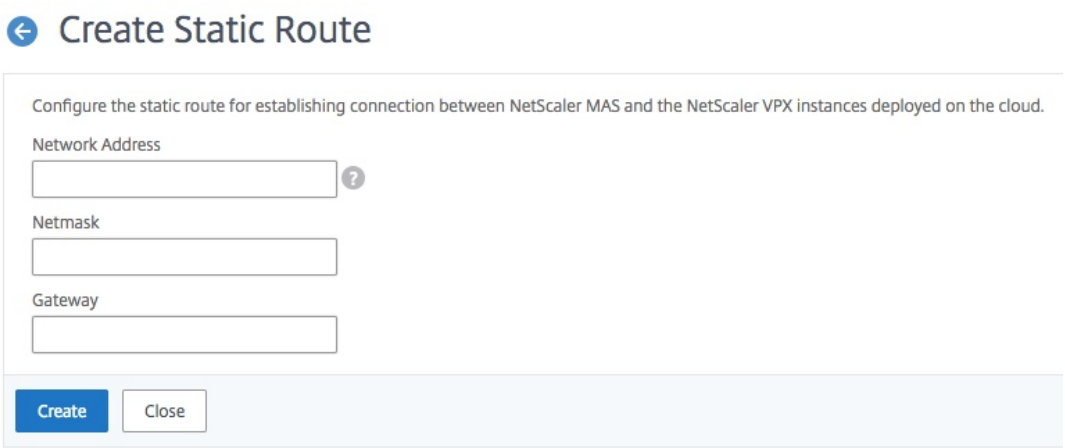

Se configura un túnel de Citrix CloudBridge Connector entre el dispositivo NetScaler ADC NS_Appliance-DC, en DC del centro de datos y el dispositivo virtual NetScaler ADC (VPX) NS_VPX_CBC en la nube pública. NS_Appliance-DC y NS_VPX_CBC permiten la comunicación entre NetScaler ADM y la instancia de NetScaler ADC VPX, NS_VPX_1, implementada en la nube pública. Una vez establecida la comunicación, puede descubrir NS_VPX_1 en NetScaler ADM.

**Para configurar esta topología**:

1. Instale, configure e inicie una instancia de NetScaler ADC VPX en la nube pública.
   - Para obtener instrucciones, consulteInstalar NetScaler ADC VPX en AWS.
   - Para obtener instrucciones, consulte Instalar NetScaler ADC VPX en Microsoft Azure.
2. Implemente y configure un dispositivo físico NetScaler ADC o aprovisionar y configurar un dispositivo virtual (VPX) de NetScaler ADC en una plataforma de virtualización del centro de datos.
   - Para obtener instrucciones, consulte Instalar una instancia de NetScaler ADC VPX en Citrix Hypervisor.
   - Para obtener instrucciones, consulte Instalar dispositivos virtuales Citrix en VMware ESXi.
   - Para obtener instrucciones, consulte Instalar dispositivos virtuales NetScaler ADC en Microsoft Hyper-V.
3. Configure Citrix CloudBridge Connector entre el centro de datos y la nube pública. Para obtener instrucciones, consulte Configuración de Citrix CloudBridge Connector.
4. Configure la ruta estática para establecer la conexión entre NetScaler ADM y las instancias de NetScaler ADC VPX implementadas en la nube, de la siguiente manera:
   a) Inicie sesión en Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Desplácese hasta **Sistema > Rutas estáticas** y haga clic en **Agregar**.




c) En el campo **Dirección de red** , introduzca la dirección de la red en la que desea establecer una ruta estática desde Citrix ADM a través del conector.

d) En el campo **Máscara** de red, introduzca la máscara de red de la red.

e) En el campo **Puerta** de enlace, introduzca la dirección de la puerta de enlace.

5. Agregue las instancias de nube de NetScaler ADC VPX al NetScaler ADM especificando el rango de direcciones IP de las instancias de NetScaler ADC VPX en la nube pública. Para obtener instrucciones detalladas, consulte Agregar instancias a NetScaler ADM.

## Administrar licencias y habilitar análisis en servidores virtuales

January 30, 2024

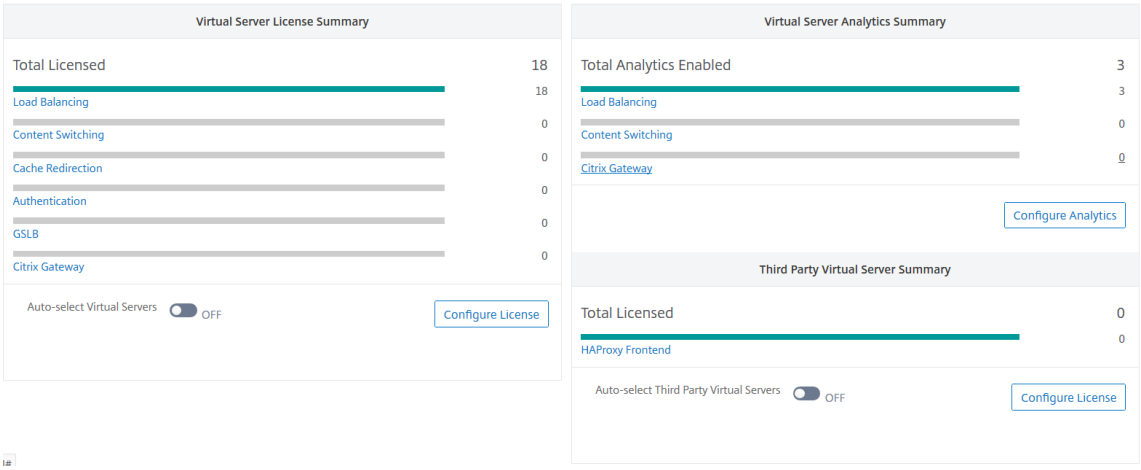
> **Nota**
>
> - La siguiente información y procedimiento para habilitar el análisis solo se aplica si la versión de Citrix ADM es **13.0 compilación 41.x** o posterior. Si la versión de Citrix ADM es anterior a **13.0 compilación 36.27**, consulte habilitar análisis.
> - De forma predeterminada, la opción **Servidores virtuales con licencia automática** está habilitada. Debe asegurarse de tener licencias suficientes para licenciar los servidores virtuales. Si tiene licencias limitadas y quiere licenciar solo los servidores virtuales selectivos según sus requisitos, inhabilite la opción **Servidores virtuales con licencia automática**. Vaya a **Sistemas > Licencias y análisis y** inhabilite la opción **Servidores virtuales con licencia automática en Asignación de licencias de servidoresvirtuales**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

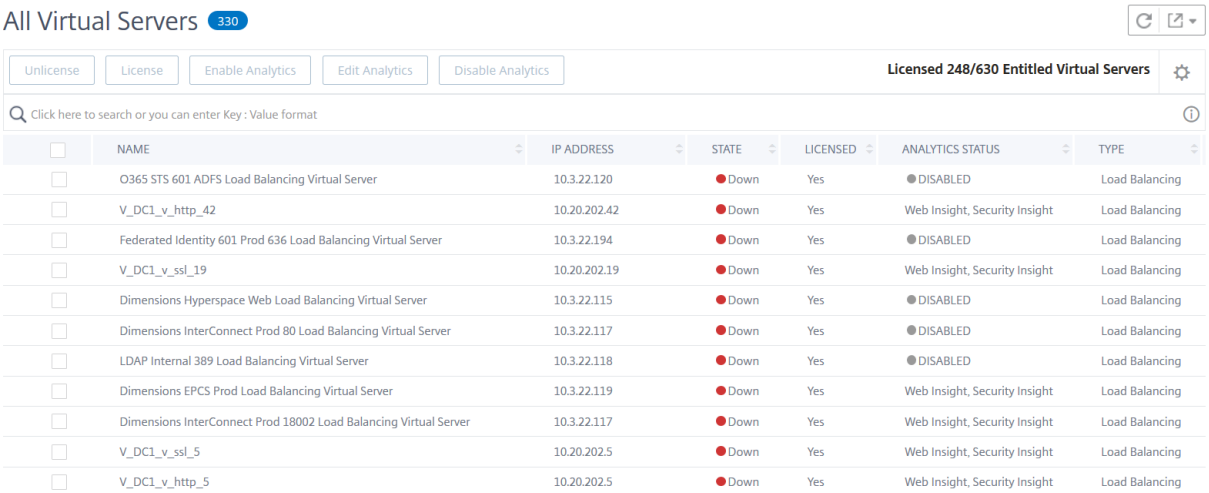
El proceso de habilitación de análisis se simplifica. Ahora puede licenciar el servidor virtual y habilitar el análisis en un único flujo de trabajo.

Vaya a **Sistema** > **Licencias y análisis** para:

- Ver el **resumen de licencia del servidor virtual**
- Ver el **resumen de análisis del servidor virtual**




Al hacer clic en **Configurar licencia** o **Configurar análisis**, aparece la página **Todos los servidores virtuales**.




En la página **Todos los servidores virtuales**, puede:

- Solicitar licencia para servidores virtuales sin licencia
- Eliminar la licencia de los servidores virtuales con licencia
- Habilite el análisis en servidores virtuales con licencia
- Modificar análisis
- Desactivar la analítica

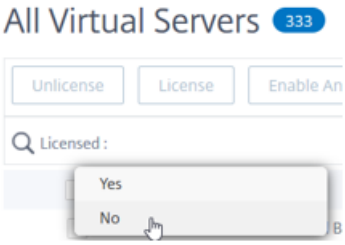
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Los servidores virtuales compatibles que permiten el análisis son el equilibrio de carga, la conmutación de contenido y Citrix Gateway.

### Administrar licencias en servidores virtuales

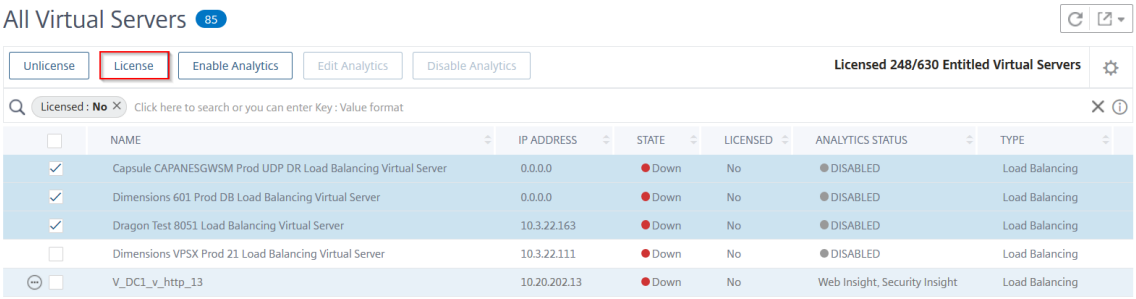
Para licenciar los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Con licencia** y seleccione **No**.




   Ahora se aplica el filtro y solo se muestran los servidores virtuales sin licencia.

2. Seleccione los servidores virtuales y, a continuación, haga clic en **Licencia**.




Para anular la licencia de los servidores virtuales, desde la página **Todos los servidores virtuales** :

1. Haga clic en la barra de búsqueda, seleccione **Licencia** y seleccione **Sí**.
2. Seleccione los servidores virtuales y haga clic en **Anular licencia**.

### Habilitar análisis

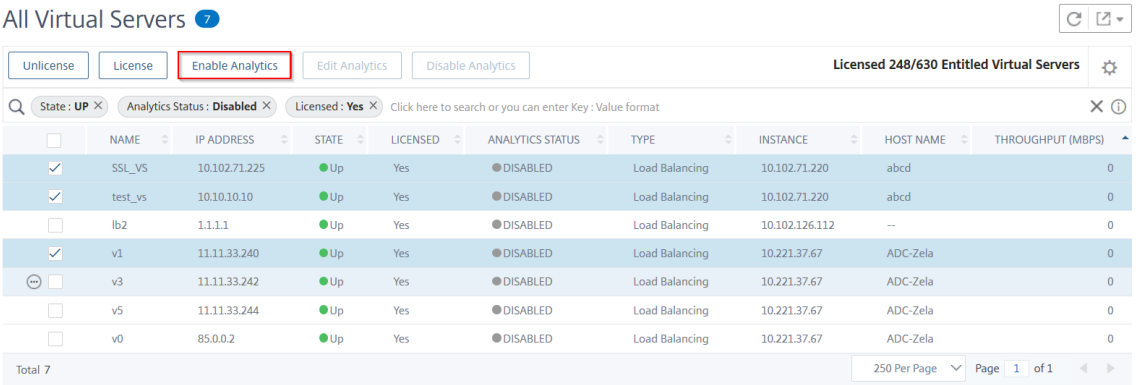
Los siguientes son los requisitos previos para habilitar el análisis de los servidores virtuales:

- Asegúrese de que los servidores virtuales tengan **licencia**
- Asegúrese de que el estado de los análisis **esté**
- Asegúrese de que los servidores virtuales estén en estado **UP**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede filtrar los resultados para identificar los servidores virtuales que se mencionan en los requisitos previos.

1. Haga clic en la barra de búsqueda, seleccione **Estado** y, a continuación, seleccione **UP**.
2. Haga clic en la barra de búsqueda, seleccione **Licencia** y, a continuación, seleccione **Sí**.
3. Haga clic en la barra de búsqueda, seleccione **Estado de análisis**y, a continuación, seleccione **Desactivado**.
4. Tras aplicar los filtros, seleccione los servidores virtuales y, a continuación, haga clic en **Habilitar análisis**.




> **Nota**
>
> Alternativamente, puede habilitar el análisis para una instancia concreta:
>
> ```
> 1.  Vaya a **Redes** > **Instancias** > **Citrix ADC** y, a
     continuación, seleccione el tipo de instancia. Por ejemplo,
      VPX.

1.  Seleccione la instancia y, en **la lista Seleccionar accióm
     n**, seleccione **Configurar análisis**

1.  En la página Configurar análisis en servidores virtuales,
     seleccione el servidor virtual y haga clic en **Habilitar
     análisis**.
> ```

5. En la ventana **Habilitar análisis**:
   a) Seleccione los tipos de información (Web Insight o Security Insight)
   b) Seleccione **Logstream** como modo de transporte

   > **Nota**
   >
   > Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

c) En **Opciones a nivel de instancia**:

- **Habilitar HTTP X-Forwarded-For**: Seleccione esta opción para identificar la dirección IP para la conexión entre el cliente y la aplicación, a través del proxy HTTP o el equilibrador de carga.
- **Citrix Gateway**: seleccione esta opción para ver los análisis de Citrix Gateway.

d) La expresión es verdadera por defecto

e) Haga clic en **OK**.

> **Nota**
>
> - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
> - Para las particiones de administración, solo se admite **Web Insight**
> - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, Citrix ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

> **Nota**
>
> Citrix ADM utiliza Citrix ADC SNIP para Logstream y NSIP para IPFIX. Si hay un firewall habilitado entre el agente Citrix ADM y la instancia de Citrix ADC, asegúrese de abrir el siguiente puerto para permitir que Citrix ADM recopile el tráfico de AppFlow:

| Modo de transporte | IP de origen | Tipo | Puerto |
|---|---|---|---|
| IPFIX | NSIP | UDP | 4739 |
| Flujo de registro | SNIP | TCP | 5557 |

### Modificar análisis

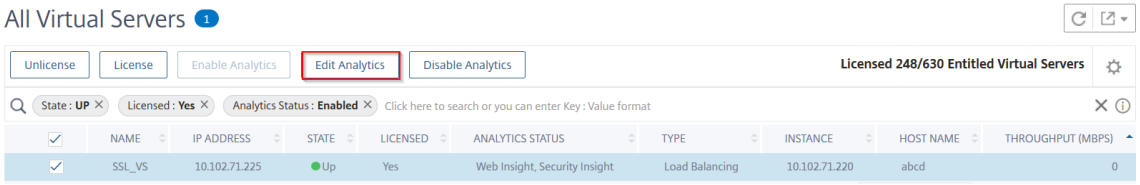
Para modificar los análisis en los servidores virtuales:

1. Seleccione los servidores virtuales

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Nota
>
> Alternativamente, también puede modificar análisis para una instancia concreta:
>
> ```
> 1.  Vaya a **Redes** > **Instancias** > **Citrix ADC** y, a continuación, seleccione el tipo de instancia. Por ejemplo, VPX.
>
> 1.  Seleccione la instancia y haga clic en **Modificar análisis**.
> ```

2. Haga clic en **Modificar análisis**




3. Modifique los parámetros que quiere aplicar en la ventana **Modificar configuración de Analytics**
4. Haga clic en **Aceptar**.

### Desactivar la analítica

Para inhabilitar los análisis en los servidores virtuales seleccionados:

1. Seleccione los servidores virtuales
2. Haga clic en **Desactivar**

Citrix ADM desactiva los análisis en los servidores virtuales seleccionados

En la siguiente tabla se describen las funciones de Citrix ADM que admite IPFIX y Logstream como modo de transporte:

| Función | IPFIX | Flujo de registro |
|---|---|---|
| Información web | • | • |
| Security Insight | • | • |
| Gateway Insight | • | • |
| HDX Insight | • | • |
| Insight SSL | No compatible | • |
| CR Insight | • | • |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Función | IPFIX | Flujo de registro |
|---|---|---|
| Reputación IP | • | • |
| AppFirewall | • | • |
| Medición del lado del | • | • |
| Syslog/Auditlog | • | • |

### Habilite el análisis en servidores virtuales para una compilación más temprana

Para habilitar el análisis en servidores virtuales para **Citrix ADM 13.0**build 36.27:

1. Vaya a **Redes** > **Instancias** > **Citrix ADC**y seleccione la instancia de Citrix ADC en la que quiere habilitar el análisis.
2. En la lista de instancias, seleccione una instancia.
3. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
4. En la Lista de aplicaciones, seleccione los servidores virtuales y haga clic en **Habilitar AppFlow**.
5. En el campo **Habilitar AppFlow**, escriba true y, en función de los análisis que desee habilitar, seleccione Security Insight o Web Insight, o ambos.

> **Nota**
>
> Citrix ADM utiliza Citrix ADC SNIP para Logstream y NSIP para IPFIX. Si hay un firewall habilitado entre Citrix ADM y la instancia de Citrix ADC, asegúrese de abrir el siguiente puerto para permitir que Citrix ADM recopile el tráfico de AppFlow:

| Modo de transporte | IP de origen | Tipo | Puerto |
|---|---|---|---|
| IPFIX | NSIP | UDP | 4739 |
| Flujo de registro | SNIP | TCP | 5557 |

- Para HDX Insight y Gateway Insight, al hacer clic en Habilitar AppFlow, debe seleccionar el servidor virtual VPN configurado en la instancia de Citrix ADC y seleccionar las casillas de verificación del protocolo ICA o HTTP en consecuencia.
- Para TCP Insight, vaya a **Sistema** > **Configuración de Analytics** > **Configurar funciones** y seleccione **Habilitar TCP Insight**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Para Video Insight, debe realizar los cambios de configuración en el dispositivo Citrix ADC. Para obtener más información sobre cómo habilitar el análisis para Video Insight, consulte Video Insight.
- Para WAN Insight:
  - Vaya a **Infraestructura > Instancias > Citrix SD-WAN WO**y seleccione el dispositivo de optimización de WAN del centro de datos.
  - En la lista **Acción**, seleccione **Habilitar Insight**.
  - Seleccione los siguientes parámetros según sea necesario:
    - Recopilación de datos geográficos para HDX Insight: comparte la dirección IP del cliente con la API Google Geo.
    - AppFlow: comienza a recopilar datos de las instancias de optimización de WAN
      - TCP y WANOpt: proporciona informes de TCP y WANOpt Insight.
      - HDX: Proporciona informes HDX Insight.
      - TCP solo para HDX: Proporciona TCP solo para los informes HDX Insight.

Puede seleccionar el modo de transporte de AppFlow a **IPFIX** o **Logstream** mientras habilita AppFlow en las instancias de Citrix ADC detectadas en Citrix ADM. Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

En la siguiente tabla se describen las funciones de Citrix ADM que admite IPFIX y Logstream como modo de transporte:

| Función | IPFIX | Flujo de registro |
|---|---|---|
| Información web | • | • |
| Security Insight | • | • |
| Gateway Insight | • | • |
| HDX Insight | • | • |
| Insight SSL | No compatible | • |
| CR Insight | • | • |
| Reputación IP | • | • |
| AppFirewall | • | • |
| Medición del lado del | • | • |
| Syslog/Auditlog | • | • |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

También puede habilitar o inhabilitar el procesamiento del tráfico de Web Insight mediante la opción Habilitar Web Insight en Citrix ADM. Si no quiere supervisar el tráfico de Web Insight, puede inhabilitar la opción. Citrix ADM no procesa el tráfico de Web Insight desde los servidores virtuales de las instancias administradas.

## Configurar servidor NTP

January 30, 2024

Puede configurar un servidor de protocolo de hora de red (NTP) en Citrix ADM para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

**Para configurar un servidor NTP en Citrix ADM**:

1. Desde la GUI de ADM, vaya a **Sistema > Administración** . En la página **Administración del sistema**, en **Configuraciones de red**, haga clic en **Servidores NTP**. A continuación, haga clic en **Agregar**.
2. En la página **Crear servidor NTP**, introduzca los siguientes detalles:
   - **Nombre del servidor/dirección IP**: Introduzca el nombre de dominio o la dirección IP del servidor NTP. El nombre o la dirección IP no se pueden cambiar después de agregar el servidor NTP.
   - **Intervalo mínimo de sondeo**: Especifique el valor mínimo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que el intervalo mínimo de sondeo sea de 64 segundos, que se puede expresar como 2^6, introduzca 6
   - **Intervalo máximo de sondeo**: Especifique el valor máximo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que el intervalo máximo de sondeo sea de 256 segundos, que se puede expresar como 2^8, introduzca 8.
   - **Identificador de clave**: introduzca el identificador de clave que se puede utilizar para la autenticación de clave simétrica con el servidor NTP. No añada un identificador de clave si decide seleccionar Autokey.
   - **Clave automática**: Seleccione **Autokey** si desea utilizar la autenticación de clave pública con el servidor NTP. No seleccione si desea agregar un identificador de clave.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Preferido**: Seleccione esta opción si desea especificar este servidor NTP como servidor preferido para la sincronización de relojes. Esto solo se aplica si hay más de un servidor configurado.

3. Haga clic en **Crear**.

**Para habilitar la sincronización NTP en NetScaler ADM:**

1. Vaya a **Sistema** > **Servidores NTP**.
2. Haga clic en **Sincronización NTP** y active la casilla de verificación **Habilitar sincronización NTP**.
3. Haga clic en **Aceptar**.

## Configurar la configuración del sistema

January 30, 2024

Antes de empezar a utilizar Citrix ADM para administrar y supervisar las instancias y aplicaciones, se recomienda configurar algunos ajustes del sistema para garantizar un rendimiento óptimo del servidor Citrix ADM.

### Configurar alarmas del sistema

Configure las alarmas del sistema para asegurarse de que conoce cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor. Para algunas categorías de alarmas, como cpuUsageHigh o memoryUsageHigh, puede establecer umbrales y definir la gravedad (como Crítica o Mayor) de cada una. Para algunas categorías, como InventoryFailed o LoginFailure, solo puede definir la gravedad. Cuando se supera el umbral de una categoría de alarma (por ejemplo, MemoryUsageHigh) o cuando se produce un evento correspondiente a la categoría de alarma (por ejemplo, LoginFailure), se graba un mensaje en el sistema y se puede ver el mensaje como un mensaje de syslog.

**Para configurar alarmas del sistema:**

1. Vaya a **Sistema > SNMP** y, a continuación, haga clic en la pestaña **Alarmas** en la esquina superior derecha.
2. Seleccione la alarma que quiere configurar y haga clic en **Modificar**.
3. En la página **Configurar alarma**, seleccione la gravedad de la alarma y establezca el umbral.
4. Para ver las alarmas que han superado el umbral o en las que se ha producido un evento, vaya a **Sistema > Auditoría** y haga clic en **Mensajes de Syslog** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Configurar notificaciones del sistema

Puede enviar notificaciones a grupos de usuarios seleccionados para diversas funciones relacionadas con el sistema. Puede configurar un servidor de notificaciones en NetScaler ADM y configurar servidores de Gateway de correo electrónico y servicio de mensajes cortos (SMS) para enviar notificaciones de correo electrónico y texto a los usuarios. La configuración de la notificación garantiza que se le notifique cualquier actividad a nivel del sistema, como el inicio de sesión del usuario o el reinicio del sistema.

**Para configurar las notificaciones del sistema:**

1. Vaya a **Sistema > Administración** . En la página **Administración del sistema**, en **Notificaciones de eventos**, haga clic en **Configurar notificación de eventos y resumen > Notificación de eventos**.
2. En la página **Configurar configuración de notificación del sistema**, seleccione la categoría o categoría de eventos generados por NetScaler ADM.
3. A continuación, configure el servidor de correo electrónico o el servidor de SMS para recibir notificaciones por correo electrónico o SMS o ambos.

## Configurar las opciones de poda del sistema

Para limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

**Para configurar la configuración de poda del**sistema :

1. Vaya a **Sistema > Administración del sistema**. En **Reproducción de datos**, haga clic en **Reproducción de datos del sistema y de la instancia**.
2. En la página **Sistema**, especifique el número de días durante los que desea conservar los datos y haga clic en **Guardar**.

## Configurar la configuración de syslog prune de la instancia

Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días después de los cuales los datos genéricos de syslog se eliminarán de NetScaler ADM.

**Para configurar los ajustes de purga del**syslog de la instancia :

1. Vaya a **Sistema > Administración > Reducción de datos** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Haga clic en **Poda de datos de sistema e instancia > Syslog**de instancia.
3. En la **página Configurar la configuración de Syslog Prune de la instancia**, especifique el número de días comprendido entre 1 y 180 en el campo Retain **Syslog Generic** Data.
4. Haga clic en **Guardar**.

## Configurar las opciones de poda del evento de instancia

Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos del servidor NetScaler ADM, puede especificar el intervalo durante el que quiere que NetScaler ADM conserve los datos de informes de red, los eventos, los registros de auditoría y los registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00:00 horas).

**Para configurar los ajustes de poda de**eventos de instancia :

1. Vaya a **Sistema > Administración** .
2. En la página **Administración del sistema**, en **Poda de datos, haga clic en Podade datos del sistema y de la instancia**.
3. En la página **de eliminación de datos**, haga clic en **Eventos de instancia**.
4. En el campo **Datos que conservar (días)** , introduzca el intervalo de tiempo, en días, durante el que desea conservar los datos en el servidor Citrix ADM y haga clic en **Guardar**.

## Configurar las opciones de copia de seguridad del sistema

NetScaler ADM realiza automáticamente una copia de seguridad del sistema todos los días a las 00:30 horas. De forma predeterminada, guarda tres archivos de copia de seguridad. Es posible que desee conservar un mayor número de copias de seguridad del sistema. También puede cifrar el archivo de respaldo. También puede optar por guardar la copia de seguridad en un servidor externo.

**Para configurar las opciones de copia de seguridad del sistema:**

1. Vaya a **Sistema > Administración** .
2. En **Copia de seguridad**, haga clic en **Configurar copia de seguridad del sistema y de la instancia**.
3. Haga clic en **Sistema** y, en la página **Configurar la configuración de respaldo del sistema**, especifique los valores requeridos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Configurar las opciones de copia de seguridad de instancia

Si hace una copia de seguridad del estado actual de una instancia de Citrix ADC, puede utilizar los archivos de copia de seguridad para restaurar la estabilidad si la instancia se vuelve inestable. Hacerlo es especialmente importante antes de realizar una actualización. De forma predeterminada, se realiza una copia de seguridad cada 12 horas y se conservan tres archivos de respaldo en el sistema.

**Para configurar las opciones de copia de seguridad de instancias**:

1. Vaya a **Sistema > Administración** .
2. En **Copia de seguridad**, haga clic en **Configurar copia de seguridad del sistema y de la instancia**.
3. Haga clic en **Instancia**, en **Configurar la configuración de copia de seguridad de la instancia**, y especifique los valores requeridos.

### Habilitar o inhabilitar funciones de ADM

Como administrador, puede habilitar o deshabilitar las siguientes funciones en la página **Sistema > Administración > Funciones configurables** :

- **Failover** del agente: La conmutación por error del agente puede producirse en un sitio que tiene dos o más agentes activos. Cuando un agente se vuelve inactivo (estado DOWN) en el sitio, el servicio NetScaler ADM redistribuye las instancias ADC del agente inactivo con otros agentes activos. Para obtener más información, consulte Configurar agentes locales para la implementación en varios sitios.
- **Función de red de sondeo** de entidad: Una entidad es una directiva, un servidor virtual, un servicio o una acción asociada a una instancia de ADC. De forma predeterminada, NetScaler ADM sondea automáticamente las entidades de función de red configuradas cada 60 minutos. Para obtener más información, consulte Descripción general de sondeos.
- **Copia de seguridad de instancia: Realice** una copia de seguridad del estado actual de una instancia de NetScaler ADC y, posteriormente, utilice los archivos de copia de seguridad para restaurar la instancia de ADC al mismo estado. Para obtener más información, consulte Realizar copias de seguridad y restaurar instancias de NetScaler ADC.
- **Auditoría de configuración de instancias**: Supervise los cambios de configuración en las instancias administradas de NetScaler ADC, solucione los errores de configuración y recupere las configuraciones no guardadas. Para obtener más información, consulte Crear plantillas de auditoría.
- **Eventos de instancia**: Los eventos representan ocurrencias de eventos o errores en una instancia de NetScaler ADC administrada. Los eventos recibidos en Citrix ADM se muestran en la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

página **Resumen de eventos** ( **Redes > Eventos** ) y todos los eventos activos se muestran en la página Mensajes de eventos ( **Redes > Eventos > Mensajes** de eventos ). Para obtener más información, consulte Eventos.

- **Informes de red de instancias**: Puede generar informes para instancias a nivel global. Además, para entidades como los servidores virtuales y las interfaces de red. Para obtener más información, consulte Informes de red.
- **Certificados SSL de instancia**: NetScaler ADM proporciona una vista centralizada de los certificados SSL instalados en todas las instancias administradas de NetScaler ADC. Para obtener más información, consulte Panel de control SSL.
- **Syslog de instancias**: Puede supervisar los eventos syslog generados en sus instancias NetScaler ADC si ha configurado el dispositivo para redirigir todos los mensajes syslog a NetScaler ADM.

Para habilitar una función, lleve a cabo los siguientes pasos:

1. Seleccione la función de la lista que quiere habilitar.
2. Haga clic en **Activar**.

> **Importante**
>
> Si una función está inhabilitada, el usuario no puede realizar las operaciones asociadas a esa función.

## Integre Citrix ADM con la instancia de ServiceNow

January 30, 2024

Cuando quiera habilitar las notificaciones de ServiceNow para los eventos de Citrix ADC y ADM, integre Citrix ADM con la instancia de ServiceNow. Esta integración utiliza el conector ITSM de Citrix para comunicarse entre Citrix ADM y la instancia de ServiceNow.

La integración de ServiceNow con ADM utiliza el servicio de adaptador ITSM para la autenticación basada en tokens. Para hacerlo, crea una instancia de punto final en ServiceNow. Para obtener más información, consulte Cómo funciona el adaptador ITSM.

Para conectar su implementación local de ADM con un adaptador ITSM, asegúrese de configurar la identidad del cliente. Para obtener más información, consulte Configurar la identidad del cliente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

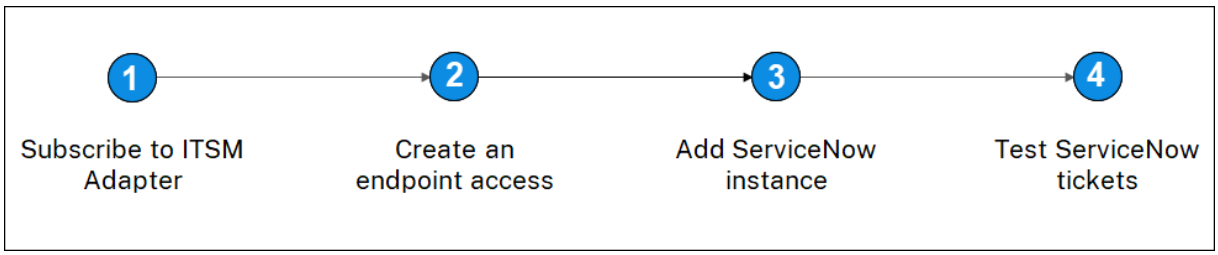
## Requisitos previos

Antes de integrar ADM con ServiceNow, asegúrese de lo siguiente:

1. Inscríbase en Citrix Cloud. Asegúrese de tener acceso para administrar los administradores de Citrix Cloud. Para obtener más información, consulte Administrar administradores de Citrix Cloud.

## ¿Cómo integrar ADM con ServiceNow?

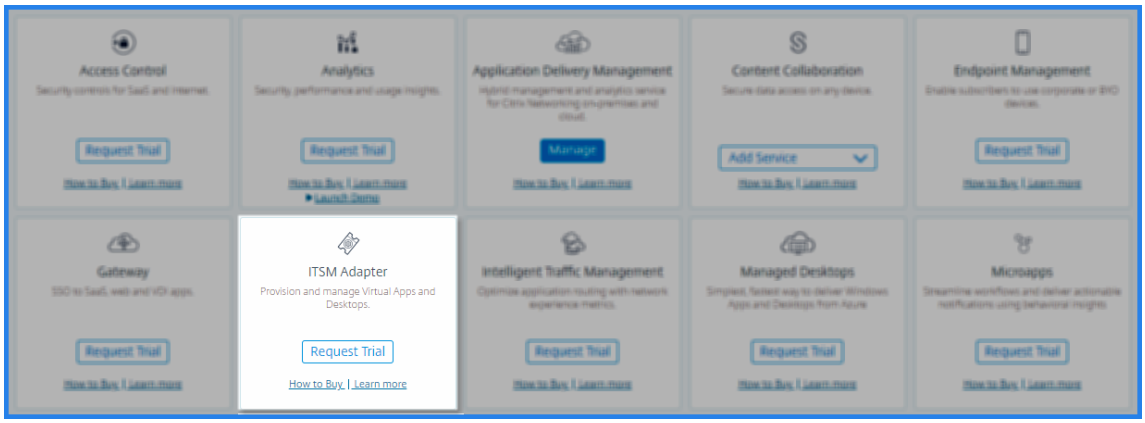
Realice los siguientes pasos para integrar Citrix ADM con ServiceNow mediante el conector ITSM:




1. Suscríbase al servicio Adaptador ITSM en Citrix Cloud.
2. Crea un acceso de punto final en la instancia de ServiceNow.
3. Agregue una instancia de ServiceNow.
4. Pruebe la generación automática de tíquets de ServiceNow en ADM.

### Paso 1: Suscríbase al servicio de adaptador ITSM en Citrix Cloud

1. En el icono **Adaptador ITSM**, haga clic en **Solicitar prueba**.

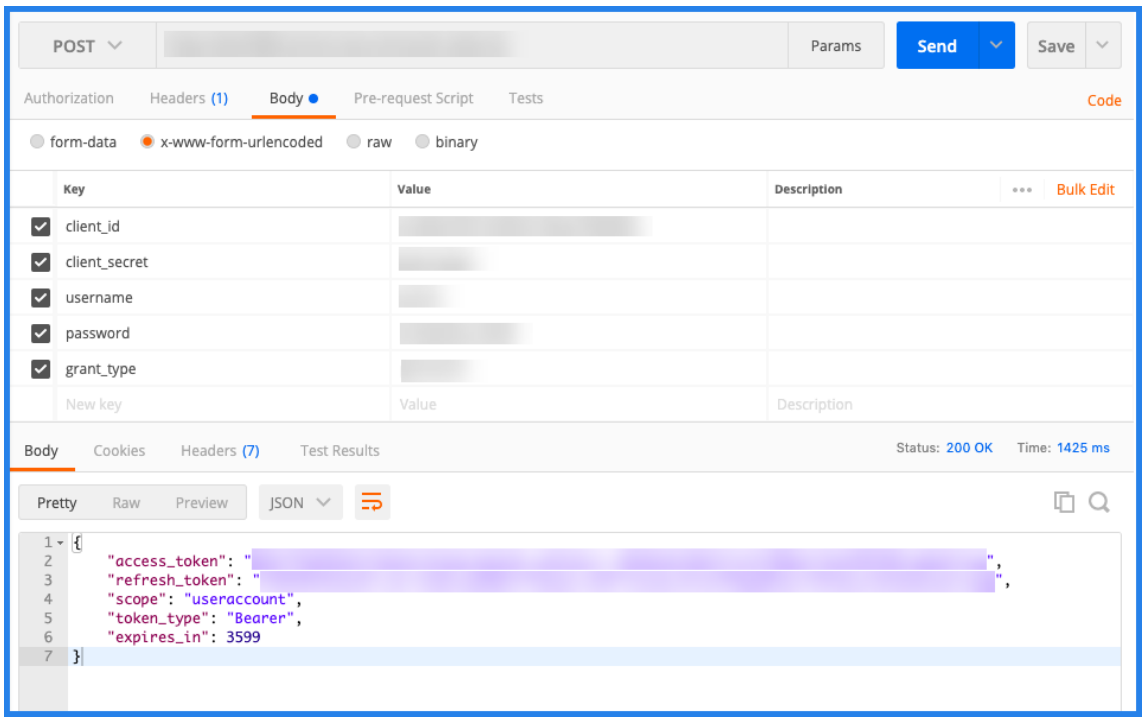



2. Desplácese hasta **Identity Access and Management** > **API Access** y anote la información de **Client ID** y **Client Secret**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Paso 2: crear un acceso de punto final en la instancia de ServiceNow**

1. Inicie sesión en su instancia de ServiceNow con credenciales de administrador.
2. Vaya a la tienda de ServiceNow. Descargue e instale el **conector ITSM de Citrix**.
3. En el panel **Citrix ITSM Connector**, seleccione **Inicio** y, a continuación, haga clic en **Autenticar**. Escriba el ID de cliente y el secreto que ha anotado en Citrix Cloud.
4. Pruebe la conexión.
5. Guarde la configuración. Aparece un acuse de recibo de ServiceNow que indica que la conexión está activa.
6. Cree un endpoint para acceder a una instancia de ServiceNow. Consulte Crear un punto de enlace para que los clientes accedan a la instancia.
7. Obtenga los tokens de acceso y actualización utilizando el ID de cliente y el secreto de cliente. Consulte Tokens de OAuth.

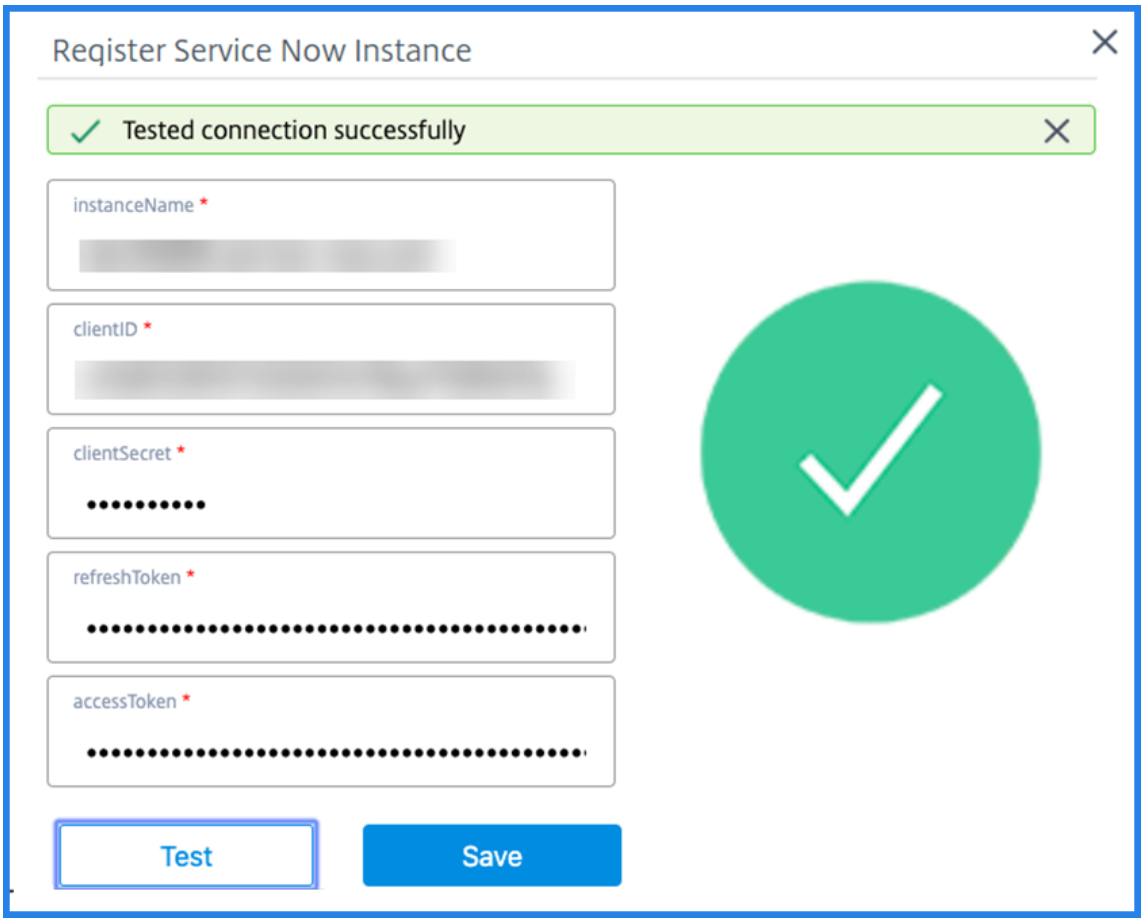



**Paso 3: Agregar una instancia de ServiceNow**

1. En la ficha **Administrar**, seleccione Agregar instancia de ServiceNow.
2. Especifique el **nombre de la instancia**, el **ID del cliente, el secreto**del cliente, el**token de actualización**y el**token de acceso**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Haga clic en **Test**.




La instancia de ServiceNow ahora está conectada al servicio ITSM Adapter.

4. Después de probar correctamente la conexión, haga clic en **Guardar** para agregar una instancia de ServiceNow.

**Paso 4: Probar la generación automática de tíquets de ServiceNow en ADM**

1. Inicie sesión en Citrix ADM.
2. Vaya a **Cuenta > Notificaciones** y selecciona **ServiceNow**.
3. Seleccione el perfil ServiceNow de la lista.
4. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

   Si quiere ver los tíquets de ServiceNow en la GUI de Citrix ADM, seleccione **Tíquets de ServiceNow**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Configurar las notificaciones de ServiceNow en ADM

Después de registrar la instancia de ServiceNow en el adaptador ITSM, puede configurar notificaciones de ServiceNow para los siguientes eventos en la GUI de Citrix ADM:

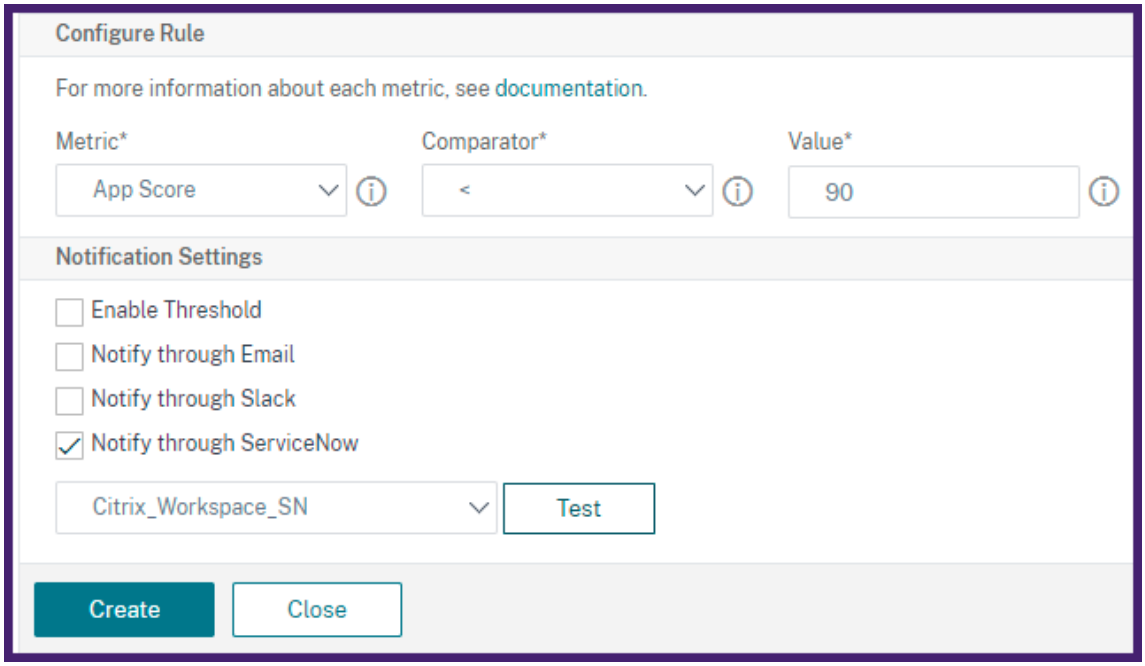
> **Importante**
>
> Esta función es compatible con ServiceNow Cloud.

- **Eventos de Citrix ADC**: Citrix ADM puede generar los incidentes de ServiceNow para el conjunto seleccionado de eventos de Citrix ADC a partir de instancias de Citrix ADC administradas seleccionadas.

  Para enviar notificaciones de ServiceNow para eventos de Citrix ADC desde las instancias administradas, debe configurar una regla de evento y asignar la acción de regla como **Enviar notificaciones de ServiceNow**.

  Cree una regla de evento en ADM navegando a **Redes** > **Eventos** > **Reglas**. Para obtener más información, consulte Enviar notificaciones de ServiceNow.

- **Análisis de aplicaciones**: Citrix ADM puede generar incidentes de ServiceNow para las aplicaciones que sobrepasen el umbral especificado.




  En este ejemplo, se genera un incidente de ServiceNow cuando la puntuación de aplicaciones de la aplicación cae por debajo de 90.

- **Los eventos del certificado SSL y de la licencia ADM**: Citrix ADM puede generar los incidentes de ServiceNow para los eventos de caducidad del certificado SSL y de caducidad de la licencia ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para enviar notificaciones de ServiceNow sobre la caducidad de un certificado SSL, consulte Caducidad del certificado SSL.

Para enviar notificaciones de ServiceNow sobre la caducidad de una licencia ADM, consulte Caducidad de la licencia de Citrix ADM.

## Exportar o programar informes de exportación

January 30, 2024

En Citrix ADM, puede exportar un informe completo para la función Citrix ADM seleccionada. Este informe proporciona una visión general de la asignación entre las instancias, las particiones y los detalles correspondientes.

Citrix ADM muestra informes de exportación programados específicos de funciones bajo funciones de ADM individuales, que puede ver, modificar o eliminar. Por ejemplo, para ver los informes de exportación de instancias de Citrix ADC, vaya a **Red > Instancias > Citrix ADC** y haga clic en el icono de exportación. Puede exportar estos informes en formato PDF, JPEG, PNG y CSV.

En **Exportar informes**, puede realizar las siguientes acciones:

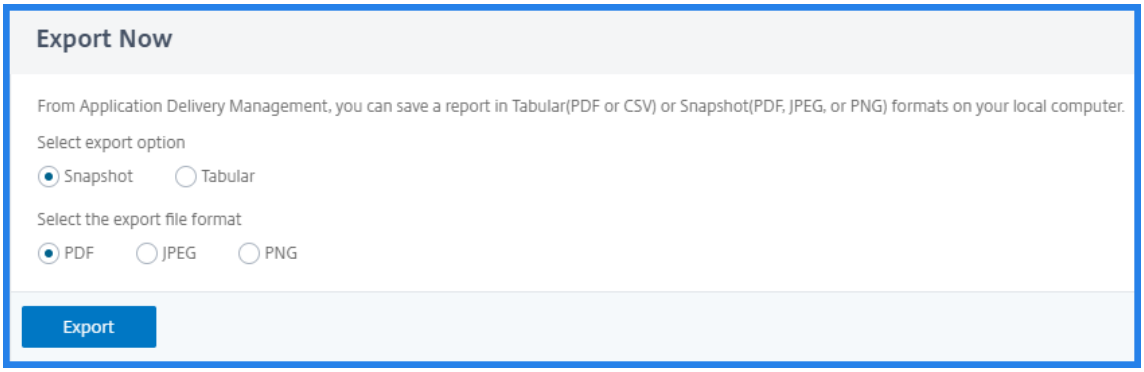
- Exportar un informe a un equipo local
- Programar informes de exportación
- Ver, modificar o eliminar los informes de exportación programados

### Exportar un informe

Para exportar un informe del ADM al equipo local, realice los siguientes pasos:

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.
2. Seleccione **Exportar ahora**.
3. Seleccione una de las siguientes opciones de exportación:
    - **Instantánea**: Esta opción exporta informes ADM como una instantánea.
    - **Tabular**: Esta opción exporta informes ADM en formato tabular. También puede elegir cuántos registros de datos exportar en formato tabular

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



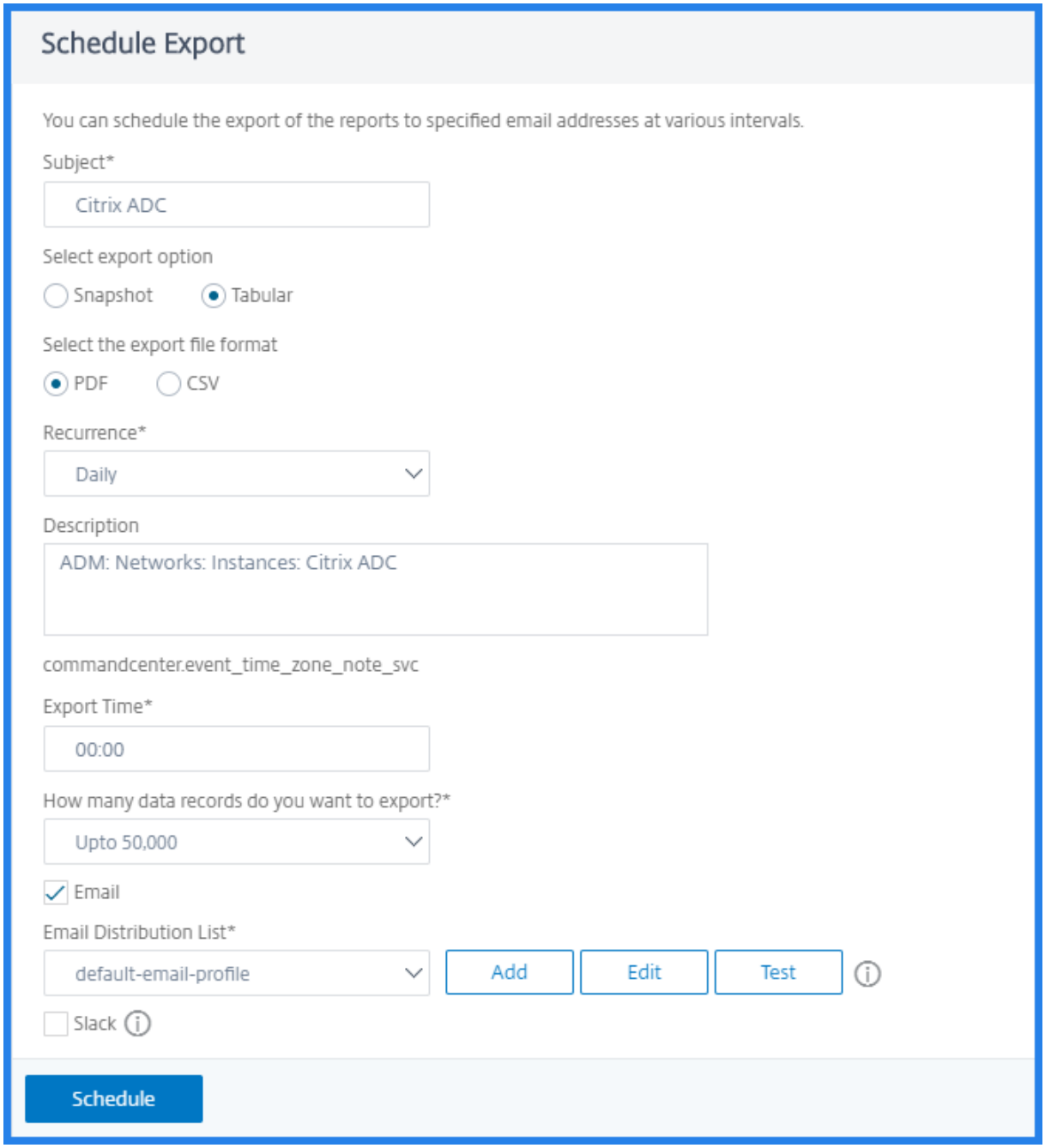

4. Seleccione el formato de archivo que quiere guardar el informe en el equipo local.
5. Haga clic en **Exportar**.

## Programar informe de exportación

Para programar el informe de exportación a intervalos regulares, especifique el intervalo de recurrencia. Citrix ADM envía el informe exportado al perfil de correo electrónico o de Slack configurado.

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.
2. Seleccione **Programar exportación** y especifique lo siguiente:
   - **Asunto**: De forma predeterminada, este campo rellena automáticamente el nombre de la función seleccionada. Sin embargo, puede reescribirlo con un título significativo.
   - **Opción Exportar** - Exportar informes ADM en una instantánea o un formato tabular. También puede elegir cuántos registros de datos exportar en formato tabular
   - **Formato**: Seleccione el formato de archivo que quiere recibir el informe en el perfil de correo electrónico o slack configurado.
   - **Recurrencia**: Seleccione **Diaria**, **Semanal**o **Mensual** de la lista.
   - **Descripción**: Especifique la descripción significativa de un informe.
   - **Hora de exportación**: Especifique a qué hora quiere exportar el informe.
   - **Correo electrónico**: A ctive la casilla de verificación y seleccione el perfil en el cuadro de lista. Si quiere agregar un perfil, haga clic en **Agregar**.
   - **Slack**: Seleccione la casilla de verificación y selecciona el perfil en el cuadro de lista. Si quiere agregar un perfil, haga clic en **Agregar**.
3. Haga clic en **Programar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Ver y modificar los informes de exportación programados

Para ver los informes de exportación, realice lo siguiente:

1. Haga clic en el icono de exportación situado en la esquina superior derecha de la página.

   La página **Exportar informe** muestra todos los informes de exportación específicos de cada función.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Seleccione el informe que quiere modificar y haga clic en **Modificar**.

## Actualizaciones

January 30, 2024

Cada versión de Citrix ADM ofrece funciones nuevas y actualizadas con mayor funcionalidad. Citrix recomienda actualizar Citrix ADM a la versión más reciente para aprovechar las nuevas funciones y correcciones de errores. En las notas de la versión que acompañan a cada anuncio de lanzamiento se incluye una lista completa de las mejoras, los problemas conocidos y las correcciones de errores. También es importante comprender el marco de licencias y los tipos de licencias que se pueden utilizar antes de comenzar a actualizar. Para obtener información sobre licencias de Citrix ADM, consulteLicencias.

La información de la ruta de actualización también está disponible en la Guía de actualización de Citrix.

### Antes de actualizar la versión

Descargue el paquete de actualización de la página de descargas de Citrix ADM y siga las instrucciones de este artículo para actualizar el sistema a la versión 13.0 más reciente. Una vez que comienza el proceso de actualización, ADM se reinicia y las conexiones existentes finalizan y vuelven a conectarse cuando finaliza la actualización. La configuración existente se conserva, pero Citrix ADM no procesa ningún dato hasta que la actualización se complete correctamente.

> **Importante**
>
> La versión y compilación de Citrix ADM deben ser **iguales o superiores a** la versión y compilación de Citrix ADC. Por ejemplo, si ha instalado Citrix ADM 12.1 compilación 50.39, asegúrese de haber instalado Citrix ADC 12.1 compilación 50.28/50.31 o anterior.

**Puntos a tener en cuenta antes de actualizar a 13.0**:

- Si actualiza desde la versión 11.1 o 12.0 56.x y versiones anteriores, realice los siguientes pasos:
  1. Actualice de la versión existente a 12.0 compilación 57.24.
  2. Actualice a la última versión de la versión 12.1.
  3. Actualice a la versión 13.0.
- Si actualiza desde 12.0 compilación 57.24 y superior, primero actualice a 12.1 y luego a 13.0.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Si actualiza desde 12.1, puede actualizar directamente a 13.0.
- Si actualiza a 13.0 67.xx y versiones posteriores, primero actualice a 13.0 64.xx y luego a 13.0 67.xx y posteriores, para una mejor experiencia del usuario.

#### Puntos importantes a tener en cuenta antes de actualizar a 13.0 67.xx y posteriores

Al actualizar el software ADM a la versión 13.0 67.xx y posterior, la base de datos ADM también se migra. Esta migración de datos se produce porque ADM ahora utiliza PostgreSQL versión 10.11.

> **Nota**
>
> No se admite la reclasificación del software ADM. No intente rebajar de categoría.

**Precauciones recomendadas**:

- Tome una instantánea del servidor Citrix ADM si está actualizando a 13.0 67.xx y versiones posteriores.
- Realice una copia de seguridad del servidor Citrix ADM antes de actualizar.
- Después de la actualización, es posible que deba restablecer las conexiones entre el servidor Citrix ADM y las instancias administradas. Un mensaje de confirmación le avisa de que las conexiones pueden fallar si continúa.
- Para los servidores de Citrix ADM en configuración de alta disponibilidad, al actualizar la versión, no realice ningún cambio de configuración en ninguno de los nodos.

  > **Advertencia**
  >
  > No actualice el explorador hasta que el proceso de actualización se haya completado correctamente. Compruebe la GUI para conocer el tiempo aproximado para completar la actualización.

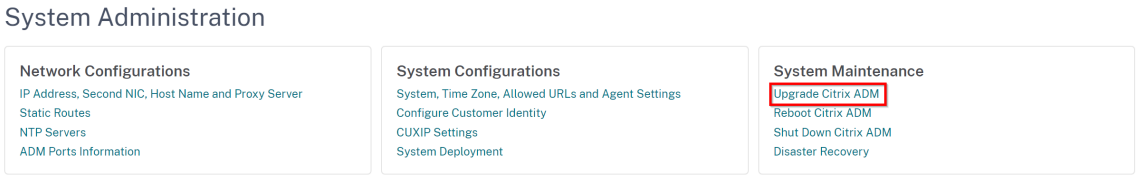
- Después de la actualización, el nodo activo puede cambiar en un par de alta disponibilidad.

### Actualizar un único servidor Citrix ADM

#### Para actualizar un único servidor Citrix ADM:

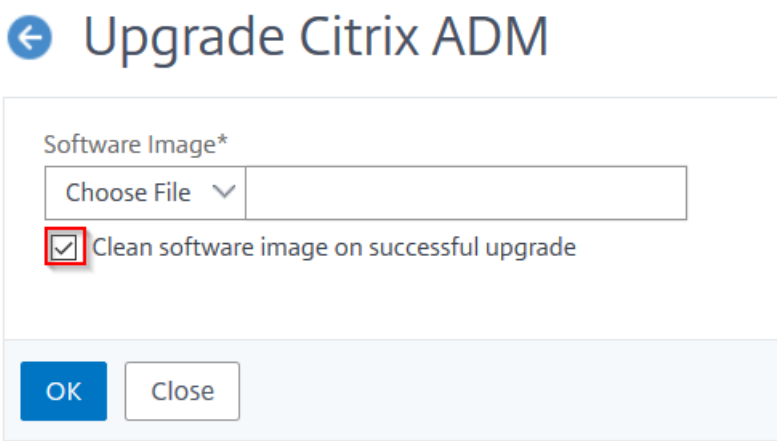
1. Inicie sesión en Citrix ADM con credenciales de administrador.
2. Vaya a **Sistema**>**Administración del sistema**. En el subencabezado **Administración del sistema**, haga clic en **Actualizar Citrix ADM**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



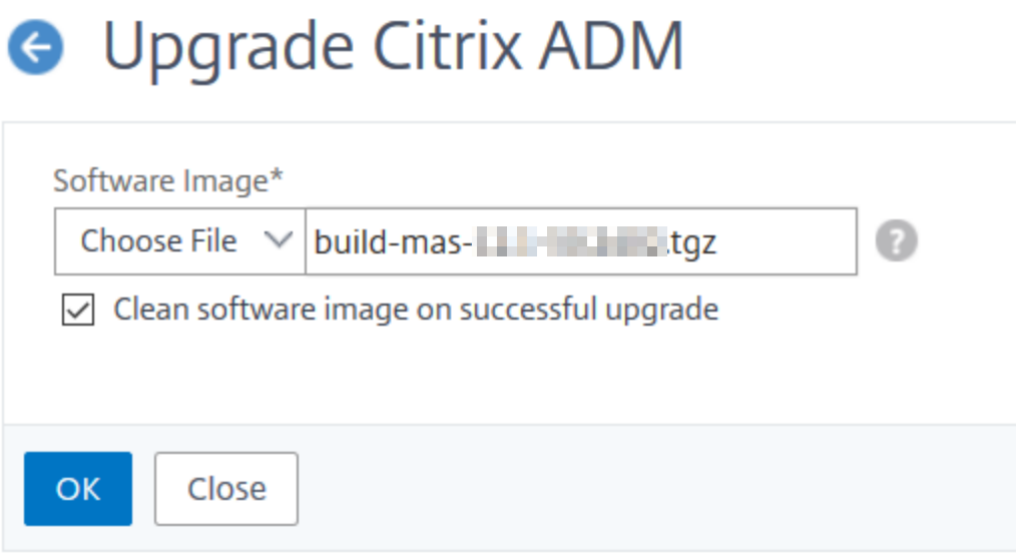

3. En la página **Actualizar Citrix ADM**, marque la casilla **Limpiar imagen de software en una actualización correcta** para eliminar archivos de imagen después de la actualización. Al seleccionar esta opción, se quitan automáticamente los archivos de imagen Citrix ADM tras la actualización.

> **Nota**
>
> Esta opción está seleccionada de forma predeterminada. Si no activa esta casilla de verificación antes de iniciar el proceso de actualización, debe eliminar manualmente las imágenes.




4. A continuación, puede cargar un nuevo archivo de imagen seleccionando **Local** (su equipo local) o **Dispositivo**. El archivo de compilación debe estar presente en el dispositivo virtual Citrix ADM.

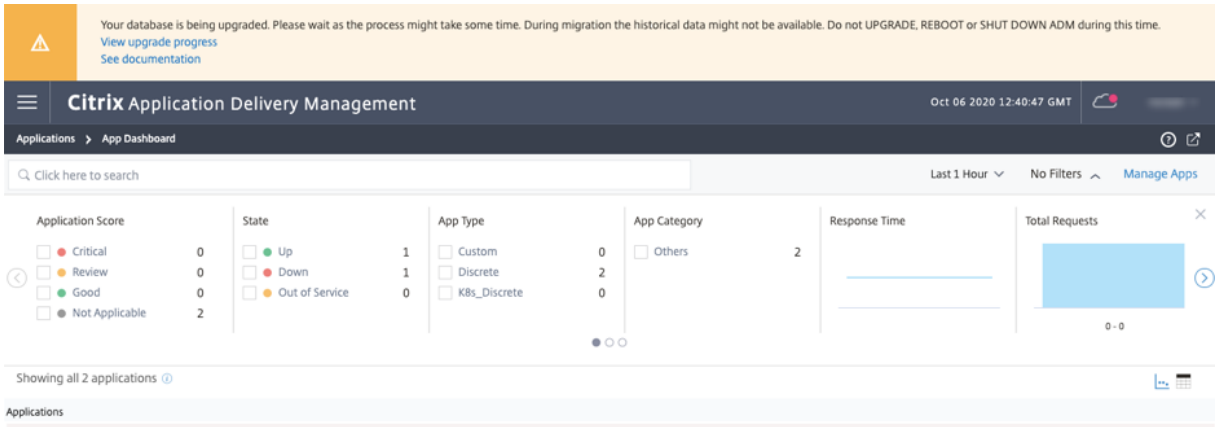
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Haga clic en **Aceptar**.
   Aparece el cuadro de diálogo Confirmar. Haga clic en **Sí**.

   Se inicia el proceso de actualización.

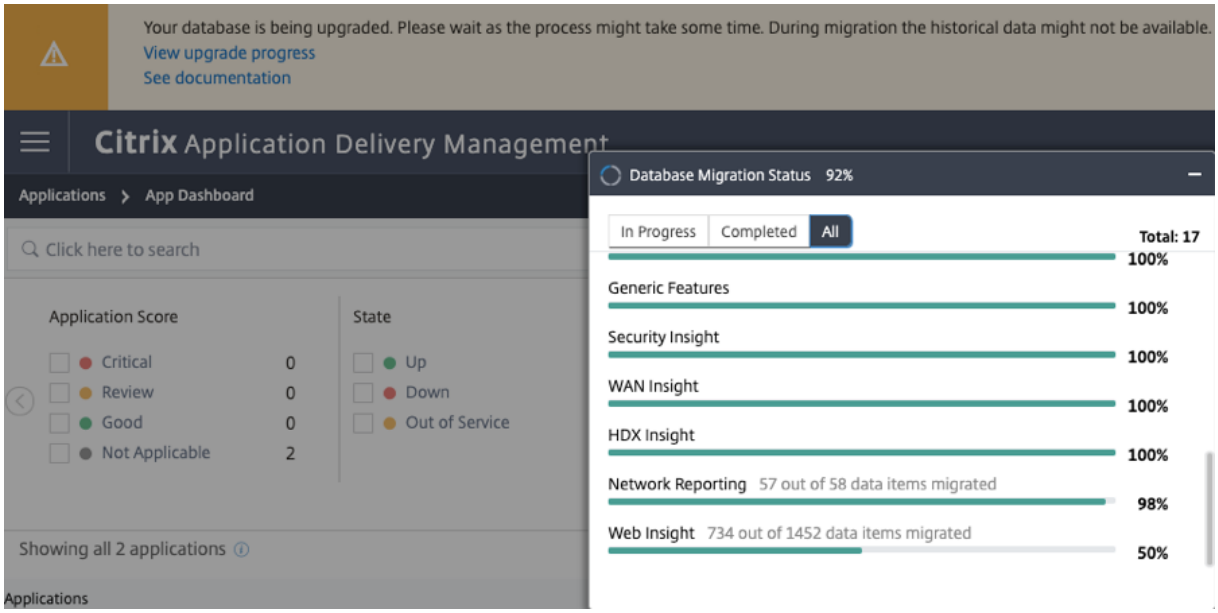
Después de migrar la configuración, puede iniciar sesión en la GUI de ADM. Al iniciar sesión, los datos históricos comienzan a migrarse en segundo plano mientras se puede continuar trabajando en ADM.




Durante la migración de datos históricos, es posible que algunos de los datos antiguos no estén disponibles. El tiempo necesario para migrar la base de datos depende del tamaño de los datos y del número de tablas.

Puede supervisar la migración de la base de datos mediante la GUI de ADM. Haga clic en **Ver progreso de actualización** y aparecerá el **estado de migración de la base de datos**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Solución de problemas de migración de bases de datos

Durante el proceso de actualización a 13.0 67.xx y versiones posteriores, a veces la migración de datos históricos de Web Insight puede parecer paralizado. En tales casos, para comprobar los detalles de la migración de datos, haga lo siguiente.

Inicie sesión en el símbolo del shell de ADM y ejecute el siguiente comando para ver los detalles granulares del progreso.

```
cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
```

Aquí hay un ejemplo de salida

```
bash-3.2# cat /var/mps/log/db_upgrade/
   web_insight_mapping_migration_status
Tue Oct  6 07:41:55 GMT 2020
157 out of 127346 done in 54 seconds
File
 /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
    af_app_client_server_resp_second_l3p_d7_dump
bash-3.2#
```

En este ejemplo, `af_app_client_server_resp_second_l3p_d7` es la entrada que se está actualizando. Y 157 entradas de 127.346 se migran en 54 segundos.

### Actualizar un par de alta disponibilidad de la versión 12.1 a la versión 13.0

Para los servidores Citrix ADM en modo de alta disponibilidad, puede actualizar accediendo al nodo activo o a la dirección IP flotante. Ambos servidores Citrix ADM se actualizan automáticamente a la ver-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

sión más reciente una vez que se inicia el proceso de actualización en cualquiera de los servidores.

> **Nota**
>
> Si va a actualizar un par de alta disponibilidad de la versión 12.0 o anterior, consulte Actualización de Citrix ADM 12.1

## Actualice la implementación de recuperación ante desastres de Citrix ADM

Actualizar la implementación de recuperación ante desastres de Citrix ADM es un proceso de dos pasos:

- Actualice los nodos de Citrix ADM configurados en modo de alta disponibilidad en el sitio principal. Más adelante, debe actualizar el nodo de recuperación ante desastres.
- Asegúrese de que ha actualizado los servidores Citrix ADM implementados en alta disponibilidad antes de actualizar el nodo de recuperación ante desastres.

### Actualizar el nodo de recuperación ante desastres de Citrix ADM

1. Descargue el archivo de imagen de actualización de Citrix ADM desde el sitio de descarga de Citrix.
2. Cargue este archivo al nodo de recuperación ante desastres con las credenciales de `nsrecover`.
3. Inicie sesión en el nodo de recuperación ante desastres con las credenciales de `nsrecover`.
4. Desplácese hasta la carpeta donde colocó el archivo de imagen y descomprima el archivo.
5. Ejecute el siguiente script:

   ./installmas

   ```
   bash-3.2# ./installmas
   ```

## Actualizar agentes en prem para la implementación en varios sitios

La actualización de la implementación del agente Citrix ADM es un proceso de tres pasos.
Asegúrese de haber realizado las siguientes tareas antes de actualizar los agentes locales:

1. Actualice los servidores Citrix ADM implementados en alta disponibilidad.
2. Actualice el nodo de recuperación ante desastres de Citrix ADM.

   Para obtener más información, consulte Actualizar la implementación de recuperación ante desastres de Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Actualizar el agente on-prem**

1. Descargue el archivo de imagen de actualización del agente Citrix ADM desde el sitio de descargas de Citrix.
2. Cargue este archivo en el nodo del agente mediante `nsrecover` credenciales.
3. Asegúrese de descargar la imagen de actualización del agente correcta. El siguiente es un ejemplo de formato de nombre de archivo de imagen:

   build-masagent-13.0-48.18.tgz
4. Inicie sesión en el agente on-prem mediante las`nsrecover` credenciales.
5. Desplácese hasta la carpeta donde colocó el archivo de imagen y descomprima el archivo.

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. Ejecute el siguiente script:

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

## Agregar un disco adicional al servidor Citrix ADM

Si el requisito de almacenamiento de Citrix ADM excede el espacio en disco predeterminado (120 GB), puede conectar un disco adicional. Puede conectar más disco en implementaciones de un solo servidor y de alta disponibilidad.

Al actualizar Citrix ADM desde las versiones 12.1 a 13.0, las particiones que había creado en el disco adicional en la versión anterior siguen siendo las mismas. Las particiones no se eliminan ni se cambian de tamaño.

El procedimiento para conectar más discos sigue siendo el mismo en la compilación actualizada. Ahora puede utilizar la nueva herramienta de partición de discos en Citrix ADM para crear particiones en el disco recién agregado. También puede utilizar la herramienta para cambiar el tamaño de las particiones en el disco más existente. Para obtener más información sobre cómo conectar más discos y utilizar la nueva herramienta de particionamiento de disco, consulte Cómo conectar un disco adicional a Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Aprovisione instancias de Citrix ADC en OpenStack mediante StyleBooks

A partir de la versión 49.23 de Citrix ADM 12.1, se ha actualizado la arquitectura de un flujo de trabajo de orquestación de OpenStack. El flujo de trabajo utiliza ahora los StyleBooks de Citrix ADM para configurar instancias de Citrix ADC. Si actualiza a Citrix ADM 13.0 desde la versión 12.0 o 12.1 compilación 48.18, debe ejecutar la siguiente script de migración:

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

Para obtener más información sobre el StyleBook `os-cs-lb-mon` y el script de migración, consulte Aprovisionamiento de la instancia de Citrix ADC VPX en OpenStack mediante StyleBook.

## Autenticación

January 30, 2024

Los usuarios se pueden autenticar internamente mediante Citrix ADM, externamente mediante un servidor de autenticación o ambas. Si se utiliza la autenticación local, el usuario debe estar en la base de datos de seguridad Citrix ADM. Si el usuario se autentica externamente, el "nombre externo"del usuario debe coincidir con la identidad de usuario externo registrada en el servidor de autenticación, según el protocolo de autenticación seleccionado.

Citrix ADM admite la autenticación externa mediante servidores RADIUS, LDAP y TACACS. Este soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los usuarios locales y externos del servidor Autenticación, Autorización y Contabilidad que están accediendo al sistema. Citrix ADM puede autenticar a los usuarios independientemente de los protocolos reales que utilicen para comunicarse con el sistema. Cuando un usuario intenta acceder a una implementación de Citrix ADM que está configurada para la autenticación externa, el servidor de aplicaciones solicitado envía el nombre de usuario y la contraseña al servidor RADIUS, LDAP o TACACS para la autenticación. Si la autenticación se realiza correctamente, se concede al usuario acceso a Citrix ADM.

### Servidores de autenticación externos

Citrix ADM envía todas las solicitudes de servicio de autenticación, autorización y auditoría al servidor remoto RADIUS, LDAP o TACACS. El servidor de autenticación, autorización y auditoría remotos recibe la solicitud, valida la solicitud y envía una respuesta a Citrix ADM. Cuando se configura para utilizar un servidor remoto RADIUS, TACACS o LDAP para la autenticación, Citrix ADM se convierte en un cliente RADIUS, TACACS o LDAP. En cualquiera de estas configuraciones, los registros de autenticación se almacenan en la base de datos del servidor host remoto. El nombre de cuenta, los permisos asigna-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

dos y los registros de contabilidad de tiempo también se almacenan en el servidor de autenticación, autorización y auditoría de cada usuario.

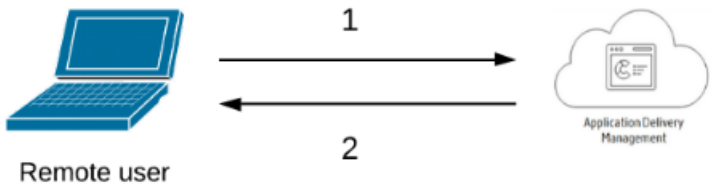
Además, puede utilizar la base de datos interna de Citrix ADM para autenticar a los usuarios localmente. Crear entradas en la base de datos para los usuarios y sus contraseñas y roles predeterminados. También puede seleccionar el orden de autenticación para tipos específicos de autenticación. La lista de servidores de un grupo de servidores es una lista ordenada. El primer servidor de la lista siempre se utiliza a menos que no esté disponible, en cuyo caso se utiliza el siguiente servidor de la lista. Puede configurar servidores para que incluyan la base de datos interna como copia de seguridad de autenticación de reserva en la lista configurada de servidores de autenticación, autorización y auditoría.

## Autenticar usuarios en Citrix ADM

Puede autenticar a sus usuarios en Citrix ADM de dos maneras:

- Usuarios locales configurados en Citrix ADM

  Después de la configuración, el siguiente es el flujo de trabajo para la autenticación de usuario en el servidor local.

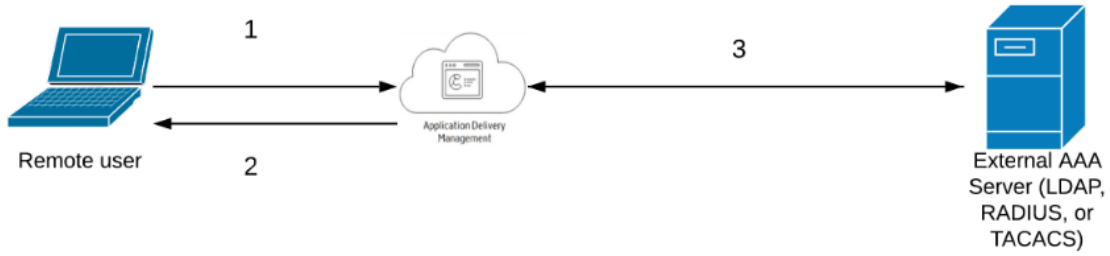



  **1** —El usuario inicia sesión en Citrix ADM

  **2** —Citrix ADM solicita a los usuarios las credenciales para la autenticación y comprueba si las credenciales coinciden en la base de datos de ADM.

- Uso de servidores de autenticación externos

  Después de la configuración, el siguiente es el flujo de trabajo para la autenticación de usuario en el servidor externo de autenticación, autorización y auditoría:




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**1** —El usuario se conecta con Citrix ADM

**2** —Citrix ADM solicita las credenciales al usuario

**3** —Citrix ADM valida las credenciales de usuario con el servidor externo de autenticación, autorización y auditoría. Si la validación se realiza correctamente, el usuario puede continuar iniciando sesión

## Configurar servidores de autenticación externos en NetScaler ADM

January 30, 2024

Después de configurar el servidor LDAP, RADIUS o TACACS, puede agregar estos servidores en NetScaler ADM.

## Agregar servidor de autenticación LDAP

January 30, 2024

Al integrar el protocolo LDAP con los servidores de autenticación RADIUS y TACAS, puede utilizar ADM para buscar y autenticar credenciales de usuario desde directorios distribuidos.

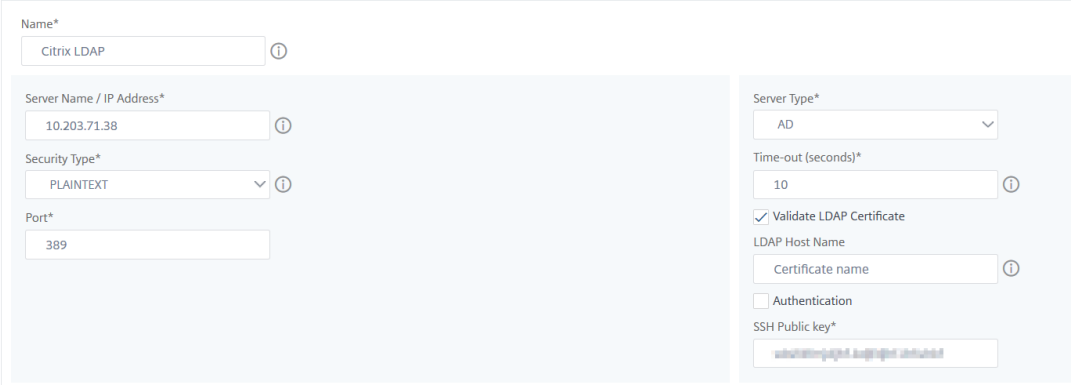
1. Vaya a **Sistema** > **Autenticación**.
2. Seleccione la ficha **LDAP** y, a continuación, haga clic en **Agregar**.
3. En la página **Crear servidor LDAP**, especifique los siguientes parámetros:
   a) **Nombre**: Especifique el nombre del servidor LDAP
   b) **Nombre del servidor/dirección IP**: Especifique la dirección IP LDAP o el nombre del servidor
   c) **Tipo de seguridad**: Tipo de comunicación requerida entre el sistema y el servidor LDAP. Seleccione una opción de la lista. Si la comunicación en texto plano no es adecuada, puede elegir la comunicación cifrada seleccionando Transport Layer Security (TLS) o SSL
   d) **Puerto**: De forma predeterminada, el puerto 389 se utiliza para PLAINTEXT. También puede especificar el puerto 636 para SSL/TLS
   e) **Tipo de servidor**: Seleccione Active Directory (AD) o Novell Directory Service (NDS) como el tipo de servidor LDAP

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

f) Tiempo de**espera (segundos)**: tiempo en segundos durante el que el sistema Citrix ADM espera una respuesta del servidor LDAP

g) **Nombre de host LDAP: active** la casilla Validar certificado LDAP y especifique el nombre de host que se introducirá en el certificado.

Desactive la opción **Autenticación** y especifique la clave pública SSH. Con la autenticación basada en claves, ahora puede obtener la lista de claves públicas almacenadas en el objeto de usuario en el servidor LDAP a través de SSH.



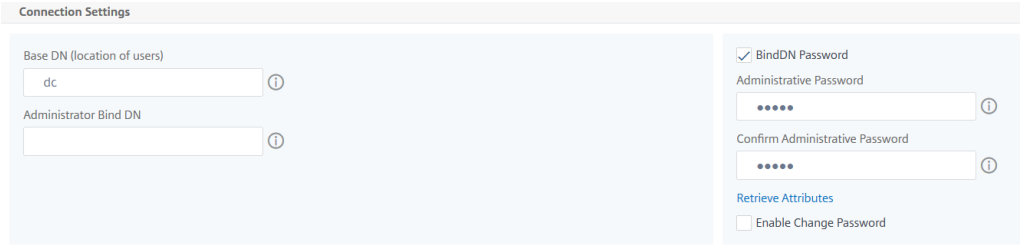

En Configuración de conexión, especifique los siguientes parámetros:

i. **Base DN**: El nodo base para que el servidor LDAP inicie la búsqueda

ii. **Administrator Bind DN**: Nombre de usuario al que se vincula al servidor LDAP. Por ejemplo, admin@aaa.local.

iii. **Contraseña de enlace de DN**: seleccione esta opción para proporcionar una contraseña de autenticación.

iv. **Habilitar cambio de contraseña**: Seleccione esta opción para habilitar el cambio de contraseña




En **Otros ajustes**, especifique los siguientes parámetros

i. **Atributo de nombre de inicio de sesión del servidor**: Atributo de nombre que utiliza el sistema para consultar el servidor LDAP externo o un Active Directory. Seleccione **samAccountname** de la lista.

ii. **Filtro de búsqueda**: Configure usuarios externos para la autenticación de dos factores según el filtro de búsqueda configurado en el servidor LDAP. Por ejemplo, vpnal-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

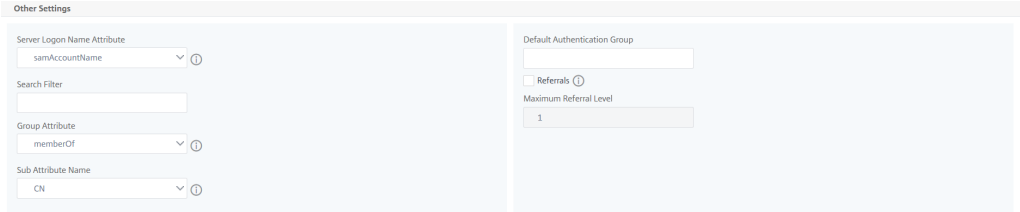
lowed=true con ldaploginame `samaccount` y el nombre de usuario proporcionado por el usuario bob produciría una cadena de búsqueda LDAP de: `&(vpnallowed=true)(samaccount=bob)`.

> Nota
>
> De forma predeterminada, los valores del filtro de búsqueda se encierran entre corchetes.

iii. **Atributo de grupo**: Seleccione memberOf de la lista.

iv. **Nombre de subatributo**: El nombre del subatributo para la extracción de grupos del servidor LDAP.

v. **Grupo de autenticación predeterminado**: Grupo predeterminado para elegir cuando la autenticación se realiza correctamente, además de los grupos extraídos.




4. Haga clic en **Crear**.

   El servidor LDAP ya está configurado.

> Nota
>
> Si los usuarios son miembros del grupo de Active Directory, el grupo y los nombres de los usuarios de Citrix ADM deben tener los mismos nombres de los miembros del grupo de Active Directory.

## Agregar servidor de autenticación RADIUS

January 30, 2024

1. Vaya a **Sistema** > **Autenticación**.
2. Seleccione la ficha **RADIUS** y, a continuación, haga clic en **Agregar**.

   En la página **Crear servidor RADIUS**, especifique los siguientes parámetros:

   a) **Nombre**: Especifique un nombre de servidor RADIUS

   b) **Nombre del servidor/Dirección IP**: Especifique la dirección IP del servidor RADIUS

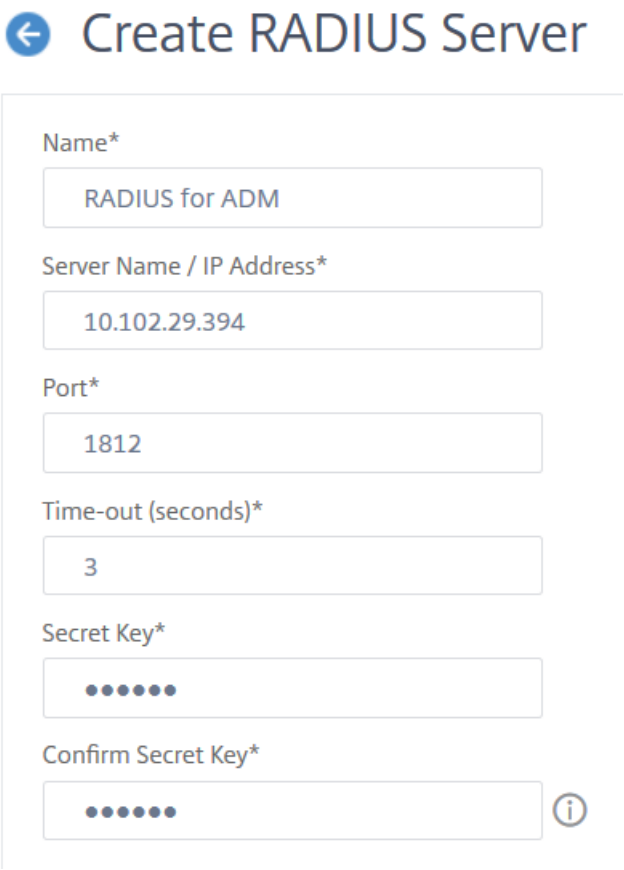
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

c) **Puerto**: Especifique el número de puerto en el que está alojado el servidor RADIUS. El puerto predeterminado es 1812

d) Tiempo de**espera (segundos)**: tiempo en segundos durante el que el sistema Citrix ADM espera una respuesta del servidor RADIUS

e) **Clave secreta**: Especifique la clave secreta RADIUS para la autenticación

f) **Confirmar la clave secreta**: Vuelva a especificar la clave para confirmarla




En **Detalles**, especifique los siguientes parámetros:

i. **ID de NAS**: Especifique el ID para enviar el identificador al servidor RADIUS

ii. **Identificador de proveedor de grupo**: Especifique el ID del proveedor para utilizar la extracción de grupos RADIUS

iii. **Prefijo de grupo**: Cadena que precede a los nombres de grupo dentro de un atributo RADIUS para la extracción de grupos RADIUS

iv. **Tipo de atributo de grupo**: Especifique el tipo de atributo para la extracción del grupo RADIUS

v. **Separador de grupos**: Cadena que delimita los nombres de grupos dentro de un atributo RADIUS para la extracción de grupos RADIUS

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

vi. **Identificador del proveedor de la dirección IP**: El ID del proveedor en RADIUS indica la IP de la intranet. Un valor de 0 indica que el atributo no está codificado por el proveedor.

vii. **Identificador de proveedor de contraseña**: Contraseña de ID de proveedor en la respuesta de RADIUS para extraer la contraseña del usuario

viii. **Tipo de atributo de dirección IP**: Atributo de dirección IP remota para que el RADIUS responda

ix. **Tipo de atributo de contraseña**: El atributo de contraseña para que el RADIUS responda

x. **Codificación de contraseñas**: Seleccione pap, chap, mschapv1 o mschapv2 de la lista. Esto indica cómo se deben codificar las contraseñas en los paquetes RADIUS que viajan del sistema al servidor RADIUS.

xi. **Grupo de autenticación predeterminado**: Grupo predeterminado para elegir cuando la autenticación se realiza correctamente, además de los grupos extraídos

Seleccione Contabilidad si quiere que el dispositivo registre la información de auditoría con el servidor RADIUS.

3. Haga clic en **Crear**.

El servidor RADIUS ahora está configurado.

## Agregar servidor de autenticación TACACS

January 30, 2024

1. Vaya a **Sistema** > **Autenticación**.
2. Seleccione la ficha **TACACS** y, a continuación, haga clic en **Agregar**.
3. En la página **Crear TACACS**, especifique los siguientes parámetros:

   a) **Nombre**: Especifique un nombre de servidor TACACS

   b) **Dirección IP**: Especifique la dirección IP del TACACS

   c) **Puerto**: Especifique el número de puerto en el que está alojado el servidor TACACS. El puerto predeterminado es 49

   d) Tiempo de**espera (segundos)**: tiempo en segundos durante el que el sistema Citrix ADM espera una respuesta del servidor LDAP

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

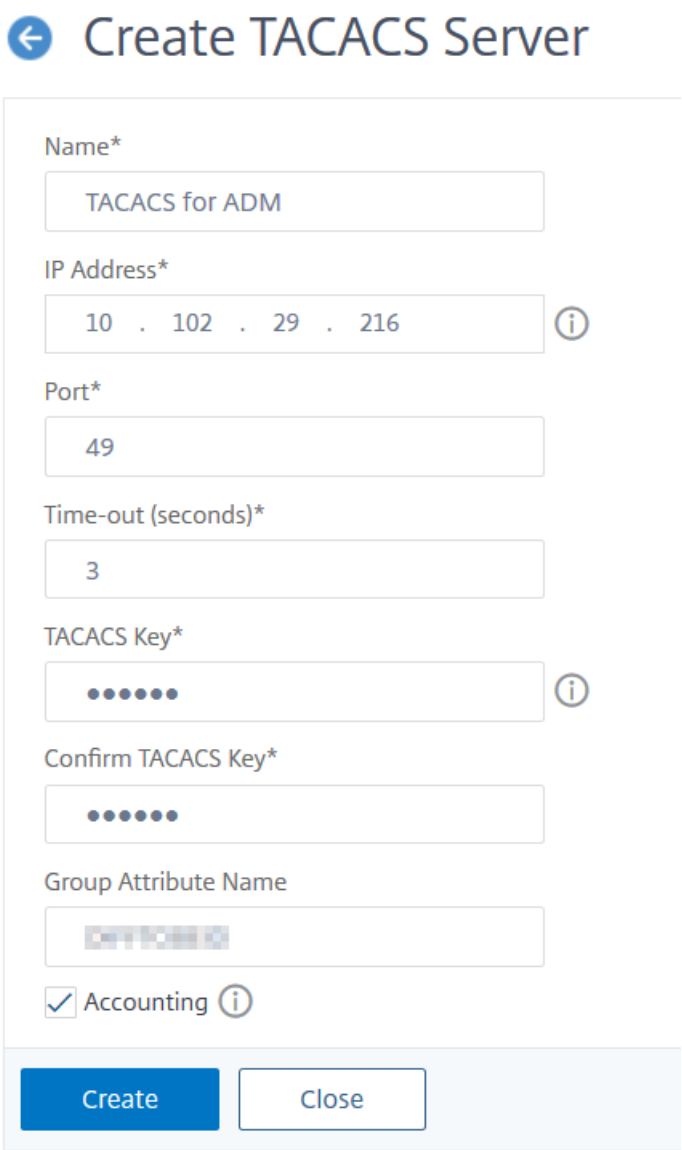
e) Clave**TACACS: especifique la clave** TACACS para la autenticación

f) **Confirme la clave TACACS**: Vuelva a especificar la clave TACACS para confirmarla

g) **Nombre de atributo de grupo**: Especifique el nombre del grupo

Seleccione **Contabilidad** si quiere que el dispositivo registre la información de auditoría con el servidor TACACS.

4. Haga clic en **Crear**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Usuarios en NetScaler ADM

January 30, 2024

Puede crear cuentas de usuario localmente en NetScaler ADM para complementar los usuarios de los servidores de autenticación. Por ejemplo, puede que quiera crear cuentas de usuario locales para usuarios temporales, como consultores o visitantes, sin crear una entrada para esos usuarios en el servidor de autenticación.

Para obtener más información sobre la configuración de usuarios, consulte Configurar usuarios.

> Nota
>
> Si los usuarios están en Active Directory, asegúrese de que el nombre del grupo en Citrix ADM sea el mismo que el del grupo Active Directory en el servidor externo.

## Grupos de usuarios en Citrix ADM

NetScaler ADM le permite autenticar y autorizar a sus usuarios mediante la creación de grupos y la adición de usuarios a los grupos. Un grupo puede tener permisos de "administrador"o de "solo lectura" y todos los usuarios de ese grupo recibirán los mismos permisos.

En Citrix ADM:

- Un grupo se define como un conjunto de usuarios que tienen permisos similares.
- Un grupo puede tener una o varias funciones
- Un usuario se define como una entidad que puede tener acceso en función de los permisos asignados.
- Un usuario puede pertenecer a uno o más grupos

Puede crear grupos locales en NetScaler ADM y utilizar la autenticación local para los usuarios de los grupos. Si utiliza servidores externos para la autenticación, configure los grupos en Citrix ADM para que coincidan con los grupos configurados en los servidores de autenticación de la red interna. Cuando un usuario inicia sesión y se autentica, si un nombre de grupo coincide con un grupo de un servidor de autenticación, el usuario hereda la configuración del grupo en NetScaler ADM.
Si utiliza la autenticación local, cree usuarios y agréguelos a los grupos configurados en Citrix ADM. A continuación, los usuarios heredan la configuración de esos grupos.

Para obtener más información sobre la configuración de grupos y la asignación de permisos de grupos, consulte Configurar grupos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Extraer un grupo de servidores de autenticación

January 30, 2024

> **Nota**
>
> La extracción del servidor TACACS se admite en **Citrix ADM 13.0**.

Citrix ADM le permite:

- Extraiga la lista de grupos a los que pertenece un usuario en el servidor de autenticación externo.
- Asignarlos a la configuración de grupo que coincida con los grupos configurados en el servidor externo.

**Ventajas**:

- No es necesario crear usuarios en NetScaler ADM, ya que se administran en el servidor externo.
- Citrix ADM realiza la autorización de los usuarios asignando permisos de grupo para acceder a servidores virtuales del equilibrador de carga específicos y para aplicaciones específicas del sistema.

## Habilitar servidores de autenticación externa de reserva y en cascada

January 30, 2024

La opción alternativa permite que la autenticación local se sustituya si se produce un error en la autenticación del servidor externo. Un usuario configurado tanto en Citrix ADM como en un servidor de autenticación externo puede iniciar sesión en Citrix ADM, incluso si los servidores de autenticación externos configurados están inactivos o no se puede acceder a ellos. Para garantizar que la autenticación alternativa funcione:

- Los usuarios que no sean NSroot deben poder acceder a Citrix ADM si el servidor externo está inactivo o no está accesible
- Debe agregar al menos un servidor externo

Citrix ADM también admite un sistema unificado de protocolos de autenticación, autorización y contabilidad (AAA) (LDAP, RADIUS y TACACS), junto con la autenticación local. Este soporte unificado proporciona una interfaz común para autenticar y autorizar a todos los usuarios y clientes AAA externos que acceden al sistema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Citrix ADM puede autenticar a los usuarios independientemente de los protocolos reales que se comuniquen con el sistema.
Los servidores de autenticación externa en cascada proporcionan un proceso continuo y sin fallos para autenticar y autorizar a los usuarios externos. Si la autenticación falla en el primer servidor de autenticación, Citrix ADM intenta autenticar al usuario mediante el segundo servidor de autenticación externo, etc. Para habilitar la autenticación en cascada, debe agregar los servidores de autenticación externos a Citrix ADM. Puede agregar cualquier tipo de servidores de autenticación externos compatibles (RADIUS, LDAP y TACACS).

Por ejemplo, considere que quiere agregar cuatro servidores de autenticación externos y configurar dos servidores RADIUS, un servidor LDAP y un servidor TACACS. Citrix ADM intenta autenticarse con los servidores externos en función de las configuraciones. En este escenario de ejemplo, Citrix ADM intenta:

- Conéctese con el primer servidor RADIUS
- Conéctese con el segundo servidor RADIUS, si la autenticación ha fallado con el primer servidor RADIUS
- Conéctese con el servidor LDAP, si la autenticación ha fallado con ambos servidores RADIUS
- Conéctese con el servidor TACACS si la autenticación ha fallado tanto con los servidores RADIUS como con el servidor LDAP.

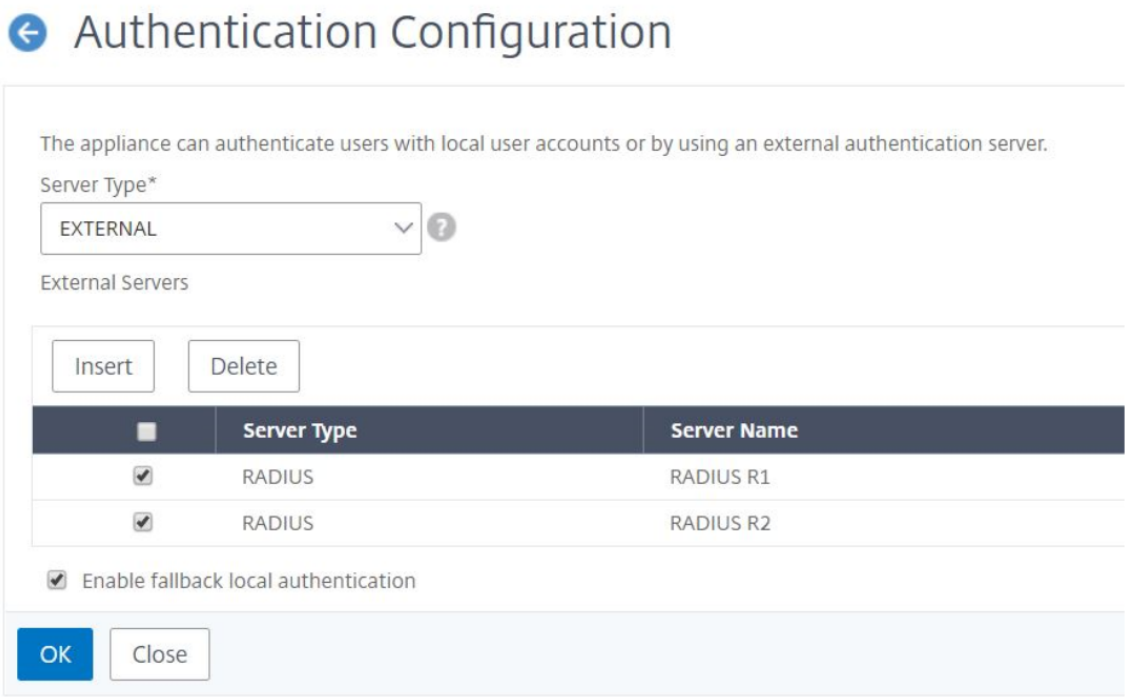
> Nota
>
> Puede configurar hasta 32 servidores de autenticación externos en Citrix ADM.

### Configurar servidores externos de reserva y cascada

1. Vaya a **Sistema** > **Autenticación**.
2. En la página **Autenticación**, haga clic en **Configuración**
3. En la página **Configuración de autenticación**, seleccione **EXTERNO** en la lista de **tipos de servidor** (solo se pueden conectar en cascada los servidores externos).
4. Haga clic en **Insertar**y, en la página **Servidores externos**, seleccione uno o varios servidores de autenticación para conectarlos en cascada.
5. Seleccione la casilla **Habilitar la autenticación local alternativa** si quiere que la autenticación local se sustituya si se produce un error en la autenticación externa.
6. Seleccione la casilla **Registrar la información del grupo externo** si quiere capturar la información del grupo de usuarios externos en el registro de auditoría del sistema.
7. Haga clic en **Aceptar** para cerrar la página.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Los servidores seleccionados se muestran en Servidores externos:




También puede especificar el orden de autenticación mediante el icono situado junto a los nombres de servidor para mover los servidores hacia activo o hacia abajo en la lista.

## Control de acceso

January 30, 2024

La autenticación es un proceso mediante el cual se verifica que alguien es quien afirma ser. Para realizar la autenticación, un usuario ya debe tener una cuenta creada en un sistema que pueda ser interrogada por el mecanismo de autenticación, o debe crearse una cuenta como parte del proceso de la primera autenticación. NetScaler Application Delivery Management (ADM) proporciona un método para autenticar usuarios locales y externos. Si bien los usuarios locales se autentican internamente, Citrix ADM admite la autenticación externa con los protocolos RADIUS, LDAP y TACACS. Cuando un usuario intenta acceder a NetScaler ADM configurado para autenticación externa, el servidor de aplicaciones solicitado envía el nombre de usuario y la contraseña al servidor RADIUS, LDAP o TACACS para la autenticación. Una vez autenticado, se utiliza el protocolo necesario para identificar al usuario en Citrix ADM.

El control de acceso es el proceso de aplicar la seguridad requerida para un recurso en particular. Es una técnica de seguridad que se puede utilizar para regular quién puede ver o utilizar los recursos en un entorno informático. El objetivo del control de acceso es limitar las acciones u operaciones que

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

un usuario legítimo de un sistema informático puede realizar. El control de acceso restringe lo que un usuario puede hacer directamente y qué programas que se ejecutan en nombre de los usuarios pueden hacer. De esta manera, el control de acceso busca evitar actividades que puedan conducir a una infracción de la seguridad. El control de acceso supone que la autenticación del usuario se ha verificado correctamente antes de la aplicación del control de acceso a través de un monitor de referencia. Citrix ADM permite un control de acceso detallado y basado en roles (RBAC) mediante el cual los administradores pueden proporcionar permisos de acceso a los usuarios en función de las funciones de los usuarios individuales dentro de una empresa. El RBAC en Citrix ADM se logra mediante la creación de políticas de acceso, funciones, grupos y usuarios.

## Control de acceso por roles

January 30, 2024

Citrix ADM proporciona un control de acceso detallado basado en funciones (RBAC), con el que puede conceder permisos de acceso en función de las funciones de los usuarios individuales de la empresa. En este contexto, el acceso es la capacidad de realizar una tarea específica, como ver, crear, modificar o eliminar un archivo. Los roles se definen de acuerdo con la autoridad y responsabilidad de los usuarios dentro de la empresa. Por ejemplo, se puede permitir a un usuario realizar todas las operaciones de red, mientras que otro puede observar el flujo de tráfico en las aplicaciones y ayudar a crear plantillas de configuración.

Los roles están determinados por las directivas. Después de crear las directivas, se crean las funciones, se vinculan las funciones a una o más directivas y se asignan las funciones a los usuarios. También puede asignar roles a grupos de usuarios.

Un grupo es un conjunto de usuarios que tienen permisos en común. Por ejemplo, los usuarios que administran un centro de datos concreto se pueden asignar a un grupo. Un rol es una identidad que se otorga a los usuarios o grupos en función de condiciones específicas. En NetScaler ADM, la creación de roles y directivas es específica de la función RBAC en NetScaler ADC. Los roles y las directivas se pueden crear, cambiar o interrumpir fácilmente a medida que evolucionan las necesidades de la empresa, sin tener que actualizar individualmente los privilegios de cada usuario.

Los roles pueden estar basados en funciones o en recursos. Por ejemplo, considere un administrador SSL/Security y un administrador de aplicaciones. Un administrador de SSL/Security debe tener acceso completo a las funciones de supervisión y administración de certificados SSL, pero debe tener acceso de solo lectura para las operaciones de administración del sistema. Un administrador de aplicaciones debe poder acceder únicamente a los recursos dentro del ámbito.

**Ejemplo:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Chris, el jefe del grupo ADC, es el superadministrador de NetScaler ADM en su organización. Chris crea tres funciones de administrador: administrador de seguridad, administrador de aplicaciones y administrador de red.

David, el administrador de seguridad, debe tener acceso completo para la administración y supervisión de certificados SSL, pero también tener acceso de solo lectura para las operaciones de administración del sistema.

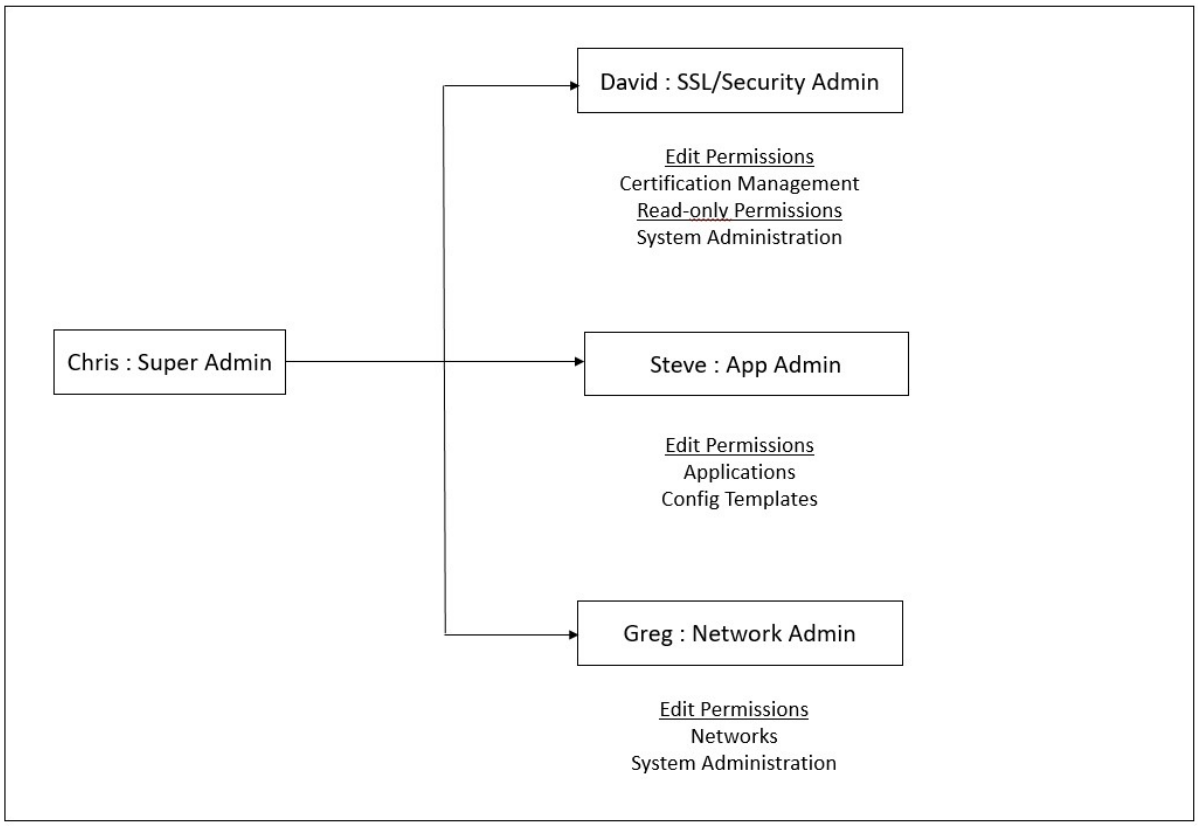
Steve, un administrador de aplicaciones, necesita acceso solo a aplicaciones específicas y a plantillas de configuración específicas.

Greg, un administrador de red, necesita acceso a la administración de sistemas y redes.

Chris también debe proporcionar RBAC para todos los usuarios, independientemente del hecho de que sean locales o externos.

Los usuarios de NetScaler ADM pueden autenticarse localmente o se pueden autenticar a través de un servidor externo (RADIUS/LDAP/TACACS). La configuración de RBAC debe ser aplicable a todos los usuarios independientemente del método de autenticación adoptado.

La imagen siguiente muestra los permisos que tienen los administradores y otros usuarios y sus roles en la organización.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Limitaciones

El RBAC no es totalmente compatible con las siguientes funciones de Citrix ADM:

- **Analytics**: RBAC no es totalmente compatible con los módulos de análisis. La compatibilidad con RBAC se limita al nivel de instancia y no es aplicable a nivel de aplicación en los módulos de análisis Web Insight, SSL Insight, Gateway Insight, HDX Insight y Security Insight. Por ejemplo:

**Ejemplo 1**: RBAC basado en instancias (compatible)

Un administrador al que se le hayan asignado algunas instancias solo puede ver esas instancias en **Web Insight** > **Instancias**y solo los servidores virtuales correspondientes en **Web Insight** > **Aplicaciones**, ya que el RBAC es compatible a nivel de instancia.

**Ejemplo 2**: RBAC basado en aplicaciones (no compatible)

Un administrador al que se le hayan asignado algunas aplicaciones puede ver todos los servidores virtuales en **Web Insight** > **Aplicaciones**, pero no puede acceder a ellos porque el RBAC no se admite a nivel de aplicaciones.

- **StyleBooks**: RBAC no es totalmente compatible con StyleBooks.
  - En NetScaler ADM, los StyleBooks y los paquetes de configuración se consideran recursos independientes. Los permisos de acceso, ya sea para ver, modificar o ambos, se pueden proporcionar para StyleBook y paquetes de configuración por separado o simultáneamente. Un permiso de visualización o edición en los paquetes de configuración permite implícitamente al usuario ver los StyleBooks, lo cual es esencial para obtener los detalles del paquete de configuración y crear paquetes de configuración.
  - No se admite el permiso de acceso para StyleBook o paquetes de configuración específicos
    Ejemplo: si ya hay un paquete de configuración en la instancia, los usuarios pueden modificar la configuración en una instancia de NetScaler ADC de destino incluso si no tienen acceso a esa instancia.
- **Orquestación**: RBAC no es compatible con Orchestration.

## Configurar directivas de acceso

January 30, 2024

Las directivas de acceso definen los permisos. Se puede aplicar una directiva a un solo usuario o grupo, o a varios usuarios y grupos. Citrix Application Delivery Management (ADM) proporciona cuatro directivas de acceso predefinidas:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. **adminpolicy**. Concede acceso a todas las funciones de Citrix ADM. El usuario tiene permisos de visualización y edición, puede ver todo el contenido de Citrix ADM y puede realizar todas las operaciones de edición. Es decir, el usuario puede realizar operaciones de adición, modificación y eliminación en los recursos.
2. **readonlypolicy**. Otorga permisos de solo lectura. El usuario puede ver todo el contenido de Citrix ADM, pero no está autorizado a realizar ninguna operación.
3. **appAdminPolicy**. Otorga permisos administrativos para acceder a las funciones de la aplicación en Citrix ADM. Un usuario sujeto a esta directiva puede agregar, modificar y eliminar aplicaciones personalizadas y puede habilitar o inhabilitar los servicios, los grupos de servicios y los distintos servidores virtuales, como la conmutación de contenido, la redirección de caché y los servidores virtuales HAProxy.
4. **appReadOnlyPolicy**. Otorga permisos de solo lectura para las funciones de la aplicación. Un usuario vinculado a esta directiva puede ver las aplicaciones, pero no puede realizar ninguna operación de adición, modificación, eliminación, activación o desactivación.

> **Nota:** Las directivas predefinidas no se pueden modificar.

También puede crear sus propias directivas (definidas por el usuario).

**Para crear directivas de acceso definidas por el usuario:**

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > Directivas de **acceso**.
2. Haga clic en **Agregar**.
3. En el campo **Nombre de la directiva**, introduzca el nombre de la directiva e introduzca la descripción en el campo **Descripción de la directiva**.

   La sección **Permisos** enumera todas las funciones de Citrix ADM, con opciones para especificar el acceso de solo lectura, habilitar-inhabilitar o modificar.
4. Haga clic en el icono (+) para expandir cada grupo de entidades en varias entidades.

   a) Seleccione la casilla de verificación de permisos situada junto al nombre de la función para conceder permisos a los usuarios.

      - **Ver:** Esta opción permite al usuario ver la función en Citrix ADM.
      - **Activar-Inhabilitar:** Esta opción solo está disponible para las **funciones Funciones de red** que permiten habilitar o inhabilitar acciones en Citrix ADM. El usuario puede habilitar o inhabilitar la función. Además, el usuario también puede realizar la acción **Encuestar ahora**.

        Cuando se concede el permiso **Habilitar-Inhabilitar** a un usuario, también se concede el permiso **Ver**. No puede anular la selección de esta opción.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Modificar:** esta opción otorga el acceso total al usuario. El usuario puede modificar la función y sus funciones.

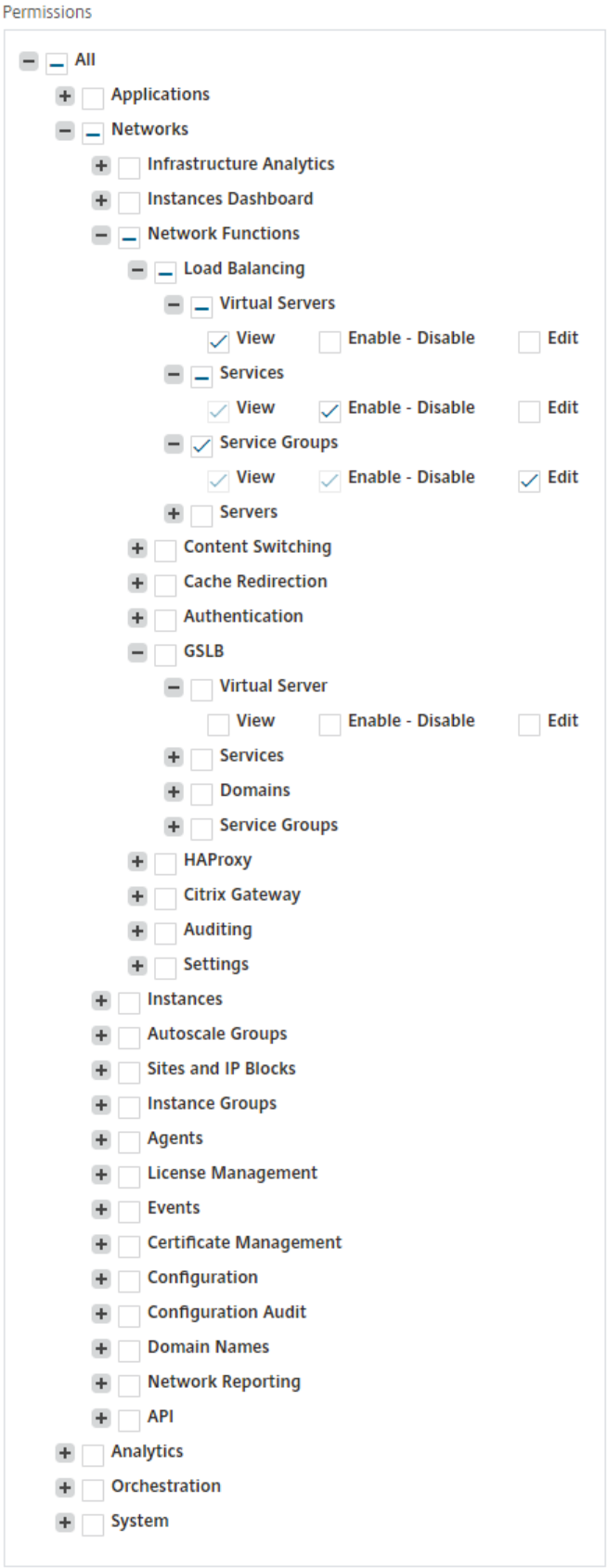
  Si concedes el permiso de **edición**, se concederán los permisos de **visualización** y de **activación y desactivación**. No puede anular la selección de las opciones seleccionadas automáticamente.

Si selecciona la casilla de verificación de la función, se seleccionan todos los permisos de la función.

> **Nota:**
>
> Amplíe Load Balancing y GSLB para ver más opciones de configuración.

En la imagen siguiente, las opciones de configuración de la función Equilibrio de carga tienen permisos diferentes:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El permiso de **visualización** se concede a un usuario para la función **Servidores virtuales**. El usuario puede ver los servidores virtuales de equilibrio de carga en Citrix ADM. Para ver los servidores virtuales, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga** y seleccione la ficha **Servidores virtuales**.

El permiso **Habilitar-Inhabilitar** se concede a un usuario para la función **Servicios**. Este permiso también otorga el permiso de **visualización**. El usuario puede habilitar o inhabilitar los servicios enlazados a un servidor virtual de equilibrio de carga. Además, el usuario puede realizar **la acción de encuesta ahora** en los servicios. Para habilitar o inhabilitar servicios, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga** y seleccione la ficha **Servicios**.

> **Nota**
>
> Si un usuario tiene el permiso **Habilitar-Inhabilitar**, la acción Habilitar o inhabilitar en un servicio está restringida en la página siguiente:
>
> a) Vaya a **Redes** > **Funciones de red**.
>
> b) Seleccione un servidor virtual y haga clic en **Configurar**.
>
> c) Seleccione la página **Vinculación del servicio de servidor virtual de equilibrio de carga**.
> Esta página muestra un mensaje de error si selecciona **Activar** o **Desactivar**.

El permiso de **edición** se concede a un usuario para la función **de grupos de servicios**. Este permiso otorga el acceso completo cuando se otorgan los permisos de **visualización** y **activación y desactivación**. El usuario puede modificar los grupos de servicios enlazados a un servidor virtual de equilibrio de carga. Para modificar los grupos de servicios, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga** y seleccione la ficha **Grupos de servicios**.

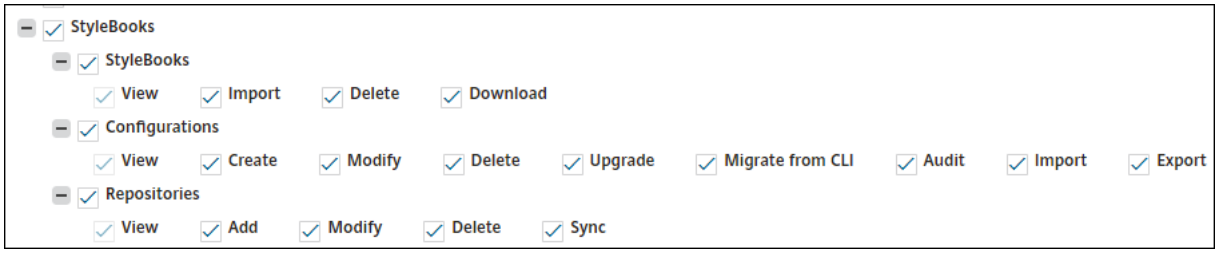
5. Haga clic en **Crear**.

## Otorgar permisos de StyleBook a los usuarios

Puede crear una directiva de acceso para conceder permisos de StyleBook, como importar, eliminar, descargar, etc.

> **Nota**
>
> El permiso Ver se habilita automáticamente cuando concede otros permisos de StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Configurar grupos

January 30, 2024

En Citrix ADM, un grupo puede tener acceso tanto a nivel de entidad como a nivel de recursos. Por ejemplo, un grupo de usuarios puede tener acceso solo a instancias seleccionadas de Citrix ADC; otro grupo con solo unas pocas aplicaciones seleccionadas, etc.

Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. A todos los usuarios de ese grupo se les asignan los mismos derechos de acceso en Citrix ADM.

Puede administrar el acceso de un usuario en Citrix ADM a nivel individual de las entidades de funciones de red. Puede asignar dinámicamente permisos específicos al usuario o al grupo a nivel de entidad.

Citrix ADM trata el servidor virtual, los servicios, los grupos de servicios y los servidores como entidades de función de red.

- **Servidor virtual (aplicaciones)**: equilibrio de carga (lb), GSLB, cambio de contexto (CS), redirección de caché (CR), autenticación (`Auth`) y Citrix Gateway (VPN)
- **Servicios**: Equilibrio de carga y servicios GSLB
- **Grupo de servicios: grupos** de servicios GSLB y equilibrio de carga
- **Servidores: servidores** de equilibrio de carga

### Crear un grupo de usuarios

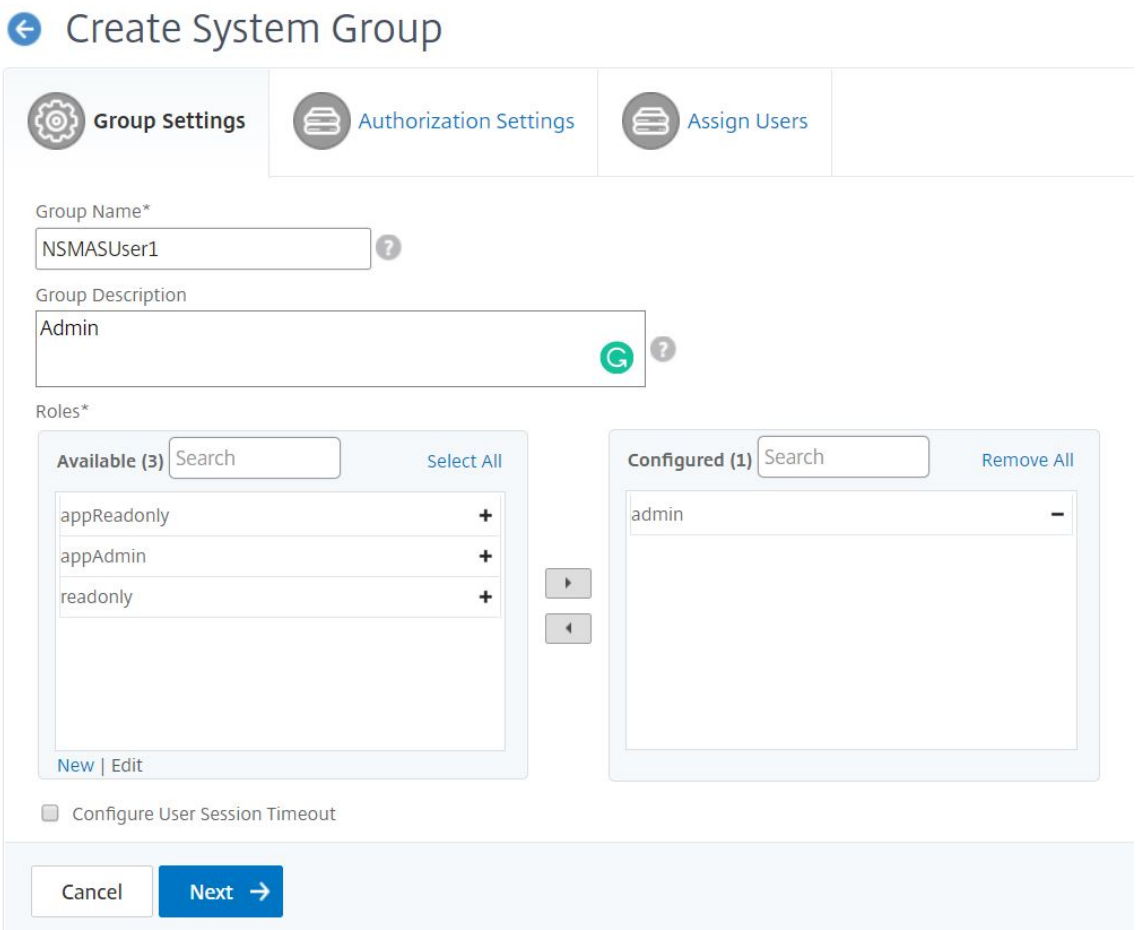
1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Grupos**.
2. Haga clic en **Agregar**.

   Aparece la página **Crear grupo de sistemas**.
3. En el campo **Nombre de grupo**, escriba el nombre del grupo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En el campo**Descripción del grupo**, escriba una descripción del grupo. Proporcionar una buena descripción del grupo le ayuda a comprender mejor el papel y la función del grupo en un momento posterior.
5. En la sección **Roles**, agregue o mueva uno o más roles a la lista **Configurado**.

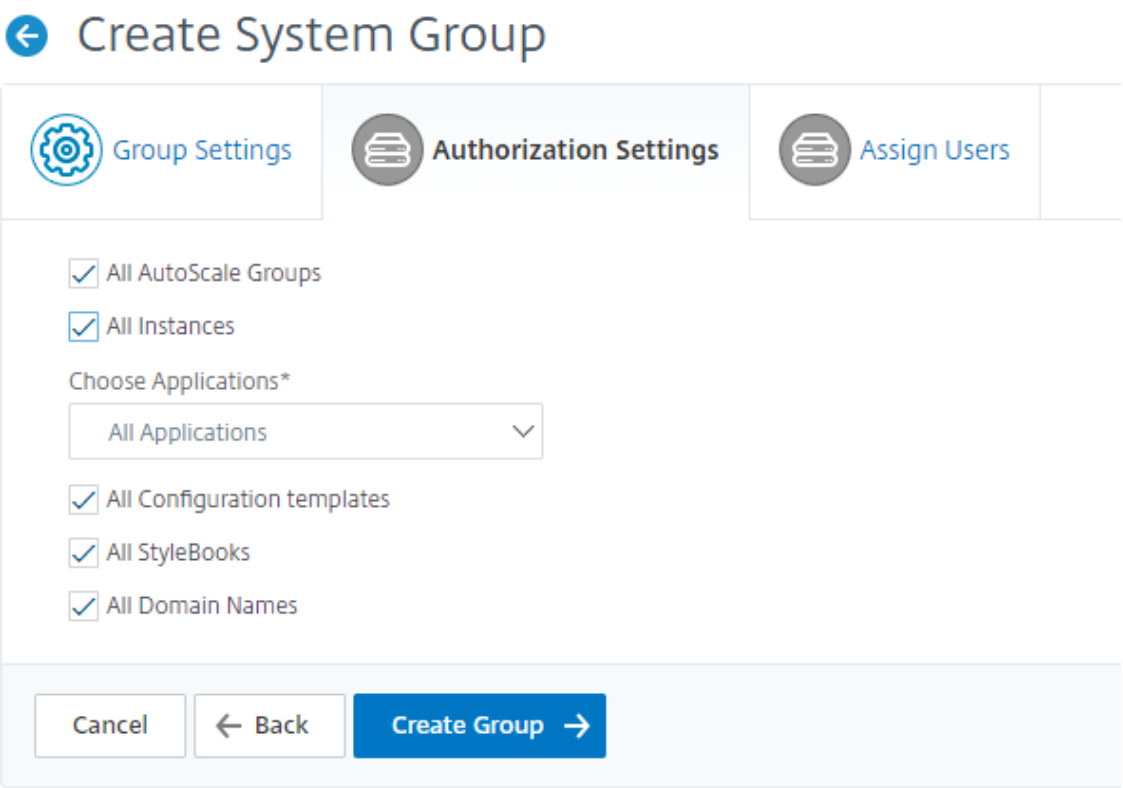
> **Nota**
> En la lista **Disponible**, puede hacer clic en **Nuevo** o **Modificar** y crear o modificar roles. También puede navegar a **Sistema** > **Administración** de **usuarios > Usuarios** y crear o modificar usuarios.




6. Haga clic en **Siguiente**. En la ficha **Configuración de autorización**, puede proporcionar la configuración de autorización para los siguientes recursos:
   - Grupos de Autoscale
   - Instancias
   - Aplicaciones
   - Plantillas de configuración
   - StyleBooks

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Paquetes de configuración
- Nombres de dominio




Es posible que quiera seleccionar recursos específicos de las categorías a las que los usuarios pueden tener acceso.

**Grupos de Autoscale:**

Si quiere seleccionar los grupos de Autoscale específicos que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los grupos de Autoscale** y haga clic en **Agregar grupos de Autoscale**.

b) Seleccione los grupos de Autoscale necesarios de la lista y haga clic en **Aceptar**.

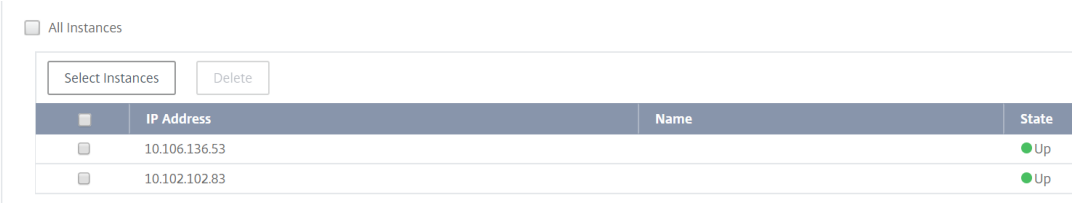
**Instancias:**

Si quiere seleccionar las instancias específicas que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todas las instancias** y haga clic en **Seleccionar instancias**.

b) Seleccione las instancias necesarias de la lista y haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Aplicaciones:**

La lista **Elegir aplicaciones** le permite conceder acceso a un usuario a las aplicaciones necesarias.

Puede conceder acceso a las aplicaciones sin seleccionar sus instancias. Porque las aplicaciones son independientes de sus instancias para conceder el acceso a los usuarios.

Al conceder a un usuario acceso a una aplicación, el usuario está autorizado a acceder solo a esa aplicación, independientemente de la selección de instancias.

Esta lista le ofrece las siguientes opciones:

- **Todas las aplicaciones:** Esta opción está seleccionada por defecto. Agrega todas las aplicaciones que están presentes en el Citrix ADM.
- **Todas las aplicaciones de instancias seleccionadas:** Esta opción solo aparece si selecciona instancias de la categoría **Todas las instancias**. Agrega todas las aplicaciones presentes en la instancia seleccionada.
- **Aplicaciones específicas:** esta opción le permite agregar las aplicaciones necesarias a las que quiere que accedan los usuarios. Haga clic en **Agregar aplicaciones** y seleccione las aplicaciones necesarias de la lista.
- **Seleccione el tipo de entidad individual:** esta opción le permite seleccionar un tipo específico de entidad de función de red y las entidades correspondientes.

  Puede agregar entidades individuales o seleccionar todas las entidades del tipo de entidad requerido para conceder acceso a un usuario.

  La opción **Aplicar también en entidades enlazadas** autoriza las entidades enlazadas al tipo de entidad seleccionado. Por ejemplo, si selecciona una aplicación y selecciona **Aplicar también a entidades enlazadas**, Citrix ADM autoriza todas las entidades que están enlazadas a la aplicación seleccionada.

  > **Nota**
  >
  > Asegúrese de haber seleccionado solo un tipo de entidad si quiere autorizar las entidades enlazadas.

Puede usar expresiones regulares para buscar y agregar las entidades de funciones de red que cumplan con los criterios de expresiones regulares de los grupos. La expresión de expresiones

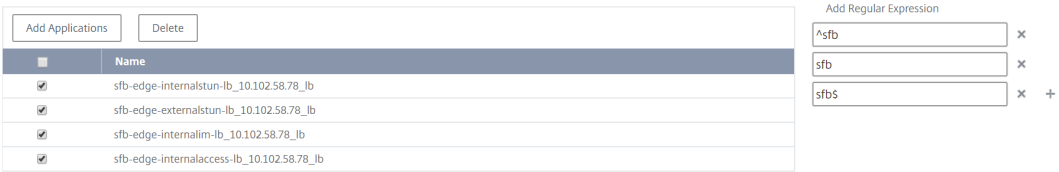
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

regulares especificada se conserva en Citrix ADM. Para agregar una expresión regular, lleve a cabo los siguientes pasos:

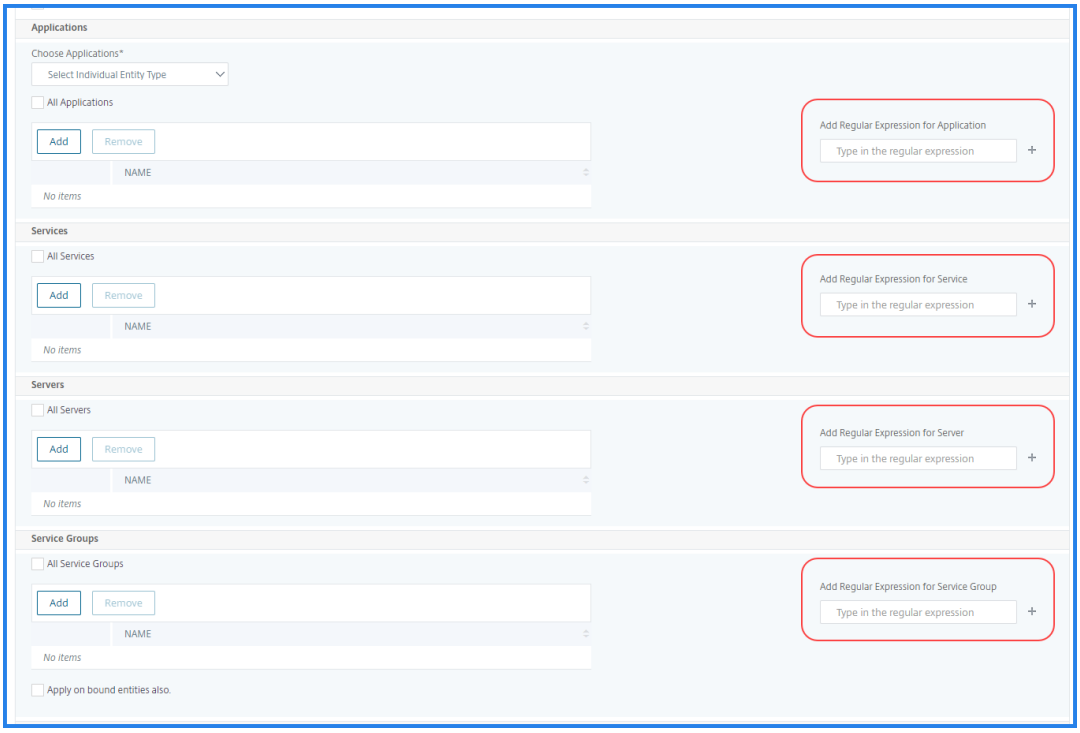
a) Haga clic en **Agregar expresión regular**.

b) Especifique la expresión regular en el cuadro de texto.

En la siguiente imagen se explica cómo utilizar la expresión regular para agregar una aplicación cuando se selecciona la opción **Aplicaciones específicas** :




En la siguiente imagen se explica cómo utilizar la expresión regular para agregar entidades de función de red al elegir la opción **Seleccionar el tipo de entidad individual** :




Si quiere agregar más expresiones regulares, haga clic en el icono **+**.

> **Nota**
>
> La expresión regular solo coincide con el nombre del servidor para el tipo de entidad **Servidores** y no con la dirección IP del servidor.

Si selecciona la opción **Aplicar también a las entidades enlazadas** para una entidad detectada, el usuario puede acceder automáticamente a las entidades que están enlazadas a la entidad

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

descubierta.

La expresión regular se almacena en el sistema para actualizar el alcance de la autorización. Cuando las nuevas entidades coinciden con la expresión regular de su tipo de entidad, Citrix ADM actualiza el alcance de la autorización para las nuevas entidades.

**Plantillas de configuración:**

Si quiere seleccionar la plantilla de configuración específica que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todas las plantillas de configuración** y haga clic en **Agregar plantilla de configuración**.

b) Seleccione la plantilla necesaria de la lista y haga clic en **Aceptar**.

**StyleBooks:**

Si quiere seleccionar el StyleBook específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los StyleBooks** y haga clic en **Agregar StyleBook al grupo**. Puede seleccionar StyleBooks individuales o especificar una consulta de filtro para autorizar StyleBooks.

   Si quiere seleccionar los StyleBooks individuales, seleccione los StyleBooks en el panel **Individuales StyleBooks** y haga clic en **Guardar selección**.

   Si quiere utilizar una consulta para buscar StyleBooks, seleccione el panel **Filtros personalizados**. Una consulta es una cadena de pares clave-valor donde las claves son `name`, `namespace`, y `version`.

   También puede utilizar expresiones regulares como valores para buscar y agregar StyleBooks que cumplan los criterios de expresiones regulares para los grupos. Una consulta de filtro personalizada para buscar StyleBooks admite las dos operaciones `And` y `Or`.

   Ejemplo :

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
    version=1.0
```

   Esta consulta enumera los StyleBooks que cumplen las condiciones siguientes:

   - El nombre de StyleBook es `lb-mon` o `lb`.
   - El espacio de nombres StyleBook es `com.citrix.adc.stylebooks`.
   - La versión de StyleBook es `1.0`.

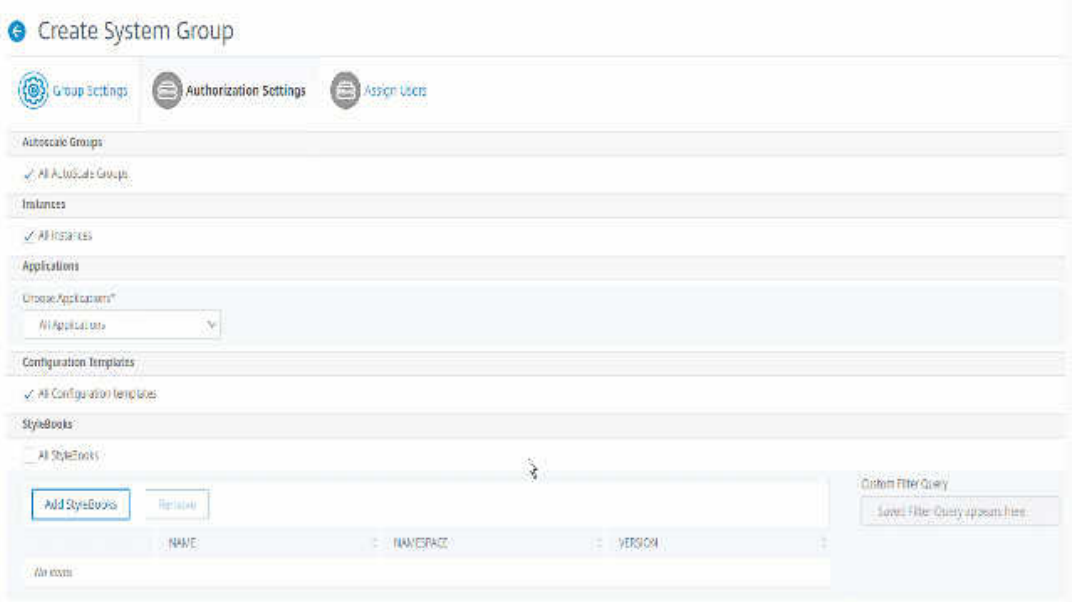
   Utilice una operación `Or` entre expresiones de valor definidas para la expresión clave.

   Ejemplo :

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- La consulta `name=lb-mon|lb` es válida. Devuelve los StyleBooks que tienen un nombre `lb-mon` o `lb`.
- La consulta `name=lb-mon | version=1.0` no es válida.

Presione `Enter` para ver los resultados de la búsqueda y haga clic en **Guardar consulta**.




La consulta guardada aparece en la **consulta de filtros personalizados**. Basado en la consulta guardada, el ADM proporciona acceso de usuario a esos StyleBooks.

b) Seleccione los StyleBooks necesarios de la lista y haga clic en **Aceptar**.

Puede seleccionar los StyleBooks necesarios cuando cree grupos y agregue usuarios a ese grupo. Cuando el usuario selecciona el StyleBook permitido, también se seleccionan todos los StyleBooks dependientes.

**Paquetes de configuración:**

En **Configpacks**, seleccione una de las siguientes opciones:

- **Todas las configuraciones**: esta opción está seleccionada de forma predeterminada. Agrega todos los paquetes de configuración que están en ADM.
- **Todas las configuraciones de los StyleBooks seleccionados**: esta opción agrega todos los paquetes de configuración del StyleBook seleccionado.
- **Configuraciones específicas**: Esta opción le permite agregar los paquetes de configuración necesarios.

  Puede seleccionar los paquetes de configuración necesarios al crear grupos y agregar usuarios a ese grupo.

**Nombres de dominio:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

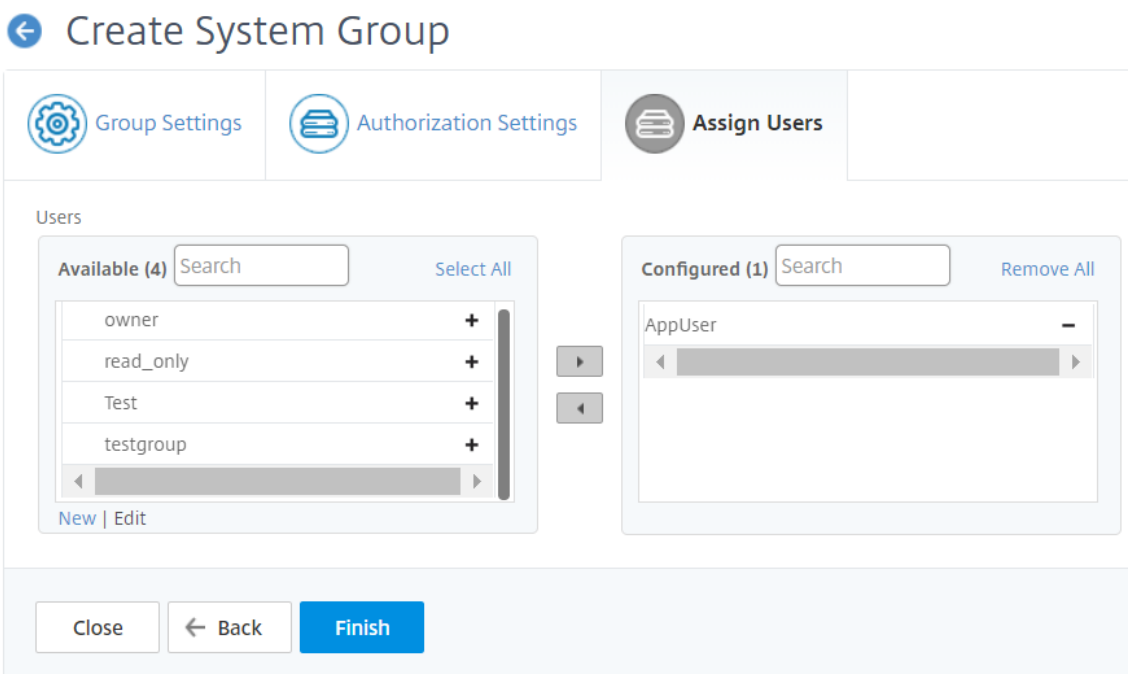
Si quiere seleccionar el nombre de dominio específico que un usuario puede ver o administrar, lleve a cabo los siguientes pasos:

a) Desactive la casilla **Todos los nombres de dominio** y haga clic en **Agregar nombre de dominio**.

b) Seleccione los nombres de dominio necesarios de la lista y haga clic en **Aceptar**.

7. Haga clic en **Crear grupo**.
8. En la sección **Asignar usuarios** , seleccione el usuario en la lista **Disponible** y añada el usuario a la lista **Configurado** .

> **Nota:**
>
> También puede agregar usuarios haciendo clic en **Nuevo**.




9. Haga clic en **Finalizar**.

### Gestione el acceso de los usuarios a través de múltiples entidades de funciones de red

Como administrador, puede administrar el acceso de los usuarios a nivel individual de las entidades de función de red en Citrix ADM. Además, puede asignar de forma dinámica permisos específicos al usuario o a un grupo a nivel de entidad mediante el filtro de expresiones regulares.

Este documento describe cómo definir la autorización de usuario a nivel de entidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Antes de comenzar, cree un grupo. Consulte Configurar grupos en Citrix ADM para obtener más información.

**Caso de uso:**

Considere un caso en el que una o más aplicaciones (servidores virtuales) están alojadas en el mismo servidor. Un superadministrador (George) quiere conceder a Steve (un administrador de aplicaciones) acceso solo a App1 y no al servidor de alojamiento.

La siguiente tabla ilustra este entorno, en el que el Servidor-A aloja las aplicaciones App-1 y App-2.

| Servidor anfitrión | Aplicación (servidor virtual) | Servicio | Grupo de servicios |
|---|---|---|---|
| Servidor A | App1 | App-service-1 | App-service-group-1 |
| Servidor A | App2 | App-service-2 | App-service-group-2 |

> **Nota:**
>
> Citrix ADM trata el servidor virtual, los servicios, los grupos de servicios y los servidores como entidades de función de red. El servidor virtual del tipo de entidad se denomina aplicación.

Para asignar permisos de usuario a las entidades de funciones de red, George define la autorización de usuario de la siguiente manera:

1. Vaya a **Cuenta > Administración de usuarios > Grupos** y agrega un grupo.
2. En la ficha **Configuración de autorización**, seleccione Elegir aplicaciones.
3. Elija **Seleccionar tipo de entidad individual**.
4. Seleccione el tipo de entidad **Todas las aplicaciones** y agregue la entidad App-1 de la lista disponible.
5. Haga clic en **Crear grupo**.
6. En **Asignar usuarios**, seleccione los usuarios que requieren el permiso. Para este caso, George selecciona el perfil de usuario de Steve.
7. Haga clic en **Finalizar**.

Con esta configuración de autorización, Steve solo puede administrar App-1 y no otras entidades de funciones de red.

> **Nota**
>
> Asegúrese de que la opción **Aplicar también a entidades enlazadas** esté desactivada. De lo contrario, Citrix ADM concede acceso a todas las entidades de función de red que están enlazadas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> a App-1. Como resultado, también otorga acceso al servidor de alojamiento.

Un superadministrador puede especificar las expresiones regulares (expresiones regulares) para cada tipo de entidad. La expresión regular se almacena en el sistema para actualizar el ámbito de autorización del usuario. Cuando las nuevas entidades coinciden con la expresión normal de su tipo de entidad, Citrix ADM puede conceder dinámicamente a los usuarios acceso a las entidades de funciones de red específicas.

Para conceder permisos a los usuarios de forma dinámica, el superadministrador puede agregar expresiones regulares en la ficha **Configuración de autorización**.

En este caso, George agrega App* como expresión regular el tipo de entidad Aplicaciones y las aplicaciones que coinciden con los criterios de expresiones regulares aparecen en la lista. Con esta configuración de autorización, Steve puede acceder a todas las aplicaciones que coincidan con la expresión regular App*. Sin embargo, su acceso está limitado solo a las aplicaciones, no al servidor alojado.

### Cómo cambia el acceso de usuario en función del ámbito de autorización

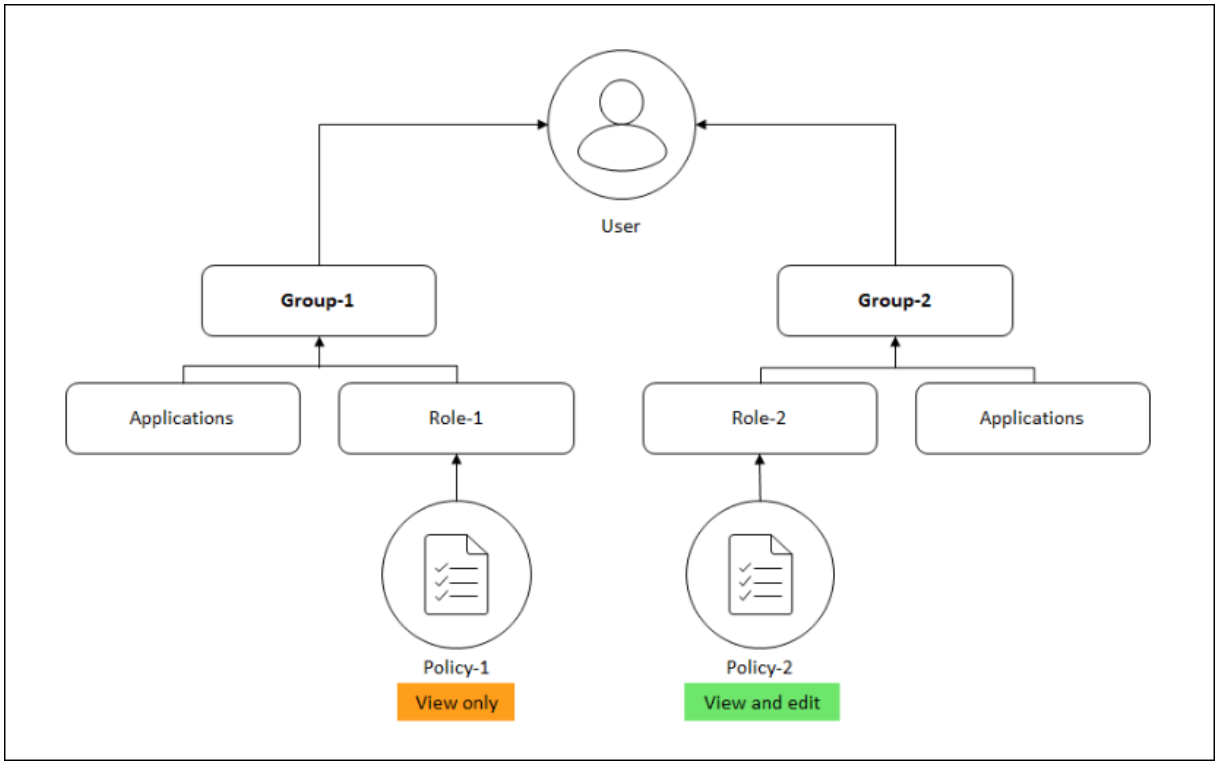
Cuando un administrador agrega un usuario a un grupo que tiene diferentes configuraciones de directiva de acceso, el usuario se asigna a más de un ámbito de autorización y directivas de acceso.

En este caso, el ADM concede al usuario acceso a las aplicaciones según el alcance de autorización específico.

Considere un usuario asignado a un grupo que tiene dos directivas de directiva 1 y directiva 2.

- **Directiva 1**: solo se muestran los permisos para las aplicaciones.
- **Directiva 2**: Ver y modificar los permisos de las aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




El usuario puede ver las aplicaciones especificadas en la Directiva 1. Además, este usuario puede ver y modificar las aplicaciones especificadas en la directiva 2. El acceso de edición a las aplicaciones Group-1 está restringido ya que no está en el ámbito de autorización Group-1.

## Asignación de RBAC al actualizar Citrix ADM de 12.0 a versiones posteriores

Al actualizar Citrix ADM de 12.0 a 13.0, no ve las opciones para proporcionar permisos de "lectura-escritura"o "lectura"al crear grupos. Estos permisos se han reemplazado por "roles y directivas de acceso", que le dan más flexibilidad para proporcionar permisos basados en roles a los usuarios. En la siguiente tabla se muestra cómo se asignan los permisos de la versión 12.0 a la versión 13.0:

| 12.0 | Permitir solo aplicaciones | 13.0 |
|---|---|---|
| admin read-write | False | `admin` |
| admin read-write | True | `appAdmin` |
| admin read-only | False | `readonly` |
| admin read-only | True | `appReadonly` |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configurar roles

January 30, 2024

En Citrix Application Delivery Management (ADM), cada función está vinculada a una o más directivas de acceso. Puede definir relaciones uno a uno, uno a varios y muchos a muchos entre directivas y roles. Puede vincular un rol a varias directivas y puede vincular varios roles a una directiva.

Por ejemplo, un rol puede estar enlazado a dos directivas, con una directiva que defina los permisos de acceso para una función y la otra que defina los permisos de acceso para otra función. Una directiva puede conceder permiso para agregar instancias de Citrix ADC en Citrix ADM y la otra directiva puede conceder permiso para crear e implementar StyleBooks y configurar instancias de Citrix ADC.

Cuando varias directivas definen permisos de edición y solo lectura para una sola función, los permisos de edición tienen prioridad.

Citrix ADM proporciona cuatro funciones predefinidas:

- **administrador**. Tiene acceso a todas las funciones de Citrix ADM. (Este rol está vinculado a adminpolicy).
- **solo lectura**. Tiene acceso de solo lectura. (Este rol está vinculado a readonlypolicy).
- **appAdmin**. Tiene acceso administrativo solo a las funciones de la aplicación en Citrix ADM. (Este rol está vinculado a appAdminPolicy).
- **appReadonly**. Tiene acceso de solo lectura a las funciones de la aplicación. (Este rol está vinculado a appReadOnlyPolicy).

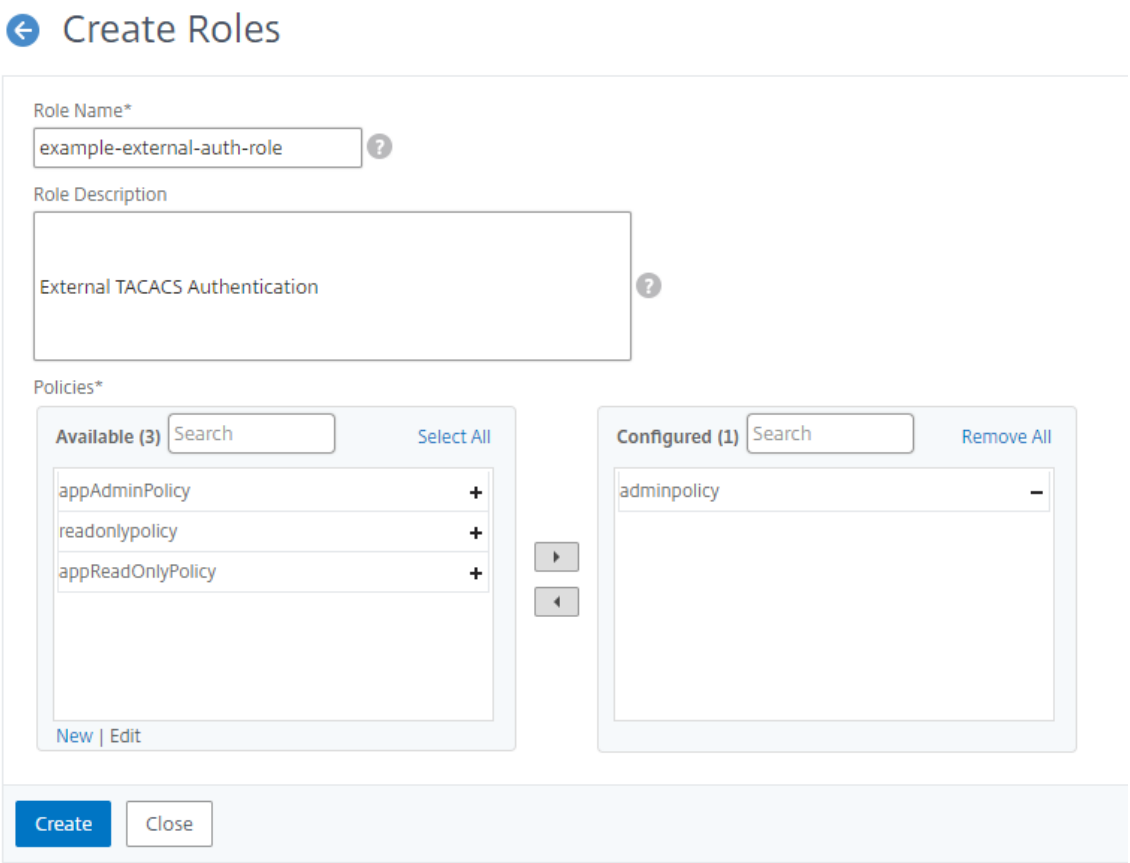
> **Nota:** Los roles predefinidos no se pueden modificar.

También puede crear sus propios roles (definidos por el usuario).

**Para crear roles y asignarles directivas:**

1. En Citrix ADM, vaya a **Sistema** > **Administración de usuarios** > **Funciones**.
2. Haga clic en **Agregar**.
3. En el campo **Nombre del rol**, introduzca el nombre del rol y proporcione la descripción en el campo **Descripción del rol** (opcional).
4. En la sección **Directivas**, agregue o mueva una o más directivas a la lista **Configurados**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Haga clic en **Crear**.

## Configurar usuarios

January 30, 2024

De forma predeterminada, Citrix Application Delivery Management (ADM) tiene un usuario:

nsroot: el usuario root (nsroot) tiene todos los privilegios administrativos en el dispositivo. El usuario nsroot es el superadministrador de Citrix ADM.

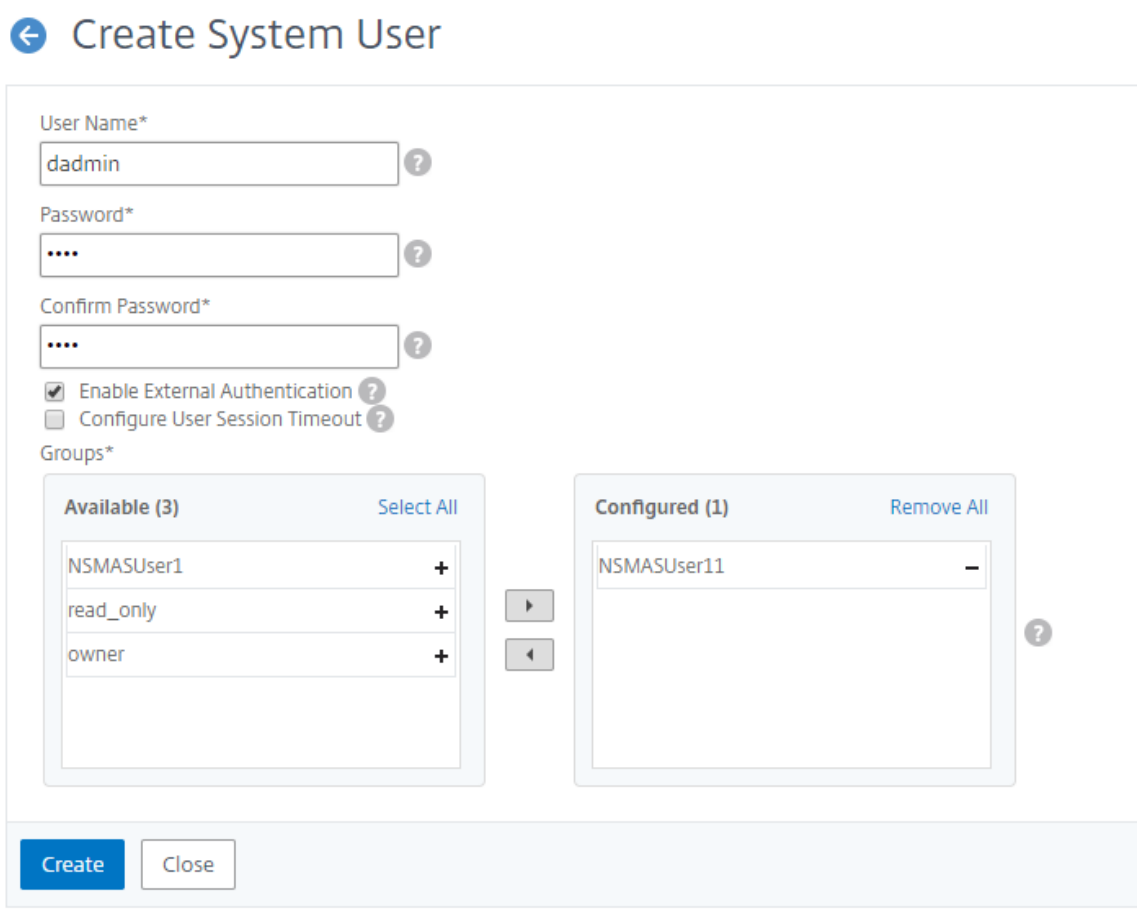
Puede crear usuarios adicionales configurando cuentas para ellos. Cuando agrega nuevos usuarios a Citrix ADM, puede definir sus permisos asignando los grupos, funciones y directivas adecuados.

Puede asignar un usuario a un grupo y vincular el grupo a roles. Puede definir una relación de uno a uno, de uno a muchos o de muchos a muchos entre los usuarios, los grupos, las funciones y las directivas de acceso. Se puede asignar un usuario a varios grupos. Un grupo puede tener varias funciones y varios grupos pueden tener funciones idénticas.

**Para configurar usuarios en Citrix ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix ADM, vaya a **Sistema** > **Administración** de **usuarios > Usuarios**.
2. Haga clic en **Agregar**.
3. Introduzca los siguientes detalles:
   a) **Nombre de usuario**. Nombre del usuario
   b) **Contraseña**. Contraseña con la que el usuario inicia sesión en Citrix ADM
4. Si lo quiere, seleccione **Habilitar la autenticación externa**para que el usuario pueda autenticarse a través de un servidor de autenticación externo.
5. Si ha creado grupos y quiere asignar al usuario a un grupo, en la sección **Grupos**, mueva uno o más grupos de la lista **Disponible** a la lista **Configurada**.




6. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Aplicaciones

January 30, 2024

La función de análisis y administración de aplicaciones de NetScaler ADM le permite supervisar las aplicaciones mediante un enfoque centrado en las aplicaciones. Este enfoque le ayuda a:

- Compruebe la puntuación y analice el rendimiento general de las aplicaciones
- Compruebe si hay algún problema que persista con el servidor o el cliente
- Detecte anomalías en los flujos de tráfico de la aplicación y tome medidas correctivas

> **Nota**
>
> Las aplicaciones hacen referencia a uno o más servidores virtuales que están configurados en las instancias (NetScaler ADC).

Puede supervisar las aplicaciones durante el tiempo que dure, por ejemplo, 1 hora, 1 día, 1 semana y 1 mes.

## Requisitos previos

- Asegúrese de haber agregado instancias de NetScaler ADC en NetScaler ADM
- Asegúrese de tener una licencia válida para sus instancias NetScaler ADC. Para obtener más información, consulte Licencias
- Asegúrese de haber aplicado una licencia para servidores virtuales. Para obtener más información, consulte Administrar licencias en servidores virtuales

## Descripción general de la aplicación

Las aplicaciones pueden ser:

- Aplicaciones discretas
- Aplicaciones personalizadas
- Aplicaciones de microservicios (k8s_discrete)

## Aplicaciones discretas

Todos los servidores virtuales con licencia se denominan aplicaciones discretas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Aplicaciones personalizadas

Los servidores virtuales de una categoría se denominan aplicaciones personalizadas. Como administrador, debe agregar aplicaciones personalizadas basadas en una categoría. A continuación, puede gestionar y supervisar las aplicaciones a través del panel de control. Obtiene la facilidad de supervisar aplicaciones específicas que se agrupan en una categoría.

Por ejemplo, puede crear una categoría para su centro de datos1 y agregar sus instancias de ADC. Tras definir una categoría y agregar la instancia para el centro de datos1, el panel de la aplicación se muestra con una categoría independiente, que incluye todas las aplicaciones relacionadas con el centro de datos1.

#### Puntos que tener en cuenta

- Las aplicaciones discretas que se agregan a las aplicaciones personalizadas se eliminan de las aplicaciones discretas.
- Todas las aplicaciones que no se agregan a ninguna categoría están disponibles como **"otras"**.
- De forma predeterminada, NetScaler ADM le permite agregar licencias para hasta 2 aplicaciones. Dependiendo de su licencia, puede seleccionar y aplicar licencias para las aplicaciones que quiere supervisar.

### Aplicaciones de microservicios

En un clúster de Kubernetes, Citrix proporciona un Ingress Controller para NetScaler ADC MPX (hardware), NetScaler ADC VPX (virtualizado) y NetScaler ADC CPX (contenedor). Para obtener más información, consulte Citrix Ingress Controller.

Las aplicaciones discretas que se configuran mediante las instancias de NetScaler ADC CPX se denominan aplicaciones de microservicios.

## Administración de aplicaciones y panel de aplicaciones

January 30, 2024

Citrix ADM le permite administrar aplicaciones desde **la**página Aplicaciones y ver los detalles de las aplicaciones desde la página **Panel** de control .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Administración de aplicaciones

La página **Aplicaciones** le permite ver todas las aplicaciones personalizadas y discretas.

En la página **Aplicaciones**, como administrador, puede:

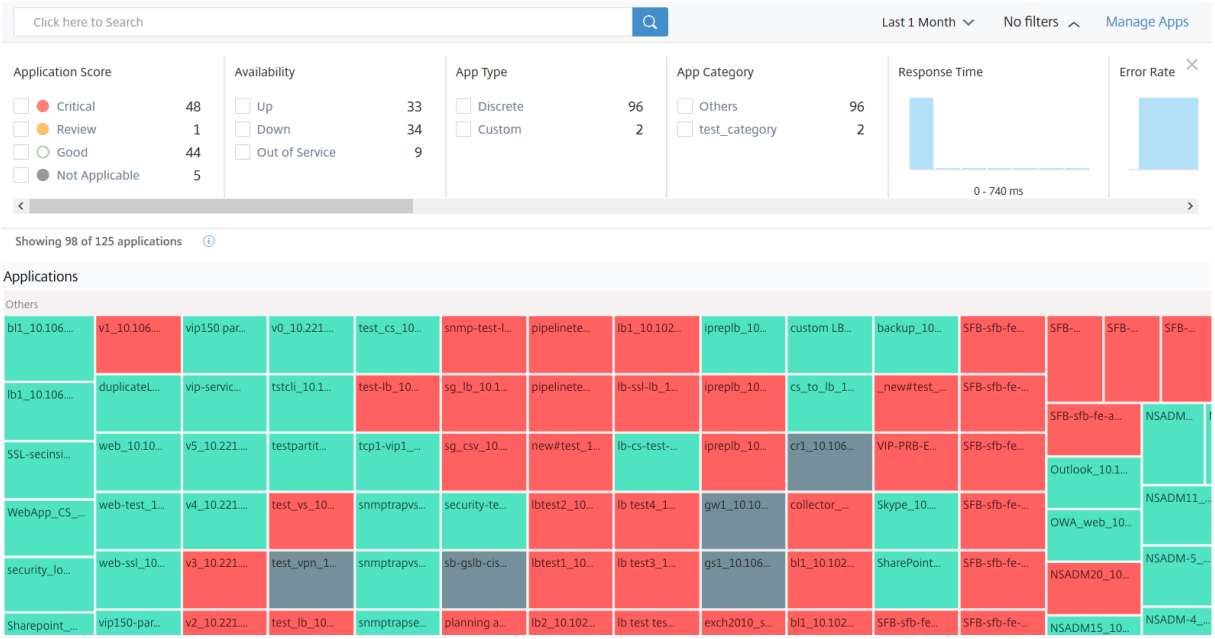
- Agregar aplicaciones
- Vea los detalles de la aplicación, como el nombre de la aplicación, el tipo de aplicación, la categoría de la aplicación, los servidores virtuales asociados, los servicios asociados, etc.
- Modificar o eliminar aplicaciones personalizadas

Después de agregar, modificar o eliminar aplicaciones, los detalles se reflejan inmediatamente en la página Aplicaciones.

Para obtener más información, consulte Administrar aplicaciones.

## Panel de aplicaciones

Vaya a **Aplicaciones** > **Panel de control** para ver la lista de aplicaciones en la vista tabular o en la vista gráfica.




Todas las aplicaciones se muestran en el panel de control solo después de que las aplicaciones comiencen a rellenar los datos. En el panel de control, haga clic en una aplicación para ver información detallada sobre el rendimiento de la aplicación. Para obtener más información, consulte Detalles de la solicitud.

Si el análisis de la aplicación no se muestra incluso después de una duración aproximada de 10 a 15 minutos, lleve a cabo los pasos de solución de problemas en el panel de control de la aplicación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Actualizaciones en el nuevo comportamiento del panel en comparación con el panel anterior**

- Después de agregar o modificar una aplicación personalizada, es posible que la aplicación tarde unos minutos en reflejarse en el panel de control.
- Si elimina una aplicación personalizada, el panel seguirá mostrando la aplicación eliminada hasta que ADM disponga de sus datos de análisis (duración máxima de un mes).

  Supongamos que creó una aplicación el 2 de enero de 2020 y la eliminó el 4 de enero de 2020. En este caso:

  - El panel de control aún puede mostrar la aplicación eliminada el 4 de enero de 2020, cuando selecciona la duración del último día, 1 semana y 1 mes.
  - El panel de control aún puede mostrar la aplicación eliminada el 5 de enero de 2020, si seleccionas la duración de la última semana y el último mes.
  - Cuando la duración excede la fecha de eliminación de la aplicación, la aplicación no se muestra en el panel. Es decir, el panel no se muestra con la aplicación eliminada el 6 de enero de 2020 (durante el último día), el 12 de enero de 2020 (durante la última semana) y después del 5 de febrero de 2020 (durante el último mes).

    > **Nota**
    >
    > Después de agregar una aplicación, si la instancia de NetScaler ADC asociada está inactiva, fuera de servicio o no se puede acceder a ella debido a un error temporal en la red:
    >
    > -Las aplicaciones asociadas a la instancia de ADC solo están visibles en la página **Aplicaciones**, pero no en el panel de control.
    >
    > - Las aplicaciones se muestran en el panel después de que la instancia de ADC esté activa y en ejecución.

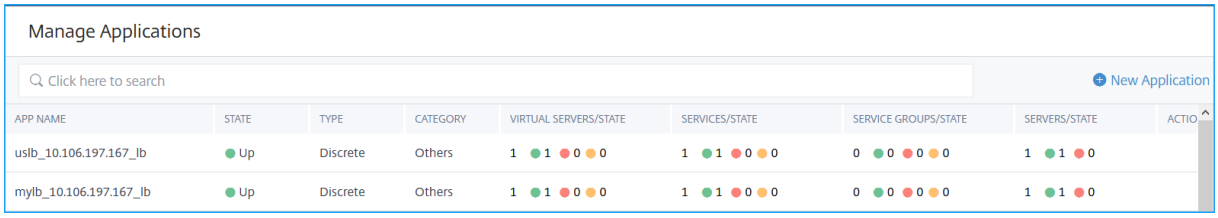
## Administración de aplicaciones

January 30, 2024

En el panel de control, haga clic en **Administrar aplicaciones** para ver los detalles de la aplicación y agregar, modificar o eliminar aplicaciones personalizadas.

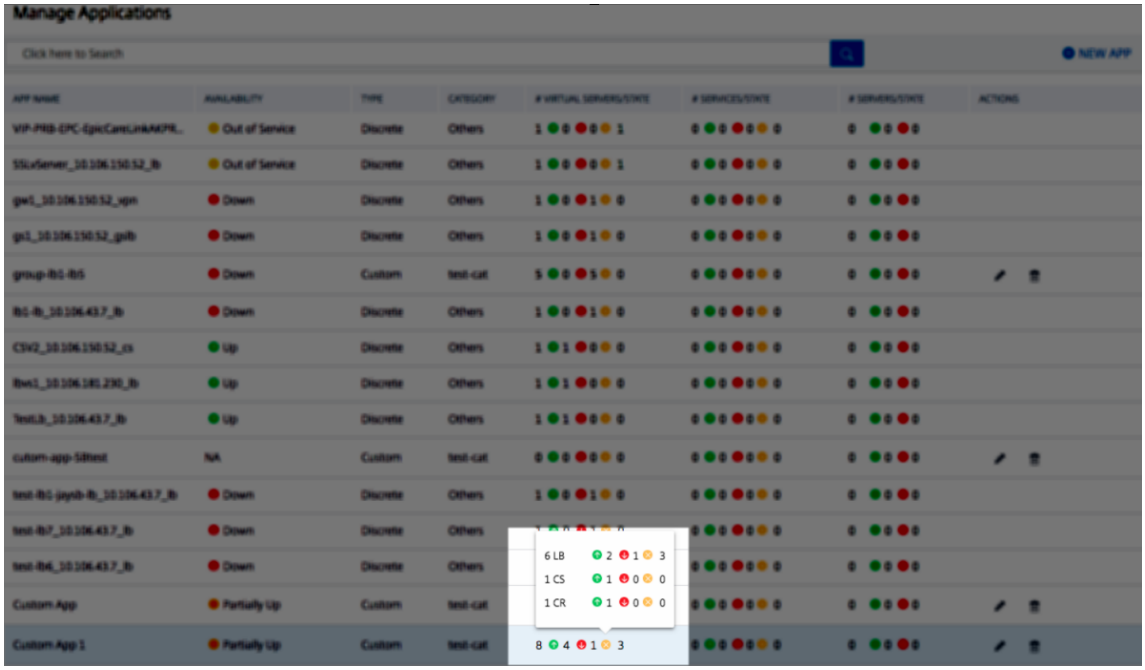
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Ver detalles de la aplicación




- **Nombre de la aplicación**: Indica el nombre de la aplicación
- **Disponibilidad**: Indica la disponibilidad actual de la aplicación, como **Activo**, **Inactivo**, **Parcialmente Activo**, **Fuera de Servicio** y **NA**
  - **Activo**: Todos los servidores virtuales asociados a la aplicación están activos.
  - **Inactivo**: Todos los servidores virtuales asociados a la aplicación están inactivos
  - **Parcialmente activo**: Uno de los dispositivos virtuales asociados a la aplicación está inactivo o fuera de servicio
  - **Fuera de servicio**: todos los servidores virtuales asociados a las aplicaciones están fuera de servicio
  - **NA**: no hay ningún servidor virtual configurado para la aplicación
- **Tipo**: indica si la aplicación pertenece a Custom o Discrete
- **Categoría**: Indica la categoría de aplicación que está agrupada
- **Servidor/estado virtual**: Indica el total de servidores virtuales configurados y el estado actual de todos los servidores virtuales. Sitúe el puntero del mouse (mouse) para ver los detalles, como el total de servidores virtuales, el tipo de servidor virtual y el estado del servidor virtual

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



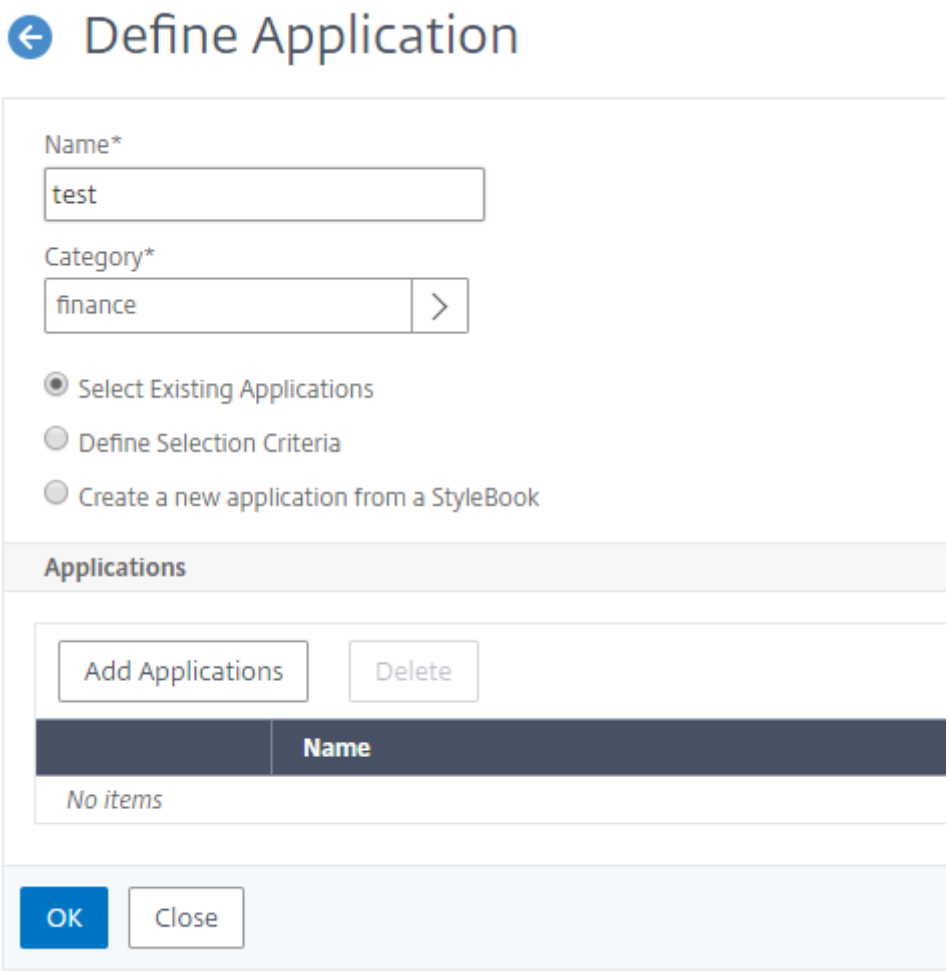

- **Servicios/estado**: Indica el total de servicios configurados y el estado actual de todos los servicios.
- **Grupos de servicios/estado**: Indica el total de grupos de servicios configurados y el estado de todos los grupos de servicios
- **Servidores/estado**: Indica el total de servidores configurados para la aplicación y el estado actual de todos los servidores
- **Acciones**: Permite modificar o eliminar las aplicaciones personalizadas

## Agregar una aplicación

1. Haga clic en **Nueva aplicación** para crear una nueva aplicación

   Aparece la página **Definir aplicación**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota:**
>
> También puede hacer clic en **Aplicaciones** y, a continuación, seleccionar **Nueva aplicación** para agregar una nueva aplicación.

2. Defina los siguientes parámetros:

| Campo | Descripción |
|---|---|
| Nombre | Nombre de la aplicación personalizada. Por ejemplo, LB_TEST. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Campo | Descripción |
| --- | --- |
| Categoría | La categoría en la que puede agrupar las aplicaciones. Haga clic para acceder a la página de categorías de aplicaciones. Seleccione la categoría y haga clic en **Seleccionar**. Para agregar una categoría<br>a) Haga clic en **Agregar**.<br>a) Introduzca un nombre de su elección.<br>a) Haga clic en **Crear**. |
| Seleccionar aplicaciones existentes | Le permite seleccionar las aplicaciones existentes agregadas a las instancias de NetScaler ADC. |
| Agregar aplicación | Muestra todos los servidores virtuales que están configurados en las instancias. Seleccione las aplicaciones de la lista y haga clic en **Aceptar**. |
| Definir criterios de selección | Opción para definir la aplicación por rango de servidores virtuales o por rango de direcciones IP de servidor/servicio de origen.<br>• **Servidor.** Especifique la dirección IP del servidor o servicio, el nombre del servidor o el puerto del servidor de fondo en el que se ejecutan las aplicaciones. Puede introducir una dirección IP, un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Campo | Descripción |
| --- | --- |
| | • **Servidores virtuales.** Puede especificar una de las siguientes opciones: la dirección IP del servidor virtual, el nombre del servidor virtual o el puerto del servidor de fondo en el que se ejecutan las aplicaciones. Puede introducir una dirección IP o un intervalo de direcciones IP o una combinación de ambas separadas por comas. Por ejemplo, puede escribir 10.102.29.20, 10.102.43.10-60, 10.216.43.45. |
| Crear una nueva aplicación a partir de un StyleBook | Permite crear una aplicación mediante el StyleBook. Para obtener más información, consulte Crear una aplicación con StyleBook. |

3. Haga clic en **Aceptar**.

> **Nota:**
>
> Actualmente, Application Dashboard solo admite servidores virtuales de equilibrio de carga y conmutación de contenido.

El panel de aplicación se muestra ahora con la categoría y todas las aplicaciones se agrupan debajo.

Si selecciona la opción **Crear una nueva aplicación a partir de un StyleBook** para la aplicación personalizada, debe permitir que Citrix ADM seleccione automáticamente los servidores virtuales para la concesión de licencias. Para habilitar la selección automática para los servidores virtuales:

a) Vaya a **Sistema** > **Licencias y análisis**.

b) En **Resumen de licencias de servidores virtuales** , haga clic en **Seleccionar**automáticamente servidores virtuales**y en Seleccionar automáticamente servidores virtuales no direccionables** para habilitarlos .

**Crear una aplicación mediante el StyleBook**

Para crear una aplicación mediante el StyleBook:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix ADM, vaya a **Aplicaciones** > **Panel** y haga clic en **Definir aplicación personalizada** para crear una aplicación personalizada.
2. En la página **Definir aplicación**, escriba el nombre de la aplicación en el campo **Nombre**.
3. Seleccione la categoría de la aplicación en la sección Categoría . NetScaler ADM permite definir categorías para agrupar las aplicaciones definidas por el usuario. También puede agregar más categorías si es necesario.
4. Haga clic para seleccionar **Crear una nueva aplicación a partir de un StyleBook** y haga clic en **Aceptar**.

   Aparece la página Elegir StyleBook. Esta página contiene todos los StyleBooks predeterminados disponibles en NetScaler ADM.
5. Seleccione el StyleBook.
   Aparece la página **Detalles de configuración**.
6. Introduzca los valores de todos los parámetros del StyleBook. También puede hacer clic en View Definition para ver la construcción del StyleBook antes de usarlo.

   Para obtener más información, consulte Usar StyleBooks predeterminados.
7. Haga clic en **Crear**.

   También puede hacer clic en **Ejecutar en seco** para comprobar las configuraciones que NetScaler ADM intenta crear en la instancia de NetScaler ADC seleccionada. Esta opción es solo para fines de prueba para ver la comprobación final de las configuraciones. Incluso si la opción Dry Run se ejecuta correctamente, es posible que la configuración real del NetScaler ADC seleccionado siga fallando por varios motivos (conflicto de IP, instancia no accesible, etc.).

## Modificar o eliminar una aplicación

Desde la página **Aplicaciones**, puede modificar o eliminar las aplicaciones personalizadas. Haga clic en el botón de edición para modificar una aplicación y haga clic en el botón de eliminar para eliminarla.

## Exportar informes del panel de aplicaciones y del panel de seguridad

NetScaler ADM le permite tomar una instantánea del panel de aplicaciones actual y exportarla como informes. En un intervalo de tiempo frecuente, es posible que los administradores de la aplicación necesiten usar estos informes para actualizar el uso de la aplicación y las sanciones de rendimiento.

Con esta función, los administradores pueden extraer estos datos como archivos.png,.jpeg o.pdf.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota:**
>
> A diferencia de otras opciones de exportación de informes de NetScaler ADM, puede exportar los informes de App Dashboard y Security Dashboard solo como archivos.pdf o png. El formato.csv no se admite actualmente.

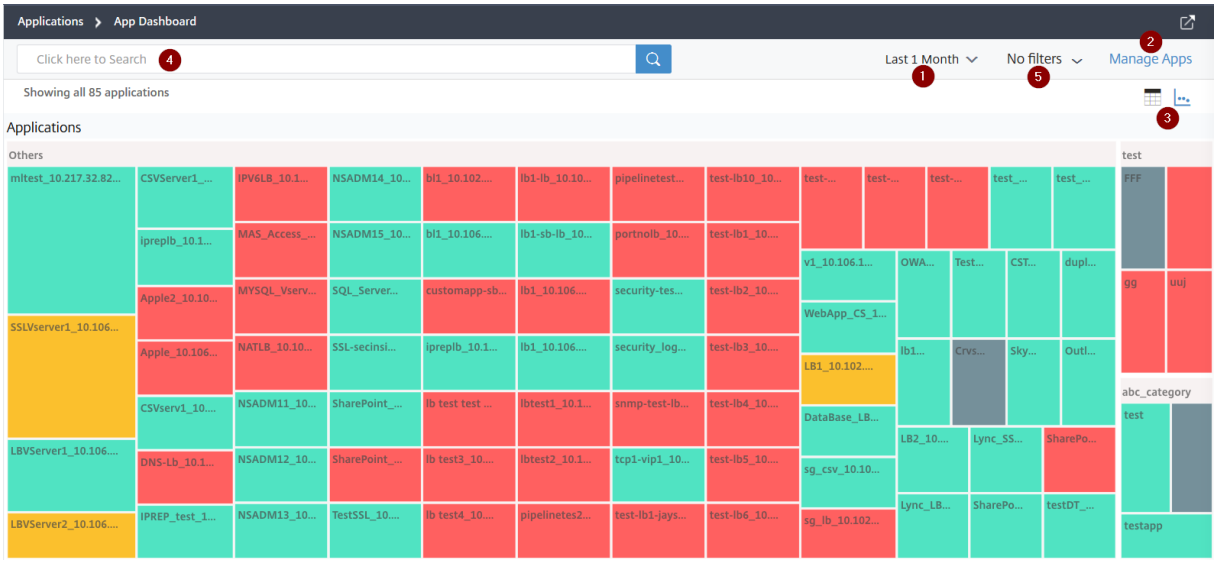
El informe se descarga en su sistema. Desde las páginas del panel de control de aplicaciones y del panel de seguridad de la aplicación, también puede navegar a páginas de segundo nivel y exportarlas como informes. Actualmente, puede descargar informes de una sola aplicación a la vez.

## Introducción al panel de aplicaciones

January 30, 2024

El panel de aplicaciones muestra las aplicaciones discretas en **Otros** y las aplicaciones personalizadas que se agrupan en sus respectivas categorías.

Ve a **Aplicación** > **Panel de control** para ver el panel de control de la aplicación.




**1**: Muestra los detalles de la aplicación para la duración seleccionada, como 1 hora, 1 día, 1 semana y 1 mes.

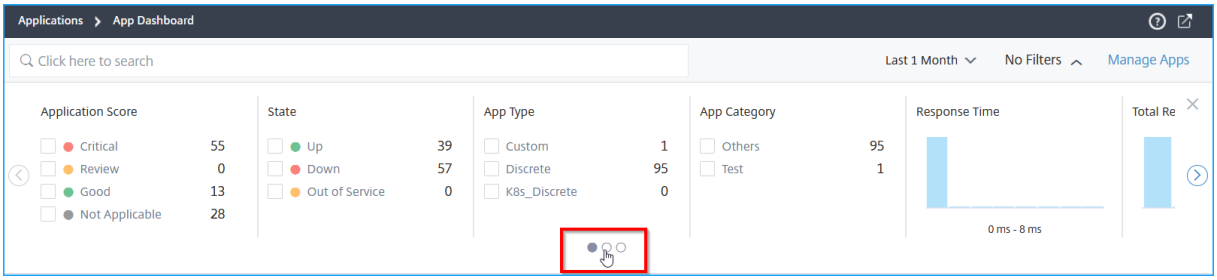
**2** —Le permite administrar aplicaciones y agregar nuevas aplicaciones

**3** —Le permite ver las aplicaciones en la vista de tabla o en la vista gráfica

**4** —Le permite buscar una aplicación mediante la barra de búsqueda

**5** —Le permite aplicar filtros para ver las aplicaciones. Haga clic para ver los detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

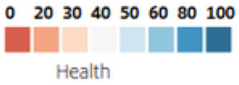



Puede seleccionar el deslizador del carrusel que le permite un acceso fácil a todas las opciones.

Puede hacer lo siguiente:

- Seleccione esta opción para ver las solicitudes en función de las puntuaciones.
  - **Crítico**: La puntuación de la aplicación está entre 0 y < 40
  - **Justo**: la puntuación de la solicitud está entre 40 y < 75
  - **Bueno**: La puntuación de la solicitud es superior a 75
  - **No aplicable**: No hay servidores virtuales configurados para la aplicación

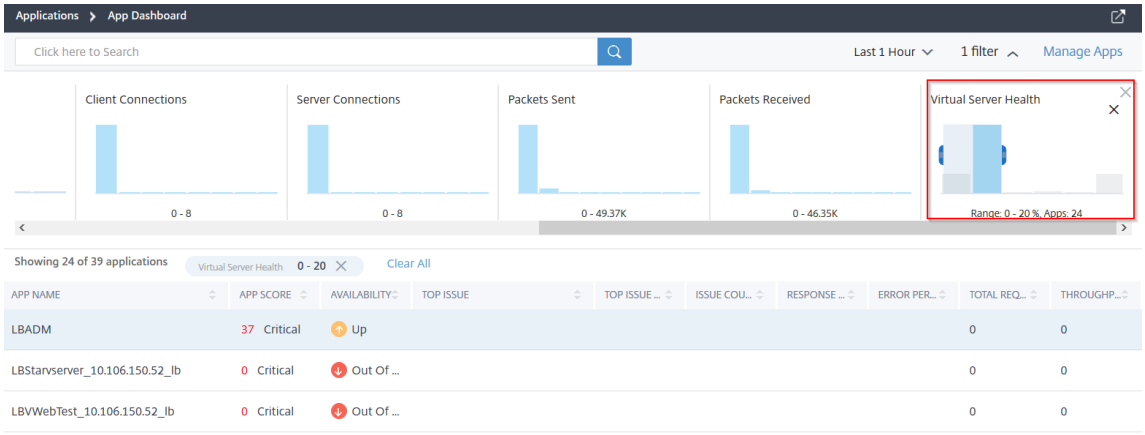
    En la siguiente tabla se describen las diferencias entre la puntuación de la aplicación anterior y la puntuación de la aplicación actual.

| Puntuación de la solicitud (crítica, revisada, buena, no aplicable) | Puntuación de la aplicación (vista anterior con leyendas de colores) |
|---|---|
| La puntuación se calcula como **100 menos la puntuación de penalización de todos los problemas actuales**de la<br>Las aplicaciones se muestran en colores como **Rojo (crítico)**, **Naranja (revisión)**, **Verde (bueno)** y **Gris (no aplicable)** | La puntuación se calcula como **100: (recurso del servidor de aplicación+recurso del sistema NetScaler ADC)**<br>Las aplicaciones se muestran en leyendas de color.   |

- Seleccione esta opción para ver las aplicaciones en función del estado de la aplicación, como Activo, Inactivo y Fuera de Servicio
- Seleccione esta opción para ver las aplicaciones según el tipo de aplicación, como Discreta o Personalizada.
- Seleccione esta opción para ver las aplicaciones según las categorías agrupadas debajo
- Arrastre el histograma para aplicar filtros y ver las aplicaciones.

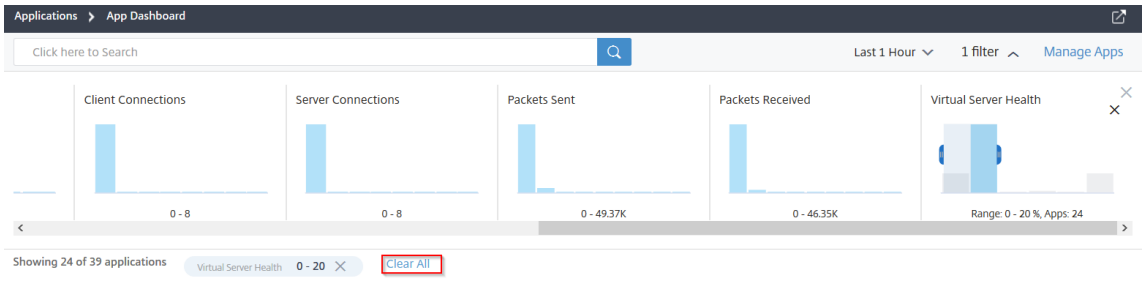
  Por ejemplo, si quiere ver aplicaciones que tienen estado del servidor virtual entre 0 y 20, arrastre el histograma de estado del servidor virtual para filtrar los resultados.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> También puede hacer clic en el histograma para ver las aplicaciones pertinentes.

Haga clic en **Borrar todo** para borrar el filtro aplicado.




A continuación se muestra el resumen de la aplicación para el que puede aplicar filtros:

- **Tiempo de respuesta**: Un histograma que muestra el tiempo de respuesta promedio recibido por las aplicaciones
- **Tasa de errores**: Un histograma que muestra el porcentaje de error promedio de 5xx errores para las aplicaciones
- **Solicitudes totales**: Un histograma que muestra el número total de solicitudes recibidas por las aplicaciones
- **Rendimiento**: Un histograma que muestra el rendimiento total de la red procesado por las aplicaciones
- **Volumen de datos**: Histograma que muestra el total de datos procesados por las aplicaciones. El volumen de datos se calcula mediante el total de bytes de solicitud y bytes de respuesta para las aplicaciones.
- **Conexiones de cliente**: Un histograma que muestra el promedio de conexiones de cliente establecidas por las aplicaciones
- **Conexiones al servidor**: Un histograma que muestra el promedio de conexiones al servidor establecidas por las aplicaciones

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Paquetes enviados**: Histograma que muestra el total de paquetes enviados por las aplicaciones.
- **Paquetes recibidos**: Un histograma que muestra el total de paquetes recibidos por las aplicaciones
- **Estado del servidor virtual**: Histograma que muestra el total de aplicaciones entre el rango de puntuación del 0% al 100%. El estado de un servidor virtual es (%) de los servicios activos asociados a la aplicación. Por ejemplo, si un servidor virtual está configurado con 2 servicios y si uno de ellos está inactivo, la puntuación es del 50%.

### Buscar y filtrar resultados mediante la barra de búsqueda

Puede colocar el puntero del mouse en la barra de búsqueda y seleccionar la categoría para refinar la búsqueda.

## Ver aplicaciones

January 30, 2024

De forma predeterminada, el panel de la aplicación muestra todas las aplicaciones. Según sus necesidades, puede utilizar la opción de filtro para ver las aplicaciones.

Showing 98 of 125 applications

| APP NAME | APP SCORE | AVAILABILITY | APP TYPE | APP CATEG... | TOP ISSUE | TOP ISSUE CATEGORY | ISSUE COU... | RESPONSE ... | ERROR PER... | TOTAL REQ... | THROUGHP... | DATA VOLU. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| web_10.107.98.70_lb | 85 Good | Up | Discrete | Others | Active Services Last Monday at 1:00 AM | Performance | 1 | 0 | 0% | 0 | 0 | 0 Bytes |
| web-test_10.107.98.70_lb | 85 Good | Up | Discrete | Others | Active Services Last Monday at 1:00 AM | Performance | 1 | 0 | 0% | 0 | 0 | 0 Bytes |
| web-ssl_10.107.98.70_lb | 85 Good | Up | Discrete | Others | Active Services Last Monday at 1:00 AM | Performance | 1 | 0 | 0% | 0 | 0 | 0 Bytes |

El panel muestra los siguientes detalles de la aplicación:

- **Nombre de la aplicación**: Indica el nombre de la aplicación
- **Puntuación de la aplicación**: Indica la puntuación de la aplicación y el estado, como **Crítica**, **Buena**, **Aceptable** y **No aplicable**
- **Disponibilidad**: Indica la disponibilidad actual de la aplicación, como **Activo**, **Inactivo**, **Parcialmente Activo**, **Fuera de Servicio** y **NA**
  - **Activo**: Todos los servidores virtuales asociados a la aplicación están activos.
  - **Inactivo**: Todos los servidores virtuales asociados a la aplicación están Inactivos.
  - **Parcialmente** activo: uno de los dispositivos virtuales asociados a la aplicación está inactivo o fuera de servicio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - **Fuera de servicio**: todos los servidores virtuales asociados a las aplicaciones están fuera de servicio.
  - **NA**: No hay servidores virtuales configurados para la aplicación.

- **Problema principal**: Indica el problema que tiene el número máximo de errores en la aplicación
- **Categoría de problema principal**: Indica la categoría del problema
- **Recuento de problemas**: Indica el número total de problemas de la aplicación
- **Tiempo de respuesta**: Indica el tiempo promedio de respuesta de la aplicación.
- **Porcentaje de error**: Indica el porcentaje de error total de 5xx errores de la aplicación

> **Nota**
>
> La métrica de porcentaje de error 5xx solo se muestra para **Citrix ADC 13.0 o posterior**. Para las versiones anteriores, el valor se muestra como **0**.

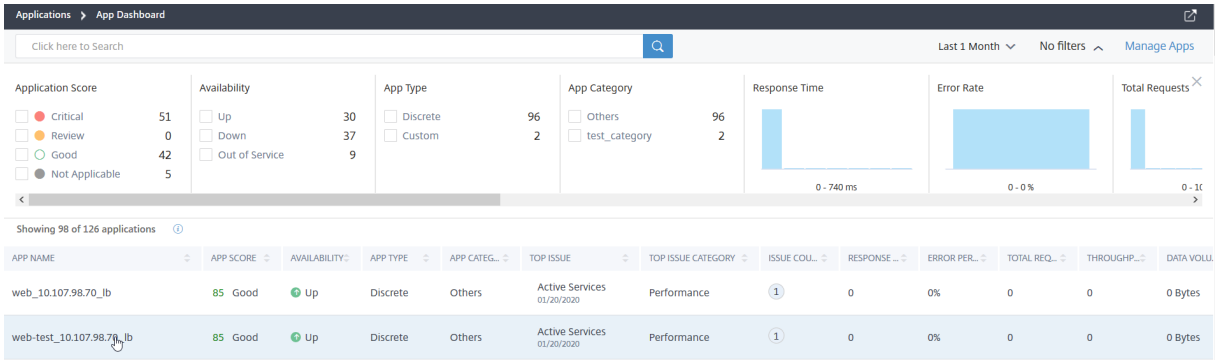
- **Solicitudes totales**: Indica el total de solicitudes recibidas por la aplicación
- **Rendimiento**: Denota el rendimiento total de la red de la aplicación. El rendimiento se calcula mediante los Req Bytes/Sec + Res Bytes/Sec para los servidores virtuales
- **Volumen de datos**: Indica el total de datos procesados por la aplicación
- **Conexiones de cliente**: Indica el promedio de conexiones de cliente establecidas por la aplicación.
- **Conexiones de servidor**: Indica el promedio de conexiones de servidor establecidas por la aplicación

## Detalles de la aplicación

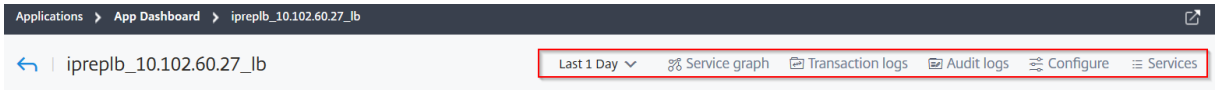
January 30, 2024

Haga clic en una aplicación del panel de control para obtener información más detallada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Se muestra la página de la aplicación seleccionada.

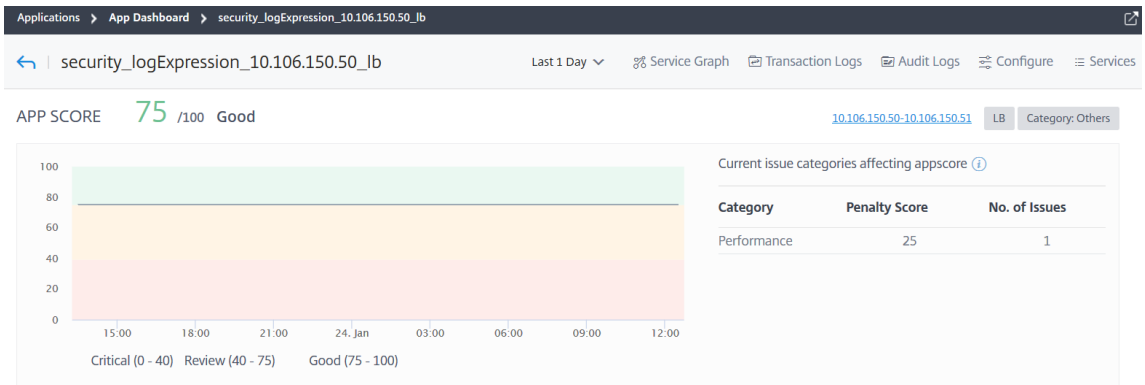



Desde la página de detalles de la solicitud:

- Seleccione la duración del tiempo de la lista para ver los detalles de la duración específica
- Haga clic en **Gráfico** de servicio para ver el gráfico de servicio de la aplicación seleccionada. Para obtener más información, consulte Service Graph for Applications
- Haga clic en **Registros** de transacciones para ver las transacciones detalladas de errores 5xx
- Haga clic en **Registros de auditoría** para ver la información detallada del registro de auditoría
- Haga clic en **Configurar** para ver o editar la configuración del servicio y del grupo de servicios de la aplicación
- Haga clic en **Servicio** para ver los servicios enlazados a la aplicación

Después de seleccionar la duración del tiempo, se muestran los siguientes detalles de la aplicación:

- **Puntuación de la aplicación**: La puntuación de la aplicación para la duración de tiempo seleccionada. La puntuación final se calcula como **100 menos la penalización total**.



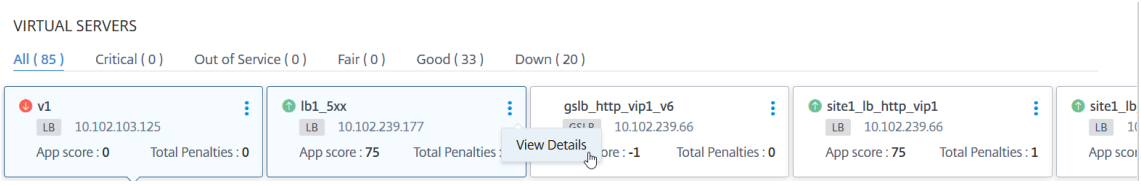

Este panel también le permite ver los problemas actuales que están afectando a la puntuación de la aplicación. Puede ver los detalles de los problemas en Problemas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

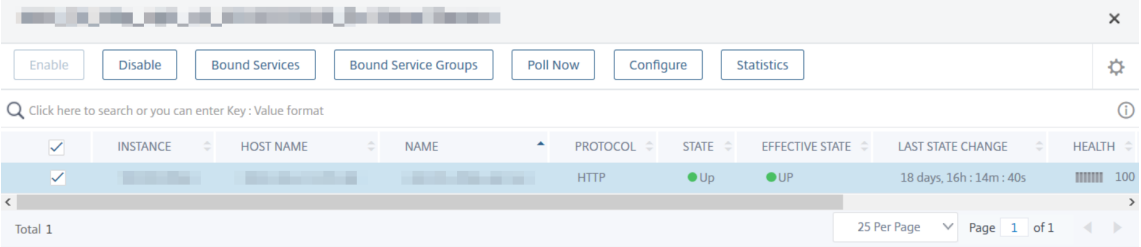
- **Servidores virtuales** —

> **Nota**
>
> La sección **Servidores virtuales** solo se muestra para las aplicaciones personalizadas. Para aplicaciones discretas, haga clic en la **dirección IP** para ver los detalles del servidor virtual.

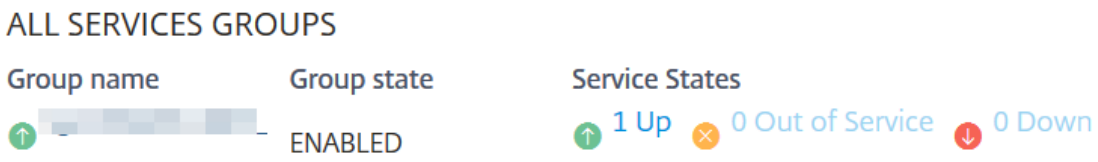
Muestra todos los servidores virtuales asociados a la aplicación personalizada



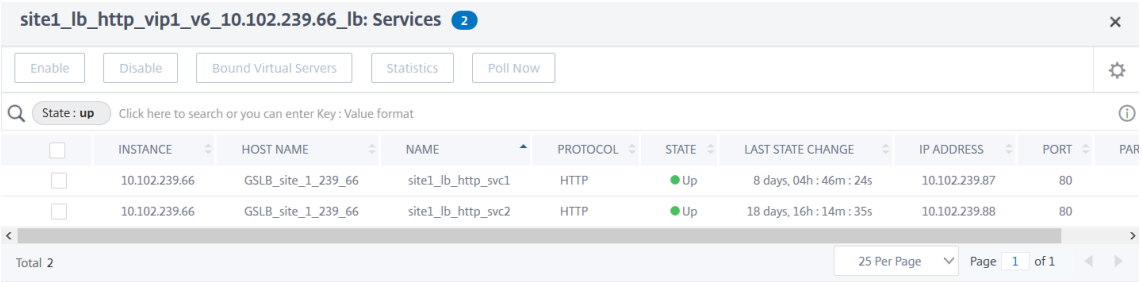

Haga clic en **Ver detalles** para ver y administrar la configuración del servidor virtual.




- **Todos los servicios**: los servicios que están vinculados a la aplicación




Haga clic para ver los detalles del servicio y administrar la configuración del servicio




- **Métricas**clave : los detalles de las métricas de la aplicación, como el **tiempo de respuesta de la aplicación**, el **porcentaje de errores** , las **solicitudes por segundo** , el **rendimiento** , el **total de conexiones** y el **volumen de datos** . Para las aplicaciones relacionadas con SSL, se muestran

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

más detalles de métricas, como **Hits de sesión**, **Velocidad de bytes cifrados, Velocidad de bytes descifrados**y**Nueva sesión SSL creada**.

> **Nota**
>
> La métrica de porcentaje de error 5xx solo se muestra para **Citrix ADC 13.0 o posterior**. Para las versiones anteriores, el valor se muestra como **0**.

En cada métrica, puede ver el valor medio y el valor de diferencia para la duración de tiempo seleccionada. El valor de la diferencia se calcula como el **primer valor menos el último valor** de la duración del tiempo seleccionado.

Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:

La siguiente imagen es un ejemplo de volumen de datos y la duración seleccionada es de 1 mes. El valor 202,66 MB es el volumen de datos total para el mes de duración y el valor 8,13 MB es el valor de la diferencia. En el gráfico, el primer valor es 14,11 y el último es 5,98. El valor de la diferencia es de 14,11 —5,98 = 8,13 MB.

Para aplicaciones relacionadas con SSL, puede ver las siguientes métricas adicionales:

- **Problemas**: Los problemas que son aplicables a la aplicación seleccionada. Puede ver los siguientes problemas junto con su categoría:

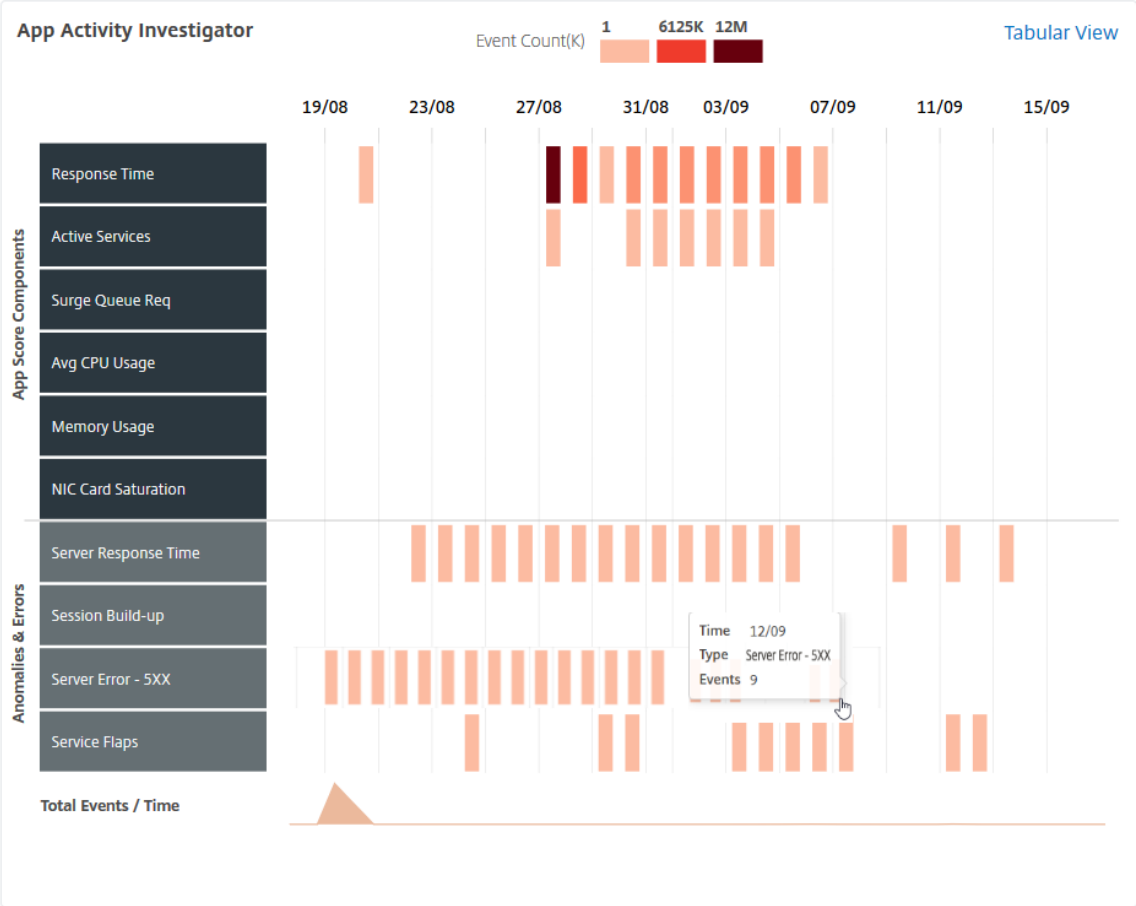
| Rendimiento | Estado de la instancia | Config | Recursos del sistema |
|---|---|---|---|
| Tiempo de respuesta | Uso medio de CPU | Servidor inestable | Tipo de persistencia incorrecto |
| Servicios Activos | Uso de memoria | Paquetes HTTP inusualmente grandes | Saturación de tarjeta NIC |
| Reutilización baja de sesiones | | TCP volver a ensamblar visitas de límite de cola | |
| Acumulación de colas de sobretensiones | | | |
| Tráfico en tiempo real SSL | | | |
| Acumulación de sesiones | | | |
| Solapas de servicio | | | |

Haga clic en cada problema para comprobar detalles como el mensaje de detección, cuándo se ha producido el problema, Acciones recomendadas y detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

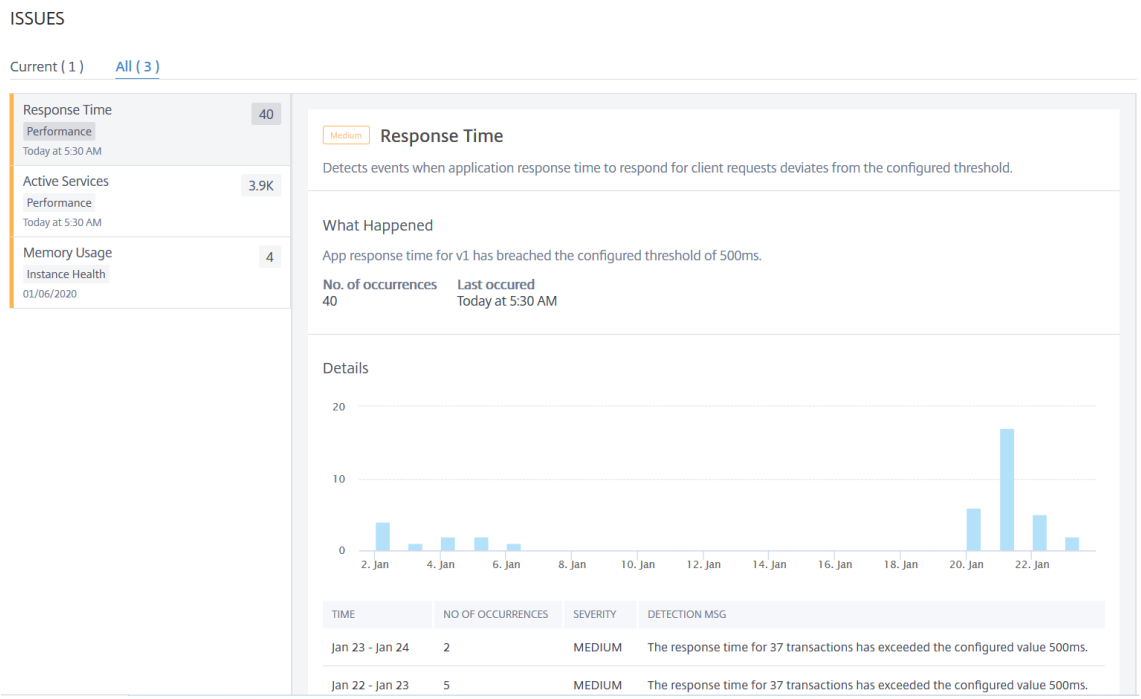
Para obtener más información, consulte Indicadores de rendimiento para análisis de aplicaciones.

La siguiente imagen es la vista anterior de la página App Activity Investigator :




Ahora puede ver todos los problemas en la sección **Problemas** , junto con la categoría que puede ver en la página **App Activity Investigator** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

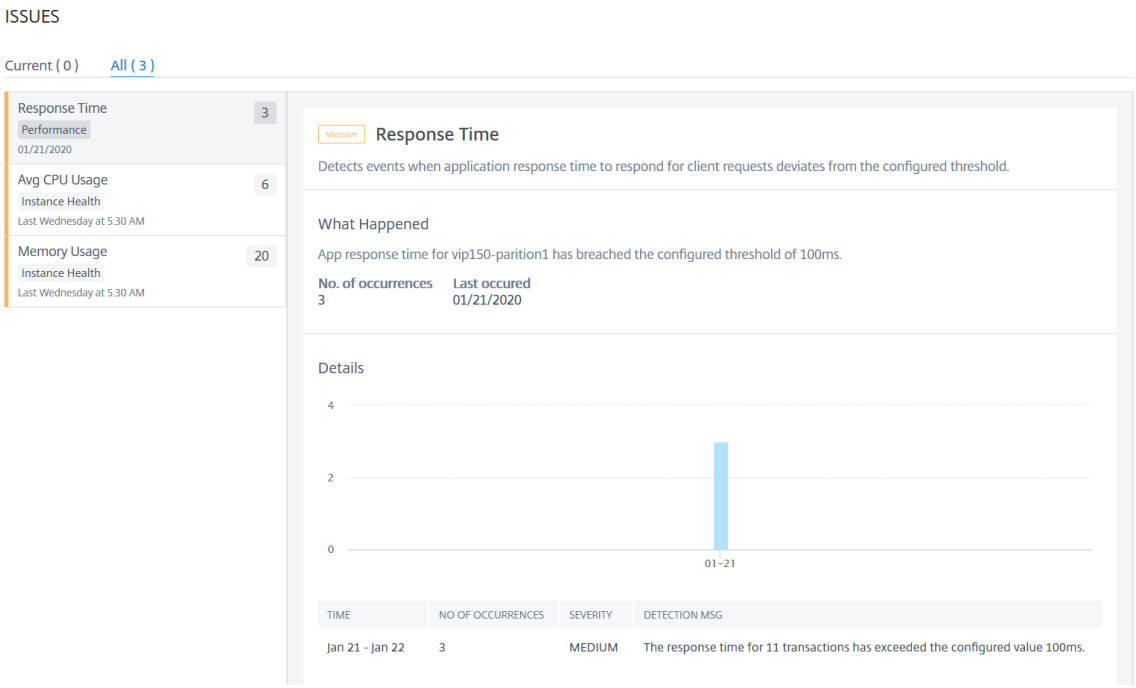



- Los problemas que aparecen en la ficha **Actual** se refieren a los problemas de la aplicación durante el tiempo seleccionado.
- Los problemas que aparecen en la ficha **Todos** se refieren a problemas totales de la aplicación.

El siguiente ejemplo son los problemas de la aplicación durante 1 día. La ficha **Actual** indica que no hay problemas actuales que afecten la puntuación de la aplicación.

La ficha **Todos** muestra el total de problemas detectados durante un día.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Seleccionar componentes de App Score y establecer umbrales

January 30, 2024

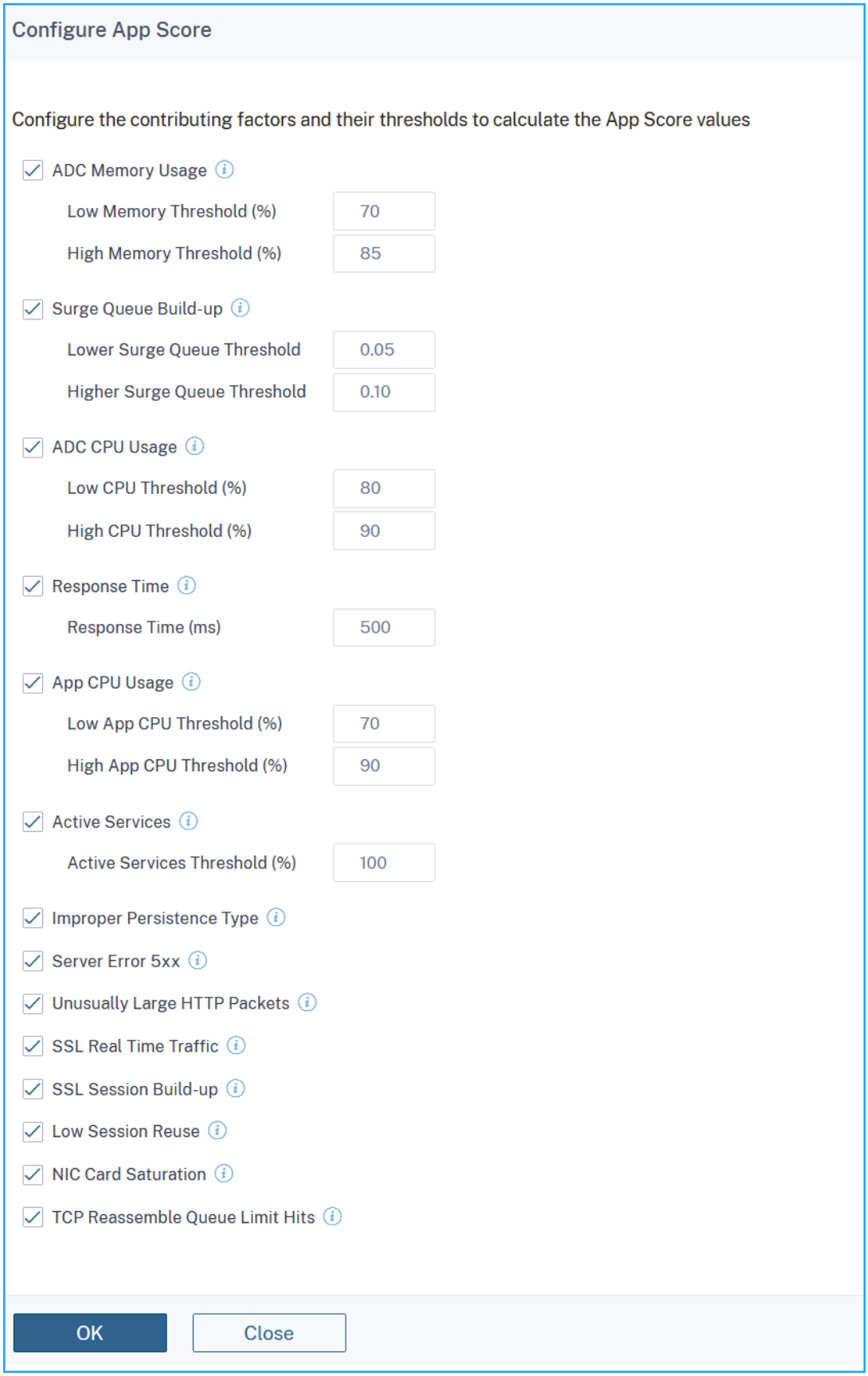
En el **Panel de aplicaciones**, como administrador, puede decidir seleccionar los componentes y configurar umbrales para el cálculo de puntuación de la aplicación. App Score es el sistema de puntuación que define:

- El funcionamiento de una aplicación
- Si la aplicación está funcionando bien en términos de capacidad de respuesta

Vaya a **Aplicaciones > Panel de control** y, a continuación, seleccione el icono de configuración.

En la página **Configurar puntuación de aplicaciones**, puede seleccionar los componentes y configurar umbrales para determinar la puntuación final de la aplicación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El cálculo de la puntuación de aplicaciones se basa en los siguientes componentes:

| Componentes de la puntuación de aplicaciones | Umbral configurado por el usuario | Descripción |
|---|---|---|
| Uso de memoria ADC | Sí | El valor umbral bajo y alto para el uso total de memoria en la instancia de NetScaler ADC |
| Acumulación de colas de sobretensión | Sí | El valor umbral bajo y alto para el total de solicitudes de aumento que están en cola y necesitan una respuesta. |
| Uso de CPU ADC | Sí | El valor umbral bajo y alto para el uso total de CPU en la instancia de NetScaler ADC. |
| Tiempo de respuesta | Sí | Intervalo de tiempo entre el envío de un paquete de solicitud y la recepción del primer paquete de respuesta del servicio configurado en el servidor virtual. |
| Uso de CPU de la aplicación | Sí | El valor umbral bajo y alto para el uso total de CPU por parte de la aplicación. |
| Servicios activos | Sí | Valor de umbral del porcentaje de servicios que deben estar activos que están enlazados al servidor virtual. |
| Tipo de persistencia incorrecto | No | Indica si el uso de persistencia en un servidor virtual es bajo. |
| Error del servidor (5xx) | No | Indica si el servidor web responde con errores 5xx. |
| Paquetes HTTP inusualmente grandes | No | Indica las ocurrencias si los mensajes HTTP con tamaño de encabezado HTTP superan los valores configurados en la instancia de NetScaler ADC. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Componentes de la puntuación de aplicaciones | Umbral configurado por el usuario | Descripción |
|---|---|---|
| Tráfico SSL en tiempo real | No | Analiza el tráfico SSL para identificar el tráfico en tiempo real y sugiere parámetros de configuración óptimos para mejorar la latencia. |
| Generación de sesiones SSL | No | Indica la acumulación de sesión durante un período de tiempo, lo que puede provocar que estas sesiones retienen una gran cantidad de memoria en la instancia de NetScaler ADC. |
| Baja reutilización de sesión | No | Indica si el número real de sesiones que reutiliza la instancia de NetScaler ADC es menor. |
| Saturación de tarjeta NIC | No | Indica el total de paquetes descartados por las interfaces. |
| TCP volver a ensamblar visitas de límite de cola | No | Indica si los paquetes fuera de orden en una conexión TCP superan el tamaño de cola de paquetes fuera de orden configurado. |

De manera predeterminada, se activan todos los componentes. Si inhabilita cualquier componente, NetScaler ADM realiza el cálculo de la puntuación final de la aplicación únicamente en función de los componentes seleccionados.

> Nota
>
> También puede continuar configurando umbrales navegando a **Analytics > Configuración** y haciendo clic en **Configurar puntuación de aplicación**.

## Detalles de aplicación para aplicaciones de microservicios

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Haga clic en una aplicación de microservicios del panel para profundizar para obtener más información detallada.

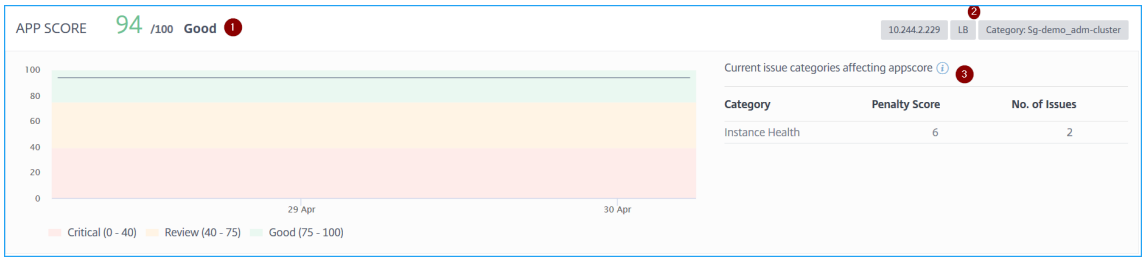
Se muestra la página de la aplicación seleccionada.

Desde la página de detalles de la solicitud:

- Seleccione la duración del tiempo de la lista para ver los detalles de la duración específica
- Haga clic en **Gráfico** de servicio para ver el gráfico de servicio de la aplicación seleccionada. Para obtener más información, consulte Service Graph for Applications
- Haga clic en **Registros** de transacciones para ver las transacciones detalladas de la aplicación seleccionada
- Haga clic en **Registros de auditoría** para ver la información detallada del registro de auditoría

Después de seleccionar la duración del tiempo, se muestran los siguientes detalles de la aplicación:

- **Puntuación de la aplicación**: La puntuación de la aplicación para la duración de tiempo seleccionada. También puede ver los problemas actuales de la aplicación, que se conoce como la puntuación de penalización aplicable en función de la categoría de emisión. La puntuación final se calcula como **100 menos la penalización total**.




**1** —Indica la puntuación actual de la aplicación

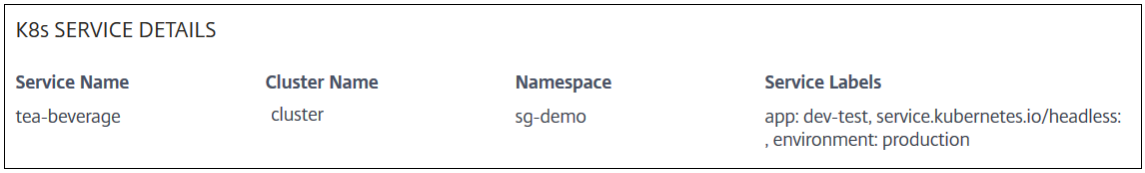
**2** —Indica la dirección IP de CPX, el tipo de aplicación, como el equilibrio de carga o el cambio de contenido, y el espacio de nombres del servicio y el nombre del clúster donde está alojado el servicio

**3** —Indica los problemas que afectan a la puntuación actual de la solicitud

Este panel también le permite ver los problemas actuales que están afectando a la puntuación de la aplicación. Puede ver los detalles de los problemas en Problemas.

- **Detalles del servicio K8s**

  Puede ver los siguientes detalles:

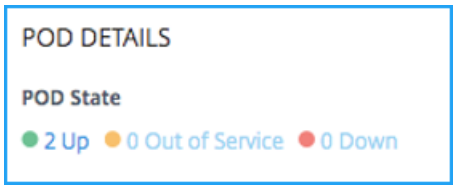



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

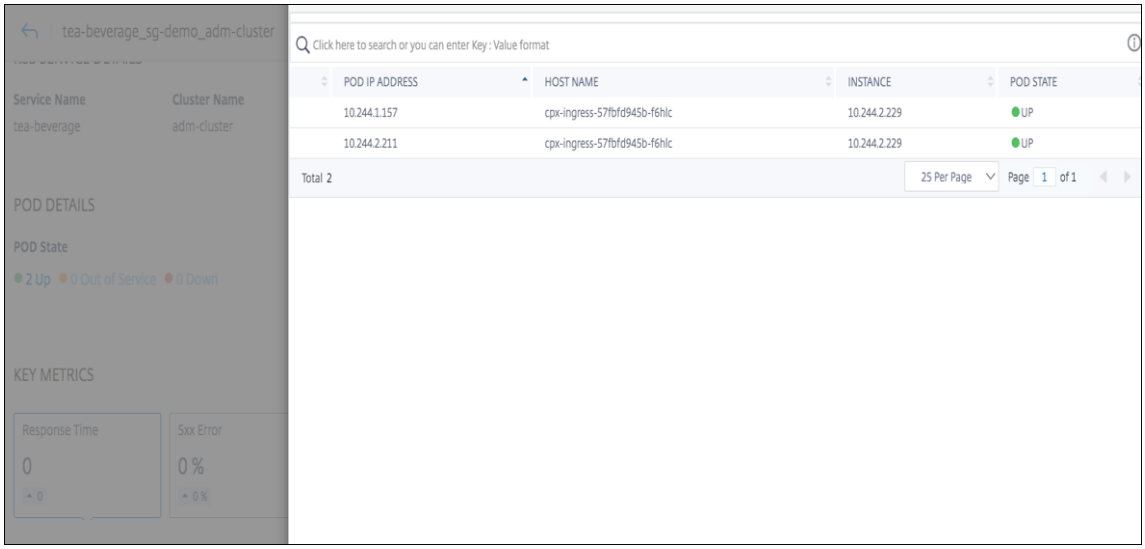
- **Nombre del servicio**: el nombre del servicio
- **Nombre del clúster: Nombre** del clúster en el que está alojado el servicio
- Espacio de**nombres**: el espacio de nombres asignado al servicio
- **Etiquetas de servicio**: las etiquetas de servicio asignadas al servicio

- **Detalles del pod**

  Un pod es un grupo de contenedores alojados en el clúster de Kubernetes. Dentro de un pod, puede implementar varias aplicaciones en contenedores. Cada pod está asociado a una dirección IP.




  Haga clic en el estado del pod para ver los detalles



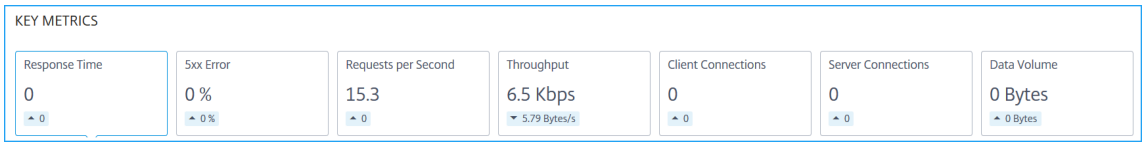

  - **Dirección IP del pod**: indica la dirección IP del pod
  - **Nombre de host**: indica el nombre de host asignado al pod
  - **Instancia**: indica la dirección IP CPX de NetScaler ADC
  - **Estado del POD**: indica el estado actual del pod

- **Métricas clave**: se muestran los detalles de las métricas clave, como el **tiempo de respuesta**, **5 veces los errores**, **las solicitudes por segundo**, el **rendimiento**, **las conexiones de los clientes**, **las conexiones del servidor**y el **volumen de datos**.

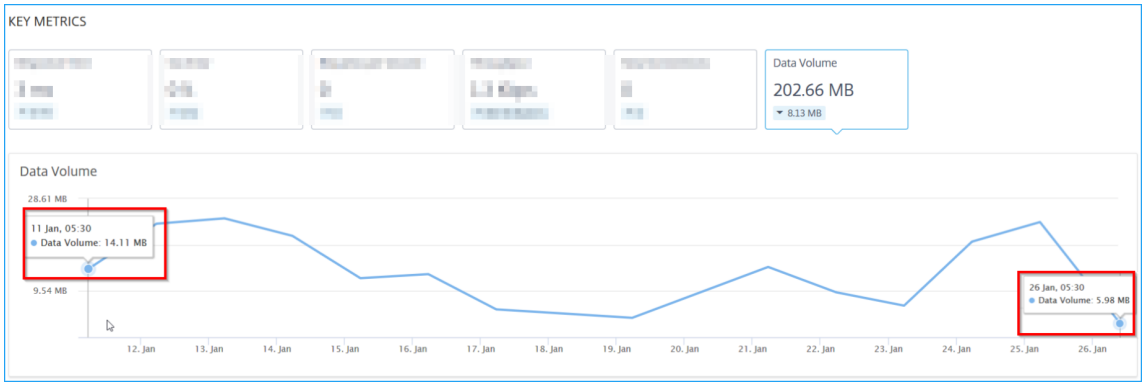
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En cada métrica, puede ver el valor medio y el valor de diferencia para la duración de tiempo seleccionada. El valor de la diferencia se calcula como el **primer valor menos el último valor** de la duración del tiempo seleccionado.

Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:




La siguiente imagen es un ejemplo de **volumen de datos** y la duración seleccionada es de 1 mes. El valor 202,66 MB es el volumen de datos total para el mes de duración y el valor 8,13 MB es el valor de la diferencia. En el gráfico, el primer valor es 14,11 y el último es 5,98. El valor de la diferencia es de 14,11 —5,98 = 8,13 MB.




- **Problemas**: Los problemas que son aplicables a la aplicación seleccionada. Puede ver los siguientes problemas junto con su categoría:

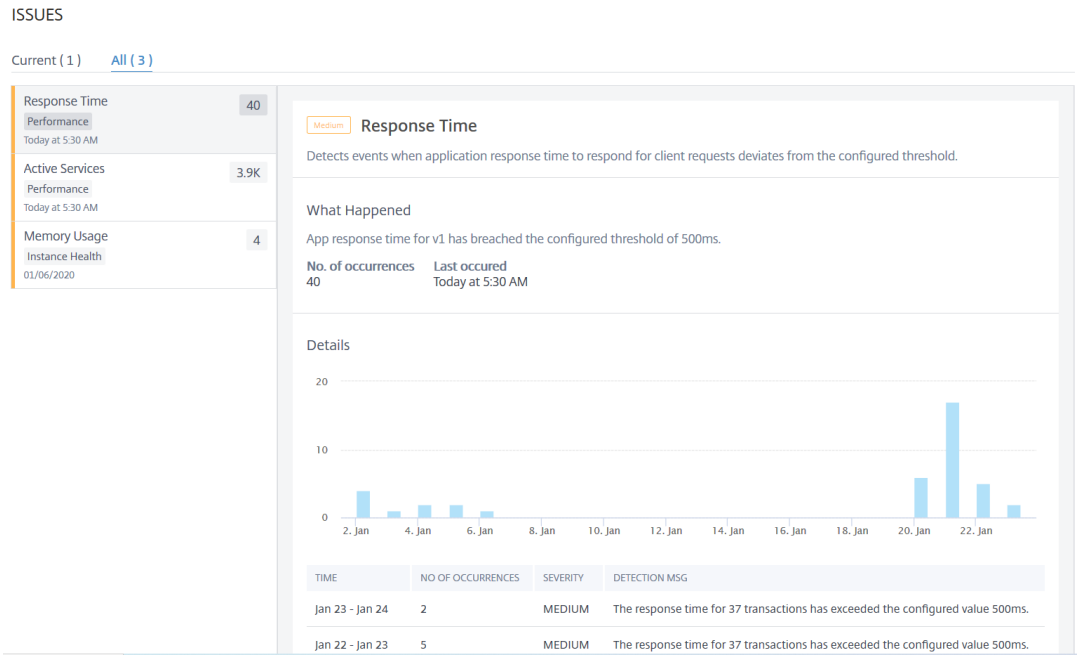
| Rendimiento | Estado de la instancia | Config | Recursos del sistema |
|---|---|---|---|
| Tiempo de respuesta | Uso medio de CPU | Alta respuesta 5xx | Tipo de persistencia incorrecto |
| Reutilización baja de sesiones | Uso de memoria | Paquetes HTTP inusualmente grandes | Saturación de tarjeta NIC |
| Acumulación de colas de sobretensiones | | TCP volver a ensamblar visitas de límite de cola | |
| Tráfico en tiempo real SSL | | | |

Haga clic en cada problema para ver la siguiente información:

- Total de ocurrencias

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Acciones recomendadas para solucionar el problema
- Los detalles del problema, como la hora, el nombre del servicio, el total de ocurrencias, la gravedad y el mensaje de detección

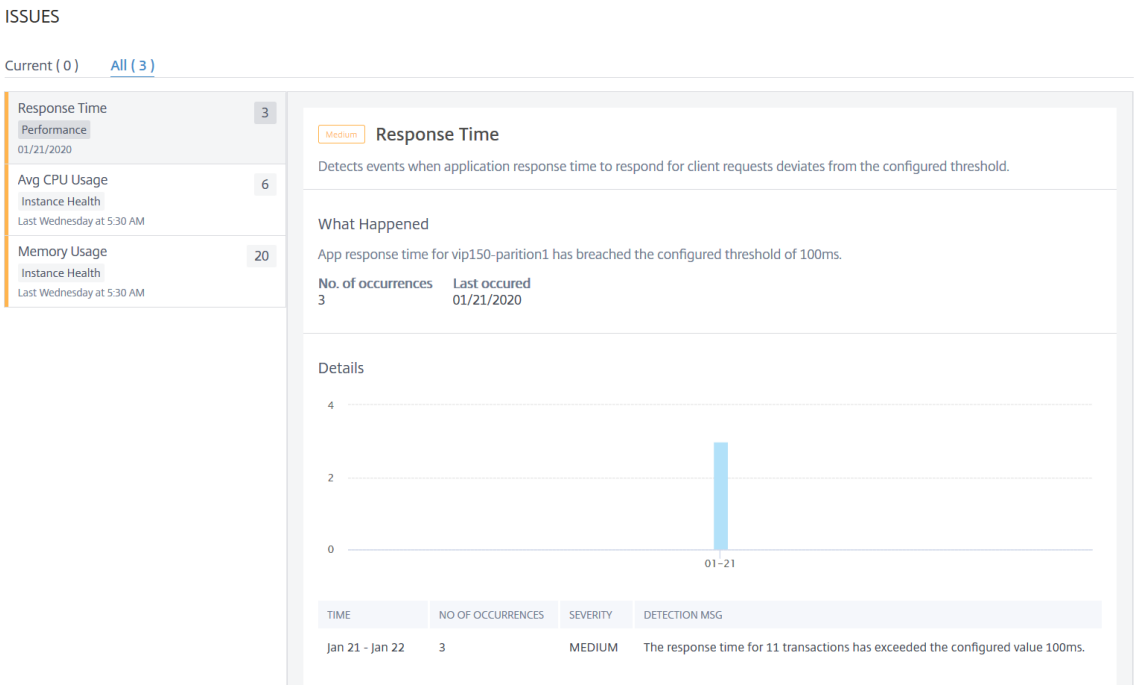



  * Los problemas que aparecen en la ficha **Actual** se refieren a los problemas de la aplicación durante el tiempo seleccionado.
  * Los problemas que aparecen en la ficha **Todos** se refieren a problemas totales de la aplicación.

El siguiente ejemplo son los problemas de la aplicación durante 1 día. La ficha **Actual** indica que no hay problemas actuales que afecten la puntuación de la aplicación.

La ficha **Todos** muestra el total de problemas detectados durante un día.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Panel de control Web Insight

January 30, 2024

La función de Web Insight mejorada se incrementa y proporciona visibilidad de métricas detalladas para aplicaciones web, clientes e instancias de NetScaler ADC. Esta Web Insight mejorada le permite evaluar y visualizar la aplicación completa desde las perspectivas de rendimiento y uso juntos. Como administrador, puede ver Web Insight para:

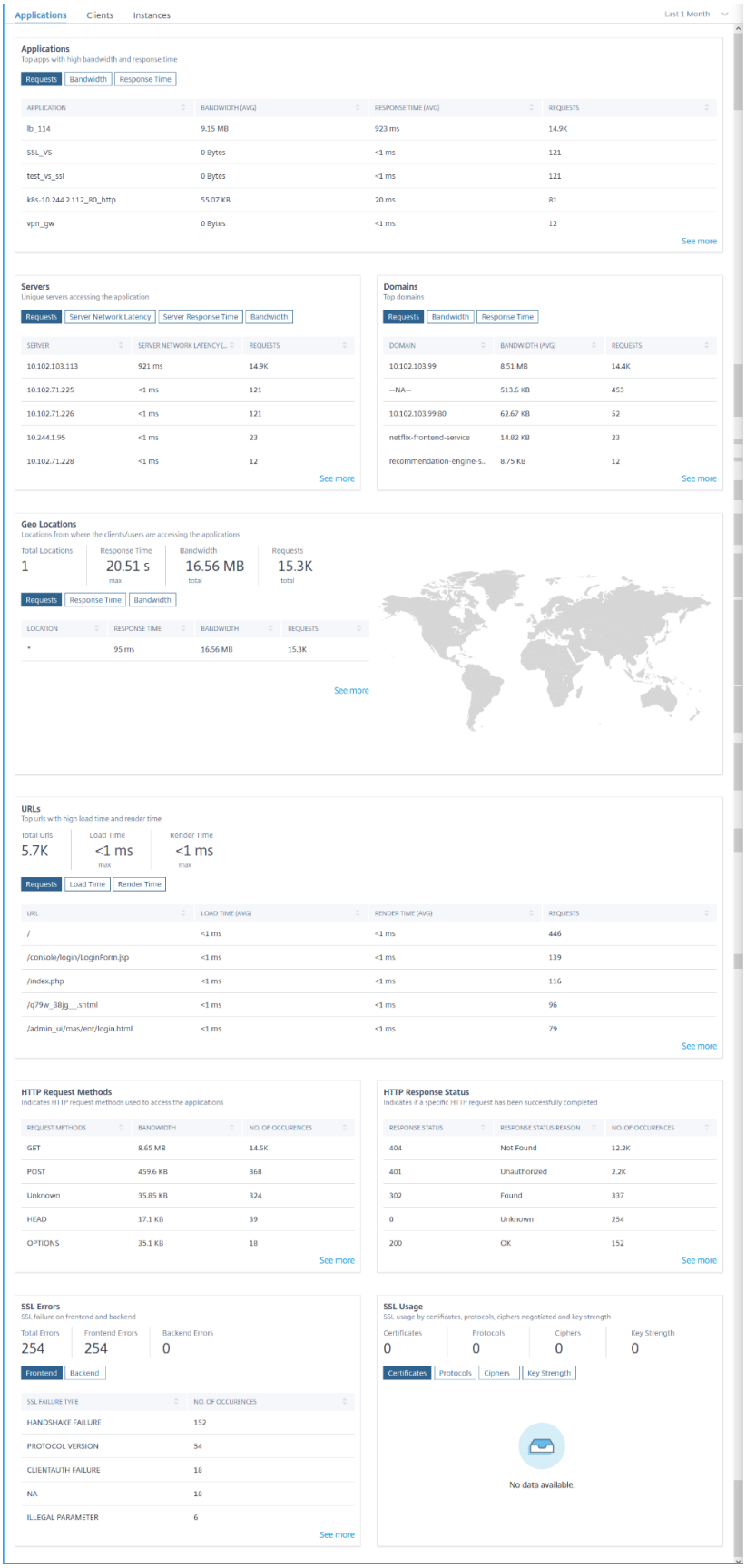
- Una aplicación. Vaya a **Aplicaciones > Panel**, haga clic en una aplicación y seleccione la ficha **Web Insight** para ver las métricas detalladas. Para obtener más información, consulte Análisis de uso de aplicaciones.
- Todas las aplicaciones. Vaya a **Aplicaciones > Web Insight** y haga clic en cada ficha (Aplicaciones, Clientes, Instancias) para ver las siguientes métricas:

| Aplicaciones | Clientes | Instancias |
|---|---|---|
| Aplicaciones | Clientes | Métricas de Instancia |
| Servidores | Ubicaciones geográficas | Aplicaciones |
| Dominios | Métodos de solicitud HTTP | Dominios |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Aplicaciones | Clientes | Instancias |
|---|---|---|
| Ubicaciones geográficas | Estado de respuesta HTTP | URLs |
| URLs | URLs | Métodos de solicitud HTTP |
| Métodos de solicitud HTTP | Sistema operativo | Estado de respuesta HTTP |
| Estado de respuesta HTTP | Exploradores web | Clientes |
| Errores SSL | Errores SSL | Servidores |
| Uso SSL | Uso SSL | Sistema operativo |
| | | Exploradores web |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

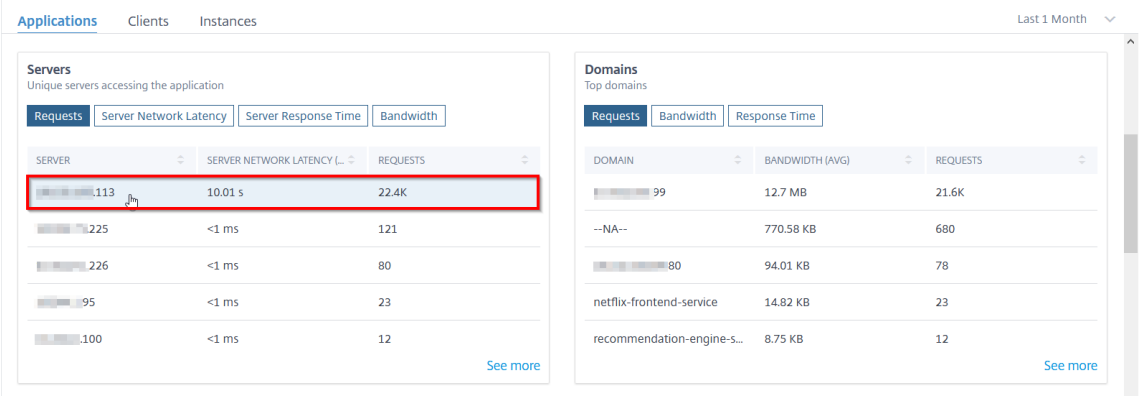



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En cada métrica, puede ver los 5 resultados principales. Puede hacer clic para profundizar más para analizar el problema y realizar acciones de solución de problemas más rápido.

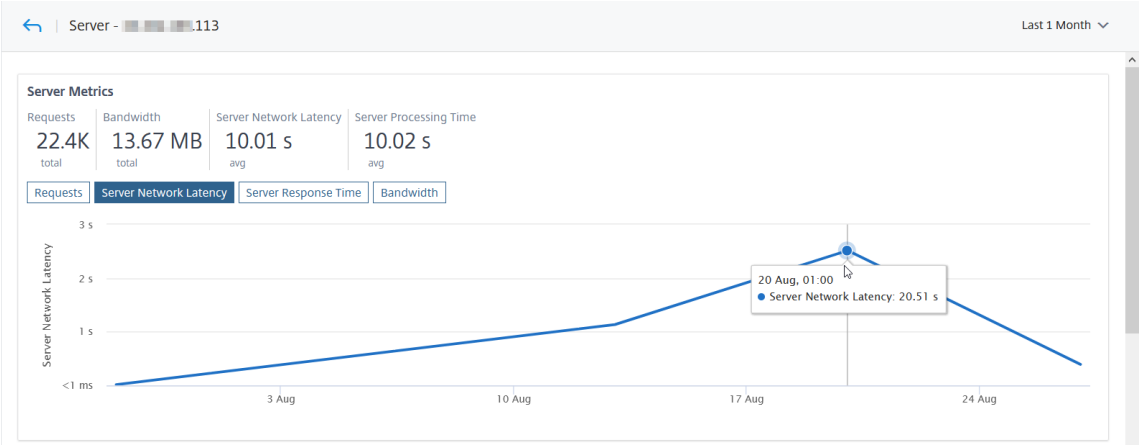
Por ejemplo, considere que quiere analizar la latencia de la red del servidor durante un mes de duración y tomar la decisión de escalar o reducir el entorno de producción. Para analizar esto:

1. Seleccione Último mes de la lista y, en la ficha **Aplicaciones**, desplácese hacia abajo hasta **Servidores**y haga clic en un servidor.




Se muestran los detalles de las métricas del servidor seleccionado.

2. Seleccione la ficha **Latencia de red del servidor** para analizar la latencia.




La latencia media indica 10.01 s y, a partir del gráfico, puede analizar que la latencia de la red del servidor durante el último 1 mes parece ser alta. Como administrador, puede tomar la decisión de escalar el entorno de producción.

Para obtener más información sobre el caso de uso de Web Insight, consulte Web Insight.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

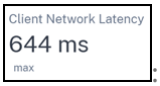
# Análisis de uso de aplicaciones

January 30, 2024

Los propietarios de aplicaciones deben tener la capacidad de evaluar y visualizar la aplicación completa desde las perspectivas de rendimiento y uso.

El **panel de aplicaciones** improvisado le permite ver todos los resultados de las aplicaciones y métricas de uso juntos. Al hacer clic en una aplicación, junto con las métricas de rendimiento de la aplicación existentes, la ficha **Web Insight** muestra los detalles de las métricas que le ayudan a:

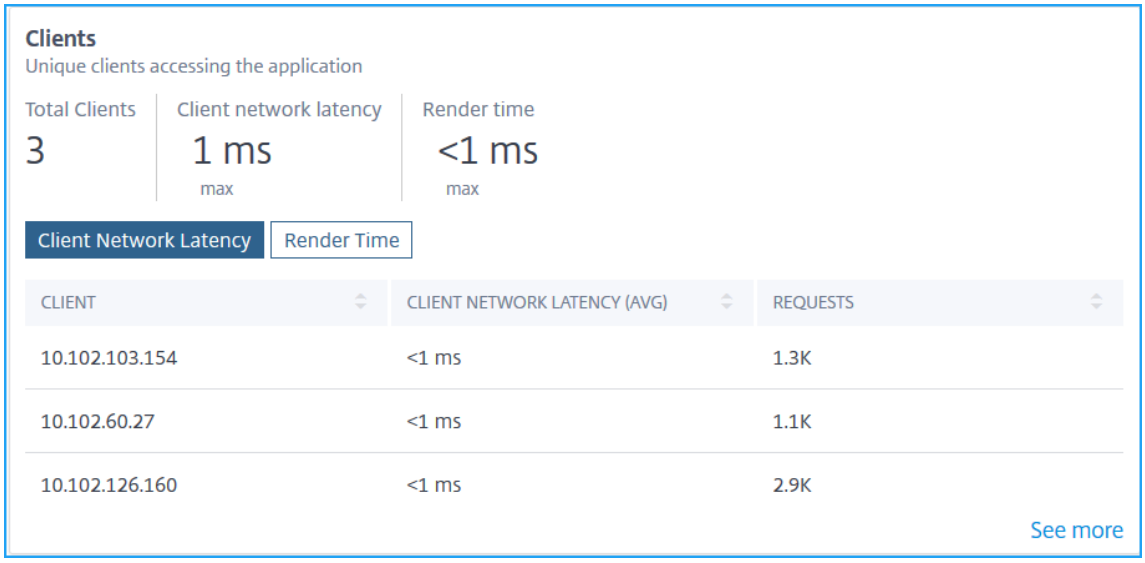
- Comprenda el uso de su aplicación.
- Correlacione cualquier desviación de rendimiento con las métricas de uso.

> **Nota**
>
> Para cada métrica, puede ver opciones que indican el valor máximo y el valor total. Por ejemplo:
>
> - 
> 
> : La latencia máxima de la red del cliente durante la duración seleccionada. Tenga en cuenta que tiene la latencia de red para el cliente 1 = 30 ms, cliente 2 = 15 ms y cliente 3 = 3 ms. En este caso, la **latencia de red del cliente** muestra 30 ms.
> -
> 
> : El ancho de banda total consumido en todos los clientes/servidores disponibles durante la duración seleccionada. Tenga en cuenta que tiene el consumo de ancho de banda para el cliente 1 = 30 MB, Cliente 2 = 45 MB, Cliente 3 = 40 MB.
> En este caso, se muestra el ancho de banda (30 MB + 45 MB + 40 MB) = 115 MB.

Las siguientes son las métricas de Web Insight que puede ver en la ficha **Uso** :

- **Clientes**: Muestra la información de los clientes que acceden a la aplicación:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Total de clientes**: Muestra el total de clientes que acceden a la aplicación.
- **Latencia de la red del cliente**: Muestra la latencia de la red desde el cliente hasta NetScaler ADC. Haga clic en la ficha **Latencia de red de cliente** para ver:
  - **Cliente**: La dirección IP del cliente.
  - **Latencia de red del cliente (promedio)**: La latencia de red promedio del cliente.
  - **Solicitudes**: El total de solicitudes del cliente.
- **Tiempo de renderización**: Muestra el tiempo necesario para procesar la respuesta del servidor. Haga clic en la ficha **Tiempo de modelizado** para ver:
  - **Cliente**: La dirección IP del cliente.
  - **Tiempo de renderización (avg)**: El tiempo medio de renderización del cliente.
  - **Solicitudes**: El total de solicitudes del cliente.

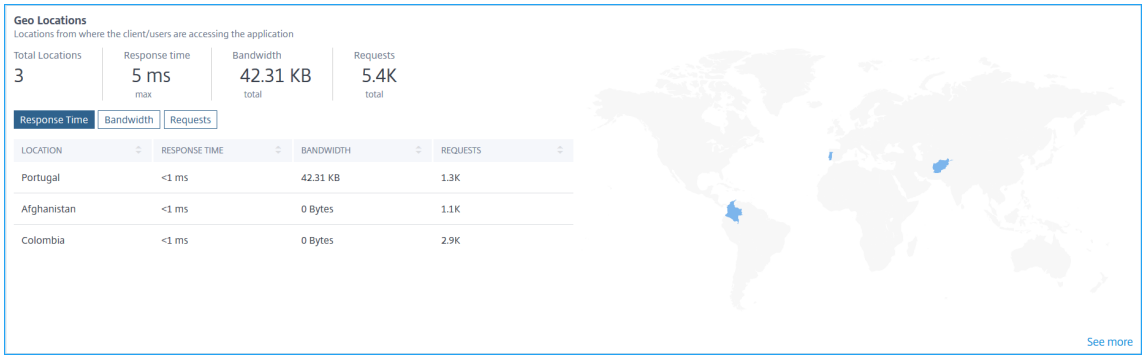
• **Servidores**: Muestra la información de los servidores que acceden a la aplicación:

- **Total de servidores**: Muestra el total de servidores que acceden a la aplicación.
- **Latencia de red del servidor**: Muestra la latencia de la red desde el servidor hasta NetScaler ADC. Haga clic en la ficha **Latencia de red del servidor** para ver:
  - **Servidor**: La dirección IP del servidor.
  - **Latencia de red del servidor (promedio)**: La latencia de red promedio del servidor.
  - **Solicitudes**: El total de solicitudes del servidor.
- **Tiempo de respuesta del servidor**: Muestra el tiempo que tarda el servidor en responder a las solicitudes. Haga clic en la ficha **Tiempo de respuesta del servidor** para ver:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

    * **Servidor**: La dirección IP del servidor.
    * **Tiempo de respuesta (avg)**: El tiempo medio de respuesta del servidor.
    * **Solicitudes**: El total de solicitudes del servidor.
  - **Ancho de banda**: Muestra el ancho de banda total consumido por los servidores. Haga clic en la ficha **Ancho de banda** para ver:
    * **Servidor**: La dirección IP del servidor.
    * **Ancho de banda**: El ancho de banda total consumido por el servidor.
    * **Solicitudes**: El total de solicitudes del servidor.

- **Ubicaciones geográficas**: Muestra la información para los clientes que acceden a la aplicación desde una ubicación en particular:

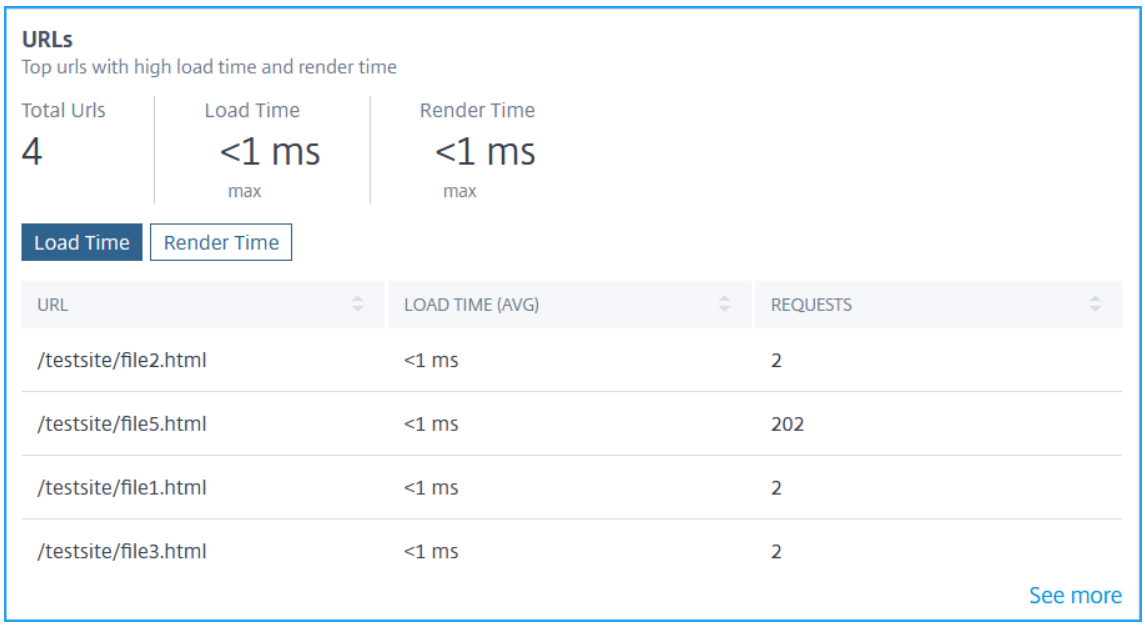



  - **Ubicaciones totales**: Muestra las ubicaciones totales de los clientes que acceden a la aplicación.
  - **Tiempo de respuesta**: Muestra el tiempo de respuesta desde la ubicación del cliente.
  - **Ancho de banda**: Muestra el ancho de banda total que consumen los clientes en todas las ubicaciones.
  - **Solicitudes**: Muestra el total de solicitudes de todas las ubicaciones de los clientes.

    Haga clic en cada ficha para ver:
    * **Ubicación**: El nombre de la ubicación.
    * **Tiempo de respuesta**: El tiempo de respuesta promedio desde la ubicación del cliente.
    * **Ancho de banda**: Ancho de banda consumido desde la ubicación del cliente.
    * **Solicitudes**: El total de solicitudes de la ubicación del cliente.

- **URL**: Muestra la información sobre las URL con una carga y un tiempo de procesamiento elevados:

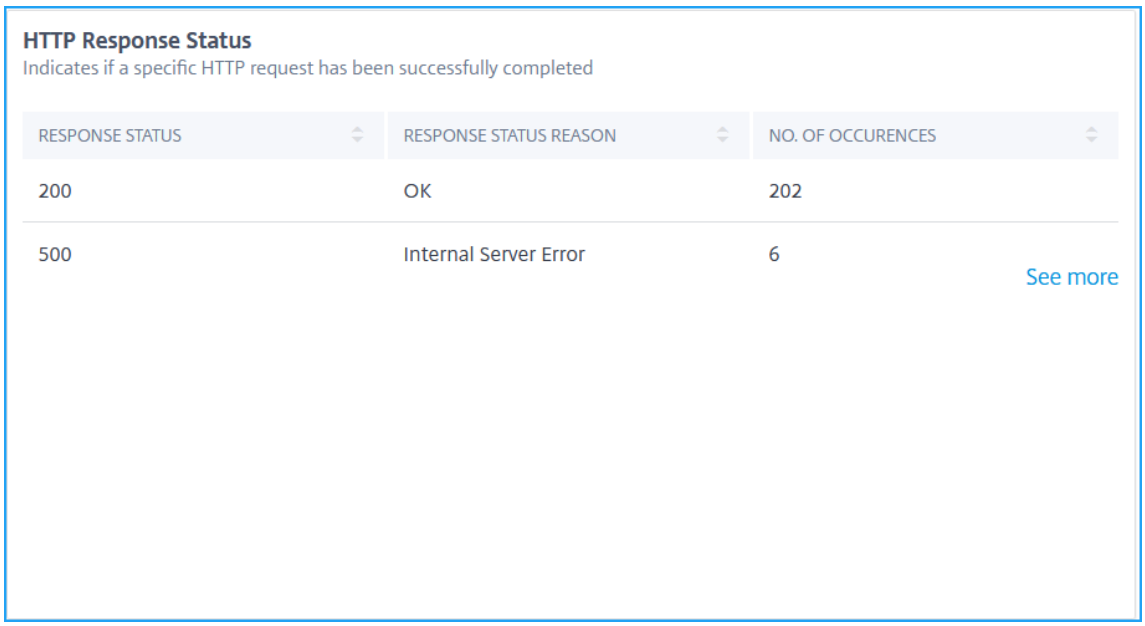
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




  - **URL totales**: Muestra el total de URL.
  - Tiempo de carga: Muestra el tiempo que tarda la URL en cargarse. Haga clic en la ficha **Tiempo de carga** para ver:
    * **URL**: El nombre de la URL.
    * **Tiempo de carga (avg)**: tiempo promedio que tarda la URL en cargarse.
    * **Solicitudes**: El total de solicitudes de la URL.
  - **Tiempo de procesamiento**: Muestra el tiempo que tarda la URL en renderizarse y mostrarse. Haga clic en la ficha **Tiempo de modelizado** para ver:
    * **URL**: El nombre de la URL.
    * **Tiempo de renderización (avg)**: El tiempo promedio que tarda la URL en renderizarse.
    * **Solicitudes**: El total de solicitudes de la URL.

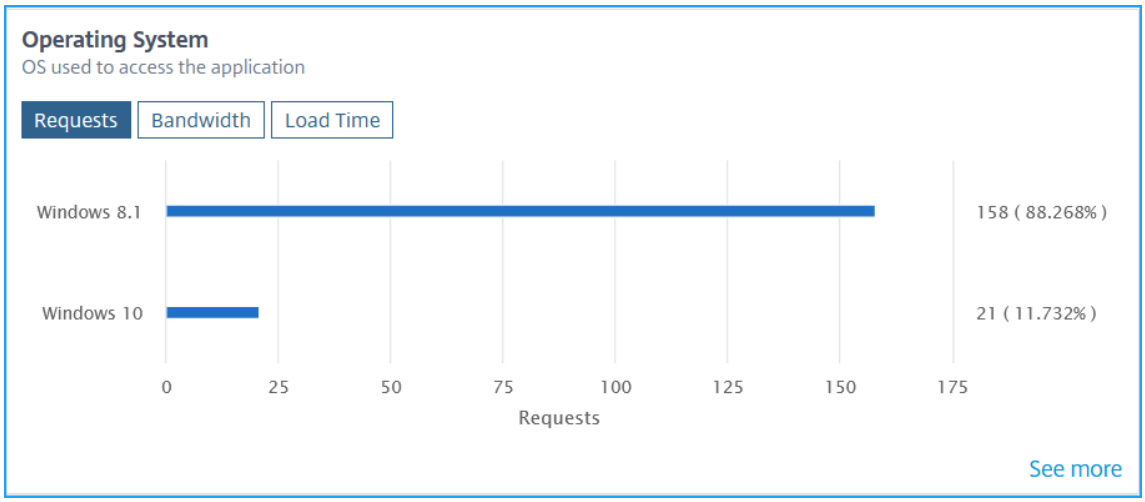
- **Estado de respuesta HTTP**: Muestra la información de una solicitud HTTP completada específica.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Estado** de la respuesta: muestra el código de respuesta, como 2xx, 4xx, 5xx, etc.
- **Motivo del estado** de la respuesta: muestra el motivo de la respuesta, como un error interno del servidor, No encontrado, etc.
- **Número de ocurrencias**: Muestra el número total de ocurrencias.

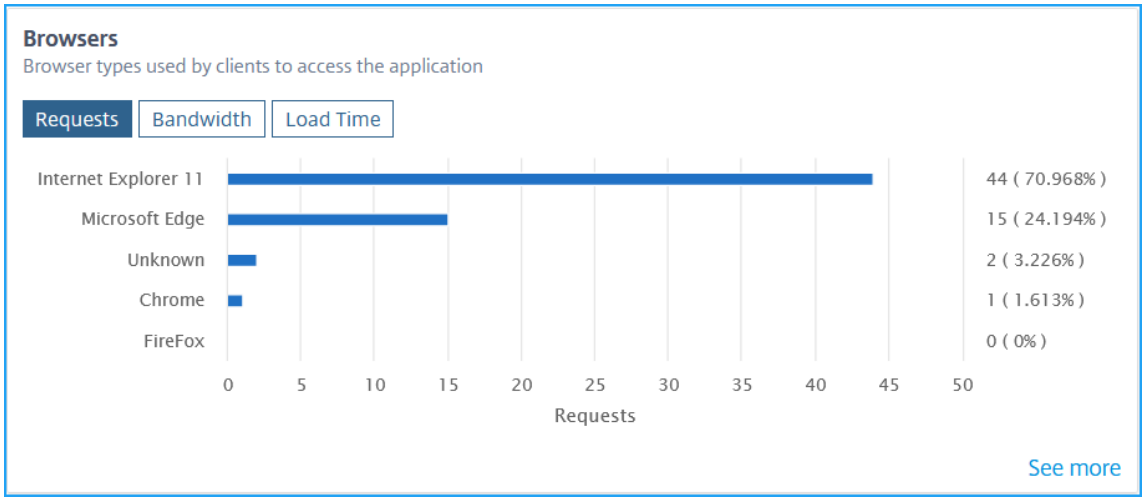
- **Sistema operativo**: Muestra la información del sistema operativo que accede a la aplicación.




- **Solicitudes**: Muestra el total de solicitudes de cada sistema operativo.
- **Ancho de banda**: Muestra el ancho de banda total consumido por cada sistema operativo.
- **Tiempo de carga**: Muestra el tiempo total que tarda cada sistema operativo en cargarse desde el servidor.

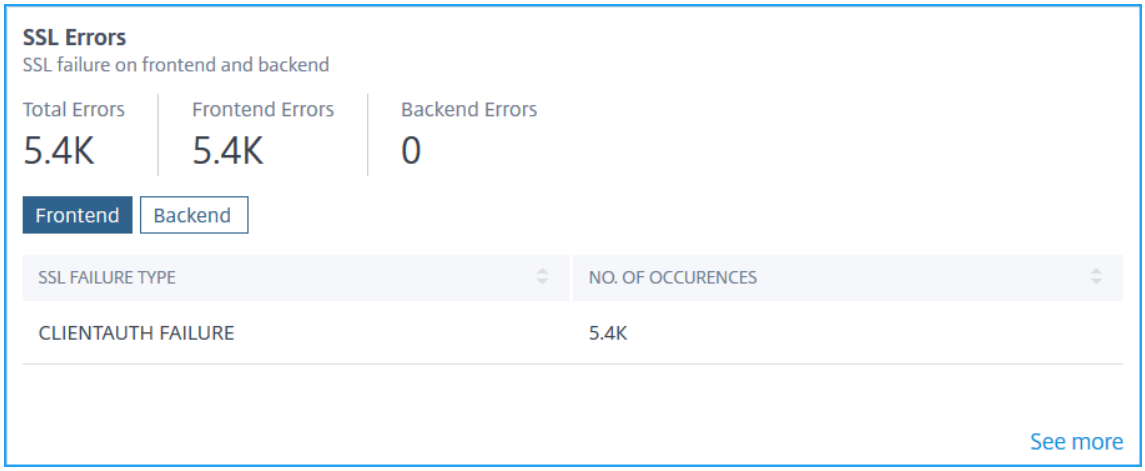
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Navegadores**: Muestra información sobre los tipos de navegadores que utilizan los clientes para acceder a la aplicación.




  - **Solicitudes**: Muestra el total de solicitudes de cada navegador.
  - **Ancho de banda**: Muestra el ancho de banda total consumido por cada navegador.
  - **Tiempo de carga**: Muestra el tiempo total que tarda un navegador en cargarse desde el servidor.

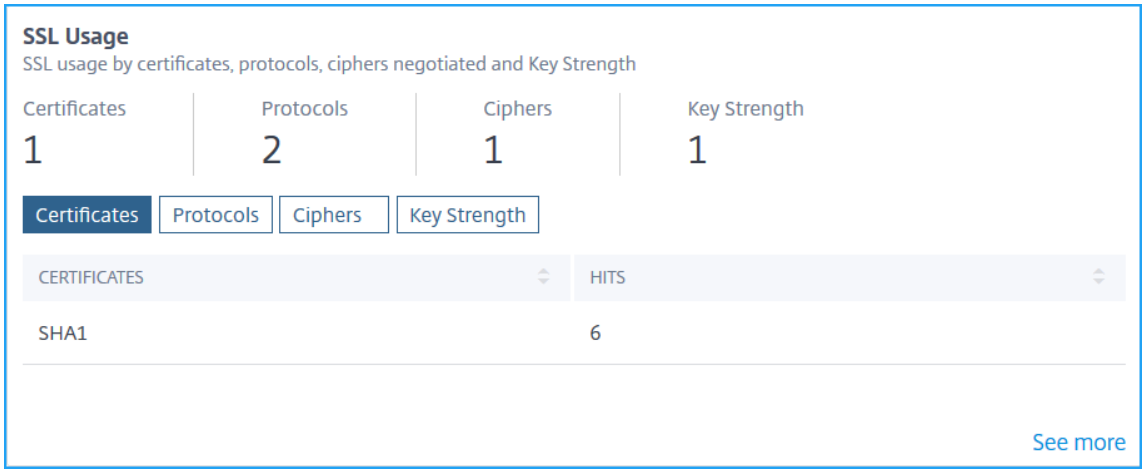
- **Errores SSL**: Muestra la información sobre los errores SSL del servidor front-end y del servidor back-end.




  - **Total de errores**: Muestra el total de errores de SSL.
  - **Frontend**: Muestra el total de errores SSL del servidor front-end. Haga clic en la ficha **Frontend** para ver el tipo de error SSL y el total de incidencias.
  - **Backend**: Muestra el total de errores SSL del servidor back-end. Haga clic en la ficha **Back-end** para ver el tipo de error SSL y el total de incidencias.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Uso de SSL**: Muestra información sobre el uso de SSL, como los certificados SSL, los protocolos, los cifrados y la fortaleza de la clave.

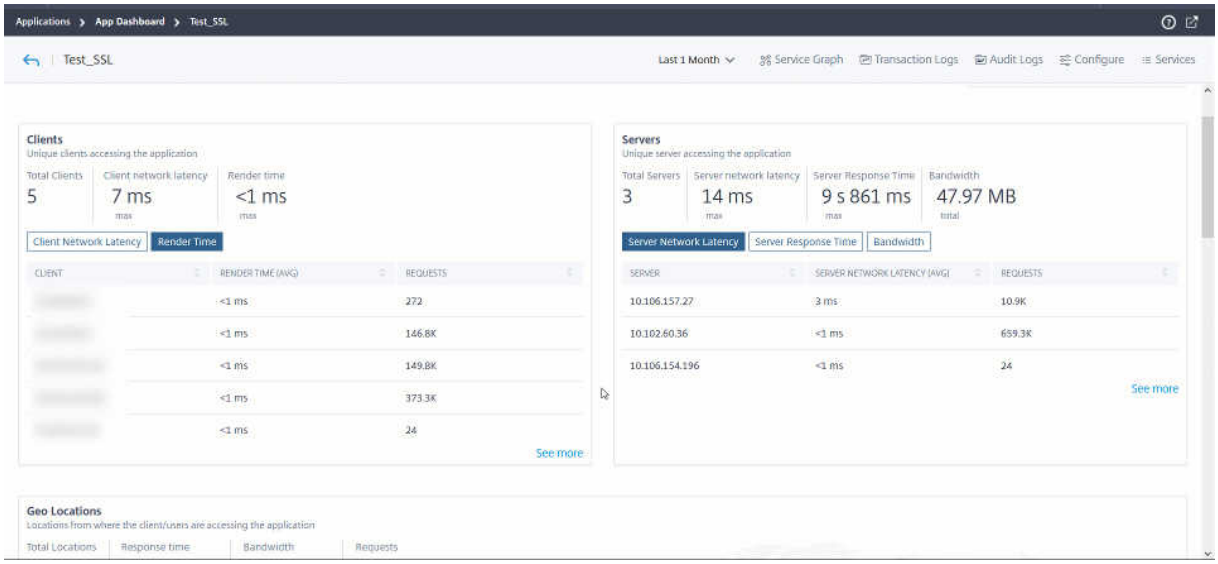



  - **Certificados**: Muestra el total de certificados SSL. Haga clic en la ficha **Certificados** para ver el nombre del certificado y el total de visitas.
  - **Protocolos**: Muestra el total de protocolos SSL. Haga clic en la ficha **Protocolos** para ver los detalles con el protocolo SSL/TSL y el total de visitas.
  - **Cifrados**: Muestra el total de cifrados. Haga clic en la ficha **Cifrados** para ver los detalles de cada nombre de conjunto de cifrado y de visitas totales.
  - Seguridad de**la clave**: Muestra la seguridad total de la clave utilizada en los certificados SSL. Haga clic en la ficha **Fuerza de tecla** para ver los detalles de cada intensidad de tecla y total de aciertos.

## Ver detalles de métricas en formato gráfico

Para cada métrica, puede ver más detalles en un formato gráfico haciendo clic en la opción **Ver más**. Haga clic en **>** para ver los detalles en un formato gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Los siguientes son los detalles que puede ver para cada métrica después de hacer clic en la opción **Ver más** :

|Nombre de Insight | Métricas |Descripción|
|—-|—-|—-|
|**Clientes**|Clientes|Denota la lista de clientes|
| |Tiempo de modelizado (AVG)|Indica el tiempo medio que tarda el cliente en representar la respuesta del servidor |
| |Latencia de red del cliente (AVG) |Indica la latencia media de red desde el cliente a la instancia de NetScaler ADC |
| |Solicitudes |Denota el total de solicitudes del cliente |
|**Servidores** |Servidor|Denota la lista de servidores |
| |Tiempo de procesamiento del servidor (AVG)|Indica el tiempo medio que tardaba el servidor en procesar las solicitudes |
| |Latencia de red de servidores (AVG) |Indica la latencia media de red desde el servidor a la instancia de NetScaler ADC |
| |Resultados|Indica el total de visitas recibidas por el servidor |
|**Ubicaciones geográficas** |Ubicaciones |Denota las ubicaciones de los clientes |
| | Tiempo de respuesta |Denota el tiempo total de respuesta desde la ubicación del cliente |
| | Ancho de banda|Denota el ancho de banda total consumido desde la ubicación |
| |Solicitudes |Denota el total de solicitudes de la ubicación |
|**URL** |Tiempo de modelizado (AVG) |Indica el tiempo medio tardado en cargar la página desde el servidor |
| | Tiempo de carga (AVG)| Denota el tiempo medio que tarda la URL en renderizarse y mostrarse |
| |Resultados |Denota el total de visitas de la URL |
|**Estado de respuesta HTTP** | Nombre|Indica el nombre del estado de respuesta como Aceptar, No encontrado, Error interno del servidor, etc. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| |Estado de respuesta |Indica el código de estado de respuesta recibido del servidor como 200, 400, 500, etc. |
| |Resultados |Indica el total de aciertos del código de respuesta |
| |Ancho de banda |Denota el ancho de banda total consumido |
|**Sistema operativo** |Sistema operativo |Denota el nombre del sistema operativo como Windows, MAC |
| |Tiempo de carga |Indica el tiempo total que tarda el sistema operativo en cargar desde el servidor|
| | Ancho de banda|Denota el ancho de banda total consumido por el sistema operativo |
| | Solicitudes|Denota el total de solicitudes del sistema operativo |
|**Exploradores web** |Exploradores web |Indica el nombre del navegador, como Mozilla Firefox, Chrome, etc. |
| |Tiempo de carga | Indica el tiempo total que tarda un navegador en cargarse desde el servidor|
| |Ancho de banda |Indica el ancho de banda total consumido por el navegador |
| |Solicitudes |Indica el total de solicitudes del navegador |
|**Errores SSL** |Tipo de fallo SSL |Indica el nombre del error, como CLIENTAUTH FAILURE |
| | Ocurrencias|Denota el total de ocurrencias para el error SSL |
|**Uso SSL** |Denota el nombre del protocolo y las versiones como TLS, SSL |
| |Veces |Denota el total de aciertos del protocolo |

Para obtener más información sobre los casos de uso de Web Insight, consulte Web Insight.

## Solucionar problemas del panel de aplicaciones

August 23, 2024

Después de agregar una aplicación en el Panel de aplicaciones, el panel muestra inmediatamente los detalles de configuración básicos de la aplicación. Los detalles de análisis de aplicaciones, como la puntuación de la aplicación, las métricas clave y los problemas comienzan a rellenarse en pocos minutos (aproximadamente 10 a 15 minutos). Para obtener más información, consulte Aplicaciones.

Debe asegurarse de que no hay ningún problema con el flujo de datos de métricas (recopilador AppFlow o perfil de Analytics) desde la instancia de NetScaler ADC. Puede obtener más información sobre el recopilador de AppFlow y el perfil de análisis en este documento.

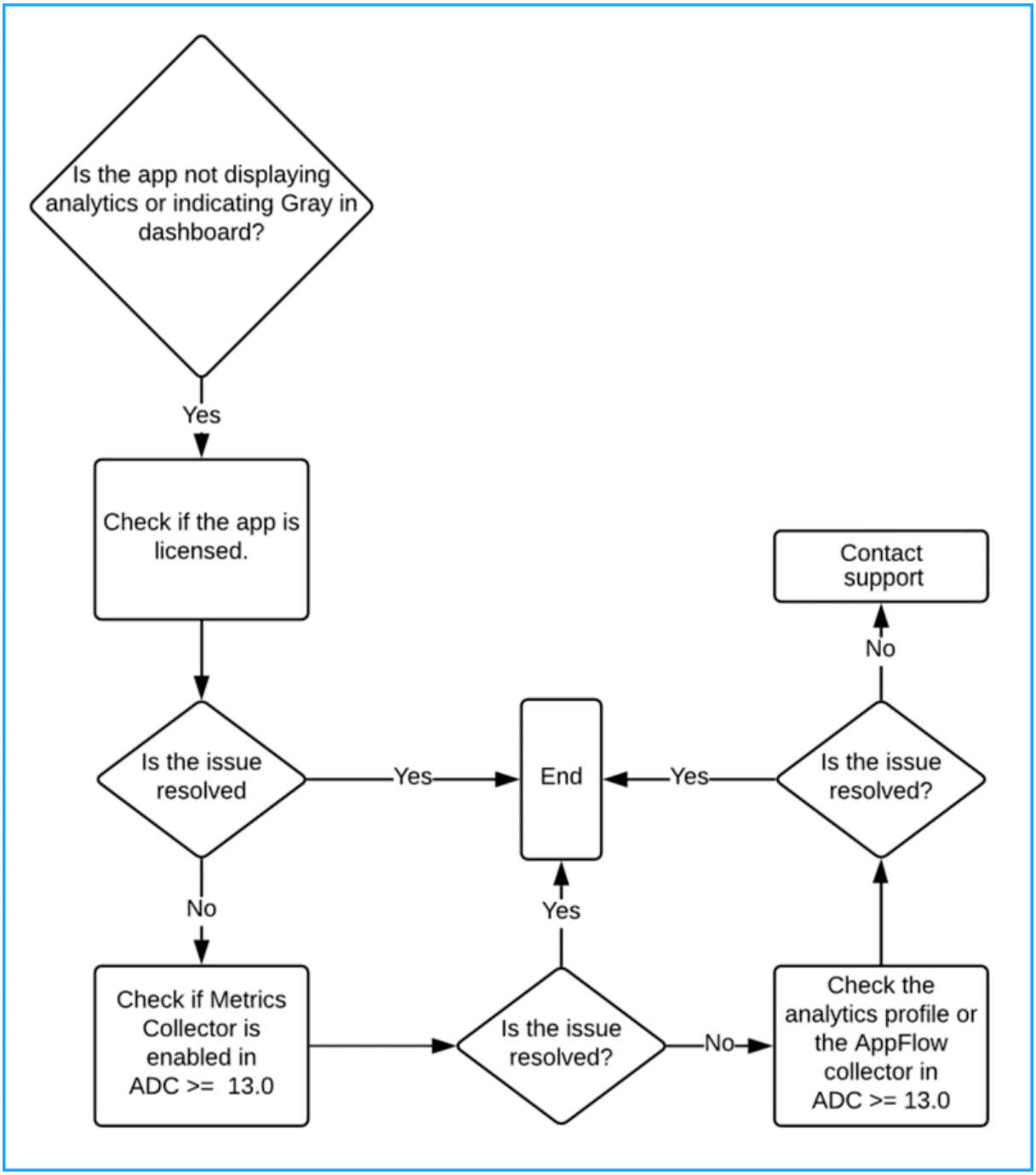
En este documento se describen los pasos de solución de problemas que debe realizar cuando:

- Si hace clic en una aplicación, los análisis de la aplicación seleccionada no muestran los datos necesarios incluso después de la duración mencionada (10-15 minutos).
- La aplicación CS o LB siempre indica color gris (estado **no aplicable**) en el Panel de aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Los procedimientos de solución de problemas mencionados en este documento solo son aplicables a servidores virtuales de **Content Switching** y **Equilibrio de carga**.

### Situación de solución de problemas




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## La aplicación tiene licencia

Debe asegurarse de que la aplicación tiene licencia.

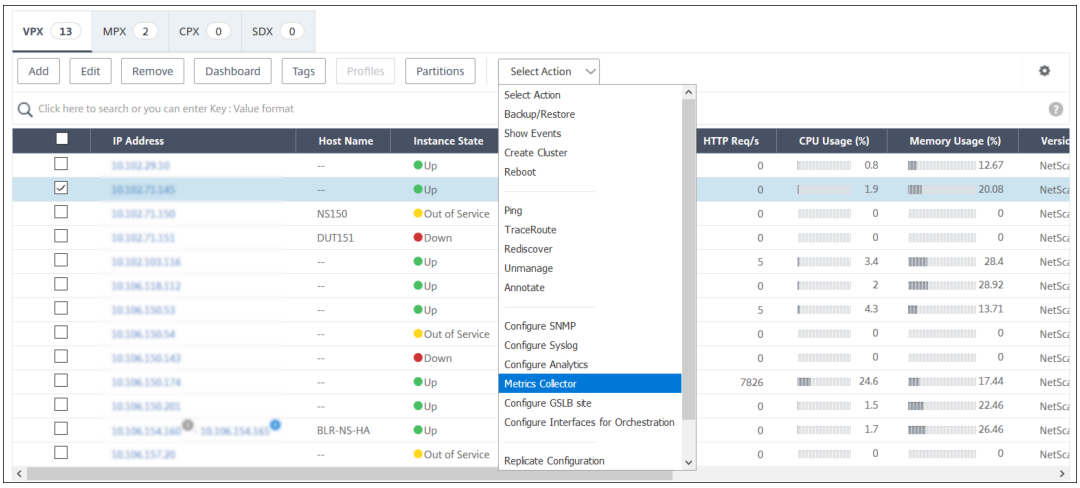
- **Servicio ADM** : vaya a **Cuenta > Suscripciones** y compruebe si la aplicación tiene licencia bajo **Resumen de licencias de servidor virtual**. Si la aplicación no tiene licencia, consulte Administrar licencias y habilitar el análisis en servidores virtuales para licenciar el servidor virtual.
- **ADM on-prem** : vaya a **Sistema > Licencias y análisis** y verifique si la aplicación tiene licencia bajo **Resumen de licencias de servidor virtual**. Si la aplicación no tiene licencia, consulte Administrar licencias y habilitar el análisis en servidores virtuales para licenciar el servidor virtual.

## El selector de métricas está habilitado

Debe asegurarse de que el **recopilador de métricas** está habilitado en la instancia de NetScaler ADC.

Para NetScaler ADC versión 13.0 o posterior, Metrics Collector se habilita de forma predeterminada, después de que la instancia de ADC se haya agregado correctamente en ADM. Para asegurarse de que el recopilador de métricas está habilitado:

1. Vaya a **Redes > Instancias**. En Instancias, seleccione el tipo de instancia (por ejemplo, NetScaler ADC VPX).
2. Seleccione la instancia de NetScaler ADC.
   a) En la lista **Seleccionar acción**, seleccione **Metrics Collector**.




3. En la página **Configurar los ajustes del recopilador de métricas**, asegúrese de que la opción **Activar** esté seleccionada. De lo contrario, seleccione la opción **Activar** y haga clic en **Aceptar**.

Después de habilitar el recopilador de métricas y si aún no puede ver los datos, valida:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El recopilador AppFlow de la instancia de Citrix ADC versión 13.0 **anterior a la compilación 47.x**.
- El perfil de análisis en la versión **47.x o** posterior de la instancia de Citrix ADC.

**Generaciones anteriores de la instancia de NetScaler ADC**

En NetScaler ADC:

1. **Ejecute el siguiente comando para asegurarse de que el recopilador está en funcionamiento y se ejecuta en el puerto 5563:**

   ```
   sh appflow collector af_collector_rest_<adm_receiver_ip>
   ```

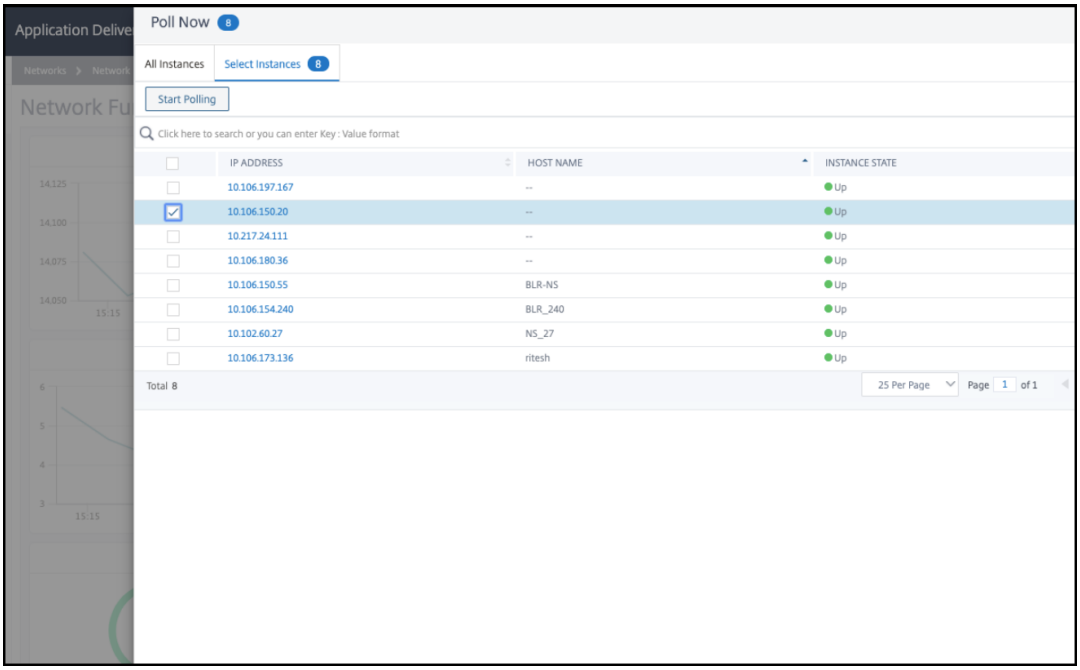
   ```
   > sh appflow collector af_collector_rest_10.102.103.114
   1) Name: af_collector_rest_10.102.103.114
   IPv4 address: 10.102.103.114
   Port: 5563
   Netprofile:
   Transport: rest
   State: UP
   Done
   ```

2. Si no hay ningún colector disponible, realice un sondeo manual de instancias en NetScaler ADM.

   a) Navegue a **Redes > Función de red > Encuesta ahora**

   b) Seleccione la instancia y haga clic en **Iniciar sondeo**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Si el sondeo falla, quite la instancia ADC de ADM y, a continuación, agregue de nuevo la instancia de ADC. Cuando se agrega la instancia de ADC, el recopilador se agrega en ADC.

Si el selector indica el estado **Inactivo**:

1. Asegúrese de que el SNIP está configurado.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   Si SNIP no está configurado, debe configurar SNIP. Para obtener más información, consulte Configuración de SNIP.

2. Asegúrese de que si la instancia de ADC es accesible a ADM.

   Puede validar haciendo una prueba de ping. Ejecute `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

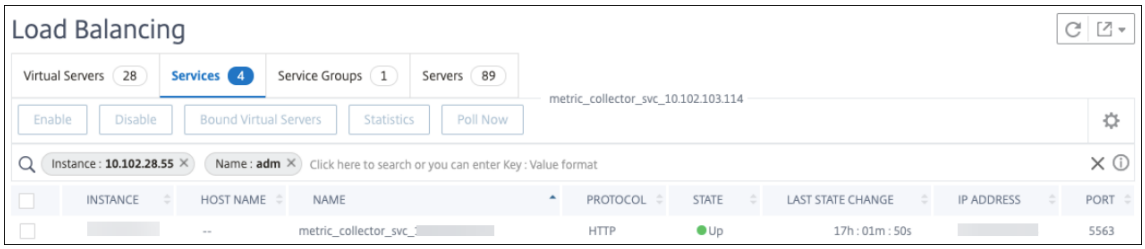
### La instancia de NetScaler ADC se compila posteriormente

En NetScaler ADM, asegúrese de que el servicio de recopilador de métricas esté disponible:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes > Función de red > Equilibrio de carga > Servicios**.
2. En la barra de búsqueda, filtra por **Instancia: (dirección IP)** y **Nombre: ADM**.
3. Asegúrese de que `adm_metric_collector_svc_<adm_receiver ip>` está disponible. La dirección IP puede ser la IP de administración de ADM o la IP del agente.

   Asegúrese de que este servicio se encuentra en estado **UP** y ejecutándose en el puerto 5563.




Si aún no puede ver los datos, asegúrese de que el servicio de recopilador está vinculado al perfil de análisis de series temporales en NetScaler ADC.

1. Iniciar sesión en NetScaler ADC
2. Ejecute este comando:

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Si el selector indica el estado **Inactivo**:

1. Asegúrese de que el SNIP está configurado.

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active    Enabled  Enabled  NA       Enabled
```

   Si SNIP no está configurado, debe configurar SNIP. Para obtener más información, consulte Configuración de SNIP.

2. Asegúrese de que si la instancia de ADC es accesible a ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede validar haciendo una prueba de ping. Ejecute `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. Asegúrese de que la conectividad de tráfico a través de telnet pueda conectar el servicio.

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

Si telnet puede conectar el servicio, existe un firewall y bloquea el flujo de datos de métricas. Debe resolver el problema del bloqueo del firewall.

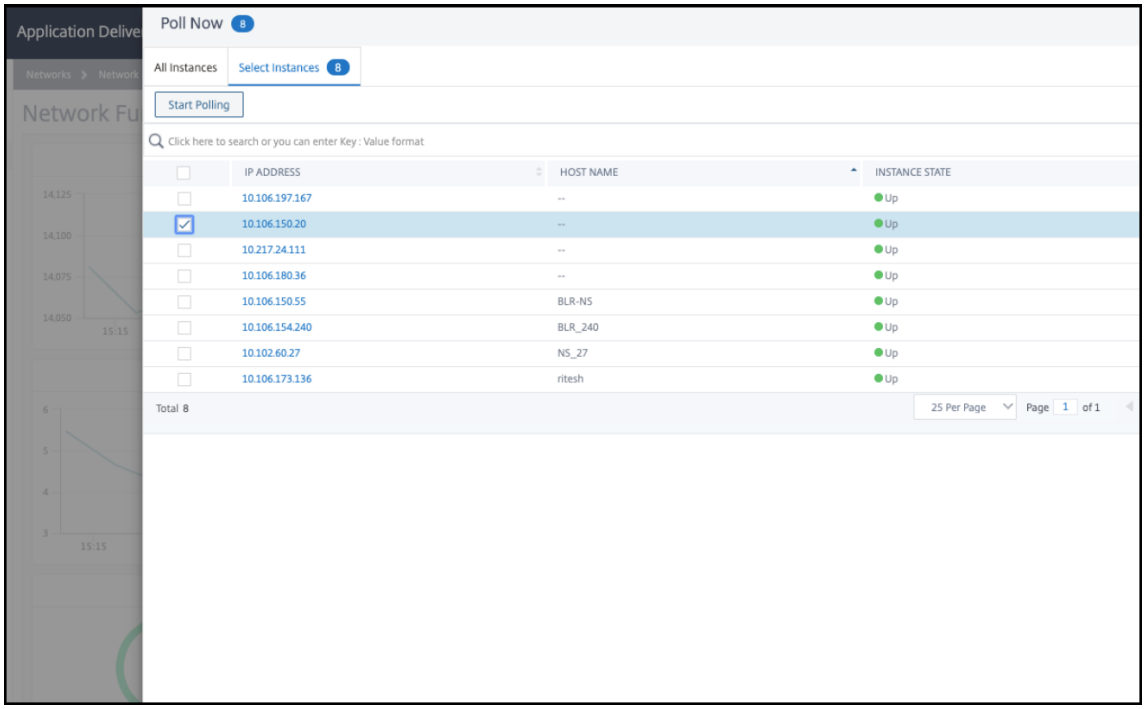
Si ningún servicio de recopilador está vinculado al perfil de análisis de series temporales en NetScaler ADC, el recopilador se muestra en blanco.

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Debe realizar un sondeo manual de instancia en NetScaler ADM.

1. Navegue a **Redes > Función de red > Encuesta ahora**
2. Seleccione la instancia y haga clic en **Iniciar sondeo**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Si el sondeo falla, agregue el servicio de recopilador directamente en la instancia de NetScaler ADC mediante los siguientes comandos:

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563
```

```
unset analyticsprofile ns_analytics_time_series_profile -collectors
```

```
set analytics profile ns_analytics_time_series_profile -collectors
 adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -
events enabled
```

Se actualiza el perfil de la serie temporal de análisis.

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

Si el problema persiste incluso después de realizar todos los pasos de solución de problemas men-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

cionados, póngase en contacto con el **Soporte técnico de Citrix**.

## Crear un umbral y una alerta para el análisis de aplicaciones

January 30, 2024

El análisis de aplicaciones en Citrix ADM permite supervisar los distintos tipos de tráfico que pasan por las instancias de Citrix ADC. Citrix ADM le permite establecer umbrales en los siguientes contadores para supervisar el tráfico y la puntuación de las aplicaciones.

Puede configurar los umbrales y supervisar la puntuación de la aplicación en relación con la CPU, la memoria, los descartes de NIC y el tiempo de respuesta.

**Para configurar la puntuación de la aplicación en NetScaler ADM:**

1. En Citrix ADM, vaya a **Análisis** > **Configuración** .
2. En la página de **ajustes** , haga clic en **Configurar puntuación de la aplicación** .
3. En la página **Configurar puntuación de aplicación**, introduzca los valores para los siguientes parámetros:

   a) **Umbral de CPU bajo**. El valor de umbral inferior del uso total de la CPU en la instancia de Citrix ADC.

   b) **Umbral de CPU alto**. El valor de umbral más alto del uso total de la CPU en la instancia de Citrix ADC.

   c) **Umbral de memoria bajo**. El valor de umbral inferior del uso total de memoria en la instancia de Citrix ADC.

   d) **Umbral de memoria alto**. El valor de umbral más alto del uso total de memoria en la instancia de Citrix ADC.

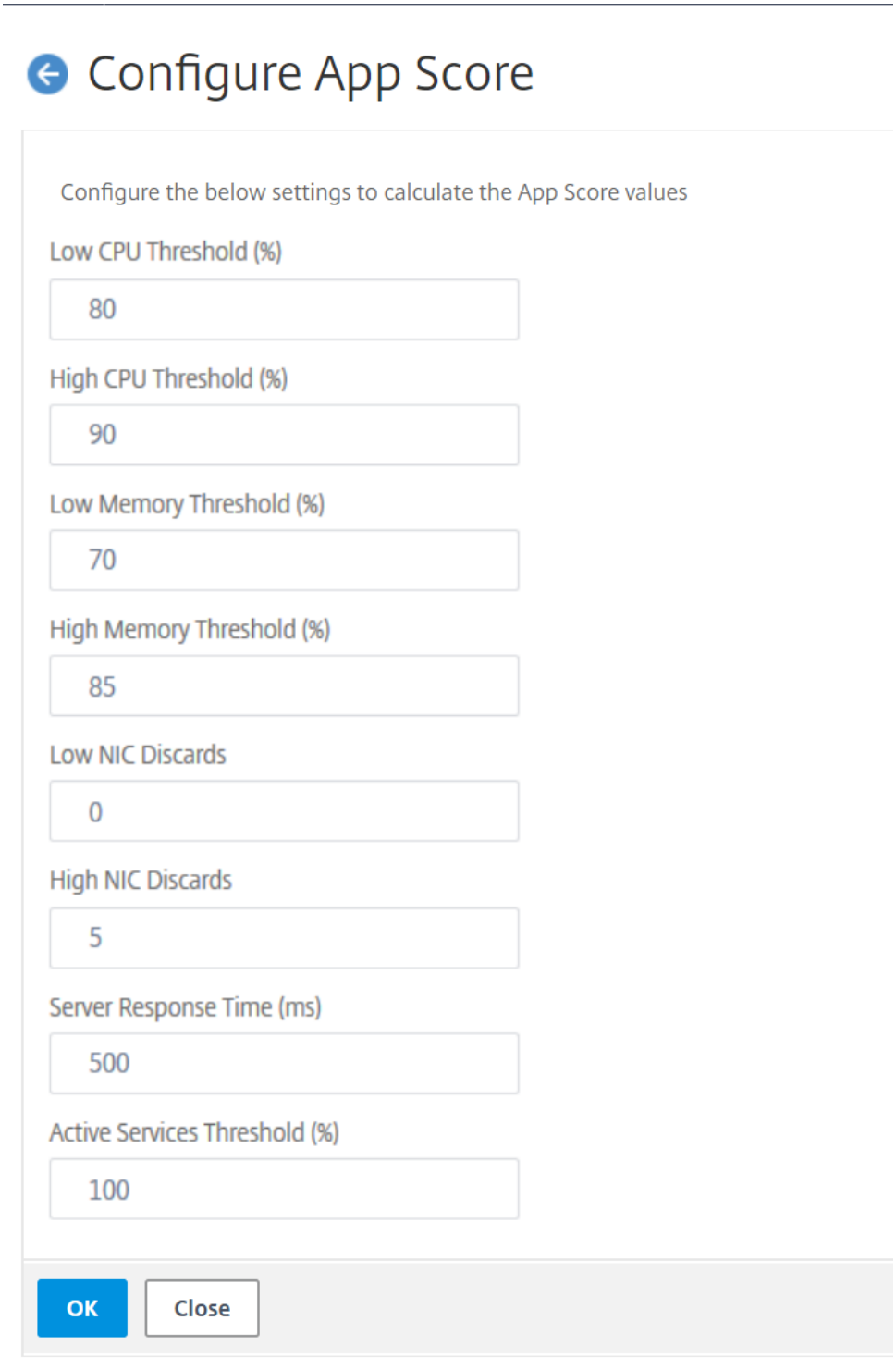
   e) **Un nivel bajo de NIC descarta el SLA**. El valor umbral inferior de los paquetes descartados por las interfaces.

   f) **Un nivel alto de NIC descarta el SLA**. El valor umbral más alto de los paquetes descartados por las interfaces.

   g) **Tiempo de respuesta**. Intervalo de tiempo entre el envío de un paquete de solicitud y la recepción del primer paquete de respuesta del servicio configurado en el servidor virtual. El valor predeterminado configurado en Citrix ADM es de 500 ms.

   h) **Umbral de servicios activos**. Valor de umbral del porcentaje de servicios que deben estar activos que están enlazados al servidor virtual.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Análisis inteligente de aplicaciones

January 30, 2024

Intelligent App Analytics le permite identificar problemas de rendimiento de las aplicaciones mediante el aprendizaje automático y algoritmos basados en reglas. La función Intelligent App Analytics de NetScaler ADM:

- Proporciona una solución fácil y escalable para monitorear y solucionar problemas de aplicaciones que se entregan a través de instancias de NetScaler ADC.
- Supervisa todos los niveles de la aplicación para reducir el tiempo de entrega necesario para solucionar problemas y mejorar el tiempo de actividad general de las aplicaciones.

En una implementación típica, miles de servidores satisfacen las necesidades de datos de los usuarios. El tráfico enviado a estos servidores se equilibra y supervisa la carga mediante servidores virtuales configurados en dispositivos NetScaler ADC. Cada servidor virtual está enlazado a varios servicios que representan a los servidores de fondo. En tales implementaciones, la función Intelligent App Analytics le ayuda a:

- Supervise, administre y tome decisiones durante las interrupciones y otros eventos
- Supervise los servidores y servicios virtuales configurados para una aplicación
- Muestre información crítica sobre servidores y servicios virtuales, de modo que pueda cambiar las configuraciones según sea necesario para lograr un rendimiento óptimo por parte de las aplicaciones.

Al escalar la comunidad de servidores de la organización, resulta difícil realizar un seguimiento de los problemas asociados con la gran cantidad de tráfico recibido en los servidores y reducir la solución de problemas requerida.

Cuando una aplicación se ejecuta y recibe una gran cantidad de tráfico, pueden surgir varios problemas. Puede ver los indicadores de rendimiento para el análisis de aplicaciones navegando a **Aplicaciones** > **Panel**, seleccionando una aplicación y desplazándose hacia abajo para ver los problemas en la sección **Problemas**.

## Configurar el análisis inteligente de aplicaciones

January 30, 2024

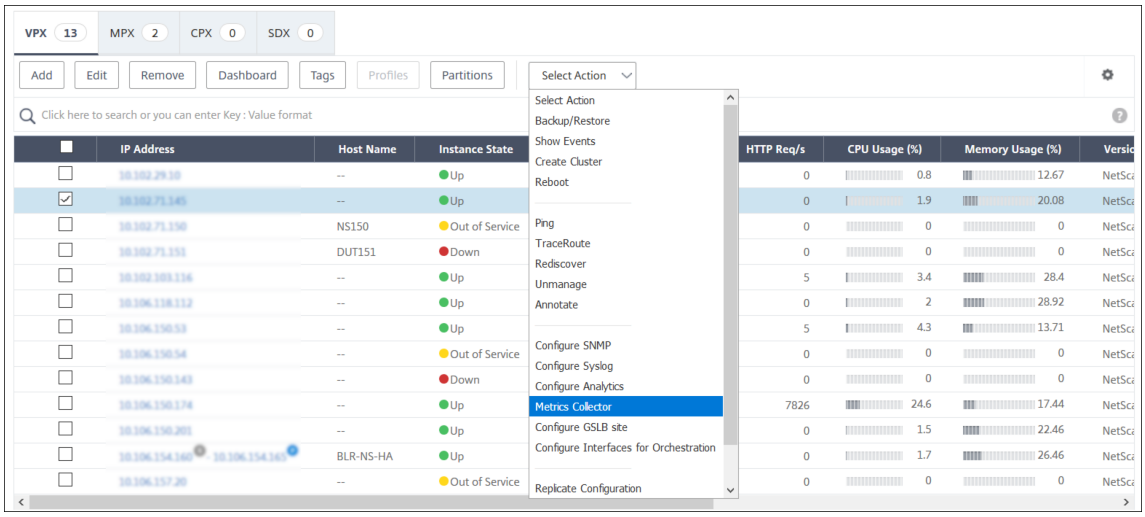
La función Intelligent App Analytics solo se admite en **Citrix ADC 12.1.50.x o versiones posteriores**. **Metrics Collector** envía los datos del contador de NetScaler ADC a NetScaler ADM, que se utiliza para

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

detectar problemas de aplicaciones. Para utilizar la función Intelligent App Analytics, **Metrics Collector** debe estar configurado en cada instancia de NetScaler ADC. De forma predeterminada, **Metrics Collector** está habilitado en NetScaler ADC, mientras agrega la instancia a NetScaler ADM.

Para asegurarte de que el **recopilador de métricas** está activado:

1. Vaya a **Redes** > **Instancias** > **Citrix ADC** y seleccione el tipo de instancia que quiere supervisar (por ejemplo, Citrix ADC VPX).
2. Seleccione la instancia de NetScaler ADC.
3. En la lista **Seleccionar acción**, seleccione **Metrics Collector**.




4. En la página **Configurar los ajustes del recopilador de métricas**, la opción **Habilitar** está seleccionada de forma predeterminada. Si esta opción no está seleccionada, asegúrese de seleccionar la opción **Habilitar** y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Para ver las anomalías de los **errores del servidor** y su **transacción web detallada**, debe habilitar el análisis en los servidores virtuales.

## Indicadores de rendimiento para análisis de aplicaciones

January 30, 2024

Puede ver los indicadores de rendimiento, junto con sus categorías que se producen en las aplicaciones web NetScaler ADC. Para ver estos indicadores, debe asegurarse de habilitar el recopilador de análisis y métricas en la instancia de ADC:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Después de habilitar el recopilador de estadísticas y métricas, puede ver los siguientes indicadores navegando a **Aplicaciones** > **Panel**, seleccionando una aplicación y desplazándose hacia abajo a la sección **Problemas** :

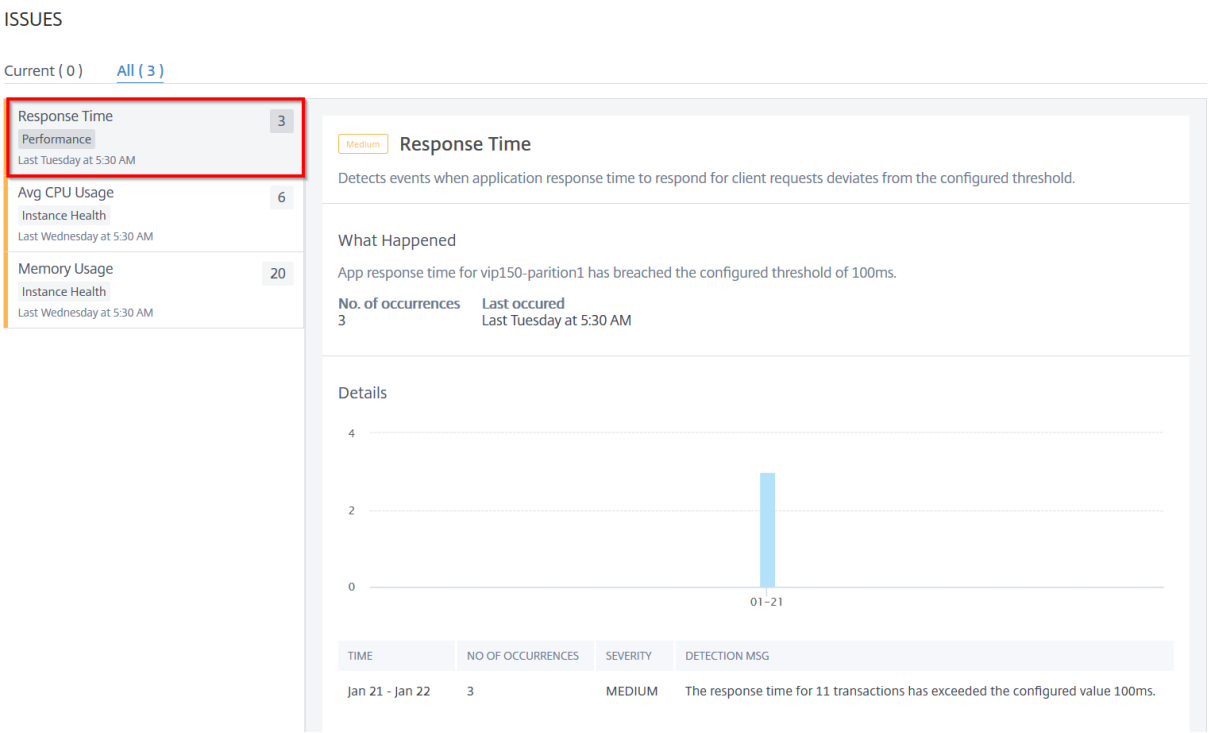
- Tiempo de respuesta
- Servicios Activos
- Uso medio de CPU
- Uso de memoria
- Saturación de tarjeta NIC
- Solapas de servicio
- Reutilización baja de sesiones
- Tipo de persistencia incorrecto
- Servidor inestable (5xx)
- Tráfico en tiempo real SSL
- Paquetes HTTP inusualmente grandes
- Aciertos límites de cola de reensamblado TCP
- Acumulación SurgeQueue

## Tiempo de respuesta

January 30, 2024

Este problema detecta cuando el tiempo de respuesta de la aplicación para responder a las solicitudes de los clientes se desvía del valor de umbral configurado. Haga clic en la ficha **Tiempo de respuesta** para ver los detalles del problema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En **Detalles**, puede ver:

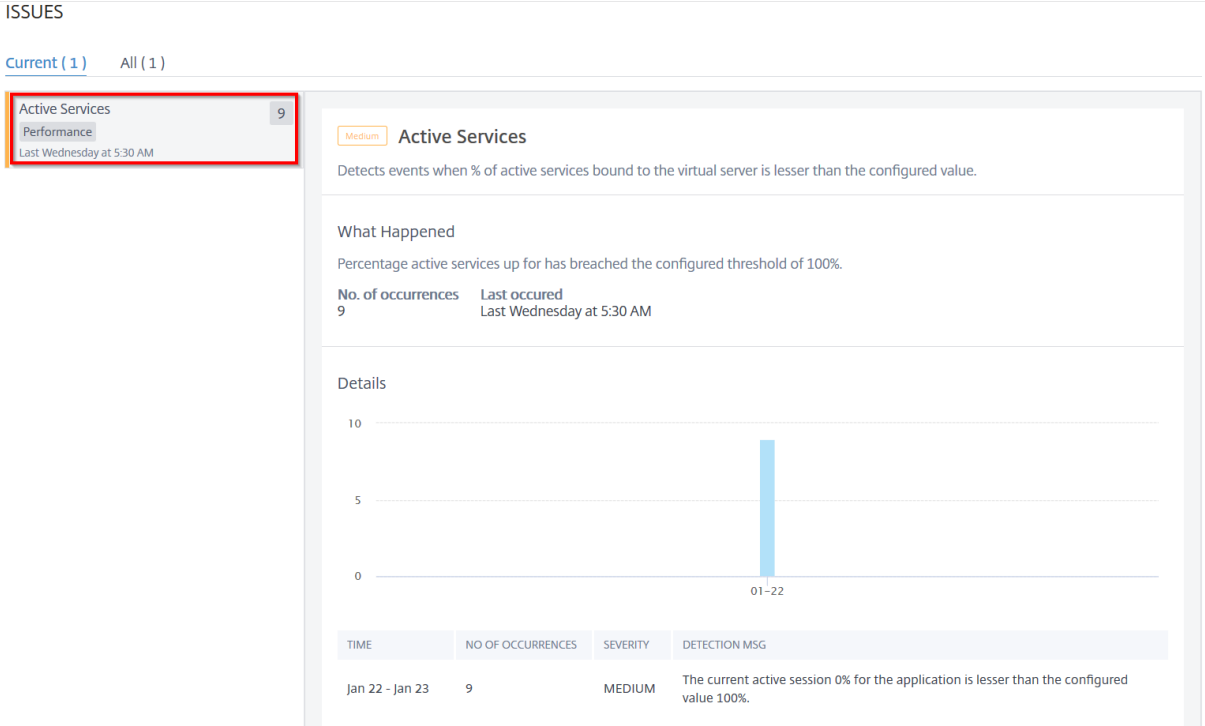
- El gráfico que indica el total de eventos del tiempo seleccionado. Haga clic para aplicar el filtro y ver los detalles
- Cuándo se ha producido el problema
- El total de ocurrencias del tiempo seleccionado
- La gravedad del problema, como baja, media y alta
- El mensaje de detección que indica el tiempo total de respuesta de transacción que supera el valor de umbral configurado

## Servicios Activos

January 30, 2024

Este problema detecta cuando el% de servicios activos enlazados al servidor virtual es inferior al valor de umbral configurado. Haga clic en la ficha **Servicios activos** para ver los detalles del problema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En **Detalles**, puede ver:

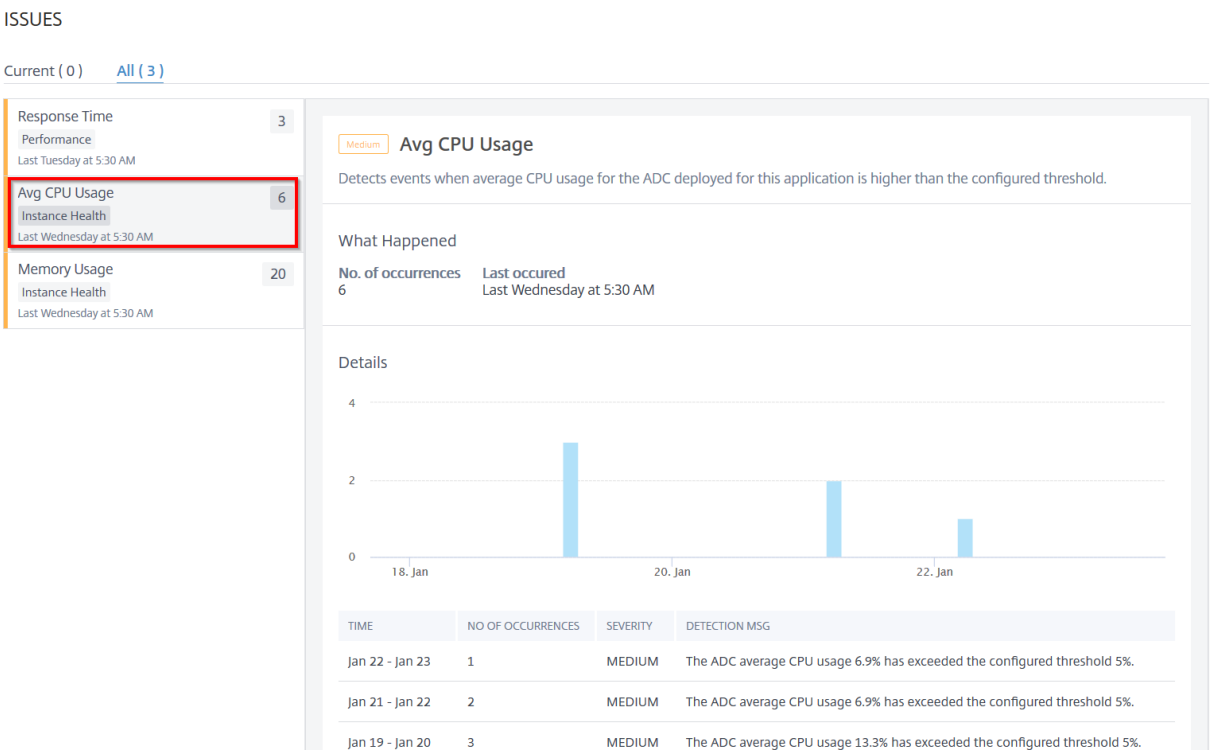
- El gráfico que indica el total de eventos durante el tiempo seleccionado. Haga clic para aplicar el filtro y ver los detalles
- Cuándo se ha producido el problema
- El total de ocurrencias durante el tiempo seleccionado
- La gravedad del problema, como baja, media y alta
- El mensaje de detección que indica el% de sesiones de servicio activas y el valor de umbral configurado

## Uso medio de CPU

January 30, 2024

Este problema detecta cuando el uso de la CPU ADC para esta aplicación supera el valor de umbral configurado. Haga clic en la ficha **Uso promedio de la CPU** para ver los detalles del problema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En **Detalles**, puede ver:

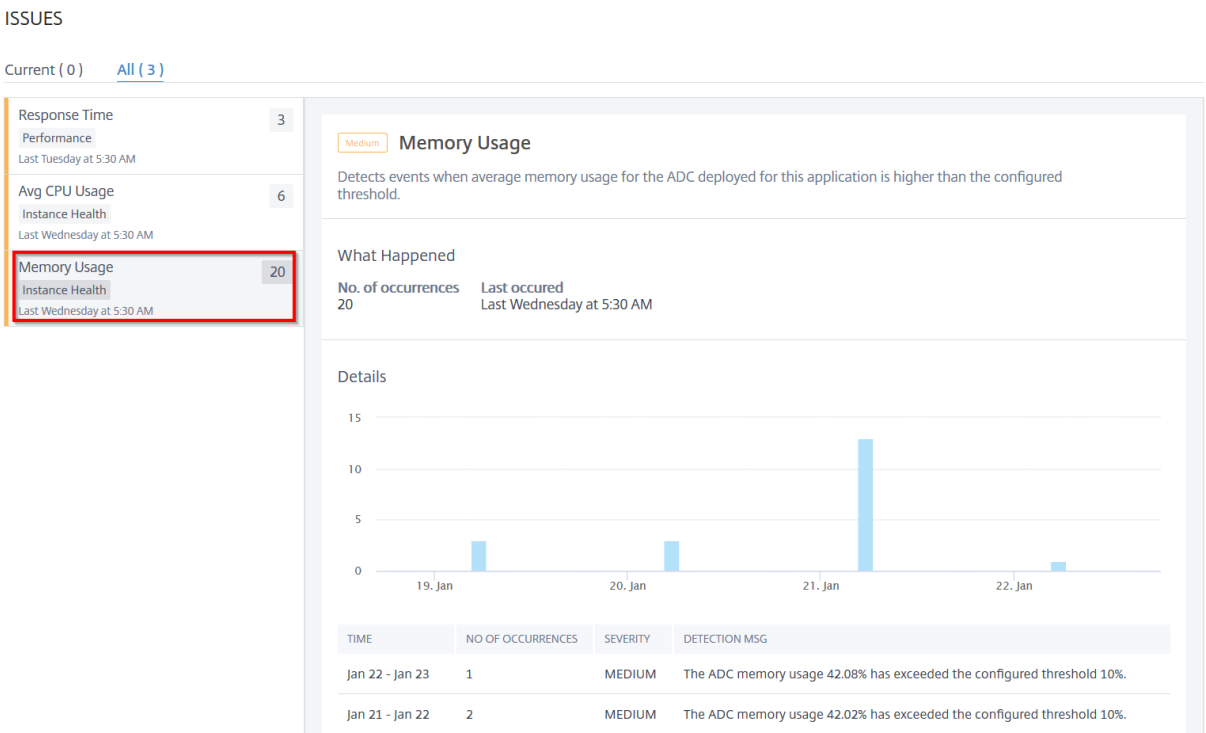
- El gráfico que indica el total de eventos durante el tiempo seleccionado. Haga clic para aplicar el filtro y ver los detalles
- Cuándo se ha producido el problema
- El total de ocurrencias durante el tiempo seleccionado
- La gravedad del problema, como baja, media y alta
- El mensaje de detección que indica el% de uso de CPU promedio del ADC y el valor umbral configurado

## Uso de memoria

January 30, 2024

Este problema detecta cuando el uso de la memoria ADC para esta aplicación supera el valor de umbral configurado. Haga clic en la ficha **Uso de memoria** para ver los detalles del problema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En **Detalles**, puede ver:

- El gráfico que indica el total de eventos durante el tiempo seleccionado. Haga clic para aplicar el filtro y ver los detalles
- Cuándo se ha producido el problema
- El total de ocurrencias durante el tiempo seleccionado
- La gravedad del problema, como baja, media y alta
- El mensaje de detección que indica el porcentaje promedio de uso de memoria ADC y el valor de umbral configurado

## Solapas de servicio

January 30, 2024

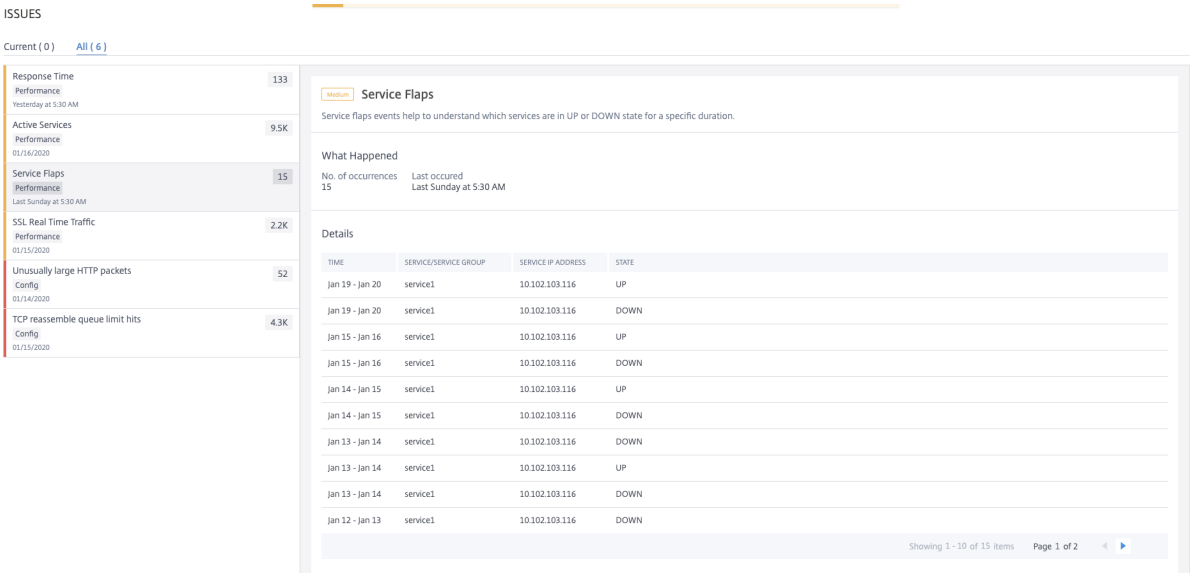
Como administrador de red, debe garantizar la disponibilidad óptima de la aplicación. Cuando hay problemas de red o de configuración, el estado y la disponibilidad de un servidor de aplicaciones pueden afectar al rendimiento general.

Al utilizar los eventos de flaps del servicio, puede identificar la aplicación que tiene problemas. Los eventos de Service Flaps también le ayudan a:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Comprenda qué servicio está en estado INACTIVO durante un período específico
- Comprenda cuántos servicios están en estado ACTIVO o INACTIVO durante un período específico

Haga clic en la ficha **Service Flaps** para ver los detalles de las solapas de servicio.




Puede ver detalles como el número de ocurrencias y la hora de la última aparición.

En **Detalles**, puede ver:

- La hora en que ocurrió la anomalía de la solapa de servicio
- El nombre del servicio/grupo de servicios
- La dirección IP del servicio
- El estado actual del servicio

## Servidor inestable

January 30, 2024

En algunos casos, el servidor web responde con códigos de estado cuando no puede gestionar las solicitudes por motivos como solicitudes no válidas, sobrecarga temporal o mantenimiento del servidor. Estos errores se muestran con códigos de error, que definen varios escenarios de los errores. Por ejemplo,

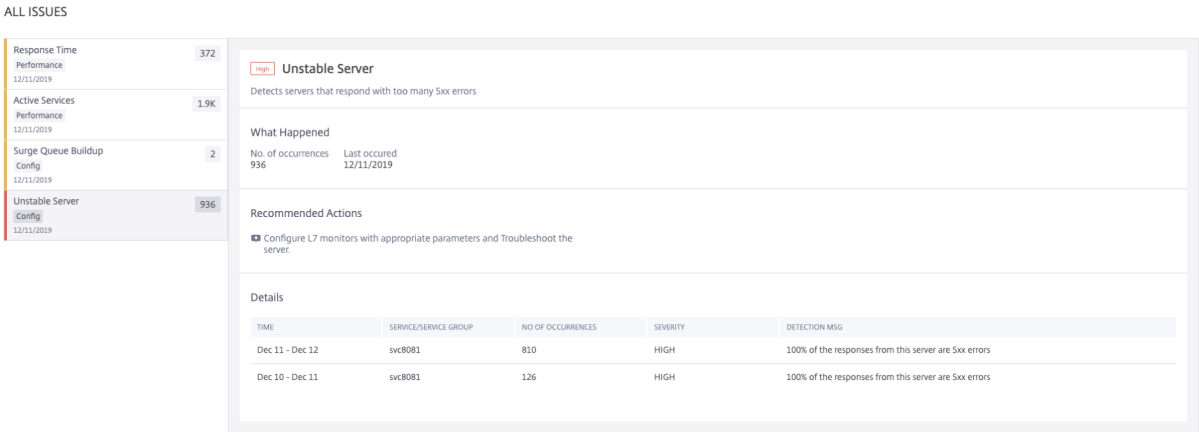
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **502 Puerta de enlace incorrecta**
  El servidor actúa como puerta de enlace o proxy y recibió una respuesta no válida del servidor ascendente.
- **503 Servicio no disponible**
  El servidor no está disponible en este momento. Es posible que los servidores estén sobrecargados o inactivos por motivos de mantenimiento.
- **504 Tiempo de espera de puerta**
  de enlace El servidor actúa como puerta de enlace o proxy y no recibió una respuesta oportuna del servidor ascendente.

Estas pueden ser condiciones temporales, pero a veces hay que implementar una medida correctiva en los servidores web para que las páginas web estén disponibles.

Con el indicador **Servidor inestable**, puede ver estos errores y tomar decisiones sobre las acciones correctivas para solucionar los problemas y garantizar que las solicitudes de los clientes se atiendan y que las páginas web estén siempre disponibles.

Seleccione la ficha **Servidor inestable** para ver los detalles del problema.




Las **acciones recomendadas** para solucionar el problema son:

- Configure los monitores L7 con los parámetros adecuados para el servidor que responde con errores de 5xx. Un monitor es una entidad que realiza un seguimiento del estado del servicio. El dispositivo sondea periódicamente los servidores mediante el monitor enlazado a cada servicio. Si un servidor no responde dentro de un tiempo de espera de respuesta especificado y los sondeos especificados fallan, el servicio se marca como INACTIVO. A continuación, el dispositivo realiza el equilibrio de carga entre los servicios restantes. Para obtener más información sobre cómo configurar un monitor, consulte Monitores personalizados
- Solucionar problemas del servidor

En **Detalles**, puede ver:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- La hora en que se produjo la anomalía del servidor inestable
- El nombre del servicio/grupo de servicios
- Total de ocurrencias
- La gravedad de la anomalía, como alta, baja y media
- El mensaje de detección indicando% de las respuestas de este servicio que informan de errores 5xx

Para obtener información detallada sobre la transacción web de errores del servidor, consulte Análisis de transacciones web para errores del servidor

## Acumulación de sesiones

January 30, 2024

Para todas las transacciones seguras, Citrix ADC realiza el proceso de descarga de SSL para la primera transacción y, a continuación, almacena la sesión SSL en función de la configuración de **reutilización** de sesiones .

Según la velocidad de tráfico, la acumulación de sesiones puede producirse durante un período de tiempo, lo que puede provocar que estas sesiones en Citrix ADC retengan una gran cantidad de memoria.

Los eventos de acumulación de sesiones alertan a los administradores y proporcionan acciones recomendadas para resolver este evento. Haga clic en la ficha **Creación de sesiones** para ver los detalles del problema

En **Detalles**, puede ver:

- La hora en que se produjo la anomalía de acumulación de la sesión
- El nombre del servidor virtual
- La gravedad de la anomalía, como alta, baja y media
- El mensaje indica que hay un número **X** de sesiones SSL disponibles en el servidor virtual y, actualmente, un número **Y** de apretones de manos SSL por segundo dentro de la sesión de tiempo de espera configurada.

La **acción recomendada** para corregir esta anomalía es reducir el tiempo de espera de la sesión o inhabilitar la reutilización de la sesión. Para obtener más información, consulte Tiempo de espera de sesión.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

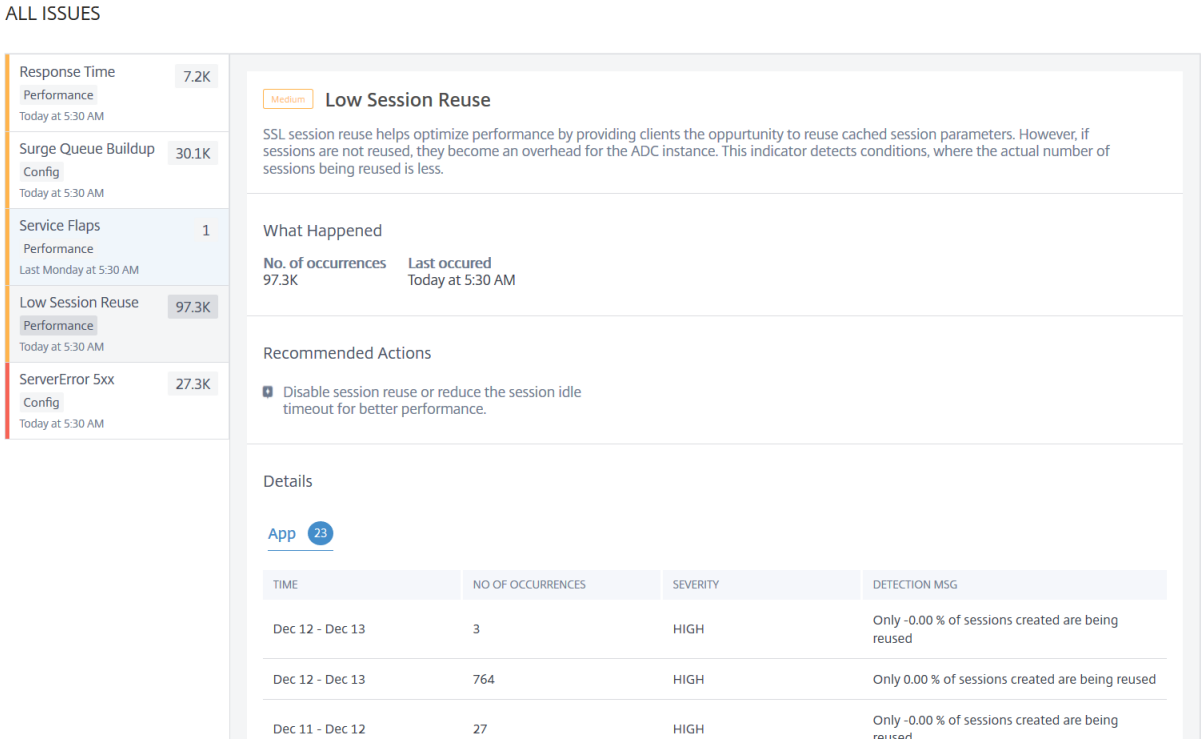
## Reutilización baja de sesiones

January 30, 2024

Las instancias de NetScaler ADC procesan transacciones SSL descargando el proceso de enlace SSL del servidor. Al recibir la respuesta del servidor, la instancia de NetScaler ADC completa la transacción segura con el cliente. Mediante los parámetros de sesión almacenados en caché, la instancia de NetScaler ADC completa el proceso de enlace SSL para las solicitudes consecutivas.

Si en caso de que estas sesiones no se reutilicen, se convierten en una sobrecarga para las instancias de NetScaler ADC. Con el indicador de **baja reutilización de sesiones**, puede identificar si el número real de sesiones que se están reutilizando es menor.

Haga clic en la ficha **Baja reutilización de sesiones** para ver los detalles del problema.




La **acción recomendada** para solucionar el problema consiste en inhabilitar la reutilización de la sesión o reducir el tiempo de espera de la sesión. Para obtener más información, consulte Reutilización de sesiones.

En **Detalles**, puede ver:

- Total de aplicaciones que tienen una reutilización de sesión baja
- La hora en que se produjo la anomalía de baja reutilización de la sesión
- Total de ocurrencias

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

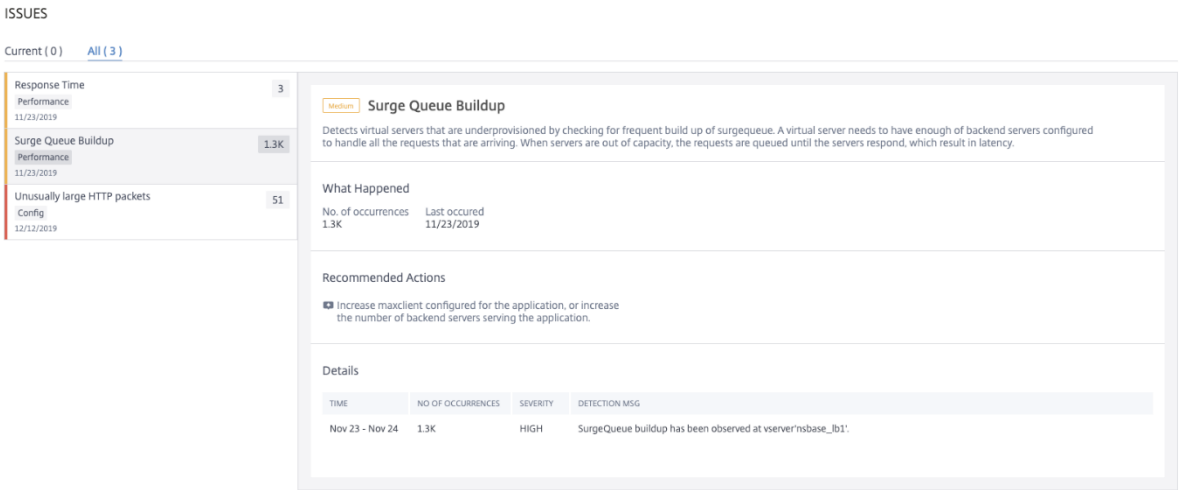
- La gravedad de la anomalía, como alta, baja y media
- El mensaje de detección que indica que solo se están reutilizando el% de las sesiones configuradas

## Acumulación SurgeQueue

January 30, 2024

Cuando un servidor recibe un aumento de solicitudes, el servidor tarda en responder a los clientes. A menudo, la sobrecarga también hace que los clientes reciban páginas de error. Un servidor virtual necesita tener suficientes servidores back-end configurados para manejar las solicitudes entrantes.

Con el indicador de **acumulación de colas de sobretensiones**, puede ver los servidores virtuales que tienen acumulación de colas de sobretensiones. Haga clic en la ficha **Surge Queue Buildup** para ver los detalles del problema.




Las **acciones recomendadas** para solucionar el problema son:

- Aumente el número de límite de conexiones de cliente. Para obtener más información, consulte Establecer un límite en la cantidad de conexiones de clientes
- Aumente los servidores back-end para atender las solicitudes de aplicación

En **Detalles**, puede ver:

- La hora en la que se produjo la anomalía de aumento de la cola
- Total de ocurrencias
- La gravedad de la anomalía, como alta, baja y media

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El mensaje de detección que indica la acumulación de cola de sobretensiones en el servidor virtual

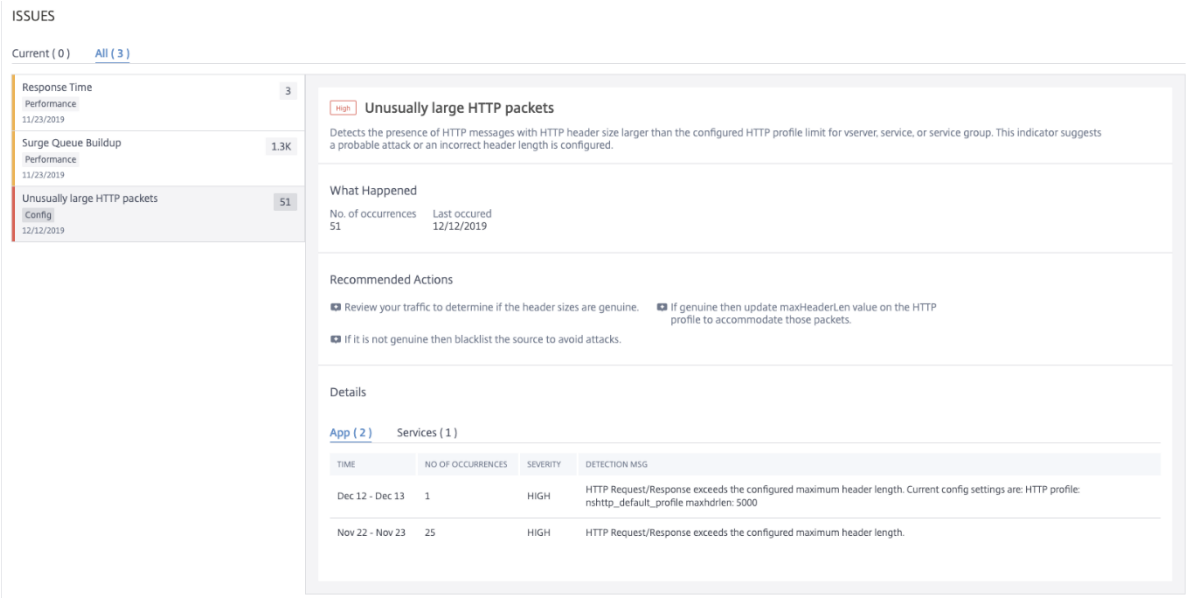
## Paquetes HTTP inusualmente grandes

January 30, 2024

Una transacción HTTP utiliza mensajes de solicitud-respuesta entre el cliente y el servidor. En los mensajes de solicitud y respuesta, los encabezados HTTP son los valores que se muestran en el protocolo HTTP. Puede configurar la longitud del encabezado HTTP en un servidor virtual, servicio o grupo de servicios para evitar errores 4xx

Cuando una solicitud/respuesta HTTP excede la longitud máxima del encabezado, puede ser un posible ataque. Con el indicador de **paquetes HTTP inusualmente grandes**, puede ver las ocurrencias en las que los mensajes HTTP con un tamaño de encabezado HTTP superan los valores configurados.

Haga clic en la ficha **Paquetes HTTP inusualmente grandes** para ver los detalles del problema.




Las **acciones recomendadas** para solucionar el problema son:

- Revise el tráfico para determinar que el tamaño del encabezado es auténtico. Si el tamaño del encabezado es original, actualice el valor del encabezado en el perfil HTTP. Para obtener más información, consulte Comprobación de desbordamientode búfer
- Si el tamaño del encabezado no es original, bloquee la lista de origen para evitar ataques.

En **Detalles**, puede ver:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El tiempo que ocurrió la anomalía
- Total de ocurrencias
- La gravedad de la anomalía, como alta, baja y media
- El mensaje de detección que indica la longitud actual del encabezado HTTP configurada en el servidor virtual, el servidor o el grupo de servicios

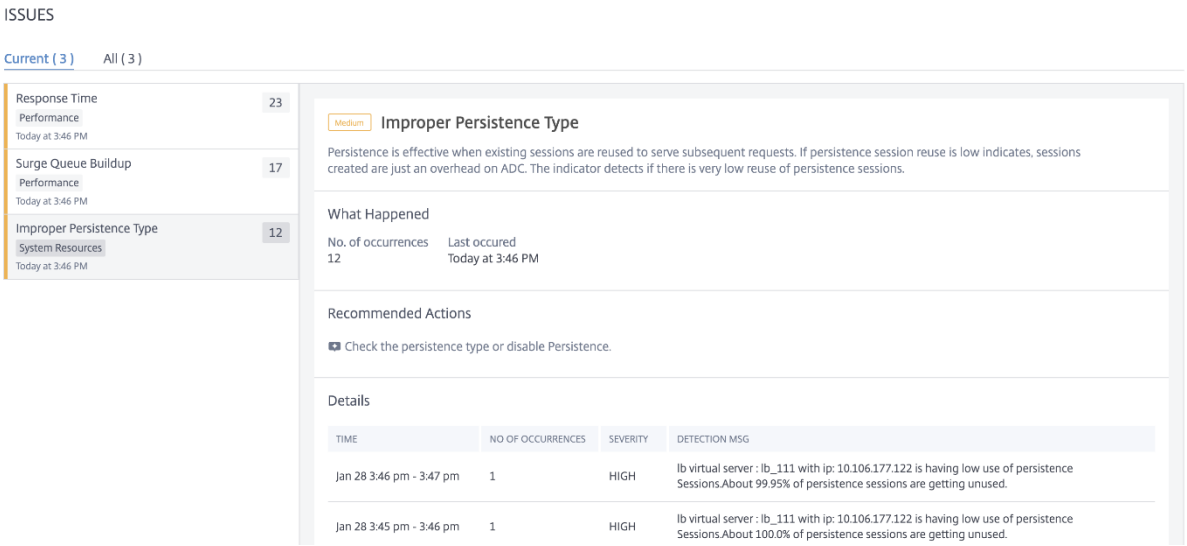
## Tipo de persistencia incorrecto

January 30, 2024

Debe configurar la persistencia en un servidor virtual si quiere mantener los estados de las conexiones en los servidores representados por ese servidor virtual (por ejemplo, las conexiones utilizadas en el comercio electrónico). A continuación, el dispositivo utiliza el método de equilibrio de carga configurado para la selección inicial del servidor, pero reenvía todas las solicitudes posteriores al mismo servidor desde el mismo cliente.

La persistencia es efectiva cuando las sesiones existentes se reutilizan para atender solicitudes posteriores. Si la reutilización de la sesión de persistencia es baja, las sesiones creadas en ADC son solo una sobrecarga.

Con el indicador de **tipo de persistencia incorrecto**, puede determinar si el uso de persistencia en un servidor virtual es bajo. Haga clic en la ficha **Tipo de persistencia incorrecto** para ver los detalles del problema.




La **acción recomendada** para solucionar el problema es comprobar el tipo de persistencia o inhabilitar la persistencia. Para obtener más información, consulte Configuración de persistencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En **Detalles**, puede ver:

- El tiempo que ocurrió la anomalía
- Total de ocurrencias
- La gravedad de la anomalía, como alta, baja y media
- El mensaje de detección que indica el% de sesiones que no se utilizan

## TCP volver a ensamblar visitas de límite de cola

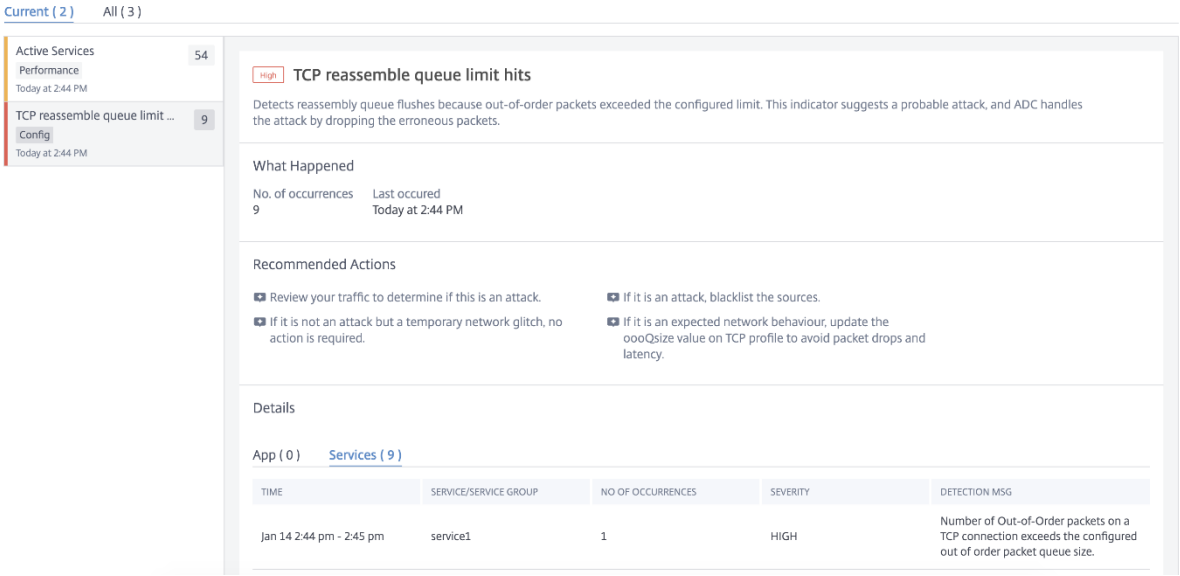
January 30, 2024

TCP mantiene una cola fuera de orden para mantener los paquetes OOO en la comunicación TCP. Esta configuración afecta a la memoria NetScaler ADC si el tamaño de la cola es largo, ya que los paquetes deben mantenerse en la memoria en tiempo de ejecución.

Este tamaño de cola debe estar en un nivel optimizado en función de las funciones de la red y de la aplicación.

Mediante el indicador de **visitas de límite de cola de reensamblar TCP**, puede ver si los paquetes fuera de orden en una conexión TCP exceden el tamaño de cola de paquetes fuera de orden configurado.

Haga clic en la ficha **Límite de visitas a la cola de reensamblaje de TCP** para ver los detalles del problema.




Las **acciones recomendadas** para solucionar el problema son:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Revisar el tráfico y bloquear la lista de origen si se trata de un ataque
- Si este comportamiento es un comportamiento de red esperado, actualice el valor de tamaño de paquetes fuera de orden en el perfil TCP. Para obtener más información, consulte Optimización de TCP
- Si se trata de una falla temporal de la red, entonces no se requiere ninguna acción adicional

En **Detalles**, puede ver:

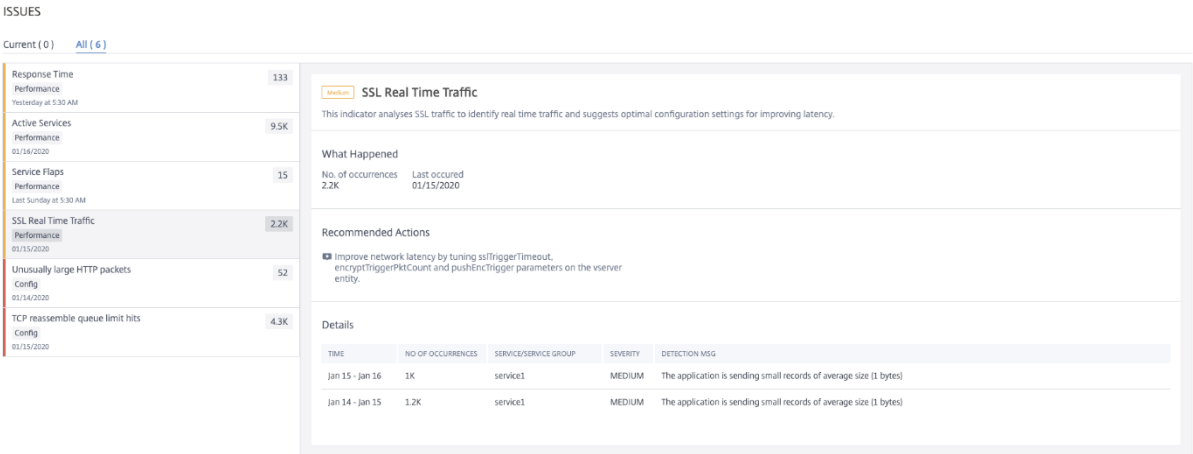
- El tiempo que ocurrió la anomalía
- Total de ocurrencias
- La gravedad de la anomalía, como baja, media y alta
- El mensaje de detección que indica el perfil TCP actual y la configuración de oooQsize

## Tráfico en tiempo real SSL

January 30, 2024

En la instancia de NetScaler ADC, puede usar un perfil SSL para procesar el tráfico SSL. El perfil SSL comprende ciertos parámetros SSL para servidores, servicios y grupos de servicios virtuales. El indicador de **tráfico SSL en tiempo real** analiza el tráfico SSL para identificar el tráfico en tiempo real y sugiere ajustes de configuración óptimos para mejorar la latencia.

Haga clic en la ficha **Tráfico SSL en tiempo real** para ver los detalles del problema.




La **acción recomendada** para solucionar el problema es mejorar la latencia de red mediante la actualización de los parámetros SSL. Para obtener más información, consulte Parámetros SSL globales.

En **Detalles**, puede ver:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El tiempo que ocurrió la anomalía
- El nombre del servicio/grupo de servicios
- La gravedad de la anomalía, como baja, media y alta
- El mensaje de detección con la configuración actual en la aplicación

## Panel de seguridad de aplicaciones

January 30, 2024

El panel **de seguridad de aplicaciones** proporciona información general sobre las métricas de seguridad para las aplicaciones detectadas/con licencia. Este panel muestra la información sobre los ataques de seguridad de las aplicaciones descubiertas o con licencia, como los ataques de sincronización, los ataques de ventanas pequeñas, los ataques de inundación de DNS, etc.

Para ver las métricas de seguridad en el panel de seguridad de la aplicación:

1. Vaya a **Aplicaciones** > **Panel de seguridad** de aplicaciones .
2. Seleccione la dirección IP de la instancia en la lista Instancia.

   Los informes incluyen la siguiente información para cada aplicación:

   - **Índice**de amenazas . Sistema de clasificación de un solo dígito que indica la importancia de los ataques a la aplicación. Cuanto más críticos sean los ataques a una aplicación, mayor será el índice de amenazas para esa aplicación. Los valores oscilan entre 1 y 7.

     El índice de amenazas se basa en la información de ataque. La información relacionada con el ataque, como el tipo de infracción, la categoría del ataque, la ubicación y los detalles del cliente, proporciona una visión de los ataques a la aplicación. La información de infracción se envía a NetScaler ADM solo cuando se produce una infracción o un ataque. Una gran cantidad de brechas y vulnerabilidades conducen a un valor elevado del índice de amenazas.

   - **Índice**de seguridad . Sistema de clasificación de un solo dígito que indica con qué seguridad ha configurado las instancias NetScaler ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. Los valores oscilan entre 1 y 7.

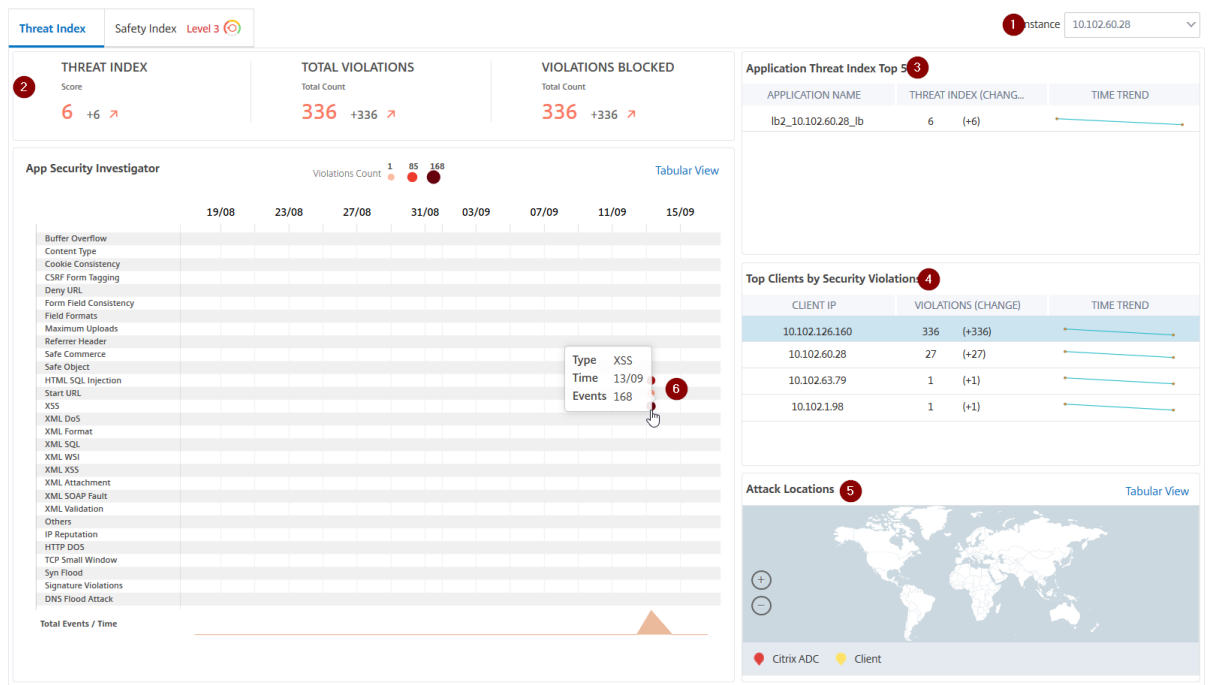
     El índice de seguridad considera tanto la configuración del firewall de aplicaciones como la configuración de seguridad del sistema NetScaler ADC. Para un valor de índice de seguridad elevado, ambas configuraciones deben ser fuertes. Por ejemplo, si se realizan comprobaciones rigurosas del firewall de aplicaciones, pero no se proporcionan medidas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

de seguridad del sistema NetScaler ADC, como una contraseña segura para el `nsroot` usuario, a las aplicaciones se les asigna un valor de índice de seguridad bajo.

Puede ver las discrepancias reportadas en el **investigador de seguridad de aplicaciones**.

## Detalles del índice de amenazas




**1**: Muestra la dirección IP de la instancia NetScaler ADC para la que puede ver detalles.

**2**: Muestra detalles como la puntuación del índice de amenazas, el total de infracciones ocurridas y el total de infracciones bloqueadas.

**3**: muestra el servidor virtual de la instancia seleccionada.

**4**: muestra las violaciones de seguridad según los clientes. Se muestra el gráfico App Security Investigator para cada cliente. Puede hacer clic en cada IP de cliente para ver los resultados.

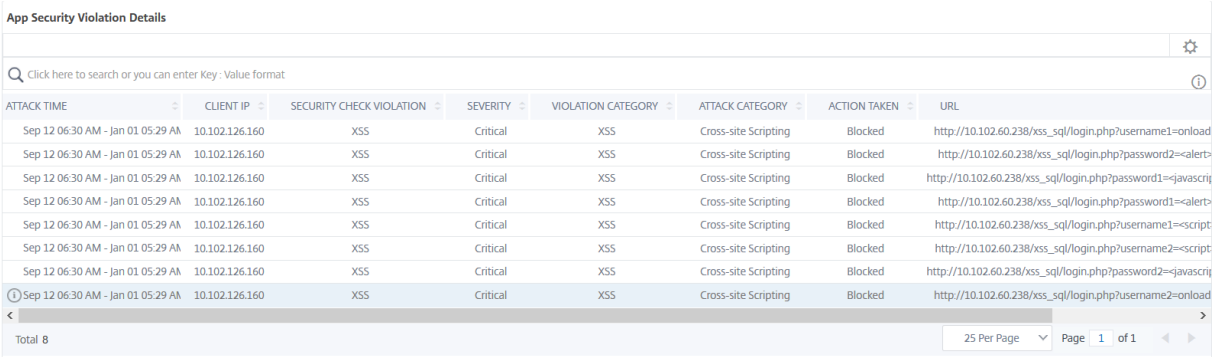
**5**: Muestra las infracciones en la vista de mapa y en la vista tabular.

**6**: muestra los detalles de la infracción. Al situar el puntero del mouse sobre el gráfico, se muestran los detalles como el tipo de infracción, la hora del ataque y el total de eventos.

Al hacer clic en un gráfico de burbujas, los detalles se muestran en la página **Detalles de infracción de seguridad de aplicaciones**. Por ejemplo, si quiere ver más detalles de la infracción de scripts entre sitios (scripts entre sitios), haga clic en el gráfico rellenado para **XSS** en **App Security Investigator**.

**Los detalles de infracción de seguridad de la aplicación** se muestran con detalles de infracción como tiempo de ataque, categoría de ataque, gravedad, URL, etc.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




También puede hacer clic en la opción **Configuración** para seleccionar las opciones que quiere que se muestren.

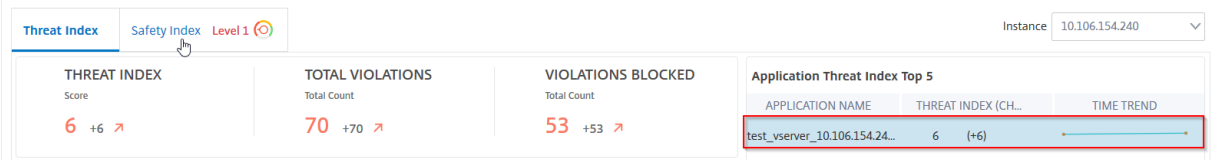
## Detalles del índice de seguridad

Después de revisar la exposición a amenazas de una aplicación, quiere determinar qué configuraciones de seguridad de la aplicación están implementadas y qué configuraciones faltan para esa aplicación. Puede obtener esta información profundizando en el resumen del índice de seguridad de la aplicación.

El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

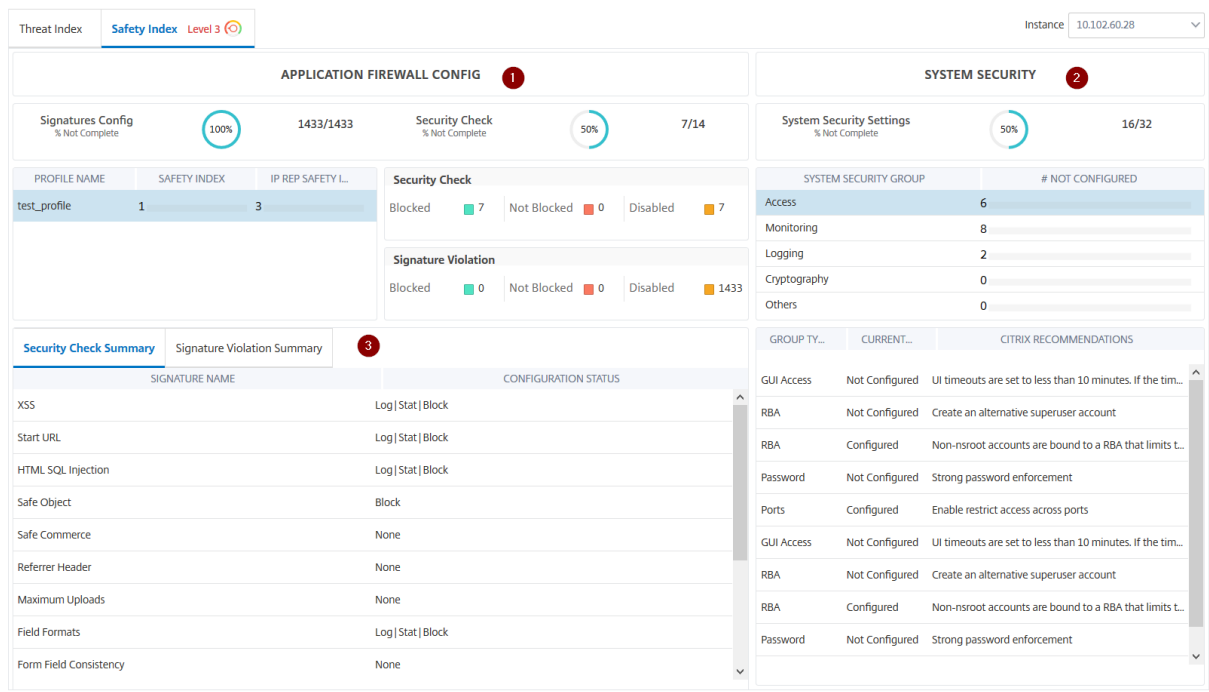
- **Configuración**del firewall de aplicaciones . Muestra cuántas entidades de firma y seguridad no están configuradas.
- **Seguridad del sistema NetScaler ADM**. Muestra cuántas opciones de seguridad del sistema no están configuradas.

Para ver los detalles del **índice de seguridad**, seleccione un servidor/aplicación virtual y haga clic en la ficha **Índice de seguridad**.




Se muestran los detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**1**: Muestra la información detallada de las configuraciones de Application Firewall.

**2**: Muestra la información detallada de Seguridad del sistema. Haga clic en cada grupo de seguridad para obtener detalles sobre el estado actual y las recomendaciones de Citrix.

**3**: Muestra el resumen de comprobación de seguridad e infracción de firma.

También puede ver un resumen del entorno de amenazas si habilita la información de seguridad para los servidores virtuales y, a continuación, navega a **Analytics** > **Security Insight**. Para obtener más información sobre el caso de uso del índice de seguridad, consulte información de seguridad

## Gráfico de servicio

January 30, 2024

La función de gráfico de servicio de NetScaler ADM permite supervisar todos los servicios de una representación gráfica. Esta función también le permite ver un análisis detallado y métricas accionables de los servicios. Puede ver el gráfico de servicio para:

- Aplicaciones configuradas en todas las instancias de NetScaler ADC
- Aplicaciones de Kubernetes
- Aplicaciones web de 3 niveles

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Gráfico de servicio para aplicaciones en todas las instancias de NetScaler ADC

La función de gráfico de servicio global le permite obtener una visualización holística de la `clients to infrastructure to application` vista. Desde esta vista gráfica de servicio de un solo panel, como administrador, puede:

- Comprender desde qué región están accediendo los usuarios a las aplicaciones específicas (aplicaciones web de 3 niveles y aplicación de microservicios)
- Visualice la vista de infraestructura (instancia de NetScaler ADC) en la que se procesa la solicitud del cliente
- Comprender si los problemas ocurren desde el cliente, la infraestructura o la aplicación
- Más detalles para solucionar el problema

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Global** para ver:

- Detalles integrales de todas las aplicaciones conectadas desde el cliente a los servidores backend
- Todas las instancias de NetScaler ADC conectadas a sus respectivos centros de datos

  > **Nota**
  >
  > Puede ver los centros de datos solo si tiene aplicaciones GSLB.

- Información de métricas del cliente
- Información de métricas de NetScaler ADC
- Todas las instancias de NetScaler ADC que tienen aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicio discretas
- Las 4 principales aplicaciones de puntuación baja que pertenecen a aplicaciones personalizadas, aplicaciones discretas y aplicaciones de microservicios
- Información de métricas para los 4 principales servidores virtuales de puntuación baja
- El estado de las aplicaciones (aplicaciones discretas, aplicaciones personalizadas y aplicaciones de microservicios) como **Crítica**, **Revisión**, **Buena** y **No Aplicable**.

Para obtener más información, consulte Vista holística de las aplicaciones en el gráfico de servicio.

### Gráfico de servicio para aplicaciones Kubernetes

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Microservicios** para ver:

- Garantice el performance general de las aplicaciones end-to-end

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Identifique los cuellos de botella creados por la interdependencia de los diferentes componentes de sus aplicaciones
- Reúna información sobre las dependencias de los diferentes componentes de sus aplicaciones
- Supervise los servicios dentro del clúster de Kubernetes
- Supervisa qué servicio tiene problemas
- Compruebe los factores que contribuyen a los problemas de rendimiento
- Ver la visibilidad detallada de las transacciones HTTP del servicio
- Analizar las métricas HTTP, TCP y SSL

Al visualizar estas métricas en NetScaler ADM, puede analizar la causa raíz de los problemas y realizar las acciones necesarias para solucionar problemas más rápidamente. El gráfico de servicio muestra sus aplicaciones en varios servicios de componentes. Estos servicios que se ejecutan dentro del clúster de Kubernetes pueden comunicarse con varios componentes dentro y fuera de la aplicación. Para empezar, consulta Configurar el gráfico de servicios.

### Gráfico de servicios para aplicaciones web de 3 niveles

Vaya a **Aplicaciones > Gráfico de servicio** y haga clic en la ficha **Aplicaciones Web** para ver:

- Detalles sobre cómo se configura la aplicación (con el servidor virtual de conmutación de contenido y el servidor virtual de equilibrio de carga)

  Para las aplicaciones GSLB, puede ver los servidores virtuales de centros de datos, instancias de ADC, CS y LB.
- Transacciones de extremo a extremo desde el cliente hasta el servicio
- La ubicación desde la que el cliente accede a la aplicación
- El nombre del centro de datos donde se procesan las solicitudes de cliente y las métricas NetScaler ADC del centro de datos asociadas (solo para aplicaciones GSLB)
- Detalles de métricas para clientes, servicios y servidores virtuales
- Si los errores son del cliente o del servicio
- El estado del servicio, como **Crítico**, **Revisado**y **Bueno**. NetScaler ADM muestra el estado del servicio según el tiempo de respuesta del servicio y el recuento de errores.
  - **Crítico (rojo)**: Indica cuándo el tiempo promedio de respuesta del servicio es superior a 200 ms Y el recuento de errores es > 0
  - **Revisión (naranja)**: Indica si el tiempo promedio de respuesta del servicio es > 200 ms O el recuento de errores es > 0

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - **Bueno (verde)**: Indica que no hay errores y que el tiempo medio de respuesta del servicio es inferior a 200 ms

- El estado del cliente, como **Crítico**, **Revisado**y **Bueno**. NetScaler ADM muestra el estado del cliente en función de la latencia de la red del cliente y el recuento de errores.
  - **Crítico (rojo)**: indica si la latencia promedio de la red del cliente es > 200 ms Y el recuento de errores es > 0
  - **Revisión (naranja)**: Indica si la latencia promedio de la red del cliente es > 200 ms O el recuento de errores es > 0
  - **Bueno (verde)**: Indica que no hay ningún error y que la latencia media de la red del cliente es < 200 ms.

- El estado del servidor virtual, como **Crítico**, **Revisado**y **Correcto**. NetScaler ADM muestra el estado del servidor virtual en función de la puntuación de la aplicación.
  - **Crítico (rojo)**: Indica si la puntuación de la aplicación es inferior < 40
  - **Reseña (naranja)**: Indica si la puntuación de la aplicación está entre 40 y 75
  - **Bueno (verde)**: Indica cuando la puntuación de la aplicación es > 75

**Puntos a tener en cuenta:**

- En el gráfico de servicios solo se muestran los servidores virtuales de equilibrio de carga, conmutación de contenido y GSLB.
- Si ningún servidor virtual está enlazado a una aplicación personalizada, los detalles no son visibles en el gráfico de servicio de la aplicación.
- Puede ver las métricas de los clientes y servicios en el gráfico de servicios solo si se producen transacciones activas entre los servidores virtuales y la aplicación web.
- Si no hay transacciones activas disponibles entre los servidores virtuales y la aplicación web, solo puede ver los detalles en el gráfico de servicios en función de los datos de configuración, como el equilibrio de carga, el cambio de contenido, los servidores virtuales GSLB y los servicios.
- Si se realizan cambios en la configuración de la aplicación, puede tardar 10 minutos en reflejarse en el gráfico de servicio.

Para obtener más información, consulte Gráfico de servicio para aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configuración del gráfico de servicio

January 30, 2024

## Requisitos de software

| Distribución de Kubernetes | Versión de Kubernetes | Interfaces de red de contene-dores (CNI) | Versión CPX | Versión CIC | Versión de Citrix ADM | Versión del agente Citrix ADM |
|---|---|---|---|---|---|---|
| Código abierto | v1.16.3 | Franela, Calico o Canal | 13.0—41.28 o posterior | 1.5.25 o posterior | 13.0—47.22 o posterior | 13.0—47.22 o posterior |

Puede configurar el clúster de Kubernetes con varias topologías de implementación y la siguiente tabla proporciona las topologías que se admiten en el gráfico de servicios:

| Topología | Gráfico de servicio soportado |
|---|---|
| Ingreso unificado o de un solo nivel | Sí |
| Doble capa | Sí |
| Cloud | Sí, pero el equilibrador de carga en la nube no se muestra en el gráfico |
| Malla de servicio lite | Sí |
| Malla de servicio | Sí |
| Servicios de tipo LoadBalancer | No |
| Servicios de tipo NodePort | No |

Para completar la configuración del gráfico de servicio en NetScaler ADM, haga clic en el tipo de topología que ha configurado para el clúster de Kubernetes y complete los procedimientos mencionados:

- Topología de ingreso unificada o de un solo nivel
- Topología de doble capa o Service Mesh Lite
- Topología de malla de servicio

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El procedimiento para configurar el gráfico de servicio para topologías de malla de servicio dual y de malla de servicio sigue siendo el mismo.

### Antes de comenzar

Puede ver el gráfico de servicios en los siguientes casos:

- Clúster de NetScaler ADM y Kubernetes en la misma red (por ejemplo, el clúster de NetScaler ADM y Kubernetes hospedado en el mismo Citrix Hypervisor).
- Citrix ADM y Kubernetes se agrupan en una red diferente. En este caso, debe configurar un agente local y registrar el agente en la red, donde se aloja el clúster de Kubernetes.

### Topología de ingreso unificada o de nivel único

Asegúrese de lo siguiente:

- Cluster Kubernetes configurado con topología de ingreso unificada o de nivel único.
- Se agregó una instancia VPX, MPX, SDX, BLX en NetScaler ADM y se habilitó **Web Insight**.
- Se agregó un clúster de Kubernetes en Citrix ADM.

### Topología de doble capa o Service Mesh Lite

Asegúrese de lo siguiente:

- Se configuró el clúster de Kubernetes con cualquiera de las topologías admitidas.
- Se configuraron rutas estáticas en NetScaler ADM para permitir la comunicación entre NetScaler ADM y NetScaler ADC CPX.

  > **Nota**
  >
  > Puede omitir este procedimiento si ha implementado NetScaler ADM como un microservicio en el mismo clúster.

- Descargué los archivos de implementación de muestra del repositorio de GitHub.
- Se agregaron los parámetros necesarios en el archivo CPX YAML para garantizar el registro correcto de CPX en Citrix ADM.
- Se agregó una instancia VPX, MPX, SDX o BLX en NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Se agregó el clúster de Kubernetes en NetScaler ADM.
- Se implementó una aplicación de microservicios de muestra.
- Implementación de NetScaler ADC CPX y CPX registrado en ADM (aplicable solo para arquitectura de dos niveles)
- Se habilitó la selección automática de servidores virtuales para licenciar los servidores virtuales.
- Se habilitó la configuración de transacciones web y transacciones TCP en **Todo** para que el agente NetScaler ADM obtenga transacciones HTTP y TCP.
- Se envió el tráfico a los microservicios.

### Topología de malla de servicio

Asegúrese de lo siguiente:

- Se configuró la versión del clúster de Kubernetes `1.14.0` con cualquiera de las siguientes topologías de malla de servicio:
  - NetScaler ADC CPX como proxy sidecar para Istio
  - NetScaler ADC como puerta de enlace de entrada para Istio

  Para obtener más información, consulte Arquitectura de implementación del adaptador NetScaler ADC Istio
- `admissionregistration.k8s.io/v1beta1` API habilitada. Puede verificar la API mediante:

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  El siguiente resultado indica que la API está habilitada:

  ```
  admissionregistration.k8s.io/v1beta1
  ```
- Se ha instalado Istio `istio v.1.3.0`.
- Versión 3.x de Helm instalada.
- Se configuraron rutas estáticas en NetScaler ADM para permitir la comunicación entre NetScaler ADM y NetScaler ADC CPX.

  > **Nota**
  >
  > Puede omitir este procedimiento si ha implementado el agente NetScaler ADM como un microservicio en el mismo clúster.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

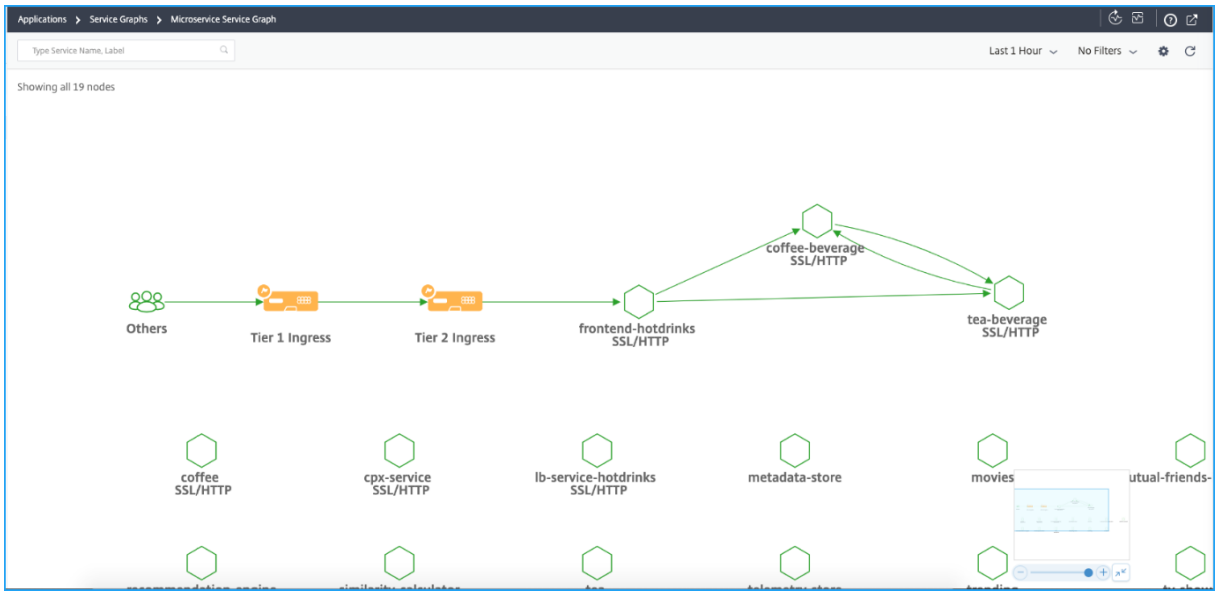
- Se configuraron los parámetros requeridos para rellenar los datos de topología de malla de servicio.
- Se implementó una aplicación de muestra.
- Se agregó el clúster de Kubernetes en NetScaler ADM.
- Se habilitó la selección automática de servidores virtuales para licenciar los servidores virtuales.
- Se habilitó la configuración de transacciones web y transacciones TCP en **Todo** para que el agente NetScaler ADM obtenga transacciones HTTP y TCP.
- Se envió el tráfico a los microservicios.

## Ver detalles en el gráfico de servicio

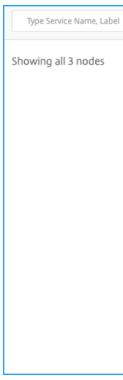
January 30, 2024

En NetScaler ADM, vaya a **Aplicación > Gráficos de servicio > Gráfico de servicio Kubernetes** y seleccione la duración del tiempo en la lista para ver los detalles del gráfico de servicio.

Topología de Mesh Lite de dos niveles o de servicio




Topología




- **Ingreso de nivel 1** : Citrix Ingress Controller dentro del clúster de Kubernetes configura una instancia de NetScaler ADC (VPX/MPX/SDX/BLX) fuera del clúster de Kubernetes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Ingreso de nivel 2** : Citrix Ingress Controller funciona como sidecar junto con la instancia de NetScaler ADC CPX dentro del clúster de Kubernetes.
- **Ingreso**: muestra todas las demás topologías de implementación.

## Panel de gráficos de servicio

**1** - Mapa de red de extremo a extremo de su aplicación que muestra cómo se comunican los servicios de sus componentes

**2** —Gráfico que indica aciertos y errores durante un tiempo específico

**3** —Barra de búsqueda para buscar servicios

**4** —Lista de horarios para seleccionar la duración del tiempo

**5** - Aplicar filtros a los servicios de visualización

**6** —Icono de configuración

**7** —Vista de acercamiento y alejamiento

**8** —Vista gráfica o vista tabular

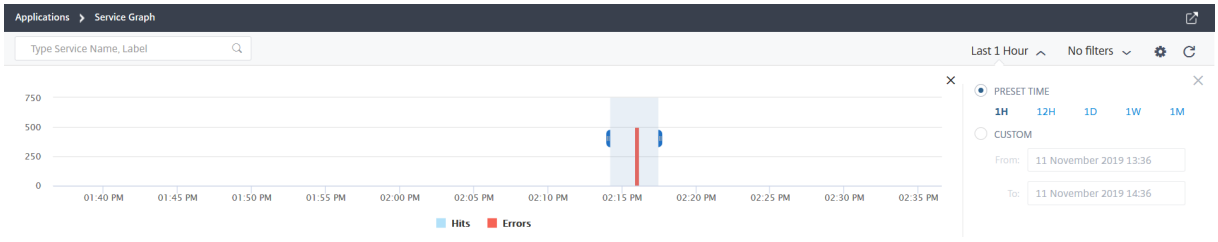
En función de la duración de tiempo seleccionada, puede ver el gráfico de servicio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Icono de servicio | Descripción |
|---|---|
| | El ancho del borde indica el número de aciertos. Cuanto mayor o mayor sea el ancho del borde, indica que el número de aciertos es mayor. |
| | El servicio con un icono de advertencia indica que el servicio tiene errores. |
| | El servicio con un icono de cronómetro indica que el servicio tiene problemas de latencia o de tiempo de respuesta. |
| | El servicio con iconos de cronómetro y advertencia indican que el servicio tiene errores y problemas de latencia/tiempo de respuesta. |

> **Nota**
>
> Si un servicio no tiene ningún icono de advertencia o cronómetro, indica que el servicio tiene anomalías o brecha de umbral para Hits.

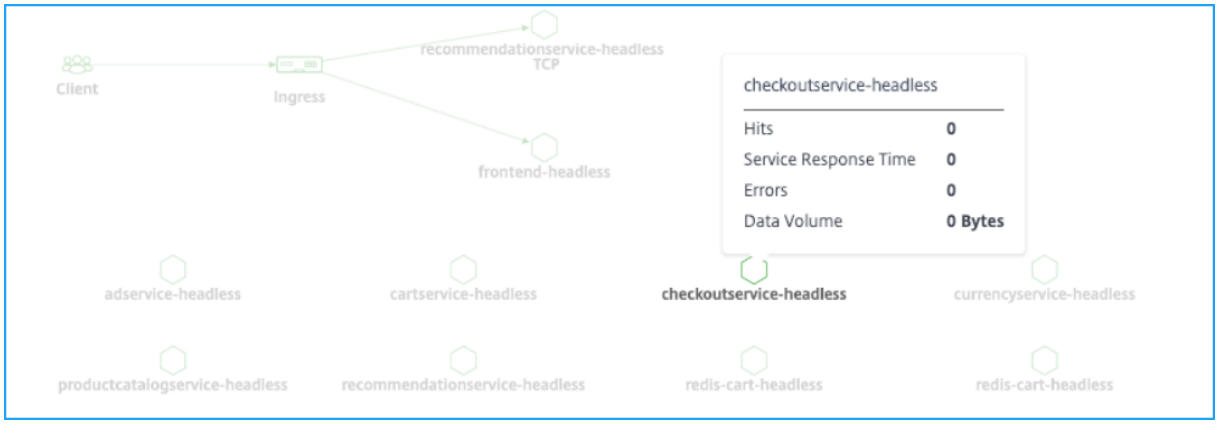
En función de la duración de tiempo seleccionada, puede ver el gráfico de servicio. Seleccione el período de tiempo del gráfico que indica aciertos para profundizar más para obtener información adicional.



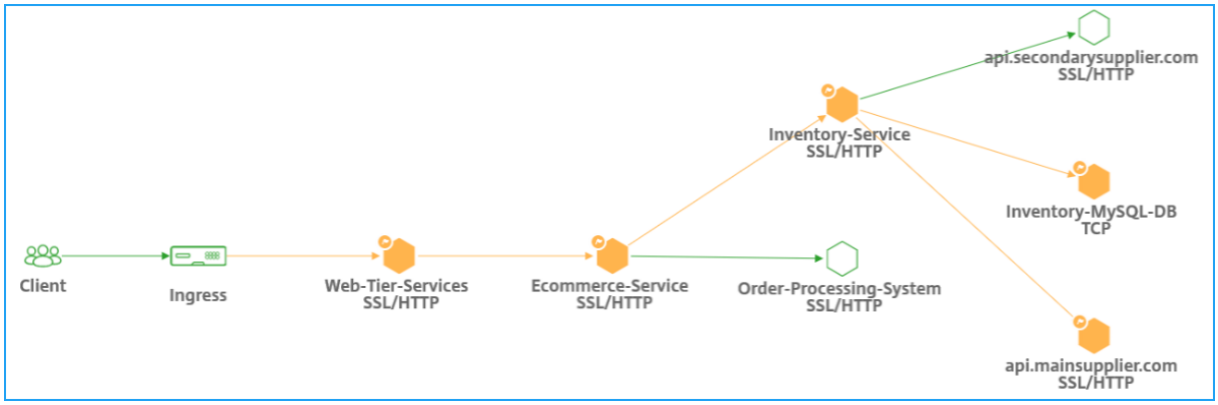

> **Nota**
>
> Si NetScaler ADM no recibe transacciones activas, solo puede ver los servicios que la instancia

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> de NetScaler ADC equilibra la carga. Al pasar el puntero del mouse sobre un servicio, todas las métricas se muestran como 0.

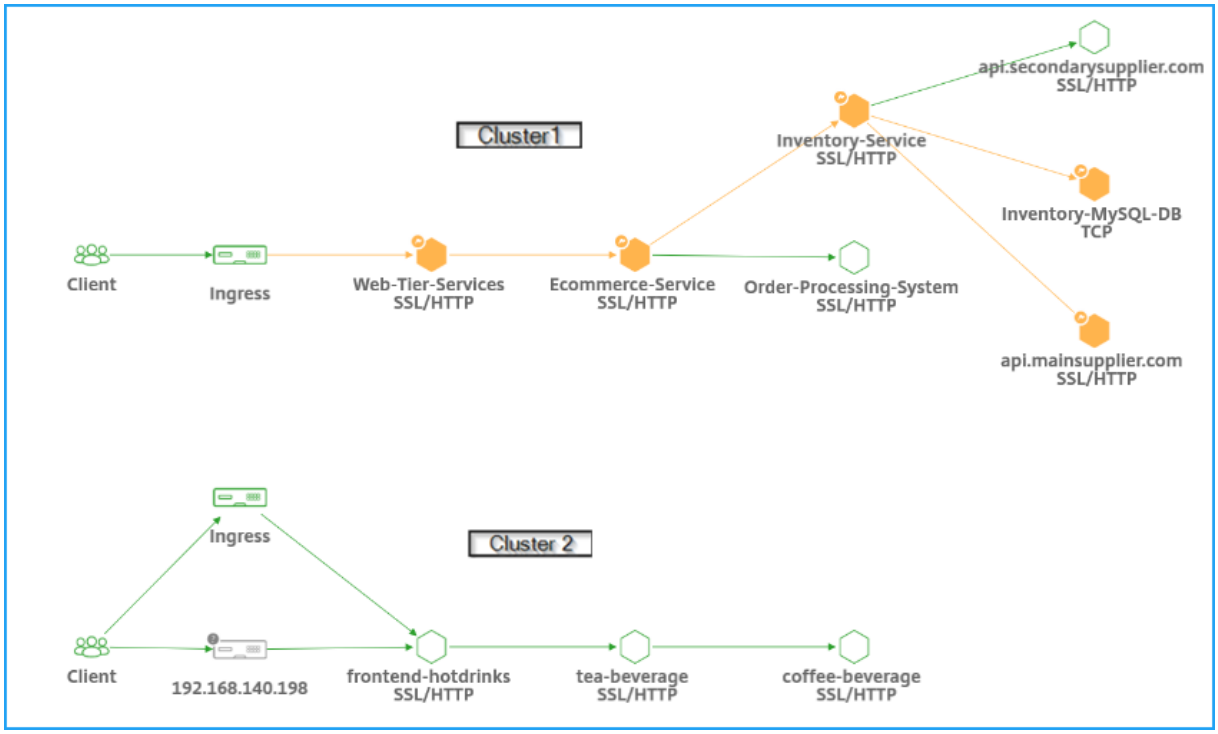



El gráfico de servicio se muestra con el protocolo utilizado por los servicios. Tenga en cuenta que tiene los siguientes servicios ejecutándose en su clúster de Kubernetes como se muestra en la imagen:




> Nota
>
> Si ha agregado varios clústeres en **Orquestación** > **Kubernetes** > **Clusters**, puede ver los servicios asociados a cada clúster.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Puede ver el siguiente estado de sus servicios:

- **Crítico (rojo)**: Indica cuándo el tiempo promedio de respuesta del servicio es superior a 200 ms Y el recuento de errores es > 0
- **Revisión (naranja)**: Indica si el tiempo promedio de respuesta del servicio es > 200 ms O el recuento de errores es > 0
- **Bueno (verde)**: Indica que no hay errores y que el tiempo medio de respuesta del servicio es inferior a 200 ms

Los siguientes son protocolos que permiten identificar el protocolo utilizado por un servicio:

- **TCP**: indica que el servicio utiliza el protocolo TCP.
- **SSL, HTTP**: indica que el servicio utiliza el protocolo SSL sobre HTTP.
- **SSL, TCP**: indica que el servicio utiliza el protocolo SSL sobre TCP.

> **Nota**
>
> El servicio sin protocolo indica que el servicio está utilizando el protocolo HTTP.

### Ver tendencias de métricas clave mediante la vista tabular

Mediante la vista tabular, puede ver:

- Métricas clave para el servicio

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

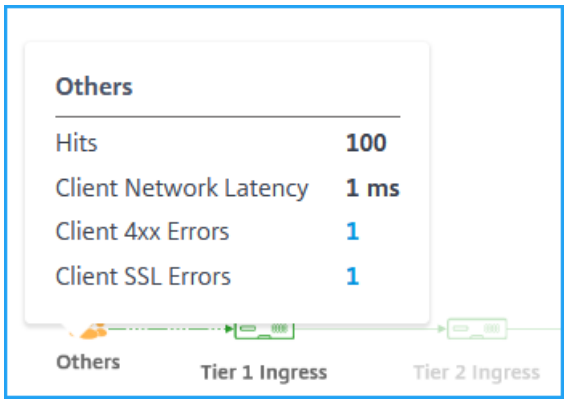
- Métricas clave entre un servicio de origen y un servicio de destino

Como administrador, mediante estas métricas clave, puede analizar las tendencias de las señales de oro para la duración de tiempo seleccionada.

## Ver métricas de cliente

Puede ver desde qué ubicación está accediendo el cliente al servicio. Como administrador, puede visualizar las métricas del cliente y analizar los problemas que se producen desde el cliente.

Coloque el puntero del mouse (mouse) sobre una región de cliente para ver las métricas.




- **Hits** - Indica el total de aciertos recibidos por el cliente.
- **Latencia de red cliente: indica la latencia** promedio de la red del cliente.
- **Errores del cliente 4xx**: indica el total de errores del cliente 4xx.
- **Errores de SSL del cliente**: indica el total de errores de SSL del cliente.

**Bloques IP en NetScaler ADM**: NetScaler ADM puede reconocer la ubicación del cliente si el cliente utiliza una dirección IP pública. NetScaler ADM tiene su archivo CSV de ubicación integrado que coincide con la ubicación según el intervalo de direcciones IP del cliente.

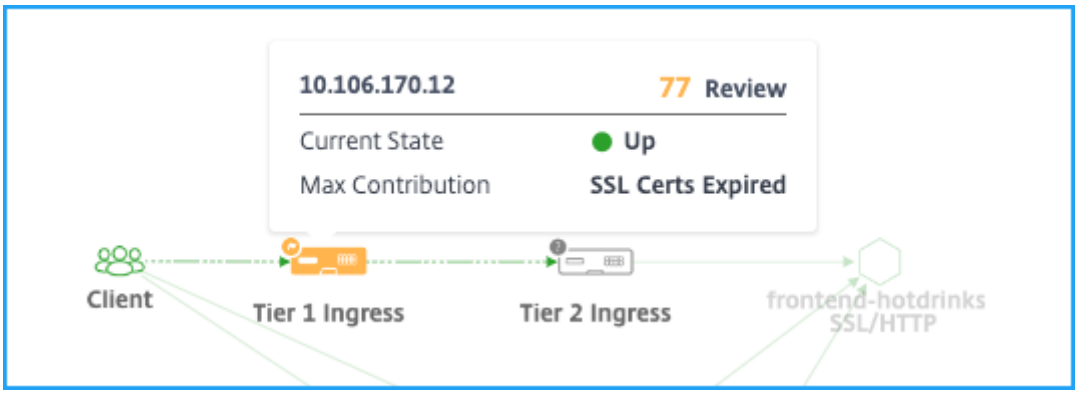
NetScaler ADM puede reconocer la ubicación del cliente con dirección IP privada solo cuando la dirección IP se agrega al servidor NetScaler ADM. Por ejemplo, si la dirección IP del cliente se encuentra dentro de un intervalo de direcciones IP privadas asociado a la ciudad A, NetScaler ADM reconoce que el tráfico se origina desde la ciudad A para este cliente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para obtener más información, consulte Crear un bloqueo de IP privada.

### Ver métricas de ingreso

Puede ver el tipo de ingreso utilizado en el clúster de Kubernetes.




- Dirección IP de NetScaler ADC y su puntuación
- **Estado actual**: indica si la instancia de NetScaler ADC es Activo, Inactivo o Fuera de estado
- **Contribución máxima**: indica el problema que está afectando a la puntuación de la instancia

Para la topología de un solo nivel, solo se puede ver una única **entrada**.

Haga clic en el botón **Ingress** (Ingress) para obtener más detalles. Para obtener más información, consulte Ver detalles de entrada para solucionar problemas.

## Ver métricas TCP y SSL

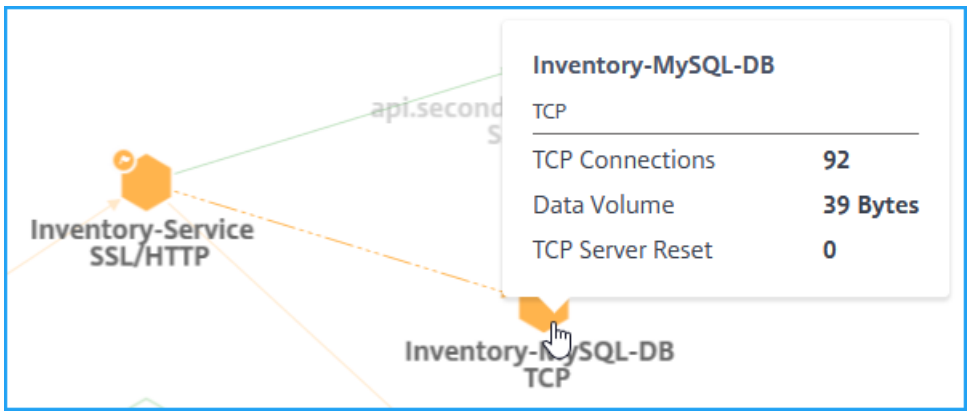
Mediante las métricas TCP y SSL, puede:

- Ver detalles de la conexión TCP entre los servicios
- Determine si los problemas relacionados con el TCP provienen del servicio de origen o de destino
- Ver si el error de SSL proviene del servicio de origen o destino
- Ver la versión del protocolo SSL utilizada por los servicios SSL

### Métricas de TCP

Pase el puntero del mouse sobre un servicio TCP o su servicio entrante asociado para ver las métricas de TCP.

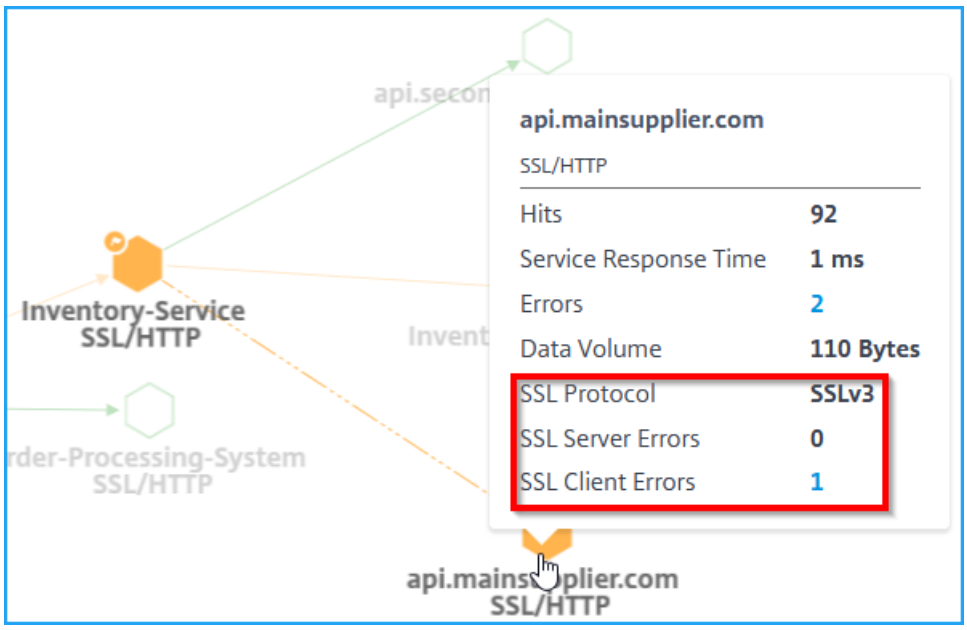
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Conexiones TCP**: número total de conexiones establecidas entre los servicios
- **Volumen de datos**: datos totales procesados por el servicio
- **Restablecimiento del servidor TCP**: reinicios totales de TCP iniciados desde el servidor

### Métricas SSL

Pase el puntero del mouse sobre un servicio que utilice el protocolo SSL para ver las métricas de SSL.




- **Errores del servidor SSL**: indica el total de errores de SSL del servidor. (Por ejemplo, certificado SSL desconocido)
- **Protocolo SSL**: indica la versión del protocolo SSL utilizada por el servicio
- **Errores del cliente SSL**: indica el total de errores de SSL del cliente. (Por ejemplo, error de autenticación de cliente SSL)

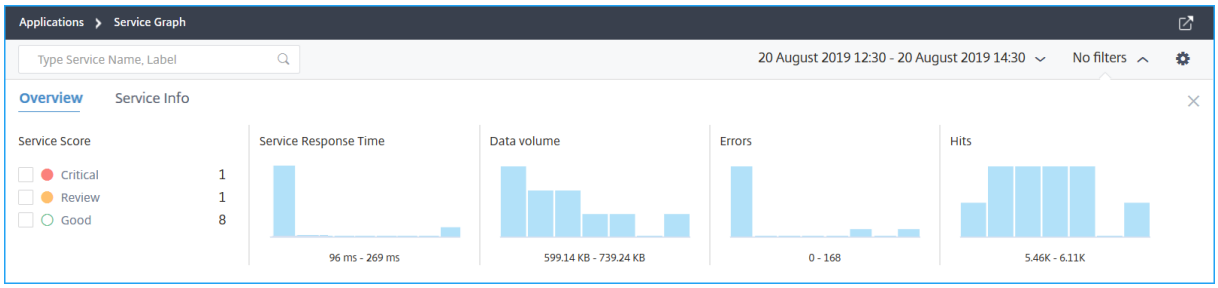
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Ver detalles del servicio

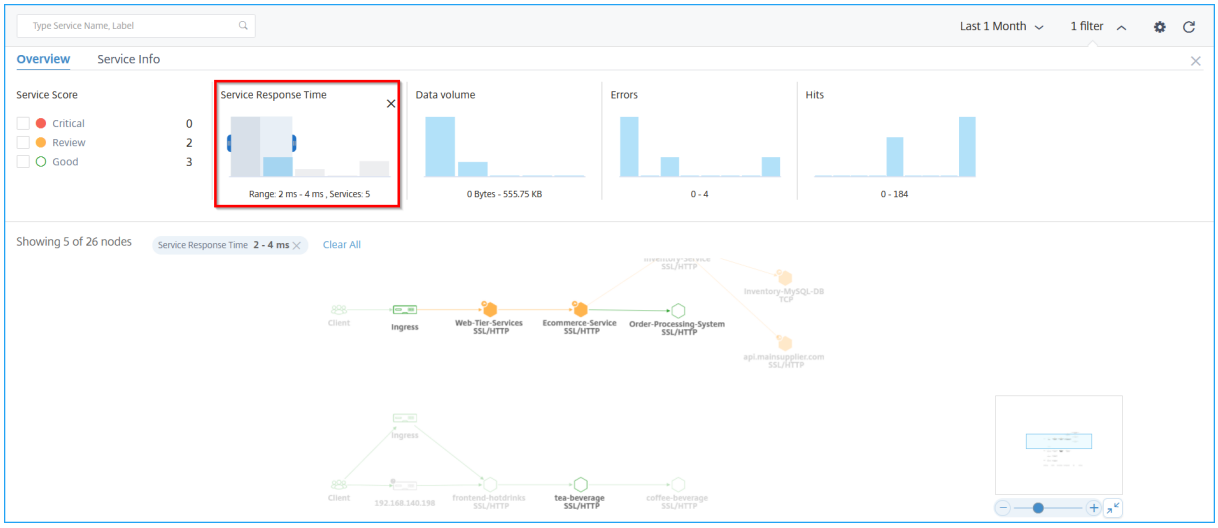
Haga clic en un servicio y seleccione **Ver detalles** para ver los detalles del servicio. Para obtener más información, consulte Ver detalles del servicio.

## Aplicar filtros

Puede aplicar filtros para ver información de servicio específica. Haga clic en la lista **Sin filtros** para ver las opciones de filtro.



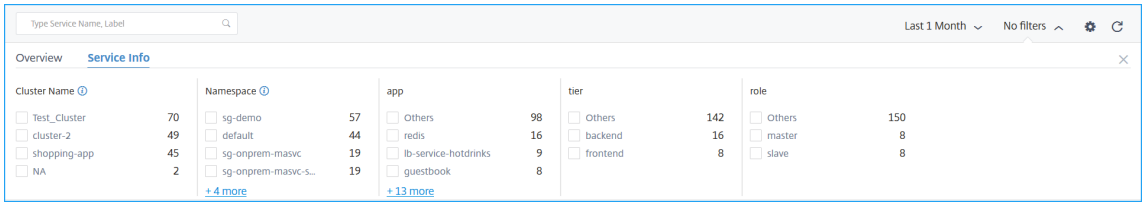

Por ejemplo, si quiere ver los servicios que tienen una latencia inferior a 150 ms, haga clic en el gráfico de barras situado debajo del **tiempo de respuesta del servicio** para mostrar los resultados.




Haga clic en **Información de servicio** para seleccionar y aplicar filtros para:

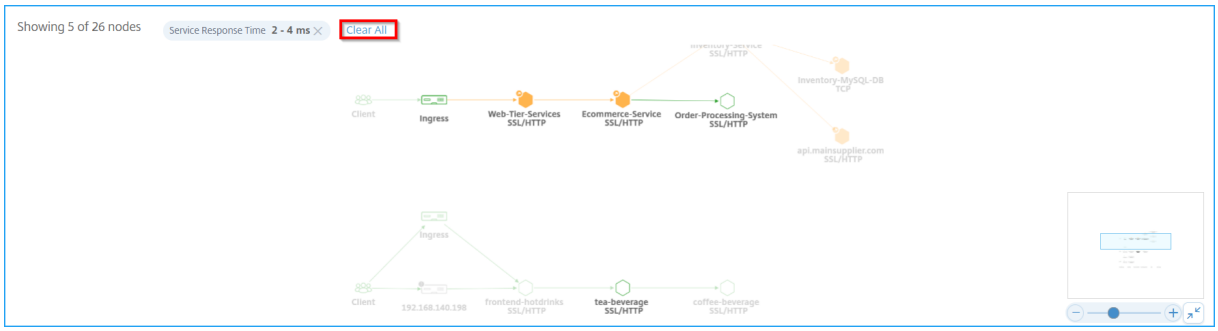
- **Cluster**: Muestra todos los servicios aplicables al clúster o clústeres seleccionados.
- **Espacio de nombres**: Muestra todos los servicios aplicables al espacio de nombres seleccionado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

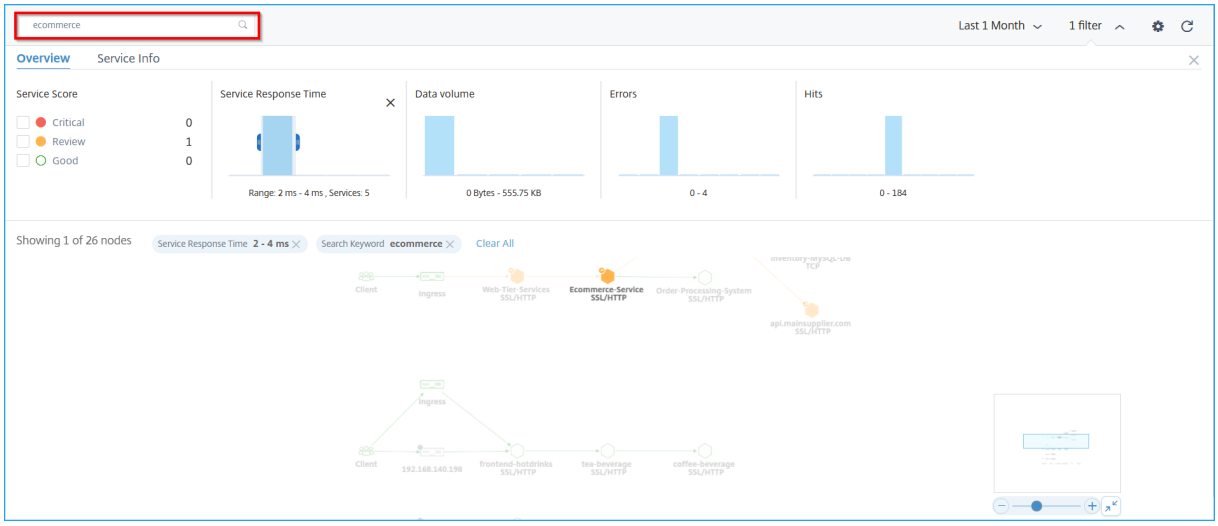



> Nota
>
> Dependiendo de las etiquetas configuradas para el servicio en la definición de servicio de Kubernetes YAML, también puede ver más opciones de filtro.

Haga clic en **Borrar todo** para borrar todos los filtros.

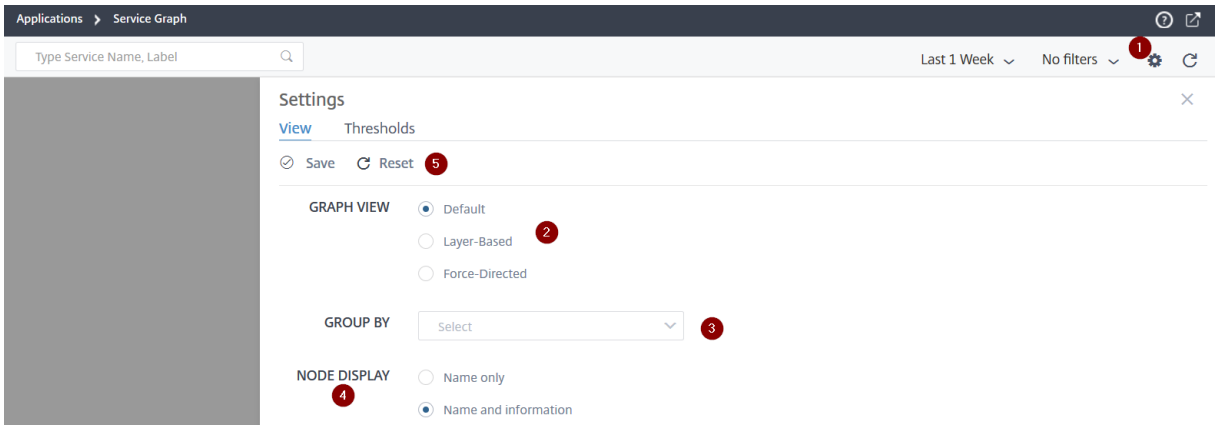



Como alternativa, también puede utilizar el cuadro de texto de búsqueda y escribir un nombre de servicio para mostrar los resultados en el gráfico de servicios.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

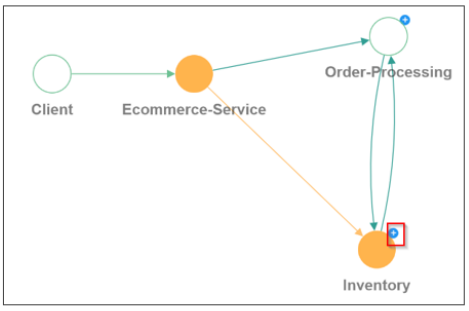
## Uso de la opción de configuración



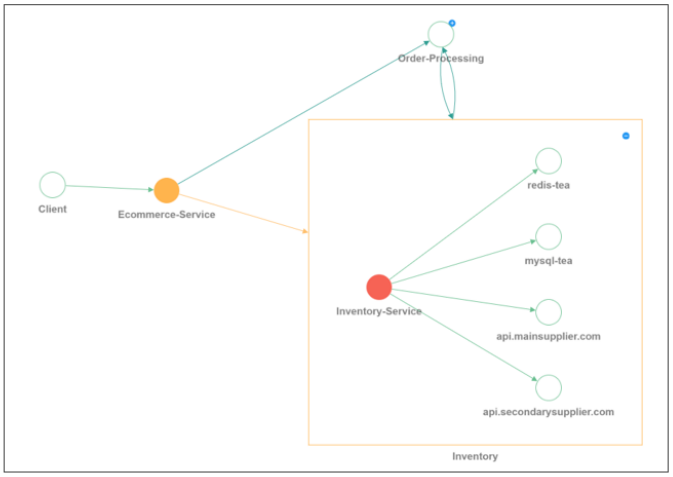

**1** —Icono de configuración

**2** —Opciones para mostrar el gráfico de servicio como vistas predeterminadas, basadas en capas o dirigidas por la fuerza

**3** —Seleccione las opciones de la lista para ver los servicios según las categorías. Después de seleccionar una categoría de la lista, haga clic en **+** en el gráfico para ver todos los servicios




Collapsed view




Expanded view

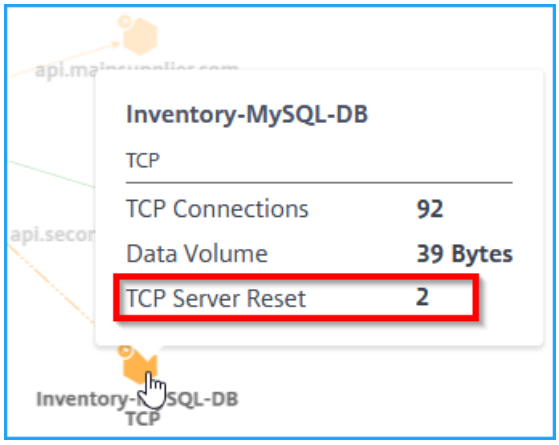
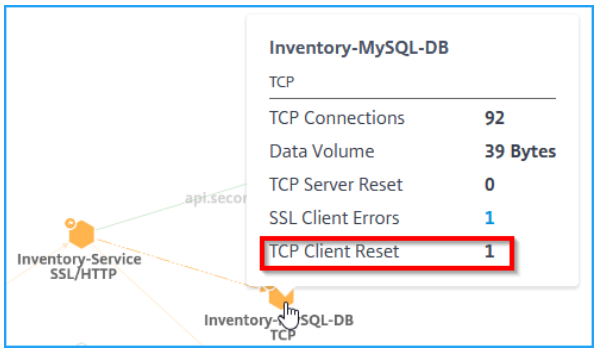
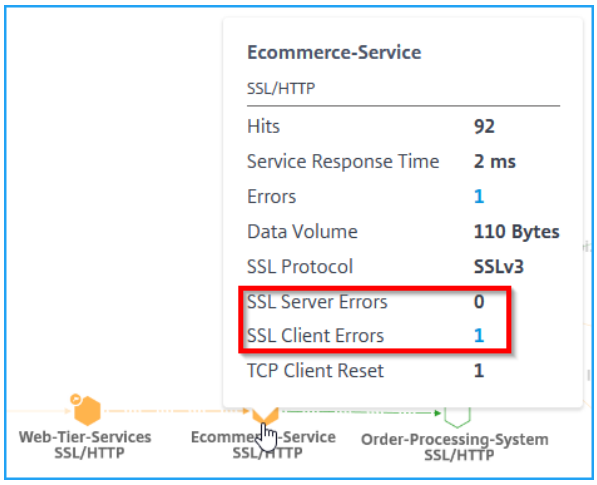
**4**: Permite seleccionar la opción sobre cómo quiere mostrar los servicios.

**5** - Opciones para guardar la configuración o restablecer los valores predeterminados.

## Analiza los errores

Pase el puntero del mouse sobre un servicio que indique errores.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Error | Descripción |
| --- | --- |
|  | El **restablecimiento del servidor TCP** indica el total de restablecimientos de TCP iniciados desde el servidor. |
|  | El **restablecimiento del cliente TCP** indica el total de restablecimientos de TCP iniciados por el cliente. |
|  | Los errores del cliente SSL indican el total de errores de SSL del cliente. (Por ejemplo, error de autenticación del cliente SSL). |

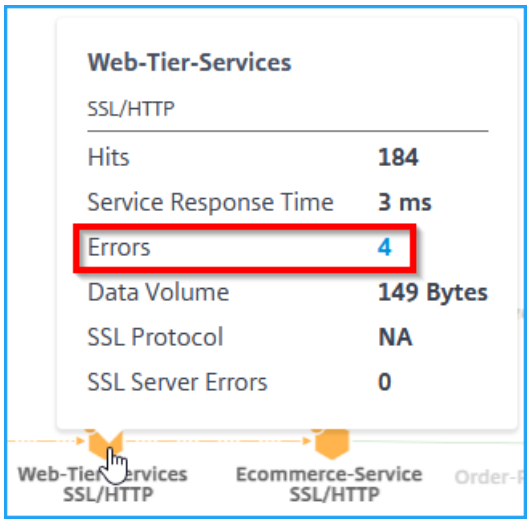
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Error | Descripción |
| --- | --- |
| | Los errores del servidor SSL indican el total de errores de SSL del servidor. (Por ejemplo, certificado SSL desconocido) |

> **Nota**
>
> - El recuento de errores del cliente (independientemente del tipo de protocolo) se muestra en cualquier servicio si el recuento de errores del cliente es igual **o superior a 1**.
> - El recuento de errores de clientes que se muestra para cualquier servicio indica que los errores provienen del cliente.

## Ver detalles de transacciones HTTP

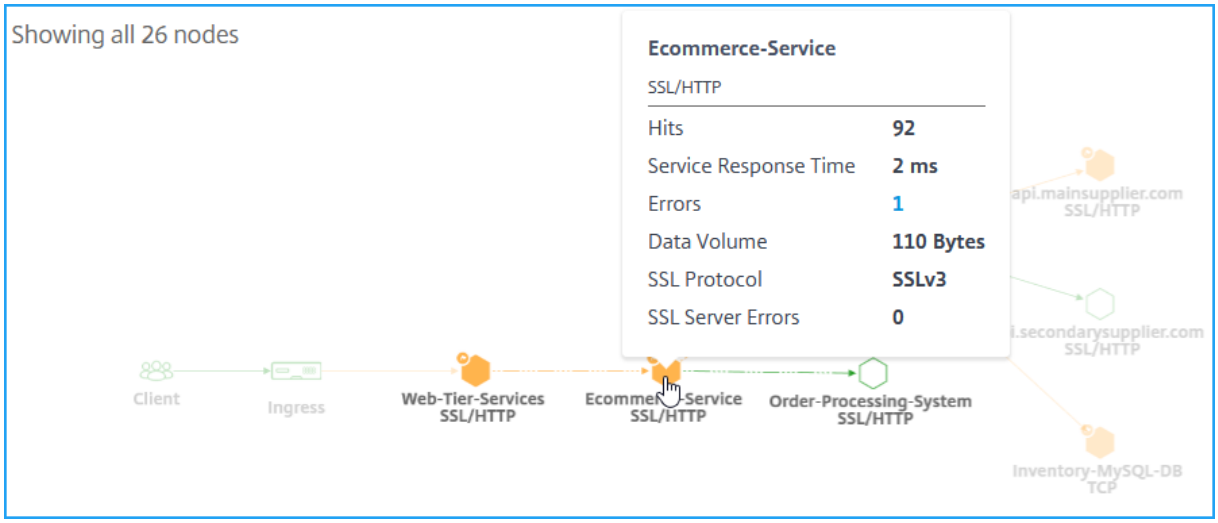
> **Nota**
>
> Puede ver los errores si pasa el puntero del mouse (mouse) sobre un servicio erróneo y haga clic en el recuento de problemas.



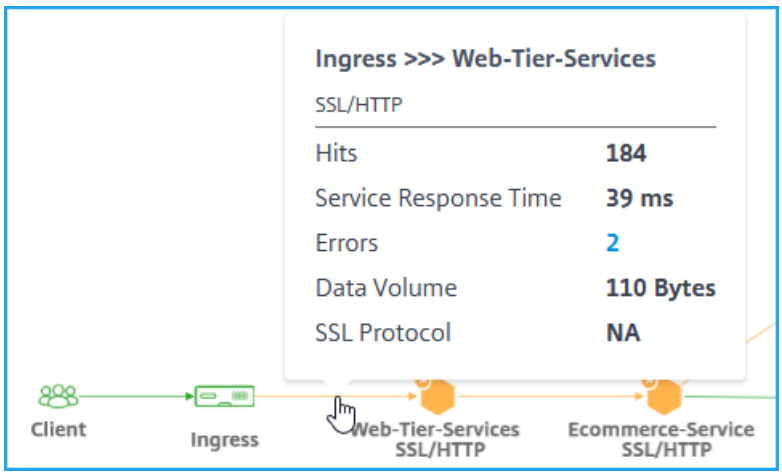

Según el ejemplo que se muestra en la imagen, puede ver un mapa de red de extremo a extremo de la aplicación que muestra cómo se comunican los servicios de componentes.

Al pasar el puntero del mouse sobre el **servicio de comercio electrónico**, puede ver los detalles de las métricas del **servicio de comercio electrónico**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




NetScaler ADM también le permite ver los detalles de las transacciones entre Ingress y los servicios. Pase el puntero del mouse para ver detalles como el total de errores, el tiempo medio de respuesta del servicio, etc., entre la entrada y el servicio.




**Visitas**: indica el número total de visitas recibidas por el servicio.

**Tiempo de respuesta del servicio**: indica el tiempo medio de respuesta que tarda el servicio en responder a Time To First Byte (TTFB).

**Errores**: indica el total de errores, como 4xx, 5xx, etc.

**Volumen de datos**: indica el volumen total de datos procesados por el servicio.

**Protocolo SSL**: indica la versión del protocolo SSL.

Haga clic en la flecha entre **Ingress** y **Service** para ver las transacciones detalladas.

Para obtener más información, consulte Ver análisis para transacciones web.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configurar umbrales en el gráfico de servicio

January 30, 2024

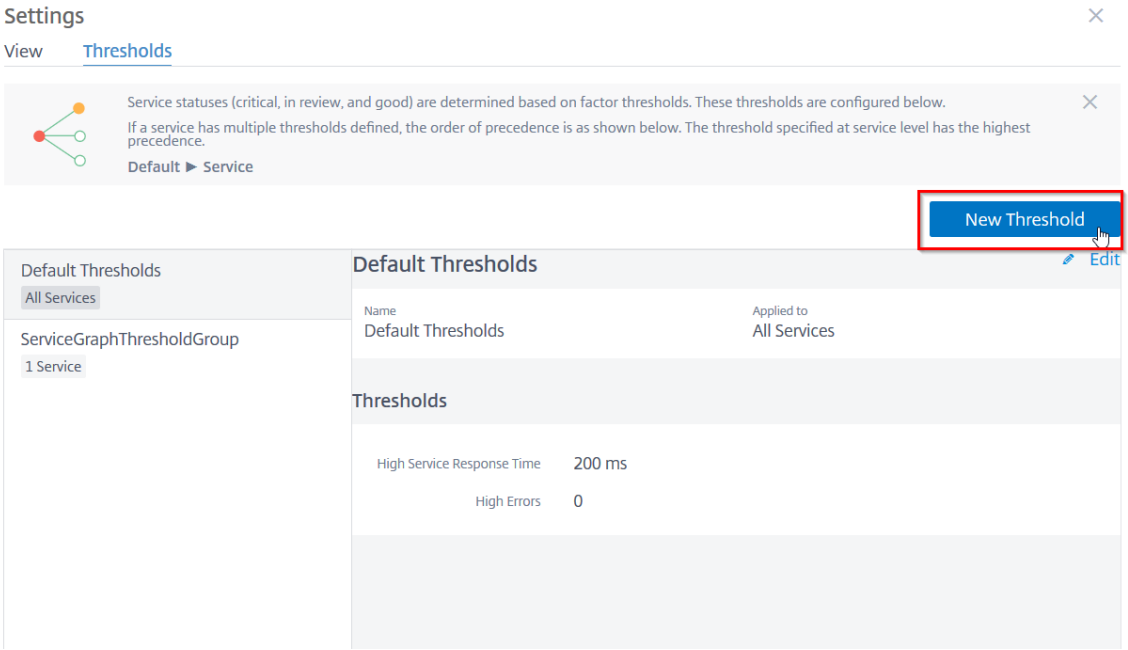
Como administrador, puede configurar umbrales para los servicios de Kubernetes. NetScaler ADM muestra el estado del servicio (Crítico, Revisión y Buena) en función del tiempo de respuesta del servicio y el recuento de errores. De forma predeterminada, puede ver el **umbral predeterminado** (tiempo de respuesta del servicio = 200 ms y recuento de errores = 0) aplicado a todos los servicios.

> **Nota**
>
> No puede eliminar el umbral predeterminado.

Para configurar un nuevo umbral:

En el gráfico de servicio:

1. Haga clic en el icono de configuración y seleccione la ficha **Umbrales**.
2. Haga clic en **Nuevo umbral** para configurar un nuevo umbral.




   Aparece la página **New Threshold**.

3. Configure los siguientes parámetros:

   a) **Nombre**: Especifique un nombre para el umbral.

   b) En **Microservicios**, seleccione los servicios que quiere aplicar el umbral

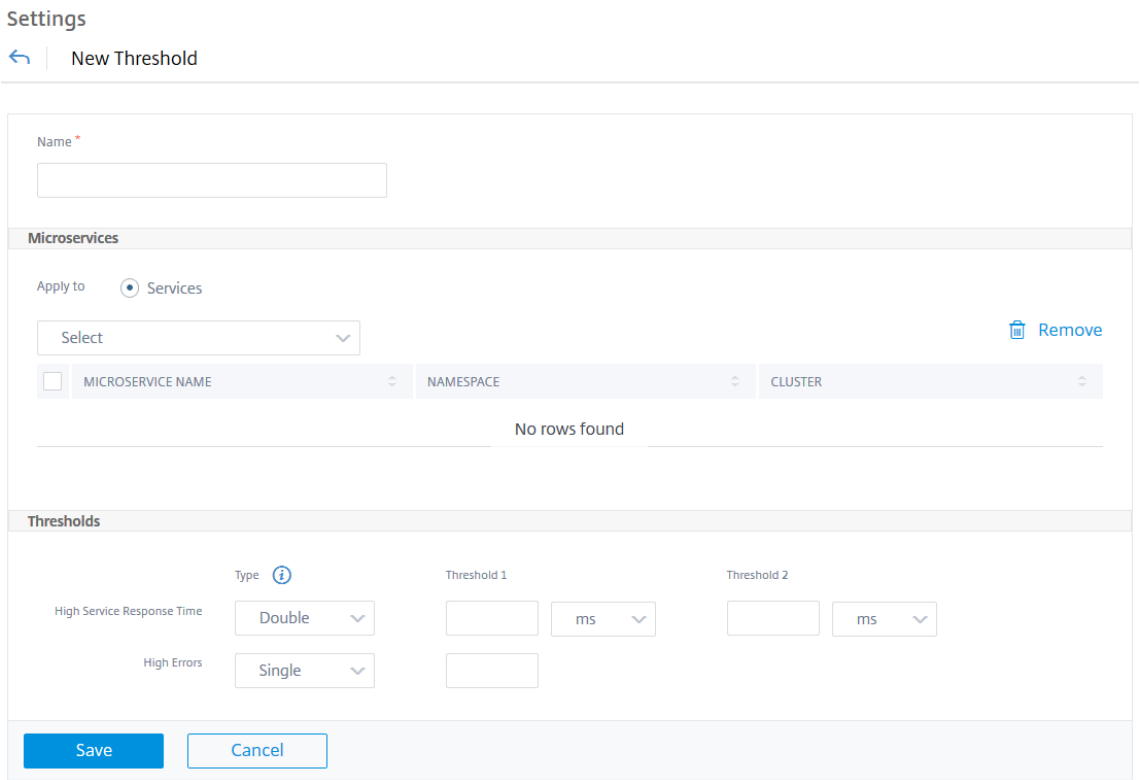
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

c) En **Umbrales**, seleccione Simple o **Doble** para obtener **un** tiempo de respuesta elevado y un alto número de errores

d) Especifique los valores de umbral.

> **Nota**
>
> Si selecciona un umbral doble, asegúrese de que:
>
> - El valor del umbral 1 es menor que el valor del umbral 2. Por ejemplo, si configura Umbral 1 como 250 ms, Umbral 2 debe ser 251 ms o superior.
> - El valor del umbral 1 no debe ser el mismo que el valor Umbral 2.

4. Haga clic en **Guardar**.




El umbral se creó correctamente. Puede ver los detalles del umbral en la página **Umbrales**.

## Umbral único

Al configurar un umbral único, NetScaler ADM:

- Compara los valores actuales con los valores de umbral configurados
- Calcula la penalización total en función de los umbrales superados
- Muestra la puntuación del servicio y el estado del servicio en función del cálculo de penalización

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Umbral doble

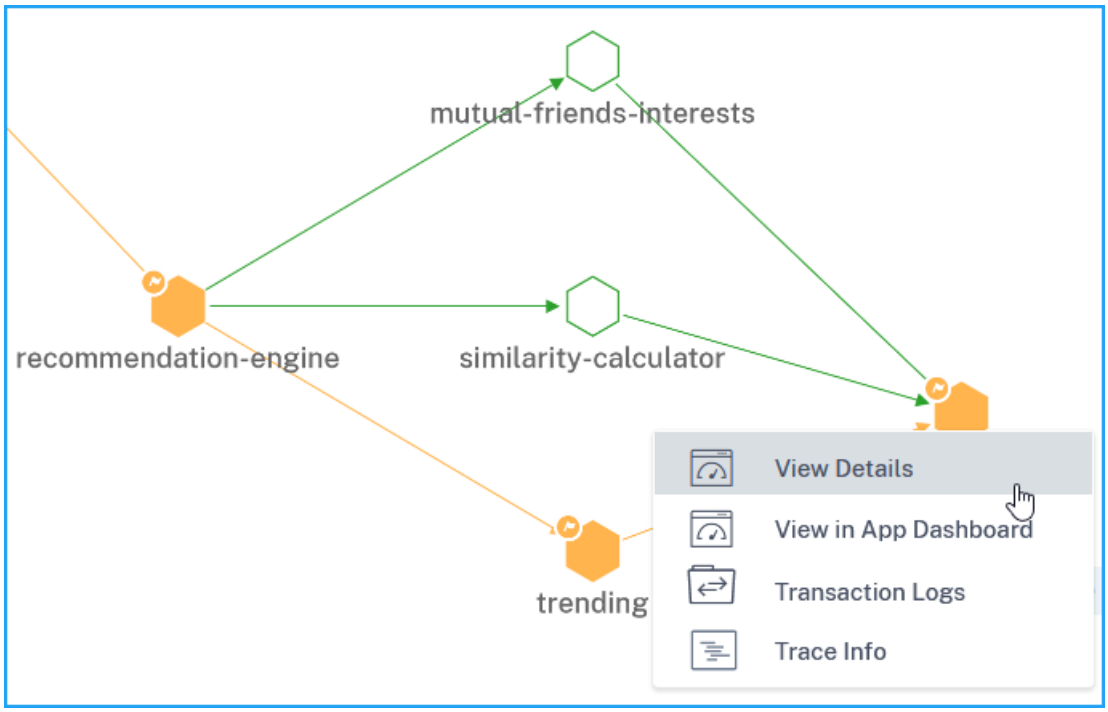
Cuando se configura el umbral doble, NetScaler ADM:

- Compara los valores actuales con los valores de umbral configurados
- Comprueba si los valores actuales son:
  - Menor que el umbral 1
  - Entre el umbral 1 y el umbral 2
  - Mayor que el umbral 2
- Calcula la penalización total en función de los umbrales superados
- Muestra la puntuación del servicio y el estado del servicio en función del cálculo de penalización

## Ver detalles del servicio

January 30, 2024

Haga clic en un servicio y seleccione **Ver detalles**.

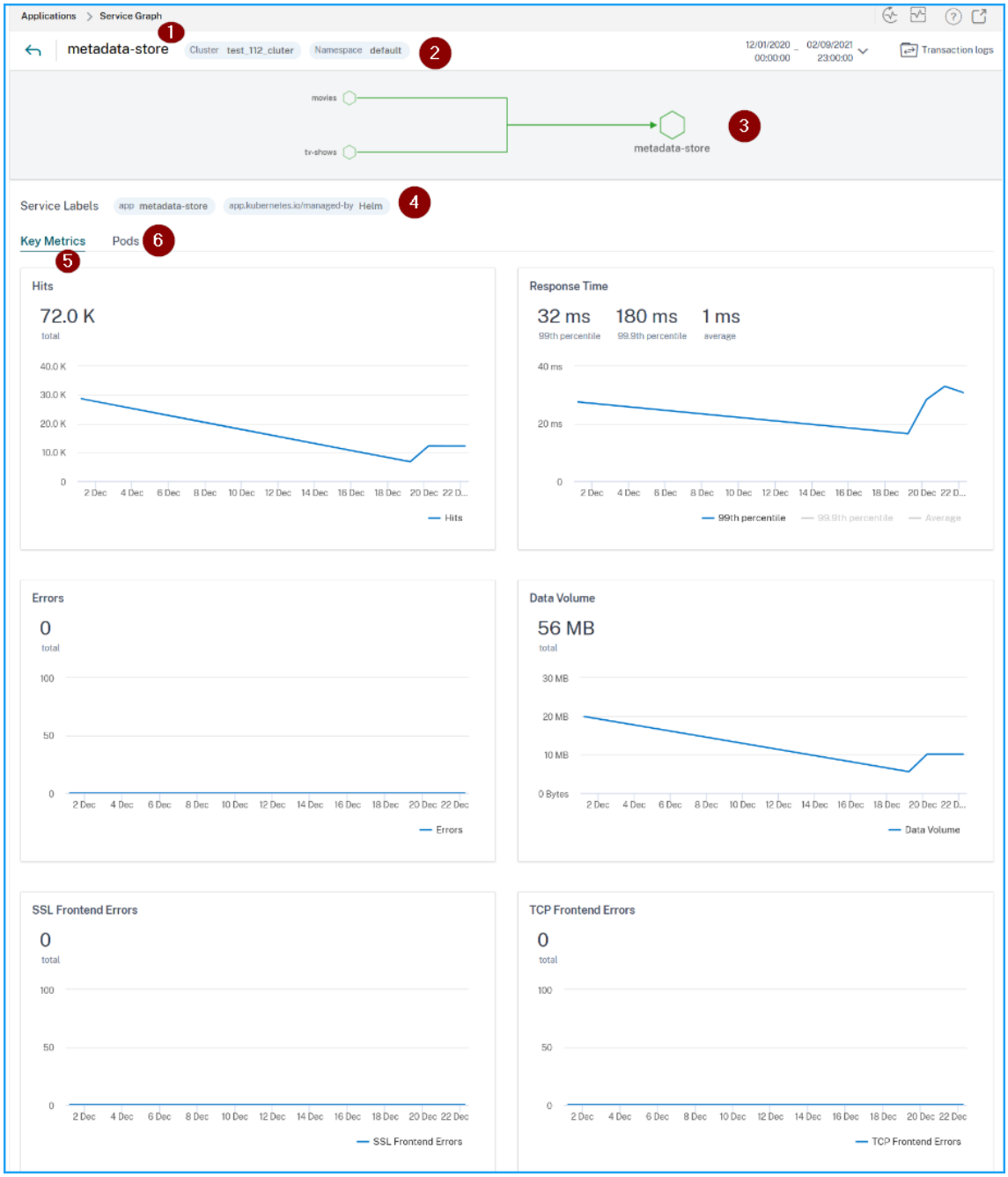



La página de detalles del servicio le permite ver:

- El nombre del clúster donde está alojado el servicio (1)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El espacio de nombres y las etiquetas de servicio del servicio (2) (4)
- Todos los servicios entrantes y salientes asociados conectados con el servicio seleccionado (3)
- Métricas clave de servicio en un formato gráfico como Hits, Tiempo de respuesta, Errores, Volumen de datos, errores de frontend SSL y errores de interfaz TCP (5).
- Los pods back-end asociados al servicio (6).




Con estas tendencias de métricas clave, puede analizar el rendimiento del servicio durante una duración de tiempo específica.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La métrica **Tiempo de Respuesta** le permite ver:

- **Percentil 99** —Indica que el 99% de las solicitudes para la duración seleccionada es inferior a 32 ms (según la imagen de ejemplo).
- **Promedio** : indica el tiempo medio de respuesta del servicio
- **Percentil 99,9** : indica el tiempo de respuesta más alto del servicio.

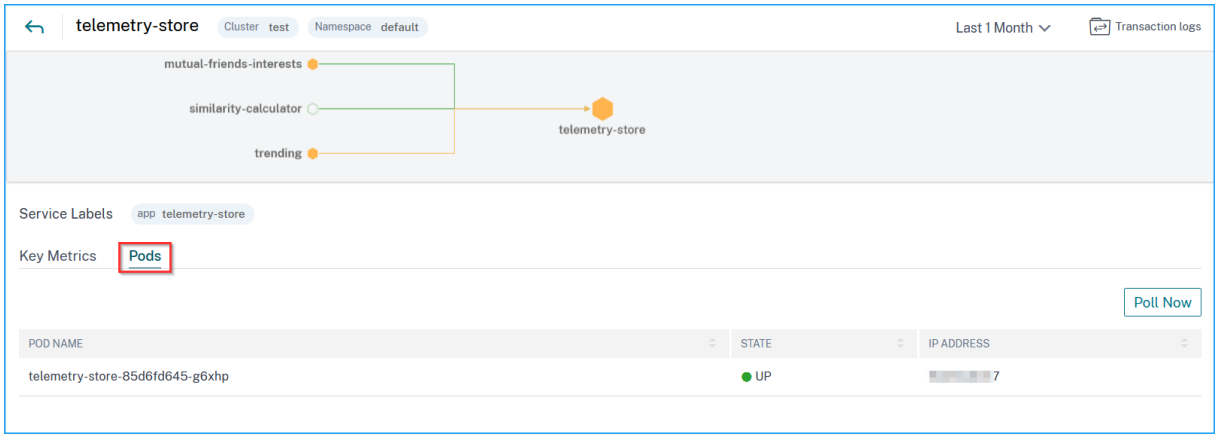
### Detalles de métricas

| Métricas | Descripción |
|---|---|
| Resultados | Número total de solicitudes recibidas por el servicio |
| Errores | El total de errores HTTP del servicio |
| Tiempo de respuesta del servicio | Tiempo medio de respuesta tomado del servicio para responder para el tiempo hasta el primer byte (TTFB). |
| Volumen de datos | El volumen total de datos procesado por el servicio |
| Errores de front-end SSL | El total de errores front-end SSL del servicio. Por ejemplo: SSL CLIENTAUTH FAILURE |
| Errores de back-end SSL | El total de errores de back-end SSL del servicio. Por ejemplo: Errores de cliente SSL |
| Errores de back-end TCP | El total de errores de back-end TCP del servicio. Por ejemplo: restablecimiento del servidor TCP |
| Errores de front-end TCP | El total de errores de front-end TCP del servicio. Por ejemplo: Restablecimiento de cliente TCP |

### Ver detalles del pod de back-end

Haga clic en la ficha **Pods** para ver los pods back-end asociados al servicio.

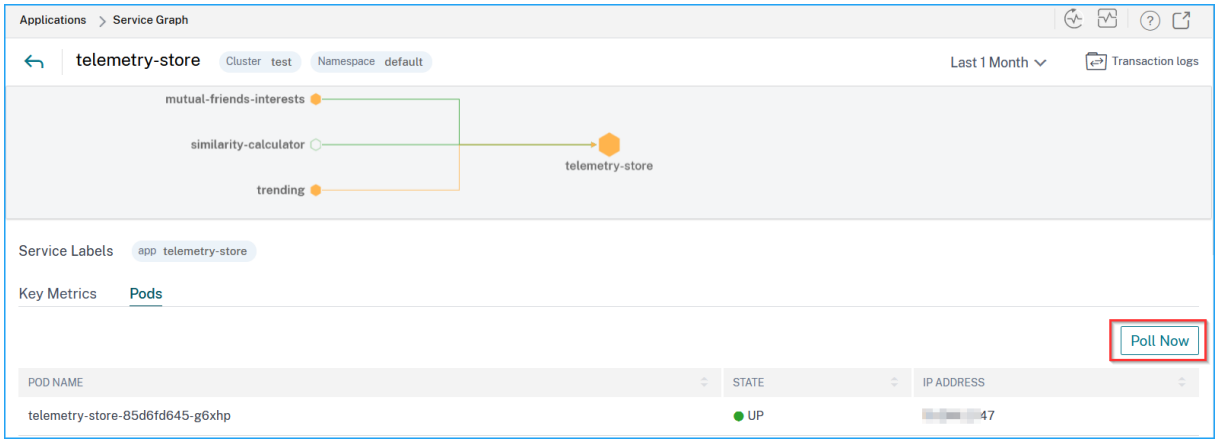
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Nombre del pod** : denota el nombre del pod
- **Estado** : indica si el pod se está ejecutando (UP) o no (DOWN).
- **Dirección IP** : indica la dirección IP del pod

### Utilice la opción Sondear ahora para obtener el estado del pod

La opción **Sondear ahora** obtiene el estado más reciente del pod del clúster.

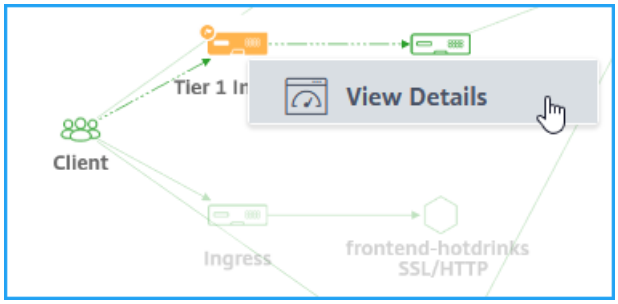



## Ver detalles de ingreso para solucionar problemas

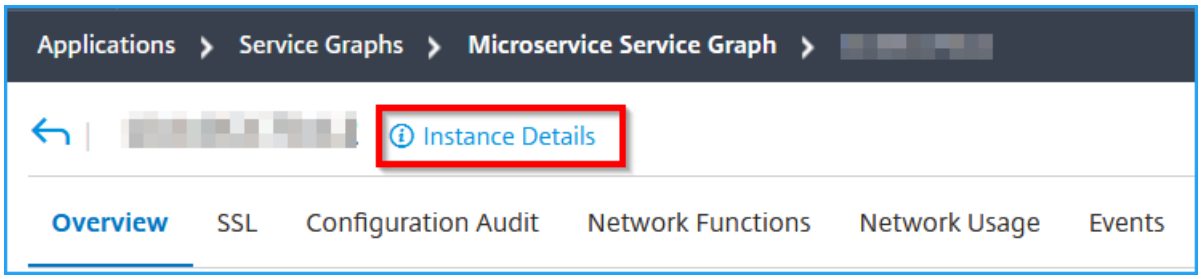
January 30, 2024

En el gráfico de servicio, haga clic en el ingreso y seleccione **Ver detalles** para visualizar los detalles de la instancia de NetScaler ADC configurada para el clúster de Kubernetes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

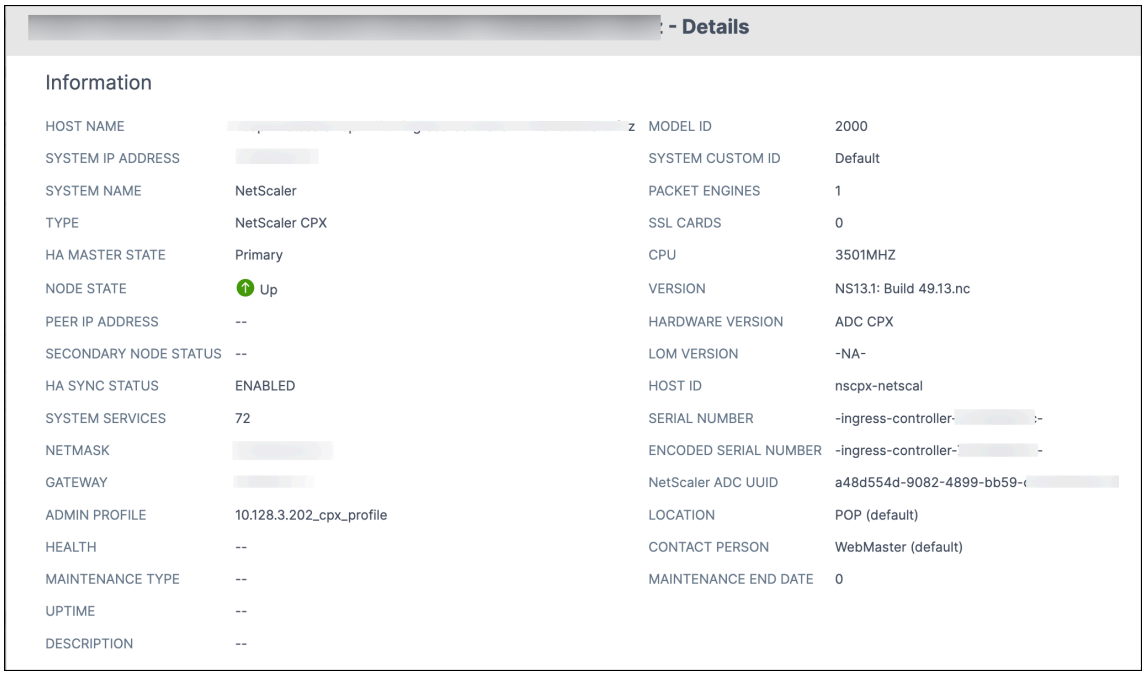



Haga clic en **Detalles de ejemplar** para ver los detalles.



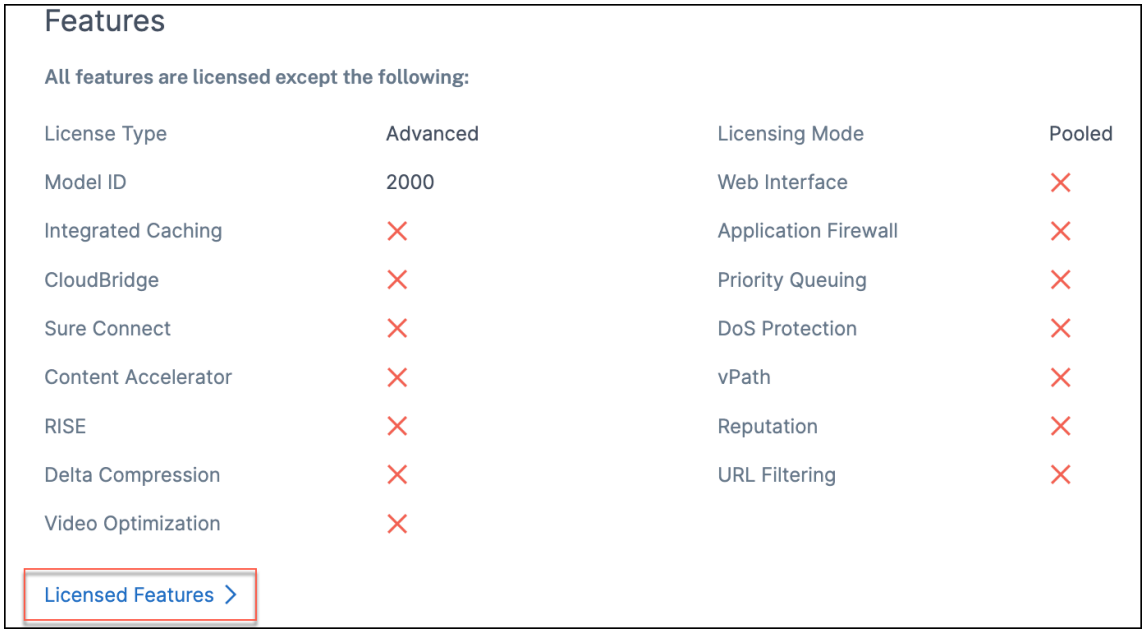

Se muestran los siguientes detalles:

- **Información**: detalles de la instancia, como el tipo de instancia, el tipo de implementación, la versión, el modelo, etc.

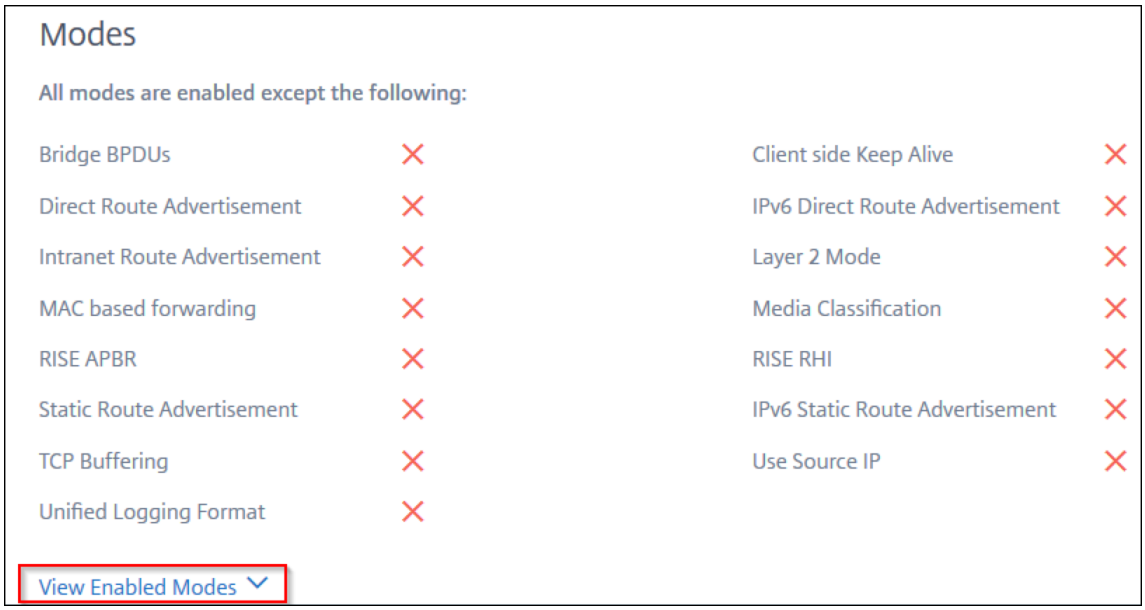



- **Funciones**: de forma predeterminada, se muestran las funciones que no tienen licencia. Haga clic en **Funciones con licencia** para ver las funciones que tienen licencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



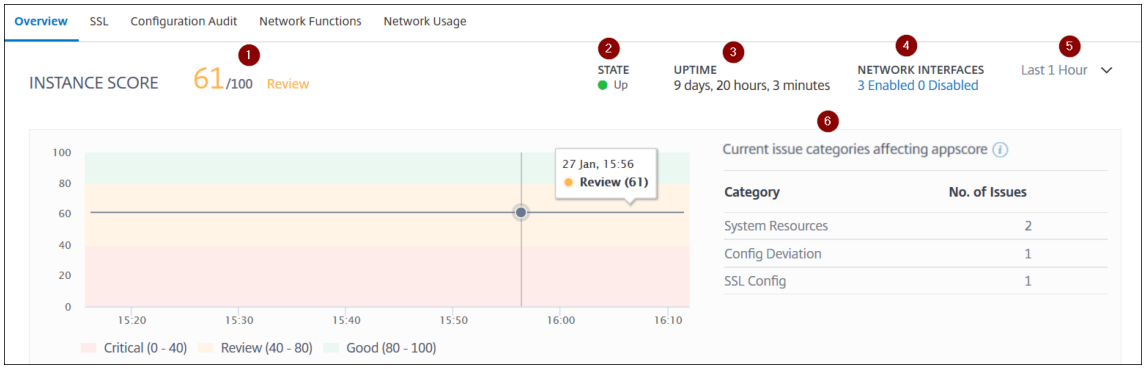

- **Modos**: de forma predeterminada, se muestran todos los modos que están inhabilitados en la instancia. Haga clic en **Ver modos habilitados** para ver los modos habilitados en la instancia.




El panel de instancias presenta una descripción general de la instancia en la que puede ver los siguientes detalles:

- **Puntuación de instancia**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**1**: indica la puntuación actual de la instancia de NetScaler ADC durante el tiempo seleccionado. La puntuación final se calcula en **100 menos el total de penaltis**. El gráfico muestra los rangos de puntuación para la duración de tiempo seleccionada.

**2**: Indica el estado actual de la instancia de NetScaler ADC, como **Activo**, **Inactivo** y **Fuera de servicio**.

**3**: indica el tiempo que la instancia de NetScaler ADC está activa y en ejecución.

**4**: indica el total de interfaces de red habilitadas y inhabilitadas para la instancia. Haga clic para ver los detalles, como el nombre de la interfaz de red y el estado (habilitada o inhabilitada).

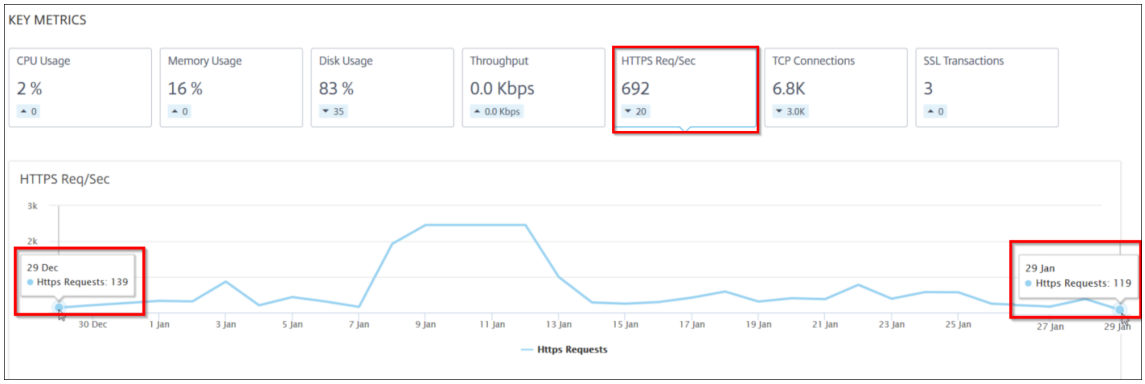
**5** —Seleccione la duración del tiempo de la lista para ver los detalles de la instancia.

**6**: muestra el total de problemas y la categoría de problemas de la instancia de ADC.

- **Métricas clave**

  Haga clic en cada ficha para ver los detalles. En cada métrica, puede ver el valor medio y el valor de diferencia para el tiempo seleccionado.

  La siguiente imagen es un ejemplo de HTTPS Req/seg y la duración seleccionada es para el último mes. El valor **692** es el promedio de HTTPS Req/seg durante el último mes de duración y el valor **20** es el valor de diferencia. En el gráfico, el primer valor es **139** y el último valor es **119**. El valor de la diferencia es **139** —**119 = 20**.




Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Uso de CPU**: el% de CPU promedio de la instancia durante el tiempo seleccionado (se muestra tanto para la CPU de paquetes como para la CPU de administración).
- **Uso de memoria**: el% promedio de uso de memoria de la instancia durante el tiempo seleccionado.
- **Uso del disco**: el% medio de espacio en disco de la instancia durante el tiempo seleccionado.
- **Rendimiento**: el rendimiento de red promedio procesado por la instancia durante el tiempo seleccionado.
- **Solicitud de HTTPS por segundo**: el promedio de solicitudes HTTPs recibidas por la instancia durante el tiempo seleccionado.
- **Conexiones TCP**: el promedio de conexiones TCP establecidas por el cliente y el servidor durante el tiempo seleccionado.
- **Transacciones SSL**: el promedio de transacciones SSL procesadas por la instancia durante el tiempo seleccionado.

• **Problemas**

Puede ver los siguientes problemas que se producen en la instancia de NetScaler ADC:

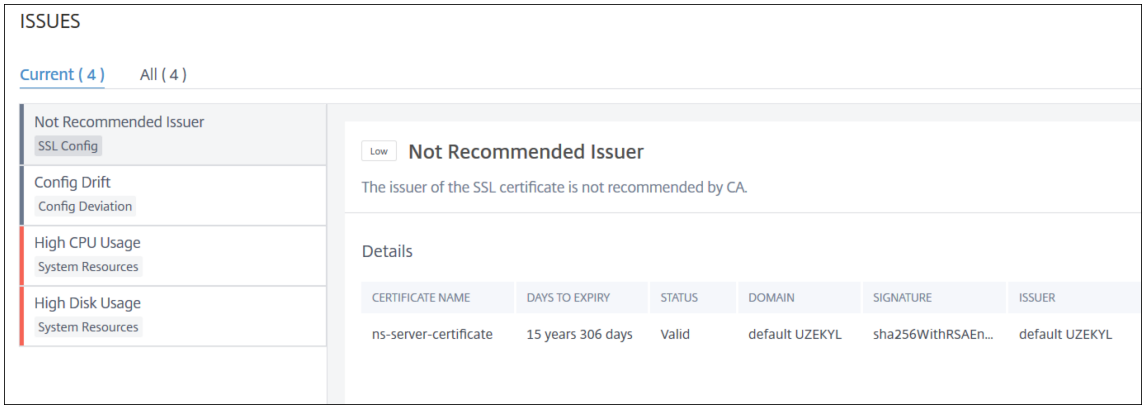
| Categoría de problema | Descripción | Problemas |
|---|---|---|
| Recursos del sistema | Muestra todos los problemas relacionados con el recurso del sistema NetScaler ADC, como CPU, memoria, uso del disco, etc. | – Alto uso de CPU<br>– Alto uso de memoria<br>– Uso elevado del disco<br>– Fallos en la tarjeta SSL<br>– Fallo de alimentación<br>– Error de disco<br>– Error de flash<br>– Descartes de NIC |
| Configuración SSL | Muestra todos los problemas relacionados con la configuración de SSL en la instancia de NetScaler ADC. | – Los certificados SSL han caducado |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Categoría de problema | Descripción | Problemas |
| --- | --- | --- |
| desviación de configuración | Muestra todos los problemas relacionados con los trabajos de configuración aplicados en la instancia de NetScaler ADC. | – Emisor no recomendado<br>– Algoritmo no recomendado<br>– No se recomienda la fuerza de la llave<br>– Deriva de configuración<br>– Ejecución vs plantilla |
| Cuestiones de capacidad | Muestra problemas de capacidad de ADC. El ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra las caídas de paquetes o incrementos de contador de límite de velocidad, si existe. Los problemas se clasifican en los siguientes parámetros de capacidad. | – Se alcanzó el límite de rendimiento |
| Redes | Muestra los problemas operativos que se producen en las instancias. | Para obtener más información, consulte Análisis de infraestructura mejorados con nuevos indicadores. |

Haga clic en cada ficha para analizar y solucionar el problema. Por ejemplo, considere que una instancia tiene los siguientes errores durante el tiempo seleccionado:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- La ficha **Actual** muestra los problemas operativos de ADC actuales que están afectando a la puntuación de la instancia.
- La ficha **Todo** muestra todos los problemas de infraestructura detectados durante la duración seleccionada.

## Seguimiento distribuido

January 30, 2024

En el gráfico de servicios, puede utilizar la vista de rastreo distribuido para:

- Analice el rendimiento general del servicio.
- Visualice el flujo de comunicación entre el servicio seleccionado y sus servicios interdependientes.
- Identificar qué servicio indica errores y solucionar el servicio erróneo
- Ver detalles de transacción entre el servicio seleccionado y cada uno de sus servicios interdependientes.

### Requisitos previos

Para ver la información de seguimiento del servicio, debe:

- Asegúrese de que una aplicación mantenga los siguientes encabezados de seguimiento, mientras envía cualquier tráfico este-oeste:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- `x-request-id`
- `x-b3-traceid`
- `x-b3-spanid`
- `x-b3-parentspanid`
- `x-b3-sampled`
- `x-b3-flags`
- `x-ot-span-context`

- Para **compilaciones CIC anteriores a 1.7.23**, actualice el archivo CPX YAML con `NS_DISTRIBUTED_TRACI` y el valor como `yes`

```
1  apiVersion: apps/v1
2  kind: Deployment
3  metadata:
4    name: cpx-ingress
5  spec:
6    selector:
7      matchLabels:
8        app: cpx-ingress
9    replicas: 1
10   template:
11     metadata:
12       name: cpx-ingress
13       labels:
14         app: cpx-ingress
15       annotations:
16     spec:
17       serviceAccountName: cpx-ingress-k8s-role
18       containers:
19         - name: cpx-ingress
20           image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
21           securityContext:
22              privileged: true
23           env:
24           - name: "EULA"
25             value: "yes"
26           - name: "KUBERNETES_TASK_ID"
27             value: ""
28           - name: "NS_MGMT_SERVER"
29             value: "192.168.0.1"
30           - name: "NS_MGMT_FINGER_PRINT"
31             value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6O:97:3D:E2:5D"
32           - name: "NS_HTTP_PORT"
33             value: "9080"
34           - name: "NS_HTTPS_PORT"
35             value: 9443"
36           - name: "LOGSTREAM_COLLECTOR_IP"
37             value: "192.168.0.1"
38           imagePullPolicy: Always
```

- Para **compilaciones CIC posteriores a 1.7.23**, debe usar un ConfigMap.

  ConfigMaps le permite separar las configuraciones de los pods y hacer que sus cargas de trabajo sean portátiles. Con ConfigMaps, puede cambiar y administrar fácilmente sus configuraciones de carga de trabajo y reducir la necesidad de codificar los datos de configuración para las especificaciones del pod.

  Con la compatibilidad con ConfigMap, puede actualizar la configuración automáticamente mientras mantiene el pod del NetScaler Ingress Controller en ejecución. No es necesario reiniciar el pod después de la actualización. Para obtener más información, consulte Compati-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

bilidad de ConfigMap para el controlador de entrada.

Mediante ConfigMap, puede habilitar o inhabilitar el seguimiento distribuido, eventos, registros de auditoría, etc. Para utilizar ConfigMap:

1. Cree un archivo YAML mediante los parámetros requeridos.

   El siguiente archivo YAML de ejemplo tiene habilitado el seguimiento distribuido y otras variables como registros de auditoría, eventos y transacciones inhabilitadas:

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
```

   > Nota
   >
   > Puede proporcionar los valores para `Samplingrate` entre 0 y 100. NetScaler ADM muestra el número de transacciones de seguimiento mencionado.

2. Implemente ConfigMap mediante:

   ```
   kubectl create -f <configmap-yaml>.yaml
   ```

3. Modifique el archivo CPX YAML y utilice uno `envFrom` o `args` para especificar los siguientes argumentos:

```yaml
envFrom:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
2   - configMapRef:
3       name: cic-configmap
```

O BIEN:

```
  args:
    - --configmap
      default/cic-configmap
```

4. Si quiere cambiar el valor de cualquier variable, modifique los valores en ConfigMap. En este ejemplo, todas las demás variables se cambian de **`false`** a **`true`**.

```
1  apiVersion: v1
2  kind: ConfigMap
3  metadata:
4    name: cic-configmap
5    namespace: default
6  data:
7    LOGLEVEL: 'debug'
8    NS_PROTOCOL: 'http'
9    NS_PORT: '80'
10   NS_HTTP2_SERVER_SIDE: 'ON'
11   NS_ANALYTICS_CONFIG:
12     distributed_tracing:
13       enable: 'true'
14       samplingrate: 100
15     endpoint:
16       server: <ADM-AgentIP> / <ADM-AppserverIP>
17     timeseries:
18       port: 5563
19       metrics:
20         enable: 'true'
21         mode: 'avro'
22       auditlogs:
23         enable: 'true'
24       events:
25         enable: 'true'
26     transactions:
27       enable: 'true'
28       port: 5557
```

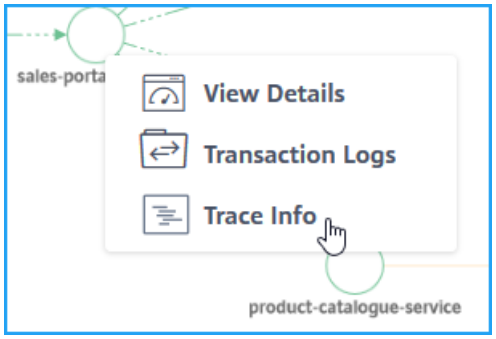
5. Vuelva a aplicar ConfigMap mediante el siguiente comando:

```
kubectl apply -f <yaml-file>.yaml
```

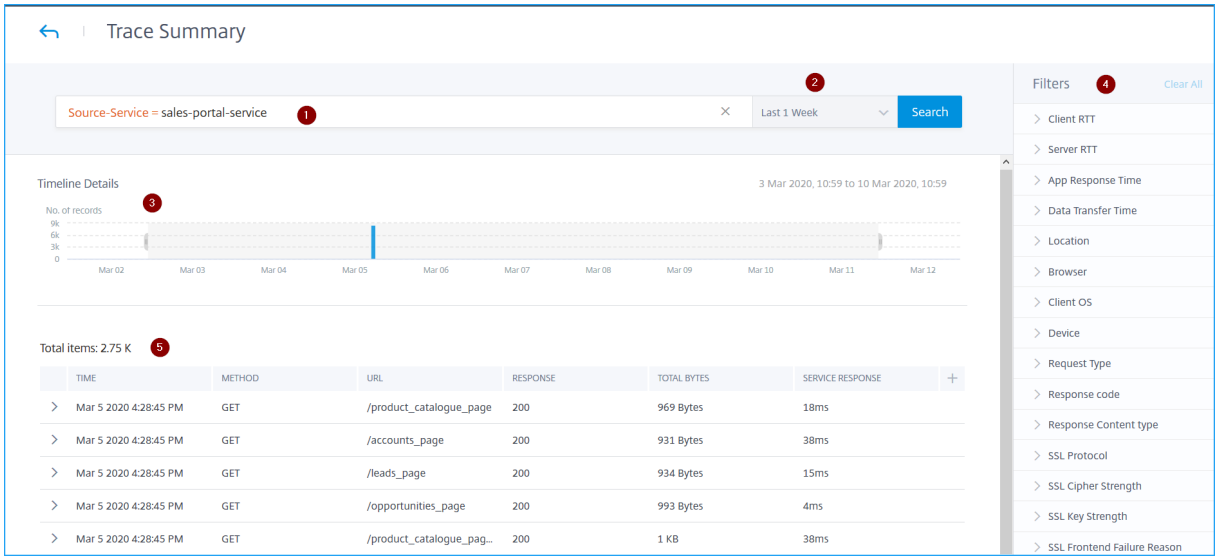
### Ver detalles de seguimiento del servicio

En el gráfico de servicios, haga clic en un servicio y seleccione **Trace Info**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Se muestra la página de resumen de rastreo para el servicio seleccionado.




El **resumen del seguimiento** muestra:

- Búsqueda avanzada que permite buscar transacciones con sugerencias y operadores (1). Para obtener más información, consulte Búsqueda avanzada.
- La lista de duración de tiempo que permite seleccionar la duración de tiempo como 1 hora, 12 horas, 1 día, 1 semana, 1 mes y hora personalizada (2).
- El gráfico de detalles de la línea de tiempo que le permite arrastrar y seleccionar para mostrar los resultados de un período de tiempo específico (3).
- El panel Filtros que le permite seleccionar opciones de cada métrica (4).
- Los detalles de la transacción del servicio seleccionado (5).

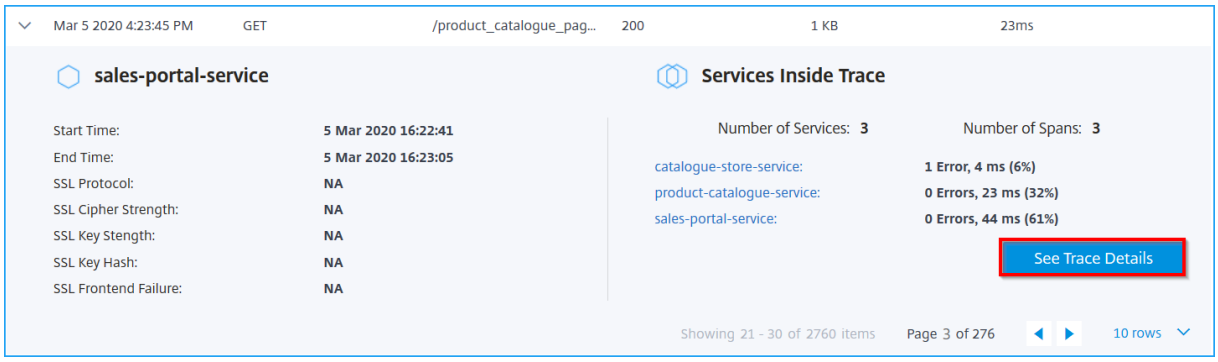
## Ver los detalles de la transacción

Haga clic en una transacción para obtener información detallada. Puede ver los detalles de la transacción del servicio seleccionado, por ejemplo:

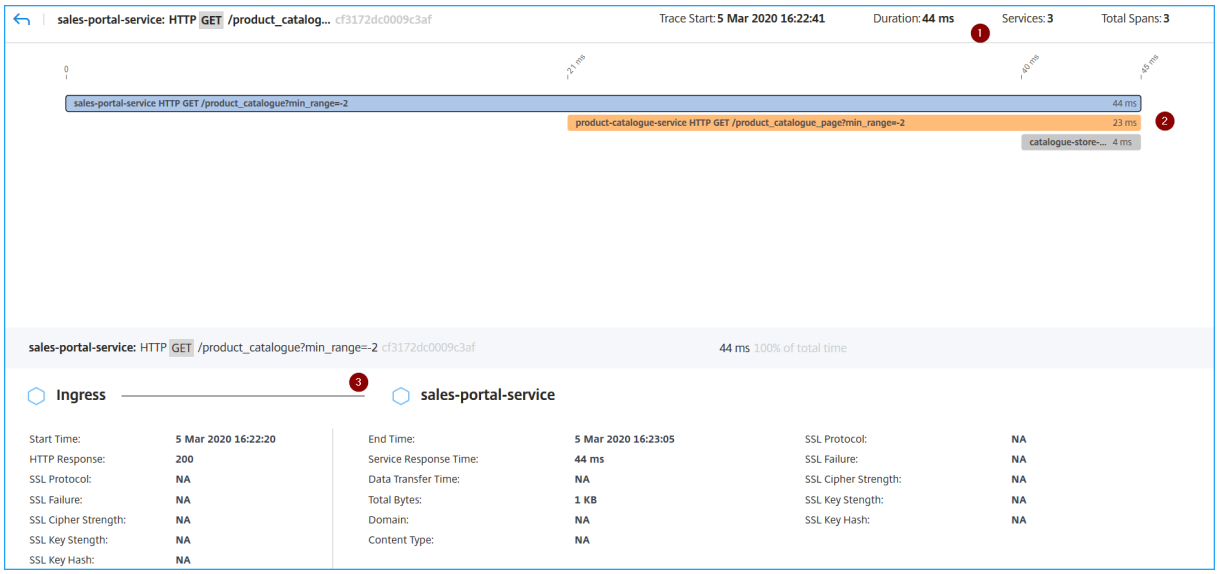
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Hora de inicio
- Hora de finalización
- Métricas SSL
- Comunicación con los servicios interdependientes (junto con los errores y el tiempo de respuesta de cada servicio).

El siguiente ejemplo indica un error de `catalogue-store-service`. Haga clic en **Ver detalles del rastreo** para obtener más información.




Aparece la página Detalles del rastreo.



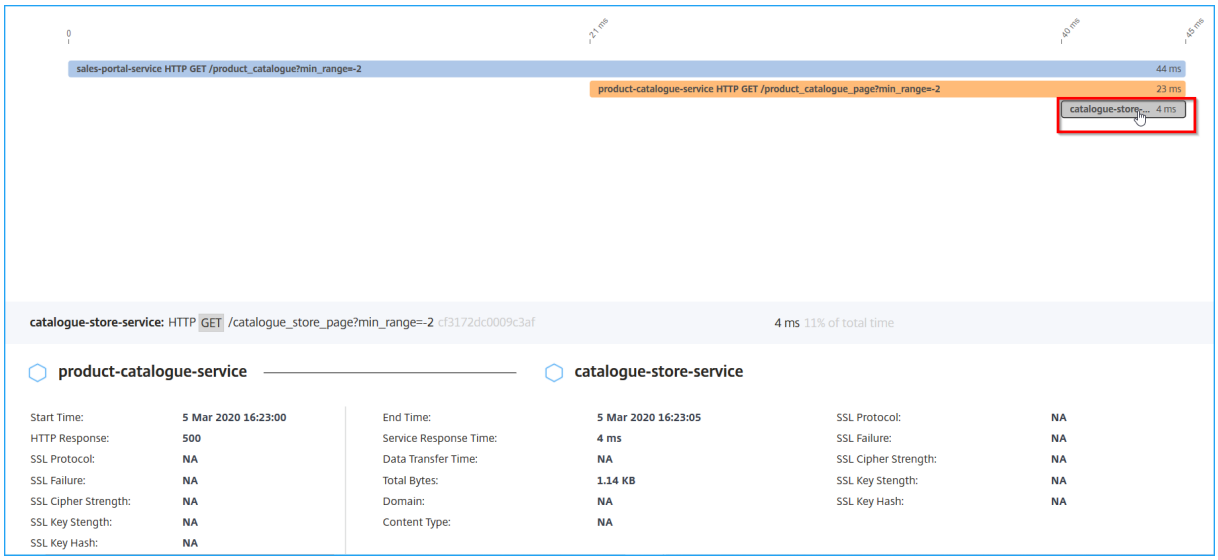

**1**: muestra la hora de inicio, el tiempo de respuesta, los servicios totales y los intervalos totales de la transacción.

**2**: muestra los detalles del servicio seleccionado que se ha comunicado con sus servicios de interdependencia. Puede hacer clic en cada transacción para ver los detalles.

**3** —Muestra los detalles de la transacción de cada servicio.

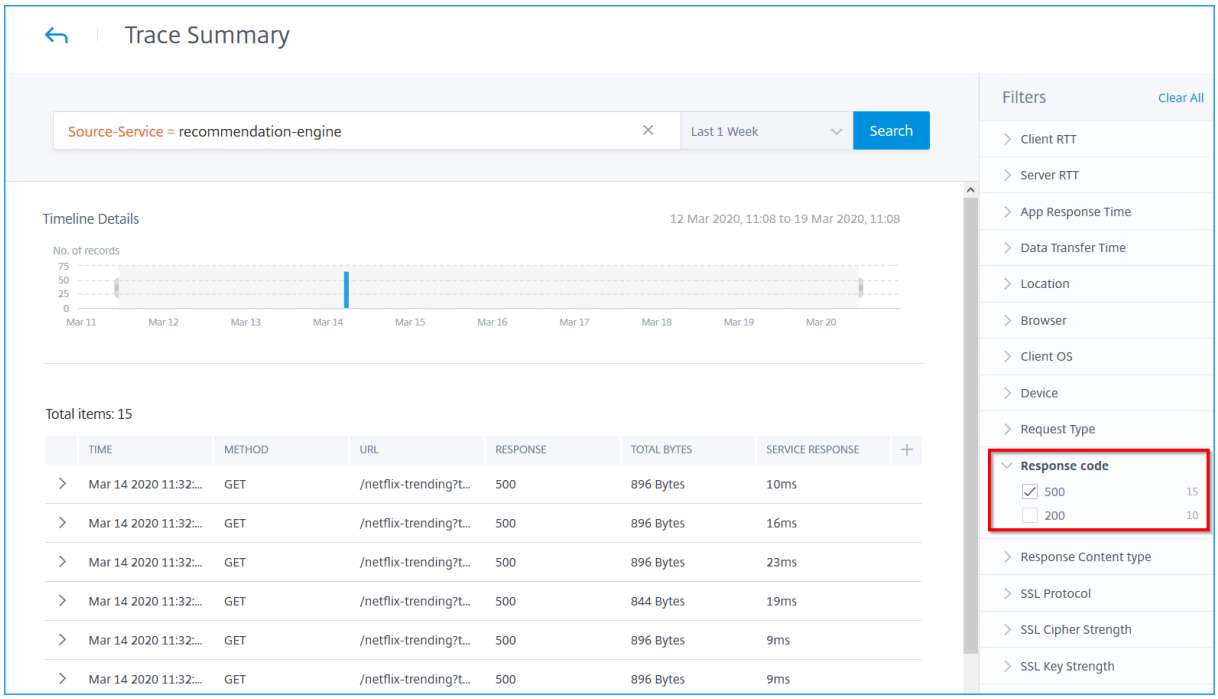
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Según la imagen de ejemplo, `catalogue-store-service` indicó un error. Haga clic en la transacción disponible para `catalogue-store-service`.




Los detalles de la transacción entre la respuesta HTTP `product-catalogue-service` y `catalogue-store-service` indican que es 500. Con estos detalles, como administrador, puede analizar el servicio erróneo y solucionar problemas de `product-catalogue-service` como resolución.

También puede filtrar los resultados seleccionando las opciones de cada métrica en el panel **Filtros**. Por ejemplo, si quiere ver todas las transacciones 5xx, haga clic en **Código de respuesta** y seleccione **500**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **RTT del cliente**: la duración del viaje de un paquete desde el cliente.
- **Servidor RTT**: el tiempo que tarda un paquete en viajar desde el servidor.
- Tiempo de**respuesta de la aplicación: tiempo**de respuesta promedio de la aplicación
- **Tiempo de transferencia**de datos: el tamaño de la transferencia de datos y la velocidad a la que la transmisión puede realizarse desde/hacia un servicio.
- **Ubicación**: La ubicación del cliente
- **Navegador**: los tipos de navegador que utilizan los clientes. Por ejemplo: Chrome, Firefox.
- **SO del cliente**: El SO del cliente se basa en los detalles del agente de usuario del explorador web.
- **Dispositivo**: Los dispositivos basados en los detalles del agente de usuario del explorador web. Por ejemplo: tableta, móvil.
- **Tipo de solicitud**: el tipo de solicitud de transacción. Por ejemplo: GET.
- **Código de respuesta**: el código de respuesta recibido del servidor. Por ejemplo: 501, 404, 200.
- **Tipo de contenido de respuesta**: el tipo de contenido de la transacción. Si la solicitud del cliente es para texto/html, la respuesta del servidor debe ser text/html.
- **Protocolo SSL**: la versión del protocolo SSL utilizada por los clientes. Por ejemplo: SSLv3.
- Nivel de**cifrado SSL**: el nivel de cifrado basado en el tamaño de la clave del certificado SSL, como alto, medio y bajo.
- Nivel de seguridad**de la clave SSL**: el nivel de cifrado SSL se calcula a partir del tamaño de la clave del certificado SSL. La longitud de la clave define la seguridad del algoritmo SSL. Por ejemplo: 2048
- **SSL Front End Failure Motivo**: El mensaje de error de protocolo de enlace SSL front-end. Por ejemplo: SSL CLIENTAUTH FAILURE

## Ver detalles de diagnóstico para datos parciales o nulos en el gráfico de servicio

August 23, 2024

Después de completar la configuración del gráfico de servicio requerida y agregar el clúster de Kubernetes en NetScaler ADM, el gráfico de servicio comienza a rellenar los datos. En algunos casos, puede observar que el gráfico de servicio muestra datos parciales o ningún dato. Algunas de las posibles razones para los datos parciales o la ausencia de datos en el gráfico de servicio son:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- La ruta estática no está configurada
- El estado del clúster de Kubernetes está indisponible
- Error en el registro CPX
- Los servidores virtuales CPX no tienen licencia
- La configuración de análisis requerida no está establecida que impide que el gráfico de servicio cargue todos los datos

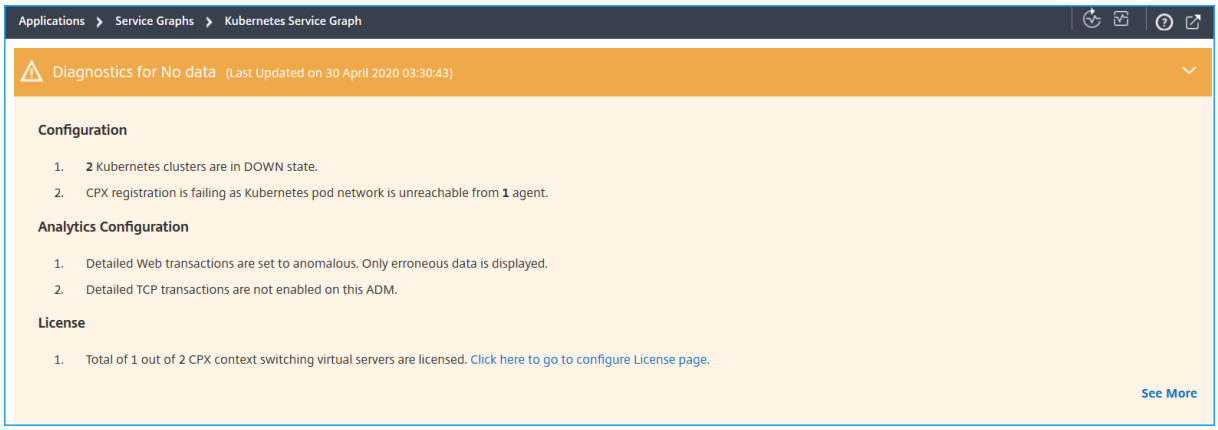
Como administrador, es posible que le resulte difícil analizar los motivos cuando vea el gráfico de servicio que muestra datos parciales o no hay datos. La página de información de diagnóstico en el gráfico de servicio le permite ver las posibles razones y las acciones necesarias para solucionar problemas de datos parciales o ningún problema de datos.

En NetScaler ADM, vaya a **Aplicaciones** > **Gráfico de servicio** y haga clic en la ficha **Microservicios**.

## Diagnósticos para no tener datos

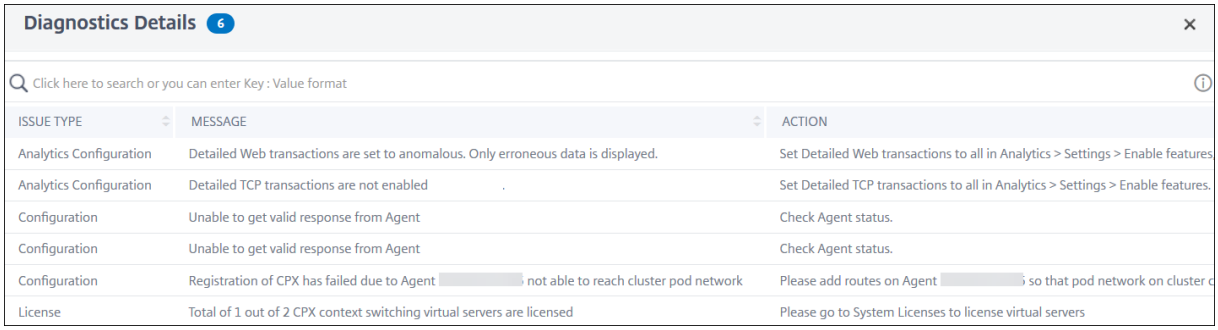
Si el gráfico de servicio no muestra ningún dato, se muestra el siguiente mensaje de diagnóstico.

Haga clic en ** para ver los detalles. Puede ver las posibles razones por las que el gráfico de servicio no muestra ningún dato. La siguiente imagen es un ejemplo de ningún dato en el gráfico de servicio.




Haga clic en **Ver más** para ver los detalles de los problemas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

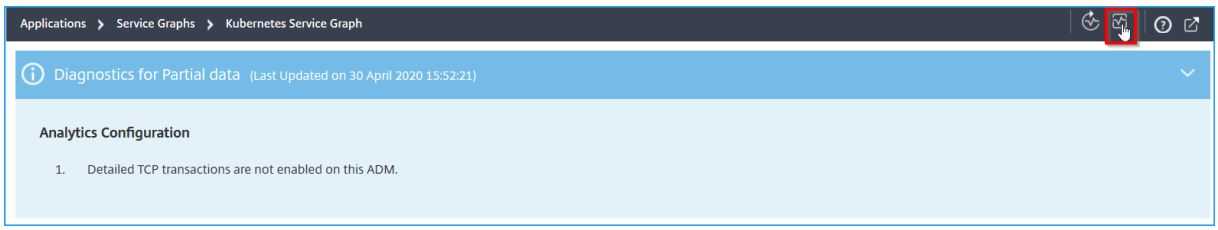



- **Tipo de problema**: indica si los problemas se producen con la configuración, la configuración de análisis o las licencias.
- **Mensaje**: indica la causa del problema.
- **Acción**: indica qué acción se debe realizar para solucionar el problema.

## Diagnósticos para datos parciales

Si el gráfico de servicio solo se muestra con datos parciales, haga clic en el botón **Mostrar diagnósticos** para ver la información de diagnóstico.

El siguiente ejemplo indica que las transacciones TCP están inhabilitadas.



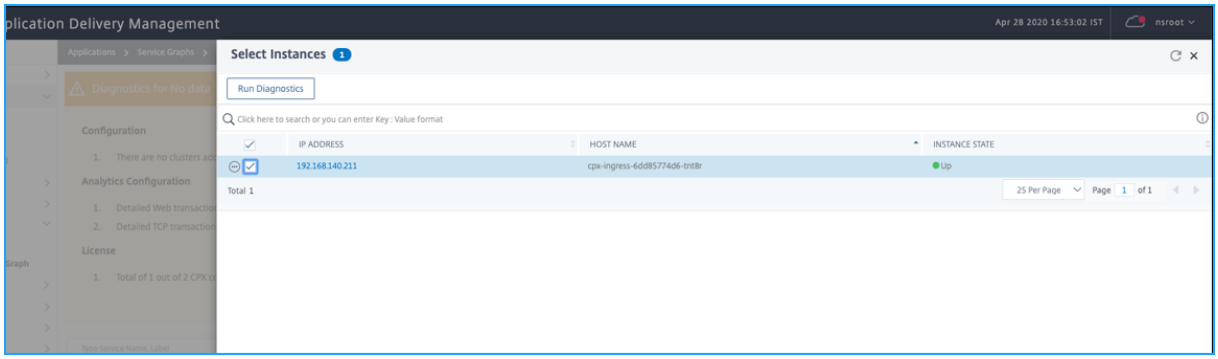

Para este ejemplo, debe habilitar la **configuración de transacción TCP** en **Todos** navegando a **Analytics** > **Configuración**.

## Solución de problemas

Como administrador, con estos mensajes de diagnóstico, puede validar estos problemas e intentar solucionarlos. Después de solucionar el problema, NetScaler ADM ejecuta automáticamente una comprobación de diagnóstico periódica en un intervalo regular. Una vez completada la comprobación de diagnóstico, se resolverá el problema de datos parciales o ningún dato en el gráfico de servicio.

También puede hacer clic en **Ejecutar diagnósticos**, seleccionar las **instancias de CPX**y hacer clic en **Ejecutar diagnósticos**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para obtener más casos de solución de problemas, consulte las preguntas frecuentes.

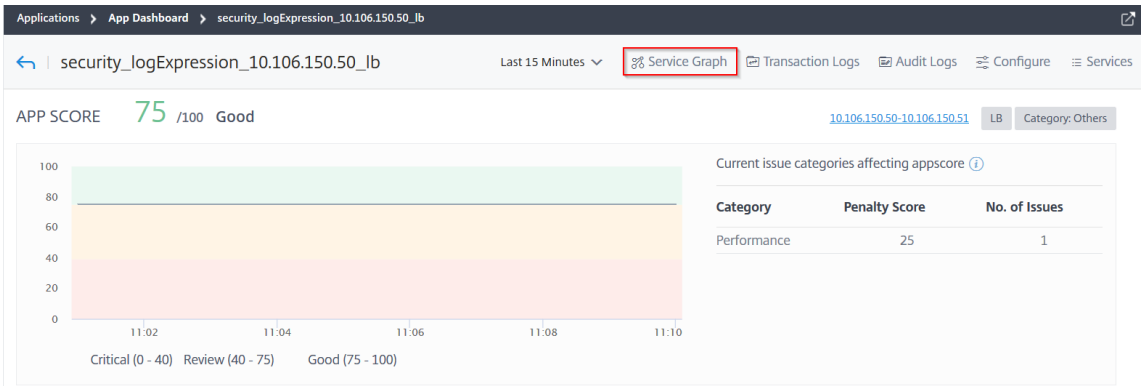
## Gráfico de servicio para aplicaciones

January 30, 2024

Para ver el gráfico de servicio de una aplicación:

1. Vaya a **Aplicaciones** > **Panel de control**.
2. Selecciona una aplicación.

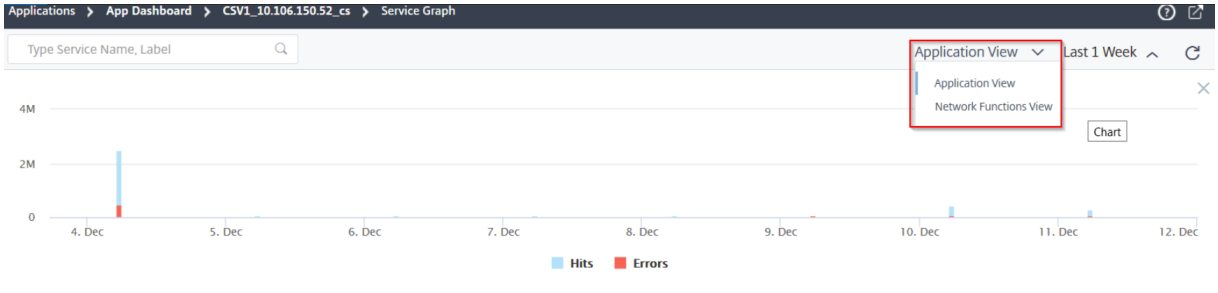
   Aparece la página de detalles de la aplicación.
3. Seleccione la duración del tiempo y haga clic en **Service Graph**.



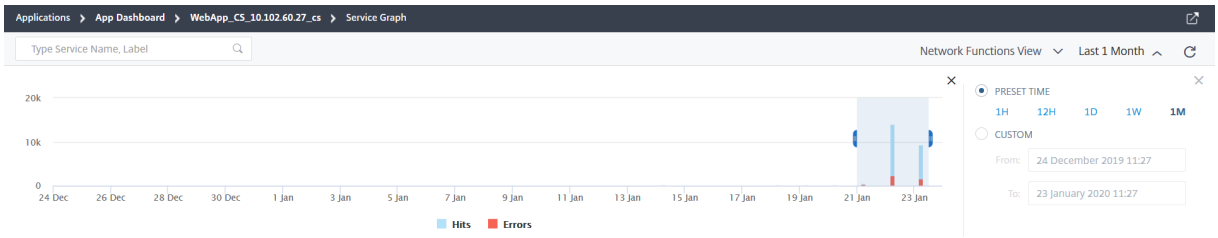

   Se muestra la página del gráfico de servicios de la aplicación seleccionada.

Puede ver el gráfico de servicios en **la vista de aplicaciones** o en la **vista de funciones de red**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

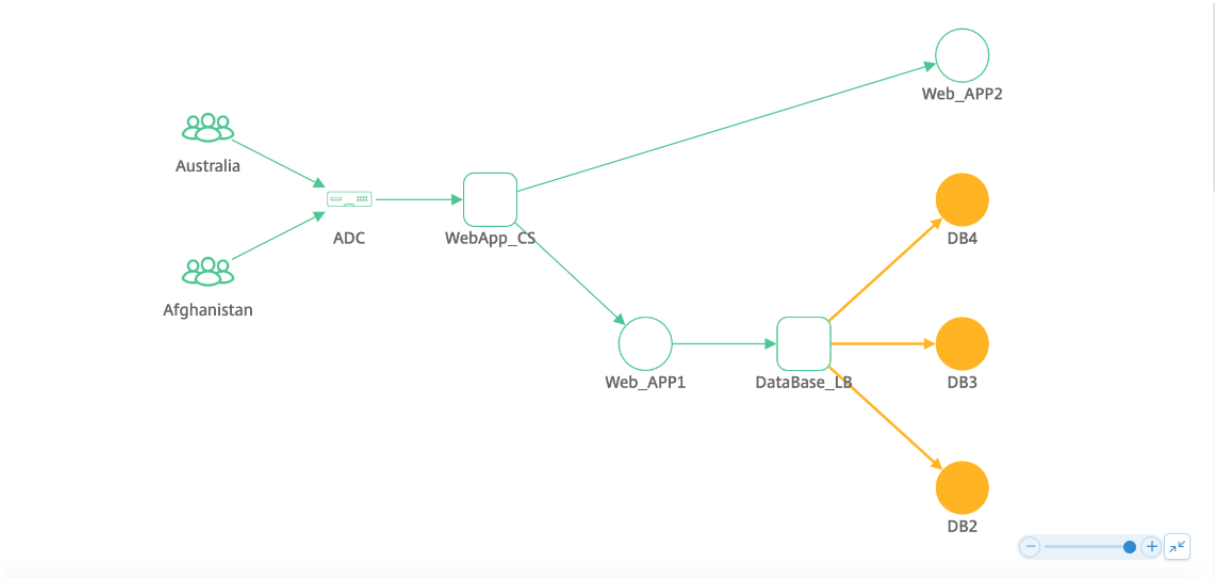



También puede arrastrar y seleccionar los aciertos y errores para modificar los resultados.




## Vista de aplicación

Muestra la descripción general de la configuración de la aplicación. En esta vista, puede visualizar la comunicación entre el cliente, el ADC y las aplicaciones web.

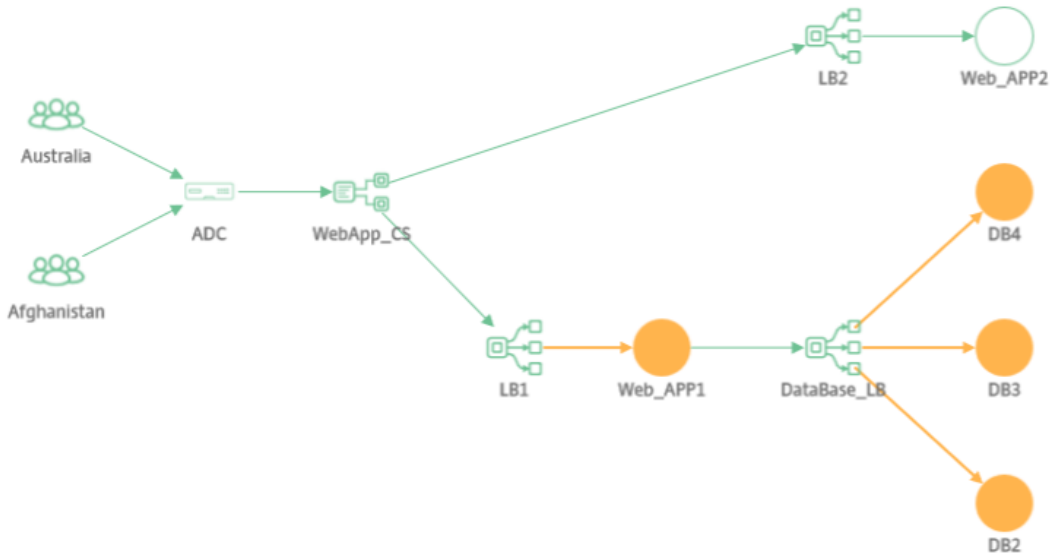



## Vista de funciones de red

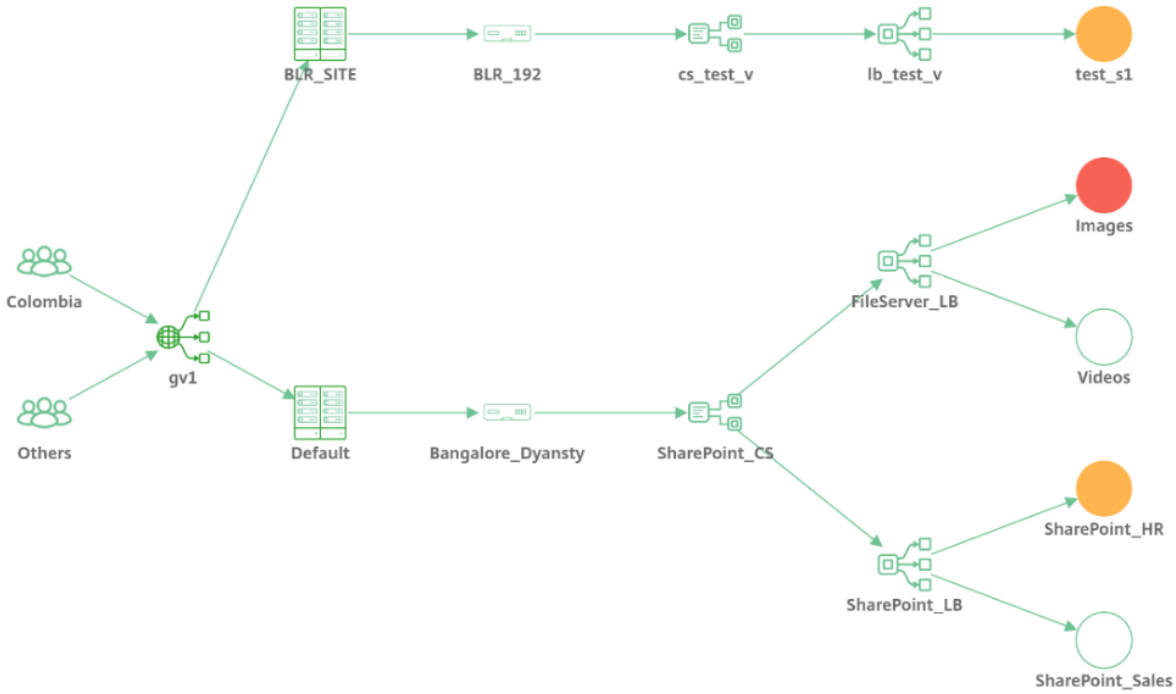
Muestra los servidores virtuales asociados a la aplicación. En esta vista, puede visualizar si el ADC se comunica con:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Servidor virtual de conmutación de contenido para acceder a la aplicación
- Servidor virtual de equilibrio de carga para acceder a la aplicación
- Servidores virtuales de conmutación de contenido y equilibrio de carga para acceder a la aplicación




Para la aplicación GSLB, los detalles se muestran junto con el centro de datos y NetScaler ADC.

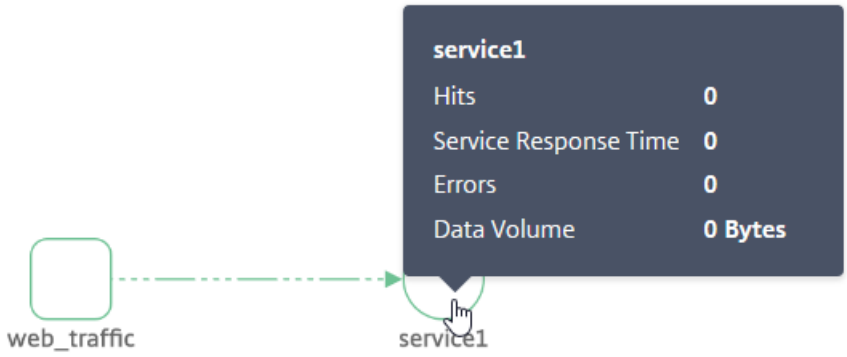



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Vista de gráfico de servicio para transacciones no activas

Si no hay transacciones activas entre el ADC y la aplicación web, el gráfico de servicio muestra solo la configuración básica de la aplicación (sin el cliente ni el ADC).

Al pasar el puntero del mouse sobre un servicio o servidor virtual, los detalles se muestran como 0 para todas las métricas, ya que no hay transacciones.



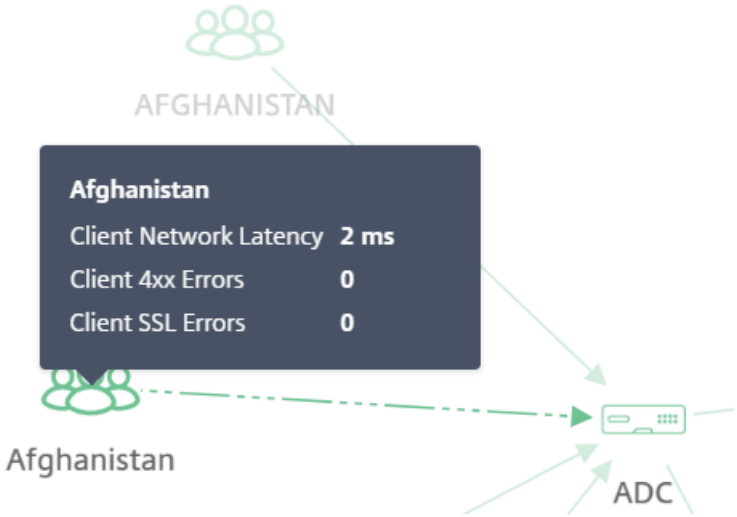

### Analice las métricas

Pase el puntero del ratón sobre cada servicio para ver los detalles de las métricas en la vista de aplicaciones o en la vista de funciones de red .

#### Métricas de clientes

Pase el puntero del mouse sobre el cliente para ver las métricas del cliente.

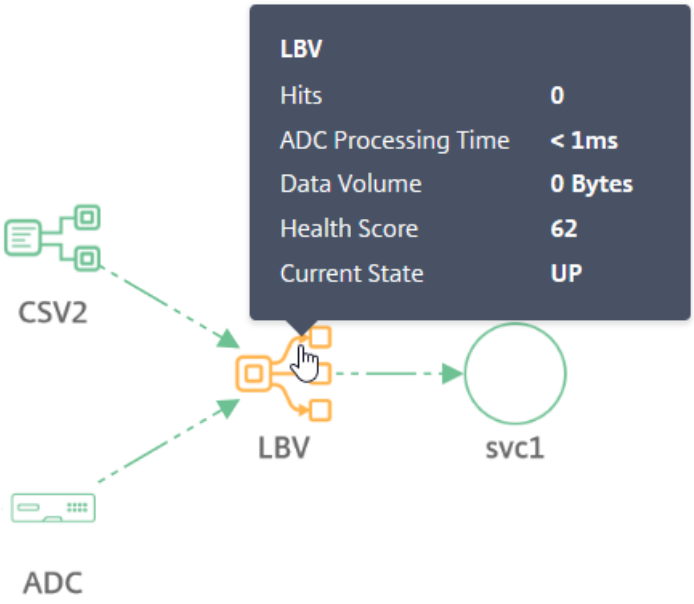
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Latencia de la red del cliente**: indica la latencia de la red del cliente.
- **Errores del cliente 4xx**: Indica el número total de errores 4xx producidos por el cliente.
- **Errores SSL del cliente**: Indica el número total de errores SSL del cliente.

### Métricas de funciones de red

Pase el puntero del mouse sobre un servicio de equilibrio de carga o cambio de contenido para ver los detalles de las métricas.



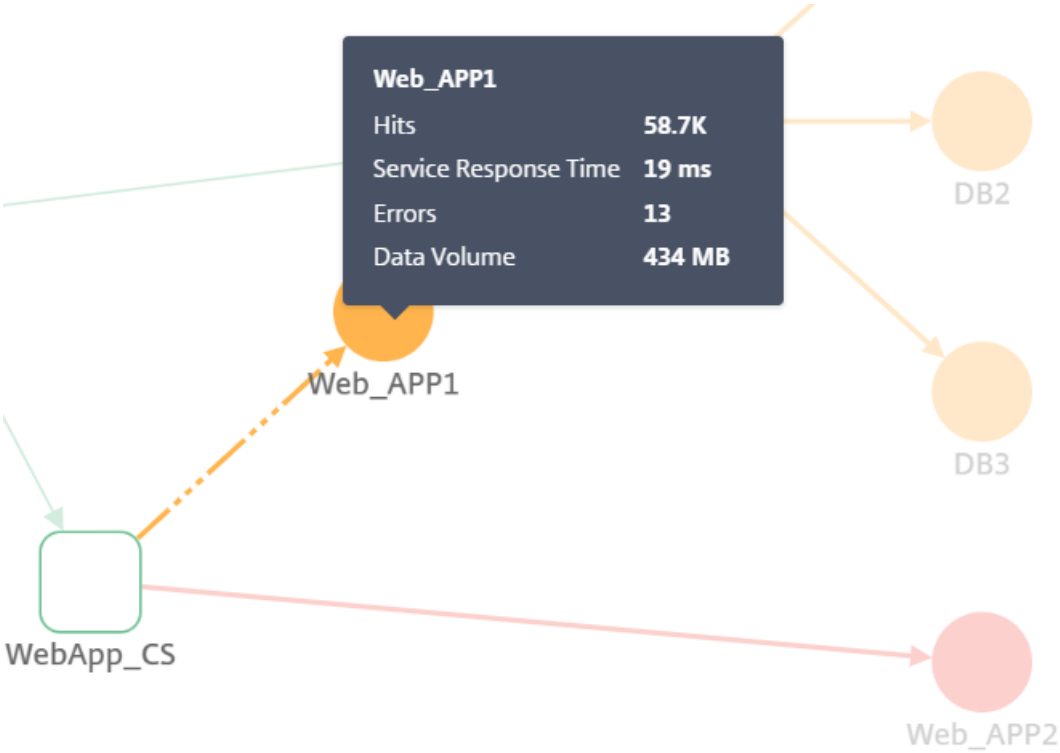

- **Hits**: Indica el número total de visitas recibidas por el servidor virtual

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Tiempo de procesamiento de ADC: indica el tiempo** de procesamiento promedio de la instancia de ADC
- **Volumen de datos**: Indica el volumen total de datos procesado por el servidor virtual
- **Puntuación de salud**: Indica la puntuación de la aplicación
- **Estado actual**: Indica el estado actual del servidor virtual

### Métricas de servicio

Pase el puntero del mouse sobre un servicio (aplicación web) para ver las métricas

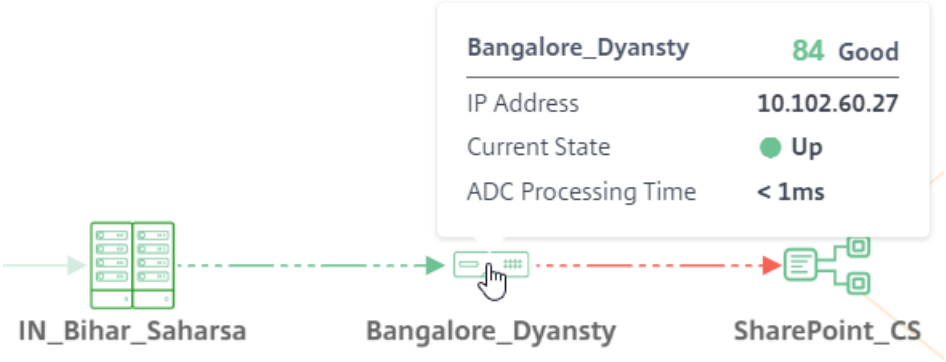



- **Visitas**: indica el número total de visitas recibidas por el servicio
- **Tiempo de respuesta del servicio**: indica el tiempo de respuesta promedio del servicio
- **Errores**: indica el total de errores ocurridos en el servicio.
- **Volumen de datos**: indica el total de datos procesados por el servicio

### Métricas de NetScaler ADC (solo para aplicaciones GSLB)

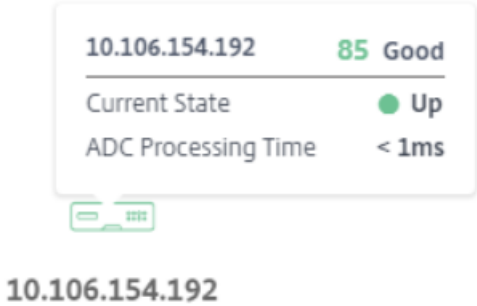
Pase el puntero del mouse sobre el ADC para ver las métricas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- Muestra el nombre del host y la puntuación ADC actual. La puntuación se calcula en función de los diferentes problemas potenciales de NetScaler ADC. Para obtener más información, consulte Puntuación de instancias.
- **Dirección IP**: Indica la dirección IP de NetScaler ADC
- **Estado actual**: Indica el estado NetScaler ADC, como Activo, Inactivo o Fuera de servicio
- **Tiempo de procesamiento de ADC**: indica el tiempo de procesamiento promedio de la instancia de ADC

> **Nota**
>
> Si no se asigna un nombre de host a NetScaler ADC:
>
> -Se muestra la dirección IP de NetScaler ADC en lugar del nombre del host.
>
> -En las métricas, no se muestra la información de la dirección IP de NetScaler ADC.

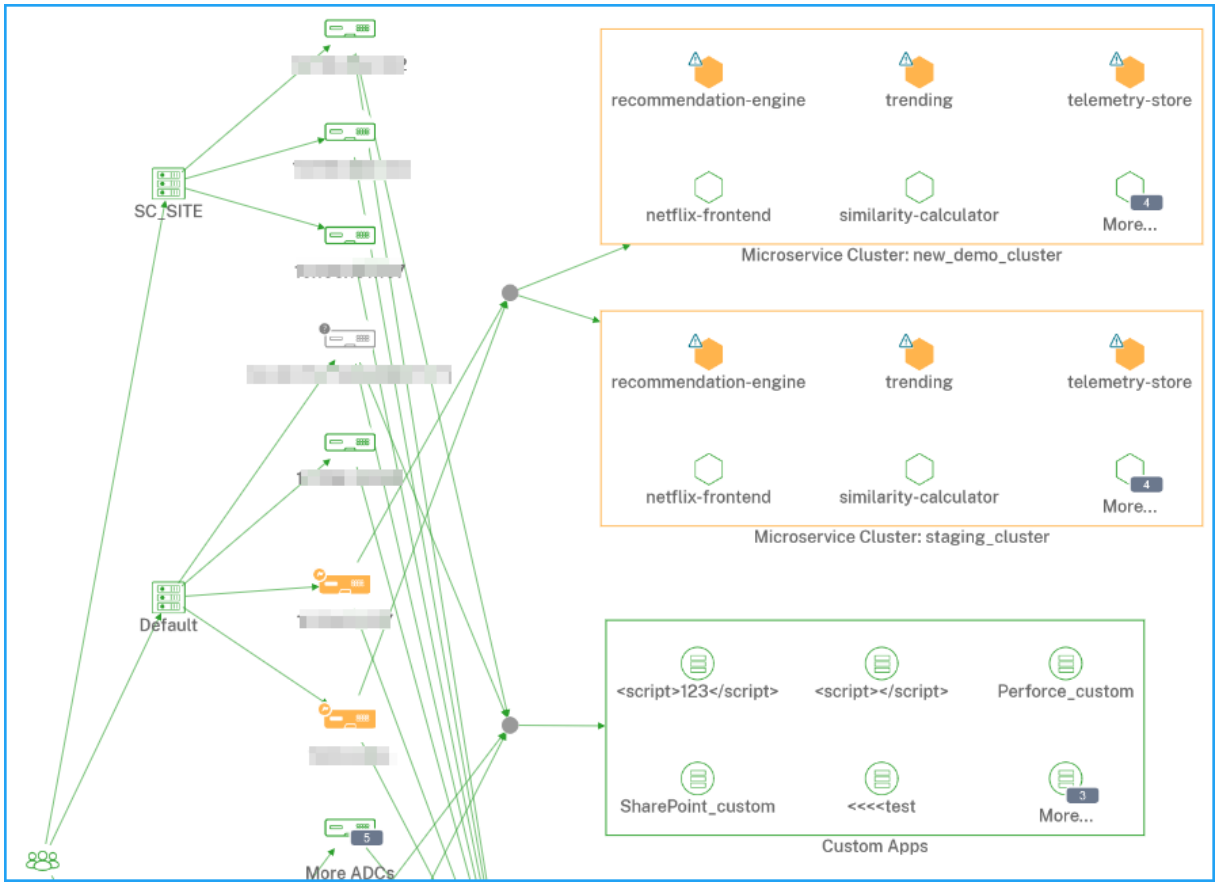



## Vista holística de todas las aplicaciones en el gráfico de servicio

January 30, 2024

Vaya a **Aplicaciones** > **Gráfico de servicio** y, a continuación, haga clic en **Global**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




El gráfico de servicio muestra lo siguiente para la duración de tiempo seleccionada:

- Región desde la que los usuarios acceden a la aplicación específica

Centros de datos en los que se alojan las instancias de NetScaler ADC

- El total de aplicaciones discretas de todas las instancias de NetScaler ADC

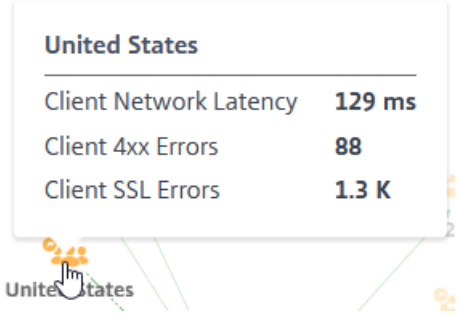
> **Nota**
>
> Si una instancia de NetScaler ADC no tiene aplicaciones discretas, el borde de flecha hacia el servidor virtual discreto desde la instancia de NetScaler ADC no está visible

- El total de aplicaciones personalizadas de todas las instancias de NetScaler ADC
- El total de aplicaciones de microservicios de la instancia de NetScaler ADC CPX

## Ver métricas de cliente

Coloque el puntero del mouse (mouse) sobre una región de cliente para ver las métricas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

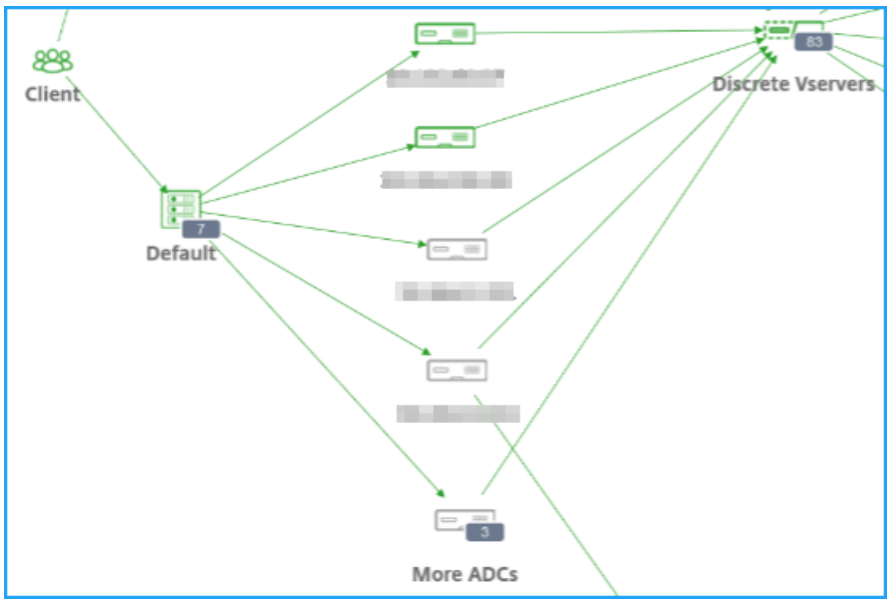



- **Latencia de red cliente: indica la latencia** promedio de la red del cliente.
- **Errores del cliente 4xx**: indica el total de errores del cliente 4xx.
- **Errores de SSL del cliente**: indica el total de errores de SSL del cliente.

## Ver detalles de NetScaler ADC

El gráfico de servicio le permite ver:

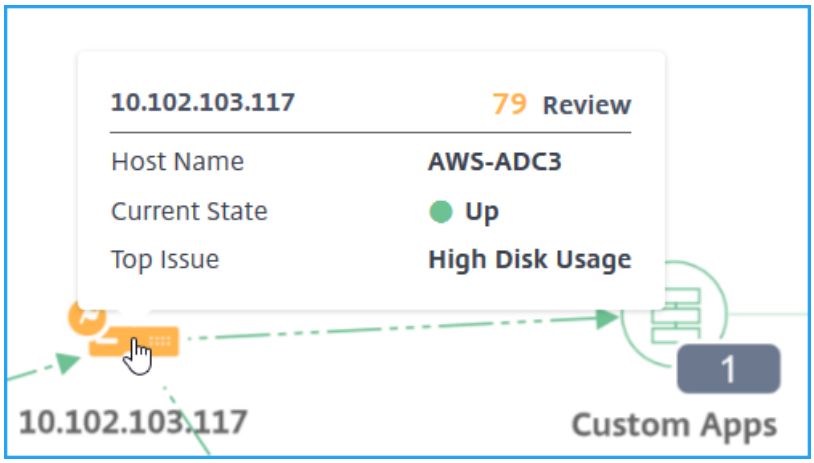
- El centro de datos agrupado con el total de instancias de NetScaler ADC
- Solo las 4 instancias NetScaler ADC con puntuación baja de cada centro de datos




Haga clic en **Más ADC** para ver todas las instancias de NetScaler ADC seleccionando las fichas de estado respectivas (Crítico, Revisar, Bien y No Aplicable).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Coloque el puntero del mouse (ratón) sobre una instancia de NetScaler ADC para ver las métricas.




Podrá ver lo siguiente:

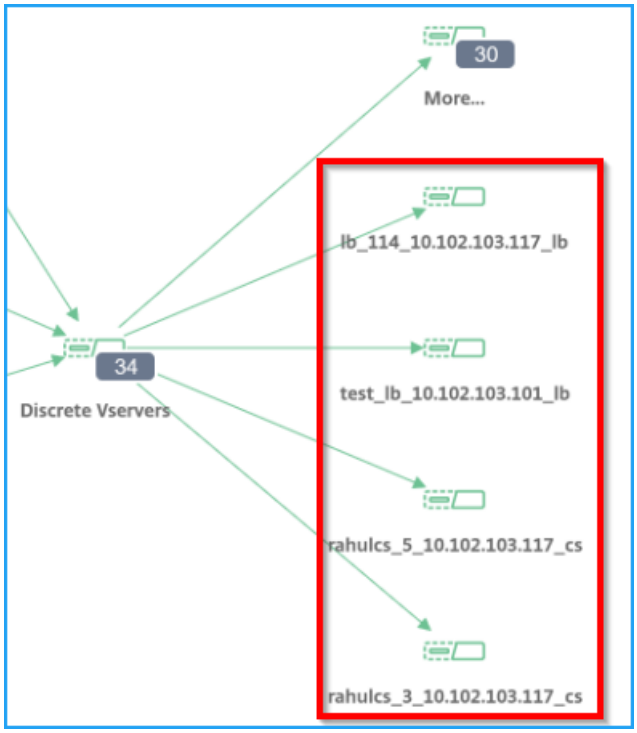
- Dirección IP y puntuación de la instancia de NetScaler ADC
- **Nombre de host**: indica el nombre de host asignado a la instancia de NetScaler ADC.
- **Estado actual**: Indica el estado actual de la instancia de NetScaler ADC, como Activo, abajo, fuera de servicio.
- **Problema**principal : indica el problema principal que afecta a la puntuación actual de Citrix ADC

Haga clic en la **instancia de NetScaler ADC** para ver los detalles de la instancia, como la puntuación de la instancia, las métricas clave y los problemas asociados con la instancia de ADC. Para obtener más información, consulte Ver detalles de instancias en Infrastructure Analytics.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Ver aplicaciones discretas

El gráfico de servicio muestra las 4 mejores aplicaciones discretas de puntuación baja.




Tenga en cuenta que tiene las siguientes aplicaciones discretas:

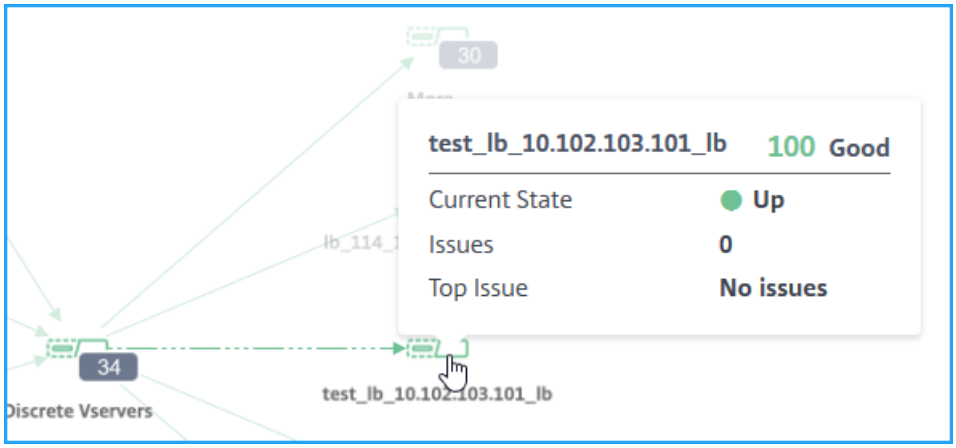
| Nombre de la aplicación | Citrix ADC | Puntuación de la aplicación | Estado de la aplicación |
|---|---|---|---|
| App1 | 10.102.29.50 | 35 (Crítico) | Activo |
| App2 | 10.102.29.90 | 100 (Bien) | Inactivo |
| App 3 | 10.102.32.40 | 49 (Revisión) | Activo |
| Aplicación 4 | 10.102.113.208 | 92 (Bien) | Inactivo |
| Aplicación 5 | 10.102.25.25 | 86 (Bien) | Activo |
| Aplicación 6 | 10.102.29.41 | 77 (Bien) | Activo |
| Aplicación 7 | 10.102.29.102 | 41 (Revisión) | Activo |

En este caso, puede ver a App1, App3, App6 y App 7 como las 4 aplicaciones con puntuaciones más bajas en el gráfico de servicios.

Del mismo modo, también puede ver las 4 aplicaciones de puntuación baja principales para aplicaciones **personalizadas** y **microservicios**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

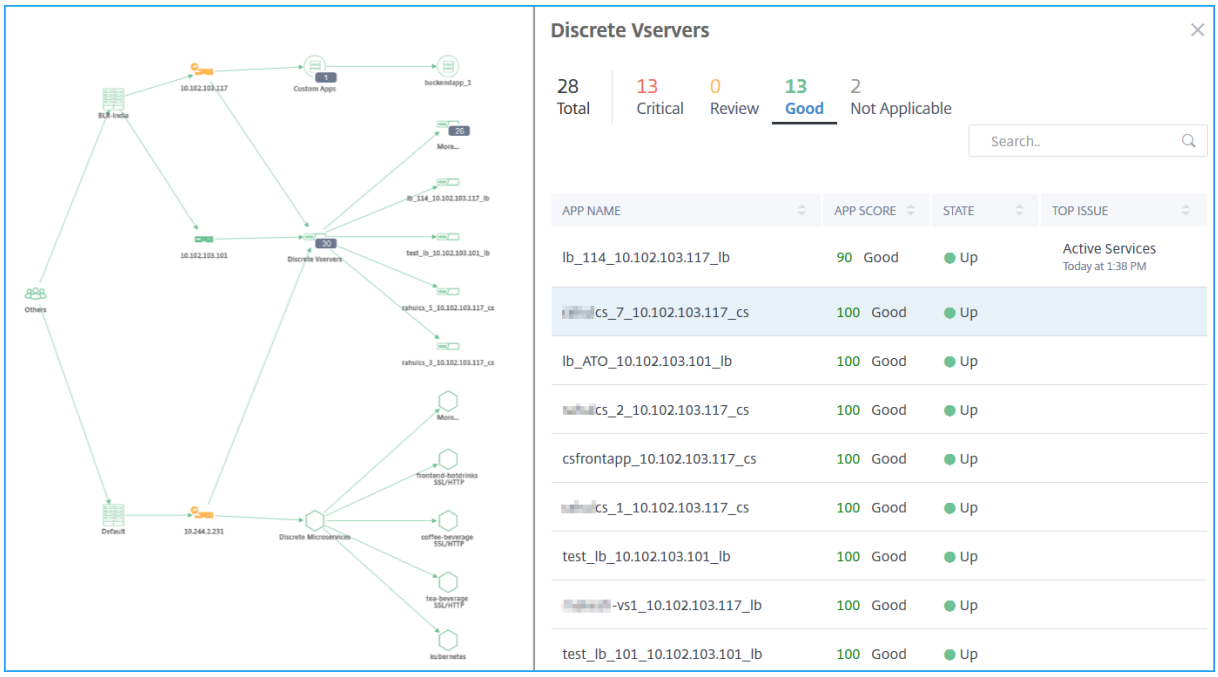
Coloque el puntero del mouse sobre un servicio para ver la información de las métricas.




Podrá ver lo siguiente:

- El nombre de la aplicación y la puntuación
- **Estado actual**: Indica el estado actual de la aplicación, como Activo o Inactivo
- **Problemas**: indica el total de problemas aplicables a la aplicación
- **Problema principal**: indica el problema principal que afecta a la puntuación general de la aplicación

Haga clic en **Más** para ver todas las aplicaciones discretas. La página Servidor virtual discreto se muestra como se muestra en la imagen siguiente:

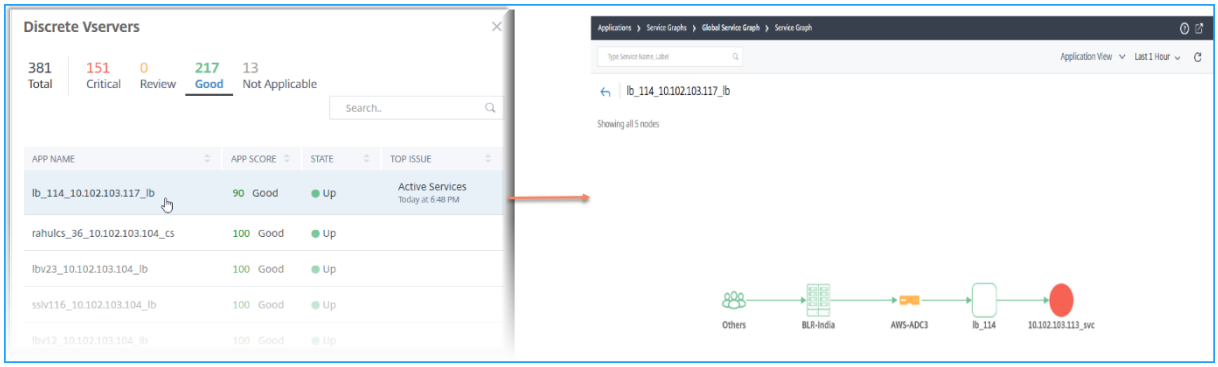



Los servidores virtuales se muestran de acuerdo con el estado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Total**: total de aplicaciones discretas
- **Crítica**: La puntuación de la aplicación está entre 0 y < 40
- **Revisión**: La puntuación de la aplicación es entre 40 y < 75
- **Bueno**: la puntuación de la aplicación es > 75
- **No aplicable**: la aplicación no está vinculada a ningún servidor virtual

Puede hacer clic en cada ficha para ver los servidores virtuales. Al hacer clic en una aplicación, se muestra el gráfico de servicio de la aplicación seleccionada.




Para obtener más información, consulte Service Graph para aplicaciones.

## Ver aplicaciones de microservicios

El gráfico de servicio también muestra todas las aplicaciones de microservicios que pertenecen a los clústeres de Kubernetes. Coloque el puntero del mouse sobre un servicio para ver los detalles de las métricas.

Podrá ver lo siguiente:

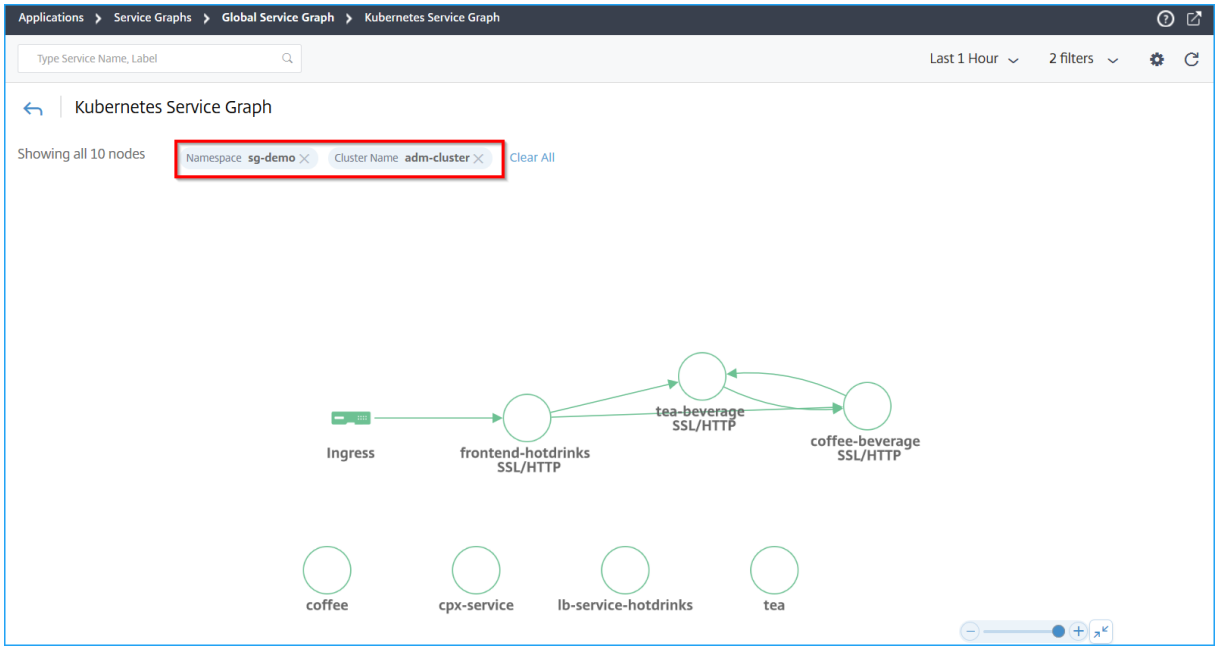
- El nombre del servicio
- El protocolo utilizado por el servicio como SSL, HTTP, TCP, SSL sobre HTTP
- **Visitas**: Número total de visitas recibidas por el servicio
- **Tiempo de respuesta del servicio**: El tiempo de respuesta promedio tomado del servicio.

  (Tiempo de respuesta = RTT del cliente + último byte de la solicitud —primer byte de la solicitud)
- **Errores**: El total de errores, como 4xx, 5xx, etc.
- **Volumen de datos**: El volumen total de datos procesados por el servicio
- **Espacio de nombres**: El espacio de nombres del servicio
- **Nombre del clúster: Nombre** del clúster en el que está alojado el servicio

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

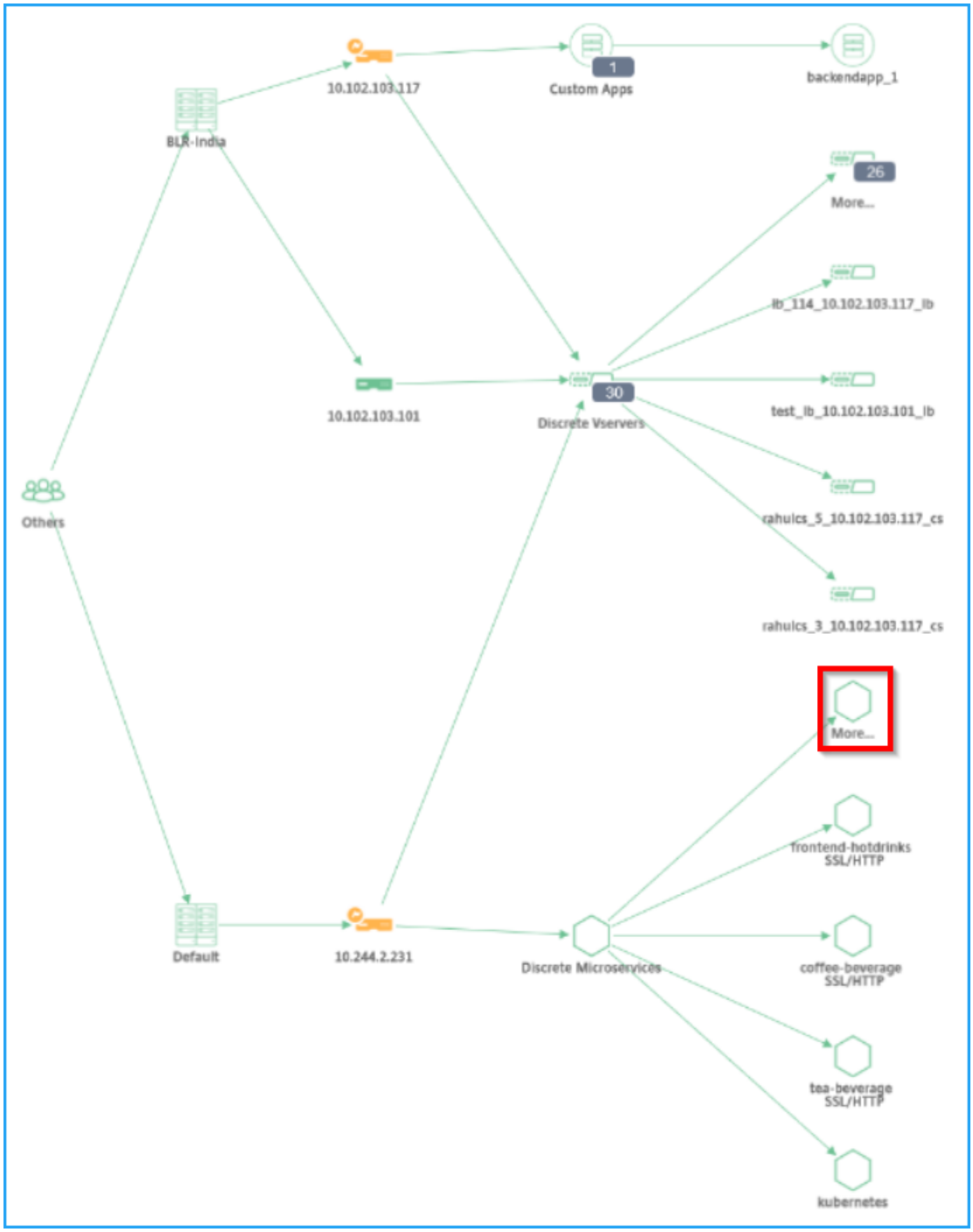
- **Errores del servidor SSL**: El total de errores SSL del servicio

Al hacer clic en un servicio, se muestra el gráfico de servicio Kubernetes para el servicio seleccionado, junto con el espacio de nombres de servicio y los filtros de nombre de clúster aplicados.




Haga clic en **Más** para ver el gráfico de servicios de Kubernetes que tiene todos los servicios. Para obtener más información sobre el gráfico de servicio de Kubernetes, consulte Gráfico de servicio para aplicaciones nativas de la nube.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



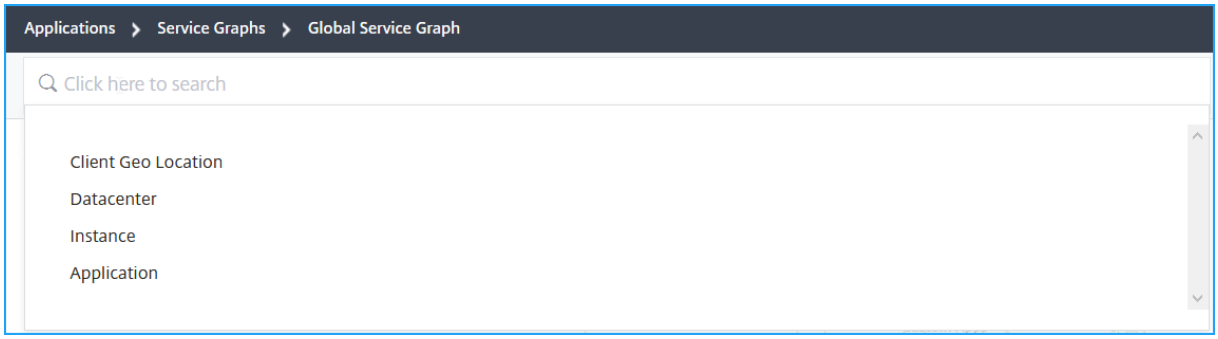

## Barra de búsqueda para filtrar resultados

Puede utilizar la barra de búsqueda para filtrar los resultados. Como administrador, esta barra de búsqueda le permite reducir rápidamente a una instancia, cliente/aplicación/centro de datos en particular, cuando tenga:

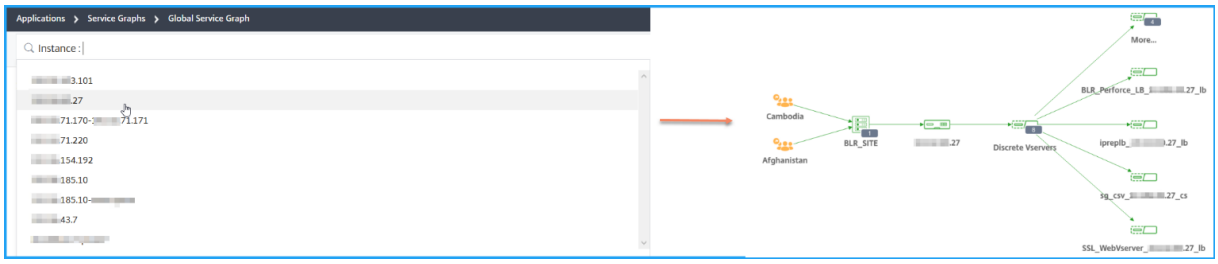
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Una gran empresa con muchos centros de datos
- Se han configurado muchas instancias de NetScaler ADC para cada centro de datos
- Se configuraron muchas aplicaciones implementadas o a las que se accede a través de cada instancia de NetScaler ADC
- Clientes que acceden a la aplicación desde diferentes ubicaciones

Coloque el puntero del mouse en la barra de búsqueda y seleccione la categoría que quiere crear el filtro.




Por ejemplo, si quiere ver una instancia ADC concreta, seleccione **Instancia** en la barra de búsqueda y seleccione la dirección IP de la instancia. El gráfico de servicio global muestra la instancia seleccionada y sus aplicaciones asociadas, centros de datos y ubicaciones de cliente.




## StyleBooks

January 30, 2024

Los StyleBooks simplifican la tarea de administrar configuraciones complejas de NetScaler ADC para sus aplicaciones. Un StyleBook es una plantilla que puede utilizar para crear y administrar configuraciones de NetScaler ADC. Puede crear un StyleBook para configurar una función específica de NetScaler ADC, o puede diseñar un StyleBook para crear configuraciones para la implementación de una aplicación empresarial, como Microsoft Exchange o Lync.

Los StyleBooks se ajustan perfectamente a los principios de la infraestructura como código que practican los equipos de DevOps, donde las configuraciones son declarativas y se controlan por versiones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Las configuraciones también se repiten y se implementan como un todo. Los StyleBooks ofrecen las siguientes ventajas:

- **Declarativo**: Los StyleBooks se escriben en una sintaxis declarativa en lugar de imperativa. Los StyleBooks le permiten centrarse en describir el resultado o el "estado deseado"de la configuración en lugar de las instrucciones paso a paso sobre cómo lograrlo en una instancia específica de NetScaler ADC. Citrix Application Delivery Management (ADM) calcula la diferencia entre el estado existente en un Citrix ADC y el estado deseado que especificó, y realiza las modificaciones necesarias en la infraestructura. Dado que los StyleBooks utilizan una sintaxis declarativa, escrita en YAML, los componentes de un StyleBook se pueden especificar en cualquier orden, y NetScaler ADM determina el orden correcto en función de sus dependencias calculadas.
- **Atomic**: Cuando usa StyleBooks para implementar configuraciones, se implementa la configuración completa o no se implementa ninguna de ellas, lo que garantiza que la infraestructura se mantenga siempre en un estado coherente.
- **Versionado**: un StyleBook tiene un nombre, un espacio de nombres y un número de versión que lo distingue de forma única de cualquier otro StyleBook del sistema. Cualquier modificación de un StyleBook requiere una actualización de su número de versión (o de su nombre o espacio de nombres) para mantener este carácter único. La actualización de la versión también permite mantener varias versiones del mismo StyleBook.
- **Composable**: una vez definido un StyleBook, el StyleBook se puede usar como unidad para crear otros StyleBooks. Puede evitar repetir los patrones de configuración comunes. También le permite establecer componentes básicos estándar en su organización. Dado que los StyleBooks están versionados, los cambios en los StyleBooks existentes dan como resultado nuevos StyleBooks, lo que garantiza que los StyleBooks dependientes nunca se rompan
- **Centrado en aplicaciones**: los StyleBooks se pueden utilizar para definir la configuración de NetScaler ADC de una aplicación completa. La configuración de la aplicación se puede abstraer mediante el uso de parámetros. Por lo tanto, los usuarios que crean configuraciones a partir de un StyleBook pueden interactuar con una interfaz sencilla que consiste en rellenar algunos parámetros para crear lo que puede ser una configuración compleja de Citrix ADC. Las configuraciones creadas a partir de StyleBooks no están vinculadas a la infraestructura. De este modo, se puede implementar una única configuración en uno o varios ADC de Citrix y también se puede mover de una instancia a otra.
- **Interfaz de usuario generada automáticamente**: NetScaler ADM genera automáticamente formularios de interfaz de usuario utilizados para rellenar los parámetros del StyleBook cuando se realiza la configuración mediante la interfaz gráfica de usuario de NetScaler ADM. Los autores de StyleBook no necesitan aprender un nuevo lenguaje de interfaz gráfica de usuario ni crear páginas y formularios de interfaz de usuario por separado.
- Basado en**API:**todas las operaciones de configuración se admiten mediante la GUI de NetScaler

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ADM o mediante las API REST. Las API se pueden usar en modo sincrónico o asíncrono. Además de las tareas de configuración, las API de StyleBooks también permiten descubrir el esquema (descripción de los parámetros) de cualquier StyleBook en tiempo de ejecución.

Puede utilizar un StyleBook para crear varias configuraciones. Cada configuración se guarda como un paquete de configuración. Por ejemplo, considere que tiene un StyleBook que define una configuración típica de la aplicación de equilibrio de carga HTTP. Puede crear una configuración con valores para las entidades de equilibrio de carga y ejecutarla en una instancia de Citrix ADC. Esta configuración se guarda como un paquete de configuración. Puede usar el mismo StyleBook para crear otra configuración con valores diferentes y ejecutarla en la misma instancia de Citrix ADC o en una instancia diferente. Se crea un nuevo paquete de configuración para esta configuración. Un paquete de configuración se guarda tanto en Citrix ADM como en la instancia de Citrix ADC en la que se ejecuta la configuración.

Puede utilizar StyleBooks predeterminados, incluidos con NetScaler ADM, para crear configuraciones para su implementación, o diseñar sus propios StyleBooks e importarlos a NetScaler ADM. Puede usar los StyleBooks para crear configuraciones mediante la GUI de NetScaler ADM o mediante las API.

Este documento incluye la siguiente información:

- Cómo ver StyleBooks
- StyleBooks predeterminados
- Libros de estilo desarrollados para aplicaciones empresariales
- StyleBooks personalizados
- APIs en StyleBooks
- Gramática de StyleBooks

## Categorías de StyleBook

January 30, 2024

Hay dos categorías de StyleBook en Citrix Application Delivery Management (ADM). Son los StyleBooks predeterminados y los StyleBooks personalizados. Ya sea predeterminado o personalizado, un StyleBook es un StyleBook público o privado. En Citrix ADM, puede ver todos los StyleBooks que están presentes en el sistema, independientemente de su tipo o estado de visibilidad. También puede ver una visualización gráfica de cómo los StyleBooks están conectados entre sí.

En este documento se explican los diferentes tipos de StyleBooks. Además, explica las siguientes acciones que puede realizar en StyleBooks de Citrix ADM:

- Descargue un StyleBook personalizado y realice modificaciones, o cree un StyleBook basado en uno existente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Ocultar ADM StyleBooks predeterminados.
- Elimine un StyleBook personalizado de Citrix ADM.
- Agregue etiquetas a los StyleBooks.

### StyleBooks predeterminados y personalizados

- Los**StyleBooks predeterminados** son los StyleBooks que se suministran con Citrix ADM y permiten crear configuraciones que puede implementar en las instancias de Citrix ADC. No puede eliminar StyleBooks predeterminados, pero puede ocultarlos de la GUI de ADM.
- Los**StyleBooks personalizados** son sus propios StyleBooks que importó a Citrix ADM.

Los StyleBooks predeterminados y personalizados pueden ser públicos o privados.

### StyleBooks públicos y privados

Los StyleBooks a partir de los cuales puede crear paquetes de configuración se pueden clasificar como StyleBooks **públicos**. Es decir, todos están disponibles para su uso directo para crear configuraciones a partir de la GUI y API de Citrix ADM.

Sin embargo, algunos StyleBooks se utilizan como bloques de construcción para otros StyleBooks. Dichos StyleBooks están marcados como **privados**. Los StyleBooks privados no se pueden utilizar directamente para crear paquetes de configuración desde la GUI de Citrix ADM. Sin embargo, aún puede mostrar y ver estos StyleBooks en Citrix ADM. Para marcar cualquiera de sus StyleBooks personalizados como **privados**, establezca el atributo private en StyleBook en **true**. Aún puede usar StyleBooks privados para crear paquetes de configuración mediante las API de Citrix ADM.

#### Ejemplo de un StyleBook marcado como privado

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
```

### Ver StyleBooks

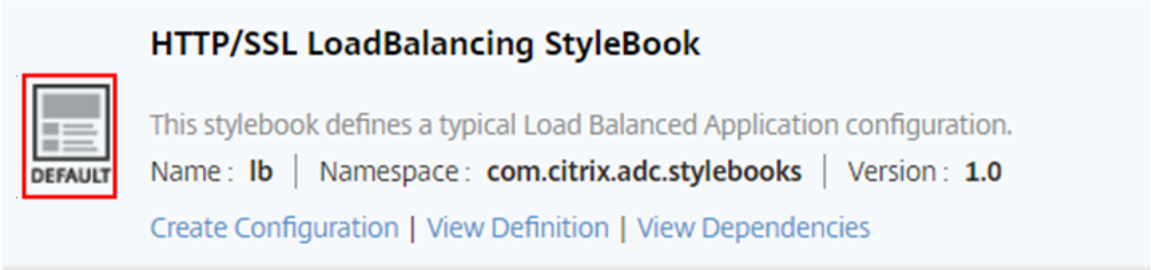
El número de StyleBooks: tanto los predeterminados como los privados están aumentando en Citrix ADM. Puede que quiera buscar el StyleBook concreto al que quiere acceder. También es posible que

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

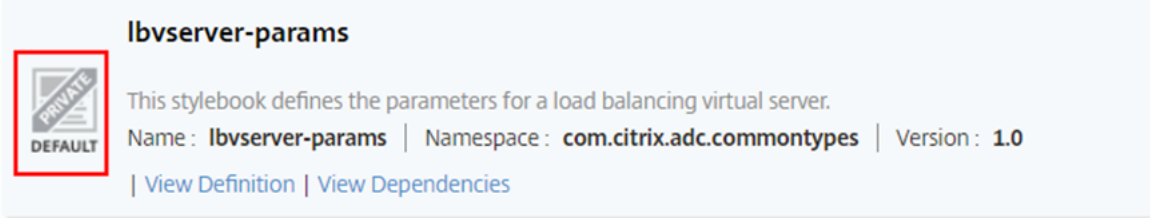
quiera ver ambos tipos de StyleBooks por separado.

En Citrix ADM, cuando vaya a **Aplicaciones** > **StyleBooks**, puede ver una lista de los StyleBooks que están presentes en el sistema.

Un StyleBook público predeterminado tiene el siguiente icono en su panel:

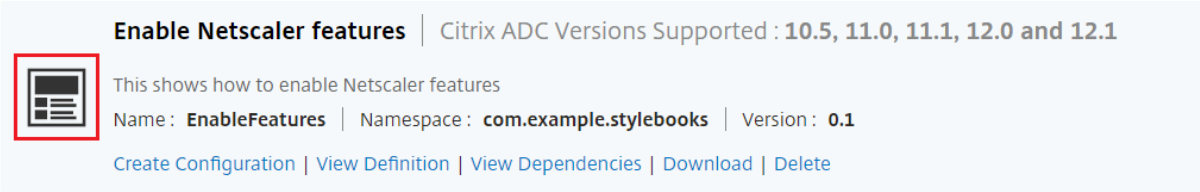



Mientras que un StyleBook privado predeterminado tiene un icono que lo declara como un StyleBook privado:

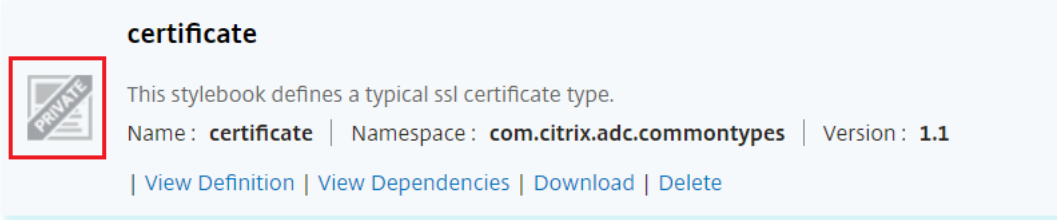



Aunque puede ver la definición y las dependencias de un StyleBook privado, no puede crear paquetes de configuración a partir de un StyleBook privado mediante la GUI. El propósito principal de un StyleBook privado es usarlo como bloque de creación para otro StyleBook. El uso de building-blocks-StyleBooks fomenta la reutilización de patrones de configuración comunes.

Un StyleBook público personalizado tiene un icono diferente, como se muestra en la siguiente imagen:

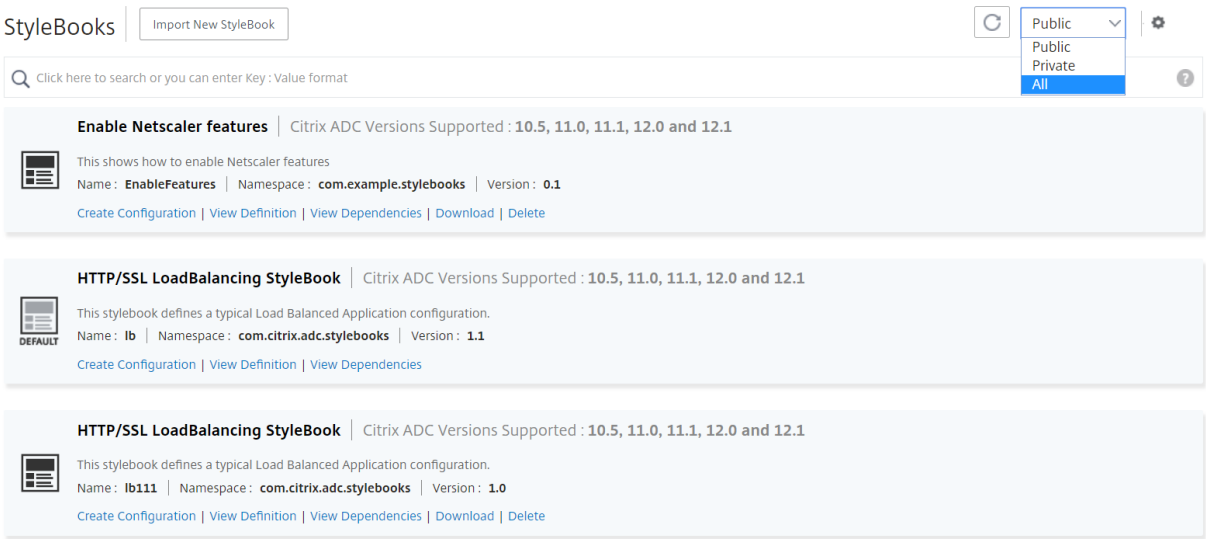



Mientras aparece un StyleBook privado personalizado con este icono:

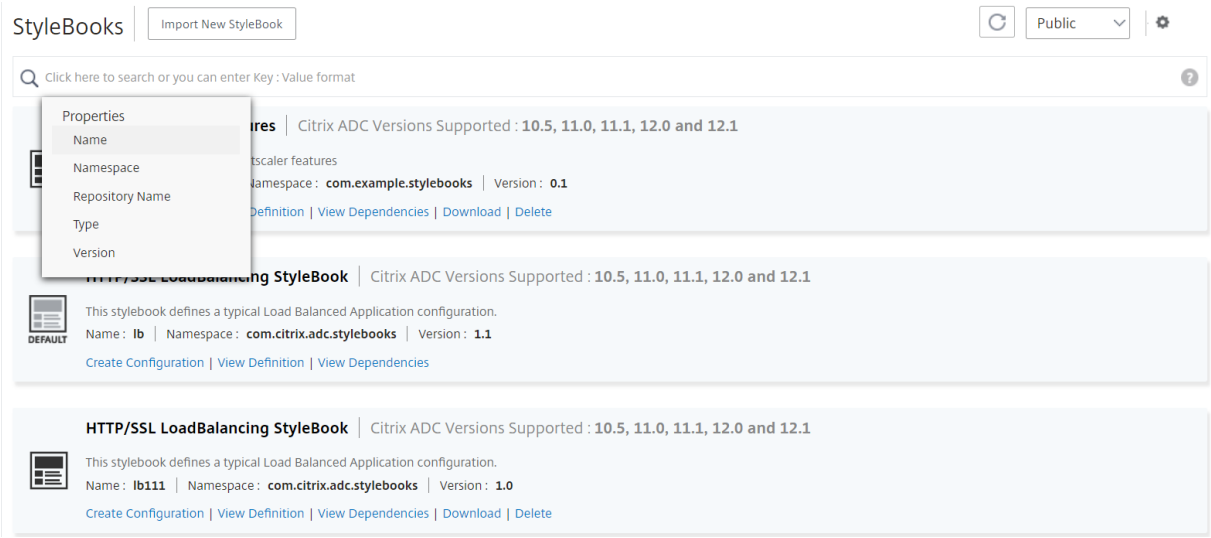



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En la parte superior derecha de la página, puede ver una opción para seleccionar el tipo de StyleBooks que deseas ver. Hay tres opciones: todos los StyleBooks, públicos o privados. Haga clic en una de las opciones.




También puede buscar un StyleBook en particular haciendo clic en el icono de búsqueda. Puede buscar por nombre, espacio de nombres y atributos de versión o una combinación de estas opciones. La operación de búsqueda no distingue entre mayúsculas y minúsculas.



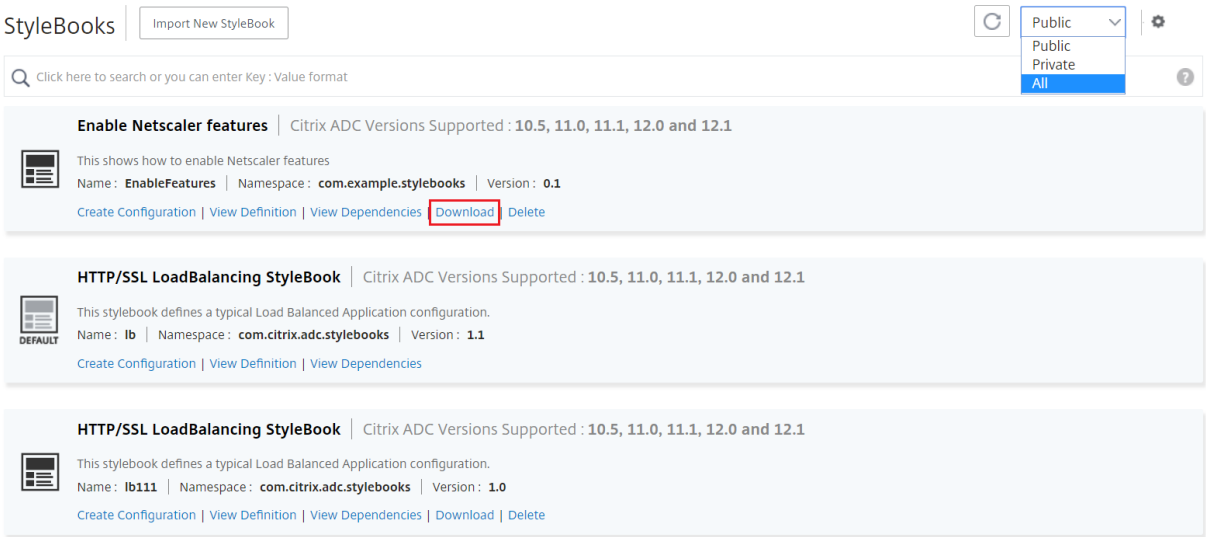

## Descargar StyleBooks personalizados

Para descargar los StyleBooks personalizados de Citrix ADM, vaya a **Aplicaciones** > **StyleBooks** > **Configuraciones**. En la lista de StyleBooks que se muestran en el panel derecho, marque la opción para descargar los StyleBooks personalizados. Haga clic en **Download**. Si el StyleBook tiene StyleBooks personalizados dependientes, puede incluir los StyleBooks dependientes en el paquete descar-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

gado.

> **Nota:**
>
> Puede descargar StyleBooks personalizados que estén marcados como públicos o privados.

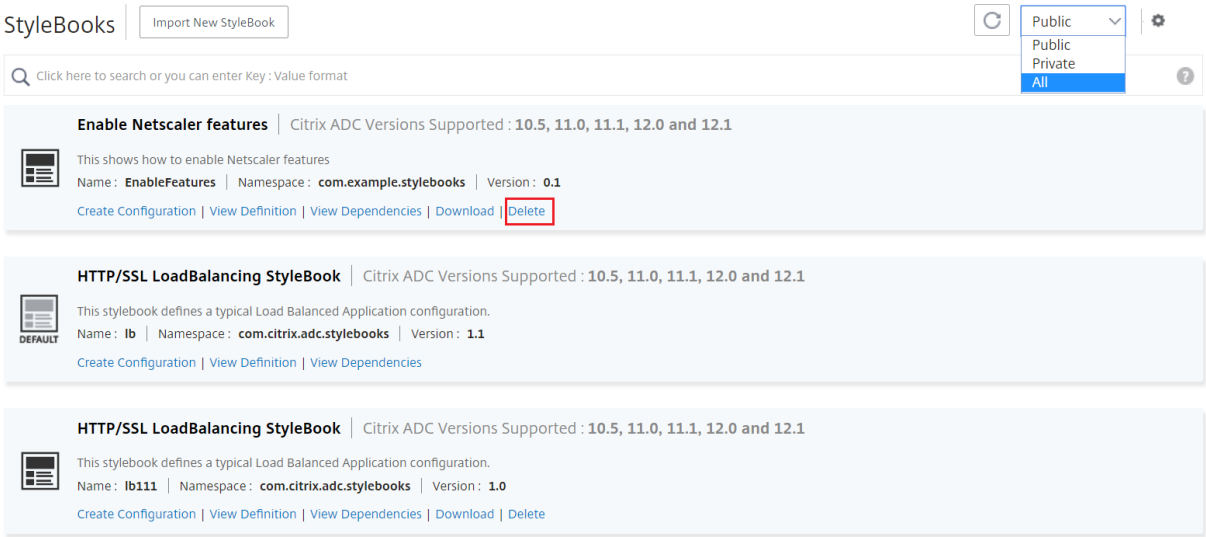



> **Nota:**
>
> No puede descargar los StyleBooks predeterminados de Citrix ADM. Puede ver sus definiciones y dependencias. Para ello, haga clic en los enlaces **Ver definición** y **Ver dependencias** del panel StyleBook.

## Eliminar StyleBooks personalizados

También puede eliminar un StyleBook personalizado haciendo clic en el botón **Eliminar**. Una ventana emergente le pide que confirme si quiere quitar StyleBook de Citrix ADM. Si el StyleBook utiliza otros StyleBooks personalizados, puede elegir quitar dichos StyleBooks activando la casilla de verificación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota:**
>
> No elimine un StyleBook personalizado si tiene StyleBooks dependientes en Citrix ADM. De lo contrario, rompería los StyleBooks existentes.

## Ver dependencias de StyleBook

Una función importante y poderosa de StyleBooks es que se pueden usar como bloques de construcción para otros StyleBooks. Puede importar un StyleBook a otro StyleBook. Un StyleBook importado se declara como un tipo y es utilizado por componentes o parámetros del segundo StyleBook. Puede estudiar los StyleBooks predeterminados existentes en Citrix ADM para saber cómo se puede crear un StyleBook encima de otro StyleBook.

Citrix ADM le permite ver una visualización gráfica de cómo los StyleBooks están conectados entre sí. Esta representación es especialmente útil para StyleBooks complejos que se crean mediante otros StyleBooks como bloques de creación. Al mirar el gráfico de dependencia, es posible ver las relaciones y dependencias entre varios StyleBooks.

Un StyleBook utilizado por otros StyleBooks no se puede quitar del sistema porque rompería los StyleBooks existentes. Mediante la visualización del gráfico de dependencia, puede identificar qué StyleBooks están impidiendo la eliminación de un StyleBook.

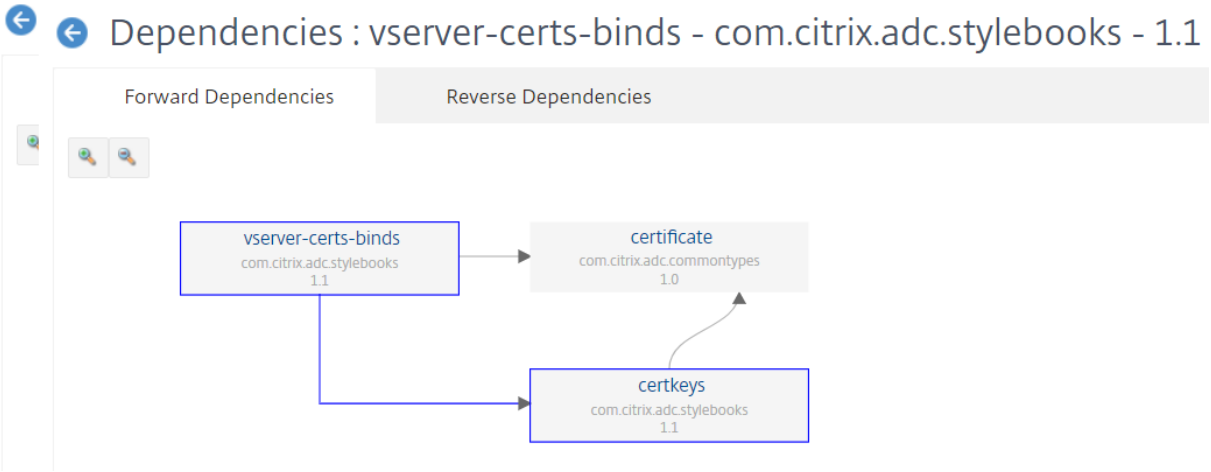
### Para ver las dependencias de StyleBook

En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**. La página StyleBooks muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplácese hacia abajo y busque su StyleBook. El icono de **StyleBook** muestra vínculos para crear una configuración, ver la definición de StyleBook y ver las dependencias de StyleBook. Haga clic en **Ver dependencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

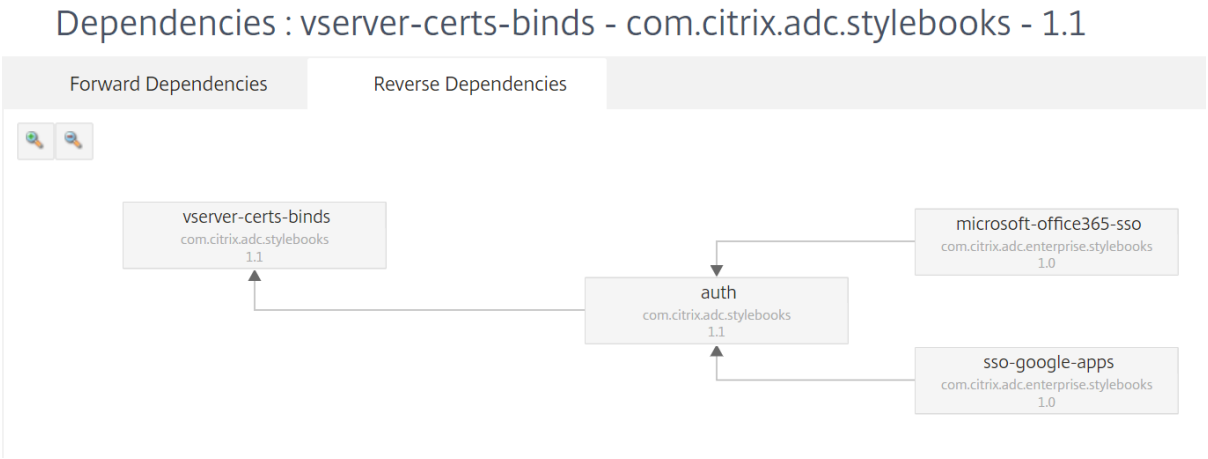
### Reenviar dependencias

La ficha **Forward Dependencies** le permite ver los diferentes StyleBooks predeterminados que utiliza su StyleBook. Siga las flechas para encontrar el StyleBook que utiliza un StyleBook. Al apuntar con el mouse a una de las flechas, se resaltan la flecha y los StyleBooks que están conectados entre sí. También puede hacer clic en los nombres de StyleBook para ver la definición de ese StyleBook.




### Dependencias inversas

La pestaña **Dependencias inversas** le permite ver gráficamente los StyleBooks que utilizan su StyleBook. Si sigue las flechas, puede ver que todos los StyleBooks en la pantalla apuntan hacia su StyleBook. Algunos StyleBooks pueden estar mediante el StyleBook directamente y algunos StyleBooks pueden estar mediante el StyleBook a través de otro StyleBook.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Auditar la configuración de ADC contra el paquete de configuración

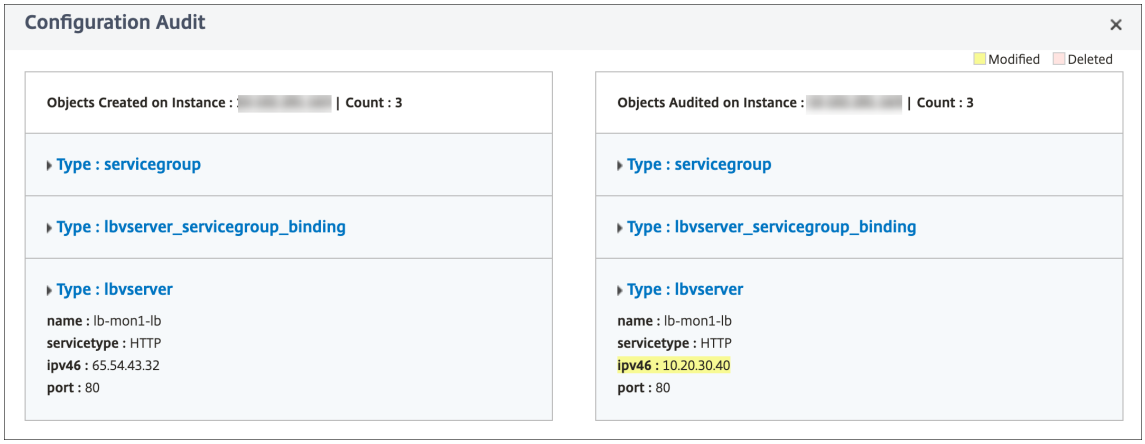
Puede comparar los cambios realizados por un paquete de configuración StyleBook con la configuración ADC actual. Con esta comparación, puede hacer lo siguiente:

- Detecte la deriva de configuración entre el paquete de configuración de StyleBook y la configuración de ADC.
- Identifique los objetos modificados y eliminados en el ADC que no reflejen los cambios realizados por el paquete de configuración.

Para comparar los cambios del paquete de configuración con la configuración de ADCs, haga lo siguiente.

1. Vaya a **Aplicaciones** > **StyleBooks** > **Configuraciones**.
2. Haga clic en **Auditoría de configuración**.

   La página Auditoría de configuración muestra los objetos creados y auditados.



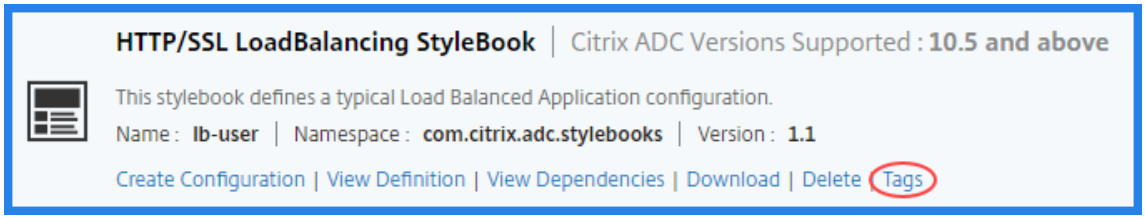

## Crear una etiqueta para el StyleBook

Puede agregar etiquetas a cualquier StyleBook en Citrix ADM. Las etiquetas son pares clave-valor que le permiten agrupar StyleBooks mediante diferentes criterios. Puede utilizar estas etiquetas mientras busca o filtra StyleBooks en Citrix ADM.

Para agregar una etiqueta al StyleBook:

1. Vaya a **Aplicaciones** > **StyleBooks**.
2. Seleccione **Etiquetas** en el StyleBook para el que quiere agregar etiquetas.

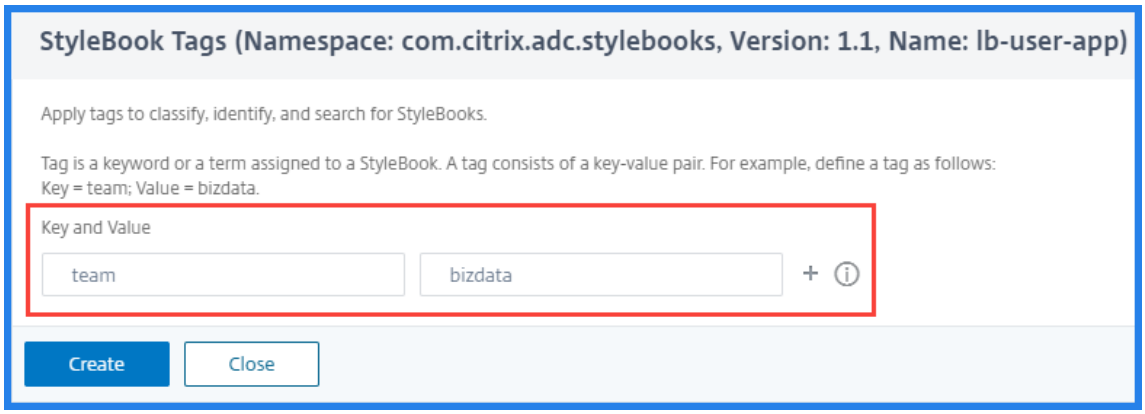
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Puede agregar etiquetas a todos los tipos de StyleBooks.

3. Especifique la información de **Key** y **Value** necesaria que le ayude a filtrar el StyleBook.

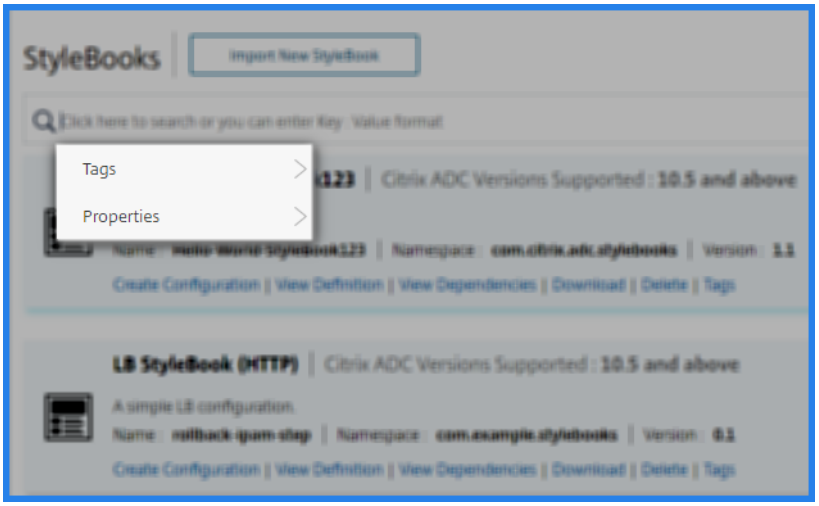
   Por ejemplo, Key=team y Value=bizdata




   Para agregar más etiquetas, haga clic en **+**.

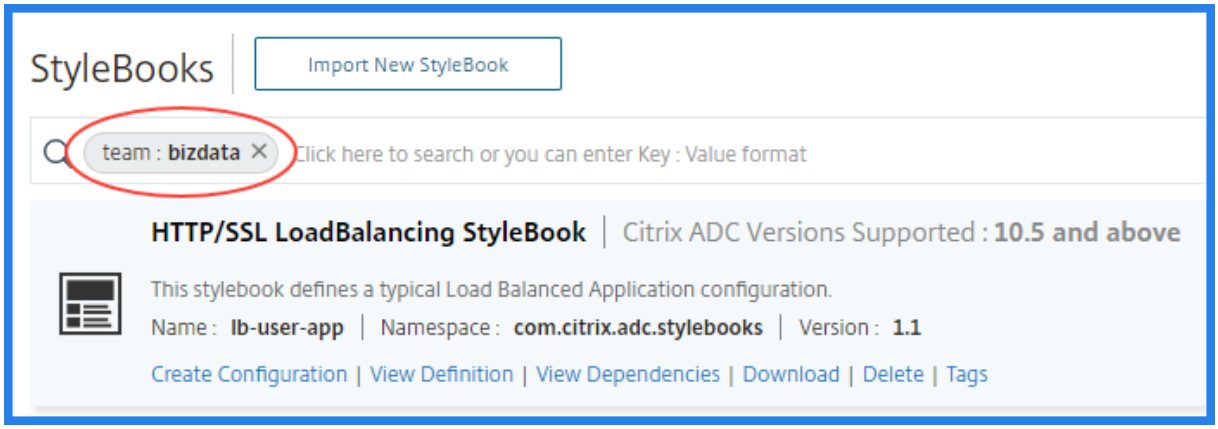
4. Haga clic en **Crear**.

Para filtrar StyleBooks mediante etiquetas, en la barra de búsqueda, haga clic en **Etiquetas** y seleccione clave y valor de la lista. Se muestran los StyleBooks que coinciden con la etiqueta especificada.




A continuación se muestra un ejemplo de búsqueda de los StyleBooks que tienen una etiqueta donde `key=team` y `value=bizdata`:

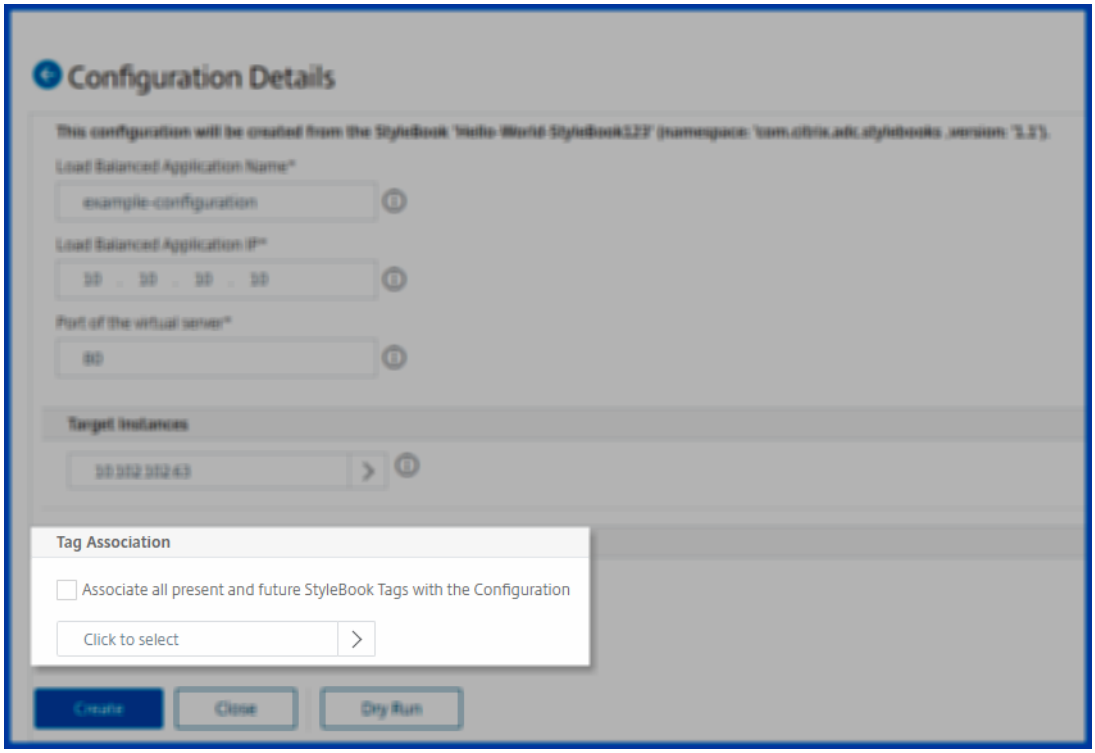
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Puede asociar las etiquetas StyleBook a su paquete de configuración. Por lo tanto, puede buscar en los paquetes de configuración mediante las propias etiquetas StyleBook.

Al crear un paquete de configuración, utilice una de las siguientes opciones en la sección **Asociación de etiquetas** :

- **Asociar todas las etiquetas de StyleBook presentes y futuras a la configuración**: Esta opción asocia todas las etiquetas StyleBook a un paquete de configuración. También se asegura de asociar las nuevas etiquetas que pueda agregar a los StyleBooks en el futuro.
- **Seleccionar etiquetas**: Esta opción muestra las etiquetas del StyleBook seleccionado. Puede seleccionar las etiquetas de StyleBook necesarias y asociarlas a un paquete de configuración.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Importar y sincronizar StyleBooks desde el repositorio de GitHub

January 30, 2024

Considere un caso en el que esté utilizando procesos de CI/CD para su desarrollo. O bien, un caso en el que está administrando todo el código fuente de la aplicación y los objetos de implementación en GitHub.

En el repositorio de GitHub, es posible que haya creado varios StyleBooks para implementar las configuraciones de Citrix ADC y administrar estos StyleBooks. Estos StyleBooks también son obligatorios en Citrix Applications and Delivery Management (ADM). Ahora puede importar directamente estos StyleBooks a Citrix ADM. No es necesario copiarlos manualmente de GitHub y, a continuación, cargarlos en Citrix ADM ni sincronizar manualmente los archivos en ADM y GitHub.

Ahora puede definir un repositorio en NetScaler ADM que represente un repositorio de GitHub. Proporciona la URL del repositorio de GitHub y tu nombre de usuario y contraseña (o token de API) creados en GitHub. Esto significa que solo los usuarios autorizados que tengan una cuenta válida en GitHub pueden importar y sincronizar StyleBooks.

Después de crear el repositorio, puede sincronizar NetScaler ADM con su repositorio de GitHub. Citrix ADM se conecta a GitHub e importa los StyleBooks que se encuentran en ese repositorio. A continuación, ADM valida los StyleBooks y los agrega a la lista de StyleBooks de Citrix ADM. Los StyleBooks no se agregan a NetScaler ADM si no se validan. Corrige los errores y envía las versiones actualizadas a tu repositorio de GitHub. Más adelante, puede intentar importarlos o sincronizarlos de nuevo en NetScaler ADM.

> **Nota**
>
> - Los archivos de StyleBooks se pueden importar y sincronizar desde cualquier rama de un repositorio de GitHub.
> - También puede importar y sincronizar los StyleBooks que tengan libros de estilo dependientes asociados a ellos.
> - La sincronización de StyleBooks desde un repositorio de GitHub debe iniciarse manualmente desde la GUI o la API de NetScaler ADM. Es decir, actualmente, la importación y sincronización de StyleBooks no ocurre automáticamente en función de la actividad de confirmación de GitHub.

## Añadir un repositorio e importar StyleBooks desde el repositorio de GitHub

Antes de comenzar, asegúrese de tener una cuenta válida en GitHub.

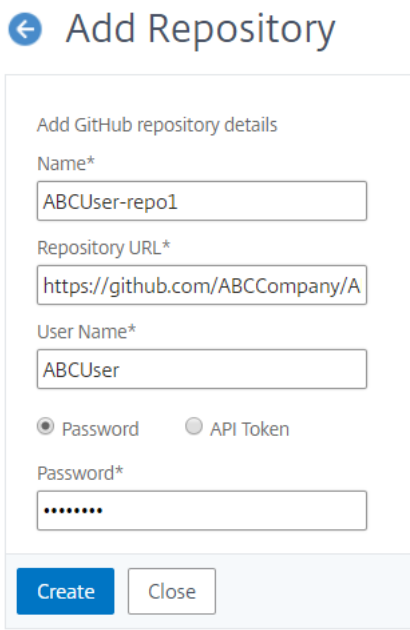
Puede importar archivos de StyleBook a ADM desde cualquier carpeta del repositorio de GitHub.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks** > **Repositorios** .
2. Haga clic en **Agregar**. En la ventana **Agregar Repositorio**, introduzca los siguientes parámetros:
   - **Nombre**. Escriba el nombre del repositorio. Este nombre puede ser el mismo que el nombre del repositorio en GitHub o uno diferente.
   - **URL del repositorio**. Escribe la URL del repositorio de GitHub.
   - **Nombre de usuario y contraseña**. Escriba el nombre de usuario y la contraseña con la que acceda a la cuenta de GitHub.

   > **Nota:**
   >
   > También puede proporcionar el token de la API en lugar de una contraseña. Los tokens de API se pueden usar en lugar de una contraseña para GitHub a través de HTTPS. Para obtener información sobre cómo crear tokens de API para su repositorio de GitHub, consulta la documentación de GitHub para crear tokens de acceso personales.

3. Haga clic en **Crear**.




   El repositorio se crea en NetScaler ADM.

4. **Para importar o sincronizar StyleBooks, seleccione el repositorio en la página**Repositorios**y haga clic en Sincronizar.**

Las otras acciones que puede utilizar aquí son:

- **Modificar**. Puede modificar la URL del repositorio, el nombre de usuario y la contraseña (o el token de API).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Eliminar**. Puede eliminar el repositorio junto con todos los StyleBooks presentes en Citrix ADM que se importaron anteriormente desde ese repositorio de GitHub.

  > **Nota**No
  >
  > puede eliminar un repositorio de NetScaler ADM si tiene StyleBooks que tengan Config-Packs asociados a ellos. En primer lugar, elimina todos los paquetes de configuración de estos StyleBooks. Más adelante, puede eliminar el repositorio de NetScaler ADM para limpiar los StyleBooks de ese repositorio.

- **Restablecer**. Puede eliminar todos los StyleBooks de Citrix ADM sincronizados de ese repositorio sin eliminar realmente la entrada del repositorio de Citrix ADM.
- **Lista de archivos**. Puede ver una lista de todos los StyleBooks presentes en NetScaler ADM que se originan en el repositorio de GitHub.

## Usar StyleBooks predeterminados

January 30, 2024

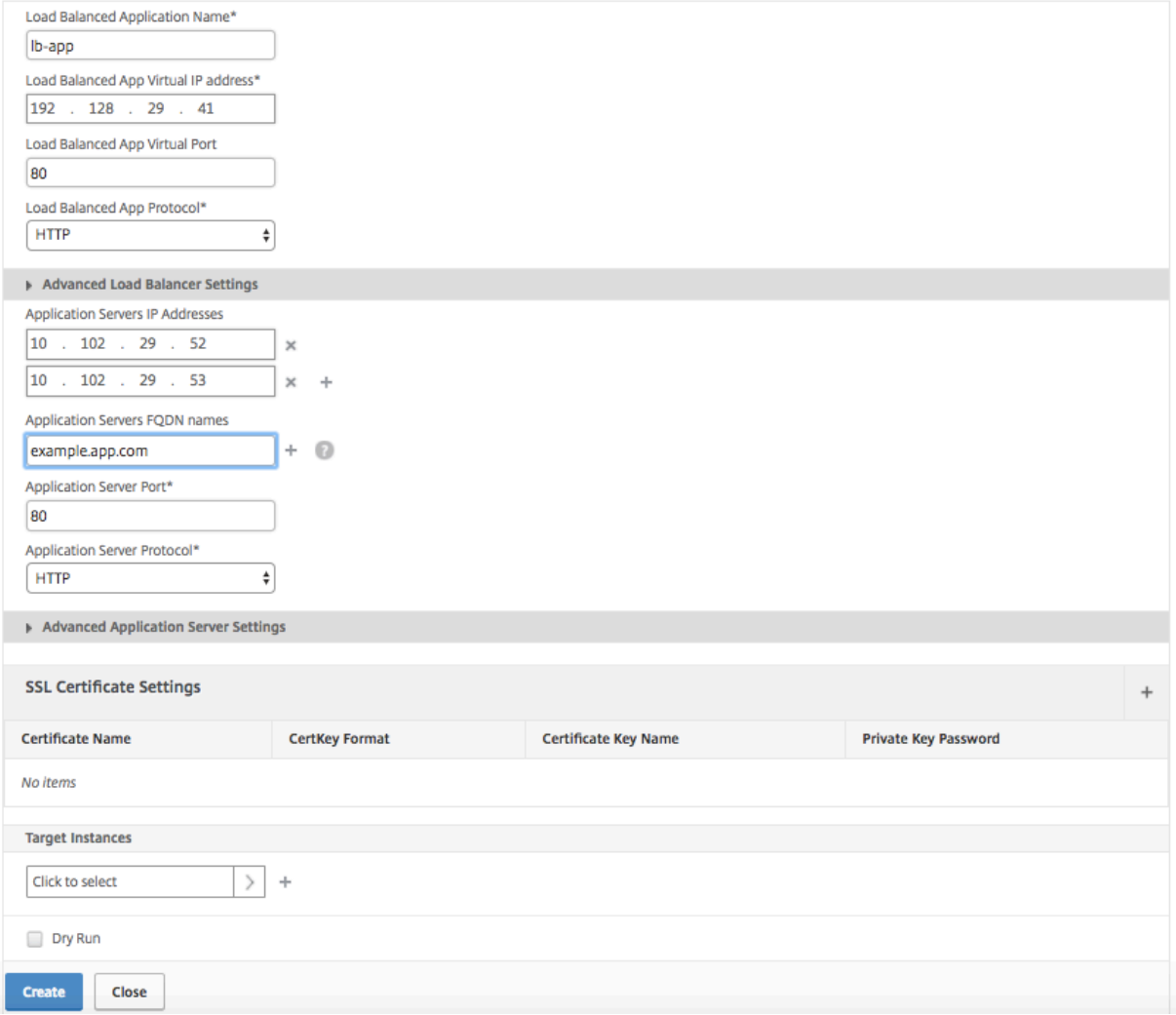
Se proporciona un conjunto de StyleBooks predeterminados con NetScaler Application Delivery Management (ADM). Cuando utiliza un StyleBook predeterminado, debe especificar valores para los parámetros en el StyleBook y seleccionar las direcciones IP de las instancias de NetScaler ADC en las que quiere ejecutar la configuración. Después de enviar la configuración, NetScaler ADM valida los valores de los parámetros que ha especificado, crea un gráfico de la configuración, se conecta a las instancias de NetScaler ADC y ejecuta la configuración en las instancias.

### Para crear una configuración a partir de un StyleBook predeterminado

1.Vaya a **Aplicaciones** > **Configuraciones > StyleBooks**. La página StyleBooks muestra todos los StyleBooks de NetScaler ADM. Esta lista incluye los StyleBooks predeterminados y personalizados. Puede escribir el nombre del StyleBook en el campo de búsqueda y presionar la tecla **Intro**. De lo contrario, puede desplazarse hacia abajo en la lista para encontrar el StyleBook.

2. Haga clic en **Crear configuración**. Especifique los valores necesarios para los parámetros.

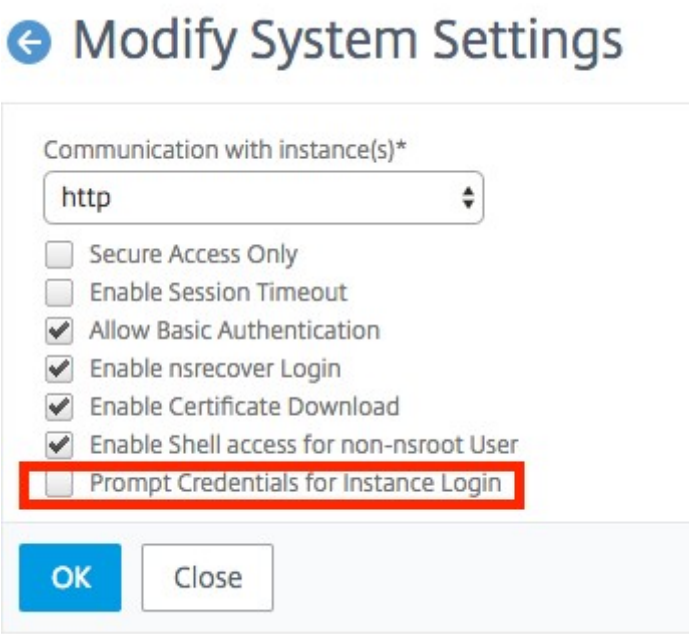
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. En **Instancias de destino**, haga clic en y seleccione la dirección IP de la instancia de NetScaler ADC en la que quiere ejecutar la configuración. Si quiere ejecutar esta configuración en varias instancias, haga clic en "+"para agregar más instancias.

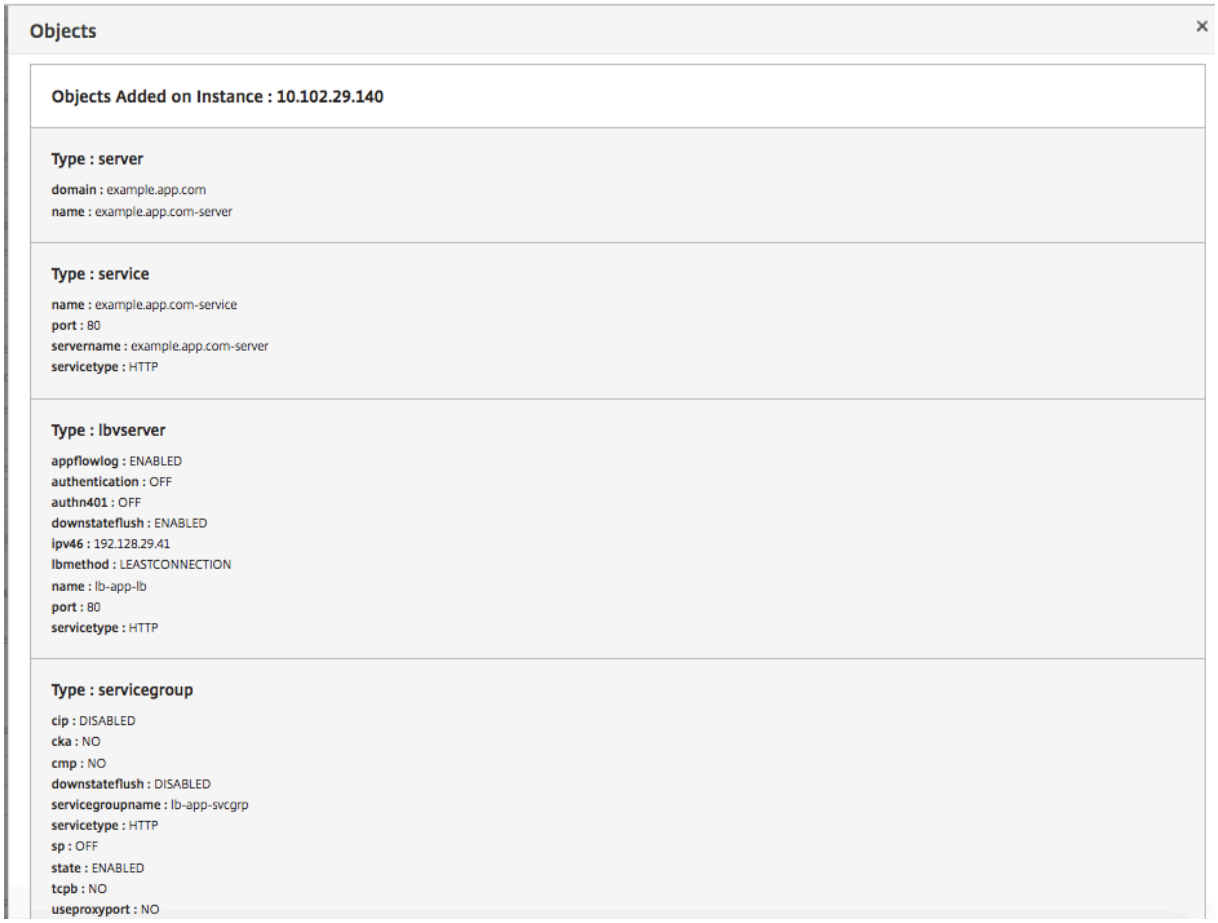
Si la opción Solicitar **credenciales para iniciar sesión en la instancia** está habilitada en **Citrix ADM** > **Sistema** > **Cambiar la configuración del**sistema**>** **Modificar** la configuración del sistema , se le solicitarán las credenciales de la instancia de Citrix ADC al ejecutar las configuraciones en las instancias de Citrix ADC seleccionadas. De lo contrario, NetScaler ADM utiliza las credenciales de instancia almacenadas en el perfil de instancia para iniciar sesión en la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Si quiere probar o validar la configuración antes de ejecutarla en la instancia de NetScaler ADC, seleccione **Simulacro** y, a continuación, haga clic en **Crear**. Si la configuración es válida, se muestran los objetos creados sobre la base de los valores proporcionados.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. Desmarque la casilla **Simulacro**y haga clic en **Crear** para crear la configuración y ejecutar la configuración en la instancia de NetScaler ADC. La configuración de StyleBook que ha creado aparece en la lista de configuraciones, como se muestra a continuación.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

Ahora puede examinar, actualizar o eliminar este paquete de configuración mediante NetScaler ADM.

## StyleBook de firewalls de aplicaciones web

January 30, 2024

Citrix Web App Firewall es un firewall de aplicaciones web (WAF) que protege las aplicaciones web y los sitios de ataques conocidos y desconocidos, incluidas todas las amenazas de la capa de aplicaciones

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

y de día cero.

NetScaler ADM ahora proporciona un StyleBook predeterminado con el que puede crear más cómodamente una configuración de firewall de aplicaciones en las instancias de NetScaler ADC.

### Implementar configuraciones de firewall de aplicaciones

La siguiente tarea le ayuda a implementar una configuración de equilibrio de carga junto con el firewall de aplicaciones y la directiva de reputación IP en instancias NetScaler ADC en su red empresarial.

**Para crear una configuración LB con la configuración del firewall de la aplicación:**

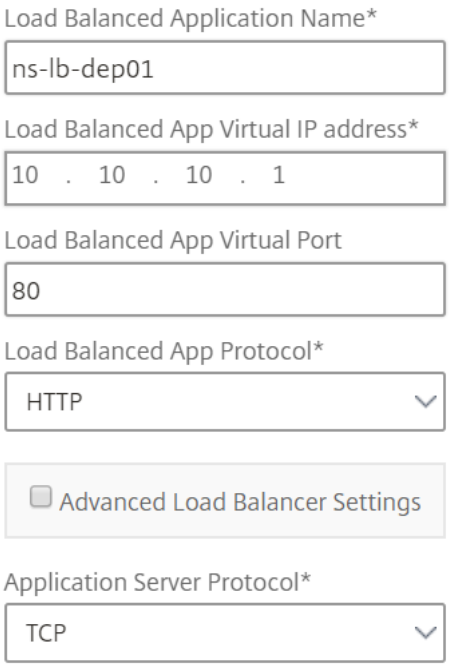
1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**. La página StyleBooks muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplácese hacia abajo y busque HTTP/SSL Load Balancing StyleBook con la directiva de firewall de aplicaciones y la directiva de reputación IP. También puede buscar el StyleBook escribiendo el nombre como `lb-appfw`. Haga clic en **Crear configuración**.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

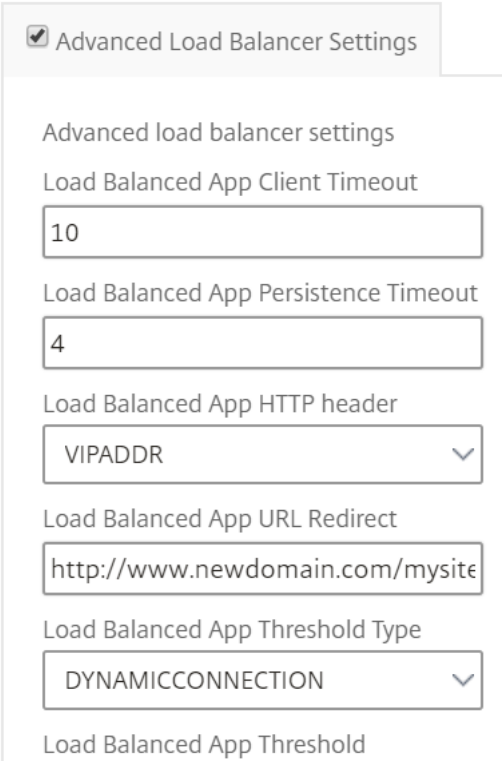
2. Introduzca valores para los siguientes parámetros:

   - **Nombre de aplicación equilibrada de carga**. Nombre de la configuración de equilibrio de carga con el firewall de aplicaciones que se implementará en la red.
   - **Cargar la dirección IP virtual de la aplicación equilibrada**. Dirección IP virtual en la que la instancia de NetScaler ADC recibe las solicitudes de los clientes.
   - **Puerto virtual de aplicación con equilibrio de carga**. El puerto TCP que utilizarán los usuarios para acceder a la aplicación con carga equilibrada.
   - **Protocolo de aplicación con equilibrio de carga**. Seleccione el protocolo de interfaz de usuario de la lista.
   - **Protocolo de servidor de aplicaciones**. Seleccione el protocolo del servidor de aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

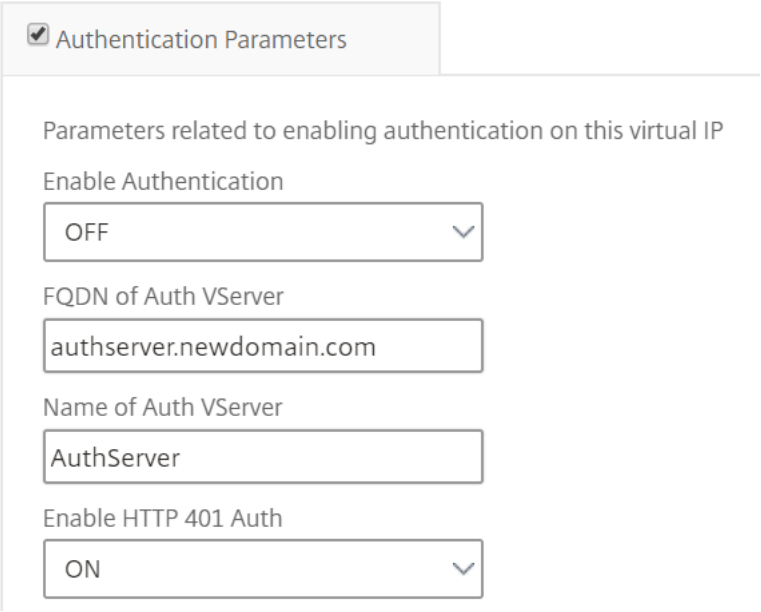



3. Como opción, puede habilitar y configurar la Configuración **avanzada del equilibrador de carga**.

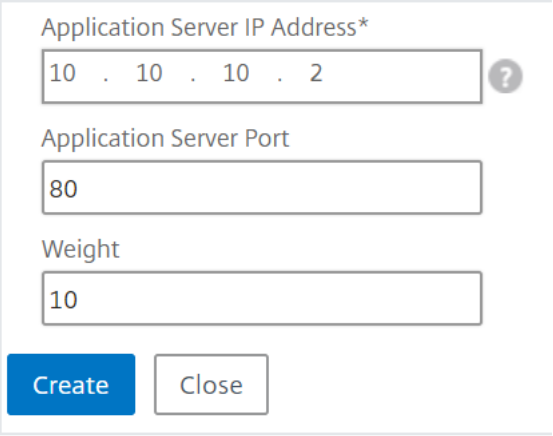



4. Opcionalmente, también puede configurar un servidor de autenticación para autenticar el tráfico para el servidor virtual de equilibrio de carga.

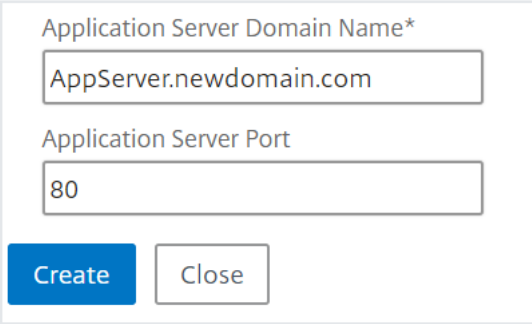
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Haga clic en “+”en la sección IPs y puertos del servidor para crear servidores de aplicaciones y los puertos en los que se puede acceder.

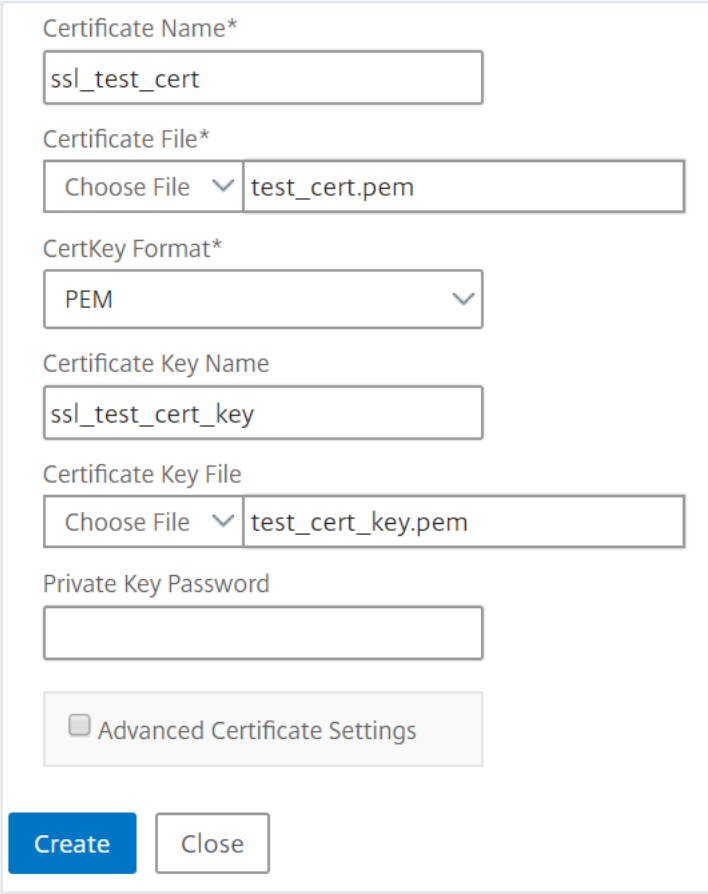



6. También puede crear nombres FQDN para servidores de aplicaciones.

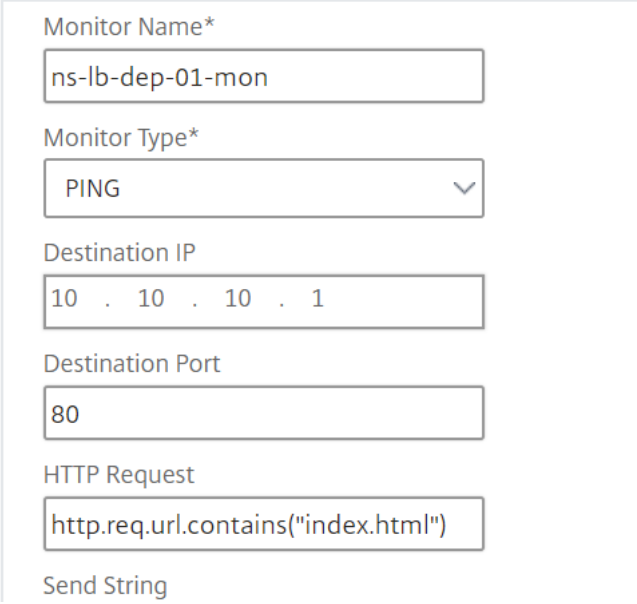



7. También puede especificar los detalles del certificado SSL.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




8. También puede crear monitores en la instancia de NetScaler ADC de destino.

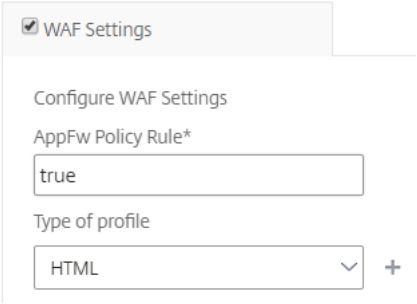



9. Para configurar un firewall de aplicaciones en el servidor virtual, habilite Configuración WAF.

   Asegúrese de que la regla de directiva del firewall de aplicaciones es verdadera si quiere aplicar

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

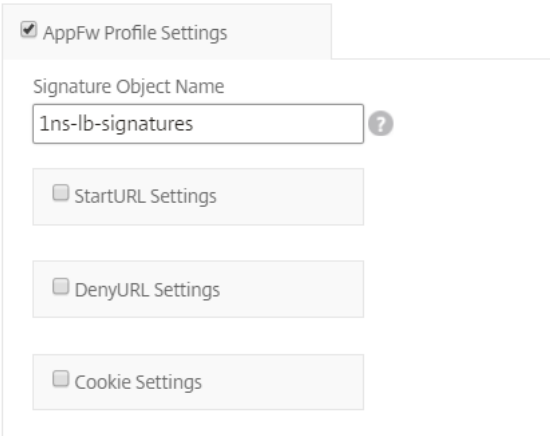
la configuración del firewall de aplicaciones a todo el tráfico de esa dirección VIP. De lo contrario, especifique la regla de directiva NetScaler ADC para seleccionar un subconjunto de solicitudes al que aplicar la configuración del firewall de aplicaciones. A continuación, seleccione el tipo de perfil que debe aplicarse: HTML o XML.




10. Si lo quiere, puede configurar las opciones detalladas del perfil del firewall de aplicaciones activando la casilla de verificación Configuración del perfil del firewall de la aplicación.
11. Opcionalmente, si quiere configurar firmas de firewall de aplicaciones, introduzca el nombre del objeto de firma que se crea en la instancia de NetScaler ADC en la que se va a implementar el servidor virtual.

    > **Nota**
    >
    > No se puede crear un objeto de firma mediante este StyleBook.

12. A continuación, también puede configurar cualquier otra configuración de perfil de firewall de aplicaciones como, por ejemplo, configuración de StartURL, configuración de DenyURL y otros.




Para obtener más información sobre el firewall de aplicaciones y la configuración de configuración, vea Firewall de aplicaciones.

13. En la sección **Instancias de destino**, seleccione la instancia de NetScaler ADC en la que quiere implementar el servidor virtual de equilibrio de carga con el firewall de la aplicación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**También
>
> puede hacer clic en el icono de actualización para agregar instancias de NetScaler ADC detectadas recientemente en NetScaler ADM a la lista de instancias disponibles en esta ventana.

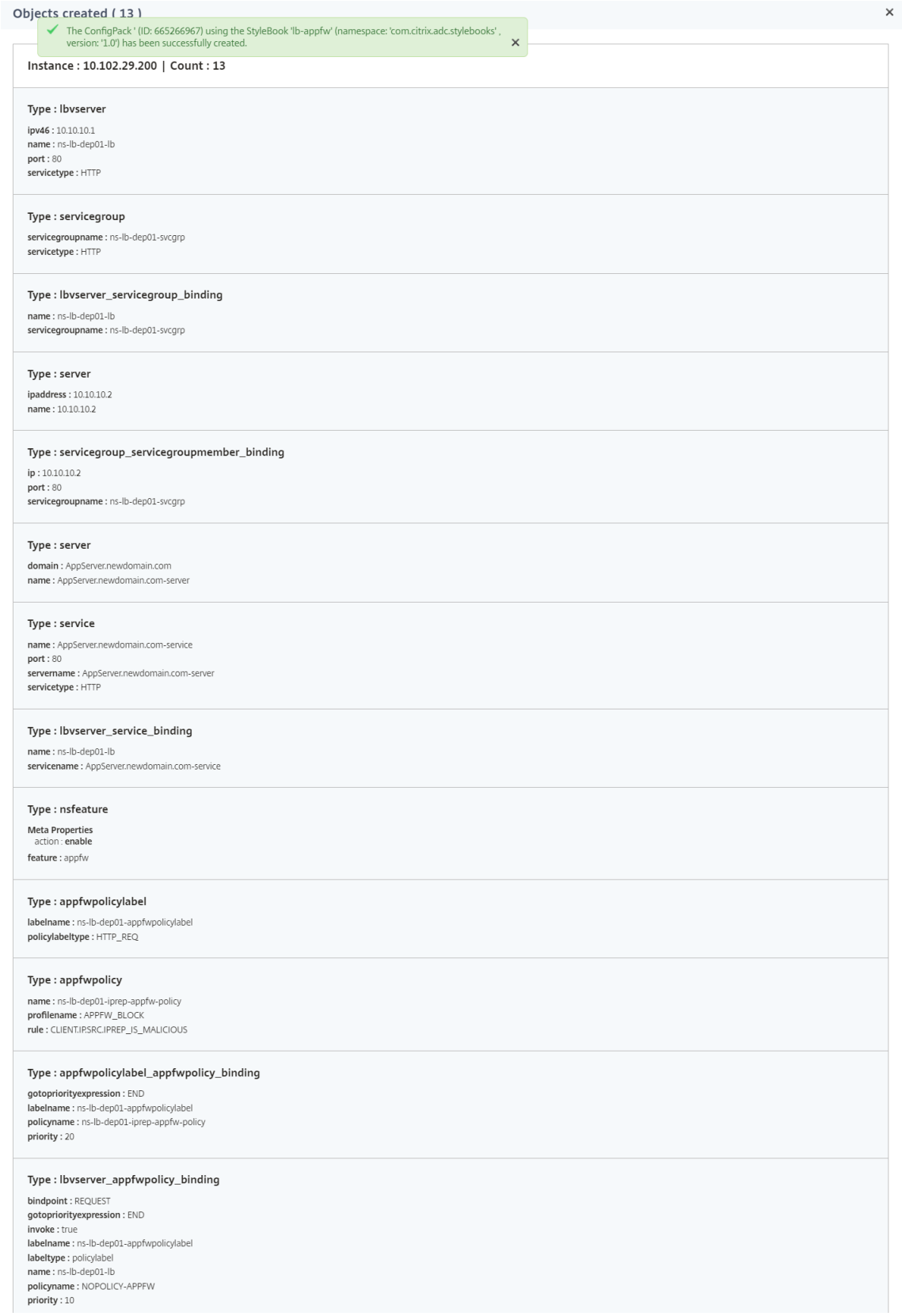
14. También puede habilitar la **verificación de reputación IP** para identificar la dirección IP que envía las solicitudes no deseadas. Puede utilizar la lista de reputación IP para rechazar de forma preventiva las solicitudes que provienen de la IP con mala reputación.
15. Haga clic **en**Crear para crear la configuración en las instancias de Citrix ADC seleccionadas.

> **Sugerencia**
>
> Citrix recomienda seleccionar Ejecución en seco para comprobar los objetos de configuración que se deben crear en la instancia de destino antes de ejecutar la configuración real en la instancia.

Cuando la configuración se crea correctamente, StyleBook crea el servidor virtual de equilibrio de carga requerido, el servidor de aplicaciones, los servicios, los grupos de servicios, las etiquetas de firewall de aplicaciones, las directivas de firewall de aplicaciones y los vincula al servidor virtual de equilibrio de carga.

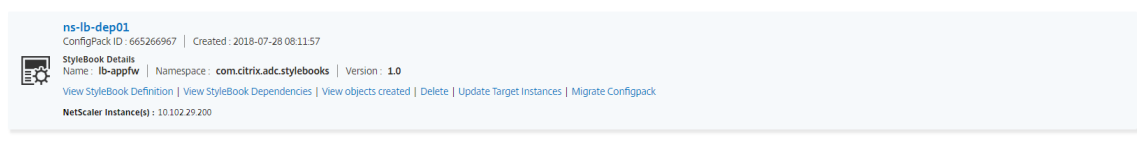
La siguiente ilustración muestra los objetos creados en cada servidor:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




16. Para ver el ConfigPack creado en NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




# Crear perfiles WAF y BOT con StyleBook

January 30, 2024

Cuando puede seleccionar una directiva para un recurso API en **API Gateway**, permite definir los criterios de selección de tráfico para autenticar una solicitud de API. Además, le permite configurar las directivas de seguridad de la API para el tráfico de la API. Para obtener más información, consulte Administrar puerta de enlace de API.

Puede configurar directivas WAF y BOT en un recurso API. Antes de configurar una directiva, asegúrese de crear su perfil en NetScaler Application Delivery Management (ADM). Utilice los siguientes StyleBooks predeterminados para crear un perfil:

- API WAF Detection StyleBook
- API BOT Detection StyleBook

## Crear un perfil WAF con StyleBook

Realice lo siguiente para crear un perfil WAF:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**. Busque el StyleBook escribiendo el nombre como `api-waf-profile`. Haga clic en **Crear configuración**.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

2. Especifique los valores para los siguientes parámetros:

   - **API WAF nombre de perfil**: un nombre para identificar un perfil WAF.
   - **Tipo de aplicación**: agregue tipos de aplicación al perfil. El perfil WAF admite tipos de aplicaciones JSON y XML.

3. Opcional, habilite **Configuración de seguridad** para especificar comprobaciones de protección HTTP, JSON o XML. También puede especificar una dirección URL de error para Citrix Web App Firewall. Para obtener más información, consulte Creación de un perfil de Web App Firewall.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. Seleccione la instancia o grupo de instancias de NetScaler ADC de destino en el que quiere implementar esta configuración.
5. Haga clic en **Crear**.

Para configurar una directiva WAF, consulte Agregar directivas a una implementación de API.

### Crear un perfil BOT con StyleBook

Realice lo siguiente para crear un perfil BOT:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**. Busque el StyleBook escribiendo el nombre como `api-bot-profile`. Haga clic en **Crear configuración**.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
2. En **Nombre de perfil BOT**, especifique un nombre para identificar un perfil BOT.
3. Opcional, habilite las siguientes opciones según sus requisitos:
   - **Habilitar comprobación de reputación IP**: esta opción identifica la dirección IP que envía solicitudes no deseadas. Puede utilizar la lista de reputación IP para rechazar de forma preventiva las solicitudes que provienen de la IP con mala reputación.
   - **Habilitar firmas BOT**: especifique el nombre de la firma BOT. Bloquea las solicitudes de la firma especificada.
   - **Lista de permitidos**: especifique dirección IPv4 o subred (CIDR). Esta opción permite que el perfil BOT omita las solicitudes de la dirección IPv4 o subred especificada.
   - **Denegar lista**: especifique la dirección IPv4 o subred (CIDR). Esta opción permite que el perfil BOT bloquee solicitudes desde la dirección IPv4 o subred especificada.
4. Seleccione la instancia o grupo de instancias de NetScaler ADC de destino en el que quiere implementar esta configuración.
5. Haga clic en **Crear**.

Para configurar una directiva de BOT, consulte Agregar directivas a una implementación de API.

## Ocultar todos los StyleBooks predeterminados

January 30, 2024

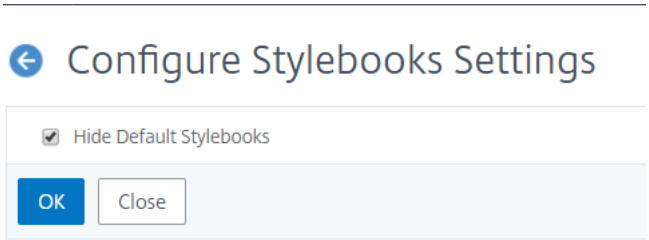
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Citrix ADM muestra todos los StyleBooks presentes en el sistema de carpetas Citrix ADM. La lista de StyleBooks incluye StyleBooks predeterminados y personalizados que pueden ser tanto privados como públicos. Como administrador, es posible que quiera ocultar todos los StyleBooks predeterminados. Puede permitir que sus usuarios vean y accedan solo a los StyleBooks personalizados creados por usted o por los usuarios.

NetScaler ADM le permite mostrar sus StyleBooks personalizados y ocultar todos los StyleBooks predeterminados que se envían con NetScaler ADM. Se proporciona una nueva opción de interfaz gráfica de usuario donde puede ocultar todos los StyleBooks predeterminados.

**Para ocultar todos los StyleBooks predeterminados**:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones > Configuración**.
2. La página de **configuración** muestra información sobre si los StyleBooks predeterminados están visibles para los usuarios o no.
3. Para ocultar los StyleBooks predeterminados, haga clic en el icono de edición situado en la parte superior derecha.
4. En la página **Configurar los ajustes de StyleBook**, seleccione la opción **Ocultar libros de estilos predeterminados**.
5. Haga clic en **Aceptar**.




Los usuarios seguirán viendo la página **Configurar los ajustes de StyleBook** si no ha optado por ocultarla mediante la función RBAC. Es posible que los usuarios sigan teniendo la opción de mostrar los StyleBooks predeterminados.

Para ocultar la página **Configurar ajustes de StyleBook**, debe crear una directiva y asignarla a los usuarios que no deberían ver los StyleBooks predeterminados.

**Para crear una directiva RBAC**:

1. En NetScaler ADM, vaya a **Cuenta** > **Administración de usuarios** > **Directivas de acceso**.
2. Haga clic en **Add** para crear una directiva.
3. Introduzca el nombre de la directiva.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En la sección **Permisos**, asegúrese de que no esté seleccionada la opción **Todas** > **Aplicaciones** > **Configuración> Configuración**y haga clic en**Aceptar**.

Después de crear directivas, debe crear roles, enlazar cada rol a una o varias directivas y asignar roles a grupos de usuarios. Para obtener más información sobre cómo asociar directivas a los usuarios, consulte Configuración del control de acceso basado en funciones.

## Migrar la configuración de aplicaciones Citrix ADC con StyleBooks Configuration Builder

January 30, 2024

> **Nota**
>
> Esta función se encuentra en versión preliminar técnica.

El generador de configuración de StyleBooks se utiliza para crear un StyleBook de configuración de aplicaciones a partir de una configuración de Citrix ADC existente. Esta función también automatiza la migración de configuración de aplicaciones de una instancia de Citrix ADC a otra instancia.

Con Configuration Builder, puede simplificar el requisito de crear un StyleBook personalizado. Esta función le permite crear un StyleBook sin tener un conocimiento profundo de la gramática y las construcciones de StyleBooks. De lo contrario, el conocimiento de la gramática y construcciones de StyleBooks es necesario para crear un StyleBook.

El Generador de configuraciones también crea un paquete de configuración que refleja la misma configuración de ADC en una nueva instancia de ADC. Con este ConfigPack, la configuración inicial de ADC de una instancia de ADC se puede duplicar en otra instancia de ADC. El origen de configuración inicial puede ser uno de los siguientes:

- **Una instancia de Citrix ADC:** Especifique la instancia en la que está alojada la configuración de la aplicación que quiere duplicar.

  El Generador de configuraciones convierte la configuración del ADC en un StyleBook y un ConfigPack incluso si no se especifica la instancia de destino. Más adelante, puede usar este paquete de configuración para migrar la configuración de ADC a otras instancias de ADC.

- **Un conjunto de comandos CLI:** Pegue la configuración desde `ns.conf` o `Application config`.

El Generador de configuración identifica la lista de distintas aplicaciones integradas en la configuración de origen. Al seleccionar la configuración de la aplicación que le interese, el Generador de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

configuraciones extrae el conjunto de comandos de la CLI para la aplicación seleccionada. Estos comandos de CLI se extraen de la configuración de origen. También identifica los atributos de implementación y configuración que podrían requerir su entrada.

- **Atributos de implementación**: Puede ver y modificar la dirección IP y el puerto de los servidores virtuales, los servicios y los miembros del grupo de servicios desde la configuración original.
- **Atributos de configuración**: Estos atributos pueden ser contraseñas o certificados especificados en la configuración de origen.

Después de especificar la información necesaria, comience a migrar o duplicar la configuración de la aplicación en una instancia ADC de destino.

Tras completar la creación y migración de la aplicación, se crea un ConfigPack en Citrix ADM junto con su StyleBook correspondiente. Este ConfigPack representa la configuración de la aplicación en la instancia ADC de destino. Para ver el ConfigPack creado, vaya a **Aplicaciones** > **StyleBooks**> **Configuraciones**.

### Funciones admitidas de Citrix ADC

El generador de configuración de StyleBook reconoce y admite las siguientes funciones de Citrix ADC en la configuración de origen:

- Conmutación de contenido
- Equilibrio de carga
- Supervisión
- Descarga de SSL
- Limitación de velocidad
- Reescritura
- Responder
- Firewall de aplicaciones web (WAF)

### Cree un StyleBook para migrar la configuración de la aplicación Citrix ADC

El siguiente procedimiento consiste en crear un StyleBook que migre la migración de la aplicación Citrix ADC en Citrix ADM:

1. Vaya a **Aplicaciones** > **StyleBooks** > **Configuraciones**.
2. Haga clic en **Migrar configuración ADC**.
3. Haga clic en **Get Started**.

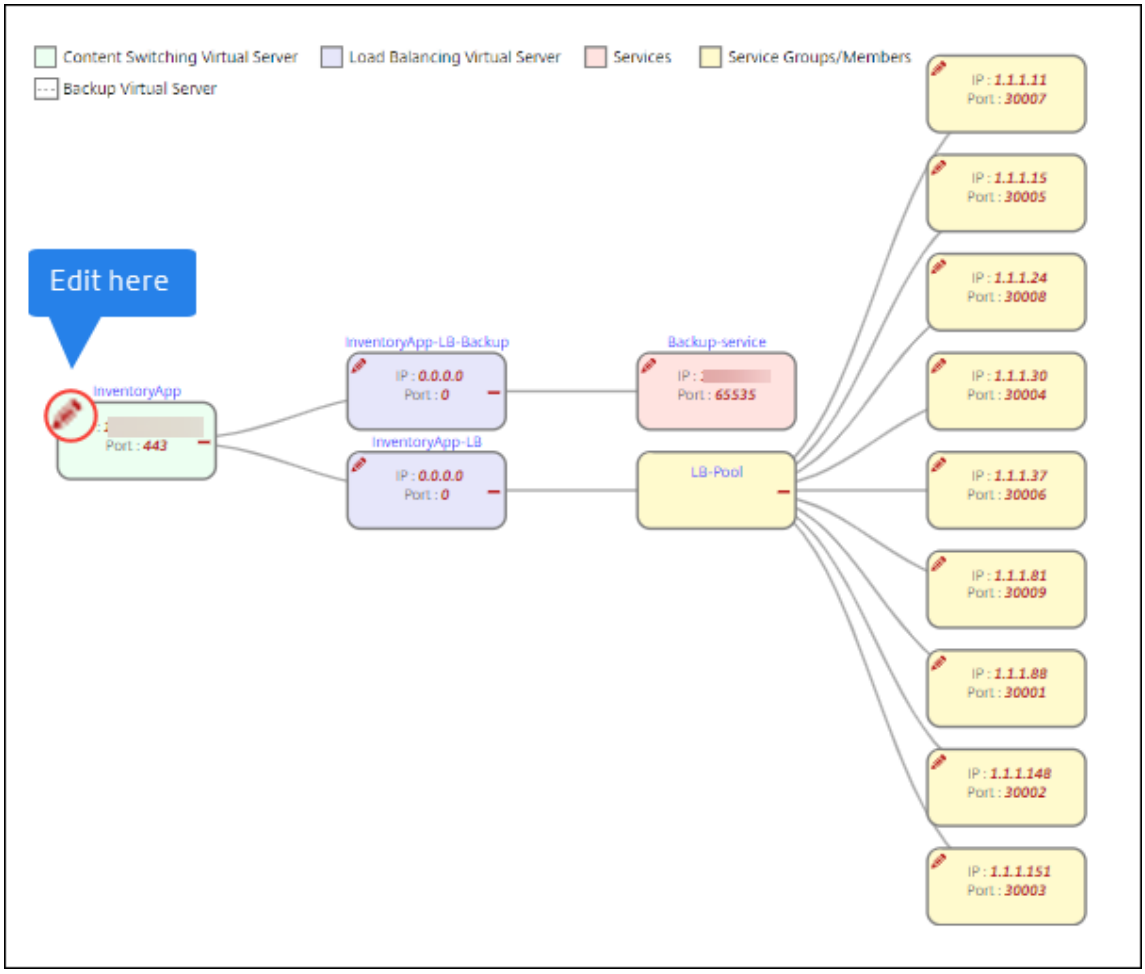
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En **Especificar configuración**, seleccione la fuente de configuración:
   - **Importar desde un ADC**: esta opción descubre las aplicaciones activas en la instancia de ADC seleccionada.
   - **Importación mediante comandos de CLI**: esta opción analiza los comandos de la CLI y extrae las aplicaciones de los comandos de la CLI.
5. Especifique la **instancia de ADC de origen** desde la que quiere migrar o duplicar la configuración de la aplicación.
6. Especifique la **instancia de ADC de destino** a la que quiere migrar o duplicar la configuración de la aplicación.
7. En **Definir aplicación**,
   a) En **Nombre de aplicación**, especifique el nombre de la aplicación.
   b) Seleccione los servidores virtuales que quiere migrar.
   c) Haga clic en **Siguiente**.
8. En **Comandos de CLI equivalentes**, revise los comandos y haga clic en **Siguiente**.

   Estos comandos son específicos de la configuración de la aplicación seleccionada.
9. En **Atributos de implementación**, puede ver y modificar la dirección IP y el puerto de los servidores virtuales, los servicios y los miembros del grupo de servicios.

   Para modificar la dirección IP y el puerto, haga clic en el icono de edición del servidor virtual, servicio o miembro del grupo de servicios en el diagrama de flujo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Esta ficha solo aparece en los siguientes casos:

- Las instancias de origen y destino son diferentes.
- Importe configuraciones mediante comandos de CLI.

10. En **Atributos de configuración**, especifique los detalles necesarios y haga clic en **Siguiente**.

    Esta ficha enumera los secretos, como claves para descifrar contraseñas y certificados.

    > **Nota**
    >
    > Antes de iniciar la migración, las configuraciones omitidas o no compatibles se muestran en cualquiera de las siguientes fichas:
    >
    > **Configuraciones no compatibles**
    >
    > **Configuraciones globales no compatibles**
    >
    > Para migrar estas configuraciones correctamente, debe aplicar las configuraciones omitidas o no compatibles por separado en la instancia de destino. Luego, haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

11. En **Migrate**, especifique los detalles de StyleBook requeridos. Haga clic en **Migrate**.

### Limitaciones

- Las expresiones nombradas y `responderhtmlpages` mencionadas en la instancia de origen no están identificadas. Asegúrese de configurar las expresiones con nombre y `responderhtmlpages` en la instancia de destino antes de la migración.
- Si la fuente tiene una configuración para `servicegroup` y la vinculación de monitores de la siguiente manera:

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  Aparece el siguiente error:

  ```
  CLI Command conversion failed: 100 - No such command [{
   "errorcode": 1090, "message": "No such argument [XXX]", "
      severity": "ERROR"  }
  ]
  ```

  Este error se produce porque Citrix ADC guarda el enlace entre el grupo de servicios y el monitor en un formato no válido. Este problema se ha corregido desde la compilación de Citrix ADC 12.1.52.15.

## StyleBooks de aplicaciones empresariales

January 30, 2024

NetScaler ADM proporciona los StyleBooks que le ayudan a implementar una configuración de ADC para aplicaciones empresariales específicas. Para obtener más información sobre estos StyleBooks, consulte los siguientes temas:

- StyleBook del SSO de Google Apps
- StyleBook del SSO de Office 365
- StyleBook de Microsoft Skype Empresarial
- StyleBook de Microsoft Exchange
- StyleBook de Microsoft SharePoint
- StyleBook proxy de Microsoft ADFS
- StyleBook del negocio electrónico de Oracle
- StyleBook de firewalls de aplicaciones web

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Crear perfiles WAF y BOT con StyleBook

## StyleBook del SSO de Google Apps

January 30, 2024

Google Apps es un conjunto de herramientas, software y productos de computación en la nube, productividad y colaboración desarrollados por Google. El inicio de sesión único (SSO) permite a los usuarios acceder a todas sus aplicaciones empresariales en la nube, incluidos los administradores que inician sesión en la consola de administración, iniciando sesión una vez para todos los servicios mediante sus credenciales de empresa.

El SSO Google Apps StyleBook de NetScaler ADM le permite habilitar el SSO para Google Apps a través de instancias de NetScaler ADC. StyleBook configura la instancia de NetScaler ADC como un proveedor de identidad SAML para autenticar a los usuarios para que accedan a Google Apps.

Al habilitar el SSO para las aplicaciones de Google en una instancia de NetScaler ADC mediante este StyleBook, se obtienen los siguientes pasos:

1. Configuración del servidor virtual de autenticación
2. Configuración de una directiva y un perfil de IdP SAML
3. Vinculación de la directiva y el perfil al servidor virtual de autenticación
4. Configuración de un servidor y una directiva de autenticación LDAP en la instancia
5. Enlazar el servidor y la directiva de autenticación LDAP a su servidor virtual de autenticación configurado en la instancia

**Detalles de configuración**:

En la siguiente tabla se enumeran las versiones de software mínimas necesarias para que esta integración funcione correctamente. El proceso de integración también admite las versiones superiores de la misma.

| Producto | Versión mínima requerida |
| --- | --- |
| Citrix ADC | Versión 11.0, Licencia Avanzada/Premium |

En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas o internas adecuadas para enrutar las solicitudes de autenticación a una dirección IP supervisada por NetScaler ADC.

**Implementación de configuraciones de StyleBook de aplicaciones de Google SSO**:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La siguiente tarea le ayudará a implementar el SSO de Google Apps StyleBook de Microsoft en su red empresarial.

### Para implementar aplicaciones de SSO Google StyleBook

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** >**StyleBooks**. La página StyleBooks muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplázate hacia abajo y busca **SSO Google Apps StyleBook**. Haga clic en **Crear configuración**.
2. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
3. Introduzca valores para los siguientes parámetros:
   a) **Nombre de la aplicación**. Nombre de la configuración de SSO de Google Apps que se implementará en la red.
   b) **Autenticación Dirección IP virtual**. Dirección IP virtual utilizada por el servidor virtual de autenticación, autorización y auditoría al que está vinculada la directiva de IdP SAML de Google Apps.
   c) **Expresión de regla SAML**. De forma predeterminada, se utiliza la siguiente expresión de NetScaler ADC Policy (PI): HTTP.REQ.HEADER("Referrer").CONTAINS("google"). Actualice este campo con otra expresión si su requisito es diferente. Esta expresión de directiva coincide con el tráfico al que se aplica esta configuración de SSO SAML y se asegura de que el encabezado Referrer proviene de un dominio de Google.
4. La sección Configuración de IdP de SAML le permite configurar la instancia de NetScaler ADC como proveedor de identidades SAML creando el perfil y la directiva de IdP SAML que utiliza el servidor virtual de autenticación, autorización y auditoría creado en el paso 3.
   a) **Nombre del emisor SAML**. En este campo, introduzca el FQDN público de su servidor virtual de autenticación. Ejemplo:`https://<Citrix ADC Auth VIP>/saml/login`
   b) **ID de proveedor de servicios (SP) SAML**. (opcional) El proveedor de identidades NetScaler ADC acepta solicitudes de autenticación SAML de un nombre de emisor que coincida con este ID.
   c) **URL de Assertion Consumer Service** Introduzca la URL del proveedor de servicios a la que el proveedor de identidades de NetScaler ADC debe enviar las afirmaciones SAML después de una autenticación de usuario exitosa. La URL del servicio al consumidor de afirmación se puede iniciar en el sitio del servidor del proveedor de identidad o en el sitio del proveedor de servicios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

d) Hay otros campos opcionales que puede introducir en esta sección. Por ejemplo, puede configurar las siguientes opciones:

   i. Perfil de enlace SAML (el perfil predeterminado es “POST”).

   ii. Algoritmo de firma para verificar/firmar las solicitudes/respuestas de SAML (el predeterminado es “RSA-SHA1”).

   iii. Método para digerir el hash de las solicitudes/respuestas de SAML (el predeterminado es “SHA-1”).

   iv. Algoritmo de cifrado (el predeterminado es AES256) y otros ajustes.

> **Nota**
>
> Citrix recomienda conservar la configuración predeterminada, ya que se ha comprobado que estos ajustes son compatibles con Google Apps.

e) También puede activar la casilla de verificación Atributos de usuario para introducir los detalles del usuario, como:

   i. Nombre del atributo de usuario

   ii. Expresión de API de NetScaler ADC que se evalúa para extraer el valor del atributo

   iii. Nombre fácil de usar del atributo

   iv. Seleccione el formato del atributo de usuario.

   Estos valores se incluyen en la afirmación SAML emitida. Puede incluir hasta cinco conjuntos de atributos de usuario en una afirmación emitida por NetScaler ADC con este StyleBook.

5. En la sección Configuración de LDAP, introduce los siguientes detalles para autenticar a los usuarios de Google Apps. Para que los usuarios del dominio puedan iniciar sesión en la instancia de NetScaler ADC mediante sus direcciones de correo electrónico corporativas, debe configurar lo siguiente:

   a) **Base LDAP (Active Directory)**. Escriba el nombre de dominio base para el dominio en el que residen las cuentas de usuario en Active Directory (AD) para el que quiere permitir la autenticación. Por ejemplo `dc=netscaler,dc=com`

   b) **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga derechos para examinar el árbol de AD. Por ejemplo,`cn=Manager,dc=netscaler,dc=com`

   c) **Contraseña de DN de enlace LDAP (Active Directory)**. Introduzca la contraseña de la cuenta de dominio para la autenticación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

d) Algunos otros campos que debe introducir en esta sección son los siguientes:

i. Dirección IP del servidor LDAP a la que se conecta NetScaler ADC para autenticar usuarios

ii. Nombre FQDN del servidor LDAP

> **Nota**
>
> Debe especificar al menos una de las dos opciones anteriores: la dirección IP del servidor LDAP o el nombre de FQDN.

iii. Puerto de servidor LDAP al que NetScaler ADC se conecta para autenticar usuarios (el valor predeterminado es 389).

iv. Nombre de host LDAP. Esto se utiliza para validar el certificado LDAP si la validación está activada (de forma predeterminada, está desactivada).

v. Atributo de nombre de inicio de sesión LDAP. El atributo predeterminado utilizado para extraer nombres de inicio de sesión es “samAccountName. “

vi. Otros parámetros opcionales de LDAP diversos

6. En la sección Certificado SSL SAML IdP, puede especificar los detalles del certificado SSL:

a) **Nombre del certificado**. Introduzca el nombre del certificado SSL.

b) **Archivo**de certificado . Elija el archivo de certificado SSL en el directorio de su sistema local o en NetScaler ADM.

c) **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones .pem y .der.

d) **Nombre de clave de certificado**. Introduzca el nombre de la clave privada del certificado.

e) **Archivo de clave de certificado**. Seleccione el archivo que contiene la clave privada del certificado de su sistema local o de NetScaler ADM.

f) **Contraseña de clave privada**. Si el archivo de clave privada está protegido por una contraseña, introdúzcala en este campo.

g) También puede activar la casilla Configuración avanzada de certificados para introducir detalles como el período de notificación de caducidad del certificado o habilitar o inhabilitar el monitor de caducidad del certificado.

7. Si lo quiere, puede seleccionar el certificado de CA SSL de IdP si el certificado de IdP de SAML introducido anteriormente requiere la instalación de un certificado público de CA en NetScaler ADC. Asegúrese de seleccionar “Es un certificado de CA”en la configuración avanzada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. Si lo quiere, puede seleccionar el certificado SSL SP de SAML para especificar el certificado SSL de Google (clave pública) que se utiliza para validar las solicitudes de autenticación de Google Apps (SAML SP).
9. Haga clic en Instancias de **destino y seleccione las instancias** de NetScaler ADC en las que quiere implementar esta configuración de SSO de Google Apps. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.

   > **Nota**
   >
   > También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

   Además,

   > **Sugerencia**
   >
   > Citrix recomienda que, antes de**ejecutar la configuración real, seleccione Ejecución en seco**para confirmar visualmente los objetos de configuración creados en las instancias NetScaler ADC de destino por el StyleBook.

## StyleBook del SSO de Office 365

January 30, 2024

Microsoft™ Office 365 es un conjunto de aplicaciones de colaboración y productividad basadas en la nube proporcionadas por Microsoft sobre una base de suscripción. Incluye las populares aplicaciones basadas en servidor de Microsoft, como Exchange, SharePoint, Office y Skype Empresarial. El inicio de sesión único (SSO) permite a los usuarios acceder a todas sus aplicaciones empresariales en la nube:

- Incluye los administradores que inician sesión en la consola de administración
- Inicio de sesión único para todos los servicios de Microsoft Office 365 con sus credenciales empresariales.

El SSO Office 365 StyleBook le permite habilitar el SSO para Microsoft Office 365 a través de instancias de NetScaler ADC. Ahora puede configurar la autenticación SAML con NetScaler ADC como proveedor de identidades (IdP) de SAML y Microsoft Office 365 como proveedor de servicios de SAML.

Para habilitar el SSO para Microsoft Office 365 en una instancia de NetScaler ADC mediante este StyleBook, se deben seguir los siguientes pasos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Configuración del servidor virtual de autenticación
2. Configuración de una directiva y un perfil de IDP de SAML
3. Vinculación de la directiva y el perfil al servidor virtual de autenticación
4. Configuración de un servidor y una directiva de autenticación LDAP en la instancia
5. Enlazar el servidor y la directiva de autenticación LDAP a su servidor virtual de autenticación configurado en la instancia.

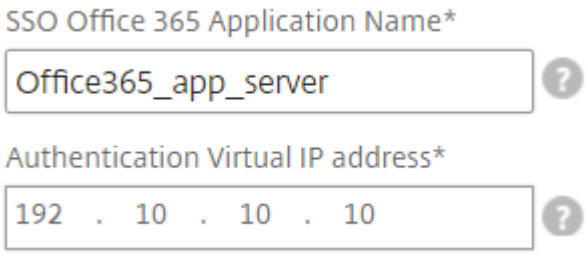
La tabla muestra las versiones de software mínimas necesarias para que esta integración funcione correctamente. El proceso de integración también debería funcionar con versiones superiores del mismo.
|Producto|Versión mínima requerida|
|———|————————|
|Citrix ADC|11.0, Licencia avanzada/premium|

En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas e internas adecuadas. Estas entradas son esenciales para enrutar las solicitudes de autenticación a una dirección IP supervisada por NetScaler ADC.

Las siguientes instrucciones le ayudarán a implementar el SSO Office 365 StyleBook en su red empresarial.

### Para implementar el SSO Microsoft Office 365 StyleBook

1. En Citrix Application Delivery Management (ADM), vaya a **Aplicaciones**> **StyleBooks** . La página **StyleBooks** muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplázate hacia abajo y busca **SSO Office 365 StyleBook**. Haga clic en **Crear configuración**.
2. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
3. Introduzca valores para los siguientes parámetros:
   a) **Nombre de la aplicación**. Nombre de la configuración de SSO de Microsoft Office 365 que se va a implementar en la red.
   b) **Autenticación Dirección IP virtual**. Dirección IP virtual que utilizará el servidor virtual AAA al que está vinculada la directiva de IdP SAML de Microsoft Office 365.

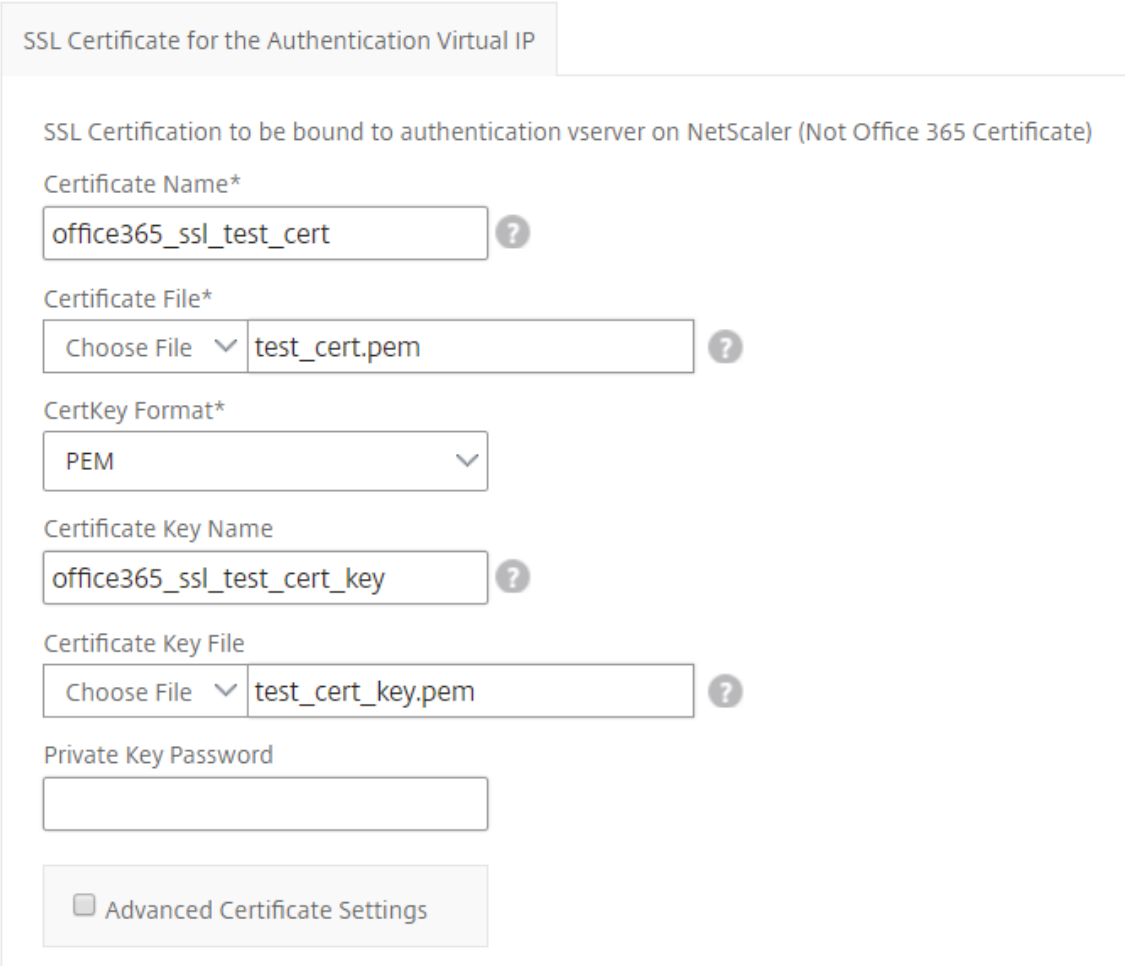



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En la sección **Configuración de certificados SSL**, introduzca los nombres del certificado SSL y la clave de certificado.

   > **Nota**
   >
   > Este no es el certificado de proveedor de servicios de Office 365. Este certificado SSL está enlazado al servidor de autenticación virtual de la instancia NetScaler ADC.

5. Selecciona los archivos correspondientes de tu carpeta de almacenamiento local. También puede escribir la contraseña de clave privada para cargar claves privadas cifradas en formato PEM.




6. También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.

7. Si lo quiere, puede seleccionar el **certificado SSL CA para la casilla de verificación IP virtual de autenticación** si el certificado SSL requiere la instalación de un certificado público de CA en NetScaler ADC. Asegúrese de elegir "Es un certificado de CA"en la sección **Configuración avanzada de certificados** anterior.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

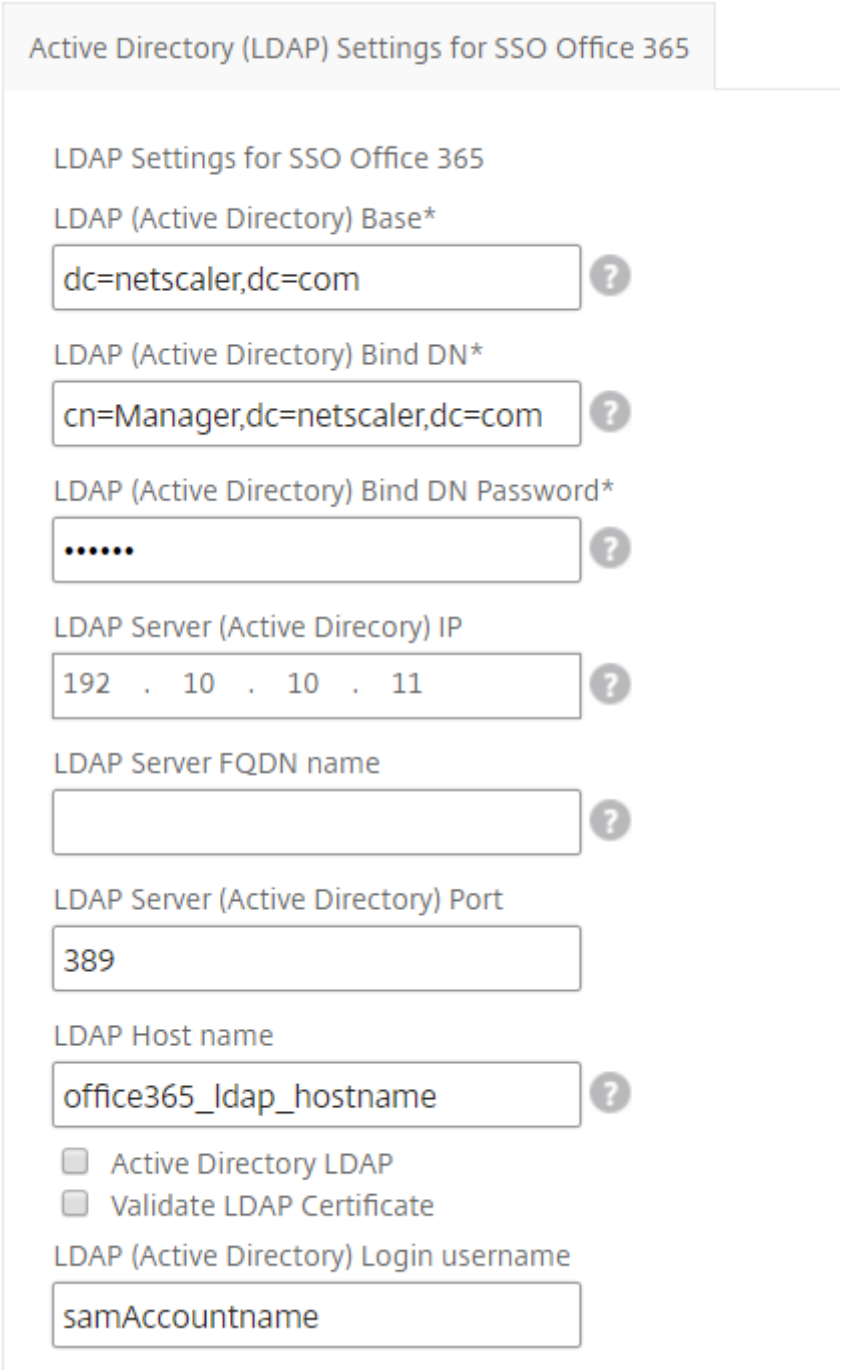
8. En la sección **Configuración de LDAP para SSO Office 365**, introduzca los siguientes detalles para autenticar a los usuarios de Office 365. Para permitir que los usuarios del dominio inicien sesión en la instancia de NetScaler ADC mediante sus direcciones de correo electrónico corporativas, configure lo siguiente:

   - **Base LDAP (Active Directory)**. Escriba el nombre de dominio base del dominio en el que residen las cuentas de usuario en Active Directory (AD) para permitir la autenticación. Por ejemplo, dc=netscaler, dc=com
   - **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga derechos para examinar el árbol de AD. Por ejemplo, cn=Manager, dc=netscaler, dc=com
   - **Contraseña de DN de enlace LDAP (Active Directory)**. Introduzca la contraseña de la cuenta de dominio para la autenticación.
   - Algunos otros campos que debe introducir en esta sección son los siguientes:
     - Dirección IP del servidor LDAP a la que se conecta NetScaler ADC para autenticar a los usuarios.
     - Nombre de FQDN del servidor LDAP.

       > **Nota**
       >
       > Debe especificar al menos una de las dos opciones anteriores: la dirección IP del servidor LDAP o el nombre de FQDN.

     - Puerto de servidor LDAP al que NetScaler ADC se conecta para autenticar usuarios (el valor predeterminado es 389). LDAPS usa 636.
     - Nombre de host LDAP. El nombre de host se usa para validar el certificado LDAP si la validación está activada (de forma predeterminada, está desactivada).
     - Atributo de nombre de inicio de sesión LDAP. El atributo predeterminado que se utiliza para extraer los nombres de inicio de sesión es “samAccountName”.
     - Otras opciones opcionales de varios LDAP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




9. En la sección **Certificado de IdP de SAML**, puede especificar los detalles de los certificados SSL utilizados para la aserción de SAML.

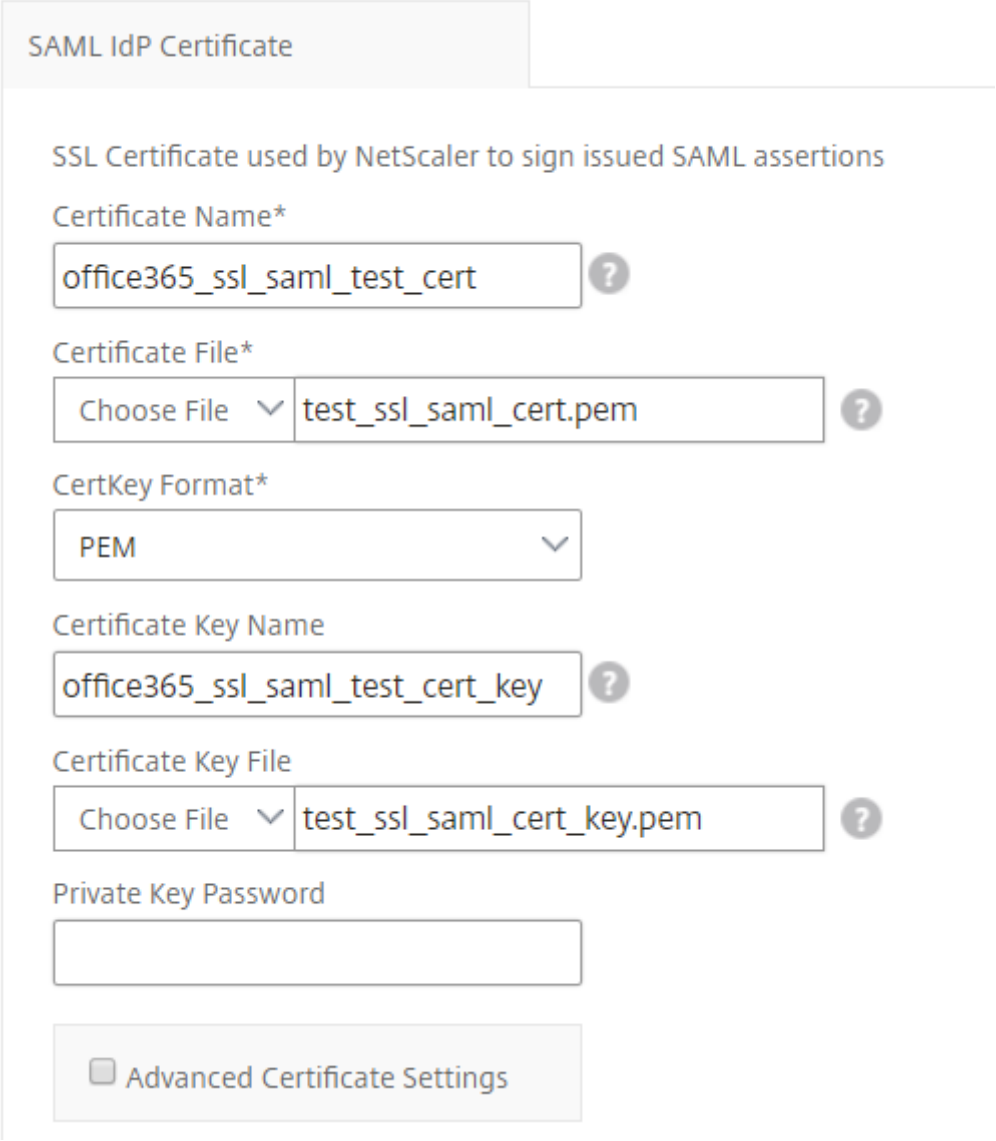
   - **Nombre del certificado**. Introduzca el nombre del certificado SSL.
   - **Archivo**de certificado . Elija el archivo de certificado SSL del directorio de su sistema local.
   - **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones de archivo.pem

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

y .der.

- **Nombre de clave de certificado**. Introduzca el nombre de la clave privada del certificado.
- **Archivo de clave de certificado**. Seleccione el archivo que contiene la clave privada del certificado del sistema local.
- **Contraseña de clave privada**. Escribe la contraseña que protege tu archivo de clave privada.

También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.



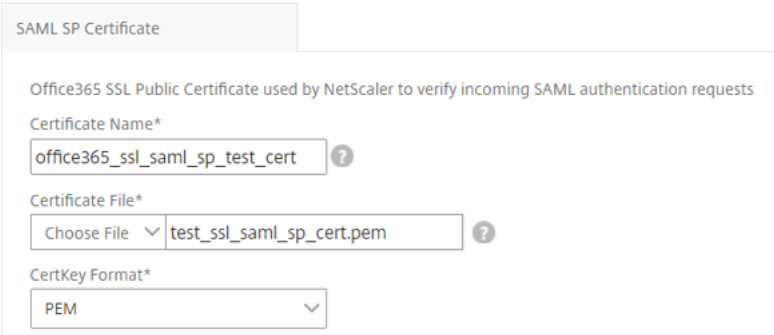

10. Opcionalmente, puede seleccionar el **Certificado de CA de IdP** de SAML si el certificado de IdP de SAML especificado anteriormente requiere que se instale un certificado público de CA en

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

NetScaler ADC. Asegúrese de seleccionar **Es un certificado de CA** en la sección **Configuración avanzada del certificado** anterior.

11. En la sección **Certificado SP de SAML**, introduzca los siguientes detalles para el certificado público SSL de Office 365. La instancia de NetScaler ADC utiliza este certificado para verificar las solicitudes de autenticación SAML entrantes.

    - **Nombre del certificado**. Escriba el nombre del certificado SSL.
    - **Archivo**de certificado . Elija el archivo de certificado SSL del directorio de su sistema local.
    - **Formato CertKey**. Seleccione el formato del certificado y los archivos de clave privada en el cuadro de lista desplegable. Los formatos admitidos son las extensiones de archivo.pem y .der.
    - También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.




12. La sección **Configuración de IDP de SAML** le permite configurar su instancia de Citrix ADC como proveedor de identidades SAML mediante la creación del perfil y la directiva de IDP de SAML que utiliza el servidor virtual AAA creado en el paso 3.

    - **Nombre del emisor SAML**. En este campo, escriba el FQDN público de su servidor virtual de autenticación. Ejemplo:`https://<Citrix ADC Auth VIP>/saml/login`
    - **Expresión de identificador de nombre**. Escriba la expresión de NetScaler ADC que se evalúa para extraer el SAML NameIdentifier enviado en la aserción SAML. Ejemplo:`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - **Algoritmo de firma**: seleccione el algoritmo para verificar/firmar las solicitudes/respuestas de SAML (el valor predeterminado es “RSA-SHA256”).
    - **Método Digest**. Seleccione el método para digerir el hash de las solicitudes/respuestas de SAML (el valor predeterminado es “SHA256”).
    - **Nombre del público**. Escriba el nombre de la entidad o la URL que representa al proveedor de servicios (Microsoft Office 365).

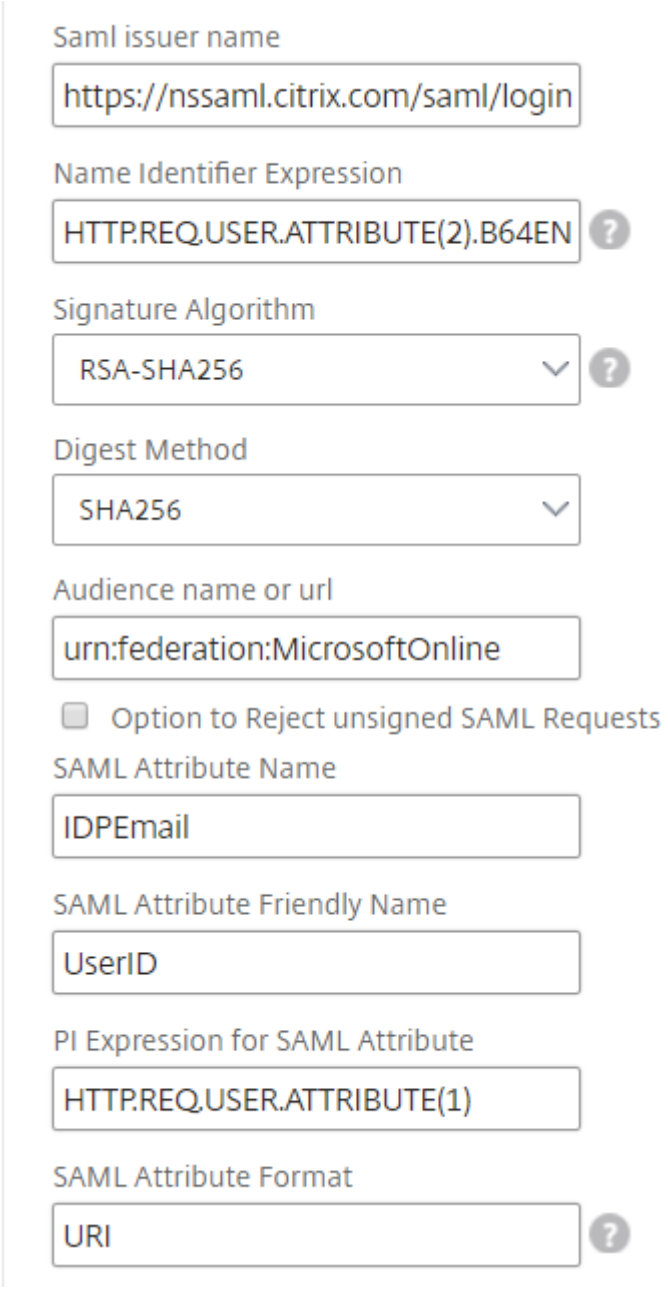
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **ID de proveedor de servicios (SP) SAML**. (opcional) El proveedor de identidades NetScaler ADC acepta solicitudes de autenticación SAML de un nombre de emisor que coincida con este ID.
- **URL de Assertion Consumer Service** Introduzca la URL del proveedor de servicios a la que el proveedor de identidades de NetScaler ADC debe enviar las afirmaciones SAML después de una autenticación de usuario exitosa. La URL del servicio al consumidor de afirmación se puede iniciar en el sitio del servidor del proveedor de identidad o en el sitio del proveedor de servicios.
- Hay otros campos opcionales que puede introducir en esta sección. Por ejemplo, puede configurar las siguientes opciones:
  - **Nombre del atributo SAML**. Nombre del atributo de usuario enviado en la aserción SAML.
  - **Nombre descriptivo del atributo SAML**. Nombre descriptivo del atributo de usuario enviado en la aserción SAML.
  - **Expresión PI para el atributo SAML**. De forma predeterminada, se utiliza la siguiente expresión de directiva de NetScaler ADC (PI): HTTP.REQ.USER.ATTRIBUTE(1). Este campo especifica el primer atributo de usuario enviado desde el servidor LDAP (correo) como atributo de autenticación SAML.
  - Seleccione el formato del atributo de usuario.

  Estos valores se incluyen en la afirmación SAML emitida.

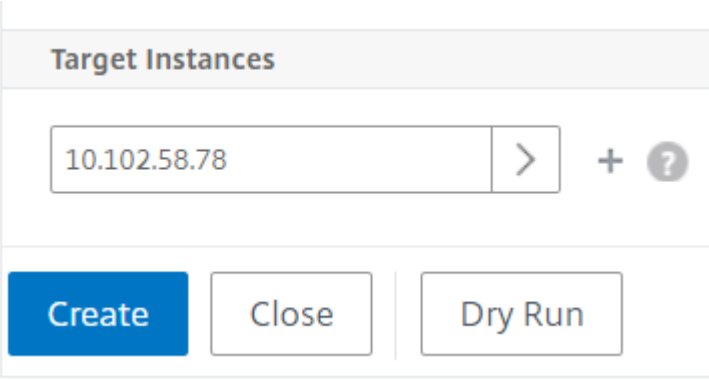
  > **Sugerencia**
  >
  > Citrix recomienda conservar la configuración predeterminada, ya que se ha probado que funciona con las aplicaciones de Microsoft Office 365.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




13. Haga clic en Instancias de **destino y seleccione las instancias** NetScaler ADC en las que quiere implementar esta configuración de SSO de Microsoft Office 365. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Sugerencia**

Citrix recomienda que, antes de ejecutar la configuración real, seleccione**Ejecutar en seco**para ver los objetos de configuración creados en las instancias de NetScaler ADC de destino por el StyleBook.

## StyleBook de Microsoft Skype Empresarial

January 30, 2024

La aplicación Skype Empresarial 2015 se basa en varios componentes externos para funcionar. La red Skype Empresarial consta de varios sistemas, como servidores y sus sistemas operativos, bases de datos, sistemas de autenticación y autorización, sistemas e infraestructura de redes y sistemas de PBX telefónicos. Skype Empresarial Server 2015 está disponible en dos versiones, Standard Edition y Enterprise Edition. La principal diferencia radica en la compatibilidad con las funciones de alta disponibilidad que solo se incluyen en la edición empresarial. Para implementar la alta disponibilidad, se deben implementar varios servidores front-end en un grupo y los servidores SQL deben reflejarse.

Una implementación de Enterprise Edition permite la creación de varios servidores con diferentes funciones.

### Componentes principales

Los componentes principales de la aplicación Skype Empresarial 2015 son:

- Servidores frontales
- Servidores Edge
- Servidores de Director
- Servidores de base de datos (SQL)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Servidores frontales

En la aplicación Skype Empresarial, el servidor front-end es el servidor principal de la red. Proporciona los enlaces y los servicios para la autenticación de usuarios, el registro, la presencia, la libreta de direcciones, las conferencias audiovisuales, el intercambio de aplicaciones, la mensajería instantánea y las conferencias web. Si va a implementar Skype Empresarial 2015 Enterprise Edition, la topología suele consistir en al menos dos servidores Front-End equilibrados de carga en un grupo Front-End con un servidor de base de datos que aloja la instancia de SQL Server que contiene la base de datos de Skype Empresarial.

### Servidores Edge

La implementación de servidores perimetrales para Skype Empresarial es necesaria si los usuarios externos que no han iniciado sesión en la red interna de su organización necesitan poder interactuar con usuarios internos. Estos usuarios externos pueden ser usuarios remotos anónimos y autenticados, socios federados u otros clientes móviles.

Hay cuatro tipos de funciones en el servidor Edge de Skype For Business:

- Access Edge, que gestiona el tráfico SIP y autentica las conexiones externas, permite la conexión remota y permite la conexión de federación
- Conferencing Web, que gestiona los paquetes de conferencia de datos y permite a los usuarios externos acceder a Skype Empresarial
- Conferencias A/V, que gestiona paquetes de conferencias A/V y extiende el audio y el vídeo, el uso compartido de aplicaciones y la transferencia de archivos a usuarios externos
- Proxy XMPP, que maneja paquetes XMPP y permite que servidores o clientes basados en XMPP se conecten a Skype Empresarial.

### Servidores de Director

La función principal del servidor de Director en Skype Empresarial 2015 es autenticar los dispositivos de punto final y “dirigir”a los usuarios al grupo que contiene su cuenta. En Skype Empresarial 2015, aunque el Director es un rol completamente dedicado y específico en un servidor independiente, es un servidor opcional. Esto facilita la seguridad al facilitar la implementación o la eliminación de las configuraciones.

Los directores son más útiles cuando existen varios grupos porque proporcionan un único punto de contacto para autenticar los puntos de conexión. Además, para los usuarios remotos, un Director sirve como salto adicional entre el grupo Edge y el grupo Front-End, lo que agrega una capa adicional de protección contra ataques.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La siguiente ilustración representa de forma diagramática la implementación de servidores de Skype en la red:

## Configuración de instancias de Citrix ADC en una empresa

En la tabla siguiente se enumeran las direcciones IP utilizadas en la configuración de ejemplo que se incluye en las instrucciones siguientes:

| Servidores de Skype Empresarial | Dirección IP virtual | Direcciones IP del servidor | Instancia Citrix ADC |
|---|---|---|---|
| Servidores Edge | VIP externo - 192.20.20.20<br>VIP interno - 10.10.10.20 | 192.20.20.21; 192.20.20.22<br>10.10.10.21; 10.10.10.22 | 10.102.29.141 |
| Servidores frontales | 10.10.10.10 | 10.10.10.11; 10.10.10.12 | 10.102.29.60 |
| Servidor de Director | 10.10.10.30 | 10.10.10.31; 10.10.10.32 | 10.102.29.93 |

**Para configurar servidores frontales**

1. En Citrix Application Delivery Management (ADM), vaya a **Aplicaciones** > **Configuración**y haga clic en **Crear nuevo**. La página **Choose StyleBook** muestra todos los StyleBooks disponibles para su uso en Citrix ADM. Desplácese hacia abajo y seleccione **Microsoft Skype Empresarial 2015 StyleBook**. El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.
2. En la sección **Servidor Edge**, introduzca las siguientes direcciones IP virtuales (VIP) y las direcciones IP de todos los servidores Edge de la red.
   a) Dirección VIP externa y direcciones IP de los servidores Edge que se utilizarán para Access Edge, las conferencias web Edge y A/V Edge.
   b) Dirección VIP interna y direcciones IP de los servidores Edge que se conectarán a la red interna.
   c) Dos servidores Edge externos y dos internos en su red.
3. En la sección **Servidor front-end**, escriba la dirección IP del servidor front-end virtual (VIP) que se va a crear para los servidores front-end de Skype Empresarial. Además, introduzca las direcciones IP de todos los servidores front-end de Skype Empresarial de la red.
4. En la sección de **Director Server**, escriba la dirección IP virtual (VIP) para los servidores de Director que se va a crear para la aplicación Skype Empresarial. Además, introduzca las direcciones

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

IP de todos los servidores de Skype Empresarial Director de la red. Cree al menos dos servidores Director para una alta disponibilidad.

5. La sección **Configuración avanzada** enumera todos los puertos predeterminados configurados en las instancias de Citrix ADC para los tres servidores de Skype.

La siguiente tabla proporciona una lista de todos los puertos y protocolos predeterminados:

| Etiqueta | Puerto | Protocolo | Descripción |
|---|---|---|---|
| Puerto HTTP | 80 | HTTP | Se utiliza para la comunicación de los servidores front-end a los FQDN de la comunidad web cuando no se utiliza HTTPS. |
| Puerto HTTPS | 443 | HTTPS | Se utiliza para la comunicación de los servidores front-end a los FQDN de la comunidad de servidores web. |
| Puerto interno de AutoDiscover | 4443 | HTTPS | Comunicaciones entre grupos mediante HTTPS (de Reverse Proxy) y HTTPS Front-End para el inicio de sesión de AutoDiscover. |
| Puerto RPC | 135 | DCOM y llamada de procedimiento remoto (RPC) | Se utiliza para operaciones basadas en DCOM, como el traslado de usuarios, la sincronización de replicadores de usuarios y la sincronización de libretas de direcciones. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Etiqueta | Puerto | Protocolo | Descripción |
|---|---|---|---|
| Puerto SIP | 5061 | TCP (TLS) | Los servidores Front-End lo utilizan para todas las comunicaciones SIP internas. |
| Puerto de enfoque SIP | 444 | HTTPS, TCP | Se utiliza para la comunicación HTTPS entre el Focus (el componente que administra el estado de la conferencia de Skype) y los servidores individuales. |
| Puerto de grupo SIP | 5071 | TCP | Se usa para las solicitudes SIP entrantes para la aplicación del grupo de respuestas. |
| Puerto SIP para compartir aplicaciones | 5065 | TCP | Se utiliza para las solicitudes de escucha SIP entrantes para compartir aplicaciones. |
| Puerto de asistente SIP | 5072 | TCP | Se utiliza para las solicitudes SIP entrantes para el operador (es decir, para las conferencias de acceso telefónico). |
| Puerto de anuncio SIP Conf | 5073 | TCP | Se utiliza para las solicitudes SIP entrantes para el servicio de anuncio de conferencia de Skype Empresarial Server (es decir, para las conferencias de acceso telefónico). |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Etiqueta | Puerto | Protocolo | Descripción |
|---|---|---|---|
| Puerto SIP CallPark | 5075 | TCP | Se utiliza para las solicitudes SIP entrantes para la aplicación CallPark. |
| Puerto de admisión de llamadas SIP | 448 | TCP | Se utiliza para el control de admisión de llamadas por el servicio de directivas de ancho de banda del servidor de Skype Empresarial. |
| Puerto TURN de admisión de llamadas SI | 5080 | TCP | El servicio de directivas de ancho de banda lo utiliza para controlar la admisión de llamadas para el tráfico TURN de Audio/Video Edge |
| Puerto de prueba de audio SIP | 5076 | TCP | Se usa para las solicitudes SIP entrantes para el servicio de prueba de audio. |
| Puerto externo HTTPS | 443 | HTTPS | Se utiliza para puertos externos para la comunicación SIP/TLS para el acceso remoto de usuarios, el acceso a conferencias web internas y las comunicaciones multimedia entrantes y salientes de STUN/TCP para acceder a los medios internos y a las sesiones de A/V. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Etiqueta | Puerto | Protocolo | Descripción |
| --- | --- | --- | --- |
| Puerto interno HTTPS | 443 | HTTPS | Se utiliza como puertos internos para la comunicación SIP/TLS para el acceso remoto de usuarios, el acceso a conferencias web internas y las comunicaciones multimedia entrantes y salientes de STUN/TCP para acceder a los medios internos y a las sesiones de A/V. |
| Puerto de acceso remoto externo SIP | 5061 | TCP | Se utiliza para puertos externos para la comunicación SIP/MTLS para el acceso remoto de usuarios o la federación. |
| Puerto de acceso remoto interno SIP | 5061 | TCP | Se utiliza como puertos internos para la comunicación SIP/MTLS para el acceso remoto de usuarios o la federación. |
| Puerto SIP STUN UDP externo | 3478 | UDP | Se utiliza para puertos externos para comunicaciones multimedia entrantes y salientes de STUN/UDP. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Etiqueta | Puerto | Protocolo | Descripción |
|---|---|---|---|
| Puerto SIP STUN UDP interno | 3478 | UDP | Se utiliza para los puertos internos para las comunicaciones multimedia entrantes y salientes de STUN/UDP. |
| Puerto IM interno SIP | 5062 | | Se utiliza para los puertos internos para la autenticación SIP/MTLS de las comunicaciones de mensajería instantánea que salen a través del firewall interno. |
| Puerto HTTP | 80 | TCP | Se utiliza para la comunicación inicial de Directores a los FQDN de la comunidad de servidores web. |
| Puerto HTTPS | 443 | HTTPS | Se utiliza para la comunicación de Directores a los FQDN de la comunidad de servidores web. |
| Puerto interno de AutoDiscover | 4443 | HTTPS | Se utiliza para las comunicaciones entre grupos de HTTPS (de Reverse Proxy) y HTTPS Director para el inicio de sesión de AutoDiscover. |
| Puerto interno SIP | 5061 | TCP | Se utiliza para las comunicaciones internas entre servidores y para las conexiones de cliente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

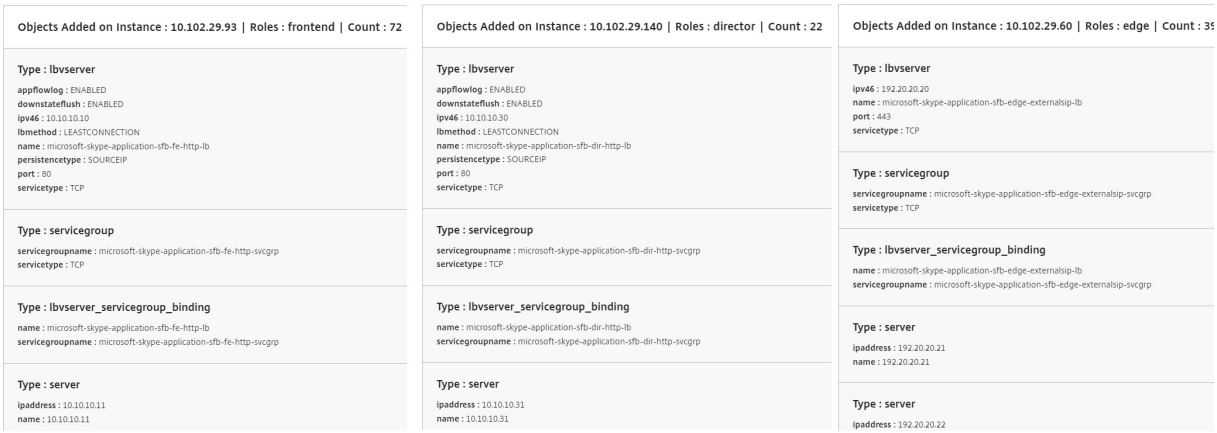
6. En la sección **Instancias de destino, seleccione las tres instancias** de Citrix ADC diferentes en las que quiere implementar los tres servidores de Skype Empresarial.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

7. Haga clic en**Crear** para crear la configuración en las instancias de Citrix ADC seleccionadas.

> **Sugerencia**
>
> Citrix recomienda seleccionar**Ejecución en seco**para comprobar los objetos de configuración que se deben crear en la instancia de destino antes de ejecutar la configuración real en la instancia.
>
> Cuando la configuración se crea correctamente, StyleBook crea 25 servidores virtuales de equilibrio de carga. Es decir, para cada puerto, se define un servidor virtual de equilibrio de carga junto con un grupo de servicios, y el grupo de servicios está enlazado al servidor virtual de equilibrio de carga. La configuración también agrega los servidores Front-End como miembros del grupo de servicios y los vincula al grupo de servicios. La cantidad de miembros del grupo de servicios creados es igual a la cantidad de servidores Front-End creados.

La siguiente ilustración muestra los objetos creados en cada servidor:




## StyleBook de Microsoft Exchange

January 30, 2024

Puede usar el StyleBook de Microsoft Exchange 2016 para implementar una configuración de Citrix ADC que optimice y proteja una aplicación empresarial de Microsoft Exchange 2016 en su red. Mi-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

crosoft Exchange 2016 es una aplicación empresarial clave para proporcionar servicios de correo electrónico, administración de información personal y mensajería a sus empleados y otras partes interesadas.

### Funciones de Citrix ADC configuradas mediante Microsoft Exchange StyleBook

El StyleBook de Microsoft Exchange 2016 habilita y configura las siguientes funciones de Citrix ADC para los servidores de Microsoft Exchange 2016:

- Equilibrio de carga: equilibrio de carga básico que permite equilibrar la carga de varios servidores de Exchange
- Conmutación de contenido: cambio de contenido que permite el acceso con una sola IP y la redirección de las consultas a los servidores virtuales de equilibrio de carga correctos
- Reescribir: redirige a los usuarios a páginas seguras
- Descarga de SSL: descarga el procesamiento de SSL al Citrix ADC y, por lo tanto, reduce la carga en el servidor Exchange

La siguiente ilustración representa de forma diagramática la implementación de servidores Exchange en la red:

### Requisitos previos

- Para la autenticación basada en certificados, todos los hosts direccionables que forman parte de la configuración de la red deben tener nombres de dominio resolubles y no solo direcciones IP.
- Asegúrese de que se pueda acceder a los puertos SIP en el servidor Microsoft Exchange 2016.

### Configuración de Microsoft Exchange StyleBook

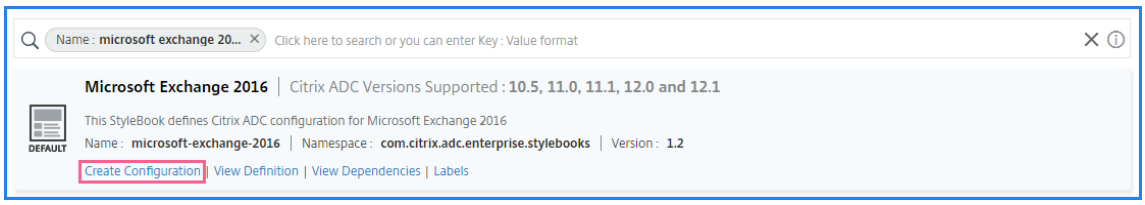
Configure el StyleBook de Microsoft Exchange en su empresa empresarial para implementar la configuración de Citrix ADC.

### Para configurar la aplicación Microsoft Exchange

1. En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**.
2. Busque **Microsoft Exchange 2016 StyleBook** y haga clic en **Crear configuración**.

   El StyleBook aparece como un formulario de interfaz de usuario en el que puede introducir los valores de todos los parámetros definidos en este StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. Introduzca los detalles de los siguientes parámetros:

   - **Nombre de la aplicación de Exchange**: Nombre de la aplicación Microsoft Exchange de la red
   - **Exchange VIP**: dirección IP virtual en Citrix ADC que recibe las solicitudes de los clientes para la aplicación Microsoft Exchange
   - **IPs de Exchange Server**: Direcciones IP de todos los servidores de Exchange de la red.

     Si quiere agregar más direcciones IP, haga clic en el icono con el signo más (**+**). Normalmente, dos servidores Exchange están configurados en la red.

4. En la sección **Certificados de Exchange**, cargue los certificados de intercambio en Citrix ADM. Introduzca los nombres del certificado y de los archivos de clave y cárguelos desde el almacenamiento local. También puede proporcionar una contraseña de clave privada para cifrar el archivo de claves.

   > **Nota**
   >
   > Asegúrese de que los archivos de certificado tengan el formato ".pem"o ".der". Citrix ADM rechaza los archivos de otros formatos.

   Si quiere especificar los detalles de caducidad del certificado o cualquier configuración avanzada, seleccione **Configuración avanzada del certificado**.

5. En la sección **Configuración de autenticación de Active Directory de Exchange**, configure los ajustes de AD introduciendo los datos.

   - **Active Directory Authentication VIP** : la dirección IP virtual utilizada para crear y configurar el servidor virtual AD (LDAP) en un dispositivo Citrix ADC.
   - **IP del servidor Active Directory**: la dirección IP del controlador de dominio de Active Directory.
   - **Cadena base de Active Directory: la cadena**base LDAP de Active Directory. Por ejemplo, CN=Users, DC=CTXNSSFB, DC=COM.
   - Nombre**distintivo de enlace LDAP (DN) de Active Directory: el nombre** distintivo (DN) de enlace de LDAP se utiliza para vincular este objeto al servidor LDAP (AD). Por ejemplo, "cn=Administrator,cn=Users,dc=acme,dc=com"

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Contraseña de**nombre distintivo (DN) de enlace LDAP de Active Directory: el nombre distintivo (DN) de enlace de LDAP es la contraseña** para la autenticación de AD
- Atributo de**nombre de usuario de Active Directory: atributo** AD para el nombre de usuario. El Citrix ADC utiliza el atributo LDAP para consultar servidores Active Directory externos. Por ejemplo, "sAMAccountName"
- **Nombre de atributo del grupo de Active Directory**: los nombres de los atributos del grupo LDAP configurados en el servidor LDAP. Por ejemplo, "memberOf"para el atributo de grupo en LDAP.
- **Nombre de subatributo de Active Directory**: Los nombres de los subatributos de LDAP configurados en el servidor LDAP. Por ejemplo, "cn"para el subatributo de LDAP.
- **Dominio de autenticación de Active Directory**: El nombre de dominio AD/LDAP utilizado para la autenticación. Por ejemplo, ctxnssfb.com.

6. En la sección**Instancias de destino**, seleccione la instancia de Citrix ADC en la que implementar esta configuración de Exchange.

   > **Nota**
   >
   > Si quiere ver las instancias de Citrix ADC detectadas recientemente, haga clic en el icono de actualización.

7. Haga clic en **Crear** para crear el archivo de configuración y ejecutar la configuración en la instancia de Citrix ADC seleccionada.

   Citrix recomienda seleccionar primero**Ejecución en seco**para comprobar los objetos de configuración que se crean en la instancia de destino antes de ejecutar la configuración real en la instancia.

Cuando la configuración se ha creado correctamente, StyleBook ha creado un servidor virtual de conmutación de contenido, cinco servidores virtuales de equilibrio de carga y una directiva LDAP vinculada a un servidor virtual de autenticación LDAP. Además, los grupos de servicios correspondientes creados y enlazados a los servidores virtuales de equilibrio de carga.

## StyleBook de Microsoft SharePoint

January 30, 2024

Microsoft SharePoint 2016 es una aplicación empresarial clave que proporciona principalmente un sistema de almacenamiento y administración de documentos, altamente configurable y compatible con todos los principales navegadores.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede usar el StyleBook de Microsoft SharePoint 2016 para implementar una configuración de Citrix ADC que optimice y proteja la aplicación empresarial de Microsoft SharePoint 2016 en su red.

## Requisitos previos

- Microsoft SharePoint 2016
- Citrix ADM, versión 12.0 y posteriores
- Citrix ADC, versión 10.5 y posterior

## Funciones de Citrix ADC configuradas por el StyleBook de Microsoft SharePoint 2016

Puede usar el StyleBook de Microsoft SharePoint 2016 para habilitar y configurar las siguientes funciones de Citrix ADC para Microsoft SharePoint 2016:

- Equilibrio de carga
- Conmutación de contenido
- Responder
- Reescritura
- Compresión
- Almacenamiento en caché integrado

### Equilibrio de carga

El equilibrio de carga de Citrix ADC distribuye uniformemente las solicitudes a los servidores de backend de SharePoint. La supervisión inteligente de los servidores de fondo evita que las solicitudes se envíen a servidores que no funcionan correctamente.

SharePoint StyleBook configura 12 servidores virtuales de equilibrio de carga, cada uno dedicado a solicitudes de equilibrio de carga para un determinado tipo de contenido, como documentos, imágenes, audio, vídeo y otros tipos de archivo.

El StyleBook de SharePoint ahora admite el modo SSL de la aplicación SharePoint mediante la configuración de servidores virtuales LB basados en SSL. Asegúrese de que SSL esté seleccionado como protocolo de interfaz. Tenga en cuenta que el puerto virtual está establecido en 443 de forma predeterminada. También puede seleccionar SSL para vincular grupos de servicios (servidores de aplicaciones de SharePoint) a los servidores virtuales de equilibrio de carga de destino. Tenga en cuenta que el protocolo de backend está configurado de forma predeterminada en HTTP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

#### Cambio de contenido

La función de cambio de contenido se utiliza para distribuir las solicitudes de los clientes en varios servidores virtuales de equilibrio de carga en función de tipos específicos de contenido de SharePoint solicitado (por ejemplo, documentos, imágenes y archivos de audio o vídeo). El módulo de conmutación de contenido dirige el tráfico entrante a un servidor virtual de equilibrio de carga óptimo que puede procesar ese tipo de contenido. Por lo tanto, puede aplicar diferentes directivas de optimización a diferentes tipos de tráfico. Por ejemplo, es posible que quiera utilizar directivas de compresión o almacenamiento en caché diferentes para los vídeos que para los documentos de texto.

#### Responder

La funcionalidad de respuesta de una instancia de Citrix ADC se puede utilizar para redirigir sin problemas a los usuarios de HTTP a HTTPS. El respondedor también se puede configurar para proporcionar páginas de error personalizadas. La directiva de respuesta determina las solicitudes (tráfico) en las que se debe realizar una acción y vincula cada directiva a un servidor virtual de equilibrio de carga. El StyleBook de SharePoint incluye una configuración que redirige a los usuarios de las URL HTTP a HTTPS.

#### Reescritura

El módulo de reescritura se utiliza para modificar los encabezados, las URL o el contenido de las solicitudes o respuestas sobre la marcha. Este módulo funciona en línea con el procesamiento del tráfico y, por lo tanto, puede cambiar el flujo de tráfico según corresponda para casos de uso particulares. Por ejemplo, la reescritura puede proporcionar acceso al contenido solicitado sin exponer detalles innecesarios sobre el servidor del sitio web.

En el StyleBook de SharePoint, la función de reescritura se utiliza para eliminar los encabezados innecesarios de las solicitudes de los usuarios.

#### Compresión

El motor de compresión Citrix ADC identifica y comprime el contenido que se puede comprimir. Este proceso mejora el tiempo de transmisión de datos y reduce los requisitos de ancho de banda de la red para los clientes, al tiempo que ahorra los ciclos de CPU en los servidores Una instancia de Citrix ADC puede comprimir datos generados tanto estáticos como dinámicamente. Aplica el algoritmo de compresión GZIP o DEFLATE para eliminar información extraña y repetitiva de las respuestas del servidor y representar la información original en un formato más compacto y eficiente. La capacidad

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

del explorador cliente para descomprimir los datos depende del algoritmo o algoritmos que admita: GZIP, DEFLATE o ambos.

Una instancia de Citrix ADC está configurada para comprimir el texto en HTML, XML, texto sin formato, hojas de estilos en cascada (CSS) y documentos de Microsoft Office, pero no comprime las imágenes en formato GIF o JPG. Los principales beneficios del tráfico comprimido incluyen la reducción de los costes de ancho de banda, la reducción de la latencia de la WAN y un mejor rendimiento

#### Almacenamiento en caché integrado

La caché en memoria de Citrix ADC puede almacenar objetos de SharePoint para entregar rápidamente el contenido solicitado con frecuencia a los usuarios. El contenido en caché incluye documentos descargados y archivos de audio, vídeo e imagen.

La siguiente ilustración representa de forma diagramática la implementación de servidores SharePoint en una instancia de Citrix ADC en la que se utiliza Citrix ADM para implementar una configuración de SharePoint StyleBook.

### Implementación de configuraciones de SharePoint StyleBook

La siguiente tarea le ayudará a implementar el StyleBook de Microsoft SharePoint 2016 en su red empresarial.

**Para implementar Microsoft SharePoint 2016 StyleBook**:

1. En Citrix ADM, vaya a **Aplicaciones** > **Administración** > **Configuración**y haga clic en **Crear nuevo**.

   La página **Choose StyleBook** muestra todos los StyleBooks disponibles para su uso en Citrix ADM.

2. Desplázate hacia abajo y selecciona **Microsoft SharePoint 2016 StyleBook**.

   > **Nota:**
   >
   > En Citrix ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**. Desplácese hacia abajo para buscar el **StyleBook de Microsoft SharePoint 2016** y haga clic en **Crear configuración**.

   El StyleBook se abre como un formulario de interfaz de usuario en el que puede introducir los valores de todos los parámetros definidos en este StyleBook.

   Introduzca valores para los siguientes parámetros:

   a) **Nombre de la aplicación SharePoint**. Nombre de la configuración de SharePoint que se va a implementar en la red.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) **IP virtual de SharePoint**. Dirección IP virtual en la que la instancia de Citrix ADC recibe las solicitudes de los clientes para la aplicación Microsoft SharePoint.

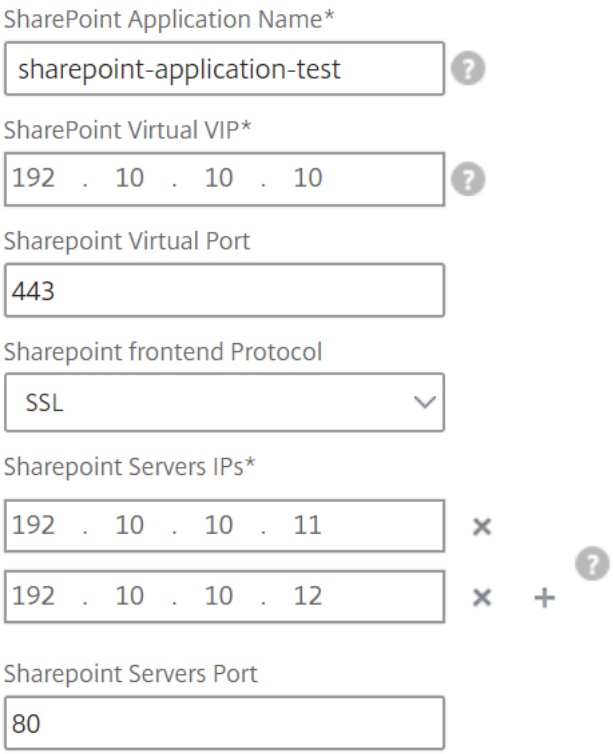
c) **Puerto virtual de SharePoint**. El puerto TCP que utilizarán los usuarios para acceder a la aplicación SharePoint

d) **Protocolo de interfaz de SharePoint**. Seleccione el protocolo de interfaz de SharePoint en la lista desplegable. Las opciones disponibles son HTTP o SSL.

> **Nota:**
>
> Si selecciona SSL, asegúrese de que el parámetro Reescritura de configuración esté habilitado en la sección Configuración avanzada de SharePoint de este StyleBook.

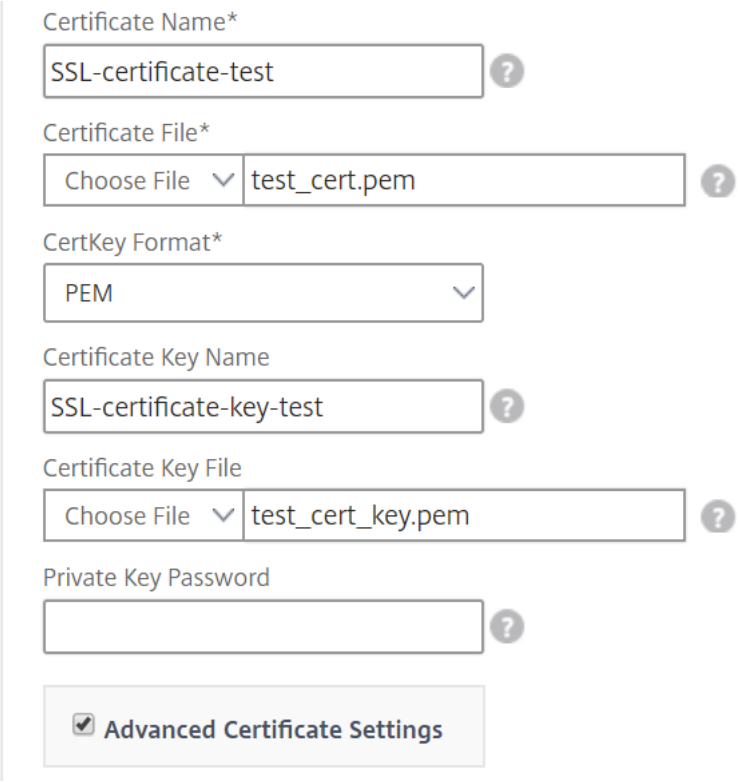
e) **IPs de SharePoint Server**. Direcciones IP de todos los servidores SharePoint de la red.

f) **Puerto de servidores SharePoint**. Número de puerto TCP utilizado por los servidores de SharePoint. De forma predeterminada, es 80. Puede modificar este valor si es necesario, pero asegúrese de que este puerto es accesible en servidores de Microsoft SharePoint 2016.

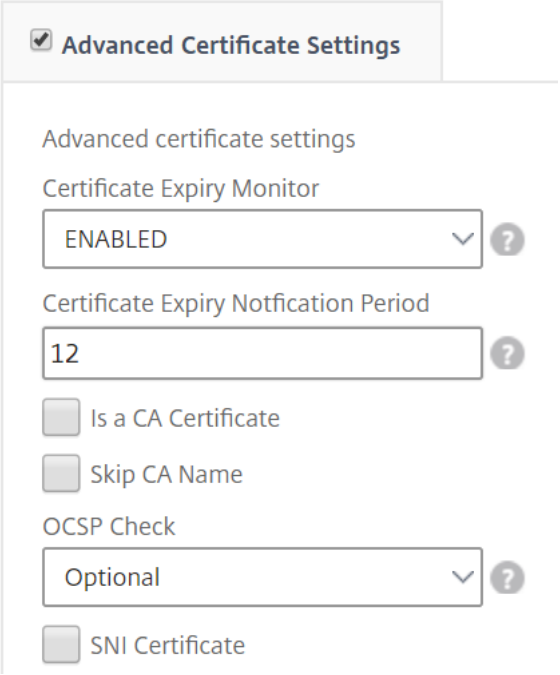



3. En la sección **Configuración de certificados SSL**, haga clic en + para introducir el nombre del certificado SSL, la clave de certificado y seleccionar los archivos respectivos de la carpeta de almacenamiento local.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



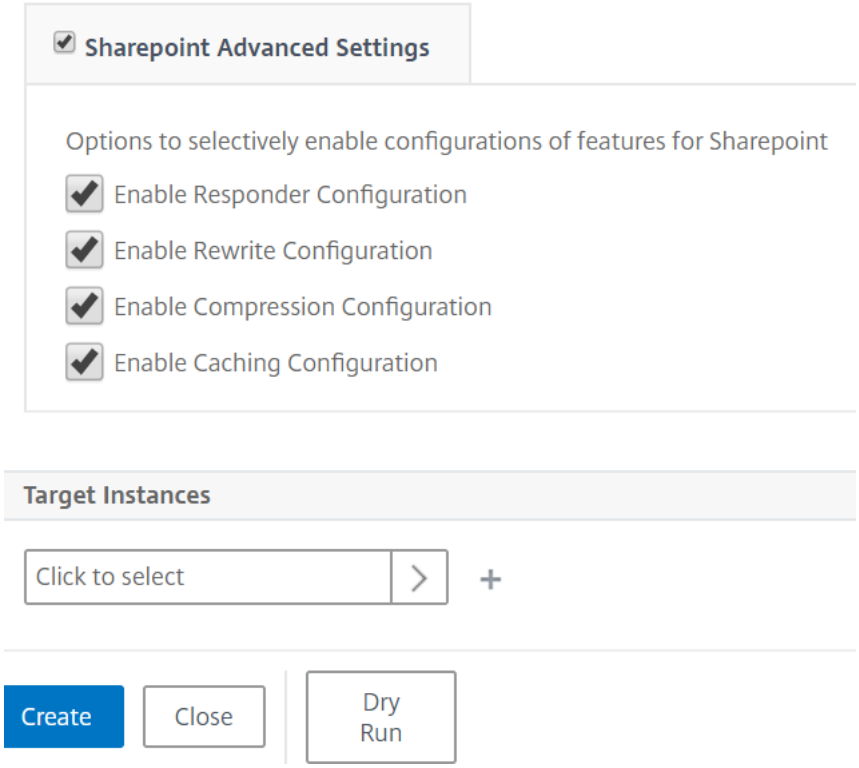

4. Si lo quiere, haga clic en **Configuración avanzada de certificados** para habilitar o inhabilitar la supervisión de caducidad de certificados SSL. Si habilita la supervisión de la caducidad de los certificados, defina el número de días para que Citrix ADM emita una alarma después de esos días cuando el certificado esté a punto de caducar. También tiene la opción de realizar la comprobación OCSP como una función opcional o una función obligatoria.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. La sección **Configuración avanzada** de SharePoint le permite habilitar las funciones de Citrix ADC que se configurarán en las instancias de Citrix ADC. Si bien las funciones de equilibrio de carga y cambio de contenido están configuradas en las instancias de forma predeterminada, puede elegir las demás funciones, es decir, la configuración del respondedor, la configuración de reescritura, la configuración de compresión y la configuración de almacenamiento en caché integrado, que deseas configurar en la instancia.
6. Haga clic en **Instancias de destino** y seleccione la instancia de Citrix ADC en la que quiere implementar esta configuración de SharePoint. Haga clic en **Crear** para crear la configuración e implementarla en la instancia de Citrix ADC seleccionada.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.




> **Nota:**
>
> Citrix recomienda que, antes de ejecutar la configuración real, seleccione **Ejecución en seco** para comprobar los objetos de configuración que se crearán en la instancia de destino.

Cuando se crea la configuración y se implementa correctamente, SharePoint StyleBook crea un servidor virtual de conmutación de contenido y 12 servidores virtuales de equilibrio de carga. También

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

crea directivas y grupos de servicios y los vincula a los servidores virtuales de equilibrio de carga. Las directivas que se creen dependen de las funciones seleccionadas en el StyleBook durante la creación del paquete de configuración.

### Visualización de los objetos definidos en la instancia de Citrix ADC

Una vez creado el paquete de configuración en Citrix ADM, puede ver todos los objetos creados en la instancia de Citrix ADC para el StyleBook de SharePoint. Vaya a **Aplicaciones** > **Administración** > **Configuración** y haga clic en **Ver objetos creados**. La siguiente ilustración muestra algunos de los objetos creados, con las direcciones IP especificadas en el ejemplo que se muestra en "Implementación de configuraciones de SharePoint StyleBook desde Citrix ADM. "

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Type : lbvserver**

**appflowlog :** DISABLED
**backuppersistencetimeout :** 20
**downstateflush :** DISABLED
**ipv46 :** 0.0.0.0
**lbmethod :** LEASTCONNECTION
**name :** sharepoint application test frontpage services lb
**persistencebackup :** SOURCEIP
**persistencetype :** COOKIEINSERT
**port :** 0
**servicetype :** HTTP
**timeout :** 20

**Type : servicegroup**

**cip :** DISABLED
**cka :** YES
**cmp :** NO
**downstateflush :** DISABLED
**healthmonitor :** NO
**servicegroupname :** sharepoint-application-test-frontpage-services-svcgrp
**servicetype :** HTTP
**sp :** ON
**state :** ENABLED
**tcpb :** NO
**useproxyport :** NO
**usip :** NO

**Type : lbvserver_servicegroup_binding**

**name :** sharepoint-application-test-frontpage-services-lb
**servicegroupname :** sharepoint-application-test-frontpage-services-svcgrp

**Type : servicegroup_servicegroupmember_binding**

**ip :** 192.10.10.11
**port :** 80
**servicegroupname :** sharepoint-application-test-frontpage-services-svcgrp

**Type : servicegroup_servicegroupmember_binding**

**ip :** 192.10.10.12
**port :** 80
**servicegroupname :** sharepoint-application-test-frontpage-services-svcgrp

**Type : csaction**

**name :** sharepoint-application-test-cs-frontpage-services-csaction
**targetlbvserver :** sharepoint-application-test-frontpage-services-lb

**Type : cspolicy**

**action :** sharepoint-application-test-cs-frontpage-services-csaction
**policyname :** sharepoint-application-test-cs-frontpage-services-cspol
**rule :** HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

**Type : csvserver_cspolicy_binding**

**name :** sharepoint-application-test-cs
**policyname :** sharepoint-application-test-cs-frontpage-services-cspol
**priority :** 10

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# StyleBook proxy de Microsoft ADFS

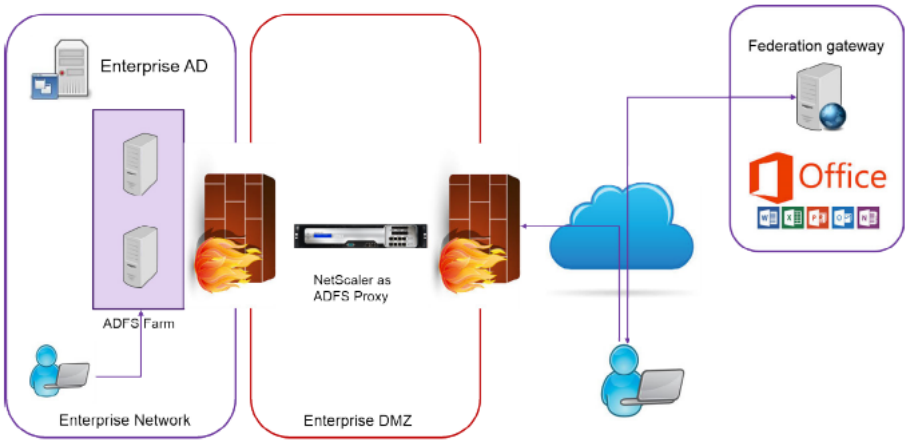
January 30, 2024

El proxy ADFS de Microsoft™ desempeña un papel importante al ofrecer acceso con inicio de sesión único tanto a los recursos internos habilitados por la federación como a los recursos en la nube. Un ejemplo de recursos en la nube es Office 365. El propósito del servidor proxy ADFS es recibir y reenviar solicitudes a servidores ADFS que no son accesibles desde Internet. El proxy ADFS es un proxy inverso y, por lo general, reside en la red perimetral (DMZ) de la organización. El proxy ADFS desempeña un papel fundamental en la conectividad de usuarios remotos y el acceso a aplicaciones.

NetScaler ADC cuenta con la tecnología precisa para permitir la conectividad, la autenticación y el manejo seguros de la identidad federada. El uso de NetScaler ADC como proxy ADFS evita la necesidad de implementar un componente adicional en la DMZ.

Microsoft ADFS Proxy StyleBook en NetScaler Application Delivery Management (ADM) permite configurar un servidor proxy ADFS en una instancia de NetScaler ADC.

La siguiente imagen muestra la implementación de una instancia de Citrix ADC como servidor proxy ADFS en la DMZ empresarial.




## Ventajas de usar NetScaler ADC como proxy ADFS

1. Satisface tanto las necesidades de equilibrio de carga como las de proxy ADFS
2. Admite casos de acceso de usuario internos y externos
3. Admite métodos enriquecidos para la autenticación previa
4. Proporciona una experiencia de inicio de sesión único para los usuarios
5. Soporta protocolos activos y pasivos

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

   a) Ejemplos de aplicaciones de protocolo activo son: Microsoft Outlook, Microsoft Skype Empresarial
   b) Ejemplos de aplicaciones de protocolo pasivo son: Aplicación web de Microsoft Outlook, exploradores web

6. Dispositivo reforzado para implementación basada en DMZ
7. Añade valor mediante el uso de funciones principales adicionales de Citrix ADC ADC

   a) Conmutación de contenido
   b) Descarga SSL
   c) Reescritura
   d) Seguridad (NetScaler ADC AAA)

Para casos basados en protocolos activos, puede conectarse a Office 365 y proporcionar sus credenciales. Microsoft Federation Gateway se pone en contacto con el servicio ADFS (a través del proxy ADFS) en nombre del cliente de protocolo activo. A continuación, la puerta de enlace envía las credenciales mediante la autenticación básica (401). NetScaler ADC gestiona la autenticación del cliente antes de acceder al servicio ADFS. Tras la autenticación, el servicio ADFS proporciona un token SAML a Federation Gateway. Federation Gateway, a su vez, envía el token a Office 365 para proporcionar acceso al cliente.

Para los clientes pasivos, el ADFS Proxy StyleBook crea una cuenta de usuario de delegación restringida de Kerberos (KCD). La cuenta KCD es necesaria para que la autenticación SSO de Kerberos se conecte a los servidores ADFS. El StyleBook también genera una directiva de LDAP y una directiva de sesión. Estas directivas se vinculan posteriormente al servidor virtual AAA de NetScaler ADC que gestiona la autenticación de los clientes pasivos.

El StyleBook también puede garantizar que los servidores DNS del NetScaler ADC estén configurados para ADFS.

La sección de configuración que aparece a continuación describe cómo configurar NetScaler ADC para gestionar la autenticación de clientes basada en protocolos activa y pasiva.

### Detalles de configuración

La siguiente tabla muestra las versiones de software mínimas necesarias para que esta integración se implemente correctamente.

| Producto | Versión mínima requerida |
|---|---|
| Citrix ADC | 11.0, Licencia avanzada/premium |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

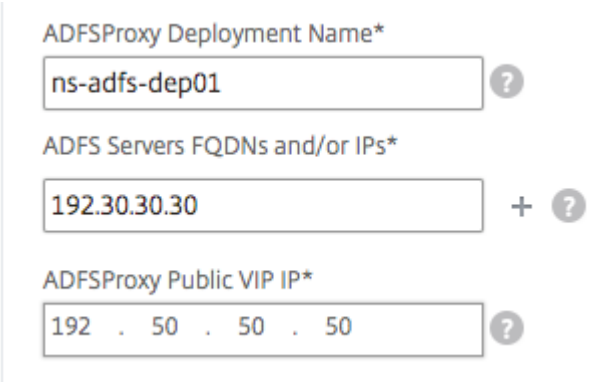
En las instrucciones siguientes se supone que ya ha creado las entradas DNS externas e internas adecuadas.

### Implementación de configuraciones de StyleBook de proxy ADFS de Microsoft desde NetScaler ADM

Las siguientes instrucciones le ayudarán a implementar el proxy StyleBook de Microsoft ADFS en su red empresarial.

#### Para implementar el proxy StyleBook de Microsoft ADFS

1. En Citrix ADM, vaya a **Aplicaciones** > **StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks disponibles para su uso en Citrix ADM.
2. Desplázate hacia abajo y busca el **proxy de Microsoft ADFS StyleBook**. Haga clic en **Crear configuración**.
   El StyleBook se abre como una página de interfaz de usuario en la que puede escribir los valores de todos los parámetros definidos en este StyleBook.
3. Escriba los valores de los siguientes parámetros:
   a) **Nombre de implementación del proxy ADFS**. Seleccione un nombre para la configuración de proxy ADFS implementada en su red.
   b) **FQDN o IP de los servidores ADFS**. Escriba las direcciones IP o los FQDN (nombres de dominio) de todos los servidores ADFS de la red.
   c) **IP VIP pública de ADFS Proxy**. Escriba la dirección IP virtual pública en el NetScaler ADC que funciona como un servidor proxy ADFS.

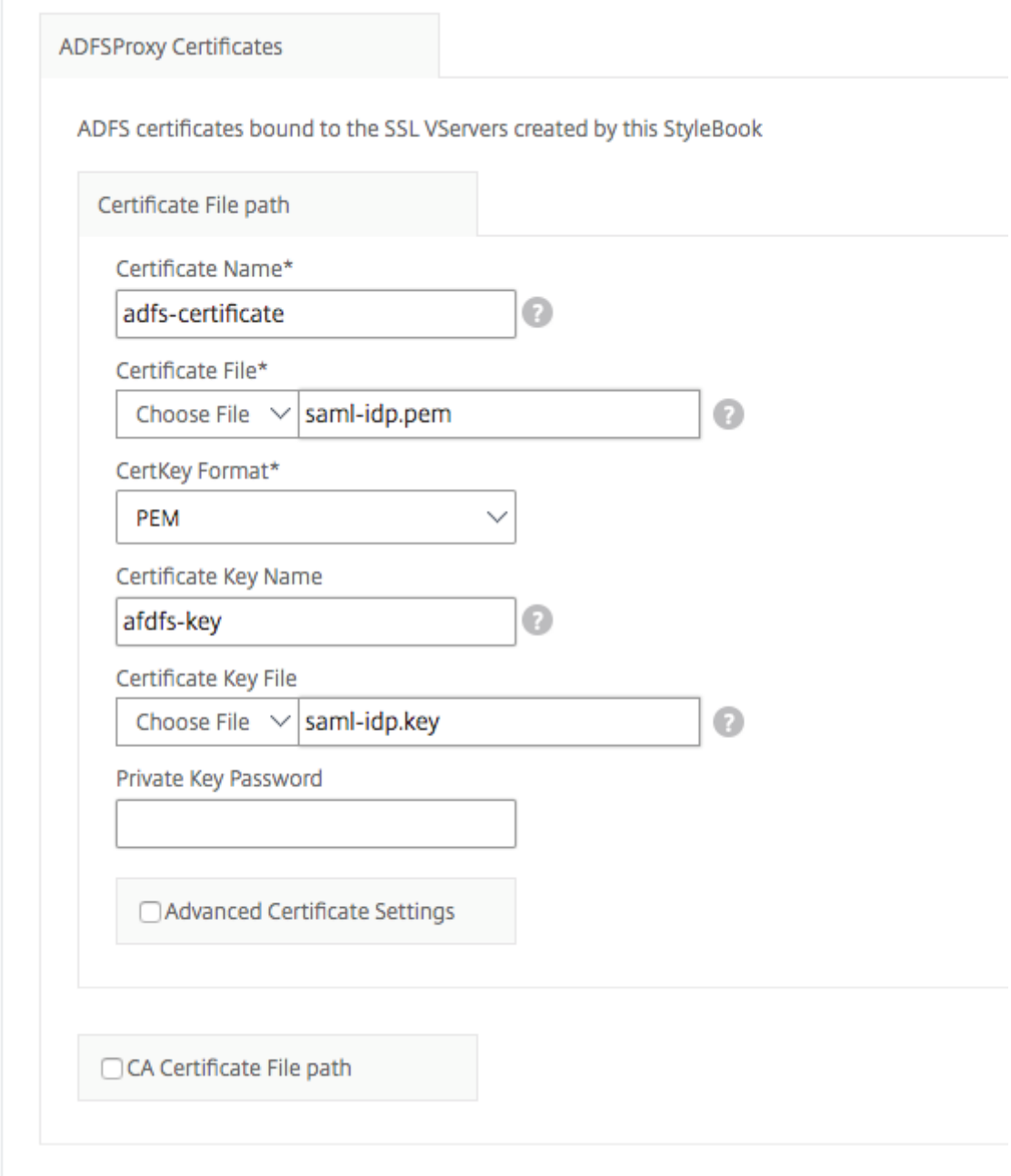



4. En la sección **Certificados de proxy ADFS**, escriba los detalles del certificado SSL y la clave de certificado.

   Este certificado SSL está enlazado a todos los servidores virtuales creados en la instancia de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Selecciona los archivos correspondientes de tu carpeta de almacenamiento local. También puede escribir la contraseña de clave privada para cargar claves privadas cifradas en formato.pem.




También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede escribir detalles como el período de notificación de caducidad del certificado, habilitar o inhabilitar el monitor de caducidad del certificado.

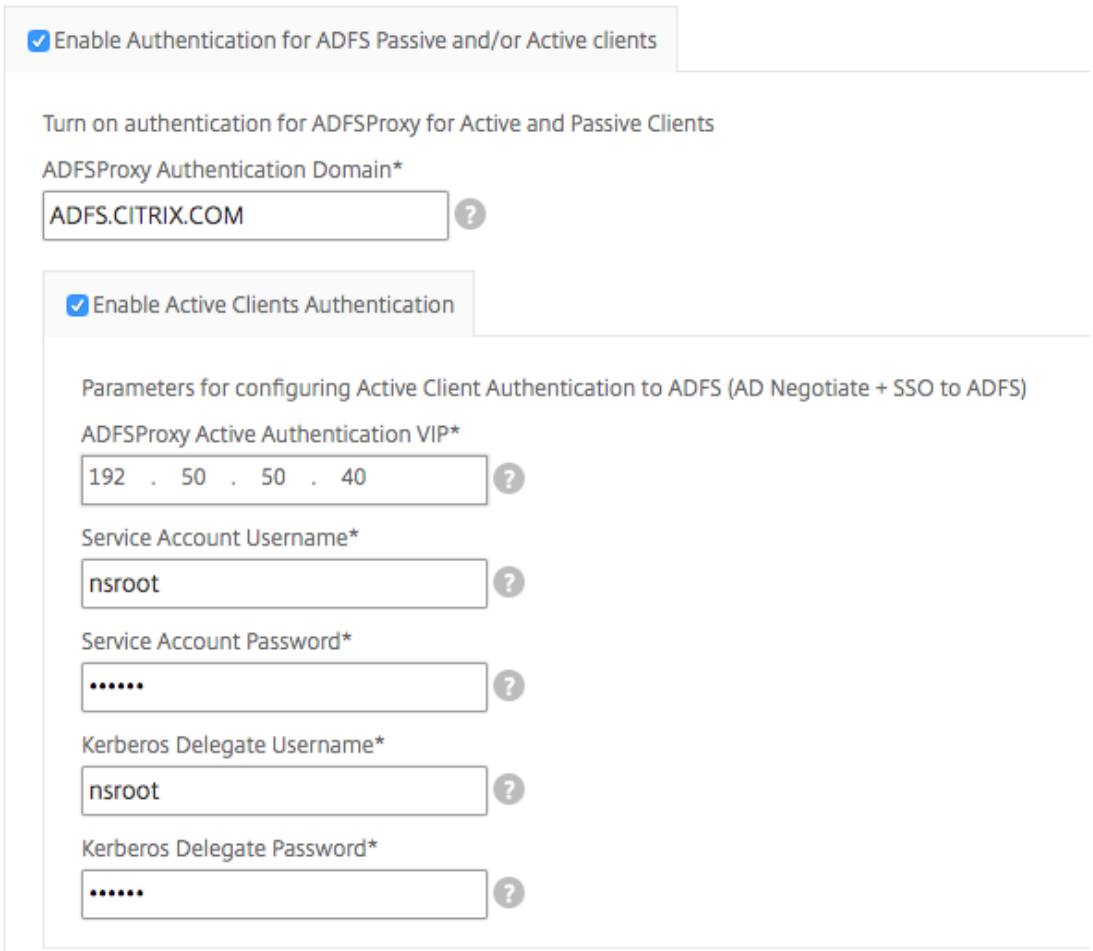
5. Opcionalmente, puede activar la casilla de verificación **Certificado de CA SSL** si el certificado SSL requiere que se instale un certificado público de CA en NetScaler ADC. Asegúrese de seleccionar **Es un certificado de CA** en la sección **Configuración avanzada del certificado**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Habilitar la autenticación para clientes activos y pasivos. Escriba el nombre de dominio DNS utilizado en Active Directory para la autenticación de usuarios. A continuación, puede configurar la autenticación para los clientes activos o pasivos, o para ambos.
7. Escriba los siguientes detalles para habilitar la autenticación para los clientes activos:

> **Nota**
>
> Es opcional configurar el soporte para los clientes activos.

   a) **Autenticación activa del proxy ADFS VIP**. Escriba la dirección IP virtual del servidor de autenticación virtual en la instancia de NetScaler ADC a la que se redirige a los clientes activos para la autenticación.
   b) Nombre de**usuario de cuenta de servicio** Escriba el nombre de usuario de la cuenta de servicio que utiliza NetScaler ADC para autenticar a los usuarios en el directorio activo.
   c) **Contraseña de cuenta de servicio** Escriba la contraseña utilizada por NetScaler ADC para autenticar a los usuarios en el directorio activo.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. Configure la autenticación para clientes pasivos habilitando la opción correspondiente y configurando la configuración de LDAP.

> **Nota**
>
> Es opcional configurar el soporte para clientes pasivos.

Escriba los siguientes detalles para habilitar la autenticación para los clientes pasivos:

a) **Base LDAP (Active Directory)**. Escriba el nombre de dominio base del dominio en el que residen las cuentas de usuario en Active Directory (AD) para permitir la autenticación. Por ejemplo, dc=netscaler, dc=com

b) **DN de enlace de LDAP (Active Directory)**. Agregue una cuenta de dominio (mediante una dirección de correo electrónico para facilitar la configuración) que tenga privilegios para examinar el árbol de AD. Por ejemplo, cn=Manager, dc=netscaler, dc=com

c) **Contraseña de DN de enlace LDAP (Active Directory)**. Escriba la contraseña de la cuenta de dominio para la autenticación.

Algunos otros campos que debe escribir en los valores de esta sección son los siguientes:

d) **IP del servidor LDAP (Active Directory)**. Escriba la dirección IP del servidor de Active Directory para que la autenticación de AD funcione correctamente.

e) ****Nombre** de FQDN **del servidor LDAP. Escriba el nombre de FQDN del servidor de Active Directory. El nombre FQDN es opcional. Proporcione la dirección IP tal como se indica en el paso 1 o el nombre del FQDN.

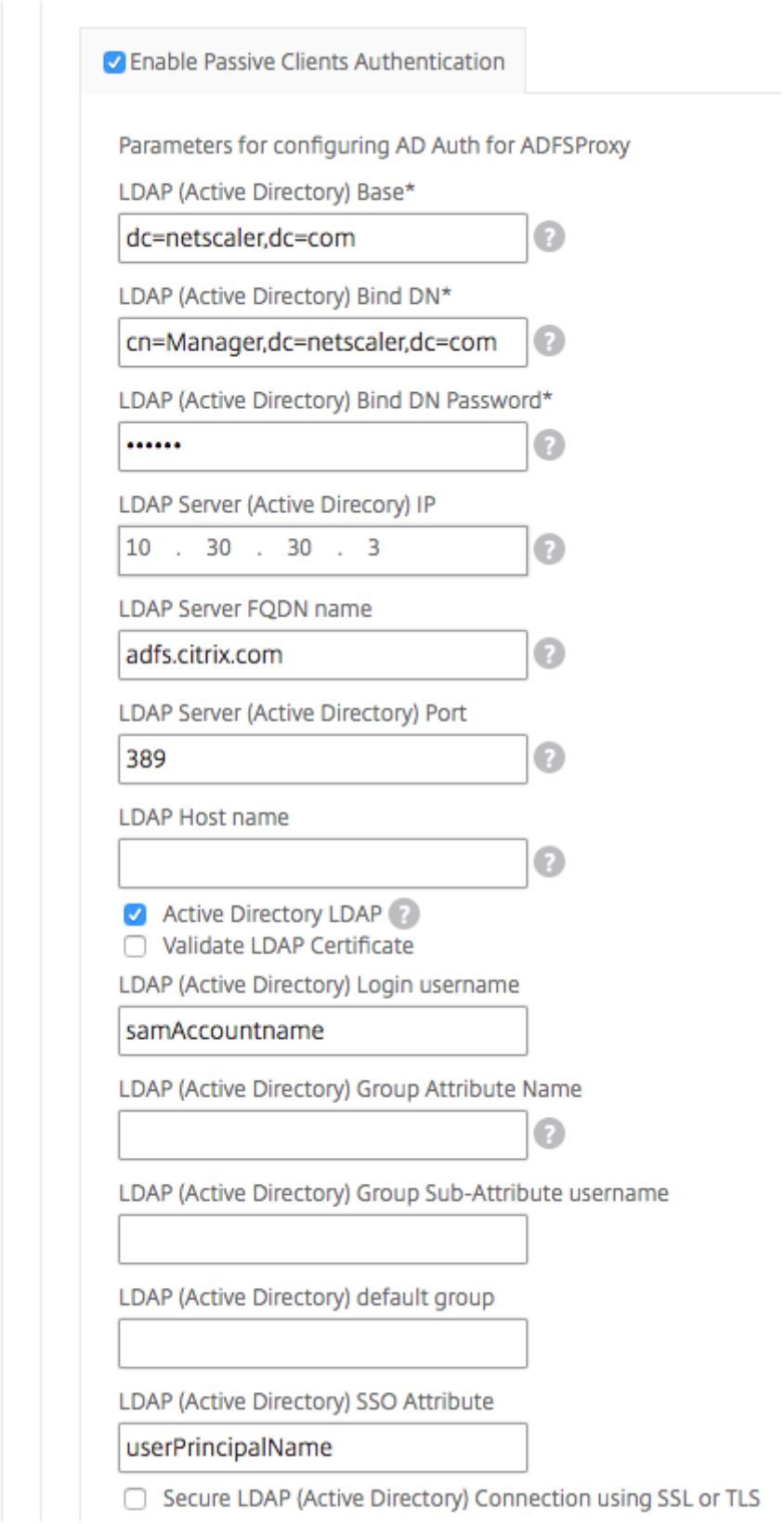
f) **Puerto de Active Directory del servidor LDAP**. De forma predeterminada, los puertos TCP y UDP del protocolo LDAP son 389, mientras que el puerto TCP del LDAP seguro es 636.

g) Nombre de**usuario de inicio de sesión LDAP (Active Directory)**. Escriba el nombre de usuario como “samAccountName”.

h) **Autenticación pasiva de proxy ADFS VIP**. Escriba la dirección IP del servidor virtual proxy ADFS para clientes pasivos.

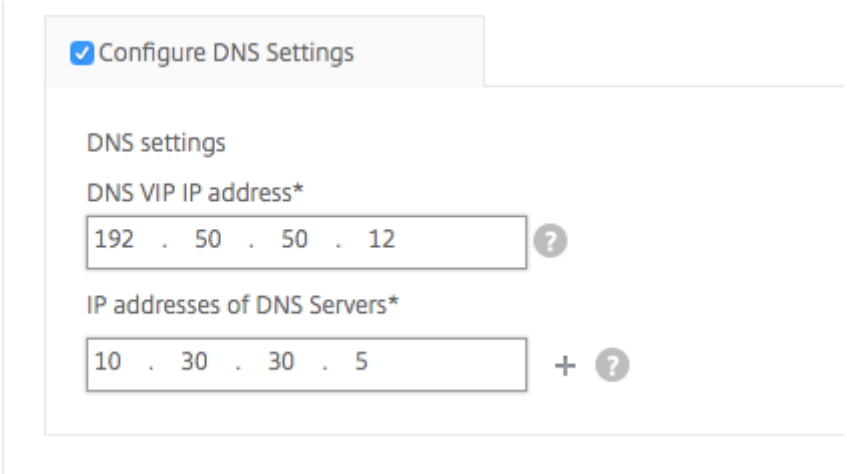
> **Nota**
>
> Los campos marcados con “*”son obligatorios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

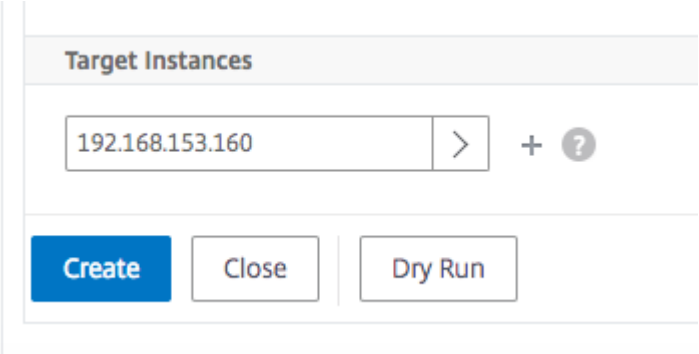



9. Opcionalmente, también puede configurar un VIP DNS para sus servidores DNS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




10. Haga clic en **Instancias de destino** y seleccione las instancias de NetScaler ADC para implementar esta configuración de proxy ADFS de Microsoft. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.




> **Nota:**
>
> Citrix recomienda que, antes de ejecutar la configuración real, seleccione **Ejecución en seco**. En primer lugar, puede ver los objetos de configuración que el StyleBook crea en las instancias NetScaler ADC de destino. A continuación, puede hacer clic en **Crear** para implementar la configuración en las instancias seleccionadas.

### Objetos creados

Se crean varios objetos de configuración cuando la configuración del proxy ADFS se implementa en la instancia de NetScaler ADC. La siguiente imagen muestra la lista de objetos creados.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Type : systemfile**

**filecontent :**
LS0tLS1CRUdJTiBDRVJUSUZjQ0FURS0tLS0tCk1jSURtVENDQW9HZ0F3SUjBZ0iCQXpBTkjna3Foa2lHOXcwQkFRc0ZB
VFHRXJKVVk6RWN1NQ1FHQ1NxR1NjYjNEUVKQVjZWApVzkxW7JWVbUxXTmhRR0ZqYldVzFKyOXljQzVzYjIwbEZEQy
1URXIPVEExTVRrd05Wb1hEVEI5TVRFeU9EQTFNVGt3TlZvd2dZZ3gKR0RBV0JnTlZCQU1NRDNsdmRXTmxaaTF6WVcx
FRa0jGaGw1YjNWalpXWXRjMkZ0YkvCaFkyMWxMV052Y25BdVkyOXRNUkI3CkVBWURWUVFLREFsQlEwMUZMVU5
GQUFPQ0FROEFNSUICQ2dLQ0FRRUF5L1gza0VCd2F05EpoQmFKR2Z6WmwxQ1FkZ2jtbDFlYgpzT3hadG4xOHNp5
9hNXQCHNmeG56K2RvbjyaUHaktEazVPYkF5cmd2NVNHaGhmL3pwQVpDa3MybkVocjh6JEIxOWoKQm8wc3NlTl
HV3VlpBakQxVitnNTVHSkdXMW9ubndyTlc0Q3ViTzMyRTFDNjh1WG1TZnlwdUlzTzlvRDF2Znov5Dh0QlM4CjFlV0Vla
0R8SkjnTiZiUk1FQWpBQU1Bc0dBMVVkRHdRRUF3SUY0REFOQmdrcWhraUc5dzBCQVFzRkFBT0NBUUVBbk1RSQpz
KOGc3CjNlUzlkbE15UkUxeXh4N3V5SXpqR0ZaV1VBcllMxL09PcUxGRHR2NEFZWXZ6UVhGL0pWM2phWjZnUkdMS0
zFRzNHdVYndgoxRW11MlNNcWxbGVVcIN5QXBuSlVWNHA0QTVDbTh6LTRVVDHzEZQRKU2THRTHZCYzhW0UjvR
N8Ves1azE1NVZSd2UKaWt3OFYzR082MmdRc0hvV05RPT0KLS0tLS1FTkQgQ0VSVEIGSUNBVEUtLS0tLQo=

**fileencoding :** BASE64
**fileiocation :** /nsconfig/ssl
**filename :** saml-idp.pem

**Type : systemfile**

**filecontent :**
LS0tLS1CRUdJTiBSU0EgUFJjVkFURSBLRVktLS0tLQpNSUIFcEFjQkFBS0NBUUVBe59YM2tFQndhdEhKaEjhV0dmelpsM
Q2eWjWY1NzajFiT0JEdU9CbVpnR59LQ59kNXjCOHNmeG4KeitKb24ycmlIR2pLRGs1T2jBUnjndjYTR2hoZI96b0FaQ2t
8hTU1tV3dyQmN0OUhKdEjxEpVUHV3VlpBakQxVitnNTVHCkpHVzFvbmS3ckSXNEN1Yk8zMkLxQzY4dvhtUJZyMH
hdbW1YT2tLb0JWaXdjREFRQUJBb0ICQUVtS1FGOEV2LVBtNXceAo3T0VsNKjlRTK3RjL2NEhtRnFjVjFpc1VoLZQ2Y2h2
WTUdnTHBZcDYwR59DcFFQdkhyNEJSS3hiVXBvQkpaZ0g0eloKRHZjT1dadJjtc0hXYVBkUmoxVDNaaHdsd21aMEQ4U
wrSXBBRHJybkdOdUNHMId4NUorNHM3VG9aMXYzc1NtRThaK2pqdWtYCk5DTFBKcnh3dFJlSXc3ajRTlenlDNWFCR1N
1RrZHhTc2ZPbFE5THgwYUNQWnFWNCQVkoycThzbkpvMXhjOW1dE9mRlBNVApGRHZNYXZwKybHQnpWTysRWT
wWDA2NWI5TnZYYnkvQkIqWDgyYkhTNlIlTjFWR2o2RVFYQmtrNmjmSXNDZ1IFQXpNQ2kKMkFhd0FTY3hTT0Q1Zm
1PZTNPU2dVMWh4WmNDdjIuMGhNNEdWVVQyVFhqWkZNWWFBWk8yNjFwdWVKbTRkMXZqdDY3CjJrN0tVclhpY
iMzgxNWStUmpyZTFrK21QN2tuL0xFQk1pVUVXV0tybXpFanRsbzhRTFhXVjZzU3ItVXjCVU11bnVLWgo1Y1BSbFdFTE
VCcUwwQjh5a0djUGVUbkRS3dLQmdRQ0BME1BMxNrazdXkpsa08bxb05/TDhrUGNYUZzckJURIBsL0QKRTcva1AvT
GR1Blb3NJK3FxQWw1aktiY3AxMFZYNUj1cS9xbm9vREVkN2d0NGNFcEM0RTUvQW85VThGWVVGR3JpcC9wdGwxC
EeloKUmlIWXlWUnRkbkU5TE5kYU5STXdpTWFCYkhFazF4R1lx5DByQnFEYUE0M184Zm9FYjdndEdCaHE2azRUempa
otLS0tLUVORCBSU0EgUFJjVkFURSBLRVktLS0tLQo=

**fileencoding :** BASE64
**fileiocation :** /nsconfig/ssl
**filename :** saml-idp.key

**Type : sslcertkey**

**cert :** saml-idp.pem
**certkey :** adfs-certificate
**inform :** PEM
**key :** saml-idp.key


© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Objects Added on Instance : 192.168.153.160 | Count : 57**

**Type : nsfeature**

**Meta Properties**
action : **enable**

**feature :** cs lb ssl rewrite aaa

**Type : lbvserver**

**ipv46 :** 192.50.50.12
**name :** ns-adfs-dep01-adfs-dns
**port :** 53
**servicetype :** DNS

**Type : service**

**ip :** 10.30.30.5
**name :** ns-adfs-dep01-dns-svc-1
**port :** 53
**servicetype :** DNS

**Type : lbvserver_service_binding**

**name :** ns-adfs-dep01-adfs-dns
**servicename :** ns-adfs-dep01-dns-svc-1

**Type : authenticationnegotiateaction**

**domain :** ADFS.CITRIX.COM
**domainuser :** nsroot
**domainuserpasswd :** nsroot
**name :** ns-adfs-dep01-negotiate-action

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : authenticationpolicy

**action :** ns-adfs-dep01-negotiate-action
**name :** ns-adfs-dep01-negotiate-policy
**rule :** true

### Type : aaakcdaccount

**delegateduser :** nsroot
**kcdaccount :** ns-adfs-dep01-adfs-auth401-kcd-
**kcdpassword :** nsroot
**realmstr :** ADFS.CITRIX.COM

### Type : tmsessionaction

**kcdaccount :** ns-adfs-dep01-adfs-auth401-kcd-
**name :** ns-adfs-dep01-adfs-auth401-tmsession-action
**persistentcookie :** ON
**persistentcookievalidity :** 3
**sso :** ON

### Type : tmsessionpolicy

**action :** ns-adfs-dep01-adfs-auth401-tmsession-action
**name :** ns-adfs-dep01-adfs-auth401-tmsession-policy
**rule :** ns_true

### Type : authenticationvserver

**authenticationdomain :** ADFS.CITRIX.COM
**failedlogintimeout :** 1
**ipv46 :** 192.50.50.40
**maxloginattempts :** 255
**name :** ns-adfs-dep01-adfs-auth401-auth-vserver
**port :** 443
**servicetype :** SSL

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-adfs-auth401-auth-vserver

### Type : authenticationvserver_authenticationpolicy_binding

**name :** ns-adfs-dep01-adfs-auth401-auth-vserver
**policy :** ns-adfs-dep01-negotiate-policy
**priority :** 10

### Type : authenticationvserver_tmsessionpolicy_binding

**name :** ns-adfs-dep01-adfs-auth401-auth-vserver
**policy :** ns-adfs-dep01-adfs-auth401-tmsession-policy
**priority :** 10

### Type : authenticationldapaction

**authentication :** ENABLED
**authtimeout :** 30
**followreferrals :** OFF
**ldapbase :** dc=netscaler,dc=com
**ldapbinddn :** cn=Manager,dc=netscaler,dc=com
**ldapbinddnpassword :** nsroot
**ldaploginname :** samAccountname
**name :** ns-adfs-dep01-ldap-action
**passwdchange :** DISABLED
**sectype :** PLAINTEXT
**serverip :** 10.30.30.3
**serverport :** 389
**ssonameattribute :** userPrincipalName
**svrtype :** AD
**validateservercert :** NO

### Type : authenticationpolicy

**action :** ns-adfs-dep01-ldap-action
**name :** ns-adfs-dep01-ldap-policy
**rule :** true

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : aaakcdaccount

**kcdaccount :** ns-adfs-dep01-adfs-ldap-kcd-acc
**realmstr :** ADFS.CITRIX.COM

### Type : tmsessionaction

**kcdaccount :** ns-adfs-dep01-adfs-ldap-kcd-acc
**name :** ns-adfs-dep01-adfs-ldap-tmsession-action
**persistentcookie :** OFF
**sso :** ON

### Type : tmsessionpolicy

**action :** ns-adfs-dep01-adfs-ldap-tmsession-action
**name :** ns-adfs-dep01-adfs-ldap-tmsession-policy
**rule :** ns_true

### Type : authenticationvserver

**authenticationdomain :** ADFS.CITRIX.COM
**failedlogintimeout :** 1
**ipv46 :** 192.50.50.30
**maxloginattempts :** 255
**name :** ns-adfs-dep01-adfs-ldap-auth-vserver
**port :** 443
**servicetype :** SSL

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-adfs-ldap-auth-vserver

### Type : authenticationvserver_authenticationpolicy_binding

**name :** ns-adfs-dep01-adfs-ldap-auth-vserver
**policy :** ns-adfs-dep01-ldap-policy
**priority :** 10

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : authenticationvserver_tmsessionpolicy_binding

**name :** ns-adfs-dep01-adfs-ldap-auth-vserver
**policy :** ns-adfs-dep01-adfs-ldap-tmsession-policy
**priority :** 10

### Type : csvserver

**ipv46 :** 192.50.50.50
**name :** ns-adfs-dep01-cs
**port :** 443
**servicetype :** SSL

### Type : lbvserver

**ipv46 :** 192.50.50.50
**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
**port :** 445
**servicetype :** SSL

### Type : servicegroup

**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
**servicetype :** SSL

### Type : lbvserver_servicegroup_binding

**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

### Type : server

**ipaddress :** 192.30.30.30
**name :** 192.30.30.30

### Type : servicegroup_servicegroupmember_binding

**ip :** 192.30.30.30
**port :** 443
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

### Type : csaction

**name :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
**targetlbvserver :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

### Type : cspolicy

**action :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
**rule :** HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

### Type : csvserver_cspolicy_binding

**name :** ns-adfs-dep01-cs
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
**priority :** 9800

### Type : lbvserver

**appflowlog :** ENABLED
**authentication :** ON
**authenticationhost :** ADFS.CITRIX.COM
**authn401 :** OFF
**authnvsname :** ns-adfs-dep01-adfs-ldap-auth-vserver
**downstateflush :** ENABLED
**ipv46 :** 192.50.50.50
**lbmethod :** LEASTCONNECTION
**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
**port :** 446
**servicetype :** SSL

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : servicegroup

**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
**servicetype :** SSL

### Type : lbvserver_servicegroup_binding

**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

### Type : servicegroup_servicegroupmember_binding

**ip :** 192.30.30.30
**port :** 443
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

### Type : csaction

**name :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
**targetlbvserver :** ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

### Type : cspolicy

**action :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
**rule :** HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

### Type : csvserver_cspolicy_binding

**name :** ns-adfs-dep01-cs
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
**priority :** 9900

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : lbvserver

**appflowlog :** ENABLED
**authentication :** OFF
**authn401 :** ON
**authnvsname :** ns-adfs-dep01-adfs-auth401-auth-vserver
**downstateflush :** ENABLED
**ipv46 :** 192.50.50.50
**lbmethod :** LEASTCONNECTION
**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
**port :** 444
**servicetype :** SSL

### Type : servicegroup

**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
**servicetype :** SSL

### Type : lbvserver_servicegroup_binding

**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

### Type : servicegroup_servicegroupmember_binding

**ip :** 192.30.30.30
**port :** 443
**servicegroupname :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

### Type : csaction

**name :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
**targetlbvserver :** ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Type : cspolicy

**action :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
**rule :** true

### Type : csvserver_cspolicy_binding

**name :** ns-adfs-dep01-cs
**policyname :** ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
**priority :** 10000

### Type : sslvserver_sslcertkey_binding

**certkeyname :** adfs-certificate
**vservername :** ns-adfs-dep01-cs

### Type : rewritepolicylabel

**labelname :** ns-adfs-dep01-request-rewritepolicylabel
**transform :** HTTP_REQ

### Type : rewritepolicylabel

**labelname :** ns-adfs-dep01-response-rewritepolicylabel
**transform :** HTTP_RES

### Type : rewriteaction

**name :** ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
**stringbuilderexpr :** "/adfs/services/trust/proxymex"
**target :** HTTP.REQ.URL
**type :** REPLACE

### Type : rewritepolicy

**action :** ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
**name :** ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
**rule :** HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Type : rewritepolicylabel_rewritepolicy_binding**

**gotopriorityexpression :** END
**labelname :** ns-adfs-dep01-request-rewritepolicylabel
**policyname :** ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
**priority :** 10

**Type : lbvserver_rewritepolicy_binding**

**bindpoint :** REQUEST
**gotopriorityexpression :** END
**invoke :** true
**labelname :** ns-adfs-dep01-request-rewritepolicylabel
**labeltype :** policylabel
**name :** ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
**policyname :** NOPOLICY-rewrite
**priority :** 10

## StyleBook del negocio electrónico de Oracle

January 30, 2024

Oracle E-Business Suite es el conjunto más completo de aplicaciones empresariales globales e integradas. Esta suite permite a las organizaciones tomar mejores decisiones, reducir los costes y aumentar el rendimiento, y consta de las siguientes aplicaciones.

- Planificación de recursos empresariales (ERP)
- Gestión de relaciones con los clientes (CRM)
- Gestión de la cadena de suministro (SCM)

Estas aplicaciones informáticas son desarrolladas o adquiridas por Oracle. El StyleBook de Oracle E-Business Suite 12.2 le permite implementar la configuración en las instancias de NetScaler ADC seleccionadas.

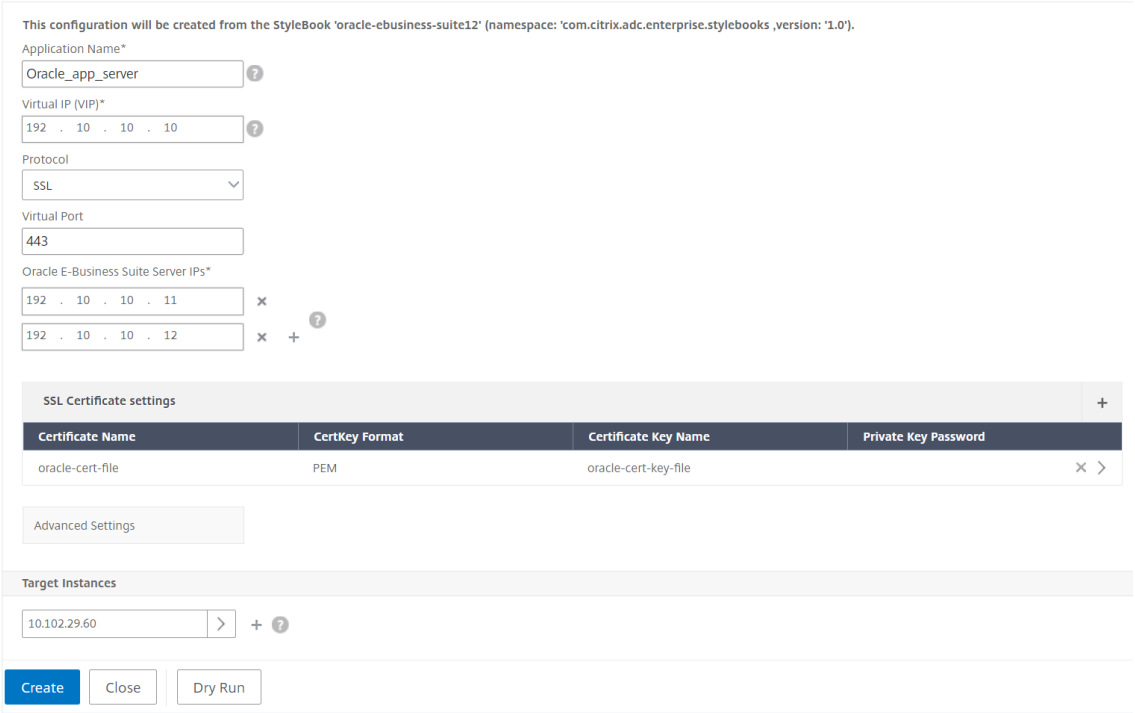
Este StyleBook crea una configuración de equilibrio de carga que incluye un servidor virtual de equilibrio de carga, un grupo de servicios y una lista de servicios. También vincula los servicios al grupo de servicios y enlaza el grupo de servicios al servidor virtual. Puede elegir la comunicación cifrada seleccionando SSL y proporcionando los archivos SSL y los archivos clave de su sistema local.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Para crear una configuración para Oracle E-Business Suite 12.2

1. En NetScaler Application Delivery Management (ADM), vaya a **Aplicaciones** > **Configuración > StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks que están disponibles en su NetScaler ADM. Desplácese hacia abajo y seleccione **Oracle E-Business Suite 12.2**. También puede utilizar la opción de búsqueda para buscar en el StyleBook.
2. Haga clic en **Crear configuración** en el panel StyleBook.
3. Escriba el nombre de la aplicación del balanceador de carga y la dirección IP virtual en la sección de configuración del balanceador de carga.
4. Seleccione el protocolo requerido. Aquí tiene dos opciones: HTTP y HTTPS/SSL. También puede escribir el número de puerto.
5. Escriba las direcciones IP de todos los servidores de aplicaciones de Oracle E-Business Suite de la red que van a equilibrar la carga. Haga clic en **+** para agregar más direcciones IP de servidor.
6. En la sección **Configuración de certificados SSL**, selecciona los archivos correspondientes de tu almacenamiento local. También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede configurar más detalles, como el período de notificación de caducidad del certificado. También puede habilitar o inhabilitar el monitor de caducidad de los certificados.

   Seleccione la instancia de NetScaler ADC de destino en la que debe crearse la configuración y haga clic en **Crear**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Sugerencia**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana. El icono de actualización solo está disponible actualmente en Citrix ADM.

## StyleBooks de Citrix StoreFront

January 30, 2024

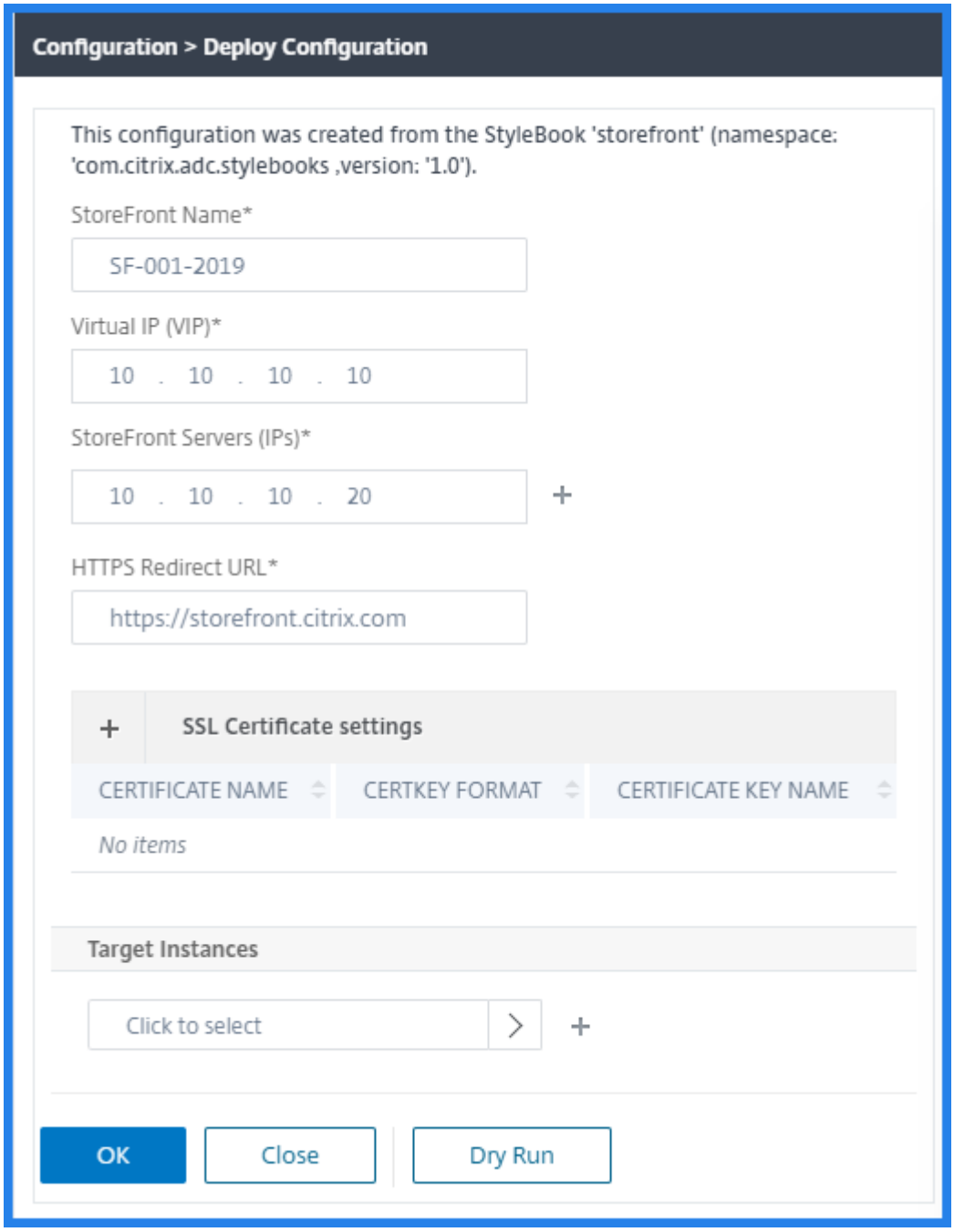
StoreFront es una tienda de aplicaciones empresariales que reúne aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en una única tienda para los usuarios. StoreFront autentica a los usuarios en los sitios que alojan recursos y administra las tiendas de aplicaciones y los escritorios a los que acceden los usuarios. Alberga la tienda de aplicaciones de su empresa, lo que le permite ofrecer a los usuarios acceso de autoservicio a las aplicaciones y escritorios que pone a su disposición.

Este StyleBook define las configuraciones de NetScaler ADC para los servidores StoreFront. Con este StyleBook, puede configurar servidores StoreFront para las instancias de NetScaler ADC deseadas. Puede elegir la comunicación cifrada seleccionando SSL y proporcionando los archivos SSL y los archivos clave de su sistema local.

### Crear una configuración para las aplicaciones Citrix StoreFront

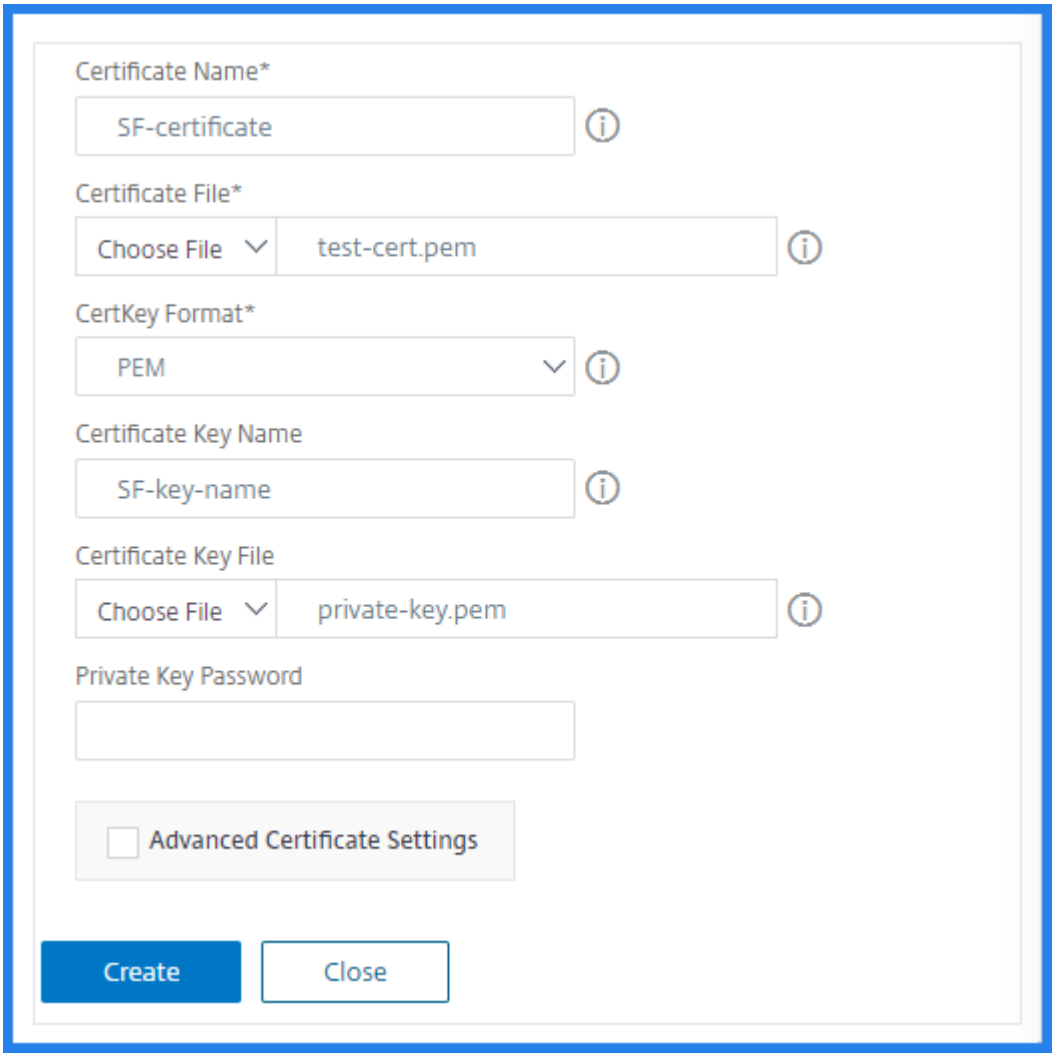
1. En la GUI de NetScaler ADM, vaya a **Aplicaciones > StyleBooks**.
2. En la barra de búsqueda, utilice las propiedades **del nombre** y busque `Citrix StoreFront`.
3. En el StyleBook de Citrix StoreFront, haga clic en Crear configuración.
4. Especifique los siguientes detalles:
   - Nombre de**StoreFront: especifique el nombre**de StoreFront. El ConfigPack de StoreFront se crea con el mismo nombre de StoreFront.
   - **IP virtual (VIP)**: especifique la dirección IP virtual en la que la instancia de Citrix ADC recibe las solicitudes de los clientes.
   - **Servidores**StoreFront : especifique las direcciones IP de los servidores StoreFront que quiere configurar con una instancia de Citrix ADC.
   - **URL de redireccionamiento de HTTPS**: especifique la URL de HTTPS a la que se redirigen las solicitudes de HTTPS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. En la sección **Configuración de certificados SSL**, introduzca los nombres del certificado SSL y la clave del certificado.
6. Selecciona los archivos correspondientes de tu carpeta de almacenamiento local. También puede escribir la contraseña de la clave privada para especificar las claves privadas cifradas en formato PEM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




7. También puede habilitar la casilla de verificación **Configuración avanzada de certificados**. Aquí puede introducir detalles como el período de notificación de caducidad del certificado, activar o desactivar el monitor de caducidad del certificado.
8. Si lo desea, seleccione la casilla **Certificado de CA SSL para la IP virtual de autenticación** si el certificado SSL requiere la instalación de un certificado público de CA en Citrix ADC. Asegúrese de elegir **Es un certificado de CA** en la sección **Configuración avanzada del certificado**.
9. Haga clic en **Crear**.
10. Haga clic en **Instancias** de destino y seleccione las instancias de Citrix ADC en las que quiere configurar los servidores StoreFront.
11. Haga clic en **Crear** para crear la configuración e implementar la configuración en las instancias de NetScaler ADC seleccionadas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Crear y utilizar StyleBooks personalizados

January 30, 2024

Puede escribir su propio StyleBook para su implementación, importarlo a Citrix Application Delivery Management (ADM) y crear objetos de configuración. También puede usar la API para crear configuraciones desde sus StyleBooks.

Este documento incluye la siguiente información:

## Antes de comenzar

Antes de empezar a crear StyleBooks, asegúrese de tener conocimiento de lo siguiente:

- API de NITRO. Para obtener más información, consulte la documentación de la APIde
- YAML

Los archivos StyleBook utilizan el formato YAML. Para obtener información sobre el formato YAML, consulte Sintaxis YAML.

La siguiente es una lista de pautas de YAML que debe tener en cuenta al crear StyleBooks:

- YAML distingue mayúsculas de minúsculas
- YAML requiere una indentación adecuada
- Utilice la tecla <spacebar> para crear una indentación adecuada. No utilice la tecla <tab>. El uso de la tecla <tab> crea un error de compilación al importar su StyleBook a MA Service.
- No utilice cadenas entre comillas. Incluya la cadena entre comillas únicamente si la cadena contiene signos de puntuación (guiones, dos puntos, etc.). Si quiere interpretar un número como una cadena, inclúyalo entre comillas o utilice la función integrada str () de StyleBooks.
- Los literales como sí/sí/sí/y/no/no/no/n/n, encendido/encendido/apagado/apagado/apagado y verdadero/verdadero/falso/falso/falso/falso se consideran booleanos y equivalen a verdadero y falso, respectivamente. Para interpretarlas como cadenas, inclúyalas entre comillas. Por ejemplo:
  - “SÍ”
  - “No”
  - “Cierto”
  - “Falso”y así sucesivamente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Antes de importar el archivo de StyleBook a NetScaler ADM, se recomienda que valide si el archivo es compatible con el formato YAML. Citrix recomienda utilizar el validador YAML integrado en StyleBooks para validar e importar el contenido YAML.
>
> Al configurar StyleBooks, solo puede usar recursos de configuración de Nitro que admitan las operaciones **Create** y **Delete** (métodos POST y DELETE HTTP). Para obtener más información, consulte la documentación de API de Nitro.

## Anatomía de un StyleBook

Escribir StyleBooks requiere que comprenda la gramática, la sintaxis y la estructura de los StyleBooks. Un StyleBook típico tiene las siguientes secciones:

- **Encabezado**: esta sección permite definir la identidad de un StyleBook y describir su función. Se trata de una sección obligatoria.
- **Importar StyleBooks**: esta sección le permite declarar a qué otros StyleBook quiere hacer referencia desde su StyleBook actual. Es necesario importar la configuración de NetScaler ADC NITRO, StyleBooks u otros StyleBooks para escribir un StyleBook. Se trata de una sección obligatoria.
- **Parámetros**: esta sección le permite definir los parámetros que necesita en su StyleBook para crear una configuración. Describe la entrada que toma su StyleBook. Se trata de una sección opcional.
- **Componentes**: esta sección le permite definir las entidades (objetos de configuración) que crea el StyleBook para una configuración específica. Esta sección se considera el núcleo de un StyleBook. Los componentes suelen utilizar la entrada proporcionada en la sección de parámetros para adaptar la configuración generada por el StyleBook. Se trata de una sección opcional.

  Un StyleBook puede tener una sección de parámetros, una sección de componentes o ambas. Un StyleBook con solo la sección de parámetros es útil para definir una lista de parámetros que pueden usar otros StyleBooks. Esto promueve la reutilización de los grupos de parámetros en un conjunto de StyleBooks. Se puede usar un StyleBook con solo una sección de componentes cuando quiera especificar los valores de los atributos en el StyleBook en lugar de definir parámetros para tomar las entradas del usuario.
- **Salidas**: mientras que la sección de parámetros define las entradas del StyleBook, esta sección opcional define sus salidas. En esta sección de salidas opcionales, puede especificar los componentes que quiere exponer a los usuarios que creen una configuración a partir de este StyleBook y a otros StyleBooks que lo importen. Los usuarios que importen StyleBooks podrán entonces hacer referencia a las propiedades de los componentes expuestos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Operaciones**: un StyleBook puede contener una sección opcional para habilitar los análisis en NetScaler ADM en cualquier servidor virtual que forme parte del StyleBook.

La siguiente ilustración muestra un esquema simple de un StyleBook.

```
name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: name
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $parameters.name
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
```

Header

Import StyleBooks

Parameters

Components

Los siguientes ejemplos le ayudan a aprender sobre la gramática y la estructura de un StyleBook y cómo escribir StyleBooks con niveles cada vez mayores de complejidad.

- StyleBook para crear un servidor virtual de equilibrio de carga
- StyleBook para crear una configuración básica de equilibrio de carga
- Crear un StyleBook compuesto
- Personaliza su StyleBook usando atributos GUI

## StyleBook para crear un servidor virtual de equilibrio de carga

January 30, 2024

En este ejemplo, diseña un StyleBook básico que crea un servidor virtual de equilibrio de carga del tipo de protocolo HTTP y escucha en el puerto 80. Los parámetros del nombre del servidor virtual, la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

dirección IP y el método de equilibrio de carga aceptan valores definidos por el usuario, es decir, son los parámetros del StyleBook.

### Header

Las seis primeras líneas de un StyleBook forman la sección de cabecera. En este ejemplo, la sección de encabezado se escribe de la siguiente manera:

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
    configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
```

La sección del encabezado incluye los siguientes detalles:

- **nombre**: un nombre para este StyleBook.
- **description**: Una descripción que define lo que hace este StyleBook. Esta descripción aparece en NetScaler ADM.
- **display-name**: nombre descriptivo del StyleBook que aparece en NetScaler ADM.
- espacio de**nombres**: un espacio de nombres forma parte de un identificador único de un StyleBook para evitar colisiones de nombres.
- **schema-version**: siempre toma el valor “1.0”en esta versión.
- **version**: El número de versión del StyleBook. Puede cambiar el número de versión al actualizar el StyleBook.

La combinación de **nombre** , **espacio**de nombres y **versión** identifica de forma única un StyleBook en el sistema. No puede tener dos StyleBooks con la misma combinación de nombre, espacio de nombres y versión en NetScaler ADM. Sin embargo, puede tener dos StyleBooks con el mismo nombre y versión pero espacios de nombres diferentes, o con el mismo espacio de nombres y versión pero nombres diferentes.

> **Nota**
>
> Tenga en cuenta que ha actualizado su StyleBook y que tiene un número de versión actualizado. Ahora, si se refiere a (es decir, si va a importar) este StyleBook en otros StyleBooks, asegúrese de actualizar también el número de versión en otros StyleBooks, para que utilicen la versión correcta del StyleBook importado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Importar StyleBooks

La sección que sigue al encabezado se denomina “import-stylebooks”. En esta sección, debe declarar el espacio de nombres y el número de versión de cualquier otro StyleBook al que quiera hacer referencia en su StyleBook actual. Esto le permite importar y reutilizar otros StyleBooks en lugar de volver a crear la misma configuración en su propio StyleBook.

En este ejemplo, la sección de importación de libros de estilo se escribe de la siguiente manera:

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
```

Cada StyleBook debe hacer referencia al espacio de nombres netscaler.nitro.config si utiliza directamente cualquiera de los objetos de configuración NITRO. Este espacio de nombres contiene todos los tipos de NetScaler ADC NITRO, como lbvserver. Como se admiten las versiones de software 10.5 y posteriores, puede utilizar StyleBook para crear y ejecutar configuraciones en cualquier instancia de NetScaler ADC que ejecute la versión 10.5 y posterior.

El prefijo utilizado en la sección de libros de estilos de importación es una forma abreviada para hacer referencia a la combinación de espacio de nombres y versión. En este caso, ns hace referencia a netscaler.nitro.config de la versión 10.5. En las secciones posteriores del StyleBook, en lugar de utilizar el espacio de nombres y la versión para hacer referencia al StyleBook importado, puede utilizar la cadena de prefijo elegida, por ejemplo, ns, en el ejemplo anterior.

La versión utilizada en los StyleBooks es la versión NetScaler ADC NITRO. Se puede usar un StyleBook basado en la versión X de Nitro para configurar cualquier Citrix ADC de la versión X o superior.

> **Nota**
>
> Para garantizar que los StyleBooks se puedan usar para configurar cualquier instancia de Citrix ADC de la versión 10.5 o posterior, Citrix recomienda que, para obtener la máxima compatibilidad, importe el espacio de nombres Nitro 10.5 en los StyleBooks que usen directamente los StyleBooks integrados de Nitro (espacio de nombres: netscaler.nitro.config, versión: 10.5).

Es importante que un StyleBook que importe otros StyleBooks esté basado en una versión de Nitro igual o superior a la de los StyleBooks que importa. Por ejemplo, un StyleBook basado en la versión 10.5 de Nitro no puede depender de, usar o importar un StyleBook basado en la 11.1. Pero un StyleBook basado en la versión 11.1 puede importar un StyleBook basado en cualquier versión inferior a 11.1.

También es posible que un StyleBook no importe en absoluto el espacio de nombres de Nitro. Esto significa que un StyleBook no necesita definir directamente los componentes de Nitro, sino que puede

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

importar (depender de) los StyleBooks que definen los componentes de Nitro. El StyleBook que importa otros StyleBooks siempre adquiere la versión de Nitro más alta en la jerarquía de sus dependencias y, por lo tanto, podría usarse para configurar los ADC de Citrix que sean de esa versión o superior.

### Parámetros

La sección de parámetros le permite declarar todos los parámetros que necesita en su StyleBook. Usted, como desarrollador de StyleBook, tiene que decidir cuál es la entrada que quiere que especifiquen los usuarios de su StyleBook. En este ejemplo, ha creado su StyleBook de forma que requiere que sus usuarios proporcionen el nombre del servidor virtual, su dirección IP y el método de equilibrio de carga.

La sección de parámetros tendría el siguiente aspecto:

```
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Name of the application configuration.
  required: true

 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

-
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for
     load balancing client request between the application servers.
  allowed-values:
   - ROUNDROBIN
   - LEASTCONNECTION
   default: ROUNDROBIN
```

> **Nota**
>
> Si no proporciona la etiqueta de un parámetro, NetScaler ADM utilizará el atributo name al mostrar este parámetro. Siempre debe definir una etiqueta para los parámetros de modo que pueda controlar cómo se muestran en NetScaler ADM.
>
> Sin embargo, al utilizar las API, el parámetro se designa por su nombre.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En esta sección, ha declarado tres parámetros indicados por sus valores de atributos de **nombre**: **nombre** para el nombre del servidor virtual, **ip** para la dirección IP del servidor virtual y **lb-alg** para el método de equilibrio de carga.

- **type**. Tipo de valor que pueden tomar estos parámetros. Por ejemplo, name y lb-alg pueden tomar un valor de cadena y el valor ip debe ser del tipo ip address. Los parámetros de un StyleBook pueden ser de cualquiera de los siguientes tipos incorporados:
- **cadena**. Una variedad de personajes. Si no se especifica una longitud, el valor de cadena puede tener cualquier número de caracteres. Sin embargo, puede limitar la longitud de un tipo de cadena utilizando los atributos longitud mínima y longitud máxima.
- **número**. Un número entero. Puede especificar el número mínimo y máximo que puede tomar este tipo mediante los atributos valor mínimo y valor máximo.
- **booleano**. Puede ser verdadera o falsa. Además, ten en cuenta que YAML considera todos los literales como booleanos (por ejemplo, Sí o No).
- **ipaddress**. Cadena que representa una dirección IPv4 o IPv6 válida.
- **puerto TCP.** Número comprendido entre 0 y 65535 que representa un puerto TCP o UDP.
- **contraseña**. Un valor de cadena opaco/secreto. Cuando NetScaler ADM muestra un valor para este parámetro, se muestra como asteriscos (*****).
- **archivo de certificados.** Archivo de certificado.
- **archivo de claves**. Archivo de clave privada del certificado.
- **archivo**. Un parámetro de este tipo requiere que el usuario cargue un archivo, por ejemplo, un archivo de certificado o clave.
- **objeto**. Consta de varios elementos y cada uno de ellos es un parámetro. Este tipo se puede utilizar para agrupar varios parámetros relacionados bajo un parámetro principal.
- **requerida**. Indica si un parámetro es obligatorio u opcional. Si se establece en true, el parámetro es obligatorio y el usuario tiene que proporcionar un valor para este parámetro al crear configuraciones con este StyleBook. De forma predeterminada, todos los parámetros son opcionales. En este ejemplo, **name** e **ip** son parámetros obligatorios, mientras que **lb-alg** es un parámetro opcional, cuyo valor predeterminado es “ROUNDROBIN”.

Utilice el atributo **predeterminado** para asignar un valor por defecto a un parámetro opcional. Al crear una configuración, si un usuario no especifica un valor, se utiliza el valor predeterminado. Por ejemplo, para el parámetro **lb-alg**, el valor predeterminado es ROUNDROBIN.

Utilice el atributo **de valores permitidos** para definir valores específicos entre los que el usuario puede elegir al crear una configuración. En este ejemplo, especificó dos valores para el parámetro **lb-alg**: ROUNDROBIN y LEASTCONNECTION.

Al importar su StyleBook y usarlo, NetScaler ADM muestra un formulario con estos tres parámetros. Los campos que se muestran para nombre e IP permiten introducir el tipo de valor de cadena y dirección IP, y el campo lb-alg se muestra como una lista desplegable con ROUNDROBIN seleccionado como valor predeterminado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Además de los tipos integrados, un parámetro puede tener otro StyleBook como tipo. Se trata de una forma de reutilizar los parámetros definidos en otros StyleBooks.

### Componentes

La última sección de este StyleBook se llama la sección de componentes y se considera como la sección más importante del StyleBook. En esta sección, se definen los objetos de configuración que debe crear el SyleBook.

Para este ejemplo, debe escribir la sección de componentes de la siguiente manera:

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
```

Este ejemplo contiene solo un componente. Los atributos principales de un componente son el nombre, el tipo y las propiedades. El tipo de componente determina las propiedades que proporciona este componente. Los componentes son de dos tipos:

- **Tipo incorporado**. El sistema proporciona este tipo y no es necesario que lo defina; por ejemplo, los tipos de entidades NITRO son “lbvserver”o “servicegroup”. En este ejemplo, utiliza un tipo de componente integrado.
- **Tipo compuesto**. Este tipo es el StyleBook que creó e importó en NetScaler ADM, o el StyleBook predeterminado que se incluye con NetScaler ADM. Puede obtener más información sobre los StyleBooks compuestos en Crear un StyleBook compuesto.

En este ejemplo, ha definido un componente denominado **lbvserver-comp**. Este componente es de tipo **ns::lbvserver** (un tipo Nitro incorporado), donde “ns”es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y la versión 10.5 que había especificado en la sección import-stylebooks, y “lbvserver”es un recurso Nitro en este espacio de nombres.

Las **propiedades** definidas aquí son los atributos del recurso “lbvserver”. Para obtener más información sobre todos los recursos disponibles de NetScaler ADC Nitro y sus atributos, consulte la documentación de la API REST de NetScaler ADC NITRO.

Las propiedades de esta sección incluyen los atributos obligatorios del recurso “lbvserver”y le permiten especificar valores para estos atributos. En este ejemplo, está especificando valores estáticos

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

para servicetype y port, mientras que las propiedades name, ipv46 y lbmethod obtienen sus valores de los parámetros de entrada. En el resto del StyleBook, puede hacer referencia a los nombres de parámetros definidos en la sección de parámetros mediante la expresión **$parameters.<parameter-name>**, por ejemplo, **$parameters.ip**.

> **Nota**
>
> Por convención, el prefijo «ns» siempre se usa para designar un espacio de nombres Citrix ADC Nitro en la sección «libros de estilo de importación». Aunque no es obligatorio, Citrix recomienda utilizar la misma convención en sus propios StyleBooks para mayor coherencia.

### Crea su StyleBook

Ahora que ha definido todas las secciones requeridas de este StyleBook, reúna todas para crear su primer StyleBook. Copie y pegue el contenido de StyleBook en un editor de texto y, a continuación, guarde el archivo como **lb-vserver.yaml**. Citrix recomienda utilizar el validador de YAML integrado en StyleBooks para validar e importar el contenido de YAML.

El contenido completo del archivo lb-vserver.yaml se reproduce a continuación:

```yaml
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP virtual server configuration"
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
29    type: ipaddress
30    required: true
31   -
32    name: lb-alg
33    label: LB Algorithm
34    description: Load Balancing Algorithm
35    type: string
36    default: ROUNDROBIN
37    allowed-values:
38     - ROUNDROBIN
39     - LEAST-CONNECTION
40
41  components:
42   -
43    name: lbvserver-comp
44    description: This StyleBook component (a Builtin Nitro StyleBook)
         builds a Citrix ADC load balancing virtual server configuration
         object.
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name
48     ipv46: $parameters.vip-ipaddress
49     lbmethod: $parameters.lb-alg
50     servicetype: HTTP
51     port: 80
```

Para comenzar a usar su StyleBook para crear configuraciones, debe importarlo a NetScaler ADM y luego usarlo. Para obtener más información, consulte Cómo utilizar StyleBooks definidos por el usuario.

También puede importar este StyleBook a otros StyleBooks (usando la construcción import-stylebooks). O bien, puede modificar este StyleBook para incluir más parámetros y componentes como se describe en la siguiente sección.

## StyleBook para crear una configuración básica de equilibrio de carga

January 30, 2024

En el ejemplo anterior, creó un StyleBook básico para crear un servidor virtual de equilibrio de carga. Puede guardar este StyleBook con un nombre diferente y, a continuación, actualizarlo para incluir parámetros y componentes adicionales para una configuración básica de equilibrio de carga. Guarde este archivo de StyleBook como **basic-lb-config.yaml**.

En esta sección, diseñará un nuevo StyleBook que cree una configuración de equilibrio de carga compuesta por un servidor virtual de equilibrio de carga, un grupo de servicios y una lista de servicios. También vincula los servicios al grupo de servicios y enlaza el grupo de servicios al servidor virtual.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Header

Para crear este StyleBook, tiene que empezar por actualizar la sección del encabezado. Esta sección es similar a la que creó para el servidor virtual de equilibrio de carga StyleBook. En la sección del encabezado, cambie el valor del **nombre** a basic-lb-config. Además, actualice la **descripción** y el **nombre de visualización** para describir este StyleBook de forma adecuada. No es necesario cambiar los valores del espacio de **nombres** ni de la **versión**. Como ha cambiado el nombre, la combinación de nombre, espacio de nombres y versión crea un identificador único para este StyleBook en el sistema.

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
```

### Importar StyleBooks

La sección Import-StyleBooks sigue siendo la misma. Hace referencia al espacio de nombres netscaler.nitro.config para usar los objetos de configuración de Nitro.

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
```

### Parámetros

Tiene que actualizar la sección de parámetros para agregar dos parámetros adicionales para definir la lista de servicios o servidores y el puerto en el que los servicios escuchan. Los tres primeros parámetros, name, ip y lb-alg, siguen siendo los mismos.

```
parameters:
 -
 name: name
 type: string
 label: Application Name
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
12     description: Application VIP that the clients access
13     required: true
14    -
15     name: lb-alg
16     type: string
17     label: LoadBalancing Algorithm
18     description: Choose the load balancing algorithm used for load
          balancing client requests between the application servers.
19       allowed-values:
20       - ROUNDROBIN
21       - LEASTCONNECTION
22        default: ROUNDROBIN
23    -
24     name: svc-servers
25     type: ipaddress[]
26     label: Application Server IPs
27     description: The IP addresses of all the servers of this application
28     required: true
29    -
30     name: svc-port
31     type: tcp-port
32     label: Server Port
33     description: The TCP port open on the application servers to receive
           requests.
34     default: 80
```

En este ejemplo, se agrega el parámetro **svc-servers** para aceptar una lista de direcciones IP de los servicios que representan los servidores de fondo de la aplicación. Este es un parámetro obligatorio como se indica por **requerido: True**. El segundo parámetro, **svc-port**, indica el número de puerto en el que escuchan los servidores. El número de puerto predeterminado es 80 para el parámetro svc-port, si el usuario no lo ha especificado.

### Componentes

También debe actualizar la sección de componentes para definir componentes adicionales de modo que utilicen los dos nuevos parámetros y creen la configuración completa de equilibrio de carga.

Para este ejemplo, debe escribir la sección de componentes de la siguiente manera:

```
1  components:
2   -
3    name: lbvserver-comp
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name + "-lb"
7     servicetype: HTTP
8     ipv46: $parameters.ip
9     port: 80
10    lbmethod: $parameters.lb-alg
11
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
12 components:
13  -
14   name: svcg-comp
15   type: ns::servicegroup
16   properties:
17    name: $parameters.name + "-svcgrp"
18    servicetype: HTTP
19
20 components:
21  -
22   name: lbvserver-svg-binding-comp
23   type: ns::lbvserver_servicegroup_binding
24   properties:
25    name: $parent.parent.properties.name
26    servicegroupname: $parent.properties.name
27  -
28   name: members-svcg-comp
29   type: ns::servicegroup_servicegroupmember_binding
30   repeat: $parameters.svc-servers
31   repeat-item: srv
32   properties:
33    ip: $srv
34    port: str($parameters.svc-port)
35    servicegroupname: $parent.properties.name
```

En este ejemplo, el componente original **lbvserver-comp** (del ejemplo anterior) ahora tiene un componente secundario llamado **svcg-comp**. Además, el componente **svcg-comp** contiene dos componentes secundarios. Al anidar un componente dentro de otro componente, el componente anidado puede crear objetos de configuración haciendo referencia a los atributos del componente principal. El componente anidado puede crear uno o más objetos para cada objeto creado en el componente principal.

El componente **svcg-comp** se usa para crear un grupo de servicios en la instancia de NetScaler ADC mediante los valores proporcionados para los atributos del recurso "servicegroup". En este ejemplo, especificará un valor estático para el tipo de servicio, mientras que el nombre obtiene su valor del parámetro de entrada. Para hacer referencia al **nombre** del parámetro definido en la sección de parámetros, utilice la notación **$parameters.name + "-svcgrp", donde**-svcgrp** se agrega (concatena) al nombre definido por el usuario.

El componente **svcg-comp** tiene dos componentes secundarios, **lbvserver-svg-binding-comp** y **members-svcg-comp**.

El primer componente secundario, **lbvserver-svg-binding-comp**, se usa para vincular un objeto de configuración entre el grupo de servicios creado por su componente principal y el servidor virtual de equilibrio de carga (lbvserver) creado por el componente principal del componente principal. La notación $principal, también llamada referencia principal, se utiliza para hacer referencia a entidades en los componentes principal. Por ejemplo, **servicegroupname: $parent.properties.name** hace referencia al grupo de servicios creado por el componente principal **svcg-comp**, y **name:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**$parent.parent.properties.name** hace referencia al servidor virtual creado por el componente principal **lbvserver-comp**.

El componente **members-svcg** se utiliza para vincular los objetos de configuración de la lista de servicios al grupo de servicios creado por el componente principal. La creación de múltiples objetos de configuración de enlace se logra mediante el uso de la construcción de **repetición** de StyleBook para iterar sobre la lista de servidores especificados en el parámetro **svc-servers**. Durante la iteración, este componente StyleBook crea un objeto de configuración Nitro de tipo **service-group_servicegroupmember_binding** para cada servicio (denominado srv en la construcción **repeat-item**) en el grupo de servicios, y establece el atributo **ip** en cada Nitro objeto de configuración a la dirección IP del servidor correspondiente.

Por lo general, puede utilizar las construcciones **repeat y**repeat-item**** **de un componente para hacer que ese componente genere varios objetos de configuración del mismo tipo. Puede asignar un nombre de variable a la construcción **repeat-item**, por ejemplo, srv, para designar el valor actual en la iteración. En las propiedades del mismo componente o en los componentes secundarios se hace referencia a este nombre de variable como **$<varname>**, por ejemplo, $srv.

En el ejemplo anterior, ha utilizado anidamiento de componentes dentro de otros para construir fácilmente esta configuración. En este caso concreto, el anidamiento de los componentes no era la única forma de crear la configuración. Podrías haber obtenido el mismo resultado sin anidar, como se muestra a continuación:

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
27    name: svcg-comp
28    type: ns::servicegroup
29    properties:
30    name: $parameters.name + "-svcgrp"
31    servicetype: HTTP
```

Aquí, todos los componentes están en el mismo nivel (es decir, no están anidados) pero el resultado obtenido (la configuración de Citrix ADC generada) es el mismo que el de los componentes anidados utilizados anteriormente. Además, el orden en el que se declaran los componentes en el StyleBook no afecta al orden de creación de los objetos de configuración. En este ejemplo, los componentes **svcg-comp y**lbvserver-comp****, aunque se declaren en último lugar, se deben crear antes de compilar el segundo componente **lbvserver-svg-binding-comp**porque hay referencias directas a estos componentes en el segundo componente.

> **Nota**
>
> Por convención, los nombres de los StyleBooks, los parámetros, las sustituciones, los componentes y las salidas aparecen en minúsculas. Cuando contienen varias palabras, están separadas por un carácter "-". Por ejemplo, "lb-bindings", "app-name", "rewrite-config", etc. Otra convención consiste en agregar el sufijo "-comp"a los nombres de los componentes.

## Resultados

La última sección que puede agregar al nuevo StyleBook es la sección de salidas donde se especifica lo que este StyleBook expone a sus usuarios (o en otros StyleBooks) después de que se use para crear una configuración. Por ejemplo, puede especificar en la sección de salidas que se muestren los objetos de configuración lbvserver y servicegroup que crearía este StyleBook.

```
1  outputs:
2   -
3    name: lbvserver-comp
4    value: $components.lbvserver-comp
5    description: The component that builds the Nitro lbvserver
        configuration object
6   -
7    name: servicegroup-comp
8    value: $components.svcg-comp
9    description: The component that builds the Nitro servicegroup
        configuration object
```

La sección de salidas de un StyleBook es opcional. No es necesario que un StyleBook devuelva las salidas. Sin embargo, al devolver algunos componentes internos como salidas, permite a los StyleBooks que importen este StyleBook una mayor flexibilidad, como se puede ver al crear un StyleBook compuesto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Se recomienda exponer un componente completo del StyleBook en la sección de resultados, en lugar de una sola propiedad de un componente (por ejemplo, exponer el $components.lbvserver-comp completo en lugar de solo el nombre $components.lbvserver-comp.properties.name). Agregue también una descripción a la salida que explique lo que representa la salida específica.

### Crea su StyleBook

Ahora que ha definido todas las secciones requeridas de este StyleBook, reúna todas para crear su segundo StyleBook. Ya ha guardado este archivo StyleBook como **basic-lb-config.yaml**. Citrix recomienda utilizar el validador de YAML integrado en la página StyleBooks para validar e importar el contenido de YAML.

El contenido completo del archivo **basic-lb-config.yaml** se reproduce a continuación:

```yaml
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for loadbalancing client requests between the application servers.
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
31    allowed-values:
32       - ROUNDROBIN
33       - LEASTCONNECTION
34    default: ROUNDROBIN
35   -
36    name: svc-servers
37    type: ipaddress[]
38    label: Application Server IPs
39    description: The IP addresses of all the servers of this application
40    required: true
41
42  components:
43   -
44    name: lbvserver-comp
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name + "-lb"
48     servicetype: HTTP
49     ipv46: $parameters.ip
50     port: 80
51     lbmethod: $parameters.lb-alg
52   -
53    name: svcg-comp
54    type: ns::servicegroup
55    properties:
56      servicegroupname: $parameters.name + "-svcgrp"
57      servicetype: HTTP
58
59   -
60    name: lbvserver-svg-binding-comp
61    type: ns::lbvserver_servicegroup_binding
62    properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65   -
66    name: members-svcg-comp
67    type: ns::servicegroup_servicegroupmember_binding
68    repeat: $parameters.svc-servers
69    repeat-item: srv
70    properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74  outputs:
75  -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
         configuration object
79  -
80    name: servicegroup-comp
81    value: $components.svcg-comp
82    description: The component that builds the Nitro servicegroup
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
        configuration object
```

Para comenzar a usar su StyleBook para crear configuraciones, debe importarlo a NetScaler ADM y luego usarlo. Para obtener más información, consulte Cómo utilizar StyleBooks definidos por el usuario.

También puede importar este StyleBook a otros StyleBooks y utilizar sus propiedades como se describe en la siguiente sección.

## Crear un StyleBook compuesto

January 30, 2024

Una función importante y poderosa de StyleBooks es que se pueden usar como bloques de construcción para otros StyleBooks. Se puede importar un StyleBook a otro StyleBook y se le puede denominar como el **tipo** que utilizan los componentes del segundo StyleBook, de forma similar a un StyleBook integrado en Nitro.

**Por ejemplo, puede usar el StyleBook**basic-lb-config**que creaste en la sección anterior para crear otro StyleBook llamado composite-example.** Para usar el StyleBook "basic-lb-config", debe importarlo al nuevo StyleBook en la sección de importación de libros de estilo.

### Crea su StyleBook

El nuevo StyleBook se vería de la siguiente manera:

```
1  name: composite-example
2  namespace: com.example.stylebooks
3  version: "0.1"
4  display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
5  description: This StyleBook defines a RoundRobin load balancing
       configuration with a monitor.
6  schema-version: "1.0"
7  import-stylebooks:
8    -
9     namespace: netscaler.nitro.config
10    version: "10.5"
11    prefix: ns
12   -
13    namespace: com.example.stylebooks
14    version: "0.1"
15    prefix: stlb
16 parameters:
17   -
18     name: name
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
19      type: string
20      label: Application Name
21      description: Give a name to the application configuration.
22      required: true
23    -
24      name: ip
25      type: ipaddress
26      label: Application Virtual IP (VIP)
27      description: The Application VIP that clients access
28      required: true
29    -
30      name: svc-servers
31      type: ipaddress[]
32      label: Application Server IPs
33      description: The IP addresses of all the servers of this
           application
34      required: true
35
36    -
37      name: response-code
38      type: string[]
39      label: List of Response Codes
40      description: List of Response Codes - Provide a list of response
           codes in integer.
41
42  components:
43    -
44      name: basic-lb-comp
45      type: stlb::basic-lb-config
46      description: This component's type is another StyleBook that builds
            the NetScaler lbvserver, servicegroups and services
           configuration objects.
47      properties:
48       name: $parameters.name
49       ip: $parameters.ip
50       svc-servers: $parameters.svc-servers
51    -
52       name: monit-comp
53       type: ns::lbmonitor
54       description: This component is a basic Nitro type (a Builtin
            StyleBook) that builds the NetScaler monitor configuration
            object.
55       properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
60         lrtm: ENABLED
61         secure: "YES"
62
63       components:
64          -
65            name: monit-svcgrp-bind-comp
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
66            type: ns::servicegroup_lbmonitor_binding
67            properties:
68              servicegroupname: $components.basic-lb-comp.outputs.
                  servicegroup-comp.properties.servicegroupname
69              monitor_name: $parent.properties.monitorname
```

En la sección Import-stylebooks, se importa el StyleBook basic-lb-config utilizando su espacio de nombres y su versión, denominados con el prefijo "stlb".

En la sección de componentes, se definen dos componentes. El primer componente es de tipo **stlb::basic-lb-config**, donde "basic-lb-config"es el nombre del StyleBook que creó en StyleBook para crear una configuración básica de equilibrio de carga. Las propiedades definidas para este componente corresponden a los parámetros obligatorios declarados en el StyleBook basic-lb-config. Sin embargo, puede utilizar cualquier parámetro del StyleBook (obligatorio y opcional). En lugar de volver a crear un lbvserver, un grupo de servicios y los enlaces de servicios y grupos de servicios, importa el StyleBook que hace todo esto como un componente y lo usa para crear estos objetos de configuración en el nuevo StyleBook.

StyleBook agrega un segundo componente, "monit-comp", que utiliza los atributos del recurso "lbmonitor"de Nitro (un StyleBook integrado) para crear un objeto de configuración de monitor. También tiene un subcomponente "monit-svcgrp-bind-comp"para crear el objeto de configuración de enlace que vincula el monitor al grupo de servicios creado en el primer componente. **Como el componente servicegroup creado en el StyleBook "basic-lb-config"se expone como salida, este StyleBook puede acceder a él mediante la expresión $components.basic-lb-comp.outputs.servicegroup-comp.** Este es un ejemplo de cómo la sección de salidas puede ser utilizada por los StyleBooks importadores para tener acceso a los componentes de los StyleBooks importados a los que no habrían podido acceder de otro modo.

A continuación, copie y pegue el contenido de StyleBook en un editor de texto y, a continuación, guarde el archivo como **composite-example.yaml**. Asegúrese de validar el contenido de YAML antes de importar el archivo en NetScaler ADM. A continuación, impórtelo a NetScaler ADM y cree una o varias configuraciones con este StyleBook.

Citrix recomienda utilizar el validador YAML integrado en StyleBooks para validar e importar el contenido YAML.

## Usar atributos de GUI en un StyleBook personalizado

January 30, 2024

Puede agregar atributos de GUI en la sección de parámetros de su StyleBook para que los campos sean intuitivos cuando se muestren en NetScaler Application Delivery Management (ADM).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Un ejemplo**. Puede agregar un nombre descriptivo al parámetro mediante el atributo label y agregar una descripción emergente para este parámetro mediante el atributo description.

```
name: ip
label: Virtual Server IP Address
description: IP address of the virtual server that represents the load
    balanced application.
type: ipaddress
required: true
```

**Un ejemplo**. Si tiene un parámetro de tipo objeto, puede definir el diseño mediante el atributo **gui**. En este ejemplo, el diseño es un objeto contraíble donde los campos se muestran en dos columnas.

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
```

**Un ejemplo**. Algunos StyleBooks de Citrix ADM solo se utilizan como componentes básicos para otros StyleBooks. Además, es posible que no quiera que los usuarios creen configuraciones directamente desde estos StyleBooks. Porque estos StyleBooks deben usarse como parte de otros StyleBooks. Marque el StyleBook como privado para asegurarse de que el StyleBook no se utiliza directamente para crear configuraciones en la GUI de NetScaler ADM.

```
name: basic-lb-config
description: This stylebook defines a simple load balancing
    configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
```

## Importar StyleBooks personalizados

January 30, 2024

Después de crear su StyleBook, debe importarlo a NetScaler Application Delivery Management (ADM) para usarlo. NetScaler ADM le permite importar un único StyleBook en formato YAML o varios archivos YAML de StyleBook como un paquete en un formulario.zip,.tgz o.gz. El sistema NetScaler ADM valida sus StyleBooks al importar. El StyleBook ya está listo para usarse en la creación de configuraciones.

NetScaler ADM también tiene un editor YAML integrado que puede utilizar para componer el con-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

tenido YAML de StyleBook. El editor YAML le permite validar sus construcciones YAML desde la propia interfaz gráfica de usuario de NetScaler ADM. No es necesario utilizar una herramienta independiente para estas comprobaciones de validación. El contenido se valida según los estándares YAML y cualquier desviación se resalta. A continuación, puede corregir el contenido e intentar importar el StyleBook a NetScaler ADM. El editor YAML integrado proporciona dos ventajas mientras escribe su propio StyleBook.

- **Codificado por colores**. El editor muestra el contenido de StyleBook analizado según las directrices de YAML, y la codificación de colores le ayuda a diferenciar fácilmente entre las claves y los valores definidos en el contenido YAML.
- **Validación de YAML**. El contenido se valida para cualquier error de YAML a medida que escribe y cualquier desviación se resalta inmediatamente. Esta validación le permite escribir texto que se ajuste a las directrices de YAML incluso antes de importar el StyleBook en ADM.

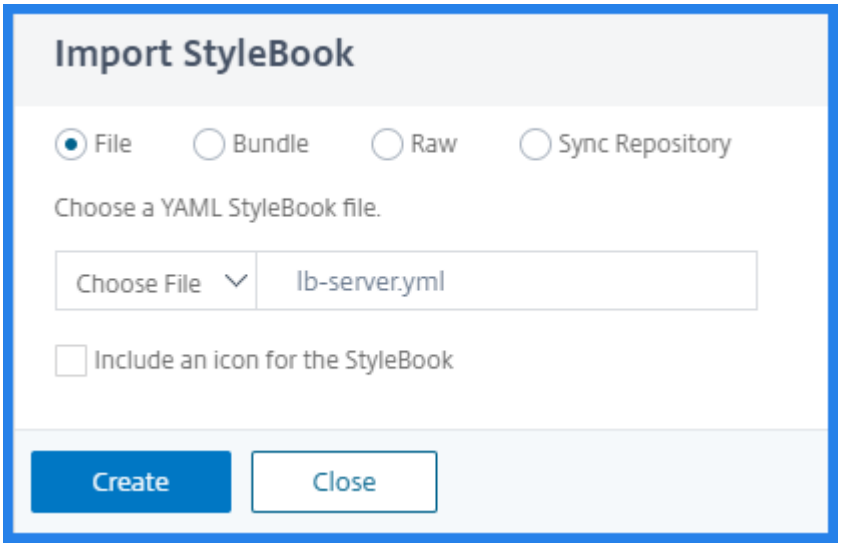
> **Nota**
>
> Actualmente, el editor valida el contenido de acuerdo con las directrices de YAML. No valida la corrección del código y los errores tipográficos.

### Para importar su StyleBook

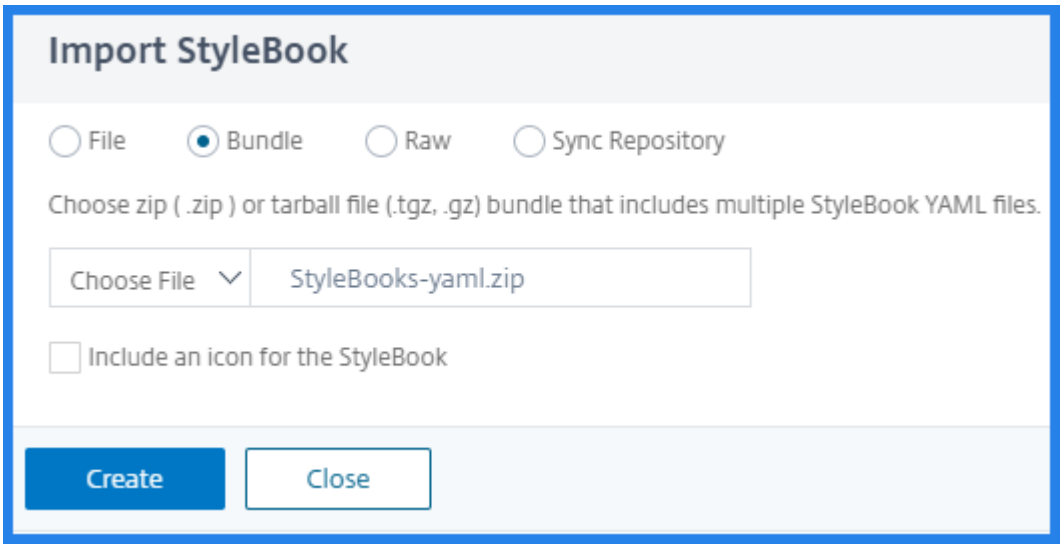
1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración** > **StyleBooks**y, a continuación, haga clic en **Importar un nuevo StyleBook**.
2. Haga clic en una de las siguientes opciones para importar un StyleBook.
   - **Archivo**: Seleccione el archivo requerido o el paquete de archivos de su almacenamiento local.

     > **Nota**
     >
     > En este ejemplo, importe el StyleBook `lb-vserver.yml` que creó en StyleBook para crear un servidor virtual de equilibrio de carga.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Paquete** : NetScaler ADM le permite importar varios StyleBooks en formato YAML. Puede importar más de un archivo YAML StyleBook comprimidos en formato zip (.zip) o tarball (.tgz,.gz).




Ahora puede incluir iconos en cada StyleBook del paquete. Asegúrese de tener la carpeta de recursos que contiene iconos en los formatos PNG, GIF o JPEG. Si el nombre del archivo de icono coincide con el nombre de StyleBook, los iconos se asignan automáticamente a los StyleBooks. De lo contrario, haga lo siguiente:

a) Agregue el `icon_mapping.json` archivo en la carpeta de recursos.

b) Asigne StyleBooks e iconos en el `icon_mapping.json` archivo de la siguiente manera:

```
<StyleBook file name> : <icon file name>
```

El siguiente es un ejemplo de paquete StyleBook:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Name | Type | Compressed size | Password ... | Size | Ratio | Date modified |
|---|---|---|---|---|---|---|
| resources | File folder | | | | | 29-07-2020 07:25 |
| .DS_Store | DS_STORE File | 1 KB | No | 7 KB | 92% | 18-08-2020 17:31 |
| exchange.yaml | YAML File | 2 KB | No | 6 KB | 78% | 31-07-2020 11:37 |
| sharepoint.yaml | YAML File | 1 KB | No | 1 KB | 56% | 29-07-2020 10:13 |
| skype.yaml | YAML File | 1 KB | No | 1 KB | 55% | 29-07-2020 10:13 |

La `resources` carpeta contiene los iconos necesarios.

| Name | Type | Compressed size | Password ... | Size | Ratio | Date modified |
|---|---|---|---|---|---|---|
| .DS_Store | DS_STORE File | 1 KB | No | 7 KB | 96% | 29-07-2020 11:55 |
| exch.png | PNG File | 3 KB | No | 3 KB | 0% | 29-07-2020 07:20 |
| icon_mapping.json | JSON File | 1 KB | No | 1 KB | 7% | 29-07-2020 07:28 |
| sharepoint.jpeg | JPEG File | 4 KB | No | 4 KB | 9% | 29-07-2020 07:19 |
| skype.png | PNG File | 7 KB | No | 7 KB | 1% | 29-07-2020 07:20 |

En este ejemplo, `sharepoint.yaml` y `skype.yaml` los archivos se asignan automáticamente a `sharepoint.jpeg` y `skype.png` respectivamente.

Para asignar `exchange.yaml` a `exch.png`, especifique lo siguiente en el `icon_mapping.json` archivo:

```
{

"exchange.yaml":"exch.png"
 }
```

Si especifica la `defaulticon` entrada, los StyleBooks se asignarán al icono predeterminado a menos que estén asignados a un icono diferente.

```
defaulticon: <icon file name>
```

En **Application > StyleBooks**, los StyleBooks importados aparecen con los iconos asignados.

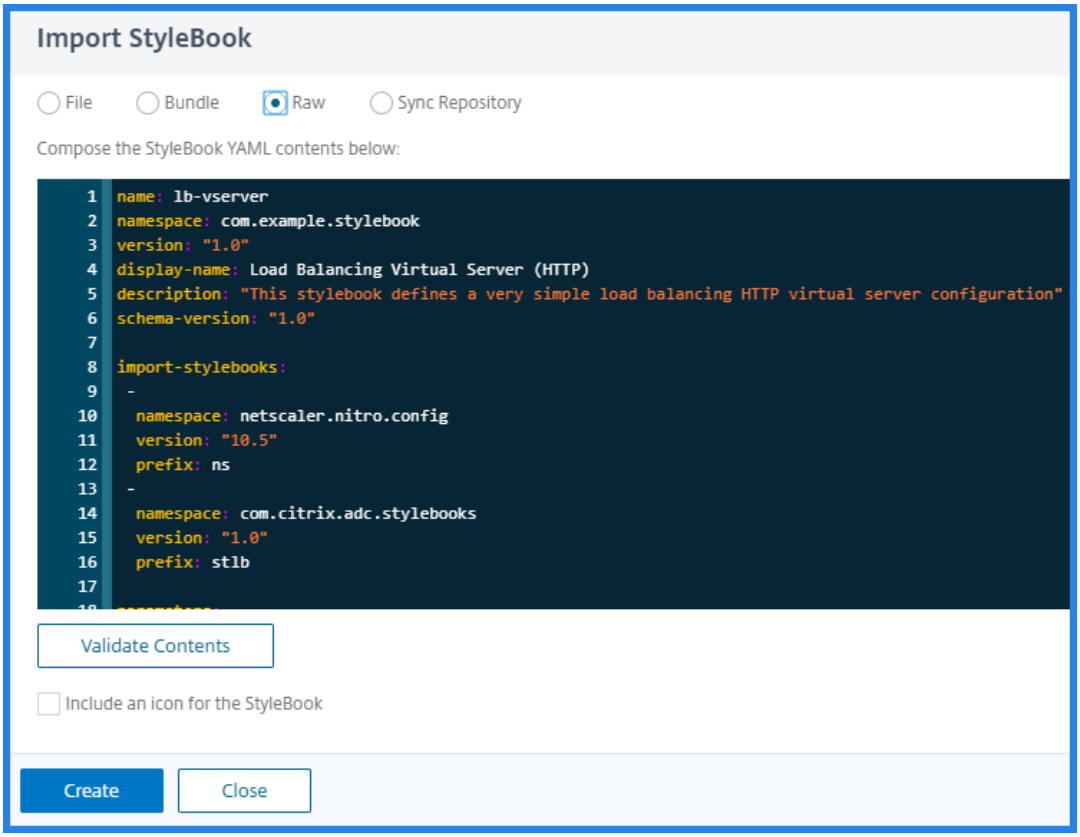
- **Raw**: Componga el contenido de su StyleBook en el editor YAML.

  Puede validar el contenido del StyleBook para comprobar los errores gramaticales del StyleBook. Para validar el contenido de StyleBook, haga clic en **Validar contenido**

  > **Nota**
  >
  > Al componer StyleBook, asegúrese de conocer los siguientes conceptos:
  >
  > - API de NITRO
  > - YAML

Para obtener más información sobre cómo escribir sus propios StyleBooks, consulta Cómo crear sus propios StyleBooks.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Sincronizar repositorio**: Esta opción muestra los repositorios agregados a ADM. Seleccione el repositorio que quiere sincronizar con ADM.

> **Nota**
>
> También puede copiar y pegar el contenido de un archivo YAML StyleBook en el editor YAML.

3. Opcional, seleccione un icono de un StyleBook.

   En **Aplicaciones > StyleBook**, el StyleBook importado aparece con este icono.

4. Haga clic en **Crear**.

   NetScaler ADM ahora valida su StyleBook para todos los errores sintácticos y semánticos de acuerdo con la gramática de StyleBook. Su StyleBook no se importa a NetScaler ADM si hay algún error.

   Si no hay ningún error, el StyleBook se importará correctamente y aparecerá en la página **StyleBooks**. Puede identificar el StyleBook por el nombre para mostrar que haya definido en la sección de encabezado del StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Si va a importar un paquete de archivos, NetScaler ADM descomprime la carpeta comprimida y valida todos los StyleBooks.
> El paquete no se importa incluso si un archivo StyleBook falla la prueba de validación.

Para obtener más información sobre la gramática y la sintaxis de StyleBook de los distintos constructos y atributos, consulte Gramática de StyleBook.

5. Haga clic en el vínculo **Crear configuración** para crear configuraciones a partir de este StyleBook.

   El StyleBook se abre como una página de interfaz de usuario en la que puede introducir los valores de todos los parámetros definidos en este StyleBook.

6. Especifique los valores necesarios para los parámetros.

   En el ejemplo siguiente,

   a) Especifique los campos obligatorios **del nombre de la aplicación** y la **dirección IP del equilibrador de carga**.

   b) Seleccione **LoadBalancing Algorithm** en la lista. De forma predeterminada, se selecciona **ROUNDROBIN**.

7. En **Instancias de destino**, seleccione la dirección IP de la instancia de NetScaler ADC donde quiere implementar la configuración.

   También puede implementar la configuración en más de un NetScaler ADC, especificando tantas instancias de destino como sea necesario.

8. Si quiere probar en los objetos de configuración de NetScaler ADC (NITRO) antes de implementar la configuración, haga clic en **Ejecutar en seco**.

   Si la configuración es válida, los objetos de configuración se crean en función de los valores especificados.

   En este ejemplo, el StyleBook crea solo un objeto de tipo `lbvserver`. Este servidor de equilibrio de carga era el único componente definido en este ejemplo básico StyleBook.

   Más tarde, haga clic en **Crear** para implementar la configuración en las instancias de NetScaler ADC seleccionadas.

Después de implementar correctamente la configuración, aparecerá un nuevo paquete de configuración en la página **Configuraciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

### Buscar StyleBooks personalizados

Citrix ADM ahora permite buscar StyleBooks según su tipo. Es decir, ahora puede buscar StyleBooks predeterminados o StyleBooks personalizados. Esta opción resulta especialmente útil cuando tiene que buscar sus StyleBooks definidos por el usuario entre muchos StyleBooks predeterminados.

#### Para buscar StyleBooks personalizados

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** > **StyleBooks**.
2. Haga clic en el icono de búsqueda situado en la parte superior derecha.
3. En la barra de búsqueda, seleccione **Tipo** y, a continuación, seleccione **Personalizado** en la sublista.
4. Citrix ADM muestra solo los StyleBooks definidos por el usuario.

## Crear y modificar un paquete de configuración

January 24, 2024

En NetScaler Application Delivery Management (ADM), puede crear un paquete de configuración a partir de un StyleBook. Además, el paquete de configuración está vinculado al StyleBook desde el que se crea. Las actualizaciones del paquete de configuración se realizan a través del StyleBook al que está vinculado.

### Crear un paquete de configuración

Realice lo siguiente para crear un paquete de configuración a partir de un StyleBook:

1. Vaya a **Aplicaciones > StyleBooks > Configuraciones**.
2. Haga clic en **Agregar**.
3. En **Elegir StyleBooks**, seleccione los StyleBooks necesarios a partir de los cuales quiere crear un paquete de configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Esta página clasifica StyleBooks en StyleBooks predeterminados y personalizados. Seleccione las fichas respectivas para encontrar los StyleBooks necesarios.

4. Especifique los detalles necesarios, como el nombre de la aplicación, la dirección IP, el puerto o el tipo de protocolo.

   Los campos GUI difieren de un StyleBook a otro StyleBook.

5. En **Instancias de destino**, seleccione instancias o grupos de instancias en los que quiera ejecutar la configuración.

   > **Nota**
   >
   > Puede implementar la configuración en más de un NetScaler ADC especificando tantas instancias de destino como sea necesario.

6. Haga clic en **Ejecutar en seco**.

   La página **Objetos** muestra los objetos que se crean, modifican o eliminan de las instancias de NetScaler ADC.

7. Haga clic en **Crear**.

   El paquete de configuración aparece en la página **StyleBook > Configuraciones**.

Si quiere modificar los paquetes de configuración existentes, seleccione el paquete de configuración y haga clic en **Modificar**.

## Cambiar el StyleBook de un paquete de configuración

A veces, debe actualizar el StyleBook para agregar funcionalidad o solucionar un problema. Si ya ha creado paquetes de configuración con el StyleBook antiguo, es posible que quiera actualizarlos para utilizar el nuevo StyleBook actualizado. Para utilizar un nuevo StyleBook, cambie el StyleBook existente del paquete de configuración.

Considere un ejemplo de StyleBook **example-lb** que implementa una configuración básica del equilibrador de carga en una instancia de ADC. Además, se crea un paquete de configuración CP1 a partir de este StyleBook.

Cuando quiera configurar monitores con la configuración básica del equilibrador de carga, necesita un nuevo StyleBook. Por lo tanto, cree **ejemplo-lb-mon** StyleBook que incluya la capacidad de configurar monitores junto con la configuración básica del equilibrador de carga.

Después de crear un StyleBook, actualice el paquete de configuración CP1 existente para agregar algunos monitores. Para ello, realice lo siguiente:

1. Vaya a **Aplicaciones > StyleBooks > Configuraciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Seleccione el paquete de configuración para el que quiere cambiar el StyleBook.

   En este ejemplo, seleccione CP1 de la lista.

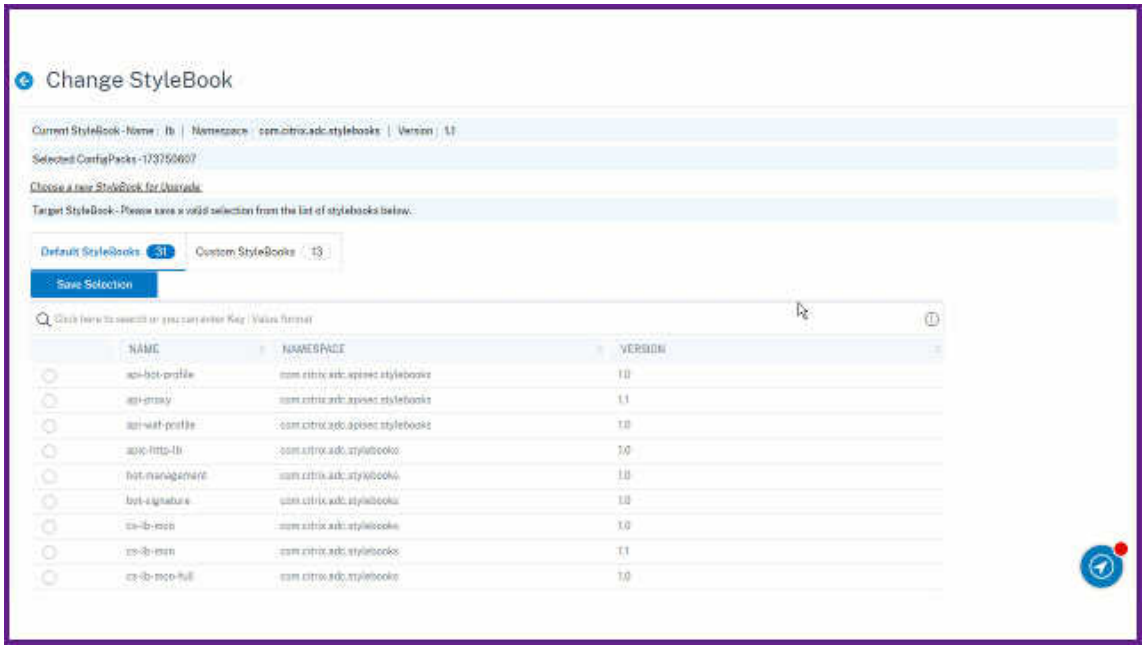
3. Haga clic en **Cambiar StyleBooks**.

4. Seleccione el StyleBook requerido de la lista. A continuación, haga clic en **Guardar selección**.

5. Haga clic en **Change**.

   En este ejemplo, seleccione **ejemplo-lb-mon** de la lista.

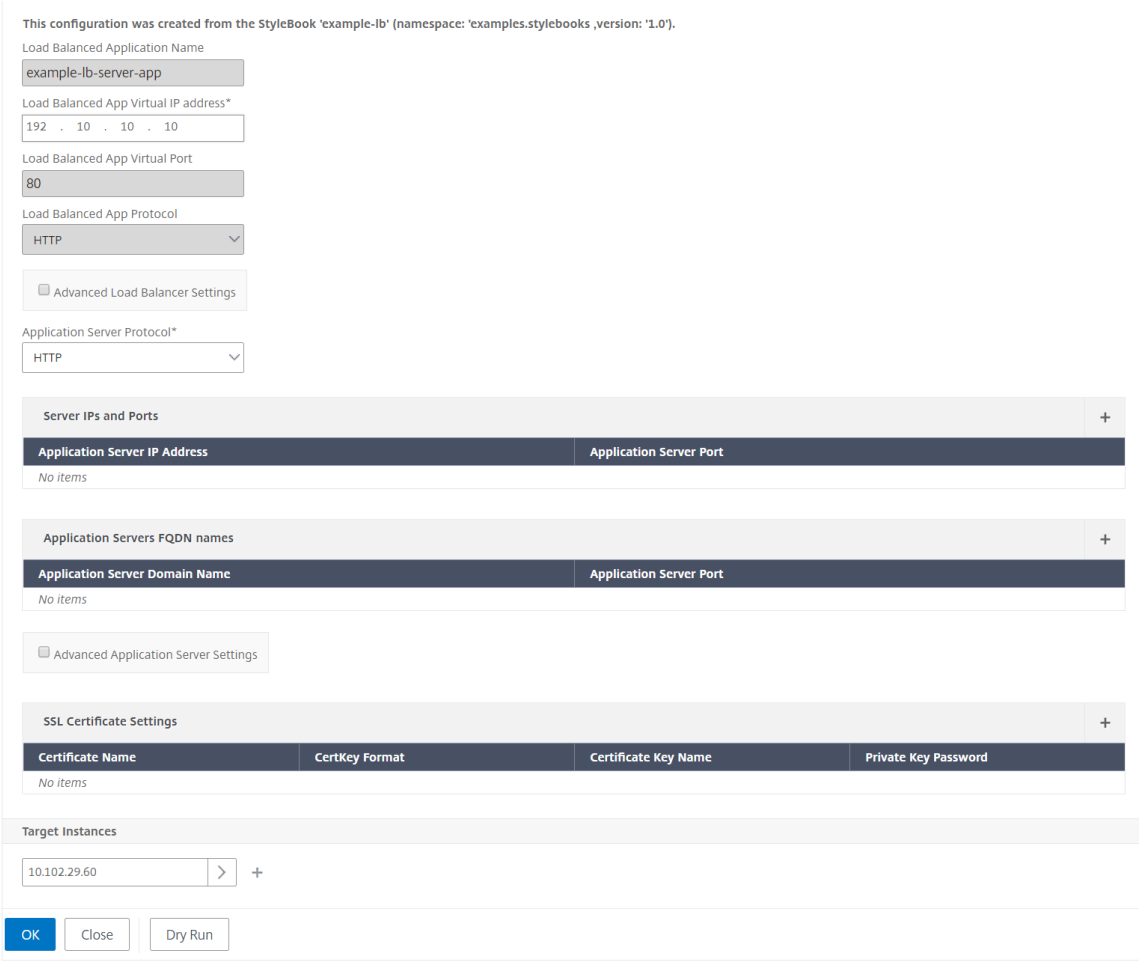
   Al cambiar el StyleBook de un paquete de configuración, los parámetros del nuevo StyleBook pueden tener una estructura diferente a la del StyleBook existente. Si la estructura de parámetros es similar a la StyleBook anterior, los valores de los parámetros se conservan automáticamente en sus respectivos campos. De lo contrario, solo se transfieren los parámetros que tengan la misma estructura entre los dos StyleBooks. Por ejemplo, el mismo nombre de parámetro, tipo, principal de parámetro y mucho más.




   Si se agregan nuevos parámetros necesarios en el nuevo StyleBook, después de cambiar el StyleBook, deberá especificar manualmente los valores de dichos parámetros.

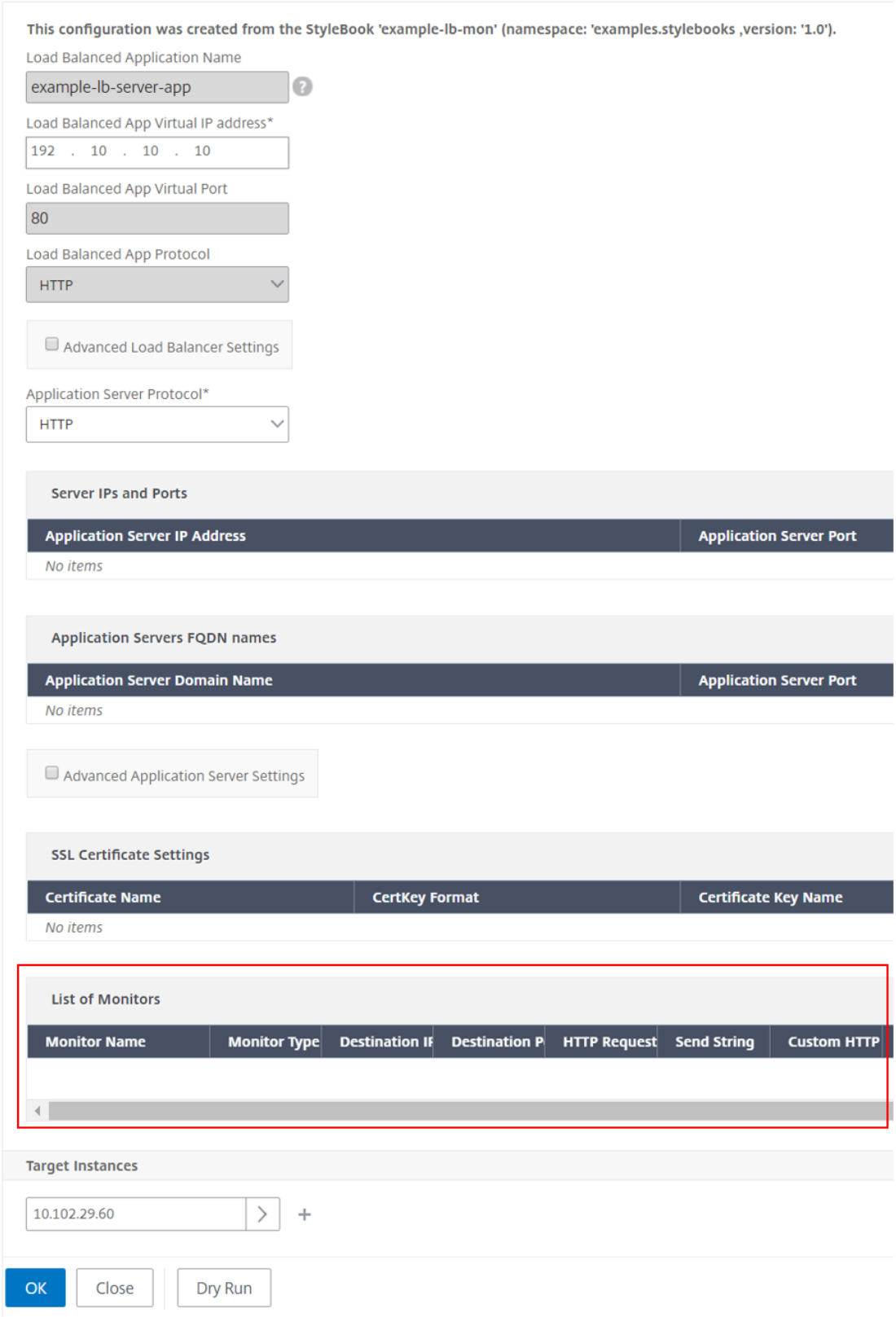
   En este ejemplo, los parámetros que aparecen en la página de configuración del **ejemplo-lb** StyleBook son los siguientes:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Los parámetros que aparecen en la página de configuración del nuevo **ejemplo-lb-mon** StyleBook son los siguientes:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En este caso, StyleBooks conservan los valores anteriores para la configuración básica del equi-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

librador de carga porque el nuevo StyleBook no ha cambiado los parámetros existentes. Y, agrega solo los nuevos parámetros. Para parámetros de supervisión, especifique manualmente los valores necesarios.

6. En **Instancias de destino**, revise las instancias seleccionadas y actualice la lista si es necesario.
7. Haga clic en **Ejecutar en seco**.

   La página **Objetos** muestra los objetos que se crean, modifican o eliminan de las instancias de NetScaler ADC.

8. Haga clic en **Aceptar**.

   En la página **StyleBook > Configuraciones**, la columna **Nombre del StyleBook** muestra el nuevo nombre de StyleBook para el paquete de configuración seleccionado. En este caso, muestra **ejemplo-lb-mon**.

### Cambiar el StyleBook que tiene varios paquetes de configuración

Cuando cambie un StyleBook existente que tiene varios paquetes de configuración, haga lo siguiente:

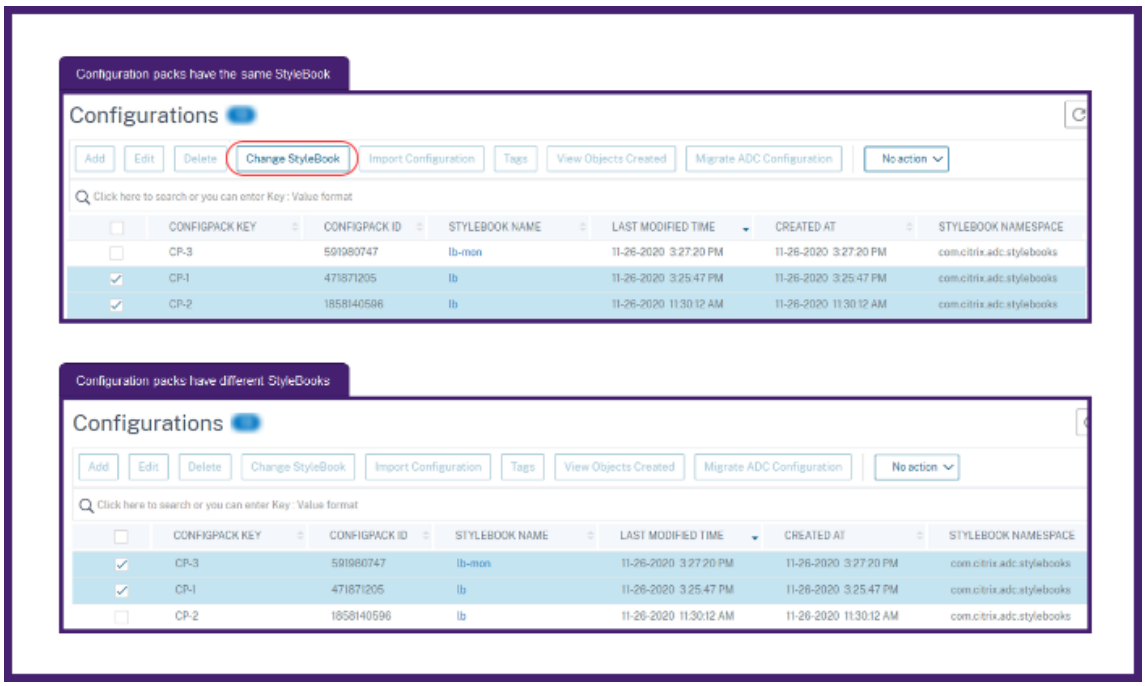
1. Importar un nuevo StyleBook a ADM.

   Normalmente, el nuevo StyleBook tiene el mismo nombre y espacio de nombres con una versión superior a la del StyleBook existente. Sin embargo, puede omitir este paso si el nombre, el espacio de nombres o la versión son diferentes.

2. Cambie el StyleBook para los paquetes de configuración asociados al StyleBook existente.

   Puede seleccionar **Cambiar StyleBook** solo cuando los paquetes de configuración seleccionados estén asociados al mismo StyleBook.

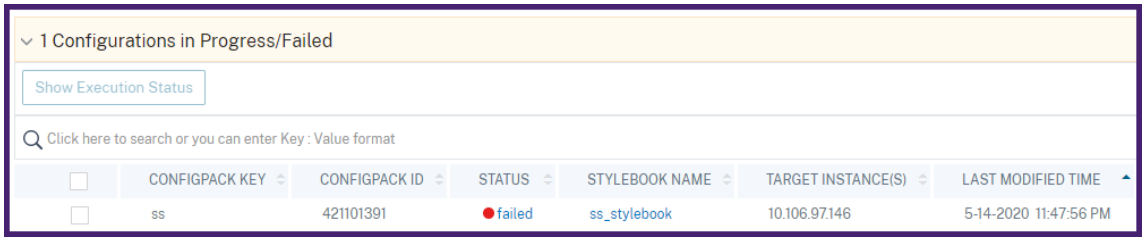
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para los paquetes de configuración seleccionados, el ADM cambia correctamente el StyleBook cuando se cumplen las siguientes condiciones:

- Todos los parámetros de configuración del StyleBook existente deben estar presentes en el StyleBook seleccionado.
- Los nuevos parámetros del StyleBook seleccionado son opcionales.

Para ver el progreso de los paquetes de configuración seleccionados, seleccione **Configuraciones en Progres/Fallo** en la página **Configuraciones**.




3. Quite el StyleBook antiguo de ADM una vez que todos los paquetes de configuración estén vinculados al nuevo StyleBook.

## Exportar o importar paquetes de configuración

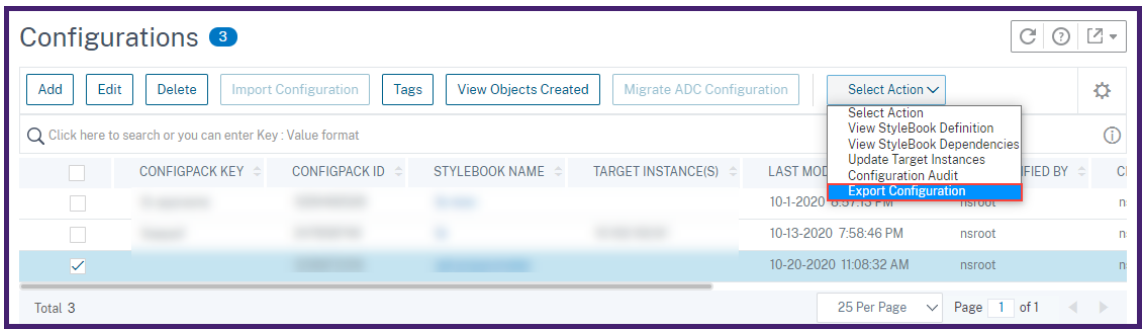
Puede exportar o importar un paquete de configuración como StyleBooks. Con esta función, puede compartir fácilmente la configuración de StyleBook con otro servidor ADM. Cuando exporta un paquete de configuración, un paquete `tgz` o un paquete `zip` se descarga al equipo local. Este paquete incluye un archivo JSON con todos los parámetros definidos en un paquete de configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Exportar configuración

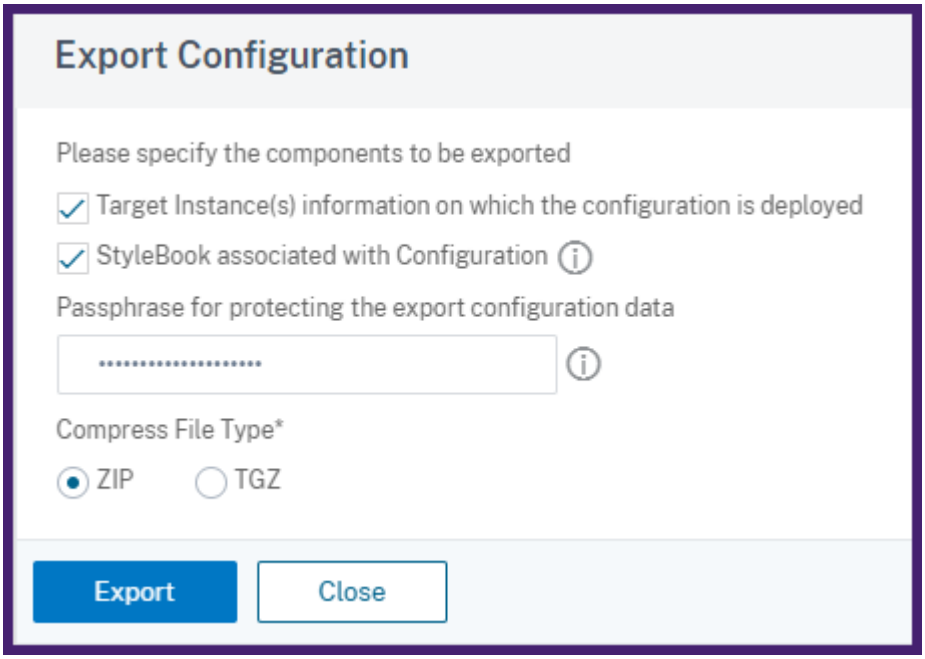
Haga lo siguiente para exportar un paquete de configuración:

1. Vaya a **Aplicaciones > StyleBooks > Configuraciones**.
2. Seleccione el paquete de configuración que quiera exportar.
3. En **Seleccionar acción**, seleccione **Exportar configuración**.




4. En el panel **Configuración de exportación**, especifique lo siguiente:
   - **Información de instancias de destino en las que se implementa la configuración**: seleccione esta opción para incluir la información de las instancias de destino con el paquete de exportación.
   - **StyleBook asociado a Configuración**: Seleccione esta opción para incluir el StyleBook en el paquete de exportación.
   - **Frase de contraseña para proteger los datos de configuración de exportación**: especifique una frase de contraseña para cifrar el paquete de exportación. Esta frase de contraseña protege los datos confidenciales de un paquete de configuración.
   - **Comprimir tipo de archivo**: seleccione el tipo de archivo **ZIP** o **TGZ**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



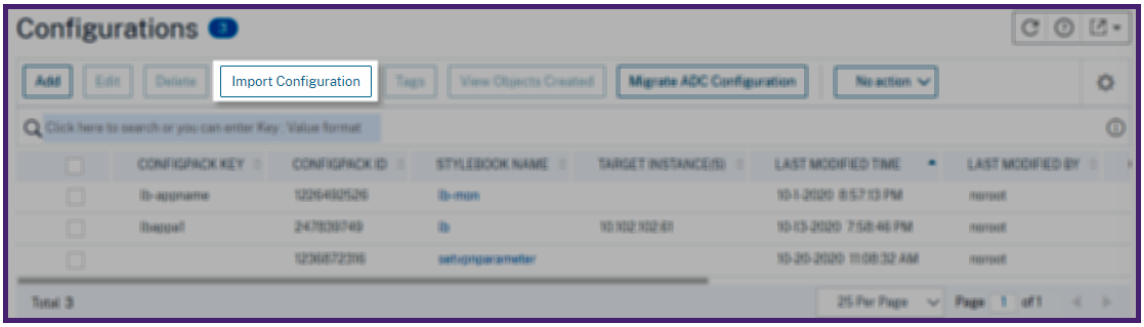

5. Haga clic en **Exportar**.

   Guarde el paquete de exportación en el equipo local.

### Importar configuración

Puede importar un paquete de configuración desde el equipo local a otro servidor ADM. Para importar un paquete de configuración, haga lo siguiente:

1. Vaya a **Aplicaciones > StyleBooks > Configuraciones**.
2. Seleccione **Importar configuración**.




3. Elija el paquete de archivos de importación desde el equipo.
4. Utilice la frase de contraseña especificada durante la exportación.
5. Opcional, en Opciones avanzadas, seleccione **Solo permitir la creación de nueva configuración si ya existen todos los objetos de configuración en ADC**.

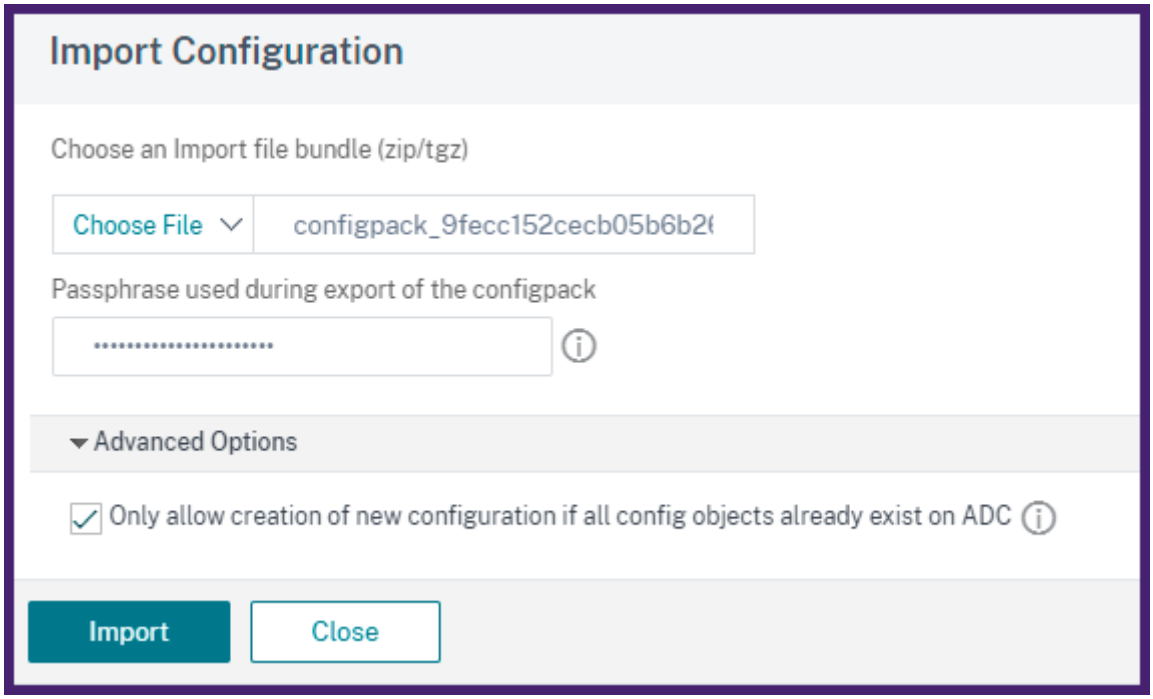
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Esta opción no modifica los objetos que ya se han creado en la instancia de ADC.

Tenga en cuenta que ha agregado la misma instancia de ADC en dos servidores ADM. Además, quiere migrar un paquete de configuración de un servidor ADM a otro servidor. Utilice esta opción para importar un paquete de configuración sin alterar sus objetos de configuración en una instancia de ADC.

> **Importante**
>
> Para utilizar esta opción, asegúrese de que el paquete de configuración especificado tiene la información de las instancias de destino. Consulte Configuración de exportación.
>
> Esta opción solo migra la configuración si todos los objetos están presentes en la instancia de destino.

6. Haga clic en **Importar**.




Al importar un paquete de configuración, ADM comprueba lo siguiente:

- **StyleBook asociado**: si el StyleBook asociado no está en el ADM, importa el StyleBook junto con el paquete de configuración.
- **Instancias de destino**: compruebe las instancias de destino e implementa la configuración en las instancias de destino especificadas. Si las instancias ADC mencionadas no están en el ADM, el paquete de configuración se importa sin instancias de destino.
- **ADM de origen**: si va a importar un paquete de configuración en el mismo servidor ADM, el paquete seleccionado actualiza el paquete de configuración existente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crea sus StyleBooks

El contenido completo de **example-lb** StyleBook se proporciona para su referencia de la siguiente manera:

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb configuration objects
    properties-default-sources:
      - $parameters
```

El contenido completo de **example-lb-mon** StyleBook se proporciona para su referencia de la siguiente manera:

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
21    - stlb::lb
22  parameters:
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
               $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
               properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
```

## Crear un StyleBook para cargar archivos a NetScaler ADM

January 30, 2024

Los StyleBooks de Citrix Application Delivery Management (Citrix ADM) permiten crear configuraciones de Citrix ADC que pueden incluir, entre otras cosas, la carga de archivos de cualquier tipo desde el sistema de archivos local a la instancia de Citrix ADC, mediante la GUI de Citrix ADM o las API.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Estos archivos pueden ser los archivos de certificado o los archivos de geolocalización de ejemplo. También puede especificar el directorio para cargar estos archivos.

### Configuración de StyleBook

El siguiente es un ejemplo de StyleBook que describe cómo cargar un archivo de geolocalización en la instancia de NetScaler ADC. Los archivos geográficos se utilizan normalmente en configuraciones GSLB para definir la proximidad estática en función de la ubicación geográfica:

### Crea tu StyleBook -1

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
```

> **Nota**
>
> El parámetro utilizado en este ejemplo es de un archivo de tipo. Puede importar este StyleBook en NetScaler ADM y utilizarlo para cargar archivos de geolocalización.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Este StyleBook requiere que el archivo ya esté presente en Citrix ADM (por ejemplo, ya lo habría copiado en Citrix ADM mediante una utilidad como scp).
Si quiere cargar un archivo en NetScaler ADC a través de NetScaler ADM sin copiarlo primero en el sistema de archivos NetScaler ADM, puede crear un StyleBook que tenga dos parámetros de "cadena" , uno es para especificar el nombre de archivo que se va a utilizar en NetScaler ADC y el otro para especificar el contenido de la y utilice estos dos parámetros en los componentes upload-file-comp. El siguiente es un StyleBook alternativo para cargar un archivo de geolocalización:

### Construye su StyleBook: 2

```
1  name: upload-geolocations-alt
2  namespace: com.citrix.adc.stylebooks.samples
3  version: "1.0"
4  display-name: GeoLocation File Upload
5  description: This StyleBook is used to upload a geolocation file to
       Citrix ADC
6  schema-version: "1.0"
7
8  import-stylebooks:
9   -
10   namespace: netscaler.nitro.config
11   version: "11.1"
12   prefix: ns
13
14 parameters:
15  -
16   name: filename
17   label: Location Filename
18   description: The name of the location file on the Citrix ADC
19   type: string
20   required: true
21  -
22   name: filecontents
23   label: Location File Contents
24   description: The contents of the location file
25   type: string
26   required: true
27
28 components:
29  -
30   name: upload-file-comp
31   type: ns::systemfile
32   properties:
33    filename: $parameters.filename
34    filelocation: "/var/Citrix ADC/inbuilt_db/"
35    filecontent: base64.encode($parameters.filecontents)
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crear configuraciones para subir archivos

El siguiente procedimiento crea una configuración en una instancia de NetScaler ADC seleccionada que cargaría un archivo de geolocalización mediante el primer StyleBook descrito anteriormente.

**Para crear una configuración para cargar archivos**:

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración**y haga clic en **Crear nuevo**. La página Choose StyleBook muestra todos los StyleBooks que están disponibles en su NetScaler ADM. Desplázate hacia abajo y selecciona el StyleBook que has importado.

   Los parámetros de StyleBook aparecen como una página de interfaz de usuario que permite introducir los valores de todos los parámetros definidos en este StyleBook.

2. Introduzca el nombre del equilibrador de carga y la dirección IP virtual en la sección de configuración básica del equilibrador de cargas.
3. En la sección **Archivo de ubicación**, introduzca el nombre o la ubicación del archivo.

   > **Nota**
   >
   > Asegúrese de que en Citrix ADM el archivo esté ubicado únicamente en la carpeta del inquilino actual. Utilice cualquier protocolo de transferencia de archivos para copiar el archivo al sistema de archivos Citrix ADM.

4. Es posible que se le pida que proporcione sus credenciales de usuario antes de acceder a las instancias de destino.
5. Seleccione la instancia de NetScaler ADC de destino en la que se debe crear la configuración y haga clic en **Crear**.

> **Nota**
>
> Citrix recomienda que seleccione**Ejecutar en seco**para comprobar los objetos de configuración que se crean en la instancia de destino antes de ejecutar la configuración real en la instancia.

Cuando la creación del paquete de configuración se realiza correctamente, el archivo se guarda en el sistema de archivos de instancia de NetScaler ADC bajo la ubicación: /var/netscaler/inbuilt_db/

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.

#### Uso de la API NetScaler ADM para crear un paquete de configuración

También puede utilizar la API de NetScaler ADM para crear un paquete de configuración que cargue archivos en la instancia de NetScaler ADC seleccionada. Para obtener más información sobre cómo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

usar las API, consulteCómo usar la API para crear configuraciones para cargar cualquier tipo de archivo.

## Crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM

January 30, 2024

Al crear una configuración de StyleBook que utilice el protocolo SSL, debe cargar los archivos de certificado SSL y los archivos de clave de certificado según lo requiera los parámetros de StyleBook. StyleBook le permite cargar directamente los archivos SSL y los archivos clave desde su sistema local mediante la GUI de NetScaler ADM. También puede utilizar las API NetScaler ADM para cargar archivos de certificado y archivos clave que ya están administrados por NetScaler ADM.

### Configuración de StyleBook

Este documento le ayuda a crear su propio servidor virtual StyleBook: **Load Balancing Virtual Server (SSL)**
con componentes para cargar certificados SSL y archivos clave. El StyleBook que se proporciona aquí como ejemplo crea una configuración básica de servidor virtual de equilibrio de carga en la instancia de NetScaler ADC seleccionada. La configuración utiliza el protocolo SSL. Para crear una configuración con este StyleBook, debe proporcionar el nombre y la dirección IP del servidor virtual, seleccionar los parámetros del método de equilibrio de carga y cargar el archivo de certificado y el archivo de clave de certificado para el servidor virtual, o utilizar un archivo de certificado y un archivo de clave de certificado que ya estén presente en NetScaler ADM. Estos se especifican en la sección “parámetros”, tal y como se muestra a continuación:

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
16    default: ROUNDROBIN
17   -
18    name: certificate
19    label: "SSL Certificate File"
20    description: "The file name of the SSL certificate file"
21    type: certfile
22   -
23    name: key
24    label: "SSL Certificate Key File"
25    description: "The file name of the server certificate's private key
         file"
26    type: keyfile
```

A continuación, se crean dos componentes en la sección de componentes del StyleBook, como se muestra a continuación. El componente “my-lbvserver-comp”es de tipo ns::lbvserver, donde:

- “ns”es el prefijo que hace referencia al espacio de nombres integrado netscaler.nitro.config y a la versión 10.5 que especificaste en la sección Import-stylebooks.
- “lbvserver”es un StyleBook integrado en este espacio de nombres. Corresponde al recurso del servidor virtual de equilibrio de carga Citrix ADC NITRO del mismo nombre.

El segundo componente “lbvserver-certificate-comp”es de tipo stlb::vserver-certs-binds. El prefijo “stlb”hace referencia al espacio de nombres “com.citrix.adc.stylebooks”y a la versión 1.0 que se especifica en la sección Import-stylebooks del StyleBook. Si el espacio de nombres “com.citrix.adc.stylebooks”puede considerarse una carpeta, “vserver-certs-binds”es otro StyleBook (o un archivo) de esa carpeta. Los StyleBooks que están en el espacio de nombres “com.citrix.adc.stylebooks”se envían como parte de NetScaler ADM.

El StyleBook «vserver-certs-binds» que utilizan los StyleBooks definidos por el usuario le permite configurar fácilmente los certificados cargando los archivos de certificado y clave en la instancia de Citrix ADC de destino y configurando el enlace de los archivos de certificado y clave a los servidores virtuales correspondientes. Las propiedades de este componente son: el nombre del servidor virtual lb y los nombres de los certificados SSL que proporciona al crear el paquete de configuración.

```
1  components:
2   -
3    name: my-lbvserver-comp
4    type: ns::lbvserver
5    properties:
6     name: $parameters.name
7     servicetype: SSL
8     ipv46: $parameters.ip
9     port: 443
10    lbmethod: $parameters.lb-alg
11   -
12    name: lbvserver-certificate-comp
13    type: stlb::vserver-certs-binds
14    description: Binds lbvserver with server certificate
15    properties:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
16     vserver-name: $components.my-lbvserver-comp.properties.name
17     certificates:
18      -
19       cert-name: $parameters.name + "-lb-cert"
20       cert-file: $parameters.certificate
21       ssl-inform: PEM
22       key-name: $parameters.name + "-key"
23       key-file: $parameters.key
```

Cuando use la API para crear una configuración a partir de tal StyleBook, use solo los nombres de archivo (no la ruta completa del archivo). Se espera que estos archivos ya estén disponibles en las carpetas de archivos de certificados y claves de NetScaler ADM. El archivo de certificado SSL cargado se almacena en NetScaler ADM en /var/mps/tenants/…El directorio /ns_ssl_certs y el archivo de clave del certificado SSL se almacenan en /var/mps/tenants/…directorio /ns_ssl_keys en NetScaler ADM.

## Crear configuraciones para cargar archivos SSL

El siguiente procedimiento crea una configuración básica de servidor virtual de equilibrio de carga en una instancia de NetScaler ADC seleccionada mediante el protocolo SSL del StyleBook especificado anteriormente. Puede utilizar este procedimiento para cargar los archivos de certificado SSL y los archivos de claves de certificado en NetScaler ADM.

### Para crear una configuración para cargar archivos

1. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración > StyleBooks**. La página **StyleBooks** muestra todos los StyleBooks que están disponibles en su Citrix ADM.
2. Desplázate hacia abajo y selecciona **Servidor virtual de equilibrio de carga (SSL)** o escribe **Servidor virtual de equilibrio de carga (SSL)** en el campo de búsqueda y presiona la tecla **Entrar** .
3. Haga clic en el enlace **Crear configuración** en el panel StyleBook.

   Los parámetros de StyleBook aparecen como una página de interfaz de usuario que permite introducir los valores de todos los parámetros definidos en este StyleBook.
4. Introduzca el nombre del equilibrador de carga y la dirección IP virtual en la sección de configuración básica del equilibrador de cargas.
5. En la sección **Configuración de certificados SSL**, seleccione los archivos correspondientes de su carpeta de almacenamiento local. Como alternativa, puede seleccionar los archivos presentes en el propio NetScaler ADM.
6. Seleccione la instancia de NetScaler ADC de destino en la que se debe crear la configuración y haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Notas:**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC detectadas recientemente en Citrix ADM a la lista de instancias disponibles en esta ventana.
>
> En Citrix ADM, los siguientes StyleBooks predeterminados, que se envían como parte de Citrix ADM, permiten crear compatibilidad con SSL cargando los certificados y claves SSL.
>
> - HTTP/SSL LoadBalancing StyleBook (lb)
> - Equilibrio de carga HTTP/SSL (con monitores) StyleBook (lb-mon)
> - Aplicación de conmutación de contenido HTTP/SSL con monitores (cs-lb-mon)
> - Ejemplo de StyleBook de aplicaciones con funciones de CS, LB y SSL (sample-cs-app)
>
> También puede crear sus propios StyleBooks que hacen uso de certificados SSL de la misma manera que se describe en el StyleBook anterior

### Crea su StyleBook

El contenido completo del archivo lb-vserver-ssl.yaml se muestra a continuación:

```yaml
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
29    type: string
30    allowed-values:
31      - ROUNDROBIN
32      - LEASTCONNECTION
33    default: ROUNDROBIN
34   -
35    name: certificate
36    label: "SSL Certificate File"
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
         file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
```

#### Uso de la API NetScaler ADM para crear un paquete de configuración

También puede utilizar la API de NetScaler ADM para crear un paquete de configuración que cargue los archivos Cert y Key en la instancia de NetScaler ADC seleccionada. Para obtener más información sobre cómo usar las API, consulte Cómo usar la API para crear configuraciones para cargar archivos de certificados y claves .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Visualización de los objetos definidos en la instancia de Citrix ADC

Después de crear el paquete de configuración de StyleBook en NetScaler ADM, haga clic en **Ver objetos creados** para mostrar todos los objetos de NetScaler ADC creados en la instancia de NetScaler ADC de destino

**Objects**

**Objects Added on Instance : 10.102.29.200**

**Type : lbvserver**

**ipv46 :** 10.10.10.1
**lbmethod :** ROUNDROBIN
**name :** vserver-1
**port :** 80
**servicetype :** SSL

**Type : systemfile**

**filecontent :**
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMzakNDQWtlZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREEvTVFzd0NRWURWUVFHRXdKVlV6RUwKTUFrR0ExVUVDQk1D
WTJFeEV6QVJCZ05WQkFjVENuTmhiblJoWTJ4aGNtRXhEakFNQmdOVkJBb1RCV0Z3Y0d4bApNQjRYRFRFMU1ERXhOekEyTURZMU5Gb1hEVEUyTURFeE56QTJNRFkxTkZvd1B6RUxNQ
WtHQTFVRUJoTUNWVk14CkN6QUpCZ05WQkFnVEFtTmhNUk13RVFZRFZRUUhFd3B6WVc1MFlXTnNZWEpoTVE0d0RBWURWUVFLRXdWaGNIQnMKWlRDQm56QU5CZ2txaGtpRzl
3MEJBUUVGQUFPQmpRQXdnWWtDZ1lFQXZFa2FoNjJFRnViTmVGUkNaQk9nN0pEZAo0dVQ1ZDBlM3UycUtaMTQrdzRjVkd5U053L1RxT2RhK1F3T0xiaU9OdDBhLzhKRDVyc096Q3N
CWHRldUsyZzRPCnhuNi8wc28zZFJKZTVKeFErNmNsT2VsVjdPbUpFTWVXZDd5WlJGbVFqZHgrZEROMjUxT25aa0pmeXN3NXdSVTUKSnpUQnRza3hRcjBQbnJ2S0tBa0NBd0VBQWFP
QjZUQ0I1akFkQmdOVkhRNEVGZ1FVam5XYVJsalF5N0pqNFozcwp0LzFIWmYvWUprZ3dad1lEVlIwakJHQXdYb0FVam5XYVJsalF5N0pqNFozc3QvMUhaZi9ZSmtpaFE2UkJNRDh4CkN6
QUpCZ05WQkFZVEFsVlRNUXN3Q1FZRFZRUUlFd0pqWVRFVE1CRUdBMVVFQnhNS2MyRnVkR0ZqYkdGeVlURU8KTUF3R0ExVUVDaE1GWVhCd2JHV0NBUUF3REFZRFZSMFRCQVV3
QXdFQi96QUxCZ05WSFE4RUJBTUNBUVI3RVFZSgpZSVpJQVliNFFnRUJCQVFEQWdFR01DNEdDV0NHU0FHRytFSUJEUVFoRmg5T1pYUlRZMkZzWlhJZ1IyVnVaWEpoCmRHVmtJRU5sY2
5ScFptbGpZWFJsTUEwR0NTcUdTSWIzRFFFQkN3VUFBNEdCQUs0RWY3aUFSRlRQUlo0b2pJWm0KTHlTeFhGaTE0SGxjK0VpMUNjejV3R09Db3pibWNXemZOZXVSSTdRQVlSSXQ3Wkh
hYWt0VGg0NXIvUHdPZXFLcgpSc2xNTzBnQ1hES3BtU2tXQ3VHdFhBbVhXU2xrTEt3bTFHL0pKdTBhSEFkdVhtRVkwNW52M016RWhTWW8xelhjCnFsYXJNcG9QUE14Qks0RmIBNWxs
QnAwTwotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg==
**fileencoding :** BASE64
**filelocation :** /nsconfig/ssl
**filename :** test_cert.pem

**Type : systemfile**

**filecontent :**
LS0tLS1CRUdJTiBSU0EgUFJJVkFURSBLRVktLS0tLQpNSUlDWEFJQkFBS0JnUUM4U1JxSHJZUVc1czE0VkVKa0U2RHNrTjNpNVBsM1I3ZTdhb3BuWGo3RGdoVWJKSTNECjlPbzUxcjVEQTR0
dUk0MjNSci93a1BtdXc3TUt3RmUxNjRyYURnN0dmci9TeWpkMUVsN2tuRkQ3cHlVNTZWWHMKNllrUXg1WjN2SmxFV1pDTjNINTBNM2JuVTZkbVFsL0t6RG5CRlRrbk5NRzJ5VEZDdlEr
ZXU4b29DUUlEQVFBQgpBb0dBUUlENjZjaDBIRFJ0NSs5VjMxc3FJbUZ1NHJCM0Zub25ZN21ZT05sOHZ4WHRqU0wwdmxGRmZSTW9rMlMvCmU3Z0tjT040Rmo1VWk1N1gwN01aV1
dXY1o0aEhrMm5jMjlmOENLSW5oelhnYjFLQjRaMGp1TnUvNE1paVIyaHIKNkFROXluV0VMRlBDTjZWMHFQZWxGYXpVbnZJaHZpMFZGZCsyRUNBY0drVHg0Z0VDUVFEMklVODhGaU
kzVFJOYwpMcVJEMHh2ZVFWMkF6ZVBEYmFnTVFFRlNWZVZ3Yk11V3RJM2J0SkdwWXMxUkpIeitOdGw0dVprRGVQbnNjZE5ZCjNJWjNsNUp4QWtFQXc5WDdKTDJaNVpyaEVpM0Yzdj
YwU1U5RWM4Z01FdVhFZlhUendCc2puanJsckRIMUI0enYKR0hSU1ImUEdYeHh5cjRKVmc4Q25kczZVOHExN0N0SUxHUUpBS1FtT3UzYjVSMzByWURCS3BTQmF3aWpsM1NiMgo5Y3
VmdkVNdVlQci9ZVXBTZTVNcEg5dXdlYXlHalNQblR6OTM3UUFNK2g0K2xWZGlkS3Q0SkJKNmtRSkJBTHVSClRaUHBEV2UrcWVleGM1MmJzcTjzZ0ZHc3Z2T3lvam5QTkU5Qkx5STBJeH
FFVnIyK25KcDlmeEpXWEI5b3JlZXcKRzV1dmdEWG9zdnlrYi83eklyRUNRRDMzV1lHeUw2MjJaRzZveHlxR1o1d1pCTFVtV1VyVE1zSngzOWZ5NUJoZgpkajNWcE10Y3plOFVKVmlPaGtyd
WNmb29tRlNPaUN4ZXhPQXM2MmVEZXNnPQotLS0tLUVORCBSU0EgUFJJVkFURSBLRVktLS0tLQo=
**fileencoding :** BASE64
**filelocation :** /nsconfig/ssl
**filename :** test_cert_key.pem

**Type : sslcertkey**

**cert :** test_cert.pem
**certkey :** vserver-1-lb-cert
**inform :** PEM
**key :** test_cert_key.pem

**Type : sslvserver_sslcertkey_binding**

**certkeyname :** vserver-1-lb-cert
**vservername :** vserver-1

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Habilitar análisis y configurar alarmas en un servidor virtual definido en un StyleBook

January 30, 2024

Puede utilizar la construcción de operaciones para configurar los análisis de Citrix ADM a fin de recopilar registros de flujo de aplicaciones en todas o algunas de las transacciones de tráfico gestionadas por cualquier componente de servidor virtual que forme parte de un StyleBook. También puede utilizar esta construcción para configurar alarmas para obtener información sobre el tráfico administrado por el servidor virtual.

El siguiente ejemplo muestra una sección de operaciones de un StyleBook:

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
```

Los atributos de la sección de análisis se utilizan para indicar a la función de análisis Citrix ADM que recopile registros de flujo de aplicaciones en un componente de servidor virtual identificado por la propiedad de destino. También puede especificar opcionalmente una propiedad de filtro que acepte una expresión de directiva NetScaler ADC para filtrar las solicitudes para las que se recopilan registros de flujo de aplicaciones en el servidor virtual.

Cuando se crea un paquete de configuración a partir de este StyleBook, la función de análisis de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

NetScaler ADM se configura para recopilar registros de flujo de aplicaciones en los servidores virtuales que se especificaron cuando se crearon en el proceso de creación de un paquete de configuración.

Los atributos de la sección alarmas se utilizan para establecer umbrales para generar alarmas y enviar notificaciones en el servidor virtual identificado por la propiedad de destino. En el ejemplo anterior, las propiedades perfil de correo electrónico y perfil de SMS se utilizan para especificar dónde se deben enviar las notificaciones. La sección de reglas define los umbrales. Por ejemplo, si el total de solicitudes manejadas por el servidor virtual es superior a 25 y durante un período definido por el usuario, se establece una alarma y se envía una notificación. La "unidad de período"especifica la frecuencia con la que se activa una alarma. Puede tomar el valor del día, la hora o la semana.

Puede utilizar los siguientes operadores al comparar el valor de métrica con el valor de umbral:

- "mayor que"para ">"
- "menor que"para "<"
- "mayor que igual"para ">="
- "menor que igual"para "<="

Tenga en cuenta que los StyleBooks utilizan nombres de API para las métricas y no los nombres que se muestran en la GUI de análisis de NetScaler ADM.

Para obtener información sobre cómo ver y analizar los datos recopilados en servidores virtuales creados como parte de un paquete de configuración, consulte la documentación de análisis de NetScaler ADM.

## Roles de instancia

January 24, 2024

En NetScaler Application Delivery Management (ADM), puede haber un caso en el que tenga que configurar varias instancias de NetScaler ADC para una sola aplicación, pero también en el que cada instancia de ADC requiera una configuración diferente para implementarlas. Un ejemplo de este caso es el predeterminado de Microsoft Skype Empresarial StyleBook.

StyleBooks admite actualmente la capacidad de crear un paquete de configuración y aplicar la misma configuración en varias instancias de NetScaler ADC. Tal caso en el que la configuración es idéntica en todas las instancias ADC, puede denominarse configuración simétrica.

Ahora, con la función "roles de instancia"de StyleBooks, puede crear una configuración asimétrica, es decir, un paquete de configuración que se puede aplicar en varias instancias de ADC, pero con diferentes configuraciones en diferentes instancias de ADC.

Cuando se utiliza una función StyleBook con funciones de instancia para crear un paquete de configuración, cada instancia de ADC de un paquete de configuración puede tener asignada una función

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

diferente. Este rol determina los objetos de configuración del paquete de configuración que recibirá la instancia de ADC.

**Puntos a tener en cuenta:**

- El conjunto de roles de instancia en un StyleBook se define al crear el StyleBook.
- Los roles se asignan a una instancia de ADC específica al crear o actualizar el paquete de configuración.

### Sección de roles de destino

Se introduce una nueva sección en un StyleBook llamada "roles de destino", donde se declaran todos los roles admitidos por el StyleBook.

Esta sección suele colocarse después de la sección "Importar libros de estilos"de un StyleBook y antes de la sección de parámetros.

En el siguiente ejemplo de StyleBook, se definen dos funciones en la sección "funciones de destino": A y B.

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
```

Puede ver que el rol B también define dos sub-propiedades opcionales, min-targets y max-targets.

Aunque estas dos subpropiedades son opcionales, los destinos mínimos especifican el número mínimo obligatorio de instancias ADC a las que se debe asignar este rol al crear un paquete de configuración a partir de este StyleBook, y max-targets especifican el número máximo de instancias ADC a las que se puede asignar este rol al crear un de este StyleBook.

Si no se especifican estas subpropiedades, no hay límite en el número de instancias ADC que se pueden configurar para ese rol. Si min-targets = 0, la configuración asociada a ese rol es opcional y si min-targets = 1, esa configuración es obligatoria y al menos se debe configurar una instancia ADC para ese rol.

### Función "predeterminada"

Además de los roles explícitamente definidos, hay un rol implícito que tienen todos los StyleBooks, y ese rol se llama como un rol predeterminado. Este rol se puede usar como cualquier otro rol en un StyleBook. Al crear un paquete de configuración, si una instancia de ADC no está asignada con un rol

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

específico, la instancia se asigna implícitamente al rol “predeterminado”. La instancia recibirá ahora todos los objetos de configuración generados por los componentes que tengan la función “predeterminada”.

### Componentes con roles

Una vez definidas las funciones que admite un StyleBook (incluida la función “predeterminada”), las funciones se pueden utilizar en la sección de componentes de un StyleBook. Si quiere que un componente se implementación solo en instancias ADC que desempeñan un determinado rol, puede especificar el atributo roles como parte del componente, como se ilustra en el siguiente ejemplo de componente:

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
```

En el ejemplo anterior, el componente genera un “lbvserver”que se implementará en las instancias que desempeñen la función A. Tenga en cuenta que el atributo roles de un componente es una lista y que a un componente se le pueden asignar varias funciones. Estas funciones se habrían declarado en la sección “funciones de destino”del StyleBook.

Nota: Si un componente de un StyleBook no especifica un atributo de rol, los objetos de configuración generados por el componente se crean en todas las instancias de NetScaler ADC, independientemente de su rol. Puede utilizar esta función de manera eficaz para crear objetos de configuración que se puedan aplicar a todas las instancias de un paquete de configuración.

Supongamos que hay un StyleBook con dos roles definidos: A y B, y que contiene cuatro componentes.

- El componente C1 tiene los roles A y B
- El componente C2 tiene el rol B
- El componente C3 no tiene ningún rol definido
- El componente C4 tiene la función “predeterminada”

La sección de componentes de este StyleBook se reproduce a continuación:

```
components:
  -
    name: C1
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
4       type: ns::lbvserver
5       roles:
6         - A
7         - B
8       properties:
9         name: lb1
10        servicetype: HTTP
11        ipv46: 1.1.1.1
12        port: 80
13    -
14      name: C2
15      type: ns::lbvserver
16      roles:
17        - B
18      properties:
19        name: lb2
20        servicetype: HTTP
21        ipv46: 12.12.12.12
22        port: 80
23    -
24      name: C3
25      type: ns::lbvserver
26      properties:
27        name: lb3
28        servicetype: HTTP
29        ipv46: 13.13.13.13
30        port: 80
31    -
32      name: C4
33      type: ns::lbvserver
34      roles:
35        - default
36      properties:
37        name: lb4
38        servicetype: HTTP
39        ipv46: 14.14.14.14
40        port: 80
```

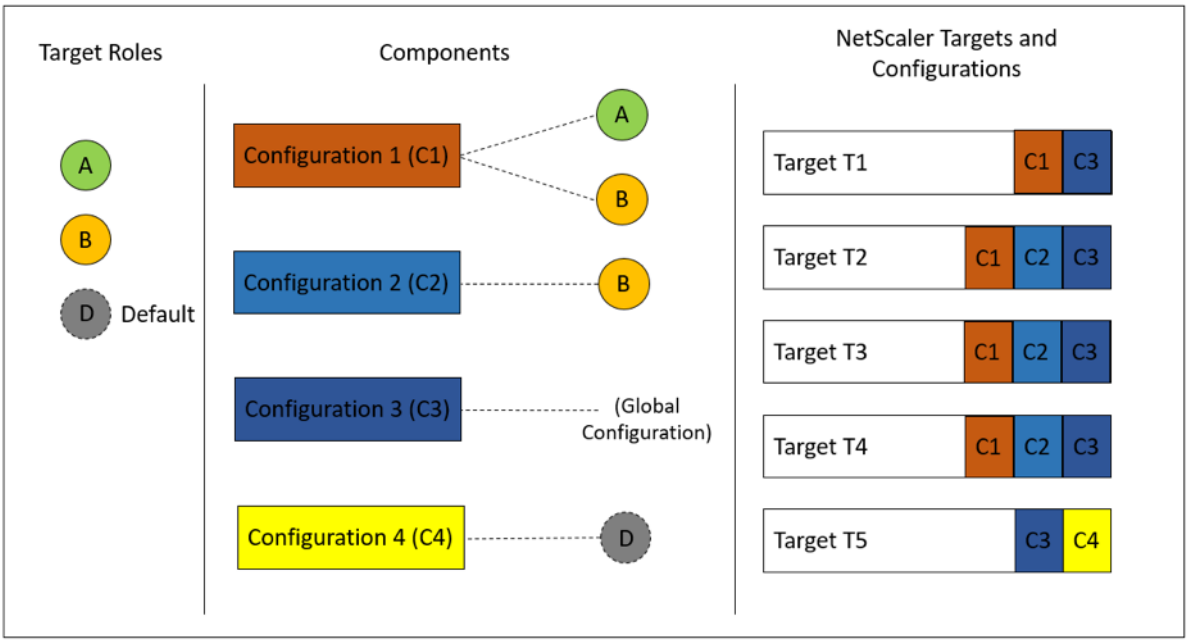
Tenga en cuenta que el componente C3 no tiene un rol definido, lo que significa que el componente se implementa en todas las instancias, independientemente de su rol. Por otro lado, el componente C4 tiene la función "predeterminada", lo que significa que se aplica a cualquier instancia que no tenga asignada una función explícita.

Ahora, considere que quiere crear un paquete de configuración con este StyleBook e implementarlo en cinco instancias de ADC. En esta etapa, puede asignar los roles a las instancias de la siguiente manera:

- La función A se asigna a las instancias T1, T2, T3 y T4
- La función B está asignada a las instancias T2, T3 y T4
- A la instancia T5 no se le asigna ningún rol

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La siguiente imagen resume las asignaciones de roles y muestra la configuración resultante que recibirá cada instancia de ADC:




Tenga en cuenta que el componente C3 se implementa en todas las instancias independientemente del rol, ya que este componente no tenía atributo roles.

También puede utilizar la función “Dry Run”al crear un paquete de configuración para ver y verificar la asignación correcta de roles y los objetos de configuración que se crearán en cada instancia de ADC.

### Crea su StyleBook

El contenido completo del StyleBook “demo-target-roles”se muestra a continuación:

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
18    -
19      name: A
20    -
21      name: B
22      min-targets: 2
23      max-targets: 5
24  components:
25    -
26      name: C1
27      type: ns::lbvserver
28      roles:
29        - A
30        - B
31      properties:
32        name: lb1
33        servicetype: HTTP
34        ipv46: 1.1.1.1
35        port: 80
36    -
37      name: C2
38      type: ns::lbvserver
39      roles:
40        - B
41      properties:
42        name: lb2
43        servicetype: HTTP
44        ipv46: 12.12.12.12
45        port: 80
46    -
47      name: C3
48      type: ns::lbvserver
49      properties:
50        name: lb3
51        servicetype: HTTP
52        ipv46: 13.13.13.13
53        port: 80
54    -
55      name: C4
56      type: ns::lbvserver
57      roles:
58        - default
59      properties:
60        name: lb4
61        servicetype: HTTP
62        ipv46: 14.14.14.14
63        port: 80
```

La siguiente imagen muestra los objetos creados para un paquete de configuración de ejemplo:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Objects created ( 9 )** ×

**Instance : 10.102.102.136 | Roles : B | Count : 3**

**Type : lbvserver**
**ipv46 :** 1.1.1.1
**name :** lb1
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 12.12.12.12
**name :** lb2
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 13.13.13.13
**name :** lb3
**port :** 80
**servicetype :** HTTP

**Instance : 10.102.102.135 | Roles : B | Count : 3**

**Type : lbvserver**
**ipv46 :** 1.1.1.1
**name :** lb1
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 12.12.12.12
**name :** lb2
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 13.13.13.13
**name :** lb3
**port :** 80
**servicetype :** HTTP

**Instance : 10.102.102.62 | Roles : A, default | Count : 3**

**Type : lbvserver**
**ipv46 :** 1.1.1.1
**name :** lb1
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 13.13.13.13
**name :** lb3
**port :** 80
**servicetype :** HTTP

**Type : lbvserver**
**ipv46 :** 14.14.14.14
**name :** lb4
**port :** 80
**servicetype :** HTTP

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Uso de API

Al utilizar la API REST, puede especificar roles para cada instancia de ADC al crear o actualizar el paquete de configuración de la siguiente manera. En el bloque «destinos», especifique el UUID de la instancia específica de Citrix ADC en la que quiere implementar los componentes individuales.

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
```

Se proporciona una API REST de muestra completa para su referencia.

POST/<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
          "roles": ["A", "B"]
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
33            }
34   ,
35          {
36
37            "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
38            "roles": ["default"]
39            }
40
41         ]
42        }
43
44   }
```

## Crear un StyleBook para realizar operaciones que no sean CRUD

January 30, 2024

Los StyleBooks administran las configuraciones de NetScaler ADC calculando los objetos de configuración necesarios en las instancias de NetScaler ADC. Estos objetos se agregan, actualizan o eliminan de la instancia cada vez que creas o actualizas un ConfigPack. Es entonces cuando se especifica el "estado deseado. "

Sin embargo, algunos objetos de configuración de Citrix ADC admiten algunas operaciones además de crear, actualizar o eliminar (operaciones CRUD). Por ejemplo, un objeto de equilibrio de carga (lbvserver) o un objeto de función de Citrix ADC (nsfeature) pueden admitir la operación de «habilitar» o «deshabilitar». Del mismo modo, las claves de certificación Citrix ADC admiten las operaciones de «vincular» y «desvincular» para vincular o desvincular un certificado a otro certificado. Estas operaciones en objetos NetScaler ADC se denominan operaciones que no son CRUD. En esta sección se describe cómo realizar operaciones que no sean CRUD en objetos de configuración que los admitan mediante StyleBooks.

> **Nota**
>
> La vinculación entre objetos de configuración (por ejemplo, vincular una clave de certificado a un lbvserver) no se considera una operación que no sea CRUD. Esto se debe a que los enlaces de Nitro se representan como objetos de configuración por derecho propio. Estos objetos se crean y eliminan como cualquier otro objeto de configuración de NetScaler ADC.

### Apoyo a las operaciones no relacionadas con CRUD

Un nuevo componente fijo llamado "meta-properties"se agrega en el componente en el mismo nivel que el componente "propiedades". El único atributo admitido en esta construcción actualmente se

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

llama “action”Este atributo puede tomar valores como “enable”o “disable”que son compatibles con ese objeto de configuración.

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
```

En el ejemplo anterior, el componente “my-lbvserver-comp”es de tipo “ns::lbvserver”. El “ns”es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y a la versión 10.5 que especificaste en la sección import-stylebooks. El “lbvserver”es un recurso de NITRO en este espacio de nombres. Como acción implícita, el styleBook crea primero el lbvserver y, a continuación, se realiza la operación de “habilitar”en él.

La acción especificada en las meta-propiedades se realiza en el objeto de configuración solo durante la creación del ConfigPack. Las actualizaciones del ConfigPack no realizan acciones que no sean de CRUD.

> **Nota**
>
> El valor del atributo action no puede ser una expresión StyleBook que se evalúe dinámicamente.

## Migrar el paquete de configuración de un StyleBook a otro StyleBook

January 24, 2024

En NetScaler Application Delivery Management (ADM), los paquetes de configuración siempre están enlazados al StyleBook desde el que se crean. Cualquier actualización del paquete de configuración solo se puede realizar a través del StyleBook al que está enlazado el paquete de configuración. NetScaler ADM ahora le permite migrar un paquete de configuración existente a un nuevo StyleBook. El nuevo StyleBook puede ser una versión más original del StyleBook actual vinculado al paquete de configuración. O bien, también puede migrar el paquete de configuración a un StyleBook completamente diferente.

Por ejemplo, creó un StyleBook llamado **example-lb**. Este StyleBook se utiliza para implementar una configuración básica del equilibrador de carga en una instancia de NetScaler ADC. Ha creado un paquete de configuración CP1 a partir de este StyleBook en una instancia de NetScaler ADC. Más tarde,

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

se dio cuenta de que su StyleBook no incluye una configuración de supervisión. **Por lo tanto, ahora ha creado un StyleBook llamado example-lb-mon.** Este StyleBook tiene la misma configuración del equilibrador de carga que example-lb StyleBook, pero agrega la capacidad de configurar monitores.

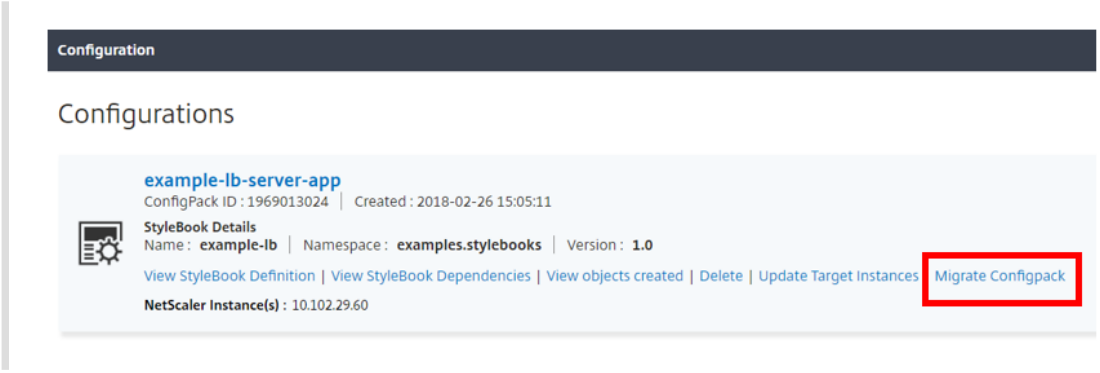
Ahora quiere actualizar la configuración existente que se creó en el paquete de configuración CP1 para agregar algunos monitores. Anteriormente, tenía que eliminar el paquete de configuración CP1 y crear un paquete de configuración CP2 desde el nuevo StyleBook para agregar monitores a la configuración. La eliminación de CP1 da como resultado la eliminación de toda la configuración creada en el paquete de configuración CP1 en una o más instancias de NetScaler ADC. Anteriormente, tenía que volver a crear un nuevo paquete de configuración a través del nuevo StyleBook escribiendo valores para todos los parámetros.

En su lugar, ahora puede migrar el paquete de configuración CP1 existente al nuevo StyleBook de ejemplo-lb-mon. Su nuevo StyleBook puede configurar los detalles del monitor de monitores. Solo los objetos de configuración relacionados con el monitor se agregan a las instancias de NetScaler ADC en las que se implementó el paquete de configuración. Tiene que proporcionar solo los detalles del monitor ahora. La configuración existente implementada en las instancias de NetScaler ADC que no ha cambiado no se verá afectada.

## Migrar paquete de configuración

**Para migrar un paquete de configuración creado con example-lb StyleBook a example-lb-mon StyleBook**

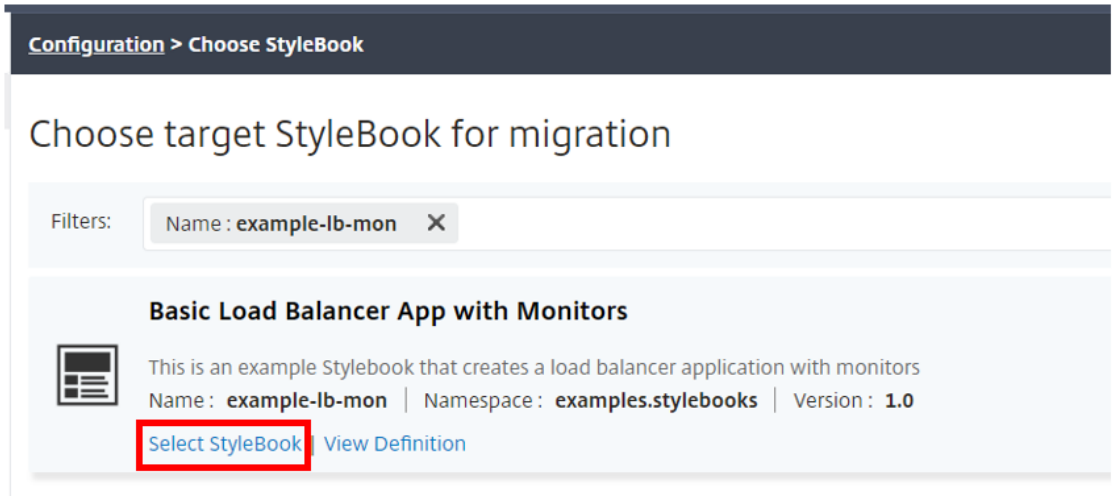
1. En Citrix ADM, vaya a **Aplicaciones** > **Configuraciones**. La página **Configuraciones** muestra todos los paquetes de configuración presentes en el sistema.
2. Desplácese hacia abajo para buscar el paquete de configuración **ejemplo-lb** que habría creado anteriormente y haga clic en **Migrar Configpack**.




3. Se abre la página **Elegir StyleBook de destino para la migración** , que muestra todos los StyleBooks disponibles en Citrix ADM. Desplácese hacia abajo para buscar el StyleBook **example-lb-**

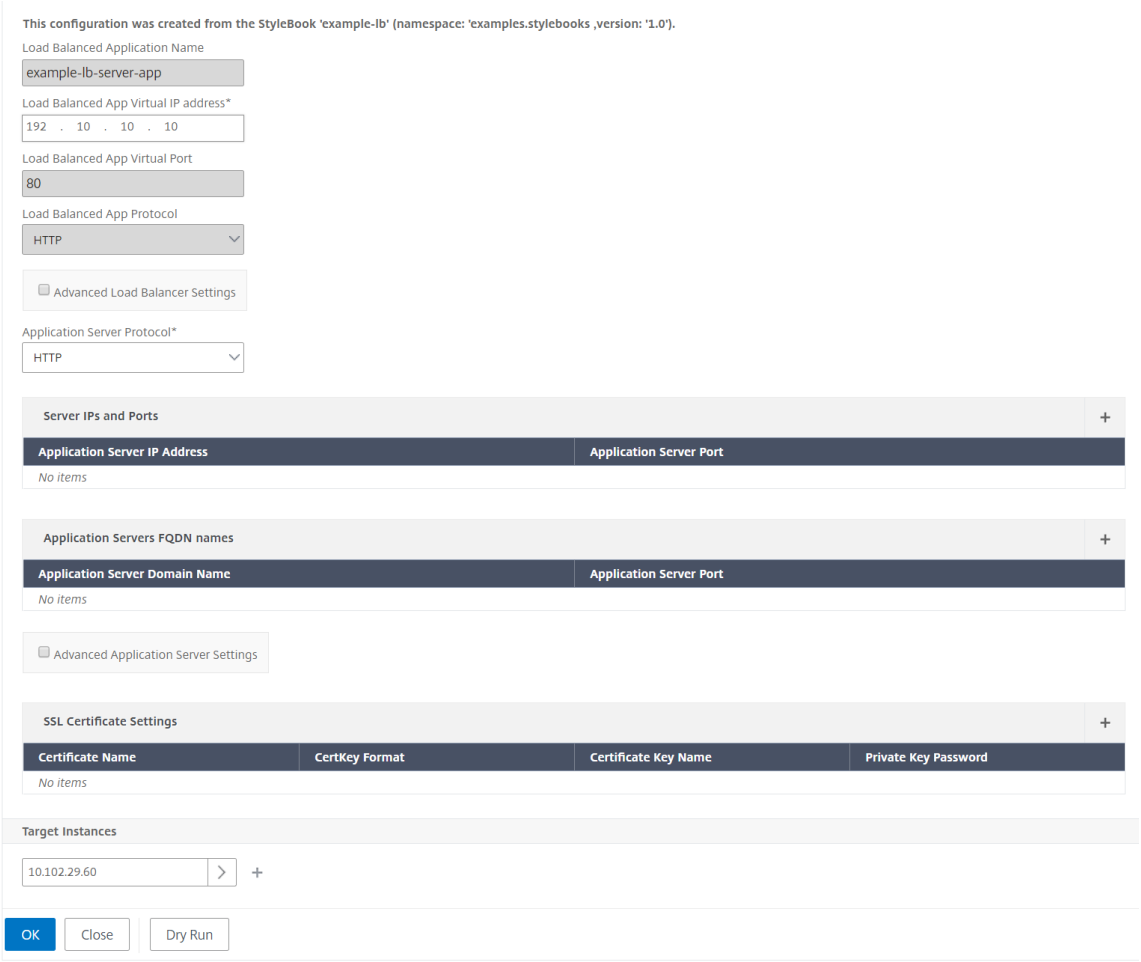
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**mon** y haga clic en **Seleccionar StyleBook**. También puede buscar el StyleBook escribiendo example-lb-mon.



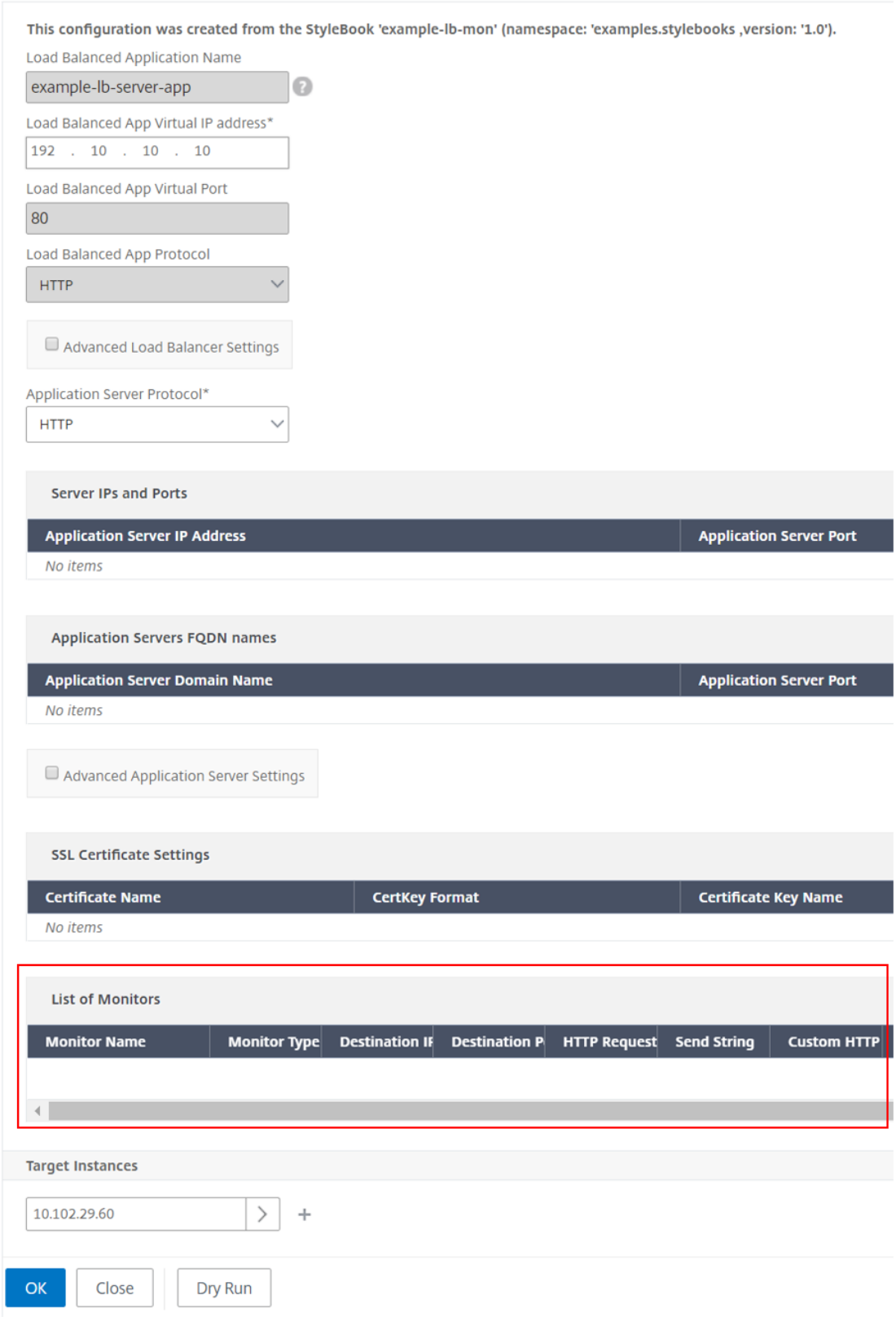

Si migras de un StyleBook a otro, es posible que todos los parámetros de los dos StyleBooks no tengan la misma estructura. Si la estructura de parámetros es similar, los valores anteriores se conservan automáticamente en los campos de parámetros. Es posible que algunos de los parámetros del nuevo StyleBook sean nuevos o que haya un cambio en su estructura. En tal caso, debe rellenar manualmente los valores de los parámetros de StyleBook. Por ejemplo, la siguiente imagen muestra los parámetros del StyleBook de ejemplo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La imagen siguiente muestra los parámetros después de migrar el paquete de configuración a example-lb-mon StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En este caso, puede ver que los StyleBooks conservan los valores anteriores para la configu-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

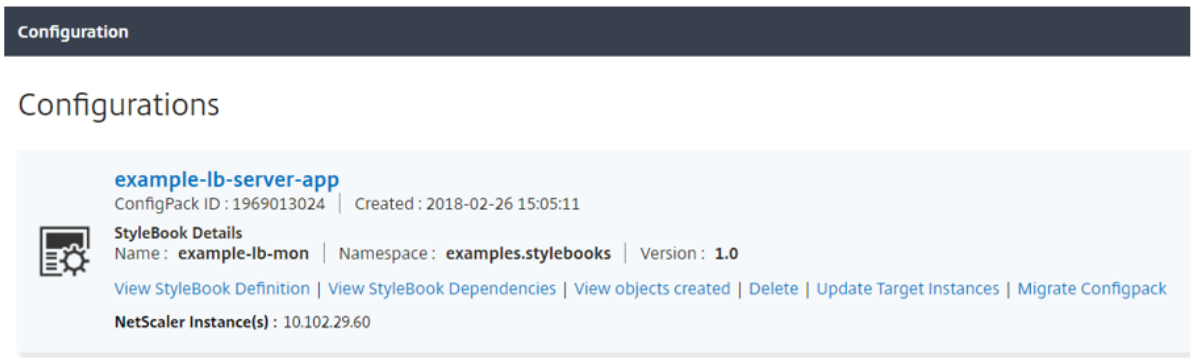
ración básica del balanceador de carga. Sin embargo, debe escribir manualmente los valores de los parámetros del monitor.

4. Escriba los valores de los nuevos parámetros utilizados para crear monitores en la instancia.
5. En **Instancias** de destino , haga clic en y seleccione la dirección IP de la instancia de Citrix ADC en la que quiere ejecutar la configuración. Tenga en cuenta que puede implementar la configuración en más de un Citrix ADC especificando tantas instancias de destino como sea necesario.
6. Haga clic en **Ejecutar en seco**. La página **Objetos** muestra los objetos que se crearían, modificarían o eliminarían recientemente de las instancias de Citrix ADC.
7. Haga clic en **Crear** para crear o actualizar la configuración de las instancias seleccionadas. El paquete de configuración se crea si las instancias de destino son nuevas. De lo contrario, se actualizan las configuraciones existentes implementadas en las instancias.

> **Nota**
>
> También puede hacer clic en el icono de actualización para agregar instancias de Citrix ADC descubiertas recientemente. Por lo tanto, estas instancias están disponibles al instante en la lista de instancias de esta ventana. El icono de actualización solo está disponible actualmente en Citrix ADM.

También puede migrar un paquete de configuración de una versión de un StyleBook a la siguiente. Aquí también es posible que tenga que escribir los valores de cualquier nuevo parámetro requerido presente en la nueva versión. También puede migrar el paquete de configuración a una versión anterior del StyleBook. En este caso, se eliminan los parámetros adicionales que no están presentes en el StyleBook anterior. La página **Objetos** muestra cualquiera de los objetos que se han eliminado de la configuración.

Después de una migración correcta, el ConfigPack está enlazado al nuevo StyleBook.




Puede ver que el nombre del paquete de configuración y el ID del paquete de configuración son los mismos que anteriormente. Pero NetScaler ADM actualiza el nombre de StyleBook a example-lb-mon desde example-lb.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crea sus StyleBooks

El contenido completo de **example-lb**StyleBook se proporciona a continuación para su referencia:

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb configuration objects
    properties-default-sources:
      - $parameters
```

El contenido completo de **example-lb-mon** StyleBook se proporciona a continuación para su referencia:

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
23    -
24      name: monitors
25      label: "List of Monitors"
26      description: "List of Monitors to monitor Application Servers"
27      type: cmtypes::monitor[]
28  substitutions:
29    mon-name(appname, monname): $appname + "-mon-" + $monname
30  components:
31    -
32      name: lb-comp
33      type: stlb::lb
34      description: Uses the default lb StyleBook to build the typical lb
           configuration objects
35      properties-default-sources:
36        - $parameters
37    -
38      name: monitors-comp
39      type: cmtypes::monitor
40      condition: $parameters.monitors
41      repeat: $parameters.monitors
42      repeat-item: mon
43      repeat-index: ndx
44      description: Builds a list of Citrix ADC monitor objects and binds
           them to the servicegroup of this LB config
45      properties-default-sources:
46        - $mon
47      properties:
48          monitorname: $substitutions.mon-name($parameters.lb-appname,
              $mon.monitorname)
49      components:
50        -
51          name: monitor-svcg-binding-comp
52          condition:  $parameters.svc-servers
53          type: ns::servicegroup_lbmonitor_binding
54          properties:
55            servicegroupname: $components.lb-comp.outputs.servicegroup.
                properties.servicegroupname
56            monitor_name: $parent.properties.monitorname
```

## Usar API para crear configuraciones a partir de StyleBooks

January 30, 2024

Una vez creado el StyleBook, tiene que importarlo a Citrix Application Delivery Management (ADM) para usarlo mediante Citrix ADM o mediante las API de Citrix ADM. NetScaler ADM valida el StyleBook al importarlo y, si la validación se realiza correctamente, el StyleBook aparece en el catálogo de StyleBooks de NetScaler ADM, listo para usarse en la creación de configuraciones.

Ahora puede usar las API de StyleBook para crear configuraciones basadas en este StyleBook. Puede

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

utilizar cualquier herramienta como la herramienta de línea de comandos curl o la extensión del explorador Chrome Postman para enviar solicitudes HTTP a NetScaler ADM.

### Ejemplo 1

Considere el StyleBook "lb-vserver"que ha creado en StyleBook para crear un servidor virtual de equilibrio de carga. Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
    example.stylebooks/0.1/lb-vserver/configpacks
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
 }

 }
```

En esta solicitud HTTP, el identificador (por ejemplo, "deecee30-f478-4446-9741-a85041903410") es el ID de instancia de NetScaler ADC en la que se crea el servidor virtual de equilibrio de carga lb1 con la dirección IP 10.102.117.31. El ID de instancia de la instancia de NetScaler ADC se recupera de NetScaler ADM.

Para obtener el ID de una instancia administrada por NetScaler ADM, puede utilizar las API de NetScaler ADM. Por ejemplo, para recuperar el ID de instancia de una instancia de Citrix ADC cuya dirección IP es 192.168.153.160, puede utilizar la siguiente API:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
    :192.168.153.160
```

```
Accept: application/json
```

La respuesta contiene el ID en la carga útil:

```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    …"id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }
```

Si el paquete de configuración se ha creado correctamente, recibirá la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }
```

Ha creado su primer paquete de configuración que se identifica de forma única mediante el id 1460806080. Puede utilizar este ID para consultar, actualizar o eliminar la configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Ejemplo 2

Puede utilizar el mismo StyleBook para crear otro paquete de configuración y ejecutarlo en las mismas instancias de NetScaler ADC o diferentes. En este ejemplo, cree otra configuración y proporcione un nombre y una dirección IP diferentes para el servidor virtual y también especifique LEASTCONNECTION como método de equilibrio de carga. Implemente esta configuración en dos instancias de NetScaler ADC.

La solicitud HTTP es la siguiente:

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
    example.stylebooks/0.1/lb-vserver/configpacks
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

    ]
   }

 }
```

En esta solicitud HTTP, el servidor virtual de equilibrio de carga lb2 con la dirección IP 10.102.117.32 se crea en las dos instancias NetScaler ADC representadas por los identificadores “deecee30-f478-4446-9741-a85041903410”y “debecc60-d589-4557-8632-a74032802412”.

Al crear correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
3  {
4
5    "configpack":
6   {
7
8      "config_id": "1657696292"
9    }
10
11  }
```

Este nuevo paquete de configuración tiene un ID diferente 165769629. Puede actualizar o eliminar esta configuración mediante este id.

### Ejemplo 3

Considere el StyleBook “basic-lb-config”que ha creado en StyleBook para crear una configuración básica de equilibrio de carga. Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
1  POST
2
3  http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
     .stylebooks/0.1/basic-lb-config/configpacks
```

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5    "configpack":
6    {
7
8      "parameters":
9      {
10
11       "name": "myapp",
12       "ip": "10.70.122.25",
13       "svc-servers":
14       ["192.168.100.11","192.168.100.12"],
15        "svc-port": 8080
16      }
17   ,
18     "target_devices":
19     [
20      {
21
22       "id": "deecee30-f478-4446-9741-a85041903410"
23       }
24   ,
25      {
26
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
27          "id": "debecc60-d589-4557-8632-a74032802412"
28          }
29
30        ]
31      }
32
33    }
```

En esta solicitud HTTP, la configuración de equilibrio de carga se ejecuta en dos instancias de NetScaler ADC. Puede iniciar sesión en estas instancias de NetScaler ADC para comprobar si se crean un servidor virtual y un grupo de servicios con dos servicios enlazados.

### Ejemplo 4

Considere el **ejemplo** compuesto de StyleBook que creó en Crear un StyleBook compuesto. Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
1  POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
       example.stylebooks/0.1/composite-example/configpacks
```

```
1  Content-Type: application/json
2  Accept: application/json
3  {
4
5    "configpack":
6    {
7
8      "parameters": {
9
10       "name": "myapp",
11       "ip": "2.2.2.2",
12       "svc-servers": ["10.102.29.52","10.102.29.53"]
13      }
14   ,
15     "target_devices":
16     [
17     {
18
19       "id": "deecee30-f478-4446-9741-a85041903410"
20      }
21   ,
22     {
23
24       "id": "debecc60-d589-4557-8632-a74032802412"
25      }
26
27     ]
28    }
29
30   }
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En esta solicitud HTTP, la configuración se crea en dos instancias de NetScaler ADC representadas por sus ID. Si inicia sesión en las instancias NetScaler ADC, puede ver los objetos de configuración creados por el StyleBook “basic-lb-config”que se importó en el StyleBook “composite-example”. También puede ver un nuevo monitor HTTP llamado “myapp-mon”que formaba parte del StyleBook de “ejemplos compuestos”.

Al crear correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }
```

#### Actualización de una configuración

Para actualizar esta configuración, por ejemplo, agregando un nuevo servidor back-end con dirección IP 10.102.29.54 al servidor virtual myapp de equilibrio de carga, utilice la API para actualizar un paquete de configuración de la siguiente manera:

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
    example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
   }
 ,
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
23      "id": "debecc60-d589-4557-8632-a74032802412"
24     }
25
26  ]
27   }
28
29   }
```

Al actualizar correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
1  200 OK
2  Content-Type: application/json
3  {
4
5     "configpack": {
6
7       "config-id": "4917276817"
8     }
9
10   }
```

### Eliminación de una configuración

Para eliminar esta configuración (de todas las instancias de NetScaler ADC), puede utilizar la API para eliminar un paquete de configuración de la siguiente manera:

```
1  DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
       example.stylebooks/0.1/composite-example/configpacks/4917276817
```

```
1  Accept: application/json
```

Al eliminar correctamente el paquete de configuración, se recibe la siguiente respuesta HTTP:

```
1  200 OK
2  Content-Type: application/json
3  {
4
5     "configpack": {
6
7       "config_id": "4917276817"
8     }
9
10   }
```

Puede iniciar sesión en la instancia de NetScaler ADC y comprobar que se han eliminado todos los objetos de configuración que forman parte de este paquete de configuración.

Si quiere quitar la configuración de instancias específicas de NetScaler ADC en lugar de todas, utilice la operación del paquete de configuración de actualización descrita anteriormente y cambie el atributo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

“target_devices”en la carga útil de JSON para quitar los identificadores de instancia específicos de NetScaler ADC.

## Usar API para crear configuraciones para cargar archivos de certificados y claves

January 30, 2024

Utilice las API de StyleBook para crear configuraciones basadas en este StyleBook. Puede utilizar cualquier herramienta como la herramienta de línea de comandos curl o la extensión del explorador Chrome Postman para enviar solicitudes HTTP a NetScaler Application Delivery Management (ADM).

Considere el ejemplo de StyleBook que creó para cargar los archivos de certificado y clave en Cómo crear un StyleBook para cargar certificados SSL y archivos de clave de certificado en NetScaler ADM. Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
    citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80"         }

       ],
           "certificates": [
               {

                   "cert-name": "server_cert",
                   "cert-file": "server_cert.pem",
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
                    "ssl-inform": "PEM",
                    "key-name": "server_key",
                    "key-file": "server_key.pem",
                    "cert-password": "secret",
                    "cert-advanced": {

                        "is-ca-cert": false,
                        "skip-ca-name": false
            }

          }

      ],
            "lb-advanced": {

                "flush-on-state-down": "ENABLED",
                "auth-params": {

                    "authentication": "OFF",
                    "authentication-http-401": "OFF"
          }
  ,
                "appflow-log": "ENABLED",
                "algorithm": "LEASTCONNECTION"
       }
  ,
            "svcg-advanced": {

                "svc-client-ip": "DISABLED",
                "svc-use-source-ip": "NO",
                "svc-use-proxy-port": "NO",
                "svc-surge-protection": "OFF",
                "svc-client-keepalive": "NO",
                "svc-tcp-buffering": "NO",
                "svc-compression": "NO",
                "svc-state": "ENABLED",
                "svc-downstate-flush": "DISABLED",
                "svc-enable-health-monitor": "NO"
       }

     }
  ,
       "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
       }

    ]
   }

  }
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Este paquete de configuración se identifica de forma única mediante el id 8c158e7a-0087-423f-91b0-0ccf16de552a. Puede utilizar este ID para consultar, actualizar o eliminar la configuración. Al actualizar correctamente el paquete de configuración, los archivos de certificado y clave se cargan en el sistema de archivos de NetScaler ADM.

## Use API para crear configuraciones para cargar cualquier tipo de archivo

January 30, 2024

También puede utilizar la API de NetScaler Application Delivery Management (ADM) para crear un paquete de configuración que cargue archivos en la instancia de NetScaler ADC seleccionada.

Considere el ejemplo de StyleBook que creó para cargar archivos de cualquier tipo enCómo crear un StyleBook para cargar archivos en NetScaler ADC MA Service. Como en el ejemplo del tema anterior, cree un paquete de configuración y especifique el valor del parámetro “locationfile”como la ruta del archivo de ubicación en NetScaler ADM.
Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera:

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
    stylebooks.samples/1.0/upload-geolocations/configpacks
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {

      "parameters": {

         "locationfile": "/var/mps/tenants/root/files/ /
         custom_geolocations.csv"
      }
 ,
      "targets": [
         {

            "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
        }

     ]
   }

```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
}
```

## Usar API para importar StyleBooks personalizados

January 30, 2024

Ahora puede utilizar las API de StyleBook para importar StyleBooks personalizados en NetScaler Application Delivery Management (ADM). Utilice la API REST para crear un paquete de configuración a partir de este StyleBook de la siguiente manera en cualquier herramienta como la herramienta de línea de comandos curl o la extensión del explorador Chrome Postman. Por ejemplo, puede importar un StyleBook denominado example-lb que se puede utilizar para crear una configuración de equilibrador de carga en una instancia de NetScaler ADC.

```
HTTP Method: POST
URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
Headers:
Content-Type: application/json
Accept: application/json
RequestBody:
{

        "stylebook":
  {

      "file_name": "example-lb.yaml",
      "source": "<base64-contents>",
      "encoding": "base64"
    }

 }
```

donde, el valor del atributo “source”, es la codificación en base64 del contenido del archivo StyleBook. Puede pegar el contenido YAML del archivo StyleBook en una herramienta en línea, por ejemplo,https://www.browserling.com/tools/file-to-base64 para obtener la cadena base64 que luego puede usar como valor para el atributo “fuente”anterior.

Mediante esta llamada a la API, también puede cargar un archivo comprimido (archivo TGZ) que contenga varios archivos StyleBook en una operación de API. Para ello, basta con cambiar el atributo file_name por el nombre de archivo .tgz y el valor del atributo source por la codificación base64 del contenido del archivo.tgz.

Después de ejecutar correctamente la API en la herramienta, obtendrá la siguiente respuesta que indica que el StyleBook se ha importado a NetScaler ADM.

```
200 OK
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Cuerpo de respuesta:**

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }
```

## Usar API para descargar StyleBooks personalizados

January 30, 2024

Puede descargar un StyleBook personalizado si proporciona la siguiente API REST de StyleBooks:

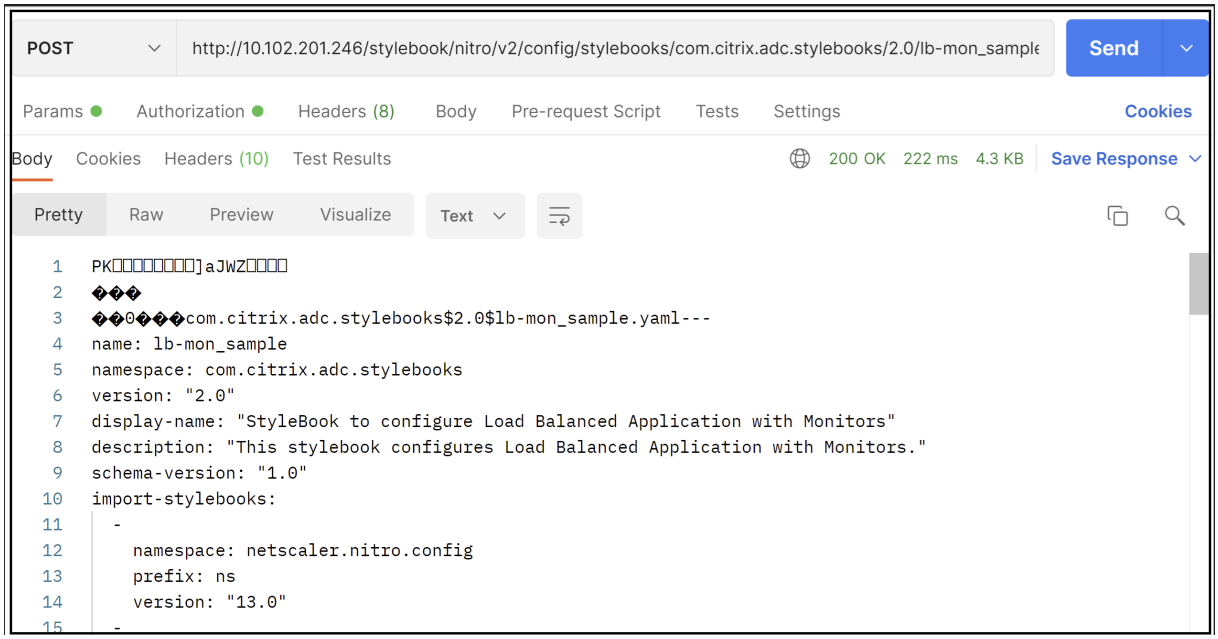
```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>/actions/download
```

Puede ejecutar la API en cualquier herramienta, como la herramienta de línea de comandos curl o la extensión del navegador Postman para Chrome, después de realizar modificaciones en los campos de dirección IP, nombre, versión y espacio de nombres.

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
    ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
```

Se descarga el StyleBook en formato.yaml.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Usar API para eliminar StyleBooks personalizados

January 30, 2024

Puede eliminar el StyleBook personalizado proporcionando la siguiente API REST de StyleBooks:

```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
```

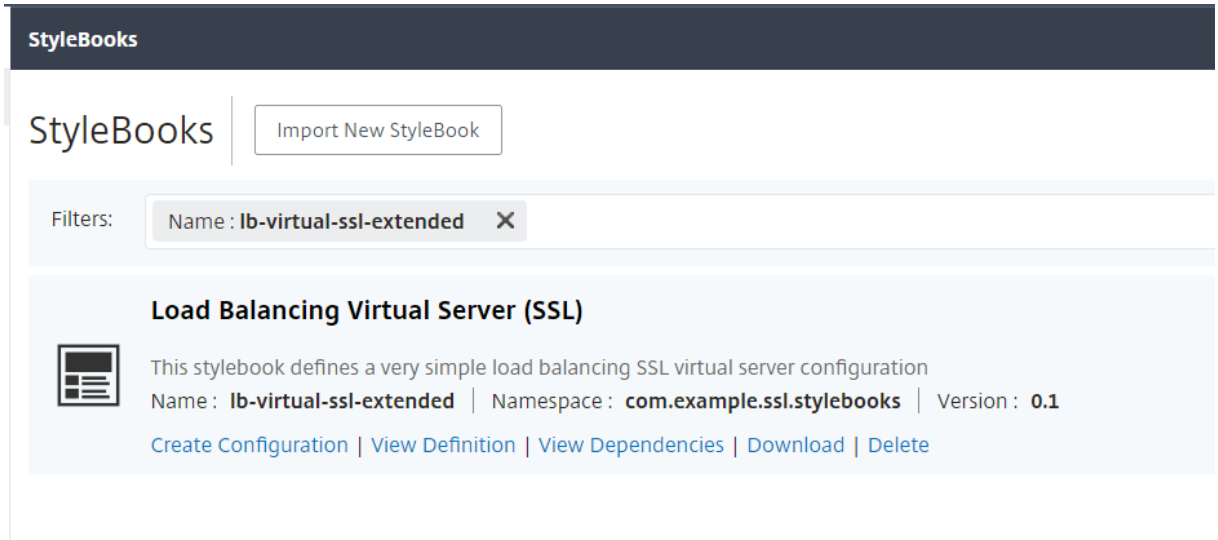
Si no se proporciona el parámetro de consulta de dependencias en la URL o su valor se establece en false, las dependencias de StyleBook no se eliminan (solo se elimina el propio StyleBook).

Cuando recibe un código de estado de respuesta HTTP de 200, significa que el StyleBook personalizado (y sus dependencias) se ha eliminado correctamente de Citrix ADM.

> **Nota**No
>
> puede eliminar un StyleBook personalizado que tenga otros StyleBooks en MA Service que dependan de él.

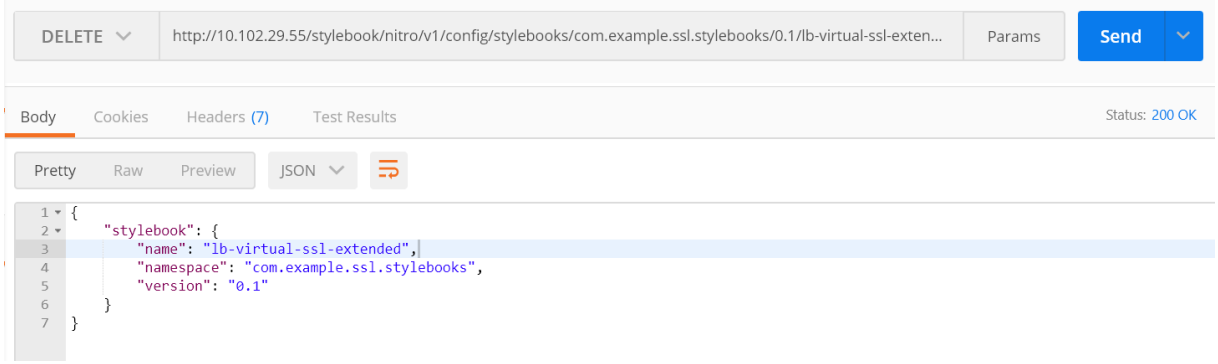
Por ejemplo, supongamos que ha creado un StyleBook denominado «lb-virtual-ssl-extended» en Citrix ADM. Más tarde decidió eliminar ese StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

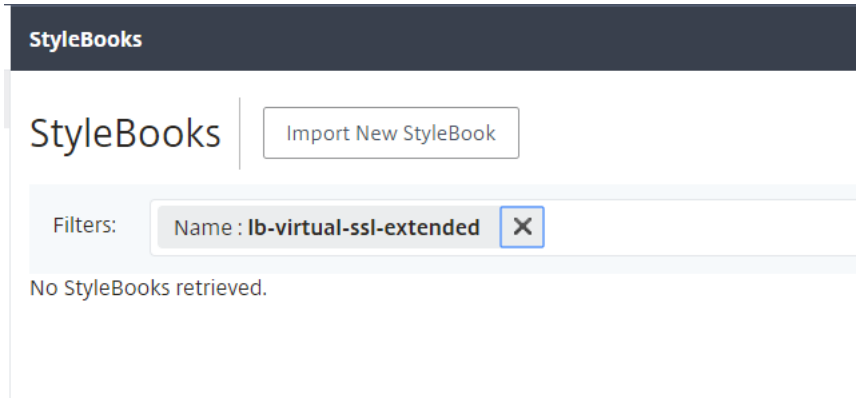



Puede ejecutar la API en cualquier herramienta, como la herramienta de línea de comandos curl o la extensión del navegador Postman para Chrome, después de realizar modificaciones en los campos de dirección IP, nombre, versión y espacio de nombres.

BORRARhttps://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false




El StyleBook se elimina de NetScaler ADM.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Gramática de StyleBooks

January 30, 2024

Puede diseñar sus propios StyleBooks, importarlos a Citrix Application Delivery Management (ADM) y, a continuación, usarlos para crear configuraciones mediante la GUI de Citrix ADM o mediante las API. Para poder crear sus propios StyleBooks, primero debes entender la gramática y la sintaxis de los diferentes constructos y atributos que puede usar.

Este documento describe las diferentes construcciones y referencias que puede utilizar al crear StyleBooks.

Haga clic en el nombre de una sección, componente fijo o referencia de la tabla siguiente para ver los detalles.

| | |
|—|—|
| [Header](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/header-section.html) | [Importar StyleBooks](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/import-stylebooks-section.html) |
| [Parameters](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-section.html) | [Construcción Parameters-Default-sources](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html) |
| [Substitutions](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions.html) | [Components](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/components.html) |
| [Propiedades opcionales](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebook grammar/optional-properties.html) | [Componentes auxiliares](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/helper-components.html) |
| [Fuentes predeterminadas de propiedades](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/properties-default-sources.html) | [Componentes anidados](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/nested-components.html) |
| [Construcción de condición](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebo grammar/condition-construct.html) | [Repetir componente fijo](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-construct.html) |
| [Construcción de condición de repetición](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/repeat-condition-construct.html) | [Outputs](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/outputs.html)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

|
| [Repeticiones anidadas](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks grammar/nested-repeats.html) | [Referencia de principal](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/parent-reference.html) |
| [Referencia de parámetros](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebo grammar/parameter-reference.html) | [Referencia de sustituciones](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/substitutions-reference.html) |
| [Referencia de componentes](/es-es/netscaler-application-delivery-management-software/13/stylebooks/styleb grammar/components-reference.html) | [Operations](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/operations.html) |
| [Referencia de variable](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks- grammar/variable-reference.html) | [Alarms](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/alarms.html) |
| [Analytics](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/analytics.html) | [Funciones integradas](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/built-in-functions.html) |
| [Expressions](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/expressions.html) | [Detección de dependencias](/es-es/netscaler-application-delivery-management-software/13/stylebooks/stylebooks-grammar/dependency-detection.html) |
| Interpolaciones in situ |

> **Nota**
>
> Al definir el elemento de repetición, el índice de repetición o los argumentos de las funciones de sustitución, no utilice las siguientes palabras reservadas para nombrar una variable definida por el usuario, `$<var-name>`
>
> - libro de estilos, parámetros, sustituciones, componentes, propiedades, salidas, elemento principal, propio, operaciones, análisis, alarmas
> - repeat-item, repeat-item-0, repeat-item-1, repeat-item-2
> - índice de repeticiones, índice de repeticiones 0, índice de repeticiones 1, índice de repeticiones 2
> - default
> - funciones, función, objetivos, objetivo
> - context, parent-context, parent_context

Para obtener información y ejemplos sobre cómo diseñar sus propios StyleBooks, consulta Cómo crear sus propios StyleBooks.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Header

January 30, 2024

Las seis primeras líneas de un StyleBook forman la sección de cabecera. Esta sección permite definir la identidad de un StyleBook y describir su función. Se trata de una sección obligatoria.

En la tabla siguiente se describen los atributos de la sección de encabezado:

|Atributo| Descripción|
|—|—|
|name |Un nombre para identificar el StyleBook. Este atributo es obligatorio. |
|display-name |Nombre descriptivo del StyleBook. Este nombre aparece en la GUI de NetScaler ADM. Este es un atributo opcional. |
|description |Un texto de descripción define lo que hace este StyleBook. Esta descripción aparece en la GUI de ADM. Este es un atributo opcional. **Nota:** Se trata de un fragmento HTML y puede usar etiquetas HTML para personalizar los encabezados o insertar imágenes mediante la etiqueta `<img>` con URL o imágenes incrustadas. |
|author |Autor, persona u organización que crea el StyleBook. Este es un atributo opcional. |
| namespace|Un espacio de nombres forma parte de un identificador único de un StyleBook para evitar colisiones de nombres. Un espacio de nombres puede ser cualquier cadena, pero se recomienda utilizarla para asignar un nombre a la empresa, el departamento o la unidad que creó o posee un conjunto de StyleBooks. Por ejemplo, puede utilizar el siguiente formato: `<company>.<department>.<unit>.stylebooks`. Se trata de un atributo obligatorio. |
|version |El número de versión del StyleBook. Puede cambiar el número de versión al actualizar un StyleBook. Los StyleBooks de diferentes versiones pueden coexistir juntos. Se trata de un atributo obligatorio. |
|schema-version |La versión del esquema de StyleBooks. Toma el valor «1.0” de la versión actual de NetScaler ADM. Se trata de un atributo obligatorio. |
|private |Si este atributo se establece en true, el StyleBook no se muestra en la GUI de NetScaler ADM. Esta es una configuración útil para los StyleBooks, que son componentes básicos de otros StyleBooks y no están pensados para que los usuarios los utilicen directamente. Este es un atributo opcional. Su valor predeterminado es false. |
|

**Ejemplo**:

```
1     name: lb
2     description: "This stylebook defines a sample load balancing
     configuration."
3     display-name: "Load Balancing StyleBook (HTTP)"
4     author: Mike Smith (ACME Infra team)
5     namespace: com.example.stylebooks
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
6     schema-version: "1.0"
7     version: "0.1"
```

La combinación de nombre , espacio de nombres y versión identifica de forma única un StyleBook en el sistema. No puede tener dos StyleBooks con la misma combinación de nombre, espacio de nombres y versión en NetScaler ADM. Sin embargo, puede tener dos StyleBooks con el mismo nombre y versión pero espacios de nombres diferentes, o con el mismo espacio de nombres y versión pero nombres diferentes.

## Importar StyleBooks

January 30, 2024

Esta es la segunda sección de tu StyleBook y te permite declarar a qué otro StyleBook quieres hacer referencia desde tu StyleBook actual. Esto le permite importar y reutilizar otros StyleBooks en lugar de volver a crear la misma configuración en su propio StyleBook. Se trata de una sección obligatoria.

Debe declarar el espacio de **nombres** y el número de **versión** de los StyleBook a los que desea hacer referencia en su StyleBook actual. Cada StyleBook debe hacer referencia al espacio de nombres netscaler.nitro.config si utiliza directamente cualquiera de los objetos de configuración NITRO. Este espacio de nombres contiene todos los tipos de Citrix ADC NITRO, como lbvserver service o monitor. Se admiten los StyleBooks para NetScaler ADC versiones 10.5 y posteriores, lo que significa que puede utilizar su StyleBook para crear y ejecutar configuraciones en cualquier instancia de NetScaler ADC que ejecute la versión 10.5 o posterior.

El atributo **prefix** utilizado en la sección import-stylebooks es una abreviatura para referirse a la combinación de espacio de nombres y versión. Por ejemplo, el prefijo “ns”se puede utilizar para hacer referencia al espacio de nombres netscaler.nitro.config con la versión 10.5. En las secciones posteriores de su StyleBook, en lugar de utilizar el espacio de nombres y la versión cada vez que quiera hacer referencia a un StyleBook con este espacio de nombres y versión, puede utilizar simplemente la cadena de prefijos elegida junto con el nombre del StyleBook para identificarlo de forma única.

**Ejemplo**:

```
1     import-stylebooks:
2      -
3        namespace: netscaler.nitro.config
4        version: "10.5"
5        prefix: ns
6     -
7      namespace: com.acme.stylebooks
8       version: "0.1"
9       prefix: stlb
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En el ejemplo anterior, el primer prefijo definido se denomina ns y hace referencia al espacio de nombres netscaler.nitro.config y a la versión 10.5. El segundo prefijo que se define se denomina stlb y hace referencia al espacio de nombres com.acme.stylebooks y a la versión 0.1.

Después de definir un prefijo, cada vez que quiera hacer referencia a un tipo o a un StyleBook que pertenece a un espacio de nombres y versión determinados, puede usar la notación**<namespace-shorthand>:: <type-name>. Por ejemplo, **ns::lbvserver** hace referencia al tipo lbvserver definido en el espacio de nombres netscaler.nitro.config, versión 10.5.

Del mismo modo, si quiere hacer referencia a un StyleBook con la versión "0.1"en el espacio de nombres com.acme.stylebooks, puede usar la notación**stlb:: <stylebook-name>**.

> **Nota**
>
> Por convención, el prefijo «ns» se utiliza para hacer referencia al espacio de nombres NITRO de Citrix ADC.

## Parámetros

January 30, 2024

Esta sección le permite definir todos los parámetros que necesita en su StyleBook para crear una configuración. Describe la entrada que toma su StyleBook. Aunque esta sección es opcional, la mayoría de StyleBook puede necesitar una. Puede considerar la sección de parámetros para definir los campos de los usuarios que utilizan StyleBook para crear una configuración en una instancia de NetScaler ADC.

Al importar el StyleBook a NetScaler ADM y utilizarlo para crear una configuración, la GUI utiliza esta sección del StyleBook para mostrar un formulario. Este formulario toma una entrada para los valores de parámetro definidos.

En la siguiente sección se describen los atributos que debe especificar para cada parámetro de esta sección:

### '**nombre**'

El nombre del parámetro que quiere definir. Puede especificar un nombre alfanumérico.

El nombre debe comenzar con un alfabeto, y puede incluir más alfabetos, números, guión (-) o guión bajo (_).

Al escribir un StyleBook, puede utilizar este atributo "name"para hacer referencia al parámetro en otras secciones mediante la notación $parameters. <name>.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

¿**Obligatorio**? Sí

### ‘**etiqueta**’

Cadena que se muestra en la GUI de ADM como nombre de este parámetro.

¿**Obligatorio**? No

### ‘**descripción**’

Cadena de ayuda que describe para qué se utiliza el parámetro. La GUI de ADM muestra este texto cuando el usuario hace clic en el icono de ayuda de este parámetro.

¿**Obligatorio**? No

### ‘**tipo**’

El tipo de valor que pueden tomar estos parámetros. Los parámetros pueden ser de cualquiera de los siguientes tipos incorporados:

- cadena: matriz de caracteres. Si no se especifica una longitud, el valor de cadena puede tener cualquier número de caracteres. Sin embargo, puede limitar la longitud de un tipo de cadena utilizando los atributos longitud mínima y longitud máxima.
- `number`: un número entero. Puede especificar el número mínimo y máximo que puede tomar este tipo mediante los atributos valor mínimo y valor máximo.
- **`boolean`**: Puede ser verdadero o falso. YAML considera todos los literales como booleanos (por ejemplo, Sí o No).
- `ipaddress`: cadena que representa una dirección IPv4 o IPv6 válida.
- `tcp-port`: número entre 0 y 65535 que representa un puerto TCP o UDP.
- `password`: Representa un valor de cadena opaca/secreta. Cuando la GUI de ADM muestra un valor para este parámetro, se muestra como asteriscos (*****).
- `certfile`: Representa un archivo de certificado. Este valor le permite cargar los archivos directamente desde su sistema local al crear una configuración de StyleBook mediante la GUI ADM. El archivo de certificado cargado se almacena en el directorio `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` de ADM.

  El archivo de certificado se agrega a la lista de certificados administrados por ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- `keyfile`: Representa un archivo de clave de certificado. Este valor le permite cargar el archivo directamente desde su sistema local al crear una configuración de StyleBook mediante la GUI ADM. El archivo de certificado cargado se almacena en el directorio `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` de ADM.

  El archivo de clave de certificado se agrega a la lista de claves de certificado administradas por ADM.

- `file`: Representa un archivo.
- `object`: este tipo se utiliza cuando se quiere agrupar varios parámetros relacionados bajo un elemento principal. Especifique el parámetro principal el tipo como "objeto". Un parámetro de tipo "objeto"puede tener una sección de "parámetros"anidada para describir los parámetros que contiene.
- `another StyleBook`: cuando se utiliza este tipo de parámetro, este parámetro espera que su valor tenga la forma de los parámetros definidos en el StyleBook que denota su tipo.

Un parámetro también puede tener una `type` que es la lista de tipos. Para ello, agregue `[]` al final del tipo. Por ejemplo, si el atributo `type` es `string[]`, este parámetro toma una lista de cadenas como entrada. Puede proporcionar una, dos o varias cadenas para este parámetro al crear una configuración a partir de este StyleBook.

¿**Obligatorio**? Sí

### '**red**'

Para `type: ipaddress`, puede especificar el atributo `network` para asignar automáticamente una dirección IP de una red de IPAM ADM.

ADM asigna automáticamente una dirección IP del atributo `network` cuando se crea una configuración de StyleBook.

Ejemplo :

```
1       name: virtual-ip
2       label: "Load Balancer IP Address"
3       type: ipaddress
4       network: "network-1"
5       required: true
```

En este ejemplo, el campo `virtual-ip` asigna automáticamente una dirección IP de `network-1`. La dirección IP se libera de nuevo a la red cuando se elimina la configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘asignación dinámica’

El atributo `dynamic-allocation` se agrega en la definición de parámetro de `type:ipaddress`. Utilice este atributo para enumerar dinámicamente las redes de IPAM de ADM. Este atributo puede tomar **`true`** o **`false`** como una entrada. Para `type: ipaddress`, especifique el atributo `dynamic-allocation: true` para mostrar dinámicamente las redes de IPAM de ADM que están en ADM. En el formulario de creación del paquete de configuración, puede hacer lo siguiente:

1. Seleccione la red IPAM requerida de la lista.
2. Especifique la dirección IP que quiere asignar desde la red IPAM seleccionada.

   Si no se especifica ninguna dirección IP, el ADM asigna automáticamente una dirección IP de la red IPAM seleccionada.

**Ejemplo:**

```
1   -
2     name: virtual-ip
3     label: "Load Balancer IP Address"
4     type: ipaddress
5     dynamic-allocation: true
6     required: true
```

En este ejemplo, el `virtual-ip` campo muestra las redes de IPAM de ADM que están en ADM. Seleccione una red de la lista para asignar automáticamente una dirección IP de la red. La dirección IP se libera de nuevo a la red cuando se elimina la configuración.

### ‘Tecla’

Especifique true o false para indicar si este parámetro es un parámetro clave para StyleBook.

Un StyleBook solo puede tener un parámetro definido como parámetro “clave”.

Al crear configuraciones diferentes a partir del mismo StyleBook (en las mismas instancias ADC o diferentes), cada configuración tiene un valor diferente/único para este parámetro.

El valor predeterminado es false.

¿**Obligatorio**? No

### “requerido”

Especifique true o false para indicar si un parámetro es obligatorio u opcional. Si se establece en true, el parámetro es obligatorio y el usuario debe proporcionar un valor para este parámetro al crear configuraciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La GUI ADM obliga al usuario a proporcionar un valor válido para este parámetro.

El valor predeterminado es false.

¿**Obligatorio**? No

### ‘allowed-values’

Utilice este atributo para definir una lista de valores válidos para un parámetro, cuando el tipo se establece en “cadena”.

Al crear una configuración a partir de la GUI de ADM, se solicita al usuario que seleccione un valor de parámetro de esta lista.

> **Nota:**
>
> Si quiere mostrar los valores de la lista como opciones de radio, defina el atributo `layout`.

**Ejemplo 1**:

```
-
      name: ipaddress
      type: string
      allowed-values:
            -  SOURCEIP
            -  DEST IP
            -  NONE
```

**Ejemplo 2**:

```
-
      name: TCP Port
      type: tcp-port
      allowed-values:
            -  80
            -  81
            -  8080
```

**Ejemplo 3**:

Lista de `tcp-ports`, donde cada elemento de la lista solo puede tener valores especificados en `allowed-values`.

```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

¿**Obligatorio**? No

### ‘predeterminado’

Utilice este atributo para asignar un valor predeterminado a un parámetro opcional. Cuando un usuario crea una configuración sin especificar un valor, se utiliza el valor predeterminado.

El parámetro no toma ningún valor si se cumplen las siguientes condiciones:

- El parámetro no tiene ningún valor predeterminado.
- Un usuario no proporciona un valor para el parámetro.

**Ejemplo 1**:

```
-
      name: timeout
      type: number
      default: 20
```

**Ejemplo 2**:

Para enumerar los valores predeterminados del parámetro:

```
-
      name: protocols
      type: string[]
      default:
            -  TCP
            -  UDP
            -  IP
```

**Ejemplo 3**:

```
-
      name: timeout
      type: number
      default: 20
```

**Ejemplo 4**:

```
-
      name: tcpport
      type: tcp-port
      default: 20
```

¿**Obligatorio**? No

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘patrón’

Utilice este atributo para definir un patrón (expresión regular) para los valores válidos de este parámetro, cuando el tipo del parámetro sea “cadena”.

**Ejemplo**:

```
-
      name: appname
      type: string
      pattern: "[a-z]+"
```

¿**Obligatorio**? No

### ‘valor mín’

Utilice este atributo para definir el valor mínimo de los parámetros de tipo `number` o `tcp-port`.

**Ejemplo**:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
```

El `min-value` de números puede ser negativo. Sin embargo, el `min-value` para `tcp-port` debe ser positivo.

¿**Obligatorio**? No

### ‘valor máx’

Utilice este atributo para definir el valor máximo de los parámetros de tipo `number` o `tcp-port`.

Asegúrese de que el valor máximo es mayor que el valor mínimo, si se define.

**Ejemplo**:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
      max-value: 15000
```

¿**Obligatorio**? No

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘longitud mín’

Utilice este atributo para definir la longitud mínima de los valores aceptados para un parámetro de tipo “cadena”.

Asegúrese de que la longitud mínima de los caracteres definidos como valores sea mayor o igual a cero.

**Ejemplo**:

```
-
      name: appname
      type: string
      min-length: 3
```

¿**Obligatorio**? No

### ‘longitud máx’

Utilice este atributo para definir la longitud máxima de los valores aceptados para un parámetro de tipo “cadena”.

Asegúrese de que la longitud máxima de los valores sea mayor o igual a la longitud de los caracteres definidos en `min-length`.

**Ejemplo**:

```
-
      name: appname
      type: string
      max-length: 64
```

¿**Obligatorio**? No

### ‘min-artículos’

Utilice este atributo para definir el número mínimo de elementos en un parámetro que es una lista.

Asegúrese de que el número mínimo de elementos sea mayor o igual a cero.

**Ejemplo**:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
```

¿**Obligatorio**? No

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘Máx-artículos’

Utilice este atributo para definir el número máximo de elementos en un parámetro que es una lista.

Asegúrese de que el número máximo de elementos sea mayor que el número mínimo de elementos si se define.

**Ejemplo**:

```
-
      name: server-ips
      type: ipaddress[]
      min-items: 2
      max-items: 250
```

¿**Obligatorio**? No

### ‘gui’

Utilice este atributo para personalizar el diseño del parámetro en la GUI de ADM.

¿**Obligatorio**? No

### ‘columnas’

Este atributo es un subatributo del atributo `gui`. Utilice este atributo para definir el número de columnas para mostrar los `type: object[]` parámetros en la GUI de ADM.

¿**Obligatorio**? No

### ‘updatable’

Este atributo es un subatributo del atributo `gui`. Utilice este atributo para especificar si el parámetro se puede actualizar después de crear la configuración. Establezca este atributo solo en tipos de parámetros simples como string, booleano o number.

Si el valor se establece en **`false`**, el campo de parámetro aparece atenuado cuando se actualiza la configuración.

¿**Obligatorio**? No

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘colapse_pane’

Este atributo es un subatributo del atributo `gui`. Utilice este atributo para especificar si el panel que define el diseño de este parámetro de objeto se puede contraer.

Si el valor se establece en true, el usuario puede expandir o contraer los parámetros secundarios bajo este parámetro principal.

**Ejemplo**:

```
gui:

 collapse_pane: true

 columns: 2
```

Ejemplo de una sección completa de parámetros:

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -

      name: ip

      label: IP Address

      description: The virtual IP address used for this application

      type: ipaddress

      required: true

   -

      name: svc-servers

      label: Servers

      type: object[]

      required: true
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
36
37        parameters:
38
39          -
40
41                name: svc-ip
42
43                label: Server IP
44
45                description: The IP address of the server
46
47                type: ipaddress
48
49                required: true
50
51          -
52
53                name: svc-port
54
55                label: Server Port
56
57                description: The TCP port of the server
58
59                type: tcp-port
60
61                default: 80
62
63          -
64
65                name: lb-alg
66
67                label: LoadBalancing Algorithm
68
69                type: string
70
71                allowed-values:
72
73                   - ROUNDROBIN
74
75                   - LEASTCONNECTION
76
77                default: ROUNDROBIN
78
79          -
80
81                name: enable-healthcheck
82
83                label: Enable HealthCheck?
84
85                type: boolean
86
87                default: true
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

A continuación se muestra un ejemplo que define todos los atributos de una lista y los valores explicados en secciones anteriores:

```
        -
            name: features-list

            type: string[]

            min-length: 1

            max-length: 3

            min-items: 1

            max-items: 3

            pattern: "[A-Z]+"

            allowed-values:

              - SP

              - LB

              - CS

            default:

              - LB
```

### ‘diseño’

Este atributo es un subatributo del atributo `gui`. Utilice este atributo para mostrar los valores de la lista como botones de opción. Establezca el atributo `layout` en `radio` en la sección de parámetros de una definición de StyleBook. Se aplica al parámetro que contiene el atributo `allowed-values`. Al crear un paquete de configuración, la GUI de ADM muestra los valores de la lista `allowed-values` como botones de opción.

Ejemplo :

```
-
    gui:
        layout: radio
    allowed-values:
        - One
        - Two
        - Three
```

Los valores Uno, Dos y Tres aparecen como botones de opción en la GUI ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ‘parámetros dependientes’

Este atributo es un subatributo del atributo `gui`. Controla dinámicamente el aspecto del parámetro o su valor inicial en el formulario de configuración de StyleBook basándose en el valor especificado en otro parámetro.

Especifique este atributo en un parámetro de origen que controle el comportamiento del parámetro en el formulario. Puede incluir varias condiciones que controlen otros parámetros. Por ejemplo, un parámetro de origen `protocol` puede tener un parámetro dependiente `certificate`, que solo aparece si el valor del parámetro `protocol` es `SSL`.

Cada condición puede tener los siguientes atributos:

- **target-parameter**: especifique el parámetro de destino al que se aplica esta condición.
- **valores de coincidencia**: especifique la lista de valores del parámetro de origen que activan la acción.
- **acción**: especifique una de las siguientes acciones en el parámetro de destino:
  - `read-only`: El parámetro se hace de solo lectura.
  - `show`: el parámetro aparece en el formulario si está oculto.
  - `hide`: el parámetro se elimina del formulario.
  - `set-value`: El valor del parámetro se establece en el valor especificado en el atributo value.
- **value**: Valor del parámetro objetivo si la acción es `set-value`.

Cuando una entrada de usuario coincide con los valores especificados en el parámetro de origen, el aspecto o el valor del parámetro de destino cambia de acuerdo con la acción especificada.

**Ejemplo:**

```
1  -
2     name: lb-virtual-port
3     label: "Load Balanced App Virtual Port"
4     description: "TCP port representing the Load Balanced application"
5     type: tcp-port
6     gui:
7       updatable: false
8       dependent-parameters:
9             -
10              matching-values:
11                - 80
12              target-parameter: $parameters.lb-service-type
13              action: set-value
14              allowed-values:
15              - HTTP
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
16                - TCP
17                - UDP
18
19      default: 80
```

En este ejemplo, el parámetro dependiente se especifica en el parámetro `lb-virtual-port` (parámetro source).

Cuando el valor del parámetro de origen se establece en `80`, el parámetro `lb-service-type` activa la acción `set-value`. Como resultado, un usuario puede seleccionar una de las siguientes opciones:

- HTTP
- TCP
- UDP

## Construcción Parameters-Default-sources

January 30, 2024

Puede utilizar esta construcción para reutilizar las definiciones de parámetros de otros StyleBooks.

Considere un caso en el que un parámetro o un grupo de parámetros se utiliza repetidamente en varios StyleBooks. Para evitar redefinir estos parámetros, cada vez que quiera crear un nuevo StyleBook, puede definirlos una vez y, a continuación, importar sus definiciones a los StyleBooks que los necesiten mediante la construcción **parameters-default-sources**.

Por ejemplo, si muchos de sus StyleBooks necesitan configurar una IP virtual, es posible que tenga que definir los mismos parámetros relacionados con las IP virtuales en cada nuevo StyleBook que cree. En su lugar, puede crear un StyleBook independiente llamado, por ejemplo, “vip-params”, donde defina todos los parámetros relacionados con él, como se muestra en el siguiente ejemplo:

```
1       -
2       name: vip-params
3       namespace: com.acme.commontypes
4       version: "1.0"
5       description: This StyleBook defines a typical virtual IP config.
6       private: true
7       schema-version: "1.0"
8       parameters:
9         -
10            name: lb-appname
11            label: Load Balanced Application Name
12           description: Name of the Load Balanced application
13            type: string
14            required: true
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
15          -
16              name: lb-virtual-ip
17              label: Load Balanced App Virtual IP address
18              description: Virtual IP address representing the Load
        Balanced application
19              type: ipaddress
20              required: true
21          -
22              name: lb-virtual-port
23              label: Load Balanced App Virtual Port
24              description: TCP port representing the Load Balanced
        application
25              type: tcp-port
26              default: 80
27          -
28              name: lb-service-type
29              label: Load Balanced App Protocol
30              description: Protocol used for the Load Balanced application
        .
31              type: string
32              default: HTTP
33              required: true
34              allowed-values:
35                   - HTTP
36                   - SSL
37                   - TCP
```

A continuación, puede crear otros StyleBooks que utilicen estos parámetros. Lo que sigue es un ejemplo de tal StyleBook.

```
1       -
2       name: acme-biz-app
3       namespace: com.acme.stylebooks
4       version: "1.0"
5       description: This stylebook defines the Citrix ADC configuration
        for Biz App
6       schema-version: "1.0"
7       import-stylebooks:
8         -
9           namespace: com.acme.commontypes
10          prefix: cmtypes
11          version: "1.0"
12      parameters-default-sources:
13            - cmtypes::vip-params
14      parameters:
15          -
16            name: monitorname
17            label: Monitor Name
18            description: Name of the monitor
19            type: string
20            required: true
21          -
22            name: type
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
23            label: Monitor Type
24            description: Type of the monitor
25            type: string
26            required: true
27            allowed-values:
28              - PING
29              - TCP
30              - HTTP
31              - HTTP-ECV
32              - TCP-ECV
33              - HTTP-INLINE
```

En StyleBook, acme-biz-app, primero se importan el espacio de nombres y la versión del StyleBook de vip-params mediante la sección "importar libros de estilos". A continuación, se agrega la construcción **parameters-default-sources** y se especifica el nombre de StyleBook, es decir, vip-params. Esto tiene el mismo efecto que definir los parámetros del StyleBook de parámetros vip-params directamente en este StyleBook.

Puede incluir parámetros de varios StyleBooks porque los parameters-default-sources es una lista y se espera que cada elemento de la lista sea un StyleBook.

Además de incluir parámetros de otros StyleBooks, también puede definir sus propios parámetros mediante la sección de parámetros. La lista completa de parámetros del StyleBook es la combinación de los parámetros incluidos en otros StyleBook y los parámetros definidos en este StyleBook. Por lo tanto, la expresión **$parameters** hace referencia a esta combinación de parámetros.

Tenga en cuenta que si un parámetro se define tanto en un StyleBook importado como en el StyleBook actual, la definición del StyleBook actual anula la definición importada de otro StyleBook. Puede utilizar esto de manera eficaz personalizando algunos de los parámetros importados si es necesario, mientras usa el resto de los parámetros importados tal como están.

La construcción parameters-default-sources también se puede utilizar en parámetros anidados como se muestra:

```
1  parameters:
2      -
3        name: vip-details
4        label: Virtual IP details
5        description: Details of the Virtual IP
6        type: object
7        required: true
8        parameters-default-sources:
9                - cmtypes::vip-params
```

Esto es similar a agregar los parámetros de los parámetros vip de StyleBook directamente como parámetros secundarios del parámetro vip-details en este StyleBook.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Sustituciones

January 30, 2024

La sección de sustituciones se usa para definir nombres abreviados para expresiones complejas que se pueden usar en el resto del StyleBook para facilitar la lectura del StyleBook. También son útiles cuando la misma expresión o valor se repite más de una vez en el StyleBook, por ejemplo, un valor constante. El uso de un nombre de sustitución para este valor le permite actualizar solo el valor de sustitución cuando sea necesario cambiarlo, en lugar de actualizarlo en cada ubicación en la que aparezca en el StyleBook, lo que podría provocar errores.

Las sustituciones también se utilizan para definir asignaciones entre valores como se describe en ejemplos más adelante en este documento.

Cada sustitución de la lista se compone de una clave y un valor. El valor puede ser un valor simple, una expresión, una función o un mapa.

En el siguiente ejemplo, se definen dos sustituciones. El primero es «http-port», que se puede usar como abreviatura de 8181. Al usar una sustitución, puede referirse a esto en el resto del StyleBook como **$substitutions.http-port** en lugar de 8181.

**sustituciones**:

puerto http: 8181

Esto le permite especificar un nombre mnemotécnico para un número de puerto, así como definir este número de puerto en un solo lugar del StyleBook, independientemente del número de veces que se utilice. Si desea modificar el número de puerto a 8080, puede modificarlo en la sección de sustitución y el cambio tendrá efecto siempre que se utilice el nombre mnemotécnico http-port. En el ejemplo siguiente se muestra cómo se utiliza una sustitución en un componente.

```
1  components:
2   -
3       name: my-lbvserver-comp
4       type: ns::lbvserver
5       properties:
6            name: $parameters.name + "-lb"
7            servicetype: HTTP
8            ipv46: $parameters.ip
9            port: \*\*$substitutions.http-port\*\*
10           lbmethod: $parameters.lb-alg
```

Una sustitución también puede ser una expresión compleja. El siguiente ejemplo muestra cómo dos sustituciones utilizan expresiones.

```
1  substitutions:
2    app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
3    app-name: str("acme-") + $parameters.name + str("-app")
```

Una expresión de sustitución también puede utilizar expresiones de sustitución existentes, como se muestra en el siguiente ejemplo.

```
1 substitutions:
2   http-port: 8181
3   app-name: str("acme-") + $parameters.name + str($substitutions.http-
     port) + str("-app")
```

Otra función útil de las sustituciones son los mapas, donde puede asignar claves a valores. El siguiente es un ejemplo de sustitución de mapas.

```
1 substitutions:
2     secure-port:
3         true: int("443")
4         false: int("80")
5     secure-protocol:
6         true: SSL
7         false: HTTP
```

En el ejemplo siguiente se muestra cómo utilizar los mapas de puerto seguro y protocolo seguro.

```
1 components:
2  -
3      name: my-lbvserver-comp
4      type: ns::lbvserver
5      properties:
6           name: $parameters.name + "-lb"
7           servicetype: $substitutions.secure-protocol[$parameters.is-
     secure]
8           ipv46: $parameters.ip
9           port: $substitutions.secure-port[$parameters.is-secure]
10          lbmethod: $parameters.lb-alg
```

Esto implica que si el usuario del StyleBook especifica el valor booleano «true» para el parámetro is-secure o selecciona la casilla correspondiente a este parámetro en la GUI de Citrix ADM, a la propiedad servicetype de este componente se le asigna el valor **SSL** y a la propiedad port el valor **443**. Sin embargo, si el usuario especifica «false» para este parámetro o desmarca la casilla correspondiente en la GUI de Citrix ADM, a la propiedad servicetype se le asigna el valor **HTTP** y al puerto se le asigna el valor **80**.

En el ejemplo siguiente se muestra cómo utilizar sustituciones como función. Una función de sustitución puede tomar uno o más argumentos. Los argumentos deben ser de tipo simple, por ejemplo, cadena, número, dirección IP, booleano y otros tipos.

**sustituciones**:

form-lb-name (nombre): $nombre + “-lb”

En este ejemplo, definimos una función de sustitución «form-lb-name» que toma un argumento de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

cadena denominado «name» **y lo usa para crear una nueva cadena con el sufijo «-lb» de la cadena del argumento name. Una expresión mediante esta función de sustitución se puede escribir como:

$substitutions.form-lb-name («mi»)

que devuelve «my-lb»

Considere otro ejemplo:

**sustituciones**:

cspol-priority(priority): 10100 - 100 * $priority

La sustitución cspol-priority es una función que toma un argumento llamado priority y lo usa para calcular un valor. En el resto del StyleBook, esta sustitución se puede utilizar como se muestra en el siguiente ejemplo:

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
         name: $parameters.csvserver-name
         policyname: $components.cspolicy-comp.properties.policyname
         priority: $substitutions.cspol-priority($parameters.pool.
   priority)
```

La sustitución también puede estar compuesta por una clave y un valor. El valor puede ser un valor simple, una expresión, una función, un mapa, una lista o un diccionario.

El siguiente es un ejemplo de una sustitución llamada «slist» cuyo valor es una lista:

```
substitutions:
  slist:
    - a
    - b
    - c
```

El valor de una sustitución también puede ser un diccionario de pares clave-valor, como se ve en el siguiente ejemplo de una sustitución llamada «sdict»:

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
```

Puede crear atributos más complejos combinando listas y diccionarios. Por ejemplo, una sustitución denominada «slistofdict» devuelve una lista de pares clave-valor.

```
  slistofdict:
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
2       -
3         a: $parameters.cs1.lb1.port
4         b: $parameters.cs1.lb2.port
5       -
6         a: $parameters.cs2.lb1.port
7         b: $parameters.cs2.lb2.port
```

Sin embargo, en el siguiente ejemplo, una sustitución «sdictoflist» devuelve un par clave-valor, donde el valor en sí mismo es otra lista.

```
1     sdictoflist:
2       a:
3         - 1
4         - 2
5       b:
6         - 3
7         - 4
```

En los componentes, estas sustituciones se pueden utilizar en construcciones de condición, propiedades, repetición, repetición de condición.

El siguiente ejemplo de un componente muestra cómo se puede utilizar una sustitución para especificar las propiedades:

```
1       properties:
2         a: $substitutions.slist
3         b: $substitutions.sdict
4         c: $substitutions.slistofdict
5         d: $substitutions.sdictoflist
```

Un caso de uso para definir una sustitución cuyo valor es una lista o un diccionario es cuando está configurando un servidor virtual de conmutación de contenido y varios servidores virtuales de equilibrio de carga. Dado que todos los servidores virtuales lb vinculados al mismo servidor virtual cs pueden tener una configuración idéntica, puede usar la lista de sustituciones y el diccionario para crear esta configuración y evitar repetirla para cada servidor virtual lb.

El siguiente ejemplo muestra la sustitución y el componente en los StyleBooks cs-lb-mon para crear una configuración de servidor virtual de conmutación de contenido. Al construir las propiedades de los StyleBooks cs-lb-mon, la compleja sustitución «lb-properties» especifica las propiedades de los servidores virtuales lb asociados al servidor virtual cs. La sustitución de “lb-properties”es una función que toma el nombre, el tipo de servicio, la dirección IP virtual, el puerto y los servidores como parámetros y genera un par clave-valor como valor. En el componente «cs-pools», asignamos el valor de esta sustitución al parámetro lb-pool para cada grupo.

```
1 substitutions:
2   cs-port[]:
3     true: int("80")
4     false: int("443")
5   lb-properties(name, servicetype, vip, port, servers):
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
6      lb-appname: $name
7      lb-service-type: $servicetype
8      lb-virtual-ip: $vip
9      lb-virtual-port: $port
10     svc-servers: $servers
11     svc-service-type: $servicetype
12     monitors:
13       -
14         monitorname: $name
15         type: PING
16         interval: $parameters.monitor-interval
17         interval_units: SEC
18         retries: 3
19 components:
20   -
21     name: cs-pools
22     type: stlb::cs-lb-mon
23     description: | Updates the cs-lb-mon configuration with the
       different pools provided. Each pool with rule result in a dummy LB
       vserver, cs action, cs policy, and csvserver_cspolicy_binding
       configuration.
24     condition: $parameters.server-pools
25     repeat: $parameters.server-pools
26     repeat-item: pool
27     repeat-condition: $pool.rule
28     repeat-index: ndx
29     properties:
30       appname: $parameters.appname + "-cs"
31       cs-virtual-ip: $parameters.vip
32       cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
       HTTP")
33       cs-service-type: $parameters.protocol
34       pools:
35         -
36           lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
       , "0.0.0.0", 0, $pool.servers)
37           rule: $pool.rule
38           priority: $ndx + 1
```

**Mapa de sustitución**:

Puede crear sustituciones que asignen las claves a los valores. Por ejemplo, considere un caso en el que quiera definir el puerto predeterminado (valor) que se utilizará para cada protocolo (clave). Para esta tarea, escriba un mapa de sustitución de la siguiente manera.

```
1 substitutions:
2      port:
3           HTTP: 80
4           DNS: 53
5           SSL: 443
```

En este ejemplo, HTTP se asigna a 80, DNS a 53 y SSL se asigna a 443. Para recuperar el puerto de un

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

protocolo determinado que se da como parámetro, utilice la expresión

$substitutions.port[$parameters.protocol]

La expresión devuelve un valor basado en el protocolo especificado por el usuario.

- Si la clave es HTTP, la expresión devuelve 80
- Si la clave es DNS, la expresión devuelve 53
- Si la clave es SSL, la expresión devuelve 443
- Si la clave no está presente en el mapa, la expresión no devuelve ningún valor

## Componentes

January 30, 2024

La construcción Componentes de un StyleBook se considera la sección más importante del StyleBook. En esta sección, definirá los objetos de configuración que deben crearse. Con esta construcción, puede crear uno o varios objetos de configuración del mismo tipo.

La construcción de componentes puede utilizar la entrada proporcionada en la sección de parámetros para adaptar la configuración generada por el StyleBook. Se trata de una sección opcional, aunque la mayoría de los StyleBooks tienen una sección de componentes.

En la tabla siguiente se describen los principales atributos de un componente.

|Atributo| Descripción|
|—|—|
| name| El nombre del componente. Puede especificar un nombre alfanumérico. El nombre debe empezar por un alfabeto y puede incluir alfabetos, números, guiones (-) o caracteres de subrayado (_) adicionales.|
|description | Descripción de la función de este componente en el StyleBook.|
| type| El tipo determina las propiedades que proporciona este componente. Los componentes tienen dos tipos: **tipo integrado: este tipo**lo proporciona el sistema y no es necesario definirlo, por ejemplo, los tipos de entidades NITRO ”lbvserver” o ”servicegroup”. Cuando un componente tiene un atributo de tipo integrado, crea un objeto de configuración de ese tipo en NetScaler ADC. Por ejemplo, si un componente hace referencia al tipo integrado «lbvserver», este componente crea un servidor virtual de equilibrio de carga en la instancia de Citrix ADC que es el destino de la configuración. **Tipo compuesto**: este tipo hace referencia a un StyleBook existente que creó e importó a NetScaler ADM. Cuando un componente tiene un atributo de tipo compuesto, crea todos los objetos de configuración, que se especifican en el StyleBook al que se hace referencia, en la instancia NetScaler ADC que es el destino de la configuración. Esto le permite combinar varios StyleBooks donde cada StyleBook crea una parte de la configuración final. Para obtener más información sobre

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

StyleBooks compuestos, consulte [Crear un StyleBook compuesto](/es-es/netscaler-application-delivery-management-software/13/stylebooks/how-to-create-custom-stylebooks).|
| properties|Los subatributos que se pueden usar para un atributo de tipo de componente. Las propiedades que son válidas para un componente están dictadas por su tipo. Para un tipo integrado, estas son las propiedades o atributos del objeto Nitro correspondiente. Para un componente cuyo tipo es otro StyleBook, es decir, un tipo compuesto, las propiedades corresponden a los parámetros definidos en ese StyleBook.|
|

**Ejemplo**:

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
```

En este ejemplo, ha definido un componente denominado my-lbvserver-comp. Este componente es de tipo ns::lbvserver (un tipo integrado), donde “ns”es el prefijo que hace referencia al espacio de nombres netscaler.nitro.config y la versión 10.5 que había especificado en la sección import-stylebooks, y “lbvserver”es un recurso NITRO en este espacio de nombres.

Las propiedades de esta sección incluyen cuatro atributos obligatorios y uno opcional (lbmethod) del recurso “lbvserver”y permiten especificar valores para estos atributos. En este ejemplo, está especificando valores estáticos para servicetype y port, mientras que las propiedades name, ipv46 y lbmethod obtienen sus valores de los parámetros de entrada. Se hace referencia a los nombres de los parámetros definidos en la sección de parámetros mediante la notación $parameters.<name>, por ejemplo, $parameters.ip.

> **Nota**
>
> Debe utilizar minúsculas para los nombres de los atributos de los tipos de recursos NITRO (sus propiedades de componentes). De lo contrario, la importación de un StyleBook fallará.

## Componentes auxiliares

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El uso principal de la sección de componentes de un StyleBook es generar objetos de configuración a través de los tipos integrados de Nitro u otro StyleBook que cree los objetos de configuración reales. Los componentes auxiliares no crean objetos de configuración por sí mismos. Los componentes auxiliares toman las entradas de otras secciones, como los objetos de parámetros, las propiedades de otros componentes o las salidas de otros componentes, y las transforman en otras formas. Otros componentes pueden usarlo posteriormente para generar los objetos de configuración reales. Un componente auxiliar puede ser de dos tipos: Tipo de objeto u otro StyleBook que no contenga una sección de componente.

El siguiente ejemplo muestra un fragmento de un StyleBook que se utiliza para crear un servidor de equilibrio de carga con monitor (lb-mon-comp) en una instancia de Citrix ADC.

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
      lb-appname: $parameters.appname
      lb-virtual-ip: $parameters.vip
      lb-virtual-port: 80
      lb-service-type: HTTP
      svc-service-type: HTTP
      svc-servers: $components.help-comp.properties
```

La sección de parámetros le permite introducir el nombre de la aplicación y las direcciones IP de los servidores de equilibrio de carga. En la sección de componentes lb-mon-comp, el parámetro svc-servers de lb-mon StyleBook espera una lista de objetos en la que cada elemento tiene dos subparámetros: ip y port.

Sin embargo, la sección de parámetros de este StyleBook solo acepta las direcciones IP del servidor

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a través de $parameters.ips. El StyleBook asume que todos los servidores se ejecutan en el puerto 80. Para crear la configuración de equilibrio de carga con lb-mon StyleBook, debe transformar $parameters.ips en una lista de objetos. Esto se logra utilizando el componente auxiliar, help-comp, en el ejemplo anterior. El componente help-comp es del tipo server-ip-port-params StyleBook. Este StyleBook no tiene ningún componente. Como resultado, no crea ningún objeto de configuración. El help-comp crea una lista de repetición sobre $parameters.ips y construye un objeto que consiste en ip y port (que se establece en un 80 estático) para cada elemento de $parameters.ips. Por lo tanto, help-comp transforma una lista de direcciones IP en una lista de objetos que se pueden usar posteriormente en lb-mon-comp para asignar la propiedad svc-servers. El resultado de help-comp se asigna a la propiedad svc-servers de lb-mon-comp.

## Propiedades opcionales

January 30, 2024

En algunos casos, una propiedad de un componente toma su valor de una expresión, que puede ser una expresión simple, como una referencia a un parámetro, o una expresión más compleja. Establecer este valor de propiedad es opcional en el componente. Puede elegir establecer el valor de la propiedad solo si la expresión devuelve un valor real; de lo contrario, puede optar por no establecer esta propiedad.

Por ejemplo, considere que una de las propiedades que quiere establecer es el lbmethod (algoritmo de equilibrio de carga) de un componente cuyo tipo es ns::lbvserver. El valor de la propiedad lbmethod se toma de un valor de parámetro proporcionado por el usuario, como se muestra a continuación:

```
components
  -
      name: lbvserver_comp
      type: ns::lbvserver
      properties:
        name: $parameters.lb-appname + "-lb"
        servicetype: $parameters.lb-service-type
        ipv46: $parameters.lb-virtual-ip
        port: 80
        lbmethod: $parameters.lb-advanced.algorithm
```

Ahora, considere que el parámetro **lb-advanced.algorithm** es un parámetro opcional. Y, si el usuario no proporciona un valor para este parámetro porque es opcional, la expresión **$parameters.lb-advanced.algorithm** se evalúa como valor en blanco. Por lo tanto, se pasa un valor no válido para la propiedad lbmethod. Para evitar tal situación, puede anotar la propiedad como opcional sufijo su nombre con “?”según se indica a continuación:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
```

¿El uso de “?”omite la propiedad si la expresión del derecho no se evalúa como nada, lo que sería equivalente, en este caso, a un componente definido de la siguiente manera:

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
```

Como **lbmethod** es opcional, su omisión hace que sea un componente válido. Tenga en cuenta que lbmethod podría tomar su valor predeterminado si uno está definido en su tipo “ns::lbvserver”.

## Properties-default-sources construct

January 30, 2024

La construcción properties-default-sources es análoga a la construcción parameters-default-sources. Mientras que la construcción parameters-default-sources permite reutilizar los parámetros existentes (de otros StyleBooks) en un StyleBook, la construcción properties-default-sources permite al usuario especificar las propiedades de un componente en función de las fuentes existentes.

Las propiedades de un componente pueden distribuirse en varias secciones del StyleBook. Por ejemplo, las propiedades pueden provenir de parámetros de objetos, sustituciones que devuelven un objeto, propiedades de otros componentes o salidas de otros componentes. En tales casos, debe redefinir las propiedades que aparecen en otras secciones del StyleBook en la definición del componente. Evidentemente, esto es redundante y puede provocar errores. Para solucionar este problema, se puede utilizar la construcción properties-default-sources. El componente fijo properties-default-sources es una lista en la que cada elemento identifica un origen para algunas propiedades del componente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Por ejemplo, considere un componente que crea una configuración de lbvserver. Este componente debe definir las propiedades del lbvserver de la siguiente manera.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
```

En el ejemplo anterior, observe que los valores de todas las propiedades definidas en la sección de componentes se toman de $parameters.lb objeto. Aunque se toman de una sola fuente, las propiedades se definen de nuevo en el StyleBook. Además, si se agrega un nuevo subparámetro al objeto $parameters.lb que sea relevante para la configuración del servidor lbvserver, debe actualizar el componente lb-comp para agregar la nueva propiedad que corresponde al nuevo subparámetro.

Para evitar redefinir las propiedades y obtener todas las propiedades relevantes de un componente sin enumerarlas explícitamente en la sección de propiedades, se puede utilizar la construcción properties-default-sources. El ejemplo anterior se puede escribir de la siguiente manera.

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
```

En el ejemplo anterior, el uso de la construcción properties-default-sources reduce el tamaño de la definición del componente, lo que permite definir un componente de forma concisa. Además, cada vez que cambia el origen de las propiedades del componente, los cambios se reflejan automáticamente. Por ejemplo, cuando se agrega una nueva propiedad, por ejemplo «persistencetype», al objeto $parameters.lb, esta propiedad se agrega a la configuración de lb-comp de forma predeterminada, ya que persistencetype es una propiedad de lbvserver. Por lo tanto, la construcción properties-default-sources proporciona una interfaz dinámica para definir los componentes sin preocuparse por los cambios que ocurren en las fuentes de las propiedades del componente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Cálculo de las propiedades del componente

En esta sección se explica cómo se obtienen las propiedades si se utiliza la construcción properties-default-sources en un componente. En primer lugar, el compilador de StyleBooks identifica la lista de propiedades de un componente en función de su tipo (en el ejemplo anterior, lbvserver). A continuación, el compilador obtiene estas propiedades de las múltiples fuentes en el orden en que están definidas (en la sección properties-default-sources del componente). Si una propiedad existe en varios orígenes, la propiedad que aparece en el último origen tiene prioridad sobre otras. Por último, una propiedad obtenida mediante la construcción properties-default-sources se puede reemplazar en la sección de propiedades del componente. Es importante tener en cuenta que la definición de una sección de componentes debe tener al menos una sección de properties-default-sources o una sección de propiedades. Puede que tenga ambas cosas.

## Componentes anidados

January 30, 2024

Al anidar un componente dentro de otro componente, el componente anidado puede crear sus objetos de configuración haciendo referencia a los objetos de configuración o al contexto creado por el componente principal. El componente anidado puede crear uno o más objetos para cada objeto creado en el componente principal. Anidar un componente dentro de otro componente no indica ninguna relación entre los objetos de configuración creados. El anidamiento es una forma de facilitar la tarea de los componentes para construir objetos de configuración dentro de un contexto existente de los componentes principales.

**Ejemplo**:

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
18          components:
19             -
20               name: lbvserver-svg-binding-comp
21               type: ns::lbvserver_servicegroup_binding
22               properties:
23                 name: $parent.parent.properties.name
24                 servicegroupname: $parent.properties.name
25                   -
26                     name: members-svcg-comp
27                     type: ns::servicegroup_servicegroupmember_binding
28                     repeat:
29                       repeat-list: $parameters.svc-servers
30                       repeat-item: srv
31                     properties:
32                       ip: $srv
33                       port: str($parameters.svc-port)
34                       servicegroupname: $parent.properties.name
```

En este ejemplo, se utiliza el anidamiento de varios niveles. El componente my-lbvserver-comp tiene un componente secundario denominado my-svcg-comp. Además, el componente my-svcg-comp tiene dos componentes secundarios. El componente my-svcg-comp se utiliza para crear un objeto de configuración de grupos de servicios en la instancia de Citrix ADC proporcionando valores a los atributos del tipo de recurso NITRO integrado «servicegroup». « El primer componente secundario del componente my-svcg, lbvserver-svg-binding-comp, se usa para vincular el grupo de servicios creado por su componente principal al servidor virtual de equilibrio de carga (lbvserver) creado por el componente principal del componente principal. La notación $principal, también llamada referencia principal, se utiliza para hacer referencia a entidades en los componentes principal. El segundo componente secundario, members-svcg-comp, se usa para vincular la lista de servicios al grupo de servicios creado por el componente principal. El enlace se logra mediante el uso de la construcción de repetición de StyleBook para iterar sobre la lista de servicios especificados para el parámetro svc-servers. Para obtener información sobre las construcciones repetidas, consulte Repetir construcción.

También puede crear los mismos objetos de configuración sin utilizar el anidamiento de componentes. Para obtener más información y ejemplos, consulte StyleBook to Create a Basic Load Balancing Configuration.

## Construcción de condición

January 30, 2024

Puede hacer que un componente sea condicional mediante una construcción de condiciones. El valor de una construcción condicional es una expresión booleana que se evalúa como verdadera o falsa. Si la condición es verdadera, el componente se usa para crear sus objetos de configuración. Si la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

condición es falsa, se omite el componente y no se crea ningún objeto de configuración a través de él. La expresión booleana se basa a menudo en valores de parámetros.

**Ejemplo**:

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
```

En este ejemplo, si el usuario especifica un valor para el parámetro opcional svc-server-ips, el motor StyleBook procesa el componente servicegroup-comp. Si la condición es falsa, es decir, si el usuario no proporciona un valor a este parámetro, se asigna un valor nulo a este parámetro y se evalúa como falso, el motor StyleBook ignora la presencia de este componente y no se crea ningún grupo de servicios.

Tenga en cuenta que la expresión booleana puede basarse en cualquier expresión válida admitida en StyleBooks (por ejemplo, si hay otro componente o si un parámetro tiene un valor determinado).

En el ejemplo siguiente se crea el objeto de configuración de NITRO tipo ns::systemfile si la condición se evalúa como true.

**Ejemplo**:

```
      components
           -
             name: pem_key_files
             type: ns::systemfile
             condition: "$components.der-certificate-files-comp or
      $components.pem-certificate-files-comp"
             properties:
                    filecontent: $certificate.keyfile.contents
                    fileencoding: "BASE64"
                    filelocation: "/nsconfig/ssl"
                    filename: $certificate.keyfile.filename
```

En este ejemplo, la condición es una expresión «OR» compleja, en la que desea que el StyleBook cree este objeto de configuración solo si otros dos componentes del StyleBook se han procesado (no se han omitido) y, por lo tanto, se crea una dependencia entre los componentes.

## Repetir componente fijo

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede utilizar la construcción **repetida** de un componente para crear varios objetos de configuración del mismo tipo.

En el ejemplo siguiente, el componente **members-svcg-comp** se utiliza para enlazar la lista de servicios al grupo de servicios creado por el componente principal. Para crear un objeto de configuración que vincule cada servidor al grupo de servicios, utilice la construcción **repeat** para recorrer la lista de servicios especificada para el parámetro **svc-servers** . Durante la iteración, el componente crea un objeto NITRO de tipo **servicegroup_servicegroupmember_binding** para cada servicio (denominado **srv** en la construcción **repeat-item**) en el grupo de servicios, y establece el atributo **ip** en cada NITRO a la dirección IP del servicio correspondiente.

**Ejemplo**:

```
components:
  -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
          components:
                -
                   name: my-svcg-comp
                   type: ns::servicegroup
                   properties:
                        name: $parameters.name + "-svcgrp"
                        servicetype: HTTP
                  components:
                         -
                         name: lbvserver-svg-binding-comp
                         type: ns::lbvserver\servicegroup\binding
                         properties:
                               name: $parent.parent.properties.name
                               servicegroupname: $parent.properties.name
                         -
                         name: members-svcg-comp
                         type: ns::servicegroup\servicegroupmember\binding
                         repeat:
                           repeat-list: $parameters.svc-servers
                           repeat-item: srv
                         properties:
                                ip: $srv
                                port: $parameters.svc-port
                                servicegroupname: $parent.properties.name
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La **repetición** es un objeto en sí misma, y **repeat-list** y **repeat-item** son atributos del objeto repetido.

- repeat-list es un atributo obligatorio que identifica la lista en la que itera el componente.
- repeat-item es opcional, y se utiliza para dar un nombre descriptivo al elemento actual en la iteración.

Si no se especifica, se puede acceder al elemento actual mediante la expresión**$repeat-item**. El último componente en el ejemplo anterior también se puede escribir de la siguiente manera:

```
1           -
2           name: members-svcg-comp
3           type: ns::servicegroup_servicegroupmember_binding
4           repeat:
5             repeat-list: $parameters.svc-servers
6           properties:
7                  ip: $repeat-item
8                  port: $parameters.svc-port
9                  servicegroupname: $parent.properties.name
```

Además de poder hacer referencia al elemento actual en blanco iterando sobre una lista, también es posible hacer referencia al índice actual del elemento de la lista mediante el índice **repetido**. En el ejemplo siguiente, **repeat-index** se utiliza para calcular un número de puerto basado en el índice actual:

```
1              name: services
2              type: ns::service
3              repeat:
4                 repeat-list: $parameters.app-services
5                 repeat-item: srv
6              properties:
7                  ip: $parameters.app-ip
8                  port: $parameters.base-port + repeat-index
9                  servicegroupname: $parent.properties.name
```

Al igual que en la construcción **repeat-item** , puedes asignar un nombre de variable diferente para hacer referencia al índice actual de la iteración. El ejemplo anterior es equivalente al siguiente ejemplo:

```
1       -
2              name: services
3              type: ns::service
4              repeat:
5                 repeat-list: $parameters.app-services
6                 repeat-item: srv
7                 repeat-index: idx
8              properties:
9                  ip: $parameters.app-ip
10                 port: $parameters.base-port + $idx
11                 servicegroupname: $parent.properties.name
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Construcción de condición de repetición

January 30, 2024

La construcción de condición de repetición se evalúa en cada iteración de una construcción de repetición y el resultado determina si se debe generar el objeto de configuración en esa iteración o pasar a la siguiente iteración. El siguiente ejemplo muestra el uso de la construcción de condición de repetición:

**Ejemplo**:

```
components
   -
      name: der-key-files-comp
      type: ns::systemfile
      repeat:
      repeat-list: $parameters.certificates
      repeat-item: certificate
        repeat-condition: $certificate.ssl-inform == DER
        properties:
         filecontent: base64($certificate.keyfile.contents)
         fileencoding: BASE64
         filelocation: /nsconfig/ssl
         filename: $certificate.keyfile.file
```

En este ejemplo, el componente der-key-files-comp itera sobre todos los certificados proporcionados por el usuario, pero solo crea objetos de configuración que corresponden a los certificados con codificación DER. En cada iteración, la expresión de condición de repetición se evalúa para probar si la codificación del certificado es del tipo DER. Si no es de tipo DER, no se genera ningún objeto de configuración en la iteración actual y la iteración se mueve al siguiente certificado de la lista.

## Repeticiones anidadas

January 30, 2024

Con la construcción de repetición anidada, puede tener más de una construcción de repetición en cada componente, según la definición del componente. Considere una repetición anidada de dos niveles. Para cada elemento de la lista externa (primera lista repetida), puede crear una lista repetida para todos los elementos de la lista interna (segunda lista repetida). El compilador StyleBook admite hasta tres repeticiones anidadas. Cada nivel de repetición tiene asociados los atributos repeat-item y repeat-index. Tanto los atributos repeat-item como repeat-index son opcionales. Además, cada repetición también puede especificar una condición de repetición.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo**:

```
parameters:
  -
      name: vips
      type: ipaddress[]
  -
      name: vip-ports
      type: tcp-port[]
components:
  -
      name: lbvservers-comp
      type: ns::lbvserver
      repeat:
         repeat-list: $parameters.vips
         repeat-item: ip
         repeat:
              repeat-list: $parameters.vip-ports
              repeat-item: port
      properties:
         name: str("lb-") + str($ip) + '-' + str($port)
         servicetype: HTTP
         ipv46: $ip
         port: $port
```

En el ejemplo anterior, para cada elemento de $parameters.vips, iteramos sobre todos los elementos de $parameters.vip-ports. Por lo tanto, para cada dirección IP especificada en $parameters.vips, creamos objetos de configuración lbvserver para todos los puertos especificados en $parameters.vip-ports. La sección de propiedades define el nombre del objeto con «lb» como prefijo para la combinación de la dirección IP y el puerto. Por lo tanto, para cada iteración, $ip + $port define una combinación única de la dirección IP y el número de puerto.

Si no se proporciona el atributo repeat-item, el compilador genera un valor predeterminado para él. Los valores predeterminados para repeat-item son: $repeat-item, $repeat-item-1, $repeat-item-2 respectivamente para cada nivel de repetición. Del mismo modo, si no se proporciona el atributo repeat-index, el compilador genera un valor predeterminado para él. Los valores predeterminados para repeat-index son: $repeat-index, $repeat-index-1 y $repeat-index-2 respectivamente para cada nivel de repetición.

El siguiente ejemplo describe la convención de nomenclatura en ausencia de los atributos repeat-item y repeat-index en un objeto repetido anidado.

**Ejemplo**:

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
         repeat-list: $parameters.vips
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
7          repeat:
8             repeat-list: $parameters.vip-ports
9      properties:
10        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
    -1)
11        servicetype: HTTP
12        ipv46: $repeat-item
13        port: $repeat-item-1
```

## Resultados

January 30, 2024

En la sección de resultados, especifique lo que un StyleBook expone a sus usuarios una vez que haya terminado de crear correctamente todos los objetos de configuración. La sección de salidas de un StyleBook es opcional. No es necesario que un StyleBook devuelva las salidas. Sin embargo, al devolver algunos componentes internos como salidas, permite que los StyleBooks que los importen tengan más flexibilidad, como puede ver al crear un StyleBook compuesto.

En la siguiente tabla se describen los atributos que se utilizan en la sección de salidas.

| Atributo | Descripción | Obligatorio |
|---|---|---|
| name | El nombre de la salida correspondiente al objeto de configuración que desea exponer. | Sí |
| description | Cadena de texto que describe la salida. | No |
| value | Este atributo especifica cómo extraer el valor devuelto por un StyleBook. | Sí |

**Ejemplo**:

```
1  outputs:
2   -
3     name: lbvserver
4     description: LBVServer component
5     value: $components.my-lbvserver-comp
6   -
7     name: svc-grp
8       description: ServiceGroup name
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
9       value: $components.my-svcg.properties.name
```

En este ejemplo, expondrá el componente **lbvserver** y el **nombre** del grupo de servicios que crearía StyleBook. El valor de la salida llamada **lbvserver** es el componente **my-lbvserver-comp**. Del mismo modo, el valor de la salida denominada **svc-grp** es el nombre del grupo de servicios creado por el componente **my-svcg**.

## Referencia de parámetros

January 30, 2024

En la construcción de componentes, se hace referencia a los parámetros definidos en la sección de parámetros mediante la `$parameters.<parametername>` notación. Si `<parametername>` en sí mismo contiene parámetros (cuando el tipo es objeto), entonces debe usar la notación `$parameters.<parametername>.<sub-parametername>`, etc.

**Ejemplo**:

```
1  parameters:
2    -
3      name: name
4      label: Name
5      type: string
6      required: true
7       -
8        name: vip
9        label: Virtual IP and Port
10       type: object
11       required: true
12       parameters:
13         -
14           name: ip
15           label: Virtual IP
16           description: The Virtual IP Address
17           type: ipaddress
18           required: true
19             -
20               name: port
21               label: The Virtual Port
22               description: The TCP port for the Virtual IP
23               type: tcp-port
24               default: 80
25 components:
26   -
27     name: my-lbvserver-comp
28     type: ns::lbvserver
29     properties:
30        name: $parameters.name
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
31          servicetype: HTTP
32          ipv46: $parameters.vip.ip
33          port: $parameters.vip.port
```

## Referencia de principal

January 30, 2024

Si utiliza componentes anidados, puede hacer referencia al componente principal mediante la notación $parent. Si el componente principal crea varios objetos de configuración utilizando el componente fijo de repetición, y dentro de cada iteración, los componentes secundarios crean otros objetos de configuración, la notación $parent siempre hace referencia a la iteración actual del componente principal. Por ejemplo, $parent.properties.name hace referencia a la propiedad name del objeto de configuración creado en la iteración actual por el padre.

**Ejemplo**:

```
1  components:
2   -
3     name: my-lbvserver-comp
4     type: ns::lbvserver
5     properties:
6       name: $parameters.name + "-lb"
7       servicetype: HTTP
8       ipv46: $parameters.ip
9       port: 80
10      lbmethod: $parameters.lb-alg
11      components:
12        -
13          name: my-svcg-comp
14          type: ns::servicegroup
15          properties:
16            name: $parameters.name + "-svcgrp"
17            servicetype: HTTP
18            components:
19             -
20               name: lbvserver-svg-binding-comp
21               type: ns::lbvserver_servicegroup_binding
22               properties:
23                  name: $parent.parent.properties.name
24                  servicegroupname: $parent.properties.name
25                    -
26                      name: members-svcg-comp
27                      type: ns::servicegroup_servicegroupmember_binding
28                      repeat: $parameters.svc-servers
29                      repeat-item: srv
30                      properties:
31                        ip: $srv
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
32                          port: str($parameters.svc-port)
33                          servicegroupname: $parent.properties.name
```

También puede desplazarse hacia activo a través de la jerarquía de componentes accediendo a las propiedades de los principales de los principales hasta los componentes de nivel superior. Por ejemplo, el nombre de propiedad del componente **lbvserver-svg-binding-comp** toma su valor del nombre de la propiedad principal de su componente principal, el componente **my-lbvserver-comp** , mediante la notación **$parent.parent**.

## Referencia de componentes

January 30, 2024

En la construcción de componentes, se hace referencia al componente de nivel superior en el StyleBook mediante el uso de la notación **$components.<componentname>**. Si hay componentes anidados dentro de un componente de nivel superior, la notación utilizada es **$components.<componentname>.components.<component-name>** para hacer referencia a ellos, y así sucesivamente.

**Ejemplo**:

```
1  components:
2   -
3      name: my-lbvserver-comp
4       type: ns::lbvserver
5       properties:
6             name: $parameters.name + "-lb"
7             servicetype: HTTP
8             ipv46: $parameters.ip
9             port: 80
10            lbmethod: $parameters.lb-alg
11   -
12      name: my-svcg-comp
13      type: ns::servicegroup
14      properties:
15           name: $parameters.name + "-svcgrp"
16           servicetype: HTTP
17  -
18      name: members-svcg-comp
19      type: ns::servicegroup_servicegroupmember_binding
20      repeat: $parameters.svc-servers
21      repeat-item: srv
22      properties:
23         ip: $srv
24           port: str($parameters.svc-port)
25           servicegroupname: $components.my-svcg-comp.properties.name
26  -
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
27      name: lbvserver-svg-binding-comp
28      type: ns::lbvserver_servicegroup_binding
29      properties:
30             name: $components.my-lbvserver-comp.properties.name
31             servicegroupname: $components.my-svcg-comp.properties.name
```

En este ejemplo, los componentes **my-svcg-comp** y **my-lbvserver-comp** tienen que construirse antes de construir el último componente **lbvserver-svg-binding-comp** porque hay referencias a estos componentes en este último componente. Estas referencias se proporcionan mediante el uso de referencias de componentes denotadas por **$components.<componentname>**.

## Referencia de sustituciones

January 30, 2024

En la sección de componentes o en la sección de operaciones, se hace referencia a las sustituciones definidas en la sección de sustituciones mediante la notación `$substitutions.<substitution-name>`. Por ejemplo, **$substitutions.http-port**.

Si una sustitución es un mapa, puede hacer referencia a un elemento en el mapa como `$substitutions.<substitutions-name>[<map-key>]`. Por ejemplo: `$substitutions.protocol-map[$parameters.port]`.

## Referencia de variable

January 30, 2024

Al utilizar las construcciones repeat y repeat-item en los componentes para crear varios objetos de configuración, puede asignar un nombre de variable a la construcción repeat-item. A continuación, se puede hacer referencia a esta variable en las propiedades de ese componente o en los componentes secundarios mediante la notación `$\<varname\>`. Tenga en cuenta que cuando la construcción repeat se usa sin la construcción repeat-item en un componente, se puede usar una variable predeterminada llamada $repeat-item para acceder a los elementos de iteración.

**Ejemplo**:

```
1 components:
2   -
3     name: server-members-comp
4     type: ns::server
5     condition: $parameters.svc-server-domain-names
6     repeat: $parameters.svc-server-domain-names
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
7       repeat-item: server-name
8       properties:
9         name: $server-name + "-server"
10        domain: $server-name
11      components:
12        -
13           name: service-members-comp
14           type: ns::service
15           properties:
16             name: $server-name + "-service"
17             servername: $parent.properties.name
18             servicetype: $parameters.svc-service-type
19             port: $parameters.svc-server-port
```

En el ejemplo anterior, se asigna un nombre de variable, server-name, a la construcción repeat-item. Este nombre de variable se hace referencia en las propiedades del mismo componente, así como en los componentes secundarios**$\<varname\>**.

## Operaciones

January 30, 2024

Las operaciones son una sección opcional de un StyleBook. En esta sección, puede configurar los análisis de Citrix Application Delivery Management (ADM) para recopilar registros de AppFlow en todas o algunas de las transacciones de tráfico. El servidor virtual creado en una instancia de NetScaler ADC mediante el StyleBook maneja estas transacciones de tráfico. En esta sección, también puede configurar NetScaler ADM para que active alarmas cuando se cumplan determinadas condiciones de tráfico en un servidor virtual.

Puede configurar NetScaler ADM a través de StyleBooks para recopilar estadísticas de tráfico de varios NetScaler ADM Insights que se enumeran a continuación:

- Información web
- Security Insight
- HDX Insight
- Citrix Gateway Insight.

Los servidores virtuales admitidos son el equilibrio de carga, la conmutación de contenido y los servidores virtuales VPN.

Habilite Web Insight y Security Insight o uno de ellos para análisis en un servidor virtual de equilibrio de carga o cambio de contenido. Sin embargo, para los servidores virtuales VPN, debe habilitar HDX Insight y NetScaler Gateway Insight o uno de ellos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cualquier NetScaler ADM Insight habilitado en instancias de NetScaler ADC mediante StyleBooks utiliza el protocolo IPFIX (AppFlow) para enviar los datos de las instancias a NetScaler ADC.

Además, al habilitar Web Insight, las medidas del lado del cliente se habilita en el equilibrio de carga y los servidores virtuales de conmutación de contenido. Con las mediciones del lado del cliente habilitadas, ADM captura el tiempo de carga y las métricas de tiempo de representación para páginas HTML, mediante inyección HTML. Mediante estas métricas, los administradores pueden identificar problemas de latencia L7.

**Ejemplo 1**:

El siguiente ejemplo muestra cómo escribir la sección de operaciones en un StyleBook para habilitar tanto HDX Insight como Citrix Gateway Insight en un servidor virtual VPN:

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
    a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                 type: hdxinsight**
                  -
                    type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
```

**Ejemplo 2**:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El siguiente ejemplo muestra cómo escribir la sección de operaciones en un StyleBook para habilitar Web Insight y Security Insight en un servidor virtual de equilibrio de carga:

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
    -
        name: lbvserver-comp
        type: ns::lbvserver
        properties:
            name: str("lb-") + str($current-target.ip)
            servicetype: HTTP
            ipv46: 1.1.21.37
            port: 80
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.lbvserver-comp
                filter: "true"
                 insights:
                 -
                  type: webinsight
                   -
                  type: securityinsight
outputs:
  -
    name: mylbs
    value: $components.lbvserver-comp
```

## Análisis

January 30, 2024

La subsección de análisis de la sección de operaciones tiene una estructura similar a la sección de componentes. Cada elemento de la sección de análisis se utiliza para configurar la función NetScaler ADM Analytics para uno o más servidores virtuales creados por el StyleBook.

Un elemento de la sección de análisis tiene los siguientes atributos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Atributo | Descripción | Obligatorio |
| --- | --- | --- |
| name | Nombre del elemento de análisis. | Sí |
| description | Una cadena de texto que describe qué es este elemento. | No |
| condition | Expresión booleana. Cuando esta condición se evalúa como falsa, se omite todo el elemento de análisis. | No |
| repeat | Itera sobre una lista. | No |
| repeat-condition | Expresión booleana. Si la expresión se evalúa como falsa, se omite la iteración actual. | No |
| repetir artículo | Nombre del elemento de la iteración actual. | No |
| repeat-index | Nombre del valor de índice de la iteración actual. | No |
| properties | La lista de propiedades de la analítica. | Sí |
| target | Una de las propiedades de la lista. La expresión de destino es el nombre de un servidor virtual, configurado en el NetScaler ADC, para el que se recopilarán los análisis. | Sí |
| filter | Una de las propiedades de la lista. El valor de este atributo es una expresión de directiva avanzada de NetScaler ADC que se utiliza para filtrar las solicitudes en el servidor virtual para las que se recopilarán los análisis. De forma predeterminada, los datos de análisis se recopilan de todo el tráfico que pasa por el servidor virtual. | No |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo**:

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
```

Cada atributo de la sección de análisis se utiliza para indicar a la función de NetScaler ADM Analytics que configure las instancias de NetScaler ADC para recopilar registros de flujo de aplicaciones en el servidor virtual identificado por la propiedad de destino.

## Alarmas

January 30, 2024

La subsección de alarmas de la sección de operaciones tiene una estructura similar y los mismos atributos que en la subsección de análisis. La única diferencia está en el atributo properties. Para obtener una lista de todos los atributos (excepto el atributo properties), consulte Analytics.

Las siguientes propiedades están disponibles en una subsección de alarmas:

| Atributo | Descripción | Obligatorio |
| --- | --- | --- |
| target | Expresión que se evalúa como el nombre de un servidor virtual, configurado en NetScaler ADC, para el que se configuran las alarmas. | Sí |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Atributo | Descripción | Obligatorio |
| --- | --- | --- |
| email-profile | Nombre de un perfil de correo electrónico que se define en la función NetScaler ADM Analytics y que contiene una lista de direcciones de correo electrónico a las que quiere notificar cuando se active la alarma. | No (se debe definir un perfil de correo electrónico o un perfil de SMS) |
| sms-profile | Nombre de un perfil SMS definido en la función de NetScaler ADM Analytics y contiene una lista de números de teléfono que quiere notificar cuando se activa la alarma. | No (se debe definir un perfil de correo electrónico o un perfil de SMS) |
| rules | Lista de reglas que definen las condiciones que desencadenarían una alarma para el servidor virtual definido por la propiedad de destino. | Sí |
| metric | Un atributo de regla. El nombre de una métrica que quiere rastrear relacionada con el servidor virtual NetScaler ADC. | Sí |
| operator | Un atributo de regla. El operador que se va a utilizar para comparar la métrica con el valor. Los operadores válidos son “mayor que”y “menor que” . | Sí |
| value | Un atributo de regla. El valor de umbral con el que se compara la métrica mediante el operador. Si el valor de la métrica supera este umbral, se activan las alarmas asociadas. | Sí |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Atributo | Descripción | Obligatorio |
|---|---|---|
| period-unit | Atributo de una regla. Frecuencia a la que se debe alertar a los usuarios si se cumple la regla de alarma. Puede contener el valor día, hora o semana. Esto significa que si se cumple la regla, se enviará una alarma una vez por unidad de período (por ejemplo, una vez al día). | Sí |

La siguiente tabla proporciona una lista de las métricas de las que se hace un seguimiento en relación con el servidor virtual NetScaler ADC.

Contadores|Descripción|Descripción detallada|Cálculo de NetScaler ADM
|—|—|—|—|
|Para un servidor virtual VPN:|
total_requests|Recuento total de lanzamientos de sesiones VPN|Número total de sesiones activas en este servidor virtual VPN que se iniciaron durante un intervalo de tiempo especificado por el usuario.|Contador que aumenta monótonamente, se incrementa con cada inicio de sesión nueva|
|app_count|Recuento de lanzamientos de aplicaciones VPN|Número total de aplicaciones VPN únicas en este servidor virtual VPN lanzadas durante un intervalo de tiempo especificado por el usuario.|El contador aumenta monótonamente cada vez que se lanza una nueva aplicación|
|app_launch_duration|Duración del lanzamiento de la aplicación VPN|Tiempo promedio necesario para lanzar una aplicación (en milisegundos)|Valor promedio calculado a través de las duraciones de tiempo de lanzamiento de todas las aplicaciones VPN iniciadas en este servidor virtual VPN|
|Otros servidores virtuales (CS, LB, Auth, GSLB) | | |
total_requests|Número de solicitudes|Número de solicitudes de clientes en este servidor virtual desde el último reinicio del dispositivo o desde la creación del servidor virtual, lo que sea más reciente. |Contador que aumenta monótonamente, se incrementa en cada nueva solicitud a este servidor virtual. |
|total_bytes|bytes|Total de bytes transferidos desde el servidor virtual a Citrix ADM durante el intervalo de tiempo especificado. |El contador aumenta monótonamente para tener en cuenta la cantidad total de bytes servidos por este servidor virtual. |
|APPLICATION_RESPONSE_TIME|Tiempo de respuesta|Tiempo de respuesta promedio del servidor virtual. |El valor promedio de los tiempos de respuesta de todas las solicitudes recibidas por este servidor virtual desde el último reinicio del dispositivo (o desde la creación del servidor virtual), lo que sea último. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Ejemplo de una sección de alarmas en un StyleBook:

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day
```

## Expresiones

January 30, 2024

Una de las funciones más potentes de un StyleBook es el uso de expresiones. Puede utilizar expresiones StyleBooks en varios casos para calcular valores dinámicos. El ejemplo siguiente es una expresión para concatenar un valor de parámetro con una cadena literal.

**Ejemplo**:

```
$parameters.appname + "-mon"
```

Esta expresión recupera el parámetro denominado `appname`y lo concatena con la cadena `-mon`.

Se admiten los siguientes tipos de expresiones:

### Expresiones aritméticas

- Adición (+)
- Resta (-)
- Multiplicación (*)
- División (/)
- Módulo (%)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplos**:

- Sumar dos números: $parameters.a + $parameters.b
- Multiplicar dos números: $parameters.a * 10
- Encontrar el resto después de la división de un número por otro:

`15%10` Resultados en 5

### Expresiones de cadena

- Concatenar dos cadenas (+)

**Ejemplo**:

Encadenar dos cadenas: str(“app-“) + $parameters.appname

### Expresiones de lista

Fusiona dos listas (+)

**Ejemplo**:

- Encadenar dos listas: $parameters.external-servers + $parameters.internal-servers
- Si `$parameters.ports-1` es [80, 81] y `$parameters.port-2` es [81, 82], `$parameters.ports-1 + $parameters.ports-2` se muestra como una lista [80, 81, 81, 82].

### Expresiones relacionales

- **==**: Comprueba si dos operandos son iguales y devuelve verdadero si son iguales, de lo contrario devuelve false.
- **!=**: Comprueba si dos operandos son diferentes y devuelve verdadero si son diferentes, de lo contrario devuelve false.
- **>**: Devuelve true si el primer operando es mayor que el segundo operando, de lo contrario devuelve false.
- **>=**: Devuelve true si el primer operando es mayor o igual que el segundo operando, de lo contrario devuelve false.
- **<**: Devuelve true si el primer operando es menor que el segundo operando, de lo contrario devuelve false.
- **<=**: Devuelve true si el primer operando es menor o igual que el segundo operando, de lo contrario devuelve false.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo**:

- Uso del operador de igualdad: `$parameters.name = = "abcd"`
- Uso del operador Desigualdad: `$parameters.name != "default"`
- Ejemplos para otros operadores relacionales
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

### Expresiones lógicas: Booleanas

- **y**: El operador lógico 'y'. Si ambos operandos son verdaderos, el resultado es verdadero; de lo contrario, es falso.
- **o**: El operador lógico 'o'. Si uno de los operandos es verdadero, el resultado es verdadero; de lo contrario, es falso.
- **no**: El operador unario. Si el operando es verdadero, el resultado es falso, y de la manera opuesta.
- **in**: Comprueba si el primer argumento es una subcadena del segundo argumento
- **en**: Comprueba si un elemento forma parte de una lista

> **Nota**
>
> Puede escribir expresiones en las que las cadenas se convierten en números y los números se convierten en cadenas. Del mismo modo, puede convertir `tcp-port` a un número, y una dirección IP se puede convertir en una cadena.
>
> Utilice un delimitador antes y después de cualquier operador. Puede utilizar los siguientes delimitadores:
>
> - Ante un operador: `spacetab`, `comma`, `(`, `)`, `[`, `]`
> - Después de un operador: `space`, `tab`, `(`, `[`
>
> Por ejemplo:
>
> - `abc + def`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- `100 % 10`
- `10 > 9`

### Expresiones de cadena literales

Puede utilizar cadenas literales cuando los caracteres especiales de una cadena tienen que tomar su forma literal. Estas cadenas pueden contener caracteres de escape, barra invertida, comillas, paréntesis, espacios en blanco, corchetes, etc. En las cadenas literales, se omite la interpretación habitual de los personajes especiales. Todos los caracteres de la cadena se conservan en su forma literal.

En StyleBooks, puede incluir expresiones de directivas de NetScaler ADC en su forma literal mediante cadenas literales. Las expresiones de directiva suelen contener caracteres especiales. Sin cadenas literales, tiene que escapar de los caracteres especiales dividiendo cadenas en subcadenas.

Para crear una cadena literal, encapsula una cadena entre caracteres especiales de la siguiente manera:

```
~{
 string }
 ~
```

Puede utilizar cadenas literales en cualquier parte del StyleBook.

> **Nota**
>
> No utilice la secuencia de caracteres `}  ~` en una cadena de entrada porque esta secuencia indica el final de una cadena literal.

Ejemplo :

```
 ~{
 HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR("=").
    AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
    ) }
 ~
```

### Expresiones de destino

En una definición de StyleBook, puede utilizar la `$current-target` expresión para hacer referencia a la instancia ADC de destino actual. Para referirse específicamente a la dirección IP de la instancia ADC de destino, utilice esta expresión de la siguiente manera:

```
$current-target.ip
```

Ejemplo :

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
```

En este ejemplo, el nombre de `lbvserver` se construye con la dirección IP de la instancia ADC de destino.

### Validación de tipo de expresión

El motor StyleBook permite una comprobación de tipos más eficaz durante el tiempo de compilación, es decir, las expresiones utilizadas al escribir el StyleBook se validan durante la importación de StyleBook en lugar de al crear el paquete de configuración.

Todas las referencias a parámetros, sustituciones, componentes, propiedades de componentes, salidas de componentes, variables definidas por el usuario (repeat-item, repeat-index, argumentos a funciones de sustitución) y así sucesivamente se validan para su existencia y tipos.

**Ejemplo de comprobaciones de tipo**:

En el ejemplo siguiente, el tipo esperado de propiedad port de `lbvserver` StyleBook es `tcp-port`. En NetScaler Application Delivery Management (ADM), las validaciones de tipo se realizan en tiempo de compilación (tiempo de importación). El compilador encuentra esa cadena y no `tcp-port` son tipos compatibles y, por lo tanto, el compilador StyleBook muestra un error y no puede importar o migrar un StyleBook.

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
```

Para compilar correctamente este StyleBook, declare lo siguiente como un número en el compilador:

`port: 80`

**Ejemplo de marcado de expresiones no válidas**:

En versiones anteriores, cuando se asignó una expresión no válida a un nombre de propiedad, el compilador no detectó expresiones no válidas y permitió que los StyleBooks se importaran en NetScaler

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ADM. Ahora, si este StyleBook se importa a NetScaler ADM, el compilador identifica dichas expresiones no válidas y lo marcarán. Como resultado, el StyleBook no puede importar a NetScaler ADM.

En este ejemplo, la expresión asignada a la propiedad name en el componente `lb-sg-binding-comp` es: `$components.lbvserver-comp.properties.lbvservername`. Sin embargo, no hay ninguna propiedad llamada `lbvservername` en el componente `lbvserver-comp`. En versiones anteriores de NetScaler ADM, el compilador habría permitido esta expresión y la habría importado correctamente. El error real se produciría cuando un usuario quisiera crear un paquete de configuración con este StyleBook. Sin embargo, ahora, este tipo de error se identifica durante la importación y el StyleBook no se importa a NetScaler ADM. Corrija manualmente dichos errores e importe los StyleBooks.

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
```

### Listas de indización

Ahora se puede acceder a los elementos de una lista indexándolos directamente:

| Expresión | Descripción |
|---|---|
| `$components.test-lbs[0]` | Hace referencia al primer elemento del componente test-lbs |
| `$components.test-lbs[0].properties.p1` | Hace referencia a la propiedad p1 del primer elemento en el componente test-lbs |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | |
|---|---|
| `$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname` | Hace referencia a `servicegroupname` la propiedad del segundo elemento del `servicegroups` componente, que es una salida del primer elemento del `lbcomps` componente |

## Interpolaciones in situ

February 2, 2024

Ahora es posible reemplazar partes de una cadena mediante expresiones de StyleBook. Cuando el compilador de StyleBook evalúe estas expresiones de cadena, la parte de la cadena que usa una expresión de StyleBook se reemplazará por el valor de la expresión. Para incluir expresiones StyleBook en una cadena, usamos la siguiente notación:

> “…%{…}%…”

donde los caracteres incluidos entre»% {“y «}%» forman una expresión de StyleBook. Estas expresiones se conocen como “interpolaciones in situ. “

Por ejemplo, la cadena “lb-%{$parameters.appname}%-svc”es una expresión de cadena con interpolación in situ de una expresión StyleBook. El valor de la expresión de cadena depende del valor de la expresión de interpolación. Considere que **$parameters.appname** está asignado con “app1”. A continuación, la expresión de cadena se evalúa como **lb-app1-svc**. Esto permite que los valores no se codifiquen en expresiones de cadena, sino que se evalúen en función de los valores definidos por el usuario.

Un caso práctico de interpolaciones in situ es parametrizar las expresiones de política en StyleBooks. Considere un caso en el que quiera escribir una expresión de directiva que compruebe si la dirección URL HTTP contiene una palabra específica, por ejemplo, “jpeg”.

Para ello, escriba una expresión de directiva de la siguiente manera: “HTTP.REQ.URL.CONTAINS(\ “jpeg\”)”.

Ahora, si desea parametrizar el objeto en la URL HTTP, puede agregar un parámetro de cadena en el StyleBook, por ejemplo, $parameters.url-object. La expresión de política debe escribirse en función de este parámetro. Para hacer eso, usa la concatenación de cadenas para lograr el resultado. La expresión se vería así:

> str(“HTTP.REQ.URL.CONTAINS(\””+ $parameters.url-object + “\”)”)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si a $parameter.url-object se le asigna “csv”, la expresión anterior se evaluará como “HTTP.REQ.URL.CONTAINS(\ “csv\”)”. Sin embargo, esta expresión no es fácil de leer. Para que esta parametrización sea fácil de leer y entender, puede utilizar interpolaciones in situ.

La expresión con interpolación in situ es ahora:

str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)

En la expresión anterior, utilizó una expresión de interpolación que agrega las comillas internas alrededor del valor de $parameters.url-object. El resultado de esta expresión es el mismo que el anterior, pero parece más intuitivo y se acerca más al resultado real.

## Tipos permitidos dentro de interpolaciones

Puede usar expresiones que generen valores de los siguientes tipos dentro de las interpolaciones: boolean, number, tcp-port, ipaddress y string. El valor generado se transforma automáticamente en una cadena cuando las interpolaciones se reemplazan con el resultado.

Las expresiones de cadena pueden tener 0, 1 o más interpolaciones. En una interpolación secuencial, diferentes partes de la expresión de cadena se pueden reemplazar por diferentes expresiones de StyleBook. Por ejemplo, la cadena lb-% {$parameters.appname} %-% {$parameters.vip}% devuelve “lb-app1-1.1.1.1”, si $parameters.appname es “app1”y $parameters.vip es “1.1.1.1”

Las expresiones de cadena también admiten interpolaciones anidadas. Es decir, una expresión de interpolación se puede anidar dentro de otra expresión de interpolación para que el valor de una expresión pueda convertirse en una entrada a la segunda expresión.

Por ejemplo, considere una cadena «% {lb-% {$parameters.port + 1}%}%»

La cadena interna “**% {$parameters.port + 1}%** “devuelve «lb-81”si $parameters.port es 80. Aquí, esta expresión está anidada dentro de otra expresión de interpolación.

En la siguiente tabla se describen los diferentes tipos de interpolaciones con ejemplos y resultados correspondientes. El valor de los parámetros utilizados en los ejemplos es:

- $parameters.appname: “lb1”
- $parámetros.vip: «1.1.1.1»
- $parameters.n1: 1
- $parameters.n2: 3

## Interpolaciones simples

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Expresión | Resultado |
| --- | --- |
| lb-% {$parameters.appname} %-def | lb-lb1-def |

### Conversiones automáticas de tipos

| Expresión | Resultado |
| --- | --- |
| lb-%{1}% | lb-1 |
| lb-%{$parameters.vip}% | lb-1.1.1.1 |
| lb-% {verdadero}% | LB-verdadero |

### Interpolaciones secuenciales

| Expresión | Resultado |
| --- | --- |
| % {$parameters.appname} %-% {str ($parameters.appname)}% | lb1-lb1 |
| lb-%{1}%-%{2}% | lb-1-2 |

### Interpolaciones anidadas

| Expresión | Resultado |
| --- | --- |
| % {abc-% {$parámetros.n1 + 1}%}% | abc-2 |
| str («% {abc-% {$parámetros.n1}%} %-% {$parámetros.n2}%») | bc-1-3 |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Interpolaciones con quotewrap

| Expresión | Resultado |
|---|---|
| str («% {quotewrap (abcd)}%»)<br>str («% {quotewrap (`https://`)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL") | «abcd<br>“«code class=”language-plaintext highlighter-rouge”>https://”+HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code> |

#### Escapar caracteres en interpolaciones

Si los caracteres «% {» o «}%» forman parte de la cadena, debe proporcionar “\» como carácter de escape para que el compilador de StyleBook no los evalúe como etiquetas de interpolación.

**Ejemplo**:

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%”if $parameters.vip is 1.1.1.1

En la siguiente tabla se describen algunas expresiones más y sus resultados:

| Categoría | Expresión | Resultado |
|---|---|---|
| Escaping interpolations | str(“%{str($parameters.n1) + }\%}%”) | 1}% |
| | lb-%{str($parameters.n1) + }\%}% | lb-1}% |
| | ”%{str($parameters.n1) + \” }\%\”}%” | 1}% |

## Funciones integradas

January 30, 2024

Las expresiones en StyleBooks pueden hacer uso de funciones integradas.

Por ejemplo, puede usar la función incorporada, `str()` para transformar un número en una cadena.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
str($parameters.order)
```

O bien, puede usar la función incorporada, `int()` para transformar una cadena en un entero.

```
int($parameters.priority)
```

La siguiente es la lista de funciones integradas admitidas en expresiones StyleBook con ejemplos de cómo se pueden usar:

### str()

La función `str()` transforma el argumento de entrada en un valor de cadena.

Tipos de argumentos permitidos:

- `string`
- `number`
- `TCP-port`
- **`boolean`**
- `IP address`

**Ejemplos**:

- La función `"set-"+ str(10)` devuelve `"set-10"`.
- La función `str(10)` devuelve `10`.
- La función `str(1.1.1.1)` devuelve `1.1.1.1`.
- La función `str(T rue)` devuelve `"T rue"`.
- La función `str(ADM)` devuelve `"mas"`.

### int()

La función `int()` toma una cadena, un número, una dirección IP, o `tcpport` como argumento y devuelve un entero.

**Ejemplos**:

- La función `int("10")` devuelve `10`.
- La función `int(10)` devuelve `10`.
- La función `int(ip('0.0.4.1'))` devuelve `1025`.

### bool()

La función `bool()` toma cualquier tipo como argumento. Si el valor del argumento es **`false`**, vacío o ausente, esta función devuelve **`false`**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

De lo contrario, regresa **true**.

**Ejemplos**:

- La función `bool(true)` devuelve **true**.
- La función `bool(false)` devuelve **false**.
- La función `bool($parameters.a)` devuelve **false** si el `$parameters.a` es **false**, vacío o ausente.

### len()

La función `len()` toma una cadena o una lista como argumento y devuelve el número de caracteres de una cadena o el número de elementos de una lista.

**Ejemplo 1**:

Si define una sustitución de la siguiente manera:

```
items: ["123", "abc", "xyz"]
```

La función `len($substitutions.items)` devuelve 3

**Ejemplo 2**:

La función `len("Citrix ADM")` devuelve `10`.

**Ejemplo 3**:

Si `$parameters.vips` tiene valores `['1.1.1.1', '1.1.1.2', '1.1.1.3']`, la función `len($parameters.vips)` devuelve 3.

### min()

La `min()` función toma ya sea una lista o una serie de números o `tcp-ports` como argumentos, y devuelve el elemento más pequeño.

**Ejemplos con una serie de números/tcp-ports**:

- La función `min(80, 100, 1000)` devuelve `80`.
- La función `min(-20, 100, 400)` devuelve `-20`.
- La función `min(-80, -20, -10)` devuelve `-80`.
- La función `min(0, 100, -400)` devuelve `-400`.

**Ejemplos con una lista de números/tcp-ports**:

- `$parameters.ports` El soporte es una lista de `tcp-ports` y tiene valores: `[80, 81, 8080]`.

  La función `min($parameters.ports)` devuelve `80`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### max()

La `max()` función toma ya sea una lista o una serie de números o `tcp-ports` como argumentos, y devuelve el elemento más grande.

**Ejemplos con una serie de números/tcp-ports**:

- La función `max(80, 100, 1000)` devuelve `1000`.
- La función `max(-20, 100, 400)` devuelve `400`.
- La función `max(-80, -20, -10)` devuelve `-10`.
- La función `max(0, 100, -400)` devuelve `100`.

**Ejemplos con una lista de números/tcp-ports**:

- `$parameters.ports` El soporte es una lista de `tcp-ports` y tiene valores: `[80, 81, 8080]`.

  La función `max($parameters.ports)` devuelve `8080`.

### bin()

La función `bin()` toma un número como argumento y devuelve una cadena que representa el número en formato binario.

**Ejemplos de expresiones**:

La función `bin(100)` devuelve `0b1100100`.

### oct()

La función `oct()` toma un número como argumento y devuelve una cadena que representa el número en formato octal.

**Ejemplos de expresiones**:

La función `oct(100)` devuelve `0144`.

### hex()

La función `hex()` toma un número como argumento y devuelve una cadena en minúsculas que representa el número en formato hexadecimal.

**Ejemplos de expresiones**:

La función `hex(100)` devuelve `0x64`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### lower()

La función `lower()` toma una cadena como argumento y devuelve la misma cadena en minúsculas.

**Ejemplo**:

La función `lower("ADM")` devuelve `adm`.

### upper()

La función `upper()` toma una cadena como argumento y devuelve la misma cadena en mayúsculas.

**Ejemplo**:

La función `upper("Citrix ADM")` devuelve `CITRIX ADM`.

### sum()

La función `sum()` toma una lista de números o `tcpports` como argumentos y devuelve la suma de los números en la lista.

**Ejemplo 1**:

Si define una sustitución de la siguiente manera:
sustituciones:

```
list-of-numbers = [11, 22, 55]
```

La función `sum($substitutions.list-of-numbers)` devuelve 88.

**Ejemplo 2**:

Si `$parameters.ports` es `[80, 81, 82]`, la función `sum($parameters.ports)` devuelve 243.

### pow()

La función `pow()` toma dos números como argumentos y devuelve un número que representa el primer argumento elevado a la potencia del segundo.

**Ejemplo**:

La función `pow(3,2)` devuelve 9.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ip()

La función `ip()` toma un entero, una cadena o una dirección IP como argumento y devuelve la dirección IP basada en el valor de entrada.

**Ejemplos**:

- Especifique una dirección IP en la función `ip`:

  La función `ip(3.1.1.1)` devuelve `3.1.1.1`.

- Especifique una cadena en la función `ip`:

  La función `ip('2.1.1.1')` devuelve `2.1.1.1`

- Especifique un entero en la función `ip`:

  - La función `ip(12)` devuelve `0.0.0.12`.
  - Cuando se especifica un entero como cadena en la función `ip`, devuelve una dirección IP equivalente de la entrada.

    La función `ip('1025')` devuelve `0.0.4.1`.

  Esta función también admite las operaciones de suma y resta enteros y devuelve una dirección IP resultante.

  - Adición: La función `ip(1025)+ ip(12)` devuelve `0.0.4.13`.
  - Resta: la función `ip('1025')- ip(12)` devuelve `0.0.3.245`.
  - Combinar suma y resta: Los `ip('1.1.1.1')+ ip('1.1.1.1')- ip(2)` retornos `2.2.2.0`.

### base64.encode()

La función `base64.encode()` toma un argumento de cadena y devuelve la cadena codificada base64.

**Ejemplo**:

La función `base64.encode("abcd")` devuelve `YWJjZA==`.

### base64.decode()

La función `base64.decode` toma una cadena codificada base64 como argumento y devuelve la cadena decodificada.

**Ejemplo**:

La función `base64.decode("YWJjZA==")` devuelve `abcd`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### exists()

La función `exists()` toma un argumento de cualquier tipo y devuelve un booleano. El valor devuelto es `True` si la entrada tiene algún valor. El valor devuelto es `False` Si el argumento de entrada no tiene un valor (es decir, no hay valor).

Tenga en cuenta que `$parameters.monitor` es un parámetro opcional. Si proporciona un valor a este parámetro al crear un paquete de configuración, existe la función (`$parameters.monitor`) devuelve `True`.

De lo contrario, regresa `False`.

### filter()

La función `filter()` toma dos argumentos.

Argumento 1: una función de sustitución que toma un argumento y devuelve un valor booleano.

Argumento 2: una lista.

La función devuelve un subconjunto de la lista original donde cada elemento evalúa `True` cuando se pasa a la función de sustitución en el primer
argumento.

**Ejemplo**:

Supongamos que hemos definido una función de sustitución de la siguiente manera.

Sustituciones:

`x(a): $a != 81`

Esta función devuelve True si el valor de entrada no es igual a `81`. De lo contrario, regresa `False`.

Supongamos que `$parameters.ports` es `[81, 80, 81, 89]`.

`filter($substitutions.x, $parameters.ports)` devuelve `[80, 89]` eliminando todas las apariciones de `81` de la lista.

### if-then-else()

La función `if-then-else()` toma tres argumentos.

Argumento 1: Expresión booleana

Argumento 2: Cualquier expresión

Argumento 3: Cualquier expresión (opcional)

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si la expresión en el argumento 1 se evalúa como `True`, la función devuelve el valor de la expresión proporcionada como argumento 2.

De lo contrario, si se proporciona el argumento 3, la función devuelve el valor de la expresión en el argumento 3.

Si no se proporciona el argumento 3, la función devuelve `no`.

**Ejemplo 1**:

La función `if-then-else($parameters.servicetype == HTTP, 80, 443)` devuelve `80` si `$parameters.servicetype` tiene valor `HTTP`. De lo contrario, la función devuelve `443`.

**Ejemplo 2**:

La función `if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` devuelve el valor de `$parameters.hport` if `$parameters.servicetype` tiene valor `HTTP`.

De lo contrario, la función devuelve el valor de `$parameters.sport`.

**Ejemplo 3**:

`if-then-else($parameters.servicetype == HTTP, 80)` devuelve `80` si `$parameters.servicetype` tiene valor `HTTP`.

De lo contrario, la función no devuelve ningún valor.

## join()

La función `join()` toma dos argumentos:

Argumento 1: lista de números `tcp-ports`, cadenas o direcciones IP

Argumento 2: cadena delimitadora (opcional)

Esta función une los elementos de la lista proporcionada como argumento uno en una cadena, donde cada elemento está separado por la cadena delimitador proporcionada como argumento dos. Si no se proporciona el argumento dos, entonces los elementos de la lista se unen como una sola cadena.

**Ejemplo**:

- `$parameters.ports` es `[81, 82, 83]`.
  - Con argumento delimitador:

    La función `join($parameters.ports, '-')` devuelve `81-82-83`.
  - Sin argumento delimitador:

    La función `join($parameters.ports)` devuelve `818283`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### split()

La función `split()` divide una cadena de entrada en varias listas dependiendo de los separadores especificados. Si no se especifica ningún separador o en blanco (`''`), esta función considera el espacio como un separador y divide la cadena en listas.

**Ejemplos:**

- La función `split('Example_string_split', 's')` devuelve `['Example_','tring_','plit']`.
- La función `split('Example string split')` devuelve `['Example','string','split']`.
- La función `split('Example string split', '')` devuelve `['Example','string','split']`.
- La función `split('Example string')` devuelve `['Example','string']`.

  Esta función considera los espacios continuos como un espacio.

### map()

La función `map()` toma dos argumentos;

Argumento 1: Cualquier función

Argumento 2: Una lista de elementos.

La función devuelve una lista donde cada elemento de la lista es el resultado de aplicar la `map()` función (argumento uno) al elemento correspondiente en el argumento dos.

Funciones permitidas en el argumento 1:

- Funciones integradas que toman un argumento:

  `base64.encode`, `base64.decode`, `bin`, `bool`, `exists`, `hex`, **`int`**, `ip`, `len`, `lower`, `upper`, `oct`, `quotewrap`, `str`, `trim`, `upper`, `url.encode`, `url.decode`

- Funciones de sustitución que toman al menos un argumento.

**Ejemplo**:

Supongamos que $parameters.nums lo es `[81, 82, 83]`.

- Mapa mediante una función integrada, str

  La función `map(str, $parameters.nums)` devuelve `["81", "82", "83"]`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El resultado de la función de mapa es la lista de cadenas donde cada elemento es cadena se calcula aplicando la función str en el elemento correspondiente en la lista de entrada ($parameters.nums).

- Mapear mediante una función de sustitución
  - Sustituciones:

    `add-10(port): $port + 10`
  - Expresión :

    La función `map($substitutions.add-10, $parameters.nums)` devuelve una lista de números: `[ 91, 92, 93 ]`

El resultado de esta función de mapa es una lista de números, cada elemento se calcula aplicando la función de sustitución `$substitutions.add-10` en el elemento correspondiente en la lista de entrada `($parameters.nums)`.

### quotewrap()

La función `quotewrap()` toma una cadena como argumento y devuelve una cadena después de agregar un carácter de comilla doble antes y después del valor de entrada.

**Ejemplo**:

La función `quotewrap("ADM")` devuelve `"mas"`

### replace()

La función `replace()` toma tres argumentos:

Argumento 1: cadena

Argumento 2: cadena o lista

Argumento 3: cadena (opcional)

La función reemplaza todas las apariciones del argumento dos por el argumento tres en el argumento uno.

Si no se proporciona el argumento tres, todas las apariciones del argumento dos se eliminan del argumento uno (en otras palabras, se reemplazan con una cadena vacía).

Reemplazar una subcadena por otra subcadena:

- La `replace('abcdef', 'def', 'xyz')` función devuelve `abcxyz`.

  Todas las ocurrencias de `def` se reemplazan por `xyz`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- `replace('abcdefabc', 'def')` devuelve `abcabc`.

  Como no hay un tercer argumento, `def` se elimina de la cadena resultante.

Especifique la lista de caracteres que quiere reemplazar en una cadena.

`$parameters.spl_chars = ['@', '#', '!', '%']`

Esta lista contiene los valores que deben reemplazarse en una cadena de entrada.

La `replace('An#example@to%replace!characters', $parameters.spl_chars, '_')` función devuelve `An_example_to_replace_characters`.

La cadena de salida tiene guión bajo (_) en lugar de caracteres especificados en la lista `$parameters.spl_chars`.

### trim()

La función `trim()` devuelve una cadena donde los espacios en blanco iniciales y finales se eliminan de la cadena de entrada.

**Ejemplo**:

La función `trim('abc ')` devuelve `abc`.

### truncate()

La función `truncate()` toma dos argumentos:

Argumento 1: cadena

Argumento 2: número

La función devuelve una cadena en la que la cadena de entrada del argumento uno se trunca a la longitud especificada por el argumento dos.

**Ejemplo**:

`truncate('Citrix ADM', 6)` devuelve `Citrix`.

### distinct()

La función `distinct()` extrae elementos únicos de una entrada de lista.

**Ejemplos:**
Si `$parameters.input_list` es `['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']`, la función `distinct($parameters.input_list)` devuelve `['ADM', 'ADC', 'VPX', 'CPX']`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### url.encode()

La función `url.encode()` devuelve una cadena donde los caracteres se transforman mediante el juego de caracteres ASCII de acuerdo con RFC 3986.

**Ejemplo**:

La función `url.encode("a/b/c")` devuelve `a%2Fb%2Fc`.

### url.decode()

La función `url.decode()` devuelve una cadena donde el argumento codificado URL se decodifica en una cadena regular de acuerdo con RFC 3986.

**Ejemplo**:

La función `url.decode("a%2Fb%2Fc")` devuelve `a/b/c`.

### is-ipv4()

La función `is-ipv4()` toma una dirección IP como argumento y devuelve el booleano `True` si la dirección IP es del formato IPv4.

La función `is-ipv4(10.10.10.10)` devuelve `True`

### is-ipv6()

La función `is-ipv6()` toma una dirección IP como argumento y devuelve el booleano `True` si la dirección IP es del formato IPv6.

La función `is-ipv6(2001:DB8::)` devuelve `True`

### startswith()

La función `startswith()` determina si una cadena comienza con un prefijo dado. Esta función requiere dos argumentos de cadena obligatorios.

`startswith(str, sub_str)`

Esta función devuelve `True` cuando la cadena (`str`) comienza con la subcadena (`sub_str`).

**Ejemplos**:

- La función `startswith('Citrix', 'Ci')` devuelve `True`.
- La función `startswith('Citrix', 'iC')` devuelve `False`
- La función `startswith('Citrix', 'Ab')` devuelve `False`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### endswith()

La función `endswith()` determina si una cadena termina con un sufijo dado. Esta función requiere dos argumentos de cadena obligatorios.

`endswith(str, sub_str)`

Esta función devuelve `True` cuando la cadena (`str`) termina con la subcadena (`sub_str`).

**Ejemplos**:

- La función `endswith('Citrix', 'ix')` devuelve `True`.
- La función `endswith('Citrix', 'Ix')` devuelve `False`.
- La función `endswith('Citrix', 'ab')` devuelve `False`.

### contains()

La función `contains()` determina si una cadena contiene una subcadena dada. Esta función requiere dos argumentos de cadena obligatorios.

`contains(str, sub_str)`

Esta función devuelve `True` cuando la subcadena (`sub_str`) está contenida en cualquier lugar dentro de la cadena (`str`).

Ejemplo :

- La `contains('Citrix', 'tri')` función devuelve `True`.
- La función `contains('Citrix', 'Ci')` devuelve `True`.
- La `contains('Citrix', 'ti')` función devuelve `False`

### substring()

Utilice la función `substring()` para extraer una subcadena de una cadena.

`substring(str, start_index, end_index)`

Esta función requiere los dos argumentos obligatorios y un argumento entero opcional.

- `str` (Obligatorio)
- `start_index` (Obligatorio)
- `end_index` (Opcional)

Esta función devuelve la subcadena de la cadena (`str`) que se encuentra entre las posiciones de índice especificadas. Si no especifica la posición del índice final, la función extrae la subcadena desde el índice inicial hasta el final de la cadena.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Cuando se especifica `end_index`, la subcadena excluye el carácter en la posición `end_index`.

Ejemplo :

- La función `substring('Citrix', 2)` devuelve `trix`
- La función `substring('Citrix', 10)` devuelve (")

  En este ejemplo, la función devuelve una cadena en blanco porque tiene una posición `start_index` no válida.
- La función `substring('Citrix', 2, 4)` devuelve `tr`

  En este ejemplo, la función extrae los caracteres entre 2 y 4 posiciones de índice.
- La función `substring('Citrix', -3)` devuelve `rix`

  Si quiere extraer caracteres que están al final de la cadena, especifique un valor negativo para el argumento `start_index`.

  En este ejemplo, la función extrae la subcadena que incluye los tres últimos caracteres de la cadena.

## Detección de dependencias

January 30, 2024

Los componentes de un StyleBook pueden hacer referencia a propiedades o secciones de otros componentes del mismo StyleBook. Los componentes son bloques completos por sí mismos y es posible que no se escriban en el mismo orden en que deben ejecutarse. El compilador StyleBook comprueba el orden en que se escriben los componentes y, a continuación, los ejecuta en un orden lógico.

**Ejemplo**:

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
13      condition: $parameters.create-binding
14      properties:
15        name: $components.lbvserver-comp.properties.name
16        servicegroupname: $components.sg-comp.properties.servicegroupname
17  -
18      name: sg-comp
19      type: ns::servicegroup
20      properties:
21        servicegroupname: mysg
22        servicetype: HTTP
```

En el ejemplo anterior, hay tres componentes definidos: **lbvserver-comp**, **lb-sg-binding-comp** y **sg-comp**. Cuando se ejecuta este StyleBook, primero se crea el lbvserver-comp. El lb-sg-binding-comp hace referencia a las propiedades de lbvserver-comp, pero no se puede crear a continuación, aunque es el segundo componente definido en el StyleBook. Esto se debe a que el lb-sg-binding-comp también depende del sg-comp que aún no se ha creado. Como resultado, el compilador reordena los componentes para que las dependencias de un componente se resuelvan cuando se crea un componente y ejecuta esta lista reordenada de componentes. El orden de ejecución del StyleBook anterior es: lbvserver-comp, sg-comp y lb-sg-binding-comp.

Por lo tanto, el autor de un StyleBook no necesita preocuparse por el orden correcto de los componentes. Los componentes pueden aparecer en cualquier orden. El compilador calcula el orden correcto de ejecución de los componentes en función de cómo los componentes se refieren entre sí. Tenga en cuenta que esta detección y reordenamiento de dependencias también funcionan para las secciones de sustituciones y salidas.

### Dependencias cíclicas

Dado que un componente puede hacer referencia a otro componente, es posible que se introduzca el ciclo de dependencias en la definición del StyleBook. Por ejemplo, si el componente A hace referencia a una propiedad definida en el componente B, que de nuevo hace referencia a una propiedad definida en el componente A. Este tipo de dependencia se denomina dependencias cíclicas. Las dependencias cíclicas no se pueden resolver automáticamente. El autor del StyleBook debe corregir manualmente la definición del StyleBook para eliminar esas dependencias cíclicas. El compilador podrá identificar dependencias cíclicas, si existen, e informarlo.

El siguiente ejemplo muestra una dependencia cíclica de componentes:

```
1  components:
2    -
3      name: lbvserver-comp
4      type: ns::lbvserver
5      properties:
6        name: $components.lb-sg-binding-comp.properties.name
7        ipv46: 10.102.190.15
8        port: 80
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
9         servicetype: HTTP
10    -
11      name: lb-sg-binding-comp
12      type: ns::lbvserver_servicegroup_binding
13      condition: $parameters.create-binding
14      properties:
15       name: mylb
16        servicegroupname: $components.sg-comp.properties.servicegroupname
17    -
18      name: sg-comp
19      type: ns::servicegroup
20      properties:
21        servicegroupname: mysg
22        servicetype: $components.lbvserver-comp.properties.servicetype
```

En el ejemplo anterior, hay tres componentes: **lbvserver-comp**, **lb-sg-binding-comp** y **sg-comp**. lbvserver-comp depende de lb-sg-binding-comp, lb-sg-binding comp depende de sg-comp y sg-comp depende de lbvserver-comp. Aquí, se forma un ciclo de dependencias entre estos componentes y esto no se puede resolver automáticamente. Como resultado, este StyleBook no se puede ejecutar. El compilador de StyleBook detecta esto e impide que StyleBook se importe a NetScaler ADM.

## Administración de instancias

January 30, 2024

Las instancias son dispositivos Citrix Application Delivery Controller (ADC) que puede administrar, supervisar y solucionar problemas mediante NetScaler Application Delivery Management (ADM). Debe agregar instancias a NetScaler ADM para supervisarlas. Se pueden agregar instancias al configurar Citrix ADM o una versión posterior. Después de agregar instancias a NetScaler ADM, se sondean continuamente para recopilar información que posteriormente se puede utilizar para resolver problemas o como datos de informes.

Las instancias se pueden agrupar como un grupo estático o como un bloque IP privado. Un grupo estático de instancias puede resultar útil cuando desee ejecutar tareas específicas, como trabajos de configuración, etc. Un bloque IP privado agrupa sus instancias en función de sus ubicaciones geográficas.

### Agregar una instancia

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde. Para agregar instancias, debe especificar el nombre de host o la dirección IP de cada instancia de Citrix ADC, o un intervalo de direcciones IP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para obtener información sobre cómo agregar una instancia a NetScaler ADM, consulte Agregar instancias a NetScaler ADM.

Cuando agrega una instancia al servidor NetScaler ADM, el servidor se agrega implícitamente como destino de captura para la instancia y recopila el inventario de la instancia. Para obtener más información, consulte Cómo NetScaler ADM descubre instancias.

Después de agregar una instancia, puede eliminarla navegando a **Redes**> **Panel** y haciendo clic en **Todas las instancias**. En la página Instancias, seleccione la instancia que quiere eliminar y haga clic en **Quitar**.

## Cómo usar el panel de instancias

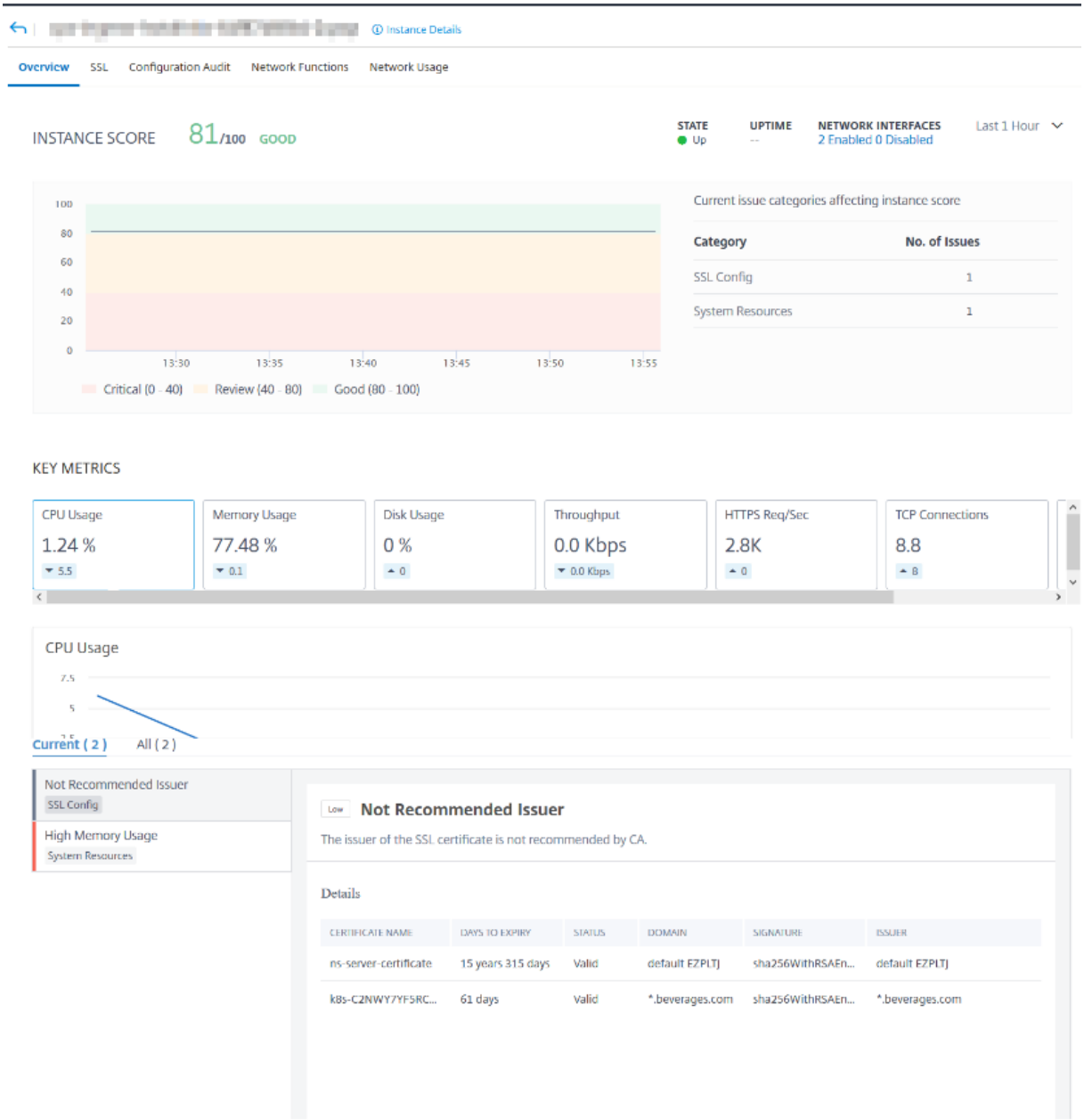
El panel de control por instancia de NetScaler ADM muestra los datos en formato tabular y gráfico de la instancia seleccionada. Los datos recopilados de su instancia durante el proceso de sondeo se muestran en el panel de control.

De forma predeterminada, cada minuto, las instancias administradas se sondean para la recopilación de datos. Información estadística como el estado, las solicitudes HTTP por segundo, el uso de CPU, el uso de memoria y el rendimiento se recopilan continuamente mediante llamadas NITRO. Como administrador, puede ver todos estos datos recopilados en una sola página, identificar problemas en la instancia y tomar medidas inmediatas para rectificarlos.

Para ver el panel de control de una instancia específica, vaya a **Redes** > **Instancias** . En el resumen, elija el tipo de instancia y, a continuación, seleccione la instancia que quiere ver y haga clic en **Panel**.

La siguiente ilustración proporciona una visión general de los diversos datos que se muestran en el panel de control por instancia:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Visión general**. La ficha de información general muestra el uso de la CPU y la memoria de la instancia elegida. También puede ver los eventos generados por la instancia y los datos de rendimiento. Aquí también se muestra información específica de la instancia, como la dirección IP, sus versiones de hardware y LOM, los detalles del perfil, el número de serie, la persona de contacto, etc. Desplácese hacia abajo más, las funciones con licencia que están disponibles en la instancia elegida junto con los modos configurados en ella.

  Para obtener más información, consulte Detalles de la instancia.

- **Tablero SSL**. Puede usar la ficha SSL del panel de control por instancia para ver o supervisar los detalles de los certificados SSL, los servidores virtuales SSL y los protocolos SSL de la instancia

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

elegida. Puede hacer clic en los "números"de los gráficos para ver más detalles.

- **Auditoría de configuración**. Puede utilizar la ficha Auditoría de configuración para ver todos los cambios de configuración que se han producido en la instancia elegida. Los gráficos de**estado guardado de la configuración de NetScaler** y de **deriva de la configuración de NetScaler**del panel muestran detalles de alto nivel sobre los cambios de configuración en las configuraciones guardadas frente a las no guardadas.
- **Funciones de red**. Mediante el panel de funciones de red, puede supervisar el estado de las entidades configuradas en la instancia de NetScaler ADC seleccionada. Puede ver gráficos de sus servidores virtuales que muestran datos como las conexiones de los clientes, el rendimiento y las conexiones de los servidores.
- **Uso de red**. Puede ver los datos de rendimiento de la red de la instancia seleccionada en la ficha Uso de la red. Puede mostrar informes de una hora, un día, una semana o un mes. La función deslizante de línea de tiempo se puede utilizar para personalizar la duración de los informes de red que se generan. De forma predeterminada, solo se muestran ocho informes, pero puede hacer clic en el icono "más"situado en la esquina inferior derecha de la pantalla para agregar un informe de rendimiento adicional.

## Supervisar sitios distribuidos globalmente

January 30, 2024

Como administrador de red, es posible que tenga que supervisar y administrar las instancias de red implementadas en ubicaciones geográficas. Sin embargo, no es fácil medir los requisitos de la red cuando se administran instancias de red en centros de datos distribuidos geográficamente.

Geomaps de NetScaler Application Delivery Management (ADM) le proporciona una representación gráfica de sus sitios y desglosa su experiencia de supervisión de red por geografía. Con las geometrías, puede visualizar la distribución de instancias de red por ubicación y supervisar los problemas de red.

En la siguiente sección se explica cómo puede supervisar los centros de datos en NetScaler ADM.

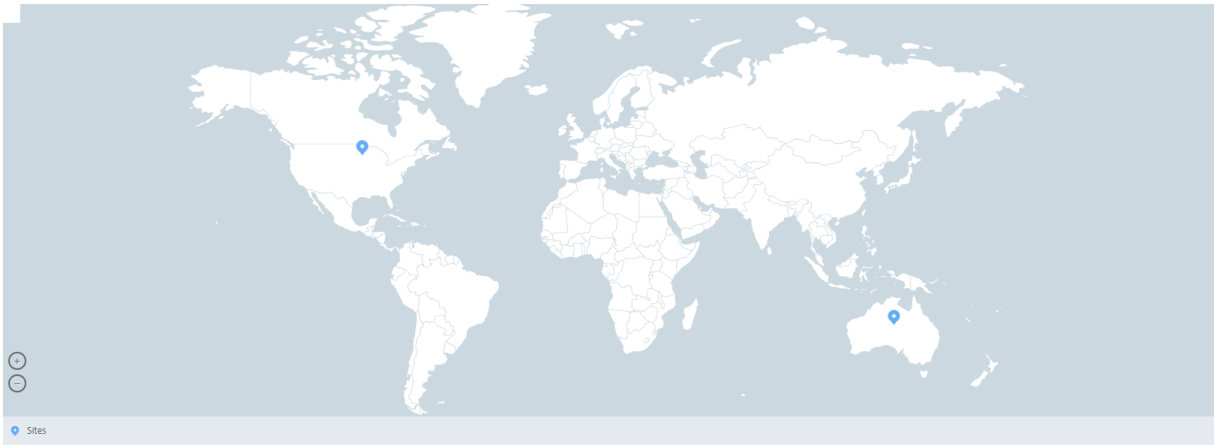
El sitio de NetScaler ADM es una agrupación lógica de instancias de Citrix Application Delivery Controller (ADC) en una ubicación geográfica específica. Por ejemplo, mientras que un sitio está asignado a Amazon Web Services (AWS) y otro sitio puede estar asignado a Azure™. Otro sitio más está alojado en las instalaciones del arrendatario. NetScaler ADM administra y supervisa todas las instancias de NetScaler ADC conectadas a todos los sitios. Puede usar NetScaler ADM para supervisar y recopilar syslog, AppFlow, SNMP y cualquier dato de este tipo que se origine en las instancias administradas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

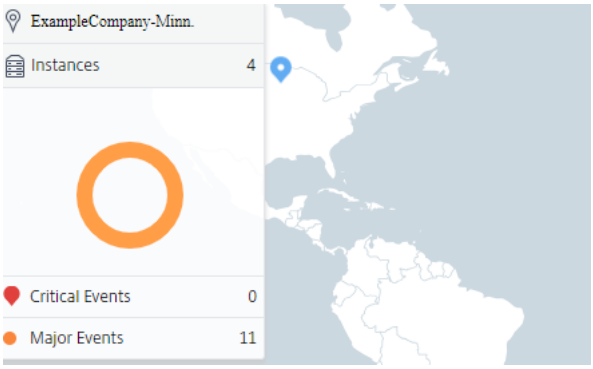
Geomaps en NetScaler ADM le proporciona una representación gráfica de sus sitios. Geomaps también desglosa su experiencia de supervisión de red por área geográfica. Con las geometrías, puede visualizar la distribución de instancias de red por ubicación y supervisar todos los problemas de red. Puede ir a la página **Redes** > **Panel** de control para obtener una representación visual de los sitios creados en el mapa mundial.

## Caso de uso

Una empresa líder de telefonía móvil, ExampleCompany, dependía de proveedores de servicios privados para alojar sus recursos y aplicaciones. La empresa ya tenía dos sedes: una en Minneapolis (Estados Unidos) y otra en Alice Springs (Australia). En esta imagen, puede ver que dos marcadores representan los dos sitios existentes.




Los marcadores también muestran un número, que muestra el número de aplicaciones en cada sitio. Puede hacer clic en estos marcadores para obtener más información sobre cada sitio.



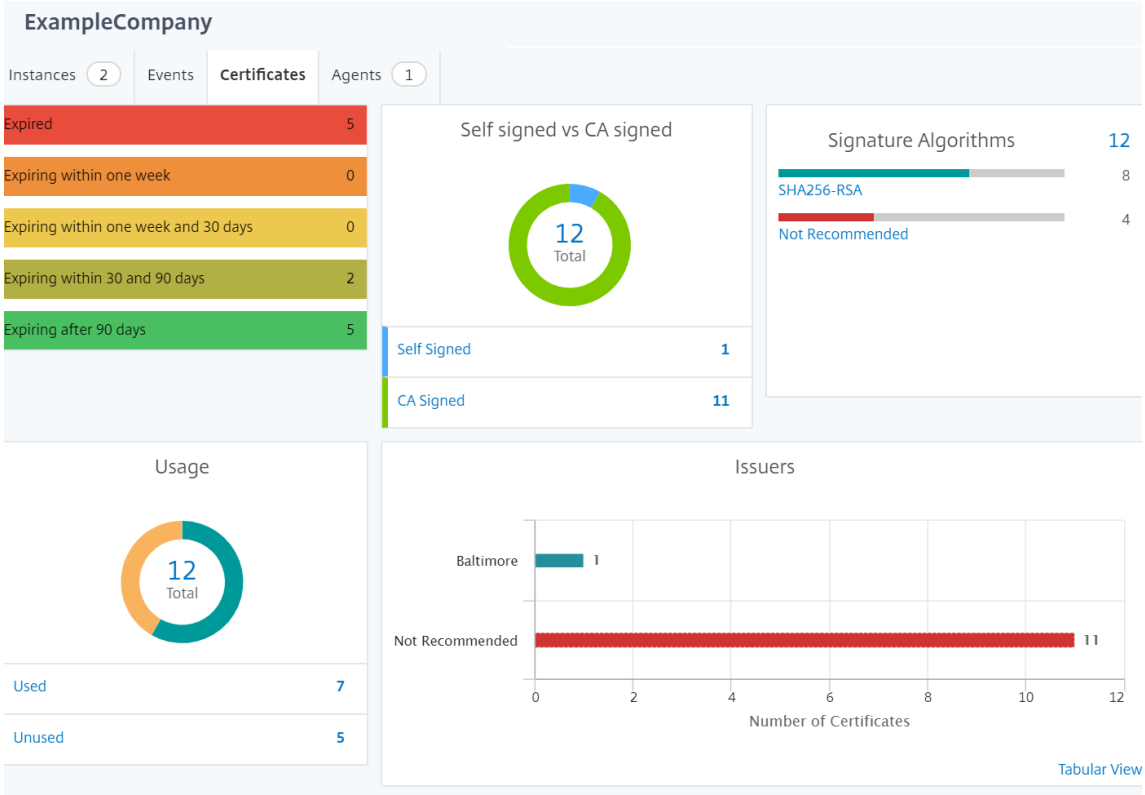

Haga clic en las fichas para ver más información:

- Ficha**Instancias**: consulte lo siguiente en esta ficha:
  - Dirección IP de cada instancia de red
  - Tipo de instancia

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - Número de eventos críticos en ellos
  - Eventos significativos y todos los eventos generados en una instancia de NetScaler ADC.

- Ficha**Eventos**: consulta una lista de los eventos importantes y críticos que se producen en las instancias.
- Ficha**Certificados**: vea lo siguiente en esta ficha:
  - Lista de certificados de todas las instancias
  - Estado de caducidad
  - Información vital y las 10 instancias principales según muchos certificados en uso.
- Ficha**Agentes**: Permite ver una lista de agentes a los que están enlazadas las instancias.




## Configuración de Geomaps

ExampleCompany decidió crear un tercer sitio en Bangalore, India. La empresa quería probar la nube descargando algunas de sus aplicaciones de TI internas menos críticas a la oficina de Bangalore. La empresa decidió utilizar los servicios de computación en la nube de AWS.

Como administrador, primero debe crear un sitio y, a continuación, agregar las instancias de NetScaler ADC en NetScaler ADM. También debe agregar la instancia al sitio, agregar un agente y vincular el

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

agente al sitio. A continuación, NetScaler ADM reconoce el sitio al que pertenecen la instancia de NetScaler ADC y el agente.

Para obtener más información sobre cómo agregar instancias de Citrix ADC, consulte Agregar instancias.

**Para crear sitios:**

Cree sitios antes de agregar instancias en NetScaler ADM. Proporcionar información de ubicación le permite localizar el sitio con precisión.

Vaya a **Redes** > **Sitios** y, a continuación, haga clic en **Agregar** .

1. En la página**Crear Sitio**, especifique la siguiente información:

   a) **Tipo de sitio**: seleccione **Centro de datos**.

   > **Nota**
   >
   > El sitio puede funcionar como centro de datos principal o como sucursal. Elija según corresponda.

   b) **Tipo**: seleccione AWS como proveedor de nube de la lista.

   > **Nota**
   >
   > Active la casilla **Usar VPC existente como sitio** en consecuencia.

   c) **Nombre del sitio**: escriba el nombre del sitio.

   d) **Ciudad**: escriba la ciudad.

   e) **Código postal**: escriba el código postal.

   f) **Región**: escriba la región.

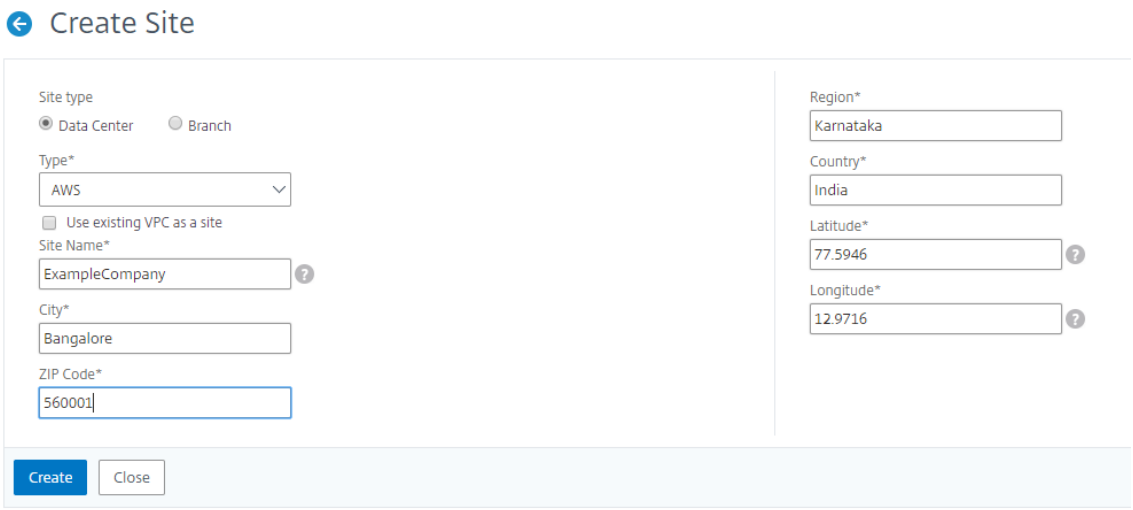
   g) **País**: Escriba el país

   h) **Latitud**: Escriba la latitud de la ubicación.

   i) **Longitud**: Escriba la longitud de la ubicación.

2. Haga clic en **Create**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



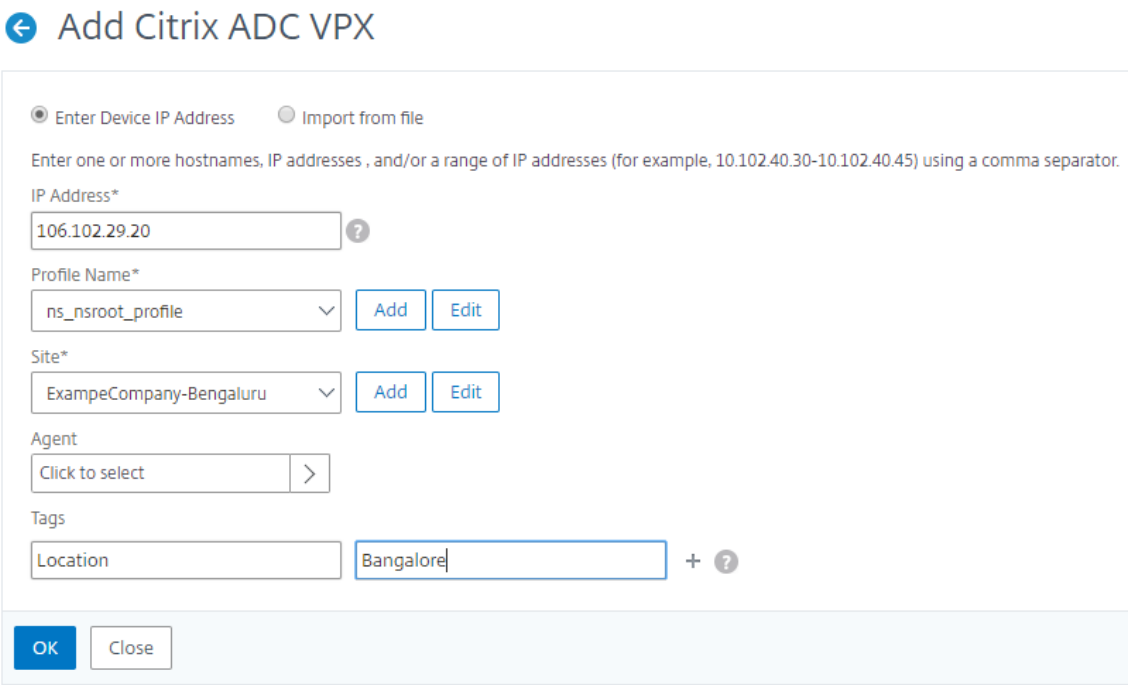

**Para agregar instancias y seleccionar sitios:**

Tras crear los sitios, debe agregar instancias en NetScaler ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

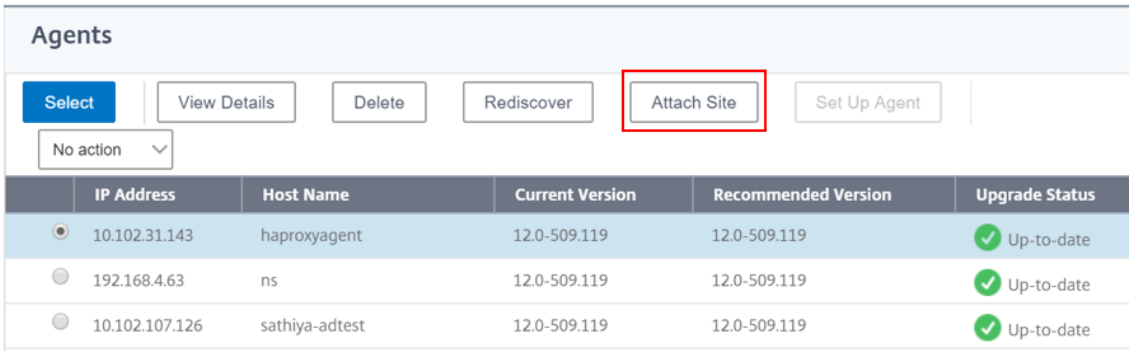
Tras crear los sitios, debe agregar instancias en NetScaler ADM. Puede seleccionar el sitio creado anteriormente o también puede crear un sitio y asociar la instancia.

1. En Citrix ADM, vaya a **Redes** > **Instancias**.
2. Seleccione el tipo de instancia que quiere crear y haga clic en **Agregar**.
3. En la página **Agregar NetScaler ADC VPX**, escriba la dirección IP y seleccione el perfil de la lista.
4. Seleccione el sitio de la lista. Puede hacer clic en el signo + situado junto al campo **Sitio** para crear un sitio o hacer clic en el icono de edición para cambiar los detalles del sitio predeterminado.
5. Haga clic en la flecha derecha y seleccione el agente de la lista que aparece.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Después de elegir el agente, debe asociar el agente con el sitio. Este paso permite que el agente esté vinculado al sitio. Seleccione el agente y haga clic en **Adjuntar sitio**.




1. Seleccione el sitio de la lista y haga clic en **Guardar**.

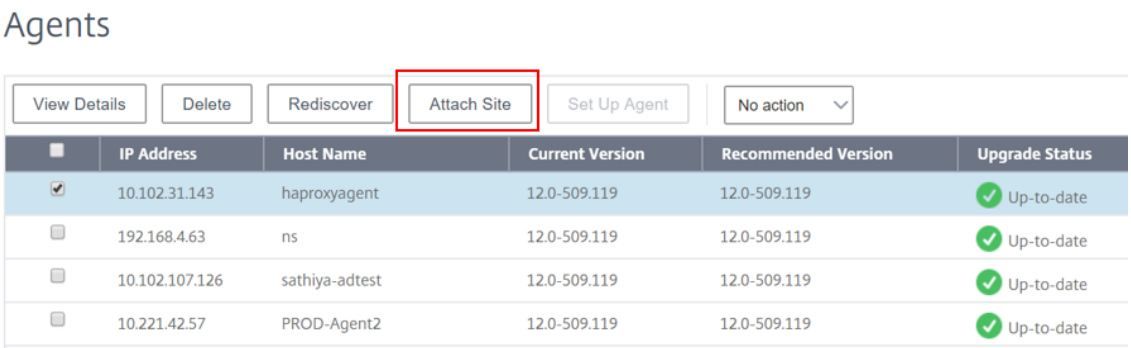
1. Haga clic en **Aceptar**.

También puede adjuntar un agente a un sitio accediendo a **Redes** > **Agentes** .

**Para asociar un agente NetScaler ADM al sitio:**

1. En Citrix ADM, vaya a **Redes** > **Agentes** .
2. Seleccione el agente y haga clic en **Adjuntar sitio**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




1. Puede asociar el sitio y hacer clic en **Guardar**.

NetScaler ADM comienza a supervisar las instancias de NetScaler ADC agregadas en el sitio de Bangalore junto con las instancias en los otros dos sitios.

## Cómo crear etiquetas y asignar a instancias

January 30, 2024

Citrix Application Delivery Management (ADM) ahora le permite asociar las instancias de Citrix Application Delivery Controller (ADC) con etiquetas. Una etiqueta es una palabra clave o un término de una palabra que puede asignar a una instancia. Las etiquetas agregan información adicional sobre la instancia. Las etiquetas pueden considerarse metadatos que ayudan a describir una instancia. Las etiquetas le permiten clasificar y buscar instancias basadas en estas palabras clave específicas. También puede asignar varias etiquetas a una sola instancia.

Los siguientes casos de uso le ayudan a comprender cómo el etiquetado de instancias le ayuda a supervisarlas mejor.

- **Caso de uso 1**: puede crear una etiqueta para identificar todas las instancias en el Reino Unido. Aquí, puede crear una etiqueta con la clave como "País"y el valor como "Reino Unido". Esta etiqueta le ayuda a buscar y supervisar todas esas instancias en el Reino Unido.
- **Caso de uso 2**: Quiere buscar instancias que se encuentran en el entorno provisional. Aquí, puede crear una etiqueta con la clave como "Propósito"y el valor como "Staging_ns. "Esta etiqueta le ayuda a separar todas las instancias que se están utilizando en el entorno de ensayo de las instancias que tienen solicitudes de cliente ejecutándose a través de ellas.
- **Caso de uso 3**: considere una situación en la que quiera conocer la lista de instancias de NetScaler ADC que se encuentran en el área "Swindon"en el Reino Unido y que son propiedad de usted, David T. Puede crear etiquetas para todos estos requisitos y asignarlas a todas las instancias que cumplan estas condiciones.

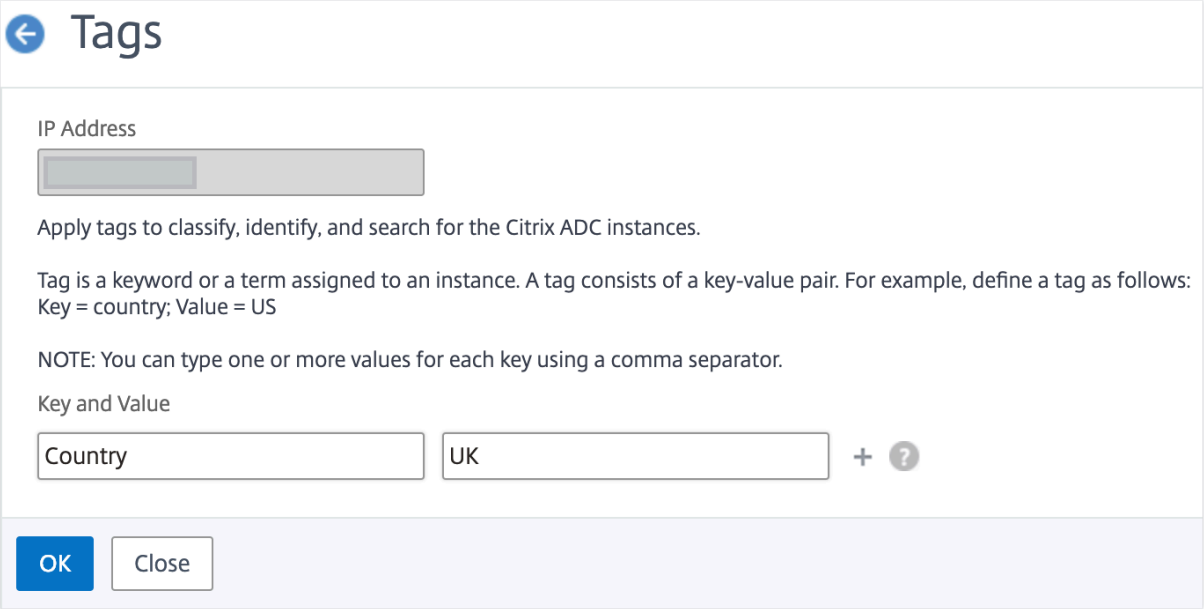
**Para asignar etiquetas a la instancia de NetScaler ADC VPX:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

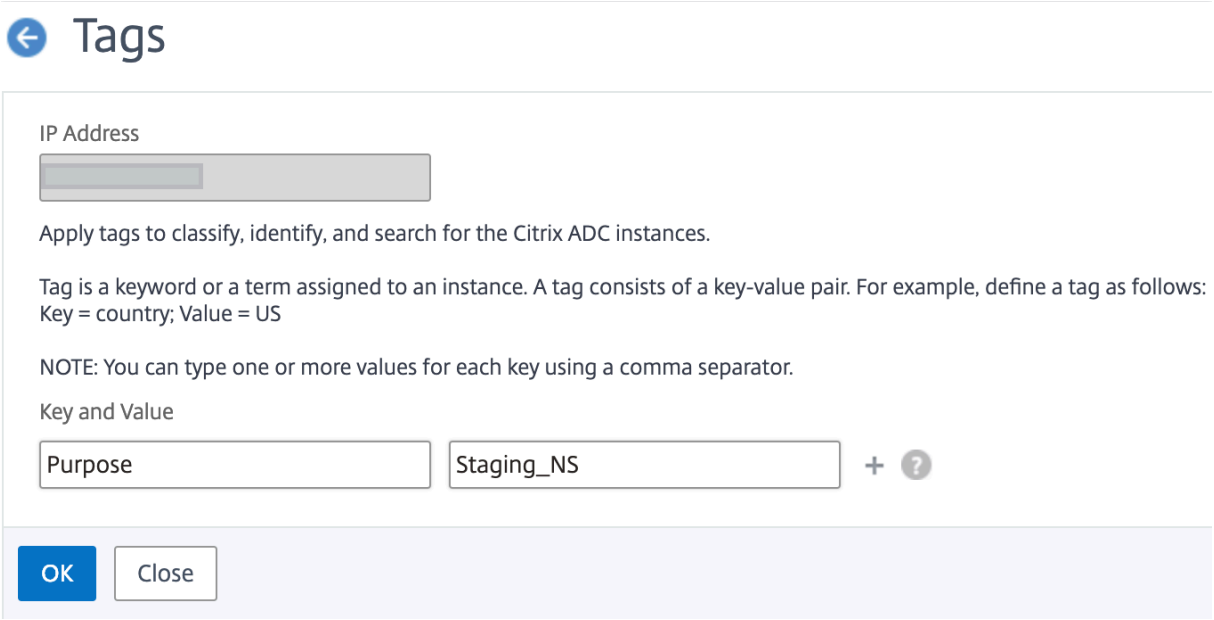
1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix ADC** .
2. Seleccione la ficha **NetScaler ADC VPX**.
3. Seleccione el Citrix VPX requerido.
4. Haga clic en **Etiquetas**.
5. Cree etiquetas y haga clic en **Aceptar**.

La ventana de **etiquetas** que aparece le permite crear sus propios pares de "clave-valor"asignando valores a cada palabra clave que cree.

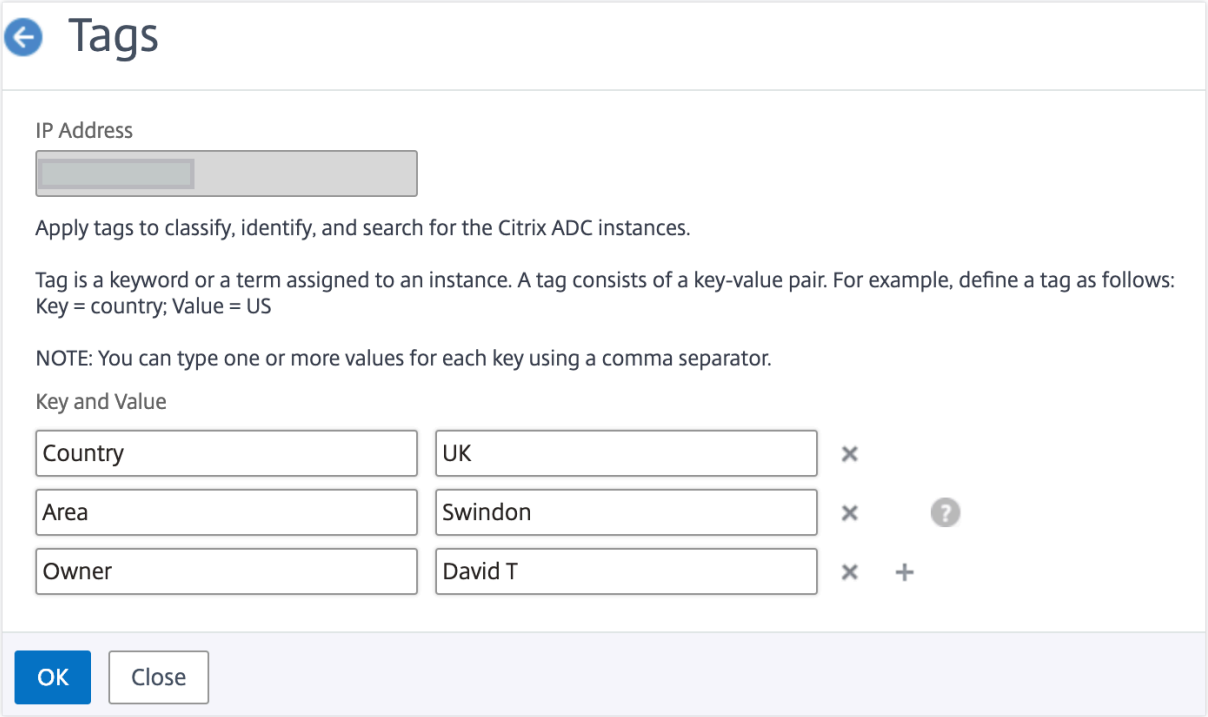
Por ejemplo, las siguientes imágenes muestran algunas palabras clave creadas y sus valores. Puede agregar sus propias palabras clave y escribir un valor para cada palabra clave.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



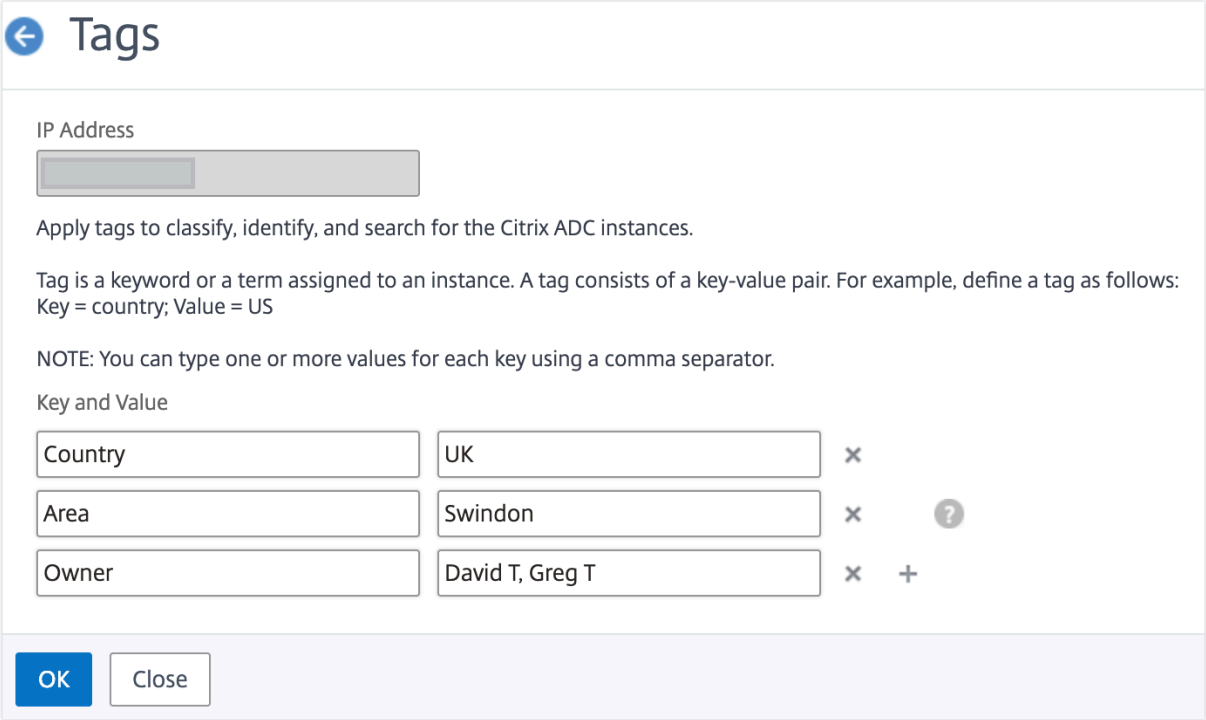

También puede agregar varias etiquetas haciendo clic en "+. "La adición de etiquetas múltiples y significativas le permite buscar de manera eficiente las instancias.




Puede agregar varios valores a una palabra clave separándolos con comas.

Por ejemplo, está asignando el rol de administrador a otro compañero de trabajo, Greg T. Puede agregar su nombre separado por una coma. Agregar varios nombres le ayuda a buscar por cualquiera de los nombres o por ambos nombres. NetScaler ADM reconoce los valores separados por comas en dos valores diferentes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para obtener más información sobre cómo buscar instancias en función de etiquetas, consulte Cómo buscar instancias mediante valores de etiquetas y propiedades.

> **Nota**Posteriormente,
>
> puede agregar nuevas etiquetas o eliminar etiquetas existentes. No hay restricción en el número de etiquetas que se crean.

## Cómo buscar instancias mediante valores de etiquetas y propiedades

January 30, 2024

Puede haber una situación en la que NetScaler Application Delivery Management (ADM) administre muchas instancias de NetScaler ADC. Como administrador, es posible que desees tener la flexibilidad de buscar en el inventario de instancias en función de ciertos parámetros. NetScaler ADM ahora ofrece una capacidad de búsqueda mejorada para buscar en un subconjunto de instancias de NetScaler ADC en función de los parámetros que defina en el campo de búsqueda. Puede buscar las instancias en función de dos criterios: etiquetas y propiedades.

- **Etiquetas**. Las etiquetas son términos o palabras clave que puede asignar a una instancia de NetScaler ADC para agregar alguna descripción adicional sobre la instancia de NetScaler ADC. Ahora puede asociar sus instancias de NetScaler ADC con etiquetas. Estas etiquetas se pueden usar para identificar y buscar mejor las instancias de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Propiedades**. Cada instancia de NetScaler ADC agregada en NetScaler ADM tiene algunos parámetros o propiedades predeterminados asociados a esa instancia. Por ejemplo, cada instancia tiene su propio nombre de host, dirección IP, versión, ID de host, ID de modelo de hardware, etc. Puede buscar instancias especificando valores para cualquiera de estas propiedades.

Por ejemplo, considere una situación en la que quiere obtener la lista de instancias de NetScaler ADC que están en la versión 12.0 y están en estado ACTIVO. Aquí, la versión y el estado de la instancia se definen mediante las propiedades predeterminadas.

Además de la versión 12.0 y el estado de funcionamiento de las instancias, también puede buscar aquellas instancias que le pertenezcan. Puede crear una etiqueta de "Propietario"y asignarle un valor "David T". Para obtener más información sobre cómo crear y asignar etiquetas, consulta Cómo crear etiquetas y asignar a instancias.

Puede utilizar una combinación de etiquetas y propiedades para crear sus propios criterios de búsqueda.

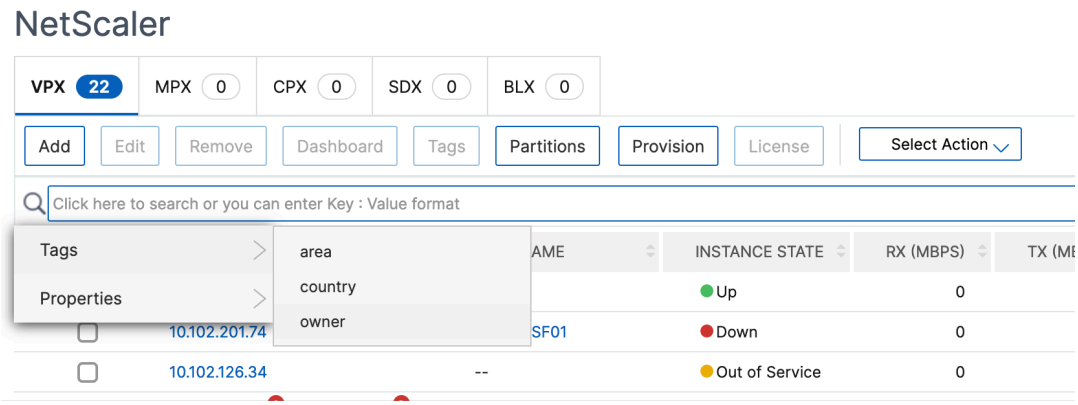
### Para buscar instancias de NetScaler ADC VPX

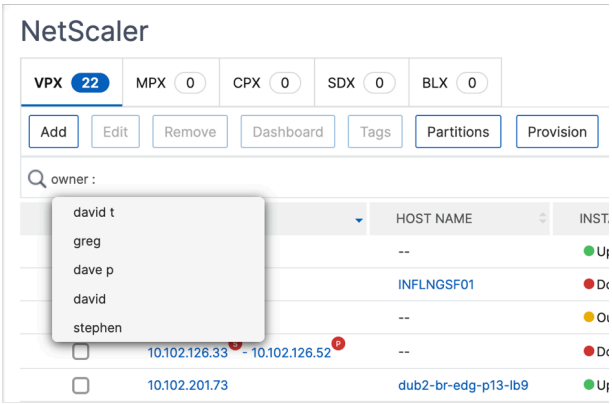
1. En Citrix ADM, vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX**.
2. Haga clic en el campo de búsqueda. Puede crear una expresión de búsqueda mediante etiquetas o propiedades o combinando ambas.

   Los siguientes ejemplos muestran cómo puede utilizar la expresión de búsqueda de manera eficiente para buscar la instancia.

   a) Seleccione la opción **Etiquetas** y seleccione **Propietario**. Selecciona "David T."

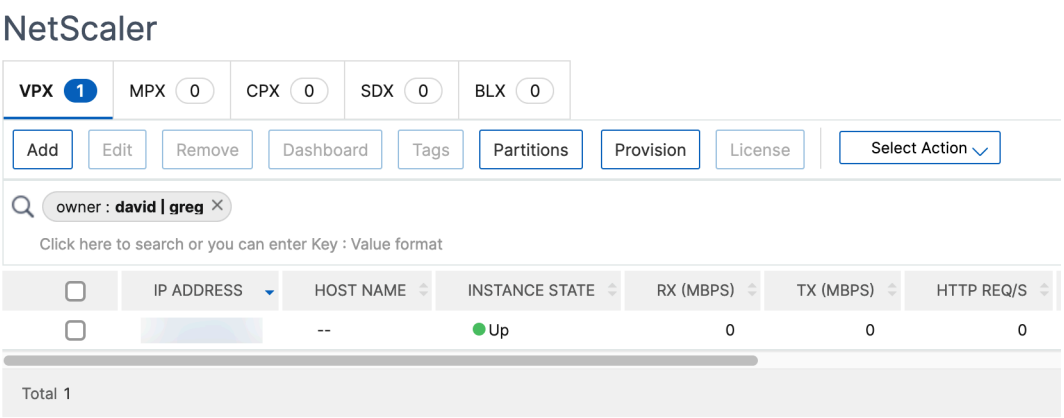
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



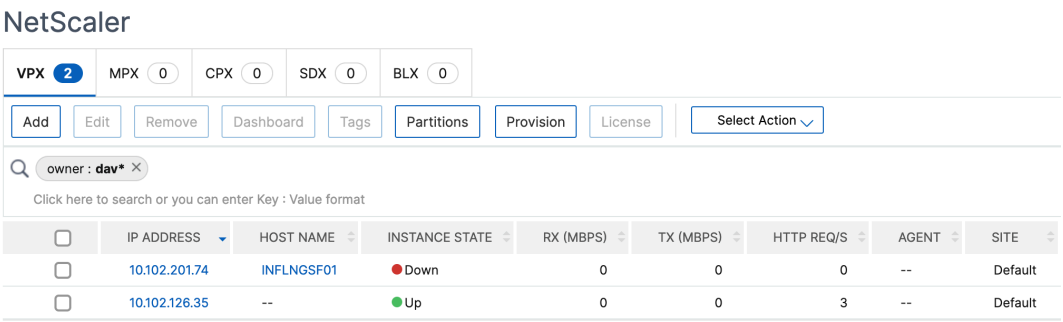

NetScaler ADM admite expresiones regulares y caracteres comodín en las expresiones de búsqueda.

b) Puede utilizar expresiones regulares para ampliar aún más los criterios de búsqueda. Por ejemplo, quiere buscar instancias que sean propiedad de David o Stephen. En tal caso, puede escribir los valores separando los valores con una expresión "|".




c) También puede utilizar caracteres comodín para reemplazar o representar uno o más caracteres. Por ejemplo, puede escribir `Dav*` para buscar todas las instancias propiedad de David T y Dave P.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> Para obtener más información sobre expresiones regulares y caracteres comodín y cómo usarlos, haga clic en el icono “información”de la barra de búsqueda.

## Administrar particiones de administración de instancias NetScaler ADC

January 30, 2024

Puede configurar particiones de administración en sus instancias de Citrix Application Delivery Controller (ADC) para que a los diferentes grupos de su organización se les asignen diferentes particiones en la misma instancia de Citrix ADC. Se puede asignar un administrador de red para administrar varias particiones en varias instancias de Citrix ADC.

Citrix Application Delivery Management (ADM) proporciona una forma sencilla de administrar todas las particiones que pertenecen a un administrador desde una única consola. Puede administrar estas particiones sin interrumpir otras configuraciones de particiones.

Para permitir que varios usuarios administren diferentes particiones de administración, debe crear grupos y, a continuación, asignar usuarios y particiones a esos grupos. Cada usuario puede ver y administrar solo las particiones del grupo al que pertenece el usuario. Cada partición de administración se considera como una instancia en NetScaler ADM. Cuando detecta una instancia de NetScaler ADC, las particiones de administración configuradas en esa instancia de NetScaler ADC se agregan al sistema automáticamente.

Tenga en cuenta que tiene dos instancias de Citrix VPX con dos particiones configuradas en cada instancia. Por ejemplo, la instancia de ADC 10.102.216.49 de Citrix tiene Partition_1, Partition_2 y Partition_3, y la instancia de NetScaler ADC 10.102.29.120 tiene p1 y p2 como se muestra en la imagen siguiente.

Para ver las particiones, vaya a**Redes > Instancias > NetScaler ADC > VPX**y, a continuación, haga clic en **Particiones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede asignar al usuario p1 las siguientes particiones: 10.102.29.120-p1 y 10.102.216.49-Partition_1. Además, puede asignar user-p2 para administrar las particiones 10.102.29.80-p2, 10.102.216.49-Partition_2 y 10.102.216.49-Partition_3.

A continuación, debe crear los dos usuarios, user-p1 y user-p2, y debe asignar los usuarios a los grupos que creó para ellos.

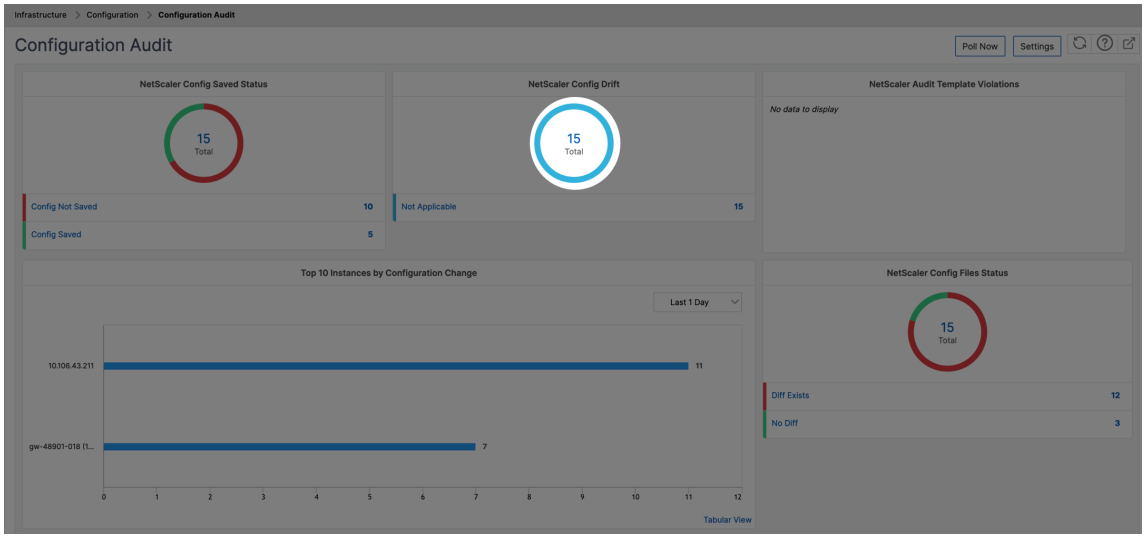
En primer lugar, debe crear dos grupos con los permisos adecuados (por ejemplo, permisos de administrador) e incluir las instancias de partición de administración necesarias en cada grupo. Por ejemplo, cree el grupo del sistema Partition1-admin y agregue las particiones 10.102.29.120-p1 y 10.102.216.49-Partition_1 de Citrix ADC a este grupo. Cree también el grupo de sistemas Partition2-admin y agregue las particiones de administración 10.102.29.120-p2, 10.102.216.49-Partition_2 y 10.102.216.49-Partition_3 de Citrix ADC y a este grupo.

Una vez creada la partición de administración, también puede utilizar la función de diferencia en el historial de revisiones y la función plantilla de auditoría para la partición de administración con fines de auditoría para fines de auditoría.

**La diferencia**del historial de revisiones para la partición de administración le permite ver la diferencia entre los cinco archivos de configuración más recientes de una instancia de Citrix ADC particionada. Puede comparar los archivos de configuración entre sí (por ejemplo, la revisión de configuración 1 con la revisión de configuración -2) o con la configuración actual en ejecución o guardada con la revisión de configuración. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. Puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

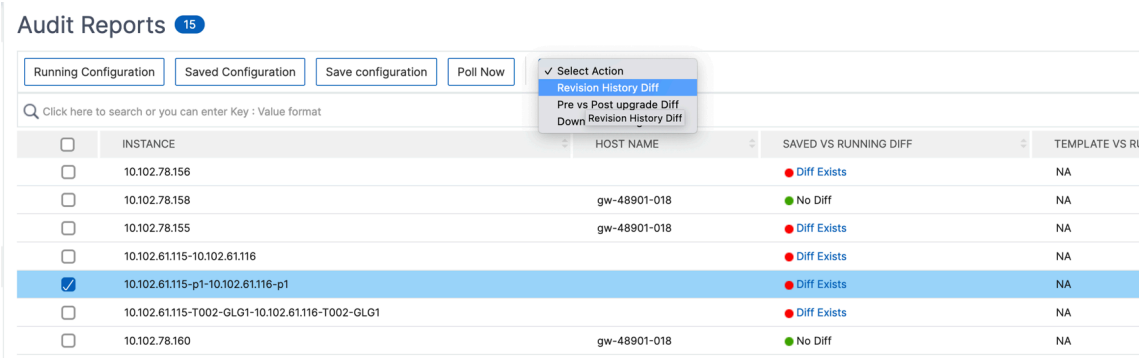
**Para ver la diferencia en el historial de revisiones:**

1. Vaya a **Redes > Auditoría de configuración.** Haga clic dentro del gráfico de donut que representa el estado de configuración de instancia. En la página **Informes de auditoría** que se abre, haga clic en la instancia de NetScaler ADC particionada.

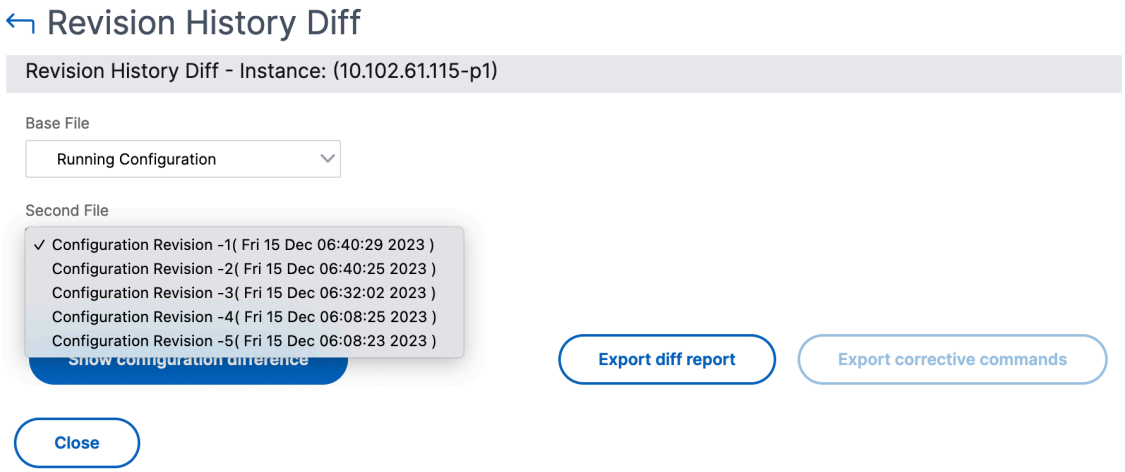



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En el menú **Acción**, haga clic en Diferencia del **historial de revisiones.**

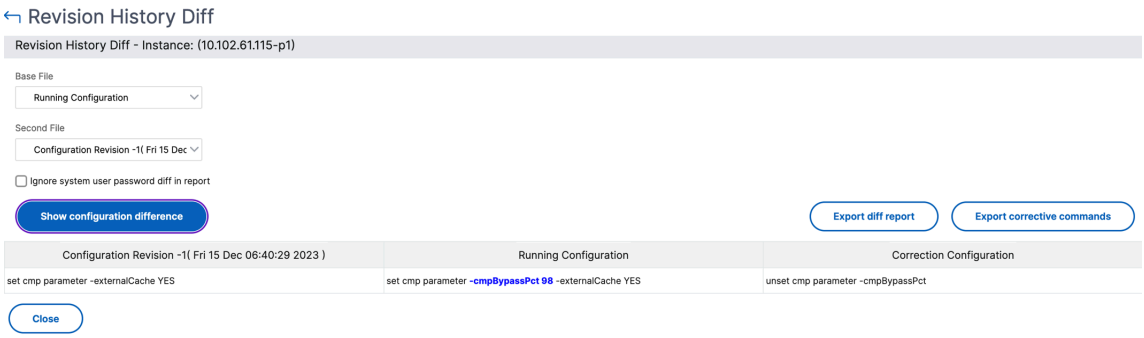



3. En la página **Diferencia del historial de revisiones**, seleccione los archivos que quiere comparar. Por ejemplo, compare la configuración guardada con la revisión de configuración -1 y, a continuación, haga clic en **Mostrar diferencia de configuración**.




4. A continuación, puede ver la diferencia entre los cinco archivos de configuración más recientes para la instancia de NetScaler ADC con particiones seleccionada, como se muestra a continuación. También puede ver los comandos de configuración correctiva y exportar estos comandos correctivos a la carpeta local. Estos comandos correctivos son los comandos que deben ejecutarse en el archivo base para obtener la configuración al estado deseado (archivo de configuración que se está utilizando para la comparación).

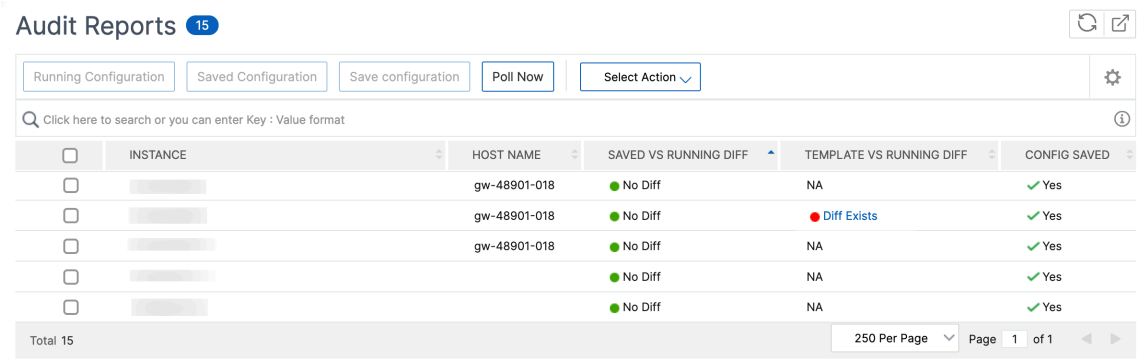
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Las plantillas de auditoría para partición** le permiten crear una plantilla de configuración personalizada y asociarla a una instancia de partición. Cualquier variación en la configuración en ejecución de la instancia con la plantilla de auditoría se muestra en la columna **Diferencia entre plantilla y ejecución** de la página **Informes de auditoría**. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. También puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

**Para ver la plantilla frente a la diferencia de ejecución:**

1. En la página **Informes de auditoría**, haga clic en la instancia de NetScaler ADC con particiones.




2. Si hay alguna diferencia entre la plantilla de auditoría y la diferencia en ejecución, la diferencia se muestra como un hipervínculo. Haga clic en el hipervínculo para ver las diferencias si las hay. Junto con las diferencias de configuración, también se muestran las configuraciones de corrección. También puede exportar todos los comandos correctivos a su carpeta local y corregir las configuraciones.

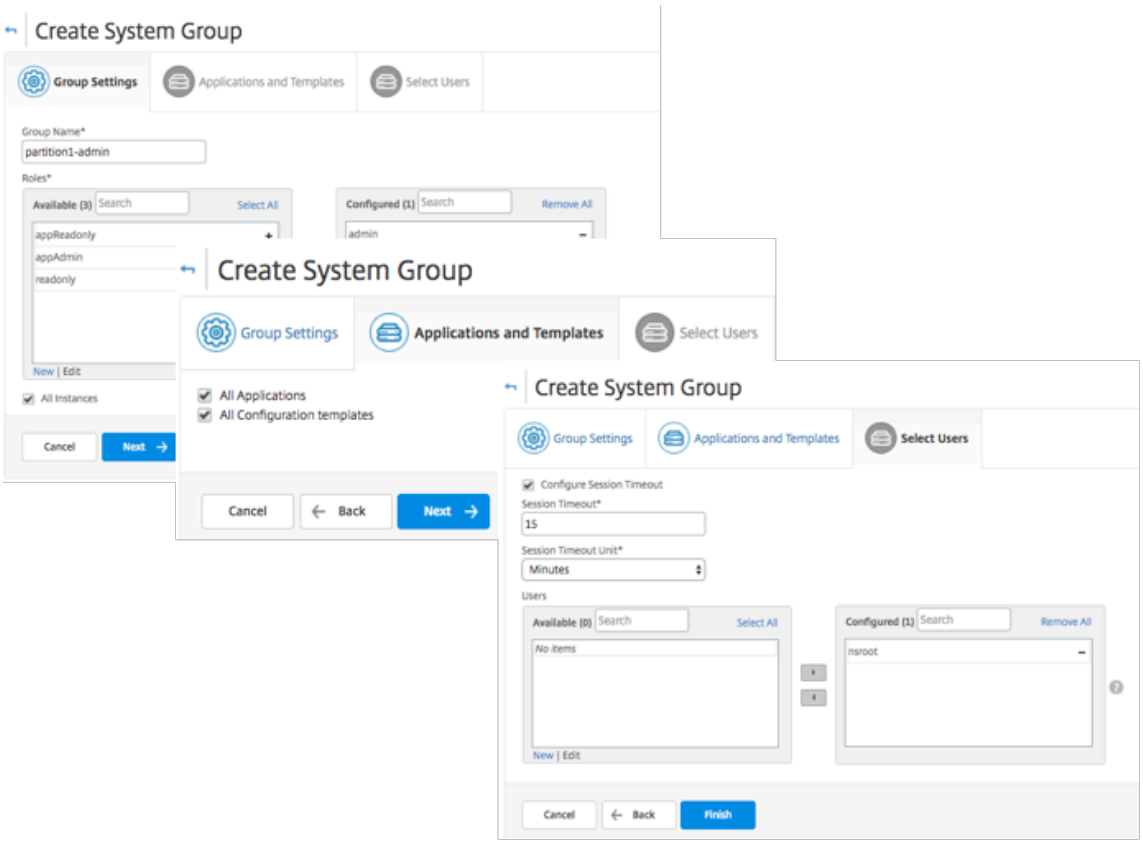
**Para crear grupos:**

1. Vaya a **Sistema > Administración de usuarios > Grupos**y, a continuación, haga clic en **Agregar**.
2. En la página **Crear Usuario del Sistema**, especifique lo siguiente:
   - Ficha **Configuración de grupo**: Introduzca el nombre del grupo y los permisos de rol. Para permitir el acceso a instancias específicas, desactive la casilla**Todas las instancias**y, a continuación, seleccione sus instancias en la página **Seleccionar instancias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Pestaña**Aplicaciones y plantillas**: Puede optar por utilizar este grupo en todas las aplicaciones y plantillas de configuración.
- **Seleccione la ficha Usuarios**: Seleccione los usuarios que desee agregar a este grupo. Puede hacer clic en el vínculo **Nuevo** de la tabla **Disponible** para crear nuevos usuarios. Opcionalmente, configure el tiempo de espera de la sesión, donde puede configurar el período de tiempo durante el tiempo que un usuario puede permanecer activo.

3. Haga clic en **Finalizar**.




**Para crear usuarios:**

1. Vaya a**Sistema > Administración de usuarios > Usuarios**y, a continuación, haga clic en **Agregar**.
2. En la página**Crear usuario del sistema**, especifique el nombre de usuario y la contraseña. Si lo desea, puede habilitar la autenticación externa y configurar el tiempo de espera de la sesión.
3. Asigne el usuario a un grupo añadiendo el nombre del grupo de la lista**Disponible**a la lista**Configurada**.
4. Haga clic en **Create**.

Ahora cierre sesión e inicie sesión con las credenciales user-p1. Puede ver y administrar solo las particiones de administración que se le asignaron para administrarlas y supervisarlas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Crear un par de alta disponibilidad de NetScaler ADC

January 24, 2024

Un par de alta disponibilidad (HA) de Citrix ADC puede proporcionar un funcionamiento ininterrumpido durante el tiempo de inactividad o los fallos de red. Puede crear un par de instancias de ADC de alta disponibilidad mediante NetScaler ADM. Para obtener más información, consulte Alta disponibilidad de NetScaler ADC.

Realice los siguientes pasos para crear un par de instancias de ADC de alta disponibilidad en NetScaler ADM:

1. Vaya a **Redes > Instancias > Citrix ADC** .
2. Seleccione una instancia ADC de la lista con la que quiere crear un par HA.

   La instancia seleccionada se convierte en la instancia principal del par HA.
3. Haga clic en Seleccionar **acción > Crear par HA**.
4. En **Selección de instancias**, realice los siguientes pasos:

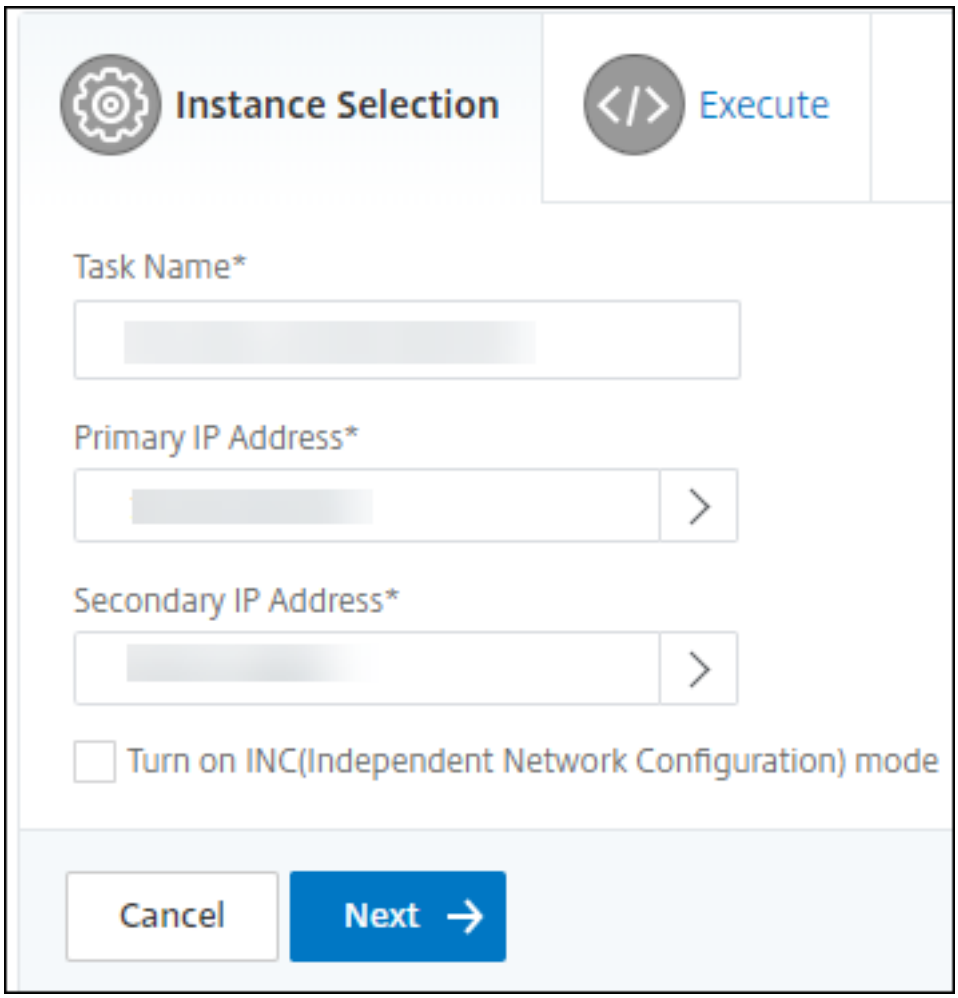
   a) En **Dirección IP secundaria**, haga clic para seleccionar una instancia secundaria.

   b) Seleccione una instancia de ADC que desee configurar como secundaria en el par HA.

   c) Si lo desea, seleccione **Activar el modo INC (Configuración de red independiente)** si tiene las instancias del par HA en dos subredes.

   d) Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. En **Execute**, puede decidir crear un par HA ahora o más adelante.

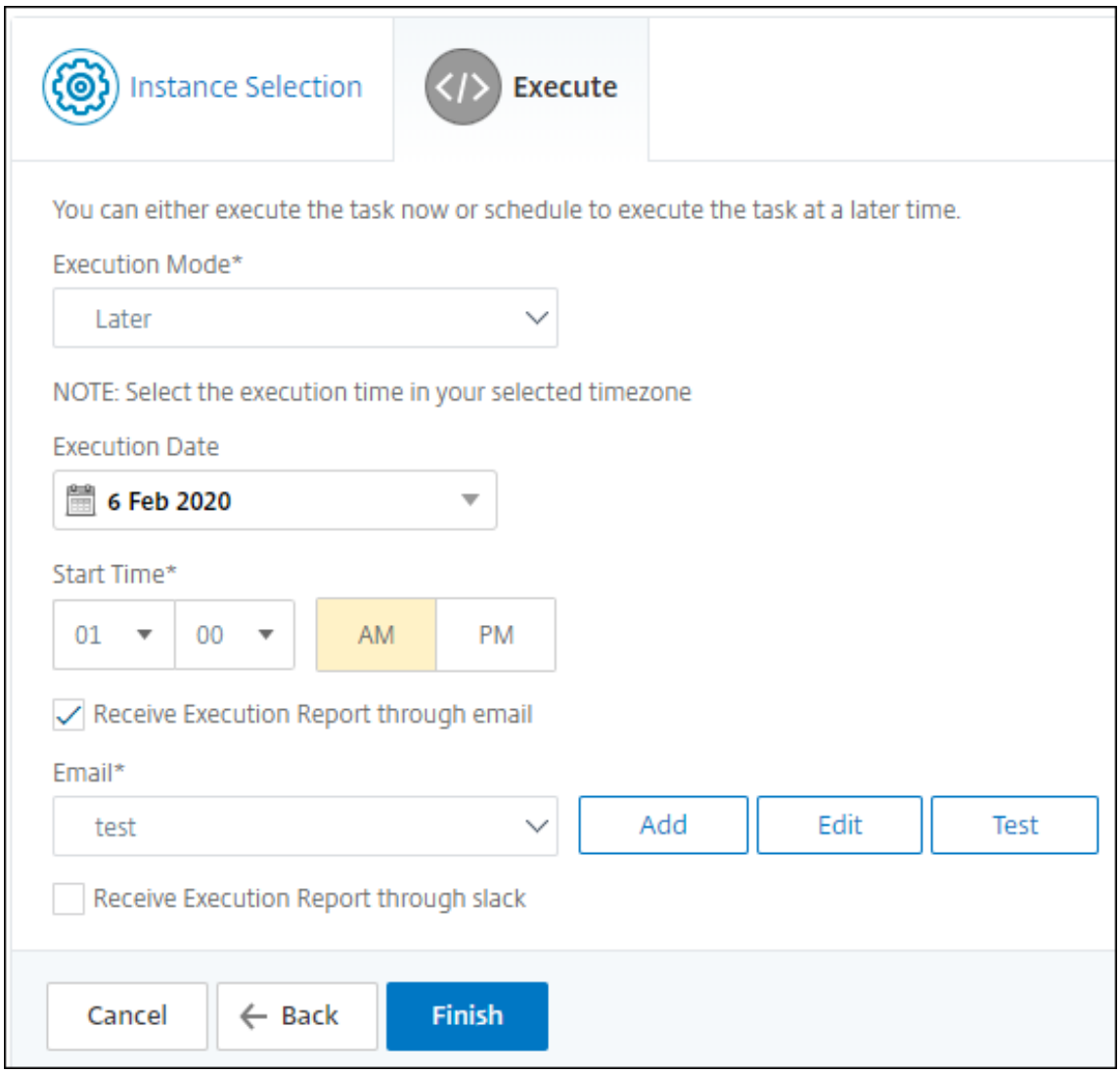
   a) En **Modo de ejecución**, seleccione uno de los siguientes modos de ejecución:

      - **Ahora**: Seleccione esta opción para crear un par HA ahora.
      - **Más adelante**: Seleccione esta opción para crear un par HA en una fecha y hora específicas.

   b) Si ha seleccionado **Más tarde** en la lista **Modo de ejecución**, seleccione **Fecha de ejecución** y **Hora de inicio** cuando quiera ejecutar esta tarea.

      > **Nota**
      >
      > El tiempo de ejecución se muestra en la zona horaria establecida en NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Puede recibir un informe de ejecución de esta tarea a través de lo siguiente:

- **Correo electrónico**: Seleccione la distribución del correo electrónico de la lista.

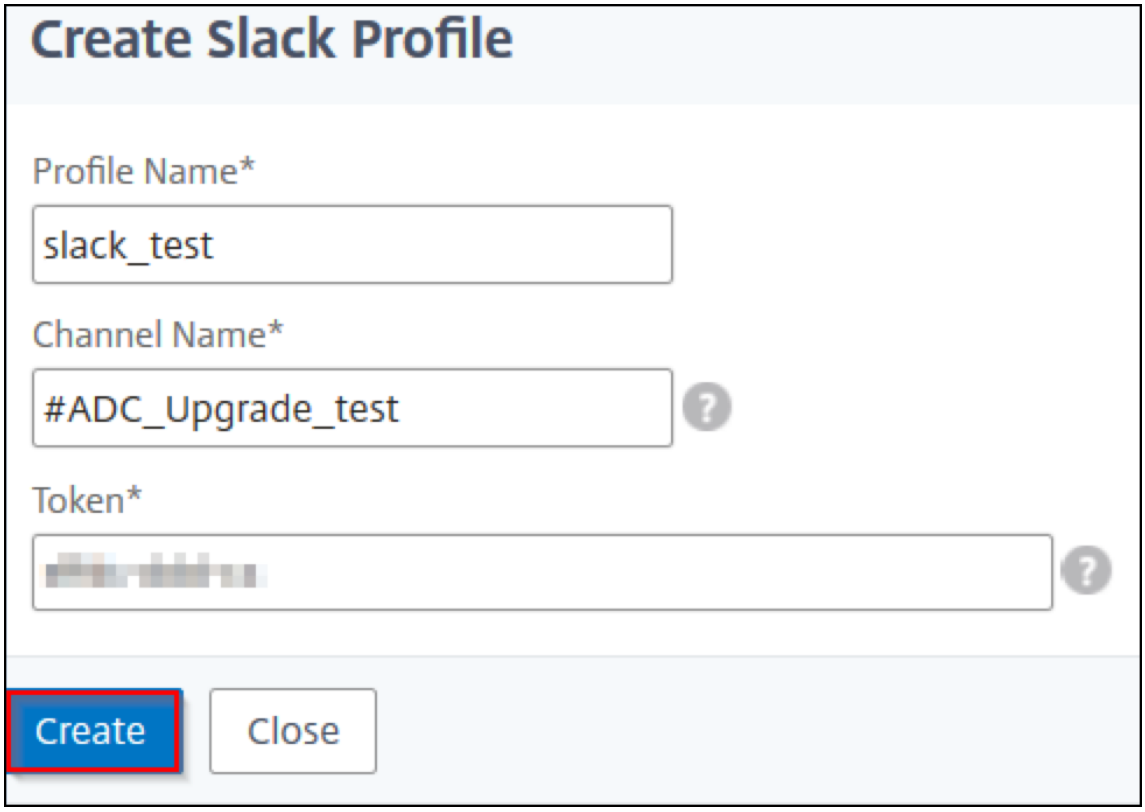
  Para agregar una lista de distribución, haga clic en **Agregar**. Especifique los parámetros necesarios para agregar la lista de distribución y haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Slack**: Selecciona el perfil de Slack de la lista.

  Para agregar un perfil de Slack, haga clic en **Agregar**. Especifique el **nombre del perfil**, **el nombre del canal**y el **token** y haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Realizar copias de seguridad y restaurar instancias de NetScaler ADC

January 30, 2024

Puede realizar una copia de seguridad del estado actual de una instancia de NetScaler ADC y posteriormente utilizar los archivos de copia de seguridad para restaurarla al mismo estado. Realice siempre una copia de seguridad de una instancia antes de actualizarla o por motivos de precaución. Una copia de seguridad de un sistema estable le permite restaurarlo a un punto estable si se vuelve inestable.

Existen varias formas de realizar copias de seguridad y restauraciones en una instancia de NetScaler ADC. Puede realizar copias de seguridad y restaurar manualmente las configuraciones de Citrix ADC mediante la GUI y la CLI. También puede utilizar Citrix ADM para realizar copias de seguridad automáticas y restauraciones manuales.

NetScaler ADM realiza una copia de seguridad del estado actual de las instancias de NetScaler ADC administradas mediante llamadas NITRO y los protocolos Secure Shell (SSH) y Secure Copy (SCP).

NetScaler ADM crea una copia de seguridad completa y restaura los siguientes tipos de instancias de NetScaler ADC:

- Citrix SDX

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Citrix VPX
- Citrix MPX
- Citrix BLX

Para obtener más información, consulte Realizar copias de seguridad y restaurar una instancia de ADC.

> **Nota**
>
> - Asegúrese de que el perfil Citrix ADM tenga acceso de administrador para realizar copias de seguridad y restaurar instancias de ADC.
> - Desde NetScaler ADM, no puede realizar la operación de copia de seguridad y restauración en un clúster de NetScaler ADC.
> - No puede usar el archivo de copia de seguridad tomado de una instancia para restaurar una instancia diferente.

Los archivos de copia de seguridad se almacenan como un archivo TAR comprimido en el siguiente directorio:

```
/var/mps/tenants/root/device_backup/
```

Para evitar problemas debido a la falta de disponibilidad de espacio en disco, puede guardar un máximo de 50 archivos de respaldo por instancia de ADC en este directorio.

Para realizar copias de seguridad y restaurar instancias de NetScaler ADC, primero debe configurar las opciones de copia de seguridad en NetScaler ADM. Tras configurar los parámetros, puede seleccionar una sola instancia de Citrix ADC o varias instancias y crear una copia de seguridad de los archivos de configuración en estas instancias. Si es necesario, también puede restaurar las instancias de Citrix ADC mediante estos archivos de copia de seguridad.

## Configurar las opciones de copia de seguridad de instancia

La página **Configuración de Copia de Seguridad de Instancia** permite configurar opciones en NetScaler ADM para realizar copias de seguridad de una instancia de NetScaler ADC seleccionada o varias instancias:

1. En Citrix ADM, vaya a **Sistema** > **Administración** .
2. En **Copia de seguridad**, seleccione **Configurar copia de seguridad del sistema y de la instancia**.
3. Seleccione **Instancia** y especifique lo siguiente:

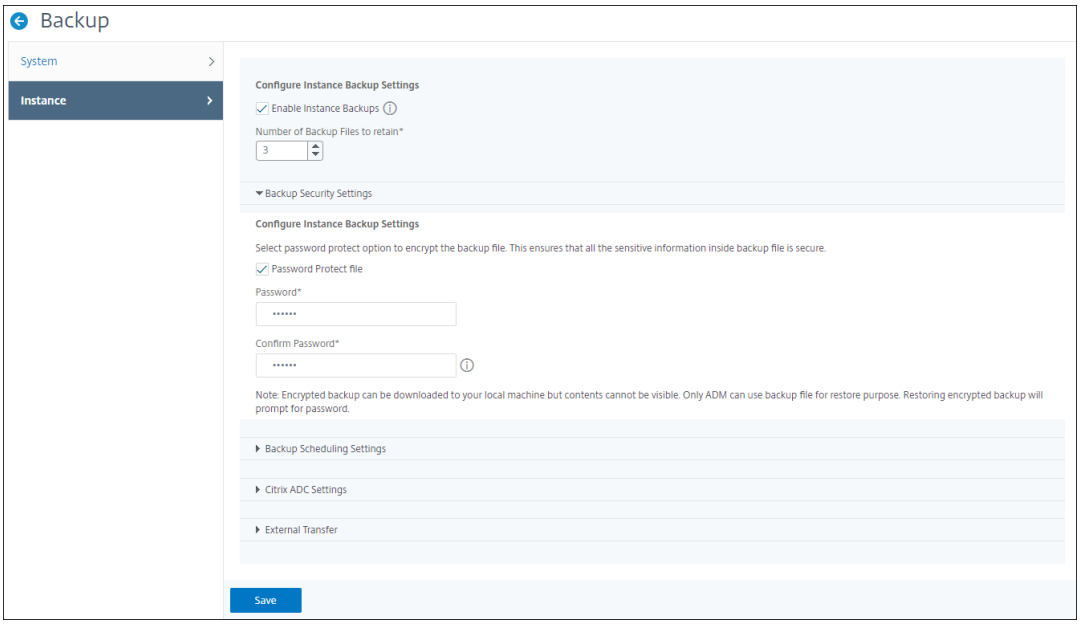
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Habilitar copias de seguridad de instancias**: De forma predeterminada, NetScaler ADM está habilitado para realizar copias de seguridad de instancias de NetScaler ADC. Desactive esta opción si no quiere crear archivos de respaldo para las instancias.
- **Archivo**protegido con contraseña : (opcional) Seleccione la opción de protección con contraseña para cifrar el archivo de respaldo. El cifrado del archivo de respaldo garantiza que toda la información confidencial del archivo de respaldo esté segura.

  > **Nota**
  >
  > Puede descargar el archivo de copia de seguridad cifrado en su equipo local, pero no puede abrirlo con NetScaler ADM GUI ni con ningún editor de texto. Se le pedirá que proporcione la contraseña al restaurar el archivo de copia de seguridad cifrado. Sin embargo, puede abrir un archivo de respaldo sin cifrar en su sistema.

- **Número de archivos de copia de seguridad que se deben conservar**: Especifique el número de archivos de copia de seguridad que se deben conservar en NetScaler ADM. Puede conservar hasta 50 archivos de respaldo por instancia de ADC. El valor predeterminado es tres archivos de copia de seguridad.

  > **Nota**
  >
  > Cada archivo de respaldo tiene en cuenta algunos requisitos de almacenamiento. Citrix recomienda almacenar un número óptimo de archivos de copia de seguridad de NetScaler ADC en NetScaler ADM según sus necesidades.



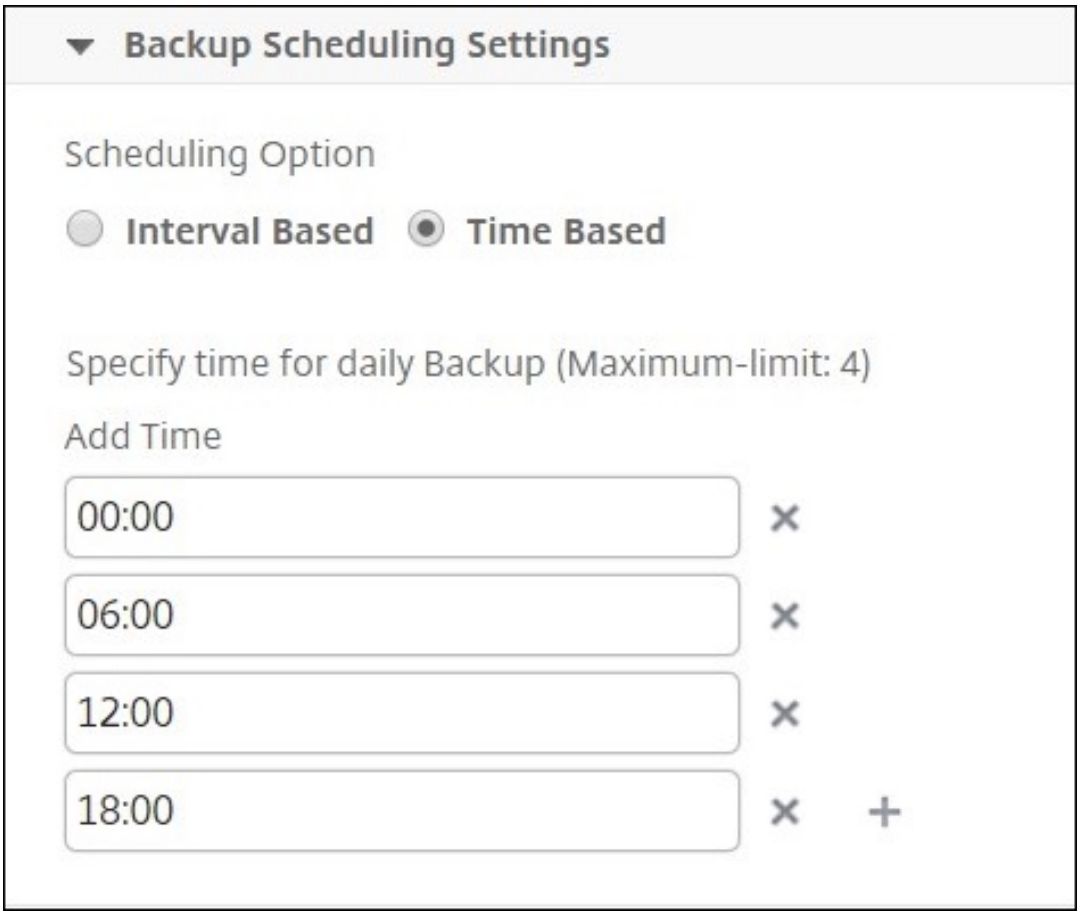

- **Configuración de programación de copias**de seguridad: (opcional) Hay dos opciones disponibles para crear archivos de copia de seguridad, aunque solo se puede utilizar una

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

opción a la vez:

a) La opción de programación de copias de seguridad predeterminada es “basada en intervalos”. Se crea un archivo de respaldo en Citrix ADM una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.

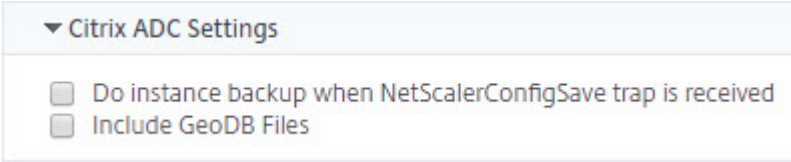
b) También puede cambiar el tipo de copias de seguridad programadas a “basadas en el tiempo. “En esta opción, especifique la hora en `hours:minutes` formato para realizar copias de seguridad de las instancias a la hora especificada. NetScaler ADM permite realizar un máximo de cuatro copias de seguridad diarias en las instancias.




- **Configuración de NetScaler ADC**: (opcional) De forma predeterminada, NetScaler ADM no crea un archivo de copia de seguridad cuando recibe la trampa “NetScalerConfigSave” . Sin embargo, puede habilitar la opción de crear un archivo de respaldo siempre que una instancia de Citrix ADC envíe una captura «NetScalerConfigSave» a Citrix ADM. Una instancia de Citrix ADC envía «NetScalerConfigSave» cada vez que se guarda la configuración de la instancia.

- **Archivos**de geodatabase : (opcional) De forma predeterminada, Citrix ADM no hace copias de seguridad de los archivos de geodatabase. Puede habilitar la opción de crear una copia de seguridad de estos archivos también.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- **Transferencia externa:**(opcional) NetScaler ADM le permite transferir los archivos de copia de seguridad de instancias de NetScaler ADC a una ubicación externa:

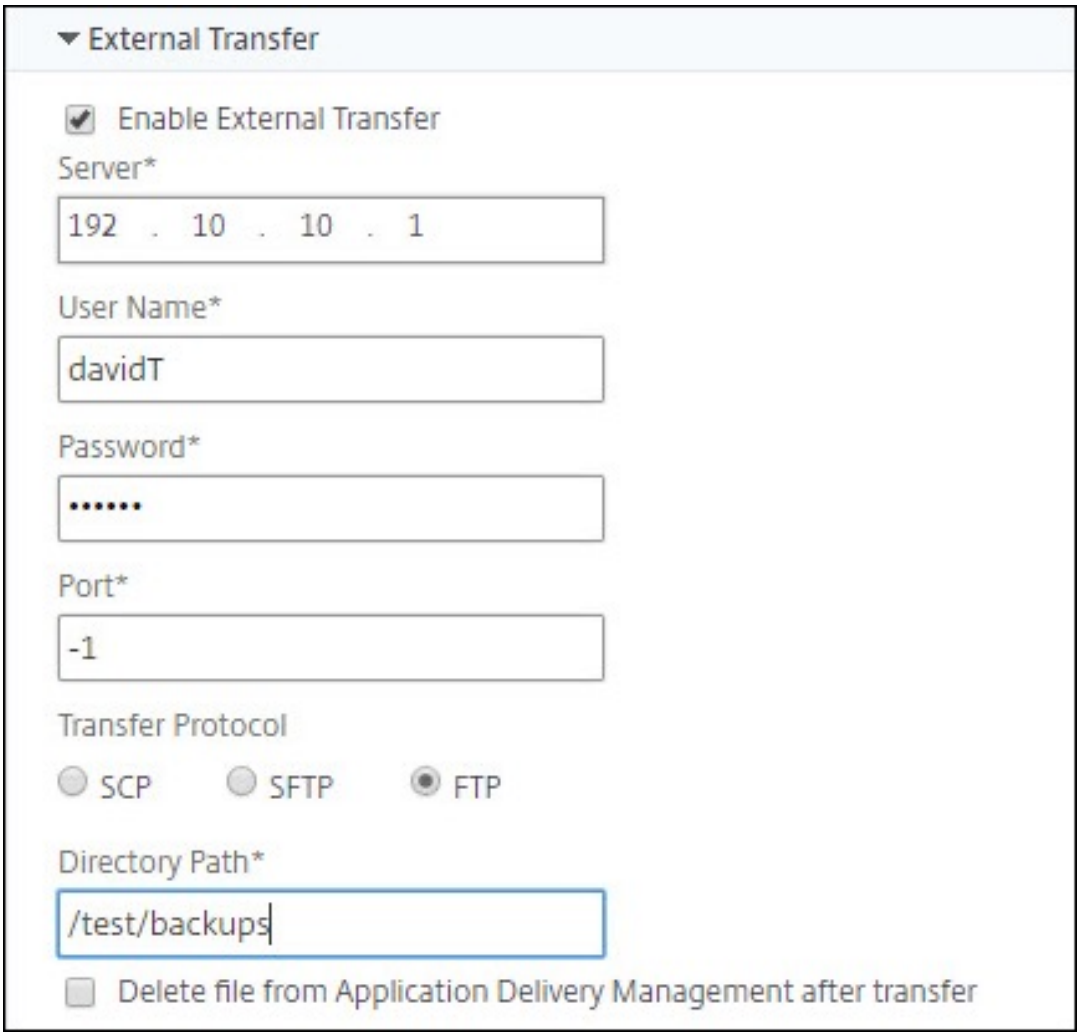
  a) Especifique la dirección IP de la ubicación.

  b) Especifique el nombre de usuario y la contraseña del servidor externo al que quiere transferir los archivos de copia de seguridad.

  c) Especifique el protocolo de transferencia y el número de puerto.

  d) Puede especificar la ruta del directorio donde debe almacenarse el archivo.

  e) Opcionalmente, también puede eliminar el archivo de copia de seguridad de Citrix ADM después de transferirlo al servidor externo.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Citrix ADM se envía una captura de SNMP o una notificación de Syslog cuando se produce un error de copia de seguridad en alguna de las instancias de Citrix ADC seleccionadas.

### Crear una copia de seguridad para una instancia de NetScaler ADC seleccionada mediante NetScaler ADM

Realice esta tarea si quiere realizar una copia de seguridad de una instancia de NetScaler ADC seleccionada o de varias instancias:

1. En Citrix ADM, vaya a **Redes** > **Instancias**. En**Instancias**, seleccione el tipo de instancias (por ejemplo, Citrix VPX) que quiere mostrar en la pantalla.
2. Seleccione la instancia de la que quiere realizar una copia de seguridad.
   - Para las instancias de MPX, VPX y BLX, seleccione **Respaldar/Restaurar** en la lista **Seleccionar acción**.
   - Para una instancia SDX, haga clic en **Copia de seguridad/restauración**.
3. En la página**Archivos de copia**de seguridad, haga clic en**Copia de**seguridad.
4. Puede especificar si quiere cifrar el archivo de copia de seguridad para obtener más seguridad. Puede introducir su contraseña o utilizar la contraseña global que especificó anteriormente en la página Configuración de copia de seguridad de instancias.
5. Haga clic en **Continuar**.

### Restaurar una instancia de NetScaler ADC con NetScaler ADM

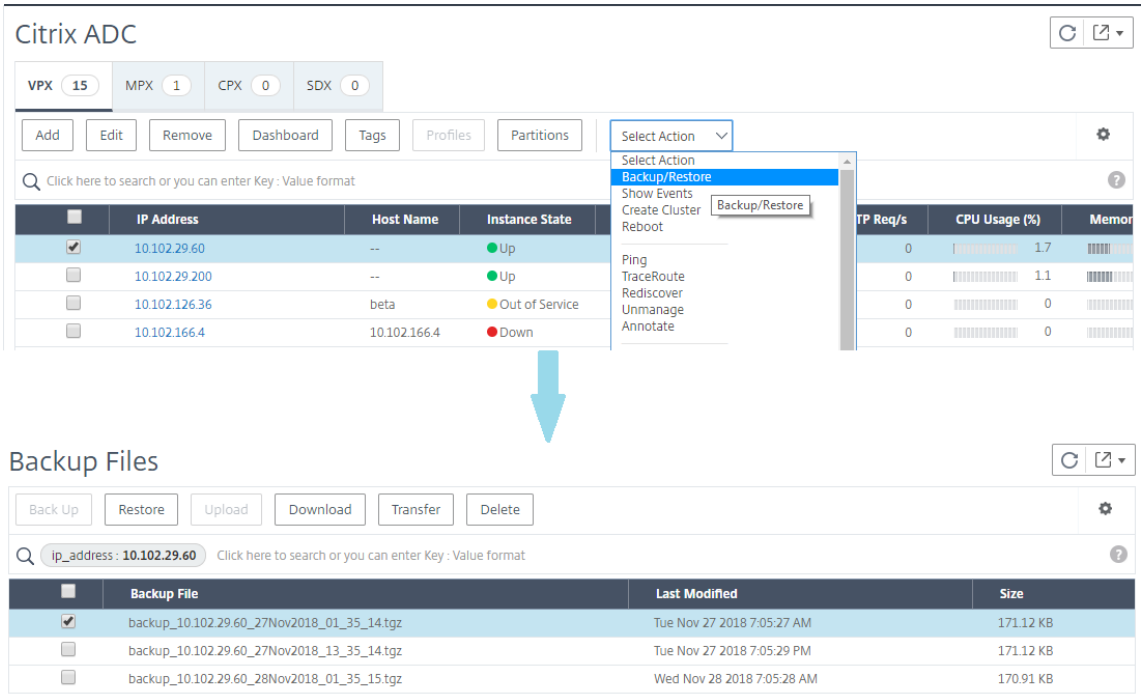
> Nota:
>
> Si tiene instancias de NetScaler ADC en un par HA, debe tener en cuenta lo siguiente:
>
> - Restaure la misma instancia desde la que se creó el archivo de copia de seguridad. Por ejemplo, consideremos un caso en el que se tomó una copia de seguridad de la instancia principal del par HA. Durante el proceso de restauración, asegúrese de restaurar la misma instancia, aunque ya no sea la instancia principal.
> - Al iniciar el proceso de restauración en la instancia de ADC principal, no puede acceder a la instancia principal y la instancia secundaria se cambia a **STAYSECONDARY**. Una vez que se completa el proceso de restauración en la instancia principal, la instancia de ADC secundaria pasa del modo **STAYSECONDARYal** modo ENABLED y vuelve a formar parte del par

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> HA. Puede esperar un posible tiempo de inactividad en la instancia principal hasta que se complete el proceso de restauración.

Realice esta tarea para restaurar una instancia de NetScaler ADC mediante el archivo de copia de seguridad que había creado anteriormente:

1. Vaya a **Redes** > **Instancias** , seleccione la instancia que desea restaurar y, a continuación, haga clic en Ver copia de **seguridad** .
2. En la página**Archivos de copia**de seguridad, seleccione el archivo de copia de seguridad que contiene la configuración que quiere restaurar y, a continuación, haga clic en**Restaurar**.




### Restaurar un dispositivo NetScaler ADC SDX con NetScaler ADM

En Citrix ADM, la copia de seguridad del dispositivo Citrix ADC SDX incluye lo siguiente:

- Instancias de NetScaler ADC alojadas en el dispositivo
- Certificados y claves SSL SVM
- Configuración de poda de instancias (en formato XML)
- Configuración de copia de seguridad de instancias (en formato XML)
- Configuración del sondeo de certificados SSL (en formato XML)
- Archivo SVM db
- Archivos de configuración NetScaler ADC de los dispositivos presentes en SDX
- Imágenes de creación de NetScaler ADC

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Imágenes de NetScaler ADC XVA, estas imágenes se almacenan en la siguiente ubicación: `/var/mps/sdx_images/`
- Imagen de paquete único de SDX (SVM+XS)
- Imágenes de instancias de terceros (si se aprovisionan)

Restaure el dispositivo Citrix ADC SDX a la configuración disponible en el archivo de respaldo. Durante la restauración del dispositivo, se elimina toda la configuración actual.

Si va a restaurar el dispositivo Citrix ADC SDX mediante una copia de seguridad de otro dispositivo Citrix ADC SDX, asegúrese de agregar las licencias y configurar los ajustes de red del Servicio de administración del dispositivo para que coincidan con los del archivo de respaldo antes de iniciar el proceso de restauración.

Antes de restaurar el dispositivo SDX, asegúrese de que la variante de plataforma del dispositivo SDX de la que se hizo la copia de seguridad sea la misma que la del dispositivo. No se puede restaurar desde una variante de plataforma diferente.

> **Nota**
>
> Antes de restaurar un dispositivo SDX RMA, asegúrese de que la versión de la copia de seguridad sea igual o superior a la versión de RMA.

Para restaurar el dispositivo SDX desde el archivo de copia de seguridad:

1. En la GUI de Citrix ADM, vaya a **Redes > Instancias > Citrix ADC** .
2. Haga clic en **Copia de seguridad/restauración**.
3. Selecciona el archivo de copia de seguridad de la misma instancia que deseas restaurar.
4. Haga clic en **Reempaquetar respaldo**.

   Cuando se realiza una copia de seguridad del dispositivo SDX, los archivos e imágenes XVA se almacenan por separado para ahorrar el ancho de banda de la red y el espacio en disco. Por lo tanto, debe volver a empaquetar el archivo de la copia de seguridad antes de restaurar el dispositivo SDX.

   Al volver a empaquetar el archivo de copia de seguridad, incluye todos los archivos de la copia de seguridad juntos para restaurar el dispositivo SDX. El archivo de copia de seguridad reempaquetado garantiza la restauración correcta del dispositivo SDX.
5. Seleccione el archivo de copia de seguridad que se ha reempaquetado y haga clic en **Restaurar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Forzar una conmutación por error a la instancia secundaria de NetScaler ADC

January 30, 2024

Es posible que desee forzar una conmutación por error si, por ejemplo, necesita reemplazar o actualizar la instancia principal de Citrix Application Delivery Controller (ADC). Puede forzar la conmutación por error desde la instancia principal o la instancia secundaria. Cuando se fuerza una conmutación por error en la instancia principal, la instancia principal se convierte en la secundaria y la secundaria en la principal. La conmutación por error forzada solo es posible cuando la instancia principal puede determinar que la instancia secundaria está activa.

Una conmutación por error forzada no se propaga ni sincroniza. Para ver el estado de la sincronización tras una conmutación por error forzada, puede ver el estado de la instancia.

Una conmutación por error forzada falla en cualquiera de las siguientes circunstancias:

- Se fuerza la conmutación por error en un sistema independiente.
- La instancia secundaria está inhabilitada o inactiva. Si la instancia secundaria se encuentra en un estado inactivo, debe esperar a que su estado sea ACTIVO para forzar una conmutación por error.
- La instancia secundaria está configurada para permanecer secundaria.

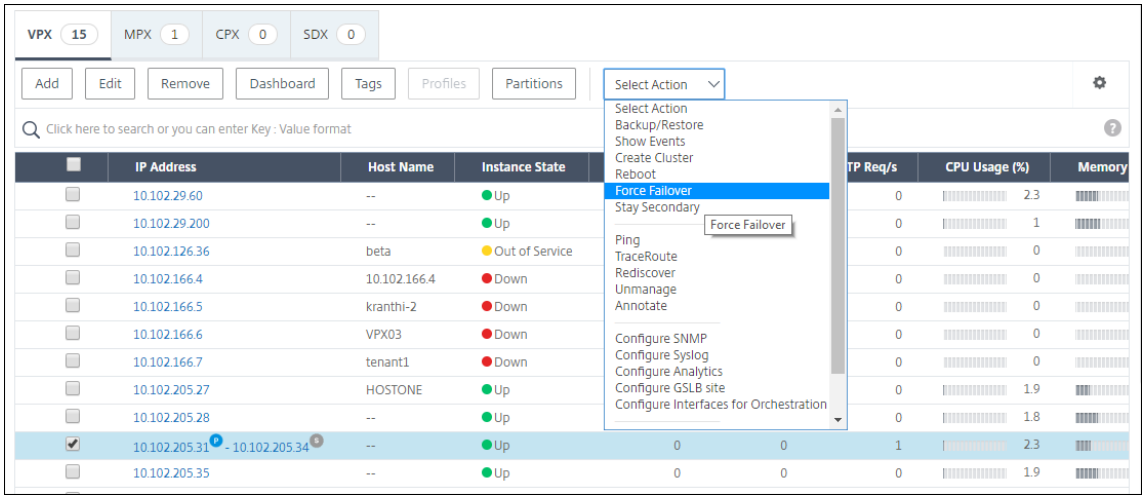
La instancia de NetScaler ADC muestra un mensaje de advertencia si detecta un posible problema al ejecutar el comando force failover. El mensaje incluye la información que activó la advertencia y solicita confirmación antes de continuar.

Puede forzar una conmutación por error en una instancia principal o secundaria.

**Para forzar una conmutación por error a la instancia secundaria de NetScaler ADC mediante NetScaler ADM:**

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes > Instancias > NetScaler ADC > ficha VPX** y, a continuación, seleccione una instancia.
2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el menú **Acción**, selecciona Forzar **la conmutación por error.**
4. Haga clic en **Sí** para confirmar la acción de conmutación por error forzada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Forzar una instancia secundaria de NetScaler ADC para que permanezca secundaria

January 30, 2024

En una configuración de HA, se puede obligar al nodo secundario a permanecer secundario independientemente del estado del nodo principal.

Por ejemplo, supongamos que el nodo principal necesita ser actualizado y el proceso tarda unos segundos. Durante la actualización, es posible que el nodo principal desaparezca durante unos segundos, pero no quiere que el nodo secundario asume el control. Desea que siga siendo el nodo secundario incluso si detecta un error en el nodo principal.

Cuando obliga al nodo secundario a permanecer secundario, seguirá siendo secundario incluso si el nodo principal se desactiva. Además, cuando se fuerza el estado de un nodo de un par de HA a permanecer secundario, no participa en las transiciones de la máquina de estado HA. El estado del nodo se muestra como STAYSECONDARY.

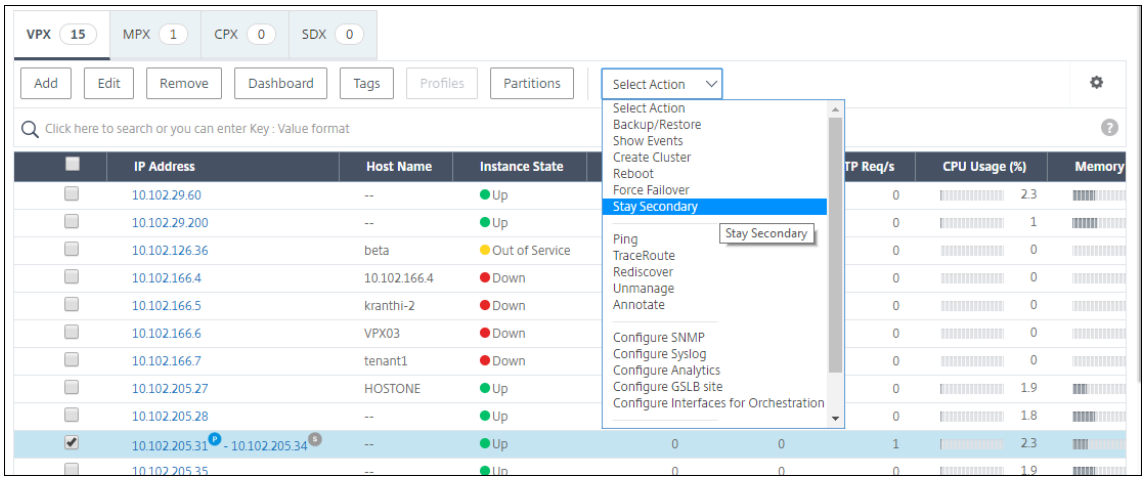
> **Nota**
>
> Cuando se fuerza a un sistema a permanecer secundario, el proceso de forzamiento no se propaga ni se sincroniza. Solo afecta al nodo en el que se ejecuta el comando.

**Para configurar una instancia secundaria de NetScaler ADC para que permanezca secundaria mediante NetScaler ADM:**

1. En Citrix Application Delivery Management (ADM), vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** y, a continuación, seleccione una instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Seleccione instancias en una configuración de alta disponibilidad de las instancias enumeradas en el tipo de instancia seleccionado.
3. En el menú **Acción**, seleccione **Permanecer secundario**.
4. Haga clic en **Sí** para confirmar la ejecución de la acción "Permanecer secundario".




## Crear grupos de instancias

January 30, 2024

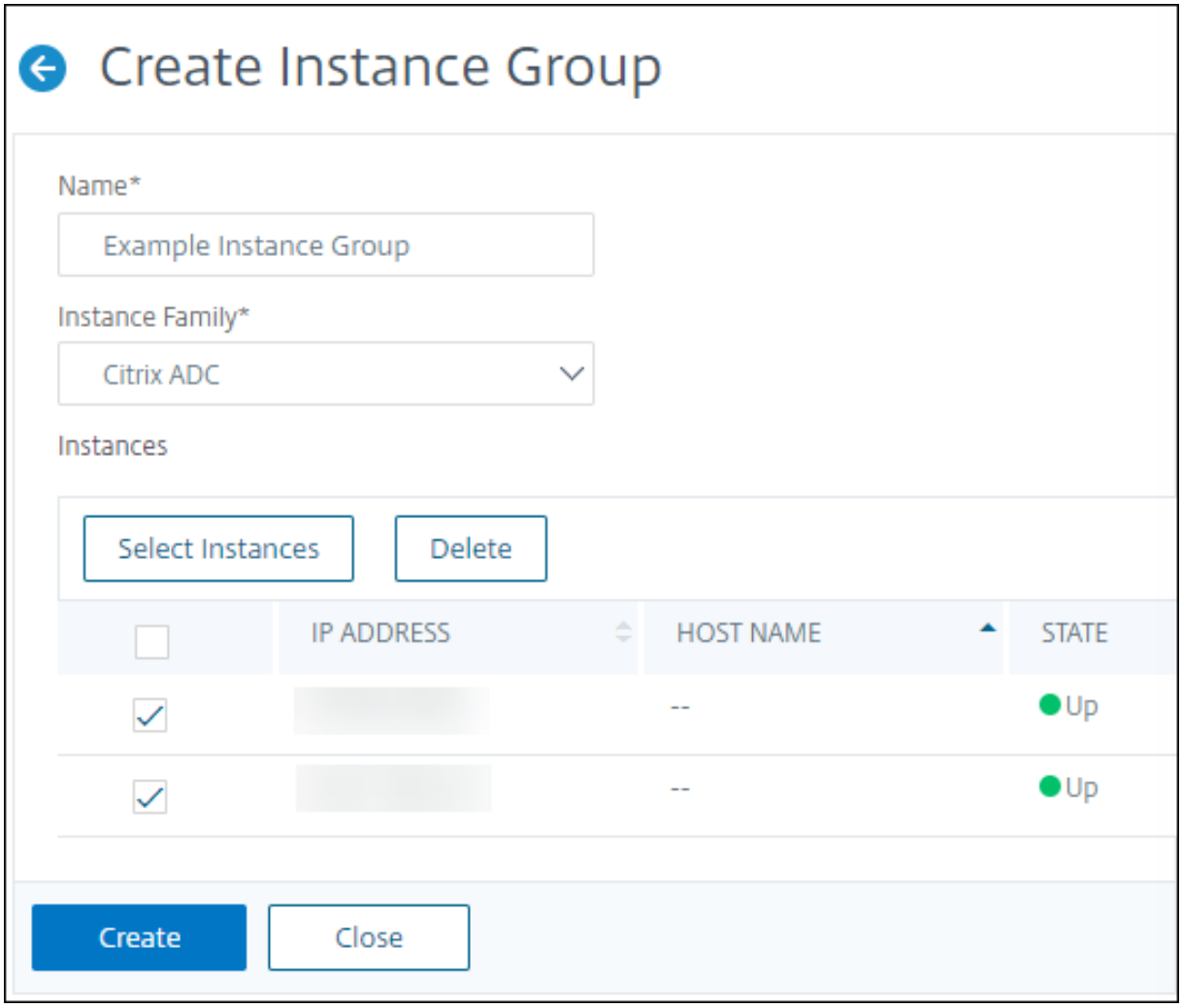
Para crear un grupo de instancias, primero debe agregar todas las instancias de NetScaler ADC a NetScaler ADM. Una vez que hayas agregado las instancias correctamente, crea grupos de instancias según su familia de instancias. La creación de un grupo de instancias le ayuda a actualizar, hacer copias de seguridad o restaurar las instancias agrupadas al mismo tiempo.

### Para crear un grupo de instancias con NetScaler ADM

1. En NetScaler ADM, vaya a **Redes** > **Grupos de instancias** y, a continuación, haga clic en **Agregar**.
2. Especifique un nombre para el grupo de instancias y seleccione **NetScaler ADC** en la lista **Familia de instancias**.
3. Haga clic en **Seleccionar instancias**. En la página **Seleccionar instancias**, seleccione las instancias que quiere agrupar y haga clic en **Seleccionar**.

   La tabla muestra las instancias seleccionadas y sus detalles. Si quieres eliminar alguna instancia del grupo, selecciona la instancia de la tabla y haz clic en **Eliminar** .
4. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Aprovisionar instancias VPX de ADC en SDX mediante ADM

January 30, 2024

Puede aprovisionar una o más instancias de ADC VPX en el dispositivo SDX mediante NetScaler ADM. El número de instancias que puede implementar depende de la licencia que haya adquirido. Si el número de instancias agregadas es igual al especificado en la licencia, ADM le impide aprovisionar más instancias de NetScaler ADC.

Antes de comenzar, asegúrese de agregar una instancia SDX en ADM donde quiera aprovisionar instancias VPX.

Para aprovisionar una instancia VPX, haga lo siguiente:

1. Vaya a **Redes > Instancias > Citrix ADC** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la ficha **SDX**, seleccione una instancia SDX en la que quiera aprovisionar una instancia VPX.
3. En **Seleccionar acción**, seleccione **Aprovisionar VPX**.

### Paso 1: Agregar una instancia VPX

El ADM utiliza la siguiente información para configurar instancias VPX en un dispositivo SDX:

- **Nombre**: especifique un nombre para una instancia de ADC.
- Establezca una red de comunicación entre SDX y VPX. Para ello, seleccione las opciones necesarias de la lista:
  - **Administrar a través de una red interna**: Esta opción establece una red interna para la comunicación entre el ADM y una instancia VPX.
  - **Dirección IP** : puede seleccionar una dirección **IPv4** o **IPv6** o ambas para administrar la instancia de Citrix VPX. Una instancia VPX solo puede tener una IP de administración (también denominada IP de NetScaler ADC). No puede quitar la dirección IP de NetScaler ADC.

    Para la opción seleccionada, asigne una máscara de red, una puerta de enlace predeterminada y un salto siguiente al servidor ADM para la dirección IP.
- **Archivo XVA**: Seleccione el archivo XVA desde el que quiere aprovisionar una instancia VPX. Utilice una de las siguientes opciones para seleccionar el archivo XVA.
  - **Local**: seleccione el archivo XVA de su equipo local.
  - **Dispositivo**: Seleccione el archivo XVA en un explorador de archivos ADM.
- **Perfil de administrador**: este perfil proporciona acceso para aprovisionar instancias VPX. Con este perfil, ADM recupera los datos de configuración de una instancia. Si tiene que agregar un perfil, haga clic en **Agregar**.
- **Agente**: Seleccione el agente al que quiere asociar las instancias
- **Sitio**: Seleccione el sitio donde quiere agregar la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Name*

example-instance-on-sdx

☑ Manage through internal network

☑ IPv4

IPv4 Address*

10 . 10 . 10 . 10

Netmask*

255 . 255 . 255 . 0

Gateway

10 . 0 . 0 . 1

Nexthop to Management Service

10 . 0 . 0 . 2

☐ IPv6

XVA File*

Choose File | NSVPX-XEN-10.1-118.7_nc.xva

Admin Profile*

ns_nsroot_profile | Add

Agent*

12.0.9.250

Site*

9k0p84w86lxn_default

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Paso 2: Asignar licencias

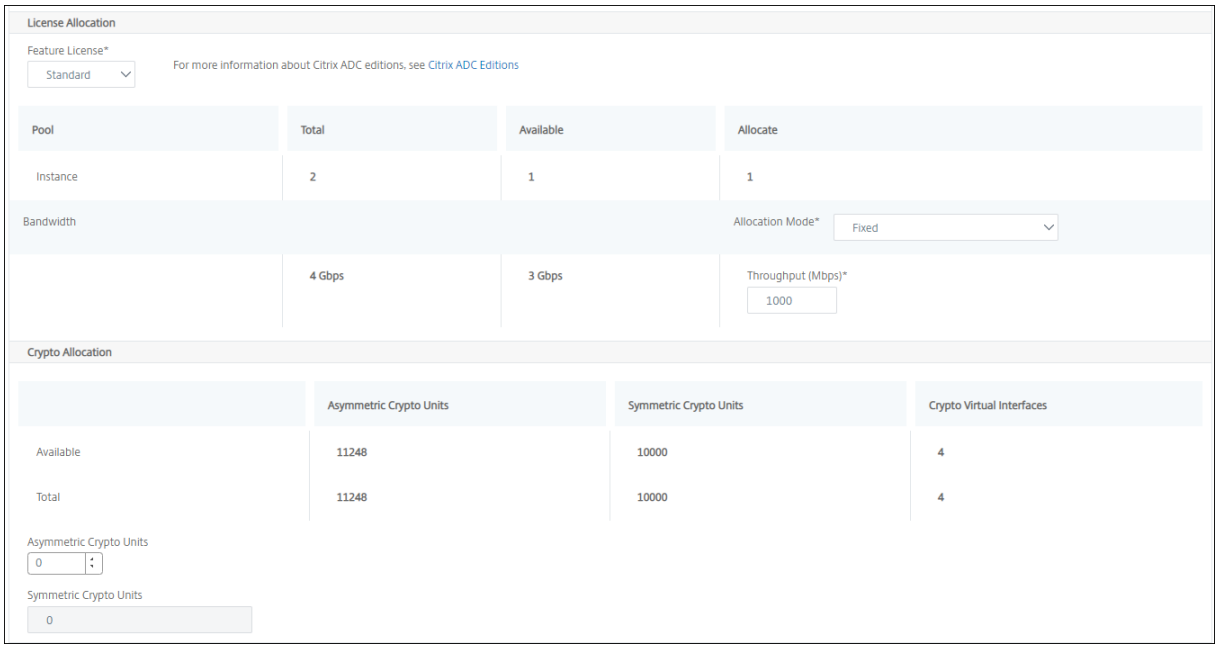
En la sección **Asignación de licencias**, especifique la licencia VPX. Puede utilizar las licencias Standard, Advanced y Premium.

- **Modo de asignación**: puede elegir los modos **fijo** o de **ráfaga** para el conjunto de ancho de banda.

  Si elige el modo **Burstable**, puede usar ancho de banda adicional cuando se alcanza el ancho de banda fijo.

- **Rendimiento**: asigne el rendimiento total (en Mbps) a una instancia.

> **Nota**
>
> Compre una licencia independiente (SDX 2-Instance Add-On Pack para Secure Web Gateway) para instancias de Citrix Secure Web Gateway (SWG) en dispositivos SDX. Este paquete de instancias es diferente de la licencia de plataforma SDX o del paquete de instancias SDX.
>
> Para obtener más información, consulte Implementación de una instancia de Citrix Secure Web Gateway en un dispositivo SDX.




A partir de la versión 12.0 57.19 de SDX, la interfaz para administrar la capacidad de cifrado ha cambiado. Para obtener más información, consulte Administrar la capacidad de cifrado.

### Paso 3: Asignar recursos

En la sección **Asignación de recursos**, asigne recursos a una instancia VPX para mantener el tráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

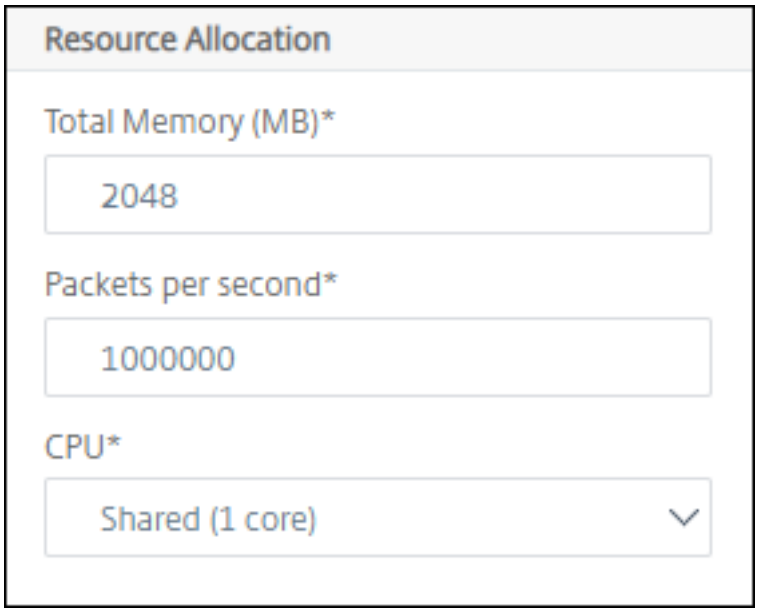
- **Memoria total (MB)**: asigna la memoria total a una instancia. El valor mínimo es 2048 MB.
- **Paquetes por segundo**: especifique la cantidad de paquetes que se van a transmitir por segundo.
- **CPU**: especifique el número de núcleos de CPU de una instancia. Puede utilizar núcleos de CPU compartidos o dedicados.

  Cuando selecciona un núcleo compartido para una instancia, las demás instancias pueden utilizar el núcleo compartido en el momento de escasez de recursos.

  Reinicie instancias en las que se reasignan núcleos de CPU para evitar cualquier degradación del rendimiento.

  Si utiliza la plataforma SDX 25000xx, puede asignar un máximo de 16 núcleos a una instancia. Además, si utiliza la plataforma SDX 2500xxx, puede asignar un máximo de 11 núcleos a una instancia.

  > **Nota**
  >
  > Para una instancia, el rendimiento máximo que se configura es de 180 Gbps.




En la siguiente tabla se enumeran las versiones de VPX admitidas, la imagen de un solo paquete y el número de núcleos que puede asignar a una instancia:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre de la plataforma | Núcleos totales | Total de núcleos disponibles para el aprovisionamiento de VPX | Núcleos máximos que se pueden asignar a una única instancia |
|---|---|---|---|
| SDX 8015, SDX 8400 y SDX 8600 | 4 | 3 | 3 |
| SDX 8900 | 8 | 7 | 7 |
| SDX 11500, SDX 13500, SDX 14500, SDX 16500, SDX 18500 y SDX 20500 | 12 | 10 | 5 |
| SDX 11515, SDX 11520, SDX 11530, SDX 11540 y SDX 11542 | 12 | 10 | 5 |
| SDX 17500, SDX 19500 y SDX 21500 | 12 | 10 | 5 |
| SDX 17550, SDX 19550, SDX 20550 y SDX 21550 | 12 | 10 | 5 |
| SDX 14020, SDX 14030, SDX 14040, SDX 14060, SDX 14080 y SDX 14100 | 12 | 10 | 5 |
| SDX 22040, SDX 22060, SDX 22080, SDX 22100 y SDX 22120 | 16 | 14 | 7 |
| SDX 24100 y SDX 24150 | 16 | 14 | 7 |
| SDX 14020 40G, SDX 14030 40G, SDX 14040 40G, SDX 14060 40G, SDX 14080 40G y SDX 14100 40G | 12 | 10 | 10 |
| SDX 14020 FIPS, SDX 14030 FIPS, SDX 14040 FIPS, SDX 14060 FIPS, SDX 14080 FIPS y SDX 14100. FIPS | 12 | 10 | 5 |
| SDX 14040 40S, SDX 14060 40S, SDX 14080 40S y SDX 14100 40S | 12 | 10 | 5 |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre de la plataforma | Núcleos totales | Total de núcleos disponibles para el aprovisionamiento de VPX | Núcleos máximos que se pueden asignar a una única instancia |
|---|---|---|---|
| SDX 25100A, 25160A, 25200A | 20 | 18 | 9 |
| SDX 25100-40G, 25160-40G, 25200-40G | 20 | 18 | 16 (si la versión es 11.1-51.x o superior); 9 (si la versión es 11.1-50.x o inferior; todas las versiones de 11.0 y 10.5) |
| SDX 26100, 26160, 26200, 26250 | 28 | 26 | 13 |
| 15000-50G | 16 | 14 | 7 |

> **Nota**
>
> En la plataforma SDX 26xxx, se puede asignar un máximo de 26 núcleos de CPU a una instancia VPX. Si se asignan unidades criptográficas a la instancia, el número máximo de núcleos depende del número de unidades criptográficas e interfaces de datos.
>
> Por ejemplo, si asigna 24000 unidades criptográficas a una instancia, puede asignar 24 núcleos de CPU y un máximo de dos interfaces de datos a la instancia. El dispositivo SDX considera las interfaces de datos y las unidades criptográficas como dispositivos PCI. Para las unidades criptográficas 26000, el aprovisionamiento de instancias VPX falla debido a que no hay espacio para agregar interfaces de datos.

### Paso 4: Agregar la administración de instancias

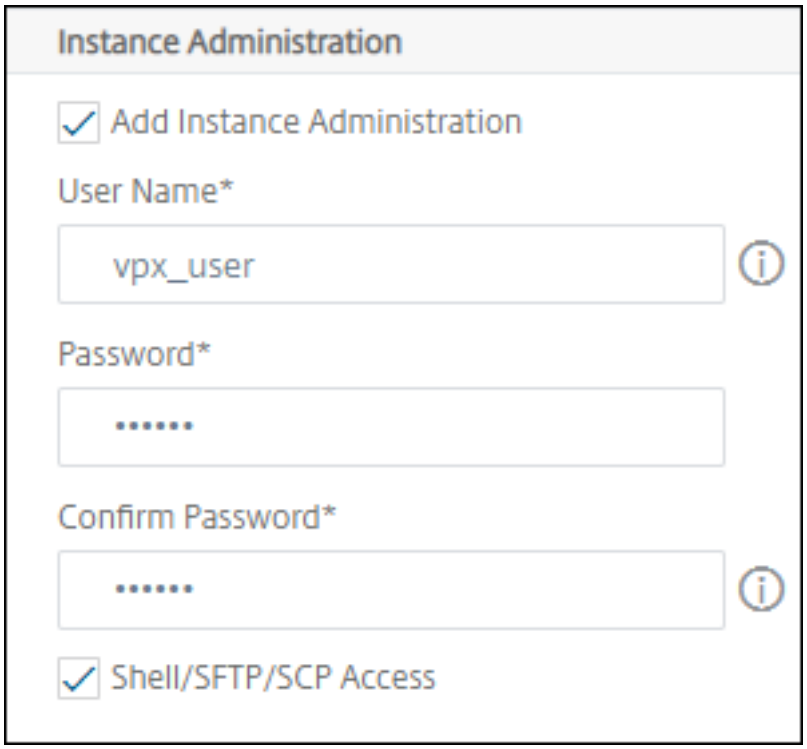
Puede crear un usuario administrador para la instancia VPX. Para ello, seleccione **Agregar administración de instancia** en la sección **Administración de instancias**.

Especifique los siguientes detalles:

- **Nombre**de usuario : nombre de usuario del administrador de instancias de Citrix ADC. Este usuario tiene acceso de superusuario, pero no tiene acceso a comandos de red para configurar VLAN e interfaces.
- **Contraseña**: especifique la contraseña del nombre de usuario.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Acceso a Shell/Sftp/Scp:**el acceso permitido al administrador de instancias de Citrix ADC. Esta opción está seleccionada de forma predeterminada.




### Paso 5: Especificar la configuración de red

Seleccione la configuración de red requerida para una instancia:

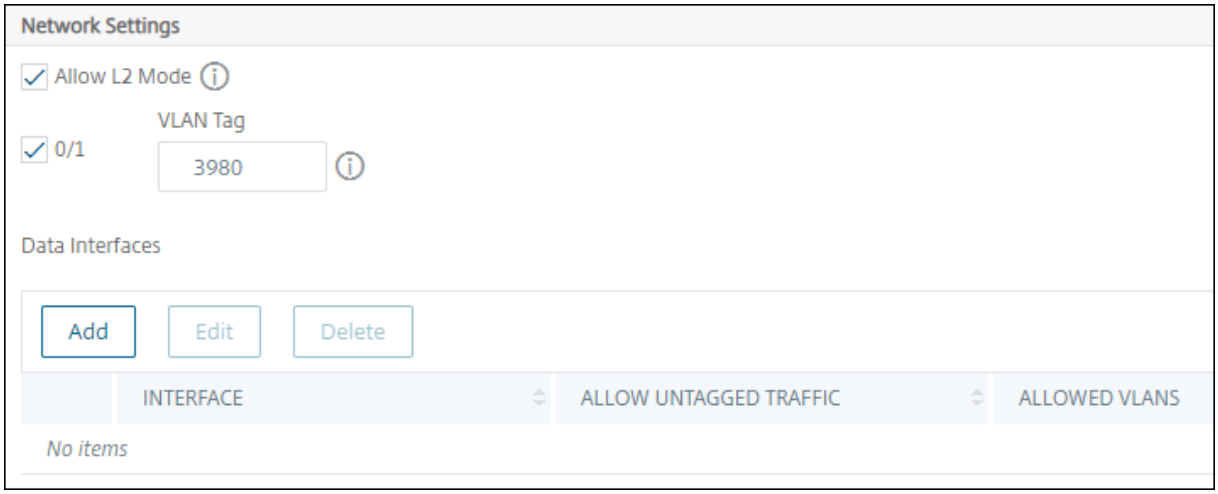
- **Permitir el modo L2 en la configuración de red**: puede permitir el modo L2 en la instancia de NetScaler ADC. Seleccione Permitir el modo L2 en Configuración de red. Antes de iniciar sesión en la instancia y habilitar el modo L2. Para obtener más información, consulte Permitir el modo L2 en una instancia de Citrix ADC.

  > **Nota**
  >
  > Si inhabilita el modo L2 para una instancia, debe iniciar sesión en la instancia e inhabilitar el modo L2 desde esa instancia. De lo contrario, podría provocar que todos los demás modos de NetScaler ADC se desactiven después de reiniciar la instancia.

- **0/1**: en **la etiqueta VLAN**, especifique un ID de VLAN para la interfaz de administración.
- **0/2**: en **la etiqueta VLAN**, especifique un ID de VLAN para la interfaz de administración.

De forma predeterminada, se seleccionan las interfaces **0/1** y **0/2**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En **Interfaces de datos**, haga clic en **Agregar** para agregar interfaces de datos y especifique lo siguiente:

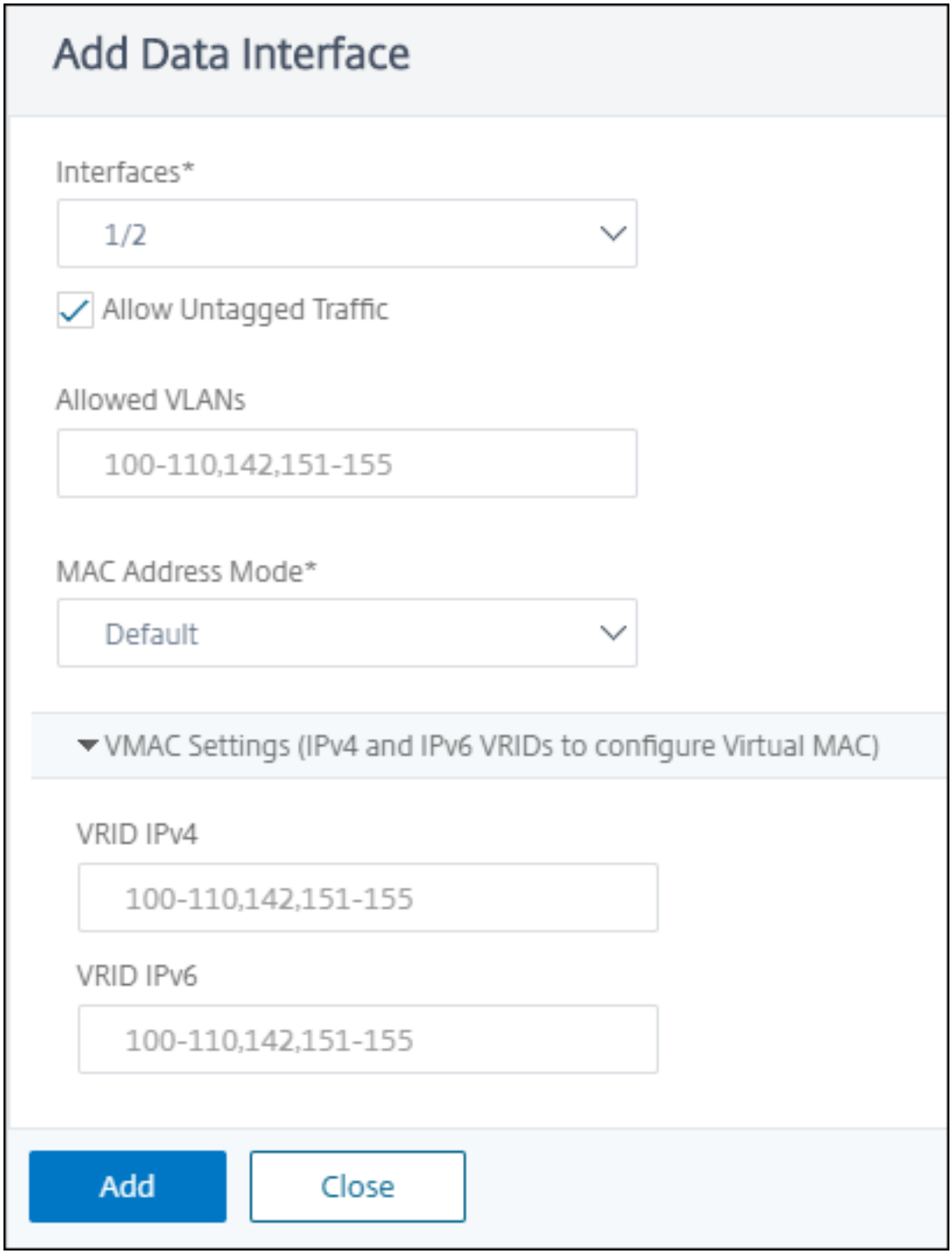
- **Interfaces**: seleccione la interfaz de la lista.

  > **Nota**
  >
  > Los identificadores de interfaz de las interfaces que se agregan a una instancia no se corresponden necesariamente con la numeración de la interfaz física en el dispositivo SDX.
  >
  > Por ejemplo, la primera interfaz que asocia con la instancia -1 es la interfaz SDX 1/4, aparece como interfaz 1/1 cuando ve la configuración de la interfaz en esa instancia. Esta interfaz indica que es la primera interfaz que asoció con instance-1.

- **VLAN permitidas**: especifique una lista de identificadores de VLAN que se pueden asociar a una instancia de NetScaler ADC.
- **Modo de dirección MAC**: asigna una dirección MAC a una instancia. Seleccione una de estas opciones:
  - **Predeterminado**: Citrix Workspace asigna una dirección MAC.
  - **Personalizado**: elija este modo para especificar una dirección MAC que anule la dirección MAC generada.
  - **Generado: Genera** una dirección MAC mediante la dirección MAC base establecida anteriormente. Para obtener información sobre cómo configurar una dirección MAC base, consulte Asignación de una dirección MAC a una interfaz.
- **Configuración de VMAC (VRID IPv4 e IPv6 para configurar Virtual MAC)**
  - **VRID IPV4**: el VRID de IPv4 que identifica el VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- VRID IPV6: el VRID IPv6 que identifica el VMAC. Valores posibles: 1-255. Para obtener más información, consulte Configuración de VMAC en una interfaz.




Haga clic en **Agregar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Paso 6 - Especificar la configuración de VLAN de administración

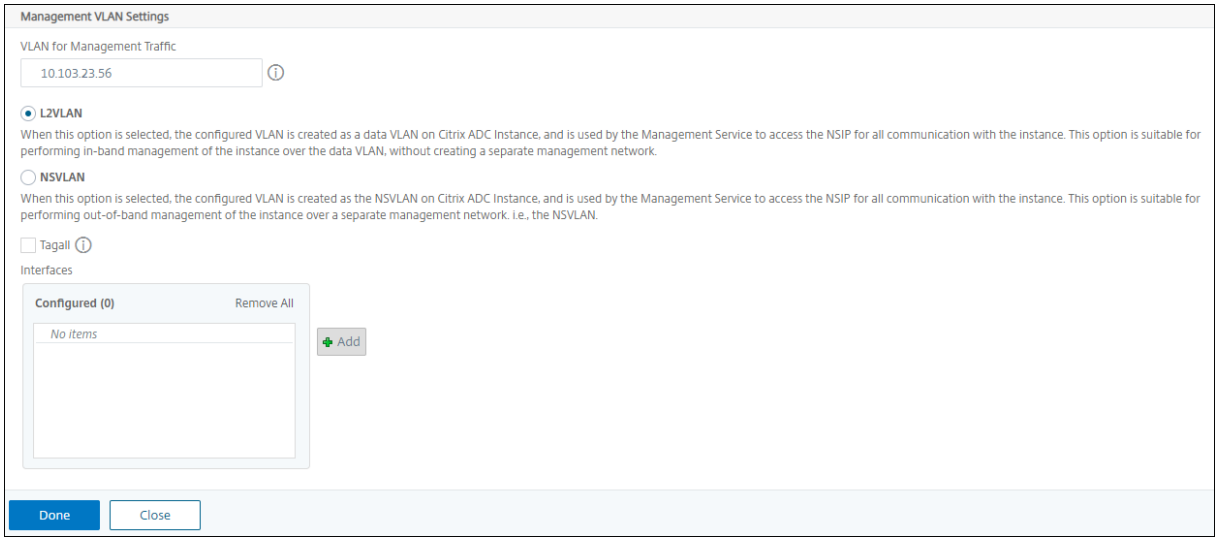
El Servicio de administración y la dirección de administración (NSIP) de la instancia VPX se encuentran en la misma subred y la comunicación se realiza a través de una interfaz de administración.

Si el Servicio de administración y la instancia se encuentran en subredes diferentes, especifique un ID de VLAN mientras aprovisione una instancia VPX. Por lo tanto, la instancia es accesible a través de la red cuando está activa.

Si su implementación requiere que solo se pueda acceder al NSIP a través de la interfaz seleccionada mientras se aprovisiona la instancia VPX, seleccione **NSVLAN**. Y, el NSIP se vuelve inaccesible a través de otras interfaces.

- Los latidos de HA se envían solo en las interfaces que forman parte de la NSVLAN.
- Puede configurar una NSVLAN solo desde la compilación `9.3-53.4` de VPX XVA y versiones posteriores.

> **Importante**
>
> - No puede cambiar esta configuración después de aprovisionar la instancia VPX.
> - El comando `clear config full` de la instancia VPX elimina la configuración de la VLAN si no se selecciona **NSVLAN**.



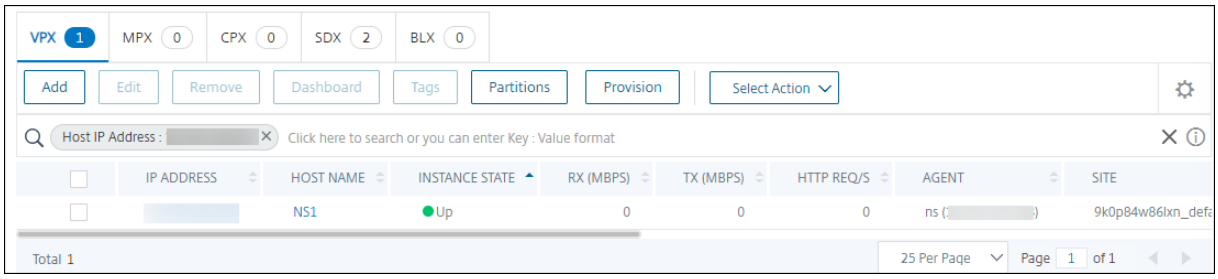

Haga clic en **Listo** para aprovisionar una instancia VPX.

### Ver la instancia VPX aprovisionada

Para ver la instancia recién aprovisionada, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes > Instancias > Citrix ADC** .
2. En la ficha **VPX**, busque una instancia por la propiedad **Dirección IP del host y especifique la dirección** IP de la instancia SDX en ella.




## Aprovisionamiento de instancias de NetScaler ADC VPX en VMware ESX

August 23, 2024

Puede utilizar ADM para automatizar la implementación y administración de una instancia de ADC VPX en VMware ESX. Cuando utiliza NetScaler ADM para aprovisionar una instancia de ADC VPX en VMware ESX, la instancia está disponible para administrarla fácilmente en la GUI de ADM.

NetScaler ADM utiliza plantillas ADC de las instancias ya implementadas para aprovisionar una nueva instancia en VMware ESX. Almacena los detalles del servidor VMware ESX necesarios en un sitio. Además, utiliza el perfil de acceso a la nube para acceder al servidor.

### Requisitos previos

Antes de aprovisionar una instancia de ADC VPX en VMware ESX, asegúrese de completar lo siguiente:

1. Instale una versión compatible de VMware ESXi (6.0, 6.5 y 6.7).
2. Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
3. Descarga de los archivos de instalación de NetScaler ADC VPX.
4. Convierta archivos ADC VPX en plantillas en ESX.
5. Crea un sitio en ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Convertir archivos ADC VPX en plantillas

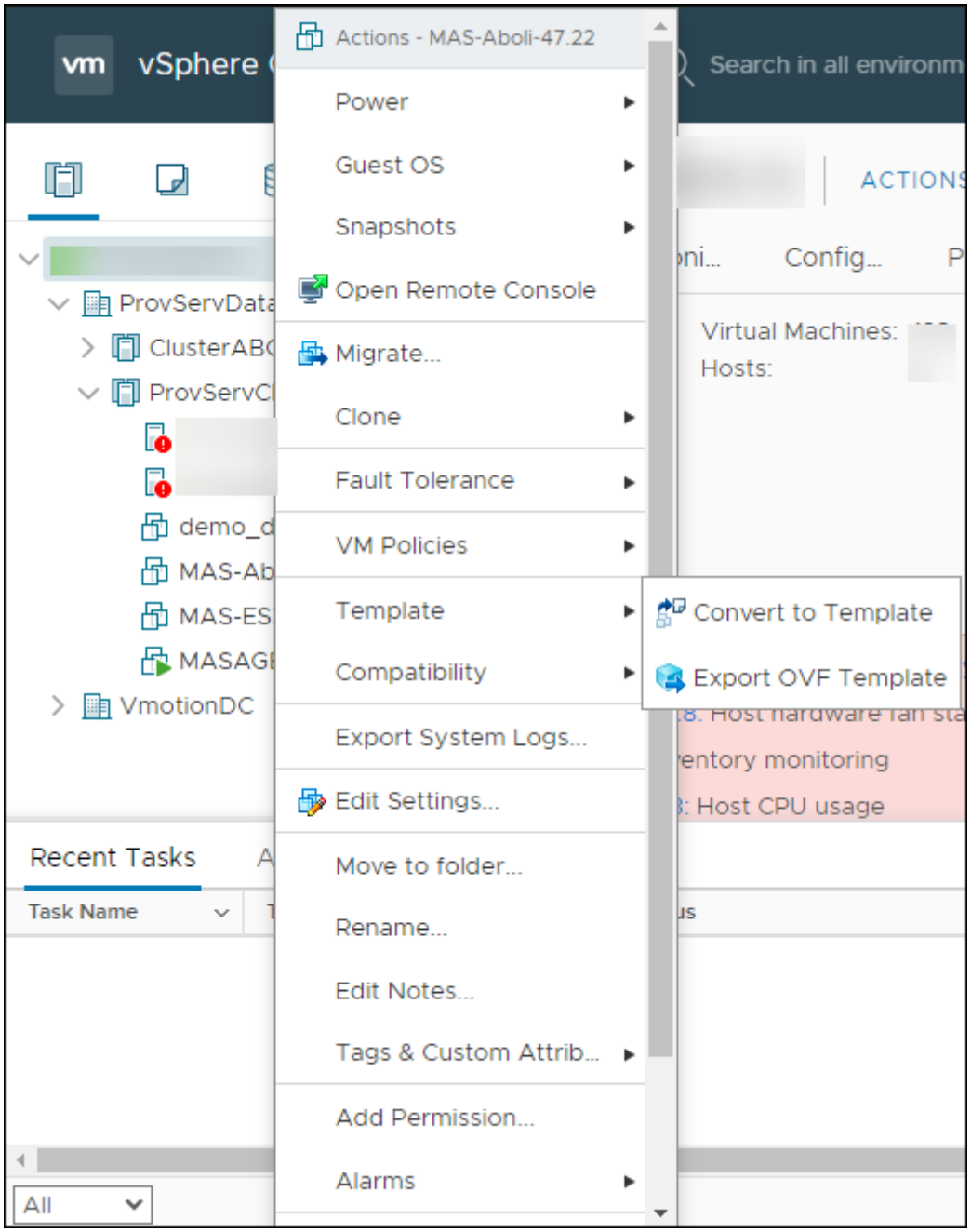
NetScaler ADM utiliza la plantilla ADC en ESX convertida por un archivo ADC VPX. Realice los siguientes pasos para convertir archivos VPX en plantillas.

1. Implemente una instancia de NetScaler ADC VPX en VMware mediante los archivos de configuración de ADC.

   Por primera vez, utilice los archivos de configuración de ADC para implementar la instancia VPX. Para obtener más información, consulte Instalar la instancia de ADC VPX en VMware.

2. Haga clic con el botón derecho del mouse en la máquina virtual **implementada**y seleccione
3. Haga clic en **Convertir en plantilla**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Crear un sitio en ADM

Cree un sitio en NetScaler ADM y agregue los detalles de VMware ESX.

1. En Citrix ADM, vaya a **Redes > Sitios**.
2. Haga clic en **Add**.
3. En el panel **Select Cloud**,

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a) Seleccione **Centro de datos** como tipo de **sitio**.

b) Seleccione **VMware vCenter** en la lista **Tipo**.

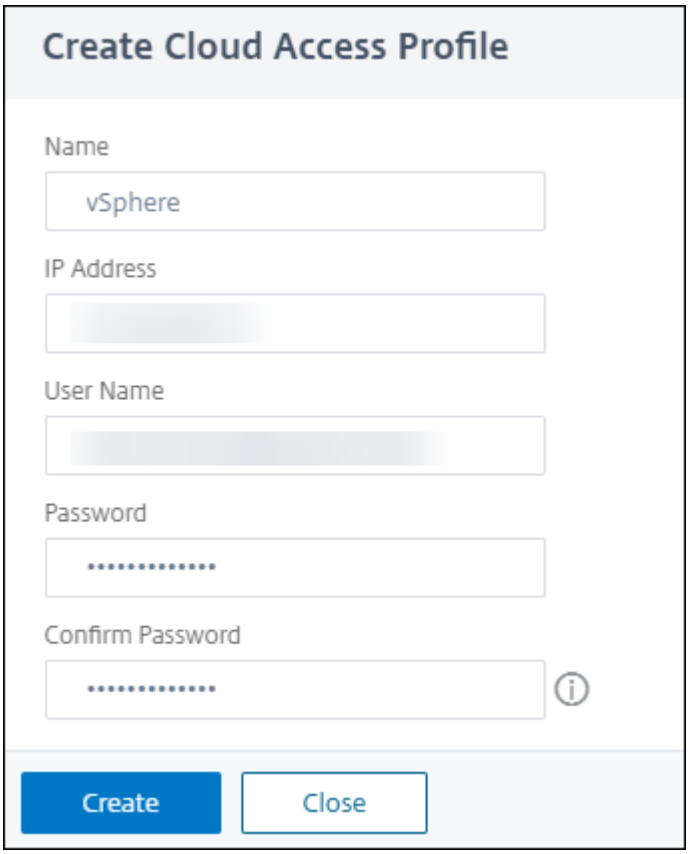
c) Haga clic en **Siguiente**.

4. En el panel **Elegir región,**

a) En el panel **Perfil de acceso a la nube**, seleccione el perfil creado para VMware ESX. Si no hay perfiles, cree un perfil.

b) Para crear un perfil de acceso a la nube, haga clic en **Agregar** y especifique lo siguiente:

- **Nombre**: especifique un nombre para identificar su perfil de acceso a la nube en Citrix ADM.
- **Dirección IP**: especifique la dirección IP del servidor VMware vCenter en el que desea aprovisionar las instancias VPX.
- **Nombre de usuario**: especifique el nombre de usuario para acceder al servidor VMware vCenter.
- **Contraseña**: especifique la contraseña para acceder al servidor VMware vCenter y confirme la contraseña.



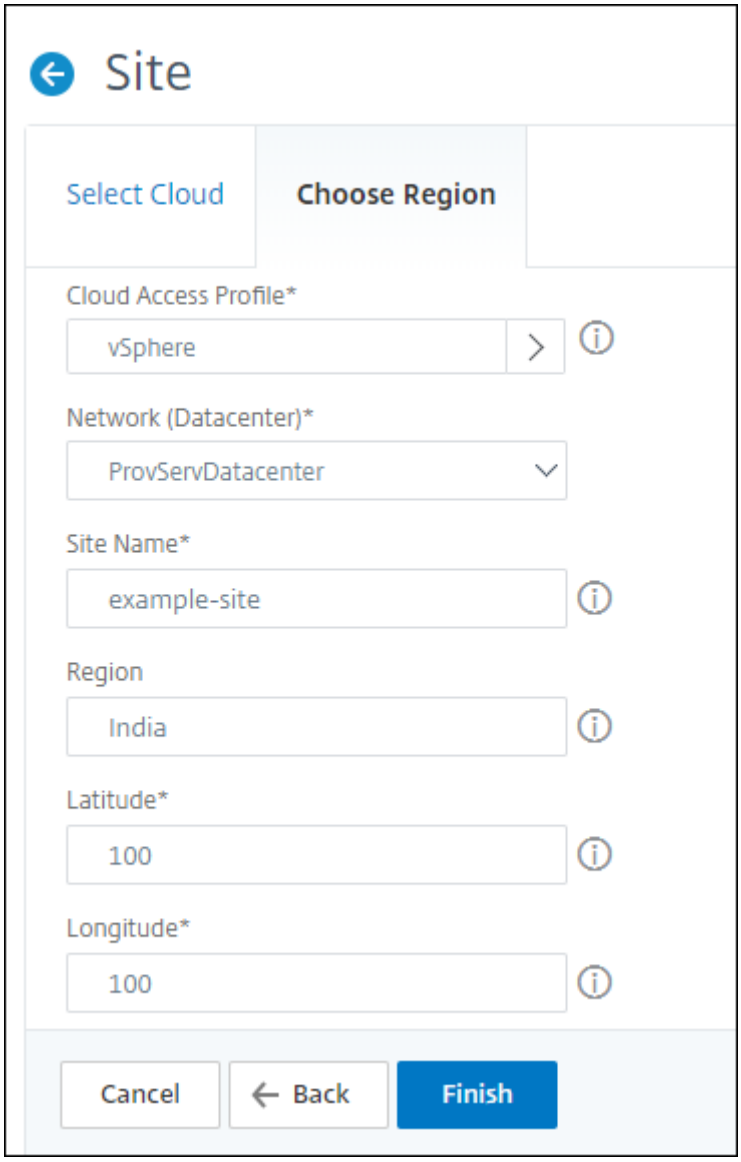

c) En **Red (centro de datos)**, seleccione el centro de datos donde tiene las plantillas ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

d) Especifique el **nombre del sitio**.

e) Especifique la **región**, **latitud**y **longitud** para identificar la ubicación geográfica del centro de datos.

f) Haga clic en **Finalizar**.




### Aprovisionamiento de una instancia en VMware ESX

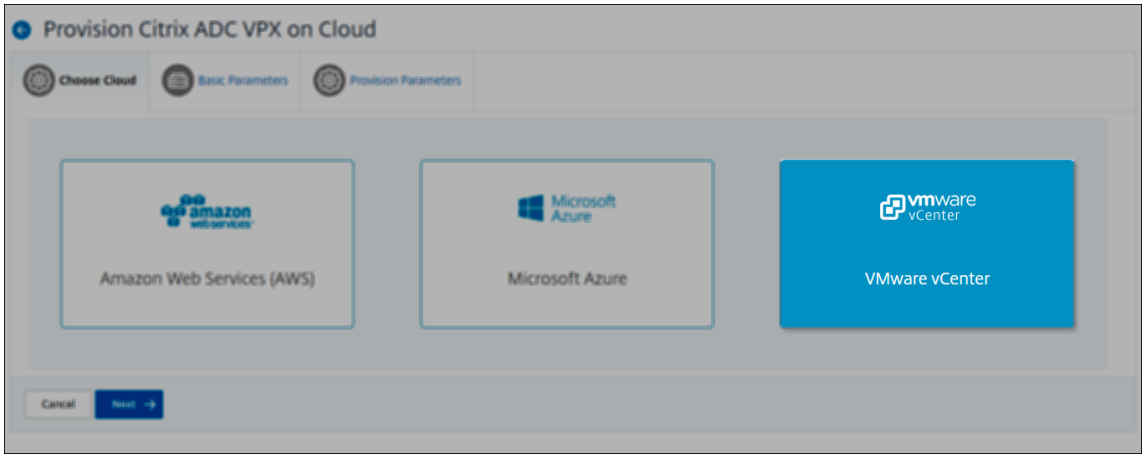
Utilice el sitio que ha asociado con VMware ESX para aprovisionar las instancias de Citrix ADC VPX.

> **Nota:**
>
> Actualmente, Citrix ADM solo admite el aprovisionamiento de instancias de ADC independientes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

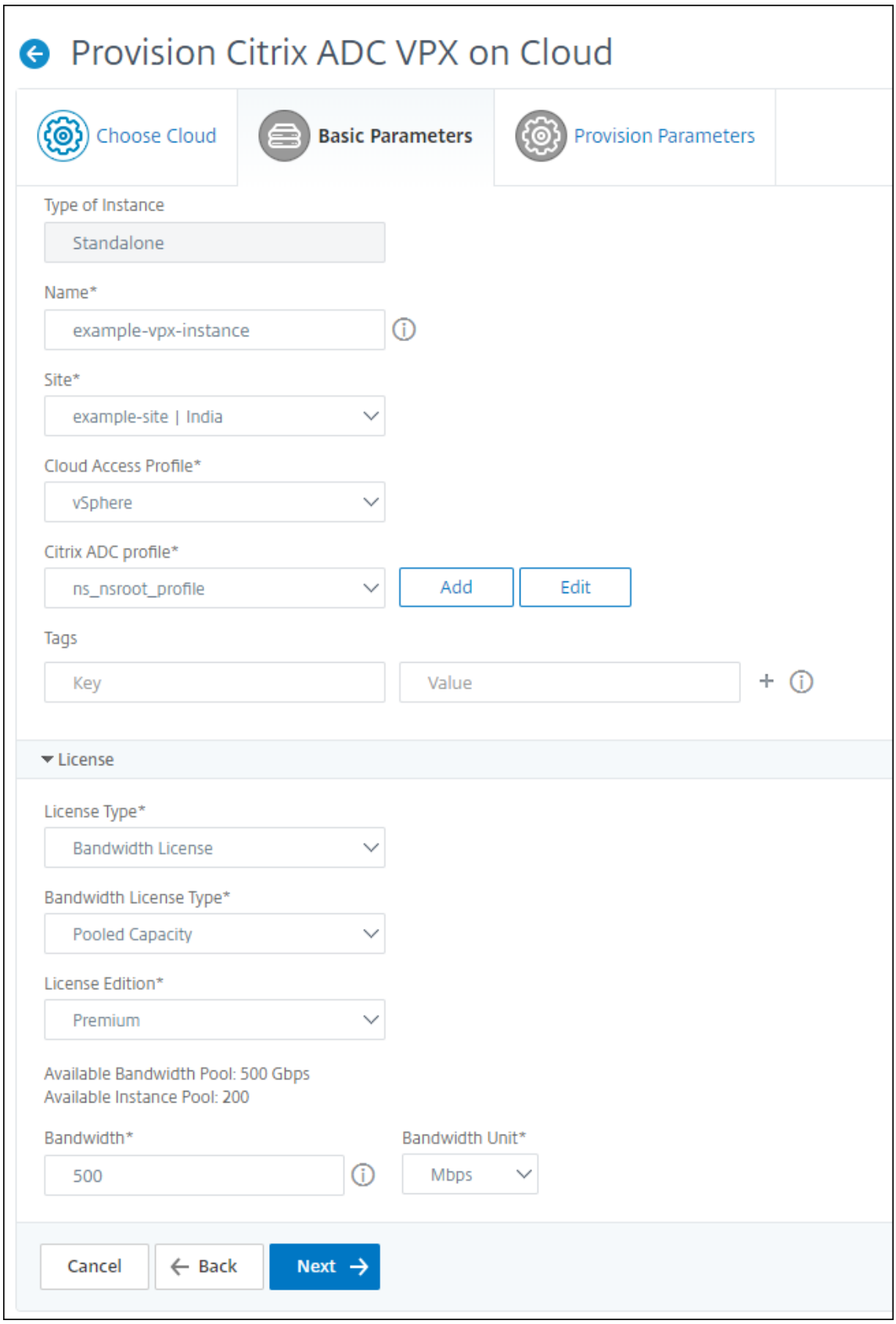
1. En Citrix ADM, vaya a **Redes > Instancias > Citrix ADC**.
2. En la ficha **VPX**, haga clic en **Aprovisionar**.

   Esta opción muestra la página **Provisionar NetScaler ADC VPX on Cloud**.
3. Seleccione **VMware vCenter** y haga clic en **Siguiente**.




4. En **Parámetros básicos**, especifique lo siguiente:
   - **Nombre**: Especifique el nombre de una instancia.
   - **Sitio**: Seleccione el sitio que ha creado anteriormente.
   - **Perfil de acceso a la nube**: Seleccione el perfil de acceso a la nube creado durante la creación del sitio.
   - **Perfil de NetScaler ADC**: Seleccione el perfil ADC para proporcionar autenticación.
   - **Licencia**: Utilice licencias de capacidad agrupada para aplicar licencias a una instancia.

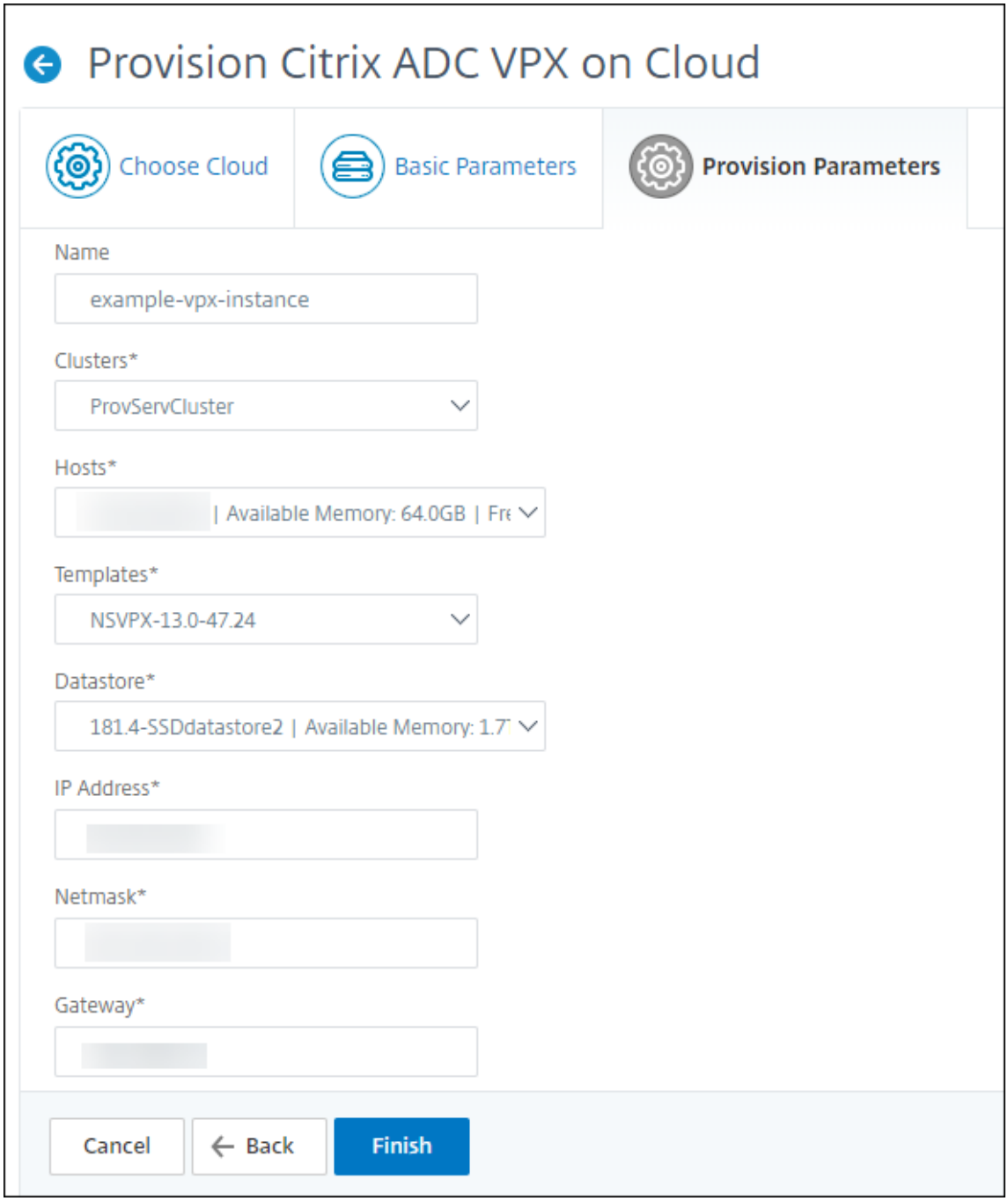
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Haga clic en **Siguiente**.
6. En **Parámetros de provisión**, especifique los siguientes detalles:
    - **Clústeres**: Seleccione el clúster en el que quiere aprovisionar una instancia.
    - **Hosts**: Seleccione el host requerido de la lista.
    - **Plantillas**: Seleccione la plantilla de la lista que quiere aplicar a una instancia.
    - **Almacene de datos**: Seleccione el almacén de datos de la lista.
    - **Dirección IP**: Especifique una dirección IP para una instancia.
    - **Máscara de red**: Especifique una máscara de red para una instancia.
    - **Puerta de enlace**: Especifique una puerta de enlace a una instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




7. Haga clic en **Finalizar**.

## Redescubrir varias instancias de Citrix VPX

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede volver a descubrir varias instancias de Citrix VPX en la configuración de NetScaler Application Delivery Management (ADM). Además, puede volver a descubrir varias instancias de Citrix VPX cuando quiera ver los estados y configuraciones más recientes de esas instancias. El servidor NetScaler ADM vuelve a descubrir todas las instancias de Citrix VPX y comprueba si se puede acceder a las instancias de Citrix Application Delivery Controller (ADC).

**Para redescubrir varias instancias de Citrix VPX:**

1. En un explorador web, escriba la dirección IP del servidor Citrix ADM (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador. Las credenciales de administrador predeterminadas son `nsroot` y `nsroot`.
3. Vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** y seleccione las instancias que quiere volver a detectar.
4. En el menú **Seleccionar acción**, haga clic en **Redescubrir**.
5. Cuando aparezca el mensaje de confirmación para ejecutar la utilidad Redetección, haga clic en **Sí**.

   La pantalla informa del progreso de la redetección de cada una de las instancias de Citrix VPX.

## Desadministrar una instancia

January 30, 2024

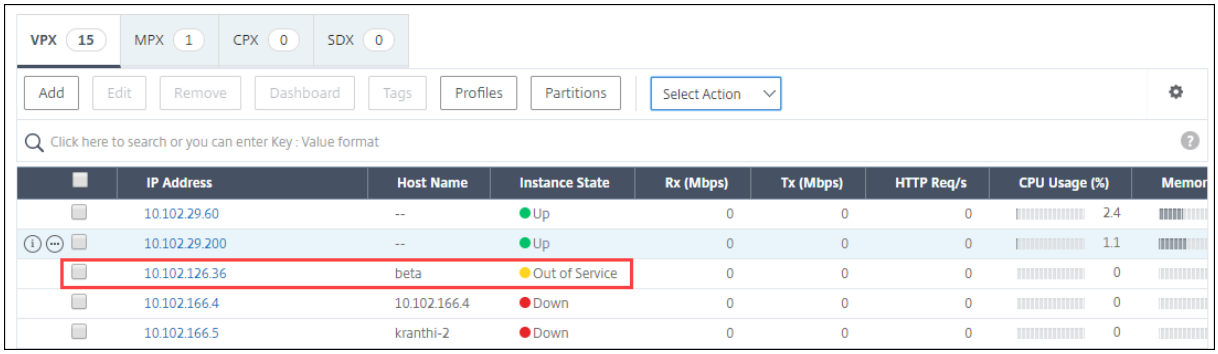
Si quiere detener el intercambio de información entre Citrix Application Delivery Management (ADM) y las instancias de la red, puede desadministrar las instancias.

**Para anular la gestión de una instancia:**

Vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX** . En la lista de instancias, haga clic con el botón derecho en una instancia y, a continuación, seleccione **Desadministrar**, o seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Desadministrar**.

El estado de la instancia seleccionada cambia a **Fuera de servicio** como se muestra en la siguiente ilustración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




NetScaler ADM ya no administra la instancia y ya no intercambia datos con NetScaler ADM.

## Rastrear la ruta a una instancia

January 30, 2024

Al rastrear la ruta de un paquete desde NetScaler Application Delivery Management (ADM) a una instancia, puede encontrar información como el número de saltos necesarios para llegar a la instancia. Traceroute traza la ruta del paquete desde el origen hasta el destino. Muestra la lista de saltos de red junto con el nombre de host y la dirección IP de cada entidad en la ruta.

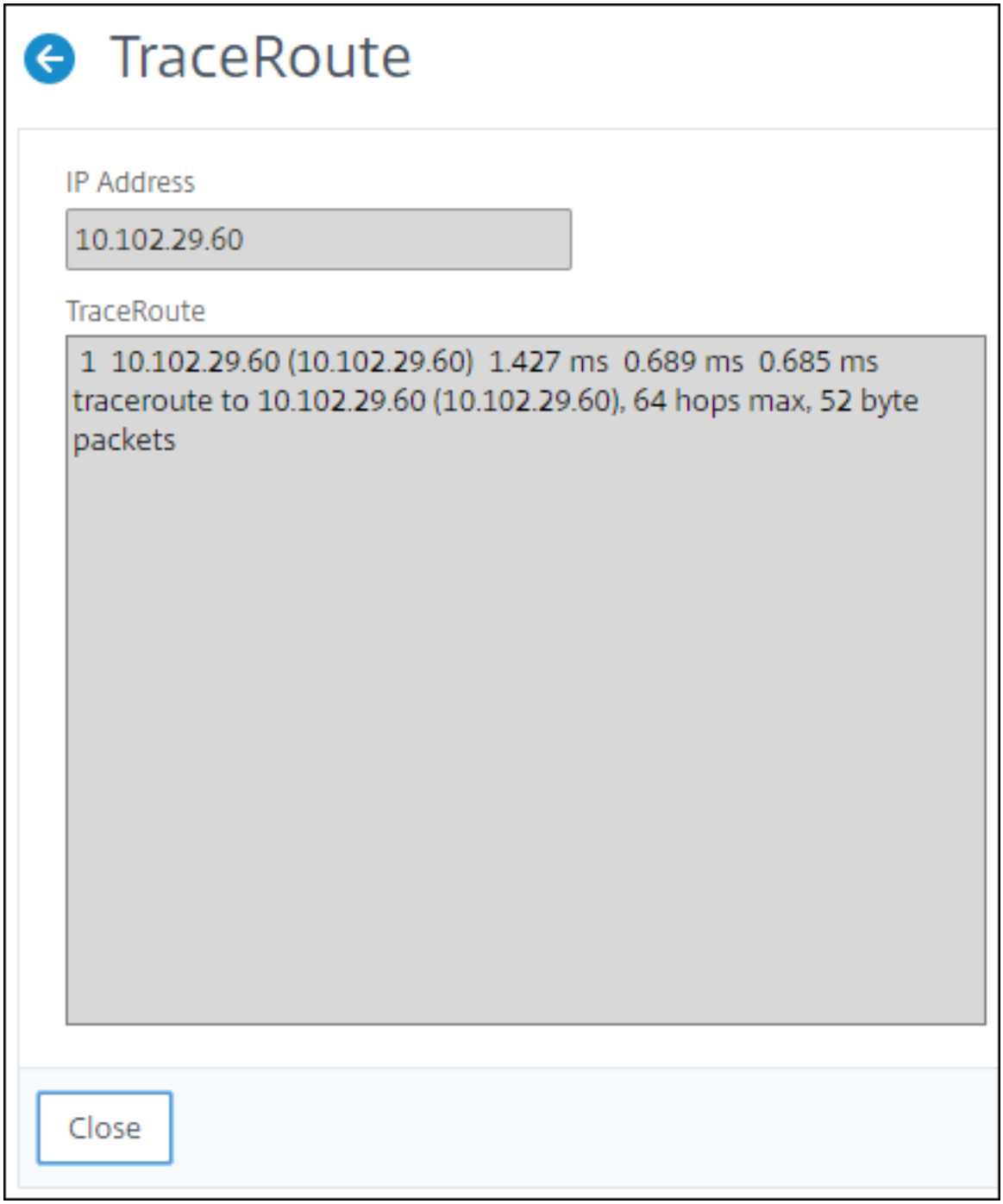
Traceroute también registra el tiempo que tarda un paquete en viajar de un salto a otro. Si hay alguna interrupción en la transferencia de paquetes, traceroute muestra dónde existe el problema.

**Para rastrear la ruta de una instancia:**

1. En Citrix ADM, vaya a la pestaña **Redes** > **Instancias** > **Citrix ADC** > **VPX**.
2. En la lista de instancias, haga clic con el botón derecho en una instancia y, a continuación, seleccione **TraceRoute** o seleccione la instancia y, en el menú **Seleccionar acción**, haga clic en **TraceRoute**.

El cuadro de mensajes de **TraceRoute** muestra la ruta a la instancia y la cantidad de tiempo, en milisegundos, que consume cada salto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Asesoramiento de actualización

January 30, 2024

Como administrador de red, puede administrar muchas instancias de ADC que se ejecutan en difer-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

entes versiones de ADC en NetScaler ADM. Supervisar el ciclo de vida de cada instancia de ADC puede ser una tarea engorrosa. Debe visitar la matriz de productos de Citrixe identificar las instancias de ADC que están llegando al final de su vida útil (EOL) o al final del mantenimiento (EOM). Luego, planea su actualización.

El asesoramiento de actualización le ayuda a supervisar el ciclo de vida de sus instancias de ADC. Identifica las instancias que están alcanzando la EOL/EOM y puede planificar las actualizaciones del ADC antes de la fecha de EOL o EOM.

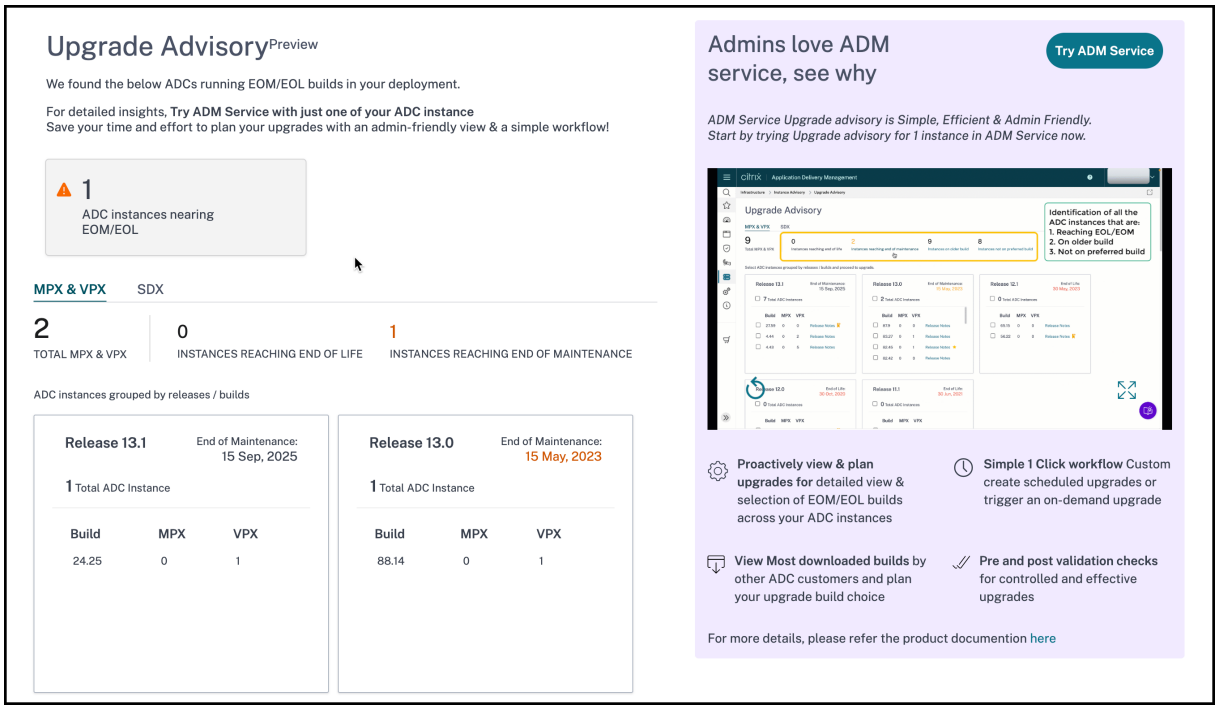
El aviso de actualización realiza un análisis de versiones en los ADC y proporciona una vista de las compilaciones de EOM/EOL en todas las instancias de ADC.

Puede seleccionar e incorporar una de las instancias de ADC al servicio ADM. Haga clic en **Probar ADM Service**e incorpore una instancia de ADC para ver información detallada. Para obtener más información sobre la función de asesoramiento de actualización del servicio ADM, obtenga una vista previa de la animación gif en la página de consejos de **actualización**.

## Consultar el aviso de actualización

Navegue **Redes > Asesor de Instancia > Asesor de Actualización** y vea la siguiente información:

- Recuento total de instancias de ADC.
- Instancias que llegan al final de la vida.
- Instancias que llegan al final del mantenimiento.




La página **Asesor de Actualización** agrupa las instancias de ADC por sus versiones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Asesoramiento de seguridad

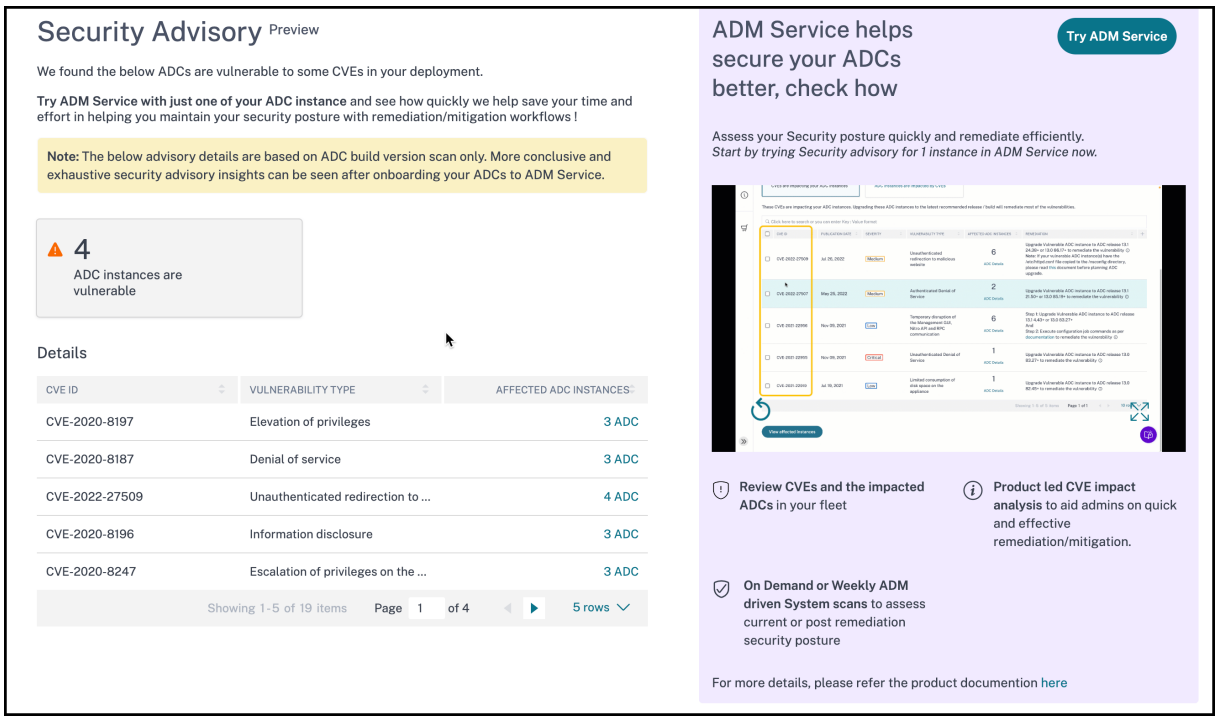
January 30, 2024

Una infraestructura segura, segura y resistente es la línea vital de cualquier organización. Las organizaciones deben realizar un seguimiento de las nuevas vulnerabilidades y exposiciones comunes (CVE) y evaluar el impacto de las CVE en su infraestructura. También deben entender y planificar la mitigación y la remediación para resolver las vulnerabilidades.

El aviso de seguridad ADM de NetScaler destaca los CVE de Citrix que ponen en riesgo sus instancias de ADC.

## Ver asesoramiento de seguridad

Para acceder al **aviso de seguridad**, vaya a **Redes > Asesoramiento de instancias > Asesoramiento de seguridad**. Puede ver el estado de vulnerabilidad de todas las instancias de ADC que administra a través de NetScaler ADM.




Security Advisory solo escanea las versiones de ADC para comprobar si hay CVEs y se muestra una tabla que muestra el número de CVEs que afectan a las instancias de ADC.

- **ID de CVE**: el ID del CVE que afecta a las instancias.
- **Tipo de vulnerabilidad**: el tipo de vulnerabilidad de este CVE.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Instancias de**ADC afectadas: el recuento de instancias**a las que afecta el ID de CVE.

Para comprobar el tipo de vulnerabilidad de un CVE en particular y la información sobre la mitigación y la corrección para resolver la vulnerabilidad, seleccione una de las instancias de ADC y haga clic en **Probar el servicio ADM** e incorpore la instancia de ADC al servicio ADM. Para obtener más información sobre la función de asesoramiento de seguridad de ADM Service, obtenga una vista previa de la animación gif en la página **de consejos de seguridad**.

## Eventos

January 30, 2024

Cuando la dirección IP de una instancia de Citrix Application Delivery Controller (ADC) se agrega a NetScaler Application Delivery Management (ADM), NetScaler ADM envía una llamada NITRO y se agrega implícitamente como destino de captura para que la instancia reciba sus capturas o eventos.

Los eventos representan ocurrencias de eventos o errores en una instancia administrada de NetScaler ADC. Por ejemplo, cuando hay un error en el sistema o un cambio en la configuración, se genera un evento y se registra en el servidor NetScaler ADM. Los eventos recibidos en NetScaler ADM se muestran en la página Resumen de eventos (**Redes** > **Eventos**) y todos los eventos activos se muestran en la página Mensajes de eventos (**Redes** > **Eventos** > **Mensajes de eventos**).

NetScaler ADM también comprueba los eventos generados en las instancias para formar alarmas de diferentes niveles de gravedad. Estas alarmas se muestran como mensajes, algunos de los cuales pueden requerir atención inmediata. Por ejemplo, la falla del sistema se puede clasificar como una gravedad de evento "Crítica"y debería abordarse inmediatamente.

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de los eventos, que pueden ser muchos, generados en toda la infraestructura de NetScaler ADC.

Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen los criterios de filtro de la regla, se ejecuta la acción asociada a la regla. Las condiciones para las que puede crear filtros son: Gravedad, instancias NetScaler ADC, categoría, objetos de error, comandos de configuración y mensajes.

También puede asegurarse de que se activan varias notificaciones para un evento durante un intervalo de tiempo específico, hasta que se borre el evento. Como medida adicional, puede personalizar su correo electrónico con una línea de asunto y un mensaje de usuario específicos, y cargar un archivo adjunto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Usar panel de eventos

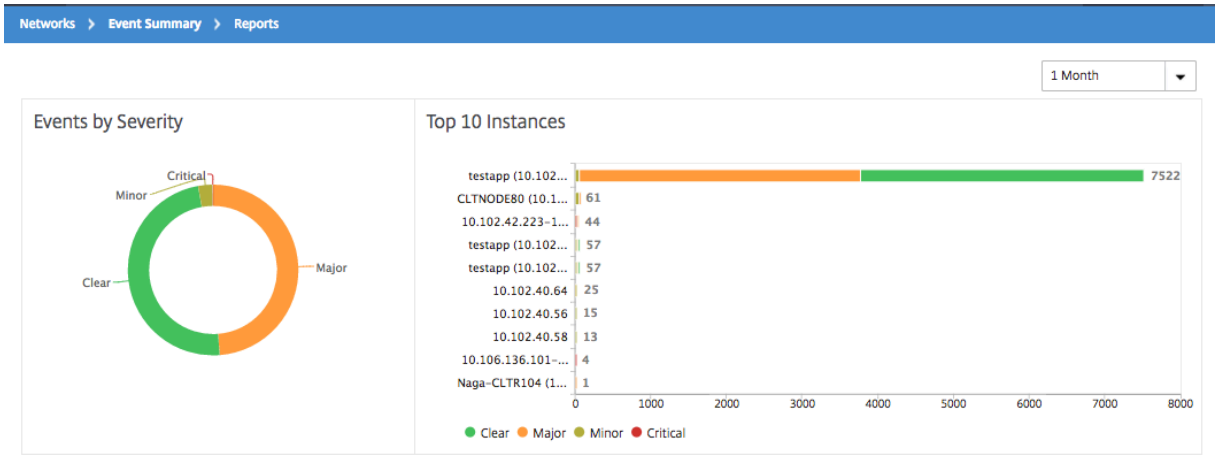
January 30, 2024

Como administrador de red, puede ver detalles como los cambios de configuración, las condiciones de inicio de sesión, los errores de hardware, las infracciones de los umbrales y los cambios en el estado de la entidad en sus instancias de Citrix Application Delivery Controller (ADC), junto con los eventos y su gravedad en instancias específicas. Puede utilizar el panel de eventos de NetScaler Application Delivery Management (ADM) para ver los informes generados con detalles sobre la gravedad de los eventos críticos en todas sus instancias de NetScaler ADC.

**Para ver los detalles en el panel de eventos:**

Vaya a **Redes** > **Eventos** > **Informes** .

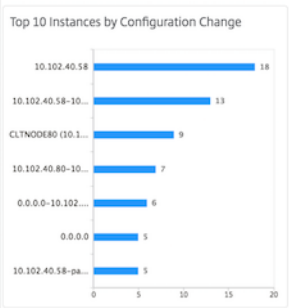
El gráfico 10 dispositivos principales del panel muestra un informe de las 10 instancias principales según el número de eventos generados en ellas. Puede hacer clic en una instancia del gráfico para ver más detalles de la gravedad del evento.



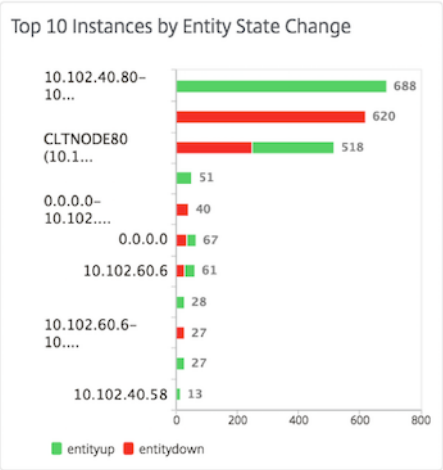

Para ver más detalles, vaya al tipo de instancia de NetScaler ADC (**Redes** > **Eventos** > **Informes** > **NetScaler ADC/ NetScaler ADC SDX/ NetScaler ADC SD-WAN WO**) para ver lo siguiente:

- Los 10 dispositivos principales por fallo de hardware
- Los 10 dispositivos principales por cambio de configuración
- Los 10 dispositivos principales por error de autenticación

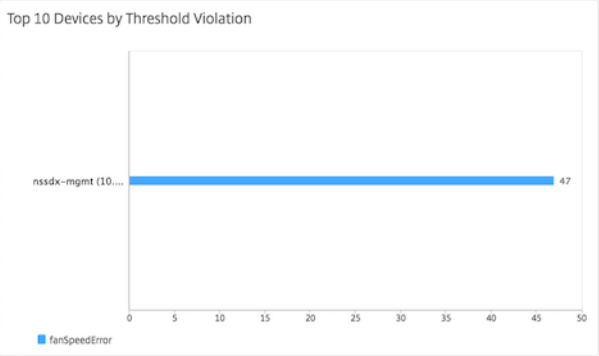
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



- Los 10 principales dispositivos por cambios de estado de entidad




- Los 10 dispositivos principales por infracción de umbral




## Establecer la edad del evento para los eventos

January 30, 2024

Puede configurar la opción de antigüedad del evento para especificar el intervalo de tiempo (en segundos). NetScaler ADM supervisa los dispositivos hasta la duración establecida y genera un evento solo si la antigüedad del evento supera la duración establecida.

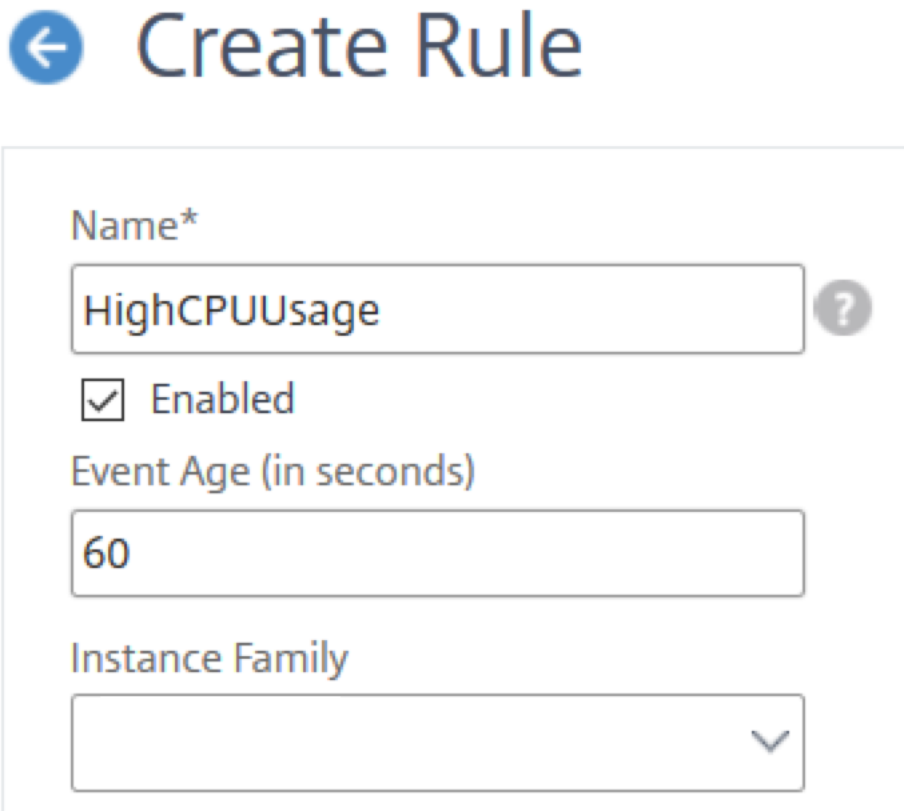
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Por ejemplo, considere que quiere administrar varios dispositivos ADC y recibir una notificación por correo electrónico cuando alguno de sus servidores virtuales deje de funcionar durante 60 segundos o más. Puede crear una regla de evento con los filtros necesarios y establecer la edad del evento de la regla en 60 segundos. A continuación, siempre que un servidor virtual permanezca inactivo durante 60 segundos o más, recibirá una notificación por correo electrónico con detalles como el nombre de la entidad, el cambio de estado y la hora.

**Para establecer la edad del evento en NetScaler ADM:**

1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar**.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. Especifique la edad del evento en segundos.




Asegúrate de configurar todas las trampas relacionadas entre sí en la sección **Categoría** y también establece la gravedad correspondiente en la sección **Gravedad** cuando establezcas la antigüedad del evento. En el ejemplo anterior, seleccione las capturas `entityup`,

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

`entitydown` y `entityofs`.

## Programar un filtro de eventos

January 30, 2024

Después de crear un filtro para la regla, si no desea que el servidor Citrix Application Delivery Management (ADM) envíe una notificación cada vez que el evento generado cumpla los criterios de filtro, puede programar el filtro para que se active solo en intervalos de tiempo específicos, por ejemplo, de forma diaria, semanal o mensual.

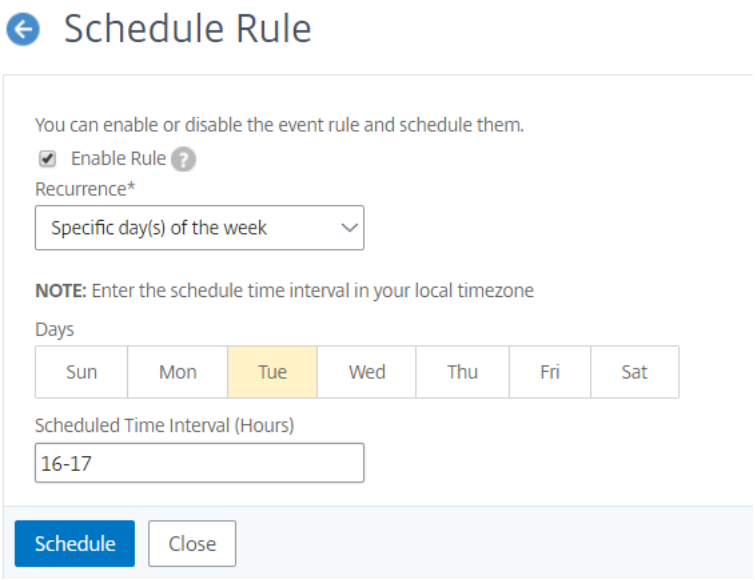
Por ejemplo, si ha programado una actividad de mantenimiento del sistema para diferentes aplicaciones en las instancias en diferentes momentos, las instancias pueden generar varias alarmas.

Si ha configurado un filtro para estas alarmas y ha habilitado las notificaciones por correo electrónico para estos filtros, el servidor envía un gran número de notificaciones por correo electrónico cuando Citrix ADM recibe estas trampas. Si quiere que el servidor envíe estas notificaciones por correo electrónico únicamente durante un período de tiempo específico, puede hacerlo programando un filtro.

**Para programar un filtro con NetScaler ADM:**

1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Reglas** .
2. Seleccione la regla para la que quiere programar un filtro y haga clic en **Ver planificación**.
3. En la página **Regla programada**, haga clic en **Programar** y especifique los siguientes parámetros:
   - **Habilitar regla**: Active esta casilla de verificación para habilitar la regla de evento programado.
   - **Periodicidad**: Intervalo en el que se planifica la regla. Seleccione un día específico de la semana o una fecha específica de un mes.
   - **Días**: seleccione el día de la semana para ejecutar la regla. Puede seleccionar varios días.
   - **Fechas**: Escriba las fechas. Puede escribir varias fechas como valores separados por comas.
   - **Intervalo de tiempo programado (horas)**: Horas en las que programar la regla (utilice el formato de 24 horas).
4. Haga clic en **Programar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Establecer notificaciones de correo electrónico repetidas para eventos

January 30, 2024

Para garantizar que se aborden todos los eventos críticos y no se omita ninguna notificación importante por correo electrónico, puede optar por enviar notificaciones por correo electrónico repetidas para las reglas de eventos que cumplan con los criterios que has seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.

Estas notificaciones por correo electrónico se envían repetidamente, a intervalos predefinidos, hasta que el destinatario reconoce haber visto la notificación o se borra la regla de evento.

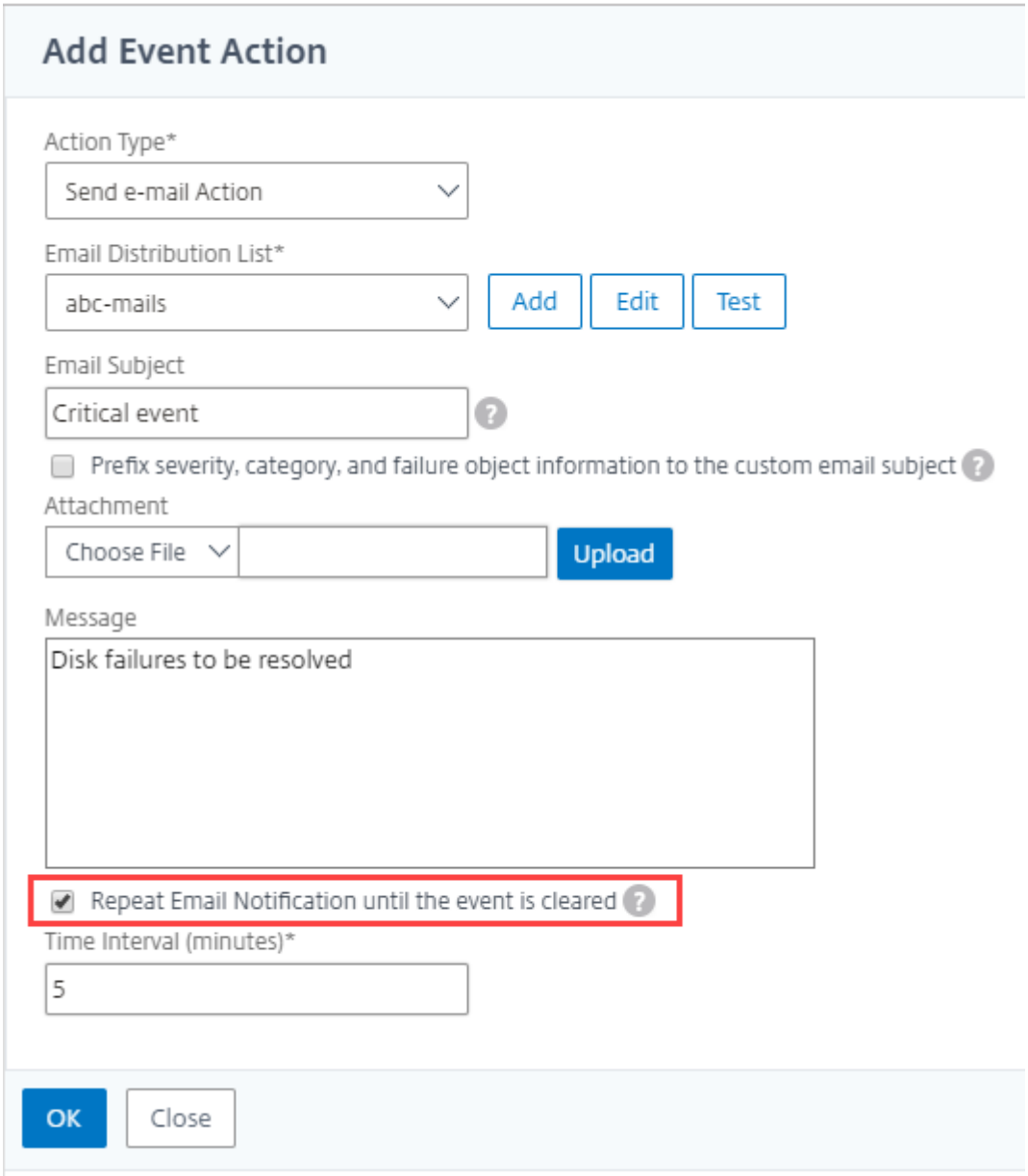
> **Nota**
>
> Los eventos solo se pueden borrar automáticamente si hay una trampa “clara”equivalente establecida y enviada desde su instancia de Citrix Application Delivery Controller (ADC).
>
> Para borrar un evento manualmente, puede hacer lo siguiente:
>
> - Vaya a **Redes > Eventos > Resumen del evento** , elija una **categoría** , seleccione un evento de la categoría y haga clic **en**Borrar .
> - O bien, vaya a **Redes > Eventos > Mensajes de eventos**. Elija un tipo de instancia y, a continuación, seleccione un evento de la siguiente cuadrícula y haga clic en **Borrar**.

**Para configurar notificaciones de correo electrónico repetidas desde NetScaler ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix Application Delivery Management (ADM), vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar** para crear una regla.
2. En la página **Crear regla**, establezca los parámetros de regla.
3. En Acciones de **reglas de eventos** , haga clic en **Agregar acción** . A continuación, seleccione **Enviar acción de correo electrónico** en la lista desplegable **Tipo de acción** y seleccione una lista de **distribución de correo electrónico**.
4. También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto al correo electrónico cuando un evento entrante coincida con la regla configurada.
5. Active la casilla de verificación **Repetir notificación por correo electrónico hasta que se desactive el evento**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Suprimir eventos

January 30, 2024

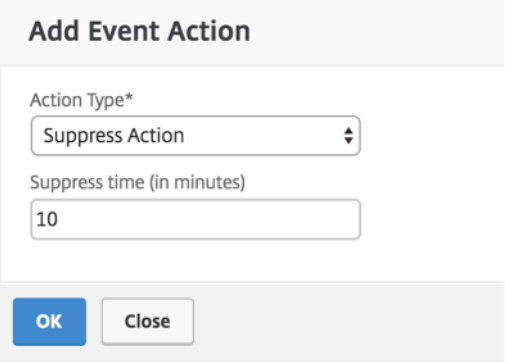
Al elegir la acción **Suprimir** evento de acción, puede configurar un período de tiempo, en minutos, durante el cual se suprime o descarta un evento. Puede suprimir el evento durante un mínimo de 1 minuto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Nota:
>
> También puede configurar el tiempo de supresión como 0 minutos y significa tiempo infinito. Si no especifica ninguna duración de tiempo, NetScaler ADM considerará el tiempo de supresión como cero y nunca caduca.

**Para suprimir eventos mediante NetScaler ADM:**

1. En Citrix Application Delivery Management (ADM), vaya a **Redes** > **Eventos** > **Reglas** . Haga clic en **Agregar**.
2. Especifique todos los parámetros necesarios para crear una regla.
3. En **Acciones de regla de evento**, haga clic en **Agregar acción** para asignar acciones de notificación al evento.
4. En la página **Agregar acción de evento**, seleccione **Suprimir acción** en la lista desplegable **Tipo de acción** y especifique el período de tiempo, en minutos, para el que debe suprimirse un evento.
5. Haga clic en **Aceptar**.




## Crear reglas de eventos

August 23, 2024

Puede configurar reglas para supervisar eventos específicos. Las reglas facilitan la supervisión de un gran número de eventos generados en toda la infraestructura.

Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen los criterios de filtro de la regla, se ejecuta la acción asociada a la regla. Las condiciones para las que puede crear filtros son: gravedad, instancias de Citrix Application Delivery Controller (NetScaler ADC), categoría, objetos de error, comandos de configuración y mensajes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

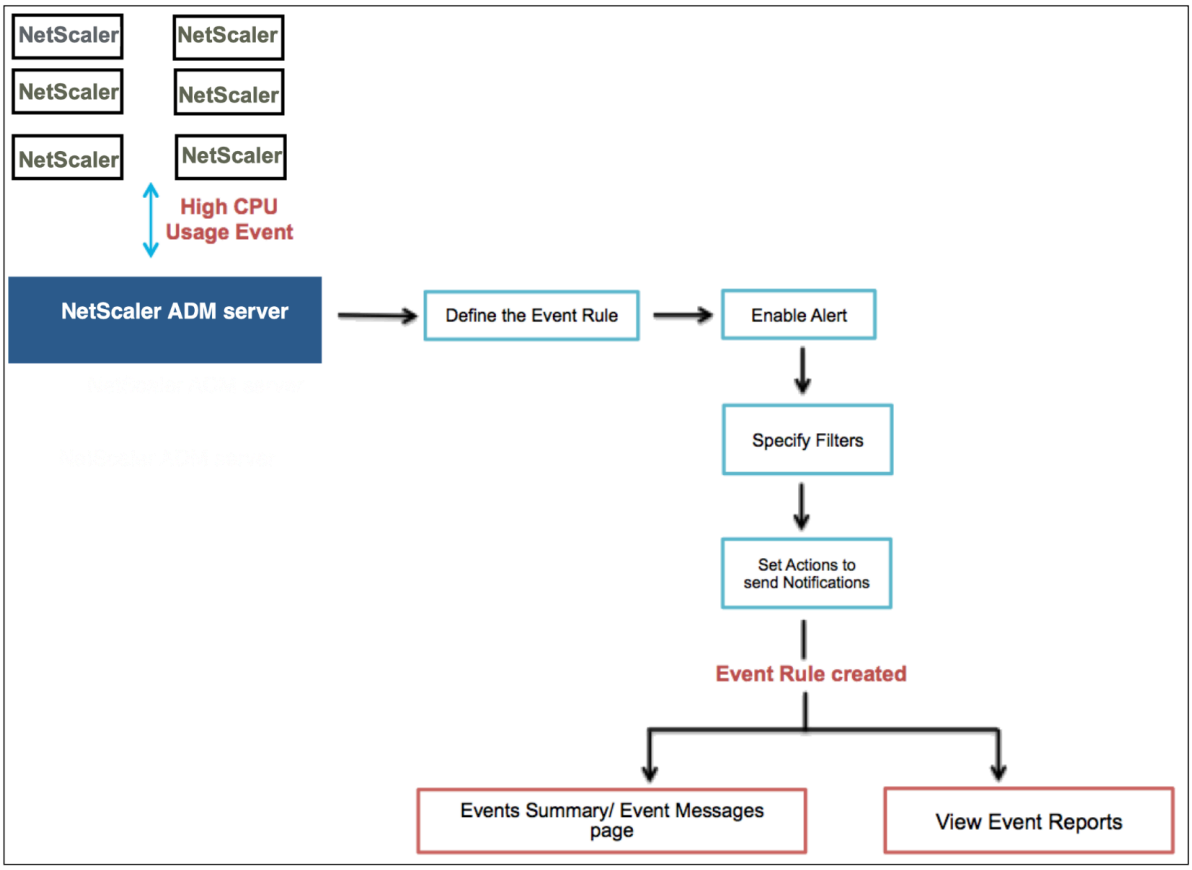
Puede asignar las siguientes acciones a los eventos:

- **Acción de envío de correo electrónico**: Enviar un correo electrónico para los eventos que coinciden con los criterios de filtrado.
- **Enviar acción de captura**: Enviar o reenviar capturas SNMP a un destino de captura externo
- **Ejecutar acción de comando**: Ejecute un comando cuando un evento entrante cumpla con la regla configurada.
- **Ejecutar acción de trabajo**: Ejecutar un trabajo es para eventos que coinciden con los criterios de filtro especificados.
- **Suprimir acción**: Suprime la eliminación de un evento durante un período de tiempo específico.
- **Enviar notificaciones de Slack**: envía notificaciones en el canal de Slack configurado para los eventos que coincidan con los criterios del filtro.
- **Enviar notificaciones de PagerDuty**: Envíe notificaciones de eventos basadas en las configuraciones de PagerDuty para los eventos que coincidan con los criterios de filtro.
- **Enviar notificaciones de ServiceNow**: Generar automáticamente incidentes de ServiceNow para un evento que coincida con los criterios de filtro.

Para obtener más información, consulte Agregar acciones de reglas de eventos

También puede hacer que las notificaciones se reenvíen en un intervalo especificado hasta que se borre un evento. Además, puede personalizar el correo electrónico con una línea de asunto específica, un mensaje de usuario y un archivo adjunto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Por ejemplo, como administrador, puede que quiera supervisar los eventos de “alto uso de CPU”para instancias específicas de NetScaler ADC si esos eventos pueden provocar una interrupción de las instancias de NetScaler ADC. Puede hacer lo siguiente:

- Crea una regla para supervisar las instancias y especifica una acción que te envíe una notificación por correo electrónico cuando se produzca un evento de la categoría “uso elevado de la CPU”.
- Programe la regla para que se ejecute a una hora específica, por ejemplo, entre las 11:00 y las 23:00 horas, de modo que no se le notifique cada vez que se genere un evento.

La configuración de una regla de evento implica las siguientes tareas:

1. Defina la regla
2. Elija la gravedad del evento que detecta la regla
3. Especifica la categoría del evento
4. Especificar instancias NetScaler ADC a las que se aplica la regla
5. Seleccionar objetos de error
6. Especificar filtros avanzados

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. Especificar las acciones que se deben realizar cuando la regla detecta un evento

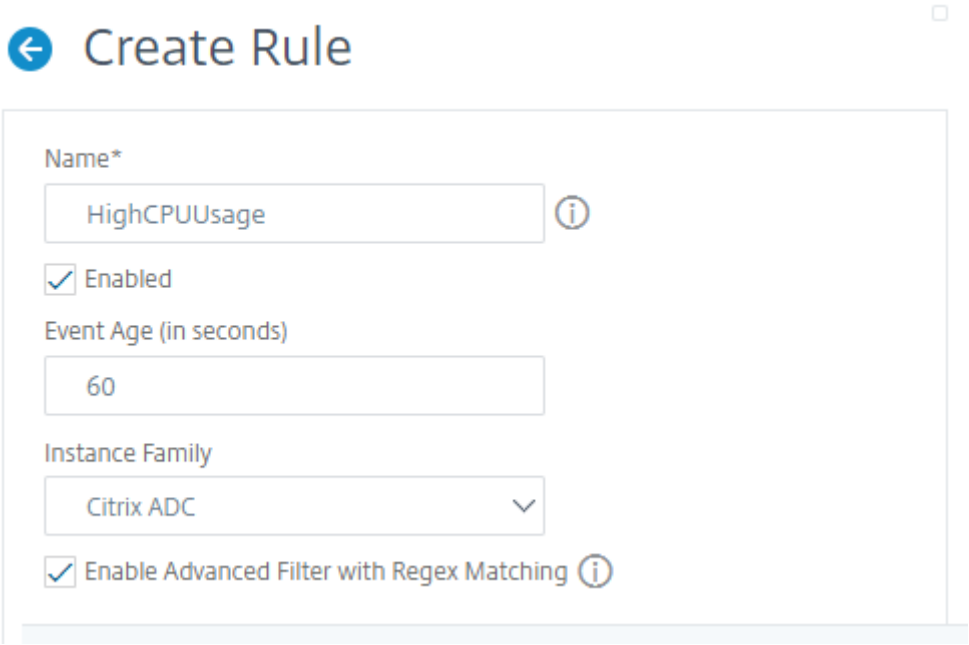
### Paso 1: Definir una regla de evento

Vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar** . Si quiere habilitar la regla, active la casilla de verificación **Habilitar regla**.

Puede configurar la opción **Event Age** para especificar el intervalo de tiempo (en segundos) tras el cual NetScaler ADM actualiza una regla de eventos.

> Nota:
>
> El valor mínimo para la antigüedad del evento es de 60 segundos. Si mantiene el campo **Edad del evento** en blanco, la regla de evento se aplica inmediatamente después de que se produzca el evento.

Según el ejemplo anterior, es posible que desee recibir una notificación por correo electrónico cada vez que su instancia de Citrix ADC tenga un evento de «uso elevado de CPU» durante 60 segundos o más. Puede establecer la antigüedad del evento en 60 segundos, de modo que cada vez que la instancia de Citrix ADC tenga un evento de «uso elevado de CPU» durante 60 segundos o más, reciba una notificación por correo electrónico con los detalles del evento.




También puede filtrar las reglas de eventos por **familia de instancias** para rastrear la instancia de NetScaler ADC desde la que NetScaler ADM recibe un evento.

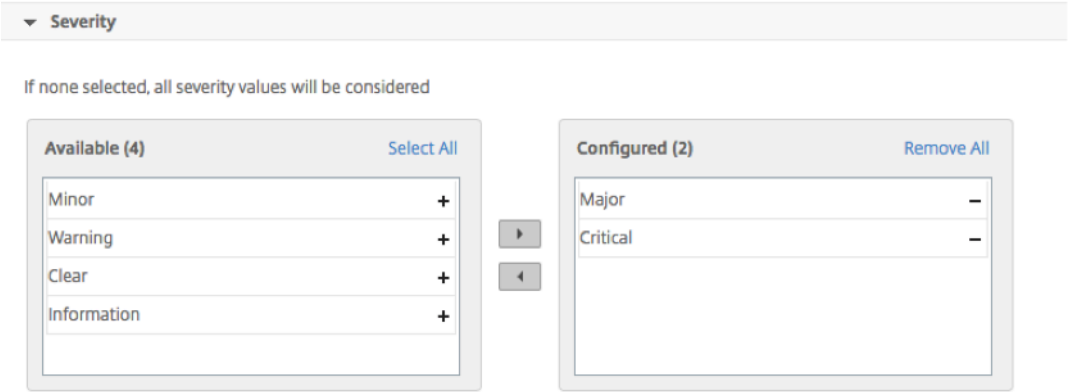
Si quiere incluir una expresión regular distinta de la coincidencia de patrones de asterisco (*), seleccione **Habilitar filtro avanzado con coincidencia de expresiones regulares**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Paso 2: Elige la gravedad del evento

Puede crear reglas de evento que utilicen la configuración de gravedad predeterminada. La gravedad especifica la gravedad actual de los eventos a los que quiere agregar la regla de eventos.

Puede definir los siguientes niveles de gravedad: Crítico, Mayor, Menor, Advertencia, Borrar e Información.



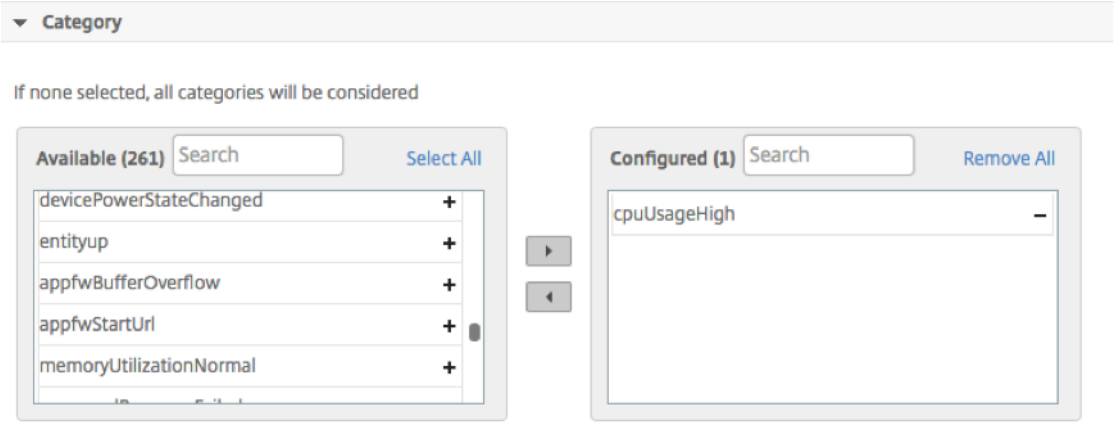

> **Nota**
>
> Puede configurar la gravedad para eventos genéricos y específicos de Advanced. Para modificar la gravedad de los eventos de las instancias NetScaler ADC administradas en NetScaler ADM, vaya a **Redes** > **Eventos** > **Configuración de eventos**. Elija la **categoría** para la que quiere configurar la gravedad del evento y haga clic en **Configurar gravedad**. Asigne un nuevo nivel de gravedad y haga clic en **Aceptar**.

### Paso 3: Especifica la categoría del evento

Puede especificar la categoría o las categorías de los eventos generados por las instancias NetScaler ADC. Todas las categorías se crean en instancias de NetScaler ADC. A continuación, estas categorías se mapean con NetScaler ADM, que se puede utilizar para definir reglas de eventos. Seleccione la categoría que quiera considerar y muévalo de la tabla **Disponible** a la tabla **Configurada**.

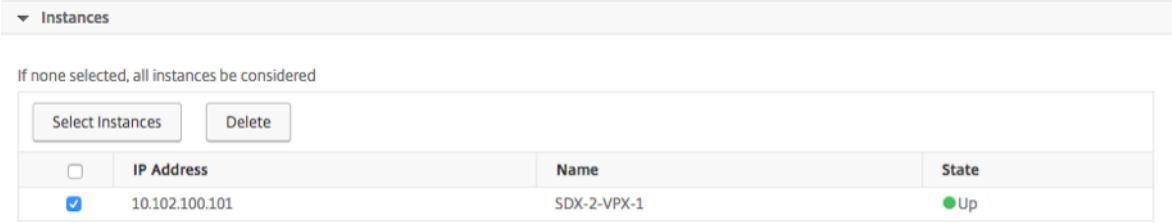
En el ejemplo anterior, tendrás que elegir “CpuUsageHigh”como categoría de eventos de la tabla que se muestra.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Paso 4: Especificar instancias de NetScaler ADC

Seleccione las direcciones IP de las instancias de NetScaler ADC para las que quiere definir la regla de eventos. En la sección **Instancias**, haga clic en **Seleccionar instancias**. En la página **Seleccionar Instancias**, elija las instancias y haga clic en **Seleccionar**.




### Paso 5: Seleccione objetos de error

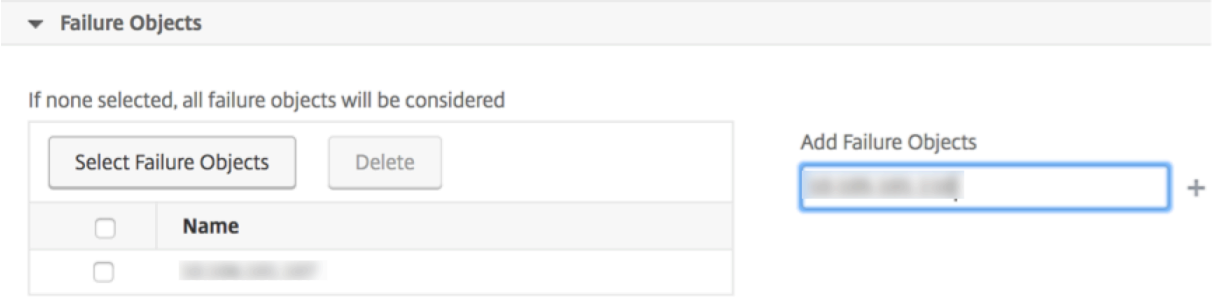
Puede seleccionar un objeto de error de la lista proporcionada o agregar un objeto de fallo para el que se haya generado un evento. También puede especificar una expresión regular para agregar objetos de error. Según la expresión regular especificada, los objetos de error se agregan automáticamente a la lista. Los objetos de error son instancias de entidad o contadores para los que se ha generado un evento.

> **Importante**
>
> Para enumerar objetos con errores mediante expresiones regulares, seleccione **Habilitar filtro avanzado con coincidencia de expresiones** regulares en el paso 1.

El objeto de error afecta a la forma en que se procesa un evento y garantiza que refleje el problema exacto tal como se notifica. Con este filtro, puede realizar un seguimiento rápido de los problemas en los objetos de falla e identificar la causa de un problema. Por ejemplo, si un usuario tiene problemas para iniciar sesión, el objeto de error aquí es el nombre de usuario o la contraseña, por ejemplo `nsroot`.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Esta lista puede contener nombres de contador para todos los eventos relacionados con umbrales, nombres de entidades para todos los eventos relacionados con entidades, nombres de certificados para eventos relacionados con certificados, etc.

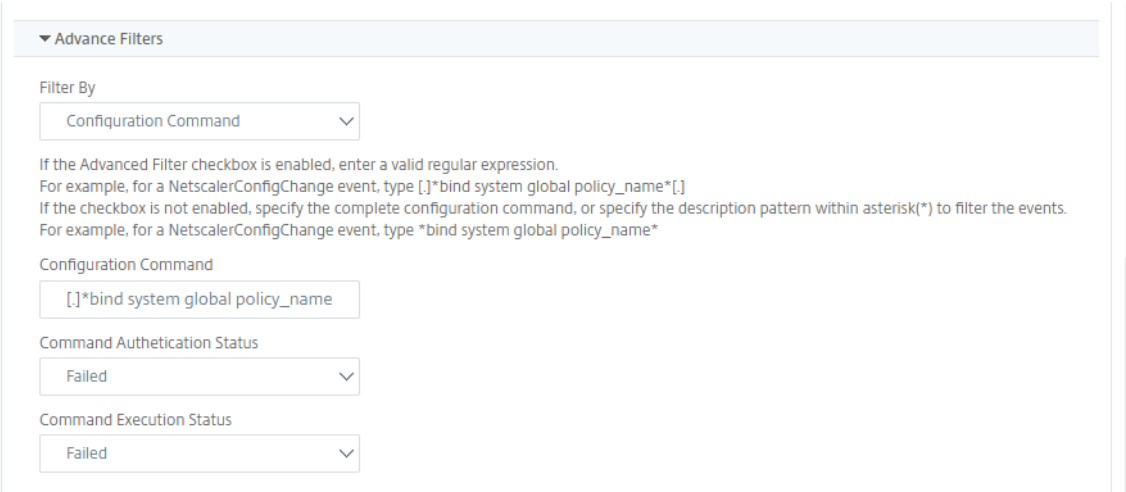



### Paso 6: Especificar filtros avanzados

Puede filtrar aún más una regla de evento por:

- **Comandos de configuración**: puede especificar el comando de configuración completo o especificar una expresión regular para filtrar los eventos.

  Puede filtrar aún más la regla de eventos según el estado de autenticación y/o el estado de ejecución del comando. Por ejemplo, para a `NetscalerConfigChange event`, escriba `[.]*bind system global policy_name[.]*`.




- **Mensajes**: puede especificar la descripción completa del mensaje o especificar una expresión regular para filtrar los eventos.
  Por ejemplo, para un evento `NetscalerConfigChange`, escriba `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`
  .

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

## Paso 7: Agregar acciones de reglas de eventos

Puede agregar acciones de regla de evento para asignar acciones de notificación a un evento. Estas notificaciones se envían o realizan cuando un evento cumple con los criterios de filtro definidos anteriormente. Puede agregar las siguientes acciones de evento:

- Enviar correo electrónico Action
- Acción de captura de envío
- Ejecutar acción de comando
- Ejecutar acción de trabajo
- Acción de supresión
- Enviar notificaciones de Slack
- Enviar notificaciones de PagerDuty
- Enviar notificaciones de ServiceNow

### Para establecer la acción de regla de evento de correo electrónico

Al elegir el tipo de acción de evento Enviar correo electrónico, se activa un correo electrónico cuando los eventos cumplen con los criterios de filtro definidos. Deberá crear una lista de distribución de correo electrónico proporcionando los detalles del servidor de correo o del perfil de correo, o puede seleccionar una lista de distribución de correo electrónico que haya creado anteriormente.

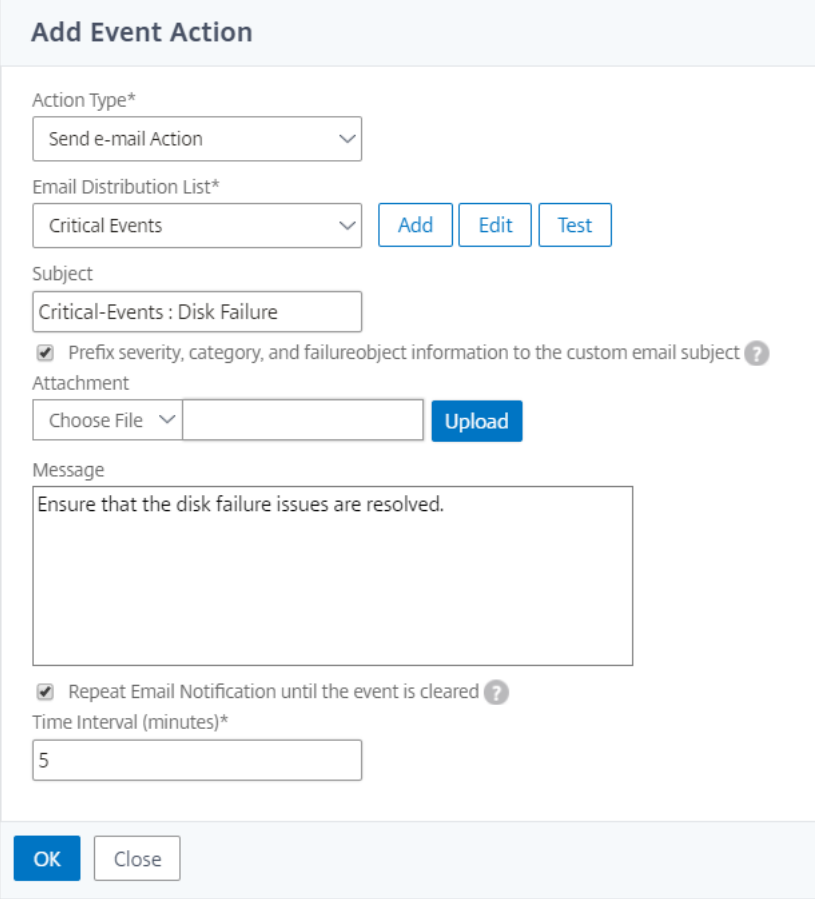
Debido a la gran cantidad de servidores virtuales que se configuran en NetScaler ADM, es posible que reciba un gran número de correos electrónicos cada día. Los correos electrónicos tienen una línea de asunto predeterminada que proporciona información sobre la gravedad del evento, la categoría del evento y el objeto de error. Sin embargo, la línea de asunto no contiene información sobre el nombre del servidor virtual en el que se originan estos eventos. Ahora tiene la opción de incluir información adicional, como el nombre de la entidad afectada, es decir, el nombre del objeto de error.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

También puede agregar una línea de asunto personalizada y un mensaje de usuario, y cargar un archivo adjunto a su correo electrónico cuando un evento entrante coincida con la regla configurada.

Al enviar correos electrónicos para notificaciones de eventos, es posible que quiera enviar un correo electrónico de prueba para probar los ajustes configurados. El botón "Probar"ahora le permite enviar un correo electrónico de prueba después de configurar un servidor de correo electrónico, las listas distribuidas asociadas y otros ajustes. Esta función garantiza que la configuración funcione bien.

También puede asegurarte de que se aborden todos los eventos críticos y no se omita ninguna notificación importante por correo electrónico. Para ello, selecciona la casilla **Repetir notificación por correo electrónico hasta que se desactive el evento** para enviar notificaciones repetidas por correo electrónico sobre las reglas de eventos que cumplan con los criterios que has seleccionado. Por ejemplo, si ha creado una regla de evento para las instancias que implican errores de disco y quiere recibir una notificación hasta que se resuelva el problema, puede optar por recibir notificaciones por correo electrónico repetidas sobre esos eventos.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para establecer la acción de regla de evento de reventado**

Al elegir el tipo de **acción de evento Enviar acción de captura**, las capturas SNMP se envían o reenvían a un destino de captura externo. Al definir una lista de distribución de trampas (o el destino de las trampas y los detalles del perfil de las trampas), los mensajes de captura se envían a detectores de trampas específicos cuando los eventos cumplen con los criterios de filtro definidos.

**Para establecer la acción Ejecutar comando**

Al elegir la acción del evento **Ejecutar acción de comando**, puede crear un comando o un script que se pueda ejecutar en NetScaler ADM para eventos que coincidan con un criterio de filtro determinado.

También puede establecer los siguientes parámetros para el script **Run Command Action** :

| Parámetro | Descripción |
|---|---|
| $fuente | Este parámetro corresponde a la dirección IP de origen del evento recibido. |
| $categoría | Este parámetro corresponde al tipo de trampas definido en la categoría del filtro |
| $entidad | Este parámetro corresponde a las instancias o contadores de entidades para los que se ha generado un evento. Puede incluir los nombres de los contadores de todos los eventos relacionados con el umbral, los nombres de las entidades de todos los eventos relacionados con la entidad y los nombres de los certificados de todos los eventos relacionados con los certificados. |
| $gravedad | Este parámetro corresponde a la gravedad del evento. |
| $failure.obj | El objeto de error afecta a la forma en que se procesa un evento y garantiza que el objeto de error refleja el problema exacto tal como se ha notificado. Esto se puede usar para rastrear problemas rápidamente e identificar el motivo de la falla, en lugar de simplemente informar eventos sin procesar. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Durante la ejecución del comando, estos parámetros se reemplazan con valores reales.

Por ejemplo, considere que quiere establecer una acción de comando de ejecución cuando el estado de un servidor virtual de equilibrio de carga es **Inactivo**. Como administrador, puede considerar la posibilidad de ofrecer una solución rápida agregando otro servidor virtual. En NetScaler ADM, puede:

- Escriba un archivo de script (.sh).

  A continuación se muestra un archivo de script (.sh) de ejemplo:

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"PASSIVE","appflowlog":"ENABLED","bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
curl --insecure -basic -u nsroot:nsroot -H "Content-type: application/json" -X POST -d $payload $url
```

- Guarde el archivo .sh en cualquier ubicación persistente del agente NetScaler ADM. Por ejemplo: `/var`.
- Proporcione la ubicación del archivo.sh en NetScaler ADM que se ejecutará cuando se cumplan los criterios de regla.

Para configurar la acción **Ejecutar comando** para crear un nuevo servidor virtual:

1. Defina la regla
2. Seleccione la gravedad del evento
3. Selecciona la categoría de eventos **entitydown**
4. Seleccione la instancia que tiene configurado el servidor virtual
5. Seleccione o cree un objeto de error para el servidor virtual
6. En **Acciones de reglas de eventos**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de comando** en la lista de **tipos de acciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. En **Lista de ejecución de comandos**, haga clic en **Agregar**.

   Aparece la página Crear lista de distribución de comandos.

   a) En **Nombre del perfil**, especifique un nombre de su elección

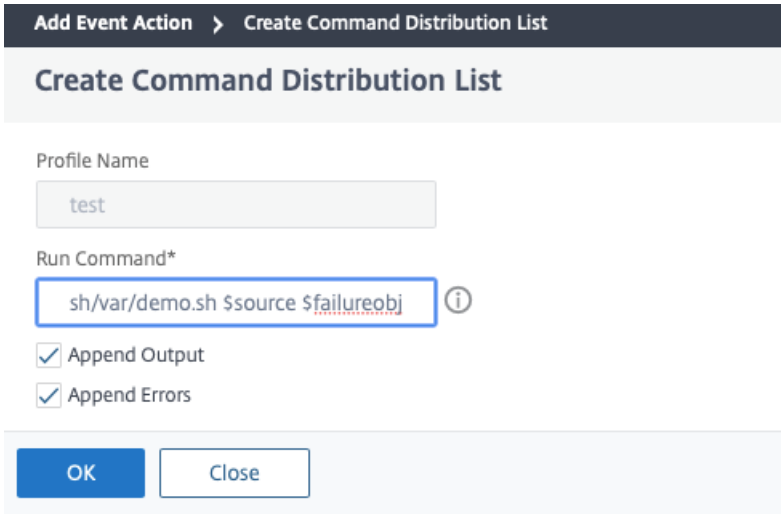
   b) En **Ejecutar comando**, especifique la ubicación del agente de NetScaler ADM, donde debe ejecutarse el script. Por ejemplo: `/sh/var/demo.sh $source $failureobj`.

   c) Seleccione **Anexar salida** y **Anexar errores**

   > **Nota**
   >
   > Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor NetScaler ADM. Si no habilita estas opciones, NetScaler ADM descarta todas las salidas y errores generados al ejecutar el script.

   d) Haga clic en **Crear**.

8. En la página **Agregar acción de evento**, haga clic en **Aceptar**.




> **Nota**
>
> Puede habilitar las opciones **Anexar salida** y **Anexar errores** si quiere almacenar la salida y los errores generados (si los hay) al ejecutar un script en los archivos de registros del servidor NetScaler ADM. Si no habilita estas opciones, NetScaler ADM descarta todas las salidas y errores generados al ejecutar el script.

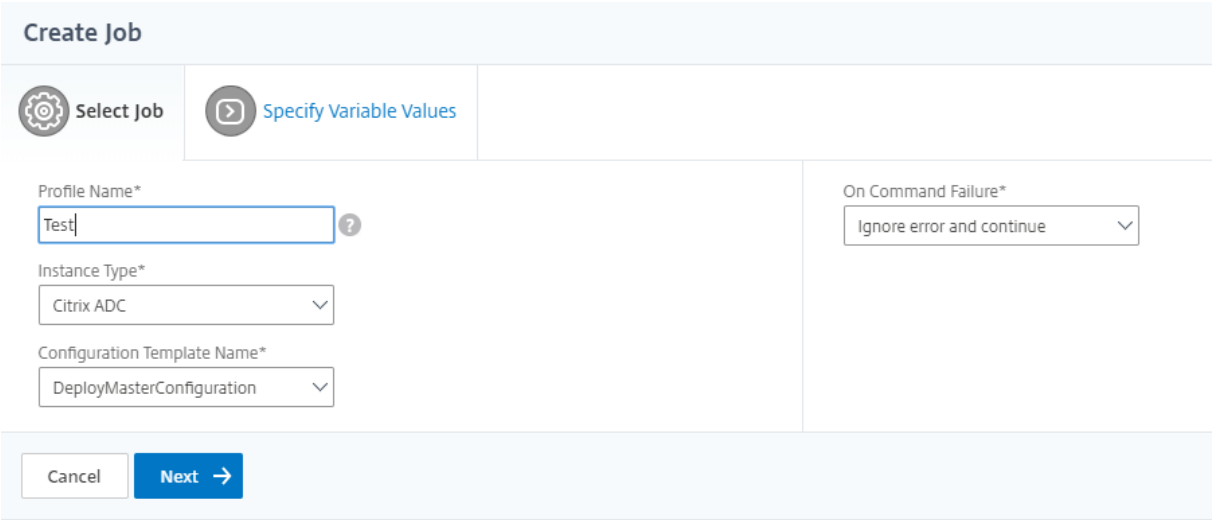
### Para establecer la acción de trabajo `Execute`

Al crear un perfil con trabajos de configuración, un trabajo se ejecuta como un trabajo integrado o un trabajo personalizado para las instancias de NetScaler ADC, NetScaler ADC SDX y Citrix SD-WAN WO,

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

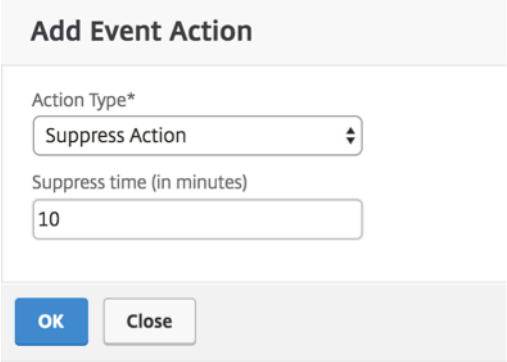
para eventos y alarmas que coincidan con los criterios de filtro especificados.

1. En **Acciones de regla de evento**, haga clic en **Agregar acción** y seleccione **Ejecutar acción de trabajo** en la lista desplegable **Tipo de acción**.
2. Cree un perfil con el trabajo que quiera ejecutar cuando los eventos cumplan con los criterios de filtro definidos.
3. Al crear un trabajo, especifique un nombre de perfil, el tipo de instancia, la plantilla de configuración y la acción que quiere realizar si los comandos del trabajo fallan.
4. En función del tipo de instancia seleccionado y de la plantilla de configuración elegida, especifique los valores de las variables y haga clic en **Finalizar** para crear el trabajo.




**Para establecer la acción de supresión**

Al elegir la **acción Suprimir** el evento Acción, puede configurar un período de tiempo, en minutos, durante el cual se suprime o se elimina un evento. Puede suprimir el evento durante un mínimo de 1 minuto.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para configurar notificaciones de Slack desde NetScaler ADM**

Configure el canal de Slack requerido proporcionando el nombre del perfil y la URL de webhook en la GUI de NetScaler ADM. Las notificaciones de eventos se envían a este canal. Puede configurar varios canales de Slack para recibir estas notificaciones

1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Reglas** y haga clic en **Agregar** para crear una regla.
2. En la página **Crear regla**, defina los parámetros de la regla, como la gravedad y la categoría. Seleccione las instancias y también los objetos de error que deben supervisarse.
3. En**Acciones de reglas de eventos**, haga clic en**Agregar acción**. A continuación, selecciona**Enviar notificaciones de Slack**en la lista de**tipos de acción** y selecciona Lista de **perfiles de Slack**.
4. También puede agregar una lista de perfiles de Slack haciendo clic en **Agregar** junto al campo **Lista de perfiles de Slack**.
5. Escriba los siguientes parámetros para crear una lista de perfiles:
   a) **Nombre del perfil**. Escriba un nombre para la lista de perfiles que se configurará en NetScaler ADM
   b) **Nombre del canal**. Escribe el nombre del canal de Slack al que se van a enviar las notificaciones de eventos.
   c) **URL del webhook**. Escribe la URL del Webhook del canal que has introducido anteriormente. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal y todas las notificaciones de eventos se envían a esta URL para que se publiquen en el canal de Slack designado. Un ejemplo de webhook es el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. Haga clic en **Crear** y haga clic en **Aceptar** en la ventana **Agregar acción de evento**.

> **Nota:**
>
> También puede agregar los perfiles de Slack desde **Sistema** > **Notificaciones** > Perfiles de **Slack**. Haga clic en **Agregar** y cree el perfil como se describe en la sección anterior.

Puede ver el estado de los perfiles de Slack que ha creado.

La regla de evento se crea ahora con filtros apropiados y acciones de regla de evento bien definidas.

**Para establecer notificaciones de PagerDuty desde NetScaler ADM**

Puede agregar un perfil de PagerDuty como opción en NetScaler ADM para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

notificaciones por correo electrónico, SMS, notificaciones push y llamadas telefónicas a un número registrado.

Antes de agregar un perfil de PagerDuty en NetScaler ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para obtener más información, consulte la documentación de PagerDuty.

Puede seleccionar su perfil de PagerDuty como una de las opciones para recibir notificaciones de las siguientes funciones:

- **Eventos**: lista de eventos que se generan para las instancias de NetScaler ADC.
- **Licencias**: lista de licencias que están actualmente activas, a punto de caducar, etc.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias NetScaler ADC.

**Para agregar un perfil de PagerDuty en ADM:**

1. Inicie sesión en NetScaler ADM mediante credenciales de administrador.
2. Vaya a **Sistema** > **Notificaciones** > **Perfiles de PagerDuty** .
3. Haga clic en **Agregar** para crear un nuevo perfil.
4. En la página Crear Perfil de PagerDuty:

   a) Proporcione un nombre de perfil de su elección.

   b) Introduzca la **clave de integración**.

      Puede obtener la clave de integración en su portal de PagerDuty.

   c) Haga clic en **Crear**.

   **Caso de uso**:

   Considere un caso que:

   - quiere enviar notificaciones a su perfil de PagerDuty.
   - han configurado la llamada telefónica como una opción en PagerDuty para recibir notificaciones.
   - quiere recibir alertas de llamadas telefónicas para eventos de NetScaler ADC.

   Para llevar a cabo la configuración:

   a) Diríjase a **Eventos** > **Reglas**

   b) En la página **Crear regla**, configure todos los demás parámetros para crear una regla.

   c) En **Crear acciones de regla**, haga clic en **Agregar acción**.

      Aparece la página **Agregar acción de evento**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

i. En **Tipo de acción**, seleccione **Enviar notificaciones de PagerDuty**.

ii. Seleccione su perfil de PagerDuty y haga clic en **Aceptar**.

Una vez completada la configuración, cada vez que se genere un nuevo evento para la instancia de NetScaler ADC, recibirá una llamada telefónica. Desde la llamada telefónica, puede decidir:

- Reconoce el evento
- Marcarlo como resuelto
- Escalar a otro miembro del equipo

**Para generar automáticamente incidentes de ServiceNow desde NetScaler ADM**

Puede generar automáticamente incidentes de ServiceNow para eventos de NetScaler ADM seleccionando el perfil de ServiceNow en la GUI de NetScaler ADM. Debe elegir el perfil ServiceNow en NetScaler ADM para configurar una regla de eventos.

Antes de configurar una regla de evento para generar automáticamente incidentes de ServiceNow, integre NetScaler ADM con una instancia de ServiceNow. Para obtener más información, consulte Configurar el adaptador ITSM para ServiceNow.

Para configurar una regla de evento, vaya a **Eventos** > **Reglas**.

1. En la página **Crear regla**, configure todos los demás parámetros para crear una regla.
2. En **Crear acciones de regla**, haga clic en **Agregar acción**.

   Aparece la página **Agregar acción de evento**.

   a) En **Tipo de acción**, seleccione **Enviar notificaciones de ServiceNow**.

   b) En el **perfil de ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.

   c) Haga clic en **Aceptar**.

## Modificar la gravedad reportada de los eventos que se producen en instancias de NetScaler ADC

January 30, 2024

Puede gestionar los informes de eventos generados en todos sus dispositivos, de modo que pueda ver los detalles de los eventos relacionados con un evento en particular en una instancia determinada y ver los informes en función de la gravedad del evento. Puede crear reglas de eventos que usen la

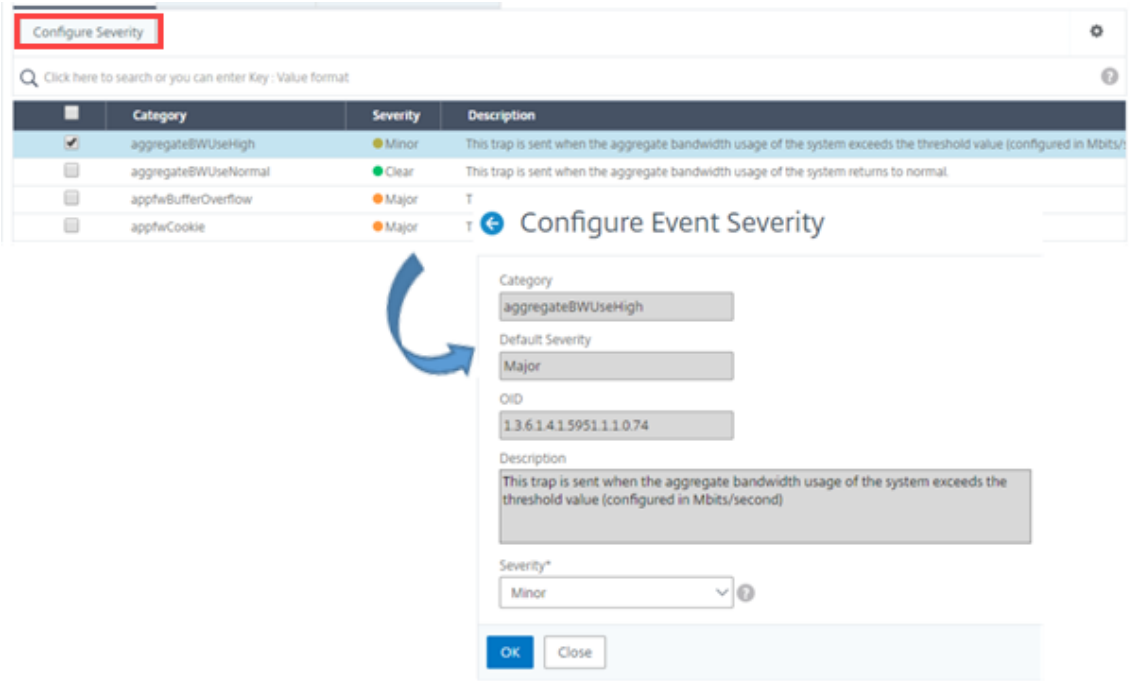
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

configuración de gravedad predeterminada y puede cambiar la configuración de gravedad. Puede configurar la gravedad para eventos genéricos y específicos de la empresa.

Puede definir los siguientes niveles de gravedad: Crítico, Mayor, Menor, Advertencia y Borrar.

**Para modificar la gravedad del evento:**

1. Vaya a **Redes > Eventos > Configuración de eventos**.
2. Haga clic en la ficha del tipo de instancia de Citrix Application Delivery Controller (ADC) que quiere modificar. A continuación, seleccione la categoría de la lista y haga clic en **Configurar gravedad**.
3. En **Configurar la gravedad del evento**, seleccione el nivel de gravedad en la lista desplegable.
4. Haga clic en **Aceptar**.



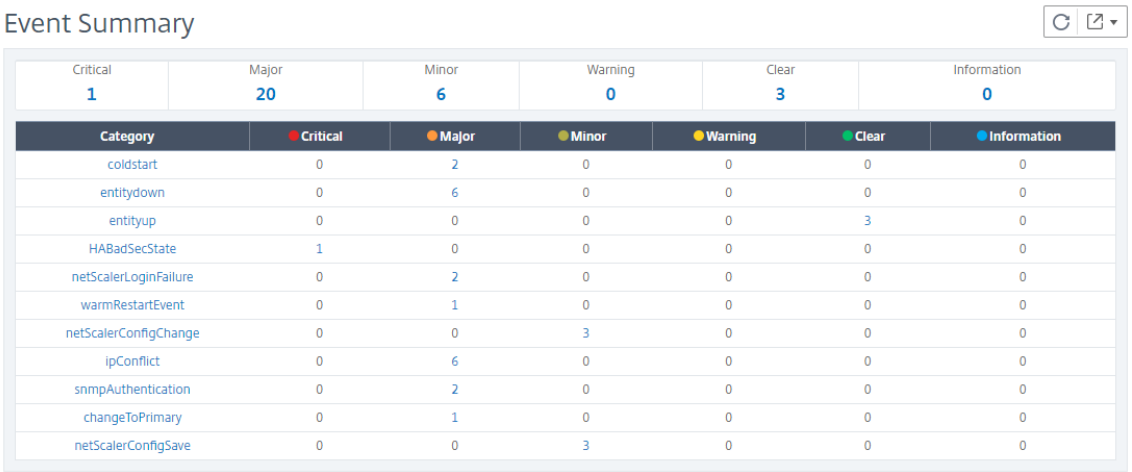

## Ver resumen de eventos

January 30, 2024

Ahora puede ver una página Resumen de eventos para supervisar los eventos y las capturas recibidas en el servidor NetScaler Application Delivery Management (ADM). Vaya a **Redes** > **Eventos** . La página Resumen de Eventos muestra la siguiente información en formato de tabla:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Resumen de todos los eventos recibidos por NetScaler ADM**. Los eventos se enumeran por categoría y sus diferentes niveles de gravedad se muestran en diferentes columnas: Crítico, Principal, Menor, Advertencia, Borrar e Información. Por ejemplo, se producirá un evento crítico cuando una instancia de Citrix Application Delivery Controller (ADC) se desactiva y deja de enviar información al servidor NetScaler ADM. Durante el evento, se envía una notificación a un administrador en la que se explica el motivo por el que la instancia está inactiva, el tiempo durante el cual ha estado inactiva, etc. A continuación, el evento se registra en la página Resumen de eventos, en la que puede ver un resumen y acceder a los detalles del evento.

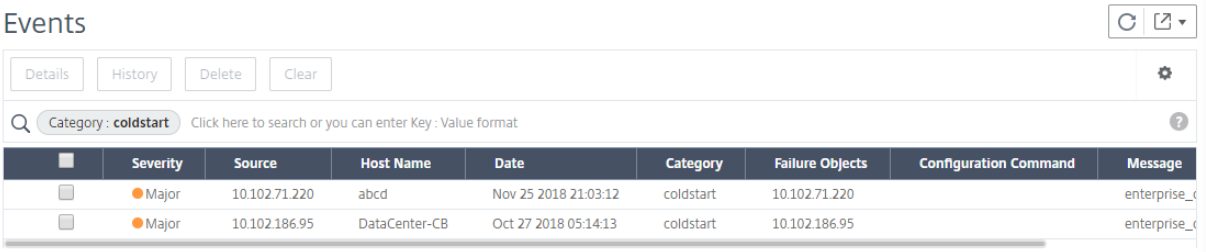



| Critical | Major | Minor | Warning | Clear | Information |
|---|---|---|---|---|---|
| 1 | 20 | 6 | 0 | 3 | 0 |

| Category | Critical | Major | Minor | Warning | Clear | Information |
|---|---|---|---|---|---|---|
| coldstart | 0 | 2 | 0 | 0 | 0 | 0 |
| entitydown | 0 | 6 | 0 | 0 | 0 | 0 |
| entityup | 0 | 0 | 0 | 0 | 3 | 0 |
| HABadSecState | 1 | 0 | 0 | 0 | 0 | 0 |
| netScalerLoginFailure | 0 | 2 | 0 | 0 | 0 | 0 |
| warmRestartEvent | 0 | 1 | 0 | 0 | 0 | 0 |
| netScalerConfigChange | 0 | 0 | 3 | 0 | 0 | 0 |
| ipConflict | 0 | 6 | 0 | 0 | 0 | 0 |
| snmpAuthentication | 0 | 2 | 0 | 0 | 0 | 0 |
| changeToPrimary | 0 | 1 | 0 | 0 | 0 | 0 |
| netScalerConfigSave | 0 | 0 | 3 | 0 | 0 | 0 |

- **Número de trampas recibidas para cada categoría**. El número de trampas recibidas, clasificadas por gravedad. De forma predeterminada, cada captura enviada desde instancias de NetScaler ADC a NetScaler ADM tiene asignada una gravedad, pero como administrador de red, puede especificar su gravedad en la GUI de NetScaler ADM.

Si hace clic en un tipo de categoría o una captura, se le lleva a la página **Eventos**, en la que se preseleccionan filtros como Categoría y Gravedad. Esta página muestra más información sobre el evento, como la dirección IP y el nombre del host de la instancia de NetScaler ADC, la fecha en la que se recibió la captura, la categoría, los objetos de error, la ejecución del comando de configuración y la notificación del mensaje.




| Severity | Source | Host Name | Date | Category | Failure Objects | Configuration Command | Message |
|---|---|---|---|---|---|---|---|
| Major | 10.102.71.220 | abcd | Nov 25 2018 21:03:12 | coldstart | 10.102.71.220 | | enterprise_ |
| Major | 10.102.186.95 | DataCenter-CB | Oct 27 2018 05:14:13 | coldstart | 10.102.186.95 | | enterprise_ |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Mostrar severidades de eventos y detalles de capturas SNMP

January 30, 2024

Al crear un evento y su configuración en Citrix Application Delivery Management (ADM), puede ver el evento inmediatamente en la página Resumen del evento. Del mismo modo, puede ver y supervisar el estado, el tiempo de actividad, los modelos y las versiones de todas las instancias de Citrix Application Delivery Controller (ADC) agregadas a su servidor Citrix ADM con todo detalle en Infrastructure Dashboard.

En el panel Infraestructura, ahora puede enmascarar valores irrelevantes para que pueda ver y supervisar con más facilidad información como eventos por severidades, estado, tiempo de actividad, modelos y versión de instancias de NetScaler ADC en detalle.

Por ejemplo, los eventos con un nivel de gravedad **crítico** pueden ocurrir con poca frecuencia. Sin embargo, cuando se produzcan estos eventos críticos en la red, es posible que quiera investigar más a fondo, solucionar problemas y supervisar dónde y cuándo ocurrió el evento. Si selecciona todos los niveles de gravedad excepto Crítico, el gráfico muestra solo las ocurrencias de eventos críticos. Además, al hacer clic en el gráfico, se le dirigirá a la página **Eventos basados en gravedad**, donde puede ver todos los detalles sobre cuándo se produjo un evento crítico durante el tiempo que ha seleccionado: el origen de la instancia, la fecha, la categoría y la notificación de mensaje enviada cuando se produjo el evento crítico.

Del mismo modo, puede ver el estado de una instancia de Citrix VPX en el Panel de control. Puede enmascarar el tiempo durante el cual la instancia estaba en funcionamiento y en ejecución, y mostrar solo las veces que la instancia estuvo fuera de servicio. Al hacer clic en el gráfico, se le lleva a la página de esa instancia, donde el filtro *fuera de servicio* ya está aplicado, y ver detalles como el nombre de host, el número de solicitudes HTTP recibidas por segundo, el uso de CPU, etc. También puede seleccionar la instancia y ver el panel de control de la instancia de Citrix en particular para obtener más detalles.

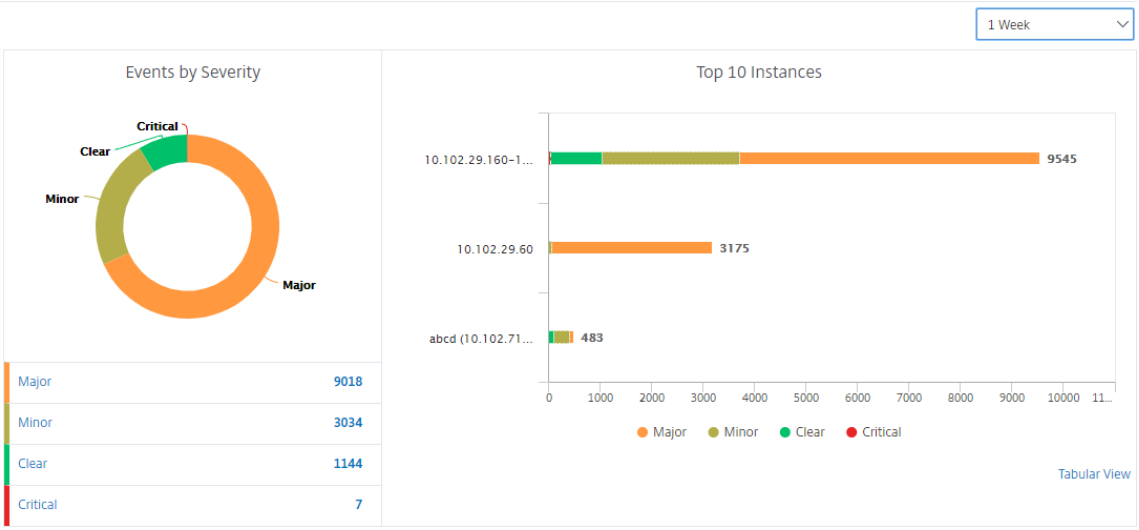
**Para seleccionar eventos específicos por gravedad en NetScaler ADM:**

1. Inicie sesión en NetScaler ADM con sus credenciales de administrador.
2. Vaya a **Redes > Panel de control**.

   O bien:

   Vaya a **Redes > Eventos > Informes**.
3. En el menú de la esquina superior derecha de la página, seleccione la duración para la que quiere ver los eventos por gravedad.

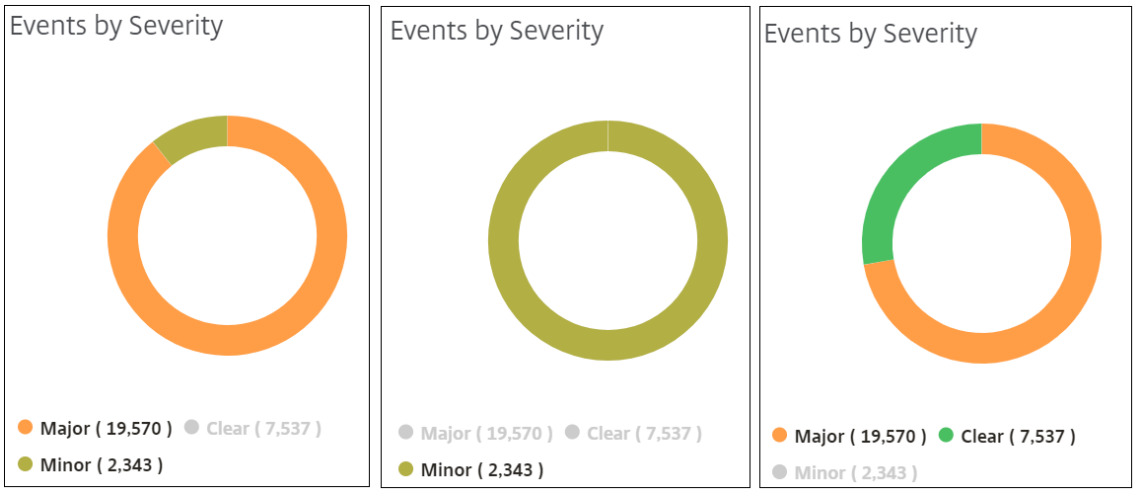
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. El gráfico de donut **Eventos por gravedad**muestra una representación visual de todos los eventos según su gravedad. Los diferentes tipos de eventos se representan como secciones de colores diferentes, y la longitud de cada sección corresponde al número total de eventos de ese tipo de gravedad.
5. Puede hacer clic en cada sección del gráfico de donut para mostrar la página de **eventos basados en gravedad** correspondiente, que muestra los siguientes detalles de la gravedad seleccionada para la duración seleccionada:
   - Origen de instancia
   - Datos del evento
   - Categoría de eventos generados por la instancia de NetScaler ADC
   - Notificación de mensaje enviada

> **Nota**
>
> Debajo del gráfico de rosquillas se puede ver una lista de las severidades que se representan en el gráfico. De forma predeterminada, un gráfico de donut muestra todos los eventos de todos los tipos de gravedad y, por lo tanto, se resaltan todos los tipos de gravedad de la lista. Puede alternar los tipos de gravedad para ver y supervisar más fácilmente la gravedad elegida.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Para ver los detalles de la captura SNMP de NetScaler ADC en NetScaler ADM:**

Ahora puede ver los detalles de cada captura SNMP recibida de sus instancias de NetScaler ADC administradas en el servidor NetScaler ADM en la página **Configuración de eventos**. Vaya a **Redes** > **Eventos** > **Configuración** de eventos . Para una captura específica recibida de su instancia, puede ver los siguientes detalles en formato tabular:

- **Categoría**: Especifica la categoría de la instancia a la que pertenece el evento.
- **Gravedad**: la gravedad del evento se indica mediante los colores y el tipo de gravedad.
- **Descripción**: especifica los mensajes asociados al evento.

Por ejemplo, en un evento con la categoría de captura **monRespTimeoutBelowThresh**, la descripción de la trampa aparece como "Esta captura se envía cuando el tiempo de espera de respuesta de una sonda de monitor vuelve a la normalidad, inferior al umbral establecido".

## Ver y exportar mensajes syslog de Citrix ADC

January 30, 2024

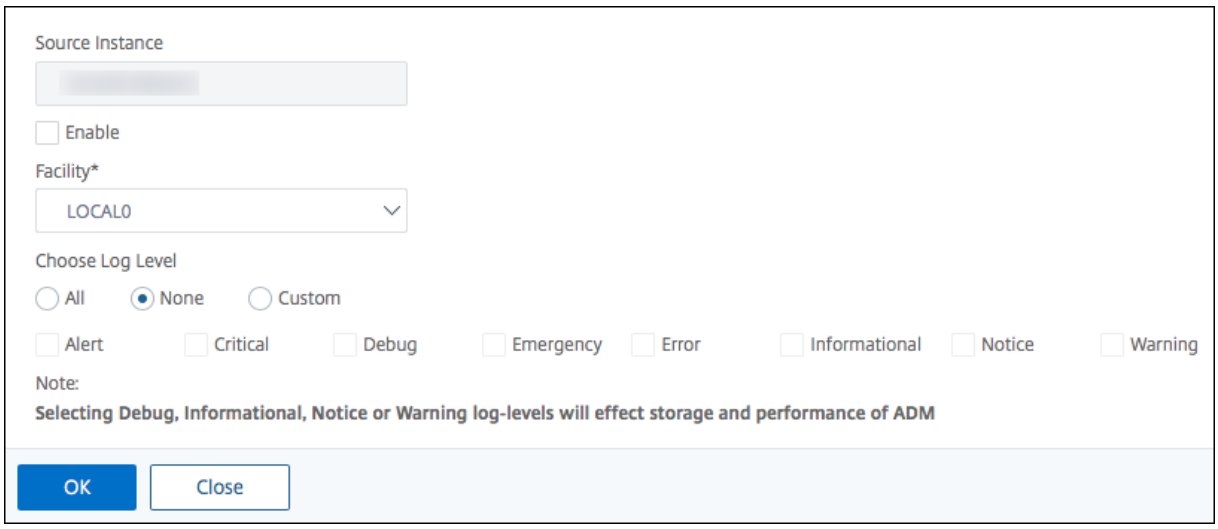
Desde el software ADM, puede supervisar los eventos syslog generados en las instancias de Citrix Application Delivery Controller (ADC). Para ello, debe configurar ADM como servidor syslog para las instancias de Citrix ADC. Después de configurar ADM, todos los mensajes syslog se redirigen de las instancias de ADC a ADM.

### Configurar ADM como servidor syslog

Siga estos pasos para configurar ADM como el servidor syslog:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Desde la GUI de ADM, vaya a **Redes > Instancias**.
2. Seleccione la instancia de Citrix ADC desde la que quiere que se recopilen y muestren los mensajes syslog en Citrix ADM.
3. En la lista **Seleccionar acción**, seleccione **Configurar Syslog**.
4. Haga clic en **Activar**.
5. En la lista desplegable de **instalaciones**, seleccione una instalación local o a nivel de usuario.
6. Seleccione el nivel de registro requerido para los mensajes de syslog.
7. Haga clic en **Aceptar**.



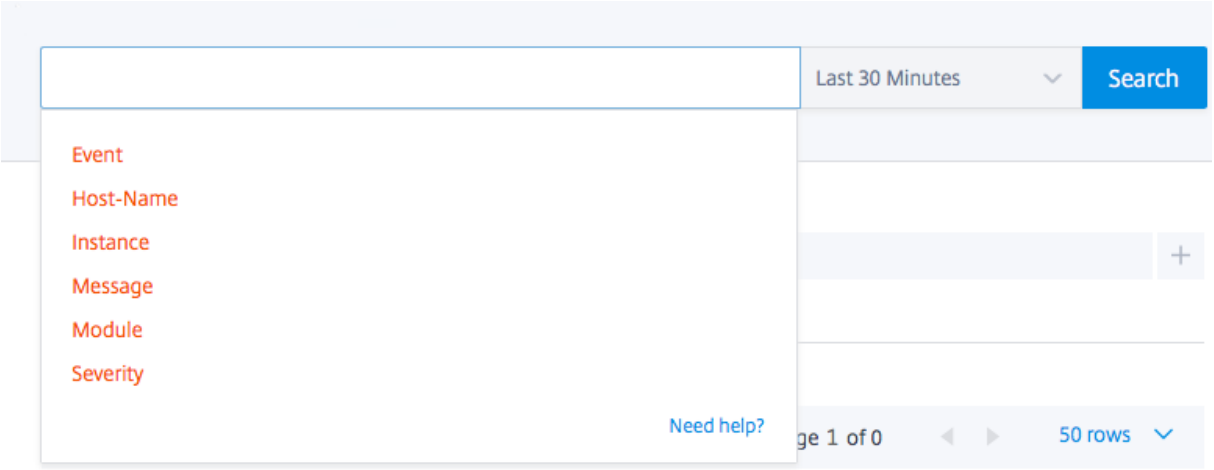

Estos pasos configuran todos los comandos syslog en la instancia de Citrix ADC y Citrix ADM comienza a recibir los mensajes syslog.

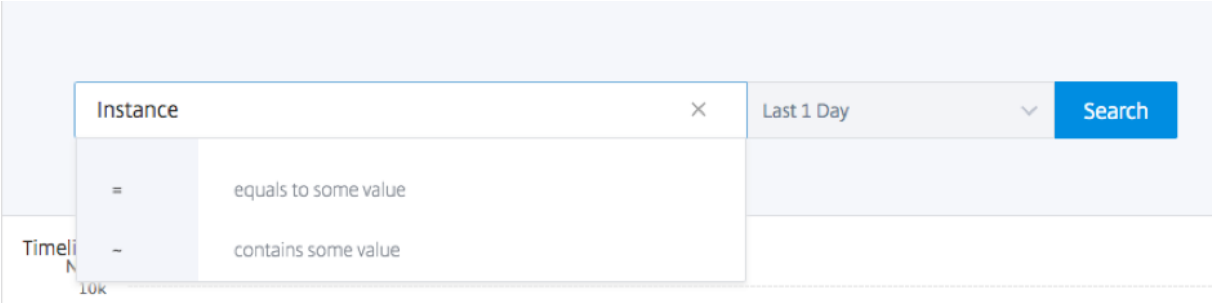
## Ver y buscar mensajes de syslog

Puede ver todos los mensajes de syslog generados en las instancias administradas de Citrix ADC. Los mensajes syslog se almacenan en la base de datos de forma centralizada y están disponibles en **Redes > Eventos > Mensajes de Syslog** para fines de auditoría. Puede combinar esta información de registro y derivar informes para análisis a partir de los datos recopilados.

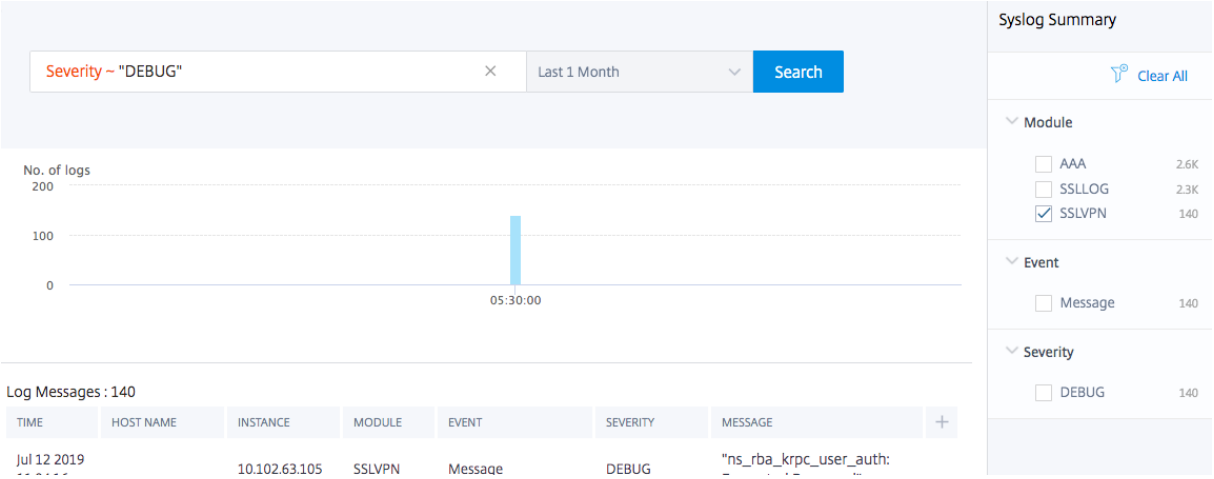
Además, puede usar filtros para reducir los resultados de búsqueda de mensajes syslog y encontrar exactamente lo que está buscando y en tiempo real. Haga clic en **¿Necesita ayuda?** para abrir la ayuda de búsqueda integrada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




A continuación, agregue el término de búsqueda. Para algunas categorías, se muestra una lista precompletada de términos de búsqueda. De forma predeterminada, el tiempo de búsqueda es de 1 día. Puede cambiar la hora y el intervalo de fechas haciendo clic en la flecha hacia abajo. Puede restringir aún más la búsqueda seleccionando opciones en el panel **Resumen de Syslog**.



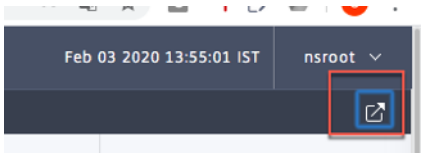

## Exportar y programar mensajes syslog

Puede ver los mensajes syslog sin iniciar sesión en ADM, programando una exportación de todos los mensajes syslog recibidos en el servidor. Puede exportar mensajes syslog generados en las instan-

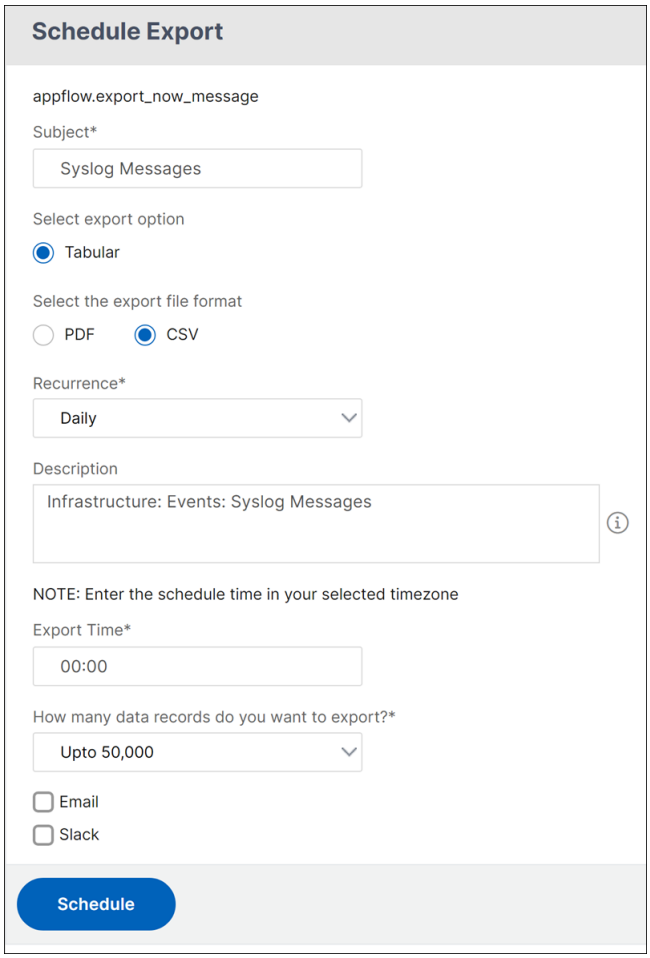
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

cias de ADC en formatos PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico o cuenta de Slack especificadas a intervalos diferentes.

Para exportar y programar los mensajes de registro, haga clic en el icono de flecha situado en la esquina superior derecha.




- Para exportar los mensajes de registro, haga clic en **Exportar informes > Exportar ahora**, seleccione el formato requerido y, a continuación, haga clic en **Exportar**.
- Para programar la exportación de mensajes syslog, haga clic en **Exportar informes > Programar informe**y defina los parámetros necesarios. Puede recibir el informe por correo electrónico o Slack.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Suprimir mensajes de syslog

January 30, 2024

Cuando se configura como un servidor syslog, Citrix Application Delivery Management (ADM) recibe todos los mensajes syslog que le envían las instancias configuradas de Citrix Application Delivery Controller (ADC). Es posible que haya una gran cantidad de mensajes que quizás no desee ver. Por ejemplo, puede que no le interese ver todos los mensajes de nivel informativo. Ahora puede descartar algunos de los mensajes syslog que no le interesan. Puede suprimir algunos de los mensajes de syslog que llegan a NetScaler ADM configurando algunos filtros. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler ADM y estos mensajes tampoco se almacenan en la base de datos de NetScaler ADM del cliente.

Puede suprimir algunos de los mensajes de syslog registrados que llegan a NetScaler ADM configurando algunos filtros. Los dos filtros que se pueden utilizar para suprimir mensajes syslog son gravedad y facilidad. También puede suprimir los mensajes procedentes de una instancia concreta de NetScaler ADC o de varias instancias. También puede proporcionar un patrón de texto para que NetScaler ADM busque y suprima mensajes. Citrix ADM elimina todos los mensajes que coinciden con los criterios. Estos mensajes descartados no aparecen en la GUI de NetScaler ADM y estos mensajes tampoco se almacenan en la base de datos del cliente. Por lo tanto, se ahorra una buena cantidad de espacio en el servidor de almacenamiento.

Algunos casos de uso para suprimir los mensajes de syslog son los siguientes:

- Si quiere ignorar todos los mensajes de nivel de información, suprima el nivel 6 (informativo)
- Si solo quiere registrar las condiciones de error del firewall, suprima todos los niveles que no sean el nivel 3 (errores)

## Supresión de mensajes de syslog mediante la creación de filtros

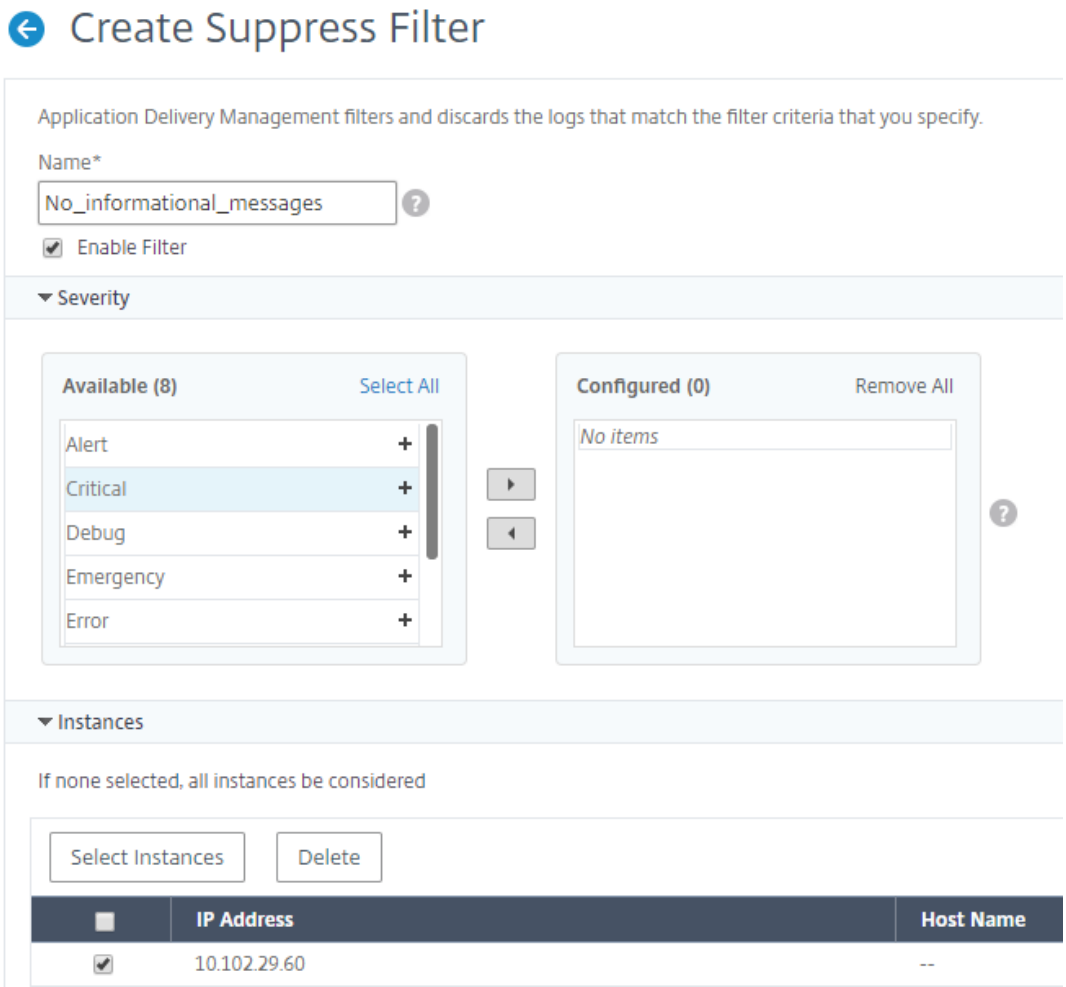
1. En Citrix ADM, vaya a **Redes** > **Eventos** > **Mensajes de Syslog** > **Filtro de supresión**.
2. En la página **Crear filtro de supresión**, actualice la siguiente información:
   a) **Nombre**: Escriba un nombre para el filtro.

   > **Nota:**
   >
   > Si los diferentes usuarios tienen diferentes accesos a varias instancias de NetScaler ADC, se deben crear diferentes filtros para diferentes instancias, ya que los usuarios solo pueden ver los filtros en los que tienen acceso a todas las instancias.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) **Gravedad**: Seleccione y agregue los niveles de registro para los que debe suprimir los mensajes. Por ejemplo, si no quiere ver ningún mensaje informativo que llegue, puede seleccionar Informativo para suprimirlos.

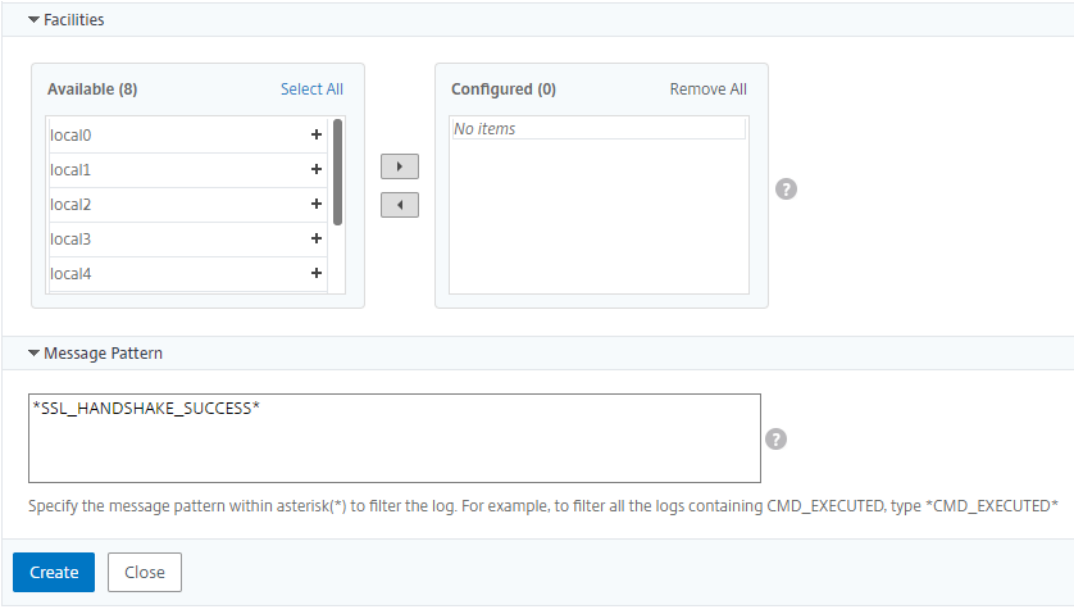
c) **Instancias**: Seleccione las instancias NetScaler ADC en las que se han configurado los mensajes syslog.




d) **Instalaciones**: Seleccione la función para suprimir los mensajes en función de la fuente que los genera.

e) **Patrón de mensajes**: También puede escribir un patrón de texto rodeado de un asterisco (*) para suprimir los mensajes. En los mensajes se busca la cadena de patrón de texto y se suprimen los mensajes que contienen este patrón.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Inhabilitar el filtro

Para permitir que los mensajes se vean en NetScaler ADM, debe inhabilitar el filtro.

1. Vaya a **Redes** > **Eventos** > **Mensajes de Syslog** > **Suprimir filtro** y, en la página **Suprimir filtro** , seleccione el filtro y haga clic en **Editar**.
2. En la página **Configurar suprimir filtro**, desactive la casilla de verificación **Habilitar filtro** para inhabilitar el filtro.

## Configurar los parámetros de poda para eventos de instancia

January 30, 2024

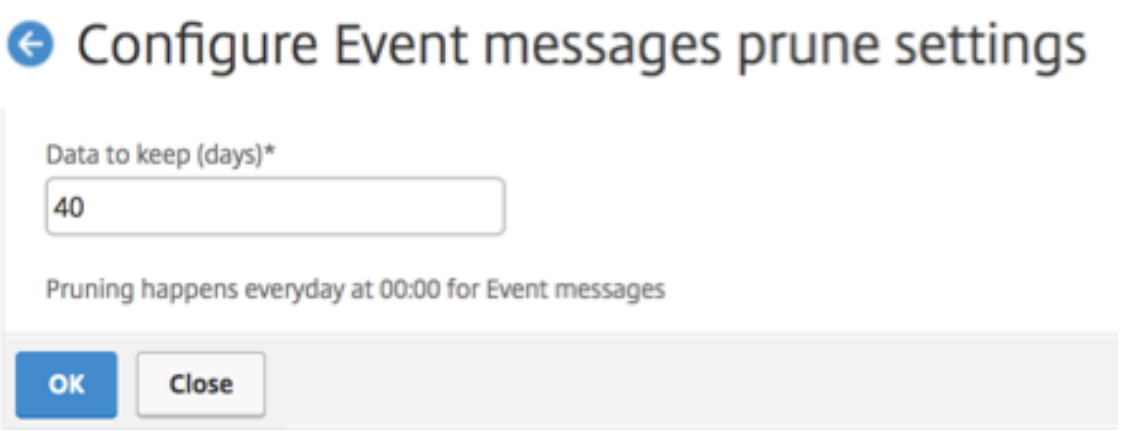
Las instancias de Citrix Application Delivery Controller (ADC) administradas por el servidor Citrix Application Delivery Management (ADM) envían datos de mensajes de eventos de forma continua para almacenarlos en Citrix ADM. Puede especificar el intervalo para el que quiere que NetScaler ADM conserve datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

> **Nota**
>
> El valor que puede especificar no puede superar los 40 días ni ser inferior a 1 día.

**Para configurar los parámetros de poda para eventos de instancia:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Sistema**>**Administración del sistema**.
2. En **Configuración de poda**, haga clic en Configuración de **poda de eventos** de **instancia** .
3. Introduzca el intervalo de tiempo, en días, para el que desea conservar los datos en el servidor Citrix ADM **y** haga clic en Aceptar.




## Administración de certificados SSL

January 30, 2024

Cualquier organización o sitio web individual que requiera el manejo de información confidencial o confidencial debe tener un certificado SSL. El certificado SSL en un servidor web ayuda a garantizar la autenticidad del servidor web al cliente conectado. No solo autentica la identidad de un sitio web, sino que también ayuda a generar la clave de sesión, que se utiliza posteriormente para el cifrado de toda la sesión.

Un certificado Secure Socket Layer (SSL), que forma parte de cualquier transacción SSL, es un formulario de datos digitales (X509) que identifica a una empresa (dominio) o a un individuo. El certificado tiene un componente de clave pública visible para cualquier cliente que quiera iniciar una transacción segura con el servidor. La clave privada correspondiente, que reside de forma segura en el dispositivo Citrix Application Delivery Controller (ADC), se utiliza para completar el cifrado y descifrado de clave asimétrica (o clave pública).

NetScaler Application Delivery Management (ADM) proporciona una consola unificada para automatizar la instalación, actualización, eliminación, vinculación y descarga de certificados SSL. Ayuda a conservar la reputación del sitio web y la confianza del cliente. Citrix ADM ahora optimiza todos los aspectos de la administración de certificados por usted. A través de una consola unificada, puede configurar directivas automatizadas para garantizar el emisor recomendado, la fuerza de clave, el

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

protocolo y los algoritmos según las directivas de TI de la organización. Al hacerlo, puede vigilar de cerca los certificados que no se utilizan o que están a punto de caducar.

Puede obtener un certificado y una clave SSL de cualquiera de las siguientes maneras:

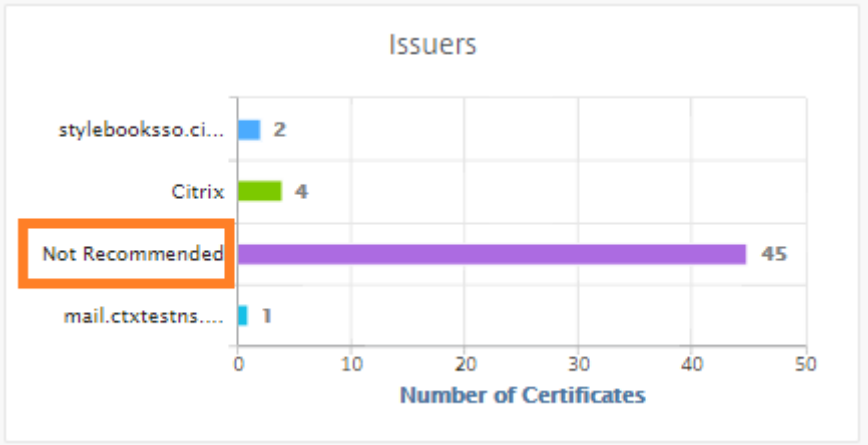
- De una entidad emisora de certificados (CA) autorizada, como Verisign
- Al generar un nuevo certificado SSL y una clave en el dispositivo Citrix ADC

## Configuración de directiva SSL empresarial

Cada empresa tiene su propia directiva SSL y define los requisitos a los que deben cumplir todos los certificados SSL. La seguridad siempre ha sido una de las principales prioridades de todos los usuarios empresariales y, por lo tanto, la configuración SSL desempeña un papel importante.

Por ejemplo, una empresa ABC ordena que todos los certificados deben tener fortalezas clave mínimas de 2.048 bits o superiores. Los certificados deben ser autorizados por entidades emisoras o entidades emisoras de confianza. Los administradores deben comprobar todos estos parámetros SSL para asegurarse de que los certificados cumplen con la directiva de la empresa. Es un trabajo tedioso verificar cada certificado manualmente. Para superar este caso, Citrix ADM le ayuda a configurar la configuración de la directiva SSL empresarial y muestra cualquier certificado de incumplimiento con la etiqueta “No recomendado”.

Puede ver el resumen de los certificados de incumplimiento (no recomendados) en el Panel de control de SSL.



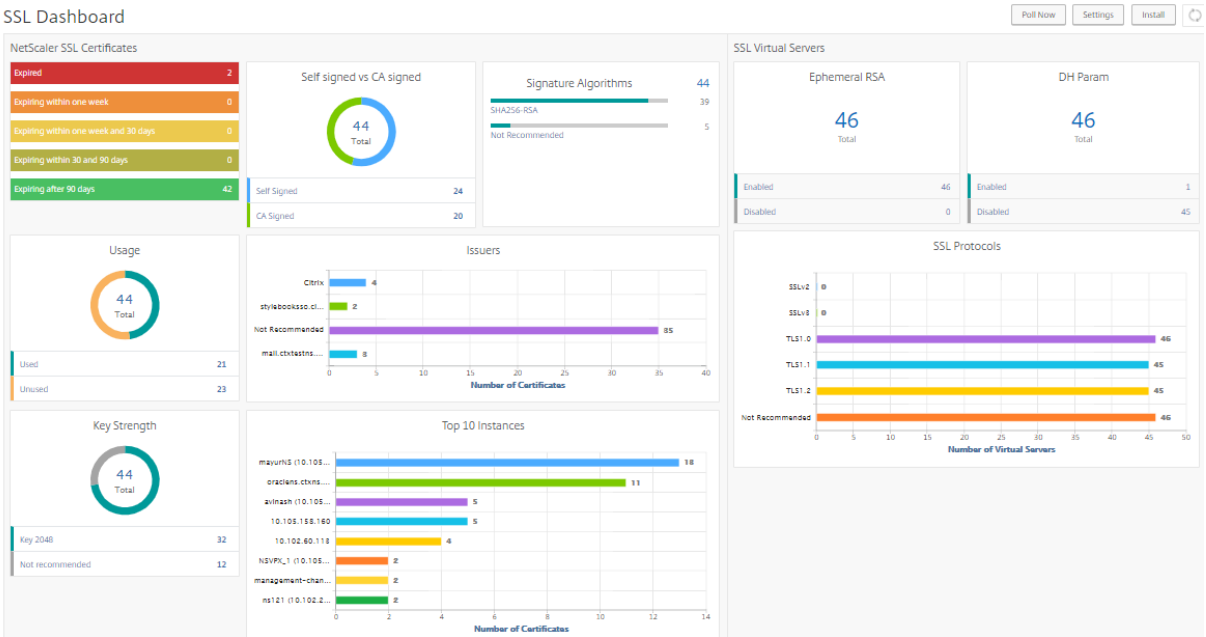

> **Nota**
>
> Los certificados “No recomendados”se clasifican en función de diferentes parámetros, y puede verlos en componentes relevantes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Cómo funciona el certificado Citrix ADM

SSL Dashboard proporciona una presentación visual de todos los certificados SSL instalados en diferentes instancias de Citrix ADC. El panel SSL incluye la siguiente información para cada certificado instalado en instancias de Citrix ADC. Se clasifica en función de lo siguiente:

- **Autofirmada frente a CA firmada.** La sección autofirmada frente a la firma de CA le ayuda a segregar los certificados en certificados autofirmados y certificados firmados por CA.
- **Algoritmos de firma.** Esta sección segrega los certificados SSL en función de los algoritmos de firma que se utilizan para el cifrado.
- **Uso.** Esta sección segrega los certificados SSL en función de certificados usados y no utilizados. Los certificados no utilizados exigen una atención especial, ya que es posible que no se hayan podido enlazar a los servidores virtuales.
- **Emisores.** Esta sección separa los certificados SSL en función del emisor de los certificados.
- **Fuerza de la clave.** Esta sección segrega los certificados SSL en función de la intensidad de clave de una clave privada.
- **Las 10 instancias principales.** Esta sección proporciona los detalles de las 10 instancias principales de Citrix ADC en función del número de certificados SSL instalados.




## Casos de uso de administración de certificados SSL

Los siguientes casos de uso describen cómo puede utilizar el certificado SSL para administrar y supervisar los certificados en varias instancias de Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Instalar certificados SSL

Imagine que tiene una flota de instancias de Citrix ADC en las que debe implementar los certificados SSL requeridos. Citrix ADM proporciona una consola unificada para implementar los certificados SSL en varias instancias de Citrix ADC en un solo intento.

Por ejemplo, es posible que quiera instalar algunos certificados SSL en una o más instancias de Citrix ADC. Con este enfoque, puede minimizar la intervención manual de instalar el certificado SSL en cada instancia de Citrix ADC. Puede realizar una instalación masiva de certificados SSL en una o más instancias de Citrix ADC.

Para obtener un resumen de los certificados SSL, inicie sesión en **Citrix ADM**y, a continuación, vaya a **Redes > Panel de SSL**.

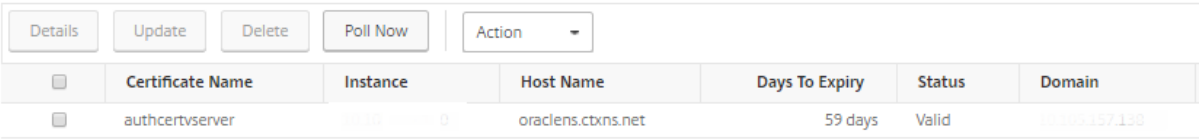
### Configuración de notificación para caducidad del certificado

En este caso de uso, es posible que tenga muchos certificados en varias instancias de Citrix ADC y se convierte en una sobrecarga para realizar el seguimiento de la caducidad de cada certificado. Es un trabajo tedioso para usted realizar un seguimiento manual de cada certificado y actualizarlo antes de que caduque. Para evitar estos casos, puede configurar Citrix ADM para que envíe las notificaciones o alertas a los perfiles configurados de correo electrónico, buscapersonas, Slack o ServiceNow configurados. De esta forma, puede mantenerse al tanto de las fechas de caducidad de los certificados y renovarlos mucho antes de las fechas de caducidad.

Por ejemplo, puede olvidarse de realizar un seguimiento del certificado que está a punto de caducar. Y el certificado caduca causando una interrupción del servicio, lo que podría afectar a numerosas aplicaciones para los usuarios. Con la configuración de notificación de caducidad de certificado ADM, puede evitar estos casos imprevistos.

Puede ver el resumen y realizar un seguimiento de los certificados que están a punto de caducar en el **panel SSL**.

Para ver el informe de certificados que caducan en cualquier duración, puede hacer clic en el mosaico para obtener los detalles de todos los certificados que caducan en esa ventana.




### Renovación de certificados

Ahora puede renovar los certificados desde Citrix ADM. Puede renovar los certificados existentes o crear los certificados basándose en lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

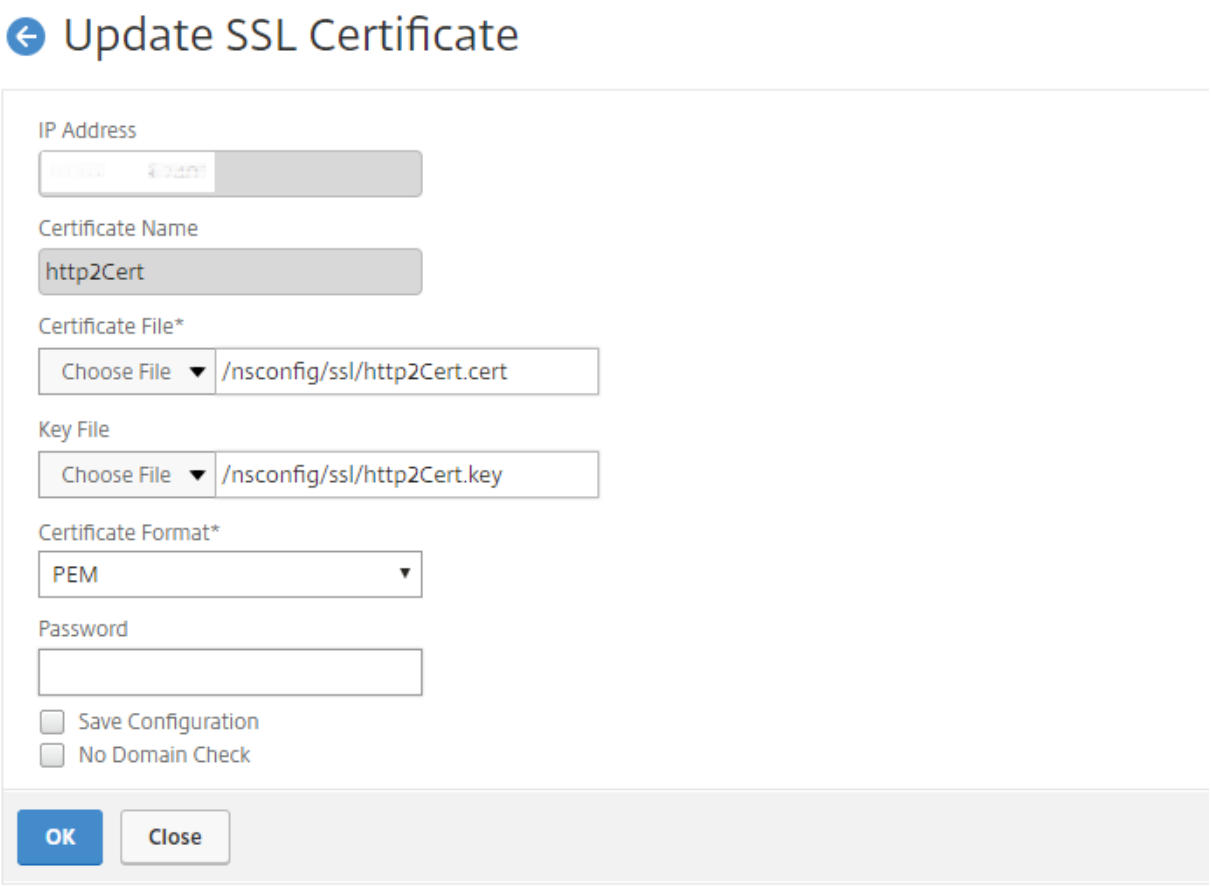
**Actualizar el certificado existente** En este caso de uso, debe actualizar un certificado existente una vez que reciba un certificado renovado de la entidad emisora de certificados (CA). Ahora puede actualizar los certificados existentes desde Citrix ADM sin iniciar sesión en las instancias de Citrix ADC.

Por ejemplo, puede haber algunos cambios o modificaciones en los certificados existentes. La CA emite certificados renovados. En lugar de ir al dispositivo Citrix ADC, ahora puede actualizar el certificado SSL desde Citrix ADM.

Para actualizar cualquier certificado, inicie sesión en Citrix ADM y, a continuación, vaya a **Redes > Panel de SSL**.

Seleccione el certificado que quiere actualizar y haga clic en **Actualizar**.

Tiene la opción de actualizar los campos relevantes del certificado seleccionado de Citrix ADM.

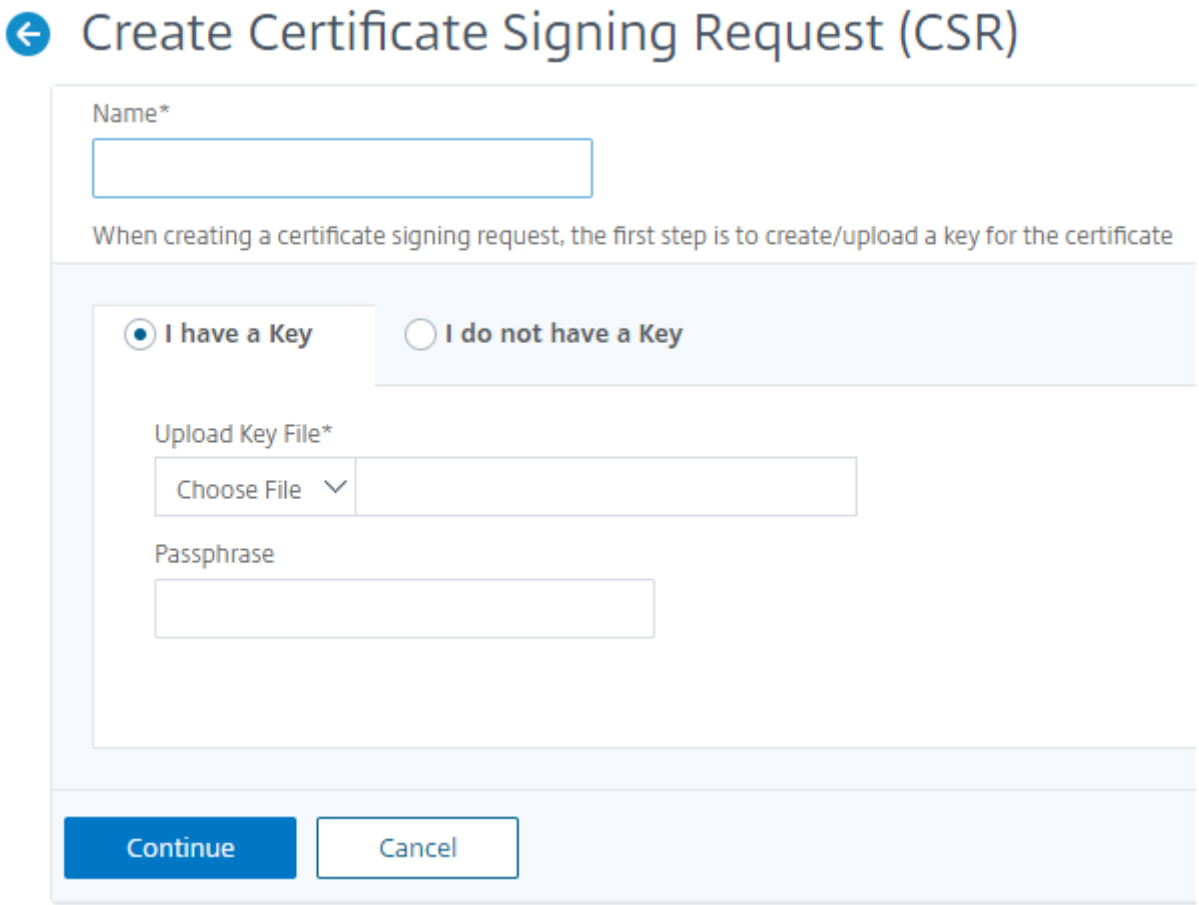



**Crear solicitud de firma de certificado** Imagine un caso de uso en el que uno de los certificados SSL no cumple con las directivas de la organización. Desea obtener un certificado nuevo de la entidad emisora de certificados. Ahora puede generar una solicitud de firma de certificado (CSR) desde Citrix ADM. Una CSR y una clave pública se pueden enviar a una entidad emisora de certificados para obtener el certificado SSL.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

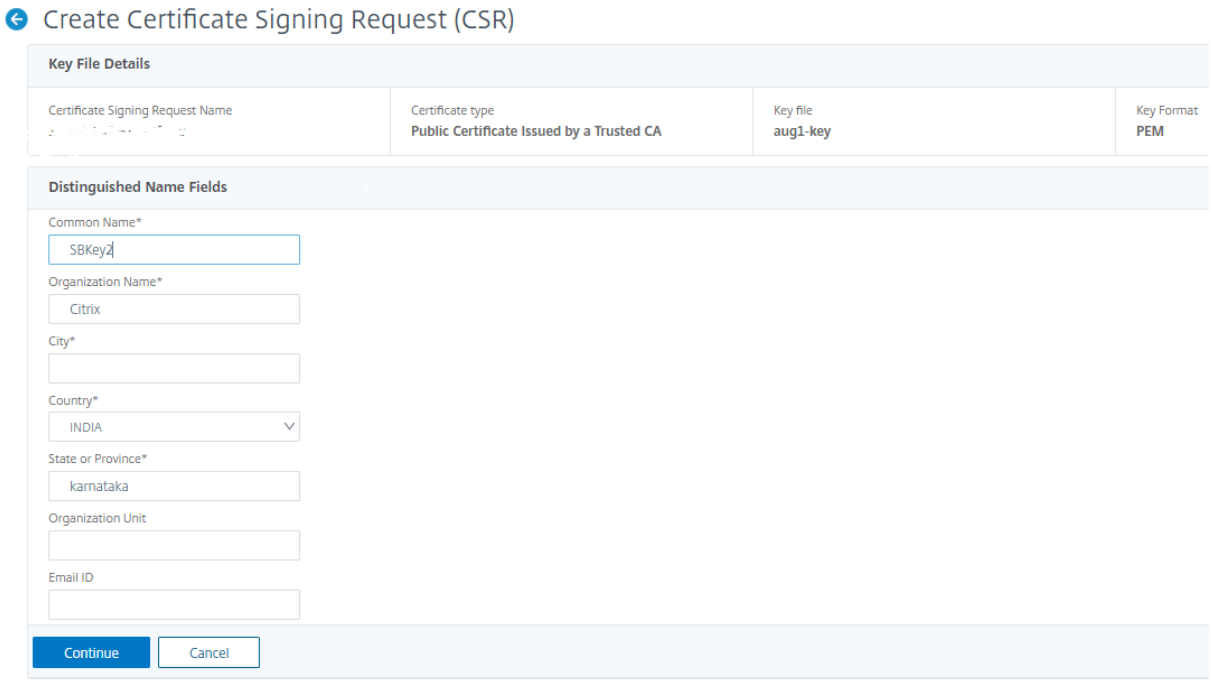
Para determinar y crear CSR, seleccione el certificado deseado y haga clic en **Crear CSR**.

Necesita tener un par de valores de clave pública o privada. Para cargar una clave, haga clic en **Elegir archivo** y selecciónelo en la lista. Para crear una clave, seleccione **No tengo una opción Clave** y especifique los parámetros relevantes.



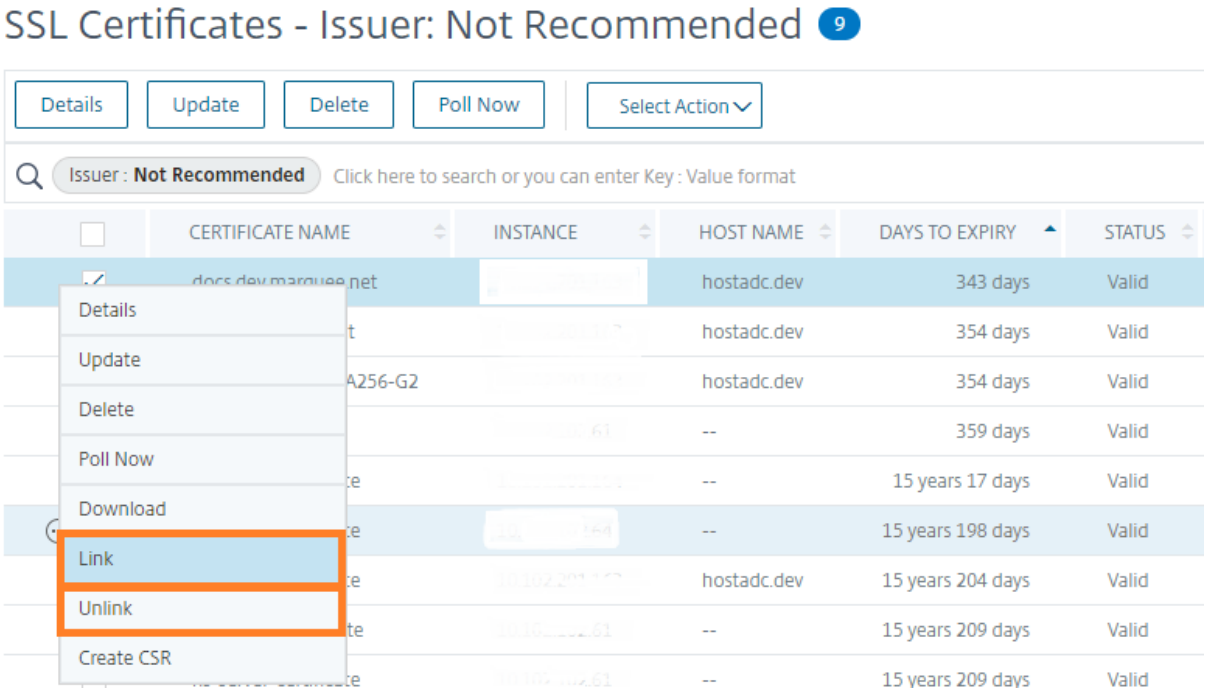

Para proporcionar más detalles de la clave seleccionada, como Nombre común, Nombre de organización, Ciudad, País, Estado, Unidad organizativa e ID de correo electrónico para crear la CSR.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Vincular y desvincular certificados SSL

Puede enlazar varios certificados SSL entre sí para crear un paquete de certificados. Para vincular un certificado a otro certificado, el emisor del primer certificado debe coincidir con el dominio del segundo certificado.



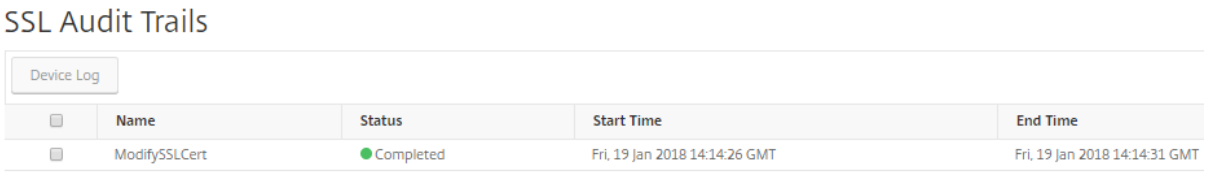

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Registros de auditoría

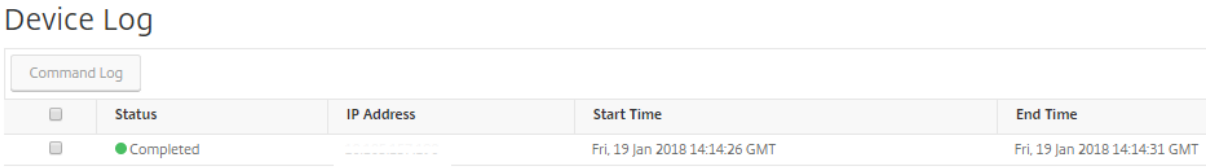
Registros de auditoría es una colección de archivos de registro de texto generados por Citrix ADM. Muestra un historial de certificados SSL que se agregan, modifican y modifican mediante Citrix ADM al dispositivo Citrix ADC específico. Los registros de auditoría también muestran la dirección IP del dispositivo Citrix ADC, el estado, la hora de inicio y la hora de finalización de la operación concreta.

En este ejemplo, es posible que quiera comprobar el cambio que se ha producido durante un período en el certificado concreto. Además, tiene una opción para ver el historial de cambios en el certificado a través del registro de dispositivos y el registro de comandos.

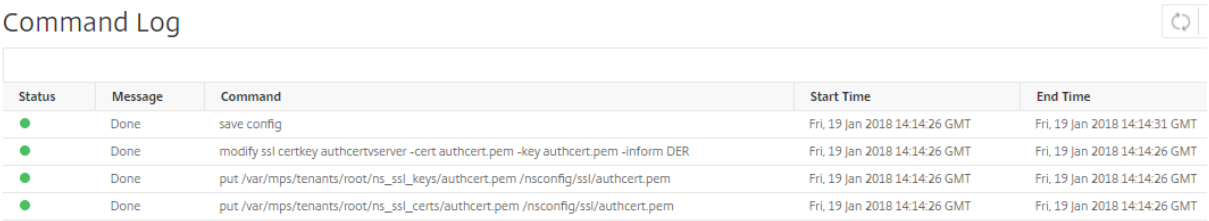
Para determinar la información de los certificados SSL, en el **Panel de control de SSL**, haga clic en **Registro de auditoría**. El resumen de la aplicación incluye el estado de los certificados SSL con Hora de inicio y Hora de finalización.




Para determinar la información del dispositivo Citrix ADC de un certificado SSL determinado, seleccione la casilla de verificación Certificado correspondiente que quiera. Haga clic en **Registro del dispositivo**.




Para ver la información del tipo de comando y el mensaje, haga clic en **Registro de comandos**.




## Usar el panel SSL

August 23, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede usar el panel de certificados SSL de Citrix Application Delivery Management (ADM) para ver gráficos que le ayuden a rastrear los emisores de certificados, los puntos fuertes clave y los algoritmos de firma. El panel de control de certificados SSL también muestra gráficos que indican lo siguiente:

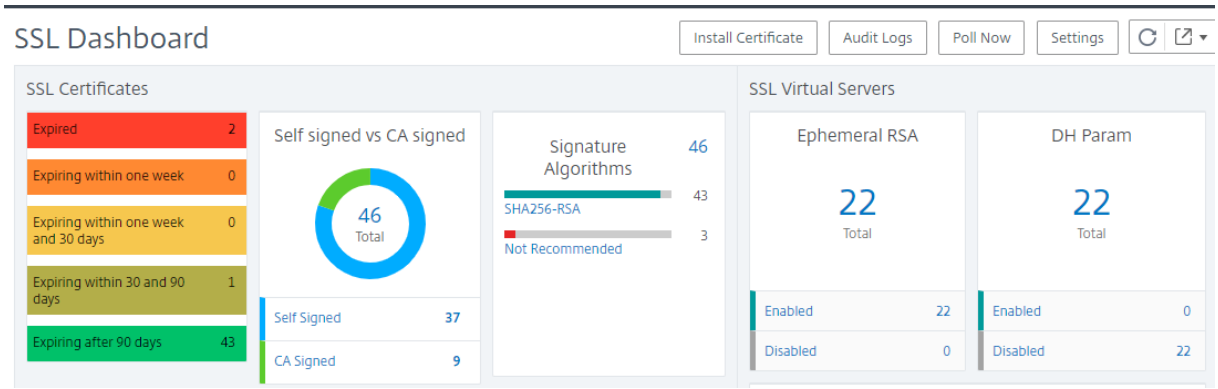
- Número de días después de los cuales caducan los certificados
- Número de certificados usados y no utilizados
- Número de certificados autofirmados y firmados por una CA
- Número de emisores
- algoritmos de firma
- Protocolos SSL
- Las 10 instancias principales por número de certificados en uso

## Para supervisar certificados SSL

Puede utilizar el panel SSL de Citrix ADM para supervisar sus certificados si su empresa tiene una directiva de SSL en la que ha definido ciertos requisitos de certificados SSL, por ejemplo, todos los certificados deben tener una fortaleza de clave mínima de 2048 bits y una entidad de CA de confianza debe autorizarlos.

En otro ejemplo, puede que haya cargado un certificado nuevo pero se haya olvidado de enlazarlo a un servidor virtual. El panel de control SSL resalta los certificados SSL que se están utilizando o no. En la sección **Uso**, puede ver el número de certificados que se han instalado y el número de certificados que se están utilizando. Puede hacer clic en el gráfico para ver el nombre de los certificados, la instancia en la que se está utilizando, su validez, su algoritmo de firma, etc.

Para supervisar los certificados SSL en Citrix ADM, vaya a**Redes**> **Tablero SSL**.




Citrix ADM le permite sondear certificados SSL y agregar todos los certificados SSL de las instancias inmediatamente a Citrix ADM. Para hacerlo,

1. Vaya a **Redes** >**Panel de control SSL**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Haga clic en **Encuesta ahora**.

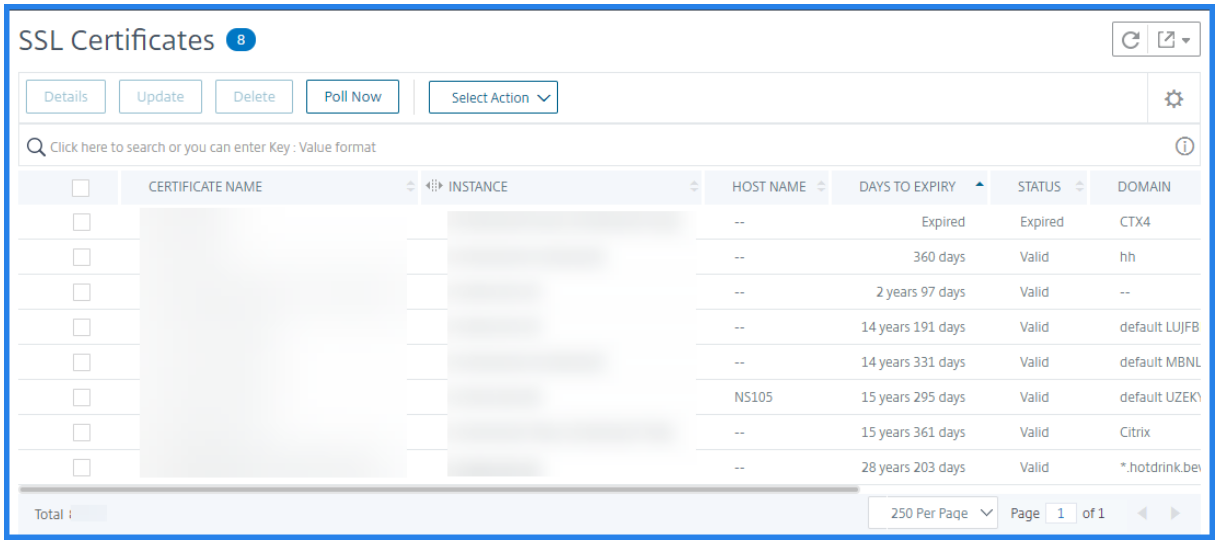
   En la página **Sondear ahora**, puede sondear todas las instancias de ADC gestionadas o seleccionar instancias específicas.

3. Haga clic en **Iniciar sondeo**.

En el **panel SSL**, puede supervisar los certificados SSL de ADC, los servidores virtuales SSL y los protocolos SSL.

Puede hacer clic en las métricas del panel para ver los detalles relacionados con los certificados SSL, los servidores virtuales SSL o los protocolos SSL.

Por ejemplo, cuando hace clic en el número bajo **Self signed vs CA signed** en el panel, la GUI de ADM muestra todos los certificados SSL en las instancias Citrix ADC.




El panel de control SSL de Citrix ADM también muestra la distribución de los protocolos SSL que se ejecutan en los servidores virtuales. Como administrador, puede especificar los protocolos que quiere supervisar a través de la directiva SSL; para obtener más información, consulte Configuración de directivas SSL. Los protocolos admitidos son SSLv2, SSLv3, TLS 1.0, TLS 1.1, TLS 1.2 y TLS 1.3. Los protocolos SSL utilizados en servidores virtuales aparecen en formato de gráfico de barras. Al hacer clic en un protocolo específico, se muestra una lista de servidores virtuales que utilizan ese protocolo.

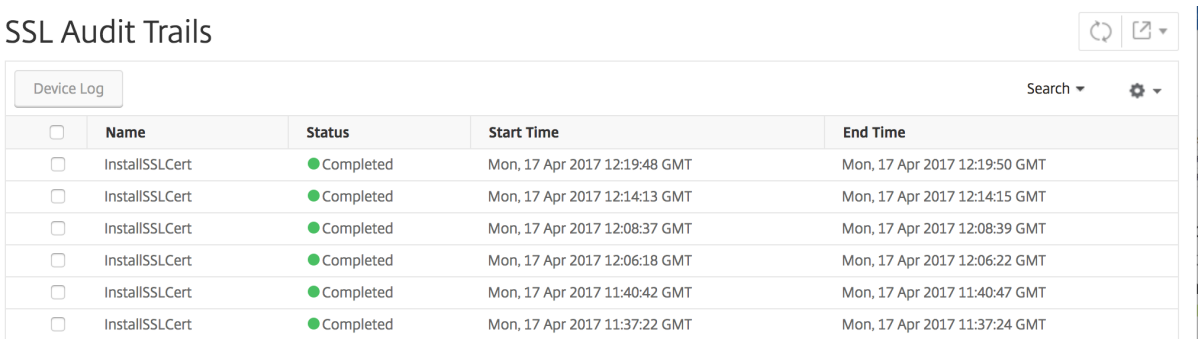
Aparece un gráfico de anillos después de habilitar o inhabilitar las teclas Diffie-Hellman (DH) o RSA efímera en el panel de control SSL. Estas claves permiten la comunicación segura con clientes de exportación incluso si el certificado del servidor no admite clientes de exportación, como en el caso de un certificado de 1024 bits. Al hacer clic en el gráfico apropiado se muestra una lista de los servidores virtuales en los que están habilitadas las claves RSA de DH o efímero.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

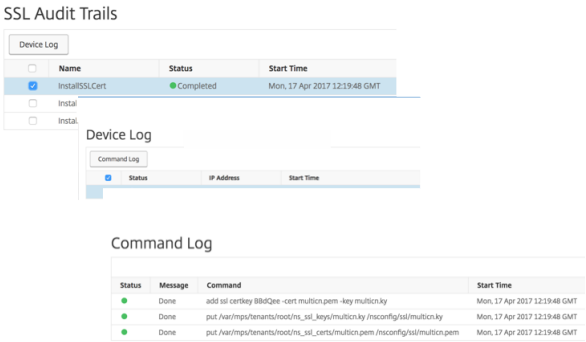
### Para ver pistas de auditoría de certificados SSL

Ahora puede ver los detalles de registro de certificados SSL en Citrix ADM. Los detalles del registro muestran las operaciones realizadas con certificados SSL en Citrix ADM, como la instalación de certificados SSL, la vinculación y desvinculación de certificados SSL, la actualización de los certificados SSL y la eliminación de certificados SSL. La información de seguimiento de auditoría es útil mientras se supervisan los cambios en los certificados SSL realizados en una aplicación con varios propietarios.

Para ver un registro de auditoría de una operación concreta realizada en Citrix ADM mediante certificados SSL, vaya a **Redes** > **Tablero de SSL** > y haga clic en **Registros de auditoría**.




Para una operación concreta realizada con certificado SSL, puede ver su estado, hora de inicio y hora de finalización. Además, puede ver la instancia en la que se realizó la operación y los comandos ejecutados en esa instancia.




### Para excluir certificados Citrix ADC predeterminados en el panel SSL

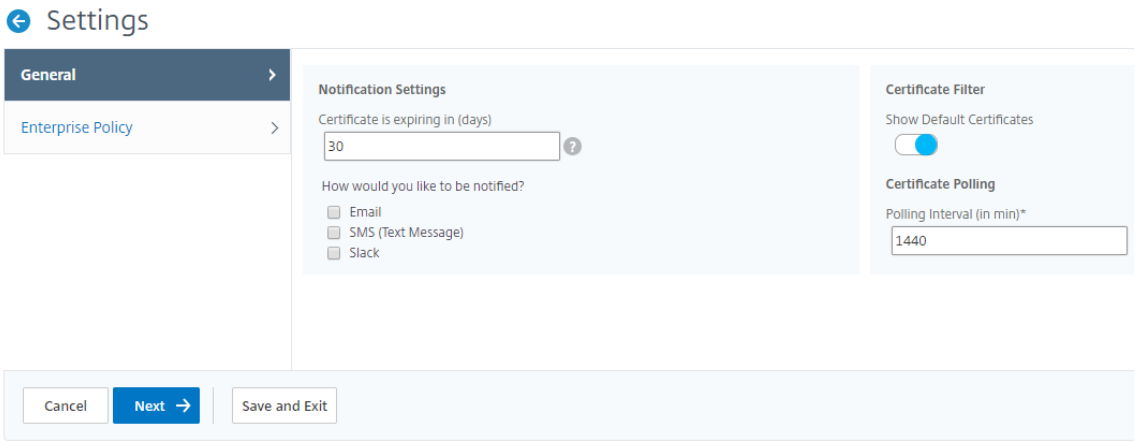
Citrix ADM le permite mostrar u ocultar los certificados predeterminados de Citrix ADC que aparecen en los gráficos de SSL Dashboard según sus preferencias. De forma predeterminada, todos los certificados se muestran en el panel SSL, incluidos los certificados predeterminados.

Para mostrar u ocultar certificados predeterminados en el panel SSL:

1. Vaya a **Networks** > **SSL Dashboard** en la GUI de Citrix ADM.
2. En la página **Tablero de SSL**, haga clic en **Configuración**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la página **Configuración**, seleccione **General**.
4. Escriba el número de días en que caduca el certificado para recibir una notificación sobre la caducidad del certificado.
5. Seleccione el método de notificación y cree los perfiles respectivos.
6. En la sección **Filtro de certificados**, desactive la casilla de verificación **Mostrar certificados predeterminados** y haga clic en **Guardar y salir**.




## Ver, cargar y descargar archivos SSL

Para ver los archivos SSL en Citrix ADM, vaya a **Redes > Panel de control SSL > Archivos SSL en Citrix ADM.**

En esta página, puede ver, cargar y descargar los siguientes archivos en Citrix ADM:

- Certificados de SSL
- Claves SSL
- CSR SSL

Para ver y descargar archivos SSL en una instancia de Citrix ADC, vaya a **Redes > Panel de control SSL > Archivos SSL en Citrix ADC**.

> **Importante**
>
> Para habilitar la descarga de archivos SSL desde instancias ADC, habilite la función **Certificados SSL de instancia**. Para obtener más información, consulte Habilitar o inhabilitar las funciones de ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configurar notificaciones para la caducidad del certificado SSL

January 30, 2024

Como administrador de seguridad, puede configurar notificaciones para que le informen cuando los certificados estén a punto de caducar e incluir información sobre las instancias de Citrix Application Delivery Controller (ADC) que utilizan esos certificados. Al habilitar las notificaciones, puede renovar sus certificados SSL a tiempo.

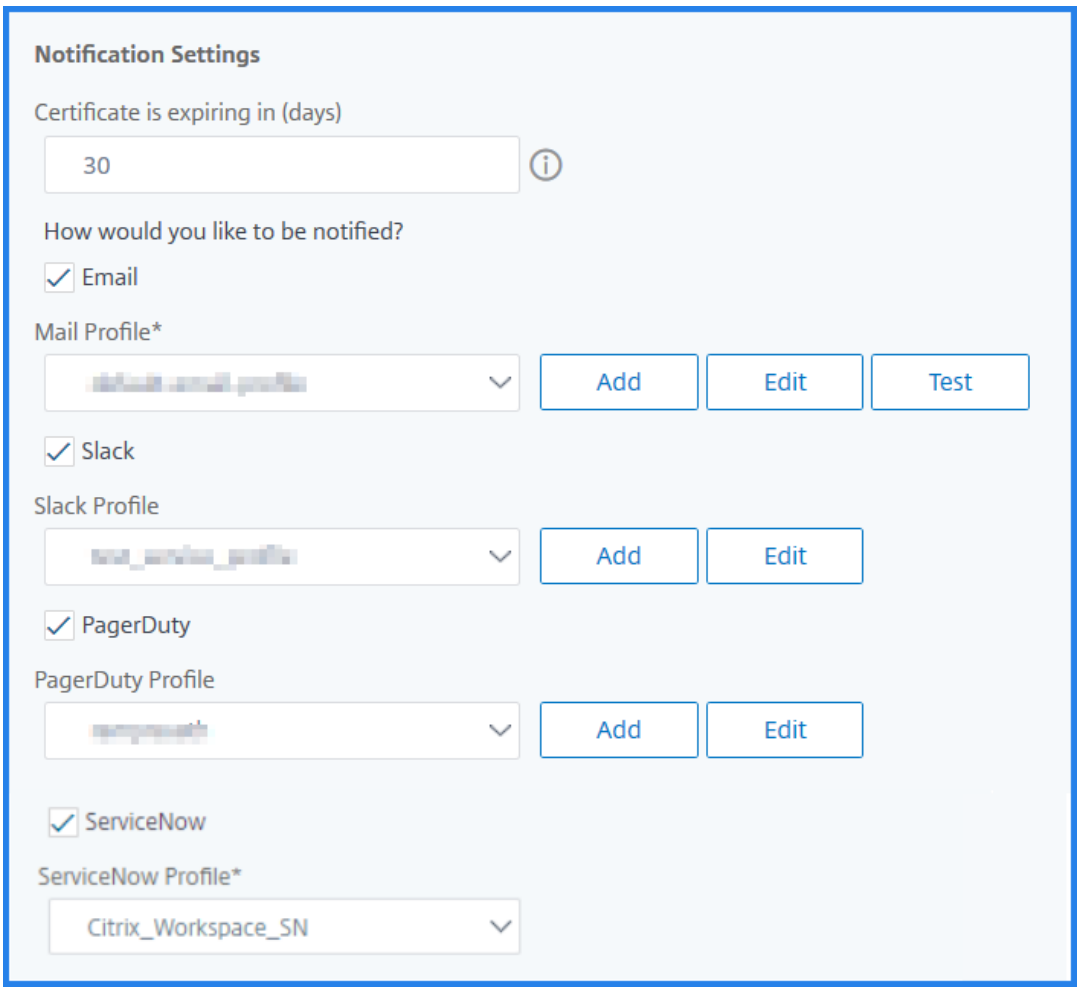
Por ejemplo, puede configurar una notificación por correo electrónico para que se envíe una lista de distribución por correo electrónico 30 días antes de la fecha de caducidad del certificado.

**Para configurar notificaciones desde NetScaler ADM:**

1. En Citrix Application Delivery Management (ADM), vaya a **Redes > Panel SSL** .
2. En la página **Tablero de SSL**, haga clic en **Configuración**.
3. En la página de **configuración de SSL**, haga clic en el icono **Editar**.
4. En la sección **Configuración de notificaciones**, especifique cuándo desea enviar la notificación en términos de número de días antes de la fecha de caducidad.
5. Elige el tipo de notificación que deseas enviar. Seleccione el tipo de notificación y la lista de distribución en el menú desplegable. Los tipos de notificación son los siguientes:
   - **Correo electrónico**: especifique un servidor de correo y los detalles del perfil. Un correo electrónico se activa cuando sus certificados están a punto de caducar.
   - **SMS**: Especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando sus certificados están a punto de caducar.
   - **Slack**: Especifique los detalles del perfil Slack.
   - **Alertas de PagerDuty**: Especifique un perfil de PagerDuty. Según la configuración de notificaciones configurada en su portal de PagerDuty, se envía una notificación cuando sus certificados están a punto de caducar.
   - **ServiceNow**: se envía una notificación al perfil predeterminado de ServiceNow cuando los certificados están a punto de caducar.

     > **Importante**
     >
     > Asegúrese de que Citrix Cloud ITSM Adapter esté configurado para ServiceNow e integrado con NetScaler ADM. Para obtener más información, consulte Integrar NetScaler ADM con la instancia de ServiceNow.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Haga clic en **Guardar y salir**.

NetScaler ADM envía ahora la captura de caducidad de certificados SSL al servidor de destino de capturas externo cuando los certificados SSL están vencidos. Citrix ADM envía una trampa cuando se cumplen las dos condiciones siguientes:

- Ha configurado el número de días para que caduque el certificado en la página de configuración del panel SSL.
- Ha agregado el destino de captura.

Puede establecer destinos de captura navegando a **Sistema > SNMP > Destinos de captura**. Escriba la dirección IP del servidor SNMP de destino al que se envían las capturas. Introduzca el número de puerto y escriba “public”(sin comillas) como cadena comunitaria.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Actualizar un certificado instalado

January 30, 2024

Tras recibir un certificado renovado de la autoridad de certificación (CA), puede actualizar los certificados existentes desde Citrix Application Delivery Management (ADM) sin necesidad de iniciar sesión en instancias individuales de Citrix Application Delivery Controller (ADC).

**Para actualizar un certificado SSL, una clave o ambos desde NetScaler ADM:**

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. En la página **Certificados SSL**, seleccione un certificado y haga clic en **Actualizar**. También puede hacer clic en el certificado SSL para ver sus detalles y, a continuación, haga clic en **Actualizar** en la esquina superior derecha de la página **Certificado SSL**.
4. En la página **Actualizar el certificado SSL**, realice las modificaciones necesarias en el certificado, la clave o ambos y haga clic en **Aceptar**.

## Instalar certificados SSL en una instancia de NetScaler ADC

January 30, 2024

Antes de instalar los certificados SSL en las instancias de Citrix Application Delivery Controller (ADC), asegúrese de que los certificados estén emitidos por CA de confianza. Además, asegúrese de que la intensidad de clave de las claves de certificado sea 2048 bits o superior y que las claves estén firmadas con algoritmos de firma seguros.

**Para instalar un certificado SSL desde otra instancia de NetScaler ADC:**

También puede importar un certificado desde una instancia de NetScaler ADC seleccionada y aplicarlo a otras instancias de NetScaler ADC de destino desde la GUI de NetScaler Application Delivery Management (ADM).

1. Vaya a **Redes** > **Panel de SSL**.
2. En la esquina superior derecha del panel SSL, haga clic en **Instalar**.
3. En la página **Instalar el certificado SSL en instancias de Citrix ADC** , especifique los siguientes parámetros:
   a) Origen de certificado
      Seleccione la opción **Importar desde instancia**.

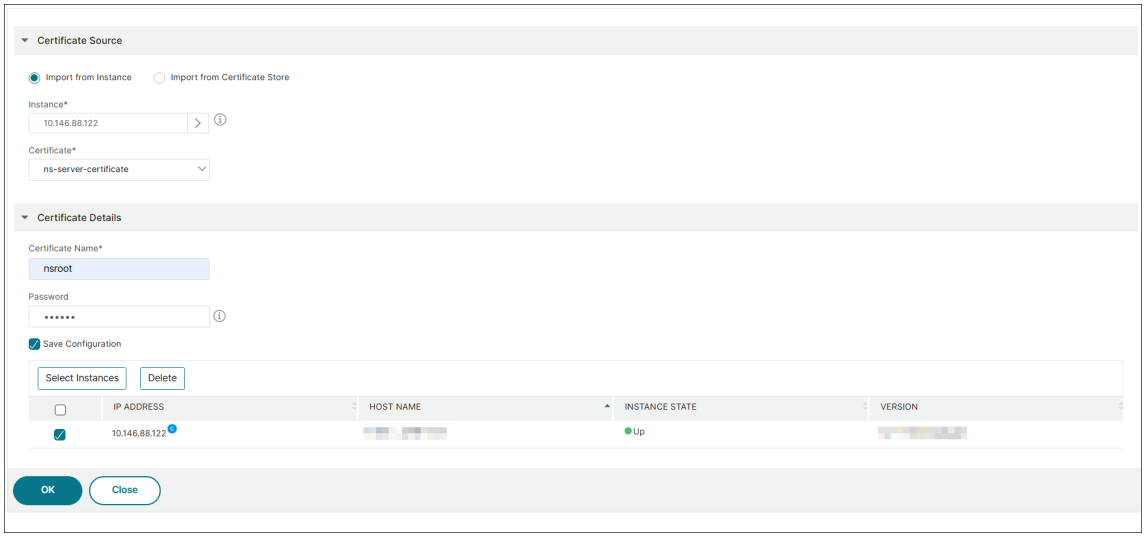
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Elija la **instancia** desde la que quiere importar el certificado.
- Elija el **Certificado** de la lista de todos los archivos de certificado SSL de la instancia.

b) Detalles del certificado

- **Nombre del certificado**. Especifique un nombre para la clave del certificado.
- **Contraseña**. Contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.

4. Haga clic en **Seleccionar instancias** para seleccionar las instancias de NetScaler ADC en las que quiere instalar sus certificados.
5. Haga clic en **Aceptar**.



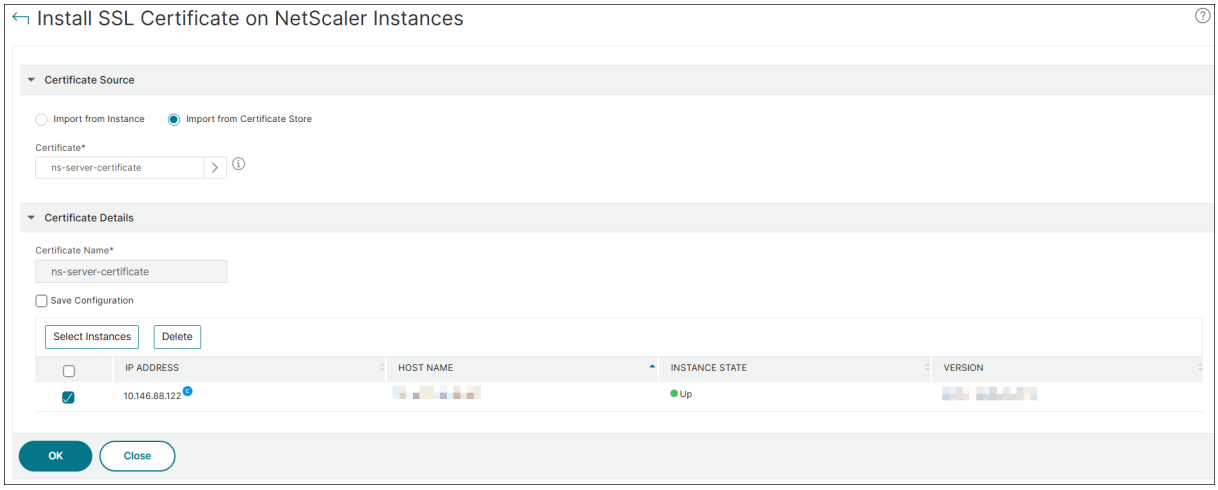

**Para instalar un certificado SSL desde NetScaler ADM:**

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. En la esquina superior derecha del panel, haga clic en **Instalar**.
3. En la página **Instalar certificado SSL en NetScaler ADC Instance**, seleccione **Cargar archivo de certificados** y especifique los parámetros siguientes:
   - **Archivo de certificado** : cargue un archivo de certificado SSL seleccionando **Local** (su equipo local) o **Appliance** (el archivo de certificado debe estar presente en la instancia virtual de NetScaler ADM).
   - **Archivo clave**: Cargue el archivo clave.
   - **Nombre del certificado**: Especifique un nombre para la clave del certificado.
   - **Contraseña**: Contraseña para cifrar la clave privada. Puede utilizar esta opción para cargar claves privadas cifradas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Seleccione instancias**: seleccione las instancias de Citrix ADM en las que quiere instalar los certificados.

4. Para guardar la configuración para usarla en el futuro, active la casilla **Guardar configuración**.
5. Haga clic en **Aceptar**.




## Crear una solicitud de firma de certificados (CSR)

January 30, 2024

Una solicitud de firma de certificado (CSR) es un bloque de texto cifrado que se genera en el servidor en el que se utilizará el certificado. Contiene información que se incluirá en el certificado, como el nombre de su organización, el nombre común (nombre de dominio), la localidad y el país.

**Para crear una CSR con NetScaler ADM:**

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL instalados y, a continuación, seleccione el certificado para el que quiere crear una CSR y seleccione **Crear CSR** en la lista **Seleccionar acción**.
3. En la página **Crear solicitud de firma de certificado (CSR)**, especifique un nombre para la CSR.
4. Lleve a cabo una de las siguientes acciones:
   - **Cargar una clave**: Selecciona la opción **Tengo una clave**. Para cargar el archivo de claves, seleccione **Local** (su máquina local) o **Appliance** (el archivo de claves debe estar presente en la instancia virtual NetScaler ADM).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Crear una clave**: seleccione la opción No tengo una clave y, a continuación, especifique los siguientes parámetros:

| | |
|---|---|
| **Algoritmo de cifrado** | Tipo de llave. Por ejemplo, RSA. |
| **Nombre de archivo de clave** | Nombre del archivo en el que está almacenada la clave RSA. |
| **Tamaño de clave** | Tamaño de la clave en bits. |
| **Valor del exponente público** | Elija **3** o **F4** de la lista desplegable proporcionada. Este valor es parte del algoritmo de cifrado que se requiere para crear la clave RSA. |
| **Formato de clave** | Por defecto, se selecciona PEM. PEM es el formato de clave recomendado para su certificado SSL. |
| **Algoritmo de codificación PEM** | En la lista desplegable, seleccione el algoritmo (**DES** o **DES3**) que quiere utilizar para cifrar la clave RSA generada. Si seleccionas este algoritmo, tendrás que proporcionar una contraseña PEM. |
| **Contraseña PEM** | Si ha elegido el algoritmo de codificación PEM, introduzca una contraseña. |
| **Confirmar contraseña PEM** | Confirma tu contraseña de PEM. |

5. Haga clic en **Continuar**.
6. En la siguiente página, proporcione más detalles.

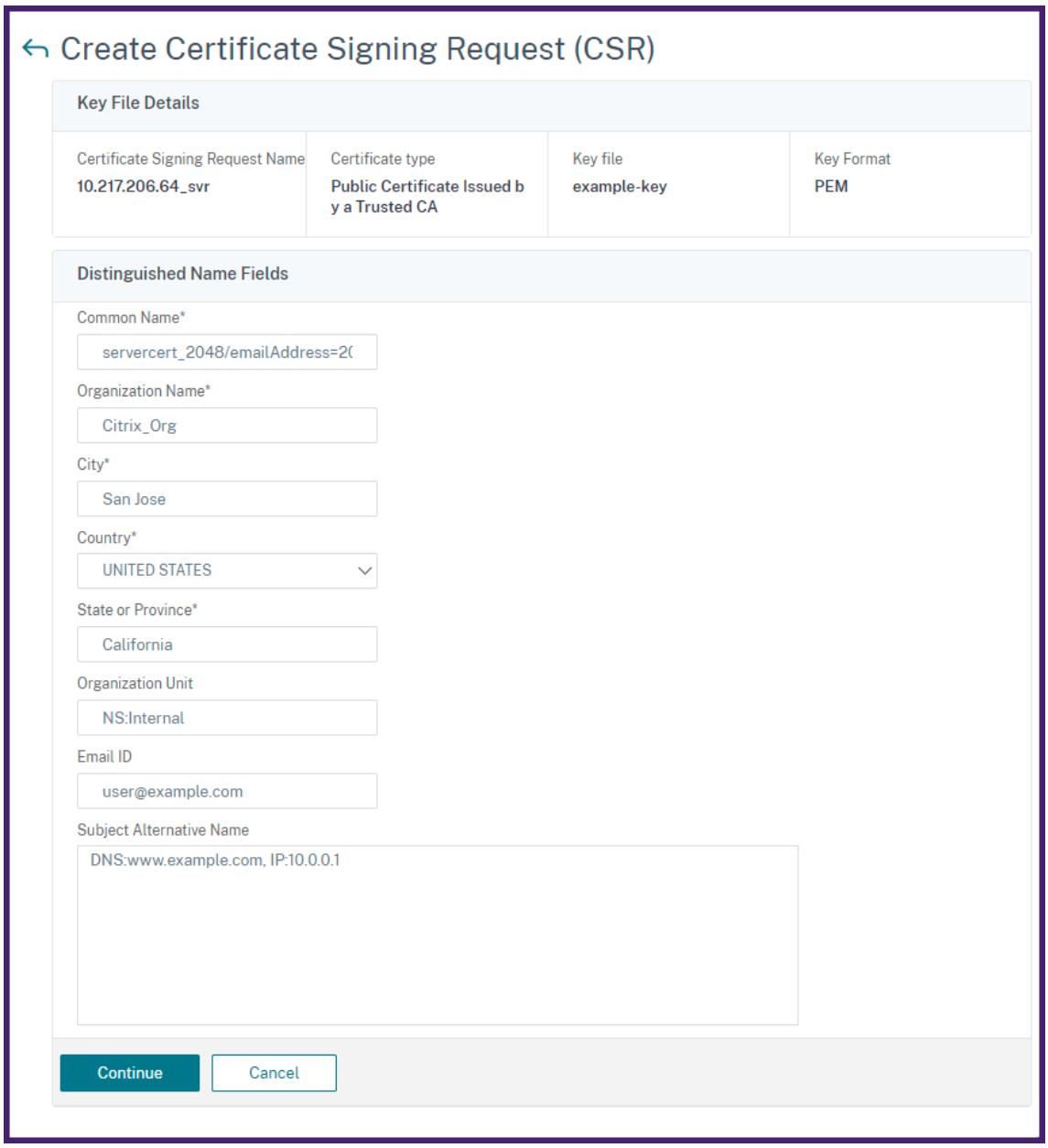
   La mayoría de los campos tienen valores predeterminados extraídos del asunto del certificado seleccionado. El asunto contiene detalles como el nombre común, el nombre de la organización, el estado y el país.

   En el campo **Nombre alternativo del sujeto**, puede especificar varios valores, como nombres de dominio y direcciones IP con un único certificado. Los nombres alternativos del sujeto ayudan a proteger varios dominios con un único certificado.

   Especifique los nombres de dominio y las direcciones IP en el siguiente formato:

```
DNS:<Domain name>, IP:<IP address>
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




En este ejemplo, asegura `10.0.0.1` y `www.example.com`.

Revise los campos y haga clic en **Continuar**.

> **Nota**
>
> La mayoría de los CA aceptan envíos de certificados por correo electrónico. La CA devuelve un certificado válido a la dirección de correo electrónico desde la que envía el CSR.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Vincular y desvincular certificados SSL

January 30, 2024

Para crear un paquete de certificados, debe vincular varios certificados entre sí. Para vincular un certificado a otro certificado, el emisor del primer certificado debe coincidir con el dominio del segundo certificado. Por ejemplo, si desea vincular el certificado A con el certificado B, el "emisor"del certificado A debe coincidir con el "dominio"del certificado B.

**Para vincular un certificado SSL a otro certificado mediante NetScaler ADM:**

1. En NetScaler Application Delivery Management (ADM), vaya a **Redes** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Seleccione el certificado que desee vincular y, a continuación, seleccione **Vincular** en la lista desplegable **Acción**.
4. En la lista de certificados coincidentes, seleccione el certificado al que quiere vincular y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Si no se encuentra ningún certificado coincidente, aparece el siguiente mensaje: No se ha encontrado ningún certificado que vincular.

**Para desvincular un certificado SSL mediante NetScaler ADM:**

1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. Haga clic en cualquiera de los gráficos para ver la lista de certificados SSL.
3. Elija uno de los certificados vinculados que estén vinculados y, a continuación, seleccione **Desvincular** en la lista desplegable **Acción**.
4. Haga clic en **Aceptar**.

> **Nota**
>
> Si el certificado seleccionado no está vinculado a otro certificado, se muestra el mensaje siguiente: El certificado no tiene ningún vínculo de CA.

## Configurar una directiva de empresa

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede configurar una directiva empresarial y agregar todas las CA de confianza, algoritmos de firma segura y seleccionar la seguridad de clave recomendada para las claves de certificado en NetScaler Application Delivery Management (ADM). Si alguno de los certificados instalados en la instancia de Citrix Application Delivery Controller (ADC) no se ha agregado a la directiva de empresa, el panel de certificados SSL muestra el emisor de esos certificados como **No recomendado**.

Además, si la fortaleza de la clave del certificado no coincide con la seguridad de la clave recomendada en la política empresarial, el panel de certificados SSL muestra la fortaleza de esas claves como **No recomendada** .

**Para configurar una directiva de empresa en NetScaler ADM:**

1. En Citrix ADM, vaya a **Infraestructura** > **Panel de control SSL** y, a continuación, haga clic en **Configuración**.
2. En la página Configuración de SSL, haga clic en el icono **Modificar** para agregar todas las CA de confianza, algoritmos de firma segura y seleccionar la seguridad de clave recomendada para sus certificados y claves.
3. Haga clic en **Guardar** para guardar la directiva de empresa.

## Encuesta de certificados SSL de instancias Citrix ADC

January 30, 2024

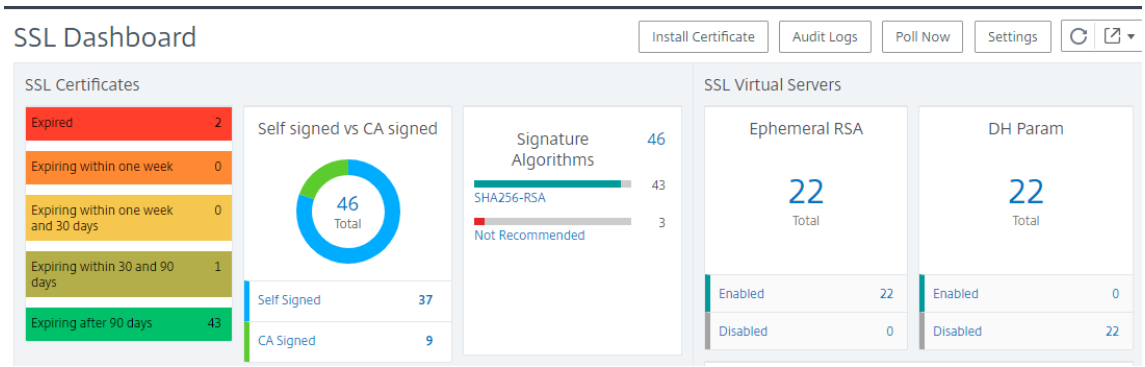
Citrix Application Delivery Management (ADM) sondea automáticamente los certificados SSL una vez cada 24 horas mediante llamadas NITRO y el protocolo Secure Copy (SCP). También puede sondear manualmente los certificados SSL para descubrir los certificados SSL recién agregados en las instancias de Citrix Application Delivery Controller (ADC). El sondeo de todos los certificados SSL de instancias Citrix ADC coloca una carga pesada en la red.

En lugar de sondear todos los certificados SSL de las instancias de Citrix ADC, puede sondear manualmente solo los certificados SSL de una o varias instancias seleccionadas.

**Para sondear certificados SSL en instancias Citrix ADC:**

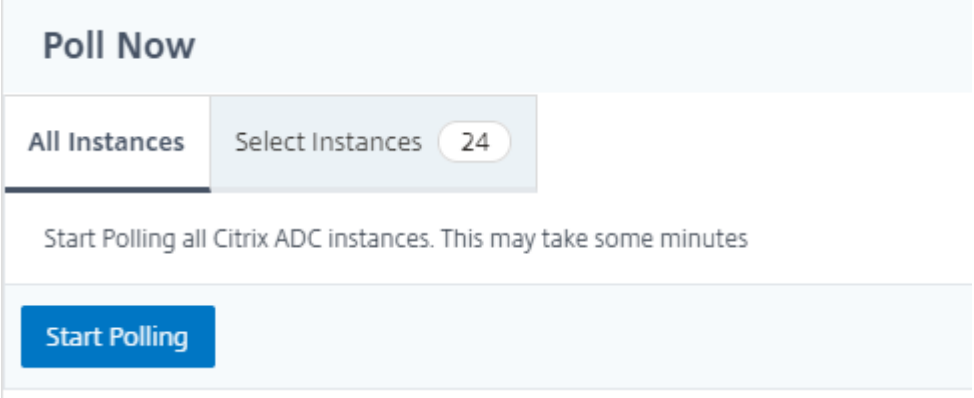
1. En Citrix ADM, vaya a **Networks** > **SSL Dashboard**.
2. En la página **SSL Dashboard**, en la esquina superior derecha, haga clic en **Sondear ahora**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

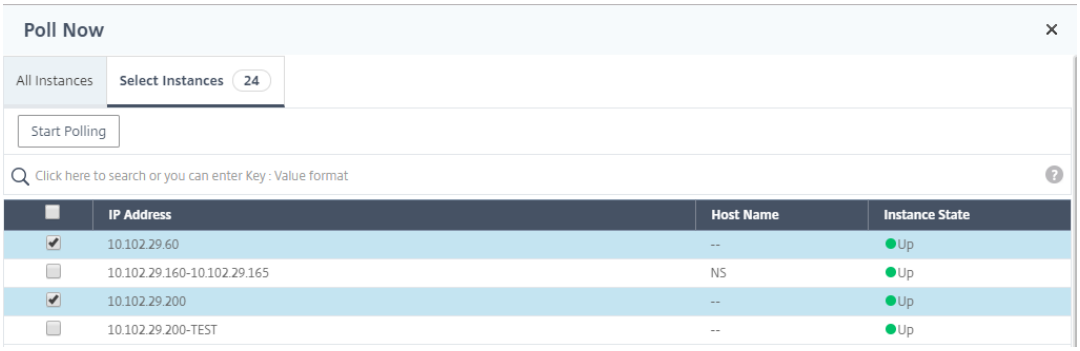



3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de Citrix ADC en la red o sondear las instancias seleccionadas.

   a) Para sondear los certificados SSL de todas las instancias de Citrix ADC, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.




   b) Para sondear instancias específicas, seleccione la ficha **Seleccionarinstancias**, seleccione las instancias de la lista y haga clic en**Sondear ahora**.




## Configurar la administración de direcciones IP (IPAM)

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

IPAM de ADM le permite asignar y liberar automáticamente las direcciones IP en las configuraciones gestionadas por ADM. Puede asignar direcciones IP desde redes o rangos de IP definidos mediante los siguientes proveedores de IP:

- Proveedor de IPAM integrado en ADM.
- Solución IPAM de Infoblox. Para obtener más información, consulte DDI de Infoblox.

Actualmente, puede usar ADM IPAM en:

- **StyleBooks**: asigna automáticamente las IP a los servidores virtuales al crear configuraciones.
- **Entrada de Kubernetes**: Asignar automáticamente una dirección IP virtual a una configuración de Ingress en un clúster de Kubernetes.

También puede realizar un seguimiento de las direcciones IP asignadas y disponibles en cada red o rango IP administrado por ADM.

## Agregar un proveedor de direcciones IP externo

ADM tiene un proveedor IPAM integrado para administrar IPs y rangos de IP. Si quiere agregar una solución de proveedor de IP externo en ADM, lleve a cabo los siguientes pasos:

1. Vaya a **Redes > IPAM**.
2. En **Proveedores**, haga clic en **Agregar**.
3. Especifique los siguientes detalles para agregar un proveedor de IP:
    - **Nombre**: especifique el nombre del proveedor IP que se va a utilizar en ADM.
    - **Proveedor**: Seleccione un proveedor de direcciones IP de la lista.
    - **URL**: Especifique la URL de la solución de IPAM que asigna direcciones IP en el entorno ADM.
    - **Nombre de usuario**: Especifique el nombre de usuario para iniciar sesión en la solución IPAM.
    - **Contraseña**: Especifique la contraseña para iniciar sesión en la solución IPAM.
4. Haga clic en **Agregar**.

## Agregar una red

Agregue una red para usar IPAM con configuraciones administradas por ADM.

1. Vaya a **Redes > IPAM**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En **Redes**, haga clic en **Agregar**.
3. Especifique los siguientes detalles:
   - **Nombre de red**: Especifique el nombre de la red para identificar la red en ADM.
   - **Proveedor**: Seleccione el proveedor de la lista.

     Esta lista muestra los proveedores agregados en ADM.
   - **Tipo de red**: Seleccione el **intervalo de direcciones IP** o **CIDR** de la lista según sus requisitos.
   - **Valor de red**: Especifique el valor de la red.

     > **Nota:**
     >
     > IPAM de ADM solo admite direcciones IPv4.

     Para el **intervalo de IP**, especifique el valor de red en el siguiente formato:

     ```
     <first-IP-address>-<last-IP-address>
     ```

     Ejemplo :

     ```
     10.0.0.20-10.0.0.100
     ```

     Para **CIDR**, especifique el valor de la red en el siguiente formato:

     ```
     <IP-address>/<subnet-mask>
     ```

     Ejemplo :

     ```
     10.70.124.0/24
     ```
4. Haga clic en **Crear**.

## Ver direcciones IP asignadas

Para ver más detalles acerca de las direcciones IP asignadas desde la red IPAM, siga estos pasos:

1. Vaya a **Redes > IPAM**.
2. En la ficha **Redes**, haga clic en **Ver todas las IP asignadas**.

   Este panel muestra la dirección IP, el nombre del proveedor, el proveedor del proveedor y la descripción. También muestra los detalles del recurso que reservaron esta dirección IP:

   - **Módulo**: muestra el módulo ADM que reserva la dirección IP. Por ejemplo, si StyleBooks reserva la dirección IP, esta columna muestra StyleBooks como módulo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Tipo de Recurso**: Muestra el tipo de recurso de ese módulo. Para el módulo StyleBooks, solo el tipo de recurso de configuraciones utiliza la red IPAM.
- **Id. de recurso**: muestra el identificador de recurso con un vínculo. Haga clic en este vínculo para acceder al recurso que utiliza la dirección IP. Para el tipo de recurso de configuración, el identificador de recurso se muestra como el identificador del paquete de configuración.

> **Nota**
>
> Si quiere liberar la dirección IP, seleccione la dirección IP que quiere liberar y haga clic en **Liberar IP asignadas**.

## Trabajos de configuración

January 30, 2024

El proceso de administración de configuración de NetScaler Application Delivery Management (NetScaler ADM) garantiza la replicación adecuada de los cambios de configuración, las actualizaciones del sistema y otras actividades de mantenimiento en varias instancias de Citrix Application Delivery Controller (ADC) en la red.

NetScaler ADM le permite crear trabajos de configuración que le ayudarán a realizar todas estas actividades con facilidad en varios dispositivos como una sola tarea. Las plantillas y los trabajos de configuración simplifican las tareas administrativas más repetitivas en una sola tarea en NetScaler ADM. Un trabajo de configuración contiene un conjunto de comandos de configuración que se pueden ejecutar en uno o varios dispositivos gestionados.

Los trabajos de configuración pueden usar comandos SSH para ejecutar los comandos de configuración o usar SCP para copiar archivos de forma local o a otro dispositivo; por ejemplo, podemos programar una conmutación por error de HA o una actualización de HA.

Puede crear un trabajo de configuración mediante una de las cuatro opciones siguientes en NetScaler ADM. Utilice uno de estos para crear un origen reutilizable de comandos e instrucciones para el sistema para ejecutar un trabajo de configuración.

1. Plantilla de configuración
2. Instancia
3. Archivo
4. Grabar y reproducir

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Plantilla de configuración

Puede crear plantillas de configuración mientras crea un trabajo y guarda un conjunto de comandos de configuración como plantilla. Al guardar estas plantillas en la página Crear trabajos , se muestran automáticamente en la página Crear plantilla .

> **Nota**
> La opción **Cambiar nombre** está inhabilitada para las plantillas de configuración predeterminadas. Sin embargo, puede cambiar el nombre de las plantillas de configuración personalizadas.

Puede utilizar una de las siguientes plantillas:

**Editor de configuración**: puede usar el editor de configuración para escribir los comandos de la CLI, guardar la configuración como una plantilla y usarla para configurar los trabajos.

**Plantilla incorporada**: puede elegir de una lista de plantillas de configuración. Estas plantillas proporcionan las sintaxis de los comandos CLI y permiten especificar valores para las variables. Las plantillas integradas aparecen en la lista, con sus descripciones en la tabla siguiente. Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, puede utilizar la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. También puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute en una etapa posterior.

### Instancia

Puede realizar una actualización de un solo paquete de las instancias de Citrix SDX que ejecuten Citrix ADC versión 11.0 y versiones posteriores. Para realizar una actualización de un solo paquete, utilice una tarea integrada en NetScaler ADM. También puede actualizar una instancia de NetScaler ADC extrayendo la configuración en ejecución o una configuración guardada y ejecutando los comandos en otra instancia de NetScaler ADC del mismo tipo. Esto le permite replicar la configuración de una instancia en la otra.

### Archivo

Puede cargar un archivo de configuración desde su máquina local y crear trabajos.

Ventajas de usar un archivo

- Puede utilizar cualquier archivo de texto para crear una fuente reutilizable de comandos de configuración.
- No se requiere ningún tipo de formato.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- El archivo se puede guardar en el equipo local.

Puede crear y guardar un archivo nuevo o importar un archivo existente y ejecutar los comandos.

### Grabar y reproducir

Mediante Crear trabajo, puede introducir sus propios comandos CLI o utilizar el botón Grabar y reproducir para obtener comandos de una sesión de NetScaler ADC. Cuando ejecuta el trabajo, los cambios en ns.conf en la instancia seleccionada se registran y copian en NetScaler ADM.

#### Artículos relacionados

- Cómo utilizar el comando SCP (put) en los trabajos de configuración
- Cómo utilizar variables en los trabajos de configuración
- Cómo crear trabajos de configuración a partir de comandos correctivos
- Cómo utilizar plantillas de configuración para crear plantillas de auditoría
- Cómo utilizar Record-and-Play para crear trabajos de configuración
- Cómo utilizar la plantilla de configuración maestra en NetScaler ADM

## Crear un trabajo de configuración

January 30, 2024

Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una o varias instancias administradas. Puede crear trabajos para realizar cambios de configuración en las instancias, replicar configuraciones en varias instancias de la red y grabar y reproducir tareas de configuración mediante la GUI de NetScaler Application Delivery Management (ADM) y convertirlas en comandos de la CLI.

Puede utilizar la función Trabajos de configuración de NetScaler ADM para crear un trabajo de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados.

**Para crear un trabajo de configuración en NetScaler ADM:**

1. Vaya a **Redes > Trabajos de configuración**.
2. Haga clic en **Crear trabajo**.
3. En la página **Crear trabajo**, en la ficha **Seleccionar configuración**, especifique el nombre del trabajo y seleccione el **tipo de instancia** de la lista.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En la lista de **fuentes** de configuración, seleccione la plantilla de trabajo de configuración que quiere crear. Agregue los comandos para la plantilla seleccionada.

   - Puede introducir los comandos o importar los comandos existentes desde las plantillas de configuración guardadas.
   - También puede agregar varias plantillas de diferentes tipos en el editor de configuración mientras crea un trabajo en los trabajos de configuración.
   - En la lista de **fuentes de configuración**, seleccione las diferentes plantillas y, a continuación, arrástrelas al editor de configuración. Los tipos de plantillas pueden ser **Plantilla de configuración**, **Plantilla integrada**, **Configuración maestra**, **Grabar y reproducir**, **Instancia** y **Archivo**.

   > **Nota**
   >
   > Si agrega la `Deploy Master Configuration Job` plantilla por primera vez, agregue una plantilla de otro tipo y, a continuación, toda la plantilla de trabajo se convierte en un `Master Configuration` tipo.

   También puede reorganizar y reordenar los comandos en el editor de configuración. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto. También puede reorganizar y reordenar la línea de comandos mientras modifica el trabajo de configuración.

   Puede definir variables que le permitan asignar valores diferentes para estos parámetros o ejecutar un trabajo en varias instancias. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada. Haga clic en la ficha**Previsualizar variables**para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.

   Puede personalizar los comandos de reversión para cada comando del editor de configuración. Para especificar los comandos personalizados, habilite la opción de reversión personalizada.

   > **Importante**
   >
   > Para que la reversión personalizada surta efecto, complete el asistente de **creación de trabajos**. Y en la ficha **Ejecutar**, seleccione la opción **Revertir comandos correctos** de la lista **Al fallar un comando**.

5. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración.

   a) En un par de alta disponibilidad de NetScaler ADC, puede ejecutar un trabajo de configuración local en un nodo primario o secundario. Seleccione en qué nodo quiere ejecutar el trabajo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Ejecutar en nodos primarios**: seleccione esta opción para ejecutar el trabajo solo en nodos primarios.
- **Ejecutar en nodos secundarios**: seleccione esta opción para ejecutar el trabajo solo en nodos secundarios.

También puede elegir tanto el nodo principal como el secundario para ejecutar el mismo trabajo de configuración. Si no selecciona nodo principal o secundario, el trabajo de configuración se ejecuta automáticamente en el nodo principal.

6. En la ficha **Especificar valores de variable**, tiene dos opciones:
   a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM.
   b) Introduzca valores comunes para las variables que ha definido para todas las instancias.
   c) Haga clic en **Siguiente**.

**Para enviar un correo electrónico y una notificación de Slack para un trabajo:**

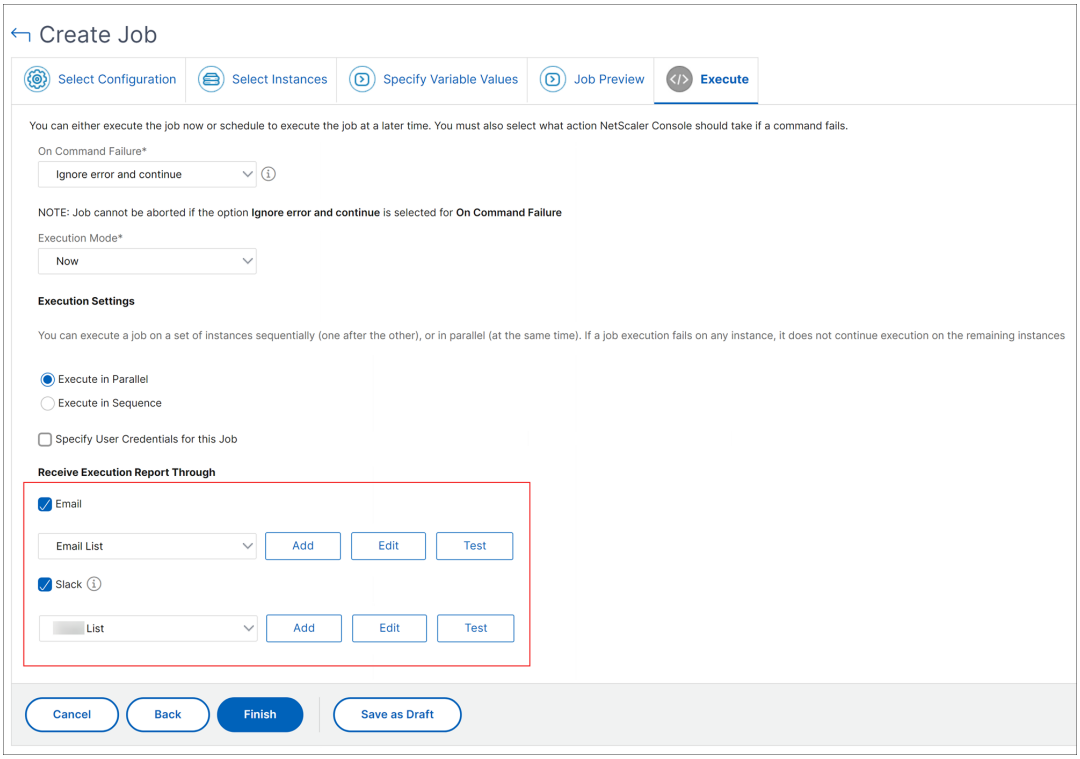
Ahora se envía un correo electrónico y una notificación de Slack cada vez que se ejecuta o se programa un trabajo. La notificación incluye detalles como el éxito o fracaso del trabajo junto con los detalles relevantes.

1. Vaya a **Redes** > **Trabajos de configuración** .
2. Seleccione el trabajo que quiere habilitar la notificación de correo electrónico y Slack y haga clic en **Modificar**.
3. En la ficha **Ejecutar**, vaya al panel **Recibir informe de ejecución mediante** :
   - Seleccione la casilla **Correo electrónico** y elija la lista de distribución de correo electrónico a la que quiere enviar el informe de ejecución.

     Si quiere agregar una lista de distribución de correo electrónico, haga clic en **Agregar** y especifique los detalles del servidor de correo electrónico.
   - Selecciona la casilla de verificación de **Slack** y elige el canal de Slack al que quieres enviar el informe de ejecución.

     Si quiere agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack requerido.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. Haga clic en **Finalizar**.

**Para enviar un correo electrónico y una notificación de Slack para un trabajo:**

Ahora se envía un correo electrónico y una notificación de Slack cada vez que se ejecuta o se programa un trabajo. La notificación incluye detalles como el éxito o fracaso del trabajo junto con los detalles relevantes.

1. Vaya a **Redes** > **Trabajos de configuración** .
2. Seleccione el trabajo que quiere habilitar la notificación de correo electrónico y Slack y haga clic en **Modificar**.
3. En la ficha **Ejecutar**, vaya al panel **Recibir informe de ejecución mediante** :
   - Seleccione la casilla **Correo electrónico** y elija la lista de distribución de correo electrónico a la que quiere enviar el informe de ejecución.

     Si quiere agregar una lista de distribución de correo electrónico, haga clic en **Agregar** y especifique los detalles del servidor de correo electrónico.
   - Selecciona la casilla de verificación de **Slack** y elige el canal de Slack al que quieres enviar el informe de ejecución.

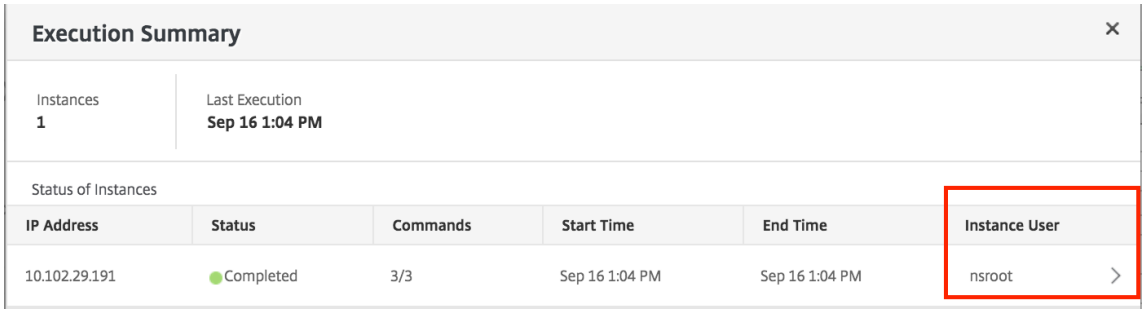
     Si quiere agregar un perfil de Slack, haga clic en **Agregar** y especifique el **nombre del perfil**, el **nombre del canal** y el **token** del canal de Slack requerido.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. Haga clic en **Finalizar**.

**Para ver los detalles del resumen de ejecución:**

1. Vaya a **Redes** > **Trabajos de configuración**.
2. Seleccione el trabajo que quiere ver el resumen de ejecución y haga clic en **Detalles**.
3. Haga clic en **Resumen de ejecución** para ver:
   - El estado de la instancia en la que se ejecuta el trabajo
   - Los comandos se ejecutan en el trabajo
   - La hora de inicio y finalización del trabajo, y
   - Nombre del usuario de la instancia




## Usar grabación y reproducción para crear trabajos de configuración

January 30, 2024

Si está acostumbrado a utilizar la GUI de Citrix ADC para configurar una instancia de Citrix ADC, a veces le resultará difícil recuperar los comandos de CLI exactos para crear una tarea de configuración y ejecutarla en varias instancias de Citrix ADC.

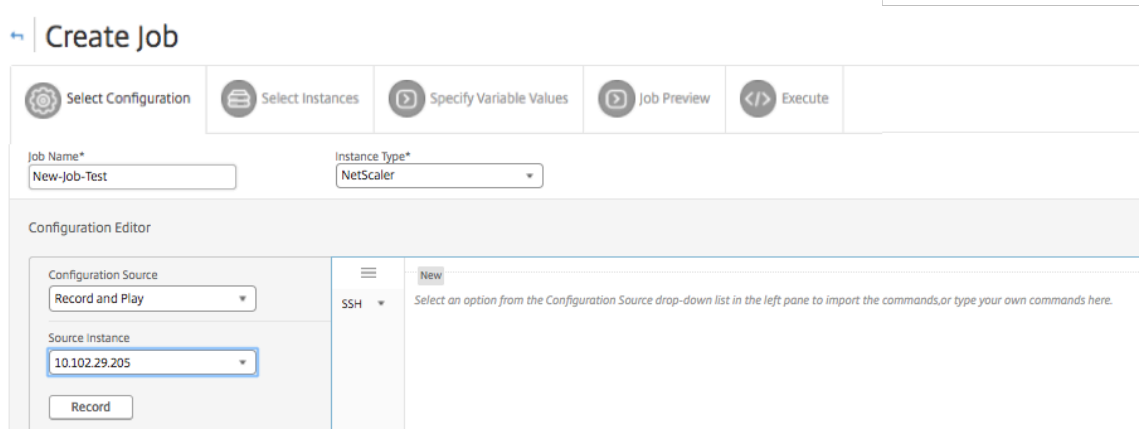
Citrix ADM le permite registrar las tareas de configuración realizadas mediante la GUI de una instancia de Citrix ADC y convertirlas en comandos de CLI. A continuación, puede crear una tarea de configuración a partir de estos comandos de CLI y ejecutar esta tarea en varias instancias.

### Para registrar la configuración de la interfaz gráfica de usuario y convertirla en una tarea de configuración

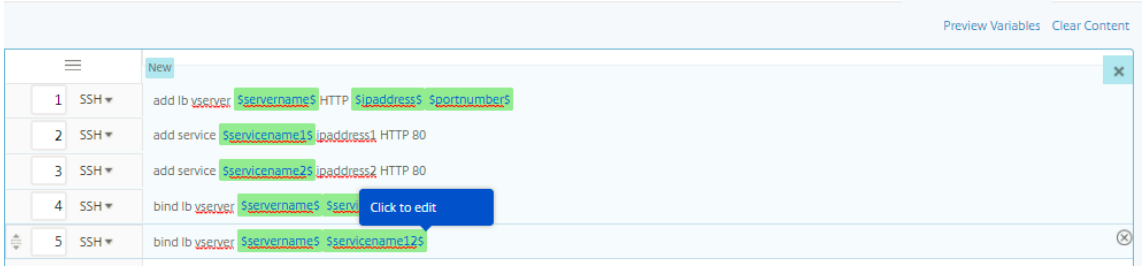
1. Vaya a **Redes** > **Trabajos de configuración** y, a continuación, haga clic en **Crear trabajo**.
2. Especifique el nombre del trabajo y el tipo de instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la lista de **fuentes de configuración**, seleccione **Grabar y reproducir**y, a continuación, seleccione la instancia de origen desde la que quiere grabar la configuración. Haga clic en **Grabar**.




4. Se abre la **GUI de Citrix ADC**. Configure las funciones y los valores que quiere que contenga la tarea de configuración. A continuación, cierre la ventana GUI de Citrix ADC y haga clic en **Detener** en el **Editor de configuración**. Los comandos aparecen como un vínculo en el panel izquierdo. Arrastre los comandos al panel derecho y, a continuación, haga clic en **Siguiente**.




A continuación, puede reorganizar y reordenar los comandos en el editor de configuración según corresponda. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto.

5. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.

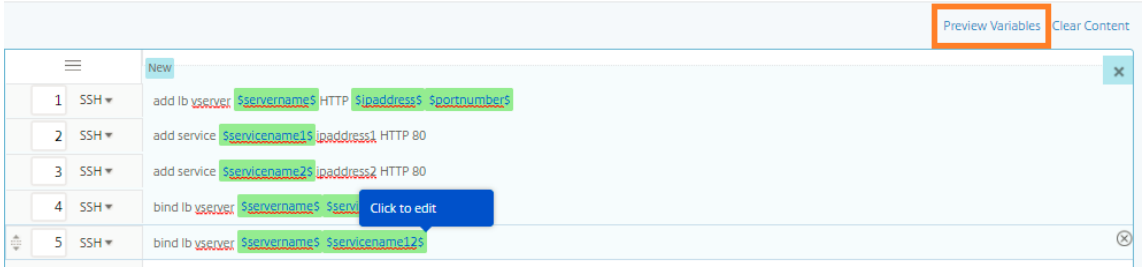
6. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:

   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.

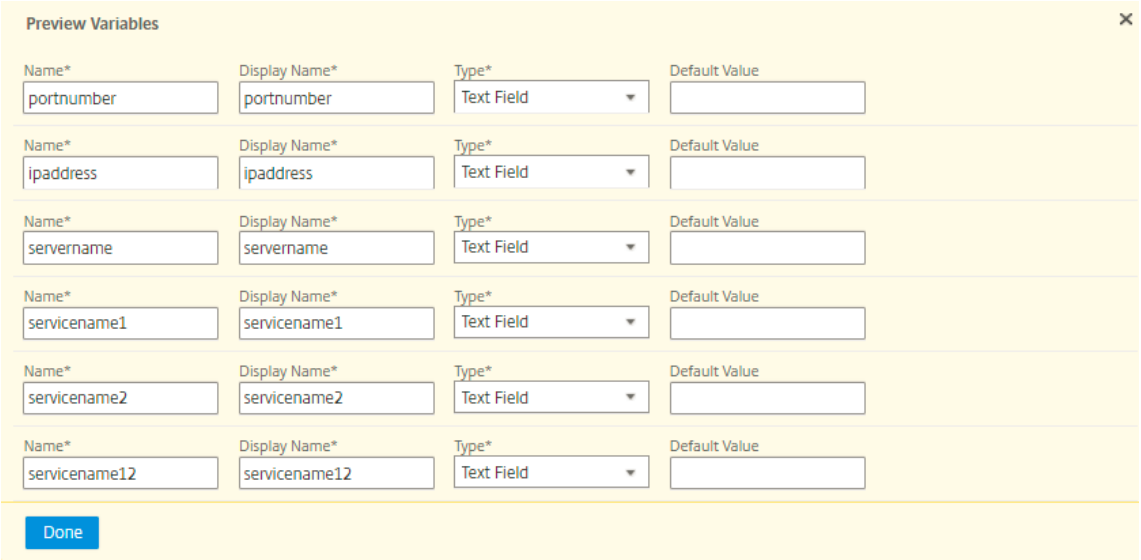
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.

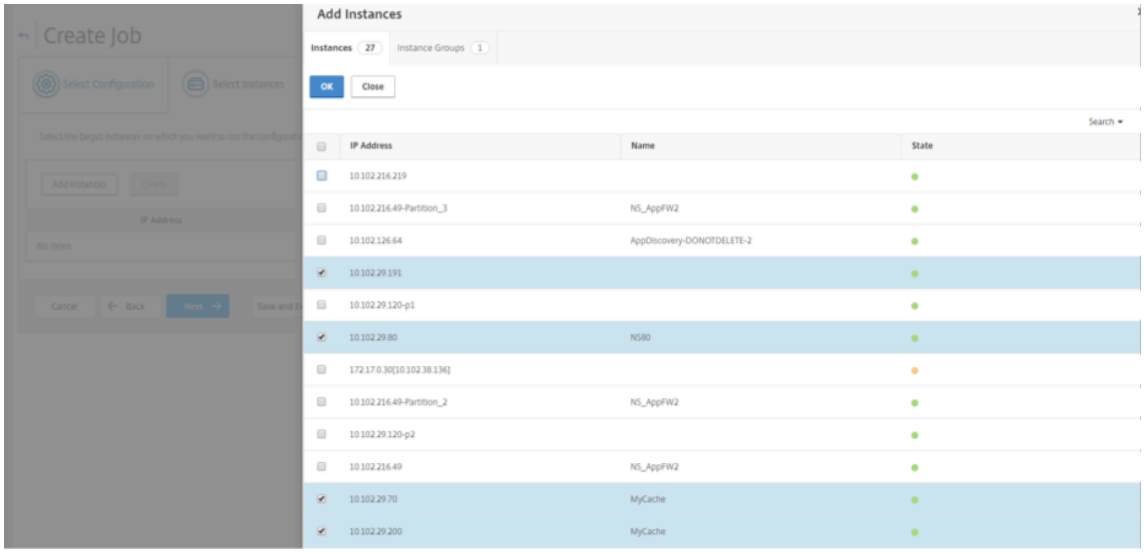



8. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.




9. Haga clic en**Agregar instancias**y seleccione las instancias en las que desee ejecutar el trabajo de configuración. Haga clic en**Aceptar**y, a continuación, en**Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




10. Si ha especificado variables en los comandos, en la ficha **Especificar valores de variable**, seleccione una de las siguientes opciones para especificar variables para las instancias:

    - **Cargar archivo de entrada para valores de variables:** haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca valores para las variables definidas en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
    - **Valores de variables comunes para todas las instancias**: introduzca valores para las variables. Las variables varían en función de la plantilla seleccionada.

    Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

    Para ver los trabajos de configuración en ejecución al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

    Para ver los trabajos de configuración ya ejecutados al editar un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).10.En la ficha **Vista previa**

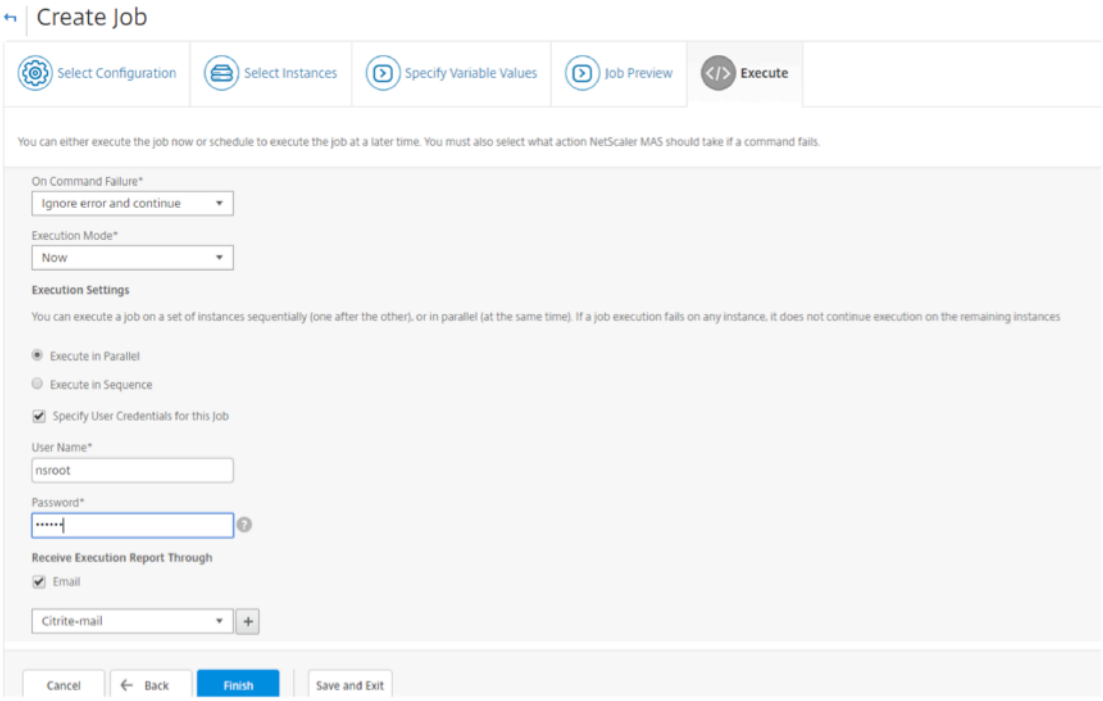
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

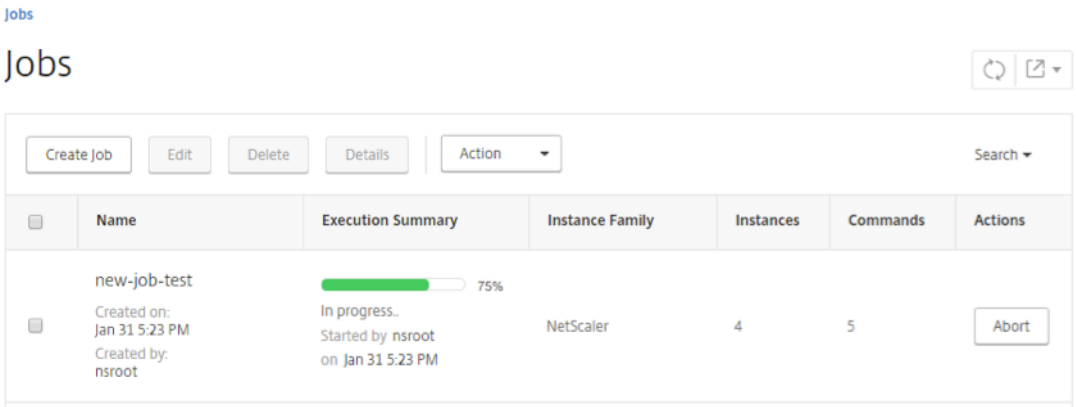
11. En la ficha**Vista previa del trabajo**, puede evaluar y verificar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

12. En la ficha**Ejecutar**, puede optar por ejecutar el trabajo ahora o programarlo para que se ejecute más tarde. También puede elegir qué acción debe realizar Citrix ADM si falla el comando.

    También puede optar por permitir que los usuarios autorizados ejecuten trabajos en las instancias administradas, y puede elegir si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.




13. En la página **Trabajos**, puede ver el progreso de la ejecución de la tarea de configuración en todas las instancias.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Utilizar trabajos de configuración para replicar la configuración de una instancia a varias instancias

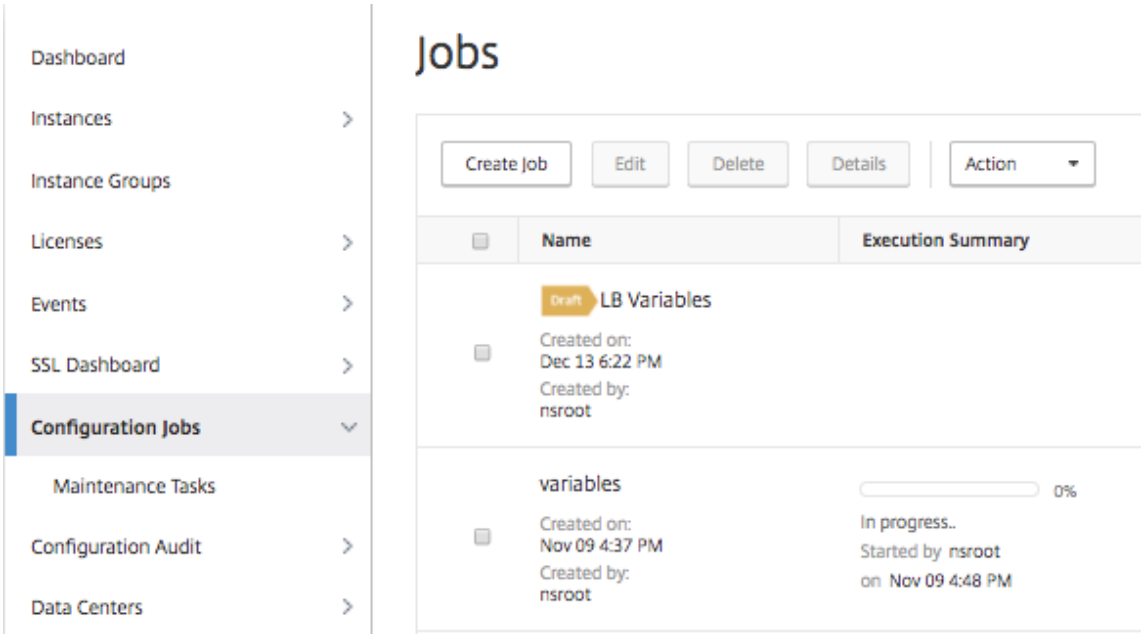
January 30, 2024

Puede utilizar la función Trabajos de configuración de Citrix ADM para extraer una configuración concreta de una instancia de Citrix ADC y replicarla en varias instancias.

Por ejemplo, es posible que haya configurado el equilibrio de carga y la optimización de front-end (FEO) en una instancia de Citrix ADC para su implementación. Sin embargo, ahora quiere replicar solo la configuración de FEO en otras instancias de Citrix ADC.

**Para recuperar y replicar la configuración de una instancia a otras instancias de Citrix ADC:**

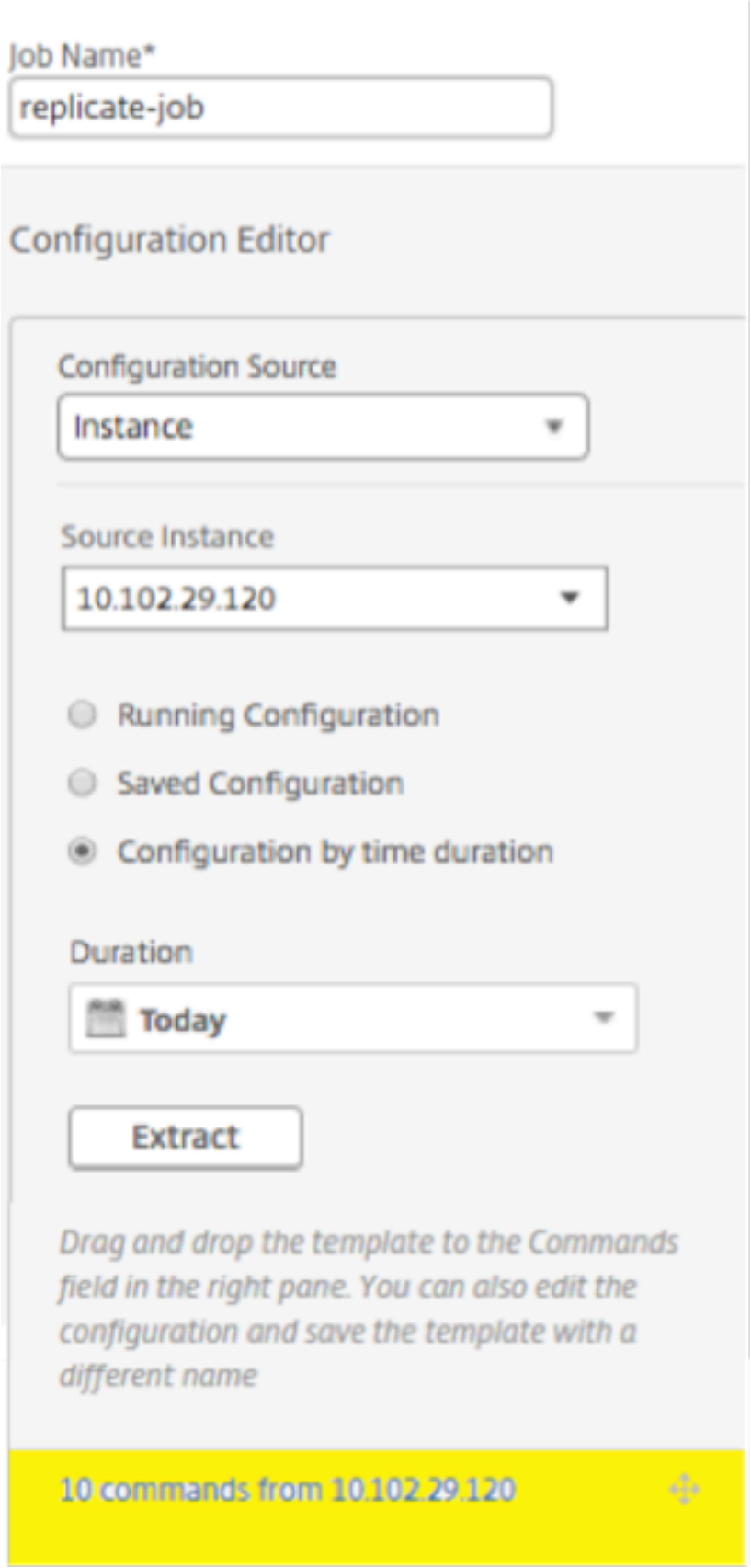
1. Vaya a **Redes** > **Trabajos de configuración** y, a continuación, haga clic en **Crear trabajo**.




2. Especifique el nombre del trabajo y el tipo de instancia.
3. Seleccione **Instancia** como **fuente de configuración** y seleccione la instancia de origen cuya configuración quiere replicar. Seleccione el tipo de configuración que quiere extraer. Si selecciona la opción "Configuración por duración de tiempo", establezca el período de tiempo en el que ejecutó esta configuración y, a continuación, haga clic en **Extraer**.

   El número de comandos ejecutados en esa instancia durante el tiempo seleccionado se muestra en la pantalla como resaltado en la imagen siguiente.

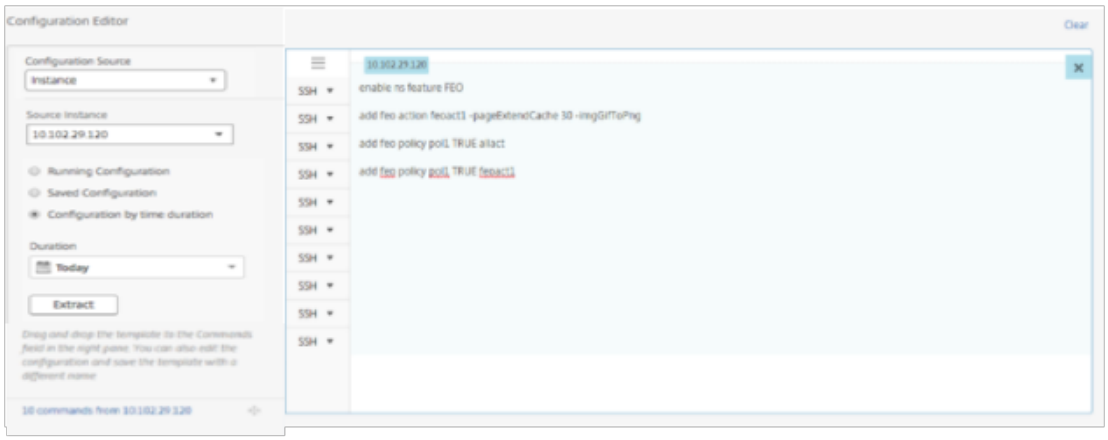
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. Arrastre los **comandos al campo Comandos** del panel derecho.

Mantenga solo los comandos relacionados con FEO y elimine manualmente los comandos relacionados con el equilibrio de carga o los comandos relacionados con cualquier otra configuración y, a continuación, haga clic en **Siguiente**.




5. Haga clic en **Agregar instancias** y agregue las instancias en las que quiere aplicar la configuración FEO. Haga clic en **Aceptar**y, a continuación, en **Siguiente**.
6. Si ha especificado variables en los comandos, en la pestaña Especificar valores de variables, haga clic en **Descargar archivo de claves** de entrada . En el archivo descargado, especifique los valores de las variables y, a continuación, cargue el archivo a Citrix ADM.
7. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
8. En la ficha **Ejecutar**, haga clic en **Finalizar** para ejecutar el trabajo en las instancias de Citrix ADC seleccionadas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Usar variables en trabajos de configuración

January 30, 2024

Un trabajo de configuración es un conjunto de comandos de configuración que se pueden ejecutar en una o más instancias administradas. Cuando ejecuta la misma configuración en varias instancias, es posible que quiera utilizar valores diferentes para los parámetros utilizados en la configuración. Puede definir variables que le permitan asignar valores diferentes para estos parámetros o ejecutar un trabajo en varias instancias.

Por ejemplo, considere una configuración básica de equilibrio de carga en la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual. Ahora, es posible que quiera tener la misma configuración en dos instancias, pero con valores diferentes para los nombres y direcciones IP del servidor y los servicios virtuales. Puede utilizar la función de trabajos de configuración para lograrlo mediante variables para definir los nombres y las direcciones IP del servidor y los servicios virtuales.

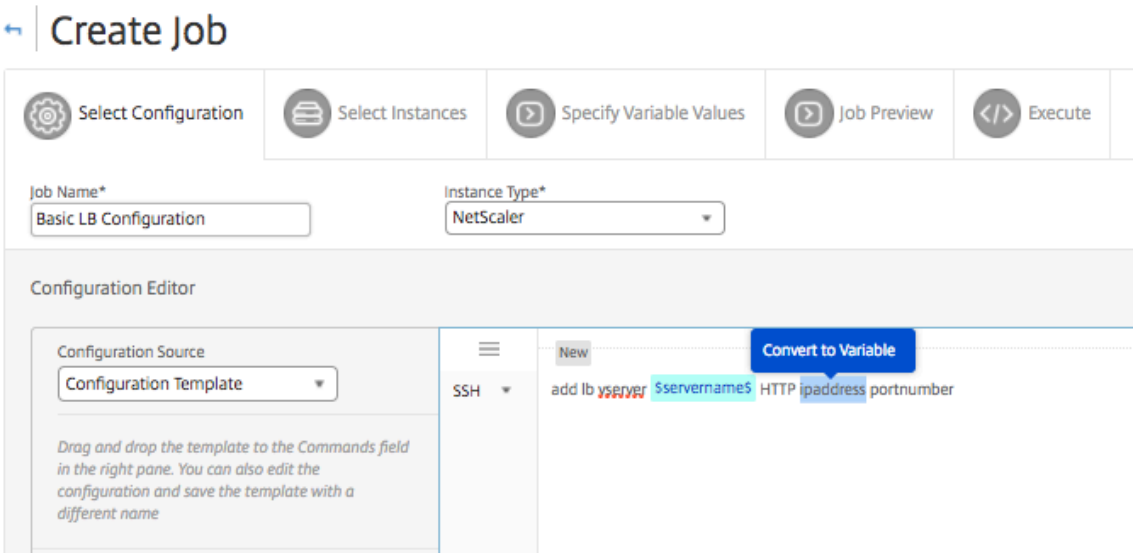
En este ejemplo, se utilizan los siguientes comandos y variables:

```
add lb vserver <servername> HTTP <ipaddress> <portnumber>
add service <servicename1> <ipaddress1> HTTP 80
add service <servicename2> <ipaddress2> HTTP 80
bind lb vserver <servername> <servicename1>
bind lb vserver <servername> <servicename2>
```

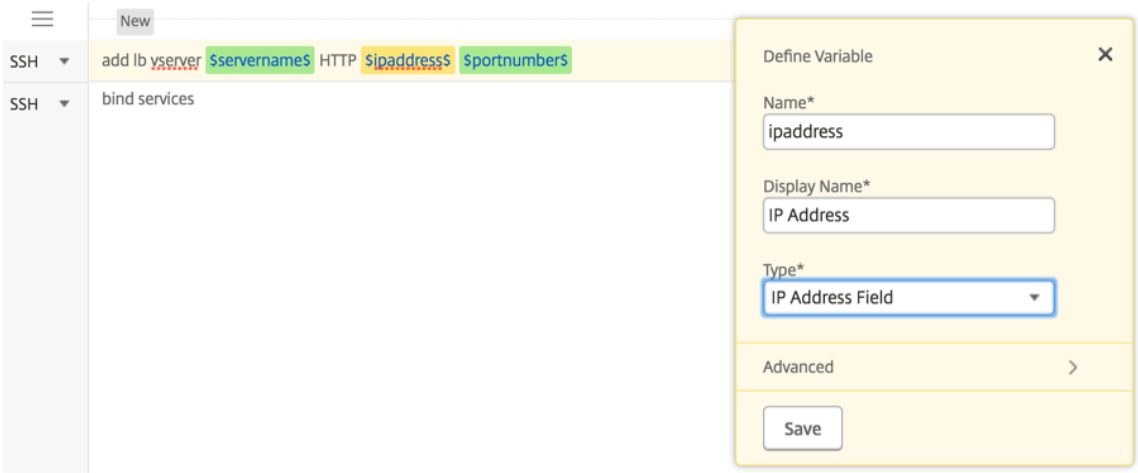
**Para crear un trabajo de configuración definiendo variables en Citrix ADM:**

1. Vaya a **Redes** > **Trabajos de configuración**.
2. Haga clic en **Crear trabajo**.
3. En la página **Crear trabajo**, seleccione los parámetros personalizados del trabajo, como el nombre del trabajo, el tipo de instancia y el tipo de configuración.
4. En el Editor de configuración, escriba los comandos para agregar un servidor virtual de equilibrio de carga, dos servicios y enlazar los servicios al servidor virtual. Haga doble clic para seleccionar los valores que quiere convertir en una variable y, a continuación, haga clic en **Convertir en variable**. Por ejemplo, seleccione la dirección IP del servidor de equilibrio de carga y `*ipaddress*`haga clic en **Convertir en variable** como se muestra en la imagen siguiente.

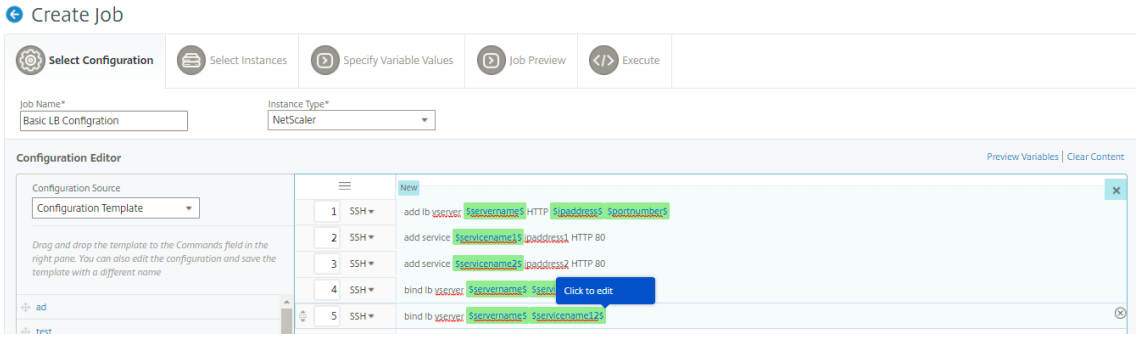
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Una vez que vea signos de dólar encierran el valor de la variable, haga clic en la variable para especificar más detalles de la variable, como el nombre, el nombre para mostrar y el tipo. También puede hacer clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable. Haga clic en **Guardar** y, a continuación, haga clic en **Siguiente**.

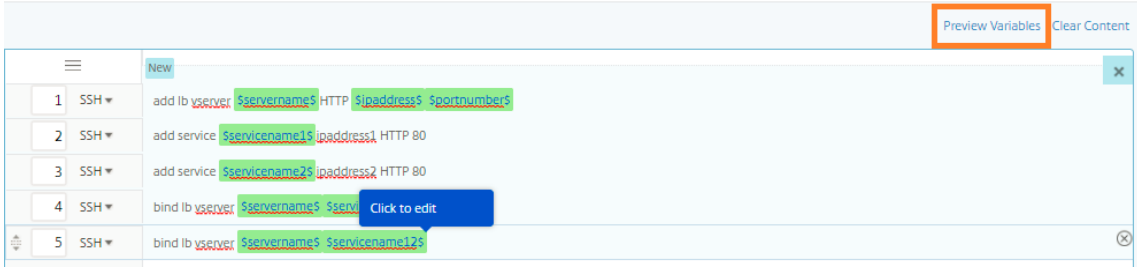



Escriba el resto de sus comandos y defina todas las variables.

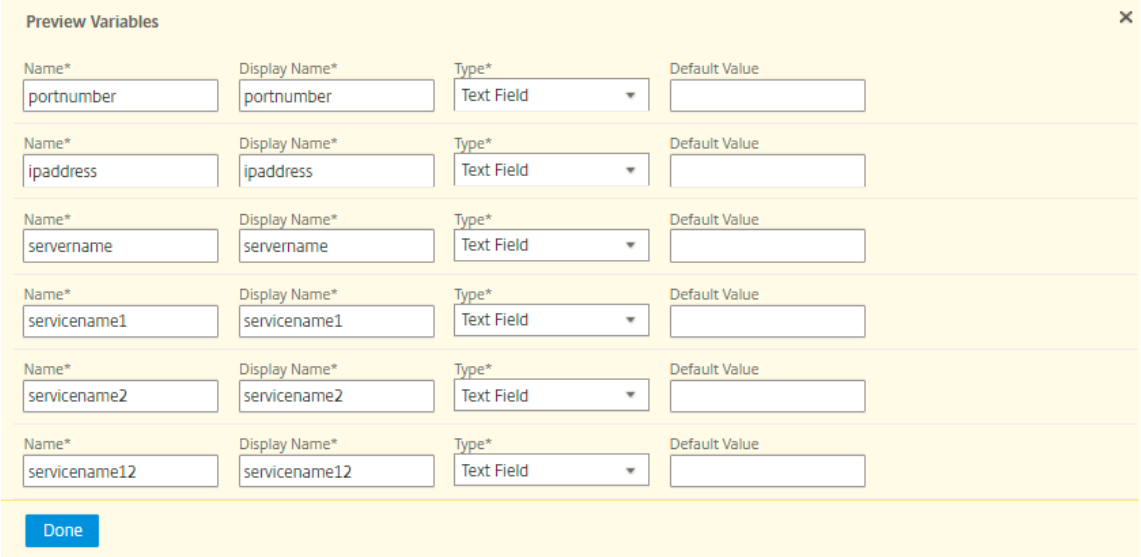



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
7. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
8. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.




9. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.




10. A continuación, puede reorganizar y reordenar los comandos en el editor de configuración

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

según corresponda. Puede mover el comando de una línea a otra arrastrando y soltando la línea de comandos. También puede mover o reorganizar la línea de comandos de una línea a cualquier línea de destino simplemente cambiando el número de línea de comandos en el cuadro de texto.

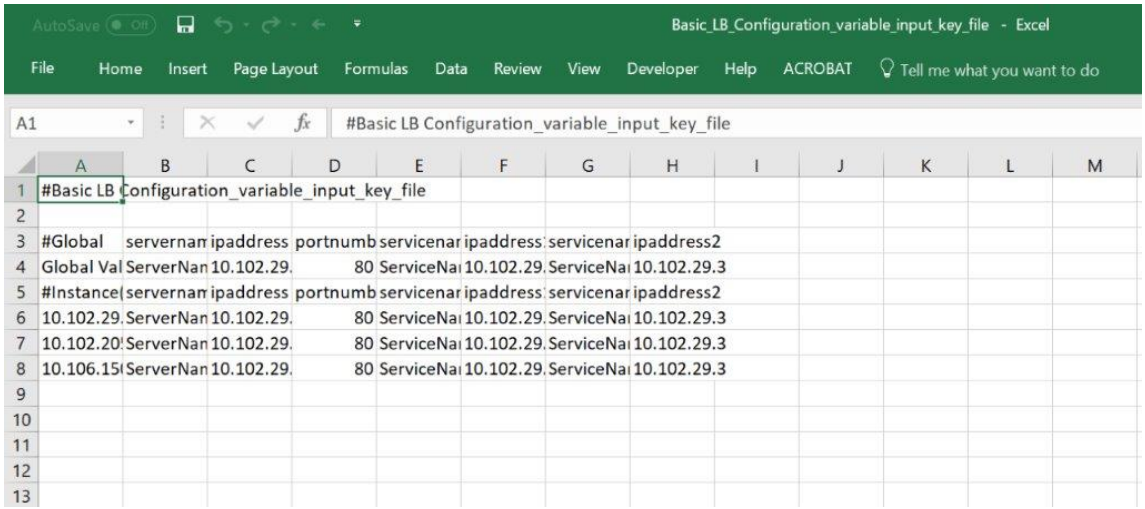
11. Seleccione las instancias en las que quiere ejecutar el trabajo de configuración.
12. En la ficha **Especificar valores variables**, seleccione la opción **Cargar archivo de entrada para valores variables**y, a continuación, haga clic en **Descargar archivo clave de entrada**. En nuestro ejemplo, deberá especificar el nombre del servidor en cada instancia, las direcciones IP del servidor y los servicios, los números de puerto y los nombres de servicio. Guarde el archivo y cárguelo. Si sus valores no están definidos con precisión, el sistema podría generar un error.
13. El archivo de claves de entrada se descarga en el sistema local y puede editarlo especificando los valores de las variables para cada instancia de Citrix ADC que haya seleccionado anteriormente y haciendo clic en **Cargar para cargar** el archivo de claves de entrada en Citrix ADM. Haga clic en **Siguiente**. El archivo de clave de entrada se descarga en su sistema local y puede modificarlo especificando los valores de las variables para cada instancia de Citrix ADC que haya seleccionado anteriormente.

    > **Nota** En el archivo de clave de entrada, las variables se definen en tres niveles:
    >
    > - Nivel mundial
    > - Nivel de grupo de instancias
    > - Nivel de instancia

    Las variables globales son valores variables que se aplican a todas las instancias. Los valores de las variables de nivel de grupo de instancias se aplican a todas las instancias que se definen en un grupo. Los valores de las variables de nivel de instancia solo se aplican a una instancia específica.

    Citrix ADM da la primera prioridad a los valores a nivel de instancia. Si no se proporcionan valores a las variables de las instancias individuales, Citrix ADM utiliza el valor proporcionado a nivel de grupo. Si no se proporcionan valores a nivel de grupo, Citrix ADM utiliza el valor de la variable proporcionado a nivel global. Si proporciona una entrada para una variable en los tres niveles, Citrix ADM utiliza el valor de nivel de instancia como valor predeterminado.
14. Haga clic en **Cargar** para cargar el archivo de claves de entrada en Citrix ADM. Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Importante**
>
> Cuando subes un archivo CSV desde un Mac, el Mac almacena el archivo CSV con punto y coma en lugar de comas. Esto hará que la configuración falle al cargar el archivo de entrada y ejecutar el trabajo. Si está utilizando un Mac, utilice un editor de texto para realizar los cambios necesarios y, a continuación, cargue el archivo.

15. También puede proporcionar valores de variable comunes en todas las instancias y hacer clic en **Cargar**para cargar el archivo de clave de entrada en Citrix ADM.

    Los archivos de entrada clave que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

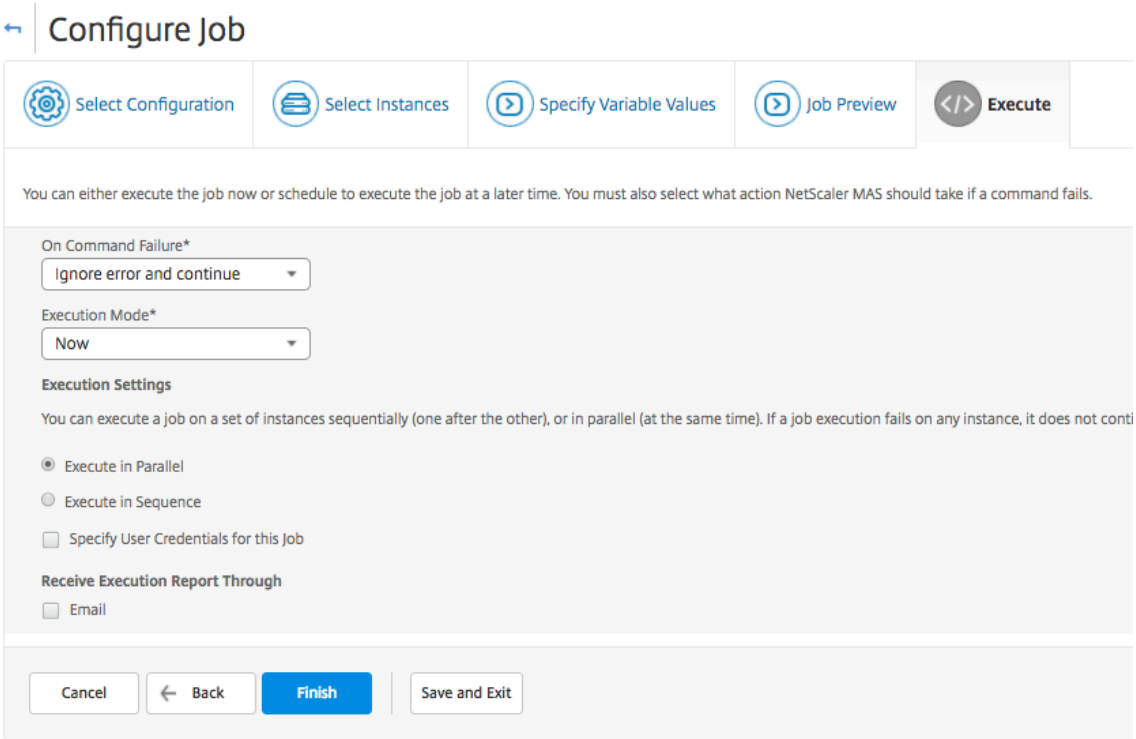
    Para ver los trabajos de configuración en ejecución al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

    Para ver los trabajos de configuración ya ejecutados al editar un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

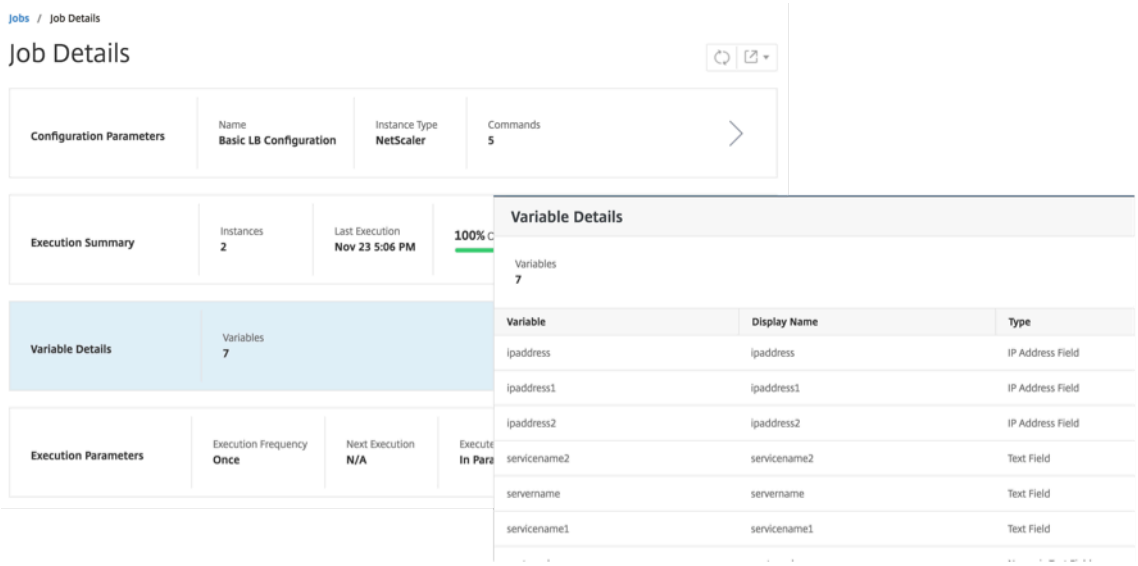
16. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

17. En la ficha **Ejecutar**, puede optar por ejecutar el trabajo ahora o programarlo para que se ejecute posteriormente. También puede elegir qué acción debe tomar Citrix ADM si el comando falla y si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo junto con otros detalles.




Después de configurar los trabajos y ejecutarlos, puede ver los detalles del trabajo navegando a **Redes** > **Trabajos de configuración** y seleccione el trabajo que acaba de configurar. Haga clic en **Detalles** y, a continuación, haga clic en **Detalles de variable** para ver la lista de variables agregadas a su trabajo.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Citrix ADM conserva los valores que ha proporcionado para las variables en **PASO 5** al guardar el trabajo y salir, o al programar la ejecución de un trabajo en un momento posterior.

## Crear trabajos de configuración a partir de comandos correctivos

January 30, 2024

Puede utilizar la función de plantilla de auditoría de Citrix Application Delivery Management (ADM) para supervisar los cambios de configuración en las instancias administradas de Citrix ADC y solucionar errores de configuración.

El flujo de trabajo típico para auditar los cambios de configuración mediante plantillas de auditoría consiste en los siguientes pasos:

1. Cree una plantilla de auditoría con un conjunto de comandos Citrix ADC válidos o esperados para auditar las configuraciones de instancias.
2. Seleccione las instancias de Citrix ADC en las que quiere ejecutar la plantilla de auditoría para comprobar si existen diferencias entre la configuración en ejecución y las configuraciones esperadas.
3. Comprenda los comandos diferenciales y correctivos y utilice la función "Crear tarea"para llevar las configuraciones de la instancia al estado deseado

Considere un caso en el que varios administradores administran cinco instancias de Citrix ADC. Todos estos administradores actualizan la configuración de la instancia existente a medida que se necesitan cambios. El superadministrador quiere asegurarse de que un determinado conjunto de configuraciones importantes permanece intacto independientemente de los cambios realizados por otros administradores. Para este caso de uso, el superadministrador crea una plantilla de la configuración que se espera que esté presente en las instancias de Citrix ADC y la ejecuta en las instancias. Citrix ADM compara la configuración de la plantilla de auditoría con la configuración en ejecución e informa de cualquier discrepancia en el panel **de auditoría de configuración**.

Si observa que hay un cambio en la configuración de algunas instancias, puede usar la función de comandos correctivos de Citrix ADM para crear un trabajo de configuración con los comandos de configuración modificados y corregidos para instancias específicas de Citrix ADC.

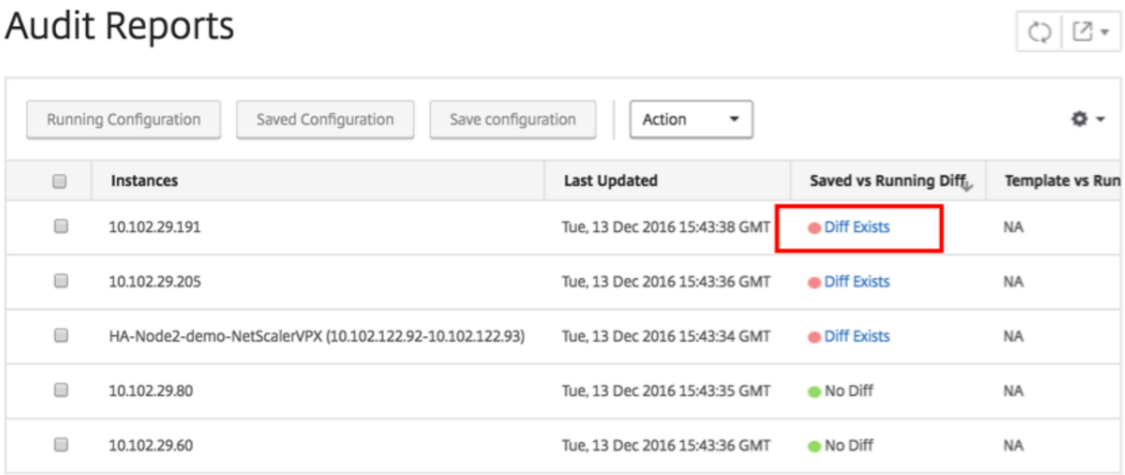
Si existe alguna diferencia entre la configuración de la plantilla de auditoría y la configuración en ejecución, aparecerá un mensaje de estado **Diff Exists** en la página **Informe de auditoría**. Al hacer clic

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

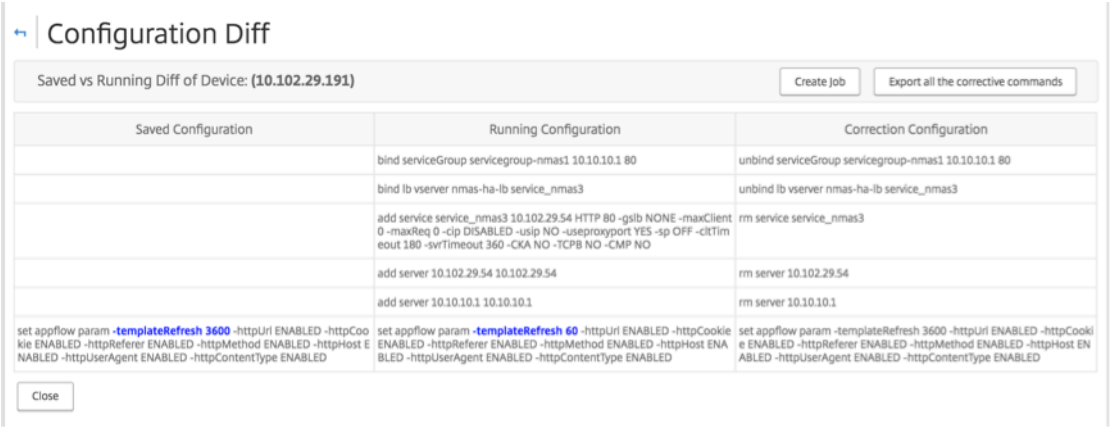
en el enlace **Diff Exits** , accederá a la página **Configuration Diff** , donde podrá ver el comando correctivo. También puede utilizar estos comandos correctivos para crear un trabajo de configuración y ejecutarlo en las instancias específicas de Citrix ADC para que vuelvan a la configuración deseada.

### Para crear un trabajo de configuración a partir de comandos correctivos en Citrix ADM

1. Vaya a **Redes** > **Auditoría de configuración**.
2. En la página **Auditoría de configuración**, haga clic dentro de cualquiera de los dos gráficos de donut para acceder a la página **Informes de auditoría**.
3. Haga clic en el enlace **Diff Exists(en la columna Diferencia entre guardados y en ejecución**de la tabla) de la instancia para la que quiera corregir los comandos de configuración. Aparecerá la página**Configuración Diff**, en la que se enumeran las diferencias entre la configuración guardada, la configuración en ejecución y la configuración de corrección para esa instancia.




4. Haga clic en **Crear Trabajo** para ir a la página **Crear Trabajo**, en la que se rellenan los comandos correctivos. Para obtener instrucciones sobre cómo crear un trabajo de configuración, consulte Cómo crear un trabajo de configuración en Citrix ADM.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Replicar la configuración en ejecución y guardada de una instancia de Citrix ADC a otra

January 30, 2024

24 de mayo de 2018

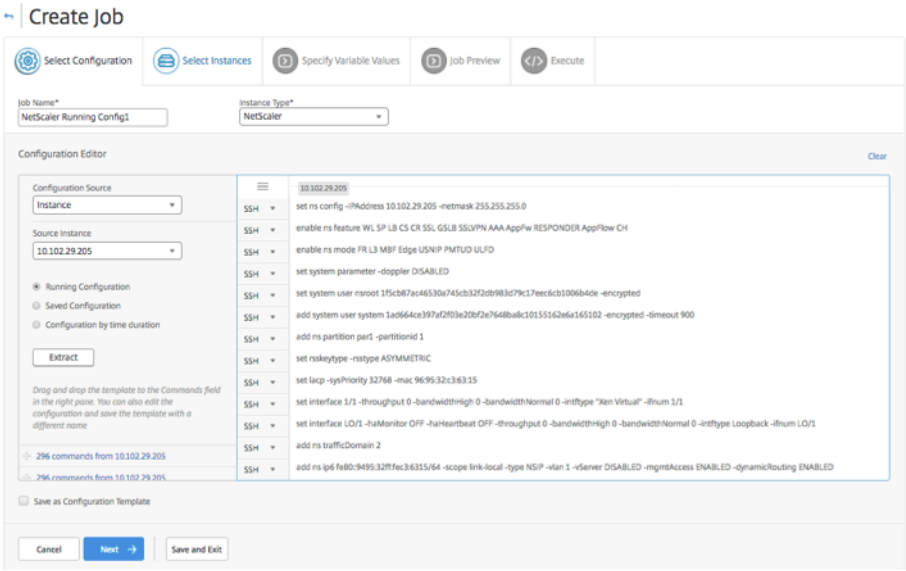
Ahora puede replicar la configuración de una instancia de Citrix ADC en otras instancias. Cuando configure un trabajo en Citrix ADM, seleccione una instancia como origen de configuración y elija la configuración en ejecución o guardada de la instancia seleccionada.

Por ejemplo, cuando selecciona **Ejecutar configuración** y hace clic en **Extraer**, Citrix ADM envía una solicitud a la instancia de Citrix ADC seleccionada para localizar la configuración en ejecución y la muestra como una plantilla. Puede arrastrar la plantilla al campo **Comandos** del panel derecho. Puede modificar los comandos, parámetros e instancias.

**Para replicar comandos de configuración en ejecución y guardados de una instancia en otra instancia en Citrix ADM:**

1. Vaya a **Redes** > **Trabajos de configuración**y haga clic en **Crear trabajo**.
2. Especifique el nombre del trabajo y el tipo de instancia. Por ejemplo, especifique *Citrix ADC Running Config1* como nombre de trabajo y el tipo de instancia como *Citrix ADC*.
3. Seleccione **Instancia** como **Origen de configuración**, seleccione la instancia de origen cuya configuración quiere replicar en otras instancias.
4. Verá las tres opciones siguientes:
   - Ejecución de la configuración
   - Configuración guardada
   - Configuración por duración de tiempo
5. Seleccione **Configuración en ejecución**y haga clic en **Extraer**. Se muestra el número de comandos de configuración ejecutados en esa instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Arrastre los comandos en el campo **Comandos** del panel derecho.
7. Puede modificar los comandos en el campo Comandos. Por ejemplo, si los comandos extraídos van a configurar una instancia de Citrix ADC. Esto podría incluir agregar particiones, configurar el equilibrio de carga, vincular el servidor de equilibrio de carga a servicios, etc. Es posible que quiera modificar los comandos para configurar las nuevas instancias de Citrix ADC sin particiones. Por lo tanto, para eliminar particiones, elimine manualmente los comandos relacionados con la creación de particiones y haga clic en **Siguiente**.
8. Haga clic en **Agregar instancias** y agregue las instancias en las que quiera aplicar los comandos de configuración en ejecución. Haga clic en **Aceptar** y, a continuación, en **Siguiente**.
9. Si ha especificado variables en los comandos, en la pestaña **Especificar valores** de variables , haga clic en **Descargar archivo de claves** de entrada . En el archivo descargado, especifique los valores de las variables y, a continuación, cargue el archivo a Citrix ADM.
10. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.

11. En la ficha **Ejecutar**, puede optar por ejecutar el trabajo ahora o programarlo para que se ejecute más tarde. También puede elegir qué acción debe realizar Citrix ADM el comando falla y si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo junto con otros detalles.

## Reutilizar trabajos de configuración de ejecución

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

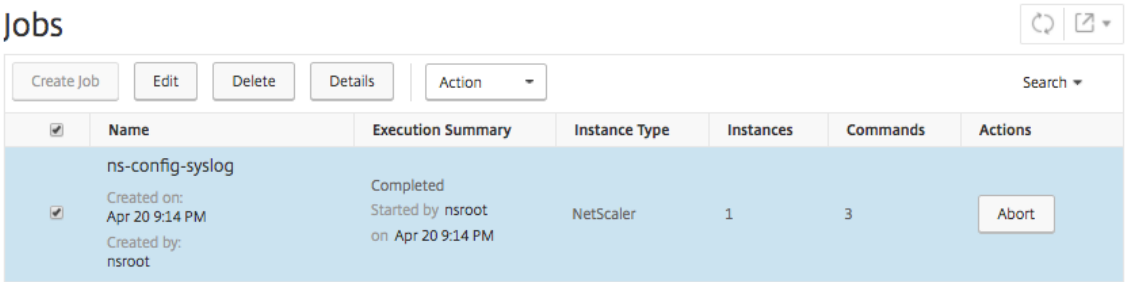
Los trabajos de configuración le permiten crear un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. También puede ejecutar el mismo conjunto de trabajos de configuración guardados después de modificar los comandos, los parámetros, el origen de configuración y las instancias del trabajo. Esto resulta útil cuando los mismos conjuntos de comandos tienen que ejecutarse en una instancia diferente, o cuando el trabajo encuentra un error y detiene la ejecución posterior.

Citrix Application Delivery Management (ADM) proporciona una función para ejecutar de nuevo los trabajos completados. Con esta función, los trabajos que se ejecutan completamente se pueden ejecutar de nuevo sin cambiar el nombre del trabajo.

> **Nota** Puede volver a ejecutar solo aquellos trabajos que se ejecutan cuando el modo de ejecución es "Ahora".

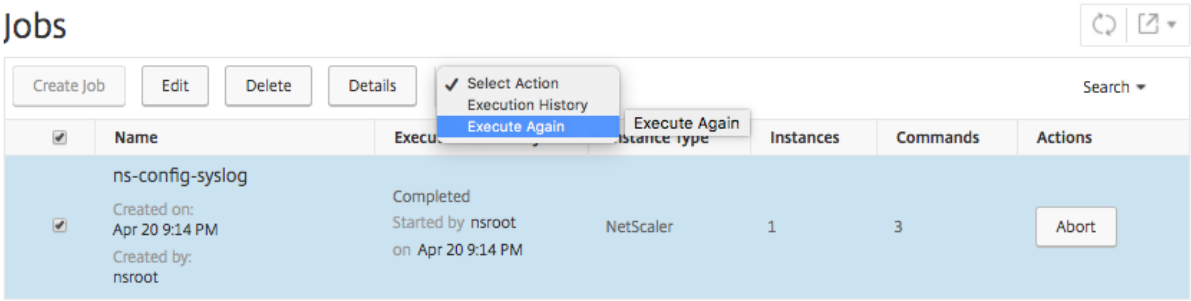
**Para modificar trabajos completados:**

1. En la página principal de Citrix ADM, vaya a **Redes > Trabajos de configuración**.
2. En la página **Trabajos**, seleccione un trabajo que muestre el resumen de ejecución como completado y haga clic en **Modificar**. También puede modificar un trabajo de configuración programado.
3. En la página **Configurar trabajo**, puede ver que el nombre del trabajo y el tipo de instancia no son modificables. Puede modificar otros campos, como la fuente de configuración, agregar instancias, modificar los valores de las variables y establecer los ajustes de ejecución.
4. Haga clic en **Finalizar** para ejecutar de nuevo el trabajo de configuración.




> **Nota**
>
> También puede seleccionar el trabajo y volver a hacer clic en **Ejecutar** para ejecutar el trabajo sin modificar ningún origen, instancia ni comando. Esto resulta útil cuando se tiene que ejecutar el mismo conjunto de comandos en las mismas instancias. A veces, el trabajo puede encontrar un error transitorio desde el lado del servidor y es posible que tenga que volver a ejecutar el trabajo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Programar trabajos creados mediante plantillas integradas

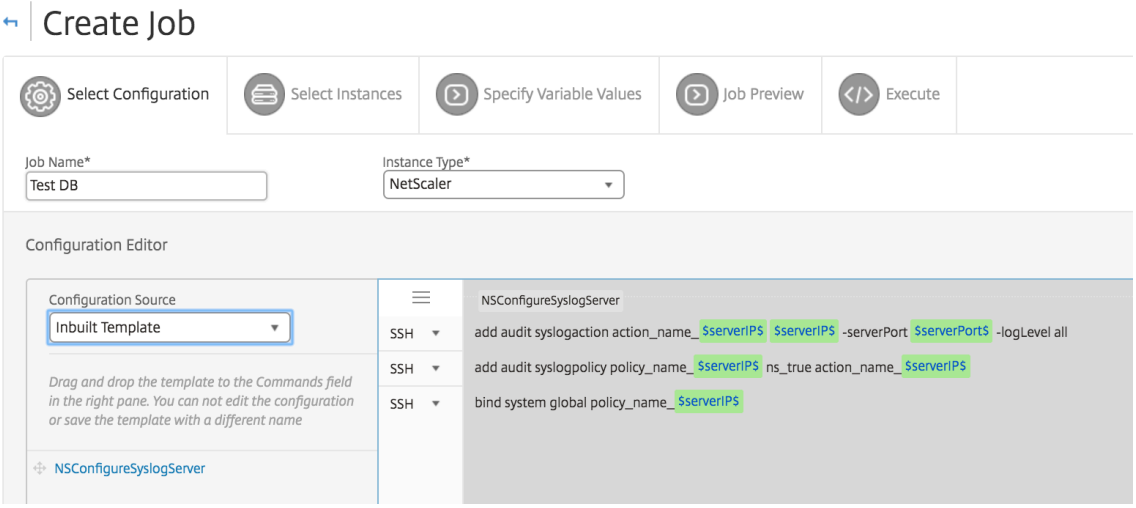
January 30, 2024

Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, utilice la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. También puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute en una etapa posterior.

### Para programar un trabajo mediante plantillas integradas en Citrix Application Delivery Management (ADM)

1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración**y, a continuación, haga clic en **Crear**trabajo.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo** y seleccione el **Tipo de Instancia** en la lista desplegable.
3. Seleccione **Plantilla incorporada** en la lista desplegable **Origen de configuración**. Arrastre el comando ***NSConfigureSyslogServer** al panel derecho y, a continuación, haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

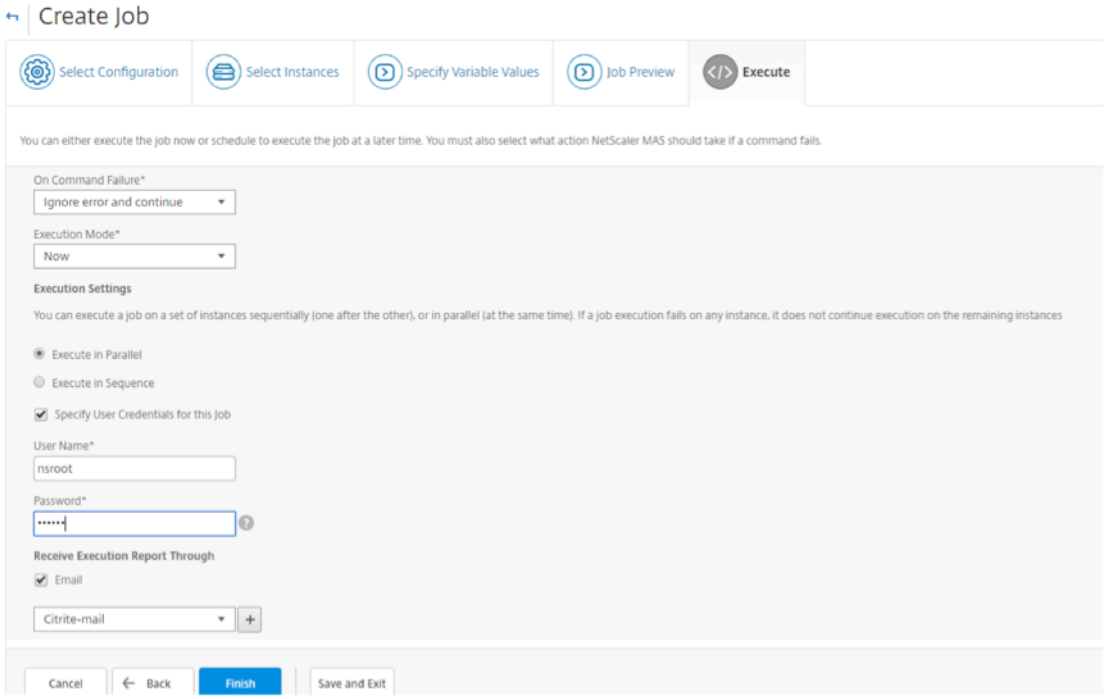



4. En la ficha **Seleccionar instancias**, haga clic en **Agregar instancias**, seleccione las instancias en las que quiere ejecutar el trabajo y, a continuación, haga clic en **Aceptar**.
5. Haga clic en **Siguiente**. En la ficha **Especificar valores variables**, seleccione una de las siguientes opciones para especificar las variables de sus instancias:
   - **Valores de variables de un archivo de entrada**: Descargue un archivo de entrada para introducir valores para las variables que ha definido en los comandos. A continuación, cargue el archivo en el servidor Citrix ADM.
   - **Valores de variables comunes para todas las instancias**: Especifique la dirección IP y el puerto del servidor syslog.
6. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
7. Haga clic en **Siguiente**.
8. En la ficha **Ejecutar**, defina las siguientes condiciones:
   - **En caso de error de comando**: si falla un comando, puede elegir ignorar los errores y continuar ejecutando el trabajo o detener la ejecución posterior del trabajo. Elija la acción que quiere ejecutar en la lista desplegable.
   - **Modo de ejecución**: Puede ejecutar el trabajo ahora o programar para ejecutar el trabajo más tarde. Si quiere programar el trabajo más adelante, debe especificar la configuración de frecuencia de ejecución para ese trabajo. Elija el cronograma que quiere que siga el trabajo en la lista desplegable.
9. También puede ejecutar un trabajo en un conjunto de instancias secuencialmente o en paralelo seleccionando el método necesario en **Configuración de ejecución**. Si se produce un error en la ejecución de un trabajo en cualquier instancia, no continúa en las instancias restantes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede optar por permitir que los usuarios autorizados ejecuten trabajos en las instancias administradas. También se puede enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.

10. Haga clic en **Finalizar**.




## Utilizar trabajos de mantenimiento para actualizar instancias de NetScaler ADC SDX

January 30, 2024

Puede realizar una actualización de un solo paquete de las instancias de NetScaler ADC SDX que ejecuten NetScaler ADC versión 11.0 y posterior. Para realizar una actualización de un solo paquete, utilice una tarea integrada en NetScaler ADM. Con esta tarea integrada, puede actualizar Citrix ADC SDX Management Service, Citrix Hypervisor y los paquetes y parches complementarios para Citrix Hypervisor.

**Para actualizar instancias de NetScaler ADC SDX con NetScaler ADM:**

1. Vaya a **Redes > Trabajos de Configuración > Trabajos de Mantenimiento**.
2. Haga clic en **Crear trabajo**. En la página **Crear Trabajo**, seleccione la tarea integrada **Actualizar NetScaler ADC SDX** para actualizar las instancias de NetScaler ADC SDX. Haga clic en **Continuar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la página**Actualizar dispositivos NetScaler ADC**, en la ficha**Selección de instancias**, especifique el**nombre del trabajo**y haga clic en**Agregar instancias.**
4. Seleccione las instancias de destino o los grupos de instancias que quiere actualizar.
5. Después de agregar las instancias o grupos de instancias de NetScaler ADC, haga clic en**Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas. La pantalla informa del progreso de la validación previa de cada una de las instancias NetScaler ADC.
6. En la página**Modificar actualización de NetScaler ADC Appliance (s)**, seleccione la ficha**Actualización**. En el menú desplegable**Imagen de software**, seleccione**Local**(su equipo local) o**Appliance**(el archivo de compilación debe estar presente en NetScaler ADM).
7. También puede ver si alguna instancia tiene errores de actualización previa a la validación. Estos errores se muestran en forma de mensaje. Los mensajes muestran los errores relacionados con el espacio en disco, la unidad de disco duro y la personalización del usuario. Si no quieres continuar con las instancias que no superaron la comprobación de actualización previa a la validación, puedes eliminar las instancias. Para eliminar las instancias, selecciónelas y haga clic en **Eliminar.**
8. En la ficha**Planificar tarea**, también puede establecer detalles de ejecución en los que puede realizar el proceso de actualización ahora o programarlo para una fecha posterior. También puede optar por realizar una copia de seguridad de su instancia de NetScaler ADC SDX, recibir un informe de ejecución por correo electrónico o realizar una actualización en dos etapas para nodos de HA.

La actualización de dos etapas para nodos en HA le da la opción de realizar la actualización inmediatamente o programar una hora para que los nodos se actualicen uno tras otro.La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.

## Crear trabajos de configuración para instancias Citrix SD-WAN WANOP

January 30, 2024

Un trabajo es un conjunto de comandos de configuración que se pueden crear y programar en una o más instancias administradas. Para las instancias WANOP de Citrix SD-WAN, puede usar las siguientes opciones para crear trabajos:

- **Plantilla de configuración**: puede usar el editor de configuración para escribir los comandos de la CLI, guardar la configuración como una plantilla y usarla para configurar los trabajos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Plantilla incorporada**: puede elegir de una lista de plantillas de configuración. Estas plantillas proporcionan las sintaxis de los comandos CLI y permiten especificar valores para las variables. Las plantillas integradas aparecen en la lista, con sus descripciones en la tabla siguiente.
- **Archivo**: Puede cargar un archivo de configuración desde su máquina local y crear trabajos.

Una vez creado un trabajo, puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute más tarde. También puede establecer la frecuencia de ejecución

| Plantilla incorporada | Descripción |
|---|---|
| Activar Cloudbridge WAN Opt | Permite el tráfico a través del dispositivo Citrix SD-WAN WANOP. |
| DisableCloudBridgeWANOpt | Deshabilita el tráfico a través del dispositivo Citrix SD-WAN WANOP. |
| RestartCloudBridgeWANOpt | Reinicia el dispositivo Citrix SD-WAN WANOP. |
| RestoreConfig | Restaura la configuración del dispositivo Citrix SD-WAN WANOP. |
| AddLink | La creación o definición de enlaces permite que el dispositivo SD-WAN WANOP evite la congestión y la pérdida de los enlaces y realice el modelado del tráfico. Puede definir el ancho de banda máximo enviado o recibido a través del enlace y también especificar que es tráfico de lado LAN o WAN. |
| Configurar ancho de banda | Establece los límites del ancho de banda y otros ajustes de administración del ancho de |
| Agregar usuario | Agrega un usuario nuevo, al que puede asignar privilegios. |
| AddUserAdvancedPlatform | Agrega un nuevo usuario permite asignar privilegios no disponibles en la `AddUser` plantilla. |
| AddService-class | Crea una clase de servicio para el dispositivo Citrix SD-WAN WANOP con una o más clases de servicio filtros y la habilita. |
| SetApplication | Establece la definición del clasificador de aplicaciones. |
| Agregar o eliminar puertos de almacenamiento en caché de vídeo | Añade o elimina el número de puerto en el que la fuente de vídeo puede enviar o recibir datos. El puerto predeterminado es 80. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Plantilla incorporada | Descripción |
|---|---|
| RemoveVideoCachingSource | Quita uno o más orígenes de almacenamiento en caché de vídeo. Especifique la dirección IP de origen de vídeo o el nombre de dominio. |
| Eliminar todo el almacenamiento en caché de vídeo | Elimina todas las fuentes de almacenamiento en caché de vídeo disponibles. |
| Estado de caché de vídeo | Activa o desactiva la función de almacenamiento en caché de vídeo en los dispositivos Citrix SD-WAN WANOP. |
| Borrar almacenamiento en caché | Borra la caché de vídeo o las estadísticas de almacenamiento en caché de vídeo. |
| Configurar almacenamiento de vídeo | Establece el tamaño máximo de los objetos en caché. Los objetos que superen este límite no se almacenan en caché. De forma predeterminada, el tamaño máximo del objeto de almacenamiento en caché es de 100 MB. |
| Agregar fuente de caché de vídeo | Añade la dirección IP o el nombre de dominio de la fuente de vídeo. Incluye opciones para habilitar o deshabilitar el almacenamiento en caché de vídeo para esa fuente. |
| Configurar servidor de licencias remoto | Configura el servidor de licencias centralizado. Especifique el modelo del servidor de licencias, la dirección IP y el número de puerto. |
| Configurar el servidor de licencias local | Establece la ubicación del servidor de licencias como local. |
| InstallCACert | Instala los certificados de CA en el dispositivo Citrix SD-WAN WANOP. Especifique el nombre del certificado, el nombre del archivo y la contraseña del almacén de claves. |
| Instale Combined Cer Key | Instala un par de archivos combinados de claves de certificado SSL. |
| Instala una clave de cert independiente | Instala el certificado SSL y la clave como archivos separados. |
| Activar WCCP | Activa el modo de despliegue del WCCP. |
| AddWCCPServiceGroup | Agrega una nueva definición de grupo de servicios WCCP para el dispositivo Citrix SD-WAN WANOP. |
| DisableWCCP | Desactiva el modo de despliegue del WCCP. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Plantilla incorporada | Descripción |
|---|---|
| Agregar directiva de modelado de tráfico | Crea una directiva de modelado de tráfico para el dispositivo Citrix SD-WAN. La directiva controla el ancho de banda de la red. |
| SetTrafficShapingPolicy | Modifica la política de modelado del tráfico del dispositivo Citrix SD-WAN WANOP. La directiva controla el ancho de banda de la red. |
| Agregar prepoblación de vídeo | Crea una entrada de prepoblación de vídeo, que le permite descargar y almacenar en caché un vídeo por adelantado. También puede especificar cuándo almacenar en caché un vídeo. |
| Actualizar la prepoblación de vídeos | Modifica una entrada de prepoblación de vídeo, que especifica cuándo almacenar en caché un vídeo. |
| Agregue la prepoblación de vídeos ahora | Configura la prepoblación de vídeo, lo que le permite descargar y almacenar en caché un vídeo inmediatamente. Puedes controlar cómo quieres descargar y almacenar en caché los vídeos desde las URL. |
| VideoPrePopulationState | Cambia, inicia, actualiza o elimina la prepoblación de vídeos. |
| Configurar Syslog Server | Establece la dirección IP y el número de puerto del servidor syslog. |
| Configurar alerta | Configura el nivel de alerta. |

**Para crear un trabajo de configuración para instancias de Citrix SD-WAN WANOP**:

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración** y, a continuación, haga clic en **Crear trabajo**.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo**.
3. En el campo **Tipo de instancia**, seleccione **Citrix SD-WAN WO**.
4. En la lista desplegable **Fuente de configuración**, seleccione una opción para crear un trabajo.

> **Nota**
>
> Seleccione **Guardar como plantilla de configuración** y especifique un nombre para

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> guardar la configuración como plantilla y volver a utilizarla.

5. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
6. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
7. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.
8. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.
9. Haga clic en **Siguiente** y, a continuación, en la pestaña **Seleccionar instancias** , haga clic en **Agregar instancias.** Seleccione las instancias en las que desea ejecutar el trabajo y, a continuación, haga clic **en**Aceptar .
10. Haga clic en **Siguiente** y, a continuación, en la ficha **Especificar valores de variable**, seleccione una de las siguientes opciones para especificar variables para las instancias:
    - **Cargar archivo de entrada para valores de variables:** haga clic en **Descargar archivo de claves** de entrada para descargar un archivo de entrada. En el archivo de entrada, introduzca valores para las variables definidas en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
    - **Valores de variables comunes para todas las instancias**: introduzca valores para las variables. Las variables varían en función de la plantilla seleccionada.

    Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

    Para ver los trabajos de configuración de ejecución al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear Trabajo**. En la página**Crear Trabajo**. En

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

la ficha **Especificar valores de variable**, seleccione la opción **Valores de variable comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

Para ver los trabajos de configuración que ya se han ejecutado al modificar un trabajo de configuración, vaya a **Red > Trabajos de configuración**, seleccione el Nombre del trabajo y haga clic en **Modificar**. En la página **Configurar trabajo**, en la ficha **Especificar valores de variable**, seleccione la opción **Valores de variable comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y luego modifique y cargue los archivos (manteniendo el mismo nombre de archivo)

11. Haga clic en **Siguiente**, en la ficha **Vista previa del trabajo**, puede evaluar y verificar los comandos que se van a ejecutar como un trabajo.
12. Haga clic en **Siguiente**, en la ficha **Ejecutar**, establezca las condiciones siguientes:
    - **En caso de error de comando**: qué hacer si un comando falla: ignorar los errores y continuar con el trabajo o detener la ejecución posterior del trabajo. Elija una acción de la lista desplegable.
    - **Modo de Ejecución**: Ejecute el trabajo inmediatamente o programe la ejecución para un momento posterior. Si planifica la ejecución para un momento posterior, debe especificar la configuración de frecuencia de ejecución para el trabajo. Elija la programación que quiere que siga el trabajo en la lista desplegable **Frecuencia de ejecución**.
13. En **Configuración de ejecución**, seleccione si quiere ejecutar el trabajo secuencialmente (uno tras otro) o en paralelo (al mismo tiempo).
14. Para enviar un informe de ejecución de trabajos por correo electrónico a una lista de destinatarios, active la casilla de verificación **Correo electrónico** en la sección **Recibir informe de ejecución a través**. En la lista desplegable que aparece, elija una lista de distribución de correo electrónico. Para crear una lista de distribución de correo electrónico, haga clic en el icono **+** e introduzca las direcciones de correo electrónico de los destinatarios y los detalles del servidor de correo electrónico.
15. Haga clic en **Finalizar**.

## Utilizar la plantilla de configuración maestra

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El uso de una plantilla de configuración principal es una opción flexible para crear e implementar una configuración maestra en varias instancias de Citrix ADC.

Como administrador, es posible que desee realizar cambios en la configuración y guardar las licencias, los certificados y otros archivos en la instancia de ADC. Puede guardar la nueva configuración como una plantilla de configuración maestra (archivo.conf).

Para guardar la plantilla de configuración maestra desde una instancia de ADC, puede realizar una de las siguientes acciones:

- En la solicitud de comando, escriba **save ns config**. La configuración se guarda en la memoria FLASH de la instancia, en el archivo /nsconfig/ns.conf.
- Desde la interfaz gráfica de usuario de la instancia, vaya a **Diagnóstico** > **Ver configuración**. Elige el tipo de configuración que quieres guardar. Por ejemplo, si quieres guardar la configuración guardada de su instancia, selecciona **Configuración guardada en**.Haga clic en el enlace **Guardar texto en un archivo** para guardar el archivo 'ns.conf'en su equipo local.

Al implementar la plantilla de configuración maestra mediante la plantilla de configuración 'DeployMasterConfiguration'al crear un trabajo, puede personalizarla aún más para cada instancia de ADC específica agregando más comandos, modificando comandos existentes y proporcionando diferentes valores variables en el archivo de entrada.

Por ejemplo, como administrador, puede que desee cargar claves de certificado en sus instancias de ADC, además del archivo ns.conf, e implementar también la configuración maestra en ellas.

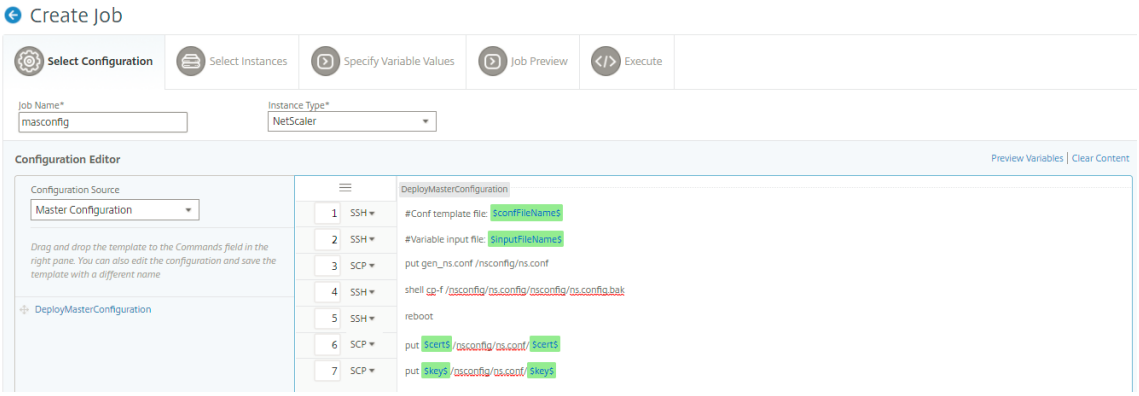
> **Importante**
>
> No puede ejecutar un trabajo de configuración mediante la plantilla DeployMasterConfiguration en instancias de Citrix ADC CPX, instancias configuradas en un clúster o en instancias ADC con particiones.

**Para crear un trabajo de configuración con la plantilla de configuración Master Config en Citrix ADM:**

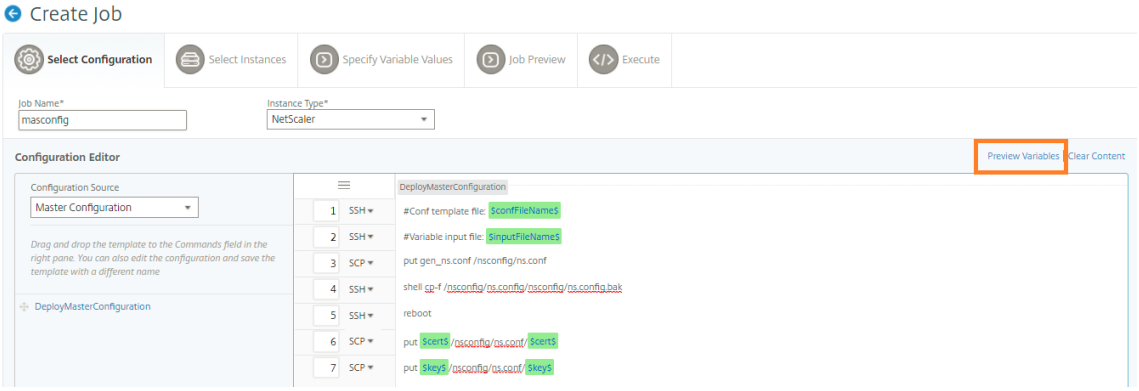
1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración**y, a continuación, haga clic en **Crear**trabajo.
2. En la página **Crear Trabajo**, en la ficha **Seleccionar Configuración**, especifique el **Nombre del Trabajo** y seleccione el **Tipo de Instancia** en la lista desplegable.
3. Seleccione **Configuración maestra** en la lista desplegable **Fuente de configuración**. Arrastre los comandos de la plantilla DeployMasterConfiguration al panel derecho. También puede agregar, modificar o eliminar comandos en el panel derecho. Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Puede agregar comandos ***put*** para agregar archivos de entrada a su plantilla. En nuestro ejemplo, debemos cargar archivos de certificado y clave además del archivo de plantilla de configuración y los archivos de entrada variable.

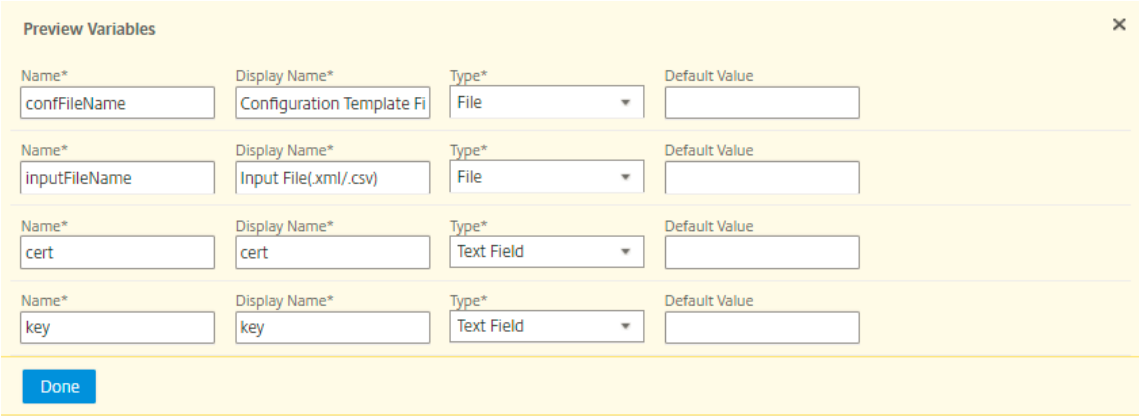



4. Puede revisar todas las variables que ha definido al crear o modificar un trabajo de configuración en una sola vista consolidada.
5. Siga uno de estos procedimientos para ver todas las variables en una sola vista consolidada:
   - Al crear un trabajo de configuración, vaya a **Redes > Trabajos de configuración**y seleccione **Crear trabajo**. En la página **Crear Trabajo**, puede revisar todas las variables que ha agregado al crear el trabajo de configuración.
   - Mientras edita un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar trabajo**, puede revisar todas las variables que se agregaron al crear el trabajo de configuración.
6. A continuación, puede hacer clic en la ficha **Vista previa de variables** para obtener una vista previa de las variables en una única vista consolidada que haya definido al crear o modificar un trabajo de configuración.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. Aparece una nueva ventana emergente que muestra todos los parámetros de variables como Nombre, Nombre para mostrar, Tipo y valor predeterminado en un formato tabular. También puede modificar y modificar estos parámetros. Haga clic en el botón **Listo** después de modificar o modificar cualquiera de los parámetros.




8. Seleccione las instancias en las que quiere ejecutar el trabajo de configuración y, a continuación, haga clic en **Siguiente**.

9. En la ficha **Especificar valores variables**, cargue lo siguiente:

   - **Archivo de plantilla de configuración (.conf)**: Cargue el archivo.conf que ha extraído de una instancia de ADC.
   - **Cargar el archivo de entrada (XML/CSV)**: Cargar el archivo de entrada con valores para las variables que ha definido en sus comandos.

   Aquí se proporciona un archivo xml de muestra para su uso. Asegúrese de que los archivos xml contienen los detalles correspondientes a las instancias ADC que está utilizando.

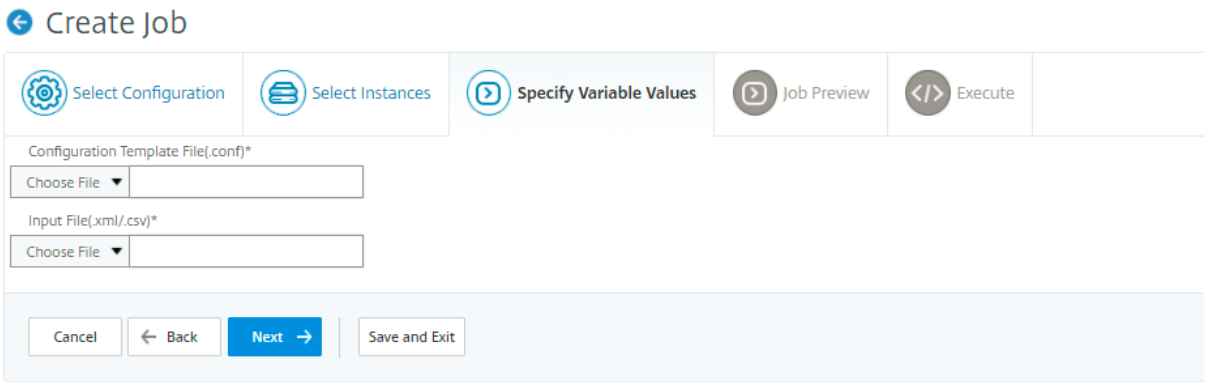
```xml
<?xml version="1.0" encoding="UTF-8" ?>

<properties>

<!--

Provide inputs for all the parameters defined in the master config file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific parameters and values.

If the same parameters are defined in global and instance tags, the instance specific parameters value will take precedence over the instance group. The instance group specific parameters value will take precedence over global parameters in the execution.
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
14
15  -  name. This attribute represents the name of the instance group.
16
17  -  device. This tag contains all the instance specific parameters
       and value.
18
19  If the same parameters are defined in global and instance tags,
       the instance specific parameters value will take precedence in
       the execution.
20
21  -  name. This attribute represents the IP Address of the instance.
        Host name is not supported for the attibute.
22
23  HA pair should be represented as <primaryip>-<secondaryip>.
       Example 10.102.2.1-10.102.2.2
24
25  In the template file, the parameter name must be specified within
       the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
       names are case sensitive.
26  -->
27
28  <global>
29
30  </global>
31  <devicegroup name="BLR_DEVS">
32  </devicegroup>
33  <device name="10.106.101.209">
34  <param name="IP" value="10.106.101.209"/>
35  </device>
36
37  <!-- HA PAIR-->
38  <!--<device name="10.102.43.154-10.102.43.155">
39  <param name="NSIP" value="10.102.43.154"/>
40  <param name="HostName" value="NS43HA"/>
41  <param name="LBSERVER" value="haserver43http"/>
42  <param name="SNMPTrapDest" value="10.102.43.130"/>
43  </device>-->
44  </properties>
```

10. Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



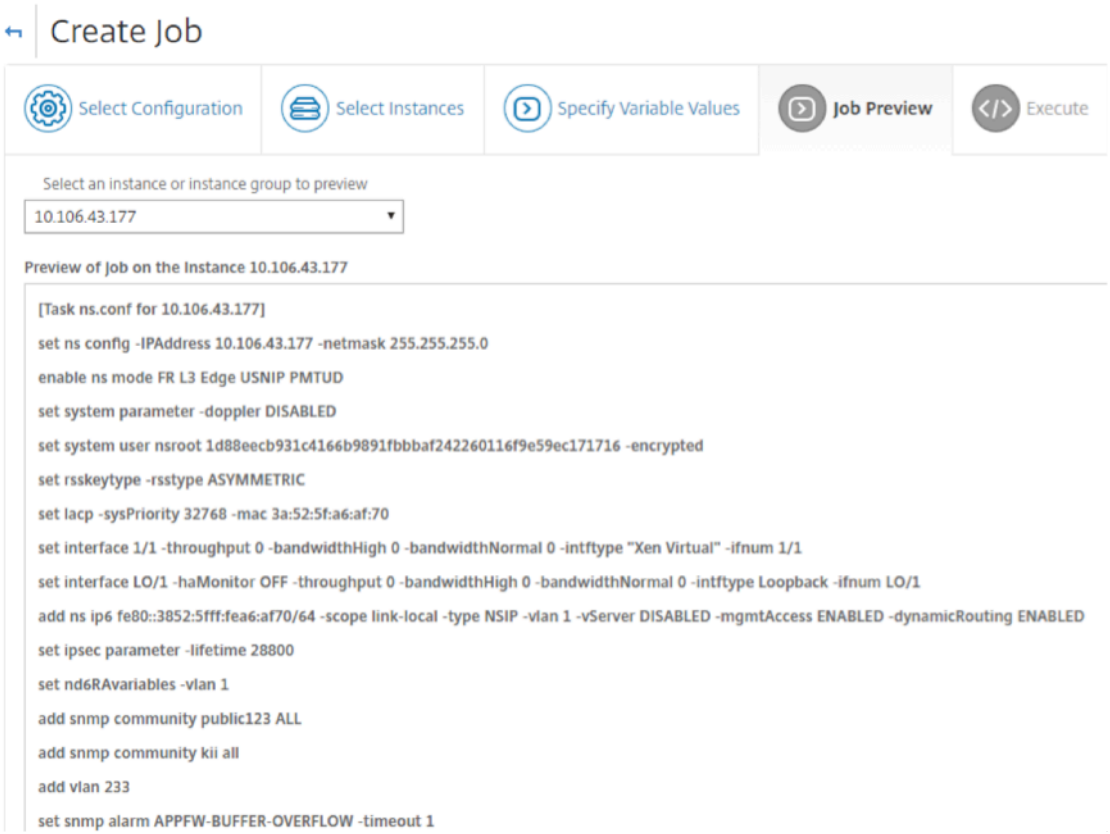

Los archivos de entrada que contienen los valores de las variables se conservan (con el mismo nombre de archivo) en los trabajos de configuración. Puede ver y modificar estos archivos de entrada que ha utilizado y cargado anteriormente al crear o modificar los trabajos de configuración.

Para ver los trabajos de configuración en ejecución al crear un trabajo de configuración, vaya a **Red > Trabajos de configuración**y haga clic en **Crear trabajo**. En la página **Crear trabajo**. En la ficha **Especificar valores de variables**, seleccione la opción **Valores de variables comunes para todas las instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

Para ver los trabajos de configuración ya ejecutados al editar un trabajo de configuración, vaya a **Red > Trabajos de configuración** , seleccione el nombre del trabajo y haga clic en **Editar** . En la página **Configurar Trabajo**, en la ficha **Especificar Valores de Variable**, seleccione la opción **Valores de Variable Comunes para todas las Instancias** para ver los archivos cargados. Para modificar los archivos de entrada, descargue el archivo de entrada y, a continuación, modifique y cargue los archivos (manteniendo el mismo nombre de archivo).

1. En la ficha **Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias y, a continuación, hacer clic en **Siguiente**.

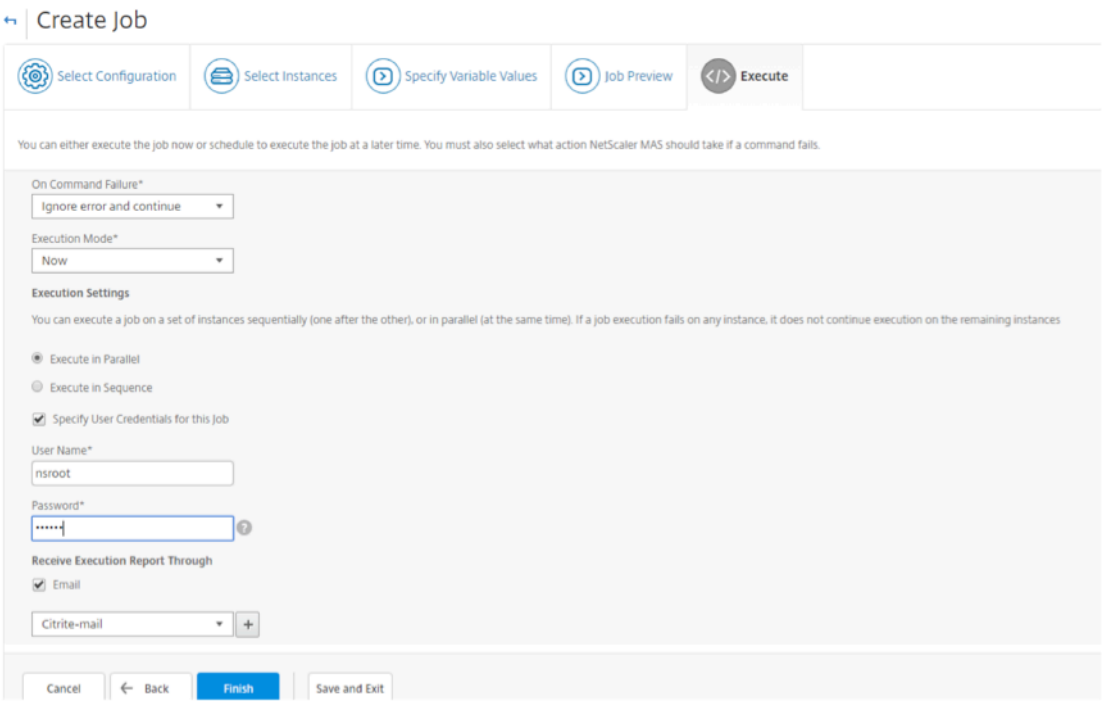
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



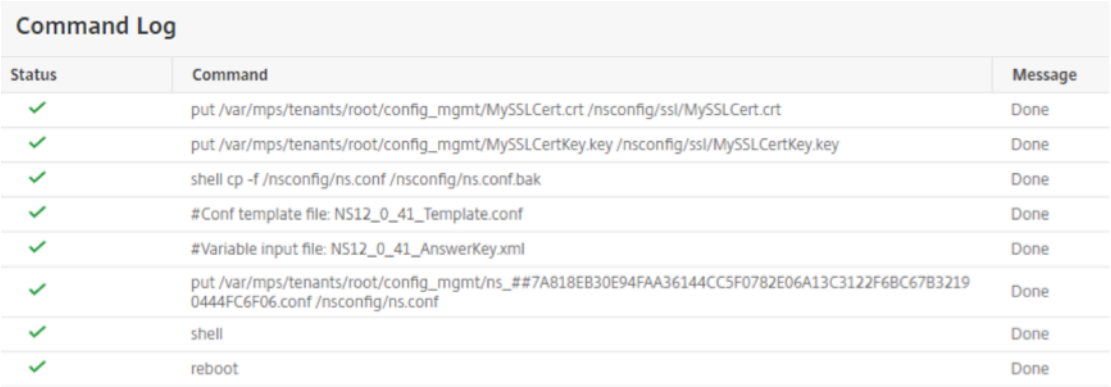

2. En la ficha**Ejecutar**, puede optar por ejecutar el trabajo ahora o programarlo para que se ejecute más tarde. También puede elegir qué acción debe realizar Citrix ADM si falla el comando.

   También puede optar por permitir que los usuarios autorizados ejecuten trabajos en las instancias administradas, y puede elegir si quiere enviar una notificación por correo electrónico sobre el éxito o el fracaso del trabajo, junto con otros detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Después de ejecutar el trabajo, puede ver los detalles del trabajo navegando a**Redes** >**Trabajos de configuración**y seleccione el trabajo que ha configurado. Haga clic en**Detalles**y, a continuación, haga clic en**Resumen de ejecución** para ver los detalles del trabajo. Haga clic en la instancia para ver los **registros de comandos** para ver los comandos ejecutados en el trabajo.



Command Log

| Status | Command | Message |
|---|---|---|
| ✓ | put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt | Done |
| ✓ | put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key | Done |
| ✓ | shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak | Done |
| ✓ | #Conf template file: NS12_0_41_Template.conf | Done |
| ✓ | #Variable input file: NS12_0_41_AnswerKey.xml | Done |
| ✓ | put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B3219 0444FC6F06.conf /nsconfig/ns.conf | Done |
| ✓ | shell | Done |
| ✓ | reboot | Done |

## Usar trabajos para actualizar instancias de Citrix ADC

January 30, 2024

Puede utilizar Citrix Application Delivery Management (ADM) para actualizar una o más instancias de Citrix ADC. Debe conocer el marco de licencias y los tipos de licencias antes de actualizar una instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cuando actualice la instancia de Citrix ADC creando un trabajo de mantenimiento, realice la comprobación previa a la validación de las instancias que quiere actualizar.

1. **Comprobar si hay personalizaciones**: Haga una copia de seguridad de sus personalizaciones y elimínelas de las instancias. Puede volver a aplicar las personalizaciones de copia de seguridad después de la actualización de la instancia.
2. **Comprobar el uso del disco**: Si la carpeta `/var` tiene menos de 6 GB de espacio y la carpeta `/flash` tiene menos de 200 MB de espacio, limpie el espacio en disco. Compruebe las siguientes rutas de carpetas para limpiar el espacio en disco:
   - `/var/nstrace`
   - `/var/log`
   - `/var/nslog`
   - `/var/tmp/support`
   - `/var/core`
   - `/var/crash`
   - `/var/nsinstall`
   - `/var/netscaler/nsbackup`
3. **Compruebe si hay problemas de hardware de disco**: Resuelva los problemas de hardware si los hay.

Puede actualizar un par ADC HA en dos etapas:

1. Cree un trabajo de actualización y ejecute en uno de los nodos inmediatamente o programe más tarde.
2. Programe el trabajo de actualización para que se ejecute en el nodo restante más adelante. Asegúrese de programar este trabajo después de la actualización del nodo inicial.

Al actualizar un par ADC HA, tenga en cuenta lo siguiente:

- El nodo secundario se actualiza primero.
- La sincronización y propagación de los nodos se desactivan hasta que ambos nodos se actualizan correctamente.
- Tras la actualización correcta del par HA, aparece un mensaje de error en el historial de ejecución. Este mensaje aparece si los nodos del par HA están en compilaciones o versiones diferentes. Este mensaje indica que la sincronización entre el nodo primario y secundario está inhabilitada.

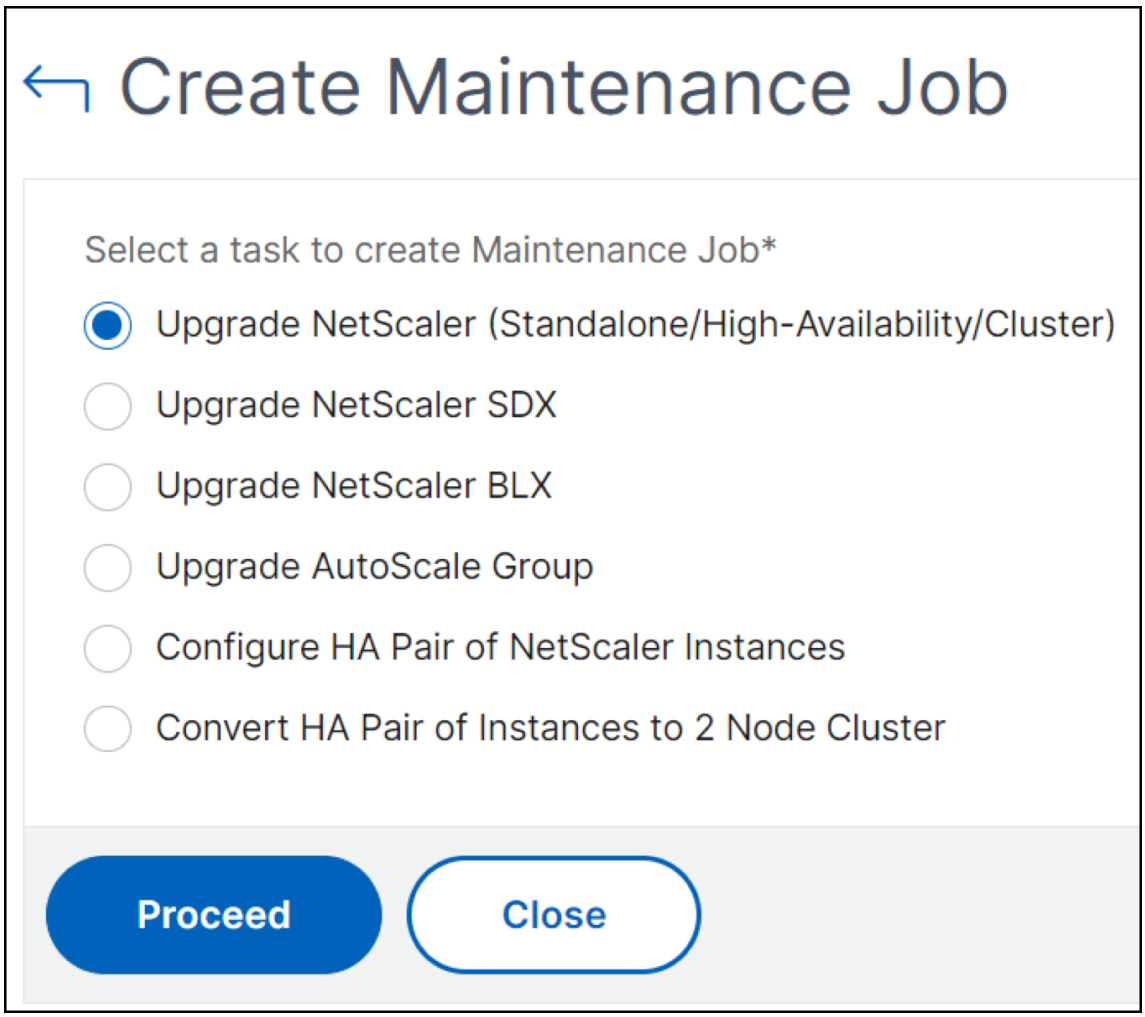
Al actualizar un clúster de ADC, el ADM realiza la validación previa a la actualización únicamente en la instancia especificada. Antes de realizar la actualización, compruebe y resuelva los problemas de personalización, uso del disco y hardware en los nodos del clúster.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Crear un trabajo de mantenimiento de actualización para actualizar instancias de ADC

> **Nota**
>
> No se admite la actualización de ADC de una versión superior a una versión inferior. Por ejemplo, si su instancia de Citrix ADC es 13.0 82.x, no puede cambiar la instancia de ADC a 13.0 79.x ni a ninguna otra versión anterior.

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar Citrix ADC (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.




3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar instancias ADC que quiera actualizar.
   - Para actualizar un par HA, especifique la dirección IP de un nodo principal o secundario.
   - Para actualizar un clúster, especifique la dirección IP del clúster.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Puede quitar las instancias fallidas y hacer clic en **Siguiente**.

   Si no tiene suficiente espacio en disco en una instancia, puede comprobar y limpiar el espacio en disco. Consulte Limpiar espacio en disco ADC.

   > **Importante**
   >
   > Si especifica la dirección IP del clúster, ADM realiza la validación previa de la actualización solo en la instancia especificada, no en los otros nodos del clúster.

6. Opcional, en **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia. Utilice una de las siguientes formas de ejecutar los comandos:

   Los scripts personalizados se utilizan para comprobar los cambios antes y después de una actualización de instancia de ADC. Por ejemplo:

   - La versión de la instancia antes y después de la actualización.
   - El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
   - Las estadísticas de los servicios y servidores virtuales.
   - Las rutas dinámicas.

   Una actualización de instancia tiene varias etapas. Ahora puede especificar estos scripts para ejecutarse en las siguientes etapas:

   - **Preactualización**: el script especificado se ejecuta antes de actualizar una instancia.
   - **Después de la actualización previa a la conmutación por error (aplicable para HA)**: esta etapa solo se aplica a la implementación de alta disponibilidad. El script especificado se ejecuta después de actualizar los nodos, pero antes de su conmutación por error.
   - **Post upgrade (aplicable para independiente)/Conmutación por error posterior a la actualización (aplicable para HA)**: el script especificado se ejecuta después de actualizar una instancia en la implementación independiente. En la implementación de alta disponibilidad, el script se ejecuta después de actualizar los nodos y su conmutación por error.

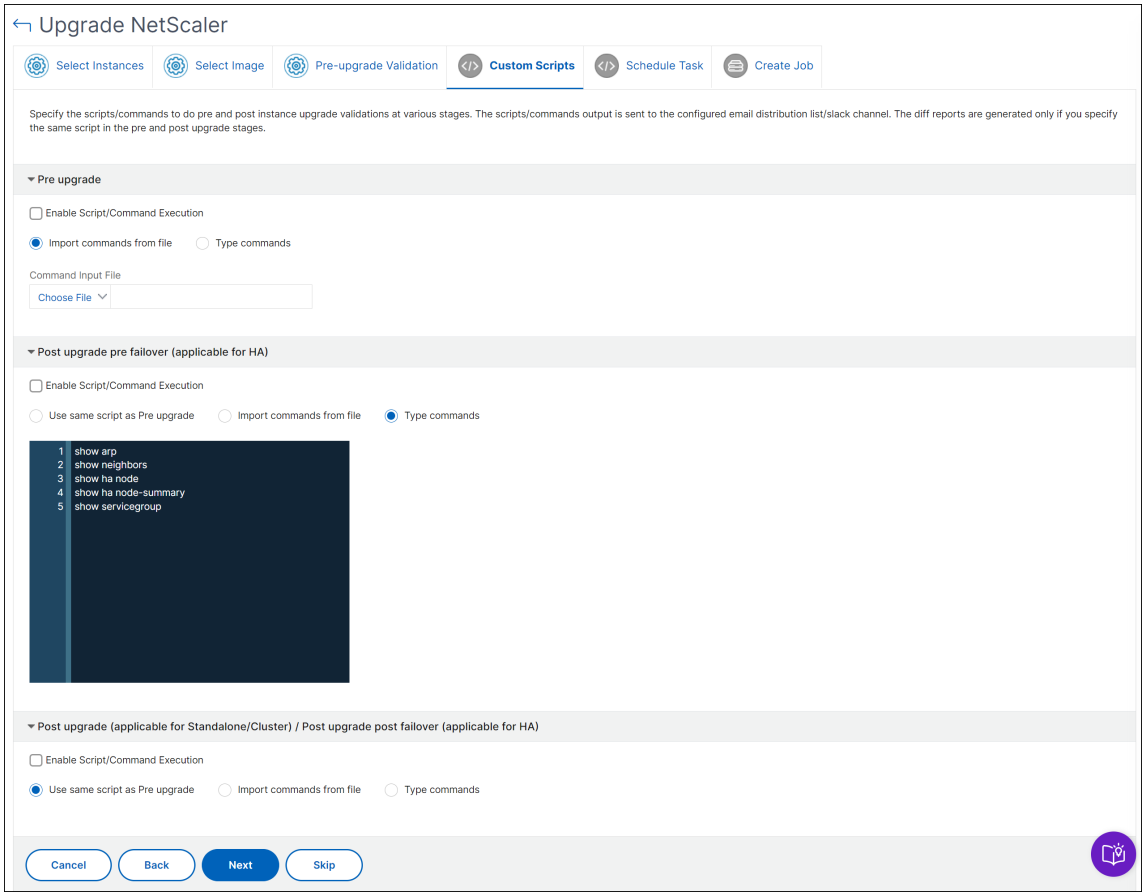
   > **Nota**
   >
   > Asegúrese de habilitar la ejecución del script en las etapas requeridas. De lo contrario, los scripts especificados no se ejecutan.

   Puede importar un archivo de script o escribir comandos directamente en la GUI de ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Importar comandos de archivo**: seleccione el archivo de entrada de comandos desde el equipo local.
- **Escriba comandos**: Introduzca los comandos directamente en la interfaz gráfica de usuario.

En las etapas posteriores a la actualización, puede utilizar el mismo script especificado en la etapa previa a la actualización.




7. En **Planificar tarea**, seleccione una de las siguientes opciones:

   - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.
   - **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

     Si quiere actualizar un par ADC HA en dos etapas, seleccione **Realizar actualización de dos etapas para nodos en HA**.

     Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.

8. En **Crear trabajo**, especifique los siguientes detalles:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a) Seleccione una de las siguientes opciones de la lista **Imagen de software**:

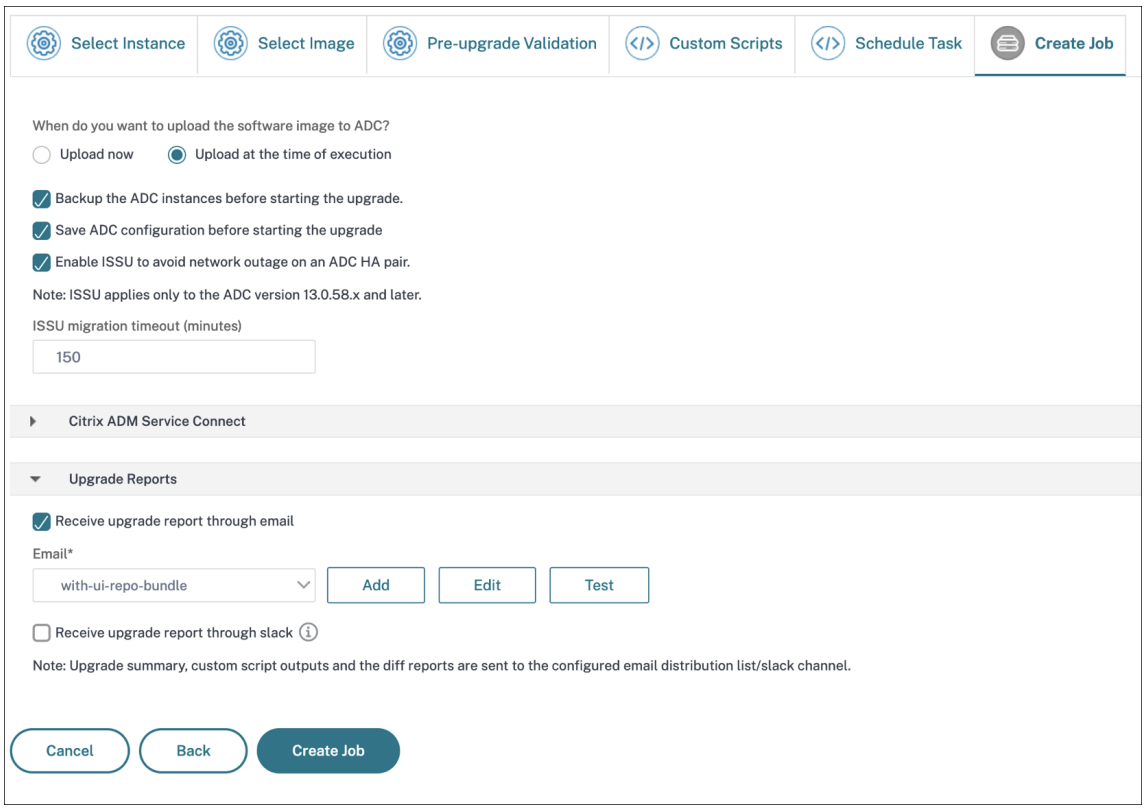
- **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
- **Dispositivo**: Seleccione el archivo de actualización de instancias en un explorador de archivos ADM. La GUI de ADM muestra los archivos de instancia que están presentes en `/var/mps/ns_images`.

b) Especifique cuándo quiere cargar la imagen en una instancia:

- **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
- **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.

- **Limpiar la imagen de software de Citrix ADC en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.
- **Realice una copia de seguridad de las instancias ADC antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias ADC seleccionadas.
- **Mantener el estado principal y secundario de los nodos HA después de la actualización**: seleccione esta opción si quiere que el trabajo de actualización inicie una conmutación por error después de la actualización de cada nodo. De esta manera, el trabajo de actualización mantiene el estado primario y secundario de los nodos.
- **Guardar configuración de ADC antes de iniciar la actualización**: guarda la configuración ADC en ejecución antes de actualizar las instancias de ADC.
- **Habilite ISSU para evitar cortes de red en el par ADC HA**: ISSU garantiza la actualización de tiempo de inactividad cero en un par de alta disponibilidad de ADC. Esta opción proporciona una funcionalidad de migración que respeta las conexiones existentes durante la actualización. Por lo tanto, puede actualizar un par ADC HA sin tiempo de inactividad. Especifique el tiempo de espera de migración ISSU en minutos.
- **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
- **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




9. Haga clic en **Crear trabajo**.

El trabajo de actualización aparece en **Redes > Trabajo de configuración > Trabajos de mantenimiento**. Cuando modifique un trabajo existente, puede cambiar a cualquier ficha si los campos obligatorios ya están rellenados. Por ejemplo, si se encuentra en la ficha **Seleccionar configuración**, puede cambiar a la ficha **Vista previa del trabajo**.

## Limpiar el espacio en disco ADC

Si se enfrenta a un problema de espacio en disco insuficiente al actualizar una instancia de ADC, limpie el espacio en disco de la propia GUI de ADM.

1. En la ficha **Validación previa a la actualización**, seleccione la instancia que tiene el problema de espacio en disco.
2. Seleccione **Comprobar espacio en disco**.

   Este panel muestra el disco de la instancia que tiene poco espacio. También muestra cuánta memoria se utiliza y está disponible en el disco.
3. En el panel **Comprobar espacio en disco**, seleccione la instancia que requiere limpieza.
4. Haga clic en **Liberar espacio en disco**.
5. Seleccione los archivos que quiere borrar.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Haga clic en **Eliminar**

### Descargar un informe diff consolidado de un trabajo de actualización de ADC

Puede descargar un informe diff de un trabajo de actualización de ADC si se especifican scripts personalizados. Un informe diff contiene las diferencias entre las salidas del script previo a la actualización y posterior a la actualización. Con este informe, puede determinar qué cambios se han producido en la instancia de ADC posterior a la actualización.

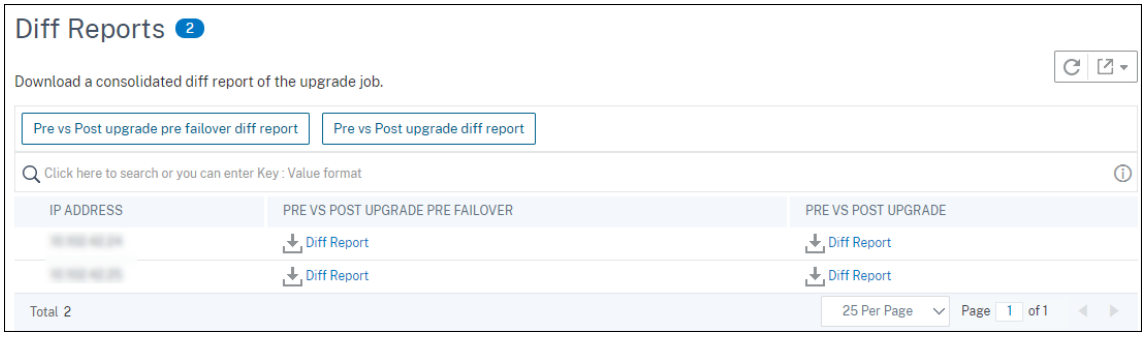
> **Nota**
>
> El informe diff solo se genera si especifica el mismo script en las etapas anterior a la actualización y posterior a la actualización.

Para descargar un informe diff de un trabajo de actualización, haga lo siguiente:

1. Vaya a **Redes > Trabajos de Configuración > Trabajos de Mantenimiento**.
2. Seleccione el trabajo de actualización para el que quiere descargar un informe de diferencias.
3. Haga clic en **Diff Reports**.
4. En **Informes de diferencias**, descargue un informe diff consolidado del trabajo de actualización seleccionado.

   En esta página, puede descargar cualquiera de los siguientes tipos de informes diff:

   - **Informe de diferencia de conmutación por error anterior a posterior a la actualización**
   - **Informe de diferencia anterior y posterior a la actualización**




## Usar plantillas de configuración para crear plantillas de auditoría

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Ahora puede utilizar comandos de configuración que se guardaron anteriormente como plantillas de configuración para crear plantillas de auditoría que se pueden aplicar a instancias específicas de Citrix ADC. Al crear una plantilla de auditoría, puede arrastrar las plantillas de configuración guardadas anteriormente al campo Comandos y modificar la plantilla para adaptarla a sus necesidades. A continuación, puede aplicar la plantilla de auditoría a instancias específicas de Citrix ADC. Citrix ADM compara estas instancias con la plantilla de auditoría e informa de cualquier discrepancia. Este proceso le ayuda a identificar errores y rectificarlos de manera oportuna.

Puede crear plantillas de configuración mientras crea un trabajo y guarda un conjunto de comandos de configuración como plantilla. Al guardar estas plantillas en la página **Crear trabajos** , se muestran automáticamente en la página **Crear plantilla** .

Por ejemplo, considere una configuración básica de equilibrio de carga para la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual.

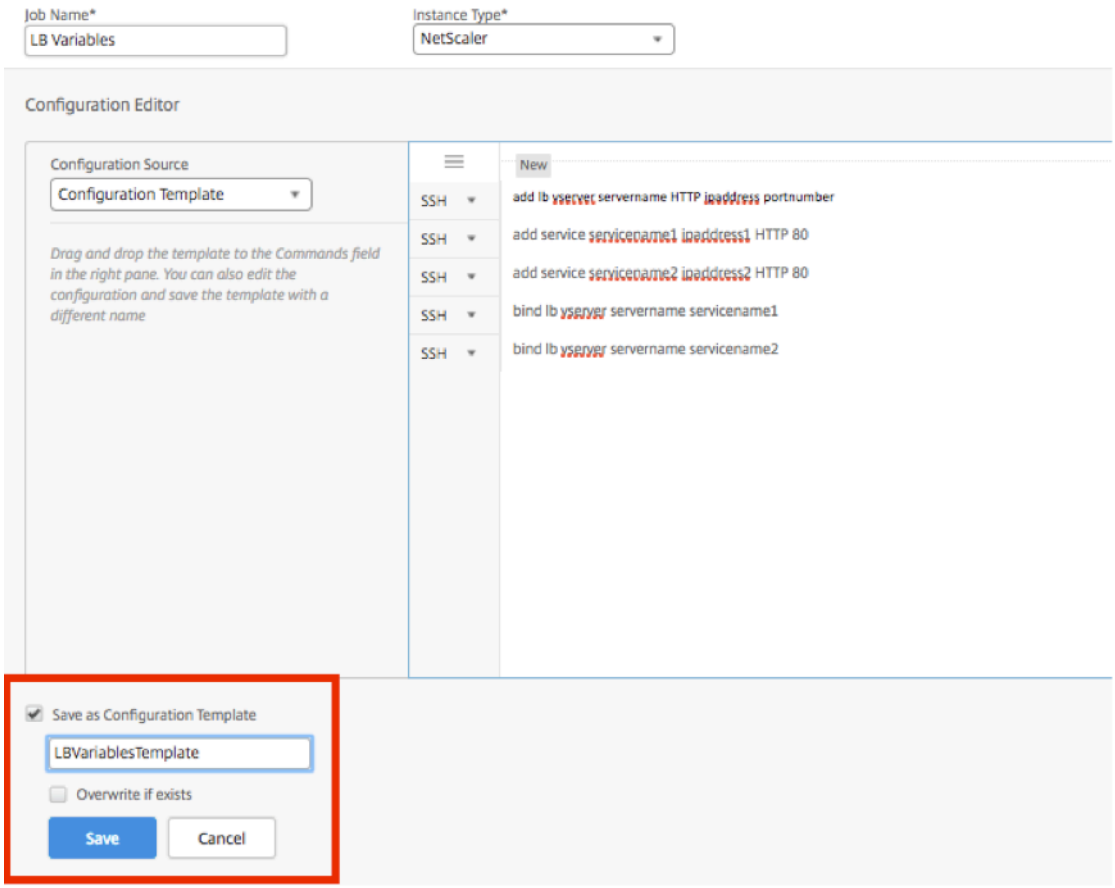
En este ejemplo se utilizan los siguientes comandos:

```
add lb vserver >servername> HTTP <ipaddress portnumber>
add service <servicename1 ipaddress1> HTTP 80
add service <servicename2 ipaddress2> HTTP 80
bind lb vserver <servername servicename1>
bind lb vserver <servername servicename2>
```

**Para guardar una plantilla de configuración en Citrix ADM:**

1. Vaya a **Redes** > **Trabajos de configuración**y haga clic en **Crear trabajo**.
2. En la página **Crear Trabajo**, especifique el nombre del trabajo y el tipo de instancia.
3. Elija la **plantilla de configuración** como fuente de configuración y, en el campo **Comandos**, introduzca comandos como los del ejemplo anterior.
4. Active la casilla **Guardar como plantilla de configuración** y especifique un nombre para la plantilla. Puede optar por sobrescribir otras plantillas que existen con el mismo nombre.
5. Haga clic en **Guardar**.

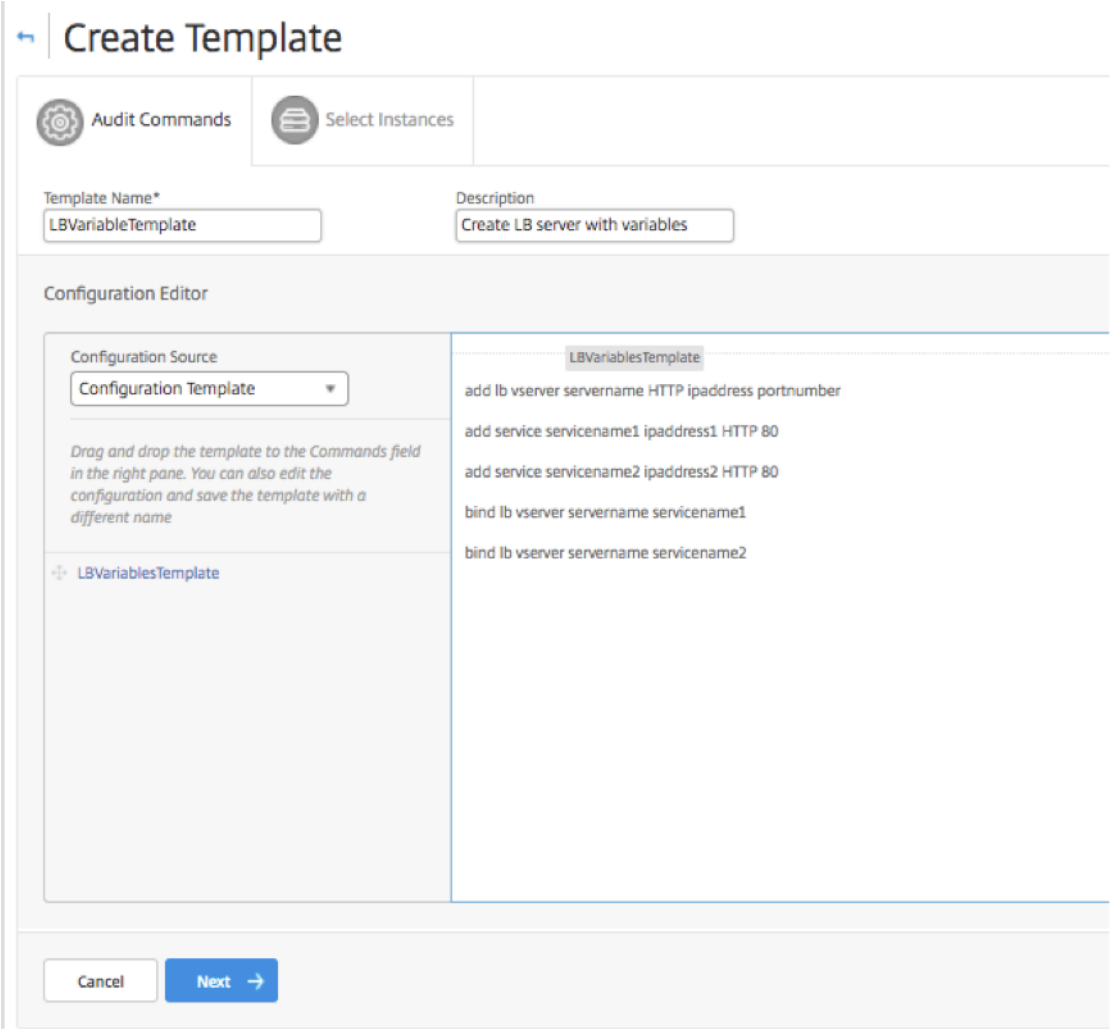
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Para utilizar una plantilla de configuración para crear una plantilla de auditoría en Citrix ADM:**

1. Vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría**y haga clic en **Agregar**.
2. En la página **Crear plantilla**, especifique un nombre para el nombre de plantilla e introduzca una descripción.
3. En la lista **Origen de configuración**, seleccione **Plantilla de configuración**y, a continuación, arrastre la plantilla al campo Comandos del panel derecho. También puede modificar la configuración y guardar la plantilla con un nombre diferente. Haga clic en **Siguiente**.
4. En la ficha **Seleccionar instancias**, haga clic en **Agregar instancias** y agregue las instancias en las que quiera ejecutar la configuración. Haga clic en **Aceptar**.
5. Haga clic en **Finalizar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta cada 12 horas en las configuraciones de las instancias especificadas.

## Usar el comando SCP (put) en trabajos de configuración

January 30, 2024

Puede utilizar la función Trabajos de configuración de Citrix ADM para crear trabajos de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados. Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una única instancia administrada o en varias instancias administradas. Por ejemplo, puede utilizar los trabajos de configuración para actualizar los dispositivos.

Los trabajos de configuración de Citrix ADM utilizan comandos Secure Shell (SSH) para configurar instancias, y puede configurar un trabajo de configuración para usar copia segura (SCP) para transferir

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

archivos de forma segura. SCP se basa en el protocolo SSH. Uno de los comandos **SCP** que puede incluir en un trabajo de configuración es el comando «put». Puede usar el comando «poner» en los trabajos de configuración para cargar o transferir uno o más archivos almacenados en un directorio local del sistema a Citrix ADM y, luego, a un directorio de la instancia o instancias de Citrix ADC.

> **Nota:** El archivo se carga en Citrix ADM y, posteriormente, se copia (coloca) en las instancias de Citrix ADC seleccionadas. El archivo cargado se almacena en Citrix ADM y solo se elimina cuando se elimina el trabajo. Esto es necesario para trabajos programados para ejecutarse más tarde.

El comando tiene la siguiente sintaxis:

```
put <local_filename> <remote_path/remote_filename>
```

Donde:

<local_filename> es el nombre del archivo local que se va a cargar.

<remote_path / remote_filename> es la ruta a un directorio remoto y el nombre que se asignará al archivo cuando se copie en ese directorio.

Al crear el trabajo de configuración, puede convertir los parámetros de nombre de archivo local y remoto en variables. Esto le permite asignar diferentes archivos a estos parámetros para el mismo conjunto de instancias de Citrix ADC cada vez que ejecute el trabajo. Además, cuando se utiliza un archivo en varios lugares de un trabajo y se quiere cambiar el nombre del archivo, se puede redefinir la variable en lugar de cambiar el nombre del archivo en todos los lugares.

**Para utilizar el comando put para cargar archivos en un trabajo de configuración:**

1. Vaya a **Redes** > **Trabajos de configuración**.
2. En la página **Trabajos**, haga clic en **Crear Trabajo**.
3. En la página **Crear trabajo**, escriba el nombre del trabajo en el campo Nombre del trabajo y, en el panel **Editor de configuración**, escriba el comando “poner”.

   Por ejemplo, si quiere crear un trabajo de configuración que copia un archivo de certificado SSL guardado en el sistema local en varias instancias de Citrix ADC, puede agregar un comando “put”que utilice una variable en lugar del nombre de un archivo determinado y definir el tipo de variable como “file”.

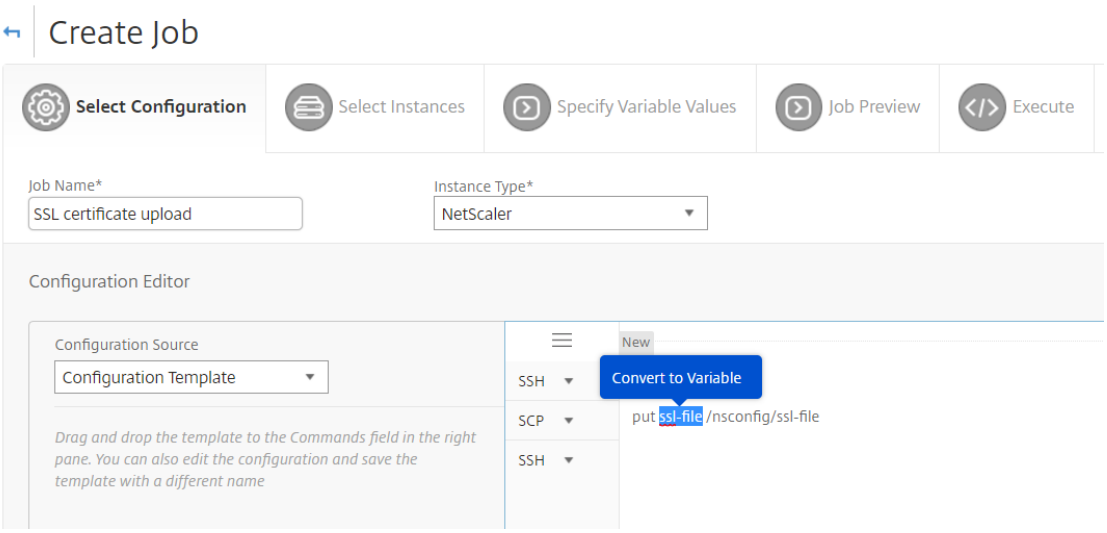
   ```
   put ssl-file /nsconfig/ssl-file
   ```

   En este ejemplo,

   - `ssl-file`: Es el nombre del archivo que debe cargarse en la instancia de Citrix ADC.
   - `/nsconfig/ssl-file` - Esta es la carpeta de destino en la instancia donde `ssl-file` se colocará el después de la ejecución de la tarea.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

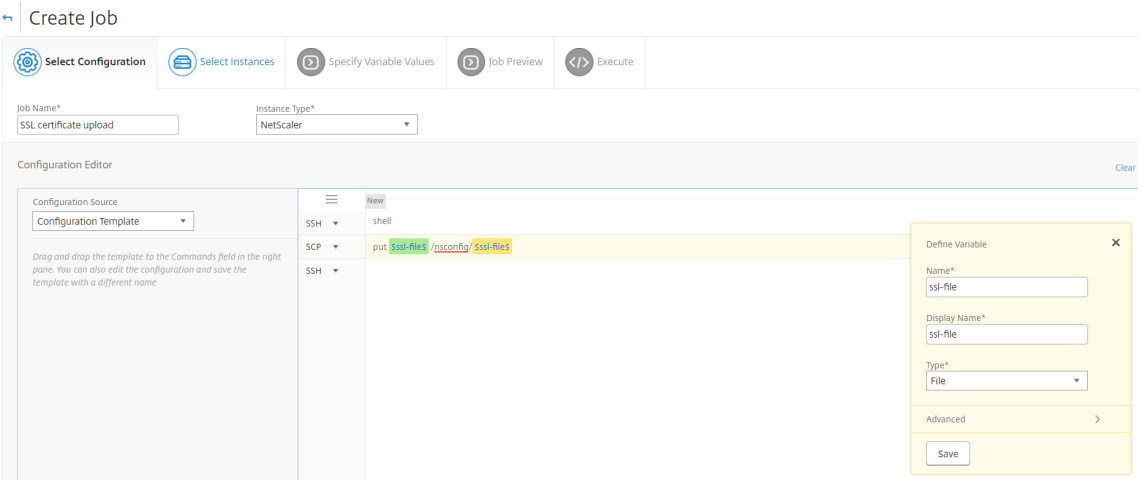
4. En el comando que escribió, seleccione el nombre de archivo que quiere convertir en una variable y, a continuación, haga clic en**Convertir en variable**, como se muestra en la ilustración siguiente.




5. Compruebe que el nombre de archivo está encerrado por signos de dólar (lo que indica que ahora es una variable) y, a continuación, haga clic en la variable.

6. Especifique los detalles de la variable, como nombre, nombre para mostrar y tipo.

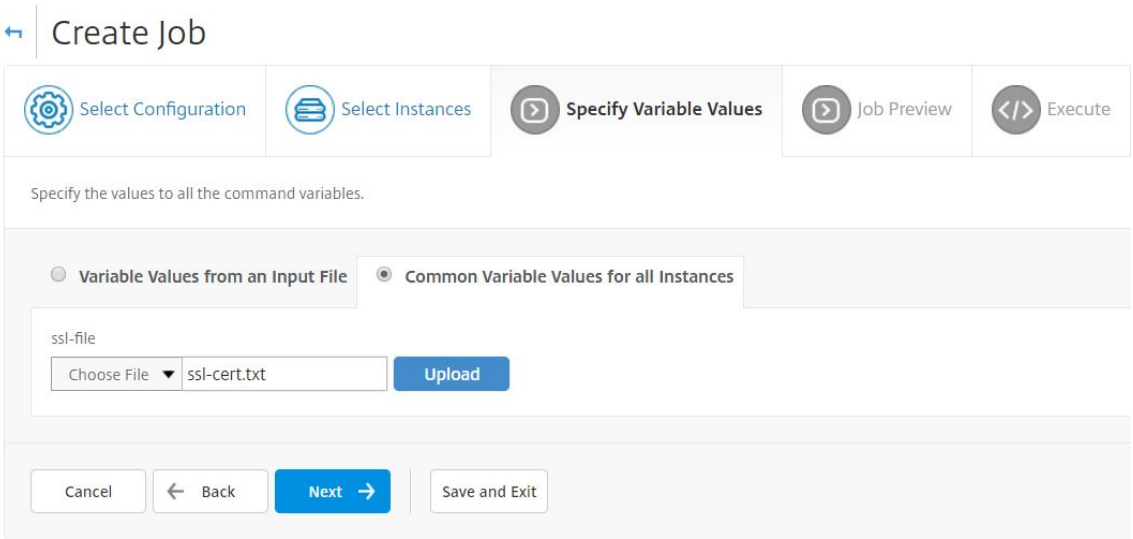
7. En la lista desplegable **Tipo**, seleccione **Archivo**. Haga clic en **Guardar**. Declarar la variable como un tipo de “Archivo”le permite cargar archivos en Citrix ADM.



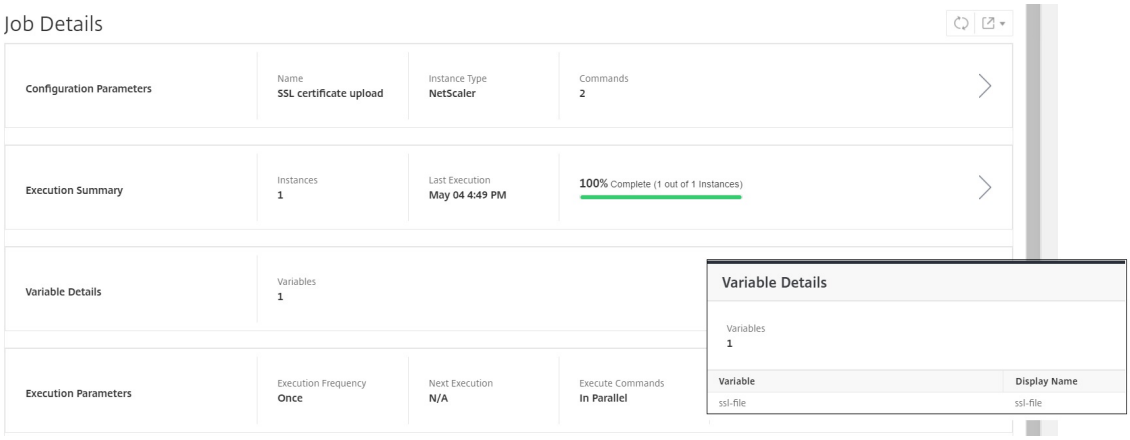

8. Haga clic en**Siguiente** y seleccione las instancias de Citrix ADC en las que quiere copiar los archivos.

9. En la ficha **Especificar valores de variables**, seleccione la sección **Valores de variables comunes para todas las instancias**, seleccione el archivo del almacenamiento local del sistema, haga clic en **Cargar** para cargar el archivo en Citrix ADM y haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




10. En la ficha**Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias.
11. En la ficha**Ejecutar**, puede ejecutar el trabajo ahora o programarlo para que se ejecute más tarde. También puede elegir qué acción debe realizar Citrix ADM si falla el comando. También puede crear una notificación por correo electrónico para recibir una notificación sobre el éxito o el fracaso del trabajo, y otros detalles. Haga clic en **Finalizar**.
12. Puede ver los detalles del trabajo navegando a**Redes** >**Trabajos de configuración**y seleccionando el trabajo configurado. Haga clic en **Detalles** y, a continuación, en **Detalles de variables** para mostrar las variables agregadas a su trabajo.




## Reprogramar trabajos configurados mediante plantillas integradas

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede reprogramar un trabajo que haya programado mediante plantillas integradas en Citrix Application Delivery Management (ADM). Por ejemplo, puede cambiar la acción que debe realizar NetScaler ADM si se produce un error en un comando. Si previamente optó por ignorar un error y continuar, puede cambiarlo para revertir todos los comandos correctos si falla un comando.

### Para reprogramar un trabajo configurado mediante plantillas integradas en NetScaler ADM

1. En Citrix ADM, vaya a **Redes** > **Trabajos de configuración** .
2. Seleccione el trabajo que quiere modificar, agregar o quitar instancias, especifique valores de variables y, a continuación, cambie las acciones de ejecución y la configuración.
3. Haga clic en **Finalizar** para reprogramar el trabajo.

> **Nota**
>
> También puede seleccionar el trabajo y hacer clic en **Ejecutar de nuevo** para ejecutar el trabajo sin modificar ningún origen, instancia ni comando. Esta función es útil cuando se tiene que ejecutar el mismo conjunto de comandos en las mismas instancias. A veces, el trabajo puede encontrar un error transitorio desde el lado del servidor y es posible que tenga que volver a ejecutar el trabajo.

## Reutilizar plantillas de auditoría de configuración en trabajos de configuración

January 30, 2024

Como administrador, ahora puede guardar los comandos de configuración como un conjunto de plantillas de configuración reutilizables al crear un trabajo y ejecutar una auditoría de configuración. La plantilla de configuración creada y guardada en Configuration Jobs está disponible en Configuration Audit para crear una plantilla de auditoría que se pueda aplicar a instancias específicas de Citrix ADC. Del mismo modo, la plantilla de auditoría creada en el módulo Auditoría de configuración está disponible en Configuration Jobs para que pueda ejecutar la plantilla como un trabajo de configuración. Cualquier cambio realizado en la plantilla es ahora visible tanto en los módulos Configuration Jobs como en Configuration Audit.

Anteriormente, el trabajo de configuración y las plantillas de auditoría de configuración tenían que crearse por separado para la misma configuración y guardarse como archivos diferentes. Esto provocó una duplicación de esfuerzos en la creación y el mantenimiento de las plantillas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Citrix Application Delivery Management (ADM) le permite guardar esta plantilla en el sistema para que la plantilla de auditoría también esté disponible en los trabajos de configuración. Ahora las plantillas de auditoría se pueden utilizar para crear trabajos de configuración. De esta forma, las plantillas se pueden usar indistintamente entre los trabajos de configuración y las auditorías de configuración.

Por ejemplo, considere una configuración básica de equilibrio de carga para la que agregue un servidor virtual de equilibrio de carga, agregue dos servicios y vincule los servicios al servidor virtual.

En este ejemplo se utilizan los siguientes comandos:

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
```

## Creación de una plantilla en auditorías de configuración y reutilización en trabajos de configuración

Realice la siguiente tarea para crear una plantilla en el módulo de auditoría de configuración y reutilizarla en el módulo de trabajos de configuración.

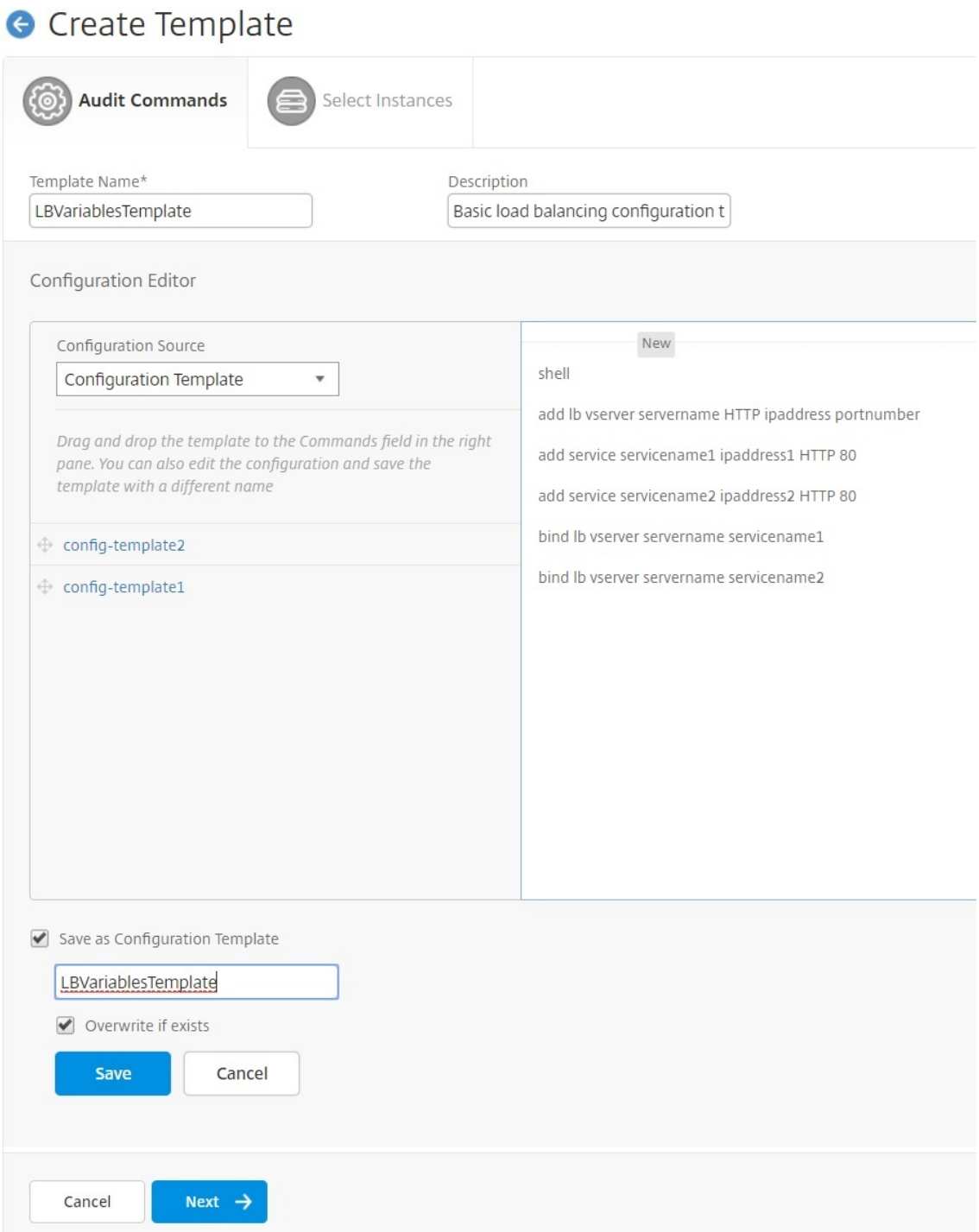
**Para crear una plantilla de auditoría:**

1. En Citrix ADM, vaya a**Redes > Auditoría de configuración > Plantilla de auditoría**y haga clic en**Agregar**.
2. En la página**Crear plantilla**, especifique el nombre de la plantilla. También puede agregar más información sobre la plantilla en el campo **Descripción**.
3. En el panel **Comandos**, escriba comandos en el ejemplo.
4. Active la casilla**Guardar como plantilla de configuración**y especifique un nombre para la plantilla; por ejemplo, puede nombrar esta plantilla como “LBVariablesTemplate. “Puede optar por sobrescribir otras plantillas que existen con el mismo nombre.

   > **Nota:** El nombre de la plantilla de auditoría puede ser el mismo que el nombre de la plantilla de configuración.

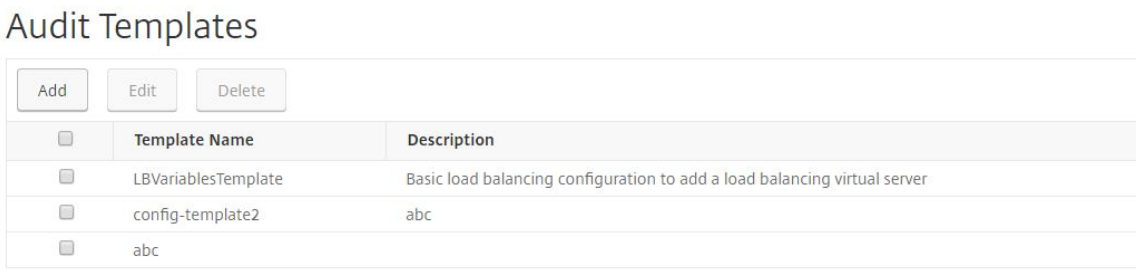
5. Haga clic en**Guardar** y haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Haga clic en **Siguiente**.
7. En la ficha **Seleccionar instancias**, seleccione las **instancias de Citrix ADC en las** que quiere ejecutar estos comandos de configuración y haga clic en **Finalizar.** La nueva plantilla está ahora visible en la lista de plantillas de auditoría.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




8. Si quiere ejecutar estos comandos de configuración, vaya a **Redes > Trabajos de configuración**y haga clic en **Crear trabajo**. La plantilla de auditoría que creó anteriormente aparece como plantilla de configuración.

**Para reutilizar la plantilla de auditoría en trabajos de configuración:**

1. Introduzca un nombre para el trabajo, seleccione el tipo de instancia y arrastre la plantilla al panel de comandos.

   Al crear el trabajo de configuración, puede convertir los parámetros de nombre de archivo local y remoto en variables. Esto le permite asignar diferentes archivos a estos parámetros para el mismo conjunto de instancias de Citrix ADC cada vez que ejecute el trabajo.

2. En el comando que ha introducido, seleccione el nombre del archivo que desee convertir en variable y, a continuación, haga clic en**Convertir en variable.**

3. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar estos comandos.

4. Si ha especificado alguna variable en los comandos, en la ficha **Especificar valores variables**, seleccione una de las siguientes opciones para especificar las variables de sus instancias:

   - Valores de variables de un archivo de entrada: descargue un archivo de entrada para introducir valores para las variables que ha definido en los comandos y, a continuación, cargue el archivo en el servidor Citrix ADM.
   - Valores de variables comunes para todas las instancias: especifique la dirección IP y el puerto del servidor syslog.

5. En la ficha**Vista previa del trabajo**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias y hacer clic en**Siguiente**.

6. En la ficha**Ejecutar**, haga clic en**Finalizar** para ejecutar el trabajo de configuración. Ahora, si quiere agregar otro servicio a este servidor de equilibrio de carga y enlazar el servicio con el servidor, puede modificar los comandos en la página de comandos y guardarlos.

7. Desplácese hasta **Plantillas de auditoría** y haga clic en **Agregar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. Arrastre la plantilla “LBVariablesTemplate”al panel de comandos. Puede ver que la plantilla se ha actualizado con los nuevos comandos.

La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta cada 12 horas en las configuraciones de las instancias especificadas. Ahora puede crear plantillas y reutilizarlas entre trabajos de configuración y módulos de auditoría de configuración.

## Importar y exportar plantillas de configuración

January 30, 2024

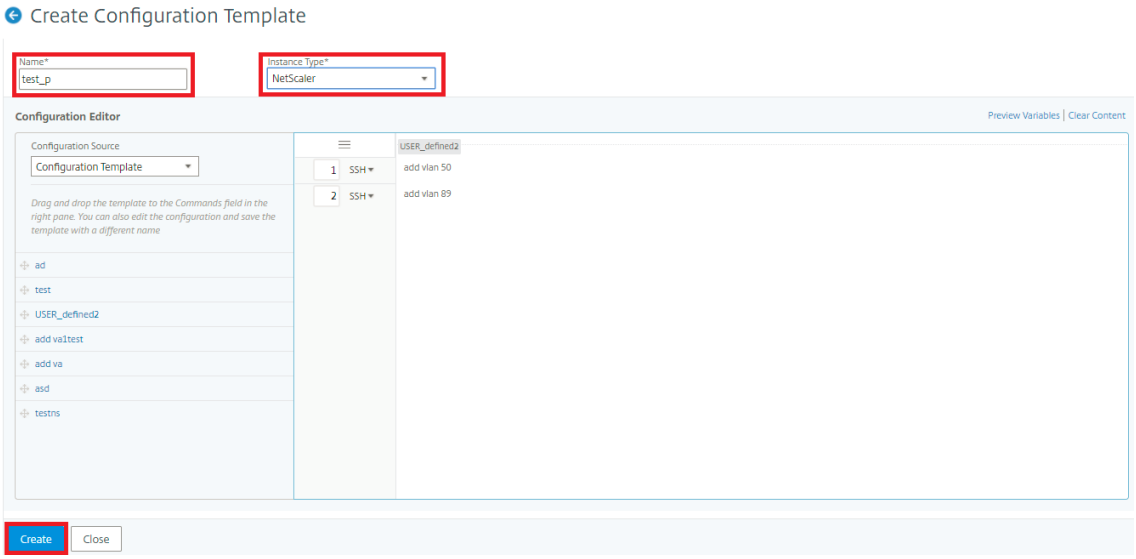
Puede exportar las plantillas de configuración desde cualquier Citrix Application Delivery Management (ADM). También puede importar el archivo al mismo Citrix ADM o a otro en cualquier momento en el futuro. Los datos de las plantillas de configuración (como los comandos de configuración, las definiciones de variables y los parámetros) no se pierden.

Puede exportar las plantillas de configuración a un formato de **archivo JSON** y guardarlas en la carpeta local. Puede importar la plantilla de configuración. archivos**json** en Citrix ADM. Este archivo puede ser nuevo o el que haya exportado desde el mismo Citrix ADM u otro.

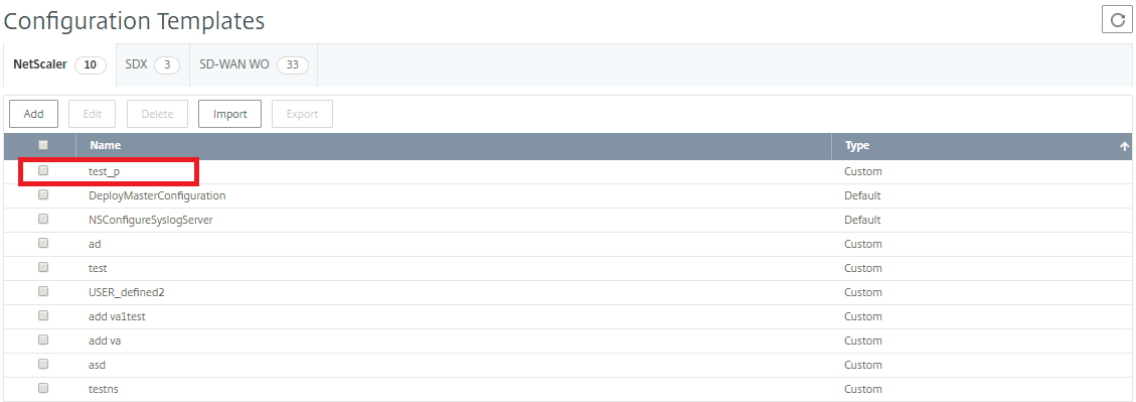
**Para exportar las plantillas de configuración:**

1. Vaya a **Redes > Trabajos de Configuración > Plantillas de Configuración**.
2. Haga clic en el botón **Agregar** para crear la plantilla de configuración.
3. En la página **Crear Plantilla de Configuración**, especifique el nombre de la plantilla de configuración y elija el tipo de instancia. En el **Editor de configuración**, seleccione el origen de configuración como Plantilla de configuración en el menú desplegable. Puede arrastrar las plantillas de configuración existentes al editor de configuración. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. Vaya a **Redes > Trabajos de configuración > Plantillas de configuración** para ver las plantillas creadas en la lista de plantillas de configuración.



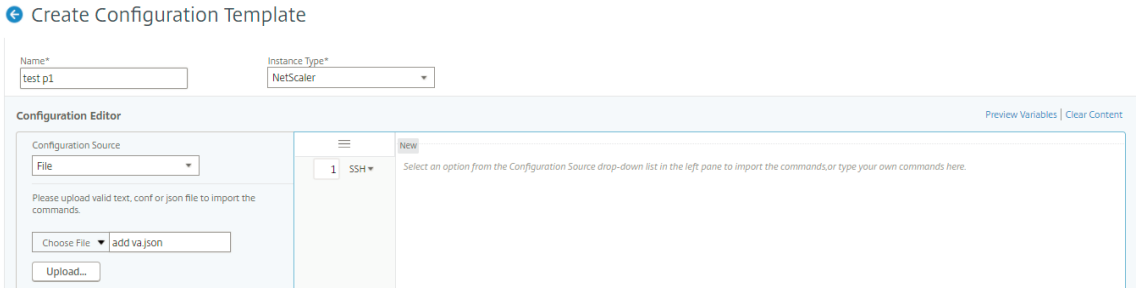

5. Seleccione la plantilla de configuración recién creada y haga clic en el botón **Exportar**.

La plantilla de configuración correspondiente se descarga en su sistema local en **formato.json**.

**Para importar las plantillas de configuración:**

1. Vaya a **Redes > Trabajos de configuración > Plantillas de configuración** y haga clic en el botón **Importar**. Seleccione la ruta en la que tiene. **json** de la plantilla de configuración y cargar los archivos **JSON**. Se recomienda encarecidamente cargar los archivos **JSON** que ya ha exportado.
2. También puede importar la plantilla de configuración mediante la opción **Archivo** del Editor de configuración.
3. Seleccione **Archivo** en el menú desplegable del **Editor de configuración**.
4. Selecciona **Elegir archivo** (. archivos **json** ) desde su sistema local y cargue la plantilla de configuración. archivos **json** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> - Cada nueva plantilla importada se almacena con una nueva cadena de identificación.
> - Puede importar las plantillas de configuración solo si el archivo está guardado en. formato **json** . Si importa las plantillas de configuración que no sean archivos **.json**, desde su sistema local, se mostrará un error y no se importarán los archivos.

## Trabajos de mantenimiento

January 30, 2024

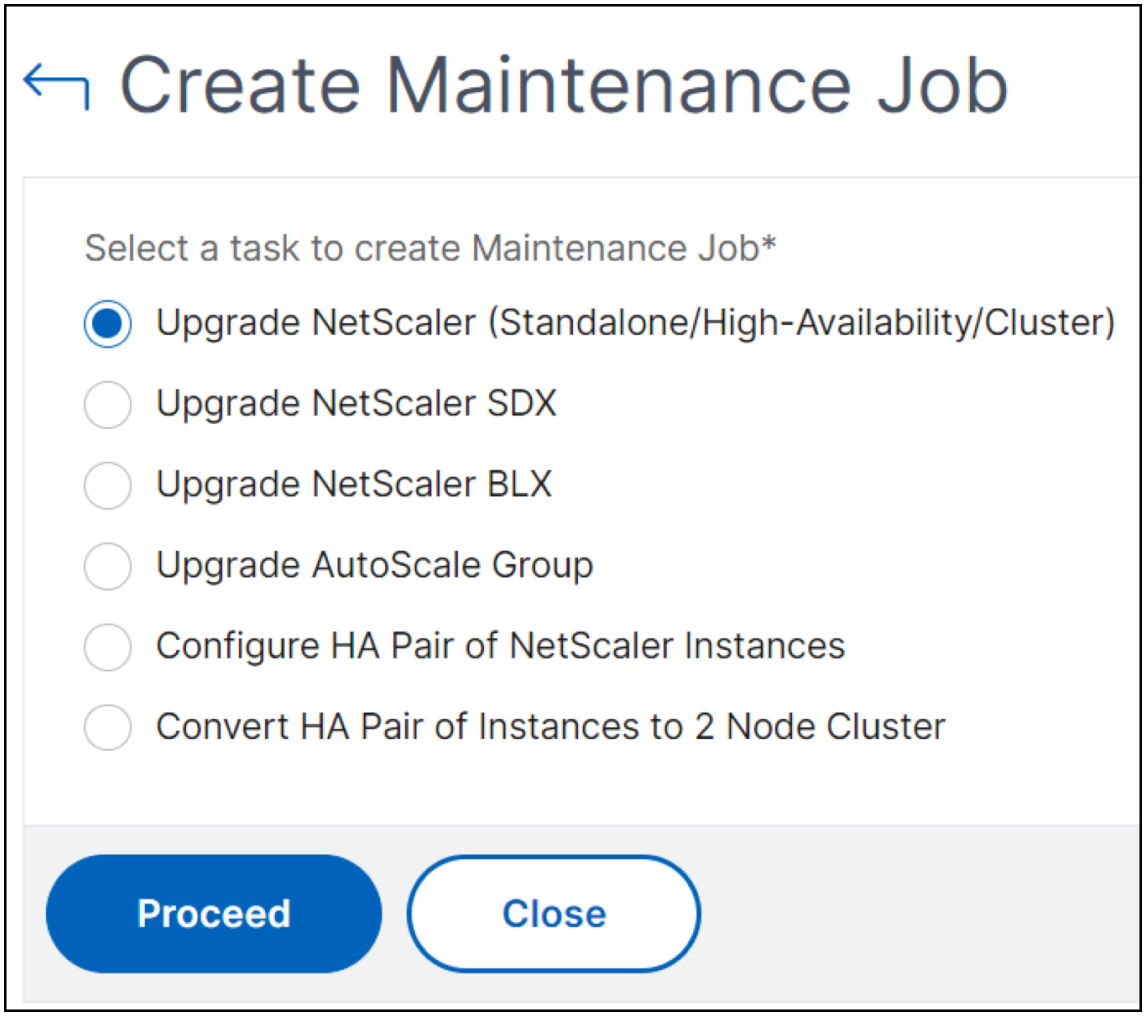
Puede crear los siguientes trabajos de mantenimiento mediante Citrix ADM. A continuación, puede programar los trabajos de mantenimiento en una fecha y hora específicas.

- Actualizar instancias de NetScaler ADC
- Actualice las instancias WAN-WO de Citrix ADC SD
- Actualizar instancias SDX de NetScaler ADC
- Actualización de instancias de NetScaler ADC en el grupo de Autoscale
- Configurar el par HA de instancias NetScaler ADC
- Convierta un par de instancias de alta disponibilidad en un clúster de 2 nodos

### Programar la actualización de instancias NetScaler ADC

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En **Crear trabajos de mantenimiento**, seleccione **Actualizar Citrix ADC (Standalone/High-Availability/Cluster)** y haga clic en **Continuar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. En **Seleccionar instancia**, escriba el nombre de su elección para **Nombre del trabajo**.
4. Haga clic en **Agregar instancias** para agregar instancias ADC que quiera actualizar.
   - Para actualizar un par HA, especifique la dirección IP del nodo principal o secundario. Sin embargo, se recomienda usar la instancia principal para actualizar el par HA.
   - Para actualizar un clúster, especifique la dirección IP del clúster.
5. Haga clic en **Siguiente** para iniciar la validación previa a la actualización en las instancias seleccionadas.

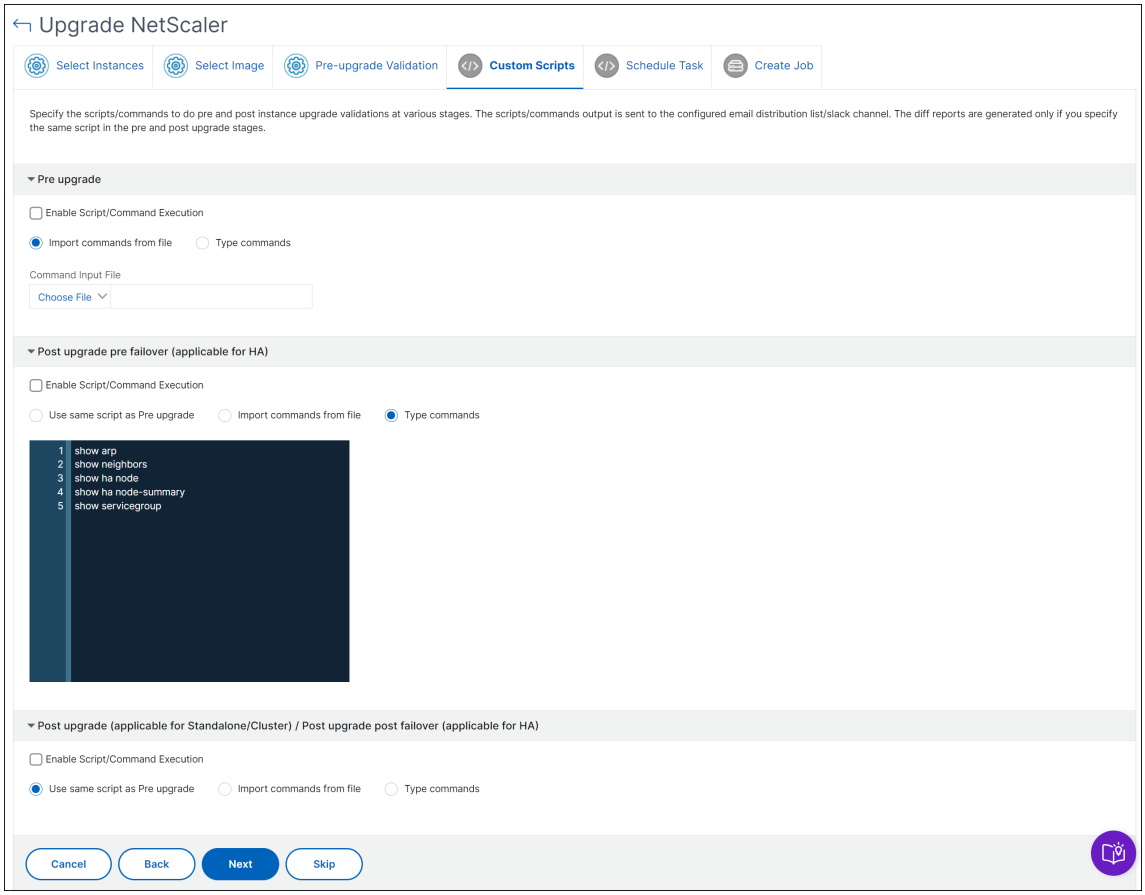
   La ficha **Validación previa a la actualización** muestra las instancias fallidas. Quite las instancias con errores y haga clic en **Siguiente**.

   > **Importante**
   >
   > Si especifica la dirección IP del clúster, ADM realiza la validación previa de la actualización solo en la instancia especificada, no en los otros nodos del clúster.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Opcional, en **Scripts personalizados**, especifique los scripts que se ejecutarán antes y después de una actualización de instancia. Utilice una de las siguientes formas de ejecutar los comandos:

   - **Importar comandos del archivo**: Seleccione el archivo de entrada de comandos del equipo local.
   - **Escribir comandos**: Introduzca comandos directamente en la GUI.




   Puede usar scripts personalizados para comprobar los cambios antes y después de una actualización de la instancia. Por ejemplo:

   - La versión de la instancia antes y después de la actualización.
   - El estado de las interfaces, los nodos de alta disponibilidad, los servidores virtuales y los servicios antes y después de la actualización.
   - Las estadísticas de los servicios y servidores virtuales.
   - Las rutas dinámicas.

7. En **Planificar tarea**, seleccione una de las siguientes opciones:

   - **Actualizar ahora**: El trabajo de actualización se ejecuta inmediatamente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Programar más tarde**: Seleccione esta opción para ejecutar este trabajo de actualización más tarde. Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar las instancias.

  Si quiere actualizar un par ADC HA en dos etapas, seleccione **Realizar actualización de dos etapas para nodos en HA**.

  Especifique la **fecha de ejecución** y la **hora de inicio** cuando quiera actualizar otra instancia en el par HA.

8. En **Crear trabajo**, especifique los siguientes detalles:

   a) Seleccione una de las siguientes opciones de la lista **Imagen de software**:

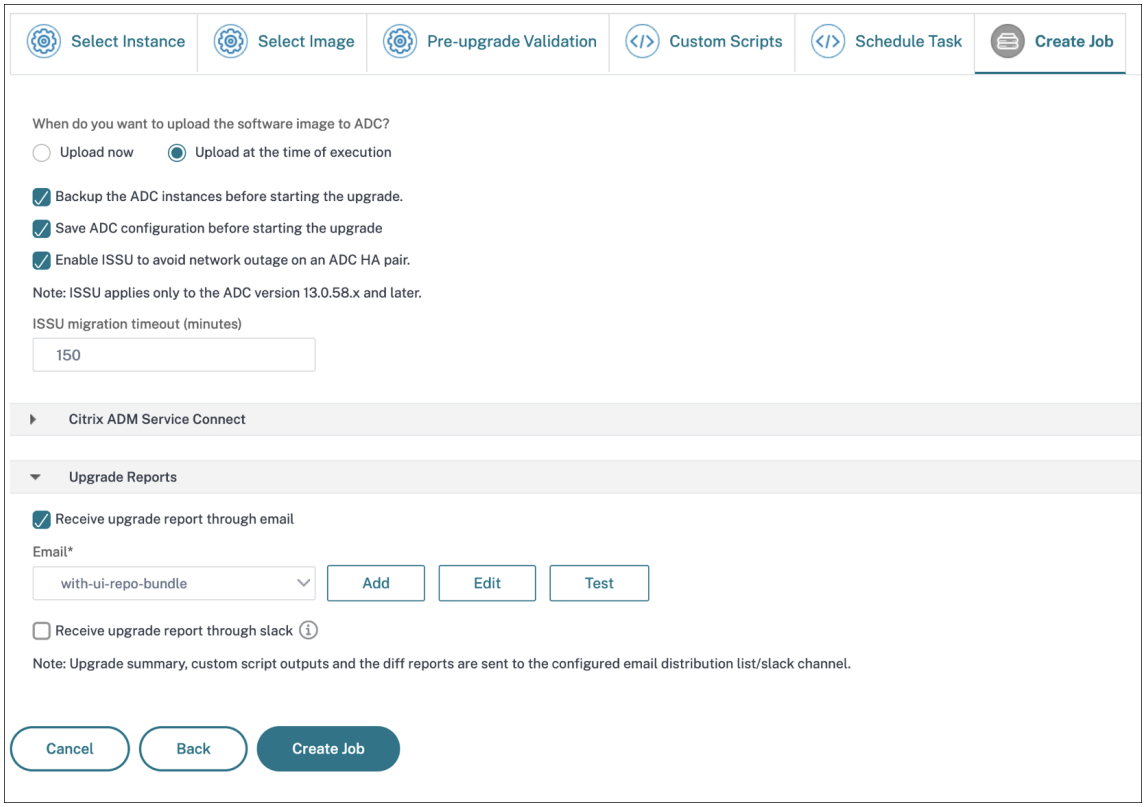
      - **Local**: Seleccione el archivo de actualización de instancias de su máquina local.
      - **Dispositivo**: Seleccione el archivo de actualización de instancias en un explorador de archivos ADM. La GUI de ADM muestra los archivos de instancia que están presentes en `/var/mps/mps_images`.

   b) Especifique cuándo quiere cargar la imagen en una instancia:

      - **Cargar ahora**: Seleccione esta opción para cargar la imagen inmediatamente. Sin embargo, el trabajo de actualización se ejecuta a la hora programada.
      - **Cargar en el momento de la ejecución**: Seleccione esta opción para cargar la imagen en el momento de la ejecución del trabajo de actualización.

   - **Limpiar la imagen de software de Citrix ADC en una actualización correcta**: Seleccione esta opción para borrar la imagen cargada en la instancia de ADC después de la actualización de la instancia.
   - **Realice una copia de seguridad de las instancias ADC antes de iniciar la actualización.** - Crea una copia de seguridad de las instancias ADC seleccionadas.
   - **Recibir informe de ejecución a través de correo electrónico**: Envía el informe de ejecución por correo electrónico. Para agregar una lista de distribución de correo electrónico, consulte Crear una lista de distribución de correo electrónico.
   - **Recibir informe de ejecución a través de Slack**: Envía el informe de ejecución en Slack. Para agregar un perfil de Slack, consulta Crear un perfil de Slack.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




9. Haga clic en **Crear trabajo**.

## Programar la actualización de instancias WO SD-WAN de NetScaler ADC

1. Vaya a **Redes** > Trabajos de **configuración > Trabajos** de **mantenimiento** . Haga clic en el botón **Crear trabajo**.
2. En la página **Crear trabajo de mantenimiento**, seleccione **Actualizar NetScaler ADC SD-WAN WO** y haga clic en **Continuar**.
3. En la página **Actualizar NetScaler ADC SD-WAN WO**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. En la lista de imágenes de software, seleccione Local (su máquina local) o Dispositivo (el archivo de compilación debe estar presente en el dispositivo virtual NetScaler ADM). Agregue las instancias WO de Citrix ADC SD-WAN en las que desea ejecutar el proceso de actualización. Haga clic en **Siguiente**.
4. Para actualizar ahora la instancia WO de NetScaler ADC SD-WAN, seleccione **Ahora** en la lista **Modo de ejecución**. Haga clic en **Finalizar**.
5. Para actualizar la instancia WO de Citrix ADC SD-WAN más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar la instancia WO de Citrix ADC SD-WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de la instancia WO de Citrix ADC SD-WAN. Haga clic en la casilla de verificación **Recibir informe de ejecución por correo** electrónico para habilitar la notificación por correo electrónico.
7. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
8. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

## Programar la actualización de instancias de NetScaler ADC SDX

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En la página **Crear trabajo de mantenimiento** , seleccione **Actualizar Citrix ADC SDX** y haga clic en **Continuar**.
3. En la página **Actualizar dispositivos NetScaler ADC SDX**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. En la lista de imágenes de software, seleccione Local (su máquina local) o Dispositivo (el archivo de compilación debe estar presente en el dispositivo virtual NetScaler ADM). Agregue las instancias de NetScaler ADC SDX en las que quiere ejecutar el proceso de actualización. Haga clic en **Siguiente**.
4. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución de la actualización de la instancia SDX de NetScaler ADC. Haga clic en la casilla de verificación **Recibir informe de ejecución por correo** electrónico para habilitar la notificación por correo electrónico.
5. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
6. Para actualizar la instancia Citrix ADC SDX ahora, seleccione **Ahora** en la lista **Modo de ejecución**. Haga clic en **Finalizar**.
7. Para actualizar la instancia de Citrix ADC SDX más adelante, seleccione Más **tarde** en la lista **Modo de ejecución**. A continuación, puede elegir la fecha de ejecución y la hora de inicio para actualizar la instancia de NetScaler ADC SDX.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el cuadro **De**, agregue la dirección de correo electrónico desde la que quiere enviar mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

## Programar la actualización del grupo de Autoscale

Realice los siguientes pasos para actualizar todas las instancias de los servicios en la nube que forman parte del grupo de Autoscale:

1. En Citrix ADM, vaya a **Redes > Trabajos de configuración > Trabajos de mantenimiento** . Haga clic en el botón **Crear trabajo**.
2. En la página **Crear trabajos de mantenimiento** , seleccione **Actualizar grupo de Autoscale** y haga clic en **Continuar** .
3. En la ficha **Configuración de actualización** :
   a) Seleccione el **grupo de escalabilidad automática** que quiere actualizar.
   b) En **Imagen**, seleccione la versión de NetScaler ADC. Esta imagen es la versión existente de las instancias de NetScaler ADC en el grupo de Autoscale.
   c) En **NetScaler ADC Image**, examine el archivo de versión de NetScaler ADC al que quiere actualizar.

      Si marca **Actualización de gracia**, la tarea de actualización espera hasta que caduque el período de conexión de drenaje especificado.
   d) Haga clic en **Siguiente**.
4. En la ficha **Programar tarea**:
   a) Seleccione una de las siguientes opciones de la lista Modo de ejecución:
      - **Ahora:**Para iniciar las instancias de NetScaler ADC, actualice inmediatamente.
      - **Más tarde:** Para iniciar la actualización de las instancias de NetScaler ADC más adelante.
   b) Si selecciona la opción **Más tarde**, seleccione Fecha de ejecución y Hora de inicio cuando quiera iniciar la tarea de actualización.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

También puedes habilitar las notificaciones por correo electrónico y Slack para recibir el informe de ejecución de la actualización del grupo Autoscale. Haga clic en la casilla de verificación **Recibir informe de ejecución a través de correo electrónico** y **Recibir informe de ejecución a través de Slack** para habilitar las notificaciones.

5. Haga clic en **Finalizar**.

## Programar la configuración del par HA de instancias NetScaler ADC

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En la página **Crear trabajo de mantenimiento**, seleccione **Configurar par de instancias de NetScaler ADC** y haga clic en **Continuar**.
3. En la página **NetScaler ADC HA Pair**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. Introduzca la dirección IP principal y la dirección secundaria y haga clic en **Siguiente**.
4. En la ficha **Programar tarea**, puede elegir configurar el par NetScaler ADC HA ahora o posterior.
5. Para configurar ahora el par Citrix ADC HA, seleccione **Ahora** en la lista **Modo de ejecución** . Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla de verificación **Recibir informe de ejecución por correo** electrónico para habilitar la notificación por correo electrónico.
6. Para configurar el par Citrix ADC HA más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de eExecution y la hora de inicio. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla de verificación **Recibir informe de ejecución por correo** electrónico para habilitar la notificación por correo electrónico.
7. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
8. En la página **Crear lista de distribución de correo** electrónico , especifique un **nombre** para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el **cuadro**De , agrega la dirección de correo electrónico desde la que deseas enviar los mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Programar la conversión de par de instancias de alta disponibilidad en clúster

1. En Citrix ADM, vaya a **Redes** > Trabajos de **configuración > Trabajos demantenimiento**. Haga clic en el botón**Crear trabajo**.
2. En la página **Crear Trabajo de Mantenimiento**, seleccione **Convertir par de instancias de HA a clúster de 2 nodos** y haga clic en **Continuar**.
3. En la página **Migrar NetScaler ADC HA al clúster**, en la ficha **Selección de instancias**, agregue un **nombre de tarea**. Especifique la dirección IP principal, la dirección secundaria, el ID del nodo principal, el ID del nodo secundario, la dirección IP del clúster, el ID del clúster y el plano posterior. Haga clic en **Siguiente**.
4. En la ficha **Programar tarea**, puede optar por migrar NetScaler ADC HA al clúster ahora o posterior.
5. Para configurar el par Citrix ADC HA más adelante, seleccione Más **tarde** en la lista **Modo de ejecución** . A continuación, puede elegir la fecha de ejecución y la hora de inicio. Puede habilitar la notificación por correo electrónico para recibir el informe de ejecución del par de NetScaler ADC HA. Haga clic en la casilla de verificación **Recibir informe de ejecución por correo** electrónico para habilitar la notificación por correo electrónico.
6. Seleccione el icono **+** para crear la lista de distribución de correo electrónico.
7. En la página **Crear lista de distribución de correo electrónico**, especifique un nombre para la lista de distribución de correo electrónico. Agregue el servidor de correo SMTP que se utilizará para enviar notificaciones por correo electrónico al servidor de correo electrónico. En el **cuadro**De , agrega la dirección de correo electrónico desde la que deseas enviar los mensajes. En el cuadro **Para** , agrega la dirección o direcciones de correo electrónico a las que enviar mensajes. También puede agregar una dirección o direcciones de correo electrónico a las que enviar copias y copias de los mensajes sin mostrar estas direcciones en los mensajes o las copias. Haga clic en **Crear**. Después de crear la lista de distribución de correo electrónico, haga clic en **Finalizar** para completar el proceso de configuración.

## Auditoría de configuración

January 30, 2024

Este documento incluye:

- Creación de plantillas de auditoría
- Visualización de Informes de Auditoría

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Modificaciones de configuración de auditoría en todas las instancias
- Obtener consejos de configuración sobre la configuración de red
- Cómo sondear la auditoría de configuración de instancias de NetScaler ADC

## Crear plantillas de auditoría

January 30, 2024

Debe asegurarse de que ciertas configuraciones se ejecuten en instancias específicas para lograr un rendimiento óptimo de la red. También querrá supervisar los cambios de configuración en las instancias administradas de Citrix Application Delivery Controller (ADC), solucionar errores de configuración y recuperar las configuraciones no guardadas tras un cierre repentino del sistema. Puede crear plantillas de auditoría con configuraciones específicas que quiera auditar en determinadas instancias. Citrix Application Delivery Management (Citrix ADM) compara estas instancias con la plantilla de auditoría e informa si hay alguna discrepancia en la configuración. Cuando hay una discrepancia en la configuración, Citrix ADM genera un informe de diferencias de configuración que permite solucionar problemas y rectificar los cambios de configuración no deseados.

Puede automatizar la ejecución de la plantilla de auditoría mediante

- Programación de la hora a la que se debe ejecutar la plantilla
- Establecer la frecuencia con la que NetScaler ADM debe ejecutar la plantilla. Puede ejecutar la plantilla diariamente, en un día específico de una semana o en una fecha específica de un mes.

Además, tiene la opción de enviar el informe de diferencias generado por NetScaler ADM a las direcciones de correo electrónico especificadas que puede configurar. Con esta opción, el usuario puede recibir el informe como datos adjuntos de correo y no es necesario que el usuario inicie sesión en NetScaler ADM para exportar los informes manualmente.

> **Nota**
> La opción **Cambiar nombre** está inhabilitada para las plantillas de configuración predeterminadas. Sin embargo, puede cambiar el nombre de las plantillas de configuración personalizadas.

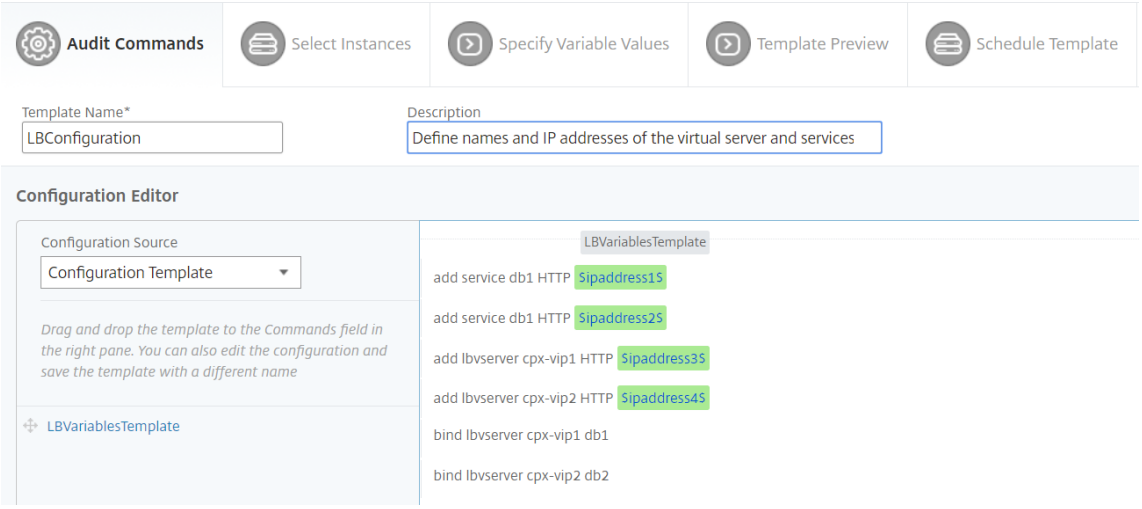
**Para crear plantillas de auditoría:**

1. Vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría** y haga clic en **Agregar** .
2. En la página**Crear plantilla** y en la ficha**Comandos de auditoría**, especifique el nombre de la plantilla y su descripción.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

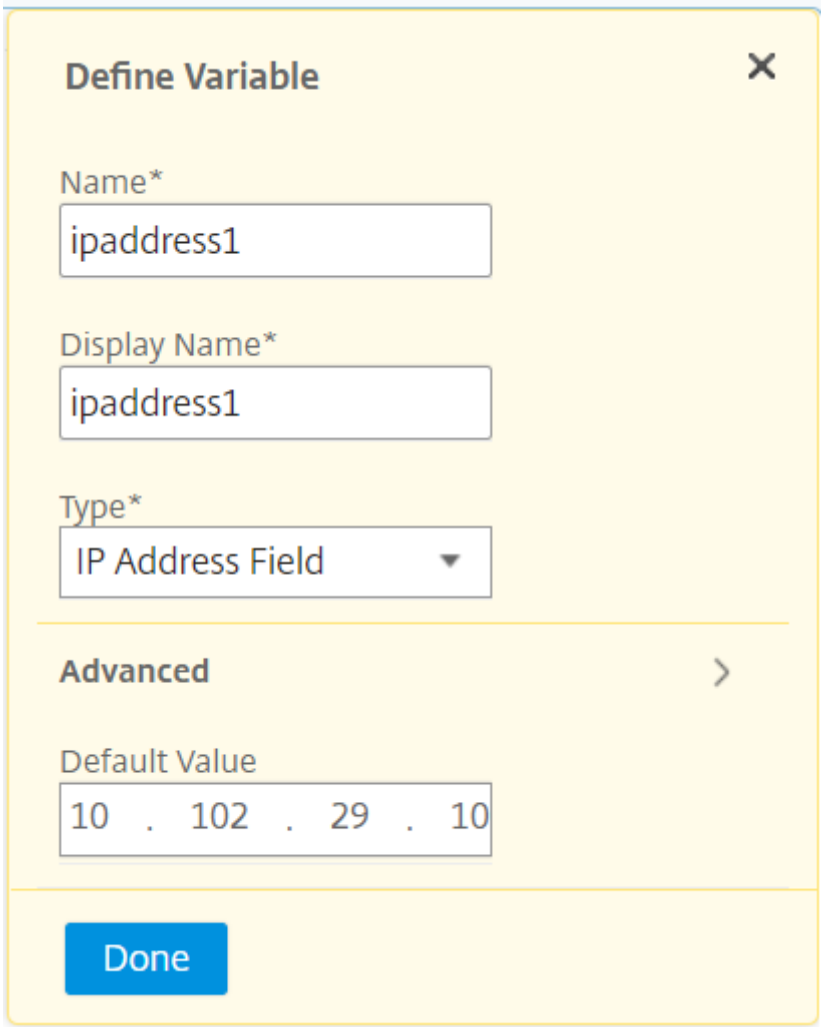
3. En la página **Editor de configuración**, escriba los comandos y guárdelos como una plantilla de configuración. También puede arrastrar una plantilla existente desde el panel izquierdo hasta el editor.

4. Seleccione los valores que desee convertir en una variable y, a continuación, haga clic en**Convertir en variable**. Por ejemplo, seleccione la dirección IP del servidor de equilibrio de carga "ipaddress1"y haga clic en**Convertir**en variable. La variable ahora se incluye con "$", como se muestra en la imagen siguiente.

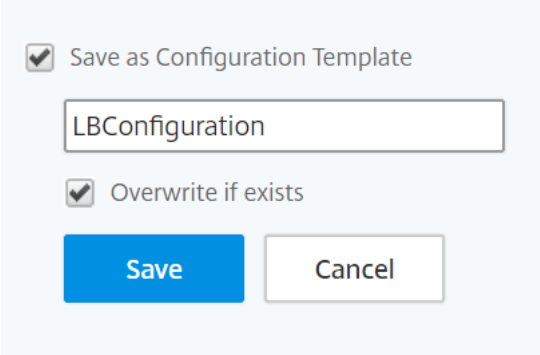



En la ventana **Definir variable**, defina las propiedades de esta variable: Nombre, nombre para mostrar y tipo de variable. Haga clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

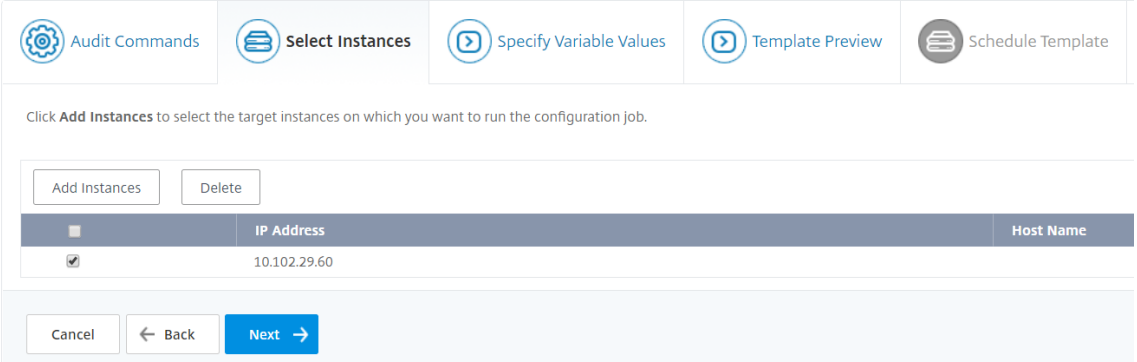



También puede guardar los comandos como una plantilla de configuración.




5. Haga clic en **Guardar** y, a continuación, en **Siguiente** .
6. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración y haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

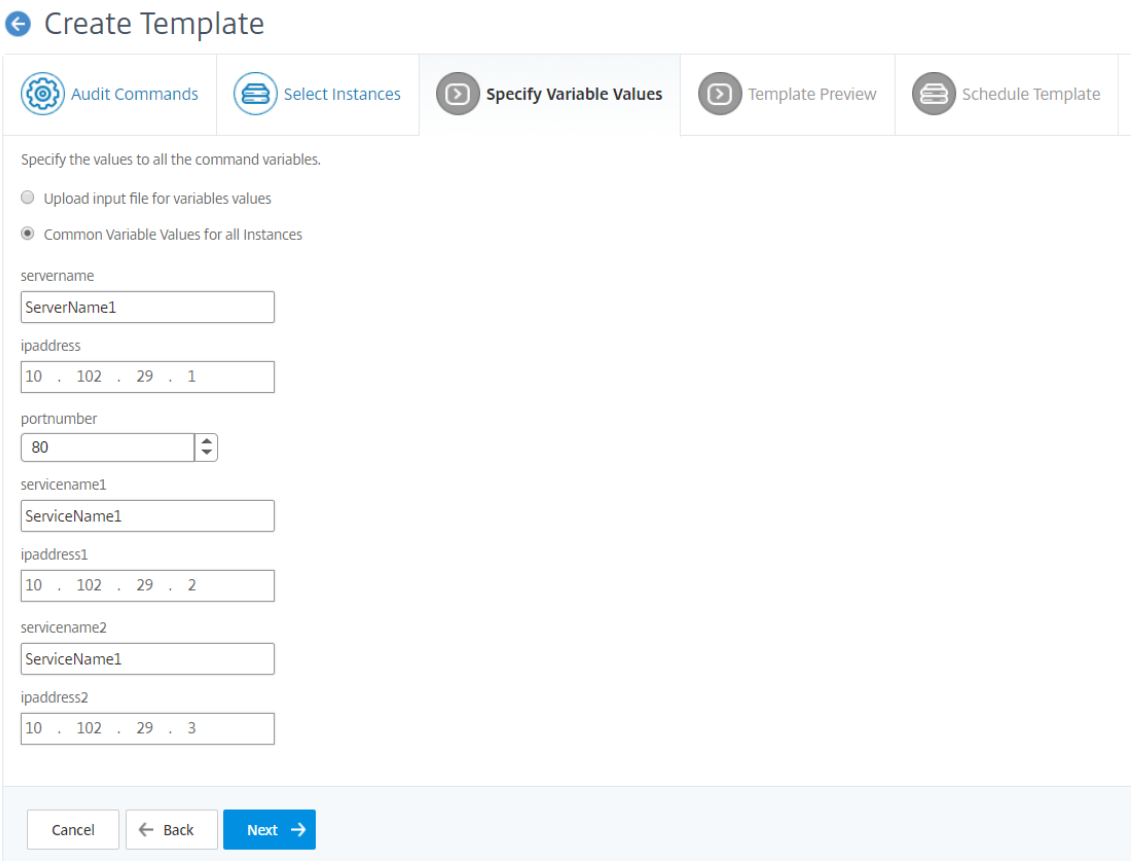



7. En la ficha **Especificar valores de variable**, tiene dos opciones:

   a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM

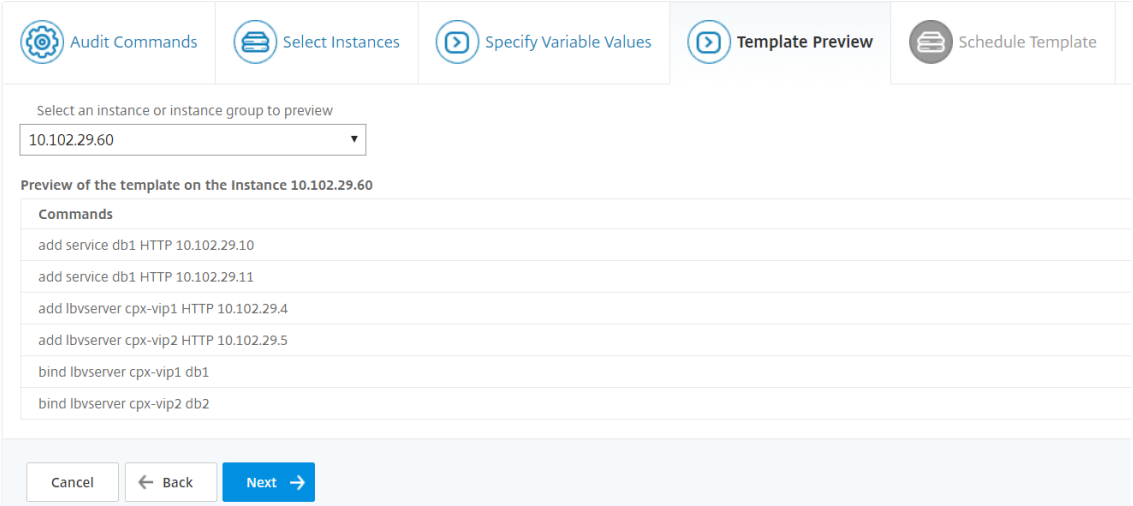
   b) Introduzca valores comunes para las variables que ha definido para todas las instancias.

8. Haga clic en **Siguiente**.




9. En la ficha **Vista previa de plantilla**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias. Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




10. En la ficha **Plantilla de programación**, tiene las siguientes opciones para programar la ejecución de la plantilla y configurar la dirección de correo para enviar el informe de diferencias.

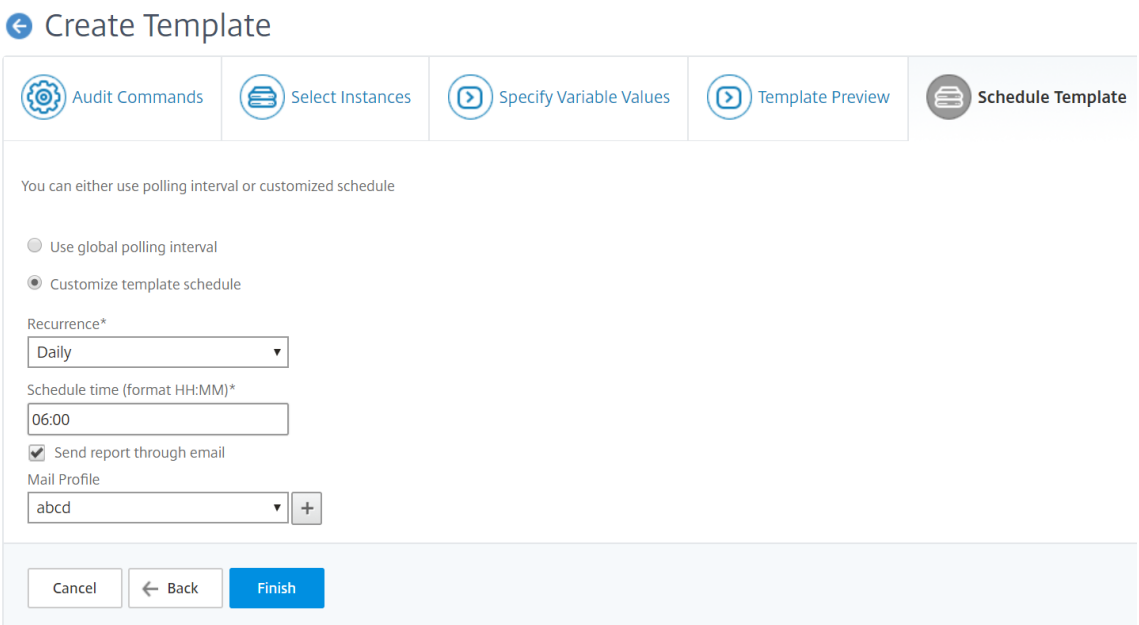
    - **Utilice el intervalo de sondeo global**. Seleccione esta opción para ejecutar la plantilla en las instancias a la vez configuradas globalmente en NetScaler ADM.

      > **Nota**
      >
      > Para configurar el intervalo de sondeo global en NetScaler ADM, vaya a **Redes** > **Auditoría de configuración** > **Plantillas de auditoría y haga** clic en **Intervalo de sondeo global**. En el campo **Intervalo de sondeo**, introduzca los minutos en los que NetScaler ADM debe sondear globalmente las instancias.

    - **Personalizar la planificación de plantillas**. Utilice esta opción para configurar la hora y la frecuencia a la que se deben ejecutar las plantillas
    - **Enviar informe por correo electrónico**. Utilice esta opción para configurar el perfil de correo al que se debe enviar el informe diff como archivo adjunto de correo.

11. Haga clic en **Finalizar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La plantilla de auditoría aparece en la lista **Plantillas de auditoría** y se ejecuta a la hora programada en las configuraciones de las instancias especificadas.

## Ver informes de auditoría

January 30, 2024

Citrix Application Delivery Management (Citrix ADM) le permite ver y descargar el informe de diferencias de auditoría de configuración en la sección de auditoría de configuración. La sección de auditoría de configuración le permite exportar el informe resumido en todas las instancias y por instancia, y también le permite exportar un informe detallado de diferencias para cada par instancia-plantilla.

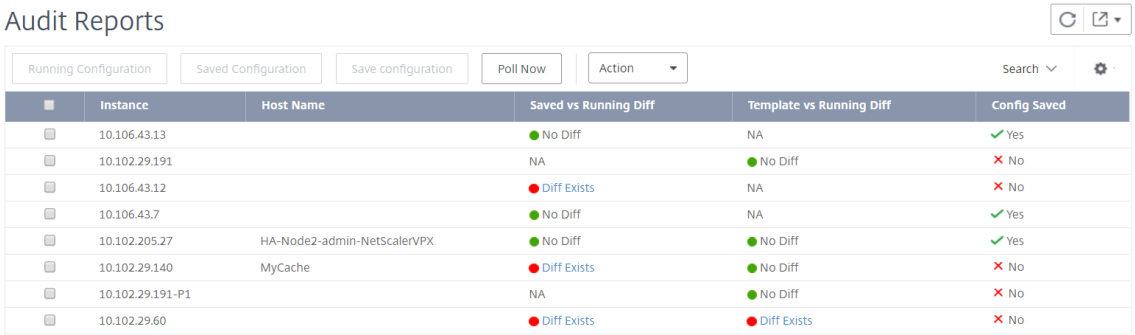
Las plantillas de auditoría que aparecen en la lista Plantillas de auditoría se ejecutan a la hora programada en las configuraciones de las instancias especificadas. El gráfico de **desviaciones de configuración de NetScaler** del panel de **auditoría de configuración** muestra detalles de alto nivel sobre los cambios de configuración entre las configuraciones guardadas y no guardadas. Al hacer clic en el gráfico de **derivas de NetScaler Config** , la siguiente página de **informes de auditoría** muestra una lista de instancias que muestra tanto «La diferencia existe» como «No hay diferencia». « Puede descargar los informes de diferencias que muestra Citrix ADM.

NetScaler ADM también ofrece una opción para programar la exportación automática de informes diff como datos adjuntos de correo. Para obtener más información sobre cómo programar la exportación de informes, consulte Creación de plantillas de auditoría.

**Para exportar informes de auditoría de configuración:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .
2. En la página **Auditoría de configuración**, haga clic dentro del gráfico de **desviaciones de configuración de NetScaler**.
3. La página **Informes de Auditoría** muestra las instancias que tienen una diferencia. La página también muestra una lista de instancias que no tienen ninguna diferencia en sus configuraciones en ejecución.

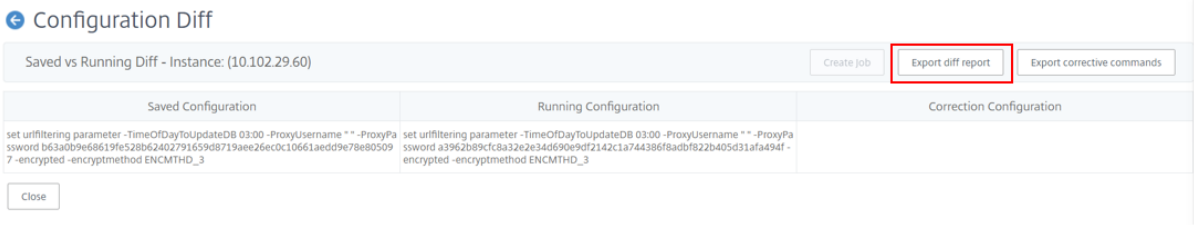



En la imagen puede ver que para algunos casos un diff está presente solo en **Saved Vs Running Diff** y para algunos casos, un diff está presente solo en **Template vs Running Diff**. En algunos casos, existen diferencias entre **Saved Vs Running Diff** y **Template vs Running Diff.**

## Diferencia guardada frente a ejecución

Puede ver un informe de la diferencia entre la configuración guardada en la instancia y la configuración que se ejecuta actualmente en esa instancia. Por ejemplo, haga clic en **Diff Exists**para ver una instancia en **Saved Vs Running Diff.**

Aquí, puede ver un informe para la configuración guardada contra la ejecución de diff de configuración para esa instancia.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Haga clic en **Exportar informe de diferencias** para descargar un archivo CSV del informe de diferencias. También puede hacer clic en Exportar comandos correctivos para exportar los comandos a un archivo.txt. A continuación, puede ejecutar los comandos en la instancia de Citrix ADM asociada desde los trabajos de configuración para corregir la configuración en esa instancia.

## Plantilla vs Diff Running

La **diferencia entre plantilla y ejecución** incluye todas las plantillas excepto **Saved Vs Running Diff**, que es la plantilla predeterminada. Puede ver la diferencia que existe entre la plantilla y la configuración en ejecución. Por ejemplo, haga clic en **Diff Exists** para una de las instancias en **Template vs Running Diff.**

| Instance | Host Name | Saved vs Running Diff | Template vs Running Diff | Config Saved |
|---|---|---|---|---|
| 10.106.43.13 | | No Diff | NA | Yes |
| 10.102.29.191 | | NA | No Diff | No |
| 10.106.43.12 | | Diff Exists | NA | No |
| 10.106.43.7 | | No Diff | NA | Yes |
| 10.102.205.27 | HA-Node2-admin-NetScalerVPX | No Diff | No Diff | Yes |
| 10.102.29.140 | MyCache | Diff Exists | No Diff | No |
| 10.102.29.191-P1 | | NA | No Diff | No |
| 10.102.29.60 | | Diff Exists | Diff Exists | No |

Ahora puede ver que dos plantillas muestran diff y que la instancia NetScaler ADM tiene una configuración diferente de la que está buscando la plantilla.

Templates of Instance: 10.102.29.60

| Templates | Diff Exists | Last Updated |
|---|---|---|
| LBVariablesTemplate | Diff Exists | Oct 10 2017 05:30:02 |
| LBConfigurationAudit | Diff Exists | Oct 27 2017 12:14:30 |

Haga clic de nuevo en**Diff Exists**. La siguiente imagen muestra la configuración que está buscando la plantilla y la configuración en ejecución que está en blanco, ya que no se ha configurado ni se ha eliminado ningún comando de este tipo. También puede ver las configuraciones de corrección o los comandos que se van a ejecutar para corregir la configuración.

Configuration Diff

Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate

Create Job | Export diff report | Export corrective commands

| Template Configuration | Running Configuration | Correction Configuration |
|---|---|---|
| add service lbservice2 10.102.29.11 HTTP 80 | | add service lbservice2 10.102.29.11 HTTP 80 |
| add service lbservice1 10.102.29.10 HTTP 80 | | add service lbservice1 10.102.29.10 HTTP 80 |
| add lb vserver lbserver1 HTTP 10.102.29.1 80 | | add lb vserver lbserver1 HTTP 10.102.29.1 80 |
| bind lb vserver servername lbservice2 | | bind lb vserver servername lbservice2 |

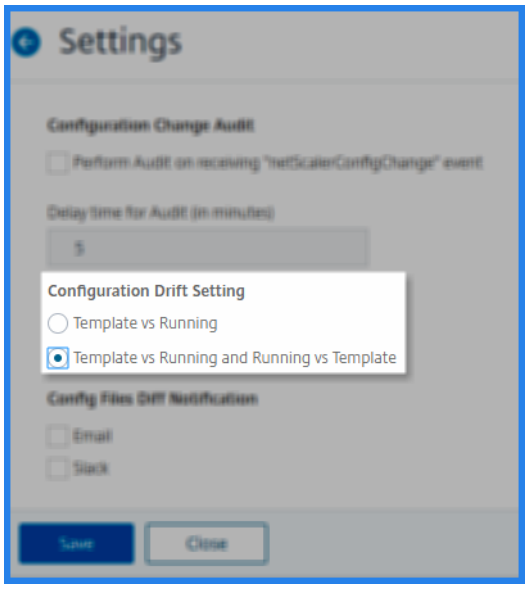
Close

También puede utilizar la configuración Plantilla frente a Ejecución y Ejecución frente a la plantilla, para comparar la configuración de ambos modos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Compara la configuración de la plantilla de auditoría con la configuración en ejecución en la instancia.
- Compara la configuración en ejecución de la instancia con la plantilla de auditoría.

De forma predeterminada, se selecciona la configuración Plantilla frente a derrapar en ejecución. Para modificar la configuración de deriva, en la GUI de ADM, seleccione **Configuración** en la página **Auditoría de configuración**.




Haga clic en **Exportar informe de diferencias** para descargar un archivo CSV del informe de diferencias. También puede hacer clic en **Exportar comandos correctivos** para exportar los comandos a un archivo.txt. A continuación, puede ejecutar los comandos de la CLI para corregir la configuración en esa instancia.

La siguiente imagen muestra un ejemplo de archivo diff CSV que se descarga en su sistema:

| | | |
|---|---|---|
| #Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate | | |
| | | |
| Template Configuration | Running Configuration | Correction Configuration |
| add service lbservice2 10.102.29.11 HTTP 80 | | add service lbservice2 10.102.29.11 HTTP 80 |
| add service lbservice1 10.102.29.10 HTTP 80 | | add service lbservice1 10.102.29.10 HTTP 80 |
| add lb vserver lbserver1 HTTP 10.102.29.1 80 | | add lb vserver lbserver1 HTTP 10.102.29.1 80 |
| bind lb vserver servername lbservice2 | | bind lb vserver servername lbservice2 |

## Ver los informes de auditoría de estado de archivo

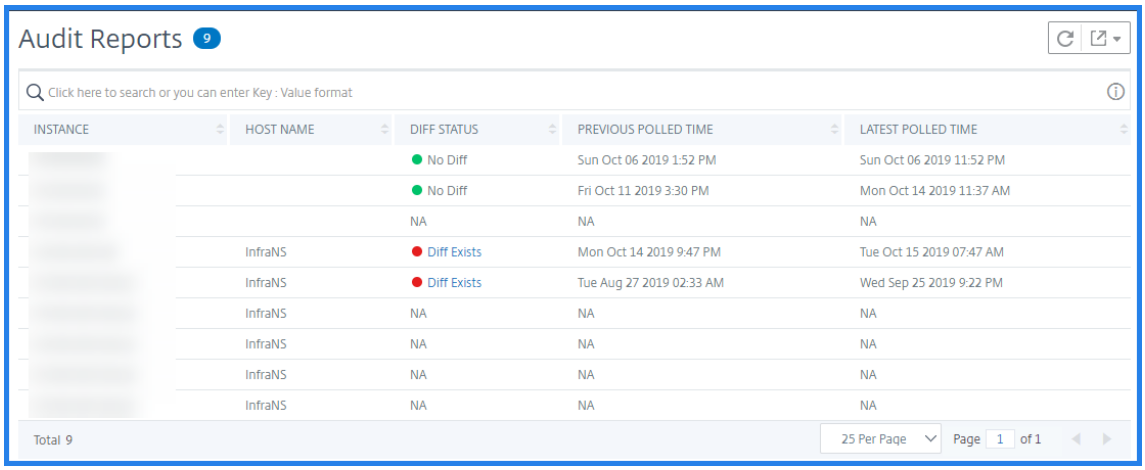
Mediante el gráfico **Estado de archivos de NetScaler ADC**, puede supervisar si se agregan, modifican o eliminan archivos de la carpeta `nsconfig`. Por ejemplo: Si el archivo de licencia se actualiza en una instancia ADC, puede comprobar cuándo se actualizó por última vez este archivo y tomar las medidas adecuadas.

Para exportar los informes de auditoría de estado de archivos para las instancias de NetScaler ADC:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

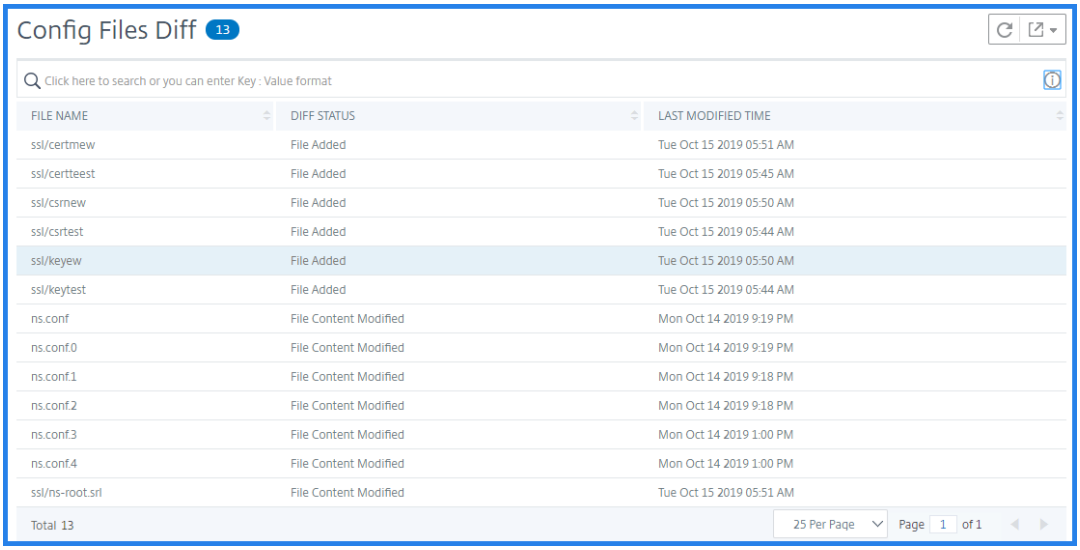
1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .
2. En la página **Auditoría de configuración**, haga clic dentro del gráfico de **estado de archivo NetScaler ADC**.

   La página **Informes de auditoría** muestra las instancias con el estado Diff.




   El **estado** de la diferencia se calcula para el intervalo entre la **hora de la encuesta anterior** y la **última hora de la encuesta**. El **estado** de la diferencia puede ser uno de los siguientes:

   - **Diff existe**: Este estado indica que los archivos han cambiado en la carpeta `nsconfig` de una instancia desde la **hora de la encuesta anterior**. Para ver lo que ha cambiado en el archivo, haga clic en **Diff Exists**.




   - **Sin diferencias**: Este estado indica que los archivos de la`nsconfig` carpeta no han cambiado desde la hora de la encuesta anterior.
   - **NA**: este estado indica que la supervisión del estado del archivo no es aplicable. Este estado aparece cuando el NetScaler ADM no sondea la instancia. Por ejemplo, cuando se

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

agrega una instancia nueva o el estado de instancia está inactivo, no se produce el sondeo de la instancia.

## Auditar los cambios de configuración en todas las instancias

August 23, 2024

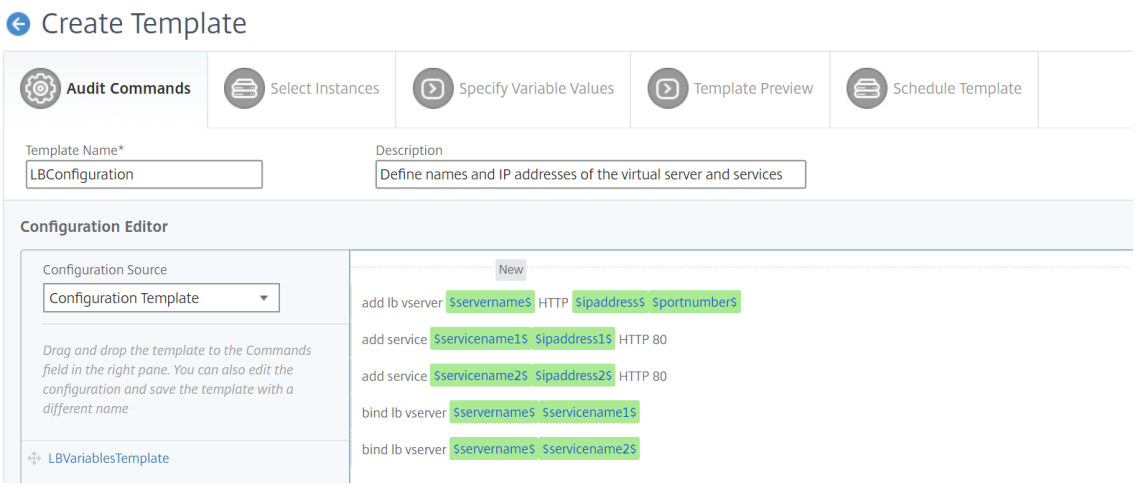
Debe asegurarse de que ciertas configuraciones se ejecuten en instancias específicas para lograr un rendimiento óptimo de la red. También querrá supervisar los cambios de configuración en las instancias administradas de Citrix Application Delivery Controller (ADC), solucionar errores de configuración y recuperar las configuraciones no guardadas tras un cierre repentino del sistema. Puede crear plantillas de auditoría con configuraciones específicas que quiera ejecutar en determinadas instancias. NetScaler Application Delivery Management (NetScaler ADM) compara estas instancias con la plantilla de auditoría y los informes si la configuración no coincide. Esto le permite solucionar problemas y rectificar los errores.

Puede automatizar la ejecución de la plantilla de auditoría programando la hora a la que debe ejecutarse la plantilla. También puede establecer la frecuencia con la que NetScaler ADM debe ejecutar la plantilla. Puede ejecutar la plantilla diariamente, en un día específico de una semana o en una fecha específica de un mes. También tiene la opción de enviar el informe de diferencias generado por Citrix ADM a las direcciones de correo electrónico especificadas que puede configurar. Con esta opción, el usuario recibe el informe como datos adjuntos de correo y no es necesario que el usuario inicie sesión en NetScaler ADM para comprobar los informes manualmente.

**Para crear plantillas de auditoría:**

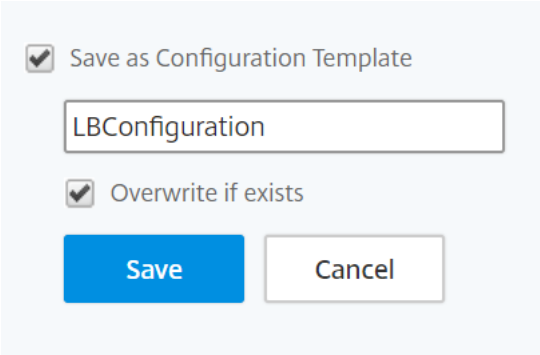
1. Vaya a**Redes > Auditoría de configuración > Plantillas de auditoría**y haga clic en**Agregar**.
2. En la página**Crear plantilla** y en la ficha**Comandos de auditoría**, especifique el nombre de la plantilla y su descripción.
3. En el **Editor de configuración**, escriba los comandos y guárdelos como una plantilla de configuración. También puede arrastrar una plantilla existente desde el panel izquierdo del editor.
4. Seleccione los valores que desee convertir en una variable y, a continuación, haga clic en**Convertir en variable**. Por ejemplo, seleccione la dirección IP del servidor de equilibrio de carga y`ipaddress`haga clic en**Convertir en variable**como se muestra en la imagen siguiente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



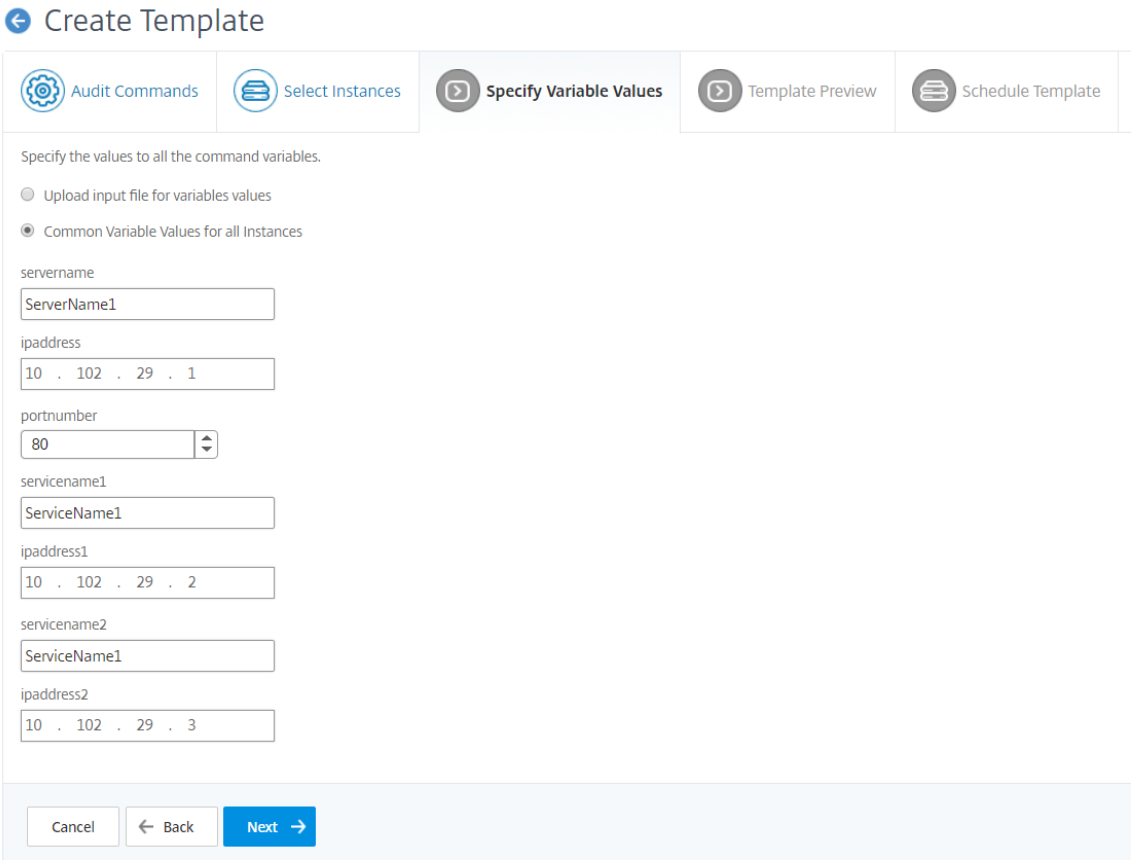

Haga clic en la opción **Avanzado** si quiere especificar un valor predeterminado para la variable.

También puede guardar los comandos como una plantilla de configuración.



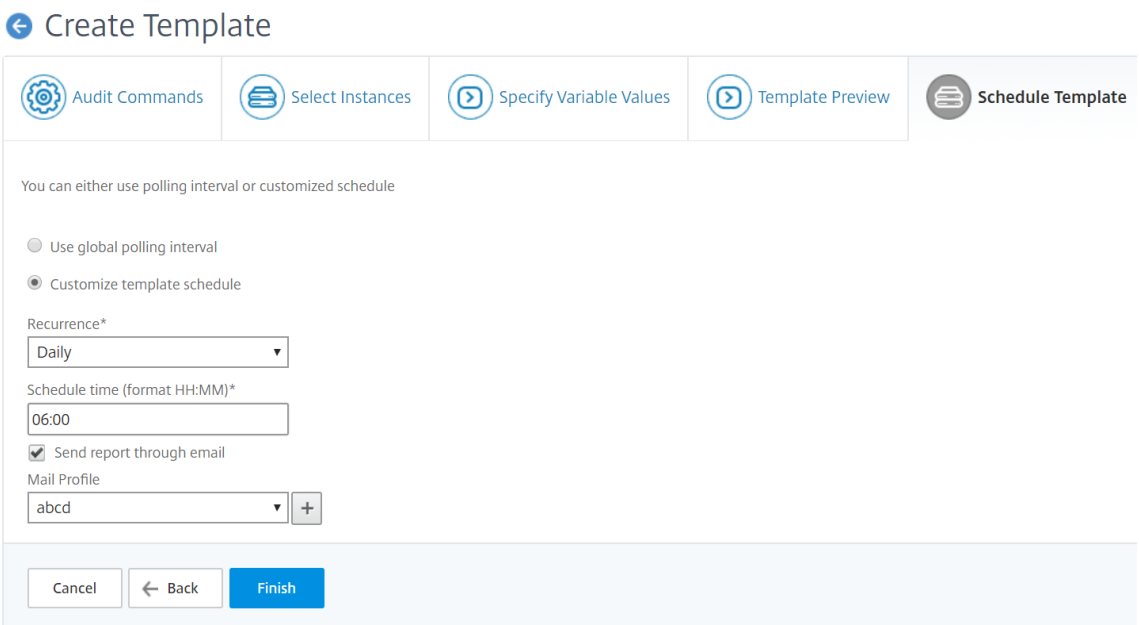

5. Haga clic en **Guardar** y, a continuación, en **Siguiente** .
6. En la ficha **Seleccionar instancias**, seleccione las instancias en las que quiere ejecutar la auditoría de configuración.
7. En la ficha **Especificar valores de variable**, tiene dos opciones:
   a) Descargue el archivo de entrada para especificar los valores de las variables que ha definido en sus comandos y, a continuación, cargue el archivo en el servidor NetScaler ADM
   b) Introduzca valores comunes para las variables que ha definido para todas las instancias.
8. Haga clic en **Siguiente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




9. En la ficha **Vista previa de plantilla**, puede evaluar y comprobar los comandos que se van a ejecutar en cada instancia o grupo de instancias. Haga clic en **Siguiente**.
10. En la ficha **Plantilla de programación**, tiene tres opciones para automatizar la ejecución de la plantilla y la dirección de correo para enviar el informe de diferencias.
    - **Utilice el intervalo de sondeo global**. Seleccione esta opción para ejecutar la plantilla en las instancias a la hora configurada globalmente en NetScaler ADM.
    - **Personalizar la planificación de plantillas**. Utilice esta opción para configurar la hora y la frecuencia a la que se deben ejecutar las plantillas
    - **Enviar informe por correo electrónico**. Utilice esta opción para configurar el perfil de correo al que se debe enviar el informe diff como un archivo adjunto de correo.
11. Haga clic en **Finalizar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



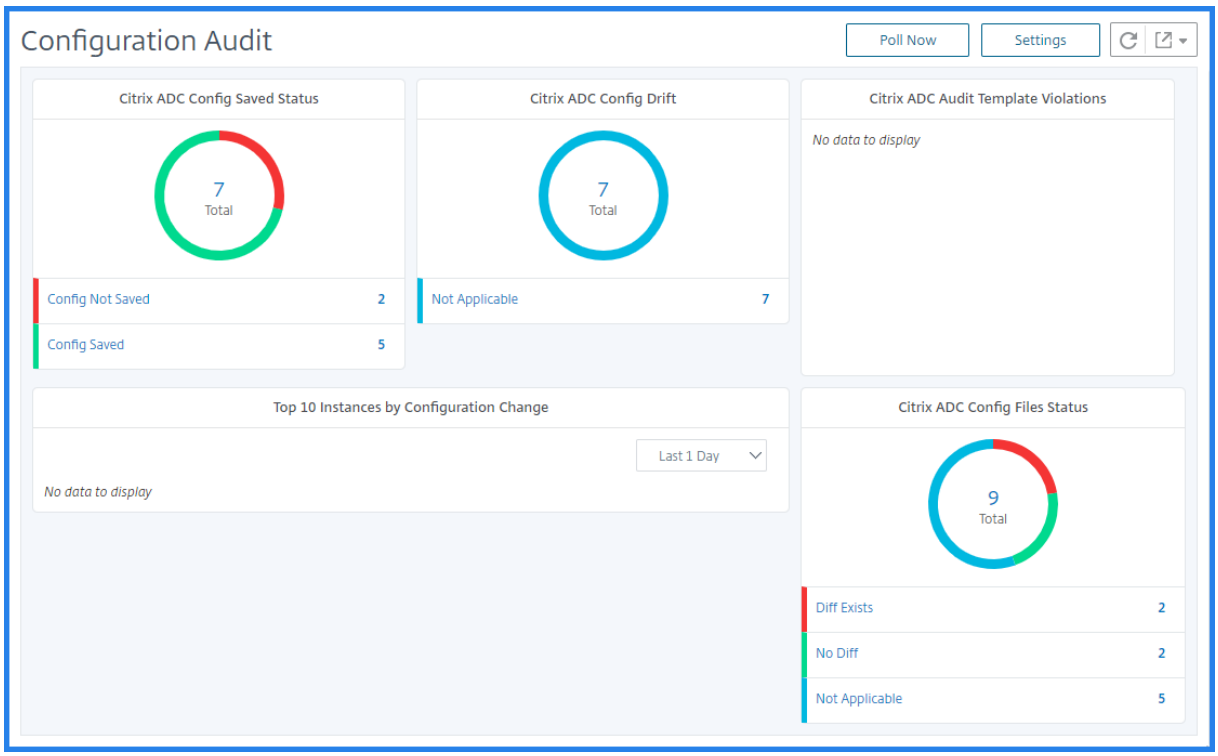

La plantilla de auditoría aparece en la lista Plantillas de auditoría y se ejecuta a la hora programada en las configuraciones de las instancias especificadas.

## Visualización de los detalles de los cambios de configuración

También puede utilizar el panel Auditoría de configuración para ver detalles de alto nivel sobre los cambios de configuración, como:

- Las diez instancias principales por cambio de configuración
- El número de configuraciones guardadas y no guardadas
- El archivo agregado, eliminado o modificado en la`nsconfig` carpeta

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

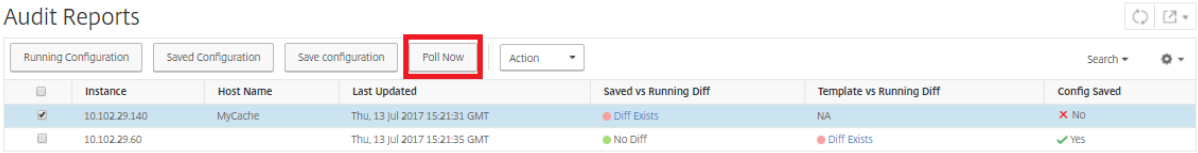



NetScaler ADM también le permite sondear auditorías de configuración manualmente y agrega todas las auditorías de configuración de las instancias inmediatamente al NetScaler ADM. Para ello, vaya a **Redes** > **Auditoría de configuración,** haga clic en Sondear **ahora** . La página emergente Sondear **ahora** le ofrece la opción de sondear todas las instancias de Citrix ADC de la red o sondear las instancias seleccionadas.

También puede forzar una auditoría en una instancia. Para ello, haga clic en cualquiera de los gráficos siguientes:

- **Estado guardado de la configuración de NetScaler ADC**
- **Deriva de configuración de NetScaler ADC**

En la página **Informes de auditoría**, seleccione la instancia y, en la lista **Acción**, seleccione **Encuesta ahora**.




El gráfico de **estado del archivo de configuración de NetScaler ADC** proporciona el estado de los archivos NetScaler ADC presentes en la`nsconfig` carpeta. NetScaler ADM registra y compara los cambios en los archivos dentro de la`nsconfig` carpeta y muestra las diferencias. Consulte Ver los informes de auditoría del estado de los archivos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Establecer notificaciones de auditoría de configuración

1. Vaya a **Redes** > **Auditoría de configuración**.
2. En la página **Auditoría de configuración**, haga clic en **Configuración**.
3. En la página **Configuración de notificaciones**, haga clic en el icono **Editar** para habilitar la configuración de notificaciones.
4. Seleccione la casilla **Habilitado** y, a continuación, seleccione una lista de distribución de correo electrónico en la lista desplegable. También puede crear una lista de distribución de correo electrónico haciendo clic en el icono **+** y especificando los detalles del servidor de correo electrónico.

## Obtener consejos de configuración sobre la configuración de la red

January 30, 2024

Configure las instancias de Citrix Application Delivery Controller (ADC) con configuraciones óptimas para que pueda lograr un rendimiento óptimo en sus aplicaciones. Sin embargo, algunas configuraciones pueden no ser configuraciones estándar, lo que podría afectar al rendimiento de sus aplicaciones.

Para ayudarle a optimizar el rendimiento de las aplicaciones, NetScaler Application Delivery Management (NetScaler ADM) analiza la configuración de instancias de NetScaler ADC y le proporciona recomendaciones. Puede aplicar las configuraciones recomendadas desde NetScaler ADM.

**Para analizar la instancia de NetScaler ADC:**

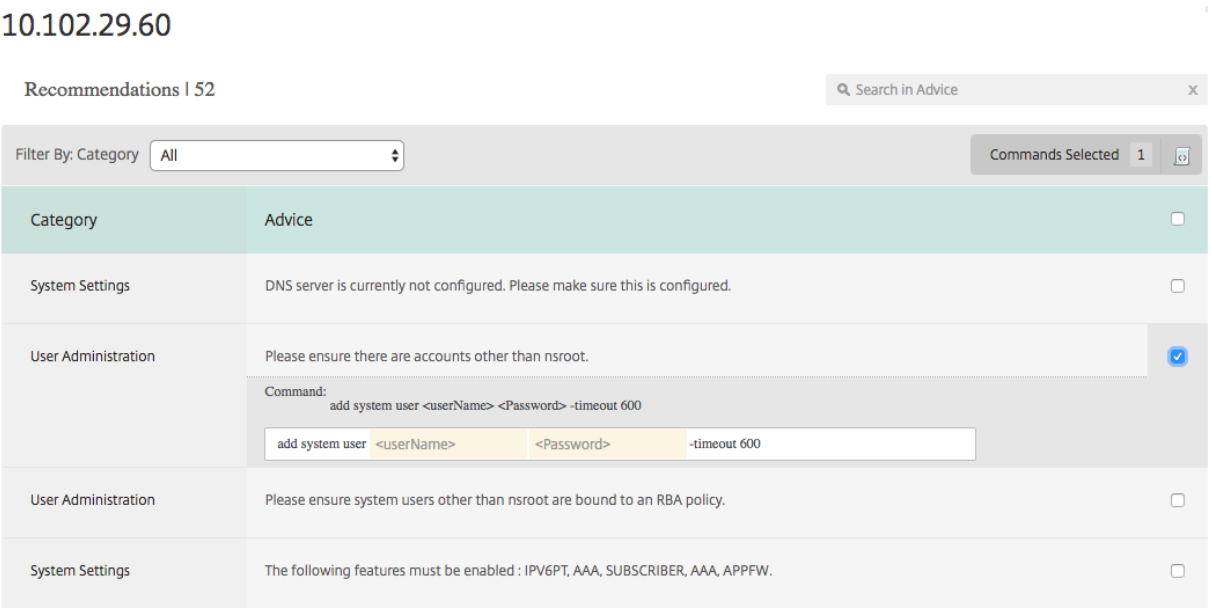
1. Vaya a **Redes** > **Auditoría de configuración** > **Asesoramiento de configuración** .
2. Lleve a cabo una de las siguientes acciones:

   - Haga clic en **Cargar archivo de configuración** y cargue el archivo de configuración de su instancia de red.

   - Haga clic en Seleccionar **dispositivo** y seleccione la instancia de Citrix ADC que quiere analizar.

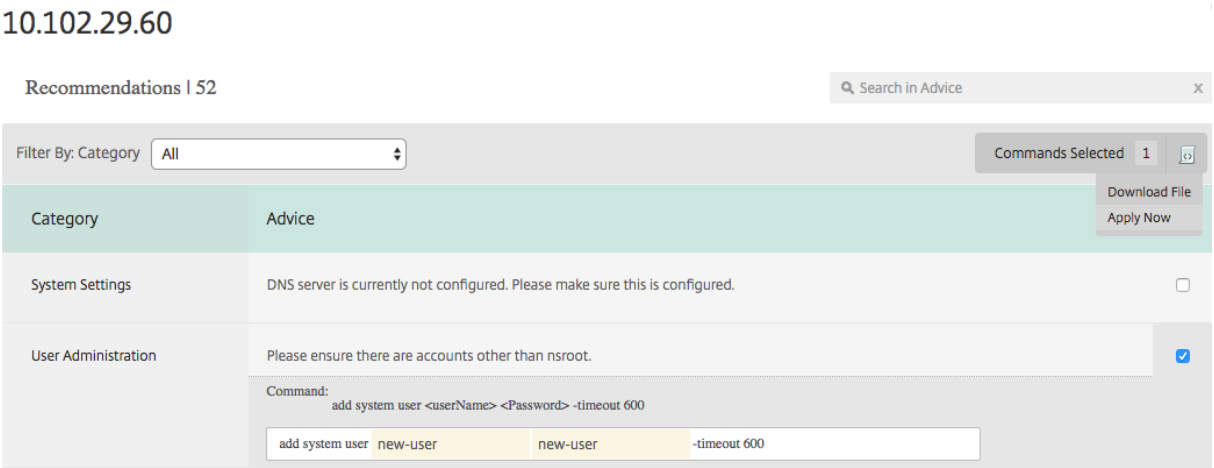
NetScaler ADM analiza la configuración de la instancia y proporciona una lista de recomendaciones de configuración como se muestra en la imagen siguiente. Haga clic en la casilla de verificación situada junto a un consejo de configuración para ver los comandos correctivos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

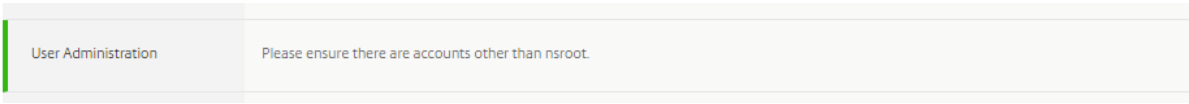



Si quiere actualizar la configuración, especifique los valores de las variables en los comandos correctivos y haga clic en **Aplicar ahora** como se muestra en la imagen siguiente.

> **Nota**
>
> Los comandos que se enumeran aquí son solo recomendaciones. Un usuario con acceso de lectura y escritura podría modificar cualquier comando mediante esta función. Asegúrese de conceder un acceso privilegiado limitado a los usuarios que considere que no deben modificar los comandos.

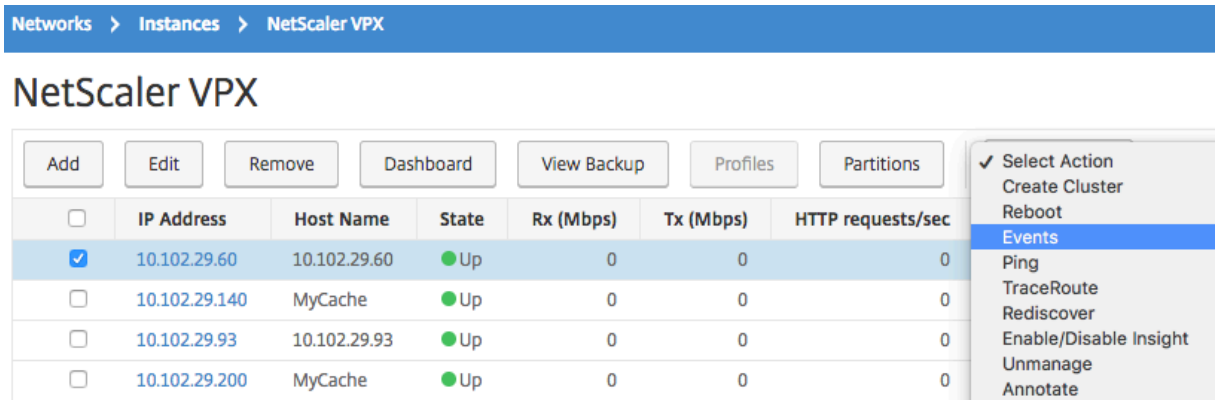



Cuando el comando se ejecuta correctamente en la instancia de red, la casilla de verificación situada junto al consejo desaparece.

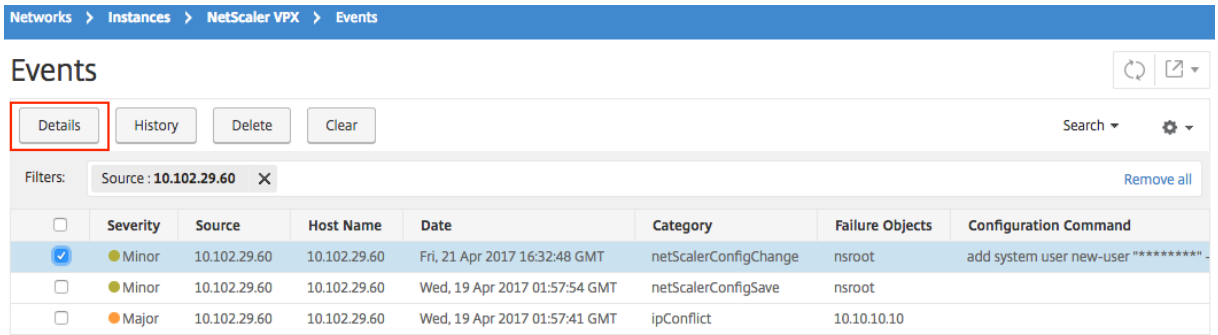



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si quiere ver los detalles de los comandos ejecutados en la instancia de red, vaya a **Redes > Instancias > <Instance_Type\>**, seleccione la dirección IP de la instancia y, a continuación, haga clic en **Eventos** en la lista desplegable **Acciones** .




En la página **Eventos**, puede ver los detalles del cambio de configuración.




## Auditoría de configuración de sondeo de instancias NetScaler ADC

January 30, 2024

Citrix Application Delivery Management (Citrix ADM) sondea automáticamente las auditorías de configuración cada 10 horas para buscar los cambios de configuración que se producen en las instancias de Citrix Application Delivery Controller (ADC). También puede sondear manualmente las auditorías de configuración para detectar cambios recientes, pero sondear todas las instancias de configuración de NetScaler ADC coloca una carga pesada en la red.

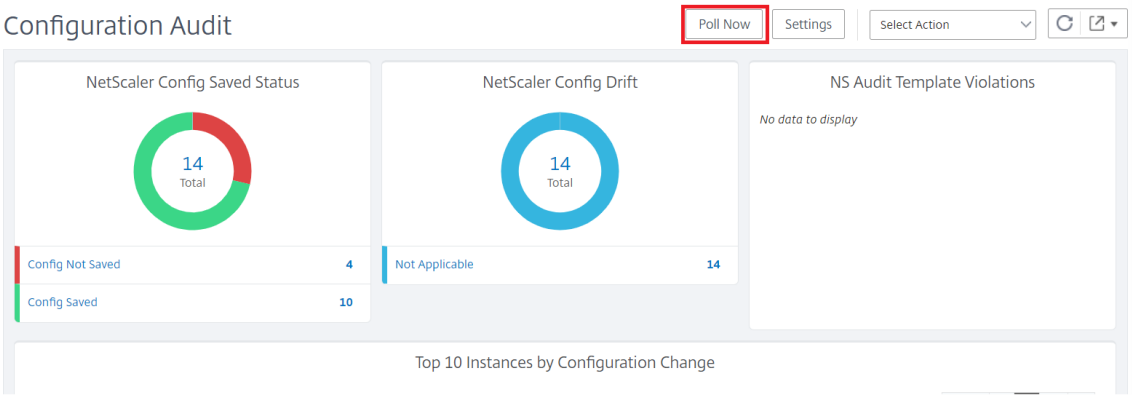
En lugar de sondear toda la auditoría de configuración de las instancias de NetScaler ADC, puede sondear manualmente solo las auditorías de configuración de una instancia o instancias seleccionadas.

**Para sondear auditorías de configuración de instancias NetScaler ADC:**

1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .

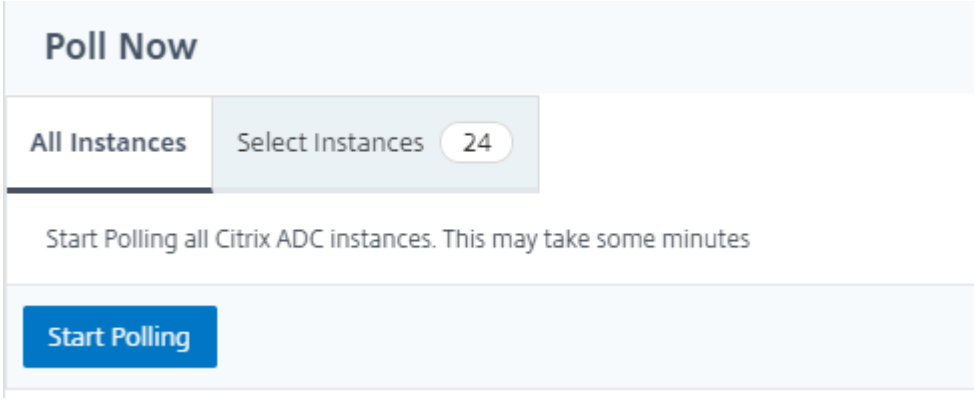
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página **Auditoría de configuración**, en la esquina superior derecha, haga clic en **Sondear ahora**.

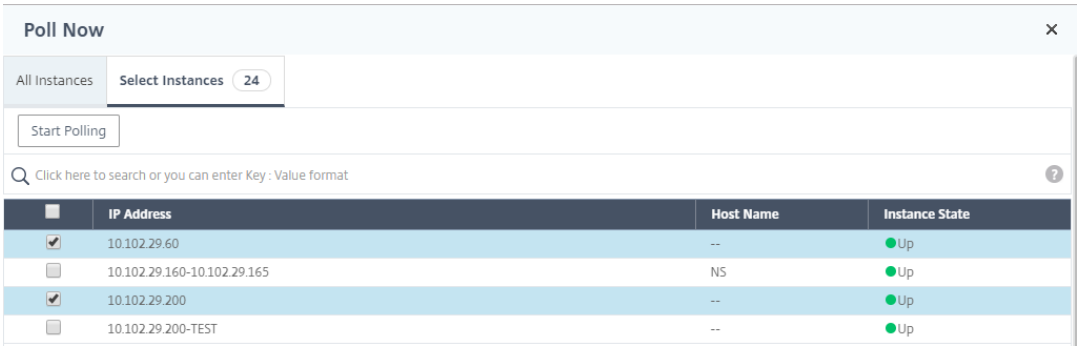



3. Aparece la página **Encuesta ahora**, que le da la opción de sondear todas las instancias de NetScaler ADC en la red o sondear las instancias seleccionadas.

   a) Para sondear todas las instancias de NetScaler ADC, seleccione la ficha **Todas las instancias** y haga clic en **Iniciar sondeo**.




   b) Para sondear instancias específicas, seleccione la ficha **Seleccionarinstancias**, seleccione las instancias de la lista y haga clic en**Sondear ahora**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Generar diferencias de auditoría de configuración para capturas SNMP de ConfigChange

January 30, 2024

Siempre que se produzca un cambio de configuración en una instancia de Citrix Application Delivery Controller (ADC) de la red, se actualiza el archivo de configuración. La instancia envía una captura SNMP de ConfigChange a Citrix Application Delivery Management (Citrix ADM). Puede habilitar NetScaler ADM para realizar una auditoría de configuración en esa instancia cuando ésta envía una captura SNMP de ConfigChange.

Si existe alguna diferencia entre la configuración de la plantilla de auditoría y la configuración en ejecución, aparecerá un mensaje de estado Diff Exists en la página Informe de auditoría. Al hacer clic en el enlace Diff Exits , accederá a la página Configuration Diff , donde podrá ver el comando correctivo. Puede utilizar estos comandos correctivos para crear un trabajo de configuración y ejecutarlo en las instancias específicas de NetScaler ADC. Cuando ejecuta el trabajo de configuración, las instancias vuelven a la configuración deseada. Para obtener más información sobre cómo crear un trabajo de configuración a partir de comandos correctivos, consulte Cómo crear trabajos de configuración a partir de comandos correctivos en NetScaler ADM.

**Para ejecutar plantillas de auditoría de configuración al recibir la captura SNMP de ConfigChange:**

NetScaler ADM le permite habilitar la opción de ejecutar la plantilla de auditoría de configuración en NetScaler ADM.

1. En Citrix ADM, vaya a **Redes** > **Auditoría de configuración** .
2. Haga clic **en ****Configuración en la página Auditoría** de configuración .
3. Haga clic en el icono de edición en la sección **Ajustes de auditoría de cambios de configuración**.
4. Seleccione la casilla **Realizar una auditoría de configuración cuando se reciba el evento netScalerConfigChange**.

> **Nota:**
>
> Se trata de una configuración global para todas las instancias. NetScaler ADM realiza una auditoría de configuración para cada instancia en la que reciba las capturas SNMP de NetScalerConfigChange en el futuro.

1. En el campo **Tiempo de espera para ejecutar la plantilla de auditoría** (en minutos), escriba los minutos. NetScaler ADM ejecuta la plantilla de auditoría de configuración en la instancia de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

NetScaler ADC después de este retraso de tiempo cuando recibe la captura de ConfigChange SNMP por esa instancia.

## Funciones de red

January 30, 2024

Con la función Funciones de red, puede supervisar el estado de las entidades configuradas en sus instancias administradas de Citrix Application Delivery Controller (ADC). Puede ver estadísticas como detalles de transacciones, detalles de conexión y rendimiento de un servidor virtual de equilibrio de carga. También puede habilitar o inhabilitar las entidades cuando planifique un mantenimiento.

El panel de funciones de red le proporciona los siguientes gráficos:

- Los 5 mejores servidores virtuales con mayor cantidad de conexiones de clientes
- Los 5 mejores servidores virtuales con el mayor número de conexiones
- Los 5 mejores servidores virtuales con un rendimiento máximo (MB/seg)
- Los 5 servidores virtuales más bajos con el rendimiento más bajo (MB/seg)
- Las 5 mejores instancias con la mayoría de los servidores virtuales
- Estado de los servidores virtuales
- Estado de los servidores virtuales de equilibrio de carga
- Protocolos

## Generar informes para entidades de equilibrio de carga

January 30, 2024

Citrix Application Delivery Management (ADM) le permite ver los informes de las entidades de instancia de Citrix Application Delivery Controller (ADC) en todos los niveles. Hay dos tipos de informes que puede descargar en Citrix ADM > Network Functions : informes consolidados e informes individuales.

**Informes consolidados**: puede descargar y ver un informe consolidado o resumido de todas las entidades que se administran en instancias de Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Este informe le permite tener una vista de alto nivel de la asignación entre las instancias, particiones y las entidades de equilibrio de carga correspondientes (servidores virtuales, grupos de servicios y servicios) de Citrix ADC que están presentes en la red.

La siguiente imagen muestra un ejemplo de un informe resumido.

| Citrix ADC IP Address | Citrix ADC HostName | Partition | Type of Virtual Server | Virtual Server | Target LB Virtual Server | Service | Service Group |
|---|---|---|---|---|---|---|---|
| | beta | | Load Balancing | | | | |
| | | | Load Balancing | | | | |
| | | | Load Balancing | | | | |
| | | | Load Balancing | | | | |
| | | | Load Balancing | lb11-lb#11.1.2.2:80 | | | lb11-svcgrp#3.4.4.4-3.4.4.4:80 |
| | | | Load Balancing | ADM-Test-LB3#10.1.1.3:80 | | | |
| | | | Load Balancing | 334-lb#1.33.2.2:80 | | | |
| | | | Load Balancing | | | | |
| | | | Load Balancing | | | | |
| | | | Load Balancing | 33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b | | | 33f97d16-0413-4e6e-9f3d-844 |
| | | | Load Balancing | 33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8 | | | 33f97d16-0413-4e6e-9f3d-844 |
| | | | Load Balancing | 33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9 | | | 33f97d16-0413-4e6e-9f3d-844 |
| | | | Load Balancing | kjbj-lb#1.2.3.4:80 | | | kjbj-svcgrp |
| | | | Load Balancing | | | | |

El informe consolidado está en formato CSV. Las entradas de cada columna se describen de la siguiente manera:

- Dirección IP de**NetScaler: la dirección IP**de la instancia de Citrix ADC se muestra en el informe
- **Nombre de host de NetScaler**: el nombre del host se muestra en el informe.
- **Partición**: se muestra la dirección IP de la partición administrativa
- **Servidor virtual**: <name_of_the_virtual_server>#virtual_IP_address :port_number
- **Servicios**: <name_of_the_service>#service -IP_Address:port_number
- **Grupos de servicio**: <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_a
  ……..,server_membern_IP_address:port

> **Nota**
>
> - Si no hay ningún nombre de host disponible, se muestra la dirección IP correspondiente.
> - Las columnas en blanco indican que las entidades respectivas no están configuradas para esa instancia de Citrix ADC.

**Informes individuales**: también puede descargar y ver informes independientes de todas las instancias y entidades. Por ejemplo, puede descargar un informe solo para servidores virtuales o servicios de equilibrio de carga o grupos de servicios de equilibrio de carga.

Citrix ADM le permite descargar el informe al instante. También puede programar el informe para que se genere a una hora fija una vez al día, una vez a la semana o una vez al mes.

## Generar un informe de equilibrio de carga combinado

1. En Citrix ADM, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página **Equilibrio de carga**,
3. En la página **Exportar** que se abre, tiene dos opciones para ver el informe:
   a) Seleccione la ficha **Exportar ahora** y haga clic en **Aceptar**.

      El informe consolidado se descarga en su sistema.

   b) Seleccione la pestaña **Programar informe** para programar la generación y exportación del informe a intervalos regulares. Especifique la configuración de recurrencia de generación de informes y cree un perfil de correo electrónico al que se exporta el informe.

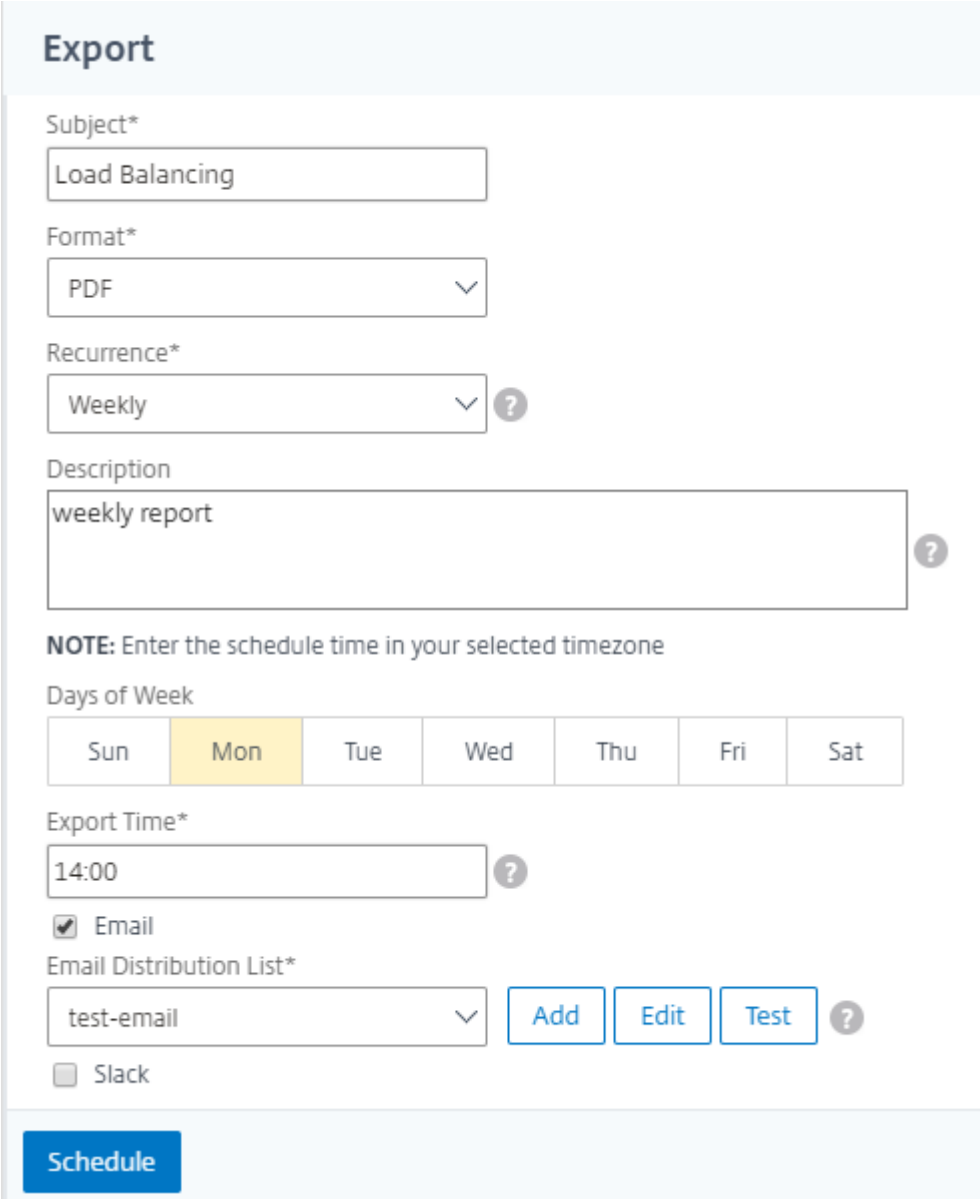
      i. **Periodicidad**: seleccione**Diariamente**,**Semanalmente**o**Mensualmente**en el cuadro de lista desplegable.

      ii. **Tiempo de recurrencia**: Introduzca la hora como Hora:Minuto en formato de 24 horas.

      iii. **Perfil de correo electrónico**: selecciona un perfil del cuadro de lista desplegable o haga clic en**+**para crear un perfil de correo electrónico.

> **Nota**
>
> Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

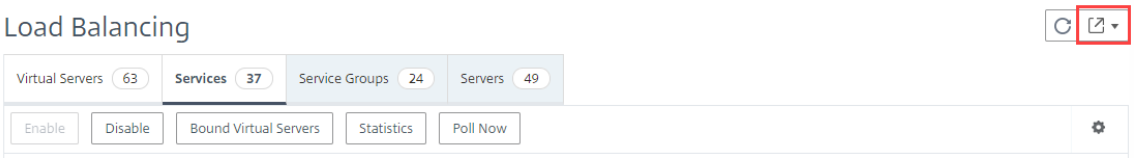
### Generar un informe de entidad de equilibrio de carga individual

Puede generar y exportar un informe individual para un tipo concreto de entidad asociada a las instancias. Por ejemplo, considere un caso en el que quiera ver una lista de todos los servicios de equilibrio de carga de la red.

1. En Citrix ADM, vaya a **Redes** > **Funciones de red** > **Equilibrio de carga > Servicios.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página **Servicios**, haga clic en el botón **Exportar** en la esquina superior derecha.




   a) Seleccione la ficha **Exportar ahora** si quiere generar y ver el informe en este instante.

   b) Seleccione **Programar exportación** para programar la generación y exportación del informe a intervalos regulares.

> **Nota**
>
> Solo puede descargar los informes o exportarlos como archivos adjuntos de correo. No puede ver los informes en la GUI de Citrix ADM.

## Exportar o programar la exportación de informes de funciones de red

January 30, 2024

Puede generar un informe completo para determinadas funciones de red, como Equilibrio de carga, Content Switching, Redirection de caché, Global Server Load Balancing (GSLB), Autenticación y Citrix Gateway en Citrix Application Delivery Management (ADM). Este informe le permite tener una vista de alto nivel de la asignación entre las instancias de Citrix ADC, las particiones y las entidades enlazadas correspondientes (servidores virtuales, grupos de servicios y servicios) presentes en la red. Puede exportar estos informes en formato de archivo CSV.

El informe muestra los siguientes datos del servidor virtual:

- Dirección IP de NetScaler
- Nombre de host
- Datos de partición
- Nombre del servidor virtual
- Tipo de servidor virtual
- Servidor virtual
- Servidor virtual LB de destino

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

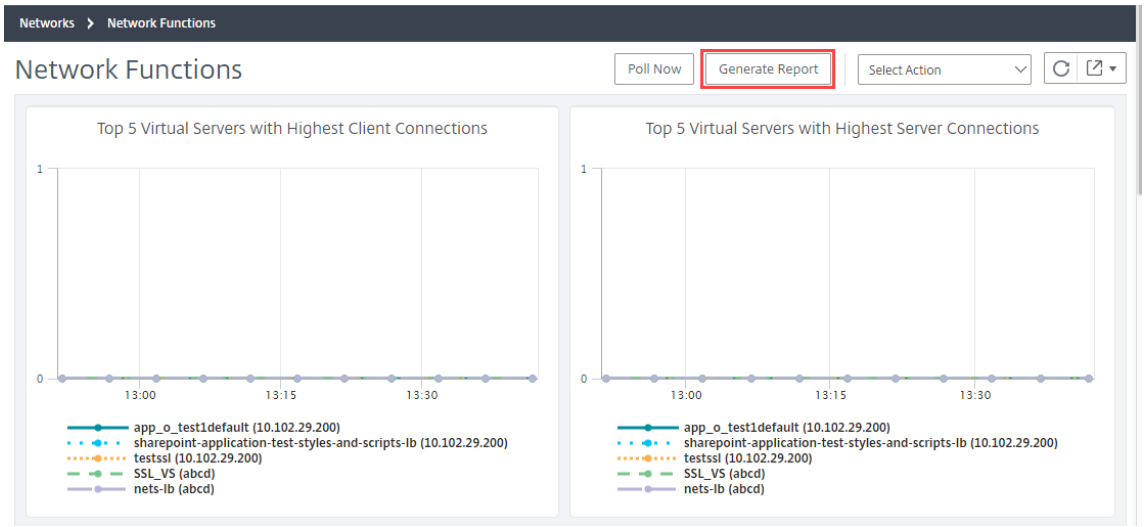
> **Nota**
>
> Para los servidores virtuales de conmutación de contenido y redirección de caché, la columna Servidor virtual de Target LB muestra todos los servidores LB, es decir, los servidores predeterminados y los servidores basados en directivas.
>
> - Nombre del servicio
> - Nombre del grupo de servicios

Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en diferentes intervalos.

> **Nota**
>
> - Para los servidores virtuales GSLB, el informe de funciones de red muestra solo los servidores virtuales GSLB y los servicios asociados.
> - Para los servidores virtuales de conmutación de contenido y redirección de caché, el informe muestra solo los enlaces a los servidores LB asociados.
> - Los servidores virtuales SSL no aparecen en este informe porque Citrix ADM no mantiene una lista independiente de servidores virtuales SSL.
> - Cuando se genera un nuevo informe, los informes antiguos se depuran automáticamente de su cuenta.
> - No puede generar un informe de funciones de red para HAProxy.

**Para exportar y programar informes de funciones de red:**

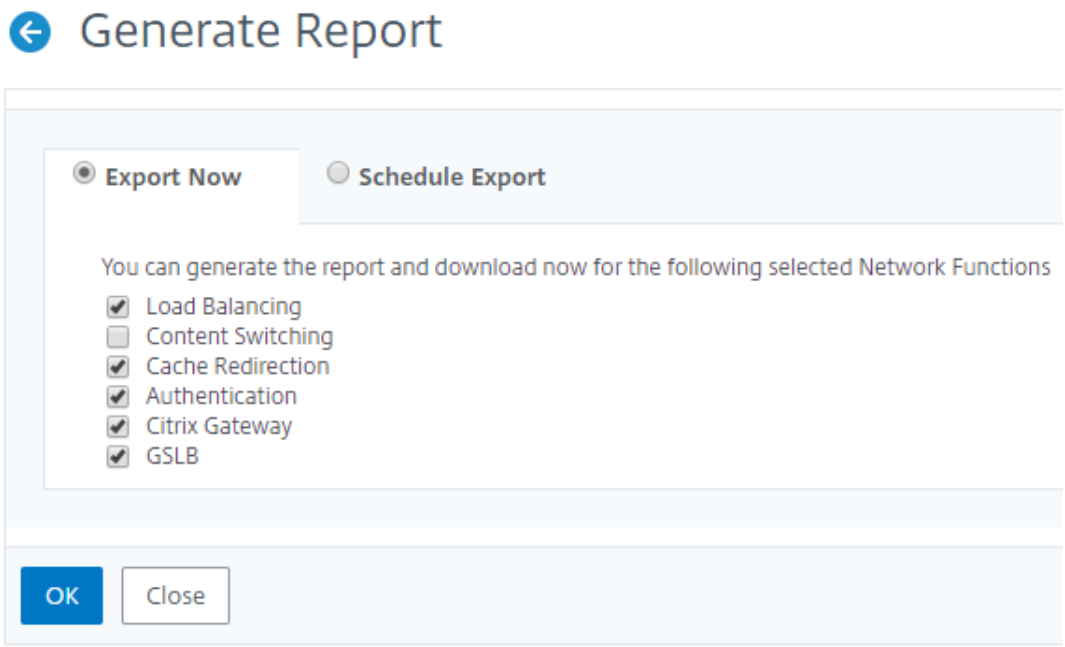
1. Vaya a**Redes > Funciones de red**.
2. En la página**Funciones de red**, en el panel derecho, haga clic en**Generar informe**en la esquina superior derecha de la página.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la página **Generar informe**, tiene las dos opciones siguientes:

   a) Seleccione la ficha **Exportar ahora** y haga clic en **Aceptar**. El informe se descarga en su sistema.




   La imagen siguiente muestra un ejemplo de un informe de funciones de red.

| NetScaler ADC IP Address | NetScaler ADC HostName | Partition | Type of Virtual Server | Virtual Server | Target LB Virtual Server | Service | Service Group |
|---|---|---|---|---|---|---|---|
| 10. | 10. | | Load Balancing | lb_test_1#10.10.10.10:80 | | adm_metric_collector_svc_10.106.171.41#10.10 | |
| 10. | 10. | | Load Balancing | lbvs_511#51.1.1.1:80 | | test_1#10.102.61.105:80 | |
| 10. | 10. | | Load Balancing | lbvs_521#52.1.1.1:80 | | test_1#10.102.61.105:80 | |
| 10. | 10. | | Load Balancing | SG_HS_DNS_MON#1.2.22.2:80 | | | sc1 |
| 10. | 10. | | Load Balancing | SG_HS_DNS_MONgdvfffs#1.3.4.5:80 | | | |
| 10. | 10. | | Load Balancing | atest94#1.1.1.11:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_101#1.10.1.1:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_1010#1.10.1.10:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_10100#1.10.1.100:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_10101#1.10.1.101:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_10102#1.10.1.102:80 | | | |
| 10. | 10. | | Load Balancing | lbvs1_10103#1.10.1.103:80 | | | |

   b) Seleccione la ficha**Informe**de programación para programar la generación y exportación del informe a intervalos regulares. Especifique la configuración de recurrencia de generación de informes y cree un perfil de correo electrónico al que se exporta el informe.

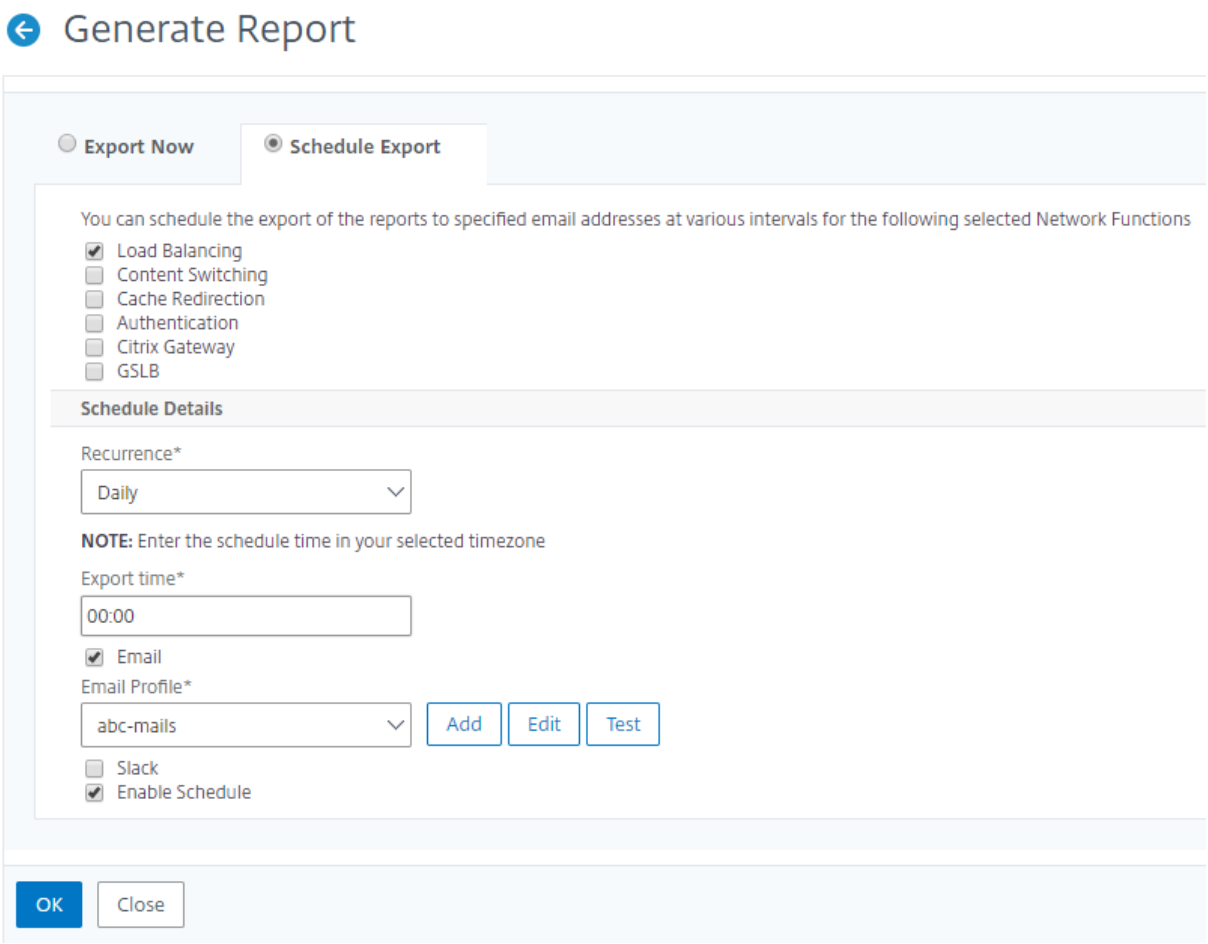
      i. **Periodicidad**: seleccione**Diariamente**,**Semanalmente**o**Mensualmente**en el cuadro de lista desplegable.

      ii. **Tiempo de recurrencia**: introduzca la hora como Hora: Minuto en formato de 24 horas.

      iii. **Perfil de correo electrónico**: selecciona un perfil del cuadro de lista desplegable o haga clic en**+**para crear un perfil de correo electrónico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Haga clic en **Habilitar programación** para programar el informe y, a continuación, haga clic en **Aceptar**. Al hacer clic en la casilla **Habilitar programación**, puede generar los informes seleccionados.




## Informes de red

January 30, 2024

Puede optimizar el uso de los recursos supervisando los informes de su red en NetScaler Application Delivery Management (NetScaler ADM). Es posible que tenga una implementación distribuida con muchas aplicaciones implementadas en varias ubicaciones. Para garantizar un rendimiento óptimo de sus aplicaciones, también ha implementado varias instancias de Citrix Application Delivery Controller (NetScaler ADC) para equilibrar la carga, cambiar el contenido o comprimir el tráfico. El rendimiento de la red puede afectar al rendimiento de la aplicación. Para continuar manteniendo el rendimiento de sus aplicaciones, debe supervisar regularmente el rendimiento de la red y asegurarse de que todos los recursos se utilizan de manera óptima.

NetScaler ADM ahora le permite generar informes no solo para instancias a nivel global, sino también

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

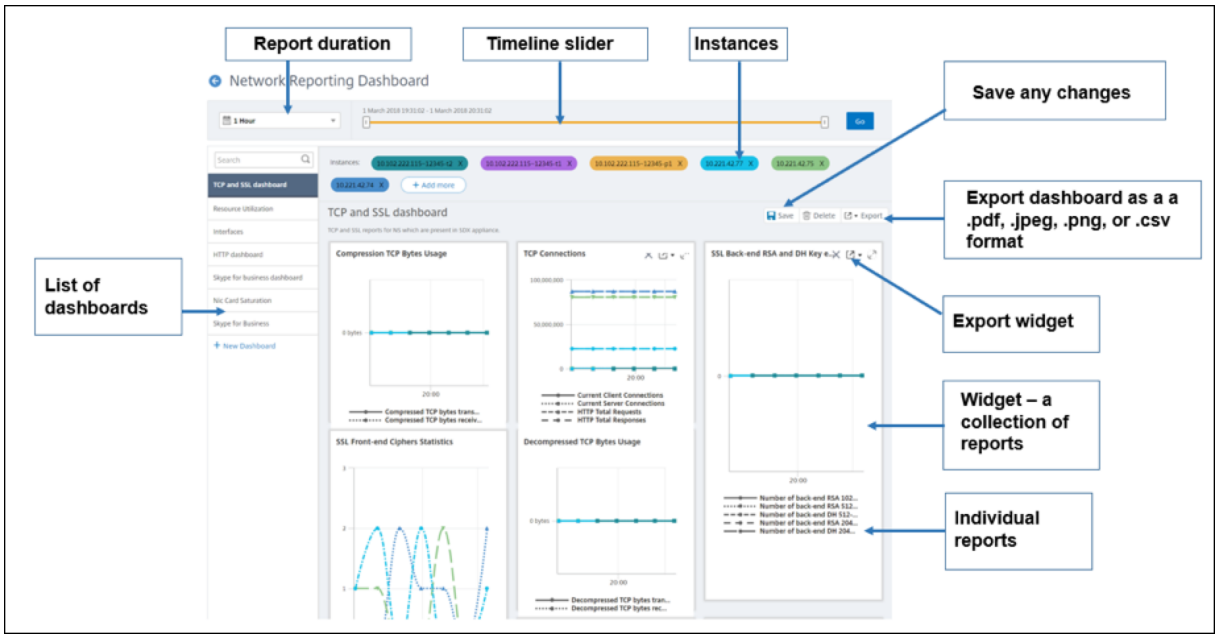
para entidades como los servidores virtuales y las interfaces de red. La familia de instancias comprende instancias de NetScaler ADC y SD-WAN. Los servidores virtuales para los que puede generar informes son los siguientes:

- Servidores, servicios y grupos de servicios de equilibrio de carga
- Servidores de conmutación de contenido
- Servidores de redirección de caché
- Equilibrio de carga de servicio global (GSLB)
- Autenticación
- Citrix Gateway

El panel de informes de red de NetScaler ADM es altamente personalizable. Ahora puede crear varios paneles para varias instancias, servidores virtuales y otras entidades.

## Panel de informes de red

La siguiente imagen muestra las distintas funciones del panel de control:




- El panel del lado izquierdo muestra todos los paneles personalizados creados en NetScaler ADM. Puede hacer clic en uno de ellos para ver los diversos informes de los que está compuesto el panel. Por ejemplo, un panel TCP y SSL contiene varios informes relacionados con protocolos TCP y SSL.
- Puede personalizar cada panel con varios widgets para mostrar varios informes. Un widget representa un informe en el panel, es decir, una colección de informes más relacionados. Por ejemplo, un informe de uso de bytes TCP de compresión contiene informes de bytes TCP comprimidos transferidos y recibidos por segundo.

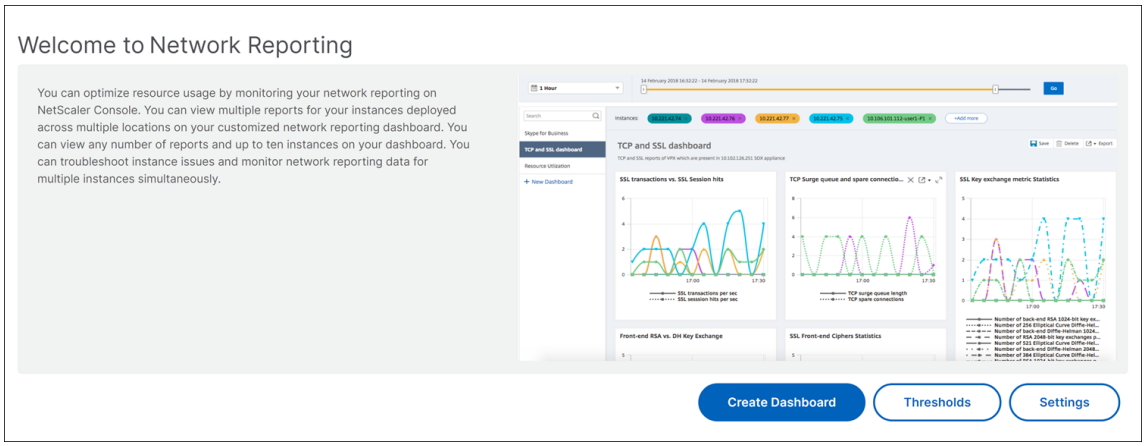
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Puede mostrar informes de una hora, un día, una semana o un mes. Además, ahora puede usar la opción de control deslizante de la línea de tiempo para personalizar la duración de los informes que se generan en NetScaler ADM.
- Para eliminar un informe, haga clic en la "X". También puede exportar el informe como formato.pdf,.jpeg,.png o.csv al sistema. También puede programar una hora y una periodicidad de cuándo se debe generar el informe. También puede configurar una lista de distribución de correo electrónico a la que se deben enviar los informes.
- La sección Instancias en la parte superior del panel muestra las direcciones IP de todas las instancias para las que se genera el informe.
- Puede eliminar instancias haciendo clic en la "X"o agregar más instancias a los informes. Sin embargo, actualmente NetScaler ADM le permite ver informes de 10 instancias.
- También puede exportar todo el panel de control en formato.pdf,.jpeg, png o.csv a su sistema. Se deben guardar todos los cambios realizados en el panel de control. Haga clic en Guardar para guardar los cambios.

En la siguiente sección se explican en detalle las tareas para crear un panel, generar informes y exportar informes.

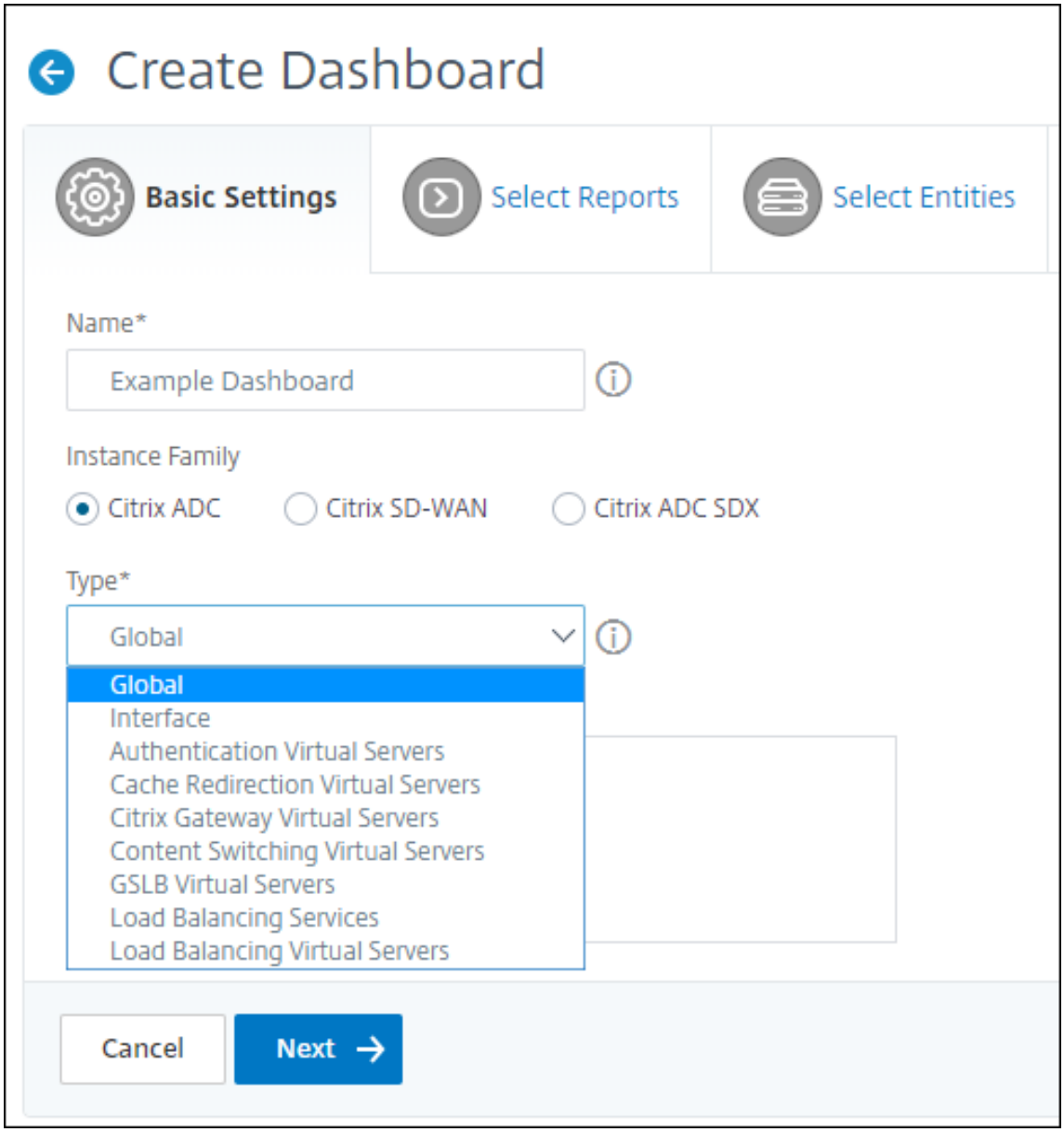
**Para ver o crear un tablero de mandos:**

1. En NetScaler ADM, vaya a **Redes** > **Informes de red**.




2. Para ver los paneles existentes, haga clic en **Ver panel**. Se abre la página **Panel** de informes de red, donde puede ver todos los paneles y widgets de informes.
3. Para crear un panel, haga clic en **Nuevo panel**. Se abre la página Crear panel.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. En la ficha Configuración básica, introduzca los siguientes detalles:

   a) **Nombre**. Escriba el nombre del panel de control.

   b) **Familia**de instancias . Seleccione el tipo de instancia: Citrix ADC, Citrix SD-WAN o Citrix ADC SDX.

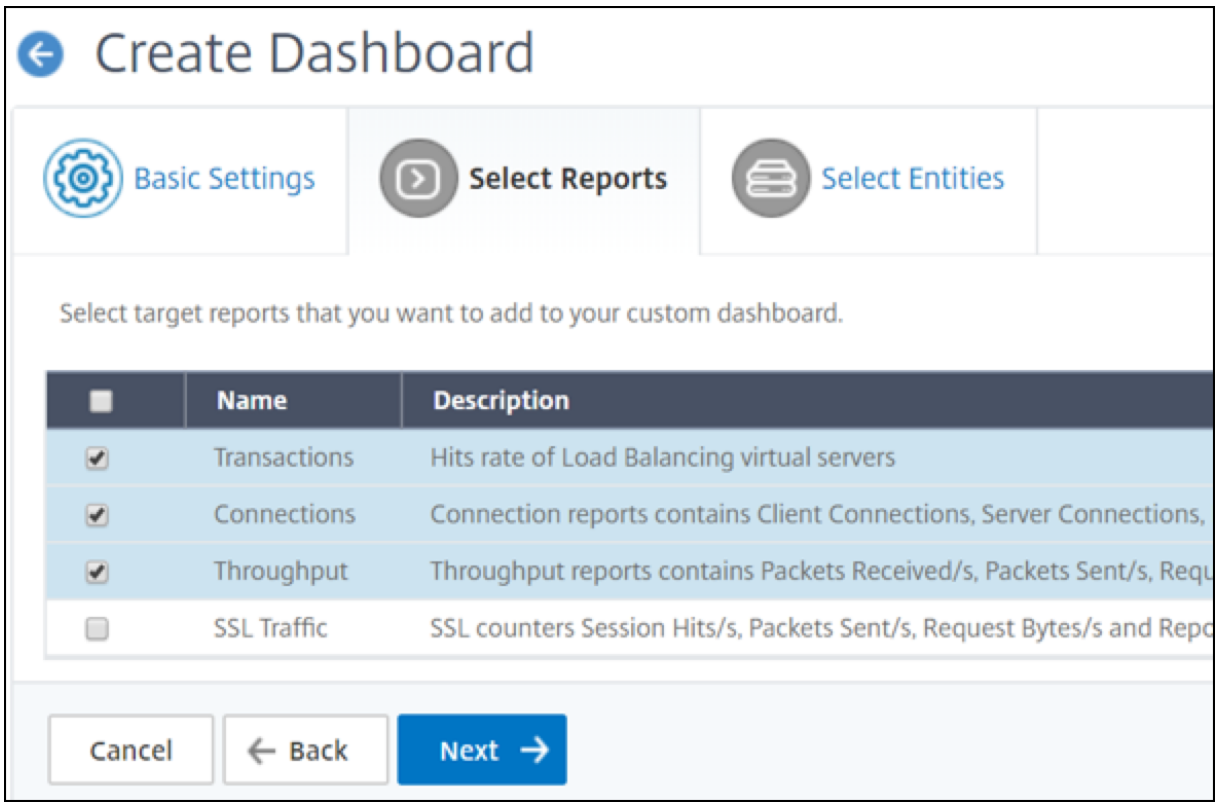
   c) **Escriba**. Seleccione el tipo de entidad para el que quiere generar informes. En este ejemplo, seleccione servidores virtuales de equilibrio de carga.

   d) **Descripción**. Escriba una descripción significativa para el panel de control.

5. Haga clic en **Siguiente**. Aparecen todos los informes compatibles para la instancia y la entidad específica.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

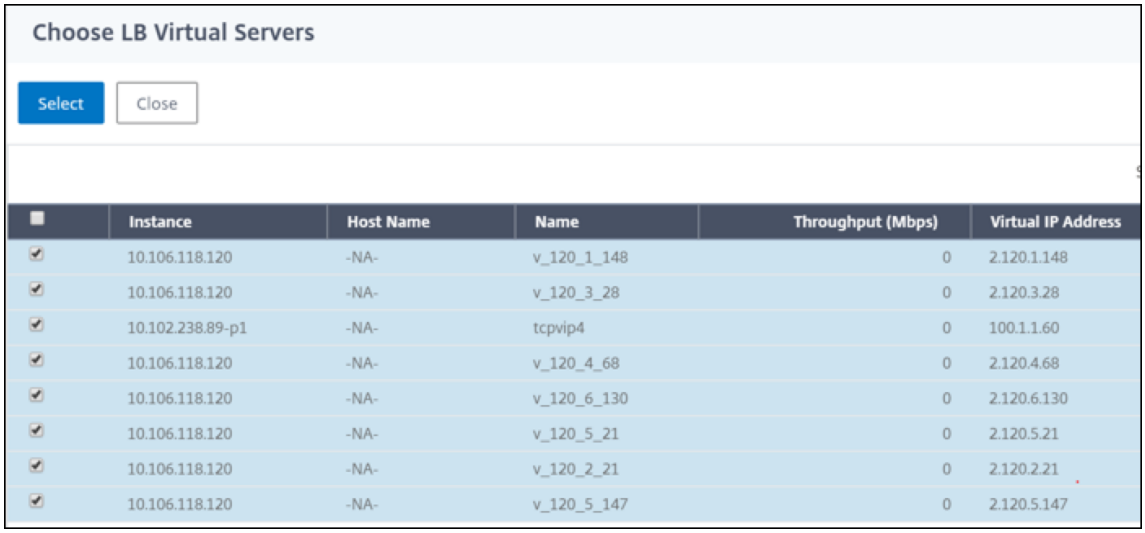
6. En la ficha **Seleccionar informes**, seleccione los informes necesarios. En este ejemplo, puede seleccionar las transacciones, las conexiones y el rendimiento. Haga clic en **Siguiente**.




1. En la ficha **Seleccionar entidades**, haga clic en **Agregar**.

   Aparecerá una ventana con la lista de entidades en función del tipo de entidad seleccionado en la ficha **Configuración básica**. En este ejemplo, aparece la ventana **Choose LB Virtual Servers**.

2. Seleccione las entidades que quiere supervisar.




3. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Se crea el panel de control y muestra todos los informes que ha seleccionado.

> **Nota**
>
> Actualmente, los cambios que realice en leyendas o filtros no se pueden guardar.

## Exportación de informes de red

Si bien puede exportar informes de widgets en los formatos.pdf, png,.jpeg o.csv, puede exportar todos los paneles solo en los formatos.pdf,.jpeg o png.

> **Nota**
>
> No puede exportar informes en NetScaler ADM si tiene permisos de solo lectura. Necesita un permiso de edición para poder crear un archivo en NetScaler ADM y poder exportarlo.

**Para exportar informes de paneles:**

1. Vaya a **Redes** > **Informes de red**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, haga clic en **Panel 1**.
4. Haga clic en el botón de exportación situado en la esquina superior derecha de la página.
5. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.

   En la página **Exportar**, puede realizar una de las siguientes acciones:
6. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
7. Seleccione la ficha **Planificar exportación**. Para programar el informe diariamente, semanalmente o mensualmente y enviar el informe a través de un correo electrónico o un mensaje de demora.

   Puede programar una exportación de la página del panel de control de **Network Reporting** de forma recurrente. Por ejemplo, puede establecer una opción para generar un informe de panel cada semana durante la hora anterior en un momento determinado. A continuación, el informe se genera cada semana y muestra el estado del panel de control. El informe anula la marca de fecha y hora, si lo establece el usuario.

> **Nota**
>
> - si selecciona Periodicidad semanal, asegúrese de seleccionar los días de la semana en los que quiere que se programe el informe.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> - Si selecciona Periodicidad mensual, asegúrese de especificar todos los días que quiere programar el informe separados por comas.

Al programar informes de red, puede personalizar el encabezado del informe escribiendo una cadena de texto en el campo **Asunto**. El informe creado a la hora programada tiene esta cadena como nombre.

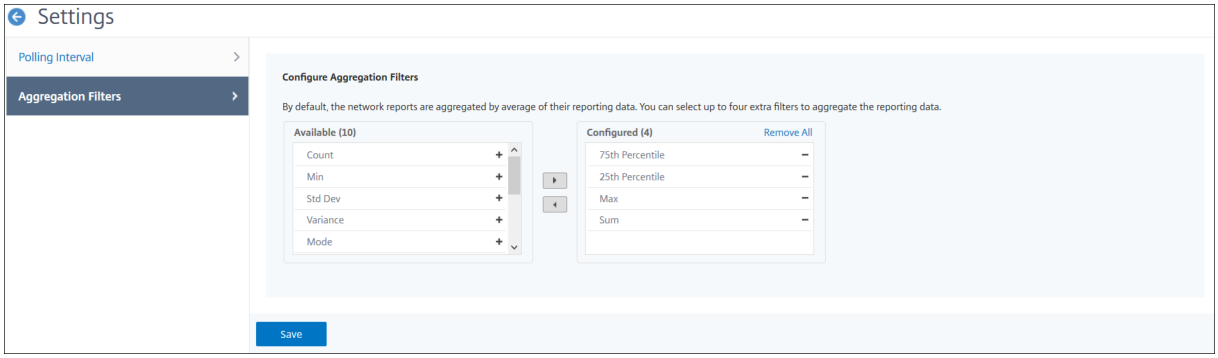
Por ejemplo, para los informes de red que se originan en un servidor virtual concreto, puede escribir el asunto "authentication-reports-10.106.118.120", donde 10.106.118.120 es la dirección IP del servidor virtual supervisado.

> **Nota:**
>
> Actualmente, esta opción solo está disponible cuando se programa la exportación de informes. No puede agregar un encabezado al informe cuando los exporta al instante.

## Ver datos de informes de red mediante la aplicación de agregaciones

Puede aplicar agregaciones a los datos de rendimiento de la red y ver el rendimiento de las aplicaciones en el panel. También puede exportar los resultados en función de sus necesidades. Al usar estas agregaciones aplicadas a los datos, puede analizar y asegurarse de que todos los recursos se utilizan de manera óptima. Vaya a **Red > Informes de red** y seleccione la duración de 1 día o más para **ver la opción Ver por**.

En los datos medios existentes, puede aplicar agregaciones seleccionando la opción de la lista **Ver por**. Cuando se aplica la agregación, los datos se actualizan para cada métrica en el tablero de mandos. Haga clic en **Configuración** y seleccione **Filtros de agregación**.




Las siguientes son las agregaciones que puede agregar:

- Recuento
- Máx.
- Mín.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

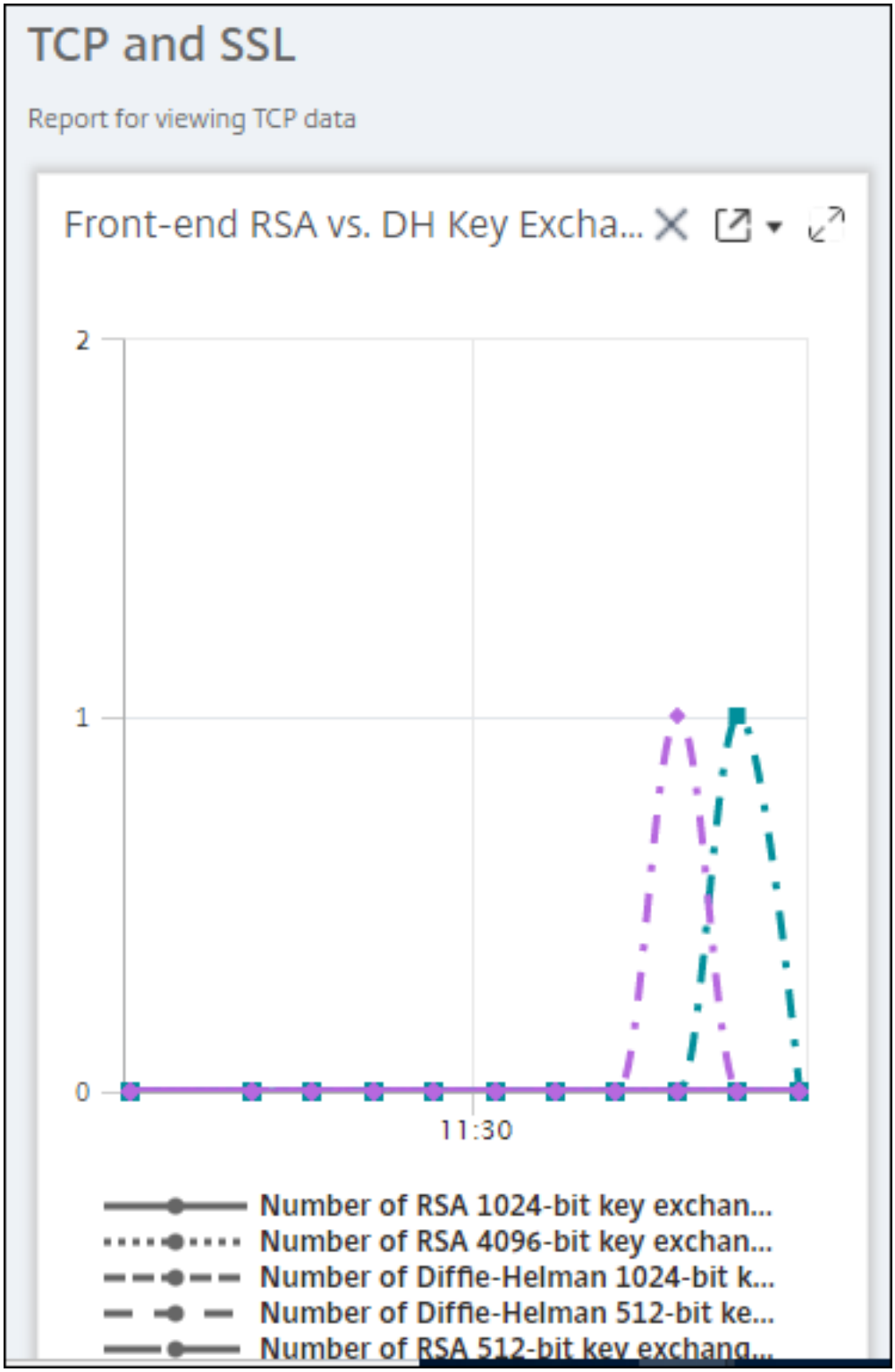
- Suma
- Desarrollo de Std
- Desviación
- Modo
- Mediana
- Percentil 25
- Percentil 75
- Percentil 95
- Percentil 99
- Primera
- Última

Puede agregar hasta 4 opciones de agregación al panel. Después de agregar las opciones de agregación, NetScaler ADM tarda aproximadamente 1 hora en generar informes para las opciones de agregación seleccionadas.

**Para exportar informes de widgets:**

1. Vaya a **Redes** > **Informes de red.**
2. Haga clic en **Ver paneles** para ver todos los paneles que ha creado.
3. En el panel izquierdo, haga clic en un panel. En este ejemplo, también haga clic en **Skype Empresarial**.
4. Seleccione un widget. Por ejemplo, seleccione **Load Balancing Virtual Server Transactions**.
5. Haga clic en el botón de exportación en la esquina superior derecha de la página
6. En la ficha **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Cómo administrar Umbrales para Informes de Red en NetScaler ADM

Para supervisar el estado de una instancia de NetScaler ADC, puede establecer umbrales en los contadores y recibir notificaciones cuando se supera un umbral. En NetScaler ADM, puede configurar los umbrales y verlos, modificarlos y eliminarlos.

Por ejemplo, puede recibir una notificación por correo electrónico cuando el contador de conexiones de un servidor virtual de conmutación de contenido alcance un valor especificado. Puede definir un umbral para un tipo de instancia específico. También puede elegir los informes que quiere generar para métricas específicas de contador de la instancia elegida.

Cuando el valor de un contador supera o cae por debajo (según lo especificado por la regla) del valor umbral, se genera un evento de la gravedad especificada para indicar un problema relacionado con el rendimiento. Cuando el valor del contador vuelve a un valor que considera normal, el evento se borra. Estos eventos se pueden ver navegando a **Redes** > **Eventos** > **Informes** . En la página Informes, puede hacer clic en el anillo **Eventos por gravedad** para ver los eventos según su gravedad.

También puede asociar una acción a un umbral, como enviar un mensaje de correo electrónico o SMS cuando se incumple el umbral.

**Para crear un umbral:**

1. En Citrix ADM, vaya a **Redes** > **Informes de red** > **Umbrales** . En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbral**, especifique los siguientes detalles:
   - **Nombre**. Nombre del umbral.
   - **Tipo de instancia**. Elija Citrix ADC o Citrix SD-WAN WO.
   - **Nombre del informe**. Nombre del informe de rendimiento que proporciona información sobre este umbral.
3. También puede establecer reglas para especificar cuándo se va a generar o borrar un evento. Puede especificar los siguientes detalles en la sección **Configurar regla** :
   - **Métrico**. Seleccione la métrica para la que quiere establecer un umbral.
   - **Comparador**. Seleccione un comparador para comprobar si el valor monitorizado es mayor o igual o menor que el valor umbral.
   - **Valor de umbral**. Escriba el valor para el que se calcula la gravedad del evento. Por ejemplo, puede que quiera generar un evento con una gravedad de evento crítica si el valor supervisado para las conexiones de clientes actuales alcanza el 80 por ciento. En este caso, escriba 80 como valor de umbral. Para ver los eventos de «gravedad crítica», vaya a **Redes** > **Eventos** > **Informes** . En la página Informes, puede hacer clic en el anillo **Eventos por gravedad** para ver los eventos según su gravedad.
   - **Valor claro**. Escriba el valor que indica cuándo borrar el valor. Por ejemplo, puede que quiera borrar el umbral de conexiones de clientes actuales cuando el valor supervisado

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

alcance el 50 por ciento. En este caso, escriba 50 como valor de borrado.

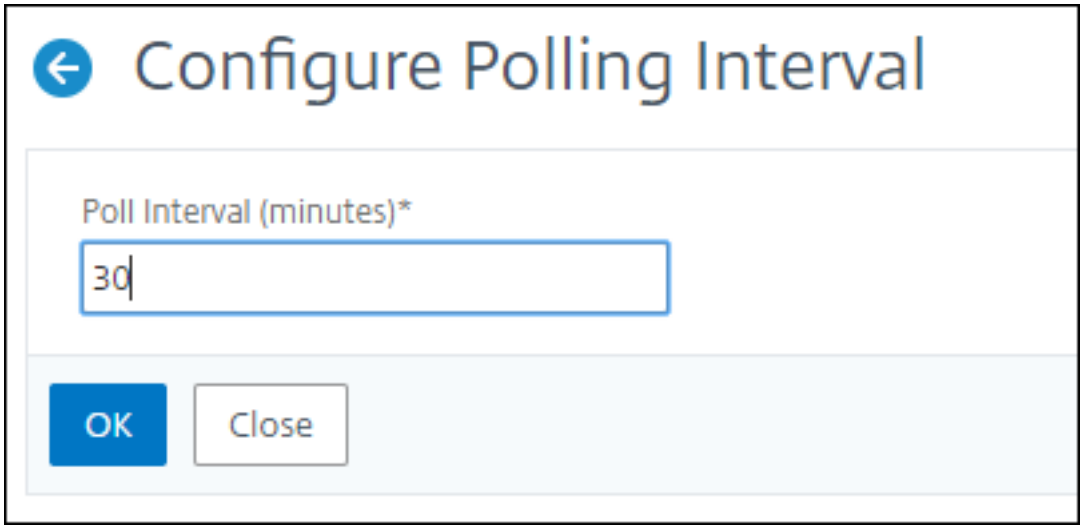
- **Gravedad del evento** Seleccione el nivel de seguridad que quiera establecer para el valor del umbral.

4. Elija la dirección IP de la instancia o instancias para las que quiere establecer el umbral.
5. También puede agregar un **mensaje de evento**. Escriba el mensaje que quiera que aparezca cuando se alcance el umbral. NetScaler ADM agrega el valor supervisado y el valor umbral a este mensaje.
6. Seleccione**Activar**para habilitar el umbral para generar alarmas.
7. Opcionalmente, puede configurar **Acciones** como notificaciones de correo electrónico o Slack, o ambas notificaciones de correo electrónico y Slack.
8. Haga clic en **Crear**.

### Establecer el intervalo de sondeo de rendimiento para los informes

De forma predeterminada, cada 5 minutos, las llamadas NITRO recopilan datos de rendimiento para la generación de informes de red. ADM recupera estadísticas de instancia como información de contadores y las agrega en función de por minuto, por hora, por día o por semana. Puede ver estos datos agregados en informes predefinidos.

Para establecer el intervalo de sondeo de rendimiento, vaya a **Redes** > **Informes de red** y haga clic en **Configurar intervalo de sondeo** . El intervalo de sondeo no puede ser inferior a 5 minutos ni superior a 60 minutos.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Configuración de la Prune de Network Reporting

Puede configurar el intervalo de depuración de los datos de informes de red en NetScaler ADM. Esta configuración limita la cantidad de datos de informes de red que se almacenan en la base de datos del servidor NetScaler ADM. De forma predeterminada, la poda ocurre cada 24 horas (a las 01.00 horas) para la red que informa de datos históricos.

> **Nota**
>
> El valor que puede especificar no puede superar los 90 días ni ser inferior a 1 día.

## Utilice los registros de auditoría de ADM para administrar y supervisar su infraestructura

January 30, 2024

Puede utilizar el servicio Citrix ADM para realizar un seguimiento de todos los eventos de ADM y syslog generados en las instancias de ADC administradas por ADM. Estos mensajes pueden ayudarlo a administrar y supervisar su infraestructura. Sin embargo, los mensajes de registro son una excelente fuente de información solo si los revisas, y ADM simplifica la forma de revisar los mensajes de registro.

Puede usar filtros para buscar mensajes de registro de auditoría y syslog de ADM. Los filtros ayudan a acotar los resultados y a encontrar exactamente lo que busca en tiempo real. La Ayuda de búsqueda integrada le guía para filtrar los registros. Otra forma de ver los mensajes de registro es exportarlos en formato PDF, CSV, PNG y JPEG. Puede programar la exportación de estos informes a direcciones de correo electrónico especificadas en distintos intervalos.

Puede revisar los siguientes tipos de mensajes de registro desde la GUI de ADM:

- Registros de auditoría relacionados con instancias de ADC
- Registros de auditoría relacionados con ADM
- Registros de auditoría de aplicaciones

### Registros de auditoría relacionados con instancias de ADC

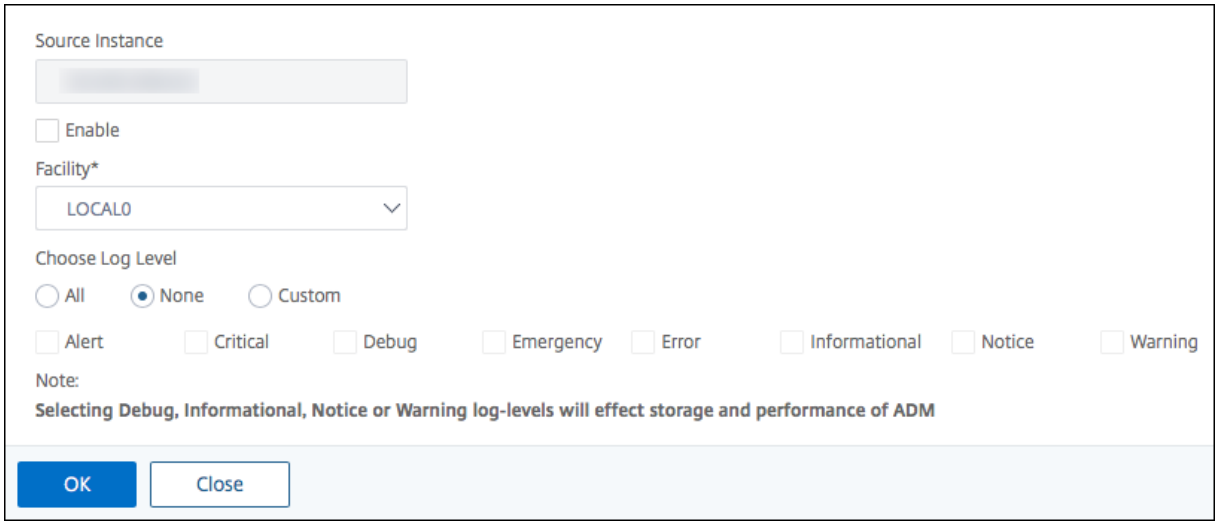
Antes de poder ver los mensajes de syslog relacionados con la instancia de ADC desde ADM, configure el servicio Citrix ADM como servidor de syslog para su instancia de Citrix ADC. Una vez completada la configuración, todos los mensajes syslog se redirigen desde la instancia a ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Configurar el servicio ADM como servidor syslog

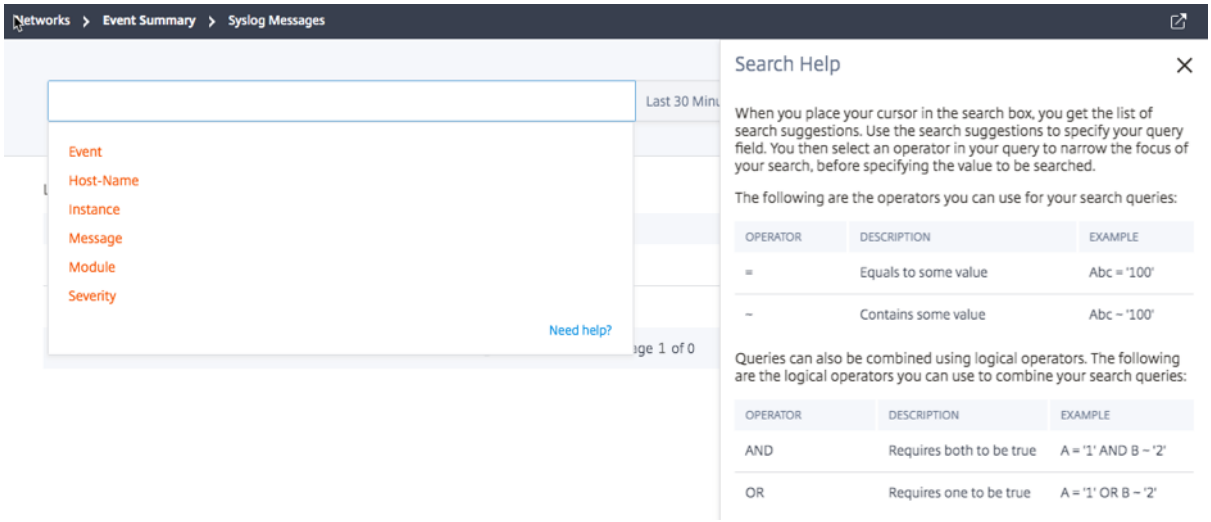
Siga estos pasos para configurar ADM como el servidor syslog:

1. Desde la GUI de ADM, vaya a **Redes > Instancias**.
2. Seleccione la instancia de Citrix ADC desde la que quiere que se recopilen y muestren los mensajes syslog en Citrix ADM.
3. En la lista **Seleccionar acción**, seleccione **Configurar Syslog**.
4. Haga clic en **Activar**.
5. En la lista desplegable de **instalaciones**, seleccione una instalación local o a nivel de usuario.
6. Seleccione el nivel de registro requerido para los mensajes de syslog.
7. Haga clic en **Aceptar**.




Estos pasos configuran todos los comandos syslog en la instancia de Citrix ADC y Citrix ADM comienza a recibir los mensajes syslog. Puede ver los mensajes navegando a **Redes > Eventos > Mensajes de Syslog**. Haga clic en **¿Necesita ayuda?** para abrir la ayuda de búsqueda integrada. Para obtener más información, consulte Ver y exportar mensajes de syslog.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.

A continuación, haga clic en **Exportar ahora** o **Planificar exportación**. Para obtener más información, consulte Ver y exportar mensajes de syslog.

## Registros de auditoría relacionados con ADM

Según reglas preconfiguradas, ADM genera mensajes de registro de auditoría para todos los eventos en, lo que le ayuda a supervisar el estado de la infraestructura. Para ver todos los mensajes del registro de auditoría presentes en el ADM, vaya a **Sistema > Mensajes del registro de auditoría**.

Para exportar los mensajes de registro, haga clic en el icono de flecha de la esquina superior derecha.

## Registros de auditoría relacionados con aplicaciones

Puede ver los mensajes de registro de auditoría para todas las aplicaciones ADM o para una aplicación específica.

- Para ver todos los mensajes de registro de auditoría de todas las aplicaciones presentes en el ADM, vaya a **Redes-> Funciones de red >Auditoría**.
- Para ver los mensajes de registro de auditoría de cualquier aplicación específica en el ADM, vaya a **Aplicación > Panel > Haga doble clic en el servidor virtual > Registro de auditoría**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Análisis

January 30, 2024

La función Citrix ADM Analytics proporciona una forma fácil y escalable de analizar varios datos de Citrix ADC para analizar y mejorar el rendimiento de las aplicaciones. Puede utilizar una o varias funciones de análisis simultáneamente en NetScaler ADM.

En la siguiente tabla se describen varias funciones de análisis compatibles con Citrix ADM:

| Función de análisis | Descripción |
| --- | --- |
| Información web | Web Insight permite la visibilidad de las aplicaciones web empresariales y permite supervisar todas las aplicaciones web en Citrix ADC. Como administrador, puede ver la supervisión integrada y en tiempo real de las aplicaciones. |
| HDX Insight | HDX Insight proporciona visibilidad de extremo a extremo para el tráfico ICA que pasa a través de NetScaler ADC. HDX Insight le permite ver las métricas de latencia de los clientes y de la red en tiempo real, los informes históricos y los datos de rendimiento de principio a fin y solucionar problemas de rendimiento. |
| Gateway Insight | Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en Citrix Gateway. |
| Security Insight | Security Insight proporciona una solución de panel único para ayudarle a evaluar el estado de seguridad de su aplicación y a tomar medidas correctivas para proteger sus aplicaciones. |
| Insight SSL | SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y le permite supervisar todas las aplicaciones web seguras de Citrix ADC. Como administrador, puede ver la supervisión integrada, en tiempo real e histórica, de las transacciones web seguras. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Función de análisis | Descripción |
| --- | --- |
| Información TCP | TCP Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión que se utilizan en las instancias de Citrix ADC para evitar la congestión de la red en la transmisión de datos. |
| Video Insight | La función Video Insight proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización de vídeo utilizadas por los dispositivos Citrix ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa. |
| WAN Insight | El análisis de WAN Insight permite a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre los dispositivos de optimización WAN del centro de datos y las sucursales. WAN Insight también proporciona visibilidad en clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz. |

## Requisitos de licencia

January 30, 2024

La siguiente tabla describe los requisitos de licencia de las instancias de NetScaler ADC para ver los distintos informes de análisis en NetScaler ADM:

| Funciones de NetScaler ADM Analytics | Requisito de licencia de NetScaler ADC |
| --- | --- |
| Información web | El informe Web Insight sobre NetScaler ADM es compatible con todas las ediciones de licencias de NetScaler ADC (Standard/Advanced/Premium). |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Funciones de NetScaler ADM Analytics | Requisito de licencia de NetScaler ADC |
|---|---|
| HDX Insight | El informe HDX Insight en NetScaler ADM es compatible con cualquiera de las siguientes licencias de NetScaler ADC: Advanced Edition (para informes de menos de 1 hora) o Premium Edition (para informes ilimitados). **Nota**: La edición de licencia estándar no es compatible. |
| Security Insight | El informe Security Insight en NetScaler ADM es compatible con las licencias Premium Edition o Advanced Edition con App Firewall. **Nota**: La edición de licencia estándar y la licencia de Firewall de aplicaciones independientes no son compatibles. |
| Insight SSL | El informe SSL Insight sobre NetScaler ADM es compatible con todas las ediciones de licencias de NetScaler ADC (Standard/Advanced/Premium). |
| Gateway Insight | El informe Gateway Insight sobre NetScaler ADM es compatible con cualquiera de las siguientes licencias de NetScaler ADC: Advanced Edition (para informes de menos de 1 hora) o Premium Edition (para informes ilimitados). **Nota**: La edición de licencia estándar no es compatible. |
| Información TCP | El informe TCP Insight es compatible con todas las ediciones de licencias de NetScaler ADC (Standard/Advanced/Premium). |
| Video Insight | El informe Video Insight sobre NetScaler ADM es compatible con NetScaler ADC Premium (VPX-T 1000 series, VPX-T) edición. |
| WAN Insight | El informe WAN Insight sobre NetScaler ADM es compatible con Citrix SD-WAN WO Edition (WAN Optimization Edition). |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Visión general de Logstream

January 30, 2024

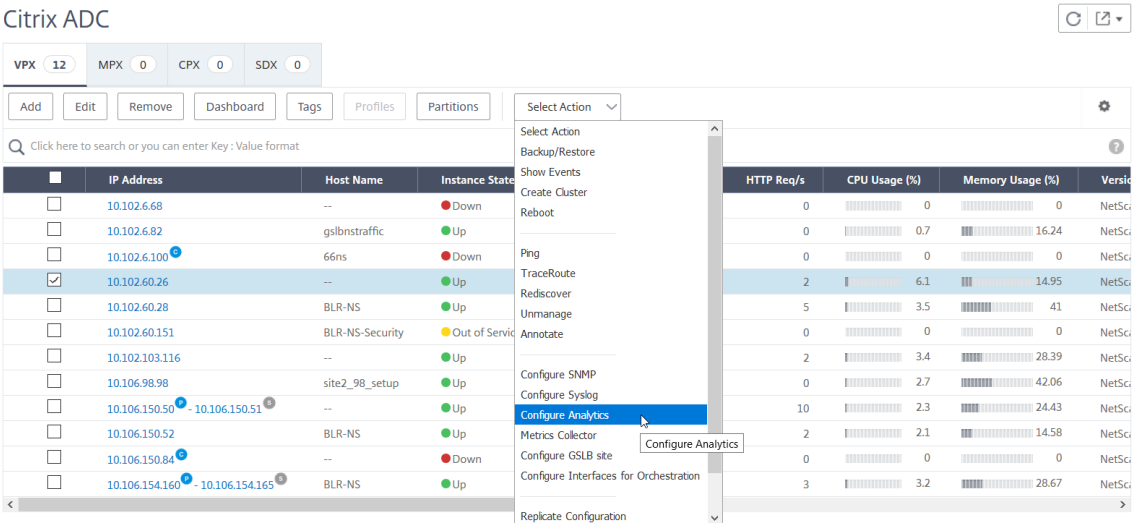
Las instancias Citrix ADC generan registros de AppFlow y son un punto central de control para todo el tráfico de aplicaciones en el centro de datos. IPFIX y Logstream son los protocolos que transportan estos registros de AppFlow desde las instancias de Citrix ADC a Citrix ADM. Para obtener más información, consulte AppFlow.

- IPFIX es un estándar abierto del Grupo de Trabajo de Ingeniería de Internet (IETF) definido en el RFC 5101. IPFIX utiliza el protocolo UDP que es un protocolo de transporte poco confiable utilizado para el flujo de datos en una dirección. Dado que IPFIX utiliza el protocolo UDP, la adhesión al estándar IPFIX permite procesar más recursos en Citrix ADM.
- Logstream es un protocolo propiedad de Citrix que se utiliza como uno de los modos de transporte para transferir eficientemente los datos de registro de análisis de las instancias de Citrix ADC a Citrix ADM. Logstream utiliza un protocolo TCP confiable y requiere menos recursos para procesar los datos.

Para Citrix ADC entre **11.1 Build 47.14 y 11.1 Build 62.8**, Logstream es el modo de transporte predeterminado para habilitar Web Insight (HTTP) e IPFIX es el único modo de transporte para habilitar otros conocimientos. Para la versión Citrix ADC desde la **12.0 hasta la versión más reciente**, puede seleccionar **Logstream** o **IPFIX** como modo de transporte.

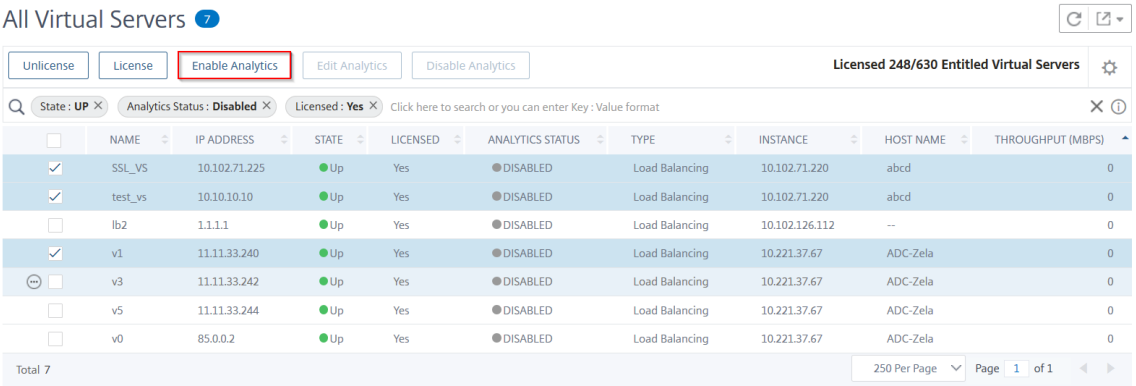
## Habilitar Logstream como modo de transporte

1. Vaya a **Redes > Instancias**y seleccione la instancia de ADC que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Seleccione los servidores virtuales y, a continuación, haga clic en **Habilitar análisis**.




4. En la ventana **Habilitar análisis**:

   a) Seleccione los tipos de información (Web Insight o Security Insight)

   b) Seleccione **Logstream** como modo de transporte

   > **Nota**
   >
   > Para Citrix ADC entre **11.1 Build 47.14 y 11.1 Build 62.8**, Logstream es el modo de transporte predeterminado para habilitar Web Insight (HTTP) e IPFIX es el único modo de transporte para habilitar otros conocimientos. Para la versión Citrix ADC desde la **12.0 hasta la versión más reciente**, puede seleccionar **Logstream** o **IPFIX** como modo de transporte.

   c) La expresión es verdadera por defecto

   d) Haga clic en **OK**.

   > **Nota**
   >
   > - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
   > - Para las particiones de administración, solo se admite **Web Insight**
   > - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error

En la siguiente tabla se describen las funciones de Citrix ADM que admiten Logstream como modo de transporte:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Función | IPFIX | Flujo de registro |
|---|---|---|
| Información web | • | • |
| Security Insight | • | • |
| Gateway Insight | • | • |
| HDX Insight | • | • |
| Insight SSL | No compatible | • |
| CR Insight | • | • |
| Reputación IP | • | • |
| AppFirewall | • | • |
| Medición del lado del | • | • |
| Syslog/Auditlog | • | • |

## Inhabilitar la recopilación de datos de URL

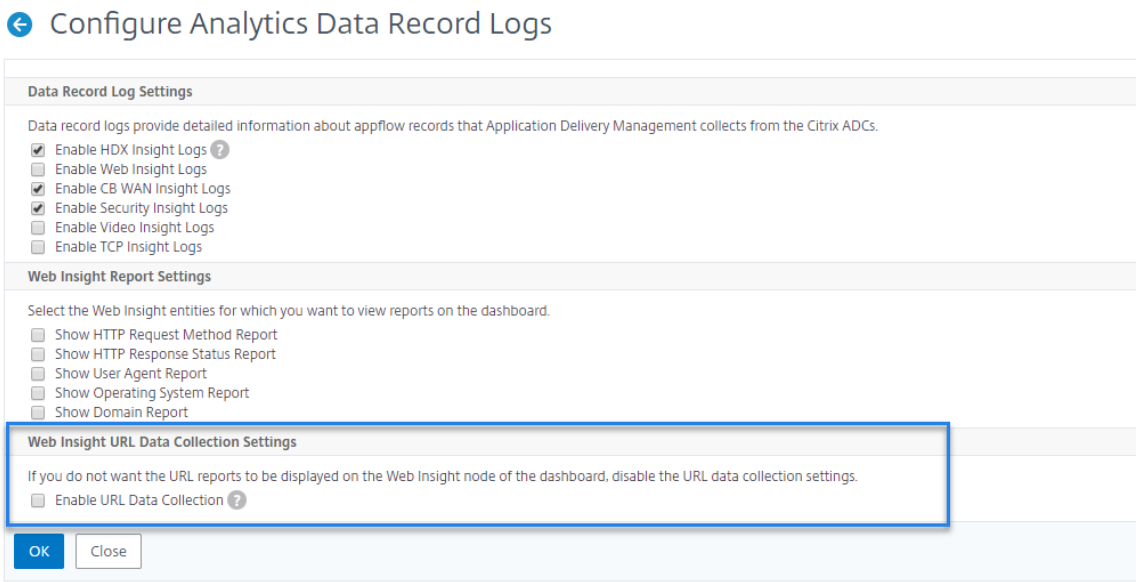
January 30, 2024

Puede inhabilitar la recopilación de datos de URL si no quiere que los informes de URL se muestren en el nodo Web Insight del panel de control de Citrix Application Delivery Management (ADM).

### Para inhabilitar la recopilación de datos de URL desde NetScaler ADM

1. En Citrix ADM, vaya a **Analytics** > **Parámetros** y, a continuación, haga clic en **Configurar registros de registros de datos** de análisis .
2. En la sección **Configuración de recopilación de datos de URL de Web Insight**, si la opción **Habilitar recopilación de datos de URL** está activada, desactive la casilla de verificación.
3. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Crear umbrales y alertas

January 30, 2024

Puede establecer umbrales y alertas para supervisar el estado de una instancia de Citrix ADC. Puede establecer umbrales en contadores y supervisar instancias y entidades en instancias administradas.

Cuando el valor de un contador supera el umbral, Citrix Application Delivery Management (ADM) genera un evento para indicar un problema relacionado con el rendimiento. Cuando el valor del contador coincide con el valor de borrado especificado en el umbral, el evento se borra, lo que significa que el umbral en particular ha vuelto a su estado normal.

También puede asociar una acción al umbral. Las acciones incluyen enviar una alerta, un correo electrónico o una notificación por SMS. Cuando se supera el umbral, Citrix ADM realiza automáticamente la acción que usted defina, como habilitar una alerta y enviar una notificación por correo electrónico o SMS.

**Para crear un umbral y una alerta mediante NetScaler ADM**:

1. En NetScaler ADM, vaya a **Analytics** > **Configuración** > **Umbrales**. En **Umbrales**, haga clic en **Agregar**.
2. En la página **Crear umbrales**, especifique los siguientes detalles:
   - **Nombre**: Nombre para configurar el umbral.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Tipo de tráfico**: Tipo de tráfico para el que desea configurar el umbral.
- **Entidad**: Categoría o tipo de recurso para el que quiere configurar el umbral.
- **Clave de referencia**: Valor generado automáticamente según el tipo de tráfico y la entidad seleccionados.
- **Duración**: Intervalo para el que quiere configurar el umbral.
- **Configurar regla**: Regla para la métrica para la que desea configurar el umbral.
- **Configuración de notificaciones** - Habilita el umbral y recibe notificaciones a través de varios canales como correo electrónico, demora o SMS cuando supere el umbral.

3. Haga clic en **Crear**.

Para HDX Insight, también puede establecer varios umbrales para los que se genere una alerta solo si se infringen todas las entidades del umbral configurado.

## Configurar umbrales adaptativos

January 31, 2024

La funcionalidad de umbral adaptativo establece el valor umbral para el número máximo de visitas en cada URL. Si el número máximo de visitas a una URL es mayor que el valor umbral establecido para la URL, se envía un mensaje syslog a un servidor syslog externo. El intervalo del valor umbral puede ser de días o semanas.

El valor umbral se calcula de la siguiente manera:

**Valor umbral = número máximo de aciertos * Multiplicador de umbral**

Donde:

- El número máximo de visitas es el número máximo de visitas en una URL.
- El multiplicador de umbral es un valor entero que se define (predeterminado: 2).

### Para crear un umbral adaptativo mediante Citrix ADM

1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Umbrales adaptativos** y, a continuación, haga clic en **Agregar**.
2. En la página **Umbrales adaptativos** , especifique los siguientes parámetros:
    - **Nombre: nombre** del umbral

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Entidad**: URL
- **Duración**: Duración del umbral (día o semana)
- **Multiplicador de umbrales**: Número entero definido por el usuario que se multiplica por el número máximo de visitas de la URL especificada para obtener el umbral adaptativo de la URL.

## Configurar la persistencia de la base de datos

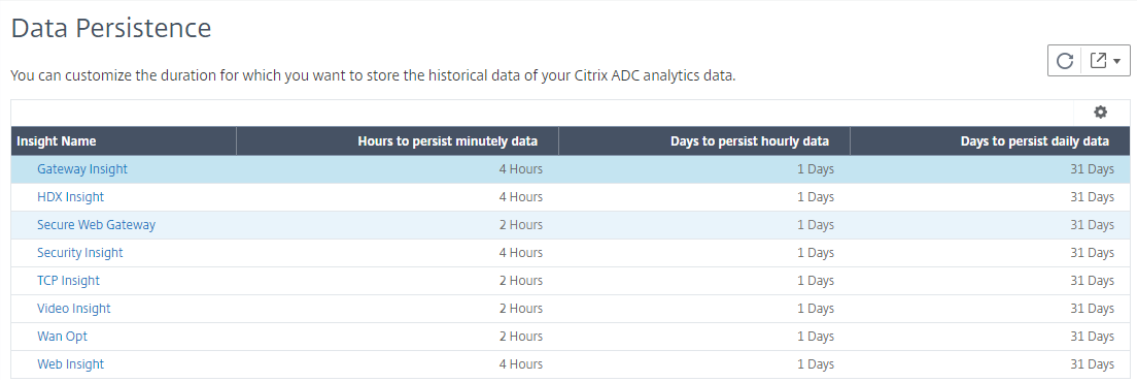
January 30, 2024

Configurar la persistencia de la base de datos en Citrix Application Delivery Management (ADM) le permite personalizar la duración durante la que desea almacenar los datos históricos de sus datos de análisis de Citrix ADC. Puede elegir los siguientes tipos de persistencia de bases de datos para los datos históricos de sus análisis:

- Horas para conservar los datos minuciosamente
- Días para conservar los datos horarios
- Días para conservar los datos por día

### Para configurar la persistencia de la base de datos

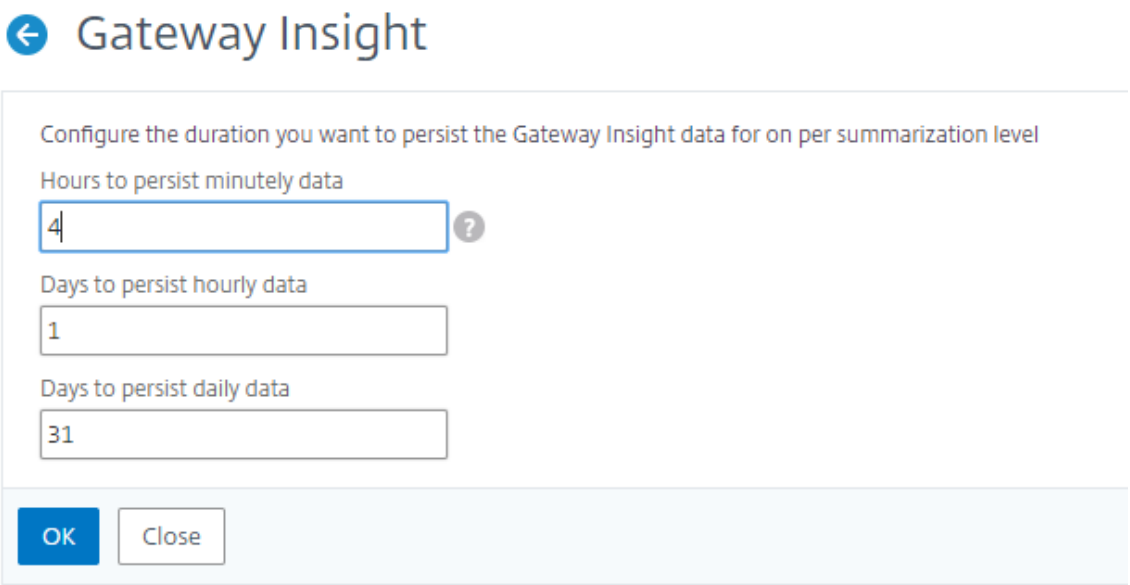
1. Vaya a > **Analytics** > **Configuración** > **Persistencia de base de datos**.
2. Haga clic en el tipo de información que quiere configurar la persistencia de la base de datos.




| Insight Name | Hours to persist minutely data | Days to persist hourly data | Days to persist daily data |
|---|---|---|---|
| Gateway Insight | 4 Hours | 1 Days | 31 Days |
| HDX Insight | 4 Hours | 1 Days | 31 Days |
| Secure Web Gateway | 2 Hours | 1 Days | 31 Days |
| Security Insight | 4 Hours | 1 Days | 31 Days |
| TCP Insight | 2 Hours | 1 Days | 31 Days |
| Video Insight | 2 Hours | 1 Days | 31 Days |
| Wan Opt | 2 Hours | 1 Days | 31 Days |
| Web Insight | 4 Hours | 1 Days | 31 Days |

3. Especifique el tiempo durante el que desea conservar los datos de Insight en Citrix ADM. Por ejemplo, para Gateway Insight, puede almacenar los datos históricos minuciosamente de los analíticos durante 2 horas, o los datos por hora durante 1 día.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Diagnósticos de autoservicio para Analytics

January 30, 2024

Citrix Application Delivery Management (ADM) realiza diagnósticos de autoservicio para identificar los problemas de licencia y configuración en las instancias administradas para las siguientes funciones de análisis:

- Información web
- HDX Insight
- Gateway Insight
- Security Insight
- Análisis de proxy de reenvío SSL

El diagnóstico de autoservicio se ejecuta cada 12 horas y genera un informe de diagnóstico si se encuentran problemas para cada una de las funciones de análisis especificadas. El informe de diagnóstico proporciona las fuentes de los problemas, los tipos de problemas y las acciones correctivas para resolverlos. El diagnóstico de autoservicio le ayuda a identificar y solucionar los problemas con mayor rapidez.

Por ejemplo, si la directiva de AppFlow no está vinculada a un servidor virtual o un servidor virtual no tiene licencia, NetScaler ADM no obtiene los datos deseados para la supervisión de Web Insight. El

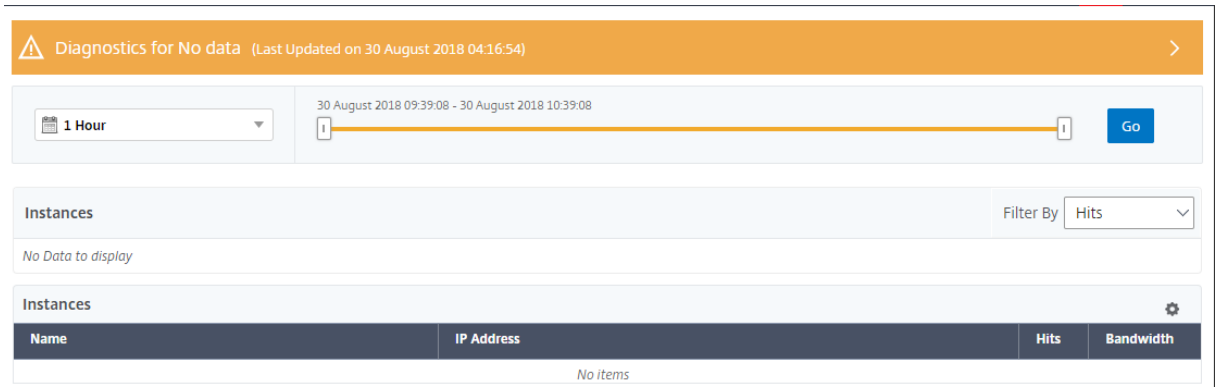
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

diagnóstico de autoservicio identifica los problemas y genera un informe de diagnóstico. Puede ver el informe de diagnóstico para comprobar los problemas y realizar las acciones correctivas.

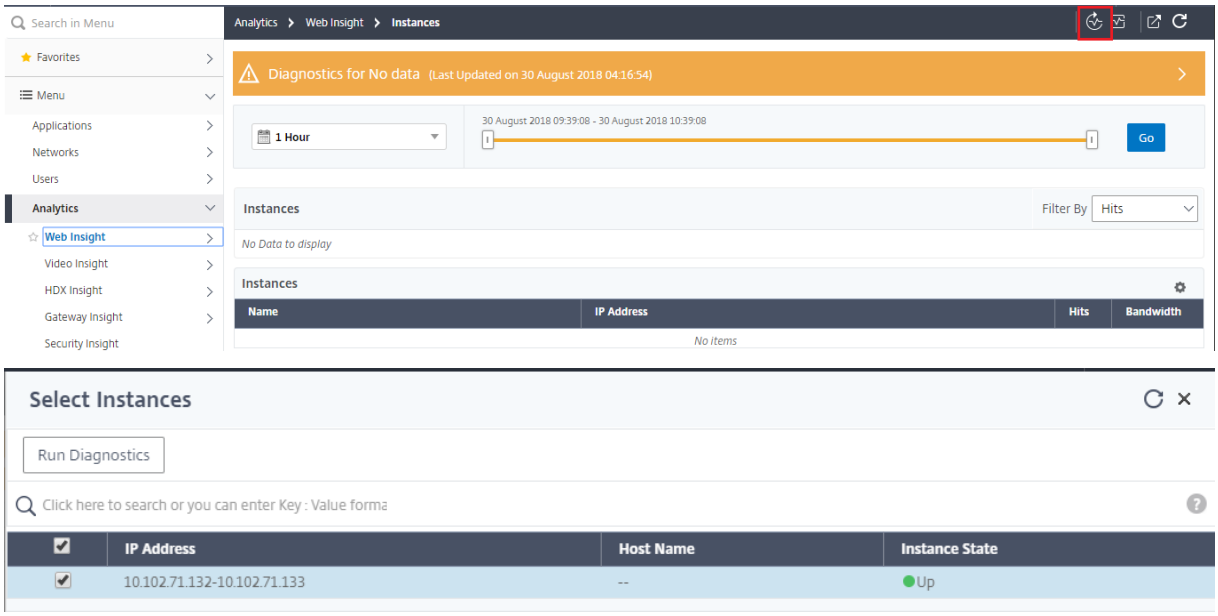
## Ver el informe de diagnóstico

Para ver los informes de diagnóstico de las funciones de análisis especificadas, debe ir al nodo de análisis correspondiente en el panel de control de NetScaler ADM.

Por ejemplo, para ver el informe de diagnóstico de Web Insight, vaya a **Analytics > Web Insight**. En la página web Insight, seleccione el icono **Mostrar diagnósticos**.




También puede ejecutar un diagnóstico instantáneo si quiere comprobar si hay problemas. Haga clic en **Ejecutar diagnósticos**. Seleccione las instancias y seleccione **Ejecutar diagnósticos**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

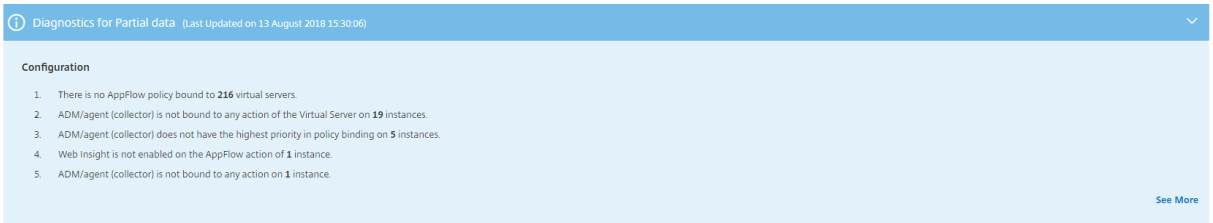
## Analizar el informe de diagnóstico

El diagnóstico de autoservicio muestra el informe de diagnóstico en un fondo naranja o azul según la gravedad de los problemas.

El informe de diagnóstico en el fondo naranja indica una criticidad mayor que el fondo azul.

Por ejemplo, hay cinco servidores virtuales configurados en su instancia de NetScaler ADC. Si no ha habilitado los parámetros de AppFlow en ningún servidor virtual, NetScaler ADM no recibirá el tráfico de Web Insight y Security Insight para su análisis. Los diagnósticos de autoservicio identifican los problemas de configuración como críticos. Verá los informes de diagnóstico en fondo naranja en Web Insight y en la función Security Insight.

Si ha habilitado AppFlow en uno de los servidores virtuales, NetScaler ADM recibe datos para análisis. Verá el informe de diagnóstico en fondo azul porque al menos un servidor virtual envía tráfico para su análisis.



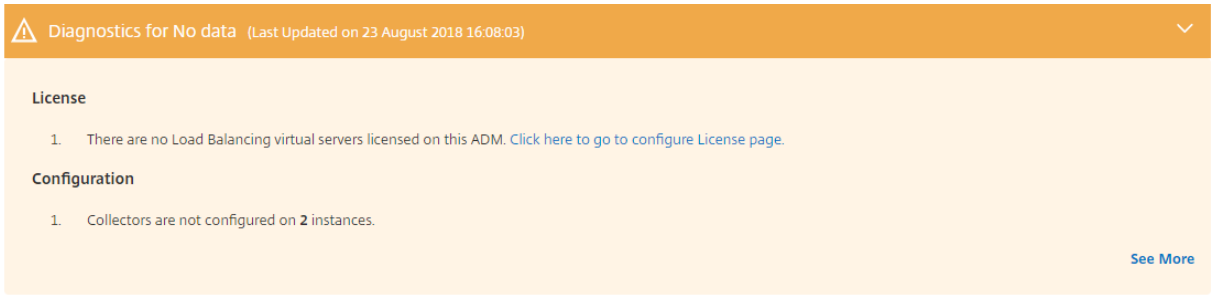

> **IMPORTANTE**: El diagnóstico de autoservicio no verifica el flujo de tráfico. Solo comprueba si existen problemas de licencia o configuración asociados con las funciones de análisis especificadas en las instancias administradas. A veces, no ve ningún dato de análisis porque no hay tráfico activo que fluya a través de los servidores virtuales.

El informe de diagnóstico tiene una página de resumen y una página de información detallada.

La página de resumen proporciona una descripción general de los tipos de problemas: licencia o configuración. La página puede contener hipervínculos que le dirijan a las páginas de configuración relevantes.

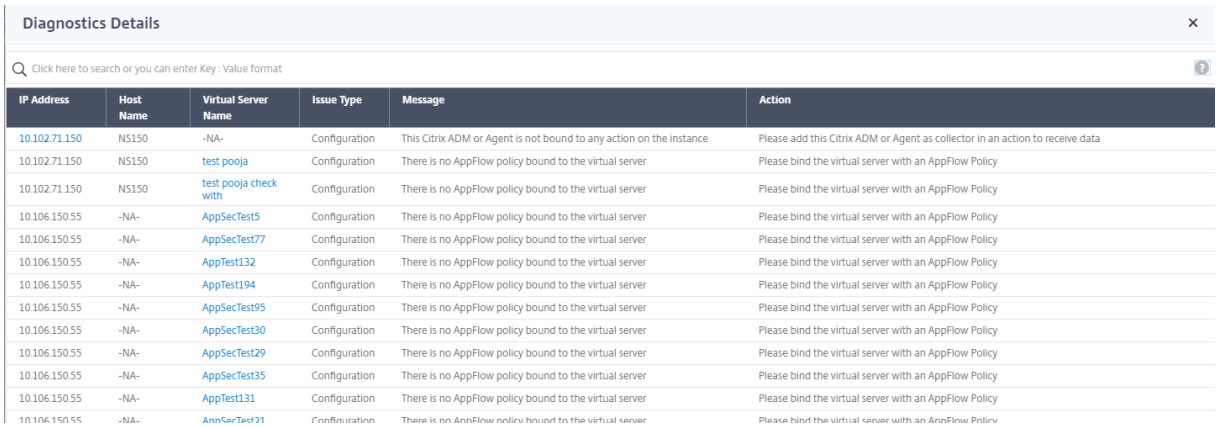
Por ejemplo, si no hay servidores virtuales de equilibrio de carga con licencia en NetScaler ADM, la página de resumen proporciona un hipervínculo que le dirige a la página **Licencias del sistema**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

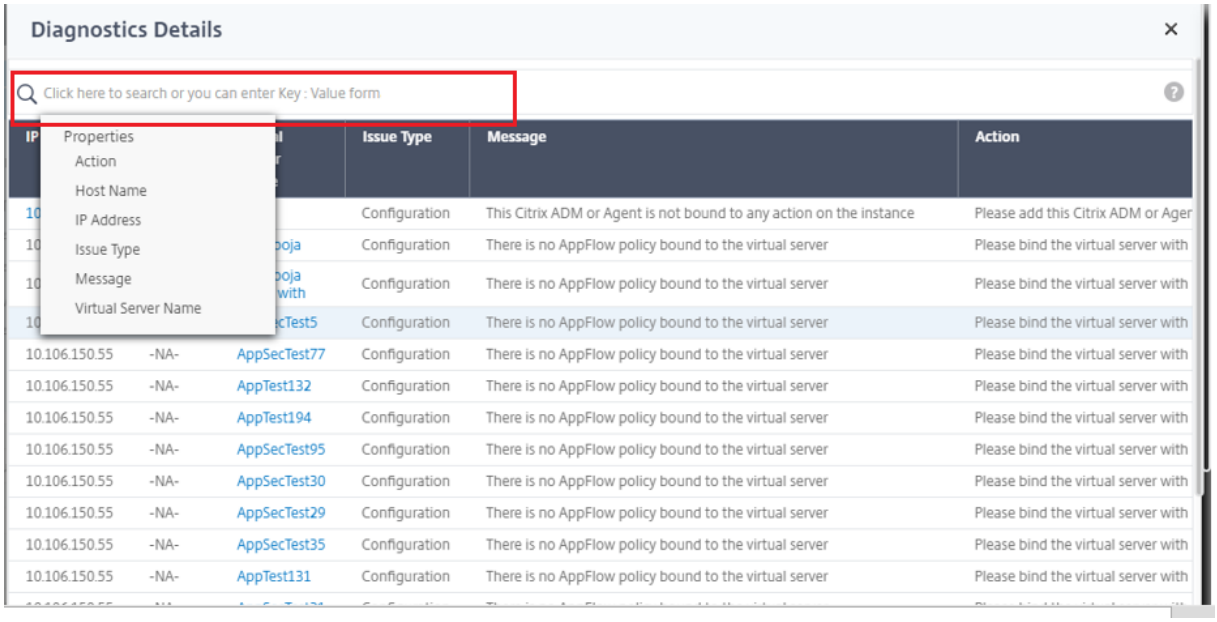



Para ver la información detallada sobre los problemas, haga clic en **Ver más** en la página de resumen.

La página de información detallada proporciona la información completa sobre los problemas y recomienda las acciones que debe realizar. Puede hacer clic en el hipervínculo en cada problema para configurar la instancia administrada o el servidor virtual.




También puede buscar los problemas en función de la acción, el nombre del host, la dirección IP y el tipo de problema, etc.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Después de resolver los problemas, debe ejecutar un diagnóstico instantáneo para generar el informe de diagnóstico más reciente.

## Información web

January 30, 2024

Web Insight permite a los administradores supervisar todas las aplicaciones web servidas por las instancias de Citrix ADC. Como administrador, puede obtener una supervisión integrada y en tiempo real de las aplicaciones de las instancias de Citrix ADC. Web Insight proporciona información crítica, como la latencia de la red del cliente y el tiempo de respuesta del servidor, lo que garantiza la supervisión y la mejora del rendimiento de las aplicaciones. Los datos utilizados para el análisis se capturan de cada transacción HTTP y HTTPS que procesa la instancia de Citrix ADC. Los datos de análisis le permiten analizar el rendimiento de las instancias, la aplicación, la URL, el cliente y el servidor de Citrix ADC en su entorno.

Los siguientes son algunos de los casos de uso en los que puede ver los datos con Web Insight:

- La lista de clientes que experimentan una latencia alta al acceder a una aplicación como SharePoint
- La aplicación principal que tuvo más visitas en una hora
- La lista de aplicaciones y URL a las que se accede desde los clientes
- El sistema operativo y el explorador utilizados por un cliente en particular
- Las aplicaciones o los servidores que envían la mayor cantidad de respuestas relacionadas con errores
- Problemas de accesibilidad con un cliente en particular
- Problemas de accesibilidad en pocas o todas las aplicaciones de un cliente en particular
- Pocas páginas de una aplicación son lentas desde un cliente en particular y desde un servidor back-end
- La aplicación es lenta cuando se accede desde un cliente particular y desde un servidor back-end

Puede habilitar Web Insight para un servidor virtual específico en una instancia seleccionada para supervisar el tráfico en la aplicación web. A continuación, la función Web Insight proporciona estadísticas para el servidor virtual en Citrix ADM.

Para habilitar Web Insight:

Si su NetScaler ADM es **13.0 compilación 41.x o posterior**:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Configurar análisis**.
3. En la página **Configurar análisis en servidores virtuales**, seleccione el servidor virtual y haga clic en **Habilitar Analytics**.
4. En la ventana **Habilitar análisis**:
   a) Seleccione **Web Insight**
   b) Seleccione **Logstream** como modo de transporte

      > **Nota**
      >
      > Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
      >
      > Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

   c) La expresión es verdadera por defecto
   d) Haga clic en **OK**.

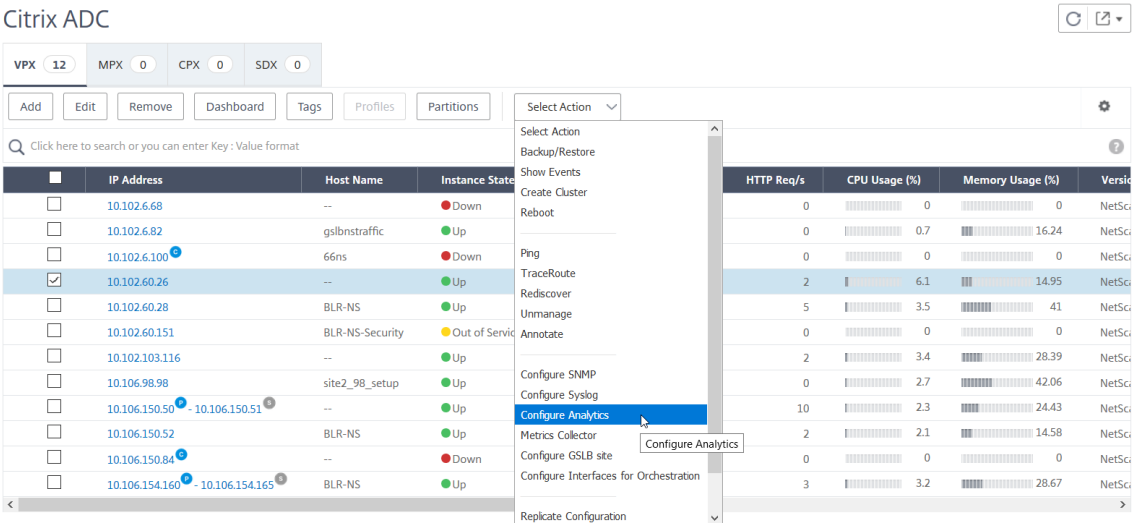
      > **Nota**
      >
      > - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
      > - Para las particiones de administración, solo se admite **Web Insight**
      > - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, Citrix ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

Si su NetScaler ADM es **13.0 compilación 36.27 o anterior**:

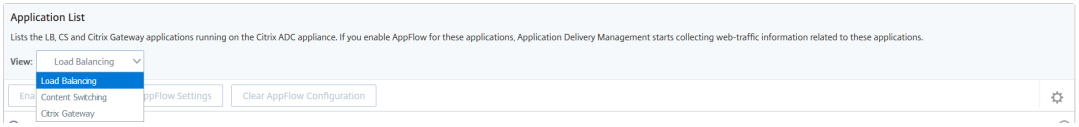
1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione la instancia de NetScaler ADC en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

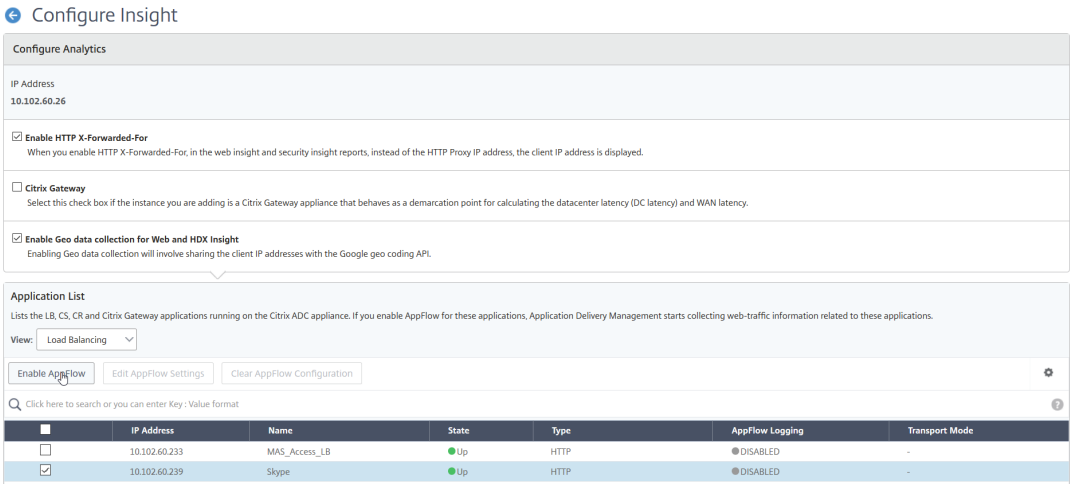



3. En la página **Configurar información** :

   a) Seleccione la **Lista de aplicaciones** para Equilibrio de carga o Content Switching.




   b) Seleccione el servidor virtual y haga clic en **Habilitar AppFlow**.



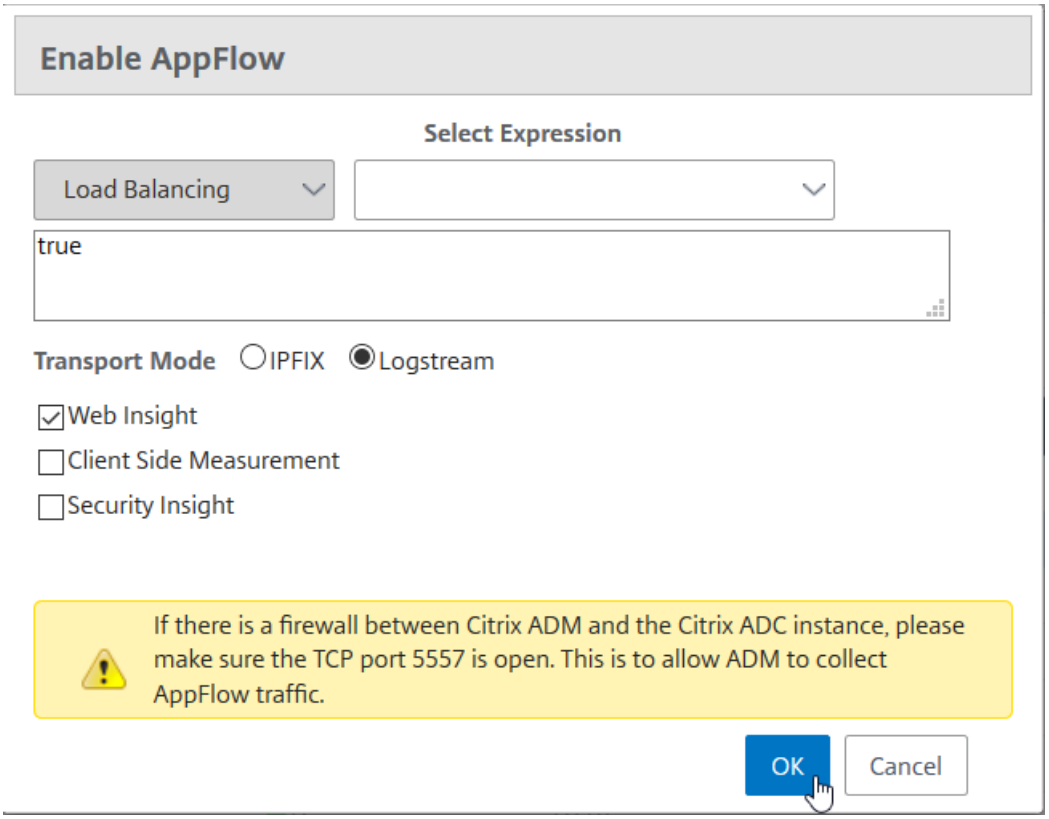

4. En el cuadro de diálogo Habilitar AppFlow:

   - Introduzca **true** en el cuadro de texto
   - Seleccione **Logstream** como modo de transporte

     > Nota: Citrix recomienda seleccionar Logstream como modo de transporte.

   - Seleccione **Web Insight** y haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Analizar problemas de aplicaciones web

Uno de los problemas comunes que un administrador debe identificar son los problemas de latencia. Como administrador, debe averiguar si el problema de latencia proviene de la red del servidor, la red del cliente o el tiempo de respuesta del servidor. Con Citrix ADM, puede identificar esta información yendo a **Analytics** > **Web Insight** .

Cuando navega a **Analytics** > **Web Insight** , se muestran las instancias de Citrix ADC que están habilitadas con Web Insight. Puede ver la información detallada de las instancias, como la dirección IP, el nombre del host, el número total de visitas y el ancho de banda.

Mediante la lista, puede seleccionar la duración del tiempo para ver las perspectivas de las instancias.

También puede utilizar el control deslizante para personalizar la duración del tiempo y hacer clic en **Ir** para mostrar los resultados.

Al hacer clic en el gráfico o en la dirección IP de la instancia, se muestra la información detallada sobre la instancia. Puede ver información sobre lo siguiente:

- **Número total de visitas**
- **Ancho de banda**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Aplicaciones**
- **Dominios**
- **URLs**
- **Métodos de solicitud HTTP**
- **Estado de respuesta HTTP**
- **Clientes**
- **Servidores**
- **Sistemas operativos**
- **Agentes de usuario**

También puede seleccionar las **entidades de Web Insight** para las que desea ver los informes en la GUI.

1. Vaya a **Analytics** > **Web Insight** > **Configuración** .
2. Haga clic en **Configurar registros de datos de Analytics**.
3. En **Configuración del informe de Web Insight**, seleccione las entidades que quiere ver los informes en la GUI.
4. Haga clic en **Aceptar**.

Para profundizar en el análisis, puede hacer clic en cada categoría de información en Web Insight en la GUI. Por ejemplo, si desea comprobar los problemas de los servidores configurados:

1. Vaya a **Analytics** > **Web Insight** > **Servidores** .
2. Se muestra la página Servidores con todos los servidores configurados.
3. Haga clic en la dirección IP del gráfico. También puede hacer clic en la dirección IP de la tabla.

   Se muestra la vista detallada del servidor seleccionado. Desde esta vista, puede comprobar si hay varios datos, como:

   - Número total de visitas recibidas por el servidor
   - Ancho de banda
   - Tiempo de procesamiento del servidor
   - Latencia de red del servidor
   - Servidores virtuales configurados para el servidor
   - Número total de clientes que acceden al servidor
   - Número total de códigos de respuesta proporcionados por el servidor

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Caso de uso 1: error interno del servidor**

Considere un caso en el que los usuarios están experimentando el error 500 de inaccesibilidad para su aplicación web. El error 500 (no encontrado) es un error de estado de respuesta HTTP que indica un problema en el servidor web, pero el servidor no indica el problema explícitamente. Para identificar y profundizar en el problema real:

1. Vaya a **Analytics** > **Web Insight** > Estado de **respuesta** .

   Se muestra la página del panel de control. El panel le proporciona las métricas que puede usar para analizar el éxito y el fracaso de las transacciones HTTP que se procesan.

2. Haga clic en **No encontrado** en el gráfico.
3. Desplázate hacia abajo para ver el **gráfico de servidores** y, en la lista **Filtrar por** , selecciona **Latencia de red de servidores** .

   El gráfico indica que cada servidor de aplicaciones tuvo un problema al recuperar la aplicación web y, por lo tanto, aumenta el tiempo de respuesta para el servidor web. El problema puede deberse a que el servidor web no responde a ninguna solicitud de ningún servidor.

**Caso de uso 2: el usuario experimenta lentitud para acceder a la aplicación web**

Considere un caso en el que su aplicación web está alojada a través de 10 servidores web diferentes. Cuando varios usuarios acceden a la aplicación al mismo tiempo, es posible que uno o más usuarios experimenten lentitud en la aplicación. Como administrador, debe analizar los siguientes casos para comprender la causa raíz del problema:

**Caso 1: Tiempo de procesamiento del servidor**:

Cuando varias solicitudes llegan a los 10 servidores web al mismo tiempo, el tiempo necesario para cargar la solicitud varía en función de:

- Número de solicitudes en la cola.
- El ancho de banda consumido por cada solicitud para procesar la transacción HTTP.

  El gráfico del servidor puede ayudarlo a comprender el tiempo de procesamiento de cada servidor para la solicitud procesada por los servidores. Del mismo modo, el gráfico de la aplicación muestra las visitas, el tiempo de respuesta y el ancho de banda consumido por cada transacción HTTP.

1. Vaya a **Analytics** > **Web Insight** > **Servidores** .
2. Seleccione el servidor en el gráfico.
3. Haga clic en **Tiempo de procesamiento del servidor** para analizar el tiempo de procesamiento del servidor.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Caso 2: Latencia del cliente**:

El tiempo de respuesta y el número total de visitas a la aplicación pueden ser la razón de la lentitud del acceso a la aplicación. Puede comprobar la latencia de la red del cliente y analizar las métricas de la latencia de la red del cliente. Para analizar la causa principal:

1. Vaya a **Analytics** > **Web Insight** > **Clientes** .
2. Seleccione el cliente del gráfico.
3. Haga clic en **Latencia de red cliente** para analizar la latencia alta.

   En este ejemplo, como administrador, puede ver que la causa raíz del problema proviene de la red del cliente porque la latencia de la red del cliente indica alta.

**Caso de uso 3: Lentitud en el acceso a la aplicación web**

Considere un caso en el que tiene servidores web para usuarios de Windows y servidores web para usuarios de Mac, y los usuarios están informando de lentitud en el acceso a la aplicación web. Como administrador, sabe que tiene:

- Configuró un servidor virtual de conmutación de contenido para usuarios de Windows.
- Configuró un servidor virtual de conmutación de contenido para usuarios de Mac.
- Se configuraron los servicios asociados enlazados a los servidores virtuales para redirigir las solicitudes en función de los usuarios de Windows y Mac.

Para analizar la causa principal del problema de lentitud de las aplicaciones web:

1. Vaya a **Analytics** > **Web Insight** > **Aplicaciones**
2. Seleccione el servidor virtual de conmutación de contenido.
   Por ejemplo, la aplicación «csTolbTarget» de la imagen es un servidor virtual de conmutación de contenido que está enlazado a otros servidores virtuales de equilibrio de carga.
3. Haga clic en el servidor virtual de conmutación de contenido para ver el otro servidor virtual de equilibrio de carga. También puede hacer clic en el nombre de la aplicación en la tabla.

También puede hacer clic en los servidores de equilibrio de carga enlazados para ver los detalles de Web Insight de esas aplicaciones.

## Analizar información para exploradores y sistemas operativos

Puedes usar Web Insight para ayudarte a separar los problemas de latencia L7 y entender el uso de los dispositivos móviles. Como administrador, la información puede ayudarlo a comprender las diferentes adopciones de los sistemas operativos en su base de usuarios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Vaya a **Analytics** > **Web Insight** > **Sistema operativo** para ver por qué hay lentitud en el acceso de los usuarios y si se debe a la incompatibilidad entre determinados exploradores. También puede ver qué sistemas operativos se están utilizando en determinados clientes y los exploradores a los que se accede. Puede comparar el tiempo de renderizado en los diferentes exploradores y profundizar en un explorador concreto para identificar qué páginas de aplicación están asociadas con el tiempo de procesamiento más alto para ese explorador.

Por ejemplo, puede seleccionar **Google Chrome** y ver los tiempos de representación correspondientes para las diferentes páginas URL de una aplicación concreta.

### Instancias NetScaler ADC implementadas en modo de alta disponibilidad

Citrix ADM proporciona informes para las instancias de ADC que se implementan en modo de alta disponibilidad. Todos los análisis admiten informes agregados para instancias en modo de alta disponibilidad.

Puede hacer clic en el nombre de las instancias que están en alta disponibilidad para ver más detalles.

### Instancias NetScaler ADC implementadas en modo de clúster

Citrix ADM proporciona informes para las instancias de ADC que se implementan en modo clúster. Todos los análisis admiten informes agregados de instancias en modo de clúster.

También puede hacer clic en el **nombre de host CLIP** para ver todos los detalles sobre las instancias de ADC que se implementan en modo de clúster.

> **Nota**
>
> - Todos los datos recopilados previamente antes de actualizar a NetScaler ADM 12.1 build 503.x permanecen mostrados como informes independientes durante el período hasta que los datos persistan.
> - Para las instancias de ADC implementadas en modo clúster, el ID del dominio de observación o los nombres de dominio de observación se sustituyen por el nombre de host CLIP y CLIP. Todos los datos recopilados anteriormente continúan reportando el ID del dominio de observación/el nombre del dominio de observación.

### Configuración de mapa geográfico de Web Insight

La función Geomaps de NetScaler ADM muestra el uso de aplicaciones web en diferentes ubicaciones geográficas en un mapa. Los administradores pueden utilizar esta información para comprender las tendencias en el uso de aplicaciones y para la planificación de la capacidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El mapa geográfico proporciona información sobre las siguientes métricas específicas de un país, estado y ciudad:

- Número total de visitas: Número total de veces que se accede a una aplicación.
- Ancho de banda: ancho de banda total consumido al atender las solicitudes
- Tiempo de respuesta: Tiempo medio necesario para enviar respuestas a las solicitudes de los clientes.

Los geomapas proporcionan información que se puede utilizar para abordar varios casos de uso, como los siguientes:

- Región que tiene el número máximo de clientes que acceden a una aplicación
- Región que tiene el tiempo de respuesta más alto
- Región que consume más ancho de banda

Citrix ADM le ofrece la opción de configurar mapas geográficos para direcciones IP privadas o direcciones IP públicas.

### Configurar geometrías para direcciones IP privadas

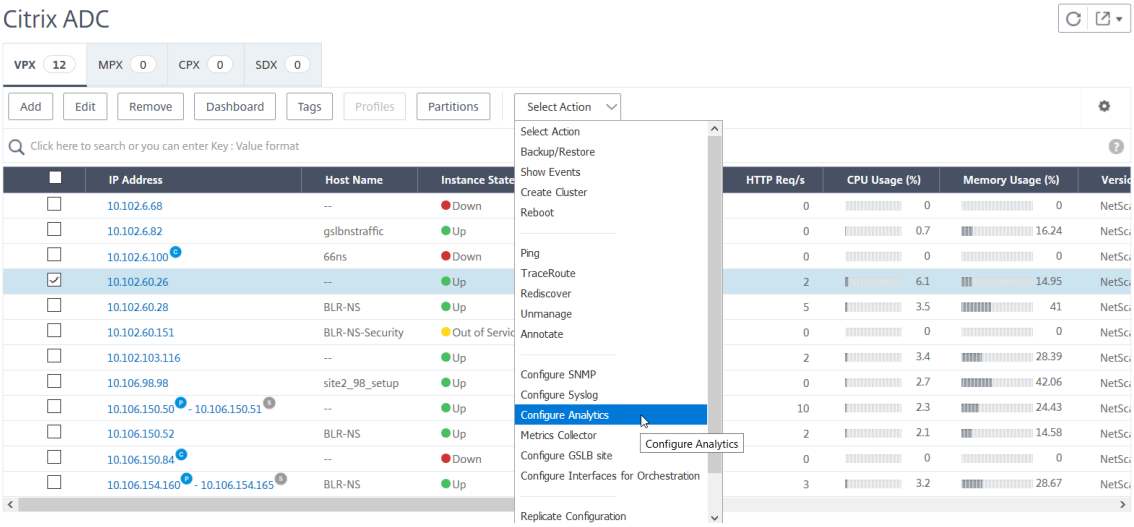
> **Nota**
>
> El siguiente procedimiento solo se aplica si su Citrix ADM es **13.0 Build 36.27 o anterior**. Para NetScaler ADM **13.0 Build 41.x o posterior**, la recopilación de datos geográficos se habilita automáticamente al habilitar Web Insight.

Para ver el tráfico de aplicaciones web originado por direcciones IP privadas en el mapa geográfico, primero debe crear bloques de direcciones IP privadas y, a continuación, habilitar la recopilación de datos geográficos.

Para habilitar la recopilación de datos geográficos:

1. Vaya a **Redes** > **Instancias** > **Citrix ADC** y seleccione la instancia de Citrix ADC.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



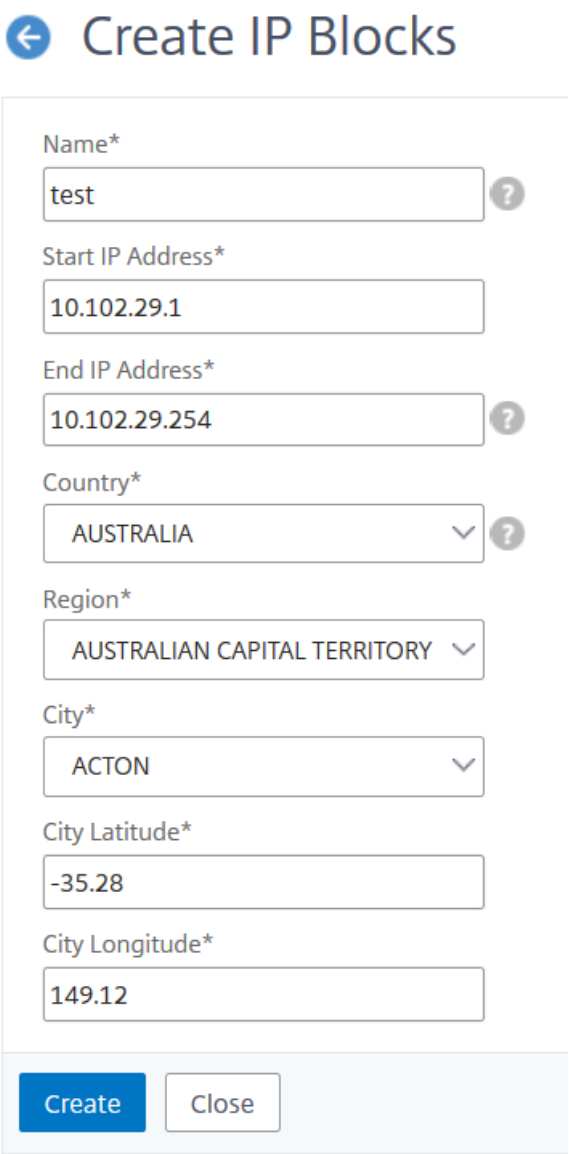

3. En la página **Configurar Insight** , seleccione **Habilitar la recopilación de datos geográficos para Web y HDX Insight**.

**Crear un bloque de IP privado** NetScaler ADM puede reconocer la ubicación de un cliente cuando la dirección IP privada del cliente se agrega al servidor NetScaler ADM. Por ejemplo, si la dirección IP de un cliente se encuentra dentro del intervalo de un bloque de direcciones IP privado asociado con Ciudad A, NetScaler ADM reconoce que el tráfico se origina desde Ciudad A para este cliente.

Para crear un bloque IP:

1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Bloques de IP** y, a continuación, haga clic en **Agregar**.
2. En la página **Crear Bloques de IP**, especifique los siguientes parámetros:
   - **Nombre**. Especifique un nombre para el bloque de IP privado
   - **Dirección IP inicial**. Especifique el rango de direcciones IP más bajo para el bloque de IP.
   - **Dirección IP final**. Especifique el rango de direcciones IP más alto para el bloque de IP.
   - **País**. Selecciona el país de la lista.
   - **Región**. Según el país, la región se rellena automáticamente, pero puede seleccionarla.
   - **Ciudad**. Según la región, la ciudad se rellena automáticamente, pero puede seleccionar la ciudad.
   - **Latitud** y **longitud de la ciudad**. Según la ciudad que selecciones, la latitud y la longitud se rellenan automáticamente.
3. Haga clic en **Crear** para finalizar.

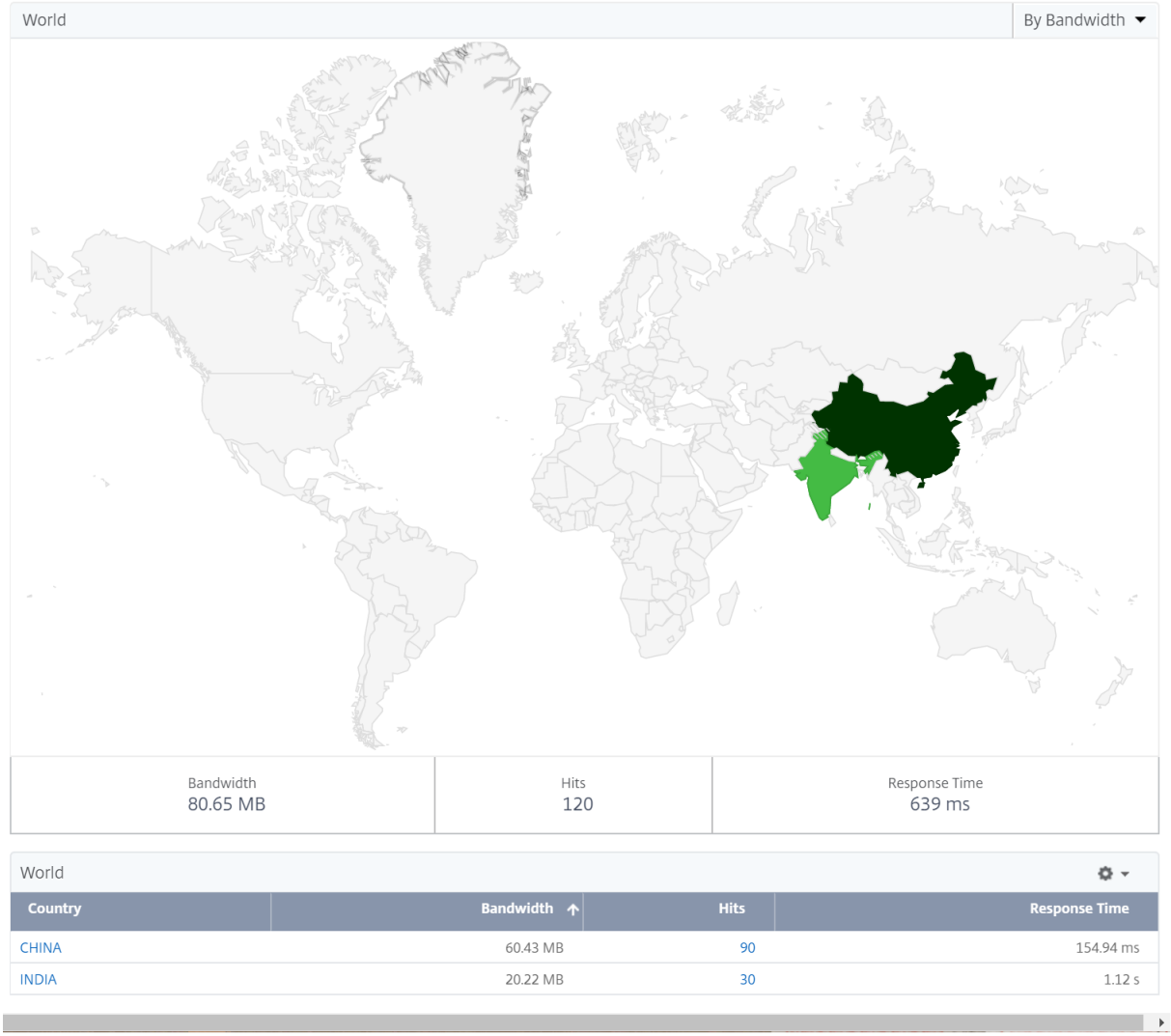
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Bloques IP públicos** Citrix ADM también puede reconocer la ubicación de un cliente si el cliente utiliza una dirección IP pública. NetScaler ADM tiene su archivo CSV de ubicación integrado que coincide con la ubicación según el intervalo de direcciones IP del cliente. Para usar el bloque de IP público, el único requisito es habilitar la recopilación de **datos** geográficos en la página **Configurar Insight** .

> Nota
>
> NetScaler ADM requiere una conexión a Internet para mostrar los mapas geográficos de una ubicación geográfica determinada. También se requiere conexión a Internet para exportar el GeoMap en formatos.pdf,.png o.jpg.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Para exportar el informe de este panel:**

Para exportar el informe de esta página, haga clic en el icono **Exportar** en la parte superior derecha de esta página. En la página **Exportar**, puede realizar una de las siguientes acciones:

1. Seleccione la ficha **Exportar ahora**. Para ver y guardar el informe en formato PDF, JPEG, PNG o CSV.
2. Seleccione la ficha **Planificar exportación**. Programar el informe a diario, semanal o mensual y enviarlo por correo electrónico o mensaje de Slack.

> **Nota**
>
> - Si selecciona Periodicidad **semanal**, asegúrese de seleccionar los días laborables en los que quiere que se programe el informe.
> - Si selecciona Periodicidad **mensual**, asegúrese de especificar todos los días que quiere pro-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> gramar el informe separados por comas.

## Configurar umbrales

Puede crear umbrales y recibir una notificación cada vez que se supere el valor del umbral. En una implementación típica, puede establecer umbrales para:

- Realice un seguimiento de las diferentes métricas
- Facilitar la planificación
- Reciba notificaciones cuando el valor de la métrica de la aplicación supere el umbral establecido

Para configurar el umbral:

1. Vaya a **Analytics** > **Configuración** > **Umbrales**.
2. En la página **Umbrales**, haga clic en **Agregar**.

   Aparece la página **Crear umbral** .
3. Especifique los siguientes detalles:

   a) **Nombre**: especifique un nombre para crear un evento.

   b) **Tipo**de tráfico : en la lista, selecciona WEB.

   c) **Entidad**: en la lista, seleccione la categoría o el tipo de recurso. De forma predeterminada, se selecciona «aplicaciones» como entidad.

   d) **Clave**de referencia: se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.

   e) **Duración**: en la lista, seleccione el intervalo de tiempo durante el que desea supervisar la entidad. Puede supervisar las entidades durante una hora, un día o una semana de duración.

   f) En la sección **Configurar regla**, cree una regla eligiendo la métrica, un comparador necesario y proporcione un valor de umbral.

   g) En la sección **Configuración de notificaciones**, seleccione **Habilitar umbral** y el modo de alerta para el que quiere obtener las alertas.
4. Haga clic en **Crear**.

## Solucionar problemas de Web Insight

Para obtener más información, consulte el documento de solución de problemas Solucionar problemas de Web Insight.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Solucionar problemas de Web Insight

January 30, 2024

Con el panel de control de NetScaler ADM Web Insight, puede visualizar el uso de las aplicaciones y supervisar todas las aplicaciones web a las que sirven las instancias de NetScaler ADC. Con Web Insight, las instancias de ADC envían datos de transacciones HTTP y SSL al ADM configurado como recopilador de AppFlow. AppFlow es el estándar de exportación de flujos que se utiliza para identificar y recopilar datos de aplicaciones y transacciones en la infraestructura de red.

Este documento le ayuda a solucionar problemas comunes de implementación de Web Insight.

## Problemas relacionados con los informes del panel de NetScaler ADM Web Insight

Si el panel de control de **ADM Web Insight ( GUI de ADM > Analytics > Web Insight** ) no muestra los informes, es posible que el problema sea uno de los siguientes:

- Problema de configuración de Web Insight
- Problema de conectividad entre NetScaler ADC y NetScaler ADM
- Problema del contador
- Problema de licencia
- Problema con la identificación del punto
- Problema de parámetros de AppFlow faltantes

### Problema de configuración: NetScaler ADM Web Insight no muestra informes

Complete estos pasos para solucionar este problema:

1. Asegúrese de que la función AppFlow esté habilitada en la instancia de NetScaler ADC. Para obtener más información, consulte Habilitar AppFlow.
2. Compruebe la configuración de Web Insight en la instancia ADC:
   a) Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de Web Insight en la directiva. Asegúrese de que el tipo de enlace es`REQUEST`. Por ejemplo: `bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
   b) Ejecute el comando `show appflow action` para comprobar la configuración de Web Insight en la acción. Asegúrese de que la`-webinsight` opción está activada
   c) Compruebe el parámetro `appflowlog` en el servidor virtual LB/CS/CR correctamente. Asegúrese de que este parámetro esté habilitado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Problema de conectividad entre NetScaler ADC y NetScaler ADM: NetScaler ADM Web Insight no muestra informes

Complete estos pasos para solucionar este problema:

1. Compruebe el estado del recopilador AppFlow en NetScaler ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler ADC y AppFlow Collector.
2. En la GUI de ADC, compruebe si las directivas de AppFlow están recibiendo visitas. Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva AppFlow. También puede ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.
3. Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

### Problema del contador: NetScaler ADM Web Insight no muestra informes

Complete estos pasos para solucionar este problema:

1. Asegúrese de que no haya problemas de configuración y conectividad de AppFlow. Para obtener más información, consulte las secciones de soluciones de este tema para conocer el problema de configuración y el problema de conectividad entre NetScaler ADC y NetScaler ADM.
2. En la instancia de ADC, en el indicador de shell, ejecute el comando `nsconmsg -g appflow_tmpl -d current` y compruebe los siguientes contadores:

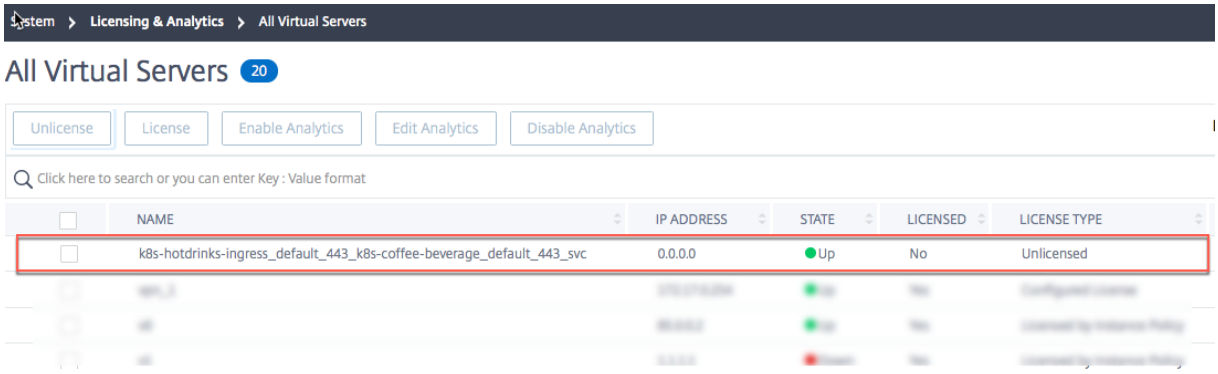
   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   Si falta alguno de los contadores, realice un seguimiento en la instancia de ADC. A continuación, confirme que la transacción esté completa y que la respuesta se esté sirviendo desde el servidor de origen. Si la transacción es correcta y faltan algunos contadores, presente un error.

### Problema de licencia: NetScaler ADM Web Insight no muestra informes

En este caso, la licencia del servidor virtual concreto para el que desea ver el informe de Web Insight aparece como «No» en **Sistema > Licencias y análisis > Configurar licencia** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Complete estos pasos para solucionar este problema:

1. En la instancia de ADC, asegúrese de que las visitas a la directiva de AppFlow aumenten y que la instancia envíe registros de AppFlow a ADM
2. Compruebe si el servidor virtual correspondiente tiene licencia. Si el servidor virtual no tiene licencia, ADM descarta los registros de AppFlow. Como resultado, los informes de Web Insight no aparecen.

### Problema de ID de punto de observación: NetScaler ADM Web Insight no muestra informes

Este problema aparece porque el ID del punto de observación no es único.

> Nota:
> Un ID de punto de observación es el identificador del NetScaler ADC desde el que se exportan los registros de AppFlow. De forma predeterminada, la IP de NetScaler ADC es el ID del punto de observación.

Complete estos pasos para solucionar este problema:

1. En la instancia de ADC, asegúrese de que las visitas a la directiva de AppFlow aumenten y que la instancia finalice los registros de AppFlow para ADM.
2. Compruebe si el servidor virtual correspondiente tiene licencia.
3. Asegúrese de que la configuración no se copie de una instancia de ADC a otra. Cuando se copia, la configuración puede crear un problema de ID de exportador, lo que hace que ADM elimine los registros de AppFlow.
4. Inicie sesión en la instancia de ADC y ejecute el comando `unset appflow param -observationpointId`.

### Problema de parámetros de AppFlow faltantes: NetScaler ADM Web Insight no muestra informes

Este problema aparece porque ADM descarta los registros de AppFlow debido a la falta de datos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Complete estos pasos para solucionar este problema:

1. Asegúrese de que, en la instancia de ADC, las visitas a la directiva de AppFlow estén aumentando y que la instancia finalice los registros de AppFlow para ADM.
2. Compruebe si el servidor virtual correspondiente tiene licencia.
3. Asegúrese de que la configuración no se copie de una instancia de ADC a otra. Cuando se copia, la configuración puede crear un problema de ID de exportador, lo que hace que ADM elimine los registros de AppFlow.
4. Asegúrese de que los siguientes parámetros de AppFlow estén habilitados en la instancia de ADC:

   a) `HTTP method logging`
   b) `HTTP domain name logging`
   c) `HTTP URL logging`
   d) `HTTP host logging`
   e) `HTTP Content-Type header logging`

### Problemas varios de Citrix ADM Web Insight

- **Problema**: en el cliente HTTP, la página no se carga cuando AppFlow está habilitado.
- **Solución**: complete los pasos siguientes para solucionar este problema:

  1. En el comando de acción AppFlow, desactive la función “pageTracking”`set appflow action <name> -pageTracing disable`. Esta acción no tiene ningún efecto en la funcionalidad.

  Si el problema no se soluciona, siga este paso:

  1. En la misma acción, desconfigure la entidad `clientsidemeasurement`: `set appflow action <name> -clientsidemeasurements disable`. Si este paso resuelve el problema, capture seguimientos en la instancia de ADC y archive un error.

- **Problema**: el dispositivo ADC se bloquea cuando AppFlow está habilitado.
- **Solución**: complete los pasos siguientes para solucionar este problema:

Si backtrace (BT) tiene funciones de AppFlow, es posible que el problema esté en la función AppFlow. Si el BT está en un código específico de una función, el problema podría estar en las funciones que utilizan AppFlow para enviar datos a los recopiladores.
En este último caso, desactive cualquier configuración de AppFlow específica de una función y verifique. No desactive la función AppFlow de forma global, ya que este paso no proporciona mucha información sobre el problema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Solución de problemas de uso de contadores

Compruebe los siguientes contadores de AppFlow para ver si hay algún problema relacionado con AppFlow o Web Insight.

| Contador | Descripción |
|---|---|
| `appflow_tot_record_drop` | Registros de AppFlow descartados debido a un recopilador no válido. Suele ocurrir cuando la configuración del recopilador cambia y las conexiones existentes utilizan la configuración del recopilador anterior. |
| `lstream_tot_trans_written` | Este contador debe incrementarse para cada transacción que se vaya a registrar. |
| `lstream_sent` | Este contador se incrementa por cada registro de transacciones que se envía. |

## HDX Insight

January 30, 2024

HDX Insight proporciona una visibilidad integral del tráfico HDX a Citrix Virtual Apps and Desktop que pasa por Citrix ADC. También permite a los administradores ver métricas de latencia de red y clientes en tiempo real, informes históricos, datos de rendimiento de extremo a extremo y solucionar problemas de rendimiento. La disponibilidad de datos de visibilidad en tiempo real e históricos permite que Citrix Application Delivery Management (ADM) admita una amplia variedad de casos de uso.

Para que aparezcan los datos, debe habilitar AppFlow en los servidores virtuales de Citrix Gateway. AppFlow se puede entregar mediante el protocolo IPFIX o el método LogStream.

> **Nota**
>
> Para permitir que se registren los cálculos del tiempo de ida y vuelta de ICA, active la siguiente configuración de directivas

- Cálculo de ida y vuelta de ICA
- Intervalo de cálculo de ida y vuelta
- Cálculo ICA de ida y vuelta para conexiones inactivas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si hace clic en un usuario individual, podrá ver cada sesión HDX, activa o terminada, que el usuario haya realizado dentro del período de tiempo seleccionado. Otra información incluye varias estadísticas de latencia y ancho de banda consumido durante la sesión. También puede obtener información sobre el ancho de banda de los canales virtuales individuales, como el audio, la asignación de impresoras y la asignación de unidades del cliente.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso a nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

También puede navegar a **HDX Insight** > **Aplicaciones** y hacer clic en **Duración del lanzamiento**para ver el tiempo que tarda la aplicación en iniciarse. También puede ver el agente de usuario de todos los usuarios conectados navegando hasta**HDX Insight**-> Usuarios.

> **Nota**HDX Insight admite Particiones de administración configuradas en instancias de Citrix ADC que se ejecutan en la versión 12.0 de software.

Los siguientes clientes ligeros admiten HDX Insight:

- Thin Clients WYSE basados en Windows
- Clientes ligeros basados en Linux de WYSE
- Thin Clients de WYSE basados en ThinOS
- Clientes ligeros basados en Ubuntu de 10 ZiG

## Identificación de la causa raíz de los problemas de rendimiento lento

### Caso 1

El usuario experimenta retrasos al acceder a Citrix Virtual Apps and Desktops.

Los retrasos pueden deberse a la latencia en la red del servidor, retrasos en el tráfico ICA causados por la red del servidor o latencia en la red del cliente.

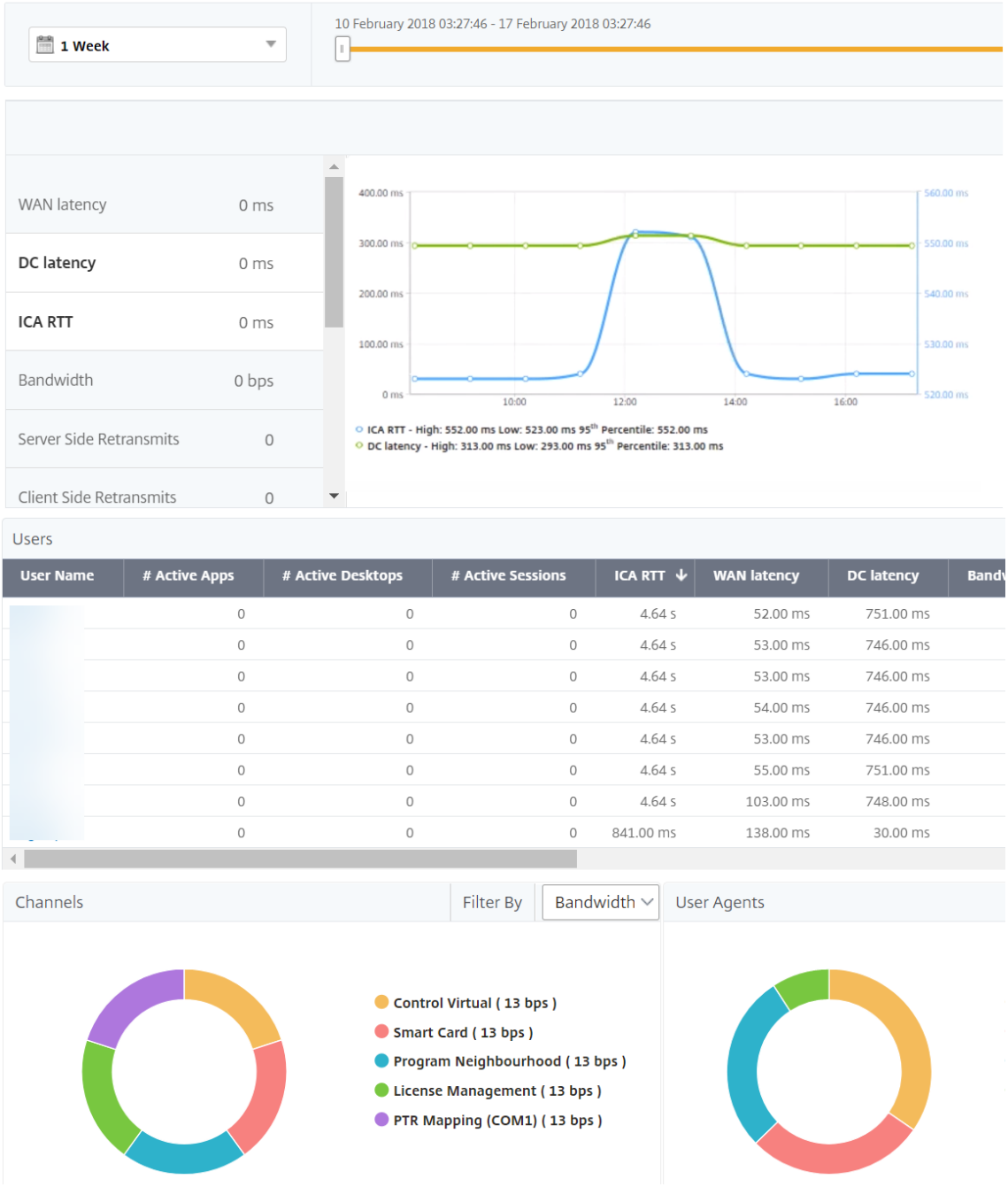
Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora de host

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

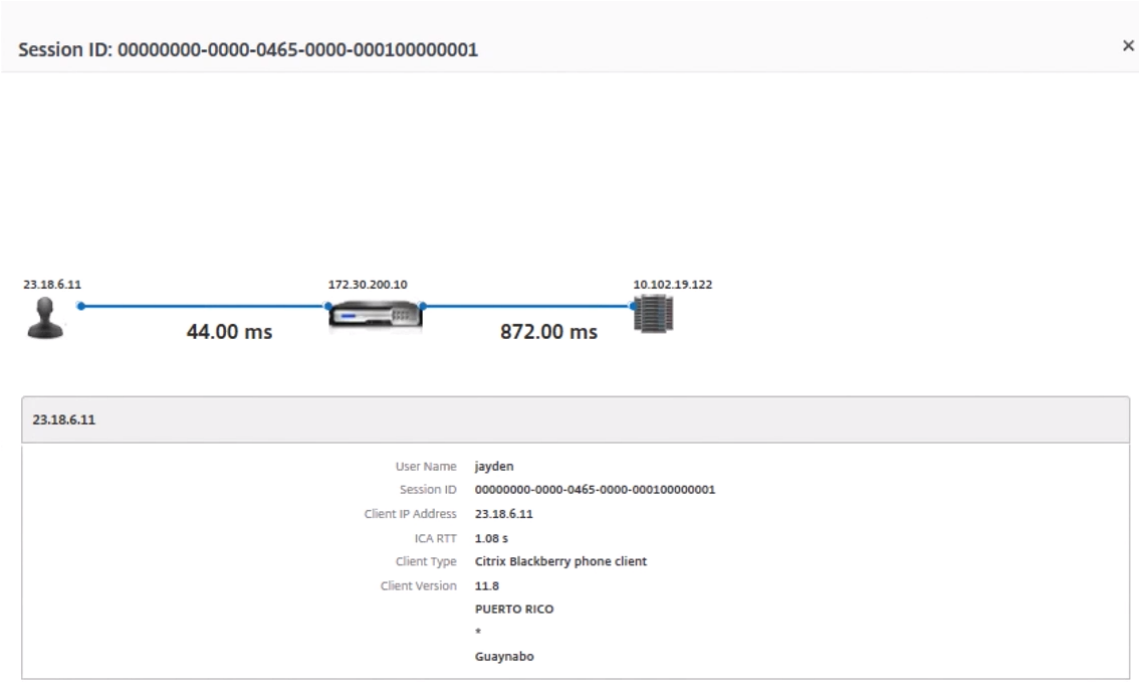
**Para ver las métricas del cliente:**

1. En la ficha**Analytics**, vaya a**HDX Insight** >**Usuarios**.
2. Desplácese hacia abajo y seleccione el nombre de usuario y seleccione el período de la lista. El período puede ser de un día, una semana, un mes o incluso puede personalizar el período del que quiere ver los datos.
3. El gráfico muestra los valores de latencia ICA RTT y DC del usuario para el período especificado como un gráfico.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En la tabla**Sesiones actuales**, coloque el mouse sobre el valor de**RTT**y observe los valores de retraso del host, latencia de DC y latencia de WAN.
5. En la tabla**Sesiones actuales**, haga clic en el símbolo del diagrama de saltos para mostrar información sobre la conexión entre el cliente y el servidor, incluidos los valores de latencia.




**Resumen** En este ejemplo, la **latencia de DC** es de 751 milisegundos, la **latencia de la WAN** es de 52 milisegundos y los **retrasos del host** son de 6 segundos. Esto indica que el usuario está experimentando un retraso debido a la latencia promedio causada por la red del servidor.

**Caso 2**

El usuario experimenta un retraso al iniciar una aplicación en Citrix Virtual App o Desktop

El retraso puede deberse a la latencia en la red del servidor, retrasos de tráfico ICA causados por la red del servidor, latencia en la red del cliente o tiempo tardado en iniciar una aplicación.

Para identificar la causa principal del problema, analice las siguientes métricas:

- Latencia de WAN
- Latencia de DC
- Demora del host

**Para ver las métricas de usuario:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En la ficha **Análisis**, vaya a **HDX** Insight **Usuarios.
2. Desplácese hacia abajo y haga clic en el nombre de usuario.
3. En la representación gráfica, anote los valores de latencia WAN, latencia de DC y RTT de la sesión en particular.
4. En la tabla **Sesiones actuales**, tenga en cuenta que el retraso del host es alto.

Current Sessions — By Start Time

| Diagram | Session ID | Session Type | ICA RTT | Host Delay | Start Time | Up Time | Client IP Address | Server IP Address | NetScaler IP Address |
|---|---|---|---|---|---|---|---|---|---|
| | 0000...000001 (NON EUEM) | Application | 784 ms | 517.00 ms | 10/29/2016 6:20:20 PM | 0 h: 2 m: 50s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 758 ms | 287.00 ms | 10/29/2016 6:20:20 PM | 0 h: 2 m: 50s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 768 ms | 191.00 ms | 10/29/2016 6:17:20 PM | 0 h: 5 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 815 ms | 608.00 ms | 10/29/2016 6:17:20 PM | 0 h: 5 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 845 ms | 107.00 ms | 10/29/2016 6:14:20 PM | 0 h: 8 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 775 ms | 555.00 ms | 10/29/2016 6:14:20 PM | 0 h: 8 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 809 ms | 86.00 ms | 10/29/2016 6:11:20 PM | 0 h: 11 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 796 ms | 591.00 ms | 10/29/2016 6:11:20 PM | 0 h: 11 m: 51s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 777 ms | 83.00 ms | 10/29/2016 6:08:19 PM | 0 h: 14 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 825 ms | 622.00 ms | 10/29/2016 6:08:19 PM | 0 h: 14 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 770 ms | 67.00 ms | 10/29/2016 6:05:19 PM | 0 h: 17 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 805 ms | 602.00 ms | 10/29/2016 6:05:19 PM | 0 h: 17 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 870 ms | 628.00 ms | 10/29/2016 6:02:19 PM | 0 h: 20 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 767 ms | 55.00 ms | 10/29/2016 6:02:19 PM | 0 h: 20 m: 52s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 788 ms | 634.00 ms | 10/29/2016 5:59:19 PM | 0 h: 23 m: 53s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 850 ms | 52.00 ms | 10/29/2016 5:59:19 PM | 0 h: 23 m: 53s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 864 ms | 569.00 ms | 10/29/2016 5:56:18 PM | 0 h: 26 m: 53s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |
| | 0000...000001 (NON EUEM) | Application | 759 ms | 48.00 ms | 10/29/2016 5:56:18 PM | 0 h: 26 m: 53s | 190.104.96.33 | 10.102.60.51 | 172.30.200.10 |

**Resumen** En este ejemplo, la**latencia de DC**es de 1 milisegundo, la**latencia de la WAN** es de 12 milisegundos, pero el**retraso del host** es de 517 milisegundos. RTT alto con latencias de DC y WAN bajas indica un error de aplicación en el servidor host.

> **Nota**HDX Insight también muestra más métricas de usuario, como la fluctuación de WAN y las retransmisiones del lado del servidor si utiliza Citrix ADM ejecutando el software 11.1 compilación 51.21 o posterior. Para ver estas métricas, vaya a **Analytics** > **HDX Insight** > **Usuarios** y seleccione un nombre de usuario. Las métricas de usuario aparecen en la tabla junto al gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

## Geomapas para HDX Insight

La funcionalidad de geomapas de Citrix ADM muestra el uso de aplicaciones en diferentes ubicaciones geográficas en un mapa. Los administradores pueden usar esta información para comprender las tendencias en el uso de las aplicaciones en diversas ubicaciones geográficas.

Puede configurar Citrix ADM para que muestre los geomapas de una ubicación geográfica o LAN determinada especificando el rango de IP privadas (direcciones IP de inicio y final) de la ubicación.

También puede ver los detalles históricos y activos de los usuarios desde los mapas de ubicación geográfica en HDX Insight. Vaya a **Analytics** > **HDX Insight** y, en la sección **Mundo** del mapa, haga clic en el país o la región de los que desee ver los detalles. Puede profundizar más para ver la información por ciudad y estado.

**Para configurar una geomapa para centros de datos:**

En la ficha **Analytics**, vaya a **Configuración** > **Bloques de IP** para configurar geometrías para una ubicación concreta.

### Caso de uso

Considere un caso en el que la organización ABC tiene 2 sucursales, una en Santa Clara y la otra en India.

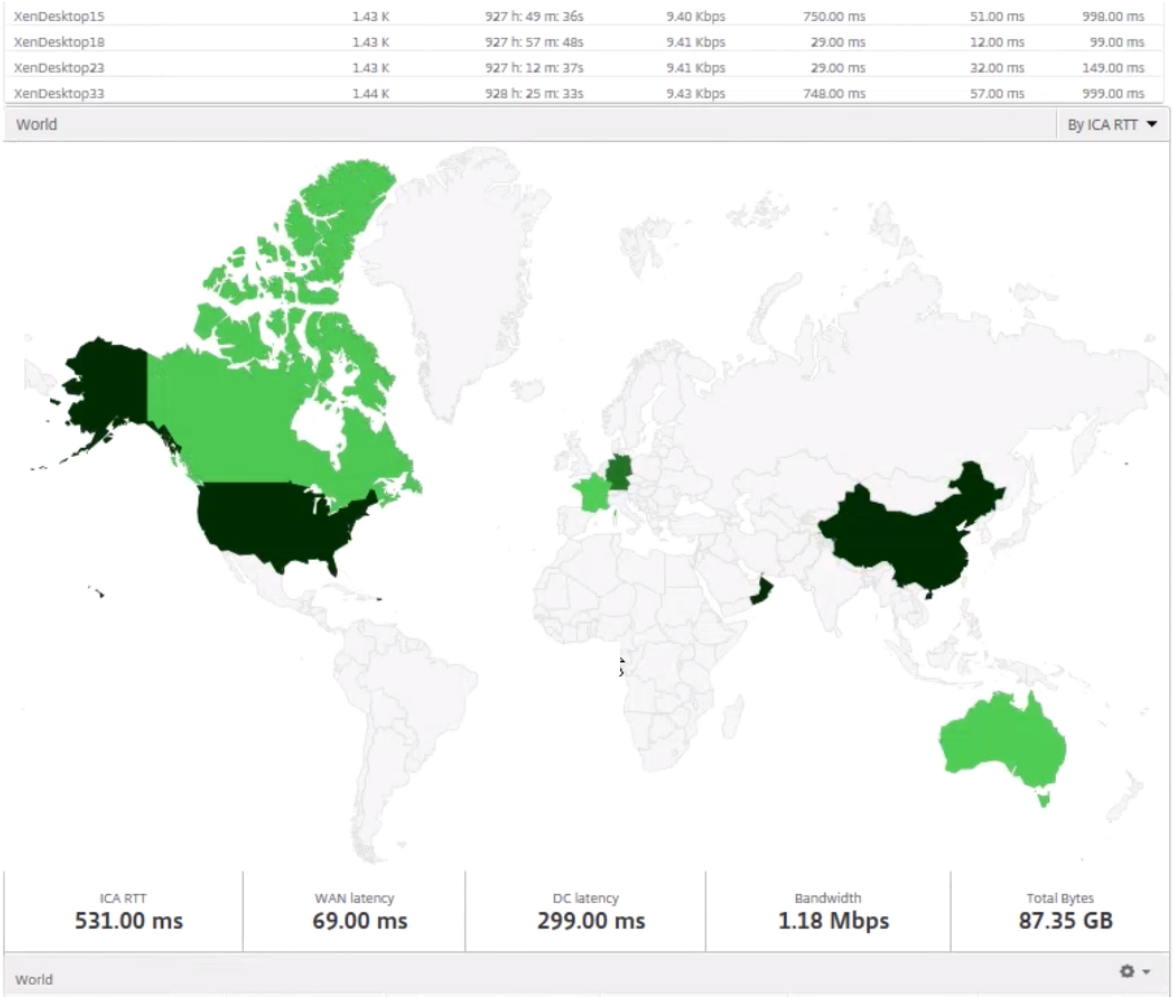
Los usuarios de Santa Clara utilizan el dispositivo Citrix Gateway en SClara.x.com para acceder al tráfico VPN. Los usuarios indios utilizan el dispositivo Citrix Gateway en India.x.com para acceder al tráfico de VPN.

Durante un intervalo de tiempo determinado, por ejemplo, de 10 a. m. a 5 p. m., los usuarios de Santa Clara se conectan a SClara.x.com para acceder al tráfico de VPN. La mayoría de los usuarios acceden

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a la misma puerta de Citrix Gateway, lo que provoca un retraso en la conexión a la VPN, por lo que algunos usuarios se conectan a India.x.com en lugar de a SClara.x.com.

Un administrador de Citrix ADC que analice el tráfico puede utilizar la funcionalidad de mapa geográfico para mostrar el tráfico en la oficina de Santa Clara. El mapa muestra que el tiempo de respuesta en la oficina de Santa Clara es alto, porque la oficina de Santa Clara solo tiene un dispositivo Citrix Gateway a través del cual los usuarios pueden acceder al tráfico de VPN. Por lo tanto, es posible que el administrador decida instalar otro Citrix Gateway, de modo que los usuarios dispongan de dos dispositivos Citrix Gateway locales a través de los cuales acceder a la VPN.




## Limitaciones

Si las instancias Citrix ADC tienen licencia Advanced, los umbrales establecidos en Citrix ADM para HDX Insight no se activarán, ya que los datos analíticos se recopilan durante solo 1 hora.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Habilitar la recopilación de datos de HDX Insight

January 30, 2024

HDX Insight permite a TI ofrecer una experiencia de usuario excepcional al proporcionar una visibilidad end-to-end sin precedentes del tráfico ICA que pasa a través de las instancias Citrix ADC o los dispositivos Citrix SD-WAN, y forma parte de Citrix Application Delivery Management (ADM) Analytics. HDX Insight ofrece capacidades de análisis de fallos y de inteligencia empresarial atractivas y potentes para la red, los escritorios virtuales, las aplicaciones y la estructura de aplicaciones. HDX Insight puede analizar al instante los problemas de los usuarios, recopilar datos sobre las conexiones de escritorio virtual y generar registros de AppFlow y presentarlos como informes visuales.

La configuración para habilitar la recopilación de datos en Citrix ADC difiere según la posición del dispositivo en la topología de implementación.

## Habilitar la recopilación de datos para monitorear los dispositivos de Citrix ADC implementados en modo de usuario LAN

Los usuarios externos que accedan a las aplicaciones de escritorio y aplicaciones virtuales de Citrix deben autenticarse en Citrix Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a Citrix Gateway. Además, en una implementación de modo transparente, el administrador debe aplicar manualmente las directivas de redirección para que las solicitudes se redirijan al dispositivo Citrix ADC.

Para superar estos desafíos y para que los usuarios de LAN se conecten directamente a las aplicaciones Citrix Virtual App y Desktop, puede implementar el dispositivo Citrix ADC en modo de usuario LAN configurando un servidor virtual de redirección de caché, que actúa como proxy SOCKS en el dispositivo Citrix Gateway.

> **Nota** Citrix ADM y el dispositivo Citrix Gateway residen en la misma subred.

Para supervisar los dispositivos Citrix ADC implementados en este modo, primero agregue el dispositivo Citrix ADC al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel.

Después de agregar el dispositivo Citrix ADC al inventario de Citrix ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - En una instancia de ADC, puede desplazarse a **Sistema > AppFlow > Colectores**para comprobar si el recopilador (es decir, NetScaler ADM) está o no. La instancia Citrix ADC envía

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

registros AppFlow a Citrix ADM mediante NSIP. Sin embargo, la instancia usa su SNIP para verificar la conectividad con Citrix ADM. Por lo tanto, asegúrese de que el SNIP esté configurado en la instancia.

- No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo de usuario de LAN mediante la utilidad de configuración de Citrix ADM.
- Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
- Para obtener información sobre las expresiones de directiva, consulteDirectivas y expresiones.

**Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:**

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [ - cltTimeout <secs>]
```

Ejemplo

```
add cr vserver cr1 HDX 10.12.2.2 443 – cacheType FORWARD – cltTimeout 180
```

> **Nota:** Si accede a la red LAN mediante un dispositivo Citrix Gateway, agregue una acción para que la aplique una directiva que coincida con el tráfico de la VPN.

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
```

Ejemplo

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Agregue Citrix ADM como un recopilador AppFlow en el dispositivo Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
```

Example:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string>
```

Ejemplo :

```
add appflow action act -collectors MyInsight
```

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
```

Ejemplo :

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
```

Ejemplo :

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Nota**
>
> El valor de tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicar al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

Ejemplo :

```
set appflow param -flowRecordInterval 60
```

8. Guarde la configuración. Tipo: `save ns config`

### Habilitar la recopilación de datos para los dispositivos Citrix Gateway implementados en modo de salto único

Cuando implementa Citrix Gateway en modo de salto único, se encuentra en el borde de la red. La instancia de Gateway proporciona conexiones ICA de proxy a la infraestructura de entrega de escritorio. El salto único es la implementación más simple y común. El modo de salto único proporciona

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

seguridad si un usuario externo intenta acceder a la red interna de una organización.
En el modo de salto único, los usuarios acceden a los dispositivos Citrix ADC a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo Citrix Gateway al inventario de Citrix Application Delivery Management (ADM) y habilitar AppFlow en ADM.

**Para habilitar la función AppFlow desde Citrix ADM:**

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.
4. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar análisis**.
6. Seleccione **HDX Insight** y, a continuación, **ICA**.
7. Haga clic en **Aceptar**.

> **Nota**
>
> cuando habilita AppFlow en modo de salto único, los siguientes comandos se ejecutan en segundo plano. Estos comandos se especifican explícitamente aquí para solucionar problemas.

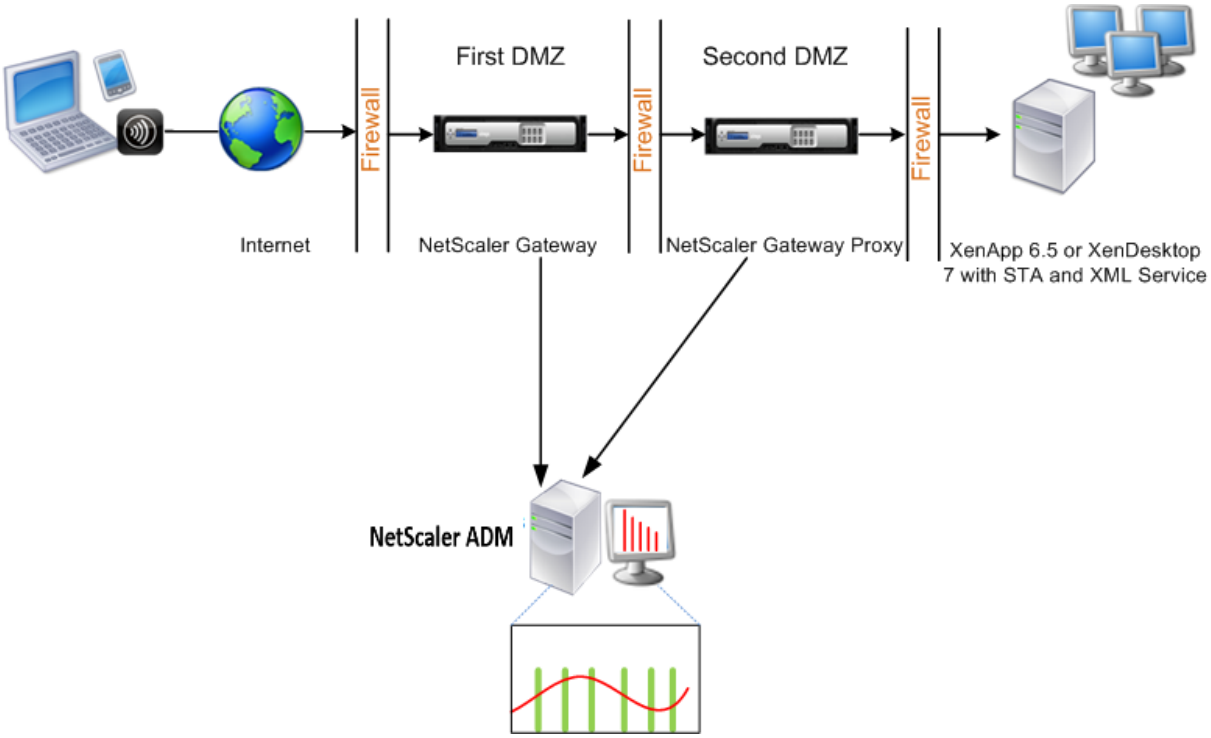
```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  enable ns feature AppFlow
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
```

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual de EUEM no está habilitado, los datos restantes de HDX Insight se mostrarán en Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Habilitar la recopilación de datos para los dispositivos Citrix Gateway implementados en modo de doble salto

El modo de salto doble de Citrix Gateway proporciona protección adicional a la red interna de una organización porque un atacante necesitaría penetrar varias zonas de seguridad o zonas desmilitarizadas (DMZ) para llegar a los servidores de la red segura. Si quiere analizar el número de saltos (dispositivos Citrix Gateway) a través de los cuales pasan las conexiones ICA, así como los detalles sobre la latencia en cada conexión TCP y cómo se compara con la latencia total de ICA percibida por el cliente, debe instalar Citrix ADM para que los dispositivos Citrix Gateway reportar estas estadísticas vitales.




Citrix Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Citrix Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

Citrix Gateway en la segunda DMZ sirve como dispositivo proxy de Citrix Gateway. Este Citrix Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El Citrix ADM se puede implementar en la subred que pertenece al dispositivo Citrix Gateway en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo Citrix Gateway. En la imagen de arriba, Citrix ADM y Citrix Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, Citrix ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Después de agregar los dispositivos Citrix Gateway al inventario de Citrix ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

y habilitar la recopilación de datos, cada uno de los dispositivos exporta los informes realizando un seguimiento del recuento de saltos y del ID de la cadena de conexiones.

Para que Citrix ADM identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un ID de cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos Citrix Gateway a través de los cuales fluye el tráfico desde un cliente a los servidores. El ID de cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos Citrix Gateway y generar los informes.

Para supervisar los dispositivos Citrix Gateway implementados en este modo, primero debe agregar Citrix Gateway al inventario de Citrix ADM, habilitar AppFlow en Citrix ADM y, a continuación, ver los informes en el panel de Citrix ADM.

## Configure HDX Insight en los servidores virtuales utilizados para Optimal Gateway

Pasos para configurar HDX Insight en servidores virtuales utilizados para Optimal Gateway:

1. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione el servidor virtual VPN configurado para la autenticación y haga clic en **Habilitar análisis**.
4. Seleccione **HDX Insight** y, a continuación, **ICA**.
5. Seleccione otras opciones avanzadas según sea necesario.
6. Haga clic en **Aceptar**.
7. Repita los pasos 3 a 6 en el otro servidor virtual VPN.

### Habilitar la recopilación de datos en Citrix ADM

Si habilita Citrix ADM para comenzar a recopilar los detalles de ICA de ambos dispositivos, los detalles recopilados serán redundantes. Es decir, tanto los dispositivos informan de las mismas métricas. Para superar esta situación, debe habilitar AppFlow para ICA en uno de los primeros dispositivos Citrix Gateway y, a continuación, habilitar AppFlow para TCP en el segundo dispositivo. Al hacerlo, uno de los dispositivos exporta registros ICA AppFlow y el otro dispositivo exporta registros TCP AppFlow. Esto también ahorra tiempo de procesamiento al analizar el tráfico ICA.

**Para habilitar la función AppFlow desde Citrix ADM:**

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Instancias** y seleccione la instancia de Citrix ADC que quiere habilitar el análisis.
4. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
5. Seleccione los servidores virtuales VPN y haga clic en **Habilitar análisis**.
6. Seleccione **HDX Insight** y, a continuación, seleccione **ICA** o **TCP** para el tráfico ICA o el tráfico TCP, respectivamente.

   > **Nota**
   >
   > Si el registro de AppFlow no está habilitado para los servicios o grupos de servicios respectivos en el dispositivo Citrix ADC, el panel Citrix ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

7. Haga clic en **Aceptar**.

#### Configuración de dispositivos Citrix Gateway para exportar datos

Después de instalar los dispositivos Citrix Gateway, debe configurar las siguientes opciones en los dispositivos Citrix Gateway para exportar los informes a Citrix ADM:

- Configure los servidores virtuales de los dispositivos Citrix Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ.
- Habilite el salto doble en Citrix Gateway en la segunda DMZ.
- Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
- Habilite uno de los dispositivos Citrix Gateway para exportar registros ICA
- Habilite el otro dispositivo Citrix Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

**Configure Citrix Gateway mediante la interfaz de línea de comandos:**

1. Configure el servidor virtual de Citrix Gateway en la primera DMZ para comunicarse con el servidor virtual de Citrix Gateway en la segunda DMZ.

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443  – secure ON
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ. Ejecute el siguiente comando en Citrix Gateway en la primera DMZ:

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. Habilite el salto doble y AppFlow en Citrix Gateway en la segunda DMZ.

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 – doubleHop ENABLED – appFlowLog ENABLED
```

4. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 – type
    OTHERTCP_REQUEST
```

6. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway:

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

**Configurar Citrix Gateway mediante la Utilidad de configuración:**

1. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda **Aplicaciones publicadas**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

   c) Haga clic en**Servidor de salto siguiente** y vincule un servidor de salto siguiente al segundo dispositivo Citrix Gateway.

2. Habilite el salto doble en Citrix Gateway en la segunda DMZ.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.

   c) Amplíe más, seleccione**Double Hop**y haga clic en**Aceptar**.

3. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.

   c) Amplíe**más**y desactive la opción**Habilitar autenticación**.

4. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda Directivas.

   c) Haga clic en el icono + y, en la lista**Elegir directiva**, seleccione**AppFlow**y, en la lista **Elegir tipo**, seleccione**Otra solicitud de TCP**.

   d) Haga clic en **Continuar**.

   e) Agregue un enlace de directiva y haga clic en **Cerrar**.

5. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Avanzado**, expanda**Directivas**.

   c) Haga clic en el icono + y, en la lista**Elegir directiva**, seleccione AppFlow y, en la lista Elegir tipo, seleccione**Otra**solicitud de TCP.

   d) Haga clic en **Continuar**.

   e) Agregue un enlace de directiva y haga clic en **Cerrar**.

6. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

   a) En la ficha **Configuración**, vaya a **Sistema** > **Appflow**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) En el panel derecho, en el grupo**Configuración**, haga doble clic en**Cambiar la configuración de Appflow**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

7. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.

   a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el **grupo Avanzado** , expanda **Aplicaciones publicadas** .

   c) Haga clic en**Servidor de siguiente salto**y vincule un servidor de siguiente salto al segundo dispositivo Citrix Gateway.

8. Habilite el salto doble en Citrix Gateway en la segunda DMZ.

   a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Configuración básica**, haga clic en el icono de edición.

   c) Amplíe Más, seleccione**Double Hop**y pulse**Aceptar**.

9. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

   a) En la pestaña Configuración , expanda Citrix Gateway y haga clic en **Servidores virtuales** .

   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo **Configuración básica**, haga clic en el icono de edición.

   c) Amplíe**más**y desactive la opción**Habilitar autenticación**.

10. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

    a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

    b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda **Directivas**.

    c) Haga clic en el icono**+**y, en la lista Elegir directiva, seleccione AppFlow y, en la lista **Elegir tipo**, seleccione**Otra solicitud de TCP**.

    d) Haga clic en **Continuar**.

    e) Agregue un enlace de directiva y haga clic en **Cerrar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

11. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA.

    a) En la pestaña Configuración , expanda **Citrix Gateway** y haga clic en **Servidores virtuales** .

    b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda**Directivas**.

    c) Haga clic en el icono**+**y, en la lista**Elegir directiva**, seleccione AppFlow y, en la lista **Elegir tipo**, seleccione**Otra solicitud de TCP**.

    d) Haga clic en **Continuar**.

    e) Agregue un enlace de directiva y haga clic en **Cerrar**.

12. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

## Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo transparente

Cuando un Citrix ADC se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un dispositivo Citrix ADC se implementa en modo transparente en un entorno de Citrix Virtual Apps and Desktop, el tráfico ICA no se transmite a través de una VPN.

Después de agregar Citrix ADC al inventario Citrix ADM, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe agregar Citrix ADM como un recopilador de AppFlow en cada dispositivo Citrix ADC y debe configurar una directiva de AppFlow para recopilar todo o el tráfico ICA específico que fluye a través del dispositivo.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo transparente mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
> - Para obtener información sobre las expresiones de directiva, consulteDirectivas y expresiones.

La siguiente ilustración muestra la implementación en red de un Citrix ADM cuando un Citrix ADC se implementa en modo transparente:

**Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:**

En el símbolo del sistema, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Inicie sesión en un dispositivo.
2. Especifique los puertos ICA en los que el dispositivo Citrix ADC escucha el tráfico.

```
set ns param --icaPorts <port>...
```

**Ejemplo:**

```
set ns param -icaPorts 2598 1494
```

> **Nota**
>
> - Puede especificar hasta 10 puertos con este comando.
> - El número de puerto predeterminado es 2598. Puede modificar el número de puerto según sea necesario.

3. Agregue NetScaler Insight Center como un recopilador AppFlow en el dispositivo Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
```

**Ejemplo:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Nota** Para ver los recopiladores AppFlow configurados en el dispositivo Citrix ADC, utilice el comando**show appflow collector**.

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
```

**Ejemplo:**

agregar acción AppFlow act-colectores MyInsight

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
```

**Ejemplo:**

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
```

**Ejemplo:**

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El valor de **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarlo al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

**Ejemplo:**

```
set appflow param -flowRecordInterval 60
```

8. Guarde la configuración. Tipo: `save ns config`

## Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto único

January 30, 2024

Cuando implementa Citrix Gateway en modo de salto único, se encuentra en el borde de la red. La instancia de Gateway proporciona conexiones ICA de proxy a la infraestructura de entrega de escritorio. El salto único es la implementación más simple y común. El modo de salto único proporciona seguridad si un usuario externo intenta acceder a la red interna de una organización.
En el modo de salto único, los usuarios acceden a los dispositivos Citrix ADC a través de una red privada virtual (VPN).

Para empezar a recopilar los informes, debe agregar el dispositivo Citrix Gateway al inventario de Citrix Application Delivery Management (ADM) y habilitar AppFlow en ADM.

**Para habilitar la función AppFlow desde ADM:**

1. Vaya a **Infraestructura** > **Instancias** y seleccione la instancia de NetScaler ADC que quiere habilitar el análisis.
2. En la lista **Acción**, seleccione **Activar/Desactivar Insight**.
3. Seleccione los **servidores virtuales VPN** y haga clic en **Habilitar AppFlow** .
4. En el campo **Habilitar AppFlow**, escriba **true** y seleccione **ICA**.
5. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Cuando habilita AppFlow en modo de salto único, los siguientes comandos se ejecutan en segundo plano. Estos comandos se especifican explícitamente aquí para solucionar problemas.
>
> - `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
> - `add appflow action \<name\> -collectors \<string\>`
> - `set appflow param -flowRecordInterval \<secs\>`
> - `disable ns feature AppFlow`
> - `enable ns feature AppFlow`
> - `add appflow policy \<name\> \<rule\> \<expression\>`
> - `set appflow policy \<name\> -rule \<expression\>`
> - `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >-priority \<positive\\_integer\>`
> - `set vpn vserver \<name\> -appflowLog ENABLED`
> - `save ns config`

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual de EUEM no está habilitado, los datos restantes de HDX Insight se mostrarán en Citrix ADM.

## Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo transparente

January 30, 2024

Cuando un Citrix ADC se implementa en modo transparente, los clientes pueden acceder a los servidores directamente, sin que intervenga ningún servidor virtual. Si un dispositivo de Citrix ADC se implementa en modo transparente en un entorno Citrix Virtual Apps and Desktops, el tráfico ICA no se transmite a través de una VPN.

Después de agregar Citrix ADC al inventario Citrix ADM, debe habilitar AppFlow para la recopilación de datos. Habilitar la recopilación de datos depende del dispositivo y del modo. En ese caso, debe agregar Citrix ADM como recopilador de AppFlow en cada instancia de Citrix ADC y debe configurar una directiva de AppFlow para recopilar todo el tráfico ICA que fluye a través del dispositivo o uno específico.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo trans-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> parente mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte lareferencia de comandos.
> - Para obtener información sobre las expresiones de directiva, consulteDirectivas y expresiones.

La siguiente ilustración muestra la implementación en red de un Citrix ADM cuando un Citrix ADC se implementa en modo transparente:

**Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:**

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Especifique los puertos ICA en los que el dispositivo Citrix ADC escucha el tráfico.

```
set ns param --icaPorts \<port\>...
```

**Ejemplo:**

```
set ns param -icaPorts 2598 1494
```

> **Nota**
>
> - Puede especificar hasta 10 puertos con este comando.
> - El número de puerto predeterminado es 2598. Puede modificar el número de puerto según sea necesario.

3. Agregue NetScaler Insight Center como un recopilador de AppFlow en la instancia de Citrix ADC.

```
add appflow collector <name> -IPAddress <ip_addr>
```

**Ejemplo:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> **Nota** Para ver los recopiladores AppFlow configurados en la instancia de Citrix ADC, utilice el comando**show appflow collector**.

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action <name> -collectors <string> ...
```

**Ejemplo:**

```
add appflow action act -collectors MyInsight
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy <policyname> <rule> <action>
```

**Ejemplo:**

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global <policyname> <priority> -type <type>
```

**Ejemplo:**

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Nota**
>
> El valor de **tipo** debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicarlo al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

8. Guarde la configuración.

```
save ns config
```

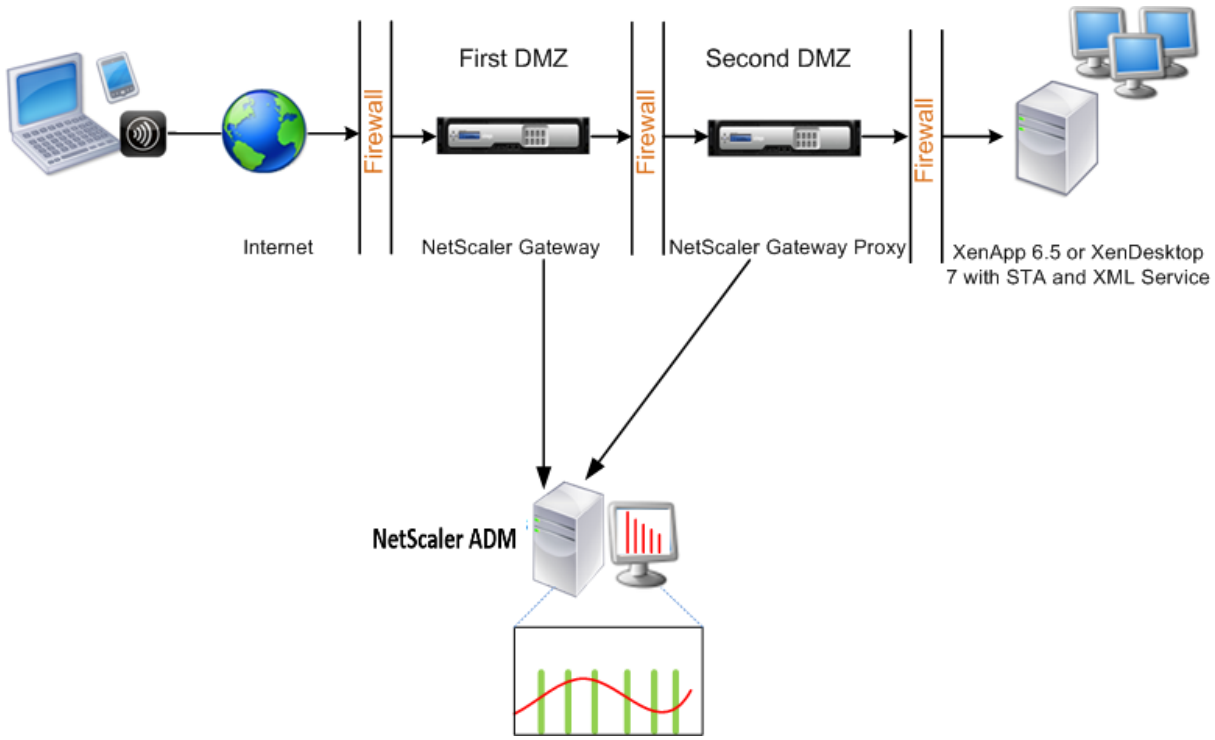
## Habilitar la recopilación de datos para dispositivos Citrix Gateway implementados en modo de salto doble

January 30, 2024

El modo de doble salto de Citrix Gateway proporciona protección adicional a la red interna de una organización, ya que un atacante tendría que penetrar en varias zonas de seguridad o zonas desmilitarizadas (DMZ) para llegar a los servidores de la red segura. Si quiere analizar el número de saltos (dispositivos Citrix Gateway) por los que pasan las conexiones ICA y también los detalles sobre la latencia de cada conexión TCP y cómo se compara con la latencia ICA total percibida por el cliente, debe instalar Citrix ADM para que los dispositivos Citrix Gateway informen de estas estadísticas vitales.

Figura 3 . Citrix ADM implementado en modo de salto doble

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Citrix Gateway en la primera DMZ maneja las conexiones de usuario y realiza las funciones de seguridad de una VPN SSL. Citrix Gateway cifra las conexiones de los usuarios, determina cómo se autentican los usuarios y controla el acceso a los servidores de la red interna.

Citrix Gateway en la segunda DMZ sirve como dispositivo proxy de Citrix Gateway. Este Citrix Gateway permite que el tráfico ICA atraviese la segunda DMZ para completar las conexiones de usuario a la comunidad de servidores.

El Citrix ADM se puede implementar en la subred que pertenece al dispositivo Citrix Gateway en la primera DMZ o en la subred que pertenece a la segunda DMZ del dispositivo Citrix Gateway. En la imagen de arriba, Citrix ADM y Citrix Gateway de la primera DMZ se implementan en la misma subred.

En modo de salto doble, Citrix ADM recopila los registros TCP de un dispositivo y los registros ICA del otro dispositivo. Después de agregar los dispositivos Citrix Gateway al inventario de Citrix ADM y habilitar la recopilación de datos, cada dispositivo exporta los informes haciendo un seguimiento del recuento de saltos y el ID de cadena de conexión.

Para que Citrix ADM identifique qué dispositivo está exportando registros, cada dispositivo se especifica con un recuento de saltos y cada conexión se especifica con un ID de cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos Citrix Gateway a través de los cuales fluye el tráfico desde un cliente a los servidores. El ID de cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos Citrix Gateway y generar los informes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para supervisar los dispositivos Citrix Gateway implementados en este modo, primero debe agregar Citrix Gateway al inventario de Citrix ADM, habilitar AppFlow en Citrix ADM y, a continuación, ver los informes en el panel de Citrix ADM.

## Habilitar la recopilación de datos en Citrix ADM

Si habilita Citrix ADM para comenzar a recopilar los detalles de ICA de ambos dispositivos, los detalles recopilados serán redundantes. Es decir, tanto los dispositivos informan de las mismas métricas. Para superar esta situación, debe habilitar AppFlow para TCP en uno de los primeros dispositivos Citrix Gateway y, a continuación, habilitar AppFlow para ICA en el segundo dispositivo. Al hacerlo, uno de los dispositivos exporta registros ICA AppFlow y el otro dispositivo exporta registros TCP AppFlow. Esto también ahorra tiempo de procesamiento al analizar el tráfico ICA.

**Para habilitar la función AppFlow desde Citrix ADM:**

1. Vaya a **Infraestructura > Instancias**y seleccione la instancia de Citrix ADC en la que quiere habilitar el análisis.
2. En la lista **Acción**, seleccione **Activar/Desactivar Insight**.
3. Seleccione los servidores virtuales VPN y haga clic en **Habilitar AppFlow**.
4. En el campo **Habilitar AppFlow**, escriba **true**y seleccione **ICA/TCP** para el tráfico ICA un tráfico TCP respectivamente.

   > **Nota**
   >
   > Si el registro de AppFlow no está habilitado para los servicios o grupos de servicios del dispositivo Citrix ADC, el panel de control de Citrix ADM no muestra los registros, incluso si la columna Insight muestra Habilitado.

5. Haga clic en **Aceptar**.

## Configurar los dispositivos Citrix Gateway para exportar datos

Después de instalar los dispositivos Citrix Gateway, debe configurar las siguientes opciones en los dispositivos Citrix Gateway para exportar los informes a Citrix ADM:

- Configure los servidores virtuales de los dispositivos Citrix Gateway en la primera y la segunda DMZ para que se comuniquen entre sí.
- Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ.
- Habilite el salto doble en Citrix Gateway en la segunda DMZ.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
- Habilite uno de los dispositivos Citrix Gateway para exportar registros ICA
- Habilite el otro dispositivo Citrix Gateway para exportar registros TCP:
- Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

**Configure Citrix Gateway mediante la interfaz de línea de comandos:**

1. Configure el servidor virtual de Citrix Gateway en la primera DMZ para comunicarse con el servidor virtual de Citrix Gateway en la segunda DMZ.

**add vpn nextHopServer** [**-secure**(ON OFF)] [**-imgGifToPng**] ...

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
```

2. Enlazar el servidor virtual de Citrix Gateway en la segunda DMZ con el servidor virtual de Citrix Gateway en la primera DMZ. Ejecute el siguiente comando en Citrix Gateway en la primera DMZ:

   **bind vpn vserver** <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
```

3. Habilite el salto doble y AppFlow en Citrix Gateway en la segunda DMZ.

**set vpn vserver** [**-doubleHop** (ENABLED DISABLED)] [**-appflowLog** (ENABLED DISABLED)]

```
set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
```

4. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.

**set vpn vserver** [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
```

5. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.

   **bind vpn vserver**<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
    OTHERTCP_REQUEST
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

6. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

   **bind vpn vserver**<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway:

**set appFlow** DISABLED)]
**param** [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
```

**Configuración de Citrix Gateway mediante la utilidad de configuración:**

1. Configure Citrix Gateway en la primera DMZ para comunicarse con Citrix Gateway en la segunda DMZ y enlazar Citrix Gateway en la segunda DMZ a Citrix Gateway en la primera DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda **Aplicaciones publicadas**.
   c) Haga clic en**Servidor de salto siguiente** y vincule un servidor de salto siguiente al segundo dispositivo Citrix Gateway.
2. Habilite el salto doble en Citrix Gateway en la segunda DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.
   c) Expanda **Más**, seleccione **Doble salto** y haga clic en **Aceptar**.
3. Inhabilite la autenticación en el servidor virtual de Citrix Gateway en la segunda DMZ.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.
   b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Configuración básica**, haga clic en el icono de edición.
   c) Amplíe**más**y desactive la opción**Habilitar autenticación**.
4. Habilite uno de los dispositivos Citrix Gateway para exportar registros TCP.
   a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo Avanzado, expanda Directivas.

c) Haga clic en el icono + y, en la lista**Elegir directiva**, seleccione**AppFlow**y, en la lista desplegable**Elegir tipo**, seleccione**Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

5. Habilite el otro dispositivo Citrix Gateway para exportar registros ICA:

a) En la ficha **Configuración**, expanda **Citrix Gateway** y haga clic en **Servidores virtuales**.

b) En el panel derecho, haga doble clic en el servidor virtual y, en el grupo**Avanzado**, expanda **Directivas**.

c) Haga clic en el icono + y, en la lista desplegable **Elegir directiva**, seleccione **AppFlow**y, en la lista desplegable Elegir tipo, seleccione **Otra solicitud TCP**.

d) Haga clic en **Continuar**.

e) Agregue un enlace de directiva y haga clic en **Cerrar**.

6. Habilite el encadenamiento de conexiones en ambos dispositivos Citrix Gateway.

a) En la ficha **Configuración**, vaya a **Sistema > Appflow**.

b) En el panel derecho, en el grupo**Configuración**, haga clic en**Cambiar configuración del flujo de aplicaciones**.

c) Seleccione **Conexión encadenamiento** y haga clic en **Aceptar**.

## Habilitar la recopilación de datos para supervisar los dispositivos de Citrix ADC implementados en modo de usuario LAN

January 30, 2024

Los usuarios externos que acceden a las aplicaciones Citrix Virtual App o Desktop deben autenticarse en Citrix Gateway. Sin embargo, es posible que los usuarios internos no necesiten ser redirigidos a Citrix Gateway. Además, en una implementación de modo transparente, el administrador debe aplicar manualmente las directivas de redirección para que las solicitudes se redirijan al dispositivo Citrix ADC.

Para superar estos desafíos y para que los usuarios de LAN se conecten directamente a aplicaciones de Citrix Virtual Apps and Desktops, puede implementar el dispositivo Citrix ADC en modo de usuario

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

de LAN configurando un servidor virtual de redirección de caché, que actúa como proxy SOCKS en el dispositivo Citrix Gateway.

Figura 4 . Citrix ADM implementado en modo de usuario de LAN

**Nota** Citrix ADM y el dispositivo Citrix Gateway residen en la misma subred.

Para supervisar los dispositivos Citrix ADC implementados en este modo, primero agregue el dispositivo Citrix ADC al inventario de NetScaler Insight, habilite AppFlow y, a continuación, consulte los informes en el panel.

Después de agregar el dispositivo Citrix ADC al inventario de Citrix ADM, debe habilitar AppFlow para la recopilación de datos.

> **Nota**
>
> - No puede habilitar la recopilación de datos en un Citrix ADC implementado en modo de usuario de LAN mediante la utilidad de configuración de Citrix ADM.
> - Para obtener información detallada sobre los comandos y su uso, consulte Referencia de comandos .
> - Para obtener información sobre las expresiones de políticas, consulte Políticas y expresiones .

**Para configurar la recopilación de datos en un dispositivo Citrix ADC mediante la interfaz de línea de comandos:**

En el símbolo del sistema, haga lo siguiente:

1. Inicie sesión en un dispositivo.
2. Agregue un servidor virtual de redirección de caché de proxy de reenvío con la IP y el puerto proxy, y especifique el tipo de servicio como HDX.

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
    cacheType <cachetype>] [ - cltTimeout <secs>]
```

**Ejemplo:**

```
add cr vserver cr1 HDX 10.12.2.2 443  – cacheType FORWARD  –
    cltTimeout 180
```

> **Nota** Si accede a la red LAN mediante un dispositivo Citrix Gateway, agregue una acción que aplique una directiva que coincida con el tráfico VPN.

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
```

**Ejemplo:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
```

3. Agregue Citrix ADM como un recopilador AppFlow en el dispositivo Citrix ADC.

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
```

**Ejemplo:**

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

4. Cree una acción AppFlow y asocie el recopilador con la acción.

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
```

**Ejemplo:**

```
add appflow action act -collectors MyInsight
```

5. Cree una directiva de AppFlow para especificar la regla para generar el tráfico.

```
add appflow policy** \<policyname\> \<rule\> \<action\>
```

**Ejemplo:**

```
add appflow policy pol true act
```

6. Enlace la directiva de AppFlow a un punto de enlace global.

```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
    type\>
```

**Ejemplo:**

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> **Nota**
>
> El valor de tipo debe ser ICA_REQ_OVERRIDE o ICA_REQ_DEFAULT para aplicar al tráfico ICA.

7. Establezca el valor del parámetro flowRecordInterval para AppFlow en 60 segundos.

```
set appflow param -flowRecordInterval 60
```

**Ejemplo:**

```
set appflow param -flowRecordInterval 60
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. Guarde la configuración.

```
save ns config
```

## Crear umbrales y configurar alertas para HDX Insight

January 30, 2024

HDX Insight en Citrix Application Delivery Management (ADM) le permite supervisar el tráfico HDX que pasa por las instancias de Citrix ADC. Citrix ADM le permite establecer umbrales en varios contadores utilizados para supervisar el tráfico de Insight. También puede configurar reglas y crear alertas en Citrix ADM.

El tipo de tráfico HDX está asociado con varias entidades, como aplicaciones, escritorios, puertas de enlace, licencias y usuarios. Cada entidad puede contener diferentes métricas asociadas a ellas. Por ejemplo, la entidad de aplicación está asociada con varios accesos, ancho de banda consumido por la aplicación y tiempo de respuesta del servidor. Una entidad de usuario puede asociarse con latencia de WAN, latencia DC, RTT ICA y ancho de banda consumido por un usuario.

La administración de umbrales de HDX Insight en Citrix ADM le permitió crear reglas y configurar alertas de forma proactiva cada vez que se superaban los umbrales establecidos. Ahora, esta administración de umbrales se amplía para configurar un grupo de reglas de umbrales. Ahora puede supervisar el grupo en lugar de las reglas individuales. Un grupo de reglas de umbral comprende una o más reglas de umbral definidas por el usuario para las métricas elegidas de entidades como usuarios, aplicaciones y escritorios. Cada regla se controla con un valor esperado que se introduce al crear la regla. En el caso de una entidad de usuario, el grupo umbral también se puede asociar a una geolocalización.

Una alerta se genera en Citrix ADM solo si se incumplen todas las reglas del grupo de umbrales configurado. Por ejemplo, puede supervisar una aplicación según el recuento total de inicios de sesión y también el recuento de lanzamientos de aplicaciones como un grupo umbral. Solo se genera una alerta si se infringen ambas reglas. Esto le permite establecer umbrales más realistas en una entidad.

A continuación se enumeran algunos ejemplos:

- Regla de umbral 1: ICA RTT (métrica) para usuarios (entidad) debe ser <= 100 ms
- Regla de umbral2: La latencia WAN (métrica) para los usuarios (entidad) debe ser <= 100 ms

Un ejemplo de grupo de umbral puede ser: {Regla de umbral 1 + Regla de umbral 2}

Para crear una regla, primero debe seleccionar la entidad que quiere supervisar. A continuación, elija una métrica mientras crea una regla. Por ejemplo, puede seleccionar la entidad de aplicaciones y,

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a continuación, seleccionar Recuento total de inicio de sesión o Recuento de inicio de aplicaciones. Puede crear una regla para cada combinación de una entidad y una métrica. Utilice los comparadores proporcionados (>, <, >= y <=) y escriba un valor de umbral para cada métrica.

> **Nota**
>
> Si no quiere supervisar varias entidades en un solo grupo, debe crear un grupo de reglas de umbral independiente para cada entidad.

Cuando el valor de un contador supera el valor de un umbral, Citrix ADM genera un evento que indica una violación del umbral y se crea una alerta para cada evento.

Debe configurar cómo recibe la alerta. Puede habilitar la alerta para que se muestre en Citrix ADM o recibirla como correo electrónico o SMS en su dispositivo móvil. Para las dos últimas acciones, debe configurar el servidor de correo electrónico o el servidor de SMS en Citrix ADM.

Los grupos de umbral también se pueden vincular a las geolocalizaciones para el supervisión geoespecífico de la entidad de usuario.

## Ejemplos de casos de uso

ABC Inc. es una empresa global y tiene oficinas en más de 50 países. La firma cuenta con dos centros de datos, uno en Singapur y otro en California que albergan las Citrix Virtual Apps and Desktops. Los empleados de la empresa acceden a las Citrix Virtual Apps and Desktops de Citrix en todo el mundo mediante la redirección basada en Citrix Gateway y Citrix GSLB. Eric, el administrador de Citrix Virtual Apps and Desktops para ABC Inc. quiere realizar un seguimiento de la experiencia del usuario en todas sus oficinas para optimizar la entrega de aplicaciones y escritorios para acceder en cualquier lugar y en cualquier momento. Eric también quiere verificar las métricas de experiencia del usuario como RTT de ICA, latencias y plantear cualquier desviación de forma proactiva.

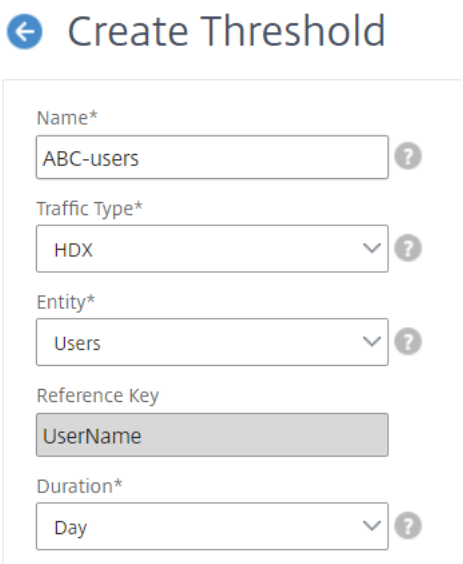
Los usuarios de ABC Inc. tienen una presencia distribuida. Algunos usuarios se encuentran cerca del centro de datos, mientras que algunos se encuentran en más lejos del centro de datos. Como la base de usuarios se distribuye ampliamente, las métricas y los umbrales correspondientes también varían entre estas ubicaciones. Por ejemplo, el ICA RTT para una ubicación cercana al centro de datos puede ser de 5 a 10 ms, mientras que el mismo para una ubicación remota puede ser de unos 100 ms.

Con la administración de grupos de reglas de umbral para HDX Insight, Eric puede establecer grupos de reglas de umbral geoespecíficos para cada ubicación y recibir alertas por correo electrónico o SMS sobre las infracciones por área. Eric también puede combinar el seguimiento de más de una métrica dentro de un grupo de reglas de umbral y reducir la causa raíz a los problemas de capacidad, en su caso. Eric ahora puede realizar un seguimiento proactivo de cualquier desviación sin tener que preocuparse por la complejidad de buscar manualmente todas las métricas de la cartera de Citrix Virtual Apps and Desktops.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para crear un grupo de reglas de umbral y configurar alertas para HDX Insight mediante Citrix ADM:**

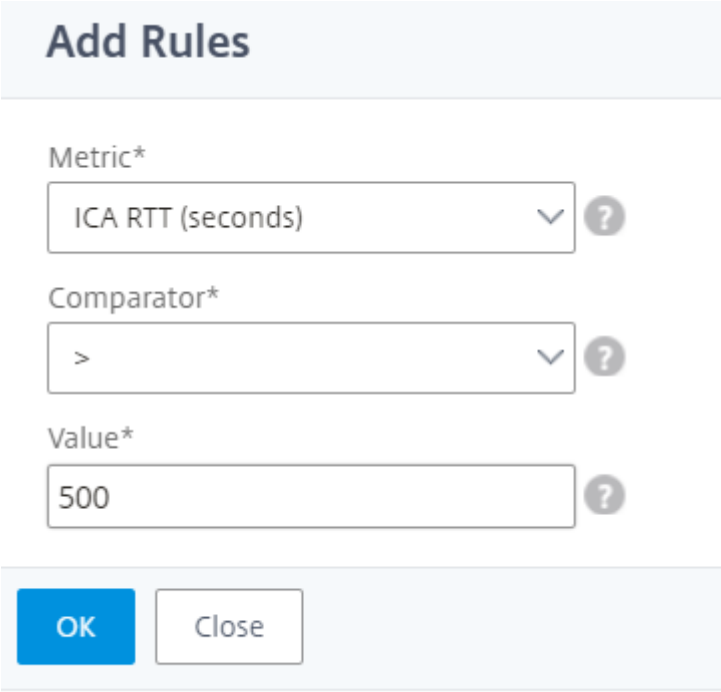
1. En Citrix ADM, vaya a **Analytics** > **Configuración** > **Umbrales**. En la página **Umbrales** que se abre, haga clic en **Agregar**.
2. En la página **Crear umbrales y alertas**, especifique los siguientes detalles:
   a) **Nombre**. Escriba un nombre para crear un evento para el que Citrix ADM genere una alerta.
   b) **Tipo de tráfico**. En el cuadro de lista, selecciona HDX.
   c) **Entidad**. En el cuadro de lista, seleccione la categoría o el tipo de recurso. Las entidades difieren para cada tipo de tráfico seleccionado anteriormente.
   d) **Clave de referencia**. Se genera automáticamente una clave de referencia en función del tipo de tráfico y la entidad que haya seleccionado.
   e) **Duración**. En el cuadro de lista, seleccione el intervalo de tiempo durante el que quiere supervisar la entidad. Puede supervisar las entidades durante una hora, un día o una semana de duración.



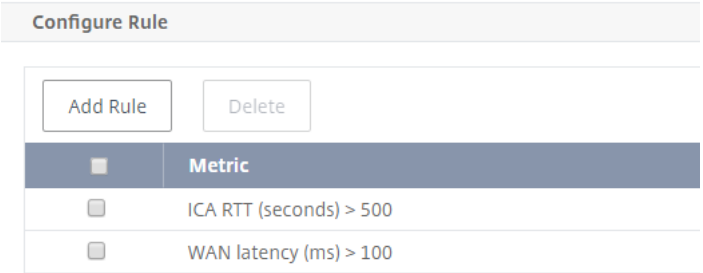

3. Creación de grupo de reglas de umbral para todas las entidades:

   Para el tráfico HDX, debe crear una regla haciendo clic en **Agregar regla.**Introduzca los valores en la ventana emergente **Agregar reglas** que se abre.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



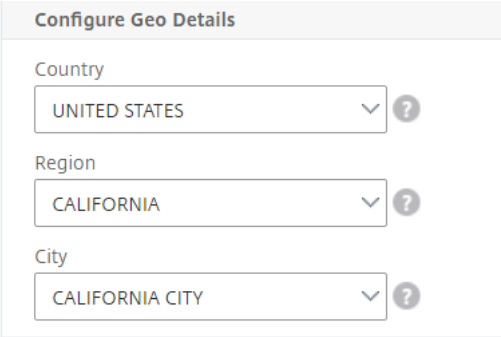

Puede crear varias reglas para supervisar cada entidad. La creación de varias reglas en un solo grupo le permite supervisar las entidades como un grupo de reglas de umbral en lugar de reglas individuales. Haga clic en **Aceptar** para cerrar la ventana.




4. Configuración del etiquetado de geolocalización para la entidad Usuarios

   Si lo quiere, puede crear una alerta basada en la ubicación para la entidad de usuario en la sección **Configurar detalles geográficos**. La siguiente imagen muestra un ejemplo de creación de un etiquetado basado en geolocalización para supervisar el rendimiento de latencia de WAN para los usuarios de la costa oeste de los Estados Unidos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Haga clic en **Habilitar umbrales** para permitir que Citrix ADM comience a supervisar las entidades.
6. Opcionalmente, configure acciones como notificaciones por correo electrónico y notificaciones por SMS.
7. Haga clic en **Crear** para crear un grupo de reglas de umbral.

## Visualización de informes y métricas de HDX Insight

January 30, 2024

HDX insight proporciona una visibilidad completa de los informes y las métricas relacionados con el tráfico HDX en sus instancias de NetScaler ADC.

Puede ver las métricas de HDX de cualquier entidad seleccionada. Las vistas incluyen las siguientes categorías de entidades:

- **Usuarios**: Muestra los informes de todos los usuarios que acceden a Citrix Virtual App o Desktop dentro del intervalo de tiempo seleccionado.
- **Aplicaciones**: muestra los informes del número total de aplicaciones y toda la información relevante relacionada, como el número total de veces que se lanzaron las aplicaciones dentro del intervalo de tiempo especificado.
- **Instancias**: Muestra los informes de las instancias NetScaler ADC que actúan como puertas de enlace para el tráfico entrante.
- **Escritorios**: muestra los informes de los escritorios utilizados en el período de tiempo seleccionado.
- **Licencias**: muestra los informes del total de licencias de VPN con SSL utilizadas dentro del intervalo de tiempo especificado.

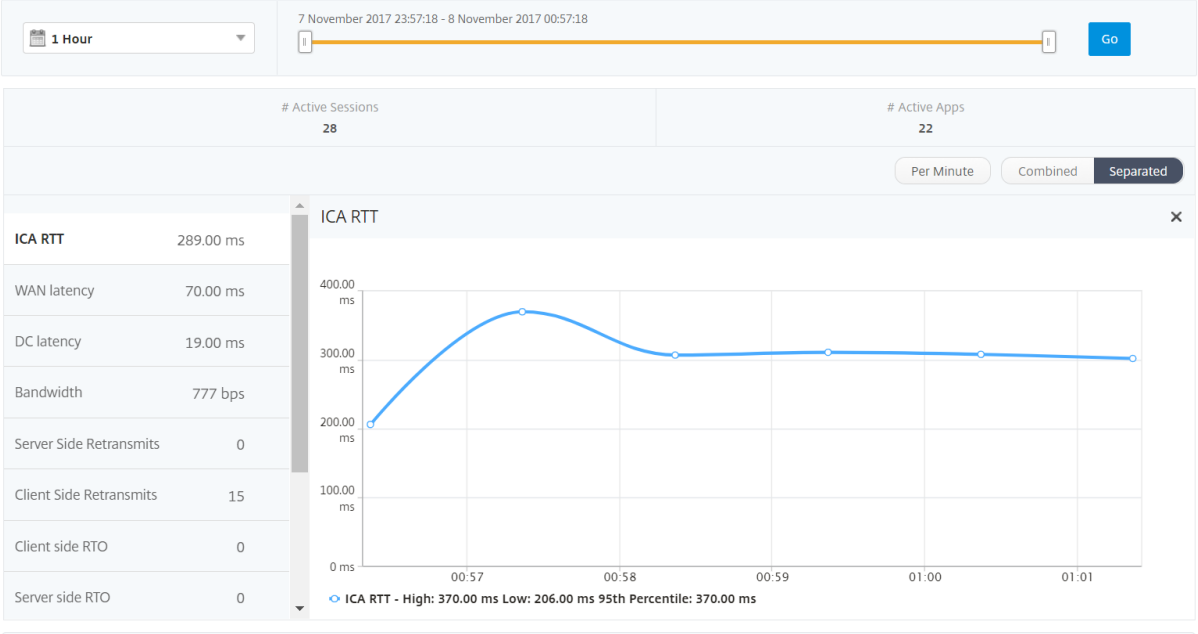
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El valor Licencias no se aplica a los dispositivos Citrix SD-WAN.

## Informes y métricas de visualización de usuarios

Los informes y métricas de esta vista se muestran por usuarios de Citrix Virtual Apps y Desktop.

Vaya a **Analytics** > **HDX Insight** > **Usuarios**.




Los informes de vista de usuario y las métricas constan de las siguientes secciones:

- Vista resumida
- Por vista de usuario
- Vista de sesión por usuario

### Vista de resumen

La vista de resumen muestra los informes de todos los usuarios que han iniciado sesión durante la línea de tiempo seleccionada. Todas las métricas e informes de esta vista muestran los valores correspondientes para el período de tiempo seleccionado, a menos que se especifique lo contrario.

**Para cambiar el período de tiempo seleccionado:**

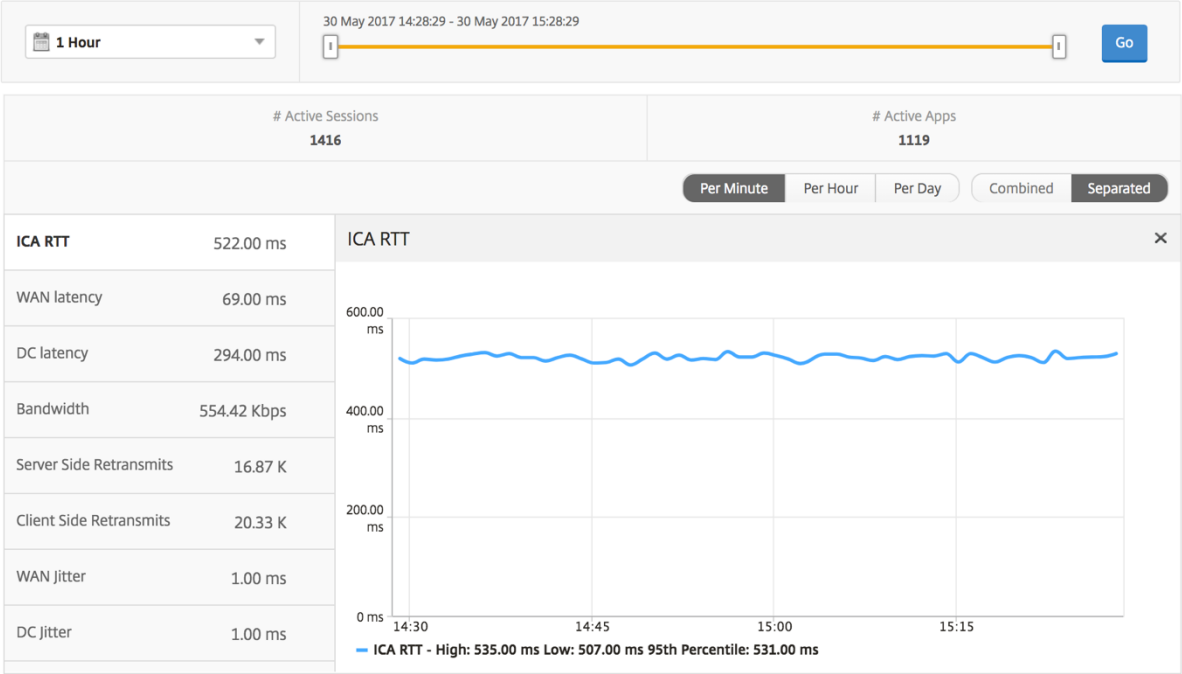
1. Utilice la lista de períodos de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.
2. Haga clic en **Ir**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico de líneas**

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Informe resumido de usuarios** A continuación se presentan las métricas específicas de este informe.

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Recuento total de aplicaciones iniciadas | Total de aplicaciones lanzadas por el usuario durante el período de tiempo seleccionado. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Escritorios activos | Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado. |

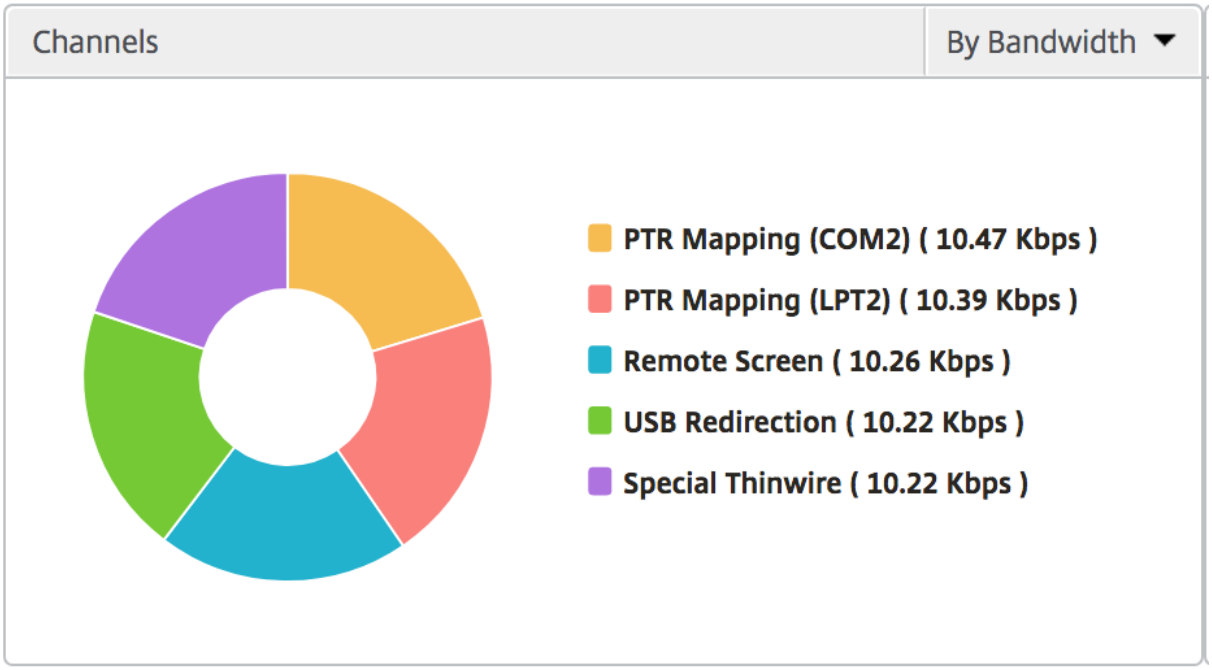
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Users

Search

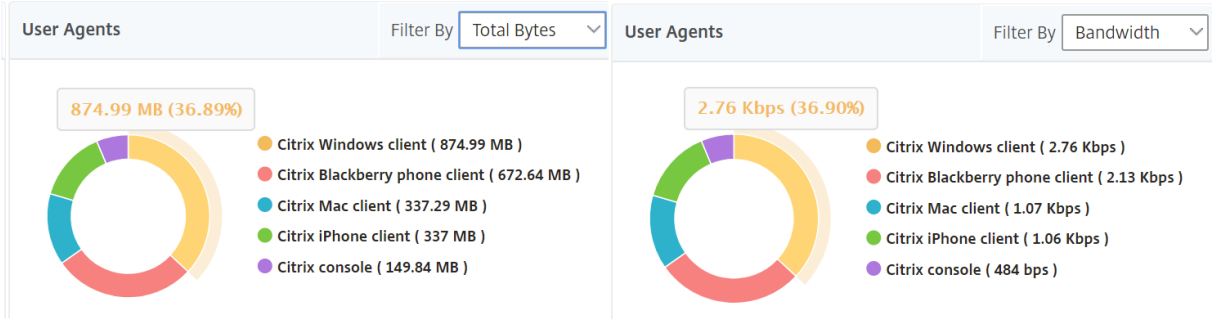
| User Name | # Active Apps | # Active Desktops | # Active Sessions | ICA RTT | WAN latency | DC latency | Bandwidth | Server Side Retransmits | Cl |
|---|---|---|---|---|---|---|---|---|---|
| liam | 59 | 59 | 118 | 999.00 ms | 57.00 ms | 751.00 ms | 47.25 Kbps | 3.74 K | |
| jayden | 59 | 59 | 118 | 999.00 ms | 52.00 ms | 751.00 ms | 47.06 Kbps | 3.71 K | |
| florinl | 59 | 0 | 59 | 997.00 ms | 52.00 ms | 754.00 ms | 23.66 Kbps | 1.88 K | |
| ramas | 59 | 0 | 59 | 997.00 ms | 778.00 ms | 1.00 ms | 7.03 Kbps | 0 | |
| omerp | 59 | 0 | 59 | 997.00 ms | 57.00 ms | 754.00 ms | 23.80 Kbps | 1.89 K | |
| grahmm | 59 | 0 | 59 | 997.00 ms | 53.00 ms | 754.00 ms | 23.80 Kbps | 1.89 K | |
| ryan | 59 | 0 | 59 | 997.00 ms | 53.00 ms | 754.00 ms | 23.69 Kbps | 1.88 K | |
| rajivs | 59 | 0 | 59 | 801.00 ms | 11.00 ms | 1.00 ms | 23.97 Kbps | 0 | |
| alexisc | 117 | 0 | 118 | 622.00 ms | 56.00 ms | 392.00 ms | 47.67 Kbps | 1.88 K | |
| juan | 59 | 59 | 118 | 169.00 ms | 31.00 ms | 29.00 ms | 47.72 Kbps | 0 | |
| lennoxl | 59 | 0 | 59 | 169.00 ms | 31.00 ms | 30.00 ms | 23.86 Kbps | 0 | |
| daniel | 59 | 59 | 118 | 149.00 ms | 31.00 ms | 29.00 ms | 47.72 Kbps | 0 | |
| woojunek | 58 | 0 | 59 | 149.00 ms | 31.00 ms | 30.00 ms | 23.85 Kbps | 0 | |
| parkerf | 59 | 0 | 59 | 149.00 ms | 31.00 ms | 30.00 ms | 23.88 Kbps | 0 | |
| randyb | 59 | 59 | 118 | 99.00 ms | 11.00 ms | 29.00 ms | 47.71 Kbps | 0 | |
| bradp | 177 | 0 | 177 | 74.00 ms | 27.00 ms | 1.00 ms | 71.75 Kbps | 0 | |

**Canales** Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.

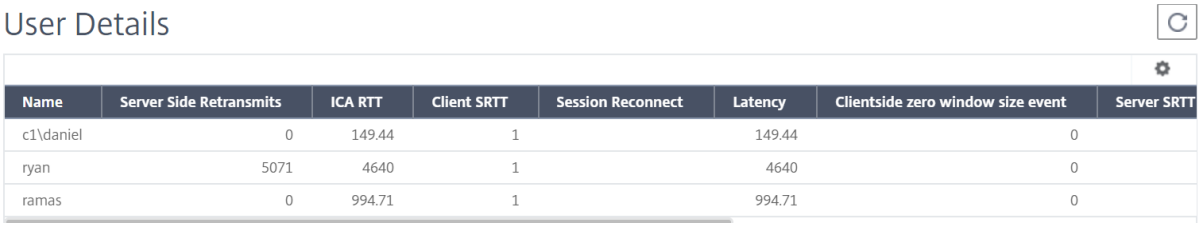



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Agentes de usuario** Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada cliente receptor en forma de gráfico de anillos. Cada segmento coloreado del gráfico representa un cliente receptor. La longitud del segmento depende de la cantidad de usuarios que inician sus aplicaciones en ese cliente receptor. También puede ordenar las métricas por ancho de banda o bytes totales.




Haga clic en cada segmento para ver los detalles de los usuarios que utilizan ese cliente receptor.



User Details

| Name | Server Side Retransmits | ICA RTT | Client SRTT | Session Reconnect | Latency | Clientside zero window size event | Server SRTT |
|---|---|---|---|---|---|---|---|
| c1\daniel | 0 | 149.44 | 1 | | 149.44 | 0 | |
| ryan | 5071 | 4640 | 1 | | 4640 | 0 | |
| ramas | 0 | 994.71 | 1 | | 994.71 | 0 | |

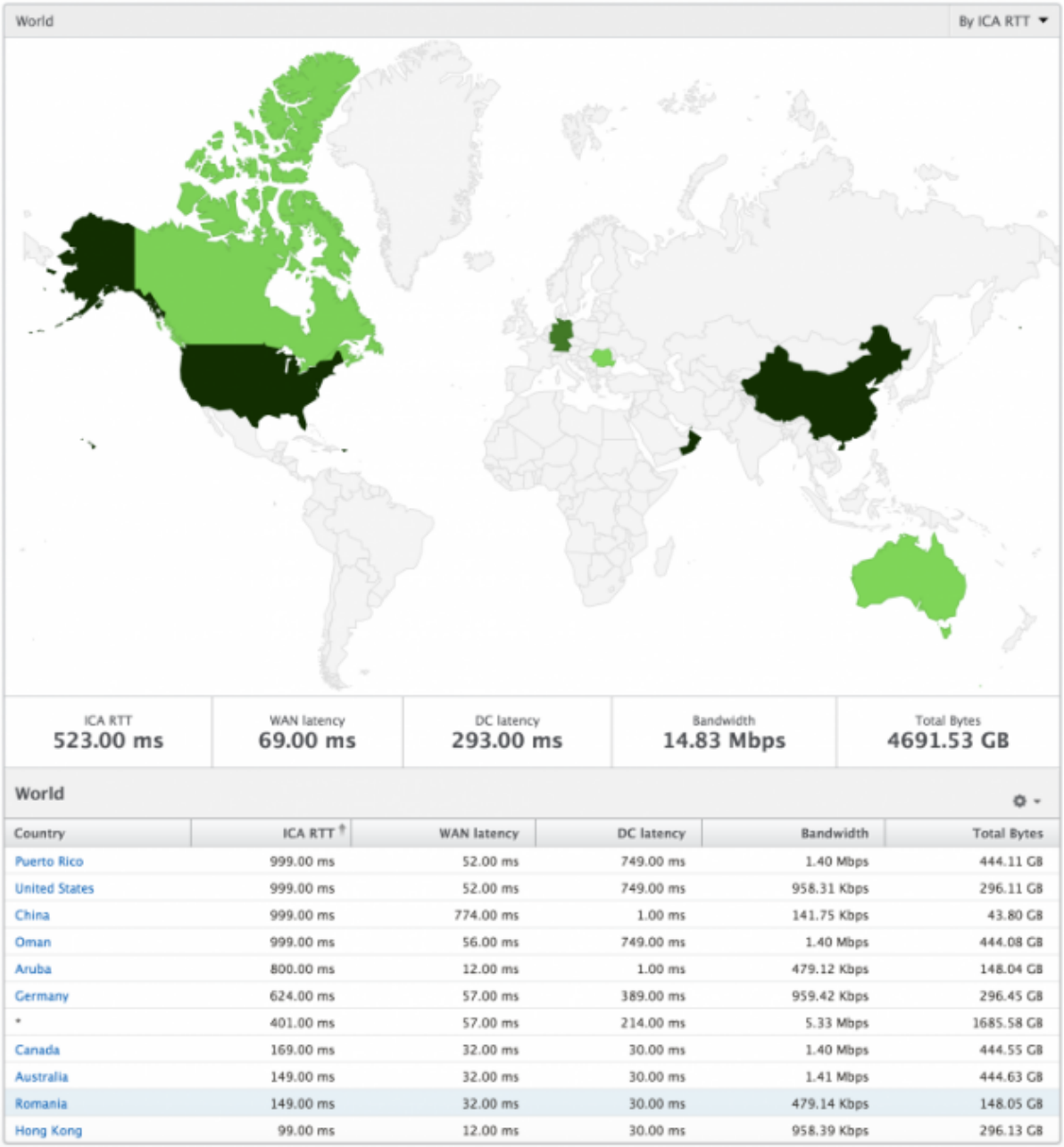
**Recuento de infracciones de umbrales** Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado.

**Mapa del mundo** La vista de mapa mundial en HDX Insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más en las ciudades, simplemente haciendo clic en la región. Los administradores pueden profundizar más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

### Por vista de usuario

La vista por usuario proporciona informes detallados de la experiencia del usuario final para cualquier usuario seleccionado en particular.

**Para navegar a métricas específicas de usuario:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Seleccione un usuario concreto en el informe Resumen de usuarios.

**Gráfico de líneas** El gráfico de líneas muestra el resumen de todas las métricas del usuario seleccionado en particular durante el período de tiempo seleccionado.

**Informe de sesiones actuales/terminadas** Este informe es pertinente para todas las sesiones de usuario actuales/terminadas del usuario seleccionado. Estas métricas se pueden ordenar por hora de inicio, reconexiones de sesión y recuento de ACR.

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

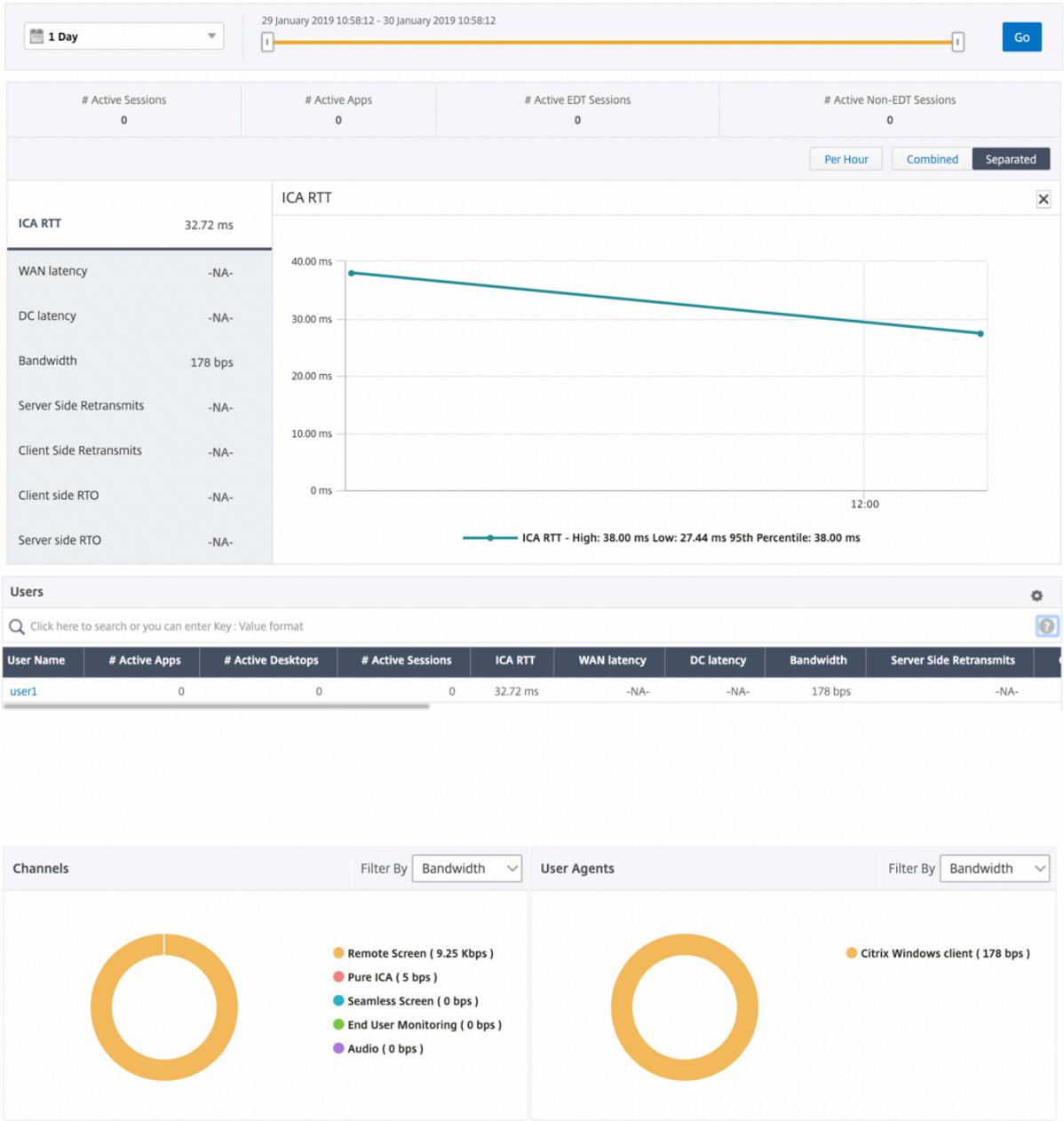
| Métricas | Descripción |
|---|---|
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |

**Soporte para EDT en HDX insights**

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos ilustrados (EDT) para mostrar análisis para HDX Insight. Es decir, ADM ahora admite los protocolos UDP y TCP. La compatibilidad de EDT con NetScaler Gateway garantiza una experiencia de usuario de alta definición durante la sesión de los escritorios virtuales para los usuarios que ejecutan Citrix Receiver

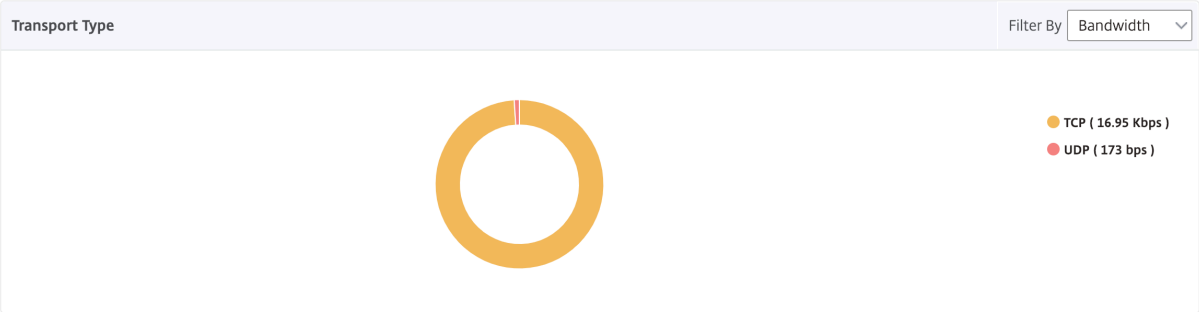
HDX Insight ahora muestra el número de sesiones de EDT y de sesiones que no son de EDT como parte del informe de sesiones activas. La tabla Usuarios muestra un informe detallado de todos los usuarios del sistema. La tabla muestra métricas como la latencia de WAN, la latencia de DC, las retransmisiones, los RTO y algunas de estas métricas no están disponibles para los usuarios que tienen sesiones de EDT, ya que se calculan a partir de la pila TCP actualmente. Por lo tanto, aparecen como “NA”.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Se ha introducido un nuevo gráfico de donut para permitirle ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.

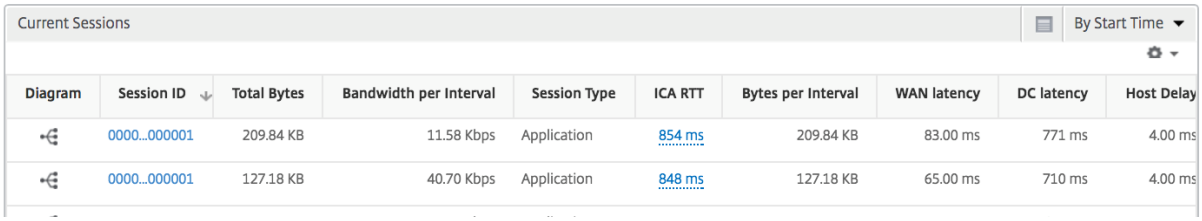
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> EDT en HDX Insight es compatible con NetScaler ADM desde la versión 12.1 compilación 50.28 y está disponible en instancias ADC desde la versión 12.1 compilación 49.23.

**Métricas de HDX Insight disponibles en NetScaler ADM 12.0 y versiones posteriores:**

| | |
|---|---|
| Latencia del lado del cliente L7 | Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |
| Latencia L7 del lado del servidor | La latencia media de L7 observada entre el dispositivo NetScaler ADC y Citrix Virtual App. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |
| Latencia de vulneración máxima | El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido. |
| Latencia de violación promedio | El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de “latencia L7 infringida”. |
| Recuento de incumplimiento de umbral L7 | Número de veces que se ha producido una infracción del umbral L7. |




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Terminated Sessions — By Start Time

| Session ID | Session Type | ICA RTT | WAN latency | DC latency | Bandwidth per Interval | Session Bandwidth | Total Bytes | Bytes per Interval |
|---|---|---|---|---|---|---|---|---|
| 0000...000001 | Application | 1.01 s | 59.00 ms | 763.00 ms | 9.40 Kbps | 9.40 Kbps | 1.38 MB | 1.38 MB |
| 0000...000001 | Desktop | 971.00 ms | 59.00 ms | 733.00 ms | 8.82 Kbps | 8.82 Kbps | 1.29 MB | 1.29 MB |
| 0000...000001 | Application | 998.00 | 51.00 ms | 732.00 ms | 9.91 Kbps | 9.91 Kbps | 1.45 MB | 1.45 MB |

**Usuarios de escritorio** Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

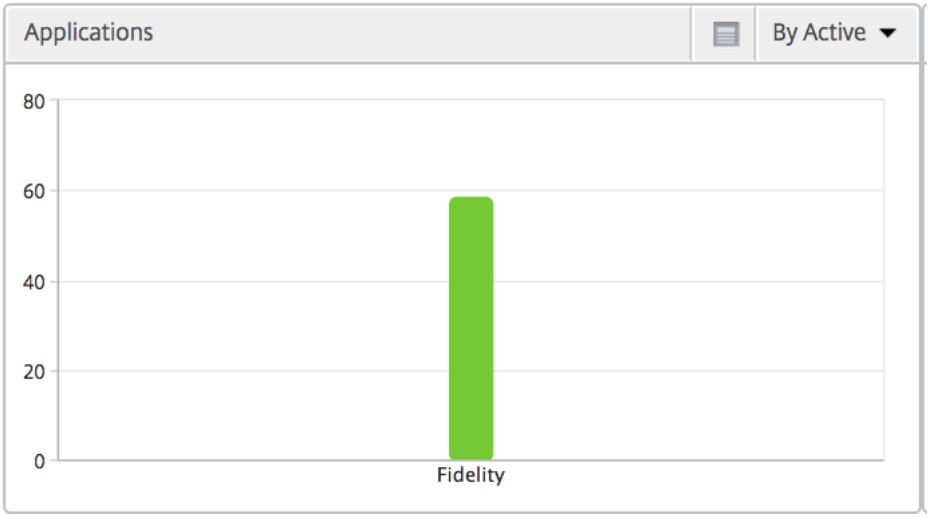
| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |

Desktop Users — By Desktop Launch Count

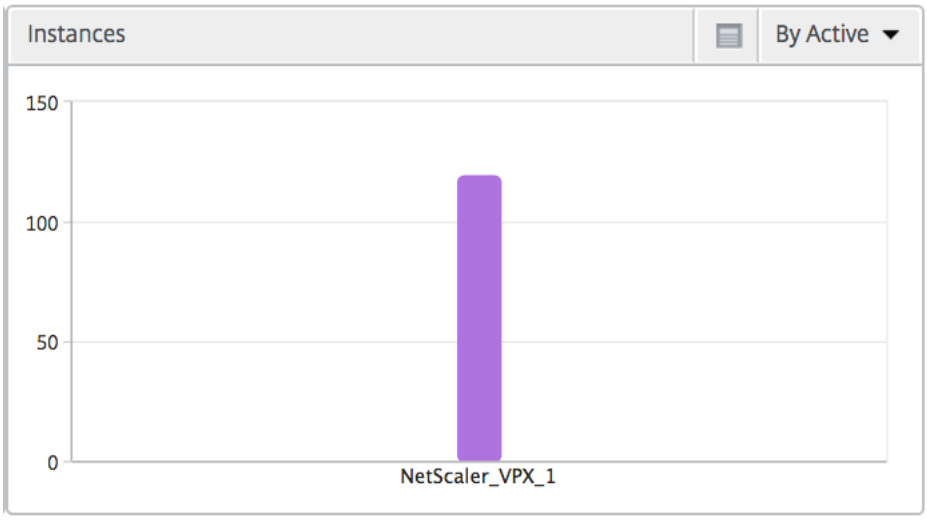
| Name | Desktop Launch Count | Bandwidth | DC latency | WAN latency | ICA RTT |
|---|---|---|---|---|---|
| XenDesktop33 | 177 | 9.38 Kbps | 749.00 ms | 57.00 ms | 1.00 s |

**Aplicaciones** Gráfico de barras que representa las aplicaciones ordenadas por Activo, recuento total de inicio de sesión, recuento total de inicio de aplicaciones y duración del lanzamiento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

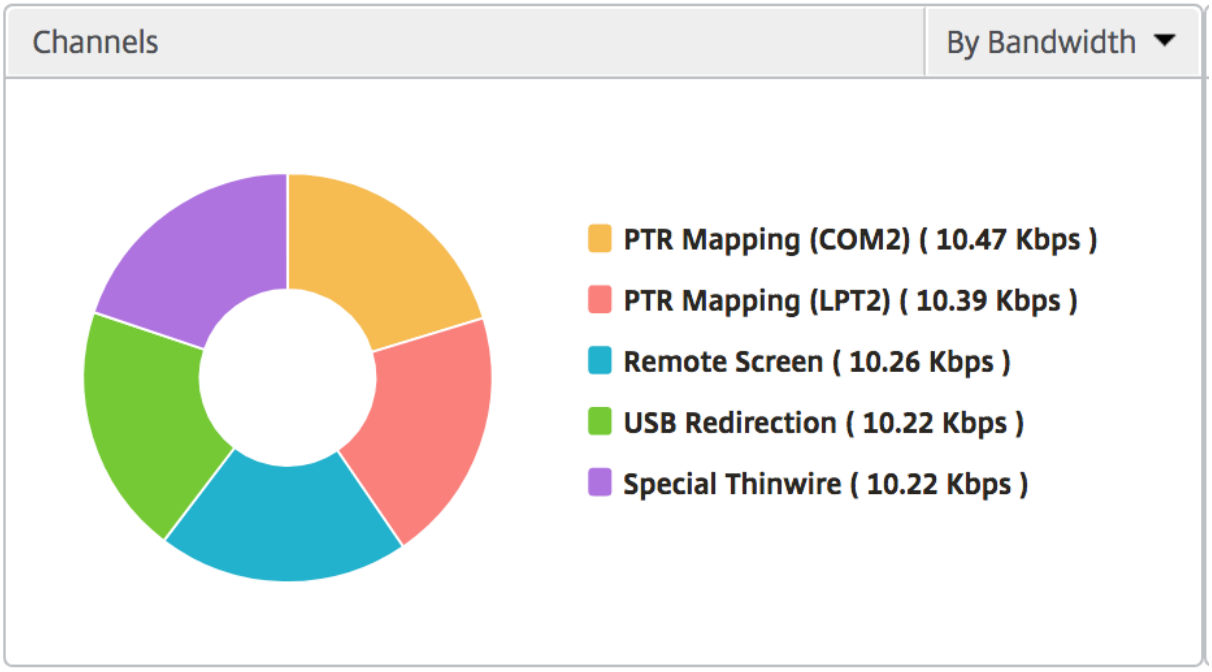



**Instancias** Un gráfico de barras que representa las instancias de NetScaler ADC ordenadas por aplicaciones activas y totales

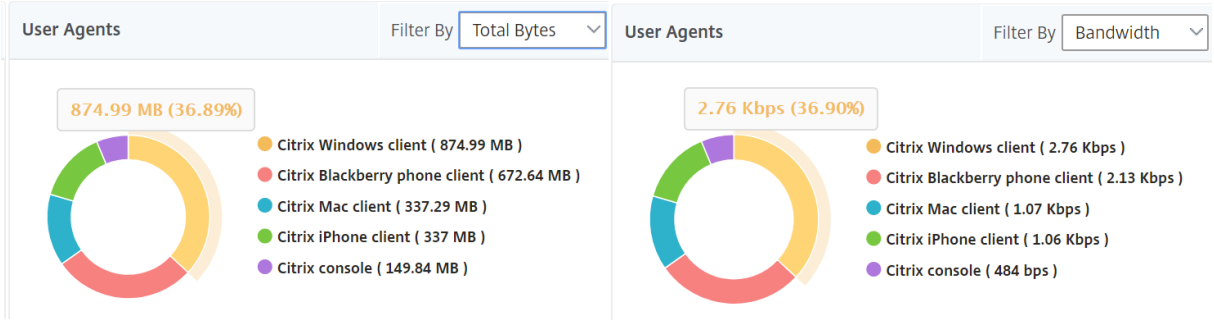



**Canales** Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Agentes de usuario** Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.




**Vista de sesión por usuario** La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

**Para ver las métricas de la sesión de un usuario seleccionado:**

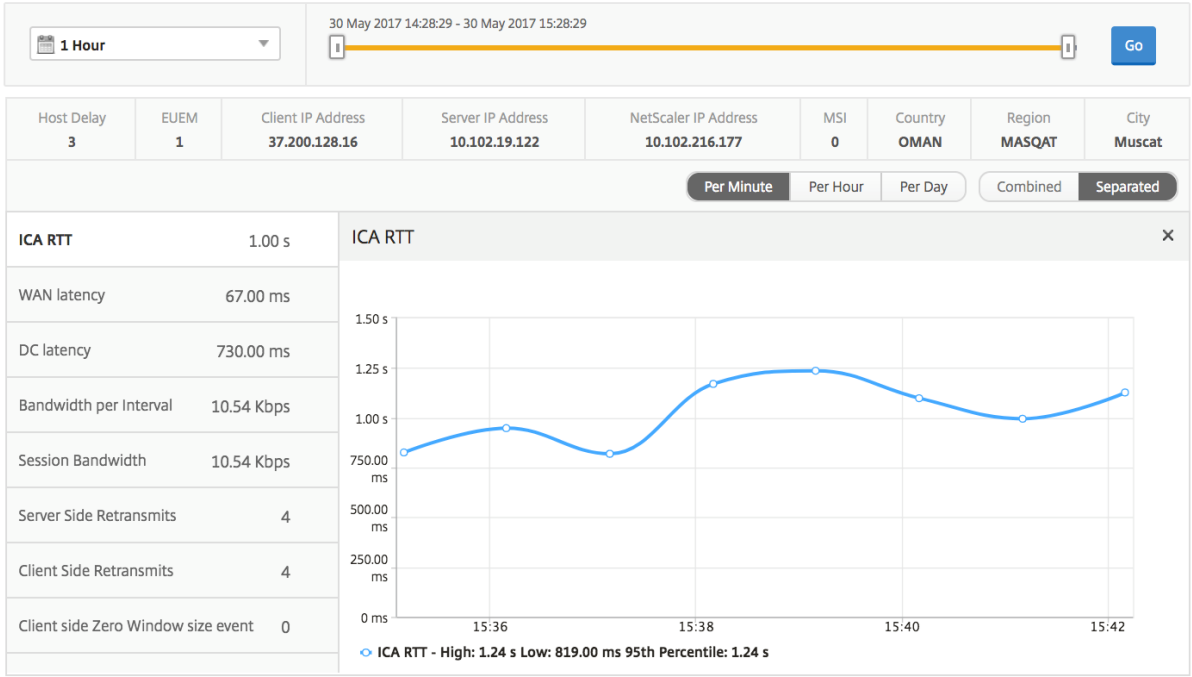
1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.
3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

**Gráfico cronológico**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

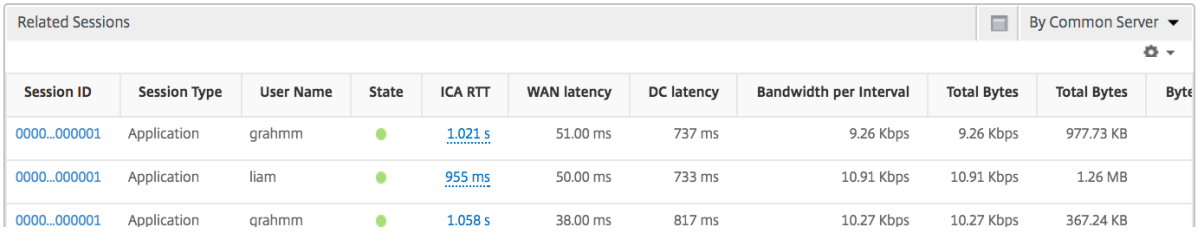
| Métricas | Descripción |
| --- | --- |
| Reconexiones de sesión | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| Recuento de ACR | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Aplicación activa** La sección **Aplicaciones activas** muestra las aplicaciones activas del usuario seleccionado. Estas aplicaciones también se pueden ordenar por número de sesiones activas y duración de inicio.

**Sesiones relacionadas** La sección Sesiones relacionadas muestra las sesiones relacionadas de las sesiones del usuario seleccionado. La relación se puede seleccionar como servidores comunes o común de NetScaler ADC.




## Informes y métricas de vista de aplicaciones

Los informes y métricas de esta vista se centran en Citrix Virtual Apps.

**Para desplazarse a la vista Aplicación:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.

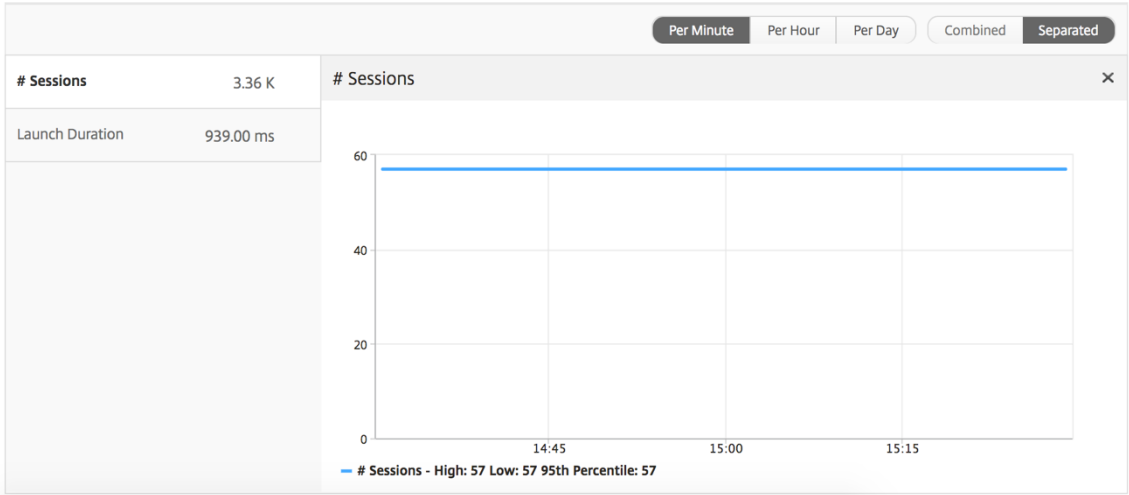
### Vista de resumen

La vista de resumen muestra los informes de todas las aplicaciones que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas/informes, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| N.º de sesiones | Número total de sesiones durante un intervalo de tiempo determinado. |
| Duración de inicios | Promedio de tiempo necesario para iniciar una aplicación. |




### Informe resumido de las aplicaciones

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de la aplicación virtual Citrix. |
| Recuento total de sesiones iniciadas | Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Recuento total de aplicaciones iniciadas | Número total de aplicaciones de Citrix Virtual App lanzadas durante el intervalo de tiempo dado. |
| Duración de inicios | Tiempo promedio que se tarda en iniciar la aplicación virtual de Citrix. |

Applications

| Name | Total App Launch Count | Launch Duration | Total Session Launch count |
|---|---|---|---|
| Microsoft Outlook | 531 | 514.00 ms | 531 |
| Microsoft Visio | 354 | 555.00 ms | 354 |
| Microsoft Word | 354 | 557.00 ms | 354 |
| Microsoft Excel | 354 | 555.00 ms | 354 |

### Informe de aplicación activa

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de la aplicación virtual Citrix. |
| State | Muestra el estado de la aplicación: Verde-Activa, Rojo-Inactiva |
| N.º de sesiones activas | Número de sesiones de usuario activas que utilizan esta aplicación durante un intervalo de tiempo determinado. |
| Aplicaciones #Active | Número de sesiones activas para esta aplicación. |

Active Applications

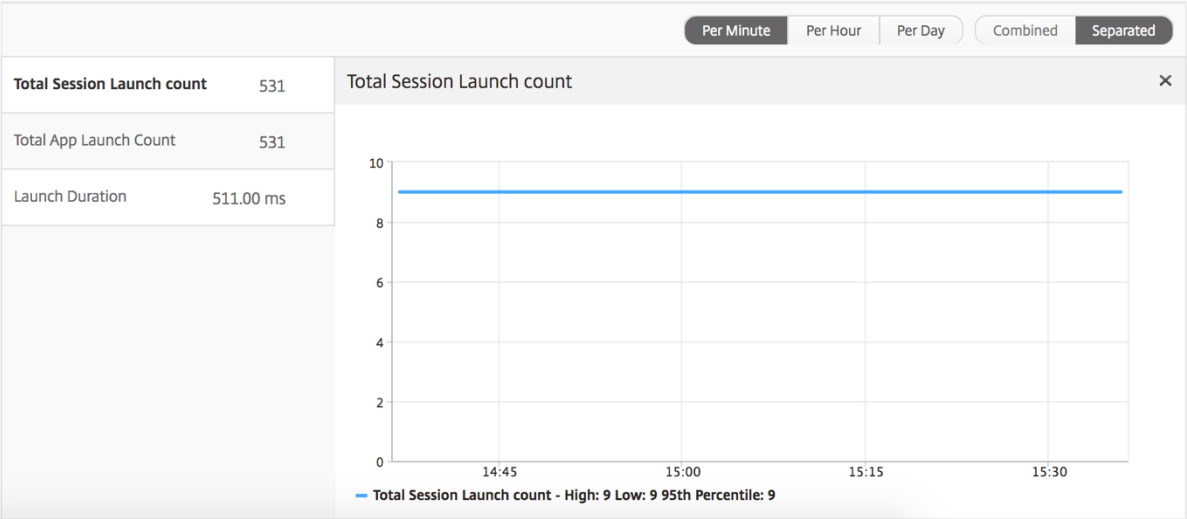
| Name | State | # Active Sessions | # Active Apps |
|---|---|---|---|
| Communicator | ● | 60 | 60 |
| Fidelity | ● | 60 | 60 |
| GoToMeeting | ● | 60 | 60 |

**Informe Umbral** El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Aplicación en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

### Gráfico de líneas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| Duración de inicios | Promedio de tiempo necesario para iniciar una aplicación. |




**Informe sobre sesiones actuales**

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

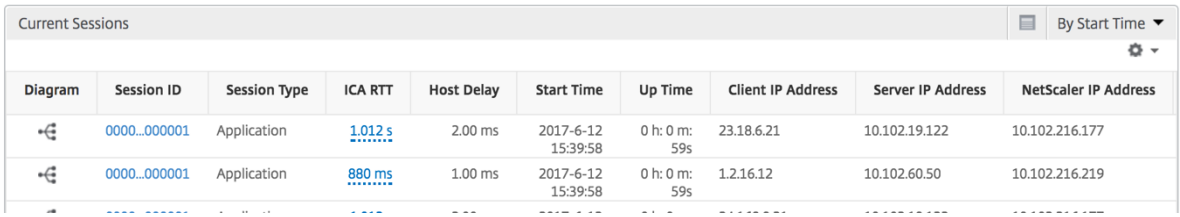
| Métricas | Descripción |
|---|---|
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Nombre de usuario | El nombre de usuario del usuario que accede a esta aplicación virtual de Citrix en particular. |
| ID de sesión | Identificador único para la sesión de Citrix Virtual App. |
| Tipo de sesión | Será “Solicitud”. |
| State | Estado de la sesión: verde para activa, rojo para inactiva. |
| Latencia de vulneración máxima | El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Latencia de violación promedio | El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de “latencia L7 infringida”. |
| Recuento de incumplimiento de umbral L7 | Número de veces que se ha producido una infracción del umbral L7. |
| Latencia del lado del cliente L7 | Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |
| Latencia L7 del lado del servidor | La latencia media de L7 observada entre el dispositivo NetScaler ADC y Citrix Virtual App. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |




### Vista de sesión por aplicación

La vista por sesión de aplicación muestra los informes de una sesión de aplicación seleccionada concreta.

**Para ver los informes de sesión:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.
3. Seleccione un usuario concreto del informe resumido de la aplicación.
4. Se seleccionó una sesión del informe de sesiones actuales.

### Gráfico de líneas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Evento de ventana cero en el lado del servidor | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

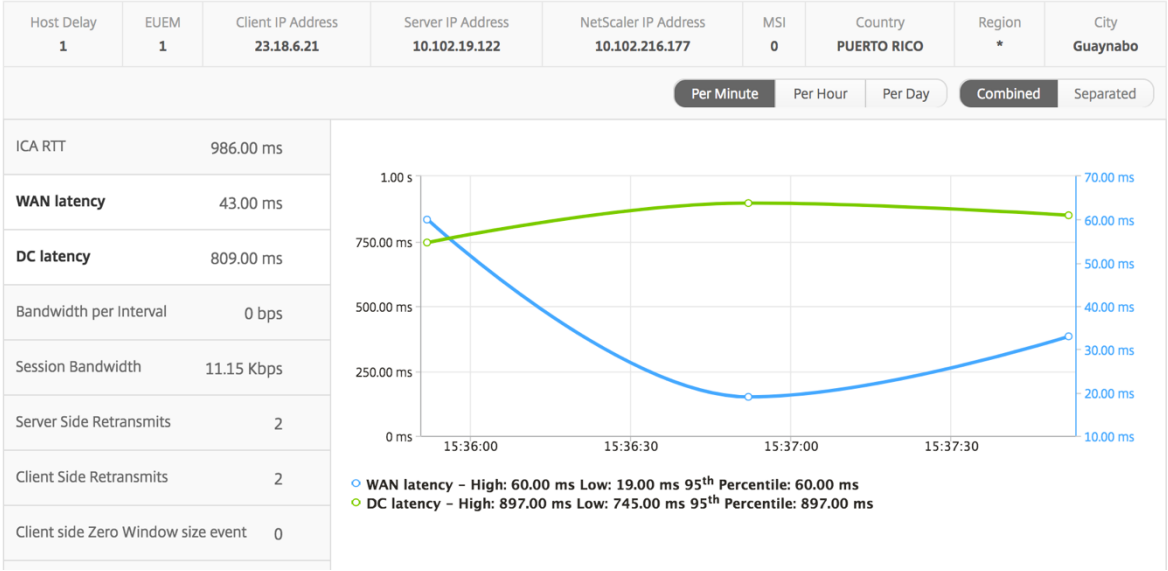
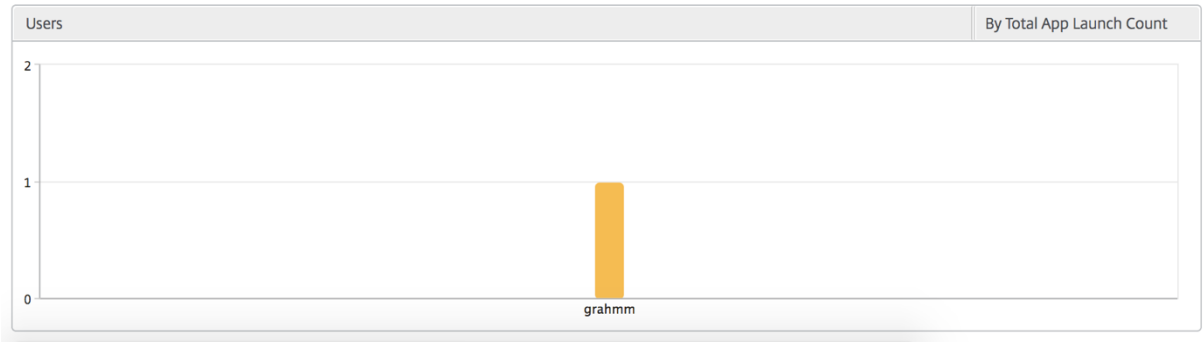



**Gráfico de barras de usuario** El gráfico de barras del usuario representa a los usuarios que han iniciado sesión en esta aplicación en particular.




## Informes y métricas de vista de escritorio

Los informes y las métricas de esta vista se centran en los Citrix Virtual Desktops.

**Para desplazarse a la vista Escritorio:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX InsightEscritorio**.

### Vista de resumen

La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

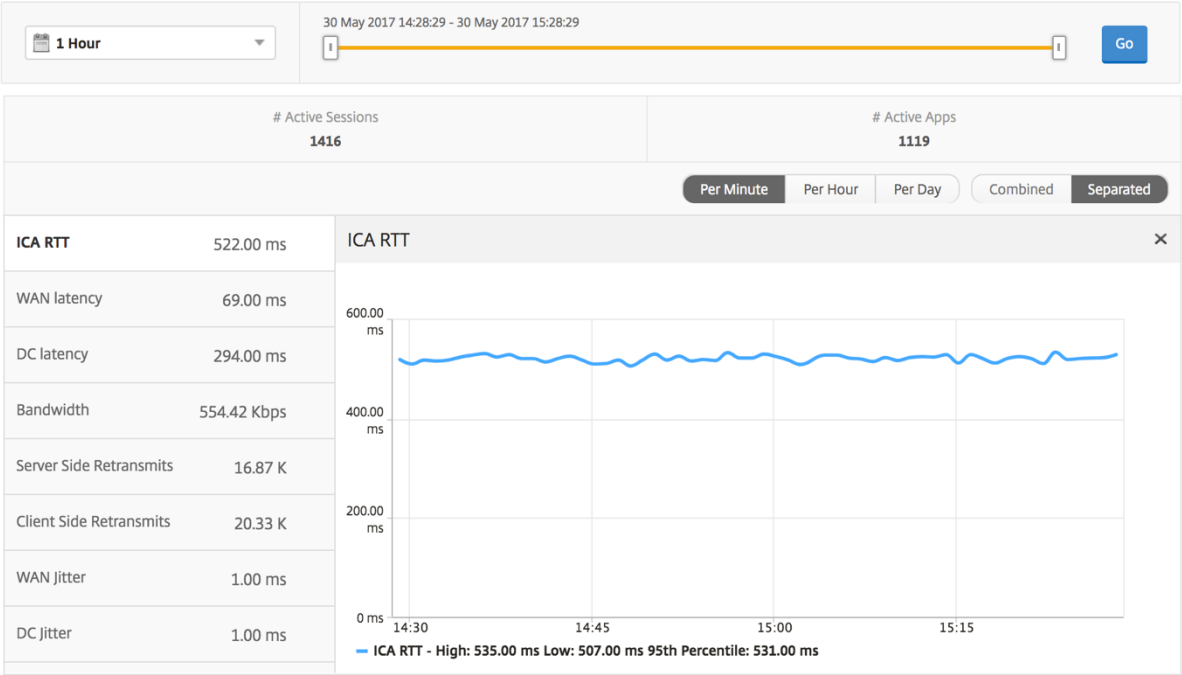
Todas las métricas/informes, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

**Gráfico de líneas**

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |




### Informe de resumen de escritorio

| Métricas | Descripción |
| --- | --- |
| Sesiones activas | Número total de sesiones activas de Citrix Virtual Desktop durante un intervalo de tiempo determinado. |
| Escritorios activos | Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |

Desktop Users

Search

| User Name | # Active Desktops | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|---|
| liam | 60 | 1.00 s | 56.00 ms | 746.00 ms | 9.27 Kbps | 251.24 MB |
| jayden | 60 | 1.00 s | 52.00 ms | 746.00 ms | 9.27 Kbps | 251.34 MB |
| juan | 60 | 169.00 ms | 32.00 ms | 30.00 ms | 9.26 Kbps | 250.99 MB |
| daniel | 60 | 149.00 ms | 31.00 ms | 30.00 ms | 9.26 Kbps | 251.02 MB |
| randyb | 60 | 99.00 ms | 11.00 ms | 30.00 ms | 9.26 Kbps | 250.97 MB |

WAN latency

**Informe Umbral** El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Escritorio en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

### Por vista de escritorio

Por vista de escritorio proporciona informes detallados de la experiencia del usuario final para un escritorio virtual de Citrix seleccionado.

**Para navegar a la vista Escritorio en particular:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Escritorio**.
3. Seleccione un **escritorio** concreto en el **informe de resumen de escritorios**.

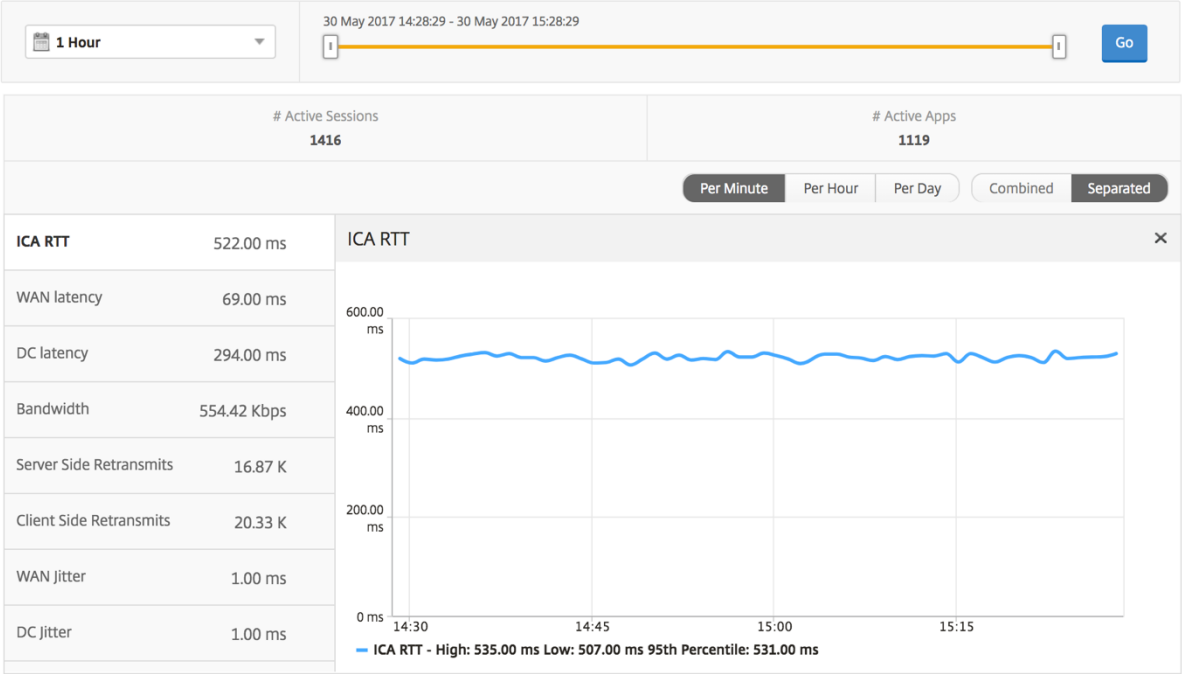
### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Informe Usuarios de escritorio** Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Desktop Users | By Desktop Launch Count

| Name | Desktop Launch Count | Bandwidth | DC latency | WAN latency | ICA RTT |
|---|---|---|---|---|---|
| XenDesktop33 | 177 | 9.38 Kbps | 749.00 ms | 57.00 ms | 1.00 s |

**Informe de escritorios de usuario activos e inactivos** Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

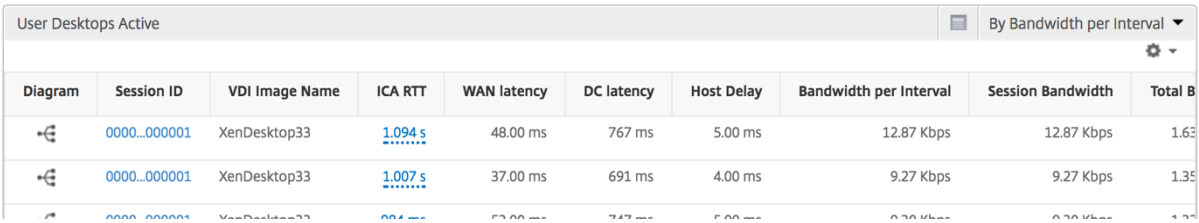
| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Nombre de la imagen VDI | Nombre del Citrix Virtual Desktops al que está conectado el usuario |
| Diagrama | |




**Por vista de sesión de escritorio**

Por vista de sesión de escritorio proporciona informes para una determinada sesión de Citrix Virtual Desktops seleccionada.

**Para desplazarse a la vista de sesión de Escritorio:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Escritorio**.
3. Seleccione un escritorio concreto en el **informe de resumen de escritorios**.
4. Seleccione una sesión del informe de sesiones actuales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico cronológico** La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

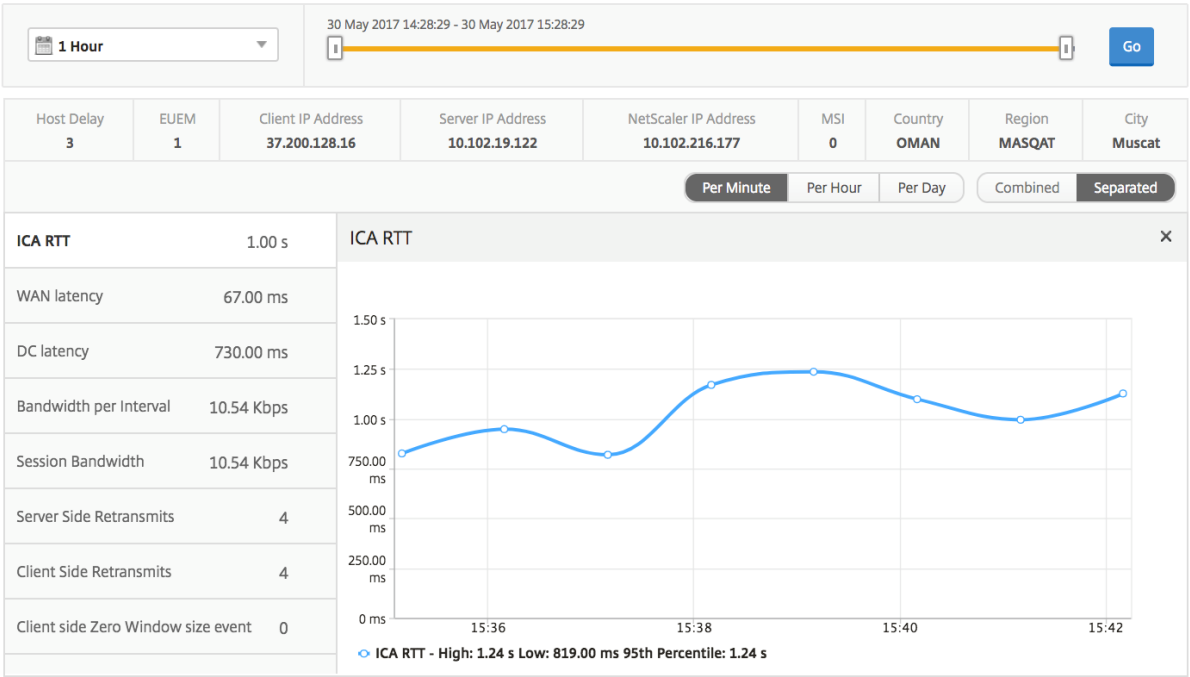
**Para ver las métricas de la sesión de un usuario seleccionado:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
3. Select un usuario concreto en la sección **Informe de resumen de usuario**.
4. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

| Métricas | Descripción |
|---|---|
| Reconexiones de sesión | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| Recuento de ACR | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |




**Informe de sesiones de escritorio relacionadas** Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |

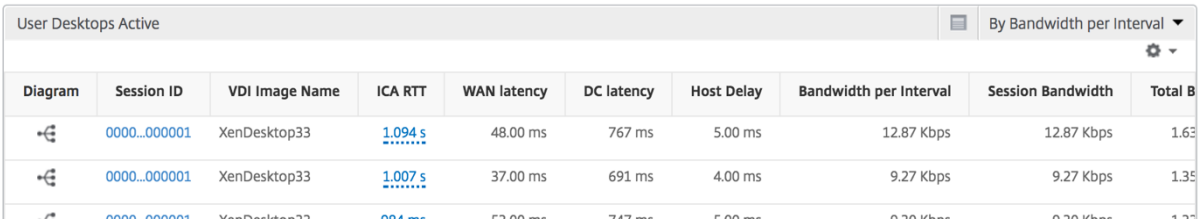
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Informes y métricas de vista de instancias

Los informes y las métricas de la vista de instancias se centran en las instancias de NetScaler ADC.

**Para desplazarse a la vista Instancia:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Instancias**.

Los informes y las métricas de vistas de instancias constan de las siguientes secciones:

- Vista resumida de la instancia
- Vista por instancia

### Vista de resumen de instancia

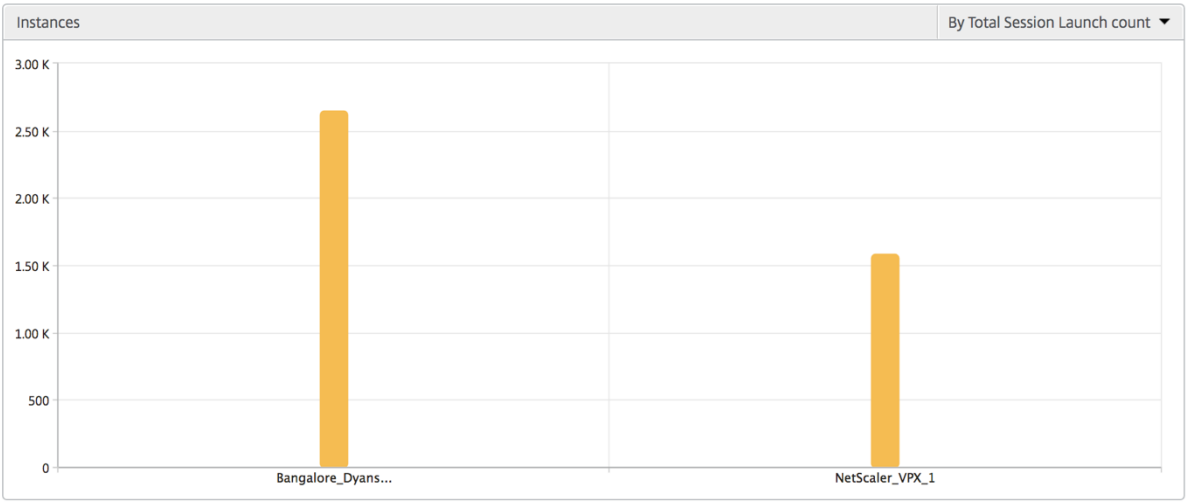
Esta vista se denomina vista de resumen, ya que muestra los informes de todas las instancias de NetScaler ADC que se agregan a NetScaler ADM.

Todas las métricas/informes a continuación, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

### Gráfico de barras de instancia

| | |
|---|---|
| Este gráfico muestra la instancia frente al recuento de inicio total de sesión | Total de aplicaciones que se pueden seleccionar de la lista en la parte superior derecha del lienzo gráfico. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Informe de resumen de instancia/instancias activas**

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de host de la instancia de NetScaler ADC. |
| Dirección IP | Dirección IP de NetScaler. |
| Recuento total de sesiones iniciadas | Número total de sesiones de usuario únicas creadas durante un intervalo de tiempo determinado. |
| Total de aplicaciones | Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado. |
| Tipo | N/D |

Instances

| Name | IP Address | Total Session Launch count | Total Apps | Type |
|---|---|---|---|---|
| Bangalore_Dyansty(10.102.216.219) | 10.102.216.219 | 2.65 K | 2.12 K | -NA- |
| NetScaler_VPX_1(10.102.216.177) | 10.102.216.177 | 1.59 K | 1.24 K | -NA- |

**Active Instances**

| Name | IP Address | # Active Sessions | # Active Apps | # Active Desktops | Type |
|---|---|---|---|---|---|
| NetScaler_VPX_1(10.102.216.177) | 10.102.216.177 | 538 | 417 | 120 | -NA- |
| Bangalore_Dyansty(10.102.216.219) | 10.102.216.219 | 900 | 720 | 180 | -NA- |

**Informe Umbral** El informe Umbral representa el recuento de umbrales incumplidos cuando se selecciona la *entidad* como Instancia en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Flujos omitidos** Un flujo omitido es un registro que omitió el análisis de la conexión ICA. Esto puede deberse a varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktop, una versión no compatible del receptor o el tipo de receptor, etc. Esta tabla muestra la dirección IP y el recuento de flujos omitidos. Es posible que estos receptores no formen parte de los receptores de la lista de permitidos. Por lo tanto, estas sesiones se saltan de la supervisión.

Skipped Flows

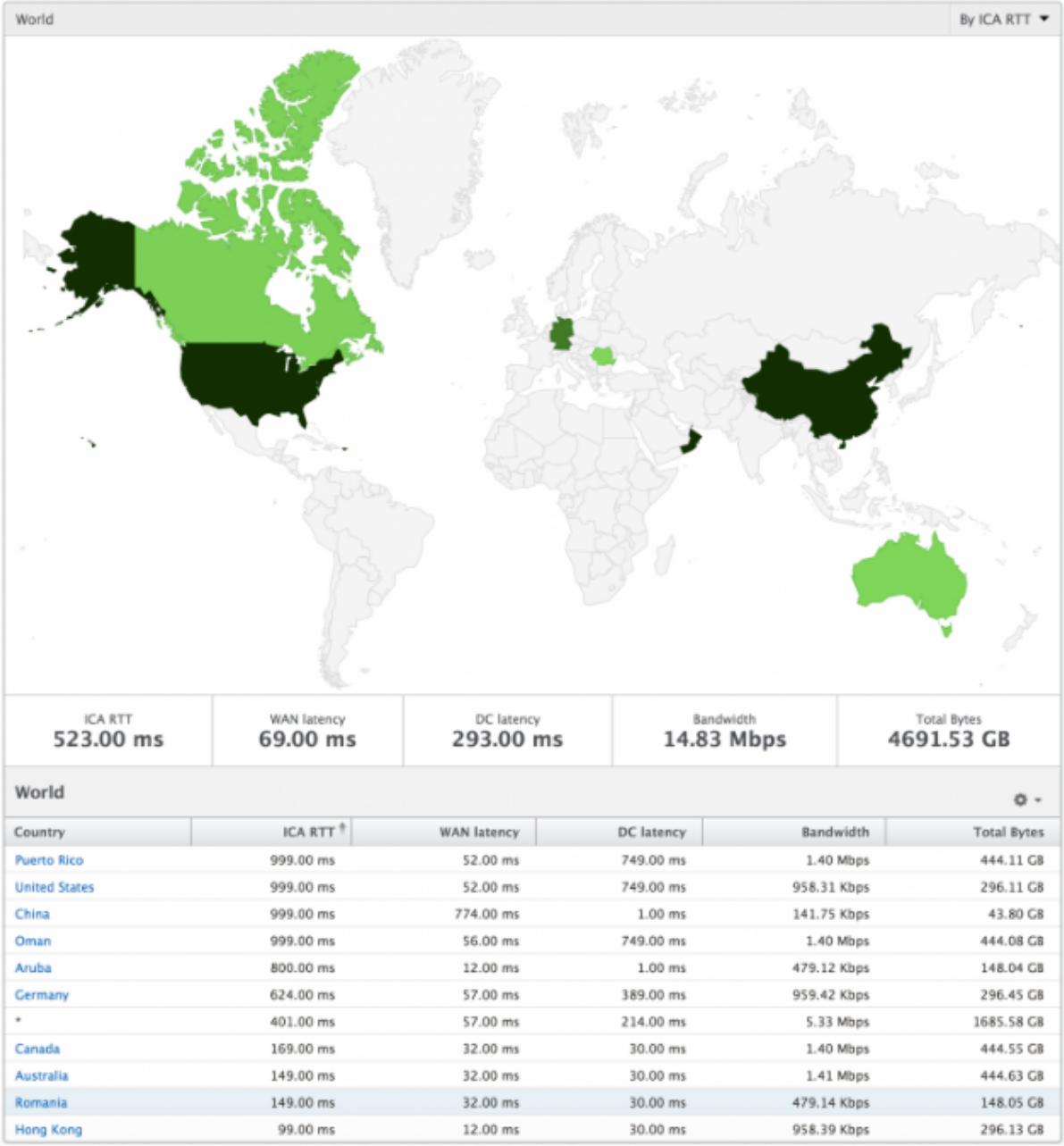
| IP Address | Skipped Count |
|---|---|
| 10.105.2.141 | 1 |
| 10.105.2.142 | 1 |

**Visión del mundo** La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión del mundo del sistema, profundizar en un país en particular y más en las ciudades, así como simplemente haciendo clic en la región. Los administradores pueden profundizar más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

### Vista por instancia

Por vista de instancia proporciona informes detallados sobre la experiencia del usuario final para una instancia específica de NetScaler ADC seleccionada.

**Para desplazarse a la vista de instancia:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Instancias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Seleccione una instancia concreta en el **informe Resumen de Instancia**.

### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| Dirección IP | Representa la dirección IP de NetScaler de la instancia seleccionada. |
| Recuento total de sesiones iniciadas | Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado. |
| Total de aplicaciones | Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado. |

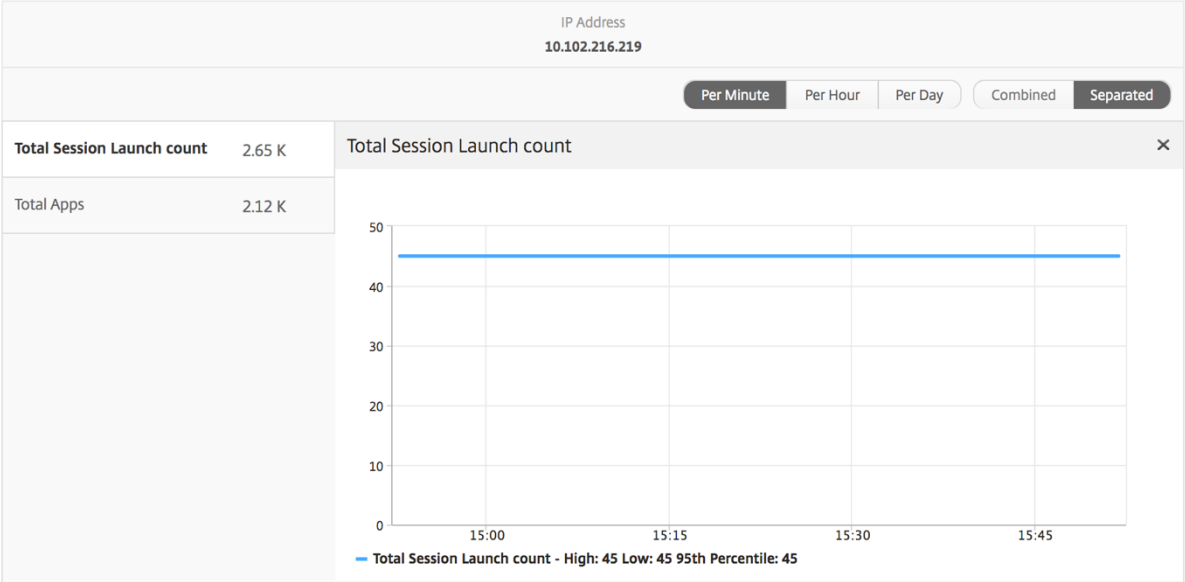
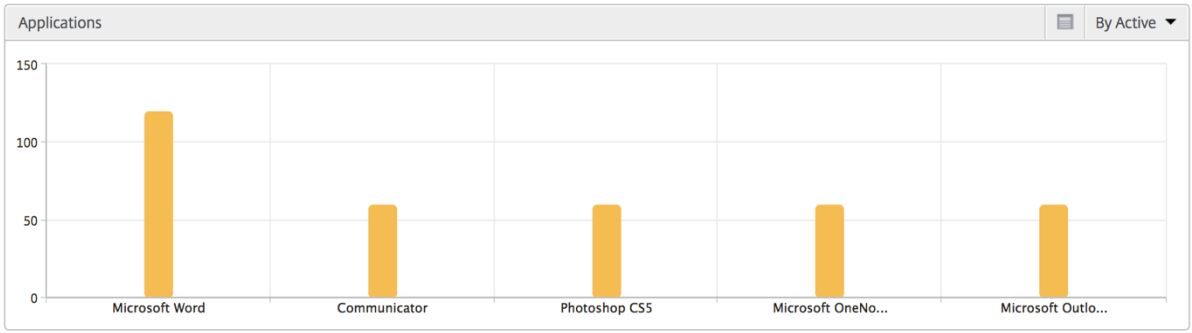


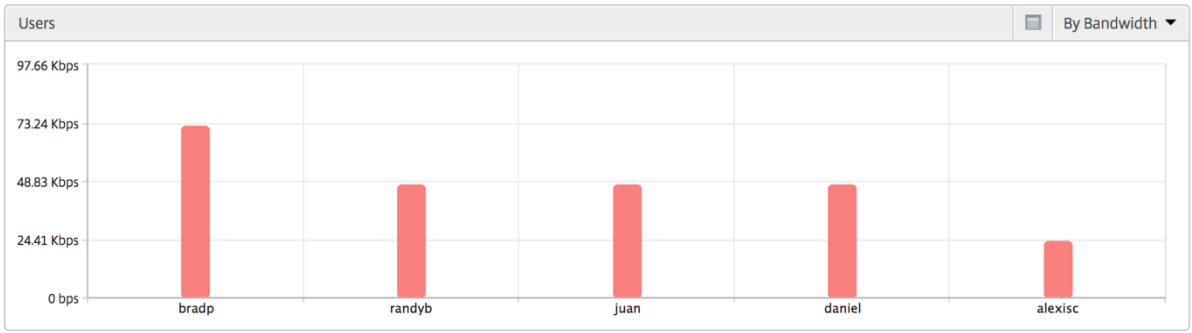

**Gráfico de barras de aplicaciones** Muestra las 5 aplicaciones principales según los siguientes criterios: por aplicaciones activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones o duración del lanzamiento.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico de barras de usuarios** El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

- Ancho de banda
- Latencia de WAN
- Latencia de DC
- RTT de ICA




**Informe Usuarios de escritorio** Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, entre NetScaler Gateway y los servidores VDI o CVAD o StoreFront. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Desktop Users | By Desktop Launch Count

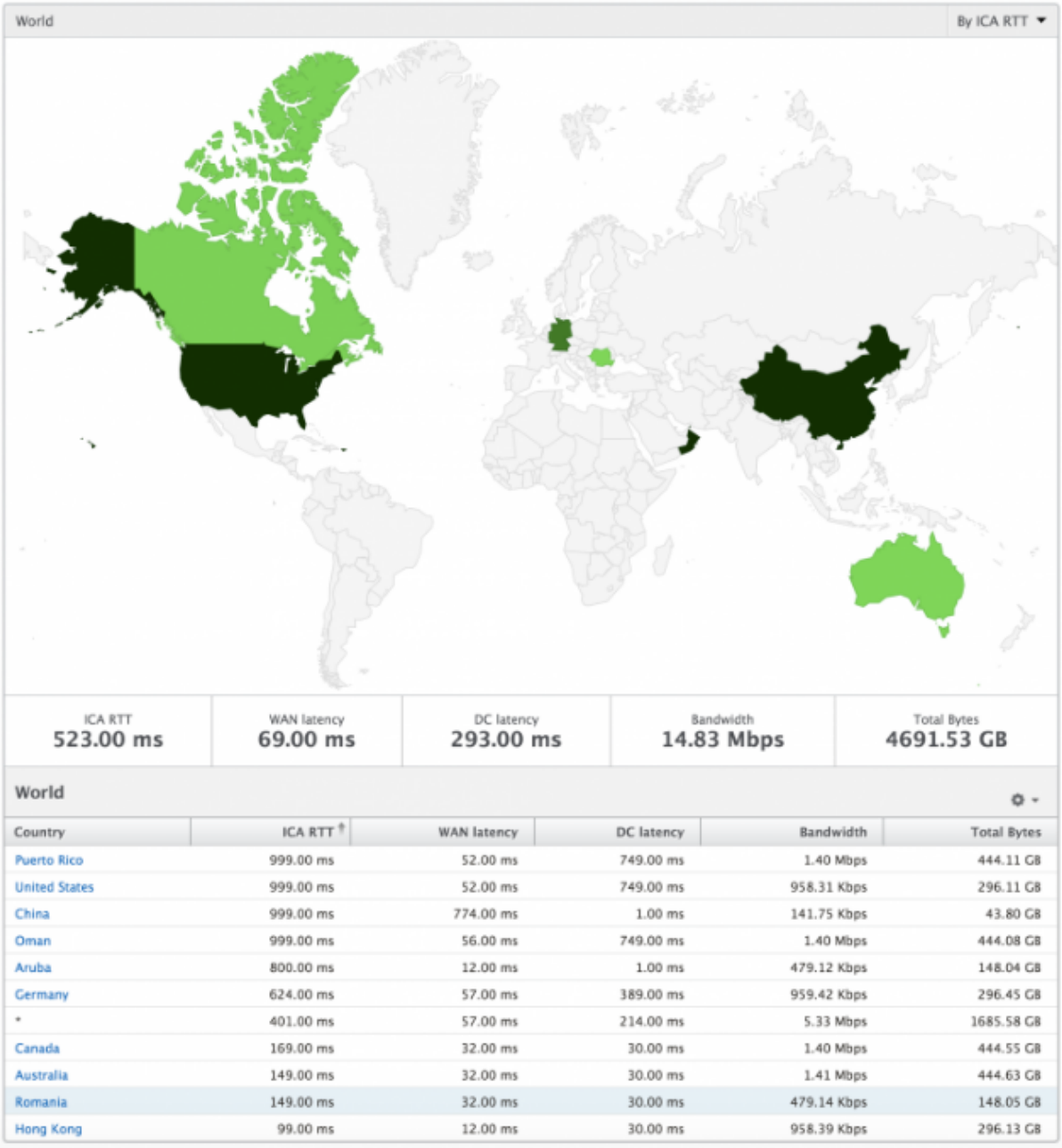
| Name | Desktop Launch Count | Bandwidth | DC latency | WAN latency | ICA RTT |
|---|---|---|---|---|---|
| XenDesktop33 | 177 | 9.38 Kbps | 749.00 ms | 57.00 ms | 1.00 s |

**Visión del mundo** La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más en las ciudades, así como hacer clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

## Informes y métricas de vista de licencias

La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

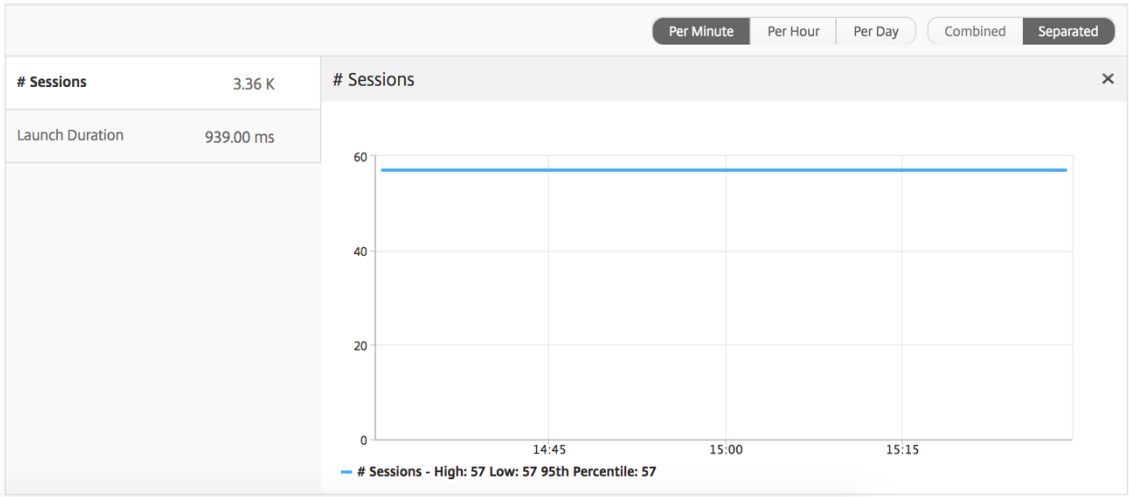
**Para navegar a la vista Licencia:**

1. Inicie sesión en su NetScaler ADM mediante un explorador web compatible.
2. Vaya a **Analytics > HDX Insight > Licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico de líneas**

| Métricas | Descripción |
| --- | --- |
| Licencias en uso | Las licencias de CCU de NetScaler Gateway que se utilizan durante el plazo seleccionado. Cada recuento representa el número de sesiones de usuario. Esto es independiente de las sesiones de aplicaciones y escritorios iniciadas por ese usuario. |
| Total de licencias | Número total de licencias CCU de NetScaler Gateway disponibles para que el cliente las utilice. |




**Informe Umbral** El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Licencia en el período seleccionado. Para obtener más información, consulte cómo crear umbrales.

## Informes y métricas de vista de aplicaciones

January 30, 2024

Los informes y métricas de esta vista se centran en Citrix Virtual Apps.

**Para desplazarse a la vista Aplicación:**

1. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

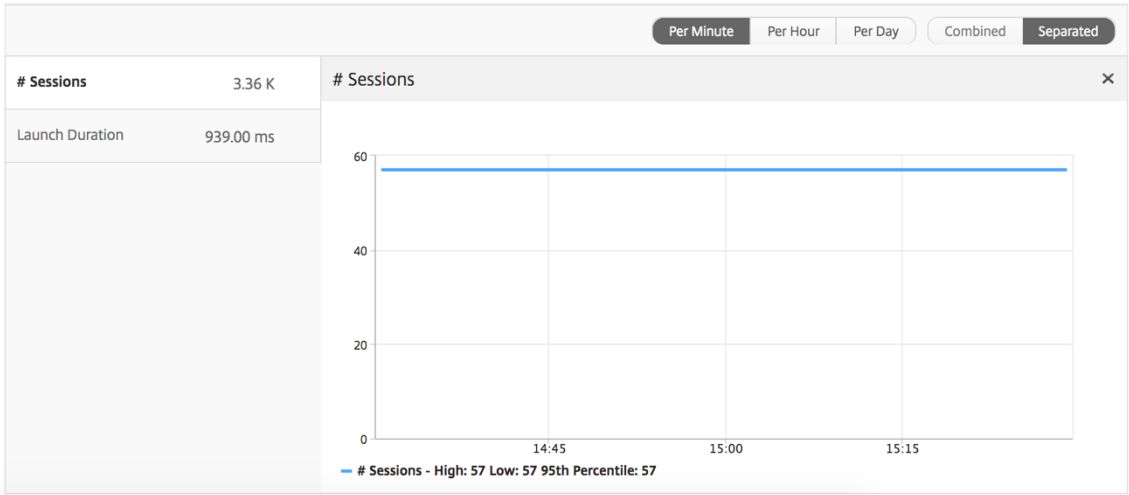
## Vista de resumen

La vista de resumen muestra los informes de todas las aplicaciones que han iniciado sesión durante la línea de tiempo seleccionada.

Todas las métricas e informes siguientes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| N.º de sesiones | Número total de sesiones durante un intervalo de tiempo determinado. |
| Duración de inicios | Promedio de tiempo necesario para iniciar una aplicación. |




### Informe resumido de las aplicaciones

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de la aplicación virtual Citrix. |
| Recuento total de sesiones iniciadas | Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Recuento total de aplicaciones iniciadas | Número total de aplicaciones de Citrix Virtual App lanzadas durante el intervalo de tiempo dado. |
| Duración de inicios | Tiempo promedio que se tarda en iniciar la aplicación virtual de Citrix. |

Applications

| Name | Total App Launch Count | Launch Duration | Total Session Launch count |
|---|---|---|---|
| Microsoft Outlook | 531 | 514.00 ms | 531 |
| Microsoft Visio | 354 | 555.00 ms | 354 |
| Microsoft Word | 354 | 557.00 ms | 354 |
| Microsoft Excel | 354 | 555.00 ms | 354 |

### Informe de aplicación activa

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de la aplicación virtual Citrix. |
| State | Muestra el estado de la aplicación: Verde-Activa, Rojo-Inactiva |
| N.º de sesiones activas | Número de sesiones de usuario activas que utilizan esta aplicación durante un intervalo de tiempo determinado. |
| Aplicaciones #Active | Número de sesiones activas para esta aplicación. |

Active Applications

| Name | State | # Active Sessions | # Active Apps |
|---|---|---|---|
| Communicator | ● | 60 | 60 |
| Fidelity | ● | 60 | 60 |
| GoToMeeting | ● | 60 | 60 |

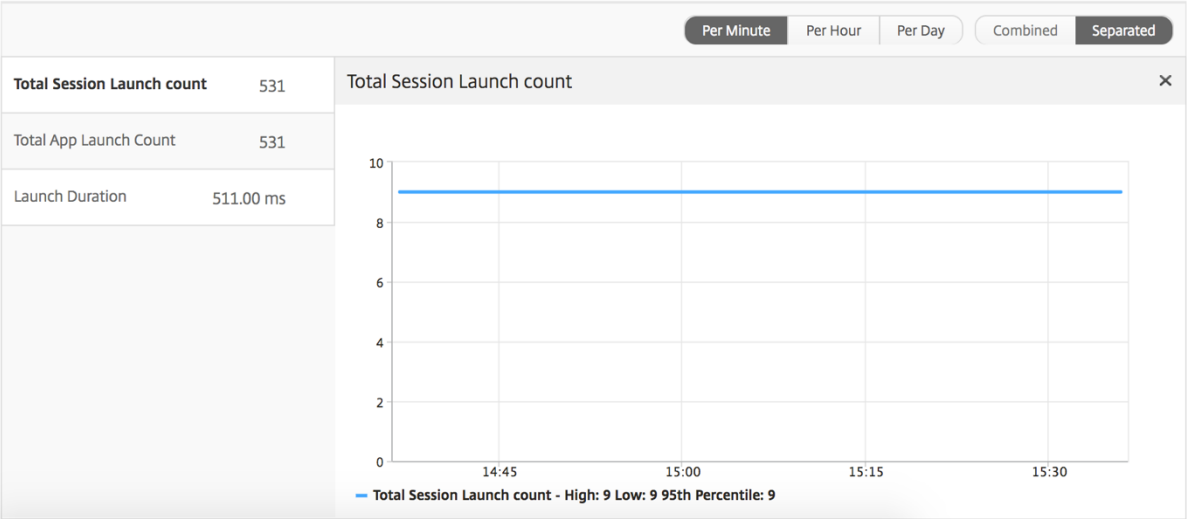
### Informe Umbral

El informe de umbrales representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Aplicación en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| Duración de inicios | Promedio de tiempo necesario para iniciar una aplicación. |




### Informe sobre sesiones actuales

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

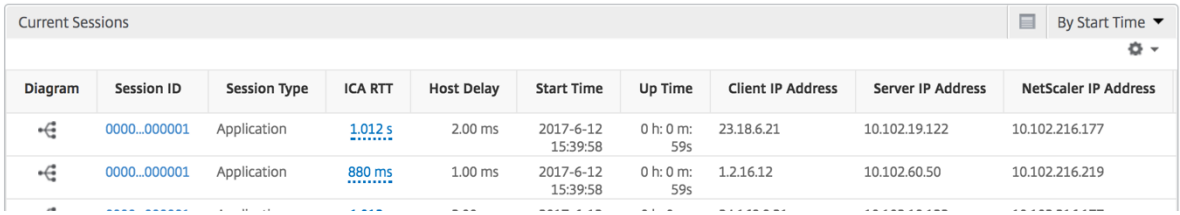
| Métricas | Descripción |
|---|---|
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Nombre de usuario | El nombre de usuario del usuario que accede a esta aplicación virtual de Citrix en particular. |
| ID de sesión | Identificador único para la sesión de Citrix Virtual App. |
| Tipo de sesión | Será “Solicitud”. |
| State | Estado de la sesión: verde para activa, rojo para inactiva. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Latencia de vulneración máxima | El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido. |
| Latencia de violación promedio | El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de "latencia L7 infringida". |
| Recuento de incumplimiento de umbral L7 | Número de veces que se ha producido una infracción del umbral L7. |
| Latencia del lado del cliente L7 | Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega. |
| Latencia L7 del lado del servidor | La latencia media de L7 observada entre el dispositivo NetScaler ADC y Citrix Virtual App. Esta métrica es útil en dispositivos que no son Citrix que están presentes en la ruta de entrega. |




### Vista de sesión por aplicación

La vista por sesión de aplicación muestra los informes de una sesión de aplicación seleccionada concreta.

**Para ver los informes de sesión:**

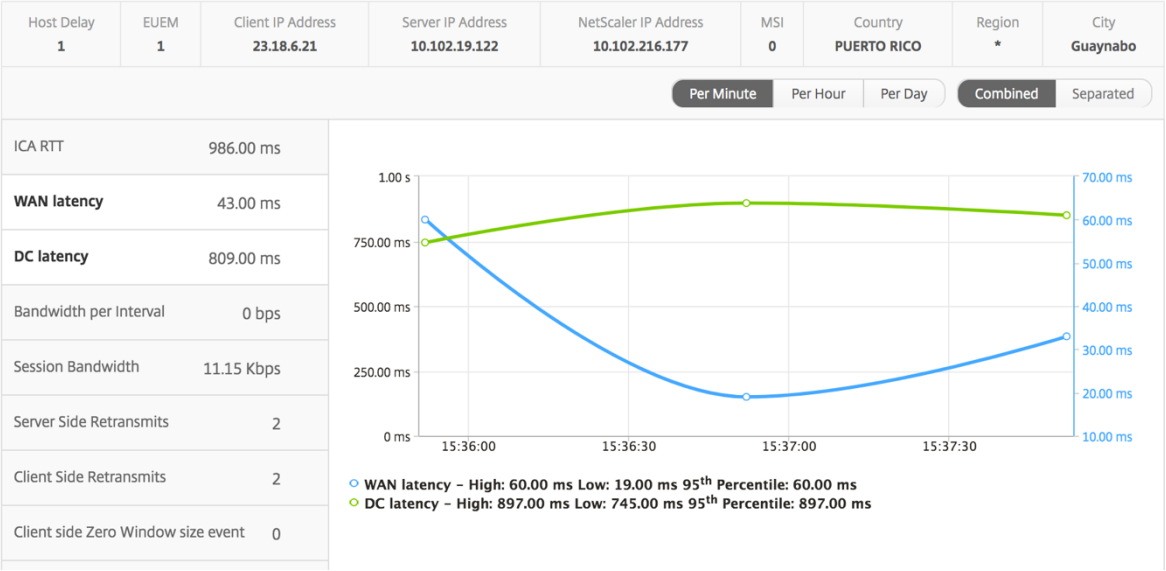
1. Vaya a **Analytics** > **HDX Insight** > **Aplicaciones**.
2. Seleccione un usuario concreto del informe resumido de la aplicación.
3. Se seleccionó una sesión del informe de sesiones actuales.

### Gráfico de líneas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

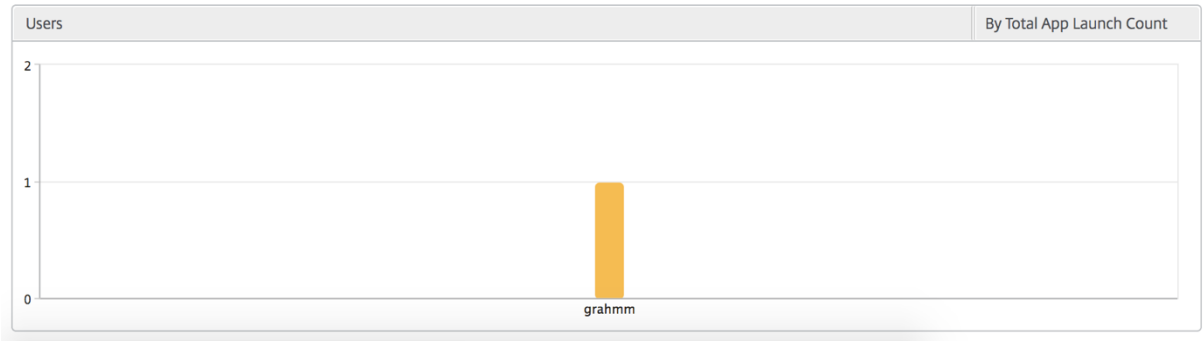
| Métricas | Descripción |
| --- | --- |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Evento de ventana cero en el lado del servidor | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Gráfico de barras de usuario

El gráfico de barras del usuario representa a los usuarios que han iniciado sesión en esta aplicación en particular.




## Informes y métricas de Desktop View

January 30, 2024

Los informes y las métricas de esta vista se centran en los Citrix Virtual Desktops.

**Para desplazarse a la vista Escritorio:**

1. Vaya a **Analytics** > **HDX InsightEscritorio**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Vista de resumen

La vista de resumen muestra los informes de todos los Citrix Virtual Desktops que han iniciado sesión durante la línea de tiempo seleccionada.

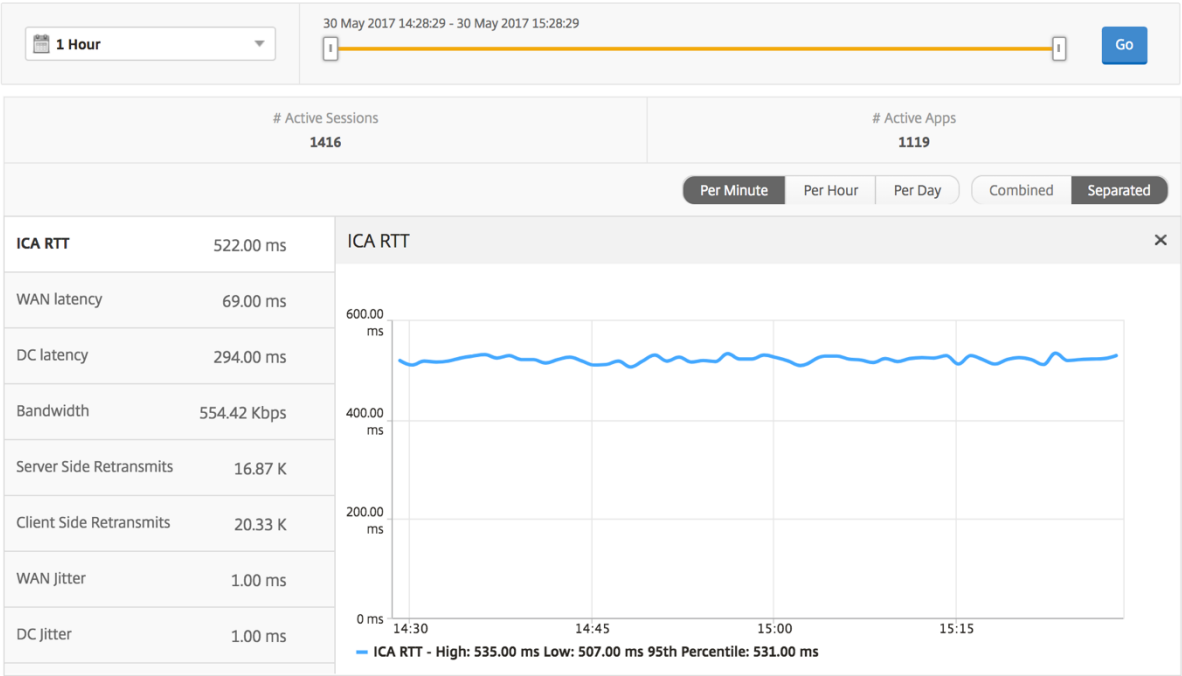
Todas las métricas/informes, a menos que se mencione explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

#### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |

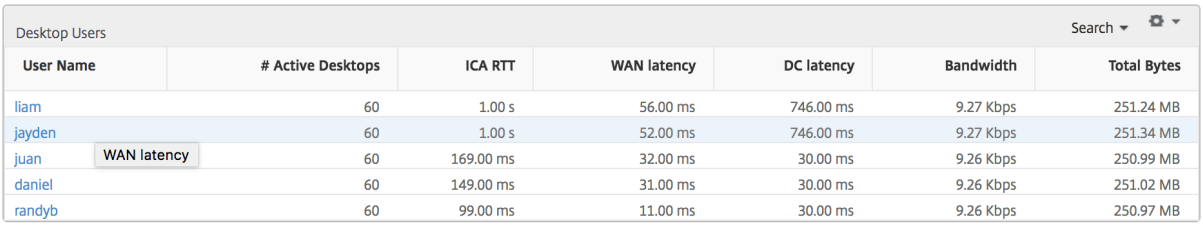



### Informe de resumen de escritorio

| Métricas | Descripción |
|---|---|
| Sesiones activas | Número total de sesiones activas de Citrix Virtual Desktop durante un intervalo de tiempo determinado. |
| Escritorios activos | Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |




| User Name | # Active Desktops | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|---|
| liam | 60 | 1.00 s | 56.00 ms | 746.00 ms | 9.27 Kbps | 251.24 MB |
| jayden | 60 | 1.00 s | 52.00 ms | 746.00 ms | 9.27 Kbps | 251.34 MB |
| juan | 60 | 169.00 ms | 32.00 ms | 30.00 ms | 9.26 Kbps | 250.99 MB |
| daniel | 60 | 149.00 ms | 31.00 ms | 30.00 ms | 9.26 Kbps | 251.02 MB |
| randyb | 60 | 99.00 ms | 11.00 ms | 30.00 ms | 9.26 Kbps | 250.97 MB |

### Informe Umbral

El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Escritorio en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

## Por vista de escritorio

Por vista de escritorio proporciona informes detallados de la experiencia del usuario final para un escritorio virtual de Citrix seleccionado.

**Para navegar a la vista Escritorio en particular:**

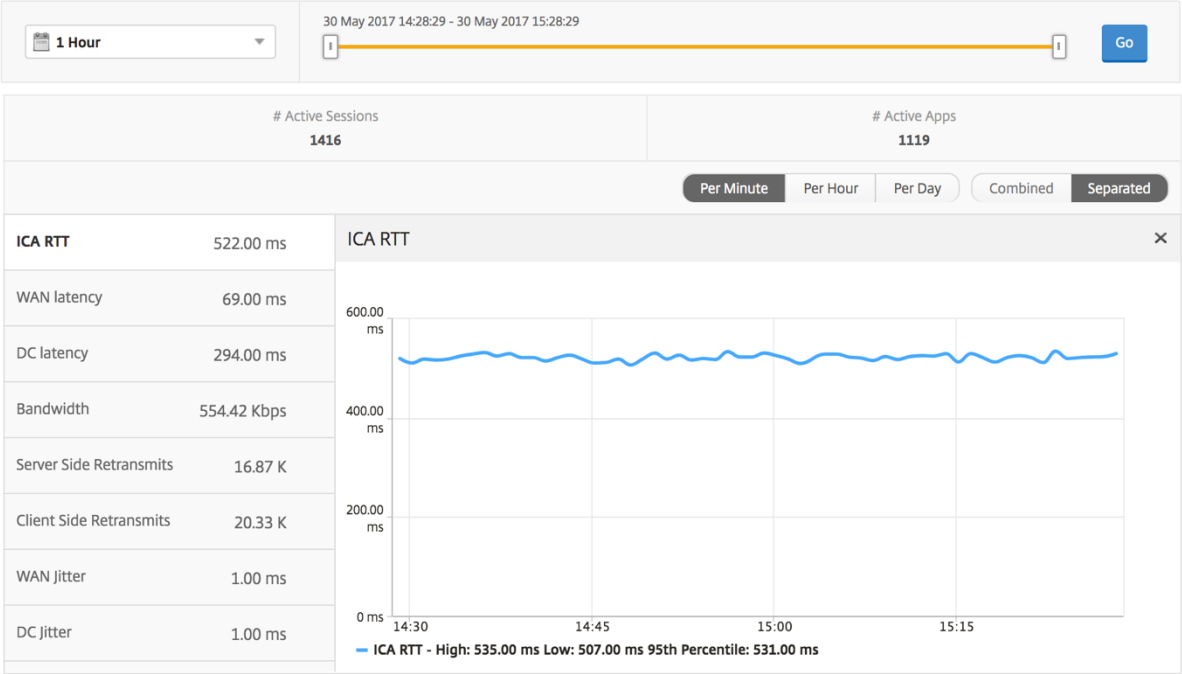
1. Vaya a **Analytics > HDX Insight > Escritorio**.
2. Seleccione un **escritorio** concreto en el **informe de resumen de escritorios**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico de líneas**

| Métricas | Descripción |
| --- | --- |
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual Apps and Desktops. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

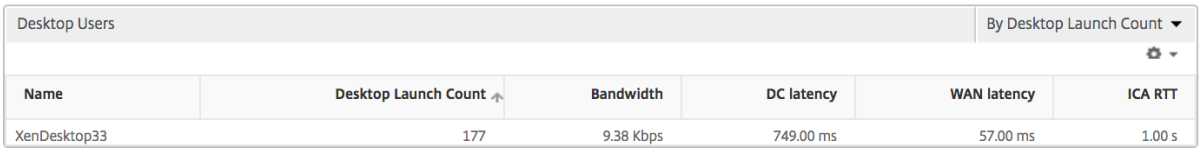



### Informe Usuarios de escritorio

Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual Apps and Desktops, respectivamente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Informe de escritorios de usuario activos e inactivos**

Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

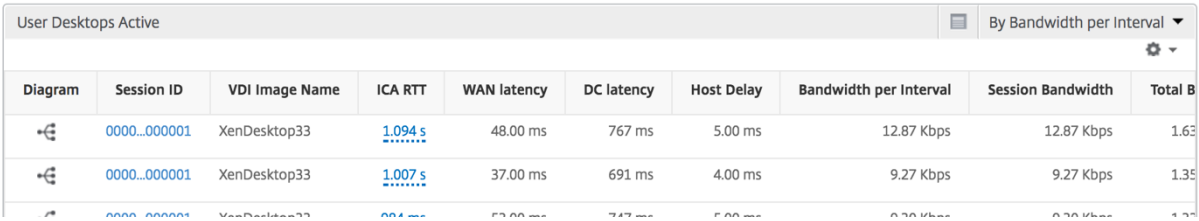
| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler ADC causado por la red de servidores. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | El RTT de ICA es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual Apps o Desktops, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Nombre de la imagen VDI | Nombre del Citrix Virtual Desktops al que está conectado el usuario |
| Diagrama | |




## Por vista de sesión de escritorio

Por vista de sesión de escritorio proporciona informes para una determinada sesión de Citrix Virtual Desktops seleccionada.

**Para desplazarse a la vista de sesión de Escritorio:**

1. Vaya a **Analytics** > **HDX InsightEscritorio**.
2. Seleccione un escritorio concreto en el **informe de resumen de escritorios**.
3. Seleccione una sesión del informe de sesiones actuales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Gráfico cronológico**

La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

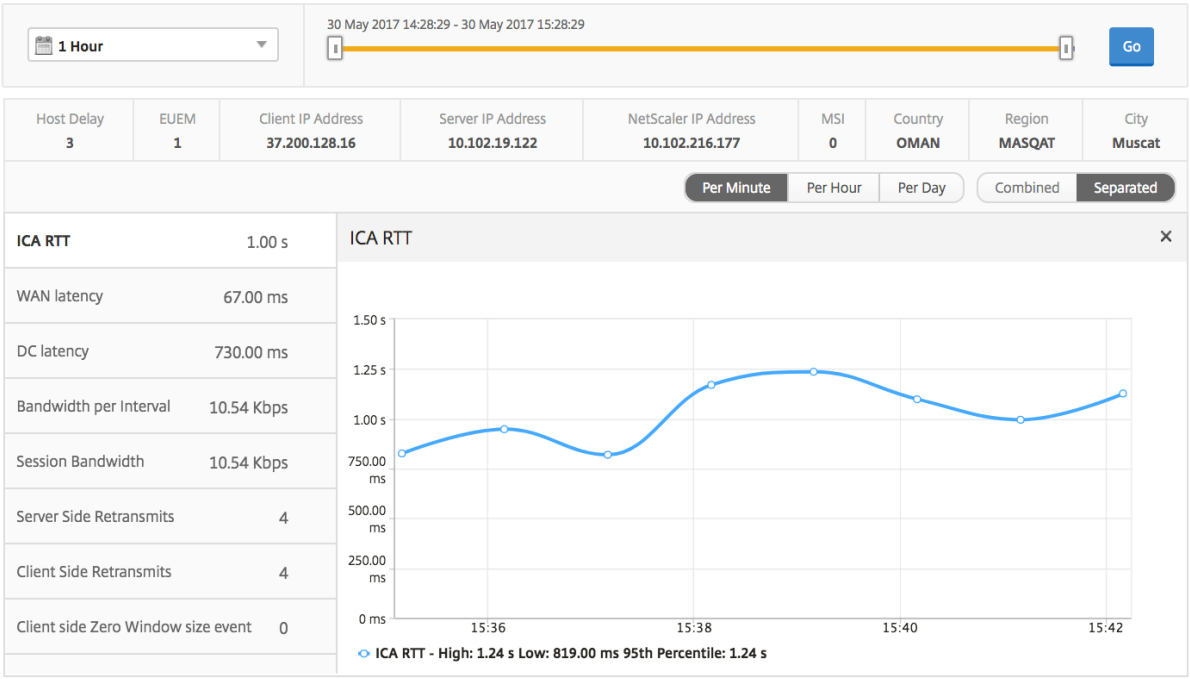
**Para ver las métricas de la sesión de un usuario seleccionado:**

1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.
3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

| Métricas | Descripción |
|---|---|
| Reconexiones de sesión | Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop. |
| Recuento de ACR | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o un escritorio alojados en Citrix Virtual App y Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |




### Informe de sesiones de escritorio relacionadas

Estas métricas siguientes se pueden ordenar por ancho de banda por intervalo, reconexiones de sesión y recuentos de ACR.

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

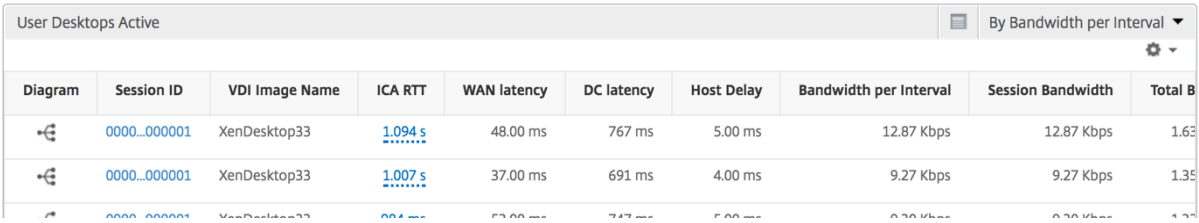
| Métricas | Descripción |
|---|---|
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa a través de los ADC de Citrix causado por la red del servidor. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, el modo usuario/transparente de NetScaler ADC Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor back-end. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se ha producido el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Nombre de la imagen VDI | Nombre del Citrix Virtual Desktops al que está conectado el usuario |

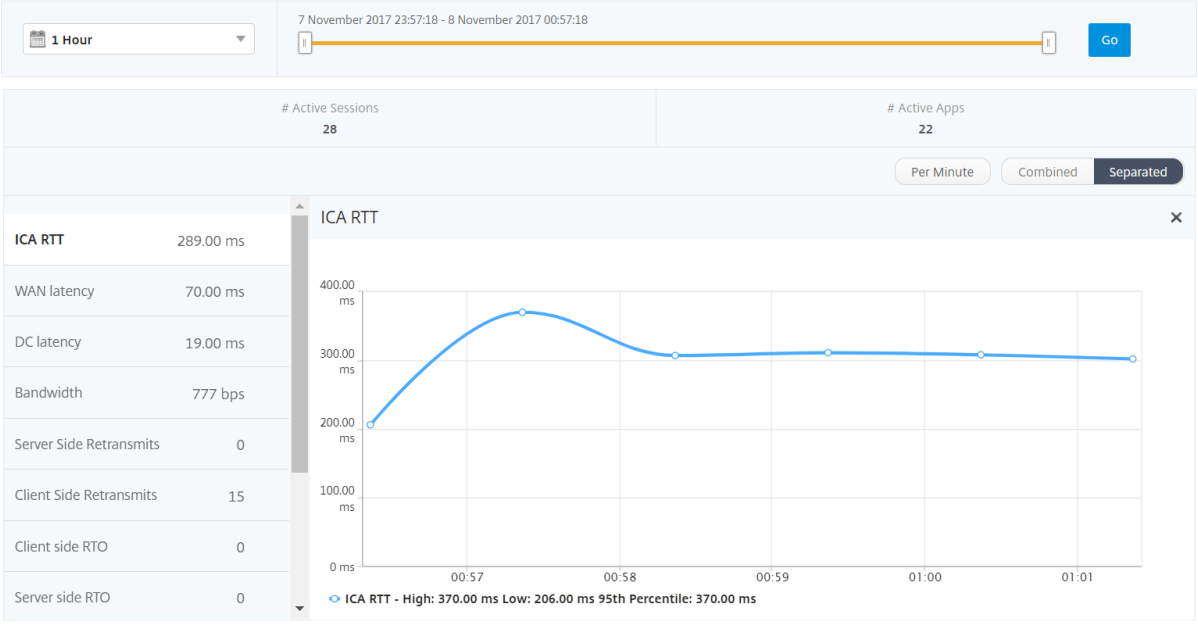



## Informes y métricas de visualización de usuarios

January 30, 2024

Los informes y métricas de esta vista se muestran por usuarios de Citrix Virtual Apps y Desktop.

Vaya a **Analytics** > **HDX Insight** > **Usuarios**.




### Vista de resumen

La vista de resumen muestra los informes de todos los usuarios que han iniciado sesión durante la línea de tiempo seleccionada. Todas las métricas e informes de esta vista muestran los valores correspondientes para el período de tiempo seleccionado, a menos que se especifique lo contrario.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para cambiar el período de tiempo seleccionado:**

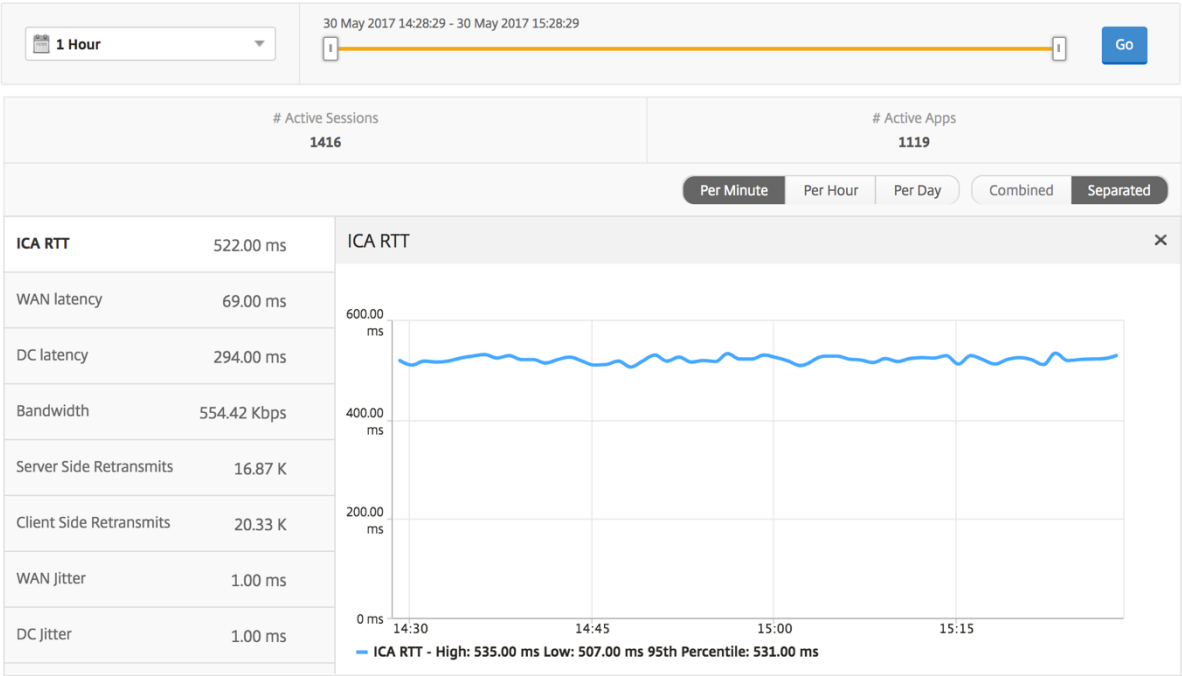
1. Utilice la lista de períodos de tiempo o el control deslizante de tiempo para establecer el intervalo de tiempo deseado.
2. Haga clic en **Ir**.

**Gráfico de líneas**

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores de fondo. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| RTO rápido del lado del servidor | Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |




**Informe resumido de usuarios**

A continuación se presentan las métricas específicas de este informe.

| Métricas | Descripción |
|---|---|
| N.º de sesiones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop. |
| N.º de aplicaciones activas | Este número indica el recuento de sesiones activas de Citrix Virtual App. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores de fondo. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Recuento total de aplicaciones iniciadas | Total de aplicaciones lanzadas por el usuario durante el período de tiempo seleccionado. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Escritorios activos | Número total de Citrix Virtual Desktops activos durante un intervalo de tiempo determinado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

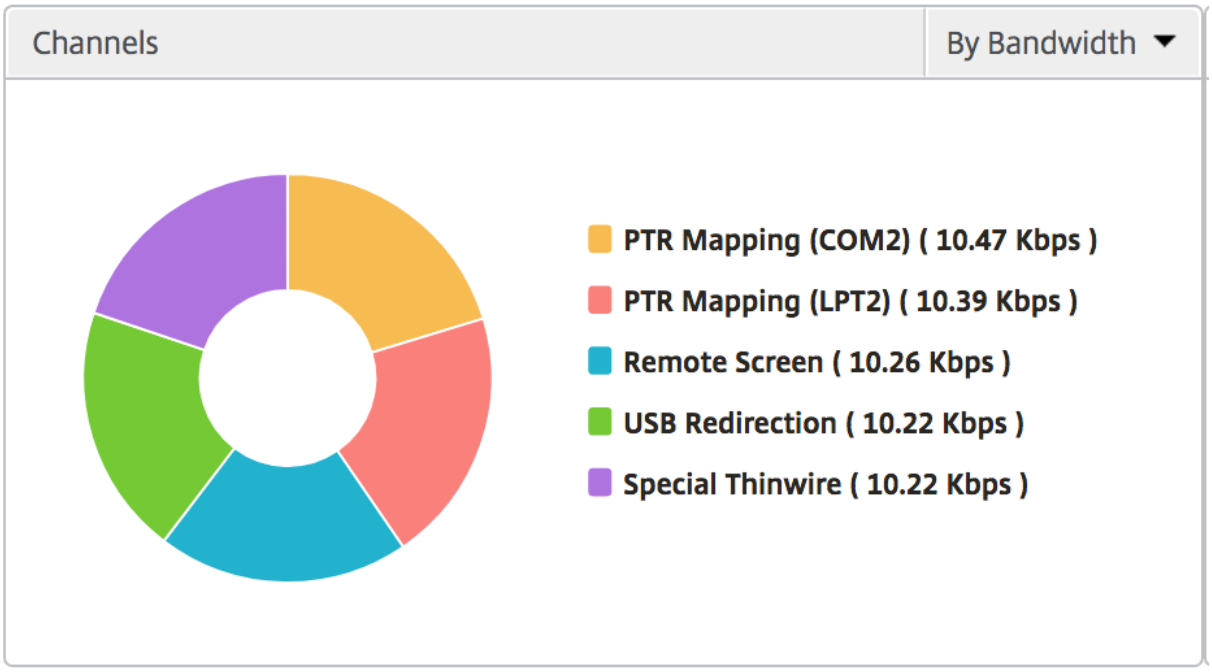
Users

Search

| User Name | # Active Apps | # Active Desktops | # Active Sessions | ICA RTT | WAN latency | DC latency | Bandwidth | Server Side Retransmits | Cl |
|---|---|---|---|---|---|---|---|---|---|
| liam | 59 | 59 | 118 | 999.00 ms | 57.00 ms | 751.00 ms | 47.25 Kbps | 3.74 K | |
| jayden | 59 | 59 | 118 | 999.00 ms | 52.00 ms | 751.00 ms | 47.06 Kbps | 3.71 K | |
| florinl | 59 | 0 | 59 | 997.00 ms | 52.00 ms | 754.00 ms | 23.66 Kbps | 1.88 K | |
| ramas | 59 | 0 | 59 | 997.00 ms | 778.00 ms | 1.00 ms | 7.03 Kbps | 0 | |
| omerp | 59 | 0 | 59 | 997.00 ms | 57.00 ms | 754.00 ms | 23.80 Kbps | 1.89 K | |
| grahmm | 59 | 0 | 59 | 997.00 ms | 53.00 ms | 754.00 ms | 23.80 Kbps | 1.89 K | |
| ryan | 59 | 0 | 59 | 997.00 ms | 53.00 ms | 754.00 ms | 23.69 Kbps | 1.88 K | |
| rajivs | 59 | 0 | 59 | 801.00 ms | 11.00 ms | 1.00 ms | 23.97 Kbps | 0 | |
| alexisc | 117 | 0 | 118 | 622.00 ms | 56.00 ms | 392.00 ms | 47.67 Kbps | 1.88 K | |
| juan | 59 | 59 | 118 | 169.00 ms | 31.00 ms | 29.00 ms | 47.72 Kbps | 0 | |
| lennoxl | 59 | 0 | 59 | 169.00 ms | 31.00 ms | 30.00 ms | 23.86 Kbps | 0 | |
| daniel | 59 | 59 | 118 | 149.00 ms | 31.00 ms | 29.00 ms | 47.72 Kbps | 0 | |
| woojunek | 58 | 0 | 59 | 149.00 ms | 31.00 ms | 30.00 ms | 23.85 Kbps | 0 | |
| parkerf | 59 | 0 | 59 | 149.00 ms | 31.00 ms | 30.00 ms | 23.88 Kbps | 0 | |
| randyb | 59 | 59 | 118 | 99.00 ms | 11.00 ms | 29.00 ms | 47.71 Kbps | 0 | |
| bradp | 177 | 0 | 177 | 74.00 ms | 27.00 ms | 1.00 ms | 71.75 Kbps | 0 | |

### Canales

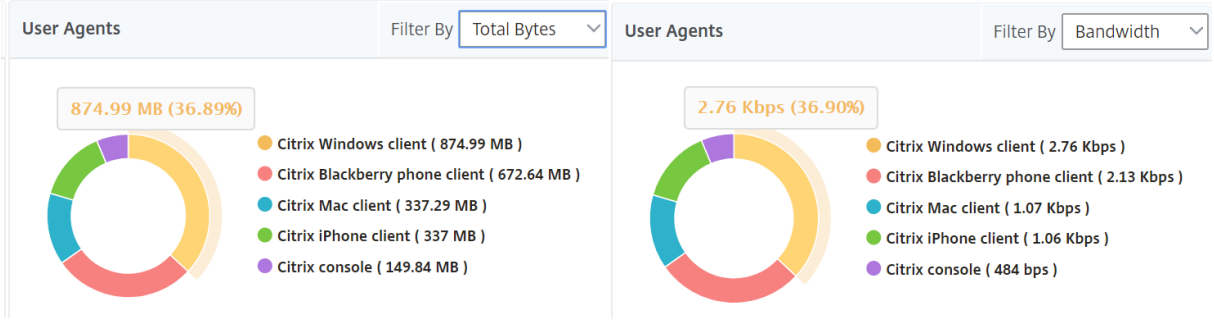
Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Agentes de usuario

Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.




### Recuento de infracciones de umbrales

Las métricas de recuento de infracciones de Umbrales representan el recuento de umbrales incumplidos en el período de tiempo seleccionado. Para obtener más información, consulta cómo crear umbrales y alertas.

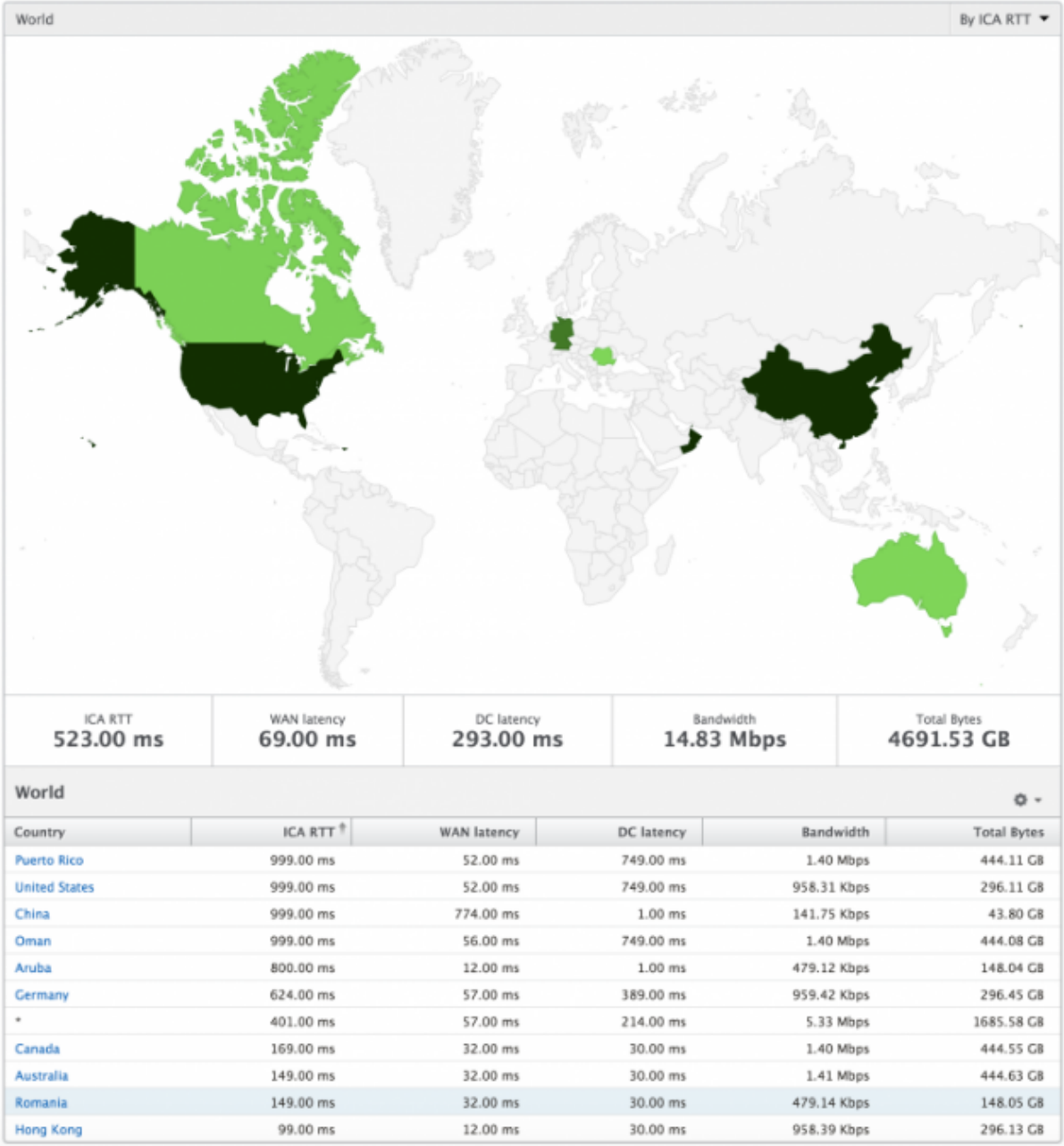
### Mapa del mundo

La vista de mapa mundial en HDX Insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más en las ciudades, así como hacer clic en la región. Los administradores pueden profundizar aún más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

## Por vista de usuario

La vista por usuario proporciona informes detallados de la experiencia del usuario final para cualquier usuario seleccionado en particular.

**Para navegar a métricas específicas de usuario:**

1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Seleccione un usuario concreto en el informe Resumen de usuarios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Gráfico de líneas

El gráfico de líneas muestra el resumen de todas las métricas del usuario seleccionado en particular durante el período de tiempo seleccionado.

### Informe de sesiones actuales/terminadas

Este informe es pertinente para todas las sesiones de usuario actuales/terminadas del usuario seleccionado. Estas métricas se pueden ordenar por hora de inicio, reconexiones de sesión y recuento de ACR.

| Métricas | Descripción |
|---|---|
| ID de sesión | Una identidad única para una sesión ICA. |
| Tipo de sesión | Aplicación/escritorio. |
| State | Verde/rojo para las sesiones activas/inactivas. |
| Demora de host | Retraso promedio en el tráfico ICA que pasa por los ADC de NetScaler ADC causado por la red de servidores. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Bytes por intervalo | Número de bytes consumidos por la sesión durante ese intervalo de tiempo en particular. |
| Hora de inicio | Hora de inicio de sesión. |
| Tiempo de actividad | Duración de la sesión. |
| Dirección IP del cliente | IP del usuario final. |
| Dirección IP del servidor | IP del servidor Backend/Citrix Virtual App. |
| Dirección IP de NetScaler | IP de administración de NetScaler (NSIP). |
| Tipo de cliente | Tipo de receptor: Citrix Windows Client, etc. |
| Versión del cliente | Versión receptor. |
| MSI | Booleano (sí/no). Indica si la sesión es ICA multisecuencia. |
| Reconexiones de sesión | Número de veces que se volvió a conectar la sesión. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Recuento de ACR | Número total de veces que un cliente vuelve a conectar automáticamente a los usuarios a sesiones desconectadas. |
| Tipo de acceso de usuario | Muestra el modo de acceso de la sesión ICA. Por ejemplo, modo usuario/transparente de NetScaler Gateway. |
| País | País desde el que se estableció la sesión. |
| Region | Región desde la que se estableció la sesión. |
| City | Ciudad desde la que se estableció la sesión. |
| Estado USB | Activo/Inactivo -Verde/Rojo. |
| Número de instancias USB aceptadas | El recuento de instancias USB aceptadas. |
| Número de instancias USB rechazadas | El recuento de instancias USB rechazadas. |
| Número de instancias USB detenidas | Se detuvo el recuento de instancias USB. |
| Nombre de host del cliente | El nombre de host del cliente. |
| Recuento de failover de HA | Número de veces que se produjo la conmutación por error de HA |
| Motivo de rescisión | Muestra el motivo de la finalización de la sesión. Por ejemplo, Tiempo de espera de sesión ICA, Sesión finalizada por el usuario. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores de fondo. |
| Total de bytes | Total de bytes consumidos por el usuario durante el período de tiempo seleccionado. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

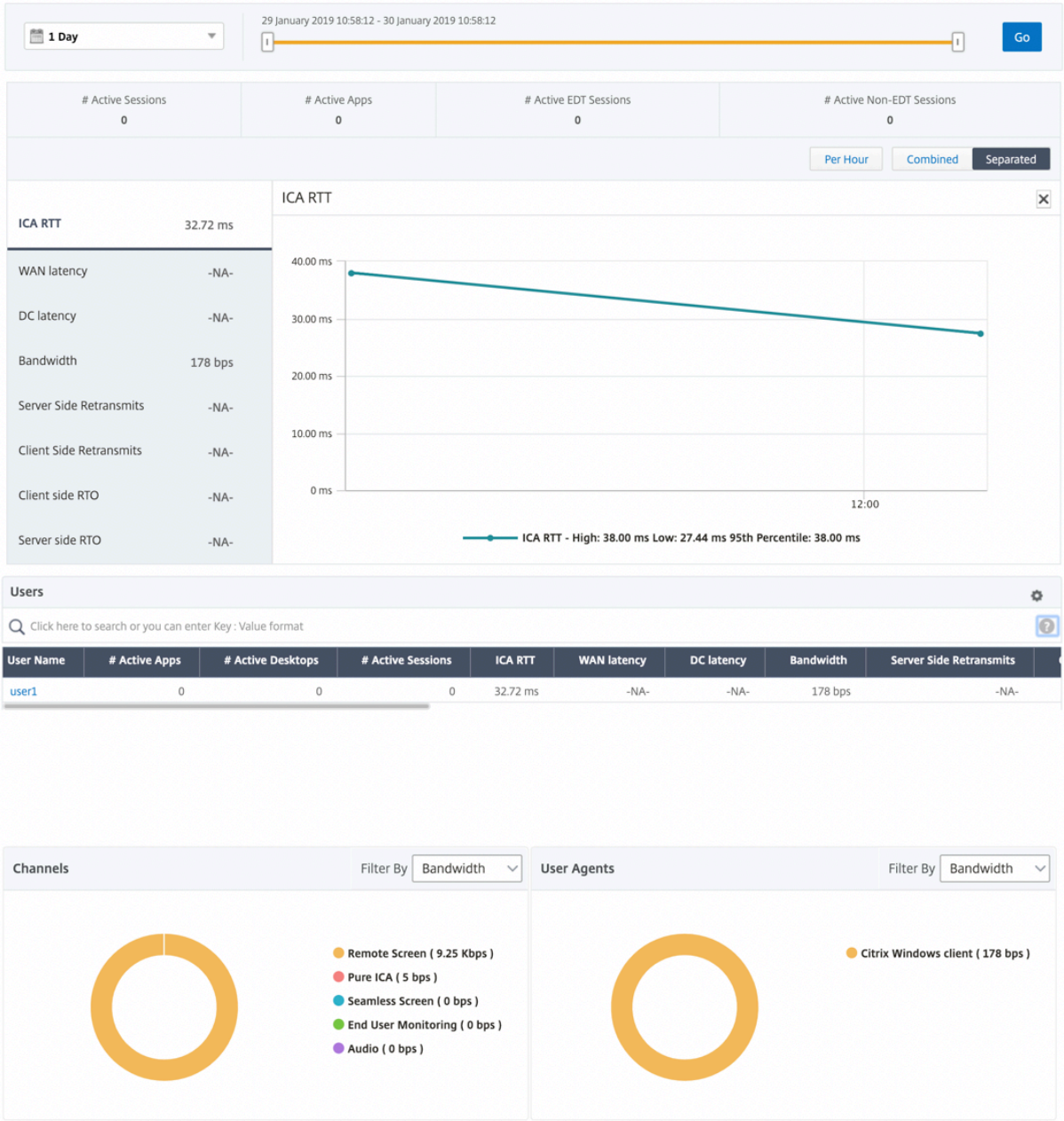
| Métricas | Descripción |
|---|---|
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| RTO rápido del lado del servidor | Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |

**Soporte para EDT en HDX insights**

NetScaler Application Delivery Management (ADM) ahora admite el transporte de datos ilustrados (EDT) para mostrar análisis para HDX Insight. Es decir, ADM ahora admite los protocolos UDP y TCP. La compatibilidad de EDT con NetScaler Gateway garantiza una experiencia de usuario de alta definición durante la sesión de los escritorios virtuales para los usuarios que ejecutan Citrix Receiver

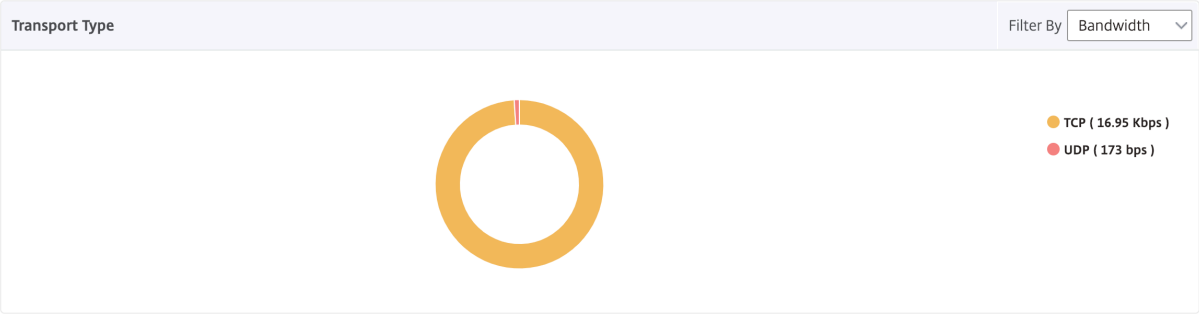
HDX Insight ahora muestra el número de sesiones de EDT y de sesiones que no son de EDT como parte del informe de sesiones activas. La tabla Usuarios muestra un informe detallado de todos los usuarios del sistema. La tabla muestra métricas como la latencia de WAN, la latencia de DC, las retransmisiones y los RTO. Algunas de estas métricas no están disponibles para los usuarios que sí tienen sesiones de EDT, ya que actualmente se calculan a partir de la pila de TCP. Por lo tanto, aparecen como “NA”.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



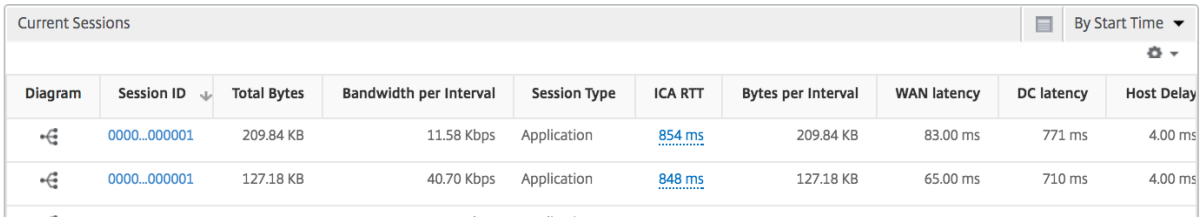

Se ha introducido un nuevo gráfico de donut para permitirle ver el ancho de banda consumido por el usuario y también el número total de bytes según el tipo de protocolo utilizado por los usuarios.

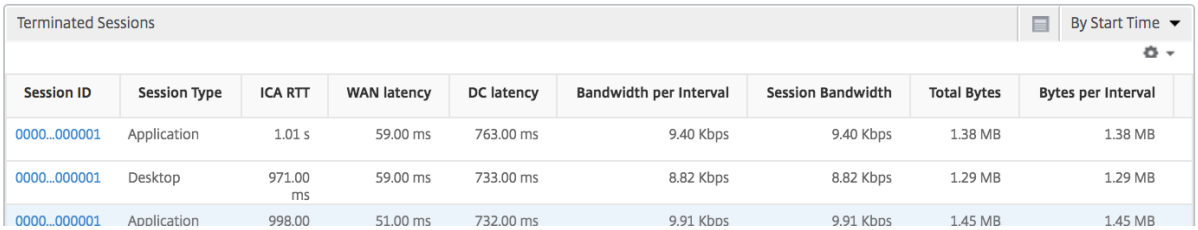
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Métricas de HDX Insight disponibles en NetScaler ADM 12.0 y versiones posteriores:**

| | |
|---|---|
| Latencia del lado del cliente L7 | Latencia media de L7 observada entre el cliente ICA y la instancia de NetScaler ADC. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |
| Latencia L7 del lado del servidor | La latencia media de L7 observada entre el dispositivo NetScaler ADC y Citrix Virtual App. Esta métrica es útil en el caso de que los dispositivos que no son Citrix estén presentes en la ruta de entrega. |
| Latencia de vulneración máxima | El valor más alto de la latencia L7 cuando se produce una violación de un umbral definido durante un intervalo de tiempo establecido. |
| Latencia de violación promedio | El valor promedio de la latencia L7 cuando el sistema se encuentra en un estado de “latencia L7 infringida”. |
| Recuento de incumplimiento de umbral L7 | Número de veces que se ha producido una infracción del umbral L7. |



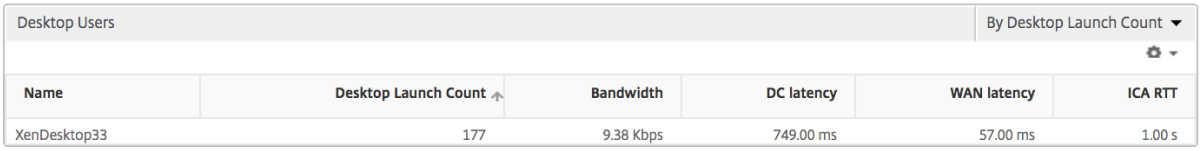




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Usuarios de escritorio

Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

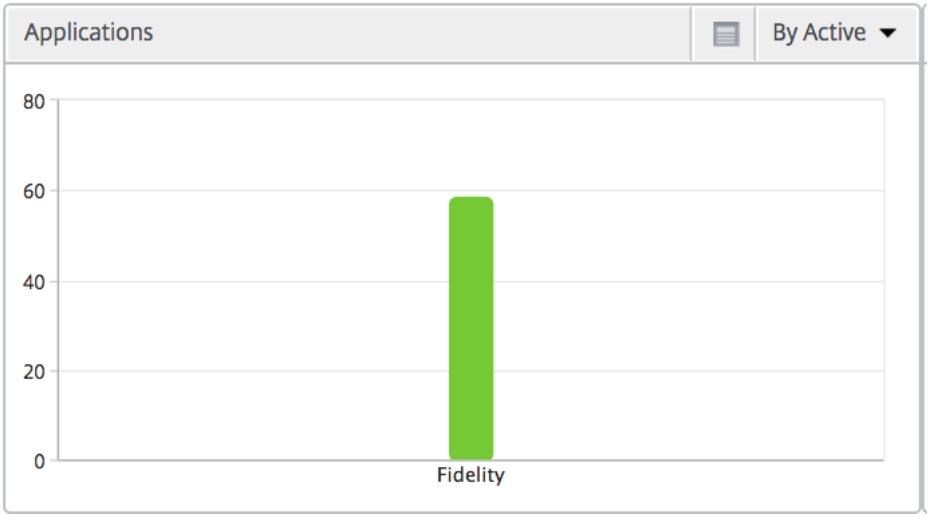
| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores de fondo. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |




### Aplicaciones

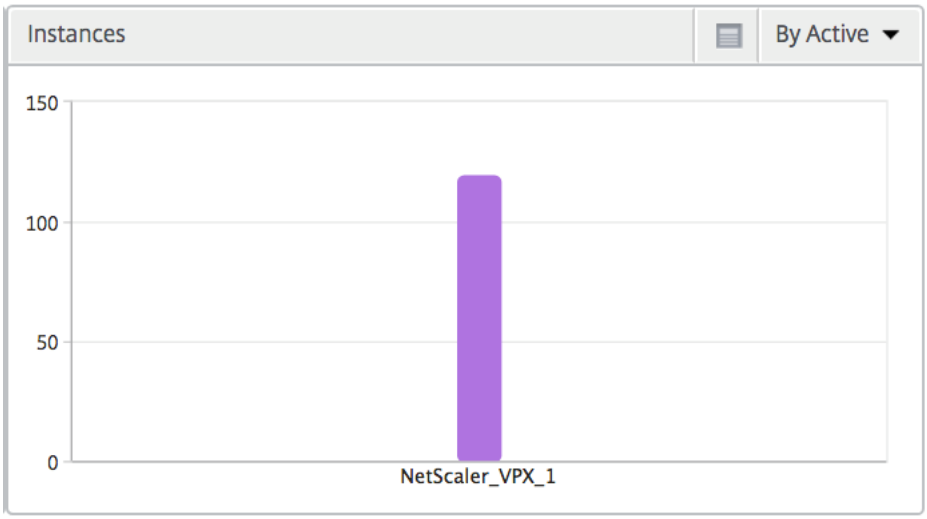
Gráfico de barras que representa las aplicaciones ordenadas por Activo, recuento total de inicio de sesión, recuento total de inicio de aplicaciones y duración del lanzamiento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Instancias**

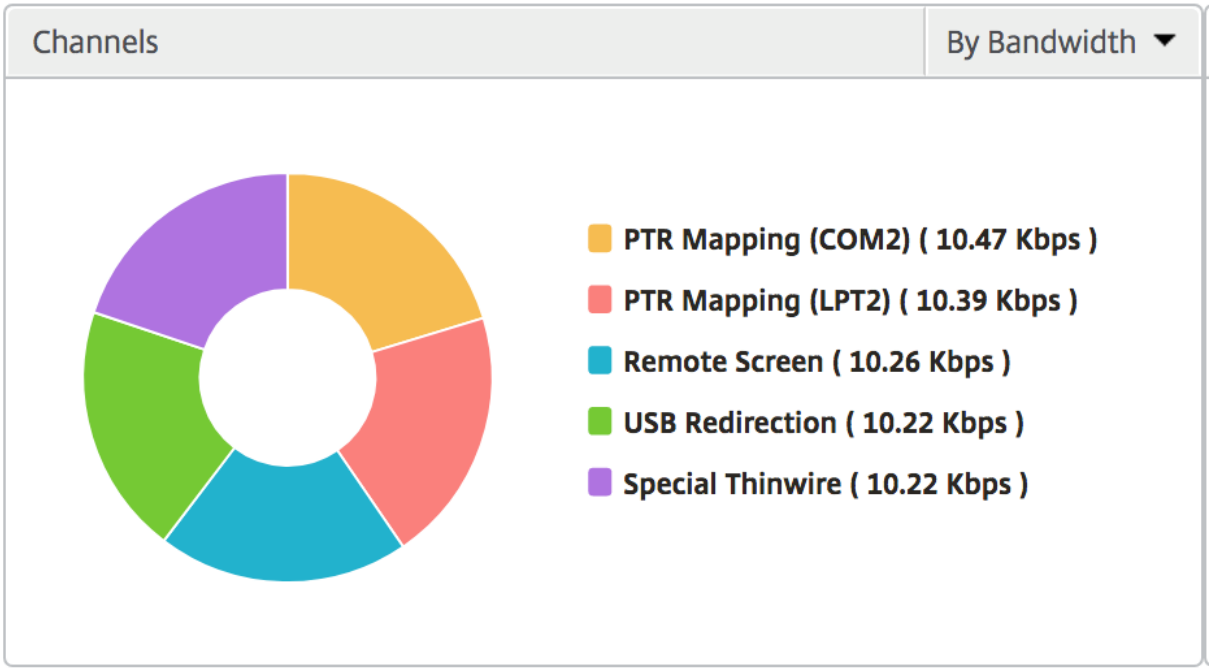
Un gráfico de barras que representa las instancias de NetScaler ADC ordenadas por aplicaciones activas y totales




**Canales**

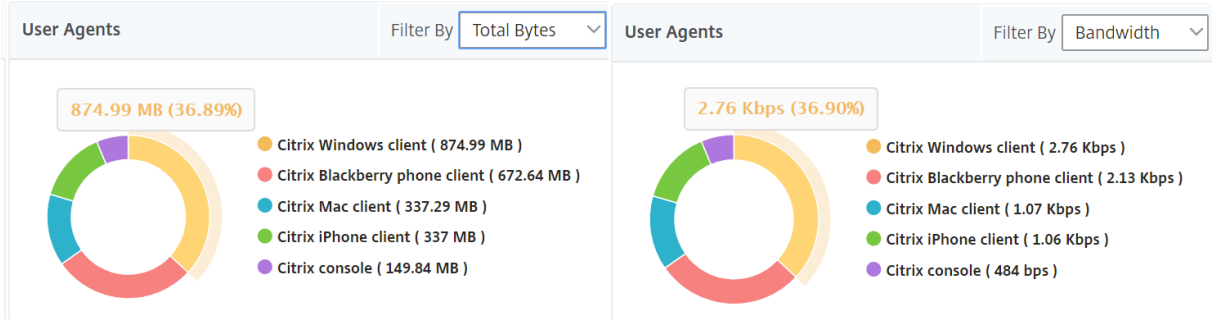
Los canales representan el ancho de banda total o los bytes totales consumidos por cada canal virtual ICA en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Agentes de usuario**

Los agentes de usuario representan el ancho de banda general y los bytes totales consumidos por cada punto final en forma de gráfico de anillos. También puede ordenar las métricas por ancho de banda o bytes totales.




## Vista de sesión por usuario

La vista de sesión por usuario proporciona informes para la sesión de un usuario seleccionado en particular.

**Para ver las métricas de la sesión de un usuario seleccionado:**

1. Vaya a **Analytics** > **HDX Insight** > **Usuarios**.
2. Select un usuario concreto en la sección **Informe de resumen de usuario**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

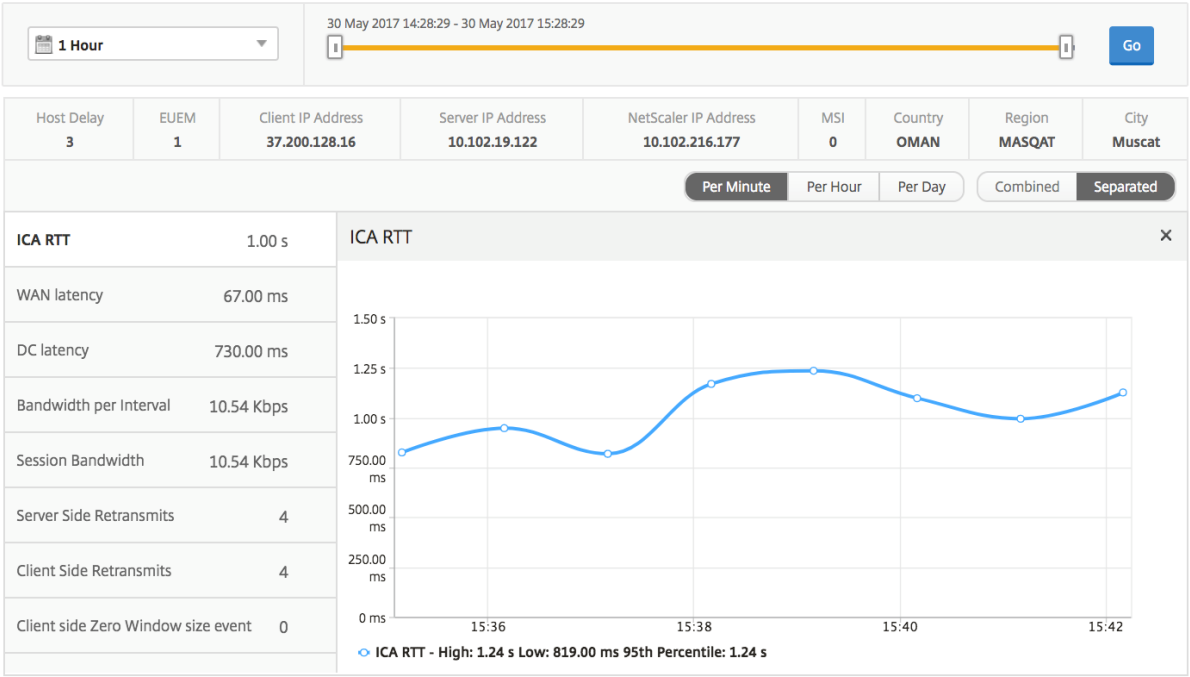
3. Seleccione una sesión en la columna **Sesiones actuales** o **Sesiones terminadas**.

**Gráfico cronológico**

| Métricas | Descripción |
|---|---|
| Reconexiones de sesión | Este número indica el recuento de sesiones activas de Citrix Virtual App and Desktop. |
| Recuento de ACR | Este número indica el recuento de sesiones activas de Citrix Virtual App. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores de fondo. |
| Ancho de banda de la sesión | El ancho de banda consumido por la sesión, independientemente del intervalo de tiempo. |
| Retransmisiones del lado del servidor | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el servidor backend. |
| Retransmisiones del lado del cliente | El número de paquetes retransmitidos en la conexión entre NetScaler ADC y el usuario final. Un alto valor de esta métrica no significa que la experiencia del usuario no sea perfecta, sino que indica una alta utilización del ancho de banda debido a las retransmisiones. |
| RTO rápido del lado del cliente | Número de veces que se agotó el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el usuario final. |
| RTO rápido del lado del servidor | Número de veces que se produjo el tiempo de espera de retransmisión en la conexión entre NetScaler ADC y el servidor back-end. |
| Ancho de banda por intervalo | El ancho de banda consumido por la sesión durante ese intervalo de tiempo en particular. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
|---|---|
| Evento de ventana cero en el lado del servidor | Este contador indica el número de veces que el servidor anunció una ventana TCP cero. |
| Evento de ventana cero en el lado del cliente | Este contador indica el número de veces que el cliente anunció una ventana TCP cero. |



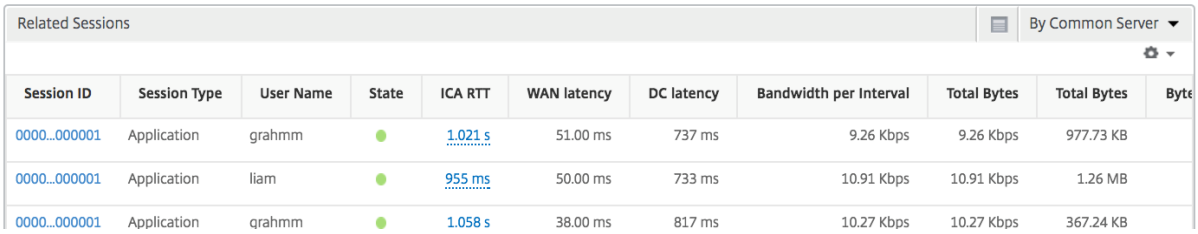

## Aplicación activa

La sección **Aplicaciones activas** muestra las aplicaciones activas del usuario seleccionado. Estas aplicaciones también se pueden ordenar por número de sesiones activas y duración de inicio.

## Sesiones relacionadas

La sección Sesiones relacionadas muestra las sesiones relacionadas de las sesiones del usuario seleccionado. La relación se puede seleccionar como servidores comunes o común de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



Related Sessions | By Common Server

| Session ID | Session Type | User Name | State | ICA RTT | WAN latency | DC latency | Bandwidth per Interval | Total Bytes | Total Bytes | Byte |
|---|---|---|---|---|---|---|---|---|---|---|
| 0000...000001 | Application | grahmm | | 1.021 s | 51.00 ms | 737 ms | 9.26 Kbps | 9.26 Kbps | 977.73 KB | |
| 0000...000001 | Application | liam | | 955 ms | 50.00 ms | 733 ms | 10.91 Kbps | 10.91 Kbps | 1.26 MB | |
| 0000...000001 | Application | grahmm | | 1.058 s | 38.00 ms | 817 ms | 10.27 Kbps | 10.27 Kbps | 367.24 KB | |

# Informes y métricas de vista de instancias

January 30, 2024

Los informes y las métricas de la vista de instancias se centran en las instancias de NetScaler ADC.

**Para desplazarse a la vista de instancia:**

1. Vaya a **Analytics** > **HDX InsightInstancias**.

## Vista de resumen de instancia

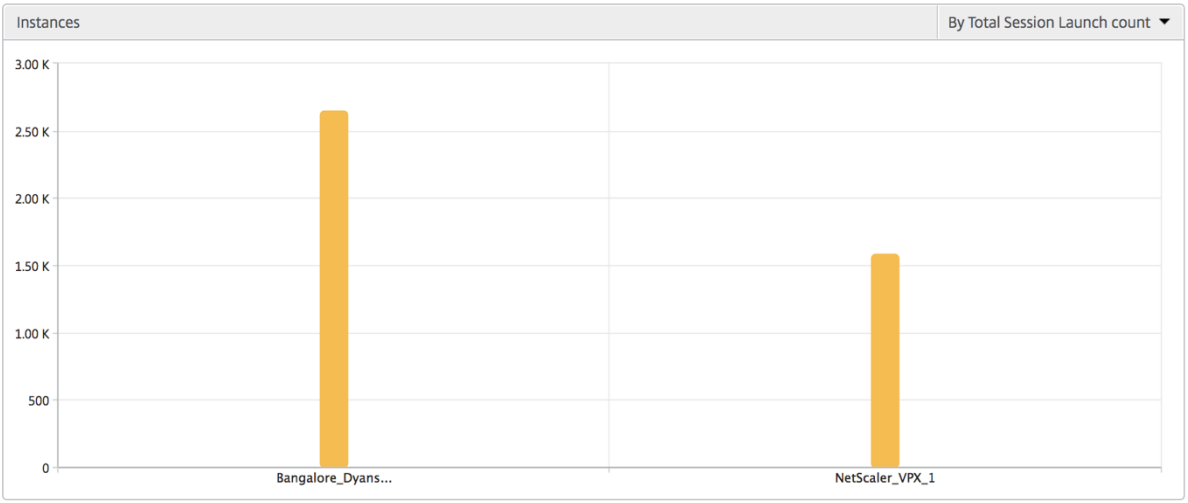
Esta vista se denomina vista de resumen, ya que muestra los informes de todas las instancias de NetScaler ADC que se agregan a NetScaler ADM.

Todas las métricas/informes, a menos que se mencionen explícitamente, tendrán los valores correspondientes para el período de tiempo seleccionado.

### Gráfico de barras de instancia

Este gráfico muestra la instancia frente al recuento total de inicio de sesión y Total de aplicaciones que se pueden seleccionar de la lista en la parte superior derecha del lienzo del gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Informe de resumen de instancia/instancias activas

| Métricas | Descripción |
|---|---|
| Nombre | Nombre de host de la instancia de NetScaler ADC. |
| Dirección IP | Dirección IP de NetScaler. |
| Recuento total de sesiones iniciadas | Número total de sesiones de usuario únicas creadas durante un intervalo de tiempo determinado. |
| Total de aplicaciones | Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado. |
| Tipo | N/D |

Instances

| Name | IP Address | Total Session Launch count | Total Apps | Type |
|---|---|---|---|---|
| Bangalore_Dyansty(10.102.216.219) | 10.102.216.219 | 2.65 K | 2.12 K | -NA- |
| NetScaler_VPX_1(10.102.216.177) | 10.102.216.177 | 1.59 K | 1.24 K | -NA- |

**Active Instances**

| Name | IP Address | # Active Sessions | # Active Apps | # Active Desktops | Type |
|---|---|---|---|---|---|
| NetScaler_VPX_1(10.102.216.177) | 10.102.216.177 | 538 | 417 | 120 | -NA- |
| Bangalore_Dyansty(10.102.216.219) | 10.102.216.219 | 900 | 720 | 180 | -NA- |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Informe Umbral

El informe Umbral representa el recuento de umbrales incumplidos cuando se selecciona la *entidad* como Instancia en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

### Flujos omitidos

Un flujo omitido es un registro que omitió el análisis de la conexión ICA. Esto puede deberse a varios motivos, como el uso de versiones no compatibles de Citrix Virtual Apps and Desktops, una versión no compatible del receptor o el tipo de receptor, etc. Esta tabla muestra la dirección IP y el recuento de flujo omitido. Es posible que estos receptores no formen parte de los receptores de la lista de permitidos. Por lo tanto, estas sesiones se saltan de la supervisión.

¡Ver **error! La referencia de hipervínculo no es válida** para obtener más detalles sobre problemas relacionados con el análisis ICA.

Skipped Flows

| IP Address | Skipped Count |
|---|---|
| 10.105.2.141 | 1 |
| 10.105.2.142 | 1 |

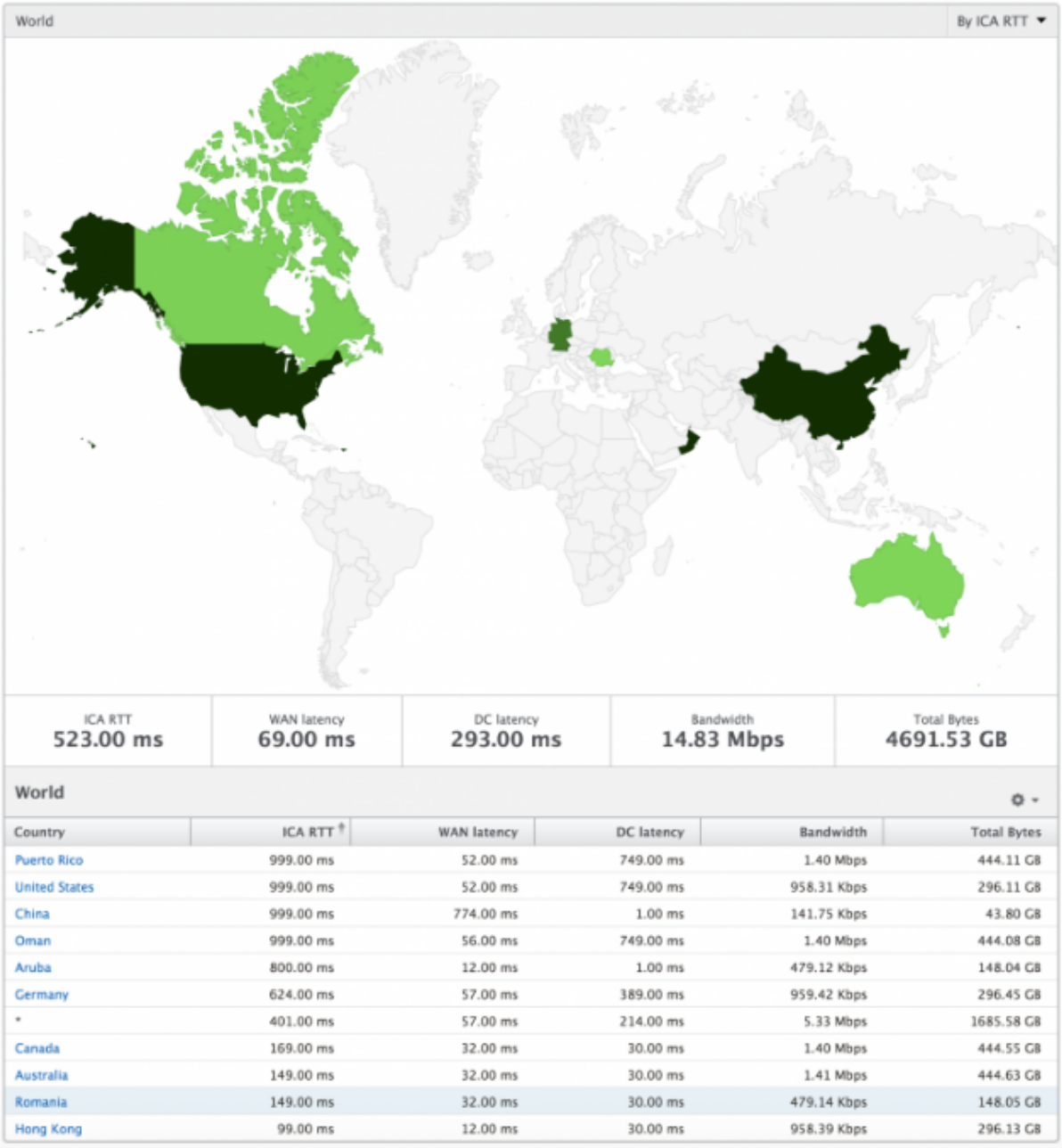
### Visión del mundo

La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más en las ciudades, así como hacer clic en la región. Los administradores pueden profundizar más para ver la información por ciudad y estado. Desde NetScaler ADC versión 12.0 y posterior, puede profundizar en los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

## Vista por instancia

Por vista de instancia proporciona informes detallados sobre la experiencia del usuario final para una instancia específica de NetScaler ADC seleccionada.

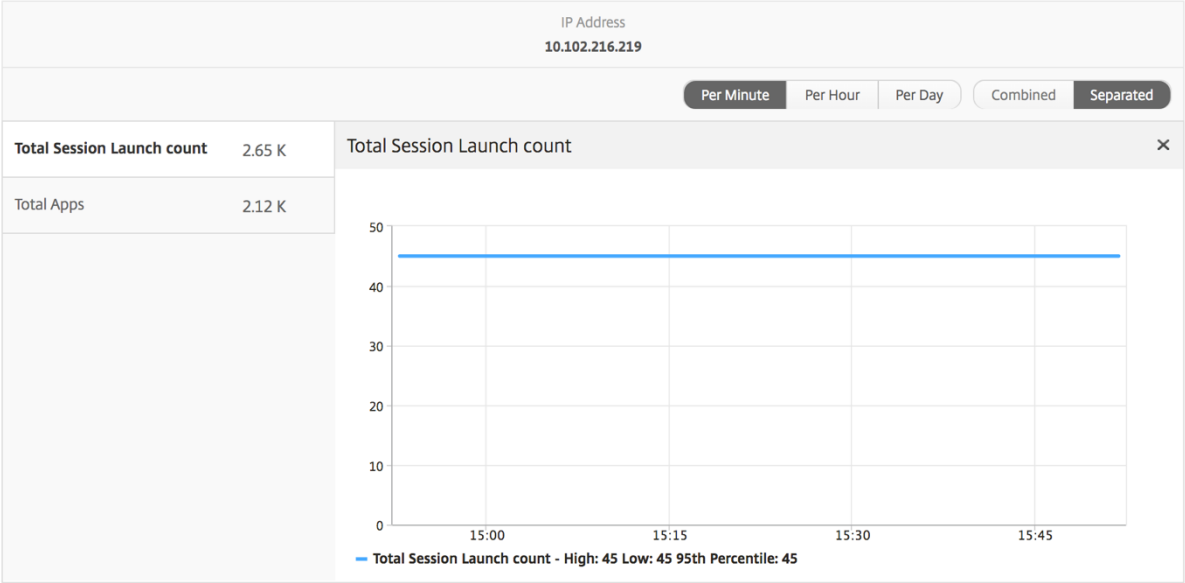
**Para desplazarse a la vista de instancia:**

1. Vaya a **Analytics** > **HDX InsightInstancias**.
2. Seleccione una instancia concreta en el **informe Resumen de Instancia**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

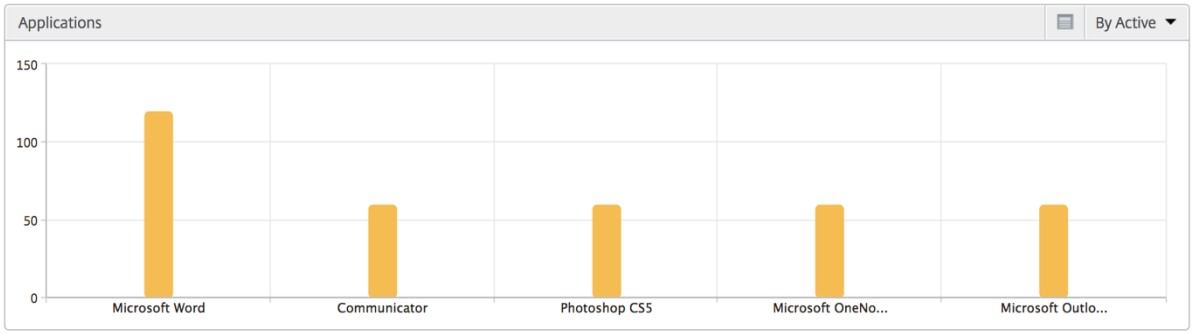
### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| Dirección IP | Representa la dirección IP de NetScaler de la instancia seleccionada. |
| Recuento total de sesiones iniciadas | Número total de sesiones activas de Citrix Virtual App durante el intervalo de tiempo dado. |
| Total de aplicaciones | Número total de aplicaciones únicas iniciadas durante un intervalo de tiempo determinado. |




### Gráfico de barras de aplicaciones

Muestra las 5 aplicaciones principales según los siguientes criterios: por aplicaciones activas, recuento total de inicios de sesiones, recuento total de inicios de aplicaciones o duración del lanzamiento.

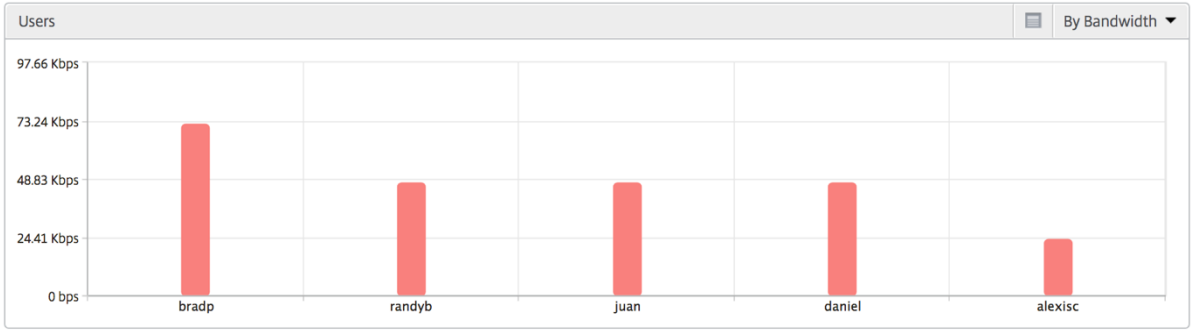



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Gráfico de barras de usuarios

El gráfico de barras Usuarios muestra los 5 usuarios principales en función de los siguientes criterios

- Ancho de banda
- Latencia de WAN
- Latencia de DC
- RTT de ICA




### Informe Usuarios de escritorio

Esta tabla ofrece información sobre las sesiones de Citrix Virtual Desktop para un usuario en particular. Estas métricas se pueden ordenar por número de lanzamientos de escritorios y ancho de banda.

| Métricas | Descripción |
|---|---|
| Nombre | Nombre del escritorio virtual de Citrix. |
| Recuento de lanzamientos | Número de veces que se ha iniciado el escritorio. |
| Ancho de banda | Total de bytes por segundo tomados para la comunicación de extremo a extremo durante el intervalo de tiempo seleccionado. |
| Latencia de DC | Latencia causada por el lado del servidor de la red. Es decir, desde NetScaler ADC hasta servidores back-end. |
| Latencia de WAN | Latencia causada por el lado cliente de la red. Es decir, desde NetScaler ADC hasta el usuario final. |
| RTT de ICA | ICA RTT es el retraso de pantalla que experimenta el usuario al interactuar con una aplicación o escritorio alojado en Citrix Virtual App o Desktop, respectivamente. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Desktop Users | By Desktop Launch Count

| Name | Desktop Launch Count | Bandwidth | DC latency | WAN latency | ICA RTT |
|---|---|---|---|---|---|
| XenDesktop33 | 177 | 9.38 Kbps | 749.00 ms | 57.00 ms | 1.00 s |

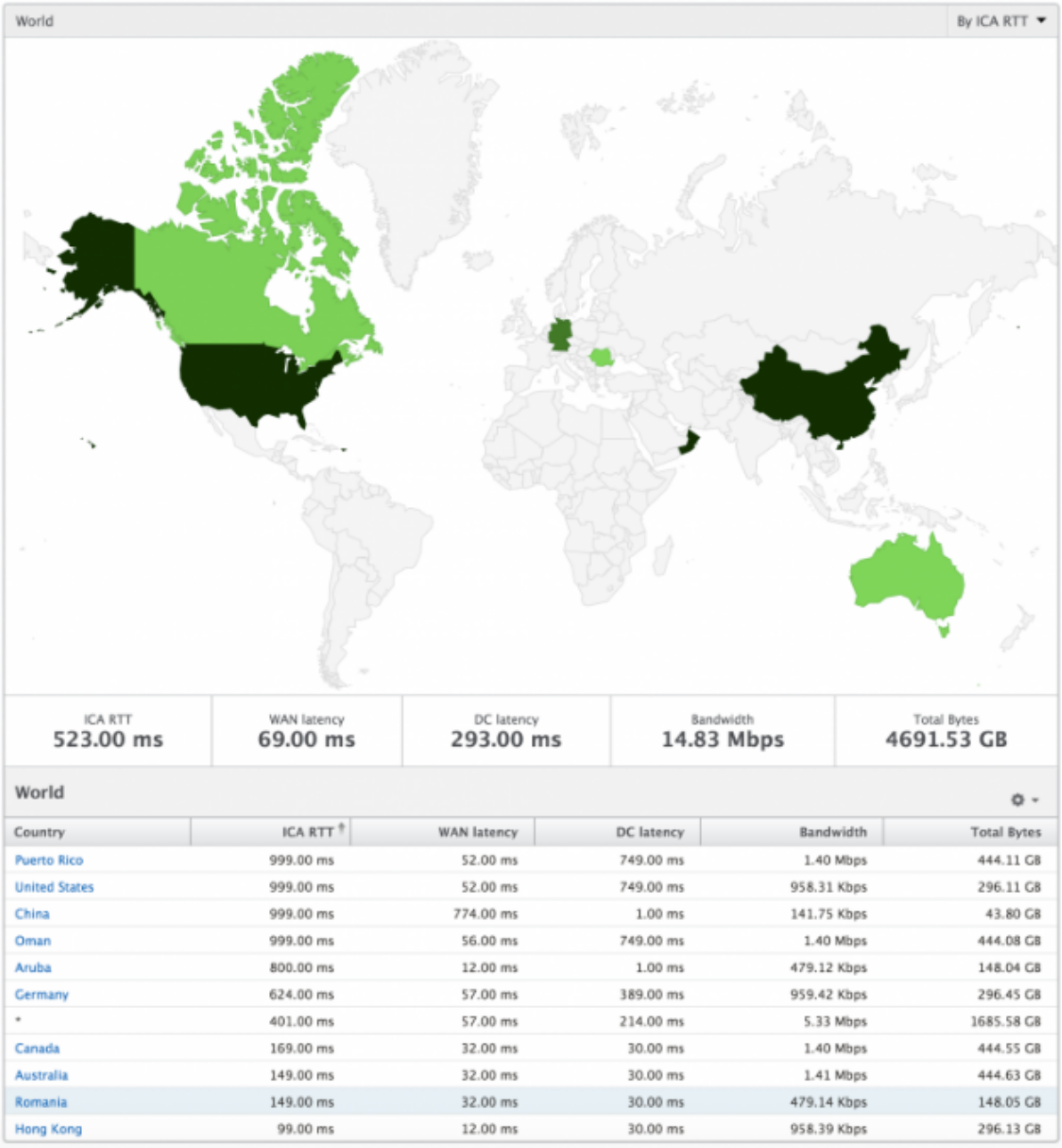
### Visión del mundo

La vista de mapa mundial en HDX insight permite a los administradores ver los detalles históricos y activos de los usuarios desde un punto de vista geográfico. Los administradores pueden tener una visión mundial del sistema, profundizar en un país en particular y más hacia las ciudades también haciendo clic en la región. Los administradores pueden profundizar más para ver la información por ciudad y estado. Desde NetScaler ADM versión 12.0 y posterior, puede acceder a los usuarios conectados desde una ubicación geográfica.

Los siguientes detalles se pueden ver en el Mapa del Mundo en HDX insights, y la densidad de cada métrica se muestra en forma de mapa térmico:

- RTT de ICA
- Latencia de WAN
- Latencia de DC
- Ancho de banda
- Total de bytes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




| Country | ICA RTT | WAN latency | DC latency | Bandwidth | Total Bytes |
|---|---|---|---|---|---|
| Puerto Rico | 999.00 ms | 52.00 ms | 749.00 ms | 1.40 Mbps | 444.11 GB |
| United States | 999.00 ms | 52.00 ms | 749.00 ms | 958.31 Kbps | 296.11 GB |
| China | 999.00 ms | 774.00 ms | 1.00 ms | 141.75 Kbps | 43.80 GB |
| Oman | 999.00 ms | 56.00 ms | 749.00 ms | 1.40 Mbps | 444.08 GB |
| Aruba | 800.00 ms | 12.00 ms | 1.00 ms | 479.12 Kbps | 148.04 GB |
| Germany | 624.00 ms | 57.00 ms | 389.00 ms | 959.42 Kbps | 296.45 GB |
| * | 401.00 ms | 57.00 ms | 214.00 ms | 5.33 Mbps | 1685.58 GB |
| Canada | 169.00 ms | 32.00 ms | 30.00 ms | 1.40 Mbps | 444.55 GB |
| Australia | 149.00 ms | 32.00 ms | 30.00 ms | 1.41 Mbps | 444.63 GB |
| Romania | 149.00 ms | 32.00 ms | 30.00 ms | 479.14 Kbps | 148.05 GB |
| Hong Kong | 99.00 ms | 12.00 ms | 30.00 ms | 958.39 Kbps | 296.13 GB |

## Informes y métricas de vista de licencias

January 30, 2024

La vista de licencia proporciona detalles sobre la información de licencia de NetScaler Gateway.

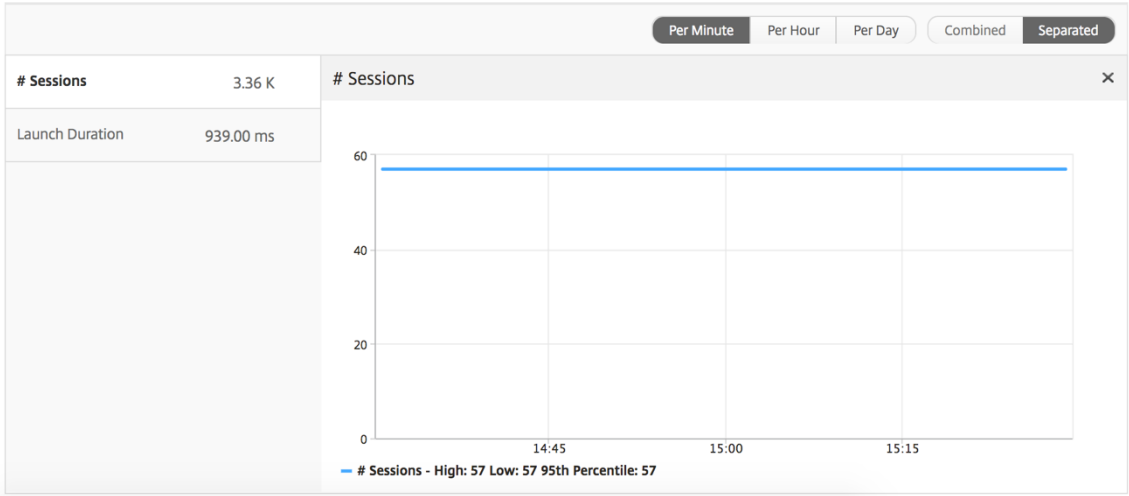
**Para navegar a la vista de licencia:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Analytics** > **HDX Insight** > **Licencias**.

### Gráfico de líneas

| Métricas | Descripción |
|---|---|
| Licencias en uso | Las licencias de CCU de NetScaler Gateway que se utilizan durante el plazo seleccionado. Cada recuento representa el número de sesiones de usuario. Esto es independiente de las sesiones de aplicaciones y escritorios iniciadas por ese usuario. |
| Total de licencias | Número total de licencias CCU de NetScaler Gateway disponibles para que el cliente las utilice. |




### Informe Umbral

El informe de umbral representa el recuento de umbrales incumplidos cuando la *entidad* se selecciona como Licencia en el período seleccionado. Para obtener más información, consultacómo crear umbrales y alertas.

## Solucionar problemas de HDX Insight

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Si la solución HDX Insight no funciona según lo esperado, es posible que el problema se deba a uno de los siguientes motivos. Consulte las listas de comprobación de las secciones correspondientes para la solución de problemas.

- Configuración de HDX Insight.
- Conectividad entre NetScaler ADC y NetScaler ADM.
- Generación de registros para el tráfico HDX/ICA en NetScaler ADC.
- Población de registros en NetScaler ADM.

### Lista de comprobación de configuración de HDX Insight

- Asegúrese de que la función AppFlow esté habilitada en NetScaler ADC. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de HDX Insight en la configuración de NetScaler ADC en ejecución.

  Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de HDX Insight. Asegúrese de que el tipo de enlace es ICA REQUEST. Por ejemplo:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  Para el modo transparente, el tipo de enlace debe ser ICA_REQ_DEFAULT. Por ejemplo:

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- Para la implementación de Access Gateway o de un solo salto, asegúrese de que la directiva de HDX Insight AppFlow esté enlazada al servidor virtual VPN, por donde fluye el tráfico HDX/ICA.
- Para el modo transparente o el modo de usuario LAN, asegúrese de que los puertos ICA 1494 y 2598 están configurados.
- Compruebe que el parámetro `appflowlog` en NetScaler Gateway o el servidor virtual VPN esté habilitado para Access Gateway o implementación de doble salto. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.
- Compruebe que “Conexión encadenamiento”está activado en NetScaler ADC de doble salto. Para obtener más información, consulte Configuración de dispositivos NetScaler Gateway para exportar datos.
- Después de la conmutación por error de HA si se analizan los detalles de HDX Insight, compruebe que el parámetro ICA “enableSRonHAFailover”está habilitado. Para obtener más información, consulte Fiabilidad de sesión en el par de alta disponibilidad de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Lista de comprobación de conectividad entre NetScaler ADC y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler ADC y AppFlow Collector.
- Compruebe los resultados de las directivas de HDX Insight AppFlow.

  Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva AppFlow.

  También puede ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.
- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

### Generación de registros para el tráfico HDX/ICA en la lista de comprobación de NetScaler ADC

Ejecute el comando `tail -f /var/log/ns.log | grep -i "default ICA Message"` para validar el registro. En función de los registros que se generan, puede utilizar esta información para solucionar problemas.

- Registro: Se **ha omitido el análisis de la conexión ICA; HDX Insight no es compatible con este host**

  **Causa**: versiones de Citrix Virtual Apps and Desktops no compatibles

  **Solución alternativa**: actualice los servidores Citrix Virtual Apps and Desktops a una versión compatible.
- Registro: **Tipo de cliente recibido 0x53, NO compatible**

  **Causa**: Versión no compatible de Citrix Workspace

  **Solución**: Actualice Citrix Workspace a una versión compatible. Para obtener más información, consulte la aplicación Citrix Workspace.
- Log: **Error de Expand Packet: Omitir todo el procesamiento hdx para este flujo**

  **Causa**: problema al descomprimir el tráfico ICA

  **Solución**: no hay informes disponibles para esta sesión de ICA hasta que se establezca una nueva sesión.
- Registro: **Transición no válida: NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT"**

  **Causa**: problema al analizar el protocolo de enlace ICA

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Solución**: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **Falta EUEM ICA RTT**

  **Causa**: No se pueden analizar los datos del canal de End-User Experience Monitoring

  **Solución**: asegúrese de que el servicio de supervisión de la experiencia del usuario final esté iniciado en los servidores Citrix Virtual Apps and Desktops. Asegúrese de usar las versiones compatibles de la aplicación Citrix Workspace.

- Registro: **encabezado de canal no válido**

  **Causa**: no se puede identificar el encabezado del canal

  **Solución**: No hay informes disponibles para esta sesión de ICA en particular hasta que se establezca una nueva sesión.

- Registro: **omitir código**

  Si ves alguno de los siguientes valores para el código de omisión, se omiten los detalles de Insight.

  > El código de omisión 0 indica que el registro se ha exportado correctamente desde NetScaler ADC.

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 100 | NS_ICA_ERR_NULL_FRAG | Error en el manejo de fragmentos ICA, probablemente debido a condiciones de memoria |
| 101 | NS_ICA_ERR_INVALID_HS_CMD | Se recibió un comando de enlace no válido |
| 102 | NS_ICA_ERR_REDUC_PARAM_CNT | Parámetro no válido especificado para la inicialización del expansor V3 |
| 103 | NS_ICA_ERR_REDUC_INIT | No se puede inicializar correctamente el expansor V3 |
| 104 | NS_ICA_ERR_REDUC_PARAM_BYTES | Bytes insuficientes para asignar un codificador a un canal |
| 105 | NS_ICA_ERR_INVALID_CHANNEL | Número de canal ICA no válido |
| 106 | NS_ICA_ERR_INVALID_DECODER | Decodificador no válido especificado para un canal |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 107 | NS_ICA_ERR_INVALID_TW_PARAM | Recuento de parámetros no válido especificado en el canal Thinwire |
| 108 | NS_ICA_ERR_INVALID_TW_DECODER | Decodificador no válido para el canal Thinwire |
| 109 | NS_ICA_ERR_REDUC_NO_DECODER | No hay decodificador definido para el canal |
| 110 | NS_ICA_ERR_REDUC_V3_EXPANDER | No se pudieron expandir los datos del canal |
| 111 | NS_ICA_ERR_REDUC_BYTES_V3_COR | Error de expansión: los bytes consumieron más de los bytes disponibles |
| 112 | NS_ICA_ERR_REDUC_BYTES_OOR | Error: desbordamiento de datos sin comprimir |
| 113 | NS_ICA_ERR_REDUC_INVALID_CMD | Comando Expander no definido |
| 114 | NS_ICA_ERR_CGP_FILL_HOLE | Error al gestionar tramas CGP divididas |
| 115 | NS_ICA_ERR_MEM_NSB_ALLOC | Error de asignación de NSB debido a condiciones de memoria baja |
| 116 | NS_ICA_ERR_MEM_REDUC_CTX_ALLOC | Error de asignación de memoria para el contexto del expansor |
| 117 | NS_ICA_ERR_ICA_OLD_SERVER | Servidor antiguo, bloques de capacidad no admitidos |
| 118 | NS_ICA_ERR_PIR_MANY_FRAG | La solicitud Packet Init está fragmentada, no se puede procesar |
| 119 | NS_ICA_ERR_INIT_ICA_CAPS | Error de inicialización de la capacidad ICA |
| 120 | NS_ICA_ERR_NO_MSI_SUPPORT | El host no admite la función MSI. Indica para la versión de XenApp inferior a 6.5 o para las versiones de XenDesktop inferiores a 5.0 |
| 121 | NS_ICA_ERR_CGP_INVALID_CMD | Se encontró un comando CGP no válido |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 122 | NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES | Bytes insuficientes en el canal |
| 123 | NS_ICA_ERR_CHANNEL_DATA | Datos incorrectos en el canal EUEM, CONTROL o SEAMLESS |
| 124 | NS_ICA_ERR_INVALID_PURE_CMD | Se recibió un comando no válido al procesar datos de canal ICA puros |
| 125 | NS_ICA_ERR_INVALID_PURE_LENG | Se encontró una longitud no válida al procesar datos de canal ICA puros |
| 126 | NS_ICA_ERR_INVALID_PURE_LEN | Se encontró una longitud no válida al procesar los datos del canal ICA PURO |
| 127 | NS_ICA_ERR_INVALID_CLNT_DATA | Longitud de datos no válida recibida del cliente |
| 128 | NS_ICA_ERR_MSI_GUID_SZ | Error en el tamaño del GUID MSI |
| 129 | NS_ICA_ERR_INVALID_CHANNEL_HEADER | Encabezado de canal no válido |
| 130 | NS_ICA_ERR_CGP_PARSE_RECONNECT | Error en la recuperación de la sesión reconectada |
| 131 | NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT | Error al inhabilitar SR |
| 132 | NS_ICA_ERR_REDUC_NOT_V3 | Versión ICA Reducer no compatible |
| 133 | NS_ICA_ERR_HS_COMPRESSION_DISABLED | Compresión desactivada, no respetada por el host |
| 134 | NS_ICA_ERR_IDENT_PROTO | No se puede identificar el protocolo ICA o CGP, visto con receptores incorrectos |
| 135 | NS_ICA_ERR_INVALID_SIGNATURE | Firma ICA o cadena mágica incorrectas |
| 136 | NS_ICA_ERR_PARSE_RAW | Error al analizar el paquete de enlace ICA |
| 137 | NS_ICA_ERR_INCOMPLETE_PKT | Paquete incompleto recibido en el protocolo de enlace |
| 138 | NS_ICA_ERR_ICAFRAME_TOO_LARGE | La trama ICA es demasiado grande, supera los 1460 bytes |
| 139 | NS_ICA_ERR_FORWARD | Error al reenviar los datos ICA |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 140 | NS_ICA_ERR_MAX_HOLES | No se puede procesar el comando CGP porque se divide más allá del límite admitido |
| 141 | NS_ICA_ERR_ASSEMBLE_FRAME | No se puede volver a montar el marco ICA correctamente |
| 142 | NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION | Omitir el análisis ICA para este receptor (cliente), ya que no está en la lista de permitidos |
| 143 | NS_ICA_ERR_LOOKUP_RECONNECT_ID | No se puede detectar el estado de análisis de la cookie de reconexión del cliente |
| 144 | NS_ICA_ERR_SYNCUP_RECONNECT_ID | Se detectó una longitud de cookie de reconexión no válida después de la |
| 145 | NS_ICA_ERR_INVALID_RECONNECT_ID | El cliente reconecta la cookie omitió la restricción necesaria |
| 146 | NS_ICA_ERR_INVALID_CLIENT_VERSION | Cadena de versión de receptor no válida recibida del cliente |
| 147 | NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID | Producto no válido recibido del cliente |
| 148 | NS_ICA_ERR_V3_HDR_CORRUPT_LEN | Longitud de canal no válida tras la expansión |
| 149 | NS_ICA_ERR_SPECIAL_THINWIRE | Error de descompresión |
| 150 | NS_ICA_ERR_SEAMLESS_INSUFFBYTE | Se encontraron bytes insuficientes para un comando transparente |
| 151 | NS_ICA_ERR_EUEM_INSUFFBYTE | Se encontraron bytes insuficientes para el comando EUEM |
| 152 | NS_ICA_ERR_SEAMLESS_INVALID_EVENT | Evento no válido para el análisis continuo de canales |
| 153 | NS_ICA_ERR_CTRL_INVALID_EVENT | Evento no válido para el análisis del canal CTRL |
| 154 | NS_ICA_ERR_EUEM_INVALID_EVENT | Evento no válido para el análisis del canal de EUEM |
| 155 | NS_ICA_ERR_USB_INVALID_EVENT | Evento no válido para el análisis de canales USB |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 156 | NS_ICA_ERR_PURE_INVALID_EVENT | Evento no válido para el análisis de canal puro |
| 157 | NS_ICA_ERR_VCP_INVALID_EVENT | Evento no válido para el análisis de canales virtuales |
| 158 | NS_ICA_ERR_ICAP_INVALID_EVENT | Evento no válido para el análisis de datos ICA |
| 159 | NS_ICA_ERR_CGPP_INVALID_EVENT | Evento no válido para el análisis de datos CGP |
| 160 | NS_ICA_ERR_BASICCRYPT_INVALIDSTATE | Estado no válido para un comando crypt en el cifrado básico |
| 161 | NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD | Comando crypt no válido en el cifrado básico |
| 162 | NS_ICA_ERR_ADVCRYPT_INVALIDSTATE | Estado no válido para un comando crypt en el cifrado RC5 |
| 163 | NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD | Comando crypt no válido en el cifrado RC5 |
| 164 | NS_ICA_ERR_ADVCRYPT_ENC | Error en el cifrado/descifrado RC5 |
| 165 | NS_ICA_ERR_ADVCRYPT_DEC | Error en el cifrado/descifrado RC5 |
| 166 | NS_ICA_ERR_SERVER_NOT_REDUCER_V3 | El VA no admite la versión 3 de Reducer |
| 167 | NS_ICA_ERR_CLIENT_NOT_REDUCER_V3 | El receptor no es compatible con Reducer Version 3 |
| 168 | NS_ICA_ERR_ICAP_INSUFFBYTE | Número inesperado de bytes en el protocolo de enlace ICA |
| 169 | NS_ICA_ERR_HIGHER_RECONSEQ | Mayor número de secuencia de reanudación de CGP de reconexiones de postes del par |
| 170 | NS_ICA_ERR_DESCSRINFO_ABSENT | No se puede restaurar el estado de análisis de ICA después de la reconexión |
| 171 | NS_ICA_ERR_NSAP_PARSING | Error al analizar los datos del canal Insight |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Omitir código | Mensaje de error | Causa del error |
|---|---|---|
| 172 | NS_ICA_ERR_NSAP_APP | Error al analizar los detalles de la aplicación de los datos del canal Insight |
| 173 | NS_ICA_ERR_NSAP_ACR | Error al analizar los detalles de ACR de los datos del canal Insight |
| 174 | NS_ICA_ERR_NSAP_SESSION_END | Error al analizar los detalles de finalización de la sesión de los datos del canal Insight |
| 175 | NS_ICA_ERR_NON_NSAP_SN | Se ha omitido el análisis de ICA en el nodo de servicio debido a la ausencia de soporte del canal Insight |
| 176 | NS_ICA_ERR_NON_NSAP_CLIENT | El cliente no admite NSAP |
| 177 | NS_ICA_ERR_NON_NSAP_SERVER | El VDA no admite NSAP |
| 178 | NS_ICA_ERR_NSAP_NEG_FAIL | Error durante la negociación de datos de NSAP |
| 179 | NS_ICA_ERR_SN_RECONNECT_TKT_FETCH | Error al recuperar el servicio reconecta el tíquet en el nodo de servicio |
| 180 | NS_ICA_ERR_SN_HIGHER_RECONSEQ | Error al recibir un número de secuencia de reconexión más alto en el nodo de servicio |
| 181 | NS_ICA_ERR_DISABLE_HDXINSIGHT_NON_NSAP | Error al inhabilitar HDX Insight para conexiones que no son NSAP |

**Registros de ejemplo:**

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT
 ns-223 0-PPE-2 : default ICA Message 1234 0 : "Session setup data
 send: Session GUID [57af35043e624abab409f5e6af7fd22c], Client IP/
Port [10.105.232.40/52314], Server IP/Port [10.106.40.215/2598], MSI
 Client Cookie [Non-MSI], Session setup time [01/09/2020:22:56:49
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [WIN2K12-215], Ctx Flags [0
x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]"
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41
GMT ns-223 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow
: Session GUID [4e3a91175ebcbe686baf175eec7e0200], Client IP/Port
 [10.105.232.40/60059], Server IP/Port [10.106.40.219/2598], MSI
Client Cookie [Non-MSI], Session setup time [01/09/2020:22:55:39
GMT], Client Type [0x0052], Receiver Version [19.12.0.23], User [
user1], Client [10.105.232.40], Server [10.106.40.219], Ctx Flags [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

### Contadores de errores

Se capturan varios contadores analizando ICA. En la siguiente tabla se enumeran los distintos contadores para el análisis ICA.
Ejecute el comando `nsconmsg –g hdx –d statswt0`para ver los detalles del contador.

| Nombre del contador HDX | Propósito | Categoría (Estadísticas/error/diagnóstico) |
|---|---|---|
| hdx_tot_ica_conn | Indica el número total de conexiones ICA puras detectadas por NS. Se incrementa cada vez que se detecta una conexión ICA basada en la firma ICA en una PCB cliente. | Estadísticas |
| hdx_tot_cgp_conn | Indica el número total de conexiones CGP detectadas por NS (Session Reliability ON). Se incrementa cada vez que se detecta una conexión CGP basada en la firma CGP en una PCB cliente. | Estadísticas |
| hdx_dbg_tot_udt_conn | Indica el número total de conexiones UDP ICA detectadas por NS | Estadísticas |
| hdx_dbg_tot_nsap_conn | Indica el número total de conexiones compatibles con NSAP detectadas por NS | Estadísticas |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre del contador HDX | Propósito | Categoría (Estadísticas/error/diagnóstico) |
|---|---|---|
| hdx_tot_skip_conn | Indica cuántas conexiones ICA omitió el analizador debido a una firma ICA o CGP no válida. | Estadísticas |
| hdx_dbg_active_conn | Total de conexiones EDT/CGP/ICA activas en ese instante. | Estadísticas |
| hdx_dbg_active_nsap_conn | Número total de conexiones EDT/CGP/ICA NSAP activas en ese instante. | Estadísticas |
| hdx_dbg_skip_appflow_disabled | Número total de instancias en las que AppFlow se desconectó de una sesión debido a la desactivación de AppFlow | Estados/Diagnósticos |
| hdx_dbg_transparent_user | Número total de accesos de usuarios transparentes | Estados/Diagnósticos |
| hdx_dbg_ag_user | Número total de accesos de usuarios de Access Gateway | Estados/Diagnósticos |
| hdx_dbg_lan_user | Número total de accesos en modo de usuario de LAN | Estados/Diagnósticos |
| hdx_basic_enc | Indica el número de conexiones ICA que utilizan cifrado básico | Estados/Diagnósticos |
| hdx_advanced_enc | Indica el número de conexiones ICA que utilizan un cifrado avanzado basado en RC5 | Estados/Diagnósticos |
| dx_dbg_wanscaler_on_clientside | Número total de conexiones CGP/ICA que tienen Citrix SD-WAN en el lado del cliente | Estados/Diagnósticos |
| hdx_dbg_wanscaler_on_serverside | Número total de conexiones CGP/ICA que tienen el lado del servidor de Citrix SD-WAN | Estados/Diagnósticos |
| hdx_dbg_reconnected_session | Número total de solicitudes de reconexión del cliente sin ningún error de NetScaler ADC | Estados/Diagnósticos |
| hdx_dbg_host_rejected_ns_reconnect | Número total de hosts rechazados reconecta solicitudes por cliente | Estados/Diagnósticos |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre del contador HDX | Propósito | Categoría (Estadísticas/error/diagnóstico) |
|---|---|---|
| hdx_euem_available | Indica el número de conexiones que tienen disponible el canal de supervisión de la experiencia del usuario final. El canal de supervisión de la experiencia del usuario final es necesario para recopilar estadísticas como ICA RTT. | Estados/Diagnósticos |
| hdx_err_disabled_sr | La fiabilidad de la sesión se inhabilita mediante el `nsapimgr`mando.La sesión no funciona para esta sesión. | Error |
| hdx_err_skip_no_msi | Al servidor XA/XD le falta la capacidad MSI. Esto indica una versión de servidor anterior, HDX Insight omite esta conexión. | Error |
| hdx_err_skip_old_server | Versión de servidor antigua no compatible | Error |
| hdx_err_clnt_not_whitelist | El receptor del cliente no está en la lista de permitidos, HDX Insight omite esta conexión | Error |
| hdx_sm_ica_cam_channel_disabled | Número total de NS_ICA_CAM_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_usb_channel_disabled | Número total de NS_ICA_USB_CHANNEL inhabilitados mediante la directiva SmartAccess | Diagnóstico |
| hdx_sm_ica_clip_channel_disabled | Número total de NS_ICA_CLIP_CHANNEL inhabilitados mediante la directiva SmartAccess | Diagnóstico |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre del contador HDX | Propósito | Categoría (Estadísticas/error/diagnóstico) |
|---|---|---|
| hdx_sm_ica_ccm_channel_disabled | Número total de NS_ICA_CCM_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_cdm_channel_disabled | Número total de NS_ICA_CDM_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_com1_channel_disabled | Número total de NS_ICA_COM1_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_com2_channel_disabled | Número total de NS_ICA_COM2_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_cpm_channel_disabled | Número total de NS_ICA_CPM_CHANNEL inhabilitados mediante la directiva de SmartAccess | Diagnóstico |
| hdx_sm_ica_lpt1_channel_disabled | Número total de NS_ICA_LPT1_CHANNEL inhabilitados mediante la directiva SmartAccess | Diagnóstico |
| hdx_sm_ica_lpt2_channel_disabled | Número total de NS_ICA_LPT2_CHANNEL inhabilitados mediante la directiva SmartAccess | Diagnóstico |
| dx_dbg_sm_ica_msi_disabled | Número total de casos en los que MSI está inhabilitado mediante la directiva SmartAccess | Diagnóstico |
| hdx_sm_ica_file_channel_disabled | El número total de NS_ICA_FILE_CHANNEL está inhabilitado mediante la directiva SmartAccess | Diagnóstico |
| hdx_dbg_usb_accept_device | Número total de dispositivos USB aceptados | Diagnóstico |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Nombre del contador HDX | Propósito | Categoría (Estadísticas/error/diagnóstico) |
|---|---|---|
| hdx_dbg_usb_reject_device | Número total de dispositivos USB rechazados | Diagnóstico |
| hdx_dbg_usb_reset_endpoint | Número total de puntos finales USB restablecidos | Diagnóstico |
| hdx_dbg_usb_reset_device | Número total de dispositivos USB restablecidos | Diagnóstico |
| hdx_dbg_usb_stop_device | Número total de dispositivos USB detenidos | Diagnóstico |
| hdx_dbg_usb_stop_device_response | Número total de respuestas de dispositivos USB detenidos | Diagnóstico |
| hdx_dbg_usb_device_gone | Número total de dispositivos USB desaparecidos | Diagnóstico |
| hdx_dbg_usb_device_stopped | Número total de dispositivos USB detenidos | Diagnóstico |

### Validación de nstrace

Compruebe el protocolo CFLOW para ver todos los registros de AppFlow que salen de NetScaler ADC.

### Población de registros en la lista de comprobación de NetScaler ADM

- Ejecute el comando `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`y compruebe los registros para confirmar que NetScaler ADM está recibiendo registros de AppFlow.
- Confirme que la instancia de NetScaler ADC se haya agregado a NetScaler ADM.
- Validar que el servidor virtual de NetScaler Gateway/VPN tiene licencia en NetScaler ADM.
- Asegúrese de que la configuración de parámetros de salto múltiple esté habilitada para el doble salto.
- Asegúrese de que NetScaler Gateway esté autorizado para el segundo salto en la implementación de doble salto.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Antes de contactar al soporte técnico de Citrix

Para una resolución rápida, asegúrese de contar con la siguiente información antes de ponerse en contacto con el soporte técnico de Citrix:

- Detalles de la implementación y la topología de la red.
- Versiones de NetScaler ADC y NetScaler ADM.
- Versiones del servidor Citrix Virtual Apps and Desktops.
- Versiones de Receiver cliente
- Número de sesiones ICA activas cuando se produjo el problema.
- Paquete de soporte técnico capturado ejecutando el `show techsupport` comando en el símbolo del sistema de NetScaler ADC.
- Paquete de soporte técnico capturado para NetScaler ADM.
- Rastreos de paquetes capturados en todos los NetScaler ADC.
  Para iniciar un seguimiento de paquete, escriba,`start nstrace -size 0'`
  Para detener un seguimiento de paquete, escriba,`stop nstrace`
- Recopilar entradas en la tabla ARP del sistema ejecutando el comando `show arp`.

### Problemas conocidos

Consulte las notas de la versión de NetScaler ADC para conocer los problemas conocidos en HDX Insight.

## Gateway Insight

January 30, 2024

En una implementación de Citrix Gateway, la visibilidad de los detalles de acceso de un usuario es esencial para solucionar problemas de error de acceso. Como administrador de red, quiere saber cuándo un usuario no puede iniciar sesión en Citrix Gateway y quiere conocer la actividad del usuario y los motivos del error de inicio de sesión. Por lo general, esta información no está disponible a menos que el usuario envíe una solicitud de resolución.

Gateway Insight proporciona visibilidad de los errores encontrados por todos los usuarios, independientemente del modo de acceso, en el momento de iniciar sesión en Citrix Gateway. Puede ver una lista de todos los usuarios disponibles, el número de usuarios activos, el número de sesiones activas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

y los bytes y licencias utilizados por todos los usuarios en un momento dado. Puede ver los errores del análisis de puntos finales (EPA), la autenticación, el inicio de sesión único (SSO) y el inicio de aplicaciones de un usuario. También puede ver los detalles de las sesiones activas y finalizadas de un usuario.

Gateway Insight también proporciona visibilidad de los motivos del error de inicio de aplicaciones para aplicaciones virtuales. Esto mejora su capacidad para solucionar cualquier tipo de problemas de inicio de sesión o inicio de aplicaciones. Puede ver la cantidad de aplicaciones iniciadas, la cantidad de sesiones totales y activas, la cantidad de bytes totales y el ancho de banda consumido por las aplicaciones. Puede ver los detalles de los usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas a un dispositivo Citrix Gateway en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento de aplicaciones para una Gateway. También puede ver los detalles de todos los usuarios asociados a una Gateway y su actividad de inicio de sesión.

Todos los mensajes de registro se almacenan en la base de datos Citrix ADM, por lo que puede ver los detalles de los errores de cualquier período de tiempo. También puede ver un resumen de los errores de inicio de sesión y determinar en qué etapa del proceso de inicio de sesión se ha producido un error.

### Puntos que tener en cuenta

- Gateway Insight se admite en las siguientes implementaciones:
  - Access Gateway
  - Unified Gateway
- La versión y la compilación de Citrix ADM deben ser iguales o posteriores a las del dispositivo Citrix Gateway.
- Se puede ver una hora de informes de Gateway Insight para instancias de Citrix ADC con licencia Advanced. Una licencia Premium es imprescindible para ver los informes de Gateway Insight más allá de una hora.

### Limitaciones

- Citrix Gateway no admite Gateway Insight cuando el método de autenticación está configurado como autenticación basada en certificados.
- Para los informes de Gateway Insight, la información de ubicación geográfica no se proporciona desde el dispositivo Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Los inicios de sesión de usuario correctos, la latencia y los detalles de nivel de aplicación para aplicaciones y escritorios ICA virtuales solo están visibles en el panel Usuarios de HDX Insight.
- En el modo de doble salto, no está disponible la visibilidad de los errores en el dispositivo Citrix Gateway en la segunda DMZ.
- No se notifican problemas de acceso al escritorio de Protocolo de escritorio remoto (RDP).
- Gateway Insight es compatible con los siguientes tipos de autenticación. Si se utiliza otro tipo de autenticación distinto de estos, es posible que veas algunas discrepancias en Gateway Insight.
  - Locales
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - OTP nativo

## Habilitar Gateway Insight

Para habilitar Gateway Insight para su dispositivo Citrix Gateway, primero debe agregar el dispositivo Citrix Gateway a Citrix ADM. A continuación, debe habilitar AppFlow para el servidor virtual que representa la aplicación VPN. Para obtener información sobre cómo agregar dispositivos a Citrix ADM, consulte Agregar dispositivos.

> **Nota**
>
> Para ver los errores del análisis de punto final (EPA) en Citrix ADM, debe habilitar la autenticación, la autorización y el registro de nombres de usuario de auditoría de AppFlow en el dispositivo Citrix Gateway.

El siguiente procedimiento para habilitar la información de Gateway es aplicable si Citrix ADM es **13.0 Build 36.27**:

1. Vaya a **Redes** >**Instancias** y seleccione la instancia para la que quiere habilitar AppFlow.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. En la página **Configurar Insight**, en **Configurar Analytics**, seleccione **Citrix Gateway**.
4. Seleccione el servidor virtual y, a continuación, haga clic en **Habilitar AppFlow**.
5. En la pantalla **Habilitar AppFlow**, en la lista **Seleccionar expresión**, haga clic en true.
6. Junto a **Modo de transporte**, active la casilla de verificación **Logstream**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Puede elegir **IPFIX** o **Logstream** como modo de transporte.
>
> Para obtener más información sobre **IPFIX** y **Logstream**, consulte **Descripción general de Logstream**.

7. Haga clic en **Aceptar**.

**Para Citrix ADM versión 13.0 Build 41.x o posterior**

1. Vaya a **Redes** >**Instancias** y seleccione la instancia.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione el servidor virtual y haga clic en **Habilitar análisis**.
4. En **Opciones avanzadas**:
   a) Seleccione **Logstream**
   b) Seleccione **Citrix Gateway**.
5. Haga clic en **Aceptar**.

**Habilitar la autenticación, autorización y auditoría de AppFlow el registro de nombres de usuario en un dispositivo Citrix Gateway mediante la GUI**

1. Vaya a **Configuración > Sistema > AppFlow > Configuración** y, a continuación, haga clic en **Cambiar configuración de AppFlow**.
2. En la pantalla **Configurar ajustes de AppFlow**, seleccione Nombre de **usuario AAA**y, a continuación, haga clic en **Aceptar**

## Ver los informes de Gateway Insight

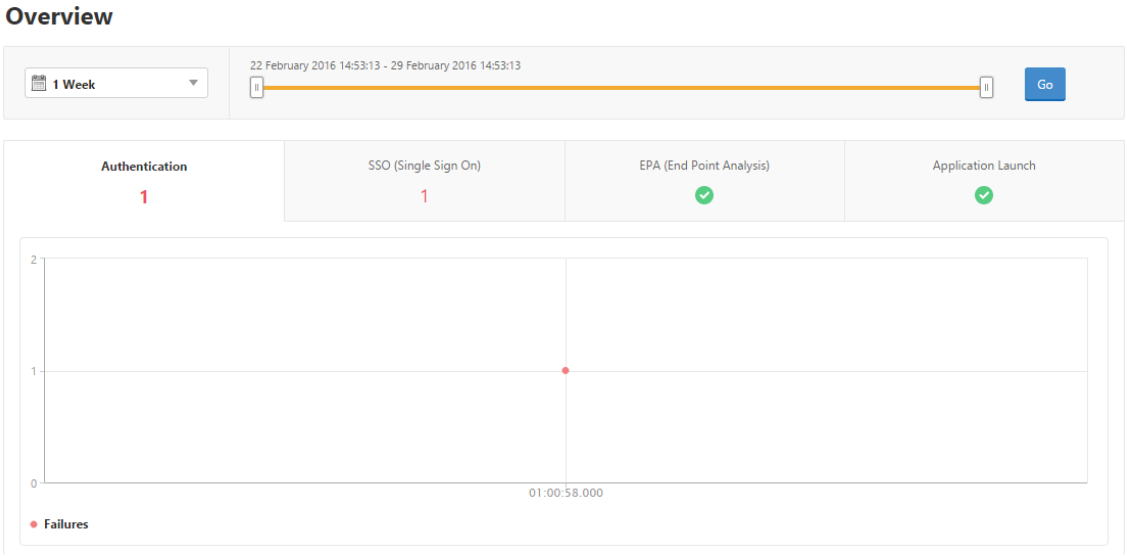
En Citrix ADM, puede ver los informes de todos los usuarios, aplicaciones y puertas de enlace asociados a los dispositivos Citrix Gateway, y puede ver los detalles de un usuario, aplicación o puerta de enlace en particular. En la sección **Descripción general**, puede ver los errores de EPA, SSO, Autenticación y Lanzamiento de aplicaciones. También puede ver un resumen de los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso de nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

**Para ver los errores de EPA, SSO, autenticación, autorización y lanzamiento de aplicaciones**

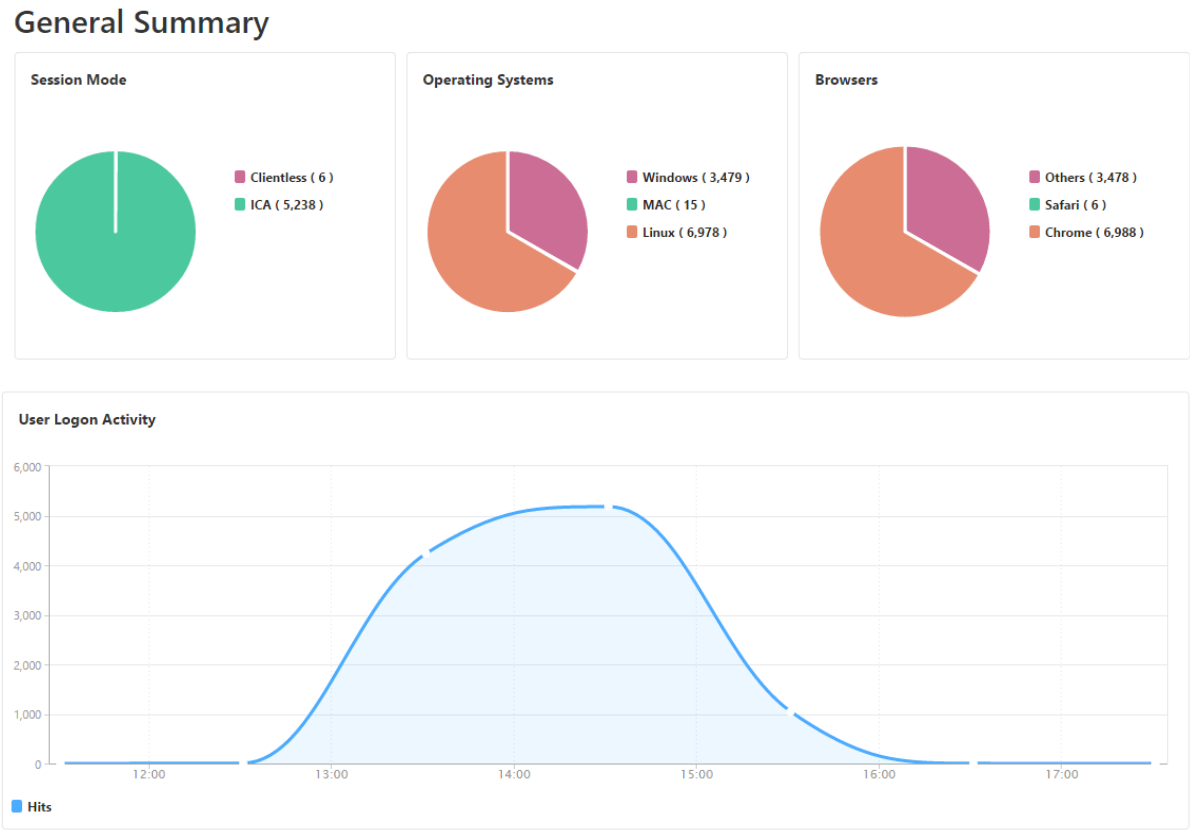
1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Haga clic en las fichas EPA (Análisis de punto final), Autenticación, Autorización, SSO (Inicio de sesión único) o Inicio de aplicación para mostrar los detalles del error.




**Para ver un resumen de los modos de sesión, los clientes y el número de usuarios**

En Citrix ADM, vaya a **Analytics > Gateway Insight**, desplácese hacia abajo para ver los informes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Visualización de informes de Gateway Insight para usuarios

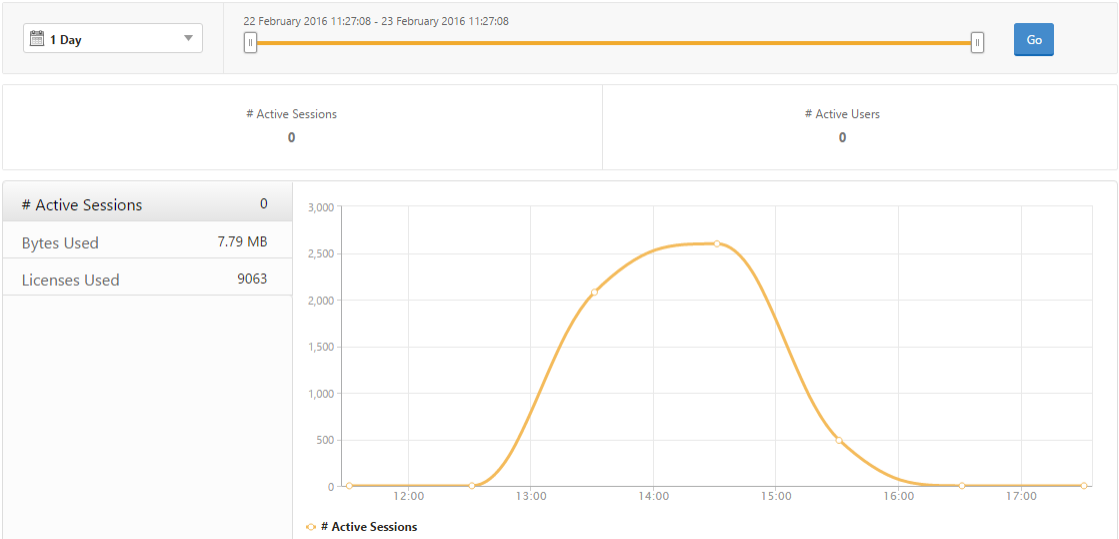
Puede ver los informes de:

- Todos los usuarios asociados con los dispositivos Citrix Gateway.
- La EPA, autenticación, inicio de sesión único y errores de inicio de aplicación para un usuario.
- Los detalles de las sesiones activas y terminadas de un usuario.
- Los tipos de modos de sesión como Túnel completo, VPN sin cliente y Proxy ICA.

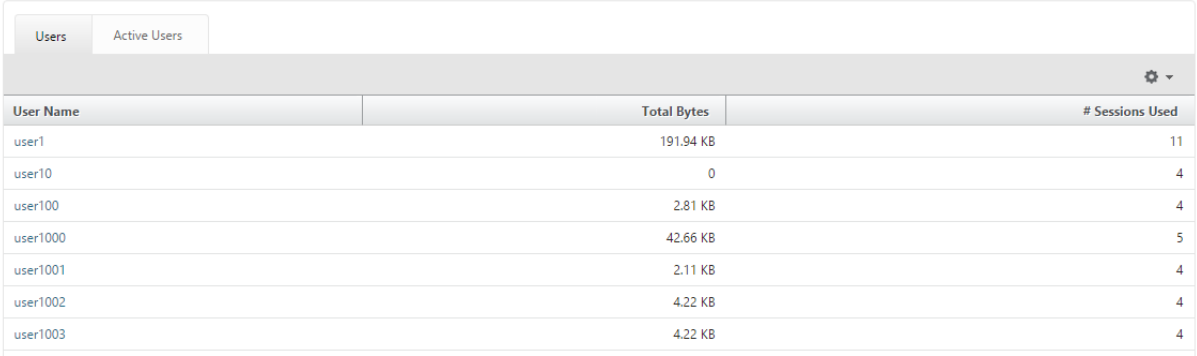
### Para ver los detalles del usuario

1. En Citrix ADM, vaya a **Analytics > Gateway Insight > Usuarios**.
2. Seleccione el período de tiempo para el que quiere ver los detalles del usuario. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. Haga clic en **Ir**.
3. Puede ver el número de usuarios activos, el número de sesiones activas, bytes y licencias utilizadas por todos los usuarios durante el período de tiempo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Desplácese hacia abajo para ver una lista de usuarios disponibles y usuarios activos.

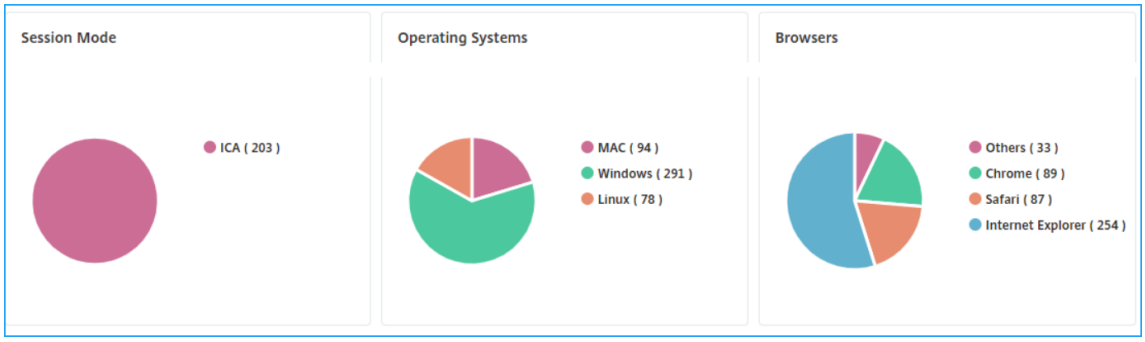


Users | Active Users

| User Name | Total Bytes | # Sessions Used |
|---|---|---|
| user1 | 191.94 KB | 11 |
| user10 | 0 | 4 |
| user100 | 2.81 KB | 4 |
| user1000 | 42.66 KB | 5 |
| user1001 | 2.11 KB | 4 |
| user1002 | 4.22 KB | 4 |
| user1003 | 4.22 KB | 4 |

En la ficha **Usuarios** o **Usuarios activos**, haga clic en un usuario para ver los siguientes detalles de usuario:

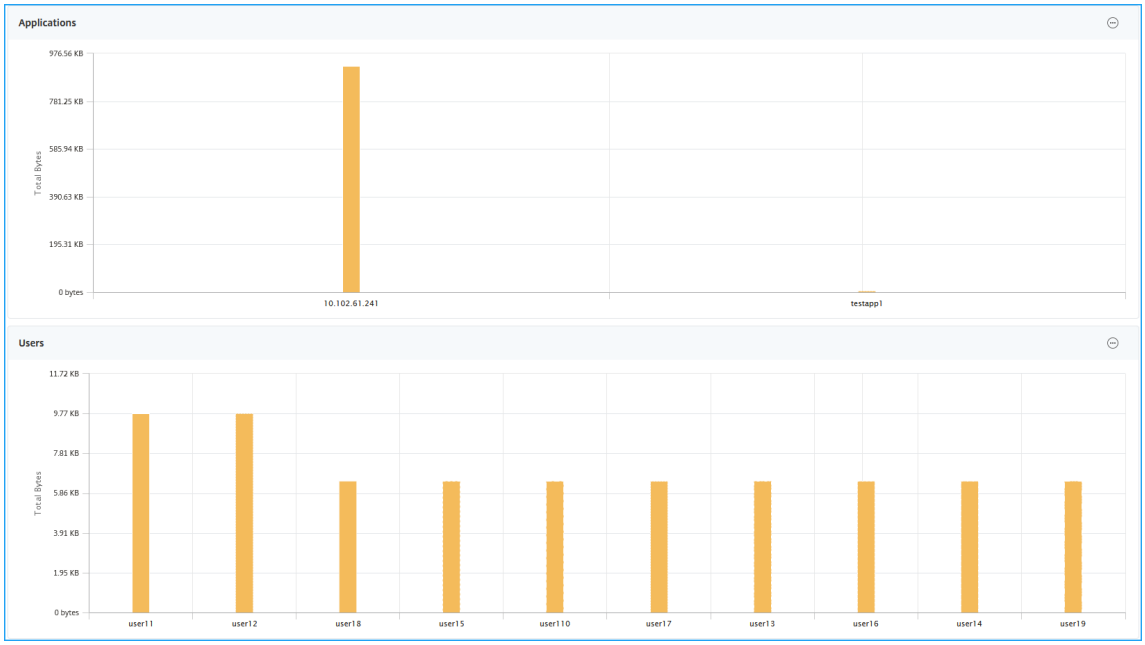
- **Detalles del usuario**: puede ver información sobre cada usuario asociado con los dispositivos de puerta de enlace de ADC. Vaya a **Analytics** > **Gateway Insight** > **Usuarios** y haga clic en un usuario para ver información sobre el usuario seleccionado, como Modo de sesión, Sistema operativo y Navegadores.



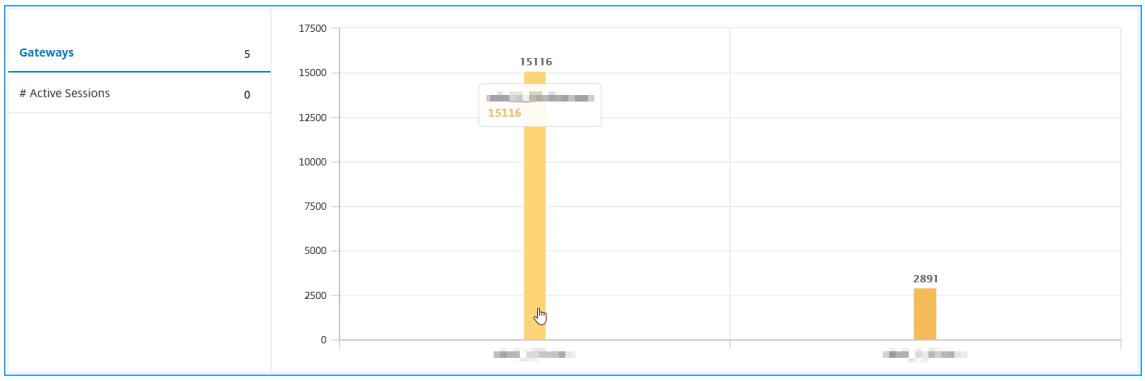

- **Usuarios y aplicaciones para la puerta de enlace seleccionada** : vaya a **Analytics** > **Gateway**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Insight** > **Gateway** y haga clic en un nombre de dominio de puerta de enlace para ver las 10 aplicaciones principales y los 10 usuarios principales asociados a la puerta de enlace seleccionada.

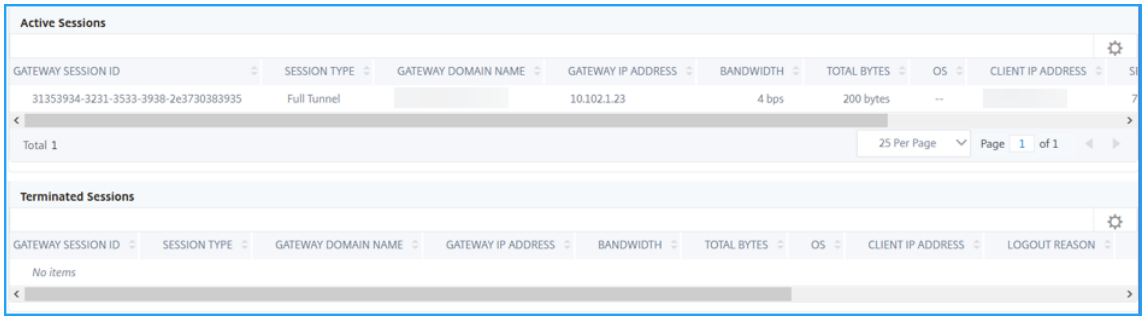



- **Ver más opción para aplicaciones y usuarios**: para más de 10 aplicaciones y usuarios, puede hacer clic en el icono más en Aplicaciones y Usuarios para ver todos los detalles de usuarios y aplicaciones asociados a la puerta de enlace seleccionada.
- **Ver detalles haciendo clic en el gráfico de barras**: al hacer clic en un gráfico de barras, puede ver los detalles relevantes. Por ejemplo, vaya a **Analytics > Gateway Insight > Gateway** y haga clic en el gráfico de barras de puerta de enlace para ver los detalles de la puerta de enlace.

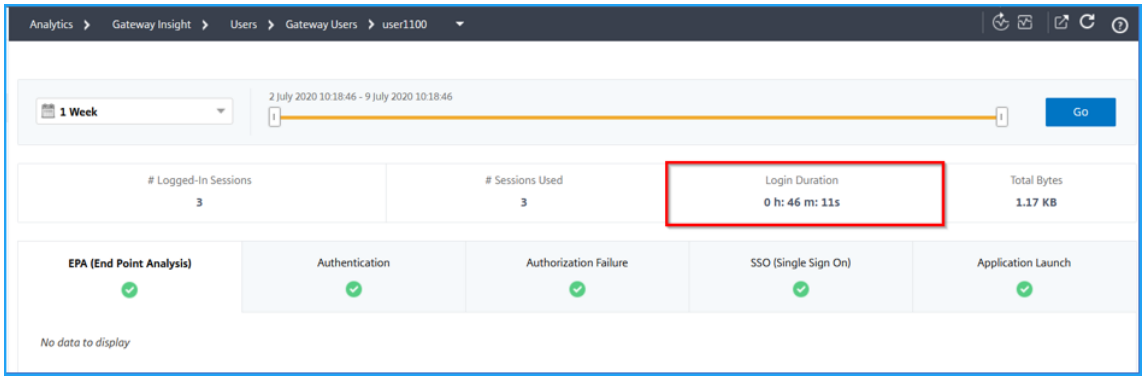



- El usuario **Sesiones Activas y SesionesTerminadas**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- El nombre del dominio de puerta de enlace y la dirección IP de la puerta de **enlace en Sesiones**
- Duración del inicio de sesión del usuario.




- El motivo de la sesión de cierre de sesión del usuario. Los motivos de cierre de sesión pueden ser:
  - Tiempo de espera excedido
  - Se cerró la sesión debido a un error interno
  - Se ha cerrado la sesión debido al tiempo de espera de la sesión inactiva
  - El usuario ha cerrado sesión
  - El administrador ha detenido la sesión

## Visualización de informes de Gateway Insight para aplicaciones

Puede ver el número de aplicaciones lanzadas, el número de sesiones totales y activas, el número total de bytes y el ancho de banda consumidos por las aplicaciones. Puede ver los detalles de los usuarios, las sesiones, el ancho de banda y los errores de inicio de una aplicación.

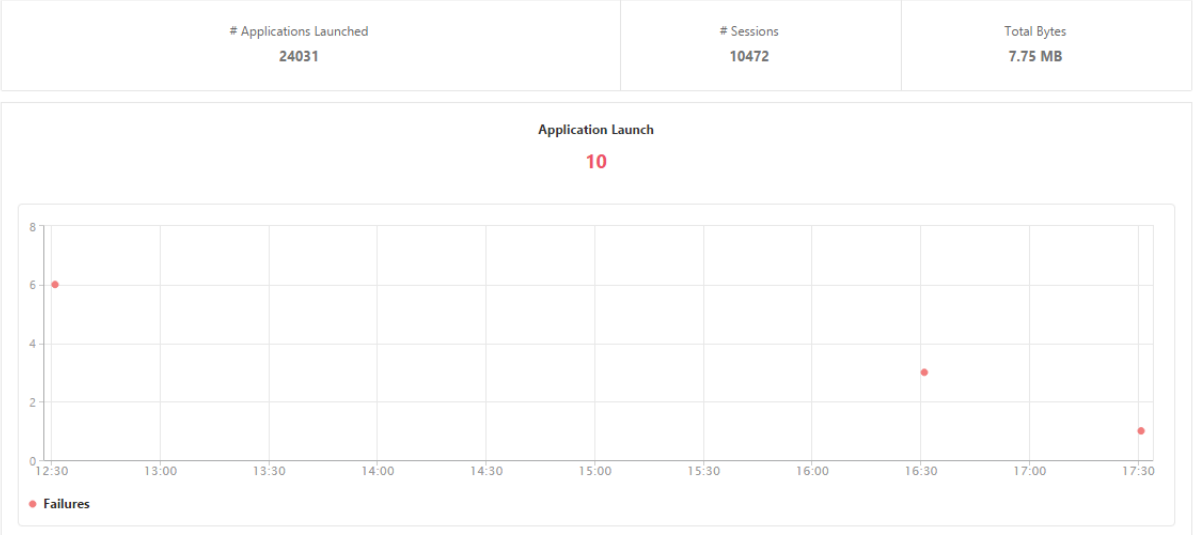
### Para ver los detalles de la aplicación

1. En NetScaler ADM, vaya a **Analytics > Gateway Insight > Aplicaciones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Seleccione el período de tiempo para el que quiere ver los detalles de la aplicación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de aplicaciones lanzadas, el número de sesiones totales y activas, el número total de bytes y el ancho de banda consumidos por las aplicaciones.




Desplácese hacia abajo para ver el número de sesiones, ancho de banda y bytes totales consumidos por ICA y otras aplicaciones.

ICA Applications | Other Applications

| Name | # Sessions | Bandwidth | Total Bytes |
|---|---|---|---|
| 10.102.61.249 | 3972 | 52 bps | 3.79 MB |
| c.go-mpulse.net | 2 | 0 bps | 1.53 KB |
| cdn.kendostatic.com | 1 | 0 bps | 805 |
| code.jquery.com | 1 | 0 bps | 1.51 KB |
| engtools.citrite.net | 2 | 0 bps | 160 |
| onebug.citrite.net | 2 | 1 bps | 86.21 KB |

En la ficha **Otras aplicaciones**, puede hacer clic en una aplicación de la columna **Nombre** para mostrar los detalles de esa aplicación.

### Visualización de informes de Gateway Insight para puertas de enlace

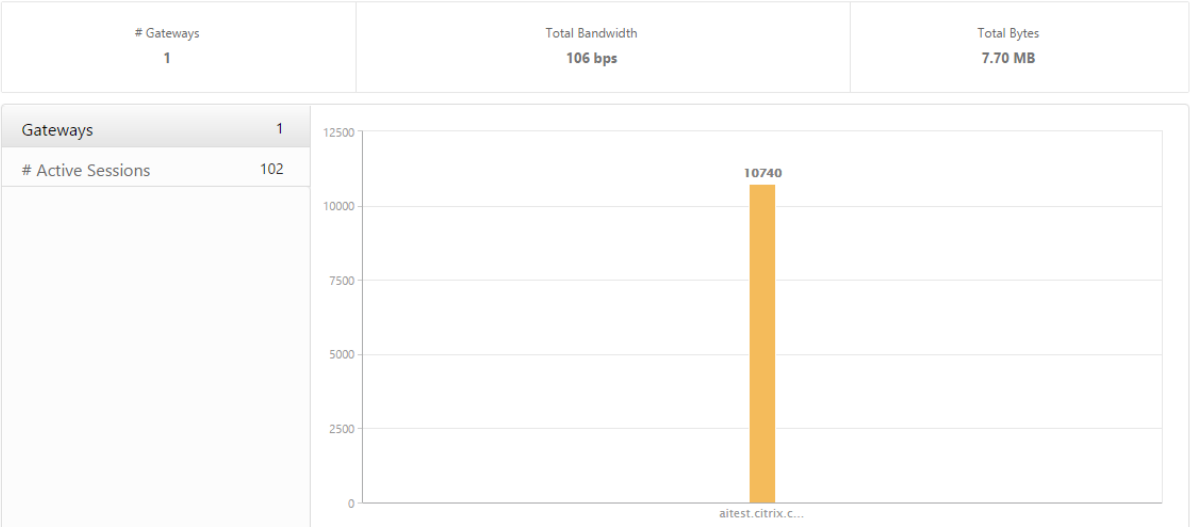
Puede ver la cantidad de puertas de enlace, la cantidad de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas a un dispositivo Citrix Gateway en un momento dado. Puede ver los errores de EPA, autenticación, inicio de sesión único y lanzamiento de aplicaciones para una Gateway. También puede ver los detalles de todos los usuarios asociados a una Gateway y su actividad de inicio de sesión.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

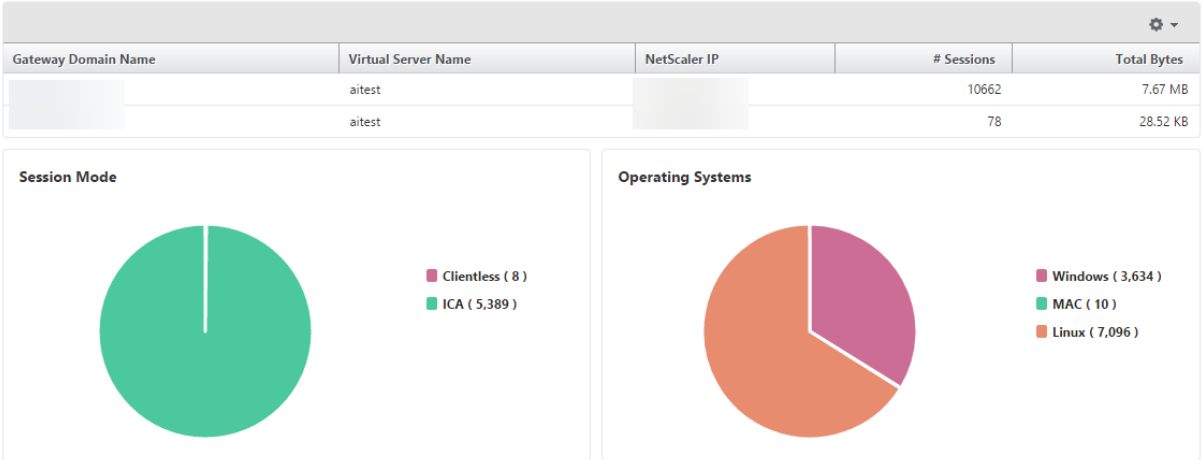
**Para ver los detalles de la Gateway**

1. En **Citrix ADM**, vaya a **Analytics > Gateway Insight > Gateway**.
2. Seleccione el período de tiempo para el que quiere ver los detalles de la Gateway. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

Ahora puede ver el número de puertas de enlace, el número de sesiones activas, el total de bytes y el ancho de banda que utilizan todas las puertas de enlace asociadas con un dispositivo Citrix Gateway en un momento dado.




Desplácese hacia abajo para ver los detalles de la Gateway, como el nombre de dominio de la puerta de enlace, el nombre del servidor virtual, la dirección IP de NetScaler, los modos de sesión y los bytes totales.




Puede hacer clic en una Gateway de la columna **Nombre de dominio de Gateway** para mostrar los errores de EPA, autenticación, inicio de sesión único e inicio de aplicaciones y otros detalles de una

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

puerta de enlace.

## Exportación de informes

Puede guardar los informes de Gateway Insight con todos los detalles que se muestran en la GUI en formato PDF, JPEG, PNG o CSV en su computadora local. También puede programar la exportación de los informes a direcciones de correo electrónico especificadas en varios intervalos.

> **Nota**
>
> - Los usuarios con acceso de solo lectura no pueden exportar informes.
> - Los informes de mapas geográficos se exportan solo si el Citrix ADM tiene conectividad a Internet.

**Para exportar un informe**

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Exportar ahora**, seleccione el formato necesario y, a continuación, haga clic en **Exportar**.

**Para programar la exportación:**

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Planificar exportación**, especifique los detalles y haga clic en **Planificar**.

**Para agregar un servidor de correo electrónico o una lista de distribución de correo electrónico:**

1. En la ficha **Configuración**, vaya a **Sistema** > **Notificaciones** > **Correo electrónico**.
2. En el panel derecho, seleccione **Servidor de correo electrónico**para agregar un servidor de correo electrónico o seleccione Lista de **distribución de correo electrónico para crear una lista** de distribución de correo electrónico.
3. Especifique los detalles y haga clic en **Crear**.

**Para exportar todo el panel de Gateway Insight:**

1. En la ficha **Panel** de control, en el panel derecho, haga clic en el botón de **exportación**.
2. En **Exportar ahora**, seleccione Formato **PDF** y, a continuación, haga clic en **Exportar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Casos de uso de Gateway Insight

Los siguientes casos de uso muestran cómo puede usar Gateway Insight para obtener visibilidad de los detalles de acceso, las aplicaciones y las puertas de enlace de los usuarios en los dispositivos Citrix Gateway.

### Un usuario no puede iniciar sesión en el dispositivo Citrix Gateway ni en los servidores web internos

Es un administrador de Citrix Gateway que supervisa los dispositivos Citrix Gateway a través de Citrix ADM y quiere ver por qué un usuario no puede iniciar sesión o en qué etapa del proceso de inicio de sesión se produjo el error.

Citrix ADM le permite ver los detalles del error de inicio de sesión del usuario en las siguientes etapas del proceso de inicio de sesión:

- Autenticación
- Análisis de puntos finales (EPA)
- Single Sign-On

En Citrix ADM, puede buscar un usuario en particular y, a continuación, ver todos los detalles de ese usuario.

**Para buscar un usuario:**

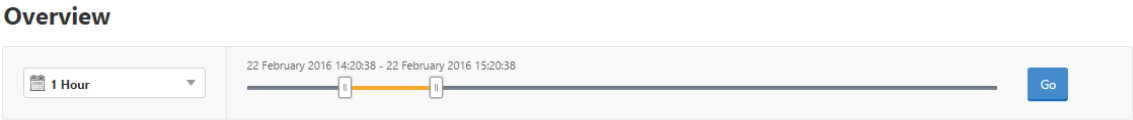
En Citrix ADM, vaya a **Analytics > Gateway Insight** y, en el cuadro de texto **Buscar usuarios**, especifique el usuario en el que quiere buscar.

### Fallos de autenticación

Puede ver errores de autenticación, como credenciales incorrectas o ninguna respuesta del servidor de autenticación. También puede ver el factor por el que falló la autenticación.

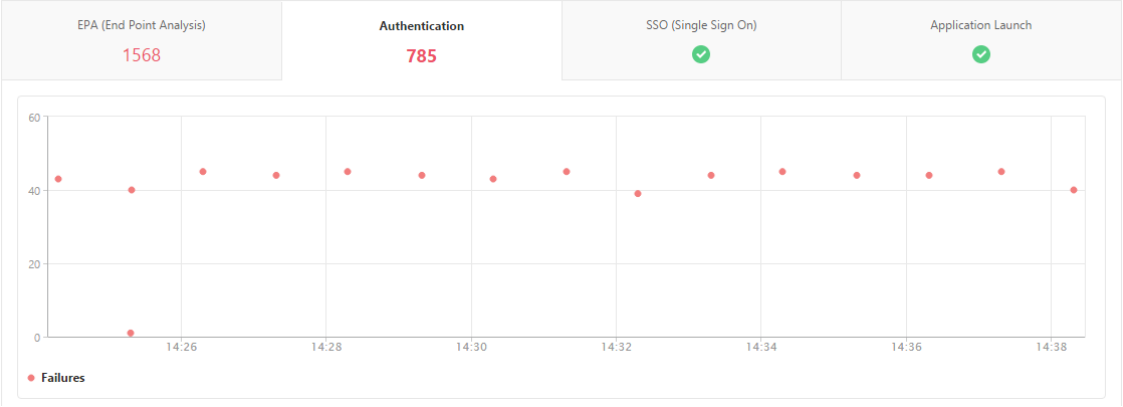
**Para ver los detalles del error de autenticación:**

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de autenticación. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Haga clic en la ficha **Autenticación**. Puede ver el número de errores de autenticación en un momento dado en el gráfico de **errores**.




Desplácese hacia abajo para ver los detalles de cada error de autenticación, como **Nombre de usuario, Dirección IP del cliente, Tiempo de error, Tipo de autenticación, Dirección IP del servidor de autenticación**, etc. en la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error de inicio de sesión y la columna **Estado** muestra el enésimo factor en el que se produjo el error.

| IP ADDRESS | VPN | CS VIRTUAL SERVER | ERROR TIME | ERROR DESCRIPTION | ERROR COUNT | STATE | AUTHEN |
|---|---|---|---|---|---|---|---|
| 183 | vpnvserver | | 15/03/2019, 06:30:04 | Server timed out | 1 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Server timed out | 4 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Server timed out | 3 | 2nd Factor | RADIUS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 1 | 1st Factor | TACACS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Server timed out | 1 | 2nd Factor | RADIUS |
| 111 | vpnvip | | 19/03/2019, 06:30:04 | Bad(format) password passed to nsaaad | 1 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 1 | 1st Factor | TACACS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 3 | 1st Factor | LDAP |
| 183 | vpnvserver | | 13/04/2019, 06:30:28 | Server timed out | 1 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Account is disabled | 1 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 1 | 1st Factor | Local |
| 183 | vpnvserver | | 12/04/2019, 06:30:13 | Server timed out | 1 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 1 | 1st Factor | TACACS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Bad(format) password passed to nsaaad | 5 | 1st Factor | LDAP |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 4 | 1st Factor | TACACS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Server timed out | 4 | 1st Factor | RADIUS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Invalid credentials passed | 1 | 1st Factor | TACACS |
| 100 | afsanity | | 04/04/2019, 06:30:23 | Server timed out | 22 | 1st Factor | RADIUS |
| 5.88 | _XD_10.217.205.88_443 | | 15/03/2019, 06:30:04 | Bad(format) password passed to nsaaad | 1 | 1st Factor | LDAP |

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de autenticación y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante el icono de configuración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

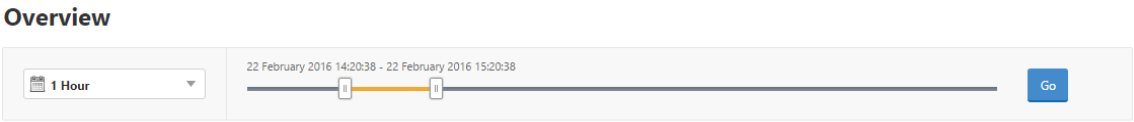
### Errores de EPA

Puede ver los errores de EPA en la etapa previa o posterior a la autenticación.

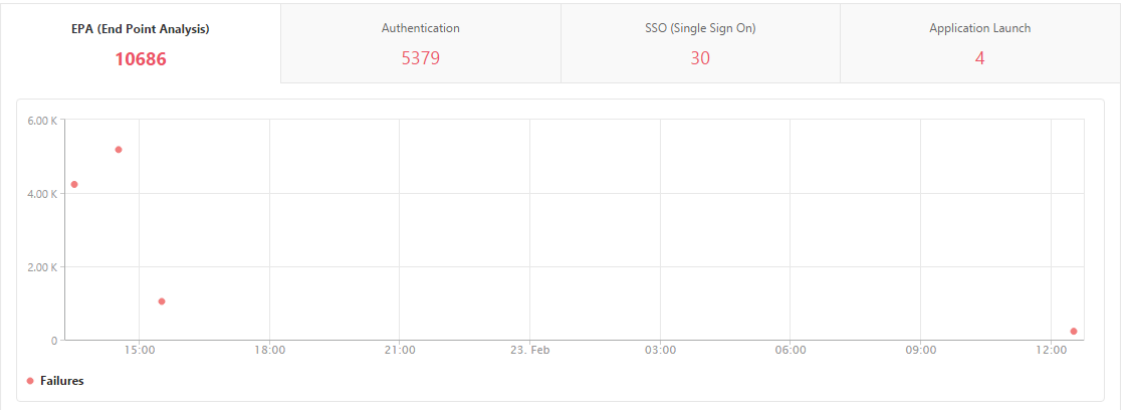
> **Importante:**
>
> - Los errores de EPA solo se registran cuando se configuran expresiones clásicas.
> - Los errores de la EPA no se notifican si la expresión avanzada se configura en la directiva de autenticación previa o posterior a la autenticación.
> - Los errores de EPA no se registran si EPA se configura como uno de los factores en un flujo de autenticación de nFactor.

**Para ver los detalles de fallo de EPA:**

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de EPA. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.




3. Haga clic en la ficha **EPA (Análisis de punto final)**. Puede ver el número de errores de EPA en un momento dado en el gráfico de **errores**.




Desplázate hacia abajo para ver los detalles de cada error de la EPA, como el nombre de **usuario, la dirección IP de NetScaler, la dirección IP de Gateway, la VPN, el tiempo de error, el nombre de la directiva, el nombre de dominio de Gateway** y más, de la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra el motivo del error EPA y la columna **Nombre de la directiva** muestra la directiva que dio lugar al error.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Username | NetScaler IP Address | Client IP Address | Gateway IP Address | VPN | Error Time | Error Description | Error Count | Policy Name | EPA Method | Gateway Domain Name |
|---|---|---|---|---|---|---|---|---|---|---|
| user1097 | 10.102.61.201 | 10.102.61.200 | 10.102.61.210 | aitest | 2/22/2016, 1:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user1098 | 10.102.61.201 | 10.102.61.200 | 10.102.61.210 | aitest | 2/22/2016, 1:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user1491 | 10.102.61.201 | 10.144.2.35 | 10.102.61.210 | aitest | 2/22/2016, 2:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user1633 | 10.102.61.201 | 10.144.2.35 | 10.102.61.210 | aitest | 2/22/2016, 3:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user17 | 10.102.61.201 | 10.102.61.200 | 10.102.61.210 | aitest | 2/22/2016, 1:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user1774 | 10.102.61.201 | 10.102.61.200 | 10.102.61.210 | aitest | 2/22/2016, 2:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |
| user197 | 10.102.61.201 | 10.144.2.35 | 10.102.61.210 | aitest | 2/22/2016, 1:30:54 PM | Post auth failed, no quar... | 1 | postauth_act | | aitest.citrix.com |

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de EPA y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

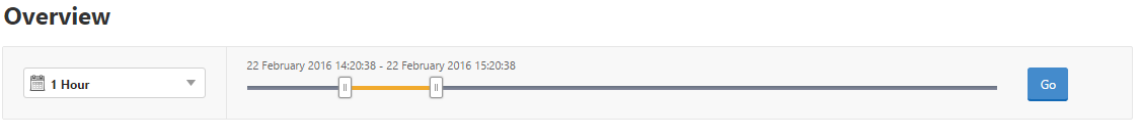
> **Nota**
>
> Citrix Gateway no informa de los errores de la EPA cuando la expresión “clientSecurity”se configura como una regla de directiva de sesión de VPN.

### Errores de SSO

Puede ver todos los errores de SSO en cualquier etapa de un usuario que accede a cualquier aplicación a través del dispositivo Citrix Gateway.

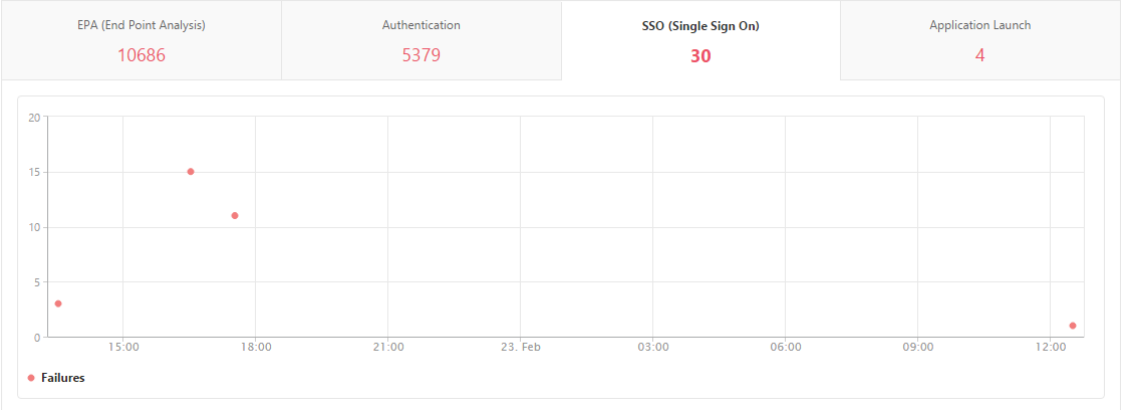
**Para ver los detalles del error de inicio de SSO:**

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección Descripción general, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.




3. Haga clic en la ficha **SSO (Inicio de sesión único)**. Puede ver el número de errores de SSO en cualquier momento dado en el gráfico de errores.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Desplácese hacia abajo para ver los detalles de cada error de SSO **, como Nombre de usuario, Dirección IP de NetScaler, Tiempo de error, Descripción del error, Nombre del recurso** y más desde la tabla de la misma ficha.

| Username | NetScaler IP Address | Client IP Address | Gateway IP Address | VPN | Error Time | Error Description | Error Count | SSO Method | Gateway Domain Name |
|---|---|---|---|---|---|---|---|---|---|
| user11 | 10.102.61.201 | 10.102.61.210 | 10.144.2.35 | aitest | 2/22/2016, 1:30:54 PM | Single Sign ON failed | 1 | AG Basic | aitest.citrix.com |
| user1 | 10.102.61.201 | 10.102.61.210 | 10.252.241.48 | aitest | 2/22/2016, 5:30:54 PM | Single Sign ON failed | 11 | NTLM | aitest.citrix.com |
| user5 | 10.102.61.201 | 10.102.61.210 | 10.252.241.48 | aitest | 2/23/2016, 12:30:54 PM | Single Sign ON failed | 1 | Basic | aitest.citrix.com |
| user31 | 10.102.61.201 | 10.102.61.210 | 10.102.61.200 | aitest | 2/22/2016, 1:30:54 PM | Single Sign ON failed | 1 | AG Basic | aitest.citrix.com |
| user23 | 10.102.61.201 | 10.102.61.210 | 10.102.61.200 | aitest | 2/22/2016, 1:30:54 PM | Single Sign ON failed | 1 | AG Basic | aitest.citrix.com |
| user1 | 10.102.61.201 | 10.102.61.210 | 10.252.241.48 | aitest | 2/22/2016, 4:30:54 PM | Single Sign ON failed | 15 | NTLM | aitest.citrix.com |

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de SSO y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

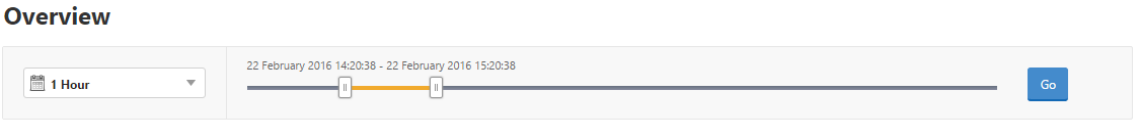
### Después de iniciar sesión correctamente en Citrix Gateway, un usuario no puede iniciar ninguna aplicación virtual

Si se produce un error en el inicio de la aplicación, puede obtener visibilidad de los motivos, como Secure Tíquet Authority (STA) o Citrix Virtual App Server, o un tíquet STA no válido. Puede ver la hora en que se produjo el error, los detalles del error y el recurso para el que falló la validación STA.

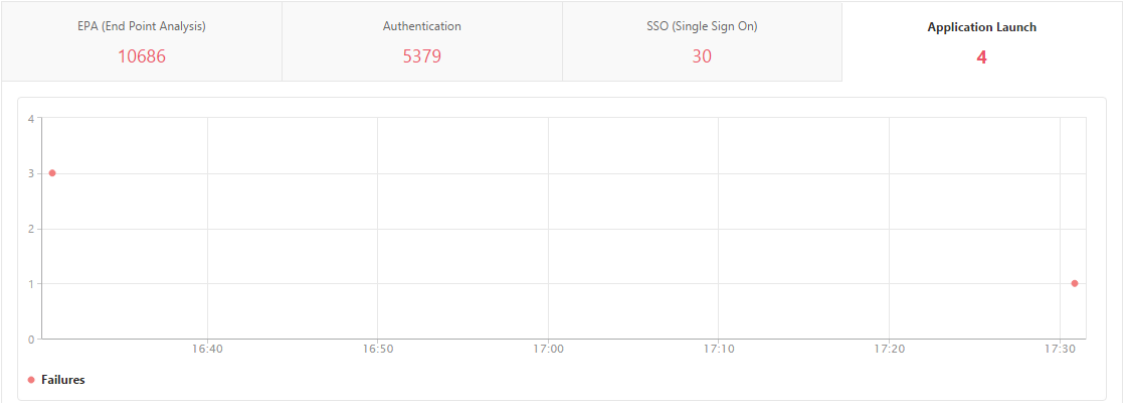
**Para ver los detalles del error de inicio de la aplicación:**

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, seleccione el período de tiempo para el que quiere ver los errores de SSO. Puede usar el control deslizante de tiempo para personalizar aún más el período de tiempo seleccionado. Haga clic en **Ir**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. Haga clic en la ficha **Inicio de la aplicación**. Puede ver el número de errores de inicio de la aplicación en un momento dado en el gráfico **Fallos**.




Desplácese hacia abajo para ver los detalles de cada error de inicio de la aplicación, como **NetScaler IP Address, Error Time, Error Description, Resource Name, Gateway Domain Name**, etc., desde la tabla de la misma ficha. La columna **Descripción del error** de la tabla muestra la dirección IP del servidor STA y la columna **Nombre del recurso** muestra los detalles del recurso para el que ha fallado la validación STA.

Puede hacer clic en un usuario en la columna **Nombre de usuario** para mostrar los errores de inicio de la aplicación y otros detalles de ese usuario. Puede personalizar la tabla para agregar o eliminar columnas mediante la flecha hacia abajo.

### Después de iniciar correctamente una nueva aplicación, un usuario quiere ver el total de bytes y ancho de banda consumidos por esa aplicación

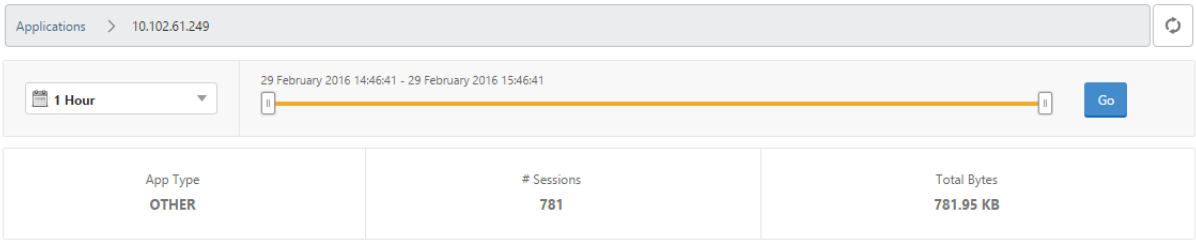
Después de haber iniciado correctamente una nueva aplicación, en Citrix ADM, puede ver el total de bytes y ancho de banda consumidos por esa aplicación.

**Para ver el total de bytes y ancho de banda consumidos por una aplicación:**

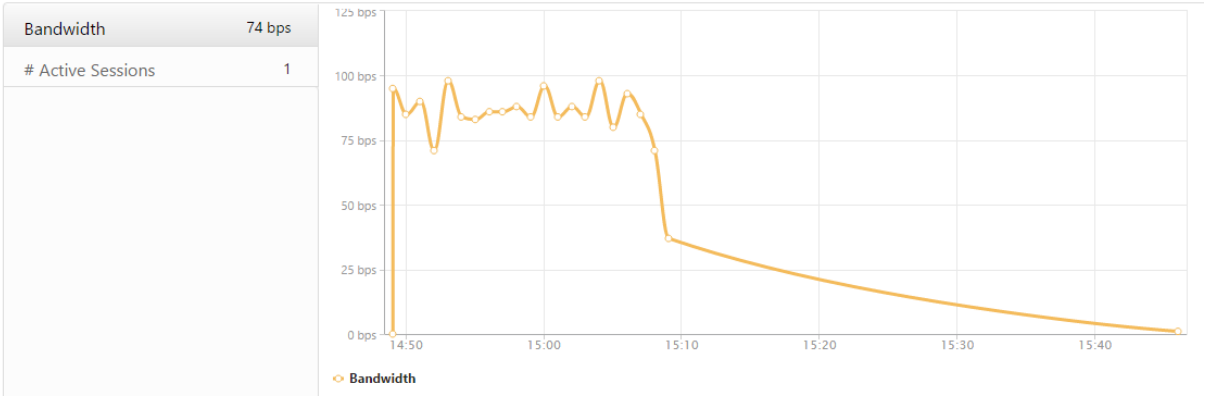
En Citrix ADM, vaya a **Analytics > Gateway Insight > Aplicaciones**, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, haga clic en la aplicación para la que quiere ver los detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Puede ver el número de sesiones y el número total de bytes consumidos por esa aplicación.




También puede ver el ancho de banda consumido por esa aplicación.




### Un usuario ha iniciado sesión correctamente en Citrix Gateway, pero no puede acceder a determinados recursos de red de la red interna

Con Gateway Insight, puede determinar si el usuario tiene acceso a los recursos de red o no. También puede ver el nombre de la directiva que dio lugar al error.

**Para ver el acceso de los usuarios para los recursos:**

1. En Citrix ADM, **vaya a Analytics > Gateway Insight > Aplicaciones**.
2. En la pantalla que aparece, desplácese hacia abajo y, en la ficha **Otras aplicaciones**, seleccione la aplicación en la que el usuario no pudo iniciar sesión.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ICA Applications | Other Applications

| Name | # Sessions | Bandwidth | Total Bytes |
|---|---|---|---|
| 10.102.61.249 | 2499 | 32 bps | 2.36 MB |
| c.go-mpulse.net | 2 | 0 bps | 1.53 KB |
| cdn.kendostatic.com | 1 | 0 bps | 805 |
| code.jquery.com | 1 | 0 bps | 1.51 KB |
| engtools.citrite.net | 2 | 0 bps | 160 |
| onebug.citrite.net | 2 | 1 bps | 86.21 KB |
| rock.citrite.net | 1 | 0 bps | 120 |

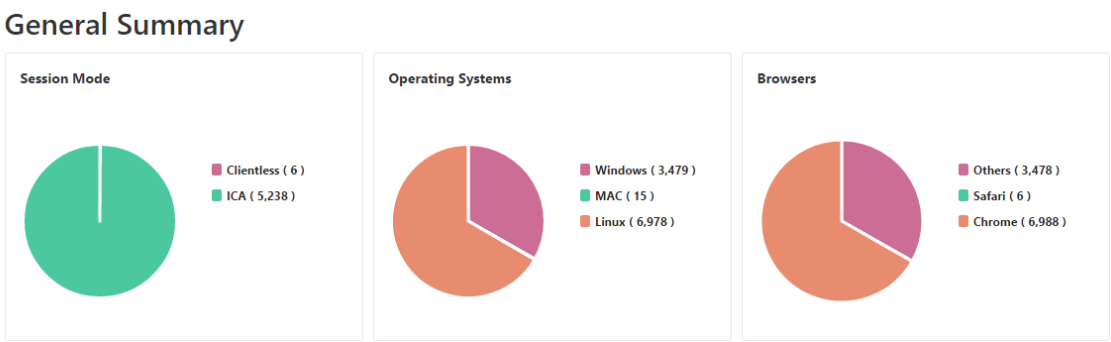
3. Desplácese hacia abajo y, en la tabla **Usuarios**, se muestran todos los usuarios que tienen acceso a esa aplicación.

**Es posible que diferentes usuarios usen distintas implementaciones de Citrix Gateway o que inicien sesión en Citrix Gateway a través de diferentes modos de acceso. El administrador debe poder ver detalles sobre los tipos de implementación y los modos de acceso**

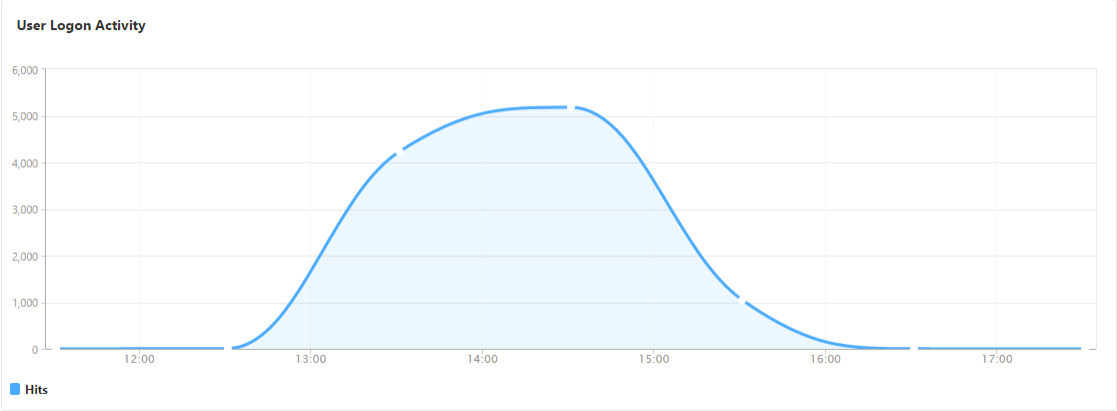
Con Gateway Insight, puede ver un resumen de los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora. También puede determinar si la implementación de un usuario es una puerta de enlace unificada o una implementación clásica de Citrix Gateway. Para implementaciones de Gateway unificada, puede ver el nombre y la dirección IP del servidor virtual de conmutación de contenido y el nombre del servidor virtual VPN.

**Para ver el resumen de los modos de sesión, el tipo de clientes y el número de usuarios que han iniciado sesión**:

1. En Citrix ADM, vaya a **Analytics > Gateway Insight**.
2. En la sección **Descripción general**, desplácese hacia abajo para ver los gráficos **Modo de sesión, Sistemas operativos, Exploradores** y **Actividad de inicio de sesión del usuario** que muestran los diferentes modos de sesión utilizados por los usuarios para iniciar sesión, los tipos de clientes y el número de usuarios que han iniciado sesión cada hora.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Solucionar problemas de Gateway Insight

January 30, 2024

Si la solución Gateway Insight no funciona como se esperaba, el problema podría estar relacionado con una de las siguientes opciones. Consulte las listas de comprobación de las secciones correspondientes para la solución de problemas.

- Configuración de Gateway Insight.
- Problema de conectividad entre NetScaler ADC y NetScaler ADM.
- Generación de registros en NetScaler ADC.
- Validaciones en NetScaler ADM.

### Lista de comprobación de configuración de Gateway Insight

- Asegúrese de que la función AppFlow está habilitada en el dispositivo NetScaler ADC. Para obtener más información, consulte Habilitar AppFlow.
- Compruebe la configuración de Gateway Insight en la configuración en ejecución de NetScaler ADC.

  Ejecute el comando `show running | grep -i <appflow_policy>` para comprobar la configuración de Gateway Insight. Asegúrese de que el tipo de enlace sea REQUEST. Por ejemplo:

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  El tipo de enlace OTHERTCP_REQUEST también es necesario para Gateway Insight.

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type
     OTHERTCP_REQUEST
  ```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Para la implementación de un solo salto, Access Gateway o Unified Gateway, asegúrese de que la directiva Gateway Insight AppFlow esté enlazada al servidor virtual VPN, donde fluye el tráfico VPN. Para obtener más información, consulte Habilitar la recopilación de datos de HDX Insight
- Para el doble salto, Gateway Insight debe configurarse en ambos saltos.
- Compruebe `appflowlog` el parámetro en el servidor virtual NetScaler Gateway/VPN. Para obtener más información, consulte Habilitación de AppFlow para servidores virtuales.

### Lista de comprobación de conectividad entre NetScaler ADC y NetScaler ADM

- Compruebe el estado del recopilador AppFlow en NetScaler ADC. Para obtener más información, consulte Cómo comprobar el estado de la conectividad entre NetScaler ADC y AppFlow Collector.
- Compruebe los aciertos de la directiva de Gateway Insight AppFlow.

  Ejecute el comando `show appflow policy <policy_name>` para comprobar los aciertos de la directiva AppFlow.

  También puede ir a **Sistema > AppFlow > Directivas** en la GUI para comprobar los aciertos de las directivas de AppFlow.
- Validar cualquier firewall que bloquee los puertos AppFlow 4739 o 5557.

### Generación de registros en la lista de comprobación de NetScaler ADC

- Ejecute el comando `nsconmsg -d stats -g ai_tot` y compruebe si hay incrementos de estadísticas en NetScaler ADC.
- Capture `nstrace logs` y compruebe si hay paquetes CFLOW para confirmar que NetScaler ADC exporta registros de AppFlow.

  > **Nota:**
  >
  > Los `nstrace logs` son necesarios solo para IPFIX. Para Logstream, los registros de nstrace no confirman si el dispositivo ADC exportó los registros AppFlow.

### Validación de registros en NetScaler ADM

- Ejecute el `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` comando para comprobar los registros para confirmar que NetScaler ADM está recibiendo registros de AppFlow.
- Asegúrese de que la instancia de NetScaler ADC se ha agregado a NetScaler ADM.
- Asegúrese de que el servidor virtual NetScaler Gateway/VPN tiene licencia en NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Validación de registros Logstream en NetScaler ADM

La validación de los datos Logstream recibidos por NetScaler ADM se puede realizar mediante los siguientes métodos:

- **Habilitar el registro de datos en NetScaler ADM**

  Una vez habilitado, los registros se pueden ver en el archivo /var/mps/log/mps_afdecoder.log

- **Habilitar el registro de bibliotecas ULFD**

  Ejecute el comando `/mps/decoder_enable_debug`

  Los registros se capturan en `/var/ulflog/libulfd.log`

  Puede inhabilitar el registro mediante el comando `/mps/decoder_disable_debug`

### Contadores de Gateway Insight

Los siguientes contadores de Gateway Insight están disponibles.

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_archivoinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_discordancia
- ai_tot_appflow_disabled
- ai_tot_appflow_pol_eval_in_gwinsight
- ai_tot_app_launch_success

### Registros de AppFlow en el registro de NetScaler ADC

A partir de la versión 13.0 compilación 71.x, puede comprobar los registros de NetScaler ADC para confirmar si se exportan los registros de AppFlow. El nivel de registro predeterminado de `syslogparams` captura todos los registros de errores e información. En caso de que no encuentre

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

una pista sobre los errores, habilite todos los niveles de registro, incluido DEBUG in, `syslogparams` para capturar incluso los registros de DEPURACIÓN.

### Registros de muestra

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> ... GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
<local0.info> ... GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
```

### Póngase en contacto con el soporte técnico de Citrix

Para una resolución rápida, asegúrese de contar con la siguiente información antes de ponerse en contacto con el soporte técnico de Citrix:

- Detalles de la implementación y la topología de la red.
- Versiones de NetScaler ADC y NetScaler ADM.
- Paquete de soporte técnico para NetScaler ADC y NetScaler ADM.
- `nstrace` durante el problema.

### Problemas conocidos

Consulte las notas de la versión de NetScaler ADC para obtener Insight sobre los problemas conocidos en Gate

## Security Insight

January 30, 2024

> Nota
>
> Si la compilación de NetScaler ADM es anterior a **13.0-79.x**, puede ver la información de seguridad navegando a **Analytics > Security > Security Insight**. Para la compilación **13.0-79.x o posterior**, puede ver los detalles de infracciones de WAF navegando a **Analytics > Seguridad > Infracciones de seguridad > Descripción general de la aplicación** y haciendo clic en **WAF** en **Desglose de aplicaciones por**.

Las aplicaciones web y de servicios web que están expuestas a Internet se han vuelto cada vez más vulnerables a los ataques. Para proteger las aplicaciones de ataques, necesita visibilidad sobre la naturaleza y el alcance de las amenazas pasadas, presentes e inminentes, datos procesables en tiempo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

real sobre ataques y recomendaciones sobre contramedidas. Security Insight proporciona una solución de panel único para ayudarle a evaluar el estado de seguridad de su aplicación y a tomar medidas correctivas para proteger sus aplicaciones.

> **Nota**
>
> Security Insight es compatible con Citrix Application Delivery Management (ADM) con dispositivos Citrix ADC que se ejecutan en la versión 11.0 Build 65.31 y versiones posteriores.

## Cómo funciona Security Insight

Security Insight es una solución intuitiva de análisis de seguridad basada en paneles que le proporciona una visibilidad completa del entorno de amenazas asociado con sus aplicaciones. La información sobre seguridad se incluye en Citrix ADM y genera informes periódicamente basados en las configuraciones de seguridad del sistema Application Firewall y Citrix ADC. Los informes incluyen la siguiente información para cada aplicación:

- **Índice de amenazas.** Un sistema de clasificación de un solo dígito que indica la gravedad de los ataques a la aplicación, independientemente de si la aplicación está protegida o no por un dispositivo Citrix ADC. Cuanto más críticos sean los ataques a una aplicación, mayor será el índice de amenazas para esa aplicación. Los valores oscilan entre 1 y 7.

  El índice de amenazas se basa en la información de ataque. La información relacionada con el ataque, como el tipo de infracción, la categoría del ataque, la ubicación y los detalles del cliente, le brinda información sobre los ataques a la aplicación. La información de infracción se envía a NetScaler ADM solo cuando se produce una infracción o un ataque. Muchas infracciones y vulnerabilidades conducen a un alto valor del índice de amenazas.

- **Índice de seguridad.** Sistema de clasificación de un solo dígito que indica con qué seguridad ha configurado las instancias NetScaler ADC para proteger las aplicaciones de amenazas y vulnerabilidades externas. Cuanto menores sean los riesgos de seguridad de una aplicación, mayor será el índice de seguridad. Los valores oscilan entre 1 y 7.

  El índice de seguridad considera tanto la configuración del firewall de aplicaciones como la configuración de seguridad del sistema NetScaler ADC. Para un valor de índice de seguridad elevado, ambas configuraciones deben ser fuertes. Por ejemplo, si se realizan comprobaciones rigurosas del firewall de aplicaciones, pero no se han adoptado medidas de seguridad del sistema NetScaler ADC, como una contraseña segura para el `nsroot` usuario, a las aplicaciones se les asigna un valor de índice de seguridad bajo.

- **Información procesable.** La información que necesita para reducir el índice de amenazas y aumentar el índice de seguridad, lo que mejora significativamente la seguridad de las aplicaciones. Por ejemplo, puede revisar la información sobre las infracciones, las configuraciones

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

de seguridad existentes y faltantes para el firewall de aplicaciones y otras funciones de seguridad, la velocidad a la que se atacan las aplicaciones, etc.

### Configurar Security Insight

Citrix ADM admite Security Insight desde todas las instancias de Citrix ADC que tengan configurado un firewall de aplicaciones.

Para configurar la información de seguridad en una instancia de ADC, primero configure un perfil de firewall de aplicaciones y una política de firewall de aplicaciones. Si bien, a continuación, puede vincular la directiva de firewall de aplicaciones de forma global, Citrix recomienda que la directiva esté enlazada al servidor virtual.

Para ver los análisis en Citrix ADM, habilite la función AppFlow en la instancia, configure un recopilador, una acción y una política de AppFlow y vincule la directiva de forma global. También en este caso, aunque puede vincular la directiva de firewall de aplicaciones de forma global, Citrix recomienda que la directiva esté enlazada al servidor virtual. Citrix también recomienda utilizar Citrix ADM para implementar las configuraciones de AppFlow en las instancias de ADC. Al configurar el recopilador, debe especificar la dirección IP del servidor NetScaler ADM en el que quiere supervisar los informes.

**Para configurar la información de seguridad en una instancia de Citrix ADC:**

1. Ejecute los siguientes comandos para configurar un perfil y una directiva de firewall de aplicaciones y enlazar la directiva de firewall de aplicaciones globalmente o al servidor virtual de equilibrio de carga.

**add appfw profile** [**-defaults** ( basic advanced )]

**set appfw profile** <name> [**-startURLAction** <startURLAction> …]

**add appfw policy** <name> <rule> <profileName>

**bind appfw global** <policyName> <priority>

o,

**bind lb vserver** <lb vserver> **-policyName** <policy> **-priority** <priority>

```
add appfw profile pr_appfw -defaults advanced
set  appfw profile pr_appfw -startURLaction log stats learn
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
   pr_appfw
bind appfw global pr_appfw_pol 1
or,
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
6 bind lb vserver outlook – policyName pr_appfw_pol – priority “ 20
    ”
```

2. Ejecute los siguientes comandos para habilitar la función AppFlow, configurar un recopilador, una acción y una directiva de AppFlow y enlazar la directiva globalmente o al servidor virtual de equilibrio de carga:

   **add appflow collector** <name> **-IPAddress** <ipaddress>

---

**set appflow param** DISABLED )]
[**-SecurityInsightRecordInterval** ]
[**-SecurityInsightTraffic** ( ENABLED

---

**agregar appflow action**\ <name\ > **-collectors** \ <string\ >

**add appflow policy** <name> <rule> <action>

**bind appflow global** <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

O bien:

**bind lb vserver** <vserver> **-policyName** <policy> **-priority** <priority>

```
1 add appflow collector col -IPAddress 10.102.63.85
2 set appflow param  -SecurityInsightRecordInterval 600 -
    SecurityInsightTraffic ENABLED
3 add appflow action act1 -collectors col
4 add appflow action af_action_Sap_10.102.63.85 -collectors col
5 add appflow policy pol1 true act1
6 add appflow policy af_policy_Sap_10.102.63.85 true
    af_action_Sap_10.102.63.85
7 bind appflow global pol1 1 END -type REQ_DEFAULT
8 or,
9 bind lb vserver Sap – policyName af_action_Sap_10.102.63.85 –
    priority “ 20 ”
```

**Para habilitar Security Insight desde NetScaler ADM:**

Si su NetScaler ADM es **13.0 Build 41.x**:

1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Configurar análisis**.
3. En la página **Configurar análisis en servidores virtuales**, seleccione el servidor virtual y haga clic en **Habilitar análisis**.
4. En la ventana **Habilitar análisis**:
   a) Seleccione **Security Insight**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Seleccione **Logstream** como modo de transporte

> **Nota**
>
> Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
>
> Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

c) La expresión es verdadera por defecto

d) Haga clic en **OK**.

> **Nota**
>
> - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
> - Para las particiones de administración, solo se admite **Web Insight**
> - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, Citrix ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

Si su Citrix ADM es **13.0 Build 36.27**:

1. Vaya a **Redes** > **Instancias** y seleccione la instancia de NetScaler ADC que quiere habilitar AppFlow.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione los servidores virtuales y haga clic en **Habilitar AppFlow** .
4. En el campo **Enable AppFlow** , escriba **true** y seleccione **Security Insight** .
5. Haga clic en **OK**.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso a nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

### Ver ubicaciones geográficas para los informes de Security Insight

Los informes de Security Insight incluyen las ubicaciones geográficas exactas desde las que se originan las solicitudes de los clientes. Puede ver las ubicaciones geográficas en Citrix ADM. El archivo de base de datos geográfica incorporado en Citrix ADC contiene la mayoría de las direcciones IP públicas. El archivo está disponible en la ubicación **/var/netscaler/inbuilt_db** en Citrix ADC.

**Para habilitar las ubicaciones geográficas:**

Ejecute los siguientes comandos para habilitar el registro de ubicación geográfica y el registro en formato CEF:

- **add locationFile** <Completar ruta con el nombre de archivo de la BD>
- **establecer la configuración de appfw -GeolocationLogging ON**
- **establecer la configuración de appfw -CEFLOGGING ON**

Si no hay ninguna dirección IP disponible en el archivo de base de datos geográfica, puede agregar la dirección IP para la ubicación geográfica. Junto con la dirección IP, también puedes añadir el nombre de la ciudad/estado/país y las coordenadas de latitud y longitud de cada ubicación.

Abra el archivo de base de datos geográfica con un editor de texto, como vi editor, y agregue una entrada para cada ubicación.

La entrada debe tener el siguiente formato:

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

Por ejemplo,

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
```

### Reputación de IP

Puede utilizar NetScaler Insight Center para supervisar y administrar la reputación IP de su tráfico entrante. Puede configurar directivas para agregar más IP como maliciosas y crear una lista de bloques personalizada.

Para obtener información sobre cómo configurar y usar la reputación de IP, consulte Reputación de IP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Supervisar la reputación IP

La función Reputación de IP proporciona información relacionada con ataques sobre direcciones IP malintencionadas. Por ejemplo, informa de la puntuación de la reputación IP, la categoría de la reputación IP, el tiempo de ataque de la reputación IP, la IP del dispositivo y los detalles sobre la dirección IP del cliente.

La puntuación de reputación IP indica el riesgo asociado a una dirección IP. La puntuación tiene los siguientes rangos:

| Puntuación de reputación IP | Nivel de riesgo |
|---|---|
| 1–20 | Alto riesgo |
| 21–40 | Sospechoso |
| 41–60 | Riesgo moderado |
| 61–80 | Riesgo bajo |
| 81–100 | Confiable |

**Para supervisar la reputación IP:**

1. Vaya a **Analytics** > **Security Insight** y seleccione la aplicación que desea supervisar.
2. En la ficha **Índice de amenazas**, seleccione **Reputación de IP.**
3. Seleccione una gravedad para mostrar más detalles de los ataques que estaban en ese nivel. Puede hacer clic en el gráfico de barras o en la tabla situada debajo del gráfico.
4. Seleccione el período de tiempo para el que desea ver los detalles. Puede usar el control deslizante de tiempo para personalizar aún más el período seleccionado. A continuación, haga clic en **Ir**.
5. Para personalizar la pantalla, haga clic en el botón de configuración.

## Umbrales

Puede establecer y ver los umbrales del índice de seguridad y el índice de amenazas de las aplicaciones en Security Insight.

**Para establecer un umbral:**

1. Vaya a **Analytics** > **Configuración** > **Umbrales** y seleccione **Agregar** .
2. Seleccione el tipo de tráfico como **Seguridad** en el campo **Tipo de tráfico** e introduzca la información requerida en los demás campos correspondientes, como Nombre, Duración y entidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la sección **Configurar regla** , utilice los campos Métrica, Comparador y Valor para establecer un umbral.

   Por ejemplo, “Índice de amenazas”“>”“5”

4. En la **configuración** de notificaciones , selecciona el tipo de notificación.
5. Haga clic en **Crear**.

**Para ver los incumplimientos de los umbrales:**

1. Vaya a **Analytics** > **Security Insight** > **Dispositivos** y seleccione la instancia de Citrix ADC.
2. En la sección **Aplicación**, puede ver el número de infracciones de umbral ocurridas para cada servidor virtual en la columna **Infracción de umbral**.

## Casos de uso de Security Insight

En los siguientes casos de uso se describe cómo puede utilizar Security Insight para evaluar la exposición a las amenazas de las aplicaciones y mejorar las medidas de seguridad.

### Obtenga una visión general del entorno de amenazas

En este caso de uso, tiene un conjunto de aplicaciones expuestas a ataques y ha configurado NetScaler ADM para supervisar el entorno de amenazas. Debe revisar con frecuencia el índice de amenazas, el índice de seguridad y el tipo y la gravedad de los ataques que puedan haber sufrido las aplicaciones, de modo que pueda centrarse primero en las aplicaciones que necesitan más atención. El panel de información de seguridad proporciona un resumen de las amenazas experimentadas por las aplicaciones durante un período de tiempo que elija y para un dispositivo NetScaler ADC seleccionado. Muestra la lista de aplicaciones, sus índices de amenazas y seguridad y el número total de ataques durante el período de tiempo elegido.

Por ejemplo, puede estar supervisando Microsoft Outlook, Microsoft Lync, SharePoint y una aplicación SAP, y es posible que quiera revisar un resumen del entorno de amenazas para estas aplicaciones.

Para obtener un resumen del entorno de amenazas, inicie sesión en **NetScaler ADM**y, a continuación, vaya a **Analytics > Security Insight**.

Se muestra información clave para cada aplicación. El período de tiempo predeterminado es 1 hora.

Para ver información de un período de tiempo diferente, seleccione un período de tiempo en la lista situada en la parte superior izquierda.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para ver un resumen de otra instancia de NetScaler ADC, en **Dispositivos**, haga clic en la dirección IP de la instancia de NetScaler ADC. Para ordenar la lista de aplicaciones por una columna determinada, haga clic en el encabezado de la columna.

### Determinar la exposición a amenazas de una aplicación

Para identificar las aplicaciones que tienen un índice de amenazas alto y un índice de seguridad bajo en el panel de control de Security Insight, debe determinar la exposición a las amenazas antes de decidir protegerlas. Es decir, desea determinar el tipo y la gravedad de los ataques que han degradado sus valores de índice. Puede determinar la exposición a amenazas de una aplicación consultando el resumen de la solicitud.

En este ejemplo, Microsoft Outlook tiene un valor de índice de amenazas de 6 y desea saber qué factores contribuyen a este índice de amenazas alto.

Para determinar la exposición a amenazas de Microsoft Outlook, en el panel **Security Insight** , haga clic en **Outlook** . El resumen de la aplicación incluye un mapa que identifica la ubicación geográfica del servidor.

Haga clic en **Índice de amenazas > Infracciones de comprobación de seguridad** y revise la información de infracción que aparece.

Haga clic en **Infracciones de firma** y revise la información de infracción que aparece.

### Determinar la configuración de seguridad existente y faltante para una aplicación

Después de revisar la exposición a amenazas de una aplicación, quiere determinar qué configuraciones de seguridad de la aplicación están implementadas y qué configuraciones faltan para esa aplicación. Puede obtener esta información profundizando en el resumen del índice de seguridad de la aplicación.

El resumen del índice de seguridad proporciona información sobre la eficacia de las siguientes configuraciones de seguridad:

- **Configuración del firewall de aplicaciones.** Muestra cuántas entidades de firma y seguridad no están configuradas.
- **Seguridad del sistema NetScaler.** Muestra cuántas opciones de seguridad del sistema no están configuradas.

En el caso de uso anterior, revisó la exposición a amenazas de Microsoft Outlook, que tiene un valor de índice de amenazas de 6. Ahora, desea saber qué configuraciones de seguridad existen para Outlook y qué configuraciones se pueden agregar para mejorar su índice de amenazas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En el panel **Security Insight** , haga clic en **Outlook** y, a continuación, en la pestaña **Índice de seguridad** . Revise la información proporcionada en el área **Resumen del índice de seguridad**.

En el nodo **Configuración del firewall de aplicaciones**, haga clic en **Outlook_Profile** y revise la información de comprobación de seguridad e infracción de firmas en los gráficos circulares.

Revise el estado de configuración de cada tipo de protección en la tabla de resumen del firewall de aplicaciones. Para ordenar la tabla en una columna, haga clic en el encabezado de la columna.

Haga clic en el nodo **NetScaler System Security** y revise la configuración de seguridad del sistema y las recomendaciones de Citrix para mejorar el índice de seguridad de las aplicaciones.

### Identificar aplicaciones que requieren atención inmediata

Las aplicaciones que requieren atención inmediata son aquellas que tienen un índice de amenaza alto y un índice de seguridad bajo.

En este ejemplo, tanto Microsoft Outlook como Microsoft Lync tienen un valor de índice de amenazas alto de 6, pero Lync tiene el menor de los dos índices de seguridad. Por lo tanto, es posible que tenga que centrar su atención en Lync antes de mejorar el entorno de amenazas para Outlook.

### Determinar el número de ataques en un tiempo dado

Es posible que quiera determinar cuántos ataques se produjeron en una aplicación determinada en un momento determinado o que quiera estudiar la tasa de ataques durante un período de tiempo específico.

En la página **Security Insight**, haga clic en cualquier aplicación y, en **Resumen de la aplicación**, haga clic en el número de infracciones. La página Total de Infracciones muestra los ataques de forma gráfica durante una hora, un día, una semana y un mes.

La tabla Resumen de la aplicación proporciona los detalles sobre los ataques. Algunos de ellos son los siguientes:

- Tiempo de ataque
- Dirección IP del cliente desde el que se produjo el ataque
- Gravedad
- Categoría de infracción
- URL desde la que se originó el ataque y otros detalles.

Aunque siempre puede ver la hora del ataque en un informe por hora como se ve en la imagen, ahora puede ver el intervalo de tiempo de ataque para los informes agregados, incluso para los informes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

diarios o semanales. Si selecciona «1 día» en la lista de períodos de tiempo, el informe Security Insight muestra todos los ataques agregados y el tiempo de ataque se muestra en un rango de una hora. Si elige "1 semana"o "1 mes", todos los ataques se agregan y el tiempo de ataque se muestra en un intervalo de un día.

### Obtener información detallada sobre infracciones de seguridad

Es posible que desee ver una lista de los ataques a una aplicación y obtener información sobre el tipo y la gravedad de los ataques, las acciones realizadas por la instancia de Citrix ADC, los recursos solicitados y el origen de los ataques.

Por ejemplo, es posible que desee determinar cuántos ataques a Microsoft Lync se bloquearon, qué recursos se solicitaron y las direcciones IP de las fuentes.

En el **panel Security Insight**, haga clic en **Lync > Total de infracciones**. En la tabla, haga clic en el icono de filtro en el encabezado de columna **Acción tomada** y, a continuación, seleccione **Bloqueado**.

Para obtener información acerca de los recursos solicitados, revise la columna **URL**. Para obtener información sobre las fuentes de los ataques, consulte la columna **IP del cliente** .

### Ver detalles de expresiones de registro

Las instancias de Citrix ADC utilizan expresiones de registro configuradas con el perfil de Application Firewall para tomar medidas en caso de ataques a una aplicación de la empresa. En Security Insight, puede ver los valores devueltos para las expresiones de registro utilizadas por la instancia de Citrix ADC. Estos valores incluyen el encabezado de la solicitud, el cuerpo de la solicitud, etc. Además de los valores de las expresiones de registro, también puede ver el nombre de la expresión de registro y el comentario de la expresión de registro definida en el perfil de Application Firewall que la instancia de Citrix ADC utilizó para tomar medidas contra el ataque.

**Requisitos previos** Asegúrese de que:

- Configure expresiones de registro en el perfil de Firewall de aplicaciones. Para obtener más información, consulte Application Firewall.
- Habilite la configuración Security Insights basada en expresiones de registro en Citrix ADM. Haga lo siguiente:
    1. Vaya a **Analytics > Configuración** y haga clic en **Habilitar funciones para Analytics** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página Habilitar función para análisis, seleccione **Habilitar Security Insight** en la sección **Configuración de Security Insight basada en expresiones de registro** y haga clic en **Aceptar**.

Por ejemplo, es posible que desee ver los valores de la expresión de registro devuelta por la instancia de Citrix ADC para la acción que llevó a cabo para atacar Microsoft Lync en su empresa.

En el panel de control de Security Insight, vaya a **Lync > Total de infracciones**. En la **tabla Resumen de la aplicación**, haga clic en la dirección URL para ver los detalles completos de la infracción en la página **Información de infracción**, incluidos el nombre de la expresión de registro, el comentario y los valores devueltos por la instancia de NetScaler ADC para la acción.

### Resaltar patrones de infracción para Web Application Firewall (WAF)

Ahora puede obtener detalles de ataques como encabezados HTTP y carga útil HTTP para solucionar problemas o analizar los ataques. Para obtener detalles de los ataques, debe actualizar el «VerboseLogLevel» en el perfil de Application Firewall mediante el siguiente comando:

```
Set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload
|patternPayloadHdr)
```

- `pattern`: Solo se registra el patrón de infracción
- `patternPayload`: Patrón de infracción + 150 bytes de valor del elemento de campo antes del patrón de ataque se registran
- `patternPayloadHdr` - Patrón de infracción + 150 bytes del valor del elemento de campo antes del patrón de ataque + se registran los encabezados de solicitud HTTP

Según la configuración «VerboseLogLevel», Citrix ADM muestra los registros detallados de expresiones de registro.

La siguiente imagen es un ejemplo que resalta el patrón de ataque para la solicitud GET:

La siguiente imagen es un ejemplo que resalta el patrón de ataque para la solicitud POST:

En estos dos ejemplos:

- **FIELDNAME**hace referencia al nombre de campo correspondiente al patrón de ataque.
- **PAYLOAD_OFFSET**hace referencia a la compensación del ataque en la carga útil real.
- **ATTACK_PATTERN** resalta el patrón de ataque e incluye 150 bytes de carga útil de prefijo en el valor.

Para obtener más información sobre la configuración del nivel de registro detallado en NetScaler ADC, consulte Facilidad para solucionar problemas con los registros de Firewall de aplicaciones web.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Determinar el índice de seguridad antes de implementar la configuración**

Las infracciones de seguridad se producen después de implementar la configuración de seguridad en una instancia de NetScaler ADC, pero es posible que quiera evaluar la eficacia de la configuración de seguridad antes de implementarla.

Por ejemplo, es posible que desee evaluar el índice de seguridad de la configuración de la aplicación SAP en la instancia de Citrix ADC con la dirección IP 10.102.60.27.

En el panel **Security Insight** , en **Dispositivos** , haga clic en la dirección IP de la instancia de Citrix ADC que configuró. Puede ver que tanto el índice de amenazas como el número total de ataques son 0. El índice de amenazas es un reflejo directo del número y el tipo de ataques a la aplicación. Cero ataques indican que la aplicación no está bajo ninguna amenaza.

Haga clic en **Sap > Índice de seguridad > SAP_profile** y evalúe la información del índice de seguridad que aparece.

En el resumen del firewall de la aplicación, puede ver el estado de configuración de diferentes configuraciones de protección. Si se establece una configuración para registrar o si no se ha configurado una configuración, se asigna a la aplicación un índice de seguridad inferior.

## Bot

January 30, 2024

> Nota
>
> Si la compilación de Citrix ADM es anterior a **13.0-79.x**, puede ver la información de los robots navegando a **Analytics > Security > Bot Insight**. Para la compilación **13.0-79.x o posterior**, puede ver los detalles del bot navegando a **Analytics > Seguridad > Infracciones de seguridad > Descripción general de la aplicación** y haciendo clic en **Bot** en **Desglose de aplicaciones por**.

Un bot es un programa de software que realiza automáticamente ciertas acciones una y otra vez a un ritmo mucho más rápido que un humano. Más del 35 por ciento del tráfico web está compuesto por bots y el 80 por ciento de las organizaciones sufren ataques de bots. Pueden interactuar con una página web, enviar formularios, hacer clic en vínculos, escanear texto o descargar contenido. Los bots pueden acceder a vídeos, publicar comentarios y tuitear en las plataformas de redes sociales. Algunos bots pueden incluso mantener conversaciones básicas con usuarios humanos. Estos se conocen como chatbots.

Un bot que realiza un servicio necesario o útil como servicio al cliente, chatbots, rastreadores de motores de búsqueda se conocen como buenos bots. Algunos bots malintencionados pueden extraer

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

o descargar contenido de un sitio web, robar credenciales de usuario, difundir contenido de spam y realizar varios otros tipos de ciberataques. Estos bots maliciosos se conocen como bots malos. Es fundamental identificar los robots defectuosos y proteger el dispositivo de los ataques de seguridad avanzados. Puede lograr esto usando un sistema de administración de bots.
Para obtener más información sobre Bot, consulte Administración de bots.

### Configurar técnicas de detección de bot en Citrix ADC

En Citrix ADC, puede configurar técnicas de detección de bots para detectar el tráfico de bots entrante. Las siguientes son las técnicas bot que se configuran en la instancia de Citrix ADC:

- **Lista de permitidos**. Esta regla contiene una lista de URL y expresiones de directivas para evaluar si hay un conjunto específico de bots buenos que pueden acceder a su recurso web.
- **Lista de bloqueos**. Esta regla contiene una lista de URL y expresiones de directiva para evaluar si un conjunto específico de bots maliciosos puede acceder a su sitio web.
- **Reputación IP**. Esta regla detecta si el tráfico entrante del bot es una dirección IP maliciosa.
- **Toma de huellas dactilares del dispositivo**. Esta regla detecta si el tráfico de bots entrantes tiene el ID de huella digital del dispositivo en el encabezado de la solicitud entrante y los atributos del navegador del tráfico de un bot cliente entrante.
- **Limitación de velocidad**. Esta tasa de regla limita varias solicitudes procedentes del mismo cliente.
- **Firmas**. Esta regla detecta y bloquea los bots en función de la detección de firmas. También evita direcciones URL no autorizadas que raspan sitios web, inicios de sesión de fuerza bruta y bots que investigan vulnerabilidades.
- **Trampas de bots**. Esta regla detecta los bots que acceden al script que está habilitado en la página web.
- **TPS**. Esta regla detecta el tráfico entrante como bots si el máximo de solicitudes y el aumento porcentual de solicitudes exceden el intervalo de tiempo configurado.

Para obtener más información sobre cómo configurar la administración de bots, consulte Configurar la administración de bots.

### Uso de Bot Insight en Citrix ADM

Después de configurar la administración de bots en Citrix ADC, debe habilitar **Bot Insight** en servidores virtuales para ver información en Citrix ADM.

Para activar **Bot Insight**:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes** > **Instancias** > **Citrix ADC** y seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione el servidor virtual y haga clic en **Habilitar análisis**.
4. En la ventana **Habilitar análisis**:
   a) Seleccione **Bot Insight**
   b) En **Opción avanzada**, selecciona **Logstream**.
   c) Haga clic en **Aceptar**.

Tras activar **Bot Insight**, vaya a **Analytics** > **Bot Insight**.

**1** - Lista de horas para ver los detalles del bot

**2** —Arrastre el control deslizante para seleccionar un rango de tiempo específico y haga clic en **Ir** para mostrar los resultados personalizados

**3** —Total de instancias afectadas por los bots

**4** —Servidor virtual para la instancia seleccionada con un total de ataques de bots

- **Total de bots**: indica el total de ataques de bots (incluidas todas las categorías de bots) encontrados en el servidor virtual.
- **Total de navegadores humanos**: indica el total de usuarios humanos que acceden al servidor virtual.
- **Proporción entre bots y humanos**: indica la proporción entre los usuarios humanos y los bots que acceden al servidor virtual.
- **Bots de firma**, **bots con huellas digitales**, **bots basados en tasas**, bots de **reputación IP, bots**de **lista permitida y bots**de **lista de bloqueo**: indica el total de ataques de bot ocurridos en función de la categoría de bot configurada. Para obtener más información sobre la categoría de bots, consulte Configurar técnicas de detección de bots en Citrix ADC.

**5**: Haga clic en **>** para ver los detalles del bot en un formato gráfico.

## Ver historial de eventos

Puede ver las actualizaciones de las firmas del bot en el **Historial de eventos** cuando:

- Se agregan nuevas firmas bot en instancias de Citrix ADC.
- Las firmas bot existentes se actualizan en las instancias de Citrix ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede seleccionar la duración del tiempo en la página de información sobre bots para ver el historial de eventos.

El siguiente diagrama muestra cómo se recuperan las firmas bot de la nube de AWS, se actualizan en Citrix ADC y ver el resumen de la actualización de firmas en Citrix ADM.

1. El programador de actualización automática de la firma de bot recupera el archivo de asignación del URI de AWS.
2. Comprueba las firmas más recientes del archivo de mapeo con las firmas existentes en el dispositivo ADC.
3. Descarga las nuevas firmas de AWS y verifica la integridad de la firma.
4. Actualiza las firmas de bot existentes con las nuevas firmas del archivo de firma del bot.
5. Genera una alerta SNMP y envía el resumen de actualización de firmas a Citrix ADM.

### Ver bots

Haga clic en el servidor virtual para ver el **resumen de la aplicación**.

**1** —Proporciona los detalles del resumen de la solicitud, tales como:

- **RPS medio**: indica el promedio de solicitudes de transacciones de bots por segundo (RPS) recibidas en los servidores virtuales.
- **Bots por gravedad**: indica las transacciones de bots más altas ocurridas en función de la gravedad. La gravedad se clasifica en función de **Crítica**, **Alta**, **Media**y **Baja**.

  Por ejemplo, si los servidores virtuales tienen 11 770 bots de gravedad alta y 1550 bots de gravedad crítica, Citrix ADM muestra **1,55 K** Críticos en **Bots por gravedad**.
- **Categoría de bot más grande**: indica los ataques de bots más altos que se produjeron en función de la categoría de bot.

  Por ejemplo, si los servidores virtuales tienen 8000 bots en la lista Bloque, 5000 Permitir bots enumerados y 10000 bots límite de velocidad superado, Citrix ADM muestra **Límite de velocidad superado 10 K** en **Categoría de bots más grande**.
- **Fuente geográfica más grande**: indica el mayor número de ataques de bots que se produjeron en función de una región.

  Por ejemplo, si los servidores virtuales tienen 5000 ataques de bots en Santa Clara, 7000 ataques de bots en Londres y 9000 ataques de bots en Bangalore, Citrix ADM **muestra Bangalore 9** K en Largest Geo Source **.**
- **Porcentaje medio de tráfico de bots**: indica la proporción de bots humanos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**2** —Muestra la gravedad de los ataques de los bots en función de las ubicaciones en la vista del mapa

**3** —Muestra los tipos de ataques de bots (buenos, malos y todos)

**4** —Muestra el total de ataques de bots junto con las acciones configuradas correspondientes. Por ejemplo, si ha configurado:

- Intervalo de direcciones IP (192.140.14.9 a 192.140.14.254) como bots de lista de bloqueo y seleccionado Drop como acción para estos intervalos de direcciones IP
- Rango IP (192.140.15.4 a 192.140.15.254) como bots de lista de bloqueo y seleccionado para crear un mensaje de registro como una acción para estos rangos de IP

  En este caso, Citrix ADM muestra:

  - Total de bots listados en bloque
  - Total de bots bajo **Abandonado**
  - Total de bots bajo **registro**

### Ver bots CAPTCHA

En las páginas web, los CAPTCHA están diseñados para identificar si el tráfico entrante proviene de un robot humano o automatizado. Para ver las actividades CAPTCHA en Citrix ADM, debe configurar CAPTCHA como una acción bot para la reputación IP y las técnicas de detección de huellas dactilares de dispositivos en una instancia de Citrix ADC. Para obtener más información, consulte Administración de bots.

Las siguientes son las actividades CAPTCHA que Citrix ADM muestra en Bot insight:

- **Se han superado los intentos de CAPTCHA**: indica el número máximo de intentos de CAPTCHA realizados después de errores de inicio de sesión
- **Cliente de Captcha silenciado**: indica la cantidad de solicitudes de clientes que se descartan o redirigen porque estas solicitudes se detectaron anteriormente como bots defectuosos con el desafío de CAPTCHA
- **Humano**: indica las entradas de captcha realizadas por los usuarios humanos
- **Respuesta captcha no válida**: indica el número de respuestas CAPTCHA incorrectas recibidas del bot o humano, cuando Citrix ADC envía un desafío CAPTCHA

### Ver bots de trampa de bots

Para ver las capturas de bot en Citrix ADM, debe configurar la captura de bot en la instancia de Citrix ADC. Para obtener más información, consulte Administración de bots.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para identificar las trampas de bot, se habilita un script en la página web y este script se oculta a los humanos, pero no a los bots. Citrix ADM identifica e informa de las trampas de bot cuando los bots acceden a este script.

Haga clic en el servidor virtual y seleccione **Zero Pixel Request**

#### Ver bots TPS

Las siguientes son las categorías de bot TPS que puede ver en Citrix ADM:

- IP de origen
- Ubicación geográfica
- Host
- URL

Haga clic en el servidor virtual para ver los bots de TPS.

Haga clic en la **categoría de bot TPS** para ver los detalles del bot.

Aparecerá la página de detalles.

#### Ver categorías de bot para aplicaciones móviles (Android)

Para ver los bots para aplicaciones móviles (Android), debe configurar la técnica de detección de huellas digitales en Citrix ADC. Para obtener más información, consulte Configurar la técnica de huella digital del dispositivo para aplicaciones móviles.

Después de configurar los ajustes en Citrix ADC, puede ver las siguientes categorías de bot en Citrix ADM:

- Límite de tasa de cliente web
- Límite de tasa de Android
- Dispositivo de cliente Web
- Dispositivo Android

Haga clic en el servidor virtual para ver las categorías de bot aplicables a la aplicación móvil.

### Ver detalles del bot

Para obtener más detalles, haga clic en el tipo de ataque de bot en **Categoría de bot**. Por ejemplo, si quiere ver los detalles de los ataques de bot en la lista de bloques, haga clic en **Lista de bloques** en **Categoría de bots**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Se muestran los detalles como el tiempo de ataque y el número total de ataques de bots.

También puede arrastrar el gráfico de barras para seleccionar el intervalo de tiempo específico que se mostrará con los ataques de los bots.

Para obtener información adicional sobre el ataque del robot, haga clic para expandir.

- **IP de instancia**: indica la dirección IP de la instancia de Citrix ADC
- **Total de bots**: indica el total de ataques de bots que se produjeron durante ese tiempo en particular
- **URL de solicitud HTTP**: indica la URL que está configurada para que aparezca en la lista de bloques
- **Código de país**: indica el país en el que se produjo el ataque del bot
- **Región**: indica la región en la que se produjo el ataque del bot
- **Nombre del perfil**: indica el nombre del perfil que proporcionó durante la configuración

### Búsqueda avanzada

También puede utilizar el cuadro de texto de búsqueda y la lista de duración, donde puede ver los detalles del bot según sus necesidades. Al hacer clic en el cuadro de búsqueda, el cuadro de búsqueda muestra la siguiente lista de sugerencias de búsqueda.

- **instance-IP: dirección IP** de la instancia de Citrix ADC
- **IP de cliente: dirección** IP del cliente
- **Tipo de bot**: tipo de bot, como bueno o malo
- Gravedad:**gravedad** del ataque del bot
- **Acción realizada**: acción realizada después del ataque del bot, como dejar caer, no realizar ninguna acción o redirigir
- **Categoría de bots**: categoría del ataque de bot, como lista de bloqueo, lista de permitidos, huella digital, etc. En función de una categoría, puede asociar una acción bot a ella
- **Detección de bots**: tipos de detección de bots (lista de bloqueo, lista de permitidos, etc.) que ha configurado en la instancia de Citrix ADC
- **Ubicación**: región/país en el que se ha producido el ataque del bot
- **request-URL**: URL que contiene los posibles ataques de bots

También puede utilizar operadores en las consultas de búsqueda para limitar el enfoque de la búsqueda. Por ejemplo, si quieres ver todos los bots defectuosos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Haga clic en el cuadro de búsqueda y selecciona **Bot-Type**
2. Vuelva a hacer clic en el cuadro de búsqueda y seleccione el operador **=**
3. Vuelva a hacer clic en el cuadro de búsqueda y seleccione **Malo**
4. Haga clic en **Buscar** para ver los resultados

## Ver detalles de infracciones de seguridad de la aplicación

January 30, 2024

Las aplicaciones web que están expuestas a Internet se han vuelto vulnerables a los ataques drásticamente. NetScaler ADM le permite visualizar detalles de infracciones accionables para proteger las aplicaciones contra ataques. Vaya a **Analytics** > **Seguridad** > **Infracciones de seguridad** para obtener una solución de un solo panel para:

- Visualice las aplicaciones con visibilidad completa de los detalles de amenazas asociados tanto a la información de seguridad como a la información sobre robots
- Acceda a las infracciones de seguridad de la aplicación en función de sus categorías como **Network**, **Bot** y **WAF**
- Tomar medidas correctivas para proteger las aplicaciones

La página **Infracciones de Seguridad** tiene las siguientes opciones:

- **Descripción general de la aplicación**: muestra una descripción general de las aplicaciones que tienen infracciones totales, infracciones de WAF y bot totales, infracciones por país, etc. Para obtener más información, consulte Descripción general de la aplicación.
- **Todas las infracciones**: muestra los detalles de infracción de seguridad de la aplicación. Para obtener más información, consulte Todas las infracciones.

### Requisito previo

Asegúrese de que el **recopilador de métricas** esté habilitado. De forma predeterminada, **Metrics Collector** está habilitado en la instancia de NetScaler ADC. Para obtener más información, consulte Configurar el análisis inteligente de aplicaciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Insight SSL

January 30, 2024

SSL Insight proporciona visibilidad de las transacciones web seguras (HTTPS) y permite a los administradores de TI monitorear todas las aplicaciones web seguras que ofrece NetScaler ADC al proporcionar una supervisión histórica e integrada en tiempo real de las transacciones web seguras. Con esta visibilidad, el administrador puede evaluar lo siguiente:

- **Determine el impacto de los cambios de configuración en el uso de los clientes**: el administrador puede entender el impacto que tiene en los clientes realizar un cambio de configuración, como desactivar SSLv3 o eliminar un cifrado como el RC4-MD5. Esto se puede hacer evaluando los datos históricos de transacciones en este protocolo y cifrado.
- **Cuantificar el rendimiento del cliente**: El administrador puede comprender el impacto en el tiempo de respuesta de la aplicación según los cifrados/protocolo SSL utilizados o los certificados negociados.
- **Seguridad de las aplicaciones**: evalúe si alguna de las aplicaciones tiene transacciones que se ejecutan con protocolos de baja seguridad, cifrados o claves de baja seguridad.

Cuando SSL Analytics está habilitado en una instancia de NetScaler ADC, las estadísticas SSL se registran y registran para cada transacción SSL. Las estadísticas muestran los detalles del flujo SSL. Además, Citrix Application Delivery Management (ADM)
registra y muestra cada conexión correcta .

SSL Insight proporciona la siguiente información crítica, que muestra NetScaler ADM Analytics:

- Versión del protocolo SSL negociada
- El cifrado negociado y la fuerza del cifrado
- Algoritmo de hash de firma del certificado utilizado
- Tipo y tamaño de certificado
- Errores de front-end y back-end de SSL

> **Nota**
>
> Para conexiones SSL correctas, el registro SSL AppFlow ocurre al final de cada transacción.

## Requisitos previos

- La instancia de NetScaler ADC en la que pretende configurar SSL Insight debe ejecutar la versión 11.1 51.21 y superior del software NetScaler ADC. Ejecute los siguientes comandos en la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

instancia ADC que ejecuta 11.1 51.21 para habilitar Logstream como tipo de transporte para SSL Insight.

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   Para las instancias ADC que ejecutan la versión 12.0 y superior, seleccione Logstream como tipo de transporte mientras habilita AppFlow desde ADM.

- La versión y la compilación de NetScaler ADM deben ser iguales o superiores a la versión y la compilación de NetScaler ADC. Por ejemplo, si ha instalado NetScaler ADM 11.1 build 61.7, asegúrese de haber instalado NetScaler ADC 11.1 build 60.14 o anterior.

## Configurar SSL Insight

Las Métricas de Insight SSL se incluyen en los informes de Web Insight si habilita los siguientes elementos:

- Habilite AppFlow for Web Insight en cada instancia de Citrix ADC.
- Habilite el modo ULFD en cada instancia de Citrix ADC.
- Habilite los parámetros necesarios de AppFlow en cada instancia de NetScaler ADC.

## Habilite la función AppFlow

> **Nota**
>
> Puede habilitar la función AppFlow desde Citrix ADM o desde cada instancia de Citrix ADC.

**Para habilitar la función AppFlow desde Citrix ADM:**

Si su NetScaler ADM es **13.0 compilación 41.x o posterior**:

1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione el tipo de instancia. Por ejemplo, VPX.
2. Seleccione la instancia y, en la lista **Seleccionar acción**, haga clic en **Configurar análisis**.
3. En la página **Configurar análisis en servidores virtuales**, seleccione el servidor virtual y haga clic en **Habilitar Analytics**.
4. En la ventana **Habilitar análisis**:

   a) Seleccione **Web Insight**

   b) Seleccione **Logstream** como modo de transporte

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Para Citrix ADC 12.0 o anterior, **IPFIX** es la opción predeterminada para el modo de transporte. Para Citrix ADC 12.0 o posterior, puede seleccionar **Logstream** o **IPFIX** como Modo de transporte.
>
> Para obtener más información sobre IPFIX y Logstream, consulte Descripción general de Logstream .

c) La expresión es verdadera por defecto

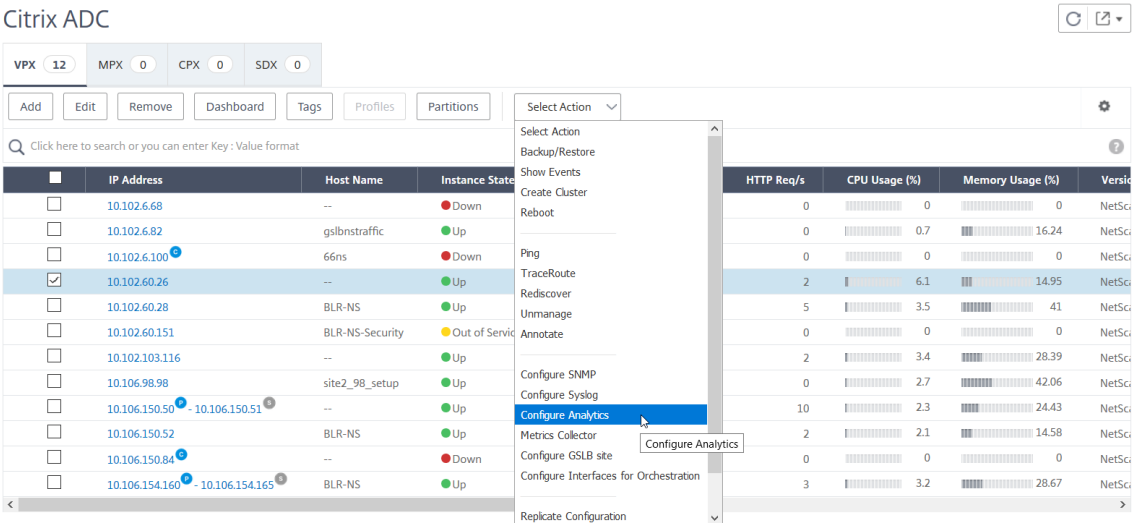
d) Haga clic en **OK**.

> **Nota**
>
> - Si selecciona servidores virtuales que no tienen licencia, Citrix ADM primero licencia esos servidores virtuales y, a continuación, habilita el análisis.
> - Para las particiones de administración, solo se admite **Web Insight**
> - En el caso de los servidores virtuales, como el redireccionamiento de caché , la autenticación y el GSLB , no puede habilitar el análisis. Aparece un mensaje de error.

Después de hacer clic en **Aceptar**, Citrix ADM procesa para habilitar el análisis en los servidores virtuales seleccionados.

Si su NetScaler ADM es **13.0 compilación 36.27 o anterior**:

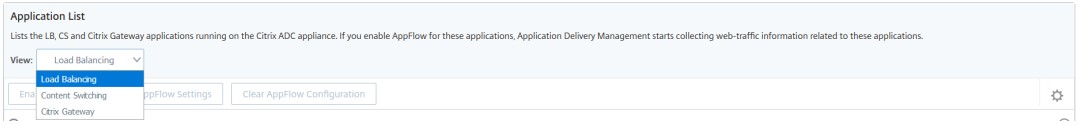
1. Vaya a **Redes** > **Instancias** > **NetScaler ADC** y seleccione la instancia de NetScaler ADC en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.



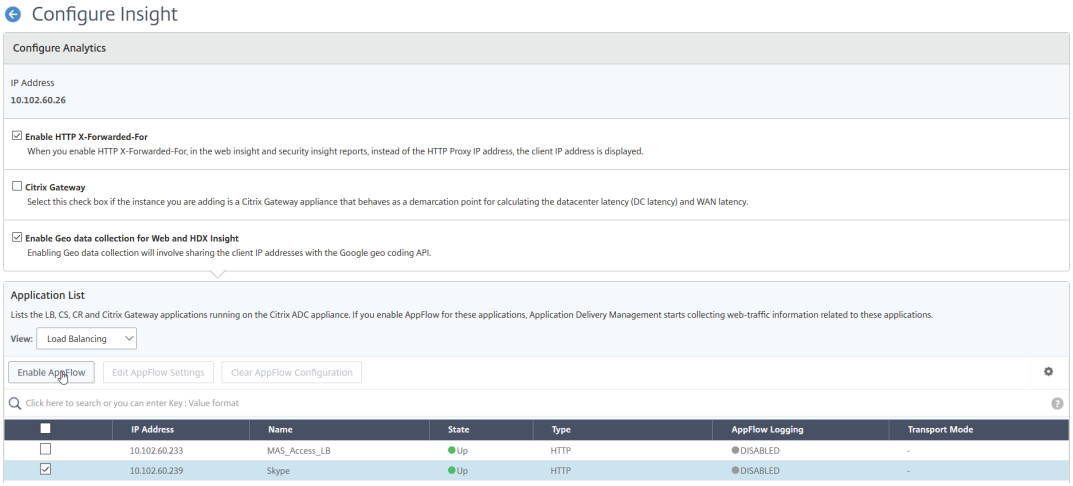

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. En la página **Configurar información** :

   a) Seleccione la **Lista de aplicaciones** para Equilibrio de carga o Content Switching.




   b) Seleccione el servidor virtual y haga clic en **Habilitar AppFlow**.



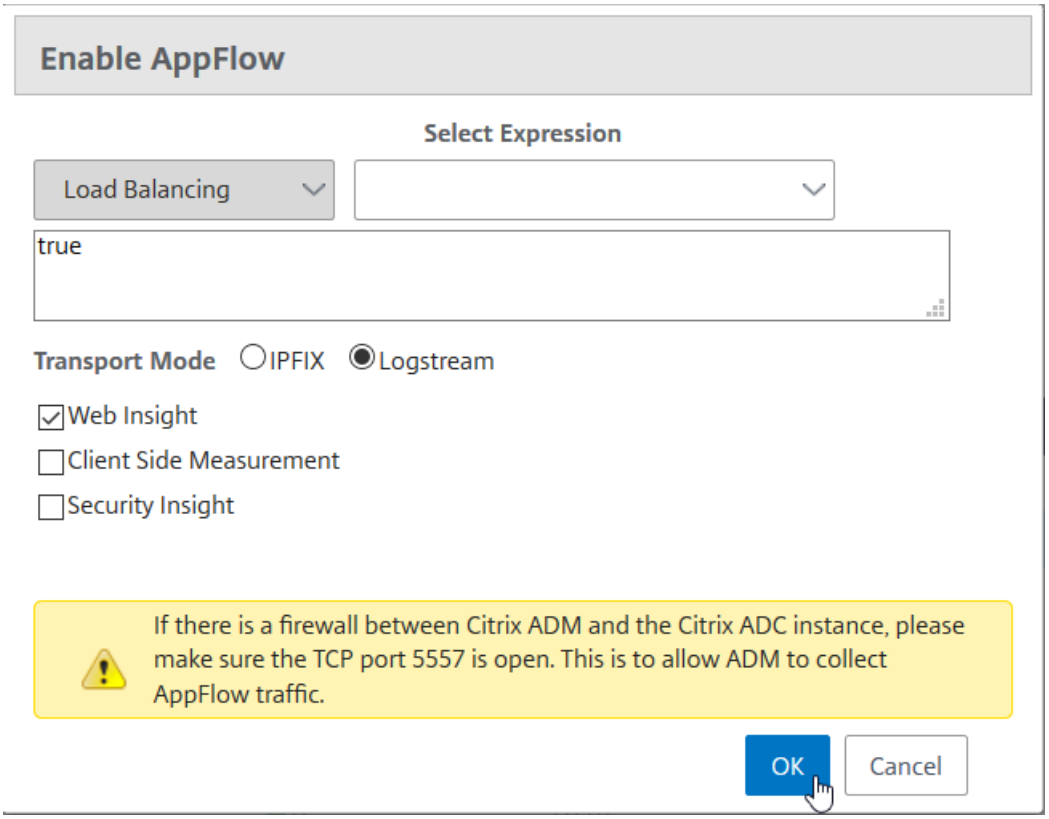

4. En el cuadro de diálogo Habilitar AppFlow:

   - Introduzca **true** en el cuadro de texto
   - Seleccione **Logstream** como modo de transporte

     > Nota: Citrix recomienda seleccionar Logstream como modo de transporte.

   - Seleccione **Web Insight** y haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Para habilitar la función AppFlow mediante la GUI de NetScaler ADC:**

En la GUI de una instancia de NetScaler ADC, vaya a **Configuración** > **Sistema** > **Configuración**, haga clic en **Configurar funciones avanzadas** y seleccione **AppFlow**.

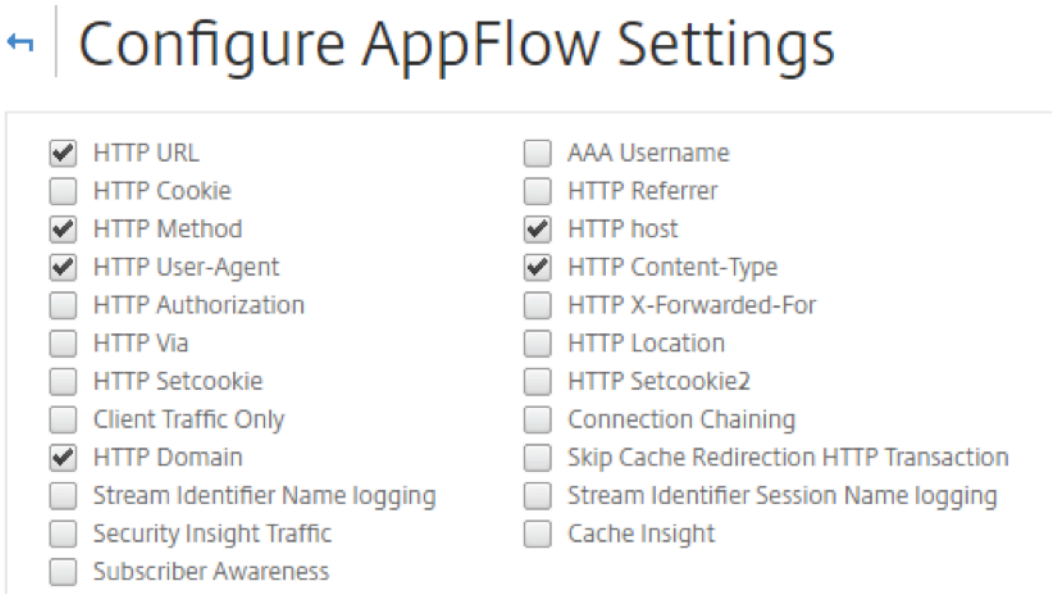
## Habilitar parámetros Insight SSL

En cada instancia de NetScaler ADC, debe habilitar algunos parámetros HTTP para mostrar registros SSL Insight en NetScaler ADM.

**Para habilitar los parámetros de SSL Insight desde la utilidad de configuración Citrix ADC:**

1. Vaya a **Configuración** > **Sistema** > **AppFlow**y haga clic en **Cambiar configuración de AppFlowSettings**.
2. Seleccione las siguientes casillas de verificación: **dominio HTTP, hostHTTP, método HTTP**, **URL HTTP, agente de usuarioHTTP, tipo de contenido HTTP**.
3. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Ver las métricas de Insight SSL

Las métricas SSL Insight de NetScaler ADM proporcionan una vista detallada del rendimiento de las transacciones SSL servidas por las instancias NetScaler ADC. Puede ver las métricas de SSL Insight a nivel de cliente, servidor o aplicación, y las métricas de las transacciones de éxito y error de SSL. Con la ayuda de estas métricas, puede analizar y optimizar la configuración de **HTTPS y la configuración del certificado SSL de NetScaler ADC**, y realizar un seguimiento de los problemas de rendimiento.

> **Nota**
>
> Al crear un grupo, puede asignar roles al grupo, proporcionar acceso a nivel de aplicación al grupo y asignar usuarios al grupo. El análisis de Citrix ADM ahora admite la autorización basada en direcciones IP virtuales. Ahora los usuarios pueden ver informes de todas las Insights solo para las aplicaciones (servidores virtuales) a las que están autorizados. Para obtener más información sobre los grupos y la asignación de usuarios al grupo, consulte Configurar grupos.

**Para supervisar las métricas de SSL Insight en NetScaler ADM:**

Puede ver las métricas de SSL para:

- Una aplicación. Vaya a **Aplicaciones > Panel**, haga clic en una aplicación y seleccione la ficha **Web Insight** para ver las métricas detalladas. Para obtener más información, consulte Análisis de uso de aplicaciones.
- Todas las aplicaciones. Vaya a **Aplicaciones > Web Insight** y haga clic en **las fichas Aplicaciones** y **Clientes** para ver las métricas de SSL.

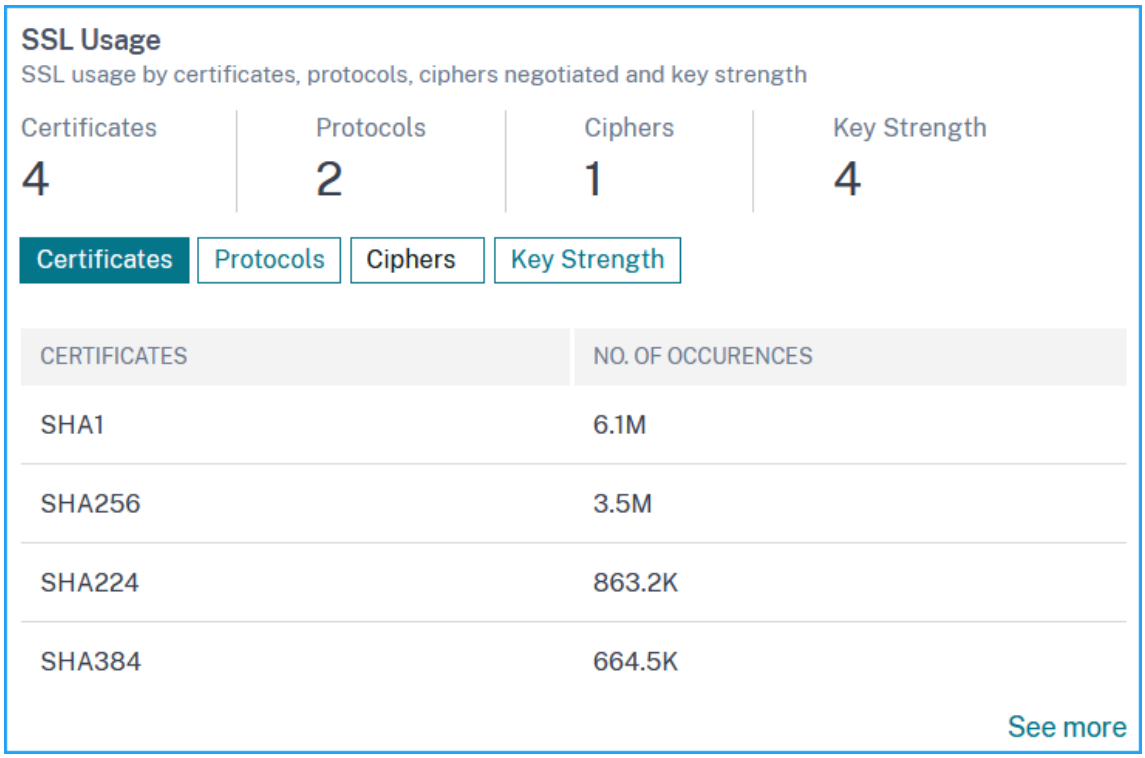
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Caso de uso: obtener una visión general de las transacciones SSL

El siguiente caso de uso describe cómo puede usar SSL Insight para evaluar el uso de varios parámetros SSL y mejorar las medidas de seguridad.

Tenga en cuenta que tiene un conjunto de aplicaciones que utilizan transacciones SSL (HTTPS) para la comunicación y que ha configurado NetScaler ADM para supervisar los componentes SSL. Es posible que tenga que revisar con frecuencia las aplicaciones para poder centrarse primero en las aplicaciones que necesitan más atención. El panel de control de **Web Insight** para una aplicación o todas las aplicaciones proporciona un resumen de los siguientes parámetros de SSL en **Errores** de **SSL y uso de SSL**:

- Certificados SSL
- Protocolos SSL
- Cifrado SSL
- Seguridad de la clave SSL
- Fallo SSL —Front end
- Fallo de SSL —Back end



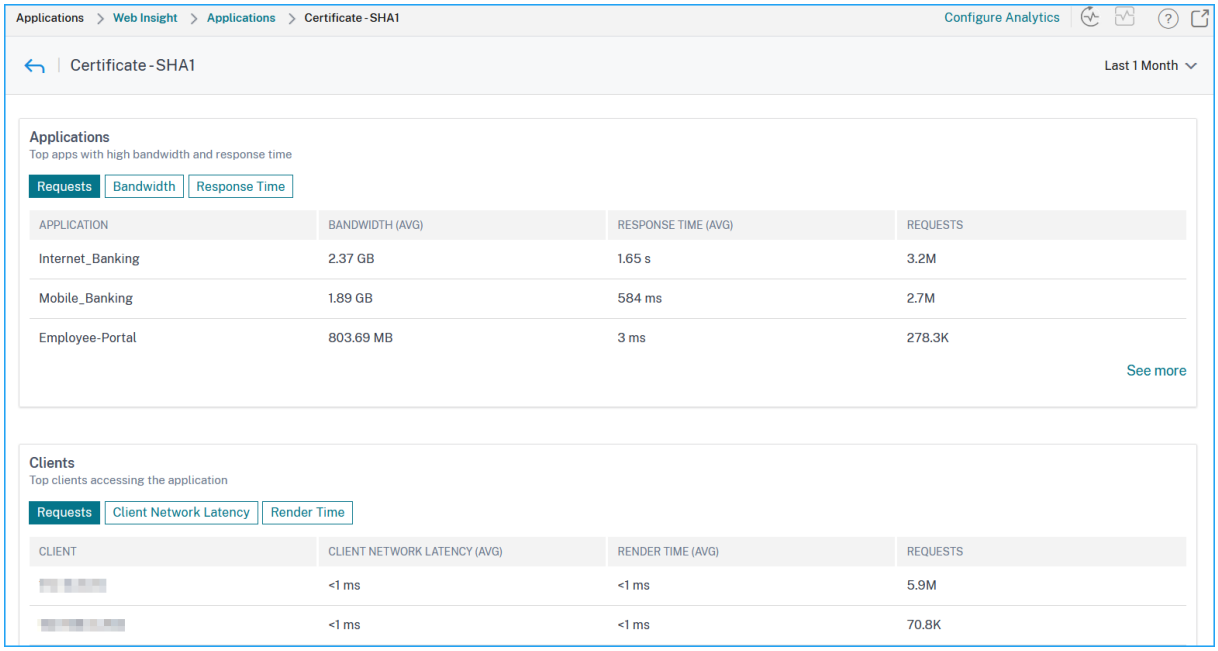

Puede hacer clic en cada ficha para ver los detalles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Caso de uso: métricas de SSL para clientes

Puede ver la lista de clientes (identificados por sus direcciones IP) y las ocurrencias totales por cliente. Vaya a **Aplicaciones > Web Insight** y seleccione la ficha **Clientes** para ver los detalles en **Uso de SSL**.

Haga clic en una métrica para ver los detalles y, en **Clientes**, haga clic en cualquier dirección IP del cliente para ver las métricas de SSL para el cliente seleccionado.




## Información TCP

January 30, 2024

La función TCP Insight de Citrix Application Delivery Management (ADM) proporciona una solución fácil y escalable para supervisar las métricas de las técnicas de optimización y las estrategias (o algoritmos) de control de la congestión que se utilizan en los dispositivos Citrix ADC para evitar la congestión de la red en la transmisión de datos. Esta función utiliza la función "Informe de velocidad de TCP", que mide el rendimiento de carga o descarga de archivos TCP con y sin optimización de TCP.

Puede ver **las métricas clave de la capa de transporte**, como el volumen de datos, el rendimiento y la velocidad, y utilizar esa información para medir el volumen de tráfico servido por las instancias de NetScaler ADC y validar los beneficios de la optimización de TCP. Para las métricas anteriores, se proporcionan desgloses por dirección de transmisión (del cliente a NetScaler ADC y de NetScaler ADC al servidor de origen), puerto TCP y LAN virtual.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Requisitos previos

Antes de empezar a configurar la función TCP Insight, asegúrese de que se cumplen los siguientes requisitos previos:

- Las instancias de NetScaler ADC se ejecutan en la versión 11.1 del software, compilación 51.21 o posterior.
- Ha instalado NetScaler ADM en la versión 11.1 del software, compilación 51.21 o posterior.
- Todos los servidores virtuales configurados para una aplicación tienen licencia para administración y supervisión en NetScaler ADM.
  Para obtener información sobre las licencias de Citrix ADM, consulte Licencias.

### Habilitación de TCP Insight

Antes de poder ver las métricas de TCP Insight, debe habilitar la función en NetScaler ADM.

**Para habilitar TCP Insight:**

1. En un explorador web, escriba la dirección IP del dispositivo virtual NetScaler ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Analytics** > **Configuración** y haga clic en **Habilitar funciones para Analytics**.
4. En la página **Habilitar funciones para Analytics**, seleccione **Habilitar TCP Insight**.
5. En la ventana de confirmación, haga clic en **Aceptar**.

### Vea las métricas de TCP Insight en NetScaler ADM

Después de habilitar TCP Insight en NetScaler ADM, puede ver información clave de la capa de transporte, como el modo de tráfico (datos de Internet o móviles), el volumen de datos, el rendimiento, las interfaces, los puertos, la velocidad media de carga y la velocidad media de descarga.

**Para mostrar métricas de TCP Insight en NetScaler ADM:**

Vaya a **Analytics** > **TCP Insight** .

Puede colocar el puntero del mouse sobre los gráficos de barras para ver el volumen de datos de las técnicas de transporte correspondientes. También puede ver el volumen de datos y otras métricas en la tabla debajo del gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota** Puede personalizar las métricas que se muestran en el gráfico mediante el icono de configuración de la tabla. También puede seleccionar el período de tiempo al que pertenecen las métricas y utilizar el control deslizante de tiempo para ajustar el período de tiempo.

También puede ver las métricas de elementos como las interfaces, los puertos y las velocidades de bits seleccionándolos de la lista **TCP Insight**.

## Casos de uso

Los siguientes casos de uso ilustran algunas de las formas de usar TCP Insight en los dispositivos NetScaler ADC:

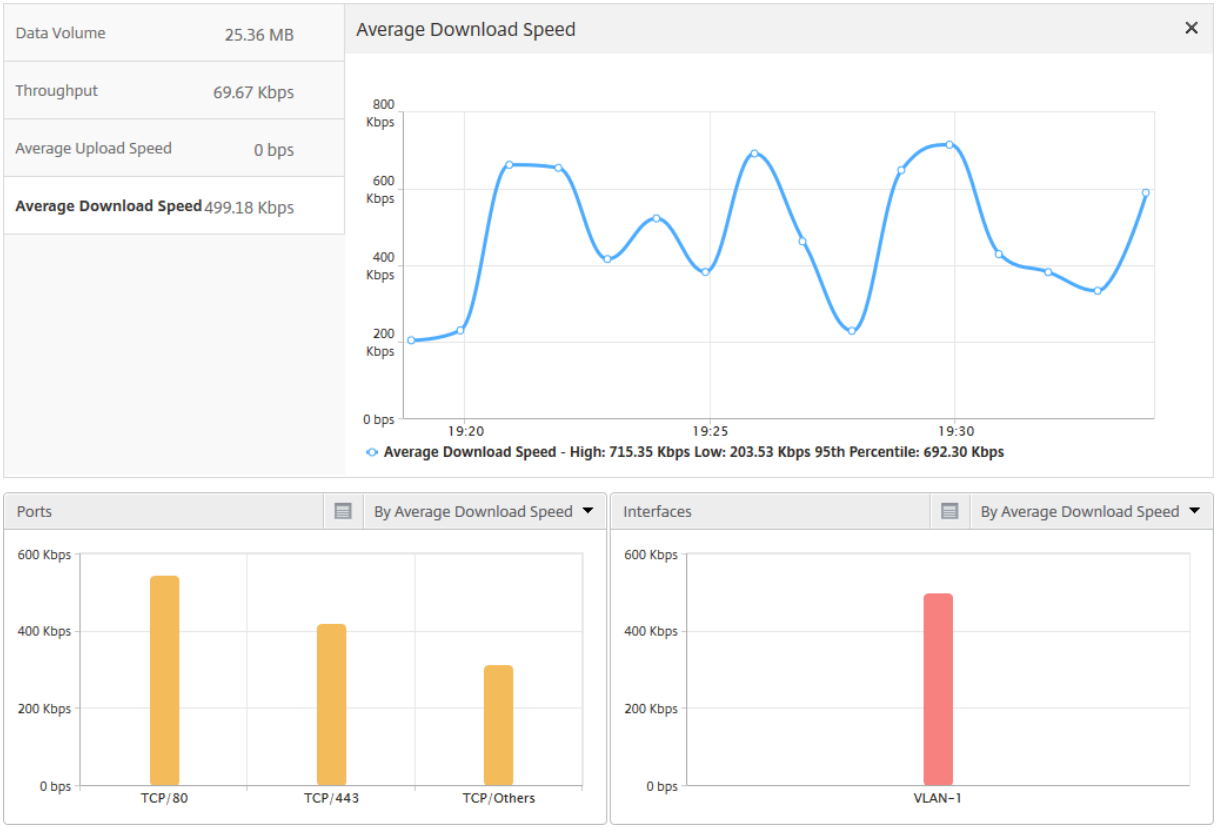
- Evalúe los beneficios de la optimización
- Ajustar parámetros TCP
- Medir el impacto de la optimización TCP en el volumen de tráfico

### Evalúe los beneficios de la optimización

¿En qué medida beneficia realmente la optimización TCP de NetScaler ADC a una red móvil (radio) o empresarial (Internet)? Puede ver la velocidad de las transferencias de datos que se realizan a través de TCP y comparar el rendimiento optimizado y no optimizado. Estas mediciones se muestran por separado para las instrucciones de descarga y carga (siempre en el lado de la radio/cliente), y para diferentes puertos de destino, HTTP (80) y HTTPS (443).
Al examinar las métricas de TCP Insight, puede cuantificar la mejora de velocidad obtenida al optimizar los flujos de TCP.

Para ver un resumen de estos parámetros, inicie sesión en NetScaler ADM y haga clic en la ficha **TCP Insight**. A continuación, haga clic en **Lados** y seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla debajo del gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

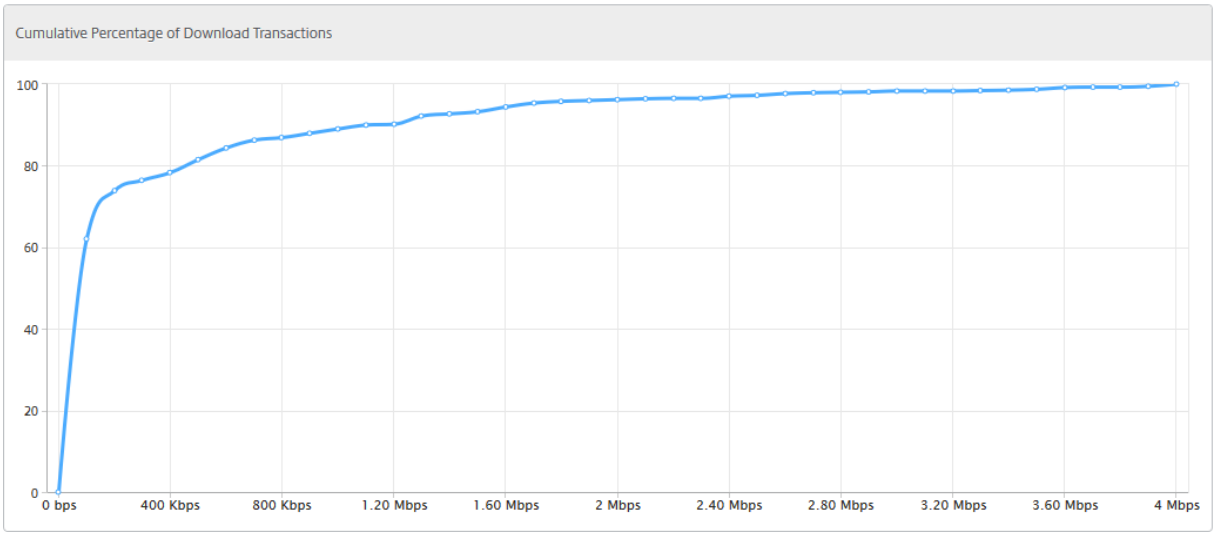



### Ajustar parámetros TCP

El uso de diferentes perfiles TCP puede generar diferentes salidas para el mismo tráfico. En tales situaciones, es posible que quiera ver y comparar las mediciones de velocidad de los períodos en los que NetScaler ADC ejecuta diferentes perfiles de optimización de TCP. Puede utilizar los resultados para ajustar los parámetros de TCP para una transmisión más rápida y desarrollar un perfil TCP que maximice la experiencia percibida por el usuario en una red de cliente específica.

Para ver los informes, inicie sesión en NetScaler ADM. A continuación, en la ficha **TCP Insight**, haga clic en **Bitrates**y seleccione la velocidad de bits deseada en el gráfico de barras o en la tabla debajo del gráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



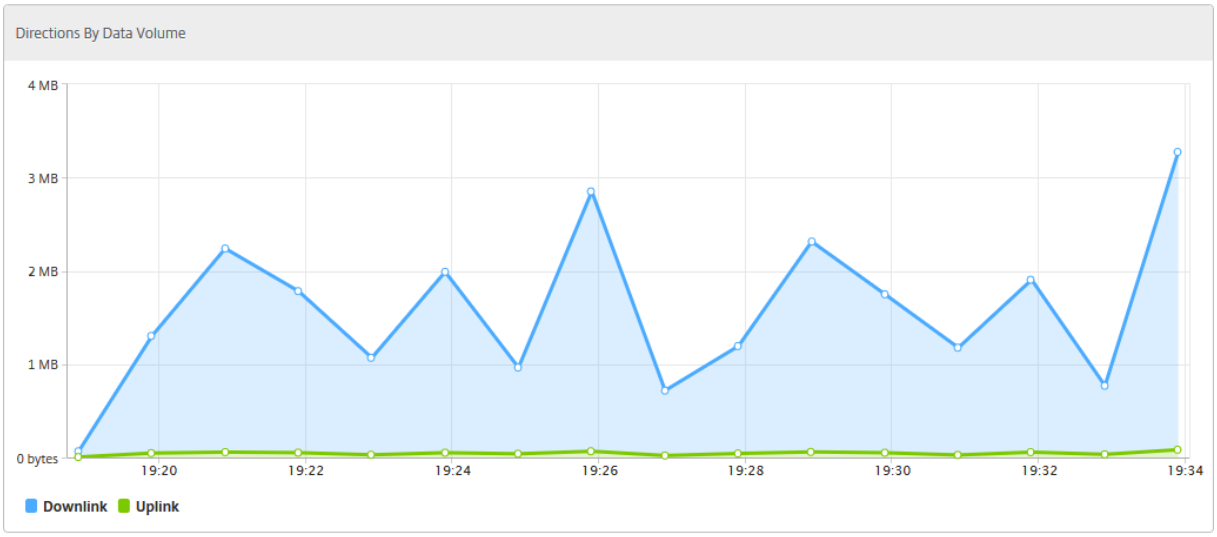

### Medir el impacto de la optimización TCP en el volumen de tráfico

Las mediciones del volumen/rendimiento de datos de la capa IP gestionadas por una instancia de NetScaler ADC se pueden comparar entre diferentes períodos de tiempo para evaluar el efecto de la optimización de TCP en el consumo de datos de los suscriptores. Las mediciones se pueden aplicar por separado para cada lado de la red (lado de la radio frente al lado de Internet), para diferentes segmentos de tráfico (delineados por diferentes interfaces o VLAN), para cada dirección (enlace descendente o enlace ascendente) y para diferentes puertos de destino (HTTP y HTTPS). La comparación se puede utilizar para confirmar que la optimización de TCP alienta a los suscriptores a consumir más datos.

Para obtener un resumen de las mediciones, inicie sesión en NetScaler ADM y, en la ficha **TCP Insight**, haga clic en **Lados**y, a continuación, seleccione **Internet** o **Radio** en el gráfico de barras o en la tabla situada debajo del gráfico.

También puede seleccionar un período de tiempo diferente de la lista de tiempos. Puede personalizar el marco de tiempo mediante el control deslizante de marco de tiempo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## WAN Insight

January 30, 2024

Los dispositivos de optimización de WAN (WO) Citrix SD-WAN optimizan la entrega de muchas aplicaciones a través de la WAN, mejorando la eficiencia del flujo de datos a través de la red entre el centro de datos y las sucursales.

Los análisis de WAN Insight permiten a los administradores supervisar fácilmente el tráfico WAN acelerado y no acelerado que fluye entre el centro de datos y los dispositivos de optimización de WAN de sucursal. WAN Insight proporciona visibilidad a los clientes, aplicaciones y sucursales de la red, para ayudar a solucionar problemas de red de manera eficaz. Los informes históricos y activos le permiten abordar problemas de forma proactiva, si los hay.

Al habilitar el análisis en el dispositivo de optimización de WAN del centro de datos, NetScaler ADM puede recopilar datos y proporcionar informes y estadísticas para el centro de datos y los dispositivos de optimización de WAN de sucursal.

**Para habilitar el análisis en el dispositivo de optimización WAN:**

1. Vaya a **Redes**> **Instancias** > **Citrix SD-WAN** y seleccione la instancia de SD-WAN WO.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. Seleccione los siguientes parámetros según sea necesario:

   - **Recopilación de datos geográficos para HDX Insight**: comparte la dirección IP del cliente con la API de Google Geo.

   - **AppFlow** : comienza a recopilar datos de las instancias de optimización de WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **TCP y WanOpt**: proporciona informes **TCP y WanOpt** Insight .
- **HDX**: Proporciona informes HDX Insight.
- **TCP solo para HDX**: Proporciona TCP solo para los informes HDX Insight.

4. Haga clic en **Aceptar**.

**Para ver informes de WAN Insight**:

1. Vaya a **Analytics** > **WAN Insight**.

> **Nota**
>
> La opción WAN Insight solo está visible después de agregar una instancia WO de SD-WAN a NetScaler ADM.

Puede ver los siguientes informes:

- **Aplicaciones** : muestra las estadísticas de uso y rendimiento de todas las aplicaciones durante la duración seleccionada.
- **Sucursales**: Muestra las estadísticas de uso y rendimiento de todos los dispositivos de sucursal de optimización WAN.
- **Clientes**: Muestra las estadísticas de uso y rendimiento de todos los clientes que acceden a los dispositivos de optimización WAN, en cada rama.

Se muestran las siguientes métricas:

| Métrica | Descripción |
|---|---|
| Conexiones rápidas activas | Número de conexiones WAN activas que se aceleran. |
| Conexiones no aceleradas activas | Número de conexiones WAN activas que no están aceleradas. |
| Latencia de WAN | Retraso, en milisegundos, que experimenta el usuario al interactuar con una aplicación. |
| Índice de compresión | Relación de compresión de datos entre la sucursal y los dispositivos del centro de datos durante la duración seleccionada. |
| Paquetes enviados | Número de paquetes que el dispositivo de optimización de WAN ha enviado a través de la red durante el tiempo seleccionado. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métrica | Descripción |
| --- | --- |
| Paquetes recibidos | Número de paquetes que el dispositivo de optimización de WAN ha recibido de la red durante el tiempo seleccionado. |
| Bytes enviados a través de WAN | Número de bytes que el dispositivo de optimización de WAN de Citrix ha enviado a través de la WAN durante el tiempo seleccionado. |
| Bytes recibidos a través de WAN | Número de bytes que el dispositivo de optimización de WAN recibió de la WAN durante el tiempo seleccionado. |
| RTO LAN | Número de veces que el dispositivo de optimización de WAN ha agotado el tiempo de espera de la retransmisión a la LAN durante el tiempo seleccionado. |
| RTO WAN | Número de veces que el dispositivo de optimización de WAN ha agotado el tiempo de espera de la retransmisión a la WAN durante el tiempo seleccionado. |
| Paquetes de retransmisión (LAN) | Número de paquetes que el dispositivo de optimización de WAN ha retransmitido a la red LAN durante el tiempo seleccionado. |
| Paquetes de retransmisión (WAN) | Número de paquetes que el dispositivo de optimización de WAN ha retransmitido a la red WAN durante el tiempo seleccionado. |

## Video Insight

January 30, 2024

La función Video Insight proporciona una solución fácil y escalable para monitorear las métricas de las técnicas de optimización de vídeo utilizadas por los dispositivos NetScaler ADC a fin de mejorar la experiencia del cliente y la eficiencia operativa, y ofrece beneficios como:

- Administre la red durante la congestión en las horas pico.
- Mejore la coherencia de la reproducción de vídeo y reduzca el bloqueo de vídeo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Habilite nuevas ofertas de servicios de video (por ejemplo, los servicios de video Binge-on).
- Permita que los clientes seleccionen la mejor calidad de vídeo sostenible.
- Ofrezca una experiencia de usuario coherente para el suscriptor.

Mientras optimiza el tráfico de vídeo, el dispositivo NetScaler ADC utiliza un mecanismo especial para acelerar dinámicamente la velocidad de bits de vídeo y una técnica de muestreo aleatorio para estimar los ahorros derivados de la técnica de optimización. Para obtener más información sobre la función de optimización de vídeo de NetScaler ADC, consulte Optimización de vídeo.Cuando integra NetScaler ADC appliance con NetScaler Application Delivery Management (ADM), recopila información clave de los datos de vídeo que fluyen a través del dispositivo NetScaler ADC. Puede utilizar esta información para comparar el rendimiento optimizado y no optimizado del tráfico de vídeo ABR, determinar el ahorro debido a la optimización, etc.

> **Nota**
>
> Las estadísticas de las sesiones no optimizadas proporcionadas en NetScaler ADM corresponden a las sesiones seleccionadas de muestreo aleatorio en NetScaler ADC Appliance. Para obtener más información sobre el muestreo aleatorio, consulteOptimización de vídeo.

Video Insight en NetScaler ADM proporciona métricas para los siguientes tipos de tráfico de vídeo:

- Descarga progresiva (PD) de vídeos a través de HTTP
- Vídeos de ABR a través de HTTP
- Vídeos de ABR a través de HTTPS
- Vídeos ABR de YouTube a través de QUIC

## Configuración de Video Insight

> **Nota**
>
> Video Insight es compatible con las instancias de NetScaler ADC con licencia NetScaler ADC Premium. La licencia NetScaler ADC Premium es compatible con las plataformas NetScaler ADC Telco (VPX T1000 y VPX-T).

Para configurar Video Insight en una instancia de Citrix ADC, primero habilite la función AppFlow, configure un recopilador, una acción y una directiva de AppFlow y vincule la directiva de forma global. Al configurar el recopilador, debe especificar la dirección IP del servidor Citrix ADM en el que desea supervisar los informes.

Para configurar la información de vídeo en una instancia de NetScaler ADC, ejecute los siguientes comandos para configurar un perfil y una directiva de AppFlow y enlazar la directiva de AppFlow globalmente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**add appflow collector** <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

**set appflow param** -**videoInsight** ENABLED

**add appflow action** <name> **-collectors** <string> **-videoAnalytics** ENABLED

**add appflow policy** <name> <rule> <action>

**bind appflow global** <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

**enable ns mode** `ulfd`

**enable feature** AppFlow

#### Sample

```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
    Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
```

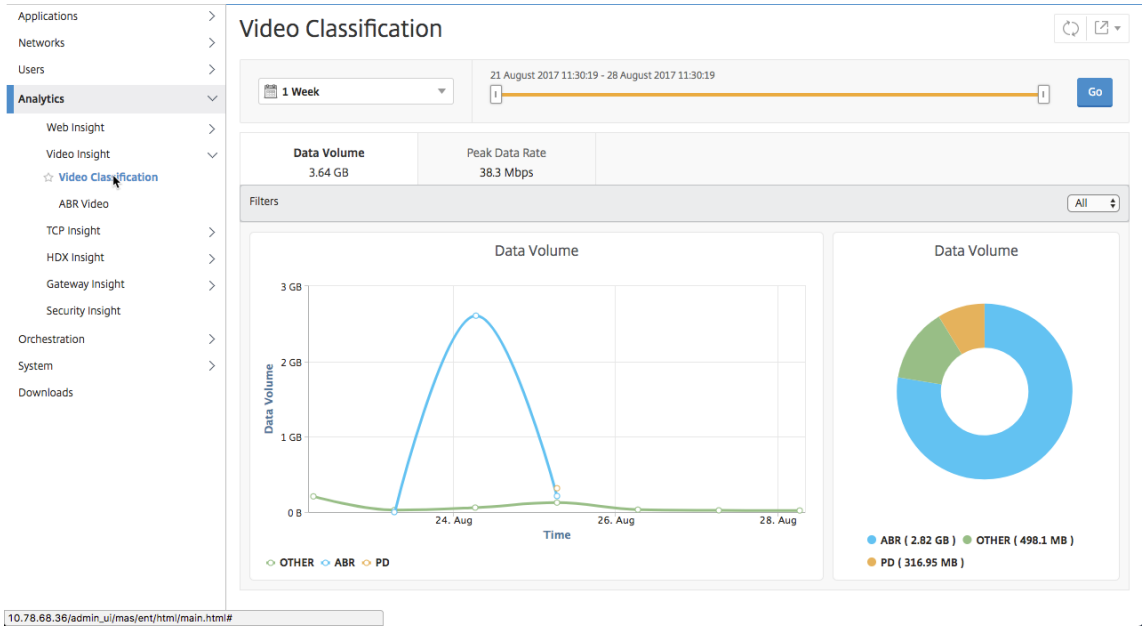
### Visualización de las métricas de Video Insight en NetScaler ADM

Después de habilitar Video Insight en NetScaler ADM, puede ver métricas de optimización de vídeo, como clasificación de vídeo, volumen de datos, velocidad máxima de datos y reproducciones de vídeo ABR. Estas métricas le ayudan a analizar su red y optimizar los vídeos para mejorar la experiencia del suscriptor, la eficiencia operativa y otros criterios de rendimiento.

**Para ver las métricas de Video Insight en Citrix ADM:**

1. En un explorador web, escriba la dirección IP del dispositivo virtual NetScaler ADM (por ejemplo, http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. Vaya a **Analytics > Video Insight**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> Los valores proporcionados por la leyenda **OTHER** en los gráficos representan los datos que no son ABR ni PD en el tráfico de vídeo, según el filtro que haya seleccionado:
>
> - **All**: Suma de datos no ABR (HTTP, HTTPS y QUIC) y no PD (HTTP) en el tráfico de vídeo.
> - **HTTP**: Suma de los datos que no son ABR y que no son PD en el tráfico de vídeo.
> - **HTTPS**: Suma de los datos de vídeo que no son ABR en el tráfico de vídeo.
> - **QUIC**: Suma de los datos de vídeo que no son ABR en el tráfico de vídeo.

## Ver la eficiencia de la red

January 30, 2024

Para un período determinado, Citrix Application Delivery Management (ADM) proporciona un gráfico que muestra la proporción de sesiones de vídeo optimizadas y no optimizadas en ese período. También muestra el porcentaje de ancho de banda ahorrado por la optimización. El porcentaje de ancho de banda ahorrado se calcula con la siguiente fórmula:

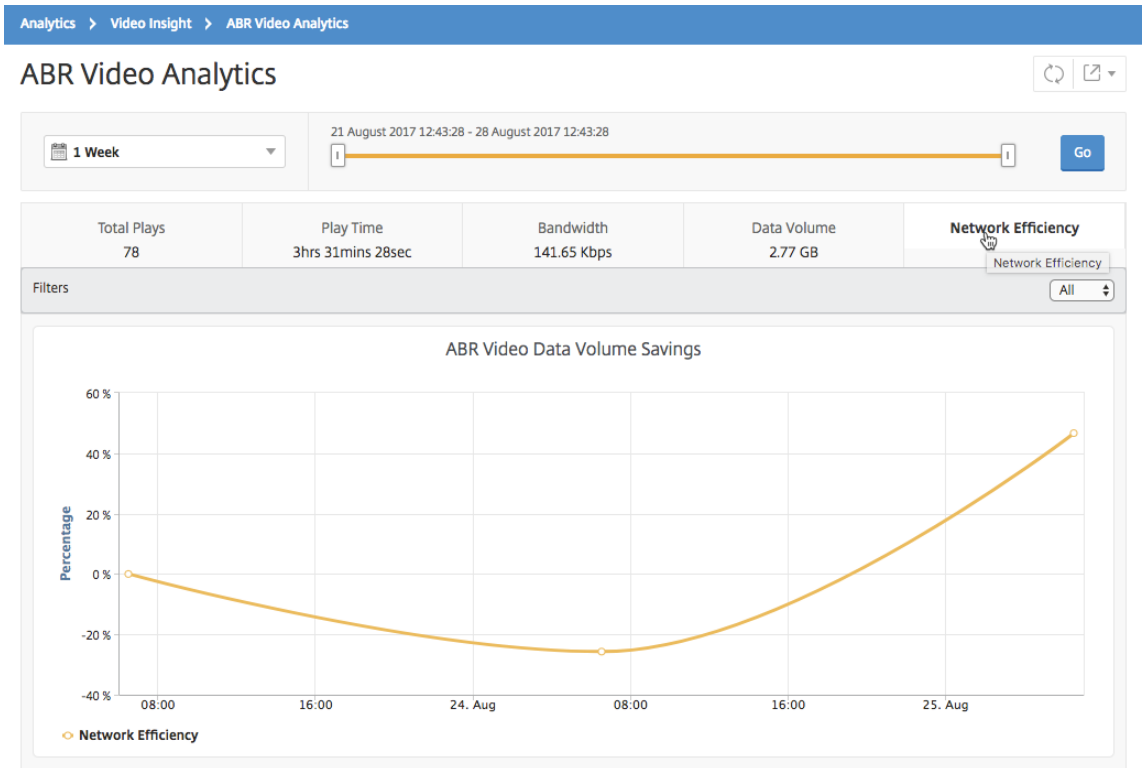
**Porcentaje de ancho de banda ahorrado** = Volumen de **datos de vídeo ABR optimizado promedio/Volumen de datos de vídeo ABR no optimizado**.

Para ver el porcentaje de ancho de banda ahorrado por la optimización:

1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Eficiencia de la red**.




## Compare el volumen de datos utilizado por los videos ABR optimizados y no optimizados

January 30, 2024

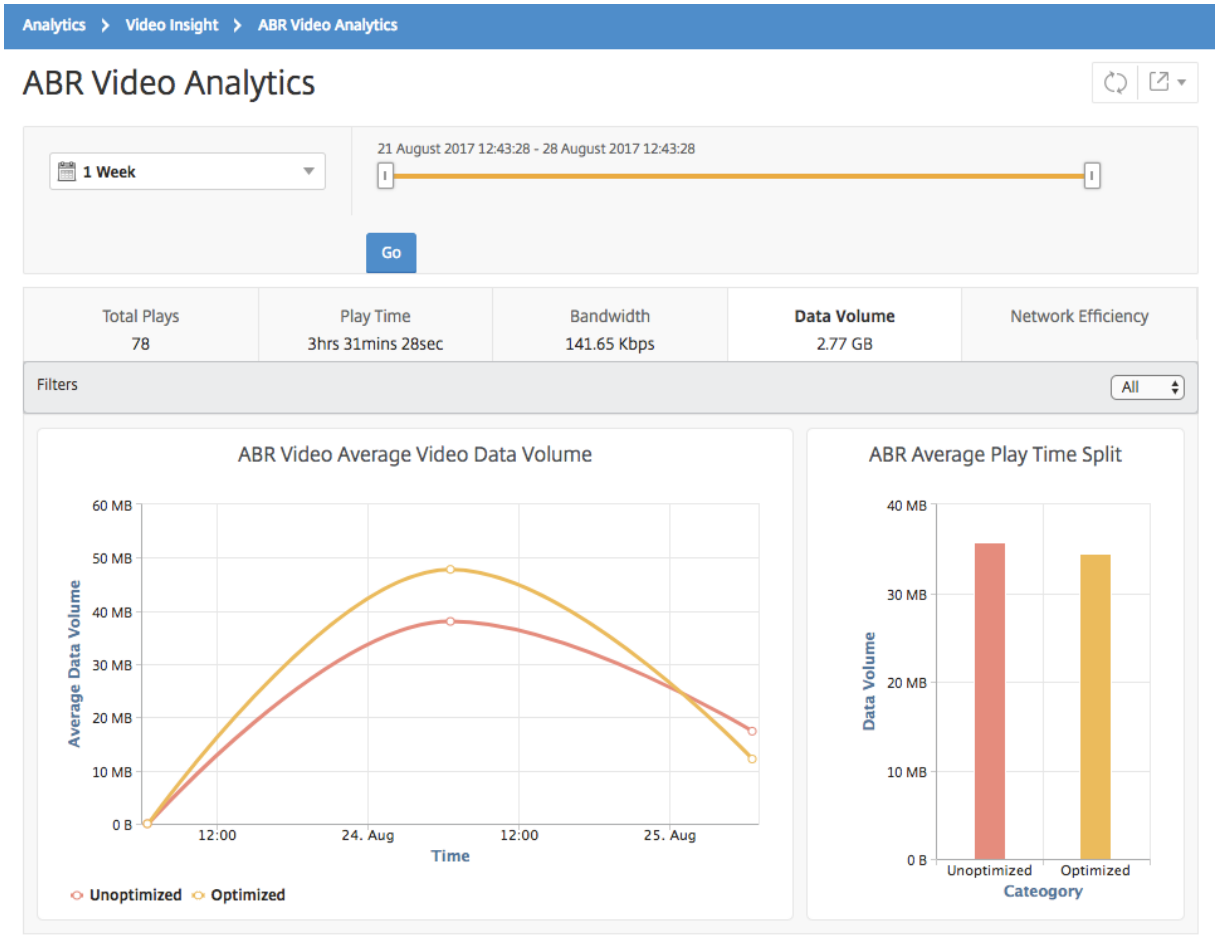
Durante un período determinado, Citrix Application Delivery Management (ADM) muestra el volumen de datos utilizado por los vídeos de ABR optimizados y no optimizados, para que pueda comparar los dos volúmenes.

Para ver el volumen de datos que utilizan los vídeos de ABR:

1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video.**
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Volumen de datos**.

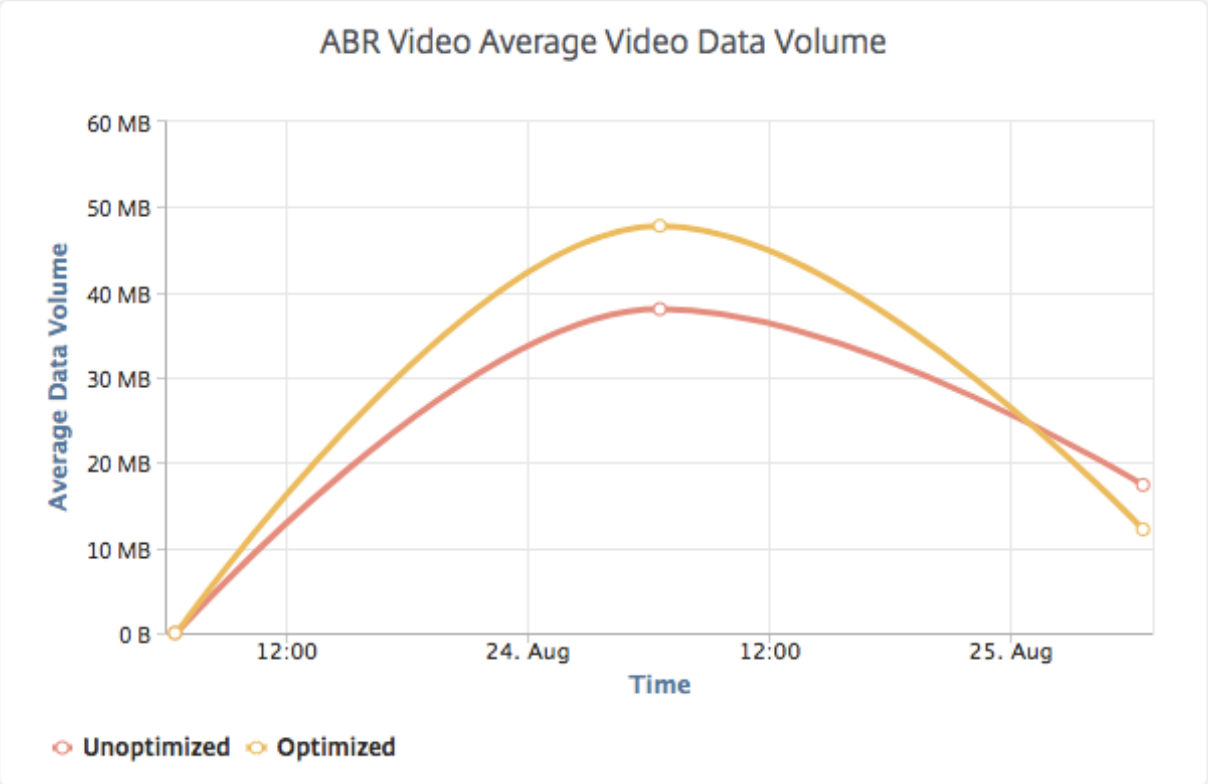
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.




La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que describe el volumen de datos promedio utilizado por los vídeos ABR y el volumen de datos consumido por los vídeos ABR optimizados y no optimizados de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el volumen de datos promedio utilizado durante un período de tiempo determinado:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Ver el tipo de vídeos transmitidos y el volumen de datos consumido de la red

January 30, 2024

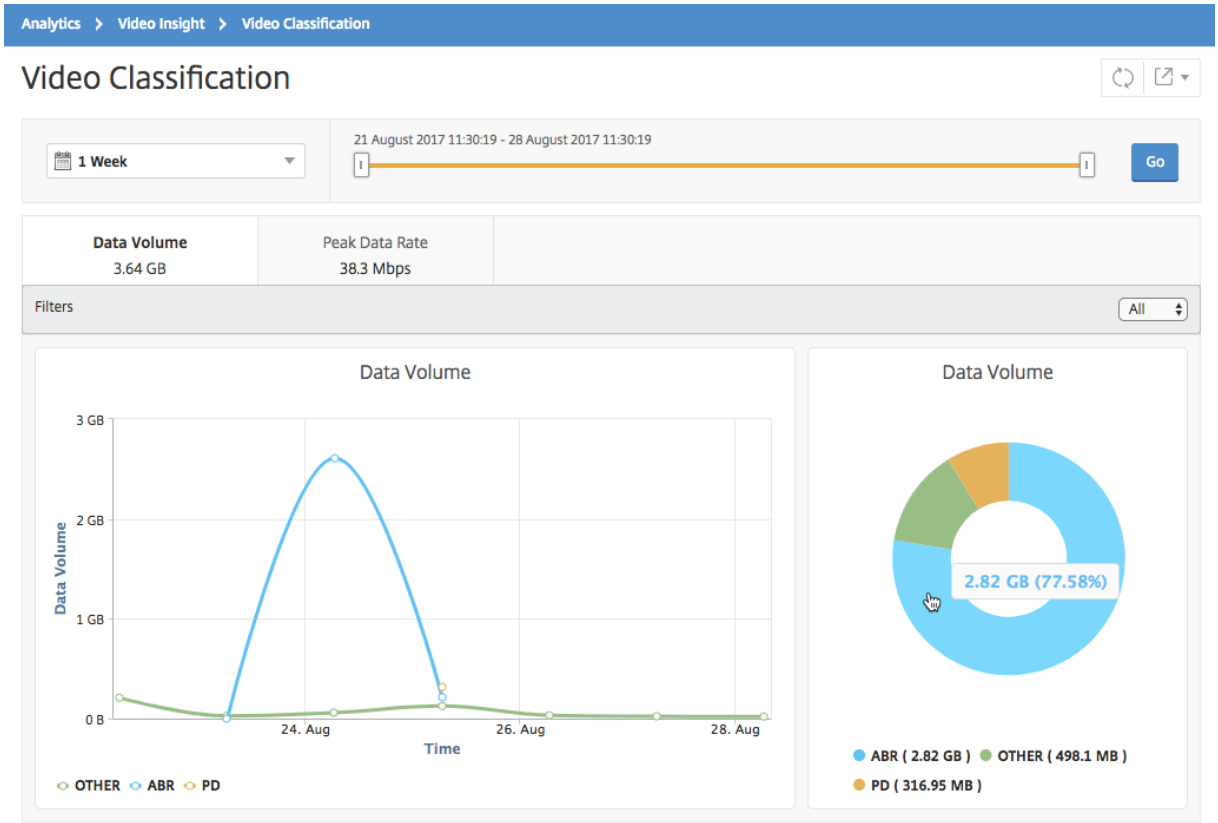
El dispositivo NetScaler ADC detecta el tráfico de vídeo cifrado o no cifrado de la red y el tipo de transmisión de vídeo (PD o ABR). NetScaler Application Delivery Management (ADM) muestra estas métricas y el volumen de datos consumido por el tráfico de vídeo durante un período de tiempo definido.

Para ver los tipos de vídeos y el volumen de datos consumido:

1. Vaya a **Analytics > Video Insight** y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir**.

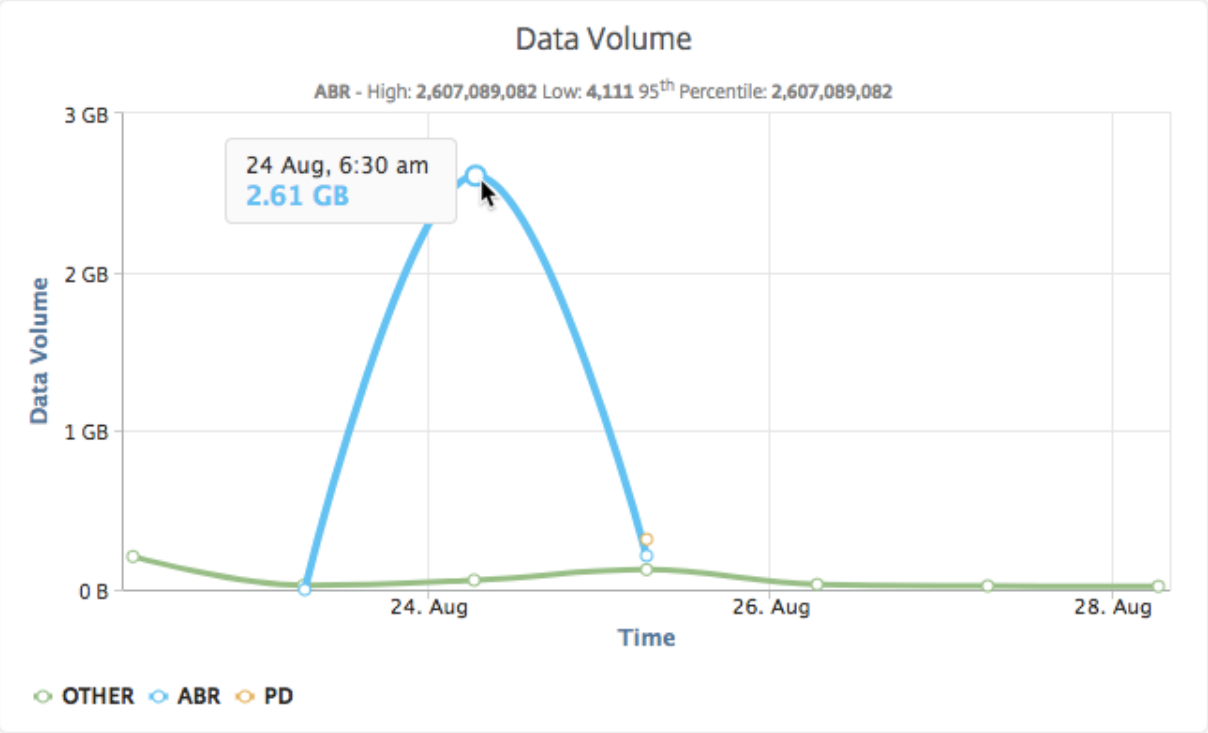
Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



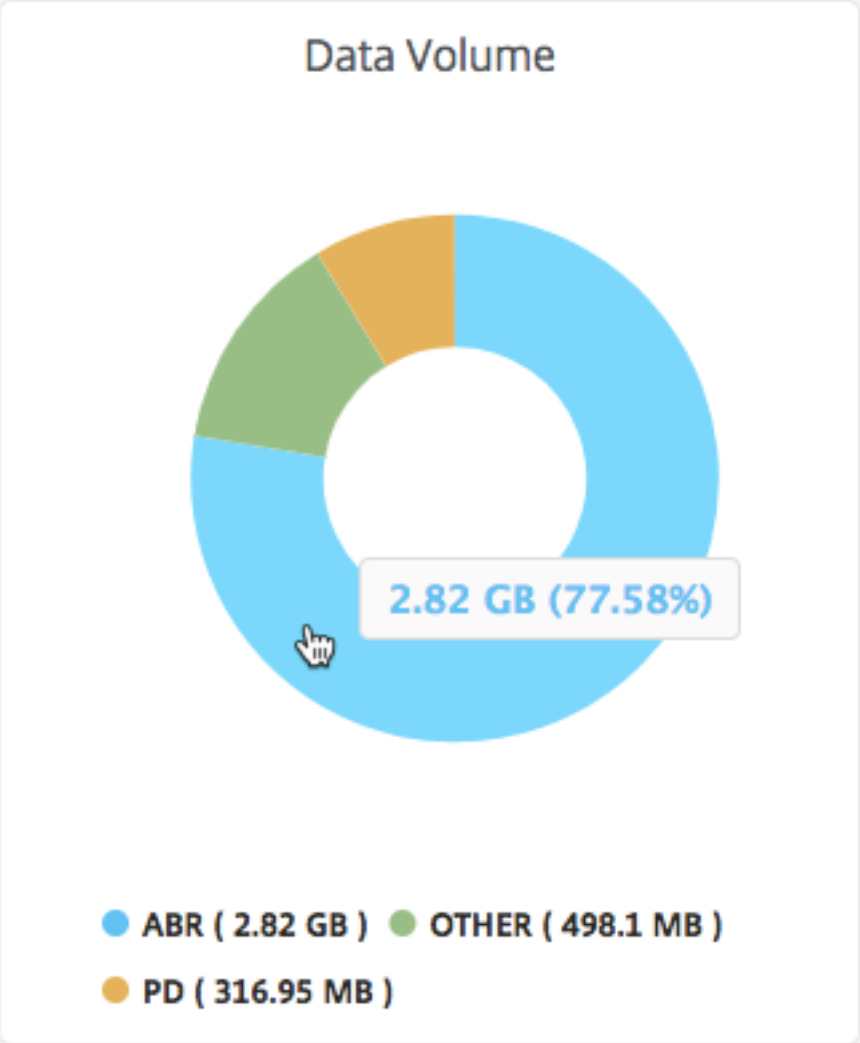

La ficha **Volumen de datos** proporciona un gráfico de líneas y un gráfico circular que muestra los tipos de transmisión de tráfico de vídeo desde la red y el volumen de datos consumido por la red. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver los datos consumidos durante un período de tiempo determinado:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Además, puede colocar el puntero del mouse sobre el gráfico circular para ver el porcentaje de volumen de datos consumido por un tipo determinado de tráfico de vídeo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Compare el tiempo de reproducción optimizado y no optimizado de los vídeos ABR

January 30, 2024

Durante un período determinado, Citrix Application Delivery Management (ADM) proporciona el tiempo de reproducción de los vídeos ABR y también le permite comparar el tiempo de reproducción de los vídeos ABR optimizados y no optimizados de la red.

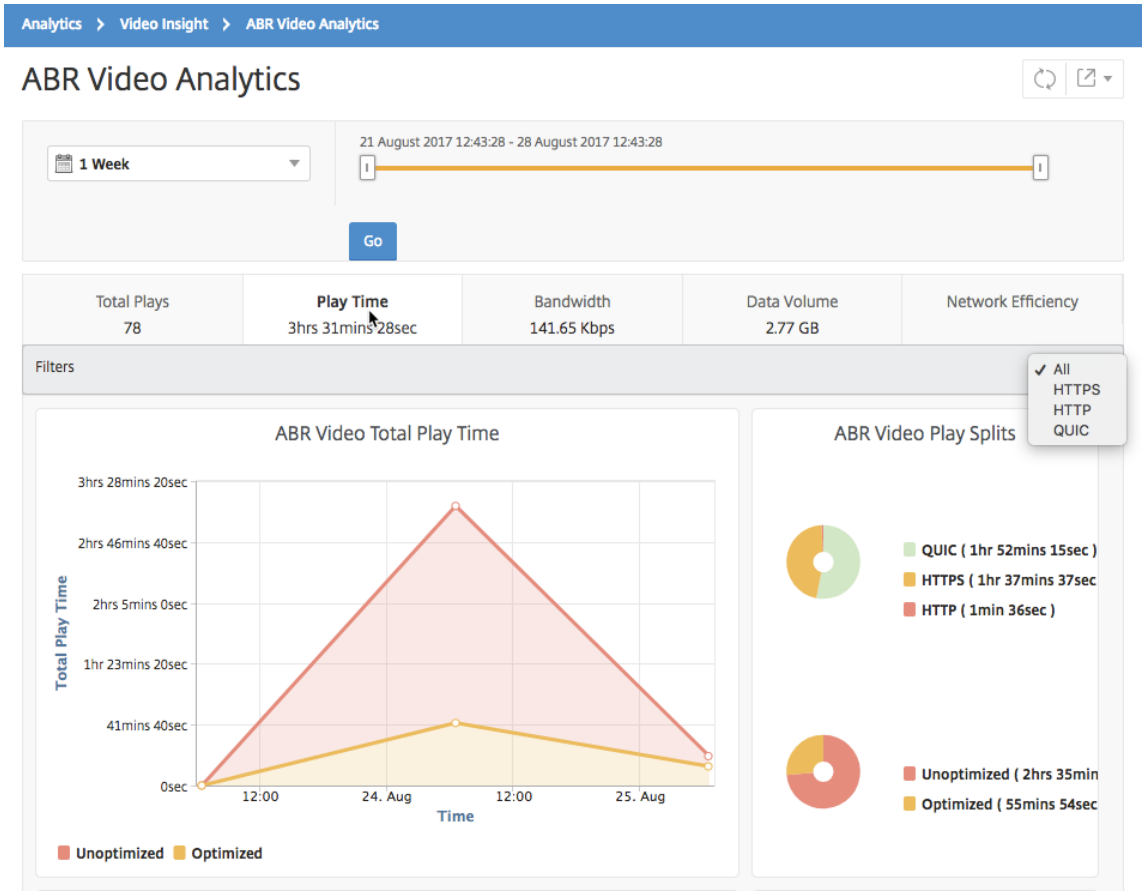
Para ver el tiempo de juego:

1. Vaya a **Analytics > Video Insight** y haga clic en **ABR Video.**
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Haga clic en **Ir** y seleccione la ficha **Tiempo de reproducción**.

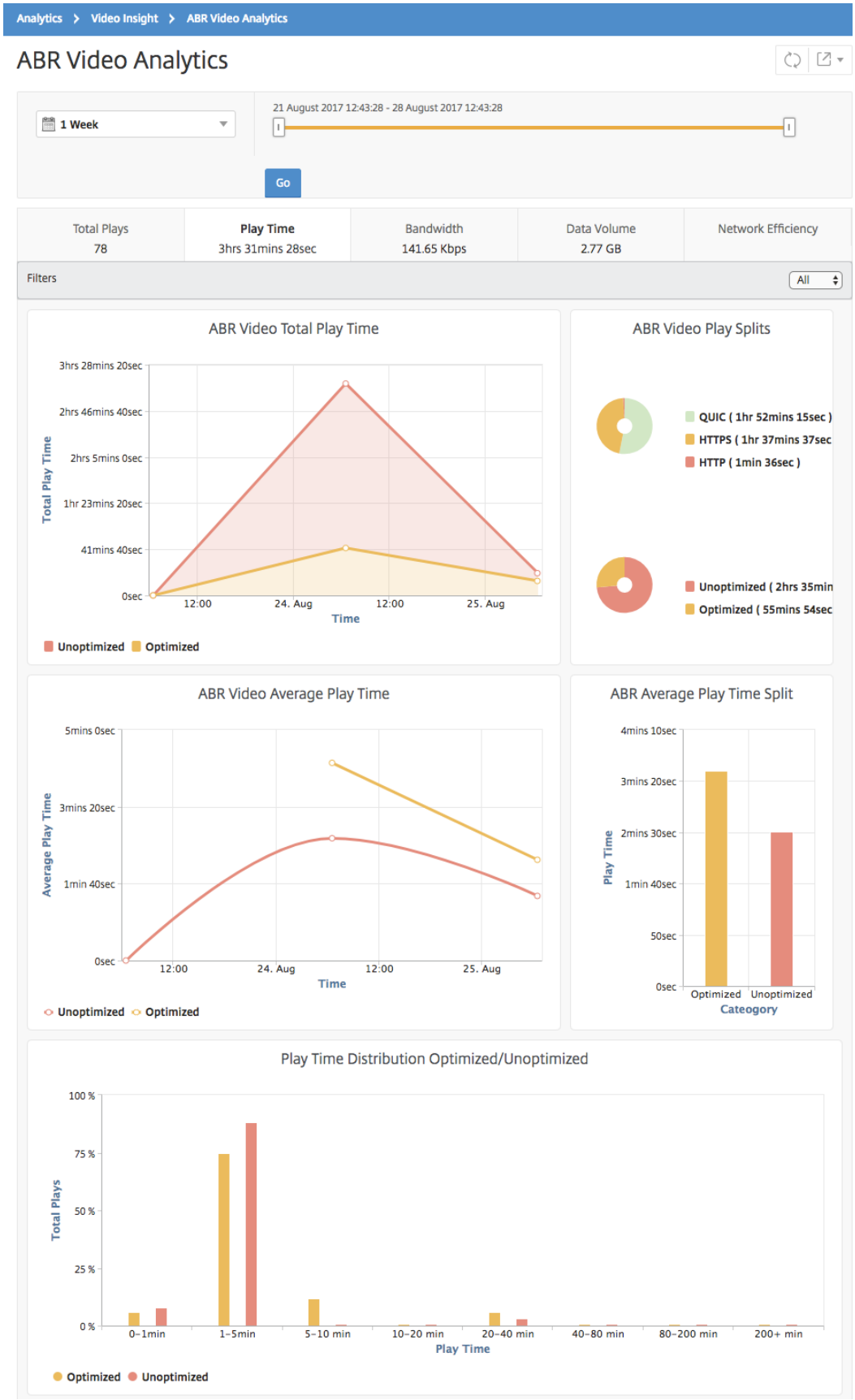
   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.




Para el marco de tiempo seleccionado, la ficha **Tiempo de reproducción** proporciona un gráfico de líneas y un gráfico circular que describe:

- Tiempo total de reproducción de los vídeos ABR de su red
- Tiempo total de reproducción de las reproducciones optimizadas y no optimizadas de vídeos ABR de su red durante el período de tiempo seleccionado
- Tiempo total de reproducción de vídeos ABR cifrados y no cifrados
- Tiempo medio de reproducción de los vídeos ABR
- Tiempo de reproducción promedio de reproducciones optimizadas y no optimizadas de vídeos ABR
- Tiempo medio de reproducción de vídeos ABR cifrados y no cifrados
- Distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Compare el consumo de ancho de banda de vídeos ABR optimizados y no optimizados

January 30, 2024

Durante un período de tiempo determinado, NetScaler Application Delivery Management (ADM) proporciona el ancho de banda que consumen los vídeos ABR optimizados y no optimizados, y también le permite comparar el ancho de banda consumido por los vídeos ABR optimizados y no optimizados en su red en función de:

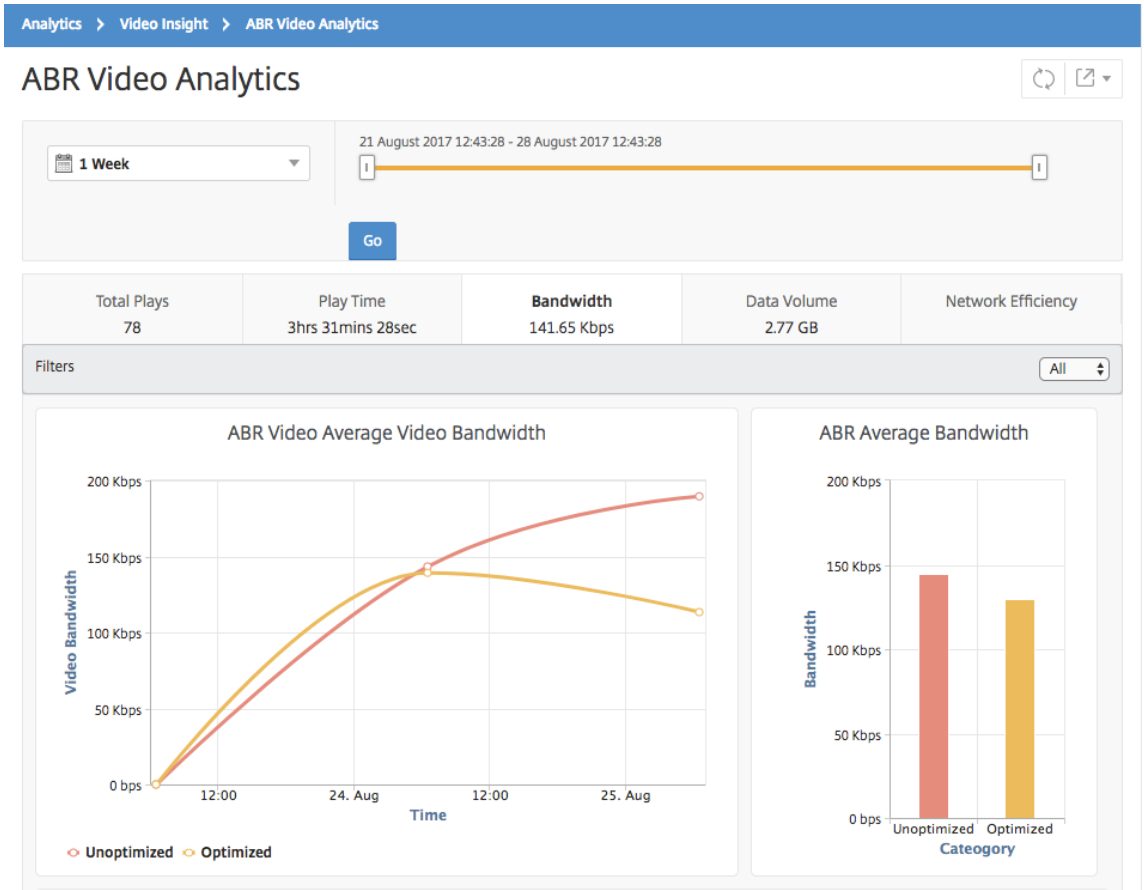
- Tiempo de reproducción
- Volumen de datos

Para ver el consumo de ancho de banda:

1. Vaya a **Analytics > Video Insight** y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Ancho de banda**.

   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.

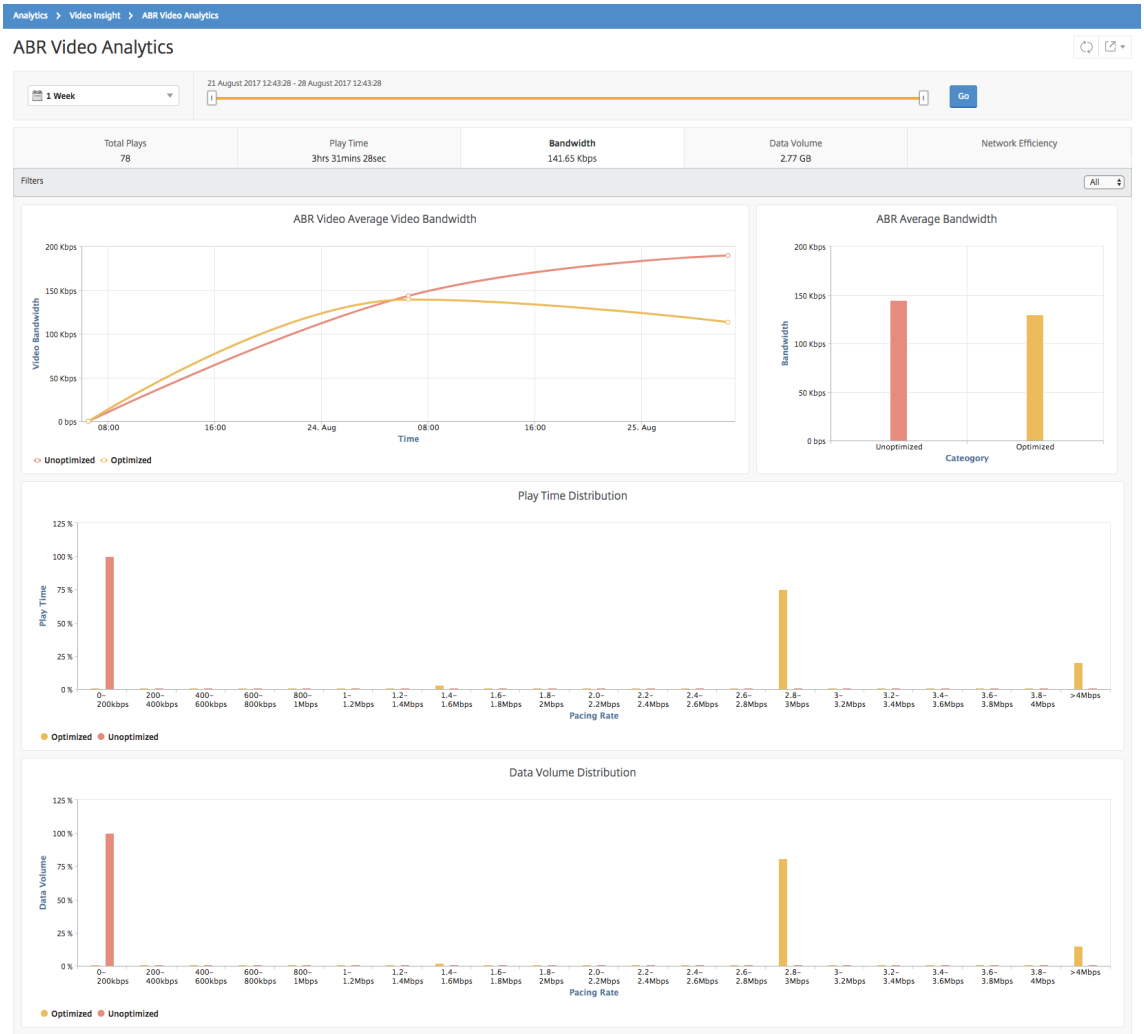
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Para el período de tiempo seleccionado, la ficha **Ancho de banda** proporciona un gráfico de líneas y un gráfico circular que describe:

- Ancho de banda promedio consumido por los vídeos ABR optimizados y no optimizados.
- El ancho de banda consumido depende de la distribución del tiempo de reproducción entre vídeos ABR optimizados y no optimizados.
- Ancho de banda consumido en función del volumen de datos distribuido entre los vídeos ABR optimizados y no optimizados.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Compare el número optimizado y no optimizado de reproducciones de videos ABR

January 30, 2024

Para un período de tiempo determinado, NetScaler Application Delivery Management (ADM) muestra el número de reproducciones de vídeos ABR y permite comparar el número de reproducciones optimizadas y no optimizadas de la red.

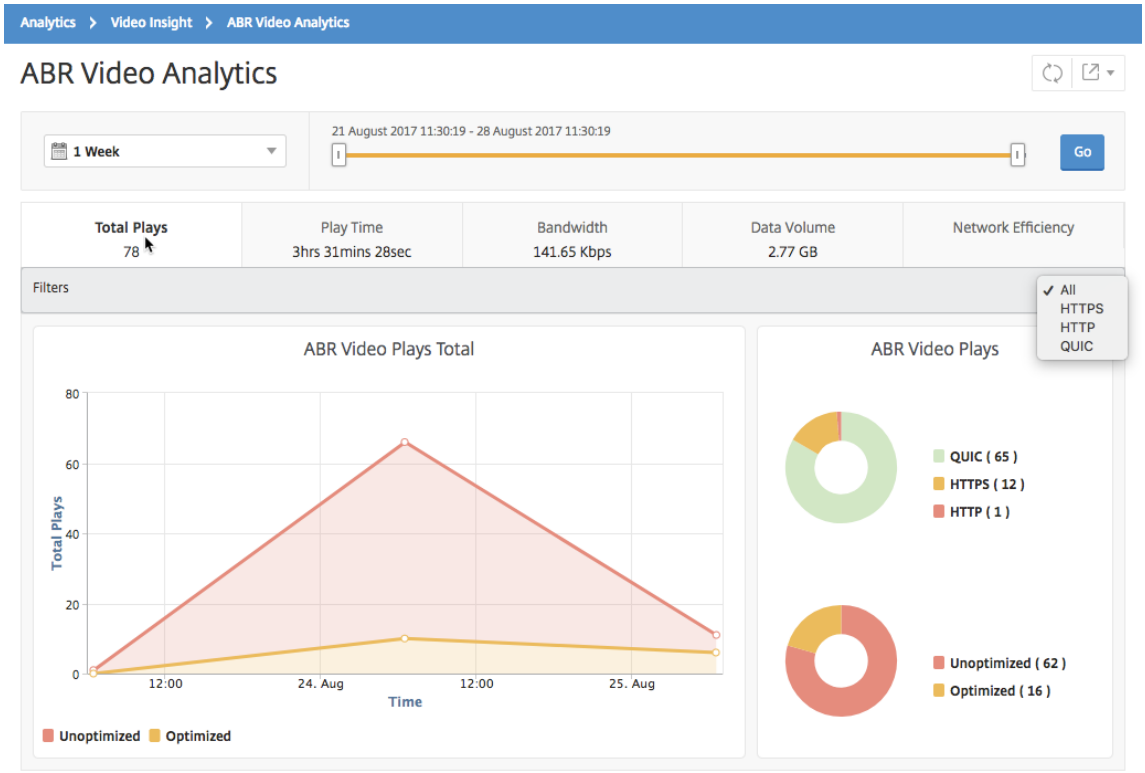
Para ver el número de jugadas:

1. Vaya a **Analytics > Video Insight**y haga clic en **ABR Video Analytics**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

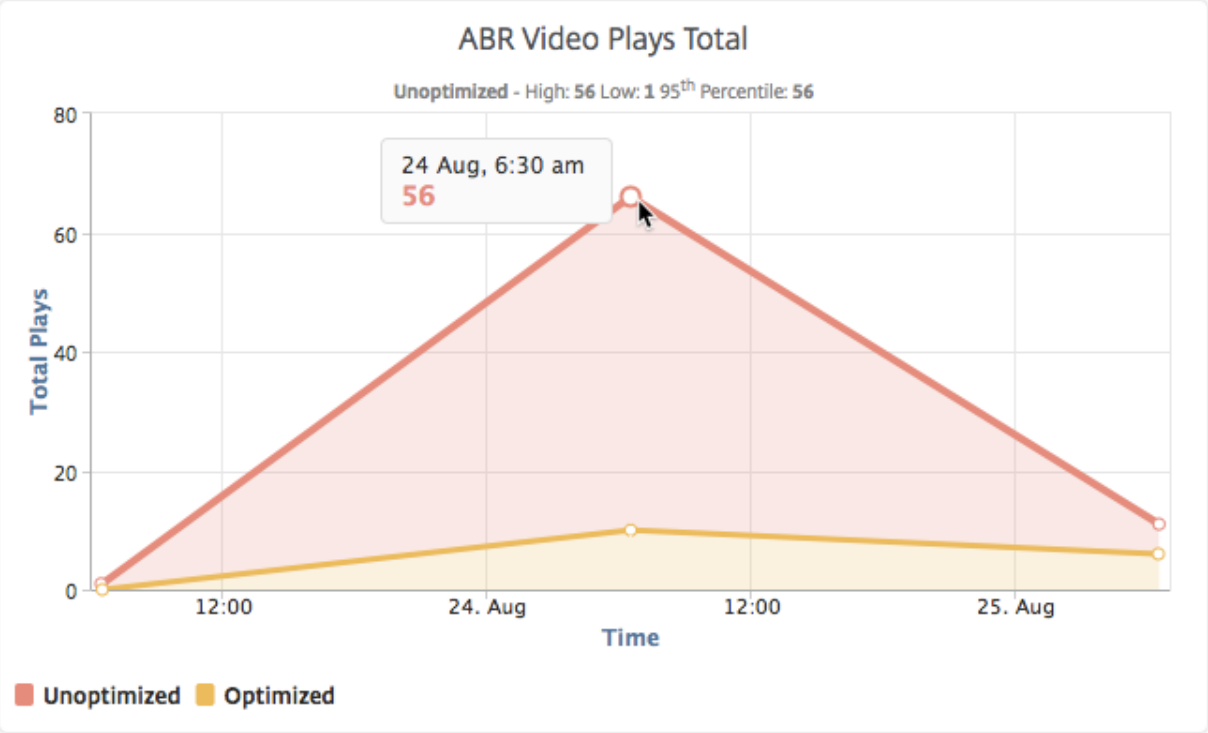
3. Haga clic en **Ir** y seleccione la ficha **N.º de reproducciones**.

   Puede utilizar la lista **Filtros** para seleccionar los vídeos HTTP, HTTPS o ABR QUIC.



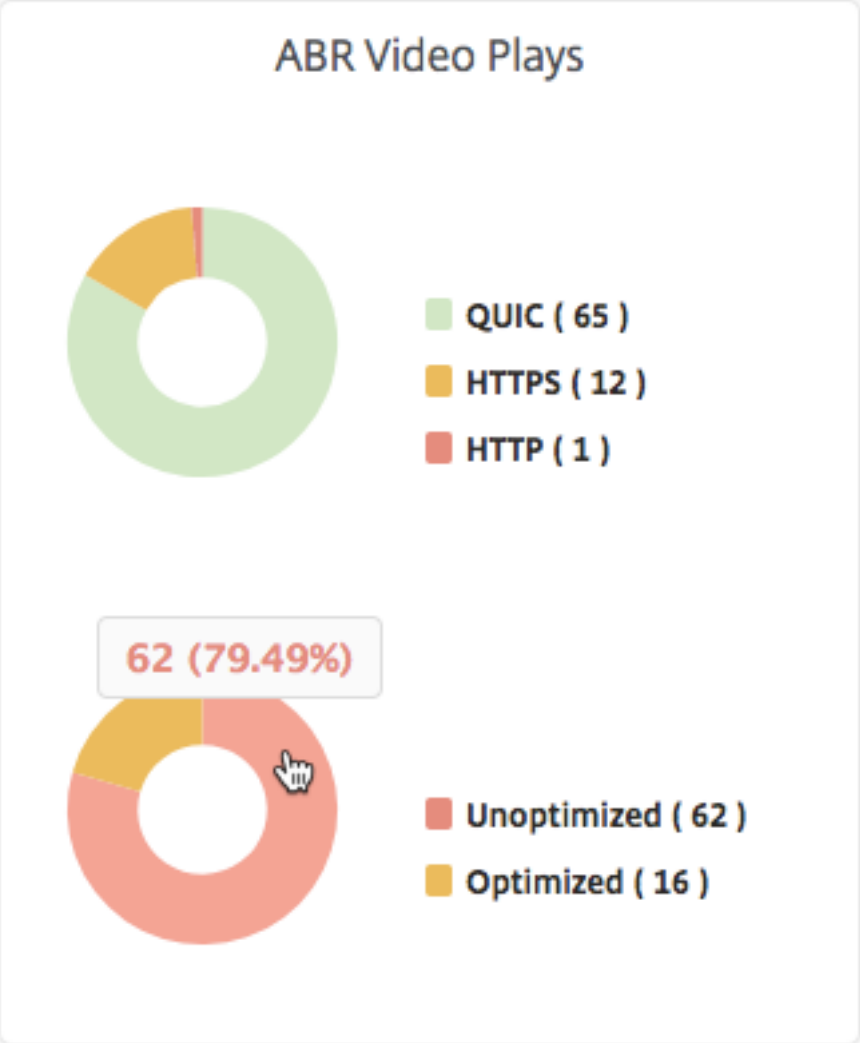

La ficha **N.º de reproducciones** proporciona un gráfico de líneas y un gráfico circular que describe el número de reproducciones de vídeos ABR de la red y el número de reproducciones optimizadas y no optimizadas de vídeos ABR de la red para el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para ver el número de reproducciones durante un período de tiempo determinado:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de reproducciones optimizadas y no optimizadas y el porcentaje de vídeos ABR cifrados y no cifrados para el período de tiempo seleccionado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Ver la velocidad máxima de datos para un período de tiempo específico

January 30, 2024

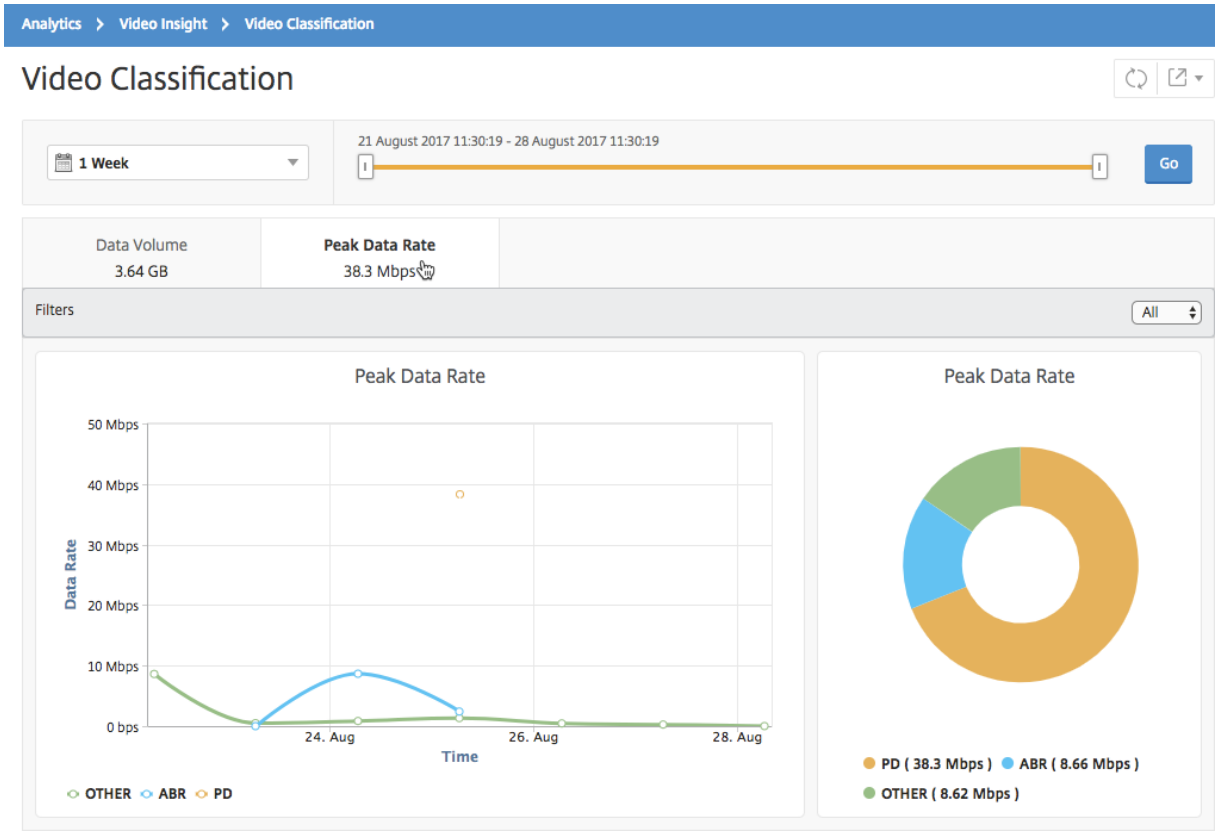
NetScaler Application Delivery Management (ADM) muestra el rendimiento máximo o la velocidad de datos del tráfico de vídeo de la red.

Para ver la velocidad máxima de datos del tráfico de vídeo:

1. Vaya a **Analytics > Video Insight**y haga clic en **Clasificación de vídeos**.
2. En el panel derecho, seleccione un período de tiempo de la lista. Puede personalizar aún más el marco de tiempo mediante el control deslizante de marco de tiempo.
3. Haga clic en **Ir** y seleccione la ficha **Tasa de datos máxima**.

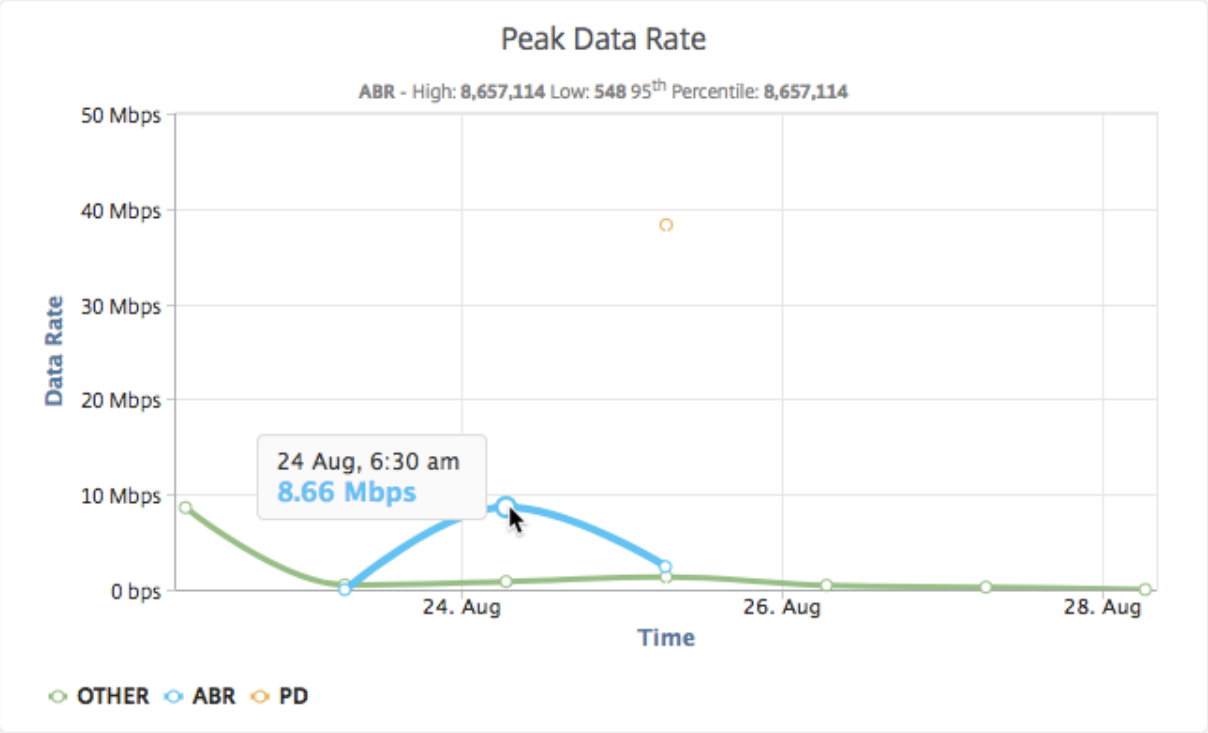
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede utilizar la lista **Filtros** para seleccionar el tráfico HTTP, HTTPS o QUIC.



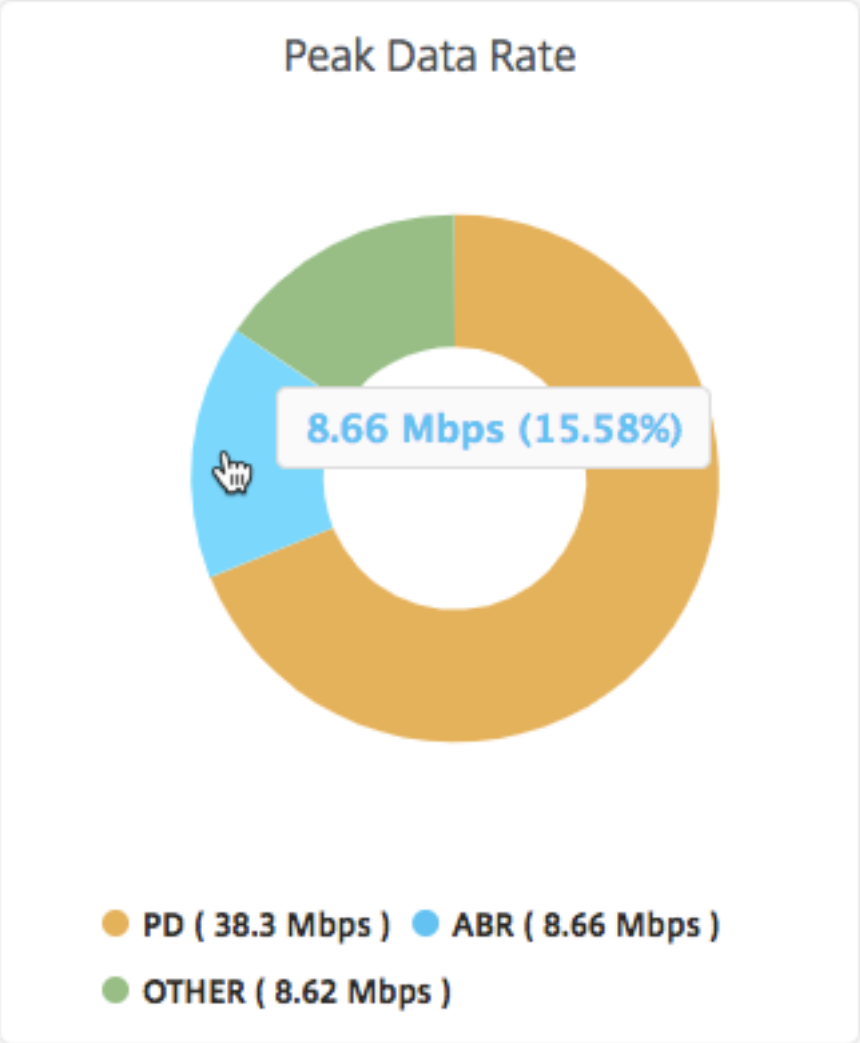

La ficha **Velocidad máxima de datos** proporciona un gráfico de líneas y un gráfico circular que describe la velocidad máxima de datos del tipo de transmisión de tráfico de vídeo desde la red y la velocidad máxima de datos del tráfico de vídeo en la red durante el período de tiempo seleccionado. Puede colocar el puntero del mouse sobre el gráfico de líneas para mostrar la velocidad máxima de datos durante un período de tiempo determinado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Además, puede colocar el puntero del mouse sobre el gráfico circular para mostrar el porcentaje de la velocidad máxima de datos consumida por el tipo de tráfico de vídeo transmitido durante el período de tiempo seleccionado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Análisis de proxy de reenvío SSL

January 30, 2024

Un dispositivo NetScaler ADC ubicado en el extremo de la red empresarial actúa como un proxy de Internet. El dispositivo puede funcionar en modo proxy transparente o modo proxy explícito y ofrece controles para interceptar el tráfico de Internet, incluido HTTPS. La decisión de interceptar, omitir o bloquear cualquier solicitud se toma en función de las directivas configuradas en el dispositivo. Un usuario se autentica antes de iniciar sesión en la red empresarial. Todas las solicitudes y respuestas se etiquetan al usuario y las actividades del usuario se registran en el dispositivo. Para obtener más información, consulte Citrix SSL Forward Proxy.

Al integrar NetScaler Application Delivery Management (ADM) con un dispositivo NetScaler ADC, la actividad de usuario registrada y los registros posteriores en el dispositivo se exportan a NetScaler

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ADM mediante logstream. NetScaler ADM recopila y presenta información sobre las actividades de los usuarios, como los sitios web visitados y el ancho de banda gastado. También informa sobre el uso del ancho de banda y las amenazas detectadas, como malware y sitios de phishing. Puede utilizar estas métricas clave para supervisar su red y tomar medidas correctivas con el dispositivo NetScaler ADC.

**Para integrar un dispositivo NetScaler ADC con NetScaler ADM:**

1. En el dispositivo NetScaler ADC, al configurar el proxy de reenvío SSL, habilite **Analytics** y proporcione los detalles de la instancia de NetScaler ADM que quiere utilizar para el análisis.
2. En NetScaler ADM, agregue el dispositivo NetScaler ADC como instancia a NetScaler ADM. Para obtener más información, consulte Agregar instancias a NetScaler ADM.

## Paneles

January 30, 2024

NetScaler Application Delivery Management (ADM) proporciona dos paneles, el Panel de **tráfico saliente y el Panel** de **usuario**. Estos paneles muestran varios gráficos que resumen los sitios web o las aplicaciones a las que se accede desde la red empresarial, así como las actividades realizadas por los usuarios de la red.

### Panel de tráfico saliente

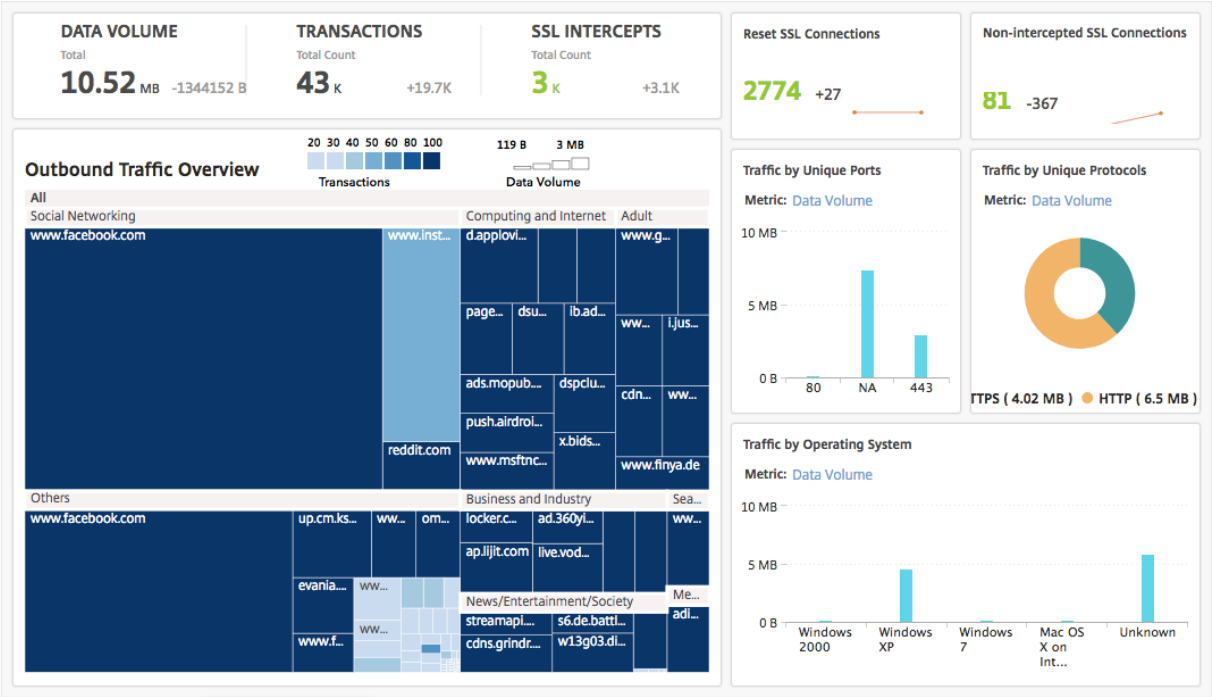
El **Panel de control de tráfico saliente** proporciona un resumen de las direcciones URL o dominios a los que se accede desde la red. Proporciona una visión holística de todas las URL o dominios por número de transacciones o volumen de datos consumido por las URL o dominios.
También proporciona detalles como los siguientes:

1. Cantidad de ancho de banda que consumen las URL o los dominios a los que se accede desde la red.
2. Número de transacciones que se produjeron al acceder a las direcciones URL y dominios de la red.
3. Número de conexiones SSL interceptadas por el dispositivo NetScaler ADC durante las transacciones.
4. Número de conexiones SSL no interceptadas por el dispositivo NetScaler ADC durante las transacciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Número de conexiones SSL restablecidas por el dispositivo NetScaler ADC durante las transacciones.
6. Cantidad de tráfico web transmitido, basado en el puerto utilizado para transmitir el tráfico, el protocolo utilizado por el tráfico web y los sistemas operativos cliente utilizados para transmitir el tráfico.

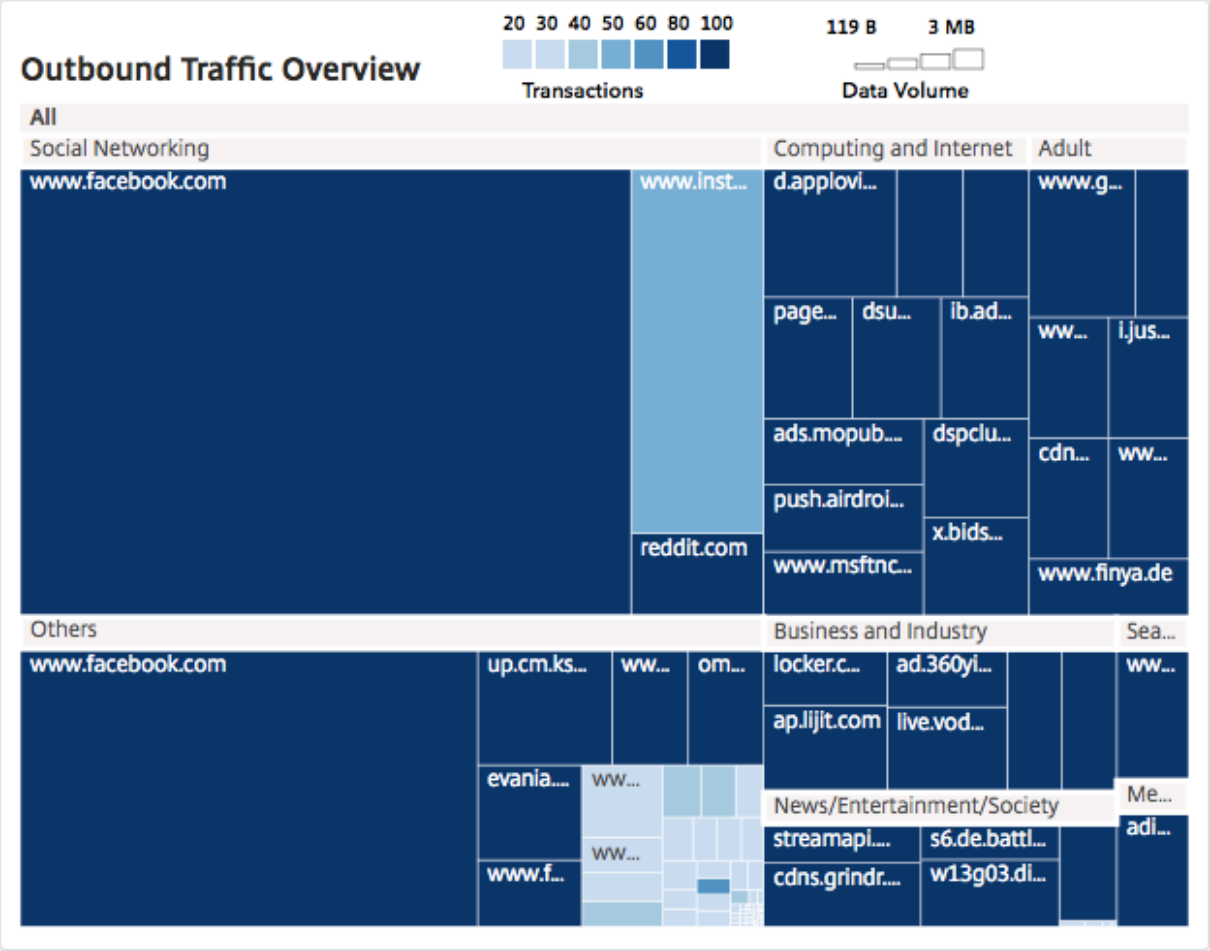
Para acceder al Panel de control de tráfico saliente, vaya a **Aplicaciones > Panel de control de tráfico saliente**.




### Ver el tráfico saliente de la red

El **Panel de control de tráfico salienteincluye un panel Información general del tráfico saliente**. En el panel**Descripción general del tráfico saliente**, NetScaler ADM agrupa las URL o dominios a los que se accede en categorías, como Compras, Noticias, Redes sociales, etc. El panel**Descripción general del tráfico saliente** muestra las URL o los dominios a los que se accede desde la red como nodos en las categorías de URL. El tamaño de los nodos se ajusta al volumen de datos consumido al acceder a la URL o al dominio. El color del nodo indica el número de transacciones que se produjeron al acceder a la dirección URL o dominio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Puede hacer clic en una categoría para filtrar los gráficos y mostrar los detalles relacionados con la categoría para el período de tiempo especificado.

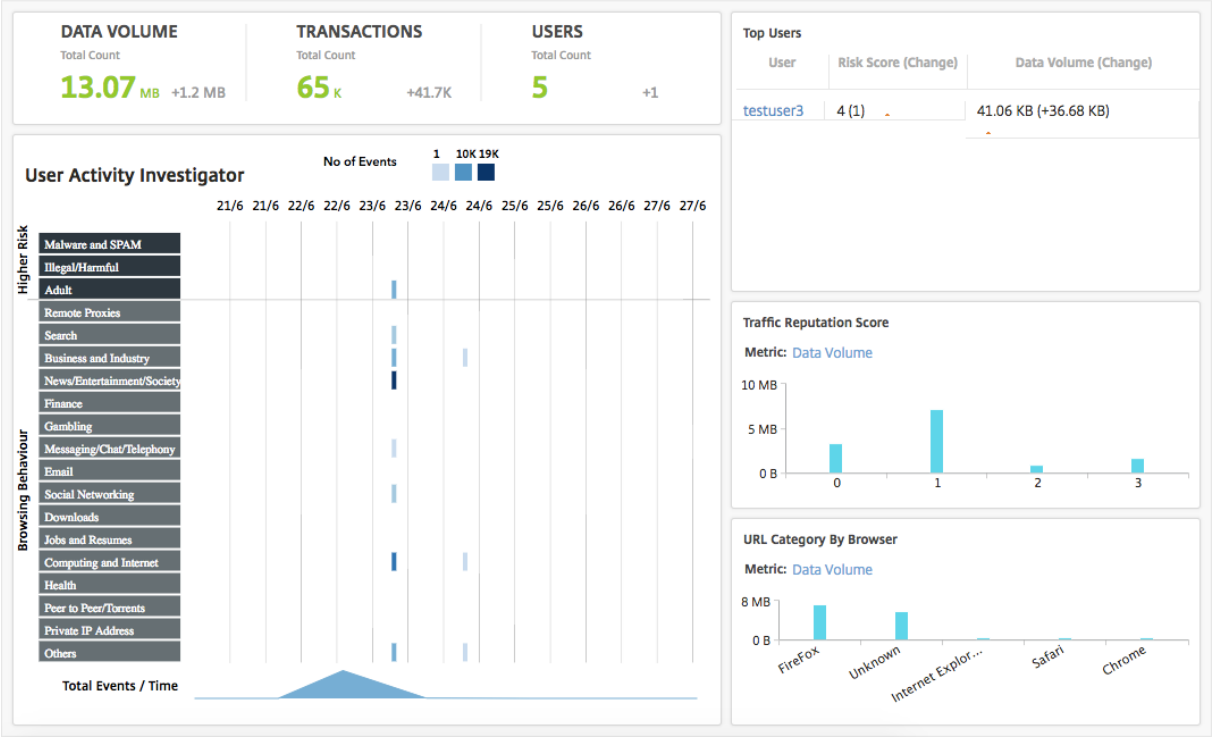
## Panel de control de usuario

El **Panel de control de usuario** muestra un resumen de las actividades realizadas por los usuarios de la empresa. Proporciona métricas clave que puede utilizar para determinar lo siguiente:

1. Comportamiento de navegación de los usuarios de su empresa.
2. Categorías de URL a las que acceden los usuarios de su empresa.
3. Los cinco usuarios principales, en función de sus puntuaciones de riesgo y del ancho de banda que consumen. Para obtener más información sobre la puntuación de riesgo, consulte Puntuación de riesgo.
4. Exploradores utilizados para acceder a las URL o dominios.
5. Cantidad del tráfico web generado por los usuarios, en función de la puntuación de la reputación del tráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para acceder al **Panel de control de usuarios**, vaya a **Usuarios > Panel de control**.



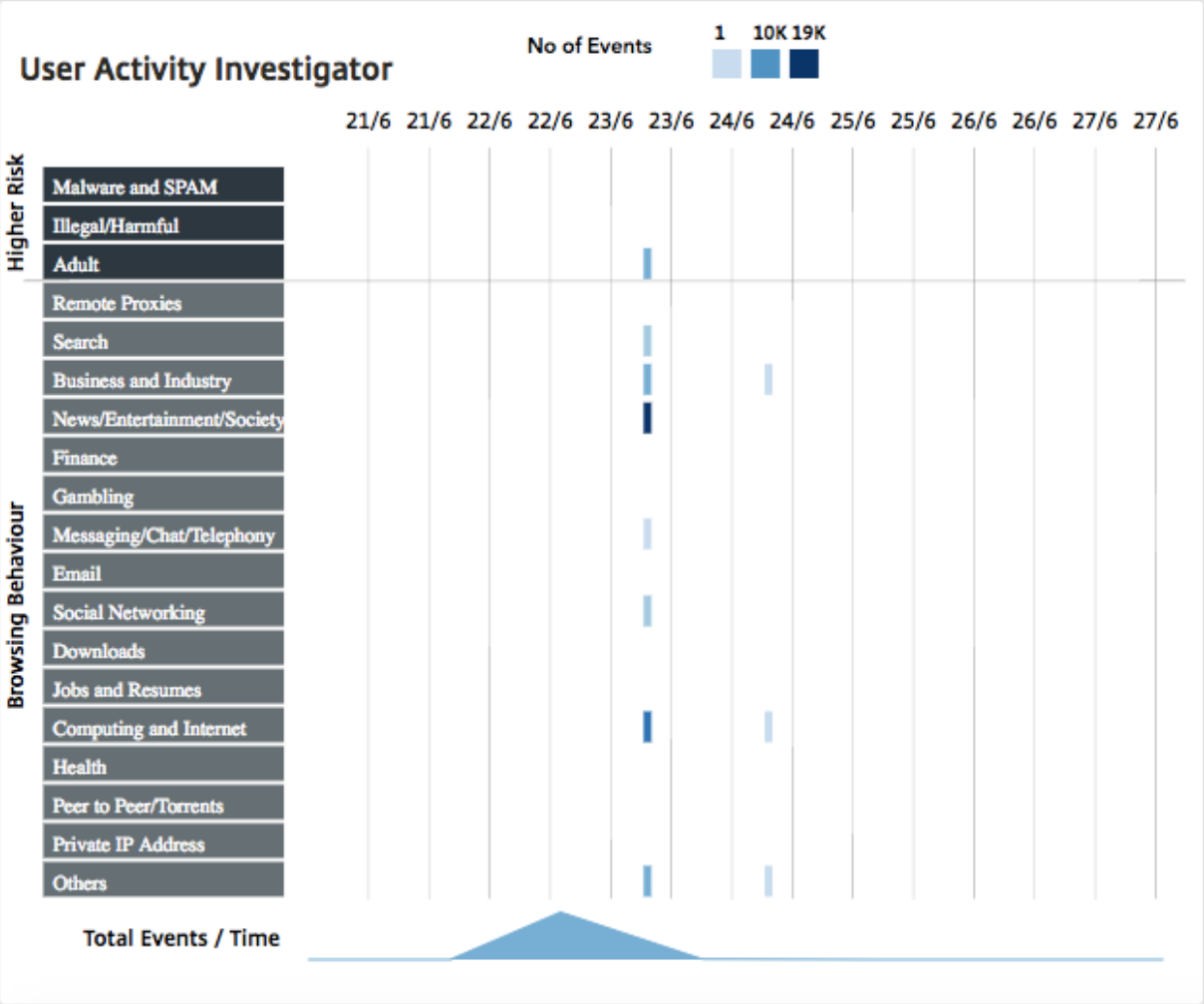

Puede hacer clic en un usuario en el panel **Usuarios principales** para filtrar los gráficos y mostrar detalles de la actividad web realizada por el usuario en el período de tiempo especificado.

### Investigador de actividad del usuario

El **Panel** de control de **usuario incluye un panel Investigador de actividad** de usuario que muestra diversas actividades web realizadas por los usuarios. Muestra las categorías de URL a las que acceden los usuarios durante el período de tiempo seleccionado, y varios eventos desencadenados por categoría de URL. Puede hacer clic en los eventos para obtener los detalles del nivel de transacción.

El **Investigador de actividad de usuario** muestra información clave, como el comportamiento de exploración del usuario, la actividad de alto riesgo del usuario y los eventos desencadenados, por categoría de URL. Los eventos se muestran como leyendas rectangulares en el gráfico. Cada una de las leyendas se agrega a intervalos de un minuto si la duración seleccionada es de una hora, y a intervalos de una hora si la duración seleccionada es de un día.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Estas leyendas se agregan y se codifican por colores según el número de eventos que se han producido. Puede colocar el puntero del mouse sobre una leyenda para mostrar detalles como la hora y el número de eventos agregados para la leyenda seleccionada. Puede personalizar el período de tiempo del gráfico seleccionando un tiempo de la lista de períodos de tiempo.

Puede hacer clic en los eventos para obtener más detalles de las transacciones.

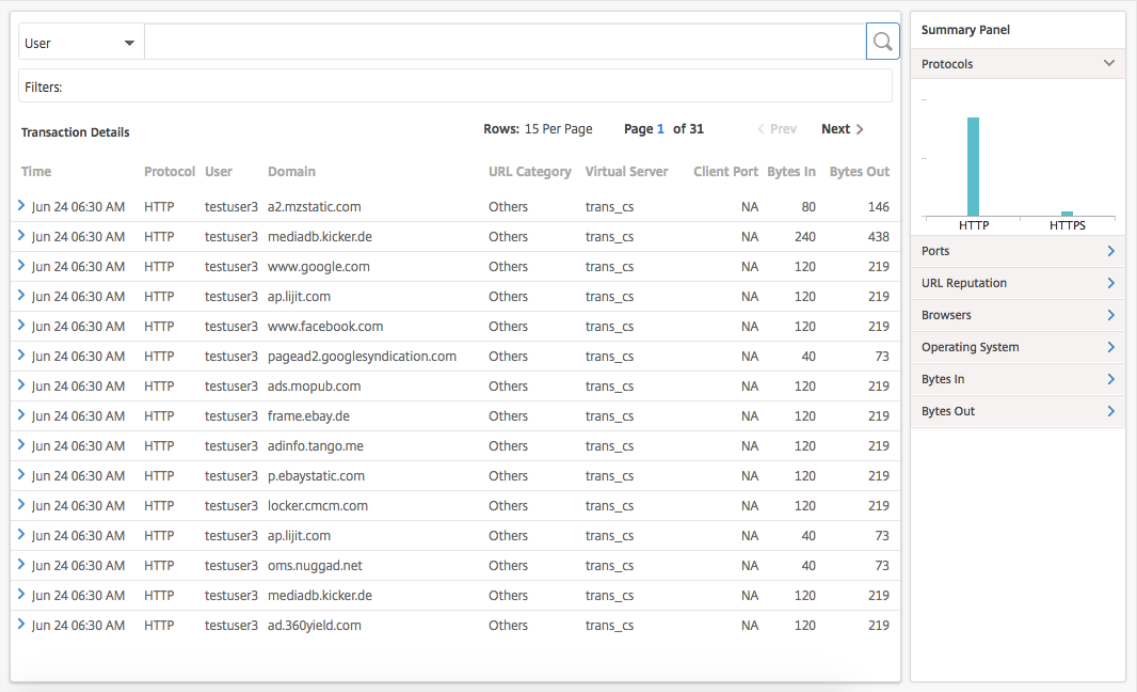
### Transacciones de usuario

La página Transacciones de Usuario muestra los detalles de las transacciones de usuario de la red. Proporciona detalles a nivel de transacción, como:

1. Hora en la que se produjo la transacción
2. Protocolo utilizado para la transacción
3. Nombre de usuario
4. Dominio al que accede el usuario

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Categoría de URL
6. Servidor proxy utilizado para interceptar la transacción
7. Detalles del puerto del cliente
8. Bytes en
9. Bytes de salida




**Panel Resumen** El **panel de resumen** muestra todas las métricas de las transacciones que están visibles en el panel **Detalles de la transacción**. Este panel le permite ordenar y ver las transacciones en el panel **Detalles de la transacción** seleccionando o deseleccionando las métricas. El **panel de resumen** muestra las siguientes métricas:

| Métricas | Descripción |
|---|---|
| Protocolos | Protocolos utilizados en las transacciones |
| Puertos | Puertos utilizados para las transacciones |
| Reputación URL | Puntuación de reputación de URL |
| Exploradores web | Exploradores utilizados para las transacciones |
| Sistema de operación | Sistema operativo utilizado para las transacciones |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Métricas | Descripción |
| --- | --- |
| Bytes en | Cantidad de datos recibidos a través del dispositivo Citrix ADC. |
| Bytes de salida | Cantidad de datos enviados a través del dispositivo Citrix ADC. |

**Puntuación de riesgo**

Risk Score es un sistema de puntuación utilizado en NetScaler ADM para determinar los riesgos asociados con los usuarios de su empresa. NetScaler ADM asigna una puntuación de riesgo basada en la puntuación de reputación de URL asignada por el dispositivo NetScaler ADC para las direcciones URL a las que acceden los usuarios de la red. Para obtener información sobre la puntuación de reputación de URL, consulte Puntuación de reputaciónde URL. En la siguiente tabla se describen las puntuaciones de riesgo asignadas por NetScaler ADM.

| Puntuación de riesgo | Descripción |
| --- | --- |
| 1 | La actividad web del usuario no se percibe como una amenaza o no es anormal. |
| 2 | La actividad web del usuario no se percibe como una amenaza o no es anormal, pero el usuario accede a “sitios desconocidos”, que no tienen puntuaciones de reputación en las URL. |
| 3 | No se detecta ninguna amenaza en la actividad web del usuario, pero este ha intentado acceder a sitios que son potencialmente vulnerables o están afiliados a sitios que son potencialmente vulnerables. |
| 4 | Usuario potencialmente comprometido. |
| 5 | La actividad web del usuario es anormal y el usuario ha accedido a sitios maliciosos conocidos. |

## Casos de uso

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Supervisión de las intercepciones SSL

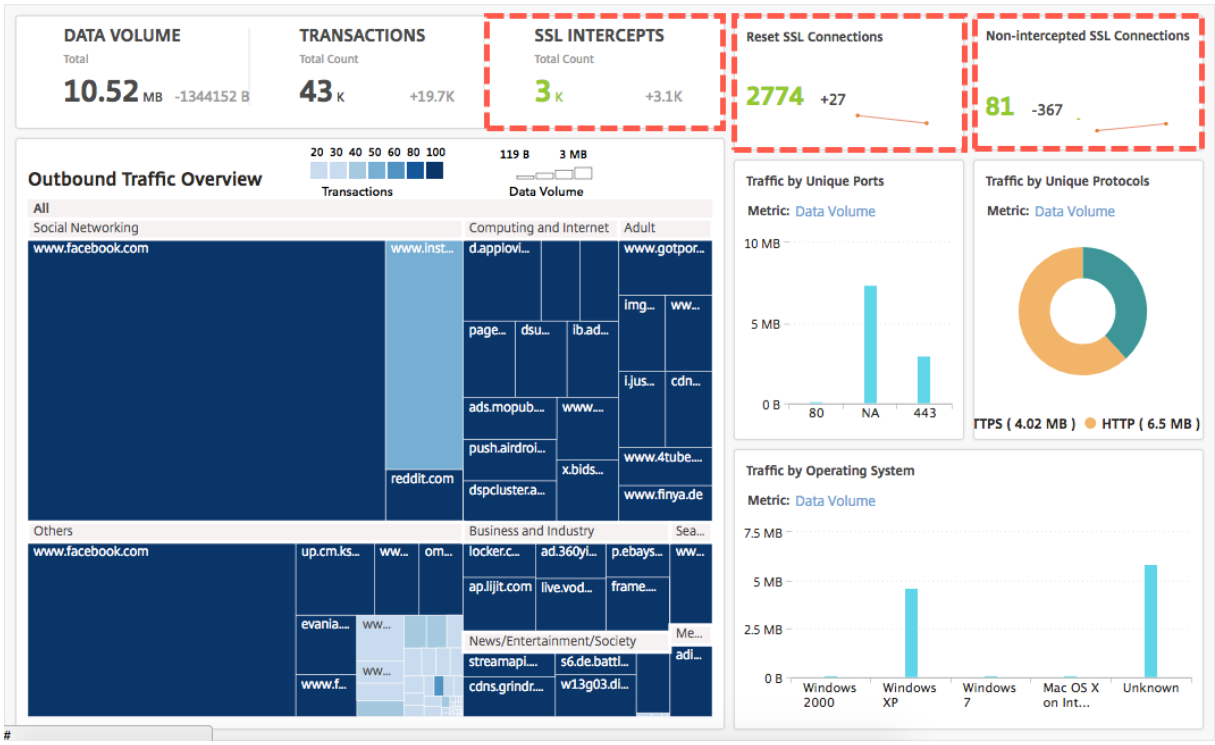
Un dispositivo NetScaler ADC le permite inspeccionar el tráfico saliente cifrado. Puede interceptar, omitir o bloquear cualquier solicitud HTTPS según las directivas configuradas en el dispositivo. NetScaler Application Delivery Management (ADM) proporciona los siguientes detalles acerca de las conexiones SSL en el **Panel de control de tráfico saliente** para un período de tiempo seleccionado:

- Número de conexiones SSL interceptadas, no interceptadas y restablecidas por el dispositivo NetScaler ADC
- Detalles de transacción de las conexiones SSL

Con estos detalles, puede ajustar aún más las directivas del dispositivo NetScaler ADC para inspeccionar de manera eficiente el tráfico saliente cifrado. Para obtener más información, consulte Citrix SSL Forward Proxy.

**Para mostrar el número de conexiones SSL que se han interceptado, no interceptado y restablecer:**

Vaya a **Aplicaciones > Panel de control de tráfico saliente**.El Panel de control de tráfico fuera de borda muestra el número de conexiones SSL interceptadas, no interceptadas y restablecidas.

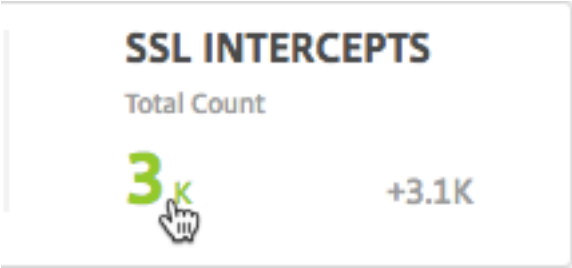



**Para mostrar los detalles de transacción de las conexiones SSL que se han interceptado:**

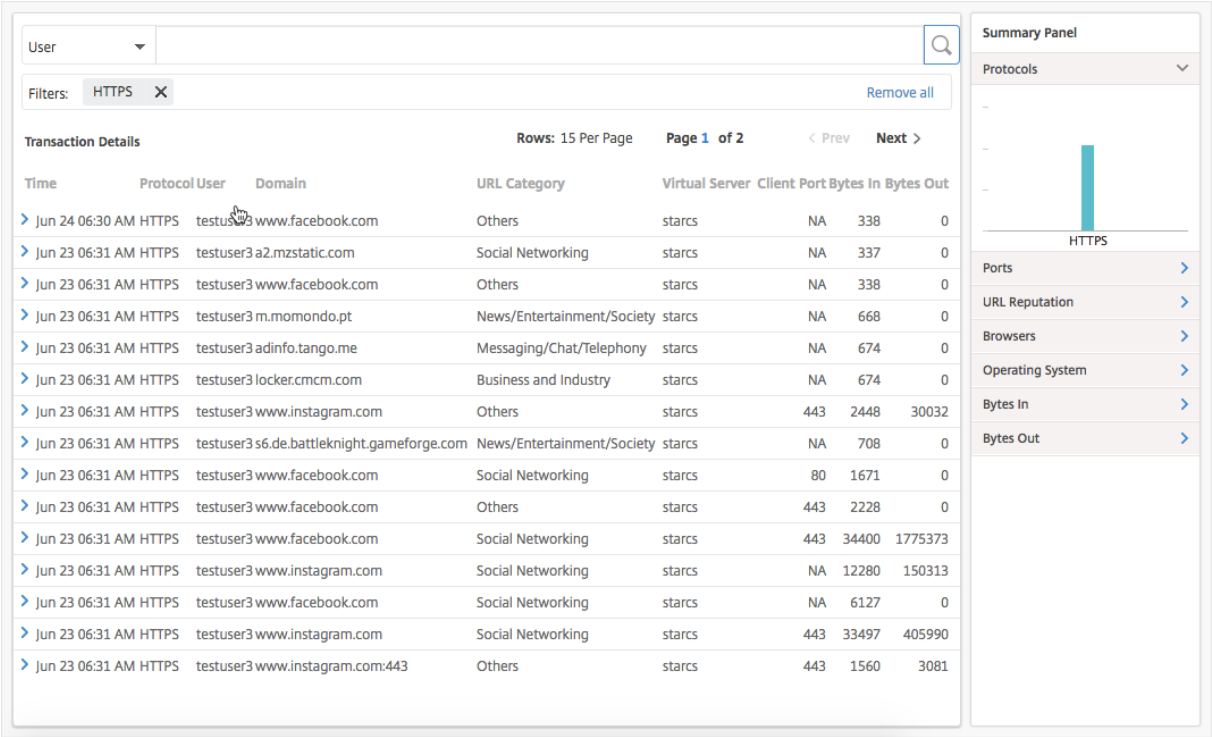
1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En el **panel de control de tráfico fuera**de borda, haga clic en el recuento total en la sección **SSL INTERCEPTS**.




Los detalles de transacción de las conexiones SSL interceptadas durante el período de tiempo seleccionado se muestran en la página **Detalles de Transacción**.



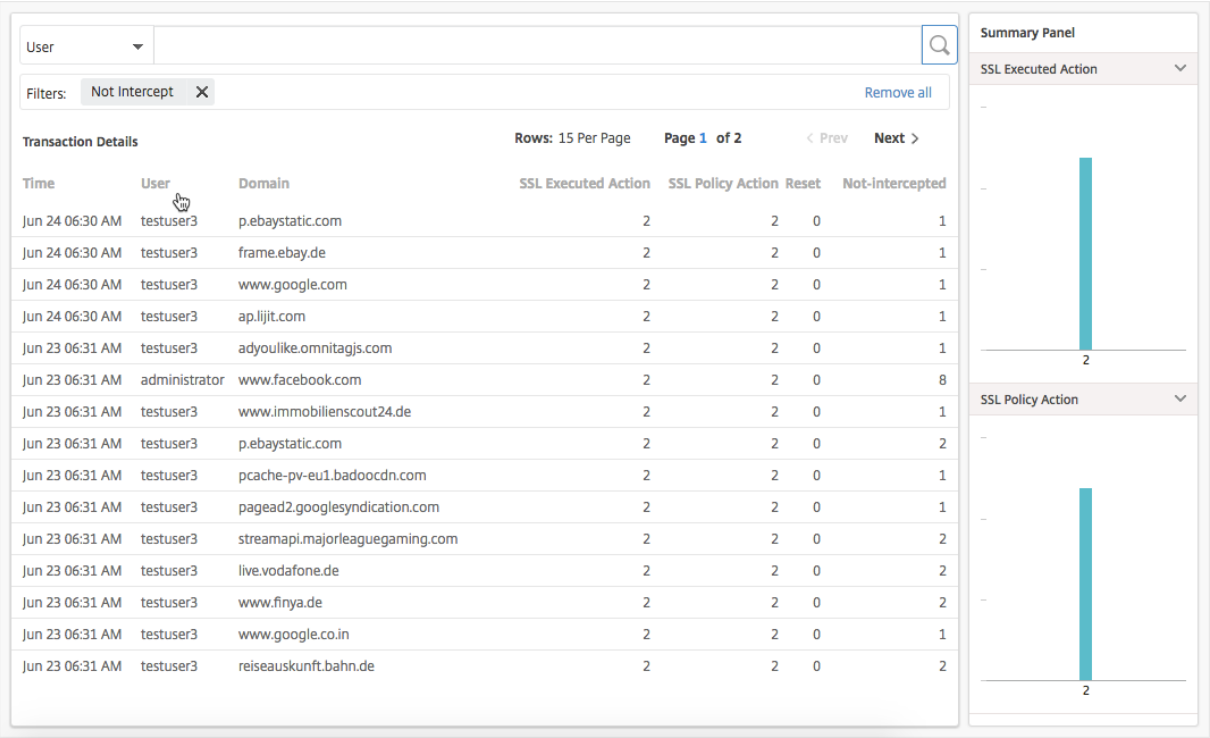

Puede filtrar aún más los detalles de las transacciones por usuario y categoría de URL.

**Para ver los detalles de las transacciones de las conexiones SSL en las que no se interceptó el tráfico:**

1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.
2. En el **Panel de control de tráfico fuera**de borda, haga clic en el recuento total de la sección **Conexiones SSL no interceptadas**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Los detalles de transacción de las conexiones SSL en las que no se interceptó tráfico durante el período de tiempo seleccionado aparecen en la página **Detalles de Transacción**.



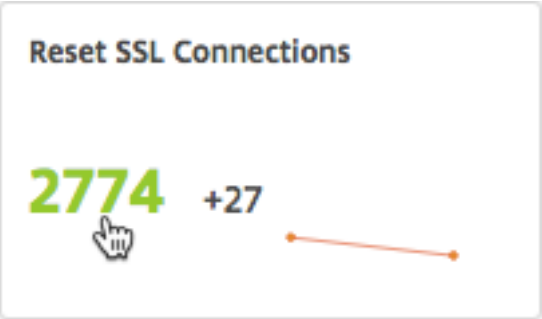

| Time | User | Domain | SSL Executed Action | SSL Policy Action | Reset | Not-intercepted |
|---|---|---|---|---|---|---|
| Jun 24 06:30 AM | testuser3 | p.ebaystatic.com | 2 | 2 | 0 | 1 |
| Jun 24 06:30 AM | testuser3 | frame.ebay.de | 2 | 2 | 0 | 1 |
| Jun 24 06:30 AM | testuser3 | www.google.com | 2 | 2 | 0 | 1 |
| Jun 24 06:30 AM | testuser3 | ap.lijit.com | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | testuser3 | adyoulike.omnitagjs.com | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | administrator | www.facebook.com | 2 | 2 | 0 | 8 |
| Jun 23 06:31 AM | testuser3 | www.immobilienscout24.de | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | testuser3 | p.ebaystatic.com | 2 | 2 | 0 | 2 |
| Jun 23 06:31 AM | testuser3 | pcache-pv-eu1.badoocdn.com | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | testuser3 | pagead2.googlesyndication.com | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | testuser3 | streamapi.majorleaguegaming.com | 2 | 2 | 0 | 2 |
| Jun 23 06:31 AM | testuser3 | live.vodafone.de | 2 | 2 | 0 | 2 |
| Jun 23 06:31 AM | testuser3 | www.finya.de | 2 | 2 | 0 | 2 |
| Jun 23 06:31 AM | testuser3 | www.google.co.in | 2 | 2 | 0 | 1 |
| Jun 23 06:31 AM | testuser3 | reiseauskunft.bahn.de | 2 | 2 | 0 | 2 |

Puede filtrar aún más los detalles de las transacciones por usuario y categoría de URL.

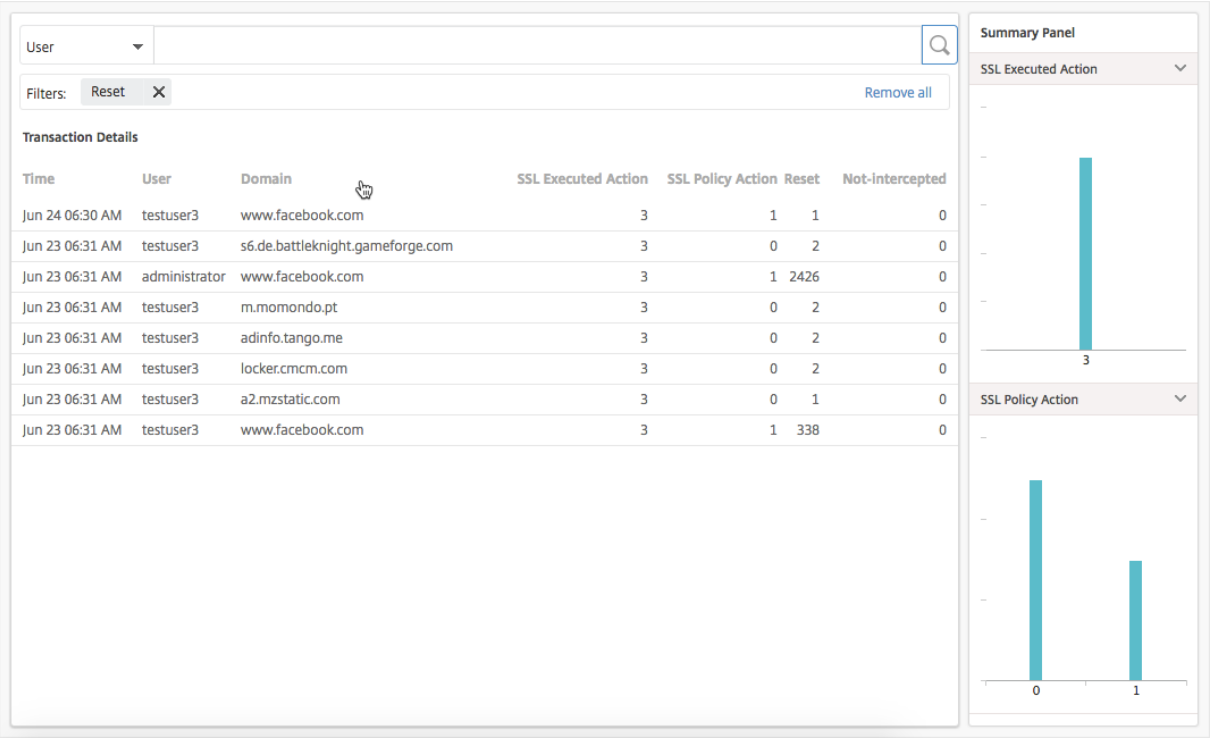
**Para mostrar los detalles de las transacciones de las conexiones SSL que se han restablecido:**

1. Vaya a **Aplicaciones > Panel de control de tráfico saliente**.
2. En el **Panel de control de tráfico fuera**de borda, haga clic en el recuento total en la sección **Restablecer conexiones SSL**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Los detalles de la transacción de las conexiones SSL en las que no se interceptó tráfico durante el período de tiempo seleccionado aparecen en la página **Detalles de la transacción**.




Puede filtrar aún más los detalles de las transacciones por la categoría de usuario y URL.

## Inspección de puntos finales

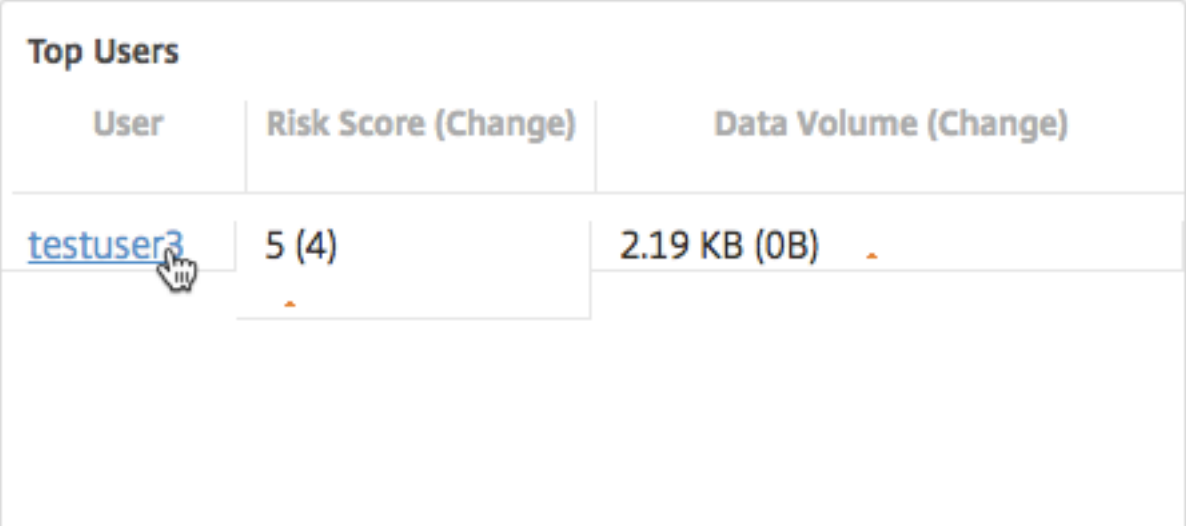
Las directivas que ha configurado en un dispositivo NetScaler ADC especifican cómo el dispositivo registra todas las actividades de los usuarios realizadas en su empresa. NetScaler ADM proporciona métricas clave que puede utilizar para determinar:

1. Comportamiento de navegación de los usuarios de su empresa.
2. Categorías de URL a las que acceden los usuarios de su empresa.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

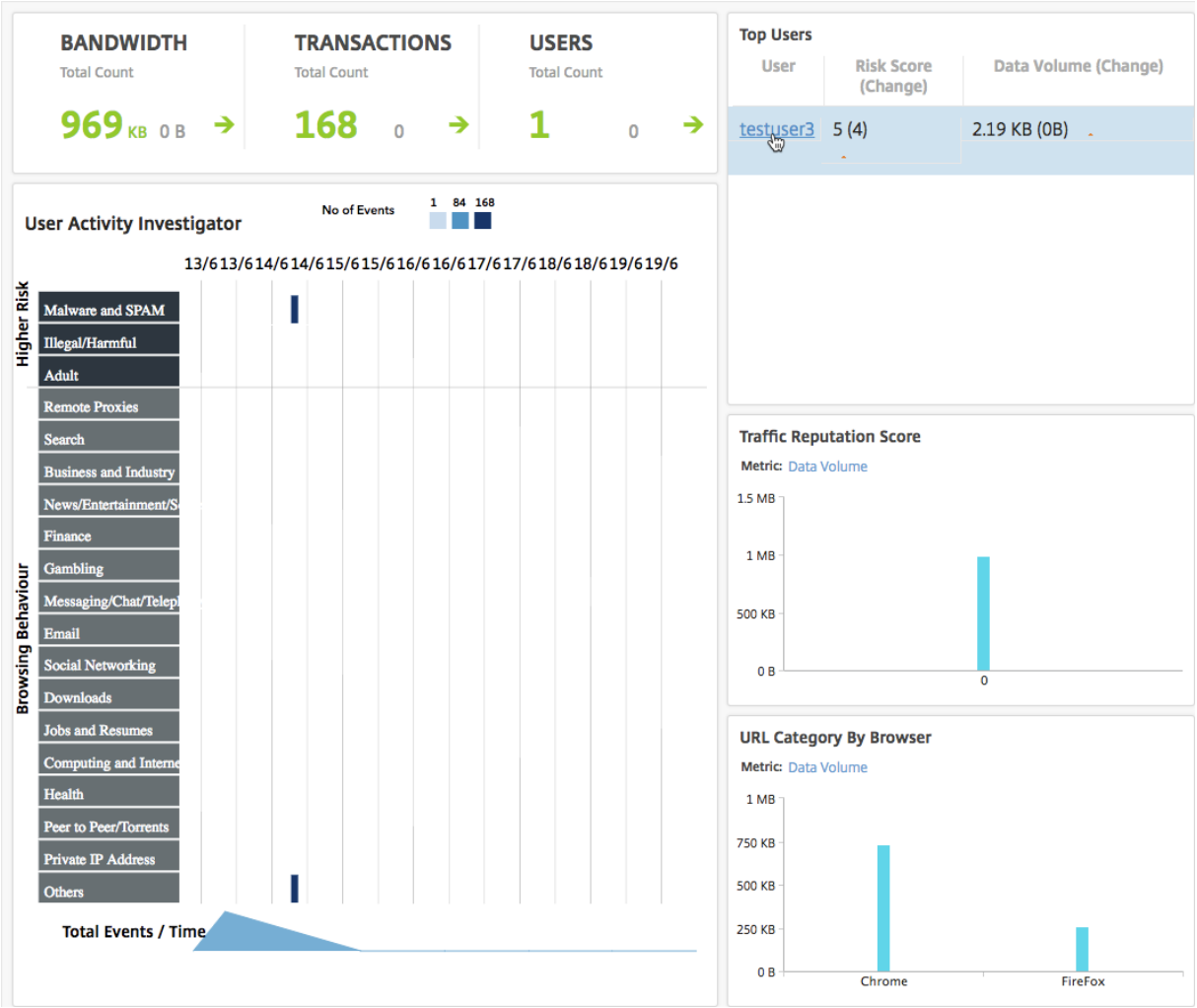
3. Los cinco usuarios principales, en función de sus puntuaciones de riesgo y del ancho de banda que consumen. Para obtener más información sobre las puntuaciones de riesgo, consulte Puntuación de riesgo.
4. Exploradores utilizados para acceder a las URL o dominios.
5. Cantidad del tráfico web generado por los usuarios, en función de la puntuación de la reputación del tráfico.

Por ejemplo, si un usuario con identificador de usuario testuser3 accede constantemente a sitios relacionados con malware de su empresa, NetScaler ADM identifica al usuario como usuario de actividad de alto riesgo y asigna una puntuación de riesgo más alta. La información de testuser3 se muestra en la sección **Usuarios principales** del **Panel de usuarios**.




Puede hacer clic en testuser3 para filtrar el **panel de usuario** y mostrar todas las métricas clave relacionadas con testuser3.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

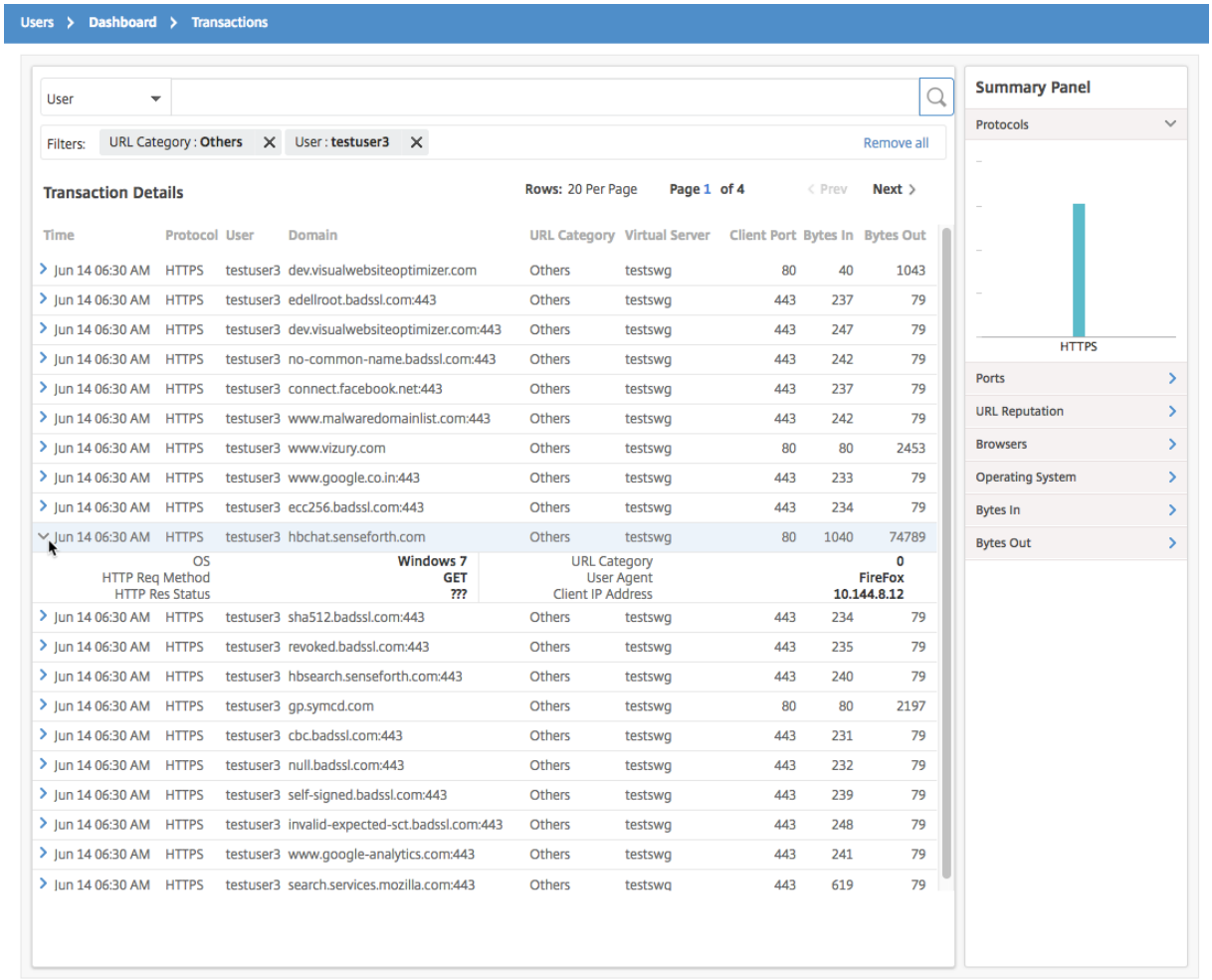



En el panel **Investigación de actividad del usuario**, la actividad de alto riesgo de testuser3 se muestra como eventos en las respectivas categorías de URL.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Puede pasar el cursor sobre los eventos para mostrar el número de eventos y hacer clic en eventos para investigar las transacciones que ocurrieron durante los eventos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



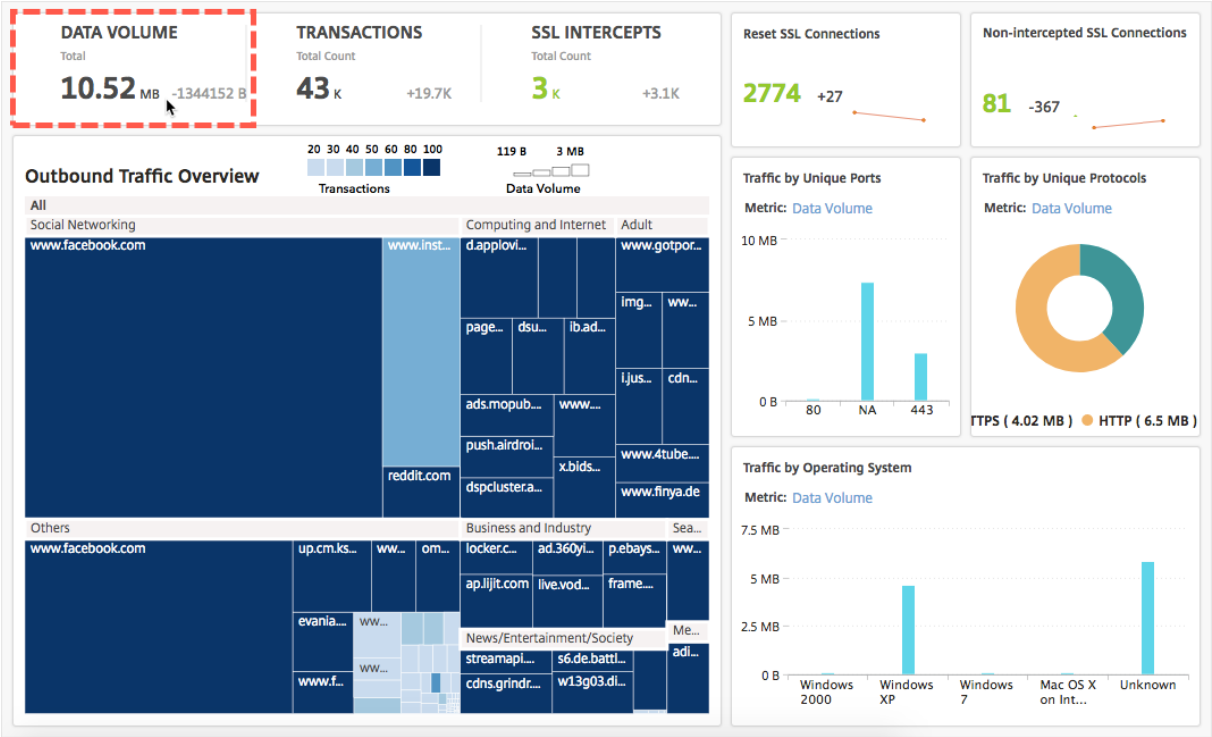

Con esta información, puede determinar si su sistema está infectado por malware, o puede comprender el patrón de consumo de ancho de banda del usuario y ajustar sus directivas NetScaler ADC. Para obtener más información, consulte la documentación de Citrix SSL Forward Proxy.

## Informes sobre el consumo de ancho de banda

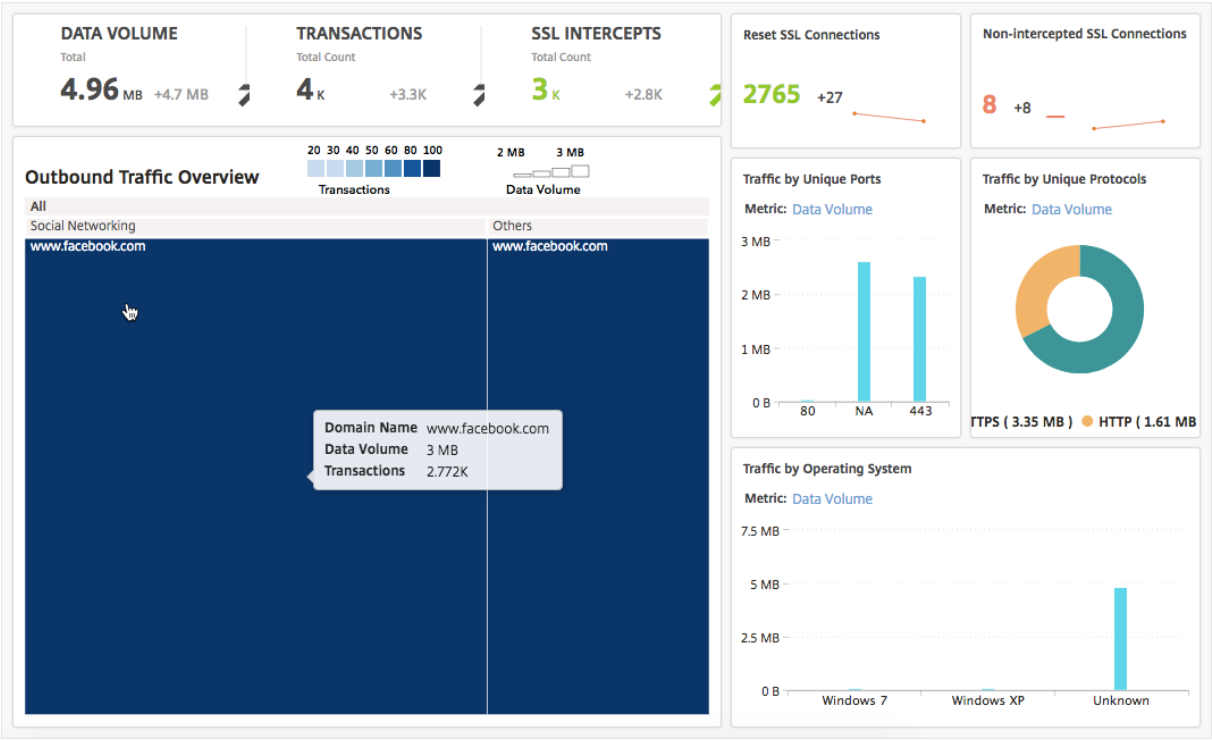
El **Panel de control de tráfico saliente** y el **Panel de usuario** proporcionan varios gráficos que resumen los sitios web o las aplicaciones a las que se accede desde la red empresarial, así como las actividades realizadas por los usuarios de la red.

El **panel de tráfico saliente** proporciona los detalles del consumo del volumen de datos por parte de las URL o los dominios a los que se accedió desde la red. Vaya a **Aplicaciones > Panel de control de tráfico saliente**, donde los detalles del volumen de datos se muestran en la sección **Volumen de datos**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



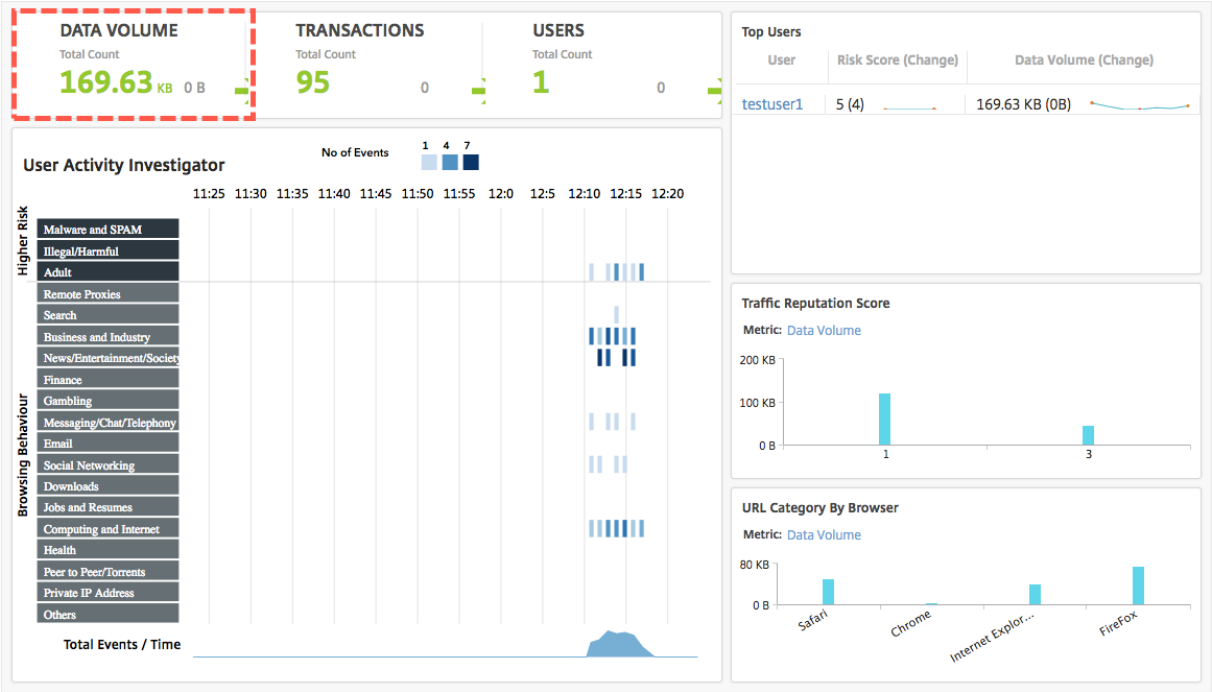

En el panel **Información general del tráfico saliente**, puede hacer clic en un dominio o dirección URL para mostrar los detalles del volumen de datos consumido por el dominio o la URL.



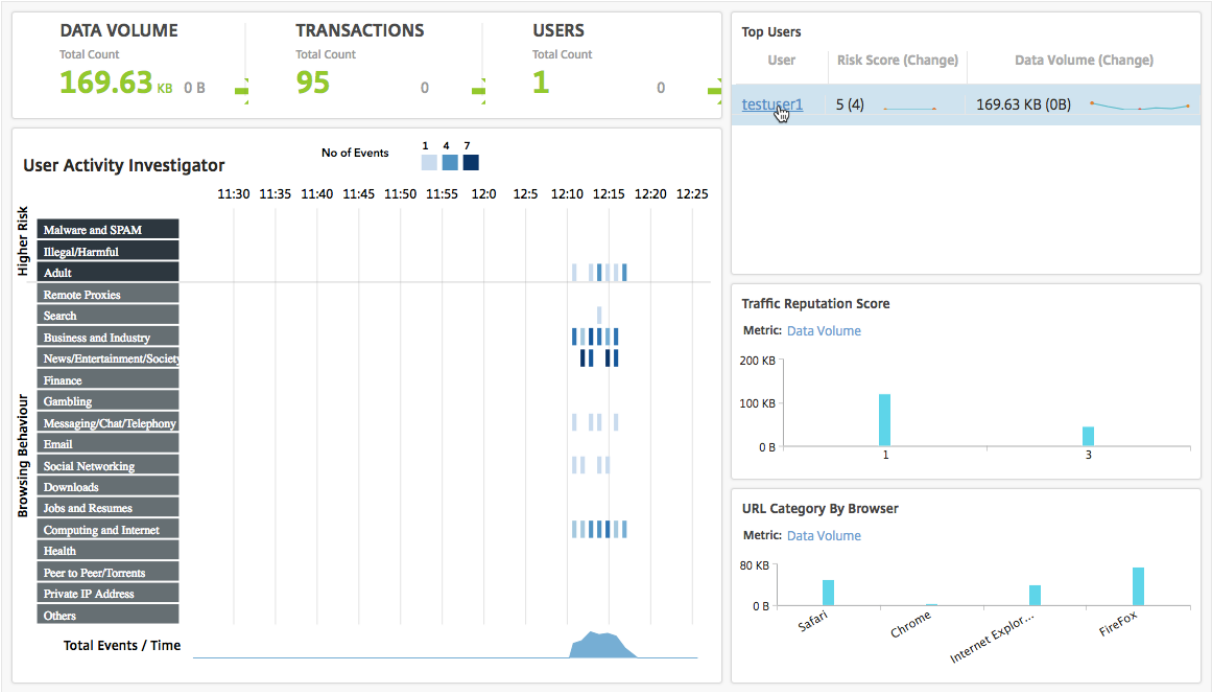

El **Panel de control de usuario** proporciona detalles sobre el ancho de banda consumido por los usuarios de la red. Vaya a **Usuarios > Panel de control** para mostrar los detalles del ancho de banda

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

consumido por los usuarios en la sección **VOLUMEN DE DATOS** del **Panel de usuario**.




Puede ver los detalles del ancho de banda consumido por un usuario seleccionándolo en la sección **Usuarios principales**. La sección **VOLUMEN DE DATOS** y otras métricas clave del gráfico se filtran para el usuario seleccionado.




Mediante estos detalles, puede comprender el consumo de ancho de banda y el motivo del consumo. Por ejemplo, si un usuario está accediendo a sitios web de redes sociales y esto ha causado un gran

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

consumo de ancho de banda, el administrador puede acceder al dispositivo NetScaler ADC y configurar una función Lista de URL para controlar el acceso a los sitios web. Para obtener más información, consulte el tema Caso de uso: filtrado de URL mediante conjunto de URL personalizado.

## Visualización de la distribución del tráfico saliente

El dispositivo NetScaler ADC proporciona funciones de categorización y filtrado de URL que puede utilizar para clasificar las URL a las que se accede desde la red. En NetScaler ADM, el **Panel de control de tráfico saliente** incluye un panel **Descripción general del tráfico saliente**. En el panel **Descripción general del tráfico saliente**, NetScaler ADM agrupa las direcciones URL o dominios a los que se accede en categorías, como Compras, Noticias, Móviles, etc. para mostrar la distribución del tráfico saliente en la red. Para un período de tiempo seleccionado, puede hacer clic en la URL para comprender:

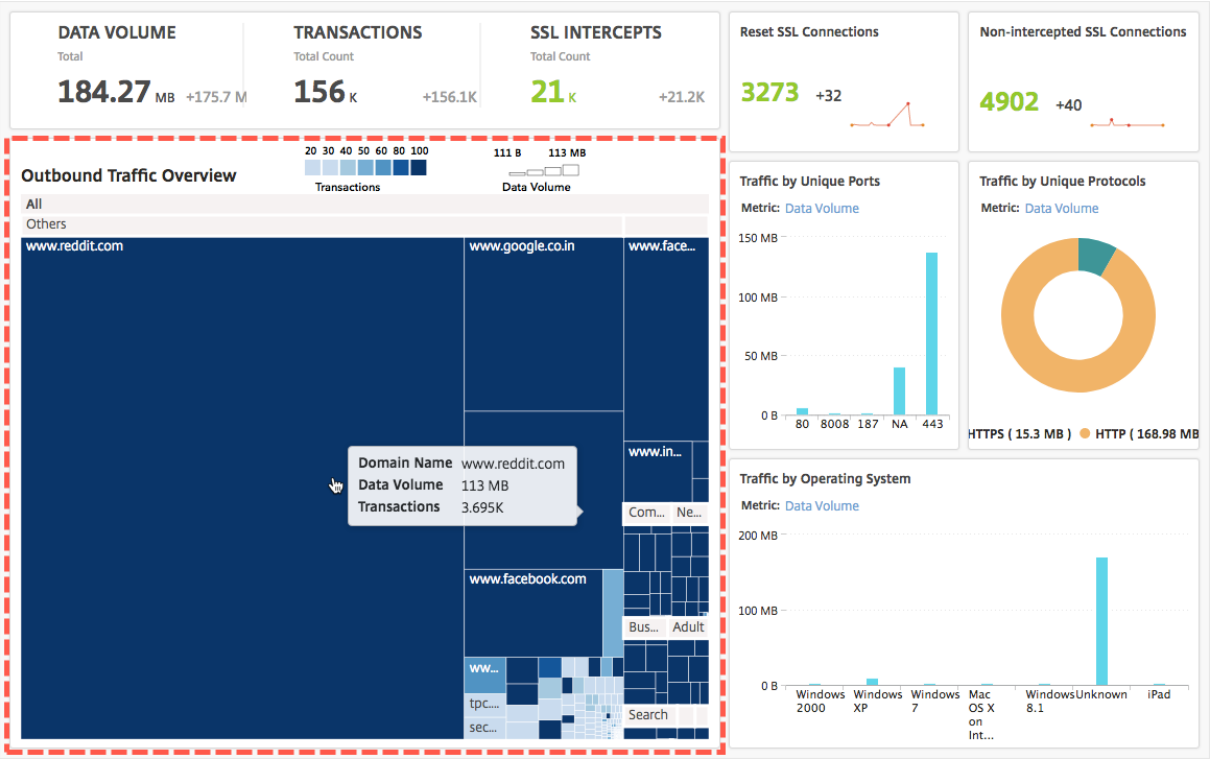
1. Ancho de banda consumido accediendo a la URL
2. Transacciones que se produjeron al acceder a la URL
3. Número de conexiones SSL que se interceptaron, no se interceptaron y se restablecieron al acceder a la URL

Con esta información, puede comprender el patrón del tráfico saliente y tomar decisiones correctivas, como bloquear determinadas URL.

**Para ver la distribución del tráfico saliente:**

Vaya a **Aplicaciones > Panel de control de tráfico saliente**.El **Panel de control de tráfico externo** muestra las direcciones URL en el panel **Información general del tráfico saliente** :

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Si quiere ver los detalles de una URL concreta, seleccione la URL.

Con esta información, puede comprender el patrón de tráfico saliente y controlar el tráfico de red mediante un filtro de URL configurado en el dispositivo NetScaler ADC. Para obtener más información, consulte Filtrado de URL.

## Orchestration

January 30, 2024

En las redes definidas por software (SDN), un controlador de aplicaciones de software administra una red y sus actividades en lugar del hardware que la soporta. Es decir, SDN permite a los administradores de red virtualizar una conectividad de red física en una conectividad de red lógica y administrar los servicios de red mediante una herramienta de administración centralizada basada en software. La SDN permite a los ingenieros y administradores de redes responder a los requisitos empresariales que cambian rápidamente.

Si bien las ventajas más conocidas de la SDN son la programabilidad del tráfico, la mayor agilidad, la capacidad de crear una supervisión de red basada en directivas y la implementación de la automatización de la red, algunas de las ventajas específicas de la SDN se enumeran a continuación:

- Aprovisionamiento de red centralizado

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Mayor seguridad de red a nivel granular
- Costes operativos reducidos
- Mayores niveles de abstracción en la nube
- Entrega de contenido garantizada
- Menor tiempo de inactividad de la red

Citrix Application Delivery Management (ADM) admite la SDN en la red empresarial al integrarse con los controladores SDN de diferentes proveedores. Citrix ADM admite tanto VMware NSX Manager como Cisco Application Policy Infrastructure Controller (APIC).

### VMware NSX Manager

Citrix ADM se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

VMware NSX Manager expone firewalls lógicos, conmutadores, enrutadores, puertos y otros elementos de red para permitir la creación de redes virtuales entre diversos hipervisores, sistemas de administración de la nube y el hardware de red asociado. También es compatible con redes externas y servicios de seguridad.

La función Cloud Orchestration de Citrix ADM permite la integración de los productos Citrix ADC con VMware NSX y proporciona las siguientes funciones:

- Capacidad de asignar una VPX preaprovisionada bajo demanda a una determinada puerta de enlace Edge como parte de la inserción del servicio.
- Capacidad para configurar funciones avanzadas de NetScaler ADC, como SSL y CS, junto con el equilibrio de carga básico a través de plantillas de aplicación en las instancias que se ejecutan dentro del entorno NSX.
- Posibilidad de desasignar un VPX de una determinada puerta de enlace Edge como parte de la eliminación del servicio y reasignar la misma VPX a otra puerta de enlace Edge.
- Capacidad para implementar rápidamente funciones de NetScaler ADC desde la consola de vCenter como parte del flujo de trabajo de implementación de toda la infraestructura necesaria para una aplicación.

Ventajas:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Asignación automatizada y a demanda de nuevos servicios de ADC como parte del flujo de trabajo de implementación de aplicaciones
- Configuración simplificada de la funcionalidad ADC avanzada y específica de la aplicación mediante plantillas de aplicación
- Separación de funciones entre múltiples usuarios y modelo de consumo de autoservicio, al tiempo que proporciona a los administradores de la nube un único punto de control
- Integración más sencilla con las API NetScaler ADM, que ayudan a admitir usos futuros imprevistos.

Para obtener más información sobre cómo configurar VMware NSX Manager en NetScaler ADM, consulte Integración de dispositivos NetScaler ADC con VMware NSX Manager.

### Modo híbrido ACI de Cisco

Cisco ACI introdujo la compatibilidad con el modo híbrido en la versión 1.3 (2f). En el modo híbrido, puede realizar la automatización de la red a través del controlador de infraestructura de políticas de aplicaciones (APIC) y delegar la configuración L4-L7 a Citrix ADM, que actúa como administrador de dispositivos en la APIC.

La solución Citrix ADC Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y Citrix ADM. Debe cargar el paquete de dispositivos de modo híbrido en la APIC. Para obtener más información, consulteNetScaler ADC Automation Using NetScaler ADM in Cisco ACI Hybrid Mode.

## OpenStack: Integración de instancias NetScaler ADC

January 30, 2024

La función Cloud Orchestration de NetScaler Application Delivery Management (ADM) permite la integración de los productos de NetScaler ADC con la plataforma OpenStack. Al utilizar esta función con la plataforma OpenStack, los usuarios de OpenStack pueden aprovechar la función de equilibrio de carga (LBaaS) del NetScaler ADC. Después de esto, los usuarios de OpenStack pueden implementar sus configuraciones de balanceador de carga desde OpenStack en la instancia de Citrix ADC.

En las siguientes secciones se proporciona una breve descripción de las funciones del flujo de trabajo de integración de Citrix ADM y OpenStack.

### Controlador NetScaler ADC para OpenStack Neutron LBaaS

El complemento LBaaS de OpenStack Neutron incluye un controlador de NetScaler ADC que permite a OpenStack comunicarse con NetScaler ADM. OpenStack utiliza este controlador para reenviar

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

cualquier configuración de equilibrio de carga realizada a través de las API de LBaaS, al NetScaler ADM, que crea la configuración del equilibrador de carga en las instancias de NetScaler ADC deseadas. OpenStack también utiliza el controlador para llamar a Citrix ADM a intervalos regulares y recuperar el estado de las diferentes entidades (como los VIP y los grupos) de todas las configuraciones de equilibrio de carga de los ADC de Citrix. El software de controlador Citrix ADC para la plataforma OpenStack se incluye junto con el Citrix ADM. Para descargar e instalar los controladores, primero debe instalar NetScaler ADM e iniciar la aplicación.

### Registrar Citrix ADM y OpenStack entre sí

Primero debe registrar la información de OpenStack en NetScaler ADM. Especifique la dirección IP del controlador OpenStack y las credenciales de usuario administrativo de la nube, así como las credenciales de usuario del controlador Citrix ADC de OpenStack. Más adelante, puede especificar las mismas credenciales de inicio de sesión en la sección Citrix ADC_Driver del archivo de configuración de Neutron (neutron.conf) para que el controlador Citrix ADC de OpenStack pueda conectarse a Citrix ADM durante las configuraciones de LB.

Una vez registrados OpenStack y Citrix ADM, ambos pueden comunicarse entre sí. Además, los usuarios de OpenStack pueden usar sus credenciales existentes en OpenStack para iniciar sesión en la interfaz de usuario de Citrix ADM y comprobar el rendimiento de sus configuraciones de LB en los ADC de Citrix.

### Arrendatarios en OpenStack

En OpenStack, un arrendatario también se denomina proyecto. Un arrendatario es un grupo de usuarios; un arrendatario o un proyecto también se pueden definir como un conjunto de recursos (procesamiento, red, almacenamiento, etc.) asignados a un grupo aislado de usuarios.

### Directivas de colocación

Las políticas de ubicación brindan la flexibilidad de decidir qué instancia de Citrix ADC se usa en cada configuración de balanceador de carga creada por los usuarios. Como alternativa, Citrix ADM también ofrece la opción de asignar una instancia de Citrix ADC en función de los inquilinos de OpenStack.

### Paquetes de servicios

Los paquetes de servicios son paquetes que combinan directivas y SLA, especificaciones de configuración de dispositivos o aprovisionamiento automático y directivas de arrendatarios y ubicación. Un

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

paquete de servicios generalmente se define en términos de las directivas de aislamiento que se proporcionan al arrendatario.

Los siguientes son algunos puntos relacionados con los paquetes de servicios:

- Un arrendatario no puede formar parte de más de un paquete de servicios.
- Se pueden asociar varios arrendatarios al mismo paquete de servicios.
- En un paquete de servicios configurado para el aprovisionamiento automático, las instancias de NetScaler ADC virtuales se pueden crear desde un solo tipo de plataforma (en la plataforma SDX o en la plataforma OpenStack Compute).

### Funciones compatibles con LBaaS V1 y LBaaS V2

Mientras que el controlador LBaaS V1 en OpenStack admite operaciones desde la interfaz de usuario de OpenStack Horizon, el controlador LBaaS V2 solo admite operaciones de línea de comandos.

La siguiente lista muestra las funciones compatibles con LBaaS V1 y LBaaS V2 en OpenStack:

- LBaaS V1
  - Equilibrio de carga
- LBaaS V2
  - Equilibrio de carga
  - Descarga SSL con certificados gestionados por **Barbican**, el administrador de claves en OpenStack
  - Paquetes de certificados (incluye a las autoridades de certificación intermediarias)
  - Soporte SNI

Este documento proporciona información sobre:

- Escenario de caso de uso
- Integración de Citrix ADM con OpenStack Workflow
- Prerequisites
- Tareas previas a la configuración en Citrix ADM y OpenStack
- Pasos de configuración de LBaaS V1 con Horizon
- Pasos de configuración para LBaaS V2 mediante línea de comandos
- Aprovisionamiento manual de la instancia de Citrix ADC VPX en OpenStack
- Integración de Citrix ADM con OpenStack Heat Services
- Supervisión de aplicaciones OpenStack en NetScaler ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Escenario de caso de uso

En el siguiente caso de uso se explica el flujo de trabajo de integración de NetScaler ADM con la plataforma OpenStack:

Una empresa, Example-Cloud-Provider, ha utilizado componentes de OpenStack para configurar una nube a fin de proporcionar infraestructura a sus arrendatarios. Steve es el administrador de este proveedor de nube, mientras que Tom es arrendatario de la infraestructura en la nube del proveedor de nube de Example-Cloud-Provider. La organización de Tom, Example-Sportsonline.com, requiere dos servidores S1 y S1, y Tom también requiere un dispositivo NetScaler ADC dedicado para equilibrar la carga entre los servidores S1 y S2 en la plataforma OpenStack.

Para cumplir con este requisito, Steve tiene que instalar y configurar tanto OpenStack como NetScaler ADM, y prepararlos para que sean compatibles entre sí. Steve tiene que crear una cuenta de arrendatario llamada Example-SportsOnline en OpenStack y, a continuación, asignar recursos a la cuenta de arrendatario. Steve también tiene que crear diferentes credenciales de inicio de sesión (usuarios) para, por ejemplo, SportsOnline, a fin de gestionar sus recursos y su configuración. Tom ahora puede crear los dos servidores S1 y S2 en OpenStack para gestionar el tráfico de su organización.

Steve tiene que registrar los detalles de OpenStack en Citrix ADM y configurar el controlador Citrix ADC LBaaS en el componente de red de OpenStack, Neutron. Una vez completado el registro, Citrix ADM muestra los detalles de todos los inquilinos de OpenStack. Steve puede seleccionar Example-SportsOnline de la lista si quiere las funciones LBaaS de Citrix ADC y configurar a Tom para que le asignen un Citrix ADC dedicado para sus configuraciones de balanceador de carga en Citrix ADM.

Para ello, Steve puede aprovisionar una instancia de Citrix ADC VPX en la capa informática (Nova) de OpenStack mediante la interfaz de usuario de Citrix ADM o permitir que MAS aprovisione automáticamente una instancia de Citrix ADC VPX a petición, cuando Tom realiza su configuración de LB en OpenStack. En cualquier caso, Citrix ADM administra la instancia VPX. Para lograrlo, Steve crea un paquete de servicios en Citrix ADM y define las condiciones del paquete de servicios que se acordaron en el SLA con Tom. Por ejemplo, Steve selecciona la directiva de aislamiento “dedicada”para proporcionar una instancia dedicada a proporcionar a Tom las configuraciones del balanceador de carga. Es decir, Steve selecciona una instancia no compartida para Tom en el paquete de servicios. A continuación, asigna muchas instancias de Citrix ADC VPX al paquete de servicios y asocia Example-SportsOnline, junto con otros inquilinos, que necesitan un Citrix ADC dedicado al paquete de servicios. Como resultado, cuando Tom realiza su primera configuración de balanceador de carga, Citrix ADM asigna una de las instancias de Citrix ADC VPX del paquete de servicios a Example-SportsOnline y también implementa su configuración en ese Citrix ADC.

Tom ahora puede crear configuraciones de equilibrio de carga mediante la creación de grupos, IP virtuales (VIP) y monitores de salud mediante OpenStack LBaaS/UI. Los grupos y los VIP de OpenStack se implementan como grupos de servicios y servidores virtuales en la instancia de Citrix ADC. Tom también puede crear monitores de estado para supervisar los servidores y enviar el tráfico de apli-

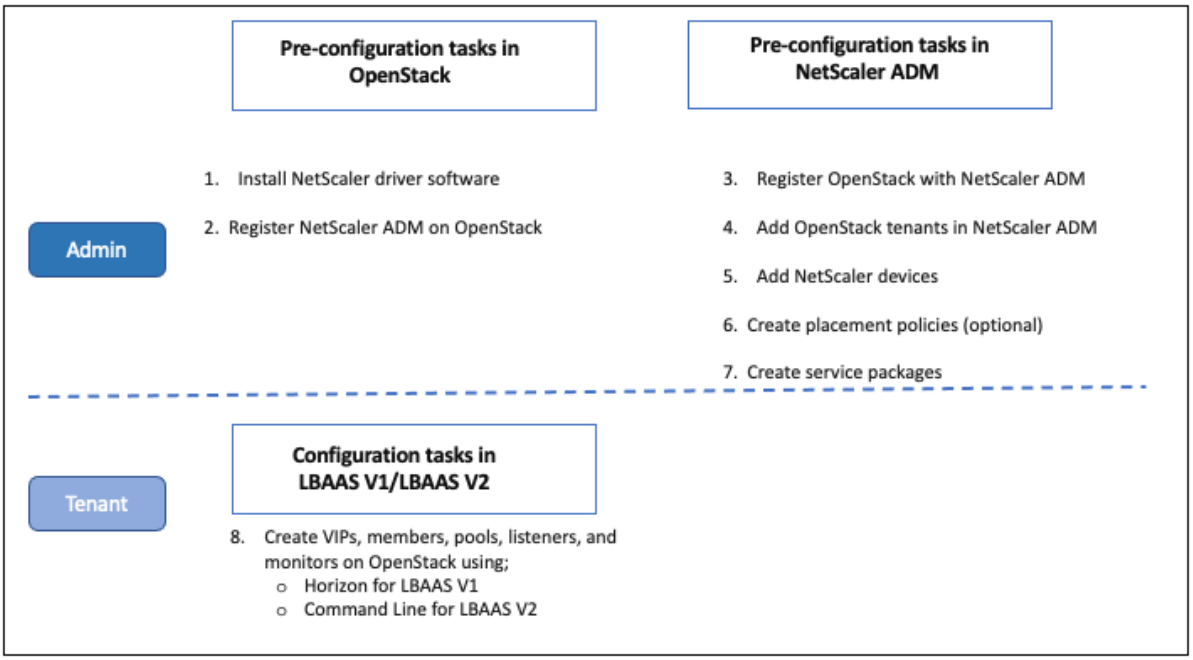
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

caciones solo a aquellos servidores que estén activos en cualquier momento y a los que se pueda acceder desde Citrix ADC.

La configuración de equilibrio de carga creada en OpenStack ahora está implementada en la instancia de Citrix ADC. Una vez configurada completamente, la instancia de NetScaler ADC VPX se hace cargo de la funcionalidad de equilibrio de carga y comienza a aceptar tráfico de aplicaciones y equilibra la carga el tráfico entre los servidores S1 y S2 creados por Tom.

### Integración de Citrix ADM con OpenStack Workflow

El siguiente diagrama de flujo muestra el flujo de trabajo que debe seguir al configurar LBaaS V1 y LBaaS V2.




## Requisitos previos

January 30, 2024

Antes de integrar la instancia virtual de Citrix ADC con la plataforma OpenStack, asegúrese de que se cumplen los siguientes requisitos:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Requisitos de software de NetScaler ADM y OpenStack

- Citrix ADM 13.0 está instalado en una estación de trabajo de hipervisor compatible que cumple con los requisitos mínimos del sistema de hardware.
- Los componentes de OpenStack están instalados y en ejecución.
- NetScaler ADM 13.0 admite las siguientes versiones de OpenStack: **Newton**, **Ocata**, **Pike**y **Queens**.

### Requisitos de hardware de NetScaler ADM

Asegúrese de que los siguientes recursos informáticos virtuales estén en su servidor OpenStack para instalar instancias virtuales de NetScaler ADC:

| Componente | Requisito |
|---|---|
| RAM | 8 GB |
| CPU virtual | 8 |
| Espacio de almacenamiento | 500 GB |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps o 100 Mbps |

> **Nota**
>
> Los requisitos de memoria y disco duro especificados son para implementar Citrix ADM en la plataforma OpenStack, teniendo en cuenta que no hay otras máquinas virtuales ejecutándose en el host. Los requisitos de hardware para OpenStack dependen del número de máquinas virtuales que se ejecutan en él.

## Tareas previas a la configuración en NetScaler ADM y OpenStack

January 30, 2024

Esta sección le ayuda a realizar las tareas previas a la configuración antes de configurar Citrix Application Delivery Management (ADM) y OpenStack.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Instalación de Citrix ADM

Instale NetScaler ADM en un Hypervisor compatible. Para obtener más información sobre cómo descargar e instalar NetScaler ADM, consulte Implementación de NetScaler ADM.

### Instalación del software del controlador NetScaler ADC y registro de NetScaler ADM en OpenStack

Descargue el paquete Citrix ADC para OpenStack desde la página de descargas de Citrix ADM.

**Para instalar el controlador Citrix ADC en la plataforma OpenStack mediante la GUI de Citrix ADM:**

1. En Citrix ADM, haga clic en **Descargas**. La página **Descargas** de NetScaler ADM le proporciona vínculos para descargar el **paquete NetScaler ADC para el software OpenStack** necesario para las versiones **Newton**, **Ocata**y **Pike** OpenStack.
2. Descargue el archivo tar del paquete Citrix ADC más reciente en un directorio temporal (por ejemplo, /tmp) de OpenStack Controller. Este paquete incluye el controlador LBaaS V2 y el plug-in Heat para todas las versiones de OpenStack.

   Downloads for OpenStack

   Citrix ADC bundle for OpenStack. Contains Citrix ADC LBaaS drivers and Heat plugin.
   Citrix ADC bundle for OpenStack has Heat plugin and drivers for both OpenStack LBaaS V1 and V2. The Citrix ADC bundle files provided here includes the following drivers and plugins: LBaaS V1 and LBaaS V2 drivers for OpenStack Liberty and Mitaka releases, LBaaS V2 driver for OpenStack Newton release and Heat plug-in for Heat across OpenStack releases

3. Ejecute el siguiente comando para extraer los archivos del archivo tar del controlador NetScaler ADC:
   ```
   tar -xvzf <name_of_tar_file>
   ```
4. Si tiene un OpenStack <Release Name> setup, en el indicador, escriba el siguiente comando:

   ```
   cd <Release Name>
   ```

   **Ejemplo**:

   ```
   cd Newton
   ```

5. Ejecute el siguiente comando para instalar el controlador y especificar la dirección IP de Citrix ADM, la contraseña del controlador Citrix ADC que configuró al registrar OpenStack en Citrix ADM y el protocolo:

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --
   protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory
   -path>
   ```

   **Ejemplo de configuración de OpenStack de nodo único**:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --
neutron-lbaas-path=/opt/stack/neutron-lbaas
```

**Ejemplo de configuración multinodo de OpenStack**:

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --
neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

> **Nota**
>
> Proporcionar la ruta del directorio `neutron-lbaas` del sistema es opcional. Proporcionar la ruta puede ayudar al script a encontrar los controladores.
>
> Una vez que Citrix ADM se haya registrado correctamente en OpenStack, también puede iniciar sesión en Citrix ADM con sus credenciales de usuario de OpenStack.
>
> Una vez que Citrix ADM se haya registrado correctamente en OpenStack, reinicie los servicios Neutron de OpenStack.

## Registro de OpenStack con Citrix ADM

**Para registrar OpenStack en Citrix ADM mediante la GUI de Citrix ADM:**

1. En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** .
2. Haga clic en **Configurar los ajustes de OpenStack.**
3. En la página **Configurar opciones de OpenStack** , puede establecer los parámetros para configurar OpenStack en Citrix ADM. Aquí tiene dos opciones: Predeterminado y Personalizado.

   Para las versiones de OpenStack de Newton y **Ocata**, puede usar el tipo de implementación predeterminado o personalizado. Sin embargo, para la versión de Pike, debe usar un tipo de implementación personalizado para registrar OpenStack en Citrix ADM.

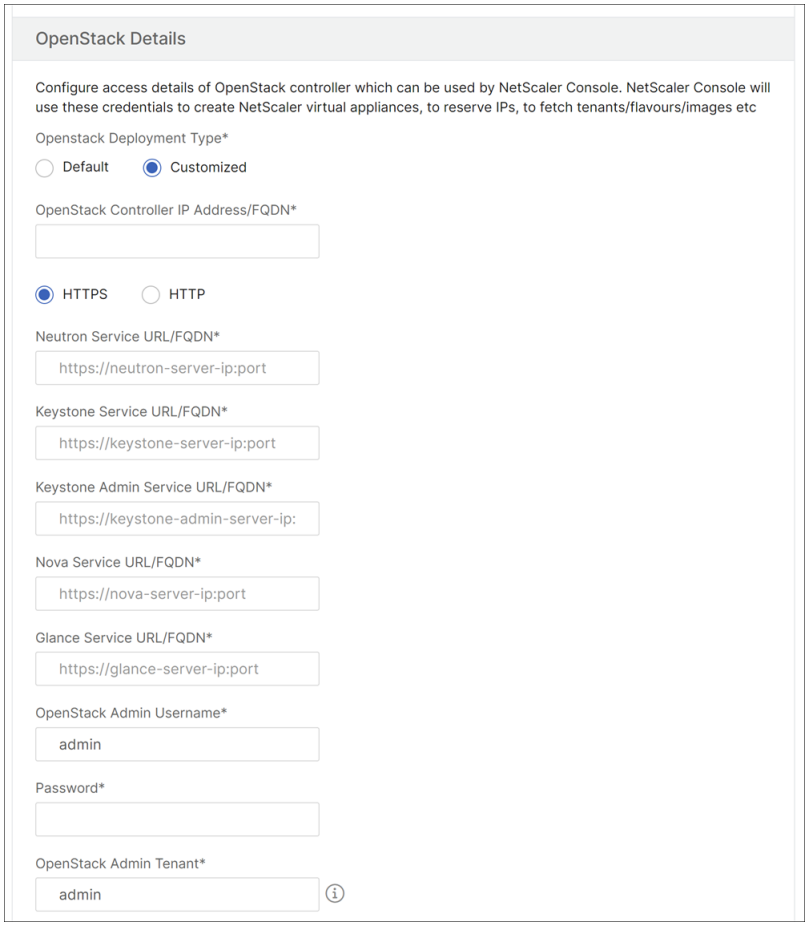
- **Tipo de implementación predeterminado**

  Seleccione**Predeterminado**si los servicios de OpenStack se ejecutan en los puertos predeterminados. Por ejemplo, el portal predeterminado para los servicios de Neutron es 9696 y el portal predeterminado para los servicios de Keystone es 5000.

1. Dirección IP de OpenStack Controller: dirección IP del controlador OpenStack (tanto el servicio **KeyStone** como el servicio **Neutron** deben estar disponibles en esta dirección IP). Por ejemplo, introduzca la dirección IP 10.102.205.23.
2. Nombre de usuario administrador de OpenStack: nombre de usuario administrativo del controlador de OpenStack. Por ejemplo, escriba admin1.
3. Contraseña: contraseña del usuario administrativo del controlador OpenStack.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. OpenStack Admin Tenant: el nombre del arrendatario administrativo de OpenStack. Por ejemplo, introduzca admin.



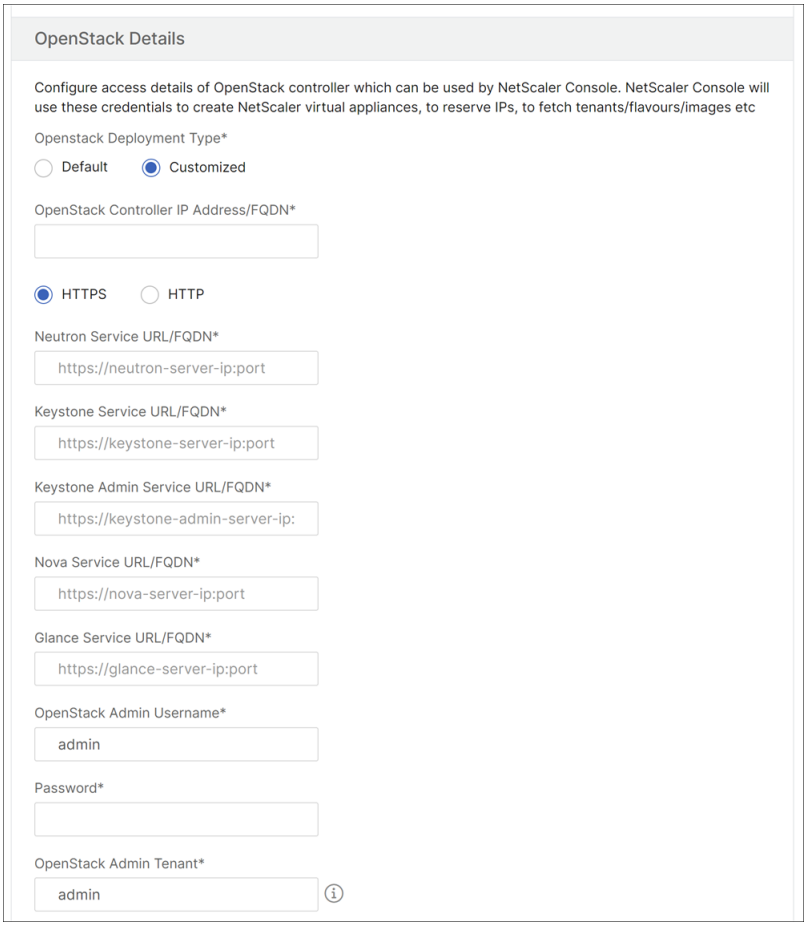

- **Tipo de implementación personalizado**

  Seleccione el tipo de implementación como**Personalizado** si los servicios de OpenStack se ejecutan en puertos distintos de los puertos predeterminados. Si estos servicios se ejecutan en puertos diferentes, especifíquelos aquí. El registro de las versiones de OpenStack Newton y **Ocata** en NetScaler ADM es diferente del registro de la versión de OpenStack Pike.

  **Lanzamiento de OpenStack por Newton y Ocata:**

  1. Especifique los números de puerto para los diversos servicios de OpenStack si está registrando la versión Newton de OpenStack.
  2. Especifique el nombre de usuario, la contraseña y el nombre de usuario de OpenStack Admin Tenant tal como especificó anteriormente en la configuración **predeterminada**.

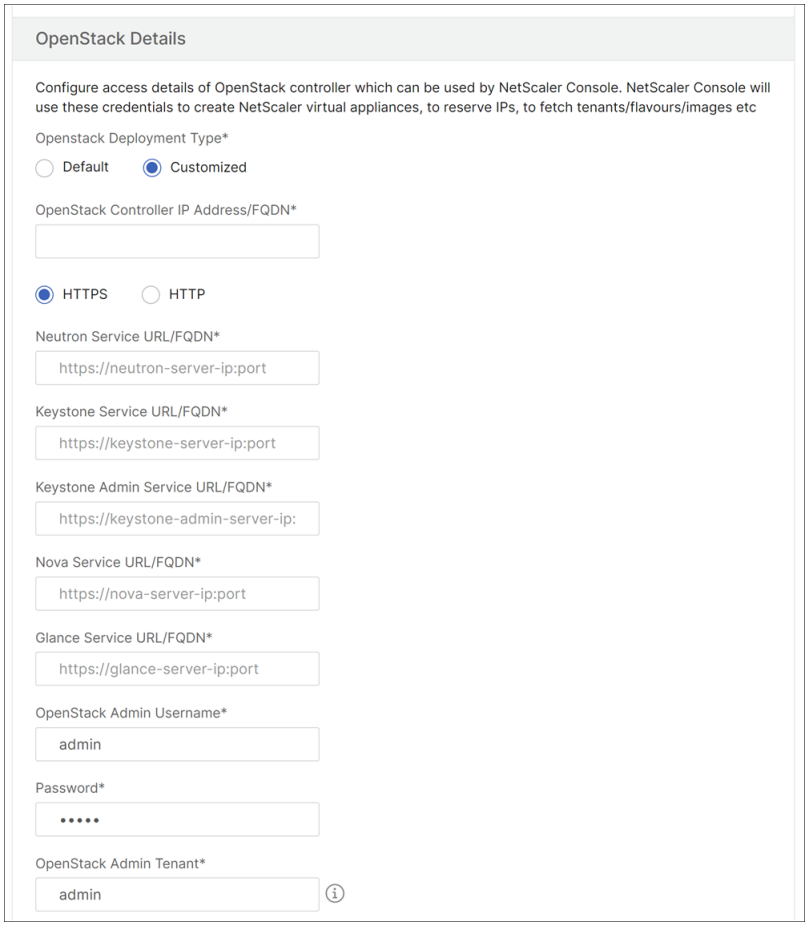
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



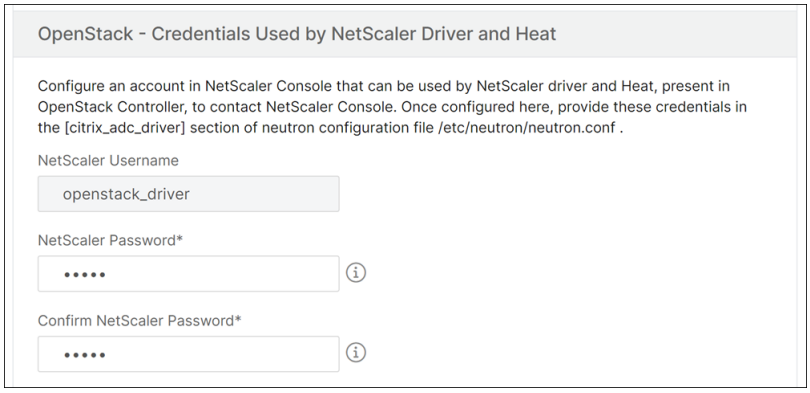

**Lanzamiento de Pike de OpenStack:**

Si está registrando la versión Pike de OpenStack introduzca los detalles de los servicios de OpenStack como se muestra en la siguiente imagen. También debe especificar el nombre de usuario, la contraseña y el nombre de usuario de OpenStack Admin Tenant como en la configuración predeterminada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




1. En la sección**OpenStack Neutron LBaaS: Credentials Used by NetScaler ADC Driver**, establezca la contraseña del controlador NetScaler ADC para la cuenta de usuario del controlador ADC de OpenStack Citrix. NetScaler ADM autentica las llamadas desde el controlador OpenStack NetScaler ADC mediante estas credenciales. Debe especificar la misma contraseña cuando ejecute el script de instalación del controlador NetScaler ADC en el controlador OpenStack.




2. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Crear un arrendatario en OpenStack

Cree un proyecto o un arrendatario en OpenStack, añada usuarios al proyecto o arrendatario y asigne funciones a todos los usuarios. **KeyStone**, el servicio de identidad de OpenStack, proporciona servicios de autenticación para cada servicio OpenStack. El servicio de autenticación utiliza una combinación de dominios, proyectos (arrendatarios), usuarios y roles.

Para obtener más información sobre cómo crear un proyecto y realizar otras tareas en OpenStack, consulte la documentación de OpenStack en.http://docs.openstack.org/

## Agregar arrendatarios de OpenStack

1. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > OpenStack > **OpenStackTenants**y, a continuación, haga clic en**Agregar**.
2. En la página **Agregar arrendatarios de OpenStack**, haga clic en **+Agregar y, a**continuación, seleccione el arrendatario de OpenStack.
3. Haga clic en **Aceptar**.

En función de si está utilizando una instancia preaprovisionada o aprovisionando automáticamente la instancia al integrar OpenStack, siga una de estas dos tareas:

- Preaprovisione los dispositivos NetScaler ADC
- Aprovisionamiento automático de los dispositivos NetScaler ADC VPX en OpenStack

## Aprovisionamiento de dispositivos NetScaler ADC

En función de si está utilizando una instancia preaprovisionada o aprovisionando automáticamente la instancia al integrar OpenStack, siga una de estas dos tareas:

- Preaprovisione los dispositivos NetScaler ADC
- Aprovisionamiento automático de los dispositivos NetScaler ADC VPX en OpenStack

### Aprovisionamiento previo de dispositivos NetScaler ADC

Instale el dispositivo Citrix ADC en cualquiera de las plataformas de hipervisores, como Citrix Hypervisor, KVM o ESX, y agregue la instancia a Citrix ADM. A continuación, NetScaler ADM administra este dispositivo que equilibra la carga el tráfico en los servidores.

**Para agregar una instancia de Citrix ADC VPX existente en Citrix ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En Citrix ADM, vaya a **Infraestructura** > **Instancias** > **Citrix ADC VPX** y, a continuación, haga clic en **Agregar**.
2. En la página **Agregar Citrix ADC VPX** , especifique la dirección IP de la instancia de Citrix ADC VPX y seleccione un perfil de instancia en la lista de **nombres de perfil**. El perfil de instancia contiene las credenciales utilizadas para iniciar sesión en Citrix ADC VPX. También puede crear un nuevo perfil de instancia haciendo clic en el icono +. Haga clic en **Aceptar**.

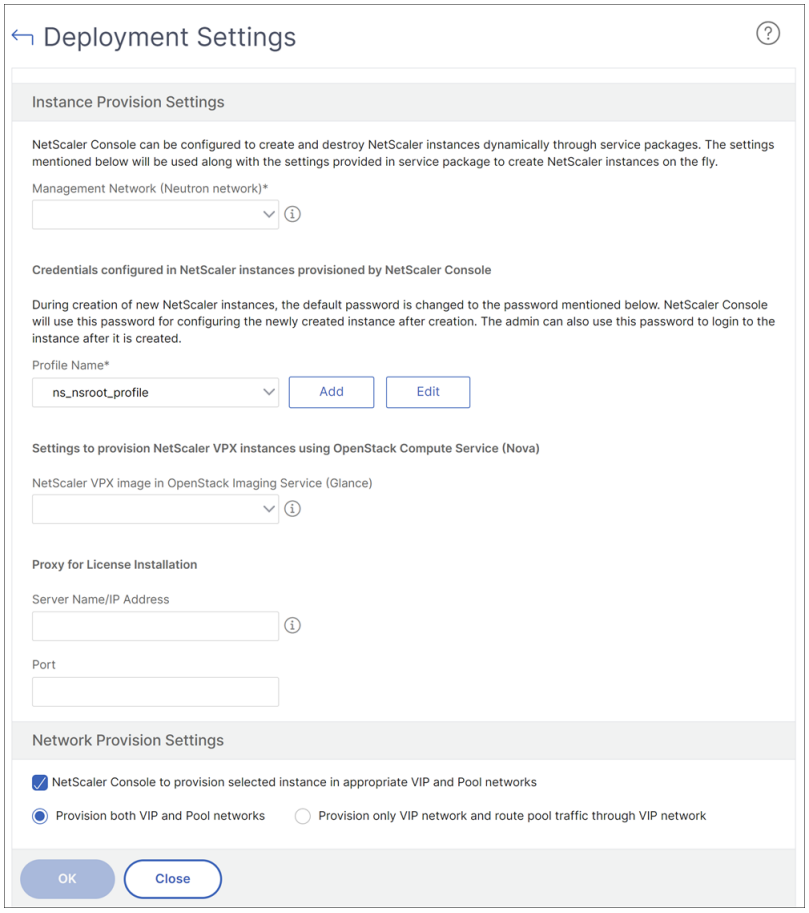
**Aprovisionamiento automático de dispositivos Citrix ADC**

Descargue la imagen de instancia de Citrix ADC requerida de la página de descargas de Citrix y cárguela en Glance, el servicio de imágenes de OpenStack. Tener una imagen disponible en Glance le permite configurar una instancia de Citrix ADC bajo demanda al asignar la instancia al inquilino.

**Para aprovisionar automáticamente los dispositivos Citrix ADC VPX en OpenStack:**

1. En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack**.
2. Haga clic en**Configuración de implementación**.
3. Defina los siguientes parámetros:
   a) Red de administración: seleccione la red de administración en OpenStack a la que está conectado el Citrix ADC VPX de aprovisionamiento automático.
   b) Nombre del perfil: seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.
   c) Licencias: proporcione los códigos de acceso de licencia de NetScaler ADM que se utilizan para licenciar nuevas instancias de NetScaler ADC aprovisionadas automáticamente. NetScaler ADM aprovisiona instancias NetScaler ADC en el proceso OpenStack en la red de administración y, a continuación, desencadena la instalación de licencias en ellas mediante el código de licencia especificado. A continuación, la instancia de NetScaler ADC descarga los archivos de licencia del sitio web de Citrix con el código de acceso de licencia especificado aquí.
   d) Imagen de NetScaler ADC VPX en un vistazo: Seleccione la imagen de NetScaler ADC VPX disponible en OpenStack Glance que se utiliza para crear una instancia de NetScaler ADC VPX.
   e) Configuración de proxy: proporcione detalles del servidor proxy Citrix ADC para instalar licencias. Esto puede ser necesario cuando Citrix ADC no tiene acceso directo a Internet a través de la red de administración.
4. Haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Creación de un paquete de servicios en NetScaler ADM

### Para crear paquetes de servicios para un inquilino en Citrix ADM:

1. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **OpenStack** > **Service Packages** y, a continuación, haga clic en **Agregar**.
2. En la página **del paquete de servicios**, especifique los siguientes parámetros:
   a) Nombre: Nombre para el paquete de servicios. Por ejemplo, escriba SVC-PKG-GOLD.
   b) Asignación de instancias de Citrix ADC: el tipo de asignación de instancias definido en el paquete de servicios en función del cual los recursos de instancias de Citrix ADC se asignan a un inquilino. Seleccione **Dedicado**. Para obtener más información sobre las directivas, consulte Directivas de aislamiento de paquetes de servicios.
   c) Aprovisionamiento de instancias de NetScaler ADC: Seleccione **Instancia existente**para asignar una instancia de NetScaler ADC existente a un arrendatario. Si quiere crear instancias de Citrix ADC durante la propia configuración, seleccione **Crear instancia bajo demanda**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

d) Tipo de instancia de Citrix ADC: seleccione **Citrix ADC VPX** .

> **Nota**
>
> Seleccione Citrix ADC VPX para asignar instancias Citrix ADC previamente aprovisionadas alojadas en la plataforma SDX.

3. Haga clic en **Continuar** para asociar a un arrendatario a un paquete de servicios.

> **Nota**
>
> Habilite el **aprovisionamiento de un par de instancias de Citrix ADC para una alta disponibilidad** , si está implementando las instancias de Citrix ADC en modo de alta disponibilidad.

4. En la sección **Asignar instancias** , haga clic en **Agregar** y, a continuación, seleccione la instancia de Citrix ADC que quiere asignar al inquilino y haga clic en **Continuar** .
5. En la sección **Asignar arrendatarios y directivas de ubicación de OpenStack**, en **OpenStack Arrendatarios, haga clic en**Agregar**y seleccione el arrendatario**.
6. Haga clic en **Continue** y, a continuación, en **Done**.

> **Nota**
>
> Si no se encuentra la directiva, se reviva el mecanismo de reserva y NetScaler ADM asigna instancias de NetScaler ADC basadas en arrendatarios. Si el arrendatario no forma parte de ningún paquete de servicios, NetScaler ADM muestra un mensaje de error que dice: “Tenant\ <admin\ > no forma parte de ningún paquete de servicios y no hay un paquete de servicios predeterminado. “

## Creación de directivas de ubicación (opcional)

Las directivas de aislamiento no se basan únicamente en los arrendatarios. Puede crear directivas de ubicación flexibles, en las que las directivas no solo se basen en el nombre o la identificación del arrendatario, sino también en otros atributos personalizados.

**Para crear políticas de colocación para un inquilino en Citrix ADM:**

1. En Citrix ADM, vaya a Orchestration > **CloudOrchestration**>**OpenStack**>**Política de ubicación**y, a continuación, haga clic en**Agregar**.
2. En la página **Agregar directiva de ubicación**, defina los siguientes parámetros:

   a) Nombre: escriba un nombre para la directiva de colocación

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Expresiones de ejemplo: seleccione una expresión de ejemplo de la lista. Estos ejemplos son útiles para construir la directiva de colocación.

c) Expresión: en este campo se rellena una expresión booleana en función de la expresión de muestra que ha seleccionado en el campo anterior. Modifique los nombres de los campos según sea necesario.

3. Haga clic en **Aceptar**.

## Habilitar el tráfico de instancias de NetScaler ADC a servidores back-end a través de la red de clientes

De forma predeterminada, en el flujo de trabajo de orquestación de OpenStack, las instancias NetScaler ADC se vinculan dinámicamente a las redes del equilibrador de carga o cliente y a las redes de miembros o servidores.

En ciertas implementaciones, también se puede acceder a los servidores a través de las redes de clientes y se pueden enrutar a través de la puerta de enlace del cliente. En estos casos, las instancias de Citrix ADC no necesitan estar enlazadas a redes de servidores, sino que solo deben estar enlazadas a redes de clientes.

Realice la siguiente configuración para configurar el tráfico a través de la puerta de enlace del cliente.

Vaya a **Orquestación > Orquestación** en la **nube** > **OpenStack** > **Configuración de implementación**y, a continuación, seleccione la opción **Aprovisionar solo redes VIP y enrutar el tráfico del grupo a través de la red VIP**.

A continuación, Citrix ADM configura la instancia de Citrix ADC para las redes de los clientes añadiendo un SNIP en esa red y, además, añadirá una ruta predeterminada a la puerta de enlace de la red del cliente. Esto permite que la instancia llegue a los servidores a través de la puerta de enlace del cliente.

## Aprovisionamiento automático de dispositivos Citrix ADC VPX implementados en la plataforma Citrix ADC SDX

Agregue la plataforma Citrix ADC SDX a Citrix ADM para que Citrix ADM aprovisione las instancias de esta plataforma bajo demanda.

**Para proporcionar automáticamente instancias de NetScaler ADC implementadas en la plataforma NetScaler ADC SDX:**

1. En la GUI de Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix ADC SDX** y haga clic en **Agregar** para agregar una plataforma Citrix ADC SDX.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Configuración de implementación.**
3. En la sección **Red** de administración , seleccione la red de administración de OpenStack a la que está conectado el Citrix ADC SDX de aprovisionamiento automático.
   a) En**Nombre de perfil**, seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.
   b) Haga clic en **Aceptar**.
4. Para aprovisionar la plataforma Citrix ADC SDX en OpenStack, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Service Package** .
   a) Haga clic en**Agregar** para crear un nuevo paquete de servicios.
   b) Introduzca el nombre del paquete de servicios.
   c) En el campo **Asignación de instancias de Citrix ADC** , seleccione **Dedicado** .
   d) En el campo **Citrix ADC Instance Provisioning** , seleccione **Create Instance OnDemand** y, en el campo **Auto Provision Platform** , seleccione **Citrix ADC SDX**.
   e) De forma predeterminada, solo las instancias de Citrix ADC VPX se aprovisionan en la plataforma Citrix ADC SDX.
   f) Haga clic en **Continuar**.
   g) En la sección**Configuración de aprovisionamiento automático**, defina las propiedades de**los recursos**.
      i. Campo**de rendimiento**. Introduzca 1000 Mbps.
      ii. Campo**Versión de NetScaler ADC**. En la lista, seleccione la versión correcta de la imagen de NetScaler ADC VPX presente en la plataforma NetScaler ADC SDX.
   h) En la sección**NetScaler ADC SDX Platforms**, haga clic en**Agregar** para agregar la plataforma SDX al paquete de servicios.
   i) Haga clic en **Continuar**.
   j) En la sección**Configurar arrendatarios de OpenStack**, haga clic en**Agregar** para agregar los arrendatarios. También puede agregar nuevos arrendatarios haciendo clic en**Nuevo**.
   k) Haga clic en **Done**.
5. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente de Neutron y ejecute las tareas de configuración. Para obtener más información sobre cómo ejecutar comandos de configuración, consulteConfiguración de LBaaS V2 mediante la línea de comandos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Configurar LBaaS V1 mediante Horizon

January 30, 2024

Tom ahora puede iniciar sesión en el portal OpenStack Horizon, crear un grupo de LBaaS y seleccionar una subred en la que se encuentren todos los miembros de este grupo. Tom tiene que agregar una dirección IP virtual (VIP) y asignar esta VIP al grupo que ha creado. Tom también puede realizar esto en la línea de comandos o mediante APIs. Los clientes externos de los servidores de Tom pueden conectarse a esta dirección VIP, que está alojada en el Citrix ADC asignado, y Citrix ADC distribuye todas las solicitudes a los miembros del grupo en los puertos configurados.

Los miembros del grupo LBaaS son los servidores con equilibrio de carga que se agregan al grupo seleccionado. Tom puede asignar un peso y un puerto a cada uno de estos miembros.

Los monitores de salud se utilizan para vigilar la salud y el buen funcionamiento de todos los miembros de la agrupación. Tom puede crear una plantilla de supervisión del estado en OpenStack especificando los límites de retraso, tiempo de espera y reintentos, y también especificar el método, la ruta de URL y los códigos HTTP esperados en caso de éxito. Después de crear un monitor, Tom tiene que asociar el monitor con el grupo que se creó previamente.

Para obtener más información sobre cómo crear grupos y otras tareas de configuración de LBaaS en OpenStack, consulte la documentación de OpenStack.

> **Importante**
>
> LBaaS V1 no es compatible con la versión Liberty de OpenStack. Para obtener más información, consulte Notas de la versión de OpenStack.

## Configurar LBaaS V2 mediante la línea de comandos

January 30, 2024

LBaaS V2 admite la descarga SSL con certificados administrados por **Barbican**, paquetes de certificados (incluye Autoridades de certificación intermediarias), compatibilidad con SNI junto con las funciones regulares de equilibrio de carga. LBaaS V2 solo admite la interfaz de línea de comandos para ejecutar tareas de configuración. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron.

> **Nota**
>
> Cargue el certificado y la clave al servicio **Barbican** cuando necesite la función de descarga SSL. Realice los pasos 1, 2 y 3 si se admite la descarga SSL; de lo contrario, continúe desde el paso 4

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

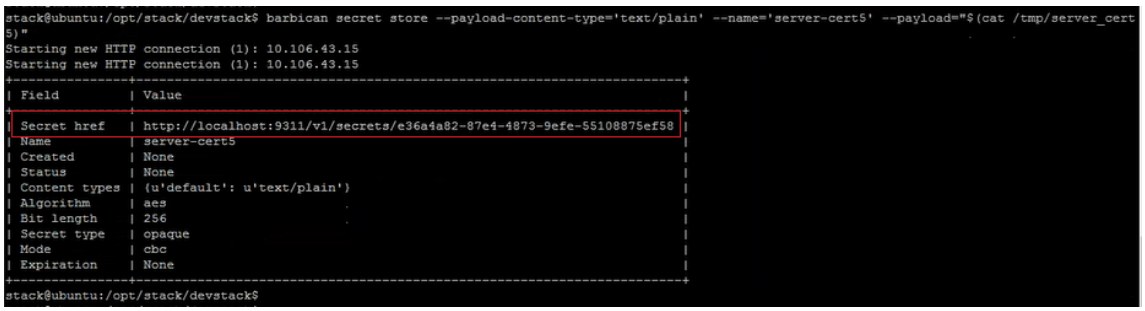
> para crear un equilibrador de carga, un agente de escucha, un grupo y un miembro.

1. Cargue el certificado al servicio **Barbican** mediante el siguiente comando:

```
barbican secret store --payload-content-type <content_type> --name
    <certificate_name> --payload<certificate_location>
```

**Ejemplo**:

```
barbican secret store --payload-content-type='text/plain' --name='
    hp_server_certificate' --payload=" hp_server/tmp/
    server_certificate"
```




2. Cargue la clave en el servicio **Barbican** mediante el siguiente comando:

```
barbican secret store --payload-content-type <content_type> --name
    <key_name> --payload<key_location>
```

**Ejemplo**:

```
barbican secret store -- payload-content-type='text/plain' --name=
    'shp_server_key' --payload="hp-server/tmp/server_key"
```

> **Nota**
>
> Cuando ejecuta estos dos comandos **Barbican** para cargar el certificado y la clave, los campos href secreto proporcionan una ubicación o url. Aquí es donde el certificado y la clave se almacenan en el sistema donde está instalado OpenStack. Copie estos vínculos y proporcione estos enlaces como parámetros cuando cree el contenedor en el servicio **Barbican** en el paso 3.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

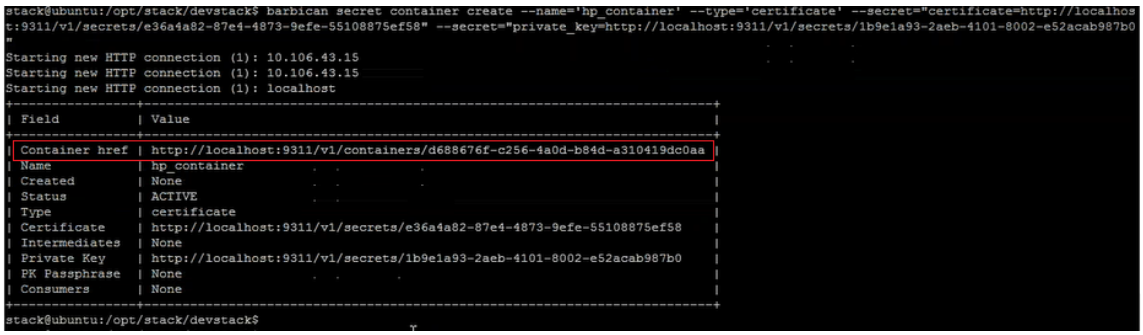
3. Cree un contenedor en el servicio **Barbican** para almacenar el certificado y la clave mediante el siguiente comando:

   En el comando, reemplace con la URL que obtuvo del campo Href secreto cuando cargó el certificado. Del mismo modo, reemplazar con la url que obtuviste del campo href secreto cuando subiste la clave.

```
barbican secret container create --name<container_name> --type<
    container_type> --secret<certificate_url> --secret<key_url>
```

   **Ejemplo**:

```
barbican secret container create --name='hp_container' --type='
    certificate' --secret="`certificate=http://localhost:9311/v1/
    secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="
    private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb
    -4101-8002-e52acab987b0`"
```




   Copie el valor href del contenedor. Debe proporcionar el enlace al contenedor al crear el oyente en el paso 6.

4. Configure las variables de entorno en OpenStack. Las variables permiten que los comandos del cliente de OpenStack se comuniquen con los servicios de OpenStack.

   **Ejemplo**:

   export OS_PASSWORD-hp

   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   export OS_IDENTITY_API_VERSION=2.0

   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
stack@ubuntu:/opt/stack/devstack$ export OS_PASSWORD=hp
stack@ubuntu:/opt/stack/devstack$ export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/
stack@ubuntu:/opt/stack/devstack$ export OS_USERNAME=hp_user
stack@ubuntu:/opt/stack/devstack$ export OS_TENANT_NAME=hp
stack@ubuntu:/opt/stack/devstack$ export OS_IDENTITY_API_VERSION=2.0
stack@ubuntu:/opt/stack/devstack$ export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"
stack@ubuntu:/opt/stack/devstack$
```

> **Nota**
>
> Establezca estas variables para cada sesión SSH antes de ejecutar otros comandos. Para obtener más información sobre las variables de entorno OpenStack, consulte Variables de entorno OpenStack.

5. Cree un equilibrador de carga con el siguiente comando:

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <
    subnet-name> --provider <netscaler>
```

**Ejemplo**:

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --
    provider netscaler
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

El estado cambia de PENDING_CREATE a ACTIVE después de crear correctamente el equilibrador de carga.

```
+--------------------------------------+------------+--------------+---------------------+------------+
| id                                   | name       | vip_address  | provisioning_status | provider   |
+--------------------------------------+------------+--------------+---------------------+------------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25    | ACTIVE              | netscaler  |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19    | ACTIVE              | netscaler  |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24    | ACTIVE              | netscaler  |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27    | ACTIVE              | netscaler  |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18    | ACTIVE              | netscaler  |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23    | ACTIVE              | netscaler  |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20    | ERROR               | netscaler  |
+--------------------------------------+------------+--------------+---------------------+------------+
```

6. Cree un agente de escucha mediante el siguiente comando:

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name>
    --name <listener-name> --protocol <protocol_type> --protocol-
    port <port_number> --default-tls-container-id<container_url>
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo**:

```
neutron lbaas-listener-create --name hp-lb-test-list  --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-port 443 --default-tls-container-id `http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`
```

> **Nota**
>
> Si está creando un agente de escucha sin soporte de descarga SSL, ejecute el siguiente comando sin proporcionar ubicaciones al contenedor:
>
> `neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-listener-create --name hp-lb-test-list --loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --prot
ocol-port 443 --default-tls-container-id http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa
Created a new listener:
+-------------------------+--------------------------------------------------------------------------------+
| Field                   | Value                                                                          |
+-------------------------+--------------------------------------------------------------------------------+
| admin_state_up          | True                                                                           |
| connection_limit        | -1                                                                             |
| default_pool_id         |                                                                                |
| default_tls_container_id | http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa |
| description             |                                                                                |
| id                      | 734a0361-153d-4983-bc2c-55a3ec2ff6fb                                          |
| loadbalancers           | {"id": "746d730b-3b63-418f-a816-d8dd5472963c"}                                 |
| name                    | hp-lb-test-list                                                                |
| protocol                | TERMINATED_HTTPS                                                               |
| protocol_port           | 443                                                                            |
| sni_container_ids       |                                                                                |
| tenant_id               | 0f30b93cd0cd4482b92d033e1628aa8f                                               |
+-------------------------+--------------------------------------------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

7. Cree un grupo con el siguiente comando:

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --listener <listener-name> --protocol <protocol_type> --name <pool-name>
```

**Ejemplo**:

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --listener demolistener --protocol http --name demopool
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-pool-create --lb-algorithm ROUND_ROBIN --listener hp-lb-test-list --protocol HTTP --name hp-lb-test
-pool
Created a new pool:
+---------------------+--------------------------------------------+
| Field               | Value                                      |
+---------------------+--------------------------------------------+
| admin_state_up      | True                                       |
| description         |                                            |
| healthmonitor_id    |                                            |
| id                  | 714c44d0-5cf7-4ef8-b84d-f6d3a258c770       |
| lb_algorithm        | ROUND_ROBIN                                |
| listeners           | {"id": "734a0361-153d-4983-bc2c-55a3ec2ff6fb"} |
| members             |                                            |
| name                | hp-lb-test-pool                            |
| protocol            | HTTP                                       |
| session_persistence |                                            |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f           |
+---------------------+--------------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

8. Cree un miembro con el siguiente comando:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number>  <pool-name>
```

**Ejemplo**:

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
Created a new member:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| address        | 15.0.0.15                            |
| admin_state_up | True                                 |
| id             | ced7a563-5ecc-474f-8d2a-cb69923215b0 |
| protocol_port  | 80                                   |
| subnet_id      | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
| tenant_id      | 0f30b93cd0cd4482b92d033e1628aa8f     |
| weight         | 1                                    |
+----------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

### Supervisión de aplicaciones OpenStack en NetScaler ADM

Los inquilinos pueden iniciar sesión en Citrix Application Delivery Management (ADM) con sus credenciales de OpenStack para supervisar los VIP y los grupos creados a partir de OpenStack desde cualquier explorador. La dirección URL debe tener el siguiente formato:

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

Donde, `mas-ip-address`, es la dirección IP NetScaler ADM que está registrada con OpenStack.

> **Nota**
>
> - Los VIP de OpenStack corresponden a los servidores virtuales de Citrix ADM.
> - Los grupos de OpenStack corresponden a los grupos de servicios de Citrix ADM.
> - Los miembros del grupo de OpenStack corresponden a los miembros del grupo de servicios en NetScaler ADM.

## Configurar la conmutación de contenido de capa 7

January 30, 2024

Citrix Application Delivery Management (ADM) se organiza con OpenStack para configurar las funcionalidades de conmutación de capa 7 (L7) o de conmutación basada en contenido en las instancias de Citrix ADC. El cambio de contenido difiere del simple equilibrio de carga en que se pueden dirigir tipos específicos de solicitudes a servidores específicos. Cuando las configuraciones L7 se crean en

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

OpenStack con una instancia de Citrix ADC como proveedor, Citrix ADM asigna una instancia de Citrix ADC e implementa las configuraciones de respuesta y conmutación de contenido correspondientes a las configuraciones L7. A continuación, las instancias de Citrix ADC pueden distribuir y equilibrar la carga de las solicitudes de los usuarios en función de las características de nivel de aplicación de las solicitudes.

La función de equilibrio de carga de capa 7 (L7) de OpenStack combina equilibrio de carga y conmutación de contenido para proporcionar una entrega optimizada de tipos específicos de contenido. Esto mejora el rendimiento del equilibrador de carga mediante la ejecución solo de las directivas que son aplicables al contenido. El equilibrio de carga de la capa 7 también facilita una mayor eficiencia de la infraestructura de la aplicación. La capacidad de separar el contenido según el tipo, URI o datos permite una mejor asignación de recursos físicos en la infraestructura de la aplicación. Por ejemplo, un usuario final que navega `http://example-sports.com/about-us` es servido por un grupo de servidores que alojan contenido sobre la empresa y los servicios, mientras que un usuario que navega `http://example-sports.com/shopping-cart-football` es servido por un grupo diferente de servidores que permite a los usuarios realizar compras en línea.

En la conmutación de L7, un equilibrador de carga se implementa como un servidor virtual de conmutación de contenido que acepta solicitudes HTTP de los usuarios y las distribuye a los servidores de aplicaciones. La conmutación L7 o el cambio de contenido permiten tener una entrada de un solo punto para acceder a una variedad de servicios de fondo (por ejemplo, no solo las aplicaciones web, los portales de servicios web, los correos web, sino también la administración de dispositivos móviles, el contenido en diferentes idiomas, etc.). Es decir, puede proporcionar una dirección IP pública para todos los servicios que ofrece a sus usuarios.

A diferencia del equilibrio de carga de nivel inferior, la conmutación de capa 7 no requiere que todos los servidores del grupo tengan el mismo contenido. Una configuración de balanceador de carga que utiliza la conmutación L7 espera que los servidores de aplicaciones o back-end de diferentes grupos tengan un contenido diferente. Los conmutadores L7 pueden dirigir solicitudes sobre la base de URI, host, encabezados HTTP o cualquier otra cosa en el mensaje de la aplicación. Los servidores de aplicaciones sirven esencialmente tipos específicos de contenido. Por ejemplo, un servidor solo puede servir imágenes, otro podría ejecutar lenguajes de scripting del lado del servidor, como PHP y ASP, y otro puede servir contenido estático como HTML, CSS y JavaScript.

### Reglas L7

Los siguientes atributos se definen en una regla para evaluar el tráfico y se comparan con los valores definidos en la regla:

- Nombre de host: el nombre de host en la solicitud HTTP se compara con el parámetro value de la regla. Por ejemplo, “www.example-sports.com”.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- ruta: la parte de ruta del URI HTTP se compara con el parámetro de valor de la regla. Por ejemplo, “www.example-sports.com/shopping-cart/football_pump.html”
- file_type: La última parte del URI se compara con el parámetro value de la regla. Por ejemplo, txt, html, jpg, PNG, xls y otros.
- header: El encabezado definido en el parámetro clave se compara con el parámetro value en la regla.
- cookie: La cookie nombrada por el parámetro clave se compara con el parámetro de valor de la regla. El valor del campo del encabezado de la solicitud de la cookie contiene un par de información de nombre y valor almacenados para esa URL; la sintaxis general es la siguiente: Cookie: name=value. Por ejemplo, una regla que busca una cookie llamada “almacenes”con el valor que empieza por “football-“se verá así: Type = Cookie, compare_type=StartsWith, key = stores value = football-.

### Tipos de comparación

Al evaluar el tráfico, la directiva L7 compara las siguientes expresiones con los atributos definidos en la regla.

- regex: coincidencia de expresiones regulares de tipo Perl
- starts_with: Cadena que comienza con
- ends_with: La cadena termina en
- contiene: La cadena contiene
- equal_to: Cadena es igual a

> **Nota**
>
> El nombre de host, la ruta, el encabezado y los atributos de cookie admiten todos los tipos de comparación, pero el atributo file_type solo admite expresiones regulares y equal_to.

### Directivas L7

Una directiva L7 procesa el tráfico HTTP entrante y devuelve un valor “verdadero”cuando coinciden todas las reglas definidas en la directiva.

En cualquier directiva L7, todas las reglas se unen de forma lógica con un operador AND. Una solicitud debe cumplir con todas las reglas para que la directiva devuelva un valor “verdadero”. La acción que realiza el balanceador de cargas se basa en el valor devuelto por la directiva. Puede crear una segunda directiva con la misma acción para lograr una operación OR lógica entre las reglas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Por ejemplo, puede crear una directiva en la que la solicitud HTTP entrante pueda contener las palabras “EXAMPLE-SPORTS”, “SPORTS-FOOTBALL”o “EXAMPLE-FOOTBALL”, de modo que el balanceador de cargas tome las medidas adecuadas de reenviar estas solicitudes al grupo de servidores de la empresa de comercio electrónico de Example-Sports para ofrecer el contenido solicitado. Puede crear otra directiva que realice la misma acción pero que coincida con “ejemplo-deportes” , “ejemplo-deportes-fútbol”o “ejemplo-fútbol”. Cuando un usuario envía una solicitud HTTP con alguna de estas seis palabras clave, el balanceador de carga reenvía la solicitud al servidor Example-Sports.

Según las reglas definidas en la directiva, una directiva L7 puede realizar cualquiera de las siguientes acciones:

- Redirigir al grupo: reenvía la solicitud al grupo de servidores de aplicaciones identificado por las reglas asociadas a la directiva L7. Es decir, puede crear una regla de aplicación para dirigir las solicitudes a un grupo de balanceadores de carga específico según el nombre de dominio. Por ejemplo, puede crear una regla que dirija algunas solicitudes a example-football.com a pool_1 y otras solicitudes a example-sports-online_purchase.com a pool_2.
- Redirigir a URL: envía al cliente una respuesta HTTP de redireccionamiento en la que el encabezado de la respuesta de ubicación contenga la nueva ubicación. El navegador actualizará la barra de direcciones con la nueva ubicación y emitirá una nueva solicitud. Los casos de uso son muchos. Por ejemplo, si la dirección de un sitio web ha cambiado, puede redirigir las solicitudes a la nueva dirección en lugar de eliminarlas. O bien, durante el mantenimiento del sitio web, puede redirigir a los usuarios a un sitio de solo lectura.
- Rechazar: rechaza la solicitud y no realiza ninguna otra acción. Por ejemplo, puede devolver una respuesta 401 no autorizada para denegar el acceso a los usuarios de páginas web restringidas.

Una configuración de conmutación de contenido consiste en un servidor virtual de conmutación de contenido, una configuración de equilibrio de carga que consiste en servidores y servicios virtuales de equilibrio de carga y directivas de conmutación de contenido. Después de crear el servidor virtual y las directivas de conmutación de contenido, enlaza cada directiva al servidor virtual de conmutación de contenido. Al vincular la directiva al servidor virtual de conmutación de contenido, se especifica el servidor virtual de equilibrio de carga de destino. Cuando una solicitud llega al servidor virtual de conmutación de contenido, el servidor virtual aplica las directivas de conmutación de contenido asociadas a esa solicitud. La prioridad de la directiva define el orden en que se evalúan las directivas vinculadas al servidor virtual de conmutación de contenido.

Cualquier grupo que tenga el identificador de escucha se puede asignar como grupo predeterminado de servidores virtuales a los que se desvía el tráfico. El grupo está vinculado vagamente a un oyente y solo se asocia a un oyente mediante la implementación de una directiva L7. También se puede crear un grupo directamente debajo de un balanceador de carga sin estar necesariamente vinculado

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a un oyente. En tal caso, el grupo se crea en el estado “pending_create”. Como las directivas de L7 están estrechamente vinculadas a los oyentes, se debe crear e implementar una directiva de L7 que contenga el ID del grupo para que el grupo se vuelva “activo”y comience a recibir solicitudes de tráfico.

Varias directivas de L7 pueden prestar servicio a un grupo, pero permanece en estado “activo”si tiene al menos una directiva asociada. Cuando se elimina la última directiva, el grupo vuelve al estado “pending_create”hasta que se cree otra directiva y se asocie a ella. Si se elimina el grupo en sí, todas las solicitudes HTTP que de otro modo habría recibido se redirigen al grupo predeterminado.

**Asignación entre las políticas L7 de OpenStack y las entidades Citrix ADC**

| OpenStack | Entidad Citrix ADC | Descripción |
| --- | --- | --- |
| Directiva L7 con acción REDIRECT_TO_POOL | Directiva de cambio de contenido > Acción de cambio de contenido | Citrix ADM crea una directiva de conmutación de contenido que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de conmutación de contenido que especifica el grupo de servidores de aplicaciones de destino para la recuperación y presentación de contenido al usuario. |
| Directiva L7 con acción REDIRECT_TO_URL | Directiva de respuesta > Acción de respuesta | Citrix ADM crea una directiva de respuesta que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de respuesta que especifica la URL de destino que se presentará a los usuarios. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | | |
|---|---|---|
| Directiva L7 con acción RECHAZAR | Directiva de respuesta > Eliminar la solicitud | Citrix ADM crea una directiva de respuesta que está enlazada al servidor virtual de conmutación de contenido y asociada a una acción de respuesta que descarta la solicitud. |

Si la acción de una directiva L7 que se evalúa como «verdadera» redirige el tráfico a un grupo que está en estado «create_pending», Citrix ADM implementa el grupo especificado junto con un servidor virtual de equilibrio de carga. Citrix ADM crea una directiva de conmutación de contenido a partir de la directiva L7 y utiliza la acción de conmutación de contenido correspondiente para redirigir las solicitudes al servidor virtual de equilibrio de carga asociado a ese grupo. Si una segunda directiva L7 redirige al mismo grupo, Citrix ADM crea una directiva de conmutación de contenido y una acción de conmutación de contenido para redirigir el tráfico al servidor virtual de equilibrio de carga existente asociado al grupo.

**Posicionamiento político**

La evaluación de las directivas de nivel 7 en OpenStack está determinada por sus prioridades. En OpenStack, de forma predeterminada, a las directivas se les asignan prioridades en el orden en que se crean. La directiva que se creó primero lleva el número “1”y las directivas que se crean posteriormente se numeran consecutivamente. Sin embargo, puede cambiar las prioridades de las directivas y asignarles prioridades diferentes. Las directivas siempre se evalúan en el orden de sus prioridades. La primera directiva que coincide con una solicitud específica siempre se ejecutará primero.

Al crear directivas, tenga en cuenta los siguientes puntos:

- Si asigna a una nueva directiva la misma prioridad que a una directiva existente, la nueva directiva tendrá esa prioridad. Se reduce la prioridad de la directiva actual. Si es necesario, las prioridades de otras directivas también se reducen para mantener el orden en que se evalúan las directivas.
- Si crea una nueva directiva sin especificar una posición, la nueva directiva simplemente se agregará a la lista.
- Si crea una nueva directiva y le asigna una posición superior a la cantidad de directivas que ya figuran en la lista, la nueva directiva se anexará a la lista, es decir, la nueva directiva siempre tendrá la siguiente prioridad disponible. Por ejemplo, si hay tres directivas A, B y C con prioridades

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1, 2 y 3, y si crea una directiva y asigna una prioridad de 8, la prioridad de la nueva directiva pasa a ser 4.

- Si agrega una directiva a la lista o elimina una directiva de la lista, los valores de posición de la directiva se reordenan desde el 1 sin omitir los números. Por ejemplo, si la directiva A, B, C y D tienen valores de posición de 1, 2, 3 y 4, y si elimina la directiva B de la lista, la directiva C ahora toma la segunda posición y la directiva D toma la tercera posición.

En NetScaler ADM, siempre hay una directiva predeterminada asociada a una `csvserver` con una prioridad de 1. Esta directiva predeterminada especifica el número de conexiones TCP que `lbvserver` procesa un determinado punto de tiempo. Por lo tanto, cuando se crean las directivas de respuesta correspondientes y las directivas de conmutación de contenido en NetScaler ADC, siempre se les asigna una prioridad 1 mayor que la prioridad de la directiva L7 correspondiente. Por ejemplo, cuando se evalúa una directiva L7 con una prioridad de 1 y se crea una directiva de cambio de contenido con una prioridad de 2. Del mismo modo, cuando se evalúa una directiva L7 con una prioridad de 2 y se crea una directiva de respuesta con una prioridad de 3.

En OpenStack, primero se evalúa la directiva "rechazar"o "redirect_to_url"y, a continuación, se evalúa la directiva "redirect_to_pool". En una instancia de NetScaler ADC, las directivas de respuesta siempre se evalúan primero para descartar la solicitud o presentar al usuario una dirección web redirigida, y las directivas de cambio de contenido se evalúan en último lugar. Este orden de evaluación no suele causar ningún conflicto si las directivas de cambio de contenido y de respuesta se excluyen mutuamente. Es decir, dos directivas L7 no deben tener expresiones idénticas. Las expresiones derivadas se agregan en las directivas de cambio de contenido y respondedor para evitar tales conflictos. Por ejemplo, escribe una expresión para rechazar todas las solicitudes a "sports-football.com"y otra expresión para permitir las solicitudes a "example-sports-football.com" . Cree las directivas de L7 para que todas las directivas de respondedor para rechazar la solicitud se organicen en la parte superior de la lista de evaluación, seguidas de las directivas de respondedor para Web Direct, seguidas de las directivas de conmutación de contenido.

En NetScaler ADM, siempre hay una directiva predeterminada asociada a una `csvserver` con una prioridad de 1. Esta directiva predeterminada especifica el número de conexiones TCP que `lbvserver` procesa un determinado punto de tiempo. Por lo tanto, cuando se crean las directivas de respuesta correspondientes y las directivas de conmutación de contenido en NetScaler ADC, siempre se les asigna una prioridad 1 mayor que la prioridad de la directiva L7 correspondiente. Por ejemplo, cuando se evalúa una directiva L7 con una prioridad de 1 y se crea una directiva de cambio de contenido con una prioridad de 2. Del mismo modo, cuando se evalúa una directiva L7 con una prioridad de 2 y se crea una directiva de respuesta con una prioridad de 3.

En OpenStack, primero se evalúa la directiva "rechazar"o "redirect_to_url"y, a continuación, se evalúa la directiva "redirect_to_pool". En NetScaler ADC, las directivas de respuesta siempre se evalúan primero para descartar la solicitud o presentar al usuario una dirección web redirigida, y las directivas de cambio de contenido se evalúan en último lugar. Este orden de evaluación no suele

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

causar ningún conflicto si las directivas de cambio de contenido y de respuesta se excluyen mutuamente. Es decir, no hay dos directivas L7 que tengan expresiones similares. Se agregan expresiones derivadas similares en las directivas de respuesta y cambio de contenido para evitar tales conflictos. Por ejemplo, escribe una expresión para rechazar todas las solicitudes a "sports-football.com"y otra expresión para permitir las solicitudes a "example-sports-football.com". Cree las directivas de L7 para que todas las directivas de respondedor para rechazar la solicitud se organicen en la parte superior de la lista de evaluación, seguidas de las directivas de respondedor para Web Direct, seguidas de las directivas de conmutación de contenido.

### Tareas de configuración

Las implementaciones de directivas y acciones del L7 se realizan mediante los comandos LBaaS de Neutron.

Configure las variables de entorno en OpenStack y cree el balanceador de carga (por ejemplo, LB1). Una vez creado correctamente el balanceador de cargas, cree el oyente y los grupos (por ejemplo, L1, P1 y P2) y agregue miembros y monitores a los grupos. Por ejemplo, P1 es el grupo predeterminado para L1, mientras que P2 es el grupo vinculado a LB1 y que administra los servidores de aplicaciones.

Para obtener más información sobre cómo configurar LBaaS V2 mediante la línea de comandos, consulte Configuración de LBaaS V2 mediante la línea de comandos.

Los siguientes comandos crean las directivas y definen las acciones específicas:

**Crear directiva L7 para eliminar solicitudes**

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```

**Ejemplo**:

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

El comando anterior crea y vincula la policy11, una directiva de respuesta, al servidor de conmutación de contenido para rechazar las solicitudes. Como no se creó ninguna regla para esta directiva, la directiva se evalúa como "falsa"y la solicitud se rechaza.

**Crear una directiva L7 para redirigir solicitudes a una URL determinada**

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

**Ejemplo**:

neutron lbaas-l7policy-create –name policy12 –action REDIRECT_TO_URL –listener admin-list1 –redirect-url `http://example-sports/about-us.html`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El comando anterior crea una acción de respuesta para redirigir las solicitudes a una dirección URL, crea una directiva de respuesta con acción y vincula esta directiva al servidor virtual de conmutación de contenido.

```
neutron lbaas-l7rule-create --type HOST_NAME --compare-type CONTAINS --value <value-string> <L7 policy name>

neutron lbaas-l7rule-create --type PATH --compare-type CONTAINS --value <value-string> <L7 policy name>
```

Las dos reglas anteriores se pueden conectar con un operador AND para derivar la expresión de la directiva de respuesta.

**Crear una directiva L7 para redirigir solicitudes a un grupo**

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <listener name> --action <action-name> --redirect-pool <redirect-pool>
```

**Ejemplo**:

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

Si esta es la primera directiva de L7, el comando anterior implementa P2 junto con LB1, crea la acción de redireccionamiento de cambio de contenido y redirige las solicitudes a LB1. Si P2 ya existe, el comando crea la acción de redirección de conmutación de contenido y redirige las solicitudes a LB1.

## Provisioning manual de la instancia NetScaler ADC VPX en OpenStack

January 30, 2024

En algunas redes empresariales, las instancias de NetScaler ADC VPX no se pueden conectar a Citrix License Server para descargar automáticamente las licencias, por motivos de seguridad. En este caso, debe implementar manualmente instancias de NetScaler ADC VPX en la plataforma OpenStack. Con el código de acceso de licencia que ha recibido de Citrix, descargue la licencia NetScaler ADC VPX apropiada y guárdela en su sistema local.

**Para aprovisionar manualmente la instancia NetScaler ADC VPX en OpenStack:**

1. Instale el software Citrix ADC Driver y registre Citrix Application Delivery Management (ADM) en OpenStack

   a) En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Haga clic en **Configurar los ajustes de OpenStack.** En la página **Configurar opciones de OpenStack** , puede establecer los parámetros para configurar OpenStack en Citrix ADM. Aquí tiene dos opciones: **Predeterminado** y **Personalizado**.

c) Seleccione **Predeterminado**si los servicios de OpenStack se ejecutan en los puertos predeterminados.

2. **Vaya a**Orquestación > Orquestación****en la nube** > **OpenStack**y haga clic en Configuración de implementación.**

   a) **Red**de administración : seleccione la red de administración en OpenStack a la que está conectado el Citrix ADC VPX de aprovisionamiento automático.

   b) **Nombre del perfil**: Seleccione el perfil en la lista desplegable. NetScaler ADM utiliza la contraseña contenida en este perfil para configurar nuevas instancias de NetScaler ADC VPX aprovisionadas automáticamente.

   c) Imagen de Citrix ADC VPX de un vistazo: seleccione la imagen de Citrix ADC VPX disponible en OpenStack Glance que se utiliza para crear una instancia de Citrix ADC VPX. La lista desplegable mostrará solo las imágenes que están presentes en OpenStack Glance.

3. En Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **OpenStack** > **Service Packages** y, a continuación, haga clic en **Agregar**.

4. En la página **del paquete de servicios**, especifique los siguientes parámetros:

   a) **Nombre**: nombre del paquete de servicios. Por ejemplo, escriba SVC-PKG-GOLD.

   b) **Asignación**de instancias de Citrix ADC : seleccione **Dedicada** o **Particionada** como el tipo de asignación de instancias definido en el paquete de servicios.

   c) **Provisioning**de instancias de Citrix ADC : seleccione **Create Instance OnDemand** para crear instancias de Citrix ADC durante la propia configuración.

   d) **Plataforma de aprovisionamiento automático**: Seleccione **OpenStack Compute**. De forma predeterminada, se seleccionará Citrix ADC VPX como tipo de instancia.

   e) **Asigne arrendatarios de OpenStack y directivas de ubicación**: en la sección Arrendatarios de OpenStack, haga clic en **Agregar**y seleccione el arrendatario.

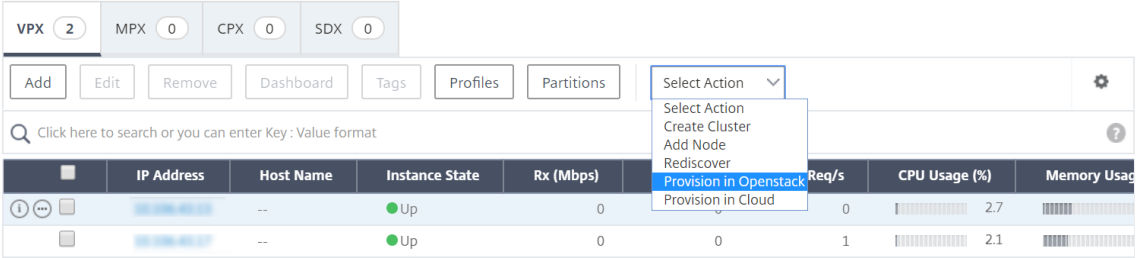
   f) Haga clic en **Continue** y, a continuación, en **Done**.

5. Vaya a **Sistema** > **Administración del sistema** > **Cambiar configuración del sistema** y seleccione **http** en la lista desplegable.

6. Vaya a **Redes** > **Instancias** > **Citrix ADC VPX** .

7. En la página **NetScaler ADC VPX**, haga clic en la lista desplegable **Administrador** y seleccione **Aprovisionar dispositivo**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




a) En la página **Provisioning de dispositivos**, escriba el nombre del dispositivo y seleccione el paquete de servicio que creó en el paso anterior.

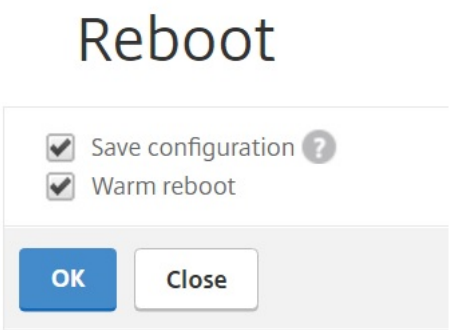
b) Haga clic en **Aceptar**.

8. **Vaya a la ficha**Orquestación > Orquestación****en la nube**>**OpenStack > Solicitudes**.** Seleccione la solicitud y haga clic en **Tareas** para ver las tareas. Cuando el estado de la tarea cambia a **Finalizado**, significa que NetScaler ADC VPX se aprovisiona en NetScaler ADM.

9. Vaya a **Redes** > **Instancias** > **Citrix ADC VPX** para comprobar que la instancia de Citrix ADC VPX aparece en la página Citrix ADC VPX.

10. Haga clic en la instancia de NetScaler ADC VPX. Cuando la instancia de NetScaler ADC VPX se abra en la ventana del explorador, inicie sesión en la instancia. Vaya a **Configuración** > **Sistema** > **Licencias** y agregue manualmente la nueva licencia. Para obtener más información sobre cómo agregar una nueva licencia, consulteDescripción general de licencias de NetScaler ADC.

11. Reinicie la instancia de NetScaler ADC VPX.




12. Después de unos minutos, puede iniciar sesión en OpenStack y, en**System** >**Instancias**, puede ver que la instancia de NetScaler ADC VPX se implementa en OpenStack.

13. Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente de Neutron y ejecute las tareas de configuración. Para obtener más información sobre cómo ejecutar comandos de configuración, consulteConfiguración de LBaaS V2 mediante la línea de comandos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Aprovisionamiento de la instancia NetScaler ADC VPX en OpenStack mediante StyleBook

January 30, 2024

En el flujo de trabajo de orquestación de OpenStack, NetScaler Application Delivery Management (ADM) ahora utiliza `os-cs-lb-mon` StyleBook para implementar configuraciones de LBAAS en instancias de NetScaler ADC asignadas al arrendatario OpenStack. Se crea un paquete de configuración para cada equilibrador de carga creado por el usuario de OpenStack.

El uso de StyleBooks para la configuración en un flujo de trabajo de OpenStack proporciona las siguientes ventajas:

- Mejor visualización viendo todos los objetos de configuración.
- Fiabilidad a través de la reversión.
- Compatibilidad con varios tipos de instancias de NetScaler ADC (NetScaler ADC HA, particiones, VPX, CPX, MPX y otros).
- Personalización mediante el uso de sus propios StyleBooks para implementar la configuración de los arrendatarios de OpenStack.

Como administrador de NetScaler ADM, vaya a **Aplicaciones** > **Configuraciones** para ver el paquete de configuración implementado en la instancia de NetScaler ADC.
Puede realizar las siguientes tareas:

- Desplácese para ver el paquete `os-cs-lb-mon` de configuración implementado para el equilibrador de carga.
- Haga clic en **View Definition** en el panel `os-cs-lb-mon` StyleBook para comprobar la configuración implementada en las instancias.
- Haga clic en **Ver objeto** para ver la lista de objetos o entidades de NetScaler ADC implementados en las instancias.

## Puntos a tener en cuenta antes de Provisioning instancias mediante StyleBooks

A partir de la versión 49.23 de Citrix ADM 12.1, se ha actualizado la arquitectura de un flujo de trabajo de orquestación de OpenStack. El flujo de trabajo utiliza ahora los StyleBooks de Citrix ADM para configurar instancias de Citrix ADC. Si va a actualizar a Citrix ADM 12.1 compilación 49.23 desde la versión 12.0 o desde la versión 12.1 compilación 48.18, debe ejecutar la siguiente script de migración:

```
/mps/scripts/migration_scripts/migrate_configurations.py
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- La ejecución del script de migración crea paquetes de configuración del `os-cs-lb-mon` StyleBook correspondientes a las configuraciones existentes de OpenStack.
- La ejecución de este script de migración es obligatoria si tenía configuraciones de OpenStack implementadas a partir de estas compilaciones anteriores.
- Puede implementar nuevas configuraciones en las instancias mediante `os-cs-lb-mon` StyleBook solo después de ejecutar el script de migración desde la versión 12.1, compilación 49.23.
- Todas las configuraciones intentadas desde OpenStack fallan hasta que se ejecuta el script de migración.

> **Nota**
>
> - Una vez que ejecute el script de migración, no podrá volver a la versión anterior de NetScaler ADM.
> - Asegúrese de que ha actualizado los controladores NetScaler ADC para OpenStack LBaaS V2 a la versión más reciente. Utilice los archivos del paquete Citrix ADC que se proporcionan junto con la última versión de Citrix ADM 13.0.

Las implementaciones de la API LBaaS V2 se realizan a través de comandos LBaaS de Neutron. Conéctese a cualquier cliente Neutron y ejecute las tareas de configuración. Para obtener más información sobre cómo ejecutar comandos de configuración, consulteConfiguración de LBaaS V2 mediante la línea de comandos.

## Licencia de check-in y check-out VPX y soporte de licencias agrupadas para el entorno OpenStack

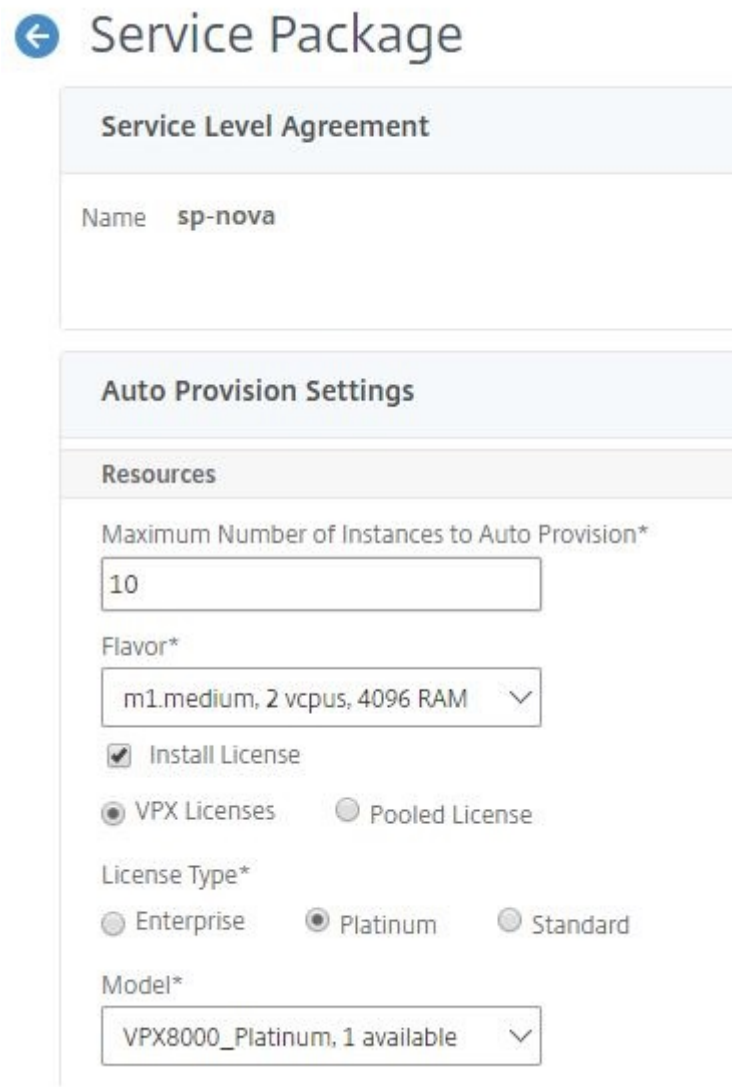
January 30, 2024

En el flujo de trabajo de orquestación de OpenStack, Citrix Application Delivery Management (ADM) crea instancias de Citrix ADC VPX bajo demanda al seleccionar el paquete de servicios con **OpenStack Compute**. Ahora, la página del paquete de servicios de la función Orchestration de Citrix ADM está mejorada para proporcionar la licencia necesaria para instalarse en las instancias de Citrix ADC VPX que se crean bajo demanda. Las licencias proporcionadas pueden ser licencias de registro y salida VPX o licencias agrupadas.

Para utilizar esta función, primero debe cargar las licencias en Citrix ADM y, a continuación, crear paquetes de servicios que utilicen OpenStack Compute.

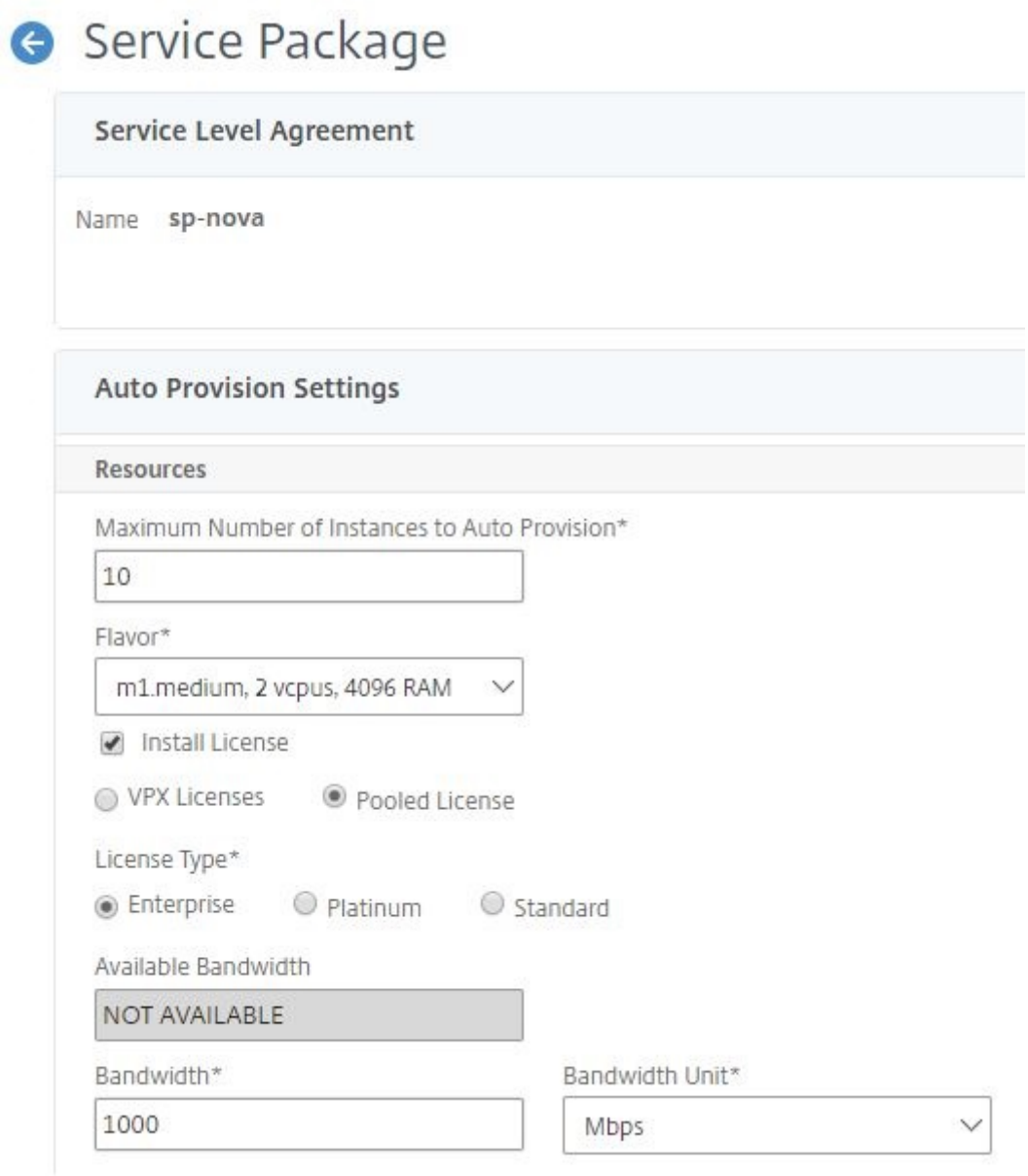
- Si se trata de una licencia de check-in y check-out, puede elegir la licencia que se va a instalar entre las distintas licencias disponibles.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




- Si se trata de una licencia de grupo, puede seleccionar tanto el ancho de banda como el tipo de edición de licencia que se va a instalar.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Cada vez que implementa el primer equilibrador de carga con NetScaler ADM como proveedor, NetScaler ADM crea la instancia NetScaler ADC VPX e instala la licencia especificada en el paquete de servicio en la instancia recién creada.

Además, cuando eliminas una instancia de equilibrio de carga existente, esa instancia ya no es necesaria. La instancia se retira del servicio y la licencia se devuelve a Citrix ADM. Esto permite un uso óptimo de las licencias disponibles en Citrix ADM.

> **Nota**
>
> Cuando Citrix ADM se implementa en modo de alta disponibilidad, tenga en cuenta que las licencias se cargan en el Citrix ADM principal o activo actual, MAS-HA-1. Cuando implementa la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

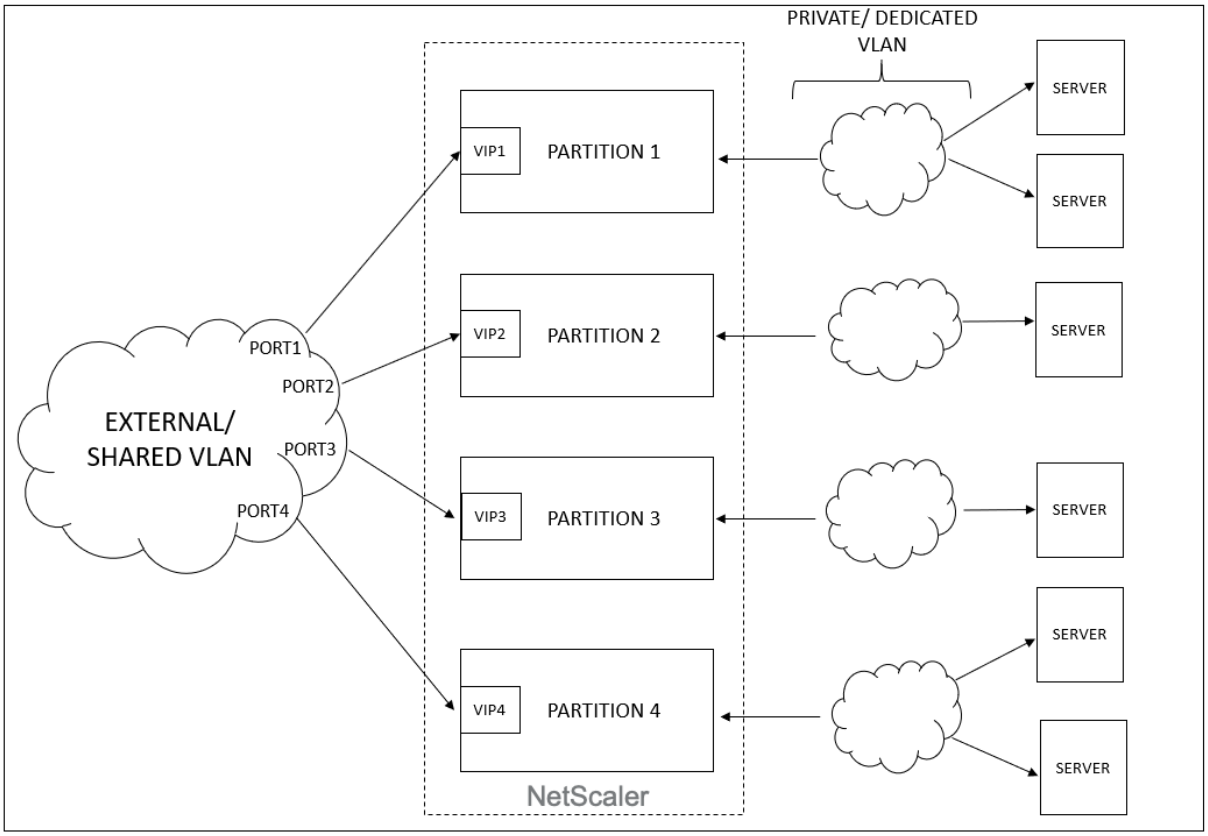
> primera solicitud y Citrix ADM crea las instancias de Citrix ADC VPX, la instancia comprueba las licencias necesarias de MAS-HA-1. En un momento posterior, suponga que el dispositivo secundario de NetScaler ADM, MAS-HA-2, que no tiene las licencias, está activo ahora. La instancia ADC VPX no puede extraer la licencia de MAS-HA-2 ahora y, por lo tanto, la instancia no se puede crear para usuarios nuevos.
>
> En tal caso, asegúrese de que el MAS-HA-1 esté activo y que ahora sea el nodo principal actual. Es decir, conmute por error manualmente el Citrix ADM de MAS-HA-2 a MAS-HA-1. Después de esto, debe volver a intentar la configuración de OpenStack y las instancias se volverán a crear con las licencias adecuadas. Para obtener más información sobre la compatibilidad con licencias en la implementación de alta disponibilidad de NetScaler ADM, consulte Alta disponibilidad.

## Compatibilidad con VLAN compartida para particiones de administración

January 30, 2024

Para los inquilinos que se conectan desde redes privadas, Citrix Application Delivery Management (ADM) admite la política de aislamiento para que cada inquilino tenga su propia partición dedicada, una VLAN dedicada y servidores dedicados. Para los arrendatarios que se conecten desde redes públicas, una VLAN dedicada requerirá el uso de demasiadas direcciones IP. Una VLAN compartida evita este problema creando una dirección IP virtual en cada partición, creando así una única subred IP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Cuando un arrendatario configura un VIP o un listener, se crea una partición admin en el dispositivo NetScaler ADC para ese arrendatario. Toda la configuración del balanceador de carga se envía a la partición de administración que se ha creado. Si el arrendatario utiliza una red compartida o una red externa para crear un balanceador de carga, se agrega la VLAN de esa red y se habilita la función de uso compartido. Cuando otro inquilino utiliza la misma red compartida para crear su balanceador de carga, la VLAN no se vuelve a agregar al Citrix ADC, sino que también se enlaza a la segunda partición. Por lo tanto, cualquier arrendatario que utilice la misma red compartida obtiene una partición enlazada a la misma VLAN.

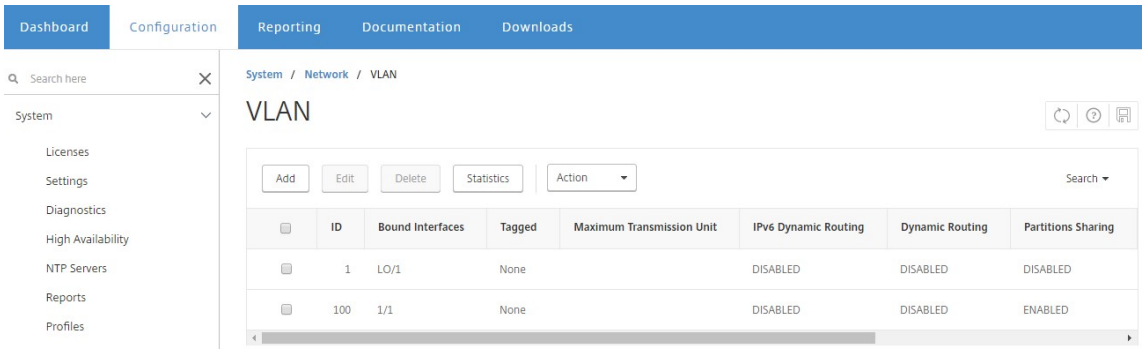
El Citrix ADM admite la dirección MAC de destino virtual. Cuando los inquilinos comparten una VLAN, Citrix ADM asigna diferentes direcciones MAC a la partición del dispositivo Citrix ADC. Esto permite compartir una VLAN entre particiones o entre todos los arrendatarios y todos los dominios de tráfico.

### Configuración de una VLAN compartida desde una instancia de Citrix ADC

1. En una instancia de Citrix ADC, vaya a **Configuración** > **Sistema** > **Red** > **VLAN**, seleccione un perfil de VLAN y haga clic en **Editar** para establecer el parámetro de partición compartida.
2. En la página **Configurar VLAN**, active la casilla **Compartir particiones**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

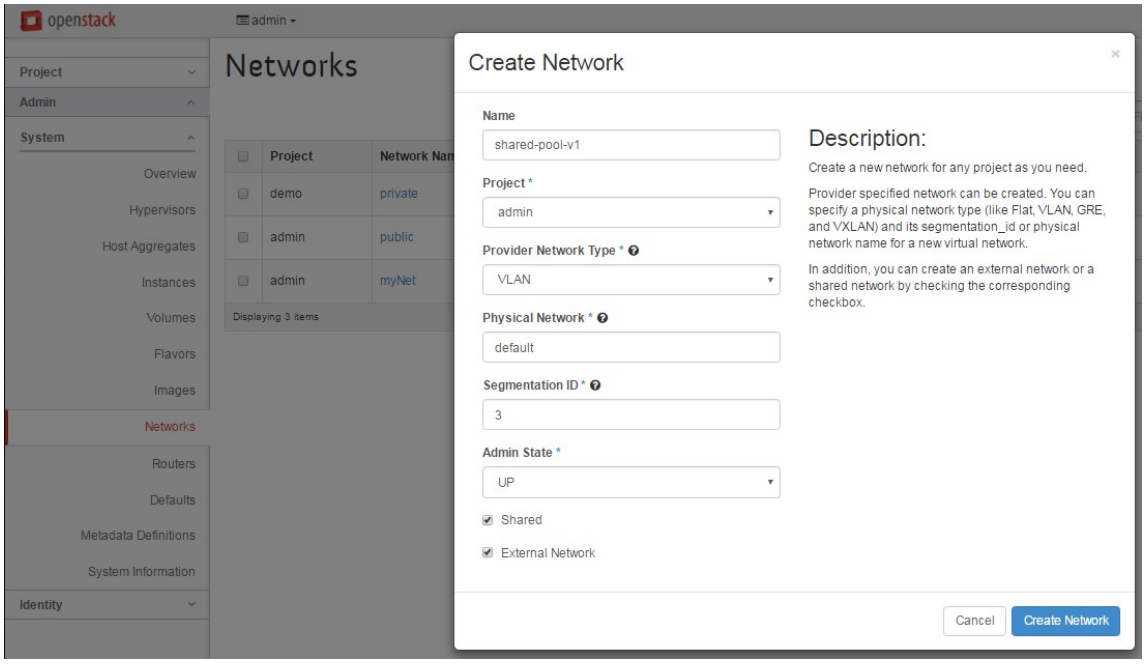
3. Haga clic en **Aceptar**.




## Configuración de VLAN compartida desde OpenStack Orchestration

1. En OpenStack, vaya a **Administración** > **Sistema** > **Redes**y, a continuación, haga clic en **Crear red**.
2. En **Crear red**, defina los siguientes parámetros:
   a) Nombre: introduzca el nombre de la red
   b) Proyecto: seleccione un proyecto de la lista desplegable
   c) Tipo de red del proveedor: seleccione **VLAN** en la lista desplegable. Esto define que la red virtual se establece como VLAN.
   d) Red física: aquí se selecciona la red física predeterminada. Puede modificar esto.
   e) Estado de administrador: de forma predeterminada, el estado administrativo de la red es ACTIVADO
   f) Seleccione Red **compartida** y **externa** para definir que la VLAN es compartida y utiliza una red externa.
3. Haga clic en **Crear red**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Flujo de trabajo de licencias de prueba

January 30, 2024

Durante el aprovisionamiento automático de la instancia de NetScaler ADC VPX mediante la orquestación de OpenStack, NetScaler Application Delivery Management (ADM) utiliza OpenStack Compute para iniciar una instancia de NetScaler ADC VPX. La instancia de NetScaler ADC VPX recién aprovisionada se pone en contacto con el portal de licencias de Citrix durante la configuración y utiliza el código de acceso de licencia para descargar e instalar automáticamente los archivos de licencias.

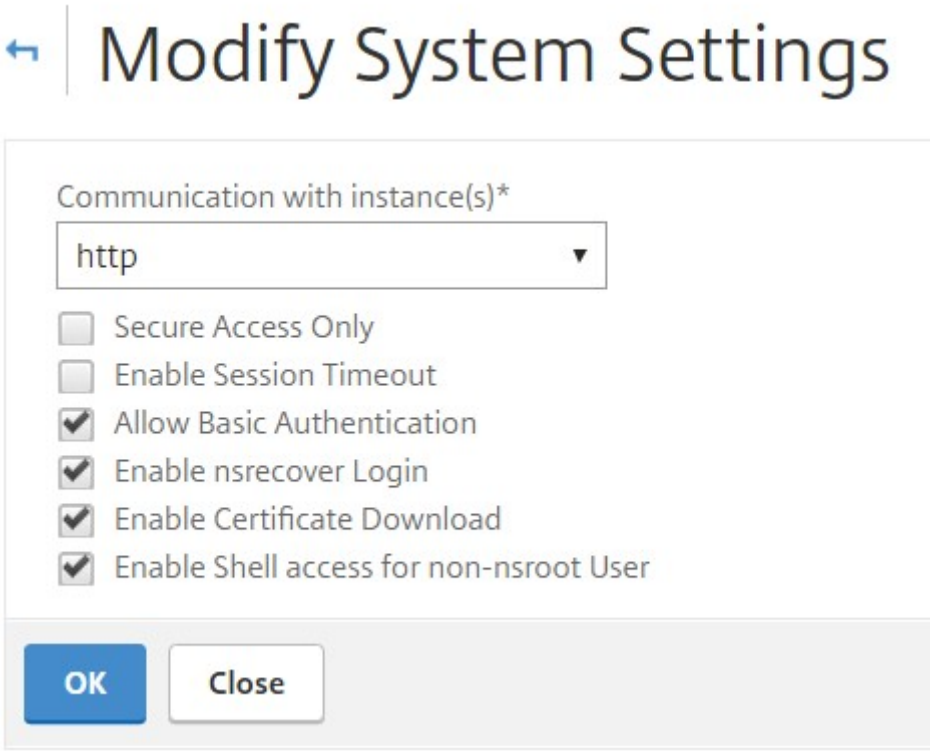
### Licencias de prueba

El personal de soporte técnico utiliza licencias de prueba cuando instala dispositivos Citrix ADM y Citrix ADC VPX in situ. Una licencia de prueba o evaluación para Citrix ADC VPX es válida durante 90 días. Si es necesario evaluar más de un Citrix ADC o extender las pruebas después de 90 días, se debe solicitar una nueva licencia de evaluación. En lugar de la instalación automática de los archivos de licencias de prueba, Citrix ADM le ofrece una solución alternativa. Puede descargar manualmente los archivos de licencia e instalarlos en Citrix ADC VPX para completar la instalación de la instancia.

Si el Citrix ADC VPX no puede conectarse a Internet, configure Citrix ADM para que actúe como servidor proxy para el portal de licencias de Citrix e instale los archivos de licencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Las instancias de Citrix ADC VPX que tienen una licencia de prueba solo pueden comunicarse con Citrix ADM en HTTP. Para configurar la comunicación HTTP en Citrix ADM, vaya a **Sistema** > **Administración del sistema** y haga clic en **Cambiar la configuración del sistema** . Seleccione **http** en la lista desplegable para establecer el método de comunicación y haga clic en**Aceptar**.




## Integración con los servicios de OpenStack Heat

January 30, 2024

OpenStack Neutron LBaaS permite servicios de equilibrio de carga central, como equilibrio de carga, descarga SSL y conmutación de contenido, para aplicaciones. LBaaS se administra a través de una API REST, y la API permite a los arrendatarios realizar llamadas REST para crear, actualizar y eliminar objetos LBaaS. Dado que LBaaS proporciona servicios de equilibrio de carga, no permite el uso de las funciones más avanzadas de NetScaler ADC durante el proceso de orquestación. El complemento Citrix ADC Heat supera esta limitación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Servicio de orquestación de calor

El servicio de orquestación térmica de OpenStack permite la implementación de aplicaciones en la nube complejas sobre la base de plantillas. La plantilla de orquestación térmica (HOT) describe la infraestructura de una aplicación en la nube en archivos de texto que los humanos pueden leer y escribir, y que pueden gestionarse mediante herramientas de control de versiones. YAML, un lenguaje estructurado, se utiliza para escribir estas plantillas. La plantilla HOT permite crear la mayoría de los tipos de recursos de OpenStack y especifica las relaciones entre los recursos definidos en ella. El complemento Citrix ADC Heat permite configurar las funcionalidades avanzadas del controlador de entrega de aplicaciones (ADC) en cualquier instancia de Citrix ADC.

### Libros de estilo Citrix ADC

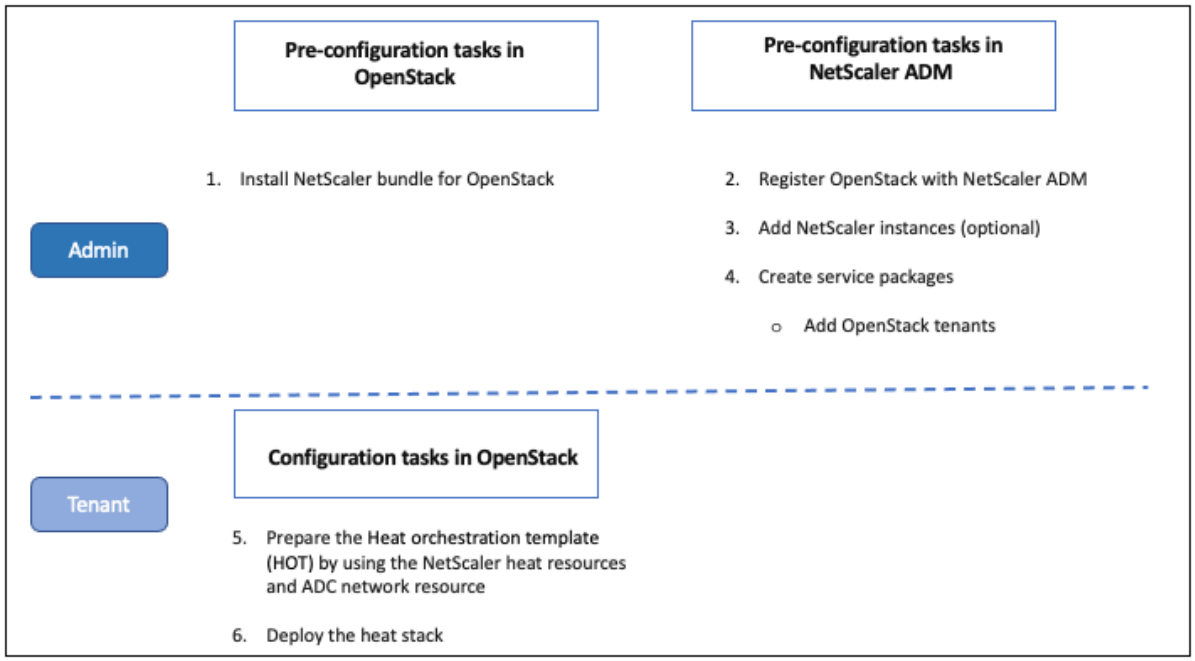
Los StyleBooks de Citrix Application Delivery Management (ADM) se pueden utilizar para crear y configurar las funcionalidades de Citrix ADC. Al igual que las plantillas de Heat, los StyleBooks también están escritos en YAML. Se pueden crear StyleBooks independientes para cada funcionalidad y se puede usar un único StyleBooks para implementar configuraciones en varias instancias de Citrix ADC.

Durante la integración de Citrix ADC con OpenStack, Citrix ADM publica todos los StyleBooks de Citrix ADM como recurso en el servicio Heat. Esto incluye tanto los StyleBooks que se envían con Citrix ADM como los StyleBooks que crea el usuario en un momento posterior. La plantilla Heat le permite configurar las funciones avanzadas de los ADC de Citrix mediante estos recursos de StyleBooks.

### Flujo de trabajo para configurar instancias de Citrix ADC mediante Heat

El siguiente diagrama de flujo ilustra el flujo de trabajo para implementar el Heat Stack:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Realice las siguientes tareas como administrador de la nube:

**Para configurar los servicios de calefacción en OpenStack:**

1. Descargue los paquetes Citrix ADC para OpenStack

   Instale los paquetes Citrix ADC en OpenStack. En Citrix ADM, vaya a **Descargas** y descargue los paquetes de controladores Citrix ADC, descomprima los paquetes y copie el contenido de la carpeta Heat del paquete en el directorio de recursos del motor Heat de OpenStack. La ruta del directorio es la siguiente:

   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. Cree una sección "netscaler_plugin"en el archivo heat.conf y actualice los siguientes parámetros en esa sección:

   [netscaler_plugin]

   a) Cuando la comunicación es HTTP, los parámetros se actualizan de la siguiente manera:

      NMAS_BASE_URI=<http://10.146.103.45:80>

      NMAS_USERNAME=

      NMAS_PASSWORD=

   b) Cuando la comunicación es https, los parámetros se actualizan de la siguiente manera:

      NMAS_BASE_URI=https://common_name_used_in_certificate

      NMAS_USERNAME=<openstack_driver_username

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH=<path_of_the_certificate_file>

Si el usuario establece ssl_cert_verify en «False», Citrix ADM envía verify=False en las llamadas de solicitud, lo que inhabilita la validación del certificado SSL. Si ssl_cert_verify se establece en «True» y la entrada cert_file_path está presente, Citrix ADM envía esta ruta en el parámetro verify de la solicitud; de lo contrario, Citrix ADM envía Verify=true.

> **Nota**
>
> Para implementar NetScaler ADM en modo "Alta disponibilidad", actualice los siguientes parámetros en el archivo heat.conf:
>
> NMAS_BASE_URI= <IP address of the front-end virtual server>

3. Reinicie el servicio Heat en OpenStack.

   Al reiniciar los servicios Citrix ADC Heat en OpenStack, todos los StyleBooks Citrix ADM definidos se importan a Heat como recursos. Además, el recurso de red Citrix ADC y el recurso de certificado se importan a OpenStack como recursos Citrix ADC Heat.

4. Registre Citrix ADM en OpenStack.

   a) En Citrix ADM, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** y haga clic en **Configurar opciones de OpenStack**.

   b) En la página **Configurar los ajustes de OpenStack**, puede establecer los parámetros para configurar OpenStack. Aquí tiene dos opciones: Predeterminado y Personalizado.

   c) Seleccione **Predeterminado** si los servicios de OpenStack se ejecutan en los puertos predeterminados. Introduzca los parámetros siguientes:

      i. Dirección IP del controlador OpenStack

      ii. Nombre de usuario del administrador

      iii. Contraseña

      iv. Arrendatario de administrador de OpenStack

      v. Controlador Citrix ADC y contraseña de Heat

      > **Nota**
      >
      > Esta es la misma contraseña (NMAS_PASSWORD) que introdujo en el archivo heat.conf.

5. Cree paquetes de servicios y defina los SLA con su arrendatario.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Se crea un inquilino en Citrix ADM para cada usuario durante el registro de OpenStack, y tanto el controlador LBaaS como el complemento Heat utilizan la información del inquilino. El complemento Heat utiliza esta información para ponerse en contacto con NetScaler ADM para importar StyleBooks como recursos de Heat en OpenStack.

> **Nota**
>
> Para obtener más información sobre la creación de paquetes de servicios y otras tareas previas a la configuración en NetScaler ADM y OpenStack, consulte Integración de NetScaler ADM con OpenStack Platform.

6. Observe que todos los StyleBooks relevantes de NetScaler ADM se importan a OpenStack Heat como recursos. Además, observe que el recurso de red NetScaler ADC y el recurso de certificado NetScaler ADC se importan a OpenStack Heat como recursos.

> **Nota**
>
> Actualmente, solo puede usar los StyleBooks que se envían con Citrix ADM.

Su arrendatario ahora puede crear la plantilla de Heat en OpenStack, introducir los valores de los parámetros de Heat requeridos e implementar la pila de calor. Cuando se implementa la pila Heat, la configuración se envía a Citrix ADM y se configuran las instancias de Citrix ADC necesarias.

**Para preparar la plantilla Heat e iniciar Heat Stack:**

1. En OpenStack, el arrendatario puede crear una plantilla de orquestación de calor (HOT) mediante los recursos de Heat.
2. En OpenStack Horizon, el administrador del arrendatario puede ir a **Proyecto** > **Orquestación** > **Pilas para crear la plantilla Heat e iniciar la Heat Stack**. Hay dos formas de crear HOT:
   - **Archivo**: Seleccione la plantilla actualizada del directorio local
   - **Entrada directa**: Copia y pega el contenido de YAML de la plantilla en la ventana

> **Nota:**
>
> Después de implementar correctamente la pila, el arrendatario puede actualizarla mediante la plantilla de cambio de pila. Sin embargo, la información de subred y la dirección IP virtual (VIP) que se proporcionaron inicialmente durante la creación de la pila no se pueden modificar.

Una vez que el inquilino implemente la pila, vaya a **Orchestration** > **Cloud Orchestration** > **OpenStack** > **Requests** in Citrix ADM para observar las listas de tareas. Además, vaya a**Aplicaciones** >**Configuración** en NetScaler ADM para observar que las instancias de NetScaler ADC se configuran correctamente en forma de paquetes de configuración de StyleBooks.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo de un NetScaler ADM StyleBooks:**

La siguiente imagen muestra un ejemplo de cómo se construye un NetScaler ADM StyleBooks y explica brevemente los componentes. Para obtener más información sobre NetScaler ADM StyleBooks y cómo usar los StyleBooks enviados, consulte StyleBooks.

```
name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
   -
      namespace: netscaler.nitro.config
      prefix: ns
      version: "10.5"
parameters:
       -
      name: name
      type: string
      required: true
      -
      name: ip
      type: ipaddress
      required: true
     -
      name: lb-alg
      type: string
      allowed-values:
        - ROUNDROBIN
        - LEASTCONNECTION
      default: ROUNDROBIN
components:
   -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
          name: $parameters.name
          servicetype: HTTP
          ipv46: $parameters.ip
          port: 80
          lbmethod: $parameters.lb-alg
```

header

StyleBooks imported

parameters

components

**Un ejemplo de plantilla de calor:**

La siguiente imagen muestra la estructura de una plantilla de calor definida en YAML y señala los recursos de StyleBooks y NetScaler ADC que se importan como recursos de calor.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
    - allowed_values: [HTTP, SSL, TCP, UDP, ANY]
    default: HTTP
    description: This is lb-service-type
    label: Service-type
    type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for_each:
            ipvar%: {get_param: server_ips}
          template:
            ip: ipvar%
            port: {get_param: server_port}
    type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator
```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

Para obtener más información sobre los servicios de Heat y cómo crear plantillas, consulte ladocumentación de OpenStack Heat.

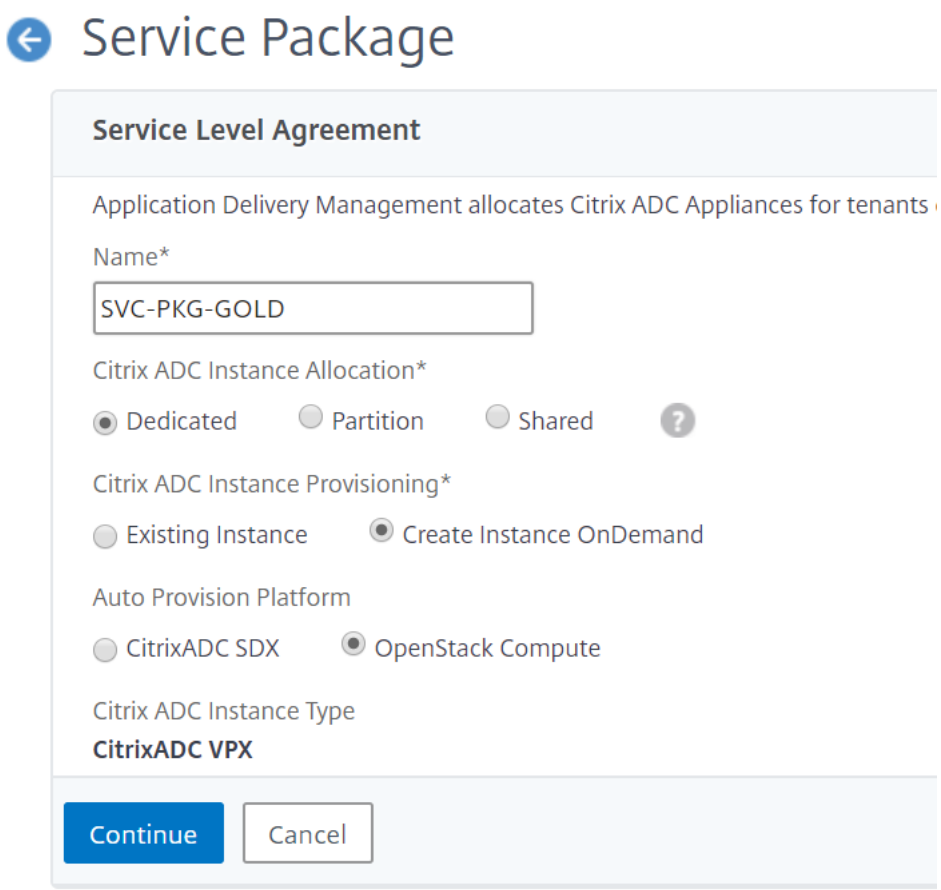
## Directivas de aislamiento de paquetes de servicio

January 30, 2024

### Directiva de aislamiento dedicada

A cada inquilino asociado al paquete de servicios Citrix Application Delivery Management (ADM) de una política dedicada se le asigna una instancia de Citrix ADC de entre las instancias que forman parte de este paquete de servicios. Esta instancia de NetScaler ADC asignada no se comparte con otros arrendatarios.

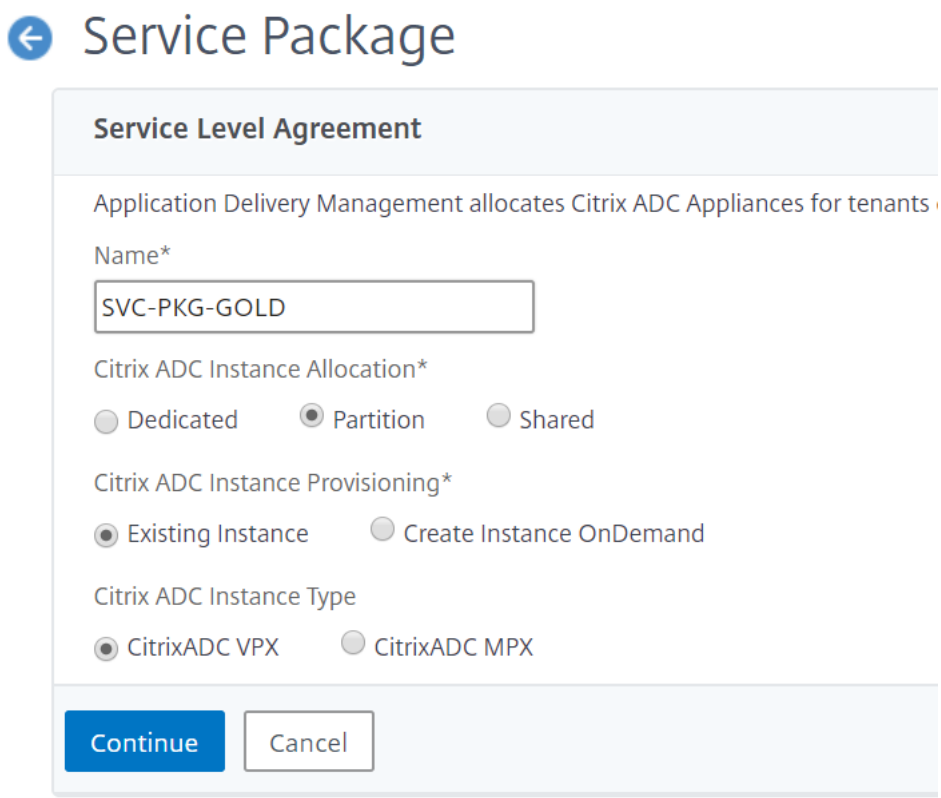
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Directiva de aislamiento de particiones

A cada arrendatario asociado al paquete de servicios de la directiva de partición se le asigna una partición de administración lógica dedicada de una instancia NetScaler ADC que forma parte del paquete de servicios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

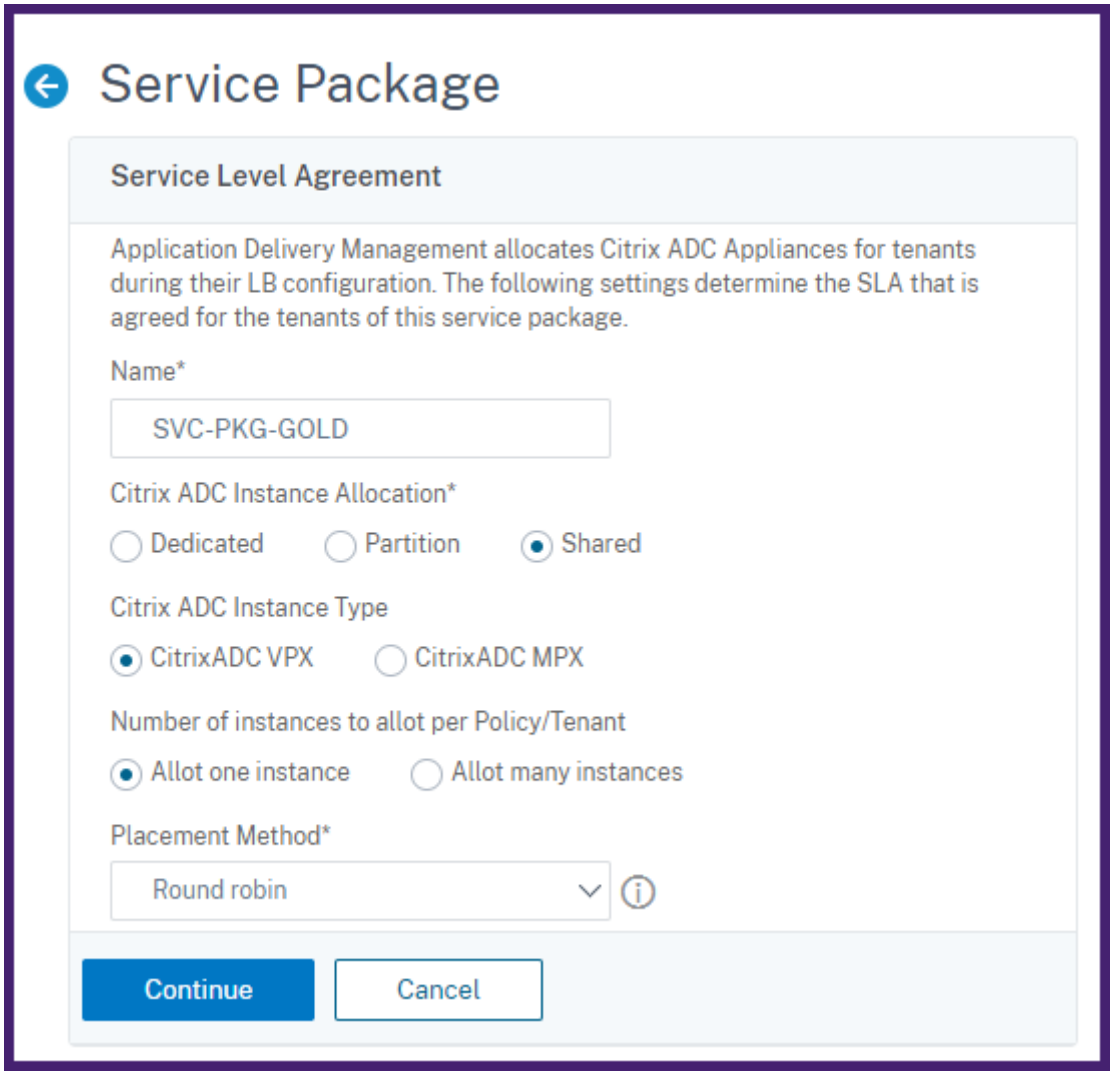



### Directiva de aislamiento compartido

Los inquilinos asociados al paquete de servicios comparten las instancias de Citrix ADC que forman parte del paquete de servicios. Todas las configuraciones de un inquilino se asignan a una instancia de Citrix ADC. En este modo, las configuraciones de varios inquilinos se pueden alojar en la misma instancia de Citrix ADC. Puede seleccionar **Citrix ADC VPX** o **Citrix ADC MPX** como tipo de dispositivo. Puede optar por asignar solo una instancia de Citrix ADC o varias instancias al paquete de servicios. Es decir, varios inquilinos pueden compartir una o varias instancias virtuales del dispositivo Citrix ADC.

> **Nota**
>
> Agregue instancias de NetScaler ADC SDX en los paquetes de servicios como instancias de NetScaler ADC VPX solamente, ya que un NetScaler ADC SDX tiene un NetScaler ADC VPX aprovisionado en él.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> También puede crear directivas de ubicación flexibles, en las que las directivas no solo se basen en el nombre o el ID del arrendatario, sino también en otros atributos personalizados. Para obtener más información sobre las directivas de ubicaciónflexible, consulte Asignación flexible de dispositivos basada en directivas.

## Asignación flexible de dispositivos basada en directivas

January 30, 2024

Citrix Application Delivery Management (ADM) asigna instancias virtuales de Citrix ADC a los arrendatarios, según los SLA acordados con los arrendatarios. La asignación de instancias virtuales a los

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

arrendatarios crea una relación de uno a uno entre la instancia y el arrendatario, en la que solo se puede asignar un arrendatario a un paquete de servicios en el centro de datos.

En algunas situaciones, es posible que los arrendatarios requieran más de una instancia o que la asignación de instancias no se base en los arrendatarios como criterio, sino en otros factores, como el ID de red o la aplicación. En estos casos, Citrix ADM permite definir con precisión las políticas de ubicación en función de expresiones definidas por el usuario para asignar una configuración de balanceador de carga a una de las instancias administradas.

Las políticas de ubicación brindan la flexibilidad de decidir qué instancia de Citrix ADC se usa en cada configuración de balanceador de carga creada por los usuarios. Las políticas de colocación flexibles de Citrix ADM ofrecen una opción adicional al método existente de asignación de instancias de Citrix ADC en función de los inquilinos.

> **Nota**
>
> Puede asignar instancias a los arrendatarios de forma manual o utilizar directivas de ubicación para asignar instancias en función de las expresiones creadas. No puede utilizar ambos métodos simultáneamente en un único paquete de servicios.

Las directivas de ubicación se basan en expresiones booleanas definidas sobre las propiedades de los principales objetos de configuración de LBaaS, como los grupos y los balanceadores de carga. La interfaz de usuario de la política de colocación de Citrix ADM proporciona expresiones predefinidas entre las que puede elegir para definir una política personalizada. Puede crear varias directivas de ubicación para diferentes expresiones. Por lo tanto, cada arrendatario puede tener varios dispositivos que se definen según los requisitos del arrendatario.

Primero debe seleccionar una expresión para que coincida con un objeto raíz que se debe configurar más adelante. El objeto raíz puede ser un objeto de grupo en el caso de LBaaS V1 y un objeto de balanceador de carga en el caso de LBaaS V2. Por lo tanto, las ubicaciones basadas en políticas de Citrix ADM son compatibles con las API V1 y V2 de LBaaS. Estas directivas de ubicación se asocian luego a los paquetes de servicios. Una vez que el objeto raíz se coloca en una instancia, los objetos sucesivos del modelo se agregan a la instancia.

Por ejemplo, el objeto de configuración del grupo puede tener las siguientes propiedades:

- tenant_id
- name
- description
- protocol
- método lb_
- identificador_de_subred

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- nombre_de_subnombre
- admin_state_up
- estado
- id_de_red
- tipo_de_red
- identificación_de_segmentación
- subnet_cidr
- subnet_gateway_ip

Los siguientes son ejemplos que muestran algunas de las expresiones que utilizan propiedades de grupo para definir una expresión para la directiva:

1. Expresión de directiva basada en nombre de grupo

```
1 config["pools"]["name"] =="high-end-pool"
```

2. Expresión de directiva basada en nombre de subred del grupo

```
1 config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
```

3. Expresión de directiva basada en nombre de subred del equilibrador de carga

```
1 config["loadbalancers"]["subnet_name"] == "mas-subnet"
```

### Adición de directiva de ubicación

1. En la página principal de Citrix ADM, vaya a **Orchestration** > **Cloud** Orchestration > **Placement Policy** y, a continuación, haga clic en **Agregar**.
2. En la página **Agregar directiva de ubicación**, defina los siguientes parámetros:
   a) Nombre: escriba un nombre para la directiva de colocación
   b) Expresiones de uso frecuente: seleccione una expresión de la lista desplegable.
   c) Expresión: en este campo se rellena una expresión lógica (booleana) en función de la expresión que ha seleccionado en el campo anterior. Modifique los nombres de los campos según sea necesario.

> **Nota**
>
> Al crear varias directivas, asegúrese de que las directivas son exclusivas entre sí.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. Haga clic en **Aceptar**.
4. **Vaya a**Orquestación > Orquestación**en la**nube**>**OpenStack**>**Paquetes de servicios**y, a continuación, haga clic en Agregar.**
5. En la página **del paquete de servicios**, defina los siguientes parámetros:
   a) Nombre: escriba un nombre para el paquete de servicios
   b) Directiva de aislamiento: seleccione Directiva **compartida**

      En la directiva de aislamiento compartido, la configuración del balanceador de carga de un arrendatario coexiste con la configuración del balanceador de carga de otros arrendatarios en el dispositivo asignado al arrendatario.
   c) Tipo de dispositivo: seleccione un **Citrix ADC VPX** o **Citrix ADC MPX** previamente aprovisionado

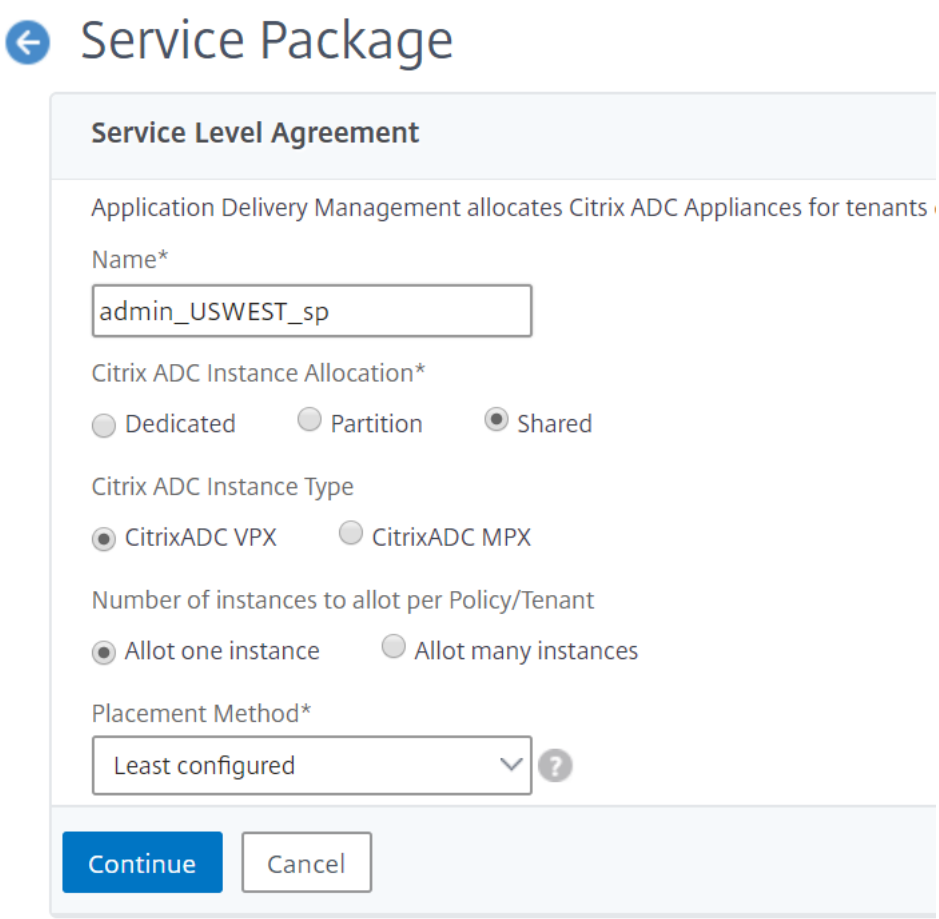
      Seleccione **Asignar un dispositivo** si desea que todas las configuraciones del balanceador de carga de un arrendatario estén vinculadas a un dispositivo. Seleccione **Asignar muchos dispositivos** si desea que cada configuración de balanceador de carga de un arrendatario se distribuya en varios dispositivos según las directivas de ubicación.

      > **Nota** Citrix ADC SDX debe agregarse a los paquetes de servicios únicamente como instancias de Citrix ADC VPX, ya que un Citrix ADC SDX tiene un Citrix ADC VPX aprovisionado.

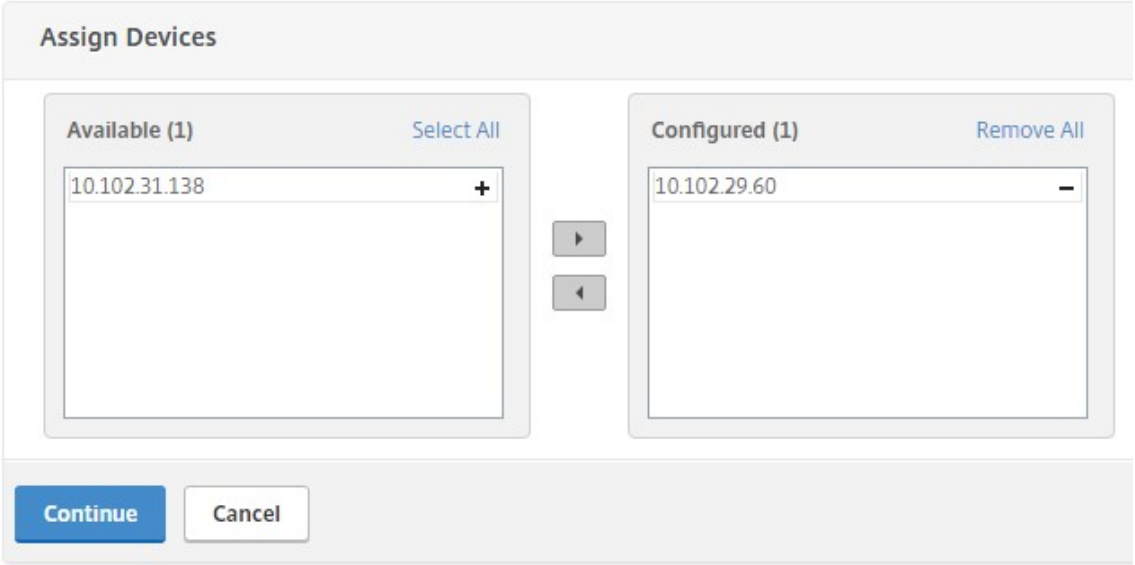
   d) Método de colocación: seleccione el **menos configurado**

      Cuando se selecciona Menos configurado, se elige como dispositivo para el arrendatario la instancia de NetScaler ADC que tiene el menor número de miembros del grupo configurados en ese momento.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

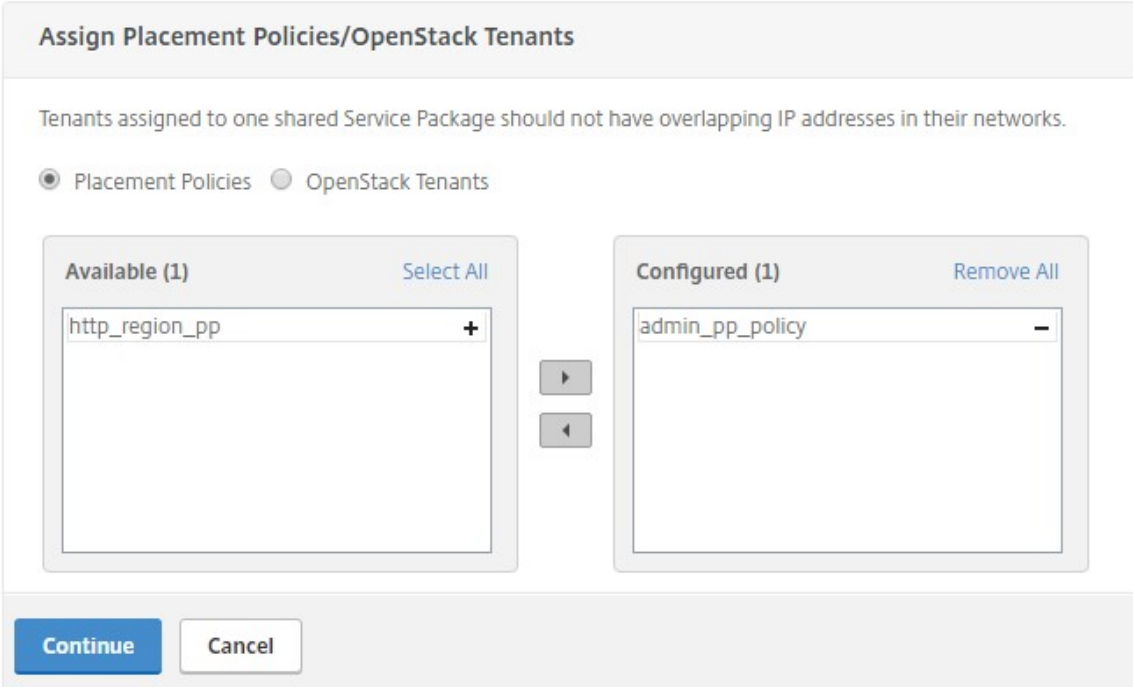



6. Haga clic en **Continuar**.
7. En la sección **Asignar dispositivos**, agregue los dispositivos NetScaler ADC disponibles a la lista de dispositivos configurados.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. Haga clic en **Continuar**.
9. En la sección **Asignar directivas de ubicación/arrendatarios de OpenStack**, agregue la directiva de ubicación que creó anteriormente.




> **Nota**
>
> Si no se encuentra la directiva, se reviva el mecanismo de reserva y NetScaler ADM asigna instancias de NetScaler ADC basadas en arrendatarios. Si el arrendatario no forma parte de ningún paquete de servicios, NetScaler ADM muestra un mensaje de error que dice:
>
> "El arrendatario `admin` no forma parte de ningún paquete de servicios y no hay un paquete de servicios predeterminado".

10. Haga clic en **Continue** y, a continuación, en **Done**.

## NSX Manager: Provisioning manual de instancias de NetScaler ADC

January 30, 2024

Citrix Application Delivery Management (ADM) se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

En este artículo se proporciona una lista de las tareas que debe realizar tanto en VMware NSX Manager como en Citrix ADM.

> **Nota**
>
> Asegúrese de que VMware NSX para vSphere 6.2 y versiones posteriores estén instalados y configurados, y que las puertas de enlace perimetrales, el DLR y las máquinas virtuales que deben tener un equilibrio de carga ya estén creados.

## Requisitos previos

- Instale VMware ESXi versión 4.1 o posterior con hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Instale VMware OVF Tool (necesaria para la versión 4.1 de VMware ESXi) en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.
- Instale NetScaler ADM en cualquiera de los hipervisores compatibles.

  Para ver las tareas de instalación de NetScaler ADM compilación 13.0, en cualquiera de los hipervisores compatibles, consulte Implementación de NetScaler ADM.

## Requisitos de hardware de VMware ESXi

En la siguiente tabla se enumeran los recursos informáticos virtuales que necesita en el servidor VMware ESXi para instalar un dispositivo virtual Citrix ADM.

| Componente | Requisito |
|---|---|
| RAM | 8 GB |
| CPU virtual | 8 |
| Espacio de almacenamiento | 500 GB |
| Interfaces de red virtual | 1 |
| Rendimiento | 1 Gbps |

> **Nota**
>
> Los requisitos de memoria y disco duro especificados anteriormente son para implementar Citrix ADM en el servidor VMware ESXi, teniendo en cuenta que no hay otras máquinas virtuales

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> ejecutándose en el host. Los requisitos de hardware del servidor VMware ESXi dependen de la cantidad de máquinas virtuales que se ejecuten en él.

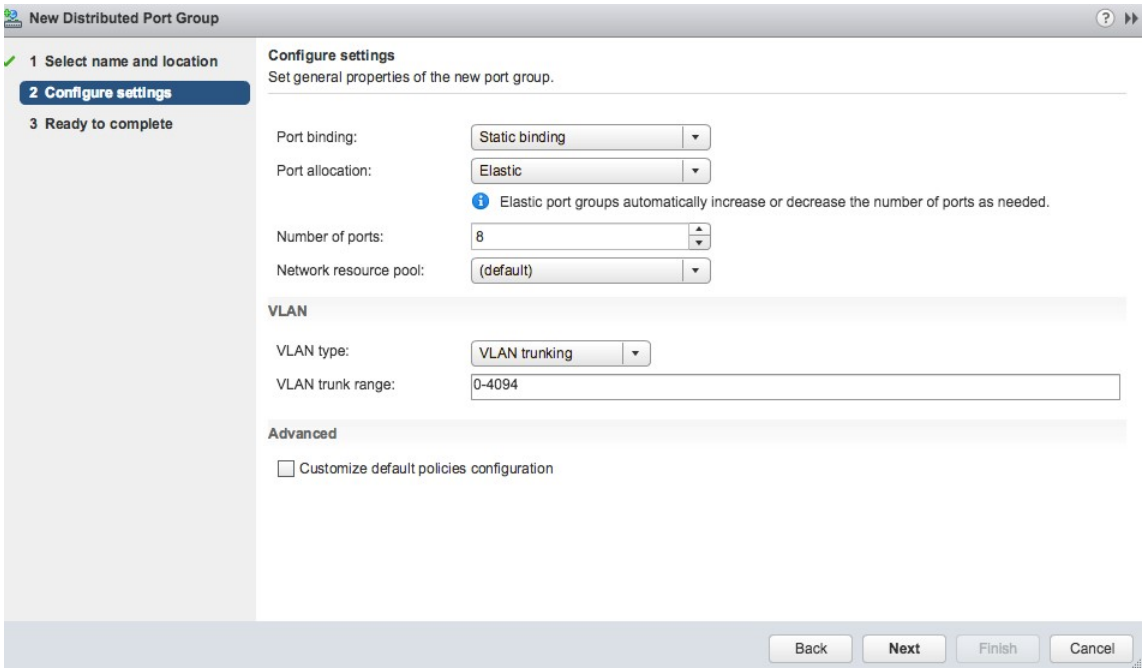
## Configuración de VMware NSX

- Cree un grupo de instancias de Citrix ADC VPX de diferentes capacidades, que se agreguen a los diferentes paquetes de servicios.

Por ejemplo:

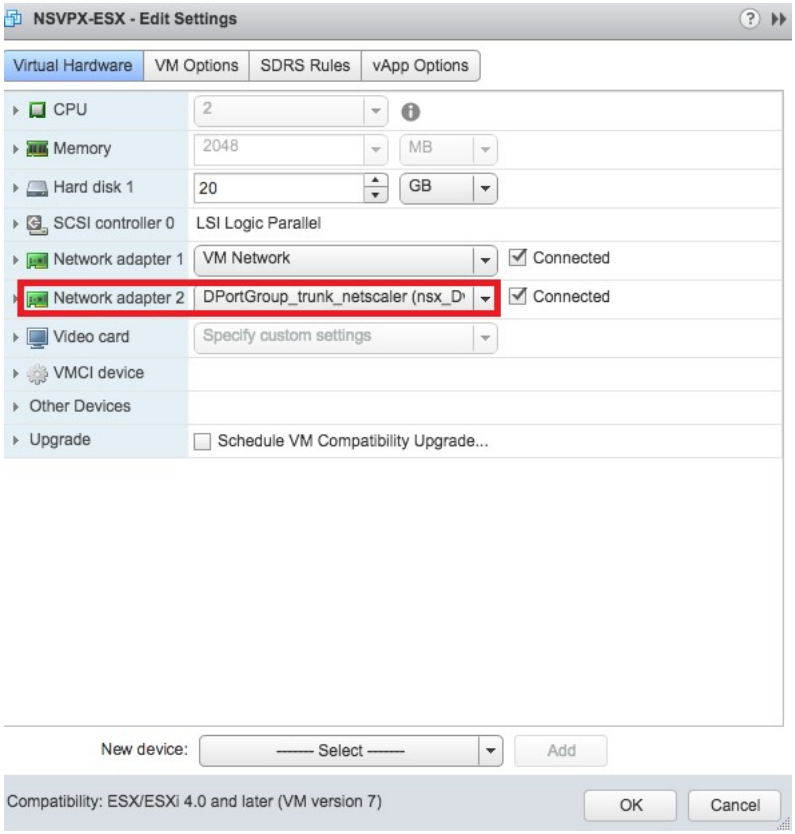
- Cree cinco instancias Citrix ADC VPX de VPX1000 (1 Gbps). Estas instancias se agregan al paquete de servicios Gold.
- Cree cinco instancias Citrix ADC VPX de VPX10 (10 Mbps). Estas instancias se agregan al paquete de servicios Bronze.

1. En el cliente vSphere, vaya a **Redes**y cree un grupo de puertos del tipo VLAN troncal con un rango, por ejemplo, 101-105 (incluso puede proporcionar el rango completo, pero crear un grupo de puertos de tipo VLAN únicamente para las VLAN necesarias).



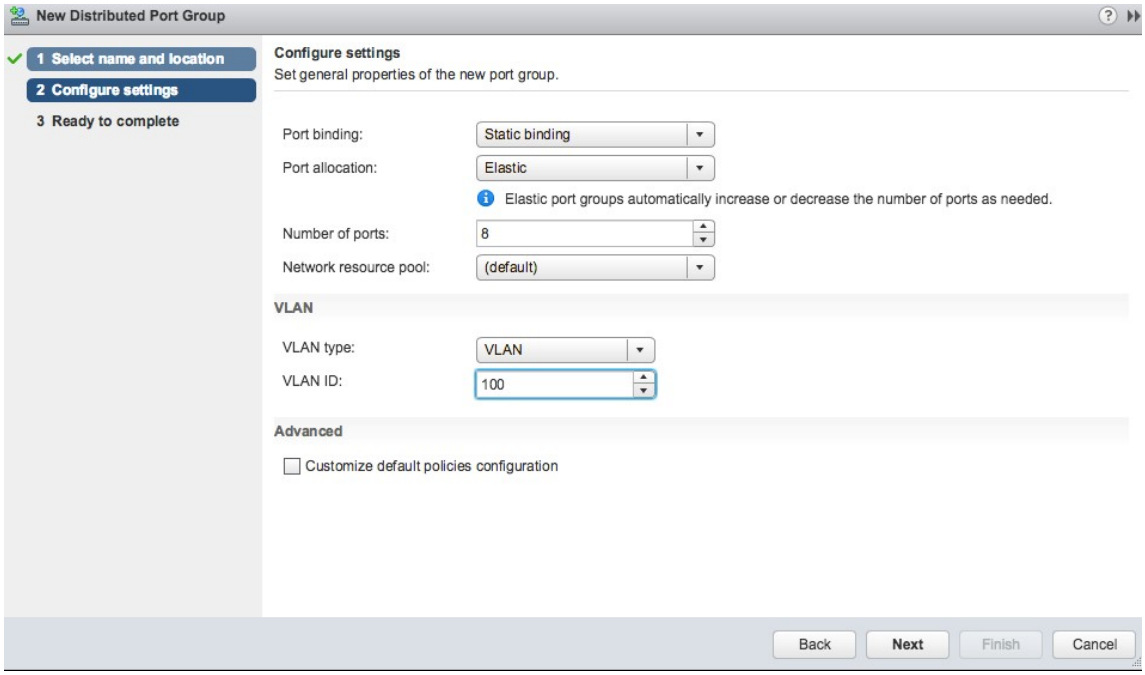

2. Cree una nueva interfaz para cada instancia de NetScaler ADC VPX y conéctela al grupo de puertos troncal de rango de VLAN creado anteriormente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




3. En el cliente vSphere, vaya a **Redes**y cree un grupo de puertos de tipo VLAN.

   Por ejemplo, si el grupo de puertos troncal inicial se creó con el rango 101-105, cree cinco grupos de puertos VLAN uno por VLAN, es decir, un grupo de puertos con VLAN 101, otro con VLAN102, etc., hasta VLAN 105.

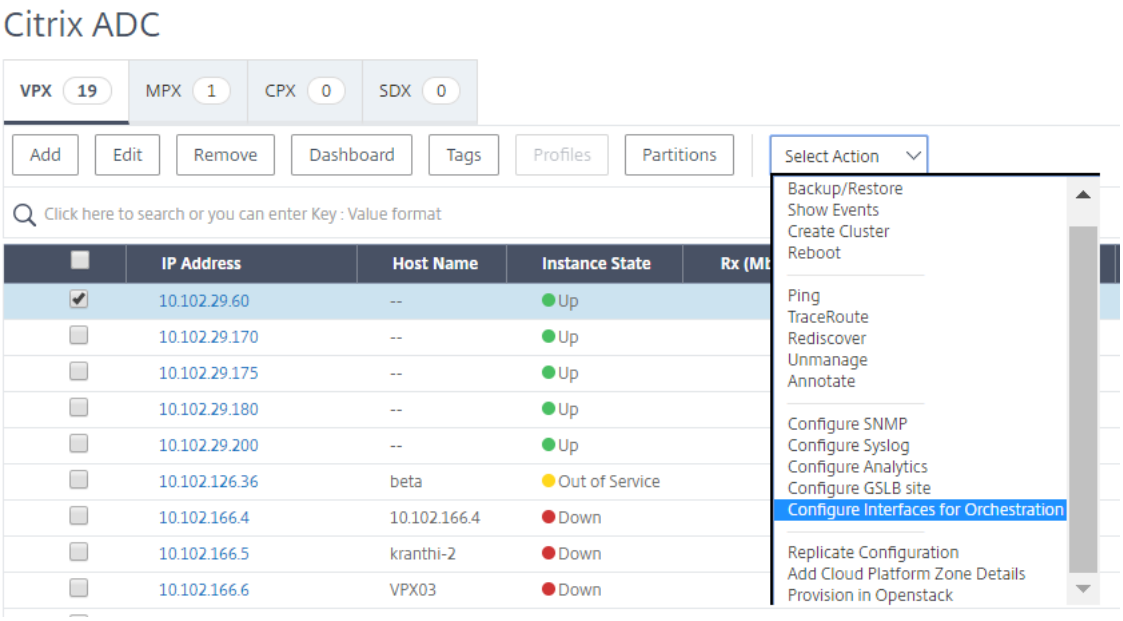



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Adición de una instancia NetScaler ADC VPX en NetScaler ADM

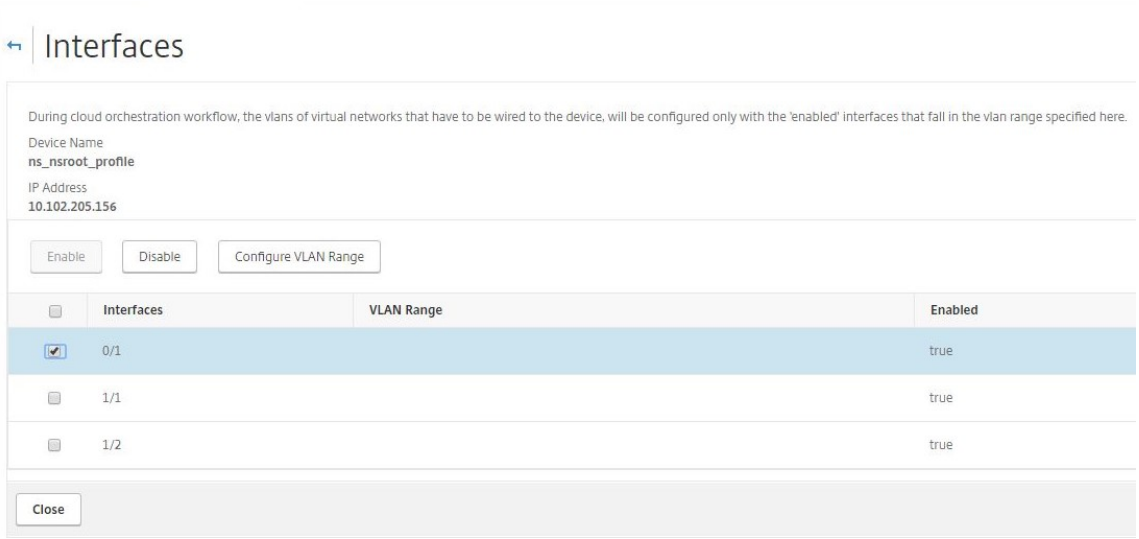
Agregue instancias de Citrix ADC VPX en Citrix ADM y especifique el rango de VLAN del grupo troncal para cada dispositivo.

1. En Citrix ADM, vaya a **Infraestructura** > **Instancias** > **Citrix ADC VPX** y haga clic en **Agregar**.
2. En la página **Agregar Citrix ADC VPX** , especifique los nombres de host de las instancias, la dirección IP de cada instancia o un rango de direcciones IP y, a continuación, seleccione un perfil de instancia en la lista de **nombres** de perfil de IP. También puede crear un nuevo perfil de instancia haciendo clic en el icono +.
3. Haga clic en **Aceptar**.
4. Seleccione la instancia de Citrix ADC VPX recién agregada de la lista de la página **Citrix ADC VPX** y haga clic en el botón de flecha hacia abajo del campo **Acción**. Seleccione **Configurar interfaces para orquestación**.

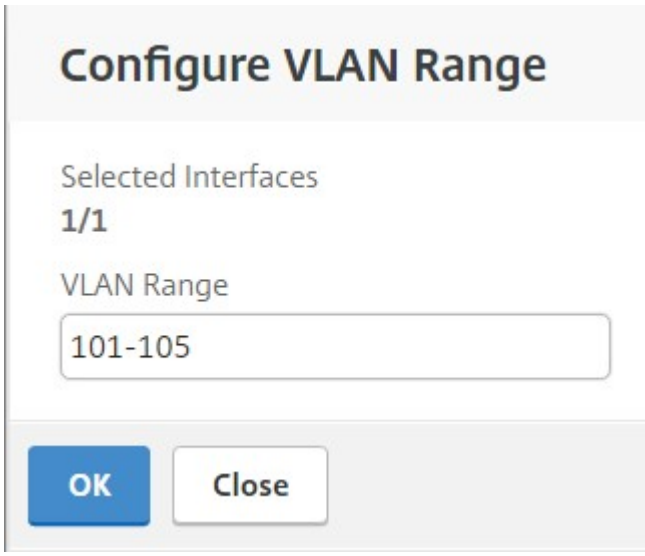



5. En la página **Interfaces**, seleccione la interfaz de administración y haga clic en **Desactivar**para impedir que la VLAN se enlace a la interfaz de administración.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. En la página **Interfaces**, seleccione la interfaz requerida y haga clic en **Configurar rango de VLAN**.
7. **Introduzca el rango de VLAN configurado en NSX Manager, haga clic en**Aceptar**y, a continuación, en Cerrar.**




## Registro de VMware NSX Manager con NetScaler ADM

Registre VMware NSX Manager en Citrix ADM para crear un canal de comunicación entre ellos.

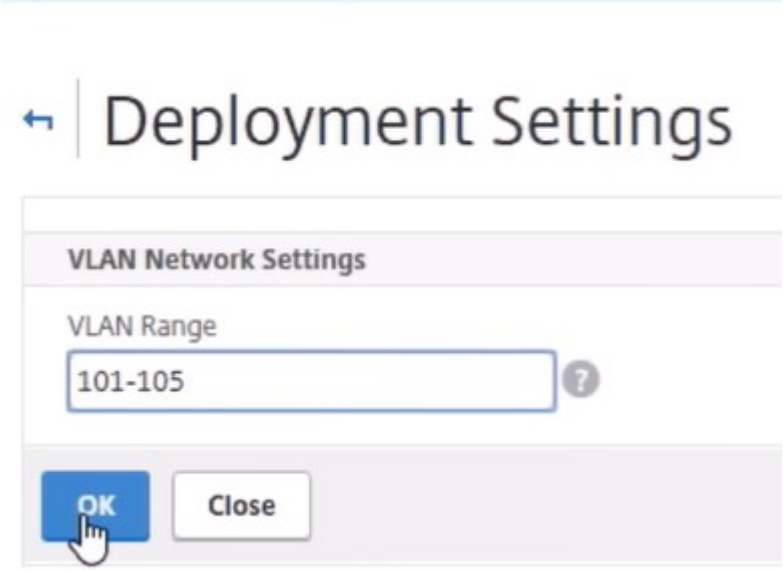
1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**en la lista desplegable y haga clic en**Configurar parámetros de NSX Manager**.
2. En la página **Configurar los ajustes de NSX Manager**, defina los siguientes parámetros:
   a) Dirección IP de NSX Manager: dirección IP de NSX Manager.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Nombre de usuario de NSX Manager: nombre de usuario administrativo de NSX Manager.

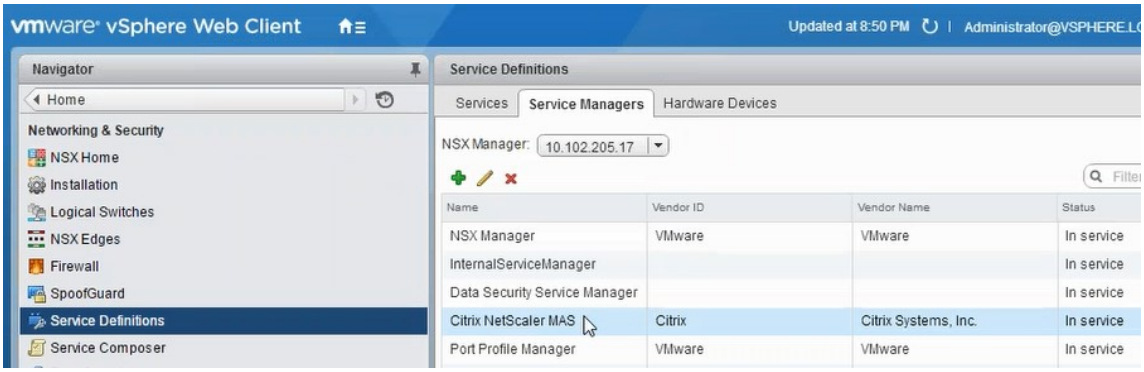
c) Contraseña: Contraseña del usuario administrativo de NSX Manager.

3. En la sección **Cuenta de NetScaler ADM utilizada por NSX Manager**, establezca el nombre de usuario y la contraseña de NetScaler ADC Driver para NSX Manager. NetScaler ADM autentica las solicitudes de configuración del equilibrador de carga desde NSX Manager mediante estas credenciales de inicio de sesión.
4. Haga clic en **Aceptar**.
5. Diríjase a **Orquestación** > **Sistema** > **Configuración de implementación.** Proporcione el rango de VLAN que se configuró en el grupo de puertos troncales.




6. Inicie sesión en NSX Manager en vSphere Web Client y vaya a **Definiciones de servicio** > **Administradores de servicio**.

   Puede ver Citrix ADM como uno de los administradores de servicios. Esto indica que el registro es correcto y que se establece un canal de comunicación entre NSX Manager y NetScaler ADM.



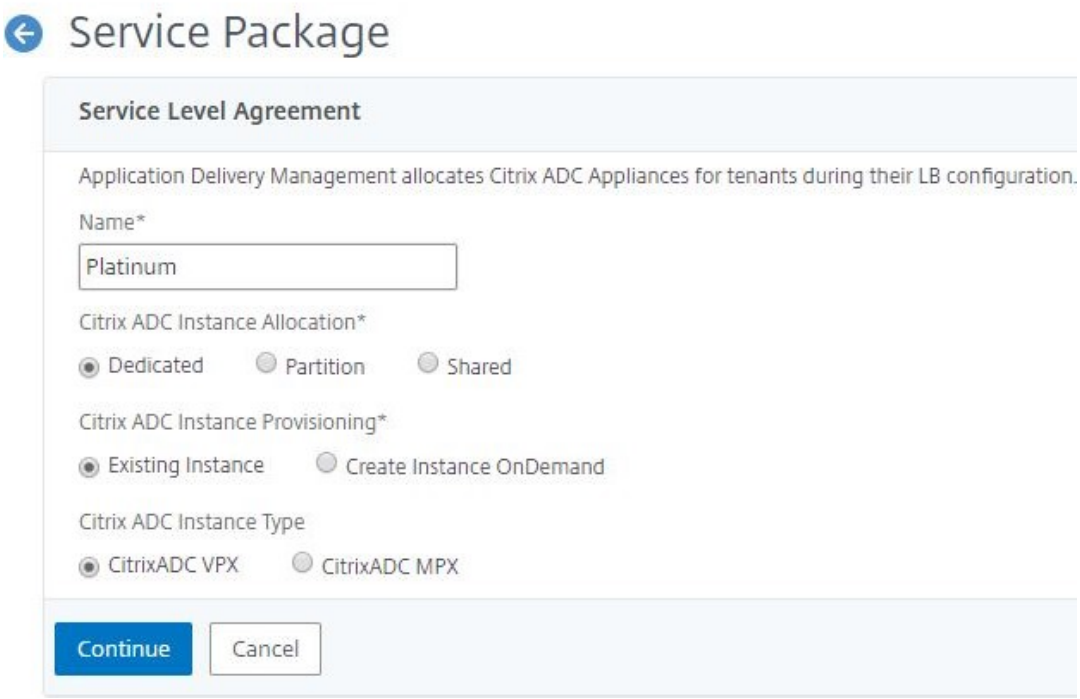

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Creación de un Service Package en NetScaler ADM

1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**>**Service Packages**y haga clic en**Agregar** para agregar un nuevo paquete de servicios.
2. En la página **Paquete de servicio**, en la sección **Parámetros básicos**, establezca los siguientes parámetros:
   a) Nombre: escriba el nombre de un paquete de servicios
   b) Directiva de aislamiento: de forma predeterminada, la directiva de aislamiento está configurada como Dedicada
   c) Tipo de dispositivo: de forma predeterminada, el tipo de dispositivo se establece en Citrix ADC VPX

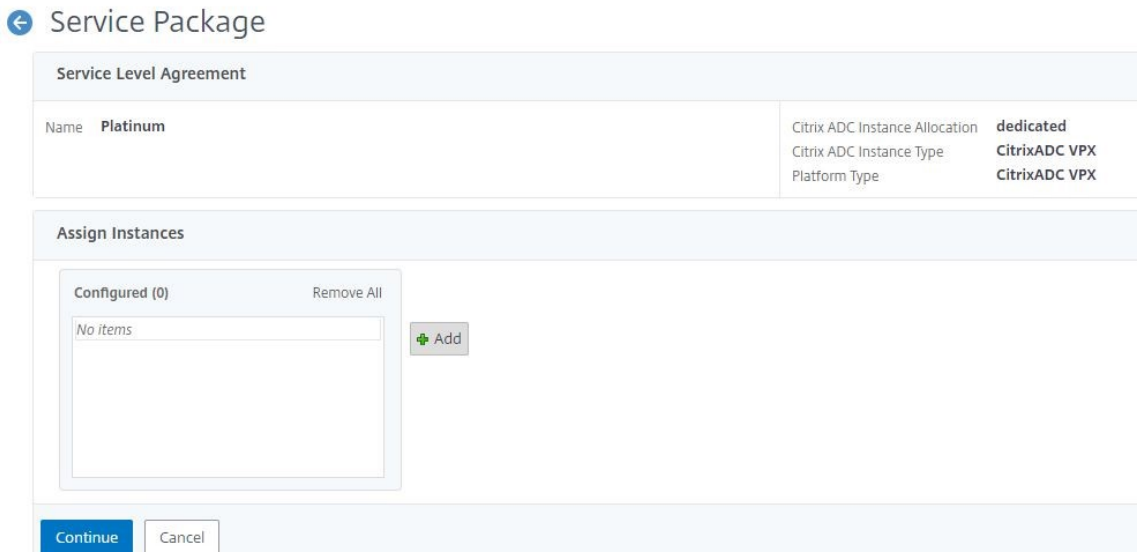
      > **Nota:**
      >
      > Estos valores están configurados de forma predeterminada en esta versión y no se pueden modificar.

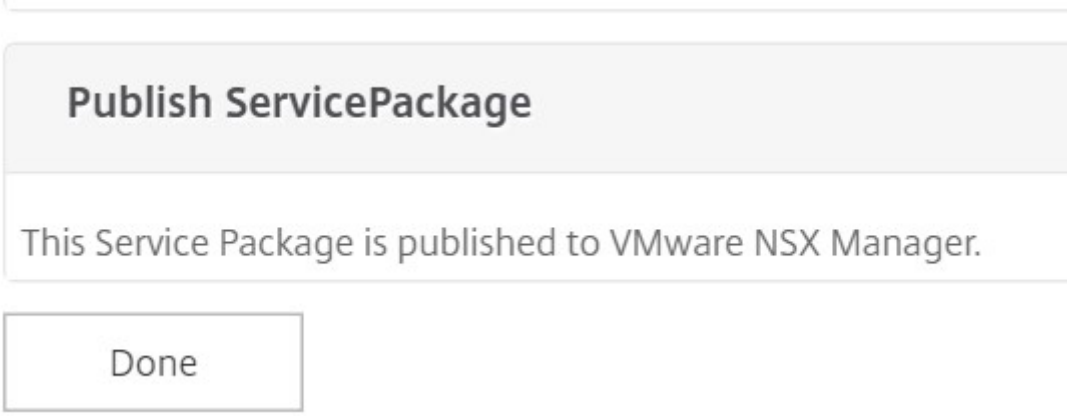
   d) Haga clic en **Continuar**.




3. En la sección **Asignar dispositivos**, seleccione el VPX preaprovisionado para este paquete y haga clic en **Continuar**.
4. En la sección **Publicar paquete de servicios**, haga clic en **Continuar** para publicar el paquete de servicios en VMware NSX y, a continuación, haga clic en **Listo**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Este procedimiento configura un paquete de servicio en NSX Manager. A un servicio se le pueden agregar varios dispositivos y varios bordes pueden usar el mismo paquete de servicios para descargar la instancia de Citrix ADC VPX a Citrix ADM.

5. **Inicie sesión en NSX Manager en vSphere Web Client y vaya a**Definiciones de servicios**> Servicios.**

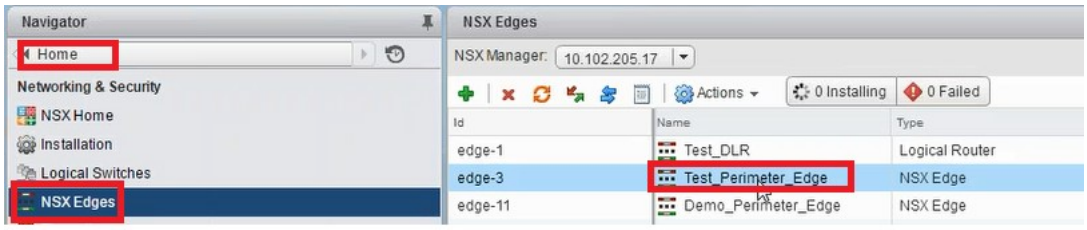
   Puede ver que el paquete de servicio NetScaler ADM está registrado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

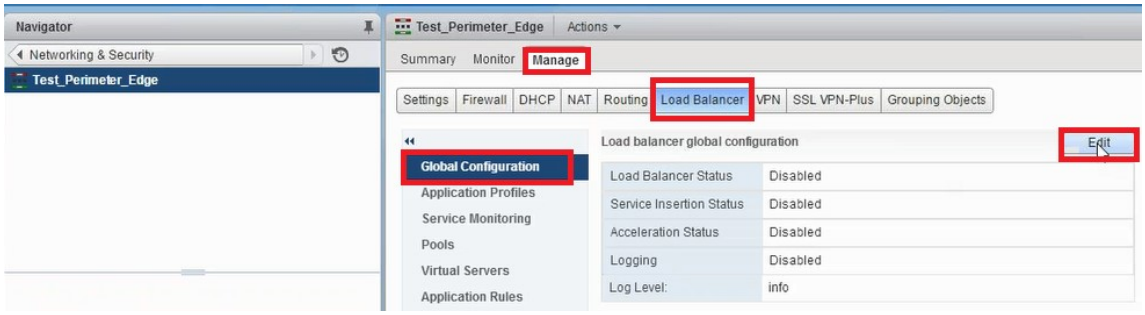
## Realización de la inserción del servicio de equilibrador de carga para Edge

Inserte el servicio de equilibrador de carga en la puerta de enlace NSX Edge creada anteriormente (transfiera la función de equilibrio de carga de NSX LB a Citrix ADC).

1. En NSX Manager, vaya a **Inicio** > **NSX Edges**y seleccione la puerta de enlace perimetral que haya configurado.

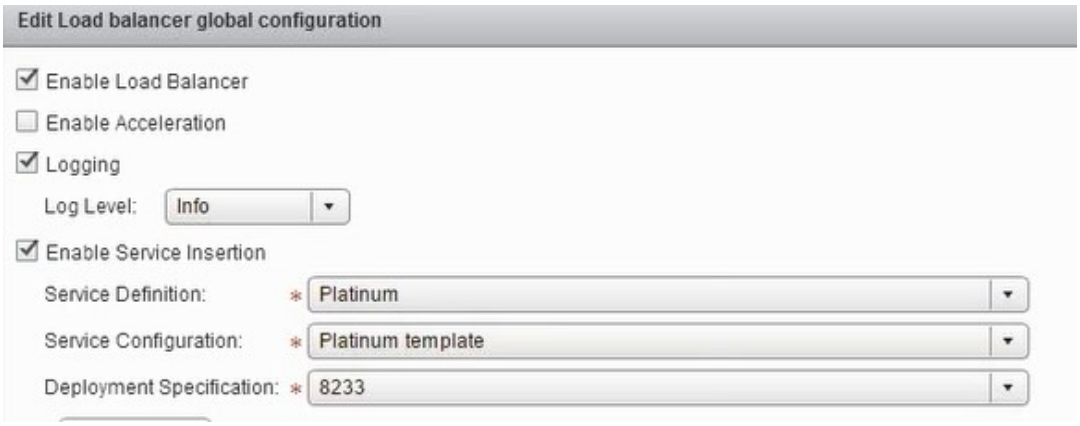



2. Haga clic en **Administrar**y, en la ficha **Equilibrador de carga**, seleccione **Configuración global**y, a continuación, en **Editar**.



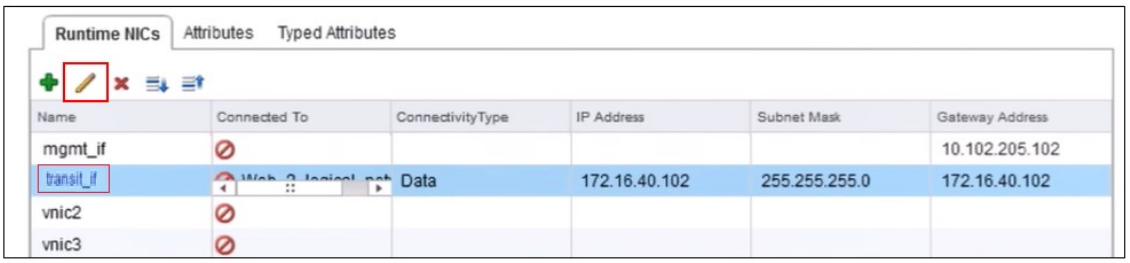

3. Seleccione **Habilitar equilibrador de carga**, **Registro**, **Habilitar inserción de servicios** para habilitarlos.

   a) En **Definición de servicio,** seleccione el paquete de servicio creado en NetScaler ADM y publicado en NSX Manager.

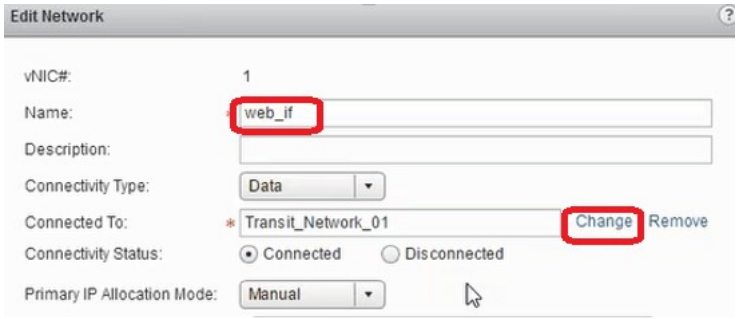



4. Seleccione las NIC en tiempo de ejecución existentes y haga clic en el icono Editar para editar las NIC en tiempo de ejecución que deben conectarse cuando se asigna Citrix ADC VPX.

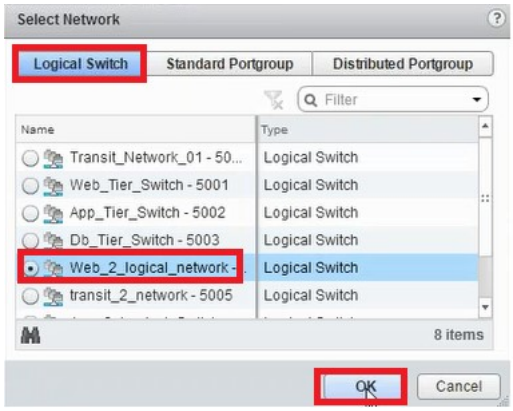
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Modifique el nombre de la NIC, especifique el tipo de conectividad como **dato**y haga clic en **Cambiar**.



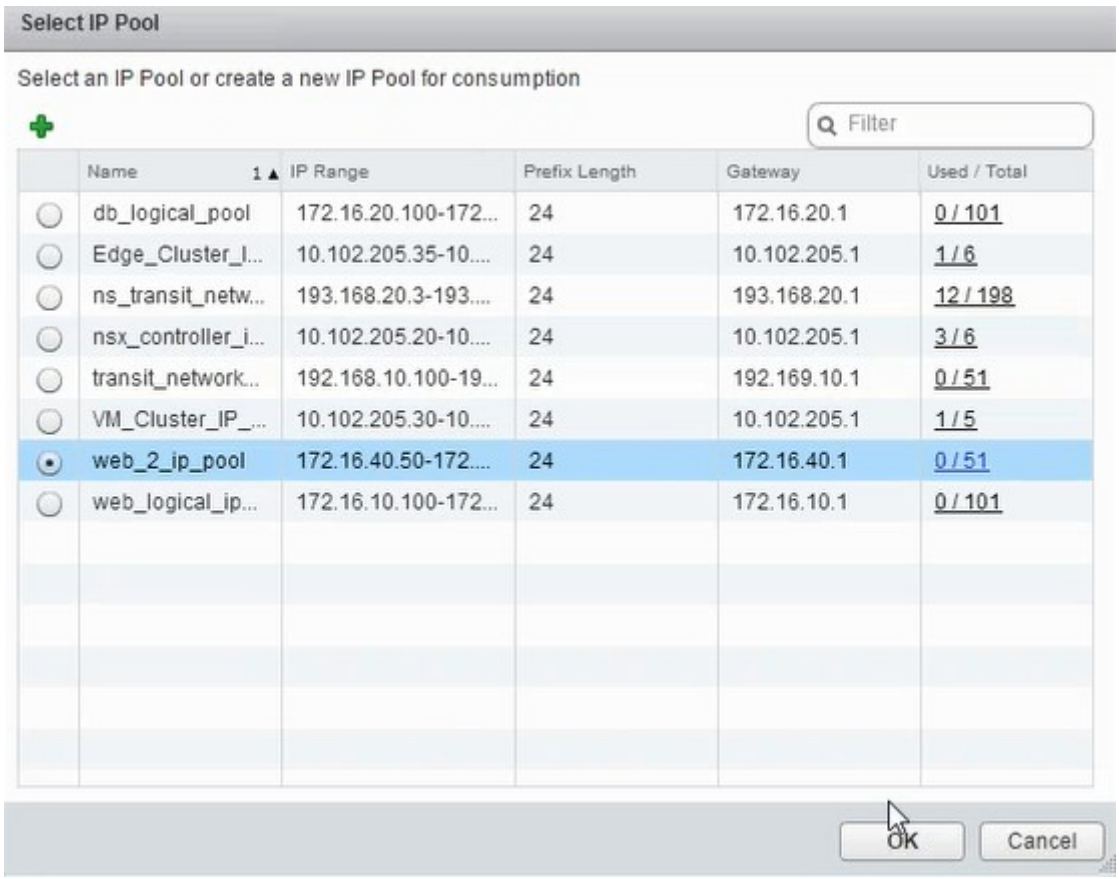

6. Seleccione el conmutador lógico web adecuado.




7. En **Modo de asignación de IP principal**, seleccione Grupo de IP en la lista desplegable y haga clic en el botón de flecha hacia abajo en el campo Grupo de IP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

8. En la ventana **Seleccionar grupo de IP**, seleccione el grupo de IP apropiado y haga clic en **Aceptar**.

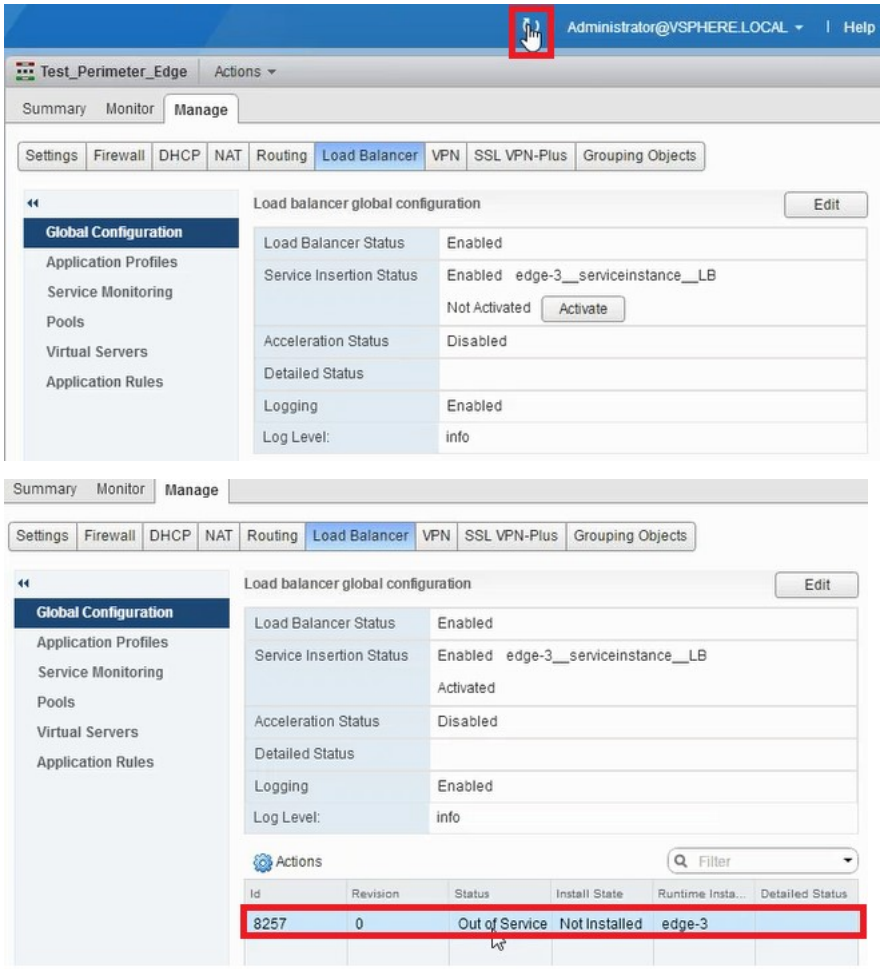



La dirección IP se adquiere y se establece como dirección IP de red de origen en el dispositivo NetScaler ADC VPX. Se crea una Gateway L2 en NSX Manager para asignar la VXLAN a VLAN.

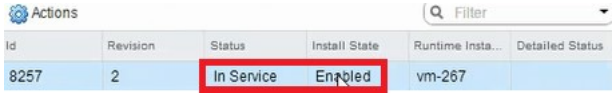
> **Nota**
>
> Todas las interfaces de datos están conectadas como NIC en tiempo de ejecución y forman parte de interfaces para DLR.

9. Actualice la vista para ver la creación del tiempo de ejecución.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




10. Una vez iniciada la máquina virtual, el valor de Estado cambia a **En servicio** y el de Estado de instalación cambia a **Habilitado**.

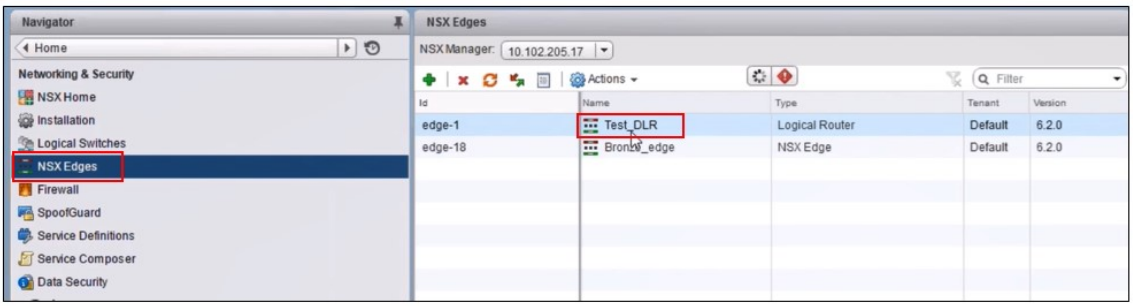



> **Nota**
>
> En NetScaler ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la inserción del servicio LB.

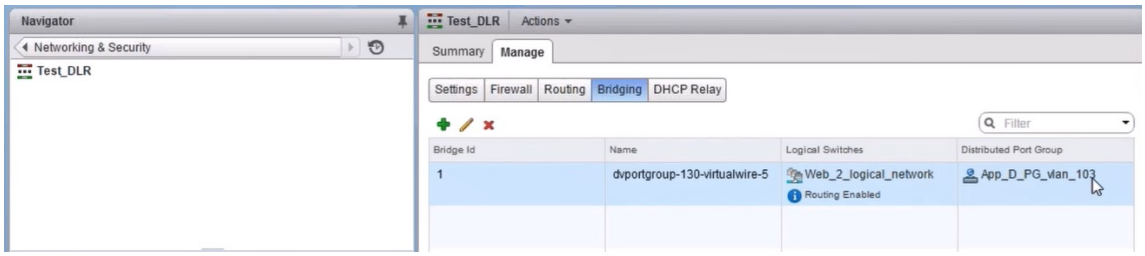
## Visualización de L2 Gateway en NSX Manager

1. Inicie sesión en NSX Manager en vSphere Web Client, vaya a **NSX Edges**y seleccione el DLR creado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



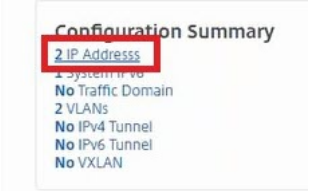

2. En la página DLR, vaya a **Administrar** > **Bridging**. Puede ver la Gateway L2 mostrada en la lista.



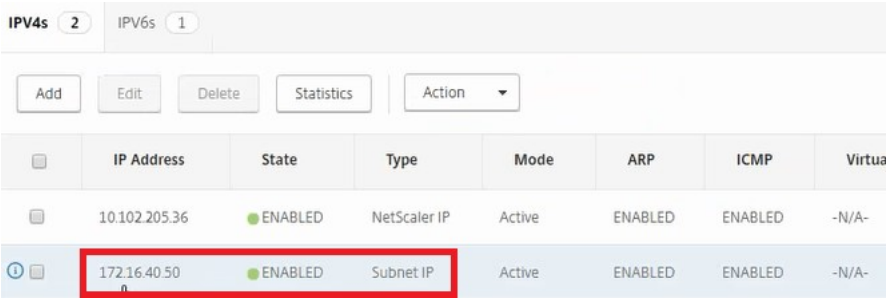

> **Nota**
>
> Se crea una Gateway L2 para cada interfaz de datos.

## Visualización de Citrix ADC asignado

1. Inicie sesión en la instancia de Citrix ADC VPX con la dirección IP que se muestra en Citrix ADM. A continuación, vaya a **Configuración** > **Sistema** > **Redes**. En el panel derecho, puede ver que se han agregado las dos direcciones IP. Haga clic en el hipervínculo de dirección IP para ver los detalles.




La dirección IP de la subred es la misma que la dirección IP de la interfaz web agregada en NSX.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Vaya a **Configuración** > **Sistema** > **Licencias** para ver las licencias que se aplican a esta instancia.

## Configuración de la instancia de NetScaler ADC VPX mediante StyleBook

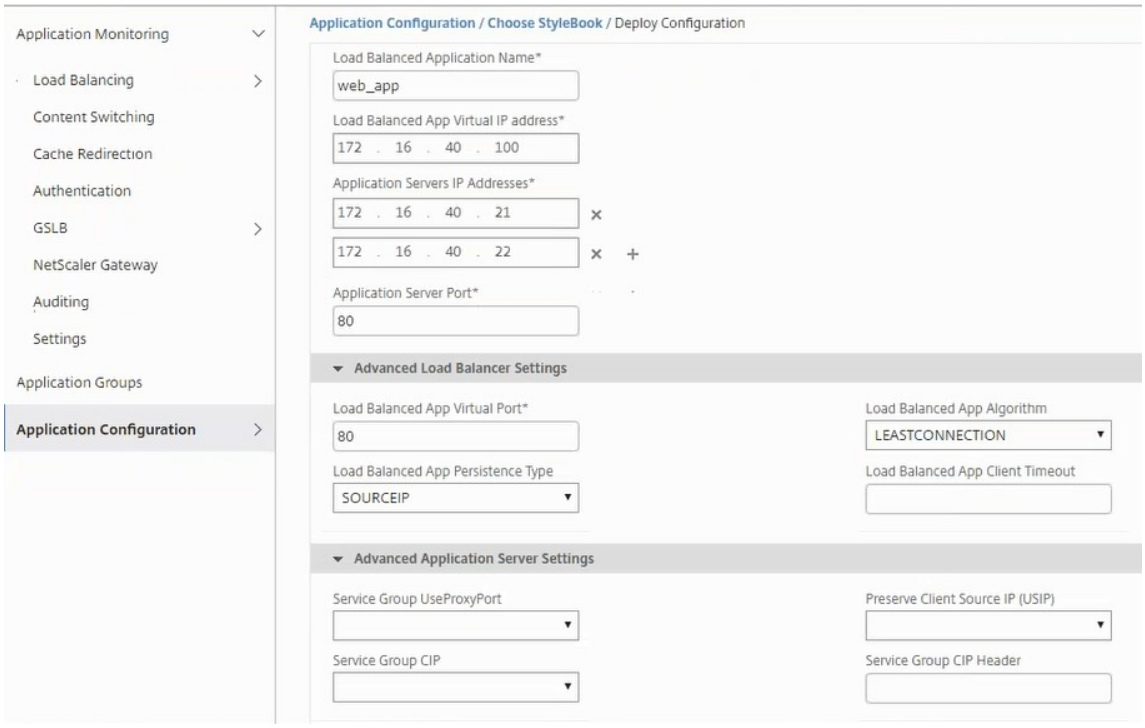
1. En NetScaler ADM, vaya a**Orchestration** >**SDN Orchestration**>**Configure NSX Manager** > **Edge Gateways**.

   Tome nota de la dirección IP de instancia de NetScaler ADC que se asigna a la puerta de enlace perimetral respectiva en la que debe aplicarse la configuración de equilibrio de carga a través de StyleBooks.

2. Cree un nuevo StyleBook. Vaya a **Aplicaciones** > **Configuración**, importe el StyleBook y seleccione el StyleBook de la lista.

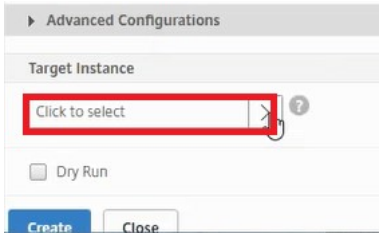
   Para crear un StyleBook nuevo, consulta Crea su propio StyleBook.

3. Especifique valores para todos los parámetros requeridos.

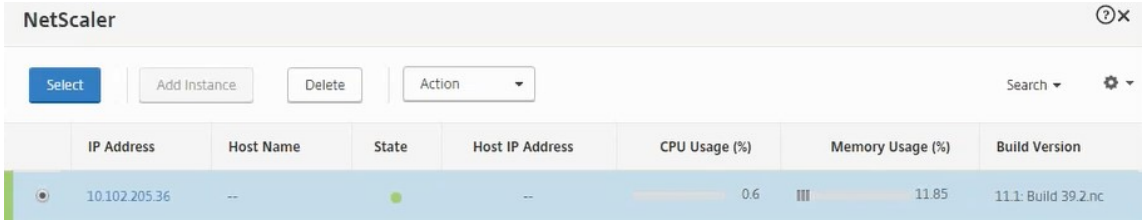



4. Especifique la instancia de Citrix ADC VPX en la que quiere ejecutar estos parámetros de configuración.

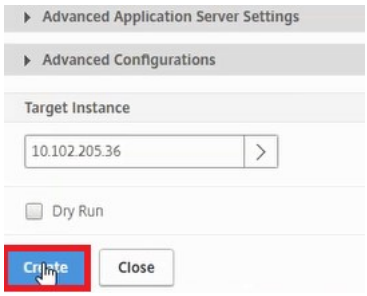
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




5. Seleccione la instancia IP mencionada anteriormente y haga clic en **Seleccionar**.

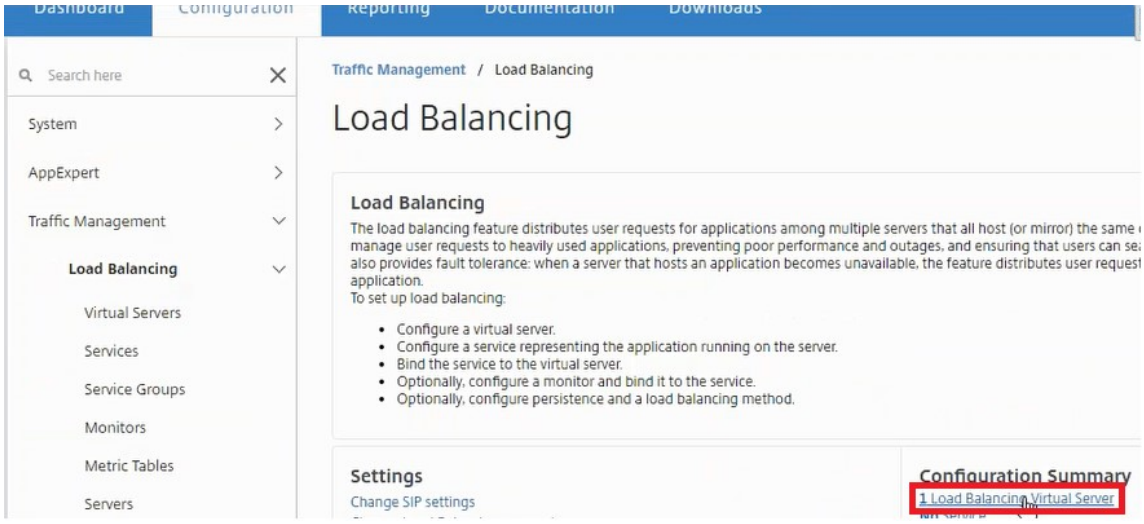



6. Haga clic en **Crear** para aplicar la configuración en el dispositivo seleccionado.



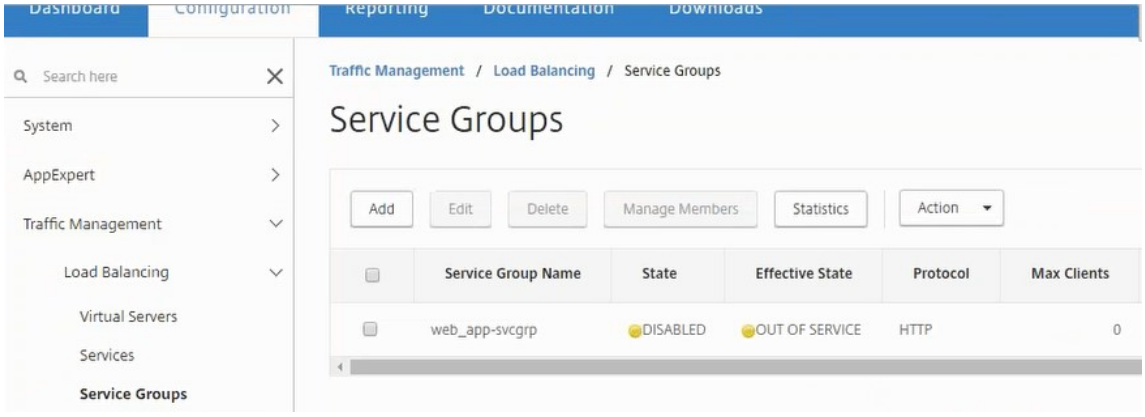

## Visualización de la configuración del equilibrador de carga

1. Inicie sesión en la instancia de NetScaler ADC VPX, vaya a **Configuración** > **Administración del tráfico** > **Equilibrio de carga** para ver el servidor virtual de equilibrio de carga que se crea.

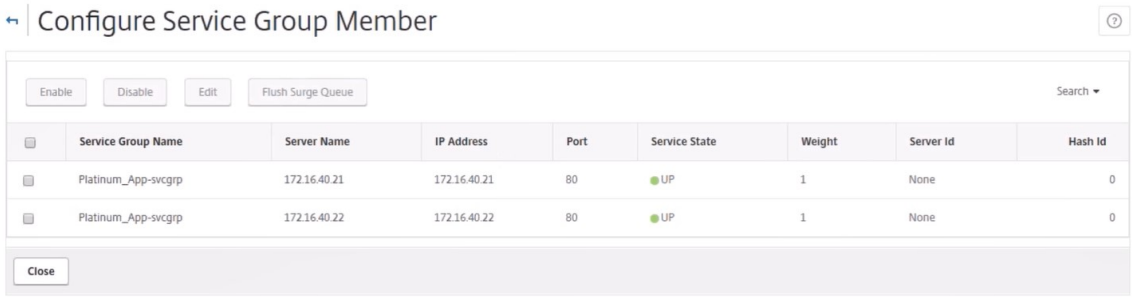



También puede ver los grupos de servicios que se crean.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




2. Seleccione el grupo de servicios y haga clic en **Administrar miembros**. La página **Configurar Miembro de Grupo de Servicio** muestra los miembros asociados al grupo de servicios.

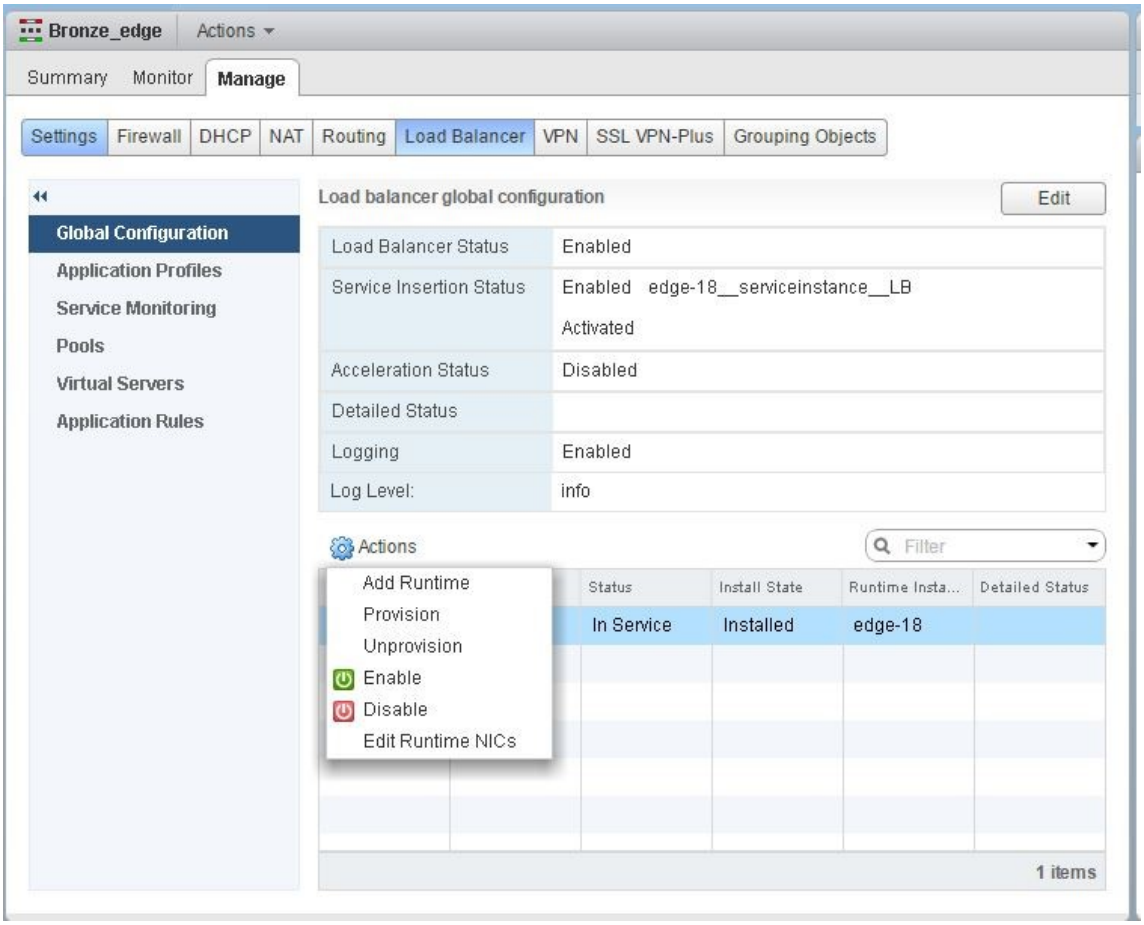



## Eliminación del servicio de equilibrador de carga

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** y haga clic en el icono **X** para eliminar la configuración de la aplicación.
2. Inicie sesión en NSX Manager en vSphere Web Client y navegue hasta la puerta de enlace perimetral a la que está conectada la instancia de Citrix ADC VPX.
3. Desplácese hasta **Administrar** > **Equilibrador de carga** > **Configuración global**, haga clic con el botón derecho en la entrada de tiempo de ejecución y haga clic en **Anular aprovisionamiento**.

> **Nota Las**
>
> puertas de enlace Edge en NetScaler ADM corresponden a las entradas en tiempo de ejecución en NSX Manager.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La instancia de NetScaler ADC VPX se representa fuera de servicio.

4. En NetScaler ADM, vaya a**Orchestration** >**SDN Orchestration**>**Configure NSX Manager** > **Edge Gateways**. Compruebe que la asignación respectiva de la puerta de enlace perimetral a la instancia eliminada no esté presente.

## NSX Manager: Provisioning automático de instancias de NetScaler ADC

January 30, 2024

### Overview

Citrix Application Delivery Management (ADM) se integra con la plataforma de virtualización de redes VMware para automatizar la implementación, la configuración y la administración de los servicios Citrix ADC. Esta integración elimina las complejidades tradicionales asociadas con la topología de la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

red física, lo que permite a los administradores de vSphere/vCenter implementar los servicios Citrix ADC de forma programática con mayor rapidez.

Durante la inserción y eliminación del servicio de equilibrio de carga en VMware NSX Manager, Citrix ADM aprovisiona y destruye dinámicamente las instancias de Citrix ADC. Este aprovisionamiento dinámico requiere que las asignaciones de licencias de Citrix ADC VPX se automaticen en Citrix ADM. Cuando las licencias de Citrix ADC se cargan en Citrix ADM, Citrix ADM desempeña la función de servidor de licencias.

## Requisitos previos

> **Nota**
>
> Esta integración solo se admite para **VMware NSX para vSphere 6.1 o versiones anteriores**.

- Citrix ADM, versión 13.0, configurada en alta disponibilidad e instalada en ESX.
- Citrix ADC VPX, versión 13.0
- Licencias de Citrix ADC VPX para instancias de Citrix ADC VPX, versión 13.0
- Instale VMware ESXi versión 4.1 o posterior con hardware que cumpla los requisitos mínimos.
- Instale VMware Client en una estación de trabajo de administración que cumpla los requisitos mínimos del sistema.
- Instale VMware OVF Tool (necesaria para la versión 4.1 de VMware ESXi) en una estación de trabajo de administración que cumpla con los requisitos mínimos del sistema.

## Implementación de alta disponibilidad de instancias Citrix ADM y Citrix ADC

Para aprovisionar la configuración de NetScaler ADM HA, instale el archivo de imagen NetScaler ADM que ha descargado del sitio de descarga de Citrix. Para obtener más información sobre cómo aprovisionar la configuración de alta disponibilidad de NetScaler ADM, consulte Implementación de NetScaler ADM en alta disponibilidad.

## Configuración de detalles de NetScaler ADM HA Endpoint

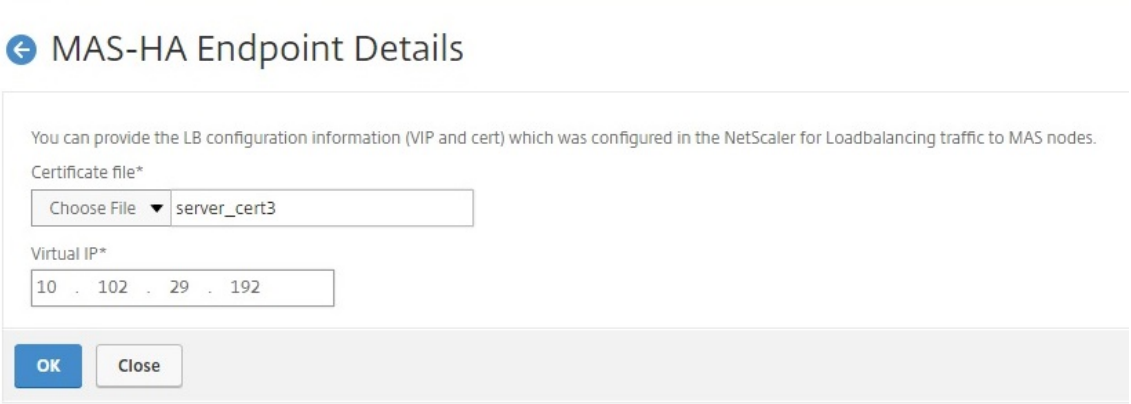
Para integrar VMware NSX Manager con Citrix ADM implementado en modo HA, primero debe introducir la dirección IP virtual de la instancia de Citrix ADC de equilibrio de carga. También debe cargar el archivo de certificado que está presente en el servidor virtual de equilibrio de carga Citrix ADC al sistema de archivos Citrix ADM.

**Para proporcionar información de configuración de equilibrio de carga en Citrix ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En el nodo Citrix ADM HA, vaya a **Sistema** > **Implementación**.
2. Haga clic en **Configuración de HA** en la esquina superior derecha y, en la página **Configuración de MAS-HA**, haga clic en **Detalles de extremo de MAS-HA**.

3. En la página **MAS-HA Endpoint Details**, cargue el mismo certificado que ya está presente en la instancia de NetScaler ADC de equilibrio de carga.
4. Introduzca la dirección IP virtual de la instancia de NetScaler ADC de equilibrio de carga y haga clic en **Aceptar**.




## Registro de VMware NSX Manager con NetScaler ADM

Al configurar dos servidores Citrix ADM en alta disponibilidad, los dos nodos del servidor están en modo activo-pasivo. Inicie sesión en el nodo principal del servidor Citrix ADM para registrar VMware NSX Manager con Citrix ADM en HA y crear un canal de comunicación entre ellos.

**Para registrar VMware NSX Manager con Citrix ADM en HA:**

1. En el nodo principal del servidor Citrix ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX Manager**.
2. Haga clic en **Configurar los ajustes de NSX Manager.**
3. En la página **Configurar los ajustes de NSX Manager**, defina los siguientes parámetros:
   a) Dirección IP de NSX Manager: dirección IP de NSX Manager.
   b) Nombre de usuario de NSX Manager: nombre de usuario administrativo de NSX Manager.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

c) Contraseña: Contraseña del usuario administrativo de NSX Manager.

4. En la sección Cuenta Citrix ADM utilizada por NSX Manager, establezca la contraseña del controlador Citrix ADC para NSX Manager.
5. Haga clic en **Aceptar**.

## Carga de licencias en NetScaler ADM

Cargue las licencias de NetScaler ADC VPX en NetScaler ADM para que NetScaler ADM pueda asignar licencias automáticamente a las instancias durante la orquestación con NSX.

**Para instalar archivos de licencia en NetScaler ADM:**

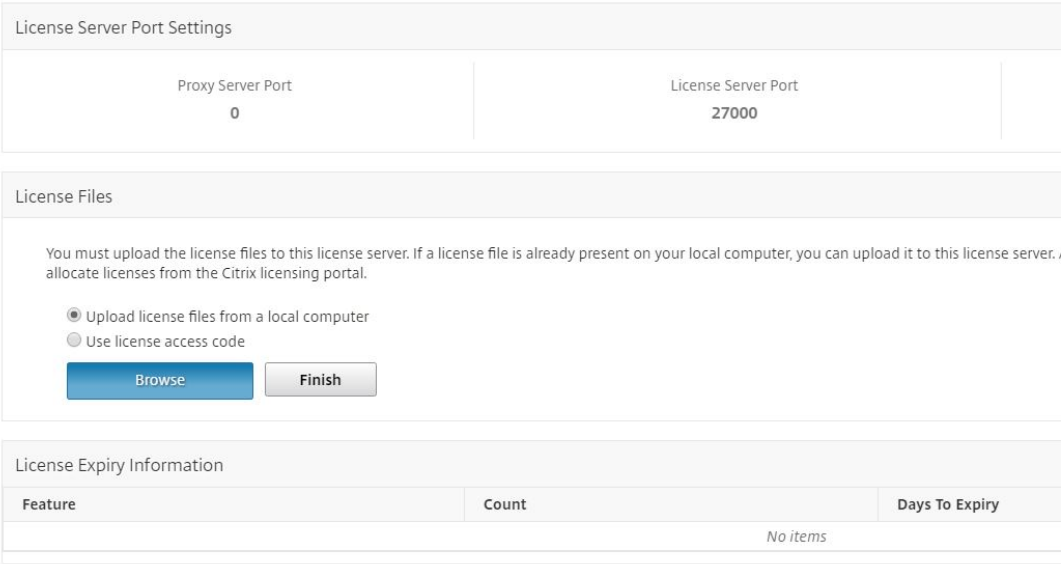
1. En Citrix ADM, vaya a **Redes** > **Licencias.**
2. En la sección **Archivos de licencia**, seleccione una de las siguientes opciones:

   a) **Cargar archivos de licencias desde un equipo**local : si ya hay un archivo de licencias en su equipo local, puede cargarlo en Citrix ADM. Para agregar archivos de licencia, haga clic **en**Examinar y seleccione el archivo de licencia (.lic) que desee agregar. Luego haga clic en **Finalizar**.

   b) **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso a licencias de las licencias que adquiera. Para añadir archivos de licencia, introduzca el código de acceso a la licencia en el cuadro de texto y, a continuación, haga clic en **Obtener licencias** .

   > **Nota**
   >
   > En cualquier momento, puede agregar más licencias a NetScaler ADM desde la Configuración de licencias.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Carga de imágenes de NetScaler ADC VPX en NetScaler ADM

Agregue las imágenes de NetScaler ADC a NetScaler ADM, de modo que NetScaler ADM utilice estas imágenes tal y como se definen en el paquete de servicio.

**Para cargar imágenes de Citrix ADC VPX en Citrix ADM:**

1. En NetScaler ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX Manager** > **Imágenes ESX NSVPX**.
2. Haga clic en **Cargar** y seleccione el paquete zip NetScaler ADC VPX de la carpeta de almacenamiento local.

## Creación de paquetes de servicios en Citrix ADM

Cree paquetes de servicio en NetScaler ADM para definir el conjunto de SLA, que indica cómo se asignan los recursos de NetScaler ADC.

**Para crear paquetes de servicios en Citrix ADM:**

1. En Citrix ADM, vaya a **Orchestration** > **SDN OrchestrationVMware NSX Manager**>**Service Packages**y haga clic en**Agregar** para agregar un nuevo paquete de servicios.
2. En la página **Paquete de servicio**, en la sección **Parámetros básicos**, establezca los siguientes parámetros:
   a) Nombre: nombre de un paquete de servicios
   b) Directiva de aislamiento: seleccione **Dedicado**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

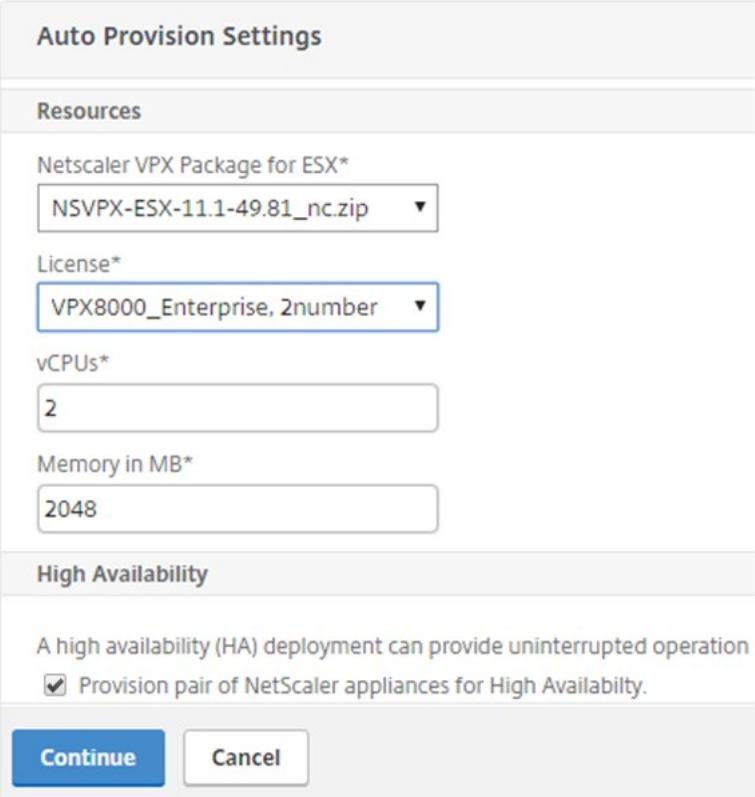
c) Provisioning de instancias de Citrix ADC: seleccione **Crear instancia bajo demanda**

d) Plataforma de aprovisionamiento automático: seleccione **CitrixADC SDX**

e) Haga clic en **Continuar**.

3. En la sección **Configuración de aprovisionamiento automático** , seleccione el paquete zip Citrix ADC VPX cargado recientemente para implementarlo en la plataforma NSX, seleccione la licencia correspondiente y haga clic en **Continuar**.

> **Nota**
>
> En la sección **Alta disponibilidad**, marque la casilla para aprovisionar instancias de NetScaler ADC para alta disponibilidad.




> **Nota**
>
> El nombre de la licencia que se muestra en el cuadro de lista que se muestra en la ilustración anterior, VPX8000_Advanced, número 2 es un ejemplo y se explica de la siguiente manera:
>
> - VPX: La licencia es implementar instancias de NetScaler ADC VPX
> - 8000: el ancho de banda consumible es de 8 GB

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> - Avanzado: Citrix proporciona tres tipos de licencias: Estándar, Avanzado y Premium
> - Número 2: se pueden implementar dos instancias de NetScaler ADC VPX mediante esta licencia
>
> **El nombre de la licencia que se muestra en el cuadro de lista Licencia depende de la licencia que haya adquirido en Citrix.**

4. Haga clic en **Continuar**.
5. El paquete de servicios se publica en NSX Manager. En NSX Manager, vaya a **Definiciones de servicios** > **Administradores de servicios**. Puede ver Citrix ADM como uno de los administradores de servicios. Esto indica que el registro se ha realizado correctamente y que se ha establecido una comunicación bidireccional entre NSX Manager y Citrix ADM.

> **Nota**
>
> Para Citrix ADM en una implementación de alta disponibilidad, las licencias solo se cargan en el nodo del servidor de licencias Citrix ADM. Los nodos NetScaler ADM están en modo activo-pasivo.

## Realización de la inserción del servicio de equilibrador de carga para Edge

Realice la inserción del servicio de equilibrador de carga en la puerta de enlace NSX Edge existente, es decir, descargue la función de equilibrio de carga del equilibrador de carga de NSX a NetScaler ADC.

**Para insertar el servicio de equilibrio de carga en NSX Edge Gateway:**

1. En NSX Manager, vaya a **Inicio** > **Redes y seguridad** > **NSX Edges**y haga doble clic para seleccionar la puerta de enlace perimetral que ha configurado.
2. Haga clic en **Administrar**y, en la ficha **Equilibrador de carga**, seleccione **Configuración global**y, a continuación, en **Editar**.
3. Seleccione **Habilitar balanceador de carga** y **Habilitar inserción de servicios** para habilitarlas.
4. En **Definición de servicio**, seleccione el paquete de servicios que se publicó en NSX Manager.
5. Configure una NIC virtual para la interfaz de administración y una o más NIC virtuales para las interfaces de datos. Seleccione las redes para la administración y los datos en consecuencia.

> **Nota**
>
> Seleccione la opción Grupo de direcciones IP en el modo de asignación de IP principal. Citrix ADM no admite la asignación manual o DHCP de direcciones IP.

6. Haga clic en el icono de actualización para ver la creación del tiempo de ejecución.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Como se implementan dos instancias de Citrix ADC VPX en una implementación de alta disponibilidad, se crean dos tiempos de ejecución en NSX Manager.
>
> Puede que tengas que actualizar la pantalla para ver los tiempos de ejecución que aparecen en la pantalla.

7. Seleccione el tiempo de ejecución, haga clic en **Acciones**y, en el menú emergente, seleccione **Instalar**. Para HA, repita esto también para el otro tiempo de ejecución.
8. Cuando se inician ambas máquinas virtuales, el valor de Estado cambia a "En servicio"y el de Estado de instalación cambia a "Habilitado".

   > **Nota**
   >
   > Puede que tenga que actualizar la pantalla para ver el cambio de estado.

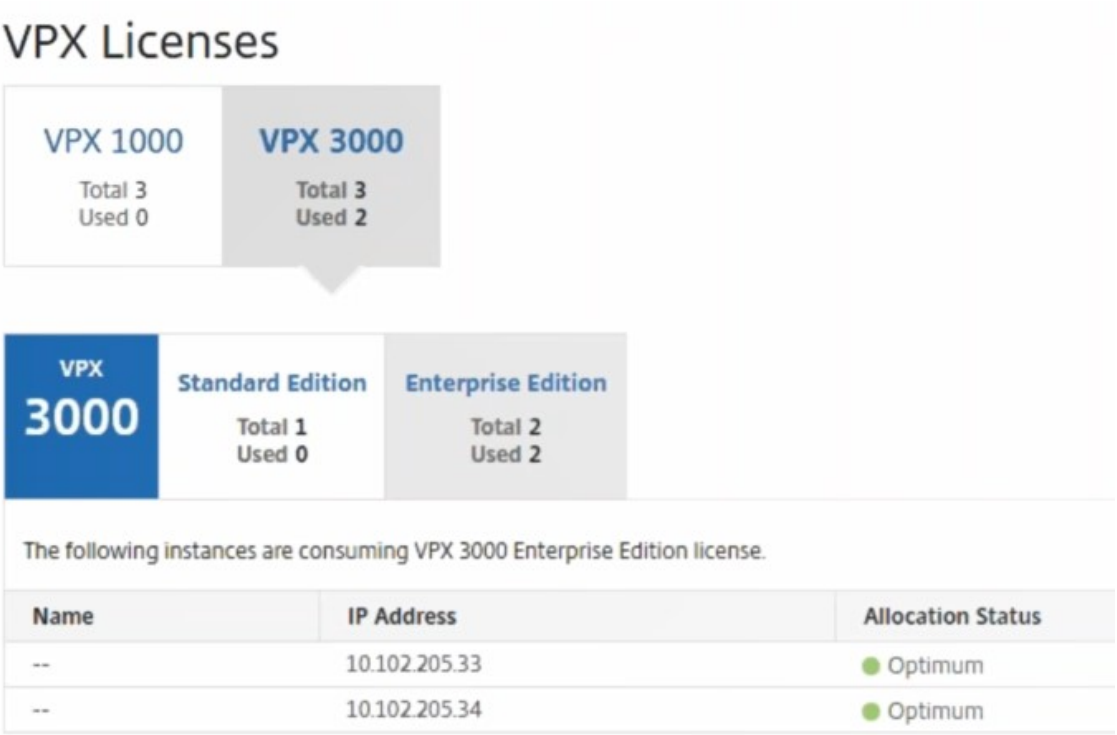
9. En Citrix ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la inserción del servicio. Puede ver que ha llegado a Citrix ADM una solicitud para crear y actualizar el tiempo de ejecución. Cuando se haya actualizado el tiempo de ejecución, seleccione la solicitud y haga clic en el botón **Tareas** para ver si Citrix ADM se ha agregado a NSX Manager.

   Para HA, habrá dos solicitudes para crear y actualizar dos tiempos de ejecución en Citrix ADM. Cuando se hayan actualizado ambos tiempos de ejecución, seleccione ambas solicitudes y haga clic en el botón **Tareas** para ver si se han agregado dos nodos Citrix ADM HA en NSX Manager.
10. En Citrix ADM, vaya a **Orchestration** > **SDN Orchestration** > **VMware NSX ManagerEdge Gateways**. En el panel lateral derecho, puede ver que el Citrix ADC VPX se ha agregado a NSX Edge Gateway.

    Para HA, puede ver que se han agregado dos instancias de NetScaler ADC VPX en modo HA a NSX Edge Gateway.
11. En Citrix ADM, vaya a **Redes** > **Licencias** > **Licencias VPX** . Seleccione la licencia NetScaler ADC VPX y la edición que haya instalado.

    Las instancias de NetScaler ADC VPX que están en modo HA consumen dos licencias y el estado se muestra en la pantalla como se muestra a continuación.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Una vez completada la inserción del servicio, puede utilizar StyleBooks para configurar las instancias de NetScaler ADC en uno de los dos métodos siguientes:

- Configuración de los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de VMware NSX Manager
- Configuración de Load Balancing Services en NetScaler ADC VPX en NetScaler ADM GUI

## Configuración de los servicios de equilibrio de carga en Citrix ADC VPX en la GUI de VMware NSX Manager

Realice la siguiente tarea para habilitar la configuración de los servicios de equilibrio de carga en el dispositivo de Gateway de NSX Edge mediante StyleBooks integrados.

En NSX Manager, vaya a **Inicio** > **Redes y seguridad** > **NSX Edges**y haga doble clic para seleccionar la puerta de enlace perimetral que ha configurado.

### Creación de grupos y miembros de grupos

Cree un grupo de servidores y miembros de diferentes capacidades.

1. Haga clic en **Administrar**y, en la ficha **Equilibrador de cargas**, seleccione **Grupos**y, a continuación, haga clic en el icono "**+**"para agregar un nuevo grupo y configurar los siguientes

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

parámetros:

a) Nombre: nombre del nuevo grupo

b) Algoritmo: seleccione un algoritmo de la base de la lista desplegable en el que se seleccionará el grupo.

c) Monitores: asegúrese de que el monitor de servicio esté configurado en default_http_monitor

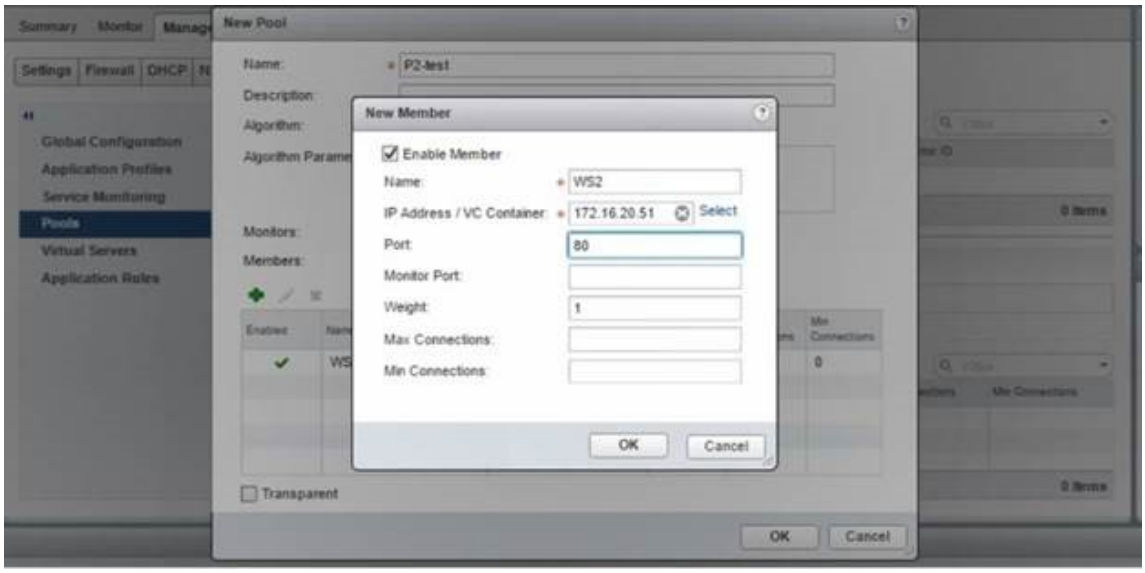
d) Miembros: haga clic en "+"para agregar miembros al grupo e introduzca los parámetros necesarios en la ventana Nuevo miembro.

   i. Nombre: nombre del miembro

   ii. Dirección IP/contenedor VC: haga clic en Seleccionar para seleccionar el objeto de la lista disponible o introducir la dirección IP del objeto.

2. Haga clic en **Aceptar**.

   Agregue tantos miembros como sea necesario.




### Creación de servidores virtuales

Cree un conjunto de servidores virtuales y asigne un grupo a cada servidor virtual.

1. Haga clic en **Administrar**y, en la ficha Equilibrador de carga, seleccione **Servidores virtuales**y, a continuación, haga clic en el icono "**+**"para agregar un servidor virtual y establezca los siguientes parámetros:

   a) Perfil de aplicación: de forma predeterminada, se muestra el perfil de servicio que creó en Citrix ADM.

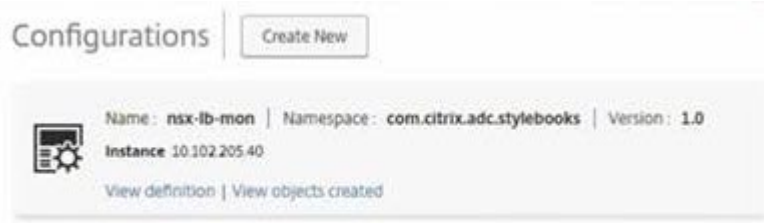
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Nombre: nombre del servidor virtual.

c) Dirección IP: haga clic en Seleccionar para seleccionar un grupo de direcciones IP existente o crear un grupo nuevo de direcciones IP.

d) Grupo predeterminado: seleccione el grupo predeterminado de la lista desplegable.

2. Haga clic en **Aceptar**.
3. En NetScaler ADM, vaya a **Orchestration** > **Solicitudes** para ver los detalles del progreso de la finalización de la creación del servicio en una o más instancias de NetScaler ADC seleccionadas.
4. En NetScaler ADM, vaya a **Aplicaciones** > **Configuración**y compruebe que se ha creado el paquete de `nsx-lb-mon` configuración.




## Configuración de Load Balancing Services en NetScaler ADC VPX en NetScaler ADM GUI

Implemente configuraciones del equilibrador de carga en la instancia de NetScaler ADC mediante NetScaler ADM StyleBooks. Para HA, la configuración se implementa en las dos instancias de Citrix ADC que están en HA.

**Para crear paquetes de configuración mediante StyleBooks:**

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración** > **Crear nuevo** y seleccione el **StyleBook HTTP/SSL LoadBalancing (con monitores)** de la lista. El StyleBook se abre como una página de interfaz de usuario en la que se introducen los valores de todos los parámetros definidos en este StyleBook.
2. Especifique valores para todos los parámetros requeridos.
3. Seleccione la instancia Citrix ADC VPX de destino que está aprovisionada en el entorno NSX y haga clic en **Crear** para aplicar la configuración en el dispositivo seleccionado. Para la implementación de alta disponibilidad, seleccione las instancias que están en modo de alta disponibilidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Verificación de la creación de servidores virtuales y grupos de servicios en instancias de Citrix ADC VPX

Puede ver que los grupos de servicios y los servidores virtuales se crean iniciando sesión en la instancia de Citrix ADC VPX.

**Para ver los grupos de servicios y los servidores virtuales:**

1. Inicie sesión en la instancia de NetScaler ADC VPX. Para la implementación de HA, debe iniciar sesión en las dos instancias de Citrix ADC que estén en HA.
2. Vaya a **Configuración** > **Sistema** > **Redes**. En el panel derecho, puede ver las direcciones IP que se han agregado. Haga clic en el hipervínculo de dirección IP para ver los detalles. Puede ver que la dirección IP de la subred es la misma que la dirección IP de la interfaz web que se agregó a NSX.
3. A continuación, vaya a **Administración del tráfico** > **Equilibrio de carga** > **Servidores virtuales** y consulte los detalles del servidor virtual.
4. A continuación, vaya a **Grupos de servicios** y consulte los detalles del grupo de servicios.
5. Por último, vaya a **Configuración** > **Sistema** > **Licencias** para ver las licencias que se aplican a esta instancia.

## Eliminar servicios de equilibrio de carga

Cuando los servicios de equilibrio de carga ya no son necesarios en las instancias de NetScaler ADC VPX implementadas en NSX Manager, puede eliminar las inserciones de servicio realizadas anteriormente.

**Para eliminar la configuración y la inserción de servicios:**

1. En Citrix ADM, vaya a **Aplicaciones** > **Configuración**, seleccione la configuración de la aplicación creada y, a continuación, elimínela haciendo clic en el icono «X».
2. En NSX Manager, navegue hasta la puerta de enlace perimetral a la que está conectada la instancia de Citrix ADC VPX. Vaya a **Administrar** > **Equilibrador de carga** > **Configuración global**, haga clic con el botón secundario en la entrada de tiempo de ejecución y, a continuación, haga clic en **Anular aprovisionamiento**. La máquina virtual está fuera de servicio.
3. En NetScaler ADM, vaya a **Orchestration** > **Cloud Orchestration** > **Edge Gateways**. Asegúrese de que no existe una asignación respectiva de la puerta de enlace Edge a la instancia eliminada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Automatización de Citrix ADC mediante Citrix ADM en el modo híbrido ACI de Cisco

January 30, 2024

Cisco ACI introdujo la compatibilidad con el modo híbrido en la versión 1.3 (2f). En el modo híbrido, puede realizar la automatización de la red a través del controlador de infraestructura de directivas de aplicaciones (APIC) y, al mismo tiempo, delegar la configuración L4-L7 a Citrix Application Delivery Management (ADM), que actúa como administrador de dispositivos en el APIC.

La solución Citrix ADC Hybrid Mode es compatible con un paquete de dispositivos de modo híbrido y Citrix ADM. Debe cargar el paquete de dispositivos de modo híbrido en la APIC. Este paquete proporciona todas las entidades configurables de red L2-L3 de Citrix ADC. StyleBook asigna la paridad de las aplicaciones desde Citrix ADM al APIC. En otras palabras, StyleBook actúa como referencia entre las configuraciones L2-L3 y L4-L7 para una aplicación determinada. Debe proporcionar un nombre de StyleBook al configurar las entidades de red desde el APIC para Citrix ADC.

La siguiente ilustración proporciona una descripción general de Citrix ADC en una solución de modo híbrido:

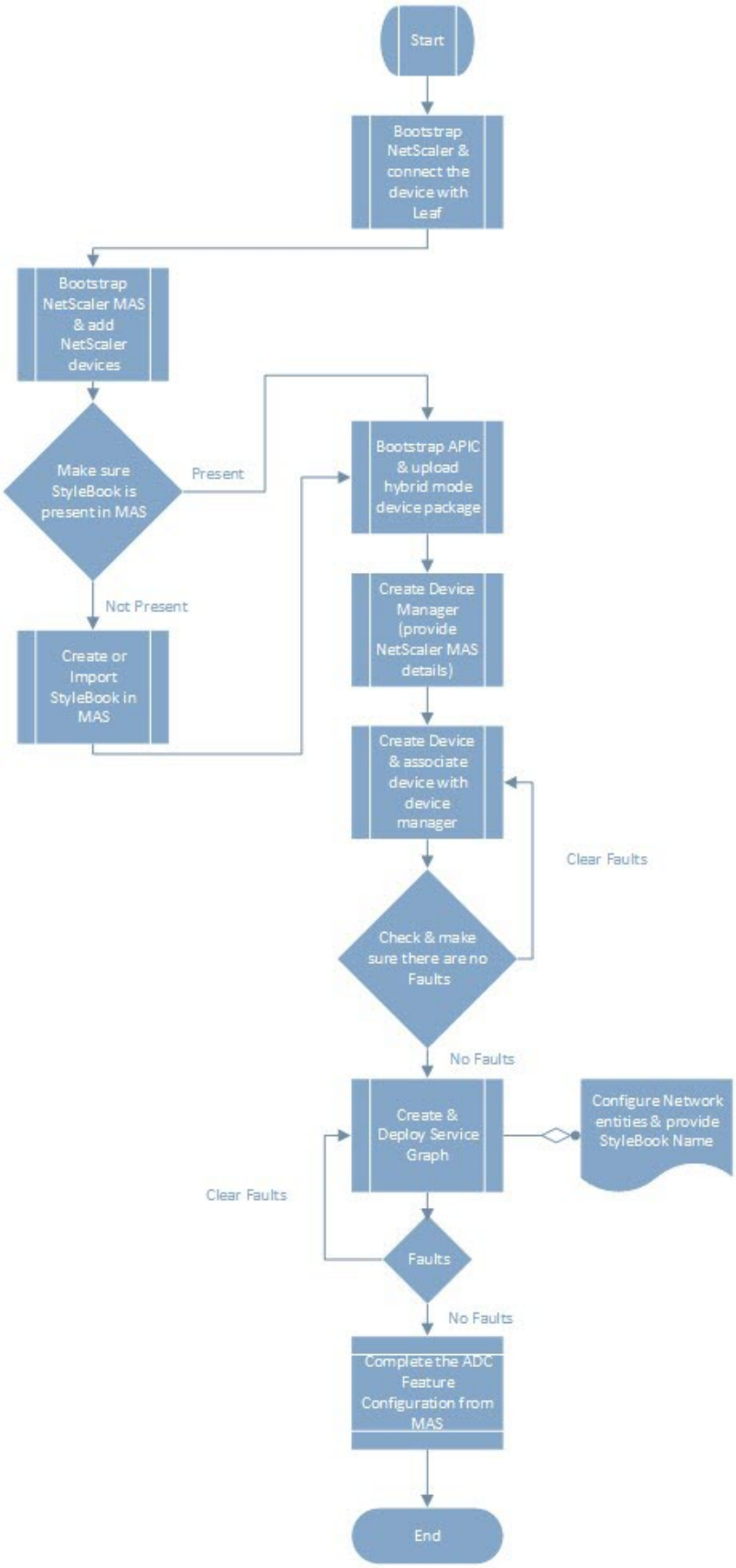
En el modo híbrido, la configuración de Citrix ADC se realiza en las dos fases siguientes:

1. La unión de redes se realiza desde el APIC de Cisco
2. La configuración se realiza desde Citrix ADM

Para cualquier aplicación determinada, el administrador de red debe proporcionar detalles específicos de la red, como las direcciones IP, el puerto, la VLAN (automatizada), etc., como parte de la creación e implementación del gráfico de servicios en el APIC de Cisco. A continuación, estos detalles de configuración se envían a Citrix ADM a través del paquete del dispositivo, y Citrix ADM los procesa internamente y configura el Citrix ADC. Un administrador de aplicaciones crea la configuración relacionada con el ADC de la aplicación mediante StyleBook en Citrix ADM y, a continuación, estas configuraciones se transfieren de Citrix ADM al Citrix ADC. Cisco APIC y Citrix ADM se comunican con el ADC a través de la red de administración.

El siguiente diagrama muestra un flujo de trabajo de Citrix ADC en la solución híbrida:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Requisitos previos

January 30, 2024

Compruebe que:

- Tiene conocimientos conceptuales sobre los componentes ACI de Cisco y los ADC de Citrix.
  - Para obtener más información sobre Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
  - Para obtener más información sobre los ADC de Citrix, consulte la documentación del producto NetScaler ADC en:http://docs.citrix.com/.
- Todos los componentes requeridos de Cisco ACI, incluido un Cisco APIC en el centro de datos, se configuran y configuran. Para obtener más información sobre Cisco ACI y sus componentes, consulte la documentación del producto en: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html.
- Ha instalado Citrix ADC 11.1 o posterior.
- Ha configurado los ADC de Citrix en Cisco ACI para que puedan administrarse mediante el APIC de Cisco.
- Ha implementado NetScaler Application Delivery Management (ADM) en su entorno. Para obtener más información, consulte NetScaler ADM 13.0.
- Se establece la conectividad de administración de APIC a NetScaler ADM y ADC.
- Tome nota de:
  - Las interfaces de conexión y las direcciones IP que se utilizan para la administración y la conectividad de rutas de datos.
  - Detalles del conmutador Leaf: direcciones IP, puertos, interfaces, etc. de Citrix ADC.

> **Nota**
>
> En esta versión, la solución de modo híbrido admite NetScaler ADC en un contexto único, es decir, no se admiten particiones administrativas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Configurar NetScaler ADC en modo híbrido mediante Cisco APIC y NetScaler ADM

January 30, 2024

Realice las siguientes tareas para configurar un Citrix ADC en modo híbrido mediante Cisco APIC y Citrix Application Delivery Management (ADM):

1. Agregue instancias de NetScaler ADC en su estructura a NetScaler ADM. Para obtener instrucciones, consulte Agregar una instancia a NetScaler ADM.
2. Utilice NetScaler ADM para crear un StyleBook para la aplicación. Para obtener instrucciones, consulte Creación de un StyleBook para la aplicación mediante NetScaler ADM.
3. Importe el paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC. Para obtener instrucciones, consulte Importación del paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC
4. Agregue NetScaler ADM como administrador de dispositivos en Cisco APIC. Para obtener instrucciones, consulte Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC
5. Utilice Cisco APIC para agregar un dispositivo NetScaler ADC en Cisco ACI. Para obtener instrucciones, consulte Agregar NetScaler ADC como dispositivo en Cisco ACI
6. Crear e implementar una plantilla de gráfico de servicio. Para obtener instrucciones, consulte Creación e implementación de un gráfico de servicio
7. Configure los parámetros L4-L7 mediante StyleBook en NetScaler ADM. Para obtener instrucciones, consulte Configurar el parámetro L4-L7 mediante StyleBook de NetScaler ADM
8. Adjuntar o desconectar eventos de punto final de la APIC de Cisco. Para obtener más información, consulte Adjuntar o separar eventos de punto final de APIC

## Crear un StyleBook para una aplicación mediante NetScaler ADM

January 30, 2024

Un StyleBook es una plantilla de configuración que puede utilizar para crear y administrar configuraciones de Citrix ADC para cualquier aplicación. Puede crear un StyleBook para configurar una función específica de Citrix ADC, como el equilibrio de carga, la descarga de SSL o la conmutación de contenido. Puede diseñar un StyleBook para crear configuraciones para una implementación de aplicaciones empresariales como Microsoft Exchange o Lync. Para obtener más información, consulte StyleBooks.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede crear su propio StyleBook para su aplicación o modificar y utilizar el StyleBook APIC-HTTP-LB suministrado con NetScaler Application Delivery Management (ADM).

Para crear su propio StyleBook para su aplicación en NetScaler ADM, consulte Cómo crear sus propios StyleBooks.

Al crear el StyleBook, asegúrese de seguir el modelo de gráfico de servicio de APIC en el StyleBook. En otras palabras, el gráfico de servicios de la APIC para cualquier aplicación sigue el modelo de consumidor y proveedor conectados a través de una función ADC. El consumidor y el proveedor se representan como un grupo de puntos finales (EPG) y tienen una relación de 1:1. También se debe seguir el mismo modelo en StyleBook, donde el proveedor EPG debe representarse como un grupo de servicios y cada punto final como un miembro del grupo de servicios. El nodo de la función ADC debe estar representado por un servidor virtual (por ejemplo, un servidor virtual de equilibrio de carga) y debe haber una relación 1:1 entre el servidor virtual y el grupo de servicios.

Básicamente, esto captura la esencia del gráfico de servicios y permite gestionar el evento de adjuntar o desconectar de la APIC, donde un evento de adjuntación vincula el punto final al grupo de servicios correspondiente y un evento de desvinculación lo desvincula. Debe asegurarse de que el gráfico de servicio y el StyleBook estén en paridad para una automatización perfecta desde las configuraciones de red L2-L3 a L4-L7 con función ADC.

## Importar paquete de dispositivos de modo híbrido NetScaler ADC en Cisco APIC

January 30, 2024

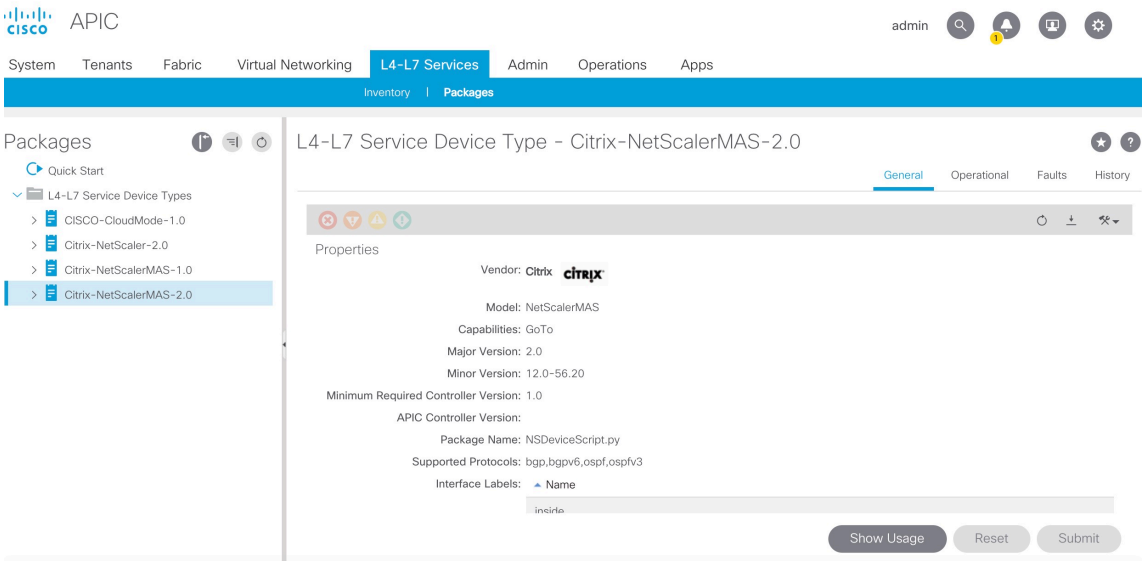
El paquete de dispositivos en modo híbrido es un paquete ligero en comparación con un modo totalmente gestionado. Solo los parámetros de red L2-L3 están disponibles en el modelo de dispositivo. El modelo de dispositivo solo tiene definida una función ADC genérica y cuatro perfiles de función basados en la implementación de Citrix ADC en la estructura (por ejemplo, un brazo y dos brazos y lo mismo con RHI). El nombre del paquete Dispositivo de modo híbrido es **NetScaler Hybrid Mode Device package 12.0 Build 56.20**. Busque el paquete de dispositivos Hybrid Mode en el sitio de descargas de Citrix, descárguelo e importe el paquete de dispositivos a la APIC.

> **Nota**
>
> El paquete de dispositivos de modo híbrido puede coexistir con un paquete de dispositivos de modo totalmente gestionado.

**Para importar el paquete de dispositivos en modo híbrido a la APIC mediante la GUI de APIC:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. **En la barra de menús, haga clic en la ficha**Servicios de nivel 4 a nivel 7**y seleccione el panel Paquetes.**
2. **En el panel de**navegación**, haga clic con el botón derecho en**Tipos de dispositivos de nivel 4 a nivel 7 y seleccione Importar paquete de dispositivos**.**
3. En el cuadro de diálogo **Importar paquete de dispositivos** , haga clic **en**Examinar para seleccionar el paquete de dispositivos de modo híbrido Citrix ADC descargado.
4. Haga clic en **Submit**.
   Tras importar correctamente el paquete del dispositivo a la APIC, en el panel de **navegación**, puede ver los detalles del paquete del dispositivo haciendo clic en el nombre del dispositivo.




> **Importante**
>
> Después de importar el paquete del dispositivo, asegúrese de que no haya errores en el APIC. Puede ver los errores haciendo clic en la ficha **Errores** de la ventana Tipos de dispositivos.

## Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC

January 30, 2024

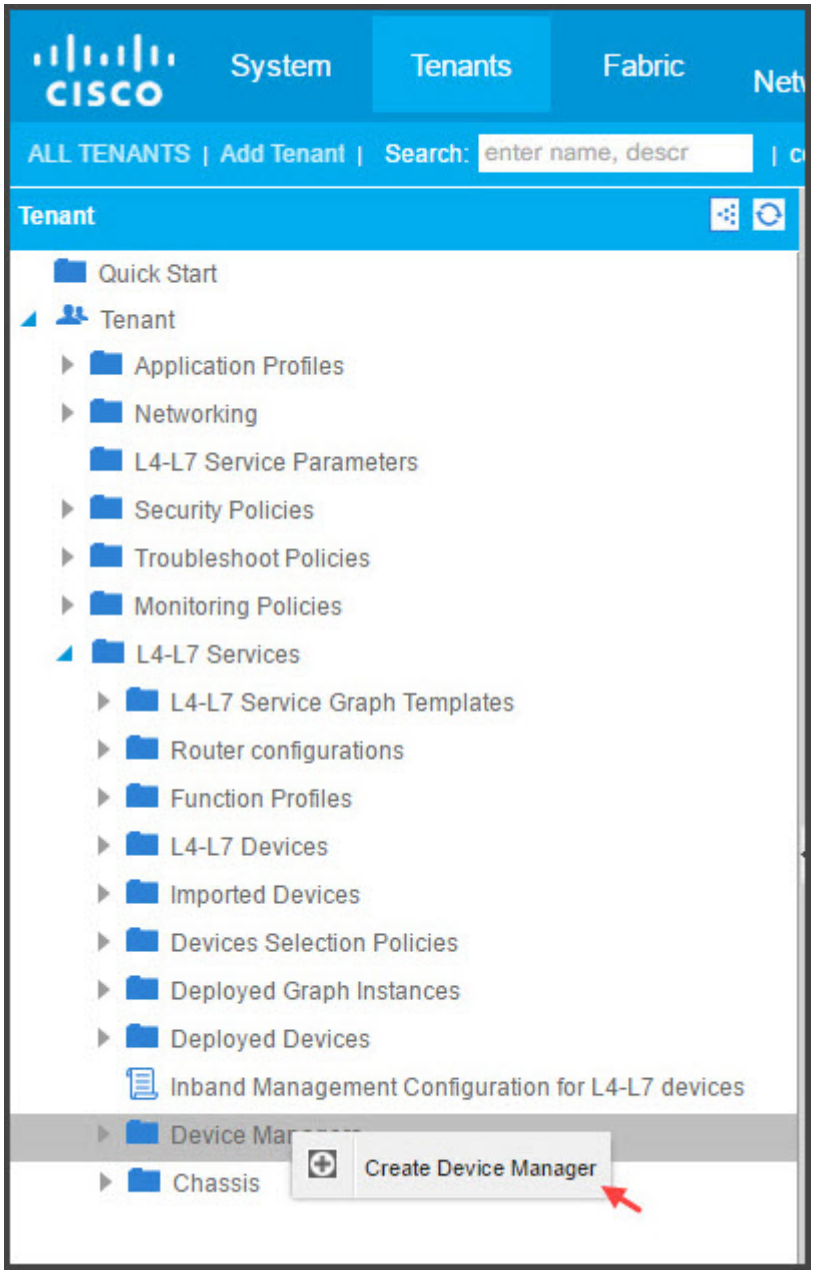
24 de mayo de 2018

Citrix Application Delivery Management (ADM) actúa como un administrador de dispositivos centralizado para Citrix ADC implementado en Cisco ACI. Debe agregar Citrix ADM como administrador de dispositivos en la APIC de Cisco.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para agregar Citrix ADM como administrador de dispositivos en la APIC mediante la GUI de APIC:**

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***nombre_de_arrendatario* > Servicios L4-L7.**
4. Haga clic con el botón derecho en **Administradores de dispositivos** y haga clic en **Crear administrador de dispositivos**.




5. En el cuadro de diálogo **Crear administrador de dispositivos**, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a) En el campo **Nombre del administrador de dispositivos** , introduzca un nombre para la implementación de Citrix ADM que desea registrar como administrador de dispositivos.

b) En la lista desplegable **EPG de administración**, seleccione la EPG de administración.

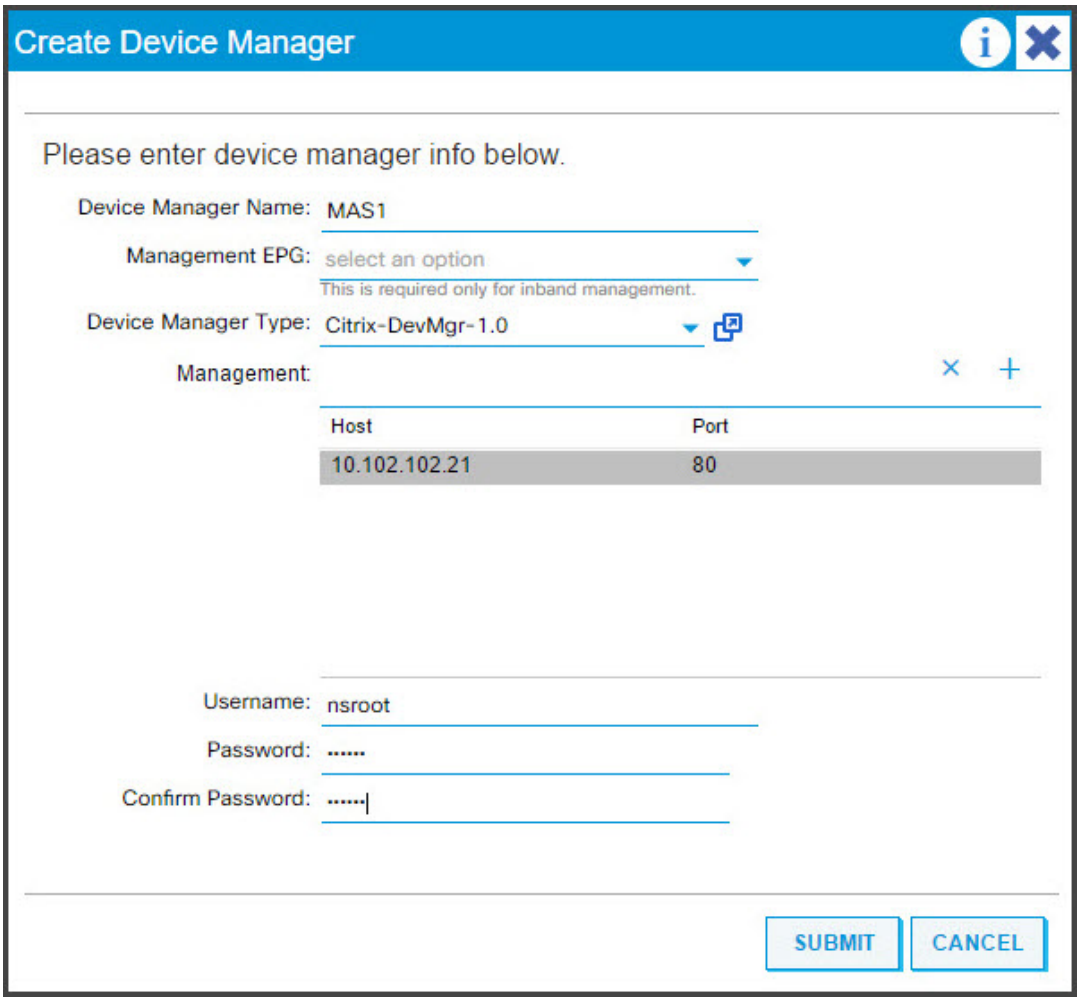
c) En la lista desplegable **Tipo de administrador de dispositivos**, seleccione **Citrix-DevMgr-1.0**.

d) En el campo **Administración** , haga clic en **+** y añada la dirección IP y los detalles del puerto de la implementación de Citrix ADM.

e) En el campo **Nombre** de usuario , introduzca el nombre de usuario para acceder a Citrix ADM.

f) En los campos **Contraseña** y **Confirmar contraseña** , introduzca la contraseña para acceder a Citrix ADM.

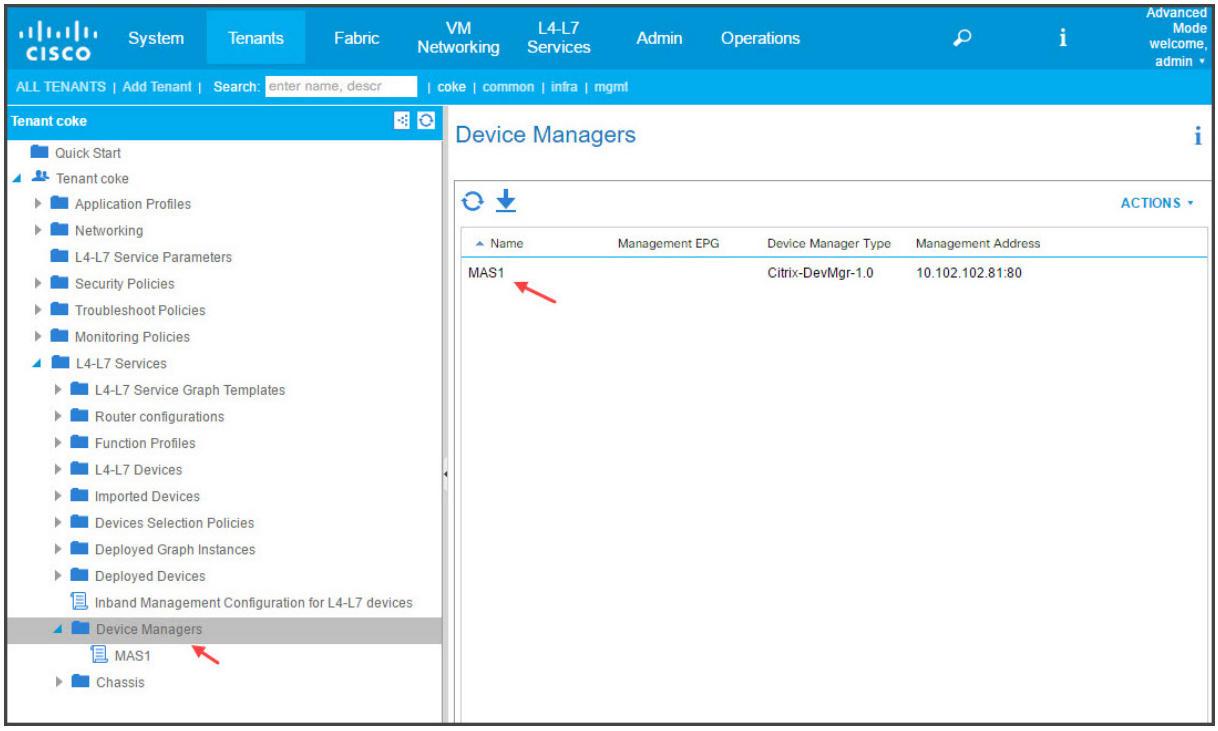
g) Haga clic en **ENVIAR**.




Una vez que Citrix ADM se haya registrado correctamente como administrador de dispositivos en la APIC, se agrega el administrador de dispositivos y se muestra en el panel de **navegación**. Para ver el

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

administrador de dispositivos registrado, en el panel de navegación, vaya a ***tenant_name* > Servicios L4-L7 > Administrador de dispositivos.**




> **Nota**
>
> Asegúrese de que no haya problemas de conectividad entre Cisco APIC y Citrix ADM y de proporcionar las mismas credenciales que utiliza para acceder al Citrix ADM. Asegúrese también de que la cuenta tenga privilegios de administrador.
>
> **Importante**
>
> Después de importar el paquete del dispositivo, asegúrese de que no haya errores en el APIC. Puede ver los errores haciendo clic en la ficha **Errores** de la ventana Tipos de dispositivos.

También puede registrar Citrix ADM como administrador de dispositivos mediante las API. A continuación se muestra una carga XML de ejemplo que muestra cómo puede utilizar las API para agregar NetScaler ADM como administrador de dispositivos.

```
<polUni>
    <fvTenant name="coke">
        <vnsDevMgr name="MAS1">
            <vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
            <vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
            <vnsCCred name="username" value="nsroot"/>
            <vnsCCredSecret name="password" value="*****("/>
        </vnsDevMgr>
    </fvTenant>
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
10 </polUni>
```

## Agregar NetScaler ADC como dispositivo en Cisco ACI mediante APIC

January 30, 2024

Debe agregar un Citrix ADC como dispositivo L4-L7 a la APIC para la automatización de la red. La APIC realiza la unión de red entre Leaf y el dispositivo Citrix ADC, según el gráfico de servicios implementado. Debe configurar los ajustes básicos de la configuración del dispositivo, como las direcciones IP de administración de la configuración, el administrador de dispositivos y las credenciales.

**Para registrar el Citrix ADC como dispositivo en la APIC mediante la GUI de APIC:**

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***nombre_arrendatario* > Servicios L4-L7 > Dispositivos L4-L7.**
4. En el panel Trabajo, seleccione **Acciones > Crear dispositivos L4-L7**.
5. En el cuadro de diálogo **Crear dispositivos L4-L7**, en la sección **General**, haga lo siguiente:
   a) Seleccione la casilla **Administrado**.
   b) En el campo **Nombre**, introduzca un nombre para el dispositivo.
   c) En la lista desplegable **de tipos de servicio**, seleccione **ADC**.
   d) En el campo **Tipo de dispositivo**, selecciona **Físico**.

      > **Nota**
      >
      > Asegúrese de que, para VMware ESX, seleccione Virtual y asocie el dominio de Virtual Machine Manager (VMM) correspondiente.

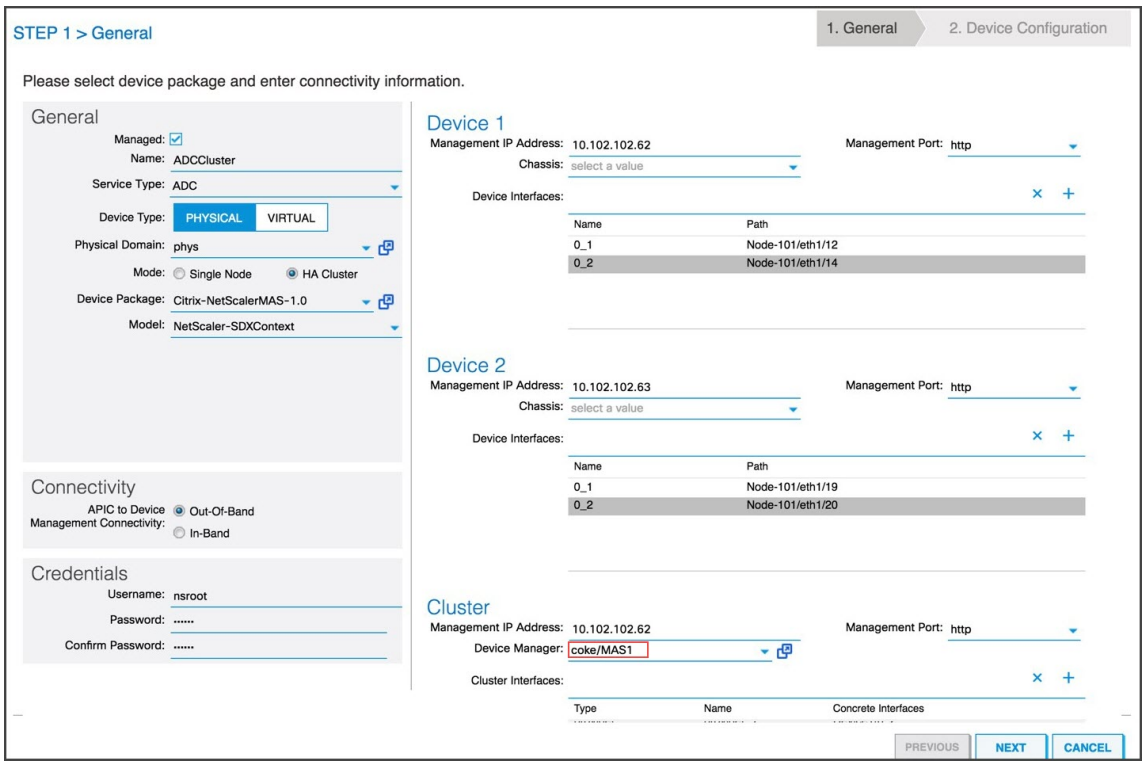
   e) En la lista desplegable **Dominio físico**, seleccione el dominio físico.
   f) En el campo **Modo**, seleccione **Nodo único** o **Clúster HA**, según sus necesidades.
   g) En la lista desplegable del **paquete de dispositivos**, seleccione **Citrix-NetScalerMAS-1.0**.
   h) En la lista desplegable **Modelo**, selecciona el modelo del dispositivo. Por ejemplo, Citrix ADC-MPX o Citrix ADC-VPX.
6. En la sección **Conectividad** , seleccione Fuera **de banda** o Dentro de **banda en** el campo **Conectividad de APIC a administración de dispositivos** , según cómo esté configurado Citrix ADC en la estructura.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. En la sección **Credenciales**, especifique el nombre de usuario y la contraseña para acceder al dispositivo.

8. En las secciones **Dispositivo 1** y **Dispositivo 2**, respectivamente, complete la configuración relacionada con la administración.

9. En la sección **Cluster**, complete la configuración relacionada con la administración del clúster. Asegúrese de que en la lista desplegable **Administrador de dispositivos**, seleccione el administrador de dispositivos que creó en Agregar NetScaler ADM como administrador de dispositivos en Cisco APIC



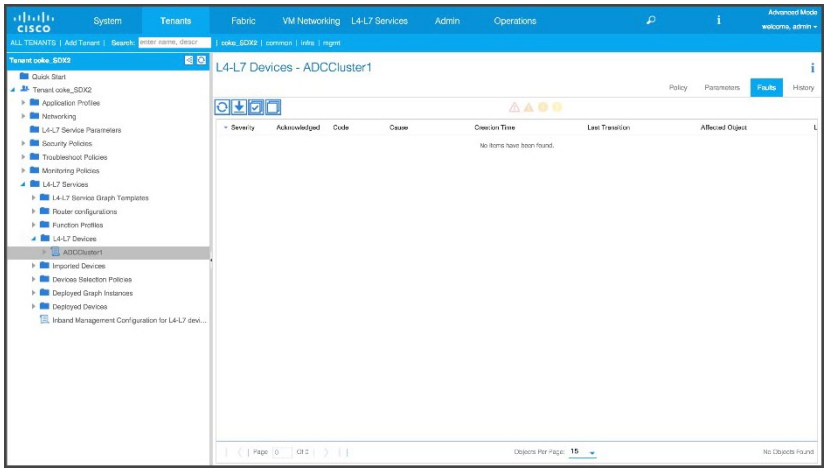

10. Haga clic en **SIGUIENTE**. Aparece la página Configuración del dispositivo. El paquete de dispositivos en modo híbrido no proporciona detalles de configuración específicos del dispositivo y el clúster, como la alta disponibilidad, las funciones y modos de habilitación/desactivación, la configuración de NTP, SNMP, alarmas SNMP, etc. Estas configuraciones deben realizarse mediante Citrix ADM.

11. Haga clic en **FINALIZAR**. Cuando haya registrado correctamente el dispositivo en la APIC, se agregará el dispositivo y se mostrará en el panel de navegación. Para ver el dispositivo registrado, en el panel de navegación, vaya a ***nombre_arrendatario* > Servicios L4-L7 > Dispositivos L4-L7 > nombre_dispositivo.**

> **Importante**
>
> Después de registrar el dispositivo, asegúrese de que no haya errores en el APIC. Puede ver

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> los errores haciendo clic en la ficha **Errores** del panel **Trabajo**.




También puede registrar un dispositivo Citrix ADC mediante API. A continuación se muestra una carga útil XML de ejemplo para agregar dispositivo L4-L7:

```
<polUni>

    <fvTenant name="coke">

    <vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

     <vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

     <vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

     <vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     <vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

     <vnsCDev name="ADC1" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /33]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /35]"/>

```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
31      </vnsCIf>
32
33      <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>
34
35      <vnsCCred name="username" value="nsroot"/>
36
37      <vnsCCredSecret name="password" value="****"/>
38
39      </vnsCDev>
40
41      <vnsCDev name="ADC2" devCtxLbl="C1">
42
43      <vnsCIf name="1_1">
44
45      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
           /34]"/>
46
47      </vnsCIf>
48
49      <vnsCIf name="1_2">
50
51      <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
           /36]"/>
52
53      </vnsCIf>
54
55      <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57      <vnsCCred name="username" value="nsroot"/>
58
59      <vnsCCredSecret name="password" value="****"/>
60
61      </vnsCDev>
62
63      <vnsLIf name="outside">
64
65      <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
           mIfLbl-outside"/>
66
67      <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
           cIf-1_1"/>
68
69      <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
           cIf-1_1"/>
70
71      </vnsLIf>
72
73      <vnsLIf name="inside">
74
75      <vnsRsMetaIf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/
           mIfLbl-inside"/>
76
77      <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC1/
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
            cIf-1_2"/>

        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
            cIf-1_2"/>

        </vnsLIf>

        </vnsLDevV

        </fvTenant>

        </polUni>
```

## Crear e implementar un gráfico de servicio

January 30, 2024

Debe usar las plantillas de gráficos de servicio APIC de Cisco en APIC para crear e implementar los ADC de Citrix. Asegúrese de utilizar el perfil de función ADC al crear e implementar un gráfico de servicio.

Una vez configurado el gráfico en el APIC, el APIC automatiza la configuración del dispositivo basándose en las definiciones de las funciones, la conectividad del dispositivo con la estructura y las entidades configuradas como parte de la implementación del gráfico. La APIC también automatiza la configuración de la red, como la asignación de VLAN y su enlace, como parte de la creación del gráfico de servicio, y la configuración se elimina una vez que se elimina el gráfico del APIC.

Un gráfico de servicio se representa como dos o más niveles de una aplicación, con la función de servicio correspondiente insertada entre ellos. Un contrato inserta un gráfico de servicio entre las EPG de origen y destino.

**Para crear un gráfico de servicio mediante la interfaz gráfica de usuario de APIC:**

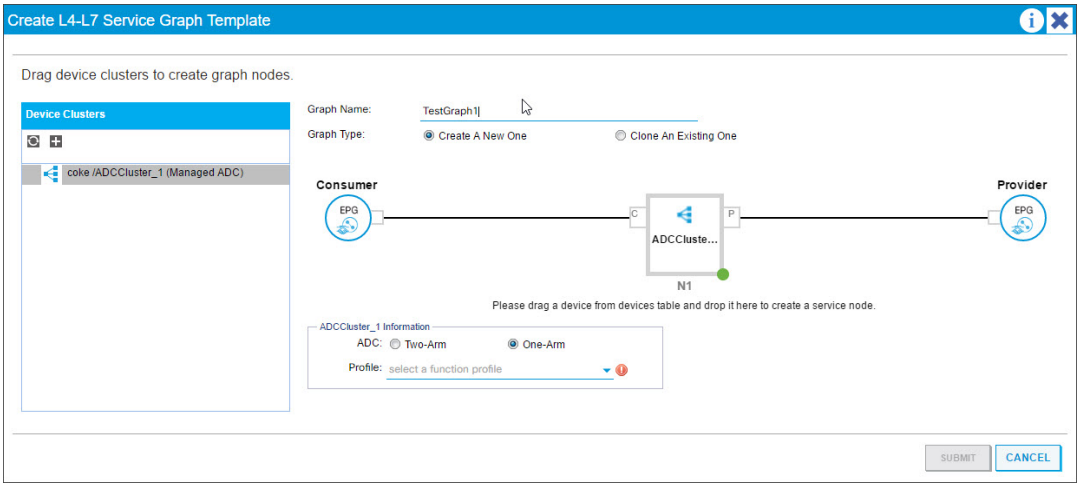
1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de **navegación**, seleccione ***tenant_name* > Servicios L4-L7 > Plantillas de gráficos de servicios L4-L7.**
4. En el panel **Trabajo**, seleccione **Acciones > Crear una plantilla de gráfico de servicio L4-L7**.
5. En el cuadro de diálogo **Crear una plantilla de gráficos de servicio L4-L7**, en la sección Clústeres de dispositivos, seleccione un clúster de dispositivos y haga lo siguiente:

    a) En el campo **Nombre del gráfico**, introduzca el nombre de la plantilla de gráfico de servicio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) En el campo **Tipo de gráfico**, seleccione **Crear uno nuevo**.

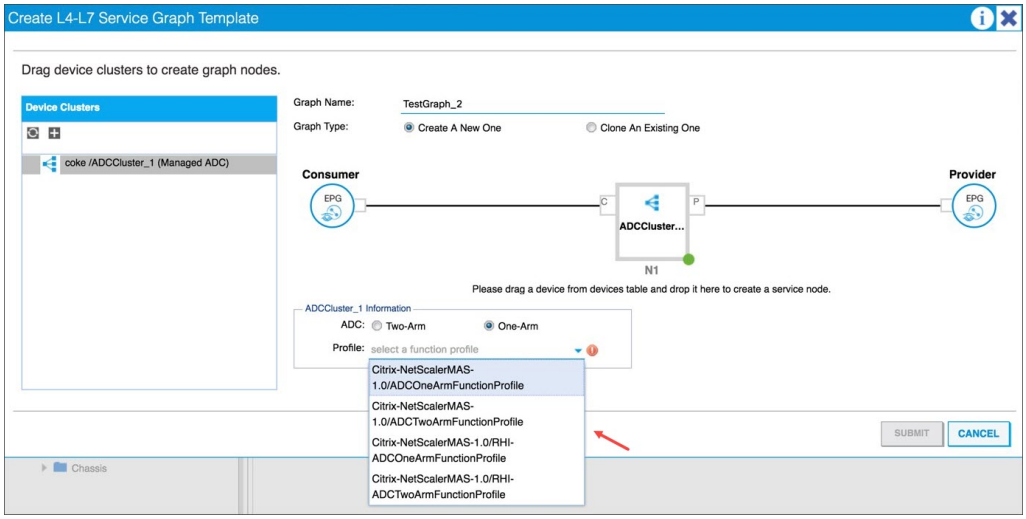
c) En la sección **Clúster de dispositivos**, arrastre el dispositivo y suéltelo entre el grupo de puntos finales del consumidor y el grupo de puntos finales del proveedor para crear un nodo de servicio.




d) En la sección < L4-L7Device_name information >**, haga lo siguiente:

i. En el campo **ADC** , seleccione **One-Arm** o **Two-Arm** , según cómo esté implementado el Citrix ADC en la estructura.

ii. En la lista desplegable **de perfiles**, seleccione el perfil de función que se proporciona en el paquete del dispositivo.

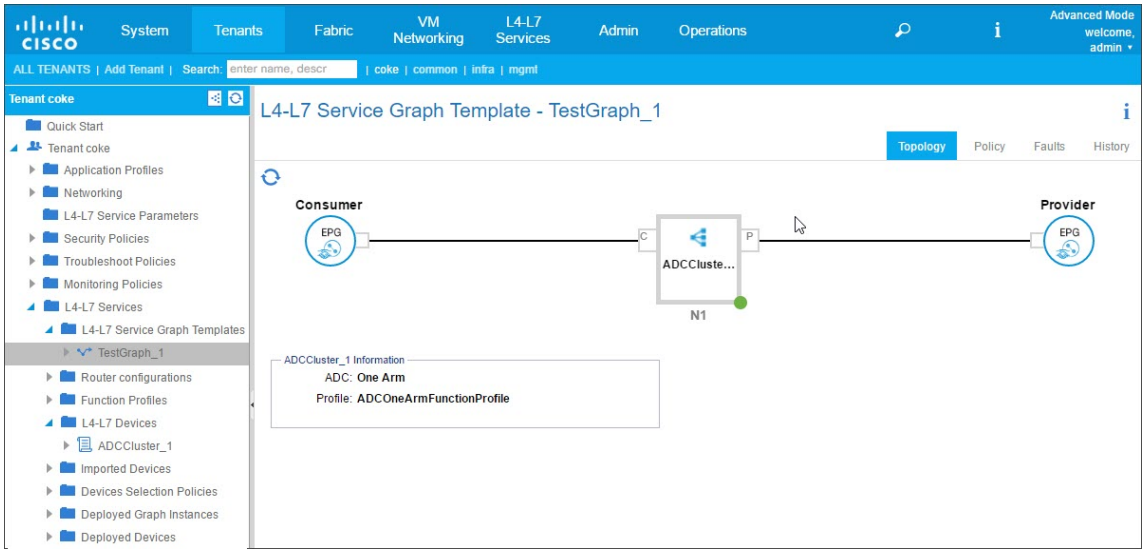



iii. Haga clic en **ENVIAR**.

6. En el panel **de navegación**, haga clic en la plantilla del gráfico de servicios. La pantalla presenta una topología gráfica de la plantilla de gráficos de servicios.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> El APIC de Cisco admite la noción de conectores, y estos conectores están visibles en el nodo ADCCluster. Los conectores definen la dirección del tráfico de red y el script del dispositivo que vincula dinámicamente la VLAN asignada a una dirección IP virtual (VIP) o IP de subred (SNIP), dependiendo de si la conexión es externa o interna. Las VLAN también están enlazadas a interfaces específicas que se utilizan para el tráfico entrante y saliente.



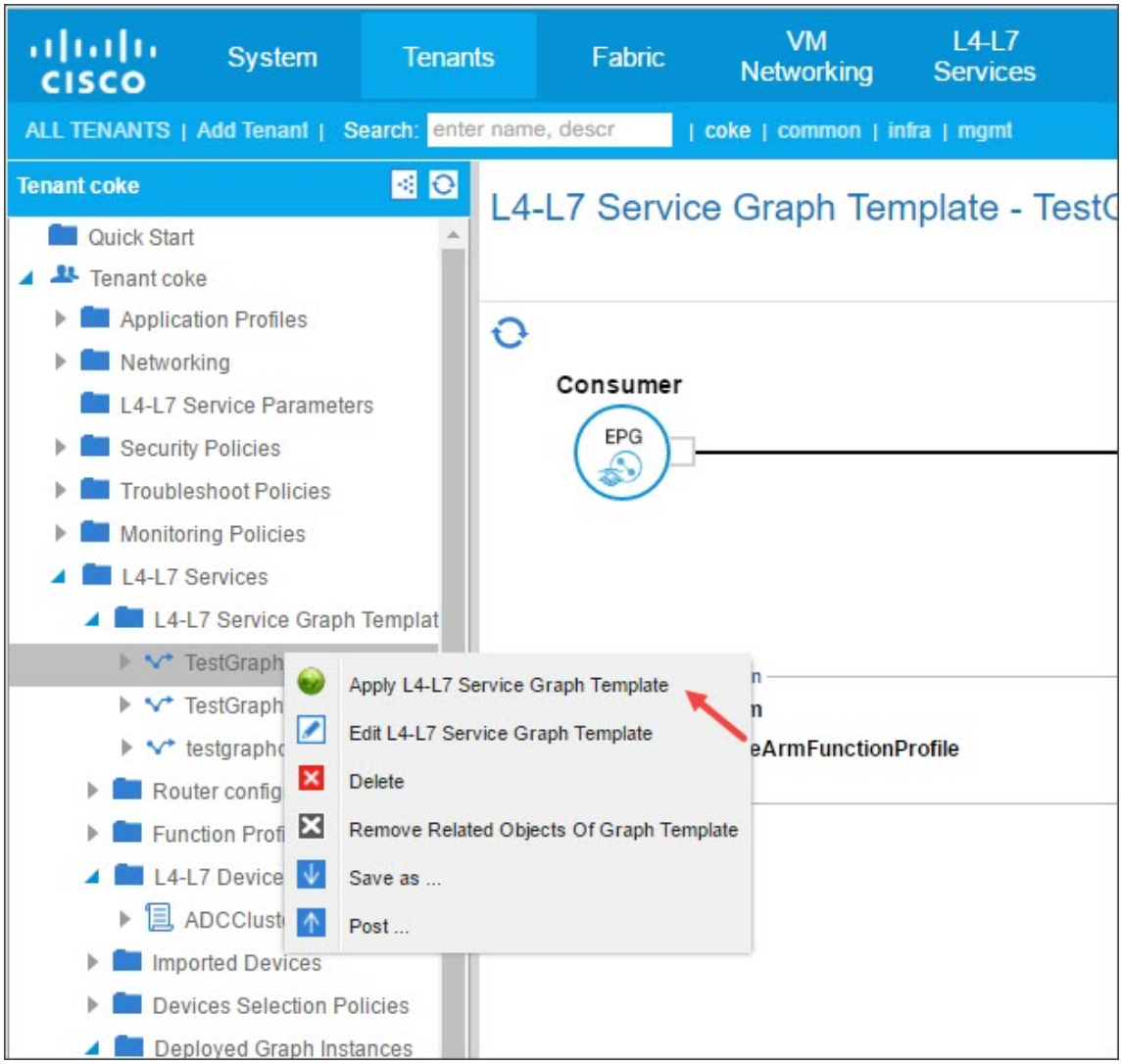

## Aplicación de la plantilla de gráficos de servicio a grupos de terminales

Una vez creada la plantilla de gráfico de servicio, debe aplicar la plantilla de gráfico de servicio creada mediante la interfaz gráfica de usuario de APIC.

**Para aplicar la plantilla de gráficos de servicios:**

1. En la barra de menús, ve a **Arrendatarios > Todos los arrendatarios**.
2. En el panel **Trabajo**, haga doble clic en el nombre del arrendatario.
3. En el panel de navegación, elija ***tenant_name* > Servicios L4-L7 > Plantillas de gráficos de servicios L4-L7.**
4. Haga clic con el botón derecho en el ***nombre de la plantilla y haga clic en*Aplicar plantilla de gráfico de servicio L4-L7**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



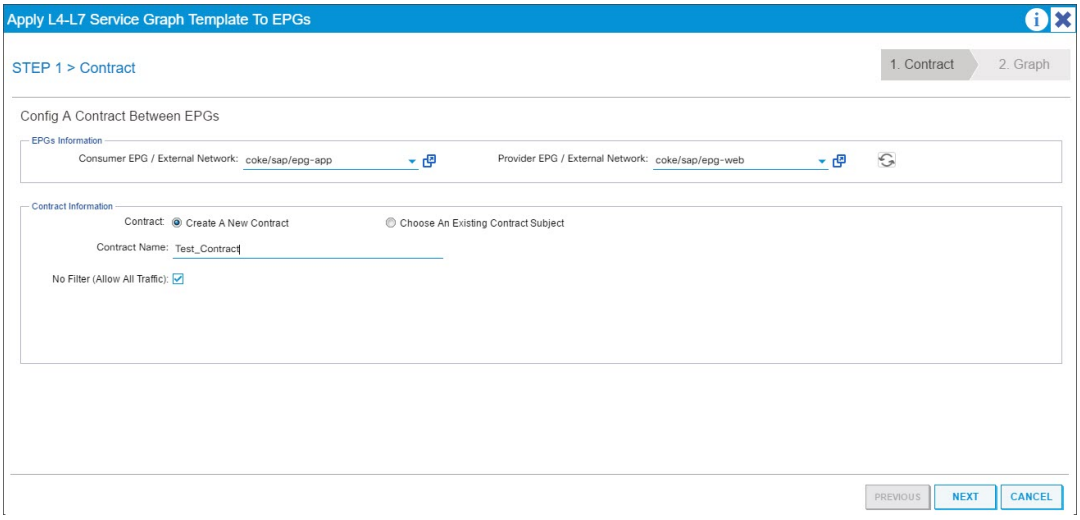

5. En el cuadro de diálogo **Aplicar plantilla de gráfico de servicio L4-L7 a las EPG**, en la sección **Información de la EPG**, complete los siguientes campos:

   a) En la lista desplegable **Consumer EPG/External Network**, seleccione el grupo de terminales de consumo.

   b) En la lista desplegable **Provider EPG/External Network**, seleccione el grupo de puntos de conexión proporcionado.

   c) En la sección **Información del contrato**, complete los campos correspondientes. La información del contrato es específica de la APIC de Cisco y está configurada como parte de las directivas de seguridad asociadas a las EPG.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




d) Haga clic en **Siguiente**.

e) En la lista desplegable **de plantillas de gráficos**, seleccione la plantilla de gráficos de servicio que creó.

f) En la sección **Conector**, haga lo siguiente:

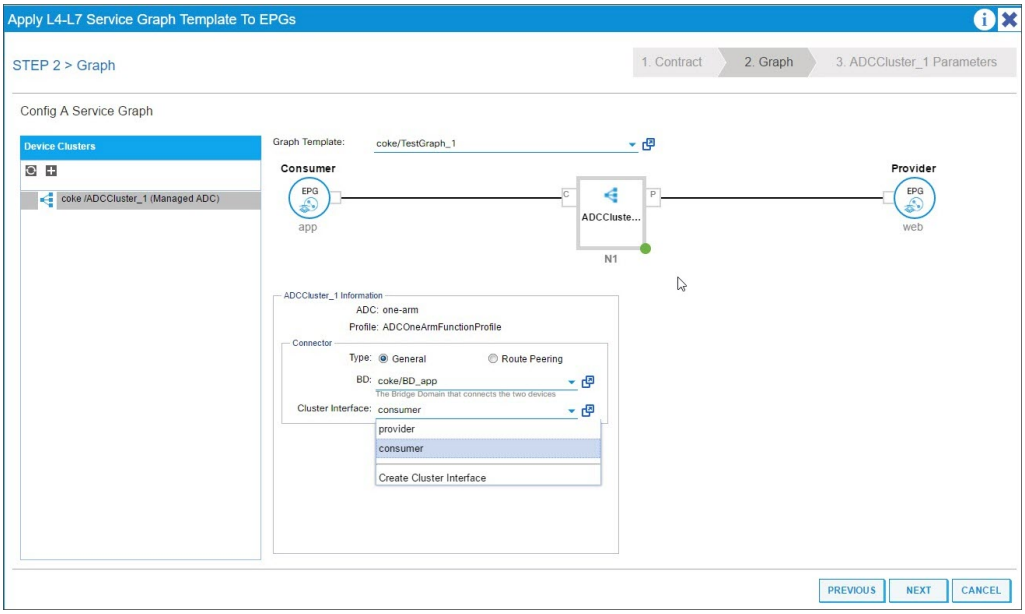
   i. En el campo **Tipo**, seleccione General.

   ii. En la lista desplegable de **BD**, seleccione el dominio puente. Los detalles del conector forman parte del dominio puente que forma parte del modelo de infraestructura APIC de Cisco.

   iii. En la lista desplegable **Interfaz de clúster**, seleccione la interfaz de clúster adecuada para el dominio puente seleccionado.

   El APIC de Cisco utiliza los dominios puente seleccionados para el tráfico de rutas de datos entre el dispositivo Citrix ADC y la estructura, según lo exige la plantilla de gráfico de servicio seleccionada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

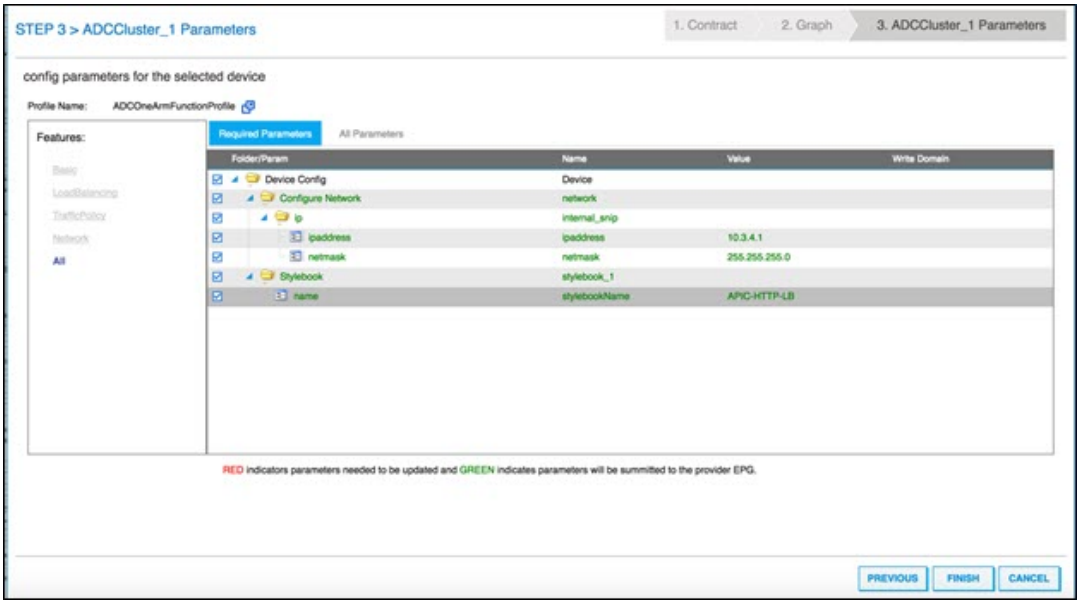



iv. Haga clic en **Siguiente**.

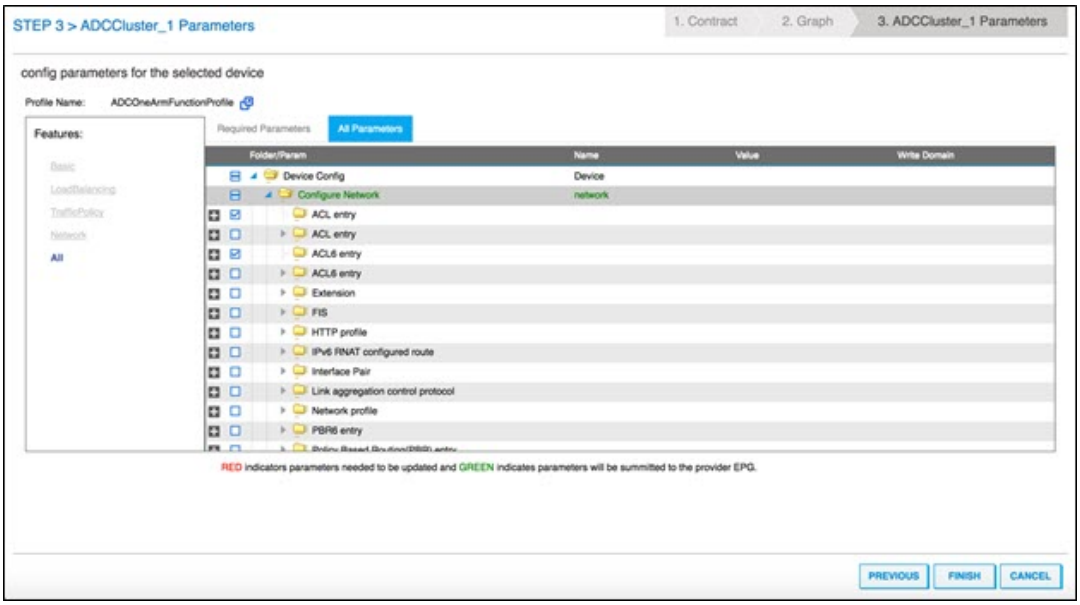
En la pantalla **Parámetros**, en la ficha **Parámetros obligatorios**, introduzca los detalles específicos de L2-L3, como la dirección IP que exige el perfil. El otro parámetro clave es el nombre de StyleBook. Puede ser el StyleBook **APIC-HTTP-LB** integrado que se proporciona en NetScaler Application Delivery Management (ADM) o puede proporcionar el nombre del StyleBook que creó en Creación de un StyleBook para la aplicación con NetScaler ADM

> **Nota**
>
> El nombre StyleBook vincula los detalles de Service Graph con la configuración L4-L7 creada con Citrix ADM para una aplicación determinada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




La GUI de Cisco APIC le permite filtrar los parámetros en función de las características (por ejemplo, el equilibrio de carga). Puede ver y configurar todos los parámetros obligatorios en la ficha **Parámetros obligatorios**, y puede ver y configurar todos los demás parámetros relacionados con la función en la ficha **Todos los parámetros**.



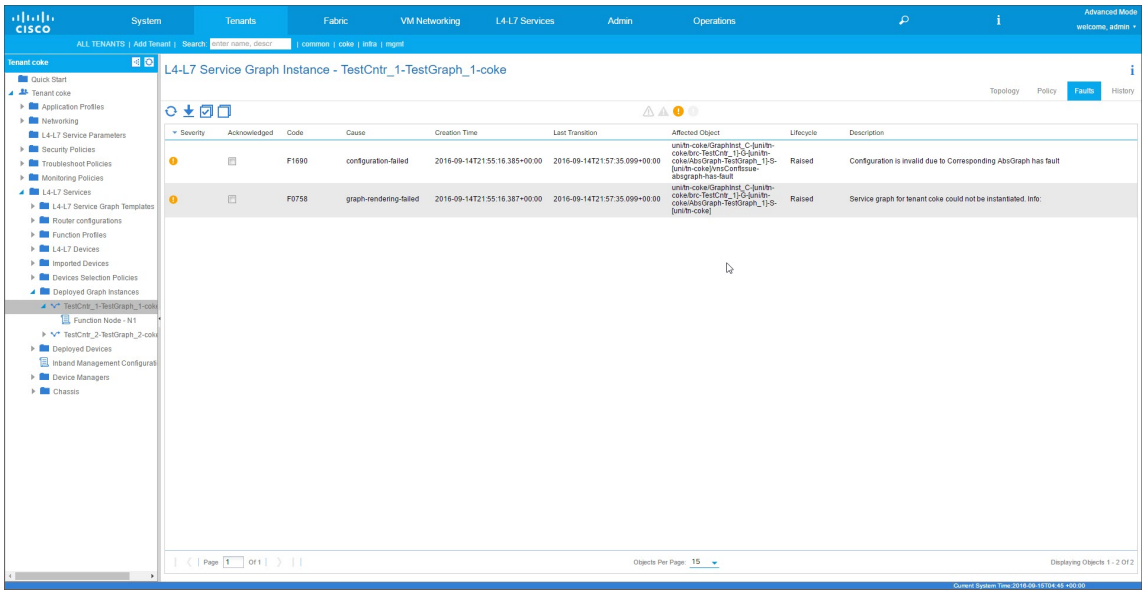

> **Nota**
>
> De forma predeterminada, un perfil integrado de un solo brazo requiere que proporciones detalles del SNIP, como la dirección IP y la máscara de red. Puede ver otros parámetros de red haciendo clic en **Todos los parámetros** y expandiendo el árbol **Configurar red** en la GUI de Cisco APIC. Aquí se enumeran todos los parámetros de red admitidos por Citrix ADC. Puede crear una instancia de cualquier entidad y pro-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> porcionar valores para los atributos enumerados desde la GUI de Cisco APIC.

6. Haga clic en **Finalizar**.

> **Importante**
>
> Después de aplicar la plantilla de gráfico de servicio, asegúrese de que no haya errores en el gráfico implementado. Puede ver los errores haciendo clic en la ficha **Errores** del panel **Trabajo**.




Como parte de la implementación de Service Graph, el paquete Hybrid Mode Device envía los detalles de configuración del APIC de Cisco al Citrix ADM. El Citrix ADM procesa internamente estas configuraciones en el Citrix ADC correspondiente y devuelve la respuesta a la APIC. Una implementación de gráficos exitosa no tendrá ningún error y el Citrix ADC se conectará correctamente en red con la estructura del gráfico correspondiente.

La APIC admite diferentes formas de configurar e implementar gráficos mediante el uso de API, y la implementación de gráficos incluye varias dependencias de algunas construcciones específicas de la API, como Tenant, contract, VLAN y namespace.

El siguiente enfoque de ejemplo ilustra una de las formas de utilizar las API de la APIC para crear e implementar gráficos L4-L7, suponiendo que los artefactos específicos de la APIC ya están configurados en la APIC.

> **Importante**
>
> Asegúrese de utilizar estas cargas XML como referencia y realice los cambios adecuados en el XML antes de utilizarlas en su entorno.

A continuación se muestra un ejemplo de cómo crear e implementar el gráfico de servicios mediante API:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

a) Crear perfil de aplicación

b) Crear detalles del gráfico de servicios

c) Adjunte el gráfico de servicio a un contrato

A continuación se muestra un ejemplo de carga XML para crear un AppProfile. El AppProfile contiene las EPG y la EPG del proveedor contiene las entidades, los atributos y sus valores específicos de Citrix ADC. En el siguiente ejemplo de carga útil XML, se crean entidades de red específicas de Citrix ADC, como el NSIP, con un conjunto de atributos y un nombre de StyleBook.

```
<polUni>
    <fvTenant name="coke">
        <!-- Application Profile -->
        <fvAp dn="uni/tn-coke/ap-sap" name="sap">
            <!-- EPG 1  -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
                <fvRsBd tnFvBDName="BD_web" />
                <!-- --------- CONFIG PAYLOAD ---------------- -->
                <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name="Network">
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip1">
                        <vnsParamInst key="ipaddress" name="ip1" value="110.110.110.2"/>
                        <vnsParamInst key="netmask" name="netmask1" value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value="SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1" graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="snip2">
                        <vnsParamInst key="ipaddress" name="ip2" value="220.220.220.2"/>
                        <vnsParamInst key="netmask" name="netmask2" value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value="SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                </vnsFolderInst>
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
25                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
26                      <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
27                  </vnsFolderInst>
28                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
29                      <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
30                  </vnsFolderInst>
31                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    external_network" name="external_network">
32                      <vnsCfgRelInst name="external_network_key" key
    ="external_network_key" targetName="Network/snip2"/>
33                  </vnsFolderInst>
34                  <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
    " name="mFCngStylebook_1">
35                      <vnsCfgRelInst name="Stylebook_key" key="
    Stylebook_key" targetName="stylebook_1"/>
36                  </vnsFolderInst>
37                  <!-- ------- END CONFIG PAYLOAD -------------- -->
38                  <fvSubnet ip="110.110.110.110/24" scope="shared"/>
39                  <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
40                  <fvRsDomAtt tDn="uni/phys-sepg" />
41                  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
42              </fvAEPg>
43              <!-- EPG 2 -->
44              <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
45                  <fvRsCons tnVzBrCPName="Ctrct1"/>
46                  <fvRsBd tnFvBDName="BD_app" />
47                  <fvSubnet ip="220.220.220.220/24" scope="shared"/>
48                  <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
49                  <fvRsDomAtt tDn="uni/phys-sepg" />
50              </fvAEPg>
51          </fvAp>
52      </fvTenant>
53  </polUni>
```

A continuación se muestra un ejemplo de carga XML para crear detalles de gráficos de servicios:

```
1  <polUni>
2      <fvTenant name="coke">
3          <vnsAbsGraph name = "Graph1">
4              <vnsAbsTermNodeProv name = "Input1">
5                  <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
6              </vnsAbsTermNodeProv>
7              <vnsAbsNode name="ADC" funcType="GoTo">
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
8                   <vnsAbsFuncConn name = "outside" attNotify="true">
9                       <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
10                  </vnsAbsFuncConn>
11                  <vnsAbsFuncConn name = "inside" attNotify="true">
12                      <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
13                  </vnsAbsFuncConn>
14                  <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction"/>
15                  <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/outtmnl"/>
16                  <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix
    -NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
    ADCOneArmServiceProfileGroup/absFuncProf-A
17  DCOneArmFunctionProfile"/>
18                  <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
    ADCCluster1"/>
19              </vnsAbsNode>
20              <vnsAbsTermNodeCon name = "Output1">
21                  <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
22              </vnsAbsTermNodeCon>
23              <vnsAbsConnection name = "CON1">
24                  <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeCon-Output1/AbsTConn" />
25                  <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-outside" />
26              </vnsAbsConnection>
27              <vnsAbsConnection name = "CON2">
28                  <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-inside" />
29                  <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/AbsTConn" />
30              </vnsAbsConnection>
31          </vnsAbsGraph>
32      </fvTenant>
33  </polUni>
```

A continuación se muestra una carga útil XML de ejemplo para adjuntar el gráfico de servicio a un contrato:

```
1  <polUni>
2      <fvTenant name="coke">
3          <vzBrCP name="Ctrct1">
4              <vzSubj name="http">
5                  <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
6              </vzSubj>
7          </vzBrCP>
8      </fvTenant>
9  </polUni>
```

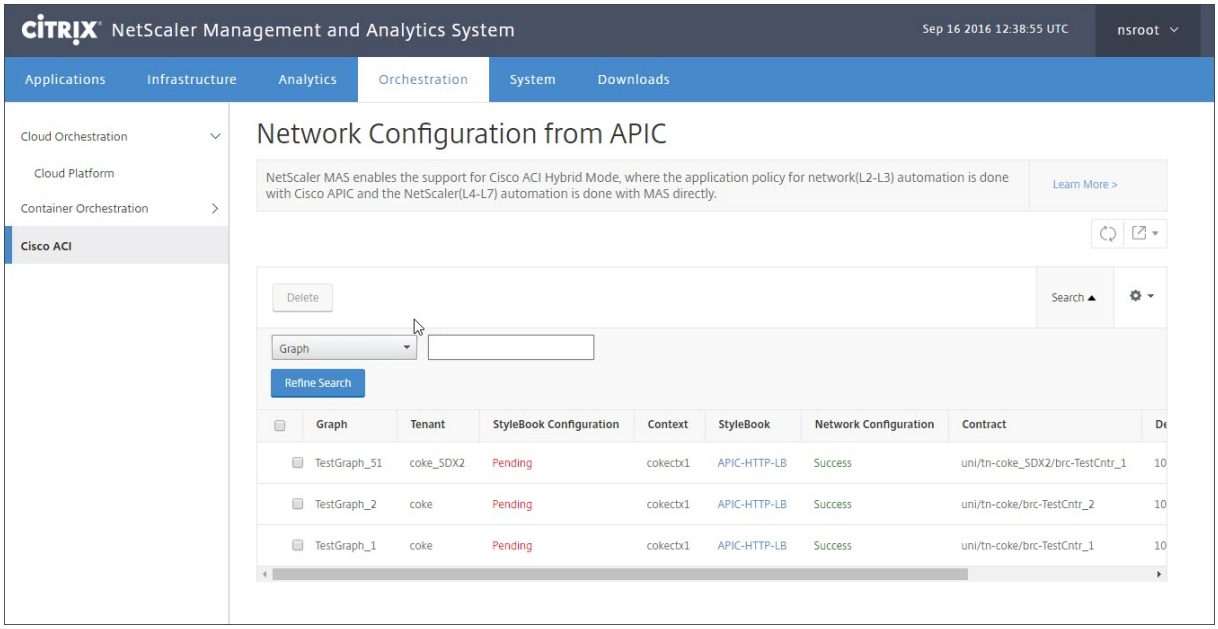
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Configure los parámetros L4-L7 desde NetScaler ADM con StyleBook

January 30, 2024

24 de mayo de 2018

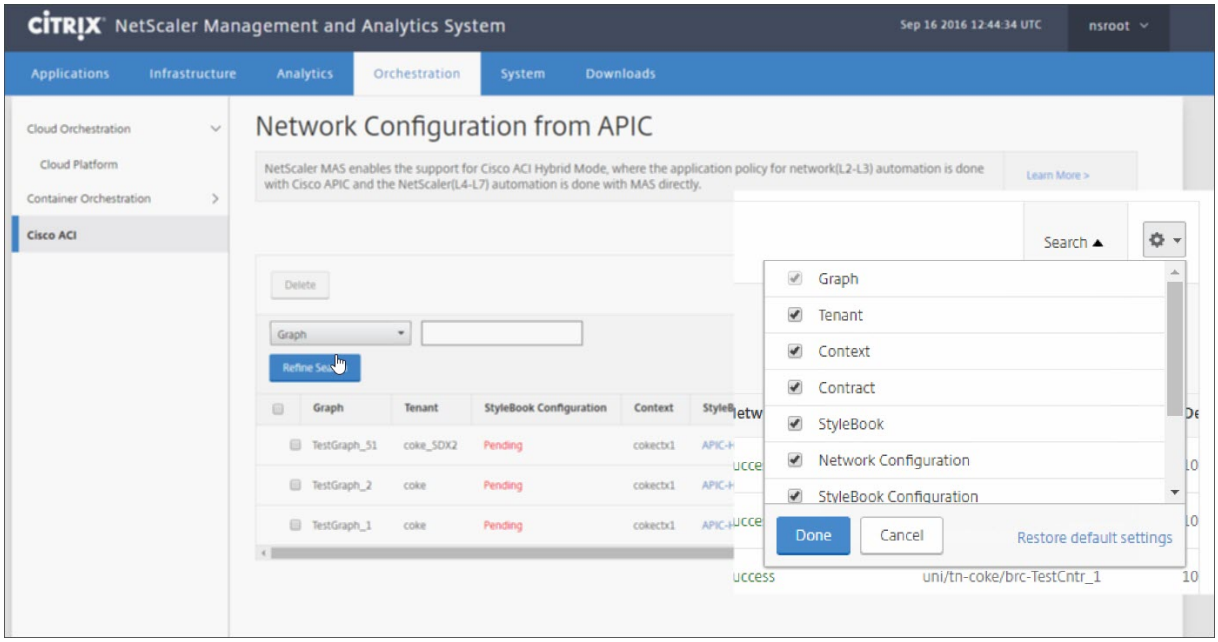
En Citrix Application Delivery Management (ADM), puede ver los detalles del gráfico del servicio implementado en la pestaña **Orchestration** , en **Cisco ACI**. La vista tabular muestra los detalles del gráfico de servicio, como el nombre del gráfico, el nombre del arrendatario, el contexto, el nombre de StyleBook y el estado de la configuración de la red.




> **Nota**
>
> Si el gráfico se elimina del APIC de Cisco, se elimina la configuración correspondiente del dispositivo, incluida la configuración L4-L7.

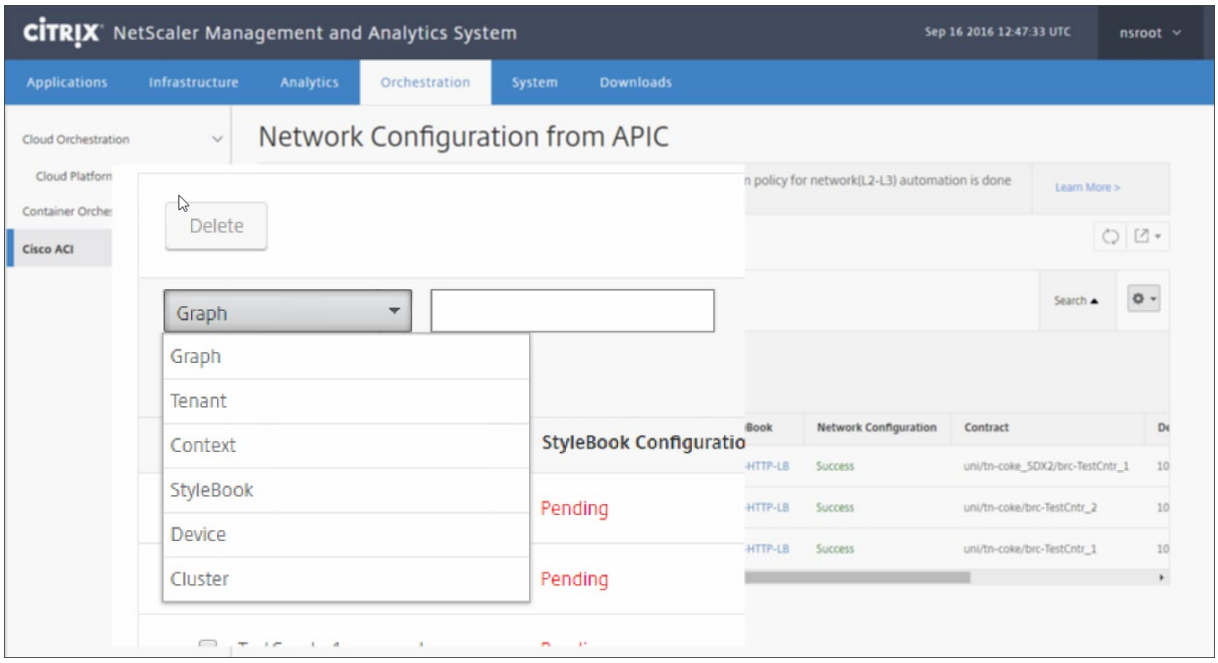
Además, la vista tabular permite ordenar cualquier columna de la tabla y filtrar los datos mediante la opción Buscar. También puede personalizar los detalles de las columnas seleccionando o deseleccionando los nombres de las columnas en la lista desplegable de columnas:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Además, puede hacer clic en el botón **Buscar** y utilizar las opciones de búsqueda para filtrar los datos. Puede seleccionar cualquier columna del cuadro desplegable e introducir el valor correspondiente para filtrar los datos que se muestran en la tabla.

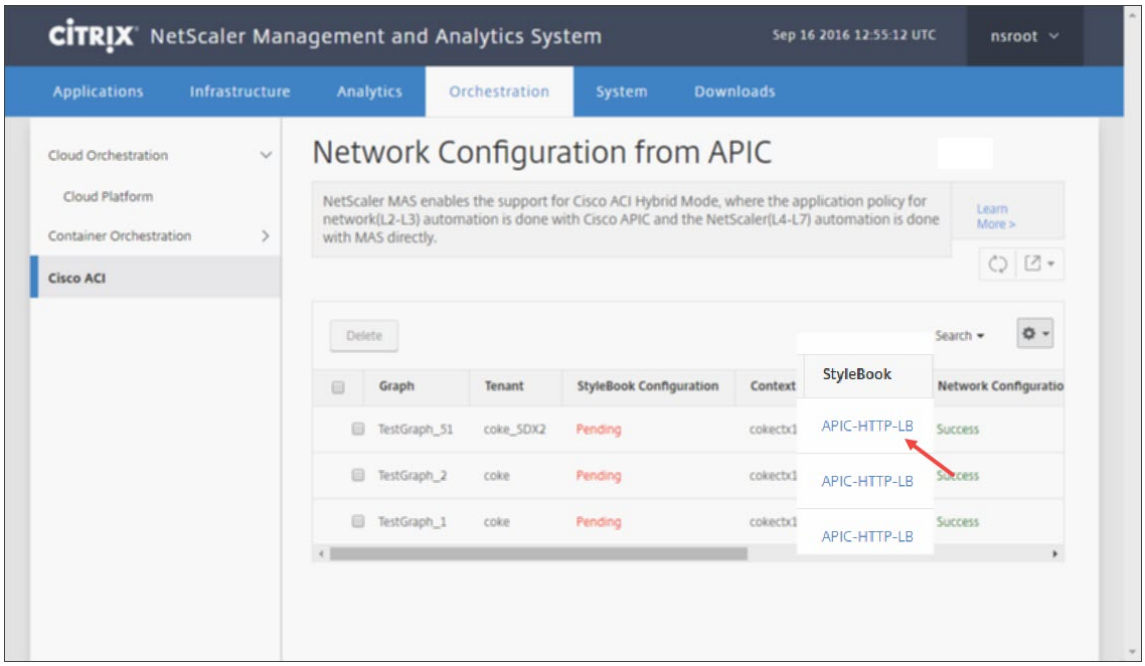
> **Nota**
>
> La función de búsqueda distingue mayúsculas de minúsculas y debe proporcionar los criterios de búsqueda exactos.



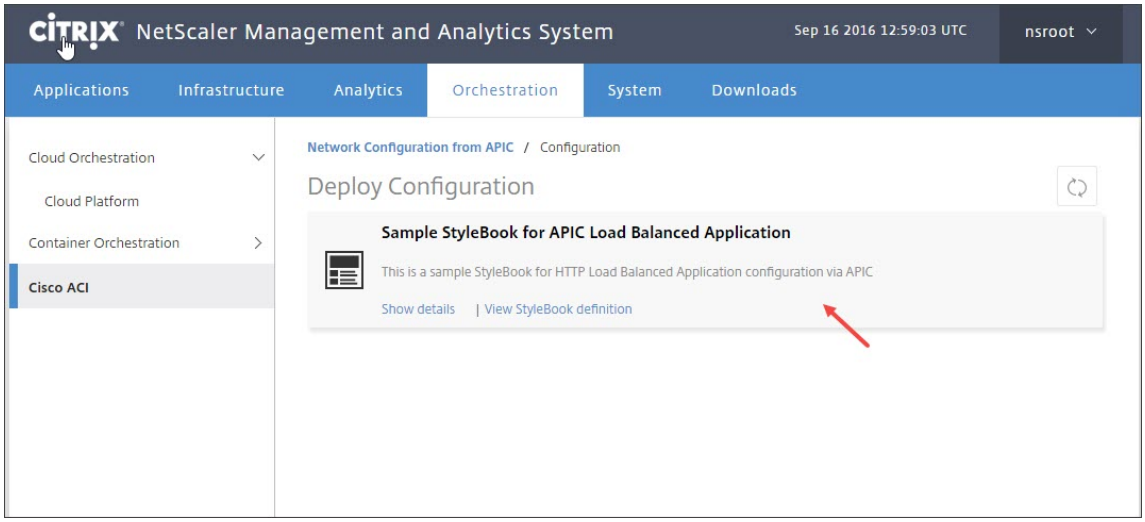

Para implementar la configuración L4-L7 mediante StyleBook en Citrix ADM:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Haga clic en el nombre del StyleBook que aparece como URL en la vista tabular.




2. En la ventana de configuración, haga doble clic en **StyleBook**.

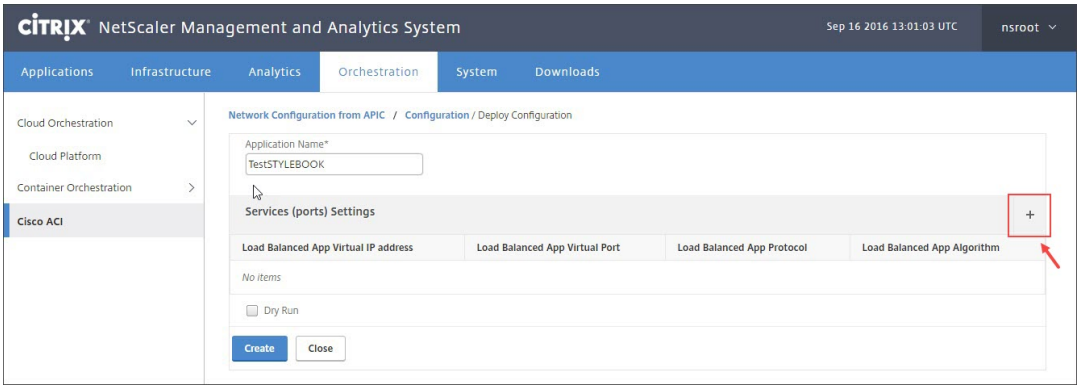



3. En la ventana Configuración de implementación, haga lo siguiente:

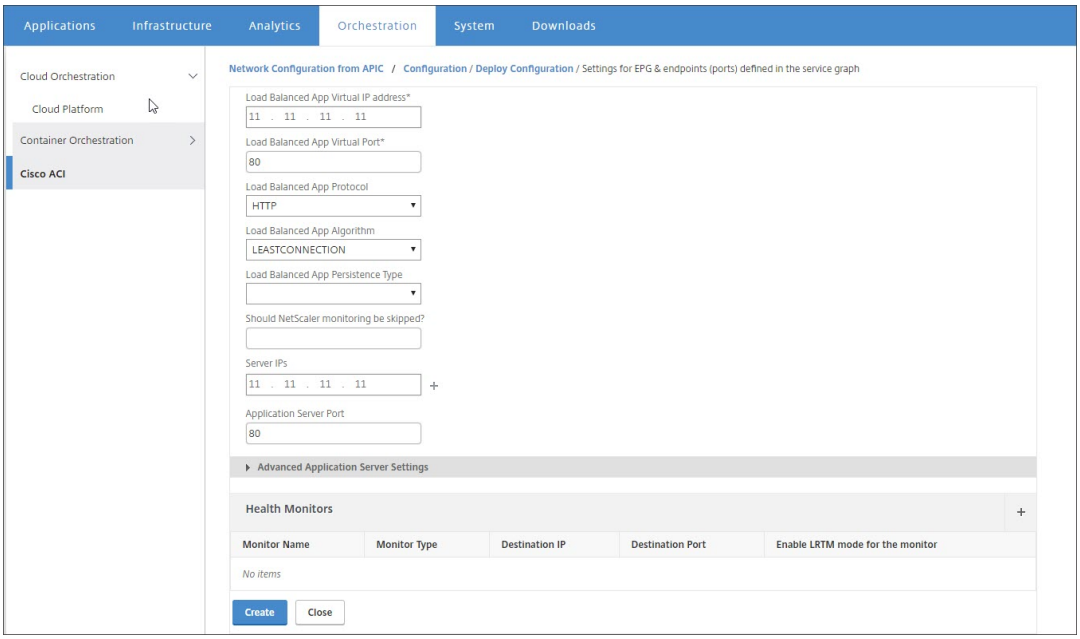
   a) En el campo **Nombre de la aplicación**, introduzca el nombre de la configuración de funciones del ADC que corresponda al gráfico de servicios de la aplicación en el APIC.

   b) En la sección Configuración del servicio (puertos), haga clic en **+**.

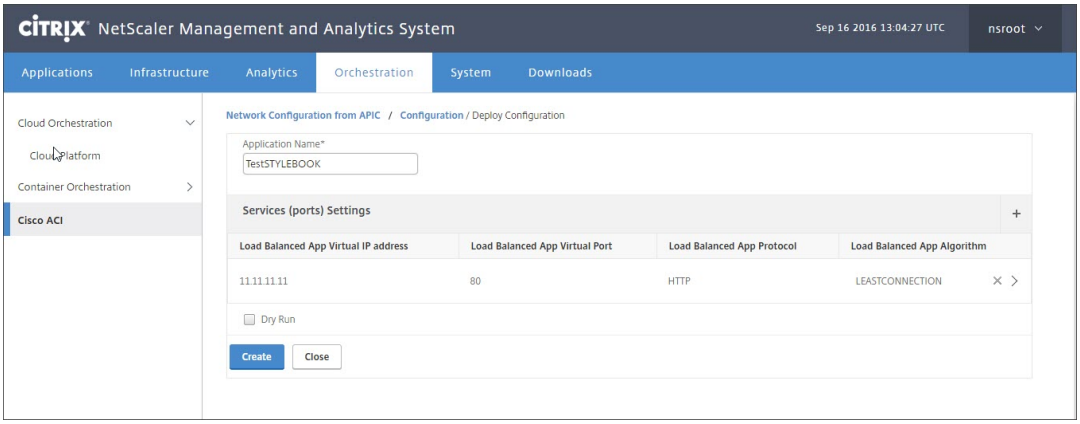
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




c) **En la**configuración de EPG y puntos finales (puertos) definida en la ventana del gráfico de servicios**, introduzca los valores del parámetro rellenado en el StyleBook y haga clic en Crear.**

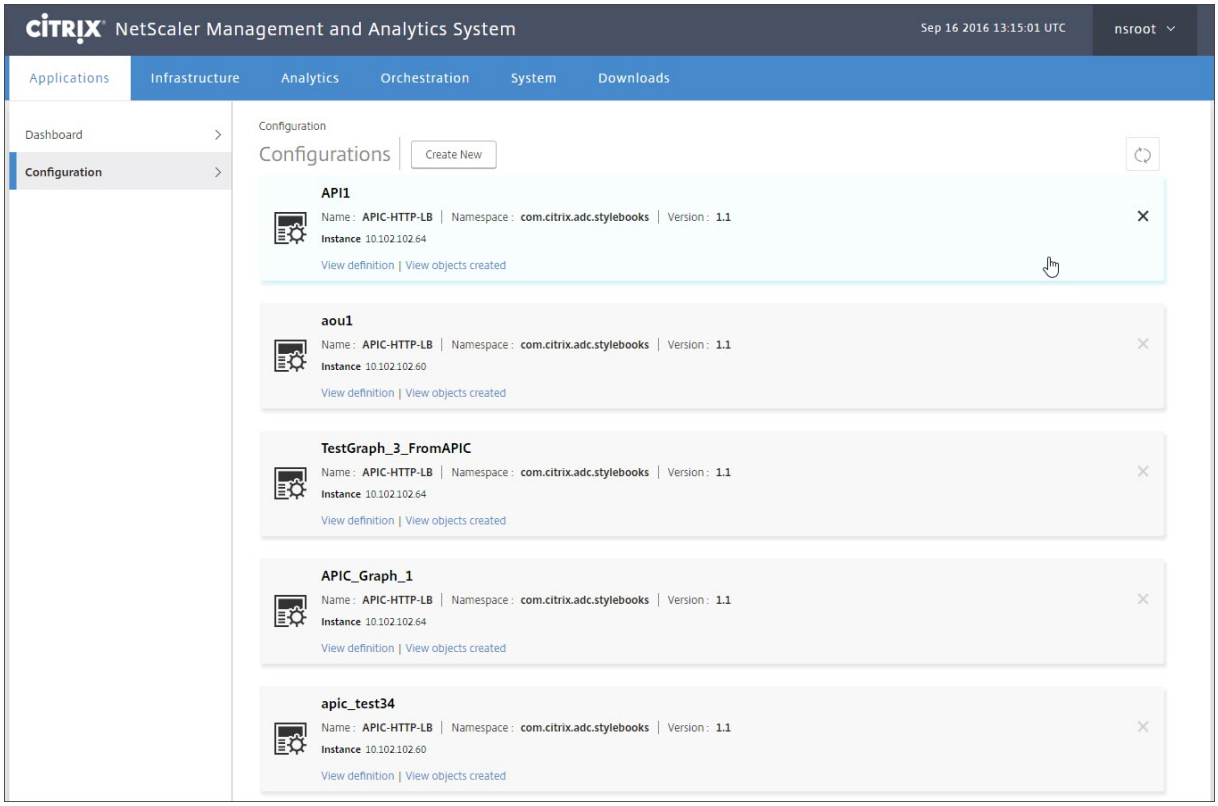



d) Haga clic en **Crear**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La configuración L4-L7 especificada en el StyleBook está implementada en Citrix ADM. **Puede ver la configuración de StyleBoook desde la ficha**Aplicación**, accediendo a Aplicación > Configuración.**




## Adjuntar y desenlazar eventos de punto final de APIC

January 30, 2024

La solución de modo híbrido gestiona implícitamente los eventos de conexión o desconexión de terminales de la APIC de Cisco. Cuando la APIC de Cisco desencadena un evento de conexión de punto final, el StyleBook de Citrix Application Delivery Management (ADM) activa automáticamente el servicegroup_servicegroupmember_binding y el punto final se desvincula durante el evento de desconexión del punto final.

Además, si no ha implementado la configuración L4-L7 en Citrix ADM antes de que se active el evento de conexión o desconexión del punto final en la APIC de Cisco, la solución conservará las direcciones IP adjuntas en la base de datos. Estas direcciones IP se enlazan al grupo de servicios correspondiente una vez creado el grupo de servicios mediante StyleBook.

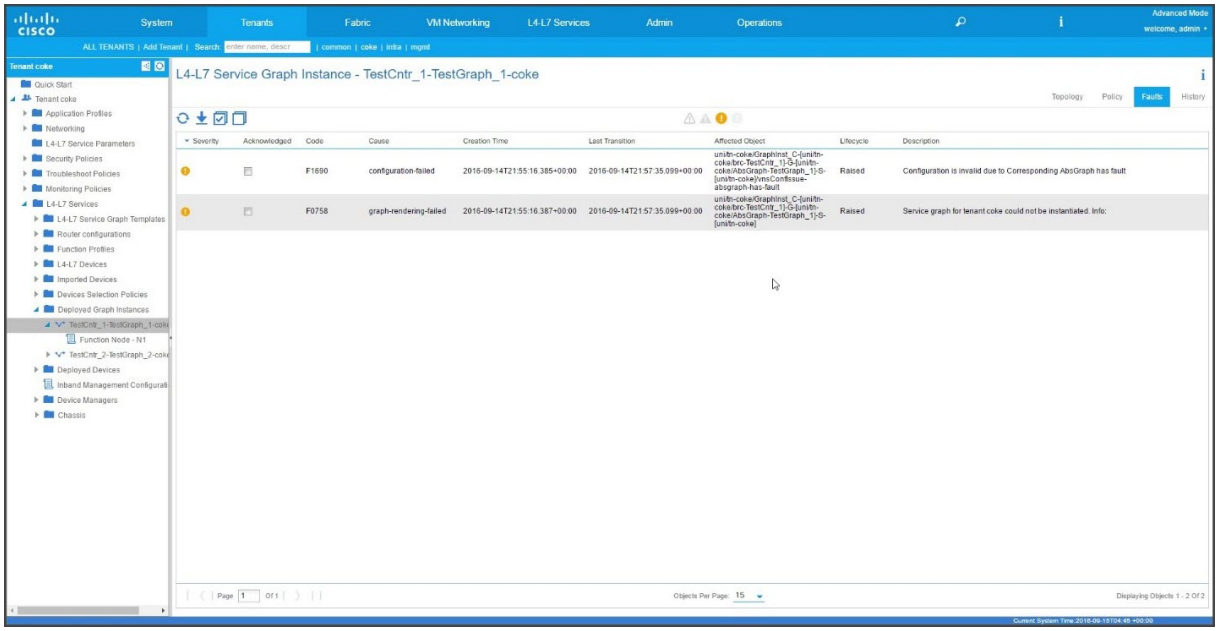
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Informes de fallos de APIC

January 30, 2024

Cuando implementa un paquete de dispositivos Citrix ADC en Cisco ACI, Cisco APIC informa de cualquier error. Puede ver los informes de errores en cualquier nivel de la APIC (por ejemplo, el gráfico de dispositivo, arrendatario, EPG o servicio). La captura de pantalla siguiente muestra un informe de errores a nivel de dispositivo. Para obtener más información sobre los errores, consulte http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html.

**Seleccione cualquier entidad de APIC y haga clic en la ficha Errores para mostrar los errores notificados por la APIC para esa entidad.**




## Registros generados por NetScaler ADM

January 30, 2024

Citrix Application Delivery Management (ADM) proporciona un registro exhaustivo que puede ayudar a solucionar problemas. Los registros generados (**admin.log**) se encuentran en: **/var/controlcenter/log/**

Puede iniciar sesión en Citrix ADM y utilizar el shell para navegar hasta la estructura de directorios de Citrix ADM. A continuación se muestra un fragmento de ejemplo de un registro NetScaler ADM para la implementación de gráficos de APIC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
'ADCHybridMode_1_Device_1': '1_1' }
, 'ackedstate': 0 }
, (7, '', '2129920_32778'): {
'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
, (1, '', 5790): {
'transaction': 0, 'ackedstate': 0, 'value': {
(3, 'ADCFunction', 'N1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'mFCngNetwork', 'mFCngnetwork'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
 }
 }
, (4, 'internal_network', 'internal_network'): {
'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
'state': 1, 'transaction': 0, 'target': 'network/internal_snip', 'ackedstate': 0 }
 }
 }
, (2, 'external', 'consumer'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
, (4, 'mFCngStylebook', 'mFCngStylebook'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0 }
 }
 }
, (2, 'internal', 'provider'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': 'ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
 }
 }
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
46   }
47  , 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-
       coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
       coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
48  , (4, 'Network', 'network'): {
49  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
50  (4, 'nsip', 'internal_snip'): {
51  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
52  (5, 'type', 'type'): {
53  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
54  , (5, 'hostroute', 'hostroute'): {
55  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
56  , (5, 'ipaddress', 'ipaddress'): {
57  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
58  , (5, 'dynamicrouting', 'dynamicRouting'): {
59  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
60  , (5, 'netmask', 'netmask'): {
61  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0
       ' }
62   }
63   }
64   }
65   }
66  , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
67  'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', '
       ackedstate': 0, 'encap': '2129920_32778' }
68  , (4, 'Stylebook', 'stylebook_1'): {
69  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
70  (5, 'name', 'stylebookName'): {
71  'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
        }
72   }
73   }
74   }
75  , 'txid': 10000 }
76   }
77
78     2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
79  'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
       uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
80  'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
       coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
       HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
81  , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
       graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
       graphInstanceId': 5790 }
82
83     2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
84     2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
85     2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
86     2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<
          eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
87     2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
            Details  = 10.102.102.62 +++++++++++++++++
      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
      2016-06-29 10:58:33,867 DEBUG Host name from device = ADCHybridMode_1
      "InProgress","message":null,"replication_status":"","target":"10.102.102.81","operation":"POST","entity_type":"apic","entity_id":null }
    }

      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
    "errorcode": 0, "message": "Done", "severity": "NONE"  }

      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from Config ++++++
      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
  'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230 }
    ++++++
      2016-06-29 10:58:44,142 DEBUG Service health details = {
    }
    collection length = 0
      2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down = 0
      2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
      2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
  ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
  'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0) }
    }

      2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List = []
      2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
  'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health' : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }

      2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
    "errorcode": 0, "message": "Done", "severity": "NONE"  }
  , sessionId = ## D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764

      2016-06-29 10:58:44,237 DEBUG ++++++ Faults respCol   = {
  '10.102.102.62': {
  '10.102.102.62': {
  u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity': u'NONE', 'operation_name': 'add_op' }
    }
  , (7, '', '2129920_32778'): {
  'vlan': {
  u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity': u'NONE', 'operation_name': 'add_op' }
    }
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
127   , (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
        internal', 'provider')), 'nsip'): {
128   'vlan_nsip_binding': {
129   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'bind_op' }
130    }
131   , (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
        internal_snip')): {
132   'nsip': {
133   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'add_op' }
134    }
135   , (): {
136    }
137   , (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
138   'vlan_interface_binding': {
139   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
         u'NONE', 'operation_name': 'bind_op' }
140    }
141    }
142
143      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
            = Done, statusCode = add_op
144      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
            = Done, statusCode = add_op
145      2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
           erMsg = Done, statusCode = bind_op
146      2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
            = Done, statusCode = add_op
147      2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
           erMsg = Done, statusCode = bind_op
148      2016-06-29 10:58:44,238 DEBUG +++++++++++++ ServiceAudit response
           = {
149   'faults': [], 'state': 0, 'health': [] }
150
151      2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
152   'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
        uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
153   'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
        coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
        HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
154   , 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
        graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
        graphInstanceId': 5790 }
155
156      2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task:
           create apic_graph
157      2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
158      2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
159      2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector
           collection from Config with type 22 for attach & detach event
           ++++++
160      2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
0: [], 1: [], 3: [] }

   2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList = []
   2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = [] dettachIpList = []
   2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName': None, 'configPackId': None, 'tenantName': u'coke_SDX2', 'styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort': None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP': None }
```

## Registros generados por el paquete de dispositivos de modo híbrido

January 30, 2024

El paquete de dispositivos Citrix ADC Hybrid Mode genera registros relacionados con la configuración y con la supervisión. Los registros generados se encuentran en **/data/devicescript/Citrix.NetScalerMAS.1.0/logs**.

A continuación se muestra un fragmento de ejemplo de un **debug.log** de Cisco APIC:

```
   2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62, 24063] Device manager details ip = 10.102.102.81, port = 80
   2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62, 24063] +++++++++++++ serviceAudit  request ++++++++++++++++
   2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62, 24063] ++++++++++ getStyleBookObjects +++++++++++++
   2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62, 24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 = {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB' }
 }
 }

   2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62, 24063] NMAS collection styleBookName= APIC-HTTP-LB
   2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62, 24063] NMAS collection retCol= {
'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook', 'stylebook_1')) }

```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
15      2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
           24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
           /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
           HTTP-LB
16      2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
           24063]  ++++ Response from styleBookresCode serviceAudit = {
17   u'stylebook': {
18   u'uses_builtin_namespaces': {
19   u'netscaler.nitro.config': u'10.5' }
20   , u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
        'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
        nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
        : "Sample StyleBook for APIC Load Balanced Application"\
        ndescription: "This is a sample StyleBook for HTTP Load Balanced
        Application configuration via APIC"\nschema-version: "1.0"\nimport-
        stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
        prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
        adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
        -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
        appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
        appname, port): $appname + "-" + str($port) + "-sg"\n
        healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
         - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
        $parameters.app-services\n    repeat-item: app\n    properties: \
        n      name: $substitutions.lb-name($parameters.appname, $app.
        virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
        virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
        $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
         name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
        app-services\n    repeat-item: app\n    properties: \n      name:
        $substitutions.sg-name($parameters.appname, $app.virtual-port)\
        n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
        advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
        cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
        cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
        skip_healthmonitor)\n    components: \n      -\n        name:
        lbvserver-svg-binding\n        type: ns::
        lbvserver_servicegroup_binding\n        properties: \n
        name: $substitutions.lb-name($parameters.appname, $app.virtual-port
        )\n          servicegroupname: $parent.properties.name\n      - \
        n        name: svg-members\n        type: ns::
        servicegroup_servicegroupmember_binding\n        condition: $app.
        server-ips\n        repeat: $app.server-ips\n        repeat-item:
        serverip\n        properties: \n          ip: $serverip\n
        port: $app.server-port\n          servicegroupname: $parent.
        properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
        $components.lbvserver\n  - \n    name: servicegroups\n    value:
        $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21   u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
        ': u'APIC-ROOT' }
22   ] }
23    }
24
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
25      2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
           24063]  ++++ Dev Mgr request details devMgrUrl = http://
           10.102.102.81/admin/v1/apic
26      2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
           24063]  ++++ Response from Device Mgr serviceAudit = {
27   "APIC":[] }
28
29      2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
           24063] +++++++++++++++ serviceAudit response = {
30   "APIC":[] }
31
32      2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
           24063] +++++++++++++++ serviceAudit response headers content type
           = application/json; charset=utf-8
33      2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
           24063] +++++++++++++++ serviceAudit response headers = {
34   'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
        c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
         'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
        10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
        application/json; charset=utf-8' }
35
36      2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
           24063] +++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
           /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37      2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 0
38      2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
39   u'journalcontext': {
40   u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
         u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': None, u'
        target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
        -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41    }
42
43      2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 1
44      2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
45   u'journalcontext': {
46   u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
         u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': None, u'
        target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
        -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47    }
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
           24063] +++++++++++++++ pollingStatus = True, pollingTime = 2
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
           24063] +++++++++++++++ pollingResponse json = {
51   u'journalcontext': {
52   u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
        Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
53    }
54
55      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
           24063] Attempts 1
56      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
           24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
            '', 5230)), transaction: 0
57      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
           24063] Attempts for {
58   'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
        'devs': {
59   'ADCHybridMode_1_Device_1': {
60   'state': 0, 'virtual': False, 'manager': {
61   'hosts': {
62   '10.102.102.81': {
63   'port': 80 }
64    }
65   , 'name': 'NMAS_1', 'creds': {
66   'username': 'nsroot', 'password': '<hidden>' }
67    }
68   , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69   'username': 'nsroot', 'password': '<hidden>' }
70    }
71    }
72   , 'manager': {
73   'hosts': {
74   '10.102.102.81': {
75   'port': 80 }
76    }
77   , 'name': 'NMAS_1', 'creds': {
78   'username': 'nsroot', 'password': '<hidden>' }
79    }
80   , 'contextaware': True, 'port': 80, 'creds': {
81   'username': 'nsroot', 'password': '<hidden>' }
82    }
83    is 0
84      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
           24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
           (0, '', 5230))
85      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
           24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
           24063] Faults: []
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
           24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
           24063] Send num: 761, type: 220, len: 382
```

## Paquete de dispositivos NetScaler ADC en el modo de orquestación de nube de ACI de Cisco

January 30, 2024

Con Application Policy Infrastructure Controller (APIC) versión 3.1, Citrix NetScaler ADC y Cisco ACI amplían la cartera de integración conjunta para proporcionar una nueva solución que aborde las necesidades del cliente. El nuevo modo de integración, ACI Cloud Orchestrator Mode*, simplifica las integraciones L4-L7 al abstraer la complejidad de la configuración a través de parámetros estandarizados. La solución funciona a la perfección para automatizar los servicios L4-L7, logrando los objetivos de implementaciones ágiles de aplicaciones, flexibilidad operativa y simplicidad.

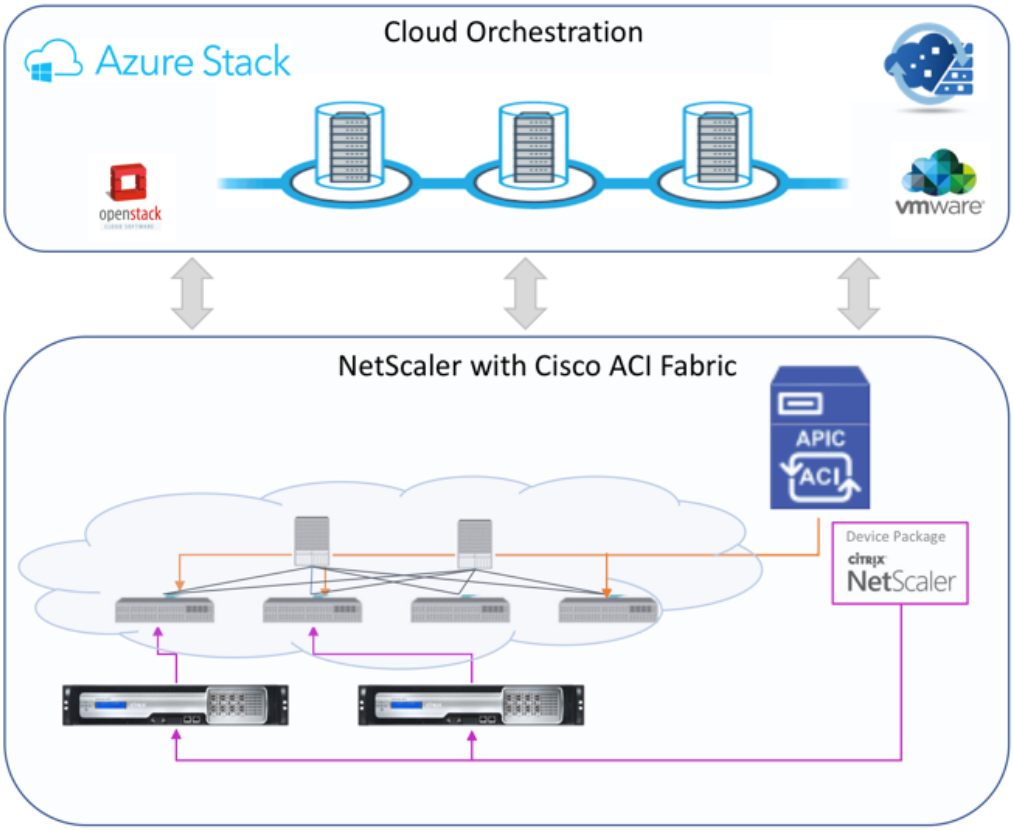
El modo Cloud Orchestrator de Cisco ACI mediante la solución NetScaler ADC proporciona los siguientes beneficios:

- La automatización de los servicios L4-L7 reduce el error humano.
- La integración prediseñada de la solución Cisco ACI lo ayuda a reducir el tiempo de implementación y aumenta el rendimiento de las aplicaciones, como las aplicaciones web, las máquinas virtuales y SQL.
- Visibilidad totalmente integrada del estado de las aplicaciones, como aplicaciones web, máquinas virtuales y SQL en componentes de red físicos y virtuales.

El modo de orquestador en la nube de ACI ahora le ofrece más opciones para utilizar la nueva GUI de APIC simplificada directamente o seleccionando cualquier orquestador de nube, como Cisco Cloud Center, Windows Azure Pack, OpenStack, vRealize o cualquier otro según sus preferencias. Este nuevo cambio se logra al exponer un conjunto de atributos ADC como esquema ADC. Estos atributos se asignan en los perfiles de función de los paquetes de dispositivos. Puede proporcionar valores para estos atributos mientras el orquestador de la nube aprovisiona el servicio ADC (Cisco Cloud Center o Wireless Application Protocol (WAP)).

La siguiente ilustración proporciona una descripción general de NetScaler ADC en una solución de orquestación en la nube:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



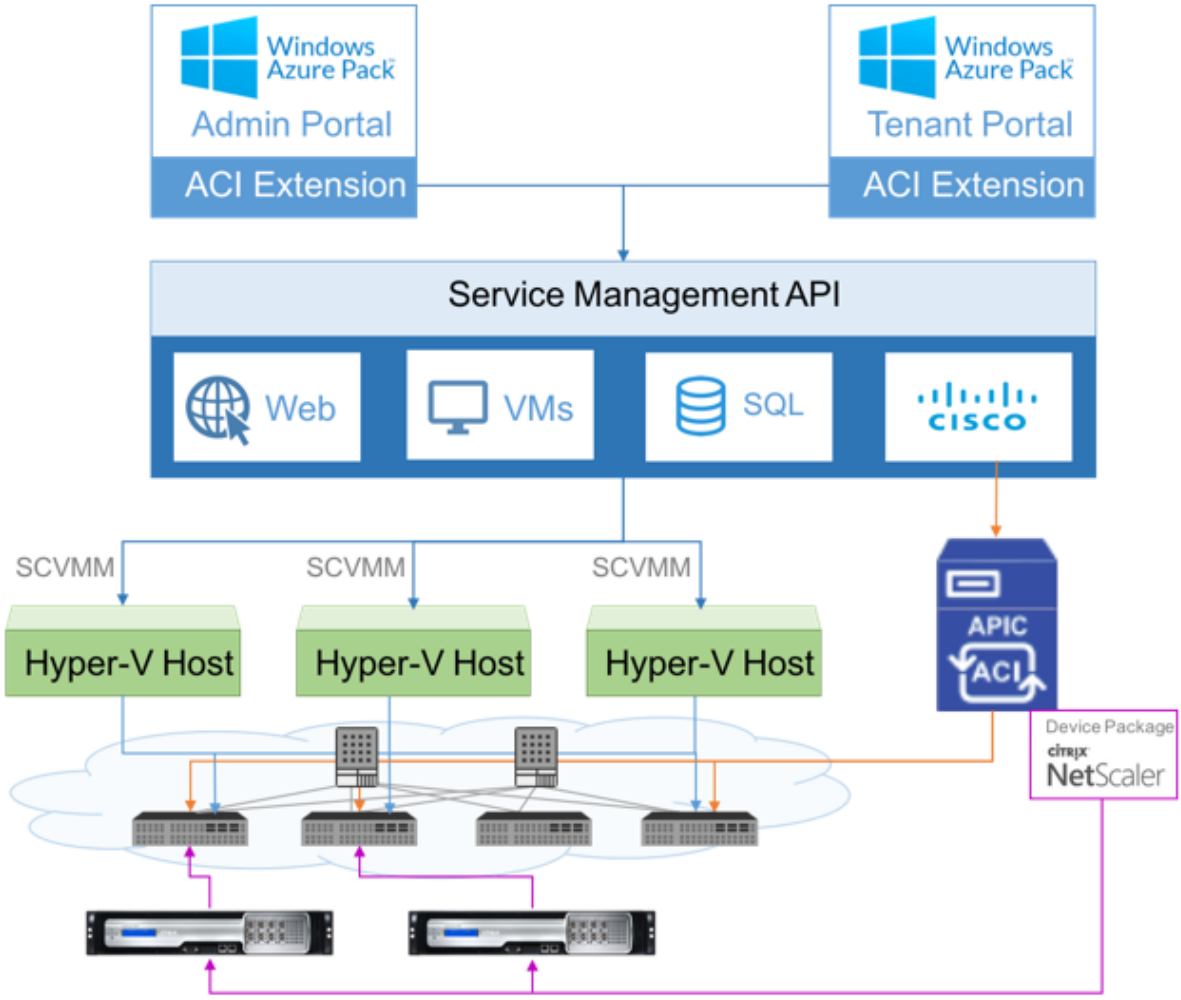

La solución de modo de orquestación en la nube que utiliza Microsoft Azure Pack implica muchos puntos de integración, como Azure Pack a Cisco APIC, Cisco APIC a System Central máquina virtual Manager (SCVMM) y Cisco APIC a NetScaler ADC. Como arrendatario en la nube privada, puede habilitar NAT, aprovisionar servicios de red y agregar un equilibrador de carga.

Azure Pack admite portales de arrendatarios y administradores, y cada uno de ellos tiene su propio conjunto de operaciones que se pueden realizar.

- Como administrador, puede realizar tareas administrativas como el registro de ACI, el rango VIP, la asociación de dispositivos NetScaler ADC con la nube de máquinas virtuales y la creación de cuentas de usuario arrendatario.
- Como arrendatario, puede realizar tareas como iniciar sesión en el portal de arrendatarios de Azure Pack y configurar la red, los dominios de puente y el enrutamiento y reenvío virtuales (VRF), y puede usar las funciones de equilibrio de carga y RNAT de NetScaler ADC.

La siguiente ilustración proporciona información general sobre Azure Pack en una solución de modo de nube:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Importante**

- El administrador de la nube puede facilitar con el esquema L4-L7 compatible con APIC y el administrador de APIC puede realizar cualquier cambio adicional directamente en el APIC. Esto le permite configurar e implementar NetScaler ADC a la par del conjunto de funciones admitidas.
- Los arrendatarios pueden implementar varias direcciones VIP con diferentes puertos para la misma red. Debe asegurarse de que la combinación de IP y puerto sea única.
- El paquete de dispositivos NetScaler ADC solo admite la implementación de un solo contexto. Cada arrendatario recibe una instancia de NetScaler ADC dedicada.
- El Protocolo de aplicaciones inalámbricas (WAP) admite dispositivos NetScaler ADC MPX y dispositivos NetScaler ADC VPX (incluye instancias NetScaler ADC VPX implementadas en la plataforma NetScaler ADC SDX).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El paquete de dispositivos en modo de orquestador de nube admite tanto el modo completamente administrado como el modo de administrador de servicios. El paquete de modo completamente administrado admite una amplia variedad de perfiles de función, como el equilibrio de carga simple, el cambio de contenido, la descarga SSL y otros perfiles. Estos perfiles de función cubren un conjunto de funciones y un modo de implementación completos de NetScaler ADC. Del mismo modo, el paquete de dispositivos en modo administrador de servicios admite la configuración e implementación de un brazo y dos brazos de NetScaler ADC mediante APIC. NetScaler Application Delivery Management (ADM) actúa como administrador de servicios para APIC y puede usar NetScaler ADM para configurar los parámetros de NetScaler ADC L4-L7.

> **Nota**
>
> En el modo administrador de servicios (modo híbrido), no puede reutilizar ni reasignar la misma dirección IP del servidor, que ya está presente en el dispositivo NetScaler ADC.

El perfil de función del modo de orquestador de nube tiene un conjunto de parámetros asignados al esquema ADC de APIC y el orquestador usa estos parámetros. El orquestador en la nube proporciona los valores para los parámetros ADC (VIP, mientras se aprovisiona NetScaler ADC a través de APIC). El orquestador se comunica con las API de APIC y pasa los detalles específicos del ADC como parte de la carga útil para un perfil de función específico. Internamente, APIC extrae los valores y los pasa al paquete de dispositivos que configura internamente el NetScaler ADC.

Para obtener más información sobre la lista completa de esquemas ADC, que son compatibles con Cisco APIC, consulte Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, versión 3.x y anteriores).

El paquete de dispositivos de modo completamente administrado admite los siguientes perfiles de función:

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM
23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

El paquete de dispositivos en modo de gestión de servicios admite los siguientes perfiles de función en modo nube:

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

NetScaler ADC admite los perfiles de función mencionados anteriormente. El APIC admite un subconjunto de estos parámetros en el esquema ADC. Si hay algún atributo no admitido por Cisco ACI presente en el perfil de función, debe clonar el perfil de función del modo de orquestador de la nube y proporcionar los valores para todos los atributos no admitidos por APIC y debe guardar los atributos. Más adelante, el orquestador puede usar el perfil de función recién clonado.

El paquete de dispositivos de Citrix Cloud Mode admite NetScaler ADC 12.0 y el modo administrador de servicios también usa NetScaler ADM 12.0. El paquete de dispositivos ha cambiado la versión del modelo de 1.0 a 2.0 y se puede usar como una nueva instalación. El paquete de dispositivos Cloud

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Orchestrator Mode no se puede actualizar desde versiones anteriores de paquetes de dispositivos ya que se ha cambiado la versión del modelo.

Los paquetes de dispositivos de Cloud Orchestrator Mode también se pueden usar en implementaciones normales. El paquete no obliga al usuario a aprovisionar NetScaler ADC a través de ningún orquestador en la nube. El paquete de dispositivos es compatible solo con APIC y APIC con Cloud Orchestrator.

## Administrar la configuración de Kubernetes Ingress en NetScaler ADM

January 30, 2024

Kubernetes (K8s) es una plataforma de orquestación de contenedores de código abierto que automatiza la implementación, el escalado y la administración de aplicaciones nativas de la nube.

Kubernetes proporciona la función Ingress, que permite que el tráfico de clientes fuera del clúster acceda a los microservicios de una aplicación que se ejecuta dentro del clúster de Kubernetes. Las instancias de ADC pueden actuar como entrada a las aplicaciones que se ejecutan dentro de un clúster de Kubernetes. Las instancias de ADC pueden equilibrar la carga y enrutar el tráfico de norte a sur desde los clientes a cualquier microservicio dentro del clúster de Kubernetes.

> **Nota**
>
> - Citrix ADM admite la función Ingress en los clústeres con la versión 1.14 y superior de Kubernetes.
> - NetScaler ADM admite dispositivos NetScaler ADC VPX y MPX como dispositivos de ingreso.
> - En el entorno de Kubernetes, la carga de instancia de NetScaler ADC equilibra solo el tipo de servicio “NodePort”.

Puede configurar varias instancias ADC para que actúen como dispositivos de ingreso en el mismo clúster o en distintos clústeres o espacios de nombres. Después de configurar las instancias, puede asignar cada instancia a diferentes aplicaciones en función de la directiva de Ingress.

Puede crear e implementar una configuración de Ingress con API o `kubectl` de Kubernetes. También puede configurar e implementar un Ingress desde NetScaler ADM.

Puede especificar los siguientes aspectos de la integración de Kubernetes en ADM:

- **Clúster**: Puede registrar o anular el registro de clústeres de Kubernetes para los que ADM puede implementar configuraciones de Ingress. Cuando registre un clúster en NetScaler ADM, especifique la información del servidor de la API de Kubernetes. A continuación, seleccione un agente de ADM que pueda llegar al clúster de Kubernetes e implementar configuraciones de Ingress.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Directivas: las** directivas de entrada se utilizan para seleccionar la instancia de ADC en función del clúster o el espacio de nombres para implementar una configuración de entrada. Especifique la información del clúster, el sitio y la instancia cuando agregue una directiva.
- **Configuración de ingreso**: Esta configuración es la configuración de ingreso de Kubernetes, que incluye las reglas de conmutación de contenido y las rutas URL correspondientes de los microservicios y sus puertos. También puede especificar los certificados SSL/TLS (para descargar el procesamiento SSL en la instancia de ADC) con los recursos secretos de Kubernetes.

NetScaler ADM asigna automáticamente las configuraciones de ingreso a instancias de ADC mediante directivas de ingreso.

Para cada configuración de Ingress correcta, NetScaler ADM genera un StyleBook ConfigPack. El ConfigPack representa la configuración ADC aplicada a la instancia de ADC que corresponde a la configuración de Ingress. Para ver el ConfigPack, vaya a **Aplicaciones > StyleBooks > Configuraciones**.

### Antes de comenzar

Para usar instancias de NetScaler ADC como dispositivos de entrada en clústeres de Kubernetes, asegúrese de tener:

- Kubernetes agrupamiento en su lugar.
- Cluster Kubernetes registrado en NetScaler ADM.

### Configurar NetScaler ADM con un token secreto para administrar un clúster de Kubernetes

Para que NetScaler ADM pueda recibir eventos de Kubernetes, debe crear una cuenta de servicio en Kubernetes para NetScaler ADM. Además, configure la cuenta de servicio con los permisos RBAC necesarios en el clúster.

1. Cree una cuenta de servicio para NetScaler ADM. Por ejemplo, el nombre de la cuenta de servicio puede ser`citrixadm-sa`. Para crear una cuenta de servicio, consulte Usar varias cuentas de servicio.
2. Utilice el`cluster-admin` rol para enlazar la cuenta de servicio NetScaler ADM. Este enlace concede un valor `ClusterRole` en todo el clúster a una cuenta de servicio. A continuación, se muestra un comando de ejemplo para vincular un rol `cluster-admin` a la cuenta de servicio.

```
kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
    =cluster-admin --serviceaccount=default:citrixadm-sa
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Después de vincular la cuenta de servicio NetScaler ADM al rol `cluster-admin`, la cuenta de servicio tiene acceso en todo el clúster. Para obtener más información, consulte `kubectl Createclusterrolebinding`.

3. Obtenga el token de la cuenta de servicio creada.

   Por ejemplo, ejecute el siguiente comando para ver el token de la cuenta de servicio `citrixadm-sa`:

```
kubectl describe sa citrixadm-sa
```

4. Ejecute el siguiente comando para obtener la cadena secreta del token:

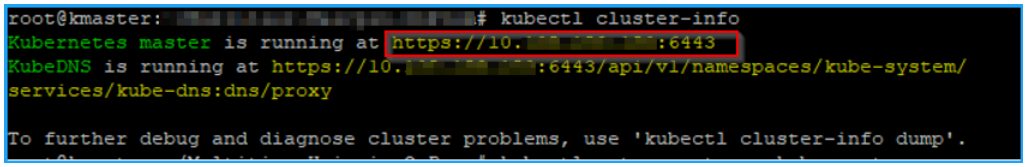
```
kubectl describe secret <token-name>
```

### Agregar el clúster de Kubernetes en NetScaler ADM

Después de configurar un agente NetScaler ADM y configurar rutas estáticas, debe registrar el clúster de Kubernetes en NetScaler ADM.

Para registrar el clúster de Kubernetes:

1. Inicie sesión en Citrix ADM con credenciales de administrador.
2. Vaya a **Orchestration** > **Kubernetes** > **Clúster**.
   Se muestra la página Clústeres.
3. Haga clic en **Agregar**.
4. En la página **Agregar clúster**, especifique los siguientes parámetros:
   a) **Nombre**: especifique un nombre de su elección.
   b) **URL del servidor API** - Puede obtener los detalles de la URL del servidor API desde el nodo principal de Kubernetes.
      i. En el nodo principal de Kubernetes, ejecute el comando `kubectl cluster-info`
      .




      ii. Introduzca la URL que aparece para **“Kubernetes master se está ejecutando en. “**
   c) **Token de autenticación**: especifique la cadena de token de autenticación que se obtiene al configurar NetScaler ADM para administrar un clúster de Kubernetes. El token de au-

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

tenticación es necesario para validar el acceso para la comunicación entre el clúster de Kubernetes y NetScaler ADM. Para generar un token de autenticación:

i. En el nodo principal de Kubernetes, ejecute los siguientes comandos:

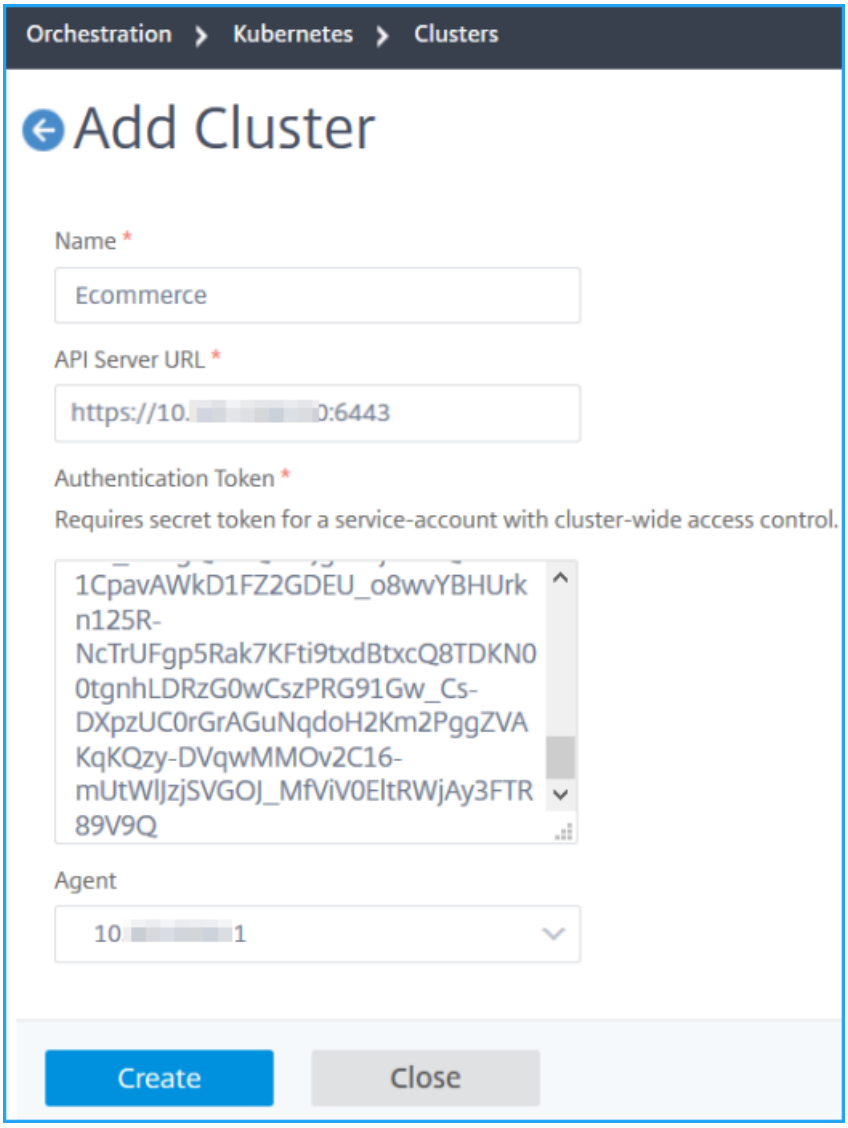
```
kubectl describe secret <token-name>
```

ii. Copie el token que se genera y péguelo como token de autenticación

Para obtener más información, consulte la documentación de Kubernetes.

d) Seleccione el agente de la lista.

e) Haga clic en **Crear**.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Definir una directiva de ingreso

La directiva Ingress decide qué NetScaler ADC se utiliza para implementar una configuración de Ingress, basada en el clúster de entrada o el espacio de nombres.

1. Vaya a **Orchestration > Kubernetes > Policy**.
2. Haga clic en **Add** para crear una directiva.
   a) Especifique el nombre de la directiva.
   b) Defina **las condiciones** para implementar la configuración de Ingress en un clúster de Kubernetes. Estas condiciones suelen basarse en el clúster de entrada y el espacio de nombres.
   c) En el panel Infraestructura,
      - **Sitio**: Seleccione un sitio de la lista.
      - **Instancia**: Seleccione la instancia de ADC de la lista.

      Las listas de **sitios** e **instancias** rellenan las opciones en función de la selección de clústeres en el panel **Condiciones**.

      Estas listas muestran los sitios o las instancias que están asociados con el agente NetScaler ADM configurado con el clúster de Kubernetes.
   d) En **Elegir red**, seleccione la red desde la que ADM asigna automáticamente las direcciones IP virtuales a una configuración de entrada.

      Esta lista muestra las redes creadas en **Redes > IPAM** .
   e) Haga clic en **Crear**.

### Implementar la configuración de Ingress

Puede implementar la configuración de Ingress desde Kubernetes mediante `kubectl`, la API de Kubernetes u otras herramientas. También puede implementar la configuración de Ingress directamente desde NetScaler ADM.

1. Vaya a **Orchestration > Kubernetes > Entradas**.
2. Haga clic en **Agregar**.
3. En el campo **Crear entrada**, especifique los siguientes detalles:
   a) Especifique el nombre del Ingress.
   b) En **Clúster**, selecciona el clúster de Kubernetes en el que quieres implementar un Ingress.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

c) Seleccione el Espacio de **nombres de clúster** en la lista. En este campo se enumeran los espacios de nombres que están presentes en el clúster de Kubernetes especificado.

d) Si lo desea, seleccione **Asignar dirección IP frontend automáticamente**.

e) Seleccione **Protocolo de entrada** en la lista. Si selecciona **HTTPS**, especifique el **secreto de TLS**.

   Este secreto incrusta el recurso secreto de Kubernetes que incorpora el certificado HTTPS y la clave privada.

   Una entrada HTTPS requiere un secreto basado en TLS configurado en el clúster de Kubernetes. Especifique los campos `tls.crt` y `tls.key` para incluir el certificado del servidor y la clave del certificado, respectivamente.

f) Para el enrutamiento de contenido, especifique los siguientes detalles:

   - **Rutas de URL**: Especifique la ruta que se asocia con el servicio y el puerto de Kubernetes.
   - **Servicio de Kubernetes**: Especifique el servicio deseado.
   - **Puerto**: Especifique el puerto de servicio.
   - **Método LB**: Seleccione el método de equilibrio de carga preferido para el servicio de Kubernetes seleccionado.

     El método seleccionado actualiza la especificación de entrada con una anotación apropiada. Por ejemplo, si selecciona el método **ROUNDROBIN**, la anotación de Citrix aparece como sigue:

     ```
     "lbmethod":"ROUNDROBIN"
     ```

   - **Tipo de persistencia**: Seleccione el tipo de persistencia de equilibrio de carga preferido para el servicio de Kubernetes seleccionado.

     El tipo de persistencia seleccionado actualiza la especificación de entrada con una anotación apropiada. Por ejemplo, si selecciona **COOKIEINSERT**, la anotación de Citrix aparece de la siguiente manera:

     ```
     "persistenceType":"COOKIEINSERT"
     ```

   Haga clic en **Agregar** para agregar más rutas de URL y puertos a la configuración de Ingress.

   Después de la implementación, la configuración de Ingress redirige el tráfico del cliente a un servicio específico en función de lo siguiente:

   - La ruta URL y el puerto solicitados.
   - El método LB y el tipo de persistencia definidos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Se espera que los servicios de Kubernetes utilizados en una configuración de ingreso sean de tipo NodePort.

g) Si lo desea, especifique una **descripción de entrada**.

h) haga clic en **Implementar**

Si quiere revisar la configuración antes de implementar, haga clic en **Generar especificación de ingreso**. La configuración de Ingress especificada aparece en formato YAML. Después de revisar la configuración, haga clic en **Implementar**.

> **Nota**
> Aplique licencias a los servidores virtuales que se crean mediante configuraciones de Ingress. Para aplicar la licencia, lleve a cabo los siguientes pasos:
>
> 1. Vaya a **Sistema > Licencias y análisis** .
> 2. En **Resumen de licencia del servidor virtual**, habilite la **selección automática de servidores virtuales**.

## Capacidad agrupada de NetScaler ADC

January 30, 2024

La capacidad agrupada de NetScaler ADC le permite compartir licencias de instancia o ancho de banda entre diferentes factores de forma ADC. Para las instancias basadas en suscripciones de CPU virtuales, puede compartir la licencia de CPU virtual en todas las instancias. Use esta capacidad agrupada para las instancias que se encuentran en el centro de datos o en las nubes públicas. Cuando una instancia ya no requiere los recursos, comprueba la capacidad asignada de nuevo en el grupo común. Reutilice la capacidad liberada en otras instancias de ADC que necesiten recursos.

Puede usar las licencias agrupadas para maximizar la utilización del ancho de banda al garantizar la asignación de ancho de banda necesaria a una instancia y no más de lo que necesita. Aumente o reduzca el ancho de banda asignado a una instancia en tiempo de ejecución sin afectar el tráfico. Con las licencias de capacidad agrupadas, puede automatizar el Provisioning de instancias.

### Cómo funcionan las licencias de capacidad agrupada de NetScaler ADC

La capacidad agrupada de NetScaler ADC tiene los siguientes componentes:

- Instancias de NetScaler ADC, que se pueden clasificar en:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - Hardware de capacidad cero
  - Instancias VPX independientes o instancias CPX o instancias BLX
- Grupo de ancho de banda
- Grupo de instancias
- NetScaler ADM configurado como servidor de licencias

## Hardware de capacidad cero

Cuando se administran a través de la capacidad agrupada de NetScaler ADC, las instancias MPX y SDX se denominan "hardware de capacidad cero"porque estas instancias no pueden funcionar hasta que no retiren los recursos del ancho de banda y los grupos de instancias. Por lo tanto, estas plataformas también se conocen como dispositivos MPX-Z y SDX-Z.

El hardware de capacidad cero requiere una licencia de plataforma para poder obtener ancho de banda y una licencia de instancia del grupo común.

> **Nota**
>
> La suscripción de licencia de instancia no es necesaria para las instancias MPX. Consulte la tabla 1 de esta página, para obtener información sobre la capacidad agrupada admitida para instancias MPX y SDX. Consulte la tabla 5 para conocer los requisitos de licencia para diferentes formatos MPX y SDX.

### Administrar e instalar licencias de plataforma

Debe instalar manualmente una licencia de plataforma mediante el número de serie del hardware o el código de acceso a la licencia. Una vez que se instala una licencia de plataforma, se bloquea en el hardware y no se puede compartir en las instancias de hardware de NetScaler ADC a pedido. Sin embargo, puede mover manualmente la licencia de plataforma a otra instancia de hardware de NetScaler ADC.

Las instancias ADC MPX que ejecutan la versión 11.1 del software ADC compilación 54.14 o posterior y las instancias SDX de ADC que ejecutan 11.1 compilación 58.13 o posterior admiten la capacidad agrupada de ADC. Para obtener más información, consulte **la Tabla 1. Capacidad agrupada compatible para instancias MPX y SDX**.

## Instancias independientes de NetScaler ADC VPX

Las instancias de NetScaler ADC VPX que ejecutan el software NetScaler ADC versión 11.1 compilación 54.14 y posteriores en los siguientes hipervisores admiten la capacidad agrupada:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

Las instancias de NetScaler ADC VPX que ejecutan el software NetScaler ADC versión 12.0 compilación 51.24 y posteriores en los siguientes hipervisores y plataformas en la nube admiten la capacidad agrupada:

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

> **Nota**
>
> Para habilitar la comunicación entre NetScaler ADM y Microsoft Azure o AWS, se debe configurar un túnel IPSEC.Para obtener más información, consulte Agregar instancias NetScaler ADC VPX implementadas en la nube a NetScaler ADM.
> A diferencia del hardware de capacidad cero, VPX no requiere licencia de plataforma. Para procesar el tráfico, debe desproteger el ancho de banda y una licencia de instancia del grupo.

### Instancias CPX independientes de NetScaler ADC

Las instancias CPX de NetScaler ADC implementadas en un host Docker admiten capacidad agrupada. A diferencia del hardware de capacidad cero, CPX no requiere una licencia de plataforma. Una única instancia CPX que consume hasta 1 Gbps de rendimiento desactiva solo una instancia y sin ancho de banda del grupo de licencias. Por ejemplo, tenga en cuenta que tiene 20 instancias CPX con un grupo de ancho de banda de 20 Gbps. Si una de las instancias de CPX consume un rendimiento de 500 Mbps, el grupo de ancho de banda permanece 20 Gbps para las 19 instancias CPX restantes.

Si la misma instancia CPX comienza a consumir 1500 Mbps de rendimiento, el grupo de ancho de banda tiene 19,5 Gbps para las 19 instancias CPX restantes.

Para licencias de grupo, puede agregar más ancho de banda solo en múltiplos de 10 Mbps.

### Instancias independientes de NetScaler ADC BLX

Las instancias de NetScaler ADC BLX admiten licencias de capacidad agrupada. Una instancia de NetScaler ADC BLX no requiere una licencia de plataforma. Para procesar el tráfico, una instancia de NetScaler ADC BLX debe desproteger el ancho de banda y una licencia de instancia del grupo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Grupo de ancho de banda

El grupo de ancho de banda es el ancho de banda total que pueden compartir las instancias de NetScaler ADC, tanto físicas como virtuales. El conjunto de ancho de banda comprende grupos separados para cada edición de software (Standard, Advanced y Premium). Una instancia determinada de NetScaler ADC no puede tener ancho de banda de diferentes grupos retirados simultáneamente. El conjunto de ancho de banda desde el que puede comprobar el ancho de banda depende de la edición de software para la que se licencia.

### Grupo de instancias

El grupo de instancias define el número de instancias VPX o CPX o instancias BLX que se pueden administrar mediante la capacidad agrupada de NetScaler ADC o el número de instancias VPX en una instancia SDX-Z.

Cuando se retira del grupo, una licencia desbloquea los recursos de la instancia MPX-Z, SDX-Z, VPX, CPX y BLX, incluidas las CPU/PE, los núcleos SSL, los paquetes por segundo y el ancho de banda.

> **Nota**
>
> El servicio de administración de un SDX-Z no consume una instancia.

### Servidor de licencias NetScaler ADM

La capacidad agrupada de NetScaler ADC utiliza NetScaler ADM configurado como un servidor de licencias para administrar las licencias de capacidad agrupada: licencias de grupos de ancho de banda y licencias de grupos de instancias. Puede usar el software NetScaler ADM para administrar licencias de capacidad agrupada sin una licencia ADM.

Al retirar licencias del ancho de banda y del grupo de instancias, el factor de forma y el número de modelo de hardware de NetScaler ADC en un hardware de capacidad cero determina

- El ancho de banda mínimo y la cantidad de instancias que una instancia de NetScaler ADC debe desproteger antes de funcionar.
- El ancho de banda máximo y el número de instancias que puede desproteger un dispositivo NetScaler ADC.
- La unidad de ancho de banda mínima para cada check-out de ancho de banda. La unidad de ancho de banda mínimo es la unidad de ancho de banda más pequeña que un NetScaler ADC debe desproteger de un grupo. Cualquier check-out debe ser un múltiplo entero de la unidad mínima de ancho de banda. Por ejemplo, si la unidad de ancho de banda mínima de un NetScaler ADC es de 1 Gbps, se pueden proteger 100 Gbps, pero no 200 Mbps o 150.5 Gbps. La unidad de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ancho de banda mínimo es diferente del requisito de ancho de banda mínimo. Una instancia de NetScaler ADC solo puede funcionar después de obtener licencia con al menos el ancho de banda mínimo. Una vez que se alcanza el ancho de banda mínimo, la instancia puede obtener más ancho de banda con la unidad de ancho de banda mínima.

Las tablas 1, 2, 3 y 4 resumen el ancho de banda máximo/instancias, el ancho de banda mínimo y la unidad mínima de ancho de banda para todas las instancias NetScaler ADC admitidas. En la tabla 5 se resumen los requisitos de licencia para diferentes factores de forma para todas las instancias de NetScaler ADC compatibles:

**Tabla 1. Capacidad agrupada admitida para instancias MPX y SDX**

| Línea de productos | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Gbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **MPX 5900Z** | 10 | 1 | N/D | N/D | 1 Gbps |
| **MPX 8005Z** | 15 | 5 | N/D | N/D | 1 Gbps |
| **MPX 8900Z** | 33 | 5 | NA | NA | 1 Gbps |
| **MPX 8900Z FIPS** | 33 | 5 | NA | NA | 1 Gbps |
| **Serie MPX 14000Z** | 100 | 20 | NA | NA | 1 Gbps |
| **Serie MPX 14000Z 40G** | 100 | 20 | N/D | N/D | 1 Gbps |
| **MPX 14000Z serie FIPS** | 100 | 20 | N/D | N/D | 1 Gbps |
| **Serie MPX 14000Z 40S** | 100 | 20 | N/D | N/D | 1 Gbps |
| **Serie MPX 15000Z** | 120 | 20 | N/D | N/D | 1 Gbps |
| **MPX 15000Z serie FIPS** | 120 | 20 | N/D | N/D | 1 Gbps |
| **Serie 50G de MPX 15000Z** | 120 | 20 | N/D | N/D | 1 Gbps |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Línea de productos | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Gbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **Serie MPX 115XX** | 42 | 15 | N/D | N/D | 1 Gbps |
| **Serie MPX 22000Z** | 120 | 40 | N/D | N/D | 1 Gbps |
| **Serie MPX 24000Z** | 150 | 100 | N/D | N/D | 1 Gbps |
| **MPX 25000Z 40G** | 200 | 100 | N/D | N/D | 1 Gbps |
| **MPX 25000ZA** | 200 | 100 | N/D | N/D | 1 Gbps |
| **Serie MPX 26000Z** | 200 | 100 | N/D | N/D | 1 Gbps |
| **Serie MPX 26000Z 100G** | 200 | 100 | N/D | N/D | 1 Gbps |
| **Serie MPX 26000Z 50S** | 200 | 100 | N/D | N/D | 1 Gbps |
| **SDX 8015Z** | 15 | 7 | 1 | 5 | 1 Gbps |
| **SDX 8900Z** | 33 | 10 | 2 | 7 | 1 Gbps |
| **Serie SDX 115XX** | 42 | 8 | 2 | 20 | 1 Gbps |
| **Serie SDX 14000Z** | 100 | 10 | 2 | 25 | 1 Gbps |
| **Serie SDX 14000Z 40G** | 100 | 10 | 2 | 25 | 1 Gbps |
| **Serie SDX 14000Z 40S** | 100 | 20 | 10 | 25 | 1 Gbps |
| **Serie SDX 14000Z FIPS** | 100 | 10 | 2 | 25 | 1 Gbps |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Línea de productos | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Gbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **SDX 15000Z 50G** | 120 | 10 | 2 (Nota: 5 instancias para versiones inferiores a 13.0 47.x) | 55 | 1 Gbps |
| **SDX 15000Z** | 120 | 10 | 2 Nota: 5 instancias para versiones inferiores a 13.0 47.x) | 55 | 1 Gbps |
| **Serie SDX 22000Z** | 120 | 20 | 20 | 80 | 1 Gbps |
| **SDX 25000Z 40G** | 200 | 50 | 10 | 115 | 1 Gbps |
| **SDX 25000ZA** | 200 | 50 | 10 | 115 | 1 Gbps |
| **SDX 26000Z 100 G** | 200 | 50 | 10 | 115 | 1 Gbps |
| **SDX 26000Z** | 200 | 50 | 10 | 115 | 1 Gbps |
| **SDX 26000Z 50** | 200 | 50 | 10 | 115 | 1 Gbps |
| **Serie SDX 24000Z** | 150 | 50 | 10 | 80 | 1 Gbps |

> Nota
>
> El ancho de banda mínimo y las instancias se aplican a las instancias SDX que ejecutan las siguientes versiones y versiones superiores: 11.1 64.x, 12.0 63.x, 12.1 54.x y 13.0 41.x.
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

**Tabla 2. Capacidad agrupada admitida para instancias CPX**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Línea de productos | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Mbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **CPX** | 10 | 10 | 1 | 1 | 10 Mbps |

**Tabla 3. Capacidad agrupada admitida para instancias VPX en hipervisores y servicios en la nube**

| Hipervisor/servicio en la nube | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Mbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **Citrix Hypervisor** | 40 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **VMware ESXi** | 100 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **Linux KVM** | 100 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **Microsoft Hyper-V** | 3 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **AWS** | 30 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **Azure** | 10 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |
| **Google Cloud** | 10 Gbps | 10 Mbps | 1 | 1 | 10 Mbps |

> Nota
>
> La cantidad mínima de compra es diferente del requisito mínimo del sistema.

**Tabla 4. Capacidad agrupada admitida para instancias BLX**

| Línea de productos | Ancho de banda máximo (Gbps) | Ancho de banda mínimo (Mbps) | Instancias mínimas | Instancias máximas | Unidad mínima de ancho de banda |
|---|---|---|---|---|---|
| **BLX** | 100 | 10 | 1 | 1 | 10 Mbps |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Tabla 5. Requisito de licencia para diferentes factores de forma**

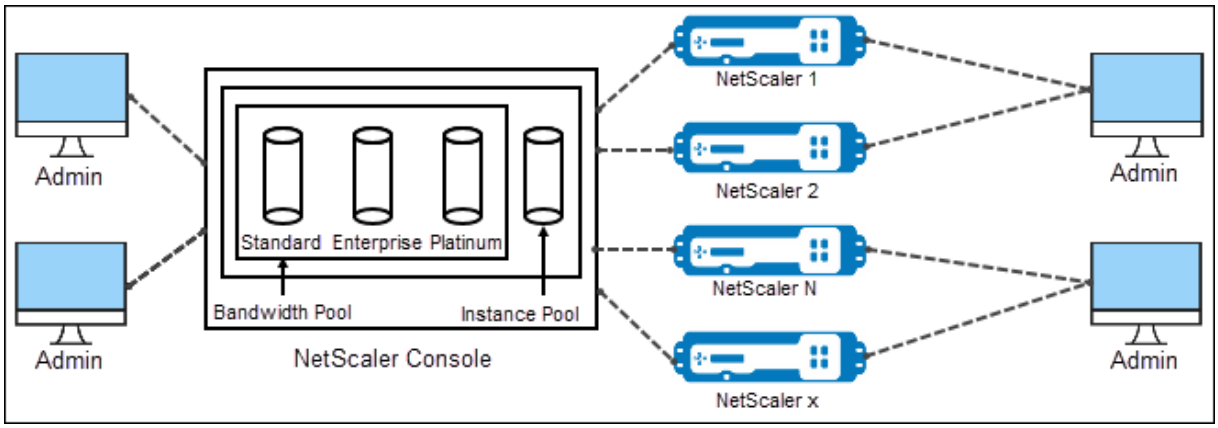
| Línea de productos | Compra de hardware de capacidad cero | Suscripción Bandwidth & Edition | Suscripción de instancias |
|---|---|---|---|
| **MPX** | Se requiere licencia | Se requiere licencia | - |
| **SDX** | Se requiere licencia | Se requiere licencia | Se requiere licencia |
| **VPX** | - | Se requiere licencia | Se requiere licencia |
| **CPX** | - | - | Se requiere licencia |
| **BLX** | - | Se requiere licencia | Se requiere licencia |

## Configurar la capacidad agrupada de Citrix ADC

January 30, 2024

Para usar la capacidad agrupada de ADC, configure Citrix ADM como un servidor de licencias para las instancias de ADC requeridas. Las instancias de ADC registran y desprotegen las licencias de ADM. Puede realizar las siguientes tareas en la GUI de ADM:

- Cargue los archivos de licencia de capacidad agrupada (ancho de banda y grupo de instancias) en el servidor de licencias.
- Asigne licencias del grupo de licencias a instancias de Citrix ADC bajo demanda.
- Consulte las licencias de las instancias de Citrix ADC (MPX-Z /SDX-Z/VPX/CPX/BLX) en función de la capacidad mínima y máxima de la instancia.
- Configure la capacidad agrupada para que las instancias FIPS de Citrix ADC registren o desprotejan licencias.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Versiones de hardware y software compatibles

Para ver las versiones de hardware y software compatibles para la capacidad agrupada, consulte Capacidad agrupada de Citrix ADC.

### Estados de capacidad agrupada de ADC

Los estados de capacidad agrupada indican el requisito de licencia en una instancia de ADC. Las instancias de ADC configuradas con capacidad agrupada muestran uno de los siguientes estados:

- **Óptimo**: la instancia se ejecuta con la capacidad de licencia adecuada.
- **Discrepancia de capacidad**: la instancia se ejecuta con una capacidad inferior a la configurada por el usuario.
- **Grace**: La instancia se ejecuta en una licencia de gracia.
- **Grace & Mismatch**: La instancia se ejecuta en gracia pero con una capacidad inferior a la configurada por el usuario.
- **No disponible**: la instancia no está registrada en ADM para su administración o la comunicación de NITRO desde ADM a las instancias no funciona.
- **No asignada**: la licencia no está asignada en la instancia.

### Paso 1: Aplicar licencias en ADM

1. En Citrix ADM, vaya a **Redes** > **Licencias**.
2. En la sección **Archivos de licencia**, seleccione **Agregar archivo de licencia** y seleccione una de las siguientes opciones:
   - **Cargue los archivos de licencia desde un equipo local**. Si ya hay un archivo de licencia en su equipo local, puede cargarlo en ADM.
   - **Utilice el código de acceso de licencia**. Especifique el código de acceso a la licencia de la licencia que ha adquirido en Citrix. A continuación, seleccione **Obtener licencias**. A continuación, selecciona **Finalizar**.

   > **Nota**
   >
   > En cualquier momento, puede agregar más licencias a ADM desde **Configuración de licencias**.

3. Haga clic en **Finalizar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Los archivos de licencia se agregan a ADM. La ficha **Información de caducidad de licencia** enumera las licencias presentes en la ADM y los días restantes hasta su caducidad.

4. En **Archivos de licencia**, seleccione el archivo de licencia que quiera aplicar y haga clic en **Aplicar licencias**.

   Esta acción permite que las instancias ADC utilicen la licencia seleccionada como capacidad agrupada.

## Paso 2: Registrar Citrix ADM como servidor de licencias

Para registrar ADM como servidor de licencias en una instancia de Citrix ADC, siga uno de los procedimientos:

- Usar GUI
- Usar CLI

### Usar la interfaz gráfica de usuario para registrar ADM como servidor de licencias

En la GUI de ADC, registre el servidor ADM como servidor de licencias.

1. Inicie sesión en la GUI de Citrix ADC.
2. Vaya a **Sistema** > **Licencias** > **Administrar licencias** .
3. Haga clic en **Agregar licencia nueva**.
4. Seleccione **Usar licencias remotas** y seleccione el modo de licencia remota de la lista.
5. En el campo **Nombre del servidor/dirección IP**, especifique la dirección IP del servidor ADM.
6. Seleccione **Registrar con Citrix ADM**.
7. Introduzca sus credenciales de ADM para registrar una instancia en Citrix ADM y haga clic en **Continuar**.
8. En **Asignar licencias**, seleccione la edición de la licencia y especifique el ancho de banda requerido.

   Por primera vez, asigne licencias en Citrix ADC. Más adelante, puede cambiar o liberar la asignación de licencias desde la GUI de ADM.
9. Haga clic en **Obtener licencias**.

   > **Importante**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Reinicie la instancia en caliente si cambia la edición de la licencia. Los cambios de configuración no surtirán efecto hasta que reinicie la instancia.

#### Usar la CLI para agregar ADM como servidor de licencias

Si una instancia de ADC no tiene GUI, use los siguientes comandos de la CLI para agregar el servidor ADM como servidor de licencias:

1. Inicie sesión en la consola ADC.
2. Agregue la dirección IP del servidor ADM:

```
> add ns licenseserver <adm-server-IP-address> -port <adm-server-port-number>
```

3. Ver el ancho de banda de licencia disponible en el servidor de licencias:

```
> sh ns licenseserverpool
```

4. Asigne el ancho de banda de licencia desde la edición de licencia requerida:

```
> set ns capacity -unit gbps -bandwidth <specify-license-bandwidth> edition <specify-license-edition>
```

La edición de licencia puede ser **Standard**, **Enterprise** o **Platinum**.

> **Importante**
>
> Warm reinicie la instancia si cambia la edición de la licencia.
>
> `reboot -w`
>
> Los cambios de configuración no surtirán efecto hasta que reinicies la instancia.

### Paso 3: Asignar licencias agrupadas a las instancias de ADC

Para asignar licencias de capacidad agrupada desde la GUI de ADM:

1. Inicie sesión en Citrix ADM.
2. Vaya a **Redes > Licencias > Licencias > Licencias de ancho de banda > Capacidad agrupada**.

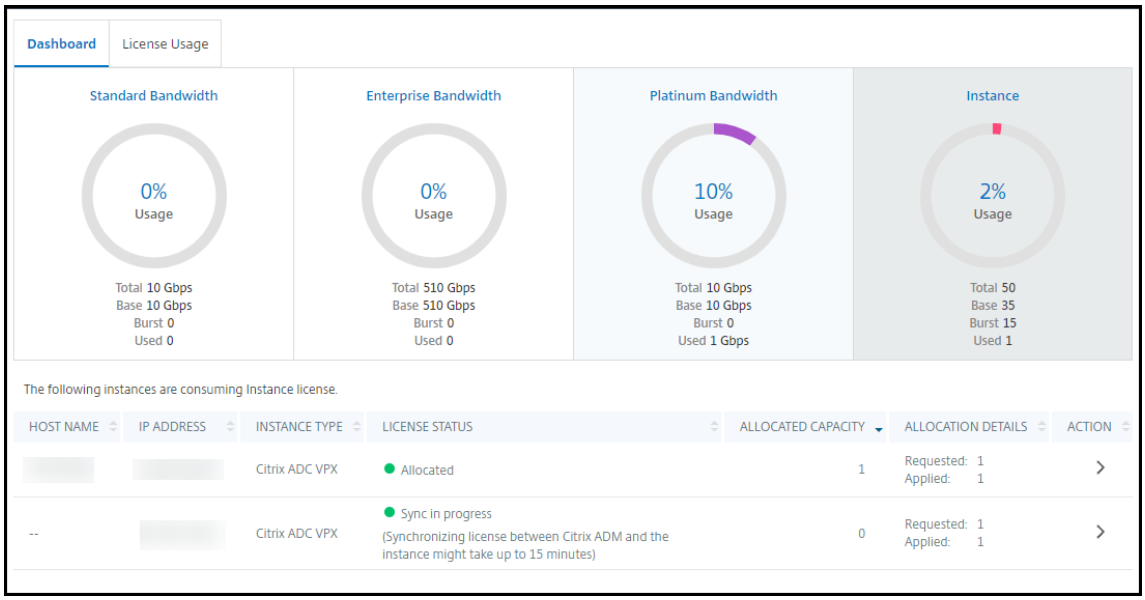
   La capacidad de instancia FIPS solo aparece si carga licencias de instancia FIPS a ADM.
3. Haga clic en el grupo de licencias que quiere administrar.

> **Nota**
>
> El campo **Capacidad asignada** no refleja el ancho de banda modificado de forma inmediata. El cambio de ancho de banda se aplica después del reinicio en caliente del ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> En **Detalles de asignación, los**campos **Solicitado** y **Aplicado se** actualizan cuando cambias la asignación de ancho de banda de la instancia.

4. Seleccione una instancia ADC de la lista de instancias disponibles haciendo clic en el botón **>**.

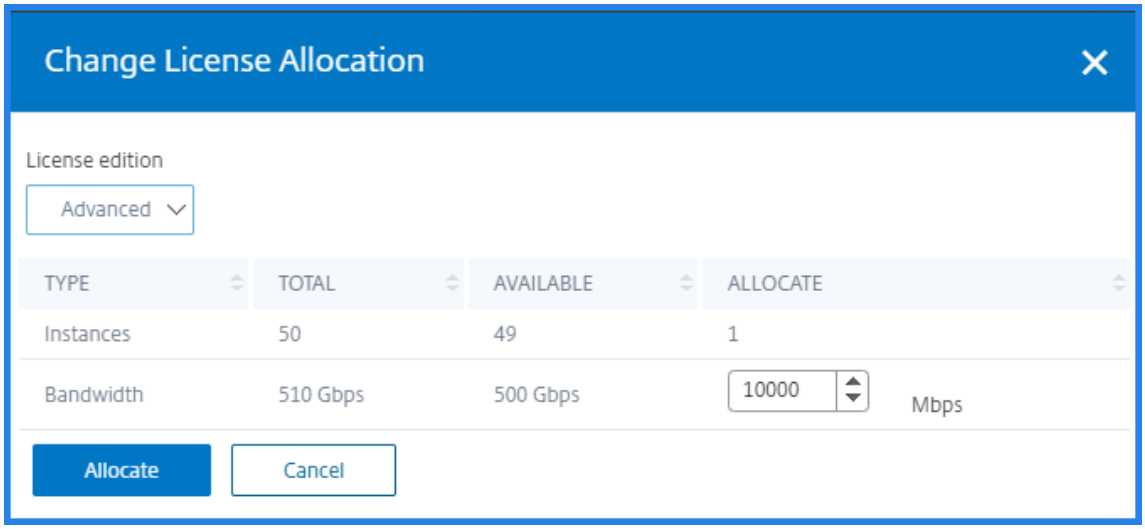



La columna Estado de la **licencia** muestra los mensajes de estado de asignación de licencias correspondientes.

> **Nota**
>
> La ficha **Instancias no administradas** muestra las instancias detectadas pero no administradas en Citrix ADM.
>
>
> 

5. Haga clic en **Cambiar asignación** o **Liberar asignación** para modificar la asignación de licencias.
6. Aparecerá una ventana emergente con las licencias disponibles en el servidor de licencias.
7. Puede elegir el ancho de banda o la asignación de instancias a la instancia configurando las opciones de la lista Asignación. Después de hacer las selecciones, haga clic en **Asignar**.
8. También puede cambiar la edición de licencia asignada desde las opciones de lista en la **ventana Cambiar asignación de licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota**
>
> Reinicie en caliente una instancia si cambia la edición de la licencia.

## Configurar la capacidad agrupada en instancias de ADC

Puede configurar licencias de capacidad agrupada en las siguientes instancias de ADC:

- Instancias ADC MPX-Z
- Instancias de ADC VPX
- Par de alta disponibilidad ADC

### Instancias de Citrix ADC MPX-Z

MPX-Z es el dispositivo ADC MPX habilitado para capacidad agrupada. MPX-Z admite la agrupación de ancho de banda para licencias de edición Premium, Advanced o Standard.

MPX-Z requiere licencias de plataforma antes de poder conectarse al servidor de licencias. Puede instalar la licencia de plataforma MPX-Z de las siguientes maneras:

- Carga del archivo de licencia desde un equipo local.
- Usar el número de serie del hardware de la instancia.
- El código de acceso a licencias de la sección **Sistema** > **Licencias** de la GUI de la instancia.

Si elimina la licencia de plataforma MPX-Z, la función de capacidad agrupada se desactiva. Las licencias de instancia se entregan al servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia MPX-Z sin necesidad de reiniciar. Solo se requiere un reinicio si quiere cambiar la edición de la licencia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota:**
>
> Cuando reinicias la instancia, esta comprueba automáticamente las licencias agrupadas necesarias para su capacidad configurada.

#### Instancias de Citrix ADC VPX

Una instancia de ADC VPX habilitada para capacidad agrupada puede extraer licencias de un grupo de ancho de banda (ediciones Premium/Advanced/Standard). Puede usar la GUI de ADC para extraer licencias del servidor de licencias.

Puede modificar dinámicamente el ancho de banda de una instancia VPX sin necesidad de reiniciar. Solo se requiere un reinicio si quiere cambiar la edición de la licencia.

> **Nota:**
>
> Cuando reinicia la instancia, las licencias de capacidad agrupada configuradas se extraen automáticamente del servidor ADM.

#### Par de alta disponibilidad Citrix ADC

Antes de empezar, asegúrese de que el servidor ADM esté configurado como un servidor de licencias. Para obtener más información, consulte Configurar ADM como servidor de licencias.

Para las instancias de ADC configuradas en un modo de alta disponibilidad, debe configurar la capacidad agrupada en cada nodo del par de alta disponibilidad. Tanto para el nodo principal como para el secundario, debe asignar licencias de la misma capacidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, necesita el doble de capacidad (2 Gbps) del grupo común. A continuación, puede asignar una capacidad de 1 Gbps a cada nodo.

Para asignar licencias de grupo a cada nodo del par, siga los pasos que se indican en Asignar licencias agrupadas a instancias de ADC. En primer lugar, asigne la licencia al primer nodo y, a continuación, repita los mismos pasos para asignar la licencia al segundo nodo.

## Configurar un servidor ADM solo como servidor de licencias agrupado

August 23, 2024

Como administrador, puede configurar un servidor ADM solo como servidor de licencias agrupado. Con esta configuración, el servidor ADM solo recibe datos de licencias de instancias ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

A veces, es posible que tenga el mandato regulatorio que requiere restringir los datos de las instancias ADC para no salir de la zona reguladora. En tales situaciones, puede implementar una instancia local de un servidor ADM local en la zona reglamentaria para utilizar las capacidades de administración, supervisión y análisis. Cuando se sigue el mismo enfoque para utilizar la función de licencias agrupadas, debe dividir las licencias agrupadas en varios servidores de licencias de ADM. Este enfoque no le proporciona la flexibilidad necesaria para asignar licencias agrupadas en todas sus instancias ADC implementadas globalmente.

Por lo tanto, configure el servidor ADM solo como servidor de licencias agrupado. El servidor ADM solo recibe datos de licencias de todas las instancias de ADC. Por lo tanto, puede cumplir con el mandato reglamentario y asignar dinámicamente licencias de capacidad agrupadas en todas las instancias de ADC implementadas globalmente.

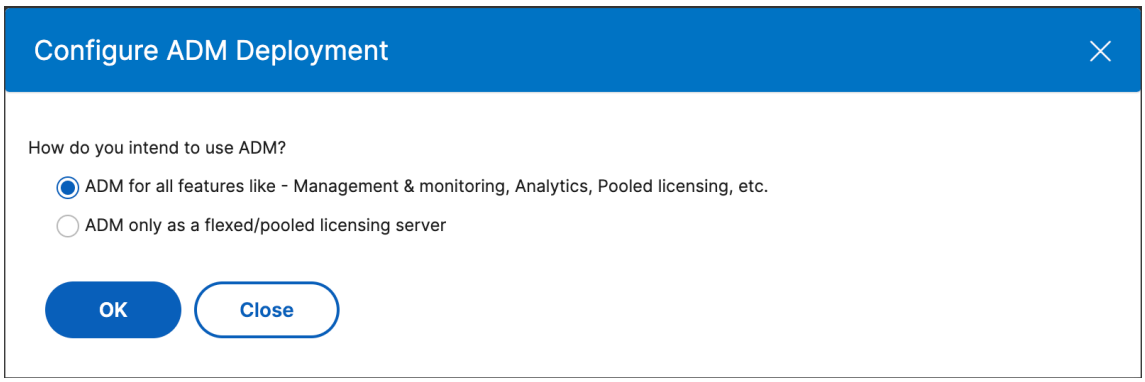
En este documento se explica cómo configurar un servidor ADM solo como servidor de licencias agrupado.

## Cómo configurar un servidor ADM solo como servidor de licencias agrupado

Antes de comenzar, asegúrese de que no se hayan agregado instancias ADC a un servidor ADM. Agregue las instancias de ADC solo después de completar el paso 4.

Haga lo siguiente para configurar un servidor ADM solo para el servidor de licencias agrupado:

1. Vaya a **Sistema > Administración** .
2. En la sección **Configuraciones del sistema**, seleccione **Implementación del sistema**.
3. En **Implementación de ADM**, seleccione **ADM solo como servidor de licencias agrupado**.




4. Haga clic en **Aceptar**.

   Esta acción solo conserva la función de licencias agrupadas e inhabilita las siguientes funciones de ADM:

   - Copia de seguridad de ADM
   - Gestión de eventos

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Administración de certificados SSL
- Informes de red
- Funciones de red
- Auditoría de configuración

> **Nota**
>
> De forma predeterminada, la función de análisis de ADM está inhabilitada. Asegúrese de inhabilitar esta función si la ha habilitado.

En el cuadro de confirmación, haga clic en **Sí**.

La GUI de ADM ahora muestra solo la función de licencias agrupadas. Y las funciones restantes no aparecen.

5. Después de configurar ADM solo para la función de licencia, agregue instancias de ADC en la página **Redes > Instancias**.

> **Nota**
>
> - Puede agregar una instancia de ADC en uno o más servidores ADM. Cuando cambie la contraseña de dichas instancias de ADC, asegúrese de actualizar la contraseña en todos los servidores ADM donde se detecte la instancia.
> - Un usuario todavía puede realizar algunas operaciones de las funciones inhabilitadas en la GUI de ADM. Por ejemplo, sondeo de eventos y copia de seguridad de ADC. Como superadministrador, Si quiere restringir tales operaciones, inhabilite los accesos de usuario para otros administradores mediante una directiva de acceso adecuada. Para obtener más información, consulte Configurar directivas de acceso en NetScaler ADM.

## Actualizar una licencia perpetua en NetScaler ADC VPX a la capacidad agrupada de NetScaler ADC

January 30, 2024

Las instancias de NetScaler ADC VPX con licencia perpetua se pueden actualizar a una licencia de capacidad agrupada de ADC. La actualización a una licencia de capacidad agrupada le permite asignar licencias del grupo de licencias a las instancias VPX según demanda. También puede configurar una licencia de capacidad agrupada para instancias de ADC configuradas en un modo de alta disponibilidad. Para configurar la licencia de capacidad agrupada para instancias VPX en modo de alta disponibilidad, consulte Actualización de la licencia perpetua en NetScaler ADC VPX High Availability Pair a NetScaler ADC Pooled Capacity.

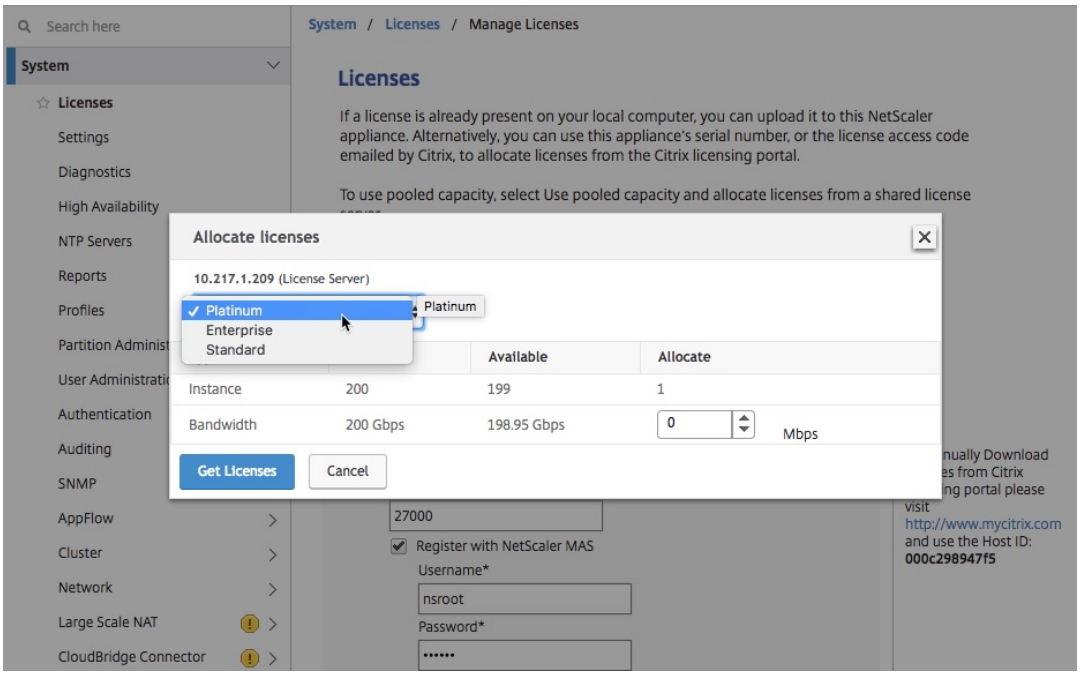
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Requisitos previos

Asegúrese de actualizar la instancia VPX a la versión 12.0.56.x.

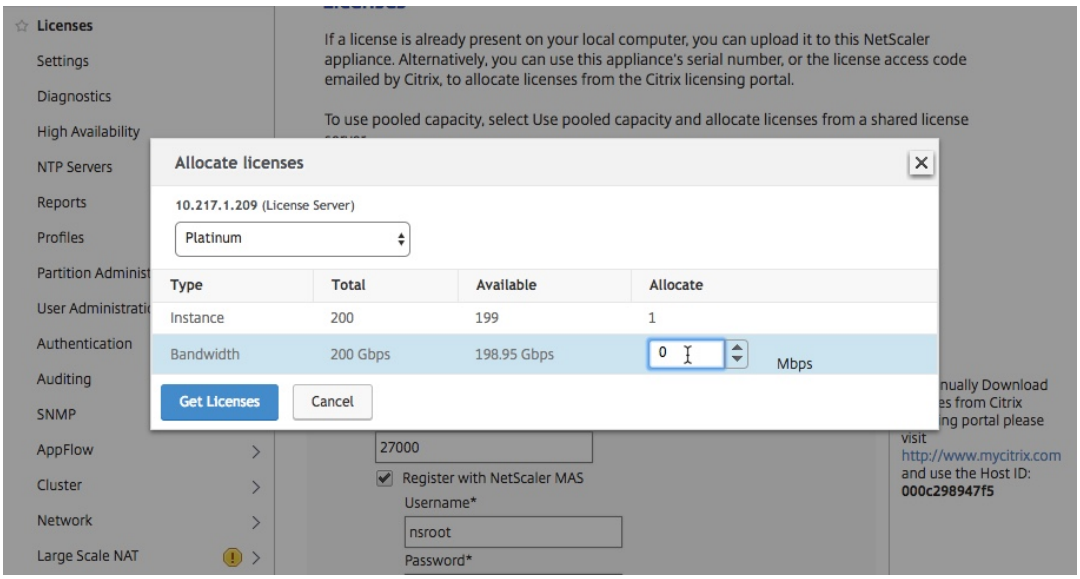
**Para actualizar a la capacidad agrupada de NetScaler ADC:**

1. En un explorador web, escriba la dirección IP de la instancia VPX, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. En la pestaña Configuración, vaya a **Sistema > Licencias** y haga clic en **Administrar licencias** .
5. En la página **Licencias**, haga clic en **Agregar nueva licencia**.
6. En la página **Licencias**, elija **Usar licencias remotas** y haga lo siguiente:
   a) En la lista desplegable del **modo de licencia remota**, seleccione Licencias **agrupadas.**
   b) En el campo **Nombre del servidor/Dirección IP**, Introduzca los detalles del servidor de licencias.
   c) Asegúrese de que la casilla de verificación **Registrar con NetScaler ADM** esté seleccionada e introduzca las credenciales de NetScaler ADM, si quiere administrar las licencias de grupo de su instancia a través de ADM.
   d) Haga clic en **Continuar**.
7. En la ventana **Asignar licencias**, haga lo siguiente:
   a) Seleccione la edición de licencia en la lista desplegable.

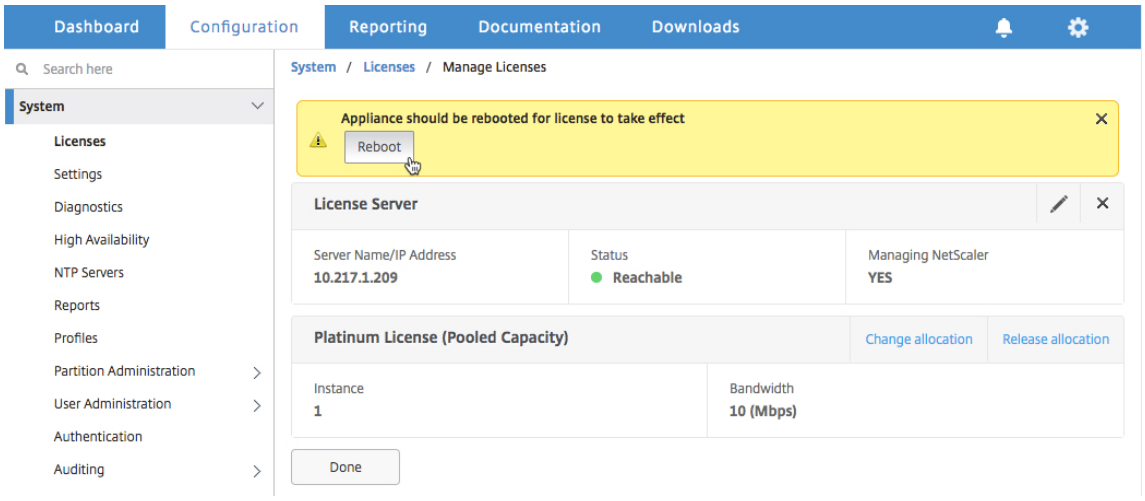



© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.




8. Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.




9. En el cuadro de diálogo Confirmar, haga clic en **Sí** .

10. Después de que se reinicie la instancia VPX, inicie sesión en la instancia. En la página de **bienvenida**, haga clic en **Continuar**.

    La página **Licencias** muestra todas las funciones que tienen licencia en el dispositivo NetScaler ADC VPX. Haga clic en **X**.

11. Vaya a **Sistema > Licencias** y haga clic en **Administrar licencias**.

    En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y el ancho de banda asignado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

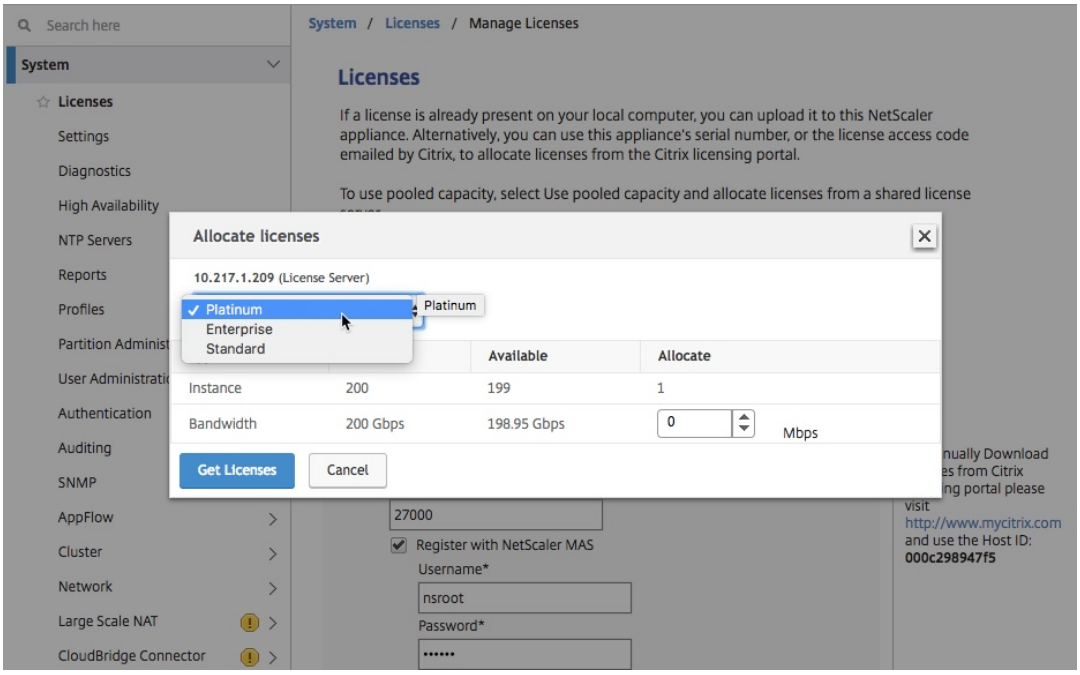
### Actualizar la licencia perpetua en el par de alta disponibilidad de NetScaler ADC VPX a la capacidad agrupada de NetScaler ADC

Para las instancias VPX configuradas en modo de alta disponibilidad, debe configurar la capacidad agrupada tanto en las instancias principales como en las secundarias del par de alta disponibilidad. Tanto para las instancias principales como para las secundarias, debe asignar licencias de la misma capacidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, necesita el doble de capacidad (2 Gbps) del grupo común. A continuación, puede asignar una capacidad de 1 Gbps a cada una de las instancias principal y secundaria del par de alta disponibilidad.

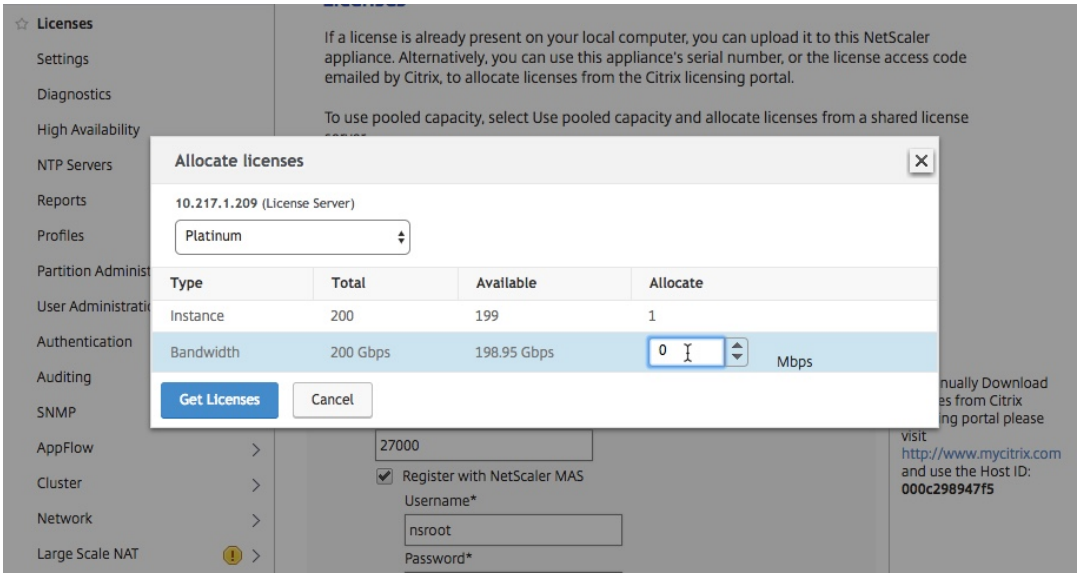
**Para actualizar una configuración existente de NetScaler ADC VPX HA a la capacidad agrupada de NetScaler ADC:**

1. Inicie sesión en la instancia VPX secundaria (nodo 2). En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como `http://192.168.100.1`.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. En la ficha Configuración, vaya a **Sistema** > **Licencias** y haga clic en **Administrar licencias**.
5. En la página **Licencias**, haga clic en **Agregar nueva licencia**.
6. En la página **Licencias**, elija **Usar licencias remotas** y haga lo siguiente:
   a) En la lista desplegable del **modo de licencia remota**, seleccione Licencias **agrupadas.**
   b) En el campo **Nombre del servidor/Dirección IP**, Introduzca los detalles del servidor de licencias.
   c) Asegúrese de que la casilla de verificación **Registrar con NetScaler ADM** esté seleccionada e introduzca las credenciales de ADM, si quiere administrar las licencias de grupo de su instancia a través de NetScaler ADM.
   d) Haga clic en **Continuar**.
7. En la ventana Asignar licencias, haga lo siguiente:
   a) Seleccione la edición de licencia en la lista desplegable.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

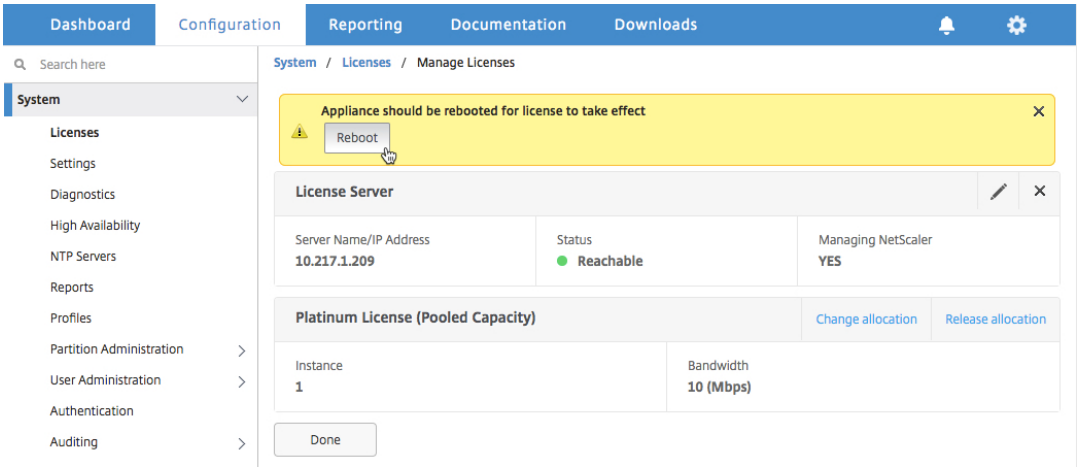



b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.




c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar en caliente la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




8. En el cuadro de diálogo **Confirmar**, haga clic en **Sí**.

   La instancia VPX se reinicia.

   Cuando se le solicite, haga clic en Reiniciar para reiniciar el dispositivo. Una vez que el dispositivo esté en funcionamiento con la nueva licencia, fuerce una conmutación por error escribiendo `force ha failover`. Esta conmutación por error garantiza que el par de alta disponibilidad esté en buen estado.

9. Inicie sesión en la instancia VPX principal existente (nodo 1) y reiníciela. Complete los siguientes pasos.

   a) En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.

   b) En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.

   c) En la página de **bienvenida**, haga clic en **Continuar**.

   d) En la ficha **Configuración**, haga clic en **Sistema**.

   e) En la página **Sistema**, haga clic en **Reiniciar**.

   f) En la página **Reiniciar**, seleccione **Reiniciar en caliente** y haga clic en **Aceptar**.

   Cuando se reinicia el nodo 1, se convierte en la instancia secundaria del par de alta disponibilidad. Si quiere cambiar la instancia principal y secundaria del par de alta disponibilidad a la configuración del par de alta disponibilidad original, fuerce una conmutación por error. Ejecute el siguiente comando en cualquier instancia del par de alta disponibilidad:

“‘

> forzar conmutación por error ha

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

10. Para comprobar que la instancia VPX se actualice a una licencia de capacidad agrupada, inicie sesión en las instancias principal y secundaria y lleve a cabo los siguientes pasos.

    a) En la página de **bienvenida**, haga clic en **Continuar**.

    b) En la pestaña Configuración, vaya a **Sistema > Licencias** y haga clic en **Administrar licencias** . En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y el ancho de banda asignado.

## Actualización de una licencia perpetua en NetScaler ADC MPX a la capacidad agrupada de NetScaler ADC

January 30, 2024

El dispositivo NetScaler ADC MPX con licencia perpetua se puede actualizar a la licencia NetScaler ADC Pooled Capacity. La actualización a la licencia NetScaler ADC Pooled Capacity le permite asignar licencias del grupo de licencias a dispositivos NetScaler ADC bajo demanda. También puede configurar la licencia de capacidad agrupada de NetScaler ADC para instancias de ADC configuradas en modo de alta disponibilidad. Para configurar la licencia de NetScaler ADC Pooled Capacity para instancias NetScaler ADC MPX en modo de alta disponibilidad, consulte Actualizar la licencia perpetua en el par de alta disponibilidad de NetScaler ADC MPX a la capacidad agrupada de NetScaler ADC.

> **Nota**
>
> La conversión de una licencia perpetua a una licencia de capacidad agrupada es un proceso unidireccional para el derecho de licencia. No puede revertir la licencia de capacidad agrupada a perpetua.
>
> **Importante**
>
> Para actualizar el dispositivo Citrix ADC MPX a la licencia Citrix ADC Pooled Capacity, debe cargar la licencia MPX-Z en el dispositivo.

**Para actualizar a la capacidad agrupada de NetScaler ADC:**

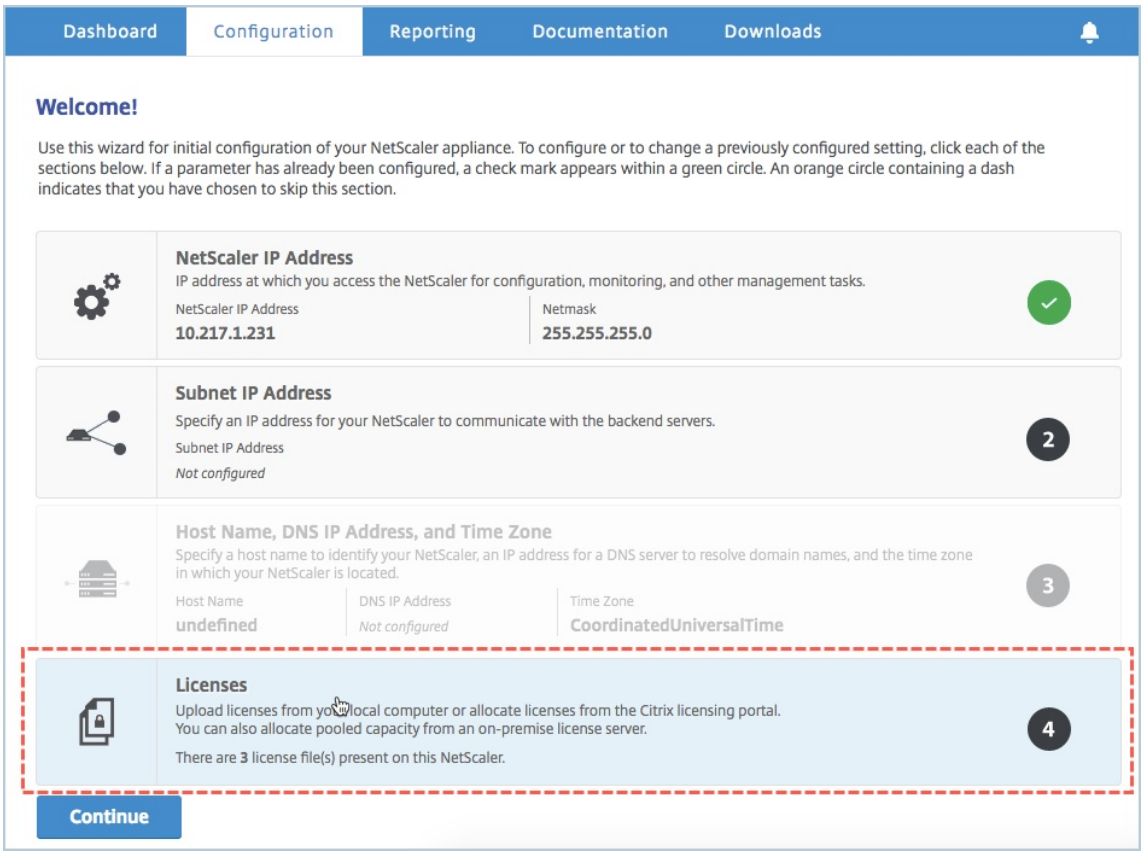
1. En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha Configuración, vaya a **Sistema** > **Licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en Agregar **nueva licencia** .
6. En la página **Licencias**, seleccione **Cargar archivos de licencia** y haga clic en **Examinar** para seleccionar la licencia de capacidad cero de su equipo local.
7. Después de cargar la licencia, haga clic en **Reiniciar** para reiniciar el dispositivo.

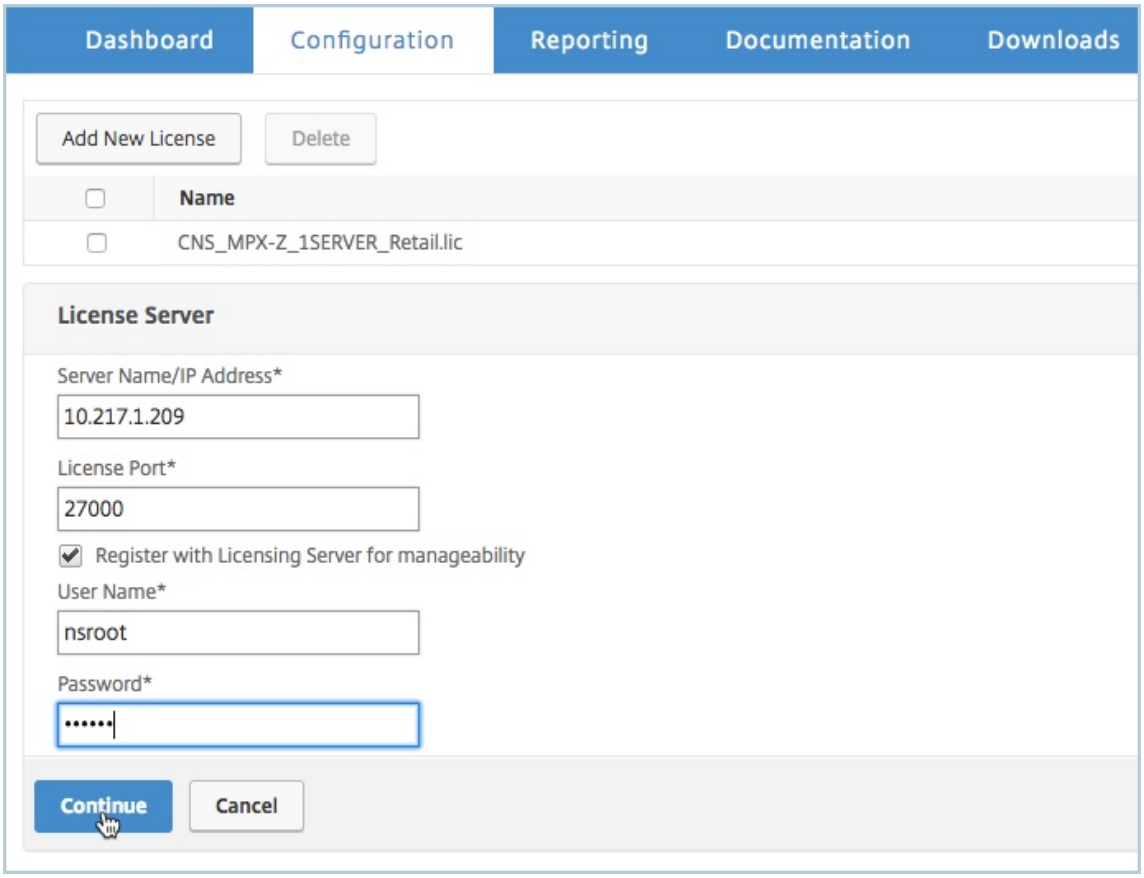
> **Advertencia**
>
> Después de aplicar la licencia MPX-Z, las funciones, incluida la descarga de SSL en el dispositivo, quedan sin licencia. El dispositivo deja de procesar solicitudes HTTPS.
>
> Si la opción **Secure Access Only** está habilitada en el dispositivo antes de la actualización, no puede conectarse al dispositivo a través de la GUI de NetScaler ADM, mediante HTTPS.

8. En la página de **confirmación** , haz clic en **Sí** .
9. Una vez reiniciado el dispositivo, inicie sesión en el dispositivo.
10. En la página de bienvenida, haga clic en la sección **Licencias** .




11. En la sección **Servidor de licencias**, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




a) En el campo **Nombre del servidor/Dirección IP**, introduzca los detalles del servidor de licencias.

b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

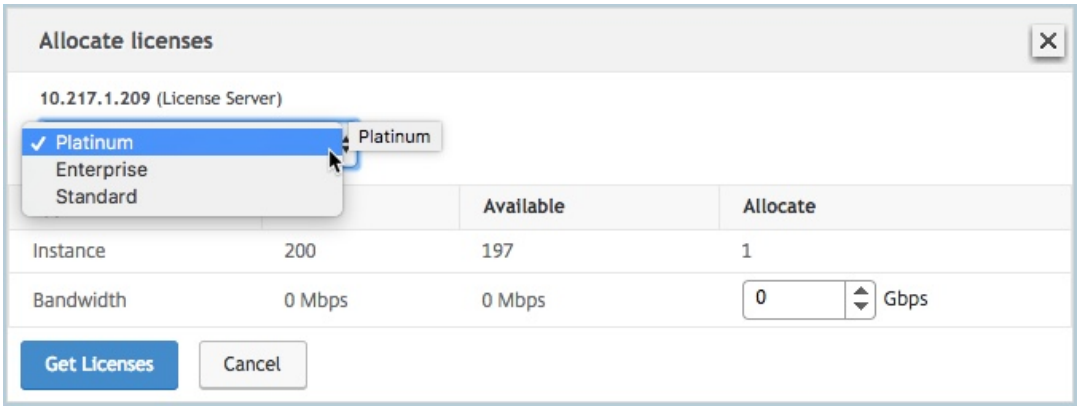
c) Si quiere administrar las licencias de grupo de su instancia a través de NetScaler ADM, seleccione la casilla de verificación **Register with Licensing Server for manageability** e introduzca las credenciales de ADM.

d) Haga clic en **Continuar**.

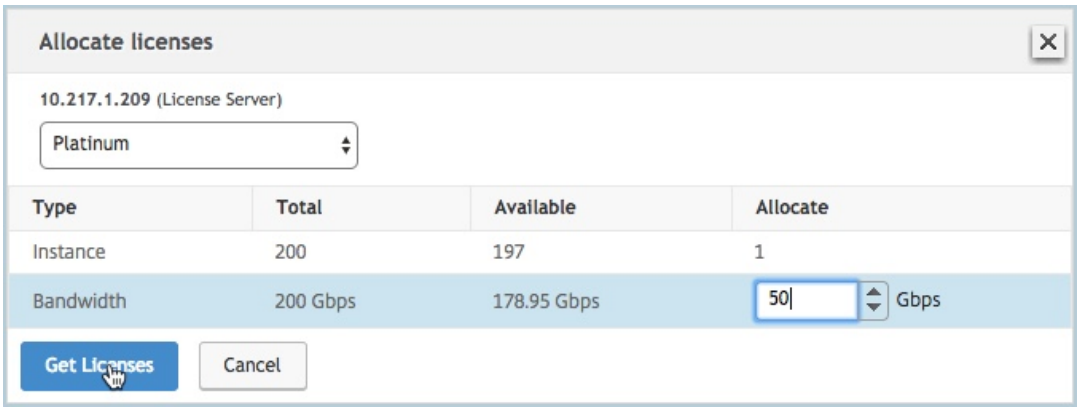
12. En la ventana Asignar licencias, haga lo siguiente:

    a) Seleccione la edición de licencia en la lista desplegable.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.




c) Cuando se le solicite, haga clic en **Reiniciar** para reiniciar el dispositivo.

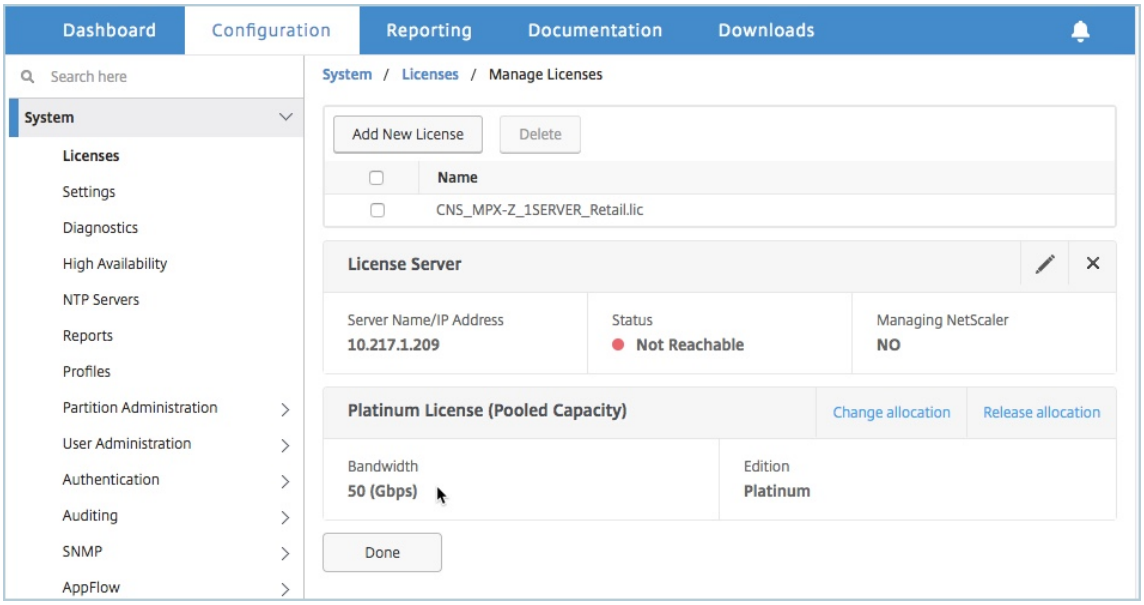
13. Una vez que se reinicie el dispositivo NetScaler ADC MPX, inicie sesión en el dispositivo NetScaler ADC MPX. En la página de **bienvenida**, haga clic en **Continuar**.

    La página **Licencias** muestra todas las funciones con licencia.

14. Vaya a **Sistema > Licencias** y haga clic en **Administrar licencias**.

    En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y el ancho de banda asignado.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Actualización de la licencia perpetua en el par de alta disponibilidad NetScaler ADC MPX a la capacidad agrupada de NetScaler ADC

Para los dispositivos MPX configurados en modo de alta disponibilidad, debe configurar la capacidad agrupada en las instancias ADC principales y secundarias en el par de alta disponibilidad. Asigne licencias de la misma capacidad a las instancias de NetScaler ADC principales y secundarias en el par de alta disponibilidad. Por ejemplo, si quiere una capacidad de 1 Gbps de cada instancia en el par de alta disponibilidad, debe asignar una capacidad de 2 Gbps del grupo común. Con una capacidad de 2 Gbps, puede asignar 1 Gbps cada una a las instancias de NetScaler ADC principal y secundaria en el par de alta disponibilidad.

> **Importante**
>
> Para actualizar el dispositivo NetScaler ADC MPX para usar la licencia NetScaler ADC Pooled Capacity, debe cargar el MPX-Z al dispositivo.

### Requisitos previos

Asegúrese de cargar la licencia MPX-Z en las instancias principales y secundarias del par de HA.

**Para cargar la licencia MPX-Z a las instancias MPX de NetScaler ADC en el par HA:**

1. En un explorador web, escriba la dirección IP del dispositivo. Por ejemplo: http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.

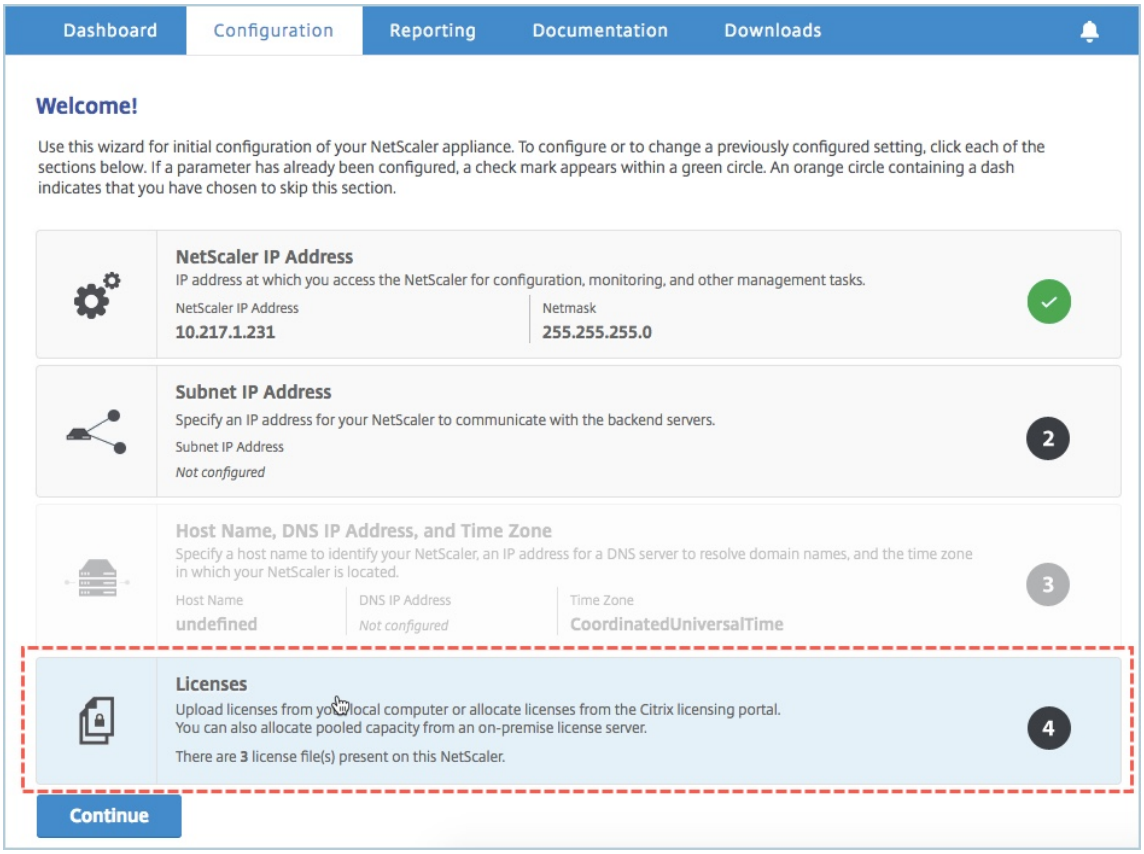
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. Cargue la licencia de capacidad cero (licencia MPX-Z). En la ficha **Configuración**, vaya a **Sistema > Licencias**.
5. En el panel de detalles, haga clic en **Administrar licencias** y, a continuación, en **Agregar nueva licencia** .
6. En la página **Licencias**, seleccione **Cargar archivos de licencia** y haga clic en **Examinar** para seleccionar la licencia de capacidad cero de su equipo local.

   Una vez cargada la licencia, se le pedirá que reinicie el dispositivo.
7. Haga clic en **Reiniciar** para reiniciar el dispositivo.
8. En la página de **confirmación** , haz clic en **Sí** .

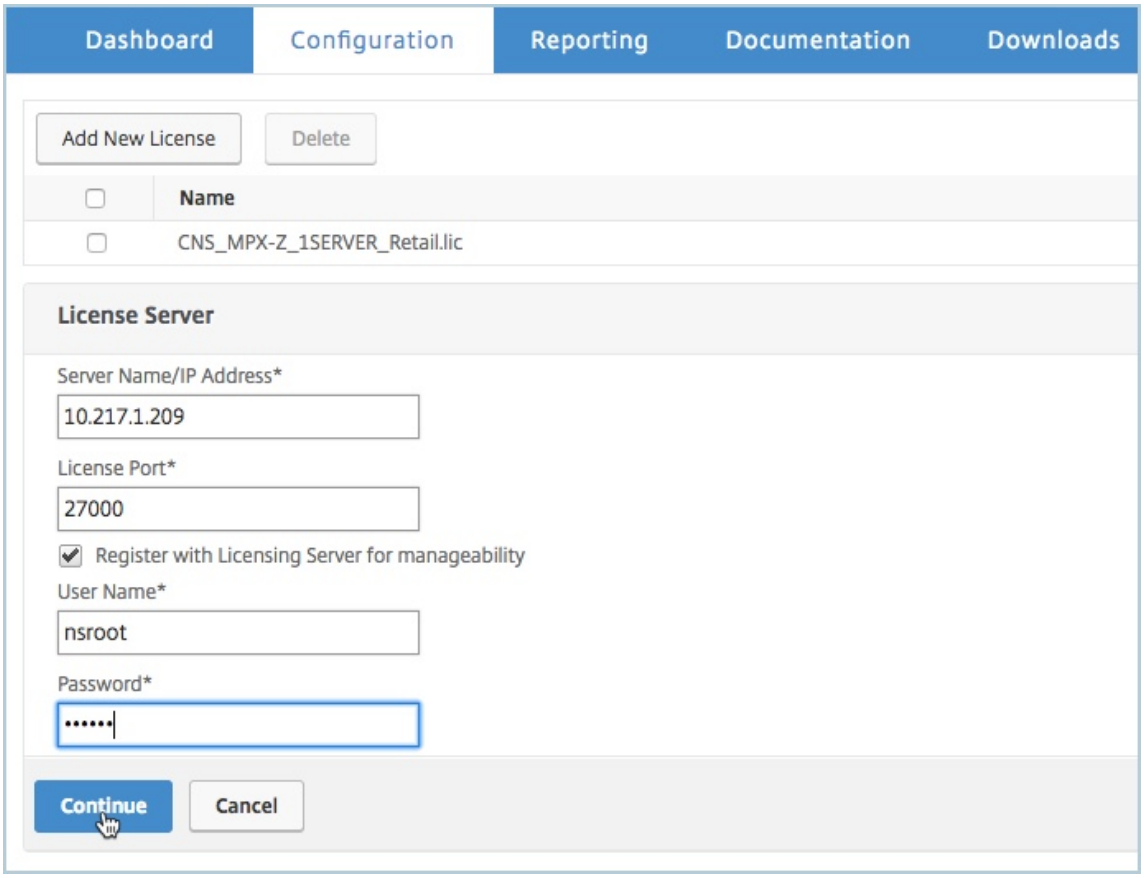
**Para actualizar una configuración de alta disponibilidad existente a la capacidad agrupada de NetScaler ADC:**

1. Inicie sesión en la instancia MPX de NetScaler ADC secundaria. En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida** , haga clic en la sección **Licencias** .




4. En la sección **Servidor de licencias**, haga lo siguiente:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




a) En el campo **Nombre del servidor/Dirección IP**, introduzca los detalles del servidor de licencias.

b) En el campo **Puerto de licencias**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

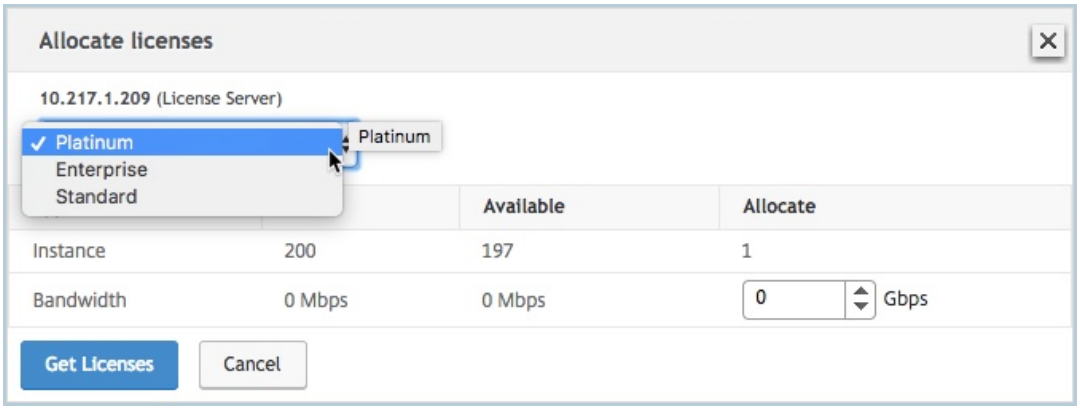
c) Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en el servidor de licencias para facilitar la administración** e introduzca las credenciales de ADM.

d) Haga clic en **Continuar**.

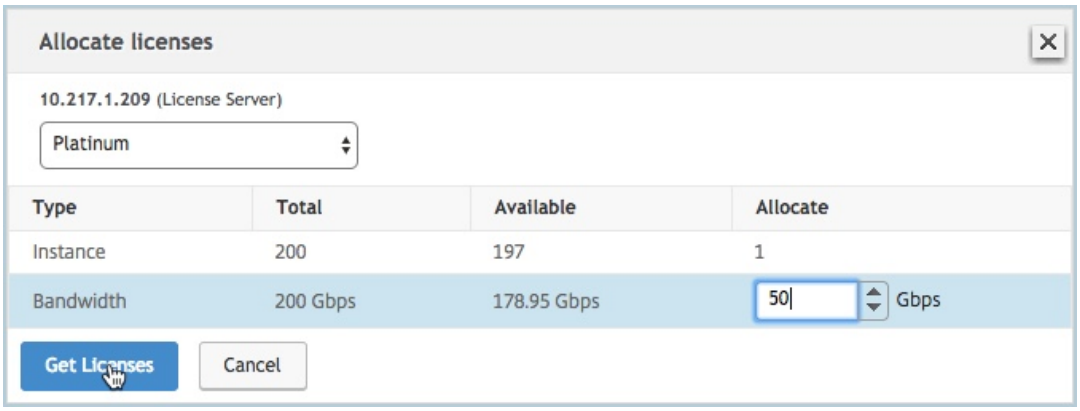
5. En la ventana **Asignar licencias**, haga lo siguiente:

   a) Seleccione la edición de licencia en la lista desplegable.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




b) Asigne el ancho de banda al dispositivo NetScaler ADC desde el menú **Asignar** y haga clic en **Obtener licencias**.




c) Cuando se le solicite, haga clic en **Reiniciar para reiniciar** el dispositivo. Una vez que el dispositivo esté en funcionamiento con la nueva licencia, fuerce una conmutación por error escribiendo `force ha failover`. Esta conmutación por error garantiza que el par de alta disponibilidad esté en buen estado.

6. Inicie sesión en el dispositivo NetScaler ADC MPX principal existente y reinicie el dispositivo. Lleve a cabo lo siguiente:

   a) En un explorador web, escriba la dirección IP del dispositivo NetScaler ADC, como http://192.168.100.1.

   b) En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.

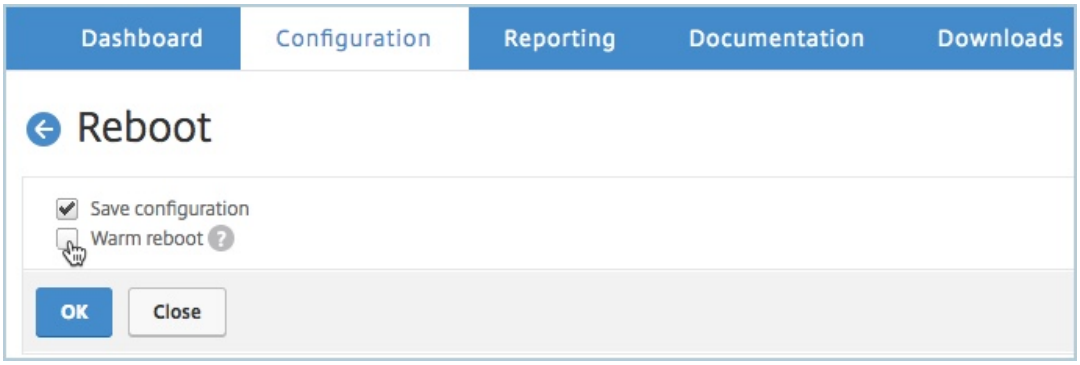
   c) En la página de **bienvenida**, haga clic en **Continuar**.

   d) En la ficha **Configuración**, haga clic en **Sistema**.

   e) En la página **Sistema**, haga clic en **Reiniciar**.

   f) En la página **Reiniciar**, seleccione **Reiniciar en caliente** y haga clic en **Aceptar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Una vez que se reinicie el dispositivo NetScaler ADC MPX principal, se convierte en el dispositivo NetScaler ADC MPX secundario en el par HA. Si quiere cambiar la instancia principal y secundaria del par de alta disponibilidad a la configuración del par de alta disponibilidad original, fuerce una conmutación por error. Ejecute el siguiente comando en cualquier instancia del par de alta disponibilidad:

```
> force ha failover
```

## Actualizar una licencia perpetua en un NetScaler ADC SDX a la capacidad agrupada de NetScaler ADC

January 30, 2024

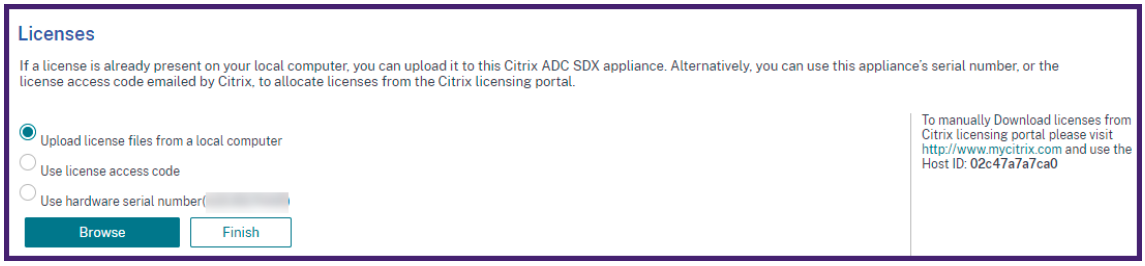
Un dispositivo NetScaler ADC SDX con licencia perpetua se puede actualizar a la licencia NetScaler ADC Pooled Capacity. La actualización a la licencia NetScaler ADC Pooled Capacity le permite asignar licencias del grupo de licencias a dispositivos NetScaler ADC bajo demanda. También puede configurar la licencia de capacidad agrupada de ADC para instancias de NetScaler ADC configuradas en modo de alta disponibilidad.

> **Nota**
>
> La conversión de una licencia perpetua a una licencia de capacidad agrupada es un proceso de autorización de licencia unidireccional. No puede revertir la licencia de capacidad agrupada a perpetua.
>
> **Importante**
>
> - Para actualizar el dispositivo SDX a la licencia NetScaler ADC Pooled Capacity, debe cargar la licencia SDX-Z en el dispositivo.
> - Asegúrese de tener el permiso para agregar instancias ADC en ADM.

**Para actualizar a la capacidad agrupada de NetScaler ADC:**

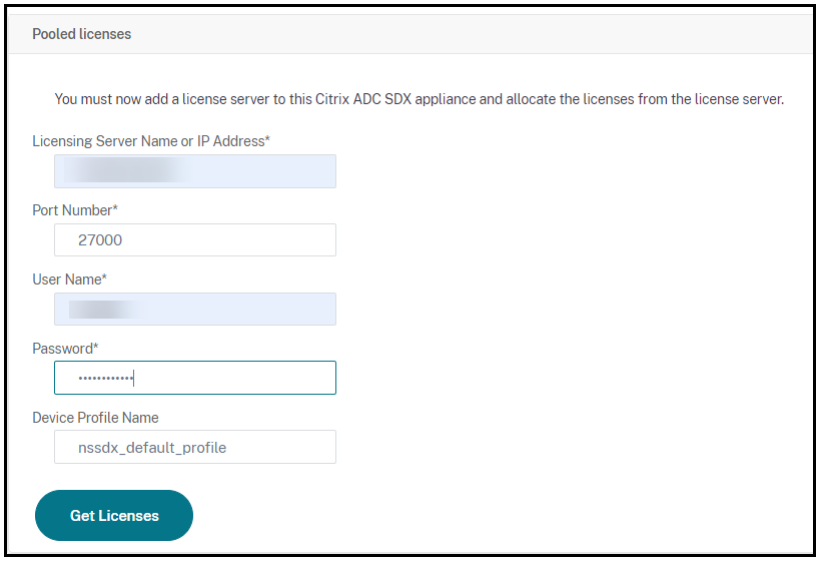
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En un explorador web, escriba la dirección IP del dispositivo SDX. Por ejemplo: http://192.168.100.1.
2. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de administrador.
3. En la página de **bienvenida**, haga clic en **Continuar**.
4. Cargue la licencia de capacidad cero. En la ficha Configuración, vaya a **Sistema** > **Licencias**.
5. En la página **Administrar licencias**, haga clic en **Agregar archivo de licencia**.
6. En la página **Licencias**, seleccione **Cargar archivos de licencia desde un equipo local** y haga clic en **Examinar** para seleccionar la licencia de capacidad cero del equipo local. A continuación, haga clic en **Finalizar**.




Una vez que la licencia de capacidad cero se aplica correctamente, la sección **Licencias agrupadas** aparece en la página **Licencias**.

7. En la sección **Licencias agrupadas**, haga lo siguiente:




   a) En el campo **Nombre del servidor de licencias o Dirección IP**, introduzca los detalles del servidor de licencias.

      Si quiere configurar el servidor ADM como un servidor de licencias, especifique la dirección IP del servidor ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

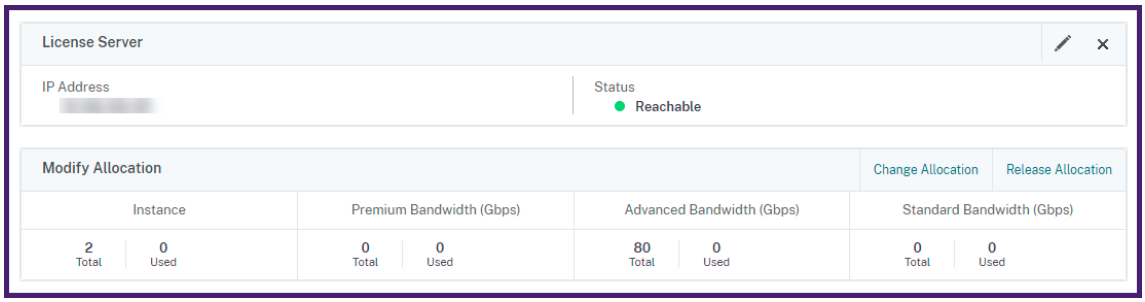
Si utiliza un agente para comunicarse con el servidor ADM, especifique la dirección IP del agente ADM.

b) En el campo **Número de puerto**, introduzca el puerto del servidor de licencias. Valor predeterminado: 27000.

c) Haga clic en **Obtener licencias**.

8. En la ventana **Asignar licencias**, especifique las instancias y el ancho de banda necesarios y haga clic en **Asignar**.

   En la página **Administrar licencias**, puede ver los detalles del servidor de licencias, la edición de licencias y las instancias asignadas y el ancho de banda desde el grupo.




> **Nota**
>
> La actualización de una licencia perpetua a capacidad agrupada no requiere reiniciar el dispositivo SDX.

## Capacidad agrupada de NetScaler ADC en instancias de NetScaler ADC en modo de clúster

January 30, 2024

Puede configurar la capacidad agrupada de NetScaler ADC en las instancias de NetScaler ADC configuradas como un clúster. Los siguientes son los requisitos previos para configurar la capacidad agrupada en instancias de NetScaler ADC en modo de clúster:

- Las instancias se ejecutan individualmente en modo de licencia de capacidad agrupada para formar el clúster.
- Todas las instancias deben ejecutarse con el mismo ancho de banda.
- Todas las instancias han extraído la capacidad agrupada desde el mismo NetScaler Application Delivery Management (ADM).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Las nuevas instancias no se pueden agregar a un clúster de NetScaler ADC existente a menos que su capacidad y las configuraciones de NetScaler ADM sean las mismas que las de las instancias existentes en el clúster.

Cualquier retirada de capacidad del clúster Citrix ADC asigna la misma capacidad a todos los nodos del clúster y el ancho de banda de salida = ancho de banda proporcionado * número de nodos.

Por ejemplo, si desactiva 50 Mbps de ancho de banda del clúster NetScaler ADC y el clúster incluye 12 instancias, cada instancia recibe automáticamente 50 Mbps. Y 600 Mbps es extraen de la agrupación.

> **Nota**
>
> Si una o más instancias del clúster dejan de responder, el clúster continúa procesando el tráfico con la capacidad de las instancias restantes.

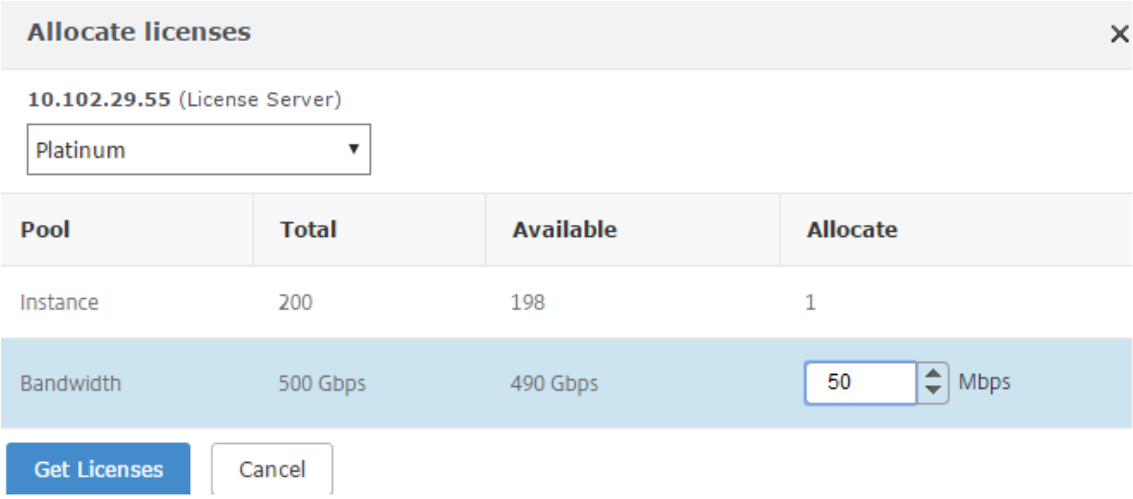
### Asigne la capacidad agrupada de ADC a un clúster de ADC

Asigne licencias a cada nodo del clúster por separado. Porque los comandos para propagar y sincronizar las licencias en los nodos del clúster están inhabilitados.

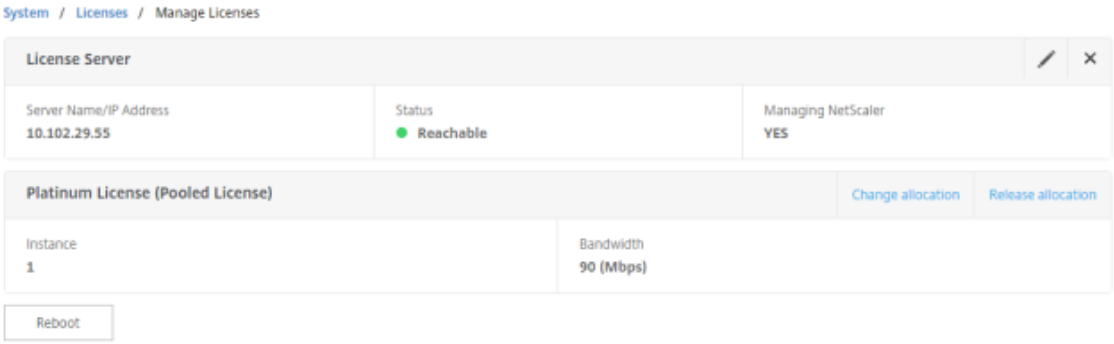
Repita el siguiente procedimiento en cada nodo del clúster:

1. En un explorador web, escriba la dirección IP (NSIP) de Citrix ADC. Por ejemplo: `http://192.168.100.1`.
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha **Configuración**, vaya a **Sistema > Licencias > Administrar licencias**, haga clic en **Agregar nueva licencia** y seleccione **Usar licencias agrupadas**.
4. Introduzca el nombre o la dirección del servidor de licencias en el campo **Nombre del servidor/Dirección IP**.
5. Si quiere administrar las licencias del grupo de instancias a través de Citrix ADM, seleccione la casilla **Registrarse en Citrix ADM para facilitar la administración** e introduzca las credenciales de ADM.
6. Seleccione la edición de licencia y el ancho de banda requerido y haga clic en **Obtener licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



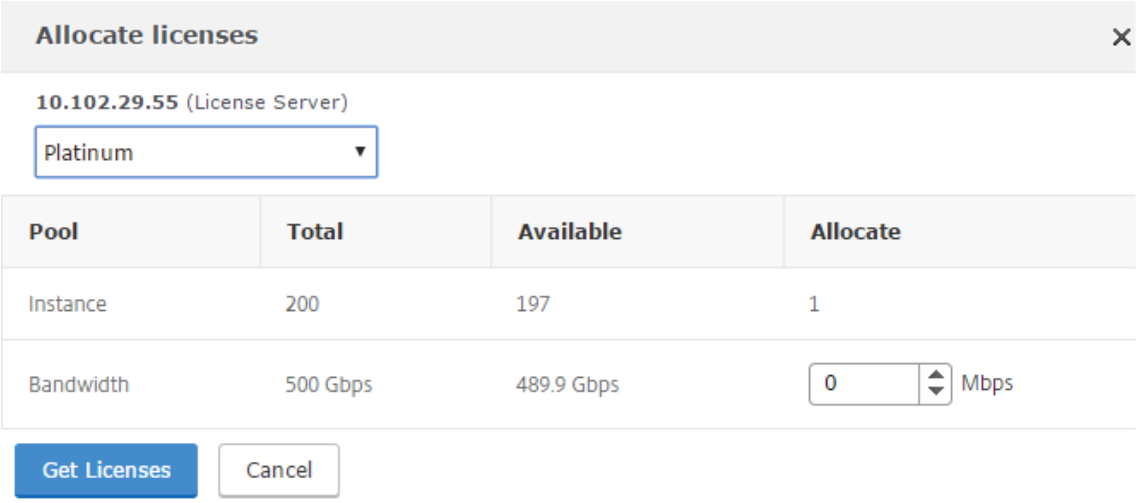

7. Puede cambiar o liberar la asignación de licencias seleccionando **Cambiar asignación** o **Liberar asignación**.




8. Si hace clic en **Cambiar asignación**, una ventana emergente muestra las licencias disponibles en el servidor de licencias.

> **Nota**
>
> La asignación de ancho de banda debe ser un múltiplo integral de la unidad de ancho de banda mínima del factor de forma correspondiente.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




9. Puede asignar ancho de banda o instancias a la instancia de Citrix ADC desde la lista desplegable **Asignar** . A continuación, haga clic en **Obtener licencias**.
10. Puede elegir la edición de licencia y el ancho de banda requerido en las listas desplegables de la ventana emergente.

> **Nota**
>
> No es necesario reiniciar si cambia la asignación de ancho de banda, pero es necesario reiniciar en caliente si cambia la edición de la licencia.

### Asigne la capacidad agrupada de ADC a un clúster de ADC mediante la CLI

Asigne licencias a cada nodo del clúster por separado. Porque los comandos para propagar y sincronizar las licencias en los nodos del clúster están inhabilitados.

Repita el siguiente procedimiento en cada nodo del clúster:

1. En un cliente SSH, introduzca la dirección IP de Citrix ADC (NSIP) e inicie sesión con las credenciales de administrador.
2. Para agregar un servidor de licencias, escriba el siguiente comando:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Para mostrar las licencias disponibles en el servidor de licencias, escriba el siguiente comando:

```
sh licenseserverpool
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
> sh licenseserverpool
        Instance Total                      : 0
        Instance Available                  : 0
        Standard Bandwidth Total            : 0 Mbps
        Standard Bandwidth Availabe         : 0 Mbps
        Enterprise Bandwidth Total          : 0 Mbps
        Enterprise Bandwidth Available      : 0 Mbps
        Platinum Bandwidth Total            : 0 Mbps
        Platinum Bandwidth Available        : 0 Mbps
        VPX25S Total                        : 1
        VPX25S Available                    : 1
        VPX200E Total                       : 1
        VPX200E Available                   : 1
        VPX1000S Total                      : 1
        VPX1000S Available                  : 1
        VPX8000E Total                      : 2
        VPX8000E Available                  : 1
 Done
```

4. Para asignar una licencia al dispositivo NetScaler ADC VPX, escriba el siguiente comando:

```
1  set capacity  – platform V[S/E/P][Bandwidth]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

## Supervisión de estado

January 30, 2024

El servidor de licencias supervisa continuamente el estado de la instancia habilitada para la capacidad agrupada de Citrix ADC. Las instancias se comunican mediante mensajes periódicos con el servidor de licencias. Si no se reciben algunos mensajes consecutivos, el servidor de licencias informa de que se ha perdido la conectividad.

Puede crear notificaciones personalizadas para complementar las alarmas predeterminadas.

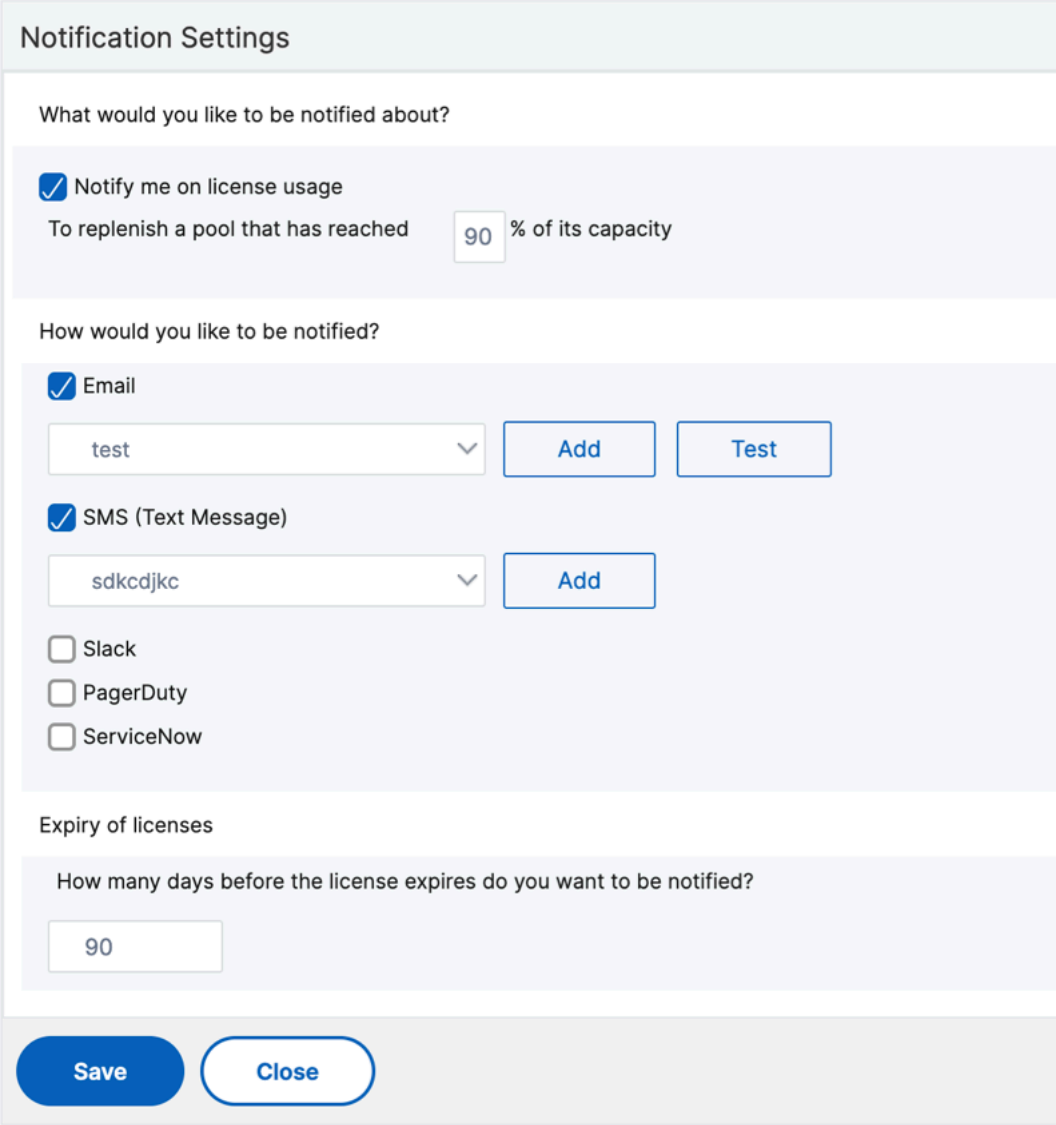
### Período de gracia

Cuando una instancia habilitada para la capacidad agrupada de Citrix ADC se encuentra en buen estado y el servidor de licencias deja de responder, la instancia sigue funcionando con la capacidad actual durante 30 días. Si la conectividad con el servidor de licencias no se restaura transcurridos 30 días, la instancia pierde su capacidad y deja de procesar el tráfico.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Notificaciones y alarmas

Las notificaciones se pueden habilitar desde Citrix Application Delivery Management (ADM) para cualquier acción realizada en la instancia. Además de la configuración de notificación personalizada, algunas alarmas están configuradas de forma predeterminada. Por ejemplo: para configurar una alarma para reponer un grupo que ha agotado un determinado porcentaje de su capacidad, vaya a **Infraestructura** > **Licencia** > Configuración > **Configuración** de **notificaciones** y haga clic en el botón de edición.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

# Comportamientos esperados cuando surgen problemas

January 30, 2024

Los siguientes son los comportamientos esperados de los servidores de licencias y las instancias de Citrix ADC cuando experimentan los problemas descritos:

## El servidor de licencias deja de responder

> **Advertencia**
>
> El servidor de licencias no responde. NetScaler ADC continúa operando con la capacidad actual durante 30 días. Después de 30 días, si no se restaura la conectividad con el servidor de licencias, NetScaler ADC pierde su capacidad actual y detiene el procesamiento del tráfico.

Si el servidor de licencias deja de responder, la instancia de NetScaler ADC entra en el período de gracia hasta que se restaure la conectividad.

## La instancia habilitada para capacidad agrupada de Citrix ADC deja de responder

Si la instancia habilitada para la capacidad agrupada de NetScaler ADC deja de responder y el servidor de licencias está en buen estado, el servidor de licencias comprueba todas las licencias de la instancia de NetScaler ADC después de 10 minutos. Cuando la instancia se reinicia, envía una solicitud para desproteger todas las licencias del servidor de licencias.

## Tanto el servidor de licencias como la instancia habilitada para la capacidad agrupada de NetScaler ADC dejan de responder

Si tanto el servidor de licencias como la instancia habilitada para capacidad agrupada de NetScaler ADC se reinician y restablecen la conexión, el servidor de licencias comprueba todas sus licencias después de 10 minutos, y las instancias habilitadas para capacidad agrupada de NetScaler ADC extraen automáticamente las licencias una vez finalizado el reinicio.

## La instancia habilitada para la capacidad agrupada de NetScaler ADC se cierra correctamente

Durante un cierre agraciado, puede optar por registrar las licencias o conservar las licencias asignadas antes del cierre agraciado. Si decide comprobar las licencias en, la instancia habilitada para capacidad agrupada de NetScaler ADC no tiene licencia después de reiniciarse. Si decide conservar las licencias, se registrarán en el servidor de licencias cuando se cierre la instancia. Una vez reiniciado la

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

instancia, restablece la conexión con el servidor de licencias y retira las licencias tal como se especifica en la configuración guardada.

Si el sistema se reinicia y la retirada falla debido a que no hay capacidad disponible en el grupo, NetScaler ADC comprueba el inventario de las licencias de grupo de NetScaler Application Delivery Management (ADM) y comprueba cualquier capacidad disponible. Se genera una alarma SNMP para notificar esta condición al usuario si el NetScaler ADC no se ejecuta con plena capacidad según la configuración. Si no hay capacidad disponible en el grupo de ancho de banda, la instancia habilitada para capacidad de agrupación quedará sin licencia.

### La red pierde conectividad

> **Mensaje de error (syslog)**
>
> El servidor de licencias no responde.

Si el servidor de licencias y las instancias habilitadas para la capacidad agrupada de NetScaler ADC están en estado correcto, pero la conectividad de red se pierde, las instancias seguirán funcionando con su capacidad actual durante 30 días. Transcurridos 30 días, si no se restablece la conectividad con el servidor de licencias, las instancias pierden su capacidad y dejan de procesar el tráfico, y el servidor de licencias registra todas sus licencias. Después de que el servidor de licencias restablece la conectividad con las instancias de NetScaler ADC, las instancias vuelven a desproteger las licencias.

## Configurar comprobaciones de caducidad para licencias de capacidad agrupadas

January 30, 2024

Ahora puede configurar el umbral de caducidad de las licencias de capacidad agrupada de NetScaler ADC. Al establecer los umbrales, Citrix Application Delivery Management (ADM) envía notificaciones por correo electrónico o SMS cuando una licencia está a punto de caducar. Una captura SNMP y una notificación también se envían cuando la licencia ha expirado en NetScaler ADM.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler ADM.

**Para configurar comprobaciones de caducidad de licencias:**

1. Vaya a **Redes** > **Licencias** .
2. En la página de **configuración de licencias**, en la sección**Información sobre la caducidad de la licencia**, encontrará los detalles de las licencias que van a caducar:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Función**: Tipo de licencia que va a caducar.
- **Recuento**: número de servidores o instancias virtuales que se verán afectados.
- **Días para caducar**: Número de días antes de la expiración de la licencia.

3. En la sección **Configuración de notificaciones** , haga clic en el icono **Editar** y especifique el umbral de alerta. Puede establecer un porcentaje de la capacidad de licencias agrupadas que se utilizará para notificar a los administradores.
4. Seleccione el tipo de notificación que quiere enviar marcando la casilla correspondiente. Los tipos de notificación son los siguientes:
   a) **Perfil de correo electrónico**: especifique un servidor de correo y los detalles del perfil. Se activa un correo electrónico cuando las licencias están a punto de caducar.
   b) **Perfil SMS**: especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando las licencias están a punto de caducar.
5. A continuación, especifique cuándo quiere enviar la notificación en términos de número de días antes de la caducidad de la licencia.
6. Haga clic en **Guardar**.

> **Nota**
>
> Cuando agrega nuevas licencias al grupo, las instancias NetScaler ADC utilizan las nuevas licencias al vencimiento de sus licencias existentes.

## Registre y desproteja las licencias de NetScaler ADC VPX y BLX

January 30, 2024

Puede asignar licencias VPX y BLX a instancias de NetScaler ADC a petición desde NetScaler Application Delivery Management (ADM). El software ADM almacena y administra las licencias, que tienen un marco de licencias que proporciona un aprovisionamiento de licencias escalable y automatizado. Una instancia puede retirar la licencia de NetScaler ADM cuando se aprovisiona. Cuando se quita o destruye una instancia, la instancia vuelve a comprobar su licencia en el software NetScaler ADM.

### Requisitos previos

Asegúrese de que se cumplen los siguientes requisitos previos:

- Está mediante una imagen de NetScaler ADC VPX que ejecuta la versión 12.0 del software. Por ejemplo: NSVPX-ESX-12.0-xx.xx_nc.zip

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Ha instalado Citrix ADM con la versión 12.0.
  Por ejemplo: MAS-ESX-12.0-xx.xx.zip

> **Nota**
>
> Para administrar las licencias VPX existentes mediante Citrix ADM, debe volver a alojar las licencias en Citrix ADM.

## Instalación de licencias en Citrix ADM

> **Nota**
>
> Antes de instalar las licencias, reinicie el dispositivo virtual Citrix ADM si ha cambiado la edición del software o el ancho de banda.

**Para instalar archivos de licencia en NetScaler ADM:**

1. En un explorador web, escriba la dirección IP del Citrix ADM (por ejemplo, http://192.168.100.1).
2. En Nombre de usuario y Contraseña, introduzca las credenciales de administrador.
3. Vaya a **Redes** > **Licencias** .
4. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:
   - **Cargar archivos de licencias desde un equipo**local : si ya hay un archivo de licencias en su equipo local, puede cargarlo en Citrix ADM.
     Para agregar archivos de licencia, haga clic en **Examinar** y seleccione el archivo de licencia (.lic) que quiera agregar. Luego haga clic en **Finalizar**.
   - **Usar código de acceso de licencia**: Citrix envía por correo electrónico el código de acceso a la licencia de las licencias que adquiera.
     Para agregar archivos de licencias, introduzca el código de acceso a la licencia en el cuadro de texto y, a continuación, haga clic en **Obtener licencias**.

   > **Nota**
   >
   > Asegúrese de estar conectado a Internet antes de utilizar el código de acceso de licencia para instalar las licencias.

   En cualquier momento, puede agregar más licencias a NetScaler ADM desde la Configuración de licencias.

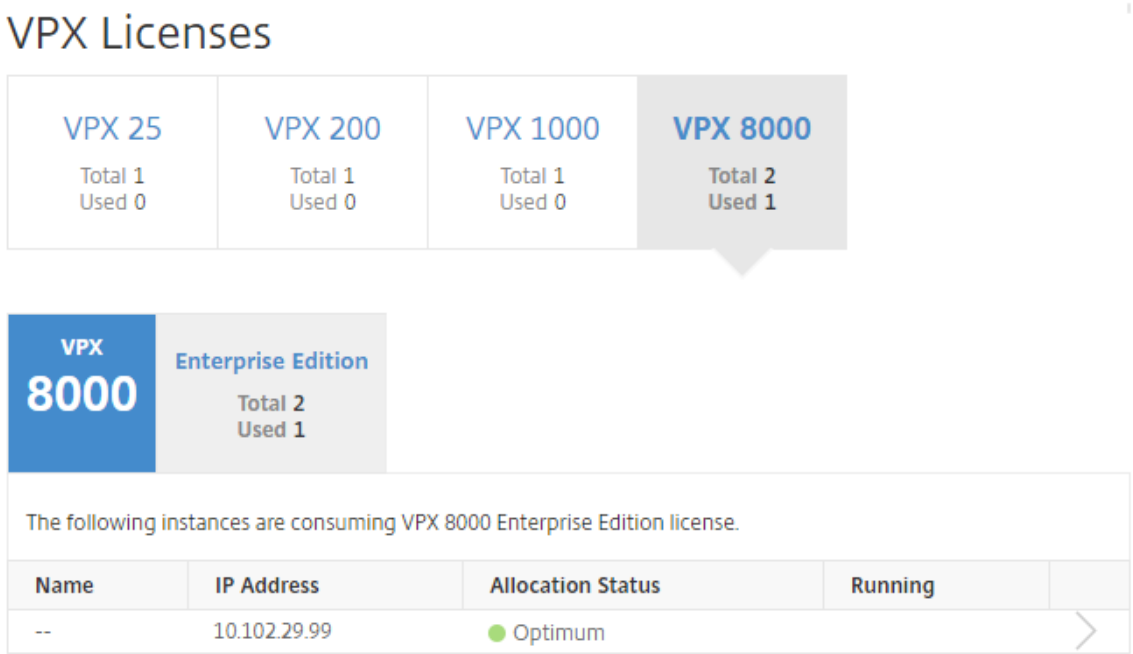
## Verificación

Puede ver las licencias disponibles y asignadas en la GUI de Citrix ADM.

**Para mostrar las licencias:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En un explorador web, escriba la dirección IP de NetScaler ADM (por ejemplo,http://192.168.100.1).
2. En **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la ficha Configuración, vaya a **Redes**> **Licencias > Licencias > LicenciasVPX.**

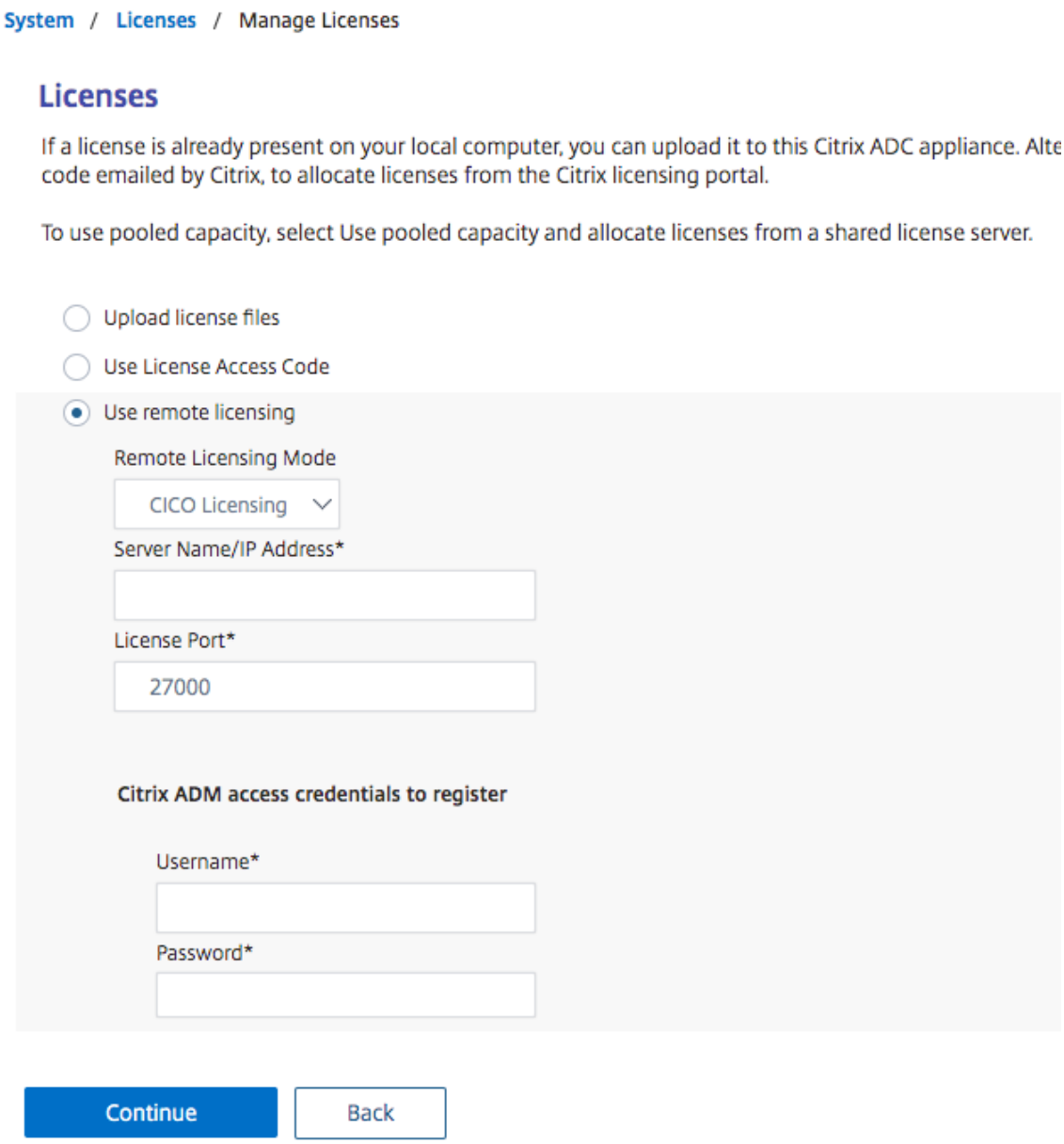



4. Puede ver las licencias asignadas en la tabla de la sección de licencias disponibles.

### Asignar licencias VPX y BLX a una instancia de ADC mediante la GUI de NetScaler ADC

1. En un explorador web, escriba la dirección IP de la instancia de NetScaler ADC (por ejemplo, http://192.168.100.1).
2. En los campos **Nombre de usuario** y **Contraseña**, introduzca las credenciales de administrador.
3. En la pestaña Configuración, vaya a **Sistema > Licencias > Administrar licencias** , haga clic en **Agregar nueva licencia** y seleccione **Usar licencias remotas > Licencias CICO** .
4. Introduzca los detalles del servidor de licencias en el **campo Nombre del servidor/dirección IP**.
5. En los campos **Nombre** de usuario y **Contraseña** de la pantalla anterior, introduzca las credenciales de Citrix ADM y haga clic en **Continuar**.

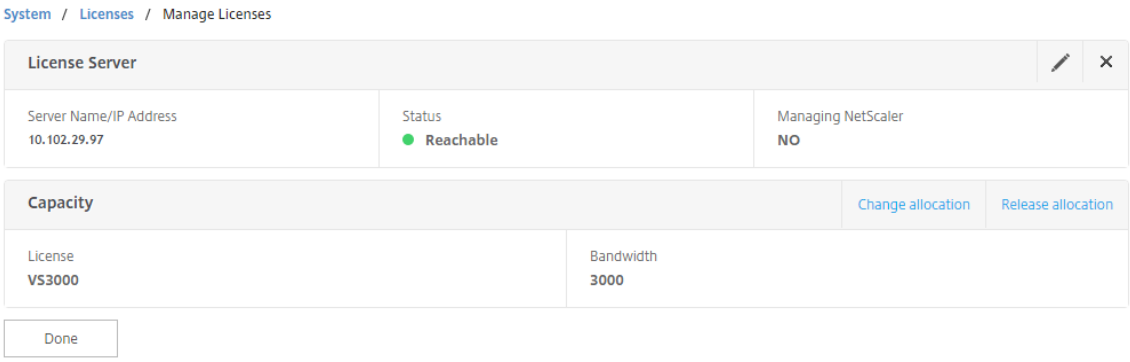
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




6. Seleccione la edición de licencia con el ancho de banda requerido, haga clic en **Obtener licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

7. Haga clic en **Reiniciar**, la instancia de NetScaler ADC se reiniciará.
8. Para cambiar o liberar la asignación de licencias, vaya a **Sistema** > **Licencias** > **Administrar licencias** y seleccione **Cambiar asignación** o **Liberar asignación.**




9. Si hace clic en **Cambiar asignación**, una ventana emergente muestra las licencias disponibles en el servidor de licencias. Seleccione la licencia requerida, haga clic en **Obtener licencias**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Asignar licencias VPX y BLX a una instancia de ADC mediante la CLI de NetScaler ADC

1. En un cliente SSH, introduzca la dirección IP de la instancia de NetScaler ADC e inicie sesión mediante credenciales de administrador.
2. Para agregar un servidor de licencias, escriba el siguiente comando:

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. Para mostrar las licencias disponibles en el servidor de licencias, escriba el siguiente comando:

```
sh licenseserverpool
```

```
> sh licenseserverpool
        Instance Total                    : 0
        Instance Available                : 0
        Standard Bandwidth Total          : 0 Mbps
        Standard Bandwidth Availabe       : 0 Mbps
        Enterprise Bandwidth Total        : 0 Mbps
        Enterprise Bandwidth Available    : 0 Mbps
        Platinum Bandwidth Total          : 0 Mbps
        Platinum Bandwidth Available      : 0 Mbps
        VPX25S Total                      : 1
        VPX25S Available                  : 1
        VPX200E Total                     : 1
        VPX200E Available                 : 1
        VPX1000S Total                    : 1
        VPX1000S Available                : 1
        VPX8000E Total                    : 2
        VPX8000E Available                : 1
 Done
```

4. Para asignar una licencia al dispositivo NetScaler ADC, introduzca el siguiente comando:

```
set capacity -platform V[S/E/P][Bandwidth]
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

### Asignar licencias VPX y BLX a una instancia de ADC mediante la API

En un explorador web o un cliente de API, inicie sesión en la instancia de NetScaler ADC con las credenciales de administrador.

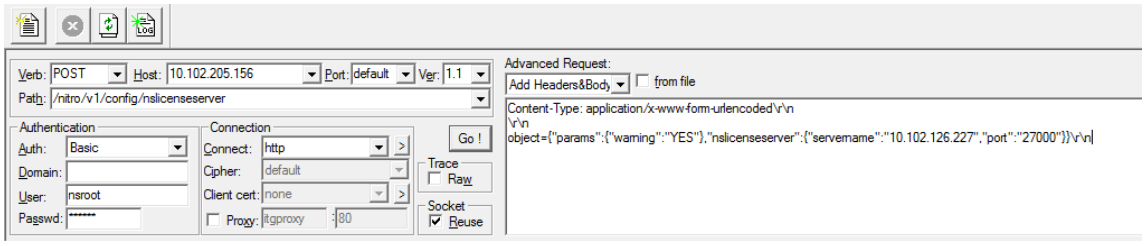
**Para agregar un servidor de licencias:**

1. Establezca el tipo de solicitud en **Publicar**.
2. Establezca la ruta en /nitro/v1/config/nslicensingserver.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Establezca la carga útil de la siguiente manera:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  " params " ;{
 warning " : " yes "  }
 , " nslicensing server " ;{
 servername " : " <Citrix ADM IP> " ,  " port " : " 27000 "  }
  }
 \r\n
```

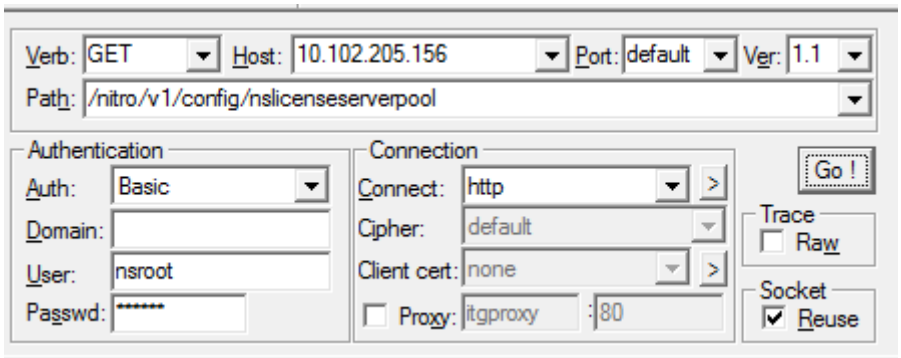



NetScaler ADM responde a la solicitud. La siguiente respuesta muestra éxito.

```
RESPONSE: **************\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

**Para ver las licencias disponibles en el servidor de licencias:**

1. Defina el tipo de solicitud en **Get**.
2. Establezca la ruta en /nitro/v1/config/nslicenseserverpool




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

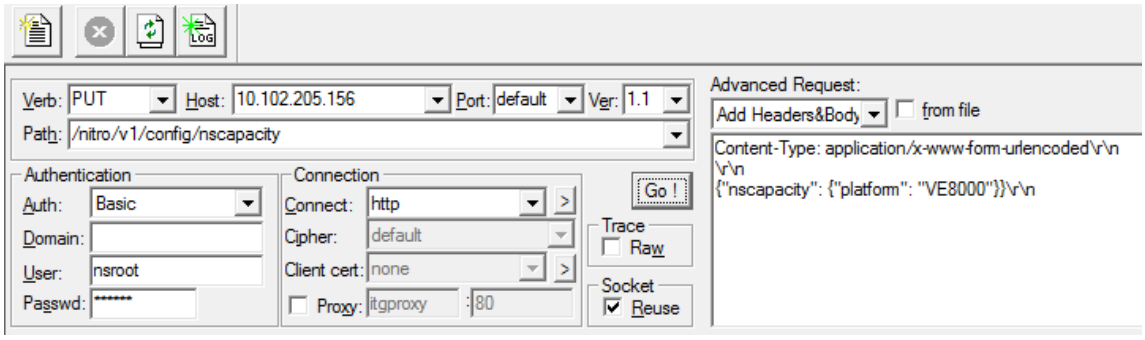
NetScaler ADM responde a la solicitud. La respuesta de ejemplo siguiente muestra el éxito y la lista de licencias disponibles en el servidor de licencias.


```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.
```


**Para asignar una licencia al dispositivo NetScaler ADC:**

1. Establezca el tipo de solicitud en **Publicar**.
2. Establezca la ruta en /nitro/v1/config/nscapacity.
3. Establezca la carga útil de la siguiente manera:

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  " nscapacity:{
  " platform " : " VE8000 "  }
   }
 \r\n
```




NetScaler ADM responde a la solicitud. La siguiente respuesta muestra éxito.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
RESPONSE: **************\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:16:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

## Actualizar una dirección IP del servidor de licencias

Puede actualizar la dirección IP del servidor de licencias en las instancias VPX y BLX, sin ningún impacto en el ancho de banda de licencias asignado en la instancia y la pérdida de datos.

**Actualización mediante la CLI**: para actualizar la dirección IP del servidor de licencias mediante la CLI, escriba el siguiente comando en la instancia:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Este comando se conecta al nuevo servidor y libera los recursos asociados con el servidor de licencias anterior.

**Actualización mediante la GUI**: Para actualizar la dirección IP del servidor de licencias mediante la GUI, vaya a **Sistema > Licencias > Administrar licencias**, haga clic en **Agregar nueva licencia**. Para obtener más información, consulte Asignar licencias VPX y BLX a una instancia de ADC mediante la GUI de NetScaler ADC.

## Configurar comprobaciones de caducidad para licencias de registro y salida de NetScaler ADC VPX y BLX

Ahora puede configurar el umbral de caducidad de licencias para las licencias de NetScaler ADC VPX y BLX. Al establecer umbrales, NetScaler ADM envía notificaciones por correo electrónico o SMS cuando una licencia caduca. También se envían una captura SNMP y una notificación cuando la licencia ha caducado en NetScaler ADM.

Se genera un evento cuando se envía una notificación de caducidad de licencia y este evento se puede ver en NetScaler ADM.

**Para configurar comprobaciones de caducidad de licencias:**

1. Vaya a **Redes** > **Licencias** .

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página de **configuración** de la **licencia, en la sección Información de caducidad** de la licencia, puede encontrar los detalles de las licencias que van a caducar:
   - **Función**: Tipo de licencia que va a caducar.
   - **Recuento**: número de servidores virtuales o instancias afectadas.
   - **Días para caducar**: Número de días antes de la expiración de la licencia.
3. En la sección**Configuración de notificaciones**, haga clic en el icono**Modificar** y especifique el umbral de alerta. Puede establecer un porcentaje de la capacidad de licencias agrupadas que se utilizará para notificar a los administradores.
4. Seleccione el tipo de notificación que quiere enviar marcando la casilla correspondiente. Los tipos de notificación son los siguientes:
   a) **Perfil de correo electrónico**: especifique un servidor de correo y los detalles del perfil. Se activa un correo electrónico cuando las licencias están a punto de caducar.
   b) **Perfil SMS**: especifique un servidor del servicio de mensajes cortos (SMS) y los detalles del perfil. Se activa un mensaje SMS cuando las licencias están a punto de caducar.
5. A continuación, especifique cuándo quiere enviar la notificación en términos de número de días antes de la caducidad de la licencia.
6. Haga clic en **Guardar**.

## Licencias de CPU virtual NetScaler ADC

January 30, 2024

Los administradores de centros de datos como usted están adoptando tecnologías más nuevas que simplifican las funciones de la red y ofrecen costes más bajos y una mayor escalabilidad. La arquitectura de centro de datos más reciente debe incluir, como mínimo, las siguientes funciones:

- Redes definidas por software (SDN)
- Virtualización de funciones de red (NFV)
- Virtualización de red (NV)
- Microservicios

Este movimiento también necesita que los requisitos de software sean dinámicos, flexibles y ágiles para satisfacer las necesidades empresariales en constante cambio. También se espera que las licencias sean administradas por una herramienta de administración central con plena visibilidad del uso.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Licencias de CPU virtuales para NetScaler ADC VPX

Anteriormente, las licencias de NetScaler ADC VPX se asignaban en función del consumo de ancho de banda de las instancias. Un NetScaler ADC VPX está restringido a usar un ancho de banda específico y otras métricas de rendimiento según la edición de licencia a la que está vinculado. Para aumentar el ancho de banda disponible, debe actualizar a una edición de licencia que proporcione más ancho de banda. En ciertos casos, el requisito de ancho de banda puede ser menor, pero el requisito es más para otro rendimiento de L7, como SSL TPS, rendimiento de compresión, etc. Es posible que la actualización de la licencia NetScaler ADC VPX no sea adecuada en estos casos. Pero es posible que tenga que comprar una licencia con gran ancho de banda para desbloquear los recursos del sistema necesarios para el procesamiento intensivo de la CPU. NetScaler ADM ahora admite la asignación de licencias a la instancia de NetScaler ADC en función de los requisitos de la CPU virtual.

En la función de licencia basada en el uso de CPU virtual, la licencia especifica el número de CPU a las que tiene derecho un NetScaler ADC VPX determinado. Por lo tanto, NetScaler ADC VPX puede desproteger licencias solo para el número de CPU virtuales que se ejecutan en él desde el servidor de licencias. NetScaler ADC VPX extrae licencias en función del número de CPU que se ejecutan en el sistema. NetScaler ADC VPX no considera las CPU inactivas al retirar las licencias.

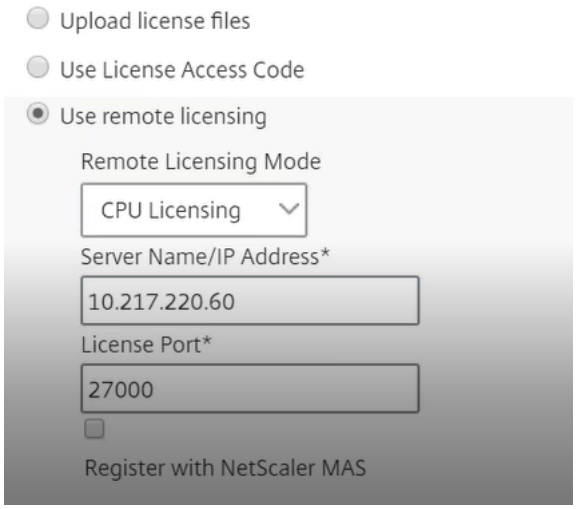
Al igual que la capacidad de licencias agrupadas y las funcionalidades de licencias CICO, el servidor de licencias NetScaler ADM administra un conjunto independiente de licencias de CPU virtuales. También en este caso, las tres ediciones gestionadas para las licencias de CPU virtuales son Standard, Advanced y Premium. Estas ediciones desbloquean el mismo conjunto de funciones que las desbloqueadas por las ediciones para licencias de ancho de banda.

Es posible que se produzca un cambio en la cantidad de CPU virtuales o que se produzca un cambio en la edición de la licencia. En tal caso, siempre debe cerrar la instancia antes de iniciar una solicitud de un nuevo conjunto de licencias. Reinicie NetScaler ADC VPX después de retirar las licencias.

**Para configurar el servidor de licencias en NetScaler ADC VPX mediante GUI:**

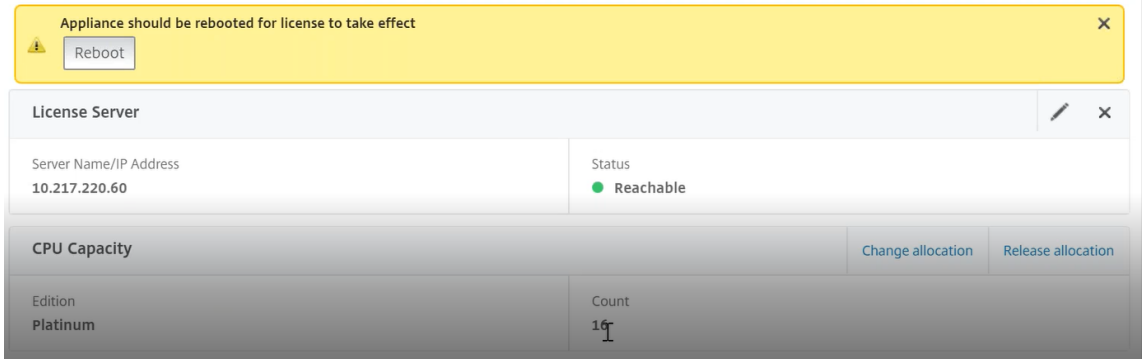
1. En NetScaler ADC VPX, vaya a **Sistema** > **Licencias** y haga clic en **Administrar licencias**.
2. En la página **Licencia**, haga clic en **Agregar nueva licencia**.
3. En la página **Licencias**, seleccione la opción **Usar licencias remotas**.
4. Seleccione las **licencias de CPU** en la lista **de modos de licencia remota**.
5. Escriba la dirección IP del servidor de licencias y el número de puerto.
6. Haga clic en **Continuar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




> **Nota:**
>
> Siempre debe registrar la instancia de NetScaler ADC VPX en NetScaler ADM. Si aún no lo ha hecho, habilite **Registrarse con NetScaler ADM** y escriba las credenciales de inicio de sesión de NetScaler ADM.

7. En la ventana **Asignar licencias**, seleccione el tipo de licencia. La ventana muestra el total de las CPU virtuales disponibles y también las CPU que se pueden asignar. Haga clic en **Obtener licencias**.
8. Haga clic en **Reiniciar** en la página siguiente para solicitar las licencias.




> **Nota**También
>
> puede liberar la licencia actual y salir de una edición diferente. Por ejemplo, ya está ejecutando una licencia de edición estándar en su instancia. Puede liberar esa licencia y luego echar un vistazo a la edición avanzada.

## Configuración del servidor de licencias en la licencia NetScaler ADC VPX mediante CLI

En la consola NetScaler ADC VPX, escriba los siguientes comandos para las dos tareas siguientes:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Para agregar el servidor de licencias al NetScaler ADC VPX:

```
add licenseserver <IP address of the license server>
```

2. Para solicitar las licencias:

```
set capacity -vcpu - edition premium
```

Cuando se le solicite, reinicie la instancia escribiendo el siguiente comando:

```
reboot -w
```

### Actualizar una dirección IP del servidor de licencias

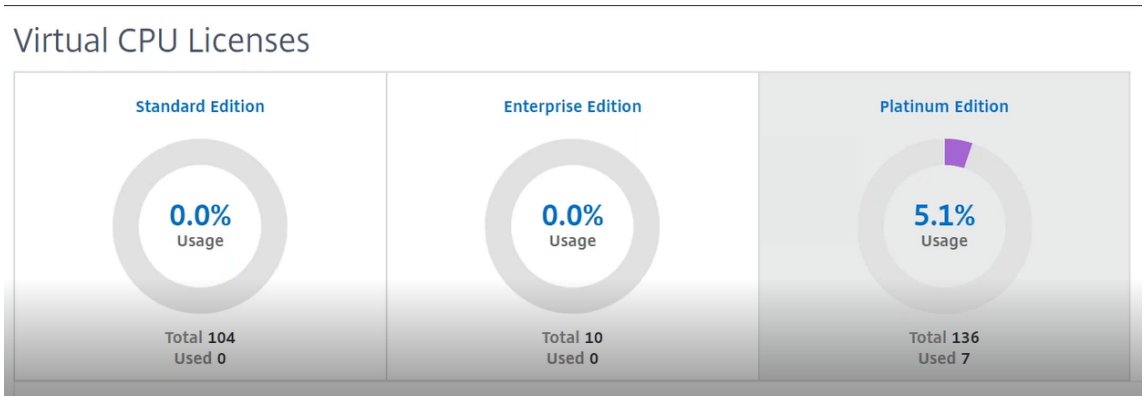
Puede actualizar la dirección IP del servidor de licencias en la instancia VPX sin que ello afecte al ancho de banda de licencias asignado a la instancia ni a la pérdida de datos. Para actualizar la dirección IP del servidor de licencias, escriba el siguiente comando en la instancia VPX:

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

Este comando se conecta al nuevo servidor y libera los recursos asociados con el servidor de licencias anterior.

## Administración de licencias de CPU virtual en NetScaler ADM

1. En Citrix ADM, vaya a **Redes** > **Licencias** > Licencias de **CPU virtuales** .
2. La página muestra las licencias asignadas para cada tipo de edición de licencia.
3. Haga clic en el número que aparece dentro de cada anillo para ver las instancias de NetScaler ADC que utilizan esta licencia.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Licencias de CPU virtual para NetScaler ADC CPX

Al aprovisionar la instancia CPX de NetScaler ADC, puede configurar la instancia CPX de NetScaler ADC para que extraiga las licencias del servidor de licencias en función del uso de la CPU de la instancia.

NetScaler ADC CPX depende del servidor de licencias, que se ejecuta en NetScaler ADM, para administrar las licencias. NetScaler ADC CPX extrae las licencias del servidor de licencias cuando se inicia. Las licencias se archivan de nuevo en el servidor de licencias cuando se cierra el NetScaler ADC CPX.

Puede descargar NetScaler ADC CPX desde Docker App Store. En el host Docker, para descargar NetScaler ADC CPX, ejecute el siguiente comando:

```
docker pull store/citrix/netscalercpx: [version]
```

Existen tres tipos de licencia disponibles para las licencias CPX:

1. Licencias de suscripción de CPU virtual compatibles con CPX y VPX
2. Licencias de capacidad agrupada
3. Licencias CP1000 que admiten vCPU de una a varias vCPU para CPX solamente

**Para configurar licencias de suscripción de vCPU al Provisioning la instancia CPX de NetScaler ADC:**

Especifique la cantidad de licencias de vCPU que utiliza la instancia CPX de NetScaler ADC.

- Este valor se introduce como una variable de entorno a través de Docker, Kubernetes o Mesos/-Marathon.
- La variable de destino es “CPX_CORES”. El CPX puede admitir de 1 a 16 núcleos.

Para especificar 2 núcleos, puede ejecutar el comando docker run de la siguiente manera:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
```

Al aprovisionar una instancia de Citrix ADC CPX, defina el servidor de licencias Citrix ADC como una variable de entorno en el comando **docker run** , como se muestra a continuación:

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> cpx:11.1
```

Donde:

- < LS_IP_ADDRESS >*es la dirección IP del servidor de* licencias de NetScaler ADC.
- <*LS_PORT*> es el puerto del servidor de licencias NetScaler ADC. De forma predeterminada, el puerto es 27000.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**De forma
>
> predeterminada, la instancia de NetScaler ADC CPX extrae la licencia del grupo de suscripciones de vCPU. La instancia de CPX extrae un número “n”de licencias si la instancia se ejecuta con “n” CPU.

**Para configurar las licencias de NetScaler ADC Pooled Capacity o CP1000 al Provisioning la instancia de NetScaler ADC CPX:**

Si desea obtener las licencias de la instancia de CPX mediante las licencias agrupadas (basadas en el ancho de banda) o el grupo privado de CPX (CP1000 o basadas en un grupo privado), debe proporcionar las variables de entorno correspondientes.

Por ejemplo,

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e PLATFORM=CP1000 cpx:11.1
```

**CP1000**. Este comando desencadena la extracción desde el grupo CP1000 (grupo privado CPX). A continuación, la instancia CPX de Citrix ADC recupera el número «n» de instancias para el número «n» de núcleos especificado para CPX_CORES. El caso de uso más común es especificar n = 1 para una extracción de una sola instancia. En los casos de uso de CPX multinúcleo, se excluyen las CPU virtuales “n”(donde “n”va del 1 al 7).

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
```

**Capacidad agrupada**. Este comando extrae una licencia del grupo de instancias y consume 1000 Mbps de ancho de banda del grupo de ancho de banda Premium, pero permite que CPX funcione hasta 2000 Mbps.En Pooled Licensing, los primeros 1000 Mbps no se cobran.

> **Nota:**
>
> Especifique el número correspondiente de vCPU para el ancho de banda objetivo deseado al retirar el grupo de ancho de banda, tal como se detalla en la siguiente tabla:

| Número de núcleos (vCPU) | Ancho de banda máximo |
|---|---|
| 1 | 1000 Mbps |
| 2 | 2000 Mbps |
| 3 | 3500 Mbps |
| 4 | 5000 Mbps |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | |
|---|---|
| 5 | 6500 Mbps |
| 6 | 8000 Mbps |
| 7 | 9300 Mbps |

## Administrar instancias de Citrix SD-WAN

January 30, 2024

Citrix ADM le permite supervisar, administrar y ver los análisis de los dispositivos Citrix SD-WAN de su red. La siguiente tabla de interoperabilidad proporciona información sobre las funciones de Citrix ADM que se admiten actualmente en cada una de las ediciones de la plataforma Citrix SD-WAN.

### Matriz de interoperabilidad de las ediciones de la plataforma Citrix SD-WAN de Citrix y funciones de NetScaler ADM

| Modificación de plataforma | Detección | Configuración | Supervisión | Informes (informes de red) | Gestión de eventos | HDX Insight | WAN Insight |
|---|---|---|---|---|---|---|---|
| Citrix SD-WAN WANOP | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Citrix SD-WAN SE | Sí | No | No | No | No | No | No |
| Citrix SD-WAN PE | Sí | No | No | No | No | Sí | No |

### Versiones de Citrix SD-WAN compatibles con Citrix ADM

| Modificación de plataforma | Versión Citrix SD-WAN | Versión Citrix ADM |
|---|---|---|
| Citrix SD-WAN WANOP | Citrix CloudBridge 7.4 y versiones posteriores | Citrix ADM 11.0 y versiones posteriores |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Modificación de plataforma | Versión Citrix SD-WAN | Versión Citrix ADM |
|---|---|---|
| Citrix SD-WAN SE | Citrix SD-WAN 9.3.0 y posterior | NetScaler ADM 12.0.53.8 y posterior |
| Citrix SD-WAN PE | Citrix SD-WAN 9.3.0 y posterior | NetScaler ADM 12.0.53.8 y posterior |

Puede agregar un dispositivo Citrix SD-WAN WANOP como instancia administrada en NetScaler ADM. Para obtener más información, consulte Agregar instancias a NetScaler ADM. Puede ver la información WAN, HDX, los informes de red y los informes de eventos para las instancias de Citrix SD-WAN WANOP.

NetScaler ADM permite que los dispositivos Citrix SD-WAN Standard Edition (SE) y Enterprise Edition (EE) se registren como instancias administradas en NetScaler ADM.

Para agregar un dispositivo Citrix SD-WAN SE/PE/AE a NetScaler ADM, configure NetScaler ADM como un recopilador AppFlow en los dispositivos Citrix SD-WAN SE/PE/AE. El dispositivo Citrix SD-WAN SE/PE/AE se agrega como instancia administrada en NetScaler ADM. El dispositivo SD-WAN SE/PE/AE envía los datos de análisis a NetScaler ADM.

Puede configurar NetScaler ADM como un recopilador AppFlow en cada dispositivo SD-WAN SE/PE/AE individualmente, o utilizar Citrix SD-WAN Center para exportar la configuración a los dispositivos administrados.

Para obtener más información, consulte Agregar instancias de Citrix SD-WAN SE/PE/AE en NetScaler ADM.

Para un dispositivo Citrix SD-WAN PE, puede ver registros de datos HDX o datos de varios saltos, dependiendo de la configuración de AppFlow. Un dispositivo Citrix SD-WAN SE proporciona solo datos de salto múltiple. Para obtener más información, consulte Visualización de informes y métricas de HDX Insight y Visualización de datos de análisis para la implementación de varios saltos.

Esta página proporciona vínculos de acceso rápido a los temas a los que puede hacer referencia para configurar NetScaler ADM y administrar los dispositivos WANOP SD-WAN mediante NetScaler ADM.

## Descripción general de Citrix ADM

Acerca de Citrix ADM

Architecture

Cómo descubre Citrix ADM las instancias

Cómo se comunica Citrix ADM con las instancias administradas

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Implementación de Citrix ADM

Implemente Citrix ADM con Citrix Hypervisor

Implementación de NetScaler ADM con Microsoft Hyper-V

Implemente Citrix ADM con VMware ESXi

Implementación de NetScaler ADM con Linux KVM Server

Implemente Citrix ADM en modo de alta disponibilidad

Migrate from NetScaler Insight Center to NetScaler ADM

Integración de NetScaler ADM con Director

## Administración de instancias

Cómo agregar instancias a Citrix ADM

Cómo crear grupos de instancias en Citrix ADM

Cómo hacer una copia de seguridad y restaurar una instancia mediante Citrix ADM

## Administración de configuración

Cómo crear trabajos de configuración a partir de comandos correctivos en Citrix ADM

Cómo programar los trabajos creados mediante plantillas integradas en Citrix ADM

Cómo reprogramar los trabajos que se configuraron mediante plantillas integradas en Citrix ADM

Cómo reutilizar los trabajos de configuración ejecutados

## Análisis

WAN Insight

HDX Insight

Cómo ver los informes de red de las instancias de Citrix SD-WAN WANOP

Cómo configurar los umbrales adaptativos

Cómo configurar el resumen de bases de datos para análisis

Cómo crear umbrales y alertas mediante Citrix ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Gestión de eventos

Cómo establecer la antigüedad de los eventos en Citrix ADM

Cómo programar un filtro de eventos mediante Citrix ADM

Cómo configurar notificaciones de correo electrónico repetidas para eventos de Citrix ADM

Cómo suprimir eventos mediante Citrix ADM

Cómo ver informes de eventos para instancias de Citrix SD-WAN WANOP

Cómo modificar la gravedad notificada de los eventos que se producen en las instancias de Citrix ADC

Cómo ver el resumen de eventos en NetScaler ADM

Cómo mostrar la gravedad de los eventos y los sesgos de las trampas de SNMP en el panel de infraestructura de Citrix ADM

## Autenticación

Cómo conectar en cascada servidores de autenticación externos

Cómo agregar servidores de autenticación RADIUS

Cómo agregar servidores de autenticación LDAP

Cómo agregar servidores de autenticación TACACS

Cómo extraer el grupo de servidores de autenticación en Citrix ADM

Cómo habilitar la autenticación local alternativa

## Sistema NetScaler ADM

Administración del sistema Citrix ADM

Cómo actualizar Citrix ADM

Cómo generar un archivo de soporte técnico para Citrix ADM

Cómo hacer copias de seguridad y restaurar el servidor Citrix ADM en una implementación de un solo servidor

Cómo hacer una copia de seguridad y restaurar una configuración de Citrix ADM en un par HA

Cómo habilitar el acceso a Shell para usuarios no predeterminados en Citrix ADM

Cómo configurar el servidor NTP en Citrix ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Cómo configurar los parámetros de SSL para Citrix ADM

Cómo configurar el intervalo de purga de Syslog para Citrix ADM

Cómo ver la información de auditoría de NetScaler ADM

Cómo configurar las opciones de notificación del sistema de NetScaler ADM

Cómo supervisar el uso de la CPU, la memoria y el disco de Citrix ADM

Cómo configurar un grupo de cifrado para Citrix ADM

Cómo crear trampas, administradores y usuarios de SNMP en Citrix ADM

Cómo asignar un nombre de host a un servidor Citrix ADM

Cómo configurar los parámetros de poda del sistema para Citrix ADM

Cómo configurar los ajustes de copia de seguridad del sistema mediante Citrix ADM

Cómo configurar y ver alarmas del sistema en NetScaler ADM

## Agregar instancias de Citrix SD-WAN

January 30, 2024

Configure NetScaler ADM como el recopilador AppFlow en el dispositivo Citrix SD-WAN SE/PE para agregar estas instancias en NetScaler ADM.Los dispositivos Citrix SD-WAN SE/PE/AE se registran como instancias administradas en NetScaler ADM y se recopilan sus registros AppFlow. Para un dispositivo Citrix SD-WAN PE, puede habilitar la plantilla **TCP solo para HDX** o la plantilla **HDX** . La plantilla **TCP solo para HDX** proporciona datos de saltos múltiples. La plantilla **HDX** proporciona datos HDX, debe habilitarse únicamente en el dispositivo del centro de datos.

Puede configurar NetScaler ADM como un recopilador AppFlow en el dispositivo SD-WAN SE/PE/AE individual, o puede configurar NetScaler ADM como el recopilador AppFlow mediante SD-WAN Center y exportar la configuración a los dispositivos administrados por él.

**Para configurar NetScaler ADM como un recopilador AppFlow en un dispositivo Citrix SD-WAN SE/PE/AE:**

1. En la interfaz web SD-WAN SE/PE/AE, vaya a **Configuración** > **AppFlow/IPfix**
2. Elija **Activar**.
3. En el campo **Intervalo de actualización de datos** , especifique el intervalo de tiempo, en minutos, en el que los informes de AppFlow se exportan al recopilador de AppFlow.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Si Citrix ADM es el recopilador de AppFlow, el intervalo de actualización de datos debe ser de 1 minuto.

4. Lleve a cabo una de las siguientes acciones:
   - Elija **HDX** para enviar datos de HDX Insight al recopilador de AppFlow. Esto debe estar habilitado en los dispositivos de la sucursal.
   - Elija **TCP solo para HDX** para enviar datos de varios saltos al recopilador de AppFlow.

> **Nota**
>
> **La opción de plantilla HDX**solo está disponible para el dispositivo Citrix SD-WAN PE; debe estar habilitada en el dispositivo Data Center

5. En el campo **Dirección IP** , escriba la dirección IP del sistema recopilador AppFlow externo (Citrix ADM Server).
6. En el campo **Puerto** , escriba el número de puerto en el que escucha el sistema recopilador AppFlow externo. El valor predeterminado es 4739.
7. Seleccione la casilla **Citrix ADM** para especificar que Citrix ADM es el recopilador de AppFlow.

> **Nota**
>
> - Actualmente, NetScaler ADM no admite la recopilación IPFIX.
> - Puede añadir hasta cuatro recopiladores de AppFlow. Citrix ADM o cualquier recopilador de AppFlow que admita el protocolo IPFIX.

8. Introduzca las credenciales del servidor Citrix ADM
9. Haga clic en **Aplicar configuración**.

Los dispositivos Citrix SD-WAN SE/PE se descubren y se enumeran en Citrix ADM. Los dispositivos Citrix SD-WAN SE/PE envían los datos de análisis a NetScaler ADM. Para obtener más información, consulte AppFlow e IPFIX.

**Para configurar NetScaler ADM como un recopilador de AppFlow mediante Citrix SD-WAN Center:**

1. En la interfaz de usuario de administración de Citrix SD-WAN Center, vaya a **Configuración** > **Configuración del**dispositivo.
2. Navegue hasta la sección **AppFlow/IPFIX** y seleccione **Incluir en archivo**.
3. Seleccione **Habilitar colección IPFIX/AppFlow**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. En el campo **Intervalo de actualización de datos**, especifique el intervalo de tiempo, en minutos, en el que se exportan los informes de AppFlow al recopilador AppFlow.

   > **Nota**
   >
   > Si Citrix ADM es el recopilador de AppFlow, el intervalo de actualización de datos debe ser de 1 minuto.

5. Lleve a cabo una de las siguientes acciones:

   - Elija **HDX** para enviar datos de HDX Insight al recopilador de AppFlow.
   - Elija **TCP para HDX** para enviar datos de información de varios saltos al recopilador de AppFlow. Esto debe estar habilitado en los dispositivos de la sucursal.

   > **Nota**
   >
   > **La opción de plantilla HDX**solo está disponible para el dispositivo Citrix SD-WAN PE; debe estar habilitada en el dispositivo Data Center.

6. En el campo **IPFIX/AppFlow Collector**, escriba la dirección IP del sistema recopilador AppFlow externo (Citrix ADM Server).
7. En el campo **Puerto** , escriba el número de puerto en el que escucha el sistema recopilador AppFlow externo. El valor predeterminado es 4739.
8. Seleccione la casilla **Citrix ADM** para especificar que Citrix ADM es el recopilador de AppFlow.
9. Introduzca las credenciales del servidor Citrix ADM.

   > **Nota**
   >
   > Puede añadir hasta cuatro recopiladores de AppFlow. Citrix ADM o cualquier recopilador de AppFlow que admita el protocolo IPFIX.

10. Guarde y exporte la configuración a los dispositivos administrados.

    Para obtener más información, consulte Cómo configurar y exportar la configuración del dispositivo a los dispositivos administrados.

Para obtener más información sobre cómo configurar NetScaler ADM como recopilador de AppFlow mediante Citrix SD-WAN Center, AppFlow e IPFIX.

NetScaler ADM detecta y enumera los dispositivos Citrix SD-WAN SE/PE.Los dispositivos Citrix SD-WAN SE/PE se detectan y aparecen en NetScaler ADM. Para ver los dispositivos Citrix SD-WAN SE/PE detectados, en la interfaz web de NetScaler ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** y seleccione **SD-WAN SE/PE/AE**.

Puede ver la dirección IP, el nombre, el estado actual, la edición del software y la versión de los dispositivos descubiertos. También puede comprobar si el dispositivo es un nodo de controlador maestro (MCN) o no.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede realizar las siguientes acciones:

- Ver y eliminar los perfiles de instancia.
- Elimine instancias de Citrix ADM.
- Redescubra instancias.

Para un dispositivo Citrix SD-WAN PE, puede ver registros de datos HDX o datos de varios saltos, dependiendo de la configuración de AppFlow. Un dispositivo Citrix SD-WAN SE proporciona solo datos de salto múltiple. Para obtener más información, consulte Visualización de informes y métricas de HDX Insight y Visualización de datos de Citrix SD-WAN Analytics para la implementación de varios saltos.

## Ver los datos de análisis de Citrix SD-WAN para la implementación de varios saltos

January 30, 2024

Una implementación de red de varios saltos tiene varios dispositivos entre el cliente y el servidor, como se muestra en la ilustración siguiente. En este tipo de implementación, los dispositivos Citrix SD-WAN SE y Citrix Gateway se agregan a Citrix ADM y AppFlow está habilitado.

Citrix ADM identifica el dispositivo del que recibe los datos en función del recuento de saltos y el ID de la cadena de conexiones. El recuento de saltos representa la cantidad de dispositivos a través de los cuales fluye el tráfico del cliente al servidor. El ID de la cadena de conexión representa las conexiones de extremo a extremo entre el cliente y el servidor.

Citrix ADM utiliza el recuento de saltos y el ID de la cadena de conexiones para correlacionar los datos de los dispositivos y genera los informes.

Para que los dispositivos Citrix SD-WAN SE envíen los datos de análisis a Citrix ADM, debe configurar la dirección IP virtual de Citrix Gateway como IP ICA de DPI y establecer el número de puerto ICA de DPI en 443.

**Para configurar los ajustes de DPI de ICA:**

1. En la interfaz de usuario del dispositivo Citrix SD-WAN SE, vaya al **Editor de configuración** > **Avanzado** > **Global** > **Aplicaciones** > **Configuración**.
2. Seleccione **Habilitar la inspección profunda de paquetes** > **Habilitar la inspección profunda de paquetes para aplicaciones ICA de Citrix** > **Habilitar ICA de transmisión múltiple**
3. En el campo **DPI ICA IP-1**, introduzca la dirección IP virtual y el prefijo de Citrix Gateway.
4. En el campo **DPI ICA Port-1**, introduzca el número de puerto 443.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

5. Haga clic en **Aplicar** y exporte la configuración al dispositivo mediante el proceso de gestión de cambios.

En Citrix ADM, para cada sesión ICA activa, puede ver un diagrama de sesión en HDX Insight. Los diagramas de sesión proporcionan detalles sobre los dispositivos de la ruta de conexión. También proporcionan información sobre la latencia del lado del cliente y del lado del servidor entre un dispositivo de red y su siguiente salto inmediato. Esta información le permite identificar la causa raíz del retraso y solucionar los problemas de rendimiento.

Citrix SD-WAN SE no envía registros de datos HDX. Solo proporciona información de TCP para HDX. Los datos de HDX Insight los proporcionan los dispositivos habilitados para HDX Insight de la red (por ejemplo, Citrix ADC o Citrix Gateway).

El dispositivo Citrix SD-WAN PE puede enviar TCP para datos HDX o datos HDX Insight, dependiendo de la configuración de AppFlow del dispositivo.La plantilla HDX debe estar habilitada en el dispositivo del centro de datos.

> **Nota**
>
> En una implementación de varios saltos, asegúrese de que solo uno de los dispositivos de red envíe datos de HDX Insight. El resto de los dispositivos de red pueden enviar datos TCP para HDX.

**Para ver los datos de varios saltos:**

En la interfaz web Citrix ADM, vaya a **HDX Insight** > **Usuarios** > **Sesiones actuales** o **HDX Insight** > **Aplicaciones** > **Sesiones actuales** y haga clic en el icono **Diagrama**.

Aparece el diagrama de topología de red.

Haga clic en cualquier elemento de la red para ver más información.

> **Nota**
>
> La información que se muestra depende del elemento de red seleccionado.

Aparecen los siguientes parámetros para los dispositivos Citrix:

- **Nombre**: nombre del dispositivo Citrix.
- **Dirección IP**: dirección IP del dispositivo.
- **Latencia WAN**: latencia causada por el lado del cliente de la red. Es decir, desde el dispositivo Citrix hasta el usuario final.
- **Latencia DC**: latencia causada por el lado del servidor de la red. Es decir, desde el dispositivo Citrix hasta los servidores back-end.
- **Estado: Estado**de accesibilidad del dispositivo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Ver informes de eventos para instancias de Citrix SD-WAN WANOP

January 30, 2024

Para ver los eventos de las 10 instancias principales de SD-WAN WANOP como representación gráfica, vaya a **Redes** > **EventosInformes**y seleccione**Citrix SD-WAN WO**.

Los eventos se muestran en función de su gravedad para cada instancia, puede hacer clic en cada gravedad para obtener más información sobre el número de eventos, cuándo ocurrió y a qué categoría pertenece.

## Ver informes de red para instancias de Citrix SD-WAN WANOP

January 30, 2024

Puede ver los informes relacionados con la red de optimización de WAN en Citrix ADM. Con estos datos, puede solucionar problemas de red o analizar el comportamiento de sus dispositivos Citrix SD-WAN WAN WANOP. Puede ver los informes de las estadísticas de red de sus dispositivos de optimización de WAN durante la última hora, un día, una semana o un mes.

Puede ver los siguientes informes:

| Informes | Descripción |
| --- | --- |
| Aceleración | Utilice este informe para analizar el patrón de tráfico acelerado (KBPS por clase de servicio) y el número de conexiones TCP aceleradas que pasan por el dispositivo de optimización de WAN. Esto incluye la cantidad de conexiones TCP que pasan por el dispositivo de optimización de WAN y que se aceleran, la cantidad de conexiones abiertas y semicerradas que se han seleccionado para la aceleración y la cantidad de conexiones medio abiertas que son candidatas a la aceleración. |
| Conexión de paso | Utilice este informe para ver las conexiones no aceleradas del dispositivo de optimización de WAN. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Informes | Descripción |
| --- | --- |
| Clase de servicio | Utilice este informe para ver los ahorros de ancho de banda enviados y recibidos según el tipo de clase de servicio definido para el dispositivo de optimización de WAN. |
| Aplicación | Utilice este informe para ver el volumen de datos enviados y recibidos en bits por segundo para las aplicaciones que se ejecutan en el dispositivo de optimización de WAN. |
| Utilización de CPU | Utilice este informe para ver la utilización de la CPU del dispositivo de optimización de WAN como porcentaje. |
| Incremento de capacidad | Utilice este informe para ver la relación de compresión de envío acumulada para el dispositivo de optimización de WAN. |
| Reducción de datos | Utilice este informe para ver el ahorro de ancho de banda de transmisión y recepción como porcentaje. También puede analizar el ancho de banda de transmisión y recibir valores de ahorro de ancho de banda por separado para el dispositivo de optimización de WAN. |
| Utilización de enlaces | Utilice este informe para ver la utilización de los enlaces de transmisión y recepción para la optimización de la WAN como porcentaje. |
| Uso del plugin | Utilice este informe para ver la cantidad de complementos conectados al dispositivo de optimización de WAN. |
| Pérdida de paquetes | Utilice este informe para ver los paquetes enviados por enlace interrumpido y los paquetes recibidos por enlace interrumpido para los enlaces definidos en el dispositivo de optimización de WAN. |
| Rendimiento | Utilice este informe para ver el volumen del enlace enviado y el volumen del enlace recibido en bits por segundo para el dispositivo de optimización de WAN. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Informes | Descripción |
| --- | --- |
| QoS | Utilice este informe para ver el volumen de QOS enviado y de recepción de QOS en bits por segundo para el dispositivo de optimización de WAN. |

**Para ver los informes de red WANOP de Citrix SD-WAN**:

1. En Citrix ADM, vaya a **Redes** > **Informes de red** > **Citrix SD-WAN WO** .
2. En la lista desplegable **Nombre** del informe, seleccione un informe que quiera ver.
3. En la lista desplegable **Instancias** , seleccione la instancia de Citrix SD-WAN WANOP para la que desea ver el informe.
4. En la lista desplegable **Duración** , seleccione el intervalo de tiempo.
5. Haga clic en **Ejecutar**.

## Respaldar instancias de Citrix SD-WAN WANOP

January 30, 2024

Puede hacer una copia de seguridad del estado actual de una instancia y, más adelante, usar los archivos de la copia de seguridad para restaurar la instancia al mismo estado. Es una buena práctica hacer una copia de seguridad de una instancia antes de actualizarla o por motivos de precaución. Una copia de seguridad de un sistema estable le permite restaurar el sistema a un punto estable en caso de que se vuelva inestable. Hay varias formas de realizar copias de seguridad y restauraciones en una instancia de Citrix SD-WAN WANOP. Puede realizar copias de seguridad y restaurar instancias manualmente mediante la GUI, la CLI o utilizar Citrix ADM para realizar copias de seguridad. Citrix ADM realiza copias de seguridad del estado actual de las instancias SD-WAN WANOP administradas de Citrix mediante llamadas NITRO, el protocolo Secure Shell (SSH) y el protocolo Secure Copy (SCP).

### Configuración de los ajustes de backup de instancias

Antes de realizar una copia de seguridad de la instancia Citrix SD-WAN WANOP en Citrix ADM, debe configurar la configuración de copia de seguridad de la instancia en Citrix ADM.

**Para configurar los ajustes de copia de seguridad de la instancia:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**. En el panel derecho, en Configuración de copia de **seguridad, selecciona Configuración** de copia de **seguridad de la instancia** .
2. Seleccione **Habilitar copias de seguridad de instancias** . Esta opción está habilitada de forma predeterminada.
3. Seleccione **Proteger archivo con contraseña** para cifrar el archivo de respaldo. El cifrado del archivo de respaldo garantiza que la información confidencial del archivo de respaldo esté segura.
4. En el campo **Número de archivos de copia de seguridad que retener**, especifique el número de archivos de copia de seguridad que se deben conservar en NetScaler ADM. Puede conservar hasta 50 archivos de respaldo.

   > **Nota**
   >
   > Cada archivo de respaldo requiere algún requisito de almacenamiento. Citrix recomienda almacenar una cantidad óptima de archivos de respaldo en Citrix ADM según sus necesidades.

5. Establezca la configuración de programación de copias de seguridad. Elija una de las siguientes opciones:

   - **Basado en intervalos**: Se crea un archivo de copia de seguridad en NetScaler ADM una vez transcurrido el intervalo especificado. El intervalo de copia de seguridad predeterminado es de 12 horas.
   - **Basado**en el tiempo : puede especificar la hora en formato «horas:minutos» a la que debe realizarse la copia de seguridad. Citrix ADM permite realizar hasta cuatro copias de seguridad diarias en las instancias.

   > **Nota**
   >
   > Omita la sección **Configuración de Citrix ADC**; esta configuración no se aplica a las instancias de SD-WAN WANOP de Citrix.

6. Seleccione **Habilitar transferencia externa para transferir** los archivos de respaldo de la instancia a una ubicación externa. Introduzca los valores de los campos siguientes:

   - **Servidor**: dirección IP del servidor externo.
   - **Nombre**de usuario: nombre de usuario del servidor externo
   - **Contraseña**: contraseña del servidor externo.
   - **Puerto**: número de puerto utilizado para comunicarse con el servidor externo.
   - **Protocolo**de transferencia : protocolo que se utilizará para transferir los archivos de copia de seguridad de Citrix ADM al servidor externo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

También puede eliminar el archivo de copia de seguridad de Citrix ADM después de transferirlo al servidor externo.

7. Haga clic en **Aceptar**.

> **Nota**
>
> Citrix ADM se envía una captura de SNMP o una notificación de Syslog cuando se produce un error de respaldo en alguna de las instancias de SD-WAN WANOP de Citrix seleccionadas.

## Creación de una copia de seguridad de una instancia de Citrix SD-WAN WANOP

El procedimiento para crear una copia de seguridad para la instancia SD-WAN WANOP de Citrix se aplica a un usuario administrador que utilice el perfil nsroot predeterminado.

Para obtener información sobre cómo un usuario personalizado puede realizar una copia de seguridad de una instancia de Citrix SD-WAN WANOP, consulte la sección Creación de una copia de seguridad de una instancia WANOP de Citrix SD-WAN para usuarios personalizados de este tema.

Asegúrese de que se agregue una instancia de Citrix SD-WAN WANOP a NetScaler ADM para obtener más información, consulte Agregar instancias a NetScaler ADM.

**Para crear una copia de seguridad para la instancia de Citrix SD-WAN WANOP:**

1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** .
2. En **SD-WAN WO**, seleccione la instancia de Citrix SD-WAN WANOP de la que quiere realizar una copia de seguridad y, a continuación, haga clic en**Copia de seguridad/restauración**.
3. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de** seguridad .
4. Cifre el archivo de respaldo mediante cualquiera de las siguientes opciones:
   - Seleccione **Archivo protegido con contraseña** e introduzca una contraseña para cifrar los archivos de respaldo.
   - Selecciona **Usar contraseña global** para usar la contraseña global que especificaste en la página de configuración de la copia de seguridad de la instancia.
5. Haga clic en **Crear copia de seguridad**

## Creación de una copia de seguridad de una instancia de Citrix SD-WAN WANOP para usuarios personalizados

Si ha creado un usuario personalizado con privilegios de administrador en la instancia WANOP de Citrix SD-WAN, utilice el siguiente procedimiento para agregar una instancia y realizar una copia de seguridad de esa instancia mediante Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

La operación de respaldo por parte de usuarios personalizados no es compatible con las plataformas SD-WAN WANOP 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100.

> **Nota**
>
> Citrix recomienda utilizar el perfil nsroot predeterminado al crear copias de seguridad de las plataformas avanzadas Citrix SD-WAN en Citrix ADM.

**Para agregar una instancia de Citrix SD-WAN WANOP y realizar una copia de seguridad para un usuario personalizado:**

1. En Citrix ADM, vaya a **Redes** > **Instancias** > **Citrix SD-WAN** y seleccione **SD WAN WO**.
2. Haga clic en **Agregar**.
3. En el campo **Dirección IP** , introduzca la dirección IP de la instancia de Citrix SD-WAN WANOP.
4. Haga clic en **Agregar** junto al campo **Nombre del perfil** para crear un perfil nuevo. Aparece la ventana **Crear perfil WO de Citrix SD-WAN** .
5. En el **campo Nombre del perfil** , introduzca un nombre para el perfil.
6. En el campo **Nombre de usuario** , introduzca el nombre de usuario del usuario personalizado que creó en la instancia de SD-WAN WANOP.
7. En el **campo Contraseña** , introduzca la contraseña que estableció para el usuario personalizado en la instancia de SD-WAN WANOP.
8. En el campo **Comunidad** , introduzca la cadena de comunicación SNMP configurada en el dispositivo SD-WAN WANOP. (por ejemplo: pública)
9. Haga clic en **Crear**.
10. En el campo **Nombre del perfil** , seleccione el perfil recién creado **y** haga clic en Aceptar .
11. Vaya a **Redes** > **Instancias** > **Citrix SD-WAN** .
12. En **SD-WAN WO**, seleccione la instancia de Citrix SD-WAN WANOP que acaba de agregar y, a continuación, haga clic en**Copia de seguridad/restauración**.
13. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de** seguridad .
14. Cifre el archivo de respaldo mediante cualquiera de las siguientes opciones:
    - Seleccione **Archivo protegido con contraseña** e introduzca una contraseña para cifrar los archivos de respaldo.
    - Selecciona **Usar contraseña global** para usar la contraseña global que especificaste en la página de configuración de la copia de seguridad de la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Puede descargar el archivo de respaldo cifrado a su máquina local, pero no puede ver su contenido. Solo Citrix ADM puede usar estos archivos de respaldo con fines de restauración. Al restaurar la copia de seguridad cifrada, se solicitará la contraseña.

15. Haz clic en **Crear copia** de seguridad .

> **Importante**
>
> ```
> 1. Para un dispositivo Citrix SD-WAN WANOP VPX, Citrix ADM solo hace copias de seguridad del archivo de configuración del broker CB.
> ```
>
> a) Para una plataforma Citrix SD-WAN WANOP avanzada, Citrix ADM hace copias de seguridad de lo siguiente: ·
>
> - Archivo de configuración de CB Broker
> - Archivo de configuración NTP
> - DNS
> - Archivo de configuración SNMPD
> - Archivo de configuración de Syslog
> - Certificado SSL, claves y políticas
> - Archivo de base de datos SVM
> - Componentes (en formato XML)
> - Recursos (en formato XML)
>
> Los archivos de los que se ha hecho una copia de seguridad en las carpetas correspondientes se enumeran en la tabla siguiente. Tenga en cuenta que si el nombre de una carpeta va seguido de un «*», se realizará una copia de seguridad de todos los archivos de esa carpeta.
>
> | Directorio | Subdirectorio o archivos |
> |---|---|
> | /br_corredor/ | CB-6BBB660a/ ws.conf |
> | /etc/ | resolv.conf |
> | /mps/ | mps_devices.xml |
> | /mpsconfig/ | ssl/*, ntp.conf, snmpd.conf, syslog.conf |
> | /mpsdb/ | mpsdb_dump.sql |
> | /ns/ | NS-6CBB660A/* |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | |
|---|---|
| /var/ | mps/policy/, *mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/* |

## Administrar instancias de HAProxy

January 30, 2024

HAProxy es un balanceador de cargas de código abierto que puede balancear la carga de cualquier servicio TCP o HTTP. Para obtener más información sobre HAProxy, consulte.http://www.haproxy.org/

Citrix Application Delivery Management (Citrix ADM) admite la versión 1.4.24 o posterior de HAProxy. Cuando agrega un host en el que ha aprovisionado las instancias de HAProxy a Citrix ADM, Citrix ADM descubre las instancias de HAProxy en el host y le permite supervisarlas. Muestra los siguientes tipos de información sobre la configuración de HAProxy en las instancias:

- Interfaz: cómo se deben reenviar las solicitudes al back-end.
- Backend: el conjunto de servidores que reciben las solicitudes reenviadas.
- Servidores: Servidores entre los que la carga HAProxy equilibra el tráfico.

Para obtener más información, consulte http://www.haproxy.org/download/1.7/doc/configuration.txt.

Además, NetScaler ADM proporciona un panel de aplicaciones HAProxy en el que puede supervisar las interfaces en tiempo real. Para obtener más información, consultePanel de control de aplicaciones HAProxy.

## Agregar instancias de HAProxy a NetScaler ADM

January 30, 2024

En Citrix Application Delivery Management (Citrix ADM), debe agregar manualmente los detalles del host en el que ha aprovisionado la instancia de HAProxy. Después de agregar esos detalles, NetScaler ADM descubre automáticamente las instancias de HAProxy aprovisionadas en el host y las agrega al Inventario de NetScaler ADM. También descubre todos los front-ends, back-ends y servidores configurados en las instancias HAProxy, y trata los front-ends como aplicaciones descubiertas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Requisitos previos

Asegúrese de lo siguiente:

- Implementó una instancia de HAProxy en un host de su implementación. Para obtener más información, consulte http://www.haproxy.org/#docs.
- Identificado y decidido sobre el número de front-ends para los que quiere ver las estadísticas de la aplicación en el Panel de aplicaciones HAProxy. De forma predeterminada, el panel de control de aplicaciones HAProxy muestra las estadísticas de 30 aplicaciones detectadas. Para obtener más información sobre el panel de aplicaciones HAProxy, consulte Panel de control de aplicaciones HAProxy Si quiere ver las estadísticas de más de 30 aplicaciones descubiertas, debe comprar una licencia independiente. Para obtener más información, consulte Licencias de terceros.

> **Importante**
>
> NetScaler ADM requiere acceso al host para descubrir las instancias de HAProxy en él. Puede proporcionar acceso a Citrix ADM proporcionando el par de claves SSH del host o mediante la contraseña del host. Si desea proporcionar acceso mediante el par de claves SSH, asegúrese de generar el par de claves privadas y públicas de SSH en el host y de agregar la clave pública a las claves autorizadas del host. Además, la cuenta de usuario SSH debe tener permisos de superusuario.

**Para agregar una instancia de HAProxy a NetScaler ADM:**

1. Navegue hasta **Redes** > **Instancias** . En **Instancias** , seleccione **HAProxy** y haga clic en **Agregar** .
2. En el cuadro de diálogo **Agregar host HAProxy**, haga lo siguiente:
1. En el campo **Dirección IP**, introduzca la dirección IP del host en el que ha aprovisionado las instancias de HAProxy.
    a) En el menú **Perfil de HAProxy** , seleccione un perfil de HAProxy existente o cree y seleccione un nuevo perfil de HAProxy. Para crear un perfil de HAProxy, haga clic en **Agregar** .
        i. En el cuadro de diálogo **Agregar perfil de HAProxy**, haga lo siguiente:
        i. En el campo **Nombre del perfil**, introduzca el nombre del perfil.
        ii. En los campos **Nombre de usuario** y **Contraseña** , introduzca las credenciales de usuario del host.
        iii. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En el menú **Sitio** , seleccione un sitio de HAProxy. Para crear y agregar un sitio nuevo al menú, haga clic en **Agregar** .
3. En el menú **Agente** , seleccione un agente.
4. En los campos Etiquetas, introduzca los valores de forma adecuada.
5. Haga clic en **Aceptar**.

NetScaler ADM descubre las instancias de HAProxy aprovisionadas en el host y puede ver todas las instancias de HAProxy en la ficha **Instancias**.

### Visualización de la configuración de una instancia HAProxy

Para ver la configuración de una instancia HAProxy en NetScaler ADM, vaya a **Redes** > **Instancias** > **HAProxy** y, en la ficha **Instancias**, seleccione la instancia HAProxy y haga clic en **Ver configuración**.

## Panel de aplicación HAProxy

January 30, 2024

El Panel de aplicaciones proporciona estadísticas en tiempo real de todos los front-ends HAProxy supervisados por NetScaler Application Delivery Management (NetScaler ADM). Enumera los front-end como aplicaciones discretas y proporciona información sobre transacciones, rendimiento y sesiones acerca de las aplicaciones.

> **Importante**
>
> Asegúrese de habilitar las **estadísticas** en el archivo de configuración de la instancia de HAProxy. Para habilitar las **estadísticas** , edite el archivo de configuración de HAProxy y, después de la sección de valores predeterminados, añada una entrada similar a la del siguiente ejemplo:

```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
```

Para acceder a la aplicación HAProxy en el panel de aplicaciones de Citrix ADM, después de agregar las instancias de HAProxy a Citrix ADM, vaya a **Aplicaciones** > **Panel**. Puede filtrar el panel para que muestre solo la aplicación HAProxy. Para filtrar el panel, seleccione **HAPROXY** que se muestra en la sección **Familia de aplicaciones del panel de información resumida de la aplicación**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Ver métricas clave de la aplicación HAProxy

El panel **Información de la aplicación** se encuentra en el primer nivel cuando se profundiza en una aplicación HAProxy. Muestra las métricas y componentes clave de la aplicación, junto con su estado. Por ejemplo, para cualquier aplicación HAProxy seleccionada, el panel **Información de la aplicación** muestra el número total de frontales HAProxy, el número total de backends HAProxy, el volumen de datos, la tendencia de las conexiones de cliente y las transacciones. Para ver las métricas clave de la aplicación HAProxy, haga clic en el icono de la **aplicación HAProxy** en el panel de la aplicación. El panel **Información de la aplicación** reemplaza al panel **Resumen de la aplicación**.

### Ver el rendimiento en tiempo real de la aplicación HAProxy

Citrix ADM le permite ver el rendimiento en tiempo real de sus aplicaciones HAProxy. Proporciona los siguientes detalles en tiempo real de la aplicación HAProxy seleccionada:

- **Transacciones.** Transacciones realizadas por la aplicación.
- **Rendimiento.** Rendimiento de la aplicación.
- **Sesiones.** Número de sesiones establecido por la aplicación.

Para ver el rendimiento en tiempo real de la aplicación HAProxy, en el **Panel de aplicaciones**, haga doble clic en el icono de la aplicación HAProxy.

De forma predeterminada, la pestaña **Transacciones** está seleccionada y se muestran las transacciones en tiempo real realizadas por la aplicación.

Para ver el rendimiento en tiempo real de la aplicación, haga clic en la ficha **Rendimiento**.

Puede hacer clic en la ficha **Sesiones** para ver el número de sesiones establecidas por la aplicación en tiempo real.

## Licencias de terceros

January 30, 2024

Después de agregar los hosts a NetScaler Application Delivery Management (NetScaler ADM), NetScaler ADM descubre automáticamente las instancias de HAProxy aprovisionadas en los hosts y las agrega a NetScaler ADM Inventory. También descubre todos los front-ends, back-ends y servidores configurados en las instancias HAProxy y considera los front-ends como aplicaciones descubiertas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede administrar y supervisar todas las aplicaciones detectadas, pero, de forma predeterminada, el panel de aplicaciones HAProxy muestra las estadísticas de la aplicación para 30 aplicaciones detectadas. Para obtener más información sobre el panel de aplicaciones HAProxy, consulte Panel de control de aplicaciones HAProxy Si desea ver las estadísticas de aplicaciones de más de 30 aplicaciones descubiertas, debe comprar una licencia independiente.

Las licencias para más front-ends están disponibles en paquetes de servidores virtuales de 100. Puede obtener una licencia válida e instalarla mediante la GUI de NetScaler ADM.

## Instalar las licencias de terceros

Puede instalar una licencia en NetScaler ADM para ver las estadísticas de aplicaciones de más de 30 aplicaciones descubiertas.

**Para instalar una licencia:**

1. Vaya a **Redes** > **Licencias** .
2. En la sección **Archivos de licencias**, seleccione una de las siguientes opciones:
   - **Cargue los archivos de licencia desde un equipo local.** Si ya hay una licencia en su equipo local, haga clic en Examinar y seleccione el archivo de licencia (.lic) que quiere usar para asignar sus licencias. Haga clic en **Finalizar**.
   - **Usar código de activación de licencia** : Citrix envía por correo electrónico la clave de licencia de la licencia que compró. Escriba la clave de licencia en el cuadro de texto y, a continuación, haga clic en **Obtener licencias**.

   > **Nota**
   >
   > Si selecciona esta opción, Citrix ADM debe estar conectado a Internet o un servidor proxy debe estar disponible.

   Puede verificar las licencias instaladas en su NetScaler ADM navegando a **Redes** > **Licencias > Licencias** de **terceros**.

## Administrar las licencias de terceros

NetScaler ADM selecciona aleatoriamente las aplicaciones detectadas en las instancias de HAProxy y las otorga automáticamente licencias. Si desea cambiar las aplicaciones detectadas seleccionadas, debe anular manualmente la licencia de las aplicaciones descubiertas con licencia y, a continuación, asignar las licencias a las aplicaciones descubiertas para las que desea licenciar.

**Para administrar las licencias de terceros:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes** > **Licencias > Licencias** > **Licencias de terceros** y haga clic en **Modificar Servidores virtuales con licencia de terceros**. El tablero de mandos muestra los front-ends administrados.
2. Seleccione los front-ends de la lista, **Marcar sin licencia**y haga clic en **Finalizar** para liberar las licencias.
3. Después de liberar las licencias, o si ya tiene licencias disponibles, haga clic en **Agregar frontend HAProxy**.
4. En el cuadro de diálogo **Elegir interfaz HAProxy, seleccione los frontend** sin licencia de la lista y haga clic en **Seleccionar**.
5. Haga clic en **Finalizar ahora**.

## Control de acceso basado en roles para instancias de HAProxy

January 30, 2024

Citrix Application Delivery Management (Citrix ADM) utiliza un control de acceso detallado basado en roles (RBAC) para controlar el acceso a los objetos de configuración. Por ejemplo, puede crear usuarios y darles acceso a instancias concretas de HAProxy, y puede especificar permisos de ver/solo lectura para el panel de aplicación HAProxy. Para obtener más información, consulte Control de acceso basado en funciones en NetScaler ADM.

## Supervisar instancias de HAProxy

January 30, 2024

El panel de HAProxy de Citrix Application Delivery Management (Citrix ADM) muestra gráficos que ayudan a realizar un seguimiento del uso de la CPU y la memoria de una instancia de HAProxy. El panel también muestra gráficos que indican lo siguiente:

- Porcentaje de CPU utilizada por la instancia de HAProxy en el host.
- Porcentaje de CPU utilizada por otras entidades del host.
- Porcentaje de CPU restante en el host.
- Porcentaje de memoria utilizada por la instancia HAProxy en el host.
- Porcentaje de memoria utilizada por otras entidades del host.
- Porcentaje de memoria restante en el host.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para supervisar una instancia de HAProxy en Citrix ADM, vaya a la pestaña **Redes** > **Instancias** > **HAProxyInstancias**, seleccione la instancia de HAProxy y haga clic en**Panel** de control.

## Ver los detalles de front-ends configurados en instancias HAProxy

January 30, 2024

NetScaler Application Delivery Management (NetScaler ADM) informa de los siguientes detalles del front-end configurado en una instancia HAProxy:

- **Dirección IP del host**. Dirección IP del host
- **Ruta**de configuración . Ruta de configuración absoluta de la instancia de HAProxy en el host.
- **Nombre**. Nombre del front-end que controla el tráfico entrante.
- **Enlazar host**. Dirección IP a la que está vinculado el front-end.
- **Puerto de enlace**. Puerto al que está vinculado el front-end.

**Para ver el front-end configurado en las instancias HAProxy:**

En NetScaler ADM, vaya a **Redes > Funciones de red > HAProxy > Frontend**.

## Ver los detalles de back-ends configurados en instancias HAProxy

January 30, 2024

NetScaler Application Delivery Management (NetScaler ADM) informa de los siguientes detalles de una aplicación back-end configurada en una instancia HAProxy:

- **Dirección IP del host**. Dirección IP del host.
- **Ruta**de configuración . Ruta de instancia de HAProxy en el host.
- **Nombre**. Nombre del back-end al que se reenvía el tráfico.
- **Algoritmo**. Algoritmo de equilibrio de carga utilizado para equilibrar el tráfico.

**Para ver el back-end configurado en las instancias HAProxy:**

En NetScaler ADM, vaya a **Redes** > **Funciones de red** > **HAProxy** > **Backends**.

## Ver los detalles de los servidores configurados en instancias HAProxy

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Citrix Application Delivery Management (Citrix ADM) informa de los siguientes detalles de los servidores configurados en una instancia de HAProxy:

- **Dirección IP del host**. Nombre del anfitrión.
- **Ruta**de configuración . Ruta absoluta del archivo de configuración de la instancia de HAProxy en el host.
- **Nombre del back-end**. Nombre del back-end en la configuración HAProxy.
- **Nombre**. Nombre del servidor en la configuración de HAProxy.
- **Dirección**del servidor . Dirección IP del servidor.
- **Puerto**de servidor . Puerto utilizado por el servidor.

**Para ver los servidores configurados en las instancias de HAProxy:**

En NetScaler ADM, vaya a **Redes** > **Funciones de red** > **HAProxy** > **Servidores**.

## Ver las instancias HAProxy con el mayor número de servidores o front-ends

January 30, 2024

En el **Panel de aplicaciones**, NetScaler Application Delivery Management (NetScaler ADM) muestra el número de instancias HAProxy que descubre y enumera las cinco instancias HAProxy principales configuradas con el mayor número de servidores o front-ends.

Para ver el **Panel de aplicaciones**, en NetScaler ADM, vaya a **Aplicaciones** > **Dashboard**.

El número de instancias HAProxy descubiertas por NetScaler ADM se muestra en la fila superior:

Para ver la lista de las cinco instancias HAProxy principales que están configuradas con el mayor número de front-ends o el mayor número de servidores, desplácese hacia abajo por el panel:

## Reiniciar una instancia de HAProxy

January 30, 2024

Para reiniciar una instancia de HAProxy desde la GUI de Citrix Application Delivery Management (Citrix ADM), puede seleccionar un reinicio completo o un reinicio suave.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Reinicio duro

El reinicio completo finaliza el proceso HAProxy en la instancia y cierra todas las conexiones establecidas. Después del reinicio se crea un nuevo proceso HAProxy y las nuevas conexiones posteriores son procesadas por el nuevo proceso HAProxy.

### Reinicio suave

El reinicio parcial desvincula el proceso HAProxy del puerto de escucha, pero el proceso HAProxy continúa procesando las conexiones existentes hasta que se cierren. Se crea un nuevo proceso HAProxy para procesar las nuevas conexiones.

**Para reiniciar una instancia de HAProxy, haga lo siguiente:**

1. Vaya a **Redes** > **Instancias** > **HAProxy** y haga clic en la pestaña **Instancia** .
2. En la ficha **Instancia**, seleccione la instancia HAProxy que quiere reiniciar.
3. Haga clic en **Reiniciar** duro para reiniciar la instancia HAProxy o haga clic en **Reiniciar** suave para reiniciar la instancia HAProxy.

## Realizar una copia de seguridad y restaurar una instancia de HAProxy

January 30, 2024

Puede realizar una copia de seguridad del estado actual de una instancia de HAProxy en un archivo de configuración de HAProxy. Si la instancia se vuelve inestable, puede utilizar el archivo de copia de seguridad para restaurar la instancia al estado estable.

**Para realizar una copia de seguridad de una instancia HAProxy mediante NetScaler ADM:**

1. En Citrix Application Delivery Management (Citrix ADM), vaya a **Redes > Instancias > HAProxy** .
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Seleccione la instancia de HAProxy de la que desea hacer una copia de seguridad y, a continuación, haga clic en **Ver copia de seguridad** .
4. En la página **Archivos** de copia de seguridad , haga clic en **Realizar copia de seguridad.**
5. Puede optar por cifrar el archivo de copia de seguridad para obtener más seguridad.
6. Haga clic en **Continuar**.

**Para restaurar una instancia mediante NetScaler ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a **Redes** > **Instancias** > **HAProxy** .
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Selecciona la instancia que quieres restaurar y, a continuación, haz clic en Ver copia de **seguridad** .
4. En la página **Archivos** de copia de seguridad, seleccione el archivo de copia de seguridad que desea restaurar y, a continuación, haga clic en **Restaurar** .

> **Nota**
>
> Al restaurar una instancia, NetScaler ADM reinicia la instancia HAProxy.

## Modificar el archivo de configuración HAProxy

January 30, 2024

Puede actualizar el front-end, el back-end, el servidor y otras opciones en el archivo de configuración HAProxy existente. Para editar el archivo de configuración de HAProxy:

- Realice una copia de seguridad del archivo de configuración HAProxy.
- Descargue el archivo de configuración HAProxy de copia de seguridad y edítelo sin conexión.
- Cargue el archivo de configuración de HAProxy actualizado en Citrix Application Delivery Management (Citrix ADM)
- Restaure la instancia de HAProxy con el archivo de respaldo actualizado.

**Para modificar el archivo de configuración HAProxy mediante NetScaler ADM:**

1. En Citrix ADM, vaya a **Redes** > **Instancias** > **HAProxy**.
2. En la página **HAProxy**, haga clic en la ficha **Instancias**.
3. Seleccione la instancia de HAProxy de la que desea hacer una copia de seguridad y, a continuación, haga clic en **Ver copia de seguridad** .
4. En la página **Archivos de copia de seguridad**, haga clic en **Hacer copia de seguridad**.
5. Haga clic en **Continuar**.

> **Nota**
>
> No cifre el archivo de respaldo.

6. En la página **Archivos de copia** de seguridad, seleccione el archivo de copia de seguridad y haga clic en **Descargar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

7. Con un editor de texto, edite el archivo de configuración de HAProxy.
8. En la página **Archivos de copia** de seguridad, haga clic en **Cargar** para examinar y seleccionar el archivo de configuración HAProxy actualizado.

   Después de cargar el archivo de configuración HAProxy actualizado, aparece en la página **Archivos de copia de seguridad**.
9. Seleccione el archivo de configuración HAProxy actualizado y haga clic en **Restaurar**.

## Administrar la configuración del sistema

January 30, 2024

En la siguiente tabla se describe la lista de opciones disponibles en **Sistema** > **Administración** :

### Configuraciones de red

| Configuraciones de red | Opciones | Descripción |
|---|---|---|
| Dirección IP, segunda NIC, nombre de host y servidor proxy | Dirección IP | Muestra los detalles de la dirección IP de configuración de red de NetScaler ADM que se utilizan para implementar NetScaler ADM |
| | Segunda NIC | Permite configurar una segunda NIC para aislar el acceso de administración de NetScaler ADM. Para obtener más información, consulte Configurar una NIC doble para acceder a NetScaler ADM |
| | Nombre de host | Permite asignar un nombre de host a NetScaler ADM. Para obtener más información, consulte Asignar un nombre de host a un servidor NetScaler ADM |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Configuraciones de red | Opciones | Descripción |
|---|---|---|
| | Servidor proxy | Permite configurar ADM como servidor proxy. Para obtener más información, consulte NetScaler ADM como servidor proxy de API |
| Rutas estáticas | | Le permite configurar rutas estáticas para establecer una conexión entre las instancias de NetScaler ADM y NetScaler ADC VPX |
| Servidores NTP | | Garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red. Para obtener más información, consulte Configurar el servidor NTP |
| Información de puertos ADM | | Permite comprender qué puerto debe estar abierto para la comunicación entre instancias ADM y ADC o SD-WAN. Para obtener más información, consulte Puertos compatibles |

## Configuraciones del sistema

| Configuraciones del sistema | Opciones | Descripción |
|---|---|---|
| Sistema, zona horaria, URL permitidas y mensaje del día | Parámetros básicos | Permite modificar la configuración del sistema, como habilitar el inicio de sesión de `nsrecover`, habilitar el tiempo de espera de sesión, etc. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Configuraciones del sistema | Opciones | Descripción |
|---|---|---|
| | Zona horaria | Le permite modificar la zona horaria que se utilizará en NetScaler ADM. La zona horaria predeterminada es UTC |
| | Lista de URL permitidas | Permite configurar direcciones URL para enviar solicitudes ininterrumpidas a ADM. Puede configurarlo con el valor “none” si no se agregará ninguna URL |
| | Mensaje del día | Le permite crear un mensaje de bienvenida en NetScaler ADM. Puede utilizar esta función para establecer mensajes de recordatorio para usted o para el usuario que inicia sesión en NetScaler ADM. Haga clic en **Habilitar mensaje**, escriba el mensaje en el cuadro de mensajes y haga clic en **Guardar** |
| Ver huella digital de ADM | | Le permite copiar el identificador de huella digital único de NetScaler ADM para empezar con el gráfico de servicios |
| Configurar la identidad del cliente | | Permite proteger los recursos de red al permitir que solo los clientes o usuarios autenticados accedan a su red. Para obtener más información, consulte Gobierno de datos |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| | |
|---|---|
| Configuración de CUXIP | Si selecciona esta casilla de verificación, las estadísticas de uso se recopilan con el único propósito de mejorar la GUI. Los datos recibidos solo los utilizan los ingenieros de Citrix y no se comparten con nadie |

## Mantenimiento del sistema

| Mantenimiento del sistema | Descripción |
|---|---|
| Actualizar Citrix ADM | Permite actualizar NetScaler ADM a través de GUI. Para obtener más información, consulte Actualización |
| Reinicie NetScaler ADM | Le permite reiniciar NetScaler ADM |
| Cierre NetScaler ADM | Le permite cerrar NetScaler ADM |
| Recuperación ante desastres | Permite ver la información del nodo de recuperación ante desastres. Para obtener más información, consulte Configurar la recuperación ante desastres |

## Poda de datos

| Poda de datos | Opciones | Descripción |
|---|---|---|
| Reproducción de datos de sistemas e instancias | Sistema | Permite limitar la cantidad de datos de informes que se almacenan en la base de datos del servidor NetScaler ADM. Para obtener más información, consulte Configurar los ajustes de poda del sistema |
| | Eventos de instancia | Le permite limitar los mensajes de eventos que informan los datos almacenados en NetScaler ADM |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Poda de datos | Opciones | Descripción |
|---|---|---|
| | Syslog de instancia | Permite limitar la cantidad de datos de syslog almacenados en la base de datos. Para obtener más información, consulte Configurar los ajustes de syslog prune de instancia |
| | Informes de red | Le permite limitar los datos de informes de red almacenados en NetScaler ADM |

**Backup**

| Backup | Opciones | Descripción |
|---|---|---|
| Configurar la copia de seguridad del sistema y de la instancia | Sistema | Permite configurar la configuración inicial de la copia de seguridad antes de realizar una copia de seguridad del sistema. Para obtener más información, consulte Configuración de respaldo del sistema |
| | Instancia | Permite configurar opciones en NetScaler ADM para realizar copias de seguridad de una instancia de NetScaler ADC seleccionada o varias instancias. Para obtener más información, consulte Configurar los ajustes de respaldo de instancias |

**Notificaciones de eventos**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Notificaciones de eventos | Opciones | Descripción |
|---|---|---|
| Configurar la notificación y el resumen de eventos | Notificación de eventos | Puede enviar notificaciones a grupos de usuarios seleccionados para varias funciones relacionadas con el sistema. Estas funciones del sistema se organizan en categorías de eventos como SystemReboot, StatusPoll, SystemState, etc. Puede configurar NetScaler Application Delivery Management (ADM) para que le envíe notificaciones por correo electrónico, SMS o Slack. Esto garantiza que se le notifique cualquier actividad a nivel del sistema, como el exceso de almacenamiento de datos o un error de respaldo. |
| | Resumen del evento | Le permite obtener un informe consolidado de los eventos importantes del sistema y las funciones |

## Configuración SSL

| Configuración SSL | Descripción |
|---|---|
| Instalar certificado SSL | Le permite instalar el certificado SSL y el archivo de clave SSL |
| Ver certificado SSL | Le permite ver los detalles del certificado SSL |
| Configuración de SSL | Para obtener más información, consulte Configurar los ajustes de SSL |
| Certificados SSL | Le permite cargar, descargar o eliminar un certificado SSL o un archivo de clave SSL |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Configuración SSL | Descripción |
| --- | --- |
| Grupos de cifrado | Para obtener más información, consulte Configurar grupos de cifrado |

### Configurar funciones

| Configurar funciones | Descripción |
| --- | --- |
| Habilitar o inhabilitar funciones | Puede habilitar o inhabilitar funciones en NetScaler ADM. Para obtener más información, consulte Habilitar o inhabilitar las funciones de ADM |

## Configurar las opciones de copia de seguridad del sistema

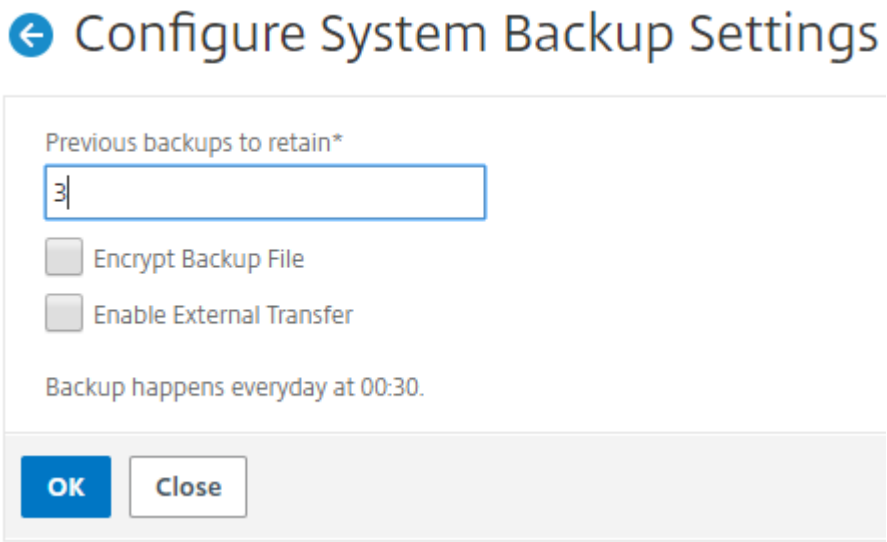
January 30, 2024

Establezca la configuración inicial de copia de seguridad del sistema antes de que necesite realizar una copia de seguridad y restaurar el sistema NetScaler Application Delivery Management (ADM).

1. Vaya a **Sistema**>**Administración del sistema**. En**Configuración de copia de seguridad**, haga clic en**Configuración de copia de seguridad del sistema**.
2. En la página **Configurar la configuración de copia de seguridad del sistema**, especifique lo siguiente:
   - Número de copias de seguridad que se deben conservar. Solo puede retener hasta 10 copias de seguridad.
   - Cifrar el archivo de copia de seguridad.
   - Habilita la transferencia externa. Puede transferir una copia de una copia del archivo de respaldo a otro sistema como medida de precaución. Para restaurar la configuración, primero debe cargar el archivo en el servidor Citrix ADM y, a continuación, realizar la operación de restauración. Especifique el servidor, el nombre de usuario y la contraseña, el puerto, el protocolo de transferencia que se va a utilizar y la ruta de acceso del directorio. Para obtener más información sobre la transferencia externa, consulteTransferir un archivo de copia de seguridad de NetScaler ADM a un sistema externo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

3. Haga clic en **Aceptar**.




## Configurar un servidor NTP

January 30, 2024

Puede configurar un servidor de Protocolo de hora de red (NTP) en NetScaler Application Delivery Management (ADM) para sincronizar su reloj con el servidor NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

**Para configurar un servidor NTP en NetScaler ADM:**

1. Vaya a **Sistema** > **Servidores NTP** y, a continuación, haga clic en **Agregar** .
2. En la página **Crear servidor NTP**, introduzca los siguientes detalles:
   - **Nombre del servidor/dirección IP**: Introduzca el nombre de dominio o la dirección IP del servidor NTP. El nombre o la dirección IP no se pueden cambiar después de agregar el servidor NTP.
   - **Intervalo mínimo de sondeo**: Especifique el valor mínimo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si quiere que el intervalo mínimo de sondeo sea de 64 segundos, que se puede expresar como 2^6, escriba 6.
   - **Intervalo máximo de sondeo**: Especifique el valor máximo del intervalo entre los mensajes NTP transmitidos, en segundos, como una potencia de 2. Por ejemplo, si desea que

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

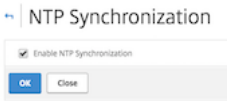
el intervalo máximo de sondeo sea de 256 segundos, que se puede expresar como 2^8, introduzca 8.

- **Identificador de clave**: introduzca el identificador de clave que se puede utilizar para la autenticación de clave simétrica con el servidor NTP. No añada un identificador de clave si decide seleccionar Autokey.
- **Clave automática**: Seleccione **Autokey** si desea utilizar la autenticación de clave pública con el servidor NTP. No seleccione si desea agregar un identificador de clave.
- **Preferido**: Seleccione esta opción si desea especificar este servidor NTP como servidor preferido para la sincronización de relojes. Esto solo se aplica si hay más de un servidor configurado.

3. Haga clic en **Crear**.

**Para habilitar la sincronización NTP en NetScaler ADM:**

1. Navegue hasta **Sistema > Servidores NTP** .
2. Haga clic en **Sincronización NTP** y active la casilla de verificación **Habilitar sincronización NTP**.
3. Haga clic en **Aceptar**.




> Nota
>
> Puede encontrar los mensajes de registro NTP en el directorio /var/log en el archivo de `/var/log/ntpd.log` archivo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Actualización de Citrix Application Delivery Management (ADM)

January 30, 2024

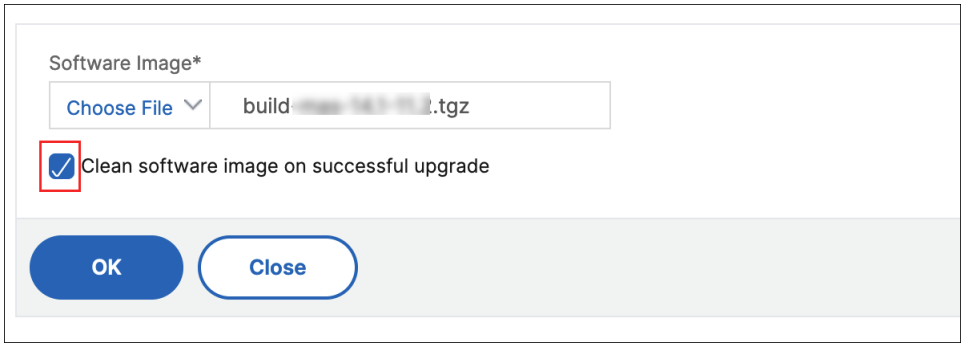
Cada versión de Citrix ADM ofrece funciones nuevas y actualizadas con mayor funcionalidad. En las notas de la versión que acompañan al anuncio de la versión se incluye una lista completa de mejoras. Tómese un momento para leer las notas de la versión antes de actualizar el software. Es importante entender el marco de licencias y los tipos de licencias antes de empezar a actualizar.

**Para actualizar Citrix ADM:**

1. Vaya a **Sistema** > **Administraciones del Sistema**. En el subtítulo **Administración del sistema**, haga clic en **Actualizar Citrix ADM**.
2. En la página Actualizar Citrix ADM, cargue un nuevo archivo de imagen seleccionando **Local** (su equipo local) o **Dispositivo**.

   > **Nota**
   >
   > Al seleccionar **Appliance**, asegúrese de que la imagen de actualización esté disponible en `/var/mps/mps_images` en NetScaler ADM.

   De formapredeterminada, la imagen de software se limpia después de una actualización correcta.
3. Haga clic en **Aceptar**.




## Cómo restablecer la contraseña para Citrix ADM

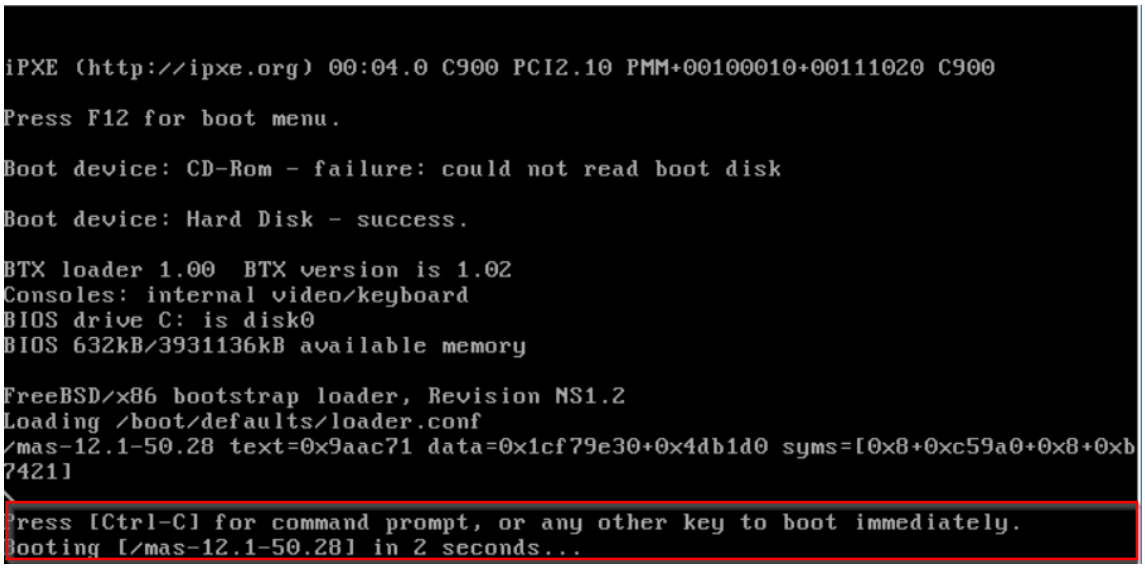
January 30, 2024

El procedimiento para restablecer la contraseña de Citrix ADM puede diferir en los hipervisores en los que está alojado. Si ha cambiado la contraseña predeterminada y quiere restablecerla, puede restablecerla reiniciando el nodo Citrix ADM.

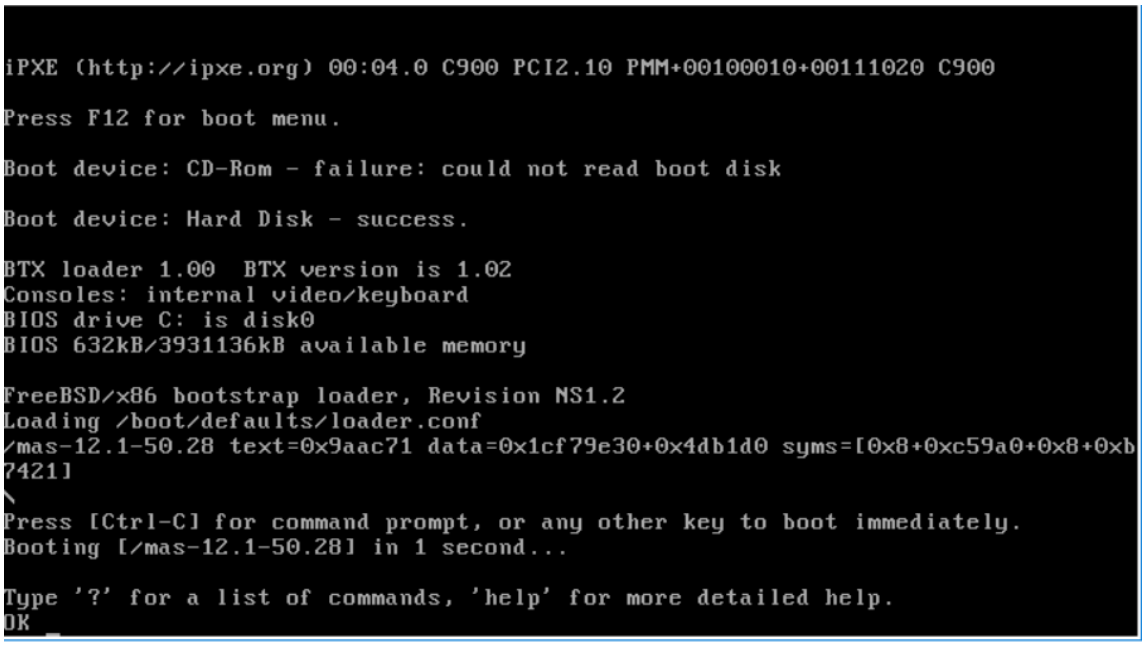
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Citrix Hypervisor con XenCenter**:

1. Inicie sesión en Citrix Hypervisor mediante XenCenter.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.




4. Ejecute el comando **boot -s** en la línea de comandos OK.




Citrix ADM se reinicia y muestra el siguiente mensaje:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
talk_to_backend: xn_num_q 1 max_q 16  err 0
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
```

5. Presiona **Entrar** para que aparezca el mensaje /u @.

```
xn0: backend features:xbd0: 122880MB <Virtual Block Device> at device/vbd/768 on
 xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@
```

6. Monte la partición flash con el siguiente comando:

```
mount dev/ad0s1a /flash
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
xenbusb_front0
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@
```

7. Cree un archivo con el siguiente comando:

   `touch /flash/mpsconfig/.recover`

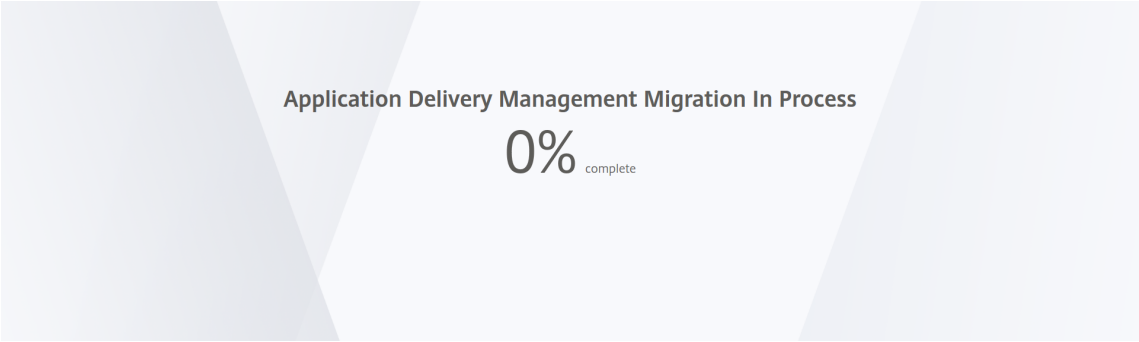
   La contraseña ahora se restablece a la contraseña predeterminada.

8. Ejecute el comando **Reboot** para reiniciar Citrix ADM.

```
xbd0: attaching as ad0
SMP: AP CPU #4 Launched!
SMP: AP CPU #5 Launched!
SMP: AP CPU #3 Launched!
SMP: AP CPU #1 Launched!
SMP: AP CPU #6 Launched!
SMP: AP CPU #2 Launched!
SMP: AP CPU #7 Launched!
vmbus_vec: 48
VM uuid: /vm/ad003cd0-2774-eac7-b10d-afb9fbf73321
UUID hex: ad003cd02774eac7b10dafb9fbf73321
GEOM: ad0s1: geometry does not match label  (16h,63s != 255h,63s) (proceeding an
yway)
Root mount waiting for: usbus0
uhub0: 2 ports with 2 removable, self powered
Root mount waiting for: usbus0
ugen0.2: <QEMU 0.10.2> at usbus0
ums0: <Endpoint1 Interrupt Pipe> on usbus0
ums0: 3 buttons and [Z] coordinates ID=0
Trying to mount root from ufs:/dev/md0c
NS-KERN /dev/md0 for compatibilty
Enter full pathname of shell or RETURN for /bin/sh:
\u@mount dev/ad0s1a /flash
\u@touch /flash/mpsconfig/.recover
\u@reboot
```

9. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

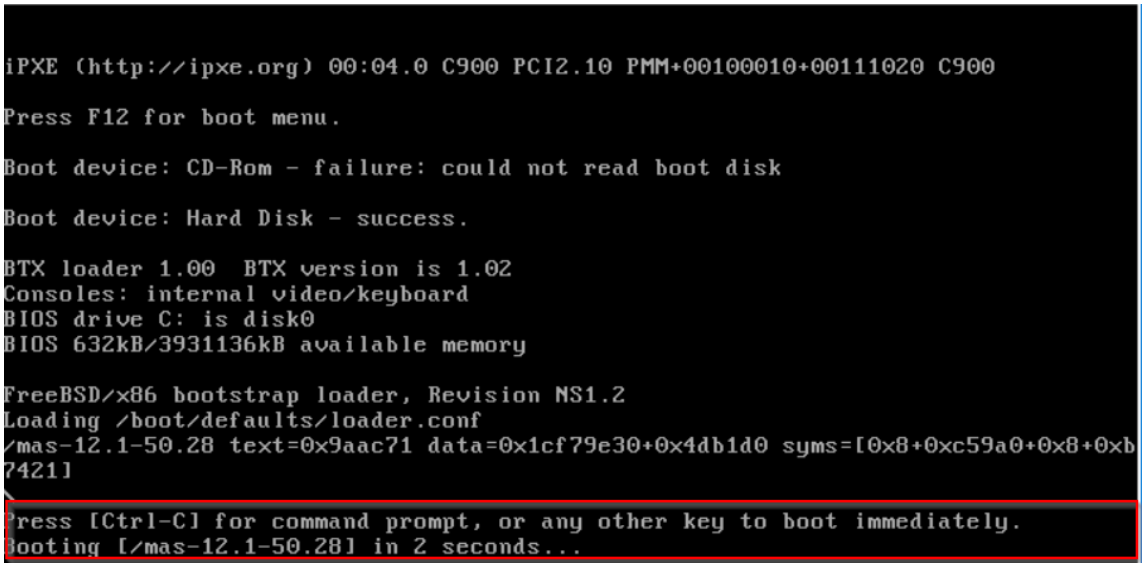



Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el Hypervisor.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie Citrix ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm -rf /etc/passwd`

**Esx mediante vSphere**:

1. Inicie sesión en ESX con vSphere.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.




4. Ejecute el comando **boot -s** en la línea de comandos OK.

   El Citrix ADM se reinicia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

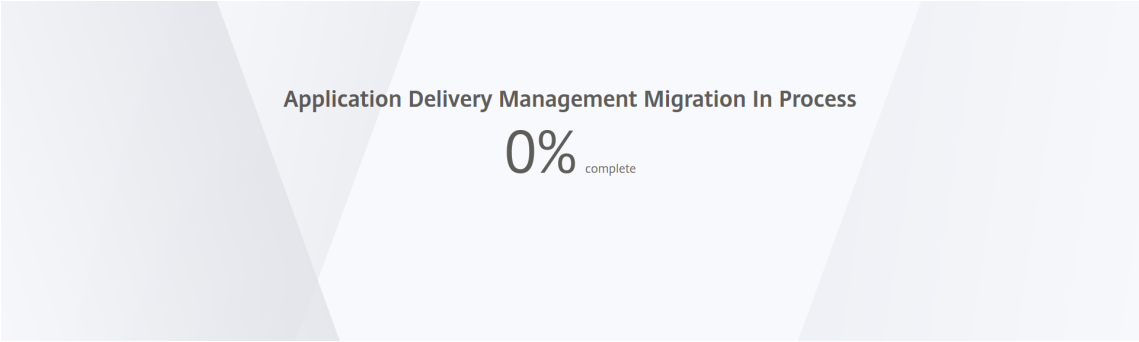
5. Presiona **Entrar** para que aparezca el mensaje /u @.
6. Monte la partición flash con el siguiente comando:

   ```
   mount dev/da0s1a /flash
   ```

7. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.
8. Ejecute el comando **Reboot** para reiniciar Citrix ADM.
9. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.

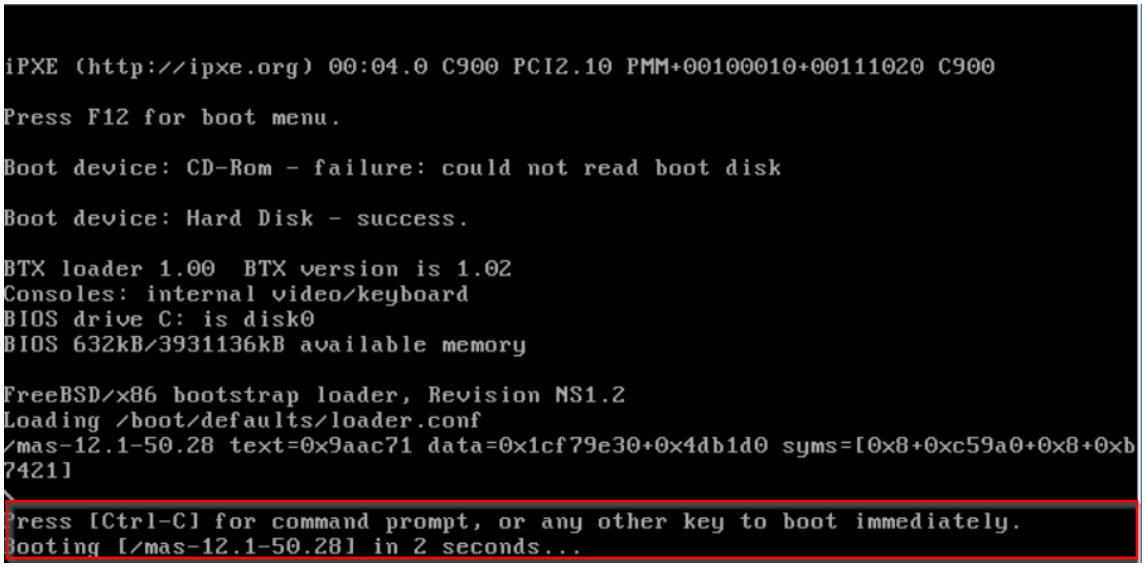
   Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el servidor ESX.

   > Nota
   >
   > Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie Citrix ADM:
   >
   > - `rm /flash/mpsconfig/master.passwd`
   > - `rm –rf /etc/passwd`

**Hyper-V mediante el administrador Hyper-V**:

1. Inicie sesión en hyper-v con el administrador de hyper-v.
2. Seleccione el nodo Citrix ADM, haga clic con el botón derecho y seleccione **Reiniciar**.
3. En la ficha **Consola**, pulse **CTL + C** para interrumpir la secuencia de arranque.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




4. Ejecute el comando **boot -s** en la línea de comandos OK.

   El Citrix ADM se reinicia.

5. Presiona **Entrar** para que aparezca el mensaje /u @.

6. Monte la partición flash con el siguiente comando:

   ```
   mount dev/ad0s1a /flash
   ```

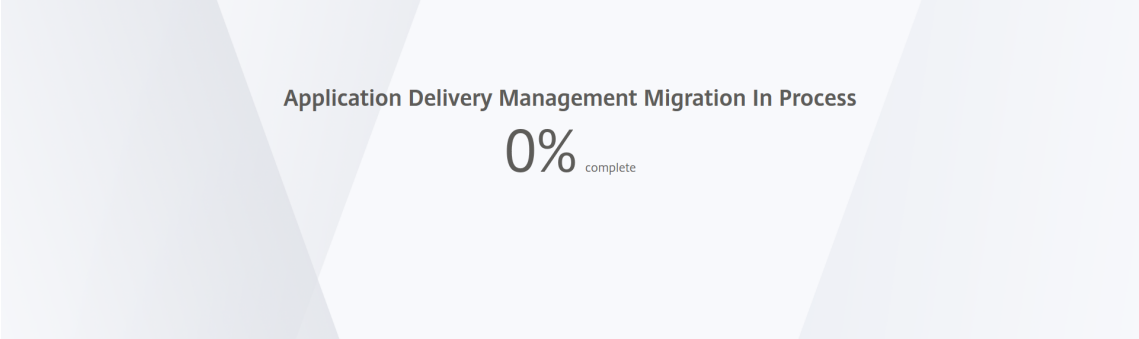
7. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.

8. Ejecute el comando **Reboot** para reiniciar Citrix ADM.

9. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.




   Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde GUI y *nsrecover/nsroot* para iniciar sesión desde el administrador de hyper-v.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie Citrix ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm -rf /etc/passwd`

**Servidor KVM Linux (SSH a servidor KVM mediante cualquier cliente SSH)**:

1. Inicie sesión en Citrix ADM mediante un cliente SSH en el servidor KVM.
2. Reinicie Citrix ADM.
3. Presione **CTL + C** para interrumpir la secuencia de arranque poco después de que aparezca el mensaje **Loading /boot/defaults/loader.conf**.
4. En el símbolo OK, ejecute el comando siguiente:

   ```
   set console='comconsole,vidconsole'
   ```

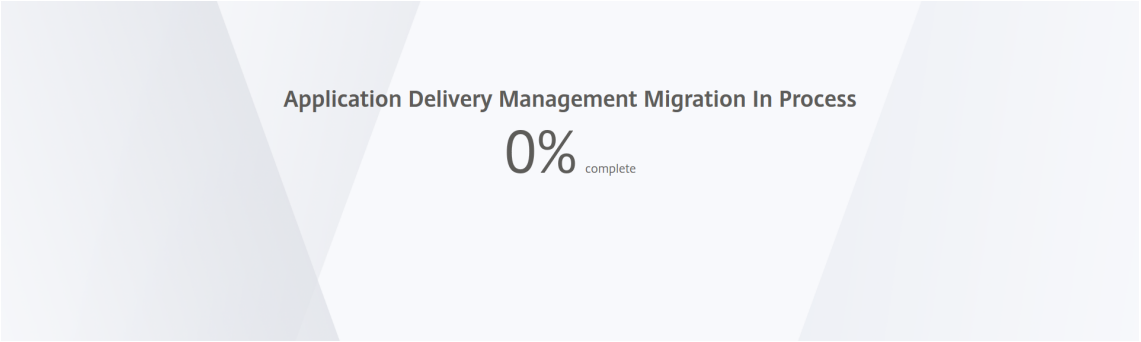
5. Ejecute el comando **boot -s** para reiniciar Citrix ADM.
6. Después de que aparezca el mensaje **Enter full path of shell o RETURN for /bin/sh:**, presione **Entrar** para obtener el mensaje /u@.
7. Monte la partición flash con el siguiente comando:

   ```
   mount dev/vtbd0s1a /flash
   ```

8. Cree un archivo con el siguiente comando:

   ```
   touch /flash/mpsconfig/.recover
   ```

   La contraseña ahora se restablece a la contraseña predeterminada.
9. Ejecute el comando **Reboot** para reiniciar Citrix ADM.
10. Acceda a la GUI de Citrix ADM y espere hasta que se complete el reinicio.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Ahora puede usar las credenciales *nsroot/nsroot* para iniciar sesión desde la GUI y *nsrecover/nsroot* para iniciar sesión desde la consola SSH.

> Nota
>
> Después de reiniciar, si la contraseña no se ha restablecido a la contraseña predeterminada, repita el mismo procedimiento (del paso 1 al paso 7). A continuación, ejecute los siguientes comandos y reinicie Citrix ADM:
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm –rf /etc/passwd`

## Configurar una NIC doble para acceder a NetScaler ADM

January 30, 2024

Puede configurar una segunda NIC para aislar el acceso de administración a NetScaler ADM. Con esta segunda función de NIC, según sus necesidades, puede elegir cómo quiere aislar el tráfico que se recibe y envía a través del Citrix ADM.

Considere un caso en el que desee aislar el tráfico para:

- Tenga todas las comunicaciones entre NetScaler ADM y sus instancias de NetScaler ADC administradas en una sola red.
- Tenga acceso de administración a NetScaler ADM en otra red.

En este caso, como administrador, puede:

- Configure una dirección IP para el tráfico entre NetScaler ADM y sus instancias administradas de NetScaler ADC.
- Configure otra dirección IP para administrar el software NetScaler ADM a fin de realizar todas las tareas administrativas del software.

> **Nota**
>
> Si NetScaler ADM está configurado como un par de HA, la dirección IP de administración configurada en la segunda NIC se asocia al nodo principal.

### Requisitos previos

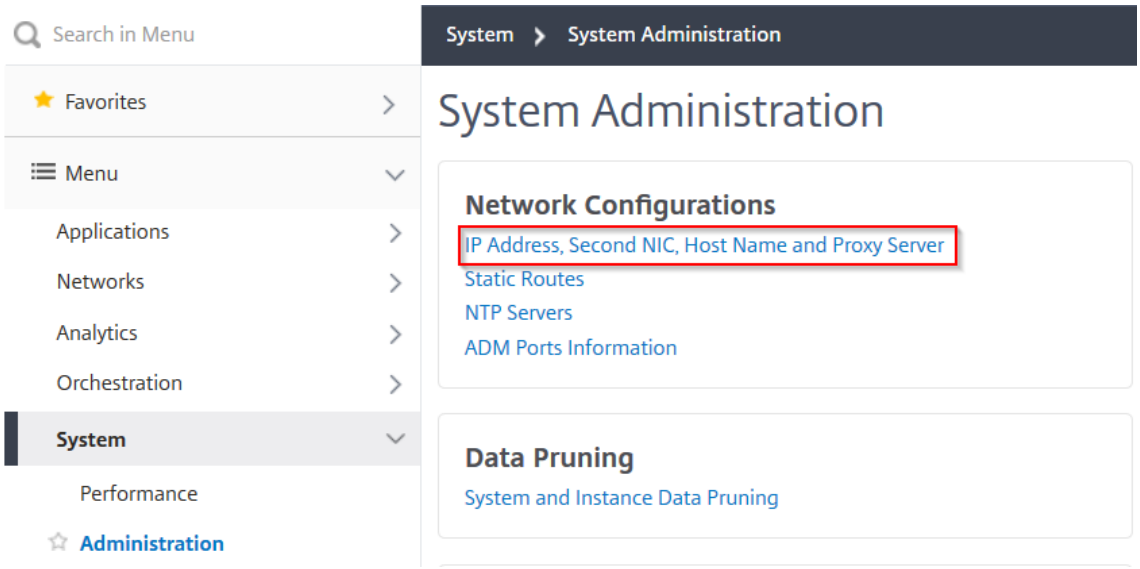
- Asegúrese de haber implementado y configurado **NetScaler ADM 13.0 Build 47.x o posterior** en el hipervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM o VMware ESXi).

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Asegúrese de haber agregado la segunda NIC al hipervisor (Citrix Hypervisor, Microsoft Hyper-V, Linux KVM o VMware ESXi).

## Configurar una segunda NIC en NetScaler ADM

1. Inicie sesión en ADM GUI.
2. Vaya a **Sistema** > **Administración**.
3. En **Configuración de red**, haga clic en **Dirección IP, Segunda NIC, Nombre de host y Servidor proxy**.




**Aparece la página de configuración de red**.

4. Haga clic en la ficha Segunda NIC y configure los siguientes parámetros:

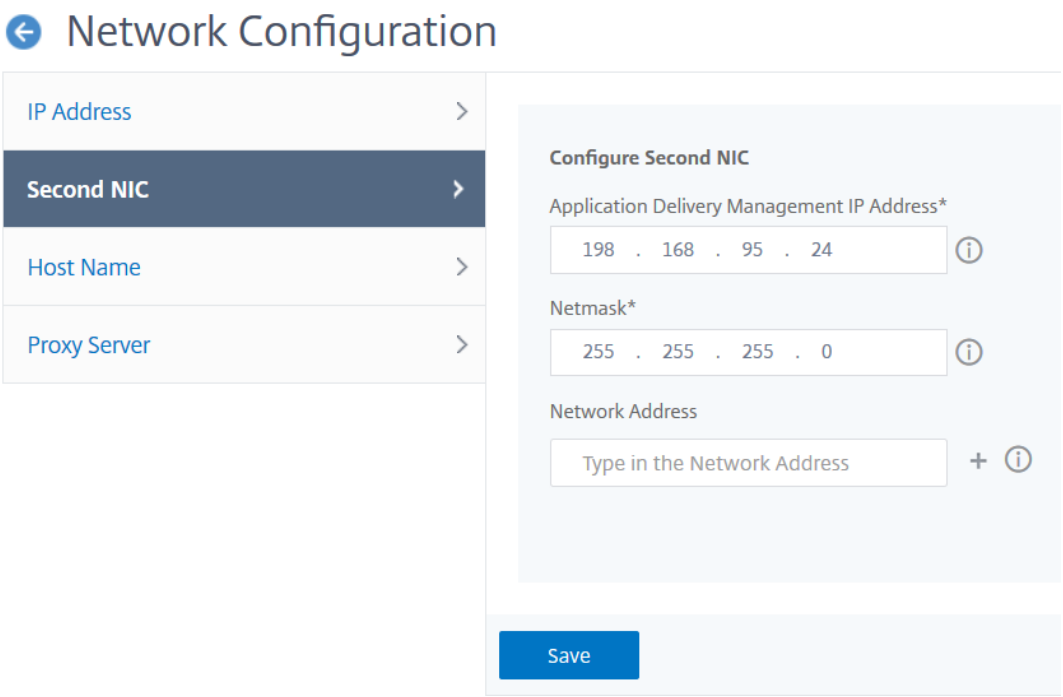
   a) **Dirección**IP de administración de entrega de aplicaciones : introduzca una dirección IP válida para acceder a Citrix ADM. Puede usar esta dirección IP para acceder a NetScaler ADM, además de la dirección IP de administración existente.

   b) **Máscara de red**: Introduzca la dirección de máscara de red para especificar el host de la red. La dirección predeterminada es 255.255.255.0.

   c) **Dirección**de red : introduzca una dirección IP para agregar una entrada de ruta para Citrix ADM. Haga clic en **+** para agregar más direcciones IP. Este campo es opcional.

   d) Haga clic en **Guardar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Configurar el intervalo de depuración de syslog

January 30, 2024

Syslog es un protocolo estándar para el registro. Tiene dos componentes: el módulo de auditoría Syslog, que se ejecuta en la instancia Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia Citrix ADC o en un sistema remoto. SYSLOG utiliza el Protocolo de datagramas de usuario (UDP) para la transferencia de datos.

Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que desea eliminar los datos de syslog.Puede especificar el número de días después de los cuales se eliminarán los siguientes datos de syslog de NetScaler Application Delivery Management (ADM):

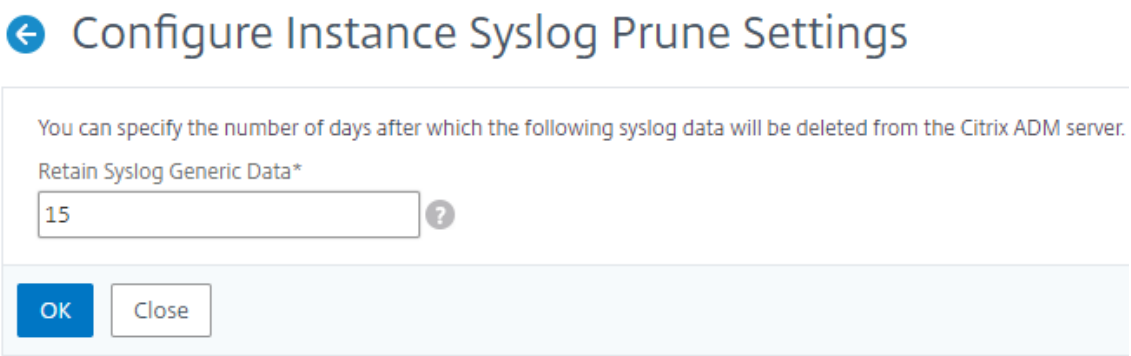
- Datos genéricos de Syslog
- Datos de AppFirewall
- Datos de NetScaler Gateway

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

También puede configurar el intervalo de poda de Citrix Gateway por tipo de syslog. Este intervalo de poda tiene prioridad sobre el intervalo de ejecución configurado para retener los datos de Citrix Gateway.

**Para configurar la configuración del intervalo de poda de syslog para NetScaler ADM:**

1. Vaya a **Sistema > Administración** .En **Poda de datos**, haga clic en **Poda de datos de sistema e instancia y, a** continuación, haga clic en **Syslog de instancia**.
2. En la página **Configurar la configuración de Syslog Prune de la instancia**, especifique **Conservar datos genéricos de Syslog (días).** Escriba el número de días durante los cuales NetScaler ADM retiene mensajes genéricos de syslog.




## Configurar los parámetros de poda del sistema y de poda de eventos

January 30, 2024

Para limitar la cantidad de datos de informes que se almacenan en la base de datos de software NetScaler Application Delivery Management (ADM), puede recortarlos. Puede especificar el intervalo para el que quiere que NetScaler ADM conserve datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

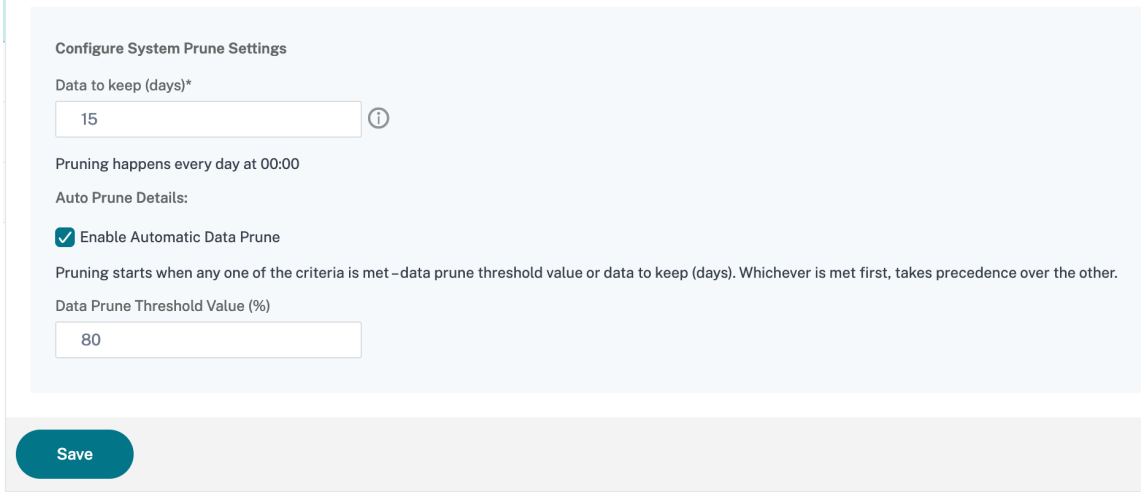
> Nota
>
> El valor que especifique no puede superar los 30 días ni ser inferior a 15 días.

**Para configurar las opciones de poda del sistema para los informes de rendimiento mediante NetScaler ADM:**

1. Vaya a **Sistema** > **Administración** . En**Reproducción de datos**, haga clic en**Reproducción de datos del sistema y de la instancia**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. En la página**Configurar configuración de ciruela del sistema**, especifique el número de días durante los que quiere conservar los datos y haga clic en**Aceptar**.



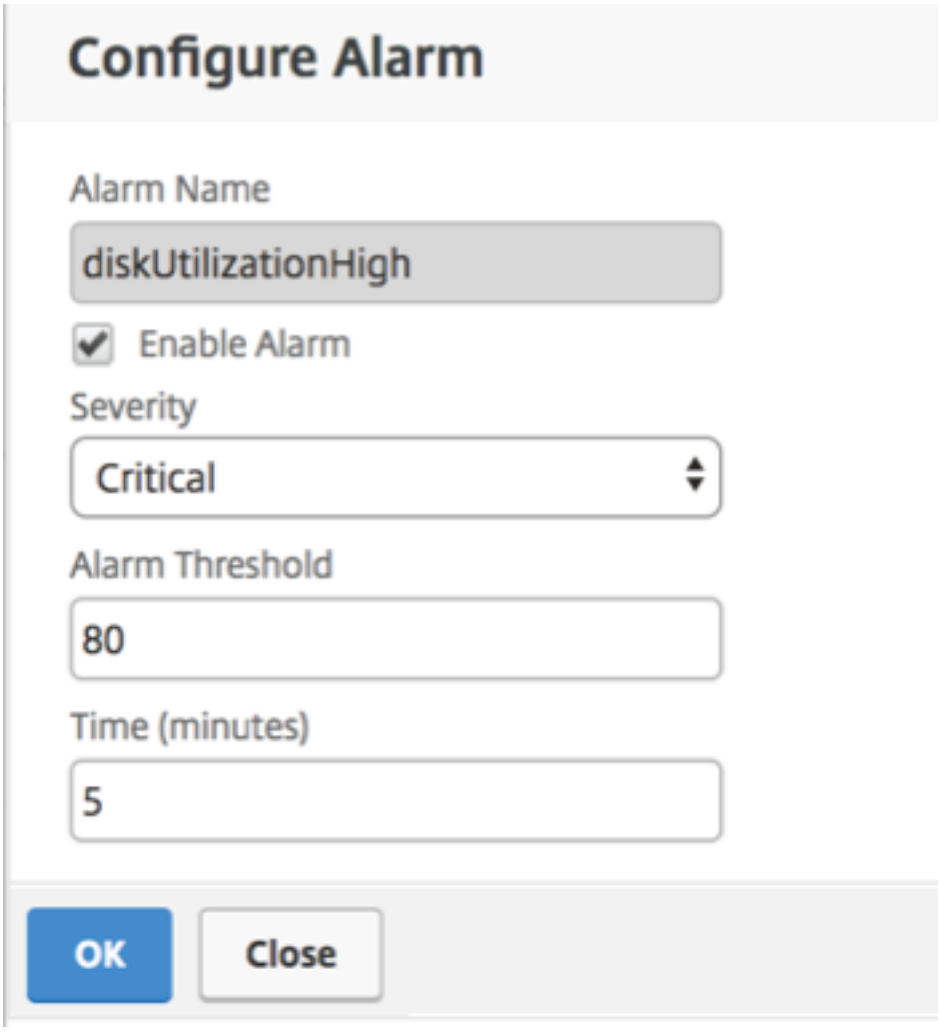

Para habilitar la poda automática,**active la casilla de verificación Habilitar recorte automático de datos**. Se activa una alarma y se envía un correo electrónico cuando el uso del disco supera el **valor umbral de purga de datos** configurado. Para cambiar el porcentaje de espacio en disco (umbral de poda), haga clic en **Modificar**.

> Nota
> La eliminación comienza cuando se cumple alguno de los criterios: valor umbral de eliminación de datos o datos que se deben conservar (días). Lo que se encuentre primero, tiene prioridad sobre el otro.

Puede configurar y habilitar la alarma**DiskUtilizationHigh**(de forma predeterminada) y especificar lo siguiente:

- **Severidad**, como Crítico.
- **Umbral**de alarma . Escriba el valor para el que se calcula la gravedad del evento.
- **Hora**. Duración (en minutos) tras la cual desea activar la alarma.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




### Configurar la configuración de podar eventos mediante NetScaler ADM

Para limitar la cantidad de datos de mensajes de eventos que se almacenan en la base de datos de NetScaler ADM, puede especificar el intervalo para el que quiere que NetScaler ADM retenga datos de informes de red, eventos, registros de auditoría y registros de tareas. De forma predeterminada, estos datos se podan cada 24 horas (a las 00.00 horas).

- Vaya a **Sistema > Administración > Poda de datos** y haga clic en **Poda de datos de Sistema e Instancia**. Haga clic en **Eventos de instancia**.
- Introduzca el intervalo de tiempo, en días, para el que desea conservar los datos en el servidor Citrix ADM y haga clic en **Guardar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Habilitar el acceso al shell para usuarios no predeterminados

January 30, 2024

Puede habilitar el acceso al shell para usuarios no predeterminados en Citrix Application Delivery Management (ADM). Puede utilizar esta función para habilitar y configurar el modo de comunicación con las instancias.

> **Nota**
>
> De forma predeterminada, el acceso a la consola está inhabilitado para los usuarios no predeterminados.

**Para habilitar el acceso al shell para usuarios no predeterminados en Citrix ADM:**

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**.
2. En **Configuración del sistema**, haga clic en **Cambiar configuración del sistema**.
3. En la página **Modificar la configuración del sistema**, configure los siguientes parámetros:
   - **Comunicación con instancias**: Seleccione el protocolo de comunicación.
   - **Acceso**seguro : habilite el acceso seguro para Citrix ADM.
   - **Habilitar el tiempo de espera de la sesión**: Especifique el período de tiempo durante el cual se mantendrá una sesión inactiva.
   - **Permitir la autenticación básica**: Permita que el servicio de administración acepte las credenciales proporcionadas mediante el Protocolo de autenticación básica.
   - **Habilitar inicio de sesión nsrecover** - Habilitar el inicio de sesión de `nsrecover` en el servicio de administración.
   - **Habilitar la descarga**de certificados : le permite descargar certificados del Citrix ADC agregado.
   - **Habilitar el acceso al shell para usuarios**que no son de nsroot : habilite el acceso al shell para los usuarios no predeterminados en Citrix ADM.
   - **Solicitar credenciales de usuario para iniciar sesión en la instancia :**permita a los usuarios introducir sus credenciales de usuario al iniciar sesión en las instancias desde Citrix ADM.
4. Haga clic en **Aceptar**.

## Recuperar servidores NetScaler ADM inaccesibles

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Citrix Application Delivery Management (ADM) ahora proporciona una herramienta de mantenimiento de bases de datos para realizar la limpieza de la base de datos del sistema. Ahora puede iniciar la herramienta Citrix ADM Utility para conectarse al sistema de archivos, eliminar algunos componentes y hacer que la base de datos sea accesible. El script de recuperación Citrix ADM es una herramienta que ayuda a recuperar espacio en el sistema de archivos borrando tablas y archivos de bases de datos antiguos o no utilizados. La herramienta le ayuda a navegar por las tablas y archivos de la base de datos en pasos sucesivos y muestra el espacio actual ocupado en el sistema de archivos por los elementos respectivos. Una vez que haya seleccionado las tablas y los archivos de la base de datos que se van a eliminar, la herramienta los elimina del sistema de archivos después de la confirmación.

## Cómo utilizar el script de recuperación de bases de datos de NetScaler ADM para una implementación independiente de NetScaler ADM

Utilice el procedimiento siguiente en un único servidor de implementación de NetScaler ADM para conectarse al sistema de archivos, eliminar algunos componentes y hacer accesible la base de datos y, a continuación, realizar las operaciones de recuperación.

1. Con un cliente SSH o la consola del hipervisor, inicie sesión en NetScaler ADM y escriba el siguiente comando:

```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. Cuando la pantalla muestre un mensaje de advertencia para detener algunos procesos NetScaler ADM, escriba “y”y presione la tecla **Intro**.

   La siguiente pantalla aparece mientras el sistema determina qué componentes de la base de datos puede eliminar sin afectar a los archivos principales del sistema.

```
-------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
-------------------------------------------------------------------------------

        This utility helps you gain disk space by performing cleanup.

                    Checking whether DB is accessible...

                              DB is accessible.

            Please wait. Gathering data. This will take some time.


                              <----------->
```

3. La pantalla muestra la lista de archivos de la base de datos. Escriba “y”y pulse la tecla Enter para iniciar el proceso de limpieza.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------  SUMMARY  ----------------------------------

                    DB component                Current size
                    ------------                ------------

                    Analytics  ------------------  184.58 MB
                    Perf Reports  ----------------  43.73 MB
                    App Summary  -----------------  12.03 MB
                    App Health Summary  -----------  6.33 MB
                    App Counter Data  -------------  5.30 MB
                    Device Syslogs  --------------  56.00 KB
                    Device Events  ---------------  40.00 KB

                    Filesystem component        Current size
                    --------------------        ------------

                    Citrix ADM Images  -----------  15.51 GB
                    Core Files  ------------------  718.37 MB
                    Citrix ADC Images  ----------  453.32 MB
                    Techsupport Bundles  --------  439.35 MB
                    Device Backup  --------------  131.79 MB
                    Citrix ADM Backup  -----------  35.21 KB
                  Citrix ADC VPX ESXi Images  -------  0.00 B
                    Citrix ADC SDX Images  ---------  0.00 B
                    Citrix ADC CPX images  ---------  0.00 B

------------------------------------------------------------------------------

        Do you wish to proceed with cleanup?
        [y/n]:
```

4. Puede seleccionar el componente específico de la base de datos que debe limpiarse y escribir el número correspondiente. Presiona la tecla **Enter**.

   Por ejemplo, para limpiar el catálogo de sistemas, seleccione la opción 8 en el menú de selección **de componentes** de la base de datos, escriba “y”y pulse la tecla **Enter** para continuar con la limpieza del catálogo del sistema.

   > **Nota** Citrix ADM incluye tablas de usuarios conocidas como catálogo del sistema. El catálogo del sistema es una ubicación de la base de datos Citrix ADM donde un sistema de administración de bases de datos relacionales almacena los metadatos del esquema, como la información sobre tablas y columnas y los registros internos. Las tablas del catálogo del sistema son como las tablas normales que pueden acumular filas infladas y muertas con el tiempo y, por lo tanto, necesitan limpiarse periódicamente para obtener un rendimiento óptimo. Es una buena práctica mantener estas tablas con regularidad. La actividad no solo libera espacio en disco, sino que también mejora el rendimiento general de la base de datos y, por lo tanto, del Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

                                DB components
                                -------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Analytics --------------- 184.58 MB
        [2]  Perf Reports ------------ 41.84 MB
        [3]  App Summary ------------- 11.84 MB
        [4]  App Health Summary ------ 6.09 MB
        [5]  App Counter Data -------- 5.09 MB
        [6]  Device Syslogs ---------- 56.00 KB
        [7]  Device Events ----------- 40.00 KB
        [8]  Clean System Catalog
        [9]  Select all
        [10] Continue without selecting

        Your input: 8
        Are you sure you want to CLEAN SYSTEM CATALOG tables?

        [y/n]: y
```

La utilidad de limpieza ofrece la opción de limpiar los componentes de la base de datos y los componentes de archivos.  Puede seleccionar cualquier componente del archivo escribiendo un número entre “1”y “9”, o escribir “11”y pulsar la tecla Enter para limpiar el componente de la base de datos.

> **Nota:**
>
> El número “11”indica que no ha seleccionado ningún componente de archivo para limpiarlo y que continúa limpiando el componente de base de datos anterior que había seleccionado anteriormente. En este ejemplo, es “catálogo del sistema”.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------

                              Filesystem components
                              ---------------------

        Enter the number corresponding to the menu entry.
        You can input multiple space separated numbers.
        E.g. '1 2 4' will select entries numbered 1, 2, and 4.

        [0]  Go back and start again
        [1]  Citrix ADM Images ------- 15.51 GB
        [2]  Core Files -------------- 718.37 MB
        [3]  Citrix ADC Images ------- 453.32 MB
        [4]  Techsupport Bundles ----- 439.35 MB
        [5]  Device Backup ----------- 131.79 MB
        [6]  Citrix ADM Backup ------- 35.21 KB
        [7]  Citrix ADC VPX ESXi Images  0.00 B
        [8]  Citrix ADC SDX Images --- 0.00 B
        [9]  Citrix ADC CPX images --- 0.00 B
        [10] Select all
        [11] Continue without selecting

        Your input: 11
```

5. Escriba “y”y vuelva a pulsar la tecla **Enter** en la pantalla de confirmación final.

```
--------------------------------------------------------------------------------
************************** Citrix ADM Cleanup Utility **************************
--------------------------------------------------------------------------------
                                FINAL CONFIRMATION

                      These components will be cleaned.

                                DB components
                                -------------

                      >>  System Catalog

        No data has been deleted yet.

        If you choose to proceed, all ADM processes will be stopped
        for the remainder of the cleanup.

        Do you wish to proceed with cleanup?
        [y/n]:
```

Se limpia el catálogo del sistema, lo que puede llevar tiempo según el tamaño de la tabla del catálogo del sistema. Una vez finalizado el proceso, aparece una pantalla de resumen.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
--------------------------------------------------------------------------------
***************************** Citrix ADM Cleanup Utility *****************************
--------------------------------------------------------------------------------
---------------------------------  SUMMARY  ----------------------------------

                                DB components
                                -------------

           Component name              Present size     Size cleared
           --------------              ------------     ------------

           System Catalog  -------------  189.15 MB  -------  0.00 B
        Cleanup complete.
        Note that even empty tables in DB may appear to occupy some
        space, this is expected.


        To prevent potential unpredictable behavior, we STRONGLY recommend
        rebooting the ADM now.

        Do you want to REBOOT the ADM?
        [y/n]:
```

6. Escriba «y» y pulse la **tecla**Intro para reiniciar Citrix ADM.

   Asegúrese de reiniciar Citrix ADM después de limpiar el sistema. Espere unos 30 minutos para que las operaciones internas de la base de datos se completen después de que NetScaler ADM se haya reiniciado. A continuación, debería poder conectarse a la base de datos Citrix ADM. Si no es así, vuelva a ejecutar el script de recuperación para liberar más espacio. Cuando Citrix ADM esté en funcionamiento, debería funcionar según lo esperado.

   > **Nota**
   >
   > El tamaño actual de la tabla de catálogo del sistema nunca es igual a cero después de la limpieza. Esto se debe a que solo se eliminan las filas vacías de la tabla y es posible que la tabla tenga algunas entradas válidas incluso después de limpiarlas.

### Cómo utilizar el script de recuperación de bases de datos Citrix ADM para una implementación de alta disponibilidad de Citrix ADM

El sistema de bases de datos para los servidores Citrix ADM en una implementación de alta disponibilidad está en modo de sincronización continua. Al utilizar la nueva herramienta de recuperación de bases de datos, no es necesario replicar el procedimiento en ambos servidores Citrix ADM.

1. Con un cliente SSH o la consola de un hipervisor, inicie sesión en el nodo principal.
2. Ejecute este comando:

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. Siga el procedimiento del paso 2 disponible para el script de recuperación de implementación independiente de NetScaler ADM

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

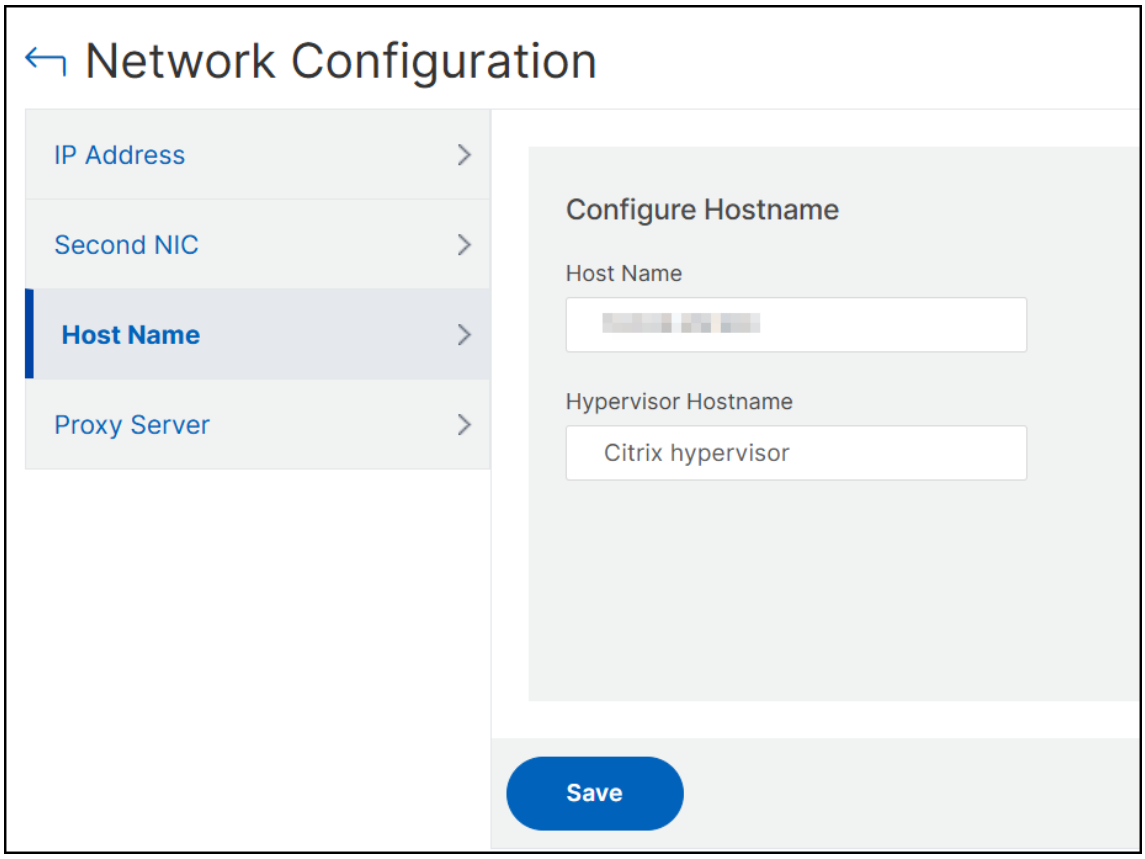
## Asignar un nombre de host a un servidor NetScaler ADM

January 30, 2024

Para identificar un servidor de NetScaler Application Delivery Management (ADM), puede asignarle un nombre de host. El nombre del host se muestra en la licencia universal de NetScaler ADM.

**Para asignar un nombre de host a un servidor de NetScaler ADM:**

1. En NetScaler ADM, vaya a **Sistema** > **Administración del sistema**.
2. En **Configuración del sistema**, haga clic en **Cambiar nombre de host**.
3. En la página **Configurar nombre de host**, escriba un nombre de host y haga clic en **Aceptar**.

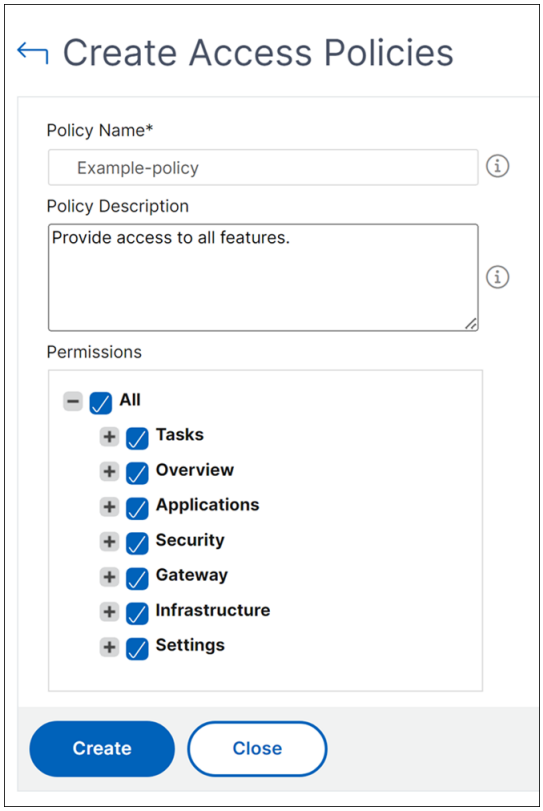



## Copia de seguridad y restauración del servidor NetScaler ADM

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede realizar copias de seguridad periódicas de su servidor Citrix ADM. Puede realizar copias de seguridad y restaurar los archivos de configuración, los detalles de la instancia, los datos del sistema, etc.

> **Importante**
>
> Citrix recomienda restaurar el servidor ADM mediante una copia de seguridad de la misma versión. Por ejemplo, si la versión de ADM es 13.0, use la copia de seguridad de ADM 13.0 para restaurar el servidor.
>
> El acceso de los usuarios para hacer copias de seguridad y restaurar el servidor ADM es limitado. La página **Sistema > Archivos de copia** de seguridad solo aparece para los usuarios que tienen acceso a todas las funciones de ADM. Un usuario puede acceder a esta página solo si su directiva de acceso tiene todos los permisos. Normalmente, los superusuarios tienen acceso a todas las funciones de ADM.
>
> 
> 
>
> Para obtener más información, consulte Configurar directivas de acceso.

Antes de actualizar, realice una copia de seguridad de los archivos de configuración del servidor ADM por razones de precaución.

La copia de seguridad incluye los siguientes componentes:

- Archivos de configuración de Citrix ADM:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

  - SNMP
  - Archivos de configuración del servidor Syslog
  - archivos NTP
  - Certificados de SSL
  - Archivos del Centro de control
- Copias de seguridad de las instancias de Citrix ADC que administra el servidor Citrix ADM.
- Plantillas de auditoría de configuración.
- Datos del sistema almacenados en la base de datos:
  - Lista de arrendatarios y usuarios creada.
  - Configuración del servidor de autenticación externo (LDAP, RADIUS y otros).
  - Se crearon trabajos de configuración y plantillas de trabajo.
- Datos de infraestructura y aplicaciones almacenados en la base de datos:
  - Datos de instancias de Citrix ADC agregadas y administradas.
  - Detalles del perfil de la instancia, detalles de la versión, detalles del grupo de instancias, etc.
  - Aplicación estática (grupo de servidores virtuales) creada por el administrador.
- Configuración SNMP.

> **Nota**
>
> Los datos de Analytics, los eventos, las licencias de ADM y los mensajes de syslog se excluyen de la copia de seguridad.

## Respaldar la configuración de NetScaler ADM

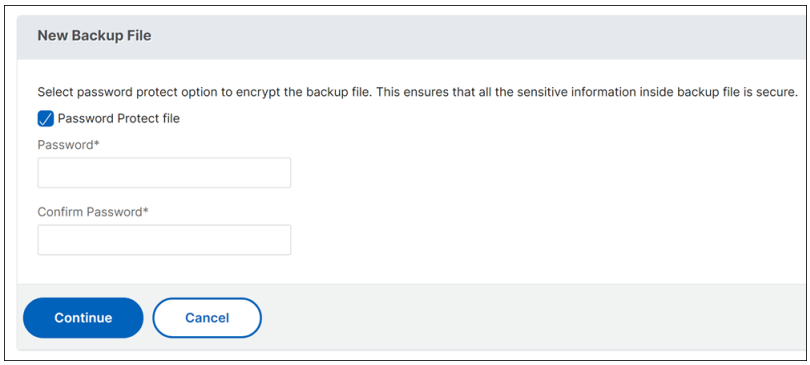
De forma predeterminada, el servidor Citrix ADM hace copias de seguridad de la configuración cada 24 horas (a las 00:30 horas). También puede programar y seleccionar la hora de la copia de seguridad. Además, puede mover una copia del archivo de la copia de seguridad a otro sistema.

La copia de seguridad se almacena como un archivo TAR comprimido que también se puede cifrar. De forma predeterminada, se conservan tres archivos de respaldo en el servidor. Para evitar problemas de espacio bajo en disco, puede almacenar un máximo de 10 archivos de copia de seguridad en el servidor NetScaler ADM. Sin embargo, Citrix recomienda almacenar algunas copias de los archivos de copia de seguridad en el servidor o transferir los archivos a otro sistema como medida de precaución.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para hacer una copia de seguridad de una configuración NetScaler ADM:**

1. Vaya a **Sistema > Archivos de respaldo**y, a continuación, haga clic en **Realizar copia**de seguridad
2. Para cifrar el archivo de copia de seguridad, active la casilla de verificación **Archivo Proteger con contraseña** y, a continuación, proporcione una contraseña para cifrar el archivo.




## Transferir un archivo de copia de seguridad NetScaler ADM a un sistema externo

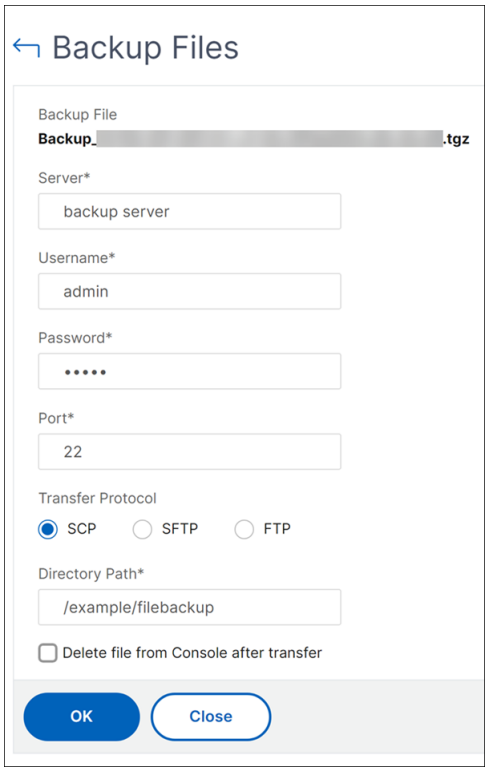
Puede transferir una copia del archivo de copia de seguridad a otro sistema como medida de precaución. Cuando quiera restaurar la configuración, primero cargue el archivo en el servidor NetScaler ADM y, a continuación, realice la operación de restauración.

**Para transferir un archivo de copia de seguridad de Citrix ADM:**

1. Vaya a**Sistema > Archivos de copia de seguridad**.
2. Seleccione el archivo de copia de seguridad que quiere mover a otro sistema y, a continuación, haga clic en**Transferir**.
3. En la página **Archivos de respaldo**, especifique los siguientes parámetros:
   - **Servidor**: Dirección IP del sistema al que desea transferir el archivo de la copia de seguridad.
   - **Nombre de usuario y contraseña**: Credenciales de usuario del nuevo sistema en el que se copian los archivos de la copia de seguridad.
   - **Puerto**: Número de puerto del sistema al que se transfieren los archivos.
   - **Protocolo de transferencia**: Protocolo que se utiliza para realizar la transferencia del archivo de respaldo. Puede seleccionar los protocolos SCP, SFTP o FTP para transferir el archivo de la copia de seguridad.
   - **Ruta del directorio**: La ubicación a la que se transfiere el archivo de copia de seguridad en el nuevo sistema.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

4. Puede eliminar el archivo de copia de seguridad de NetScaler ADM después de la transferencia activando la casilla de verificación **Eliminar archivo de Administración de entrega de aplicaciones después de la transferencia**.
5. Haga clic en **Aceptar** para realizar la transferencia.




> **Nota**
>
> Para guardar una copia del archivo de copia de seguridad en su sistema local, vaya a **Sistema > Archivos de copia**de seguridad, seleccione el archivo que quiere copiar y, a continuación, haga clic en **Descargar**.

## Restaurar la configuración de NetScaler ADM desde un archivo de copia de seguridad

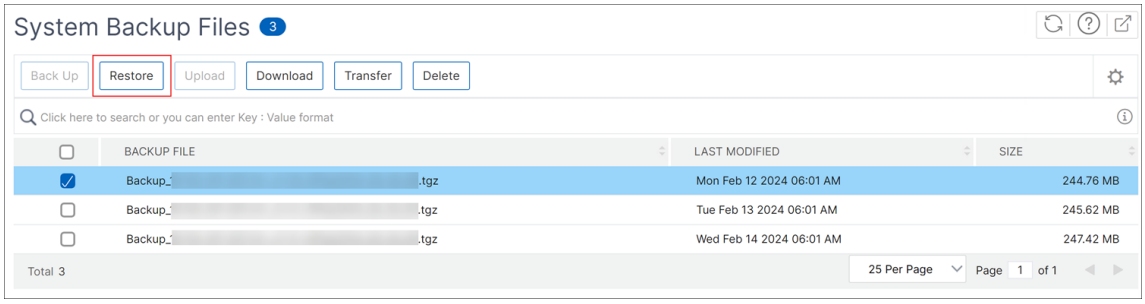
Al restaurar la configuración de Citrix ADM a partir de un archivo del que se hizo una copia de seguridad anteriormente, la operación de restauración desactiva el archivo de copia de seguridad y, a continuación, restaura la configuración. La operación de restauración elimina la configuración existente y la reemplaza por la configuración del archivo de copia de seguridad.

> **Nota**
>
> La operación de restauración falla si se cambia el nombre del archivo de copia de seguridad o si se modifica el contenido del archivo de respaldo.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Para restaurar una configuración de NetScaler ADM a partir de un archivo de copia de seguridad:**

1. Navegue hasta **Sistema > Archivos** de respaldo .
2. Seleccione el archivo de copia de seguridad que quiere restaurar y, a continuación, haga clic en **Restaurar**.




3. En el cuadro de diálogo de confirmación, haga clic en **Sí**.

> **Nota**
>
> Para restaurar la configuración a partir de un archivo de copia de seguridad almacenado en un sistema externo, cargue el archivo de copia de seguridad en el servidor ADM antes de realizar la operación de restauración. Para cargar el archivo, vaya a **Sistema > Archivos de copia**de seguridad y, a continuación, haga clic en **Cargar**.

## Ver información de auditoría

January 24, 2024

Syslog es un protocolo estándar para el registro. Tiene dos componentes: el módulo de auditoría Syslog, que se ejecuta en la instancia Citrix Application Delivery Controller (ADC), y el servidor Syslog, que puede ejecutarse en el sistema operativo (SO) FreeBSD subyacente de la instancia Citrix ADC o en un sistema remoto. SYSLOG utiliza el Protocolo de datagramas de usuario (UDP) para la transferencia de datos.

Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

Puede supervisar los mensajes de syslog que genera un dispositivo Citrix ADC si configura el dispositivo para redirigir los mensajes de syslog a Citrix Application Delivery Management (ADM). Puede programar un trabajo para crear servidores syslog que generen diferentes tipos de datos syslog mediante la función de plantillas integradas de Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Primero, configure un servidor syslog al que la instancia pueda enviar información de registro. A continuación, especifique el formato de fecha y hora para grabar los mensajes de registro.

**Para configurar un servidor syslog en Citrix ADM:**

1. Vaya a**Sistema**>**Auditoría.** En **Resumen de configuración**, seleccione Servidores **Syslog.** O puede ir a **Sistema** > **Auditoría > ServidoresSyslog**.
2. **En la página del**servidor Syslog**, haga clic en Agregar.**
3. En la página **Crear servidor de Syslog**, introduzca los siguientes valores:
   - **Nombre**: Nombre del servidor syslog.
   - **Dirección IP**: Dirección IP del servidor syslog.
   - **Puerto: puerto** del servidor Syslog.
4. Elija los niveles de registro (Todos, Ninguno o Personalizado). En consecuencia, seleccione los niveles de gravedad.
5. Haga clic en **Create**.

**Para configurar el formato de fecha y hora de syslog en Citrix ADM:**

1. Vaya a**Sistema**>**Auditoría.** En**Resumen de configuración**, seleccione Servidores**Syslog.**
2. **En la página**Servidor Syslog, seleccione un servidor**syslog y, a continuación, haga clic en Parámetros de Syslog.**
3. En la página**Configurar parámetros de Syslog**, especifique el formato de fecha y hora.
4. Haga clic en **Aceptar**.

**Para ver los mensajes de syslog en Citrix ADM:**

Ahora puede ver todos los mensajes de syslog generados en las instancias administradas de Citrix ADC si ha configurado la instancia para redirigir los mensajes de syslog al servidor Citrix ADM. Los mensajes de syslog se almacenan en la base de datos del servidor Citrix ADM de forma centralizada y estarán disponibles en el Visor de Syslog para fines de auditoría. Puede consolidar esta información de registro y obtener informes para el análisis a partir de los datos recopilados.

Puede filtrar esta información por módulo, tipo de evento y gravedad. También puede configurar syslog para registrar diferentes tipos de eventos.

**Para ver el**visor de Syslog**, vaya a**Sistema**> Auditoría.** En la página**de auditoría**, en Mensajes de**auditoría, seleccione Mensajes**de**Syslog**. Elija los filtros adecuados para ver los mensajes de registro del sistema.

## Configurar la configuración de SSL

January 30, 2024

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

SSL (Secure Socket Layer) y TLS (Transport Layer Security) son protocolos de redes de seguridad de uso común que proporcionan una comunicación cifrada entre los usuarios y los servidores. Puede configurar los parámetros de SSL en Citrix Application Delivery Management (ADM) y especificar el tipo de clientes que se conectan al sistema.

**Para configurar los parámetros de SSL para Citrix ADM:**

1. Vaya a **Sistema** > **Administración del sistema**. En **Configuración del sistema**, haga clic en **Configurar la configuración de SSL**.
2. En la página de **configuración SSL**, revise la configuración actual del protocolo y los conjuntos de cifrado aplicados al sistema.
3. Para modificar la configuración del protocolo, vaya a **Editar configuración** > **Configuración de protocolo** y realice los cambios que desee.
4. Para modificar los conjuntos de cifrado aplicados, vaya a **Editar configuración** > **Suites de cifrado** y realice los cambios que desee.
5. Haga clic en Aceptar **y**, a continuación, en **Cerrar** .

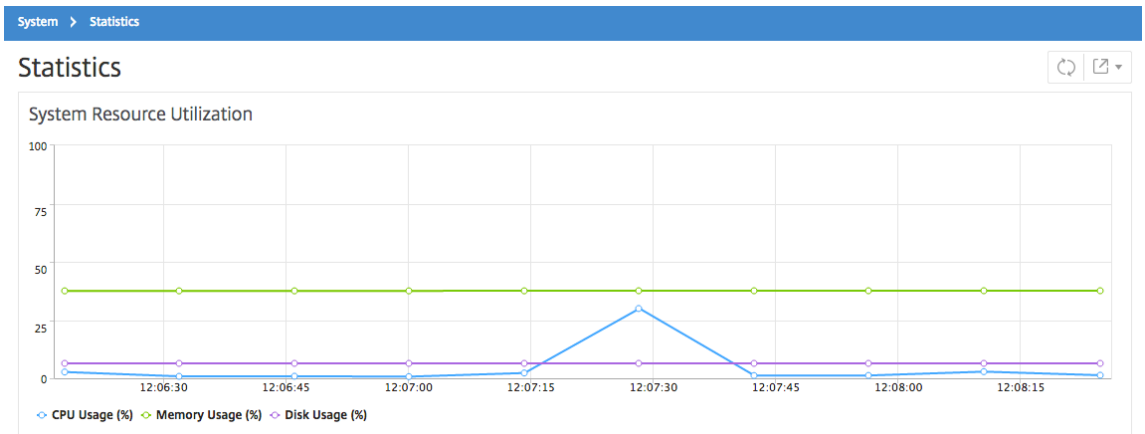
## Supervisar el uso de CPU, memoria y disco

January 24, 2024

Puede utilizar la información mantenida en los registros y las estadísticas. Esta información también se muestra en los informes que ayudan a configurar y mantener Citrix Application Delivery Management (ADM).

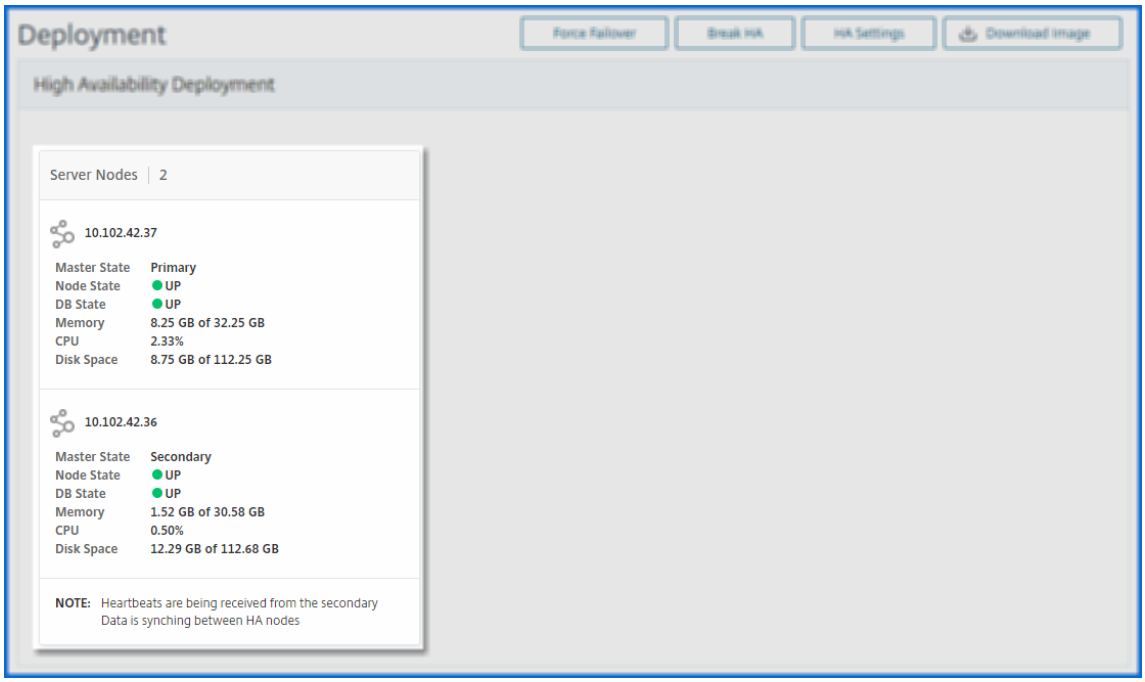
Para supervisar el uso de la CPU, la memoria y el disco,

- **Implementación independiente.** Vaya a **Sistema** > **Estadísticas**. Puede ver gráficos de utilización de CPU, memoria y disco en tiempo real.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Implementación de alta disponibilidad.** Navegue hasta **Sistema** > **Implementación** . Las estadísticas de la memoria, la CPU, el espacio en disco y las instancias administradas se muestran numéricamente como se muestra en la siguiente ilustración:




## Configurar las opciones de notificación

January 24, 2024

Puede seleccionar un tipo de notificación para recibir notificaciones para las siguientes funciones:

- **Eventos**: lista de eventos que se generan para las instancias de NetScaler ADC. Para obtener más información, consulte Agregar acciones de reglas de eventos.
- **Licencias**: lista de licencias que están actualmente activas, a punto de caducar, etc. Para obtener más información, consulte Caducidad de la licencia de NetScaler ADM.
- **Certificados SSL**: Lista de certificados SSL que se agregan a instancias NetScaler ADC. Para obtener más información, consulte Caducidad del certificado SSL

ADM admite los siguientes tipos de notificación:

- Correo electrónico
- SMS
- Slack
- PagerDuty

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- ServiceNow

Para cada tipo de notificación, la GUI de ADM muestra la lista de distribución o el perfil configurados. El ADM envía notificaciones a la lista de distribución o perfil seleccionado.

## Crea una lista de distribución de correo electrónico

Para recibir notificaciones por correo electrónico para las funciones de ADM, debe agregar un servidor de correo electrónico y una lista de distribución.

Realice los siguientes pasos para crear una lista de distribución de correo electrónico:

1. Vaya a **Sistema > Notificaciones** .
2. En **Correo electrónico**, haga clic en **Agregar**.
3. En **Crear lista de distribución de correo electrónico**, especifique los siguientes detalles:
    - **Nombre**: Especifique el nombre de la lista de distribución.
    - **Servidor de correo electrónico**: Seleccione el servidor de correo electrónico que envía la notificación por correo electrónico. Si desea agregar un servidor de correo electrónico, haga clic en **Agregar**.
    - **Desde**: Especifique la dirección de correo electrónico desde la que ADM debe enviar los mensajes.
    - **Para**: Especifique las direcciones de correo electrónico a las que ADM tiene que enviar mensajes.
    - **Cc**: Especifique las direcciones de correo electrónico a las que ADM debe enviar copias de los mensajes.
    - **Bcc**: Especifique las direcciones de correo electrónico a las que ADM debe enviar copias de los mensajes sin mostrar las direcciones.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

4. Haga clic en **Crear**.

Repita este procedimiento para crear varias listas de distribución de correo electrónico. La ficha **Correo electrónico** muestra todas las listas de distribución de correo electrónico presentes en

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

ADM.

### Crea una lista de distribución de SMS

Para recibir notificaciones por SMS para las funciones de ADM, debe agregar un servidor SMS y números de teléfono.

Realice los siguientes pasos para configurar los ajustes de notificación SMS:

1. Vaya a **Sistema > Notificaciones** .
2. En **SMS**, haga clic en **Agregar**.
3. En **Crear lista de distribución de SMS**, especifique los siguientes detalles:
   - **Nombre**: Especifique el nombre de la lista de distribución.
   - **Servidor de SMS**: seleccione el servidor de SMS que envía la notificación por SMS.
   - **Para**: Especifique el número de teléfono al que ADM debe enviar mensajes.
4. Haga clic en **Crear**.

Repita este procedimiento para crear varias listas de distribución de SMS. La ficha **SMS** muestra todas las listas de distribución de SMS presentes en ADM.

### Crear un perfil de Slack

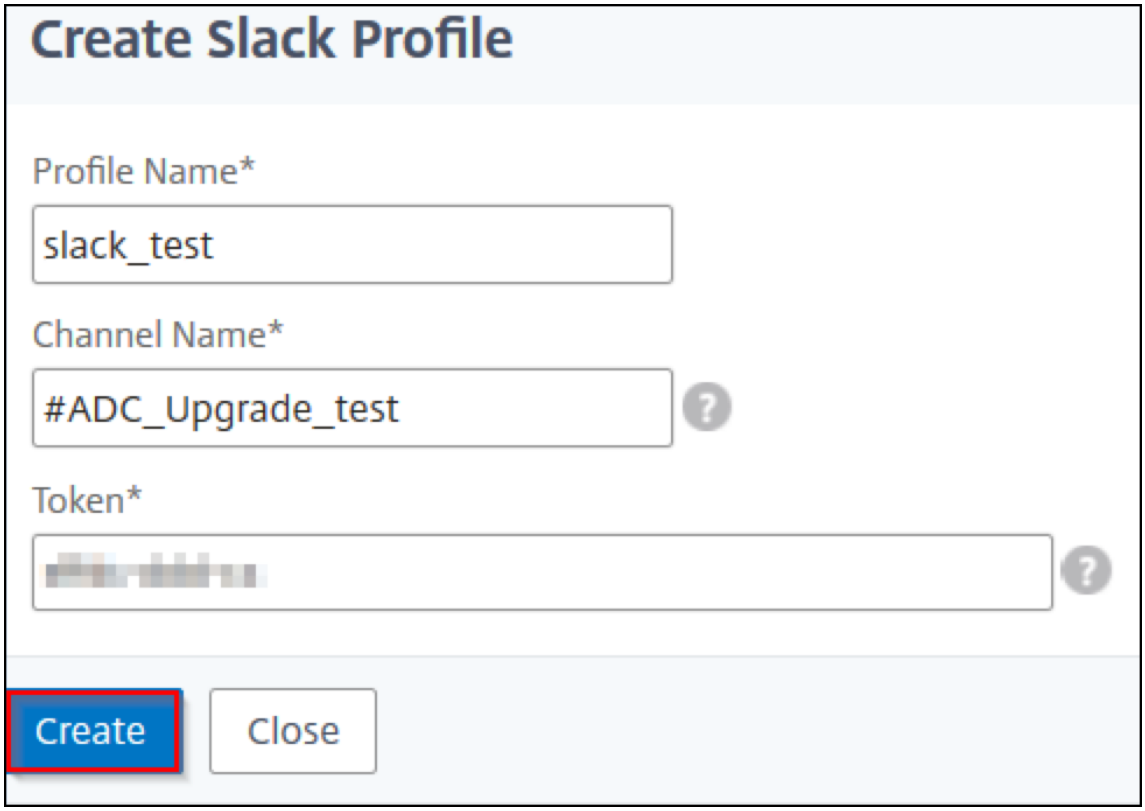
Para recibir notificaciones de Slack sobre las funciones de ADM, debes crear un perfil de Slack.

Realice los siguientes pasos para crear un perfil de Slack:

1. Vaya a **Sistema > Notificaciones** .
2. En **Slack**, haga clic en **Agregar**.
3. En **Crear perfil de Slack**, especifica los siguientes detalles:
   - **Nombre de perfil**: especifique el nombre del perfil. Este nombre aparece en la lista de perfiles de Slack.
   - **Nombre del canal**: Especifica el nombre del canal de Slack al que ADM debe enviar las notificaciones.
   - **URL del webhook**: especifique la URL del webhook del canal. Los webhooks entrantes son una forma sencilla de publicar mensajes de fuentes externas en Slack. La URL está vinculada internamente al nombre del canal. Además, todas las notificaciones de eventos se envían a esta URL se publican en el canal Slack designado. Un ejemplo de webhook es

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

el siguiente: https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK




4. Haga clic en **Crear**.

Repite este procedimiento para crear varios perfiles de Slack. La ficha **Slack** muestra todos los perfiles de Slack presentes en ADM.

### Crear un perfil de PagerDuty

Puede agregar un perfil de PagerDuty para supervisar las notificaciones de incidentes en función de las configuraciones de PagerDuty. PagerDuty le permite configurar notificaciones a través de correo electrónico, SMS, notificaciones push y llamadas telefónicas en un número registrado.

Antes de agregar un perfil de PagerDuty en NetScaler ADM, asegúrese de haber completado las configuraciones necesarias en PagerDuty. Para empezar a usar PagerDuty, consulta la documentación de PagerDuty.

Realice los siguientes pasos para crear un perfil de PagerDuty:

1. Vaya a **Sistema > Notificaciones** .
2. En **PagerDuty**, haga clic en **Agregar**.
3. En **Crear perfil de PagerDuty**, especifique los siguientes detalles:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Nombre de perfil**: especifique un nombre de perfil de su elección.
- **Clave de integración**: especifique la clave de integración. Puede obtener esta clave en su portal PagerDuty.

4. Haga clic en **Crear**.

Para obtener más información, consulte Servicios e integraciones en la documentación de PagerDuty.

Repita este procedimiento para crear varios perfiles de PagerDuty. La ficha **PagerDuty** muestra todos los perfiles PagerDuty presentes en ADM.

### Ver el perfil de ServiceNow

Si quiere habilitar las notificaciones de ServiceNow para eventos de NetScaler ADC y eventos de ADM, debe integrar NetScaler ADM con ServiceNow mediante el conector ITSM. Para obtener más información, consulte Integrar NetScaler ADM con la instancia de ServiceNow.

Realice los siguientes pasos para ver y verificar el perfil ServiceNow:

1. Vaya a **Sistema > Notificaciones** .
2. En **ServiceNow**, seleccione el perfil **Citrix_Workspace_SN** de la lista.
3. Haga clic en **Probar** para generar automáticamente un tíquet de ServiceNow y verificar la configuración.

   Si quiere ver los tíquets de ServiceNow en la GUI de Citrix ADM, seleccione **Tíquets de ServiceNow**.

## Generar un archivo de soporte técnico

January 30, 2024

Citrix recomienda generar un archivo de datos y estadísticas de NetScaler Application Delivery Management (ADM) antes de ponerse en contacto con el soporte técnico para solucionar un problema. El archivo es un archivo TAR que puede enviar al equipo de soporte técnico.

> **Nota**
>
> Para los servidores NetScaler ADM en modo de alta disponibilidad, puede generar un archivo de soporte técnico desde cualquiera de los servidores. Citrix recomienda no utilizar la dirección IP

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> del servidor virtual de equilibrio de carga para generar el archivo de soporte técnico.

**Para configurar y enviar un archivo de soporte técnico desde NetScaler ADM:**

1. Vaya a **Sistema** > **Diagnóstico** > **Soporte técnico y, a**continuación, haga clic en **Generar archivo de soporte técnico**.
2. En la página **Generar archivo de soporte**, seleccione las siguientes opciones:

- **Recopilar registros de depuración**: Seleccione esta opción para recopilar `afdecoder` registros.
- **Duración**: Introduzca la duración para la que se deben recopilar los registros de depuración. Solo verá esta opción si activa la opción **Recopilar registros de depuración**.
- **Recopilar distribución de datos**: Seleccione esta opción para recopilar registros distintos y diversos de la base de datos.

```
The archive file is created as a TAR file.

For example, the archive file that is created might be named as
    follows:   Citrix_ADM_<ADM_IP_address>_<DDMMYY>_<time_stamp>.
    tar.gz
```

1. Puede enviar los archivos de soporte técnico al equipo de soporte de dos maneras:

   a) Puede descargar el archivo de la GUI de ADM a su almacenamiento local y, a continuación, utilizar un navegador web para cargarlo en CIS.

   b) También puede cargar los archivos de soporte técnico al sitio web de Citrix Insight Services (CIS) ejecutando un script en la consola ADM.

      i. Mediante SSH, inicie sesión en la consola ADM.

      ii. Cambie al símbolo del Shell y escriba:

      */mps/collector_upload.pl*

El comando completo se muestra a continuación con los atributos que debe proporcionar:

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
    proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
     <sr>] [-description <description>] [-debug] <file>
```

La ventaja de ejecutar el script de Perl es que no tiene que descargar el archivo de soporte técnico de ADM a su sistema local y luego subirlo a CIS. Como opción, puede cargar el archivo en CIS directamente mediante un proxy de la consola ADM.

Asegúrese de tener una cuenta en CIS. Puede usar las credenciales de su cuenta de Citrix para cargar archivos a CIS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

¿Qué pasa si no tiene un servidor proxy? ¿O qué pasa si tiene algunos problemas con los proxies de reenvío SSL? (Esto puede ocurrir si el script de Perl no confía en el certificado raíz del servidor proxy) . Aún puede cargar el archivo directamente desde el shell ADM a CIS.

> **Nota:**
>
> Puede seguir descargando el archivo y enviarlo por correo electrónico al equipo de soporte técnico de Citrix en caso de que ADM no pueda cargar el archivo a CIS desde la consola. O bien, puede descargar el archivo de ADM a su almacenamiento local y, a continuación, utilizar un navegador web para cargarlo en CIS.

## Configurar un grupo de cifrado

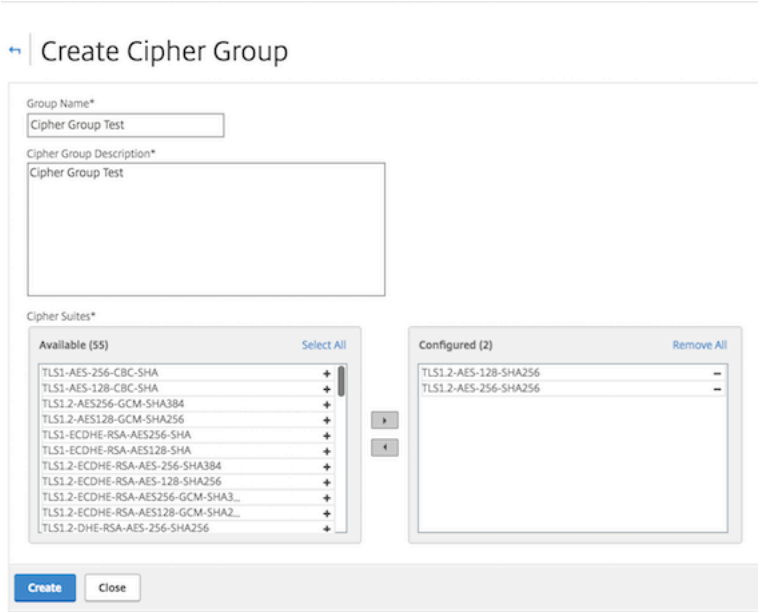
January 24, 2024

Un grupo de cifrado es un conjunto de conjuntos de cifrado que se vincula a un servidor virtual SSL, servicio o grupo de servicios en la instancia de Citrix Application Delivery Controller (ADC). Un conjunto de cifrado comprende un protocolo, un algoritmo de intercambio de claves (`Kx`), un algoritmo de autenticación (`Au`), un algoritmo de cifrado (`Enc`) y un algoritmo de código de autenticación de mensajes (`Mac`).

**Para agregar un grupo de cifrado en NetScaler ADM:**

1. Navegue hasta **Sistema** > **Administración**
2. En **Configuración de SSL**, haga clic en **Grupos de cifrado**
3. Haga clic en **Agregar**.
4. En la página **Crear Grupo de Cifrados**, introduzca los siguientes detalles:
   - **Nombre del grupo**: Nombre del grupo de cifrado.
   - **Descripción del grupo de cifrado**: Proporcione una descripción del grupo de cifrado.
   - Conjuntos de**cifrado: haga clic en Agregar para seleccionar los conjuntos** de cifrado de la lista Disponible y, a continuación, mover los conjuntos de cifrado seleccionados (o todos) a la lista configurados.
5. Haga clic en **Crear**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Crear destino de capturas SNMP, comunidad de administradores y usuarios

January 30, 2024

Siempre que se produce una condición anormal en el Citrix ADM, se genera una captura de SNMP. A continuación, las capturas se envían a un dispositivo remoto denominado servidor de destino de capturas o *destino de capturas SNMP* . Aquí, Citrix ADM se configura como destino de captura. Puede consultar al agente SNMP para obtener información específica del sistema desde un dispositivo remoto denominado *administrador SNMP*. A continuación, el agente busca en la base de información de administración (MIB) los datos solicitados y los envía al administrador SNMP.

**Para crear un destino de captura SNMP en Citrix ADM:**

1. Vaya a **Sistema** > **SNMP** > **Destinos de captura**.
2. En **CapTURAS SNMP**, haga clic en **Agregar** para crear una captura SNMP y, a continuación, especifique los siguientes detalles:
   - **Versión.** Seleccione la versión de SNMP que desee utilizar.
   - **Servidor de destino.** Nombre o dirección IP del destino de la trampa.
   - **Puerto.** Introduzca el puerto de destino de la trampa. El puerto está configurado en 162 de forma predeterminada.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Comunidad.** Especifique la cadena de comunidad que se utilizará al enviar una trampa al oyente de la trampa.

3. Haga clic en **Crear**.

> **Nota**
>
> Si está creando un destino de captura SNMP v3, especifique las credenciales de usuario de SNMP a las que desea vincular la captura. Para agregar una credencial de usuario de SNMP, haga clic en **Insertar** y, a continuación, agregue el usuario de la lista de usuarios de SNMP disponibles.

**Para crear una comunidad de administradores de SNMP:**

1. Vaya a **Sistema** > **SNMP** > **Gestores**.
2. En **SNMP Manager**, haga clic en **Agregar** para crear una comunidad de administradores de SNMP y, a continuación, especifique los siguientes detalles:
   - **Gestor SNMP.** Introduzca el nombre o la dirección IP del administrador SNMP.
   - **Comunidad.** Especifique la cadena de comunidad que se utilizará al enviar las trampas al oyente de trampas.
3. Si lo desea, puede seleccionar la casilla **Habilitar red de administración** para especificar la máscara de **red, que es la máscara**de subred de la red del administrador de SNMP.
4. Haga clic en **Crear**.

**Para crear un usuario SNMP**:

1. Vaya a **Sistema** > **SNMP** > **Usuarios**.
2. En **Usuario SNMP**, haga clic en **Agregar**.
3. Introduzca el nombre de usuario y asigne un nivel de seguridad al usuario desde el menú.
4. En función del nivel de seguridad asignado al usuario, proporcione protocolos de autenticación adicionales, como protocolos de autenticación, contraseñas de privacidad y asigne vistas SNMP.

## Configurar y ver alarmas del sistema

January 30, 2024

Puede habilitar y configurar un conjunto de alarmas para supervisar el estado de sus servidores NetScaler Application Delivery Management (ADM). Debe configurar las alarmas del sistema para

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

asegurarse de que conoce cualquier problema crítico o importante del sistema. Por ejemplo, es posible que quiera recibir una notificación si el uso de CPU es alto o si hay varios errores de inicio de sesión en el servidor. Para algunas categorías de alarmas, como cpuUsageHigh o memoryUsageHigh, puede establecer umbrales y definir la gravedad (como Crítica o Mayor) de cada una. Para algunas categorías, como InventoryFailed o LoginFailure, solo puede definir la gravedad. Cuando se supera el umbral de una categoría de alarma (por ejemplo, MemoryUsageHigh) o cuando se produce un evento correspondiente a la categoría de alarma (por ejemplo, **LoginFailure**), se graba un mensaje en el sistema y puede verlo como mensaje de syslog. Además, puede configurar las notificaciones para recibir un correo electrónico o un SMS correspondiente a la configuración de la alarma.

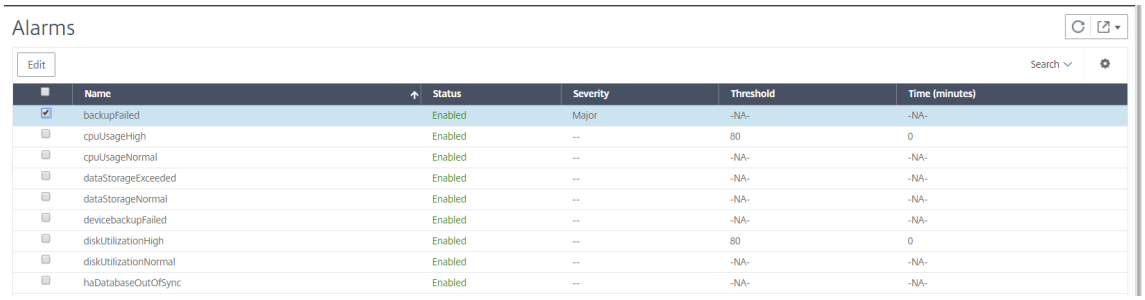
Puede asignar o modificar la gravedad de una alarma. Los niveles de gravedad que puede asignar son Crítico, Principal, Menor, Advertencia e Informativo.

Considere un caso en el que desee supervisar cada vez que se produzca un intento fallido de copia de seguridad. Puede habilitar la alarma BackupFailed y asignarle una gravedad, como Major, a ella. Siempre que NetScaler ADM intente realizar una copia de seguridad de los archivos del sistema y cuando el intento falla, se activa una alarma. Puede ver el mensaje en Citrix ADM u recibir notificaciones por correo electrónico o SMS.

Para configurar la alarma, debe seleccionar la alarma BackupFailed y especificar el nivel de gravedad como Principal. La alarma está activada de forma predeterminada.

**Para configurar y ver una alarma del sistema mediante NetScaler ADM:**

1. Navegue hasta **Sistema > SNMP** . Haga clic en **Alarmas** en la esquina superior derecha.



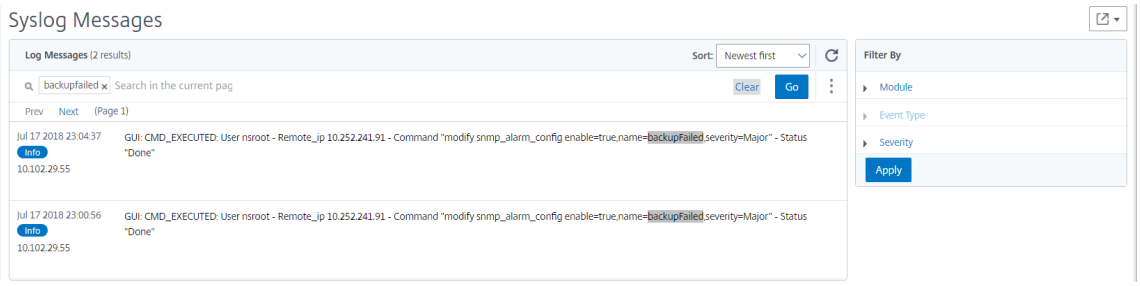

2. Seleccione la alarma que desee configurar (por ejemplo, BackupFailed) y haga clic en **Editar** para modificar su configuración.
3. La alarma está activada de forma predeterminada. Asigne un nivel de gravedad (ejemplo: Principal) y, a continuación, haga clic en **Aceptar**.

> **Nota**
>
> Para algunas alarmas, no puede establecer un umbral.
> Cuando se activa la alarma, puede ver el evento generado como un mensaje de syslog.

**Para ver el evento generado por la alarma BackupFailed mediante Citrix ADM:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

1. Vaya a**Sistema**>**Auditoría.**
2. En la página**de auditoría**, en Mensajes de**auditoría, seleccione Mensajes**de**Syslog**.
3. En el campo de búsqueda, escriba el nombre de la alarma.
   En este ejemplo, puede ver que se generó un evento para un intento de copia de seguridad fallido.




   También puede configurar notificaciones para enviarle un correo electrónico o un texto SMS (Servicio de mensajes cortos) cuando se activa una alarma. Para obtener información sobre cómo configurar las notificaciones del sistema, consulte Cómo configurar los valores de notificación del sistema de NetScaler ADM.

## NetScaler ADM como servidor proxy API

January 30, 2024

Además de poder recibir solicitudes de API REST de NITRO para sus propias funciones de administración y análisis, Citrix Application Delivery Management (Citrix ADM) puede funcionar como un servidor proxy de API REST para sus instancias administradas. En lugar de enviar solicitudes de API directamente a las instancias administradas, los clientes de API REST pueden enviar las solicitudes de API a Citrix ADM. Citrix ADM puede diferenciar entre las solicitudes de API a las que debe responder y las solicitudes de API que debe reenviar sin cambios a una instancia administrada.

Como servidor proxy de API, Citrix ADM le ofrece las siguientes ventajas:

- **Validación de solicitudes de API**. Citrix ADM valida todas las solicitudes de API comparándolas con las políticas configuradas de seguridad y control de acceso basado en roles (RBAC). Citrix ADM también reconoce a los inquilinos y garantiza que la actividad de las API no sobrepase los límites de los inquilinos.
- **Auditoría centralizada**. Citrix ADM mantiene un registro de auditoría de toda la actividad de la API relacionada con sus instancias administradas.
- **Administración de sesiones**. NetScaler ADM libera a los clientes de API de la tarea de mantener sesiones con instancias administradas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Cómo funciona Citrix ADM como servidor proxy de API

Cuando quiere que NetScaler ADM reenvíe una solicitud a una instancia administrada, configure el cliente de API para que incluya cualquiera de los siguientes encabezados HTTP en la solicitud de API:

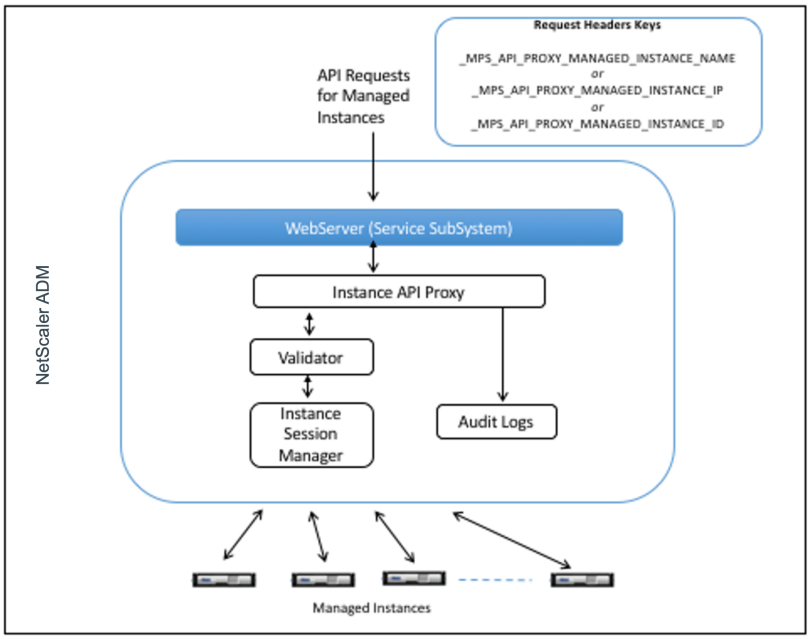
| valores de encabezado | Descripción |
|---|---|
| _MPS_API_PROXY_MANAGED_INSTANCE_NAME | Nombre de la instancia administrada. |
| _MPS_API_PROXY_MANAGED_INSTANCE_IP | Dirección IP de la instancia administrada. |
| _MPS_API_PROXY_MANAGED_INSTANCE_ID | ID de la instancia administrada. |
| _MPS_API_PROXY_TIMEOUT | Valor de tiempo de espera para una solicitud de API de NITRO. Establezca el valor de tiempo de espera en segundos. Cuando se establece un tiempo de espera de proxy, ADM espera la duración especificada antes de agotar el tiempo de espera de la solicitud. |
| _MPS_API_PROXY_MANAGED_INSTANCE_USERNAME | Nombre de usuario para acceder a la instancia de ADC administrada. |
| _MPS_API_PROXY_MANAGED_INSTANCE_PASSWORD | Contraseña para acceder a la instancia de ADC administrada. |
| _MPS_API_PROXY_MANAGED_INSTANCE_SESSID | Id. de sesión para acceder a la instancia administrada. |

> **Nota:**
>
> En **Sistema > Administración > Configuraciones del sistema > Configuración básica**, si selecciona **Solicitar credenciales para el inicio de sesión de la instancia**, asegúrese de configurar el nombre de usuario y la contraseña de una instancia administrada. Como alternativa, también puede especificar el ID de sesión de instancia.

La presencia de cualquiera de estos encabezados HTTP ayuda a NetScaler ADM a identificar una solicitud de API como una que debe reenviar a una instancia administrada. El valor del encabezado ayuda a Citrix ADM a identificar la instancia administrada a la que debe reenviar la solicitud.

Este flujo se representa en la siguiente ilustración:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




Como se muestra en la ilustración anterior, cuando uno de estos encabezados HTTP aparece en una solicitud, NetScaler ADM procesa la solicitud de la siguiente manera:

1. Sin modificar la solicitud, Citrix ADM la reenvía al motor proxy de la API de la instancia.
2. El motor proxy de la API de instancia reenvía la solicitud de API a un validador y registra los detalles de la solicitud de API en el registro de auditoría.
3. El validador se asegura de que la solicitud no infrinja las directivas de seguridad configuradas, las directivas de RBAC, los límites de arrendamiento, etc. Realiza comprobaciones adicionales, como una comprobación para determinar si la instancia administrada está disponible.

Si la solicitud de API es válida y se puede reenviar a la instancia administrada, NetScaler ADM identifica una sesión mantenida por el Administrador de sesiones de la instancia y, a continuación, envía la solicitud a la instancia administrada.

> **Nota**
>
> Asegúrese de que la opción **Solicitar credenciales para inicio de sesión de instancia** está inhabilitada. Para ello:
>
> 1. Vaya a **Sistema > Administración** .
> 2. En **Configuraciones del sistema**, seleccione **Sistema, Zona horaria, URL permitidas y Mensaje del día**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Cómo usar NetScaler ADM como servidor proxy API

En los siguientes ejemplos se muestran las solicitudes de API REST que un cliente de API envía a un servidor Citrix ADM que tiene una dirección IP de 192.0.2.5. Se requiere Citrix ADM para reenviar las solicitudes, sin cambios, a una instancia gestionada con la dirección IP 192.0.2.10. Todos los ejemplos utilizan el encabezado _MPS_API_PROXY_MANAGED_INSTANCE_IP.

Antes de enviar a Citrix ADM las solicitudes de API, el cliente de API debe:

- Inicie sesión en Citrix ADM
- Obtener un identificador de sesión
- Incluye el ID de sesión en las solicitudes de API posteriores.

La solicitud de la API de inicio de sesión tiene el siguiente formato:

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }
```

Citrix ADM responde a la solicitud de inicio de sesión con una respuesta que incluye el identificador de sesión. El siguiente ejemplo de cuerpo de respuesta muestra un identificador de sesión:

```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
21
22
23        "tenant_name": "Owner",
24
25        "permission": "superuser",
26
27        "session_timeout": "36000",
28
29        "challenge_token": "",
30
31        "username": "",
32
33        "login_type": "",
34
35        "challenge": "",
36
37        "client_ip": "",
38
39        "client_port": "-1",
40
41        "cert_verified": "false",
42
43        "sessionid": "##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45        "token": "b2f3f935e93db6a"
46       }
47
48
49    ]
50
51   }
```

**Ejemplo 1: Recuperar las estadísticas del servidor virtual de equilibrio de carga**

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
1     GET /nitro/v1/stat/lbvserver
2     Content-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

Donde el valor del encabezado de cookie es el ID de sesión devuelto por la llamada a la API de inicio de sesión. Y el valor de _MPS_API_PROXY_MANAGED_INSTANCE_IP es la dirección IP del ADC.

**Ejemplo 2: Crear un servidor virtual de equilibrio de carga**

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

```
POST /nitro/v1/config/lbvserver/sample_lbvserver
Content-type: application/json
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

{

     "lbvserver":{

         "name":"sample_lbvserver",
         "servicetype":"HTTP",
         "ipv46":"10.102.1.11",
         "port":"80"
      }

 }
```

**Ejemplo 3: Modificar un servidor virtual de equilibrio de carga**

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
PUT /nitro/v1/config/lbvserver
Content-type: application/json
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

{

   "lbvserver":{

        "name":"sample_lbvserver",
        "appflowlog":"DISABLED"
    }

 }
```

**Ejemplo 4: Eliminar un servidor virtual de equilibrio de carga**

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
DELETE /nitro/v1/config/lbvserver/sample_lbvserver
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Ejemplo 5: Descargue la configuración de ejecución de CLI en el ADC**

El cliente debe enviar a NetScaler ADM una solicitud de API del siguiente formulario:

```
GET /nitro/v1/config/nsrunningconfig
Accept-type: application/json
_MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
SESSID: ##
   D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
```

## Visualice problemas con Infrastructure Analytics

January 30, 2024

Un objetivo clave para los administradores de red es supervisar las instancias de NetScaler ADC. Las instancias de ADC ofrecen información interesante sobre el uso y el rendimiento de las aplicaciones y escritorios a los que se accede mediante ellas. Los administradores deben supervisar la instancia de ADC y analizar los flujos de aplicación procesados por cada instancia de ADC. Pueden remediar cualquier problema probable de configuración, configuración, conectividad, certificados y otros que puedan afectar el uso o el rendimiento de las aplicaciones. Por ejemplo, un cambio repentino en el patrón de tráfico de la aplicación puede deberse a un cambio en la configuración SSL, como la desactivación de un protocolo SSL. Los administradores deben poder identificar rápidamente la correlación entre estos puntos de datos para garantizar lo siguiente:

- La disponibilidad de las aplicaciones se encuentra en un estado óptimo
- No hay problemas de consumo de recursos, hardware, capacidad o cambio de configuración
- No hay inventarios no utilizados
- No hay certificados caducados

La función de análisis de infraestructura simplifica el proceso de análisis de datos al correlacionar varias fuentes de datos y cuantificarlas en una puntuación medible que define el estado de una instancia. Con esta función, los administradores tienen un único punto de contacto para saber si hay un problema, el origen del problema y las posibles soluciones que pueden realizar.

### Análisis de infraestructura

La función de análisis de infraestructura de Citrix Application Delivery Management (ADM) recopila todos los datos recopilados de las instancias de Citrix ADC y los cuantifica en una **puntuación** de instancias que define el estado de las instancias. La puntuación de la instancia se resume en una vista

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

tabular o como visualización de paquetes circulares. La función Análisis de infraestructura le ayuda a visualizar los factores que provocaron o podrían provocar un problema en las instancias. Esta visualización también le ayuda a determinar las acciones que deben realizarse para evitar que el problema se repita.

## Puntuación de instancia

La puntuación de la instancia indica el estado de una instancia de ADC. Una puntuación de 100 significa una instancia perfectamente sana sin problemas. La puntuación de la instancia captura diferentes niveles de posibles problemas en la instancia. Es una medida cuantificable de la salud de las instancias y múltiples "indicadores de salud"contribuyen a la puntuación.

Los**indicadores de salud son los** componentes básicos de la puntuación de la instancia, donde la puntuación se calcula periódicamente para un "período de supervisión"predefinido, en función de todos los indicadores detectados en esa ventana de tiempo. Actualmente, Infrastructure Analytics calcula la puntuación de la instancia una vez cada hora en función de los datos recopilados de las instancias.
Un indicador se puede definir como cualquier actividad (un evento o un problema) que pertenezca a una de las siguientes categorías de las instancias.

- Indicadores de recursos del sistema
- Indicadores de eventos críticos
- Indicadores de configuración SSL
- Indicadores de desviación de configuración

## Indicadores de salud

- Indicadores de recursos del sistema

  Los siguientes son los problemas críticos de recursos del sistema que pueden ocurrir en las instancias de NetScaler ADC y que NetScaler ADM puede supervisar.

  - Uso**elevado de la CPU**. El uso de la CPU ha superado el valor de umbral más alto en la instancia de NetScaler ADC.
  - **Alto uso de memoria**. El uso de memoria ha superado el valor de umbral superior en la instancia de NetScaler ADC.
  - **Uso elevado del disco**. El uso del disco ha superado el valor umbral superior en la instancia de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Errores de disco**. Hay errores en el disco duro 0 o en el disco duro 1 del hipervisor en el que está instalada la instancia de ADC.
- **Fallo de alimentación**. La fuente de alimentación ha fallado o se ha desconectado de la instancia de ADC.
- **Fallo en la tarjeta SSL**. La tarjeta SSL instalada en la instancia ha fallado.
- **Errores de flash**. Se observan errores de Compact Flash en la instancia de NetScaler ADC.
- La**NIC descarta**. Los paquetes descartados por la tarjeta NIC han cruzado el valor de umbral más alto en la instancia de NetScaler ADC.

Para obtener más información sobre estos errores de recursos del sistema, consulta El panel de instancias.

- Indicadores de eventos críticos

  Los siguientes eventos críticos se identifican mediante la función de administración de eventos de ADM, que se configura con una gravedad crítica.

  - **Fallo de sincronización de HA**. La sincronización de la configuración entre las instancias de ADC en alta disponibilidad falló en el servidor secundario.
  - **No tiene latidos**. El servidor principal de un par de instancias de ADC en alta disponibilidad no recibe los latidos del servidor secundario.
  - **Tiene un mal estado secundario**. El servidor secundario de un par de instancias de ADC con alta disponibilidad se encuentra en estado secundario Inactivo, Desconocido o Permanecer.
  - **La versión HA no coincide**. La versión de las imágenes del software ADC instaladas en un par de instancias de ADC en alta disponibilidad no coincide.
  - **Fallo de sincronización del clúster**. La sincronización de la configuración entre las instancias de ADC en el modo de clúster ha fallado.
  - **La versión del clúster no coincide**. La versión de las imágenes del software ADC instaladas en las instancias de ADC en modo de clúster no coincide.
  - **Fallo de propagación del clúster**. Se produjo un error al propagar las configuraciones a todas las instancias de un clúster.

    > **Nota**
    >
    > Puede tener la lista de eventos SNMP críticos cambiando los niveles de gravedad de los eventos. Para obtener más información sobre cómo cambiar los niveles de gravedad, consulte Modificar la gravedad informada de los eventos que se producen en las instancias de NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Para obtener más información sobre los eventos en Citrix ADM, consulte Eventos.

- Indicadores de configuración SSL
  - **No se recomienda la fuerza clave**. La fortaleza clave de los certificados SSL no se ajusta a los estándares de Citrix
  - **Emisor no recomendado**. Citrix no recomienda el emisor del certificado SSL.
  - **Los certificados SSL han caducado**. El certificado SSL instalado en la instancia ADC ha caducado.
  - **Los certificados SSL están vencidos**. El certificado SSL instalado en la instancia ADC está a punto de caducar en la próxima semana.
  - **Algoritmos no recomendados**. Los algoritmos de firma de certificados SSL instalados en la instancia ADC no se ajustan a los estándares de Citrix.

Para obtener más información sobre los certificados SSL, consulte Panel de control SSL.

- Indicadores de desviación de configuración
  - **Plantilla Config Drift**. Hay una desviación (cambios sin guardar) en la configuración con respecto a las plantillas de auditoría que ha creado con configuraciones específicas que quiere auditar en determinadas instancias.
  - **Desviación de configuración predeterminada**. Hay una desviación (cambios no guardados) en la configuración de los archivos de configuración predeterminados.

Para obtener más información sobre las desviaciones de la configuración y cómo ejecutar informes de auditoría para comprobar las desviaciones de la configuración, consulte Ver informes de auditoría.

### Ver problemas de capacidad ADC

Cuando una instancia ADC ha consumido la mayor parte de su capacidad disponible, puede producirse la caída de paquetes al procesar el tráfico del cliente. Este problema provoca un bajo rendimiento en una instancia de ADC. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC.

Para ver las cuestiones relativas a la capacidad de los CCA,

1. Vaya a **Redes > Análisis de infraestructura**.
2. Expanda la instancia para la que quiere ver los problemas de capacidad.

El ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra las caídas de paquetes o incrementos de contador de límite de velocidad, si existe. Los problemas se clasifican según los siguientes parámetros de capacidad:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Límite de rendimiento alcanzado**: El número de paquetes descartados en la instancia una vez alcanzado el límite de rendimiento.
- **Se alcanzó el límite de CPU PE**: La cantidad de paquetes descartados en todas las NIC una vez alcanzado el límite de CPU PE.
- **Se alcanzó el límite de PPS**: El número de paquetes descartados en la instancia una vez alcanzado el límite de PPS.
- **Límite de velocidad de procesamiento de SSL**: Número de veces que se ha alcanzado el límite de rendimiento de SSL
- **Límite de velocidad SSL TPS**: El número de veces que se ha alcanzado el límite de SSL TPS.

El ADM calcula la puntuación de la instancia en el umbral de capacidad definido.

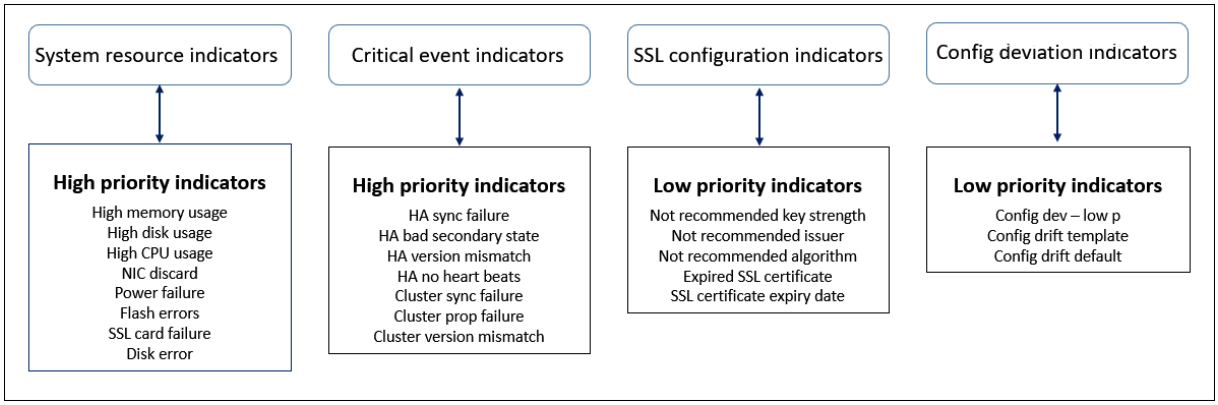
- Umbral bajo: 1 incremento del contador de límite de velocidad o caída de paquetes
- Umbral alto: Incremento del contador de límite de velocidad o caída de 10000 paquetes

Por lo tanto, cuando una instancia de ADC supera el umbral de capacidad, la puntuación de la instancia se ve afectada.

Cuando los paquetes caen o el contador de límite de velocidad aumenta, se genera un evento bajo la categoría `ADCCapacityBreach`. Para ver estos eventos, vaya a **Cuentas > Eventos del sistema**.

### Valor de los indicadores de salud

Los indicadores se clasifican en indicadores de alta prioridad e indicadores de baja prioridad sobre la base de sus valores de la siguiente manera:




Los indicadores de salud dentro del mismo grupo de indicadores tienen diferentes pesos asignados a ellos. Un indicador podría contribuir más a reducir la puntuación de la instancia que otro indicador. Por ejemplo, un uso elevado de memoria reduce la puntuación de la instancia más que el uso elevado del disco, el uso elevado de la CPU y el descarte de NIC. Si una instancia tiene un mayor número de indicadores detectados, menor será la puntuación de la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El valor de un indicador se calcula según las siguientes reglas. Se dice que el indicador se detecta de una de las tres formas siguientes:

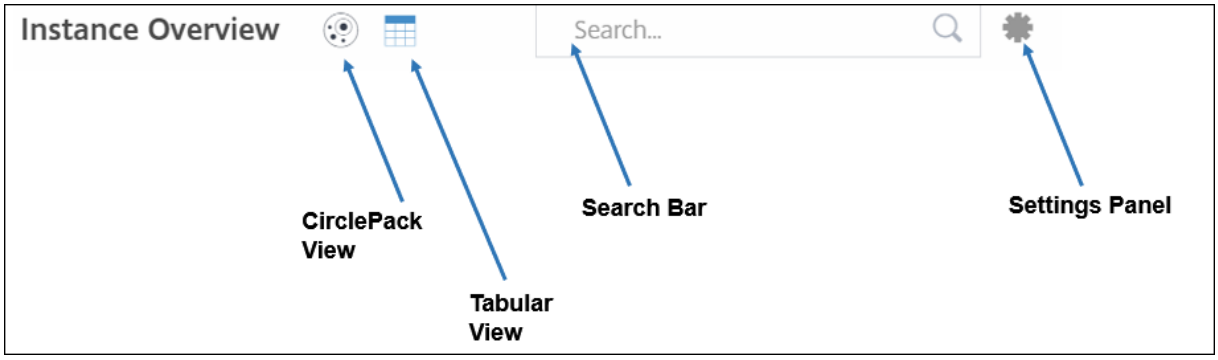
1. **Basado en una actividad**. Por ejemplo, un indicador de recursos del sistema se activa cada vez que se produce un corte de energía en la instancia y este indicador reduce el valor de la puntuación de la instancia. Cuando se borra el indicador, se elimina la penalización y la puntuación de la instancia aumenta.
2. **Basado en la violación del valor umbral**. Por ejemplo, se activa un indicador de recursos del sistema cuando la tarjeta NIC descarta paquetes y se infringe el nivel de umbral.
3. **Basado en la brecha de valor de umbral bajo y alto**. En este caso, un indicador se puede activar de dos maneras:
    - Cuando el valor del indicador se encuentra entre los umbrales más bajo y más alto, en cuyo caso se aplica una penalización parcial a la puntuación de la instancia.
    - Cuando el valor supera el umbral alto, en cuyo caso se aplica una penalización total a la puntuación de la instancia.
    - No se aplicará ninguna penalización a la puntuación de la instancia si el valor cae por debajo de un umbral bajo.

Por ejemplo, el uso de la CPU es un indicador de recursos del sistema que se activa cuando el valor de uso cruza el umbral inferior y también cuando el valor cruza el umbral alto.

## Panel de análisis de infraestructura

Vaya a **Redes** > **Análisis de infraestructura** .

Infrastructure Analytics se puede ver en formato **Circle Pack** o **Tabular**. Puede alternar entre los dos formatos.



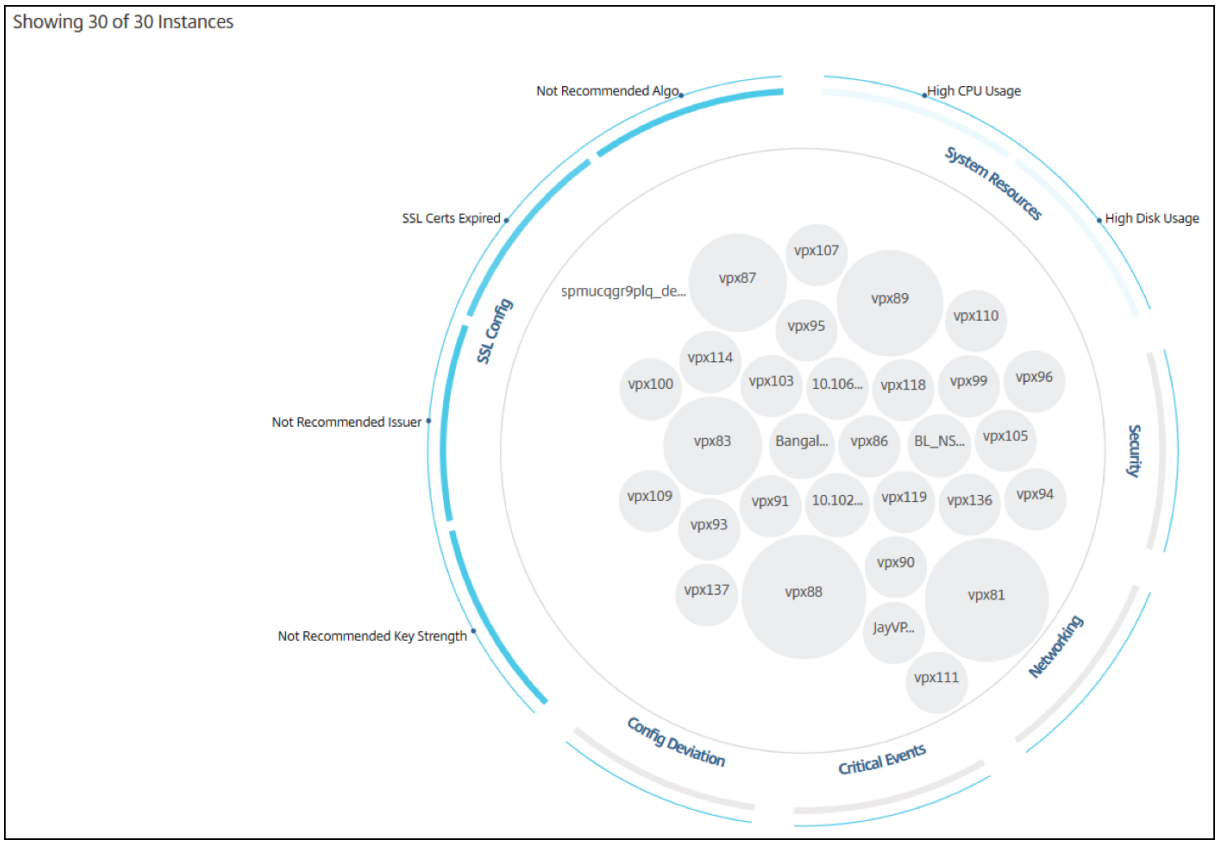

- En la vista Tabular, puede buscar una instancia escribiendo el nombre de host o la dirección IP en la barra de búsqueda.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- De forma predeterminada, la página Infrastructure Analytics muestra el panel de resumen en la parte derecha de la página.
- Haga clic en el icono de **configuración** para mostrar el panel de **configuración**.
- En ambos formatos de vista, el panel de resumen muestra los detalles de todas las instancias de la red.

## Vista circular del paquete

Los diagramas de empaquetado circular muestran los grupos de instancias como círculos muy organizados Suelen mostrar jerarquías en las que los grupos de instancias más pequeños tienen un color similar al de otros grupos de la misma categoría o están anidados dentro de grupos más grandes. Los paquetes de círculo representan conjuntos de datos jerárquicos y muestran diferentes niveles en la jerarquía y cómo interactúan entre sí.




### Círculos de instancia

**Color**. Cada instancia se representa en Circle Pack como un círculo coloreado. El color del círculo indica el estado de la instancia.

- **Verde**: la puntuación de la instancia está entre 100 y 80. La instancia está en buen estado.

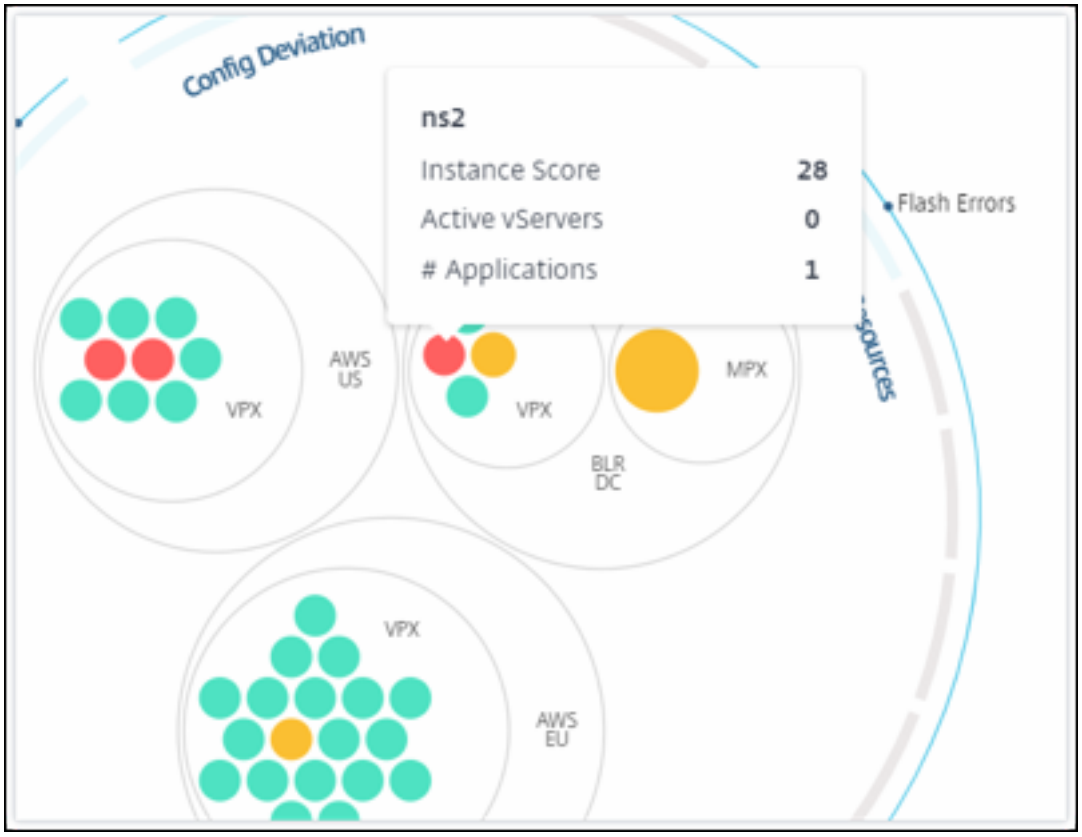
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Amarillo**: La puntuación de la instancia está entre 80 y 50; se han detectado algunos problemas que deben revisarse.
- **Rojo**: la puntuación de la instancia es inferior a 50. La instancia se encuentra en una etapa crítica, ya que se han observado varios problemas en esa instancia.

**Talla** El tamaño de estos círculos de colores indica la cantidad de servidores virtuales configurados en esa instancia. Un círculo más grande indica que hay un mayor número de servidores virtuales.

Puede pasar el puntero del mouse sobre cada uno de los círculos de la instancia (círculos de colores) para ver un resumen. La sugerencia de la herramienta al pasar el mouse muestra el nombre de host de la instancia, el número de servidores virtuales activos y el número de aplicaciones configuradas en esa instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



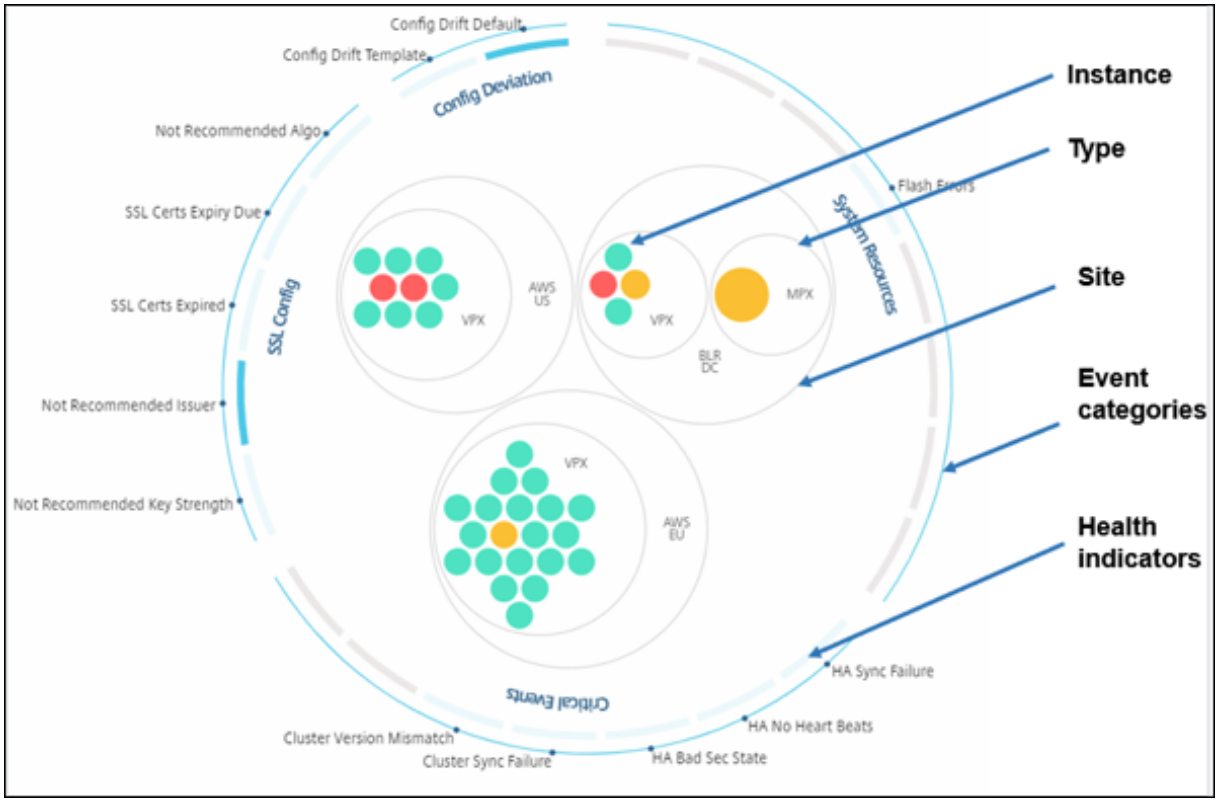

**Círculos de instancia agrupados**

El paquete circular, al principio, comprende círculos de instancias que se agrupan, anidan o empaquetan dentro de otro círculo según los siguientes criterios:

- el sitio en el que se implementan
- el tipo de instancias implementadas: VPX, MPX, SDX y CPX
- el modelo virtual o físico de la instancia de ADC
- la versión de la imagen ADC instalada en las instancias

La siguiente imagen muestra un paquete de círculo donde las instancias se agrupan primero por el sitio o centro de datos donde se implementan y, a continuación, se agrupan en función de su tipo, VPX y MPX.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



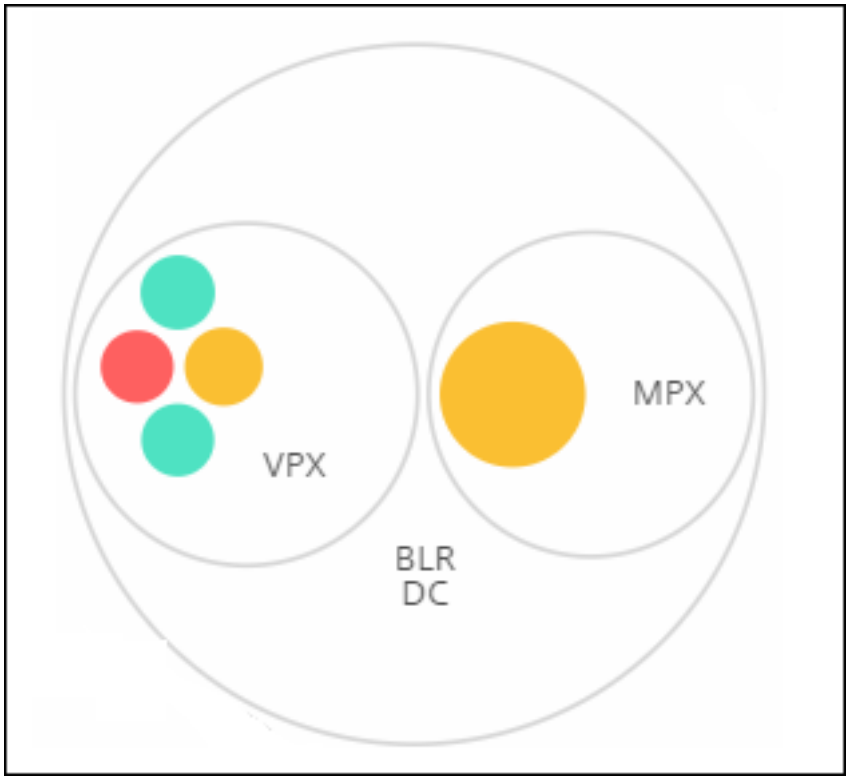

Todos estos círculos anidados están delimitados por dos círculos exteriores. Los dos círculos exteriores representan las cuatro categorías de eventos supervisados por el NetScaler ADM (recursos del sistema, eventos críticos, configuración de SSL y desviación de configuración) y los indicadores de estado que contribuyen.

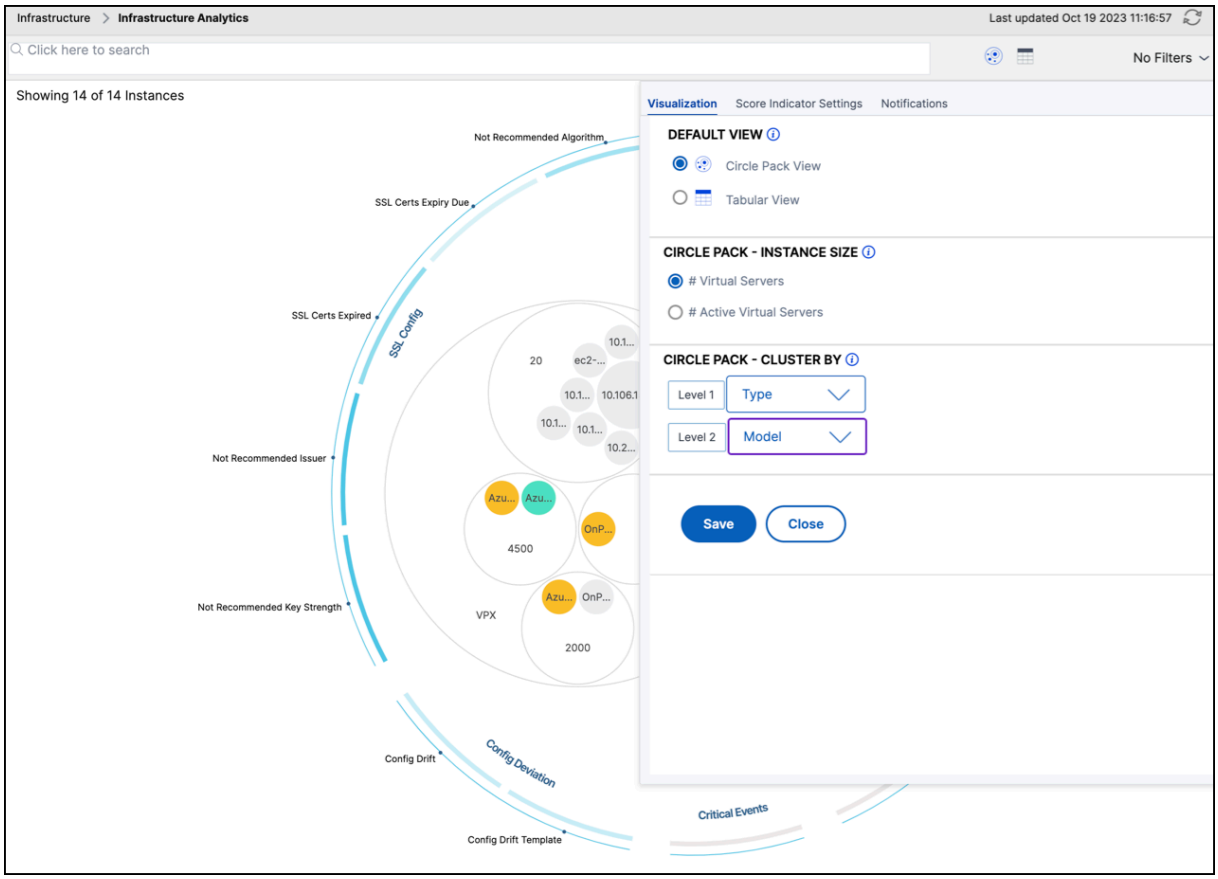
### Círculos de instancia agrupados

NetScaler ADM supervisa muchas instancias. Para facilitar la supervisión y el mantenimiento de estas instancias, Infrastructure Analytics permite agruparlas en dos niveles. Es decir, las agrupaciones de instancias se pueden anidar dentro de otra agrupación.

Por ejemplo, el centro de datos de BLR tiene dos tipos de instancias de ADC: VPX y MPX, implementadas en él. Primero puede agrupar las instancias de ADC por su tipo y, a continuación, agrupar todas las instancias por el sitio en el que están agrupadas. Ahora puede identificar fácilmente cuántos tipos de instancias se implementan en los sitios que está administrando.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



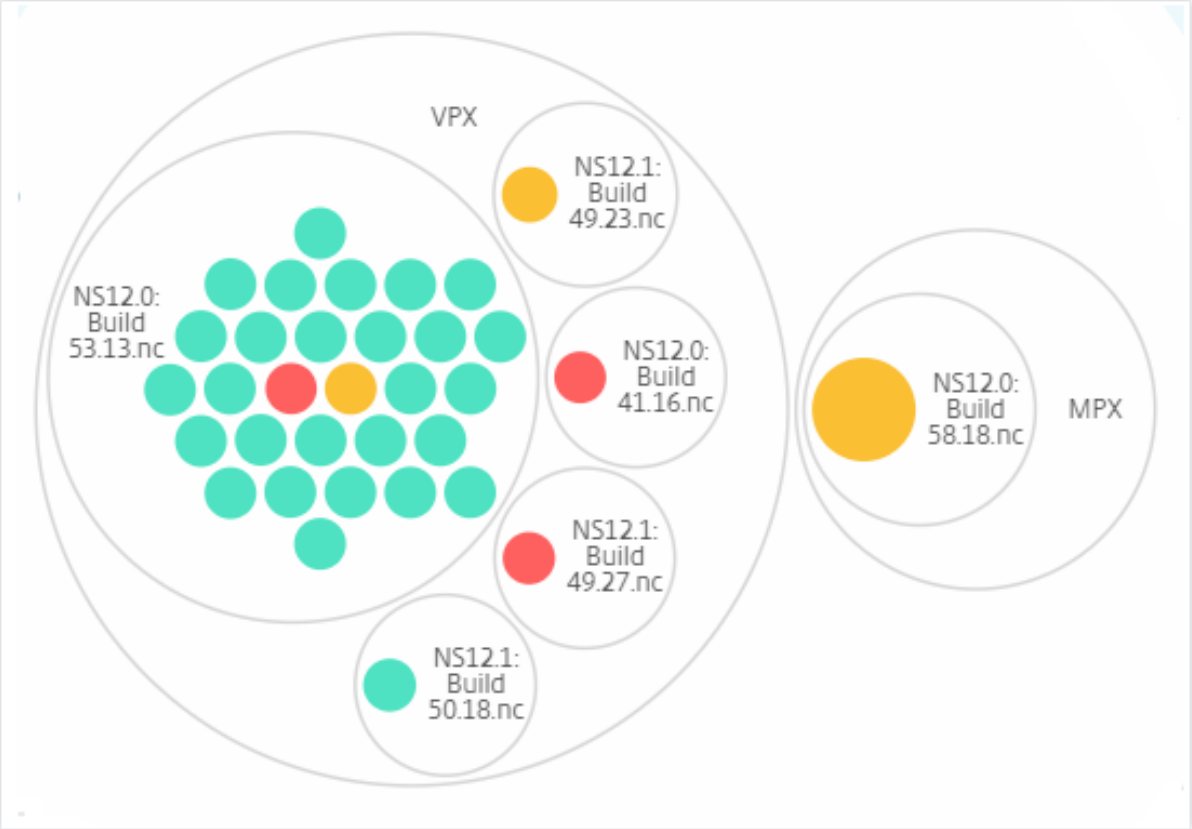

Algunos ejemplos más de clustering de dos niveles son los siguientes:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Sitio y modelo:**

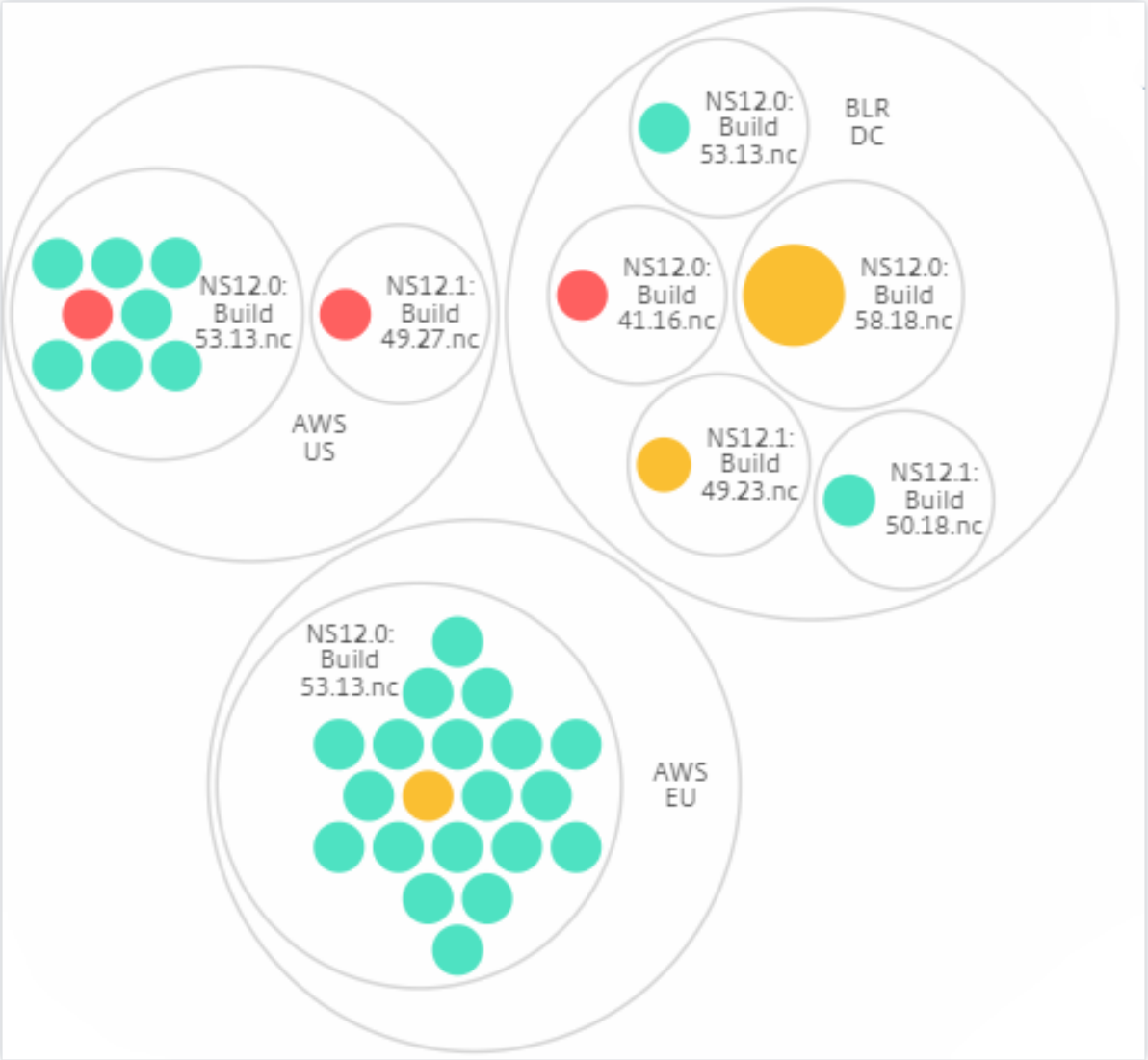
**Tipo y versión:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Sitio y versión:**

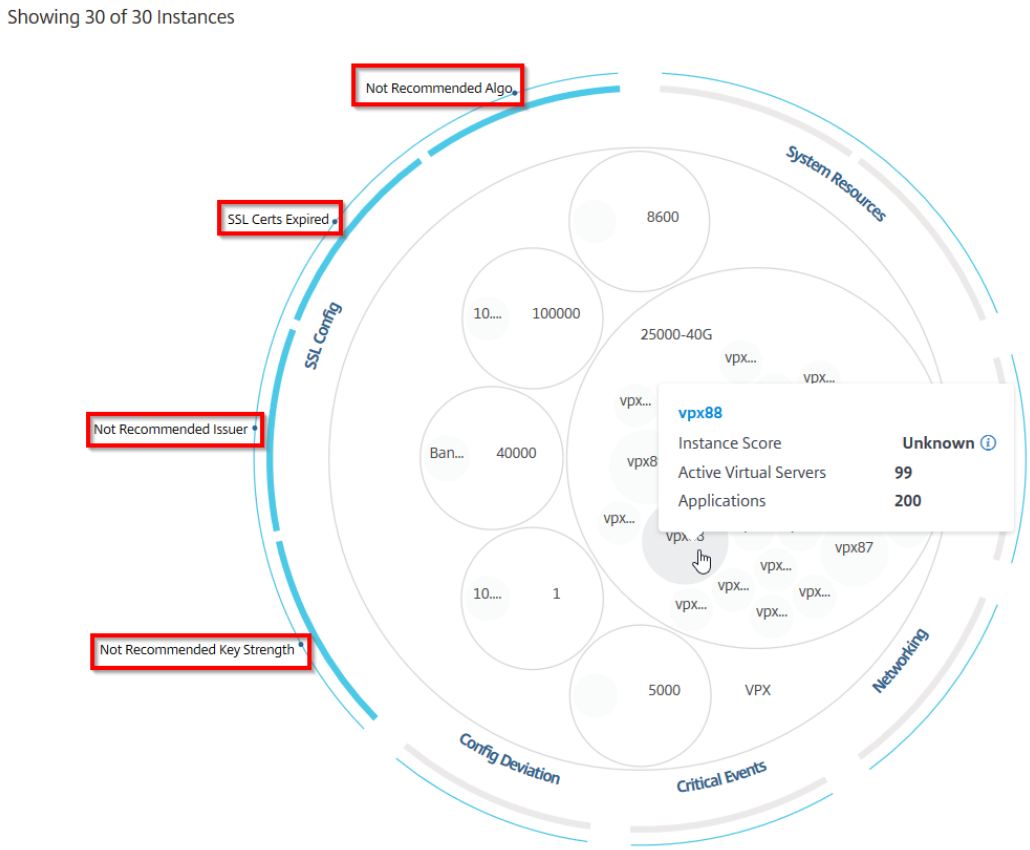
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Cómo usar Circle Pack**

Haga clic en cada uno de los círculos coloreados para resaltar esa instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

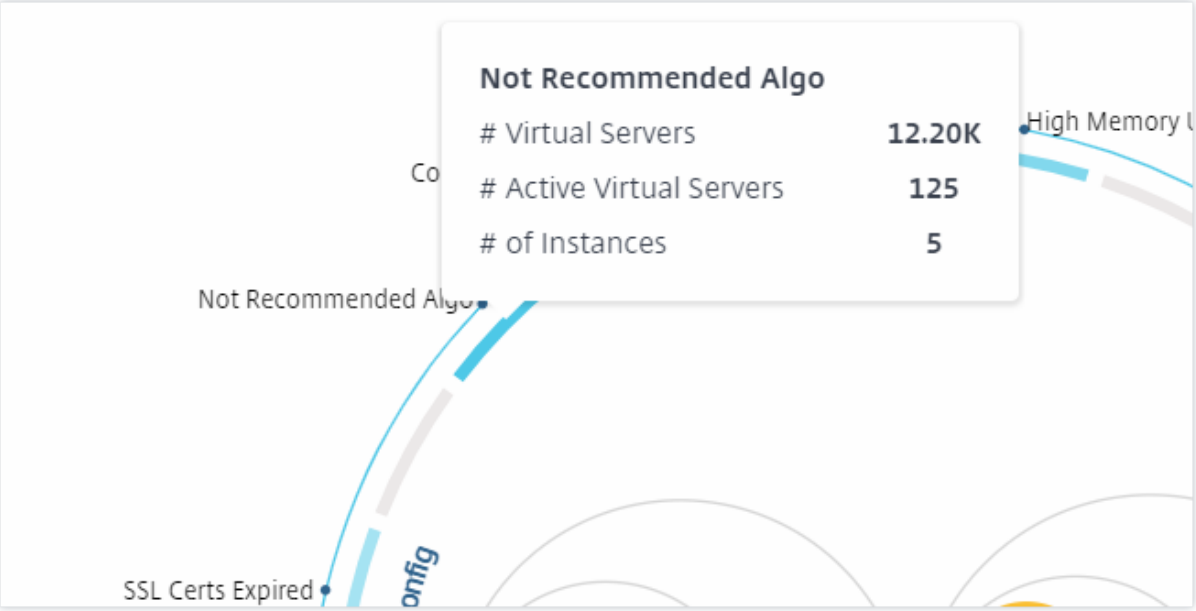



Dependiendo de los eventos que se hayan producido en ese caso, solo los indicadores de salud aparecen resaltados en los círculos exteriores. Por ejemplo, las dos imágenes siguientes de Circle Pack muestran diferentes conjuntos de indicadores de riesgo, aunque ambas instancias se encuentran en un estado crítico.

También puede hacer clic en los indicadores de estado para obtener más detalles sobre el número de instancias que han informado de ese indicador de riesgo. Por ejemplo, haga clic`Not recommended`

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

`Algo` para ver el informe resumido de ese indicador de riesgo.



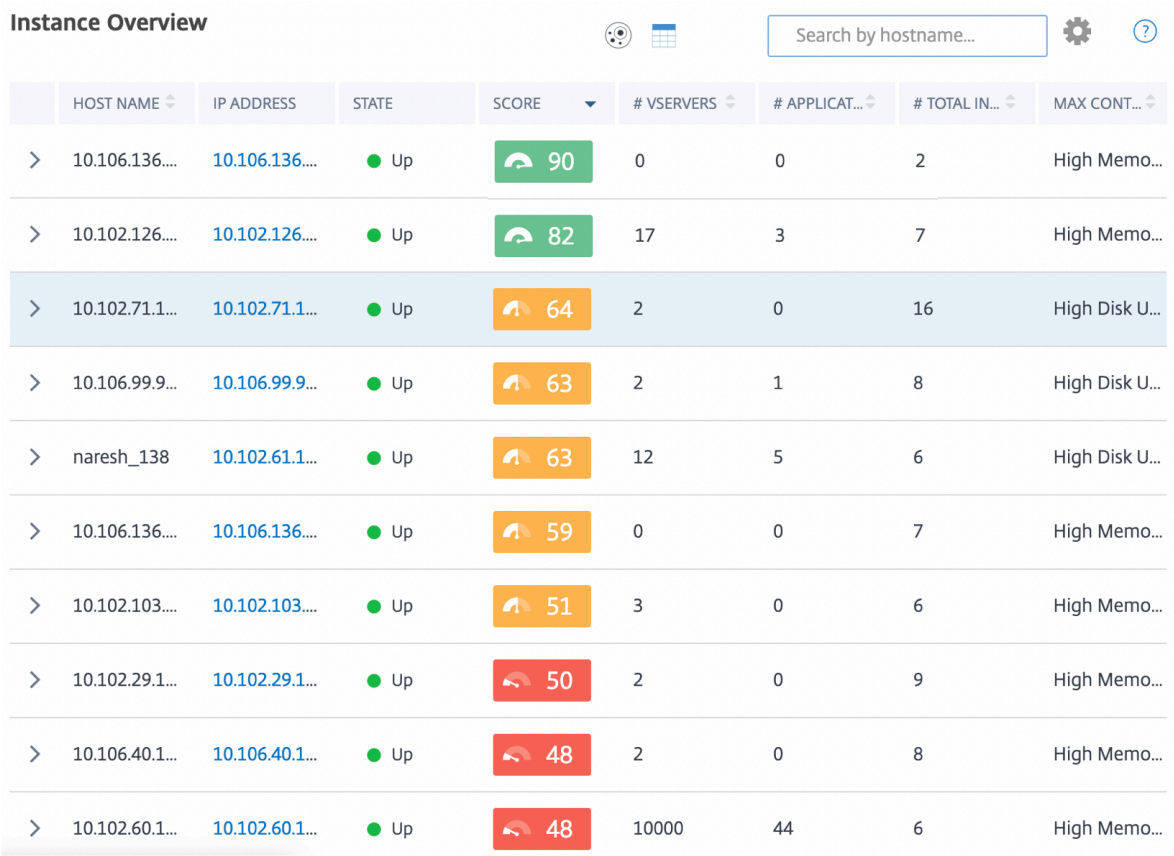

### Vista tabular

La vista tabular muestra las instancias y los detalles de esas instancias en un formato tabular. Los detalles que se muestran son los siguientes:

- Nombre de host de la instancia
- La dirección IP de la instancia
- Estado de la instancia
- Puntuación de instancia
- Número de servidores virtuales configurados en esa instancia
- Número de aplicaciones configuradas en esa instancia
- Número total de indicadores de riesgo
- El evento que contribuye más a reducir la puntuación de la instancia

Las instancias que se encuentran en estado crítico aparecen en la parte superior de la tabla, seguidas de las instancias que deben revisarse y, a continuación, las instancias en buen estado.

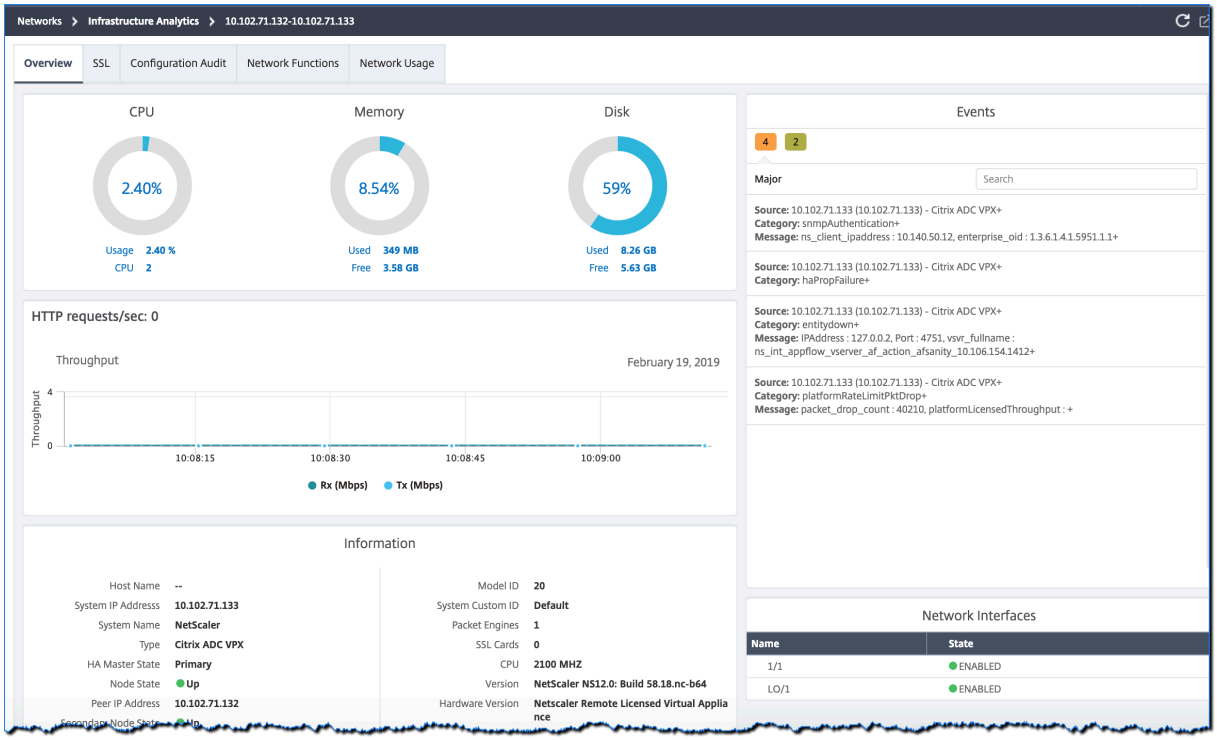
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 



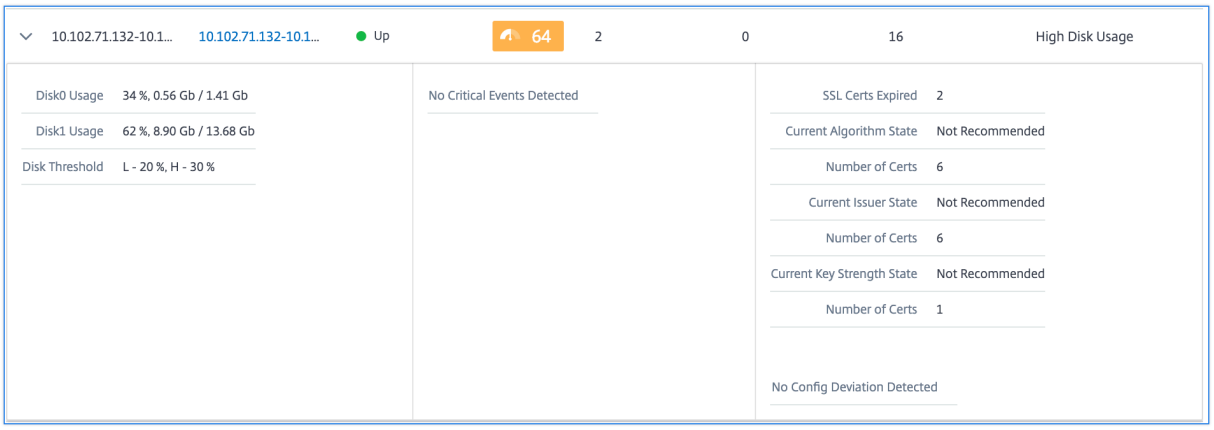

| HOST NAME | IP ADDRESS | STATE | SCORE | # VSERVERS | # APPLICAT... | # TOTAL IN... | MAX CONT... |
|---|---|---|---|---|---|---|---|
| 10.106.136.... | 10.106.136.... | Up | 90 | 0 | 0 | 2 | High Memo... |
| 10.102.126.... | 10.102.126.... | Up | 82 | 17 | 3 | 7 | High Memo... |
| 10.102.71.1... | 10.102.71.1... | Up | 64 | 2 | 0 | 16 | High Disk U... |
| 10.106.99.9... | 10.106.99.9... | Up | 63 | 2 | 1 | 8 | High Disk U... |
| naresh_138 | 10.102.61.1... | Up | 63 | 12 | 5 | 6 | High Disk U... |
| 10.106.136.... | 10.106.136.... | Up | 59 | 0 | 0 | 7 | High Memo... |
| 10.102.103.... | 10.102.103.... | Up | 51 | 3 | 0 | 6 | High Memo... |
| 10.102.29.1... | 10.102.29.1... | Up | 50 | 2 | 0 | 9 | High Memo... |
| 10.106.40.1... | 10.106.40.1... | Up | 48 | 2 | 0 | 8 | High Memo... |
| 10.102.60.1... | 10.102.60.1... | Up | 48 | 10000 | 44 | 6 | High Memo... |

Haga clic en la dirección IP de la instancia en la vista tabular para ver más detalles de esa instancia en el panel de control. El panel de instancias presenta una descripción general de la instancia en la que puede ver la CPU, la memoria y el uso del disco de la instancia. También puede ver detalles relacionados con la administración de certificados SSL, auditoría de configuración, funciones de red y un informe de red que muestra el uso detallado de la red de la instancia. Desplázate hacia abajo para ver la lista de las funciones y los modos habilitados en esta instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




También puede hacer clic en la flecha situada al principio de cada fila para expandir la fila y obtener más detalles.




La fila de la tabla expandida muestra los errores que se han producido en la instancia en todas las categorías. En el ejemplo anterior, puede ver que se han producido errores en los recursos del sistema, en la configuración de SSL y en los archivos de configuración. Sin embargo, no se ha informado de ningún evento crítico en la instancia.

## Cómo utilizar el panel de resumen

El **Panel de resumen** le ayuda a centrarse de manera eficiente y rápida en las instancias que necesitan revisión o estado crítico. El panel se divide en tres fichas: descripción general, información de

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

la instancia y perfil de tráfico. Los cambios que realice en este panel modifican la visualización en los formatos de vista Circle Pack y Tabular. En las siguientes secciones se describen estas fichas con más detalle. Los ejemplos de las siguientes secciones le ayudan a utilizar los diferentes criterios de selección de manera eficiente para analizar los problemas reportados por las instancias.

**Descripción general**:

La ficha **Descripción general** permite supervisar las instancias en función de los errores de hardware, el uso, los certificados caducados y otros indicadores similares que pueden ocurrir en las instancias. Los indicadores que puede supervisar aquí son los siguientes:

- Uso de CPU
- Uso de memoria
- Uso del disco
- Fallos del sistema
- Eventos críticos
- Caducidad de los

Los ejemplos siguientes ilustran cómo puede interactuar con el panel **Visión general** para aislar las instancias que informan de errores.

**Ejemplo 1: Ver las instancias que se encuentran en estado de revisión:**

Seleccione la casilla **Revisar** para ver solo las instancias que no informan de errores críticos, pero que aún requieren atención.

Los histogramas del panel **Descripción general** representan un número agregado de instancias en función de los eventos de uso elevado de la CPU, alto uso de memoria y uso elevado del disco. Los histogramas se califican en 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% y 100%. Pase el puntero del mouse sobre uno de los gráficos de barras. La leyenda de la parte inferior del gráfico muestra el rango de uso y el número de instancias en ese rango. También puede hacer clic en el gráfico de barras para mostrar todas las instancias de ese rango.

**Ejemplo 2: Vea las instancias que consumen entre el 10 y el 20% de la memoria asignada:**

En la sección de uso de memoria, haga clic en el gráfico de barras. La leyenda muestra que el rango seleccionado es del 10 al 20% y que hay 29 instancias que funcionan en ese rango.

También puede seleccionar varios rangos en estos histogramas.

**Ejemplo 3: Vea las instancias que consumen mucho espacio en disco en varios rangos:**

Para ver las instancias que han consumido espacio en disco entre un 0 y un 10%, arrastre el puntero del mouse sobre los dos rangos.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Nota**
>
> Haga clic en “X”para eliminar la selección. También puede hacer clic en **Restablecer** para eliminar varias selecciones.

Los gráficos de barras horizontales del panel **Descripción general** indican el número de instancias que informan de errores del sistema, eventos críticos y estado de caducidad de los certificados SSL. Seleccione la casilla de verificación para ver esas instancias.

**Ejemplo 4: Ver instancias de certificados SSL caducados:**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

**1**: Haga clic en la lista **Filtro**.

**2** - En la sección **Caducidad de los certificados SSL**, seleccione la casilla de verificación **Vencidos** para ver las instancias.

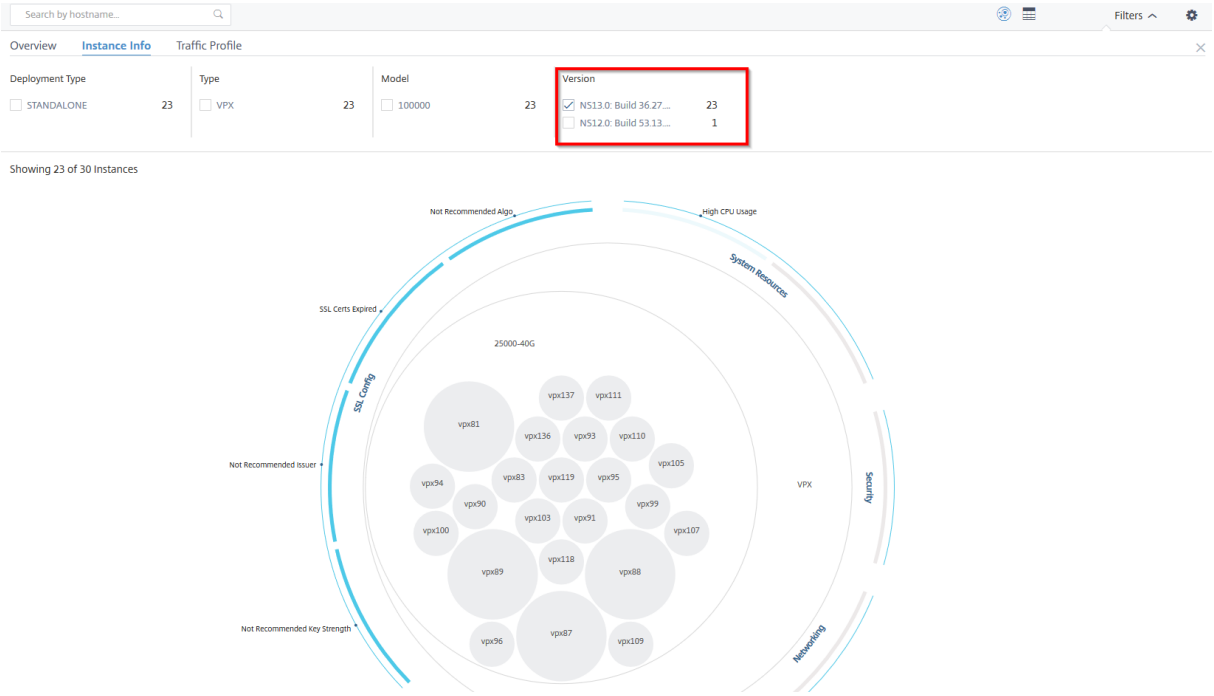
### Información de la instancia

El panel de **información de la instancia** le permite ver las instancias según el tipo de implementación, el tipo de instancia, el modelo y la versión de software. Puede seleccionar varias casillas de verificación para reducir la selección.

**Ejemplo 5: Ver las instancias VPX de ADC con un número de compilación específico:**

Seleccione la versión que quiere ver.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Perfil de tráfico

Los histogramas del panel **de perfil de tráfico** representan un número agregado de instancias en función del rendimiento con licencia de las instancias, el número de solicitudes, conexiones y transacciones gestionadas por las instancias. Seleccione el gráfico de barras para ver las instancias de ese rango.

### Ejemplo 6: Ver instancias que admiten conexiones TCP:

La siguiente imagen muestra el número de instancias que admiten conexiones TCP.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

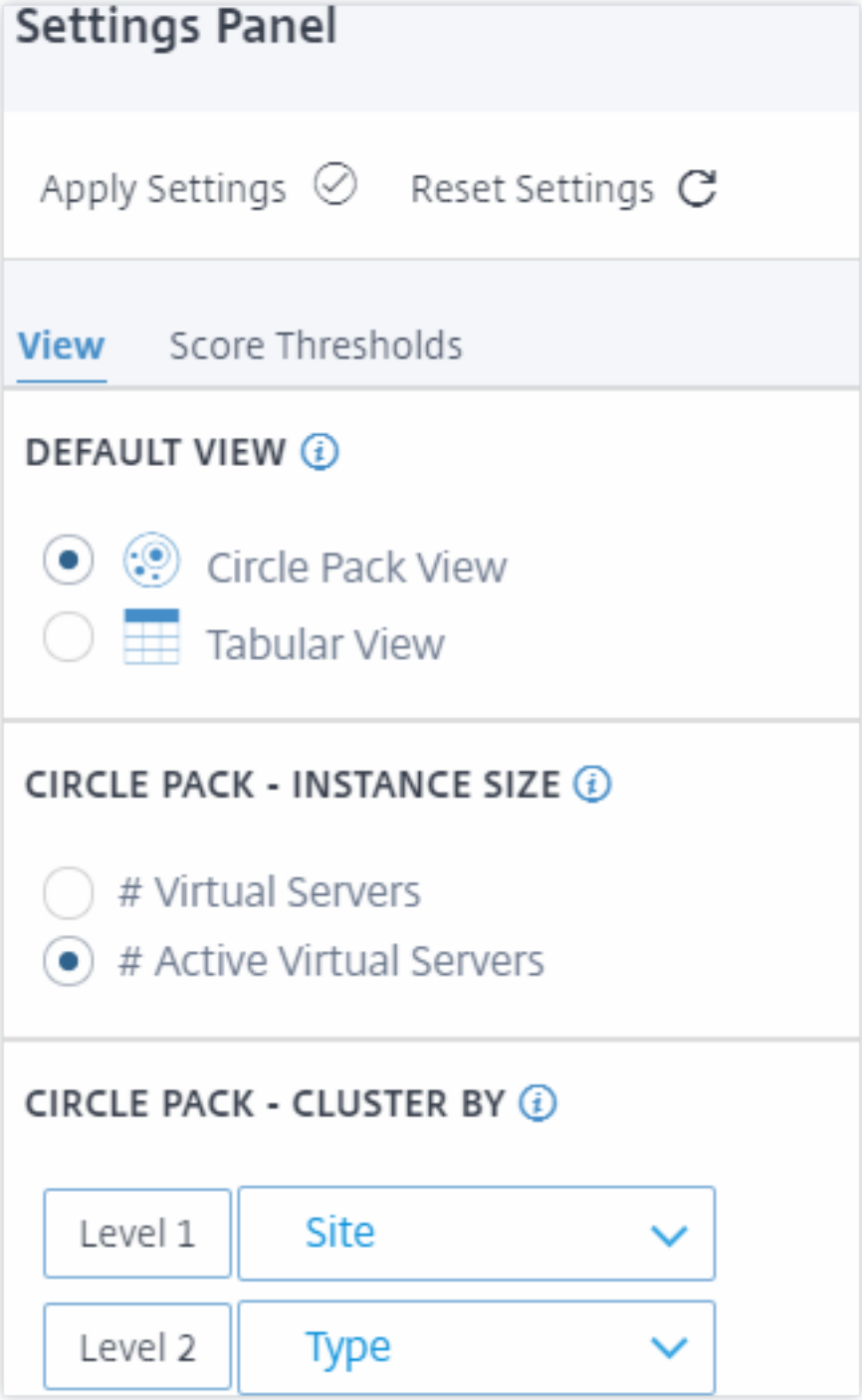
## Cómo usar el panel de configuración

El panel de **configuración** le permite configurar la vista predeterminada de Infrastructure Analytics. También le permite establecer los valores de umbral bajos y altos para un uso elevado de la CPU, un uso elevado del disco y un uso elevado de la memoria. El panel de ajustes está dividido en dos fichas: Umbrales de visualización y puntuación.

### Ver

- **Vista predeterminada**. Seleccione el formato **Circle Pack** o Tabular como vista predeterminada en la página de análisis. El formato que selecciona es el que aparece cada vez que accede a la página en NetScaler ADM.
- **Paquete circular: tamaño de instancia**. Permita que el tamaño del círculo de instancias sea igual al número de servidores virtuales o al número de servidores virtuales activos.
- **Paquete Circle, Cluster By**. Decida el agrupamiento de dos niveles de los círculos de instancia. Para obtener más información sobre la agrupación en clústeres de instancias, consulta Círculos de instancias en clústeres.

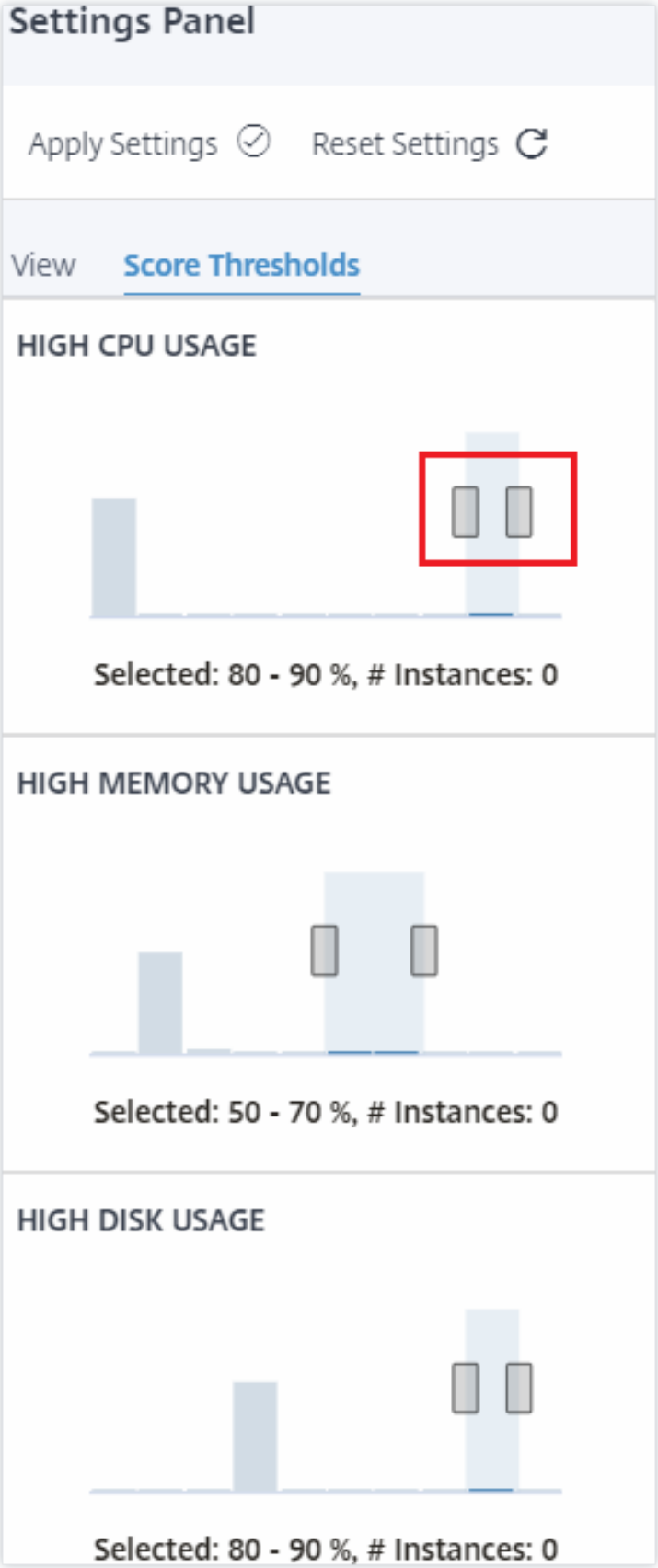
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




**Umbrales de puntuación**

Puede modificar los valores de umbral bajo y alto para un uso elevado de CPU, memoria y disco en función de los requisitos de tráfico de su organización. Arrastre los controladores de cada uno de los Histograma de selección para establecer los valores.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> **Nota**
>
> Haga clic en **Aplicar configuración** para aplicar estos cambios o haga clic en **Restablecer** para eliminar todos los cambios.

## Cómo visualizar los datos en el panel

Con Infrastructure Analytics, los administradores de red ahora pueden identificar las instancias que necesitan más atención en cuestión de segundos. Para entender la visualización de datos con más detalle, consideremos el caso de Chris, un administrador de red de ExampleCompany.

Chris mantiene muchas instancias de Citrix ADC en la organización. Algunas de las instancias procesan mucho tráfico y Chris necesita supervisarlas de cerca. Chris observa que algunas instancias con mucho tráfico ya no procesan todo el tráfico que pasa por ellas. Antes, para analizar esta reducción, Chris tuvo que leer varios informes de datos procedentes de diversas fuentes. Chris tuvo que pasar más tiempo tratando de correlacionar los datos manualmente y determinar qué instancias no están en un estado óptimo y necesitan atención.

Chris usa la función de análisis de infraestructura para ver visualmente el estado de todas las instancias.

Los dos ejemplos siguientes ilustran cómo Infrastructure Analytics ayuda a Chris en la actividad de mantenimiento:

**Ejemplo 1: Para supervisar el tráfico SSL:**

Chris observa en el Circle Pack que una instancia tiene una puntuación de instancia baja y que esa instancia se encuentra en estado "Crítico". Chris hace clic en esa instancia para ver cuál es el problema. El resumen de la instancia muestra que hay un error en la tarjeta SSL en esa instancia y que la instancia no puede procesar el tráfico SSL (el tráfico SSL se ha reducido). Chris extrae esa información y envía un informe al equipo para investigar el problema inmediatamente.

**Ejemplo 2: Para supervisar los cambios de configuración:**

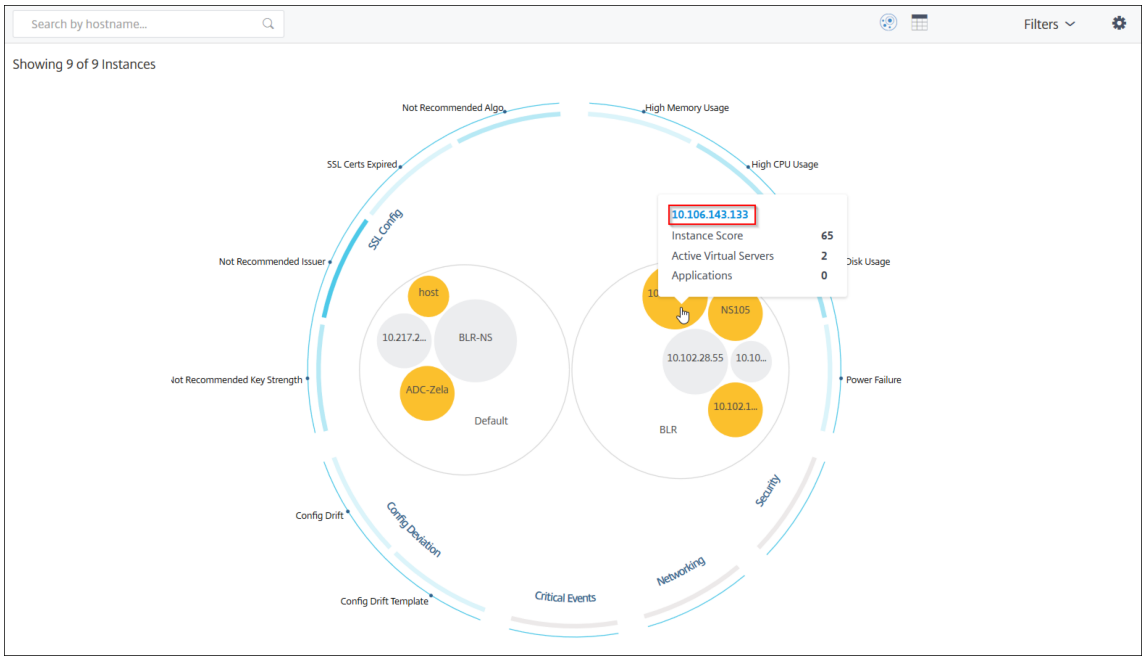
Chris también observa que otra instancia está en estado "Revisar"y que recientemente se ha producido una desviación de configuración. Cuando Chris hace clic en el indicador de riesgo de desviación de configuración, se da cuenta de que se han realizado cambios de configuración relacionados con RC4 Cipher, SSL v3, TLS 1.0 y TLS 1.1, que podrían deberse a problemas de seguridad. Chris también observa que el perfil de tráfico de transacciones SSL de esta instancia ha disminuido. Chris exporta este informe y lo envía al administrador para indagar más.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

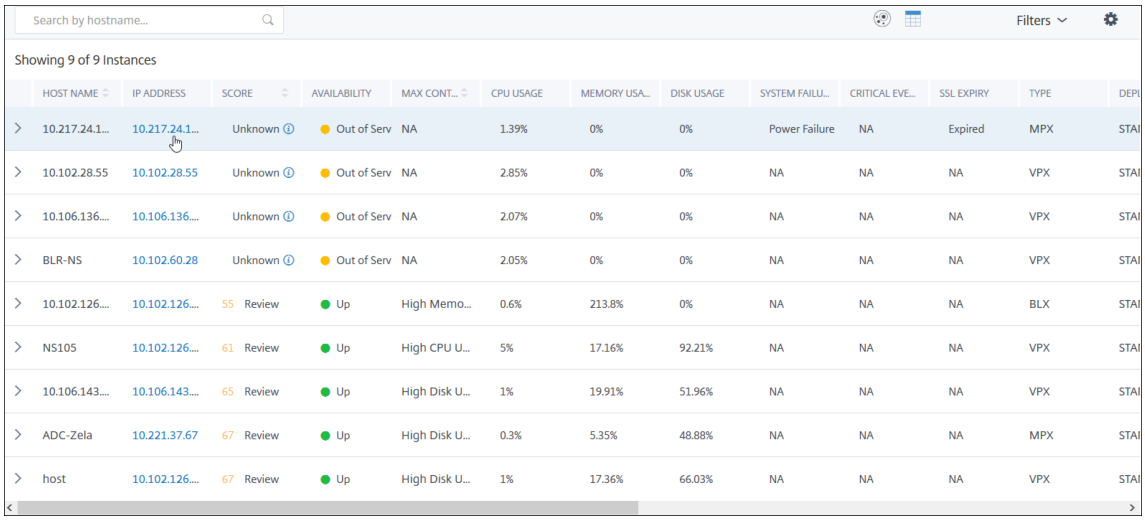
# Ver detalles de instancia en Infrastructure Analytics

January 30, 2024

1. Vaya a **Redes** > **Análisis de infraestructura**
2. Haga clic en la vista de paquete de círculo y seleccione la dirección IP.




También puede hacer clic en una dirección IP en la vista de tabla.




- **Nombre de host**: indica el nombre de host asignado a la instancia de ADC
- **Dirección IP**: indica la dirección IP de la instancia de ADC

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Puntuación**: Denota la puntuación de instancia ADC y el estado como Crítico, Bueno y Justo
- **Disponibilidad**: Indica el estado de la instancia de ADC, como **Activo**, **Inactivo**o **Fuera de servicio**.
- **Contribución máxima**: Indica la categoría de problema en la que la instancia de ADC tiene el número máximo de errores.
- **Uso de la CPU**: indica el% de CPU actual que utiliza la instancia
- **Uso de memoria**: indica el% de memoria actual que utiliza la instancia
- **Uso del disco**: indica el% de disco actual utilizado por la instancia
- **Fallo del sistema**: indica el número total de errores del sistema de instancias
- **Eventos críticos**: Indica la categoría de eventos en la que la instancia NetScaler ADC tiene el máximo de eventos
- **Caducidad del SSL**: Indica el estado del certificado SSL instalado en la instancia de ADC
- **Tipo**: Indica el tipo de instancia ADC como VPX, SDX, MPX o CPX
- **Implementación**: indica si la instancia de ADC se implementa como una instancia independiente o un par de HA
- **Modelo**: indica el número de modelo de la instancia de ADC
- **Versión**: indica la versión y el número de compilación de la instancia ADC
- **Rendimiento**: indica el rendimiento de la red actual desde la instancia de ADC.
- **Solicitud de HTTPS por segundo**: indica las solicitudes HTTPS actuales por segundo recibidas por la instancia de ADC
- **Conexión TCP**: indica las conexiones TCP actuales establecidas
- **Transacción SSL**: indica las transacciones SSL actuales procesadas por la instancia de ADC
- **Sitio**: indica el nombre del sitio en el que está implementada la instancia de ADC.

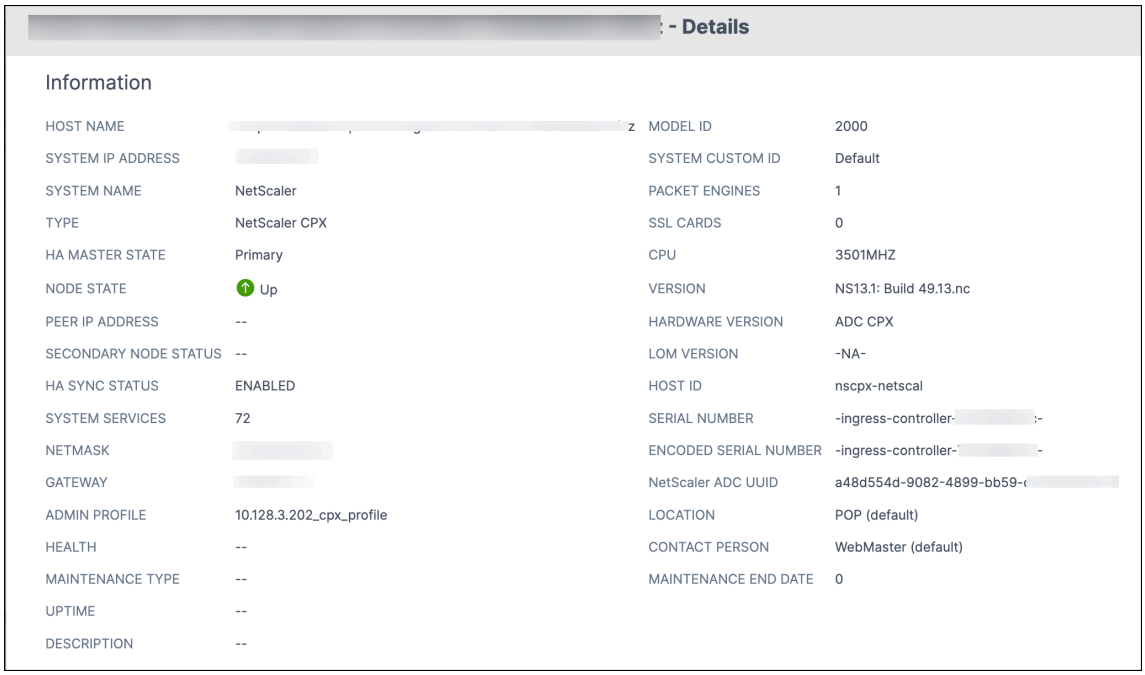
> **Nota**
>
> Cada 5 minutos, se actualizan los valores actuales de uso de la CPU, de memoria, de disco, de rendimiento, etc.

Haga clic en **Detalles de ejemplar** para ver los detalles.

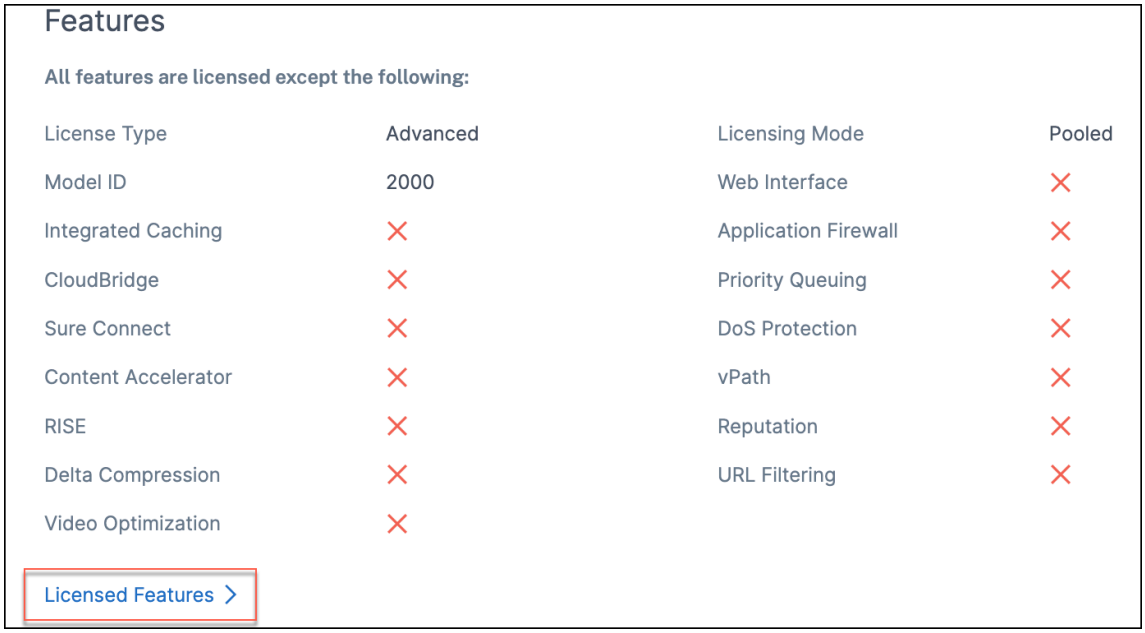
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Se muestran los siguientes detalles:

- **Información**: Detalles de la instancia, como el tipo de instancia, el tipo de implementación, la versión o el modelo.

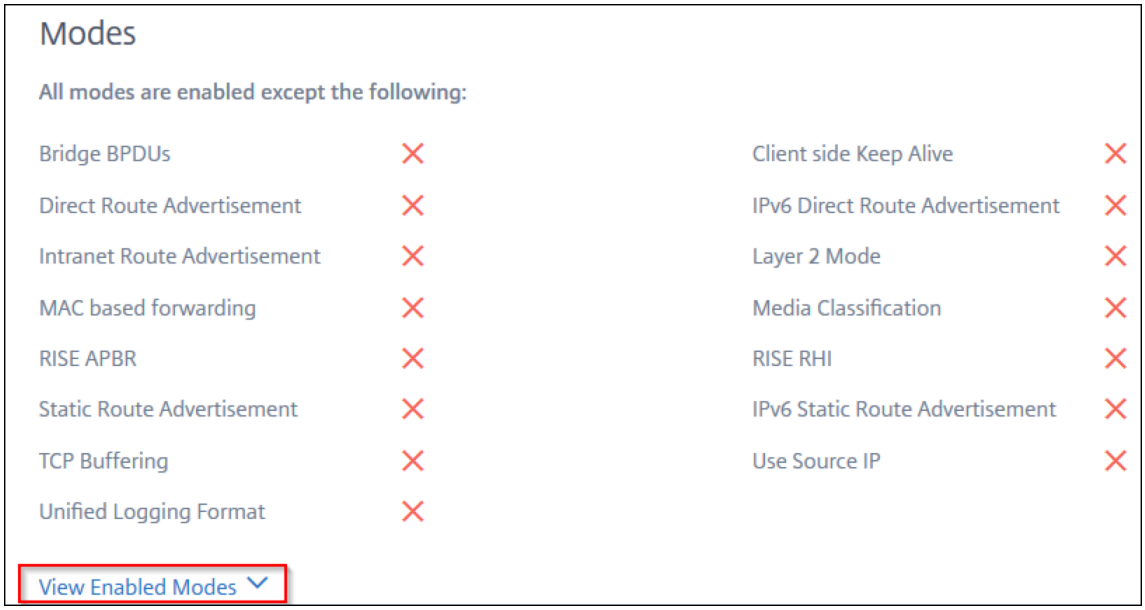



- **Funciones**: de forma predeterminada, se muestran las funciones que no tienen licencia. Haga clic en **Funciones con licencia** para ver las funciones que tienen licencia.



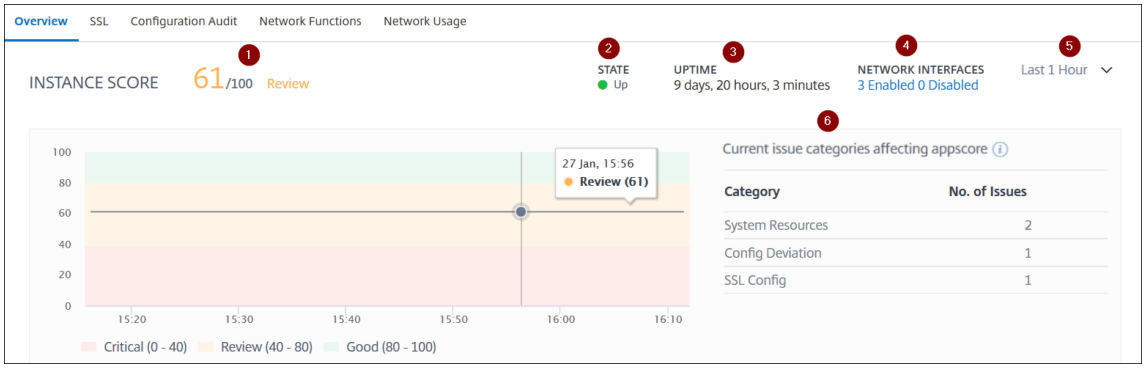

- **Modos**: de forma predeterminada, se muestran todos los modos que están inhabilitados en la instancia. Haga clic en **Ver modos habilitados** para ver los modos habilitados en la instancia.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




El panel de instancias presenta una descripción general de la instancia en la que puede ver los siguientes detalles:

- **Puntuación de instancia**




**1**: indica la puntuación actual de la instancia de NetScaler ADC durante el tiempo seleccionado. La puntuación final se calcula en **100 menos el total de penaltis**. El gráfico muestra los rangos de puntuación para la duración de tiempo seleccionada.

**2**: Indica el estado de la instancia de NetScaler ADC, como **Activo**, **Inactivo** y **Fuera de servicio**.

**3**: indica el tiempo que la instancia de NetScaler ADC está activa y en ejecución.

**4**: indica el total de interfaces de red habilitadas y inhabilitadas para la instancia. Haga clic para ver los detalles, como el nombre de la interfaz de red y el estado (habilitada o inhabilitada).

**5** —Seleccione la duración del tiempo de la lista para ver los detalles de la instancia.

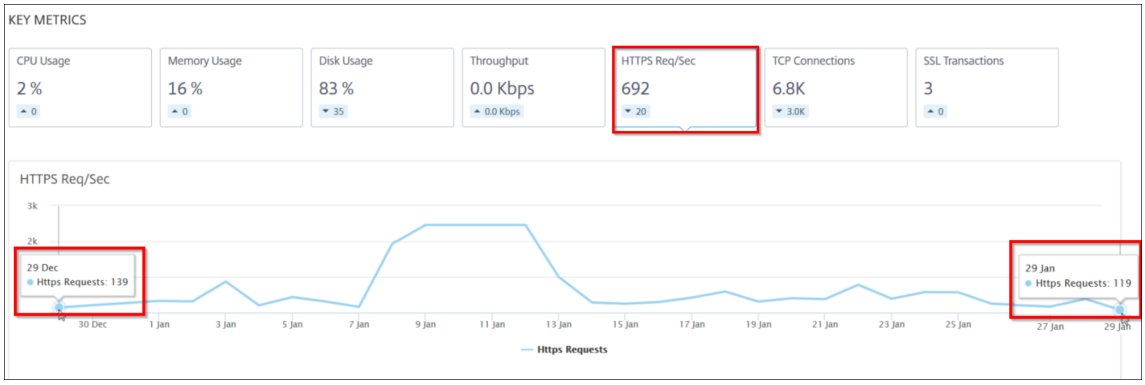
**6**: muestra el total de problemas y la categoría de problemas de la instancia de ADC.

- **Métricas clave**

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Haga clic en cada ficha para ver los detalles. En cada métrica, puede ver el valor medio y el valor de diferencia para el tiempo seleccionado.

La siguiente imagen es un ejemplo de HTTPS Req/Sec y la duración seleccionada es de 1 hora. El valor **692** es la media de las Req/Sec de HTTPS para el mes de duración y el valor **20** es el valor de la diferencia. En el gráfico, el primer valor es **139** y el último valor es **119**. El valor de la diferencia es **139 —119 = 20**.




Puede ver las siguientes métricas de instancia en un formato de gráfico para la duración de tiempo seleccionada:

- **Uso de CPU**: el% de CPU promedio de la instancia durante el tiempo seleccionado (se muestra tanto para la CPU de paquetes como para la CPU de administración).
- **Uso de memoria**: el% promedio de uso de memoria de la instancia durante el tiempo seleccionado.
- **Uso del disco**: el% medio de espacio en disco de la instancia durante el tiempo seleccionado.
- **Rendimiento**: el rendimiento de red promedio procesado por la instancia durante el tiempo seleccionado.
- **Solicitud de HTTPS por segundo**: el promedio de solicitudes HTTPs recibidas por la instancia durante el tiempo seleccionado.
- **Conexiones TCP**: el promedio de conexiones TCP establecidas por el cliente y el servidor durante el tiempo seleccionado.
- **Transacciones SSL**: el promedio de transacciones SSL procesadas por la instancia durante el tiempo seleccionado.

- **Problemas**

Puede ver los siguientes problemas que se producen en la instancia de NetScaler ADC:

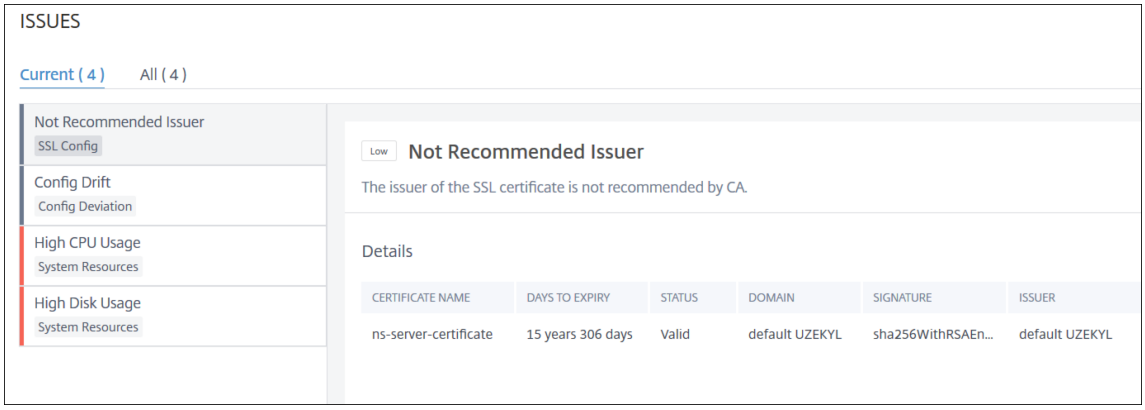
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Categoría de problema | Descripción | Problemas |
| --- | --- | --- |
| Recursos del sistema | Muestra todos los problemas relacionados con los recursos del sistema Citrix ADC, como la CPU, la memoria y el uso del disco. | – Alto uso de CPU<br>– Alto uso de memoria<br>– Uso elevado del disco<br>– Fallos en la tarjeta SSL<br>– Fallo de alimentación<br>– Error de disco<br>– Error de flash<br>– Descartes de NIC |
| Configuración SSL | Muestra todos los problemas relacionados con la configuración de SSL en la instancia de NetScaler ADC. | – Los certificados SSL han caducado<br>– Emisor no recomendado<br>– Algoritmo no recomendado<br>– No se recomienda la fuerza de la llave |
| desviación de configuración | Muestra todos los problemas relacionados con los trabajos de configuración aplicados en la instancia de NetScaler ADC. | – Deriva de configuración<br>– Ejecución vs plantilla |
| Eventos críticos | Muestra todos los eventos críticos relacionados con las instancias de NetScaler ADC configuradas en el par HA y en el clúster. | – Fallo de Cluster Prop<br>– Fallo de sincronización del clúster<br>– Las versiones del clúster no coinciden |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Categoría de problema | Descripción | Problemas |
|---|---|---|
| | | – HA: Estado secundario incorrecto<br>– HA No Heat Beats<br>– Fallo de sincronización de HA<br>– No coincide la versión de HA |
| Redes | Muestra los problemas operativos que se producen en las instancias. | Para obtener más información, consulte Análisis de infraestructura mejorados con nuevos indicadores. |

Haga clic en cada ficha para analizar y solucionar el problema. Por ejemplo, considere que una instancia tiene los siguientes errores durante el tiempo seleccionado:




- La ficha **Actual** muestra los problemas que afectan actualmente a la puntuación de la instancia.
- La ficha **Todo** muestra todos los problemas de infraestructura detectados durante la duración seleccionada.

## Ver los problemas de capacidad en una instancia de ADC

January 30, 2024

Cuando una instancia ADC ha consumido la mayor parte de su capacidad disponible, puede producirse la caída de paquetes al procesar el tráfico del cliente. Este problema provoca un bajo

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

rendimiento en una instancia de ADC. Al comprender estos problemas de capacidad del ADC, puede asignar licencias adicionales de forma proactiva para estabilizar el rendimiento del ADC.

En la **vista Circle Pack**, puede ver los problemas de capacidad de la instancia de ADC si existe.

Para ver las cuestiones relativas a la capacidad de los CCA,

1. Vaya a **Redes > Análisis de infraestructura**.
2. Seleccione la vista de paquete de círculos.

> **Nota**
>
> En **Infrastructure Analytics**, el paquete circular y las vistas tabulares muestran los eventos y problemas que ocurrieron en la última hora.

La siguiente ilustración sugiere los problemas de capacidad existentes en la instancia seleccionada:

Los problemas se clasifican según los siguientes parámetros de capacidad:

- **Límite de rendimiento alcanzado**: El número de paquetes descartados en la instancia una vez alcanzado el límite de rendimiento.
- **Se alcanzó el límite de CPU PE**: La cantidad de paquetes descartados en todas las NIC una vez alcanzado el límite de CPU PE.
- **Límite de PPS alcanzado**: la cantidad de paquetes descartados en la instancia después de alcanzar el límite de PPS.

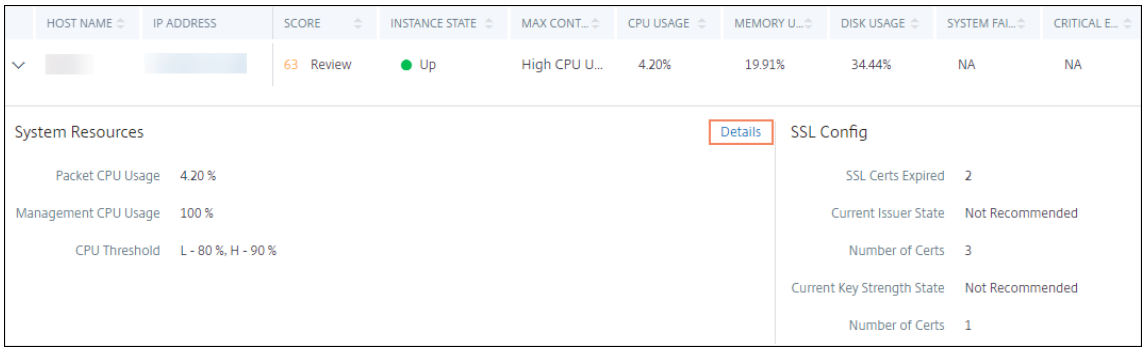
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- **Límite de velocidad de procesamiento de SSL**: Número de veces que se ha alcanzado el límite de rendimiento de SSL
- **Límite de velocidad SSL TPS**: El número de veces que se ha alcanzado el límite de SSL TPS.

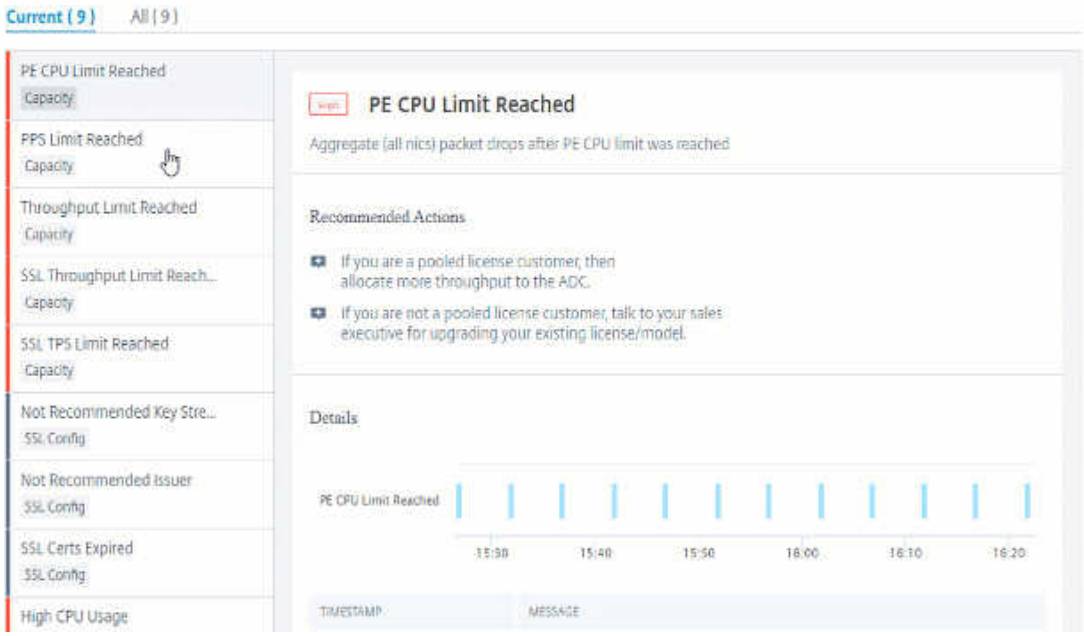
## Vea las acciones recomendadas para resolver problemas de capacidad

El ADM recomienda acciones que puedan resolver problemas de capacidad. Para ver las acciones recomendadas, realice los siguientes pasos:

1. En **Redes > Análisis de infraestructura**, seleccione la vista tabular.
2. Seleccione la instancia que tiene problemas de capacidad y haga clic en **Detalles**.




3. En la página de instancias, desplázate hacia abajo hasta la sección **Problemas**.
4. Seleccione cada problema y consulte las acciones recomendadas para resolver los problemas de capacidad.




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

El ADM sondea estos eventos cada cinco minutos desde la instancia de ADC y muestra las caídas de paquetes o incrementos de contador de límite de velocidad, si existe.

El ADM calcula la puntuación de la instancia en el umbral de capacidad definido.

- **Umbral bajo**: 1 incremento del contador de límite de velocidad o caída de paquetes
- **Umbral alto**: Incremento del contador de límite de velocidad o caída de 10000 paquetes

Por lo tanto, cuando una instancia de ADC infringe el umbral de capacidad, la puntuación de la instancia se ve afectada.

Cuando los paquetes caen o el contador de límite de velocidad aumenta, se genera un evento bajo la categoría `ADCCapacityBreach`. Para ver estos eventos, vaya a **Cuentas > Eventos del sistema**.

## Análisis de infraestructura mejorado con nuevos indicadores

January 30, 2024

Con NetScaler ADM Infrastructure Analytics, puede:

- Vea un nuevo conjunto de problemas operativos que se producen en las instancias de NetScaler ADC.
- Consulta los mensajes de error y consulta las recomendaciones para solucionar los problemas.

Como administrador, puede identificar rápidamente la causa principal del análisis de los problemas.

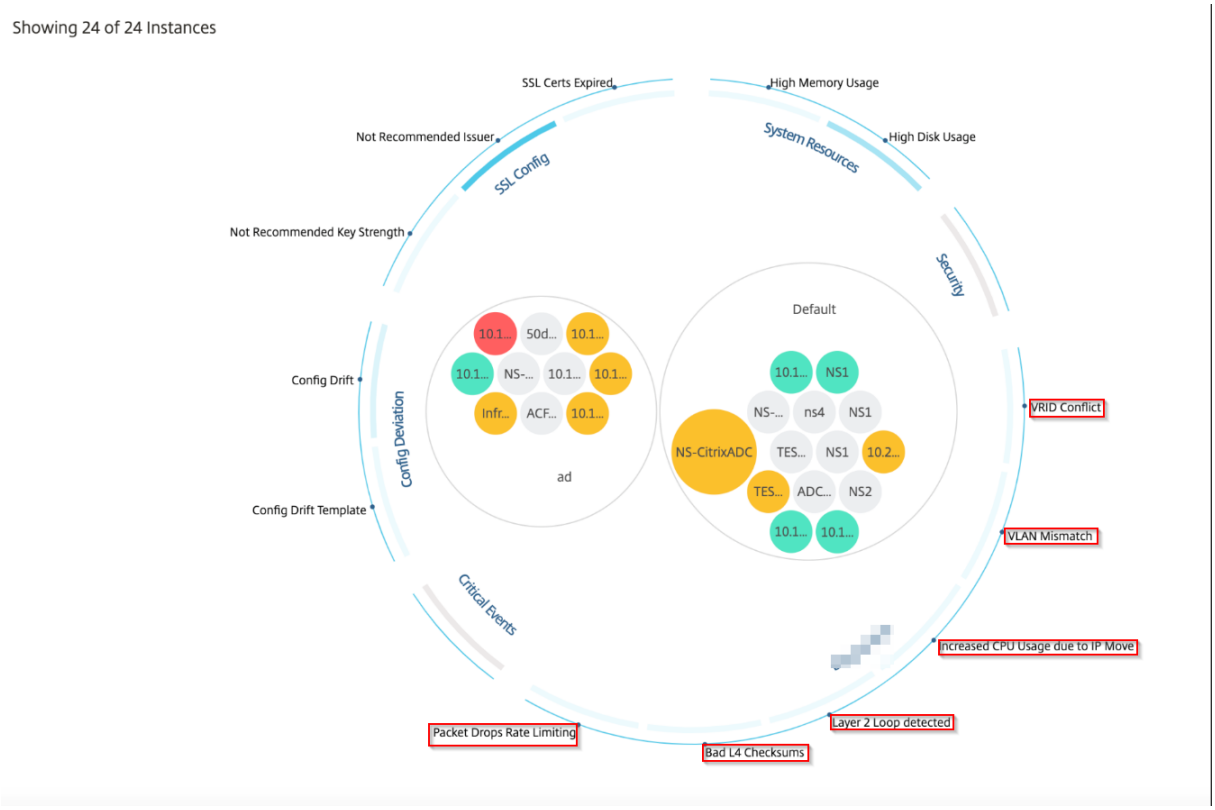
> **Nota**
>
> Los indicadores de reglas no son compatibles con:
>
> - Instancias de NetScaler ADC configuradas en modo de clúster.
> - Instancias NetScaler ADC configuradas con particiones de administración.

En NetScaler ADM, vaya a **Redes** > **Infrastructure Analytics** para ver los indicadores de:

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

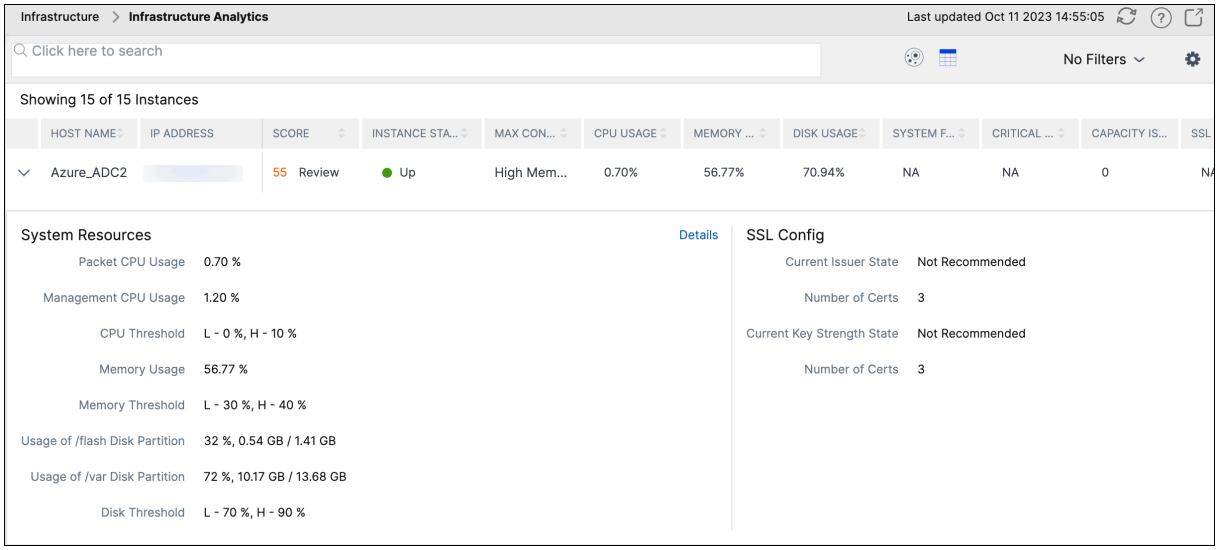
| Nombre del indicador en Infrastructure Analytics | Descripción |
|---|---|
| **Error de asignación de puertos** | Detecta cuándo NetScaler ADC usa SNIP para comunicarse con una nueva conexión de servidor y el total de puertos disponibles en ese SNIP está agotado. La acción recomendada es agregar otro SNIP en la misma subred. |
| **No hay configuración de ruta predeterminada** | Detecta cuándo se interrumpe el tráfico debido a la falta de disponibilidad de rutas. |
| **Conflicto de IP** | Detecta si se configura o se aplica una misma dirección IP en dos o más instancias de una red. |
| **Conflicto de VRID** | Detecta cuando se producen problemas de acceso intermitentes para el VRID especificado. |
| **Discordancia de VLAN** | Detecta si se produce algún error durante la configuración de la VLAN enlazada a las subredes IP. |
| **Ataque de ventana pequeña TCP** | Detecta si hay un posible ataque a una ventana pequeña en curso. Esta alerta es solo a título informativo, porque ADC ya mitiga este ataque. |
| **umbral de control de velocidad** | Detecta cuándo se descartan paquetes según el umbral de control de velocidad configurado. |
| **Límite de persistencia** | Detecta cuándo se impone el máximo de visitas a la memoria NetScaler ADC. |
| **No coincide el nombre del sitio de GSLB** | Detecta cuándo se producen errores de sincronización de la configuración de GSLB debido a una falta de coincidencia en |
| **Encabezado IP con formato incorrecto** | Detecta cuándo fallan las comprobaciones de seguridad de los paquetes IPv4. |
| **Sumas de comprobación L4 incorrectas** | Detecta si la validación de la suma de comprobación para los paquetes TCP falla. |
| **Mayor uso de CPU debido al movimiento de IP** | Detecta si es necesario actualizar un gran número de equipos Mac. |
| **Dirección excesiva de paquetes** | Detecta altos niveles de dirección de paquetes de software debido al uso del tipo de clave rss asimétrica. |
| **Loop de capa 2** | Detecta la presencia de bucles de capa 2 en la red. |
| **Discordancia de VLAN etiquetada** | Detecta cuándo se reciben paquetes de VLAN etiquetados en una interfaz sin etiquetar. |

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 




## Vista tabular

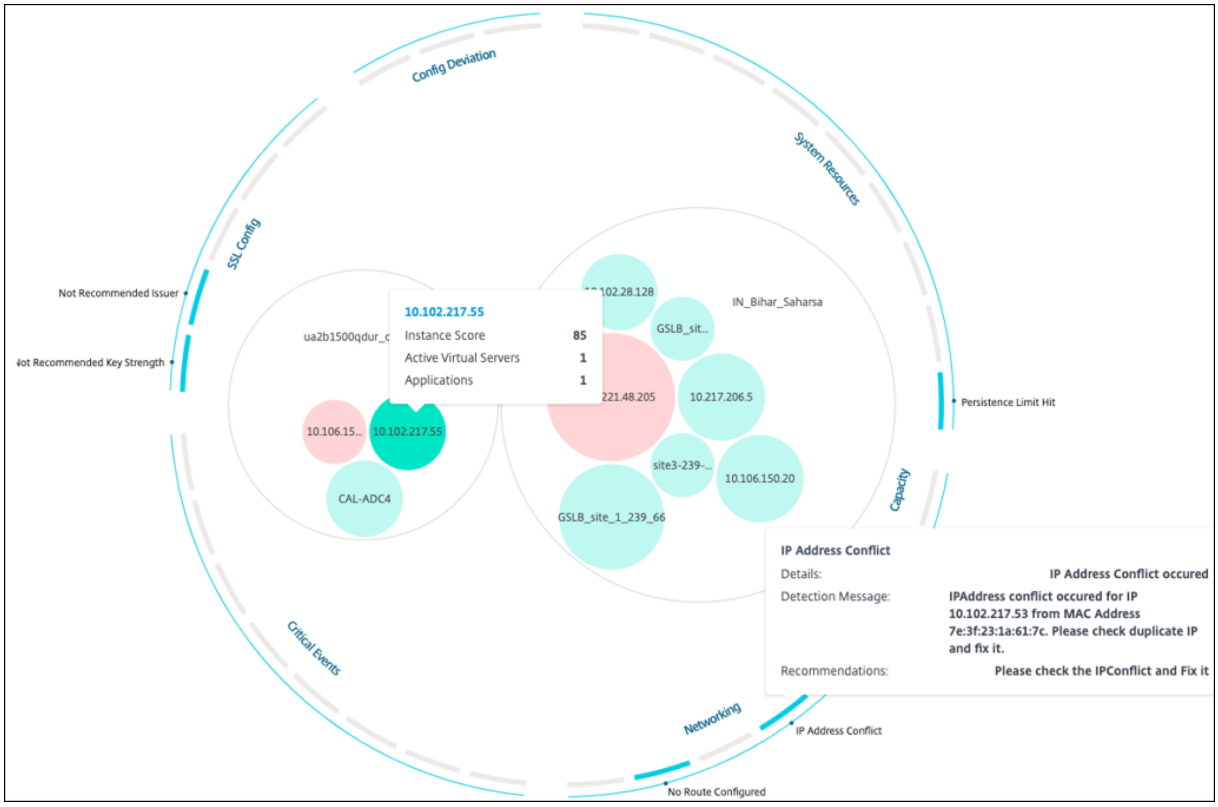
También puede ver anomalías mediante la opción de vista tabular en **Infrastructure Analytics**. Vaya a **Redes** > **Análisis de infraestructura** y, a continuación, haga clic en para mostrar todas las instancias administradas. Haga clic en > para ampliar y obtener más información




© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### Ver detalles de una anomalía

Por ejemplo, si desea ver los detalles del **conflicto de direcciones IP** en la red, haga clic en la anomalía que aparece en relación con el conflicto de direcciones IP para ver los detalles.




- **Detalles**: Indica qué anomalía se ha detectado
- **Mensaje de detección**: Indica la dirección MAC para la que la dirección IP tiene el conflicto
- **Recomendaciones**: Indica el elemento de acción para resolver este conflicto de direcciones IP

## Preguntas frecuentes

January 30, 2024

En esta sección se proporcionan las preguntas frecuentes sobre las siguientes funciones de NetScaler Application Delivery Management (NetScaler ADM). Haga clic en el nombre de una función en la siguiente tabla para ver la lista de preguntas frecuentes de esa función.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

| Análisis | Autenticación | Administración de configuración |
|---|---|---|
| Administración de certificados | Implementación | Implementación (recuperación ante desastres) |
| Gestión de eventos | Administración de instancias | StyleBooks |
| Administración del sistema | | |

## Análisis

### ¿Es necesario habilitar el canal virtual EUEM en instancias de NetScaler Gateway implementadas en modo de salto único?

Los datos de canal virtual de EUEM forman parte de los datos de HDX Insight que el Citrix ADM recibe de instancias de Gateway. El canal virtual EUEM proporciona los datos sobre ICA RTT. Si el canal virtual EUEM no está habilitado, los datos restantes de HDX Insight se seguirán mostrando en NetScaler ADM.

El canal virtual EUEM es un servicio predeterminado que se ejecuta en las aplicaciones Citrix Virtual Desktop (VDA). Si no se está ejecutando, inicie el proceso “Citrix End User Experience Monitoring”en los servicios de VDA.

### ¿Cómo puedo habilitar NetScaler ADM para supervisar el tráfico de aplicaciones web y escritorios virtuales?

1. Vaya a **Infraestructura** > **Instancias** > **NetScaler ADC** y seleccione la instancia de NetScaler ADC en la que quiere habilitar el análisis.
2. En la lista **Seleccionar acción**, seleccione **Configurar análisis**.
3. En la página **Configurar análisis** que se abre, seleccione todos los servidores virtuales en los que quiere habilitar el análisis y haga clic en **Habilitar AppFlow**. Para obtener más información, consulte Cómo habilitar el análisis en instancias.

> Nota
>
> Para las instancias NetScaler ADC de la versión 11.0, versión 65.30 y versiones posteriores, no hay ninguna opción en NetScaler ADM para habilitar Security Insight explícitamente. Asegúrese de configurar los parámetros de AppFlow en las instancias NetScaler ADC, de modo que NetScaler ADM comience a recibir el tráfico de Security Insight junto con el tráfico de Web Insight. Para obtener más información sobre cómo establecer los parámetros de AppFlow en las instancias

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

> de NetScaler ADC, consultePara establecer los parámetros de AppFlow mediante la utilidad de configuración.

**Después de agregar las instancias NetScaler ADC, ¿NetScaler ADM comienza automáticamente a recopilar información analítica?**

No. Habilite el análisis en los servidores virtuales alojados en instancias de NetScaler ADC administradas por NetScaler ADM. Para obtener más información, consulte Cómo habilitar el análisis en las instancias.

**¿Es necesario acceder al dispositivo NetScaler ADC individual para habilitar el análisis?**

No. Toda la configuración se realiza desde la interfaz de usuario de NetScaler ADM, que enumera los servidores virtuales alojados en la instancia específica de NetScaler ADC. Para obtener más información, consulte Cómo habilitar el análisis en las instancias.

**¿Cuáles son los tipos de servidores virtuales que se pueden enumerar en una instancia de NetScaler ADC para habilitar el análisis?**

Actualmente, la interfaz de usuario de NetScaler ADM incluye los siguientes servidores virtuales para permitir el análisis:

- Servidor virtual de equilibrio de carga
- Servidor virtual de conmutación de contenido
- Servidor virtual VPN
- Servidor virtual de redirección de caché

**¿Cómo conecto un disco adicional a NetScaler ADM?**

Para adjuntar un disco adicional a NetScaler ADM:

1. Apague la máquina virtual NetScaler ADM.
2. En el hipervisor, conecte un disco adicional del tamaño de disco requerido a la máquina virtual NetScaler ADM.

   Por ejemplo, Consideremos que quiere aumentar el espacio en disco a 200 GB, en una máquina virtual NetScaler ADM de 120 GB. En este caso, debe adjuntar un espacio en disco de 200 GB en lugar de 80 GB. Los 200 GB de espacio en disco recién conectados se utilizarán para almacenar datos de base de datos, archivos de registro NetScaler ADM. Los 120 GB de espacio en disco

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

existentes se utilizan para almacenar archivos principales, archivos de registro del sistema operativo, etc.

3. Inicie la máquina virtual NetScaler ADM.

#### ¿Qué quiere decir con que los recopiladores no están configurados en las instancias de NetScaler ADC?

Un recopilador recibe los registros de AppFlow generados por el dispositivo NetScaler ADC.

NetScaler ADM recibe tráfico de Security Insight y Web Insight de las instancias de NetScaler ADC cuando la función AppFlow está habilitada. Cuando habilita la función AppFlow en una instancia de NetScaler ADC, debe especificar al menos un recopilador al que se envían los registros de AppFlow. Si los recopiladores no están configurados en las instancias de NetScaler ADC, NetScaler ADM no recibe el tráfico de las instancias.

Por ejemplo, se agregan cinco instancias de NetScaler ADC a NetScaler ADM. Si no se especifican recopiladores para dos instancias, no fluye tráfico a NetScaler ADM. Los diagnósticos de autoservicio detectan el problema y lo muestran como "Los recopiladores no están configurados en 2 instancias. "

Para obtener más información sobre cómo configurar la función AppFlow, consulte Configuración de la función AppFlow.

#### ¿Qué hace la habilitación de mediciones del lado del cliente?

Con las mediciones del lado del cliente habilitadas, ADM captura el tiempo de carga y las métricas de tiempo de representación para páginas HTML, mediante inyección HTML. Mediante estas métricas, los administradores pueden identificar problemas de latencia L7.

### Autenticación

#### ¿Qué es el equilibrio de carga de las solicitudes de autenticación?

La función de equilibrio de carga del servidor de autenticación permite a NetScaler ADM equilibrar la carga de las solicitudes de autenticación que se dirigen a los servidores de autenticación externos. El equilibrio de carga de los servidores de autenticación garantiza que la carga de autenticación se divida entre varios servidores de autenticación y, por lo tanto, evita que un servidor de autenticación se sobrecargue. Puede crear un servicio de autenticación para conectarse y obtener información de usuario de su servidor de autenticación externo existente mediante protocolos de autenticación como LDAP, RADIUS o TACACS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ¿Por qué necesitamos conectar servidores de autenticación externos en cascada?

Los servidores de autenticación externos en cascada proporcionan un procesamiento de autenticación ininterrumpido, lo que permite el acceso a usuarios legítimos en caso de que falle un servidor de autenticación. No hay límite en cuanto a los tipos de servidores de autenticación que se pueden aplicar en cascada. Puede tener todos los servidores de RADIUS, todos los servidores de LDAP o una combinación de servidores de RADIUS y LDAP.

### ¿Cuántos servidores de autenticación externos puedo conectar en cascada?

Puede conectar en cascada hasta 32 servidores de autenticación externos en NetScaler ADM.

### ¿Tengo una alternativa cuando falla la autenticación externa?

Puede haber una situación en la que la autenticación externa falle por completo, incluso cuando haya conectado varios servidores en cascada. Por ejemplo, es posible que no se pueda acceder a los servidores externos o que no se hayan introducido las credenciales de un nuevo usuario en ninguno de los servidores de autenticación externos. Para evitar el bloqueo de usuarios en tal situación, puede habilitar la autenticación local de reserva. Para obtener más información, consulteAutenticación local alternativa.

### ¿Qué es la autenticación local de reserva?

La autenticación local alternativa es una opción para autenticar a los usuarios localmente cuando la autenticación externa falla. Si falla la autenticación externa, NetScaler ADM accede a la base de datos de usuarios local para autenticar a los usuarios.

En Citrix ADM, vaya a **Sistema** > **Autenticación** > **Configuración de autenticación** . En esta página, puede agregar varios servidores de autenticación externos en una cascada y seleccionar la opción **Habilitar autenticación local de reserva**.

### ¿Qué es una extracción de grupos de usuarios externos?

Si ha agregado servidores externos para autenticar a los usuarios, puede importar (extraer) grupos de usuarios existentes en NetScaler ADM. Debe importar los grupos de usuarios una vez y proporcionar un permiso de grupo a un grupo de usuarios en lugar de importar usuarios individuales y darles permisos individuales. No tiene que volver a crear los usuarios en NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ¿Por qué necesitamos asignar permisos de grupo?

Cuando utiliza la función de equilibrio de carga de NetScaler ADC, puede integrar NetScaler ADM con servidores de autenticación externos e importar información de grupos de usuarios desde los servidores de autenticación. Inicie sesión en NetScaler ADM y cree manualmente la misma información de grupo en NetScaler ADM y asigne permisos a esos grupos. El permiso de usuario y grupo de usuarios se administra en NetScaler ADM y no en el servidor externo. Los usuarios tienen diferentes permisos de acceso basados en funciones en los servidores externos. Configure los mismos permisos para los usuarios de NetScaler ADM también. En lugar de configurar los permisos individualmente para cada usuario, puede configurar un permiso de nivel de grupo para que los miembros del grupo de usuarios puedan acceder a servicios específicos en los servidores virtuales con equilibrio de carga. Los permisos típicos que puede asignar son permisos para administrar instancias de NetScaler ADC, instancias de Citrix SDX, servidores virtuales, etc., de modo que los usuarios de ese grupo puedan administrar solo esas instancias o servidores virtuales. Más adelante podrá modificar los permisos otorgados a los usuarios a nivel de grupo. Incluso puede eliminar uno o más grupos de usuarios; otros usuarios del grupo seguirán funcionando en NetScaler ADM.

## Administración de configuración

### ¿Puedo realizar la configuración en varias instancias de NetScaler ADC simultáneamente con NetScaler ADM?

Sí, puede usar trabajos de configuración para realizar la configuración en varias instancias de NetScaler ADC.

### ¿Qué son los trabajos de configuración en NetScaler ADM?

Un trabajo es un conjunto de comandos de configuración que puede crear y ejecutar en una o más instancias administradas. Puede crear trabajos para realizar cambios de configuración en todas las instancias, replicar configuraciones en varias instancias de la red y realizar tareas de configuración de grabación y reproducción mediante la GUI de NetScaler ADM. También puede convertir las tareas grabadas en comandos de CLI.

Puede utilizar la función Trabajos de configuración de NetScaler ADM para crear un trabajo de configuración, enviar notificaciones por correo electrónico y comprobar los registros de ejecución de los trabajos creados.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

#### ¿Puedo programar trabajos con plantillas integradas en NetScaler ADM?

¡Sí! Puede programar un trabajo mediante la opción de plantilla integrada. Un trabajo es un conjunto de comandos de configuración que puede ejecutar en una o más instancias administradas. Por ejemplo, puede utilizar la opción de plantilla integrada para programar un trabajo para configurar servidores syslog. Puede optar por ejecutar el trabajo inmediatamente o programar el trabajo para que se ejecute más tarde.

Puede guardar la configuración de un trabajo creado previamente y volver a ejecutar el trabajo después de modificar los comandos, los parámetros, el origen de configuración y las instancias de destino. Esto resulta útil cuando el mismo conjunto de comandos tiene que ejecutarse en una instancia diferente, o cuando el trabajo encuentra un error y detiene la ejecución posterior.

### Administración de certificados

#### ¿La eliminación de certificados SSL de NetScaler ADM conduce a la eliminación de certificados de las instancias de NetScaler ADC?

No

### Implementación

#### ¿Cuáles son el nombre de usuario y la contraseña predeterminados?

- Después de completar la configuración de red inicial, puede iniciar sesión en NetScaler ADM desde el hipervisor o la consola SSH, con el nombre de usuario y la contraseña predeterminados (nsrecover/nsroot).
- El nombre de usuario y la contraseña predeterminados para iniciar sesión desde la GUI son *nsroot/nsroot*.

#### ¿Cómo cambiar la contraseña predeterminada?

Para cambiar la contraseña:

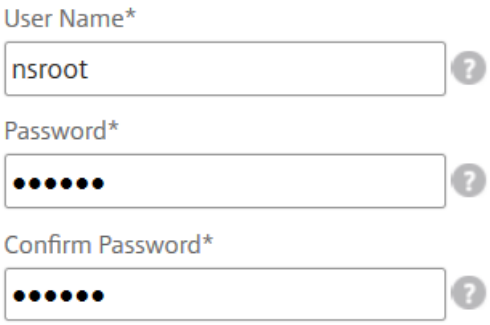
1. En Citrix ADM, vaya a **Sistema** > **Administración** de **usuarios > Usuarios**.

   Se muestra la página Usuarios.
2. Seleccione el nombre de usuario **nsroot** y haga clic en **Modificar**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Se muestra la página Configurar usuario del sistema.

3. Seleccione **Cambiar contraseña** y cree una contraseña de su elección.




4. Haga clic en **Aceptar**.

   Ahora puede usar la nueva contraseña para iniciar sesión desde la GUI y el hipervisor o la consola SSH.

   > Nota
   >
   > No puede modificar el nombre de usuario.

**¿Cómo restablecer la contraseña?**

Puede ver esta documentación para restablecer la contraseña.

**En un par de alta disponibilidad, si la contraseña se cambia en el nodo principal y si la opción Romper par de alta disponibilidad se selecciona más adelante, ¿cuál es el comportamiento?**

Puede iniciar sesión en ambos nodos independientes con su nueva contraseña.

**Si dos servidores independientes tienen contraseñas diferentes, ¿cuál es el impacto de la implementación de estos dos servidores en un par de alta disponibilidad?**

Se recomienda tener una contraseña predeterminada para ambos servidores cuando implemente dos servidores independientes en el par de alta disponibilidad.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**La configuración de HA está completa, pero no se puede acceder a la GUI del nodo principal. ¿Cuál puede ser la razón?**

La configuración tarda unos minutos en surtir efecto. Puede intentar acceder de nuevo después de unos minutos.

**La configuración de HA está completa, pero no se puede acceder a la GUI de la dirección IP flotante. ¿Cuál puede ser la razón?**

Después de la configuración de alta disponibilidad, primero debe acceder a la GUI del nodo principal y completar la implementación. Para obtener más información, consulte Implementar el nodo principal y el secundario como un par de alta disponibilidad. Una vez completada la implementación, el servidor se reinicia y se prepara para la implementación de alta disponibilidad. A continuación, puede acceder a la GUI de la dirección IP flotante.

**¿Qué base de datos admite NetScaler ADM independiente y NetScaler ADM HA?**

Tanto NetScaler ADM independiente como NetScaler ADM HA admiten PostgreSQL.

**¿Cuál es la posible pérdida de datos en el nodo secundario?**

El nodo secundario escucha los mensajes de latido que el nodo principal envía a través de la base de datos NetScaler ADM. Si el nodo secundario no recibe los latidos durante más de 180 segundos, el nodo secundario realiza una comprobación basada en SSH en el nodo principal. Si el latido y la comprobación basada en SSH fallan, se considera que el nodo principal está inactivo.

En este caso, el nodo secundario pasa a ser el nodo principal y el período de 180 segundos se puede considerar como la posible pérdida de datos en el nodo secundario.

**¿Qué ocurre si el nodo principal está inactivo?**

El nodo secundario se hace cargo y se convierte en el nodo principal.

**¿Cómo volver a instalar el nodo que ha fallado?**

Se recomienda instalar una compilación de VM nueva. Para volver a instalar:

1. Rompe el par de alta disponibilidad. Navegue hasta **Sistema** > **Implementación**

   Se muestra la página de implementación. Haga clic en **Romper alta disponibilidad**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

2. Elimine el nodo fallido del Hypervisor.
3. Importe el archivo de imagen XVA al hipervisor.
4. En la ficha Consola, configure Citrix ADM con las configuraciones de red iniciales. Para obtener más información, consulte Registrar e implementar el primer servidor (nodo principal) y Registrar e implementar el segundo servidor (nodo secundario).
5. Reimplemente el par de alta disponibilidad.

#### ¿NetScaler ADM admite almacenamiento SAN?

Citrix recomienda hospedar NetScaler ADM VHD en un almacenamiento local. Cuando se aloja en dispositivos de almacenamiento en una SAN, es posible que NetScaler ADM no funcione como se esperaba. Por lo tanto, no se admite la implementación de ADM en SAN.

#### ¿Admite NetScaler ADM un disco adicional?

Sí. Una nueva instalación del par NetScaler ADM HA asigna 120 GB de almacenamiento de forma predeterminada. Para obtener más de 120 GB de almacenamiento, puede agregar un disco adicional para obtener un máximo de 3 TB de almacenamiento. No se admite la adición de más de un disco adicional.

#### Después de inhabilitar el par de alta disponibilidad, ¿qué sucede con la dirección IP flotante configurada?

Ya no se puede acceder a la dirección IP flotante y debe volver a implementar el par de alta disponibilidad.

#### ¿Puedo dar una dirección IP flotante diferente al volver a implementar?

Sí. Puede configurar una nueva dirección IP flotante.

#### ¿Por qué no es accesible la GUI del nodo secundario?

El nodo secundario es solo un servidor de réplicas de lectura y actúa como nodo principal solo si el nodo principal está inactivo por cualquier motivo. Citrix recomienda acceder a la GUI del nodo principal o a la GUI de direcciones IP flotantes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Si el nodo principal está inactivo durante un período prolongado, ¿se pueden realizar las configuraciones con la GUI de direcciones IP flotantes?**

Sí. Puede seguir realizando configuraciones y las configuraciones se guardan en el nodo secundario. Cuando el nodo principal regresa, se sincronizarán todas las configuraciones.

**Si es necesario cambiar la dirección IP del nodo principal o la dirección IP del nodo secundario o la dirección IP flotante en el futuro (por ejemplo, cambiarla a IPv6), ¿cuáles son las soluciones recomendadas?**

No se admite el cambio de direcciones IP en el par de alta disponibilidad sin romper el par de alta disponibilidad.

Para actualizar la dirección IP del nodo principal o del nodo secundario:

1. Rompe el par de alta disponibilidad. Navegue hasta **Sistema** > **Implementación** .

   Aparecerá la página Implementación. Haga clic en **Romper alta disponibilidad**.

   a) Inicie sesión en el nodo principal mediante un cliente SSH o desde el hipervisor.

   b) Use `nsrecover` como nombre de usuario e introduzca la contraseña que ha establecido.

   c) Introduzca **networkconfig**. Realice el procedimiento del **paso 3** disponible en Register e implemente el primer servidor (nodo principal).

      Durante la configuración de red inicial, puede proporcionar una dirección IP diferente.

   d) Realice el mismo procedimiento para el nodo secundario y continúe con el procedimiento del **paso 3** disponible en Registrar e implementar el segundo servidor (nodo secundario).

Para actualizar la dirección IP flotante:

1. Navegue hasta **Sistema** > **Implementación** .

   Aparecerá la página Implementación.

   a) Haga clic en **Configuración de HA**.

   b) Haga clic en **Configurar dirección IP flotante para el modo de alta disponibilidad**.

   c) Introduzca la dirección IP flotante y haga clic en **Aceptar**.

**¿ADM admite procesadores AMD?**

No. ADM no admite procesadores AMD.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

## Implementación (recuperación ante desastres)

### ¿Con qué frecuencia se produce la replicación entre el sitio principal y el sitio de recuperación ante desastres?

La replicación entre el sitio principal y el sitio de recuperación ante desastres es en tiempo real.

### Después de iniciar el script de reserva en el sitio de recuperación ante desastres, ¿el sitio de recuperación ante desastres se convierte en el sitio primario temporal hasta que el sitio principal se recupera y funciona completamente?

No. El sitio de recuperación ante desastres se convertirá ahora en el sitio principal. Para revertir el par de alta disponibilidad como sitio principal, consulte Revertir configuraciones al sitio principal original

### Si se selecciona la opción Pareja de HA, ambos nodos funcionan como un servidor independiente. Dado que la compatibilidad con DR no se aplica al servidor independiente, ¿qué ocurre con el sitio de recuperación ante desastres si se selecciona Romper par de alta disponibilidad?

Si selecciona la opción Romper par de alta disponibilidad, se termina la replicación entre el sitio principal y el sitio de DR. Debe volver a configurar el sitio de recuperación ante desastres como parte de la reimplementación del par de alta disponibilidad.

## Gestión de eventos

### ¿Cómo puedo hacer un seguimiento de todos los eventos que se han generado en mis instancias de NetScaler ADC administradas con NetScaler ADM?

Como administrador de red, puede ver detalles como cambios de configuración, condiciones de inicio de sesión, errores de hardware, violaciones de umbrales y cambios de estado de la entidad en sus instancias de NetScaler ADC, junto con los eventos y su gravedad en instancias específicas. Puede usar el panel de eventos de NetScaler ADM para ver los informes generados para los detalles de gravedad de eventos críticos en todas las instancias de NetScaler ADC.

### ¿Qué son las reglas del evento?

Con NetScaler ADM, puede configurar reglas para supervisar eventos específicos. Las reglas de eventos facilitan la supervisión de una gran cantidad de eventos generados en la infraestructura de Citrix ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

Puede filtrar un conjunto de eventos configurando reglas con condiciones específicas y asignando acciones a las reglas. Cuando los eventos generados cumplen los criterios de filtro de la regla, se ejecuta la acción asociada a la regla.

Las condiciones para las que puede crear filtros son gravedad, instancias NetScaler ADC, categorías y objetos de error. Las acciones que puede asignar a los eventos son el envío de una notificación por correo electrónico, el reenvío de capturas SNMP desde las instancias administradas de NetScaler ADC a NetScaler ADM y el envío de una notificación por SMS.

## Administración de instancias

### ¿Qué sucede si una instancia de ADC no puede conectarse a ADM después de la asignación de ancho de banda cuando se utiliza la licencia de capacidad agrupada de NetScaler ADC?

Si falla el latido entre la instancia de ADC y ADM, la instancia entra en un período de gracia de 30 días. Y después de restablecer la comunicación, las licencias de capacidad agrupadas comienzan a funcionar. Cuando se encuentra en período de gracia, las funciones ADC no se ven afectadas. Después de 30 días de período de gracia, la instancia de ADC inicia el reinicio en caliente y no tiene licencia.

### ¿Qué son los centros de datos en NetScaler ADM?

Un centro de datos NetScaler ADM es una agrupación lógica de las instancias de NetScaler ADC en una ubicación geográfica específica. Cada servidor puede supervisar y administrar varias instancias de NetScaler ADC dentro de un centro de datos. Puede usar el servidor Citrix ADM para administrar datos como el syslog, el flujo de tráfico de aplicaciones y las capturas de SNMP de las instancias administradas. Para obtener más información sobre la configuración de centros de datos, consulte Cómo configurar centros de datos para geomapas en Citrix ADM.

### ¿Cuáles son los diferentes dispositivos Citrix compatibles con NetScaler ADM?

Las instancias son los dispositivos Citrix o los dispositivos virtuales que quiere descubrir, administrar y supervisar desde NetScaler ADM. Debe agregar estas instancias al servidor de NetScaler ADM. Puede agregar los siguientes dispositivos Citrix y dispositivos virtuales a Citrix ADM:

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Citrix SD-WAN PE

Puede agregar instancias mientras configura el servidor Citrix ADM por primera vez o más tarde.

### ¿Qué es un perfil de instancia?

NetScaler ADM utiliza un perfil de instancia para acceder a una instancia.

Un perfil de instancia contiene el nombre de usuario y la contraseña para acceder a una o más instancias. Hay un perfil predeterminado disponible para cada tipo de instancia. Por ejemplo, ns-root-profile es el perfil predeterminado para las instancias de Citrix ADC. Contiene las credenciales de administrador de NetScaler ADC predeterminadas. Cuando cambias las credenciales necesarias para acceder a las instancias, puede definir perfiles de instancia personalizados para esas instancias.

### ¿Podemos agregar instancias de SD-WAN ilimitadas en NetScaler ADM? ¿NetScaler ADM puede gestionar todos los contadores escalares y vectoriales para SD-WAN?

Actualmente, no hay límite de licencias para las instancias de SD-WAN que se pueden agregar a NetScaler ADM. NetScaler ADM tiene un conjunto de informes integrados que sondea internamente los contadores escalares y vectoriales.

### ¿Puedo detectar de nuevo varias instancias de Citrix VPX en NetScaler ADM?

Sí, puede redescubrir varias instancias de Citrix **VPX** en NetScaler ADM para conocer los estados y configuraciones más recientes de las instancias.

Vaya a **Redes** > **Instancias** > **NetScaler ADC > VPX,** seleccione las instancias que quiere volver a detectar y, en la lista **Acción**, haga clic en **Redescubrir**. Para obtener más información, consulte Cómo redescubrir varias instancias VPX.

### ¿Se puede instalar NetScaler ADM en Citrix SDX?

No

### ¿Puedo agregar una instancia de NetScaler ADC en el software ADM mediante una dirección IP pública?

Sí, puede hacerlo mediante la traducción de direcciones de red (NAT).

- Para agregar una sola instancia: utilice la IP NAT de la dirección IP pública de la instancia de ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- Para agregar un par de HA de ADC: agregue las direcciones IP de NAT del par de HA en este formato:

  `<NAT public IP of the primary instance>#<NAT public IP of the secondary instance>`

- Para agregar un clúster de ADC: agregue todas las direcciones IP públicas de NAT de todas las instancias del clúster, cada una separada por una coma, y agregue la IP de NAT de la IP DEL CLÚSTER entre paréntesis o corchetes. Un formato de ejemplo: NAT1, NAT2, NAT3,(NATIP de CLUSTERIP).

Para obtener más información, consulte estos temas:

- Agregar instancias a Citrix ADM
- Configuración de la traducción de direcciones de red

#### ¿Cómo registrar un nodo de recuperación ante desastres si se cambian las credenciales del nodo de recuperación ante desastres?

Restablezca las credenciales del nodo de recuperación ante desastres (DR) a`nsrecover`/`nsroot` mediante el siguiente comando:

```
./mps/change_freebsd_password.sh <username> <password>
```

Para registrar un nodo de DR, siga los pasos de Implementar y registrar el nodo de DR de NetScaler ADM mediante la consola de DR.

### StyleBooks

#### ¿Se pueden usar StyleBooks para configurar diferentes instancias de NetScaler ADC que se ejecutan en diferentes versiones del software NetScaler ADC?

Sí, puede utilizar StyleBooks para configurar diferentes instancias de NetScaler ADC que se ejecuten en versiones diferentes si no hay discrepancia entre los comandos entre diferentes versiones.

#### Cuando se utiliza un StyleBook para configurar varias instancias de NetScaler ADC al mismo tiempo y se produce un error en la configuración de una instancia de NetScaler ADC, ¿qué sucede?

Si se produce un error al aplicar la configuración a una instancia de NetScaler ADC, la configuración no se aplica a más instancias y se deshacen las configuraciones ya aplicadas.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**¿Las copias de seguridad de NetScaler ADC realizadas a través de NetScaler ADC incluyen configuraciones aplicadas a través de StyleBooks?**

Sí

## Administración del sistema

**¿Puedo asignar un nombre de host a mi servidor NetScaler ADM?**

Sí, puede asignar un nombre de host para identificar su servidor NetScaler ADM. Para asignar un nombre de host, vaya a **Sistema** > **Administración del sistema** > **Configuración del sistema** y haga clic en **Cambiar nombre de host** .

El nombre del host se muestra en la licencia universal de NetScaler ADM. Para obtener más información, consulteCómo asignar un nombre de host a un servidor NetScaler ADM.

**¿Puedo realizar una copia de seguridad y restaurar mi configuración de NetScaler ADM?**

Sí, puede realizar copias de seguridad de los archivos de configuración (archivos NTP y certificados SSL), de los datos del sistema, de la infraestructura y de las aplicaciones, y de todas las configuraciones **SNMP**. Si su NetScaler ADM se vuelve inestable, puede utilizar los archivos de copia de seguridad para restaurar su NetScaler ADM a un estado estable.

Para realizar una copia de seguridad y restaurar la configuración de NetScaler ADM, vaya a **Sistema** > **Configuración avanzada** > **Archivos de copia de seguridad** y haga clic en **Copia de seguridad** o **Restaurar**, según sea el caso. Para obtener más información, consulteCómo realizar una copia de seguridad y restaurar la configuración en NetScaler ADM.

Citrix recomienda utilizar esta función antes de realizar una actualización o por motivos de precaución.

**¿Qué son los umbrales y las alertas en NetScaler ADM?**

Puede establecer umbrales y alertas para supervisar el estado de una instancia de NetScaler ADC y supervisar las entidades de las instancias administradas.

Cuando el valor de un contador supera el umbral, NetScaler ADM genera una alerta para indicar un problema relacionado con el rendimiento. Cuando el valor del contador vuelve al valor de borrado especificado en el umbral, el evento se borra.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

### ¿Puedo generar un archivo de asistencia técnica para NetScaler ADM?

Sí. Citrix recomienda generar un archivo de datos y estadísticas de NetScaler ADM antes de ponerse en contacto con la asistencia técnica para solucionar un problema. El archivo es un archivo TAR que puede enviar al equipo de soporte técnico.

Puede generar un archivo de soporte técnico que contenga registros de depuración, la duración durante la cual se recopilaron los registros de depuración y registros distintos y diversos de la base de datos de NetScaler ADM.

Para configurar y enviar un archivo de soporte técnico, vaya a **Sistema** > **Diagnóstico** > **Soporte técnico** y, a continuación, haga clic en **Generar archivo de soporte técnico** . Para obtener más información, consulteCómo generar un archivo de soporte técnico para NetScaler ADM.

### ¿Qué es la depuración de syslog?

Syslog es un protocolo estándar para el registro. Syslog permite el aislamiento del sistema que genera la información y del sistema que almacena la información. Puede consolidar la información de registro y obtener información de los datos recopilados. También puede configurar syslog para registrar diferentes tipos de eventos.

Para limitar la cantidad de datos de syslog almacenados en la base de datos, puede especificar el intervalo en el que quiere purgar los datos de syslog. Puede especificar el número de días tras los cuales se eliminarán de Citrix ADM todos los datos genéricos de Syslog, AppFirewall y Citrix Gateway.

### ¿Puedo configurar el servidor NTP en NetScaler ADM?

Puede configurar un servidor de Protocolo de hora de red (NTP) en NetScaler ADM para sincronizar el reloj de NetScaler ADM con el servidor de NTP. La configuración de un servidor NTP garantiza que el reloj NetScaler ADM tenga la misma configuración de fecha y hora que los demás servidores de la red.

Para configurar un servidor NTP, vaya a **Sistema** > **Servidores NTP** y, a continuación, haga clic en **Agregar**. Para obtener más información, consulteCómo configurar el servidor NTP en NetScaler ADM.

### ¿A partir de qué versión se admite la implementación de alta disponibilidad activa-pasiva de NetScaler ADM?

El modo de implementación de alta disponibilidad activa-pasiva de NetScaler ADM es compatible con la versión 12.0, compilación 51.24, de NetScaler ADM.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**Tenía una configuración de alta disponibilidad activa-activa de NetScaler ADM y había configurado un dispositivo NetScaler ADC con un servidor virtual de equilibrio de carga para un acceso unificado a la GUI. ¿Cómo actualizo esta configuración?**

Después de actualizar el par NetScaler ADM HA al modo activo-pasivo, debe ejecutar el siguiente comando en el dispositivo NetScaler ADC para actualizar la configuración de equilibrio de carga:

**add lb monitor** MAS_Monitor **TCP-ECV -send "GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n\"" "-recv "{\"status-code\":0, \"is_passive\":0}"-LRTM DISABLED**

**¿Puedo configurar el equilibrio de carga del par de alta disponibilidad de NetScaler ADM en una instancia de NetScaler ADC mediante el puerto 443?**

No, no puede configurar el equilibrio de carga del par de NetScaler ADM HA en una instancia de NetScaler ADC mediante el puerto 443.

Cuando configura `http-ecv` y `https-ecv` supervisa en NetScaler ADC, no supervisa correctamente los nodos de NetScaler ADM HA.

**¿Se puede utilizar un archivo de copia de seguridad del servidor NetScaler ADM para restaurar la configuración de otro servidor NetScaler ADM?**

Sí

**Después de que NetScaler ADM realice una copia de seguridad de una instancia de NetScaler ADC, ¿se puede usar ese archivo de copia de seguridad para restaurar la configuración de otra instancia de NetScaler ADC a través de NetScaler ADM?**

Sí. Descargue el archivo de respaldo de Citrix ADM, cárguelo en el repositorio de respaldo de otra instancia de Citrix ADC y restaure esa instancia. Asegúrese de que la información de red y la información de autenticación no entren en conflicto. Por ejemplo, compruebe si hay conflictos de direcciones IP o puertos, perfiles de contraseña que no coincidan. Asegúrese también de que la instancia VPX restaurada tenga la misma dirección NSIP y licencia NetScaler ADC que la que se realizó la copia de seguridad.

Antes de restaurar una instancia en un par de alta disponibilidad, asegúrese de que las direcciones IP y el estado (principal o secundario) almacenados en el archivo de respaldo coincidan con los de la configuración de alta disponibilidad original. Compruebe también que el nuevo primario y secundario tengan el mismo tipo de licencia NetScaler ADC.

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**¿Podemos obligar a Citrix ADM a utilizar una dirección SNIP para comunicarse con las instancias de Citrix ADC, en lugar de utilizar la dirección NSIP del servidor Citrix ADM?**

Sí, puede agregar una dirección SNIP (con administración habilitada) en NetScaler ADM para comunicarse con instancias de NetScaler ADC.

**Cuando hago copias de seguridad de instancias de NetScaler ADC en NetScaler ADM, ¿el resultado es una copia de seguridad completa o básica?**

Las copias de seguridad de las instancias de NetScaler ADC de NetScaler ADM son copias de seguridad completas.

**¿Existe una guía de solución de problemas para NetScaler ADM?**

Sí. Consulte https://support.citrix.com/article/CTX224502.

**¿Cómo se administran las instancias de NetScaler ADC cuando se produce una conmutación por error de alta disponibilidad de NetScaler ADM?**

Si la comprobación basada en latidos y SSH falla, se considera que el nodo principal está inactivo y el nodo secundario pasa a ser el nodo principal. Todas las instancias de NetScaler ADC se actualizan con los últimos detalles del nodo principal como destino de captura SNMP de forma predeterminada.

El nuevo nodo principal (activo) de NetScaler ADM comprueba si el nodo activo anteriormente estaba configurado como el recopilador AppFlow o servidor syslog; si lo era, el nuevo primario agrega los detalles del recopilador de AppFlow o del servidor syslog a la información enviada a las instancias.

Para syslog reemplaza los detalles del servidor antiguo.

**¿Qué ocurre cuando el nodo NetScaler ADM HA que se no funcionaba vuelve a funcionar?**

Después de volver al servicio, el nodo NetScaler ADM permanece pasivo a menos que el nodo activo conmute por error.

**¿Cómo se distribuyen las instancias de NetScaler ADC en los nodos de alta disponibilidad de NetScaler ADM?**

Todas las instancias de NetScaler ADC son administradas por el nodo principal de NetScaler ADM.

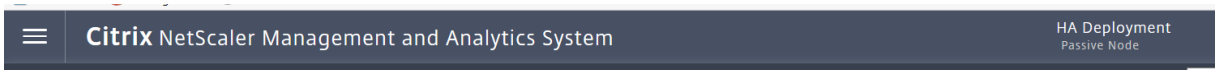
© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

**¿Cómo se administran las licencias de servidor virtual si hay una conmutación por error de alta disponibilidad de NetScaler ADM?**

Si el nodo principal de NetScaler ADM en el que se aplican las licencias de servidor virtual falla, el nuevo nodo principal administra las licencias de servidor virtual durante un período de gracia de 30 días. Vuelva a aplicar las licencias en el nuevo primario antes de que finalice el período de gracia. Para obtener alternativas, póngase en contacto con el soporte técnico de Citrix.

**¿Es obligatorio un equilibrador de carga para la configuración de NetScaler ADM HA?**

No, pero si no hay un equilibrador de carga, se debe acceder a los nodos NetScaler ADM a través de sus propias direcciones IP. El nodo pasivo está marcado con la etiqueta «Pasivo» y Citrix recomienda no crear ninguna configuración en el nodo pasivo.




**¿NetScaler ADM admite una base de datos externa?**

No

**¿Se puede usar una instancia de NetScaler ADC que administra NetScaler ADM como equilibrador de carga para la alta disponibilidad de NetScaler ADM?**

Sí

**¿Qué datos se sincronizan entre los nodos de HA de NetScaler ADM?**

Se sincroniza la base de datos completa de NetScaler ADM y se sincronizan las siguientes carpetas:

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/

© 1999–2025 Cloud Software Group, Inc. All rights reserved. 

- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.