Citrix Application Delivery Management 12.1

Machine translated content

Disclaimer

Contents

发行说明

February 6, 2024

Citrix Application Delivery Management (ADM) 12.1 发行说明描述了构建中的新功能、对现有功能的增强以及已知问题。12.1 版本的发行说明部分包括以下部分：

- 新增功能：内部版本中发布的现有功能的新增功能和增强功能。
- 已知问题：内部版本中存在的问题及其解决方法（如果适用）。
- 已修复的问题：内部版本中已解决的问题。

要查看完整的发行说明文档，请单击以下链接。

发行说明	出版日期	版本
Citrix ADM 12.1 版本的 Build 62.21 发布 Rotes	发布时间：2021 年 5 月 13 日	发行说明版本：1.0
Citrix ADM 12.1 版本的 Build 61.18 发布 Rotes	发布时间：2021 年 2 月 4 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 60.16 的发行说明	发布时间：2020 年 11 月 6 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 59.16 的发行说明	发布时间：2020 年 9 月 28 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 58.14 的发行说明	发布时间：2020 年 8 月 20 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 57.18 的发行说明	发布时间：2020 年 6 月 11 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 56.22 的发行说明	发布时间：2020 年 3 月 30 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 55.13 的发行说明	发布时间：2019 年 11 月 7 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 54.13 的发行说明	发布时间：2019 年 9 月 20 日；9 月 26 日更新	发行说明版本：2.0
Citrix ADM 12.1 版本的版本 53.12 的发行说明	发布时间：2019 年 8 月 28 日	发行说明版本：3.0
Citrix ADM 12.1 版本的版本 52.15 的发行说明	发布时间：2019 年 6 月 10 日	发行说明版本：1.0

发行说明	出版日期	版本
Citrix ADM 12.1 版本的 Build 50.43 版本的发行说明	发布时间：2019 年 5 月 17 日	发行说明版本：2.0
Citrix ADM 12.1 版本的 Build 50.39 版本的发行说明	发布时间：2019 年 5 月 17 日	发行说明版本：2.0
Citrix ADM 12.1 版本的 Build 50.33 的发行说明	发布时间：2019 年 4 月 16 日	发行说明版本：1.0
Citrix ADM 12.1 版本的 Build 50.30 的发行说明	发布时间：2019 年 1 月 14 日	发行说明版本：1.0
Citrix ADM 12.1 版本的 Build 50.28 的发行说明	发布时间：2018 年 12 月 1 日	发行说明版本：1.0
Citrix ADM 12.1 版本的版本 49.23 的发行说明	发布时间：2018 年 8 月 29 日	发行说明版本：1.0
Citrix ADM 12.1 版本的 Build 48.18 的发行说明	发布时间：2018 年 6 月 18 日	发行说明版本：2.0

> 注意
>
> 这些发行说明未记录安全相关的修复。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

快速入门

February 6, 2024

本文档将完整介绍如何首次开始部署和设置 Citrix Application Delivery Management (ADM)。本文档适用于管理 Citrix 网络设备（Citrix SD-WAN WO、Citrix Gateway 等）以及 HAProxy 等第三方设备的网络和应用程序管理员。无论您计划使用 Citrix ADM 管理的设备类型是什么，都请按照本文档中的步骤进行操作。

如果您是 Citrix ADM 的现有用户，建议您在将服务器 升级到最新 版本的 Citrix ADM 之前查看发行说明、系统要求 和 许可 详细信息。

步骤 **1-**检查系统要求

开始在数据中心中部署 Citrix ADM 之前，查看软件要求、浏览器要求、端口信息、许可证信息及限制。

- 许可证信息。可以在没有许可证的情况下管理和监视任何数量的实例和实体。但是，在未应用许可证的情况下，只能管理 30 个发现的应用程序以及只能查看 30 个虚拟服务器的分析信息。要管理 30 个以上的应用程序或要查看 30 个以上虚拟服务器的分析信息，必须购买相应的许可证。了解更多。
- 操作系统和接收器要求。查看此信息以确保您有适用于支持的操作系统的正确 Receiver 版本。了解更多。
- 浏览器要求。要访问 Citrix ADM GUI，必须确保您拥有所需的浏览器和版本正确。了解更多。
- 端口。确保 Citrix ADM 已打开所需的端口，以便与 Citrix ADC 或 SD-WAN 实例或 Citrix ADC 和 SD-WAN 实例进行通信。了解更多。
- **Citrix ADC** 实例要求。不同的 Citrix ADC 软件版本支持不同的 Citrix ADM 功能。查看此信息，以确保您已将 Citrix ADC 实例升级到正确版本。了解更多。
- **Citrix SD-WAN** 实例要求。查看此信息，以确保您已将 Citrix SD-WAN 实例升级到正确的版本，并且具有正确的平台版本。了解更多。

步骤 **2-**部署 **Citrix ADM**

要管理和监视应用程序和网络基础架构，必须首先在其中一个虚拟机管理程序上安装 Citrix ADM。您可以将 Citrix ADM 部署为单个服务器或高可用性模式。如果您要使用 Citrix ADC Insight Center，可以迁移至 Citrix ADM 并利用管理、监视、调配和应用程序管理功能以及分析功能。

- 单服务器部署。在 Citrix ADM 单服务器部署中，数据库与服务器集成，并且单个服务器处理所有流量。您可以使用 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 Citrix ADM。请参阅：
  - Citrix Hypervisor 上的 Citrix ADM
  - 搭载 Microsoft Hyper-V 的 Citrix ADM
  - 搭载 VMware ESXi 的 Citrix ADM
  - 搭载 Linux KVM 服务器的 Citrix ADM
- 高可用性部署。两台 Citrix ADM 服务器的高可用性部署 (HA) 可提供不间断的操作。在高可用性设置中，必须在主动-被动模式下部署两个 Citrix ADM 节点，在同一子网中使用相同的软件版本和内部版本，并且必须具有相同的配置。通过高可用性部署，在 Citrix ADM 主节点上配置浮动 IP 地址的功能消除了单独的 Citrix ADC 负载平衡器的需要。要了解更多信息，请参阅在高可用性部署中配置。

步骤 **3-**将实例添加到 **Citrix ADM**

实例是要从 Citrix ADM 发现、管理和监视的 Citrix 设备、虚拟设备或第三方设备。如果要管理和监视实例，必须将这些实例添加到 Citrix ADM 服务器。您可以将以下实例添加到 Citrix ADM 中：

- Citrix ADC

  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HAProxy

将实例添加到 Citrix ADM 服务器后，服务器会隐式与实例通信并收集这些实例的清单。

了解更多

步骤 **4 -** 在虚拟服务器上启用分析

要查看应用程序通信流的分析数据，必须在接收特定应用程序的流量的虚拟服务器上启用分析功能。

了解更多

步骤 **5-**在 **Citrix ADM** 上配置 **NTP** 服务器

在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

了解更多

步骤 **6-**配置系统设置以获得最佳 **Citrix ADM** 性能

在开始使用 Citrix ADM 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

- 配置系统警报。您必须配置系统警报，以确保您了解任何关键或主要的系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。
- 配置系统通知。您可以为各种系统相关功能选择用户组发送通知。您可以在 Citrix ADM 中设置通知服务器，还可以配置电子邮件和短消息服务 (SMS) Gateway 服务器以向用户发送电子邮件和文本通知。这可确保您将收到任何系统级活动（例如，用户登录或系统重新启动）通知。
- 配置系统修剪设置。要限制 Citrix ADM 服务器数据库中存储的报告数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时修剪一次（在 00.00 点）。
- 配置系统备份设置。Citrix ADM 每天 00:30 自动备份系统。默认情况下，它保存三个备份文件。您可能希望保留更多数量的系统备份。

- 配置实例备份设置。如果备份 Citrix ADC 实例的当前状态，则可以使用备份文件恢复稳定性，以防实例变得不稳定。在执行升级之前这样做尤其重要。默认情况下，每 12 小时进行一次备份，且有三个备份文件保留在系统中。
- 配置实例事件修剪设置。要限制 Citrix ADM 服务器数据库中存储的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。
- 配置实例 **syslog** 清除设置。要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定从 Citrix ADM 中删除以下系统日志数据的天数：
  - 通用系统日志数据
  - AppFirewall 数据
  - Citrix Gateway 数据。

  了解更多

接下来做什么

部署并设置了 Citrix ADM 后，可以开始管理和监视您的实例和应用程序。

管理 **Citrix ADC** 实例和应用程序。Citrix ADC 实例支持所有 Citrix ADM 功能。您可以开始使用任何功能。

管理 **Citrix ADC SD-WAN** 实例。SD-WAN WO 实例并非所有 Citrix ADM 功能都受支持，例如，不支持证书管理或配置审核。要了解支持哪些功能以及如何使用它们，请参阅使用 Citrix ADM 管理 Citrix SD-WAN WO。

管理 **HAProxy** 实例和应用程序。您可以监视 HAProxy 部署中配置的前端、后端和服务器。您还可以使用应用程序管理功能监视 Citrix ADM 监视的前端的实时统计信息。要了解 HAProxy 支持哪些功能以及如何使用这些功能，请参阅使用 Citrix ADM 管理和监视 HAProxy 实例。

所有操作方法文章

February 6, 2024

Citrix Application Delivery Management (Citrix ADM)“操作方法文章”是关于 Citrix ADM 功能的简单、相关且易于实施的文章。这些文章包含有关 Citrix ADM 一些常见功能（例如实例管理、应用程序管理、样书、证书管理及分析）的信息。

单击下表中的功能名称可以查看对应功能的方法文章列表。

主题				
实例管理	事件管理	样书	证书管理	Citrix ADM 系统

主题				
应用程序管理	配置管理	身份验证	分析	网络功能

实例管理

如何监视分布全球的站点

如何管理 Citrix ADC 实例的管理分区

如何向 Citrix ADM 中添加实例

如何在 Citrix ADM 上创建实例组

如何在 Citrix ADM 中为地理地图配置站点

如何使用 Citrix ADM 强制故障转移到辅助 Citrix ADC 实例

如何使用 Citrix ADM 强制辅助 Citrix ADC 实例保持辅助状态

如何使用 Citrix ADM 备份和还原实例

如何使用 Citrix ADM 控制板监视 HAProxy 实例

如何显示在 HAProxy 实例上配置的前端的详细信息

如何显示在 HAProxy 实例上配置的后端的详细信息

如何显示在 HAProxy 实例上配置的服务器的详细信息

如何从 Citrix ADM 重新启动 HAProxy 实例

如何使用 Citrix ADM 备份和还原 HAProxy 实例

如何使用 Citrix ADM 编辑 HAProxy 配置文件

如何重新发现多个 Citrix ADC VPX 实例

如何轮询 Citrix ADM 中的 Citrix ADC 实例和实体

如何在 Citrix ADM 上取消管理实例

如何跟踪从 Citrix ADM 到实例的路由

配置管理

如何在 Citrix ADM 上创建配置作业

如何在配置作业中使用 SCP (put) 命令

如何使用 Citrix ADM 升级 Citrix ADC SDX 实例

如何在 Citrix ADM 中安排使用内置模板创建的作业

如何重新安排使用 Citrix ADM 中的内置模板配置的作业

如何重用已执行的配置作业

如何使用 Citrix ADM 升级 Citrix ADC 实例

如何在 Citrix ADM 上的配置作业中使用变量

如何在 Citrix ADM 中使用配置模板创建审核模板

如何在 Citrix ADM 上使用纠正命令创建配置作业

如何在 Citrix ADM 中将正在运行和保存的配置命令从一个 Citrix ADC 实例复制到另一个实例

如何在 Citrix ADM 中为 Citrix SD-WAN WO 实例创建配置作业

如何使用录制和播放来创建配置作业

如何使用配置作业将配置从一个实例复制到多个实例

如何在 Citrix ADM 上使用主配置模板

如何轮询 Citrix ADC 实例的配置审核

如何在配置作业中重用配置审核模板

如何导入和导出配置模板

如何为 ConfigChange SNMP 陷阱生成配置审核差异

证书管理

如何在 Citrix ADM 中配置企业策略

如何通过 Citrix ADM 在 Citrix ADC 实例上安装 SSL 证书

如何从 Citrix ADM 更新已安装的证书

如何使用 Citrix ADM 链接和取消链接 SSL 证书

如何使用 Citrix ADM 创建证书签名请求 (CSR)

如何设置来自 Citrix ADM 的 SSL 证书到期通知

如何在 Citrix ADM 上使用 SSL 控制板

如何从 Citrix ADC 实例轮询 SSL 证书

应用程序管理

如何在 Citrix ADM 中创建应用程序定义

样书

如何查看不同的样书组

如何使用 Citrix ADM 附带的样书

如何创建自己的样书

如何在 Citrix ADM 中使用用户定义的样书

如何使用 API 基于样书创建配置

如何对在样书中定义的虚拟服务器启用分析和配置警报

如何创建样书以将文件上载到 Citrix ADM

如何使用 API 创建配置以上载任何文件类型

如何创建样书以将 SSL 证书文件和证书密钥文件上载到 Citrix ADM

如何使用 API 创建配置以上载证书和密钥文件

如何在企业中使用 Microsoft Skype for Business 样书

如何在企业中使用 Microsoft Exchange 样书

如何在企业中使用 Microsoft SharePoint 样书

分析

如何对实例启用分析

如何配置自适应阈值

如何配置 SLA 管理

如何配置用于分析的数据库汇总

如何使用 Citrix ADM 创建阈值和警报

如何从 Citrix ADM 禁用用于分析的 URL 数据收集

如何查看您的网络中通过流技术推送的视频类型和使用的数据量

如何查看特定时间范围内的峰值数据速率

如何比较 ABR 视频的优化和未优化的播放次数

如何比较 ABR 视频的优化和未优化的播放时间

如何比较优化和未优化 ABR 视频的带宽消耗

如何比较优化和未优化的 ABR 视频使用的数据量

如何查看网络效率

事件管理

如何在 Citrix ADM 上设置事件的事件期限

如何使用 Citrix ADM 安排事件过滤器

如何在 Citrix ADM 中设置事件的重复电子邮件通知

如何使用 Citrix ADM 禁止显示事件

如何使用事件控制板来监视事件

如何在 Citrix ADM 上创建事件规则

如何修改 Citrix ADC 实例上发生的事件的报告严重性

如何在 Citrix ADM 中查看事件摘要

如何在 Citrix ADM 上显示 SNMP 陷阱的事件严重性和 SNMP 陷阱偏差

如何使用 Citrix ADM 导出系统日志消息

如何在 Citrix ADM 中禁止显示 syslog 消息

如何配置实例事件的修剪设置

身份验证

如何级联外部身份验证服务器

如何添加 RADIUS 身份验证服务器

如何添加 LDAP 身份验证服务器

如何添加 TACACS 身份验证服务器

如何在 Citrix ADM 中提取身份验证服务器组

如何启用回退本地身份验证

Citrix ADM 系统

如何升级 Citrix ADM

如何重置 Citrix ADM 的密码

如何为 Citrix ADM 生成技术支持文件

如何在单个服务器部署中备份和还原 Citrix ADM 服务器

如何备份和还原高可用性对中的 Citrix ADM 配置

如何在 Citrix ADM 中为非默认用户启用 shell 访问权限

如何在 Citrix ADM 上配置 NTP 服务器

如何为 Citrix ADM 配置 SSL 设置

如何为 Citrix ADM 配置 syslog 清除时间间隔

如何查看 Citrix ADM 的审核信息

如何配置 Citrix ADM 的系统通知设置

如何监视 Citrix ADM 的 CPU、内存和磁盘使用情况

如何为 Citrix ADM 配置密码组

如何在 Citrix ADM 上创建 SNMP 陷阱、管理员和用户

如何为 Citrix ADM 服务器分配主机名

如何为 Citrix ADM 配置系统修剪设置

如何使用 Citrix ADM 配置系统备份设置

如何在 Citrix ADM 上配置和查看系统警报

如何诊断 Citrix ADC 实例并排除故障

网络功能

如何生成负载平衡实体的报告

如何导出或计划导出网络函数报告

概述

February 6, 2024

Citrix Application Delivery Management (ADM) 是一种集中式管理解决方案，通过为管理员提供企业范围的可视性，并自动执行需要跨多个实例执行的管理作业，从而简化了操作。您可以管理和监视 Citrix 应用程序网络产品，其中包括 Citrix ADC MPX、Citrix ADC VPX、Citrix ADC SDX、Citrix ADC CPX、Citrix Gateway 和 Citrix SD-WAN。可以使用 ADM 从单个统一的控制台对整个全局应用程序交付基础结构进行管理、监视和故障排除。

ADM 是一种在 Citrix Hypervisor、VMware ESXi 和 Linux KVM 上运行的虚拟设备。ADM 通过收集以下有关 Web 应用程序和虚拟桌面流量的详细信息，解决了应用程序可见性难题：

- 用户会话级别信息
- 网页性能数据
- 数据库信息流经站点的 ADC 实例，并提供可操作的报告。

ADM 使 IT 管理员能够在短短几分钟内进行故障排除并主动监视客户问题。

功能和解决方案

February 6, 2024

Citrix Application Delivery Management (ADM) 提供以下功能：

应用程序分析和管理

应用程序性能分析

“App Score”（应用程序分数）是定义应用程序执行良好情况的评分系统产品。它显示应用程序在响应方面的执行情况是否良好，是否不易遭受威胁，以及所有系统是否已启动并运行。

应用程序安全分析

“App Security Dashboard”（应用程序安全性控制板）提供应用程序的安全状态的历史视图。例如，它显示安全违规、签名违规和威胁指数等主要安全指标。应用程序安全控制面板还显示与攻击相关的信息，如 syn 攻击、小窗口攻击和已发现的 ADC 实例的 DNS 洪水攻击。

网络

Instances

使您能够管理 Citrix ADC、Citrix Gateway、Citrix SD-WAN 和 HAProxy 实例。

实例组

让您能够对您的实例分组，如下所示：

- 静态组：允许您定义可以在不同任务（例如配置作业等）中使用的设备组。
- 专用 IP 块：让您可以根据地理位置对您的实例分组。

事件管理

当 ADC 实例的 IP 地址添加到 ADM 时，ADM 会发送 NITRO 调用，并隐式地将自身添加为实例接收陷阱或事件的陷阱目标。

事件表示受管 ADC 实例上发生的事件或错误。

证书管理

Citrix ADM 现在可以为您简化证书管理的各个方面。通过一个控制台可以建立自动化策略以确保合适的颁发者、密钥强度和正确的算法，同时密切跟踪未使用或即将过期的证书。要开始使用 ADM 的 SSL 控制板及其功能，您必须了解什么是 SSL 证书，以及如何使用 ADM 跟踪 SSL 证书。

配置管理

Citrix ADM 允许您创建配置作业，以帮助您在多个实例上轻松执行配置任务，例如创建实体、配置功能、复制配置更改、系统升级和其他维护活动。配置作业和模板将最重复的管理任务简化为 ADM 上的单个任务。

配置审核

让您能够监视和识别您的实例中的配置的异常情况。

- 配置建议：让您可以识别配置异常情况。
- 审核模板：让您可以监视某个特定配置的变化。

网络报告

您可以通过监视 ADM 上的网络报告来优化资源使用情况。

分析

Web Insight

提供对企业 Web 应用程序的可见性，并允许 IT 管理员通过提供应用程序的集成实时监视来监视 Citrix ADC 所服务的所有 Web 应用程序。Web Insight 提供用户和服务器响应时间之类的关键信息，从而让 IT 组织能够监视并改进应用程序性能。

HDX Insight

为通过 Citrix ADC 的 ICA 流量提供端到端的可见性。HDX Insight 让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。

Gateway Insight

通过它可以查看用户在登录时遇到的失败，无论访问模式为何。可以查看某个给定时间登录的用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。

Security Insight

提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。

SSL Insight

SSL Insight 提供安全 Web 事务 (HTTPS) 的可见性，并允许 IT 管理员通过对安全 Web 事务提供集成、实时和历史监视，监视 Citrix ADC 提供的所有安全 Web 应用程序。

TCP Insight

TCP Insight 提供了一种简单且可扩展的解决方案，用于监视 ADC 实例中使用的优化技术和拥塞控制策略（或算法）的指标，以避免数据传输中的网络拥塞。

Video Insight

Video Insight 功能提供了一种简单且可扩展的解决方案，用于监视 Citrix ADC 实例使用的视频优化技术的指标，以改善客户体验和运营效率。

WAN Insight

通过 WAN Insight 分析，管理员可以轻松监视数据中心与分支 WAN 优化设备之间传输的加速和未加速 WAN 流量。通过 WAN Insight 还可以查看网络上的客户端、应用程序和分支，从而有助于有效地对网络问题进行故障排除。

调配

Cloud Orchestration（云调配）

支持将 Citrix ADC 产品与 OpenStack 云调配集成。Citrix ADM 和 OpenStack 相互实现对方的 API，从而实现了 Citrix ADC 实例的负载平衡功能 (LBaaS) 与 OpenStack 云调配的集成。

Orchestration

Citrix ADM 通过与不同供应商的 SDN 控制器集成，支持企业网络中的 SDN。ADM 同时支持 VMware NSX Manager 和 Cisco Application Policy Infrastructure Controller (APIC)。

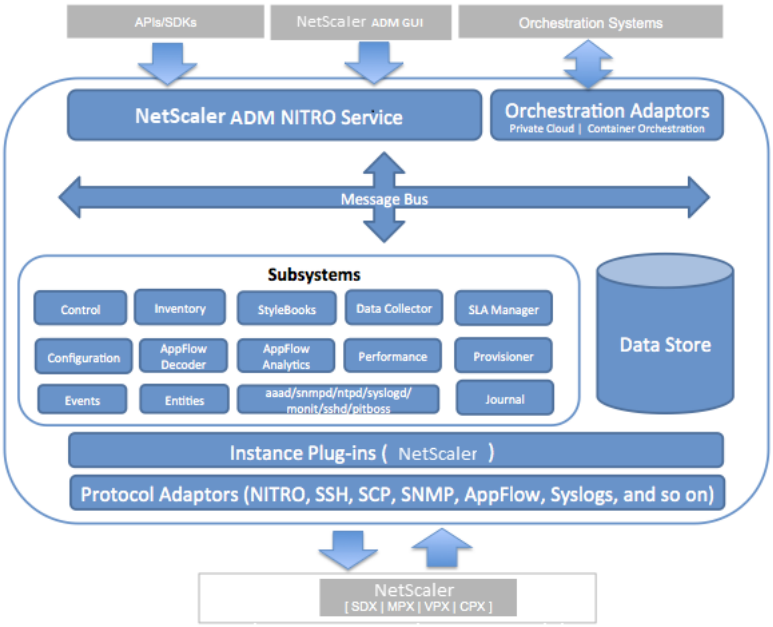
体系结构

February 6, 2024

Citrix Application Delivery Management (ADM) 数据库与服务器集成，服务器管理所有关键进程，如数据收集、NITRO 调用。服务器在其数据存储中存储实例详细信息清单，例如主机名、软件版本、运行和保存的配置、证书详细信息、实例上配置的实体。单服务器部署适用于处理较小通信量或将数据存储较短时间的情况。

当前，ADM 支持两种类型的软件部署：单服务器部署和高可用性。

下图显示了 ADM 中的不同子系统，以及 ADM 服务器和受管实例之间的通信方式。



ADM 中的服务子系统充当 Web 服务器，使用端口 80 和 443 处理从 GUI 或 API 发送到 ADM 中的子节目的 HTTP 请求和响应。这些请求通过使用 IPC（进程间通信）机制通过消息总线（消息处理系统）发送到子系统。请求会发送到控制子系统，该子系统处理信息或将其发送到合适的子系统。每个其他子系统（清单、样书、数据收集器、配置、AppFlow 解码器、AppFlow 分析、性能、事件、实体、SLA 管理器、设置程序和日志）均具有特定角色。

实例插件是共享库，它们对 ADM 支持的每种实例类型都是唯一的。信息通过 NITRO 调用，或者通过 SNMP、Secure Shell (SSH) 或安全复制 (SCP) 协议在 ADM 和托管实例之间传输。然后对这些信息进行处理并存储在内部数据库（数据存储）中。

Citrix ADM 如何发现实例

February 6, 2024

实例是您想要从 Citrix Application Delivery Management (ADM) 发现、管理和监视的 Citrix 设备或虚拟设备。要管理和监视这些实例，必须将它们添加到 Citrix ADM 服务器。您可以将以下 Citrix 设备和虚拟设备添加到 ADM：

- Citrx ADC 实例
  - Citrix MPX
  - Citrix VPX
  - Citrix SDX
  - Citrix CPX
- Citrix Gateway 实例

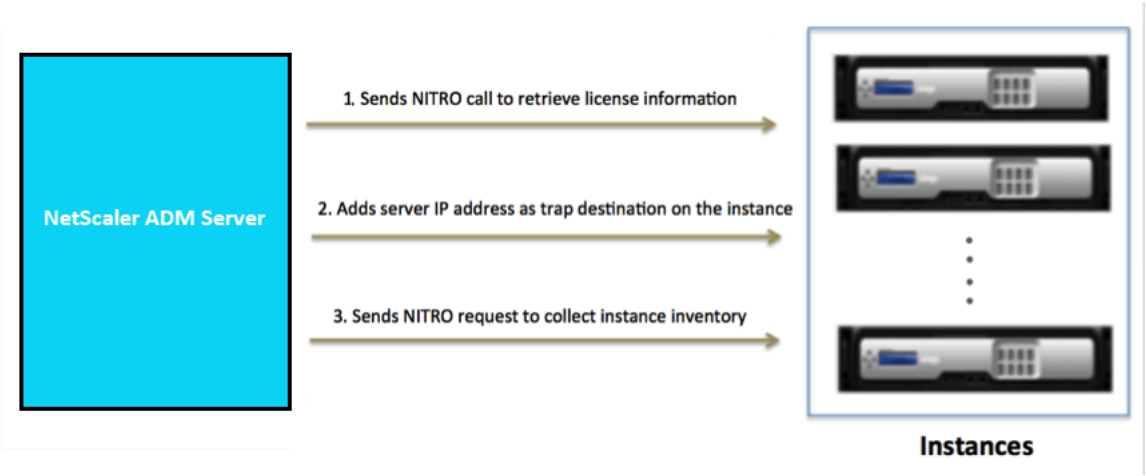
- Citrix SD-WAN 实例

可以在第一次设置 Citrix ADM 服务器时添加实例，也可在以后添加。

> 注意
>
> Citrix ADM 使用 Citrix ADC 实例的 NetScaler IP (NSIP) 地址进行通信。ADM 还可以发现具有启用管理访问权限的子网 IP (SNIP) 地址的 ADC 实例。有关必须在 ADC 实例和 ADM 之间打开的端口的信息，请参阅 端口。
>
> 对于 Citrix SD-WAN WO，ADM 使用实例的管理 IP 地址进行通信。
>
> 您无法在 ADM 中添加 Citrix SD-WAN SE /PE 实例。您可以在 Citrix SD-WAN SE/PE 设备上将 ADM 配置为 AppFlow 收集器。

将实例添加到 ADM 服务器时，服务器会隐式地将自身添加为实例的陷阱目标，并收集实例的清单。

下图描述了 ADM 如何隐式发现和添加实例。



如图所示，Citrx ADM 隐式执行以下步骤。

1. Citrix ADM 使用实例配置文件详细信息登录到实例。ADM 使用 ADC NITRO 调用检索实例的许可证信息。根据许可信息，它确定该实例是否为 ADC 实例以及 ADC 平台的类型（例如 Citrix ADC MPX、ADC VPX、ADC VPX、ADC SDX 或 Citrix Gateway）。成功检测实例后，该实例将添加到 ADM 的数据库中。

   对于 Citrix SD-WAN WO 实例，ADM 不会使用许可信息检测实例。它向实例发送一个 NITRO 请求以检查实例类型和版本。

   如果实例配置文件没有包含正确的凭据，此步骤可能会失败。对于 ADC MPX、ADC VPX、ADC SDX 和 Citrix Gateway 实例，如果未将许可应用于实例，则此步骤也可能会失败。

   > 注意
   >
   > 使用 HTTP，即使未在实例上配置许可证，您也可以将所有实例添加到 ADM。

2. ADM 将其的 IP 地址添加到实例上的陷阱目的地列表中。这允许 ADM 接收在 ADC 实例上生成的陷阱。

   如果实例上的陷阱目标数超过陷阱目标最大限制，此步骤可能会失败。实例的最大限制为 20。

对于 Citrix SD-WAN WO 实例，ADM 将其 IP 地址作为实例上的 SNMP 管理器添加。

3. ADM 通过发送 NITRO 请求从实例收集库存。它收集实例详细信息，例如，主机名、软件版本、正在运行和保存的配置、证书详细信息、实例上配置的实体等。

   如果存在网络或防火墙问题，此步骤可能会失败。

   要了解如何向 ADM 添加实例，请参阅 添加实例。

轮询概述

February 6, 2024

轮询是一个过程，在这个过程中，Citrix Application Delivery Management (ADM) 从 Citrix ADC 实例收集某些信息。您可能已在全球范围内为您的组织配置了多个 Citrix ADC 实例。要通过 Citrix ADM 监视您的实例，Citrix ADM 必须从所有托管 ADC 实例中收集某些信息，例如 CPU 使用率、内存使用率、SSL 证书、许可功能、许可类型等。以下是 ADM 和托管实例之间发生的不同类型的轮询：

- 实例轮询
- 清单轮询
- 性能数据收集
- 实例备份轮询
- 配置审核投票
- SSL 证书轮询
- 实体轮询

Citrix ADM 使用 NITRO 呼叫、安全外壳 (SSH) 和安全复制 (SCP) 等协议来轮询来自 Citrix ADC 实例的信息。

Citrix ADM 如何轮询托管实例和实体

默认情况下，Citrix ADM 会定期自动进行轮询。Citrix ADM 还允许您为几种轮询类型配置轮询间隔，并允许您在需要时手动进行轮询。

下表描述了轮询类型、轮询间隔、使用的协议等的详细信息：

轮询类型	轮询间隔	民意调查信息	使用的协议	轮询间隔配置
实例轮询	每 5 分钟（默认）	统计信息，例如状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量。	NITRO call。	否
清单轮询	每 30 分钟（默认情况下）	清单详细信息，如构建版本、系统信息、许可功能和模式。	NITRO 通话和 SSH	否
性能数据收集	每 5 分钟（默认）	网络报告信息	NITRO call	否
实例备份轮询	每 12 小时（默认情况下）	托管 ADC 实例当前状态的备份文件	NITRO 调用、SSH 和 SCP。	是。导航到 网络 > 实例 > **Citrix ADC**。选择实例，然后从 选择操 作”列表中单击“备 份/还原。
配置审核投票	每 10 小时（默认情况下）	ADC 实例上发生的配置更改（例如，正在运行的配置与保存的配置）	SSH、SCP 和 NITRO 通话	是。导航到“网络”>“配置审核”。在“配置审核”页上，单击设置并配置配置审核轮询的轮询间隔。您可以手动轮询配置审核，并将实例的所有配置审核立即添加到 Citrix ADM。为此，请导航到“网络”>“配置审核”，然后单击“立即轮询”。立即投票 页面允许您轮询网络中的所有实例或选定实例。
SSL 证书轮询	每 24 小时一次（默认）	安装在 Citrix ADC 实例上的 SSL 证书。	NITRO 电话和 SCP	是。导航到“网络”>“**SSL** 控制板”。在“SSL 控制面板”页上，单击设置以配置轮询间隔。

轮询类型	轮询间隔	民意调查信息	使用的协议	轮询间隔配置
				您可以手动轮询 SSL 证书，并将实例的所有证书立即添加到 Citrix ADM。为此，请导航到 网络 > **SSL** 控制板，然后单击立 即轮询。立即投票 页面允许您轮询网络中的所有实例或选定实例。
实体轮询	每 30 分钟（默认情况下）	在实例上配置的所有实体。实体是附加到 ADC 实例的策略、虚拟服务器、服务或操作。	NITRO 调用。	可以，但不能设置为少于 10 分钟。要进行配置，请导航至 网络 > 网络功能。在“网络功能”页上，单击设置以配置轮询间隔。 您可以手动轮询实体，并将实例的所有实体立即添加到 Citrix ADM。为此，请导航到“网络”> 网络功能”，然后单击“立即轮询。立即轮询 页面允许您轮询网络中的所有实例或选定的实例

> 注意：除
>
> 了轮询之外，Citrix ADM 还通过发送到实例的 SNMP 陷阱接收由托管 ADC 实例生成的事件。例如，系统发生故障或配置发生更改时生成事件。
>
> 在实例备份期间，SSL 文件、CA 证书文件、ADC 模板、数据库信息等将下载到 Citrix ADM。在配置审核过程中，ns.conf 文件会下载并存储在文件系统中。从托管 Citrix ADC 实例收集的所有信息都存储在数据库内部。

轮询实例的不同方式

以下是 Citrix ADM 在托管实例上执行的不同轮询方式：

- 对实例进行全局轮询
- 手动轮询实例
- 对实体进行人工投票

对实例进行全局轮询

Citrix ADM 会根据您配置的时间间隔自动轮询网络中的所有托管实例。尽管默认轮询间隔为 30 分钟，但您可以通过导航到“网络”>“网络功能”>“设置”，根据需要设置间隔。

手动轮询实例

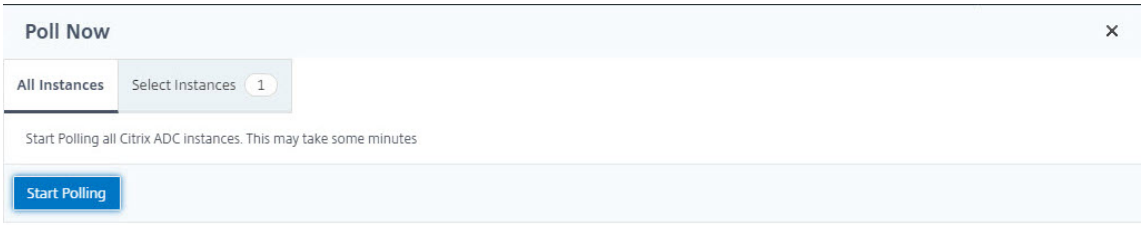
当 Citrix ADM 管理多个实体时，轮询周期需要更长的时间才能生成报告，这可能会导致屏幕空白或系统可能仍显示较早的数据。

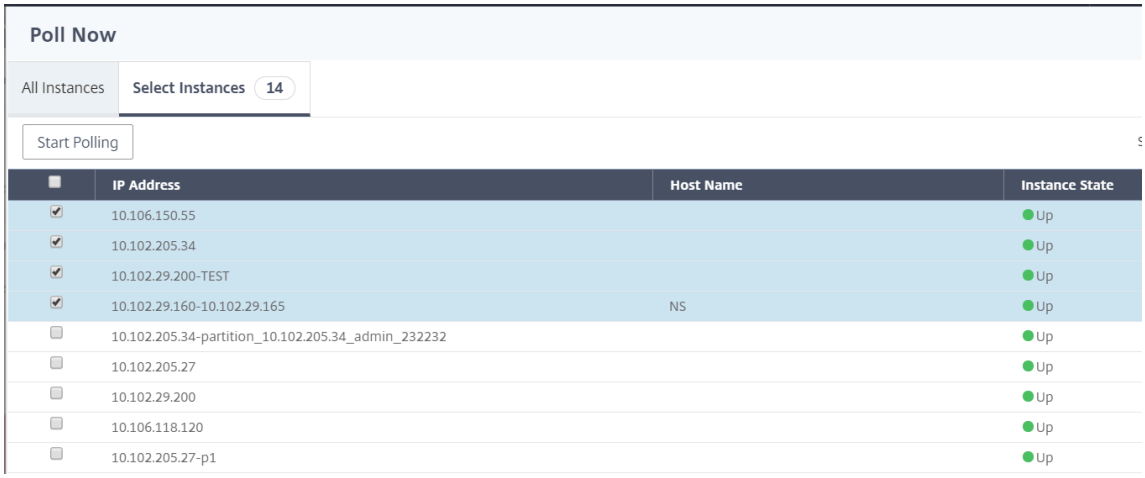
在 Citrix ADM 中，如果不进行自动轮询，则有一个最短的轮询间隔周期。如果您添加新的 Citrix ADC 实例，或者更新了实体，则在下一次轮询之前，Citrix ADM 无法识别新实例或对实体所做的更新。并且，没有办法立即获取虚拟 IP 地址列表来执行进一步操作。您必须等待最小轮询时间间隔过去。尽管您可以通过手动轮询来发现新添加的实例，但这会导致对整个 NetScaler 网络进行轮询，从而给网络带来沉重的负载。Citrix ADM 现在允许您在任何给定时间仅轮询选定的实例和实体，而不是轮询整个网络。

Citrix ADM 会自动轮询托管实例，以在一天中的设定时间收集信息。选定轮询减少了 Citrix ADM 显示绑定到这些选定实例的实体的最新状态所需的刷新时间。

轮询 **Citrix ADM** 中的特定实例：

1. 在 Citrix ADM 中，导航到“网络”>“网络功能”。
2. 在 网络功能 页上的右上角，单击 立即轮询。
3. 弹出页面“立即轮询”为您提供了轮询网络中所有 Citrix ADC 实例或轮询选定实例的选项。
   a) “所有实例”选项卡-单击“开始轮询”以轮询 所有实例。
   b) 选择实例 选项卡-从列表中选择实例
4. 单击 开始轮询。





Citrix ADM 启动手动轮询并添加所有实体。

对实体进行人工投票

Citrix ADM 还允许您仅轮询绑定到特定实例的几个选定实体。例如，您可以使用此选项来了解实例中特定实体的最新状态。在这种情况下，您无需轮询整个实例即可了解一个更新实体的状态。当您选择并轮询一个实体时，Citrix ADM 只会轮询该实体，并在 Citrix ADM GUI 中更新状态。

以虚拟服务器处于 关闭状态的示例为例。在下一次自动轮询之前，该虚拟服务器的状态可能已更改为 UP。要查看虚拟服务器的更改状态，可能需要只轮询该虚拟服务器，以便在 GUI 上立即显示正确的状态。

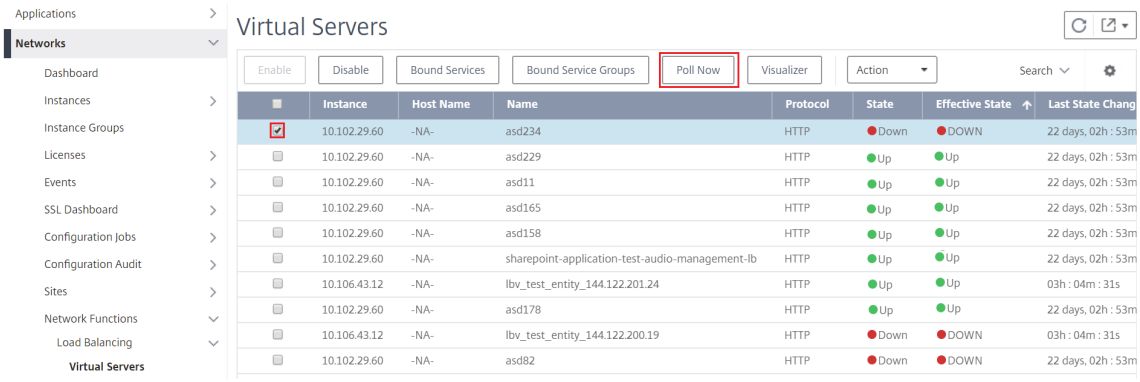
现在，您可以轮询以下实体以查看其状态的任何更新：服务、服务组、负载平衡虚拟服务器、缓存减少虚拟服务器、内容切换虚拟服务器、身份验证虚拟服务器、VPN 虚拟服务器、GSLB 虚拟服务器和应用程序服务器。

> 注意
>
> 如果您轮询虚拟服务器，则只轮询该虚拟服务器。服务、服务组和服务器等相关实体不进行轮询。如果您需要轮询所有关联实体，则必须手动轮询这些实体，或者必须轮询实例。

要轮询 **Citrix ADM** 中的特定实体，请执行以下操作：

例如，此任务可帮助您轮询负载平衡虚拟服务器。同样，您也可以轮询其他网络函数实体。

1. 在 Citrix ADM 中，导航到网络 > 网络功能 > 负载平衡 > 虚拟服务器。
2. 选择将状态显示为“关闭”的虚拟服务器，然后单击“立 即轮询”。虚拟服务器的状态现在更改为 UP。



数据治理

February 6, 2024

客户身份验证对组织至关重要，因为它使组织能够通过仅允许经过身份验证的客户或用户访问其网络来保护其网络资源。作为管理员，在允许用户连接到 Citrix 网络中的资源之前，请务必确定他们的身份。

从 12.1 版本 50.x 版本起，Citrix Application Delivery Management (ADM) 要求您在开始访问信息之前在 ADM GUI 上进行身份验证。要求您必须在 Citrix 云服务上注册自己，然后才能在 ADM 上进行身份验证。您必须在 ADM GUI 上提供 Citrix 云用户凭据。有关更多信息，请参阅 注册 Citrix Cloud。

有不同的方法可以在 Citrix ADM 上对自己进行身份验证。如果您是 ADM 上的新用户或现有用户，则以下各节将介绍工作流。

工作流程（如果您是新用户）

1. 在选定的虚拟机管理程序上完成 Citrix ADM 的安装。
2. 配置各种必需的 IP 地址。
3. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址。
4. 在“用户名”和“密码”字段中，输入管理员 凭据。
5. 将打开“配置客户身份”页面，您必须在其中使用 Citrix 云凭据表明自己的身份。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 进行注册。
6. 单击“身份验证”，然后提供您在 Citrix Cloud 上注册时使用的电子邮件地址。
7. 选中“我同意共享遥测数据”旁边的复选框，然后单击“提交”。

工作流程（如果您是现有用户）升级到 **12.1** 版本最新版本

1. 将 Citrix ADM 升级到 12.1 版本的最新版本后，在网络浏览器中键入 Citrix ADM 的 IP 地址。
2. 在“用户名”和“密码”字段中，输入管理员 凭据。
3. 将打开“配置客户身份”页面，您必须在其中使用 Citrix 云凭据表明自己的身份。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 进行注册。
4. 单击“身份验证”，然后提供您在 Citrix Cloud 上注册时使用的电子邮件地址。
5. 选中“我同意共享遥测数据”旁边的复选框，然后单击“提交”。

作为现有用户，您以后还可以通过以下两种方式之一在 ADM 上配置您的身份：

- 导航到“** 系统”>“系统 管理”，然后单击“身份验证”。
- 单击 ADM GUI 右上角的云端符号。成功进行身份验证后，“X”变为绿色复选标记。

> 注意：
>
> 确保以下域被列入白名单：
>
> - *.citrixnetworkapi.net
> - *.blob.core.windows.net

将您的数据上载到 Citrix ADM 并使用 Citrix ADM 的功能，即表示您同意并同意 Citrix 可以收集、存储、传输、维护、处理和使用有关您的 Citrix 产品和服务的技术、用户或相关信息。

Citrix 收到的信息将始终按照 Citrix.com 隐私政策进行处理。

许可

February 6, 2024

当通过 https 协议发现 Citrix ADC 实例时，Citrix Application Delivery Management (ADM) 需要经过验证的 Citrix ADC 许可证才能管理和监视 Citrix ADC 实例。

可以在没有许可证的情况下管理和监视任何数量的实例和实体。但是，在未应用许可证的情况下，只能在应用程序控制板上管理 30 个发现的应用程序以及只能查看 30 个虚拟服务器的分析信息。要管理 30 个以上发现的应用程序或要查看 30 个以上虚拟服务器的分析信息，必须购买并应用许可证。

	Citrix ADM 功能	[免费] 无论虚拟服务器数量多少，都不需要 Citrix ADM 许可证	超过 30 台虚拟服务器需要 Citrix ADM 许可证	Citrix ADC 许可证要求
分析	Web Insight	否	是	不适用
	HDX Insight*	否	是	Enterprise（报告 < 1 小时）Premium（报告 = 无限制）
	Security Insight	否	是	拥有应用程序防火墙许可证的高级版（或）企业版
	SSL Insight	否	是	不适用
	Gateway Insight	否	是	Enterprise（报告 < 1 小时）Premium（报告 = 无限制）
	TCP Insight	否	是	不适用
	Video Insight	否	是	Premium (Citrix-T 1000 系列、VPX-T)
	WAN Insight	否	不适用	Citrix SD-WAN 实例应为优化版 (WANOP)
应用程序				
	应用程序统计信息（应用程序控制板、应用程序安全性控制板）	否	是	应用程序控制面板和应用程序安全控制板上的 Citrix ADC Web App Firewall 相关信息需要具有应用程序防火墙许可证的高级版（或）企业版。
	样书	是	否	不适用
网络				
	许可证服务器	是	否	不适用
	库存管理—基础架构控制面板、实例组、实例控制面板和站点	是	否	不适用

	Citrix ADM 功能	[免费] 无论虚拟服务器数量多少，都不需要 Citrix ADM 许可证	超过 30 台虚拟服务器需要 Citrix ADM 许可证	Citrix ADC 许可证要求
	事件管理和 Syslog	是	否	不适用
	配置作业、配置审核和配置建议	是	否	不适用
	网络报告（实例级别）	是	否	不适用
	网络报告（虚拟服务器级别）	是	否	不适用
	网络管理（虚拟服务器、服务、服务组、服务器的可见性和管理）	是	否	不适用
	SSL 证书管理、监视和控制板（实例级别）	是	否	不适用
	SSL 证书控制板（虚拟服务器级别）	是	否	不适用
系统				
	RBAC 和外部身份验证（实例级别）	是	否	不适用
	RBAC 和外部身份验证	是	否	不适用
调配				
	OpenStack 集成	是	否	不适用
	VMware NSX 集成	是	否	不适用
	Cisco APIC 集成	是	否	不适用
	容器集成	是	否	不适用
第三方负载平衡器				
	HAProxy：跨主机/实例/后端/服务器/前端、下载或上载配置以及重启设备的可见性。	是	否	不适用
	应用程序控制板	否	是（需要单独的许可证）	不适用

* 要让 Citrix Director 与 Citrix ADM 集成，Citrix Director 应拥有高级许可证。

更多虚拟服务器的许可证在 10 个虚拟服务器包中提供。可以通过 Citrix ADM GUI 获取有效许可证，并在 Citrix ADM 服务器上添加许可证。

高可用性

Citrix ADM 服务器可以包含 VIP、CICO 和池容量许可证。向 ADM 服务器颁发许可证时，许可证将绑定到服务器的主机 ID。而且，将许可证分配给其他 ADM 服务器受到限制。

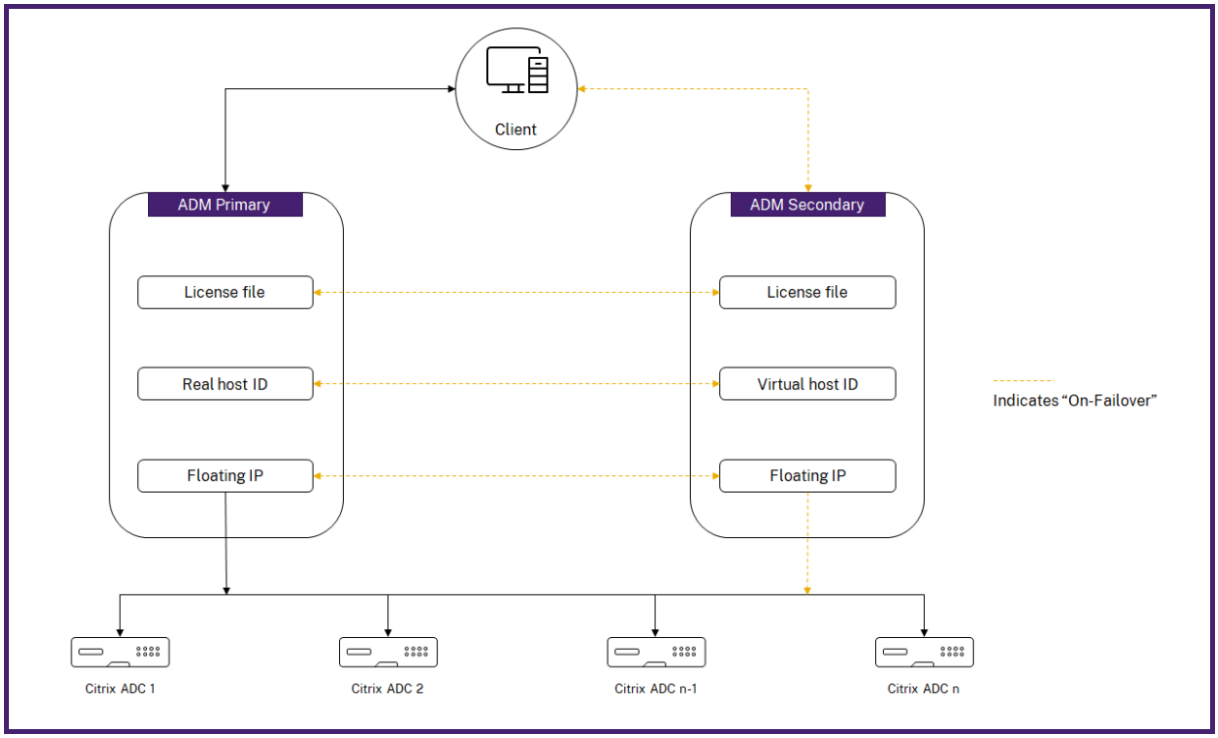
如果将 ADM 高可用性对配置为许可证服务器，则主服务器和辅助服务器必须具有相同的许可证文件。因此，在 ADM 高可用性部署中，Citrix ADM 支持将相同的许可证文件分配给两台服务器。

> 注意
>
> - 如果您已安装 Citrix ADM 12.1.49.x 或更早版本，则可以获得 30 天的宽限期来维护辅助节点上的许可。宽限期过后，必须联系 Citrix 以重新托管原始许可证。
> - 对于 12.1.50.x 或更高版本，Citrix ADM 许可证会自动同步到辅助节点。
> - 池许可证从 12.1.50.x 或更高版本自动同步到辅助节点。

ADM 高可用性节点之间的许可证如何同步

无论何时发生故障切换，从属服务器都会承担主服务器的角色。主服务器的真实主机 ID 配置为新主服务器的虚拟主机 ID。许可证文件使用虚拟主机 ID 识别新的主服务器。

- **Real Host ID**（真实主机 ID）- 此 ID 由 ADM 服务器的 MAC 地址生成。每个 ADM 独立部署都有一个唯一的主机 ID。
- 虚拟主机 **ID** -此 ID 是在 HA 部署期间自动生成的。ADM 主服务器的真实主机 ID 用作从属服务器的虚拟主机 ID。此 ID 以加密格式存储在 ADM 数据库中，对此 ID 的修改受到限制。虚拟主机 ID 优先于真实的主机 ID。



假设 Node-1 是主服务器，Node-2 是辅助服务器。Node-1 的虚拟主机 ID 与 Node-2 同步。

1. Node-1 中可用的许可证文件将同步到 Node-2。
2. Node-1 上的任何新许可证文件都会定期同步到 Node-2。
3. ADM 确保许可证服务器仅在 Node-1 上运行，以避免许可证容量增加一倍。
4. Citrix ADC 实例使用浮动 IP 地址从 Node-1 中签出许可证。

许可证被锁定到 ADC 实例。要从 Citrix ADM HA 中签出许可证，实例需要特定设备的 IP 地址。当您在主服务器上应用许可证时，该服务器将负责许可，并将所有未来的许可证应用于该实例。只能从安装了许可证的服务器中删除许可证。

调配

调配模块独立于许可，且始终可用。

升级虚拟服务器许可证

可以在 Citrix ADM 中升级许可以监视和管理 Citrix ADC 设备上托管的多个虚拟服务器。

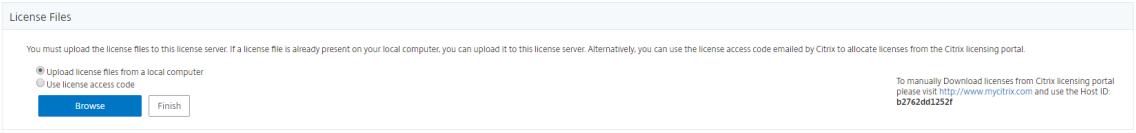
要升级您的设备许可证，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到“网络”>“许可证”**>**“设置”。

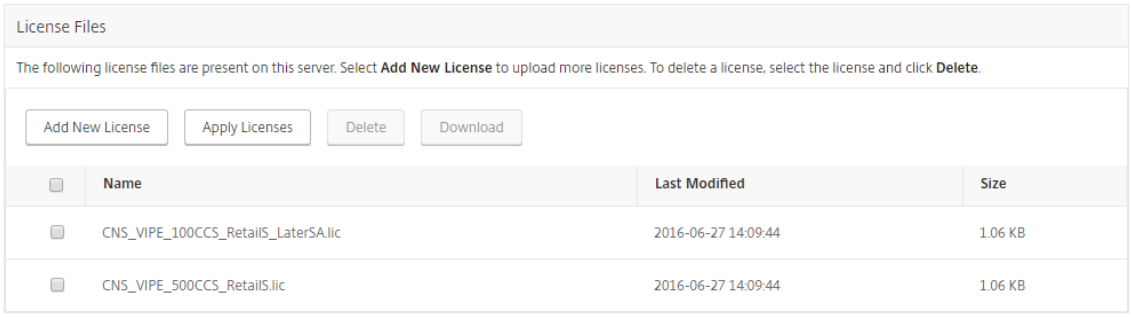
3. 在详细信息窗格中，转到许可证文件，然后选择以下选项之一：

   - 从本地计算机上载许可证文件。如果您的本地计算机上已存在许可证，请单击“浏览”，然后选择要用于分配许可证的许可证文件 (.lic)。单击 **Finish**（完成）。
   - 使用许可证激活码。Citrix 通过电子邮件发送您购买的许可证的许可证访问代码。在文本框中输入许可证访问代码，然后单击 **Get Licenses**（获取许可证）。

   > 注意
   >
   > 如果选择此选项，则 Citrix ADM 必须连接到 Internet，否则必须有代理服务器可用。

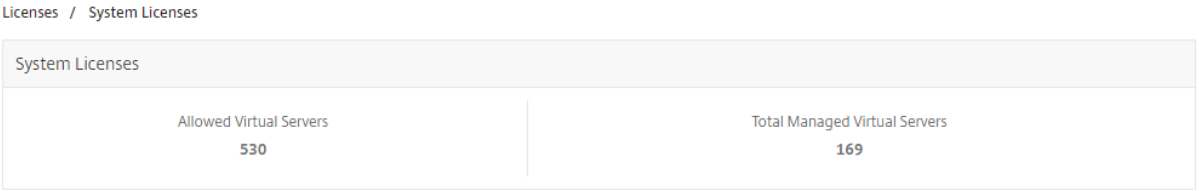


4. 您可以随时从“许可证设置”页面添加更多许可证。



验证

您可以通过导航到网络 > 许可证 > 系统许可证来验证安装在 Citrix ADM 上的许可证。



为虚拟服务器授予许可

您可以通过 Citrix ADM 选择要管理和监视的虚拟服务器。如果发现的 Citrix ADC 实例托管的虚拟服务器总数低于已安装的虚拟服务器许可证数量，则 Citrix ADM 会为所有虚拟服务器提供许可证。

您可以通过 Citrix ADM 选择要管理和监视的虚拟服务器。

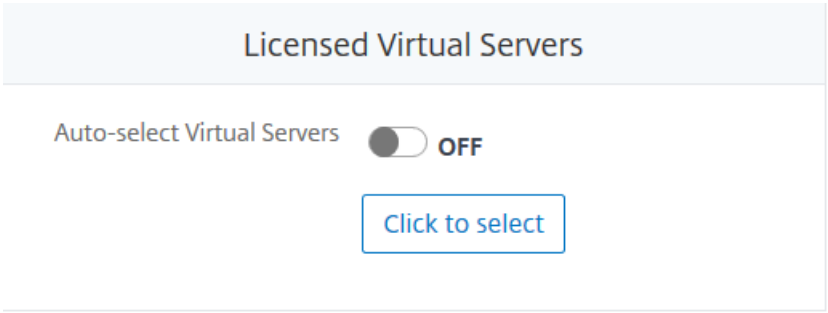
注意事项：

- 默认情况下，Citrix ADM 会在每个虚拟服务器轮询周期后自动对虚拟服务器进行随机许可。
- 如果在 Citrix ADM 中发现的虚拟服务器总数少于安装的虚拟服务器许可证数，默认情况下，Citrix ADM 将许可使用所有虚拟服务器。
- 要手动选择虚拟服务器，或要仅对有限的虚拟服务器进行许可，您必须先禁用自动许可虚拟服务器，然后选择您要管理的虚拟服务器。
- Citrix ADM 不许可不可寻址的虚拟服务器。要管理它们，必须手动对其进行许可。

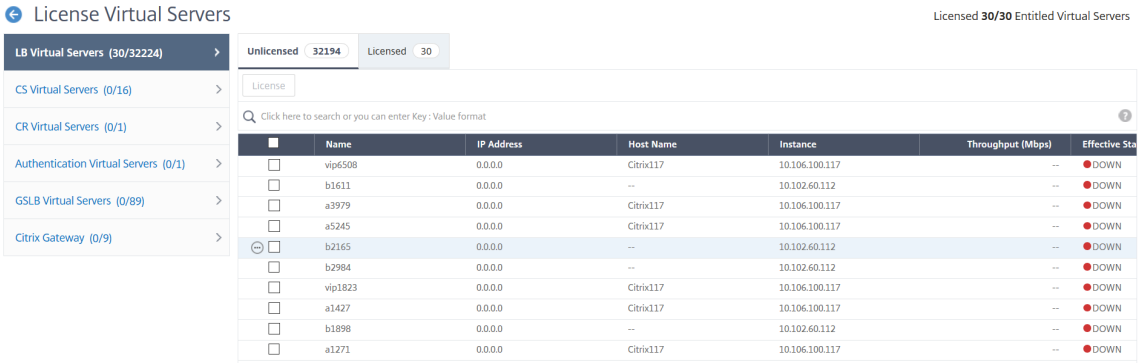
要管理许可的虚拟服务器，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到 网络 **>** 许可证 **>** 系统许可证。

   将显示“系统许可证”控制板。
3. 在“许可的虚拟服务器”下，禁用“自动选择虚拟服务器”，然后 单击“点击选择”选项。



4. 在“许可证虚拟服务器”屏幕中，通过单击相关选项卡选择虚拟服务器的类型。



5. 在“未许可”选项卡中，选择要许可的虚拟服务器，然后单击“许 可”。从“已许可”选项卡中，选择要取消许可的虚拟服务器，然后单击“取消许可”。
6. 单击“下一步”移至其他虚拟服务器的选项卡，或单击“保存并退出”以许可所选虚拟服务器。

为不可寻址的虚拟服务器配置自动许可支持

默认情况下，Citrix ADM 不会自动将许可证应用于不可寻址的虚拟服务器。对于不可寻址的虚拟服务器的许可，必须禁用自动许可选项，然后手动选择不可寻址的虚拟服务器。这会增加您在应用许可证时最初手动选择不可寻址服务器的工作量。您还需要在将新的不可寻址虚拟服务器添加到网络时手动选择这些服务器。

Citrix ADM 在“网络”>“许可证”>“系统许可证”下提供了一个新选项。也就是说，新选项 自动选择不可寻址的虚拟服务器。启用此选项现在允许您明确指定许可还必须包括不可寻址的虚拟服务器。

> 注意
>
> - 默认情况下，Citrix ADM 仍不会自动选择不可寻址的虚拟服务器进行许可。
> - 应用程序分析（应用程序控制板）是当前在许可的非寻址虚拟服务器上支持的唯一分析。

虚拟服务器许可证的到期检查

现在，您可以在 Citrix ADM 中查看虚拟服务器许可证到期的状态并设置警报。

查看许可证的状态：

1. 导航到 网络 > 许可证 > 系统许可证。
2. 在 **License Expiry Information**（许可证过期信息）部分中，可以看到要过期的许可证的详细信息：
    - **Feature**（功能）：要过期的许可证类型。
    - **Count**（计数）：受影响的虚拟服务器或实例的数量。
    - **Days to expiry**（过期天数）：距离过期的天数。

要配置许可证的通知设置，请执行以下操作：

1. 导航到“网络”>“许可证”**>**“设置”。
2. 在 **Notification Settings**（通知设置）部分中，单击铅笔图标并编辑参数。
    - 电子邮件配置文件：当许可证达到阈值或将要过期时发送通知的电子邮件配置文件或通讯组列表。
    - **SMS** 配置文件： SMS 配置文件或分发列表，用于在许可证达到阈值或即将到期时发送通知。
    - **Alert Threshold**（警报阈值）：设置汇集的许可证的百分比，以通过电子邮件或 SMS 通知管理员。
    - **License Expiry Threshold**（许可证过期阈值）：距离由“Alert Threshold”（警报阈值）确定的许可证数过期的天数。
    - **Days to expiry**（过期天数）：距离过期的天数。

系统要求

February 6, 2024

在安装 Citrix Application Delivery Management (ADM) 之前，必须了解软件要求、浏览器要求、端口信息、许可证信息和限制。

Citrix ADM 的要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU 注意：Citrix 建议在 Citrix ADM 部署中使用固态硬盘 (SSD) 技术。
存储空间	默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。使用《Citrix ADM HA 部署指南》中“最大限制”部分（第 7 页）中提及的大小计算器。本指南可在我们的下载站点**NetScaler MAS** 版本 **12.1 >** 早期版本下找到。 注意：您需要 Citrix 帐户才能访问部署指南和大小计算器。 如果您的 Citrix ADM 存储需求超过 120 GB，则必须附加一个额外的磁盘。您只能再添加一个磁盘。 Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。 有关更多信息，请参阅 如何将其他磁盘附加到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

> 注意
>
> AMD 芯片组不支持 Citrix ADM。

Citrix ADM 内部部署代理的要求

组件	要求
RAM	8 GB 注意：默认值为 8 GB。Citrix 建议您将默认值增加到 32 GB 以获得更好的性能。
虚拟 CPU	2 个 CPU 注意：默认值为 2 个 CPU。Citrix 建议您将默认值增加到 8 个 CPU 以获得更好的性能。
存储空间	30 GB
虚拟网络接口	1
吞吐量	1 Gbps

> 注意
>
> AMD 芯片组不支持 Citrix ADM 代理。

Citrix ADM 功能所需的最低 Citrix ADC 版本

> 重要
>
> Citrix ADM 版本和内部版本应 等于或高 于您的 Citrix ADC 版本和内部版本。例如，如果您已安装 Citrix ADM 12.1 Build 50.39，请确保已安装 Citrix ADC 12.1 Build 50.28/50.31 或更早版本。

Citrix ADM 功能	Citrix ADC 软件版本
样书	10.5 及更高版本
OpenStack/CloudStack 支持	11.0 及更高版本（如果需要分区） 11.1 及更高版本，如果需要在共享虚拟 LAN 上分区
NSX 支持	11.1 Build 47.14 及更高版本 (VPX)
Mesos/Marathon 支持	10.5 及更高版本
备份/还原	对于 Citrix ADC，10.1 及更高版本 对于 Citrix SDX，11.0 及更高版本
监视/报告和使用作业进行配置	10.1 及更高版本
分析功能	
Web Insight	10.5 及更高版本

Citrix ADM 功能	Citrix ADC 软件版本
HDX Insight	10.1 及更高版本
Security Insight	11.0.65.31 及更高版本
Gateway Insight	11.0.65.31 及更高版本
Cache Insight	10.5 及更高版本 *
SSL Insight	12.0 及更高版本

* 运行版本 11.0 版本 Build 66.x 的 Citrix ADC 实例的 Citrix ADM 不支持集成缓存指标。

Citrix SD-WAN 实例管理的要求

Citrix SD-WAN 平台版本/版本和 **Citrix ADM** 功能的互操作性矩阵

平台版本	**Citrix SD-WAN WANOP**	**Citrix SD-WAN SE**	**Citrix SD-WAN PE**
发现	是	是	是
配置	是	否	否
监视	是	否	否
报告（网络报告）	是	否	否
事件管理	是	否	否
HDX Insight	是	否	否
WAN Insight	是	否	否
HDX Insight（多跃点部署）	是	是	否

Citrix SD-WAN 实例支持的瘦客户端

Citrix ADM 支持以下瘦客户端来监视 Citrix SD-WAN 部署：

- Dell Wyse WTOS 型号 R10L Rx0L 瘦客户端
- NComputing N400
- Dell Wyse WTOS 型号 CX0 C00X Xenith

- Dell Wyse WTOS 型号 TXO T00X Xenith2
- Dell Wyse WTOS 型号 CX0 C10LE
- Dell Wyse WTOS 型号 R00LX Rx0L HDX 瘦客户端
- Dell Wyse Enhanced SUSE Linux Enterprise，型号 Dx0D、D50D
- Dell Wyse ZX0 Z90D7 (WES7) 瘦客户端

Citrix ADM 分析的要求

Citrix ADM 功能所需的最低 **Citrix Virtual Apps and Desktops** 版本

Citrix ADM 功能	Citrix Virtual Apps and Desktops 版本
HDX Insight	Citrix Virtual Apps and Desktops 7.0 及更高版本

> 注意
>
> Citrix Gateway 功能（在版本 9.3 和 10.x 中标记为接入网关企业版）必须在 Citrix ADC 实例上可用。Citrix ADM 不支持独立 Access Gateway Standard 设备。

Citrix ADM 可以为在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上发布并通过 Citrix Receiver 访问的应用程序生成报告。但是，此功能取决于安装了 Receiver 的操作系统。目前，Citrix ADC 不会解析通过在 iOS 或 Android 操作系统上运行的 Citrix Receiver 访问的应用程序或桌面的 ICA 流量。

支持 **HDX Insight** 的瘦客户端

- 基于 Dell Wyse Windows 的瘦客户端
- 基于 Dell Wyse Linux 的瘦客户端
- Dell Wyse ThinOS 的瘦客户端
- 基于 10ZiG Ubuntu 的瘦客户端
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

HDX Insight 需要 **Citrix ADC** 实例许可证

Citrix ADM 针对 HDX Insight 收集的数据取决于所监视的 Citrix ADC 实例的版本和许可证。HDX Insight 报告仅针对运行 10.5 及更高版本的 Citrix ADC 白金和企业设备显示。

Citrix ADC 许可证/持续时间	5 分钟	1 小时	1 天	1 周	1 个月
Standard	否	否	否	否	否
Enterprise	是	是	否	否	否
Platinum	是	是	是	是	是

受支持的虚拟机管理程序

下表列出了 Citrix ADM 支持的虚拟机管理程序。

虚拟机管理程序	版本
Citrix Hypervisor	7.1 和 7.4
VMware ESX	6.0、6.5 和 6.7
Microsoft Hyper-V	2012 R2 和 2016
通用 KVM	RHEL 7.4 和 Ubuntu 16.04

支持的操作系统和 **Receiver** 版本

下表列出了 Citrix ADM 支持的操作系统以及每个系统当前支持的 Citrix Receiver 版本：

操作系统	Receiver 版本
Windows	4.0 标准版
Linux	13.0.265571 及更高版本
Mac	11.8 (Build 238301) 及更高版本
HTML5	1.5*
Chrome 应用程序	1.5*

* 适用于 Citrix CloudBridge（Citrix SD-WAN WANOP）7.4 及更高版本。

支持的浏览器

下表列出了 Citrix ADM 支持的 Web 浏览器：

Web 浏览器	版本
Internet Explorer	11.0 及更高版本
Google Chrome	Chrome 19 及更高版本
Safari	Safari 5.1.1 及更高版本
Mozilla Firefox	Firefox 3.6.25 及更高版本

支持的端口

Citrix ADM 使用 Citrix ADC IP（称为 NSIP）地址与 Citrix ADC 进行通信。对于 Citrix ADC 实例与 Citrix ADM 或 Citrix SD-WAN 实例和 Citrix ADM 之间的通信，必须在 Citrix ADM 中打开以下端口：

> 注意
>
> 如果您已在高可用性模式下配置 Citrix ADC，Citrix ADM 将使用 Citrix ADC 子网 IP（管理 SNIP）地址与 Citrix ADC 进行通信。对于使用 SNIP 与 Citrix ADM 进行通信，以下端口保持不变。

类型	端口	详细信息	通信方向
TCP	80/443	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 NITRO 通信。443。用于高可用性模式下 Citrix ADM 服务器之间的 NITRO 通信。	Citrix ADM 到 Citrix ADC 和 Citrix ADM
TCP	22	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 SSH 通信。用于以高可用性模式部署的 Citrix ADM 服务器之间的同步。而且，ADM 代理与 Citrix ADC 之间的 SSH 通信需要此端口。	Citrix ADM 至 Citrix ADC，将 Citrix ADM 代理转至 Citrix ADC
UDP	4739	用于从 Citrix ADC 或 Citrix SD-WAN 实例到 Citrix ADM 的 AppFlow 通信。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM
ICMP	无保留的端口	检测在高可用性模式下部署的 Citrix ADM 和 Citrix ADC 实例、SD WAN 实例或辅助 Citrix ADM 服务器之间的网络可访问性。	
UDP	161, 162	接收从 Citrix ADC 实例到 Citrix ADM 的 SNMP 事件。	** 端口 161** -Citrix ADM 到 Citrix ADC
			** 端口 162** - Citrix ADC 到 Citrix ADM
UDP	514	将系统日志消息从 Citrix ADC 或 Citrix SD-WAN 实例接收到 Citrix ADM。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM
TCP	25	将 SMTP 通知从 Citrix ADM 发送给用户。	
TCP	389/636	用于身份验证协议的默认端口。用于 Citrix ADM 和 LDAP 外部身份验证服务器之间的通信。	Citrix ADM 到 LDAP 外部身份验证服务器

UDP	123	用于与多个时间源同步的默认 NTP 服务器端口。
RADIUS	1812	用于身份验证协议的默认端口。用于 Citrix ADM 和 RADIUS 外部身份验证服务器之间的通信。|Citrix ADM 到 RADIUS 外部身份验证服务器
TACACS	49	用于身份验证协议的默认端口。用于 Citrix ADM 和 TACACS 外部身份验证服务器之间的通信。|Citrix ADM 到 TACACS 外部身份验证服务器
TCP	5563	接收来自 Citrix ADC 实例的 ADC 度量（计数器）、系统事件和审核日志消息到 Citrix ADM。|Citrix ADC 到 Citrix ADM
TCP	5557/5558	用 ** 于 ** 从 Citrix ADC 到 Citrix ADM 的 Logstream 通信（适用于 Security Insight、Web Insight 和 HDX Insight）。|Citrix ADC 到 Citrix ADM
TCP	5454	在高可用性模式下，Citrix ADM 节点之间用于通信和数据库同步的默认端口。|Citrix ADM 主节点到 Citrix ADM 辅助节点
TCP	27000	用于 Citrix ADM 许可证服务器和 CPX 实例之间通信的许可证端口。|Citrix ADC 到 Citrix ADM
TCP	7279	Citrix 供应商守护程序端口。|Citrix ADC 到 Citrix ADM
TCP| 443/8443/7443| Citrix ADM 代理与 Citrix ADM 之间通信的端口。ADM 代理启动与 Citrix ADM 的通信。| Citrix ADM 代理与 Citrix ADM 的通信	

限制

在 12.1 Citrix ADM 中，以下功能支持 IPv6 格式的 IP 地址：

1. 针对 Citrix ADM GUI 的管理访问权限
2. Citrix ADC 的管理访问权限
3. 注册和库存
4. “网络”控制板
5. “SSL”控制板
6. 配置作业
7. 配置审核
8. 网络功能
9. 网络报告
10. ADC 实例的备份和恢复
11. 来自 Citrix ADC 的 SNMP 事件

以下功能不支持 IPv6：

1. 高可用性浮动 IP
2. 从支持 IPv6 的 ADC 接收的系统日志
3. ADC 上支持 IPv6 的样书

4. 分析
5. 池许可

部署

February 6, 2024

要管理和监视应用程序和网络基础架构，必须首先在其中一个虚拟机管理程序上安装 Citrix ADM。您可以将 Citrix ADM 部署为单个服务器或高可用性模式。如果您使用的是 NetScaler Insight Center Insight Center，则可以迁移到 Citrix ADM，除了分析功能外，还可以使用管理、监视、编排和应用程序管理功能。

- 单服务器部署。在 Citrix ADM 单服务器部署中，数据库与服务器集成，并且单个服务器处理所有流量。您可以使用 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 Citrix ADM。请参阅：
  - Citrix Hypervisor 上的 Citrix ADM
  - 搭载 Microsoft Hyper-V 的 Citrix ADM
  - 搭载 VMware ESXi 的 Citrix ADM
  - 搭载 Linux KVM 服务器的 Citrix ADM
- 高可用性 **(HA)** 部署。部署两台 Citrix Citrix ADM 服务器的 HA 可实现不间断的操作。在高可用性设置中，两个 Citrix ADM 节点必须以主动-被动模式部署在同一子网上使用相同的软件版本和版本，并且必须具有相同的配置。通过高可用性部署，能够在 Citrix ADM 主节点上配置浮动 IP 地址就无需单独的 NetScaler 负载平衡器。请参阅：在高可用性部署中配置。
- 从 **NetScaler Insight Center** 迁移到 **Citrix ADM**。您可以在不丢失现有配置、设置或数据的情况下将 NetScaler Insight Center 部署迁移到 Citrix ADM。使用 Citrix ADM，您不仅可以查看 NetScaler 和 NetScaler SD-WAN 实例生成的各种分析，还可以通过单个统一的控制台对整个全球应用交付基础设施进行管理、监视和故障排除。请参阅：从 NetScaler Insight Center 迁移到 Citrix ADM
- 将 **Citrix ADM** 与 **Director** 集成。Director 与 Citrix ADM 集成以进行网络分析和性能管理。请参阅：将 Citrix ADM 与 Director 集成

安装 **Citrix ADM** 的必备条件

February 6, 2024

您可以下载适用于 Microsoft HyperV、VMware ESXi、Linux KVM 和 Citrix Hypervisor 平台的 Citrix ADM 作为虚拟设备进行安装。在安装

Citrix ADM 之前，必须了解所有这些平台上的软件要求、浏览器要求、端口信息、许可证信息和限制。

有关安装 Citrix ADM 的特定平台要求和详细步骤，请参阅以下主题：

- Citrix Hypervisor 上的 Citrix ADM
- 采用 Microsoft HyperV 的 Citrix ADM
- 搭载 VMware ESXi 的 Citrix ADM
- 搭载 Linux KVM 服务器的 Citrix ADM

Citrix ADM 版本 12.1 的一般要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。 所需的默认存储空间为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。使用《Citrix ADM HA 部署指南》中“最大限制”部分（第 7 页）中提及的大小计算器。本指南可在我们的 下载站点**NetScaler MAS** 版本 **12.1 >** 早期版本下找到。注意：您需要 Citrix 帐户才能访问部署指南和大小计算器 如果您的 Citrix ADM 存储需求超过 120 GB，则必须附加一个额外的磁盘。 Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。您只能再添加一个磁盘。 有关更多信息，请参阅 如何将其他磁盘附加到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps

> 注意：
>
> Citrix 建议您在本地存储上托管 Citrix ADM VHD。当托管在 SAN 中的存储设备上时，Citrix ADM 可能无法按预期工作。

Citrix Hypervisor 上的 Citrix ADM

February 6, 2024

要在 Citrix Hypervisor（以前称为 XenServer）上安装 Citrix ADM，您需要首先将 Citrix ADM .xva 映像文件下载到本地计算机。您需要使用 Citrix XenCenter 来执行 Citrix ADM 的安装。

> 注意：
>
> Citrix ADM 不支持 XenMotion。

必备条件

在安装 Citrix ADM 之前，请验证是否已满足以下要求：

- Citrix Hypervisor 7.1 或更高版本安装在符合最低要求的硬件上。
- 在满足最低要求的管理工作站上安装 XenCenter。您必须使用 XenCenter 才能在 Citrix Hypervisor 上安装 Citrix ADM。
- 您已经下载了 Citrix ADM .XVA 映像文件。

XenCenter 系统要求

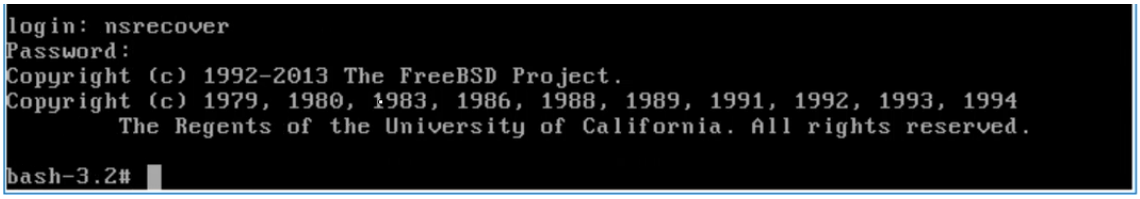
XenCenter 是一款 Windows 客户端应用程序。它不能与 Citrix Hypervisor 主机在同一台计算机上运行。下表说明了最低系统要求。

组件	要求
操作系统	Windows 7、Windows Server 2003 或 Windows 10
.NET Framework	2.0 版或更高版本
CPU	750 兆赫兹 (MHz)，建议：1 千兆赫兹 (GHz) 或更快
RAM	1 GB，建议：2 GB
网络接口卡	100 Mbps 或速度更高的 NIC

安装 Citrix Application Delivery Management

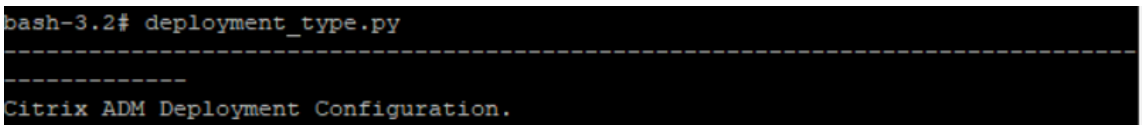
1. 将 XVA 映像文件导入 Citrix Hypervisor，然后从 控制台选项卡配置初始 网络配置选项。

2. 指定所需的 IP 地址后，保存配置设置。
3. 出现提示时，使用 ns 恢复/nsroot 凭据登录。



> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置并保存配置。

4. 通过在 shell 提示符处键入命令来执行部署脚本：`/mps/deployment_type.py`



5. 选择部署类型为 **Citrix ADM** 服务器。如果不选择任何选项，默认情况下，它部署为服务器。

6. 键入是将 Citrix ADM 部署为独立部署。
7. 键入是以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，您可以稍后更新初始配置设置。

验证

安装服务器后，您可以通过在网络浏览器中键入 Citrix ADM 服务器的 IP 地址来访问图形用户界面 (GUI)。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

搭载 **Microsoft Hyper-V** 的 **Citrix ADM**

February 6, 2024

若要在 Microsoft Hyper-V 上安装 Citrix ADM，您必须首先将 Citrix ADM 映像文件下载到本地计算机。此外，请确保您的系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。

必备条件

在安装 Citrix ADM 虚拟设备之前，请验证是否满足以下要求：

- 在满足最低要求的硬件上安装 Microsoft Hyper-V 6.2 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 Microsoft Hyper-V 管理器。
- 您已下载 Citrix ADM 映像文件。

Microsoft Hyper-V 系统要求

Microsoft Hyper-V 是 Windows 客户端应用程序。下表说明了最低系统要求。

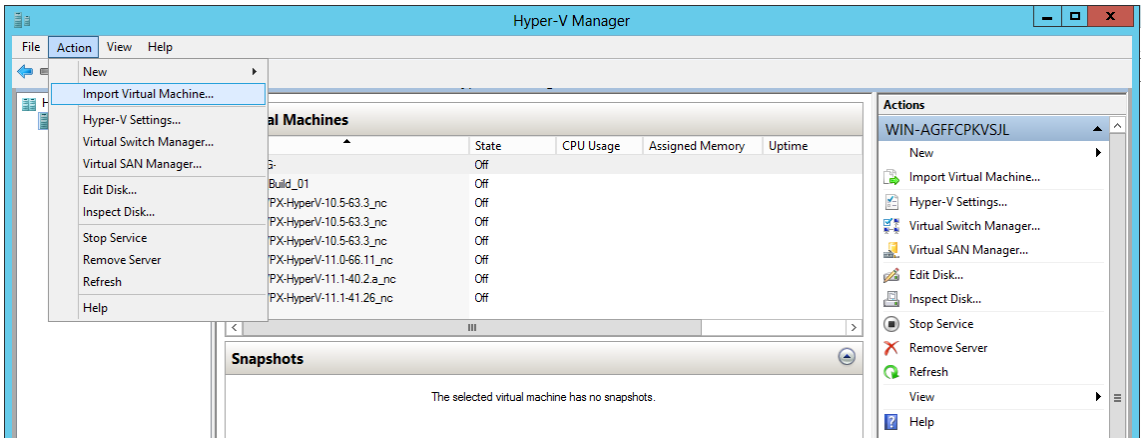
组件	要求
操作系统	Windows Server 2012 R2
.NET Framework	2.0 版或更高版本
CPU	750 兆赫兹 (MHz)，建议：1 千兆赫兹 (GHz) 或更快
RAM	1 GB，建议：2 GB
网络接口卡	100 Mbps 或速度更高的 NIC

安装 **Citrix Application Delivery Management**

您可以安装的 Citrix ADM 服务器的数量取决于 Hyper-V 服务器上的可用内存。

要安装 **Citrix ADM**，请执行以下操作：

1. 在工作站上启动 Hyper-V 管理器客户端。
2. 在 **Action**（操作）菜单上，单击 **Import Virtual Machine**（导入虚拟机）。



3. 导入 Hyper-V 映像，然后执行以下操作：

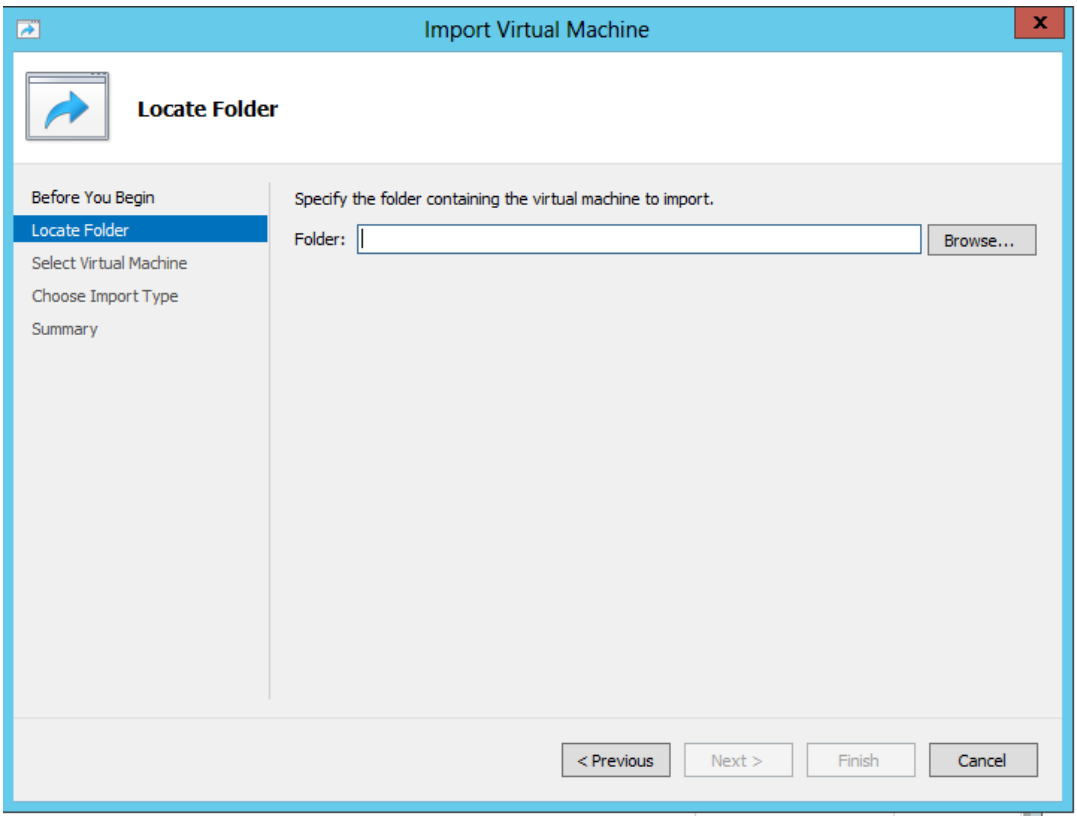
   a) 在“导入虚拟机”对话框的“查找文件夹”部分，浏览到保存 Citrix ADM Hyper-V 映像的文件夹，选择该文件夹，然后单击“下一步”。

   b) 在“Select Virtual Machine”（选择虚拟机）部分，选择适当的虚拟机名称。

   c) 在 **Choose Import Type**（选择导入类型）部分，选择“Copy the virtual machine (create a new unique ID)”（复制虚拟机 (创建新的唯一 ID)）选项，并单击“Next”（下一步）。

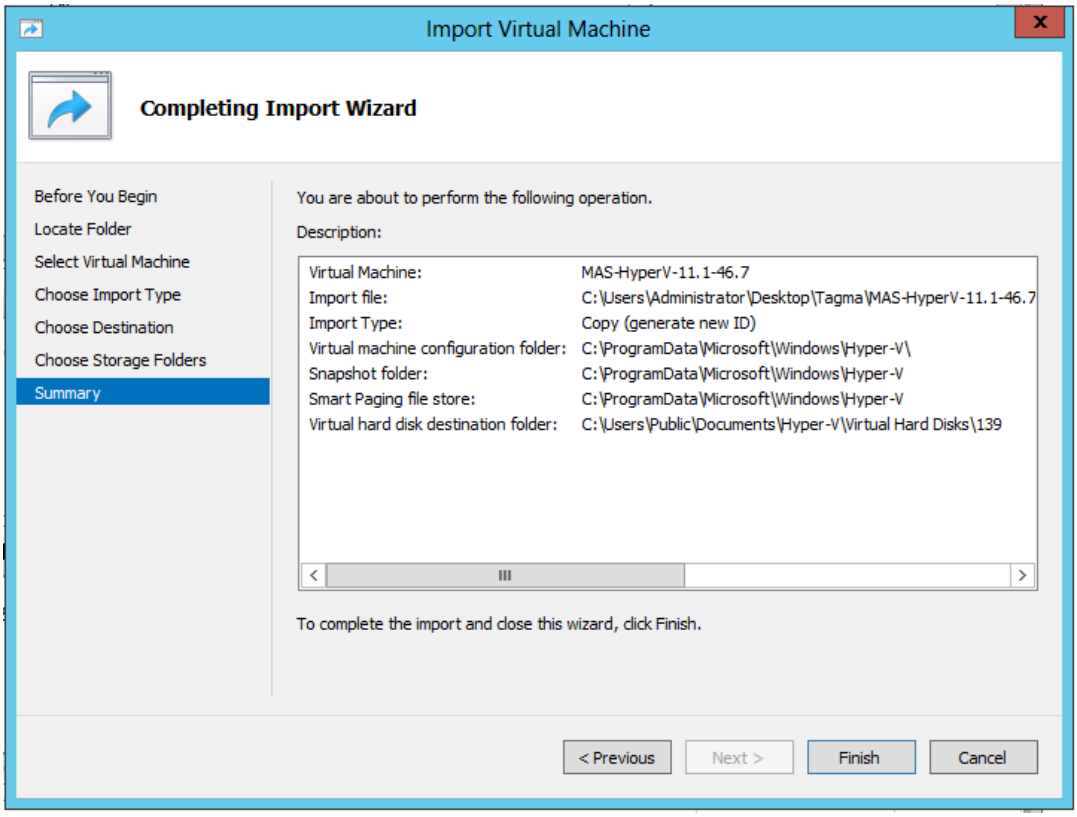
   d) 在 **Choose Destination**（选择目标）部分，可以指定要存储虚拟机文件的文件夹。

   > 注意
   >
   > 默认情况下，向导将虚拟机文件导入您本地主机上的默认 Hyper-V 文件夹。



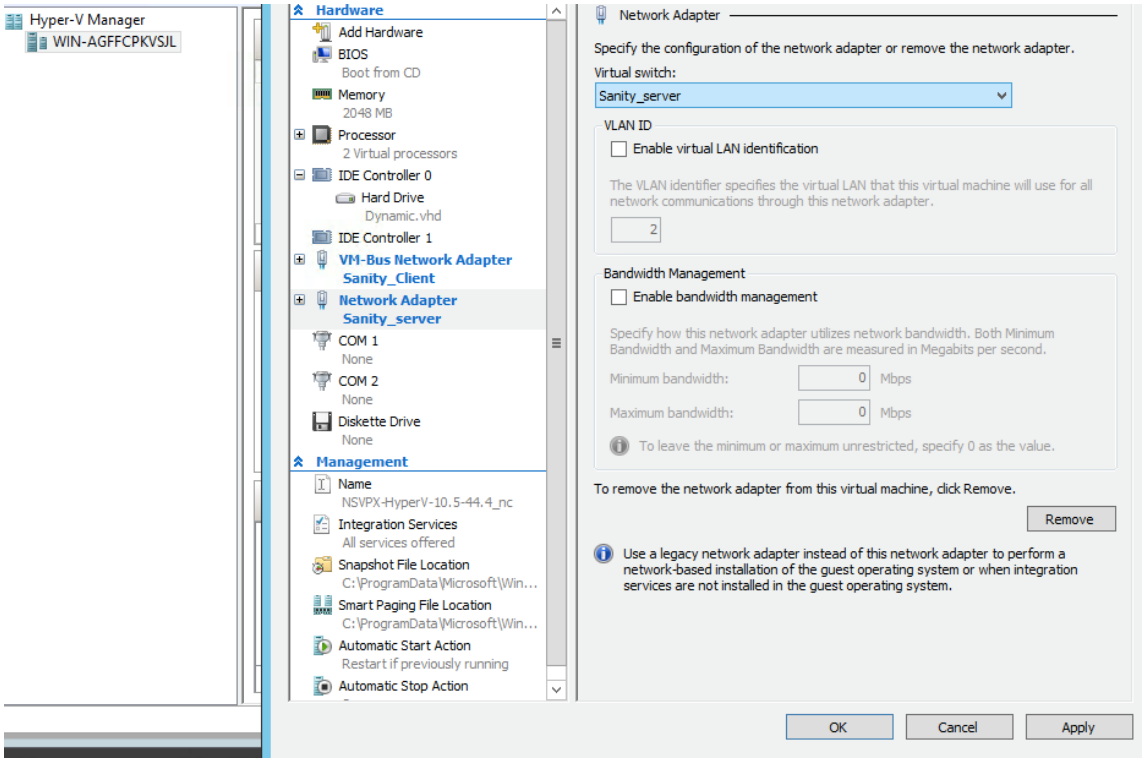
e) 在 **Choose Storage Folders**（选择存储文件夹）部分，可以选择要存储虚拟硬盘的位置，然后单击 **Next**（下一步）。

f) 可以在摘要窗格中确认虚拟机详细信息，单击 **Finish**（完成）。



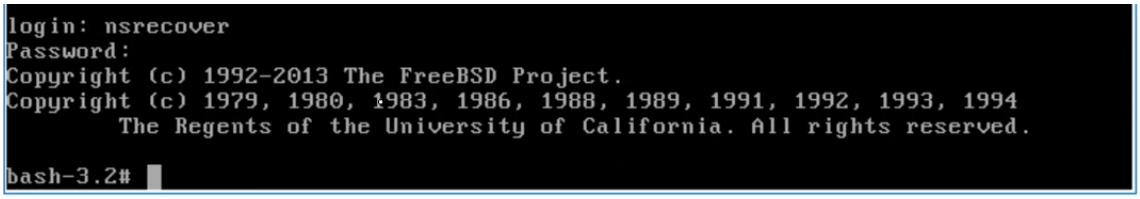
Citrix ADM Hyper-V 图像显示在右窗格中。

4. 右键单击 Citrix ADM Hyper-V 映像，然后单击 设置。
5. 在出现的对话框的左侧窗格中，导航到 硬件 > **VM_Bus** 网络适配器，然后在右侧窗格中，从网络下拉列表中选择相应的网络。



6. 单击 **Apply**（应用），然后单击 **OK**（确定）。
7. 右键单击 Citrix ADM Hyper-V 映像，然后单击“连接”。
8. 在控制台窗口中，单击“开始”按钮。
9. 配置初始网络配置选项。

10. 指定所需的 IP 地址后，保存配置设置。
11. 出现提示时，使用 nsrecover/nsroot 凭据登录。



> 注意
>
> 登录后，如果要更新初始网络配置，请键入 networkconfig，更新配置并保存配置。

12. 在 shell 提示符下键入命令来执行部署脚本：

```
deployment_type.py
<!--NeedCopy-->
```

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

13. 选择部署类型为 **Citrix ADM** 服务器。如果不选择任何选项，默认情况下，它部署为服务器。

```
------------------------------------------------------------------------------
-------------
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. 键入是 将 Citrix ADM 部署为独立部署。
15. 键入是以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，您可以稍后更新初始配置设置。

验证

安装服务器后，您可以通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问图形用户界面 (GUI)。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

搭载 **VMware ESXi** 的 **Citrix ADM**

February 6, 2024

要在 VMware ESXi 上安装 Citrix ADM 虚拟设备，请使用 VMware vSphere 客户端。

必备条件

在开始安装虚拟设备之前，请确认以下要求：

- 安装受支持的 VMware ESXi 版本（6.0、6.5 和 6.7）。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 下载 Citrix ADM 安装文件。

> 注意
>
> Citrix ADM 不支持 vMotion。

安装 **Citrix ADM**

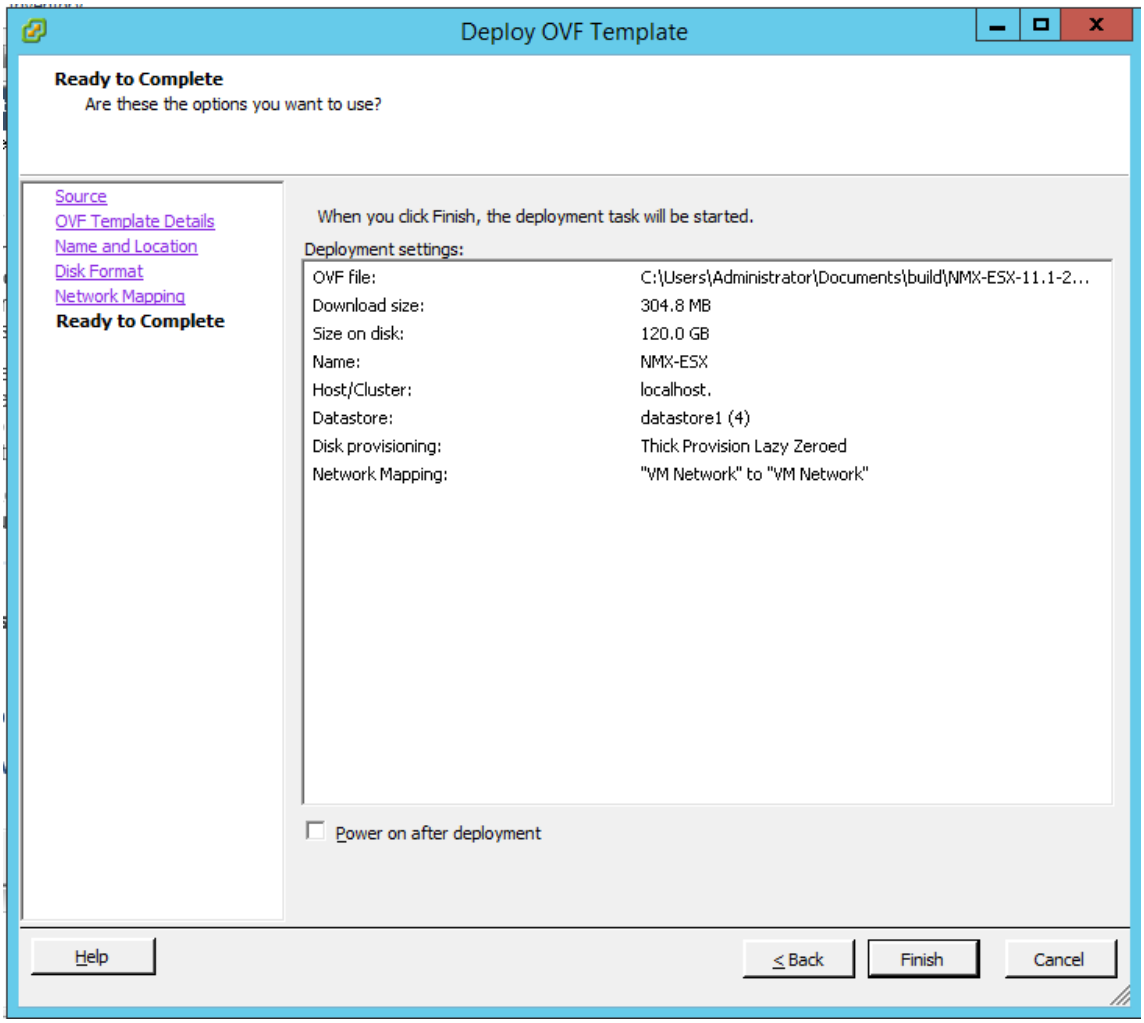
1. 在工作站上启动 VMware vSphere Client。
2. 在 **IP address / Name**（IP 地址/名称）文本框中，键入要连接到的 VMware ESXi 服务器的 IP 地址。
3. 在 **User Name**（用户名）和 **Password**（密码）文本框中，键入管理员凭据，然后单击 **Login**（登录）。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在 **Deploy OVF Template**（部署 OVF 模板）对话框中，在 **Deploy from file or URL**（从文件或 URL 部署）中，选择.ovf 文件，然后单击 **Next**（下一步）。

   > 注意
   >
   > 如果出现包含以下文字的警告消息：The operating system identifier is not supported on the selected host（在所选主机上不支持操作系统标识符），请检查 VMware 服务器是否支持 FreeBSD 操作系统。单击是。

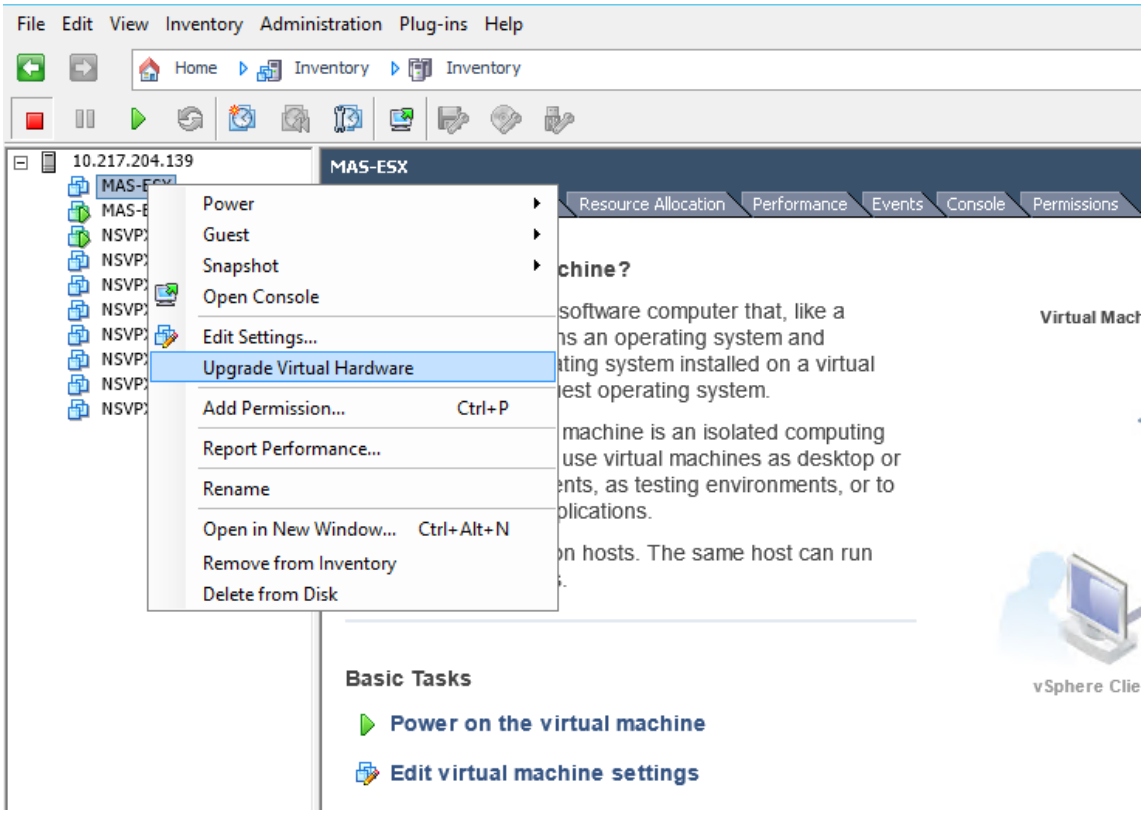
6. 在 **OVF Template Details**（OVF 模板详细信息）页面上，单击 **Next**（下一步）。
7. 键入 Citrix ADM 虚拟设备的名称，然后单击 **Next**（下一步）。
8. 指定 “Disk Format”（磁盘格式）：选择” Thin provisioned format”（瘦置备格式）或 “Thick provisioned format”（密集置备格式）。

   > 注意
   >
   > Citrix 建议选择 **Thick provisioned format**（密集置备格式）。

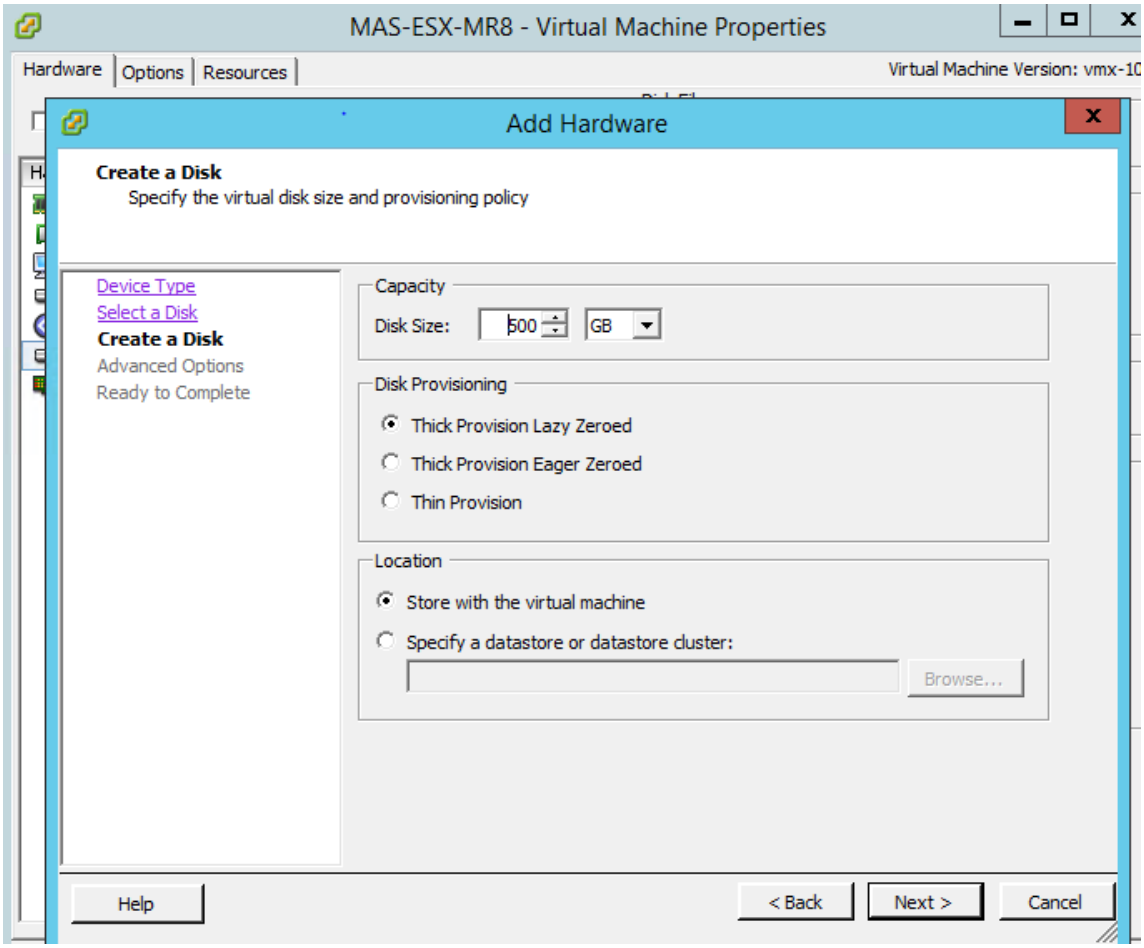
9. 单击 **Finish**（完成）开始安装过程。



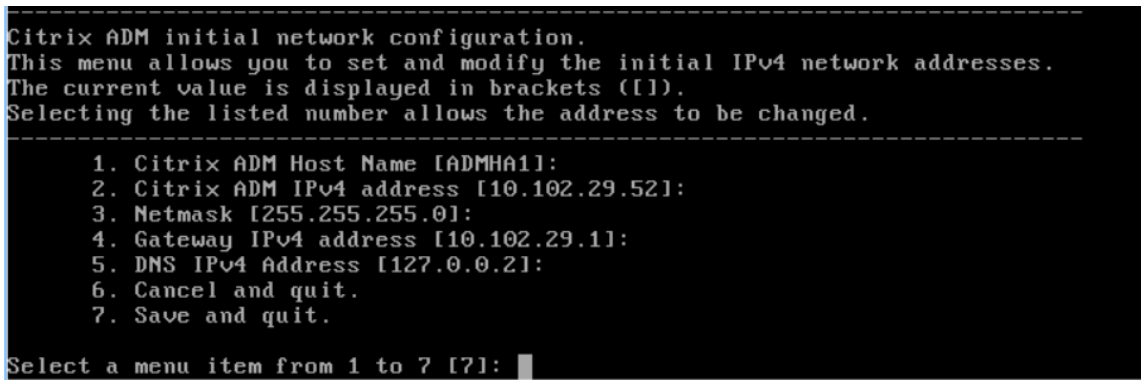
10. 此时您可以随时启动 Citrix ADM 虚拟设备。
11. 在导航窗格中，选择您安装的虚拟设备。在清单菜单中，右键单击虚拟机，然后单击升级虚拟硬件。在 **Confirm Virtual Machine**（确认虚拟机）对话框中，单击 **Yes**（是）。



12. 在 **Inventory**（清单）菜单中，单击 **Virtual Machine**（虚拟机），然后选择 **Edit Settings**（编辑设置）。
13. 在 **Virtual Machine Properties**（虚拟机属性）对话框中的 **Hardware**（硬件）选项卡上，单击 **Memory**（内存），然后在右侧窗格中指定 **Memory Size**（内存大小）为 32 GB。
14. 单击 **CPUs**（CPU），然后在右侧窗格中指定 CPU 为 8。单击确定。
15. 根据您的要求添加额外的磁盘。



16. 在导航窗格中，选择您安装的虚拟设备。在清单菜单中，单击虚拟机，单击电源，然后单击开机。
17. 单击控制台选项卡以显示 Citrix ADM 初始网络配置选项。



18. 指定所需的 IP 地址后，保存配置设置。
19. 出现提示时，使用 ns 恢复/nsroot 凭据登录。


```
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#
```

> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置并保存配置。

20. 在 shell 提示符下键入命令来执行部署脚本：

```
deployment_type.py
<!--NeedCopy-->
```

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

21. 选择部署类型为 **Citrix ADM** 服务器。如果不选择任何选项，默认情况下，它部署为服务器。

```
------------------------------------------------------------------------------
-------------
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. 键入是将 Citrix ADM 部署为独立部署。
23. 键入是以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，您可以稍后更新初始配置设置。

验证

安装服务器后，可以通过在浏览器中键入 Citrix ADM 服务器的 IP 地址来访问 GUI。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

> 注意
>
> 在 VMware ESXi 上部署时，Citrix ADM 可能需要长达 30 分钟或更长时间才能启动。

搭载 **Linux KVM** 服务器的 **Citrix ADM**

February 6, 2024

可在其上配置 Citrix Application Delivery Management (ADM) 的虚拟化平台包括 Linux-KVM。

在 Linux-KVM 上安装 Citrix ADM 之前，请确保系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。确认 *virsh*（用于管理虚拟机的命令行工具）在虚拟机管理程序上可用。

使用您的管理员凭据登录到 Citrix.com 网站，访问最新的 Citrix ADM 安装文件，然后将其下载到您的计算机上。然后，在您的 Linux-KVM 平台上安装 Citrix ADM，并针对您的网络进行配置。

必备条件

在安装 Citrix ADM 虚拟设备之前，请验证 Linux-KVM 版本 3.6.11-4 及更高版本安装在符合最低要求的硬件上。

硬件要求

组件	要求
CPU	具有英特尔 VT-X 处理器中包含的硬件虚拟化功能的 64 位 x86 处理器。至少提供 2 个 CPU 内核以托管 Linux-KVM。注意 要测试 CPU 是否支持 Linux 主机，请在主机 Linux shell 提示符下输入以下命令：`*. egrep'^flags.\* ( vmx | svm )' /proc/cpuinfo*` 如果该扩展的 BIOS 设置被禁用，则必须在 BIOS 中启用它们。没有具体的处理器速度建议，但速度越高，Citrix ADM 的性能就越好。
内存 (RAM)	最低 4 GB，用于主机 Linux 内核。添加 VM 所需的其他内存。
硬盘	计算主机 Linux 内核和 VM 的空间要求。单个 Citrix ADM 虚拟机需要 120 GB 的磁盘空间。

> 注意
>
> 考虑到主机上没有其他虚拟机运行，指定的内存和硬盘要求用于在 OpenStack 平台上部署 Citrix ADM。OpenStack 的硬件要求取决于其上运行的虚拟机数量。

软件要求

Citrix 建议较新的内核，例如 64 位版本的 3.6.11-4 内核或更高版本。

网络要求　Citrix ADM 仅支持一个 Virtio 准虚拟化网络接口。此接口应连接到 Linux-KVM 主机的管理网络，以便 Citrix ADM 和 Linux-KVM 可以通信。

下载 **Citrix ADM** 安装文件

要从 www.citrix.com 下载 Citrix ADM 安装程序文件，请执行以下操作：

1. 打开 Web 浏览器并在地址栏中键入 www.citrix.com。
2. 将鼠标悬停在“登录”选项上，然后单击“我的帐户”，输入您的 Citrix 凭据，然后再次单击“登录”。
3. 导航至“下载”部分。
4. 从“下载”下拉列表中，选择 **Citrix Application Delivery Management**。
5. 在 **Citrix Application Delivery Management** 页面上，选择发行版。例如，选择 版本 **12.1**。
6. 单击“产品软件”将其展开，然后单击最新版本。例如，选择 **Citrix ADM** 版本（功能阶段）**12.1** 版本 **49.23/49.37**。

   将显示选定的构建页面。
7. 在“跳转到下载”下拉列表中，选择 适用于 **KVM** 的 **Citrix ADM** 镜像，**12.1 Build xx.xx**
8. 单击下载文件，接受最终用户许可协议，并将压缩的映像文件下载到您本地计算机上的任何文件夹。

在 **Linux-KVM** 上安装 **Citrix Application Delivery Management**

1. 使用 SSH，登录 KVM 主机。
2. 在 CLI 提示窗口中，通过使用任何一个文件传输程序，将映像复制到服务器上的一个文件夹中。
3. 导航到保存下载的映像的目录。
4. 在命令行上执行以下操作：

   a) 列出目录中的文件以确认映像文件是否存在。

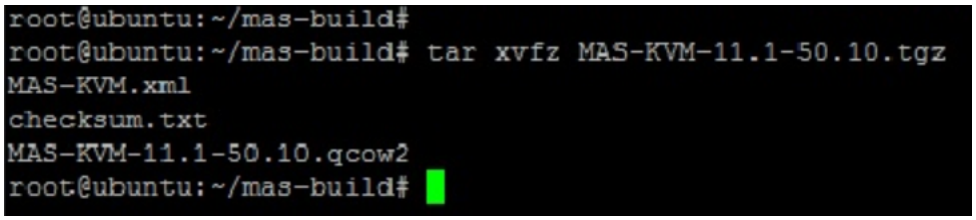
b) 使用 tar 命令可取消 Citrix Application Delivery Management 映像文件。解压缩的包中包含以下组件：

i. 指定 Citrix ADM 属性的域 XML 文件

ii. 指定域磁盘映像的校验和的文本文件

iii. 域磁盘映像

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



iv. 创建 MAS-KVM.xml 副本，保存为 MAS1-KVM.xml，作为备份选项。使用 vi 编辑器打开 MAS1-KVM.xml 文件。

v. 在 MAS1-KVM.xml 中编辑以下网络连接属性：

A. name-指定名称。

B. mac-指定 MAC 地址。

C. 源文件-指定绝对磁盘映像源路径。文件路径必须为绝对路径。

> 注意
>
> 域名和 MAC 地址必须具有唯一性。

D. 模式-指定模式。

E. 模型类型-设置为 Virtio。

F. 源代码开发-指定接口。

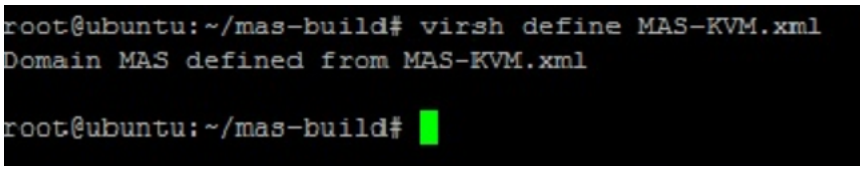
```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

vi. 使用以下命令在 MAS1-KVM.xml 文件中定义 VM 属性：*virsh define <FileName>.xml*

```
virsh define MAS-KVM.xml
```



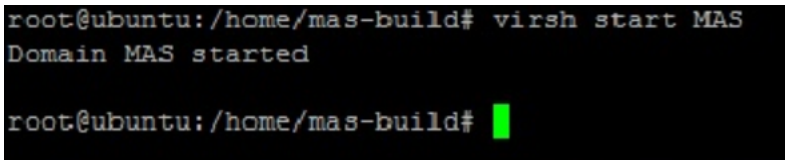
```
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```



输入以下命令启动 Citrix ADM：*virsh start [ ]*

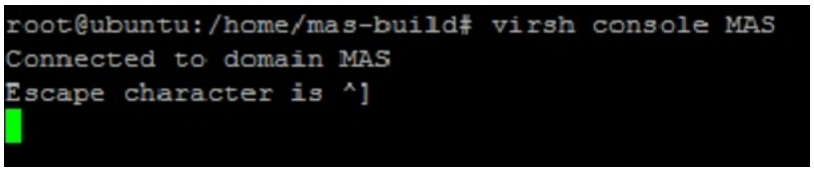
vii.

```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



viii. 您可以使用以下命令连接到 Citrix ADM 虚拟机：*virsh console <DomainName>*

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```



配置 Citrix Application Delivery Management

> 注意
>
> 在有些 Linux KVM 主机上，如果 FreeBSD 来宾有多个 CPU，他们将无法正确重新启动。重新启动 Citrix ADM 虚拟设备时，Citrix ADM CLI 和 GUI 将变得无响应。有关详细信息，请参见https://bugs.launchpad.net/qemu/+bug/1329956
>
> 要避免 Citrix ADM 虚拟设备重新启动时 Citrix ADM CLI 和 GUI 无响应，请关闭 KVM 主机上的所有虚拟机，然后在 KVM 主机上执行以下操作：
>
> 1. 使用以下命令删除 *kvm_Intel* 模块：

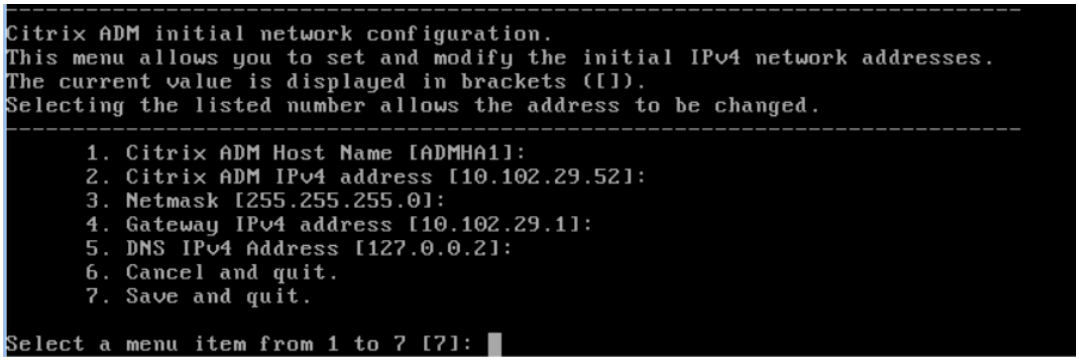
2. 禁用 APICV 并使用以下命令重新加载 Kvm_ 英特尔模块：
   模块探测器 *Kvm_* 英特尔启用 *_ APICV=N*
3. 在 KVM 主机上启动虚拟机。

安装 Citrix ADM 后，等待大约 10 分钟以使服务可用，然后登录 Citrix ADM。

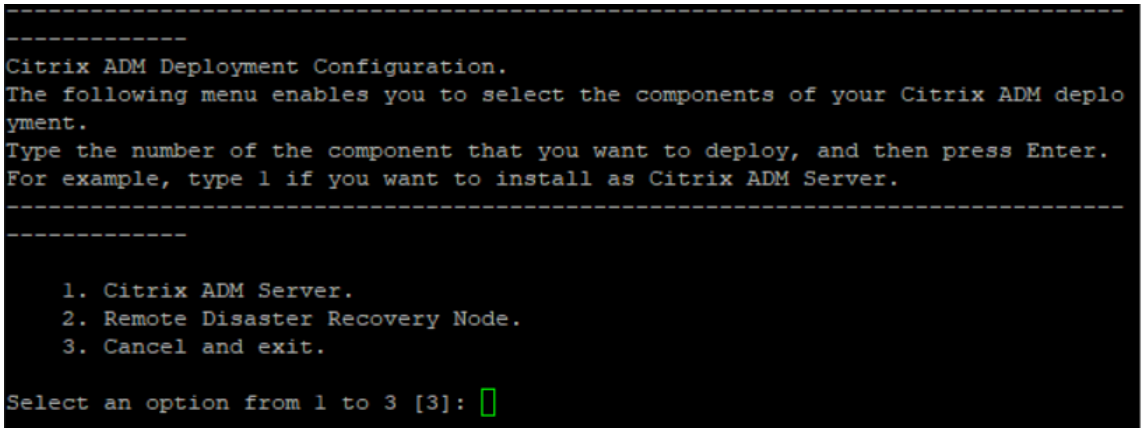
1. 在命令行上，使用默认的系统管理员凭据登录系统：
   - 用户名：nsroot
   - 密码：nsroot

   > 注意
   >
   > 首次登录后，必须更改管理密码。然后，配置 MAS 以在您的网络中运行。您可以从 Citrix ADM 用户界面更改密码。在 Citrix ADM 主页上，导航到“系统”>“用户管理”>“用户”。选择用户并单击 **Edit**（编辑），然后在“Password”（密码）字段中更新密码。

2. 在提示符下，键入：*shell*
3. 键入 网络配置 以进入 Citrix ADM 初始网络配置菜单。配置管理 IP 地址。
4. 要完成 Citrix ADM 的初始网络配置，请按照提示操作。控制台显示 Citrix ADM 初始网络配置选项，用于设置 Citrix ADM 的以下参数。默认情况下，已填充主机名。
   a) 输入 **2** 以更新 Citrix ADM IPv4 地址-用于访问 Citrix ADM 的管理 IP 地址
   b) 输入 **3** 更新网络掩码-与管理 IP 地址关联的子网掩码
   c) 输入 **4** 以更新 Gateway IPv4 地址—Citrix ADM 管理 IP 地址子网的默认网关 IP 地址
   d) 输入 **7** 保存并退出-保存配置更改并退出系统。

5. 在 shell 提示符下键入命令来运行部署脚本：*deployment_type.py*
6. 在显示的部署屏幕中，选择作为 **Citrix ADM** 服务器的部署类型。



7. 键入 是 将 Citrix ADM 部署为独立部署。
8. 键入“是”以重新启动 Citrix ADM 服务器。
9. Citrix ADM 服务器重新启动后，通过命令行或 GUI 使用默认管理员凭据作为 nsroot/nsroot 登录到 Citrix ADM。

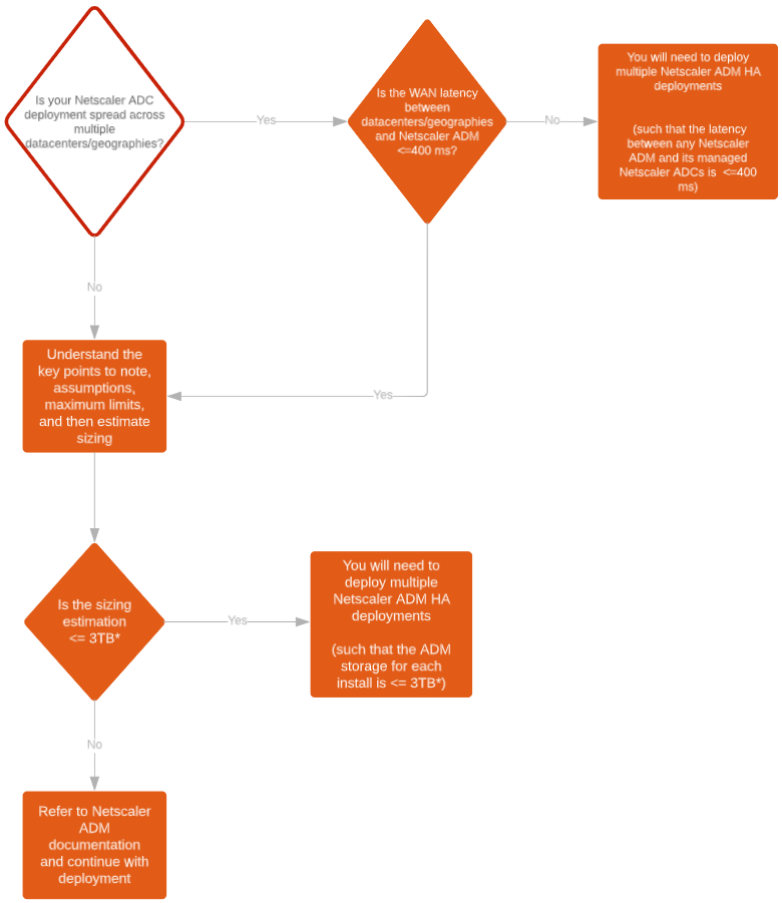
   您可以稍后通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问 Citrix ADM。登录服务器的默认管理员凭据是 *nsroot/nsroot*。

配置高可用性部署

February 6, 2024

高可用性 (HA) 是指在不中断服务的情况下始终可供用户使用的系统。高可用性设置在系统停机、网络或应用程序故障期间至关重要，是任何企业的关键要求。在主动-被动模式下以相同配置部署两个 Citrix ADM 节点的高可用性可提供不间断的操作。

部署方案



> 注意
>
> 单个 Citrix ADM HA 部署的验证最大存储限制为 3 TB。有关详细信息，请参阅 部署指南。
>
> 重要
>
> 要使用 **HTTPS** 访问 **Citrix ADM 12.1 Build 48.18** 或更高版本，请执行以下操作：
>
> 如果您已将 Citrix ADC 实例配置为在高可用模式下对 Citrix ADM 进行负载平衡，请先删除 Citrix ADC 实例。然后，配置浮动 IP 地址以在高可用模式下访问 Citrix ADM。

以下是在 Citrix ADM 中部署高可用性的好处：

- 一种改进的监视主节点和辅助节点之间心跳的机制。
- 提供数据库的物理流式复制，而不是逻辑双向复制。
- 能够在主节点上配置浮动 IP 地址，从而无需单独使用 Citrix ADC 负载平衡器。
- 使用浮动 IP 地址可轻松访问 Citrix ADM 用户界面。
- 仅在主节点上提供 Citrix ADM 用户界面。通过使用主节点，您可以消除访问辅助节点和更改辅助节点的风险。

- 配置浮动 IP 地址可处理故障转移情况，无需重新配置实例。
- 提供检测和处理脑分裂情况的内置能力。

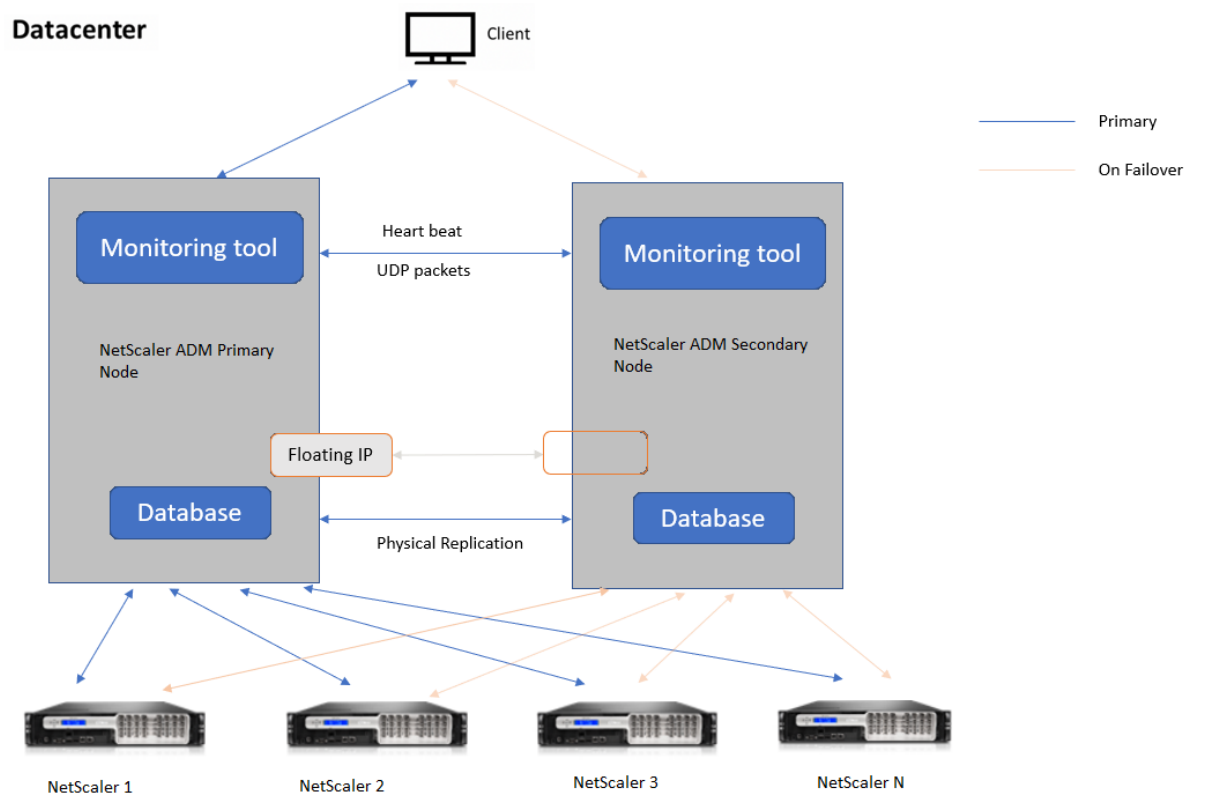
下表描述了高可用性部署中使用的术语。

条款	说明
主节点	在高可用性部署中注册的第一个节点。
辅助节点	在高可用性部署中注册的第二个节点。
心跳	一种用于在高可用性设置中在主节点和辅助节点之间交换消息的机制。这些消息决定了每个节点上应用程序的状态和运行状况。
浮动 IP 地址	浮动 IP 是一种可以立即从同一子网中的一个节点移动到另一个节点的 IP 地址。在内部，它被设置为主节点网络接口上的别名。如果出现故障转移，则浮动 IP 地址将从旧的主地址无缝移动到新的主地址。它在高可用性设置中非常有用，因为它允许客户端使用单个 IP 地址与高可用性节点进行通信。

> 说明
>
> 有关端口和协议的详细信息，请参阅 端口。

高可用性体系结构的组件

下图显示了在高可用性模式下部署的两个 Citrix ADM 节点的体系结构。



在高可用性部署中，一个 Citrix ADM 节点配置为主节点 (MAS 1)，另一个配置为辅助节点 (MAS 2)。如果主节点由于任何原因导致故障，辅助节点将接管作为新的主节点。

监视工具

监视工具是一个内部进程，用于监视、发出警报和处理故障转移情况。该工具处于活动状态，并在每个节点上以高可用性运行。它负责启动子系统、在两个节点上启动数据库、决定是否存在故障转移是主节点还是辅助节点，等等。

主节点

主节点接受连接并管理实例。所有进程，例如 AppFlow、SNMP、LogStream、syslog 等，都由主节点管理。主节点上可以访问 Citrix ADM 用户界面。浮动 IP 地址是在主节点上配置的。

辅助节点

辅助节点监听从主节点发送的心跳消息。辅助节点上的数据库仅处于只读副本模式。辅助节点中没有任何进程处于活动状态，并且无法在辅助节点上访问 Citrix ADM 用户界面。

物理流式复制

主节点和辅助节点通过心跳机制进行同步。通过数据库的物理流式复制，辅助节点以只读副本模式启动。辅助节点监听从主节点收到的心跳消息。如果辅助节点在 180 秒的时间段内未收到任何心跳信号，则认为主节点已关闭。然后，辅助节点接管主节点。

心跳消息

Heartbeat 消息是在主节点和辅助节点之间发送和接收的用户数据报数据包 (UDP)。它监视 Citrix ADM 和数据库的所有子系统，以交换有关节点状态、运行状况、进程等的信息。信息每秒在高可用性节点之间共享。如果出现故障转移或高可用性状态中断，则会将通知作为警报发送给管理员。

浮动 **IP** 地址

浮动 IP 地址与高可用性设置中的主节点相关联。它是为主节点 IP 地址指定的别名，客户端可以使用该别名连接到主节点中的 Citrix ADM。由于浮动 IP 地址是在主节点上配置的，因此在故障转移时不需要重新配置实例。实例重新连接到相同的 IP 地址以访问新的主节点。

需要注意的要点

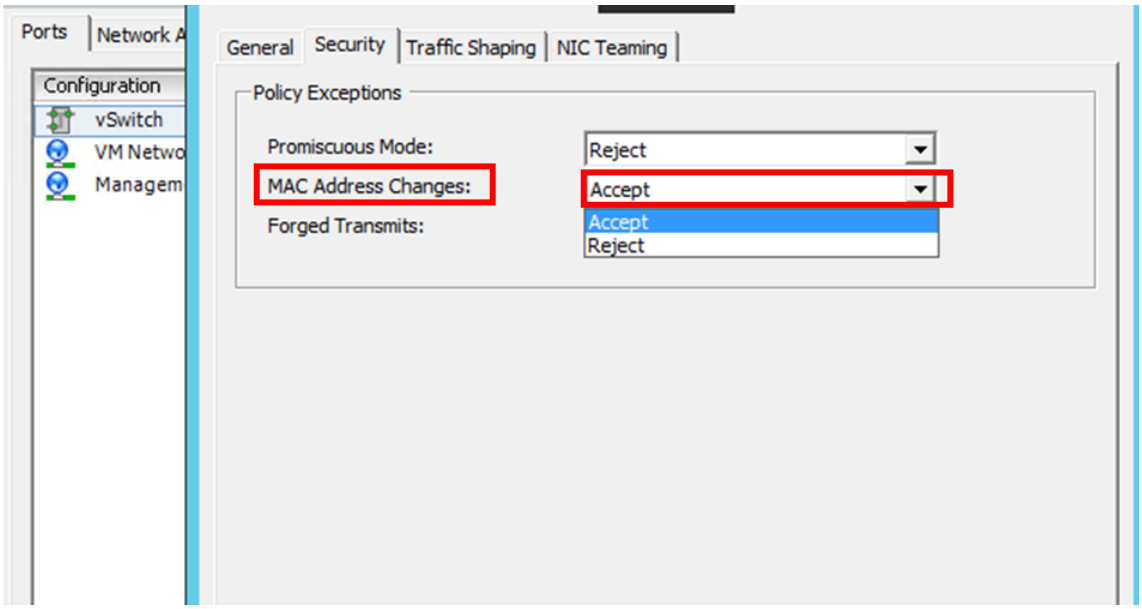
- 在高可用性设置中，两个 Citrix ADM 节点都以主动-被动模式部署。它们必须位于相同的子网上，使用相同的软件版本和版本，并且具有相同的配置。
- 浮动 IP 地址：
  - 浮动 IP 地址是在主节点上配置的。
  - 如果存在故障转移，则无需重新配置实例。
  - 您可以使用主节点 IP 或浮动 IP 地址，从用户界面访问高可用性节点。

    > 注意
    >
    > Citrix 建议您使用浮动 IP 地址访问用户界面。

- 数据库：
  - 在高可用性设置中，所有配置文件会以一分钟的间隔自动从主节点同步到辅助节点。
  - 数据库同步通过数据库的物理复制立即发生。
  - 辅助节点上的数据库处于只读副本模式。
- Citrix ADM 升级：
  - 内部流程隐含地从早期版本升级 Citrix ADM。

> 注意
>
> 升级成功后，必须配置浮动 IP 地址。

- UDP 默认端口 5005 在两个节点上都可用，用于发送心跳信号和接收消息。
- MAC 地址
  虚拟机管理程序中“MAC 地址更改”选项的设置会影响虚拟机接收的流量。允许在虚拟交换机上启用 MAC 地址更改，以便浮动 IP 地址在故障转移后无缝移动到新的主节点。
  例如，在 VMware ESXi 上以高可用性部署 Citrix ADM 时，请确保接受对 MAC 地址的更改。ESXi 现在允许请求将活动 MAC 地址更改为初始 MAC 地址以外的其他地址。



必备条件

在为 Citrix ADM 节点设置高可用性之前，请注意以下先决条件：

- Citrix ADM 高可用性部署由 Citrix ADM 版本 12.0 版本 51.24 支持。
- 从 Citrix 下载站点下载 Citrix Application Delivery Management 映像文件 (.xva)：https://www.citrix.com/downloads/

Citrix 建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了虚拟计算资源的最低要求：

组件	要求
RAM	**32 GB**

组件	要求
虚拟 CPU	**8** 个 **CPU**
存储空间	Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。如果您的 Citrix ADM 存储要求超过 120 GB，则必须附加额外的磁盘。注意 您只能添加一个额外的磁盘。Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。有关更多信息，请参阅 如何将其他磁盘附加到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序	版本
Citrix Hypervisor	6.2 和 6.5
VMware ESXi	5.5 和 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu 和 Fedora

将 **Citrix ADM** 设置为高可用性模式

1. 注册并部署第一台服务器（主节点）。
2. 注册并部署第二台服务器（辅助节点）。
3. 部署主节点和辅助节点以进行高可用性设置。

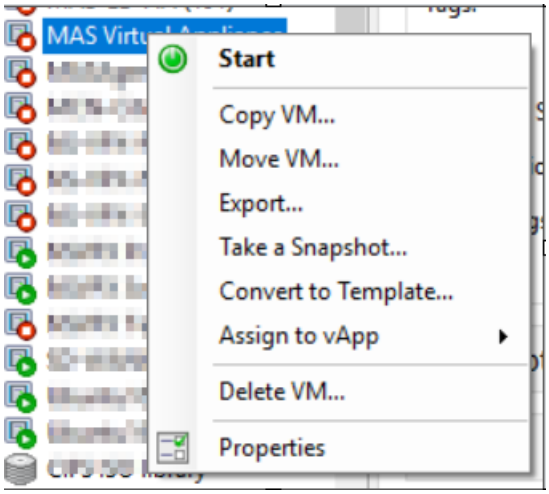
注册并部署第一台服务器（主节点）

要注册第一个节点，请执行以下操作：

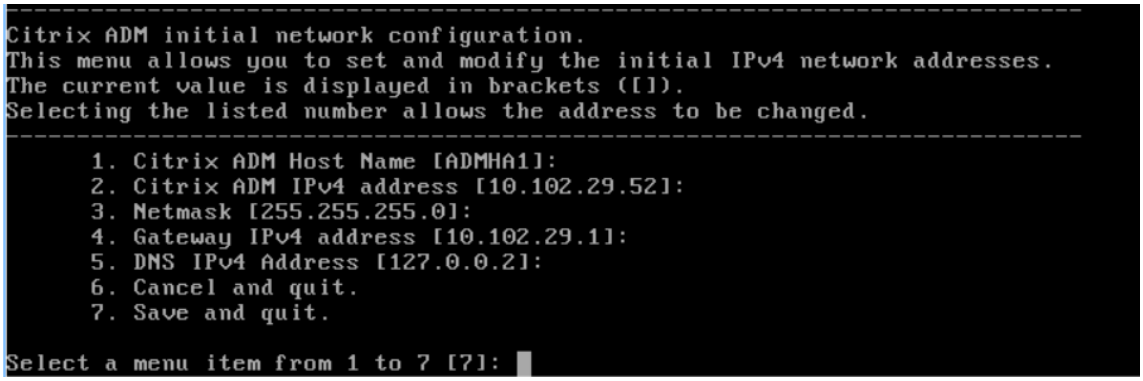
1. 使用从 Citrix 下载站点下载的.xva 映像文件并将其导入您的虚拟机管理程序。

   > 注意
   >
   > .xva 图像文件可能需要几分钟才能导入并启动。您可以在屏幕底部看到状态。
   >
   >
   >

2. 导入成功后，右键单击并单击“开始”。



3. 在控制台选项卡中，使用初始网络配置配置 Citrix ADM。



4. 初始网络配置完成后，系统将提示登录。使用以下凭据登录—*nsrecover/nsroot*。

> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置并保存配置。

5. 要部署主节点，请输入 **/mps/**部署类型**.py**。将显示 Citrix ADM 部署配置菜单。

6. 选择 **1** 将 Citrix ADM 服务器注册为主节点。


```
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]:
```

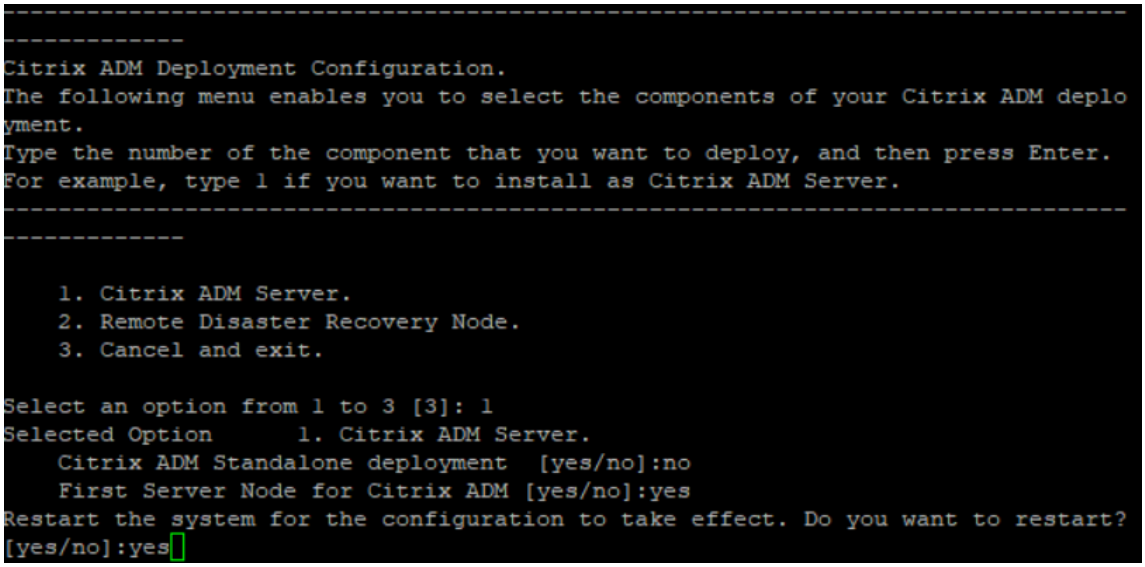
7. 控制台会提示您选择 Citrix ADM 独立部署。输入否 以确认部署为高可用性。

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

8. 控制台提示您选择第一个服务器节点。输入 **Yes** 以确认节点为第一个节点。

```
------------------------------------------------------------------------------
------------
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. 控制台提示您重新启动系统。输入“是”以重新启动。



系统将重新启动，并在 Citrix ADM 用户界面中显示为主节点。

注册并部署第二台服务器（辅助节点）

1. 使用从 Citrix 下载站点下载的 **.xva** 映像文件并将其导入您的虚拟机管理程序。
2. 在控制台选项卡中，使用初始网络配置配置 Citrix ADM，如下图所示。
3. 完成初始网络配置后，系统会提示登录。使用以下凭据登录—*nsrecover/nsroot*。

   > 注意
   >
   > 登录后，如果要更新初始网络配置，请键入 `networkconfig`，更新配置并保存配置。

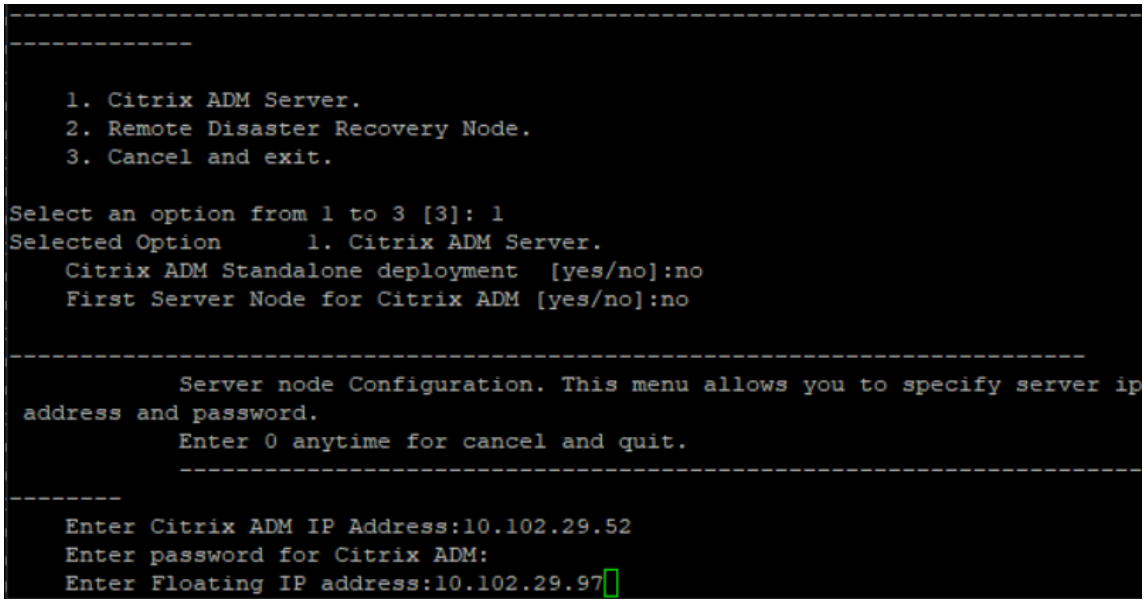
4. 要部署辅助节点，请输入 **/mps/**部署类型**.py**。此时将显示 Citrix ADM 部署配置菜单。
5. 选择 **1** 将 Citrix ADM 服务器注册为辅助节点。
6. 控制台会提示您选择 Citrix ADM 作为独立部署。输入否 以确认部署为高可用性。
7. 控制台提示您选择第一个服务器节点。输入否 以确认节点为第二台服务器。


```
--------------------------------------------------------------------------------
-------------
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. 控制台会提示您输入主节点的 IP 地址和密码。

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

    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. 控制台提示您输入浮动 IP 地址。



10. 控制台提示您重新启动系统。输入“是”以重新启动。

> 注意
>
> - 浮动 IP 地址是节点高可用性部署的必备条件。
> - 如果配置中存在任何问题，系统将显示错误消息。
> - 系统重新启动，需要几分钟才能使配置生效。

将主节点和辅助节点部署为高可用性对

注册后，主节点和辅助节点都将显示在 Citrix ADM 用户界面上。将这些节点部署到高可用性对中。

> 注意
>
> - 在将节点部署到高可用性对之前，请确保在初始网络配置完成后重新启动辅助节点。
> - 高可用性部署完成后，使用浮动 IP 地址访问 Citrix ADM 用户界面。

要将节点作为高可用性对部署，请执行以下操作：

1. 打开 Web 浏览器并输入第一个 Citrix ADM 服务器节点的 IP 地址。
2. 在用户名和密码 字段中，输入管理员凭据。
3. 在主页中单击“开始”。
4. 选择部署类型作为在高可用性模式下部署的两台服务器，然后单击下一步。
5. 在“部署”页上，单击“部署”。

6. 将显示一条确认消息。单击是。

   Citrix ADM 将重新启动，配置需要大约 10 分钟才能生效。

   > 注意：
   >
   > 您现在可以开始使用浮动 IP 地址。

7. 使用管理员凭据登录 Citrix ADM，在主页中单击“开始”，然后根据需要完成以下操作：

   a) 添加 Citrix ADC 实例

   b) 配置客户身份

   > 注意：
   >
   > 您也可以单击“跳过”以稍后完成，然后单击“完成”。

8. 导航到“系统”>“部署”以验证部署。

   有关更多信息，请参阅 常见问题解答。

禁用高可用性功能

您可以在 Citrix ADM 高可用性对上禁用高可用性，并将这些节点转换为独立的 Citrix ADM 服务器。

> 注意
>
> 禁用主节点的高可用性。

要禁用高可用性，请执行以下操作：

1. 在 Web 浏览器中，输入 Citrix ADM 服务器主节点的 IP 地址。
2. 在“用 户名”和“密码”字段中，输入管理员凭据。
3. 在“系统”选项卡上，导航到“部署”，然后单击“中断高可用性”。

   此时将显示一个对话框。单击“是”中断高可用性部署。

重新部署高可用性

禁用独立部署的高可用性后，可以再次将其重新部署到高可用性模式。重新部署高可用性类似于首次部署高可用性。有关更多详细信息，请参阅 将主节点和辅助节点部署为高可用性对。

高可用性故障切换方案

遇到下列情况之一时，会发生故障转移：

- 节点故障：主节点停机，180 秒内未检测到来自主节点的心跳。
- 应用程序运行状况故障：主节点已启动并正在运行，但其中一个 Citrix ADM 进程已关闭。

大脑分裂场景

当由于网络链路停机而导致两个节点之间没有通信时，那么：

- 主节点继续作为主节点运行
- 由于无法接收心跳，辅助节点取代主节点
- 这两个节点都将运行各自的数据库实例

例如，在企业中，已将两个 Citrix ADM 节点部署为主节点和辅助节点。由于可能出现网络链路中断，两个 Citrix ADM 节点之间的通信完全中断。由于在 180 秒内没有心跳交换，因此两个节点都认为自己是主节点。两个节点都充当活动节点并运行自己的数据库实例。

使用 Citrix ADM 12.1，网络链路和心跳恢复后，这种脑分裂的情况可以得到妥善处理。高可用性同步会自动恢复。恢复时间取决于节点之间链路的数据和速度。

> 注意
>
> 在 split-brain 状态下，当新主节点以高可用性重新加入旧主节点时，在旧主节点上发生的更改将重置。分裂大脑期间在新主节点上发生的变化仍然完好无损。

配置灾难恢复以实现高可用性

February 6, 2024

灾害是由自然灾害或人为事件引起的业务功能突然中断。灾难会影响数据中心的运营，之后必须完全重建和恢复灾难现场丢失的资源和数据。数据中心中的数据丢失或停机至关重要，并使业务连续性崩溃。

Citrix ADM 12.1 灾难恢复 (DR) 功能为以高可用性模式部署的 Citrix ADM 提供完整的系统备份和恢复功能。恢复时，恢复站点中提供证书、配置文件和数据库的完整备份。

下表描述了在 Citrix ADM 中配置灾难恢复时使用的术语。

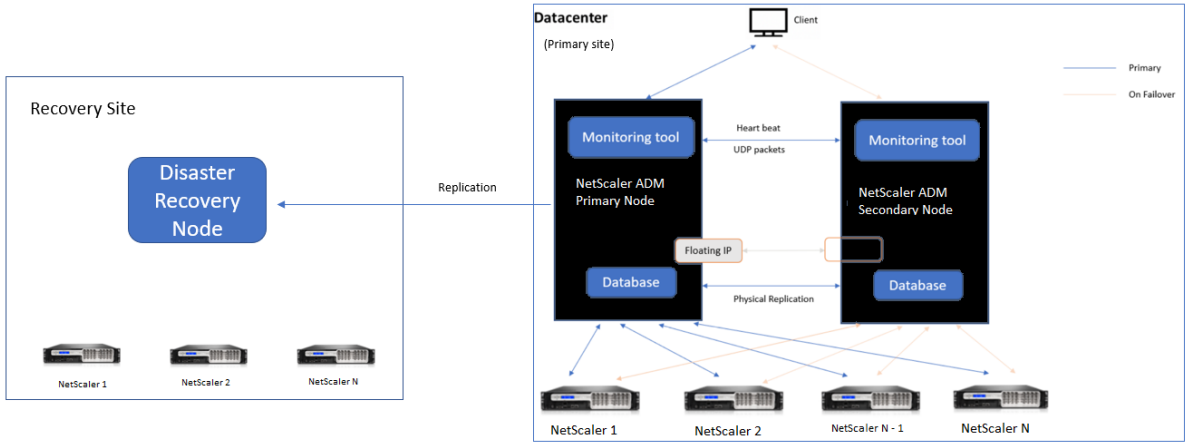
条款	说明
主站点（数据中心 A）	主站点以高可用性模式部署了 Citrix ADM 节点。
恢复站点（数据中心 B）	恢复站点具有以独立模式部署的灾难恢复节点。此节点处于只读模式，在主站点关闭之前无法运行。
灾难恢复节点	恢复节点是部署在恢复站点中的独立节点。如果灾难袭击主站点并且无法正常工作，则此节点可以运行（到新的主节点）。

> 注意：主站点和 DR 站点通过端口 5454 和 22 相互通信，默认情况下这些端口处于启用状态。
> 有关端口和协议的详细信息，请参阅 端口。

灾难恢复工作流程

下图显示了灾难恢复工作流程、灾难前的初始设置以及灾难发生后的工作流程。

灾难前的初始设置



该图显示灾难发生之前的灾难恢复设置。

主站点以高可用性模式部署了 Citrix ADM 节点。要了解更多信息，请参阅 高可用性部署

恢复站点具有远程部署的独立 Citrix ADM 灾难恢复节点。灾难恢复节点处于只读模式，从主节点接收数据以创建数据备份。还发现了恢复站点中的 Citrix ADC 实例，但它们没有任何流量流经这些实例。在备份过程中，所有数据、文件和配置都将从主节点复制到灾难恢复节点上。

必备条件

在设置灾难恢复节点之前，请注意以下先决条件：

- 要启用灾难恢复设置，主站点必须将 Citrix ADM 节点配置为高可用模式。
- 在主站点独立部署 Citrix ADM 不支持灾难恢复功能。
- Citrix ADM HA 对（在主站点中）和独立节点（在灾难恢复站点中）必须具有相同的软件版本、版本和配置。

Citrix 建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了配置灾难恢复节点的最低要求：

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。如果您的 Citrix ADM 存储要求超过 120 GB，则必须附加额外的磁盘。注意 您只能添加一个额外的磁盘。Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。有关更多信息，请参阅 如何将其他磁盘附加到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序	版本
Citrix Hypervisor	6.2 和 6.5
VMware ESXi	5.5 和 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	Ubuntu 和 Fedora

首次灾难恢复设置

- 在高可用性模式下部署 Citrix ADM
- 部署并注册 Citrix ADM 灾难恢复节点
- 从用户界面启用和禁用灾难恢复设置

在高可用性模式下部署 **Citrix ADM**

要设置灾难恢复设置，请确保在高可用性模式下部署 Citrix ADM。有关以高可用性方式部署 Citrix ADM 的信息，请参阅高可用性部署

> 注意
>
> - 在高可用模式下部署的 Citrix ADM 必须升级到 Citrix ADM 发行版 12.1。
> - 向主节点注册灾难恢复节点时，必须使用浮动 **IP** 地址。

部署并注册 **Citrix ADM** 灾难恢复节点

要注册 Citrix ADM 灾难恢复节点，请执行以下操作：

1. 从 Citrix 下载站点下载.xva 映像文件并将其导入到您的虚拟机管理程序中。
2. 在控制台选项卡中，使用初始网络配置配置 Citrix ADM。

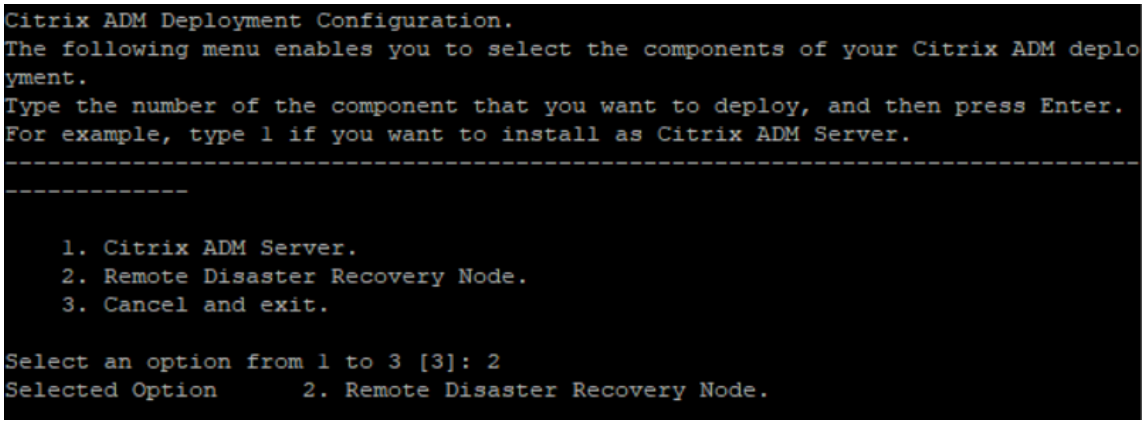
   > 注意
   >
   > 灾难恢复节点可以位于不同的子网上。

   ```
   ------------------------------------------------------------------------------
   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. 初始网络配置完成后，系统将提示登录。使用以下凭据登录—*nsrecover/nsroot*。
4. 要部署灾难恢复节点，请键入 **/mps/**部署 **_type.py** ，然后按 Enter 键。此时将显示 Citrix ADM 部署配置菜单。

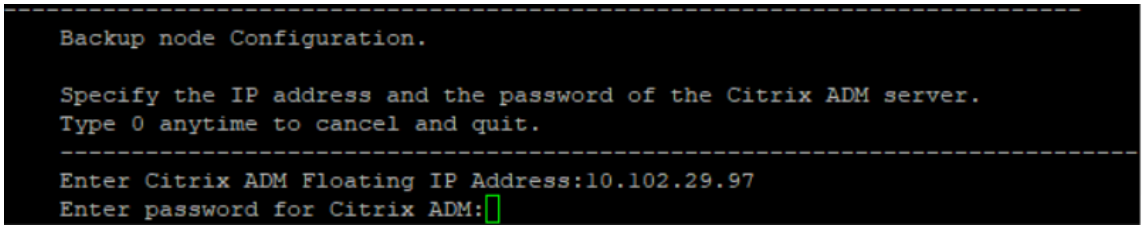
   ```
   bash-3.2# /mps/deployment_type.py
   ------------------------------------------------------------------------------
   -------------
   Citrix ADM Deployment Configuration.
   The following menu enables you to select the components of your Citrix ADM deplo
   yment.
   Type the number of the component 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. 选择 **2** 注册灾难恢复节点。

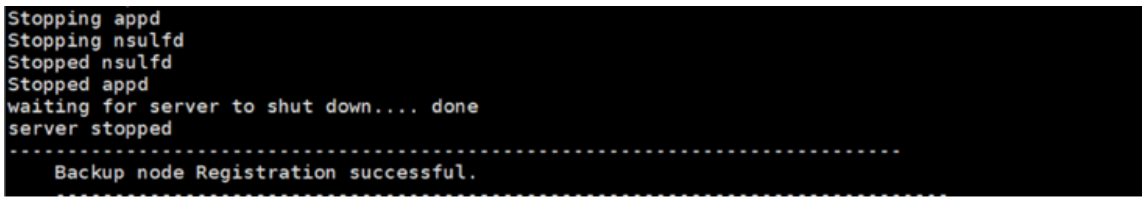


6. 控制台提示输入高可用性节点和密码的浮动 IP 地址。

7. 输入浮动 IP 地址和密码，将灾难恢复节点注册到主节点。



灾难恢复节点现在已成功注册。



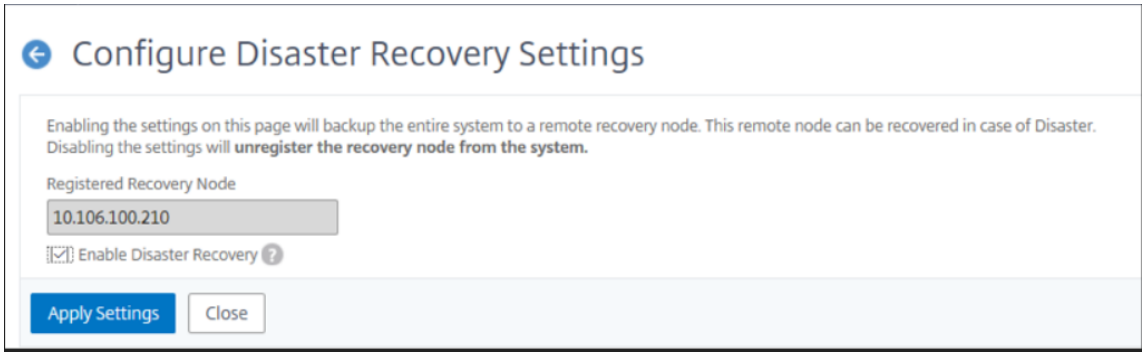
> ** 注
>
> 意 ** 灾难恢复节点没有 GUI。

从 **Citrix ADM GUI** 中启用灾难恢复设置

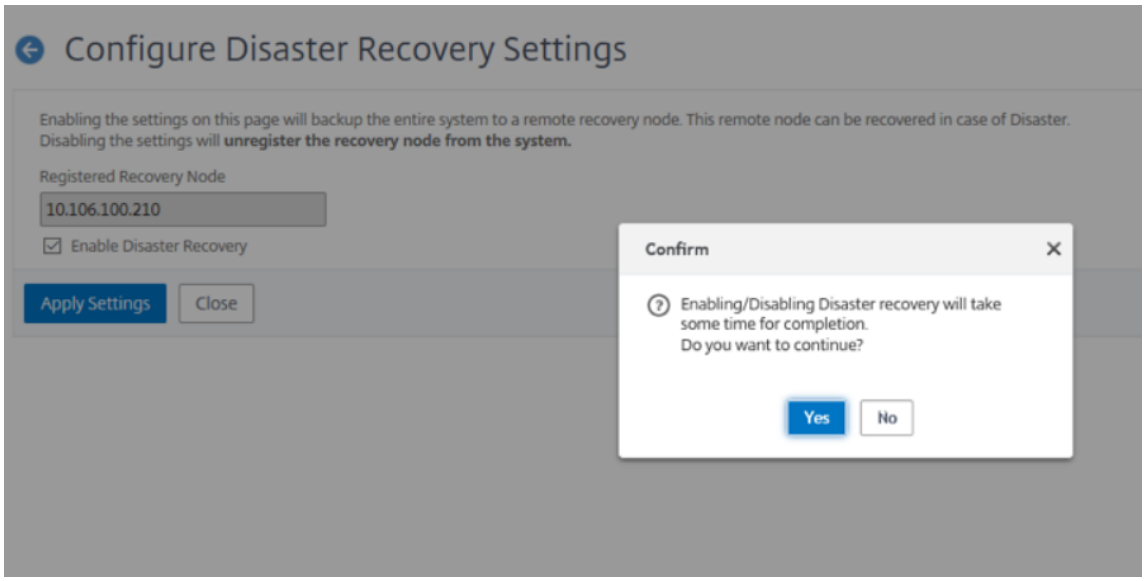
成功注册灾难恢复节点后，您可以从 Citrix ADM 主站点用户界面启用灾难恢复设置。

1. 导航到 系统 **>** 系统管理 **>** 灾难恢复设置。

2. 在“配置灾难恢复设置”页面上，选中“启用灾难恢复”复选框，然后单击“应用设置”。



3. 将显示一个确认对话框。单击“是”继续。



> 注意
>
> 系统备份所需的时间取决于数据大小和 WAN（广域网）链路速度。

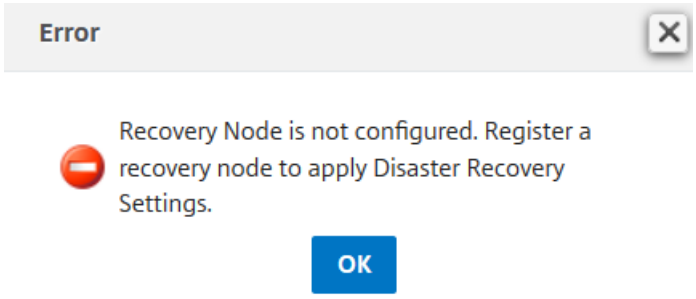
要禁用灾难恢复设置，请清除“启用灾难恢 复”复 选框，然后单击“应用设置”。

将显示一个确认对话框。单击“是”继续。

> 重要
>
> - 管理员有责任检测主站点上是否发生了灾难。
> - 灾难恢复工作流程不是自动化的，管理员必须在主站点关闭后手动启动。
> - 管理员必须通过在恢复站点的灾难恢复节点上执行恢复脚本来手动启动该过程。
> - 如果您在主站点中升级 HA 对，则必须手动升级 DR 站点中的独立节点。

如果您禁用“启用灾难恢复”选项并单击“应用设置”，则 Citrix ADM 不允许您再次选择“启用灾难恢复”选项。

当您单击“灾难恢复设置”时，会显示以下错误消息：



要再次启用 DR 节点，请为高可用性对重新配置 DR 节点：

a) 使用 Hypervisor 或 SSH 控制台登录 DR 节点。

b) 按照 部署中的步骤配置灾难节点，然后注册 Citrix ADM 灾难恢复节点。

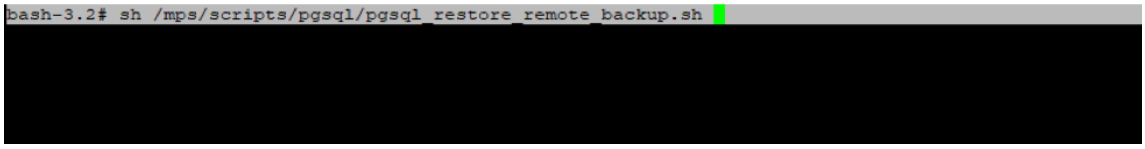
c) 启用灾难恢复选项。

有关更多信息，请参阅 常见问题解答。

灾难发生后的工作流程

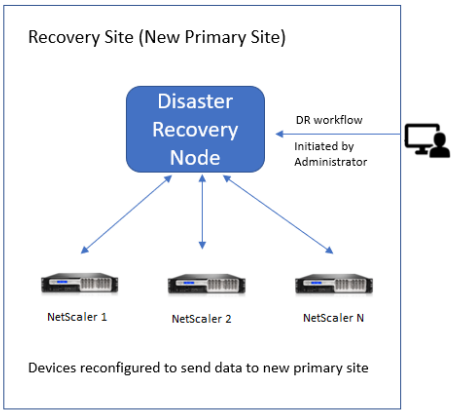
灾难发生后主站点出现故障时，必须按以下方式启动灾难恢复工作流程：

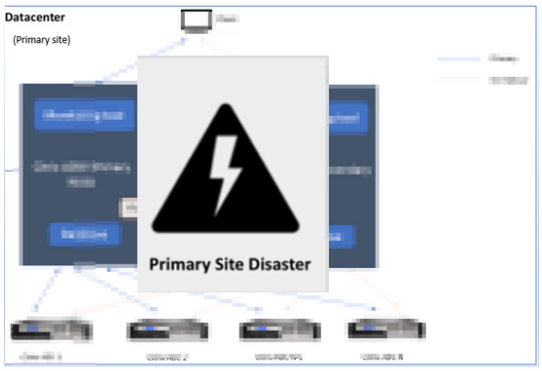
1. 管理员发现灾难袭击了主站点，该站点无法运行。
2. 管理员启动恢复过程。
3. 管理员必须在灾难恢复节点(恢复站点)上手动执行以下恢复脚本：**/mps/scripts/pgsql/pgsql_restore_remote_backup**



4. 在内部，Citrix ADC 实例会自动重新配置，以将数据发送到灾难恢复节点，该节点现在已成为新的主站点。

   下图显示灾难袭击主站点后的灾难恢复工作流。





> 注意：
>
> 在灾难恢复站点启动脚本后，灾难恢复站点现在成为新的主站点。您还可以访问 DR 用户界面。

灾后恢复

灾难发生且管理员启动恢复脚本后，灾难恢复站点现在将成为新的主站点。

> 重要
>
> - 如果您已经安装了 Citrix ADM 12.1.49.x 或更早版本，则可以在 30 天宽限期内联系 Citrix，在 Citrix ADM（灾难恢复站点）上重新托管原始许可。
> - 对于 12.1.50.x 或更高版本，Citrix ADM 许可会自动同步到灾难恢复站点（无需联系 Citrix 获取许可）。
> - 12.1.50.x 或更高版本支持灾难恢复站点的池化许可证。如果您已为实例应用了池许可证，请手动将实例重新配置到 DR 站点。

为多站点部署配置本地代理

February 6, 2024

在 Citrix ADM 的早期版本中，部署在远程数据中心的 Citrix ADC 实例可以通过在主数据中心运行的 Citrix ADM 进行管理和监视。Citrix ADC 实例将数据直接发送到主 Citrix ADM，从而消耗了 WAN（广域网）带宽。此外，分析数据的处理会使用主 Citrix ADM 的 CPU 和内存资源。

客户的数据中心遍布全球。在客户可以选择的以下场景中，代理商发挥着至关重要的作用

- 在远程数据中心安装代理，从而减少 WAN 带宽消耗。
- 限制直接向主 Citrix ADM 发送流量进行数据处理的实例数量。

> 注意
>
> - 建议在远程数据中心中为实例安装代理，但不是强制安装代理。如果需要，用户可以直接将 Citrix ADC 实例添加到主 Citrix ADM 中。
> - 如果您已经为远程数据中心安装了代理，则代理与主站点之间的通信是通过浮动 IP 地址进行的。有关详细信息，请参阅端口。
> - 您可以安装代理并将池许可证应用于远程数据中心的实例。在这种情况下，主站点和远程数据中心之间的通信是通过浮动 IP 地址进行的。

在 Citrix ADM 12.1 中，可以将实例配置为使用代理与位于不同数据中心的主要 Citrix ADM 进行通信。

> 注意
>
> 只有 Citrix ADM 高可用性部署才支持用于多站点部署的本地代理。

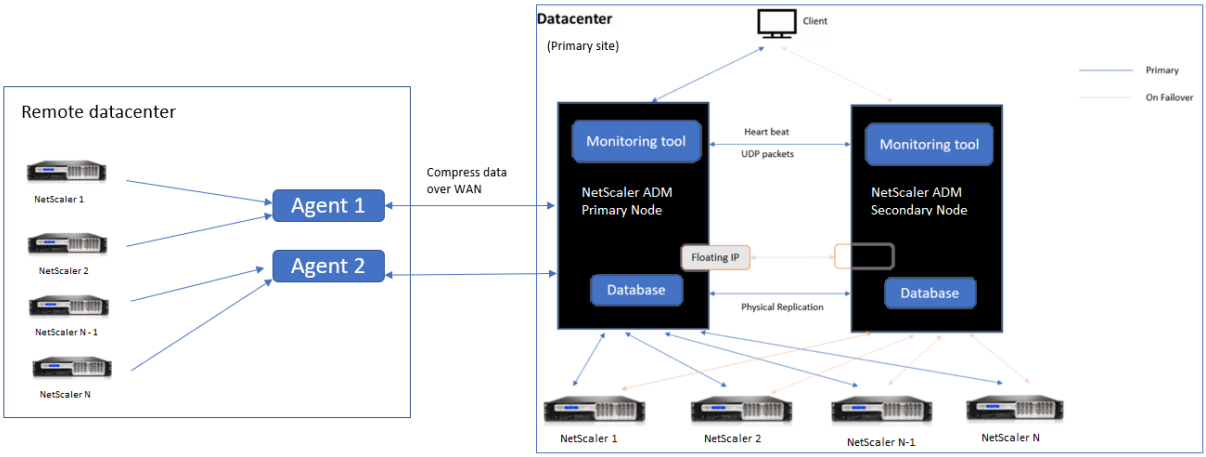
代理在不同数据中心的主 Citrix ADM 和发现的实例之间起到中介作用。以下是安装代理的好处：

- 这些实例配置为代理，以便将未处理的数据直接发送到代理，而不是主 Citrix ADM。代理执行第一级数据处理，然后将经过处理的数据以压缩格式发送到主 Citrix ADM 进行存储。
- 代理和实例位于同一个数据中心，以便更快地处理数据。
- 对代理进行群集可在代理故障转移时重新分配 Citrix ADC 实例。当站点中的一个代理出现故障时，来自 Citrix ADC 实例的流量将切换到同一站点中的另一个可用代理。

  > 注意
  >
  > 每个站点要安装的代理数取决于正在处理的流量。目前，Citrix 已验证每个站点有两个代理用于代理故障转移场景。Citrix 建议您在每个站点至少安装两个代理，以便在代理发生故障转移时流量流向另一个代理。

体系结构

下图显示了两个数据中心中的 Citrix ADC 实例以及使用基于多站点代理的体系结构的 Citrix ADM 高可用性部署。



主站点在高可用性配置中部署了 Citrix ADM 节点。主站点中的 Citrix ADC 实例直接向 Citrix ADM 注册。

在辅助站点中，代理部署并向主站点中的 Citrix ADM 服务器注册。这些代理在群集中工作，以便在发生代理故障转移时处理连续的流量。辅助站点中的 Citrix ADC 实例通过位于该站点内的代理向主 Citrix ADM 服务器注册。实例将数据直接发送到代理，而不是主 Citrix ADM。代理处理从实例接收到的数据，并以压缩格式将其发送到主 Citrix ADM。代理通过安全通道与 Citrix ADM 服务器通信，并压缩通过该通道发送的数据以提高带宽效率。

入门

- 在数据中心安装代理

  - 注册代理
  - 添加代理
- 添加 Citrix ADC 实例
  - 添加新实例
  - 更新现有实例

在数据中心安装代理

您可以安装和配置代理，以启用主 Citrix ADM 与另一个数据中心中的托管 Citrix ADC 实例之间的通信。

您可以在企业数据中心的以下虚拟机管理程序上安装代理：

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM 服务器

> 注意
>
> 只有 Citrix ADM 高可用性部署才支持用于多站点部署的本地代理。

在开始安装代理之前，请确保拥有 Hypervisor 必须为每个代理提供的所需虚拟计算资源。

组件	要求
RAM	8 GB 注意：Citrix 建议您将默认值增加到 32 GB 以提高性能。
虚拟 CPU	2 个 CPU 注意：Citrix 建议您将默认值增加到 8 个 CPU 以提高性能。
存储空间	30 GB
虚拟网络接口	1
吞吐量	1 Gbps

端口

出于通信目的，代理和 Citrix ADM 内部部署服务器之间必须打开以下端口。

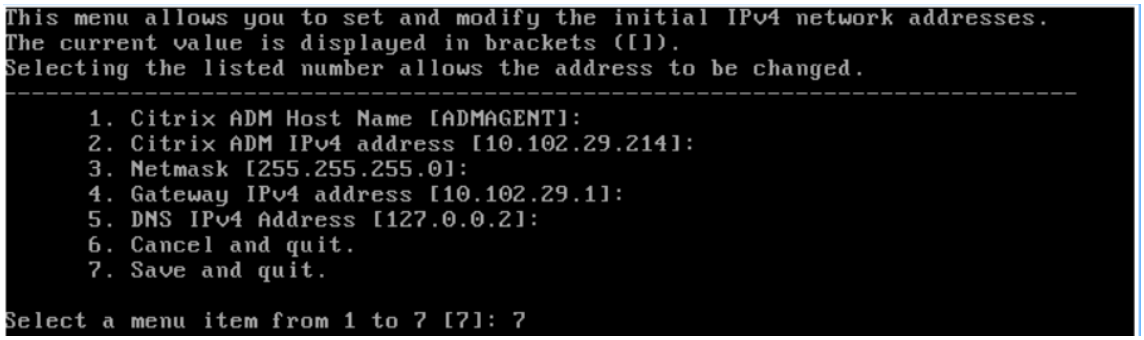
类型	端口	详细信息
TCP	8443, 7443, 443	用于代理与 Citrix ADM 内部部署服务器之间的出站和入站通信。

代理和 Citrix ADC 实例之间必须打开以下端口。

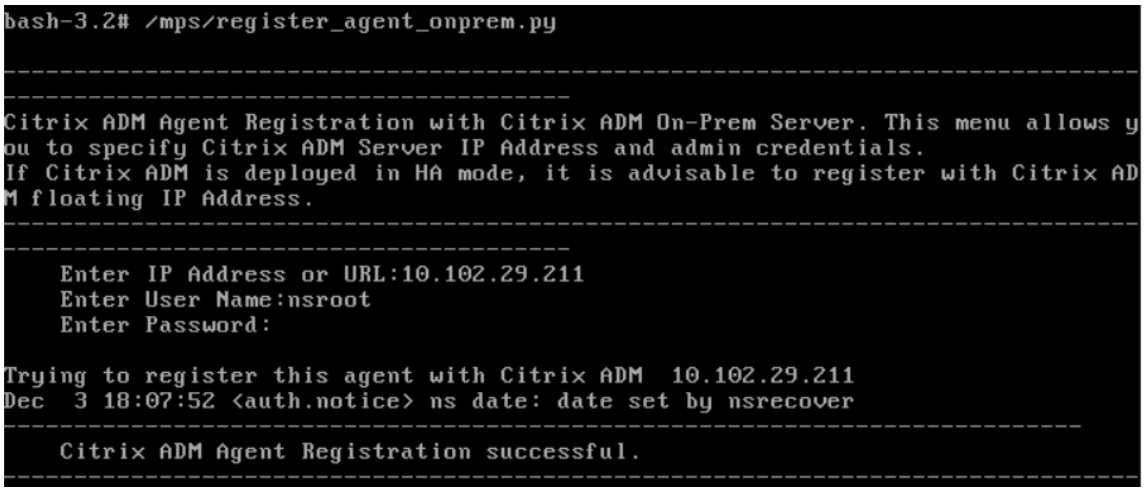
类型	端口	详细信息
TCP	80	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的 NITRO 通信。
TCP	22	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的 SSH 通信。用于以高可用性模式部署的 Citrix ADM 服务器之间的同步。
UDP	4739	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的 AppFlow。
ICMP	无保留的端口	检测在高可用性模式下部署的 Citrix ADM 和 Citrix ADC 实例、SD WAN 实例或辅助 Citrix ADM 服务器之间的网络可访问性。
SNMP	161, 162	将 SNMP 事件从 Citrix ADC 实例接收到代理。
Syslog	514	将系统日志消息从 Citrix ADC 或 Citrix SD-WAN 实例接收到代理。
TCP	5557	用于代理和 Citrix ADC 实例之间的 Logstream 通信。

注册代理

1. 使用从 Citrix 下载站点下载的代理映像文件，并将其导入到 Hypervisor 中。代理映像文件的命名模式如下所示：**MASAGENT-<HYPERVISOR>-<Version.no>**。例如：**MASAGENT-XEN-12.1-xy.xva**
2. 在控制台选项卡中，使用初始网络配置配置 Citrix ADM。
3. 输入 Citrix ADM 主机名、IPv4 地址和网关 IPv4 地址。选择选项 7 以保存并退出配置。



4. 注册成功后，控制台将提示登录。使用 *nsrecover/nsroot* 作为凭据。
5. 要注册代理，请输入 **/mps/register_agent_onprem.py**。将显示 Citrix ADM 代理注册凭据，如下图所示。
6. 输入 Citrix ADM 浮动 IP 地址和用户凭据。



注册成功后，代理将重新启动以完成安装过程。

代理重新启动后，访问 Citrix ADM GUI，从主菜单转到“网络”**>**“代理”页面以验证代理的状态。新添加的座席将显示为“启动”状态。

> 注意
>
> Citrix ADM 会显示代理的版本，并检查代理是否为最新版本。下载图标表示代理不是最新版本，需要升级。Citrix 建议您将代理版本升级到 Citrix ADM 版本。

将代理添加到站点

1. 选择代理，然后单击“连接站点”。
2. 在附加站点页面中，从列表中选择一个站点或使用加号 (+) 按钮创建一个新站点。
3. 单击“保存”。

> 注意
>
> - 默认情况下，所有新注册的代理都将添加到默认数据中心。
> - 请务必将代理与正确的站点相关联。如果出现代理故障，分配给它的 Citrix ADC 实例将自动切换到同一站点中的其他正常运行的代理。

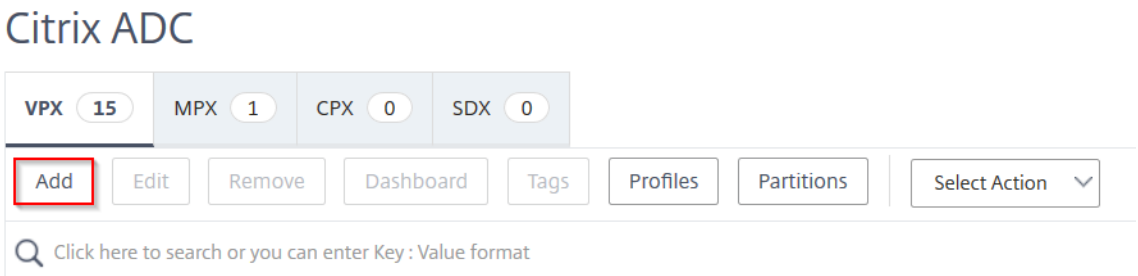
添加 **Citrix ADC** 实例

实例是您希望通过代理从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 或代理中：

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Citrix Secure Web Gateway
- Citrix SD-WAN WO

添加新实例

1. 导航到“网络”**>**“实例”，然后选择实例类型。例如，Citrix ADC。
2. 单击“添加”以添加新实例。

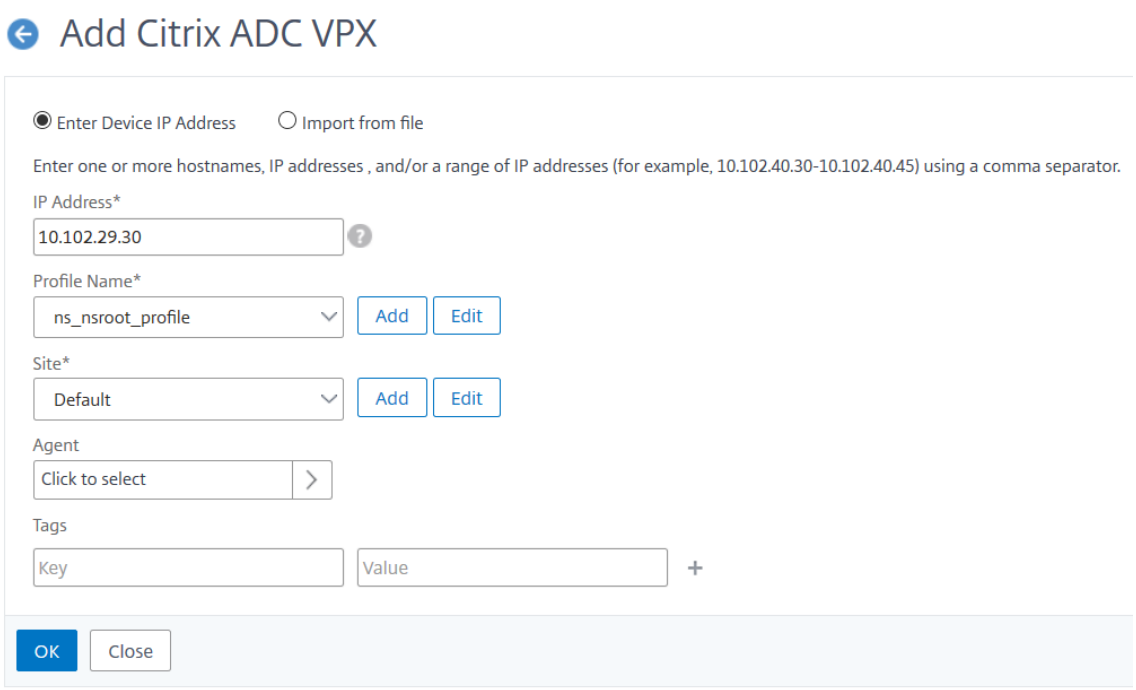


3. 选 中输入设备 **IP** 地址 并输入 IP 地址。
4. 从“配置文件名称”中，选择相应的实例配置文件，或单击 **+** 图表创建新的配置文件。

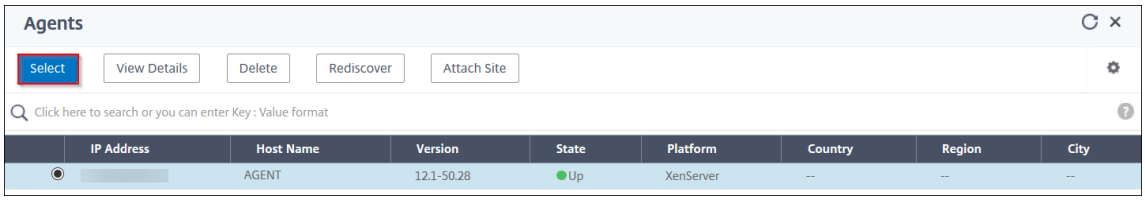
> 注意
>
> 对于每种实例类型，都有默认配置文件可用。例如，ns-root-profile 是 Citrix ADC 实例的默认配置文件。

5. 选择要与该实例关联的 站点。

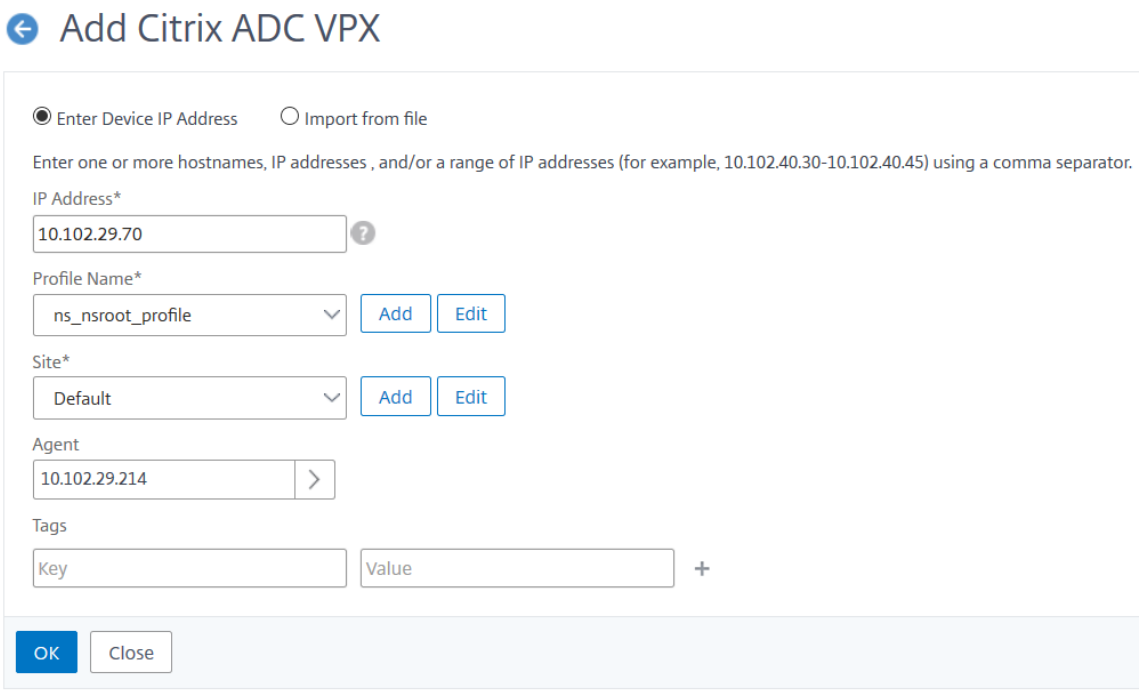
> 注意
>
> 根据所选站点，显示与该站点关联的代理列表。确保选择要与该实例关联的 站点。



6. 单击以选择代理。在代理 页面中，选择要与实例关联的代理，然后单击选择。



7. 在“添加 Citrix VPX”页面上，单击“确定”。



更新现有实例以将其连接到代理

如果已将实例添加到主 Citrix ADM 中，则可以通过编辑添加实例工作流程并选择代理将其附加到代理。

1. 导航到“网络”**>**“实例”，然后选择实例类型。例如，Citrix ADC。
2. 单击“编辑”按钮编辑现有实例。
3. 单击以选择代理。
4. 在“代理”页面中，选择要与实例关联的代理，然后单击“确定”。

> 注意
>
> 确保选择要与该实例关联的 站点。

访问实例的 **GUI** 以验证事件

添加实例并配置代理后，访问实例的 GUI 以检查陷阱目标是否已配置。

在 Citrix ADM 中，导航到“网络”**>**“实例”。在“实例”下，选择要访问的实例类型（例如 Citrix ADC VPX），然后单击特定实例的 IP 地址。

所选实例的 GUI 将显示在弹出窗口中。

默认情况下，代理被配置为实例上的陷阱目标。要进行确认，请登录实例的 GUI 并检查陷阱目的地。

> 重要
>
> 建议为远程数据中心中的 Citrix ADC 实例添加代理，但不是强制性的。
>
> 如果要将实例直接添加到主 MAS，请勿在添加实例时选择代理。

对代理进行群集

代理群集 一词指的是将连接到某个站点的代理进行逻辑分组的机制，这样，如果其中一个代理出现故障，向其发送流量的 Citrix ADC 实例会自动重新配置为开始向该组或站点中的其他运行状况良好的代理发送流量。

将代理群集在远程站点的好处是，如果一个代理出现故障，Citrix ADM 会检测到该代理，并隐含地将所有实例重新分配给该群集中的其他可用代理。

例如，我们有两个代理 10.106.1xx.2x 和 10.106.1xx.7x，它们在班加罗尔站点连接并投入运行，如下所示。

如果一个代理出现故障，Citrix ADM 将检测到它并将状态显示为关闭。

连接到该代理的实例会自动重新配置为使用来自同一群集的另一个代理作为陷阱目标、syslog 服务器等。

> 注意
>
> 重新配置实例时会有一些延迟。

将 **Citrix ADM** 单服务器部署迁移到高可用性部署

February 6, 2024

可以将您的 Citrix ADM 单服务器升级为由两台 Citrix ADM 服务器组成的高可用性部署。一对高可用性的 Citrix ADM 服务器处于主动-被动模式，并且两台服务器具有相同的配置。在这种类型的主动-被动部署中，一个 Citrix ADM 服务器配置为主节点，另一个配置为辅助节点。如果出于任何原因主节点出现故障，则辅助节点接管。

要将 Citrix ADM 单服务器迁移到高可用性对，您需要预置一个新的 Citrix ADM 服务器节点，将其配置为第二台 Citrix ADM 单服务器，并将两台 Citrix ADM 服务器作为高可用性对进行部署。

将 Citrix ADM 单服务器迁移到高可用模式涉及以下步骤：

1. 修改现有服务器节点
2. 预配第二个服务器节点
3. 以 HA 模式部署两个节点
4. 配置高可用性对

修改现有 **Citrix ADM** 服务器节点

要将 Citrix ADM 从单服务器迁移到高可用模式，必须将服务器节点的初始部署类型更改为高可用模式。

1. 在工作站或便携式计算机上，打开现有 Citrix ADM 服务器节点的主机。例如，假设您已将 IP 地址为 10.106.171.17 的 Citrix ADM 部署为独立服务器。
2. 登录到 Citrix ADM。默认凭据是 nsroot 和 nsroot。
3. 在 shell 提示符中，键入 **/mps/**部署类型**.py**，然后按 **Enter** 键。
4. 选择部署类型作为 Citrix ADM 服务器。如果不选择任何选项，默认情况下，它部署为服务器。

```
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. 部署控制台提示您选择服务器部署（作为独立部署）。键入 **No** 以确认部署为高可用性对。
6. 控制台提示选择（第一个服务器节点）。输入 **Yes**（是）确认节点为第一个服务器节点。
7. 控制台提示重新启动服务器。
8. 键入 **Yes** 以重新启动。

```
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
```

预配第二个服务器节点

必须在虚拟机管理程序上预配第二个服务器。使用在安装第一个服务器时使用的同一映像文件，或从 Citrix 下载站点获取相同版本的映像文件。

1. 将映像文件导入到 Hypervisor，然后从控制台选项卡配置初始网络配置选项，如以下屏幕中所述：


```
--------------------------------------------------------------------------------
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]:
```

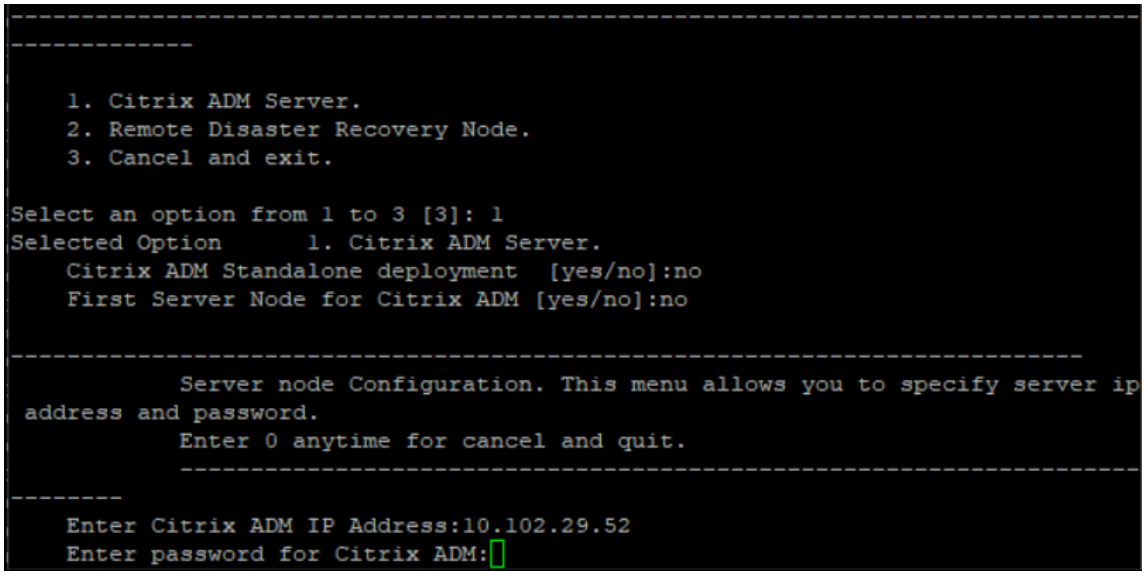
2. 指定所需的 IP 地址后，在 shell 提示符中键入 /mps/部署 _type.py，然后按 Enter 键。
3. 选择部署类型作为 **Citrix ADM** 服务器。
4. 部署控制台提示您选择服务器部署（作为独立部署）。键入 **No** 以确认部署为高可用性对。

```
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
```

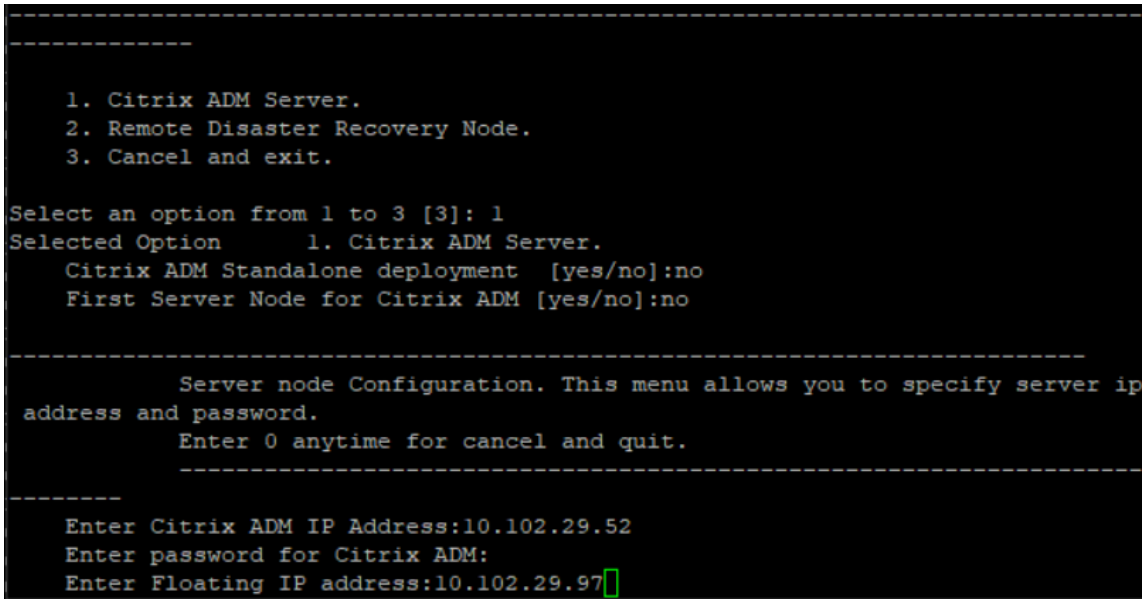
5. 控制台随后提示选择（第一个服务器节点）。键入 **No** 以确认该节点为第二个服务器节点。

```
--------------------------------------------------------------------------------
-------------
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. 输入第一台服务器的 IP 地址和密码。



7. 输入第一个节点的浮动 IP 地址。



8. 控制台提示您重新启动系统。输入“是”以重新启动。

在高可用性模式下部署两台服务器

要完成两个服务器节点作为高可用性对的安装过程，您必须从先前存在的 Citrix ADM 服务器节点的 GUI 中部署这些节点。部署两个服务器节点时，两个服务器之间即开始内部通信。

1. 在 Web 浏览器中，键入先前存在的 Citrix ADM 服务器节点的 IP 地址。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。

3. 在“系统”选项卡上，导航到“部署”，然后单击“部 署”。
4. 此时将显示一条确认消息。单击是。

> 注意
>
> 在高可用性下部署 Citrix ADM 后，您可以使用浮动 IP 访问主节点。从 12.1 版本开始，您无法访问辅助节点。

5. 尽管您在配置第二个服务器节点时输入了浮动 IP，但您可以在“系统”页面上选择更新 FIP。单击 **HA** 设置 > 为高可用性模式配置浮动 **IP** 地址。您可以查看之前配置的浮动 IP 地址。您可以输入新的 IP 地址，然后单击“确定”。

从 **NetScaler Insight Center** 迁移至 **Citrix ADM**

February 6, 2024

现在，您可以将 NetScaler Insight Center 部署迁移到 Citrix ADM，而不会丢失现有配置、设置或数据。使用 Citrix ADM，您不仅可以查看与应用关联的 NetScaler 实例生成的各种分析，还可以通过单个统一的控制台管理、监视整个全球应用交付基础架构并对其进行故障排除。

> 注意
>
> 当前仅 NetScaler Insight Center 独立实例支持迁移。

必备条件

在将 NetScaler Insight Center 虚拟设备迁移到 Citrix ADM 之前，请验证是否满足以下要求：

- 安装了 NetScaler Insight Center 11.1 Build 47.14 或更高版本。
- 您已下载了 Citrix ADM 12.0 版本 57.24 .tgz 映像文件。

> 注
>
> 意您需要安装 Citrix ADM 12.0 版本 57.24，然后升级到最新的 Citrix ADM 12.1 版本。有关详细信息，请参阅升级。

- 您已下载了 Citrix ADM 12.1 最新版本的.tgz 映像文件。

硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	120 GB 注意 Citrix 建议您使用 **500 GB** 以获得更好的性能。此外，Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序要求	
Citrix Hypervisor	6.2, 6.5
VMWare ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu、Fedora

安装程序

要将 **NetScaler Insight Center** 迁移到 **Citrix ADM**，请执行以下操作：

1. 登录 NetScaler Insight Center 的 shell 提示窗口。
2. 将 Citrix ADM 12.0 版本 57.24 下载到 */var/mps/mps_* 映像 文件夹中。
3. 通过使用焦油 **-zxvf** 构建**-mas-12.0-57.24.tgz** 命令解除 **TGZ** 文件。

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. 使用安装 Citrix ADM 。**/**安装 **mas** 命令。

```
bash-3.2# ./installmas
```

5. 安装 Citrix ADM 12.0 版本 57.24 后，需要通过执行上述步骤升级到最新的 Citrix ADM 12.1 版本。

迁移后，在 NetScaler Insight Center Insight Center 清单中发现的所有 NetScaler 实例 都会显示在 Citrix ADM 的“网络”>“实例”部分中。但是，第一次时，需要手动轮询发现的设备上托管的虚拟服务器。

> 注意
>
> 在 Citrix ADM 中，默认情况下，管理和监视在发现的 NetScaler 实例中创建的 30 个虚拟服务器无需支付许可费用。要监视和管理 30 个以上的虚拟服务器，请安装所需的 MAS 许可证。有关更多详细信息，请参阅Citrix ADM 许可。

将 **Command Center** 配置迁移到 **Citrix ADM**

February 6, 2024

现在，您可以将 Command Center 配置迁移到 Citrix Application Delivery Management (ADM)，而不会丢失 Command Center 部署和 Citrix ADM 部署的现有配置、设置或数据。迁移过程完成后，您可以在 Citrix ADM 中查看迁移的 Command Center 配置。

需要注意的事项

- 以下部署支持将 Command Center 配置迁移到 Citrix ADM：
  - Command Center 独立部署到 Citrix ADM 独立部署或 Citrix ADM 高可用性部署。
  - Command Center 高可用性适用于 Citrix ADM 独立部署或 Citrix ADM 高可用性部署。

  > 注意：
  >
  > 在将 Command Center 独立或高可用性部署迁移到 Citrix ADM 独立或高可用性部署时，您必须仅使用 Command Center 和 Citrix ADM 高可用性部署的主节点 IP 地址。
- 您可以在相同或不同的 Citrix ADM 部署上多次运行 Command Center 工具：
  - 每当您首次为同一 Citrix ADM 运行 Command Center 工具后，对于已经迁移并存在于 Citrix ADM 中的配置，日志都会显示为失败。
  - 如果在 Command Center 中从早些时候运行该工具到现在为同一 Citrix ADM 添加了任何新配置，则除新的自定义任务之外的所有此类配置都将迁移到 Citrix ADM。
- Citrix ADM、Citrix ADC SDX 和 Citrix SD-WAN WO 设备支持将 Command Center 配置迁移到 Citrix ADM。
- Command Center 和 Citrix ADM 之间的所有通信都在 HTTPS 连接上进行。
- 强烈建议在迁移 Command Center 配置之前备份 Citrix ADM 的现有数据。
- Command Center 迁移完成后，会在 Citrix ADM 中自动发现 Citrix ADC 的管理分区。

限制

以下 Command Center 配置不会从 Command Center 设备迁移到 Citrix ADM：

- 设备备份配置文件
- SD-WAN WO 设备配置文件中的超时详细信息
- 不会迁移事件和警报触发器下的以下详细信息：
  - 运行命令操作的中止详细信息
  - 运行任务详细信息
  - 不会迁移所有参数（严重性/类别/实例/失败对象）为空的触发器
  - 如果选择了实例的 HA 群集、主要和辅助状态，则不会迁移具有处于这三种状态的实例的触发器
- 不会迁移无说明的自定义任务
- 事件严重性设置
- 事件规则计划详细信息
- Syslog 阻止过滤器
- 配置任务详细信息
- 审核模板
- 无设备的审核策略
- 审核策略计划详细信息
- 组 RBAC 授权的范围设置
- 数据库监视和管理设置
- 性能自定义报告
- 性能阈值
- 故障/syslog/报告/实体监视的自定义视图
- AppFirewall 和 NS 网关报告及其计划详细信息
- SD-WAN WO 自动配置详细信息
- 高可用性设置
- 计划的系统备份设置
- 数据库重试设置
- Syslog 清除计划时间
- 所有统计数据，例如，所有模块的 syslog、事件和审核日志。

必备条件

在将 Command Center 配置迁移到 Citrix ADM 之前，请确保满足以下必备条件：

- 您运行的是 Command Center 5.2 Build 48.2 或更高版本。
- 您已经安装并配置了 Citrix ADM 版本 12.0 版本 51.24 或更高版本。
- 仅由管理用户运行 Command Center 配置迁移。
- 要成功迁移自定义任务，必须在 Command Center 中填写说明字段。
- Command Center 和 Citrix ADM 之间的通信基于 NITRO。必须在 Command Center 和 Citrix ADM 上配置并打开必要的 SSL（安全套接字层）和 TLS（传输层安全）协议设置，才能进行 NITRO 通信。

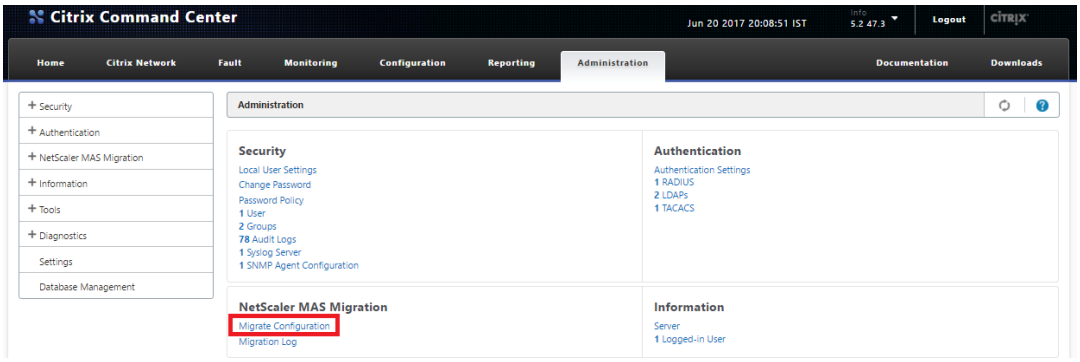
> 注意
>
> 如果您使用的是 Command Center 版本早于 5.2 版本 48.2，则必须将 Command Center 版本升级到 5.2 版本 48.2，然后将 Command Center 配置迁移到 Citrix ADM。有关升级 Command Center 设备的详细信息，请参阅 升级 Command Center。

迁移配置

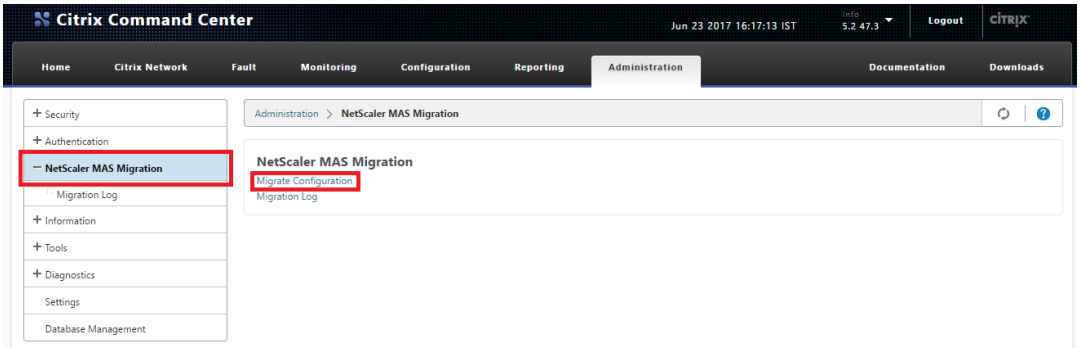
要将 Command Center 配置迁移到 Citrix ADM，您需要 Command Center 设备的 IP 地址和管理员凭据。

要将 **Command Center** 配置迁移到 **Citrix ADM**，请执行以下操作：

1. 在 Web 浏览器中，键入 Command Center 设备的 IP 地址。
2. 在“用户名”和“密码”字段中，键入管理员凭据并登录。
3. 成功登录后，在显示的屏幕上，选择“管 理”选项卡，然后执行以下操作之一：
   - 在右侧窗格的 **Citrix ADM** 迁移下，选择 迁移配置，如下图所示。

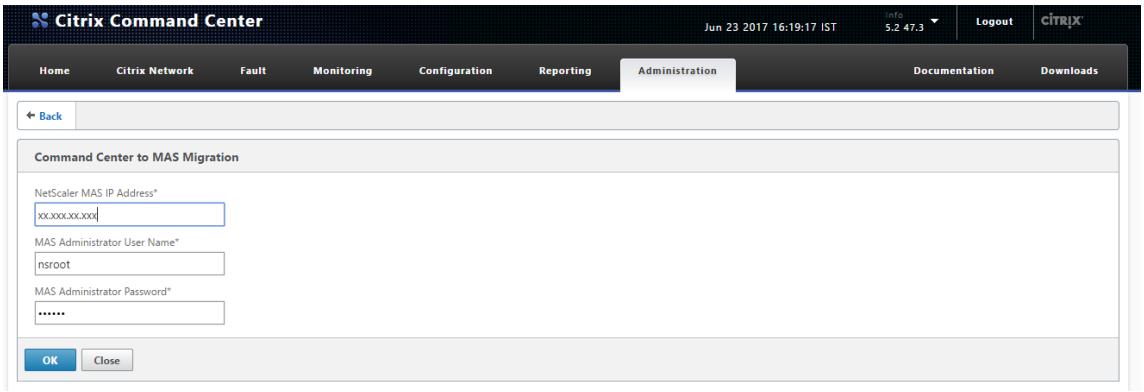


   - 在左窗格中，选择 **Citrix ADM** 迁移，然后单击“迁移配置”，如下图所示。

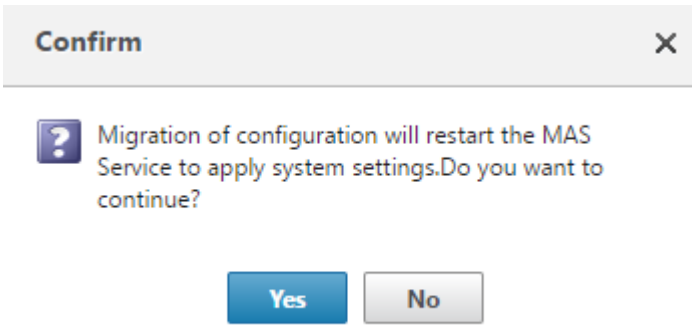


4. 在 **Command Center** 到 **MAS** 迁移对话框中，输入 Citrix ADM 服务器的 IP 地址和管理员凭据，然后单击“确定”。Command Center from the time the tool was run earlier to no

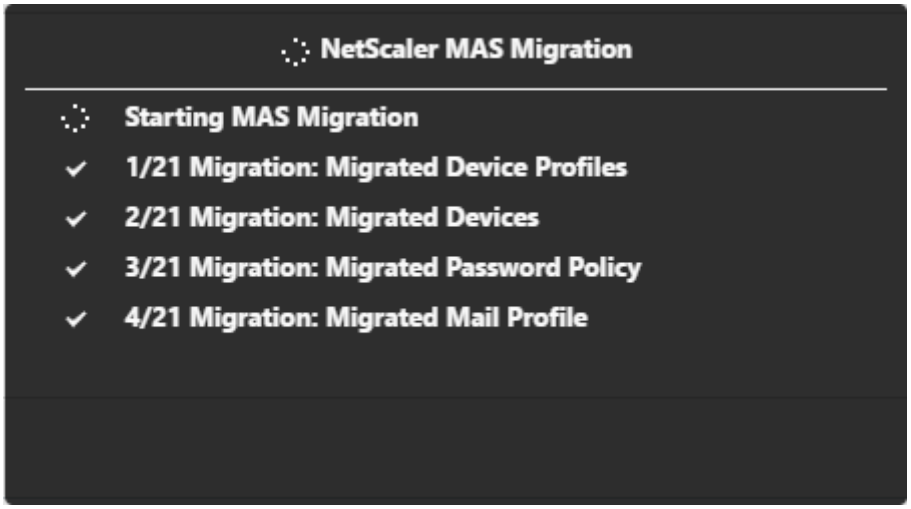
> 注意：
>
> 如果是 Citrix ADM 高可用性部署，请输入主节点 IP 地址。



5. 在确认提示时，单击 是。



屏幕上将报告迁移任务的进度。



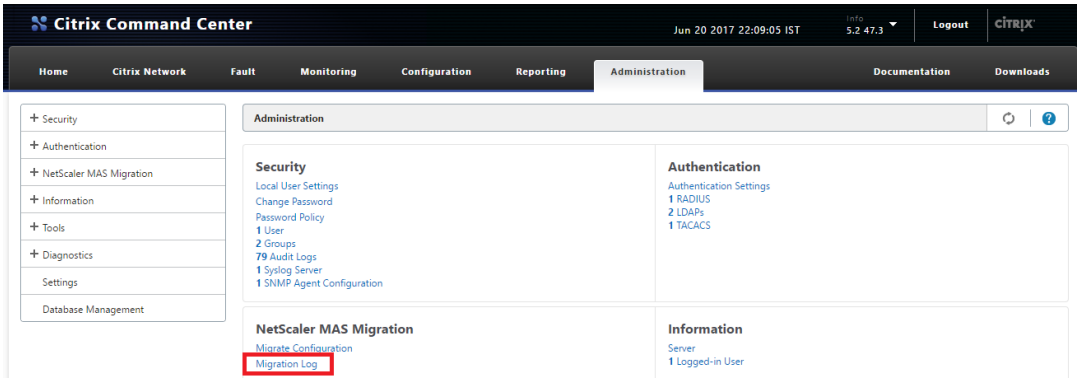
迁移配置 操作将 Citrix ADM 部署的详细信息及其管理员凭据作为输入。然后，迁移配置操作将 Command Center 部署的配置迁移到 Citrix ADM 部署。

任务完成后，您可以从 Command Center 迁移日志和 Citrix ADM 数据中验证迁移的 Command Center 配置。

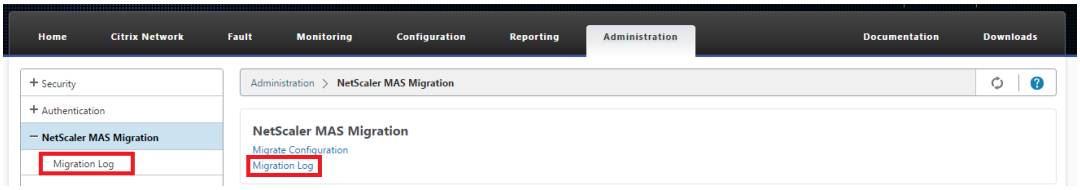
使用 **Command Center** 迁移日志确认迁移

1. 在 Command Center GUI 中的“管理”选项卡上，执行以下操作之一：

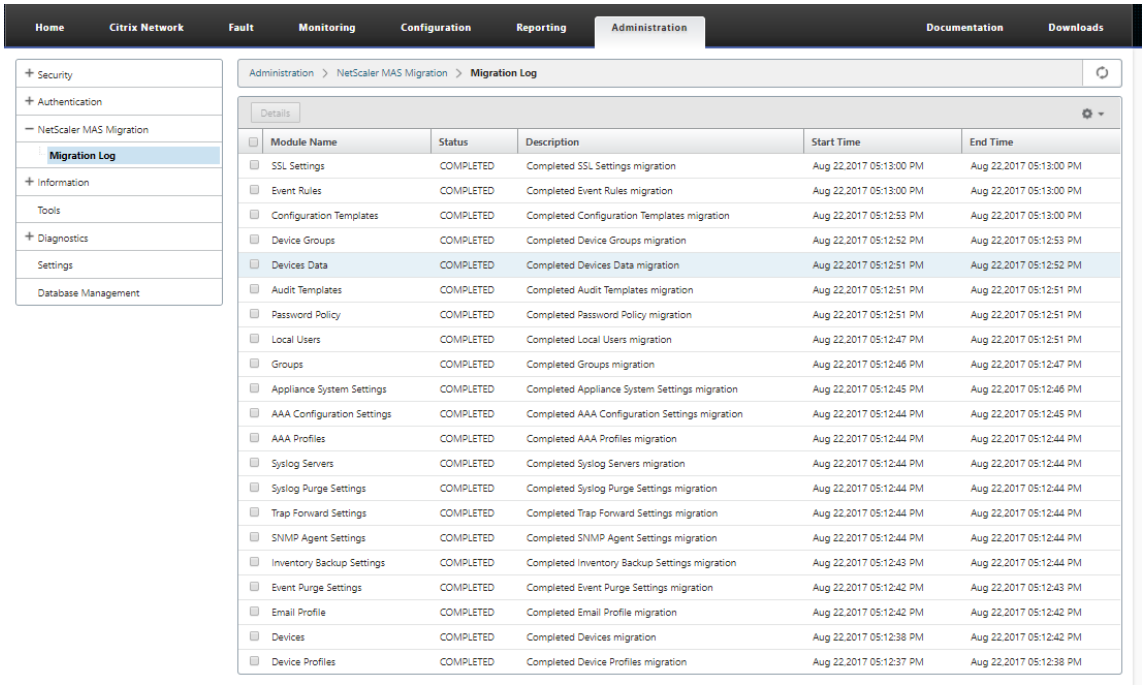
   - 在右侧窗格的 **Citrix ADM** 迁移下，单击“迁移日志”。

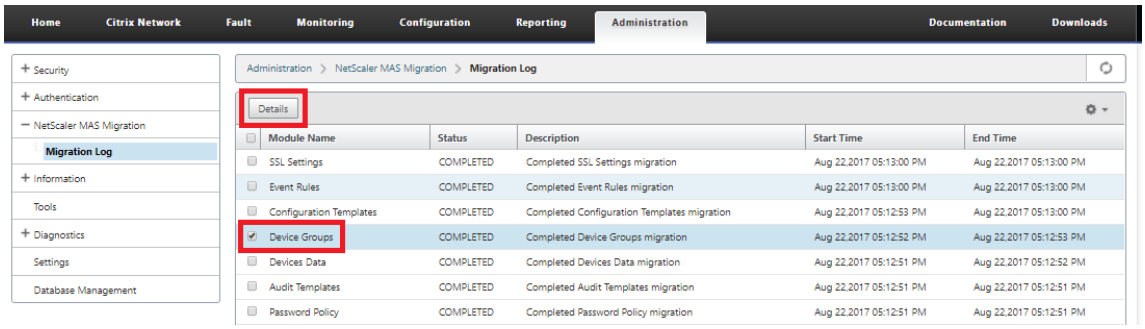
   - 在左窗格中，选择 **Citrix ADM** 迁移，然后单击 “迁移日志”。

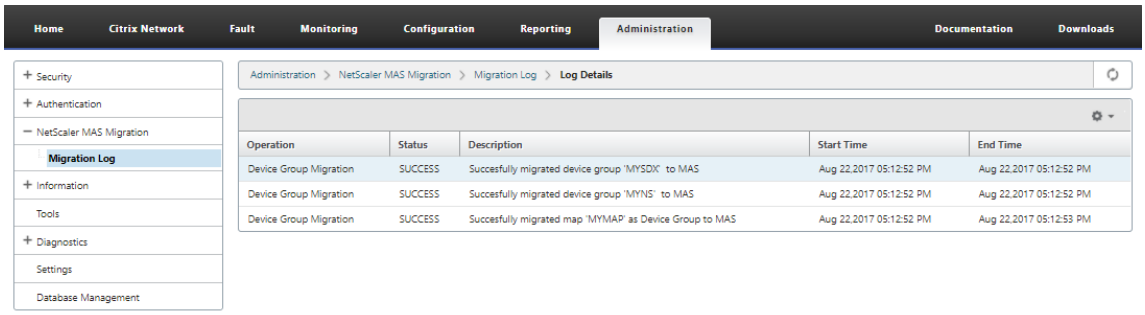
2. 查看迁移日志列表。



3. 要显示更多详细信息，请选择 模块名称，或者要显示特定模块的详细信息，请选择该模块，然后单击详 细信息。



4. 以下示例显示了某个选定模块的日志详细信息。



使用 **Citrix ADM** 验证迁移

在迁移过程中，Command Center 配置将迁移到 Citrix ADM，并在 Citrix ADM GUI 中显示为 Citrix ADM 配置。

迁移过程完成后，Citrix ADM 服务器重新启动，可能会暂时停机。当 Citrix ADM 服务器启动并运行时，通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问 Citrix ADM GUI。

下表显示了迁移配置的 Citrix ADM 术语与 Command Center 中使用的术语的对应关系。

Command Center 术语	Citrix ADM 术语
设备配置文件	实例配置文件
设备及其状态（例如托管/未托管）	实例及其状态（例如托管/未托管）
设备批注	实例批注
设备组	实例组
地图	实例组
事件和警报触发器	事件规则
内置和自定义任务命令	创建作业编辑器下的配置模板
定期审核策略	审核模板
密码策略	密码策略
用户（仅限本地用户）	系统用户
组 *	系统组
身份验证配置文件和身份验证设置	身份验证配置文件和身份验证配置
电子邮件设置	电子邮件服务器/电子邮件通讯组列表
Syslog 服务器	Syslog 服务器
SSL 设置	SSL 设置
SNMP 代理配置	SNMP 管理器
陷阱转发设置	陷阱设置
事件清除设置	事件删除设置
清单设置	实例备份设置
Syslog 清除设置	Syslog 删除设置
设备网络设置，例如 DNS、NTP 和时区	Citrix ADM 网络设置，例如 DNS、NTP 和时区

* 在 Citrix ADM Command Center 具有所有权限的组将迁移为具有“管理员”角色的组。在 Citrix ADM 中，所有其他 Command Center 组均作为具有“只读”角色的组进行迁移。

将 **Citrix ADM** 与 **Citrix Director** 集成

February 6, 2024

Director 与 Citrix ADM 集成，用于网络分析和性能管理。

- 网络分析从 Citrix ADM 获取 HDX Insight 报告，并提供网络的应用程序和桌面视图。通过此功能，Director 对部署中的 ICA 通信提供高级分析视图。
- 性能管理提供历史保留和趋势报告。通过历史数据保留与实时评估，可以创建趋势报告，其中包括容量趋势和运行状况趋势。

将 Citrix ADM 与 Director 集成后，HDX Insight 报告会在 Director 中为您提供以下信息：

- “Trends”（趋势）页面中的“Network”（网络）选项卡显示对部署中的应用程序、桌面和用户产生的延迟和带宽影响。
- 用户详细信息页可以显示特定于某个特殊用户会话的延迟和带宽信息。

必备条件

HDX Insight 到 **Citrix ADM** 迁移的硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8
存储空间	500 GB. Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

软件要求

在迁移到 Citrix ADM 虚拟设备之前，请验证是否满足以下要求：

- 已安装 Director 1811 版
- 已安装 NetScaler HDX Insight 10.1 版或更高版本
- HDX Insight 和 Citrix ADM 支持 Citrix VDA 版本 7.0 及更高版本

- Citrix Virtual Apps and Desktops 7.0 版及更高版本支持 Citrix Workspace
- 请确保有 MAC Citrix Receiver for Mac 11.8 版及更高版本以及 Windows Citrix Receiver for Windows 14.0 版和更高版本，以显示准确的 ICA RTT 指标
- 安装了 Citrix ADM 版本 11.0 及更高版本。有关如何安装 Citrix ADM 的更多信息，请参阅 部署 Citrix ADM。

限制

- 此功能的可用性取决于组织的许可证和管理员权限。
- ICA 会话的往返程时间 (RTT) 可正确显示 Citrix Receiver for Windows 3.4 或更高版本以及 Citrix Receiver for Mac 11.8 或更高版本的数据。对于早期版本的 Receiver，数据无法正确显示。
- 在“Trends”（趋势）视图中，不会针对 VDA 7 之前的版本收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。
- 对于已经有存储空间低于 500 GB 的外部硬盘的部署，不能添加其他硬盘。

> 注意
>
> - 有关 Director 的更多信息以及将 Citrix ADM 与 Director 集成的步骤，请参阅http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director.html。
> - 有关 HDX Insight 的详细信息，请参阅http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html。

将其他磁盘附加到 **Citrix ADM**

February 6, 2024

Citrix Application Delivery Management (ADM) 存储需求根据您的 Citrix ADM 大小估计确定。默认情况下，Citrix ADM 为您提供 120 GB 的存储容量。如果存储数据需要超过 120 GB，则可以附加一个额外的磁盘。

> 注意
>
> - 在初始部署 Citrix ADM 时，估计存储需求并将其他磁盘连接到服务器。
> - 对于 Citrix ADM 单服务器部署，除了默认磁盘之外，您只能将一个磁盘连接到服务器。
> - 对于 Citrix ADM 高可用性部署，必须向每个节点附加一个附加磁盘。两个磁盘的大小必须相同。
> - 如果之前连接了容量较低的外部磁盘，则必须先删除该磁盘，然后再连接新磁盘。

> - 您可以附加容量大于 2 TB 的额外磁盘。如有必要，磁盘的大小也可以小于 2 TB。
> - Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。

本文档介绍了有关附加新磁盘、创建分区和调整其他磁盘大小的以下方案：

1. 附加一个新的磁盘
2. 启动磁盘分区工具
3. 在新的附加磁盘中创建分区
4. 调整现有附加磁盘的大小
5. 删除附加磁盘上的分区

在独立的 **Citrix ADM** 中附加一个附加磁盘

执行以下步骤将磁盘连接到虚拟机：

1. 关闭 Citrix ADM 虚拟机。
2. 在 Hypervisor 中，将所需磁盘大小的附加磁盘连接到 Citrix ADM 虚拟机。

   新连接的较大磁盘存储数据库数据和 Citrix ADM 日志文件。现有的 120 GB 默认磁盘现在用于存储核心文件、操作系统日志文件等。
3. 启动 Citrix ADM 虚拟机。

Citrix ADM 磁盘分区工具

Citrix ADM 现在提供了 **Citrix ADM** 磁盘分区工具，这是一种新的命令行工具。此工具的功能详细说明如下：

1. 使用该工具，您可以在新添加的附加磁盘中创建分区。
2. 您还可以使用此工具调整现有附加磁盘的大小。但现有的外部磁盘不应大于 2 TB。

   > 注意
   >
   > - 不可能在不丢失数据的情况下调整现有磁盘的大小超过 2 TB。这是由于平台上的已知限制。
   > - 要创建大于 2 TB 的存储容量，必须删除现有分区并使用此新工具创建分区。
3. 使用此新工具，您可以在磁盘上显式执行任何分区操作。该工具为您提供了对磁盘和相关数据的清晰可见性和控制权。

   > 注意：
   >
   > 您只能在已连接到 Citrix ADM 服务器的其他磁盘上使用此工具。使用此工具无法在主（默认）120 GB 磁

> 盘中创建分区。

启动磁盘分区工具

1. 使用 SSH 客户端（例如 PuTTY）打开与 Citrix ADM 的 SSH 连接。
2. 使用管理员凭据登录到 Citrix ADM。
3. 切换到 shell 提示符并键入：

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

```
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):
```

> 注意
>
> 对于高可用性部署中的 Citrix ADM，您必须在两个节点中启动该工具，然后在将磁盘附加到相应的虚拟机后创建分区或调整分区大小。

在新的附加磁盘中创建分区

每当添加新的辅助磁盘时，**create** 命令用于创建分区。使用“remove”命令删除现有分区后，也可以使用此命令在现有辅助磁盘上创建分区。

```
(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.
```

> ** 注
>
> 意：** 使用磁盘分区工具创建分区时，没有 2 TB 的大小限制。该工具可以创建大于 2 TB 的分区。在对磁盘进行分区时，会自动添加大小为 32 GB 的交换分区。然后，主分区将使用磁盘上的所有剩余空间。

执行命令后，将创建 GUID 分区表 (GPT) 分区方案。此外，还会创建一个 32 GB 的交换分区和数据分区来使用其余空间。然后在主分区上创建一个新的文件系统。

> 注意
>
> 此过程可能需要几秒钟，并且不能中断该过程。


```
(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...
```

创建命令完成后，虚拟机将自动重新启动，以便装载新分区。

```
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
```

重新启动后，新分区以 /var/mps 挂载。

```
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
```

添加的交换分区在“create”命令的输出中显示为交换空间。

```
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
```

> 注意
>
> 创建分区后，该工具将重新启动虚拟机。

调整现有附加磁盘中的分区大小

您可以使用 **resize** 命令调整连接的（辅助）磁盘的大小。您可以调整具有主引导记录 (MBR) 或 GPT 方案的磁盘的大小。磁盘的大小应小于 2 TB，最大 2 TB。

> 注意
>
> - “调整大小”命令旨在在不丢失任何现有数据的情况下运行。但是 Citrix 建议您在尝试调整大小之前将此磁盘中的关键数据备份到外部存储。在调整大小操作期间磁盘数据可能损坏的情况下，数据备份非常有用。
> - 调整分区大小时，请确保以 100 GB 空间为增量增加磁盘空间。这种增量增加可确保您不必更频繁地调整大小。

```
(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.
```

“resize”命令会检查所有前提条件，如果满足所有前提条件并在您同意调整大小后继续执行。它会停止访问磁盘的进程，其中包括 Citrix ADM 子系统、PostgreSQL 数据库进程和 Citrix ADM 监视器进程。进程停止后，将卸载磁盘，以便为调整大小做好准备。调整大小是通过扩展分区以占用全部可用空间，然后扩大文件系统来完成的。如果磁盘上存在交换分区，则会在调整大小后将其删除并在磁盘末尾重新创建。本文档的创建命令部分讨论了交换分区。

> 注意
>
> “不断增长的文件系统”过程可能需要一些时间才能完成，并注意不要在进程中中断该过程。调整分区大小后，该工具将重新启动虚拟机。

```
(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...
```


调整大小过程中的所有中间步骤（停止应用程序、调整磁盘大小、增加文件系统）都显示在控制台上。进程完成后，将看到以下消息。

```
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
```

重新启动后，可以使用“df”命令观察到大小的增加。以下是增加大小后的前后的详细信息：

```
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
```

删除其他磁盘中的分区

辅助磁盘上的现有分区最多可以调整为 2 TB 的大小。这是由于分区存在已知限制。如果需要大于 2 TB 的磁盘，请使用磁盘分区工具连接新磁盘并对其进行分区。您还可以使用 remove 命令 删除 现有分区，然后创建一个分区。

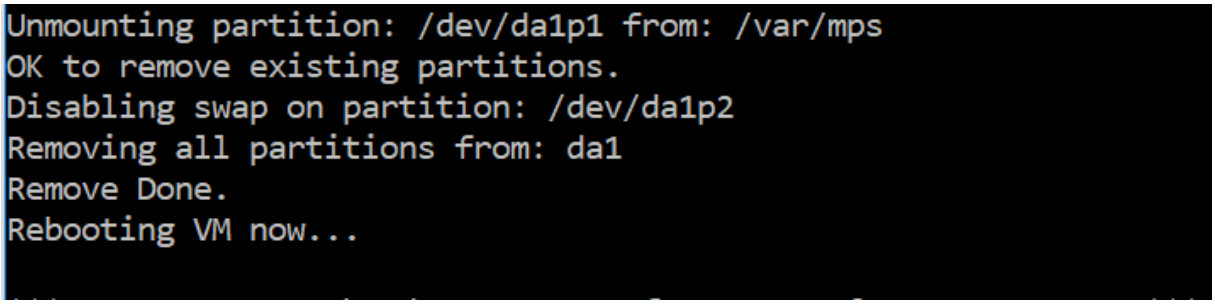
> 注意：
>
> 移除现有分区将删除所有现有数据。因此，在使用此命令之前，任何关键数据都必须备份到外部存储。

```
(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.
```

运行 “remove” 命令要求您进行确认，一旦确认，它将停止使用辅助磁盘的所有进程（例如 ADM 子系统、PostgreSQL 进程和 ADM 监视器）。如果交换分区存在并且在分区上启用了交换，则交换将被禁用。

```
(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
```

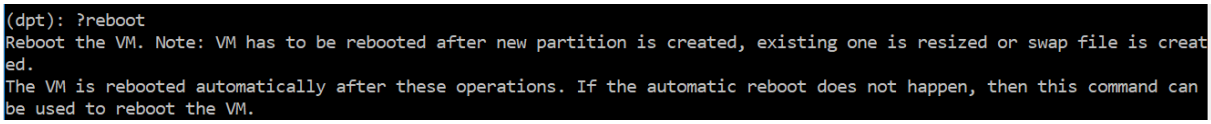
键入“y”时，该命令将卸载磁盘并删除磁盘上的所有分区。



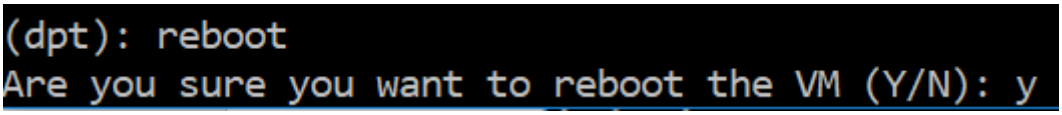
> 注意
>
> 移除分区后，该工具将重新启动虚拟机。

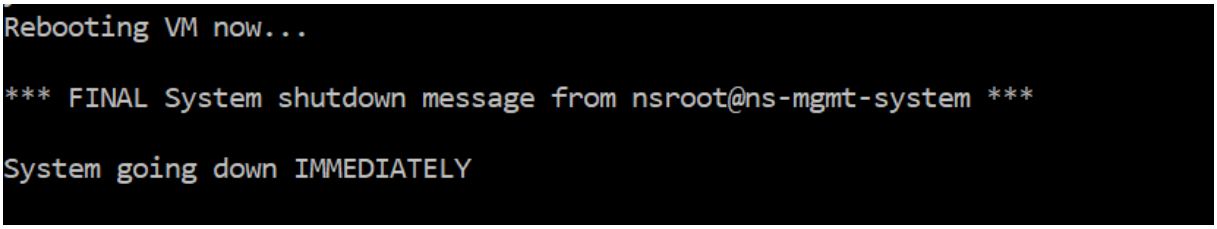
重新启动虚拟机

创建分区或调整分区大小后，或者创建交换文件时，请重新启动虚拟机。这些更改只有在重新启动后才会生效。为此，工具中提供了 重新启动 命令。



系统会提示您进行确认，一旦确认，它将停止所有进程（例如 ADM 子系统、PostgreSQL 进程和 ADM 监视器）。然后重新启动虚拟机。





创建磁盘数据的备份文件

以下是在调整分区大小或删除分区之前备份 Citrix ADM 数据时应遵循的步骤。

> 注意：
>
> 创建备份文件需要磁盘空间。Citrix 建议您在执行备份命令之前确保有足够的可用磁盘空间（50% 或更多）。

1. 停止 ADM。

```
/mps/masd stop
<!--NeedCopy-->
```


2. 停止 PostgreSQL。

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. 停止 ADM 监视器。

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. 创建压缩程序。

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> ** 注
>
> 意 ** 此操作需要时间，具体取决于要备份的数据的大小。

5. 生成校验和。

```
md5 mps_backup.tgz > mps_backup_checksum
<!--NeedCopy-->
```

6. 远程复制程序包和校验和。

```
scp
<!--NeedCopy-->
```

7. 验证复制的程序包是否正确。生成传输文件的校验和，并与源校验和进行比较。

8. 从 ADM 虚拟机中移除压缩包。

```
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

其他命令

除了前面列出的命令外，您还可以在工具中使用以下命令：

帮助命令：

要列出支持的命令，请键入 **help** 或 **?** 然后按回车键。要获得每个命令的进一步帮助，请按下 帮助 或 **?** 后跟命令名称，然后按 Enter 键。


```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

信息命令：

info 命令提供有关附加辅助磁盘的信息（如果该磁盘存在）。该命令提供设备名称、分区方案、人类可读形式的大小以及磁盘块的数量。该方案可以是 MBR 或 GPT。MBR 方案表示磁盘已使用早期版本的 Citrix ADM 版本进行分区。基于 MBR/GPT 的分区可以调整大小，但不能超过 2 TB。GPT 分区方案意味着磁盘是使用 Citrix ADM 12.1 或更高版本进行分区的。

> 注意
>
> GPT 分区在创建时可以大于 2 TB。但是，在创建具有较小大小的磁盘后，无法将磁盘大小调整为大于 2 TB 的大小。这是平台的已知限制。

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

创建交换文件命令：

Citrix ADM 主磁盘上的默认交换分区为 4 GB，因此默认交换空间为 4 GB。对于 Citrix ADM 的默认内存配置（2 GB），此交换空间已足够。但是，使用更高内存配置运行 Citrix ADM 时，需要在磁盘上分配更多的交换空间。

> 注意
>
> 交换分区通常是在操作系统安装过程中在硬盘驱动器 (HDD) 上创建的专用分区。这样的分区也称为交换空间。交换分区用于模拟额外主内存的虚拟内存。

默认情况下，在早期版本的 Citrix ADM 中添加的辅助磁盘没有创建交换分区。“create_swapfile”命令适用于使用较旧 Citrix ADM 版本创建的没有交换分区的辅助磁盘。命令会检查以下内容：

- 存在辅助磁盘
- 正在装入的磁盘
- 磁盘的大小（至少 500 GB）
- 交换文件的存在

“create_swapfile”命令仅在内存大于或等于 16 GB 时才有用，而在内存不足时不起作用。因此，此命令还会在继续创建交换文件之前检查内存。

```
(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.
```

如果满足所有条件，并且用户同意继续操作，则会在辅助磁盘上创建一个 32 GB 的交换文件。交换文件创建过程需要几分钟才能完成，请注意不要在创建过程中中断该过程。成功完成后，将重新启动以使交换文件生效。

```
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.
```

重新启动后，可以使用 top 命令观察到交换量的增加。

```
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
```

退出命令：

要退出工具，请键入 exit 并按 **Enter** 键。

```
(dpt): exit
bash-3.2#
```

将其他磁盘连接到部署在高可用性中的 Citrix ADM

让我们考虑一种情况，即您已在没有任何辅助磁盘的高可用性设置中配置了一对 Citrix ADM 服务器。另外，让我们假设您添加了两个或更多的 Citrix ADC 实例，检查并确保所有进程都在运行。您可能希望在此设置中向虚拟机添加辅助磁盘。在高可用性设置中，您必须向两个节点添加其他磁盘，如以下任务中所述：

1. 假设 Citrix ADM 节点名称是“adm_primary”和“adm_Secondiard”。
2. 首先，在 ADM_Secondary 上运行分区工具，然后添加辅助磁盘。添加磁盘后，虚拟机将重新启动。
3. 在 ADM_Secondary 重新启动后将其关闭。
4. 现在在 ADM_Primary 上运行分区工具并添加辅助磁盘。添加磁盘后，虚拟机将重新启动。

   确保向两个节点添加容量相似的磁盘。例如，如果向主节点添加容量为 500 GB 的磁盘，则还要向辅助节点添加容量为 500 GB 的磁盘。
5. ADM_Primary 重新启动后，请检查它是否为主节点。
6. 现在启动 ADM_Secondary 节点。确保它已作为辅助节点启动，并且数据库已同步。
7. 确认所有数据仍然存在。

执行以下步骤以增加两个节点上的 **RAM** 容量：

1. 关闭 ADM_ 次级并根据需要增加 RAM 大小。不要重新启动节点。
2. 关闭 ADM_ 主要内存并根据需要增加内存大小。

   确保在两个节点上均等地增加 RAM 大小。例如，如果将主节点上的 RAM 大小增加到 16 GB，也可以在辅助节点上执行相同的操作。
3. 重新启动 ADM_Primary。
4. 在 ADM_Primary 重新启动后，请检查它是否为主节点。
5. 现在启动 ADM_Secondary 节点。重新启动后，请确保它已作为辅助数据库启动，并且数据库同步工作正常。
6. 现在确认所有数据仍然存在。

> 注意：
>
> 添加辅助磁盘后，主节点需要一些时间才能启动。此外，向两个节点添加辅助磁盘和增加 RAM 容量的整个过程都需要两个节点关闭一段时间。在规划此维护活动时，请考虑这种停机时间。

配置

February 6, 2024

只能使用图形用户界面 (GUI) 访问 Citrix ADM 服务器。您必须访问 GUI 才能添加实例、管理和监视您的实例和应用程序、查看分析以及配置 Citrix ADM 服务器。

工作站必须安装受支持的 Web 浏览器才能访问配置实用程序和控制板。

支持以下浏览器。

Web 浏览器	版本
Internet Explorer	11.0 及更高版本
Google Chrome	Chrome 19 及更高版本
Safari	Safari 5.1.1 及更高版本
Mozilla Firefox	Firefox 3.6.25 及更高版本

要访问 **Citrix ADM GUI**，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。这是您在安装服务器时指定的同一 IP 地址。
2. 在“用户名”和“密码”字段中，输入管理员凭据。默认管理员凭据是 nsroot/nsroot。

   登录到 Citrix ADM 后，您必须执行以下操作才能开始：

   - 向Citrix ADM 添加实例。如果要管理和监视这些实例，则必须向 Citrix ADM 服务器添加实例。
   - 在虚拟服务器上启用分析。要查看应用程序通信流的分析数据，必须在接收特定应用程序的流量的虚拟服务器上启用分析功能。
   - 在Citrix ADM 上配置 NTP 服务器。您必须在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。
   - 配置系统设置以实现最佳 Citrix ADM 性能。在开始使用 Citrix ADM 管理和监视您的实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

将实例添加到 **Citrix ADM**

February 6, 2024

实例是您想要从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备。如果要管理和监视实例，必须将这些实例添加到 Citrix ADM 服务器。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 中：

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

- Citrix Gateway
- Citrix SD-WAN

可以在第一次设置 Citrix ADM 服务器时添加实例，也可在以后添加。然后，您必须指定 Citrix ADM 可以用来访问该实例的实例配置文件。

> 注意
>
> - Citrix ADM 使用 Citrix ADC 实例的 NetScaler IP (NSIP) 地址进行通信。有关 Citrix ADC 实例和 Citrix ADM 之间必须打开的端口的信息，请参阅端口。
> - 对于 Citrix SD-WAN WO 和 Citrix SD-WAN EE 实例，Citrix ADM 使用实例的管理 IP 地址进行通信。
> - 要了解 Citrix ADM 如何发现实例，请参阅 发现实例。

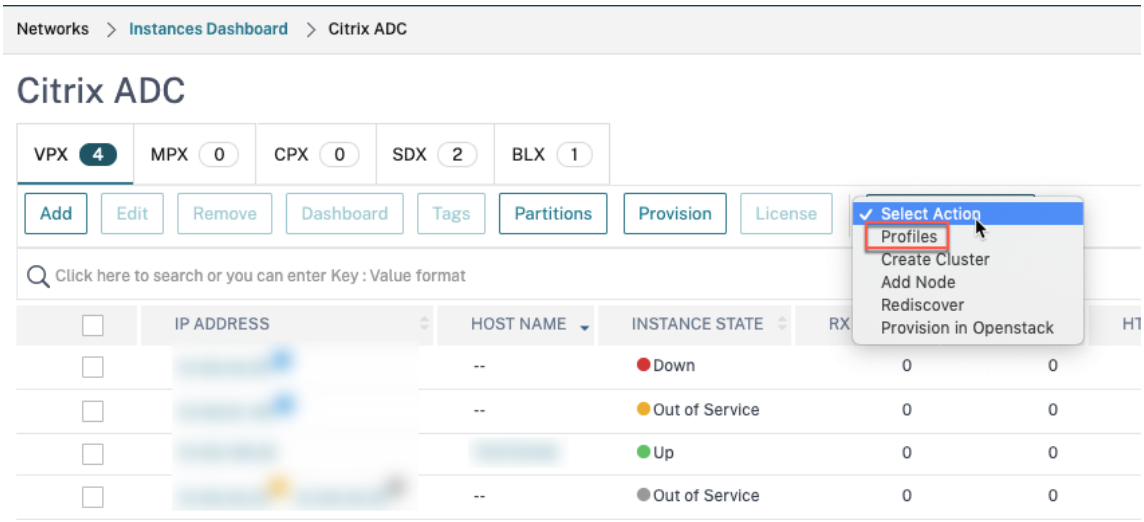
如何创建 **Citrix ADC** 配置文件

Citrix ADC 配置文件包含要添加到 Citrix ADM 的实例的用户名、密码、通信端口和身份验证类型。对于每个实例类型，都有一个默认的配置文件。例如，nsroot 是 Citrix ADC 实例的默认配置文件。默认配置文件通过使用默认 Citrix ADC 管理员凭据来定义。如果更改了实例的默认管理员凭据，可以为那些实例定义自定义实例配置文件。如果在发现实例后更改实例的凭据，则必须编辑实例配置文件或创建一个配置文件，然后重新发现实例。

您可以从“实例”页面或在添加或更改实例 时创建 Citrix ADC 配置文件。

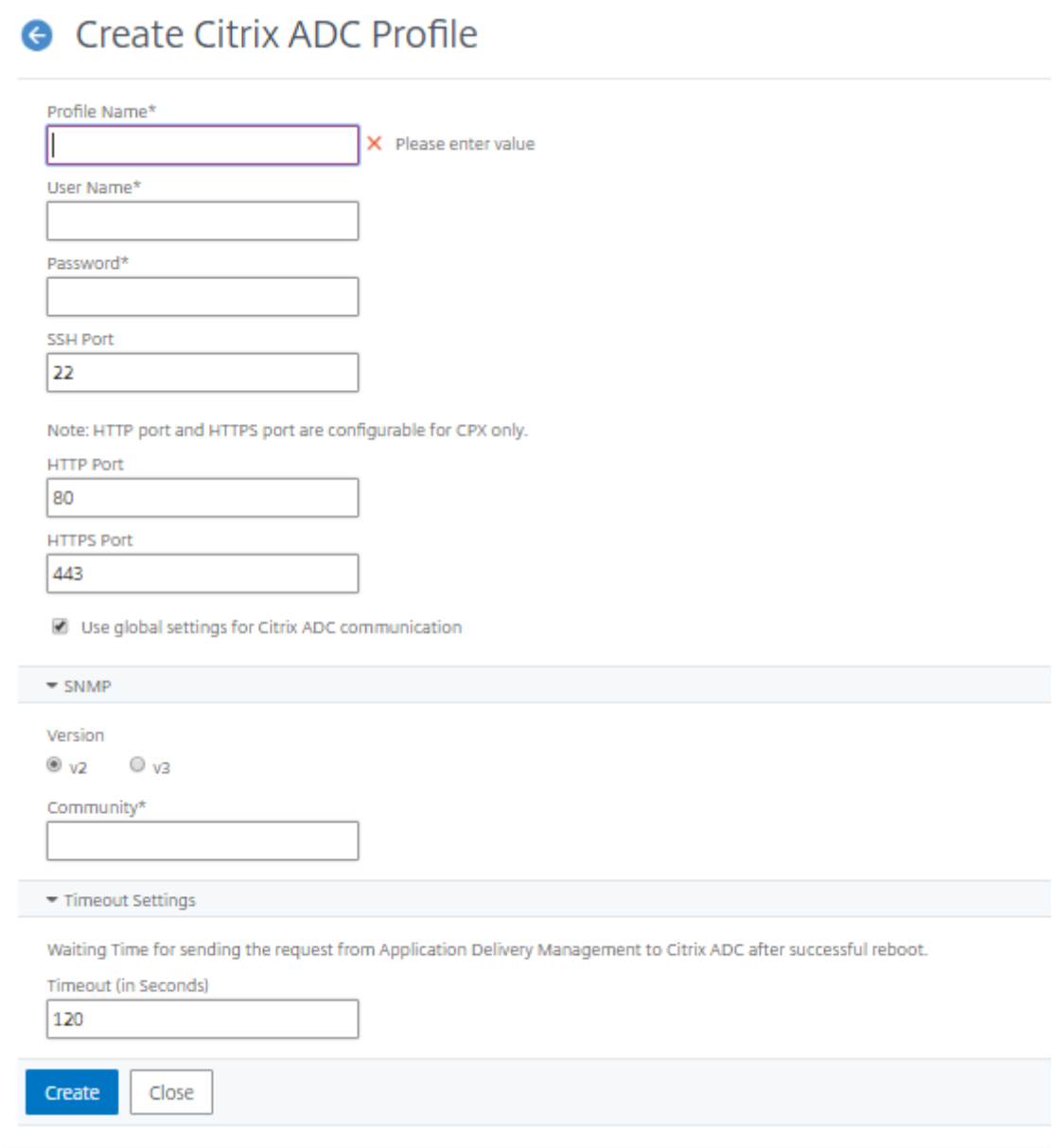
要从“实例”页创建 **Citrix ADC** 配置文件，请执行以下操作：

1. 导航到 网络 **>** 实例。
2. 选择一个实例。例如，Citrix ADC。
3. 在 Citrix ADC 页面上，选择 配置文件。



4. 在“管理员配置文件”页面上，选择“添加”。

5. 在创建 **Citrix ADC** 配置文件页面上，执行以下操作：



a) 配置文件名称：为 Citrix ADC 实例指定配置文件名称。

b) 用户名：指定登录到 Citrix ADC 实例的用户名。

c) 密码：指定登录到 Citrix ADC 实例的密码。

d) **SSH** 端口：指定 Citrix ADM 与 Citrix ADC 实例之间的 SSH 通信端口。

e) **HTTP** 端口：指定 Citrix ADM 与 Citrix ADC 实例之间的 HTTP 通信端口。

> 注意
>
> 默认 HTTP 端口是 80。您还可以指定可能在 Citrix ADC CPX 实例中配置的非默认或自定义 HTTP 端口。自定义 HTTP 端口只能用于 Citrix ADM 和 Citrix ADC CPX 之间的通信。

f) **HTTPS** 端口：指定 Citrix ADM 与 Citrix ADC 实例之间的 HTTPS 通信端口。

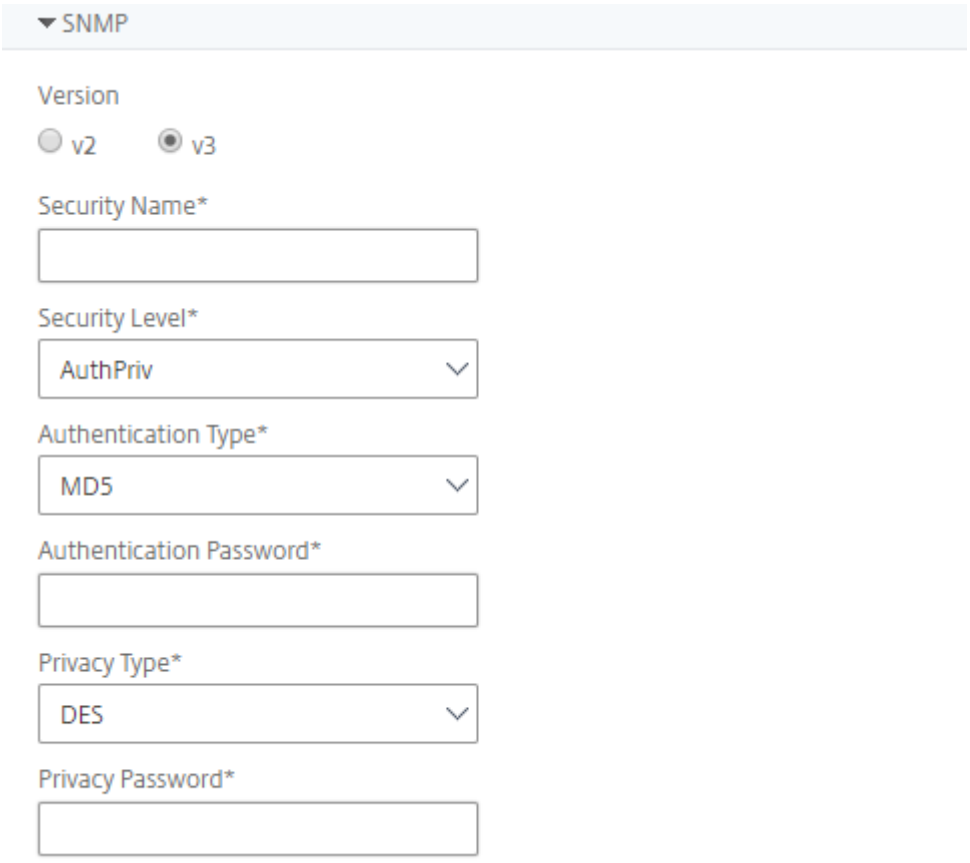
> 注意
>
> 默认 HTTPS 端口是 443。您还可以指定可能在 Citrix ADC CPX 实例中配置的非默认或自定义 HTTPS 端口。自定义 HTTPS 端口只能用于 Citrix ADM 和 Citrix ADC CPX 之间的通信。

g) 使用全局设置进行 **Citrix ADC** 通信：如果要使用系统设置进行 Citrix ADM 和 Citrix ADC 实例之间的通信，请选择此选项，否则请选择 http 或 https。

h) **SNMP** 版本：选择 **SNMPv2** 或 **SNMPv3** ，然后执行以下操作：

i. 如果选择 SNMPv2，请指定用于身份验证的社区名称。

ii. 如果选择 SNMPv3，请指定安全名称和安全级别。根据安全级别，选择 身份验证类型 和 隐私类型。



> 注意
>
> 对于 Citrix ADC SDX，仅支持 **SNMPv2**。

i) 超时设置：指定 Citrix ADM 在重新启动后向 Citrix ADC 实例发送连接请求之前必须等待的时间。

j) 选择创建。

将 **ADC** 实例添加到 **Citrix ADM**

可以在第一次设置 Citrix ADM 服务器时添加实例，也可在以后添加。

要添加实例，您必须指定每个 Citrix ADC 实例的主机名或 IP 地址，或指定 IP 地址范围。

对于 SD-WAN 实例，则指定每个实例的 IP 地址，或指定 IP 地址范围。请注意，Citrix ADM 仅支持 Citrix SD-WAN WO 和 Citrix SD-WAN PE 版本。

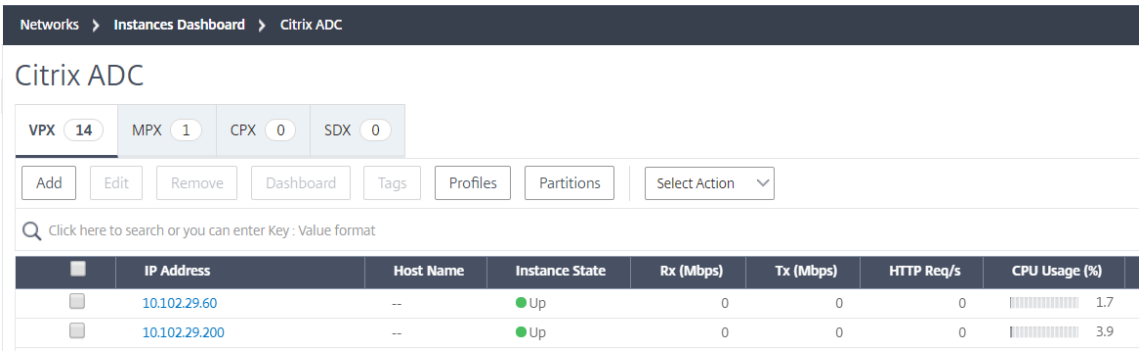
> 注意
>
> - 要添加在群集中配置的 Citrix ADC 实例，必须指定群集 IP 地址或群集设置中的任何一个单独节点。但是，在 Citrix ADM 上，群集仅由群集 IP 地址表示。
> - 对于设置为 HA 对的 Citrix ADC 实例，添加一个实例时，将自动添加该对中的另一个实例。

如果将两台 Citrix ADM 服务器设置为 高可用性模式，则在添加实例时，流量源将通过 ADM 浮动 IP 地址。

当您从使用本地代理配置的远程数据中添加实例时，流量源是通过 ADM Agent 进行的。

要将实例添加到 **Citrix ADM**，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到“网络”>“实例”>“**Citrix ADC**”。选择要添加的实例类型（例如，Citrix ADC VPX），然后单击添加。



3. 选择以下选项之一：
   - 输入设备 **IP** 地址-对于 Citrix ADC 实例，请指定每个实例的主机名或 IP 地址，或指定 IP 地址范围。对于 SD-WAN 实例，则指定每个实例的 IP 地址，或指定 IP 地址范围。
   - **Import from file**（从文件导入）- 上载包含要添加的所有实例的 IP 地址的文本文件。

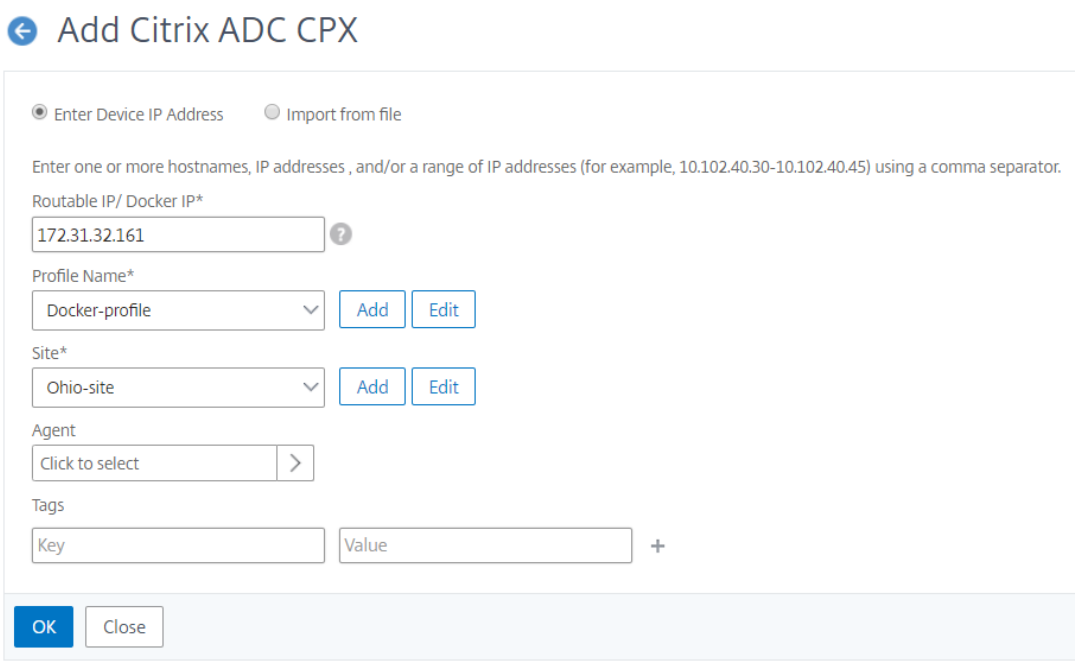
4. 在配置文件名称中，选择相应的实例配置文件，或通过单击 + 图标创建新的配置文件。
5. 在站点中，选择要添加实例的位置，或通过单击 **+** 图标创建新位置。
6. 单击“确定”启动向 Citrix ADM 添加实例的过程。

> 注意
>
> 如果要重新发现实例，请导航到“网络”>“实 例”>“**Citrix ADC**”。选择要重新发现的实例，然后从“选择操作”列表中单击“重新发现”。

将 **ADC CPX** 实例添加到 **Citrix ADM**

Citrix ADM 已得到增强，可为 CPX 功能中已完成的改进提供支持。Citrix ADC CPX 实例现已通过提供 CPX 的 IP 地址和设备配置文件添加到 Citrix ADM 中。CPX 实例的添加过程现在类似于在 ADM 中添加其他 ADC 类型（如 VPX 或 MPX）。此外，CPX 在 ADM 中的注册也得到了加强。当 CPX 启动时，Citrix ADM 会自动发现并注册 CPX 实例。不再通过 Docker 主机发现 CPX 实例。

1. 导航到“网络”>“实例”>“**Citrix ADC**”，然后单击“**CPX**”选项卡。
2. 单击添加。
3. 此时将打开“添加 **Citrix ADC CPX**”页。为以下参数输入值：
    a) 可以通过提供 CPX 实例的可访问 IP 地址或托管 CPX 实例的 Docker 容器的 IP 地址来添加 CPX 实例。
    b) 选择 CPX 实例的配置文件。
    c) 选择要在其中部署实例的站点。
    d) 选择代理。
    e) 作为一种选择，您可以为实例输入键-值对。通过添加键值对，您可以轻松地在以后搜索实例。



> 注意
>
> 对于 Citrix ADC CPX 实例，在创建 CPX 实例配置文件时，必须指定主机的 **HTTP**、**HTTPS**、**SSH** 和 **SNMP** 端口详细信息。您还可以在“起始端口”和“端口数”字段中指定主机发布的端口范围。

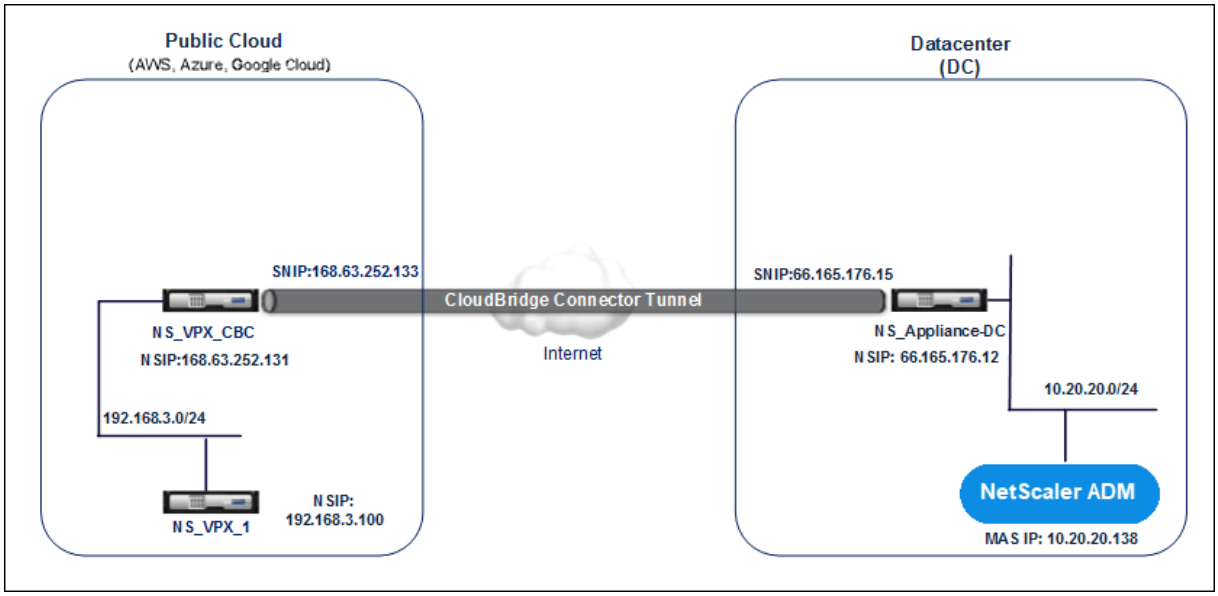
4. 单击确定。

将部署在云中的 **Citrix ADC VPX** 实例添加到 **Citrix ADM**

February 6, 2024

您可以使用 Citrix ADM 管理和监视部署在公有云（如 Amazon Web Services (AWS) 或 Microsoft Azure）上的 Citrix ADC VPX 实例。您需要在 Citrix ADM 和部署在公有云上的 Citrix ADC VPX 实例之间建立第 3 层连接。要建立第 3 层连接，您可以使用诸如 NetScaler CloudBridge Connector、Citrix SD-WAN、直接连接到 AWS、Azure 中的 VPN 或 Equinix 等第三方连接器等解决方案。

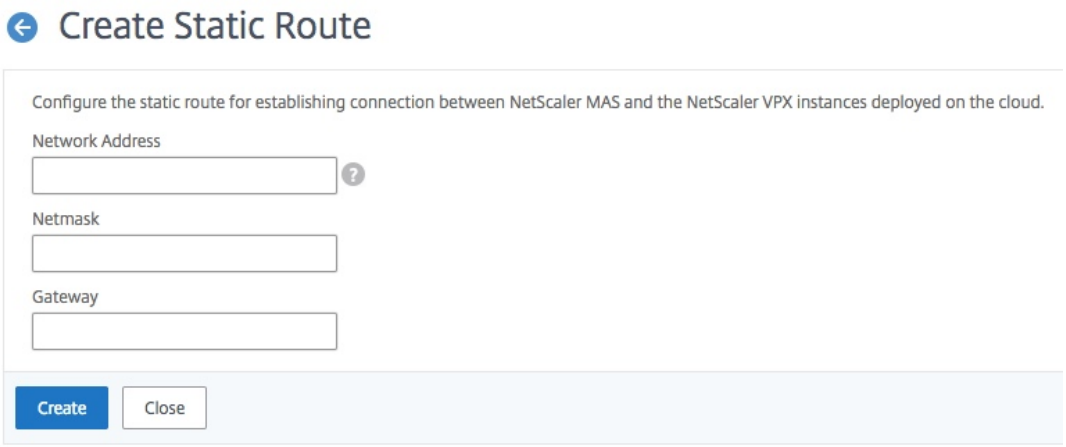
以下示例拓扑使用 NetScaler CloudBridge 连接器来实现 Citrix ADM 与云中部署的 Citrix ADC VPX 实例之间的第 3 层连接。



在数据中心 DC 中的 Citrix ADC 设备 NS_ 应用程序直流和 Citrix ADC 虚拟设备 (VPX) NS_VPX_CBC 之间设置了云桥连接器隧道。NS_Appliance-DC 和 NS_VPX_CBC 可实现 Citrix ADM 与部署在公有云中的 Citrix ADC VPX 实例 NS_VPX_1 之间的通信。建立通信后，您可以在 Citrix ADM 中发现 NS_VPX_1。

要配置此拓扑，请执行以下操作：

1. 在公有云中安装、配置和启动 Citrix ADC VPX 实例。
   - 有关说明，请参阅在 AWS 上安装 Citrix ADC VPX。
   - 有关说明，请参阅在 Microsoft Azure 上安装 Citrix ADC VPX。
2. 部署和配置 Citrix ADC 物理设备，或在数据中心的虚拟化平台上配置和配置 Citrix ADC 虚拟设备 (VPX)。
   - 有关说明，请参阅在 Citrix Hypervisor 上安装 Citrix ADC 虚拟设备。
   - 有关说明，请参阅在 VMware ESXi 上安装 Citrix 虚拟设备。
   - 有关说明，请参阅在 Microsoft Hyper-V 上安装 Citrix ADC 虚拟设备。
3. 在数据中心与公有云之间配置 CloudBridge Connector。有关说明，请参阅配置 CloudBridge Connector。
4. 配置静态路由，以便在 Citrix ADM 与部署在云端的 Citrix ADC VPX 实例之间建立连接，如下所示：
   a) 登录到 Citrix ADM。
   b) 导航到“系统”**>**“静态路由”，然后单击“添加”。



c) 在“网络地址”字段中，输入要建立从 Citrix ADM 通过连接器的静态路由的网络地址。

d) 在“网络掩码”字段中，输入网络的网络掩码。

e) 在“网关”字段中，输入网关的地址。

5. 通过指定公有云中 Citrix ADC VPX 实例的 IP 地址范围，将 Citrix ADC VPX 云实例添加到 Citrix ADM。有关详细说明，请参阅 将实例添加到 Citrix ADM。

在虚拟服务器上启用分析

February 6, 2024

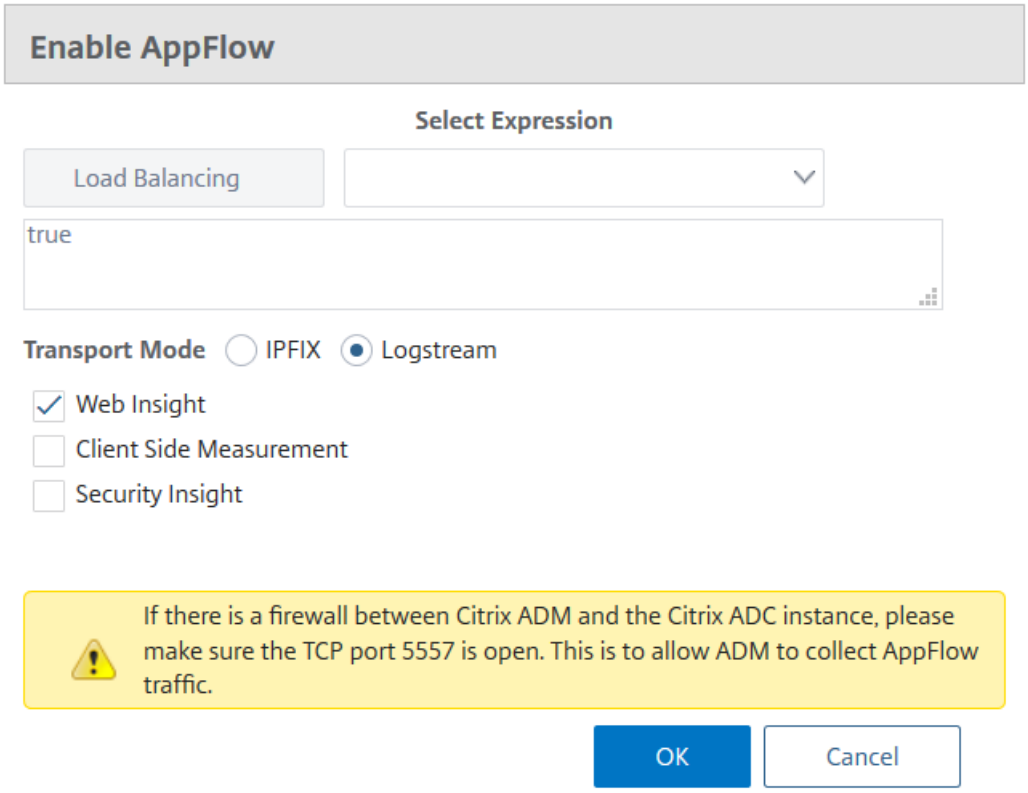
可以为选定实例上表示应用程序服务器的特定虚拟服务器启用分析，并监视该应用程序服务器的流量。分析功能可为虚拟服务器提供统计信息。

> 注意
>
> 对于 11.0 版本、65.30 版本及更高版本的 Citrix ADC 实例，Citrix ADM 上没有显式启用安全智能分析的选项。确保在 Citrix ADC 实例上配置 AppFlow 参数。AppFlow 参数配置完成后，Citrix ADM 开始接收 Security Insight 流量以及 Web Insight 流量。有关如何在 Citrix ADC 实例上设置 AppFlow 参数的详细信息，请参阅使用配置实用程序设置 AppFlow 参数。

要在 **Citrix ADM** 上的每个实例上启用分析，请执行以下操作：

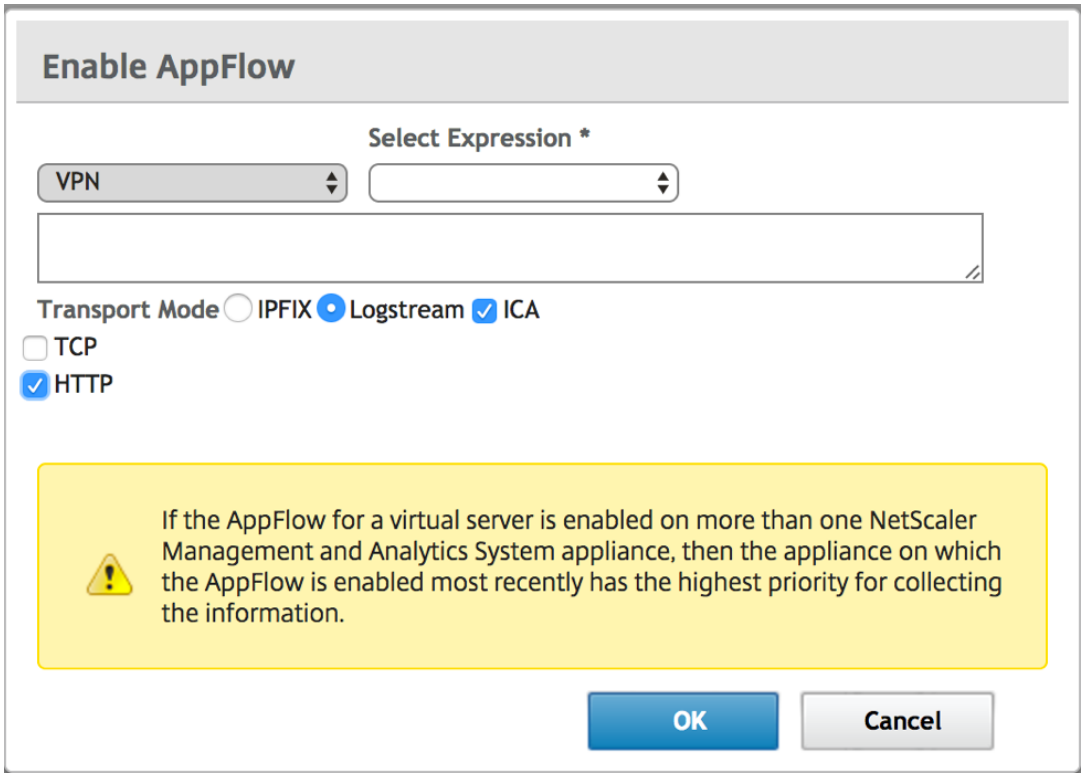
1. 导航到 网络 > 实例，然后选择要启用分析的 Citrix ADC 实例。例如，Citrix ADC。
2. 从实例列表中，选择一个实例。
3. 从“选择 操作”列表中，选 择“配置分析”。
4. 在“应用程序列表”中，选择虚拟服务器，然后单击“启用 **AppFlow**”。

5. 在“启用 **AppFlow**”字段中，键入 **true**，然后根据要启用的分析，选择 **Security Insight** 或 Web**Insight**，或两者兼而有之。



> 注意
>
> Citrix ADM 使用 Citrix ADC SNIP 作为 Logstream，将 NSIP 用于 IPFIX。如果在 Citrix ADM 和 Citrix ADC 实例之间启用了防火墙，请确保打开以下端口以使 Citrix ADM 能够收集 AppFlow 流量：
>
> | 传输模式 | 源 IP | 类型 | 端口 |
> | --- | --- | --- | --- |
> | IPFIX | NSIP | UDP | 4739 |
> | Logstream | SNIP | TCP | 5557 |

- 对于 **HDX Insight** 和 **GatewayInsight**，在单击“启用 **AppFlow**”时，需要选择在 Citrix ADC 实例上配置的 **VPN** 虚拟服务器，然后相应地选择 **ICA** 或 **HTTP** 复选框。



- 对于 **TCP Insight**，导航到“系统”>“分析设置”>“配置功能”，然后选择“启用 **TCP Insight**”。
- 对于 **Video Insight**，您需要在 Citrix ADC 设备上更改配置。有关如何为 Video Insight 启用分析的更多详细信息，请参阅 Video Insight。
- 对于 **WAN Insight** 来说，
  a) 导航到 基础架构 > 实例 > **NetScaler SD-WAN WO**，然后选择数据中心广域网优化设备。
  b) 从操作下拉列表中，选择启用 **Insight**。
  c) 根据需要选择以下参数：
    - HDX Insight 的地理数据收集：与 Google Geo API 共享客户端 IP 地址。
    - AppFlow：开始从广域网优化实例收集数据。
      * TCP 和 WANOpt：提供 TCP 和 WANOpt Insight 报告。
      * HDX：提供 HDX Insight 报告。
      * TCP 仅适用于 HDX：仅为 HDX Insight 报告提供 TCP。

在 Citrix ADM 中发现的 Citrix ADC 实例上启用 AppFlow 时，您可以选择 AppFlow 传输模式到 IPFIX 或 Logstream。有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。

下表介绍了支持 IPFIX 和 Logstream 作为传输模式的 Citrix ADM 的功能：

功能	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

您还可以使用 Citrix ADM 中的“启用 Web Insight”选项 启用或禁用 **Web Insight** 流量的处理。如果您不想监视 Web 智能分析通信，则可以禁用该选项。有关详细信息，请参阅 Citrix ADM 处理 Web Insight 流量。

配置 **NTP** 服务器

February 6, 2024

您可以在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

要在 **Citrix ADM** 上配置 **NTP** 服务器，请执行以下操作：

1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器），然后单击 **Add**（添加）。
2. 在 **Create NTP Server**（创建 NTP 服务器）页面上，输入以下详细信息：
    - **Server Name/IP Address**（服务器名称/IP 地址）–输入 NTP 服务器的域名或 IP 地址。添加了 NTP 服务器后无法更改名称或 IP 地址。
    - **Minimum Poll Interval**（最小轮询时间间隔）–指定传输的 NTP 消息之间的最小时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最小轮询时间间隔是 64 秒（可以表示为 2^6），则输入 6。
    - **Maximum Poll Interval**（最大轮询时间间隔）–指定传输的 NTP 消息之间的最大时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最大轮询时间间隔是 256 秒（可以表示为 2^8），则输入 8。

- **Key Identifier**（密钥标识符）- 输入可以用于 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择“Autokey”（自动密钥），请勿添加密钥标识符。
- **Autokey**（自动密钥）- 如果希望 NTP 服务器使用公钥身份验证，请选择 **Autokey**（自动密钥）。如果要添加密钥标识符，请勿选择。
- **Preferred**（首选）–如果希望将此 NTP 服务器指定为进行时钟同步的首选服务器，请选择此选项。这仅在配置多个服务器时适用。

3. 单击创建。

要在 **Citrix ADM** 上启用 **NTP** 同步，请执行以下操作：

1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。
2. 单击 **NTP Synchronization**（NTP 同步），并选中 **Enable NTP Synchronization**（启用 NTP 同步）复选框。
3. 单击确定。

配置系统设置

February 6, 2024

在开始使用 Citrix ADM 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

配置系统警报

您应该配置系统警报，以确保您可以了解任何严重或重大系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。对于有些警报类别（例如 cpuUsageHigh 或 memoryUsageHigh），您可以为每项设置阈值并定义严重性（例如“Critical”（严重）或“Major”（重大））。对于有些类别（例如 inventoryFailed 或 loginFailure），只能定义严重性。当某个警报类别（例如，memoryusageHigh）的阈值被突破时，或者当发生与该警报类别对应的事件（例如 LoginFailure）时，系统会记录一条消息，您可以将该消息作为 syslog 消息查看。

要配置系统警报，请执行以下操作：

1. 导航到“系统”**>**“警报”，选择要配置的警报，然后单击“**”编辑”。
2. 在“配置警报”页面上，选择警报严重性，然后设置阈值。
3. 要查看已超过阈值或已发生事件的警报，请导航到 系统 **>** 审核，然后单击 **Syslog** 消息。

配置系统通知

可以发送通知来为一些系统相关的功能选择用户组。您可以在 Citrix ADM 中设置通知服务器，还可以配置电子邮件和短消息服务 (SMS) Gateway 服务器以向用户发送电子邮件和文本通知。这可确保您将收到任何系统级活动（例如，用户登录或系统重新启动）通知。

要配置系统通知，请执行以下操作：

1. 导航到 **System**（系统）**> Notifications**（通知）。在“设置”下，单击“更改通知设置”。
2. 在“配置系统通知设置”页上，选择 Citrix ADM 生成的事件的类别或类别。
3. 然后，配置电子邮件服务器或 SMS 服务器以通过电子邮件或/和 SMS 接收通知。

配置系统删除设置

要限制存储在 Citrix ADM 服务器数据库中的报告数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时修剪一次（在 00.00 点）。

要配置系统修剪设置，请执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。在“删除设置”下，单击“系统清理设置”。
2. 在“配置系统清理设置”页中，指定保留数据的天数，然后单击“** 确定”。

配置系统备份设置

Citrix ADM 每天在 00:30 时间自动备份系统。默认情况下，它保存三个备份文件。您可能希望保留更多数量的系统备份。您还可以加密备份文件。您还可以选择在外部服务器上保存备份。

要配置系统备份设置，请执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。
2. 在“备份设置”下，单击“系统备份设置”。
3. 在“配置系统备份设置”页面上，指定所需的值。

配置实例备份设置

如果您备份 Citrix ADC 实例的当前状态，则可以在该实例变得不稳定时使用备份文件恢复稳定性。在执行升级之前这样做尤其重要。默认情况下，每 12 小时进行一次备份，且有三个备份文件保留在系统中。

要配置实例备份设置：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。
2. 在“备份设置”下，选择 实例备份设置，然后指定所需的值。

配置实例事件修剪设置

要限制存储在 Citrix ADM 服务器数据库中的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

要配置实例事件修剪设置，请执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。
2. 在“删除设置”下，单击“实例事件删除设置”。
3. 输入要在 Citrix ADM 服务器上保留数据的时间间隔（以天为单位），然后单击“** 确定”。

配置实例 **syslog** 清除设置

要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定将从 Citrix ADM 中删除通用系统日志数据的天数。

要配置实例系统日志清除设置，请执行以下操作：

1. 导航到 **System**（系统）> **System Administration**（系统管理）。在“删除设置”下，单击“实例 **Syslog** 清除设置”。
2. 在“配置实例 Syslog 清除设置”页面中，在“保留 Syslo g 通用数据”字段中指定 **1** 到 180 之间的天数。
3. 单击确定。

升级

February 6, 2024

每个 Citrix ADM 版本都提供了新的和更新的功能，并增强了功能。Citrix 建议您将 Citrix ADM 升级到最新版本，以利用新功能和错误修复。增强功能、已知问题和缺陷修复的完整列表在每个版本发布时附带的发行说明中提供。在开始升级之前，了解许可证框架和可以使用的许可证类型也很重要。有关 Citrix ADM 许可信息，请参阅许可。

升级路径信息也可在 Citrix 升级指南中找到。

升级准备

从 Citrix ADM 的“Downloads”（下载）页面下载升级包，并按照本文中的说明将您的系统升级到最新的内部版本 12.1。启动升级操作后，Citrix ADM 将重新启动，现有连接将终止并在升级成功完成后重新连接。现有配置将保留，但在升级成功完成之前，Citrix ADM 不会处理任何数据。

> 重要
>
> Citrix ADM 版本和内部版本应 等于或高 于您的 Citrix ADC 版本和内部版本。例如，如果您已安装 Citrix ADM 12.1 Build 50.39，请确保已安装 Citrix ADC 12.1 Build 50.28/50.31 或更早版本。

升级到 **12.1** 之前的注意事项：

- 如果您要从 11.1 版本或 56.x 之前的 12.0 版本升级到 Citrix ADM 12.1 Build 48.18 版本，请执行以下步骤。
  - 从现有版本升级到 12.0 版本 57.24。
  - 然后，升级到版本 12.1 的最新版本。

    您必须遵循此两步流程，因为成功升级到 12.1 版本需要某些清理程序。这些过程仅从 12.0 版本 56.x 开始可用。
- 在 12.1 中，高可用性部署能够在主节点上配置浮动 IP 地址，无需单独的 Citrix ADC 负载平衡器。由于这一改进，高可用性部署必须位于同一子网上。如果您当前的部署位于不同的子网上，则必须阅读本文以了解升级过程。
- 使用 12.1 时，已删除高级备份支持。升级到 Citrix ADM 12.1 后，高级备份功能将不再可用。查看这篇文章了解更多详情。

> 注意
>
> 您无法将 Citrix ADM 从 12.1 版本降级到早期版本的任何版本。

建议的预防措施：

- 在升级之前，请备份 Citrix ADM 服务器。
- 在升级后，可能必须在 Citrix ADM 服务器与托管实例之间重新建立连接。如果继续，会有确认提示向您警告连接可能失败。
- 对于高可用性设置中的 Citrix ADM 服务器，升级时，请勿在其中任何一个节点上进行任何配置更改。

  > 警告
  >
  > 在升级过程成功完成之前，请勿刷新浏览器。完成升级过程可能需要几分钟。

- 升级后，活动节点可以在高可用性对中进行更改。

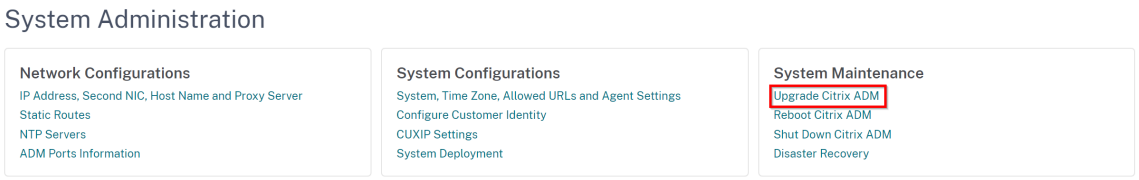
升级单个 **Citrix ADM** 服务器

要升级单个 **Citrix ADM** 服务器，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 服务器的 IP 地址。

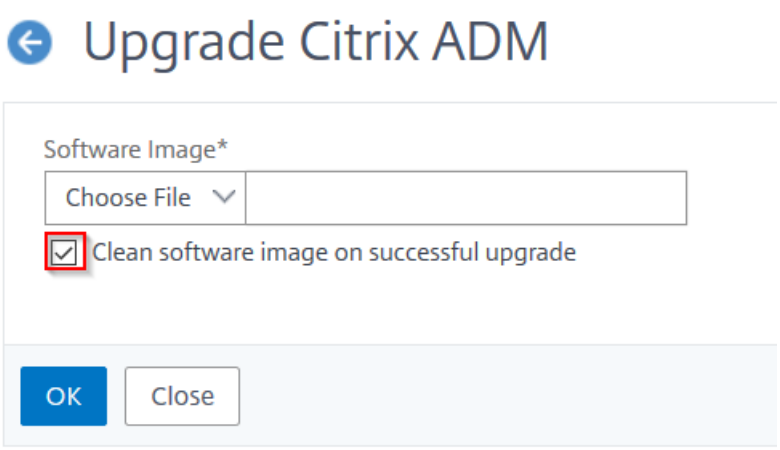
> 注意
>
> 对于高可用性模式下的 Citrix ADM 服务器，键入高可用性对中任一 Citrix ADM 服务器或负载平衡虚拟服务器的 IP 地址。

2. 在“用户名”和“密码”字段中，输入管理员凭据。
3. 导航到 “系统” > “系统管理”。在“系统管理”子标题下，单击“升级 **Citrix ADM**”。

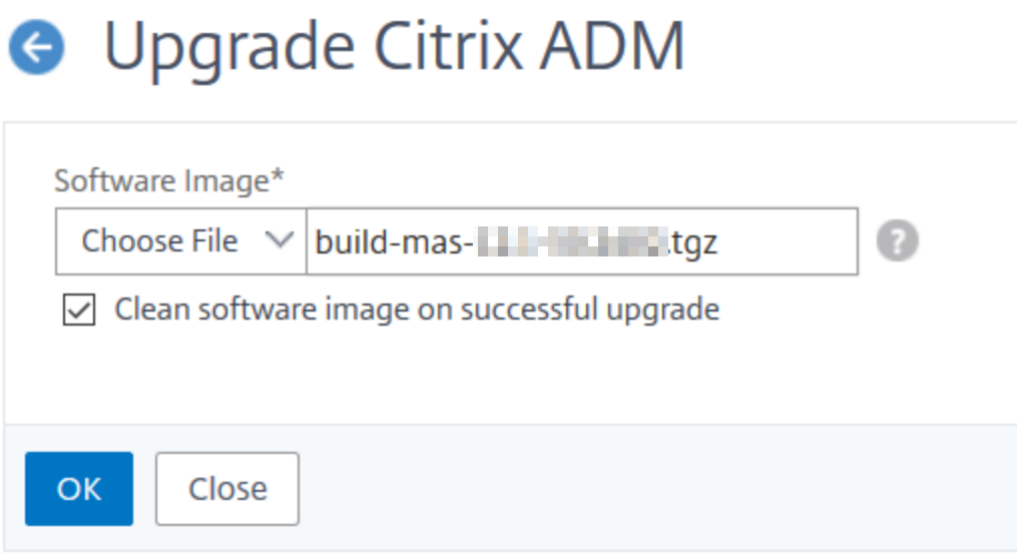


4. 在升级 **Citrix ADM** 页面上，选中成功升级时清理软件映像复选框以在升级 后删除映像文件。选择此选项会在升级时自动删除 Citrix ADM 映像文件。

> 注意
>
> 此选项默认处于选中状态。如果在开始升级过程之前未选中此复选框，则必须手动删除映像。



5. 然后，您可以通过选择“本地 计算机”或“设备”来上载新图像文件。构建文件必须存在于 Citrix ADM 虚拟设备上。



此时将显示“确认”对话框。单击确定。

6. 单击确定。

   升级过程开始。

将高可用性对从早期版本升级到 **12.1**

对于处于高可用性模式的 Citrix ADM 服务器，您可以通过访问主动节点或负载平衡虚拟服务器 IP 地址进行升级。在任一服务器中启动升级过程后，两个 Citrix ADM 服务器都会自动升级到最新版本。

> 重要
>
> 在高可用性模式下升级 **Citrix ADM** 时的注意事项
>
> 在高可用性模式下将 Citrix ADM 从早期版本升级到 12.1 时，高可用性连接由在辅助节点上运行的“加入 HA”脚本在内部建立。升级过程所花费的时间取决于网络基础架构、数据库中存在的数据和链路速度。在两个节点之间重新建立连接可能需要几个小时。在此期间，主节点不接收来自辅助节点的任何心跳信号。在升级过程完成之前，您会在主界面上看到缺少心跳的通知。升级过程结束后，辅助节点重新启动并完成高可用性部署。
>
> 注意
>
> 要了解升级状态，请使用 SSH 登录到每个节点，运行以下命令并检查输出：
>
> pgrep -lf installmas
>
> pgrep -lf maintenance
>
> pgrep -lf join_streaming_replication
>
> pgrep -lf pg_basebackup

> 如果这些命令中的任何一个显示任何节点上正在运行的进程，则升级正在进行中，不应中断。请勿在此期间重新启动 Citrix ADM，也不要尝试在辅助节点上强制进行故障转移。
>
> 升级过程完成后，有时您可能无法使用 nsroot/nsroot 或您的用户凭据登录。这是因为 Citrix ADM 子系统尚未完全重启或者迁移可能仍在进行中。请勿重新启动 Citrix ADM 或不要尝试恢复密码。这可能会产生不良影响，系统可能会表现不一致。如果需要，您可以尝试使用 nsrecover/<your_password_for_the_nsroot_user> 凭据登录。
>
> 升级之后和开始操作之前，请确保主节点和辅助节点均已升级且重新启动已完成。
>
> 注意
>
> 您无法使用 CLI 在高可用性模式下升级 Citrix ADM。

Citrix ADM 服务器中的池化许可，具有高可用性：

在高可用性模式下部署 Citrix ADM 服务器时，许可证文件将连接到主节点并使用主服务器的 hostID 或 MAC 地址进行配置（节点锁定）。从 12.1 版本起，Citrix ADM 现在以高可用性支持池许可证功能。要在两个节点上配置池化许可功能，两个节点上必须有相同的许可证文件。要在辅助节点上安装相同的许可证，必须将许可证重新托管到辅助节点的 hostID（MAC 地址）。

以 Citrix ADM 有两个处于高可用性模式的服务器节点 S1 和 S2 为例。原始许可证文件 L1 安装在服务器 S1 上。现在应将重新托管的许可证文件 L2 分配给 S2。

按照以下步骤将高可用性模式下的 Citrix ADM 从 12.0 升级到 12.1 并配置池化许可证功能：

1. 在高可用性模式下登录 Citrix ADM 服务器的主节点并执行升级过程。
2. 在辅助服务器节点 S2 上安装重新托管的许可证文件 L2。

   此时：

   - 如果 S2 是主节点，则可以通过访问该实例的 GUI 来安装 L2 许可证。
   - 如果 S2 是辅助节点，则必须手动执行故障转移，以便 S2 现在成为主节点。使用 GUI 在新的主节点上安装许可证 L2。
     这是因为您只能通过 GUI 访问高可用性的主服务器。
3. 在新的主节点上配置浮动 IP 地址。
4. 删除 Citrix ADC 实例上的许可证服务器 IP 地址，然后将其重新配置为使用浮动 IP 地址。在所有 Citrix ADC 实例上执行此操作。

Citrix 建议您通过在 Citrix ADC 实例上创建维护窗口来执行 Citrix ADM 高可用性池化许可升级。这是因为删除许可证服务器并添加浮动 IP 地址会导致 Citrix ADC 实例暂时恢复到最低带宽支持。

高可用性升级方案

Citrix ADM 服务器可能在两种情况下以高可用性模式部署。

- 主服务器和辅助服务器部署在同一个子网上。
- 主服务器和辅助服务器部署在不同的子网中。

此升级文档可帮助您在这两种情况下升级 Citrix ADM。

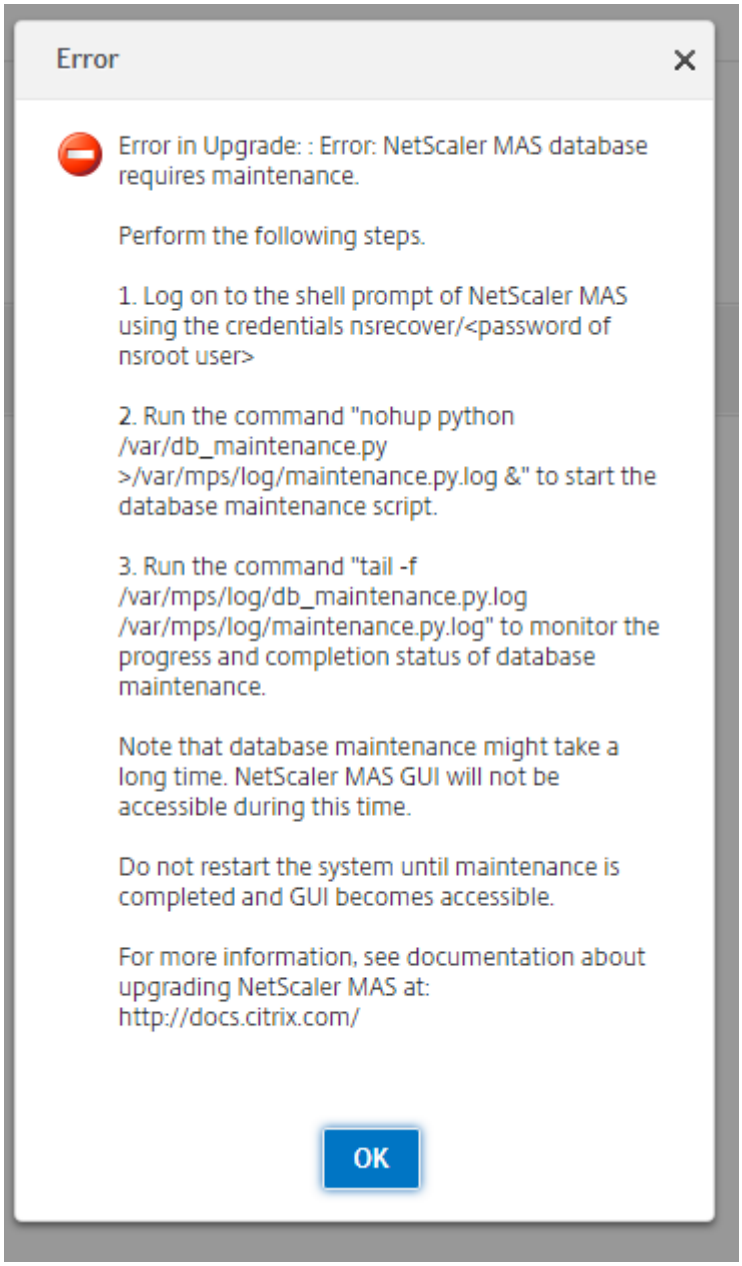
- 在同一子网上升级高可用性设置
- 升级不同子网中的高可用性设置

升级同一子网上的高可用性设置

在同一子网上以高可用性模式部署的 Citrix ADM 服务器的升级由 Citrix ADM 12.1 自动处理。

要升级在同一子网上以高可用性模式部署的 **Citrix ADM**，请执行以下操作：

1. 登录到主节点并导航到“系统”>“系统管理”。
2. 在“系统管理”下，单击“升级 **Citrix ADM**”。
3. 如果升级期间出现错误，则会显示以下错误消息。按照主服务器上消息中提到的说明进行操作。

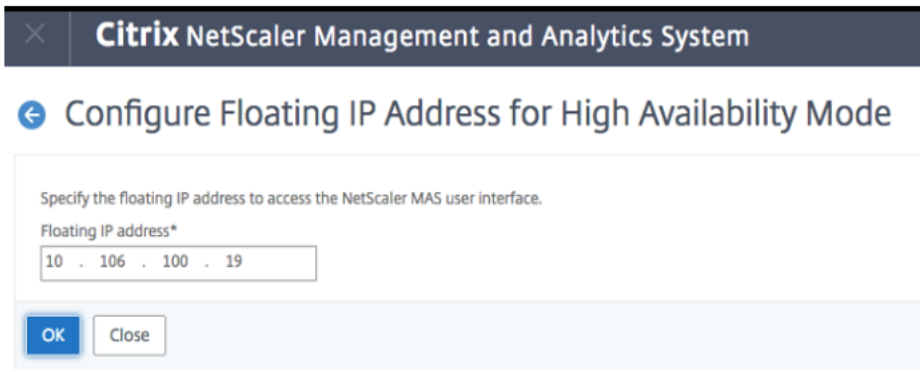


4. 作为升级过程的一部分，必须通过 CLI 执行清理程序。在清理过程中，辅助节点成为主节点。无法通过其 GUI 访问旧的主节点。在清理过程进行期间，请勿重新启动旧的主节点和新的主节点。清理过程完成后，通过新的主节点继续执行升级过程。
5. 升级过程完成后，两个节点必须同步其数据库。完成同步和启动新的辅助节点所花费的时间取决于数据库中存在的数据。

   > 注意
   >
   > 升级成功后，必须使用 Citrix ADM 用户界面配置浮动 IP 地址。

6. 要配置浮动 IP 地址，请导航到“系统”**>**“部署”**>**“为高可用性模式配置浮动 **IP** 地址”。

7. 指定浮动 IP 地址，如下图所示，然后单击“确定”。



升级不同子网中的高可用性设置

在高可用性模式下部署在不同子网上的 Citrix ADM 服务器的升级必须由管理员处理。

在这种情况下，Citrix ADM HA 节点 1（主节点）位于子网 1 中，Citrix ADM HA 节点 2（辅助节点）位于子网 2 中。

要升级在不同子网上以高可用性模式部署的 **Citrix ADM**，请执行以下操作：

1. 手动中断高可用性设置。有关更多信息，请参阅 禁用高可用性。
2. 升级 Citrix ADM 独立节点 1。有关如何升级 Citrix ADM 的更多信息，请参阅 升级单个 Citrix ADM 服务器。
3. 在子网 1 中设置并注册新的 Citrix ADM 独立节点 3。
4. 注册节点 1 和节点 3 后，在高可用性模式下部署这两个节点。有关详细信息，请参阅 将主节点和辅助节点部署为高可用性对。

   > 注意
   >
   > 配置浮动 IP 地址是强制性的。

5. 删除 Citrix ADM 节点 2。

将高可用性对从之前的 **12.1** 版本升级到最新版本

您可以将部署在高可用性下的 Citrix ADM 服务器从早期的 12.1 版本升级到更高的 12.1 版本。

要升级在高可用性模式下部署的 Citrix ADM，请执行以下操作：

1. 从 Citrix.com 下载页面下载 Citrix ADM 12.1 build 49.37 图像文件。
2. 登录到主节点并导航到“系统”>“系统管理”。
3. 在“系统管理”下，单击“升级 **Citrix ADM**”。
4. 导航到图像所在的文件夹。

   升级时，请勿对任一节点进行任何配置更改。

> 警告
>
> - 在升级过程成功完成之前，请勿刷新浏览器。完成升级过程可能需要几分钟。

升级后，活动节点可以在高可用性对中进行更改。

升级 **Citrix ADM** 灾难恢复部署

升级 Citrix ADM 灾难恢复部署分为两个步骤：

您必须先升级主站点中在高可用性模式下配置的 Citrix ADM 节点。稍后您必须升级灾难恢复节点。

在升级灾难恢复节点之前，请确保已升级了以高可用性部署的 Citrix ADM 服务器。

- 如果您要将处于高可用性模式的 Citrix ADM 服务器从旧版本升级到 12.1，请参阅本文档中的将高可用性对从早期版本升级到 12.1。
- 如果您要在高可用性对的基础上从较早的 12.1 版本升级到更高的 12.1 版本，请参阅本文档中的将高可用性对从先前的 12.1 版本升级到最新版本。

升级 **Citrix ADM** 灾难恢复节点

1. 从 Citrix 下载站点下载 Citrix ADM 升级映像文件。
2. 使用“nsrecover”凭据将此文件上载到灾难恢复节点。
3. 使用“nsrecover”凭据登录到灾难恢复节点。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Fri Aug 31 05:41:16 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-mas-12.1-500.113.tgz
```

4. 导航到放置图像文件的文件夹并解压缩该文件。
5. 运行以下脚本：

   ./installmas

```
bash-3.2# ./installmas
```

为多站点部署升级内部部署代理

升级 Citrix ADM 代理部署的过程分为三个步骤。

在升级本地代理之前，请确保已完成以下任务：

1. 升级在高可用性中部署的 Citrix ADM 服务器。

   - 如果您要将处于高可用性模式的 Citrix ADM 服务器从旧版本升级到 12.1，请参阅本文档中的将高可用性对从早期版本升级到 12.1。
   - 如果您要在高可用性对的基础上从较早的 12.1 版本升级到更高版本的 12.1 版本，请参阅将高可用性对从之前的 12.1 版本升级到最新版本

2. 升级 Citrix ADM 灾难恢复节点。

   有关详细信息，请参阅 升级 Citrix ADM 灾难恢复部署。

升级本地代理

1. 从 Citrix 下载站点下载 Citrix ADM 代理升级映像文件。
2. 使用“nsrecover”凭据将此文件上载到代理节点。
3. 确保您下载了正确的代理升级映像。图像文件名采用以下格式：

   build-masagent-12.1-48.18.tgz

4. 使用“nsrecover”凭据登录到本地代理。
5. 导航到放置图像文件的文件夹并解压缩该文件。

```
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. 运行以下脚本：

   ./installmasagent

```
bash-3.2# ./installmasagent
```

取消对 **Citrix ADM** 高级备份和还原功能的支持

现在，您可以使用 Citrix ADM 版本 12.1 中提供的新灾难恢复功能对 Citrix ADM 服务器进行完整备份，而不必使用高级备份功能来完整备份 Citrix ADM 高可用性设置并帮助处理业务连续性用例。

> 重要
>
> 1. 升级到 Citrix ADM 12.1 后，高级备份功能将不再可用。要删除高级备份功能并继续使用灾难恢复功能进行备份，请参阅 升级到 Citrix ADM 12.1 后备份 Citrix ADM。只有 Citrix ADM HA 支持灾难恢复。

> 2. 要继续对 Citrix ADM 服务器进行部分备份，其中包括配置文件、实例详细信息、系统数据等，然后要在独立部署中恢复 Citrix ADM 服务器（部分备份），请参阅 如何在单服务器部署中备份和恢复 Citrix ADM 服务器。

如果主服务器发生灾难，请使用灾难恢复功能在同一台主服务器上启动和配置 Citrix ADM，而不会丢失数据。该功能仅在 Citrix ADM 版本 12.1 的高可用性设置中部署的 Citrix ADM 服务器上可用。

升级到 **Citrix ADM 12.1** 后备份您的 **Citrix ADM** 服务器

要继续备份 Citrix ADM 服务器，Citrix 建议执行以下操作：

1. 通过执行以下操作删除 Citrix ADM 上的远程备份设置：
   a) 导航到“系统”>“系统管理”>“高级系统备份设置”。
   b) 在“配置高级备份设置”页面中，选择“否”以禁用远程备份。
   c) 单击 应用设置。请等待 Citrix ADM 服务器重新启动并应用更改后的设置。
   d) 删除您的远程备份节点。
2. 部署和配置新的 Citrix ADM 服务器，使用在上述步骤中重新启动的现有 Citrix ADM 服务器创建高可用性设置。
   - 要了解有关 Citrix ADM 独立部署的更多信息，请参阅部署 Citrix ADM。
   - 要了解有关 Citrix ADM HA 部署的更多信息，请参阅高可用性部署。
3. 配置灾难恢复以继续备份和恢复数据。有关灾难恢复的更多信息，请参阅配置灾难恢复以实现高可用性。

将其他磁盘添加到 **Citrix ADM** 服务器

如果您的 Citrix ADM 存储要求超过默认磁盘空间（120 千兆字节），则可以附加一个额外的磁盘。在单服务器部署和高可用性部署中，您可以连接其他磁盘。

将 Citrix ADM 从发行版 12.0 升级到 12.1 时，您在早期版本的附加磁盘上创建的分区保持不变。这些分区不会被删除，也不会调整它们的大小。

在升级后的版本中，附加额外磁盘的过程保持不变。现在，您可以使用 Citrix ADM 中的新磁盘分区工具在新添加的磁盘中创建分区。您也可以使用工具来调整现有附加磁盘中的分区大小。有关如何连接其他磁盘和使用新的磁盘分区工具的更多信息，请参阅 如何将其他磁盘连接到 Citrix ADM。

使用样书在 **OpenStack** 中预配 **Citrix ADC** 实例

从 Citrix ADM 12.1 版本 49.23 起，OpenStack 调配工作流程的架构已更新。该工作流程现在使用 Citrix ADM 样书来配置 Citrix ADC 实例。如果要从版本 12.0 或版本 12.1 版本 48.18 升级到 Citrix ADM 12.1 版本 49.23，则必须运行以下迁移脚本：


```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

有关“os-cs-lb-mon”样书和迁移脚本的更多信息，请参阅 使用样书在 OpenStack 上预配 Citrix ADC VPX 实例

身份验证

February 6, 2024

May 24, 2018

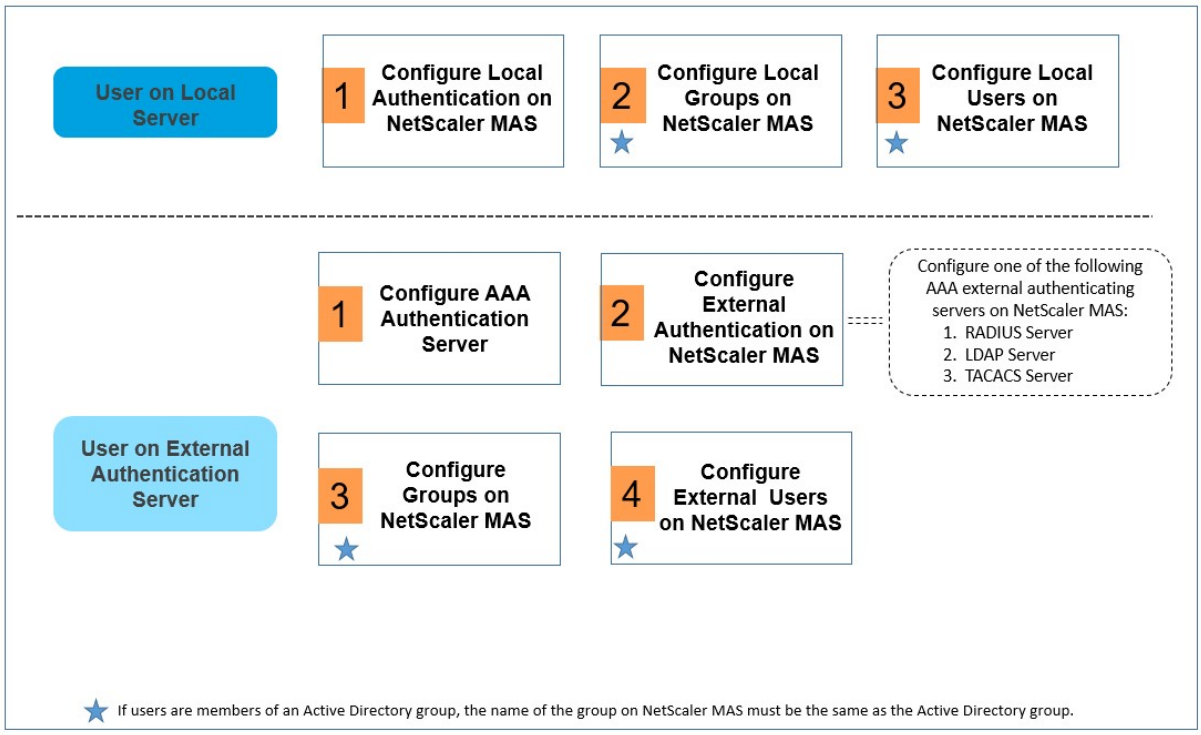
用户可以通过 Citrix Application Delivery Management (ADM) 进行内部身份验证，也可以通过身份验证服务器进行外部身份验证，或两者兼而有之。如果使用本地身份验证，则用户必须位于 Citrix ADM 安全数据库中。如果在外部对用户进行身份验证，则用户的“外部名称”应该匹配向身份验证服务器注册的外部用户标识，具体取决于选定的身份验证协议。

Citrix ADM 支持通过 RADIUS、LDAP 和 TACACS 协议进行外部身份验证。此统一支持提供公用接口来对访问系统的所有本地和外部身份验证、授权和记帐 (AAA) 服务器用户进行身份验证和授权。Citrix ADM 可以对用户进行身份验证，无论用户使用何种实际协议与系统进行通信。当用户尝试访问配置为外部身份验证的 Citrix ADM 实现时，所请求的应用服务器会将用户名和密码发送到 RADIUS、LDAP 或 TACACS 服务器进行身份验证。如果身份验证成功，则使用相应的协议在 Citrix ADM 中识别用户。

您可以通过两种方式在 Citrix ADM 中对用户进行身份验证：

- 通过使用 Citrix ADM 本地服务器
- 使用外部身份验证服务器

以下流程图显示了对本地或外部用户进行身份验证时要遵循的工作流程：



配置外部身份验证服务器

Citrix ADM 支持多种协议来提供外部身份验证、授权和记账 (AAA) 服务。

Citrix ADM 将所有身份验证、授权和记账 (AAA) 服务请求发送到远程 RADIUS、LDAP 或 TACACS+ 服务器。远程 AAA 服务器接收请求，验证请求，然后向 Citrix ADM 发送响应。当配置为使用远程 RADIUS、TACACS+ 或 LDAP 服务器进行身份验证时，Citrix ADM 将变成 RADIUS、TACACS+ 或 LDAP 客户端。在其中任何配置中，身份验证记录都存储在远程主机服务器数据库中。每个用户的登录和注销帐户名称、分配的权限和时间记帐记录也都存储在 AAA 服务器中。

此外，您可以使用 Citrix ADM 的内部数据库在本地对用户进行身份验证。可在数据库中创建用户及其密码和默认角色条目。还可以针对特定类型的身份验证创建服务器组。服务器组中的服务器列表是有序列表。除非列表中的第一个服务器不可用，否则始终使用该服务器，如果不可用，则使用列表中的下一个服务器。可以在一个组中配置不同类型的服务器，还可以将内部数据库包含为配置的 AAA 服务器列表的回退身份验证备份。

配置 **RADIUS** 身份验证服务器

您可以将 Citrix ADM 配置为使用一台或多台 RADIUS 服务器对用户的访问进行身份验证。您的配置可能需要使用网络访问服务器 IP (NAS IP) 地址或网络访问服务器标识符 (NAS ID)。将 Citrix ADM 配置为使用 RADIUS 身份验证服务器时，请遵循以下准则：如果启用使用 NAS IP 地址，则设备会将其配置的 IP 地址发送到 RADIUS 服务器，而不是发送建立 RADIUS 连接时使用的源 IP 地址。

- 如果配置 NAS ID，设备会将标识符发送到 RADIUS 服务器。如果不配置 NAS ID，则设备将其主机名发送到 RADIUS 服务器。
- 如果启用 NAS IP 地址，则设备忽略配置的任何 NAS ID，并使用 NAS IP 与 RADIUS 服务器通信。

要配置 **RADIUS** 身份验证服务器，请执行以下操作：

1. 在 Citrix ADM 中，导航到系统 > 身份验证 > **RADIUS**。
2. 在 **RADIUS** 页面上，单击“添加”。
3. 在“创建 **RADIUS** 服务器”页面上，设置参数并单击“创建”将服务器添加到 RADIUS 身份验证服务器列表中。以下参数是必需的：
   a) 名称。RADIUS 服务器的名称。
   b) 服务器名称**/IP** 地址。RADIUS 服务器的服务器名称或 IP 地址。
   c) **Port**（端口）。默认情况下，端口 1812 用于 RADIUS 身份验证。如有需要，可以指定其他端口号。
   d) 超时（秒）。Citrix ADM 系统等待 RADIUS 服务器响应的时间，以秒为单位。
   e) 密钥。任何字母数字表达式。这是 Citrix ADM 和 RADIUS 服务器之间共享的密钥，用于启用通信。
4. 单击“详细信息”展开该部分并设置其他参数，然后单击“创建”。

有关如何添加 RADIUS 服务器的更多详细信息，请参阅 如何添加 RADIUS 身份验证服务器。

配置 **LDAP** 身份验证服务器

您可以将 Citrix ADM 配置为使用一台或多台 LDAP 服务器对用户的访问进行身份验证。LDAP 授权要求在 Active Directory、LDAP 服务器和 Citrix ADM 上使用相同的组名。字符和大小写也必须匹配。

要配置 **LDAP** 身份验证服务器，请执行以下操作：

1. 在 Citrix ADM 中，导航到 系统 > 身份验证 > **LDAP**。
2. 在 **LDAP** 页面上，单击添加。
3. 在“创建 **LDAP** 服务器”页面上，设置参数并单击“创建”将服务器添加到 LDAP 身份验证服务器列表中。以下参数是必需的：
   a) 名称。LDAP 服务器的名称。
   b) 服务器名称**/IP** 地址。LDAP 服务器的服务器名称或 IP 地址。
   c) 安全类型。系统与 LDAP 服务器之间所需的通信类型。从下拉列表中选择。如果纯文本通信无法满足要求，还可以选择加密通信，即选择传输层安全性 (TLS) 或 SSL。
   d) **Port**（端口）。默认情况下，端口 389 用于 LDAP 身份验证。如有需要，可以指定其他端口号。

e) 服务器类型。选择 **Active Directory (AD)** 或 **Novell Directory Service (NDS)** 作为 LDAP 服务器的类型。

f) 超时（秒）。Citrix ADM 系统等待 LDAP 服务器响应的时间，以秒为单位。

您可以提供其他详细信息。您还可以通过选中“验证 LDAP 证书”复选框并指定要在 证书上输入的主机名来验证 L DAP 证书。可以添加的其他一些参数包括用于针对目录服务进行查询的域名服务器 (DN) 详细信息、默认身份验证组、组属性及其他属性。

通常，在绑定 DN 的基础上删除用户名并指定用户所属组，即得到基础 DN。在“Administrator Bind DN”（管理员绑定 DN）文本框中，键入管理员绑定 DN 以用于对 LDAP 目录的查询。

基本 DN 的语法示例如下：

- ou=users,dc=ace,dc=com
- cn=Users,dc=ace,dc=com

绑定 DN 的语法示例如下：

- domain/user name
- ou=administrator,dc=ace,dc=com
- user@domain.name (for Active Directory)
- cn=Administrator,cn=Users,dc=ace,dc=com

您在 Citrix ADM 中定义的组名和用户名必须与 LDAP 服务器上配置的组名和用户名相似。

> 注意
>
> 配置 RADIUS 或 LDAP 服务器时，您可以在“详细信息”部分中输入 默认身份验证组的名称。身份验证成功时，将选择此默认组为用户授权，无论用户是否绑定到某个组。然后，用户收到基于用户是否分配到该组在此默认组和其他组上配置的权限组合。

有关如何添加 LDAP 服务器的更多详细信息，请参阅 如何添加 LDAP 身份验证服务器。

有关如何级联外部身份验证服务器的更多详细信息，请参阅 如何级联外部身份验证服务器。

配置 **TACACS** 身份验证服务器

与 RADIUS 和 LDAP 一样，TACACS 处理网络访问的远程身份验证服务。

配置 **TACACS** 身份验证服务器：

1. 在 **Citrix ADM** 中，导航到系统 > 身份验证 > **TACACS**。
2. 在 **TACACS** 页面上，单击“添加”。
3. 在创建 **TACACS** 服务器页面上，输入以下详细信息：

a) TACACS 服务器的名称。

b) TACACS 服务器的 IP 地址。

c) 端口和超时（以秒为单位）

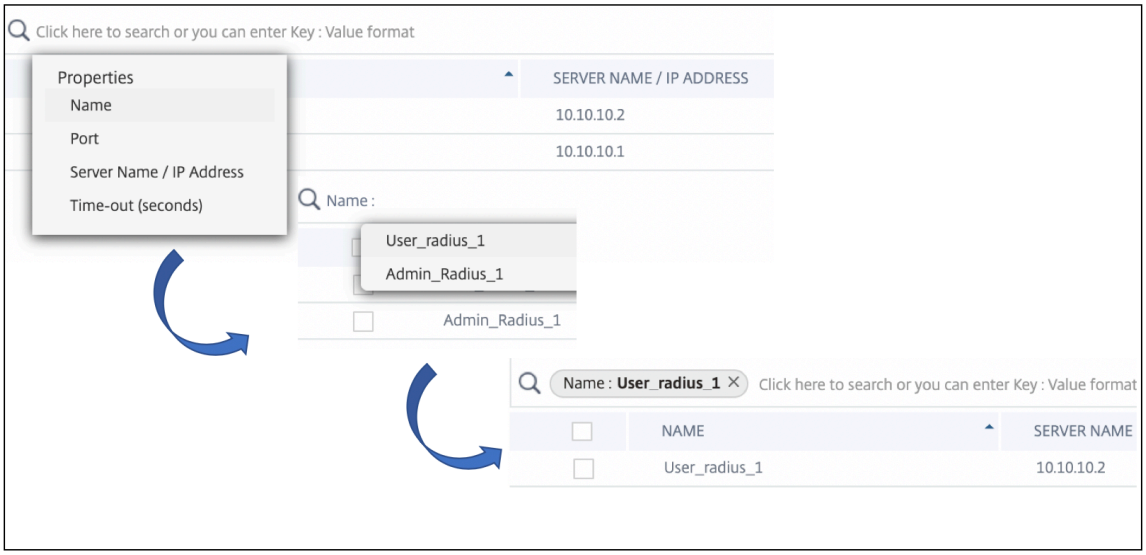
d) 系统和 TACACS 服务器共享用于通信的密钥。

e) 如果您希望设备在 TACACS 服务器上记录审核信息，请选择“会计”。

4. 单击创建。

有关如何添加 TACACS 服务器的更多详细信息，请参阅 如何添加 TACACS 身份验证服务器。

> 注意
>
> 要搜索在 Citrix ADM 中添加的身份验证服务器，请在搜索栏中单击并选择所需的搜索条件。



在 **Citrix ADM** 中配置用户的本地身份验证

如果您使用本地身份验证，请创建用户，然后将他们添加到在 Citrix ADM 上创建的组中。配置用户和组后，您可以应用授权和会话策略、创建书签、指定应用程序以及指定用户有权访问的文件共享和服务器的 IP 地址。

要在 **Citrix ADM** 中配置本地身份验证，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“身份验证”，然后单击“身份验证配置”。
2. 在“身份验证配置”页面上，从“服务器类型”下拉框中选择“本地”，然后单击“** 确定”。

在 **Citrix ADM** 中配置外部身份验证

在 Citrix ADM 中配置外部身份验证服务器时，在这些外部服务器上进行身份验证的用户组将被导入到 Citrix ADM 中。您无需在 Citrix ADM 上创建用户。用户由 Citrix ADM 在外部服务器上进行管理。但是，您必须确保在 Citrix ADM 中

保持用户组在外部身份验证服务器上的权限级别。Citrix ADM 通过分配组权限来对用户进行授权，以访问特定的负载平衡虚拟服务器和系统上的特定应用程序。如果以后从系统中删除某个身份验证服务器时，将会自动从系统中删除组和用户。

要在 **Citrix ADM** 中配置外部身份验证，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“身份验证 **”，然后单击“身份验证 ** 配置”。
2. 在“身份验证配置”页面上，从“服务器类型”下拉列表中选择“外部”。
3. 单击“插入”。
4. 在“外部服务器”页面上，选择身份验证服务器。（可选）可以选择多个身份验证服务器进行级联。

   > 注意
   >
   > 只能级联外部服务器。

5. 如果您希望在外部 身份验证失败时接管本地身份验证，请选择“启用备 用本地身份验证”。
6. 单 击“确定”关闭页面。

   所选服务器显示在“身份验证服务器”页面上。

   还可以使用服务器名称旁边的图标在列表中上下移动服务器来指定身份验证顺序。

在 **Citrix ADM** 中配置组

Citrix ADM 允许您通过创建组并将用户添加到组来对用户进行身份验证和授权。组可以具有“管理”或“只读”权限，组中的所有用户将具有相同的权限。

在 Citrix ADM 中，组被定义为具有类似权限的用户的集合。组可以有一个或多个角色。用户定义为可以具有基于分配的权限的访问权限的实体。用户可以属于一个或多个组。

您可以在 Citrix ADM 中创建本地组，并对组中的用户使用本地身份验证。如果您使用外部服务器进行身份验证，请在 Citrix ADM 上配置组，使其与内部网络中身份验证服务器上配置的组相匹配。当用户登录并通过身份验证时，如果组名与身份验证服务器上的组匹配，则用户将继承 Citrix ADM 上该组的设置。

配置组后，可以应用授权和会话策略、创建书签、指定应用程序以及指定用户有权访问的文件共享和服务器的 IP 地址。

如果您使用本地身份验证，请创建用户并将其添加到在 Citrix ADM 上配置的组中。然后，用户继承这些组的设置

> 注意
>
> 如果用户是 Active Directory 组的成员，则该组的名称和 Citrix ADM 上的用户名必须与 Active Directory 组中的用户名相同。

要在 **Citrix ADM** 中配置用户组，请执行以下操作：

1. 在 Citrix ADM 中，导航到 系统 > 用户管理 > 组。
2. 在“组 **”页面上，单击“添 ** 加”以创建组。默认情况下，在 Citrix ADM 中创建两个组，权限设置为管理员和只读。您可以向这些组添加您的用户，也可以为您的用户创建其他组。
3. 在 创建系统组页面的组 设置 选项卡上，键入组的名称，并将 角色 设置为管理员或只读。您可以选择“配置用户会话超时”来为该组登录的用户会话设置超时限制。

   > 注意
   >
   > 确保在 Citrix ADM 上创建的用户组的名称与在外部身份验证服务器上创建的用户组的名称相同。如果不同，系统将无法识别组，因此组成员将不会被提取到系统中。

4. 在“授权设置”选项卡中，选择所需的组。单击创建组。
5. 在“分配用户”选项卡中，选择要添加到组的用户。当您在 Citrix ADM 的“配置用户”中配置用户时，用户会添加到此表中。
6. 单击完成。

在系统中创建了组后，外部身份验证服务器中的所有用户都被提取到系统中。如果组名匹配外部身份验证服务器上的组名，用户会在登录系统时继承所有授权定义。

在 **Citrix ADM** 中配置用户

您可以在 Citrix ADM 上本地创建用户帐户，以补充身份验证服务器上的用户。例如，您可能要为临时用户（例如顾问或来宾）创建本地用户帐户，但不在身份验证服务器上为这些用户创建条目。如果您要对外部身份验证服务器上的用户进行本地身份验证，请确保身份验证服务器和 Citrix ADM 上都有相同的用户。

要在 **Citrix ADM** 中配置用户，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“用户管理”>“用 户”。
2. 在“** 用户”页面上，单击“添 ** 加”将 用户添加到 Citrix ADM。
3. 在 创建系统用户 页面上，设置以下参数：

   a) 用户名。用户的名称

   b) 密码。用户登录 Citrix ADM 时使用的密码

   c) 启用外部身份验证。如果未启用此功能，则用户将被验证为本地用户。

   d) 配置用户会话超时。用户可以保持活动的时间。可以分钟或小时为单位设置此时间段。

4. 在 组 ** 表格中，选择要向其添加用户的组。在 Citrix ADM 的配置用户组中配置组时，组成员将添加到此表中。
5. 单击创建。

> 注意
>
> 如果用户在 Active Directory 上，请确保 Citrix ADM 中的组名与外部服务器上 Active Directory 组的组名相同。

如何提取身份验证服务器组

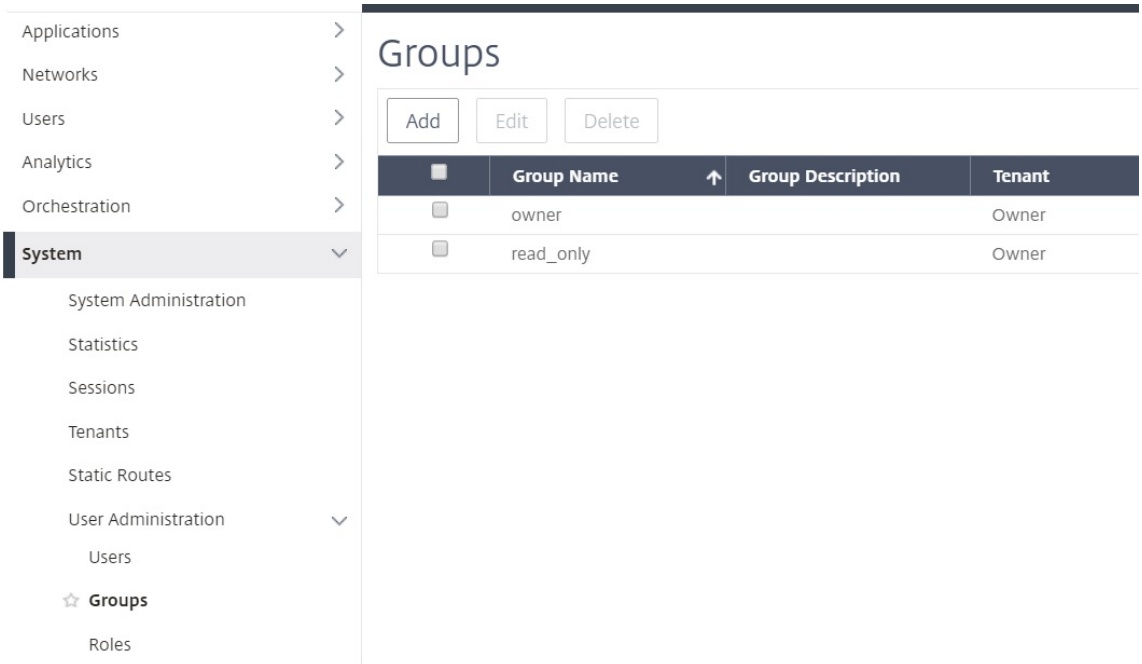
February 6, 2024

Citrix Application Delivery Management (ADM) 允许您提取外部身份验证服务器上存在的用户组，并根据他们的角色需求和 Citrix ADC 定义为他们分配权限。这有两个优势：

1. 您不必在 Citrix ADM 上创建用户。尽管这些组已提取到 Citrix ADM 服务器中，但它们是在 Citrix ADM 的外部服务器上进行管理的，而不是将它们添加到系统中。
2. Citrix ADM 通过为系统上的特定应用程序分配访问特定负载平衡器虚拟服务器的组权限来执行用户授权。将来，从系统删除特殊身份验证服务器时，会自动从系统删除组和用户。

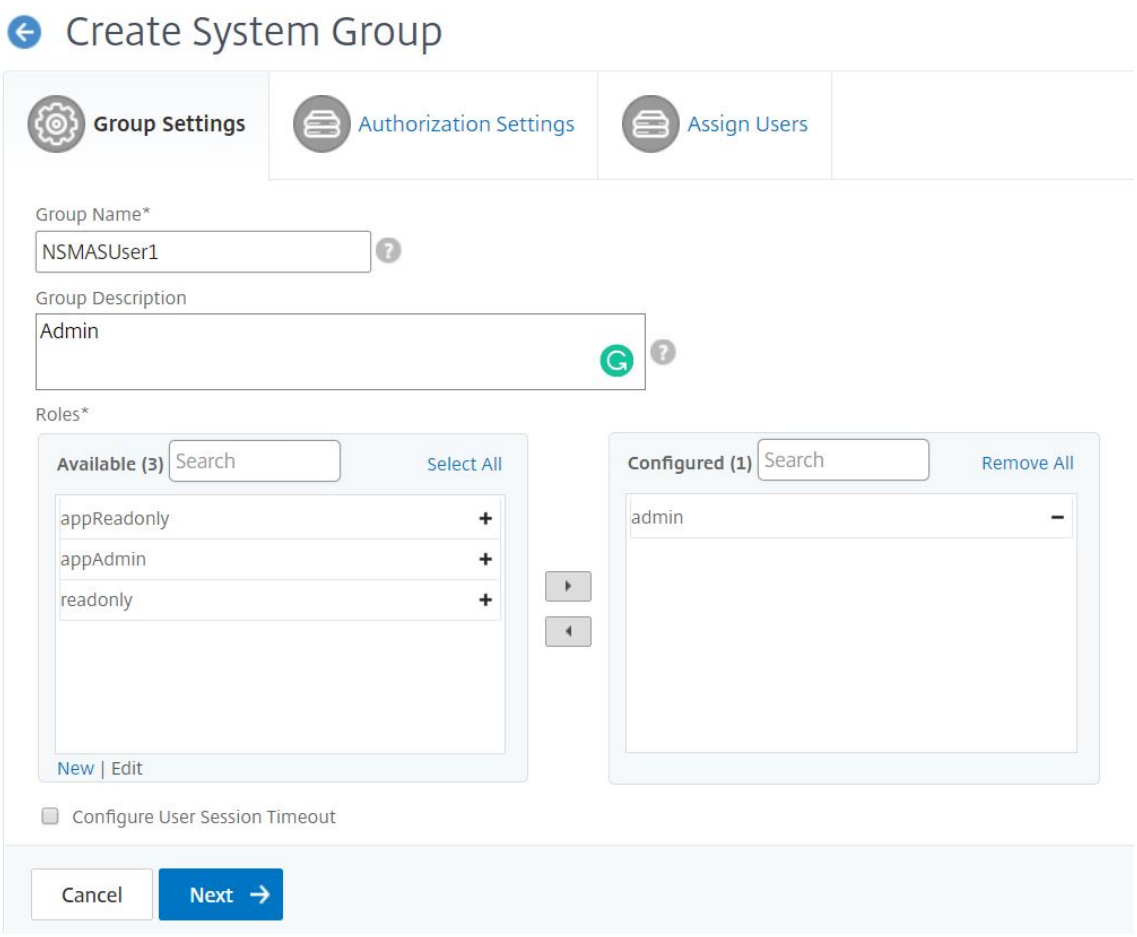
配置组和分配组权限

1. 在 Citrix ADM 中，导航到 系统 > 用户管理 > 组。
2. 单击“添加”创建组。



3. 在“组设置”选项卡中，键入组名称，将权限设置为管理员、只读、AppReadOnly 或 AppAdmin。可以配置的其他选项为会话超时，在其中可以设置该组的用户登录的会话的超时限制，还可以设置组成员可以访问的 VM 实例。

> 注意
>
> 确保在 Citrix ADM 上创建的用户组名称与在外部身份验证服务器上创建的用户组名称完全相同。如果不同，系统将不会识别组，且组成员将不会被提取到系统中。



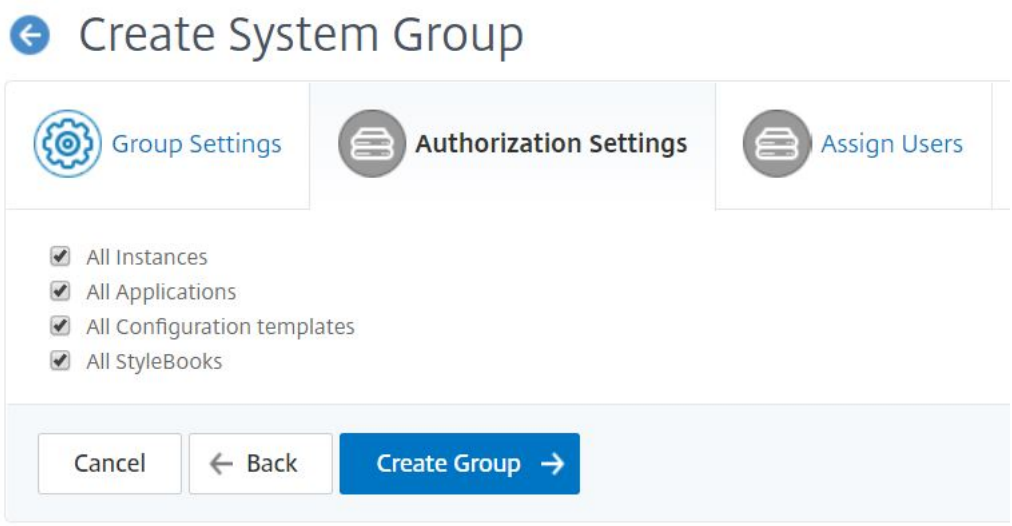
4. 在 授权设置 选项卡中，您可以为以下四个组提供授权设置：

   - 实例
   - 应用程序
   - 配置模板
   - 样书

默认情况下，您的用户可以访问上述所有组。您可以清除复选框并为每个组提供选择性访问权限。

例如：

- 您可以清除“实例”复选框并仅选择要向用户提供访问权限的必需实例。
- 清除“所有应用程序”复选框并仅选择所需的应用程序和模板。在 Citrix ADM 中向组中添加应用程序时，可以使用正则表达式搜索和添加符合组正则表达式条件的应用程序。绑定到这些组的用户只能访问这些特定的应用程序。指定的正则表达式保留在 Citrix ADM 中。也就是说，Citrix ADM 允许将添加正则表达式文本框中提供的正则表达式存储在系统中，并在新应用程序满足此正则表达式时动态更新授权范围。向系统中添加新应用程序时，Citrix ADM 会将搜索条件应用于新应用程序，符合条件的应用程序将动态添加到组中。您不必手动将新应用程序添加到该组中。应用程序在系统中动态更新，相应的组用户可以在 Citrix ADM 的相应模块下查看应用程序。
- 清除“所有配置模板”复选框以仅允许访问所需的模板。
- 清除“所有样书”复选框，然后选择您的用户可以访问的必需样书。
- 您可以在创建组并将用户添加到该组时选择所需的样书。当用户选择允许的样书时，也会选择所有相关样书。该样书的配置包也包含在用户有权访问的内容中。



在系统中创建了组后，外部身份验证服务器中的所有用户都被提取到系统中。您可以通过选择组并单击“编辑”来进行检查。“Create System Group”（创建系统组）中的“Users”（用户）表显示与组连接的用户列表。您也可以在“分配用户”选项卡中将用户分配到组。

如果组名匹配外部身份验证服务器上的组名，用户会在登录系统时继承所有授权定义。

添加 **LDAP** 身份验证服务器

February 6, 2024

将 LDAP 协议与 RADIUS 和 TACAS 身份验证服务器集成时，可以使用 Citrix ADM 搜索和验证分布式目录中的用户凭据。

1. 导航到“系统”>“身份验证”。
2. 选择“**LDAP**”选项卡，然后单击“添加”。
3. 在 创建 **LDAP** 服务器 页面上，指定以下参数：

   a) 名称 -指定 LDAP 服务器名称

   b) 服务器名称**/IP** 地址 -指定 LDAP IP 地址或服务器名称

   c) 安全类型 -系统与 LDAP 服务器之间所需的通信类型。从列表中选择。如果纯文本通信不足，则可以通过选择传输层安全 (TLS) 或 SSL 来选择加密通信

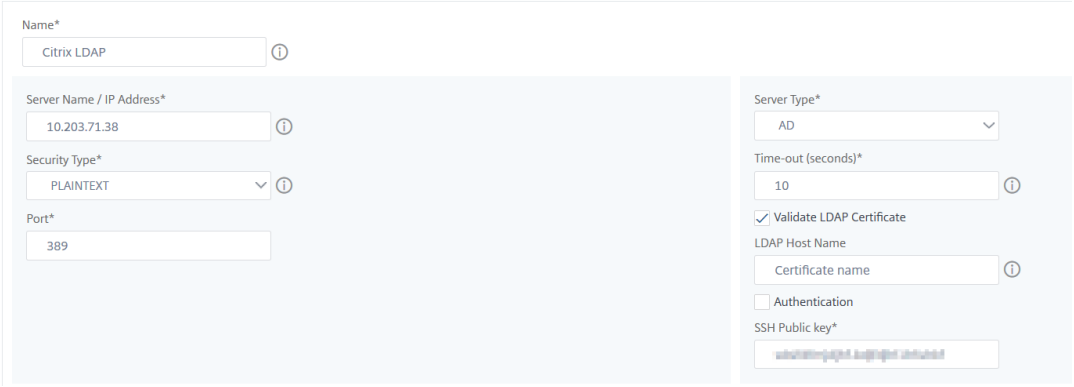
   d) 端口—默认情况下，端口 389 用于普通文本。您也可以为 SSL/TSL 指定端口 636

   e) 服务器类型—选择 Active Directory (AD) 或 Novell Directory Service (NDS) 作为 LDAP 服务器的类型

   f) 超时（秒）—Citrix ADM 系统等待 LDAP 服务器响应的时间（以秒为单位）

   g) **LDAP** 主机名 -选中“验证 LDAP 证书”复选框并指定要在证书上输入的主机名

   清除“身份验证”选项并指定 SSH 公钥。使用基于密钥的身份验证，您可以获取存储在用户对象上的公钥列表。这些公钥通过 SSH 存储在 LDAP 服务器中。



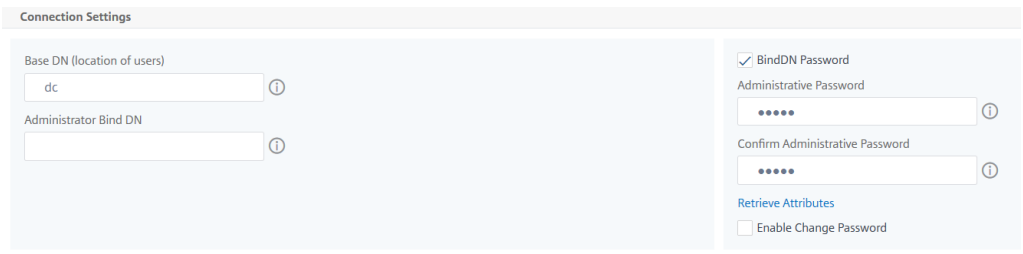
   在“连接设置”下，指定以下参数：

   i. 基本 **DN** —LDAP 服务器开始搜索的基本节点

   ii. 管理员绑定 **DN** —绑定到 LDAP 服务器的用户名。例如，admin@aaa.local。

   iii. 绑定 **DN** 密码 -选择此选项可提供用于身份验证的密码

   iv. 启用更改密码 -选择此选项可启用密码更改



在“其他设置”下，指定以下参数

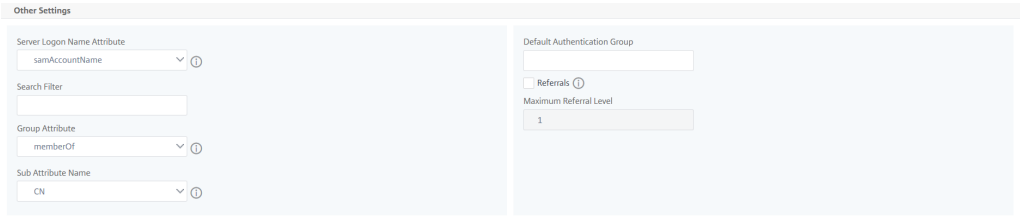
i. 服务器登录名称属性 -系统用于查询外部 LDAP 服务器或 Active Directory 的名称属性。从列表中选择 **samAccountname**。

ii. 搜索筛选 器—根据 LDAP 服务器中配置的搜索筛选器配置外部用户进行双重身份验证。例如，使用 ldaploginame samaccount 和用户提供的用户名 bob 的 vpnallowed=true 会生成 LDAP 搜索字符串为: &(vpnallowed=**true**)(samaccount=bob)。

iii. 组属性—从列表中选择成员。

iv. 子属性名称—从 LDAP 服务器提取组的子属性名称。

v. 默认身份验证组 -除提取的组外，还可选择身份验证成功时的默认组。



4. 单击创建。

LDAP 服务器现已配置完毕。

> 注意
>
> 如果用户是 Active Directory 组成员，则该组和 Citrix ADM 上的用户名必须具有相同的 Active Directory 组成员的名称。

如何启用回退本地身份验证

February 6, 2024

使用回退本地身份验证功能，在外部身份验证失败时，可以进行本地身份验证。即使配置的外部身份验证服务器已关闭或无法访问，在 Citrix Application Delivery Management (ADM) 和外部身份验证服务器上配置的用户也可以登录 Citrix ADM。为了回退本地身份验证发挥作用，请确保这三个因素：

- 即使外部身份验证服务器出现故障，您也应该能够访问 Citrix ADM。
- 应在 Citrix ADM 和外部身份验证服务器上同时进行配置。
- 您应该至少添加一个外部服务器。

要启用回退本地身份验证，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“身份验证 **”，然后单击“身份验证 ** 配置”。

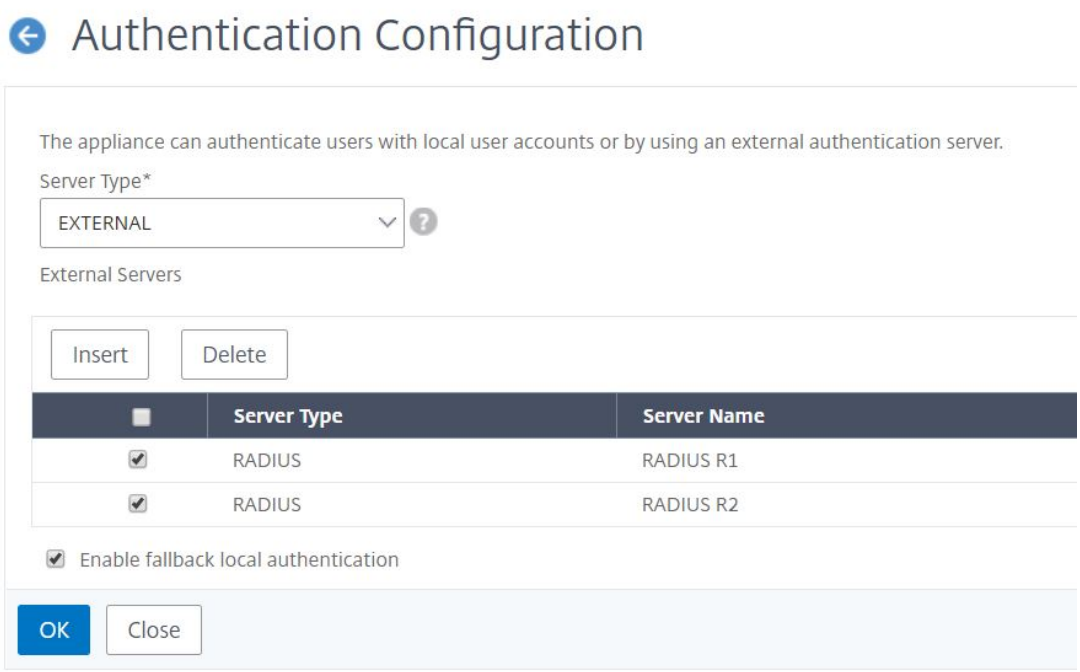
2. 从“服务器类型”列表中选择“外部”。

> 注意 如果从列表中选择 **LOCAL**，则用户身份验证将在默认的本地身份验证服务器上进行。

3. 单击“插入”，从显示的外部服务器列表中选择一个外部服务器，然后单击“确定”添加外部服务器。

> 注意 在执行此步骤之前，您应该已经添加了外部服务器，以使它们出现在列表中。有关如何添加外部服务器的详细信息，请参阅以下文章：
>
> - 如何添加 Radius 服务器
> - 如何添加 LDAP 服务器
> - 如何添加 TACACS 服务器

4. 选择“启用 备用本地身份验证 ”选项。



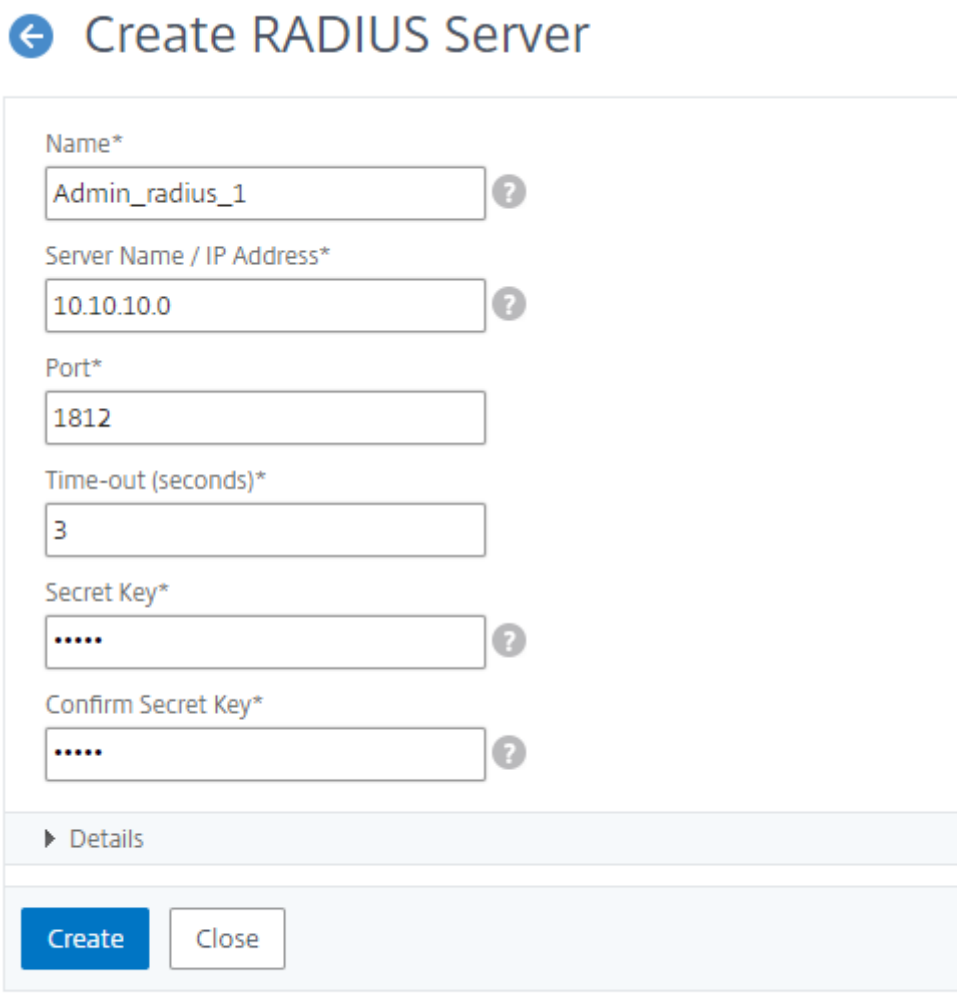
如何添加 **RADIUS** 身份验证服务器

February 6, 2024

RADIUS 身份验证服务器通过使用用户数据报协议 (UDP) 运行。RADIUS 服务器接收用户的连接请求，对用户进行身份验证。然后，服务器将配置信息返回给向用户提供服务的系统。RADIUS 服务器连接至网络访问服务器 (NAS)。NAS 发送访问请求 (Access-Request) 时，RADIUS 服务器在其数据库中搜索用户名和其他详细信息。如果数据库中不存在该用户名，RADIUS 服务器会立即发送访问拒绝消息，或者可以在 Citrix ADM 上加载默认配置文件。在 RADIUS 中，身份验证和授权是结合在一起的。如果用户详细信息通过了身份验证，RADIUS 服务器将返回访问接受 (Access-Accept) 响应。它还会发送属性-值对列表，说明要用于特定会话的参数。

配置 **RADIUS** 身份验证服务器

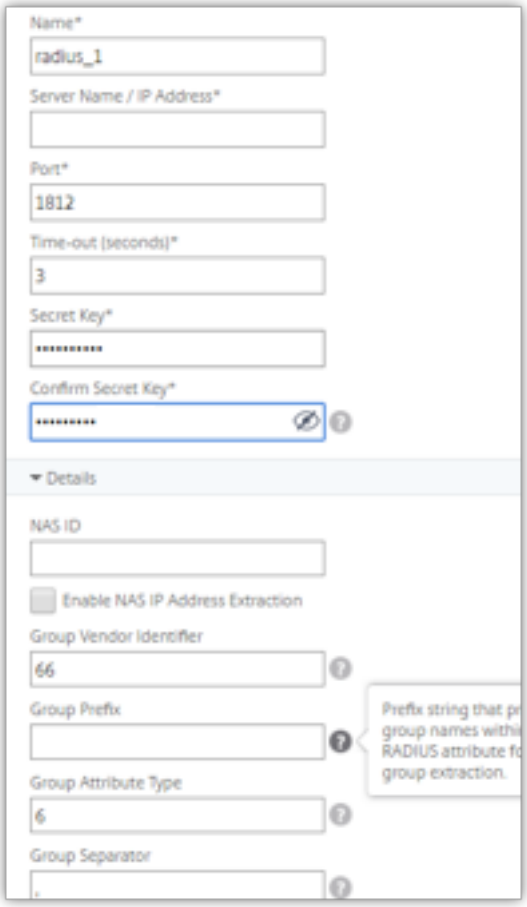
1. 在 Citrix ADM 中，导航到系统 > 身份验证 > **RADIUS**。
2. 在 **RADIUS** 页面上，单击“添加”。
3. 在“创建 **RADIUS** 服务器”页面上，设置参数，然后单击“创建”将服务器添加到 RADIUS 身份验证服务器列表中。
4. 以下参数是创建 RADIUS 服务器的必备参数：
    - 名称—键入 RADIUS 服务器的名称
    - 服务器名称**/IP** 地址—键入服务器名称或 RADIUS 服务器的 IP 地址
    - 端口—默认情况下，端口 1812 用于 RADIUS 身份验证消息。如有必要，您可以指定其他端口号。
    - 超时（秒）—键入秒数。Citrix ADM 系统等待 RADIUS 服务器响应的时间。
    - 密钥—键入任何字母数字表达式。在 Citrix ADM 和 RADIUS 服务器之间共享的用于通信的密钥。
5. 单击“详细信息”展开该部分并设置其他参数。



在添加 RADIUS 服务器时，您可以提供更多可选详细信息。可以输入的其他一些参数包括 NAS 详细信息、供应商信息、属性信息及密码身份验证类型。

> 注
>
> 意要使 RADIUS 身份验证生效，请确保在 Citrix ADM 上配置的组与通过 RADIUS 用户提取的组相同。根据分配给组的权限对用户进行授权。
>
> 例如，以 FreeRadius 服务器中的一个场景为例，其中，
>
> - 明文密码 = “1.citrix”
> - 组名称 = “radiusgroup1，group1”
>
> 在这种情况下，用户属于两个组：radiusgroup1 和 group1。在这种情况下，组分隔符为 “

,” 如果您以属于 “radiusgroup1” 组的 RADIUS 用户 “radiusUser1” 身份登录 Citrix ADM，请确保在 Citrix ADM 上也配置相同的组名 “radiusgroup1”。



像提供有关供应商 ID、属性类型、组分隔符（如果适用）的详细信息，以便进行组提取，如下图所示。

```
#
# Created for Citrix Use

# currently only using attribute 6 in this setup.

VENDOR Citrix 66


BEGIN-VENDOR Citrix
ATTRIBUTE Group-Names 6 string
END-VENDOR Citrix
```

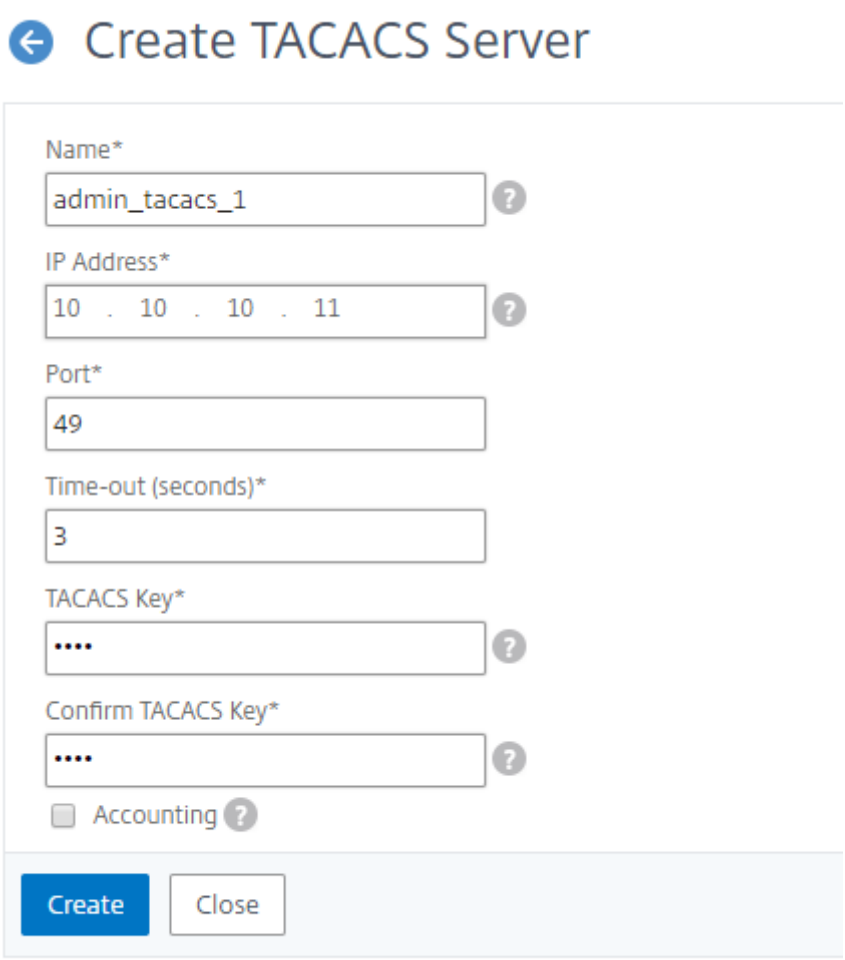
如何添加 **TACACS** 身份验证服务器

February 6, 2024

TACACS 与 RADIUS 和 LDAP 一起处理网络访问的远程身份验证服务。

配置 **TACACS** 身份验证服务器

1. 在 **Citrix ADM** 中，导航到 系统 > 身份验证 > **TACACS**。
2. 在 **TACACS** 页面上，单击“添加”。
3. 在 创建 **TACACS** 服务器 页面上，输入以下详细信息：
    a) TACACS 服务器的名称。
    b) TACACS 服务器的 IP 地址。
    c) 端口和超时（以秒为单位）
    d) 键入系统和 TACACS 服务器共享用于通信的密钥。
4. 如果您希望设备在 TACACS 服务器上记录审核信息，请选择“记账”。
5. 单击创建。



如何级联外部身份验证服务器

February 6, 2024

Citrix Application Delivery Management (ADM) 支持统一的身份验证、授权和记账 (AAA) 协议系统，包括 RADIUS、LDAP 和 TACACS，此外还支持本地服务器对本地用户和组进行身份验证。该统一支持提供公用接口来对访问系统的所有本地和外部 AAA 客户端进行身份验证和授权。无论用户要与系统通信的实际协议如何，Citrix ADM 都可以对用户进行身份验证。

级联外部身份验证服务器提供持续无故障的外部用户身份验证和授权处理。如果第一个身份验证服务器上的身份验证失败，Citrix ADM 将尝试使用第二个外部身份验证服务器对用户进行身份验证，依此类推。要启用级联身份验证，需要将外部身份验证服务器添加到 Citrix ADM。可以添加任何类型的受支持的外部身份验证服务器（RADIUS、LDAP 和 TACACS）。例如，如果要添加四个外部身份验证服务器用于级联身份验证，可以添加两个 RADIUS 服务器、一个 LDAP

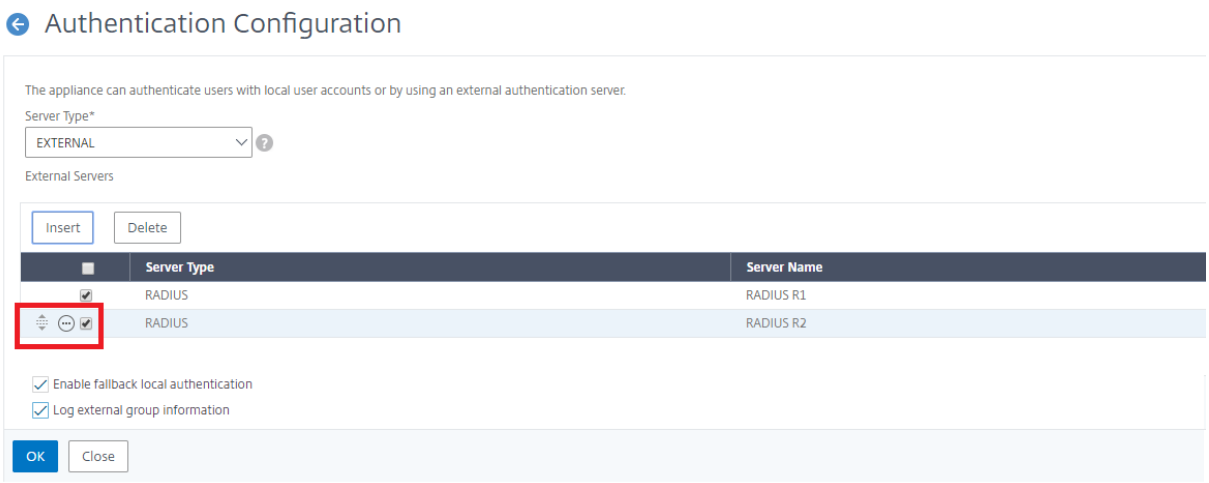
服务器和一个 TACACS 服务器，或者所有服务器都可以是 RADIUS 类型。您可以在 Citrix ADM 中配置多达 32 个外部身份验证服务器。

配置级联外部身份验证服务器

1. 在 Citrix ADM 中，导航到“系统”>“身份验证”。
2. 在“身份验证”页面上， 单击“身份验证配置”。
3. 在“身份验证配置”页面上，从“服务器类型”下拉列表中选择“外部”（只能级联外部服务器）。
4. 单击“插入”，然后在“外部服务器”页面上，选择要级联的一个或多个身份验证服务器。
5. 如果您希望在外部 身份验证失败时接管本地身份验证，请选择“启用备 用本地身份验证”。
6. 单 击“确定”关闭页面。

所选服务器显示在“外部服务器”下，如下图所示。

还可以使用服务器名称旁边的图标在列表中上下移动服务器来指定身份验证顺序。



访问控制

February 6, 2024

身份验证是验证某人是否属实的过程。为了执行身份验证，用户必须已在身份验证机制可以查询的系统中创建了帐户，或必须在首次身份验证过程中创建帐户。Citrix Application Delivery Management (ADM) 提供了一种对本地用户和外部用户进行身份验证的方法。虽然本地用户需要进行内部身份验证，但 Citrix ADM 支持通过 RADIUS、LDAP 和 TACACS 协议进行外部身份验证。当用户尝试访问配置为外部身份验证的 Citrix ADM 时，请求的应用程序服务器将用户名和密码发送到 RADIUS、LDAP 或 TACAS 服务器进行身份验证。通过身份验证后，在 Citrix ADM 中使用所需的协议识别用户。

访问控制是对特定资源强制实施所需安全的过程。它是用于控制哪些人可以查看或使用计算环境中的资源的安全技术。访问控制的目的是限制计算机系统的合法用户可以执行的操作。访问控制约束用户可以直接执行的操作，以及允许代表用户执行的程序执行的操作。这样，访问控制可尽力阻止可能导致违反安全的活动。访问控制假定在通过参考监视器强制实施访问控制之前已成功完成用户的身份验证。Citrix ADM 允许细化的基于角色的访问控制 (RBAC)，管理员通过它可以根据企业中各个用户的角色为用户提供访问权限。Citrix ADM 中的 RBAC 是通过创建访问策略、角色、组和用户来实现的。

基于角色的访问控制

February 6, 2024

Citrix Application Delivery Management (ADM) 提供精细的、基于角色的访问控制 (RBAC)，您可以根据企业内个人用户的角色授予访问权限。在此上下文中，访问是指能够执行特定任务，例如，查看、创建、修改或删除文件。角色是根据企业中用户的授权和职责进行定义。例如，可以允许一个用户执行所有网络操作，而另一个用户可以观察应用程序中的通信流以及协助创建配置模板。

角色由策略决定。创建策略后，即可创建角色、将每个角色绑定到一个或多个策略以及为用户分配角色。您还可以为用户组分配角色。

组是拥有共同权限的用户集合。例如，管理特定数据中心的用户可以分配到一个组。角色是根据特定情况授予用户或组的身份。在 Citrix ADM 中，创建角色和策略特定于 Citrix ADC 中的 RBAC 功能。可以根据企业逐步发展的需求轻松地创建、更改或停用角色和策略，而无需单独更新每个用户的权限。

角色可以基于功能，也可以基于资源。例如，假定一个 SSL/安全管理员和一个应用程序管理员。SSL/安全管理员对 SSL 证书管理和监视功能必须拥有完整访问权限，但对系统管理操作应该拥有只读访问权限。应用程序管理员应该只能访问其范围内的资源。

示例：

ADC 集团负责人 Chris 是其组织中 Citrix ADM 的超级管理员。他创建三个管理员角色：安全管理员、应用程序管理员和网络管理员。

安全管理员 David 对 SSL 证书管理和监视必须拥有完整访问权限，但对系统管理操作应该拥有只读访问权限。

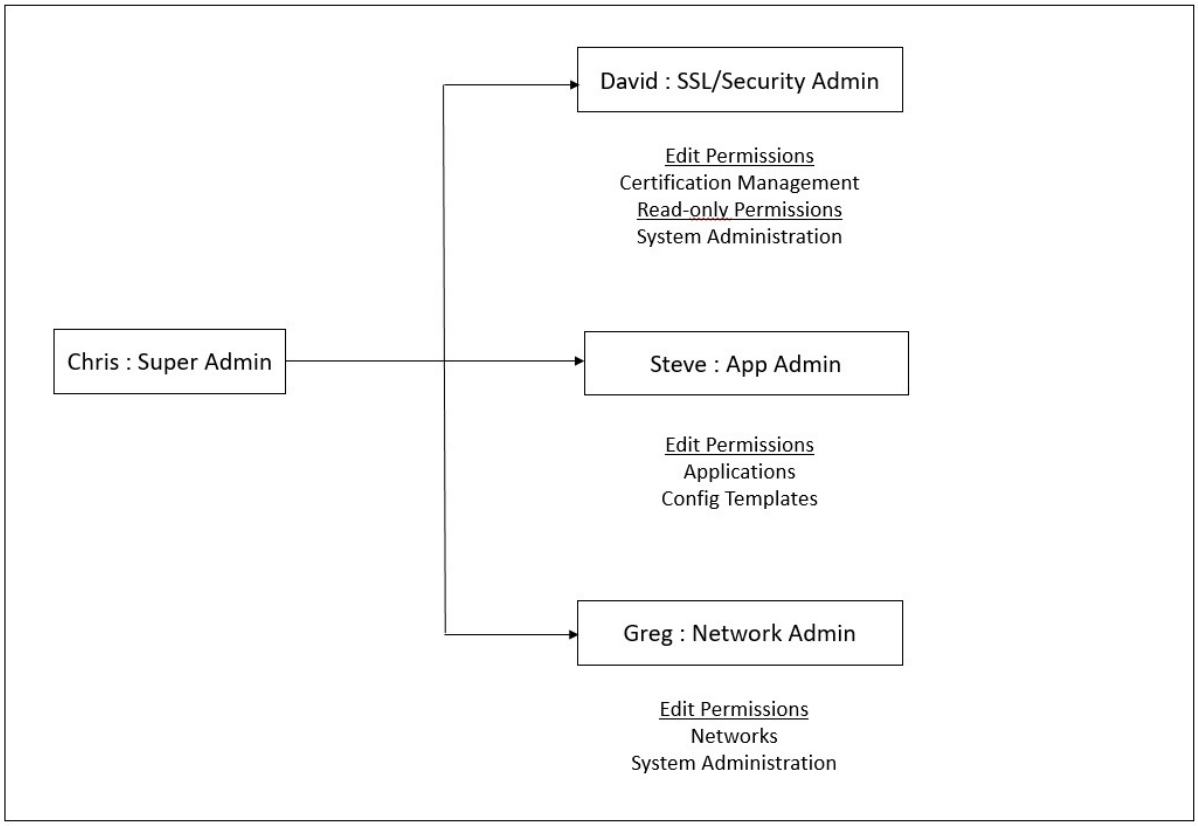
应用程序管理员 Steve 需要只对特定应用程序和特定配置模板拥有访问权限。

网络管理员 Greg 需要访问系统和网络管理的权限。

Chris 还必须为所有用户提供 RBAC，无论用户是本地、外部还是多租户。

Citrix ADM 用户可以通过本地身份验证，也可以通过外部服务器（RADIUS/LDAP /TACAS）进行身份验证。RBAC 设置必须适用于所有用户，无论采用的身份验证方法是什么。

下图显示了管理员和其他用户拥有的权限以及他们在组织中的角色。



限制

以下 Citrix ADM 功能不完全支持 RBAC：

- 分析-分析 模块中不完全支持 RBAC。在 Web Insight、SSL Insight、Gateway Insight、HDX Insight 和 Security Insight 分析模块中，RBAC 支持限于实例级别，不适用于应用程序级别。例如：

示例 **1**：基于实例的 RBAC（支持）

分配了几个实例的管理员只能在 **Web Insight** > 实例下看到这些实例，只能在 **Web Insight** > 应用程序下看到相应的虚拟服务器，因为实例级别支持 RBAC。

示例 **2**：基于应用程序的 RBAC（不支持）

分配了几个应用程序的管理员可以在 **Web Insight** > 应用程序 下查看所有虚拟服务器，但无法访问它们，因为应用程序级别不支持 RBAC。

- 样书—样书不完全支持 RBAC。
  - 在 Citrix ADM 中，样书和配置包被视为单独的资源。可以为样书和配置包单独或并行提供访问权限（查看和/或编辑）。对配置包的查看或编辑权限隐式允许用户查看样书，这对于获取配置包详细信息和创建新配置包必不可少。

  - 不支持特定样书或配置包的访问权限
    示例：如果实例上已有配置包，则用户可以修改目标 Citrix ADC 实例上的配置，即使他们没有该实例的访问权限也是如此。

- 调配 -调配不支持 RBAC。

配置访问策略

February 6, 2024

访问策略定义权限。一个策略可以应用于一个用户或组，也可以应用于多个用户和多个组。Citrix Application Delivery Management (ADM) 提供四种预定义的访问策略：

1. 管理员政策。授予访问所有 Citrix ADM 功能的权限。用户具有查看和编辑权限，可以查看所有 Citrix ADM 内容，并可以执行所有编辑操作。即，用户可以对资源执行添加、修改和删除操作。
2. **readonlypolicy**。授予只读权限。用户可以查看 Citrix ADM 上的所有内容，但无权执行任何操作。
3. **appAdminPolicy**。授予用于访问 Citrix ADM 中应用程序功能的管理权限。绑定到此策略的用户可以添加、修改和删除自定义应用程序，并可以启用或禁用服务、服务组和各种虚拟服务器，例如，内容切换、缓存重定向和 HAProxy 虚拟服务器。
4. **appReadOnlyPolicy**。授予对应用程序功能的只读权限。绑定到此策略的用户可以查看应用程序，但不能执行任何添加、修改或删除、启用或禁用操作。

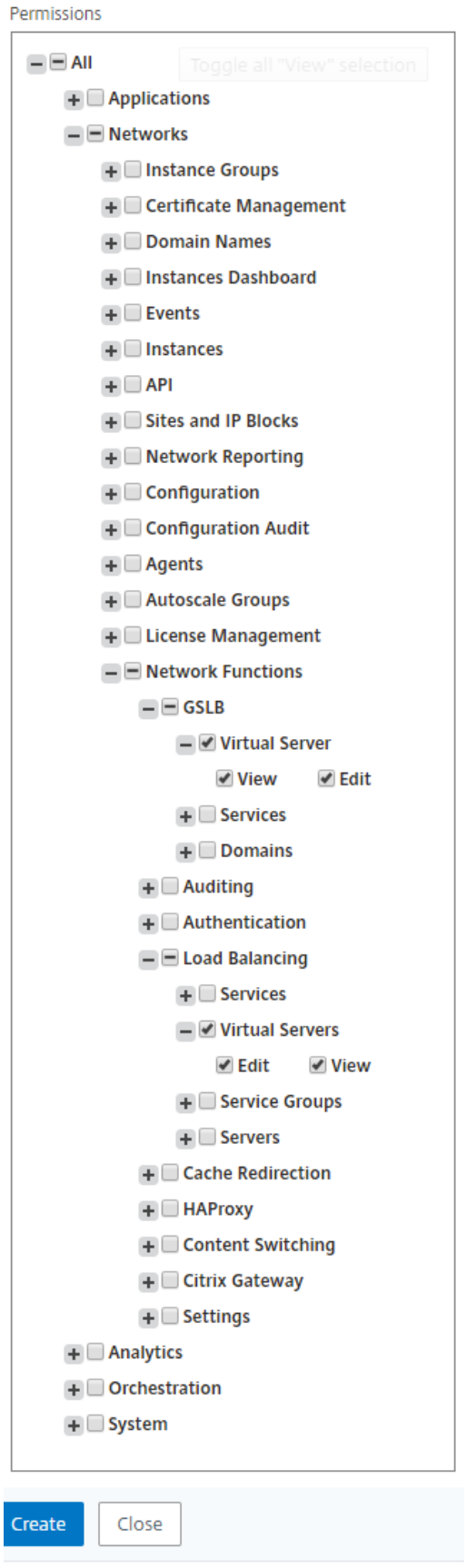
> 注意 无法编辑预定义的策略。

您还可以创建自己（用户定义）的策略。

要创建用户定义访问策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“用户管理”>“访问策略”。
2. 单击添加。
3. 在 策略名称 字段中，输入策略的名称，然后在 策略描述字段中输入描述。
4. 权限部分列出了所有 Citrix ADM 功能，以及用于指定只读权限或编辑权限的选项。单击 (+) 图标将每个功能组展开为多个功能。必须选中功能名称旁边的复选框才能向用户授予查看或编辑权限。Edit（编辑）选项包含查看权限。选择“查看”以获得只读权限，或选择“编辑”以获得完全访问权限。

   > 注意 展开负载平衡和 GSLB 以查看更多配置选项。

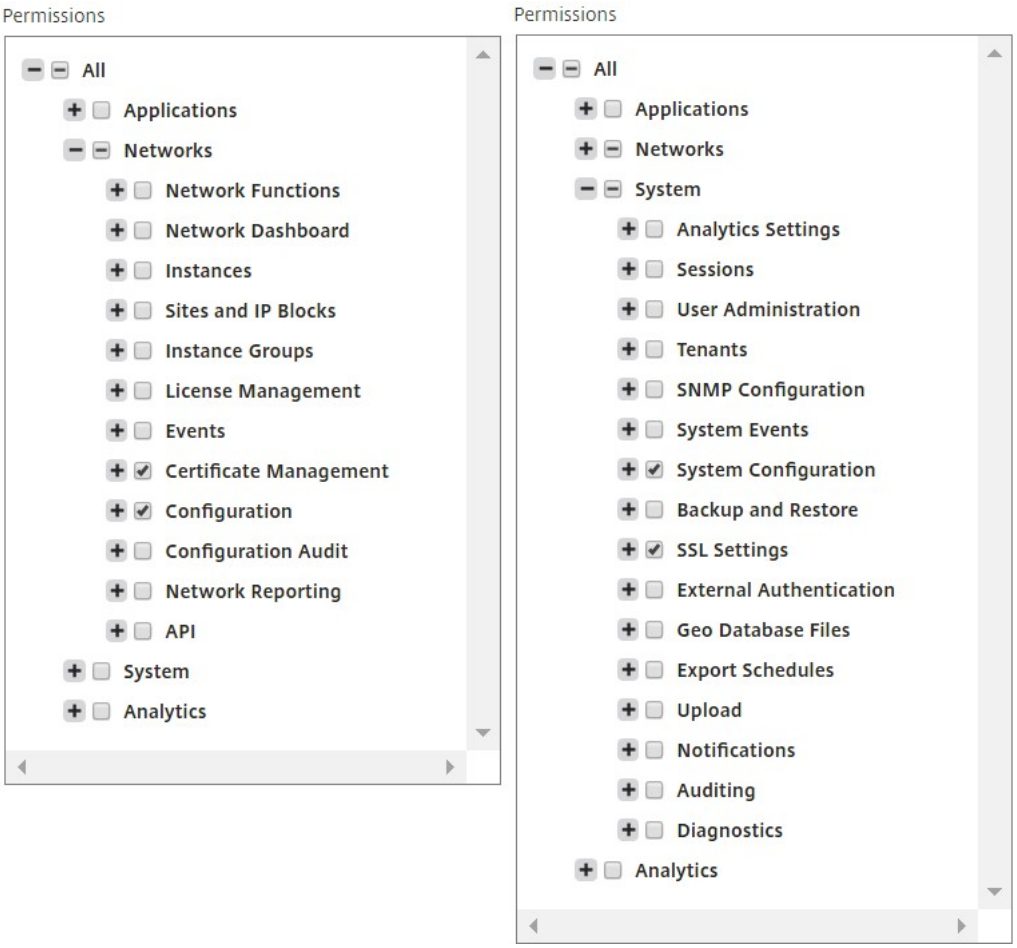


> 注意 选择“编辑”可能会在内部分配未在“权限”部分显示为已启用的依赖 权限。例如，为故障管理启用编辑权限时，Citrix ADM 会在内部提供配置邮件配置文件或创建 SMTP 服务器设置的权限，以便用户可以将报表作为邮件发送。

示例：

David 是 Citrix ADM 中 SSL 证书管理/安全的管理员。在分配给 David 的策略中，管理员在“权限”部分选中以下复选框：

- 网络 > 配置 > 编辑
- 网络 > 证书管理 > 编辑
- 系统 > **SSL** 设置 > 编辑
- 系统 > 系统配置 > 编辑



5. 单击创建。

配置组

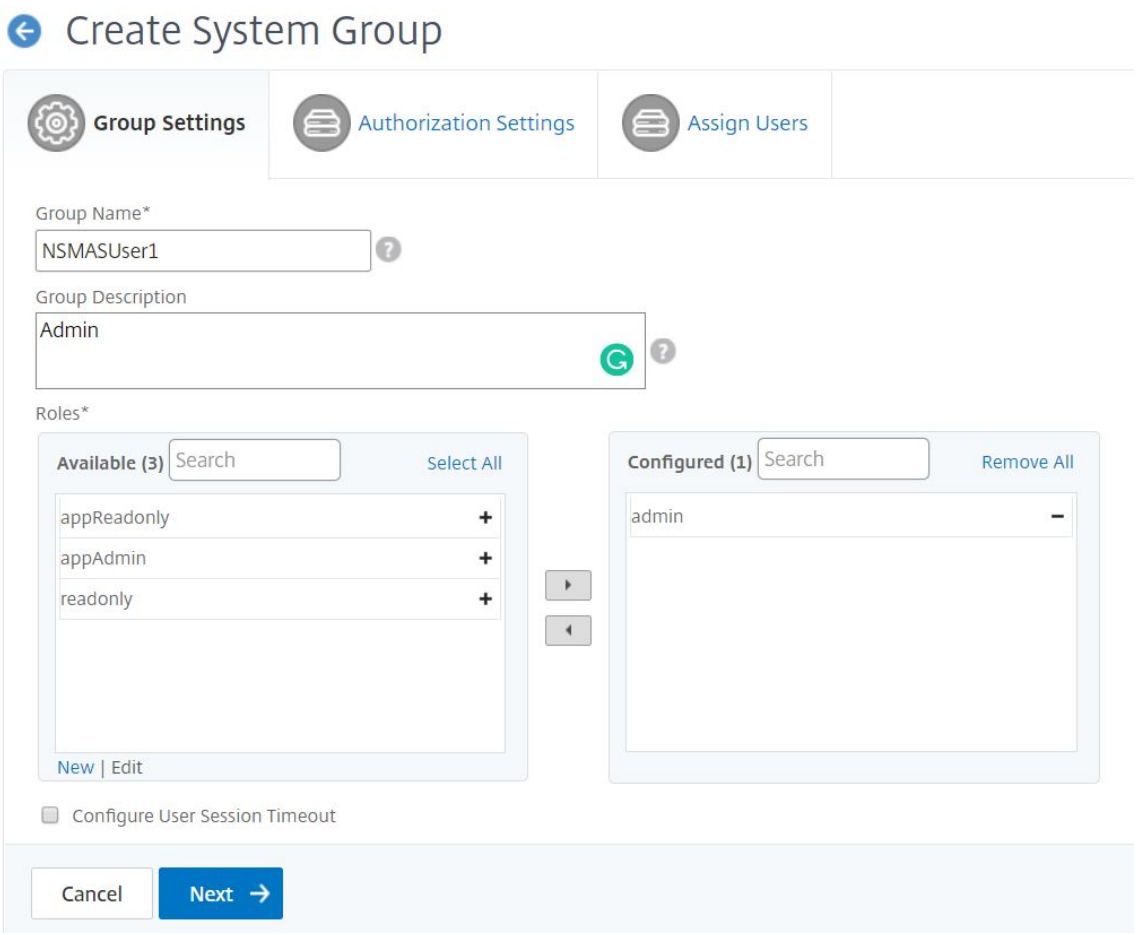
February 6, 2024

在 Citrix Application Delivery Management (ADM) 中，组可以同时拥有功能级和资源级访问权限。例如，一组用户可能只能访问选定的 Citrix ADC 实例；另一组用户只能访问选定的几个应用程序，依此类推。创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。该组中的所有用户都在 Citrix ADM 中分配相同的访问权限。

要创建用户组并为用户组分配角色，请执行以下操作：

1. 在 Citrix ADM 中，导航到 系统 > 用户管理 > 组。
2. 单击添加。
3. 在 组名称 字段中，输入组的名称。
4. 在“组描述”字段中，键入组的描述。对小组进行良好的描述有助于您在以后更好地了解该组的角色和职能。
5. 在“角色”部分中，将一个或多个角色添加或移动到“已配置”列表中。

   > 注意 在“可用”列表下，您可以单击“新建”或“编辑”，然后创建或修改角色。或者，您可以导航到“系统”>“用户管理”>“用 户”，然后创建或修改用户。



> 注意
>
> 您可以通过单击“新建”来创建新角色，也可以导航到“系统”>“用户管理”>“用户”，然后通过此屏幕创建新用户。

6. 单击下一步。在授权设置选项卡上，您可以为以下四个组提供授权设置：

   - 实例
   - 应用程序
   - 配置模板
   - 样书

   默认情况下，您的用户可以访问上述所有组。您可以清除复选框并为每个组提供选择性访问权限。

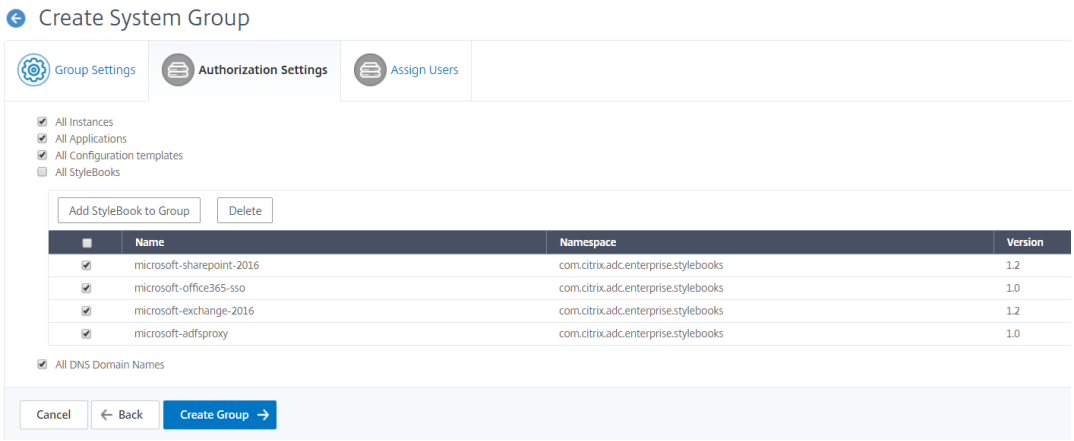
   例如：

   - 您可以清除“实例”复选框并仅选择要向用户提供访问权限的必需实例。
   - 清除“所有应用程序”复选框并仅选择所需的应用程序和模板。在 Citrix ADM 中向组中添加应用程序时，可以使用正则表达式搜索和添加符合组正则表达式条件的应用程序。绑定到这些组的用户只能访问这些特

定的应用程序。指定的正则表达式保留在 Citrix ADM 中。也就是说，Citrix ADM 允许将添加正则表达式文本框中提供的正则表达式存储在系统中，并在新应用程序满足此正则表达式时动态更新授权范围。向系统中添加新应用程序时，Citrix ADM 会将搜索条件应用于新应用程序，符合条件的应用程序将动态添加到组中。您不必手动将新应用程序添加到该组中。应用程序在系统中动态更新，相应的组用户可以在 Citrix ADM 的相应模块下查看应用程序。

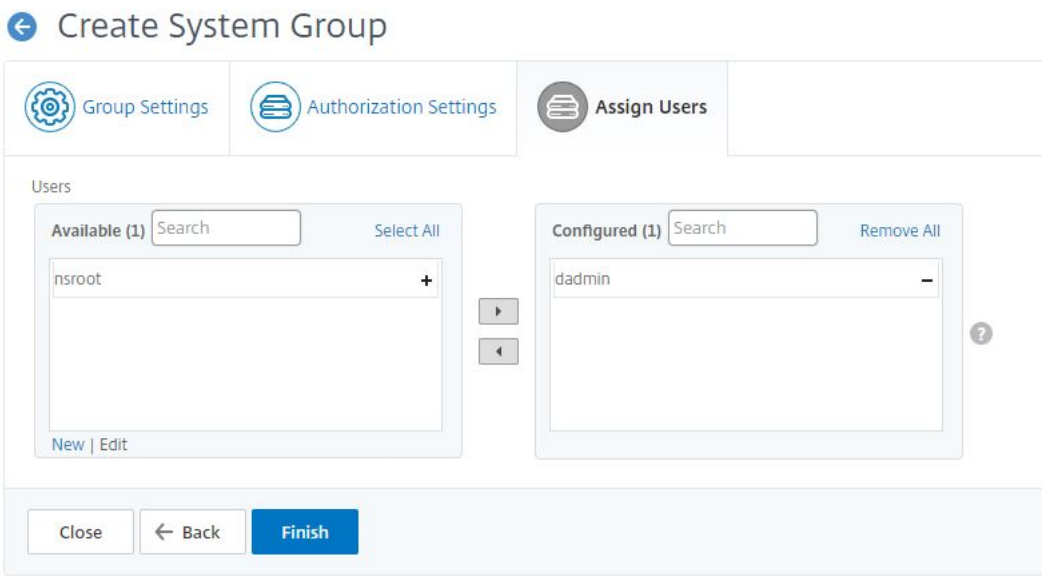
- 清除“所有配置模板”复选框以仅允许访问所需的模板。
- 清除“所有样书”复选框，然后选择您的用户可以访问的必需样书。

  您可以在创建组并将用户添加到该组时选择所需的样书。当用户选择允许的样书时，也会选择所有相关样书。该样书的配置包也包含在用户有权访问的内容中。



- 清除“所有 **DNS** 域名”复选框，然后从列表中添加您希望用户访问的域名。

7. 单击创建组。
8. 在“分配用户”选项卡中，从“可用”列表中选择用户，然后将该用户添加到“已配置”列表中。例如，“dadmin”。



> 注意 您也可以通过单击“新建”来添加 新用户。

9. 单击完成。

> 注意
>
> 作为 Citrix ADM 管理员，您可以根据 RBAC 中的访问策略设置向您的用户提供单个 ADM 模块 UI 的“仅限查看”权限或“查看和编辑”权限。如果将用户分配到两个或多个组，也就是说，如果用户在内部映射到多个授权范围和多个访问策略，则 ADM 会合并所有这些组的权限并相应地对用户进行授权。
>
> 例如，假设 User1 被分配到具有两个访问策略（P1 和 P2）的组。每种策略都有不同的权限类型。P1 具有“只读”权限，而 P2 具有“查看和编辑”权限。您希望您的用户查看一组作为 P1 策略一部分的应用程序，并编辑另一组作为 P2 策略一部分的应用程序。但是，作为默认行为，Citrix ADM 将两种权限类型组合在一起，并向用户分配“查看和编辑”权限。因此，您的用户现在可以查看和编辑所有应用程序了。
>
> ADM 不支持这样的用例，即您可以为同一个用户分配不同类型的权限。您只能向用户分配一种权限。ADM 可以允许 User1 查看所有应用程序或一组选定的应用程序，也可以允许 User1 查看和编辑所有应用程序或选定的应用程序集。

将 **Citrix ADM** 从 **12.0** 升级到 **12.1** 时的 **RBAC** 映射

将 Citrix ADM 从 12.0 升级到 12.1 时，在创建组时看不到提供“读写”或“读取”权限的选项。这些权限已替换为“角色和访问策略”，使用这些策略可以更加灵活地为用户提供基于角色的权限。下表显示了 12.0 版中的权限如何映射到 12.1 版：

12.0	仅允许应用程序	12.1
admin read-write	False	admin
admin read-write	True	appAdmin
admin read-only	False	readonly
admin read-only	True	appReadonly

配置角色

February 6, 2024

在 Citrix Application Delivery Management (ADM) 中，每个角色都受一个或多个访问策略的约束。您可以在策略与角色之间定义一对一、一对多和多对多关系。您可以将一个角色绑定到多个策略，也可以将多个角色绑定到一个策略。

例如，一个角色可能绑定到两个策略，其中一个策略定义对一个功能的访问权限，另一个策略定义对另一个功能的访问权限。一项策略可能授予在 Citrix ADM 中添加 Citrix ADC 实例的权限，另一项策略可能授予创建和部署样书以及配置 Citrix ADC 实例的权限。

如果多个策略定义对某一个功能的编辑和只读权限，则编辑权限优先。

Citrix ADM 提供了四个预定义的角色：

- **admin**。可以访问所有 Citrix ADM 功能。（此角色绑定到 adminpolicy。）
- **readonly**。拥有只读访问权限。（此角色绑定到 readonlypolicy。）
- **appAdmin**。仅对 Citrix ADM 中的应用程序功能具有管理访问权限。（此角色绑定到 appAdminPolicy。）
- **appReadonly**。对应用程序功能拥有只读访问权限。（此角色绑定到 appReadOnlyPolicy。）

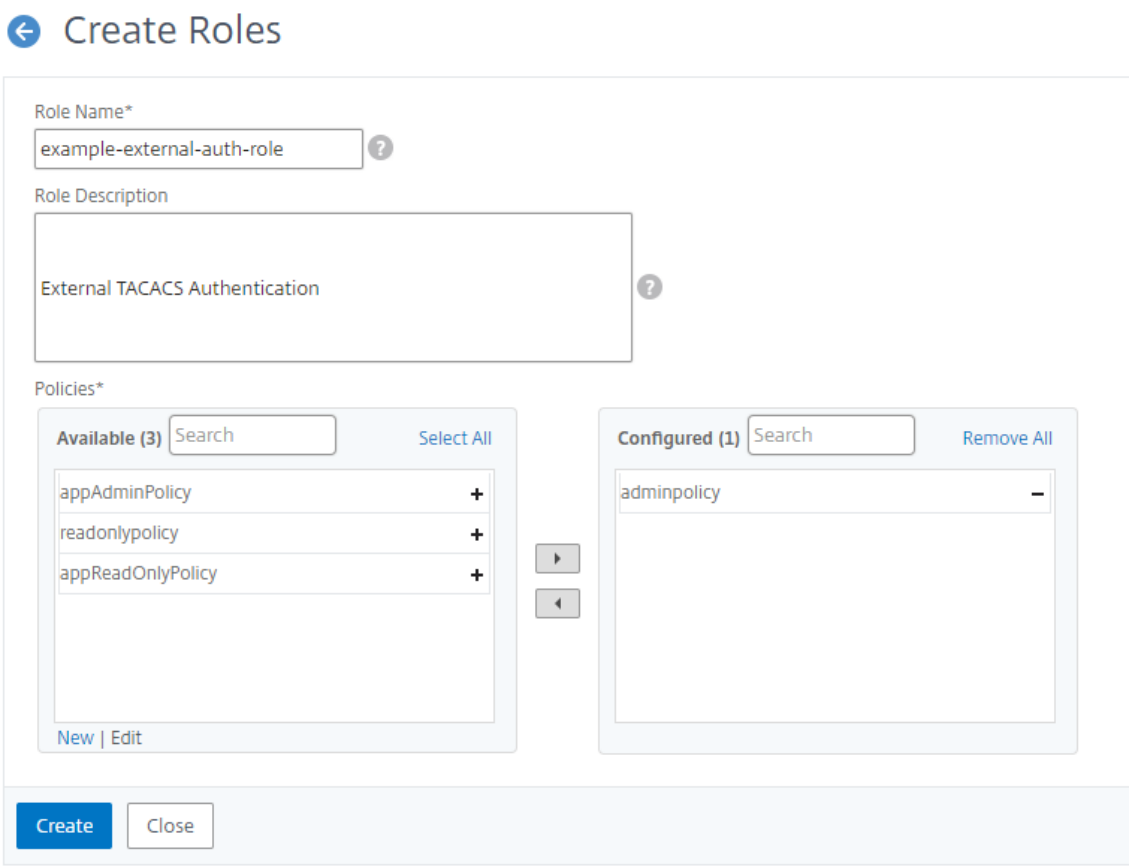
> 注意 无法编辑预定义的角色。

您还可以创建自己（用户定义）的角色。

要创建角色并为其分配策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“用户管理”>“角色”。
2. 单击添加。
3. 在“角色名称”字段中，输入角色的名称，然后在“角色描述”字段中提供描述（可选）。

4. 在“策略”部分中，将一个或多个策略添加或移动到“已配置”列表中。



5. 单击创建。

配置用户

February 6, 2024

默认情况下，Citrix Application Delivery Management (ADM) 只有一个用户：

nsroot - root 用户 (nsroot) 具有设备的完全管理权限。nsroot 用户是 Citrix ADM 的超级管理员。

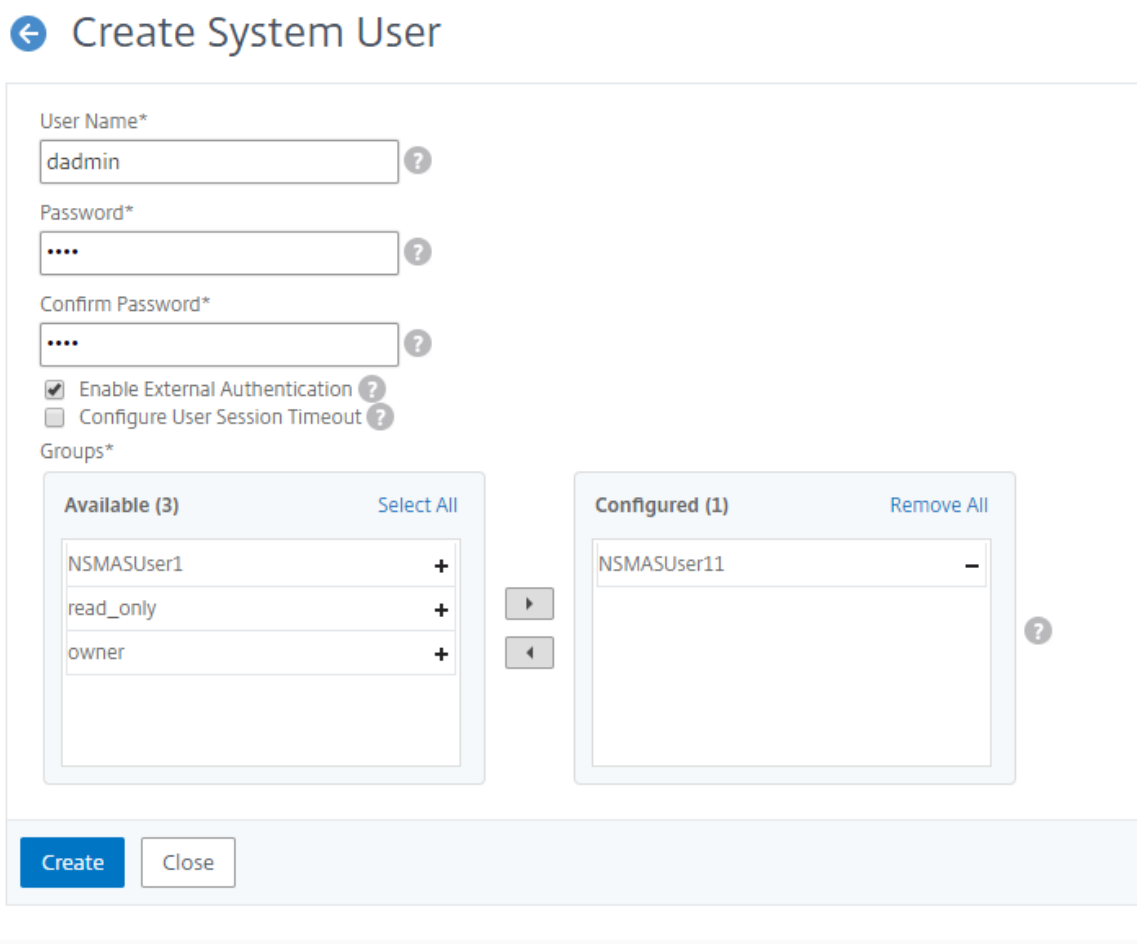
您可以创建其他用户，方法是为其配置帐户。向 Citrix ADM 添加新用户时，您可以通过分配相应的组、角色和策略来定义他们的权限。

可以将用户分配到组并将组绑定到角色。您可以在用户、组、角色和访问策略之间定义一对一、一对多或多对多关系。可将一个用户分配到多个组。一个组可以有多个角色，多个组可以有相同角色。

要在 **Citrix ADM** 中配置用户，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“用户管理”>“用 户”。

2. 单击添加。
3. 输入以下详细信息：
   a) 用户名。用户的名称
   b) 密码。用户登录 Citrix ADM 时使用的密码
4. 或者，选择 启用外部身份验证，以便可以通过外部身份验证服务器对用户进行身份验证。
5. 如果您已创建组并想要将用户分配到组，请在“组”部分中，将一个或多个组从“可用”列表移至“已配置”列表。



6. 单击创建。

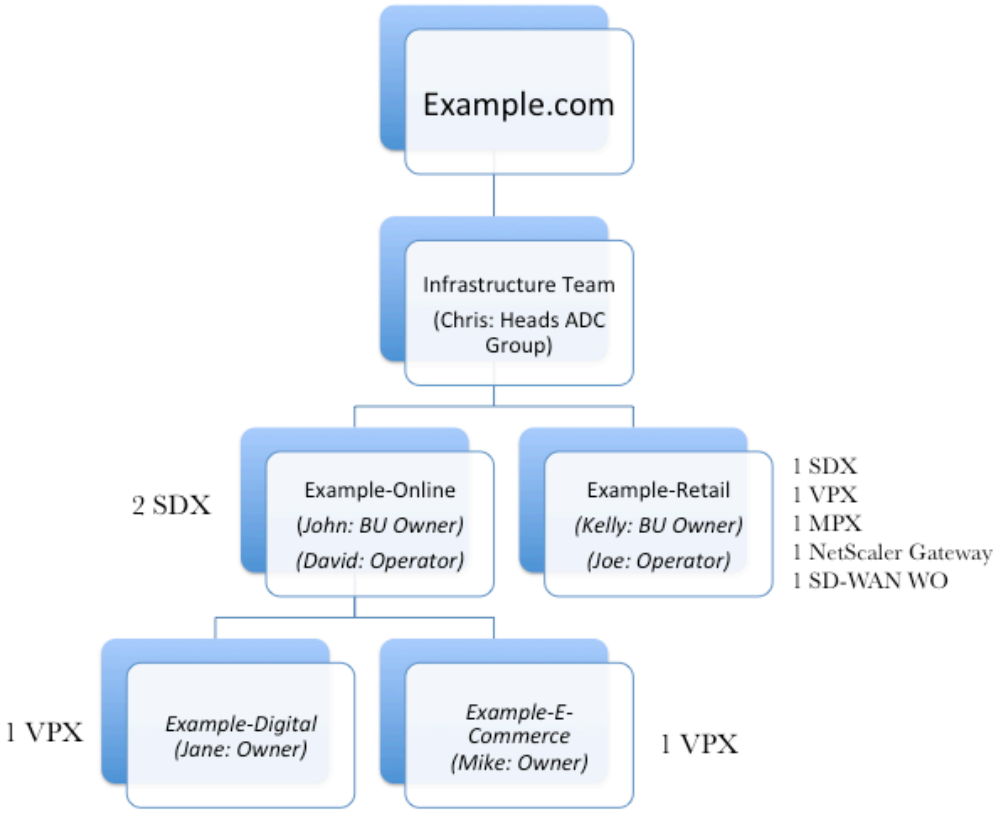
多租户：为租户提供专属管理环境

February 6, 2024

Citrix Application Delivery Management (ADM) 提供多租户功能，您可以在其中为多个租户配置系统。每个租户都可以添加其网络实例、管理和监视这些实例和应用程序以及创建他们自己的用户和组。任何租户都不能查看其他租户的实例和应用程序。只有系统管理员可以查看所有租户的所有实例、应用程序和报告。但是系统管理员不能为租户创建用户。所有系统级任务只能由系统管理员执行。

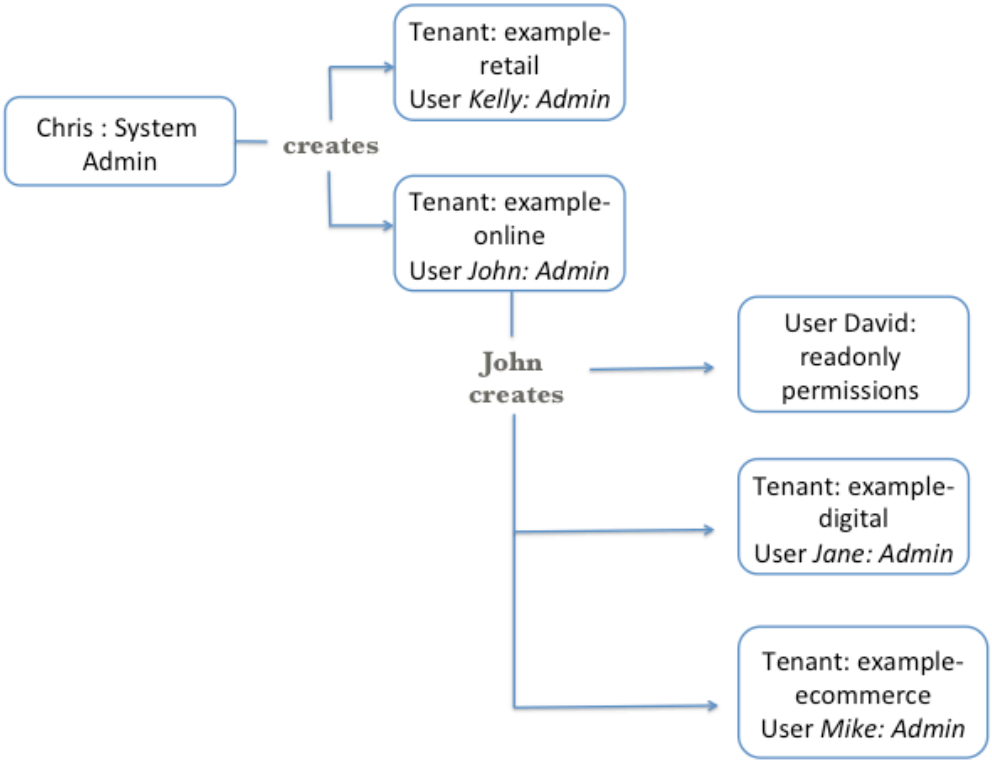
假设这样一个场景：example.com 这个组织内部有一个基础结构组和多个业务部门。他们希望集中管理其网络中的所有实例。但是，他们希望为每个业务部门提供专用环境。

下图显示了如何构建 example.com 组织基础结构组。他们希望四个业务部门中每一个都有专用管理环境。此图还显示了每个业务部门要管理的实例数。



ADC 组长克里斯是 Citrix ADM 的系统管理员。Chris 为两个业务部门 Example-online 和 Example-Retail 创建两个租户，并分配两个用户作为这些租户的管理员。每个租户管理员现在都可以在其租户环境中添加更多用户、添加他们要管理的实例以及创建子租户。

下图显示了本示例中 Citrix ADM 中创建的租户和用户。

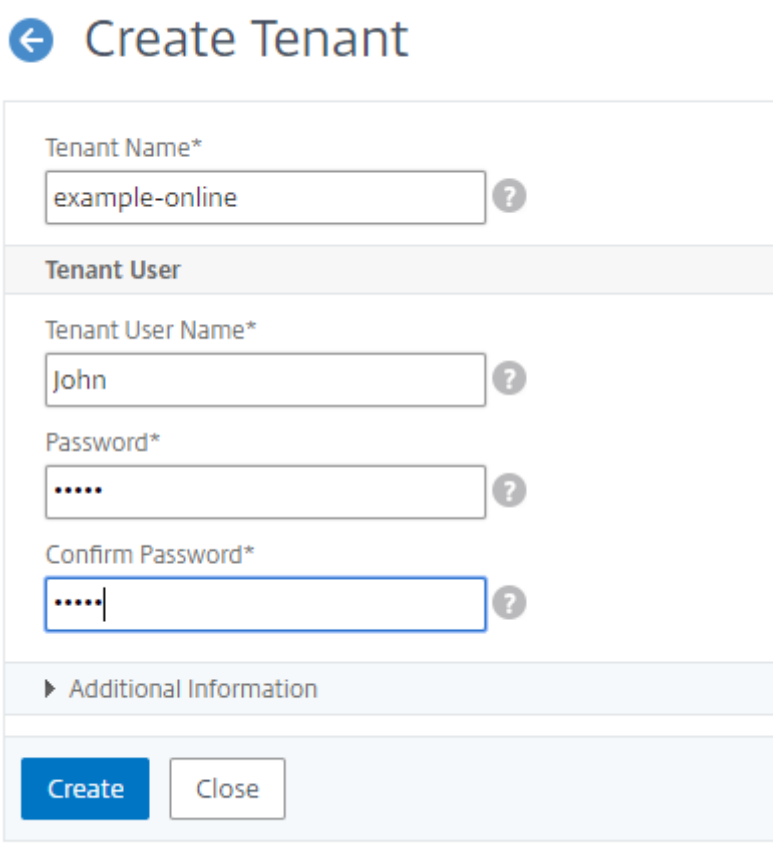


添加租户

在此示例中，系统管理员 Chris 创建两个租户：example-online 和 example-retail。Chris 在创建租户时，还为每个租户创建默认的管理员用户。

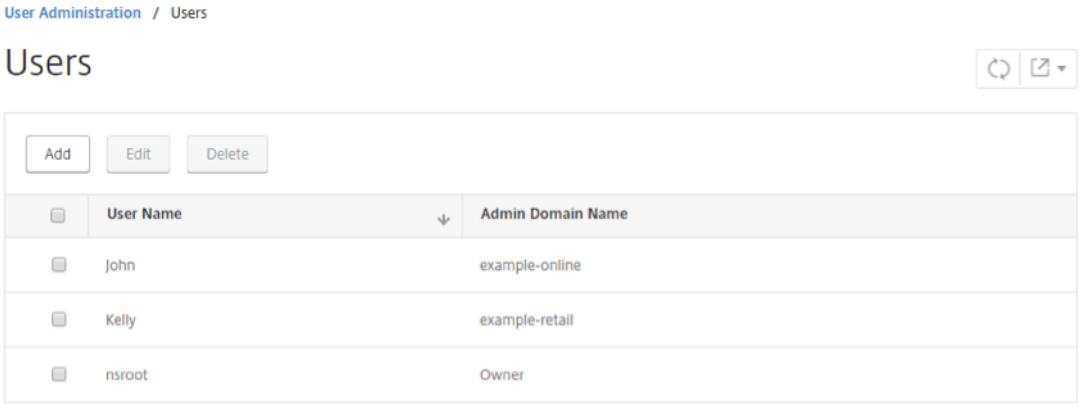
添加租户

1. 导航到“系统”>“租户”，然后单击“添加”。
2. 在 创建租户 页面上，指定租户名称和要指定为该租户管理员的租户用户名。此外还提供密码。
3. 单击创建。



在“租户”页上，可以查看创建的租户列表。

您还可以在“系统”>“用户管理”>“用户”页面上查看每个租 户的管 理员用 户 列表。

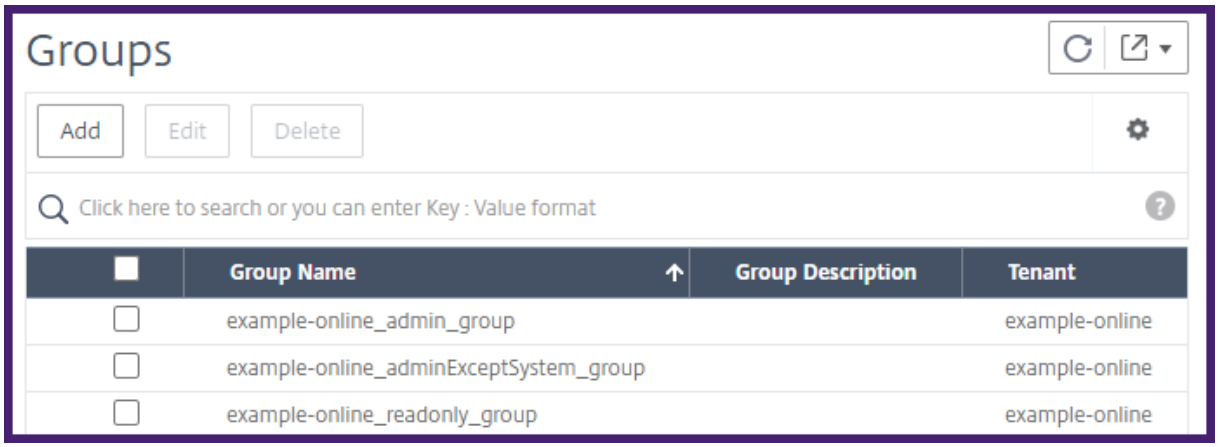


创建租户时，系统将创建三个默认系统组：管理员组、AdminAUTSystem_Group 和只读组。

示例：

示例在线租户具有以下默认组：

- example-online_admin_group
- example-online_adminExceptSystem_group
- example-online_readonly_group

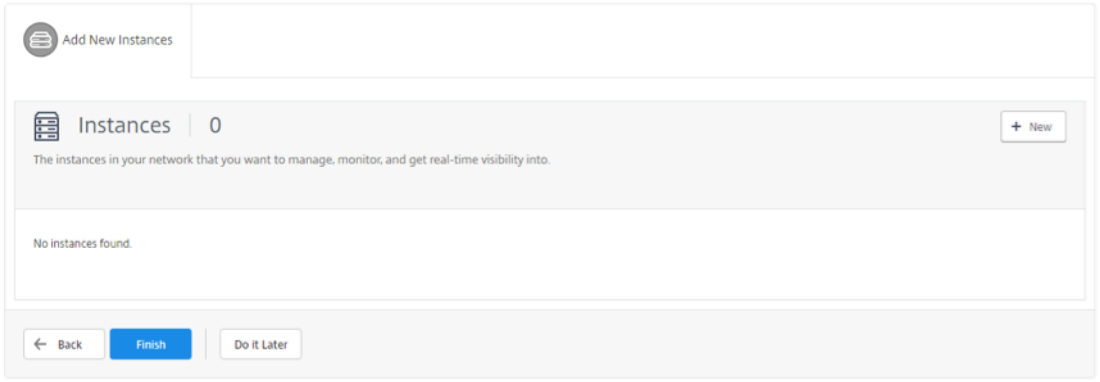


以租户用户身份登录到 **Citrix ADM**

创建租户后，租户用户可以使用租户用户凭据登录 Citrix ADM。为此，租户必须提供域名和用户名，例如 example-online\John。

将实例添加为租户用户

租户登录后，Citrix ADM 会提示租户添加实例。单击 **+ New**（+ 新建）可添加要管理的实例。此外，可以单击“Do it Later”（以后执行），在以后从“Infrastructure”（基础结构）选项卡中添加实例。有关详细信息，请参阅将实例添加到 *Citrix ADM*。



在此示例中，John 添加了两个 Citrix ADC SDX 实例。

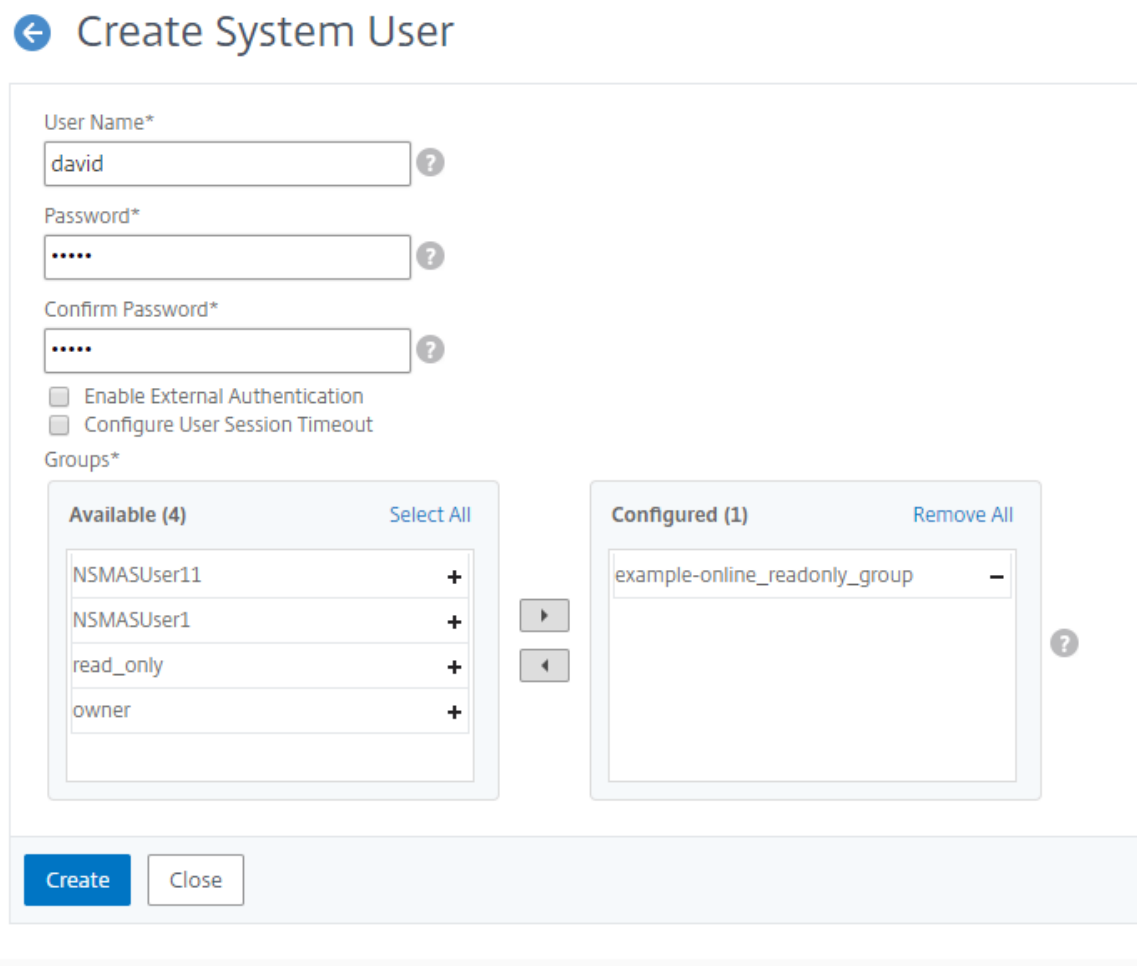
指定 Citrix ADM 可用于访问实例的实例类型、IP 地址（用逗号分隔）和配置文件名称，然后单击“** 确定”。

创建用户

租户管理员 John 现在想为 David 创建用户，以便 David 可以监视此租户的所有实例和应用程序。但是，Chris 不希望 David 对实例执行任何配置任务或更改租户的任何系统设置。因此，Chris 为 David 创建用户时设置只读权限。

要创建用户，请执行以下操作：

1. 导航到“系统”>“用户管理”>“用户”，然后单击“添加”。
2. 在“创建系统用户”页上，为要创建的用户指定用户名和密码。
3. 在“组”下，选择要分配给此用户的组。在此示例中，example-online_readonly_group 分配给用户 David。



在租户内创建租户

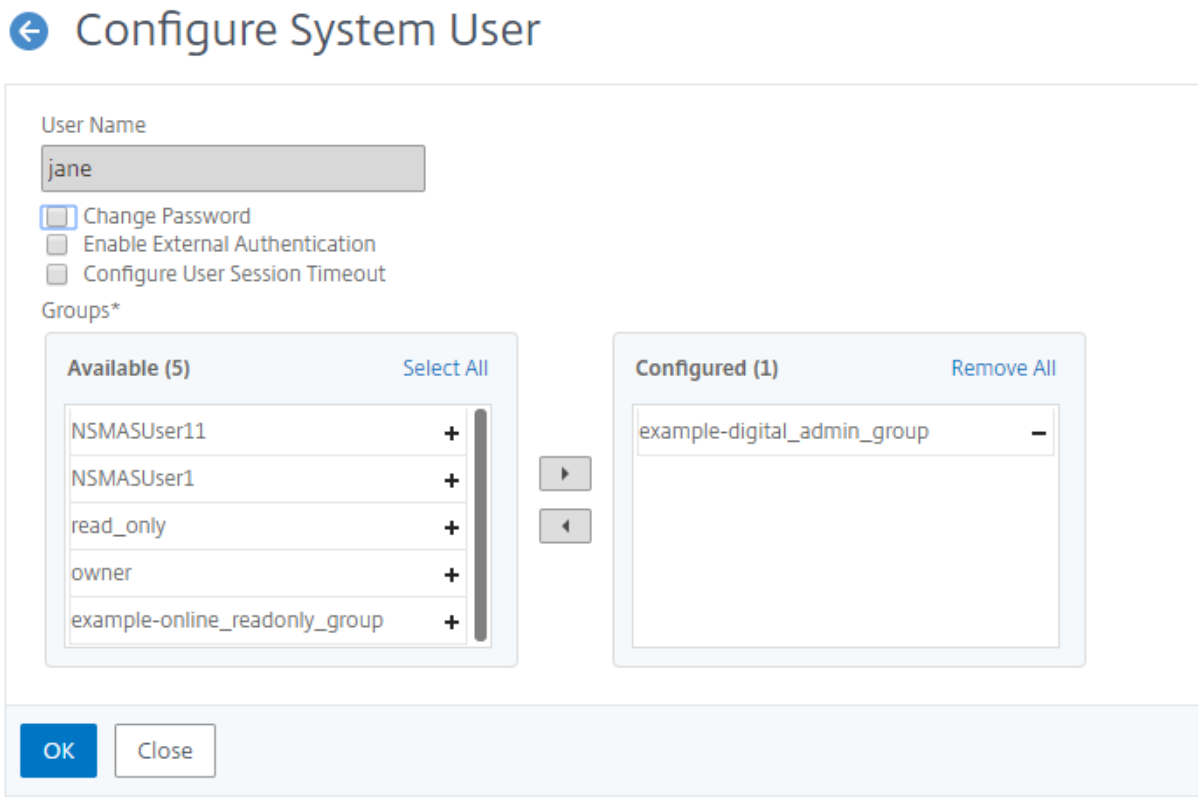
如果租户管理员要对其租户做进一步的划分，可以创建子租户。但是，他只能创建一层子租户。在此示例中，John 创建两个子租户 example-digital 和 example-ecommerce。创建这两个子租户时，Chris 将 Jane 和 Mike 分别分配为管理员用户。

要在租户内创建租户，请按照添加租户中所述的步骤进行操作。

您可以查看在“租户”页上创建的 租户。

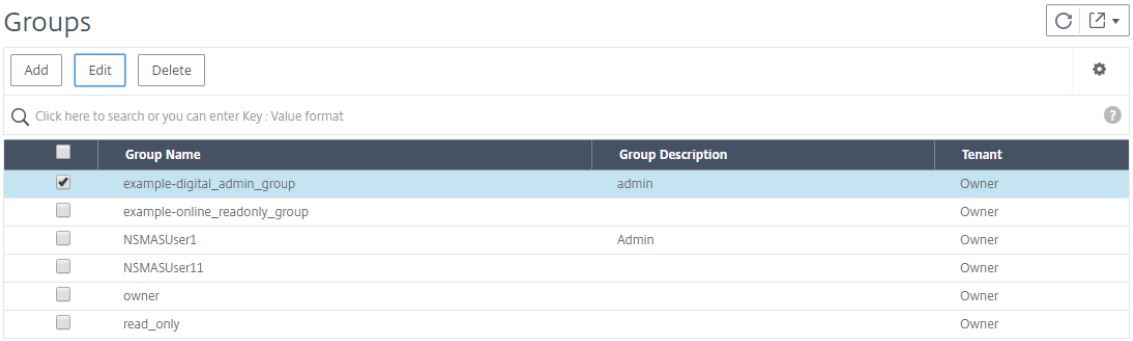
还可以查看分配给用户的权限。导航到“系统”>“用户管理”>“用户”，选择一个用户，然后单击“编辑”。

在“配置系统用户”页面的“组”下，您可以查看分配给该用户的组。在此示例中，可以看到 example-digital_admin_group 分配给 Jane。

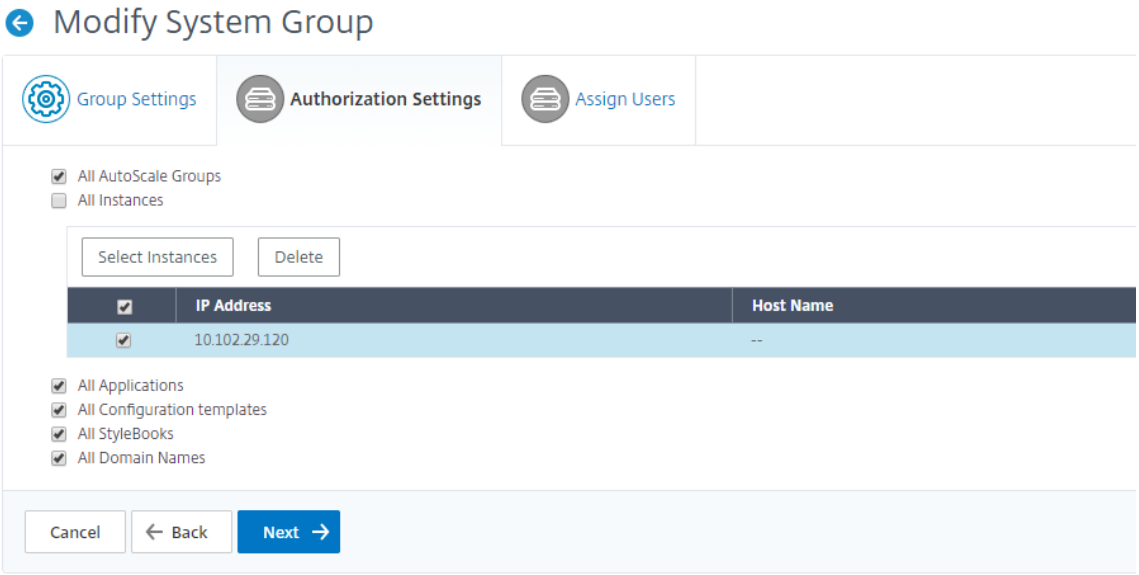


作为租户管理员，如果您已经向 Citrix ADM 添加了实例，则可以将实例分配给租户中的用户或子租户进行管理和监视。例如，John 可以将一个 VPX 实例分配给 Jane 进行管理。

1. 导航到“系统”>“用户管理”>“组”。
2. 选择将用户分配到的组，然后单击“编辑”。



3. 在“修改系统组”页上的“授权设置”选项卡上，清除“所有实例”复选框。



4. 选择您希望用户管理的实例，然后单击 选择实例。
5. 单击下一步，然后单击完成。

应用程序

February 6, 2024

Citrix ADM 的应用程序分析和管理功能增强了以应用程序为中心的方法，可帮助您应对各种应用程序交付挑战。通过此方法可以查看应用程序的运行状况分数，帮助您确定安全风险，以及帮助您检测应用程序通信流中的异常并采取更正措施。

下图概述了您可以为应用程序管理和分析执行的各种任务：

应用程序可以是已发现的应用程序、HAProxy 应用程序或自定义应用程序。

发现的应用程序

自动为每个托管虚拟服务器生成的应用程序。发现的应用程序将始终有一个虚拟服务器，不能直接编辑或删除这些应用程序。

自定义应用程序

用户基于发现的应用程序创建的应用程序。Citrix ADM 允许您添加、编辑和删除这些应用程序。自定义应用程序由以下人员创建：

- 一台或多台虚拟服务器
- 一个或多个 HAProxy 前端。

创建自定义应用程序时，所有已发现的添加到自定义应用程序的应用程序都将从应用程序控制板中移除。

需要注意的事项

- 您无法在多个自定义应用程序中添加已发现的应用程序。
- 如果所有发现的应用程序已分配给其他自定义应用程序，则不能创建自定义应用程序。您需要删除现有的自定义应用程序来释放发现的应用程序，才能进一步组合新的自定义应用程序。
- 您无法创建包含虚拟服务器和 HAProxy 前端的自定义应用程序。

HAProxy 应用程序

为每个托管 HAProxy 前端自动创建 HAProxy 离散应用程序。您还可以对这些应用程序进行分组，以形成类似于 Citrix ADC 应用程序的自定义应用程序。有关更多信息，请参阅使用 Citrix ADM 管理和监视 HAProxy 实例。

需要注意的事项

HAProxy 应用程序不支持以下应用程序控制面板功能或指标：

- 应用活动调查
- 应用程序得分
- Threat Index（威胁指数）
- 峰值使用趋势
- 吞吐量
- Server Connections（服务器连接数）
- Transactions（事务数）

创建自定义应用程序

您可以通过在定义应用程序时添加一个或多个发现的应用程序来创建自定义应用程序。

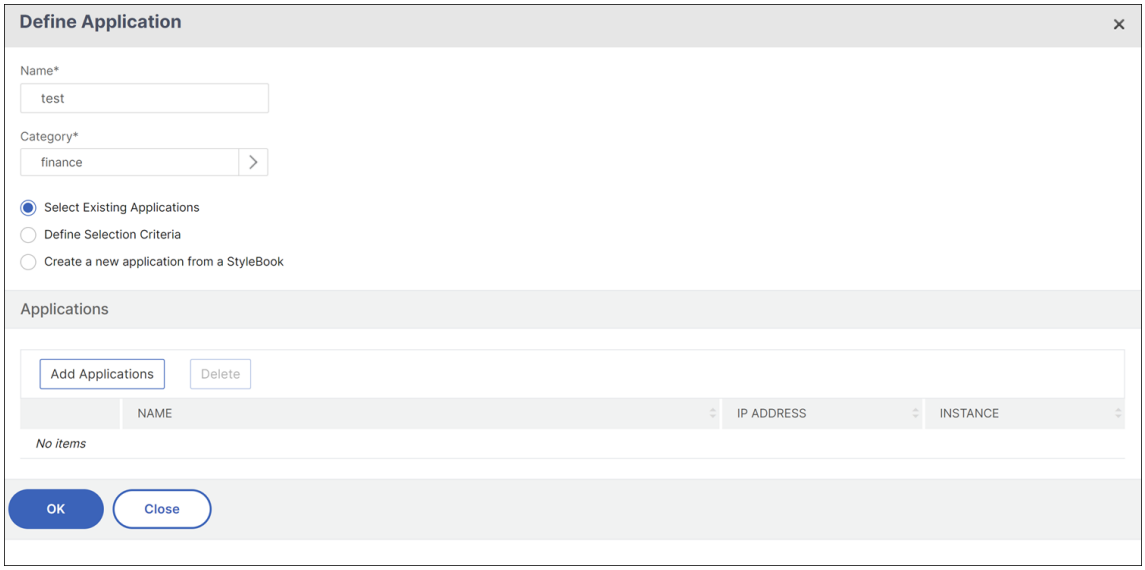
要创建自定义应用程序，请执行以下操作：

1. 导航到应用程序 > 控制板，然后单击定义自定义应用程序。
2. 在“Define Application”（定义应用程序）屏幕上，设置以下参数：

字段	说明
名称	自定义应用程序的名称
类别	类别的名称，在应用程序控制板上，与该类别相关的所有应用程序都将分为一组。
Select Existing Applications（选择现有应用程序）	如果定义标准基于 Citrix ADM 监视的许可虚拟服务器，则可以选择添加虚拟服务器。
Define Selection Criteria（定义选择条件）	该选项用于按虚拟服务器范围或按源服务器/服务 IP 地址范围定义应用程序。 • 服务器。指定在其中运行应用程序的后端服务器的服务器或服务 IP 地址、服务器名称或端口。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。 • 虚拟服务器。指定以下项之一：在其中运行应用程序的后端服务器的虚拟服务器 IP 地址、虚拟服务器名称或端口。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。

3. 单击确定。

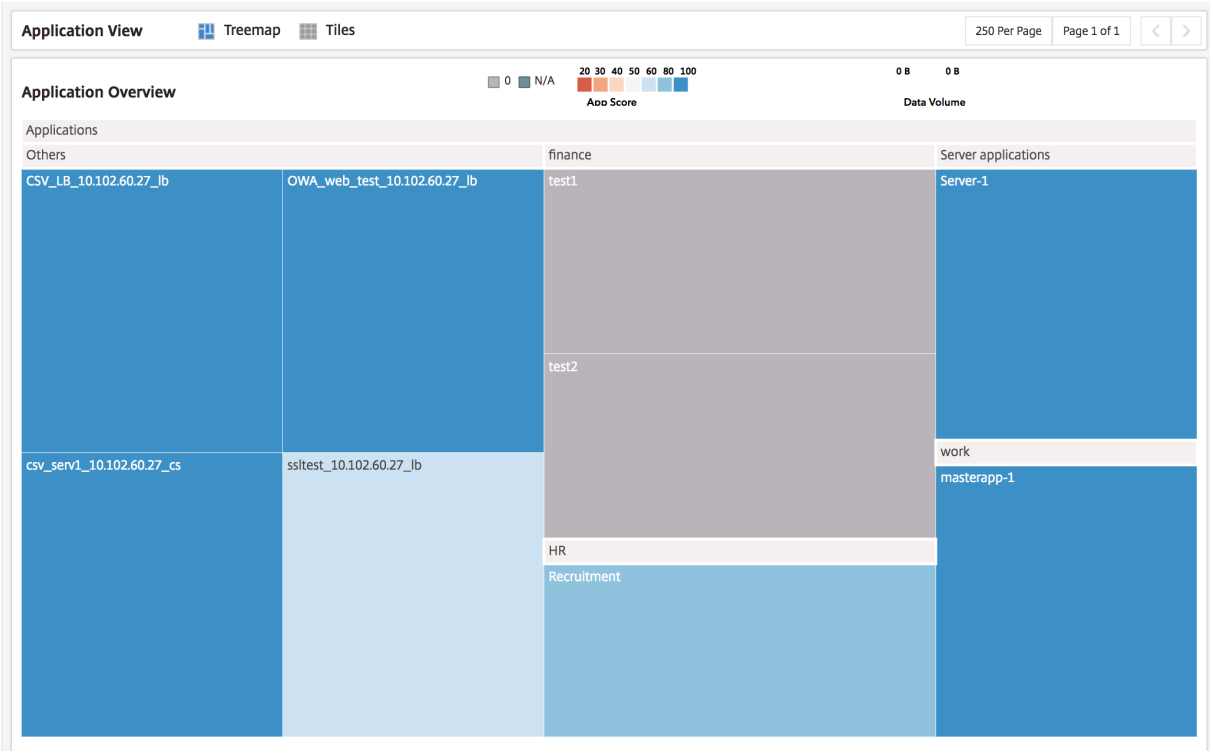
> 注意
>
> 目前，应用程序控制板仅支持负载平衡和内容交换虚拟服务器。



对您的应用程序进行分组

通过对应用程序分组可以轻松地对其进行管理和监视。可以在定义应用程序时选择或创建类别来对应用程序分组。要创建或选择类别，请在定义应用程序时 单 ** 击“类别”字段旁边的 按钮。

未添加到任何类别的应用程序显示在“其他”类别下。



“应用程序”控制板

应用程序控制面板提供由 Citrix ADM 监视的所有应用程序的整体视图，并提供与所有应用程序相关的关键信息。例如，该控制板显示应用程序的性能和安全指标、计数器和运行状态。要显示有关特定应用程序的信息，请选择该应用程序。此外，“Summary Panel”（摘要面板）中的条形图会显示所有监视的应用程序的指标，例如应用程序分数和威胁指数。

查看您的应用程序

应用程序控制板在树状图中将应用程序显示为节点，其大小与应用程序的数据量相对应。磁贴的颜色指示应用程序的应用程序分数，红色表示运行状况最差，蓝色表示运行状况良好。

通过从应用程序控制板屏幕中选择一个选项，可以将应用程序控制板视图切换为树状图或图块，在其中您可以以卡片的形式查看应用程序的详细信息。默认情况下，应用程序控制板中显示 250 个应用程序，要查看更多应用程序，请单击下一页选项。

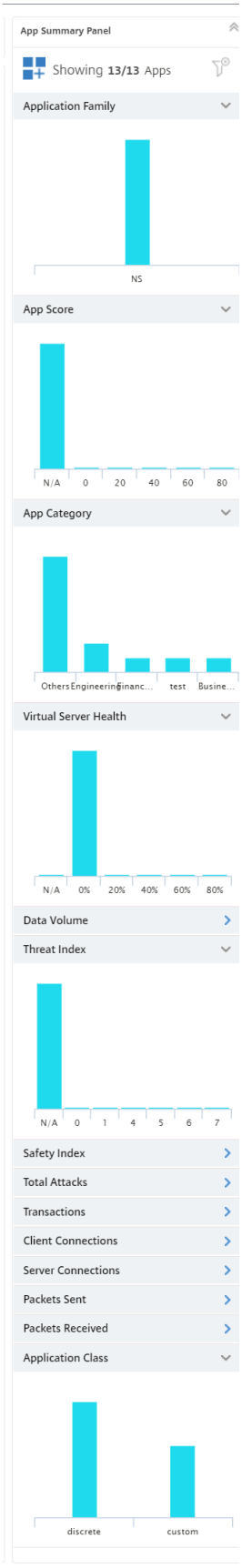
应用程序按定义应用程序时选择的类别进行分组。可以从应用程序摘要面板中选择应用程序指标来对应用程序排序或查看应用程序。例如，如果要显示应用程序分数在 20-40 范围内的应用程序，请从“App Summary Panel”（应用程序摘要面板）的“App Score”（应用程序分数）部分中选择合适的条形图。同样，可以在“App Summary Panel”（应用程序摘要面板）中选择其他指标。

应用程序摘要面板

“App Summary Panel”（应用程序摘要面板）显示应用程序控制板上可见的所有应用程序的指标。可以在此面板中选择或取消选择应用程序指标来在控制板中对应用程序排序和查看应用程序。“App Summary Panel”（应用程序摘要面板）显示以下指标：

指标	说明
应用程序家族	根据配置应用程序的 Citrix ADC 实例的类型对应用程序数量进行分组的条形图。
应用程序得分	定义应用程序性能的评分系统
应用程序类别	显示在 Citrix ADM 中定义的所有类别的直方图的条形图。现在，所有离散应用程序都显示在“其他”类别下，自定义应用程序显示在各自的类别名称下。
虚拟服务器运行状况	显示每个类别下的应用程序数量的条形图。这些应用程序的健康评分值分别为 0%、20%、40%、60%、80%和 100%。
Data Volume（数据量）	一种评分系统，它根据应用程序的数据量对应用程序的数量进行分组。数据量是根据应用程序请求的总字节数和从应用程序收到的响应字节数计算得出的。

指标	说明
Threat Index（威胁指数）	一种个位数评级系统，无论应用是否受到 Citrix ADC 设备的保护，它都会显示应用程序受到攻击的严重程度。
安全指数	一个单位数评级系统，用于指示您配置 Citrix ADC 实例以保护应用程序免受外部威胁和漏洞的安全性。
Total Attacks（攻击总数）	针对应用程序的攻击总数
Transactions（事务数）	应用程序执行的事务范围。
Client Connections（客户端连接数）	应用程序建立的客户端连接数。
Server Connections（服务器连接数）	应用程序建立的服务器连接数。
Packets Sent（发送的数据包数）	应用程序发送的数据包的数量。
Packets Received（接收的数据包数）	应用程序接收到的数据包的数量。
应用程序类别	根据应用程序是离散应用程序还是自定义应用程序对应用程序数量进行分组的条形图。

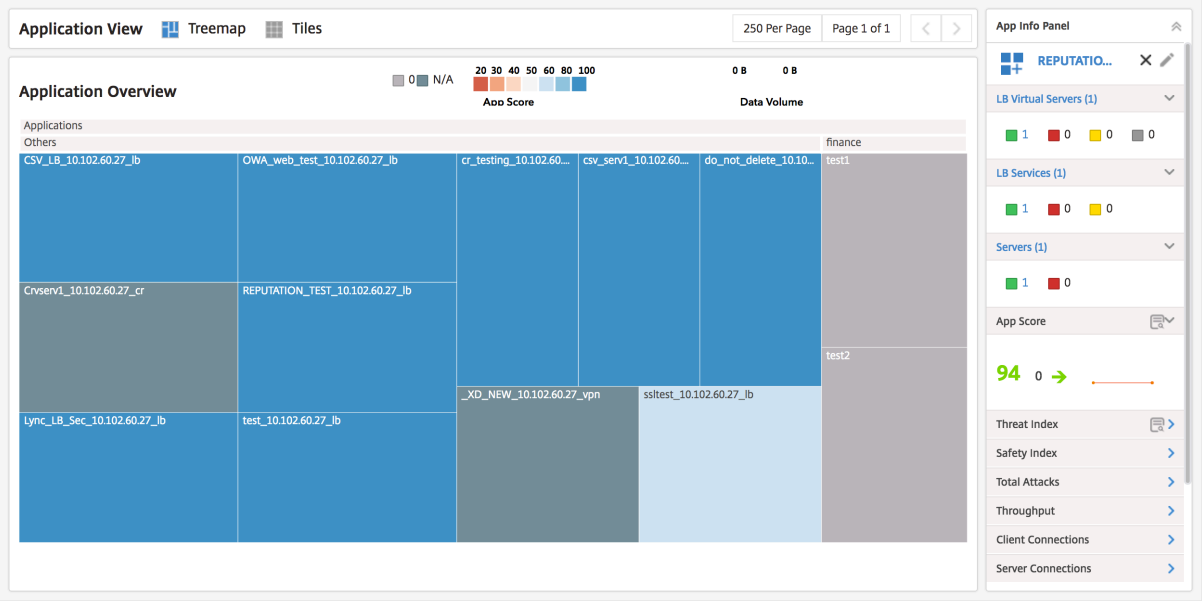


例如，在应用程序摘要面板中，向下滚动以查找“虚拟服务器运行状况”条形图。在虚拟服务器运行状况条图中，Citrix ADM 根据虚拟服务器运行状况的百分比对应用程序进行分类。条形图显示虚拟服务器运行状况值介于 0% 到 100% 之间的应用程序的数量。

虚拟服务器运行状况表示分组在离散应用程序下的虚拟服务器的运行状况。但是，如果存在包含两个或多个虚拟服务器的自定义应用程序，则在组中考虑最少的虚拟服务器运行状况。

现在，您可以应用筛选器，并仅查看应用程序控制板中与选择条件匹配的应用程序。点击显示 0% 的栏。此栏显示虚拟服务器运行状况介于 0% 到 20% 之间的应用程序的数量。现在，您可以隔离虚拟服务器运行状况较低的应用程序并采取补救措施

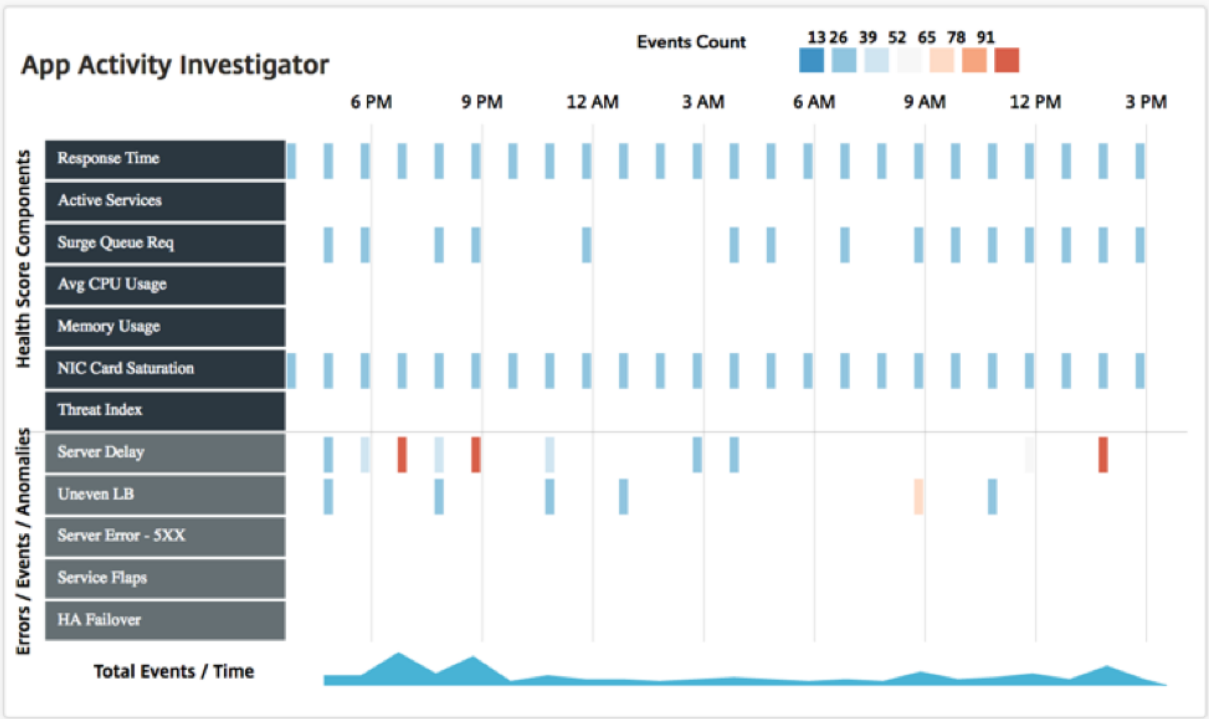
应用程序信息面板　“App Info Panel”（应用程序信息面板）位于逐级浏览应用程序时的第一级。该面板显示应用程序的主要指标和组件，以及其状态。例如，对于任何选定的应用程序，“App Info Panel”（应用程序信息面板）均显示虚拟服务器总数、服务总数、应用程序分数和其他信息。要显示“App Info Panel”（应用程序信息面板），请单击应用程序控制板上的任何应用程序磁贴。“App Info Panel”（应用程序信息面板）随后将替换“App Summary Panel”（应用程序摘要面板）。



应用程序活动调查员　“App Activity Investigator”（应用程序活动调查器）是从应用程序逐级浏览时的第二级之一。可以通过选择“App Info Panel”（应用程序信息面板）上的搜索图标或双击应用程序控制板上的应用程序磁贴来访问“App Activity Investigator”（应用程序活动调查器）。

“App Activity Investigator”（应用程序活动调查器）显示“App Score”（应用程序分数）组件、“Errors”（错误数）、“Events”（事件数）和“Anomalies”（异常数）等主要信息。

如果选定的持续时间是一小时，则每个图例以一分钟的时间间隔进行汇总，如果选定的持续时间是一天，则每个图例以一小时的时间间隔进行汇总。



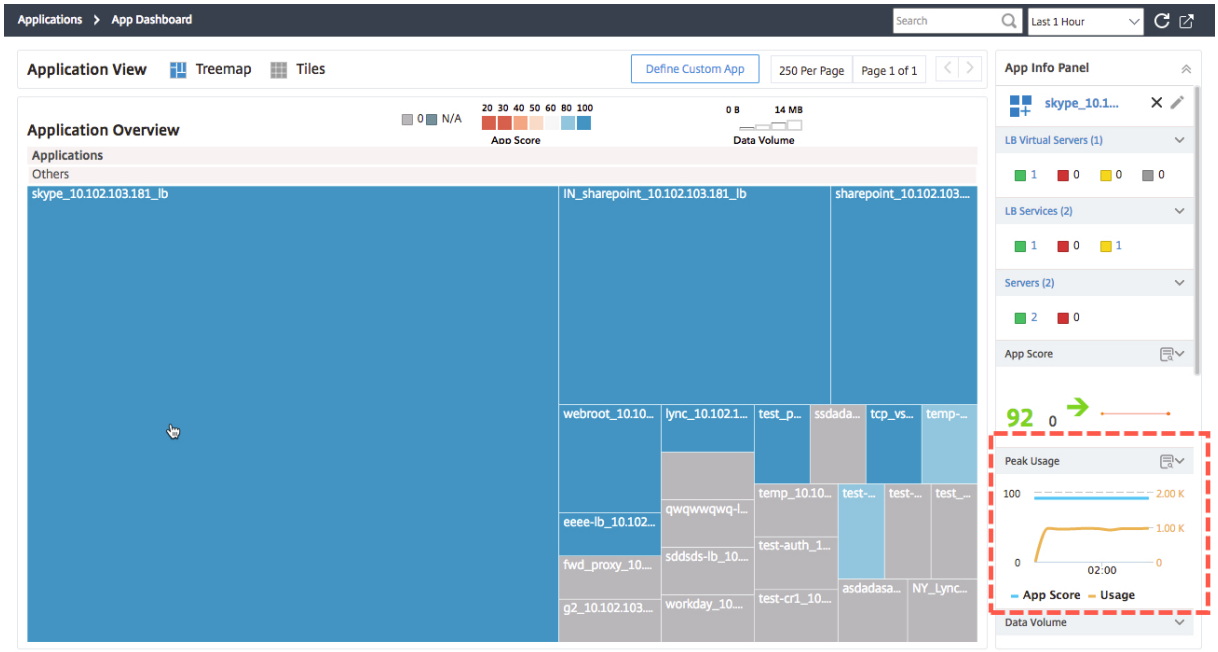
这些偏差以矩形图方式显示在图形中。这些图例会进行汇总，并按照发生的事件数进行颜色编码。蓝色表示最小事件数，红色表示最大事件数。可以将鼠标指针悬停在图例上来显示选定图例的详细信息，例如，错误类型、时间和汇总的事件数。可以从时间段下拉框中选择时间来自定义图形的时间段。

应用程序使用趋势　在大多数情况下，作为企业主，您根据统计数据和数据对应用程序的有效性和使用趋势做出决定。要了解应用程序的使用趋势，您必须整理来自部署中多个实体的信息，例如后端基础架构、代理、CDN 网络等。然后，关联收集到的信息以获得正确的分析，这会消耗大量时间。

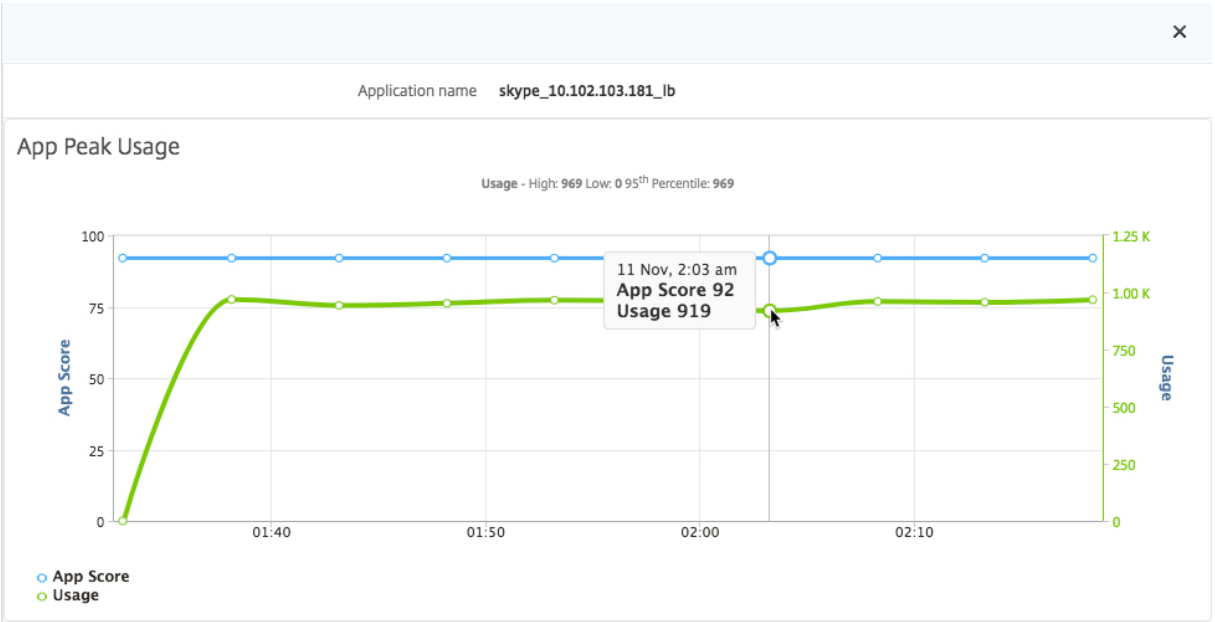
相反，在您的部署中作为 ADC 部署的 Citrix ADC 设备包含有关该应用的所有信息以及该应用的使用情况统计信息。您可以将此信息转发给 Citrix ADM。Citrix ADM 收集这些信息，并提供有关应用程序使用情况和性能的详细见解。您可以使用这些见解根据应用程序的使用情况和性能做出有效的决策。

应用程序控制板中的应用程序信息面板提供应用程序的峰值使用趋势。您可以使用峰值使用趋势来评估应用程序的性能，并采取适当的措施来提高应用程序的性能。

要查看应用程序的峰值使用趋势，请导航到应用程序 **>** 应用程序控制面板。选择应用程序，应用程序的峰值使用趋势将显示在“应用程序信息面板”的“峰值使用量”部分下。



您可以进一步单击“峰值使用情况”部分，查看应用程序分数和应用程序使用情况。使用此信息，您可以识别应用程序的峰值使用情况，并将其与相应的 App Score 相关联，以评估在高峰使用期间对应用程序的性能影响。



Time	App Score	Usage
Nov 11 01:33 AM	92	0
Nov 11 01:38 AM	92	969
Nov 11 01:43 AM	92	943
Nov 11 01:48 AM	92	952
Nov 11 01:53 AM	92	966
Nov 11 01:58 AM	92	960
Nov 11 02:03 AM	92	919
Nov 11 02:08 AM	92	960
Nov 11 02:13 AM	92	957
Nov 11 02:18 AM	92	968

导出应用程序控制板和安全控制板的报告

Citrix ADM 允许您拍摄当前应用程序控制板和应用程序安全控制板页面的快照并将其导出为报告。在频繁的时间间隔内，应用管理员可能需要使用这些报告来更新应用使用情况和性能损失。

通过此功能，管理员可以将此数据提取为.png 或.pdf 报表。

> 注意
>
> 与 Citrix ADM 中的其他报告导出选项不同，您只能将应用程序控制面板和安全控制面板报告导出为.pdf 或.png 文件。目前不支持.jpg 和.csv 等其他选项。

1. 在应用程序控制面板或应用程序安全控制面板页面上，单击页面右上角的导出图标。
2. 选择导出选项作为.pdf 或.png 文件。
3. 单击确定。

报告将下载到您的系统中。在“应用程序控制面板”和“应用程序安全控制面板”页面中，您还可以导航到二级页面并将其导出为报告。目前，您一次只能下载一个应用程序的报告。

应用程序性能分析

February 6, 2024

“App Score”（应用程序分数）是定义应用程序执行良好情况的评分系统产品。它显示应用程序在响应性方面是否表现良好，并且是否已启动和运行所有系统。“App Score”（应用程序分数）在应用程序级别显示。该分数的计算基于以下三个主要组件：

- 应用程序性能分数（应用程序的 **APDEX** 分数）。从应用程序的服务器响应时间变化派生。
- **Citrix ADC** 系统资源. 基于另外三个组件派生：
  - CPU 使用率
  - Memory Usage（内存使用率）
  - NIC 卡饱和度
- 应用程序服务器资源。从另外两个组件派生出来：
  - Percentage of Active Services（活动服务百分比）
  - Surge Queue Requests（浪涌队列请求）

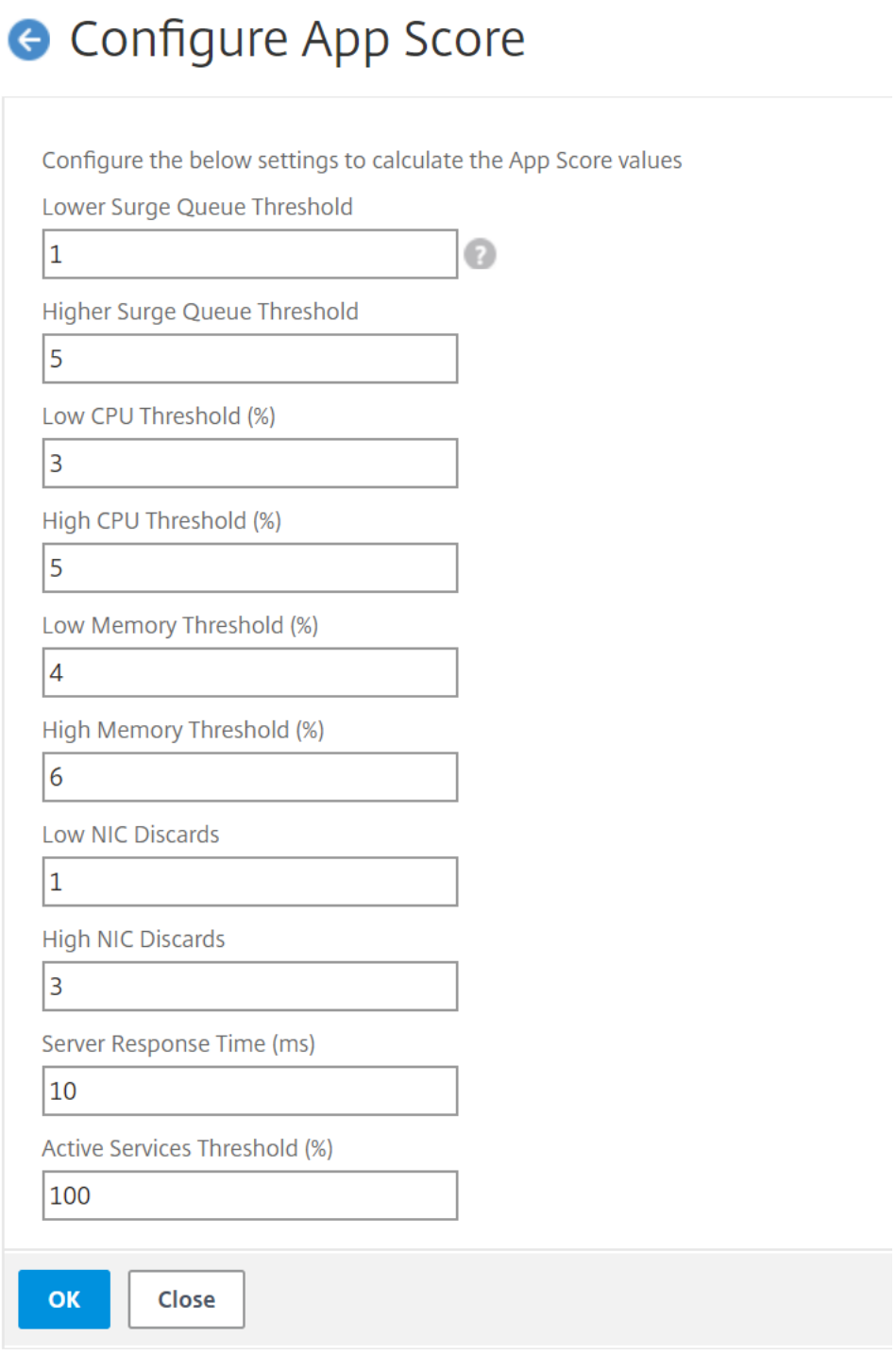
应用程序分数是根据这些分数计算的，其中 Citrix ADC 系统资源分数和应用程序服务器资源分数从应用程序性能分数中减去。App Score 适用于所发现的负载平衡和内容交换虚拟服务器定义的所有应用程序，以及您在应用程序控制板上定义的自定义应用程序。

要在 **Citrix ADM** 中配置应用程序分数，请执行以下操作：

1. 在 Citrix ADM 中，导航到 分析 > 设置。
2. 在“设置”页面上，单击“配置应用程序分数”。
3. 在配置应用程序分数页面上，输入以下参数的值：
   a) 降低浪涌队列阈值。虚拟服务器和已建立的连接等待提交的连接总数的比率较低的阈值。
   b) 更高的浪涌队列阈值。虚拟服务器和已建立连接的等待提交的连接总数的比率较高的阈值。
   c) 低 **CPU** 阈值 **(%)**。Citrix ADC 实例中 CPU 总使用率的较低阈值。
   d) 高 **CPU** 阈值 **(%)**。Citrix ADC 实例中 CPU 总使用量的阈值越高。
   e) 低内存阈值 **(%)**。Citrix ADC 实例中总内存使用量的较低阈值。
   f) 高内存阈值 **(%)**。Citrix ADC 实例中总内存使用量的阈值越高。
   g) 低网卡丢弃。接口丢弃的数据包的下限阈值。
   h) 高网卡丢弃。接口丢弃的数据包的较高阈值。

i) 响应时间。发送请求数据包与从虚拟服务器上配置的服务接收第一个响应数据包之间的时间间隔。Citrix ADM 中配置的默认值为 500 毫秒。

j) 活跃服务阈值。绑定到虚拟服务器的服务必须处于活动状态的百分比阈值。



4. 单击确定。

应用程序安全分析

February 6, 2024

“App Security Dashboard”（应用程序安全性控制板）提供应用程序的安全状态的历史视图。例如，它显示安全违规、签名违规和威胁指数等主要安全指标。应用程序安全控制面板还显示与攻击相关的信息，例如已发现的 Citrix ADC 实例的同步攻击、小窗口攻击和 DNS 洪水攻击。

> 注意
>
> 要查看应用程序安全控制面板的指标，应在要监视的 Citrix ADC 实例上启用 AppFlow for Security Insight。

要在应用程序安全控制板上查看 **Citrix ADC** 实例的安全指标，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix Application Delivery Management 的 IP 地址（例如，http://192.168.100.1）。
2. 在用户名和密码中，输入管理员凭据。
3. 导航到应用程序 > 应用程序安全控制面板，然后从设备 下拉列表中选择实例 **IP** 地址。

可以单击图中绘制的气泡，进一步深入查看“App Security Investigator”（应用程序安全性调查器）上报告的差异。

创建应用程序定义

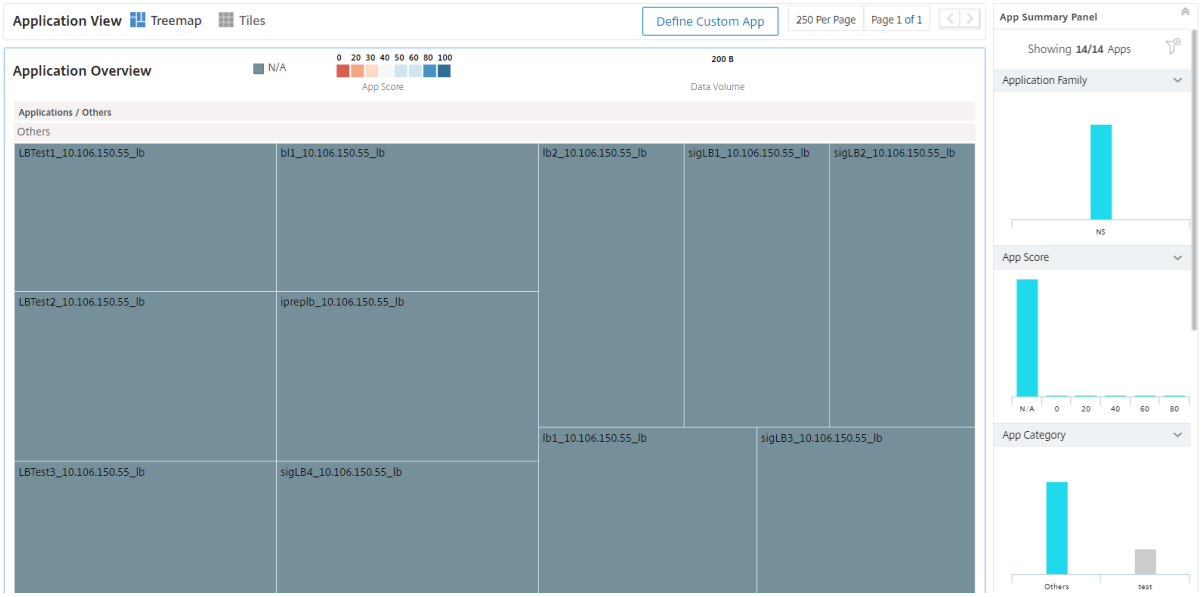
February 6, 2024

您可以根据 Citrix ADM 中发现的应用程序集合定义自定义应用程序。

在 Citrix ADM 中，导航到 **Application Dashboard**（应用程序控制板），**Application Overview**（应用程序概览）页面将显示默认应用程序。这些默认应用程序或“离散应用程序”是您拥有默认许可证的 30 个应用程序。在业务环境中安装 Citrix ADM 时，您会发现这些应用程序。

当您创建“自定义应用程序”时，自定义应用程序会取代离散的应用程序。在控制板上，自定义应用程序根据创建它们时选择的类别排列。

您可以按两种方式查看发现的应用程序和自定义应用程序：树状图和磁贴。



可以通过静态配置或动态配置创建自定义应用程序。

1. 应用程序的静态定义 -在静态定义中，您可以定义应用程序。在 Citrix ADC 实例上配置新虚拟服务器时，此定义不会更新。您必须手动更新此列表以包含更多虚拟服务器。
2. 应用程序的动态定义 -在动态定义中，您可以使用下面列出的三个条件之一来定义应用程序：

   a) 服务器。指定运行应用程序的服务器或服务 IP 地址、服务器名称或后端服务器的端口。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。

   b) 虚拟服务器。您可以指定以下任一项：

      i. 虚拟服务器 IP 地址

      ii. 虚拟服务器名称，或

      iii. 运行应用程序的后端服务器的端口。

   可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。

3. 样本。您可以使用 Citrix ADM 中已存在的默认样本或自定义样本创建自定义应用程序。样本简化了为应用程序管理复杂的 Citrix ADC 配置的任务。选择 Citrix ADM 中存在的样本，然后键入样本参数值 Citrix ADM 基于所选样本在目标 Citrix ADC 实例上创建配置（配置包）。Citrix ADM 还创建一个自定义应用程序，其中包括在配置包中定义的所有虚拟服务器。

> 注意
>
> 如果有足够的 Citrix ADC 许可证可用，则会创建自定义应用程序和配置包。

当您创建满足上述三个条件之一中定义的这些条件的应用程序时，当 Citrix ADM 轮询实体时，该应用程序会在应用程序控制板中自动更新。要手动启动轮询，请单击位于 **Applications**（应用程序）选项卡中的 **Poll Now**（立即轮询）。

创建应用程序

1. 在 Citrix ADM 中，导航到 应用程序 > 控制板，然后单击 定义自定义应用程序 以创建自定义应用程序。
2. 在“定义应用程序”窗口中，在“名称”字段中键入应用程序的 名称。
3. 从“类别”部分中选择应用程序 类别。Citrix ADM 允许您定义类别以对用户定义的应用程序进行分组。您还可以根据需要添加更多类别。
4. 您可以使用以下三种方法之一创建自定义应用程序：

   a) 选择现有应用程序。要选择现有应用程序，请确保已启用“选择现有应用程序”。从“应用程序”部分的列表中选择 应用 程序。单击“添加应用程序”将新应用程序添加到列表中。

   b) 定义选择条件。您还可以定义在 Citrix ADM 中添加应用程序的选择条件。您可以使用以下三种方法之一添加应用程序：

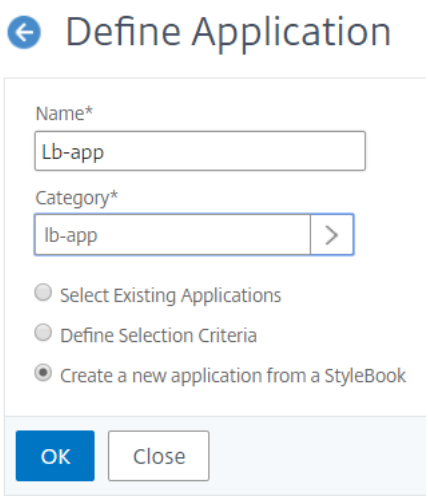
      i. 指定虚拟服务器的 IP 地址。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。

      ii. 指定运行应用程序或服务的服务器的名称。

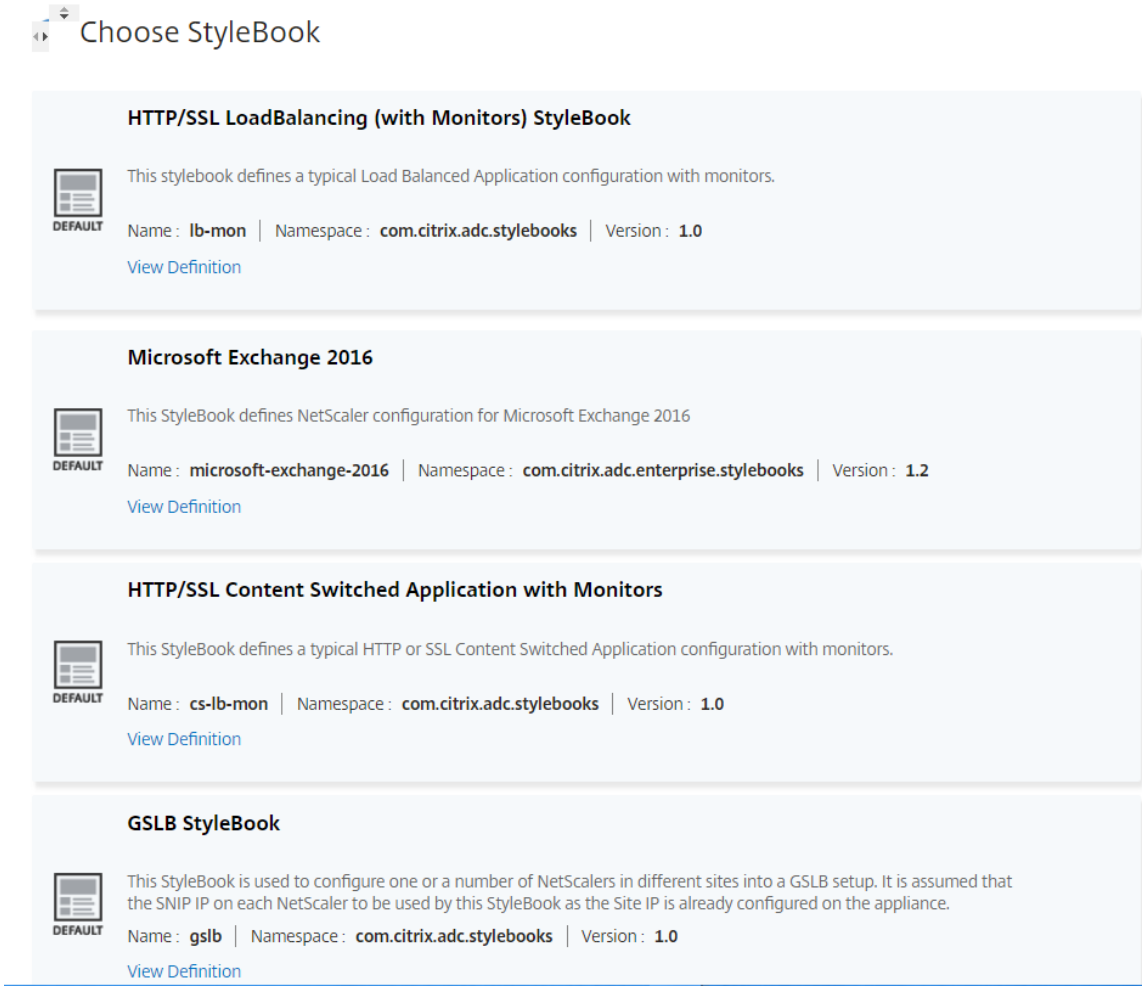
      > 注意
      >
      > 您还可以使用通配符扩展名搜索服务器名称。例如，ssl* 会将所有 ssl 虚拟服务器添加到应用程序。

      iii. 指定选定应用程序在服务器上侦听的端口号。

   c) 从样本创建新应用程序。在 Citrix ADM 中选择所需的样本，以在 Citrix ADC 实例上创建配置包，并将虚拟服务器与自定义应用程序关联。



5. 单击确定。如果您选择使用样书创建应用程序，则会打开“选择样书”页面。此页面包含 Citrix ADM 中存在的所有样本的列表。

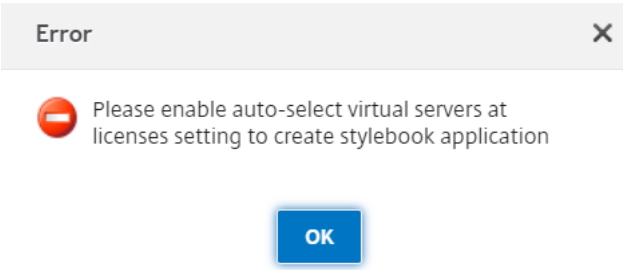


6. 选择样书。样本作为用户界面窗体打开。键入样书中所有参数的值。在使用样书之前，您也可以单击“查看定义”来查看样书的结构。有关如何使用自定义或默认样本的详细信息，请参阅 使用默认样书。
7. 现在，在样本的目标部分中选择的 Citrix ADC 实例上创建自定义应用程序和配置包

> 注意
>
> 如果有足够的 Citrix ADM 许可证可用，则会创建自定义应用程序和配置包。

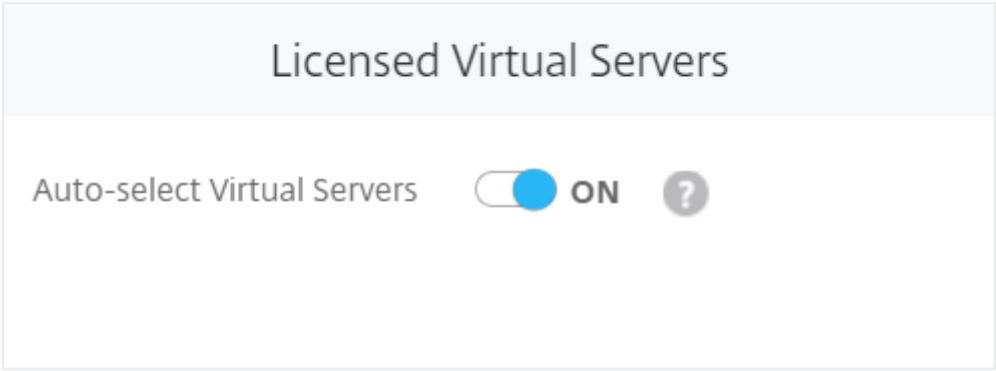
自动选择虚拟服务器进行许可

使用样本选项创建配置时，必须允许 Citrix ADM 自动选择要授权的虚拟服务器。如果您尚未启用自动选择，您可能会收到错误消息，如下图所示：



要启用虚拟服务器的自动选择：

1. 在 Citrix ADM 中，导航到网络 > 许可证 > 系统许可证。
2. 单击自动选择虚拟服务器以启用许可使用的虚拟服务器部分中的选项。



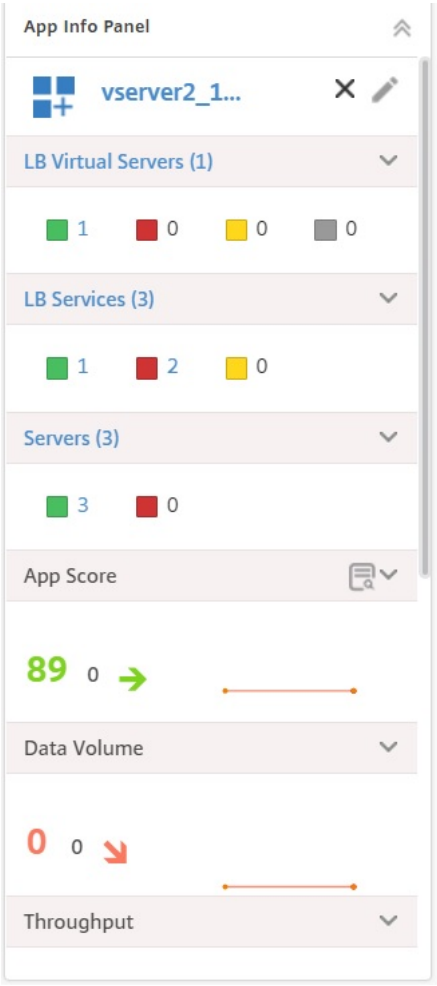
启用后，Citrix ADM 会自动选择要许可的虚拟服务器。如果未启用，则必须显式选择虚拟服务器。

在 **Citrix ADM** 中查看应用程序详细信息

Citrix ADM 在最右侧一个名为 **App Info Panel**（应用程序信息面板）的单独窗格中显示应用程序的所有详细信息。

要查看应用程序信息面板，请执行以下操作：

1. 在 Citrix ADM 中，导航到“应用程序”>“控制板”。
2. 在“应用程序概述”部分，单击要查看其详细信息的应用程序。



绑定到您选择的应用程序的实体纵向排列在 **App Info Panel**（应用程序信息面板）窗格中。窗格中垂直排列的框显示以下内容：

- 每个实体的名称
- 处于活动状态的实体数量
- 处于非活动状态的实体
- 不服务的实体

此处显示的实体为虚拟服务器、服务、服务组和应用程序服务器。该窗格还显示其他数据，例如，应用程序分数、数据量、吞吐量、服务器端连接数和客户端连接数以及每个应用程序中发生的事务数。

您可以查看每个应用程序的处于不同状态的虚拟服务器、服务和服务组计数。您可以单击实体名称或显示的计数来直接启用或禁用实体。您还可以启用或禁用其他绑定实体，例如，虚拟服务器、服务和服务组。

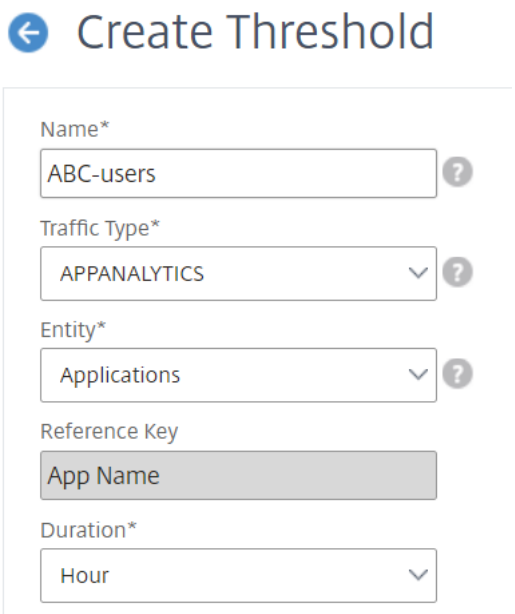
有关如何配置负载平衡服务器的详细信息，请参阅通过应用程序控制板创建负载平衡支持。

为应用程序分析创建阈值和警报

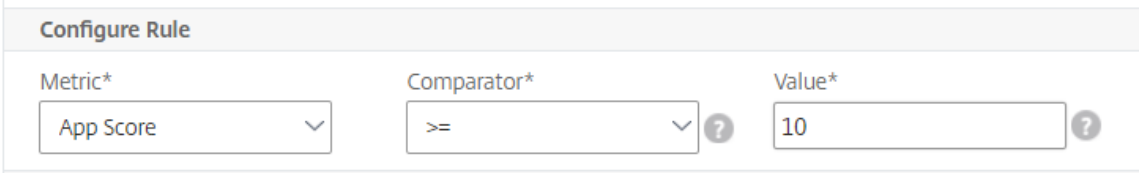
February 6, 2024

Citrix ADM 上的应用程序分析允许您监视通过 Citrix 实例的各种类型的流量。Citrix ADM 允许您在用于监视洞察流量的各种计数器上设置阈值。您还可以在 Citrix ADM 中配置规则和创建警报。

1. 在 Citrix ADM 中，导航到分析 > 设置 > 阈值。在“阈值”页上，单击“添加”。
2. 在“创建阈 值”页面上，指定以下详细信息：
   a) 名称。键入用于创建 Citrix ADM 生成警报的事件的名称。
   b) 流量 类型。从列表框中，选择安全分析。
   c) 实体。从列表框中，选择类别或资源类型。默认情况下，选择“应用程序”作为实体。
   d) 参考 密钥。参考密钥是根据您选择的流量类型和实体自动生成的。
   e) 持续时间。从列表框中选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。

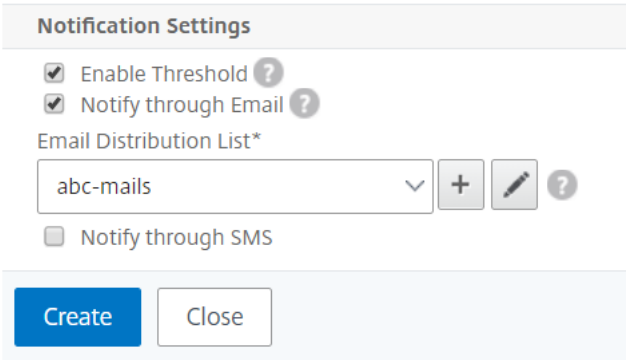


3. 在“配置规则”部分中，通过选择“应用分数”指标、所需的比较器来创建规则，并提供阈值。



4. 单击“启用阈 值”以允许 Citrix ADM 开始监视实体。

5.（可选）配置操作，如电子邮件通知和 SMS 通知。单击创建。



样书

February 6, 2024

样本简化了为应用程序管理复杂的 Citrix ADC 配置的任务。样书是可以用来创建和管理 Citrix ADC 配置的模板。可以创建用于配置 Citrix ADC 特定功能的样书，也可以设计样书为企业应用程序部署（例如 Microsoft Exchange 或 Lync）创建配置。

样书非常符合 DevOps 团队实践的基础结构即代码原则，其中，配置是声明性且版本受控的。配置还是重复使用的，并作为整体部署。样书具有以下优势：

- 声明式：样书是用声明式语法而不是命令式语法编写的。样书允许您专注于描述配置的结果或“所需状态”，而不是关于如何在特定 Citrix ADC 实例上实现配置的分步说明。Citrix Application Delivery Management (ADM) 计算 Citrix ADC 上的现有状态与您指定的所需状态之间的差异，然后对基础架构进行必要的编辑。由于样本使用用 YAML 编写的声明语法，因此样本的组件可以按任意顺序指定，Citrix ADM 根据其计算的依赖关系确定正确的顺序。
- 原子：使用样书部署配置时，将部署完整配置或不部署任何配置，这可确保基础结构始终处于一致状态。
- 版本化：样书具有将其与系统中的任何其他样书唯一区分开的名称、命名空间和版本号。对样书进行任何修改均需要更新其版本号（或者其名称或命名空间）以维护此唯一特征。此外，通过版本更新可以维护同一样书的多个版本。
- 可组合：定义了样书后，可以将该样书用作构建其他样书的单元。您可以避免重复使用配置的公用模式。此外，通过它您还可以在您的组织中建立标准构建块。由于样书是版本化的，因此，对现有样书进行更改会产生新的样书，从而确保绝不会意外破坏依赖样书。
- 以应用程序为中心：可以使用样书定义完整应用程序的 Citrix ADC 配置。可以使用参数提取应用程序的配置。因此，基于样书创建配置的用户可以与一个简单界面交互，包括填写一些参数来创建复杂的 Citrix ADC 配置。基于样书创建的配置不绑定到基础结构。因此，可以在一个或多个 Citrix ADC 上部署单个配置，也可以在实例之间移动单个配置。

- 自动生成的 **UI**：Citrix ADM 会自动生成 UI 表单，用于在使用 Citrix ADM GUI 进行配置时填写样书的参数。样书作者无需了解新的 GUI 语言或单独创建 UI 页面和表单。
- **API** 驱动：通过使用 Citrix ADM GUI 或通过 REST API 支持所有配置操作。可以在同步模式或异步模式下使用 API。除了配置任务外，通过样书 API 还可以在运行时发现任何样书的架构（参数说明）。

可以使用一个样书创建多个配置。每个配置都保存为一个配置包。例如，假设有一个定义典型 HTTP 负载平衡应用程序配置的样书。可以创建包含用于负载平衡实体的值的配置，然后在 Citrix ADC 实例上执行该配置。此配置保存为一个配置包。可以使用同一样书创建包含不同值的另一个配置，然后在同一或不同的 Citrix ADC 实例上执行该配置。即为此配置创建一个新配置包。配置包可以同时保存在 Citrix ADM 中和对其执行该配置的 Citrix ADC 实例中。

可以使用 Citrix ADM 附带的默认样书为您的部署创建配置，也可以设计您自己的样书并将其导入 Citrix ADM。您可以使用 Citrix ADM GUI 或使用 API 来基于样书创建配置。

本文档包含以下信息：

- 如何查看样书
- 默认样书
- 为业务应用程序开发的样书
- 自定义样书
- 样书中的 API
- 样书语法

样书组

February 6, 2024

Citrix Application Delivery Management (ADM) 中的样书可以通过两种方式进行分组。它们可以分组为默认样书或自定义样书。或者，它们也可以分组为公共或私人样书。在 Citrix ADM 中，您可以查看系统中存在的所有样书。Citrix ADM 还允许您对样书进行排序和查看。您还可以查看样书之间如何连接的图形显示。

本文档还介绍了如何下载和删除自定义样书。您可以下载自定义样书进行修改或在之前的样书的基础上创建新的样书。您还可以删除自定义样书。

默认和自定义样书

- 默认样书是 Citrix ADM 文件系统中存在的样书，它们允许您创建可以在 Citrix ADC 实例上部署的配置。
- 定制样书是您自己的样书，您可以编写并导入到 Citrix ADM，也可以创建配置对象。

默认样书和自定义样书都可以是公开的也可以是私有的。

公共和私人样书

您可以从中创建配置包以部署在 Citrix ADC 实例上的样书可以归类为“公共”样书。也就是说，它们都可供您直接用于创建配置。

但是，有些样书被用作其他样书的基石。这些构件是默认样书所包含的内置样书。这样的样书被称为“私有”样书。尽管它们不直接用于在实例上创建配置包，但您可能希望在 Citrix ADM 上显示这些样书。要将样书标记为私有，可以使用私有属性来防止样书在 Citrix ADM 上列出。

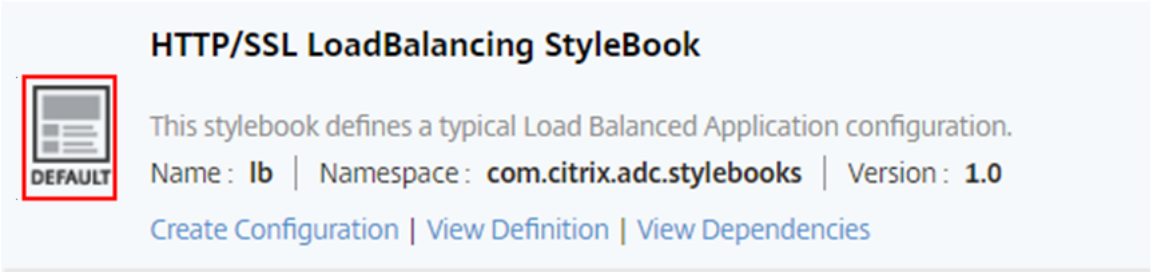
```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration and is a building block to build other load balancing
   configurations.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

查看样书

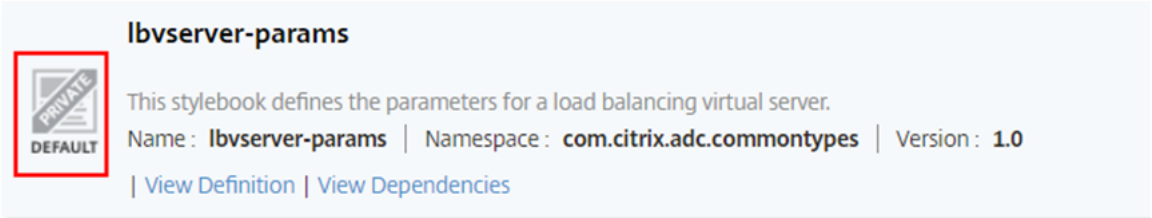
Citrix ADM 中的样书（包括默认样书和私有样书）的数量都在增加。您可能需要搜索您想要访问的特定样书。您可能还想分别查看这两种类型的样书。

在 Citrix ADM 中，当您导航到应用程序 > 样书时，您可以查看系统中存在的样书列表。

默认的公共样书面板上有以下图标：

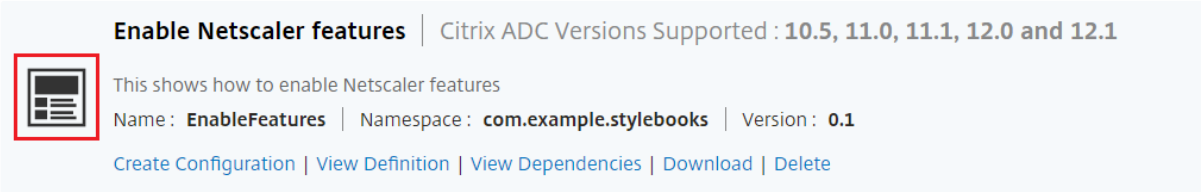


而默认的私有样书有一个将其声明为私有样书的图标：

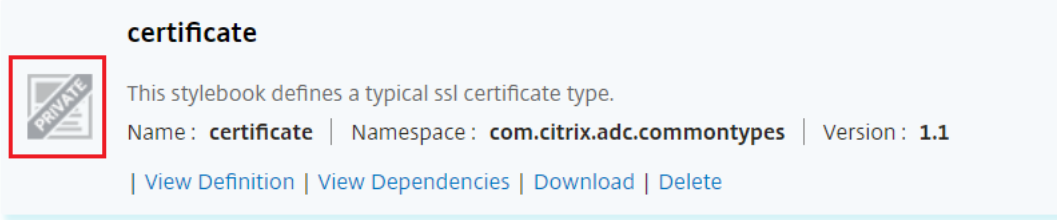


虽然您可以查看专用样书的定义和依赖关系，但无法从专用样书创建配置包。您仍然可以在自己的样书中使用私人样书。

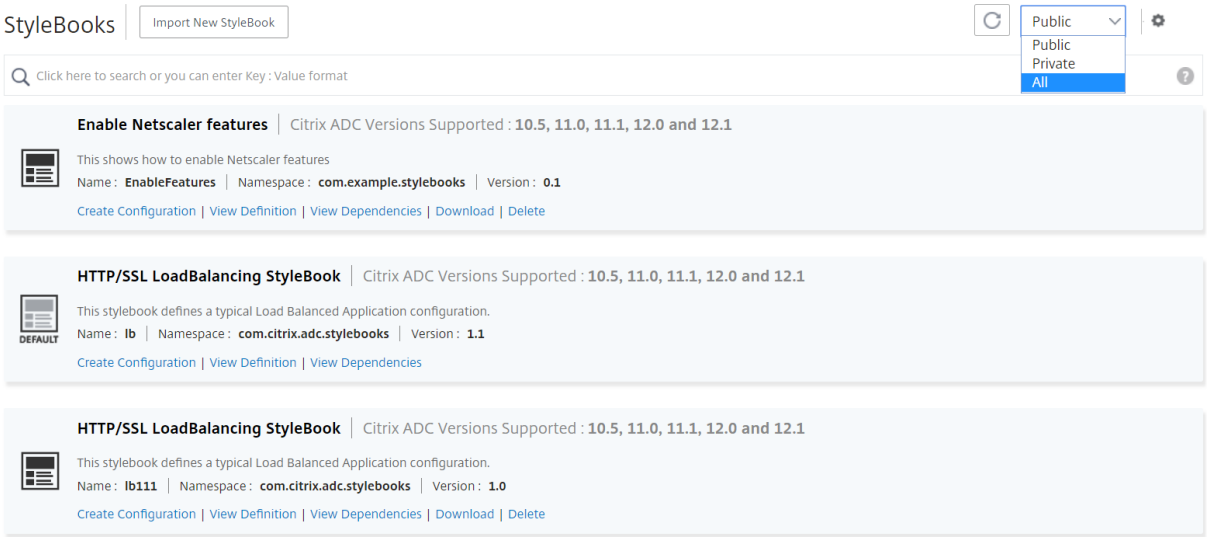
自定义构建的公共样书具有不同的图标，如下图所示：



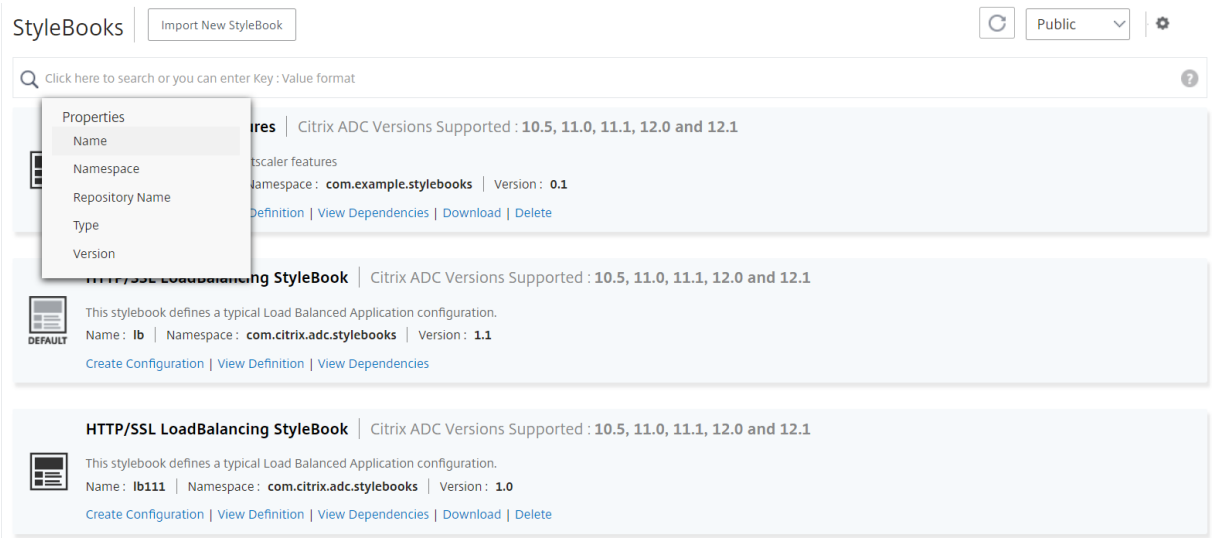
同时，自定义构建的专用样书将显示以下图标：



在页面右上角，您可以看到对样书进行排序的选项。共有三个选项——全部、公共或私有样书。单击其中一个选项。



您也可以通过单击搜索图标来搜索特定样书。可用的三个搜索选项是名称、命名空间和版本。搜索操作不区分大小写。



查看样书依赖关系

Citrix ADM 允许您查看样书之间如何连接的图形显示。

在 Citrix ADM 中，您可以使用默认样书为部署创建配置。您也可以设计自己的样书并将其导入到 Citrix ADM。

样书一个重要的强大功能是它们可以用作其他样书的构建块。您可以将样书导入到另一个样书中。导入的样书被声明为一种类型，并由第二本样书的组件或参数使用。

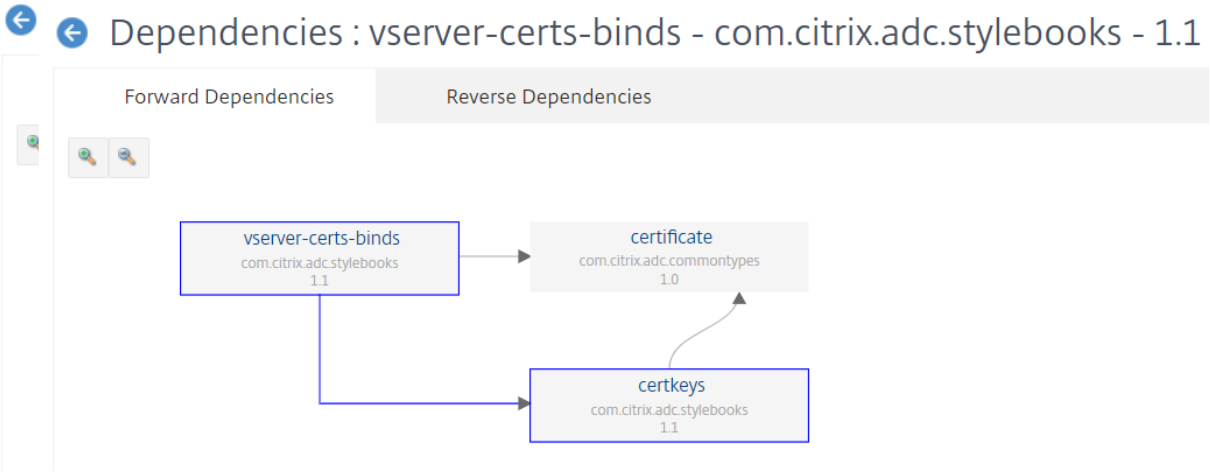
无法从系统中删除其他样书使用的样书。但是，样书的图形显示可以让您知道哪些样书阻碍了样书的移除。通过查看图表，可以看到多本样书之间的关系。

查看样书依赖关系

在 Citrix ADM 中，导航到应用程序 > 样书。“样书”页面显示可供您在 Citrix ADM 中使用的所有样书。向下滚动并找到您的样书。样书面板显示创建配置、查看样书定义和查看样书依赖关系的链接。单击 查看依赖关系。

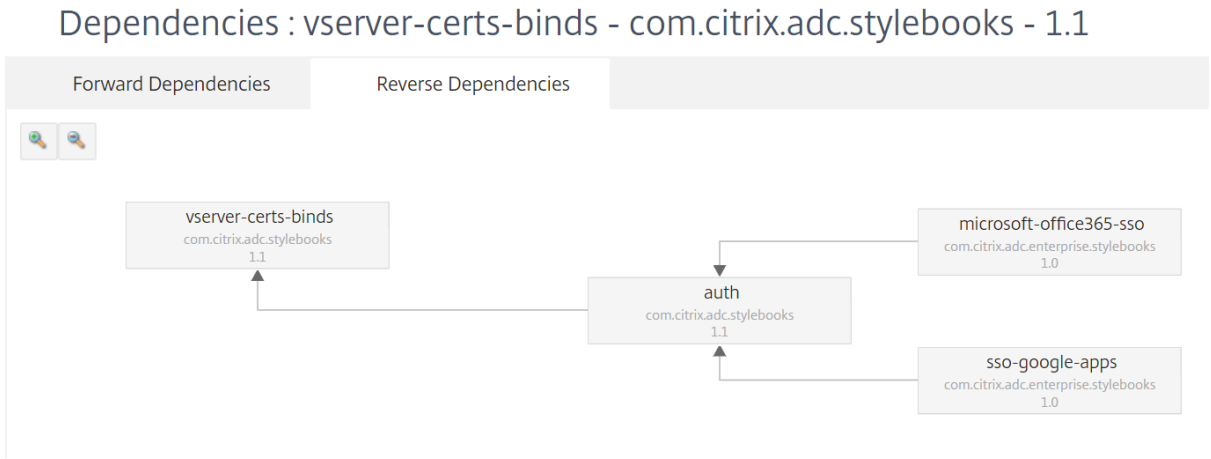
前向依赖关系

“转发依赖关系”选项卡允许您查看样书正在使用的不同默认样书。按照箭头查找样书正在使用的样书。当您将鼠标指向其中一个箭头时，该箭头和相互连接的样书将突出显示。您也可以单击样书名称来查看该样书的定义。



逆向依赖关系

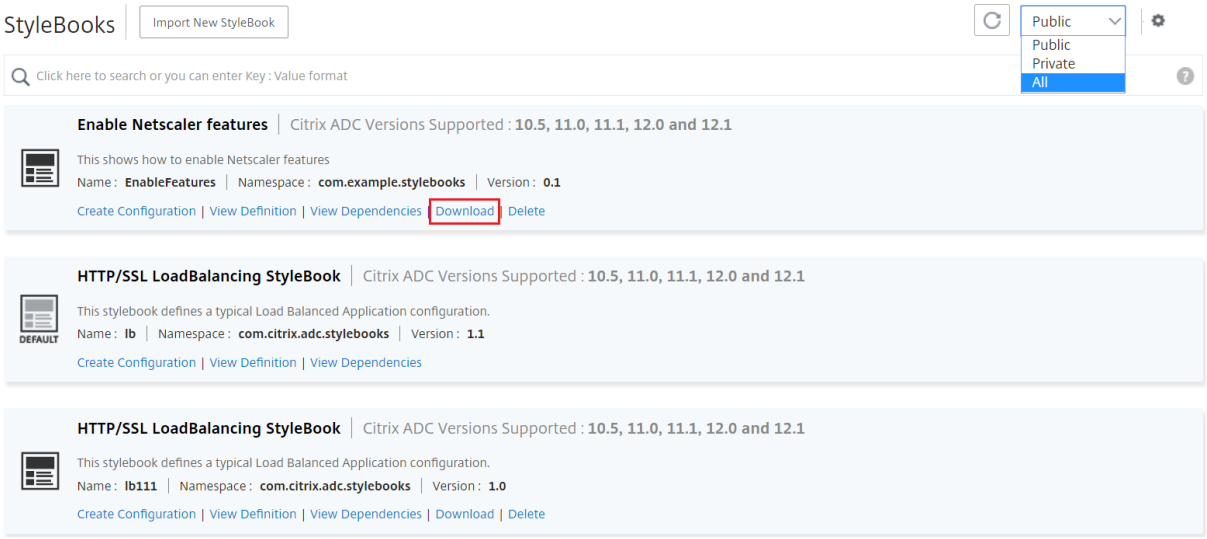
“反向依赖关系”选项卡允许您以图形方式查看使用样书的样书。如果您跟着箭头走，您可以看到显示屏中的所有样书都指向您的样书。有些样书可能直接使用样书，有些样书可能正在通过其他样书使用样书。



下载自定义样书

要从 Citrix ADM 下载自定义样书，请导航到应用程序 > 样书 > 配置。在右侧面板上显示的样书列表中，自定义样书可以选择下载它们。单击下载。如果样书有相关的自定义样书，则即使这些样书也会下载到您的系统中。

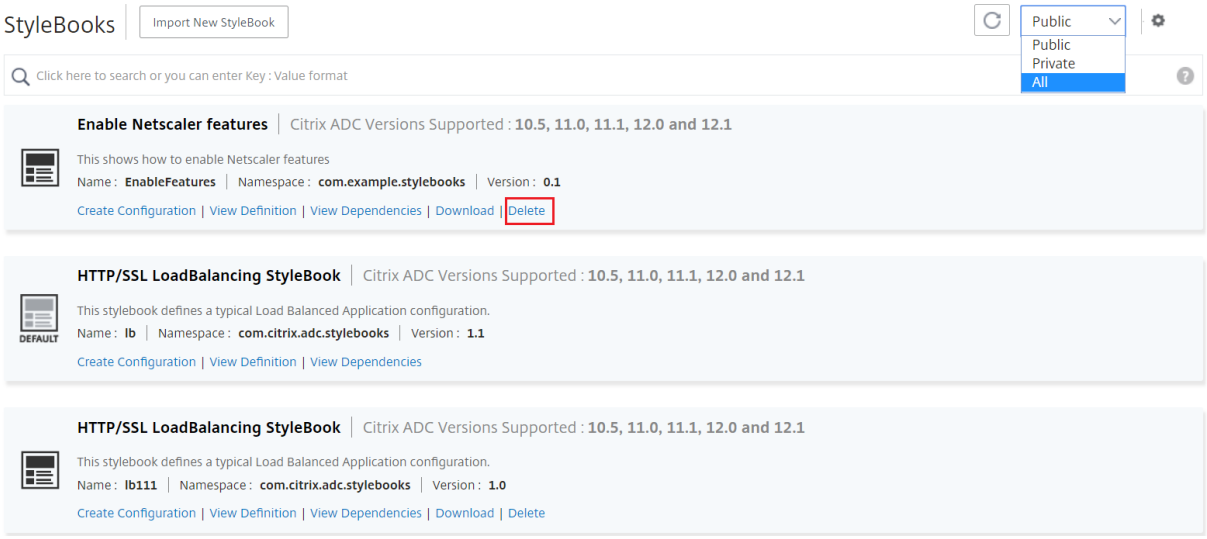
> 注意
>
> 您不能下载标记为公共或私有的默认样书或自定义样书。



> 注意
>
> 您无法下载 Citrix ADM 默认样书。但是，您可以通过单击样书面板上的“查看定义”和“查看依赖关系”链接来查看它们的定义和依赖关系。

删除自定义样书

您还可以通过单击样书面板右侧的“X”图标来删除自定义样书。弹出窗口会提示您确认是否要从 Citrix ADM 中删除样书。如果样书使用其他自定义样书（其他样书未使用），则也可以通过选中该复选框来选择将其删除。



> 注意
>
> 您不能删除 Citrix ADM 中具有其他样书依赖于该样书的自定义样书。

从 **GitHub** 存储库导入和同步样书

February 6, 2024

假设您正在使用 CI/CD 流程进行开发，或者您正在管理 GitHub 中的所有部署对象。您可能已经创建了几本用于部署 Citrix ADC 配置的样本，而且您正在管理 GitHub 存储库中的样本。现在，您可以直接将这些样本导入 Citrix 应用程序和交付管理 (ADM)。您无需手动将它们从 GitHub 中复制出来然后上载到 Citrix ADM。

现在，您可以通过提供 GitHub 仓库 URL 在 Citrix ADM 中定义一个代表 GitHub 仓库的仓库。您必须提供在 GitHub 中创建的用户名和密码（或 API 令牌）。这意味着只有在 GitHub 中拥有有效帐户的授权用户才能导入和同步样书。

创建存储库后，您可以将 Citrix ADM 与您的 GitHub 存储库同步。Citrix ADM 导入该存储库中的样书，然后对其进行验证，并将其添加到 Citrix ADM 中的样书列表中。如果样本无法验证，则不会添加到 Citrix ADM 中。您必须更正错误并将更新版本提交到您的 GitHub 存储库中。稍后，您可以尝试将它们导入或将它们再次同步到 Citrix ADM 中。

> 注意
>
> - 目前，您只能导入和同步没有相关样本的样书。也就是说，样书必须具有在一个文件中定义所需的所有配置。
> - 来自 GitHub 存储库的同步需要从 Citrix ADM GUI 或 API 手动启动。也就是说，目前，样书的导入不会根据 GitHub 的提交活动自动进行。
>
> 目前，您只能从主分支导入样书文件。

必备条件

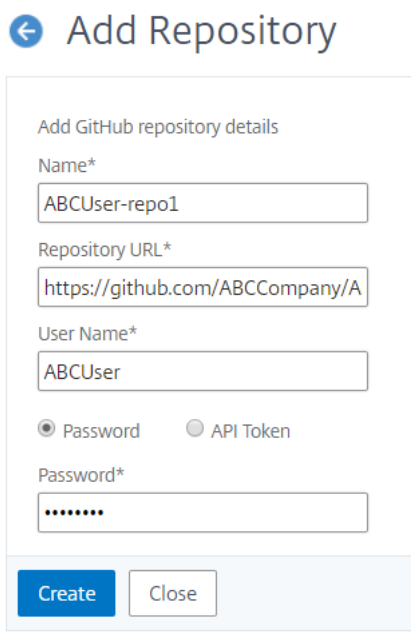
- 您必须在 GitHub 中拥有一个有效的帐户。
- 样书文件必须存在于 GitHub 存储库中主分支的根文件夹中。

添加存储库并从 **GitHub** 导入样本

1. 在 Citrix ADM 中，导航到 应用程序 > 配置 > 存储库。
2. 单击添加。在 添加存储库 窗口中，输入以下参数：
   - 名称。键入存储库的名称。此名称可以与 GitHub 中的存储库名称相同，也可以与其他名称相同。
   - 存储库 **URL**。键入 GitHub 存储库的 URL。
   - 用户名和密码。键入用于访问 GitHub 帐户的用户名和密码。

     > 注意 您也可以提供 API 令牌来代替密码。API 令牌可以通过 HTTPS 使用代替 GitHub 的密码。您还可以使用它们通过基本身份验证向 API 进行身份验证。

3. 单击创建。



在 Citrix ADM 中创建存储库。

4. 要导入或同步 样书，请在“存储库”页面中选择 存储库，然后单击“同步”。

您可以在此处使用的其他操作是：

- 编辑。您可以编辑存储库 URL、用户名和密码（或 API 令牌）。
- 删除。您可以删除存储库以及 Citrix ADM 中存在的所有样本，这些样本是之前从该 GitHub 存储库导入的。

  > 注意
  >
  > 如果某个存储库具有与其关联的 ConfigPack 的任何样本，则无法从 Citrix ADM 中删除该存储库。

- 重置。您可以删除 Citrix ADM 中从该存储库同步的所有样本，而无需实际删除 Citrix ADM 中的存储库条目。
- 列出文件。您可以看到来自 GitHub 存储库的 Citrix ADM 中存在的所有样书的列表。

使用默认样书

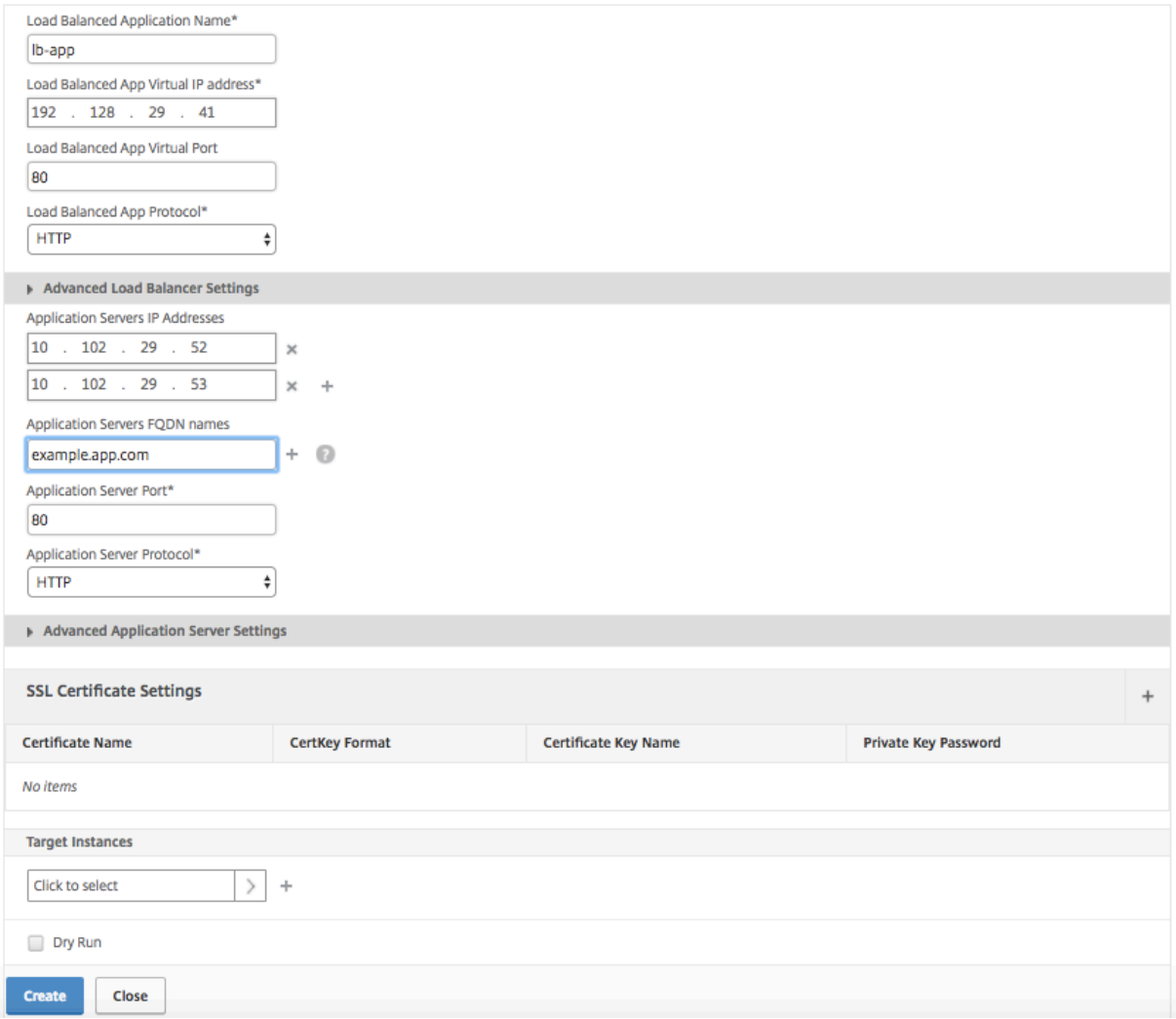
February 6, 2024

Citrix Application Delivery Management (ADM) 提供了一组默认样本。使用默认样书时，必须为样本中的参数指定值，然后选择要在其中执行配置的 Citrix ADC 实例的 IP 地址。提交配置后，Citrix ADM 将验证您指定的参数值，创建配置图，连接到 Citrix ADC 实例，然后在实例上执行配置。

从默认样本创建配置

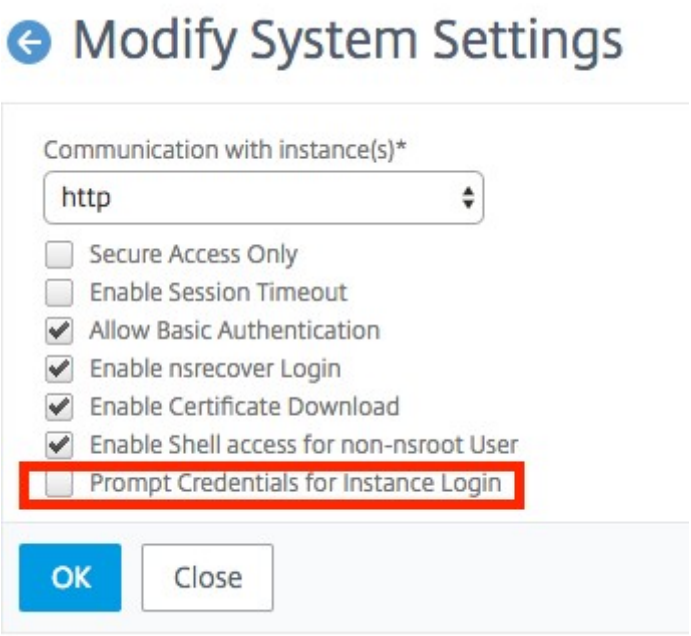
1. 导航到“应用程序”>“配置”**>**“样本”。样书页面显示 Citrix ADM 中的所有样书。此列表包括默认样本和自定义样本。可以在搜索字段中键入样书的名称，然后按 **Enter** 键。否则，您可以向下滚动列表来找到样本。

2. 单击“创建配置”。指定参数所需值。

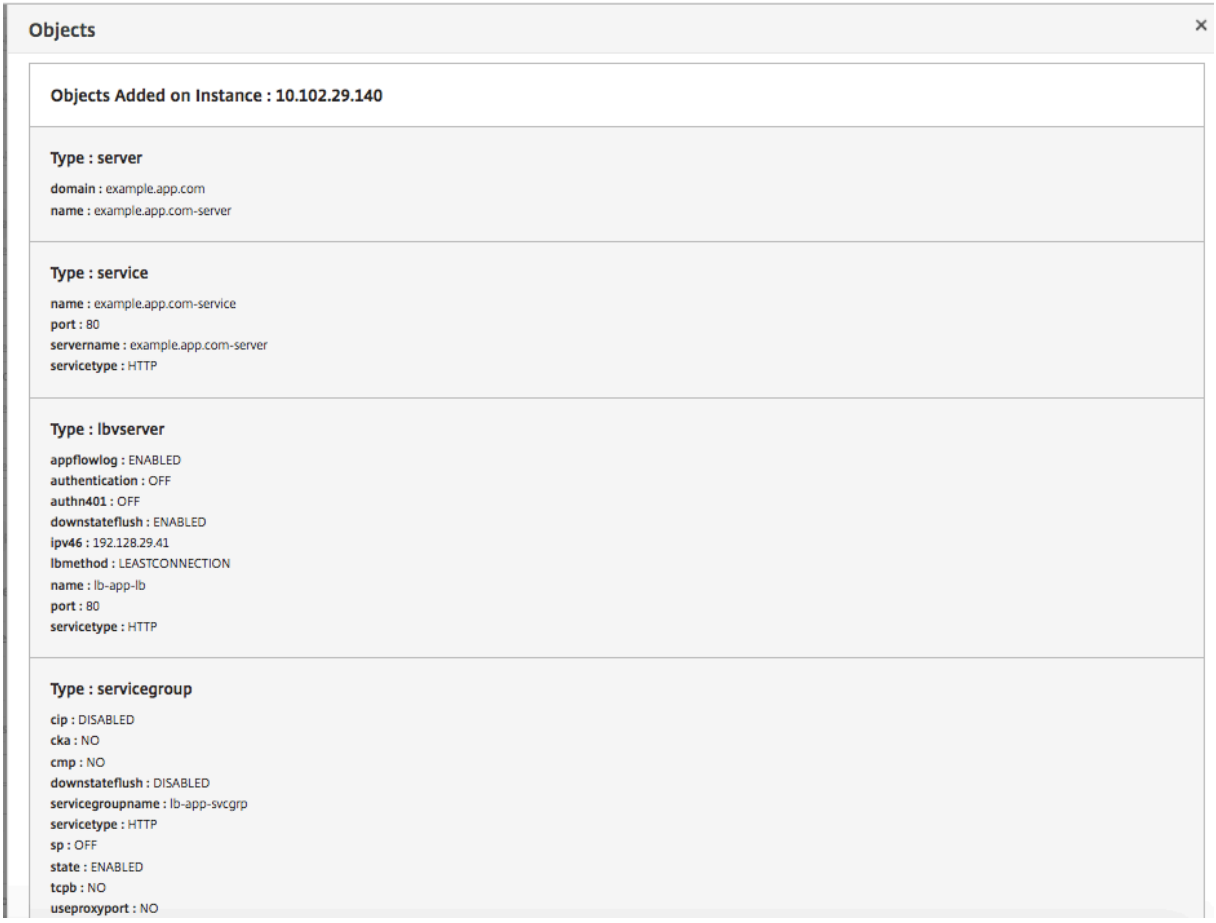


3. 在“目标实例”下，单击并选择要在其中执行配置的 Citrix ADC 实例的 IP 地址。如果要在多个实例上执行此配置，请单击“+”添加更多实例。

如果在 ****Citrix ADM**> 系统 **>** 更改系统设置 **>** 修改系统 ** 设 置中启用了“提示实例登录凭据”选项，则在选定的 Citrix ADC 实例上执行配置时，系统会提示您输入 Citrix ADC 实例凭据。否则，Citrix ADM 使用存储在实例配置文件中的实例凭据登录到实例。



如果要在 Citrix ADC 实例上执行配置之前对其进行测试或验证，请选择试运行，然后单击创建。如果配置有效，将显示根据您提供的值创建的对象。



4. 清除试运行复选框，然后单击创建以在 Citrix ADC 实例上创建配置并执行配置。您创建的样书配置将显示在配置列表中，如下所示。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

现在，您可以使用 Citrix ADM 检查、更新或删除此配置包。

隐藏所有默认样书

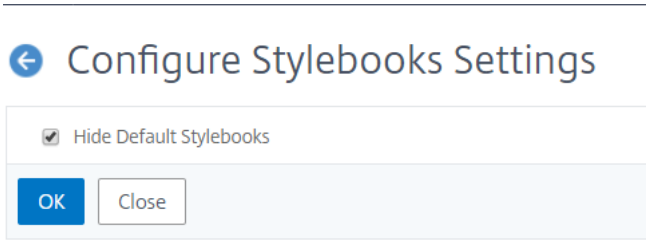
February 6, 2024

Citrix ADM 列出了 Citrix ADM 文件夹系统中存在的所有样本。样书列表包括默认和自定义样书，这些样书既可以是私有的，也可以是公有的。作为管理员，您可能需要隐藏所有默认样书。您可以允许您的用户仅查看和访问由您或用户创建的自定义样书。

Citrix ADM 允许您显示自定义样书并隐藏 Citrix ADM 附带的所有默认样书。提供了一个新的 GUI 选项，您可以在其中隐藏所有默认样书。

要隐藏所有默认样书，请执行以下操作：

1. 在 Citrix ADM 中，导航到 应用程序 > 配置 **>** 设置。
2. 设置 页面显示用户是否可以看到默认样书的信息。
3. 要隐藏默认样书，请单击右上角的编辑图标。
4. 在 配置样书设置 页面上，选择 隐藏默认样书 选项。
5. 单击确定。



如果您未选择使用 RBAC 功能隐藏“配置样书设置”页面，则用户仍然可以看到该页面。用户可能仍然可以选择取消隐藏默认样书。

要隐藏“配置样书设置”页面，必须创建一个策略并将该策略分配给那些不应看到默认样书的用户。

要创建 **RBAC** 策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 帐户 > 用户管理 > 访问策略。
2. 单击添加以创建策略。
3. 输入策略名称。
4. 在“权限”部分中，确保未选择“全部”>“应用程序”>“配置”>“设置”，然后单击“确定”。

创建策略后，您必须创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户组。要了解有关如何将策略与用户关联的更多信息，请参阅 配置基于角色的访问控制。

SSO Google Apps 样书

February 6, 2024

Google Apps 是由 Google 开发的云计算、生产力和协作工具、软件和产品的集合。单一登录 (SSO) 使用户能够通过使用企业凭据对所有服务进行一次登录，访问其所有企业云应用程序（包括登录管理员控制台的管理员）。

Citrix ADM SSO Google Apps 样书允许您通过 Citrix ADC 实例为 Google Apps 启用 SSO。样书将 Citrix ADC 实例配置为 SAML 身份提供商，用于对访问 Google Apps 的用户进行身份验证。

使用此样书在 Citrix ADC 实例中为 Google 应用程序启用 SSO 会产生以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IDP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略
5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器

配置详细信息：

下表列出了此集成成功运行所需的最低软件版本。集成过程还应适用于同一版本的更高版本。

产品	所需的最低版本
Citrix ADC	版本 11.0，Enterprise/Platinum 许可证

以下说明假定您已经创建了适当的外部和/或内部 DNS 条目，以将身份验证请求路由到 Citrix ADC 监视的 IP 地址。

部署 **SSO Google Apps** 样书配置：

以下任务可帮助您在企业网络中部署 Microsoft SSO Google Apps 样书。

部署 **SSO** 谷歌应用程序样书

1. 在 Citrix ADM 中，导航到“应用程序”>“配置”>“样书”。“样书”页面显示了所有在 Citrix ADM 中可供您使用的样书。向下滚动并找到 **SSO Google Apps** 样书。单击 创建配置。
2. 样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。
3. 输入以下参数的值：
   a) 应用程序名称。要在您的网络中部署的 SSO Google 应用程序配置的名称。
   b) 验证虚拟 **IP** 地址。Google Apps SAML IdP 策略绑定到的 AAA 虚拟服务器使用的虚拟 IP 地址。
   c) **SAML** 规则表达式。默认情况下，使用以下 Citrix ADC 策略 (PI) 表达式：HTTP.REQ.HEADER(“Referer”).CONTAINS(“google”)。如果您的要求不同，请使用其他表达式更新此字段。此策略表达式与应用这些 SAML SSO 设置的流量匹配，并确保 Referer 标头来自 Google 域。
4. SAML IdP 设 置部分允许您通过创建由在步骤 3 中创建的 AAA 虚拟服务器使用的 SAML IDP 配置文件和策略将 Citrix ADC 实例配置为 SAML 身份提供商。
   a) **SAML** 发行者名称。在此字段中，输入您的身份验证虚拟服务器的公共 FQDN。示例：`https://<Citrix ADC Auth VIP>/saml/login`
   b) **SAML** 服务提供商 **(SP) ID**。（可选）Citrix ADC 身份提供商接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。
   c) 断言消费者服务 **URL**。输入服务提供商的 URL，成功进行用户身份验证后，Citrix ADC 身份提供商需要在其中发送 SAML 声明。断言消费者服务 URL 可以在身份提供商服务器站点或服务提供商站点启动。
   d) 您还可以在此部分中输入其他可选字段。例如，您可以设置以下选项：
      i. SAML 绑定配置文件（默认为“POST”配置文件）。
      ii. 用于验证/签署 SAML 请求/响应的签名算法（默认为“RSA-SHA1”）。
      iii. 摘要 SAML 请求/响应的哈希值的方法（默认为“SHA-1”）。
      iv. 加密算法（默认为 AES256）和其他设置。

      > 注意
      >
      > Citrix 建议您保留默认设置，因为这些设置已经过测试，以便与 Google Apps。

   e) 您还可以启用用户属性复选框以输入用户详细信息，例如：
      i. 用户属性的名称
      ii. 用于提取属性值的 Citrix ADC PI 表达式
      iii. 该属性的用户友好名称
      iv. 选择用户属性的格式。

这些值包含在发布的 SAML 断言中。您可以在 Citrix ADC 使用此样书发布的声明中包含多达五组用户属性。

5. 在 LDAP 设置部分中，输入以下详细信息以对 Google Apps 用户进行身份验证。为了使域用户能够使用其公司电子邮件地址登录 Citrix ADC 实例，必须配置以下内容：

   a) **LDAP**（**Active Directory**）基地。输入要允许身份验证的 Active Directory (AD) 中用户帐户所在的域的基本域名。例如，dc=netscaler，dc=com

   b) **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，cn=Manager、dc=netscaler、dc=com

   c) **LDAP**（**Active Directory**）绑定 **DN** 密码。输入用于身份验证的域帐户的密码。

   d) 您需要在本节中输入的其他几个字段如下所示：

      i. Citrix ADC 连接用于对用户进行身份验证的 LDAP 服务器 IP 地址

      ii. LDAP 服务器的 FQDN 名称

      > 注意
      >
      > 您必须指定以上两项中的至少一个-LDAP 服务器 IP 地址或 FQDN 名称。

      iii. Citrix ADC 连接到的用于对用户进行身份验证的 LDAP 服务器端口（默认值为 389）。

      iv. LDAP 主机名。如果验证处于打开状态（默认情况下，它处于关闭状态），则用于验证 LDAP 证书。

      v. LDAP 登录名属性。用于提取登录名的默认属性是“samAccountname”。

      vi. 其他可选的其他 LDAP 设置

6. 在 SAML IdP SSL 证书部分中，您可以指定 SSL 证书的详细信息：

   a) 证书名称。输入 SSL 证书的名称。

   b) 证书文件。从本地系统或 Citrix ADM 上的目录中选择 SSL 证书文件。

   c) 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式是.pem 和.der 文件扩展名。

   d) 证书密钥名称。输入证书私钥的名称。

   e) 证书密钥文件。选择包含来自本地系统或 Citrix ADM 的证书私钥的文件。

   f) 私钥密码。如果您的私钥文件受密码保护，请在此字段中输入。

   g) 您还可以启用“高级证书设置”复选框来输入诸如证书到期通知期限之类的详细信息，启用或禁用证书到期监视器。

7. 或者，如果上面输入的 SAML IdP 证书要求在 Citrix ADC 上安装 CA 公共证书，则可以选择 IdP SSL CA 证书。确保在高级设置中选择“是 CA 证书”。

8. 或者，您可以选择 SAML SP SSL 证书来指定用于验证来自 Google Apps (SAML SP) 的身份验证请求的 Google SSL 证书（公钥）。
9. 单击“目标实例”，然后选择要在其上部署此 Google Apps SSO 配置的 Citrix ADC 实例。单击 创 建”以创建配置并在所选 Citrix ADC 实例上部署配置。

   > 注意
   >
   > 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

还有

> 提示
> >
> > Citrix 建议在执行实际配置之前，选择 **Dry Run** 以直观地确认样书在目标 Citrix ADC 实例上创建的配置对象。

SSO 办公室 365 样本

February 6, 2024

Microsoft™ Office 365 是一套基于云的生产力和协作应用程序，由 Microsoft 以订阅方式提供。它包括 Microsoft 流行的基于服务器的应用程序，如 Exchange、SharePoint、Office 和 Skype for Business。单点登录 (SSO) 使用户能够访问其所有企业云应用程序：

- 包括登录管理员控制台的管理员
- 使用其企业凭据一次性登录所有 Microsoft Office 365 服务。

SSO Office 365 样书允许您通过 Citrix ADC 实例为 Microsoft Office 365 启用 SSO。您现在可以配置 SAML 身份验证，将 Citrix ADC 作为 SAML 身份提供商 (IdP)，Microsoft Office 365 作为 SAML 服务提供商。

使用此样书在 Citrix ADC 实例中为 Microsoft Office 365 启用 SSO 涉及以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IDP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略
5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器。

该表列出了此集成成功运行所需的最低软件版本。集成过程还应适用于同一版本的更高版本。

产品	所需的最低版本
——	————————
Citrix ADC	11.0，Enterprise/Platinum 许可证

以下说明假定您已经创建了相应的外部和内部 DNS 条目。这些条目对于将身份验证请求路由到 Citrix ADC 监视的 IP 地址至关重要。

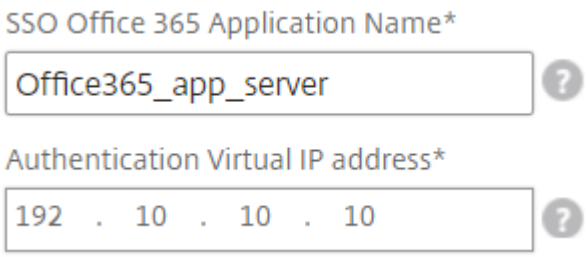
以下说明可帮助您在企业网络中实现 SSO Office 365 样书。

部署 **SSO Microsoft Office 365** 样书

1. 在 Citrix Application Delivery Management (ADM) 中，导航到应用程序 > 样本。样书页面显示了所有可供您在 Citrix ADM 中使用的样书。向下滚动并找到 **SSO Office 365** 样书。单击 创建配置。
2. 样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。
3. 输入以下参数的值：

   a) 应用程序名称。要在您的网络中部署的 SSO Microsoft Office 365 配置的名称。

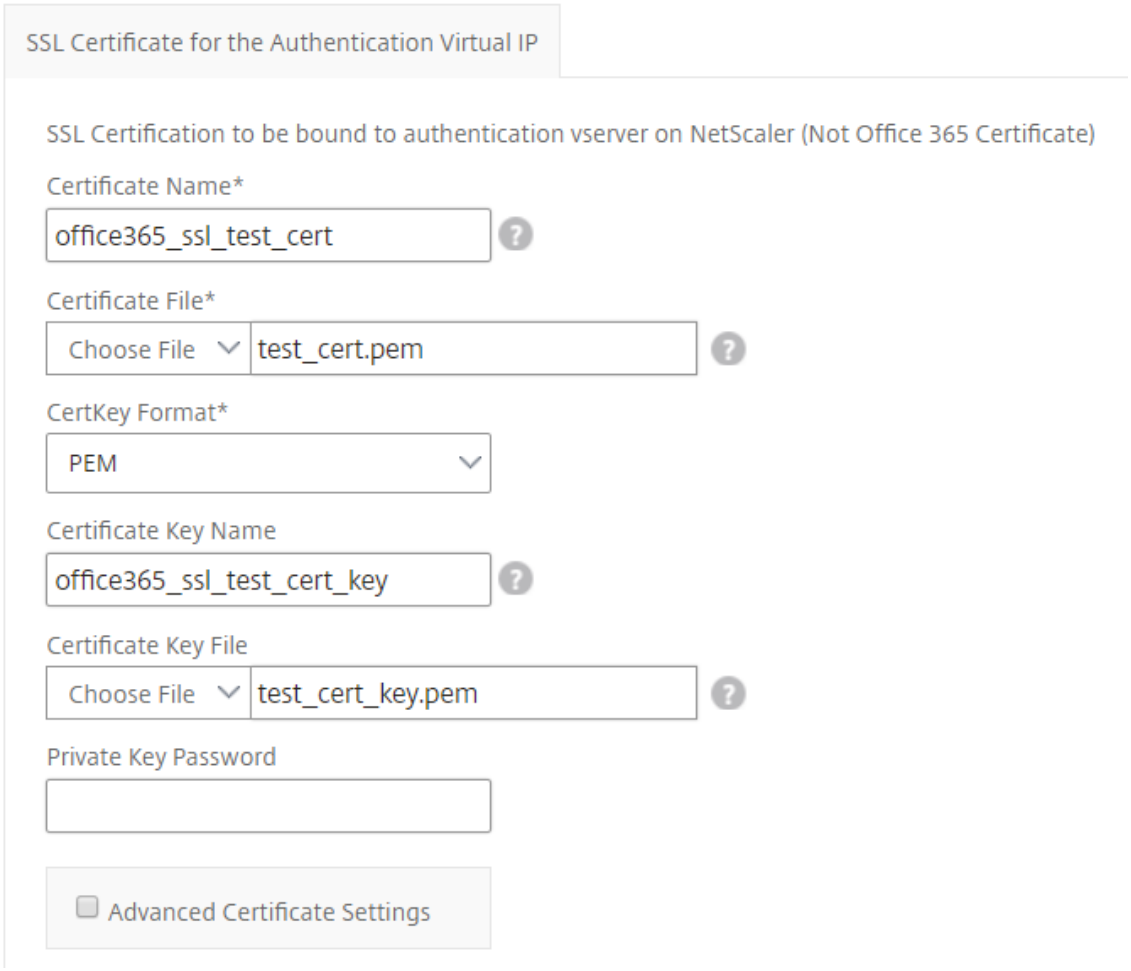
   b) 验证虚拟 **IP** 地址。虚拟 IP 地址供绑定 Microsoft Office 365 SAML IdP 策略的 AAA 虚拟服务器使用。



4. 在 **SSL** 证书设置部分，输入 SSL 证书和证书密钥的名称。

   > 注意
   >
   > 这不是 Office 365 服务提供商证书。此 SSL 证书绑定到 Citrix ADC 实例上的虚拟身份验证服务器。

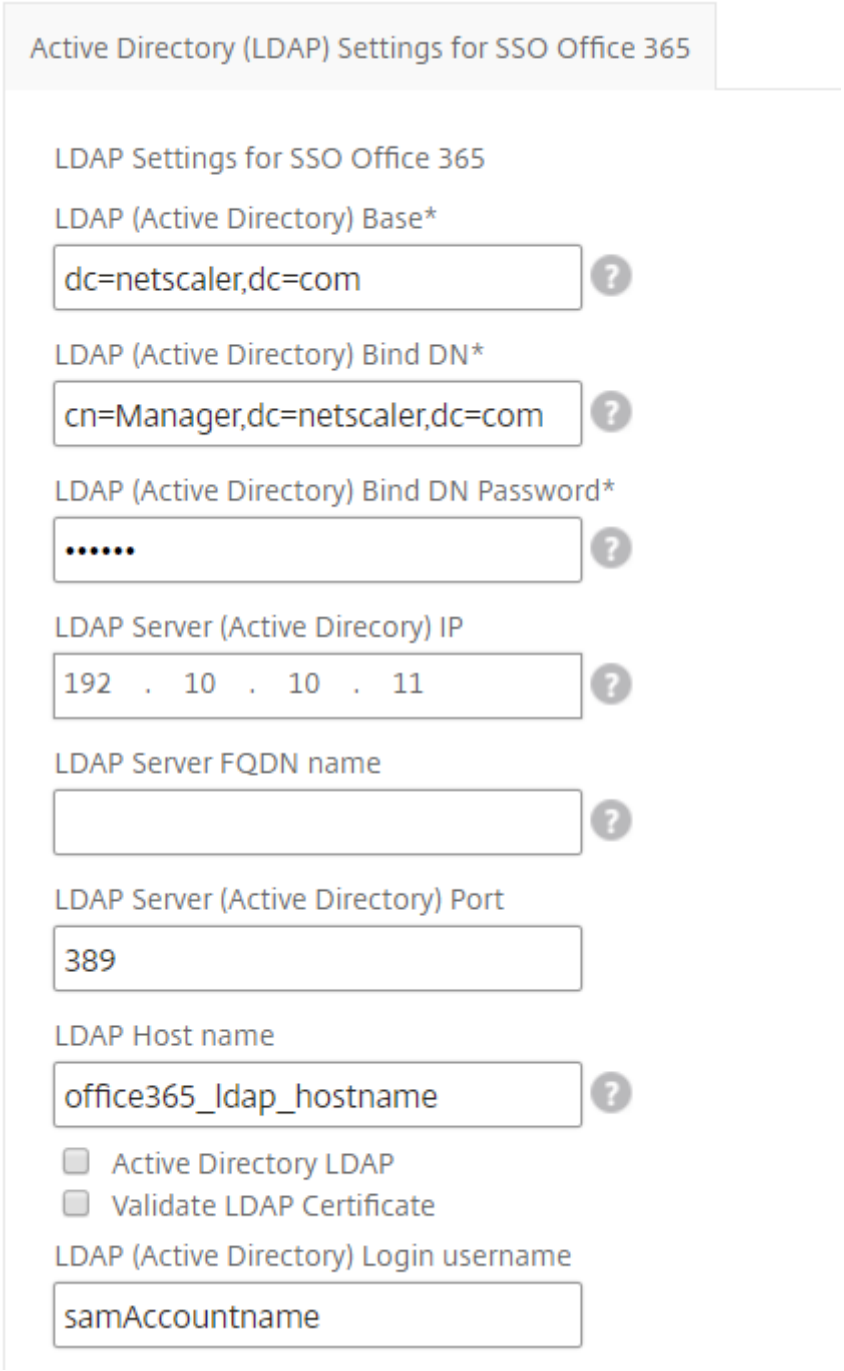
5. 从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以加载 PEM 格式的加密私钥。



6. 您还可以启用 高级证书设置”复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。
7. 或者，如果 **SSL** 证书要求在 **Citrix ADC** 上安装 **CA** 公共证书，则可以选择 **SSL CA** 证书作为身份验证虚拟 IP 复选框。确保在上述“高级证书设置”部分中选择“是 **CA** 证书”。
8. 在 **SSO Office 365** 的 **LDAP** 设置 部分，输入以下详细信息以对 Office 365 用户进行身份验证。要允许域用户使用其公司电子邮件地址登录 Citrix ADC 实例，请配置以下内容：
   - **LDAP**（**Active Directory**）基地。输入用户帐户驻留在 Active Directory (AD) 中的域的基本域名以允许身份验证。例如，dc=netscaler，dc=com
   - **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，cn=Manager、dc=netscaler、dc=com
   - **LDAP**（**Active Directory**）绑定 **DN** 密码。输入用于身份验证的域帐户的密码。
   - 您需要在本节中输入的其他几个字段如下所示：
     - Citrix ADC 连接的 LDAP 服务器 IP 地址，用于对用户进行身份验证。
     - LDAP 服务器的 FQDN 名称。

> 注意
>
> 您必须指定以上两项中的至少一个-LDAP 服务器 IP 地址或 FQDN 名称。

- Citrix ADC 连接到的用于对用户进行身份验证的 LDAP 服务器端口（默认值为 389）。LDAPS 使用 636。
- LDAP 主机名。如果启用了验证（默认情况下处于关闭状态），则主机名用于验证 LDAP 证书。
- LDAP 登录名属性。用于提取登录名的默认属性是“samAccountname”。
- 其他可选的其他 LDAP 设置。

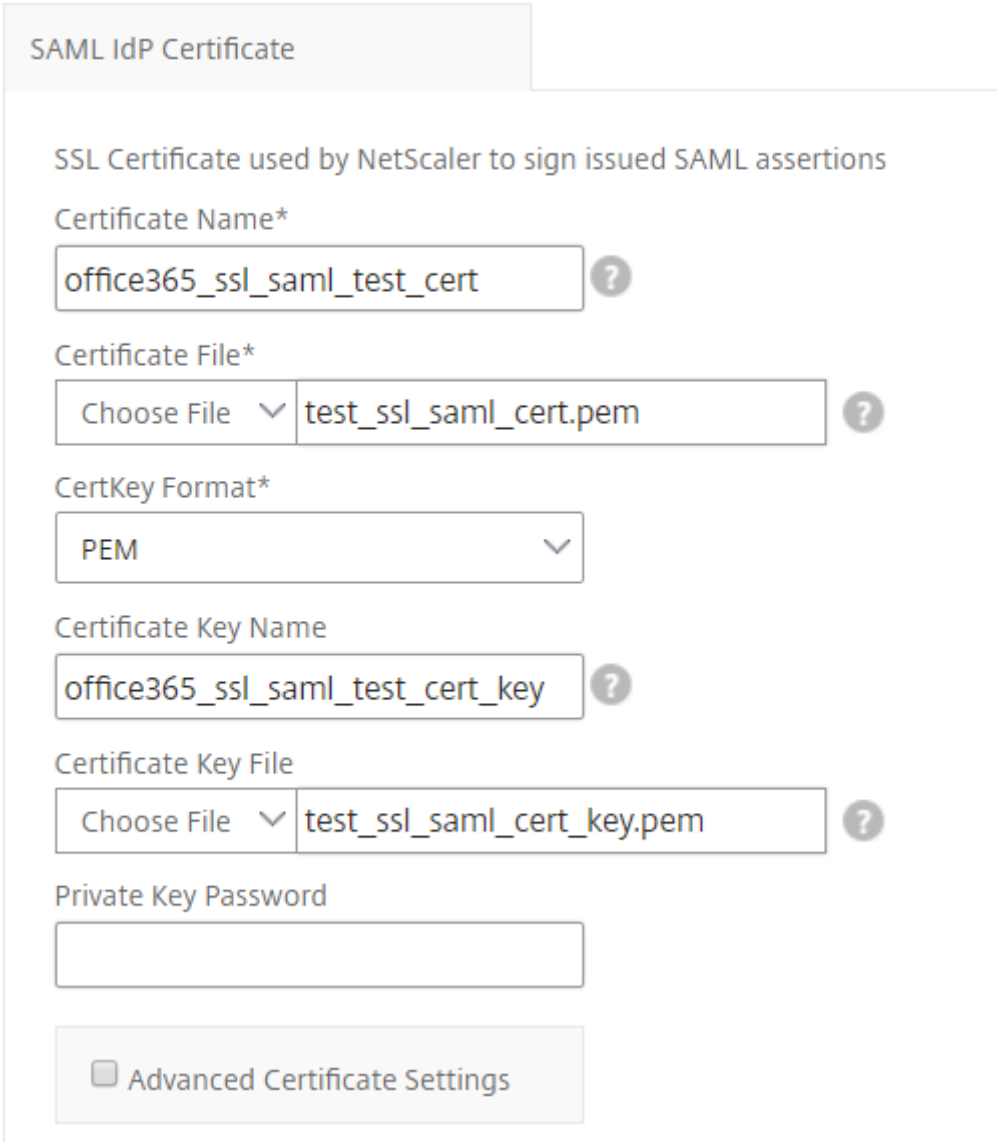


9. 在 **SAML IdP** 证书 部分，可以指定用于 SAML 断言的 SSL 证书的详细信息。

   - 证书名称。输入 SSL 证书的名称。
   - 证书文件。从本地系统上的目录中选择 SSL 证书文件。
   - 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式是.pem 和.der 文件扩展名。
   - 证书密钥名称。输入证书私钥的名称。

- 证书密钥文件。从本地系统中选择包含证书私钥的文件。
- 私钥密码。键入保护您的私钥文件的密码。

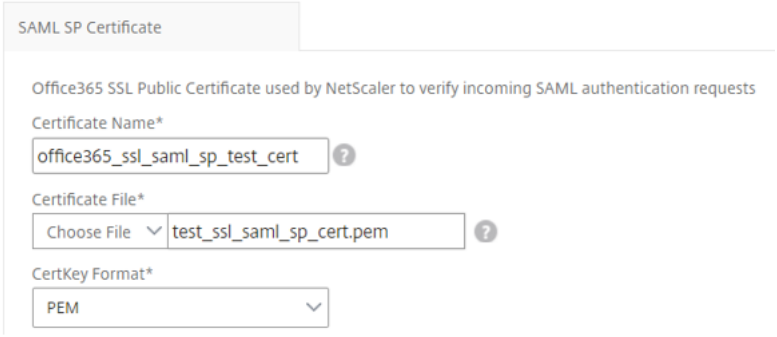
您还可以启用 高级证书设置”复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。



10. 或者，如果上面输入的 **SAML IdP** 证书 要求在 Citrix ADC 上安装 CA 公共证书，则可以选择 SAML IdP CA 证书。确保在上面的“高级证书设置”部分中选择“是 CA 证书”。
11. 在 **SAML SP** 证书 部分中，输入 Office 365 SSL 公共证书的以下详细信息。Citrix ADC 实例使用此证书来验证传入的 SAML 身份验证请求。

    - 证书名称。键入 SSL 证书的名称。
    - 证书文件。从本地系统上的目录中选择 SSL 证书文件。

- 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式是.pem 和.der 文件扩展名。
- 您还可以启用 高级证书设置” 复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。

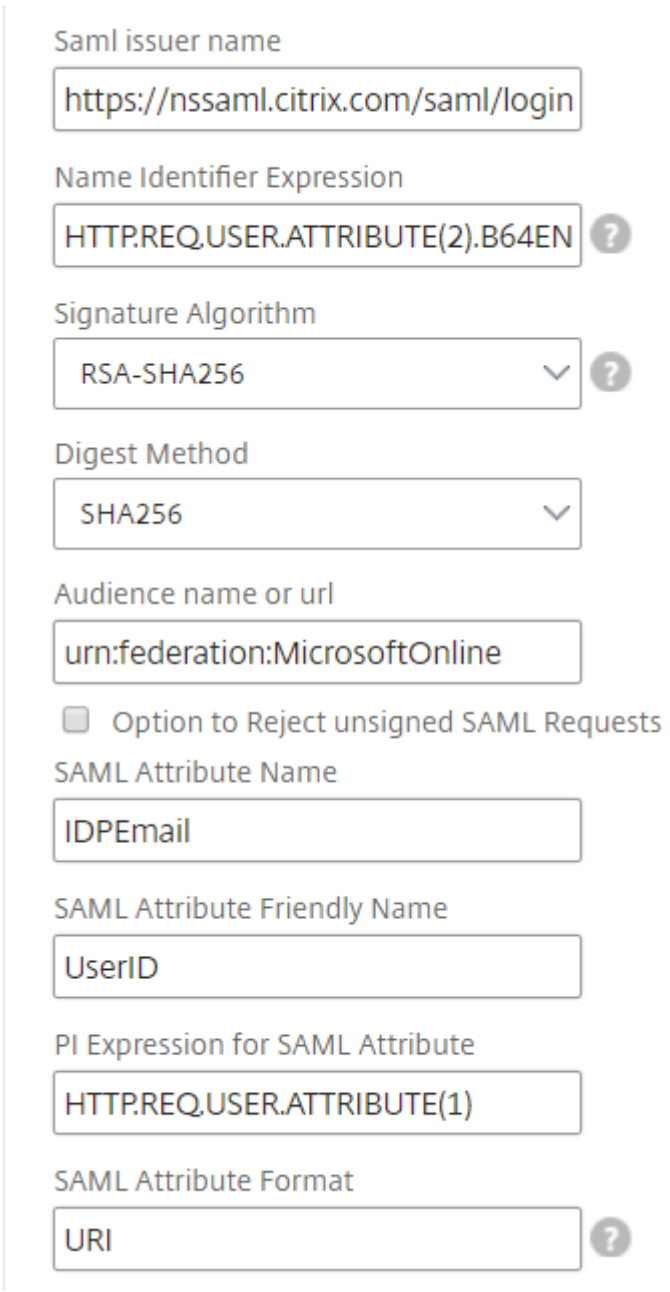


12. **SAML IdP** 设 置部分允许您通过创建由在步骤 3 中创建的 AAA 虚拟服务器使用的 SAML IDP 配置文件和策略将 Citrix ADC 实例配置为 SAML 身份提供商。

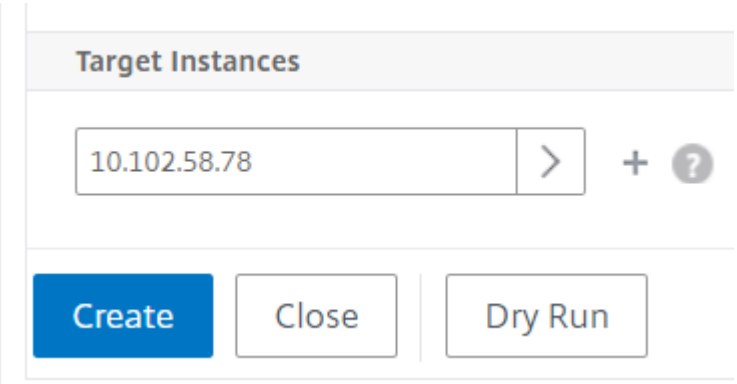
    - **SAML** 发行者名称。在此字段中，键入您的身份验证虚拟服务器的公共 FQDN。示例：`https://<Citrix ADC Auth VIP>/saml/login`
    - 名称标识符表达式。键入 Citrix ADC 表达式，该表达式经过评估以提取 SAML 断言中发送的 SAML NameIdentifier。示例：`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - 签名算法：选择用于验证/签署 SAML 请求/响应的算法（默认为 “RSA-SHA256”）。
    - 摘要方法。选择 SAML 请求/响应的哈希摘要方法（默认为 “SHA256”）。
    - 受众姓名。键入代表服务提供商的实体名称或 URL（Microsoft Office 365）。
    - **SAML** 服务提供商 **(SP) ID**。（可选）Citrix ADC 身份提供商接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。
    - 断言消费者服务 **URL**。输入服务提供商的 URL，成功进行用户身份验证后，Citrix ADC 身份提供商需要在其中发送 SAML 声明。断言消费者服务 URL 可以在身份提供商服务器站点或服务提供商站点启动。
    - 您还可以在此部分中输入其他可选字段。例如，您可以设置以下选项：
        - **SAML** 属性名称。在 SAML 断言中发送的用户属性的名称。
        - **SAML** 属性的友好名称。在 SAML 断言中发送的用户属性的友好名称。
        - **SAML** 属性的 **PI** 表达式。默认情况下，使用以下 Citrix ADC 策略 (PI) 表达式：HTTP.REQ.USER.ATTRIBUTE (1)。此字段将从 LDAP 服务器（邮件）发送的第一个用户属性指定为 SAML 身份验证属性。
        - 选择用户属性的格式。

    这些值包含在发布的 SAML 断言中。

> 提示
>
> Citrix 建议您保留默认设置，因为这些设置已经过测试，可以与 Microsoft Office 365 应用程序配合使用。



13. 单击 目标 实例，然后选择要在其上部署此 Microsoft Office 365 SSO 配置的 Citrix ADC 实例。单击 创 建”以创建配置并在所选 Citrix ADC 实例上部署配置。



> 提示
>
> Citrix 建议在执行实际配置之前，选择干运行以查看样书在目标 Citrix ADC 实例上创建的配置对象。

Microsoft Skype for Business 样本

February 6, 2024

Skype for Business 2015 应用程序的运行需要依赖于多个外部组件。Skype for Business 网络由多个系统组成，例如，服务器及其操作系统、数据库、身份验证和授权系统、网络系统和基础结构以及电话 PBX 系统。Skype for Business Server 2015 有两个版本：标准版和企业版。主要差别是对高可用性功能的支持，只有企业版中提供这些功能。要实现高可用性，必须为池部署多个前端服务器，以及必须镜像 SQL 服务器。

通过企业版部署，可以创建多个具有不同角色的服务器。

主要组件

Skype for Business 2015 应用程序中的主要组件如下：

- 前端服务器
- 边缘服务器
- Director 服务器
- 数据库 (SQL) 服务器

前端服务器

在 Skype for Business 应用程序中，前端服务器是您的网络中的核心服务器。它为用户身份验证、注册、联机状态、通讯簿、A/V 会议、应用程序共享、即时消息和网络会议提供链接和服务。如果您要部署 Skype for Business 2015 企业版，则拓扑通常至少包含两个在具有数据库服务器的前端池中平衡负载的前端服务器，该数据库服务器托管存放 Skype for Business 数据库的 SQL 服务器实例。

边缘服务器

如果未登录到组织内部网络的外部用户需要能够与内部用户交互，则必须为 Skype for Business 部署 Edge 服务器。这些外部用户可能是经过身份验证的匿名远程用户、联盟的合作伙伴或其他移动客户。

Skype For Business 边缘服务器中有四种类型的角色：

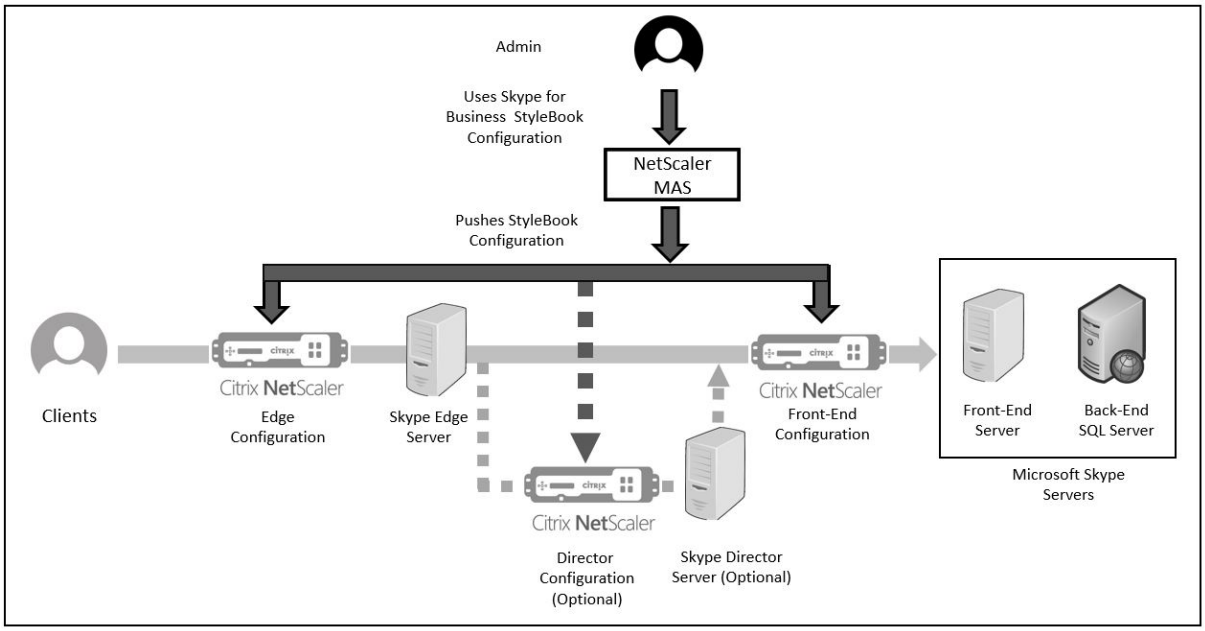
- 接入边缘处理 SIP 流量并验证外部连接，允许远程连接并允许联合连接
- Web Conferencing（网络会议），用于处理数据会议数据包以及允许外部用户访问 Skype for Business
- A/V Conferencing（A/V 会议），用于处理 A/V 会议数据包，以及将音频和视频、应用程序共享和文件传输扩展到外部用户
- XMPP Proxy（XMPP 代理），用于处理 XMPP 数据包，以及允许基于 XMPP 的服务器或客户端连接到 Skype for Business。

Director 服务器

在 Skype for Business 2015 中 Director 服务器的主要功能是对端点进行身份验证，以及将用户“导向”至包含其帐户的池。在 Skype for Business 2015 中，尽管 Director 是独立服务器上完全专用的特定角色，但它是可选服务器。这样，可以更加轻松地部署或删除配置，从而方便实现安全性。

在存在多个池的情况下，控制器最有用，因为它们为验证端点提供了单一联系点。此外，对于远程用户，Director 用作边缘池与前端池之间的附加跃点，从而添加了额外的一层保护来抵御攻击。

下图以图解方式表示了 Skype 服务器在网络中的部署：



在企业中配置 **Citrix ADC** 实例

下表列出了下面的说明中包含的示例配置中使用的 IP 地址：

Skype for Business 服务器	虚拟 IP 地址	服务器 IP 地址	Citrix ADC 实例
边缘服务器	外部 VIP - 192.20.20.20	192.20.20.21；192.20.20.22	10.102.29.141
	内部 VIP - 10.10.10.20	10.10.10.21；10.10.10.22	
前端服务器	10.10.10.10	10.10.10.11；10.10.10.12	10.102.29.60
Director 服务器	10.10.10.30	10.10.10.31；10.10.10.32	10.102.29.93

配置前端服务器

1. 在 Citrix Application Delivery Management (ADM) 中，导航到应用程序 > 配置，然后单击新建。“选择样书”页面显示所有可供您在 Citrix ADM 中使用的样书。向下滚动并选择 **Microsoft Skype for Business 2015** 样书。样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。
2. 在 边缘服务器 部分，输入网络中所有边缘服务器的以下虚拟 IP (VIP) 地址和 IP 地址。
   a) 将用于访问边缘、网络会议边缘和 A/V 边缘的边缘服务器的外部 VIP 地址和 IP 地址。
   b) 将要连接到内部网络的 Edge 服务器的内部 VIP 地址和 IP 地址。
   c) 您的网络中的两个外部和两个内部边缘服务器。
3. 在前端服务器部分中，输入要为 Skype for Business 前端服务器创建的虚拟前端服务器 (VIP) 的 IP 地址。另外，输入网络中所有 Skype for Business 前端服务器的 IP 地址。
4. 在 **Director** 服务器部分中，输入要为 Skype for Business 应用程序创建的 Director 服务器的虚拟 IP 地址 (VIP)。此外，还输入网络中所有 Skype for Business Director 服务器的 IP 地址。至少创建两个 Director 服务器以实现高可用性。
5. 高级设置 部分列出了在 Citrix ADC 实例上为三台 Skype 服务器配置的所有默认端口。

下表为您提供了所有默认端口和协议的列表：

标签	端口	协议	说明
HTTP 端口	80	HTTP	用于在未使用 HTTPS 时从前端服务器到 Web 场 FQDN 的通信。

标签	端口	协议	说明
HTTPS 端口	443	HTTPS	用于从前端服务器到 Web 场 FQDN 的通信。
自动发现内部端口	4443	HTTPS	用于自动发现登录的 HTTPS（从反向代理）和 HTTPS 前端池间通信。
RPC 端口	135	DCOM 和远程过程调用 (RPC)	用于基于 DCOM 的操作，例如移动用户、用户复制器同步以及通讯簿同步。
SIP 端口	5061	TCP (TLS)	由前端服务器用于所有内部 SIP 通信。
SIP Focus 端口	444	HTTPS、TCP	用于 Focus（管理 Skype 会议状态的组件）与单个服务器之间的 HTTPS 通信。
SIP 组端口	5071	TCP	用于响应组应用程序的传入 SIP 请求。
SIP 应用程序共享端口	5065	TCP	用于传入 SIP 侦听请求以进行应用程序共享。
SIP 参与人员端口	5072	TCP	用于参与人员的传入 SIP 请求（即用于调用拨入式会议）。
SIP 会议公告端口	5073	TCP	用于 Skype for Business 服务器会议公告服务的传入 SIP 请求（即用于调用拨入式会议）。
SIP CallPark 端口	5075	TCP	用于 CallPark 应用程序的传入 SIP 请求。
SIP 调用允许端口	448	TCP	用于 Skype for Business 服务器带宽策略服务实施的调用允许控制。
SIP 调用允许 TURN 端口	5080	TCP	用于带宽策略服务针对音频/视频边缘 TURN 流量实施的调用允许控制。
SIP 音频测试端口	5076	TCP	用于音频测试服务的传入 SIP 请求。

标签	端口	协议	说明
HTTPS 外部端口	443	HTTPS	用于以下情况的外部端口：远程用户访问的 SIP/TLS 通信、访问内部网络会议，以及访问内部媒体和 A/V 会话的 STUN/TCP 入站和出站媒体通信。
HTTPS 内部端口	443	HTTPS	用于以下情况的内部端口：远程用户访问的 SIP/TLS 通信、访问内部网络会议，以及访问内部媒体和 A/V 会话的 STUN/TCP 入站和出站媒体通信。
SIP 外部远程访问端口	5061	TCP	用于远程用户访问或联合的 SIP/MTLS 通信的外部端口。
SIP 内部远程访问端口	5061	TCP	用于远程用户访问或联合的 SIP/MTLS 通信的内部端口。
SIP 外部 STUN UDP 端口	3478	UDP	用于 STUN/UDP 入站和出站媒体通信的外部端口。
SIP 内部 STUN UDP 端口	3478	UDP	用于 STUN/UDP 入站和出站媒体通信的内部端口。
SIP 内部 IM 端口	5062		用于通过内部防火墙传输的出站 IM 通信的 SIP/MTLS 身份验证的内部端口。
HTTP 端口	80	TCP	用于从 Director 到 Web 场 FQDN 的初始通信。
HTTPS 端口	443	HTTPS	用于从 Director 到 Web 场 FQDN 的通信。
自动发现内部端口	4443	HTTPS	用于自动发现登录的 HTTPS（从反向代理）和 HTTPS Director 池间通信。
SIP 内部端口	5061	TCP	用于服务器与客户端连接之间的内部通信。

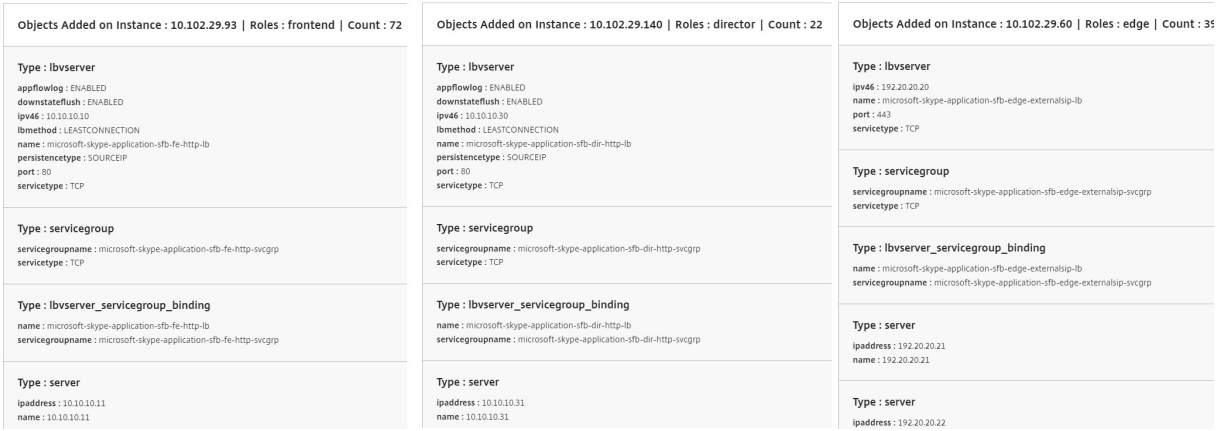
6. 在“目标实例”部分，选择三个不同的 Citrix ADC 实例，用于部署三台 Skype for Business 服务器。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

7. 单击创建 可在选定的 Citrix ADC 实例上创建配置。

> 提示
>
> Citrix 建议您选择干运行以检查必须在目标实例上创建的配置对象，然后再对实例执行实际配置。
>
> 成功创建配置后，样书将创建 25 个负载平衡虚拟服务器。即，对于每个端口，均定义一个负载平衡虚拟服务器以及一个服务组，且服务组绑定到负载平衡虚拟服务器。此外，该配置还将前端服务器添加为服务组成员，并将其绑定到服务组。创建的服务组成员数等于创建的前端服务器数。

下图显示了每个服务器中创建的对象：



配置 **Microsoft Exchange** 样书

February 6, 2024

您可以使用 Microsoft Exchange 2016 样书部署 Citrix ADC 配置，以优化和保护网络中的 Microsoft Exchange 2016 企业应用程序。Microsoft Exchange 2016 是关键的企业应用程序，用于为您的员工和其他利益干系人提供电子邮件、个人信息管理和消息传送服务。

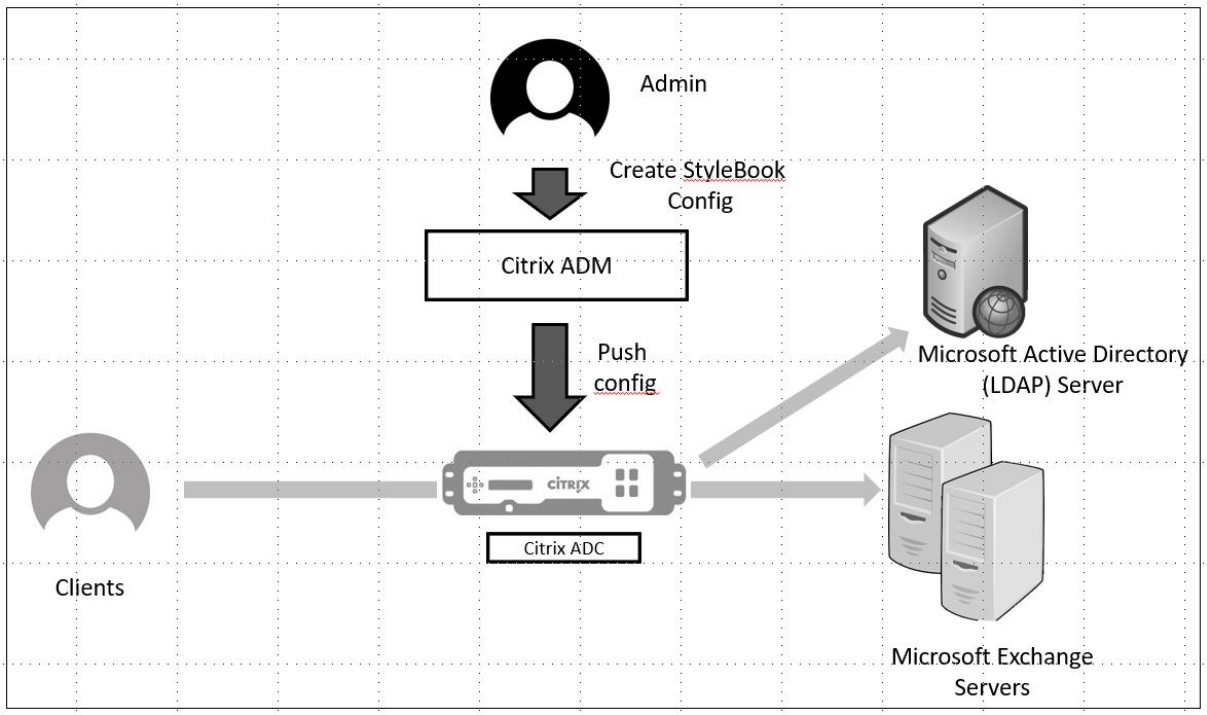
使用 **Microsoft Exchange** 样书配置的 **Citrix ADC** 功能

Microsoft Exchange 2016 样书为 Microsoft Exchange 2016 服务器启用和配置了以下 Citrix ADC 功能：

- 负载平衡 - 实现对多个 Exchange 服务器进行负载平衡的基本负载平衡功能
- 内容切换 - 实现对正确的负载平衡虚拟服务器进行单个 IP 访问，以及将查询重定向到正确的负载平衡虚拟服务器
- 重写 - 将用户重定向到安全页面

- SSL 卸载-将 SSL 处理卸载到 Citrix ADC，从而减少了 Exchange 服务器的负载

下图以图解方式表示了 Exchange 服务器在网络中的部署：



必备条件

- 对于基于证书的身份验证，属于网络设置一部分的所有可寻址主机均必须有可解析的域名，而不只是 IP 地址。
- 请确保可以在 Microsoft Exchange 2016 服务器中访问 SIP 端口。

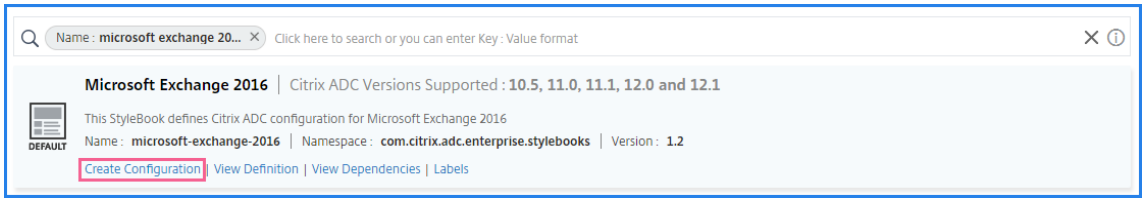
配置 **Microsoft Exchange** 样书

在商业企业中配置 Microsoft Exchange 样书以部署 Citrix ADC 配置。

配置 **Microsoft Exchange** 应用程序

1. 在 Citrix ADM 中，导航到应用程序 > 样书。
2. 搜索 **Microsoft Exchange 2016** 样书，然后单击“创建配置”。

   样书以用户界面表单形式显示，您可以在此为此样书中定义的所有参数输入值。



3. 输入以下参数的详细信息：

   - 交换应用程序名 称-网络中的 Microsoft Exchange 应用程序的名称
   - **Exchange VIP** - Citrix ADC 上的虚拟 IP 地址，用于接收客户对 Microsoft Exchange 应用程序的请求
   - **Exchange Server IP** -网络中所有 Exchange 服务器的 IP 地址。

     如果要添加更多 IP 地址，请单击加号 (**+**) 图标。通常，网络中配置两个 Exchange 服务器。

4. 在“交换证书”部分中，将交换证书上载到 Citrix ADM。输入证书和密钥文件的名称，然后从本地存储上载。您还可以提供私钥密码来加密密钥文件。

   > 注意
   >
   > 确保证书文件采用“.pem”或“.der”格式。Citrix ADM 拒绝其他格式的文件。

   如果要指定证书到期详细信息或任何高级设置，请选择 高级证书设置。

5. 在 **Exchange Active Directory** 身份验证配置 部分中，通过输入数据来配置 AD 设置。

   - **Active Directory** 身份验证 **VIP** - 用于在 Citrix ADC 设备上创建和配置 AD (LDAP) 虚拟服务器的虚拟 IP 地址。
   - **Active Directory** 服务器 **IP**-您的 Active Directory 域控制器的 IP 地址。
   - **Active Directory** 基本字符串-Active Directory 中的 LDAP 基本字符串。例如，CN=Users,DC=CTXNSSFB,DC=CO
   - **Active Directory LDAP** 绑定专有名称 **(DN)** -LDAP 绑定专有名称 (DN) 用于将此对象绑定到 LDAP 服务器 (AD)。例如 cn=Administrator,cn=Users,dc=acme,dc=com
   - **Active Directory LDAP** 绑定专有名称 **(DN)** 密码——LDAP 绑定专有名称 (DN) 是 AD 身份验证的密码
   - **Active Directory** 用户名属性 -用户名的 AD 属性。Citrix ADC 使用 LDAP 属性来查询外部 Active Directory 服务器。例如 sAMAccountName
   - **Active Directory** 组属性名称-在 LDAP 服务器上配置的 LDAP 组属性名称。例如，LDAP 中组属性的“memberOf”。
   - **Active Directory** 子属性名称 -LDAP 服务器上配置的 LDAP 子属性名称。例如，“cn”表示 LDAP 中的子属性。
   - **Active Directory** 身份验证域 -用于身份验证的 AD/LDAP 域名。例如 ctxnssfb.com。

6. 在“目标实例”部分，选择要在其上部署此 Exchange 配置的 Citrix ADC 实例。

> 注意
>
> 如果要查看最近发现的 Citrix ADC 实例，请单击刷新图标。

7. 单击“创建”创建配置文件并在选定的 Citrix ADC 实例上执行配置。

   Citrix 建议您先选择干运行检查在目标实例上创建的配置对象，然后再在实例上执行实际配置。

成功创建配置后，样书创建了一个内容切换虚拟服务器、五个负载平衡虚拟服务器和一个绑定到一个 LDAP 身份验证虚拟服务器的 LDAP 策略。此外，相应的服务组创建并绑定到负载平衡虚拟服务器。

Microsoft SharePoint 样书

February 6, 2024

Microsoft SharePoint 2016 是关键的企业应用程序，主要提供文档管理和存储系统，它是高度可配置的，且所有重要浏览器都支持它。

您可以使用 Microsoft SharePoint 2016 样书部署 Citrix ADC 配置，以优化和保护网络中的 Microsoft SharePoint 2016 企业应用程序。

必备条件

- Microsoft SharePoint 2016
- Citrix ADM，版本 12.0 及更高版本
- Citrix ADC 版本 10.5 及更高版本

Microsoft SharePoint 2016 样书配置的 Citrix ADC 功能

您可以使用 Microsoft SharePoint 2016 样书为 Microsoft SharePoint 2016 启用和配置以下 Citrix ADC 功能：

- 负载平衡
- 内容交换
- 响应方
- 重写
- 压缩
- 集成缓存

负载平衡

Citrix ADC 负载平衡将请求平均分配到后端 SharePoint 服务器。对后端服务器进行智能监视可以防止请求发送到出现故障的服务器。

SharePoint 样书配置 12 个负载平衡虚拟服务器，每个服务器专门用于按照特定类型的内容（例如，文档、图片、音频、视频及其他文件类型）对请求进行负载平衡。

SharePoint 样书现在通过配置基于 SSL 的 LB 虚拟服务器来支持 SharePoint 应用程序的 SSL 模式。确保选择 SSL 作为前端协议。请注意，虚拟端口默认设置为 443。您也可以选择 SSL 将服务组（SharePoint 应用程序服务器）绑定到目标负载平衡虚拟服务器。请注意，默认情况下，后端协议设置为 HTTP。

内容切换

内容切换功能用于根据特定类型的 SharePoint 请求内容（例如，文档、图片及音频或视频文件）在多个负载平衡虚拟服务器之间分配客户端请求。内容切换模块将传入流量导向到可以处理相应类型的内容的最优匹配负载平衡虚拟服务器。因此，您可以对不同类型的流量应用不同的优化策略。例如，您可能想对视频使用与文本文档不同的压缩或缓存策略。

响应方

Citrix ADC 实例的响应器功能可用于将用户从 HTTP 无缝重定向到 HTTPS。还可以配置响应方来提供自定义的错误页面。Responder 策略确定必须对哪些请求（流量）采取操作，并将每个策略绑定到负载平衡虚拟服务器。SharePoint 样书包含用于将用户从 HTTP 重定向至 HTTPS URL 的配置。

重写

重写模块用于即时修改请求/响应头、URL 或内容。此模块以内联方式进行流量处理，因此可以根据需要针对特定用例更改通信流。例如，重写可以提供对请求内容的访问，而不会公开有关 Web 站点服务器的不必要的详细信息。

在 SharePoint 样本中，重写功能用于从用户请求中删除不必要的标头。

压缩

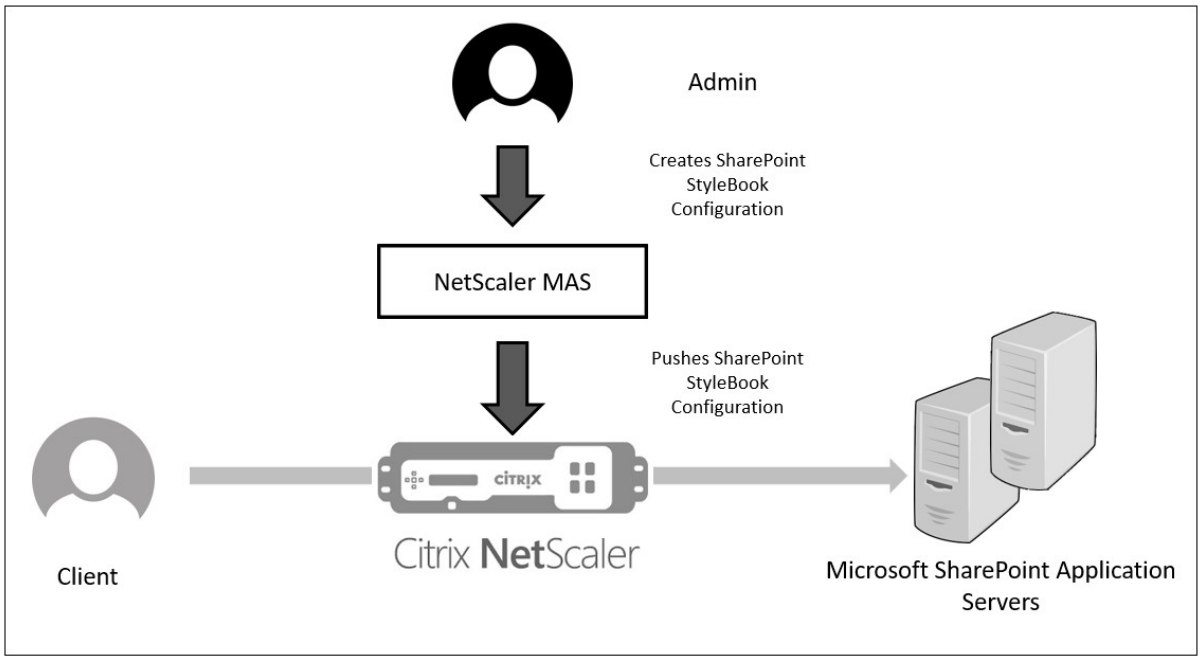
Citrix ADC 压缩引擎识别并压缩可压缩的内容。此过程可减少数据传输时间、降低客户端的网络带宽要求，同时缩短 SharePoint 内容服务器上的 CPU 周期。Citrix ADC 实例可以压缩静态和动态生成的数据。它应用 GZIP 或 DEFLATE 压缩算法从服务器响应中删除无关和重复的信息，并以更加简洁和有效的格式表示原始信息。客户端浏览器解压缩数据的能力取决于它支持的算法：GZIP 或/和 DEFLATE。

Citrix ADC 实例配置为压缩 HTML、XML、纯文本、层叠样式表 (CSS) 和 Microsoft Office 文档中的文本，但不压缩 GIF 或 JPG 格式的图像。压缩流量的主要优势包括降低带宽成本、减少 WAN 延迟以及提高服务器性能。

集成缓存

Citrix ADC 内存缓存可以存储 SharePoint 对象，以便快速向用户提供经常请求的内容。缓存的内容包括下载的文档和音频、视频及图片文件。

下图以图形方式显示了 SharePoint 服务器在由 Citrix ADC 实例前端的网络中的部署，该实例使用 Citrix ADM 部署 SharePoint 样书配置。



部署 **SharePoint** 样书配置

以下任务将帮助您在您的企业网络中部署 Microsoft SharePoint 2016 样书。

部署 **Microsoft SharePoint 2016** 样书：

1. 在 Citrix ADM 中，导航到“应用程序”>“管理”>“配置”，然后单击“新建”。

   “选择样书”页面显示所有可供您在 Citrix ADM 中使用的样书。

2. 向下滚动并选择 **Microsoft SharePoint 2016** 样书。

   > 注意
   >
   > 在 Citrix ADM 中，导航到 应用程序 > 配置 > 样书。向下滚动以找到 **Microsoft SharePoint 2016** 样书，然后单击创建配置。

   样书以用户界面表单打开，您可以在其中输入此样书中定义的所有参数的值。

   输入以下参数的值：

   a) **SharePoint** 应用程序名称。要在您的网络中部署的 SharePoint 配置的名称。

b) **SharePoint** 虚拟 **IP**。Citrix ADC 实例接收客户端对 Microsoft SharePoint 应用程序的请求的虚拟 IP 地址。

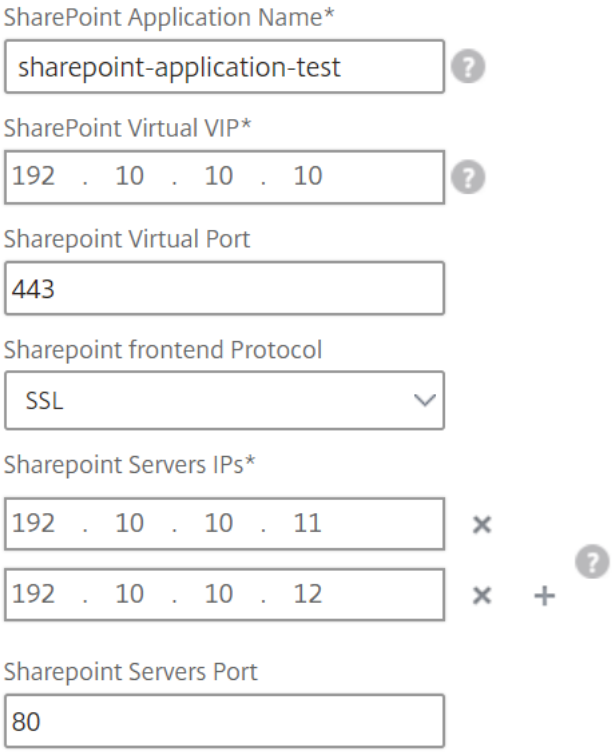
c) **SharePoint** 虚拟端口。用户在访问 SharePoint 应用程序时使用的 TCP 端口

d) **SharePoint** 前端协议。从下拉列表中选择 SharePoint 前端协议。可用的选项包括 HTTP 或 SSL。

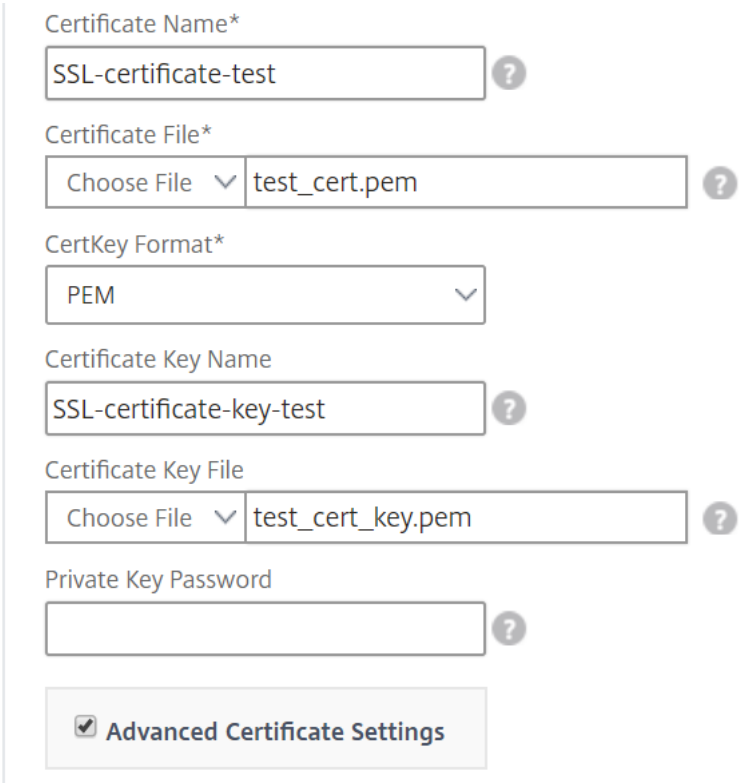
> 注意
>
> 如果选择 SSL，请确保在本样书的 SharePoint 高级设置部分中启用重写配置参数。

e) **SharePoint** 服务器 **IP** 地址。网络中所有 SharePoint 服务器的 IP 地址。

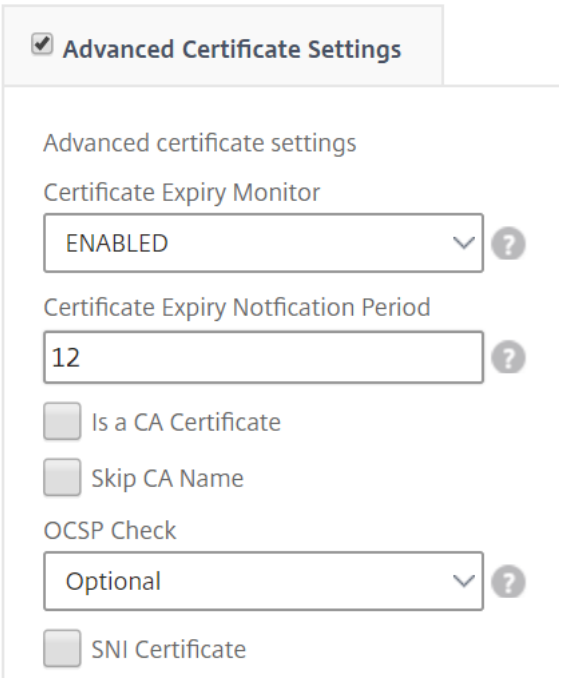
f) **SharePoint** 服务器端口。SharePoint 服务器使用的 TCP 端口号。默认情况下，此端口号为 80。您可以根据需要编辑此值，但请确保可以在 Microsoft SharePoint 2016 服务器上访问此端口。



3. 在 **SSL** 证书设置 部分中，单击“+”以输入 SSL 证书的名称、证书密钥，然后从本地存储文件夹中选择相应的文件。



4. （可选）单击 高级证书设置 以启用或禁用 SSL 证书到期监视。如果您启用证书到期监视，请设置天数，以便 Citrix ADM 在证书即将过期的这段天后发出警报。您还可以选择将 OCSP 检查设置为可选功能或强制功能。

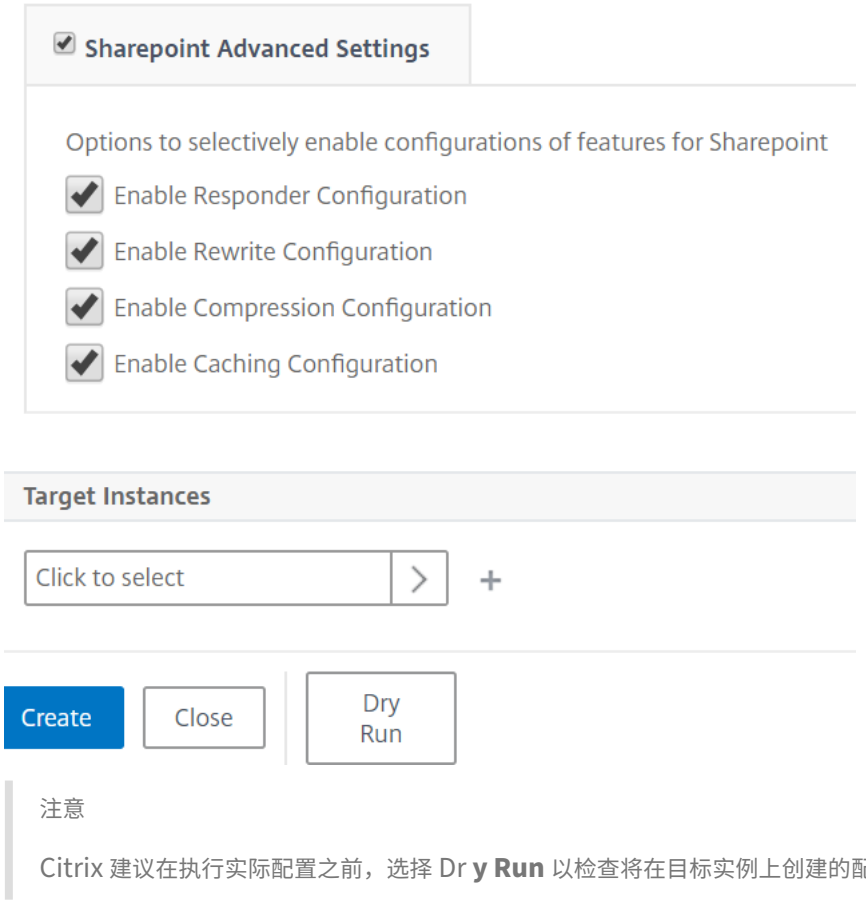


5. 通过 SharePoint 高级设置 部分，您可以启用将在 Citrix ADC 实例上配置的 Citrix ADC 功能。虽然默认情况下在实例上配置负载平衡和内容切换功能，但您可以选择要在实例上配置的其他功能，即，响应方配置、重写配

置、压缩配置以及集成缓存配置。

6. 单击“目标实例”，然后选择要在其上部署此 SharePoint 配置的 Citrix ADC 实例。单击“创建”创建配置并在选定的 Citrix ADC 实例上部署配置。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。



> 注意
>
> Citrix 建议在执行实际配置之前，选择 Dr **y Run** 以检查将在目标实例上创建的配置对象。

创建并成功部署配置后，SharePoint 样书将创建一个内容切换虚拟服务器和 12 个负载平衡虚拟服务器。它还将创建策略和服务组，并将其绑定到负载平衡虚拟服务器。创建哪些策略取决于在创建配置包的过程中在样书中选择的功能。

查看在 **Citrix ADC** 实例上定义的对象

在 Citrix ADM 上创建配置包后，您可以查看在 Citrix ADC 实例上为 SharePoint 样书创建的所有对象。导航到“应用程序”>“管理”>“配置”，然后单击“查看创建的对象”。下图显示了一些已创建的对象，其中示例中指定的 IP 地址如“从 Citrix ADM 部署 SharePoint 样书配置”。

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

Microsoft ADFS 代理样书

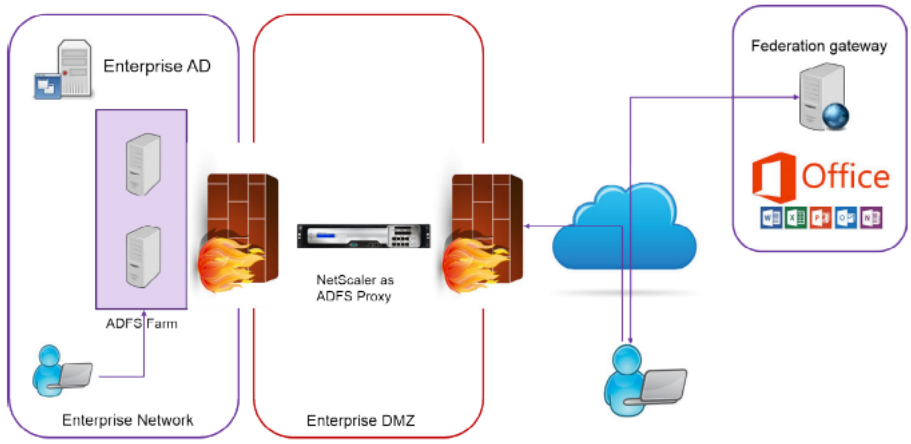
February 6, 2024

Microsoft™ ADFS 代理通过为支持内部联合的资源和云资源提供单点登录访问权限来发挥重要作用。云资源的一个例子是 Office 365。ADFS 代理服务器的目的是接收请求并转发到无法从互联网访问的 ADFS 服务器。ADFS 代理是一种反向代理，通常位于组织的外围网络 (DMZ) 中。ADFS 代理在远程用户连接和应用程序访问方面起着关键作用。

Citrix ADC 拥有精确的技术，可以实现安全连接、身份验证和联合身份处理。使用 Citrix ADC 作为 ADFS 代理无需在 DMZ 中部署额外的组件。

Citrix Application Delivery Management (ADM) 中的 Microsoft ADFS 代理样本允许您在 Citrix ADC 实例上配置 ADFS 代理服务器。

下图显示了在企业 DMZ 中部署 Citrix ADC 实例作为 ADFS 代理服务器的情况。



使用 Citrix ADC 作为 ADFS 代理的好处

1. 同时满足负载平衡和 ADFS 代理的需求
2. 支持内部和外部用户访问方案
3. 支持丰富的预身份验证方法
4. 为用户提供单点登录体验
5. 支持主动和被动协议
    a) 活动协议应用程序的示例有：Microsoft Outlook、Microsoft Skype for Business
    b) 被动协议应用程序的示例有—Microsoft Outlook Web 应用程序、网络浏览器
6. 用于基于 DMZ 的部署的强化设备
7. 通过使用其他核心 Citrix ADC 功能增加价值
    a) 内容交换

b) SSL 卸载
c) 重写
d) 安全性（Citrix ADC AAA）

对于基于协议的活跃方案，您可以连接到 Office 365 并提供您的证书。Microsoft Federation Gateway 将代表活动协议客户端联系 ADFS 服务（通过 ADFS 代理）。然后，网关使用基本身份验证 (401) 提交证书。Citrix ADC 在访问 ADFS 服务之前处理客户端身份验证。身份验证后，ADFS 服务向联邦网关提供 SAML 令牌。反过来，联邦网关将令牌提交给 Office 365 以提供客户端访问权限。

对于被动客户端，ADFS 代理样书创建 Kerberos 约束委托 (KCD) 用户帐户。KCD 帐户是连接 ADFS 服务器的 Kerberos SSO 身份验证所必需的。样书还生成 LDAP 策略和会话策略。这些策略稍后绑定到处理被动客户端身份验证的 Citrix ADC AAA 虚拟服务器。

样书还可以确保 Citrix ADC 上的 DNS 服务器配置为 ADFS。

以下配置部分介绍如何设置 Citrix ADC 以处理基于主动和被动协议的客户端身份验证。

配置详细信息

下表列出了成功部署此集成所需的最低软件版本。

产品	所需的最低版本
Citrix ADC	11.0，Enterprise/Platinum 许可证

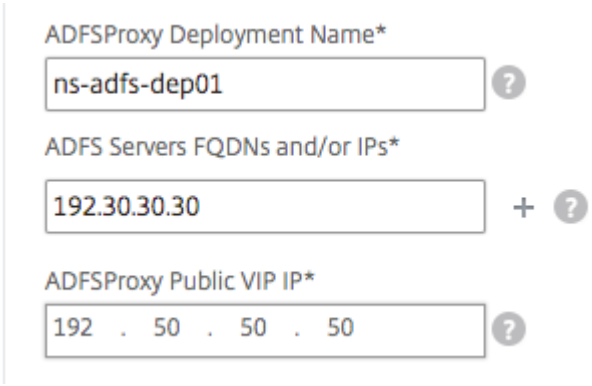
以下说明假定您已经创建了相应的外部和内部 DNS 条目。

部署 **Citrix ADM** 的 **MicrosoftFS** 代理样书配置

以下说明可帮助您在企业网络中实现 Microsoft ADFS 代理样书。

部署 **Microsoft ADFS** 代理样书

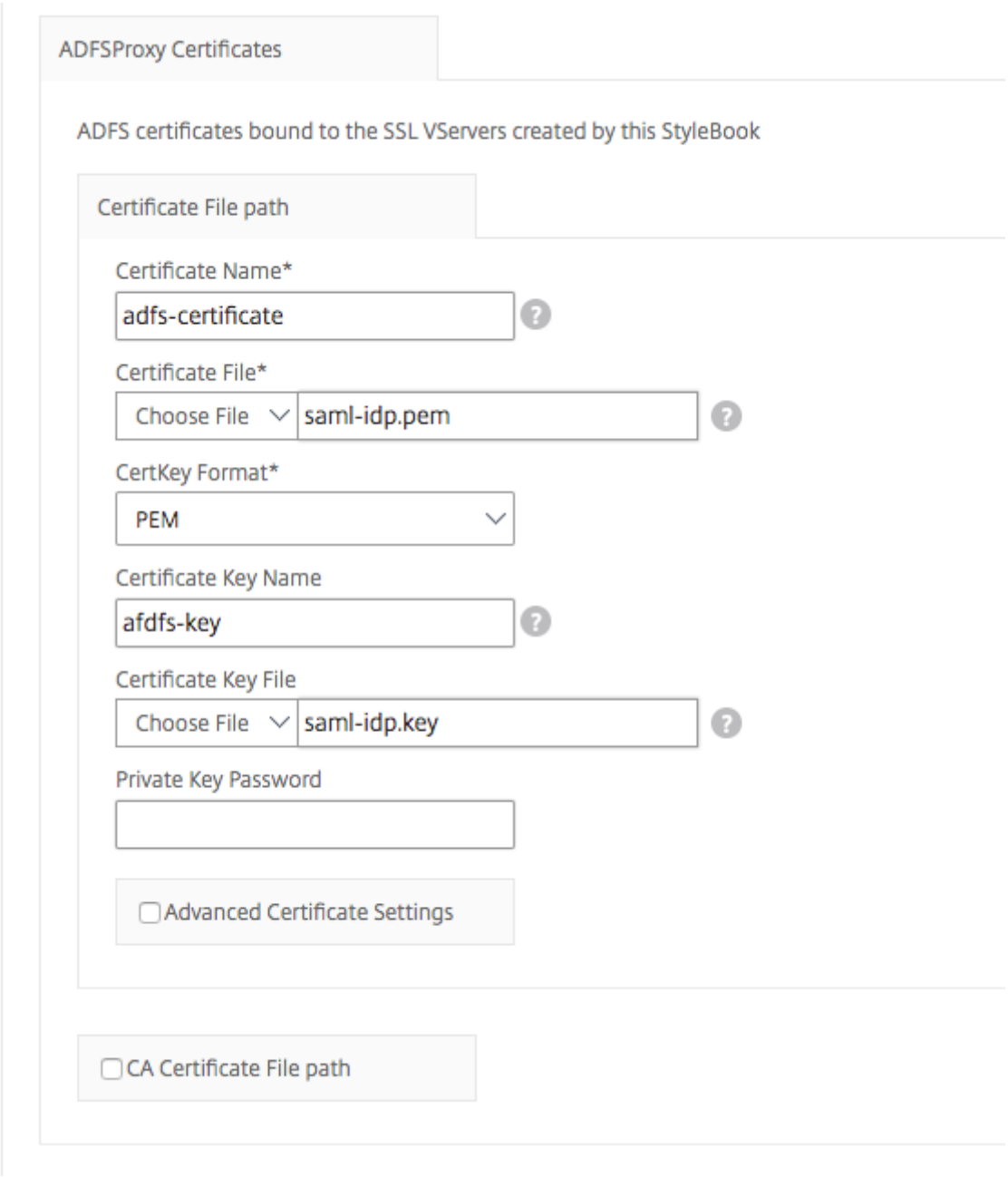
1. 在 Citrix ADM 中，导航到应用程序 > 样书。样书页面显示了所有可供您在 Citrix ADM 中使用的样书。
2. 向下滚动并找到 **Microsoft ADFS** 代理样书。单击 创建配置。
   样书以用户界面页的形式打开，可以在该页面上键入此样书中定义的所有参数的值。
3. 键入以下参数的值：
   a) **ADFS** 代理部署名称。为在您的网络中部署的 ADFS 代理配置选择一个名称。
   b) **ADFS** 服务器 **FQDN** 或 **IP**。键入网络中所有 ADFS 服务器的 IP 地址或 FQDN（域名）。
   c) **ADFS** 代理公共 **VIP IP**。键入作为 ADFS 代理服务器执行的 Citrix ADC 上的公用虚拟 IP 地址。



4. 在 **ADFS** 代理证 书”部分中，键入 SSL 证书和证书密钥的详细信息。

   此 SSL 证书绑定到在 Citrix ADC 实例上创建的所有虚拟服务器。

   从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以加载.pem 格式的加密私钥。



您还可以启用 高级证书设置”复选框。您可以在此处键入诸如证书到期通知期限之类的详细信息，启用或禁用证书到期监视器。

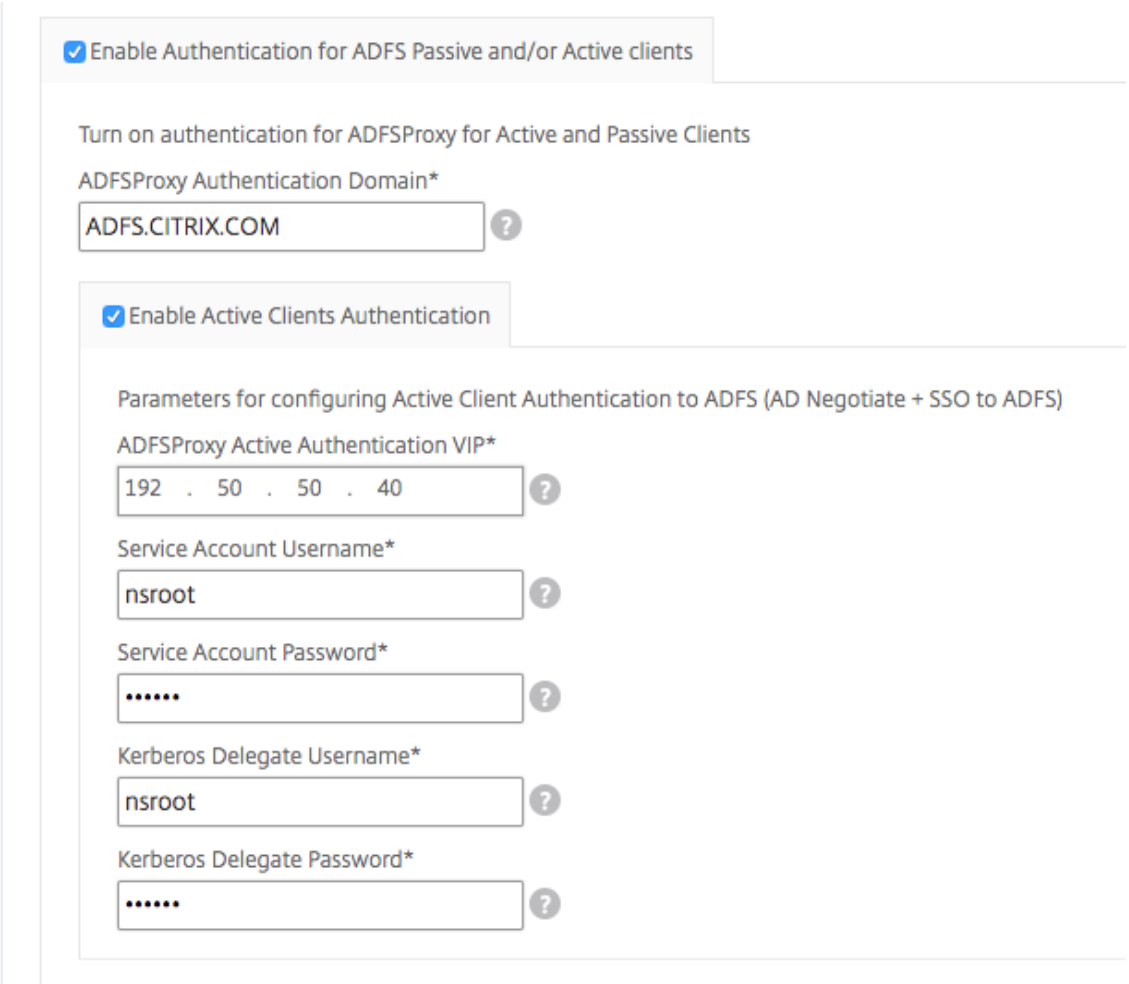
5. （可选）如果 **SSL** 证书 要求在 Citrix ADC 上安装 CA 公共证书，则可以选中 SSL CA 证书复选框。确保在“高级证书设置”部分中选择“是 CA 证书”。
6. 为主动客户端和被动客户端启用身份验证。键入 Active Directory 中用于用户身份验证的 DNS 域名。然后，您可以为主动或被动客户端配置身份验证，或者同时为两者配置身份验证。
7. 键入以下详细信息以启用活动客户端的身份验证：

> 注意
>
> 配置对活动客户端的支持是可选的。

a) **ADFS** 代理主动身份验证 **VIP**。在 Citrix ADC 实例上键入虚拟身份验证服务器的虚拟 IP 地址，活动客户端将被重定向到进行身份验证。

b) 服务帐户用户名。键入 Citrix ADC 用于在活动目录中对用户进行身份验证的服务帐户用户名。

c) 服务帐户密码。键入 Citrix ADC 用于在 Active Directory 中对用户进行身份验证的密码。



8. 通过启用相应的选项并配置 LDAP 设置，为被动客户端配置身份验证。

> 注意
>
> 配置对被动客户端的支持是可选的。

键入以下详细信息以启用被动客户端的身份验证：

a) **LDAP**（**Active Directory**）基地。键入用户帐户驻留在 Active Directory (AD) 中的域的基本域名以允许身份验证。例如，dc=netscaler，dc=com

b) **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，cn=Manager、dc=netscaler、dc=com

c) **LDAP**（**Active Directory**）绑定 **DN** 密码。键入用于身份验证的域帐户的密码。

您必须在本部分的值中键入的其他几个字段如下所示：

d) **LDAP** 服务器（**Active Directory**）**IP**。键入活动目录服务器的 IP 地址，以便 AD 身份验证正常运行。

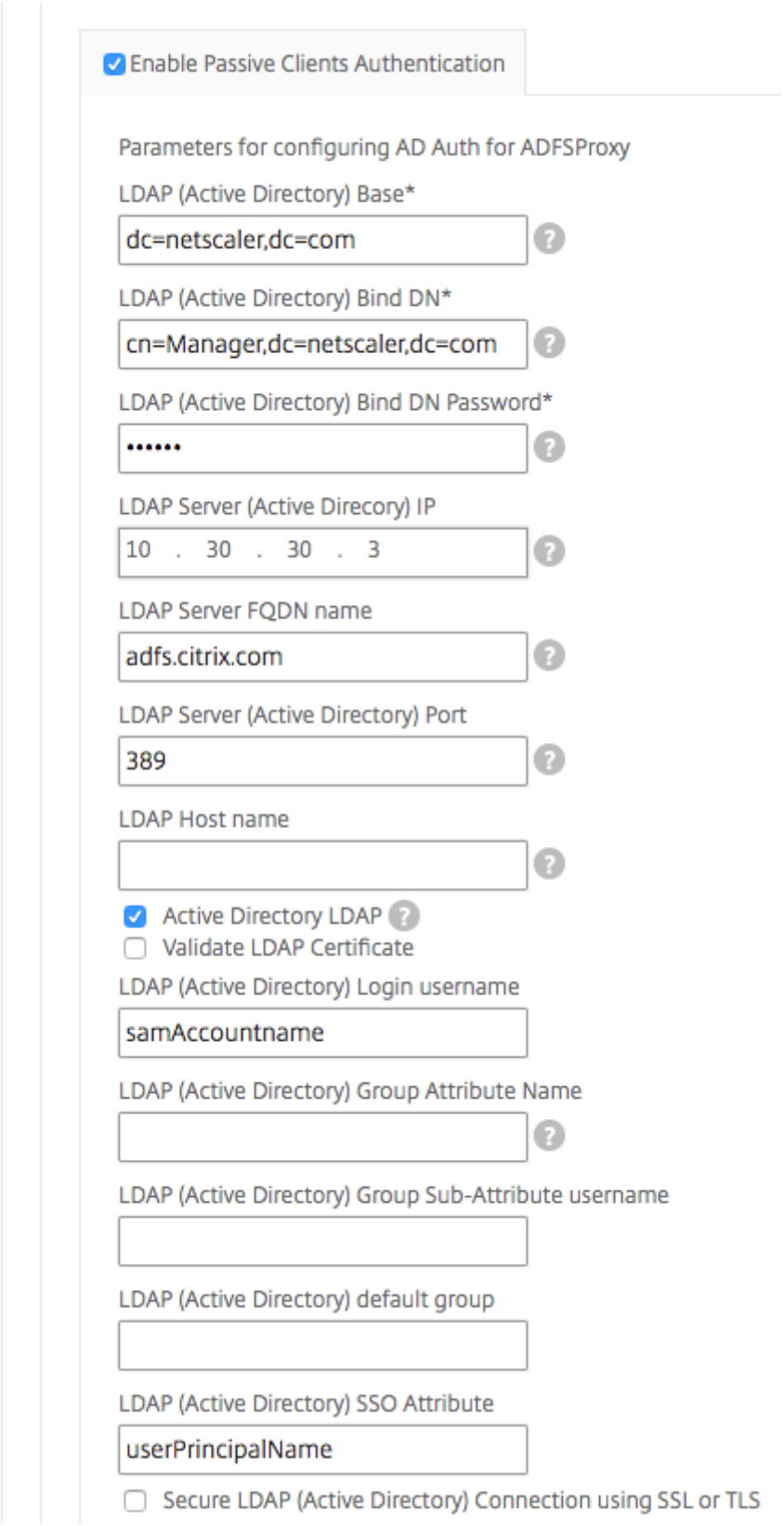
e) **LDAP** 服务器 **FQDN** 名称。键入活动目录服务器的 FQDN 名称。FQDN 名称是可选的。按照步骤 1 提供 IP 地址或 FQDN 名称。

f) **LDAP** 服务器 **Active Directory** 端口。默认情况下，LDAP 协议的 TCP 和 UDP 端口为 389，而安全 LDAP 的 TCP 端口为 636。

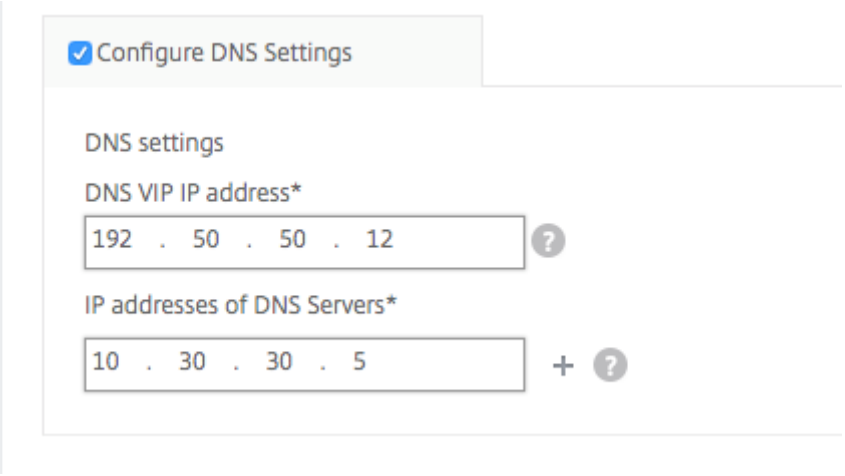
g) **LDAP**（**Active Directory**）登录用户名。将用户名键入“sAMAccountName”。

h) **ADFS** 代理被动身份验证 **VIP**. 键入被动客户端的 ADFS 代理虚拟服务器的 IP 地址。

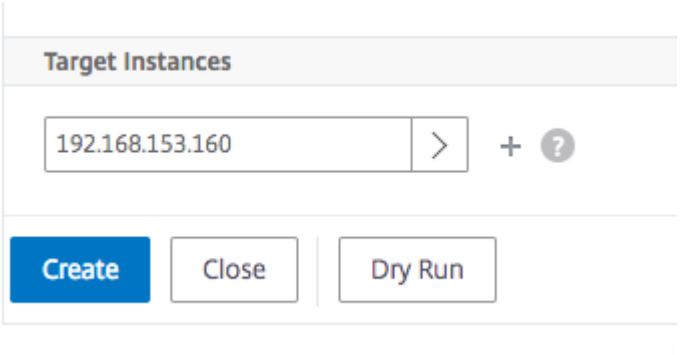
> 注意
>
> 标有“*”的字段是必填字段。



9. 您也可以为 DNS 服务器配置 DNS VIP。



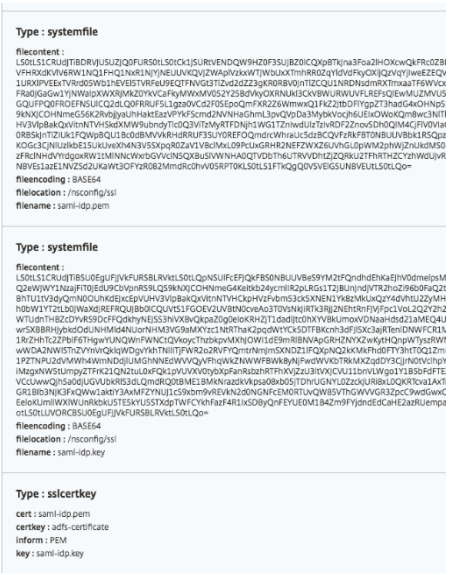
10. 单击 目标实例，然后选择要部署此 Microsoft ADFS 代理配置的 Citrix ADC 实例。单击 创 建”以创建配置并在所选 Citrix ADC 实例上部署配置。

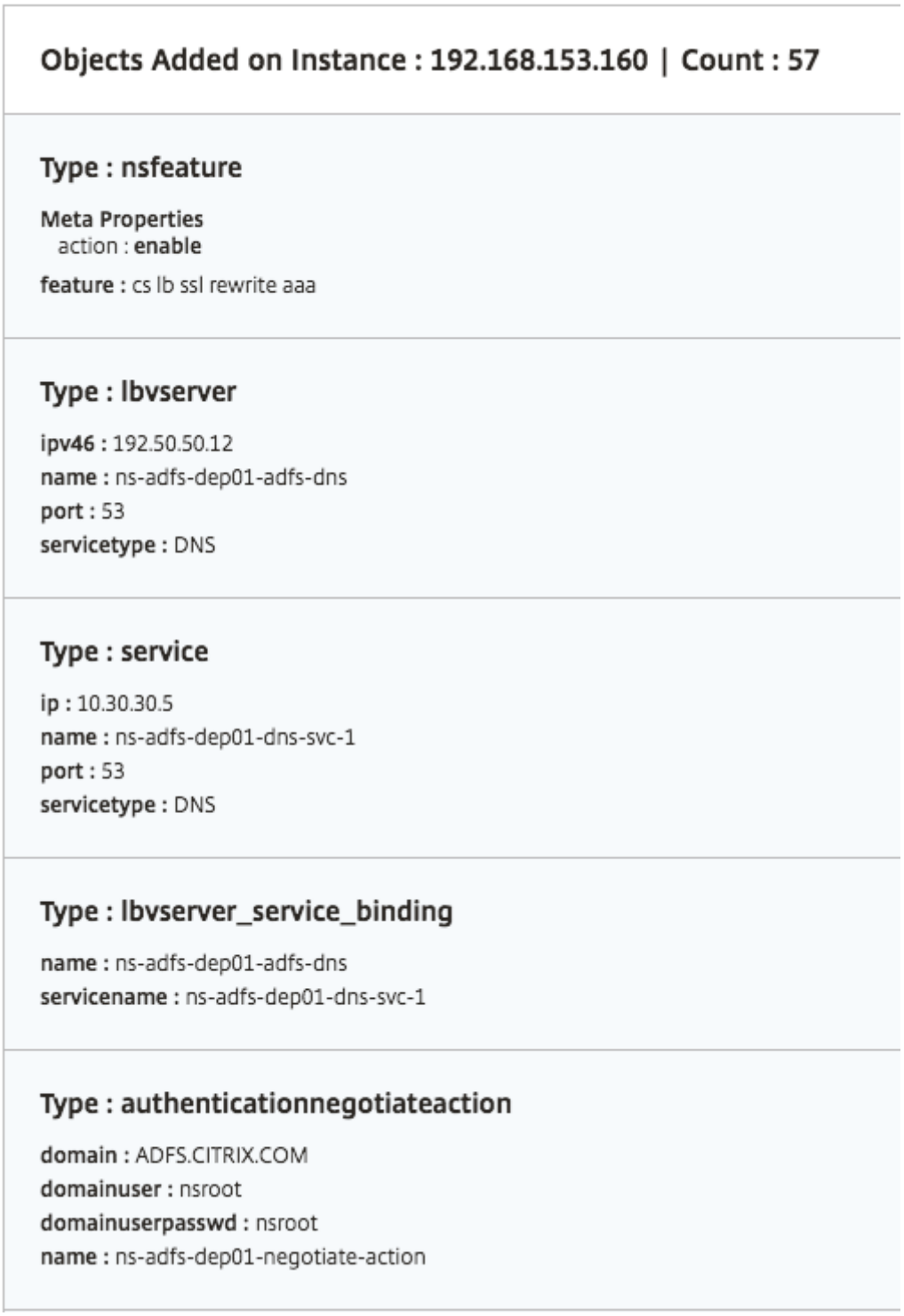


> 注意
>
> Citrix 建议在执行实际配置之前，选择干运行。您可以首先查看样本在目标 Citrix ADC 实例上创建的配置对象。然后，您可以单击“创建”在所选实例上部署配置。

创建的对象

在 Citrix ADC 实例上部署 ADFS 代理配置时，会创建多个配置对象。下图显示创建的对象的列表。





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

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

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

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

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

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

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

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

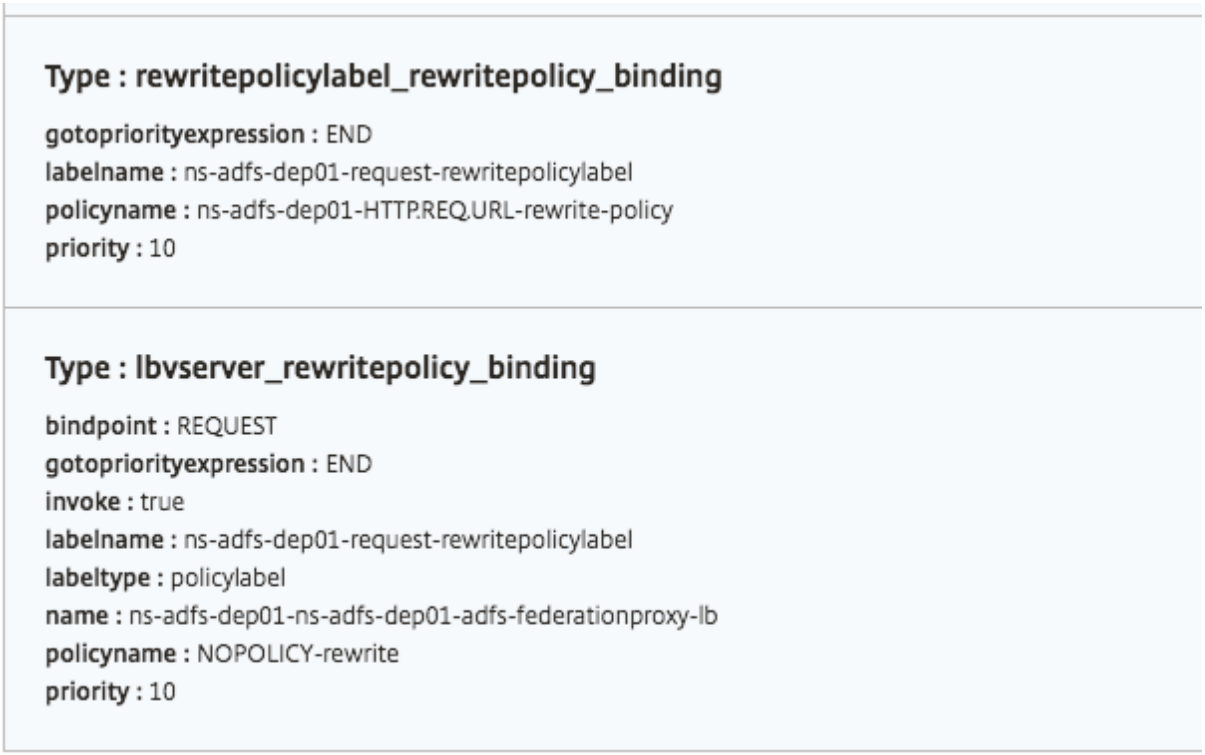
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

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"))



甲骨文电子商务样书

February 6, 2024

Oracle 电子商务套件是最全面的集成式全球业务应用程序套件。该套件使组织能够做出更好的决策、降低成本和提高性能，它由以下应用程序组成。

- 企业资源规划 (ERP)
- 客户关系管理 (CRM)
- 供应链管理 (SCM)

这些计算机应用程序要么是由 Oracle 开发的，要么是收购的。Oracle 电子商务套件 12.2 样书允许您在选定的 Citrix ADC 实例上部署配置。

此样书创建负载平衡配置，该配置包括负载平衡虚拟服务器、服务组和服务列表。它还将服务绑定至服务组，并将服务组绑定至虚拟服务器。您可以通过选择 SSL 并从本地系统提供 SSL 文件和密钥文件来选择加密通信。

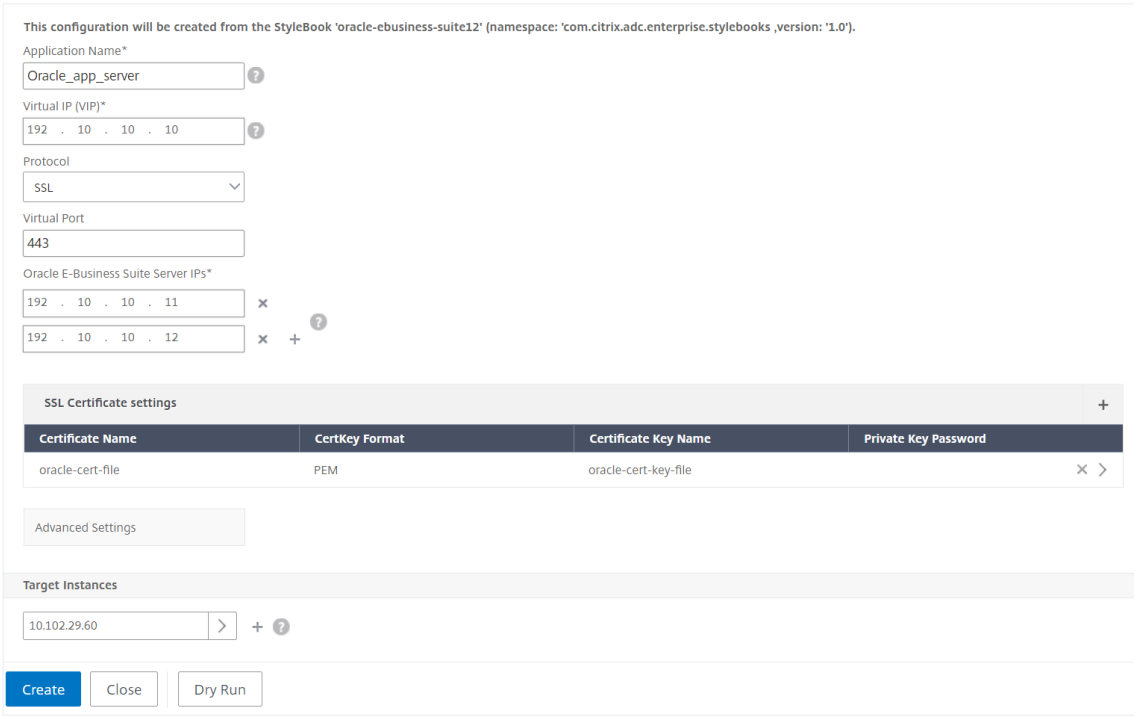
为 **Oracle** 电子商务套件 **12.2** 创建配置

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 应用程序 **>** 配置 **>** 样书。样书页面显示您的 Citrix ADM 中可用的所有样书。向下滚动并选择 **Oracle** 电子商务套件 **12.2**。您也可以使用搜索选项搜索

样书。

2. 在“样书”面板中单击“创建配置”。
3. 在负载平衡器设置部分中键入负载平衡器应用程序的名称和虚拟 IP 地址。
4. 选择所需的协议。这里有两个选项——HTTP 和 HTTPS/SSL。您也可以键入端口号。
5. 键入网络中要进行负载平衡的所有 Oracle 电子商务套件应用程序服务器的 IP 地址。单击 **+** 添加更多服务器 IP 地址。
6. 在 **SSL** 证书设置 部分，从本地存储中选择相应的文件。您还可以启用 高级证书设置”复选框。在这里，您可以配置更多详细信息，例如证书到期通知期限。您也可以启用或禁用证书到期监视器。

   选择必须在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。



> 提示
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。刷新图标当前仅在 Citrix ADM 上可用。

创建和使用自定义样书

February 6, 2024

您可以为部署编写自己的样书，将其导入到 Citrix Application Delivery Management (ADM)，然后创建配置对象。还可以使用 API 根据您的样书创建配置。

本文档包含以下信息：

开始之前的准备工作

开始创建样书之前，请确保您了解以下内容：

- NITRO API。有关更多信息，请参阅 Nitro API 文档
- YAML

样书文件使用 YAML 格式。有关 YAML 格式的信息，请参阅 YAML 语法。

下面是创建样书时必须了解的 YAML 准则列表：

- YAML 区分大小写。
- YAML 要求使用正确的行首缩进。
- 使用 <spacebar> 键创建正确的缩进。不要使用 <tab> 键。在将样书导入 MA Service 时，使用 <tab> 键会导致编译错误。
- 请勿在字符串两边加引号。仅当字符串包含标点符号（破折号、冒号等）时才在字符串两边加引号。如果要将数字解释为字符串，请在数字两边加引号或使用样书的内置函数 str()。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off 和 TRUE/true/truthy/FALSE/False/false/-falsely 等字面值被视为布尔值，分别等同于 true 和 false。要将它们解释为字符串，请在其两边加引号。例如：
  - “YES”
  - “No”
  - “True”
  - “False”等等。

> 注意
>
> 在将样书文件导入 Citrix ADM 之前，建议您验证您的文件是否符合 YAML 格式。Citrix 建议您使用样书中的内置 YAML 验证程序来验证和导入 YAML 内容。
>
> 配置样本时，您只能使用支持创建和删除操作的 Nitro 配置资源（POST 和 DELETE HTTP 方法）。有关更多信息，请参阅 Nitro API 文档。

样书解析

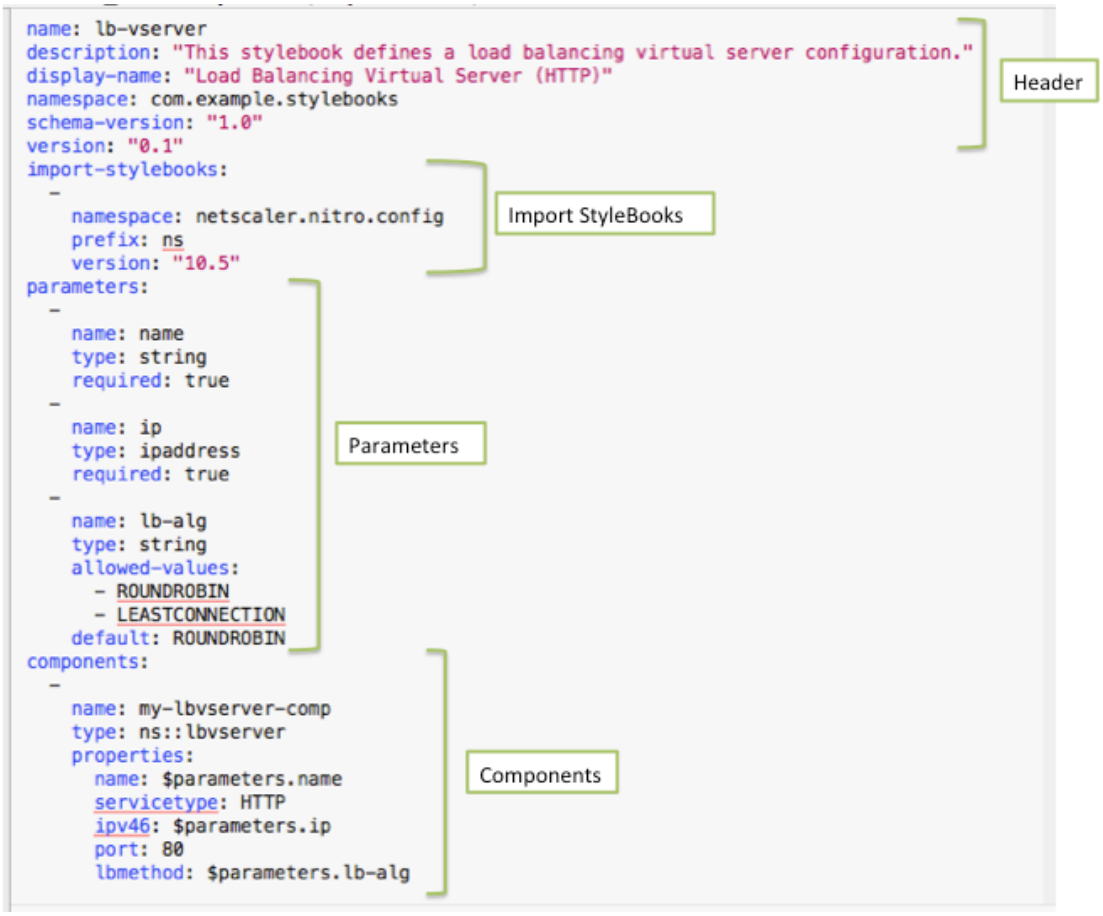
编写样本要求您了解样本的语法、句法和结构。典型的样书包含以下部分：

- 标题：本节允许您定义样书的标识并描述其用途。这是必需的部分。

- 导入样书：此部分用于声明要在当前样书中引用哪个其他样书。编写样书需要导入 Citrix ADC NITRO 配置样书或其他样书。这是必需的部分。
- 参数：此部分用于定义样书中所需的参数以创建配置。它描述样书接收的输入。这是可选部分。
- 组件：此部分允许您定义样书为特定配置创建的实体（配置对象）。此部分被视为样本的核心。组件通常使用 parameters 部分中提供的输入来改写样本生成的配置。这是可选部分。

  样书可以包含参数部分或组件部分，也可以同时包含两者。如果要定义其他样本可以使用的一组参数，可以使用仅含 parameters 部分的样本。这有利于在一组样本之间重用参数组。如果要在样本中指定属性值，而不是定义参数来接收用户输入，可以使用仅含 components 部分的样本。
- 输出：参数部分定义样书的输入时，此可选部分定义其输出。在此可选输出部分，可以指定要向基于此样本创建配置的用户和导入此样本的其他样本呈现的组件。之后，用户和导入样书可以引用呈现的组件的属性。
- 操作：样书可能包含一个可选部分，用于在作为样书一部分的任何虚拟服务器上在 Citrix ADM 中启用分析。

下图显示了一个简单的样书概况。



以下示例帮助您了解样书的语法和结构，以及如何编写复杂程度不断增加的样书。

- 用于创建负载平衡虚拟服务器的样书
- 用于创建基本负载平衡配置的样书

- 创建复合样书
- 使用 GUI 属性自定义您的样书

用于创建负载平衡虚拟服务器的样书

February 6, 2024

在此示例中，设计一个创建协议类型为 HTTP 且侦听端口 80 的负载平衡虚拟服务器的基本样书。虚拟服务器名称、IP 地址和负载平衡方法参数接受用户定义的值，即它们是样本的参数。

标题

样本的前六行构成标头部分。在此示例中，标头部分编写如下：

```
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"
<!--NeedCopy-->
```

标头部分包含以下详细信息：

- **name**：此样书的名称。
- **description**：定义此样书做什么的说明。此描述显示在 Citrix ADM 上。
- **display-name**：出现在 Citrix ADM 上的样书的描述性名称。
- **namespace**：样书的唯一标识符的命名空间形式部分，以避免发生名称冲突。
- **schema-version**：在此版本中，其值总是“1.0”。
- **version**：样书的版本号。可以在更新样本时更改版本号。

name、**namespace** 和 **version** 组合在系统中唯一标识样书。在 Citrix ADM 中不能有两本具有相同名称、命名空间和版本组合的样书。但可以有两个 name 和 version 相同但 namespace 不同或 namespace 和 version 相同但 name 不同的样书。

> 注意
>
> 假定您已更新您的样书，且您有更新的 version 号。现在，如果您要在其他样书中引用（即您要导入）此样书，请务必也在其他样书中更新 version 号，以便它们使用正确版本的导入样书。

导入样书

标头后面的部分称为“import-样书”。在此部分中，必须在当前样书中声明要引用的任何其他样书的 namespace 和 version 号。这样可以导入并重用其他样本，而不是在您自己的样本中重新构建相同的配置。

在此示例中，import-样书部分编写如下：

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

直接使用任何一个 NITRO 配置对象的每个样书都必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 Citrix ADC NITRO 类型，例如 LBVServer。由于支持 10.5 及更高版本的软件版本，因此您可以使用样书在运行 10.5 及更高版本的任何 Citrix ADC 实例上创建和运行配置。

import-样书部分中使用的前缀是指代命名空间和版本组合的简写。在此示例中，ns 是指版本为 10.5 的 netscaler.nitro.config。在样书的后面部分，并非使用命名空间和版本来指代被导入样书，可以使用上述示例中选择的前缀字符串，例如 ns。

样本中使用的版本是 Citrix ADC NITRO 版本。基于 Nitro 版本 X 的样本可用于配置 X 或更高版本的任何 Citrix ADC。

> 注意
>
> 为确保您的样本可用于配置 10.5 或更高版本的任何 Citrix ADC 实例，Citrix 建议您在直接使用 Nitro 内置样本的样本中导入 Nitro 10.5 命名空间 (namespace: netscaler.nitro.config, version: 10.5)。

重要的是，导入其他样书的样书必须基于与其导入的样书相同或更高版本的 Nitro 版本。例如，基于 Nitro 版本 10.5 的样书不能依赖或使用或导入基于 11.1 的样书。但是，基于版本 11.1 的样书可以导入基于小于 11.1 的任何版本的样书。

样书 也有可能根本不导入 Nitro 命名空间。这意味着样书无需直接定义 Nitro 组件，但可以导入（依赖）定义 Nitro 组件的样书。导入其他样本的样本始终获取其依赖关系层次结构中的最高 Nitro 版本，因此可用于配置该版本或更高版本的 Citrix ADC。

参数

parameters 部分用于声明样本中需要的所有参数。作为样本开发人员，您必须决定您希望样本的用户要指定哪些输入。在此示例中，构建的样本要求其用户提供虚拟服务器的名称、其 IP 地址以及负载平衡方法。

parameters 部分类似如下：

```
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
<!--NeedCopy-->
```

> 注意
>
> 如果您不提供参数的标签，则 Citrix ADM 在显示此参数时使用名称属性。您必须始终为参数定义标签，以便控制它们在 Citrix ADM 中的显示方式。
>
> 但使用 API 时，参数由其 name 指定。

在此部分中，声明了三个参数，它们以其 **name** 属性值来指示 - **name** 表示虚拟服务器名称，**ip** 表示虚拟服务器的 IP 地址，以及 **lb-alg** 表示负载平衡方法。

- 类型。这些参数可以采用的值类型。例如，name 和 lb-alg 可以接收字符串值，ip 值必须属于 IP 地址类型。样书中的参数可以是以下任何内置类型：
- 字符串。字符数组。如果未指定长度，则字符串值可以接收任何数量的字符。但是，可以使用 min-length 和 max-length 属性限制字符串类型的长度。
- 数字。一个整数。可以使用 min-value 和 max-value 属性指定此类型可以接收的最小数和最大数。
- 布尔值。可以是真的，也可以是假的。另外请注意，所有文字都被 YAML 视为布尔值（例如 Yes 或 No）。
- **ipaddress**。表示有效 IPv4 或 IPv6 地址的字符串。
- **tcp** 端口。一个介于 0 到 65535 之间的数字，代表 TCP 或 UDP 端口。
- 密码。一个不透明/秘密的字符串值。当 Citrix ADM 显示此参数的值时，它将显示为星号 (*****)。
- **certfile**。证书文件。

- 密钥文件。证书私钥文件。
- 文件。这种类型的参数要求用户上载文件，例如证书或密钥文件。
- 对象。由多个元素组成，每个元素都是一个参数。此类型可以用于对一个父参数下多个相关参数进行分组。
- 必需的。说明参数是必需的还是可选的。如果设置为 true，表示参数是必需的，用户必须在使用此样书创建配置时提供此参数值。默认情况下，所有参数都是可选的。在此示例中，名称 和 **ip** 是必填参数，而 **lb-alg** 是可选参数，其默认值为“ROUNDROBIN”。

可使用 **default** 属性为可选参数分配默认值。创建配置时，如果用户未指定值，则使用默认值。例如，**lb-alg** 参数的默认值是 ROUNDROBIN。

可使用 **allowed-values** 属性来定义用户创建配置时可从中选择的特定值。在此示例中，为 **lb-alg** 参数指定了两个值 - ROUNDROBIN 和 LEASTCONNECTION。

当您导入样本并使用它时，Citrix ADM 会显示一个包含这三个参数的表单。显示的 name 和 ip 字段用于输入字符串和 IP 地址类型的值，lb-alg 字段显示为下拉列表，在其中 ROUNDROBIN 选为默认值。

> 注意
>
> 除了内置类型外，参数的类型还可以是另一个样书。这就是重用其他样书中定义的参数的方式。

组件

此样书的最后一部分称为 components 部分，它被视为样书中最重要的部分。在此部分，定义必须由样本创建的配置对象。

例如，必须按如下所示编写 components 部分：

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

此示例仅包含一个组件。组件的主要属性是 name、type 和 properties。组件的类型确定此组件提供哪些属性。组件有两种类型：

- 内置类型。此类型由系统提供，您无需对其进行定义，例如，NITRO 实体类型 “lbvserver” 或 “servicegroup”。在此实例中，使用的是内置组件类型。
- 复合类型。此类型是您创建并导入到 Citrix ADM 中的样书或 Citrix ADM 附带的默认样书。您可以在创建复合样书中了解有关复合样本的更多信息。

在此示例中，您定义了一个名为 **lbvserver-comp** 的组件。此组件的类型为 **ns::lbvserver**（内置的 Nitro 类型），其中“ns”是指您在导入样式书籍部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀，“lbvserver”是该命名空间中的 Nitro 资源。

此处定义的 **properties** 是“lbvserver”资源的属性。要了解有关所有可用的 Citrix ADC Nitro 资源及其属性的更多信息，请参阅 Citrix ADC NITRO REST API 文档。

此部分中的属性包括“lbvserver”资源的必需属性，用于为这些属性指定值。在此示例中，为 servicetype 和 port 指定静态值，而 name、ipv46 和 lbmethod 属性从输入参数获取其值。在样书的其余部分中，可以使用 **$parameters.<parameter-name>** 表示法（例如 **$parameters.ip**）来引用在 parameters 部分定义的参数名称。

> 注意
>
> 按照惯例，在“导入样式手册”部分中始终使用前缀“ns”来指定 Citrix ADC Nitro 命名空间。尽管这不是必需的，但 Citrix 建议在您自己的样书中采用相同的约定以保持一致性。

构建您的样书

现在已定义了此样书的所有必要部分，将它们全部汇聚在一起即可构建您的第一个样书。将样书内容复制并粘贴到一个文本编辑器，然后将文件保存为 **lb-vserver.yaml**。Citrix 建议您使用样书中的内置 YAML 验证器来验证和导入 YAML 内容。

lb-vserver.yaml 文件的完整内容再现如下：

```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"
    type: ipaddress
    required: true
  -
    name: lb-alg
    label: LB Algorithm
    description: Load Balancing Algorithm
    type: string
    default: ROUNDROBIN
    allowed-values:
      - ROUNDROBIN
      - LEAST-CONNECTION

components:
  -
    name: lbvserver-comp
    description: This StyleBook component (a Builtin Nitro StyleBook)
       builds a Citrix ADC load balancing virtual server configuration
       object.
    type: ns::lbvserver
    properties:
      name: $parameters.name
      ipv46: $parameters.vip-ipaddress
      lbmethod: $parameters.lb-alg
      servicetype: HTTP
      port: 80
<!--NeedCopy-->
```

要开始使用样本创建配置，您必须将其导入 Citrix ADM，然后使用它。有关详细信息，请参阅如何使用用户定义的样书。

还可以将此样书导入其他样书（使用 import-样书构造）。或者，可以修改此样书以包含更多参数和组件，如下一节中所述。

用于创建基本负载平衡配置的样书

February 6, 2024

在前面的示例中，您构建了一个基本样书来创建负载平衡虚拟服务器。可以用不同的名称保存此样书，然后对其更新以包含用于基本负载平衡配置的其他参数和组件。将此样书文件保存为 **basic-lb-config.yaml**。

在本节中，将设计一个新样本，用于创建由负载平衡虚拟服务器、服务组和一组服务组成的负载平衡配置。它还将服务绑定至服务组，并将服务组绑定至虚拟服务器。

标题

要构建此样本，必须先更新标头部分。此部分与为负载平衡虚拟服务器样本创建的标头部分类似。在标头部分中，将 **name** 值更改为 basic-lb-config。此外，更新 **description** 和 **display-name** 以适当说明此样书。不必更改 **namespace** 和 **version** 值。因为已更改了名称，所以 name、namespace 和 version 组合构成了此样书在系统中的唯一标识符。

```
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"
<!--NeedCopy-->
```

导入样书

import-stylebooks 部分保持不变。它引用 netscaler.nitro.config 命名空间以使用 Nitro 配置对象。

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

参数

必须更新 parameters 部分以添加两个其他参数来定义一组服务或服务器以及服务侦听的端口。前三个参数 name、ip 和 lb-alg 保持不变。

```
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 used for load
       balancing client requests between the application servers.
      allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
       default: ROUNDROBIN
  -
    name: svc-servers
    type: ipaddress[]
    label: Application Server IPs
    description: The IP addresses of all the servers of this application
    required: true
  -
    name: svc-port
    type: tcp-port
    label: Server Port
    description: The TCP port open on the application servers to receive
        requests.
    default: 80
<!--NeedCopy-->
```

在此示例中，添加了参数 **svc-servers** 以接受代表应用程序后端服务器的服务 IP 地址列表。这是必需参数，由 **required: true** 指明。第二个参数 **svc-port** 表示服务器侦听的端口号。如果用户未指定，svc-port 参数的默认端口号是 80。

组件

必须还要更新 components 部分以定义其他组件，以便它们可以使用两个新参数并构建完整的负载平衡配置。

例如，必须按如下所示编写 components 部分：

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: 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: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

在此示例中，原始组件 **lbvserver-comp** （来自前面的示例）现在有一个名为 **svcg-comp** 的子组件。而且，**svcg-comp** 组件中有两个子组件。通过在一个组件里面嵌套另一个组件，嵌套的组件可以通过引用父组件中的属性来创建配置对象。嵌套的组件可以为父组件中创建的每个对象创建一个或多个对象。

svcg-comp 组件用于通过使用为资源“servicegroup”的属性提供的值在 Citrix ADC 实例上创建服务组。在此示例中，为 servicetype 指定静态值，而 name 从输入参数获取其值。通过使用 **$parameters.name +** “**-svcgrp**”表示法来引用在参数部分中定义的参数名称，其中 **-svcgrp** 附加（连接）到用户定义的名称。

组件 **svcg-comp** 有两个子组件，**lbvserver-svg-binding-comp** 和 **members-svcg-comp**。

第一个子组件 **lbvserver-svg-binding-comp** 用于在其父组件创建的服务组与父组件创建的负载平衡虚拟服务器 (lbvserver) 之间绑定配置对象。$parent 表示法（也称为父引用）用于引用父组件中的实体。例如，**servicegroupname: $parent.properties.name** 指由父组件 **svcg-comp** 创建的服务组，**name: $parent.parent.properties.name** 指由父组件 **lbvserver-comp** 创建的虚拟服务器。

成员 **svcg** 组件用于将服务列表之间的配置对象绑定到父组件创建的服务组。创建多个绑定配置对象是通过使用样书的重复构造迭代参数 **svc-servers** 中指定的一组服务器来完成。在迭代期间，这个样书组件为服务组中的每项服务（在重复项结构中称为 srv）创建 **servicegroup_servicegroupmember_binding** 类型的 Nitro 配置对象，并将每个 Nitro 配置对象中的 **ip** 属性设置为相应服务器的 IP 地址。

通常，您可以在组件中使用 重复项和重复项构造来使该组件生成多个相同类型的配置对象。您可以将变量名分配给重复项构造（例如 srv），以指定迭代中的当前值。这个变量名在同一个组件的属性或子组件中被引用为 **$**<varname\ >，例如 $srv。

在上述示例中，使用了在组件中相互嵌套组件来轻松构造此配置。在此特殊情况下，嵌套组件不是唯一的配置构建方式。您本可以在不嵌套的情况下获得同样的结果，如下所示：

```
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
   -
    name: svcg-comp
    type: ns::servicegroup
    properties:
    name: $parameters.name + "-svcgrp"
    servicetype: HTTP
<!--NeedCopy-->
```

在这里，所有组件都处于相同级别（也就是说，它们不嵌套），但实现的结果（生成的 Citrix ADC 配置）与之前使用的嵌套组件相同。此外，样书中组件的声明顺序不影响配置对象的创建顺序。在此示例中，尽管最后声明了组件 **svcg-comp** 和 **lbvserver-comp**，但必须在构建第二个组件 **lbvserver-svg-binding-comp** 之前构建，因为第二个组件中有对这些组件的前向引用。

> 注意
>
> 按约定，样书的名称、参数、替代项、组件和输出采用小写。如果它们包含多个词语，词语以“-”字符分隔。例如“lb-bindings”、“app-name”、“rewrite-config”等。另一个约定是为组件名称添加后缀“-comp”字符串。

输出

可以添加到新样本的最后一个部分是 outputs 部分，在其中指定在此样本用于创建配置后，此样本向其用户呈现的内容（或在其他样本中）。例如，可以在输出部分指定要呈现将由此样书创建的 lbvserver 和 servicegroup 配置对象。

```
outputs:
 -
  name: lbvserver-comp
  value: $components.lbvserver-comp
  description: The component that builds the Nitro lbvserver
     configuration object
 -
```



```
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

样书的输出部分是可选的。样书不必返回输出。但是，如果将一些内部组件作为输出返回，导入此样书的任何样书就可以有更大的灵活性，这在创建复合样书时可以看到。

> 注意
>
> 最好在 outputs 部分呈现样书的整个组件，而不仅仅是组件的单个属性（例如，呈现整个 $components.lbvserver-comp，而不仅仅是名称 $components.lbvserver-comp.properties.name）。另外在输出中添加说明，解释特定输出表示的内容。

构建您的样书

现在已定义了此样书的所有必要部分，将它们全部汇聚在一起即可构建您的第二个样书。已将此样书文件保存为 **basic-lb-config.yaml**。Citrix 建议您使用样书页面中的内置 YAML 验证器来验证和导入 YAML 内容。

basic-lb-config.yaml 文件的完整内容再现如下：

```
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
```



```
29    label: LoadBalancing Algorithm
30    description: Choose the loadbalancing algorithm (method) used for
         loadbalancing client requests between the application servers.
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  -
```



```
  name: servicegroup-comp
  value: $components.svcg-comp
  description: The component that builds the Nitro servicegroup
     configuration object
<!--NeedCopy-->
```

要开始使用样本创建配置，您必须将其导入 Citrix ADM，然后使用它。有关详细信息，请参阅如何使用用户定义的样书。

还可以将此样书导入其他样书并使用其属性，如下一节中所述。

创建复合样本

February 6, 2024

样书一个重要的强大功能是它们可以用作其他样书的构建块。样书 可以导入到另一个样书中，可以将其称为第二个样书的组件使用的 类型，类似于 Nitro 内置样书。

例如，您可以使用您在上一节中构建的 **basic-lb-config** 样书来构建另一本名为 **composite-example** 的样书。要使用“basic-lb-config”样书，必须在新样书的 import-样书部分将其导入。

构建您的样书

新样书类似如下：

```
name: composite-example
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
description: This StyleBook defines a RoundRobin load balancing
   configuration with a monitor.
schema-version: "1.0"
import-stylebooks:
  -
   namespace: netscaler.nitro.config
   version: "10.5"
   prefix: ns
  -
   namespace: com.example.stylebooks
   version: "0.1"
   prefix: stlb
parameters:
  -
    name: name
    type: string
    label: Application Name
    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
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
70  <!--NeedCopy-->
```

在 import-样书部分，使用 basic-lb-config 样书的命名空间和版本将其导入，引用时加前缀“stlb”。

在 components 部分，定义了两个组件。第一个组件的类型为 **stlb:: basic-lb-config**，其中“basic-lb-config”是您在样书中为创建 基本负载平衡配置而创建的样书的名称。为此组件定义的数据对应于 basic-lb-config 样书中声明的必需参数。但是，您可以使用样书的任何参数（包括必填参数和可选参数）。与其重新构建 lbvserver、服务组以及服务和服务组绑定，不如将完成所有这些操作的样书作为组件导入，然后使用它在新的样书中创建这些配置对象。

样书添加第二个组件“monit-comp”（使用 Nitro 资源“lbmonitor”（内置样书）的属性）来创建监视器配置对象。它还有子组件“monit-svcgrp-bind-comp”用来创建绑定配置对象，该对象将监视器绑定到第一个组件中创建的服务组。由于在“basic-lb-config”样书中创建的 servicegroup 组件是作为输出公开的，因此此样书可以使用表达式 **$components.basic-lb-comp.outputs.servicegroup-comp** 来访问它。此示例说明导入样书如何能够使用 outputs 部分来访问原本无法访问的被导入样书中的组件。

接下来，将样书内容复制并粘贴到文本编辑器中，然后将该文件保存为 **composite-example.yaml**。在 Citrix ADM 中导入文件之前，请务必验证 YAML 内容。然后，将其导入 Citrix ADM 并使用此样书创建一个或多个配置。

Citrix 建议您使用样本中的内置 YAML 验证程序来验证和导入 YAML 内容。

在自定义样书中使用 **GUI** 属性

February 6, 2024

您可以在样书的参数部分中添加 GUI 属性，以便在 Citrix Application Delivery Management (ADM) 上显示时使字段直观。

示例。您可以使用标签属性为参数添加描述性名称，并使用描述属性为该参数添加工具提示。

```
1  name: ip
2  label: Virtual Server IP Address
3  description: IP address of the virtual server that represents the load
      balanced application.
4  type: ipaddress
5  required: true
6  <!--NeedCopy-->
```

示例。如果您有对象类型的参数，则可以使用 **gui** 属性定义布局。在此示例中，布局是字段以两列显示的可折叠对象。

```
1  name: svcg-advanced
2  label: Advanced Application Server Settings
3  type: object
4  required: false
5  gui:
6   collapse_pane: true
```



```
 columns: 2
<!--NeedCopy-->
```

示例。您还可以将类型为 object[]（对象列表）的参数的摘要视图显示为表格，其中内部参数表示列。要在摘要视图中包含或排除内部参数，可以按如下方式在 gui 部分中使用 summary_display 属性：

```
name: settings
label: Settings
type: object[]
parameters:
  -
    name: name
    label: Name
    description: Name of this setting
    type: string
    gui:
      summary_display: true
<!--NeedCopy-->
```

示例。Citrix ADM 上的某些样书仅用作其他样书的构建块。而且，您可能不希望用户直接从这些样书创建配置。因为这些样书将用作其他样书的一部分。将样书标记为私有，以确保样书不会直接用于在 Citrix ADM GUI 中创建配置。

```
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"
<!--NeedCopy-->
```

使用自定义样本

February 6, 2024

生成样书后，必须将其导入到 Citrix ADM 才能使用。Citrix ADM 允许您以 YAML 形式导入单个样本或多个样本 YAML 文件作为.zip、.tgz 或.gz 形式的捆绑包导入。Citrix ADM 系统会在导入时验证您的样书。样本现已准备就绪，可用于创建配置。

Citrix ADM 还具有内置的 YAML 编辑器，您可以使用该编辑器来撰写样本 YAML 内容。YAML 编辑器允许您从 Citrix ADM GUI 本身验证您的 YAML 结构。您无需为这些验证检查使用单独的工具。内容根据 YAML 标准进行验证，并突出显示任何偏差。然后，您可以更正内容并尝试将样书导入 Citrix ADM。内置的 YAML 编辑器在编写自己的样书时有两个优点。

- 颜色编码。编辑器显示按照 YAML 指南解析的样本内容，颜色编码可帮助您轻松区分 YAML 内容中定义的键和值。

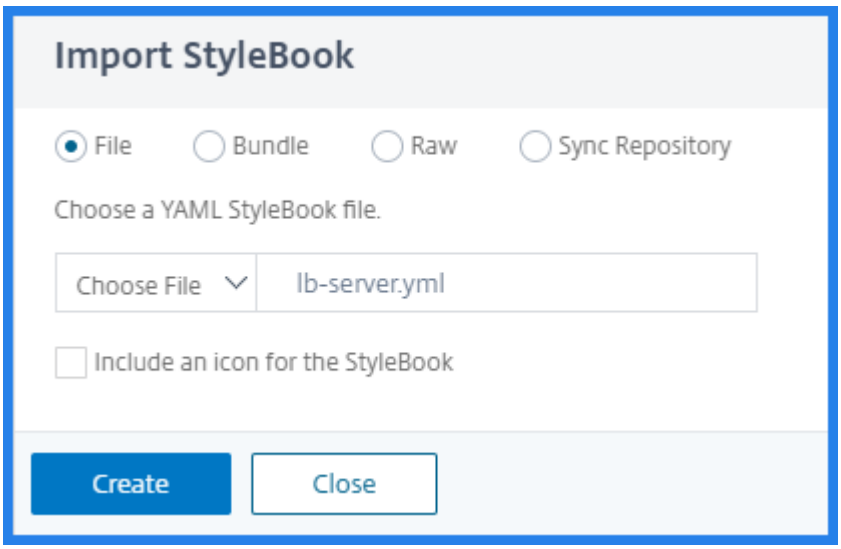
- **YAML** 验证。在您输入时，系统会验证内容是否存在任何 YAML 错误，并且任何偏差都会立即突出显示。这样，即使在 Citrix ADM 中导入样本之前，您也可以编写符合 YAML 准则的文本。目前，编辑器根据 YAML 指南对内容进行验证。它不验证代码的正确性和印刷错误。

导入您的样书

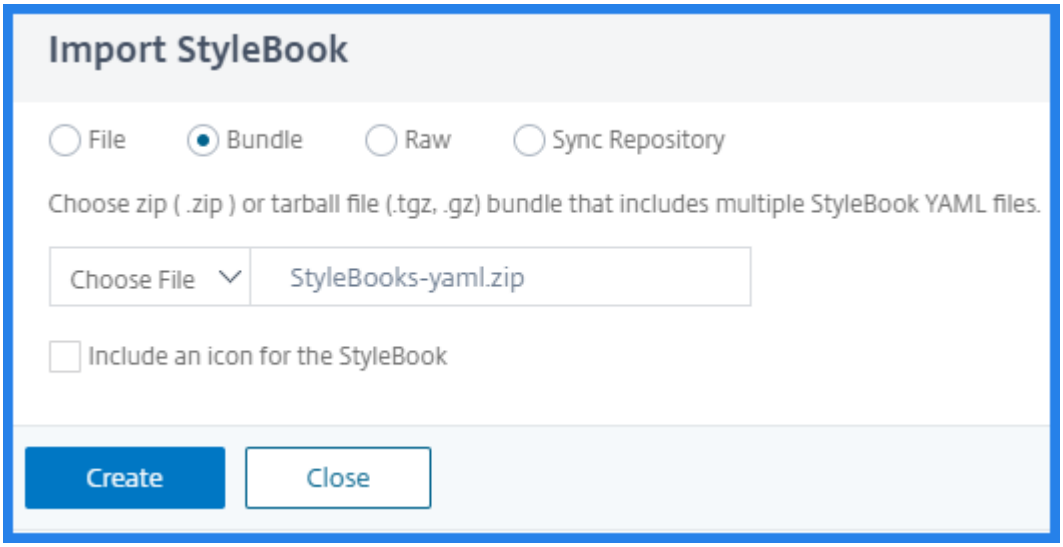
1. 在 Citrix ADM 中，导航到 应用程序 > 配置 > 样本，然后单击 “导入新样本”。
2. 单击可供您导入样本的三个选项之一。

   a) 文件。从本地存储中选择所需的文件或文件包。

   > 注意
   >
   > 在本示例中，导入您在样书 中创建的“lb-vserver.yaml”样书以创建负载平衡虚拟服务器。

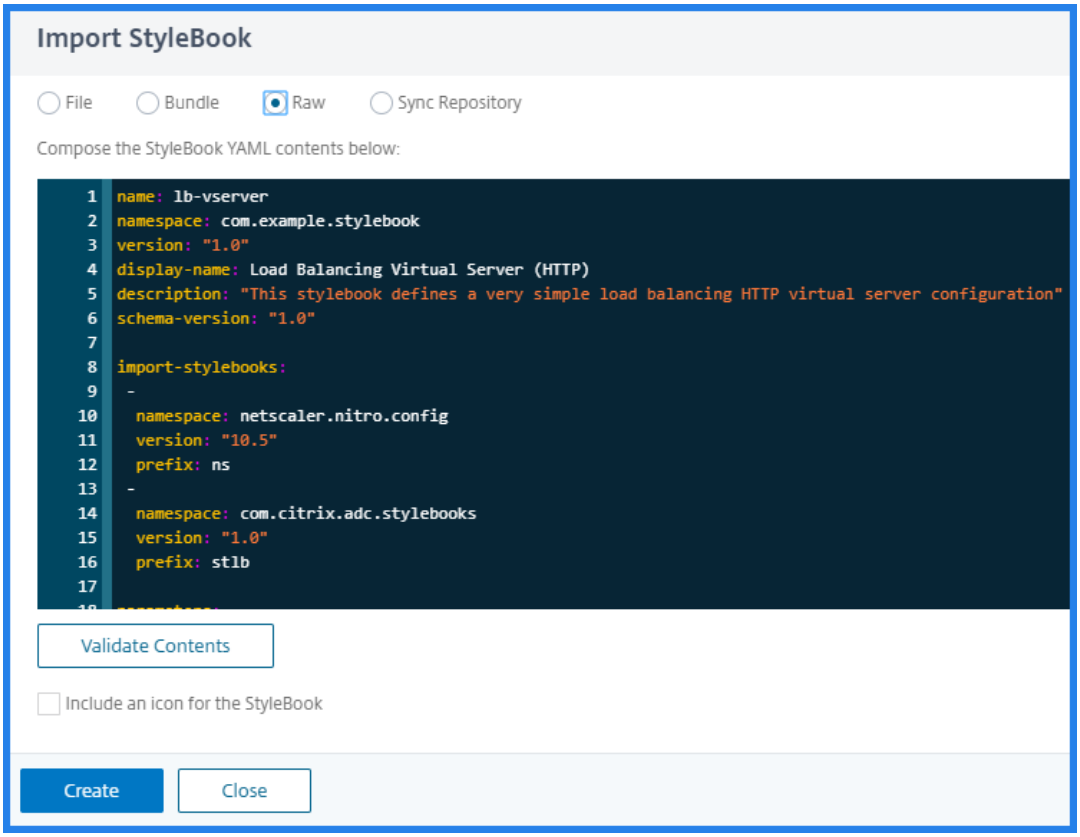
   b) 捆绑。Citrix ADM 允许您以 YAML 格式导入多个样本。您可以导入多个 YAML 样本文件，这些文件以压缩为压缩 (.zip) 格式或格式 (.tgz, .gz) 格式压缩。



c) 原始。在 YAML 编辑器中撰写样书的内容。

> 注意
>
> 在撰写样书时，请确保您了解以下内容：
>
> - NITRO API
> - YAML

有关如何编写自己的样书的详细信息，请参阅 如何创建自己的样书。



> 注意
>
> 您还可以从样本 YAML 文件复制和粘贴内容以验证内容。

3. 单击创建。

   Citrix ADM 现在根据样本语法验证样本是否存在所有语法和语义错误。如果出现任何错误，则不会将您的样书导入到 Citrix ADM 中。如果没有错误，样本已成功导入，并且现在在样本页面上列出。您可以通过在样书标题部分中定义的显示名称来识别样书。

   > 注意
   >
   > 如果您要导入文件包，Citrix ADM 会解压缩压缩压缩的文件夹并验证所有样书。
   > 即使一个样本文件未通过验证测试，也不会导入捆绑包。

   有关样书语法和不同结构和属性的语法的更多信息，请参阅 样书语法。

4. 要使用此样书创建配置，请 单击“创建配置”链接。样书将以用户界面页面形式打开，您可以在此为此样书中定义的所有参数输入值。

5. 指定参数所需值。在下面的示例中，您可以看到 应用程序名 称和 负载平衡器 **IP** 地址 字 段显示为必填字段，并且可以接受用户值。 **LB** 算法 只有两个值可供选择，默认情况下，ROUNDROBIN 处于选中状态。

6. 在“目标实例 ”下，单击并选择要运行配置的 Citrix ADC 实例的 IP 地址。您还可以根据需要指定任意数量的目标实例，在多个 Citrix ADC 上部署配置。

如果您想在实际创建配置之前查看将在 Citrix ADC 上创建的 Citrix ADC（Nitro）配置对象，请 单击 **Dry Run**。如果您的配置有效，则会显示将基于您提供的值创建的配置对象。在此示例中，此示例样本仅创建一个类型 lbvserver 的对象。这个 lbvserver 是在这个基本示例样本中定义的唯一组件。稍后您可以单击 “创建”在所选的 Citrix ADC 实例上实际创建配置。

创建完成后，新的配置包将在“配置”页面上列出。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

搜索自定义风格书

Citrix ADM 现在允许您根据样本类型搜索样本。也就是说，您现在可以搜索默认样书或自定义 样书。当您必须在大量默认样书中搜索用户定义的样书时，此选项特别有用。

搜索自定义样书

1. 在 Citrix ADM 中，导航到 应用程序 > 配置 > 样本。
2. 单击右上角的搜索图标。
3. 在出现的搜索栏中，从第一个列表中选择“类型”，然后从下一个选项列表中选择“自定义”。
4. Citrix ADM 仅显示用户定义的样本。

创建样本以将文件上载到 **Citrix ADM**

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 样书允许您在使用 Citrix ADM GUI 或 API 将任何类型的文件从本地文件系统上载到 Citrix ADC 实例时创建 Citrix ADC 配置，其中可能包括其他配置。这些文件可以是示例证书文件或地理定位文件。您也可以指定上载这些文件的目录。

样书配置

以下是样书示例，描述了如何在 Citrix ADC 实例上上载地理位置文件。地理文件通常用于 GSLB 配置中，用于根据地理位置定义静态邻近：

创建您的样书**-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)
<!--NeedCopy-->
```

> ** 注
>
> 意 ** 此示例中使用的参数是类型文件。您可以在 Citrix ADM 中导入此样本并使用它上载地理定位文件。

这本样书要求该文件已经存在于 Citrix ADM 中（例如，您已经使用像 scp 这样的实用工具将其复制到 Citrix ADM 了）。

如果要通过 Citrix ADM 将文件上载到 Citrix ADC 而不首先将其复制到 Citrix ADM 文件系统，则可以构建一个样本，其中包含两个“string”参数，一个用于指定要在 Citrix ADC 上使用的文件名，另一个用于指定文件，然后在上载文件组件中使用这两个参数。以下是上载地理位置文件的替代样书：

创建您的样书-2

```
name: upload-geolocations-alt
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: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
   filename: $parameters.filename
   filelocation: "/var/Citrix ADC/inbuilt_db/"
   filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```

创建用于上载文件的配置

以下过程在选定的 Citrix ADC 实例上创建配置，该配置将使用上述第一本样书上载地理定位文件。

要创建上载文件的配置，请执行以下操作：

1. 在 Citrix ADM 中，导航到“应用程序”>“配置”，然后单击“新建”。“选择样书”页面显示您的 Citrix ADM 中所有可用的样书。向下滚动并选择您导入的样书。

   样书参数显示为用户界面页面，允许您输入此样书中定义的所有参数的值。

2. 在基本负载平衡器设置部分中输入负载平衡器的名称和虚拟 IP 地址。

3. 在“位置文件”部分中，输入文件的名称或位置。

> 注意：
>
> 确保在 Citrix ADM 中，文件仅位于当前租户的文件夹下。使用任何文件传输协议将文件复制到 Citrix ADM 文件系统。

4. 在访问目标实例之前，可能会要求您提供用户凭据。
5. 选择需要在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。

> 注意：
>
> Citrix 建议您选择干运行以检查在目标实例上创建的配置对象，然后再对实例执行实际配置。

成功创建配置包后，文件将保存在 Citrix ADC 实例文件系统中的位置：/var/netscaler/inbuilt_db/

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

使用 **Citrix ADM API** 创建配置包

您还可以使用 Citrix ADM API 创建用于将文件上载到选定的 Citrix ADC 实例的配置包。有关如何使用 API 的更多信息，请 参阅如何使用 API 创建配置以上载任何文件类型。

创建样本以将 **SSL** 证书和证书密钥文件上载到 **Citrix ADM**

February 6, 2024

创建使用 SSL 协议的样书配置时，必须上载样书参数所需的 SSL 证书文件和证书密钥文件。样书允许您使用 Citrix ADM GUI 直接从本地系统上载 SSL 文件和密钥文件。您还可以使用 Citrix ADM API 上载已由 Citrix ADM 管理的证书文件和密钥文件。

样书配置

本文档帮助您创建自己的样书- 负载平衡虚拟服务器 **(SSL)**
，其中包含用于上载 SSL 证书和密钥文件的组件。此处提供的样书作为示例在选定的 Citrix ADC 实例上创建了基本的负载平衡虚拟服务器配置。该配置使用 SSL 协议。要使用此样书创建配置，必须提供虚拟服务器的名称和 IP 地址，选择负载平衡方法参数，然后上载虚拟服务器的证书文件和证书密钥文件，或者使用已经存在的证书文件和证书密钥文件存在于 Citrix ADM 中。这些内容在 parameters 部分中指定，如下所示：

```
parameters:
 -
  name: name
```



```
    type: string
    required: true
  -
    name: ip
    type: ipaddress
    required: true
  -
    name: lb-alg
    type: string
    allowed-values:
      - ROUNDROBIN
      - LEASTCONNECTION
    default: ROUNDROBIN
  -
    name: certificate
    label: "SSL Certificate File"
    description: "The file name of the SSL certificate file"
    type: certfile
  -
    name: key
    label: "SSL Certificate Key File"
    description: "The file name of the server certificate's private key
       file"
    type: keyfile
<!--NeedCopy-->
```

然后在样本的 components 部分中创建两个组件，如下所示。my-lbvserver-comp 组件的类型为 ns::lbvserver，其中：

- “ns”是指代在 import-样书部分中指定的内置命名空间 netscaler.nitro.config 和版本 10.5 的前缀。
- lbvserver 是此命名空间中的内置样书。它对应于同名的 Citrix ADC NITRO 负载平衡虚拟服务器资源。

第二个组件“lbvserver-certificate-comp”的类型为 stlb::vserver-certs-binds。前缀“stlb”指代在样书的 import-样书部分中指定的命名空间 com.citrix.adc. 样书和版本 1.0。如果 com.citrix.adc. 样书命名空间可以视为文件夹，则 vserver-certs-binds 是该文件夹中的另一个样书（或文件）。位于命名空间“com.citrix.adc. 样本”中的样本将作为 Citrix ADM 的一部分发送。

用户定义样本使用的“v 服务器 cers-binds”样本允许您通过将证书和密钥文件上载到目标 Citrix ADC 实例，并配置证书和密钥文件绑定到相应的虚拟服务器，轻松配置证书。此组件的属性是-lb 虚拟服务器的名称和您在创建 configpack 时提供的 SSL 证书的名称。

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   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:
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
24  <!--NeedCopy-->
```

使用 API 基于此类样书创建配置时，只使用文件名（而不是完整文件路径）。这些文件预计已在 Citrix ADM 的证书和密钥文件文件夹中可用。上载的 SSL 证书文件存储在 Citrix ADM 的 /var/mps/tenants/…/ns_ssl_certs 目录，SSL 证书密钥文件存储在 /var/mps/tenants/…Citrix ADM 中的 /ns_ssl_keys 目录。

创建用于上载 **SSL** 文件的配置

以下过程使用上面指定的样书中的 SSL 协议在选定的 Citrix ADC 实例上创建基本的负载平衡虚拟服务器配置。您可以使用此过程在 Citrix ADM 中上载 SSL 证书文件和证书密钥文件。

创建配置用于上载文件

1. 在 Citrix ADM 中，导航到 应用程序 **>** 配置 **>** 样书。“样书”页面显示 Citrix ADM 中可用的所有样书。
2. 向下滚动并选择 负载平衡虚拟服务器 **(SSL)** 或在搜索字段中键入负载平衡虚拟服务器 **(SSL)** ，然后按 **Enter** 键。
3. 单击“样书”面板中的“创建配置”链接。

   样书参数显示为用户界面页面，允许您输入此样书中定义的所有参数的值。
4. 在基本负载平衡器设置部分中输入负载平衡器的名称和虚拟 IP 地址。
5. 在 **SSL** 证书设置 部分，从本地存储文件夹中选择相应的文件。或者，您可以选择 Citrix ADM 本身上存在的文件。
6. 选择需要在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。

> 备注：
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。
>
> 在 Citrix ADM 中，以下作为 Citrix ADM 一部分提供的默认样本允许您通过上载 SSL 证书和密钥来创建 SSL 支持。

> - HTTP/SSL 负载平衡样书 (lb)
> - HTTP/SSL 负载平衡（具有监视器）样本 (lb-mon)
> - HTTP/SSL 内容交换应用程序（具有监视器）(cs-lb-mon)
> - 使用 CS、LB 和 SSL 功能的示例应用程序样本 (sample-cs-app)
>
> 您还可以创建自己的样本，以上面的样本中所述的同一方式利用 SSL 证书

构建您的样书

lb-vserver-ssl.yaml 文件的完整内容如下所示：

```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
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
```



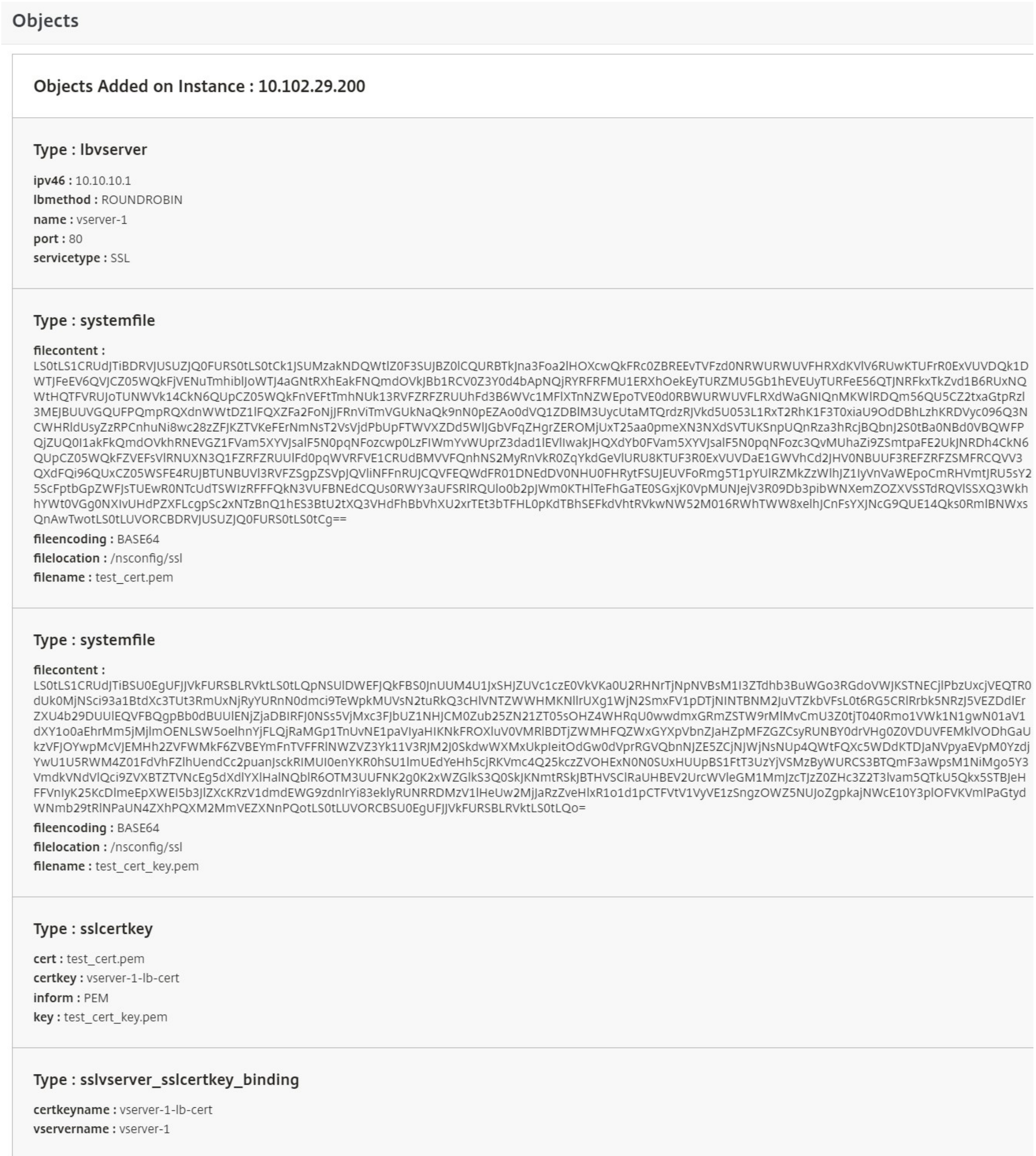
```
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile

components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
    name: $parameters.name
    servicetype: SSL
    ipv46: $parameters.ip
    port: 443
    lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $ components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```

使用 **Citrix ADM API** 创建配置包

您还可以使用 Citrix ADM API 创建配置包，将证书和密钥文件上载到选定的 Citrix ADC 实例。有关如何使用 API 的更多信息，请 参阅如何使用 API 创建配置来上载证书和密钥文件。

查看在 **Citrix ADC** 实例上定义的对象

在 Citrix ADM 上创建样书配置包（配置包）后，单击“查看创建的对象”以显示在目标 Citrix ADC 实例上创建的所有 Citrix ADC 对象



在样书中定义的虚拟服务器上启用分析并配置警报

February 6, 2024

您可以使用操作构造配置 Citrix ADM 分析，以收集由作为样书一部分的任何虚拟服务器组件处理的所有或部分流量事务的应用程序流记录。还可以使用此构造来配置警报，以深入了解虚拟服务器管理的流量。

以下示例显示了样书的 operations 部分：

```
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"
<!--NeedCopy-->
```

分析部分中的属性用于指示 Citrix ADM 分析功能收集由目标属性标识的虚拟服务器组件上的 appflow 记录。您还可以选择指定一个过滤器属性，该过滤器属性接受 Citrix ADC 策略表达式，以筛选在虚拟服务器上收集应用程序流记录的请求。

通过此样本创建配置包时，Citrix ADM 分析功能将配置为收集虚拟服务器上指定的 AppFlow 记录，这些记录是在创建配置包的过程中创建的。

alarms 部分的属性用于设置阈值，以在由目标属性标识的虚拟服务器上生成警报并发送通知。在上述示例中，email-profile 属性和 sms-profile 属性用于指定应向哪里发送通知。rules 部分定义阈值。例如，如果虚拟服务器处理的请求总数超过 25 并在用户定义的期间，即设置警报并发送通知。“period-unit”指定触发警报的频率。它可以采取日、小时或每周的值。

可以在比较指标值与阈值时使用以下运算符：

- “greaterthan”表示“>”
- “lessthan”表示“<”
- “greaterthanequal”表示“>=”
- “lessthanequal”表示“<=”

请注意，样本使用 API 名称作为指标，而不是 Citrix ADM 分析 GUI 上显示的名称。

要了解如何查看和分析在作为配置包一部分创建的虚拟服务器上收集的数据，请参阅 Citrix ADM 分析文档。

实例角色

February 6, 2024

在 Citrix Application Delivery Management (ADM) 中，可能存在必须为单个应用程序配置多个 Citrix ADC 实例的情况，但也可能需要在每个 ADC 实例上部署不同的配置。这种情况下的一个示例是默认的 Microsoft Skype for Business 样书。

样书目前支持创建配置包并在多个 Citrix ADC 实例上应用相同配置的功能。在所有 ADC 实例上配置相同的情况下，可以称为对称配置。

现在，借助样书的“实例角色”功能，您可以创建非对称配置，即可以应用于多个 ADC 实例的配置包，但在不同的 ADC 实例上具有不同的配置。

当使用带有实例角色的样书功能创建配置包时，可以为配置包中的每个 ADC 实例分配不同的角色。此角色确定 ADC 实例将接收的配置包的配置对象。

注意事项：

- 样书中的一组实例角色是在创建样书时定义的。
- 在创建或更新配置包时，会将角色分配给特定的 ADC 实例。

目标角色部分

样书中引入了一个名为“目标角色”的新章节，其中声明了样书支持的所有角色。

此部分通常位于样书的“import-StyleBooks”部分之后和参数部分之前。

在以下样书示例中，在“目标角色”部分中定义了两个角色——A 和 B。

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
<!--NeedCopy-->
```

您可以看到角色 B 还定义了两个可选子属性，即最小目标和最大目标。

尽管这两个子属性是可选的，但最小目标指定了从该样书创建配置包时应分配此角色的最小强制性 ADC 实例数，而最大目标则指定从该样书创建配置包时可以分配此角色的最大 ADC 实例数。

如果未指定这些子属性，则可以为该角色配置的 ADC 实例数量没有限制。如果最小目标 = 0，则与该角色关联的配置是可选的，如果最小目标 = 1，则该配置是必需的，并且至少需要为该角色配置一个 ADC 实例。

角色“默认”

除了明确定义的角色外，还有一个所有样书都具有的隐式角色，该角色被称为默认角色。此角色可以像样书中的任何其他角色一样使用。创建配置包时，如果未为 ADC 实例分配特定角色，则该实例将被隐式分配给“默认”角色。实例现在将接收由具有“默认”角色的组件生成的任何配置对象。

具有角色的组件

定义了样书可以支持的角色（包括“默认”角色）后，这些角色可以在样书的组件部分中使用。如果希望仅在发挥特定角色的 ADC 实例上部署组件，则可以将角色属性指定为组件的一部分，如以下组件示例所示：

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

在上面的示例中，组件生成一个“lbvserver”，该服务器将部署在扮演角色 A 的实例上。请注意，组件的角色属性是一个列表，可以为一个组件分配多个角色。这些角色本来可以在样书的“目标角色”部分中声明的。

注意：如果样书中的某个组件未指定角色属性，则无论其角色如何，都会在所有 Citrix ADC 实例上创建由该组件生成的配置对象。您可以有效地使用此功能来创建可应用于 configpack 所有实例的配置对象。

让我们假设有一个定义了两个角色的样书-A 和 B，其中包含四个组件。

- 组件 C1 具有角色 A 和 B
- 组件 C2 具有作用 B
- 组件 C3 未定义任何角色
- 组件 C4 的角色为“默认”

本样书的组件部分转载如下：

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
```



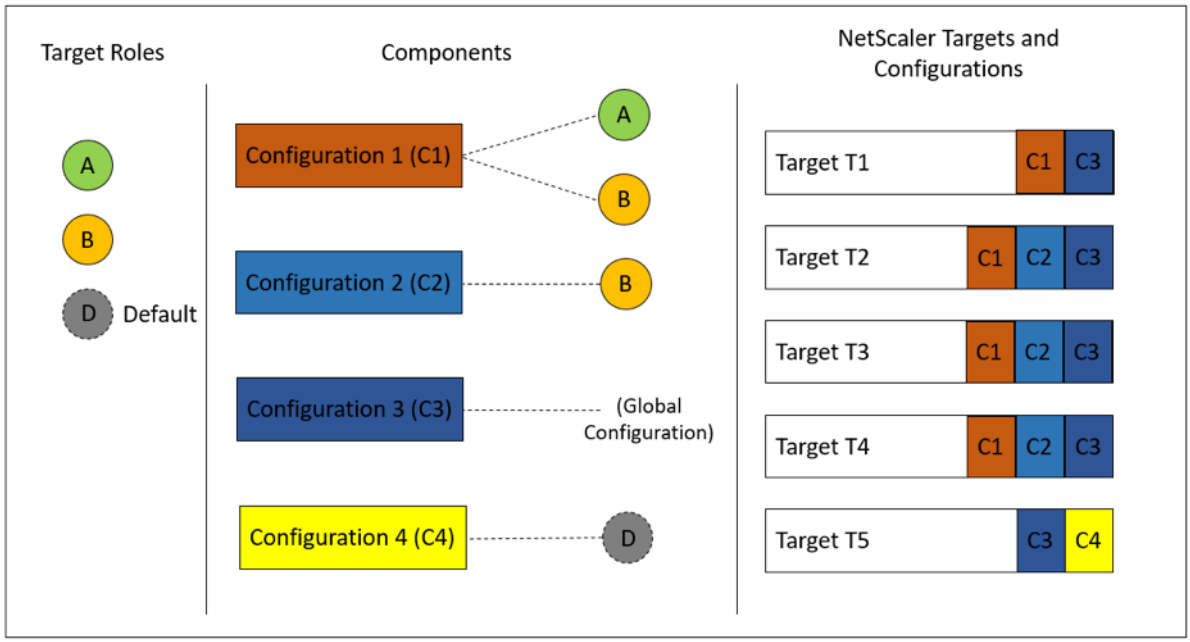
```
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

请注意，组件 C3 没有定义角色，这意味着无论其角色如何，该组件都部署在所有实例上。另一方面，组件 C4 具有“默认”角色，这意味着它应用于没有分配明确角色的任何实例。

现在，假设您想使用这本样书创建一个配置包，并将其部署在五个 ADC 实例上。在此阶段，您可以通过以下方式将角色分配给实例：

- 角色 A 分配给实例 T1、T2、T3 和 T4
- 角色 B 分配给实例 T2、T3 和 T4
- 实例 T5 未分配任何角色

下图总结了角色分配，并显示了每个 ADC 实例将收到的结果配置：



请注意，组件 C3 部署在所有实例上，而不考虑角色如何，因为此组件没有角色属性。

您还可以在创建配置包时使用“试运行”功能来查看和验证将在每个 ADC 实例上创建的角色和配置对象的正确分配。

构建您的样本

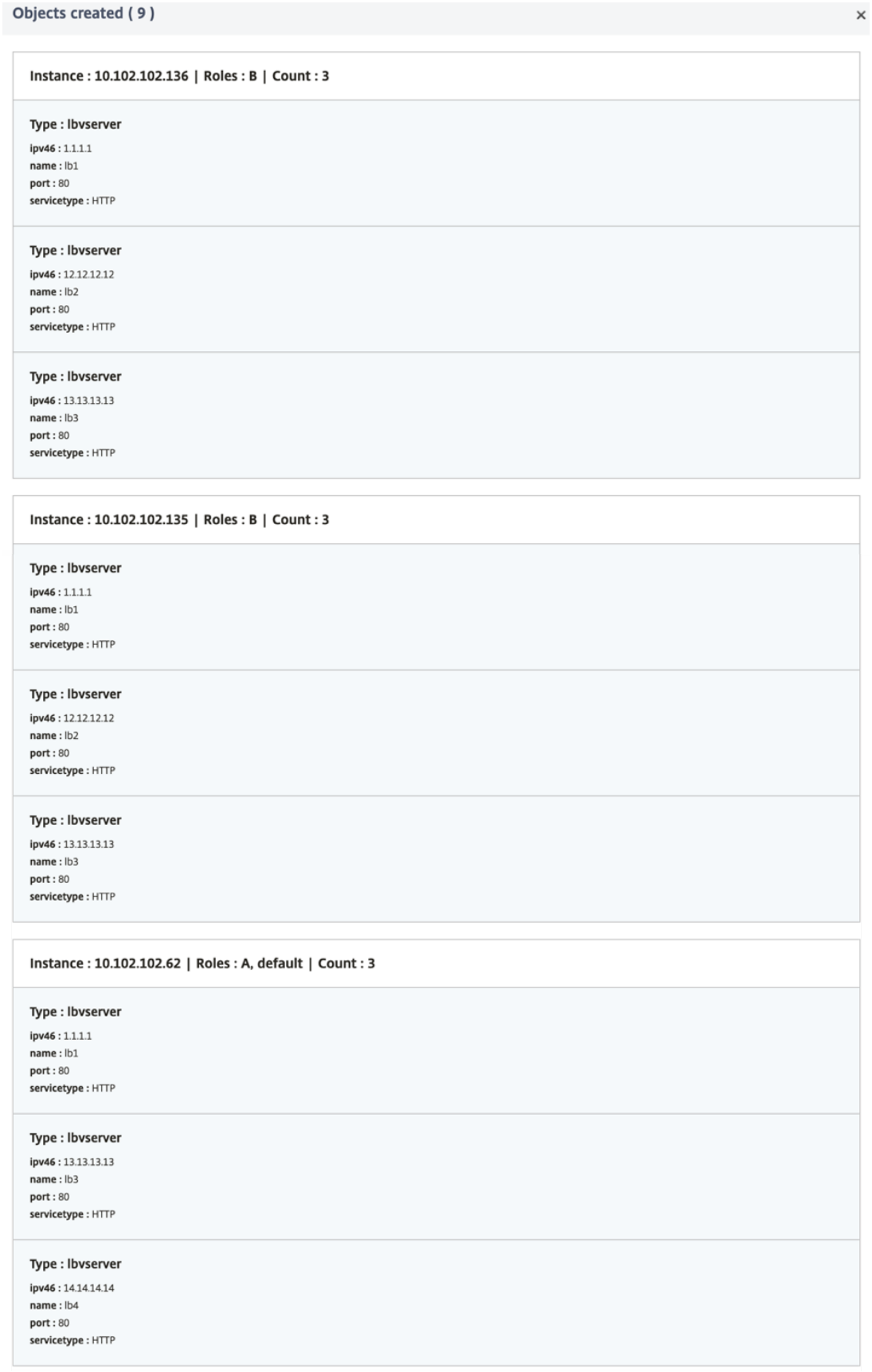
样书“演示目标角色”的全部内容如下：

```
---
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:
  -
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
```



```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

下图显示了为示例配置包创建的对象：



使用 **API**

使用 REST API 时，可以在创建或更新配置包时为每个 ADC 实例指定角色，如下所示。在“目标”块中，指定要在其上部署单个组件的特定 Citrix ADC 实例的 UUID。

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

我们提供了一个完整的示例 REST API 供您参考。

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"]
         }
```



```
 ,
        {

          "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
          "roles": ["default"]
         }

       ]
      }

 }

<!--NeedCopy-->
```

创建样书以执行非 **CRUD** 操作

February 6, 2024

样本通过计算 Citrix ADC 实例上的必要配置对象来管理 Citrix ADC 配置。每次创建或更新 ConfigPack 时，都会在实例中添加、更新或删除这些对象。这是当您指定“所需的状态”时的情况。

但是，某些 Citrix ADC 配置对象支持除创建、更新或删除（CRUD 操作）之外的一些操作。例如，负载平衡器对象 (lbvserver) 或 Citrix ADC 功能对象 (nsfeature) 可以支持“启用”或“禁用”操作。同样，Citrix ADC 证书密钥支持“链接”和“取消链接”操作，将证书链接或取消与另一个证书的链接。对 Citrix ADC 对象的这些操作称为非 CRUD 操作。本节介绍如何使用样书对支持它们的配置对象执行非 CRUD 操作。

> 注意
>
> 配置对象之间的绑定（例如，将证书密钥绑定到 lbvserver）不被视为非 CRUD 操作。这是因为 Nitro 绑定本身就被表示为配置对象。创建和删除这些对象与任何其他 Citrix ADC 配置对象一样。

支持非 **CRUD** 操作

组件中添加了一个名为“元属性”的新结构，其级别与“属性”构造相同。此结构当前支持的唯一属性称为“action”此属性可以采用该配置对象支持的“启用”或“禁用”等值。

```
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
<!--NeedCopy-->
```

在上面的示例中，“my-lbvserver-comp”组件的类型为“ns:: lbvserver”。“ns”是指您在“import-stylebooks”部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀。“lbvserver”是这个命名空间中的 NITRO 资源。作为隐式操作，lbvserver 首先由样书创建；然后对其执行“启用”操作。

元属性中指定的操作仅在创建 ConfigPack 期间对配置对象执行。对 ConfigPack 的更新不执行非 CRUD 操作。

> ** 注
>
> 意 ** 操作属性的值不能是动态评估的样本表达式。

使用 **API** 从样书创建配置

February 6, 2024

构建样本后，您必须将其导入到 Citrix Application Delivery Management (ADM)，以便使用 Citrix ADM 或 Citrix ADM API 来使用样本。Citrix ADM 会在您导入样书时对其进行验证，如果验证成功，您的样书将出现在 Citrix ADM 样书目录中，随时可以用于创建配置。

现在可以使用样书 API 基于此样书创建配置。您可以使用任何工具（如 curl 命令行工具或邮差 Chrome 浏览器扩展）将 HTTP 请求发送到 Citrix ADM。

示例 **1**

考虑您在样书中创建的“lb-vserver”样书，用于创建负载平衡虚拟服务器。使用 REST API 从此样本创建配置包，如下所示：

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
    example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {
```



```
9
10        "name": "lb1",
11        "ip": "10.102.117.31"
12       }
13  ,
14     "target_devices":
15     [
16       {
17
18         "id": "deecee30-f478-4446-9741-a85041903410"
19        }
20
21     ]
22  }
23
24  }
25
26  <!--NeedCopy-->
```

在此 HTTP 请求中，ID（例如 deecee30-f478-4446-9741-a85041903410）是在其中创建 IP 地址为 10.102.117.31 的负载平衡虚拟服务器 lb1 的 Citrix ADC 实例的实例 ID。Citrix ADC 实例的实例 ID 是从 Citrix ADM 中检索的。

要获取由 Citrix ADM 管理的实例的 ID，可以使用 Citrix ADM API。例如，要检索 IP 地址为 192.168.153.160 的 Citrix ADC 实例的实例 ID，您可以使用以下 API：

```
1  GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
       :192.168.153.160
2  <!--NeedCopy-->
```

```
1  Accept: application/json
2  <!--NeedCopy-->
```

在有效负载中，响应包含 ID：

```
1  200
2  OK
3  Content-Type: application/json
4  {
5
6    "errorcode": 0,
7    "message": "Done",
8    "operation": "get",
9    "resourceType": "ns",
10   "username": "nsroot",
11   "tenant_name": "Owner",
12   "resourceName": "",
13   "ns":
14   [
15     {
16
17     "is_grace": "false",
18     "hostname": "",
19     "std_bw_config": "0",
```



```
    "gateway_deployment": "false",
    ···"id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

如果配置（配置包）已成功创建，您将收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

您已经创建了第一个使用 ID 1460806080 进行唯一标识的配置（配置包）。可以使用此 ID 查询、更新或删除该配置。

示例 **2**

您可以使用同一样本创建另一个配置或配置包，并在相同或不同的 Citrix ADC 实例上执行它。在此示例中，创建另一个配置并为虚拟服务器提供不同的名称和 IP 地址，另外还指定 LEASTCONNECTION 作为负载平衡方法。在两个 Citrix ADC 实例上部署此配置。

HTTP 请求如下：

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {
```



```
10
11        "name": "lb2",
12        "ip": "10.102.117.32",
13        "lb-alg": "LEASTCONNECTION"
14       }
15  ,
16     "target_devices"
17     [
18      {
19  "id": "deecee30-f478-4446-9741-a85041903410" }
20  ,
21      {
22  "id": "debecc60-d589-4557-8632-a74032802412" }
23
24     ]
25    }
26
27  }
28
29  <!--NeedCopy-->
```

在此 HTTP 请求中，在由 ID deecee30-f478-4446-9741-a85041903410 和 debecc60-d589-4557-8632-a74032802412 表示的两个 Citrix ADC 实例上创建 IP 地址为 10.102.117.32 的负载平衡虚拟服务器 lb2。

成功创建配置包后，会收到以下 HTTP 响应：

```
1  200 OK
2  Content-Type: application/json
3  {
4
5     "configpack":
6    {
7
8       "config_id": "1657696292"
9     }
10
11   }
12
13 <!--NeedCopy-->
```

这个新的配置包有一个不同的 ID 165769629。您可以通过使用此 ID 更新或删除此配置。

示例 **3**

考虑在用于创建基本负载平衡配置的样书中创建的 “basic-lb-config” 样书。使用 REST API 从此样本创建配置包，如下所示：

```
1  POST
2
3  http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
       .stylebooks/0.1/basic-lb-config/configpacks
```



```
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers":
      ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "target_devices":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

    ]
   }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，负载平衡配置在两个 Citrix ADC 实例上执行。您可以登录到这些 Citrix ADC 实例，以验证是否创建了绑定了两个服务的虚拟服务器和服务组。

示例 **4**

考虑在创建复合样书中创建的复合样书 **composite-example**。使用 REST API 从此样本创建配置包，如下所示：

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
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"]
     }
 ,
    "target_devices":
    [
    {

      "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
    {

      "id": "debecc60-d589-4557-8632-a74032802412"
     }

    ]
  }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，将在两个由其 ID 表示的 Citrix ADC 实例上创建配置。如果您登录到 Citrix ADC 实例，则可以查看导入到“复合示例”样本中的“基本 lb-config”样本创建的配置对象。您还可以看到名为“myapp-mon”的新 HTTP 监视器，它属于“composite-example”样书的一部分。

成功创建配置包后，会收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```


更新配置

要更新此配置，例如，通过将 IP 地址 10.102.29.54 的新后端服务器添加到负载平衡虚拟服务器 myapp 中，请使用 API 更新配置包，如下所示：

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
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"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
   }

]
 }

 }

<!--NeedCopy-->
```

在成功更新配置包时，会收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

```



```
 }

<!--NeedCopy-->
```

删除配置

要删除此配置（从所有 Citrix ADC 实例中），可以使用 API 删除配置包，如下所示：

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

成功删除配置包后，会收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

您可以登录到 Citrix ADC 实例并验证是否已删除此配置包中的所有配置对象。

如果要从特定 Citrix ADC 实例而不是从所有实例中删除配置，请使用上述更新配置包操作，并在 JSON 有效负载中更改“target t_devices”属性以删除特定的 Citrix ADC 实例 ID。

使用 **API** 创建配置以上载证书和密钥文件

February 6, 2024

可使用样本 API 基于此样本创建配置。您可以使用任何工具（如 curl 命令行工具或 Postman Chrome 浏览器扩展）将 HTTP 请求发送到 Citrix Application Delivery Management (ADM)。

考虑在 如何创建用于将 SSL 证书和证书密钥文件上载到 Citrix ADM 的样书中为上载证书和密钥文件而创建的样书示例。使用 REST API 从此样本创建配置包，如下所示：

```
POST
```



```
https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
<!--NeedCopy-->
```

```
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",
                   "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"
        }

    ]
   }

}

<!--NeedCopy-->
```

此配置包是通过使用 id 8c158e7a-0087-423f-91b0-0ccf16de552a 的唯一标识的。可以使用此 ID 查询、更新或删除该配置。成功更新配置包后，证书和密钥文件将上载到 Citrix ADM 文件系统。

使用 **API** 创建配置以上载任何文件类型

February 6, 2024

您还可以使用 Citrix Application Delivery Management (ADM) API 来创建用于将文件上载到选定的 Citrix ADC 实例的配置包。

请考虑如何创建样本以将文件上载到 Citrix ADC MA 服务中为上载任何类型的文件而创建的样书示例。如上述主题中的示例所示，创建配置包并将参数“位置文件”的值指定为 Citrix ADM 上位置文件的文件路径。
使用 REST API 从此样书创建配置包，如下所示：

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
   stylebooks.samples/1.0/upload-geolocations/configpacks
```



```
<!--NeedCopy-->
```

```
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"
         }

     ]
   }

 }

<!--NeedCopy-->
```

使用 **API** 导入自定义样书

February 6, 2024

您现在可以使用样本 API 将自定义样本导入到 Citrix Application Delivery Management (ADM) 中。使用 REST API 在任何工具（如 curl 命令行工具或 Postman Chrome 浏览器扩展）中创建此样本的配置包，如下所示。例如，您可以导入名为 exam-lb 的样书，该样书可用于在 Citrix ADC 实例上创建负载平衡器配置。

```
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"
    }

 }

<!--NeedCopy-->
```

其中，“来源”属性的值是样书文件内容的 base64 编码。例如，您可以将样书文件的 YAML 内容粘贴到在线工具（例如 https://www.browserling.com/tools/file-to-base64）中以获取 base64 字符串，然后将其用作上述“源”属性的值。

使用此 API 调用，您还可以在一个 API 操作中上载包含多个样书文件的压缩 tarball 文件（.tgz 文件）。为此，只需将 file_name 属性更改为.tgz 文件名，将源属性的值更改为.tgz 文件内容的 base64 编码即可。

在工具中成功运行 API 后，您会收到以下响应，指示样书已导入 Citrix ADM。

```
200 OK
<!--NeedCopy-->
```

响应正文：

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


 }

<!--NeedCopy-->
```

使用 **API** 下载自定义样书

February 6, 2024

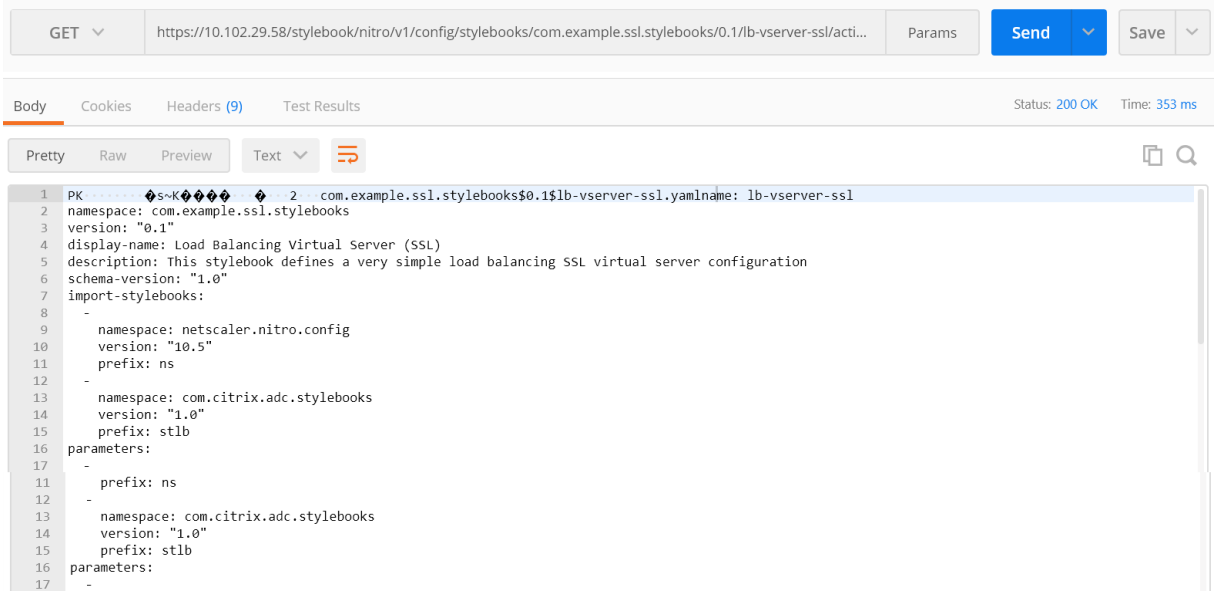
您可以通过提供以下样书 REST API 来下载自定义样书：


```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

修改 IP 地址、名称、版本和命名空间字段后，您可以在 curl 命令行工具或 Postman chrome 浏览器扩展程序等任何工具中运行 API。

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
    ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

将下载.yaml 格式的样本。



使用 **API** 删除自定义样书

February 6, 2024

您可以通过提供以下样书 REST API 来删除自定义样书：

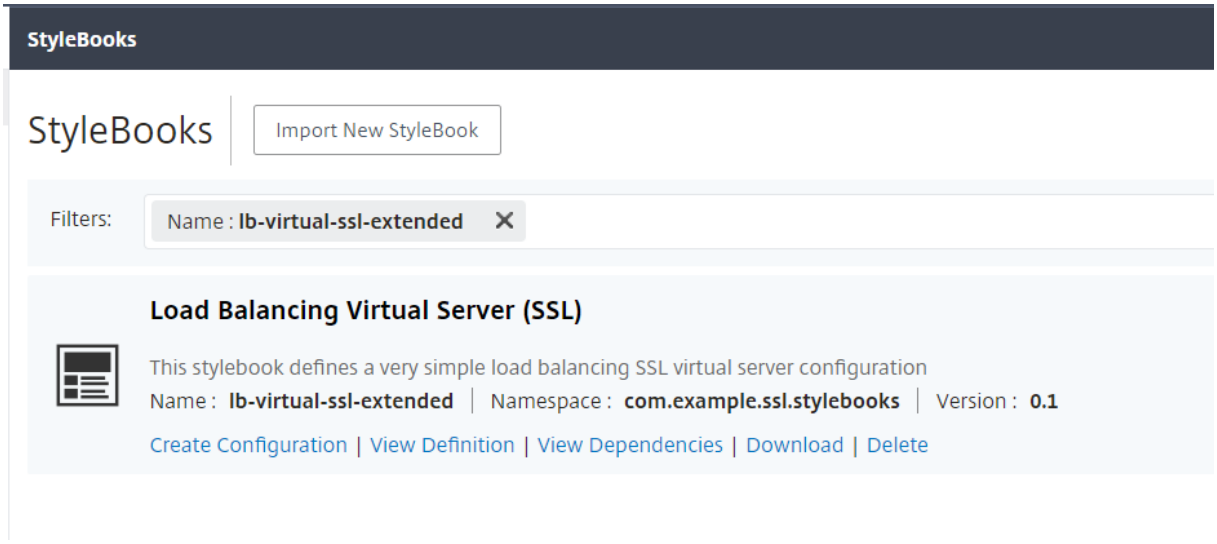
```
DELETE

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

如果未提供 URL 中的依赖关系查询参数或将其值设置为 false，则不会删除样书依赖关系（仅删除样书本身）。

当您收到的 HTTP 响应状态代码为 200 时，这意味着自定义样书（及其依赖关系）已从 Citrix ADM 中成功删除。

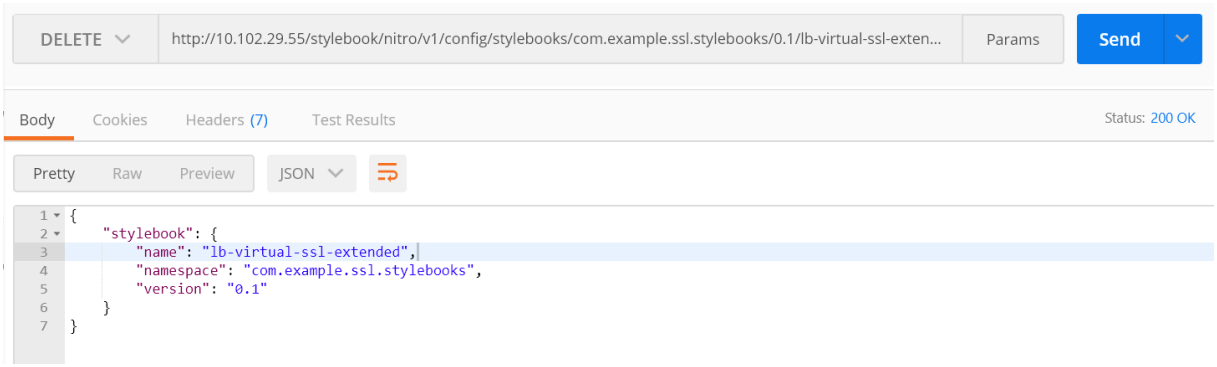
> 注意
>
> 您不能删除具有其他样书的 MA 服务中依赖于它的自定义样书。

例如，假设您在 Citrix ADM 中创建了一本名为“lb-virtual-ssl-extended”的样书。您后来决定删除该样书。

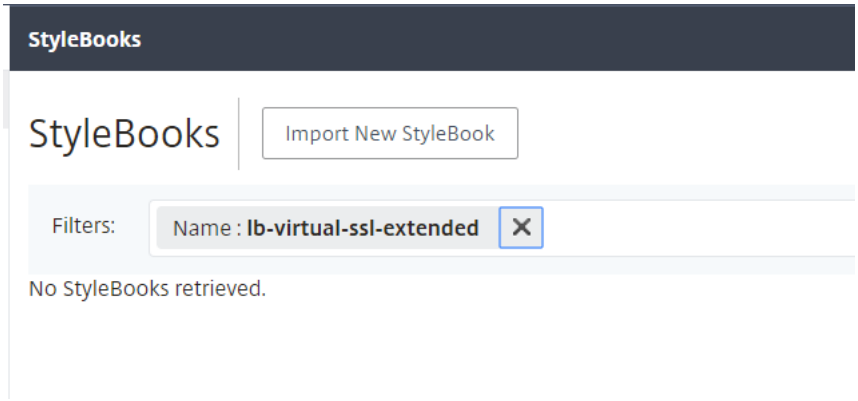


修改 IP 地址、名称、版本和命名空间字段后，您可以在 curl 命令行工具或 Postman chrome 浏览器扩展程序等任何工具中运行 API。

删除https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



样本将从 Citrix ADM 中删除。



样书语法

February 6, 2024

您可以设计自己的样本，将其导入到 Citrix Application Delivery Management (ADM)，然后使用它们通过使用 Citrix ADM GUI 或使用 API 创建配置。为了能够创建您自己的样书，必须先了解您可以使用的不同构造和属性的语法和句法。

本文档介绍了创建样书时可以使用的不同构造和引用。

单击下表中的部分、构造或引用名称可查看详细信息。

–	–
[Header](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/header-section.html)	[导 入 样 书](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/import-stylebooks-section.html)
[Parameters](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-section.html)	[参 数-默 认 源 代 码 构 造](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameters-default-sources-construct.html)
[Substitutions](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions.html)	[Components](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components.html)
[可选属性](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/optional-properties.html)	[帮助程序组件](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/helper-components.html)
[属性默认来源](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/properties-default-sources.html)	[嵌 套 组 件](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-components.html)

[条件构造](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/condition-construct.html)	[重复构造](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-construct.html)
[重复条件构造](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/repeat-condition-construct.html)	[Outputs](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/outputs.html)
[嵌套重复](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/nested-repeats.html)	[父级引用](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parent-reference.html)
[参数引用](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/parameter-reference.html)	[替换引用](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/substitutions-reference.html)
[组件引用](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/components-reference.html)	[Operations](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/operations.html)
[变量引用](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/variable-reference.html)	[Alarms](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/alarms.html)
[Analytics](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/analytics.html)	[内置函数](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/built-in-functions.html)
[Expressions](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/expressions.html)	[依赖性检测](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/stylebooks-grammar/dependency-detection.html)
就地插值

> 注意
>
> 在为替换函数定义重复项、重复索引或参数时，不要使用以下保留字来命名用户定义的变量 $<var-name>
>
> - stylebook、parameters、substitutions、components、properties、outputs、parent、self、operations、analytics、alarms
> - repeat-item、repeat-item-0、repeat-item-1、repeat-item-2
> - repeat-index、repeat-index-0、repeat-index-1、repeat-index-2
> - default
> - roles、role、targets、target
> - context、parent-context、parent_context

有关如何设计您自己的样书的信息和示例，请参阅如何创建您自己的样书。

标题

February 6, 2024

样本的前六行构成标头部分。此部分用于定义样本的标识，以及介绍它做什么。这是必需的部分。

下表介绍标头部分的属性：

属性	解吸
–	–
name	用于标识样书的名称。此属性是必需的。
description	定义样书做什么的说明。此描述显示在 Citrix ADM GUI 上。这是可选属性。
display-name	样书的描述性名称。这个名字出现在 Citrix ADM GUI 上。这是可选属性。
author	创建样书的作者个人或组织。这是可选属性。
namespace	命名空间构成样本的唯一标识符的一部分，以避免发生名称冲突。命名空间可以是任何字符串，但良好的做法是用它来表示创建和拥有一组样书的公司、部门或单位。例如，您可以使用以下格式：<company>.<department>.<unit>.stylebooks。这是必需属性。
version	样本的版本号。可以在更新样本时更改版本号。不同版本的样书可以共存在一起。这是必需属性。
schema-version	样书架构的版本。在当前版本的 Citrix ADM 中，它的值为“1.0”。这是必需属性。
private	如果将此属性设置为 true，则样书不会显示在 Citrix ADM GUI 上。对于构建用于其他样书的块且不打算由用户直接使用的样书，这是很有用的设置。这是可选属性。其默认值为 false。

示例：

```
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
6      schema-version: "1.0"
7      version: "0.1"
8  <!--NeedCopy-->
```

name、namespace 和 version 组合在系统中唯一标识样书。在 Citrix ADM 中不能有两本具有相同名称、命名空间和版本组合的样书。但可以有两个 name 和 version 相同但 namespace 不同或 namespace 和 version 相同但 name 不同的样书。

导入样书

February 6, 2024

这是样本的第二个部分，在此部分可以声明要在当前样本中引用哪个其他样本。这样可以导入并重用其他样本，而不是在您自己的样本中重新构建相同的配置。这是必需的部分。

必须在当前样书中声明要引用的样书的 **namespace** 和 **version** 号。直接使用任何一个 NITRO 配置对象的每个样书都必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 Citrix ADC NITRO 类型，例如 lbvserver 服务或监视器。支持 Citrix ADC 10.5 及更高版本的样本，这意味着您可以使用样本在运行 10.5 或更高版本的任何 Citrix ADC 实例上创建和运行配置。

import-stylebooks 部分中使用的 **prefix** 属性是指代命名空间和版本组合的简写。例如，“ns”前缀可以用于指代命名空间 netscaler.nitro.config 和版本 10.5。在样书的后面部分中，不必每次要引用具有此命名空间和版本的样书时使用命名空间和版本，只需将所选前缀字符串与样书名称一起使用即可唯一标识它。

示例：

```
      import-stylebooks:
       -
         namespace: netscaler.nitro.config
         version: "10.5"
         prefix: ns
      -
       namespace: com.acme.stylebooks
        version: "0.1"
        prefix: stlb
<!--NeedCopy-->
```

在上述示例中，定义的第一个前缀名为 ns，它指代命名空间 netscaler.nitro.config 和版本 10.5。定义的第二个前缀名为 stlb，它指代命名空间 com.acme. 样书和版本 0.1。

定义了前缀后，每次要引用属于一个特定命名空间和版本的类型或样书时，可以使用表示法 **<namespace-shorthand>::<type-name>**。例如，**ns::lbvserver** 指代在命名空间 netscaler.nitro.config（版本 10.5）中定义的类型 lbvserver。

同样，如果要引用 com.acme. 样书命名空间中版本为“0.1”的样书，可以使用表示法 **stlb::< 样书-name>**。样书-name>

> 注意
>
> 按照惯例，前缀“ns”用于指 Citrix ADC 的 NITRO 命名空间。

参数

February 6, 2024

在此部分可以定义样本中用于创建配置所需的所有参数。它描述样本接收的输入。尽管这是一个可选部分，但大多数样书可能需要一个。您可以考虑参数部分来定义希望用户在使用样本在 Citrix ADC 实例上创建配置时回答的问题。

当您将样本导入 Citrix ADM 并使用它创建配置时，GUI 会使用样本的此部分显示一个表单，该表单接收已定义的参数值的输入。

以下部分介绍了需要为本节中的每个参数指定的属性：

name

要定义的参数的名称。可以指定字母数字名称。

名称必须以字母开头，可以包括其他字母、数字、连字符 (-) 或下划线 (_)。

请注意，编写样书时，可以通过采用表示法 $parameters.<name> 使用此 “name” 属性在其他部分中引用该参数。

强制性？是

label

在 ADM GUI 中显示为此参数的名称的字符串。

强制性？否

description

说明参数用途的帮助字符串。当用户单击此参数的帮助图标时，ADM GUI 会显示此文本。

强制性？否

type

这些参数可以接收的值类型。参数可以是以
下内置类型之一：

- string：字符数组。如果未指定长度，则字符串值可以接收任何数量的字符。但是，可以使用 min-length 和 max-length 属性限制字符串类型的长度。
- number：整数数字。可以使用 min-value 和 max-value 属性指定此类型可以接收的最小数和最大数。
- boolean：可以为 true 或 false。另外请注意，所有文字都被 YAML 视为布尔值（例如 Yes 或 No）。
- ipaddress：表示有效的 IPv4 或 IPv6 地址的字符串。
- tcp-port：表示 TCP 或 UDP 端口的 0 到 65535 之间的数字。
- password：表示不透明/机密字符串值。当 Citrix ADM GUI 显示此参数的值时，它将显示为星号 (*****)。

- certfile：表示证书文件。这允许您在使用 ADM GUI 创建样书配置时直接从本地系统上载文件。上载的证书文件存储在 /var/mps/tenants/ 目录中 ADM 中的 /ns_ssl_certs。

  证书文件将被添加到 ADM 管理的证书列表中。

- keyfile：表示证书密钥文件。这允许您在使用 Citrix ADM GUI 创建样书配置时直接从本地系统上载文件。上载的证书文件存储在 /var/mps/tenants/ 目录中 Citrix ADM 中的 /ns_ssl_keys。

  证书密钥文件将添加到 Citrix ADM 管理的证书密钥列表中。

- file：表示文件。
- object：要将多个相关参数分组在一个父元素下时使用此类型。必须将父参数的类型指定为“object”。类型为“object”的参数可以有嵌套的“parameters”部分以描述其包含的参数。
- 另一个样本：当您使用此类型的参数时，此参数期望其值采用样本中定义的参数的形式，表示其类型。

通过在类型末尾添加“[]”，参
数的类型也可以是上面列出的任何类型的列表。例如，如果 type 属性是 string []，则此
参数将字符串列表作为输入。在从此样本创建配置时，您可以为
此参数提供一个、两个或多个字符串。

强制性？是

key

指定 true 或 false 指示此参数是否是样本的主要参数。

样书只能有一个定义为“key”参数的参数。

当您从同一样书（在相同或不同的 Citrix ADC 实例上）创建不同的配置时，每个配置对此
参数具有不同/唯一值。

默认值为 false。

强制性？否

必需

指定 true 或 false 指示参数是必需的还是可选的。如果
设置为 true，则该参数是必需的，用户在创建配置时必须为此
参数提供值。

Citrix ADM GUI 强制用户为此参数提供有效值。

默认值为 false。

强制性？否

> 注意：
>
> 如果参数具有 `type: object` 和 `required: false`，则不计算此参数的子参数。

如果希望子参数的默认值生效，请按如下方式为主参数设置 `required: true`：

```
    type: object
    required: true
    gui:
      collapse_pane: true
<!--NeedCopy-->
```

折叠 se_pane 属性显示对象及其子参数在 UI 中折叠，除非用户展开窗格。

allowed-values

类型设置为“string”时，此属性用于定义参数的有效值列表。

从 Citrix ADM GUI 创建配置时，系统会提示用户从此列表中选择一个参数值。

示例 **1**：

name：ipaddress

type：string

预定值：

- SOURCEIP
- 最重要的 IP
- NONE（无）

示例 **2**：

name: TCP Port

type：tcp-port

预定值：

- 80
- 81
- 8080

示例 **3**：

(tcp-port 列表，其中列表的每个元素只能在允许值中
指定值)

name: tcpports

type: tcp-port[]

预定值：

- 80
- 81
- 8080
- 8081

强制性？否

default

此属性用于为可选参数指定默认值。在创建配
置时，如果用户未指定值，则使用默认值。

从 Citrix ADM GUI 创建配置时，如果用户没有为没有默认值的参数
提供值，则不会
为该参数设置任何值。

示例 **1**：

name: timeout

type: number

def ault: 20

示例 **2**：

（其中，参数的默认值是值列表）：

name: protocols

type: string[]

默认值：

- TCP
- UDP
- IP

示例 **3**：

name: timeout

type: number

default: 20

示例 **4**：

name: tcpport

type：tcp-port

default: 20

强制性？否

pattern

当参数的类型为“string 时，使用此属性定义此
参数的有效值的模式（正则表达式）。

示例：

name: appname

type: string

pattern: “[a-z]+”

强制性？否

min-value

此属性用于定义类型为“number”或“tcp-port”的参数的最小值。

示例：

name: audio-port

type: tcp-port

min-value: 5000

数字的最小值可以为负，但 tcp 端口的最小值不应为
负值。

强制性？否

max-value

使用此属性定义类型为“数字”或
“tcp 端口”的参数的最大值。

如果已定义，最大值应大于最小值。

示例：

name: audio-port

type: tcp-port

min-value: 5000

max-value: 15000

强制性？否

min-length

使用此属性可定义
类型为“string”的参数所接受的值的最小长度。

定义为值的字符的最小长度应大于或
等于零。

示例：

name: appname

type: string

min-length: 3

强制性？否

max-length

使用此属性可以定义
类型为“string 的参数所接受的值的最大长度。

值的最大长度应大于或等于以最小长
度定义的字符长度。

示例：

name: appname

type: string

max-length: 64

强制性？否

min-items

使用此属性定义列表参数中的最小项目
数。

最小项目数应大于或等于零。

示例：

name: server-ips

type: ipaddress[]

min-items: 2

强制性？否

max-items

使用此属性可定义作为
列表的参数中的最大项数。

如果已定义，最大项目数应大于最小项目数。

示例：

name: server-ips

type: ipaddress[]

min-items: 2

max-items: 250

强制性？否

gui

使用此属性在 Citrix ADM GUI 中自定义“对象”类型的
参数的布局。

强制性？否

columns

这是 gui 属性的子属性。使用它来定义要在 Citrix ADM GUI
中显示的列数。

强制性？否

updatable

这是 gui 属性的子属性。使用此选项指定是否
可以在创建配置后更新参数。

如果值设置为 false，则更新配置时参数字段灰显。

强制性? 否

collapse_pane

这是 gui 属性的子属性。使用此选项可指定定
义此对象参数布局的窗格是否可折叠。

如果值设置为 true，则用户可以展开或折叠此父参数下方的子参数。

示例：

```
    gui:

     collapse_pane: true

     columns: 2

     updatable: false
<!--NeedCopy-->
```

完整的 parameters 部分示例：

```
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

```



```
23          type: ipaddress
24
25          required: true
26
27       -
28
29          name: svc-servers
30
31          label: Servers
32
33          type: object[]
34
35          required: true
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
88  <!--NeedCopy-->
```

下面的示例定义前面的部分中说明的所有列表属性和值：

“‘YAML
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

参数-默认源代码构造

February 6, 2024

可以使用此构造来重用其他样书中的参数定义。

假设这样一个场景：一个参数或一组参数在多个样本中重复使用。为了避免重新定义这些参数，每次要创建新样书时，可以将其定义一次，然后使用 **parameters-default-sources** 构造将其定义导入需要这些参数的样书。

例如，如果多个样书需要配置虚拟 IP，可能必须在创建的每个新样书中定义与虚拟 IP 有关的相同参数。但是可以创建一个单独的样书（例如，名为“vip-params”），在其中定义与其有关的所有参数，如以下示例中所示：

```
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
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
38  <!--NeedCopy-->
```

之后可以创建利用这些参数的其他样书。下面是这样一个样本示例。

```
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
```



```
      schema-version: "1.0"
      import-stylebooks:
        -
          namespace: com.acme.commontypes
          prefix: cmtypes
          version: "1.0"
      parameters-default-sources:
            - cmtypes::vip-params
      parameters:
          -
            name: monitorname
            label: Monitor Name
            description: Name of the monitor
            type: string
            required: true
          -
            name: type
            label: Monitor Type
            description: Type of the monitor
            type: string
            required: true
            allowed-values:
              - PING
              - TCP
              - HTTP
              - HTTP-ECV
              - TCP-ECV
              - HTTP-INLINE
<!--NeedCopy-->
```

在 acme-biz-app 样书中，首先通过使用“import-样书”部分导入 vip-params 样书的命名空间和版本。然后添加 **parameters-default-sources** 构造，并指定样书名称，即 vip-params。这与在此样本中直接定义 vip-params 样本的参数效果一样。

由于 parameters-default-sources 是一个列表，且列表中的每个项目都需要是一个样书，因此可以包括多个样书中的参数。

除了包括其他样本中的参数外，还可以使用 parameters 部分定义您自己的参数。样本的完整参数列表是从其他样本中添加的参数和此样本中定义的参数的组合。因此，表达式 **$parameters** 是指此参数组合。

请注意，如果一个参数在导入的样本和当前样本中都定义了，则当前样本中的定义覆盖从其他样本导入的定义。可以在需要时自定义一些导入参数，同时按原样使用其余导入参数，有效利用这一点。

parameters-default-sources 构造还可以用于嵌套的参数中，如下所示：

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
```



```
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```

这与在此样书中将 vip-params 样书的参数直接作为 vip-details 参数的子参数添加类似。

substitutions

February 6, 2024

substitutions 部分用于定义可在样本其余部分使用的复杂表达式的简写名称，以使样本更加清晰。在样本中多次重复使用相同表达式或值（例如，一个常数值）时，它们也很有用。通过为此值使用替换名称，您可以在需要更改此值时只更新替换值，而不是在样本中出现的每一处更新它（这很容易出错）。

替换还用于定义值之间的映射，如本文档中后面的示例中所述。

列表中的每个替换都由一个关键字和一个值组成。值可以是简单值、表达式、函数或映射。

在以下示例中，定义了两个替换。第一个替换是可以用作 8181 的简写名称的“http-port”。通过使用替换，可以在样书的其余部分以 **$substitutions.http-port** 引用它，而不是使用 8181。

替换：

http-port: 8181

这让您可以为端口号指定助记名称，并在样书中的一个地方定义此端口号，无论它被使用多少次。如果要将端口号修改为 8080，可以在替换部分修改它，该更改将在使用助记名称 http-port 的任何位置生效。以下示例说明了如何在组件中使用替换。

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

替换也可以是复杂的表达式。以下示例说明了两个替换如何使用表达式。

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

替换表达式还可以使用现有替换表达式，如以下示例中所示。


```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
    port) + str("-app")
<!--NeedCopy-->
```

替换的另一个有用功能是映射，即可以将关键字映射到值。下面是一个映射替换示例。

```
substitutions:
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

以下示例说明了如何使用映射 secure-port 和 secure-protocol。

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: \*\*$substitutions.secure-protocol[$parameters.
    is-secure]\*\*
          ipv46: $parameters.ip
          port: \*\*$substitutions.secure-port[$parameters.is-secure
    ]\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

这意味着，如果样书的用户将参数 is-secure 的布尔值指定为“真”，或者在 Citrix ADM GUI 中选中与该参数对应的复选框，则会为该组件的服务类型属性分配 值 **SSL**，并将端口属性的值 分配为 **443**。但是，如果用户为此参数指定“假”或清除 Citrix ADM GUI 中的相应复选框，则会为服务类型属性分配 值 **HTTP**，并将端口的值 分配为 **80**。

以下示例说明了如何将替换用作函数。替换函数可以接受一个或多个参数。参数应属于简单类型，例如，字符串、数字、IP 地址、布尔值和其他类型。

替换：

form-lb-name(name): $name + “-lb”

在此示例中，我们定义了一个替换函数“form-lb-name”，它接受一个名为“name”的字 ** 符串参数，并使用它来创建一个新字符串，该字符串在名称参数中为该字符串添加后缀“-lb”。使用此替换函数的表达式可以编写如下：

$substitutions.form-lb-name(“my”)

此表达式返回“my-lb”

看看另外一个示例：

替换：

cspol-priority(priority): 10100 - 100 * $priority

替换 cspol-priority 是一个函数，它接收名为 priority 的参数，并使用它来计算值。在样书的其余部分，可以使用此替换，如以下示例中所示：

```
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)
<!--NeedCopy-->
```

替换也可以由键和值组成。值可以是简单值、表达式、函数、映射、列表或字典。

以下是名为“slist”的替换示例，其值为列表：

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

替换的值还可以是键值对字典，如以下示例中所示，这是名为“sdict”的替换：

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

您可以组合列表和字典来创建更加复杂的属性。例如，一个名为“slistofdict”的替换返回键值对列表。

```
  slistofdict:
    -
      a: $parameters.cs1.lb1.port
      b: $parameters.cs1.lb2.port
    -
      a: $parameters.cs2.lb1.port
      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

但是，在以下示例中，名为“sdictoflist”的替换返回一个键值对，其中值本身是另一个列表。

```
  sdictoflist:
```



```
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```

在组件中，这些替换可以用于 condition、properties、repeat、repeat-condition 构造中。

以下组件示例显示了如何使用替换指定属性：

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

定义其值是列表或字典的替换的用例是当您配置一个内容交换虚拟服务器和多个负载平衡虚拟服务器时。由于绑定到同一 cs 虚拟服务器的所有 lb 虚拟服务器可能有相同的配置，因此，您可以使用替换列表和字典来构建此配置以避免对每个 lb 虚拟服务器重复使用该配置。

以下示例显示 cs-lb-mon 样本中用于创建内容交换虚拟服务器配置的替换和组件。构建 cs-lb-mon 样本的属性时，复杂的替换“lb-properties”指定与 cs 虚拟服务器关联的 lb 虚拟服务器的属性。“lb-properties”替换是一个函数，接受名称、服务类型、虚拟 IP 地址、端口和服务器作为参数，并生成键值对作为值。在“cs-pools”组件中，我们将此替换的值指定给每个池的 lb-pool 参数。

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    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
39 <!--NeedCopy-->
```

替代映射：

您可以创建将键映射到值的替换。例如，假设这样一个场景：您想要定义要用于每个协议（键）的默认端口（值）。对于此任务，按如下所示编写替换映射。

```
1 substitutions:
2      port:
3           HTTP: 80
4           DNS: 53
5           SSL: 443
6 <!--NeedCopy-->
```

在此示例中，HTTP 映射到 80，DNS 映射到 53，SSL 映射到 443。要检索作为参数提供的特定协议的端口，请使用表达式

$substitutions.port[$parameters.protocol]

该表达式根据用户指定的协议返回值。

- 如果键为 HTTP，则表达式返回 80
- 如果键为 DNS，则表达式返回 53
- 如果键为 SSL，则表达式返回 443
- 如果映射中没有键，则该表达式不返回任何值

组件

February 6, 2024

样本中的 components 构造被视为样本中最重要的部分。在此部分，定义必须要创建的配置对象。通过使用此构造，可以构建相同类型的一个或多个配置对象。

components 构造使用 parameters 部分中提供的输入来改写样本生成的配置。这是一个可选部分，尽管大多数样本都有一个 components 部分。

下表介绍了组件的主要属性。

属性	说明
–	–
name	组件的名称。可以指定字母数字名称。名称必须以字母开头，可以包括其他字母、数字、连字符 (-) 或下划线 (_)。
description	样书中此组件的角色的说明。
type	类型确定此组件提供哪些属性。组件有两种类型：** 内置 ** 类型：这种类型由系统提供，您不必对其进行定义，例如，NITRO 实体类型 “lbvserver” 或 “servicegroup”。当组件具有内置类型属性时，它会在 Citrix ADC 上创建该类型的配置对象。例如，如果某个组件引用内置类型 “lbvserver”，则该组件会在作为配置目标的 Citrix ADC 实例上创建一个负载平衡虚拟服务器。** 复合类型 **：此类型指您创建并导入 Citrix ADM 的现有样书。当组件具有复合类型属性时，它会在作为配置目标的 Citrix ADC 实例上创建所有配置对象，这些对象在引用的样书中指定。这让您可以组合多个样书，其中每个样书创建最终配置的一部分。有关复合样书的详细信息，请参阅 [创建复合样书](/zh-cn/netscaler-application-delivery-management-software/12-1/stylebooks/how-to-create-custom-stylebooks)。
properties	可以用于组件类型属性的子属性。组件的有效属性由其类型决定。对于内置类型，有效属性是对应的 Nitro 对象的属性。对于其类型是另一个样书的组件（即复合类型），属性对应于该样书中定义的参数。

示例：

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

在此示例中，定义了名为 my-lbvserver-comp 的组件。此组件的类型为 ns::lbvserver（内置类型），其中 “ns” 是指代在 import-样书部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀，“lbvserver” 是此命名空间中的 NITRO 资源。

此部分中的属性包括 “lbvserver” 资源的四个必需属性和一个可选属性 (lbmethod)，您可以为这些属性指定值。在此示例中，为 servicetype 和 port 指定静态值，而 name、ipv46 和 lbmethod 属性从输入参数获取其值。您可以使用 $parameters 来引用参数部分中定义的参数名称。\ <name\ > 表示法，例如 $parameters.ip。

> 注意
>
> NITRO 资源类型的属性名称（其组件属性）必须使用小写。否则，样书 导入将失败。

帮助程序组件

February 6, 2024

样书中 components 部分的主要用途是通过 Nitro 内置类型或创建实际配置对象的另一个样书来生成配置对象。帮助程序组件本身不会生成配置对象。帮助程序组件接收来自其他部分（例如，参数对象、其他组件的属性或其他组件的输出）的输入，并将其传输到其他表单中。以后，其他组件可以使用这些内容来生成实际配置对象。帮助程序组件的类型有两种：对象类型或不包含组件部分的另一个样书。

以下示例显示了样本的片段，该片段用于在 Citrix ADC 实例上创建具有监视器（lb-mon-comp）的负载平衡服务器。

```
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
<!--NeedCopy-->
```


parameters 部分允许您输入应用程序的名称和负载平衡服务器的 IP 地址。在 lb-mon-comp 组件部分中，lb-mon 样本的 svc-servers 参数要求为对象列表，其中每项都有两个子参数：ip 和 port。

但是，此样书的 parameters 部分仅通过 $parameters.ips 接受服务器 IP。该样书假定所有服务器都在端口 80 上运行。要使用 lb-mon 样本创建负载平衡配置，必须将 $parameters.ips 传输到对象列表。这是通过使用帮助程序组件（上述示例中的 help-comp）来实现的。help-comp 组件的类型为 server-ip-port-params 样本。此样书没有任何组件。因此，它不会创建任何配置对象。help-comp 基于 $parameters.ips 创建重复列表，并为 $parameters.ips 的每项构造由 ip 和 port（设置为静态 80）组成的对象。因此，help-comp 将 IP 地址列表传输到对象列表，以后可以在 lb-mon-comp 中使用该对象列表来分配 svc-servers 属性。help-comp 的结果即分配给 lb-mon-comp 的 svc-servers 属性。

可选属性

February 6, 2024

在有些情况下，组件的一个属性从一个表达式接收其值，表达式可以是简单表达式（例如参数引用），也可以是较复杂的表达式。在组件中设置此属性值是可选的。可以选择仅当表达式返回实际值时设置该属性值，否则可以选择不设置此属性。

例如，假设要设置的其中一个属性是其类型为 ns::lbvserver 的组件的 lbmethod（负载平衡算法）。属性 lbmethod 的值取自用户提供的一个参数值，如下所示：

```
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
<!--NeedCopy-->
```

现在，考虑参数 **lb-**高级 **d.** 算法 是一个可选参数。而且，如果用户没有为此参数提供值，因为该参数是可选的，则表达式 **$** 参数 **s.lb-**高级 **d.** 算法将计算 为空值。因此，为 lbmethod 属性传递的值无效。为了避免这种情况，可以在属性名称后面添加后缀“?”将属性标注为可选，如下所示：

```
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
<!--NeedCopy-->
```

使用“?“如果右侧的表达式计算为什么，则忽略该属性，在这种情况下，这将等同于定义如下的组件：

```
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
<!--NeedCopy-->
```

由于 **lbmethod** 是可选的，忽略它后，此组件仍是有效组件。请注意，如果在 lbmethod 的类型“ns::lbvserver”中定义了默认值，则 lbmethod 可能采用其默认值。

属性-默认源构造

February 6, 2024

properties-default-sources 构造类似于 parameters-default-sources 构造。parameters-default-sources 构造允许在样本中重用（来自其他样本的）现有参数，properties-default-sources 构造允许用户根据现有来源指定组件的属性。

组件的属性可以分布在样本的多个部分中。例如，属性可能来自对象参数、返回对象的替换、其他组件的属性或其他组件的输出。在此类情况下，您需要在组件的定义中重新定义在样本的其他部分中出现的属性。显然，这是多余的，且可能会导致出错。为了解决此问题，可以使用 properties-default-sources 构造。properties-default-sources 构造是一个列表，其中每项均标识组件的一些属性的一个来源。

例如，假定一个创建 lbvserver 配置的组件。此组件应按以下所示定义 lbvserver 的属性。

```
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
<!--NeedCopy-->
```

在上述示例中，看到 components 部分中定义的所有属性的值均取自 $parameters.lb 对象。尽管它们取自一个来源，但在样书中再次定义了属性。此外，如果向 $parameters.lb 对象添加与 lbvserver 的配置相关的新子参数，您需要更新 lb-comp 组件以添加与新子参数对应的新属性。

为了避免重新定义属性以及为了提取某个组件的所有相关属性而无需明确在 properties 部分中列出它们，可以使用 properties-default-sources 构造。上述示例可以编写如下。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

在上述示例中，通过使用 properties-default-sources 构造，减小了组件定义的规模，这样，您可以简明地定义组件。此外，每当组件的属性的来源更改时，更改会自动反映出来。例如，在 $parameters.lb 对象中添加新属性“persistencetype”时，由于 persistencetype 是 lbvserver 的属性，因此，默认情况下，此属性添加到 lb-comp 的配置。因此，properties-default-sources 构造提供了定义组件的动态接口，而无需担心组件的属性的来源发生的更改。

计算组件的属性

本节讨论如果在组件中使用 properties-default-sources 构造，如何提取属性。首先，样本编译器根据组件的类型（在上述示例中为 lbvserver）标识组件的属性列表。然后，编译器按这些属性的定义顺序（在组件的 properties-default-sources 部分中）从多个来源中提取它们。如果某个属性存在于多个来源中，则出现在最后一个来源中的该属性的优先级高于其他来源中的该属性。最后，可以在组件的 properties 部分中覆盖使用 properties-default-sources 构造提取的属性。请务必注意，components 部分的定义至少应有一个 properties-default-sources 部分或一个 properties 部分。可以有两者。

嵌套组件

February 6, 2024

通过在一个组件中嵌套另一个组件，嵌套的组件可以通过引用父组件创建的配置对象或上下文来创建其配置对象。嵌套的组件可以为父组件中创建的每个对象创建一个或多个对象。在一个组件中嵌套另一个组件并不表示创建的配置对象之

间有任何关系。嵌套是一种简化组件的任务以在父组件的现有上下文中构造配置对象的方式。

示例：

```
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: $srv
                      port: str($parameters.svc-port)
                      servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

在此示例中，使用了多层嵌套。组件 my-lbvserver-comp 有一个名为 my-svcg-comp 的子组件。而且 my-svcg-comp 组件里面有两个子组件。my-svcg-comp 组件通过为内置 NITRO 资源类型“服务组”的属性提供值，用于在 Citrix ADC 实例上创建服务组配置对象。my-svcg 组件的第一个子组件 lbvserver-svg-binding-comp 用于将其父组件创建的服务组绑定到父组件的父组件创建的负载平衡虚拟服务器 (lbvserver)。$parent 表示法（也称为父引用）用于引用父组件中的实体。第二个子组件 members-svcg-comp 用于将一组服务绑定到父组件创建的服务组。绑定是通过使用样书的 repeat 构造迭代为参数 svc-servers 指定的一组服务来完成。有关 repeat 构造的信息，请参阅 Repeat 构造。

还可以在不使用组件嵌套的情况下创建相同配置对象。有关详细信息和示例，请参阅用于创建基本负载平衡配置的样书。

条件构造

February 6, 2024

可以使用 condition 构造使组件成为有条件的组件。condition 构造的值是求值结果为 true 或 false 的布尔表达式。如果条件为 true，则使用该组件构建其配置对象。如果条件为 false，则跳过该组件，不通过它创建配置对象。布尔表达式通常基于参数值。

示例：

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
<!--NeedCopy-->
```

在此示例中，如果用户为可选参数 svc-server-ips 指定一个值，则样书引擎将处理组件 servicegroup-comp。如果条件为 false，即如果用户没有为此参数提供值，则系统为此参数指定空值，且求值结果为 false，那么样本引擎将忽略此组件，且不创建服务组。

请注意，布尔表达式可以基于样书中支持的任何有效表达式（例如，另一个组件是否存在，或一个参数是否有特定值）。

以下示例在条件求值结果为 true 时构建 NITRO 类型 ns::systemfile 的配置对象。

示例：

```
     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
<!--NeedCopy-->
```

在此示例中，条件是一个复杂的“OR”表达式，只有在样书中的其他两个组件已经处理（未跳过）时，才希望样书才创建此配置对象，从而在组件之间创建依赖关系。

重复构造

February 6, 2024

您可以使用组件的 **repeat** 构造来构建多个相同类型的配置对象。

在下面的示例中，**members-svcg-comp** 组件用于将一组服务绑定到父组件创建的服务组。为了创建将每个服务器绑定到服务组的配置对象，请使用 **repeat** 构造来迭代为参数 **svc-servers** 指定的服务列表。在迭代过程中，该组件为服务组中的每个服务（在 **repeat-item** 构造中称为 **serv**）创建一个类型为 **service-group_servicegroupmember_binding** 的 NITRO 对象，并将每个 NITRO 对象中的 **ip** 属性设置为相应服务的 IP 地址。

示例：

```
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
```



```
<!--NeedCopy-->
```

repeat 本身就是一个对象，**repeat-list** 和 **repeat-item** 是重复对象的属性。

- repeat-list 是必需属性，它标识组件迭代的列表。
- repeat-item 是可选的，用于为迭代中的当前项目指定友好名称。

如果未指定，则可以使用表达式 **$repeat-item** 访问当前 项目。上述示例中的最后一个组件还可以编写如下：

```
            -
            name: members-svcg-comp
            type: ns::servicegroup_servicegroupmember_binding
            repeat:
              repeat-list: $parameters.svc-servers
            properties:
                   ip: $repeat-item
                   port: $parameters.svc-port
                   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

除了能够在列表上以白色迭代方式引用当前项目外，还可以使用 repeat-index 引用列表中项目的当前索引 。在以下示例中，重复索引 用于基于当前索引计算端口号：

```
               name: services
               type: ns::service
               repeat:
                  repeat-list: $parameters.app-services
                  repeat-item: srv
               properties:
                   ip: $parameters.app-ip
                   port: $parameters.base-port + repeat-index
                   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

与 **repeat-item** 构造类似，您可以指定不同的变量名来引用迭代的当前索引。上述示例与以下示例等同：

```
      -
               name: services
               type: ns::service
               repeat:
                  repeat-list: $parameters.app-services
                  repeat-item: srv
                  repeat-index: idx
               properties:
                   ip: $parameters.app-ip
                   port: $parameters.base-port + $idx
                   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```


重复条件构造

February 6, 2024

在 repeat 构造的每个迭代中都对 repeat-condition 构造求值，并由结果确定是在相应迭代中构建配置对象，还是移至下一个迭代。以下示例说明了 repeat-condition 构造的使用：

示例：

```
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
<!--NeedCopy-->
```

在此示例中，der-key-files-comp 组件迭代用户提供的所有证书，但仅构建与采用 DER 编码的证书对应的配置对象。在每个迭代中，都对 repeat-condition 表达式求值来测试证书编码是否属于类型 DER。如果不属于类型 DER，则不在当前迭代中构建配置对象，且迭代移至列表中的下一个证书。

嵌套重复

February 6, 2024

通过使用嵌套的重复构造，根据组件的定义，一个组件中可以有多个重复构造。假定一个嵌套的重复有两个级别。对于外层列表（第一个 repeat-list）中的每个元素，您可以为内层列表（第二个 repeat-list）的所有元素创建一个重复列表。样本编译器最多支持三个嵌套的重复。每个重复级别都有与之关联的 repeat-item 和 repeat-index 属性。repeat-item 和 repeat-index 属性是可选的。此外，每个重复还可以指定 repeat-condition。

示例：

```
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
<!--NeedCopy-->
```

在上述示例中，对于 $parameters.vips 中的每项，均对 $parameters.vip-ports 的所有项进行迭代。因此，对于 $parameters.vips 中指定的每个 IP 地址，均为 $parameters.vip-ports 中指定的所有端口创建 lbvserver 配置对象。properties 部分定义对象的名称，并以“lb”作为 IP 地址和端口的组合的前缀。因此，对于每个迭代，$ip + $port 均定义 IP 地址和端口号的唯一组合。

如果未提供 repeat-item 属性，则编译器将为其生成默认值。repeat-item 的默认值为：分别对应每个重复级别的 $repeat-item、$repeat-item-1、$repeat-item-2。同样，如果未提供 repeat-index 属性，则编译器将为其生成默认值。repeat-index 的默认值为：分别对应每个重复级别的 $repeat-index、$repeat-index-1 和 $repeat-index-2。

以下示例说明了嵌套的重复对象中没有 repeat-item 和 repeat-index 属性时的命名约定。

示例：

```
components:
-
     name: lbvservers-comp
     type: ns::lbvserver
     repeat:
         repeat-list: $parameters.vips
         repeat:
            repeat-list: $parameters.vip-ports
     properties:
        name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
    -1)
         servicetype: HTTP
         ipv46: $repeat-item
         port: $repeat-item-1
<!--NeedCopy-->
```


输出

February 6, 2024

在 outputs 部分，指定样本成功完成创建所有配置对象后向其用户呈现的内容。样书的输出部分是可选的。样书不必返回输出。但是，如果将一些内部组件作为输出返回，导入它的任何样本就可以有更大的灵活性，这在创建复合样本时可以看到。

下表介绍了 outputs 部分中使用的属性。

属性	说明	强制
name	与您要呈现的配置对象对应的输出的名称。	是
description	描述输出的文本字符串。	否
value	此属性指定如何提取样本返回的值。	是

示例：

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

在此示例中，呈现将由样书创建的 **lbvserver** 组件和服务组名称。名为 **lbvserver** 的输出的值是组件 **my-lbvserver-comp**。同样，名为 **svc-grp** 的输出的值是组件 **my-svcg** 创建的服务组的名称。

参数引用

February 6, 2024

在组件构造中，通过使用符号来引用参数部分中定义 $parameters.<parametername> 的参数。如果 <parametername> 本身包含参数（当类型为对象时），则必须使用表示法 $parameters.<parametername>.<sub-parametername>，依此类推。

示例：


```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```

父级引用

February 6, 2024

如果您要使用嵌套的组件，可以使用 $parent 表示法来引用父组件。如果父组件使用 repeat 构造构建多个配置对象，且在每个迭代中，子组件构建其他配置对象，那么 $parent 表示法始终引用父组件的当前迭代。例如，$parent.properties.name 引用父组件的当前迭代中构建的配置对象的 name 属性。

示例：

```
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: $parameters.svc-servers
                      repeat-item: srv
                      properties:
                        ip: $srv
                        port: str($parameters.svc-port)
                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

还可以通过访问父组件的父组件的属性，在组件的层次结构中一直向上导航到顶层组件。例如，组件 **lbvserver-svg-binding-comp** 的属性名称通过使用 **$parent .parent** 表示法从其父代的父代（**my-lbvserver-comp** 组件）的属性名称中获取其值。

组件引用

February 6, 2024

在组件构造中，您可以使用 **$components** 来引用样书中的顶级组件。 \ <componentname\ > 表示法。如果顶级组件中有嵌套组件，则使用的表示法是 **$components**。**\ <componentname\ >.** 组件。\ <component-name\ > 来引用它们，依此类推。

示例：

```
components:
 -
```



```
    name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
 -
     name: my-svcg-comp
     type: ns::servicegroup
     properties:
          name: $parameters.name + "-svcgrp"
          servicetype: HTTP
 -
     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.my-svcg-comp.properties.name
 -
     name: lbvserver-svg-binding-comp
     type: ns::lbvserver_servicegroup_binding
     properties:
            name: $components.my-lbvserver-comp.properties.name
            servicegroupname: $components.my-svcg-comp.properties.name
<!--NeedCopy-->
```

在此示例中，必须先构建组件 **my-svcg-comp** 和 **my-lbvserver-comp**，再构建最后一个组件 **lbvserver-svg-binding-comp**，因为在这最后一个组件中有对这些组件的引用。这些引用是通过使用由 **$components** 表示的组件引用提供的。\ <componentname\ >。

替换引用

February 6, 2024

在组件部分或操作部分中，您可以使用 **$substitutions.<substitution-name>** 表示法来引用替换部分中定义的替换。例如，**$substitutions.http-port**。

如果替换是地图，则可以将地图中的元素称为 **$substitutions.<substitutions-name>[<map-key>]**。例如，**$substitutions.protocol-map[$parameters.port]**。

变量引用

February 6, 2024

在 components 中使用 repeat 和 repeat-item 构造来构建多个配置对象时，可以为 repeat-item 构造指定变量名称。然后，可以使用 **$\<varname\>** 表示法在该组件的属性中或子组件中引用此变量。注意，在组件中使用 repeat 构造时没有使用 repeat-item 构造，可以使用名为 $repeat-item 的默认变量来访问迭代项。

示例：

```
components:
  -
    name: server-members-comp
    type: ns::server
    condition: $parameters.svc-server-domain-names
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
           port: $parameters.svc-server-port
<!--NeedCopy-->
```

在上面的示例中，为 repeat-item 构造指定了变量名称 server-name。在同一组件的属性以及子组件 **$\<varname\>** 的属性中都引用了这个变量名。

operations

February 6, 2024

操作是样书中的一个可选部分。在本节中，您可以配置 Citrix Application Delivery Management (ADM) 分析，以收集有关所有或部分流量事务的 AppFlow 记录。使用样书在 Citrix ADC 实例上创建的虚拟服务器处理这些流量事务。在本节中，您还可以将 Citrix ADM 配置为在虚拟服务器上满足某些流量条件时触发警报。

您可以通过样书配置 Citrix ADM，从各种 Citrix ADM Insights 中收集流量统计信息，如下所示：

- Web Insight
- Security Insight

- HDX Insight
- Citrix Gateway Insight。

支持的虚拟服务器包括负载平衡、内容交换和 VPN 虚拟服务器。

启用 Web Insight 和 Security Insight 或其中之一，以便在负载平衡或内容交换虚拟服务器上进行分析。但是，对于 VPN 虚拟服务器，您必须同时启用 HDX Insight 和 Citrix Gateway Insight 或其中一个。

通过样本在 Citrix ADC 实例上启用的任何 Citrix ADM Insight 都使用 IPFIX 协议 (AppFlow) 将数据从实例发送到 Citrix ADC。

此外，启用 Web Insight 时，在负载平衡和内容交换虚拟服务器上启用“客户端测量”。

示例 **1**:

以下示例说明如何在样书中编写操作部分，以便在 VPN 虚拟服务器上同时启用 HDX Insight 和 Citrix Gateway Insight:

```
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
<!--NeedCopy-->
```

示例 **2**:

以下示例显示如何在样书中编写操作部分，以便在负载平衡虚拟服务器上启用 Web Insight 和 Security Insight:

```
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
<!--NeedCopy-->
```

分析

February 6, 2024

operations 部分的 analytics 子部分的结构与 components 部分类似。分析部分中的每个元素都用于为样书创建的一个或多个虚拟服务器配置 Citrix ADM Analytics 功能。

analytics 部分中的元素具有以下属性：

属性	说明	强制
name	analytics 元素的名称。	是
description	说明此元素是什么的文本字符串。	否
condition	布尔表达式。此 condition 求值结果为 false 时，将跳过整个 analytics 元素。	否
重复	迭代列表。	否
repeat-condition	布尔表达式。如果该表达式的求值结果为 false，则将跳过当前迭代。	否
repeat-item	当前迭代中项目的名称。	否
repeat-index	当前迭代的索引值的名称。	否
properties	analytics 的属性列表。	是
target	列表中的其中一个属性。目标表达式是在 Citrix ADC 上配置的虚拟服务器的名称，将收集其分析结果。	是
filter	列表中的其中一个属性。此属性的值是 Citrix ADC 高级策略表达式，用于筛选虚拟服务器上将收集分析结果的请求。默认情况下，收集通过虚拟服务器的所有通信的分析数据。	否

示例：

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```


分析部分中的每个属性用于指示 Citrix ADM 分析功能配置 Citrix ADC 实例，以便在由目标属性标识的虚拟服务器上收集应用程序流记录。

警报

February 6, 2024

operations 部分的 alarms 子部分的结构与 analytics 子部分类似，属性与 analytics 子部分相同。唯一的区别是 properties 属性。有关所有属性（properties 属性除外）的列表，请参阅分析。

alarms 子部分中具有以下属性：

属性	说明	强制
target	计算为虚拟服务器名称的表达式，该表达式在 Citrix ADC 上配置，并为其配置了警报。	是
email-profile	在 Citrix ADM Analytics 功能中定义的电子邮件配置文件的名称，包含触发警报时要通知的电子邮件地址列表。	否（必须定义 email-profile 或 sms-profile）
sms-profile	在 Citrix ADM Analytics 功能中定义的 SMS 配置文件的名称，该配置文件包含要在触发警报时通知的调用号码列表。	否（必须定义 email-profile 或 sms-profile）
rules	定义将会为 target 属性定义的虚拟服务器触发警报的条件的规则列表。	是
metric	规则的属性。您要跟踪的与 Citrix ADC 虚拟服务器相关的指标的名称。	是
operator	规则的属性。运算符用于将指标与值比较。有效运算符为“greaterthan”和“lessthan”。	是
value	规则的属性。通过使用运算符将指标与其比较的阈值。如果指标值超过此阈值，则触发关联的警报。	是
period-unit	规则的属性。满足警报规则时向用户发出警报的频率。其值可以是天、小时或周。这表示，如果满足规则，则每个 period-unit 发送一次警报（例如，一天一次）。	是

下表提供了跟踪的与 Citrix ADC 虚拟服务器相关的指标列表。

Counters（计数器）| 说明 | 详细描述 |Citrix ADM 计算
|–|–|–|–|
| 对于 VPN 虚拟服务器：|
total_requests|VPN 会话启动总数 | 在用户指定的时间间隔内在此 VPN 虚拟服务器上启动的活动会话总数。| 单调递增的计数器，在每次新会话启动时递增 |
app_count	VPN 应用程序启动计数	在用户指定的时间间隔内在此 VPN 虚拟服务器上启动的唯一 VPN 应用程序总数。	单调递增的计数器，基于每次新应用程序启动
app_launch_duration	VPN 应用程序启动持续时间	启动应用程序所用平均时间（以毫秒为单位）	基于在此 VPN 虚拟服务器上启动的所有 VPN 应用程序的启动持续时间计算得出的平均值
其他虚拟服务器（CS、LB、身份验证、GSLB）	
Total_Request| 请求数	请求数	自上次设备重新启动以来或创建虚拟服务器以最近为准的虚拟服务器上的客户端请求数。| 单调递增计数器，每次向此虚拟服务器发出新请求时递增。|
总字节	字节	在指定时间间隔内从虚拟服务器传输到 Citrix ADM 的总字节数。	单调增加计数器以考虑此虚拟服务器提供的总字节数。
应用程序 _ 响应 _ 时间	响应时间	虚拟服务器的平均响应时间。	此虚拟服务器自设备上次重新启动（或创建虚拟服务器）以来收到的所有请求的响应时间的平均值（以最后者为准）。

样本中的 alarms 部分示例：

```
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

<!--NeedCopy-->
```


表达式

February 6, 2024

样本其中一个最强大的功能是使用表达式。可以在各种方案中使用样本表达式来计算动态值。下面的示例显示了一个将参数值与文字字符串连接的表达式。

示例：

```
$parameters.appname + “-mon”
```

此表达式检索名为 appname 的参数，并将其与字符串“-mon”连接。

支持以下类型的表达式：

算术表达死

- 添加 (+)
- 潜水 (-)
- 乘法 (*)
- 分隔 (/)
- 模数 (%)

示例：

- 添加两个数字：$parameters.a + $parameters.b
- 乘以两个数字：$parameters.a * 10
- 在一个数字除以另一个数字后查找剩余数字：

15 % 10 结果为 5

字符串表达式

- 连接两个字符串 (+)

示例：

连接两个字符串：str(“app-“) + $parameters.appname

列表表达式

合并两个列表 (+)

示例：

- 连接两个列表：$parameters.external-servers + $parameters.internal-servers
- 如果 $parameters.ports-1 为 [80, 81]，$parameters.port-2 为 [81, 82]，则 $parameters.ports-1 + $parameters.ports-2 结果为列表 [80, 81, 81, 82]

关系表达式

- == ：测试两个操作数是否相同，如果相同，则返回 true，否则返回 false。
- != ：测试两个操作数是否不同，如果不同，则返回 true，否则返回 false。
  - ：如果第一个操作数大于第二个操作数，则返回 true，否则返回 false。
  - =：如果第一个操作数大于或等于第二个操作数，则返回 true，否则返回 false。
- < ：如果第一个操作数小于第二个操作数，则返回 true，否则返回 false。
- <= ：如果第一个操作数小于或等于第二个操作数，则返回 true，否则返回 false。

示例：

- 等式运算符的使用：$parameters.name = = “abcd”
- 使用不等号运算符：$parameters.name != “default”
- 其他关系运算符示例
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

逻辑（布尔）表达式

- and：逻辑“与”运算符。如果两个操作数为 true，则结果为 true，否则为 false。
- or：逻辑“或”运算符。如果其中一个操作数为 true，则结果为 true，否则为 false。
- not：一元运算符。如果操作数为 true，则结果为 false，反之亦然。
- in: 测试第一个参数是否为第二个参数的子字符串
- in：测试项目是否属于列表的一部分

> 注意

> 您可以键入转换表达式，通过使用这种表达式，字符串转换可以为数字，数字可以转换为字符串。同样，tcp-port 可以转换为数字，IP 地址可以转换为字符串。

必须在任何运算符前后使用分隔符。可以使用以下分隔符：

> - 在运算符前面：空格、Tab、逗号、(、)、[、]
> - 在运算符后面：空格、Tab、(、[
> - 例如：
> - abc + def
> - 100 % 10
> - 10 > 9

表达式类型验证

样书引擎现在允许在编译期间进行增强的类型检查，即，在导入样书本身的过程中，而不是在创建配置包时，验证编写样书时使用的表达式，

所有对参数、替换、组件、组件属性、组件输出、用户定义的变量（重复项、重复索引、替换函数的参数）的引用都是验证它们的存在和类型。

类型检查示例：

在以下示例中，lbvserver 样书的预期 port 属性类型为 tcp-port。在 Citrix Application Delivery Management (ADM) 早期版本中，样本编译器将该值计算为字符串，并导入并执行样本。现在，在编译时（导入时）进行类型验证。编译器发现 string 和 tcp-port 不是兼容的类型，因此样书编译器抛出错误，且样书导入或迁移失败。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP

You should now declare this as a number for the compiler to
   successfully compile this StyleBook.

  port: 80
<!--NeedCopy-->
```

标记无效表达式的示例：

在早期版本中，当将无效表达式分配给属性名称时，编译器未检测到无效表达式，并允许将样本导入 Citrix ADM。现在，如果将此样本导入到 Citrix ADM，编译器将识别此类无效表达式并将其标记为。因此，样本不会导入到 Citrix ADM。

在此示例中，为 lb-sg-binding-comp 组件中的 name 属性分配的表达式为：$components.lbvserver-comp.properties.lbvservername。但组件 lbvserver-comp 中没有称为 lbvservername 的属性。在早期的 Citrix ADM 版本中，编译器将允许此表达式并成功导入该表达式。当用户要使用此样书创建配置包时，实际上会失败。但是现在，在导入过程中会识别此类错误，并且样本不会导入到 Citrix ADM。您必须手动更正此类错误并导入样书。

```
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
<!--NeedCopy-->
```

为列表建立索引

现在，可以直接为列表中的项目建立索引来访问它们：

** 表达式 **	** 说明 **
$components.test-lbs[0]	引用 test-lbs 组件中的第一个项目
$components.test-lbs[0].properties.p1	引用 test-lbs 组件中的第一个项目的属性 p1
$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname	引用 service-groups 组件中的第二个项目的属性 servicegroupname，这是 lbcomps 组件的第一个项目的输出。

原位内插

February 6, 2024

现在可以替换字符串中使用样书表达式的部分。样本编译器对这些字符串表达式进行求值时，字符串中使用样本表达式的部分将替换为表达式的值。要在字符串中包括样书表达式，我们使用以下表示法：

“…%{…}%…”

其中，“%{”和“}%”之间包括的字符构成样本表达式。这些表达式称为“原位内插”。

例如，字符串“lb-%{$parameters.appname}%-svc”是包含原位内插样本表达式的字符串表达式。字符串表达式的值取决于内插表达式的值。假定为 **$parameters.appname** 分配了 app1。然后，字符串表达式的计算结果为 **lb-app1-svc** 这就允许不在字符串表达式中对值进行硬编码，而是根据用户定义的值求值。

原位内插的一个实际用例是在样本中参数化策略表达式。假设这样一个场景：您要编写一个策略表达式，用于检查 HTTP URL 是否包含特定的单词，例如“jpeg”。

为此，您可以编写如下所示的策略表达式:”HTTP.REQ.URL.CONTAINS(\“jpeg\”)”。

现在，如果您要参数化 HTTP URL 中的对象，可以在样本中添加字符串参数，例如 $parameters.url-object。应基于此参数编写策略表达式。为此，应使用字符串连接来达到效果。该表达式类似如下：

str(“HTTP.REQ.URL.CONTAINS(\”” + $parameters.url-object + “\”)”)

如果为 $parameter.url-object 分配“csv”，则上述表达式的求值结果将为“HTTP.REQ.URL.CONTAINS(\“csv\”)”。但是，此表达式不易阅读。为了使此参数化形式易于阅读和理解，可以使用原位内插。

现在，包含原位内插的表达式为：

str(“HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)”)

在上述表达式中，使用了一个在 $parameters.url-object 值两边添加内部引号的内插表达式。此表达式的结果与上述表达式相同，但它更加直观且更接近实际结果。

内插中允许的类型

您可以在内插中使用生成以下类型值的表达式：boolean、number、tcp-port、ipaddress 和 string。内插替换为结果时，生成的值会自动转换为字符串。

字符串表达式可以有 0、1 个或更多内插。在顺序内插中，字符串表达式的不同部分可以替换为不同的样本表达式。例如，如果 $parameters.appname 为“app1”且 $parameters.vip 为“1.1.1.1”，字符串 lb-%{$parameters.appname}%-%{$parameters.vip}% 返回“lb-app1-1.1.1.1”

字符串表达式还支持嵌套内插。即，内插表达式可以嵌套在另一个内插表达式中，以便一个表达式的值可以作为另一个表达式的输入。

例如，考虑一个字符串“%{lb-%{$parameters.port + 1}%}%”

如果 $parameters.port 为 80，则内部字符串“**%{$parameters.port + 1}%**”返回“lb-81”。此处此表达式嵌套在另一个插值表达式中。

下表介绍了不同类型的内插，并提供了示例和相应的结果。示例中使用的参数值为：

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

简单插值

表达式	结果
lb-%{$parameters.appname}%-def	lb-lb1-def

自动类型转换

表达式	结果
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

顺序插值

表达式	结果
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

嵌套内插

表达式	结果
%{abc-%{$parameters.n1 + 1}%}%	abc-2
str(“%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%”)	bc-1-3

包含 **quotewrap** 的内插

表达式	结果
str(“%{quotewrap(abcd)}%”) str(“%{quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	“abcd “«code class=” language-plaintext highlighter-rouge” >https://” +HTTP.REQ.HOSTNAME+HTTP.REQ.URL</code>

内插中的转义字符

如果字符“% {”或“}%”是字符串的一部分，则必须提供“\”作为转义字符，这样样书编译器就不会将它们视为插值标签。

示例：

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%” if $parameters.vip is 1.1.1.1

下表介绍了另外一些表达式及其结果：

类别	表达式	结果
转义内插	str(“%{str($parameters.n1) + }\%}%”)	1}%
	lb-%{str($parameters.n1) + }\%}%	lb-1}%
	” %{str($parameters.n1) + \” }\%\” }%”	1}%

内置函数

February 6, 2024

样本中的表达式可以利用内置函数。

例如，可以使用内置函数 str() 将数字转换为字符串。

str($parameters.order)

或者，可以使用内置函数 int() 将字符串转换为整数。

int($parameters.priority)

下面是样书表达式中支持的内置函数列表以及这些函数的用法示例。

str()

str () 函数将输入参数转换为字符串值。

允许的参数类型：

- string
- number
- TCP 端口
- 布尔值
- IP 地址

示例：

- “set-“+ str(10) 返回“set-10”
- str(10) 返回“10”
- str(1.1.1.1) 返回“1.1.1.1”
- str (T rue) 返回“T 规则”
- str(mas) 返回“mas”

int()

int () 函数接受一个字符串、数字或 tcpport 作为参数并返回一个整数。

示例：

- int(“10”) 返回 10
- int(10) 返回 10

bool()

bool（）函数接受任何类型作为参数。如果参数值为 false、空或不存在，则此函数返回 false。

否则返回 true。

示例：

- bool(true) 返回“true”
- bool(false) 返回“false”
- bool($parameters.a) 返回 false，前提为
- $parameters.a 为 false、空或不存在。

len()

len () 函数将字符串或列表作为参数，并返回字符串中的字符数或列表中的项目数。

示例 **1**：

如果按以下所示定义 substitution：

items: [“123”，“abc”，“xyz”]

len($substitutions.items) 返回 3

示例 **2**：

len（“netscaler mas”）返回 13

示例 **3**：

如果为 $parameters.vip 分配了值 [‘1.1.1.1’，‘1.1.1.2’，‘1.1.1.3’]，则
len($parameters.vips) 将返回 3

min()

min () 函数接受一个列表或一系列数字或 tcp-port 作为参数，并返回最小的项目。

包含一系列编号**/TCP** 端口的示例：

- min(80, 100, 1000) 返回 80
- min(-20, 100, 400) 返回 -20
- min(-80, -20, -10) 返回 -80
- min(0, 100, -400) 返回 -400

包含编号**/tcp** 端口列表的示例：

- 支持 $parameters.ports 是一个 tcp 端口列表，其值为：[80、81、8080]。

  min($parameters.ports) 返回 80。

max()

max () 函数接受一个列表或一系列数字或 tcp-port 作为参数，并返回最大的项目。

包含一系列编号**/TCP** 端口的示例：

- max(80, 100, 1000) 返回 1000
- max(-20, 100, 400) 返回 400
- max(-80, -20, -10) 返回 -10
- max(0, 100, -400) 返回 100

包含编号**/tcp** 端口列表的示例：

- 支持 $parameters.ports 是 TCP 端口列表且值为：[80, 81, 8080]。

  max($parameters.ports) 返回 8080。

bin()

bin () 函数接受一个数字作为参数，并返回一个以二进制格式表示数字的字符串。

表达式示例：

bin(100) 返回“0b1100100”

oct()

oct () 函数接受一个数字作为参数，并返回一个以八进制格式表示数字的字符串。

表达式示例：

oct(100) 返回“0144”

hex()

hex () 函数接受一个数字作为参数，并返回一个以十六进制格式表示数字的小写字符串。

表达式示例：

hex(100) 返回“0x64”

lower()

lower () 函数接受一个字符串作为参数，并以小写形式返回相同的字符串。

示例：

lower(“MAS”) 返回“mas”

upper()

upper () 函数接受一个字符串作为参数，并以大写形式返回相同的字符串。

示例：

upper（“netscaler_mas”）返回“NET SCALER_MAS”

sum()

sum () 函数将数字列表或 tcpport 作为参数，并返回列表中数字的总和。

示例 **1**：

如果按如下方式定义替
代：替代：

- 数字列表：
  - 11
  - 22
  - 55

  总和（美元替换，数字列表）返回 88

示例 **2**：

如果 $parameters.ports 为 [80, 81, 82]，则 sum($parameters.ports) 返回 243

pow()

pow () 函数接受两个数字作为参数，并返回一个数字，该数字表示第一个参数提高到第二个参数的
幂。

示例：

pow(3,2) 返回 9

ip()

ip 函数接收字符串或 IP 地址作为参数，并基于输入值返回 IP 地址。

示例：

- ip（“2.1.1.1”）返回“2.1.1.1”
- ip(3.1.1.1) 返回“3.1.1.1”

base64.encode()

base64.code () 函数接受一个字符串参数并返回 base64 编码的字符串。

示例：

base64.encode（“abcd”）返回“YWJjZA==”

base64.decode()

base64.decode 函数接收 base64 编码的字符串作为参数，并返回解码的字符串。

示例：

base64.decode（“YWJjZA==”）返回“abcd”

存在 ()

exists 函数接收任何类型的参数，并返回布尔值。如果输入有任何值，则返回值为 True。返回值为 False 如果输入参数没有值（即没有值）。

假定 $parameters.monitor 是一个可选参数。如果您在创建配置包时为此参数提供值，则 exists($parameters.monitor) 返回 True。

否则返回 False。

筛选器 ()

filter () 函数接受两个参数。

参数 1：接收一个参数并返回布尔值的 substitution 函数。

参数 2：列表。

该函数返回原始列表的子集，其中每个元素在第一个参数中传递给替换函数时计算结果为“True”。

示例：

假定按如下所示定义了 substitution 函数。

substitutions:

```
x(a): $a != 81
```

如果输入值不等于 81，则此函数返回 True。否则返回 False。

假设，

$parameters.ports 是 [81、80、81、89]

filter($substitutions.x, $parameters.ports) 从列表中删除出现的所有 81，返回 [80, 89]。

如果-然后-否则 ()

if-then-else () 函数接受三个参数。

参数 1：布尔表达式

参数 2：任何表达式

参数 3：任何表达式（可选）

如果参数 1 中的表达式求值结果为 True，则该函数返回作为参数 2 提供的表达式的值。

否则，如果提供了参数 3，该函数返回参数 3 中的表达式的值。

如果未提供参数 3，则该函数不返回值。

示例 **1**：

如果 $parameters.servicetype 的值为 “HTTP”，则 if-then-else($parameters.servicetype == HTTP, 80, 443) 返回 “80”。否则，该函数返回
“443”。

示例 **2**：

如果 $parameters.servicetype 的值为 HTTP，则 if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport) 将返回 $parameters.hport 的值。

否则，该函数返回 $parameters.sport 的值。

示例 **3**：

如果 $parameters.servicetype 的值为 “HTTP”，则 if-then-else($parameters.servicetype == HTTP, 80) 返回 “80”。

否则，该函数不返回任何值。

连接 ()

join () 函数接受两个参数：

参数 1：数字、TCP 端口、字符串或 IP 地址列表

参数 2：分隔符字符串（可选）

该函数将作为参数一提供的列表的元素连接为一个字符串，其中的每个元素以作为参数二提供的分隔符字符串分隔开。如果未提供参数二，则列表中的元素连接在一起作为一个字符串。

示例：

- $parameters.ports 为 [81, 82, 83]。
  - 使用分隔符参数：

    join ($parameters.ports, '-') 返回“81-82-83”
  - 没有分隔符参数：

    加入 ($parameters.ports) 返回“818283”

地图 ()

map 函数接收两个参数；

参数 1：任何函数

参数 2：元素列表。

函数返回一个列表，其中列表中的每个元素都是将 map 函数（参数 1）应用于参数 2 中的相应元素的结果。

参数 1 中允许的函数：

- 采用一个参数的内置函数：

  base64.encode、base64.decode、bin、bool、exists、hex、int、ip、len、lower、upper、oct、quotewrap、str、trim、upper、url.encode、url.decode
- 至少接收一个参数的 substitution 函数。

示例：

假定 $parameters.nums 为 [81, 82, 83]。

- 使用内置函数 str 的 map

  map(str, $parameters.nums) 返回 [“81”，“82”，“83”]

  map 函数的结果是字符串列表，其中的每个元素是对输入列表 ($parameters.nums) 中的对应元素应用 str 函数计算所得的字符串。
- 使用 substitution 函数的 map
  - 替换：

    add-10(port): $port + 10
  - 表达式：

    map($substitutions.add-10,

    $parameters.nums) 返回数字列表：
    [91、92、93]

此 map 函数的结果是数字列表，每个元素是对输入列表 ($parameters.nums) 中的对应元素应用 substitution 函数 $substitutions.add-10 计算所得。

报价包装 ()

quotewrap 函数接收字符串作为参数，并返回在输入值前后添加了双引号字符的字符串。

示例：

quotewrap (“mas”) 返回 “” mas “”

替换 ()

replace 函数接收三个参数：

参数 1：字符串

参数 2：字符串

参数 3：字符串（可选）

该函数将参数一中出现的所有参数二替换为参数三。

如果未提供参数三，则从参数一中删除出现的所有参数二（也就是说，替换为空字符串）。

将一个子字符串替换为另一个字符串：

- replace(‘abcdef’ , ‘def’ , ‘xyz’) 返回 “abcxyz”。
  - 出现的所有 “def” 替换为 “xyz”。
- replace(‘abcdefabc’ , ‘def’) 返回 “abcabc”。
  - 由于没有第三个参数，因此从结果字符串中删除了 “def”。

修剪 ()

trim 返回从输入字符串中去掉前导空格和尾随空格的字符串。

示例：

trim (‘abc’) 返回 “abc”

截断 ()

truncate 函数接收两个参数：

参数 1：字符串

参数 2：数字

该函数返回参数一中的输入字符串截断为参数二中指定的长度的字符串。

示例：

truncate（‘netscaler mas’, 9) 返回“netscaler”

url.encode

url.encode 函数返回其中的字符根据 RFC 3986 使用 ASCII 字符集进行转换的字符串。

示例：

url.encode（“a/b/c”) 返回“a%2Fb%2Fc”

url.decode

url.decode 返回其中的 URL 编码参数根据 RFC 3986 解码为常规字符串的字符串。

示例：

url.decode（“a%2Fb%2Fc”) 返回“a/b/c”

is-ipv4 ()

is-ipv4 () 函数将 IP 地址作为参数，如果 IP 地址为 IPv4 格式，则返回“真”。

is-ipv4 (10.10.10.10) 返回“真”

is-ipv6 ()

is-ipv6 () 函数将 IP 地址作为参数，如果 IP 地址为 IPv6 格式，则返回“真”。

is-ipv6 (2001:DB8::) 返回“真”

依赖性检测

February 6, 2024

样书中的组件可以引用同一样书中的其他组件的属性或部分。组件本身是完整的块，它们的编写顺序可能与必须执行的顺序不同。样本编译器会检查组件的编写顺序，然后按逻辑顺序执行这些组件。

示例：


```
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
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--NeedCopy-->
```

在上面的例子中，定义了三个组件- **lbvser-comp**，**lb-sg-**绑定**-**复合和 **sg-comp**。执行此样本时，先创建 lbvserver-comp。lb-sg-binding-comp 引用 lbvserver-comp 属性，但尽管它是样本中定义的第二个组件，但不能接下来创建它。这是因为 lb-sg-binding-comp 还依赖也要创建的 sg-comp。因此，编译器对组件重新排序以使组件的依赖项按组件的创建时间进行解析，然后执行此重新排序的组件列表。上述样本的执行顺序为：lbvserver-comp、sg-comp 和 lb-sg-binding-comp。

这样，样书的作者不必担心组件的正确顺序。组件可以按任何顺序显示。编译器根据组件相互引用的情况计算组件的正确执行顺序。请注意，此依赖项检测和重新排序也适用于 substitutions 和 outputs 部分。

循环依赖项

由于组件可能会引用其他组件，因此可能会在样本的定义中引入依赖项循环。例如，如果组件 A 引用组件 B 中定义的一个属性，而后者也引用组件 A 中定义的一个属性。这种依赖项称为循环依赖项。循环依赖项无法自动解析。样本的作者应该手动更新更正样本定义以消除此类循环依赖项。编译器能够识别循环依赖项（如果存在）并报告。

以下示例显示了组件的循环依赖项：

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
```



```
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
23  <!--NeedCopy-->
```

在上面的示例中，有三个组件：**lbvserver-comp**、**lb-sg-binding-comp** 和 **sg-comp**。lbvserver-comp 依赖于 lb-sg-binding-comp，lb-sg-binding comp 依赖于 sg-comp，sg-comp depends 依赖于 lbvserver-comp。此处，在这些组件之间形成了依赖项循环，这无法自动解析。因此，无法执行此样书。样本编译器检测到此问题并阻止样本导入 Citrix ADM。

实例管理

February 6, 2024

实例是 Citrix Application Delivery Controller (ADC) 设备，您可以使用 Citrix Application Delivery Management (ADM) 管理、监视和故障排除。必须向 Citrix ADM 添加实例才能对其进行监视。您可以在设置 Citrix ADM 时或稍后添加实例。将实例添加到 Citrix ADM 后，系统会持续轮询这些实例，以收集以后可用于解决问题或作为报告数据的信息。

实例可以分组为静态组或专用 IP 块。当您想要运行特定任务（例如配置作业等）时，静态实例组可能很有用。专用 IP 块根据实例的地理位置对实例进行分组。

添加实例

您可以在首次设置 Citrix ADM 服务器时添加实例，也可以在以后添加实例。要添加实例，您必须指定每个 Citrix ADC 实例的主机名或 IP 地址，或指定 IP 地址范围。

要了解如何向 Citrix ADM 添加实例，请参阅 向 Citrix ADM 添加实例。

将实例添加到 Citrix ADM 服务器时，服务器会隐式地将自身添加为实例的陷阱目标，并收集实例的清单。要了解更多信息，请参阅 Citrix ADM 如何发现实例。

添加实例后，您可以通过导航到“网络”>“控制板”并单击“所有实例”来将其删除。在“实例”页面上，选择要删除的实例，然后单击 删除”。

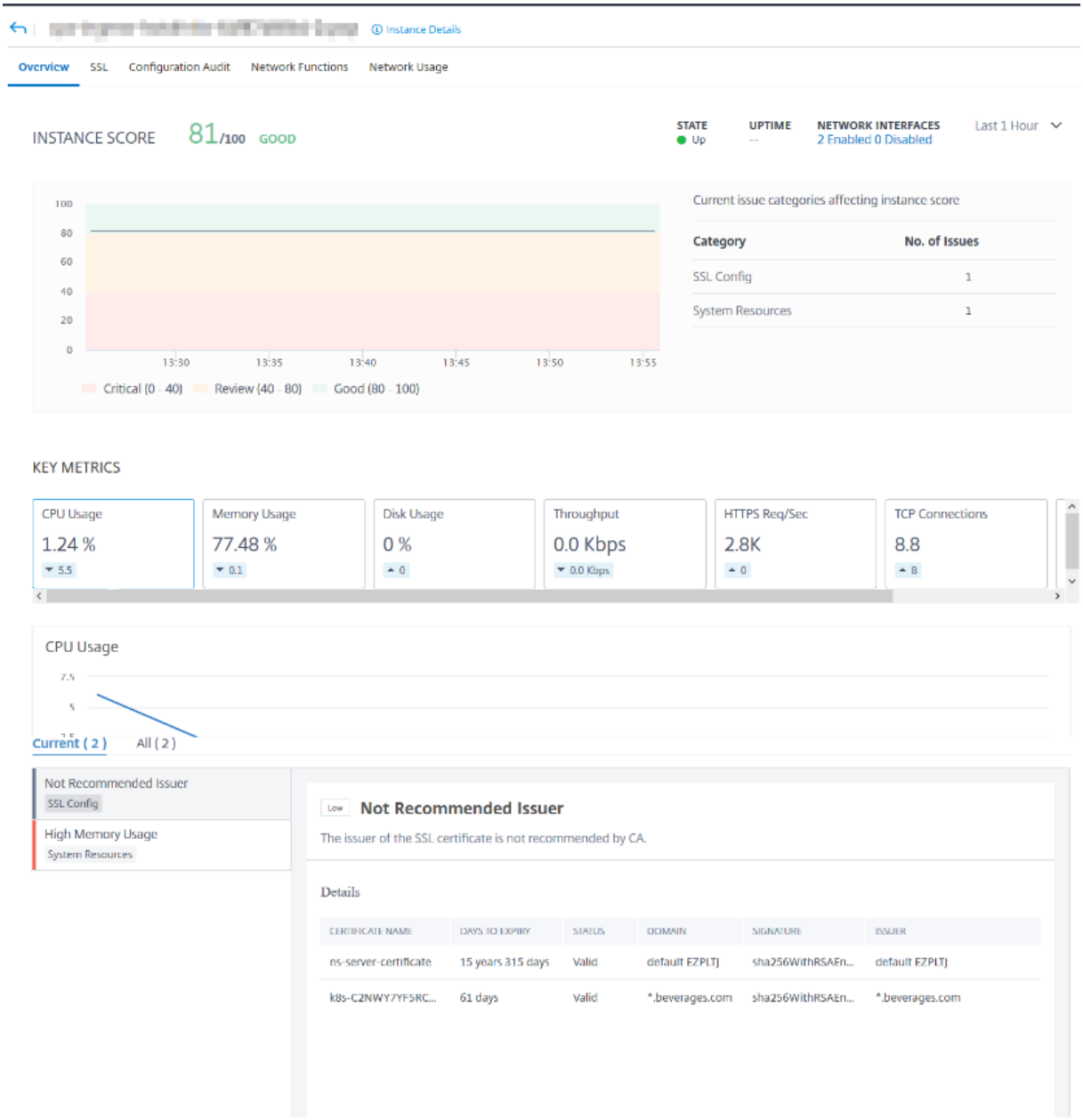
如何使用实例控制面板

Citrix ADM 中的每实例控制板以表格和图形格式显示选定实例的数据。在轮询过程中从您的实例收集的数据显示在控制面板上。

默认情况下，每分钟轮询托管实例以进行数据收集。使用 NITRO 调用持续收集状态、每秒 HTTP 请求、CPU 使用率、内存使用率和吞吐量等统计信息。作为管理员，您可以在单个页面上查看所有这些收集的数据，确定实例中的问题，并立即采取措施来纠正这些问题。

要查看特定实例的控制板，请导航到“网络”>“实例”。从摘要中选择实例类型，然后选择要查看的实例，然后单击 控制板。

下图概述了每个实例控制板上显示的各种数据：



- 概述。概述选项卡显示所选实例的 CPU 和内存使用情况。您还可以查看实例生成的事件和吞吐量数据。此处还显示特定实例的信息，例如 IP 地址、其硬件和 LOM 版本、配置文件详细信息、序列号、联系人等。通过进一步向下滚动，您所选实例上可用的许可功能及其上配置的模式。
- **SSL** 控制板。您可以使用每个实例控制面板上的 SSL 选项卡来查看或监视所选实例的 SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。您可以单击图表中的“数字”以显示更多详细信息。
- 配置审核。您可以使用配置审核选项卡查看所选实例上发生的所有配置更改。控制面板上的 **NetScaler** 配置保存状态 和 **NetScaler** 配置偏移图表显示了有关已保存配置更改的高级详细信息，这些更改针对未保存的配置进行了保存。
- 网络功能。使用网络功能控制板，您可以监视在所选 Citrix ADC 实例上配置的实体的状态。您可以查看虚拟服

务器的图表，这些图表显示客户端连接、吞吐量和服务器连接等数据。

- 网络使用情况。您可以在网络使用情况选项卡上查看所选实例的网络性能数据。您可以显示一小时、一天、一周或一个月的报告。时间轴滑块功能可用于自定义正在生成的网络报告的持续时间。默认情况下，仅显示八份报告，但您可以单击屏幕右下角的“加号”图标来添加其他性能报告。

监视分布全球的站点

February 6, 2024

作为网络管理员，您可能必须监视和管理部署在不同地理位置的网络实例。但是，在分布在地理位置上的数据中心管理网络实例时，要衡量网络的要求并不容易。

Citrix Application Delivery Management (ADM) 中的地理地图为您提供站点的图形表示，并按地理位置细分网络监视体验。通过 Geomap，您可以按位置呈现网络实例分布，并监视网络问题。

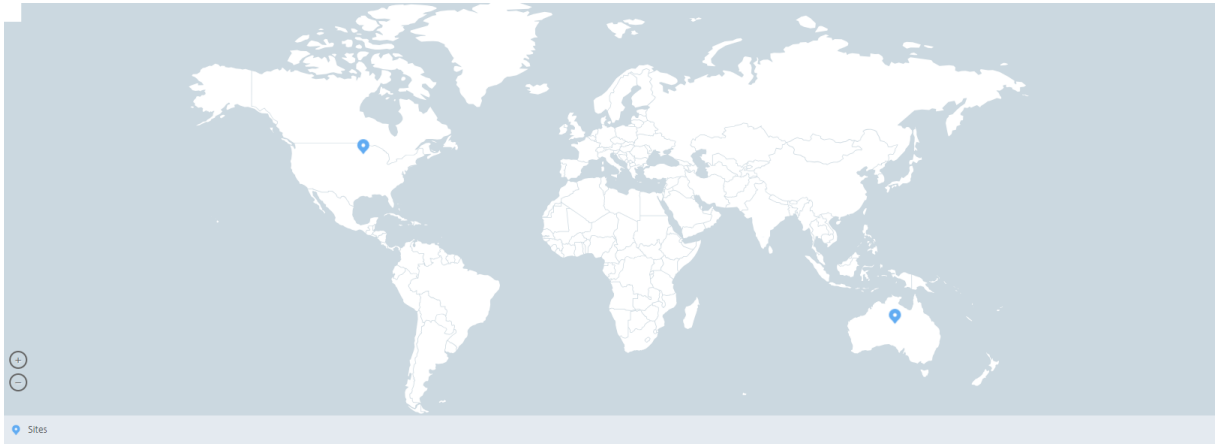
以下部分介绍如何监视 Citrix ADM 中的数据中心。

Citrix ADM 站点是特定地理位置中的 Citrix 应用程序 Delivery Controller (ADC) 实例的逻辑分组。例如，当一个站点被分配给 Amazon Web Services (AWS) 时，另一个站点可能被分配给 Azure™。还有另一个网站托管在租户的场所内。Citrix ADM 管理和监视连接到所有站点的所有 Citrix ADC 实例。您可以使用 Citrix ADM 监视和收集系统日志、AppFlow、SNMP 以及来自托管实例的任何此类数据。

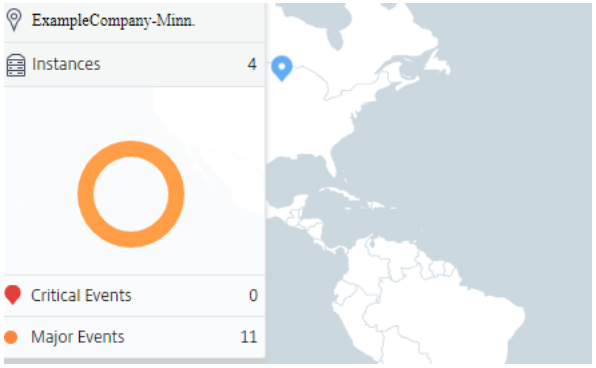
Citrix ADM 中的地理地图为您提供站点的图形表示。Geomaps 还会按地理位置细分您的网络监视体验。通过地理图，您可以按位置可视化您的网络实例分布并监视所有网络问题。您可以导航到“网络”>“** 控制板”页面，直观地显示在世界地图上创建的站点。

用例

一家领先的移动运营商公司 ExampleCompany 依靠私有服务提供商来托管其资源和应用程序。该公司已经有两个基地——一个位于美国的明尼阿波利斯，另一个在澳大利亚的爱丽斯泉。在此图中，您可以看到两个标记代表两个现有站点。

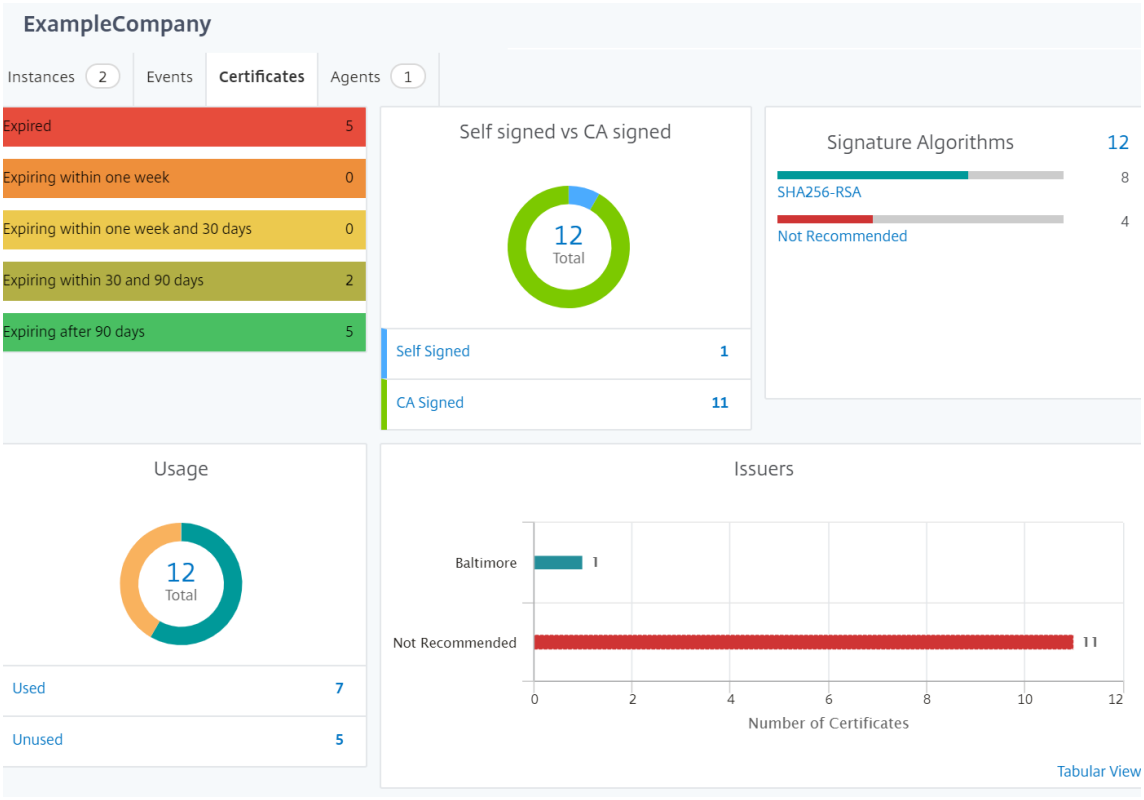


标记还会显示一个数字，显示每个站点中的应用程序数。您可以单击这些标记以了解有关每个站点的详细信息。



单击选项卡以查看详细信息：

- “实例”选项卡：在此选项卡中查看以下内容：
  - 每个网络实例的 IP 地址
  - 实例的类型
  - 他们身上的关键事件数量
  - 在 Citrix ADC 实例上引发的重大事件和所有事件。
- “事件”选项卡：查看实例上引发的关键和重要事件列表。
- “证书”选项卡：在此选项卡中查看以下内容：
  - 所有实例的证书列表
  - 到期状态
  - 重要信息以及许多正在使用的证书中排名前 10 位的实例。
- 代理选项卡：查看绑定实例的代理列表。



配置地理地图

ExampleCompany 决定在印度班加罗尔创建第三个站点。该公司希望通过将一些不太重要的内部 IT 应用程序转移到班加罗尔办公室来测试云。该公司决定使用 AWS 云计算服务。

作为管理员，您必须先创建一个站点，然后在 Citrix ADM 中添加 Citrix ADC 实例。您还必须将实例添加到站点，添加代理，并将代理绑定到站点。然后，Citrix ADM 会识别 Citrix ADC 实例和代理所属的站点。

有关添加 Citrix ADC 实例的更多信息，请参阅添加实例。

要创建站点：

在 Citrix ADM 中添加实例之前，请先创建站点。通过提供位置信息，您可以精确地定位站点。

导航到 “网络” > “站点”，然后单击 “添加”。

1. 在“创建站点”页中，指定以下信息：

   a) 站点类型：选择 数据中心。

   > 注意
   >
   > 该站点可以用作主数据中心或分支机构。相应地选择。

   b) 类型：从列表中选择 AWS 作为云提供商。

> 注意相应
>
> 选中“使用现有 **VPC** 作为站点”框。

c) 站点名称：键入站点的名称。

d) 城市：键入城市。

e) 邮政编码：键入邮政编码。

f) 区域：键入区域。

g) 国家：键入国家

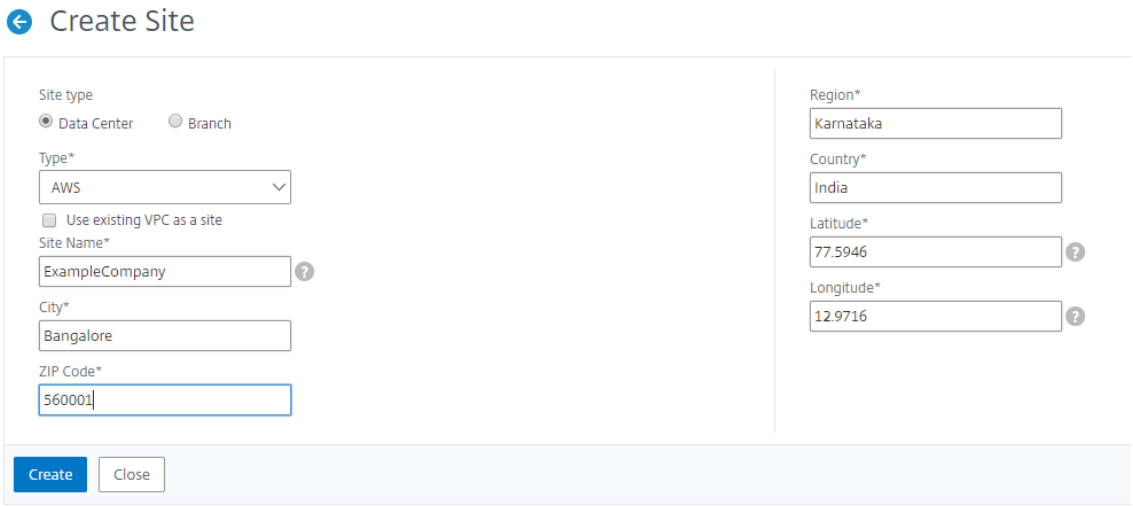
h) 纬度：键入位置的纬度。

对于南纬，请指定负值。示例：`-77.5946`。

i) 经度：键入位置的经度。

对于西经，指定负值。示例：`-12.9716`。

2. 单击创建。



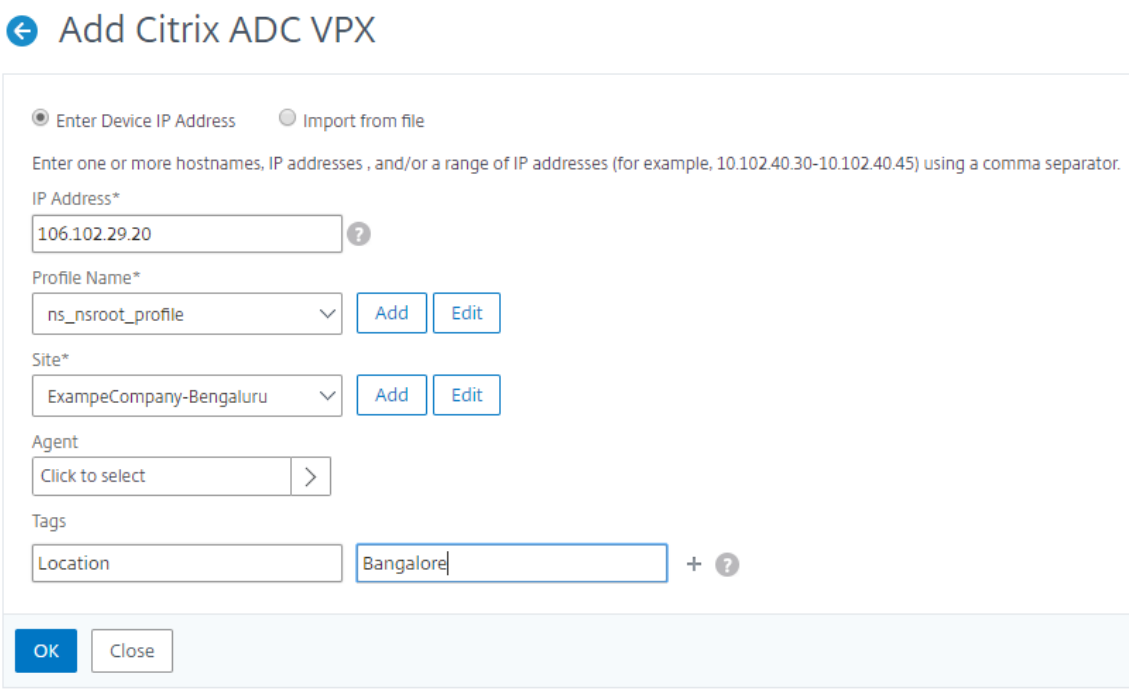
要添加实例并选择站点，请执行以下操作：

创建站点后，必须在 Citrix ADM 中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

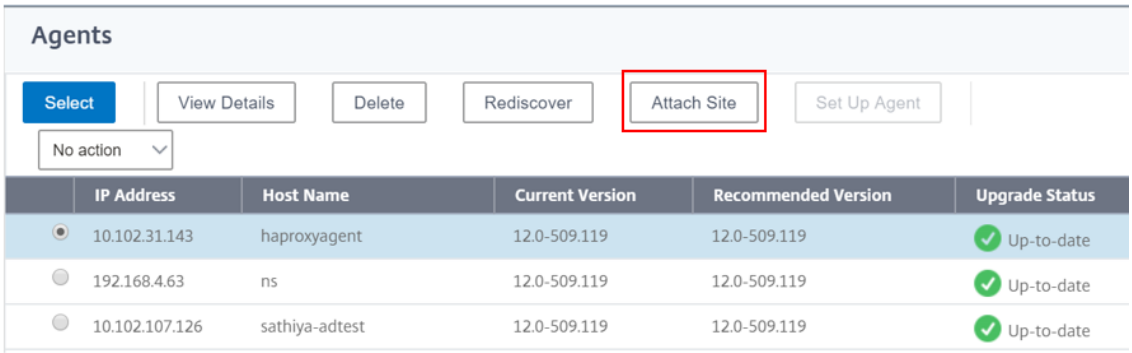
创建站点后，必须在 Citrix ADM 中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

1. 在 Citrix ADM 中，导航到“网络”>“实例”。
2. 选择要创建的实例类型，然后单击 添加。
3. 在 添加 **Citrix ADC VPX** 页面上，键入 IP 地址并从列表中选择配置文件。
4. 从列表中选择站点。您可以单击“站 点”字段旁边的 + 号来创建站点，也可以单击“编辑”图标更改默认站点的详细信息。

5. 单击向右箭头，然后从显示的列表中选择座席。



6. 选择代理后，您必须将代理与站点关联。此步骤允许代理绑定到站点。选择代理并单击 附加站点。



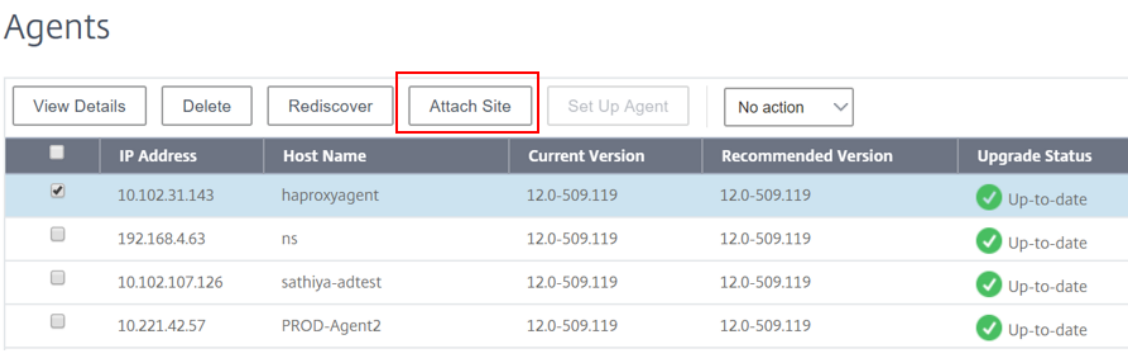
1. 从列表中选择站点，然后单击 保存”。

1. 单击确定。

您也可以通过导航到“网络”>“** 代理”将 代理连接到站点。

要将 **Citrix ADM** 代理与站点关联，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > 客户端。
2. 选择代理，然后单击“附加站点”。



1. 您可以关联网站并单击 保存”。

Citrix ADM 开始监视在班加罗尔站点中添加的 Citrix ADC 实例以及其他两个站点中的实例。

如何创建标记并分配给实例

February 6, 2024

现在，Citrix Application Delivery Management (ADM) 允许您将 Citrix 应用程序 Delivery Controller (ADC) 实例与标签相关联。标签是您可以分配给实例的关键字或单词术语。这些标签添加了有关实例的一些其他信息。可以将标签视为有助于描述实例的元数据。标签允许您根据这些特定关键字对实例进行分类和搜索。您还可以将多个标签分配给单个实例。

以下用例可帮助您了解对实例进行标记将如何帮助您更好地监视实例。

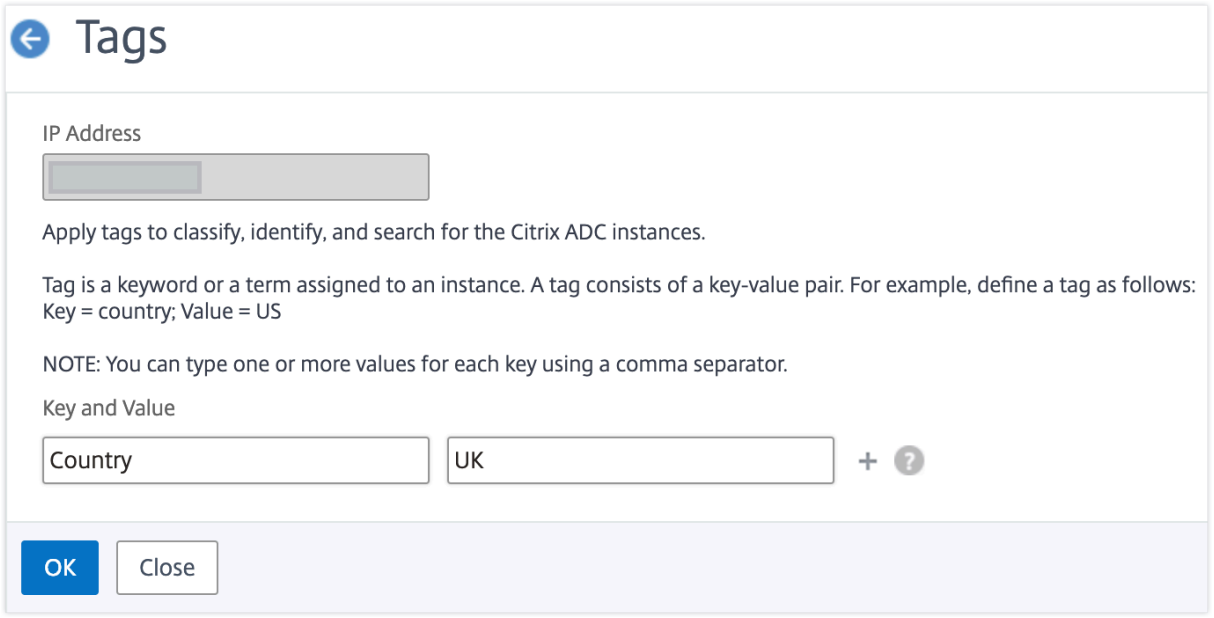
- 使用案例 **1**：您可以创建标记来标识位于英国的所有实例。在这里，您可以创建一个标签，其密钥为“国家”，值为“英国”。此标签可帮助您搜索和监视所有位于英国的实例。
- 使用案例 **2**：您要搜索处于临时环境中的实例。在这里，您可以创建一个标签，其密钥为“目的”，值为“Staging_NS”。此标记可帮助您将正在暂存环境中使用的所有实例与运行客户端请求的实例隔离开来。
- 使用案例 **3**：考虑一种情况，您希望找出位于英国 Swindon 区域并由您 David T. 拥有的 Citrix ADC 实例列表。您可以为所有这些要求创建标签，并将其分配给满足这些条件的所有实例。

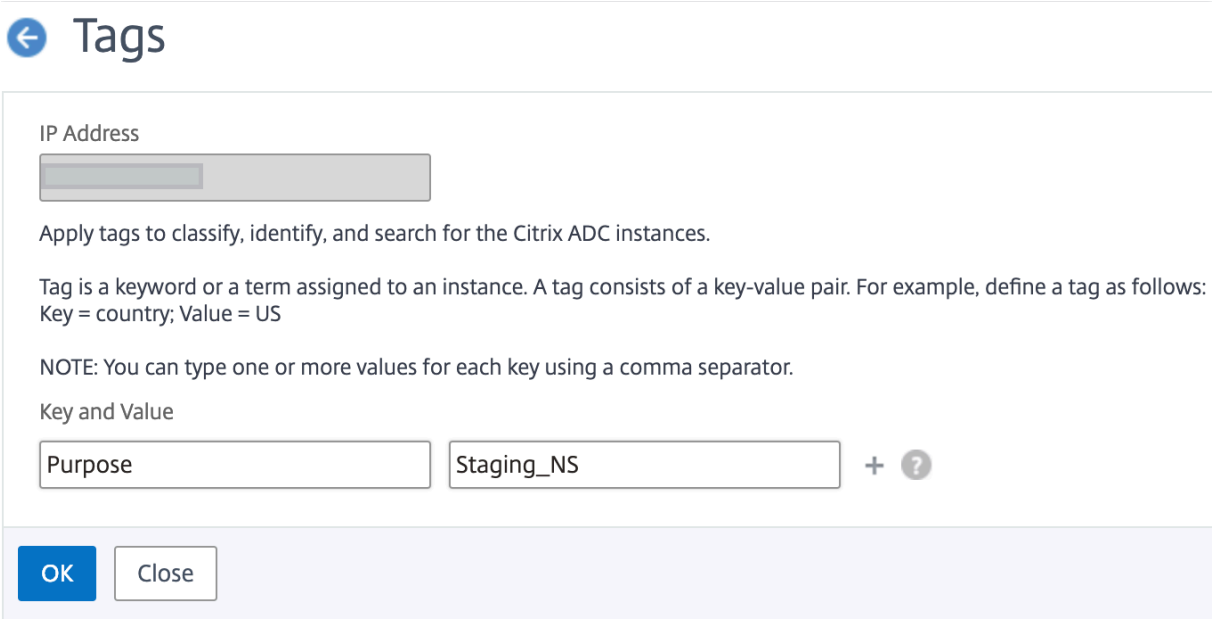
要为 **Citrix ADC VPX** 实例分配标签，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > 实例 > **Citrix ADC** 。
2. 选择 **Citrix ADC VPX** 选项卡。
3. 选择所需的 Citrix VPX。
4. 单击“标签”。
5. 创建标签并单击“确定”。

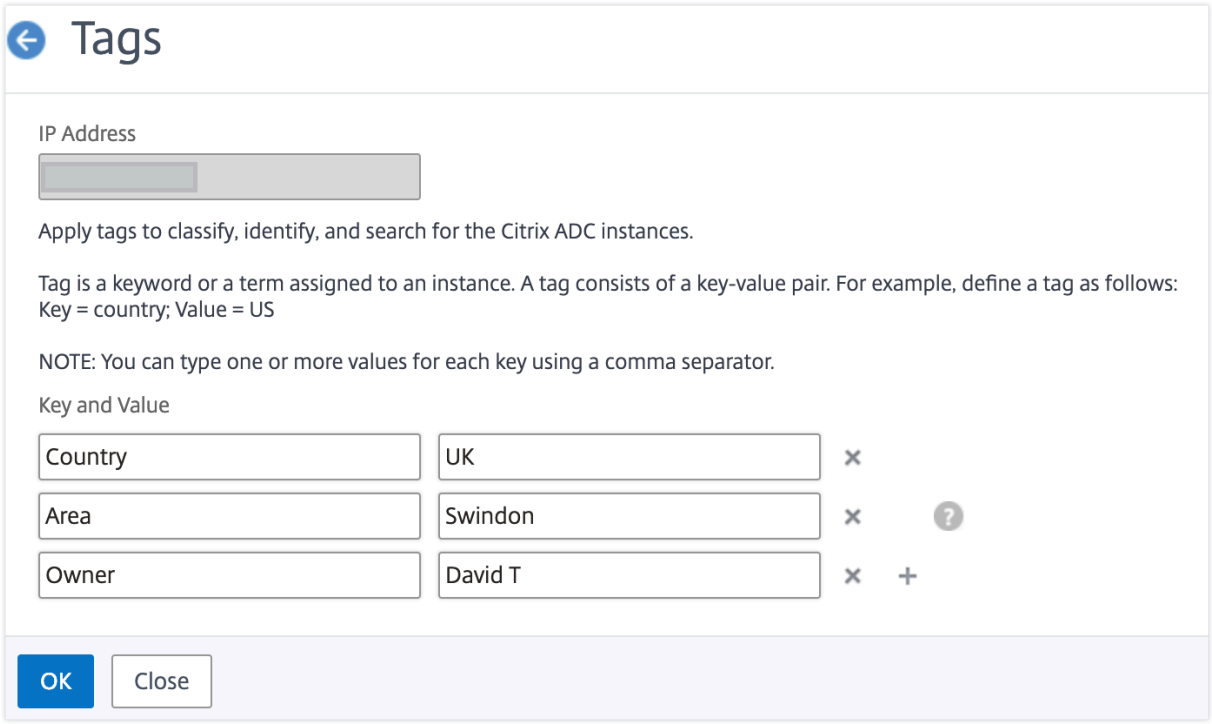
出现的“标签”窗口允许您通过为创建的每个关键字分配值来创建自己的“键值”对。

例如，下图显示了创建的几个关键字及其值。您可以添加自己的关键字并为每个关键字键入一个值。



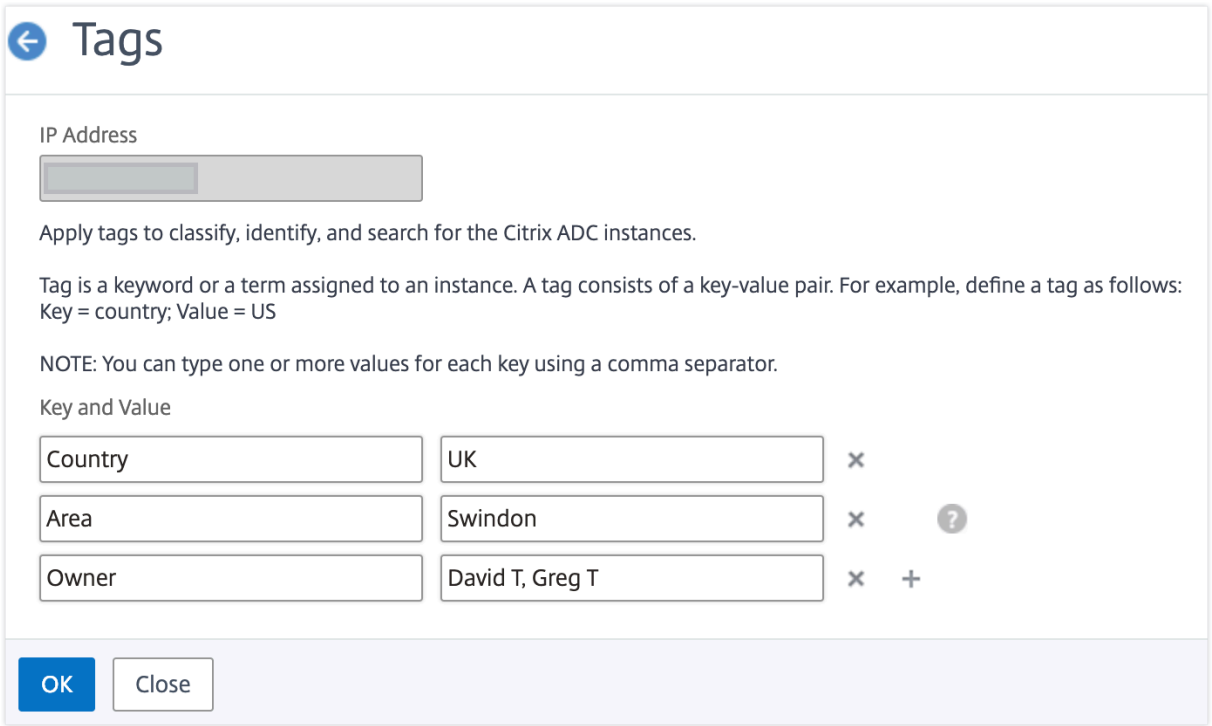


您也可以通过点击“+”添加多个标签。添加多个有意义的标签可让您非常有效地搜索实例。



您可以通过用逗号分隔来向关键字添加多个值。

例如，您正在为另一位同事 Greg T 分配管理员角色。您可以添加他的名字，用逗号分隔。添加多个名称可帮助您按其中一个名称或两个名称进行搜索。Citrix ADM 将逗号分隔的值识别为两个不同的值。



要了解有关如何根据标签搜索实例的更多信息，请参阅 如何使用标签和属性的值搜索实例。

> 注意
>
> 您以后可以添加新标签或删除现有标签。您创建的标签数量没有限制。

如何使用标记和属性的值搜索实例

February 6, 2024

可能存在 Citrix Application Delivery Management (ADM) 管理大量 Citrix ADC 实例的情况。作为管理员，您可能希望灵活地根据特定参数搜索实例清单。Citrix ADM 现在提供了改进的搜索功能，可以根据您在搜索字段中定义的参数搜索 Citrix ADC 实例的子集。您可以根据两个标准（标签和属性）搜索实例。

- 标签。标签是您可以分配给 Citrix ADC 实例的术语或关键字，以添加有关 Citrix ADC 实例的其他描述。现在，您可以将您的 Citrix ADC 实例与标签相关联。这些标签可用于更好地识别和搜索 Citrix ADC 实例。
- 属性。在 Citrix ADM 中添加的每个 Citrix ADC 实例都有一些与该实例关联的默认参数或属性。例如，每个实例都有自己的主机名、IP 地址、版本、主机 ID、硬件模型 ID 等。您可以通过为这些属性中的任何一个指定值来搜索实例。

例如，假设您想要找出版本为 12.0 且处于 UP 状态的 Citrix ADC 实例列表。在这里，实例的版本和状态由默认属性定义。

除了实例的 12.0 版本和 UP 状态外，您还可以搜索您拥有的那些实例。您可以创建一个“所有者”标签并为该标签分配一个值“David T”。有关如何创建和分配标签的更多信息，请参阅如何创建标签并分配到实例。

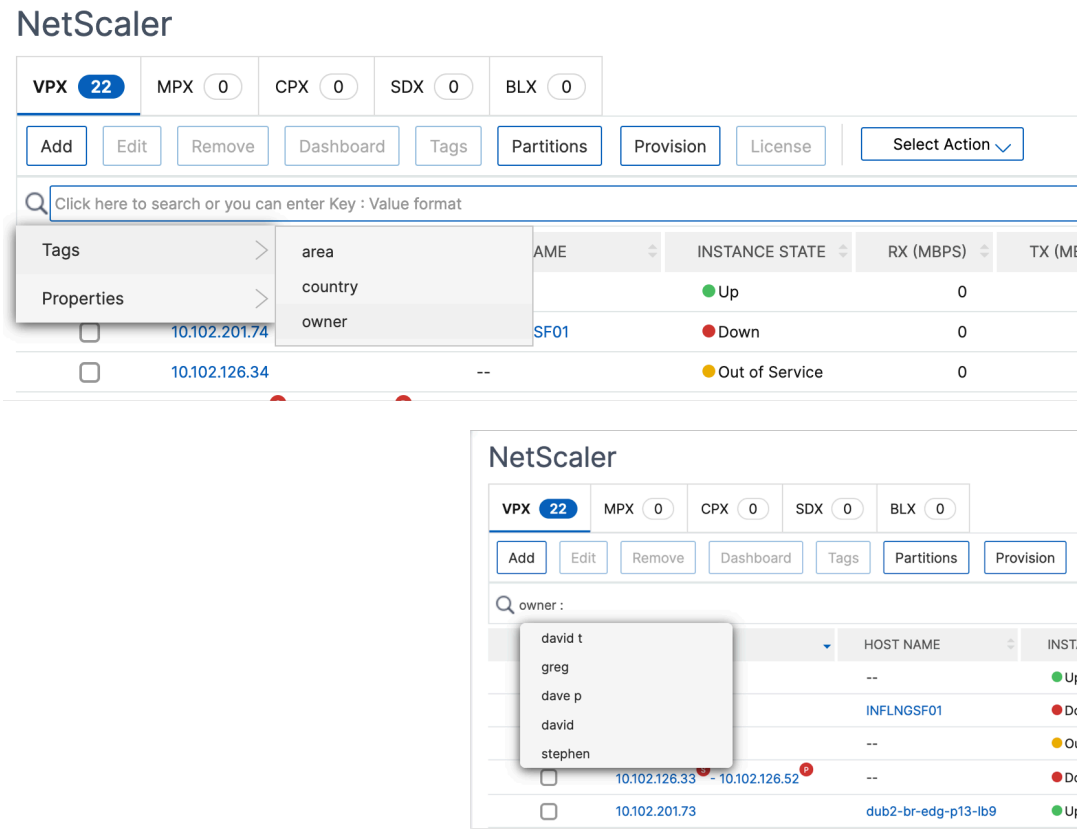
您可以使用标签和属性的组合来创建自己的搜索条件。

搜索 **Citrix ADC VPX** 实例

1. 在 Citrix ADM 中，导航到“网络”>“实例”>“**Citrix ADC**”>“**VPX**”选项卡。
2. 单击搜索字段。您可以使用标签或属性或将两者结合起来来创建搜索表达式。

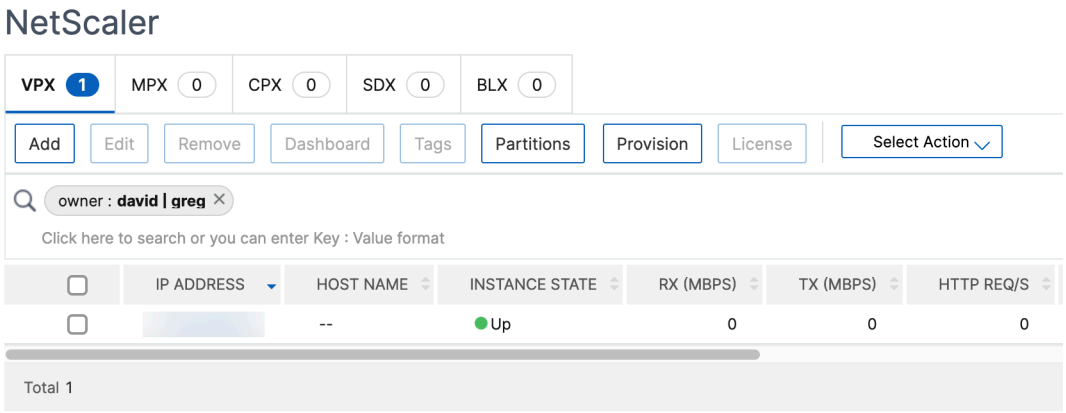
   以下示例显示如何有效地使用搜索表达式来搜索实例。

   a) 选择“标签”选项，然后选择“所有者”。选择“大卫 T.”

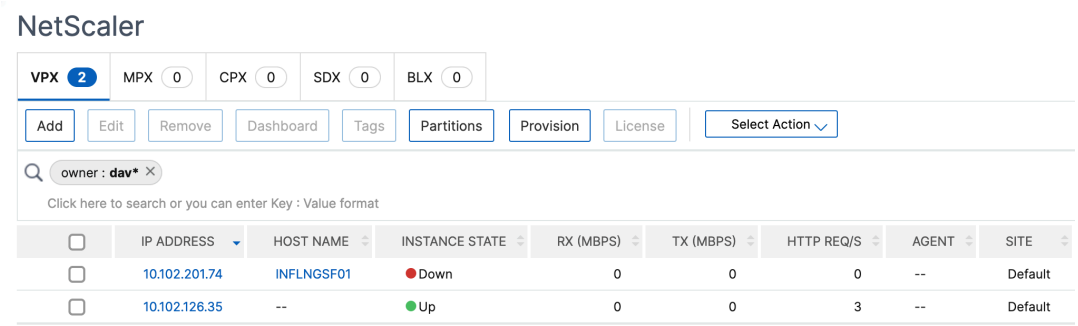


Citrix ADM 支持搜索表达式中的正则表达式和通配符。

b) 您可以使用正则表达式来进一步扩展搜索条件。例如，您要搜索由 David 或 Stephen 拥有的实例。在这种情况下，您可以通过使用“|”表达式分隔值来键入值。



c) 您还可以使用通配符替换或表示一个或多个字符。例如，您可以键入“Dav*”来搜索 David T 和 Dave P 拥有的所有实例。



> 注意有
>
> 关正则表达式和通配符以及如何使用它们的详细信息，请单击搜索栏中的“信息”图标。

管理 **Citrix ADC** 实例的管理分区

February 6, 2024

您可以在 Citrix 应用程序 Delivery Controller (ADC) 实例上配置管理分区，以便在同一 Citrix ADC 实例上为组织中的不同组分配不同的分区。可以分配一个网络管理员来管理多个 Citrix ADC 实例上的多个分区。

Citrix Application Delivery Management (ADM) 提供了从单个控制台管理员拥有的所有分区的无缝方式。您可以在不中断其他分区配置的情况下管理这些分区。

要允许多个用户管理不同的管理分区，您必须创建组，然后将用户和分区分配给这些组。每个用户只能查看和管理用户所属组中的分区。每个管理分区都被视为 Citrix ADM 中的一个实例。当您发现 Citrix ADC 实例时，在该 Citrix ADC 实例上配置的管理分区会自动添加到系统中。

请考虑您有两个 Citrix VPX 实例，并在每个实例上配置了两个分区。例如，Citrix ADC 实例 10.102.216.49 具有分区 1、分区 2 和分区 3，而 Citrix ADC 实例 10.102.29.120 具有 p1 和 p2，如下图所示。

要查看分区，请导航到网络 **>** 实例 **> Citrix ADC > VPX**，然后单击 分区。

您可以为用户分配以下分区：10.102.29.120 分区和 10.102.216.49 分区 1 分区。而且，您可以指定 user-p2 来管理分区 10.102.29.80-p2、102.216.49-Partition_2 和 10.102.216.49-Partition_3。

之后，必须创建两个用户 user-p1 和 user-p2，且必须将用户分配到为其创建的组。

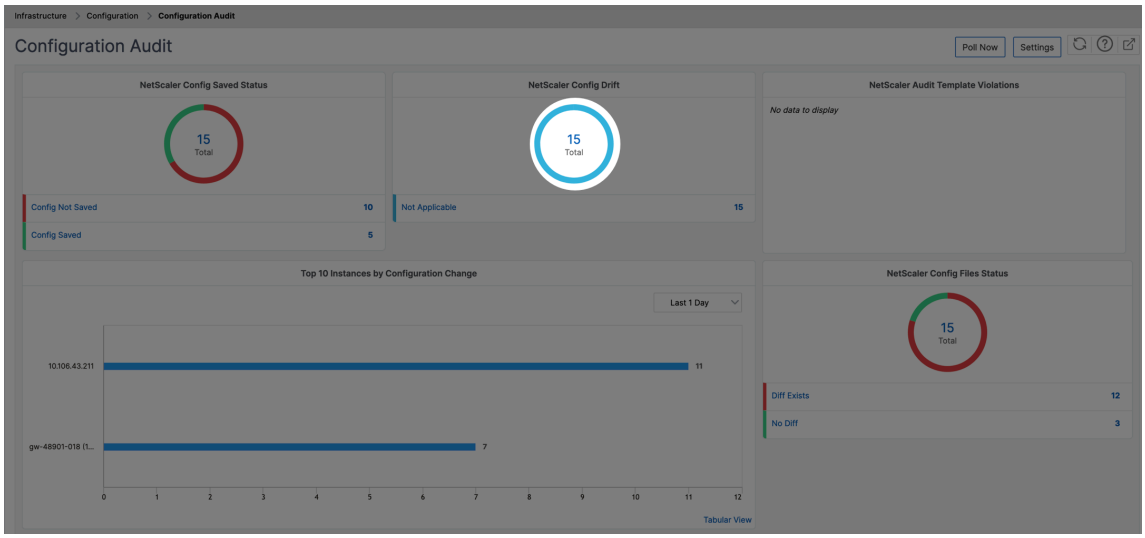
首先，您必须创建两个具有适当权限的组（例如：管理员权限），并在每个组中包含所需的管理员分区实例。例如，创建系统组分区-管理员，然后将 Citrix ADC 管理分区 10.102.29.120-p1 和 10.102.216.49 分区 1 添加到此组中。同时创建系统组分区-管理员，并将 Citrix ADC 管理分区 10.102.29.120-p2、10.102.216.49-分区 2 和 10.102.216.49 分区 3 添加到此组中。

创建管理分区后，您还可以使用修订历史差异功能和管理员分区审核模板功能进行审核

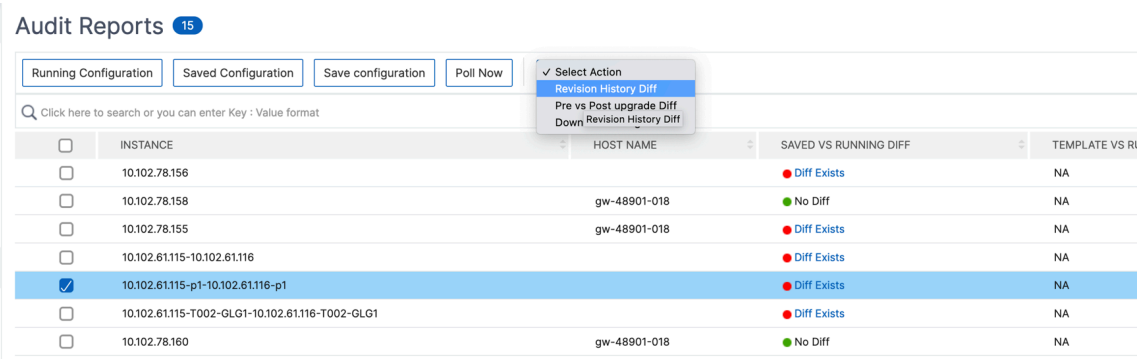
管理分区的修订历史记录差 异允许您查看分区 Citrix ADC 实例的五个最新配置文件之间的差异。您可以将配置文件相互比较（例如配置修订版-1 和配置修订版 -2），也可以将配置文件与当前正在运行/保存的配置与配置修订版进行比较。除了配置的差异外，还显示了校正配置。您可以将所有更正命令导出到本地文件夹并更正配置。

要查看修订历史记录差异，请执行以下操作：

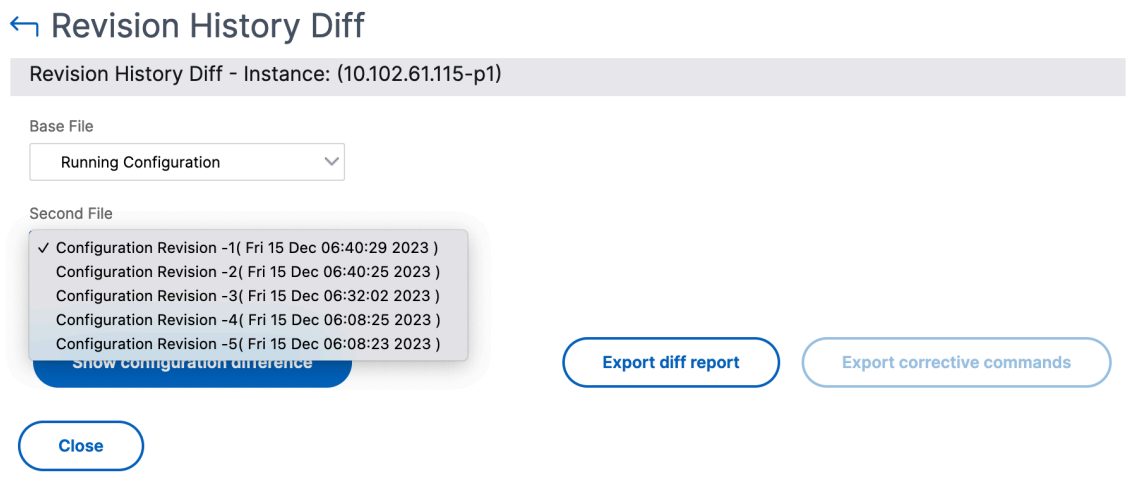
1. 导航到网络 **>** 配置审核。在表示实例配置状态的圆环图中单击。在打开的“审核报告”页中，单击已分区的 Citrix ADC 实例。



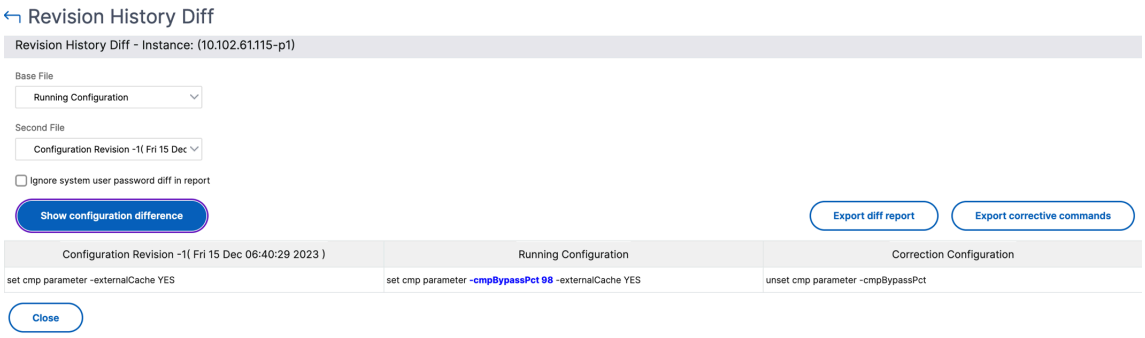
2. 在“操 作”菜单中，单击“修订历史记录比较”。



3. 在 修订历史记录差异 页面上，选择要比较的文件。例如，将保存的配置与配置修订版-1 进行比较，然后单击 显示配置差异。



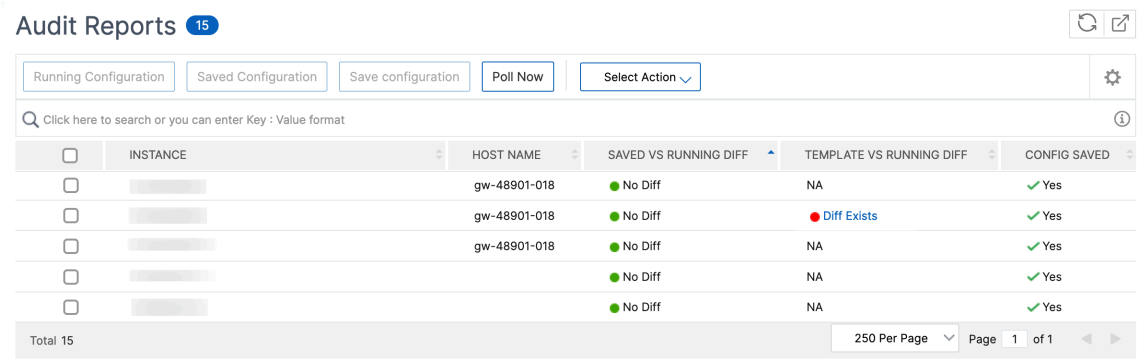
4. 然后，您可以查看所选分区 Citrix ADC 实例的五个最新配置文件之间的差异，如下所示。您还可以查看更正配置命令并将这些更正命令导出到本地文件夹。这些纠正命令是需要在基本文件上执行的命令，以便使配置达到所需状态（用于比较的配置文件）。



分区审核模板 允许您创建自定义配置模板并将其与分区实例关联。审核报告页面的模板与运行差异列显示在 审核报告 页面的 模板与运行差异 列中。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。

要查看模板与运行差异，请执行以下操作：

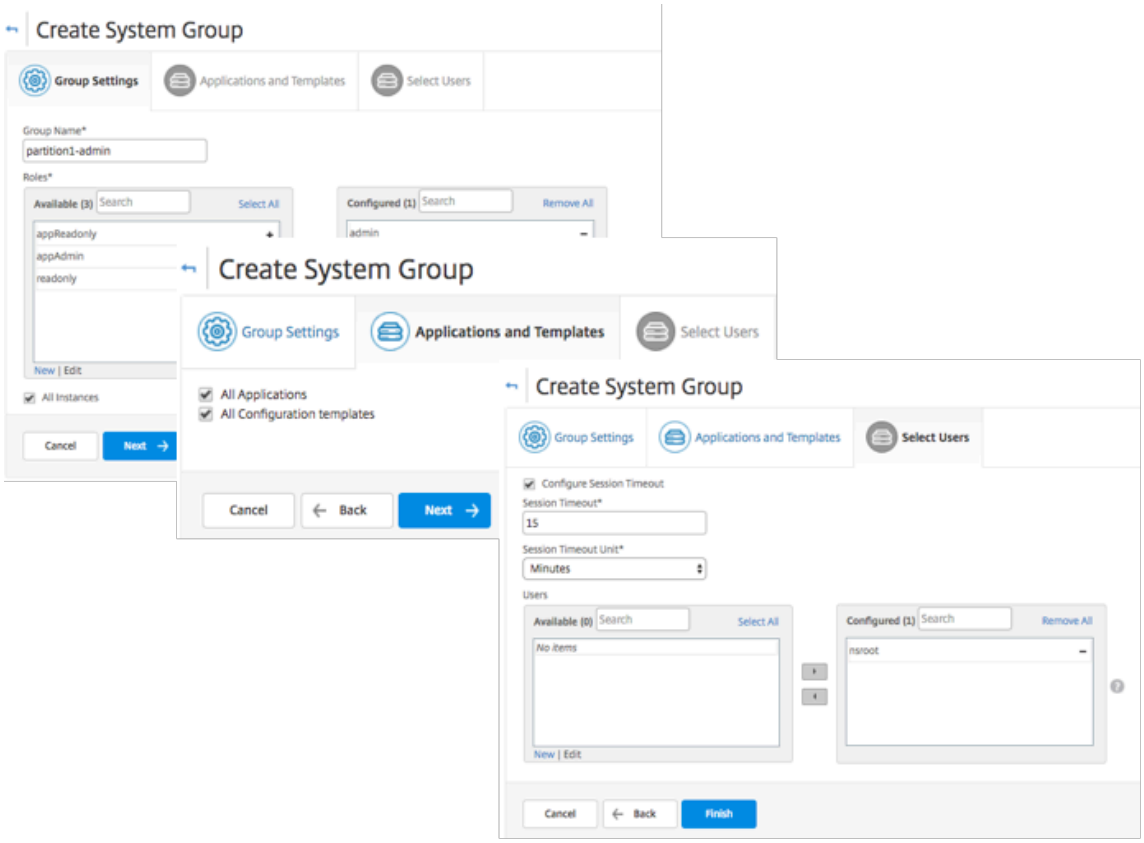
1. 在 审核报告 页面中，单击已分区的 Citrix ADC 实例。



2. 如果审核模板和运行配置之间存在任何差异，则差异显示为超链接。单击超链接可查看差异（如果存在）。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。

要创建组，请执行以下操作：

1. 导航到“系统”>“用户管理”>“组”，然后单击“添加”。
2. 在“创建系统用户”页中，指定以下内容：
   - “组设置”选项卡：输入组名称和角色权限。要允许访问特定实例，请清除“所有实例”复选框，然后在“选择实例”页面上 选择您的实例。
   - “应用程序和模板”选项卡：您可以选择在所有应用程序和配置模板中使用此组。
   - 选择用户 选项卡：选择要添加到此组的用户。您可以单击“可 用”表格中的“** 新 ** 建”链接来创建新用户。（可选）配置会话超时，在此可以配置用户可以保持活动状态的时间期限。
3. 单击完成。



要创建用户：

1. 导航到“系统”>“用户管理”>“用户”，然后单击“添加”。
2. 在“创建系统用户”页上，指定用户名和密码。（可选）您可以启用外部身份验证以及配置会话超时。
3. 通过将“可用”列表中的组名添加到“已配置”列表，将用户分配到组。
4. 单击创建。

现在注销并使用 user-p1 凭据登录。只能查看和管理为您分配的管理分区以进行管理和监视。

备份和还原 **Citrix ADC** 实例

February 6, 2024

您可以备份 Citrix ADC 实例的当前状态，然后使用备份的文件将其恢复到相同的状态。在升级实例之前或出于预防原因，您必须始终备份实例。稳定系统的备份使您能够将其恢复到稳定点，如果系统变得不稳定。

有多种方法可以在 Citrix ADC 实例上执行备份和恢复。您可以使用 GUI 和 CLI 手动备份和还原 Citrix ADC 配置。您还可以使用 Citrix ADM 执行自动备份和手动恢复。

Citrix ADM 使用 NITRO 调用和安全外壳 (SSH) 和安全复制 (SCP) 协议复制托管 Citrix ADC 实例的当前状态。

Citrix ADM 创建完整备份并恢复以下 Citrix ADC 实例类型：

- Citrix SDX
- Citrix VPX
- Citrix MPX

有关更多信息，请参阅 [备份和恢复 ADC 实例]。(https://docs.citrix.com/en-us/citrix-adc/12-1/system/basic-operations/backup-restore-citrix-adc-appliance.html)

> 注意
>
> - 在 Citrix ADM 中，您无法在 Citrix ADC 群集上执行备份和还原操作。
> - 不能使用从一个实例创建的备份文件来还原另一个实例。

备份的文件作为压缩的 TAR 文件存储在以下目录中：

```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

为了避免由于磁盘空间不可用而引起的问题，您可以在此目录中最多保存 50 个备份文件。

要备份和还原 Citrix ADC 实例，必须首先在 Citrix ADM 上配置备份设置。配置设置后，您可以选择单个 Citrix ADC 实例或多个实例，并在这些实例中创建配置文件的备份。如有必要，您还可以使用这些备份的文件还原 Citrix ADC 实例。

配置实例备份设置

使用“实例备份设置”页可以配置 Citrix ADM 上的设置，以备份选定的 Citrix ADC 实例或多个实例：

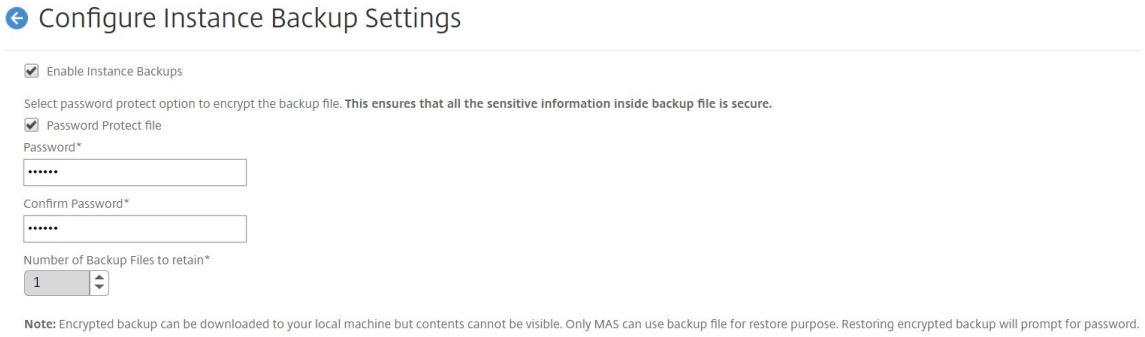
在 Citrix ADM 中，导航到“系统”>“系统管理”。在右侧窗格的“实例设置”下，选择 实例备份设置，然后指定以下内容：

1. 启用实例备份：默认情况下，Citrix ADM 处于启用状态，以备份 Citrix ADC 实例。如果您不想创建实例的备份文件，请清除此选项。
2. 密码保护文件：（可选）选择密码保护选项以加密备份文件。加密备份文件可确保备份文件内的所有敏感信息都是安全的。

   > 注意
   >
   > 您可以将加密的备份文件下载到本地计算机，但无法使用 Citrix ADM GUI 或任何文本编辑器打开该文件。该文件可以单独由 Citrix ADM 检索和使用。还原加密的备份文件时，系统会提示您提供密码。但您可以在您的系统上打开未加密的备份文件。

3. 要保留的备份文件数：指定要在 Citrix ADM 中保留的备份文件数。您最多可以保留 50 个 Citrix ADC 实例当前状态的备份文件。默认是三个备份文件。

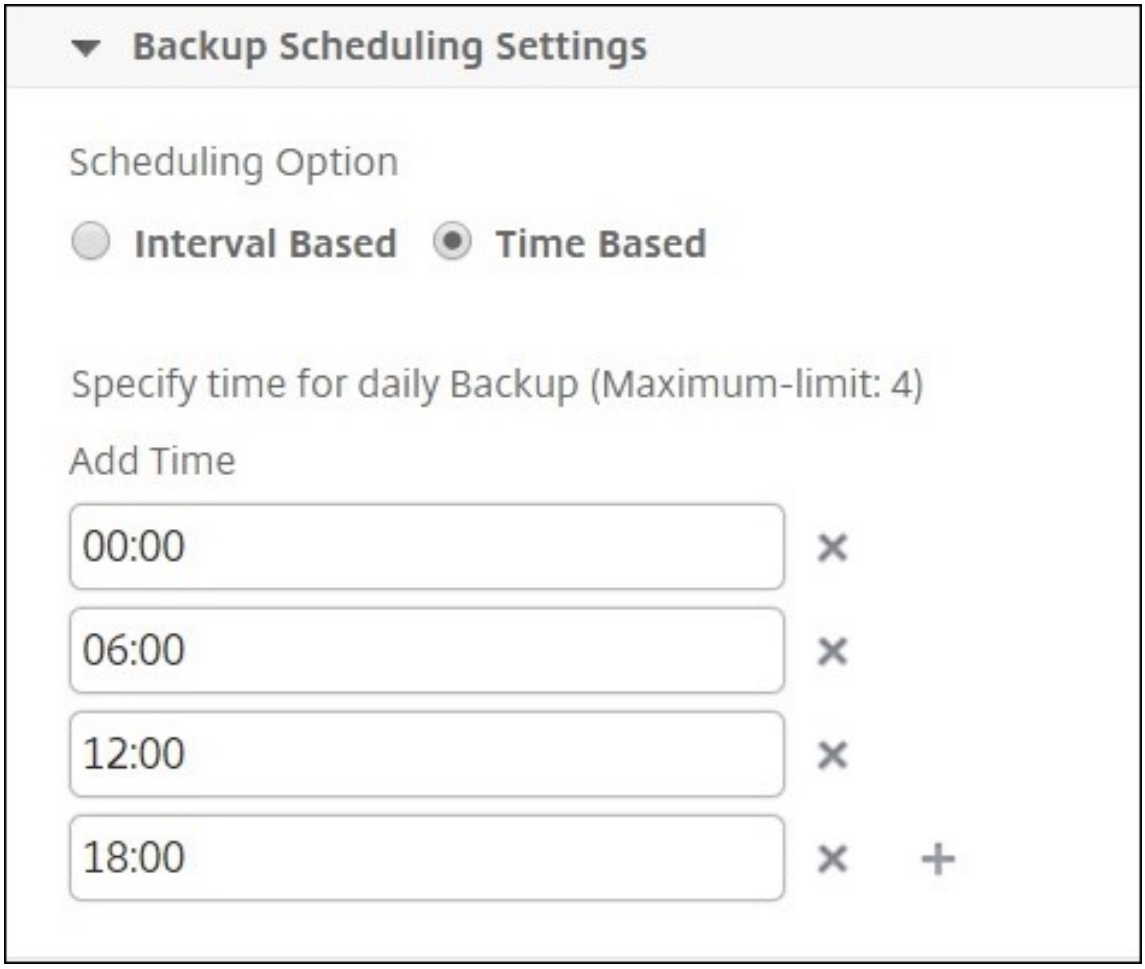
   > 注意
   >
   > 每个备份文件都涉及一定的存储需求。Citrix 建议您根据您的要求在 Citrix ADM 上存储最佳数量的 Citrix ADC 备份文件。



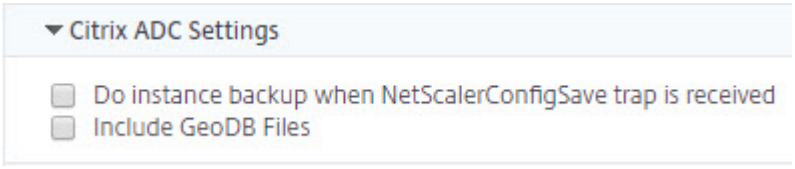
4. 备份计划设置：（可选）有两个选项可用于创建备份文件，但一次只能使用一个选项：

   a) 默认的备份计划选项是“基于间隔”。在指定的时间间隔过后，将在 Citrix ADM 中创建一个备份文件。默认备份时间间隔是 12 小时。

   b) 您还可以将定时备份的类型更改为“基于时间”。在此选项中，以 hours:minutes 格式指定进行备份的时间。Citrix ADM 允许在实例上进行最多四次每日备份。

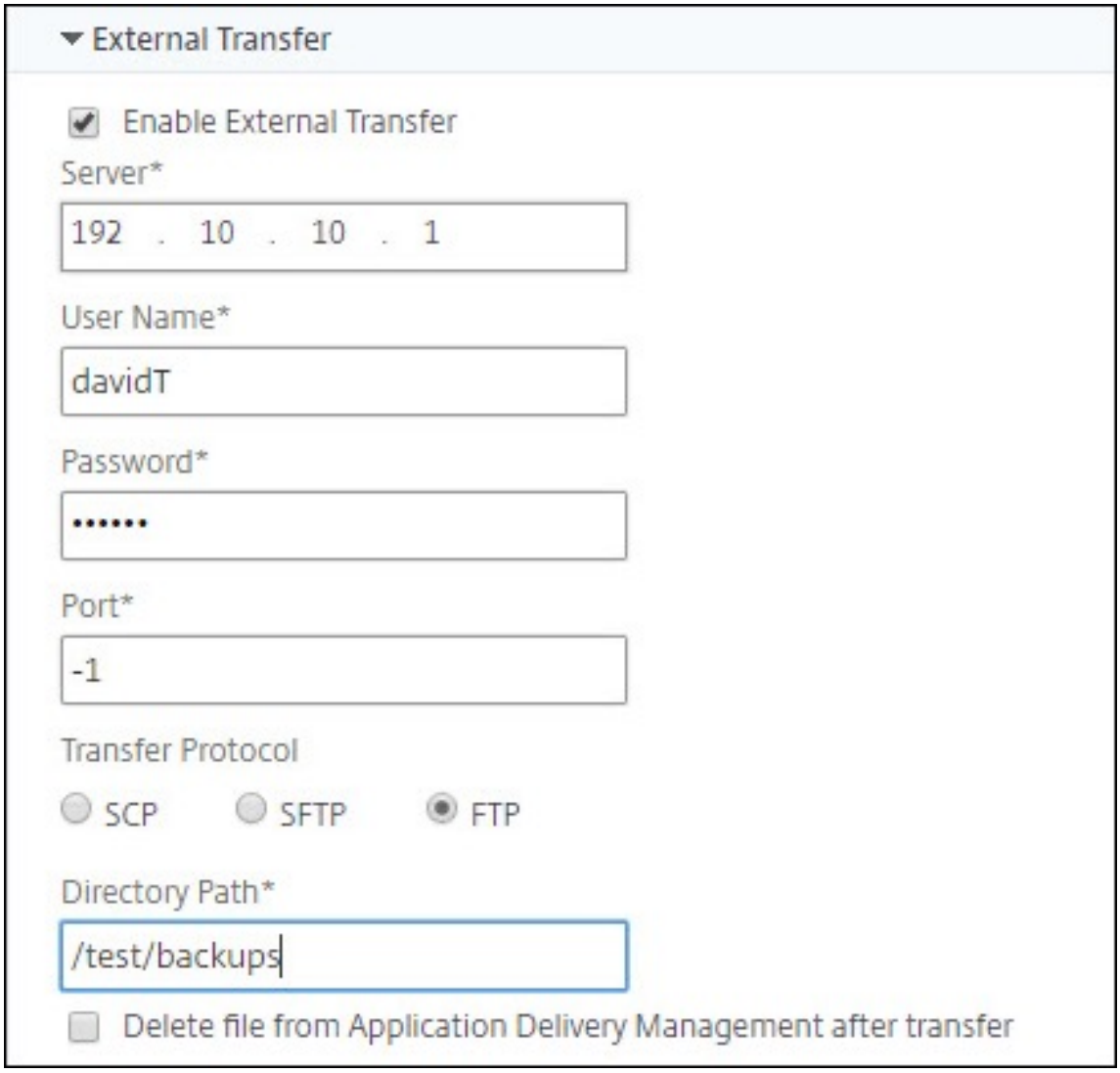


5. **Citrix ADC** 设置：（可选）默认情况下，Citrix ADM 在收到“NetScalerConfigSave”陷阱时不会创建备份文件。但是，每当 Citrix ADC 实例向 Citrix ADM 发送“NetScalerConfigSave”陷阱时，您都可以启用创建备份文件的选项。Citrix ADC 实例每次保存实例上的配置时都会发送“NetScalerConfigSave”。
6. 地理数据库文件：（可选）默认情况下，Citrix ADM 不备份地理数据库文件。您也可以启用该选项以创建这些文件的备份。



7. 外部传输：（可选）Citrix ADM 允许您将 Citrix ADC 实例备份文件传输到外部位置：
   a) 指定位置的 IP 地址。
   b) 指定要将备份文件传输到的外部服务器的用户名和密码。
   c) 指定传输协议和端口号。
   d) 您可以指定需要存储文件的目录路径。

e) 在将备份文件传输到外部服务器后，您还可以选择将其从 Citrix ADM 中删除。



> 注意
>
> 当任何选定的 Citrix ADC 实例出现备份失败时，Citrix ADM 会向自身发送 SNMP 陷阱或系统日志通知。

使用 **Citrix ADM** 为选定的 **Citrix ADC** 实例创建备份

如果要备份选定的 Citrix ADC 实例或多个实例，请执行以下任务：

1. 在 Citrix ADM 中，导航到“网络”>“实例”。在“实例”下，选择要在屏幕上显示的实例类型（例如 Citrix VPX）。
2. 选择要备份的实例。
   - 对于 MPX 和 VPX 实例，从“选择操作”列表中选择“备份/恢复”。
   - 对于 SDX 实例，请单击 备份/恢复。

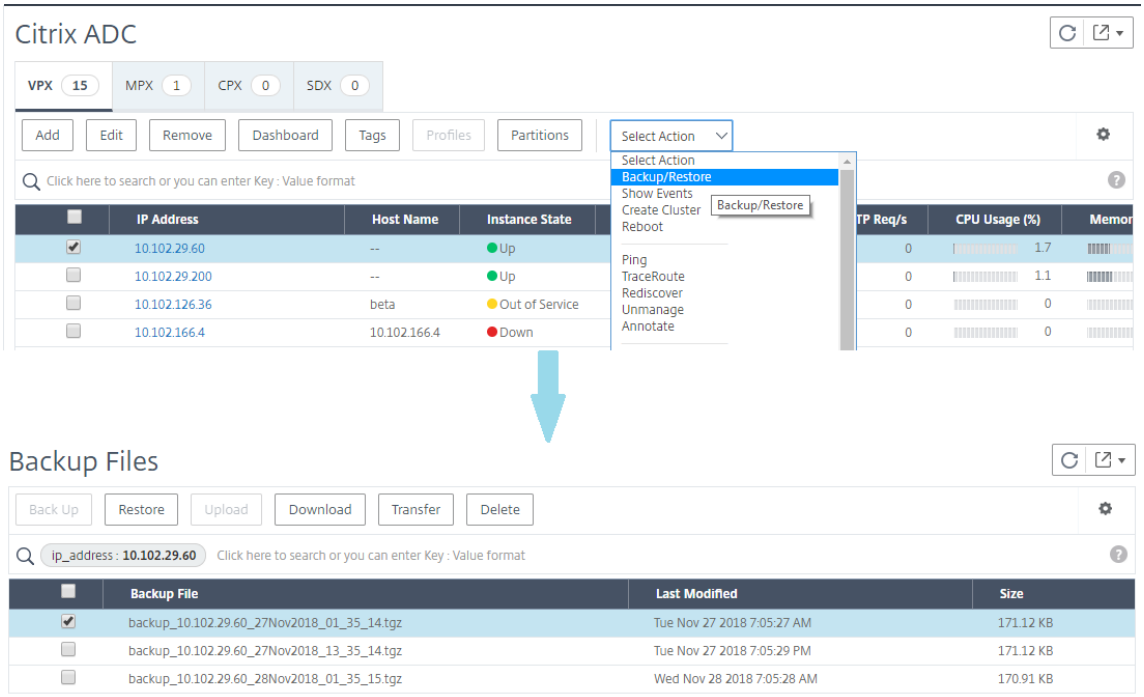
3. 在“备份文件”页上，单击“备份”。
4. 您可以指定是否加密备份文件以提高安全性。您可以输入密码，也可以使用之前在 实例备份设置页面上指定的全局密码。
5. 单击 继续。

使用 **Citrix ADM** 还原 **Citrix ADC** 实例

> 注意：
>
> 如果您在 HA 对中有 Citrix ADC 实例，则需要注意以下几点：
>
> - 恢复创建备份文件的同一个实例。例如，让我们考虑一下从 HA 对的主实例中获取备份的情况。在还原过程中，确保您恢复的是同一个实例，即使它不再是主实例。
> - 当您在主 ADC 实例上启动还原过程时，您无法访问主实例，辅助实例将更改为 **STAYSECONDARY**。在主实例上完成还原过程后，辅助 ADC 实例将从 **STAYSECONDARY** 更改为 **ENABLED** 模式，并再次成为 HA 对的一部分。在还原过程完成之前，您可以预期主实例可能会停机。

执行此任务可通过使用您之前创建的备份文件还原 Citrix ADC 实例：

1. 导航到“网络”>“** 实例”，选择要还原的实例，然后单 击“查看 ** 备份”。
2. 在“备份文件”页上，选择包含要还原的设置的备份文件，然后单击还原。



使用 **Citrix ADM** 恢复 **Citrix ADC SDX** 装置

在 Citrix ADM 中，Citrix ADC SDX 设备的备份包括以下内容：

- 设备上托管的 Citrix ADC 实例
- SVM SSL 证书和密钥
- 实例删除设置（XML 格式）
- 实例备份设置（XML 格式）
- SSL 证书轮询设置（XML 格式）
- SVM 数据库文件
- SDX 上存在的设备的 Citrix ADC 配置文件
- Citrix ADC 构建映像
- Citrix ADC XVA 图像，这些图像存储在以下位置：
  `/var/mps/sdx_images/`
- SDX 单捆绑包映像 (SVM+XS)
- 第三方实例映像（如果已预配）

您必须将 Citrix ADC SDX 设备恢复到备份文件中可用的配置。在设备还原过程中，会删除整个当前配置。

如果要使用其他 Citrix ADC SDX 设备的备份还原 Citrix ADC SDX 设备，请确保在启动还原过程之前添加许可证并配置设备的管理服务网络设置以匹配备份文件中的设置。

确保已备份的 Citrix ADC SDX 平台变体与您尝试还原的变体相同。不能从另一个平台变体还原。

> 注意：
>
> 在恢复 SDX RMA 装置之前，请确保备份版本与 RMA 版本相同或更高。

要从备份文件中恢复 SDX 装置，请执行以下操作：

1. 在 Citrix ADM GUI 中，导航到 网络 **>** 实例 **> Citrix ADC**。
2. 点击 备份**/**还原。
3. 选择要恢复的同一个实例的备份文件。
4. 单击“重新打包备份”。

   备份 SDX 设备时，XVA 文件和图像将分开存储，以节省网络带宽和磁盘空间。因此，在恢复 SDX 设备之前，必须重新打包备份的文件。

   当您重新打包备份文件时，它会将所有备份文件包含在一起以恢复 SDX 设备。重新打包的备份文件可确保成功恢复 SDX 设备。
5. 选择重新打包的备份文件，然后单击“恢复”。

强制故障转移到辅助 **Citrix ADC** 实例

February 6, 2024

例如，如果您需要更换或升级主 Citrix Application Delivery Controller (ADC) 实例，则可能需要强制进行故障转移。可以从主要实例或辅助实例强制执行故障转移。对主要实例强制执行故障转移时，主要实例变为辅助实例，而辅助实例变为主要实例。仅当主要实例可以确定辅助实例处于“UP”（运行）状态时才有可能执行强制故障转移。

强制故障转移不会传播，也不会同步。要在执行强制故障转移后查看同步状态，可以查看实例的状态。

在下列任何一种情况下，强制故障转移会失败：

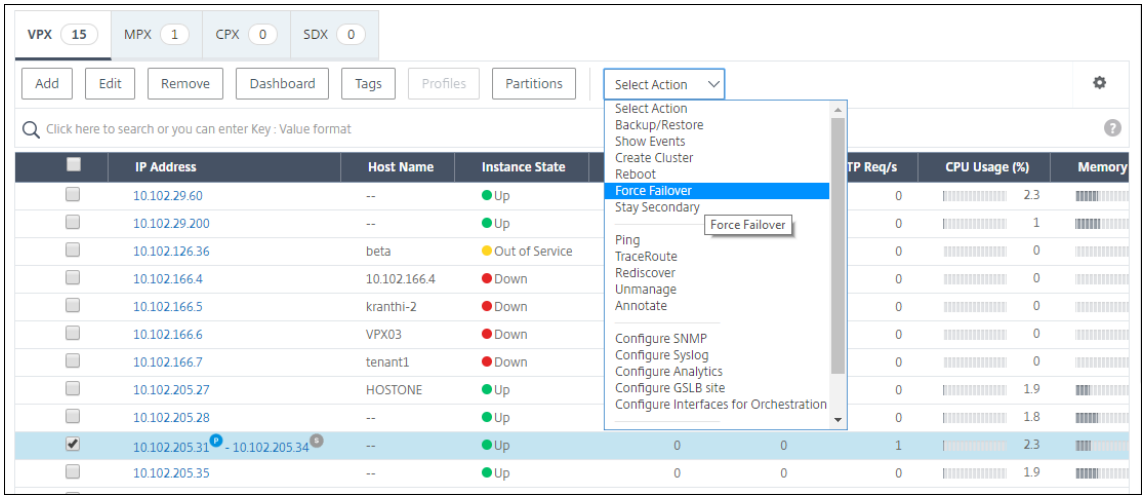
- 在独立的系统上强制执行故障转移。
- 辅助实例处于禁用或非活动状态。如果辅助实例处于非活动状态，必须等待其状态变为“UP”（运行）时才能强制执行故障转移。
- 辅助实例配置为保持辅助状态。

如果 Citrix ADC 实例在您运行强制故障转移命令时检测到潜在问题，则会显示一条警告消息。该消息包括触发警告的信息，并在继续之前要求确认。

可以对主要实例或辅助实例强制执行故障转移。

要使用 **Citrix ADM** 强制故障切换到辅助 **Citrix ADC** 实例，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到“网络”>“实例”>“**Citrix ADC**”>“**VPX**”选项卡，然后选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 从“操作”菜单中选择“强制故障转移”。
4. 单击 **Yes**（是）确认强制执行故障转移操作。



强制辅助 **Citrix ADC** 实例保持辅助状态

February 6, 2024

在 HA 设置中，辅助节点可以被强制保持辅助状态，无论主节点的状态为何。

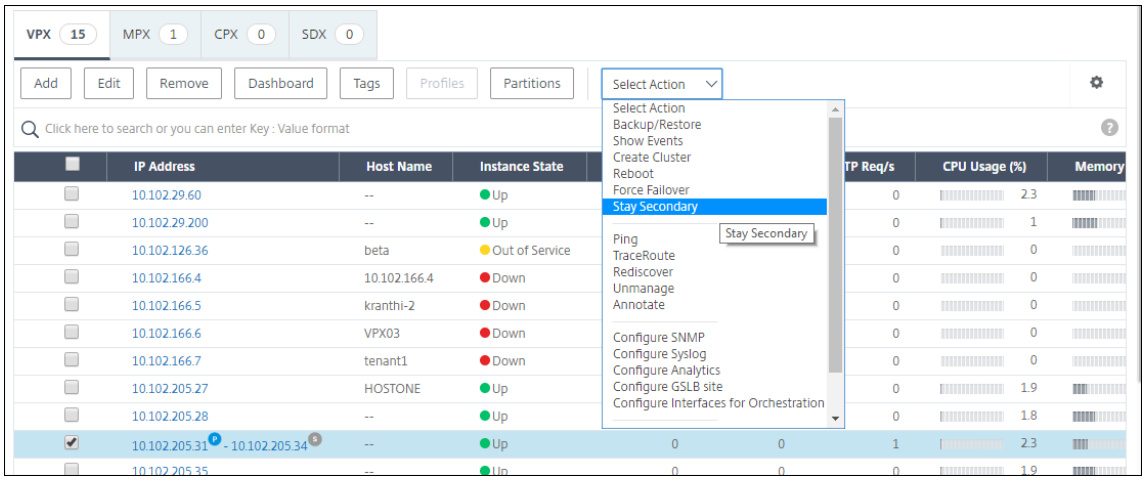
例如，假定主节点需要升级，该过程需要数秒。在升级过程中，主节点可能关闭数秒，但您不希望辅助节点接管，而是希望其保持为辅助节点，即使它检测到主节点上发生故障。

如果强制辅助节点保持辅助状态，即使主节点关闭，它仍将保持辅助状态。此外，如果强制使 HA 对中一个节点状态保持辅助状态，它将不会参与 HA 状态计算机转换。该节点的状态显示为 STAYSECONDARY。

> 注意
>
> 强制系统保持辅助状态时，强制过程不会传播或同步。它仅影响对其运行命令的节点。

要使用 **Citrix ADM** 配置辅助 **Citrix ADC** 实例保持辅助实例，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “网络” > “实例” > “**Citrix ADC**” > “**VPX**” 选项卡，然后选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 从 “操作” 菜单中选择 “保持辅助状态”。
4. 单击 **Yes**（是）确认执行 “Stay Secondary”（保持辅助状态）操作。



创建实例组

February 6, 2024

要创建实例组，必须先将所有 Citrix Application Delivery Controller (ADC) 实例添加到 Citrix Application Delivery Management (ADM)。成功添加了实例后，根据其设备系列创建实例组。通过创建实例组，可以对已分组的所有实例同步执行升级、备份和还原等操作，而不是对每个实例单独执行这些操作。

要使用 **Citrix ADM** 创建实例组，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“实例组”，然后单击“添加”。
2. 为您的实例组命名，然后从列表中选择实例系列。
3. 从“实例 系列”菜单中选择实例 类型。
4. 单击“选择实例”，然后从滑入的窗口中选择实例。
5. 单击创建。

重新发现多个 **Citrix VPX** 实例

February 6, 2024

现在，您可以在 Citrix Application Delivery Management (ADM) 设置中重新发现多个 Citrix VPX 实例。以前，您只能重新发现单个 Citrix VPX 实例。当您想要查看多个 Citrix VPX 实例的最新状态和配置时，您可以重新发现这些实例。Citrix ADM 服务器将重新发现所有 Citrix VPX 实例，并检查 Citrix 应用程序 Delivery Controller (ADC) 实例是否可访问。

要重新发现多个 **Citrix VPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 服务器的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。默认管理员凭据为 nsroot 和 nsroot。
3. 导航到“网络”>“实例”>“**Citrix ADC**”>“**VPX**”选项卡，然后选择要重新发现的实例。
4. 在“选择操作”菜单中，单击“重新发现”。
5. 当显示运行“重新发现”实用程序的确认消息时，单击 是”。

   屏幕将报告每个 Citrix VPX 实例的重新发现进度。

取消托管实例

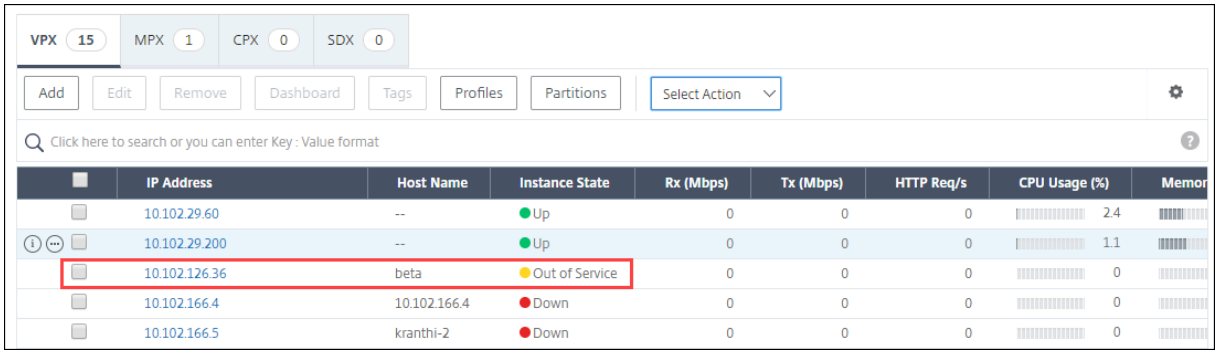
February 6, 2024

如果要停止 Citrix Application Delivery Management (ADM) 和网络中的实例之间的信息交换，则可以取消管理这些实例。

要取消管理实例，请执行以下操作：

导航到“网络”>“实例”>“**Citrix ADC**”>“**VPX**”选项卡。在实例列表中，右键单击某个实例，然后选择取 消管理，或选择该实例，然后从“选择操作”列表中选择“取 消管理”。

所选实例的状态将更改为“停止服务”，如下图所示。



该实例不再由 Citrix ADM 管理，也不再与 Citrix ADM 交换数据。

跟踪到实例的路由

February 6, 2024

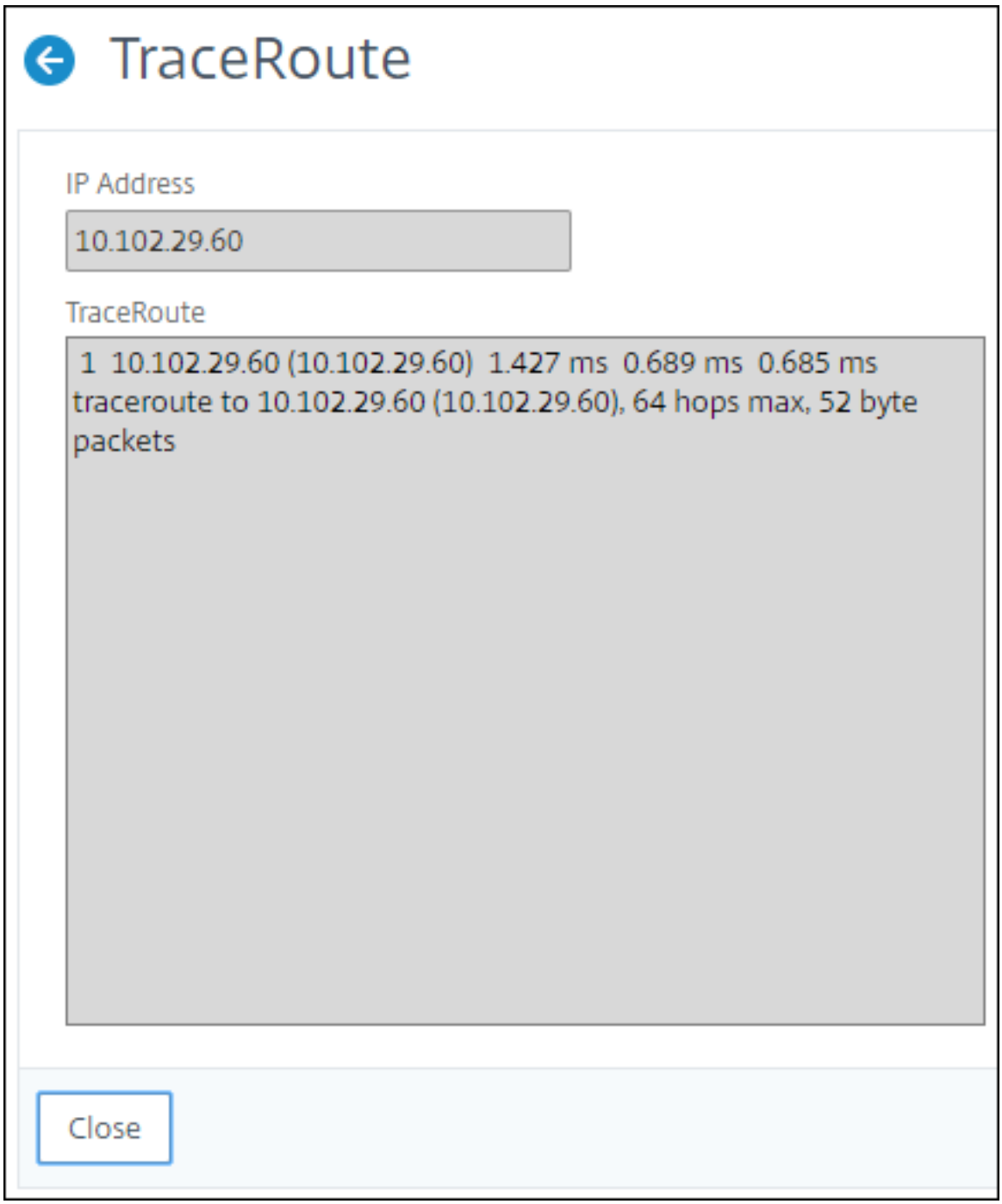
通过跟踪数据包从 Citrix Application Delivery Management (ADM) 到实例的路由，您可以找到到达实例所需的跳数等信息。Traceroute 会跟踪数据包从源到目标的路径。它显示网络跃点列表以及路由中每个实体的主机名和 IP 地址。

Traceroute 也记录数据包从一个跃点传输到另一个跃点所用时间。如果在数据包传输中有任何中断，路由跟踪会显示问题所在位置。

要跟踪实例的路由，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“实例”>“**Citrix ADC**”>“**VPX**”选项卡。
2. 在实例列表中，右键单击某个实例，然后选择 T **racerOute** 或选择该实例，然后从“选择操 作”菜单中单击 T **racerUte**。

“TraceRoute”（路由跟踪）消息框将显示实例的路由以及每个跃点所用时间（以毫秒为单位）。



事件

February 6, 2024

将 Citrix 应用程序 Delivery Controller (ADC) 实例的 IP 地址添加到 Citrix Application Delivery Management

(ADM) 时，Citrix ADM 会发送一个 NITRO 调用，并隐式地将自身添加为实例接收陷阱或事件的陷阱目标。

事件表示托管 Citrix ADC 实例上发生的事件或错误。例如，当发生系统故障或配置更改时，系统会在 Citrix ADM 服务器上生成并记录事件。Citrix ADM 中接收的事件显示在“事件摘要”页面（“网络”>“事件”）中，所有活动事件都显示在“事件消息”页面（“网络”>“事件”**>**“事件消息”）中。

Citrix ADM 还会检查在实例上生成的事件，以形成不同严重级别的警报，并将其显示为消息，其中一些可能需要立即关注。例如，系统故障可能分类为“Critical”（严重）事件严重性，并需要立即解决。

可以配置规则以监视特定事件。规则使监视在 Citrix ADC 基础架构中生成的大量事件变得更加容易。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的过滤条件时，将执行与规则关联的操作。您可以创建筛选器的条件包括：严重性、Citrix ADC 实例、类别、故障对象、配置命令和消息。

您还可以确保在特定的时间间隔内针对某个事件触发多个通知，直到事件被清除。此外，您可以为您的电子邮件自定义特定主题行、用户消息以及上载附件。

使用事件控制板

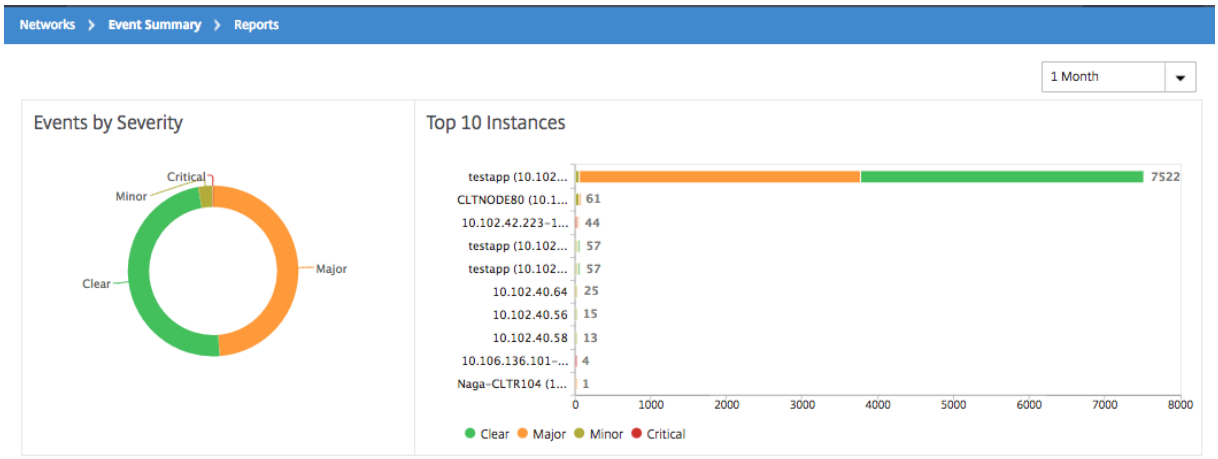
February 6, 2024

作为网络管理员，您可以查看 Citrix Application Delivery Controller (ADC) 实例上的配置更改、登录条件、硬件故障、阈值违规和实体状态更改等详细信息，以及特定实例上的事件及其严重性。您可以使用 Citrix Application Delivery Management (ADM) 的事件控制板查看针对所有 Citrix ADC 实例的关键事件严重性详细信息生成的报告。

要查看事件控制板上的详细信息：

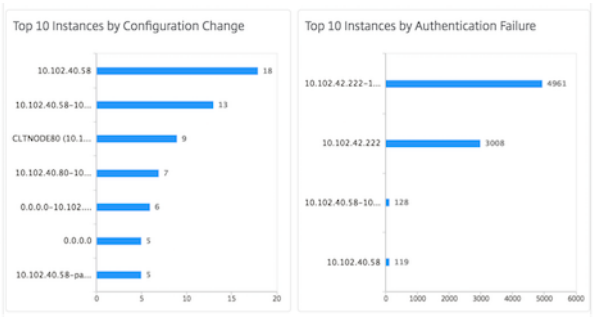
导航到 网络 > 事件 > 报表。

控制板上的“Top 10 Devices”（前 10 位的设备）图中显示按实例上生成的事件数排在前 10 位的实例的报告。可以单击图上某个实例查看事件严重性的进一步详细信息。

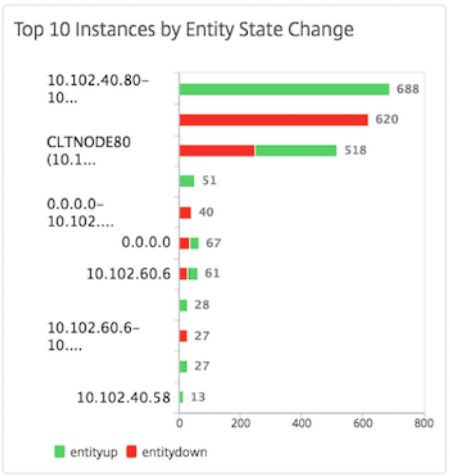


您可以导航到 Citrix ADC 实例类型（网络 > 事件 > 报告 > **NetScaler/ NetScaler SDX/ NetScaler SD-WAN WO**）以查看以下内容，以查看更多详细信息：

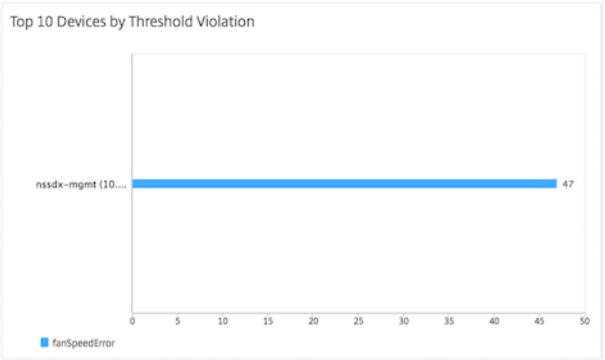
- Top 10 devices by hardware failure（按硬件故障排在前 10 位的设备）
- Top 10 devices by configuration change（按配置变更排在前 10 位的设备）
- Top 10 devices by authentication failure（按身份验证失败排在前 10 位的设备）



- Top 10 devices by entity state changes（按实体状态变化排在前 10 位的设备）



- Top 10 devices by threshold violation（按阈值违反排在前 10 位的设备）



设置事件的事件期限

February 6, 2024

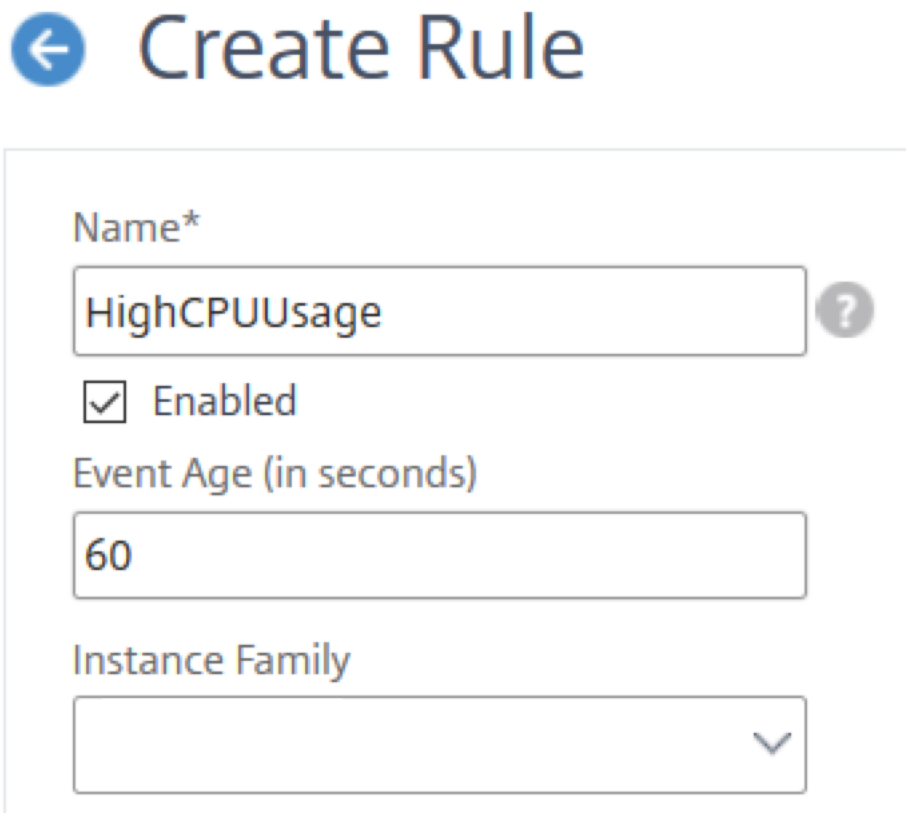
您可以设置事件时间选项来指定时间间隔（以秒为单位）。Citrix ADM 会监视设备直到设置的持续时间，并且只有在事件持续时间超过设定的持续时间时才生成事件。

> 注意：
>
> 事件持续时间的最小值为 60 秒。如果将“事 件时 间”字段保留为空，则事件发生后立即应用事件规则。

例如，假设您想要管理各种 ADC 设备，并在任何虚拟服务器停机 60 秒或更长时间时通过电子邮件收到通知。您可以创建具有必要筛选器的事件规则，并将规则的事件期限设置为 60 秒。然后，每当虚拟服务器关闭 60 秒或更长时间时，您将收到一封电子邮件通知，其中包含实体名称、状态更改和时间等详细信息。

要在 **Citrix ADM** 中设置事件期限，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“事件”>“** 规则”，然后单击“添加 **”。
2. 在 **Create Rule**（创建规则）页面上，设置规则参数。
3. 指定事件期限（以秒为单位）。



确保在“类别”部分中设置所有共同相关陷阱，并在设置事件年龄时在“严 重性”部分中设置相应的严重性。在上面的示例中，选择实体、实体和实体陷阱。

安排事件过滤器

February 6, 2024

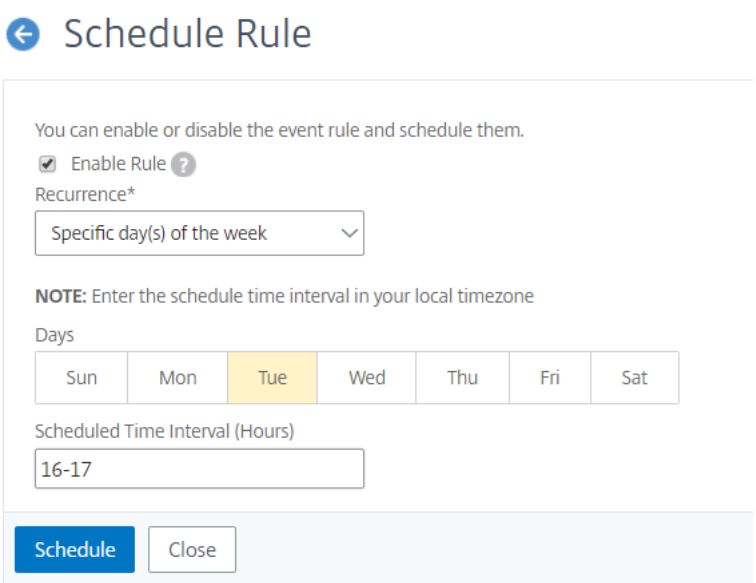
为规则创建筛选器后，如果不希望 Citrix Application Delivery Management (ADM) 服务器在每次生成的事件满足筛选条件时发送通知，则可以将筛选器安排为仅在特定时间间隔（如每日、每周或每月）触发。

例如，如果为实例上的不同应用程序计划了在不同时间进行系统维持活动，实例可能会生成多个警报。

如果您为这些警报配置了筛选器，并为这些筛选器启用了电子邮件通知，服务器会在 Citrix ADM 收到这些陷阱时发送大量电子邮件通知。如果希望服务器仅在特定的时间段发送这些电子邮件通知，可以通过计划过滤器来实现。

要使用 **Citrix ADM** 计划筛选器，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > 事件 > 规则。
2. 选择要为其计划过滤器的规则，并单击 **View Schedule**（查看计划）。
3. 在 **Scheduled Rule**（计划的规则）页面上，单击 **Schedule**（计划）并指定以下参数：
   - **Enable Rule**（启用规则）- 选中此复选框以启用计划的事件规则。
   - **Recurrence**（定期循环）- 计划规则的时间间隔。选择一周中的特定日期或一个月中的特定日期。
   - 天：选择一周中的哪一天来运行规则。您可以选择多天。
   - 日期：输入日期。可以键入多个日期作为逗号分隔值。
   - 计划时间间隔 **(**小时**)** —小时，计划规则的时间（使用 24 小时格式）。
4. 单击 **Schedule**（计划）。



为事件设置重复的电子邮件通知

February 6, 2024

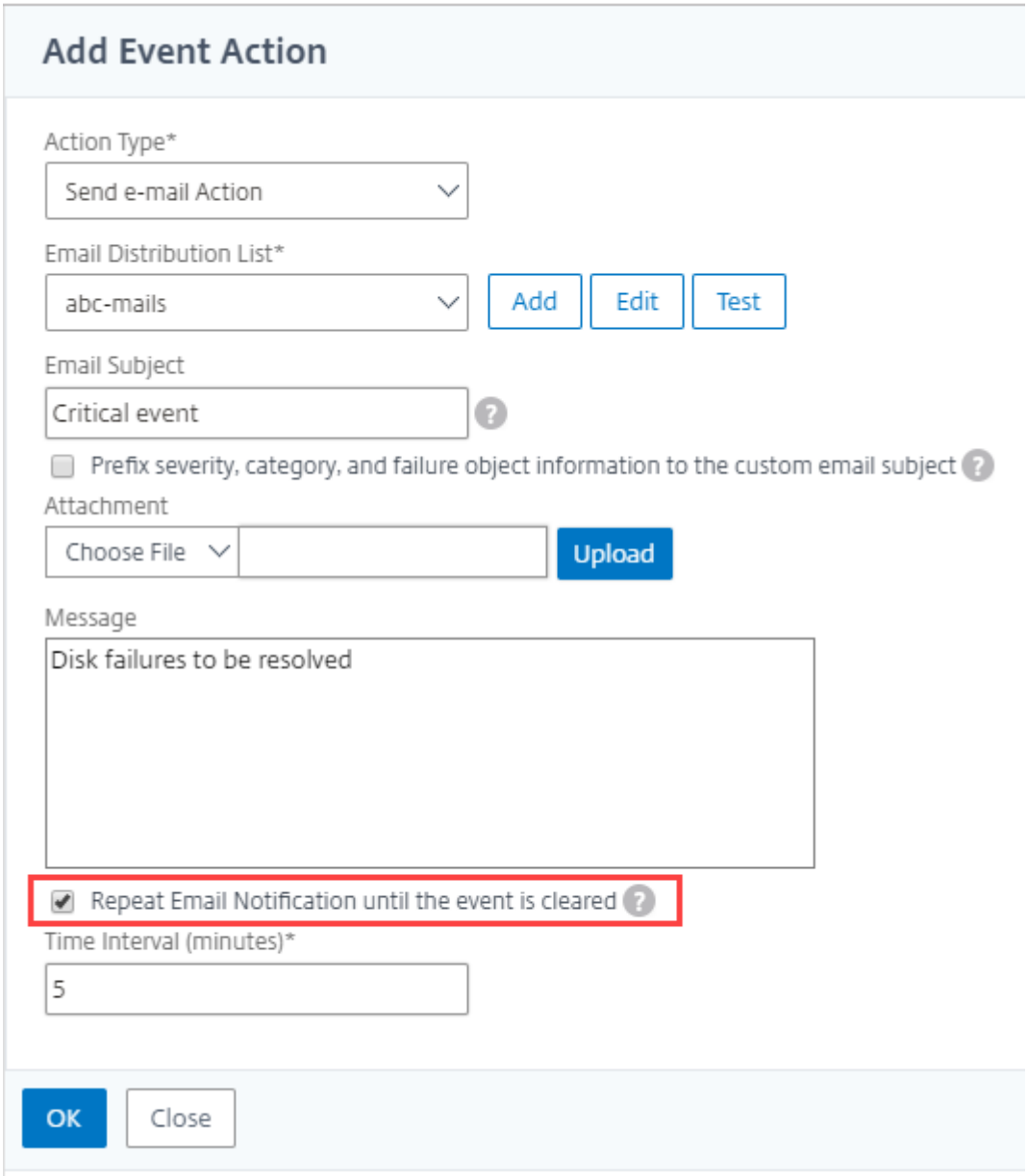
为了确保所有严重事件都被解决且没有重要电子邮件通知丢失，可以选择为满足所选择条件的事件规则发送重复的电子邮件通知。例如，如果为涉及磁盘故障的实例创建了事件规则，并希望在问题解决之前一直收到通知，可以选择接收有关那些事件的重复电子邮件通知。

这些电子邮件通知会按预定义的时间间隔重复发送，直到收件人确认看到通知或事件规则被清除。

> 注意
>
> 只有在设置了等效的“清除”陷阱并从您的 Citrix Application Delivery Controller (ADC) 实例发送时，才能自动清除事件。
>
> 要手动清除事件，可以执行以下操作：
>
> - 导航到“网络” > “事件” > “事件摘要”，选择一个 类别 并在该类别中选择一个事件，然后单击“清除”。
> - 或者，导航到“网络” > “事件” > “事件消息”。选择一个实例类型，然后从下面的网格中选择一个事件，然后单击 清除”。

要设置来自 **Citrix ADM** 的重复电子邮件通知，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 网络 > 事件 > ** 规则，然后单击“添加 **”以创建规则。
2. 在 **Create Rule**（创建规则）页面上，设置规则参数。
3. 在“事件规则操作”下，单击“添加操作”。然后，从“操作类型”下拉列表中选择“发送电子邮件操作”，然后选择电子邮件分发列表。
4. 您还可以在传入事件满足配置的规则时添加自定义的主题行和用户消息，以及将附件上载到您的电子邮件。
5. 选中 **Repeat Email Notification until the event is cleared**（重复发送电子邮件通知，直到事件被清除）复选框。



禁止显示事件

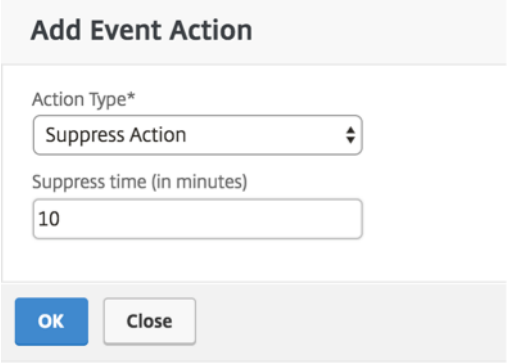
February 6, 2024

选择“抑制操作”事件操作时，可以配置一个时间段（以分钟为单位），在此时间段内抑制或删除事件。可以最短阻止事件 1 分钟。

要通过使用 **Citrix ADM** 隐藏事件，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到“网络”>“事件”>“规则”。单击添加。

2. 指定创建规则所需的所有参数。
3. 在 **Event Rule Actions**（事件规则操作）下方，单击 **Add Action**（添加操作）为事件分配通知操作。
4. 在“添加事件操作”页面上，从“操作类型”下拉列表中选择“抑制 操作”，然后指定需要抑制事件的时间段（以分钟为单位）。
5. 单击确定。



创建事件规则

February 6, 2024

May 24, 2018

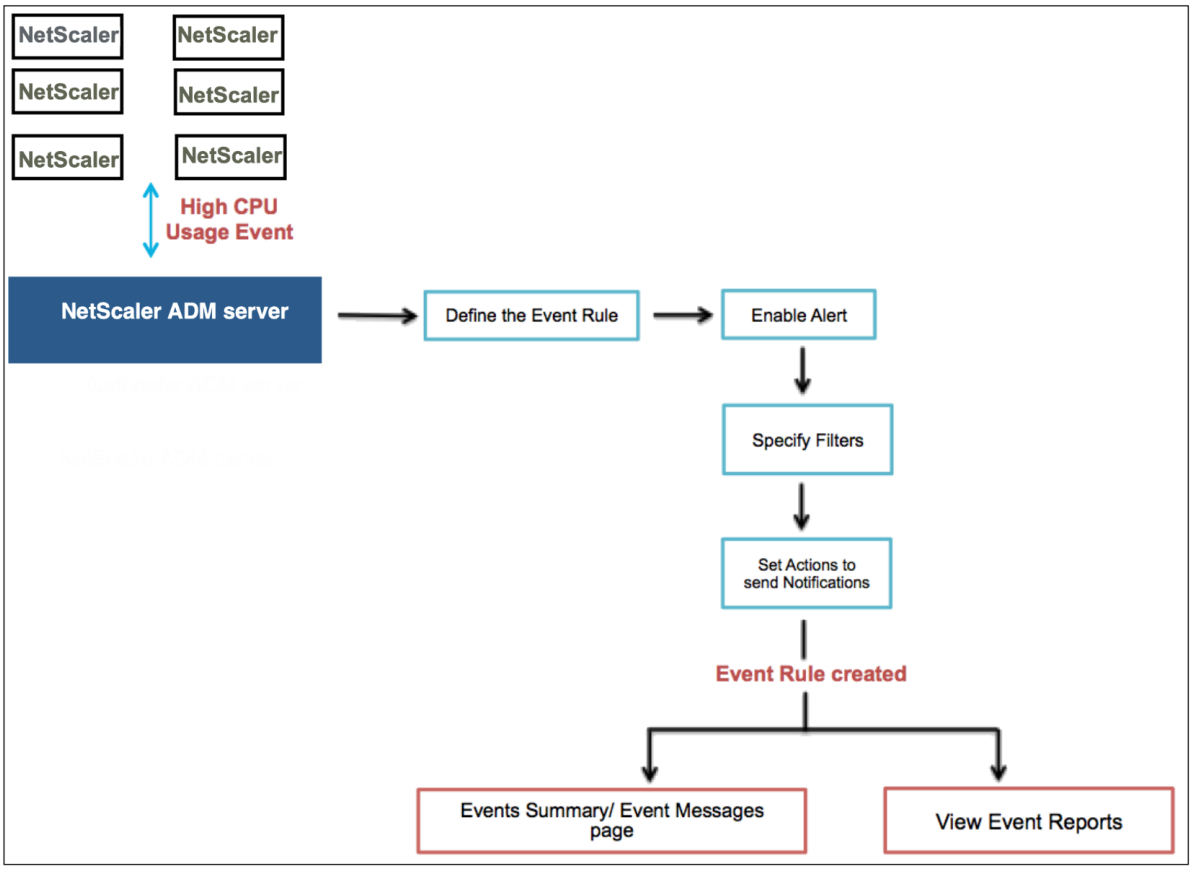
可以配置规则以监视特定事件。规则使监视在 Citrix Application Delivery Controller (ADC) 基础架构中生成的大量事件变得更加容易。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的过滤条件时，将执行与规则关联的操作。您可以创建筛选器的条件包括：严重性、Citrix ADC 实例、类别、故障对象、配置命令和消息。

可以为事件分配以下操作：

- 发送电子邮件操作：针对符合筛选条件的事件发送电子邮件。
- 发送陷阱操作：向外部陷阱目标发送或转发 SNMP 陷阱
- 发送短信操作：为每个符合筛选条件的事件发送一条短消息服务 (SMS) 消息。
- 运行命令操作：当传入事件满足配置的规则时运行命令。
- 执行作业操作：执行作业是针对与您指定的筛选条件匹配的事件。
- 隐藏操作：在特定时间段内禁止删除事件。

您还可以设置以指定的时间间隔重新发送通知，直到清除了事件。并且，您可以为电子邮件自定义特定主题行、用户消息和/或附件。



例如，作为管理员，您可能希望监视特定 Citrix ADC 实例的“CPU 使用率高”事件，如果这些事件可能导致 Citrix ADC 实例中断。您可以创建规则以监视实例，指定操作以在发生“高 CPU 使用率”类别的事件时向您发送电子邮件通知。您可以计划规则以在特定时间（例如 11 AM 到 11 PM 之间）运行，这样，您不会在每次生成事件时收到通知。

配置事件规则涉及以下任务：

1. 定义规则
2. 选择规则检测的事件的严重性
3. 指定事件的类别
4. 指定应用规则的 Citrix ADC 实例
5. 指定失败对象
6. 指定任何其他过滤器
7. 指定规则检测到事件时采取的操作

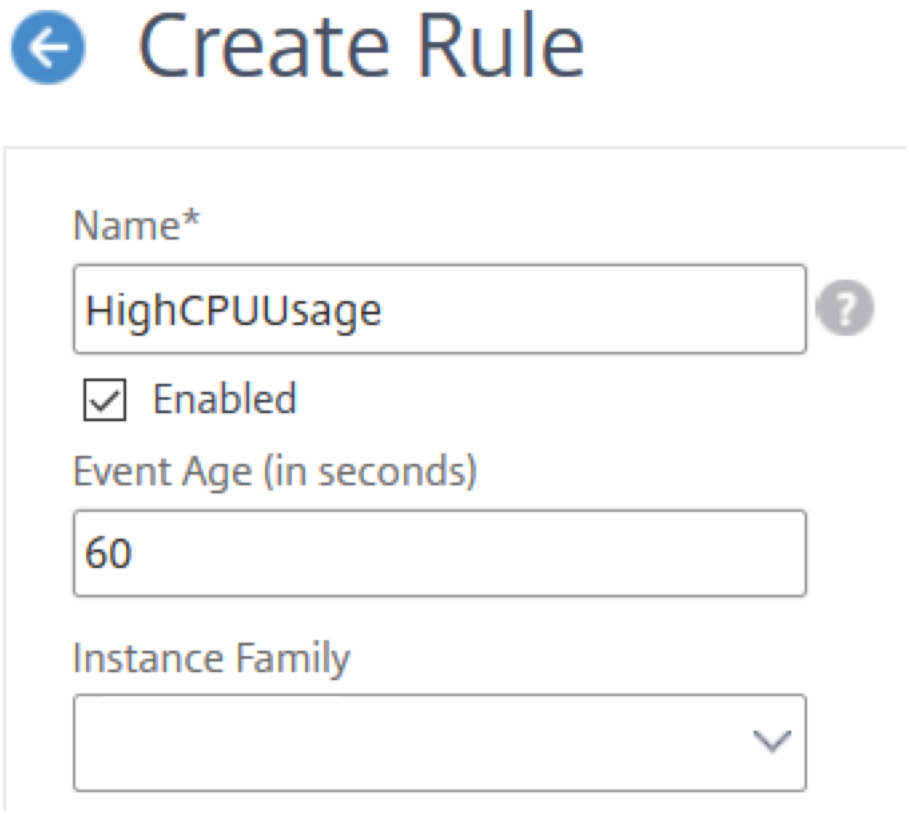
步骤 **1-**定义事件规则

导航到“网络”>“事件”>“规则”，然后单击“添加”。如果要启用规则，请选中“启用规则”复选框。

您可以设置“事件时期”选项来指定 Citrix Application Delivery Management (ADM) 刷新事件规则的时间间隔（以秒为单位）。

> 注意：
>
> 事件持续时间的最小值为 60 秒。如果将“事 件时 间”字段保留为空，则事件发生后立即应用事件规则。

根据上面的示例，您可能希望在 Citrix ADC 实例在 60 秒或更长时间内每次出现“高 CPU 使用率”事件时收到电子邮件通知。您可以将事件时长设置为 60 秒，这样，每当您的 Citrix ADC 实例出现 60 秒或更长时间的“高 CPU 使用率”事件时，您都会收到一封包含该事件详细信息的电子邮件通知。

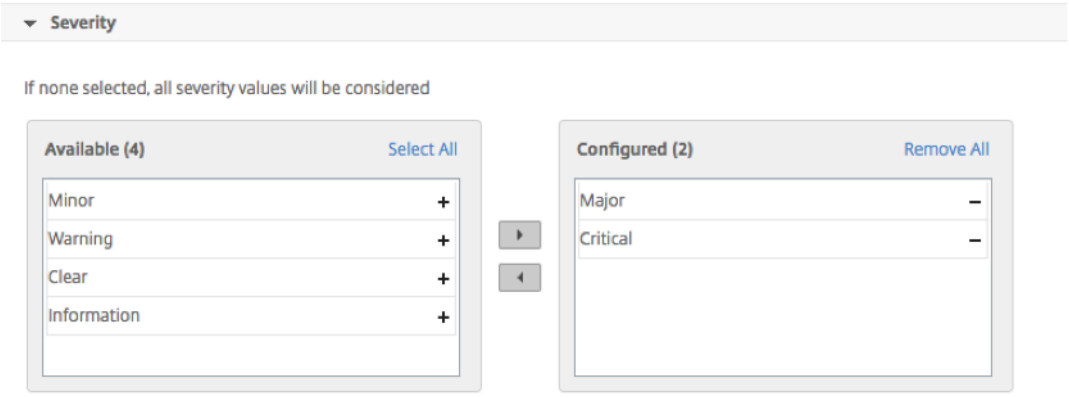


您还可以按 设备系列 筛选事件规则，以跟踪 Citrix ADM 接收事件的 Citrix ADC 实例。

步骤 **2-**选择事件的严重性

可以创建使用默认严重性设置的事件规则。“Severity”（严重性）指定要为其添加事件规则的事件的当前严重性。

可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）、Clear（清除）及 Information（信息）。

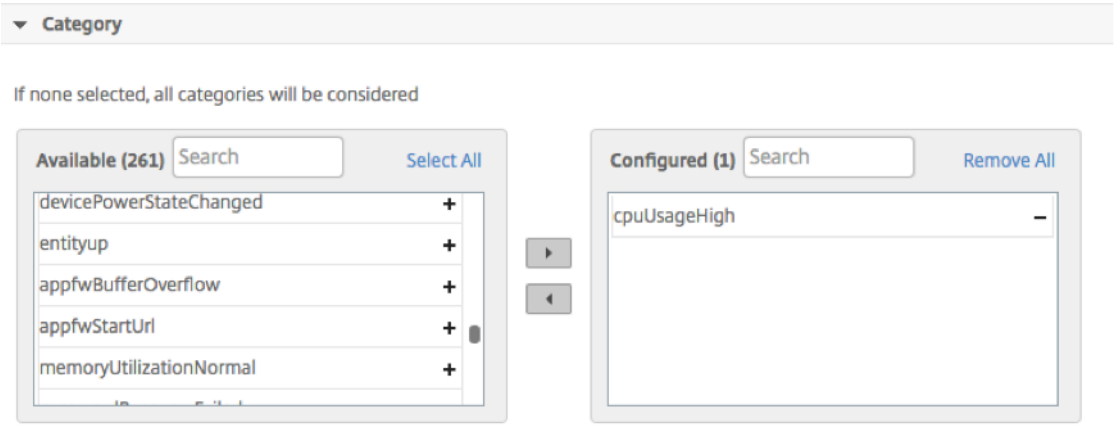


> 注意
>
> 可以为一般事件和企业特定的事件配置严重性。要修改 Citrix ADM 上管理的 Citrix ADC 实例的事件严重性，请导航至 网络 > 事件设置。选择要为其配置事件严重性的类别，然后单击配置严重性。分配新的严重性级别，然后单击确定”。

步骤 **3 -** 指定事件类别

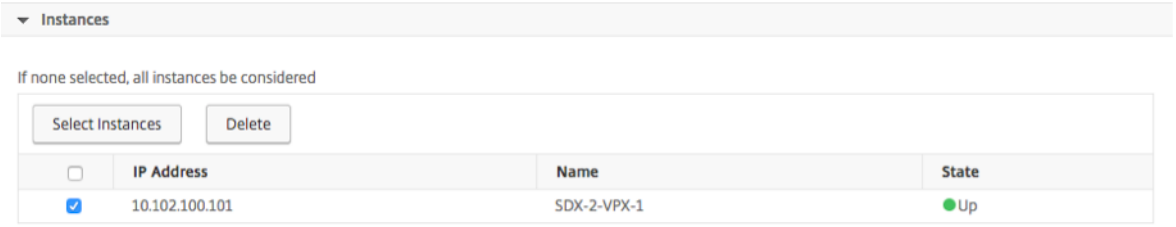
您可以指定 Citrix ADC 实例生成的事件的类别或类别。所有类别都在 Citrix ADC 实例上创建。然后使用可用于定义事件规则的 Citrix ADM 映射这些类别。选择要考虑的类别，然后将其从 可用 表移动到 已配置 表。

在上述示例中，您需要从显示的表中选择“cpuUsageHigh”作为事件类别。



步骤 **4-**指定 **Citrix ADC** 实例

选择要为其定义事件规则的 Citrix ADC 实例的 IP 地址。在“实 例”部分中，单击“选择实例”。在“选 择实例 页面中，选择您的实例，然后单击“选 择。

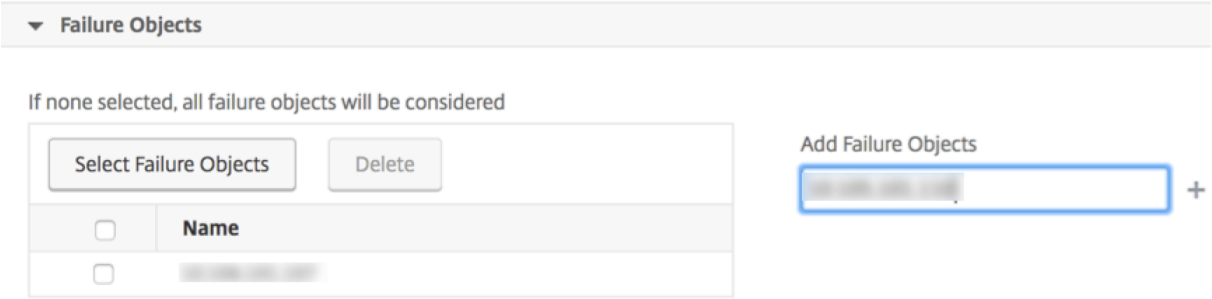


步骤 **5-**选择失败对象

您可以从提供的下拉列表中选择失败对象，也可以添加已为其生成事件的失败对象。失败对象是已为其生成事件的实体实例或计数器。

失败对象影响事件的处理方式，并确保失败对象反映通知的确切问题。这可以用于快速追查问题以及确定失败的原因，而不是仅仅报告原始事件。例如，如果用户有登录问题，则此处的失败对象是用户名或密码，例如 nsroot。

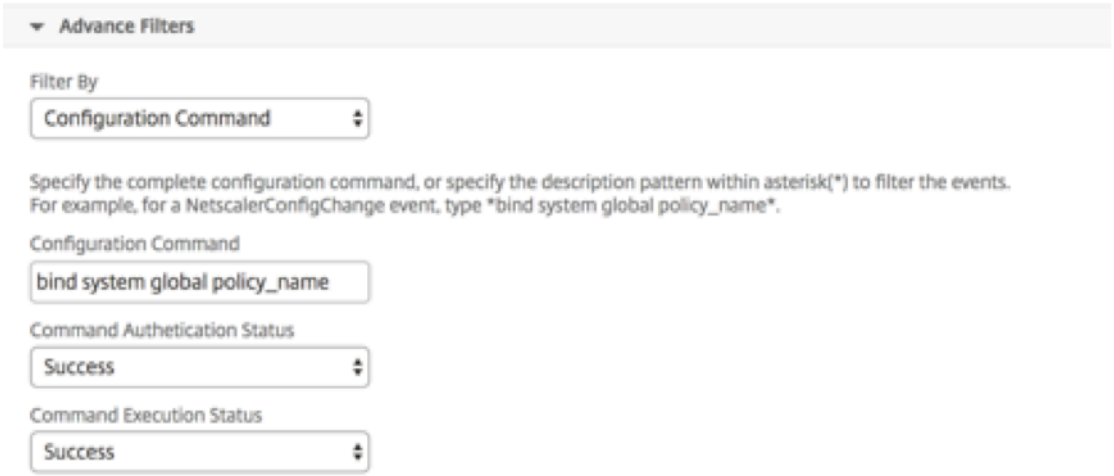
此列表可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、证书相关事件的证书名称等。



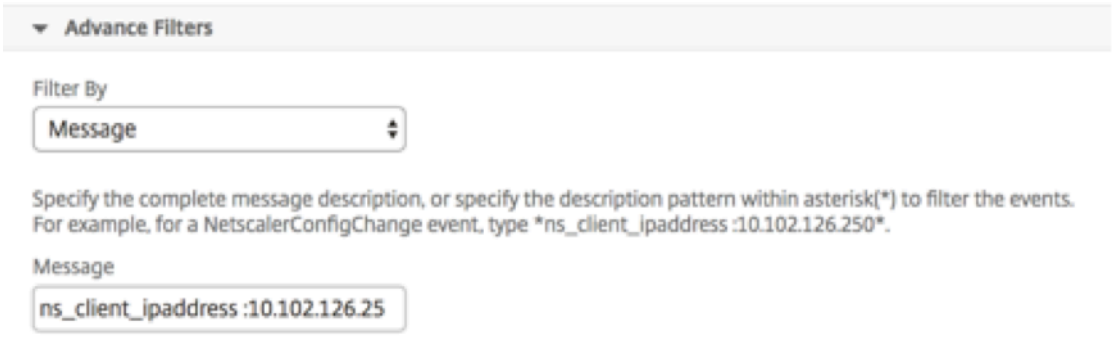
步骤 **6-**指定其他筛选器

您可以按以下内容进一步过滤事件规则：

- 配置命令 -您可以指定完整的配置命令，也可以在星号 (*) 中指定描述模式来筛选事件。除了命令外，您还可以选择按命令的身份验证状态和/或其执行状态进一步过滤事件规则。例如，对于 NetscalerConfigChange 事件，键入 *bind system global policy_name*。



- 消息 -您可以指定完整的消息描述，也可以在星号 (*) 中指定描述模式来筛选事件。
  例如，对于 NetscalerConfigChange 事件，键入 *ns_client_ipaddress :10.102.126.250*。



步骤 **7-**添加事件规则操作

您可以添加事件规则操作来为事件分配通知操作。当某个事件满足您在上面设置的已定义过滤条件时，将会发送或执行这些通知。您可以添加以下事件操作：

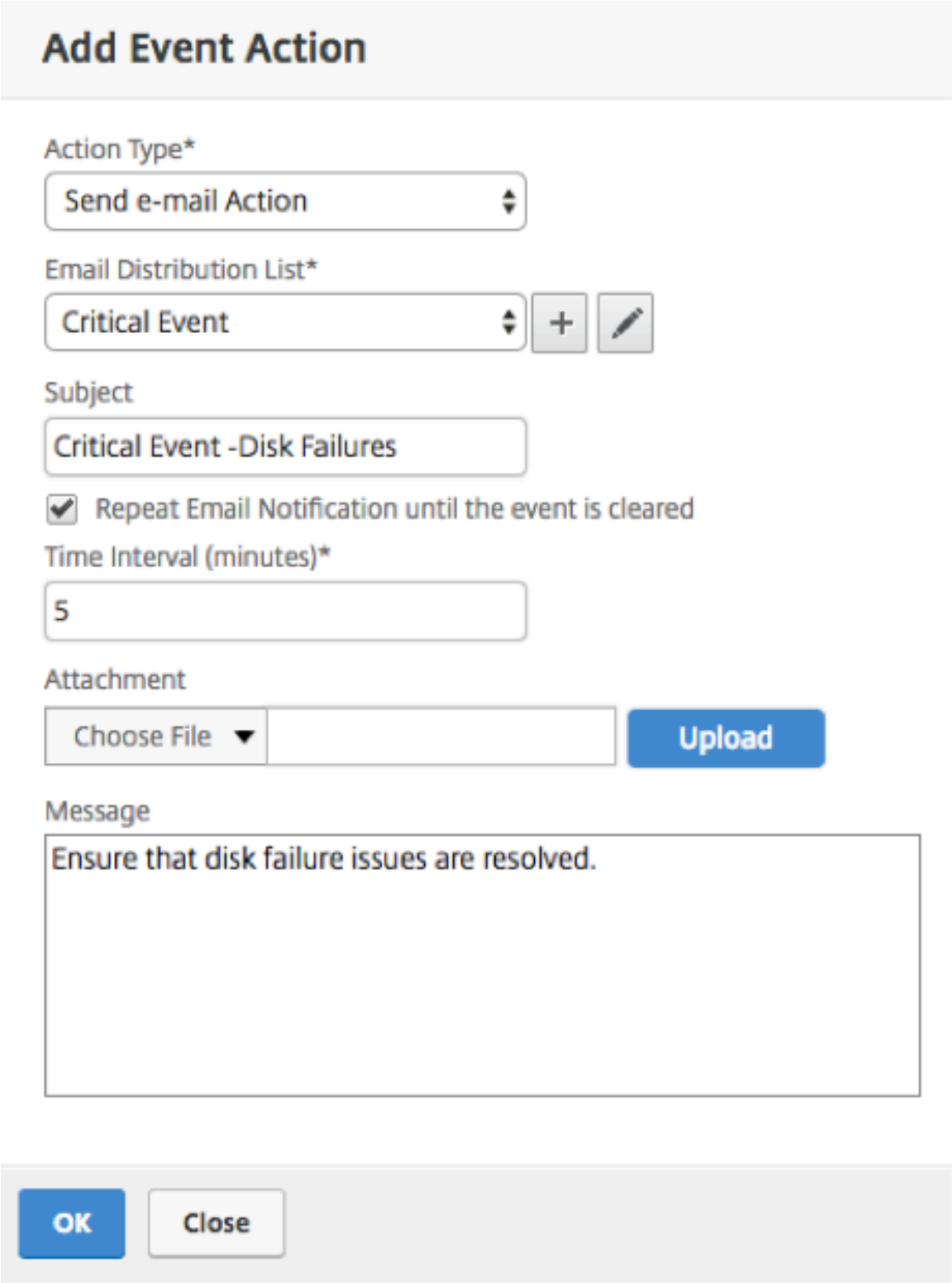
- Send e-mail Action（发送电子邮件操作）
- Send Trap Action（发送陷阱操作）
- Send SMS Action（发送 SMS 操作）
- Run Command Action（运行命令操作）
- Execute Job Action（执行作业操作）
- Suppress Action（阻止操作）

要设置电子邮件事件规则操作，请执行以下操作：

选择“Send e-mail Action”（发送电子邮件操作）事件操作类型后，当事件满足定义的过滤条件时将触发电子邮件。您将需要通过提供邮件服务器或邮件配置文件详细信息来创建电子邮件通讯组列表，也可以选择您之前创建的电子邮件通讯组列表。

您还可以在传入事件满足配置的规则时添加自定义的主题行和用户消息，以及将附件上载到您的电子邮件。

使用此选项，您还可以通过选中“在事件 清除之前重复发送电子邮件通知”复选框，针对符合所选条件的事件规则重复发送电子邮件通知，从而确保所有关键事件都得到解决，不会错过任何重要的电子邮件通知。例如，如果为涉及磁盘故障的实例创建了事件规则，并希望在问题解决之前一直收到通知，可以选择接收有关那些事件的重复电子邮件通知。



要设置陷阱事件规则操作，请执行以下操作：

选择 发送陷阱操 作”事件操作类型时，SNMP 陷阱将被发送或转发到外部陷阱目标。通过定义陷阱通讯组列表（或陷阱目标和陷阱配置文件详细信息），当事件满足定义的过滤条件时将向特定的陷阱侦听器发送陷阱消息。

要设置 **SMS** 事件规则操作，请执行以下操作：

当您选择“发送短信操作”事件操作类型时，将为每个符合筛选条件的事件发送一条 短消息服务 (SMS) 消息。您将需要通过提供 SMS 服务器或 SMS 配置文件详细信息来创建 SMS 通讯组列表，也可以选择您之前创建的 SMS 通讯组列表。

要设置“**Run Command Action**”（运行命令操作），请执行以下操作：

选择 运行命令操作”事件操 作时，可以创建一个命令或脚本，这些命令或脚本可以在 Citrix ADM 上执行匹配特定筛选条件的事件。例如，如果在托管实例上更改了配置时发生严重性为“Critical”（严重）的事件，则可以运行命令脚本。

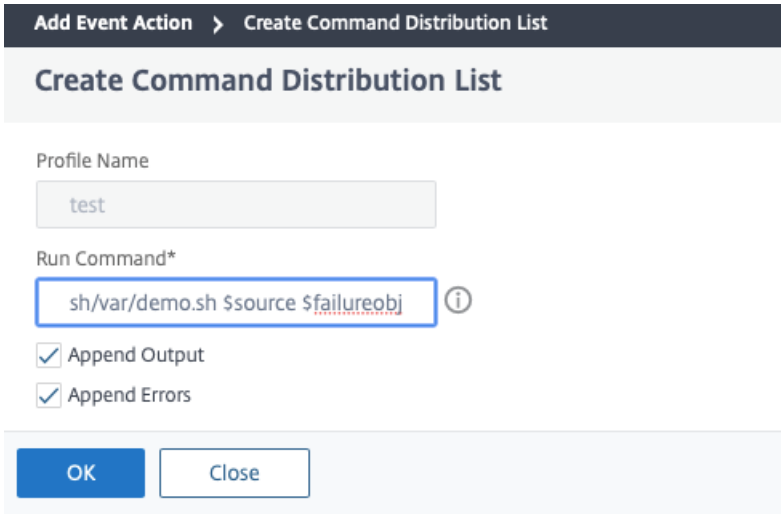
您也可以为 运行命令操作 脚本设置以下参数：

参数	说明
$source	此参数对应于接收的事件的源 IP 地址。
$category	此参数对应于过滤器类别下定义的陷阱类型。
$entity	此参数对应于已为其生成事件的实体实例或计数器。它可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、所有证书相关事件的证书名称。
$severity	此参数对应于事件的严重性。
$failureobj	失败对象影响事件的处理方式，并确保失败对象反映通知的确切问题。这可以用于快速追查问题以及确定失败的原因，而不是仅仅报告原始事件。

> 注意
>
> 在命令执行期间，这些参数将替换为实际值。

要在 **Citrix ADM** 上配置“运行命令操作”事件操作，请执行以下操作：

1. 在“事件规则操作”下，单击“添加操作”，然后从“操作类型”下拉列表中选择“运行命令 操作”。
2. 在“创建命令分发列表”页面上，指定配置文件名称和要运行的命令。当事件满足定义的过滤条件时，将执行此命令。

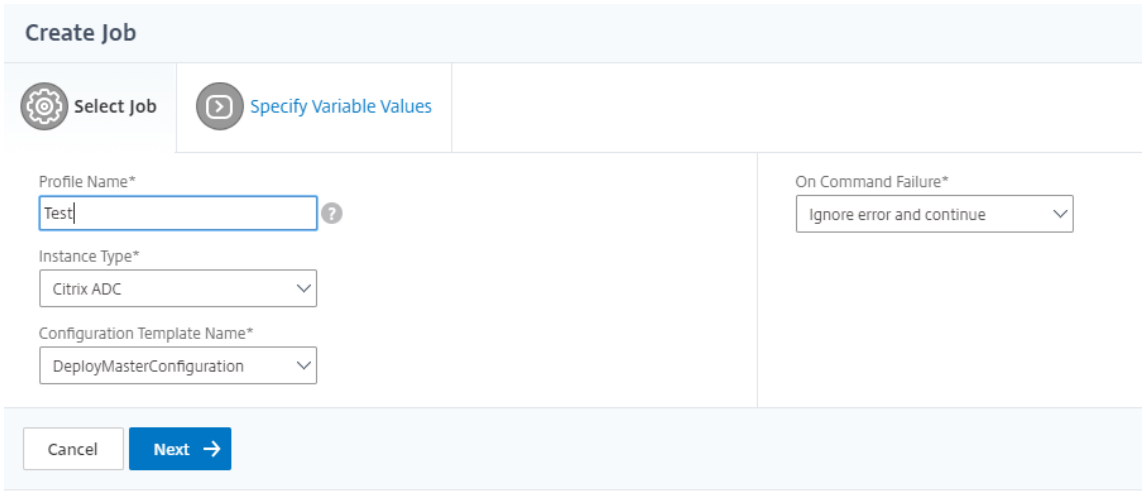


> 注意
>
> 如果要在 **Citrix ADM** 服务器日志文件中运行命令脚本时存储输出和生成的错误（如果有），则可以启用追加输出”和“追加错误”选项。如果不启用这些选项，Citrix ADM 将放弃运行命令脚本时生成的所有输出和错误。

要设置“**Execute Job Action**”（执行作业操作），请执行以下操作：

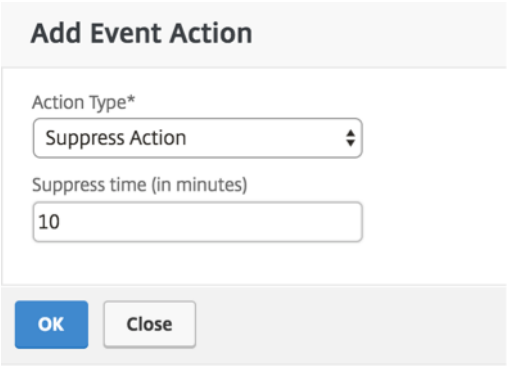
通过创建包含配置作业的配置文件，对于符合您指定的筛选条件的事件和警报，作业将作为内置作业或定制作业执行，适用于 Citrix ADC、Citrix SDX 和 Citrix SD-WAN WO 实例。

1. 在“事件规则操作”下，单击“添加操作”，然后从“操作类型”菜单中选择“执 ** 行作业 操作”。
2. 与要在事件满足定义的过滤条件时运行的作业一起创建配置文件。
3. 创建作业时，指定配置文件名称、实例类型、配置模板以及作业上的命令失败时要执行的操作。
4. 根据选定的实例类型和所选配置模板，指定变量值，然后单击“完成”创建作业。



要设置“**Suppress Action**”（阻止操作），请执行以下操作：

选择 禁止操 作”事件操作时，可以配置禁止或删除事件的时间段（以分钟为单位）。可以最短阻止事件 1 分钟。



现在已创建具有适当过滤器和定义明确的事件规则操作的事件规则。

修改报告的 **Citrix ADC** 实例上发生的事件的严重性

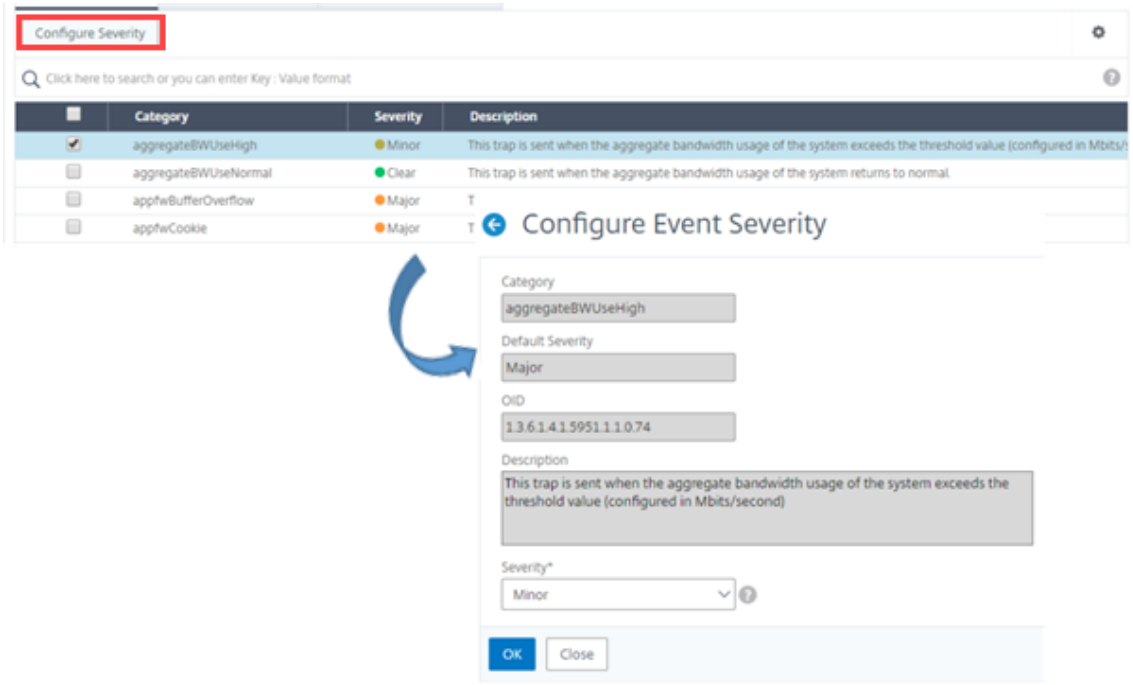
February 6, 2024

您可以管理您的所有设备上生成的事件的报告，以便可以查看有关特定实例上特定事件的事件详细信息，以及根据事件严重性查看报告。可以创建使用默认严重性设置的事件规则，并可以更改严重性设置。可以为一般事件和企业特定的事件配置严重性。

可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）及 Clear（清除）。

要修改事件严重性：

1. 导航到“网络”>“事件”**>**“事件设置”。
2. 单击要修改的 Citrix Application Delivery Controller (ADC) 实例类型的选项卡。然后，从列表中选择类别，然后单击 配置严重性。
3. 在 **Configure Event Severity**（配置事件严重性）中，从下拉列表中选择严重级别。
4. 单击确定。

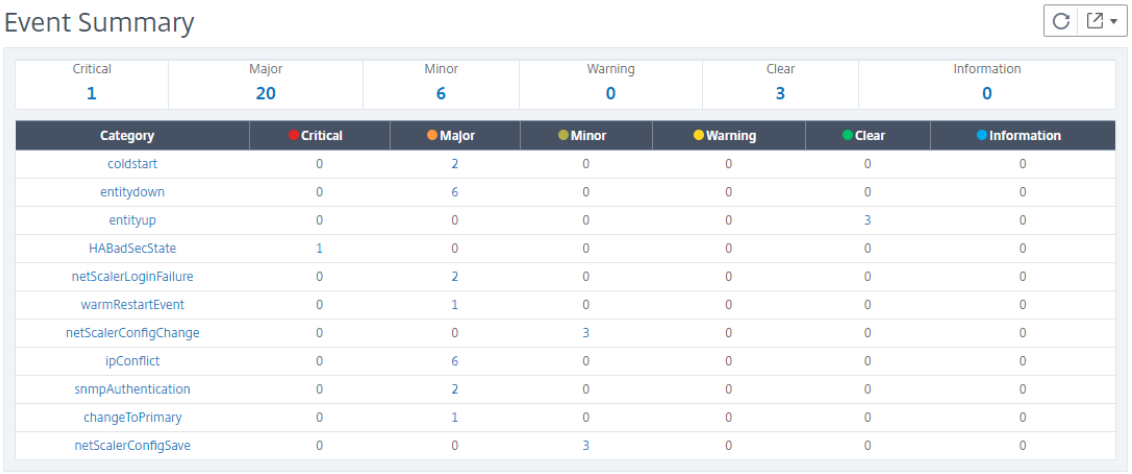


查看事件摘要

February 6, 2024

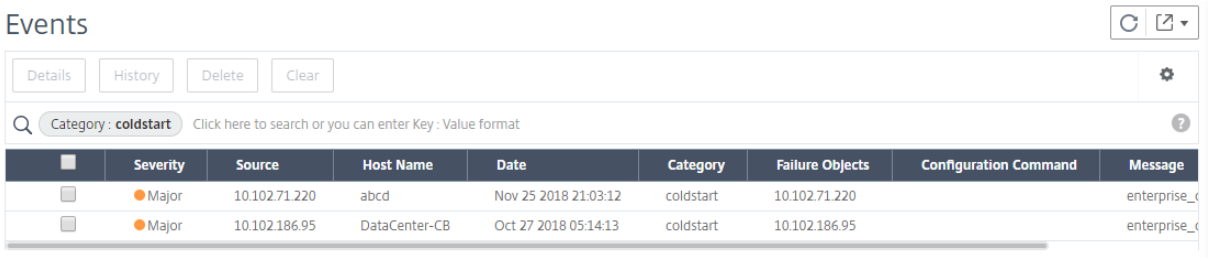
现在，您可以查看“事件摘要”页面，以监视 Citrix Application Delivery Management (ADM) 服务器上收到的事件和陷阱。导航到“网络”>“事件”。“Events Summary”（事件摘要）页面以表格形式显示以下信息：

- **Citrix ADM** 收到的所有事件的摘要。事件按类别列出，不同的严重性显示在不同的列中：“Critical”（严重）、“Major”（重大）、“Minor”（较小）、“Warning”（警告）、“Clear”（清除）和“Information”（信息）。例如，当 Citrix 应用程序 Delivery Controller (ADC) 实例关闭并停止向 Citrix ADM 服务器发送信息时，将发生严重事件。发生该事件期间，系统将向管理员发送通知，说明实例关闭的原因，已关闭的时间等。然后，该事件记录在“Events Summary”（事件摘要）页面上，您可以在该页面上查看摘要并访问事件的详细信息。



- 每个类别收到的陷阱数量。收到的陷阱数，按严重性分类。默认情况下，从 Citrix ADC 实例发送到 Citrix ADM 的每个陷阱都具有分配的严重性，但作为网络管理员，您可以在 Citrix ADM GUI 中指定其严重性。

如果您单击类别类型或陷阱，则会进入“
事件 页面，在该页面上预先选择类别和严重性等筛选器。此页显示有关事件的详细信息，例如 Citrix ADC 实例的 IP 地址和主机名、接收陷阱的日期、类别、故障对象、配置命令运行以及消息通知。



显示事件严重性和 **SNMP** 陷阱详细信息

February 6, 2024

在 Citrix Application Delivery Management (ADM) 中创建事件及其设置时，可以立即在“事件摘要”页面上查看该事件。同样，您可以在基础架构控制面板上详细查看和监视添加到您的 Citrix ADM 服务器的所有 Citrix Application Delivery Controller (ADC) 实例的运行状况、正常运行时间、模型和版本。

在基础结构控制板上，您现在可以屏蔽不相关的值，以便更轻松地查看和监视按严重性划分的事件、运行状况、正常运行时间、型号和 Citrix ADC 实例版本等信息。

例如，严重级别为“严 重”的事件可能很少发生。但是，如果您的网络上发生严重事件，您可能想要对事件的发生地点和时间进一步进行调查、故障排除和监视。如果您选择“Critical”（严重）以外的所有严重级别，则图形将仅显示发生的严重事件。此外，通过单击图表，您将进入“基于严重性的事件”页，在该页中可以查看有关在所选持续时间内发生关键事件的所有详细信息：实例源、日期、类别和发生严重事件时发送的消息通知。

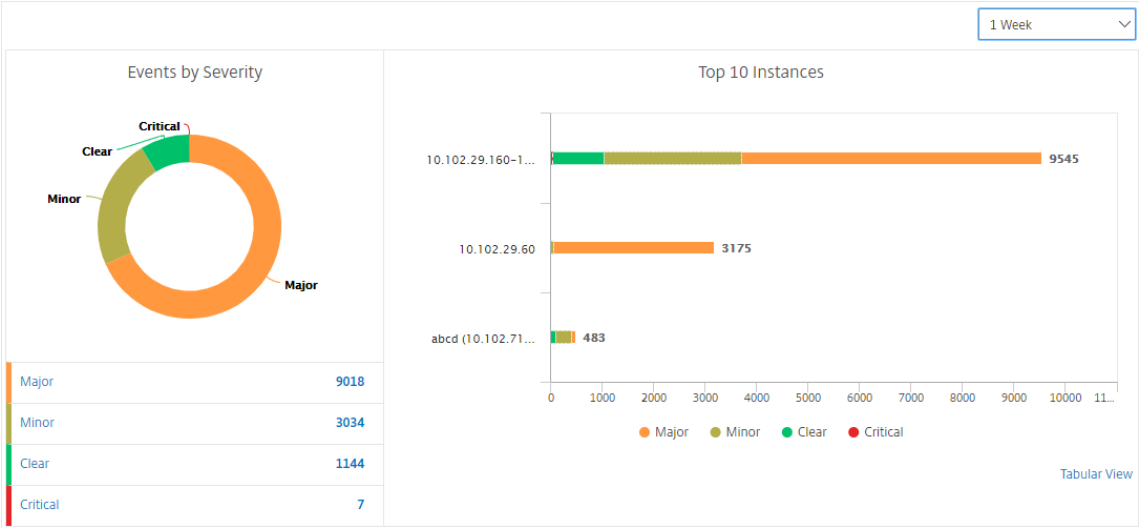
同样，您可以在控制板上查看 Citrix VPX 实例的运行状况。您可以屏蔽实例已启动并运行的时间段，只显示实例停止工作的时间段。通过单击图表，您将进入该实例的页面，其中已应用 了不服务 筛选器，并查看详细信息，如主机名、每秒接收的 HTTP 请求数、CPU 使用率等。您还可以选择实例并查看特定 Citrix 实例的控制板以了解更多详细信息

要在 **Citrix ADM** 中按严重性选择特定事件，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到 网络 **>** 控制板。

   或者，

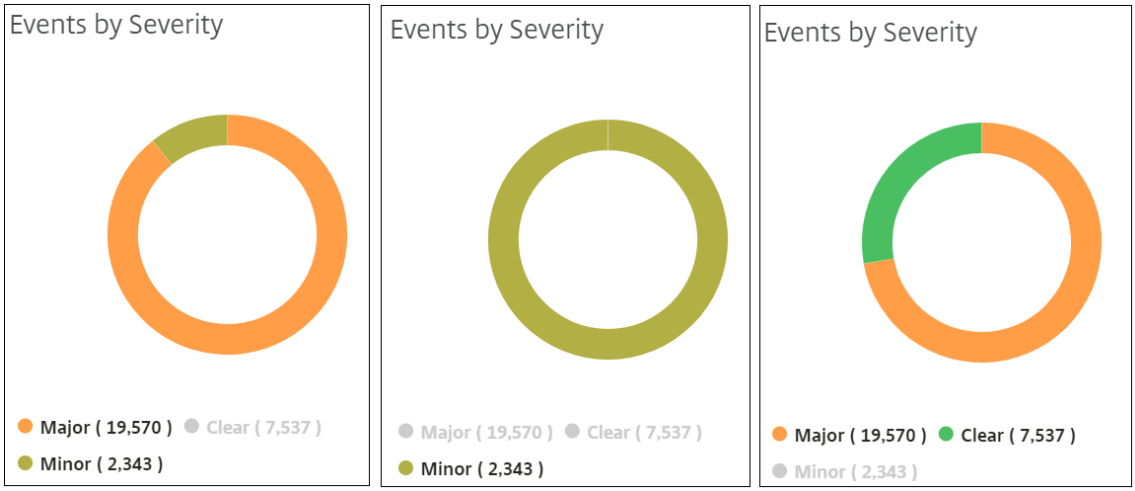
   导航到 网络 **>** 事件 **>** 报告。
3. 从页面右上角的菜单中，选择要按严重程度查看事件的持续时间。



4. “按严重程度列出的事件”圆环图显示按严重程度显示所有事件的可视化表示。不同类型的事件以不同的彩色部分表示，每个部分的长度对应于该严重性类型的事件总数。
5. 您可以单击圆环图上的每个部分来显示相应的 基于严重性的事件 页面，该页面显示所选持续时间内所选严重性的以下详细信息：

   - 实例源
   - 事件日期
   - 由 Citrix ADC 实例生成的事件类别
   - 发送的消息通知

   > 注意
   >
   > 在甜甜圈图下方，您可以看到图表中表示的严重性列表。默认情况下，圆环图显示所有严重性类型的所有事件，因此，列表中的所有严重性类型均突出显示。您可以切换严重性类型以更加轻松地查看和监视您选择的严重性。



要查看 **Citrix ADM** 上的 **Citrix ADC SNMP** 陷阱详细信息，请执行以下操作：

现在，您可以在“事件设 置”页面上查看从 Citrix ADM 服务器上的托管 Citrix ADC 实例收到的每个 SNMP 陷阱的详细信息。导航到“网络”>“事件”**>**“事件设置”。对于从您的实例接收的特定陷阱，您可以以表格形式查看以下详细信息：

- 类别 -指定事件所属实例的类别。
- 严重性 -事件的严重性由颜色及其严重性类型表示。
- 说明 -指定与事件关联的消息。

例如，陷阱类别为 **monresptimeoutBelowThresh** 的事件，该陷阱的描述显示为“当监视探测器的响应超时恢复正常，小于设定的阈值时，就会发送此陷阱。”

导出 **syslog** 消息

February 6, 2024

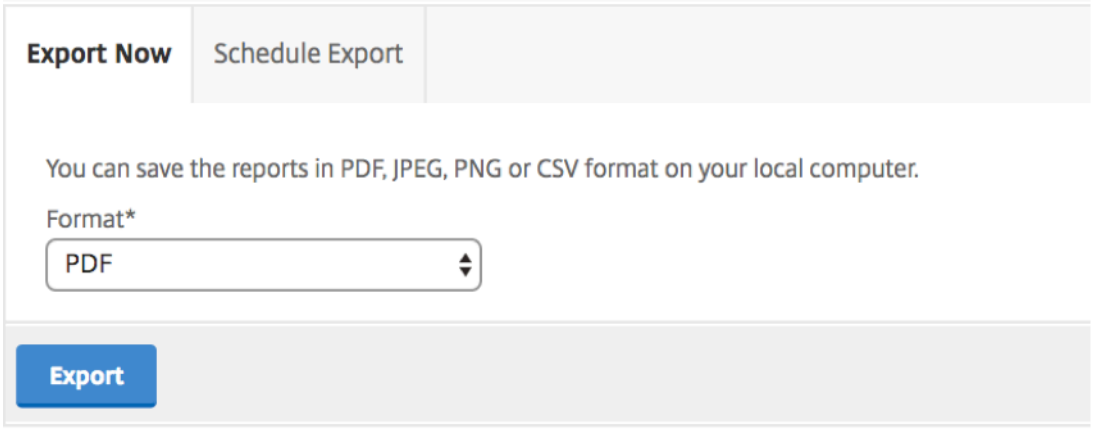
现在，您可以通过计划导出服务器上收到的所有 syslog 消息，而无需登录到 Citrix Application Delivery Management (ADM) 即可查看 syslog 消息。您可以以 PDF、CSV、PNG 和 JPEG 格式导出在 Citrix Application Delivery Controller (ADC) 实例上生成的系统日志消息。您可以计划以各种时间间隔将这些报告导出到指定的电子邮件地址。

> 注意
>
> 有关配置系统日志服务器、系统日志数据和时间格式以及如何在 Citrix ADM 上查看系统日志消息的详细信息，请参阅查看审核信息。

要查看系统日志消息，请导航到“网络”>“事件”>“系统日志消息”。在右侧窗格的 Syslog **Viewer** 下， 您可以按模块、事件类型、严重程度和源 IP 地址筛选要查看的系统日志消息。单击 “应用”生成 syslog 消息。

要使用 **Citrix ADM** 导出系统日志消息报告，请执行以下操作：

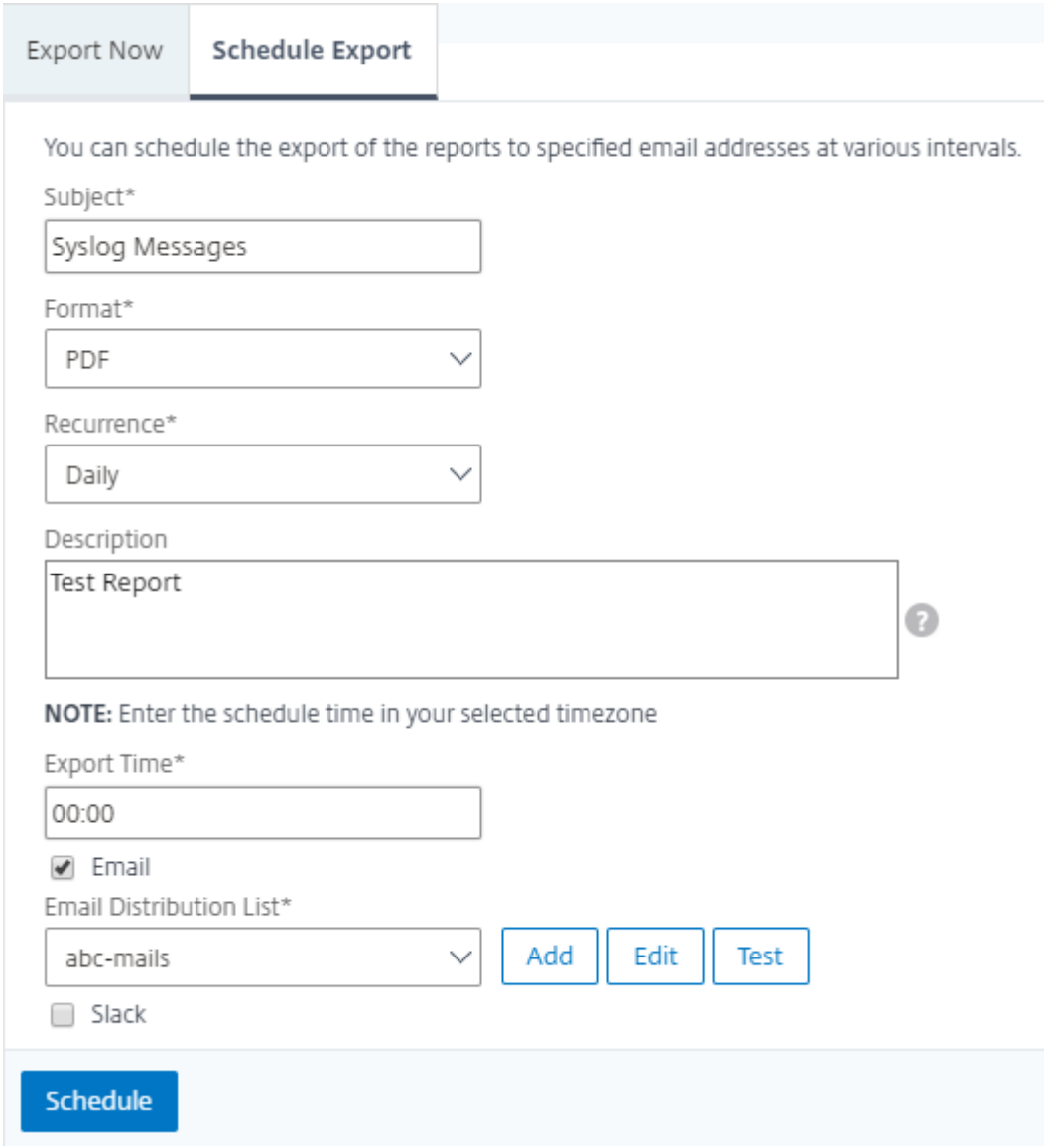
1. 导航到“网络”>“事件”>“系统日志消息”。
2. 在右侧窗格中，单击“Syslog Messages”（syslog 消息）页面右上角的导出按钮。
3. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。



要使用 **Citrix ADM** 计划导出系统日志消息报告，请执行以下操作：

1. 导航到“网络”>“事件”>“系统日志消息”。
2. 在 **Syslog** 消息 页面的右侧窗格中，单击“导出”。
3. 在“计 划报告 选项卡下，设置以下参数：

   - 说明：描述导出报表原因的消息。
   - 格式：导出报告的格式。
   - 重复：导出报告的间隔。
   - 导出时间：导出报表的时间。按您的本地时区以 24 小时格式输入时间。
   - 电子邮件通讯组列表：通过电子邮件接收报告的收件人列表。从提供的下拉列表中选择电子邮件通讯组列表。生成报告且满足计划的时间条件时触发电子邮件。 如果要创建新的电子邮件分发列表，请单击 **+** 并提供邮件服务器和邮件配置文件详细信息。



如何通过使用 **Citrix ADM** 配置事件修剪设置

要限制存储在 Citrix ADM 服务器数据库中的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时修剪一次（在 00.00 点）。

导航到“系统”>“系统管理”。在“实 例设置”下，单击“事件删除设置”。输入要在 Citrix ADM 服务器上保留数据的时间间隔（以天为单位），然后单击“** 确定”。

禁止显示 **syslog** 消息

February 6, 2024

当配置为 syslog 服务器时，Citrix Application Delivery Management (ADM) 会收到配置的 Citrix 应用程序 Delivery Controller (ADC) 实例发送给它的所有 syslog 消息。可能有大量您可能不想看到的消息。例如，您可能不希望看到所有信息级别的消息。现在您可以丢弃其中一些您不感兴趣的 syslog 消息。您可以通过设置一些过滤器来抑制进入 Citrix ADM 的某些系统日志消息。Citrix ADM 删除与条件匹配的所有邮件。这些删除的消息不会显示在 Citrix ADM GUI 上，这些消息也不会存储在客户的 Citrix ADM 数据库中。

您可以通过设置一些过滤器来抑制某些已记录的 syslog 消息进入 Citrix ADM。用于阻止 syslog 消息的两个过滤器是严重性和设施。您还可以隐藏来自特定 Citrix ADC 实例或多个实例的消息。您还可以为 Citrix ADM 提供用于搜索和禁止消息的文本模式。Citrix ADM 删除与条件匹配的所有邮件。这些删除的消息不会显示在 Citrix ADM GUI 上，这些消息也不会存储在客户数据库中。因此，在存储服务器上节省了大量空间。

阻止 syslog 消息的一些用例如下：

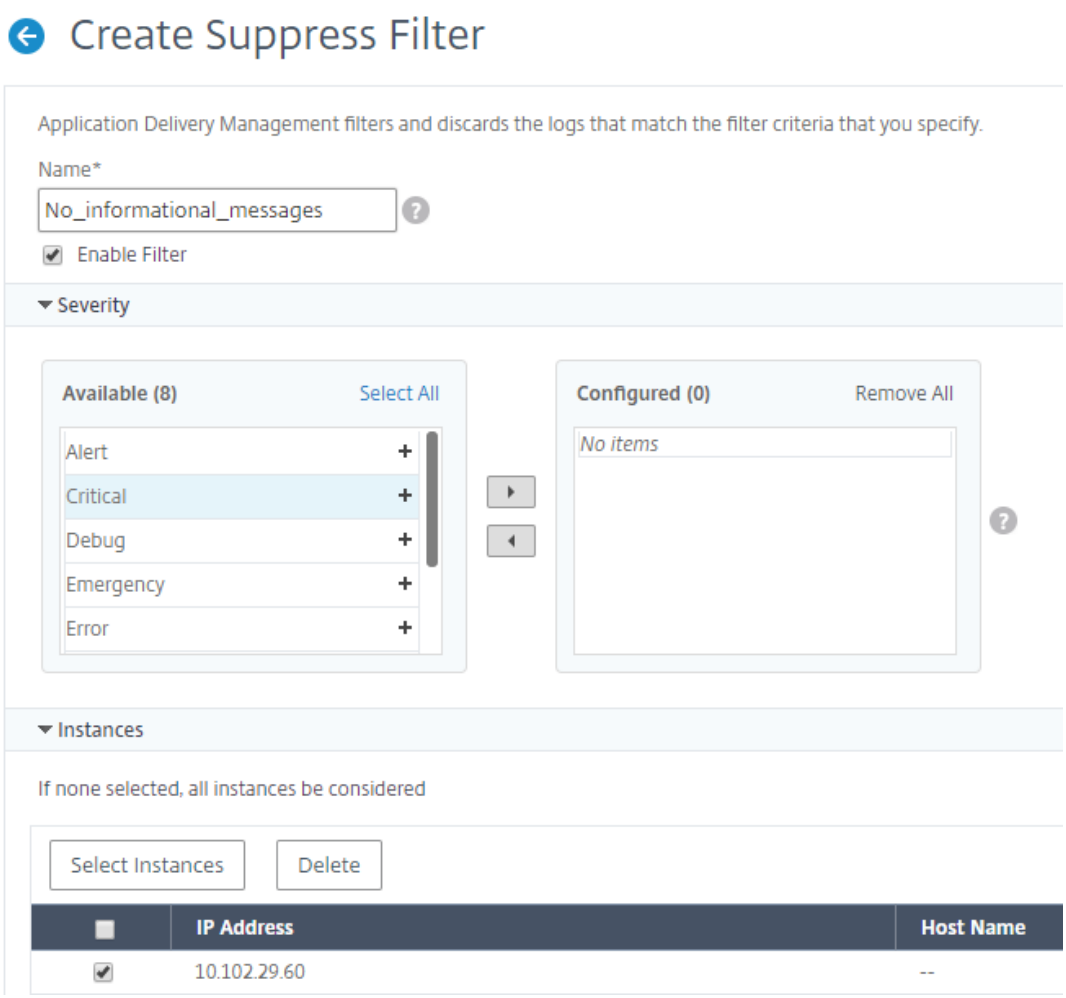
- 如果您要忽略所有信息级别消息，则阻止级别 6（信息）
- 如果您仅要记录防火墙错误状况，则阻止级别 3（错误）以外的所有级别

通过创建筛选器禁止 **syslog** 消息

1. 在 Citrix ADM 中，导航到“网络”>“事件”>“系统日志消息”>“禁止筛选器”。
2. 在“创建隐藏过滤器”页上，更新以下信息：
   a) 名称 -键入筛选器的名称。

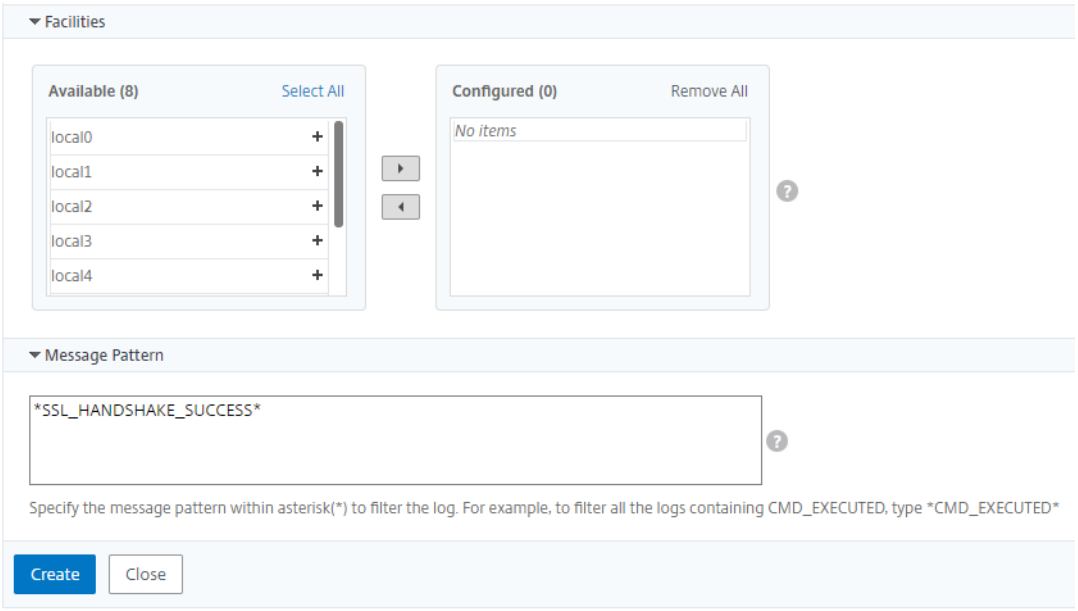
   > 注意
   >
   > 如果不同的用户对多个 Citrix ADC 实例具有不同的访问权限，则必须为不同的实例创建不同的筛选器，因为用户只能看到他们有权访问所有实例的筛选器。

   b) 严重性 -选择并添加必须隐藏消息的日志级别。例如，如果您不想查看传入的任何信息消息，则可以选择“Informational”（信息）以阻止这些消息。
   c) 实例 -选择已配置 syslog 消息的 Citrix ADC 实例。



d) 协作室 -根据生成消息的源选择要隐藏消息的协作室。

e) 消息模式 -您也可以键入用星号 (*) 包围的文本模式来隐藏消息。将在消息中搜索该文本模式字符串，并阻止包含此模式的那些消息。



禁用过滤器

要允许在 Citrix ADM 上查看消息，必须禁用筛选器。

1. 导航到 网络 > 事件 > **Syslog** 消息 > 抑制过滤器，然后在“抑制过滤器”页面上，选择过滤器并单击“** 编辑”。
2. 在“配置禁止筛选器”页上，清除“启用筛选器”复选框以禁用筛选器。

配置实例事件的删除设置

February 6, 2024

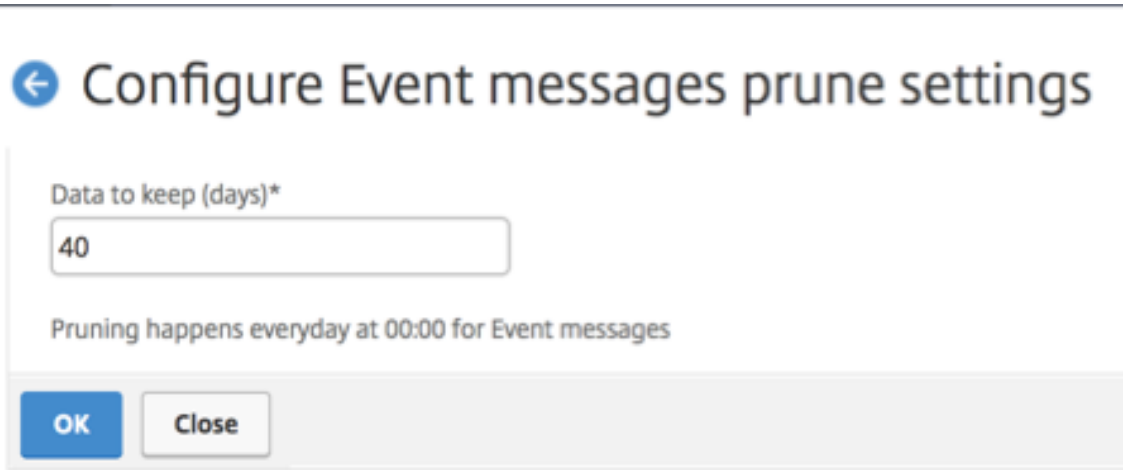
由 Citrix Application Delivery Management (ADM) 服务器管理的 Citrix Application Delivery Controller (ADC) 实例不断发送事件消息数据以存储在 Citrix ADM 上。您可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时修剪一次（在 00.00 点）。

> 注意
>
> 您可以指定的值不能超过 40 天或小于 1 天。

要配置实例事件的修剪设置，请执行以下操作：

1. 导航到“系统”>“系统管理”。
2. 在“修剪设置”下，单击“实例 事件修剪设置”。

3. 输入要在 Citrix ADM 服务器上保留数据的时间间隔（以天为单位），然后单击“确定”。



SSL 控制板

February 6, 2024

Citrix Application Delivery Management (ADM) 现在可以为您简化证书管理的各个方面。通过一个控制台可以建立自动化策略以确保合适的颁发者、密钥强度和正确的算法，同时密切跟踪未使用或即将过期的证书。要开始使用 Citrix ADM 的 SSL 控制面板及其功能，您必须了解什么是 SSL 证书以及如何使用 Citrix ADM 来跟踪您的 SSL 证书。

安全套接字层 (SSL) 证书是任何 SSL 事务的一部分，是标识公司（域）或个人的数字数据表单 (X509)。证书具有公钥组成部分，想要启动与服务器的安全事务的任何客户端都可以看见该组成部分。相应的私钥安全地驻留在 Citrix Application Delivery Controller (ADC) 设备上，用于完成非对称密钥（或公钥）加密和解密。

您可以通过以下任何一种方式获取 SSL 证书和密钥：

- 来自授权证书颁发机构 (CA)
- 通过在 Citrix ADC 设备上生成新的 SSL 证书和密钥

Citrix ADM 提供了在所有托管 Citrix ADC 实例上安装的 SSL 证书的集中视图。在 SSL 控制面板上，您可以查看有助于跟踪证书颁发者、密钥强度、签名算法、过期或未使用的证书等的图表。您还可以查看您的虚拟服务器上运行的 SSL 协议的分布情况以及这些服务器上启用的密钥。

您还可以设置通知，以便在证书即将过期时通知您，并包括有关哪些 Citrix ADC 实例使用这些证书的信息。

您可以将 Citrix ADC 实例的证书链接到 CA 证书。但是，请确保链接到同一 CA 证书的证书具有相同的来源和相同的颁发者。将证书链接到 CA 证书后，可以取消它们的链接。

使用 **SSL** 控制板

February 6, 2024

您可以使用 Citrix Application Delivery Management (ADM) 中的 SSL 证书控制面板查看图表，以帮助您跟踪证书颁发者、关键优势和签名算法。SSL 证书控制板还显示指示以下信息的图形：

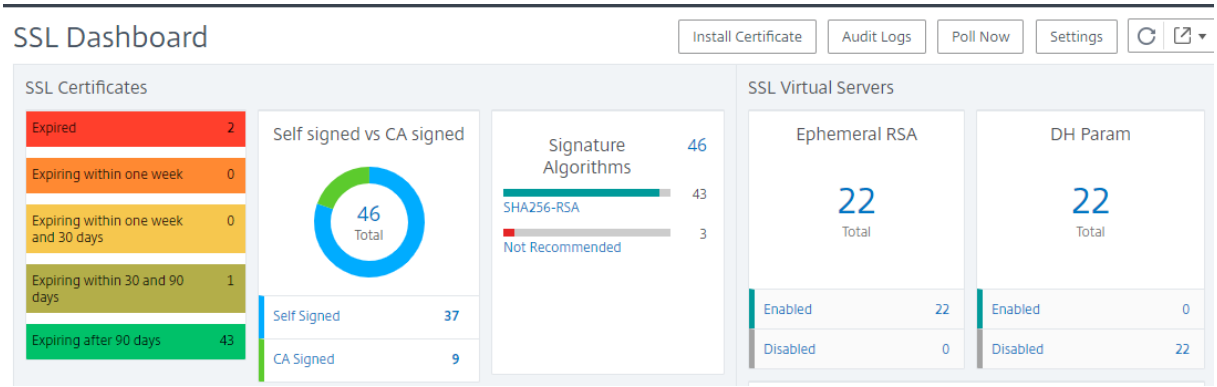
- 证书过期前的天数
- 已使用证书和未使用证书的数量
- 自签名证书和 CA 签名证书的数量
- 颁发者数
- 签名算法
- SSL 协议
- 按使用的证书数排在前 10 位的实例

监视 **SSL** 证书

如果贵公司已定义某些 SSL 证书要求（例如，所有证书的最小密钥强度必须为 2048 位，并且必须由受信任的 CA 颁发机构授权，则可以使用 Citrix ADM 上的 SSL 控制板监视您的证书。

再例如，您可能上载了新证书，但忘记将其绑定到虚拟服务器。SSL 控制板会突出显示正在使用或未使用的 SSL 证书。在“Usage”（使用情况）部分中，您可以看到已安装的证书数，以及正在使用的证书数。您可以进一步单击图形，以查看证书名称、使用证书的实例、证书的有效性以及证书的签名算法等。

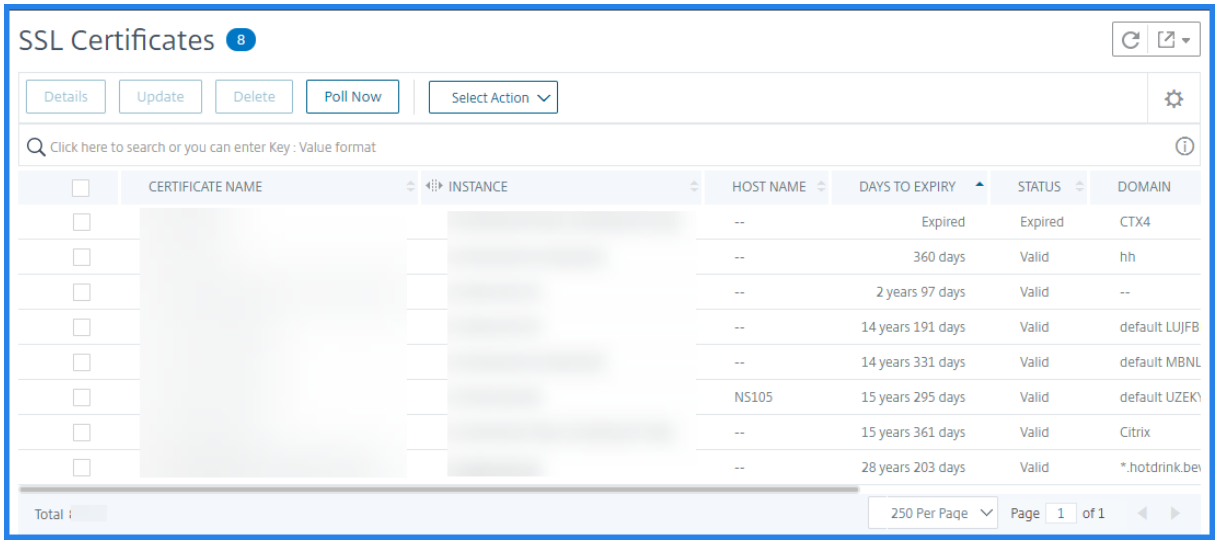
要在 Citrix ADM 中监视 SSL 证书，请导航到“网络”>“**SSL** 控制板”。



Citrix ADM 允许您轮询 SSL 证书，并立即将实例的所有 SSL 证书添加到 Citrix ADM 中。为此，请导航到“网络”>“**SSL** 控制面板”，然后单击“立即投票”。将弹出“立即投票”页面，提供轮询网络中所有 Citrix Application Delivery Controller (ADC) 实例或轮询所选实例的选项。

您可以使用 Citrix ADM SSL 控制面板查看或监视 Citrix ADC SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。“总”数是超级链接，您可以单击这些链接来显示与 SSL 证书、SSL 虚拟服务器或 SSL 协议有关的详细信息。

例如，当用户单击“自签名对比”下的数字 52 时 CA signed”在上图中，出现了一个新窗口，显示了 Citrix ADC 实例上的 52 个 SSL 证书的详细信息。



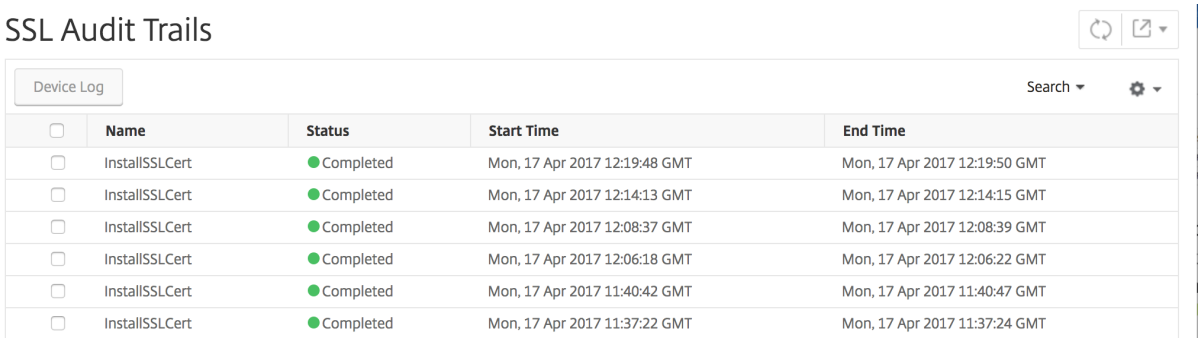
Citrix ADM SSL 控制板还显示了虚拟服务器上运行的 SSL 协议的分布情况。作为管理员，您可以通过 SSL 策略指定要监视的协议。支持的协议为 SSLv2、SSLv3、TLS1.0、TLS1.1 和 TLS1.2。虚拟服务器上使用的 SSL 协议以条形图格式显示。单击特定协议可显示使用该协议的虚拟服务器的列表。

启用或禁用了 Diffie-Hellman (DH) 密钥或 Ephermeral RSA 密钥后，将在 SSL 控制板上显示圆环图。即使服务器证书不支持导出客户端，使用这些密钥也可以与导出客户端进行安全通信，就像使用 1024 位证书一样。单击适当的图表可显示启用了 DH 密钥或 Ephemeral RSA 密钥的虚拟服务器的列表。

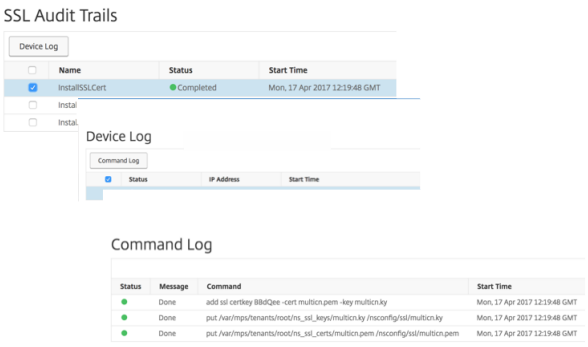
查看 **SSL** 证书的审核追踪

您现在可以在 Citrix ADM 上查看 SSL 证书的日志详细信息。日志详细信息显示在 Citrix ADM 上使用 SSL 证书执行的操作，例如：安装 SSL 证书、链接和取消链接 SSL 证书、更新 SSL 证书和删除 SSL 证书。监视具有多个所有者的应用程序上进行的 SSL 证书更改时，审核追踪信息很有用。

要查看使用 SSL 证书在 Citrix ADM 上执行的特定操作的审核日志，请导航到 网络 > SS L 控制面板 > **SSL** 审核记录。



对于使用 SSL 证书执行的特定操作，您可以查看其状态、开始时间和结束时间。此外，您还可以查看在其上执行操作的实例以及在该实例上执行的命令。

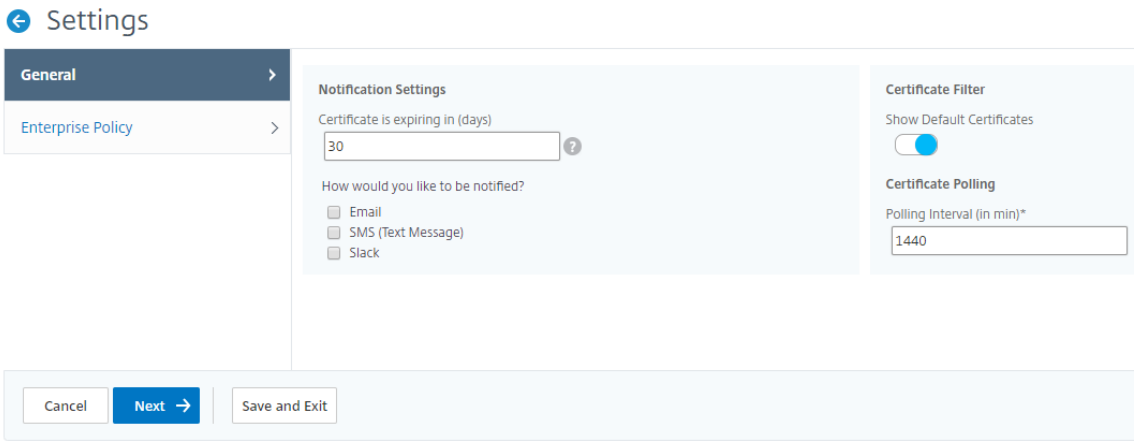


排除 **SSL** 控制板上的默认 **Citrix ADC** 证书

Citrix ADM 允许您根据自己的喜好显示或隐藏 SSL 控制面板图表上显示的默认 Citrix ADC 证书。默认情况下，所有证书（包括默身份验证书）都显示在 SSL 控制面板上。

要在 SSL 控制板上显示或隐藏默身份验证书，请执行以下操作：

1. 在 Citrix ADM GUI 中导航到 网络 > **SSL** 控制板。
2. 在“**SSL** 控制板”页面上，单击“设置”。
3. 在 设置 页面上，选择 常规。
4. 键入证书到期的天数以接收有关证书到期的通知。
5. 选择通知方法并创建相应的配置文件。
6. 在“证书筛选器”部分，清除“显示默身份验证书”复选框，然后单击“保存并退出”。



设置 SSL 证书过期通知

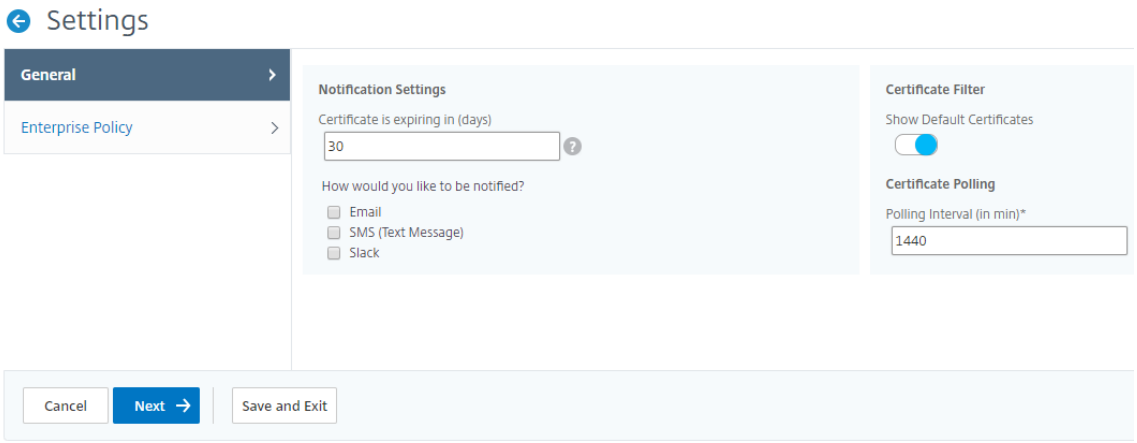
February 6, 2024

作为安全管理员，您可以设置通知，在证书即将到期时通知您，并包含有关哪个 Citrix Application Delivery Controller (ADC) 实例使用这些证书的信息。通过启用通知，您可以及时续订您的 SSL 证书。

例如，您可以设置在您的证书即将过期前的 30 天向电子邮件通讯组列表发送电子邮件通知。

要设置来自 **Citrix ADM** 的通知，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到“网络”>“**SSL** 控制板”。
2. 在 **SSL** 控制面板 页面上，单击 设置。
3. 在“**SSL** 设置”页上，单击“编 辑”图标。
4. 在 **Notification Settings**（通知设置）部分，指定要何时（过期日期前的天数）发送通知。
5. 选择要发送的通知类型。从下拉菜单中选择通知类型和通讯组列表。通知类型如下：
   - **Email**（电子邮件）- 指定邮件服务器和配置文件详细信息。证书要过期时将触发电子邮件。
   - **SMS** - 指定短信服务 (SMS) 服务器和配置文件详细信息。证书要过期时将触发 SMS 消息。
   - **Slack** -指定 Slack 配置文件详细信息。
6. 单击“保存并退出”。



现在，当您的 SSL 证书到期时，Citrix ADM 将 SSL 证书过期陷阱发送到外部陷阱目标服务器。满足以下两个条件时，Citrix ADM 会发送陷阱：

- 您已在 SSL 控制面板设置页面中配置了证书过期的天数。
- 您已添加陷阱目标。

您可以通过导航到“系统”>“SNM P”>“** 陷阱目的地”来设置 陷阱 ** 目的地。键入发送陷阱的目标 SNMP 服务器的 IP 地址。输入端口号并键入“public”（不带引号）作为社区字符串。

更新已安装的证书

February 6, 2024

从证书颁发机构 (CA) 收到续订的证书后，您可以从 Citrix Application Delivery Management (ADM) 更新现有证书，而无需登录到单个 Citrix 应用程序 Delivery Controller (ADC) 实例。

要从 **Citrix ADM** 更新 **SSL** 证书、密钥或两者，请执行以下操作：

1. 在 Citrix ADM 中，导航到网络 > **SSL** 控制板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 在 **SSL Certificates**（SSL 证书）页面上，选择证书并单击 **Update**（更新）。或者，单击 SSL 证书以查看其详细信息，然后单击 **SSL** 证书 页面右上角的 更新。
4. 在 **Update SSL Certificate**（更新 SSL 证书）页面上，对证书和/或密钥进行所需的修改，并单击 **OK**（确定）。

在 **Citrix ADC** 实例上安装 **SSL** 证书

February 6, 2024

在 Citrix Application Delivery Controller (ADC) 实例上安装 SSL 证书之前，请确保证书由可信 CA 颁发。此外，请确保证书密钥的密钥强度为 2048 位或更高，并且密钥使用安全签名算法进行签名。

要从另一个 **Citrix ADC** 实例安装 **SSL** 证书，请执行以下操作：

您还可以从选定的 Citrix ADC 实例导入证书，并从 Citrix Application Delivery Management (ADM) GUI 将其应用到其他目标 Citrix ADC 实例。

1. 导航到“网络”>“**SSL** 控制板”。
2. 在 SSL 控制板的右上角，单击 安装。
3. 在 **NetScaler** 实例上安装 **SSL** 证书页面上，指定以下参数：

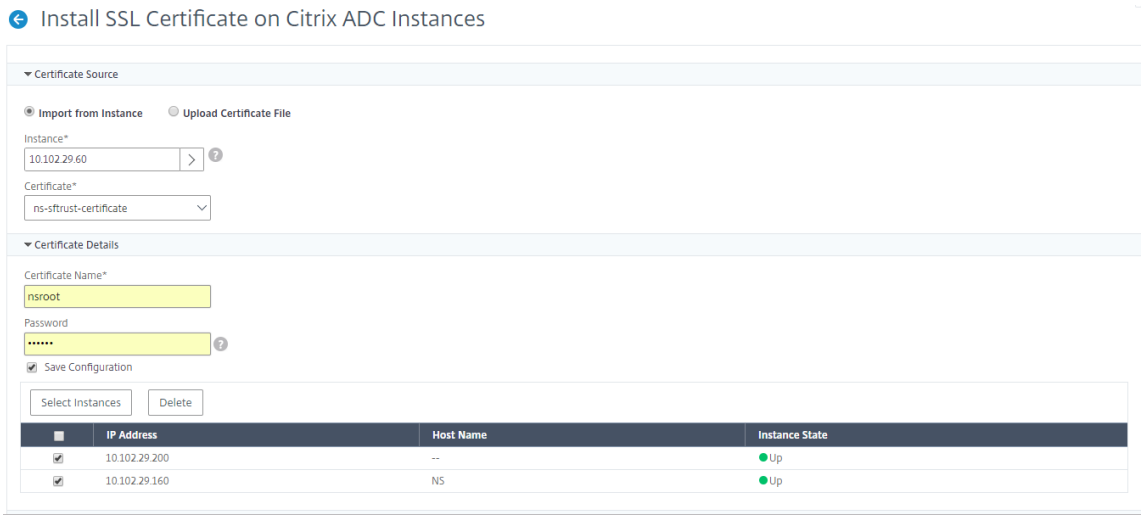
   a) 证书源选
   择要 从实例导入的选项。

   - 选择要从中导入证书的 实例。
   - 从实例上所有 SSL 证 书文件的列表中选择证书。

   b) 证书详细信息

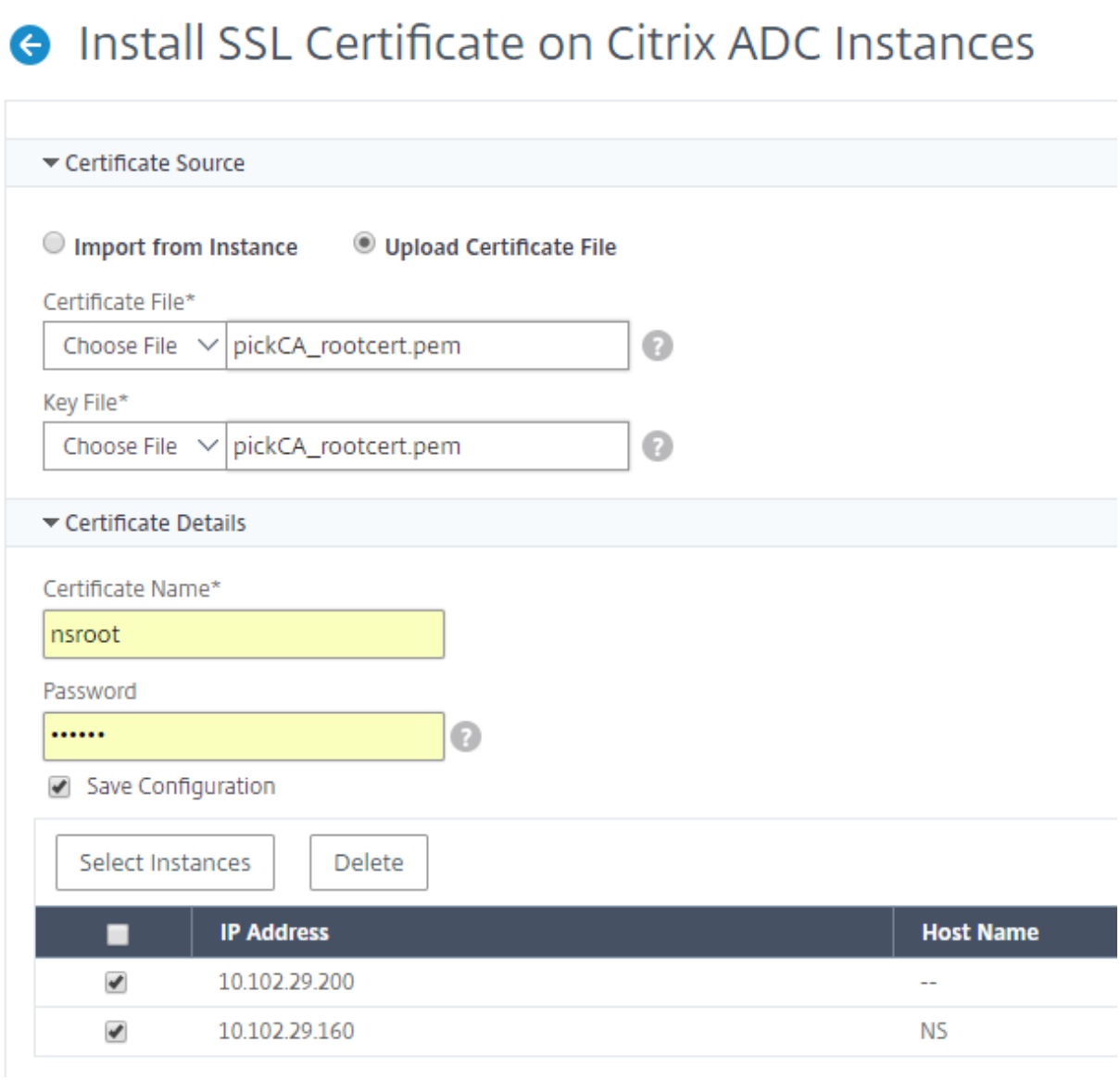
   - 证书名称。指定证书密钥的名称。
   - 密码。用于加密私钥的密码。可以使用此选项上载加密的私钥。

4. 单击“选择实例”以选择要安装证书的 Citrix ADC 实例。
5. 单击确定。



要从 **Citrix ADM** 安装 **SSL** 证书，请执行以下操作：

1. 在 Citrix ADM 中，导航到网络 > **SSL** 控制板。
2. 在控制板的右上角，单击 **Install**（安装）。
3. 在“在 **NetScaler** 实例上安装 **SSL** 证书”页上，选择“上载证书文件”并指定以下参数：
    - 证书文件 -通过选择本 地（您的本地 计算机）或 装置（证书文件必须存在于 Citrix ADM 虚拟实例上）来上载 SSL 证书文件。
    - **Key File**（密钥文件）- 上载密钥文件。
    - **Certificate Name**（证书名称）–指定证书密钥的名称。
    - **Password**（密码）- 用于对私钥进行加密的密码。可以使用此选项上载加密的私钥。
    - 选择实例 -选择要在其上安装证书的 Citrix ADM 实例。
4. 要保存配置以备将来使用，请选中“保存配置”复选框。
5. 单击确定。



创建证书签名请求 **(CSR)**

February 6, 2024

证书签名请求 (CSR) 是将在其中使用证书的服务器上生成的加密文本块。它包含将包含在证书中的信息，例如您组织的名称、公用名（域名）、区/县和国家/地区。

要使用 **Citrix ADM** 创建 **CSR**，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到“网络”>“**SSL** 控制板”。
2. 单击任何图形以查看已安装 SSL 证书的列表，然后选择要为其创建 CSR 的证书，然后从选择 操作列表中选择创建 **CSR** 。

3. 在 **Create Certificate Signing Request (CSR)**（创建证书签名请求 (CSR)）页面上，为 CSR 指定名称。
4. 执行以下操作之一：
   - **Upload a key**（上载密钥）- 选择 **I have a Key**（我有密钥）选项。要上载密钥文件，请选择本 地（您的本地计算机）或 设备（密钥文件必须存在于 Citrix ADM 虚拟实例上）。
   - 创建密钥 -选择“我没有密钥”选项，然后指定以下参数：

加密算法	Type of key（密钥类型）。例如 RSA。
Key File Name（密钥文件名称）	存储 RSA 密钥的文件的名称。
密钥大小	密钥大小（以位为单位）。
Public Exponent Value（公共指数值）	从提供的下拉列表中选择 **3** 或 **F4** 。此值属于创建 RSA 密钥所需的密码算法的一部分。
Key Format（密钥格式）	默认情况下，选择 PEM。PEM 是建议的 SSL 证书密钥格式。
PEM Encoding Algorithm（**PEM** 编码算法）	在下拉列表中，选择要用于加密生成的 RSA 密钥的算法（**DES** 或 **DES3**）。如果选择此算法，则需要提供 PEM 密码。
PEM Passphrase（**PEM** 密码）	如果选择了“PEM Encoding Algorithm”（PEM 编码算法），请输入密码。
Confirm PEM Passphrase（确认 **PEM** 密码）	确认 PEM 密码。

5. 单击 **Continue**（继续）。
6. 在后面的页面上，提供其他详细信息。如果要在不更改默认值的情况下创建 CSR，请单击 **Continue**（继续）。

> 注意
>
> 大多数字段都有从所选证书的主题提取的默认值。主题包含公用名、组织名称、省/市/自治区和国家/地区之类的详细信息。
>
> 大多数 CA 接受通过电子邮件提交证书。CA 将向您提交 CSR 时使用的电子邮件地址返回有效证书。

链接和取消链接 **SSL** 证书

February 6, 2024

可以将多个证书链接在一起来创建证书捆绑包。要将证书链接到另一个证书，第一个证书的颁发者必须匹配第二个证书的域。例如，如果要将证书 A 链接到证书 B，证书 A 的“颁发者”必须匹配证书 B 的“域”。

要使用 **Citrix ADM** 将一个 **SSL** 证书链接到另一个证书，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到“网络”>“**SSL** 控制板”。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择要链接的证书，然后从 **Action**（操作）下拉列表中选择 **Link**（链接）。
4. 从匹配的证书列表中选择要链接到的证书，然后单击 **OK**（确定）。

> 注意
>
> 如果未找到匹配的证书，将显示以下消息：No certificate found to link（未找到证书进行链接）。

要使用 **Citrix ADM** 取消 **SSL** 证书的链接，请执行以下操作：

1. 在 Citrix ADM 中，导航到网络 > **SSL** 控制板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择链接的任一已链接证书，然后从 **Action**（操作）下拉列表中选择 **Unlink**（取消链接）。
4. 单击确定。

> 注意
>
> 如果所选证书未链接到另一个证书，将显示以下消息：Certificate does not have any CA link（证书没有任何 CA 链接）。

配置企业策略

February 6, 2024

您可以在 Citrix Application Delivery Management (ADM) 中配置企业策略并添加所有受信任的 CA、安全签名算法，并为证书密钥选择推荐的密钥强度。如果您的 Citrix 应用程序 Delivery Controller (ADC) 实例上安装的任何证书尚未添加到企业策略中，则 SSL 证书控制板将这些证书的颁发者显示为“不推荐”。

此外，如果证书密钥强度与企业策略中的推荐密钥强度不一致，SSL 证书控制板上那些密钥的强度将显示为“Not Recommended”（不推荐）。

要在 **Citrix ADM** 上配置企业策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 基础架构 > **SSL** 控制面板，然后单击“设置”。
2. 在“SSL 设置”页面上，单击“编辑”图标以添加所有受信任的 CA、安全签名算法，然后为您的证书和密钥选择推荐的密钥强度。

3. 单击 **Save**（保存）以保存企业策略。

轮询 **Citrix ADC** 实例中的 **SSL** 证书

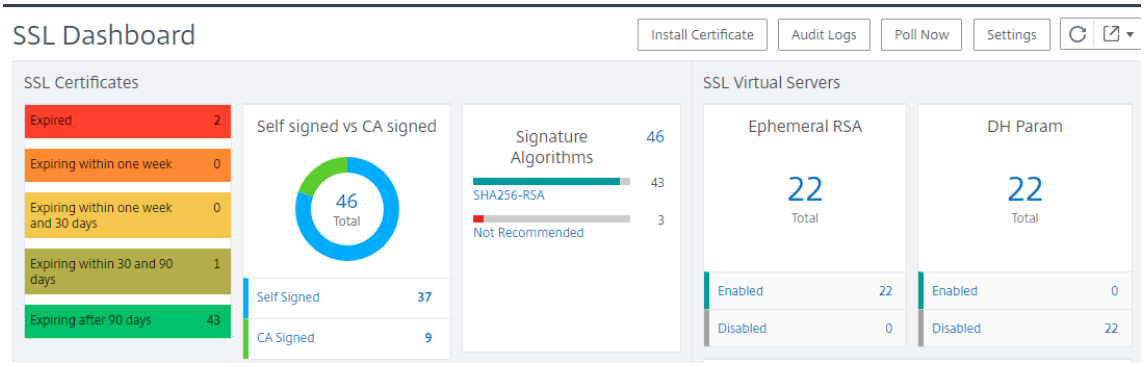
February 6, 2024

Citrix Application Delivery Management (ADM) 使用 NITRO 调用和安全复制 (SCP) 协议，每 24 小时自动轮询一次 SSL 证书。您也可以手动轮询 SSL 证书，在 Citrix Application Delivery Controller (ADC) 实例上发现新添加的 SSL 证书。轮询所有 Citrix ADC 实例 SSL 证书会给网络带来沉重负载。

您可以仅手动轮询一个或多个选定实例的 SSL 证书，而不是轮询所有 Citrix ADC 实例 SSL 证书。

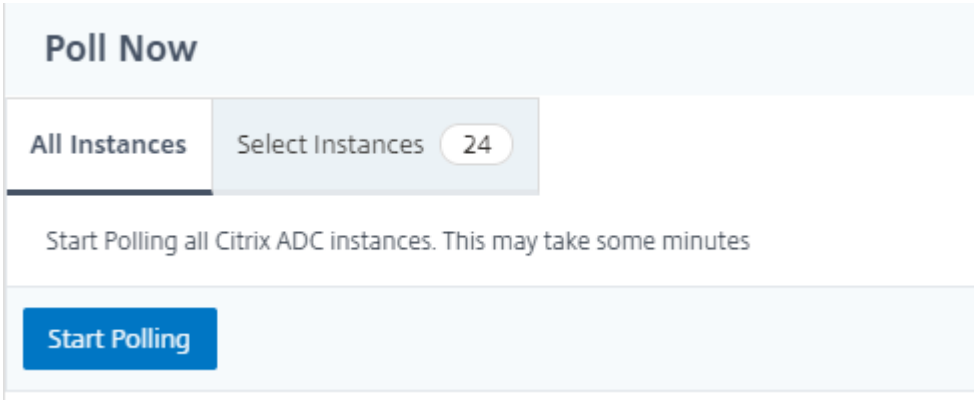
要在 **Citrix ADC** 实例上轮询 **SSL** 证书，请执行以下操作：

1. 在 Citrix ADM 中，导航到网络 > **SSL** 控制板。
2. 在 **SSL** 控制板 页面的右上角，单击 立即轮询。

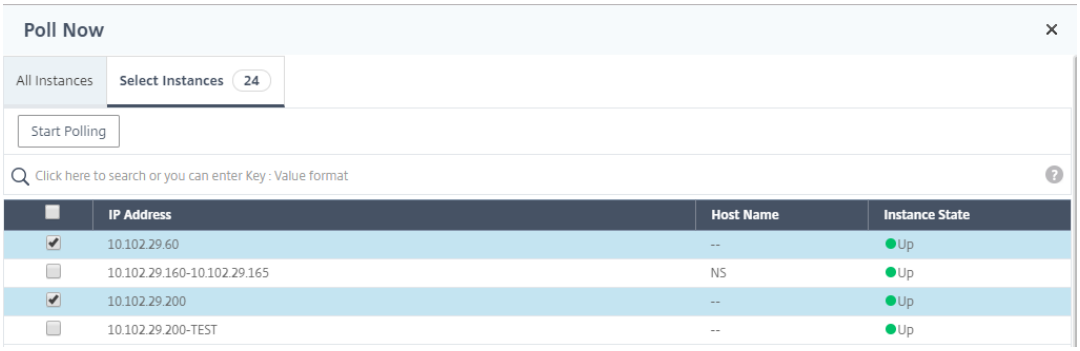


3. 将弹出“立即轮询”页面，您可以选择轮询网络中的所有 Citrix ADC 实例或轮询所选实例。

   a) 要轮询所有 Citrix ADC 实例的 SSL 证书，请选择“所有实例”选项卡，然后单击“开始轮询”。



   b) 要轮询特定实例，请选择 选择实例选 项卡，从列表中选择实例，然后单击 立即轮询。



配置作业

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 配置管理流程可确保在网络中的多个 Citrix Application Delivery Controller (ADC) 实例之间正确复制配置更改、系统升级和其他维护活动。

Citrix ADM 允许您创建配置作业，这将有助于您在多个设备上轻松执行所有这些活动作为单个任务。配置作业和模板将最重复的管理任务简化为 Citrix ADM 上的单个任务。配置作业包含可以在一个或多个托管设备上运行的一组配置命令。

配置作业可以使用 SSH 命令执行配置命令，也可以使用 SCP 将文件副本从本地存储复制到另一个设备，例如，可以计划 HA 故障转移或 HA 升级。

您可以在 Citrix ADM 中使用以下四个选项之一来创建配置作业。可使用以下项之一创建针对系统的可重用命令和指令源以执行配置作业。

1. 配置模板
2. 实例
3. 文件
4. 录制和播放

配置模板

您可以在创建新作业并将一组配置命令保存为模板时创建配置模板。在“Create Jobs”（创建作业）页面上保存这些模板时，它们会自动显示在“Create Template”（创建模板）页面上。您可以使用以下模板之一：

配置编辑器：您可以使用配置编辑器键入 CLI 命令，将配置保存为模板，然后使用它来配置作业。

内置模板：您可以从配置模板列表中进行选择。这些模板提供了 CLI 命令的语法，并允许您为变量指定值。下表中列出了内置模板及其说明。可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例

如，可以使用内置模板选项计划作业来配置 syslog 服务器。还可以选择立即执行作业，也可以选择计划在以后的某个阶段执行作业。

实例

您可以对运行 Citrix ADC 11.0 版及更高版本的 Citrix SDX 实例执行单捆绑升级。要执行单捆绑升级，请使用 Citrix ADM 中的内置任务。您还可以通过提取正在运行的配置或已保存的配置并在同一类型的另一个 Citrix ADC 实例上执行命令来升级 Citrix ADC 实例。这样，您可以在一个实例上复制另一个实例的配置。

文件

您可以从本地计算机上载配置文件并创建作业。

使用文件的优势

- 您可以使用任何文本文件来创建可重用的配置命令源。
- 不需要进行任何种类的格式设置。
- 文件可以保存在您的本地计算机上。

您可以创建并保存新文件，也可以导入现有文件，然后运行命令。

录制和播放

使用创建作业，您可以输入自己的 CLI 命令，也可以使用“录制和播放”按钮从 Citrix ADC 会话中获取命令。运行作业时，选定实例上 ns.conf 中的更改将被记录并复制到 Citrix ADM。

相关文章

- 如何在配置作业中使用 SCP (put) 命令
- 如何在配置作业中使用变量
- 如何使用更正命令创建配置作业
- 如何使用配置模板创建审核模板
- 如何使用录制和播放来创建配置作业
- 如何在 Citrix ADM 上使用主配置模板

创建配置作业

February 6, 2024

作业是可以在一个或多个托管实例上创建并运行的一组配置命令。您可以使用 Citrix Application Delivery Management (ADM) GUI 创建作业以跨实例进行配置更改、在网络上的多个实例上复制配置以及录制和播放配置任务，并将其转换为 CLI 命令。

可以使用 Citrix ADM 的配置作业功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

要在 **Citrix ADM** 上创建配置作业，请执行以下操作：

1. 导航到“网络” **>** “配置作业”。
2. 单击 创建作业。
3. 在 创建作业 页面的 选择配置 选项卡下，指定任务名称并从下拉列表中选择实例类型。
4. 在 配置源 下拉列表中，选择要创建的配置作业模板。为选定模板添加命令。您可以输入命令或从保存的配置模板中导入现有命令。在配置作业中创建作业时，还可以在配置编辑器中添加不同类型的多个模板。从“配置源”下拉列表中，选择不同的模板，然后将模板拖放到配置编辑器中。模板类型可以是配置模板、内置模板、主配置、录制和播放、实例和文件。

   > 注意
   >
   > 如果您首次添加部署主配置作业模板，然后添加不同类型的模板，则整个作业模板将为主配置类型。

5. 您还可以在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。您还可以在以后编辑配置作业时重新排列和重新排序命令行。
6. 您可以定义变量，以便您可以为这些参数分配不同的值或在多个实例上执行某个作业。您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。单击“预 览变 量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。
7. 在“选择 实例”选项卡中，选择要运行配置审核的实例，然后 单击“下一步”。
8. 在“指定变量值”选项卡中，有两个选项：

   a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。

   b) 输入您为所有实例定义的变量的通用值

9. 单击下一步。
10. 您可以在“作业预览”选项卡上评估和验证要在每个实例上运行的命令。要评估回滚命令，请选中“预览回滚 命令”复选框
11. 在“执 行”选项卡中，选择立即执行作业或计划稍后执行作业。此外，您还必须选择命令失败时 Citrix ADM 应采取的操作。

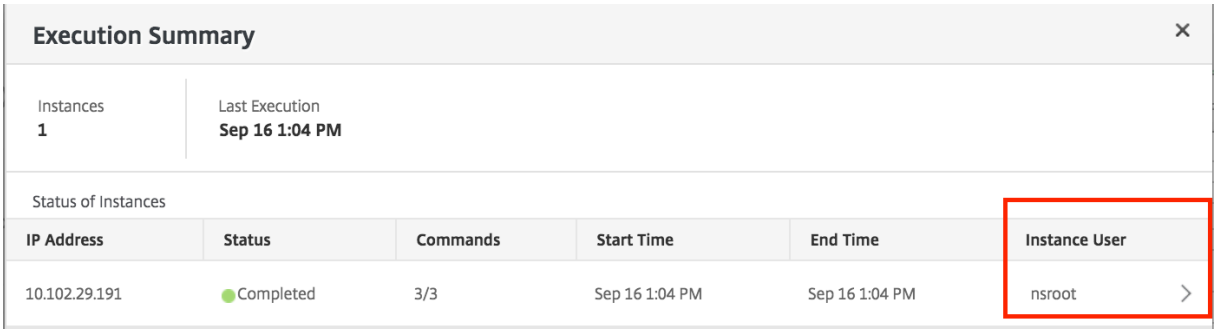
要发送任务的电子邮件通知，请执行以下操作：

现在每次执行或计划作业时，都会发生电子邮件通知。通知中包含作业成功或失败之类的详细信息以及相关的详细信息。

创建作业后，在“Execute”选项卡中的“Receive Execution Report Through”（执行报告接收方式）下方选中 **Email**（电子邮件）复选框。从下拉列表中选择电子邮件通讯组列表。还可以单击 **+** 图标并指定电子邮件服务器详细信息来创建电子邮件通讯组列表。

要查看执行摘要详细信息，请执行以下操作：

导航到“网络”>“配置作业”。选择一个作业，并单击 **Details**（详细信息）。单击“执行摘要”可查看执行该作业的实例的状态、在该作业上执行的命令、作业的开始和结束时间以及实例用户名。



使用录制和播放创建配置作业

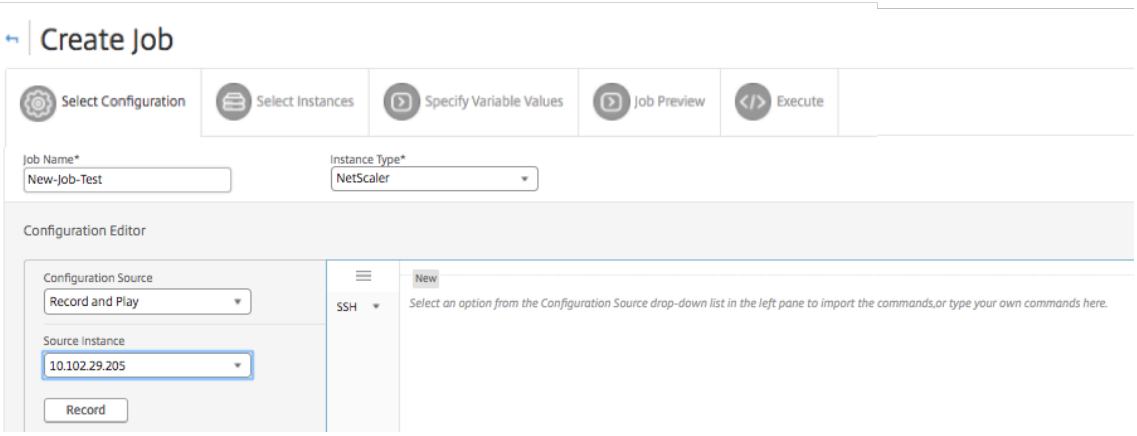
February 6, 2024

如果您习惯使用 NetScaler GUI 配置 NetScaler 实例，有时，您可能发现很难想起准确的 CLI 命令来创建配置任务，并在多个 NetScaler 实例上运行该任务。

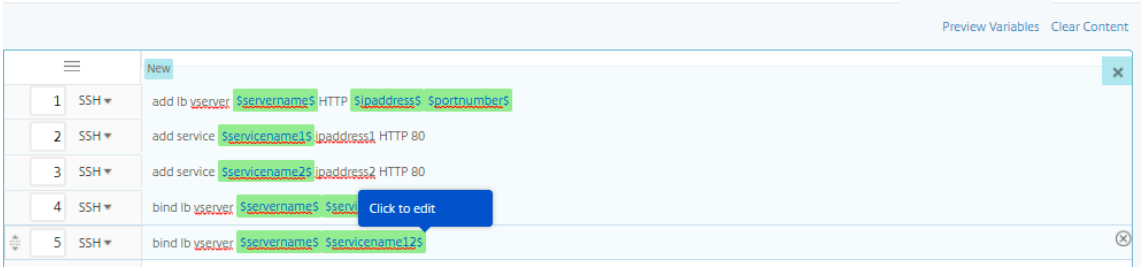
Citrix ADM 使您能够记录使用 NetScaler 实例的 GUI 执行的配置任务，并将其转换为 CLI 命令。之后可以使用这些 CLI 命令创建配置任务，并在多个实例上运行此任务。

录制 **GUI** 配置并将其转换为配置任务

1. 导航到 **Networks**（网络）**> Configuration Jobs**（配置作业），然后单击 **Create Job**（创建作业）。
2. 指定作业名称和实例类型。
3. 从“配置源”列表中，选择“录制并播放”，然后选择要从中录制配置的源实例。单击 **Record**（录制）。



4. 将打开 **NetScaler GUI**。配置您希望配置任务包含的功能和设置。然后关闭 NetScaler GUI 窗口并单击 **Configuration Editor**（配置编辑器）中的 **Stop**（停止）。在左侧窗格中，命令显示为链接。将命令拖放到右侧窗格，然后单击 **Next**（下一步）。

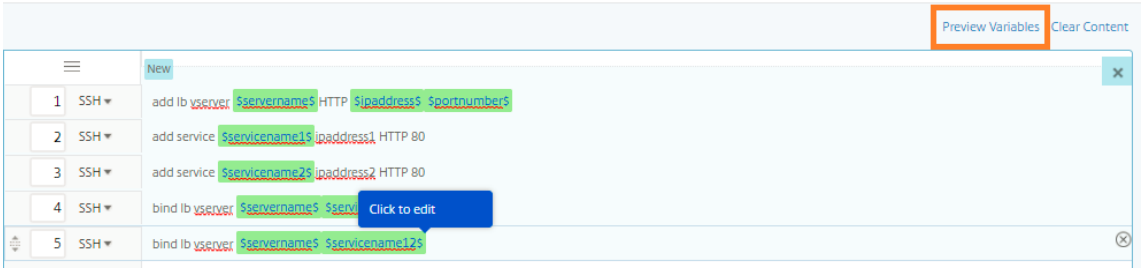


然后，您可以根据需要在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。

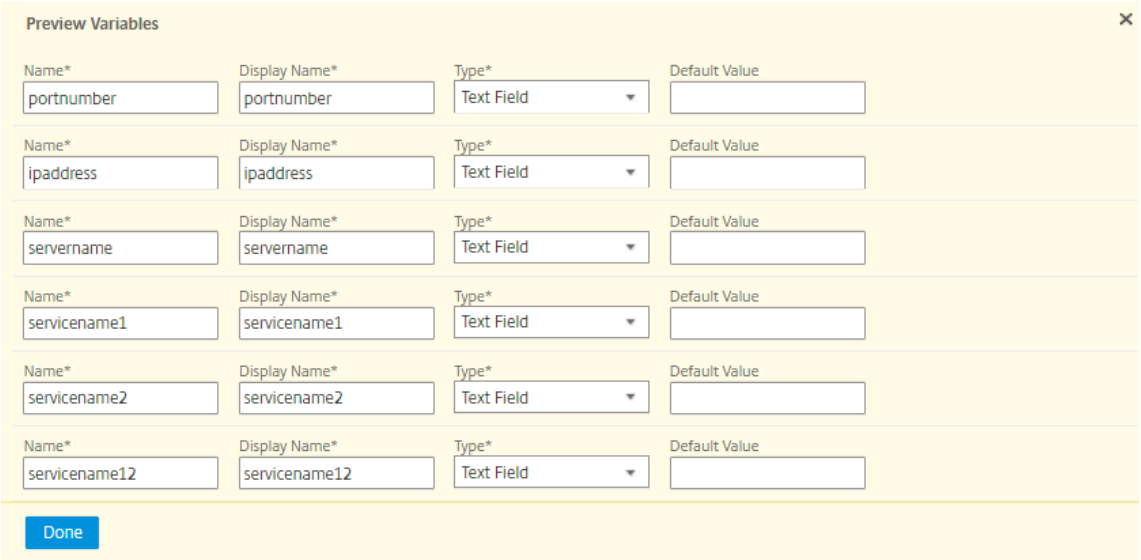
5. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
6. 执行以下操作之一可在单个统一视图中查看所有变量：

   - 创建配置作业时，导航到网络 **>** 配置作业，选择创建作业。在 创建作业 页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 网络 **>** 配置作业，选择作业名称并单击 编辑。在“配置作业”页上，您可以查看创建配置作业时添加的所有变量。

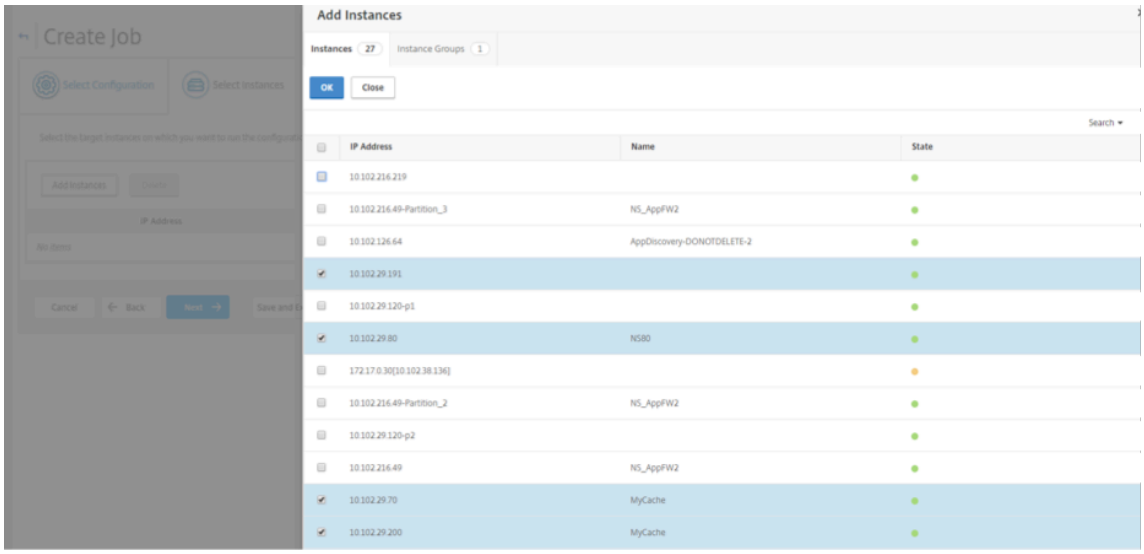
7. 然后，您可以单击“预览变量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



8. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完 成”按钮。



9. 单击添加实例，然后选择要在其上运行配置作业的实例。单击“确定”，然后单击“下一步”。



10. 如果在命令中指定了变量，请在“指定变量值”选项卡上，选择以下选项之一以指定实例的变量：

    - 上载变量值的输入文件： 单击 “下载输入密钥 文件”以下载输入文件。在输入文件中，输入已在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
    - 所有实例的公用变量值：输入变量值。变量因选定的模板而不同。

    包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上载的这些输入文件。

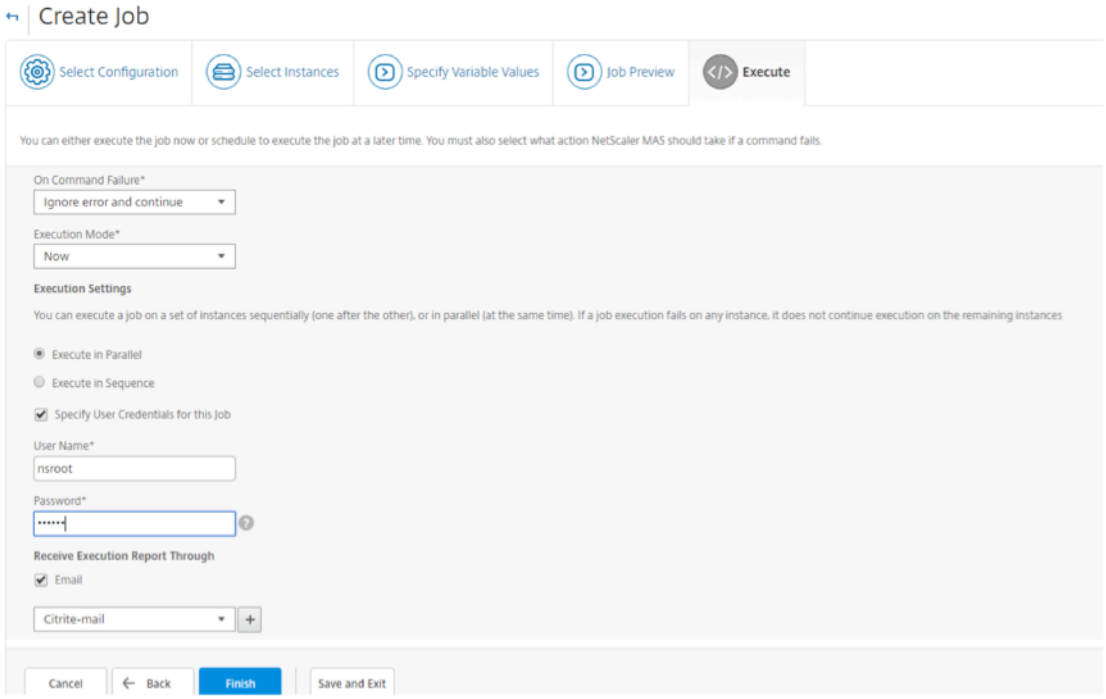
    要在创建配置作业时查看已执行的配置作业，请导航到网络 > 配置作业，然后单击 创建作业。在 创建任务 页面中。在“指定变量值”选项卡上，选择“所有实例的通用变量值”选项以查看上载的文件。要编辑输入文件，请下

载输入文件，然后编辑和上载文件（保持相同的文件名）。

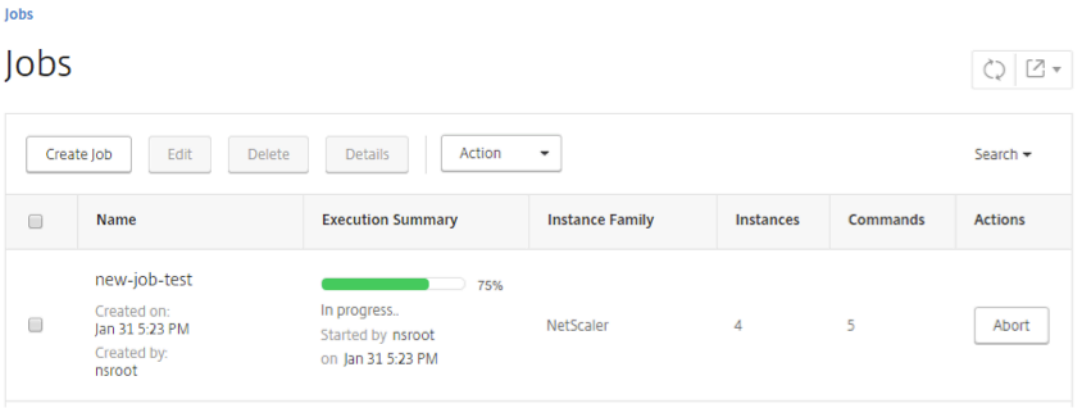
要在编辑配置作业时查看已执行的配置作业，请导航到“网络”**>**“配置作业”，选择“作业名称”，然后单击“编辑”。在 配置作业 页面的 指定变量值 选项卡上，选择 所有实例的公用变量值 选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）.10. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

11. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
12. 在“执行”(**Execute**) 选项卡上，您可以选择立即执行作业或计划在以后执行作业。您还可以选择命令失败时 Citrix ADM 应采取的操作。

    您还可以选择允许授权用户在您的托管实例上执行作业，并可以选择是否发送有关作业成功或失败以及其他详细信息的电子邮件通知。



13. 在“作 业 页面上，您可以查看所有实例上的配置任务执行进度。



使用配置作业将配置从一个实例复制到多个实例

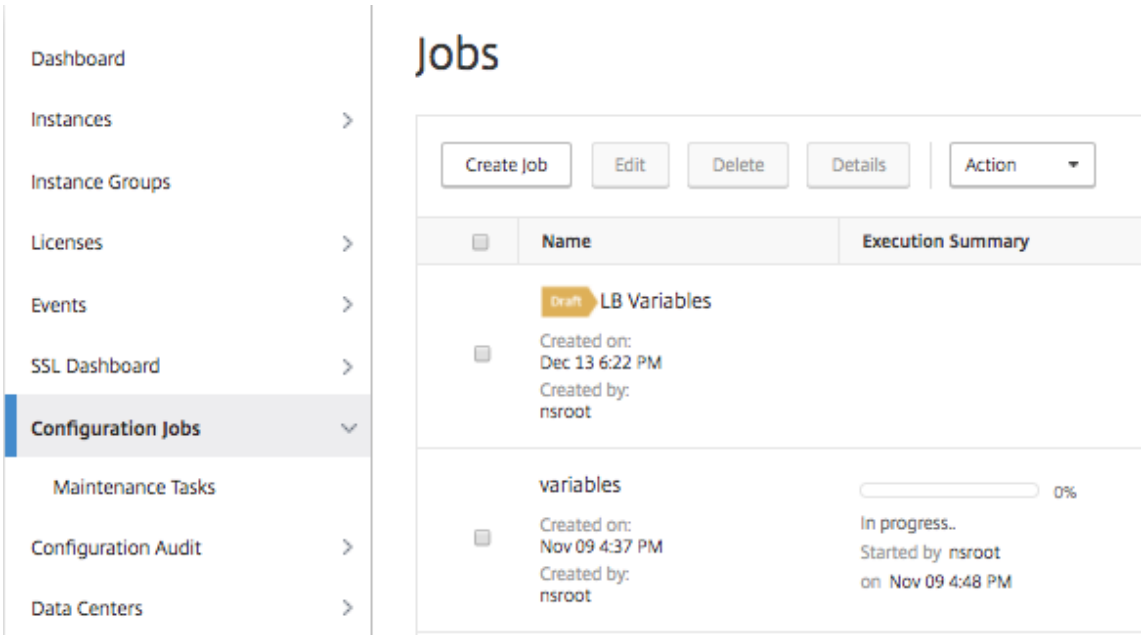
February 6, 2024

您可以使用 Citrix ADM 的“配置作业”功能从 NetScaler 实例中提取特定配置并将其复制到多个实例上。

例如，您可能已经在 NetScaler 实例上为部署配置了负载平衡和前端优化 (FEO)。但是，现在您希望只将 FEO 配置复制到其他 NetScaler 实例。

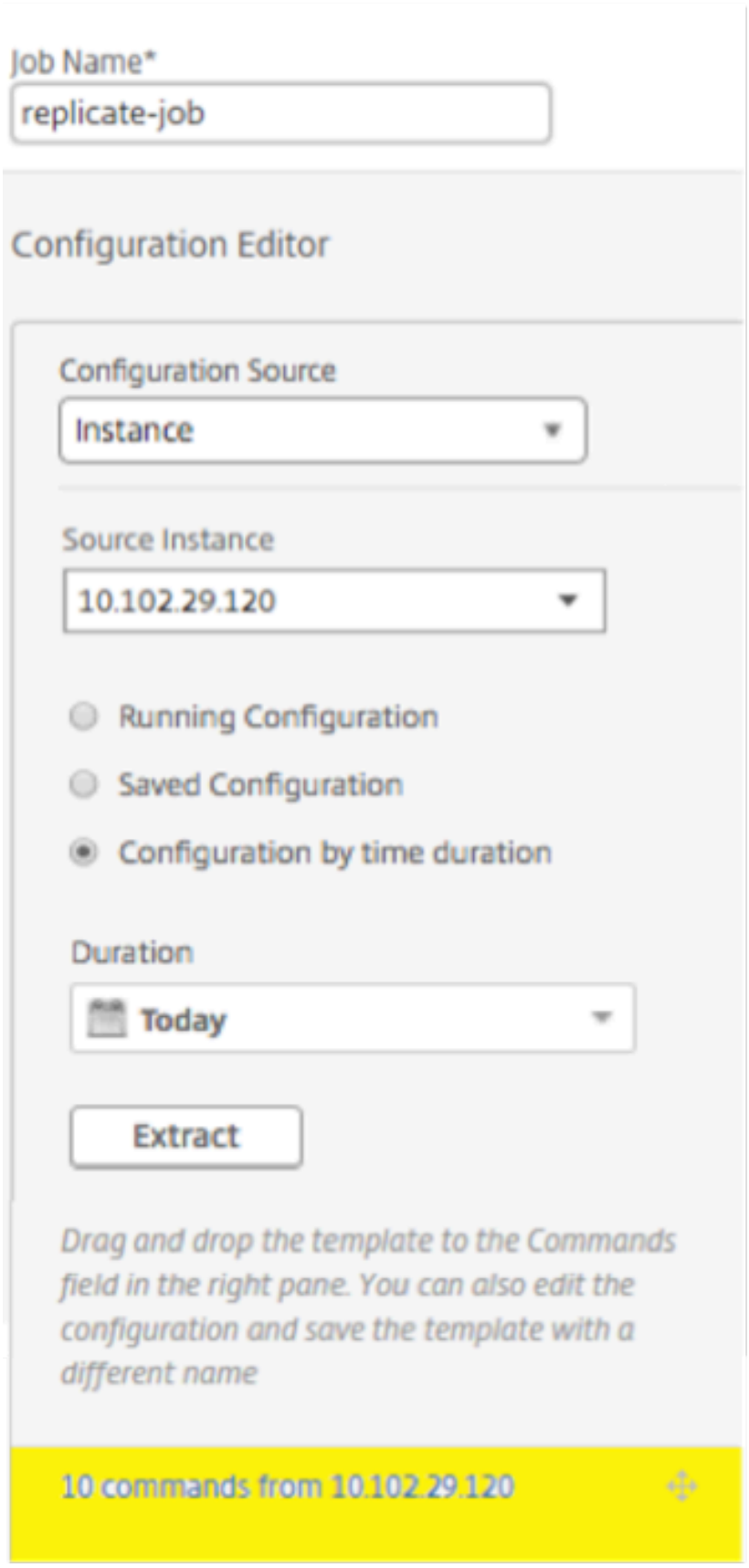
要检索配置并将其从一个实例复制到其他 **NetScaler** 实例，请执行以下操作：

1. 导航到 **Networks**（网络）> **Configuration Jobs**（配置作业），然后单击 **Create Job**（创建作业）。



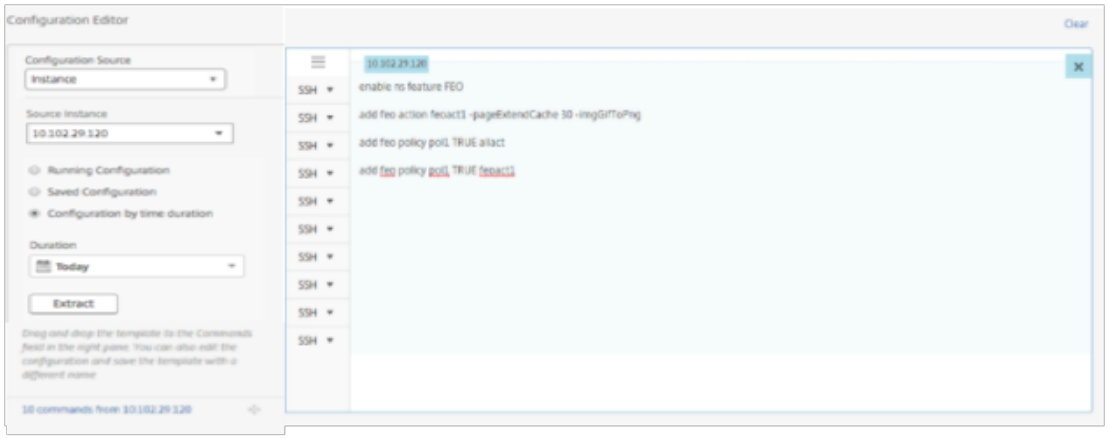
2. 指定作业名称和实例类型。
3. 选择 实例 作为 配置源，然后选择要复制其配置的源实例。选择要提取的配置类型。如果您选择“按时间持续时间配置”，设置运行此配置的时间段，然后单击 提取”。

   在选择的持续时间内该实例上执行的命令数显示在屏幕上，如下图中突出显示的部分。



4. 将命令拖放到右窗格的“命令”字段中。

仅保留与 FEO 有关的命令，手动删除与负载平衡有关的命令，或与任何其他配置有关的命令，然后单击 **Next**（下一步）。



5. 单击 添加实例，然后添加要应用 FEO 配置的实例。单击“确定”，然后单击“下一步”。
6. 如果在命令中指定了变量，请在“Specify Variable Values”（指定变量值）选项卡上单击 **Download Input Key File**（下载输入密钥文件）。在下载的文件中，指定变量的值，然后将文件上载到 Citrix ADM。
7. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
8. 在 **Execute**（执行）选项卡上，单击 **Finish**（完成）以对选择的 NetScaler 实例执行作业。

在配置作业中使用变量

February 6, 2024

配置作业是可以在一个或多个托管实例上执行的一组配置命令。在多个实例上执行相同配置时，您可能希望配置中所用参数使用不同的值。您可以定义变量，以便您可以为这些参数分配不同的值或在多个实例上执行某个作业。

例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。现在，您可能希望两个实例上的配置相同，但虚拟服务器和服务名称和 IP 地址的值不同。您可以使用配置作业功能来实现这一点，即使有变量来定义虚拟服务器和服务名称和 IP 地址。

在此示例中，使用了以下命令和变量：

add lb vserver **servername** HTTP **ipaddress portnumber**

add service **servicename1 ipaddress1** HTTP 80

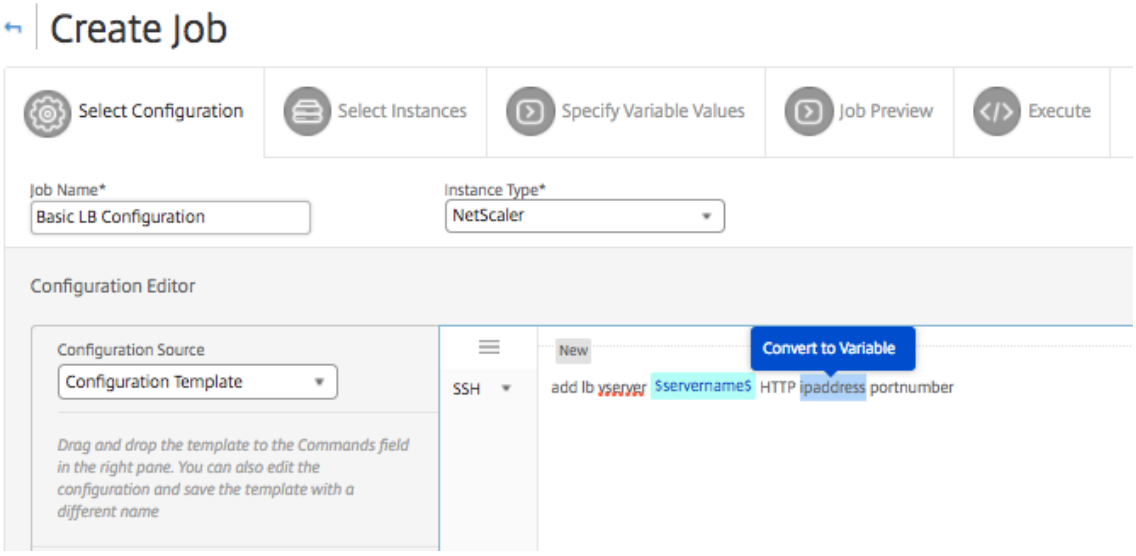
add service **servicename2 ipaddress2** HTTP 80

bind lb vserver **servername servicename1**

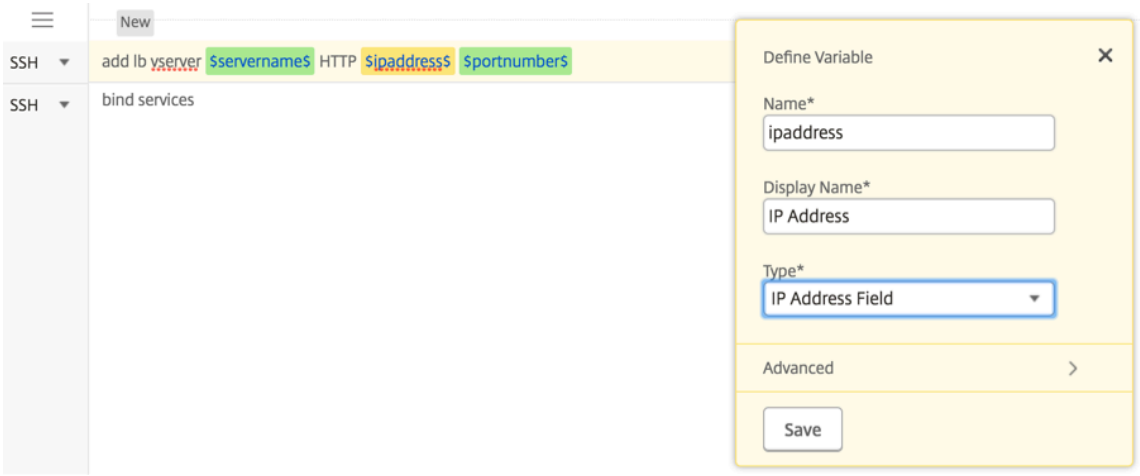
bind lb vserver **servername servicename2**

要通过在 **Citrix ADM** 中定义变量来创建配置作业，请执行以下操作：

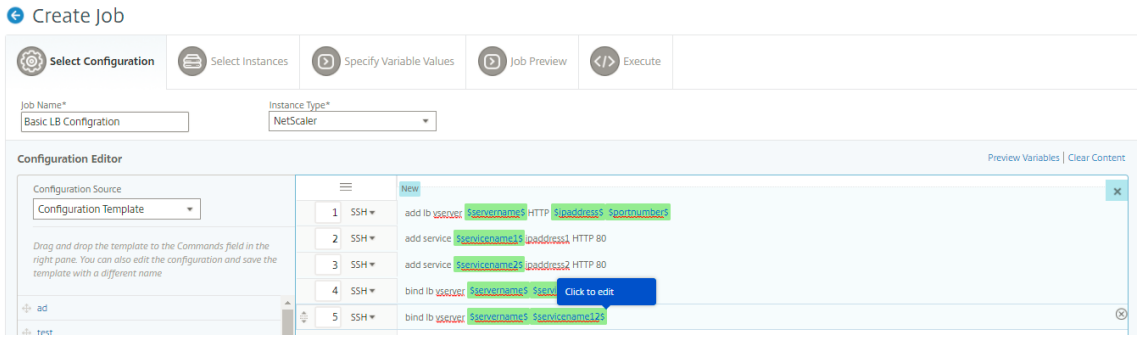
1. 导航到“网络”>“配置作业”。
2. 点击 创建任务。
3. 在 C **reat** e Job 页面上，选择自定义作业参数，例如任务名称、实例类型和配置类型。
4. 在“Configuration Editor”（配置编辑器）中，键入命令以添加一个负载平衡虚拟服务器、两个服务以及将服务绑定到虚拟服务器。双击选择要转换为变量的值，然后单击“转换为变量”。例如，选择负载平衡服务器 IP 地址的 *IP* 地址，然后单击“转换为变量”，如下图所示。



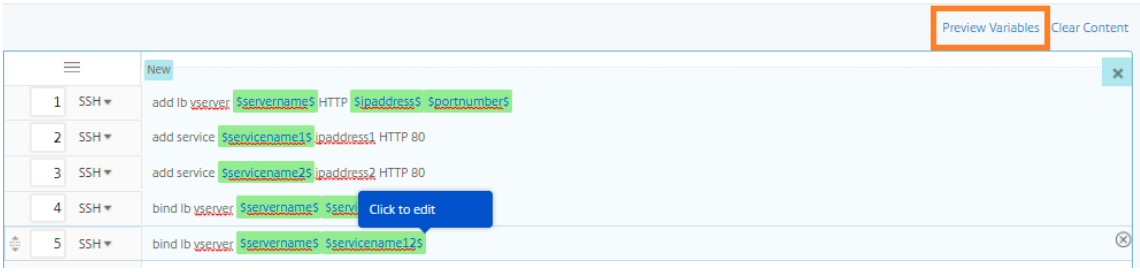
5. 看到美元符号括住变量值后，单击变量以进一步指定变量的详细信息，例如，名称、显示名称和类型。如果要进一步为变量指定默认值，也可以单击 高 级”选项。单击 保存，然后单击 下一步。



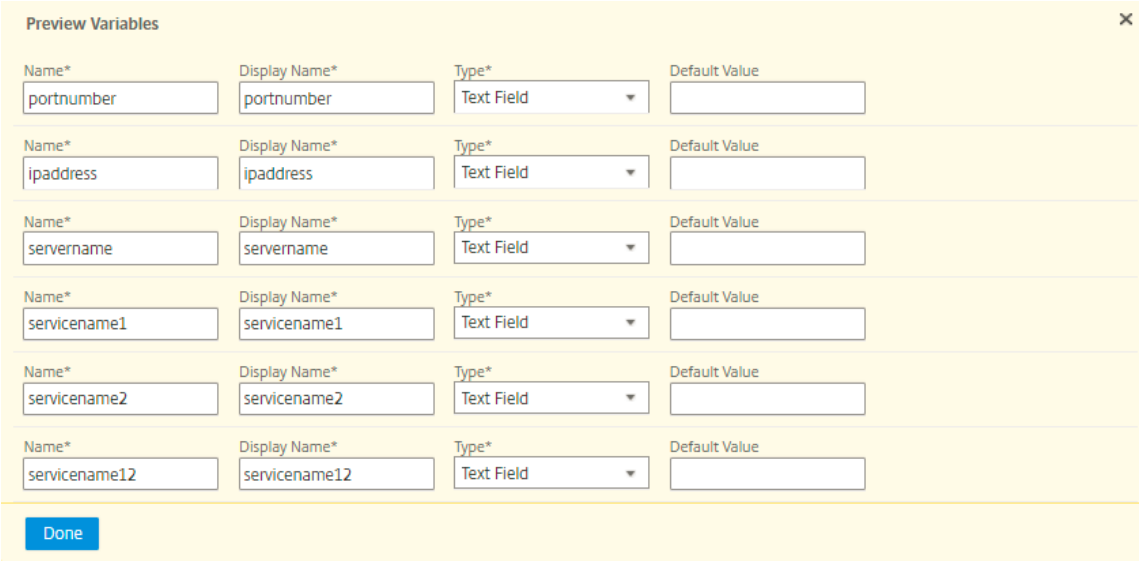
键入命令的其余部分，并定义所有变量。



6. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
7. 执行以下操作之一可在单个统一视图中查看所有变量：
   - 创建配置作业时，导航到网络 **>** 配置作业，选择创建作业。在 创建作业 页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 网络 **>** 配置作业，选择作业名称并单击 编辑。在“配置作业”页上，您可以查看创建配置作业时添加的所有变量。
8. 然后，您可以单击“预览变量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



9. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完 成”按钮。

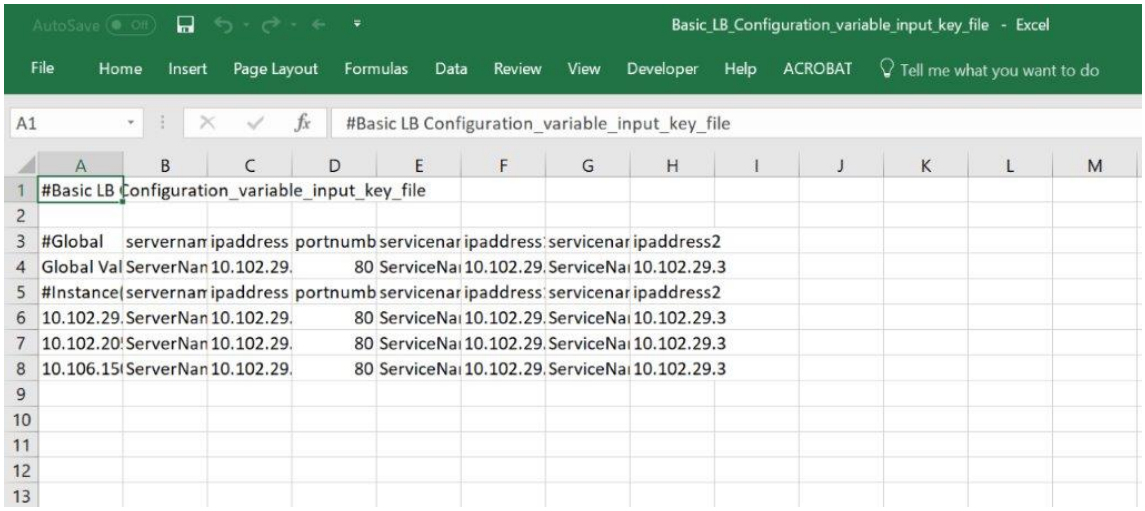


10. 然后，您可以根据需要在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。
11. 选择要对其运行配置作业的实例。
12. 在“指定变量值”选项卡中，选择“上载变量值的输入文件”选项，然后单击“下载输入密钥文件”。在我们的示例中，您将需要指定每个实例上的服务器名称、服务器和服务的 IP 地址、端口号以及服务名称。保存文件并将其上载。如果未准确定义您的值，系统可能会抛出错误。
13. 输入密钥文件已下载到您的本地系统，您可以通过为之前选择的每个 NetScaler 实例指定变量值来对其进行编辑，然后 单击“上载”将输入密钥文件上载到 Citrix ADM。单击下一步。输入密钥文件将下载到您的本地系统，您可以通过为您之前选择的每个 NetScaler 实例指定变量值来对其进行编辑。

    > 注意 在输入密钥文件中，变量定义在三个级别：
    >
    > - 全局级别
    > - 实例组级别
    > - 实例级别

    全局变量是应用于所有实例的变量值。实例组级别变量值应用于在组中定义的所有实例。实例级变量值仅应用于特定实例。

    Citrix ADM 将实例级别值置于第一优先级。如果没有为单个实例的变量提供任何值，Citrix ADM 将使用在组级别提供的值。如果未在组级别提供任何值，Citrix ADM 将使用在全局级别提供的变量值。如果为所有三个级别的变量提供输入，Citrix ADM 将使用实例级别值作为默认值。
14. 单击“上载”将输入密钥文件上载到 Citrix ADM。单击下一步。



> 重要
>
> 当您从 Mac 上载 CSV 文件时，Mac 会使用分号而不是逗号存储 CSV 文件。这将导致配置失败，当您上载输入文件并运行作业。如果您使用的是 Mac，请使用文本编辑器进行必要的更改，然后上载文件。

15. 您还可以为所有实例指定通用变量值，然后单击“上载”将输入密钥文件上载到 Citrix ADM。

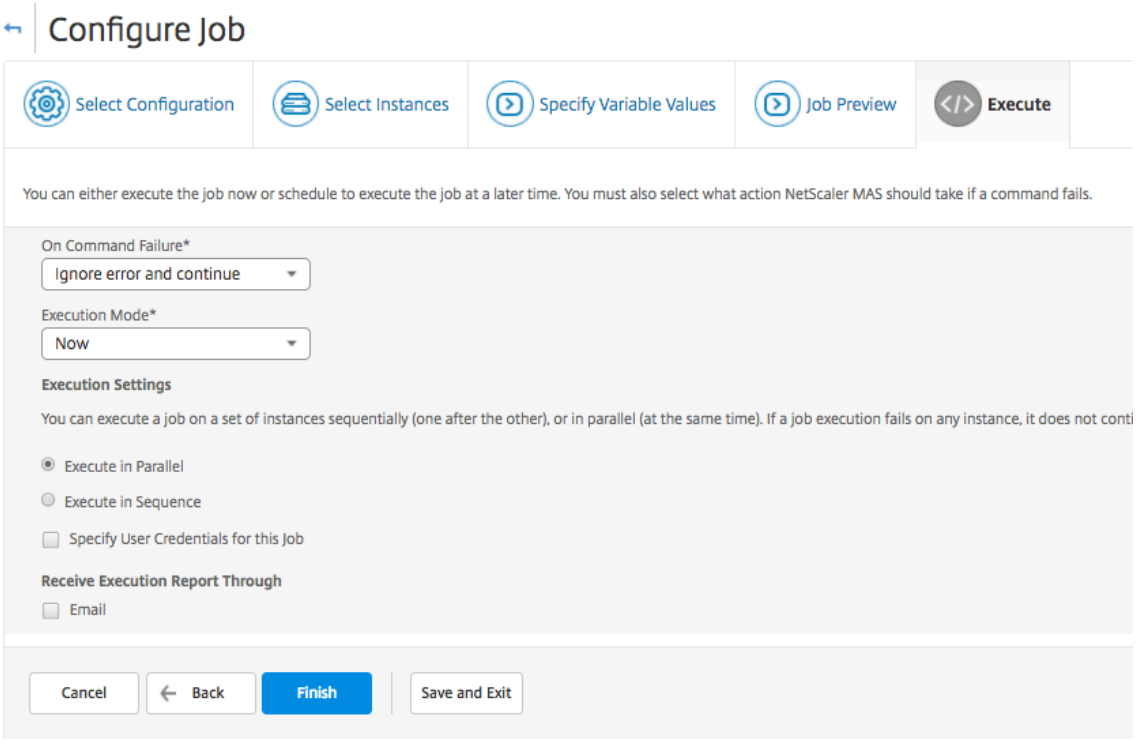
    包含变量值的键输入文件在配置作业中保留（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上载的这些输入文件。

    要在创建配置作业时查看已执行的配置作业，请导航到网络 **>** 配置作业，然后单击 创建作业。在 创建任务 页面中。在“指定变量值”选项卡上，选择“所有实例的通用变量值”选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）。

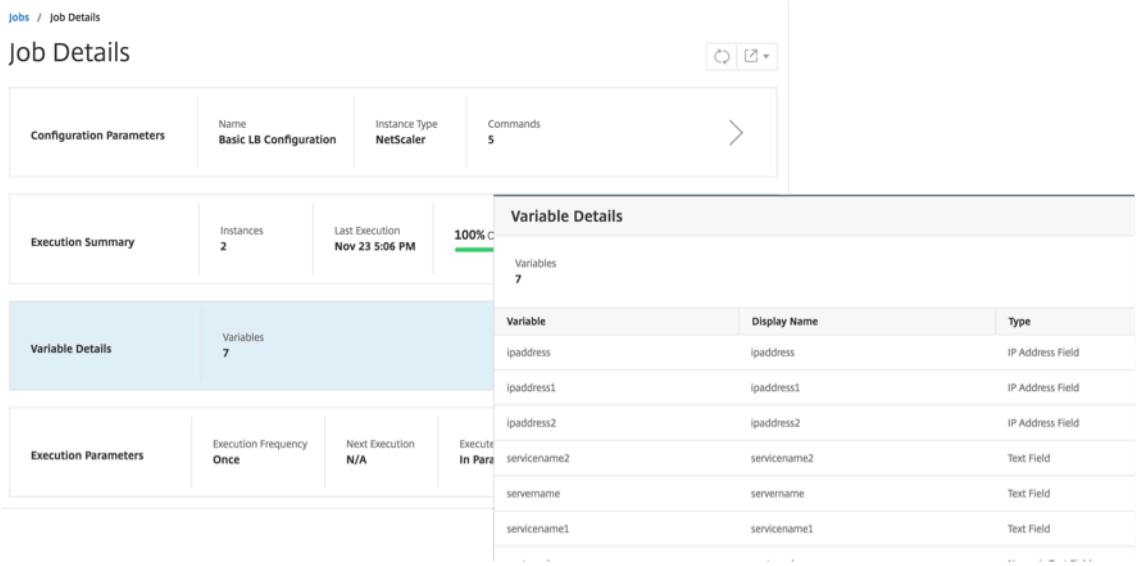
    要在编辑配置作业时查看已执行的配置作业，请导航到“网络”**>**“配置作业”，选择“作业名称”，然后单击“编辑”。在 配置作业 页面的 指定变量值 选项卡上，选择 所有实例的公用变量值 选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）。

16. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

17. 在“执行”选项卡中，您可以选择立即执行作业，也可以将其安排在稍后执行。您还可以选择在命令失败时以及是否要发送有关任务成功或失败的电子邮件通知以及其他详细信息时，Citrix ADM 应采取的操作。



配置并执行任务后，您可以导航到 网络 > 配置作业，然后选择刚才配置的作 业，以查看作业的详细信息。单击“详细信息”，然后单击“变量详细信息”以查看添加到作业中的变量列表。



> 注意
>
> 当您保存作业并退出时，或者安排作业在稍后时间点运行时，Citrix ADM 将保留为步骤 **5** 中的变量提供的值。

通过更正命令创建配置作业

February 6, 2024

您可以使用 Citrix Application Delivery Management (ADM) 中的审核模板功能监视托管 Citrix ADC 实例中的配置更改，并对配置错误进行故障排除。

使用审核模板来审核配置更改的典型工作流包括以下步骤

1. 使用一组有效/预期的 Citrix ADC 命令创建审核模板，用于审核实例配置。
2. 选择要运行审核模板的 Citrix ADC 实例，以检查正在运行的配置和预期的配置之间是否存在差异。
3. 了解差别/更正命令，并利用“Create Job”（创建作业）功能使实例的配置进入期望状态

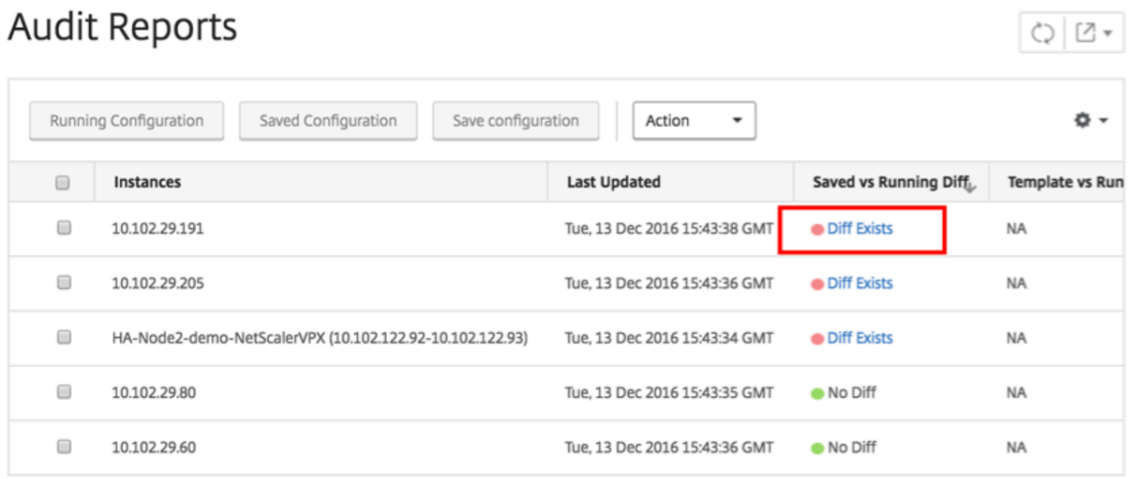
考虑一种情况，即多个管理员正在管理五个 Citrix ADC 实例。所有这些管理员在需要任何更改时更新现有实例配置。超级管理员想要确保，无论其他管理员做了什么更改，一组特定的重要配置保持不变。对于此用例，超级管理员创建了一个配置模板，该模板预计将出现在 Citrix ADC 实例上，然后针对这些实例运行该模板。Citrix ADM 将审核模板配置与正在运行的配置进行比较，并在配置 审核控制板上报告任何不匹配 情况。

如果您注意到某些实例的配置发生了变化，则可以使用 Citrix ADM 更正命令功能使用修改和更正后的特定 Citrix ADC 实例的配置命令创建配置作业。

如果审核模板配置和正在运行的配置之间存在任何差异，则审核报告页面上将显示差异存在状态消息。单击 差异退出 链接将转到 配置差异 页面，您可以在其中查看纠正命令。您还可以使用这些更正命令创建配置作业，然后在特定的 Citrix ADC 实例上执行该任务，使它们恢复到所需的配置。

使用 **Citrix ADM** 上的更正命令创建配置作业

1. 导航到“网络”>“配置审核”。
2. 在 配置审核 页面上，单击两个圆环图中的任意一个以访问 审核报告 页面。
3. 单击要更正配置命令的实例的差异存在链接（在表中“保存的与正在运行的差异”列下）。此时将显示 配置差异 页面，其中列出了该实例的“已保存配置”、“正在运行的配置”和“更正配置”之间的差异。



4. 单击 创建作业 以转到 创建作业 页面，在该页面上预先填充了纠正命令。有关如何创建配置作业的说明，请参阅 如何在 Citrix ADM 上创建配置作业。

将运行和保存的配置从一个 **NetScaler** 实例复制到另一个实例

February 6, 2024

May 24, 2018

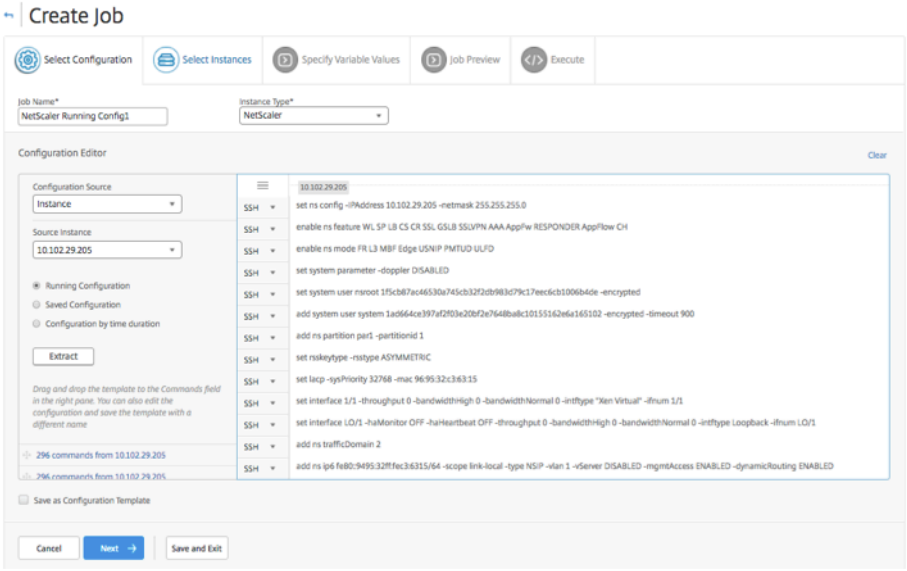
现在可以将 NetScaler 实例的配置复制到其他实例。在 Citrix ADM 中配置作业时，请选择一个实例作为配置源，然后选择所选实例的正在运行或保存的配置。

例如，当您选择“正在 运行的配置 并单击 提取 时，Citrix ADM 会向选定的 NetScaler 实例发送请求以查找正在运行的配置，并将其显示为模板。您可以将模板拖放到右侧窗格的 命令 字段中。您可以修改命令、参数和实例。

要将一个实例的运行和保存的配置命令复制到 **Citrix ADM** 上的另一个实例，请执行以下操作：

1. 导航到“网络”>“配置作业”，然后单击“创建作业”。

2. 指定作业名称和实例类型。例如，将 NetScaler Running Config1 指定为您的任务名称，将实例类型指定为 *NetScaler*。
3. 选择 实例 作为 配置源，选择要在其他实例上复制其配置的源实例。
4. 您将看到以下三个选项：
   - Running Configuration（正在运行的配置）
   - Saved Configuration（保存的配置）
   - Configuration by time duration（按持续时间的配置）
5. 选择“运行配置”，然后单击“提取”。将显示在相应实例上执行的正在运行的配置命令数。



6. 将命令拖放到右窗格的“命令”字段中。
7. 您可以在“Commands”（命令）字段中编辑命令。例如，如果提取的命令是要设置 NetScaler 实例。这可能包括添加分区、设置负载平衡以及将负载平衡服务器绑定到服务等。您可能想要编辑您的命令，以设置不包含分区的新 NetScaler 实例。因此，要删除分区，请手动删除与创建分区相关的命令，然后单击“下一步”。
8. 单击“添加实 例”，然后添加要应用运行配置命令的实例。单击“确定”，然后单击“下一步”。
9. 如果您在命令中指定了变量，请在“指定变量值”选项卡上，单击“下载输入密钥文件”。在下载的文件中，指定变量的值，然后将文件上载到 Citrix ADM。
10. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

11. 在“执行”选项卡中，您可以选择立即执行作业，也可以将其安排在稍后执行。您还可以选择 Citrix ADM 应采取什么操作，命令会失败，如果您想发送有关任务成功或失败以及其他细节的电子邮件通知。

重复使用已执行的配置作业

February 6, 2024

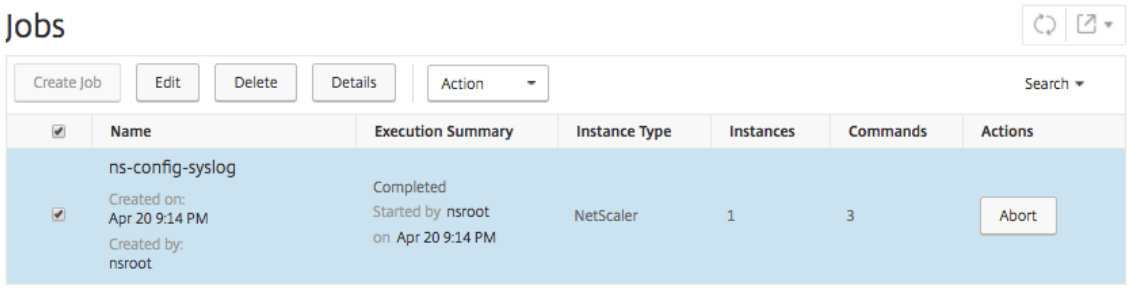
配置作业允许您创建一组配置命令，您可以在一个或多个托管实例上运行。还可以在修改作业中的命令、参数、配置来源及实例后，运行同一组保存的配置作业。当必须在不同的实例上执行相同的命令集时，或者当作业遇到错误并停止进一步执行时，这很有用。

Citrix Application Delivery Management (ADM) 提供了重新执行已完成作业的功能。通过此功能，完整执行的命令可以在不更改作业名称的情况下重新运行。

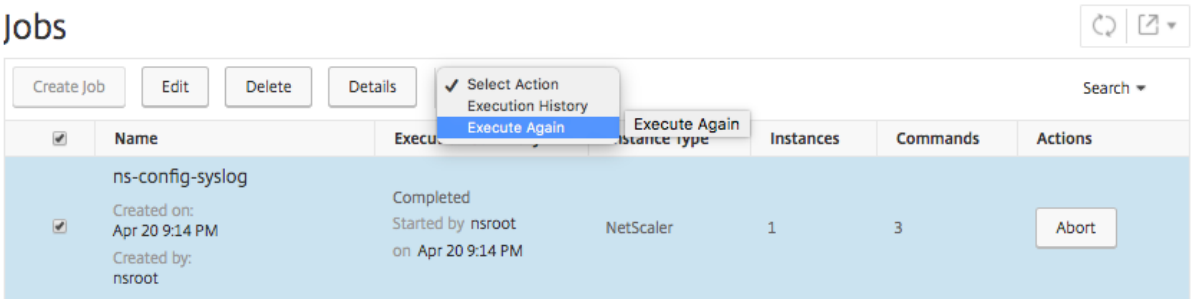
> 注意 只能重新执行执行模式为“现在”时执行的那些作业。

要编辑已完成的作业，请执行以下操作：

1. 在 Citrix ADM 主页上，导航到网络 **>** 配置作业。
2. 在作业页面中，选择显示“执行摘要”为“已完成”的作业，然后单击编辑。还可以编辑计划的配置作业。
3. 在 **Configure Job**（配置作业）页面上，可以看到“Job Name”（作业名称）和“Instance type”（实例类型）都是不可编辑。可以修改其他字段（例如，配置来源）、添加实例、编辑变量值以及设置执行设置。
4. 单击 完成 再次运行配置作业。



> 注意
>
> 您还可以选择作业，然后再次单击 执行 以运行作业，而不修改任何源、实例和命令。如果必须对相同实例运行相同的一组命令，这很有用。有时，作业可能会遇到来自服务器端的暂时错误，并且您可能需要再次运行作业。



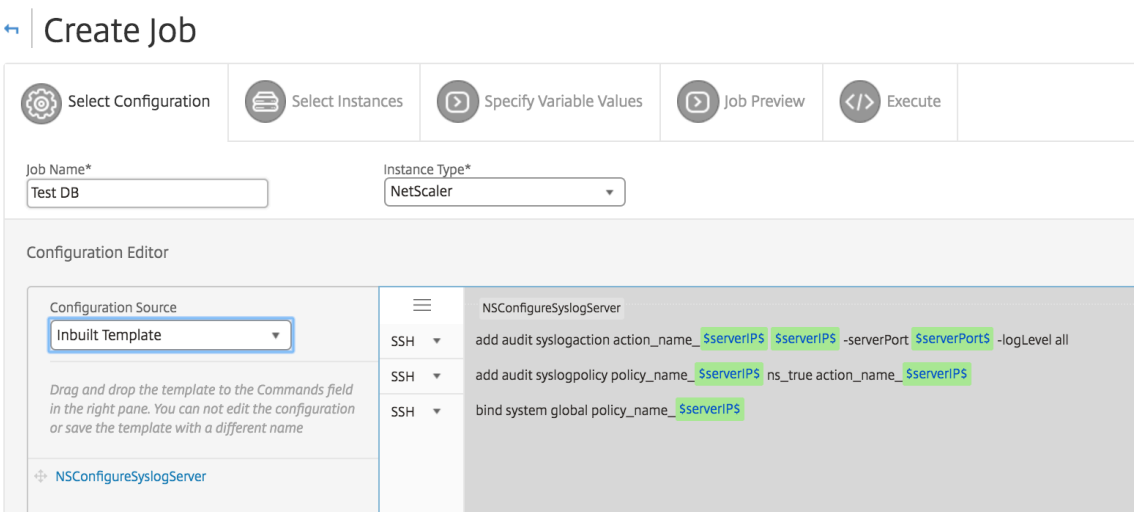
安排使用内置模板创建的作业

February 6, 2024

可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，使用内置模板选项调度作业以配置 syslog 服务器。您也可以选择立即执行作业，或将作业安排在稍后阶段执行。

使用 **Citrix Application Delivery Management (ADM)** 中的内置模板来安排作业

1. 在 Citrix ADM 中，导航到“网络”>“配置作业”，然后单击“创建作业”。
2. 在 创建作业 页上的 选择配置 选项卡上，指定 作业名称 并从下拉列表中选择 实例类型。
3. 从 配置源下拉列表中选择内置模板。将 ***NSConfigureSyslogServer** 命令拖放到右侧窗格中，然后单击“下一步”。



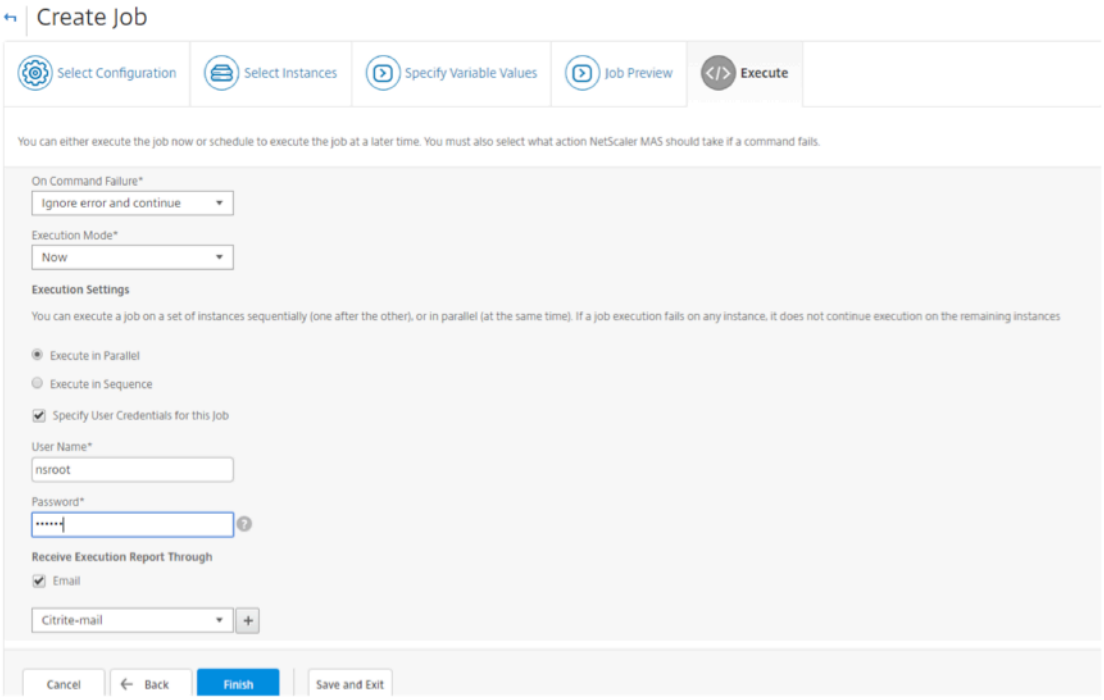
4. 在选择实例选项卡上，单击添加实例，选择要在其上运行作业的实例，然后单击“确定”。
5. 单击下一步。在 **Specify Variable Values**（指定变量值）选项卡中，选择以下选项之一来为您的实例指定变量：
   - 输入文件中的变量值 -下载输入文件以输入您在命令中定义的变量的值。然后，将文件上载到 Citrix ADM 服务器。
   - **Common variable values for all instances**（用于所有实例的公用变量值）- 指定 syslog 服务器 IP 地址和端口。
6. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
7. 单击下一步。
8. 在执行选项卡上，设置以下条件：

- **On Command Failure**（命令失败时）- 如果命令失败，可以选择忽略错误并继续执行作业，也可以选择停止进一步执行作业。从下拉列表中选择要执行的操作。
- 执行模式 -您可以立即执行作业，也可以安排稍后执行作业。如果要稍后安排作业，则必须指定该作业的执行频率设置。从下拉列表中选择希望作业遵从的计划。

9. 通过在“执行设置”下选择所需的方法，也可以按顺序或并行地在一组实例上 执行作业。如果在任一实例上作业执行失败，它不会继续在其余实例上运行。

   您可以选择允许授权用户在您的托管实例上执行任务。还可以发送关于作业成功或失败的电子邮件通知以及其他详细信息。

10. 单击完成。



使用维护作业升级 **NetScaler SDX** 实例

February 6, 2024

您可以对运行 NetScaler 11.0 版及更高版本的 NetScaler SDX 实例执行单捆绑升级。要执行单捆绑升级，请使用 Citrix ADM 中的内置任务。通过此内置任务，您可以升级 NetScaler SDX 管理服务、Citrix Hypervisor 以及 Citrix Hypervisor 的补充包和修补程序。

要使用 **Citrix ADM** 升级 **NetScaler SDX** 实例，请执行以下操作：

1. 导航到 网络 > 配置作业 > 维护作业。

2. 单击 创建作业。在“创建作业”页面中，选择“升级 **NetScaler SDX** 内置任务”来升级您的 NetScaler SDX 实例。单击继续。
3. 在一个或多 个“升级 NetScaler 设 备”页面上，在“实例选 择”标签中 ，指定任务名 称，然后单击“添加实例”。
4. 选择要升级的目标实例或实例组。
5. 添加 NetScaler 实例或实例组后，单击下一步 以启动所选实例的升级前验证。屏幕上将报告其中每个 NetScaler 实例的预验证进度。
6. 在修改升级 **NetScaler** 设备 页面上，选择升级选项卡。从 “软件映像”菜单中，选择 “本地”（您的本地计算机）或 “设备”（编译文件必须存在于 Citrix ADM 上）。
7. 您还可以查看是否有任何实例存在验证前升级错误。这些错误以消息形式显示。这些消息显示与磁盘空间、硬盘驱动器和用户自定义项相关的错误。如果您不想继续处理预验证升级检查失败的实例，可以删除这些实例。要删除实例，请选择实例，然后单击删除。
8. 在“计划任务”选项卡上，您还可以设置执行详细信息，您可以立即执行升级过程或计划在以后的日期执行升级过程。您还可以选择备份 NetScaler SDX 实例，通过电子邮件接收执行报告，或者在 HA 中对节点执行两阶段升级。

HA 中节点的两阶段升级使您可以选择立即执行升级，也可以安排一个接一个更新节点的时间。在两个节点成功升级之前，禁用节点的同步和传播。

为 **Citrix SD-WAN WANOP** 实例创建配置作业

February 6, 2024

作业是可以在一个或多个托管实例上创建并计划的一组配置命令。对于 Citrix SD-WAN WANOP 实例，您可以使用以下选项创建作业：

- 配置模板：您可以使用配置编辑器键入 CLI 命令，将配置保存为模板，然后使用它来配置作业。
- 内置模板：您可以从配置模板列表中进行选择。这些模板提供了 CLI 命令的语法，并允许您为变量指定值。下表中列出了内置模板及其说明。
- 文件：您可以从本地计算机上载配置文件并创建作业。

创建作业后，可以选择立即执行作业，也可以选择计划以后执行作业。还可以设置执行频率

内置模板	说明
EnableCloudBridgeWANOpt	启用通过 Citrix SD-WAN WANOP 设备的流量。
DisableCloudBridgeWANOpt	禁用通过 Citrix SD-WAN WANOP 设备的流量。

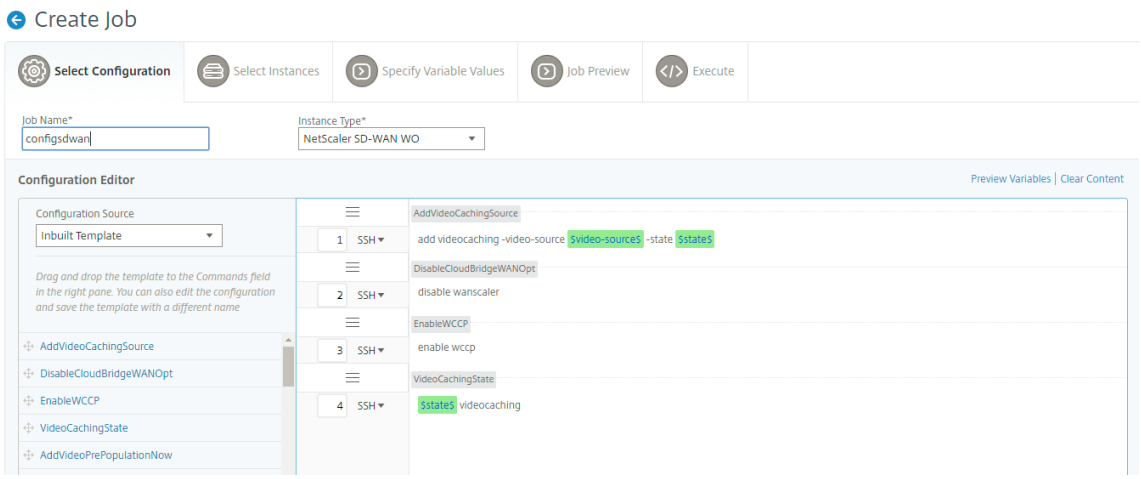
内置模板	说明
RestartCloudBridgeWANOpt	重新启动 Citrix SD-WAN WANOP 设备。
RestoreConfig	还原 Citrix SD-WAN WANOP 设备的配置。
AddLink	通过创建或定义链接，SD-WAN WANOP 设备可以防止链接上的拥塞和丢失，并执行流量调整。您可以定义通过链路发送或接收的最大带宽，并指定它是 LAN 端或 WAN 端流量。
ConfigureBandwidth	设置带宽限制和其他带宽管理设置。
AddUser	添加新用户，可以为其分配权限。
AddUserAdvancedPlatform	通过添加新用户，您可以分配 AddUser 模板中不可用的权限。
AddService-class	为 Citrix SD-WAN WANOP 设备创建具有一个或多个服务类筛选器的服务类并启用它。
SetApplication	设置应用程序分类器定义。
AddorRemoveVideoCachingPorts	添加或删除视频 源可以发送或接收数据的端口号。默认端口为 80。
RemoveVideoCachingSource	删除一个或多个视频缓存源。指定 视频源 IP 地址或域名。
RemoveAllVideoCaching	删除所有可用视频缓存源。
VideoCachingState	启用或禁用 Citrix SD-WAN WANOP 设备上的视频缓存功能。
ClearVideoCaching	清除视频缓存或视频缓存统计信息。
SetVideoCaching	设置缓存对象的最大大小。不会缓存 大于此限制的对象。默认情况下，最大缓存对象大小为 100 MB。
AddVideoCachingSource	添加视频源的 IP 地址或域名。包括用于为该源启用或禁用视频缓存的选项。
ConfigureRemoteLicenseServer	配置集中式许可证服务器。指 定许可证服务器型号、IP 地址和端口号。
ConfigureLocalLicenseServer	将许可证服务器位置设为本地。
InstallCACert	在 Citrix SD-WAN WANOP 设备上安装 CA 证书。指定证书名称、文件名和密钥库密码。
InstallCombinedCerKey	安装组合的 SSL 证书-密钥对文件。
InstallSeperateCertKey	将 SSL 证书和密钥作为单独的文件进行安装。
EnableWCCP	启用 WCCP 部署模式。
AddWCCPServiceGroup	为 Citrix SD-WAN WANOP 设备添加新的 WCCP 服务组定义。

内置模板	说明
DisableWCCP	禁用 WCCP 部署模式。
AddTrafficShapingPolicy	为 Citrix SD-WAN 设备创建流量调整策略。该策略控制网络带宽。
SetTrafficShapingPolicy	修改 Citrix SD-WAN WANOP 设备的流量调整策略。该策略控制网络带宽。
AddVideoPrePopulation	创建视频预填入条目，使您能够提前下载 和缓存视频。还可以指定何时缓存视频。
UpdateVideoPrePopulation	修改视频预填充条目，该条目指定何时缓存视频。
AddVideoPrePopulationNow	配置视频预填充，使您能够立即下载和缓存视 频。您可以控制从 URL 下载和缓存 视频的方式。
VideoPrePopulationState	更改、开始、更新或删除视频预填充。
ConfigureSyslogServer	设置 syslog 服务器的 IP 地址和端口号。
ConfigureAlert	配置警报级别。

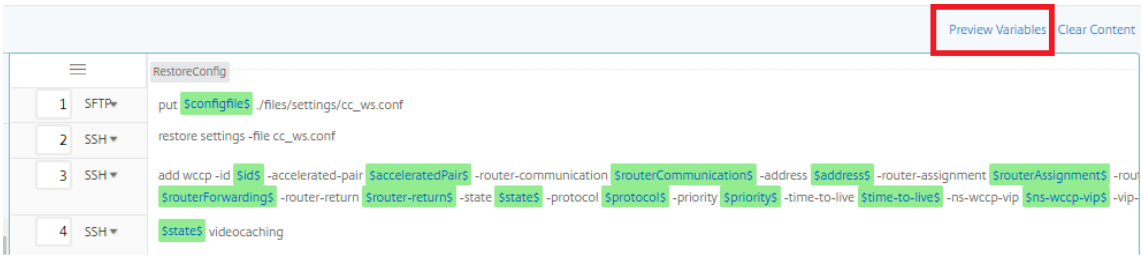
要为 **Citrix SD-WAN WANOP** 实例创建配置作业，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“配置作业”，然后单击“创建作业”。
2. 在 创建作业 页上的 选择配置 选项卡下，指定 作业名称。
3. 在“实例类型”字段中，选择 **Citrix SD-WAN WO**。
4. 在 配置源 下拉列表中，选择一个选项来创建作业。

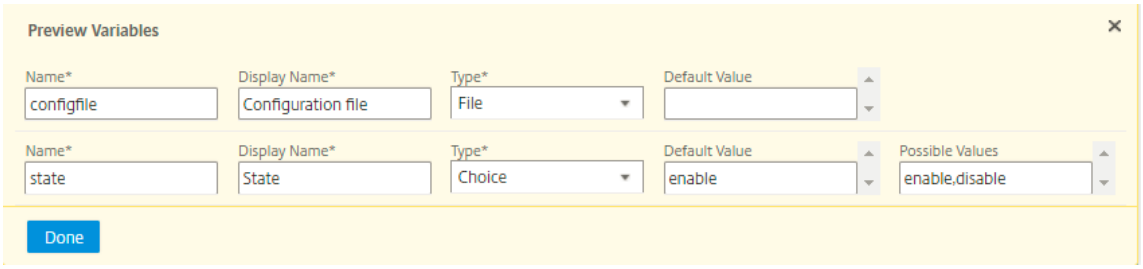
> 注意
>
> 选择 另存为配置模板”，然后指定一个名称以将配置另存为模板并重复使用。



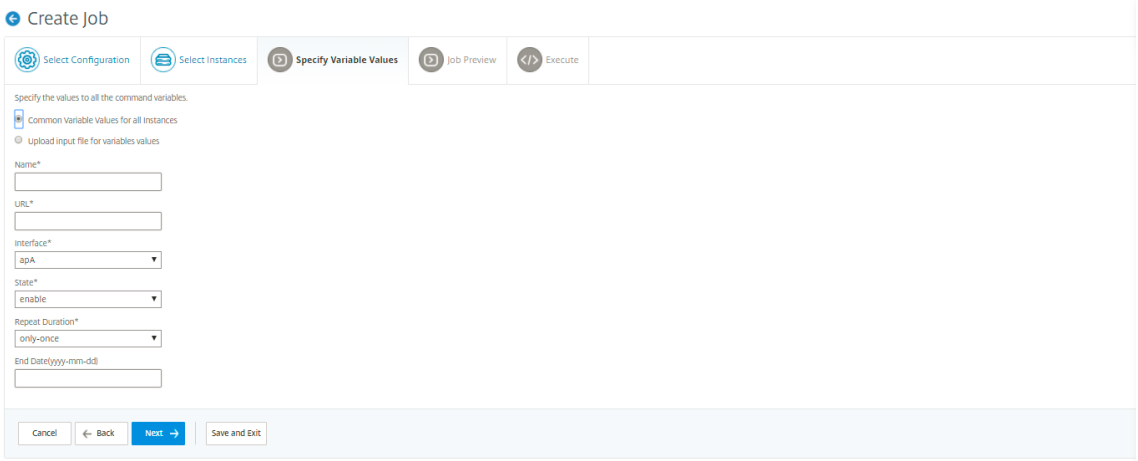
5. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
6. 执行以下操作之一可在单个统一视图中查看所有变量：
   - 创建配置作业时，导航到网络 **>** 配置作业，选择创建作业。在 创建作业 页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 网络 **>** 配置作业，选择作业名称并单击 编辑。在“配置作业”页上，您可以查看创建配置作业时添加的所有变量。
7. 然后，您可以单击“预览变量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



8. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完 成”按钮。



9. 单击 “下一步”，然后在“选择实例 ”选项卡上，单击 “添加实例”。选择要运行作业的实例，然后单击确定。
10. 单击 “下一步”，然后在 “指定变量值 ”选项卡上，选择以下选项之一为您的实例指定变量：
    - 上载变量值的输入文件： 单击 “下载输入密钥 文件”以下载输入文件。在输入文件中，输入已在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
    - 所有实例的公用变量值：输入变量值。变量因选定的模板而不同。



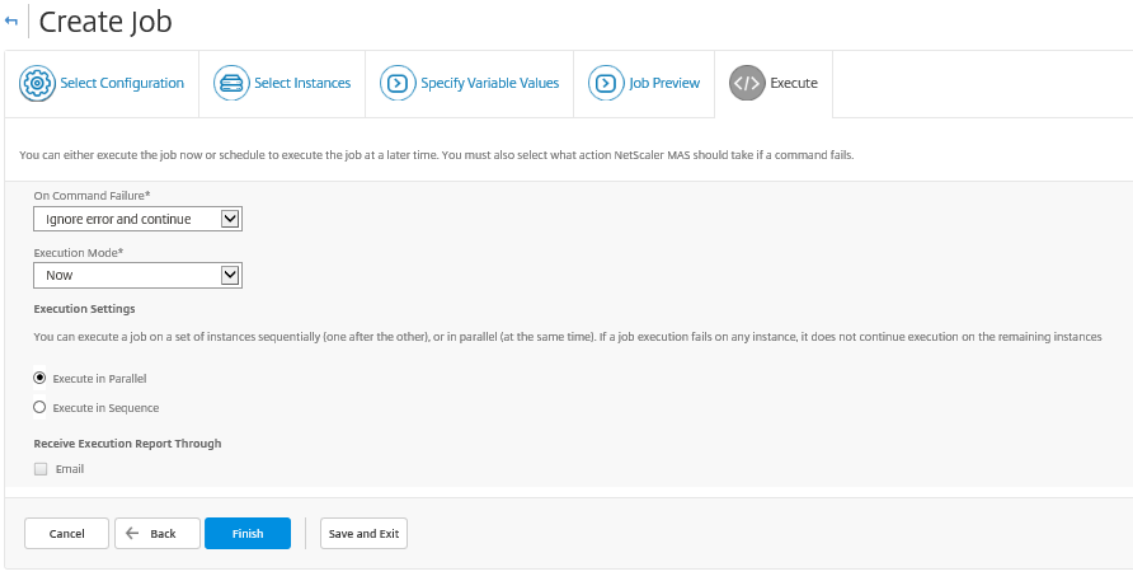
包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上载的这些输入文件。

要在创建配置作业时查看已执行的配置作业，请导航到“网络”**>**“配置作业”，然后单击“创建作业”。在“创建作业”页中。在指定变量值选项卡上，选择所有实例的公用变量值 选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）。

要在编辑配置作业时查看已执行的配置作业，请导航到“网络”**>**“配置作业”，选择“作业名称”，然后单击“编辑”。在配置作业页面的指定变量值选项卡上，选择所有实例的公用变量值 选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）

11. 单击“下一步”，在“作业预览”选项卡上，您可以评估和验证要作为作业执行的命令。
12. 单击下一步，在执行选项卡上，设置以下条件：

    - 命令失败时：如果命令失败该怎么办：忽略错误并继续执行作业，或者停止进一步执行作业。从下拉列表中选择操作。
    - 执行模式：立即执行作业，或安排稍后执行。如果计划以后执行，必须为作业指定执行频率设置。从 执行频率 下拉列表中选择您希望作业遵循的计划。



13. 在“执行设置”下，选择按顺序（一个接一个）或并行（同时）执行作业。
14. 要通过电子邮件将任务执行报告发送给收件人列表，请选中“通过电子邮件接收执行报告”部分中的电子邮件 复选框。从显示的下拉列表中选择电子邮件通讯组列表。要创建电子邮件通讯组列表，请单击 **+** 图标并输入收件人的电子邮件地址和电子邮件服务器的详细信息。
15. 单击完成。

使用主配置模板

February 6, 2024

使用主配置模板是在多个 Citrix ADC 实例上创建和部署主配置的灵活选项。

作为管理员，您可能需要更改配置并将许可证、证书和其他文件保存在 ADC 实例上。您可以将新配置保存为主配置模板 (.conf 文件)。

要从 ADC 实例保存您的主配置模板，您可以执行以下操作之一：

- 在命令提示符处，输入 **save ns** 配置。配置将保存在实例的闪存中的 /nsconfig/ns.conf 文件中。
- 在实例的 GUI 中，导航到 诊断 > 查看配置。选择您要保存的配置种类。例如，如果您想保存已保存的实例配置，请选择 已保存的配置。单击“将文本保存到文件”链接将“ns.conf”文件保存到本地计算机上。

在创建新作业时使用“DeployMasterConfiguration”配置模板部署主配置模板时，您可以通过添加其他命令、修改现有命令以及在输入文件中提供不同的变量值来为每个特定 ADC 实例进一步对其进行自定义。

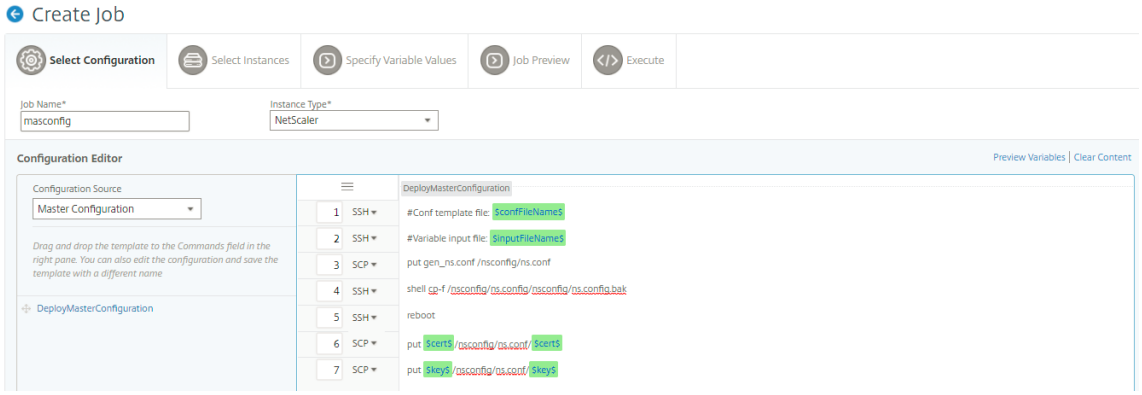
例如，作为管理员，您可能希望除 ns.conf 文件外将证书密钥上载到 ADC 实例，并在这些实例上部署主配置。

> 重要
>
> 您无法使用 DeployMasterConfiguration 模板在 Citrix ADC CPX 实例、群集中配置的实例或分区 ADC 实例上执行配置作业。

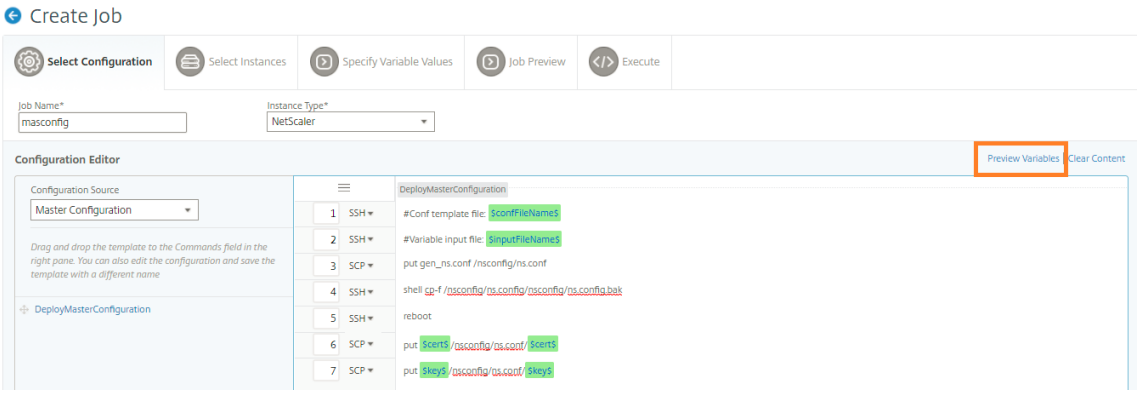
要使用 **Citrix ADM** 上的主配置配置模板创建配置作业，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“配置作业”，然后单击“创建作业”。
2. 在 创建作业 页上的 选择配置 选项卡上，指定 作业名称 并从下拉列表中选择 实例类型。
3. 从 配置源下拉列表中选择主配置。将 DeployMasterConfiguration 模板的命令拖放到右侧窗格。您也可以在右侧窗格中添加、修改或删除命令。单击下一步。

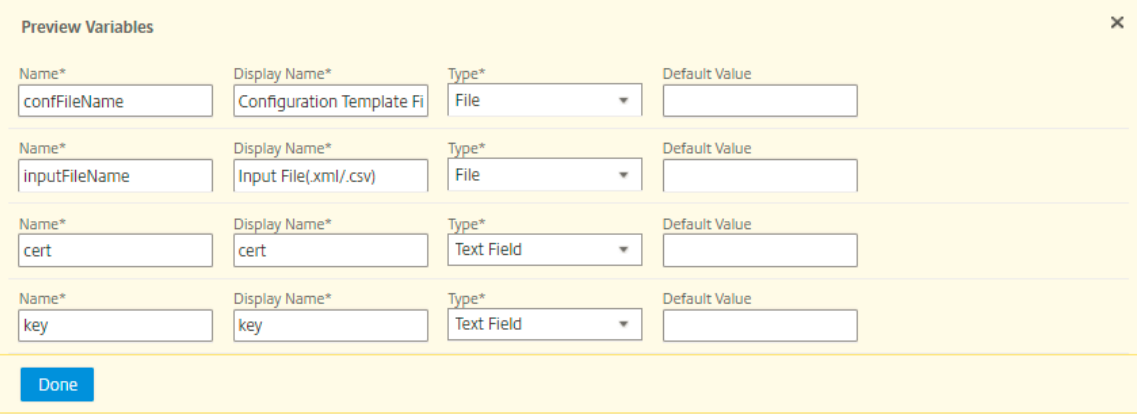
   > 注意
   >
   > 您可以添加 ***put*** 命令以将输入文件添加到模板中。在我们的示例中，除了配置模板文件和变量输入文件外，我们还需要上载证书和密钥文件。



4. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
5. 执行以下操作之一可在单个统一视图中查看所有变量：
   - 创建配置作业时，导航到网络 **>** 配置作业，选择创建作业。在 创建作业 页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 网络 **>** 配置作业，选择作业名称并单击 编辑。在“配置作业”页上，您可以查看创建配置作业时添加的所有变量。
6. 然后，您可以单击“预览变量”选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



7. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完 成”按钮。



8. 选择要在其上运行配置作业的实例，然后单击 下一步”。
9. 在“指定变量值”选项卡上，上载以下内容：

   - 配置模板文件 **(.conf)** -上载从 ADC 实例提取的.conf 文件。
   - 上载输入文件 **(.xml/csv)** -使用您在命令中定义的变量值上载输入文件。

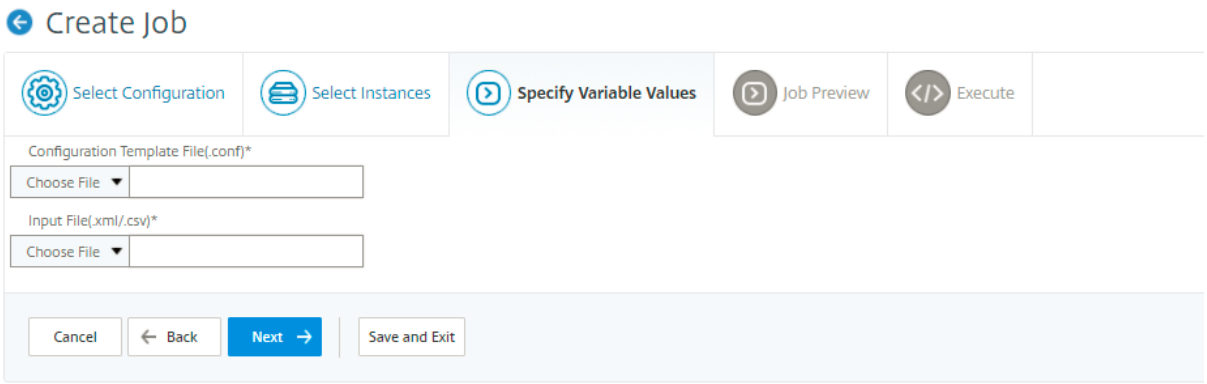
   此处提供了示例 xml 文件供您使用。确保 xml 文件包含与您正在使用的 ADC 实例相对应的详细信息。

```
<?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.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters
    and value.

If the same parameters are defined in global and instance tags,
    the instance specific parameters value will take precedence in
    the execution.

-  name. This attribute represents the IP Address of the instance.
     Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>.
    Example 10.102.2.1-10.102.2.2

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.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```

10. 单击 **Next**（下一步）。

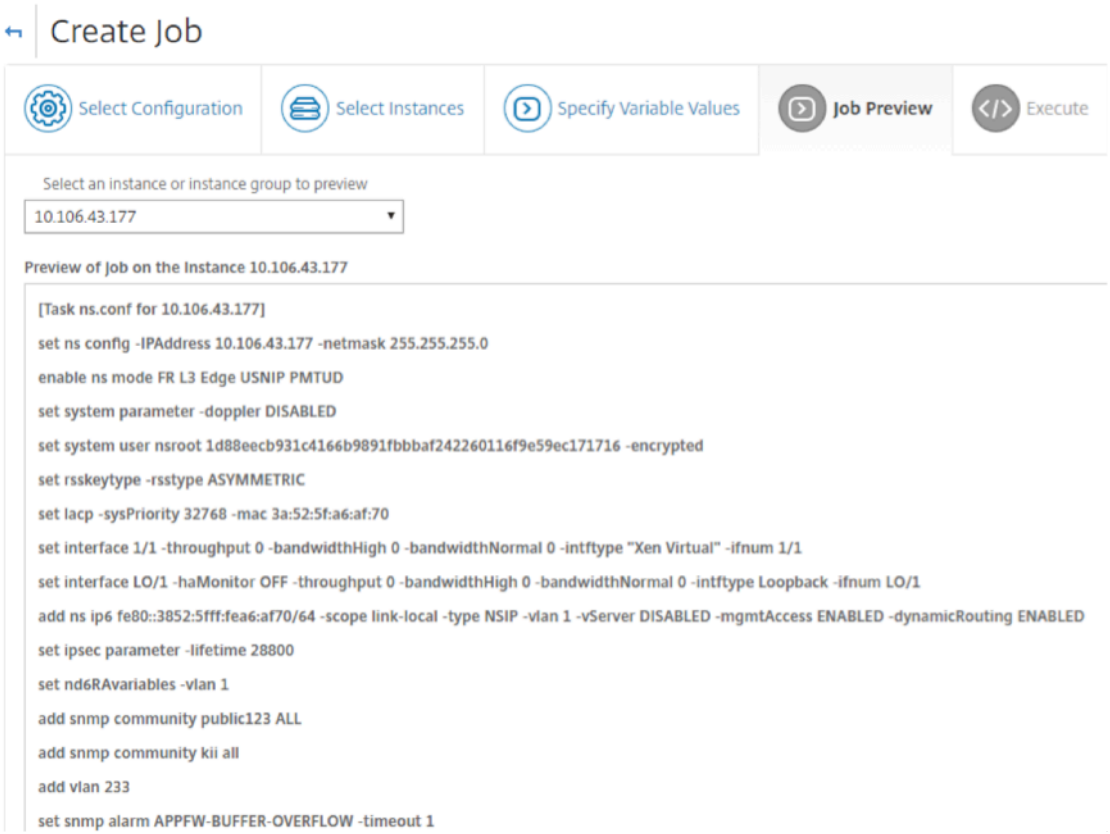


包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上载的这些输入文件。

要在创建配置作业时查看已执行的配置作业，请导航到网络 **>** 配置作业，然后单击 创建作业。在 创建任务 页面中。在“指定变量值”选项卡上，选择“所有实例的通用变量值”选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）。

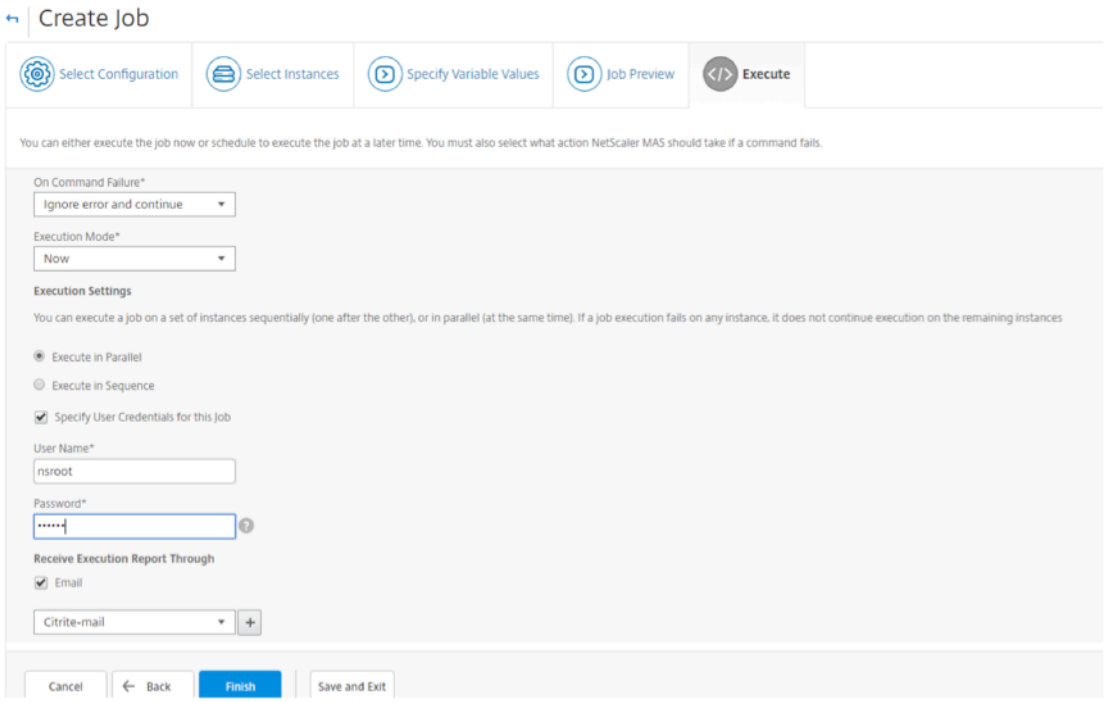
要在编辑配置作业时查看已执行的配置作业，请导航到“网络” **>** “配置作业”，选择“作业名称”，然后单击“编辑”。在配置作业 页面的 指定变量值 选项卡上，选择 所有实例的公用变量值 选项以查看上载的文件。要编辑输入文件，请下载输入文件，然后编辑和上载文件（保持相同的文件名）。

1. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令，然后单击下一步。

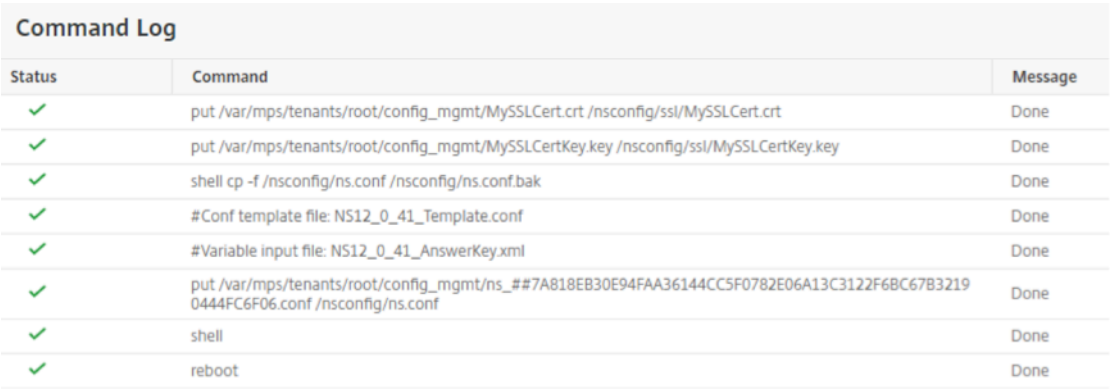


2. 在“执行”选项卡上，您可以选择立即执行作业，也可以将其安排在稍后执行。您还可以选择命令失败时 Citrixx ADM 应采取的操作。

   您还可以选择允许授权用户在您的托管实例上执行作业，并可以选择是否发送有关作业成功或失败以及其他详细信息的电子邮件通知。



执行作业后，您可以通过导航到网络 > 配置作业来查看作业详细信息，然后选择刚才配置的作业。单击“详细信息”，然后单击“执行摘要”以查看作业的详细信息。单击实例查看 命令日志，查看在作业中执行的命令。



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_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

使用作业升级 **Citrix ADC** 实例

February 6, 2024

您可以使用 Citrix Application Delivery Management (ADM) 升级一个或多个 Citrix ADC 实例。在升级实例之前，请确保您已将正确的编译文件和文档文件上载到 Citrix ADC 实例。在升级实例之前，您必须了解许可证框架和许可证类型。

通过创建维护任务升级 Citrix ADC 实例时，可以执行以下操作：

- 对正在升级的实例执行预验证检查。预验证检查包括以下检查：

1. 检查 Citrix ADC 实例上的任何现有自定义项并删除自定义项。您可以在升级过程完成后重新应用所有自定义项。
2. 检查 Citrix ADC 实例的磁盘使用情况。如果磁盘使用率超过 80%，则清理磁盘空间。
3. 检查 Citrix ADC 实例的磁盘硬件问题。

- 分两个阶段执行 Citrix ADC HA 对升级。
  1. 立即在节点上执行升级任务，甚至可以为以后安排升级任务。
  2. 稍后安排其他节点的升级。它必须在升级初始节点后进行计划。

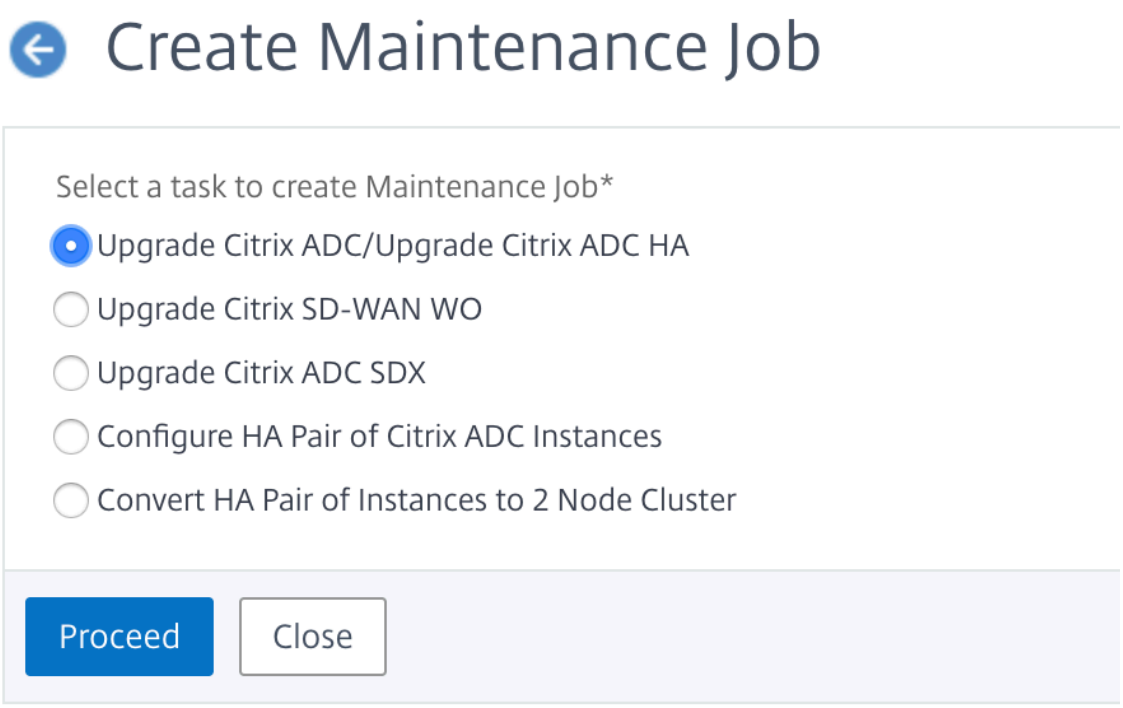
升级 Citrix ADC HA 对时，请注意以下事项：

- 目前，首先升级 HA 对的第二个节点，然后计划稍后完成第一个节点的升级。
- 在两个节点成功升级之前，禁用节点的同步和传播。
- 升级这两个节点后，如果 HA 对中的节点位于不同的版本或版本上，您将在执行历史记录中看到一条错误消息（表明未启用 HA Sync）。

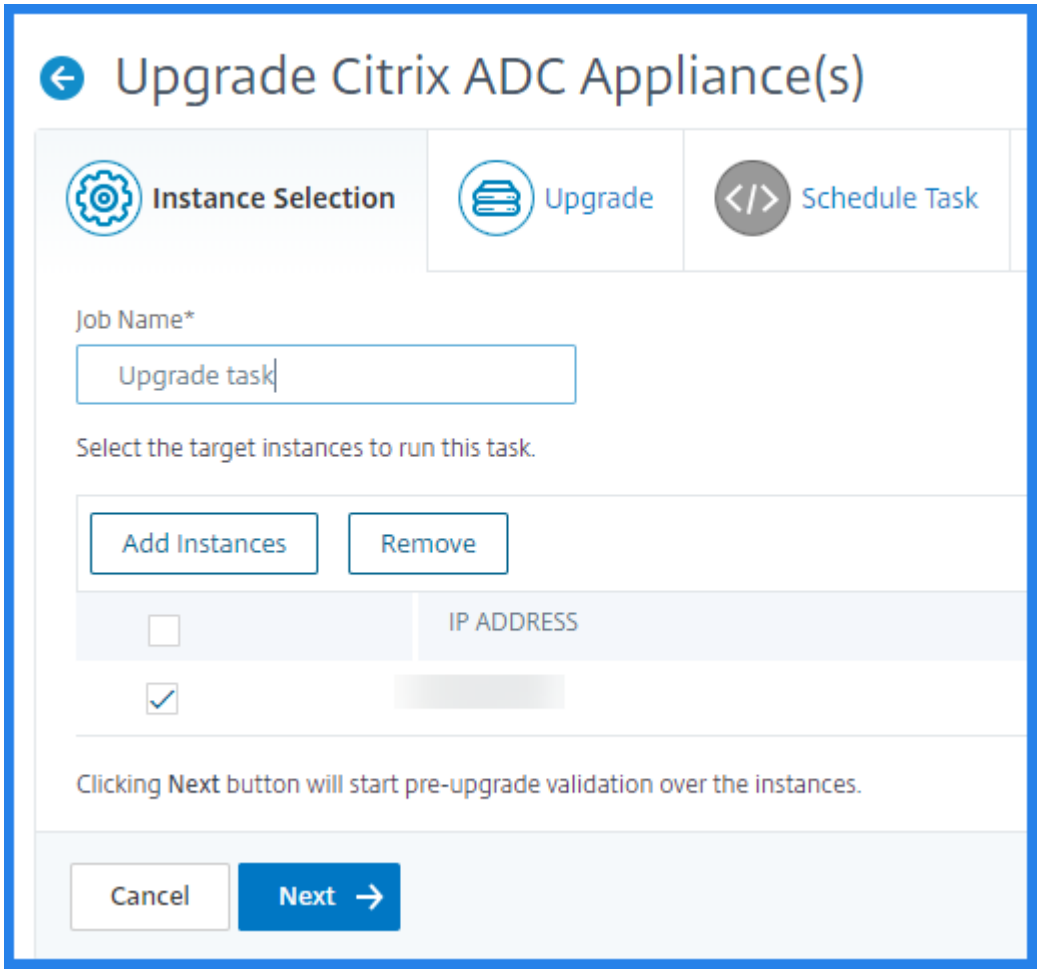
要创建维护任务以升级 **Citrix ADC** 实例，请执行以下操作：

> 注意
>
> 不支持 ADC 从更高版本升级到更低版本。例如，如果您的 Citrix ADC 实例为 13.0 82.x，则无法将 ADC 实例降级到 13.0 79.x 或任何其他早期版本。

1. 导航到网络 > 配置作业 > 维护作业。
2. 在“维护作业”页中，单击 创建作业”。
3. 在创建维护作业页面中，选择 升级 **Citrix ADC/** 升级 **Citrix ADC HA** ，然后单击 继续。



4. 在一个或多个升级 Citrix ADC 设备页面上，在 实例选择 选项卡中，指定 作业名称，然后单击 添加实例。



5. 选择要升级的目标实例或实例组。

   注意

   - 要在高可用性模式下升级 Citrix ADC 实例，您必须选择主实例或辅助实例的 IP 地址。但是，建议始终使用主节点进行升级。
   - 要在群集模式下升级 Citrix ADC 实例，请选择群集 IP 地址。

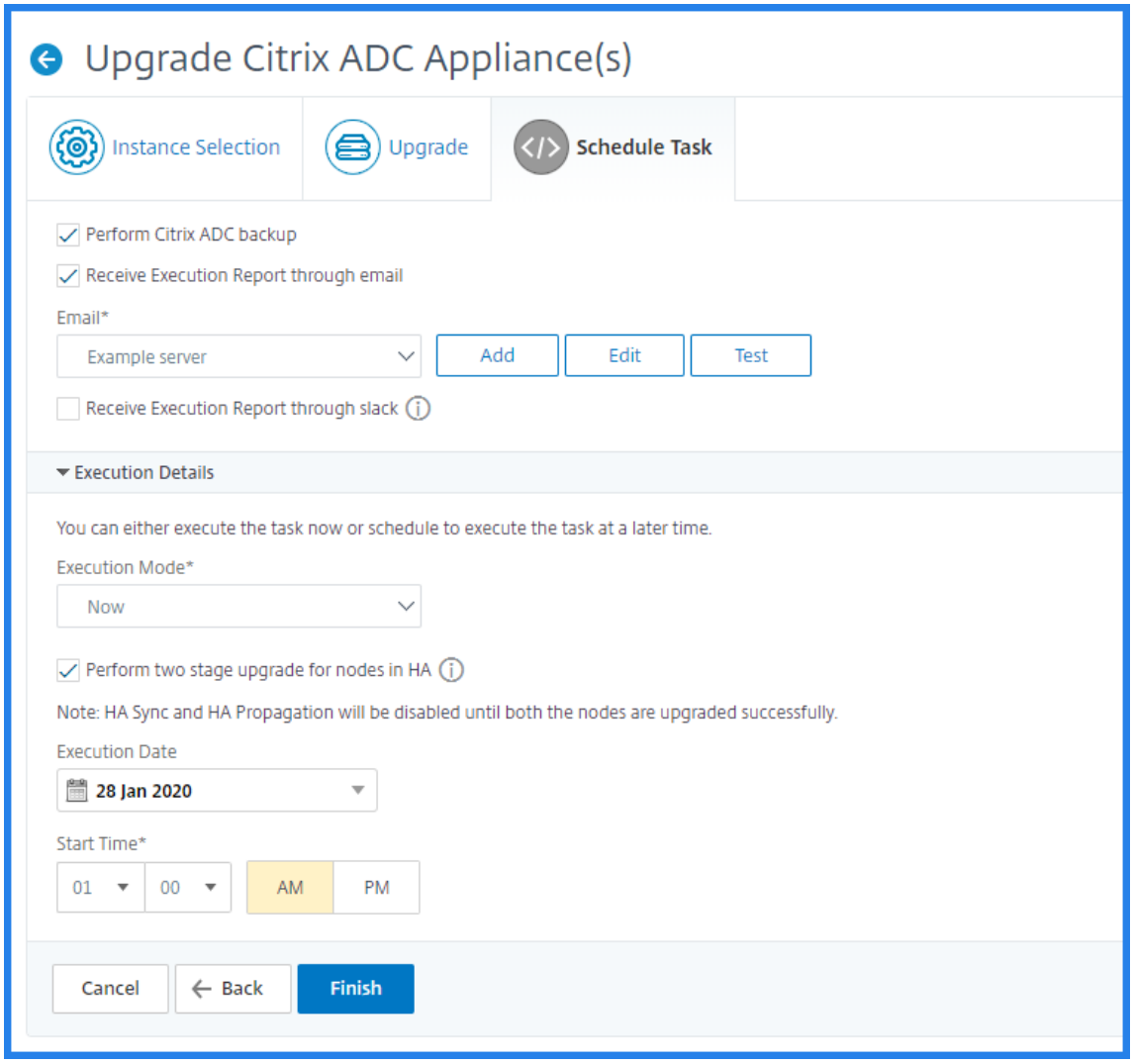
6. 添加 Citrix ADC 实例或实例组后，单击 下一步开始对所选实例进行升级前验证。屏幕将报告每个 Citrix ADC 实例的预验证进度。
7. 在 升级 **Citrix ADC** 设备 页面上，选择 升级 选项卡。从 软件映像菜单中，选择本 地（您的本地计算机）或 设备（构建文件必须存在于 Citrix ADM 上）。
8. 您还可以查看是否有任何实例存在验证前升级错误。这些错误以消息形式显示。这些消息显示与磁盘空间、硬盘驱动器和用户自定义项相关的错误。

如果您不想继续处理预验证升级检查失败的实例，可以删除这些实例。要移除实例，请选择实例，然后单击“删除”。

1. 单击下一步。

> 注意
>
> 强烈建议仅在 Citrix ADC 实例的升级前验证检查通过时继续升级过程。

2. 在 计划任务 选项卡上，您还可以设置执行详细信息，以便立即执行升级过程或将升级过程安排在以后的日期。
3. 您可以启用电子邮件通知以接收升级 Citrix ADC 实例的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。要创建电子邮件通讯组列表：
   - 选择 **+** 图标以创建电子邮件分发列表。
   - 在“创建电子邮件通讯组列表”页面上，为电子邮件通讯组列表指定一个 名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。
4. 在 Sch **edule Task** 选项卡上，您还可以对高可用性中的节点执行两阶段升级。您可以立即执行升级，也可以安排一个时间让节点一个接一个地更新。在两个节点成功升级之前，禁用节点的同步和传播。



使用配置模板创建审核模板

February 6, 2024

现在可以使用之前保存为配置模板的配置命令来创建可以应用于特定 NetScaler 实例的审核模板。创建审核模板时，可以将以前保存的配置模板拖放到“Commands”（命令）字段中，并编辑该模板以满足您的要求。然后可以将审核模板应用于特定 NetScaler 实例。Citrix ADM 将这些实例与审核模板进行比较，并报告任何不匹配。此过程可帮助您发现错误并及时对其进行纠正。

您可以在创建新作业并将一组配置命令保存为模板时创建配置模板。当您在“创建作业”页面上保存这些模板时，它们会自动显示在“创建模板”页面上。

例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。

此示例使用以下命令：

add lb vserver **servername** HTTP **ipaddress portnumber**

add service **servicename1 ipaddress1** HTTP 80

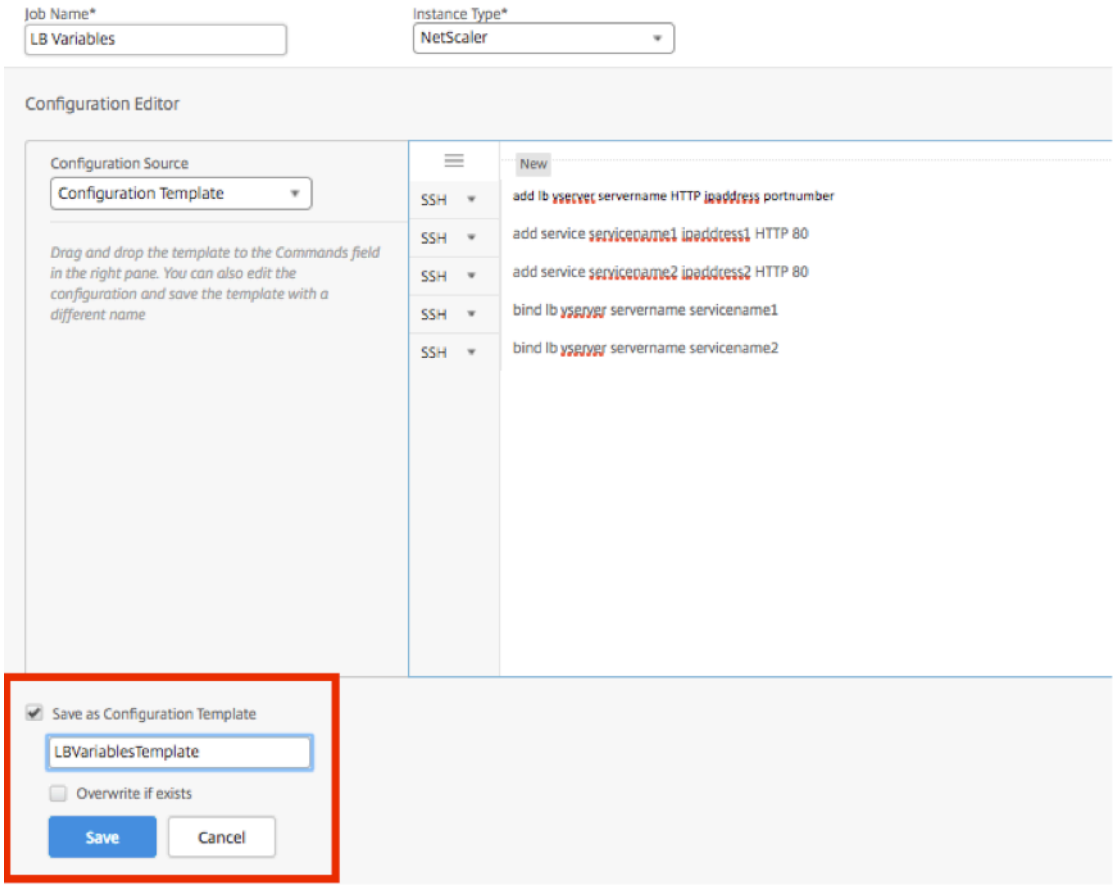
add service **servicename2 ipaddress2** HTTP 80

bind lb vserver **servername servicename1**

bind lb vserver **servername servicename2**

要在 **Citrix ADM** 中保存配置模板，请执行以下操作：

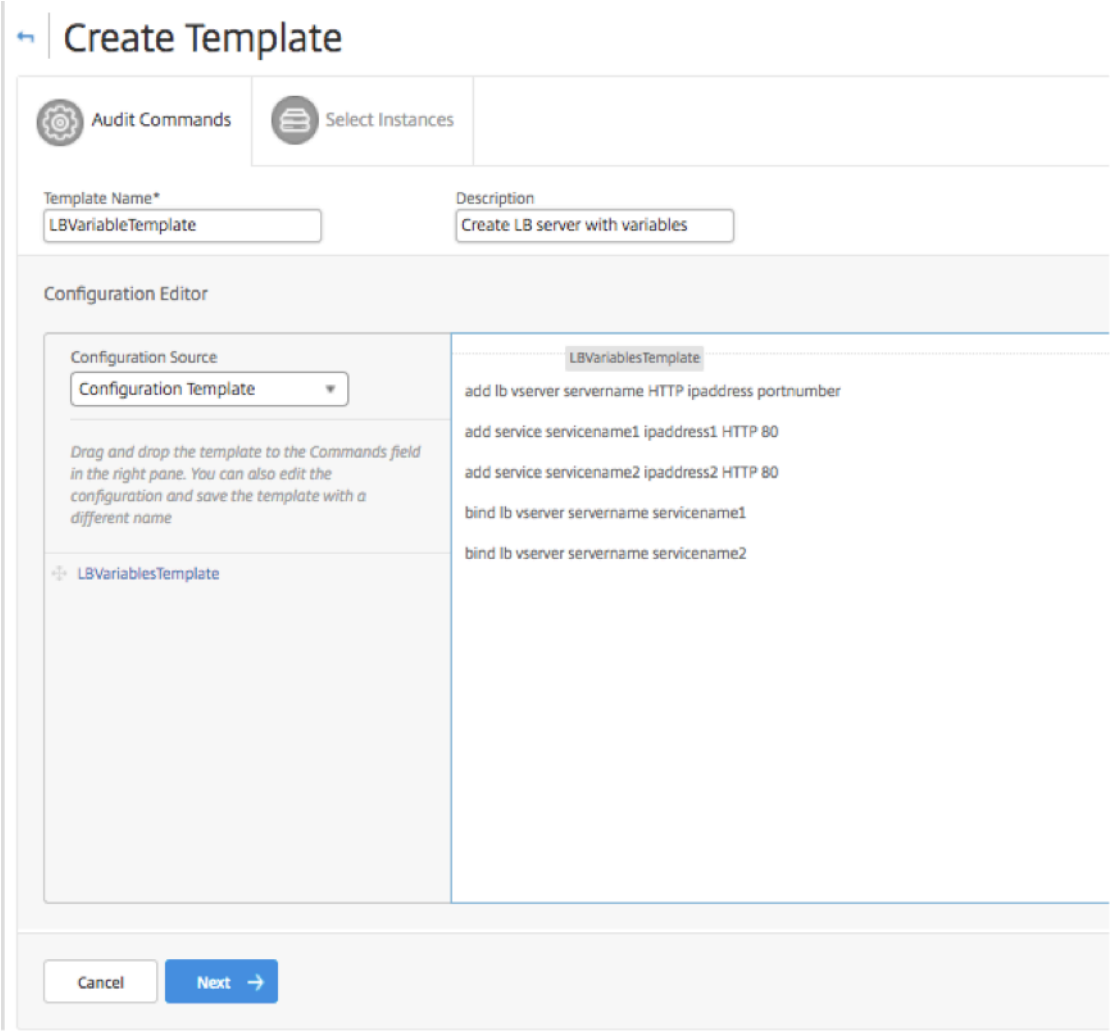
1. 导航到“网络”>“配置作业”，然后单击“创建作业”。
2. 在 创建任务 页面上，指定作业名称和实例类型。
3. 选择 配置模板 作为配置源，然后在 命令 字段中输入诸如上例中的命令。
4. 选中“另存为配置模板”复选框并指定模板的名称。您可以选择覆盖已有的其他同名模板。
5. 单击保存。



要使用配置模板在 **Citrix ADM** 中创建审核模板，请执行以下操作：

1. 导航到“网络”>“配置审核”>“审核模板”，然后单击“添加”。

2. 在 创建模板 页面上，指定模板名称的名称，然后输入描述。
3. 从“配置源”列表中，选择“配置模板”，然后将模板拖放到右窗格的“命令”字段中。您也可以编辑配置并使用另一个名称保存模板。单击下一步。
4. 在“选择实例”选项卡上，单击“添加实 例”，然后添加要在其上运行配置的实例。单击确定。
5. 单击完成。



审核模板显示在“Audit Templates”（审核模板）列表中，每 12 小时根据指定实例的配置运行一次。

在配置作业中使用 **SCP**（放置）命令

February 6, 2024

您可以使用 Citrix ADM 的 配置作业 功能创建配置作业、发送电子邮件通知和检查所创建作业的执行日志。作业是可以在一个或多个托管实例上创建并运行的一组配置命令。例如，您可以使用配置作业进行设备升级。

Citrix ADM 中的配置作业使用安全外壳 (SSH) 命令来配置实例，您可以配置配置作业以使用安全复制 (SCP) 安全地传输文件。SCP 基于 SSH 协议。您可以在配置作业中包含的其中一个 SCP 命令是 “put” 命令。您可以在配置作业中使用 “put” 命令将存储在系统本地目录中的一个或多个文件上载或传输到 Citrix ADM，然后上载到一个或多个 NetScaler 实例上的某个目录。

> 注意 该文件已上载到 Citrix ADM，稍后会被复制（放置）到选定的 NetScaler 实例。上载的文件存储在 Citrix ADM 中，只有在删除作业时才会删除。这对于计划在以后执行的作业是必需的。

该命令语法如下：

```
put <local_filename> <remote_path/remote_filename>
```

其中，

<local_filename> 是要上载的本地文件的名称。

<remote_path / remote_filename> 是远程目录的路径，以及将文件复制到该目录时要分配给该文件的名称。

创建配置作业时，可以将本地和远程文件名参数转换为变量。这样，每次执行作业时，针对同一组 NetScaler 实例，可以为这些参数分配不同的文件。此外，在一个作业中的多个位置使用某个文件时，如果您要重命名文件，可以重新定义变量，而不是在所有位置更改文件名。

要使用 **put** 命令在配置作业中上载文件，请执行以下操作：

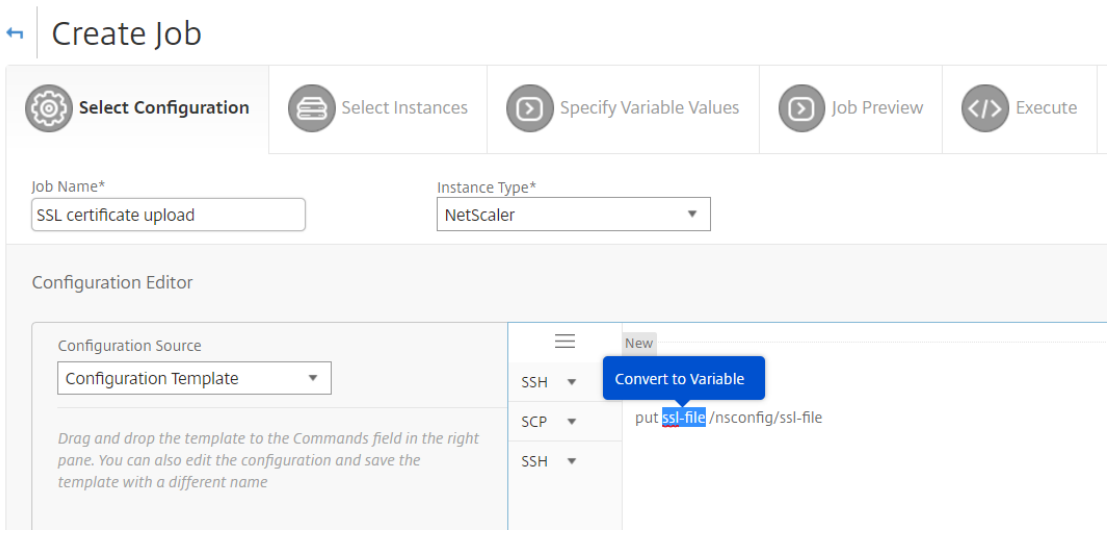
1. 导航到 “网络” > “配置作业”。
2. 在作业页上，单击创建作业。
3. 在 创建作业 页面上，在 “作业名称” 字段中输入作业的名称，然后在 配置编辑器 窗格中输入 “put” 命令。

   例如，如果您要创建一个配置作业以将保存在您本地系统上的 SSL 证书文件复制到多个 NetScaler 实例，您可以添加使用变量而不是特定文件的名称的 “put” 命令，并将变量类型定义为 “file”。

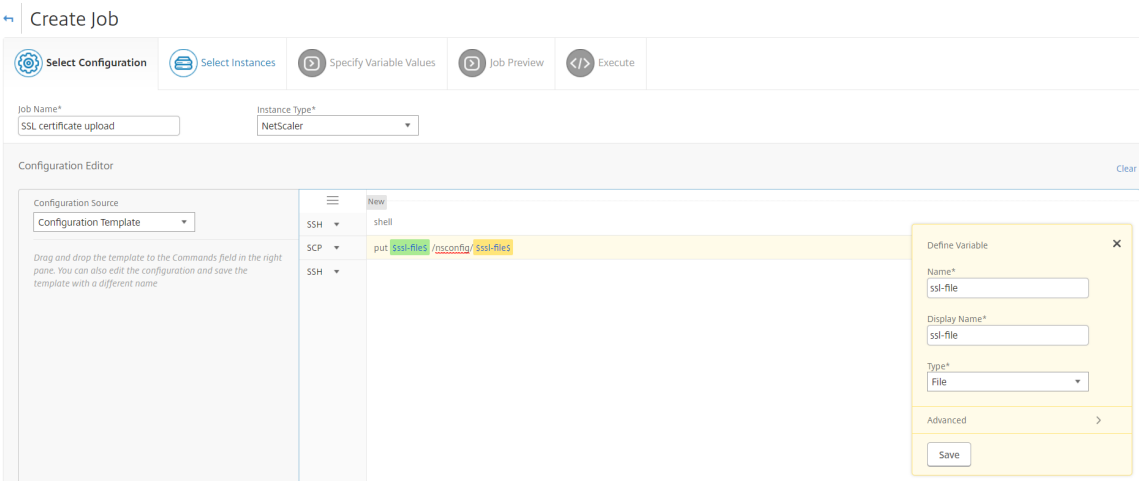
   ```
   1 put ssl-file /nsconfig/ssl-file
   2 <!--NeedCopy-->
   ```

   在此示例中，

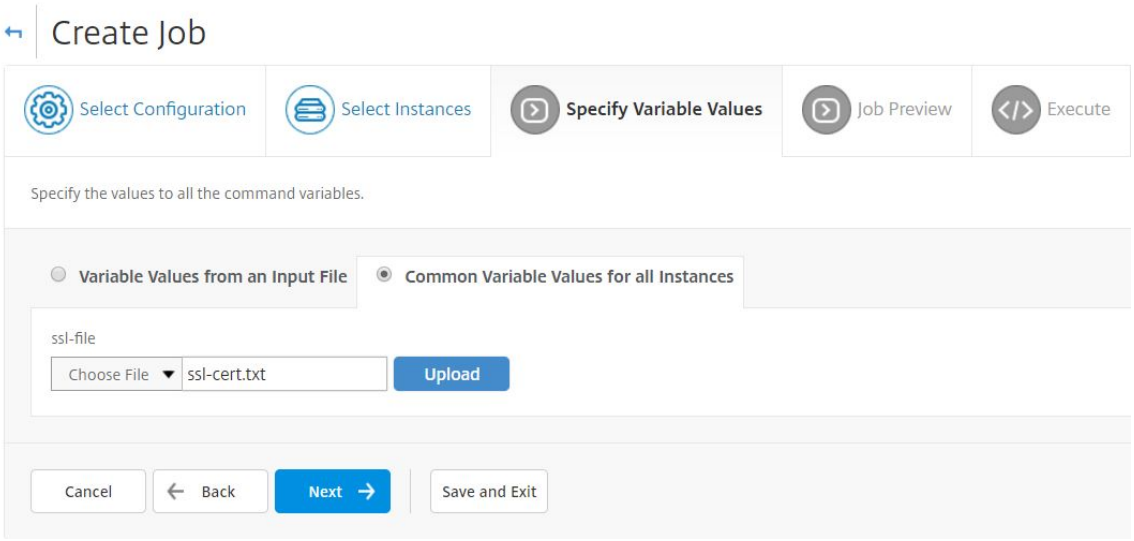
   - ssl-file - 这是需要在 NetScaler 实例中上载的文件的名称。
   - /nsconfig/ssl-file - 这是实例上的目标文件夹，执行任务后 ssl-file 将放置在该文件夹中。
4. 在刚才输入的命令中，选择要转换为变量的文件名，然后单击 “转换为变量”，如下图所示。



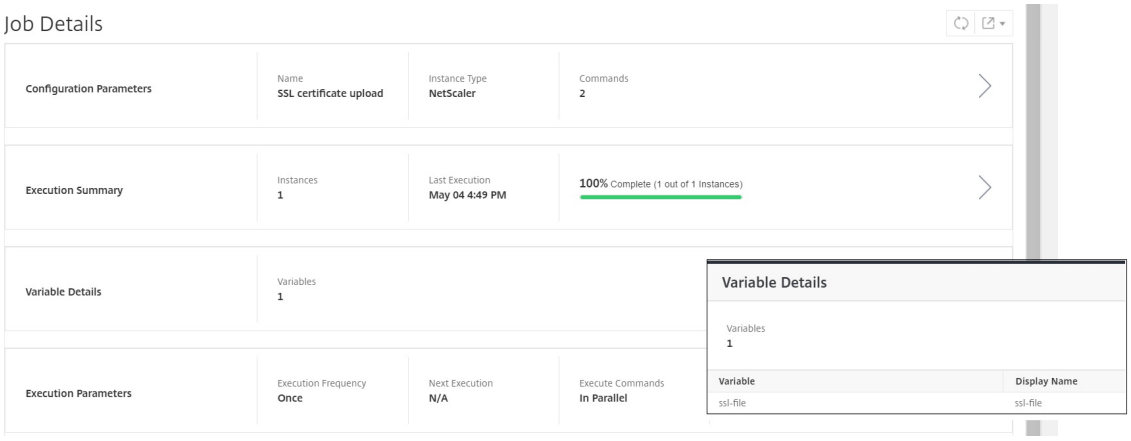
5. 验证文件名是否已用美元符号括起来（表示它现在是一个变量），然后单击变量。
6. 指定变量的详细信息，例如名称、显示名称和类型。
7. 从“类型”下拉列表中选择“文件”。单击保存。将变量声明为“文件”类型允许您将文件上载到 Citrix ADM。



8. 单击“下一步”，然后选择要将文件复制到的 NetScaler 实例。
9. 在“指定变量值”选项卡上，选择 所有实例的公用变量值 部分，从系统上的本地存储中选择文件，单击“上载”将文件上载到 Citrix ADM，然后单击“下一步”。



10. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
11. 在“执行”选项卡上，您可以立即执行作业，也可以将其安排在稍后执行。您还可以选择命令失败时 Citrix ADM 应采取的操作。您还可以创建电子邮件通知以接收有关作业成功或失败以及其他详细信息的通知。单击完成。
12. 要查看作业详细信息，请导航到“网络”>“配置作业”，然后选择刚才配置的作业。单击“详细信息”，然后单击“变量详细信息”列出添加到作业的变量。



重新计划通过使用内置模板配置的作业

February 6, 2024

您可以使用 Citrix Application Delivery Management (ADM) 中的内置模板重新安排您计划的作业。例如，您可以更改 Citrix ADM 在命令失败时必须采取的操作。如果之前选择了忽略错误并继续，可以将其更改为在命令失败时回滚所有成功的命令。

重新计划通过使用 **Citrix ADM** 中的内置模板配置的作业

1. 在 Citrix ADM 中，导航到“网络”>“配置作业”。
2. 选择要编辑的作业，添加或删除实例、指定变量值，然后更改执行操作和设置。
3. 单击 **Finish**（完成）重新计划作业。

> 注意
>
> 您还可以选择作业，然后单击“再次执行”以运行作业，而不修改任何源、实例和命令。如果必须对相同实例运行相同的一组命令，这很有用。有时，作业可能遇到服务器端发生临时错误，您可能必须重新运行作业。

在配置作业中重复使用配置审核模板

February 6, 2024

作为管理员，您现在可以在创建任务和运行配置审核时将配置命令保存为一组可重复使用的配置模板。在“配置任务”中创建和保存的配置模板在“配置审核”中可用，用于创建可应用于特定 Citrix ADC 实例的审核模板。同样，可以在“Configuration Jobs”（配置作业）中访问在“Configuration Audit”（配置审核）模块中创建的审核模板，以便可以将模板作为配置作业运行。现在，在模板中所做的任何更改在“Configuration Jobs”（配置作业）模块和“Configuration Audit”（配置审核）模块中均可见。

以前，必须为同一配置单独创建配置作业模板和配置审核模板，并将其保存为不同的文件。这导致在创建和维护模板时所做工作量加倍。

Citrix Application Delivery Management (ADM) 允许您将此模板保存在系统中，以便审核模板也可在 配置作业中使用。现在可以使用审核模板创建配置作业。这样，可以在配置作业与配置审核之间互换使用模板。

例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。

此示例使用以下命令：

```
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
<!--NeedCopy-->
```


在“**Configuration Audit**”（配置审核）中创建模板并在“**Configuration Jobs**”（配置作业）中重用该模板

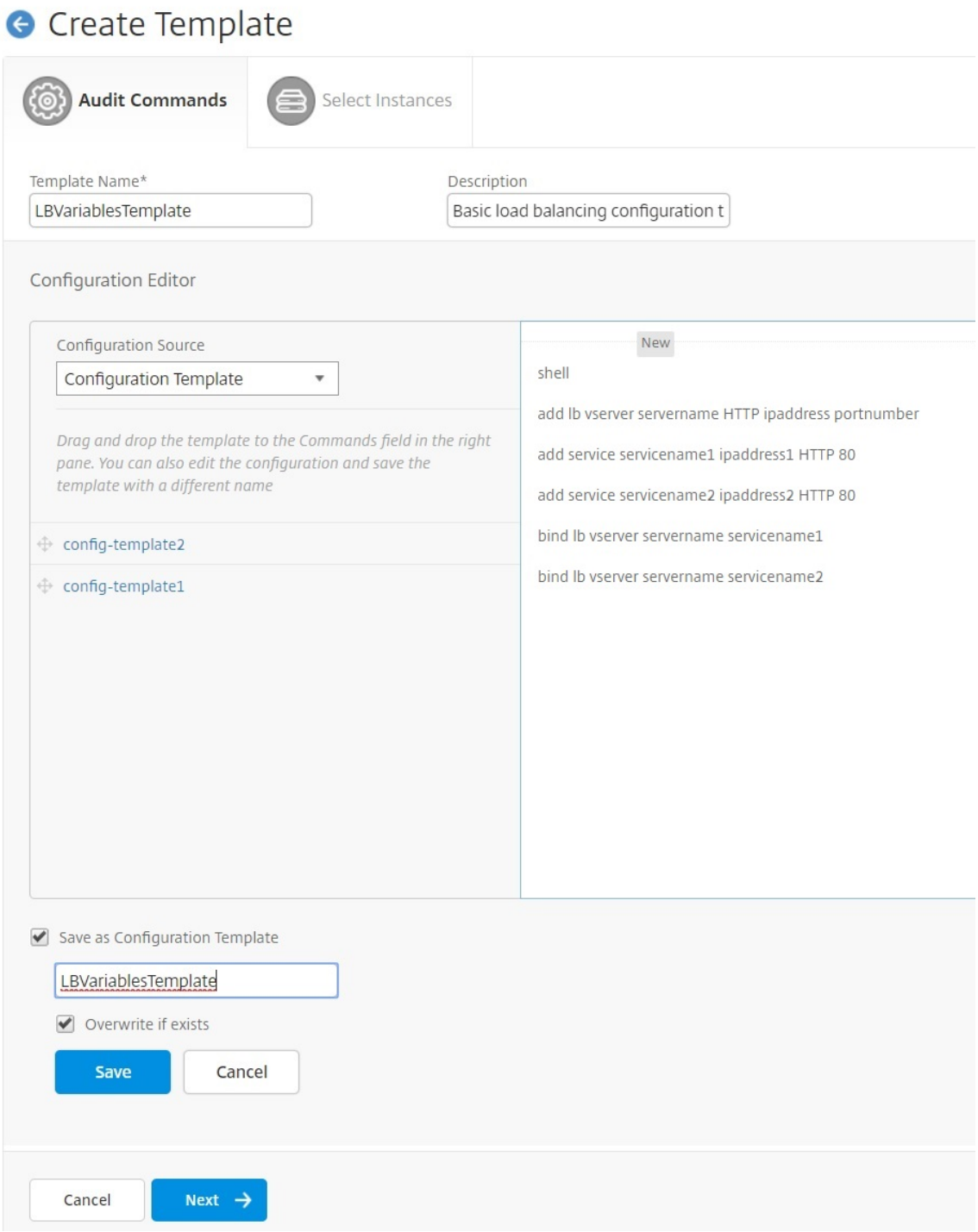
执行以下任务，在配置审核模块上创建模板，并在配置作业模块中重复使用该模板。

要创建审核模板，请执行以下操作：

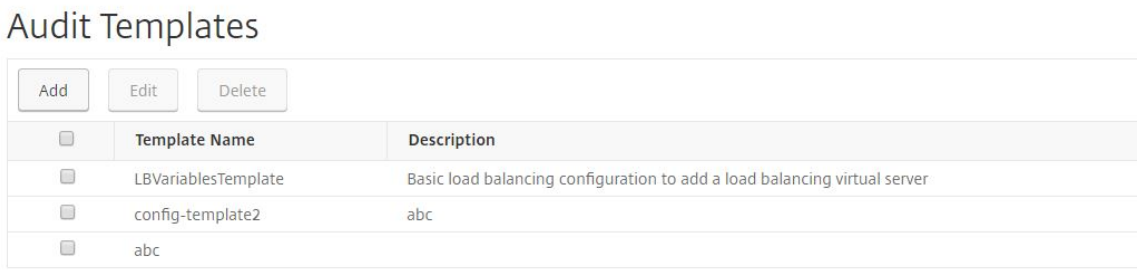
1. 在 Citrix ADM 中，导航到“网络”**>**“配置审核”**>**“审核模板”，然后单击“添加”。
2. 在“创建模板”页面上，指定模板名称。您还可以在 描述 字段中添加有关模板的更多信息。
3. 在 命令窗格中，输入示例中的命令。
4. 选中“另存为配置模板”复选框并为模板指定名称，例如，您可以将此模板命名为“LBVariablesTemplate”。您可以选择覆盖已有的其他同名模板。

   > 注意 审核模板名称可以与配置模板名称相同。

5. 单击“保存”，然后单击“下一步”。



6. 单击下一步。
7. 在“选择实例”选项卡中，选择要在其上运行这些配置命令的 **Citrix ADC** 实例，然后单击“完成”。新模板现在显示在审核模板列表中。



8. 要运行这些配置命令时，请导航到网络 > 配置作业，然后单击创建作业。您之前创建的审核模板将作为配置模板列出。

要在配置作业中重复使用审核模板，请执行以下操：

1. 输入作业的名称并选择实例类型，然后将模板拖放到命令窗格中。

   创建配置作业时，可以将本地和远程文件名参数转换为变量。这样，您就可以在每次执行作业时为同一组 Citrix ADC 实例为这些参数分配不同的文件。

2. 在您输入的命令中，选择要转换为变量的文件名，然后单击转换为变量。
3. 在 选择实例 选项卡中，选择要在其上运行这些命令的实例。
4. 如果您在命令中指定了任何变量，请在“指定变量值”选项卡中，选择以下选项之一为您的实例指定变量：

   - 输入文件中的变量值 - 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
   - Common variable values for all instances（用于所有实例的公用变量值）- 指定 syslog 服务器 IP 地址和端口。

5. 在“作业预览”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令，然后单击“下一步”。
6. 在“执行”选项卡中，单击“完成”以运行配置作业。现在，如果您要将另一个服务添加到此负载平衡服务器，并将该服务绑定到该服务器，可以在命令页面上编辑命令并将其保存。
7. 导航到 审核模板，然后单击 添加。
8. 将“LBVariablesTemplate”模板拖放到命令窗格中。您可以看到该模板中已更新了新命令。

审核模板显示在“Audit Templates”（审核模板）列表中，每 12 小时根据指定实例的配置运行一次。您现在可以创建模板，并在“Configuration Jobs”（配置作业）模块与“Configuration Audit”（配置审核）模块之间重用这些模板。

导入和导出配置模板

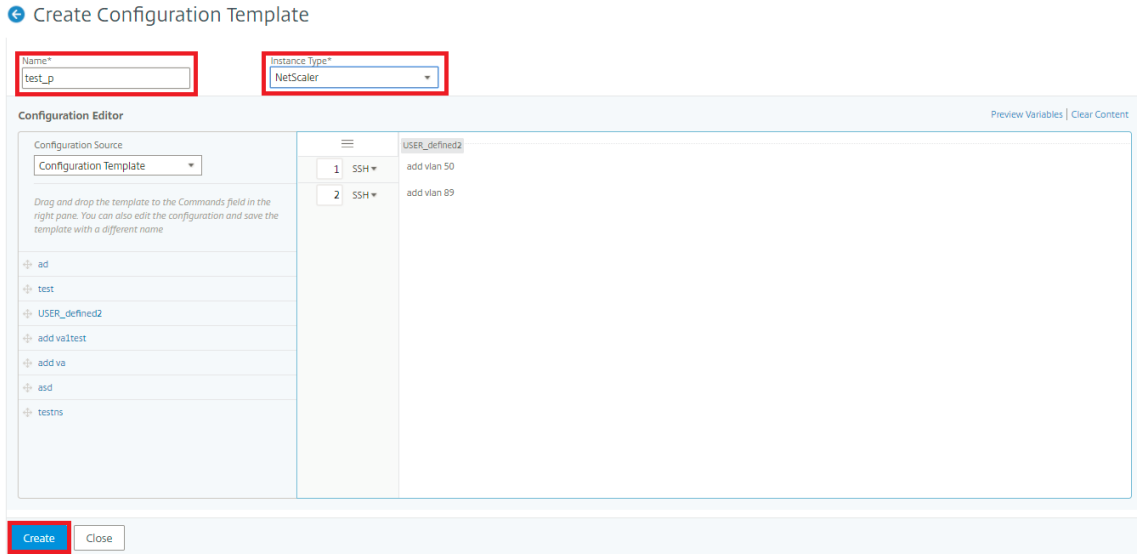
February 6, 2024

您可以从任何 Citrix Application Delivery Management (ADM) 中导出配置模板。您也可以在将来的任何时候将文件导入到同一个或另一个 Citrix ADM 中。配置模板数据（如配置命令、变量定义和参数）不会丢失。

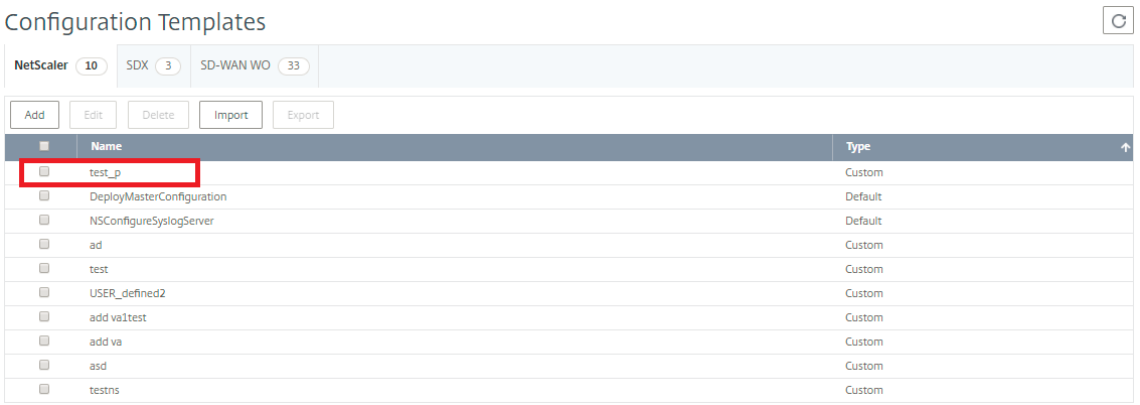
您可以将配置模板导出为 **.json** 文件格式，并将其保存在本地文件夹中。您可以将配置模板.**json** 文件导入到 Citrix ADM 中。此文件可能是新文件，也可能是您从相同或其他 Citrix ADM 中导出的文件。

要导出配置模板，请执行以下操作：

1. 导航到“网络” **>** “配置作业” **>** “配置模板”。
2. 单击“添加”按钮创建配置模板。
3. 在 创建配置模板 页面上，指定配置模板名称，然后选择实例类型。在 配置编辑器下，从下拉菜单中选择配置源作为配置模板。您可以将现有的配置模板拖放到配置编辑器中。单击创建。



4. 导航到 网络 **>** 配置作业 **>** 配置模板，查看在配置模板列表中创建的模板。

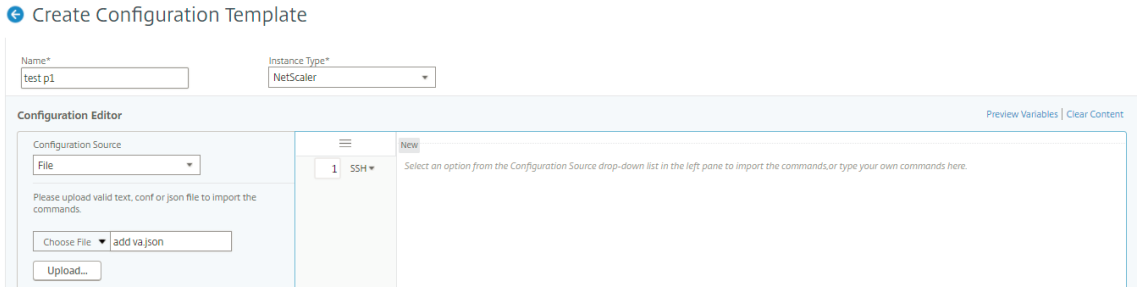


5. 选择新创建的配置模板，然后单击 导出 按钮。

相应的配置模板以 **.json** 格式在本地系统上下载。

要导入配置模板，请执行以下操作：

1. 导航到 网络 **>** 配置作业 **>** 配置模板，然后单击 导 入按钮。选择您拥有的路径。配置模板的 **json** 文件并上载.**json** 文件。强烈建议上载. 已导出的 **json** 文件。
2. 您也可以使用配置编辑器上的“文件”选项导入配置模板 **。
3. 从 配置编辑器的 下拉菜单中选择 文件。
4. 选择“选择文件”（.**json** 文件）来自您的本地系统，然后上载配置模板.**json** 文件。



> 注意
>
> - 每个新导入的模板都存储有新的 ID 字符串。
> - 只有将文件保存在中时，您才能导入配置模板。**json** 格式。如果从本地系统导入 **.json** 文件以外的配置模板，则会显示错误并导入文件失败。

维护作业

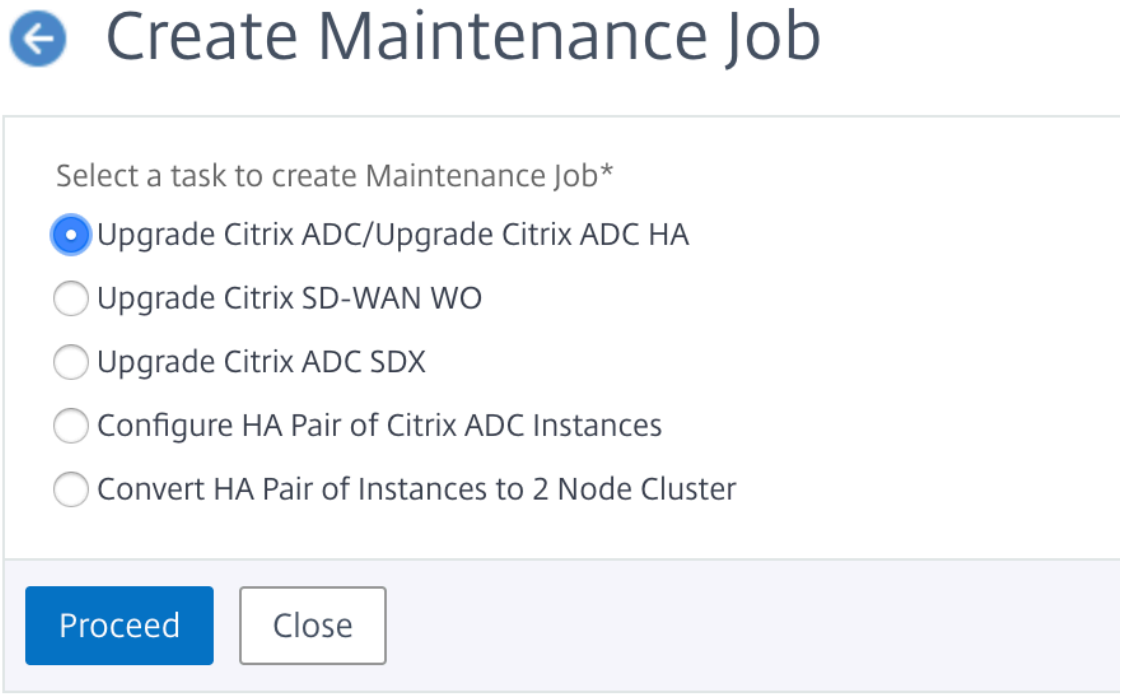
January 29, 2024

您可以使用 Citrix ADM 创建以下维护任务。然后，您可以将维护任务安排在特定的日期和时间。

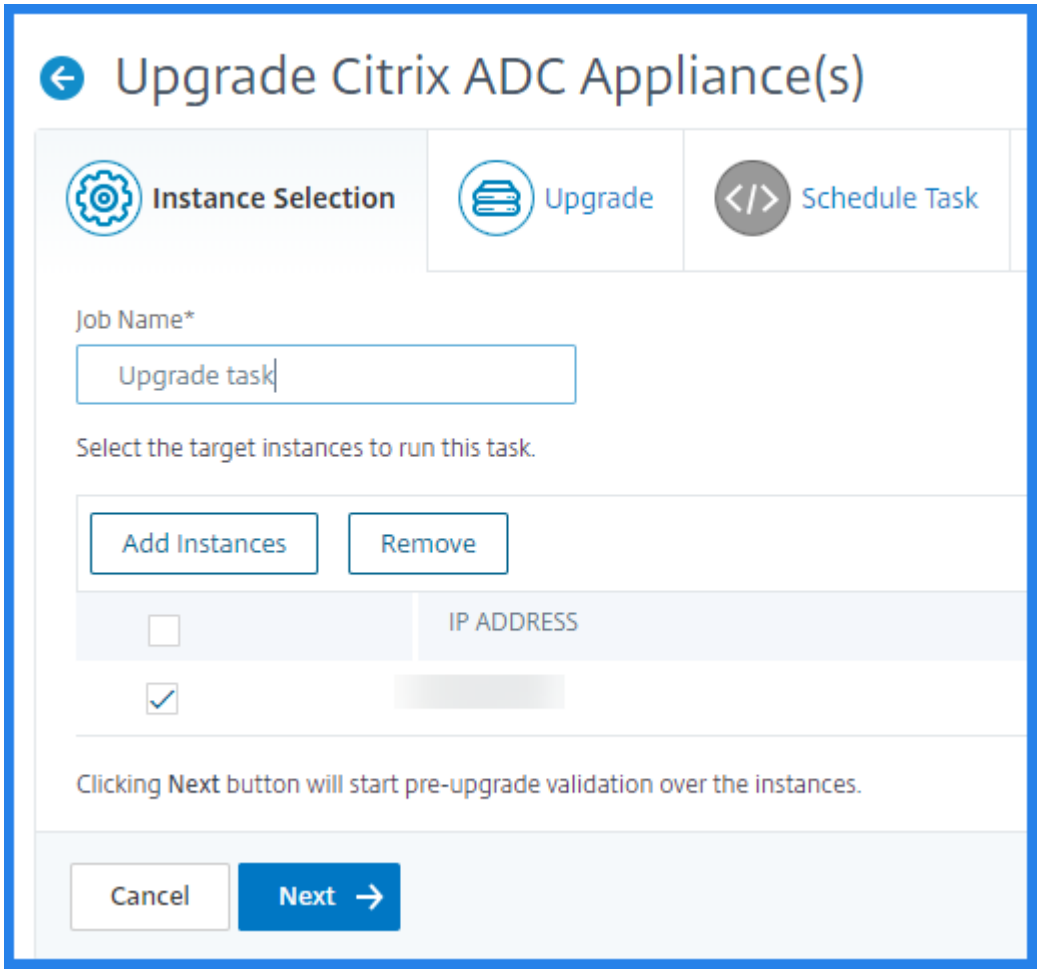
- 升级 Citrix ADC 实例
- 升级 Citrix SD WAN-WO 实例
- 升级 Citrix ADC SDX 实例
- 配置 Citrix ADC 实例的高可用性对
- 将 HA 对实例转换为 2 节点群集

计划升级 **Citrix ADC** 实例

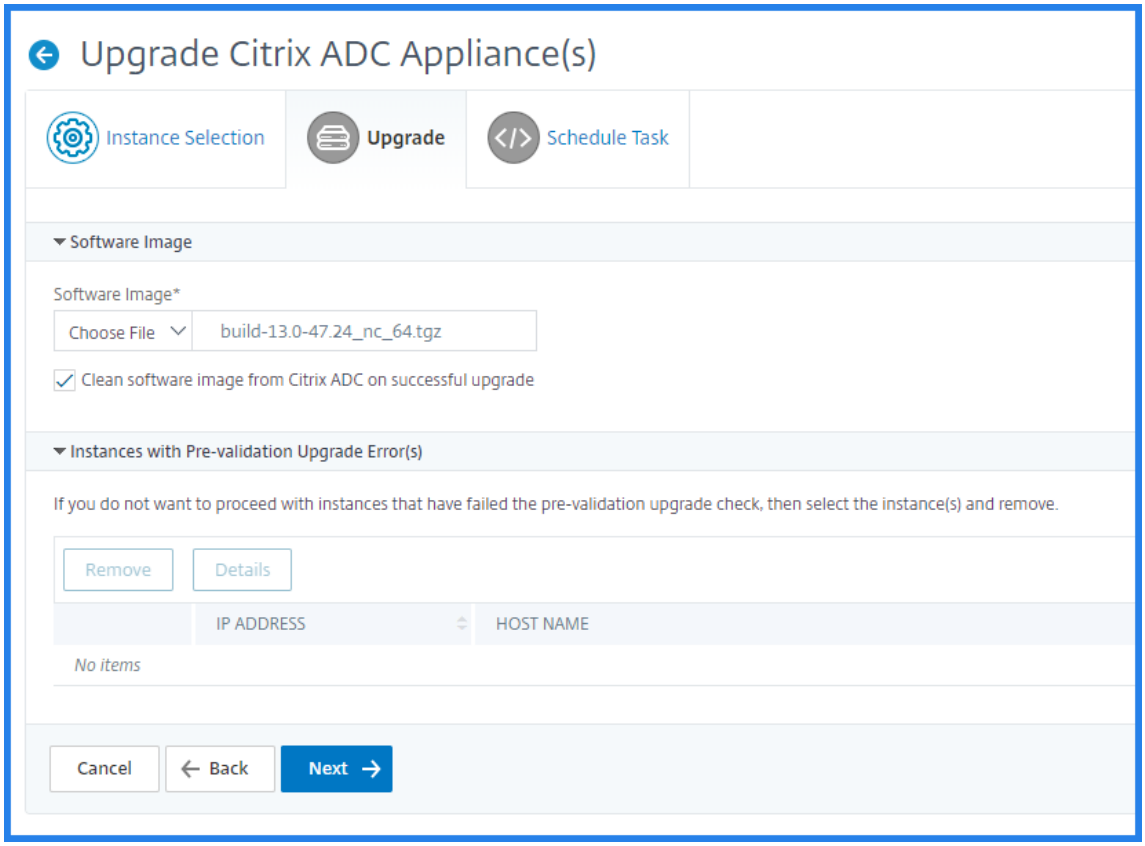
1. 导航到网络 > 配置作业 > 维护作业。单击“创建作业”按钮。
2. 在“创建维护任务”页面上，选择升级 **Citrix ADC**/升级 **Citrix ADC HA**，然后单击继续。



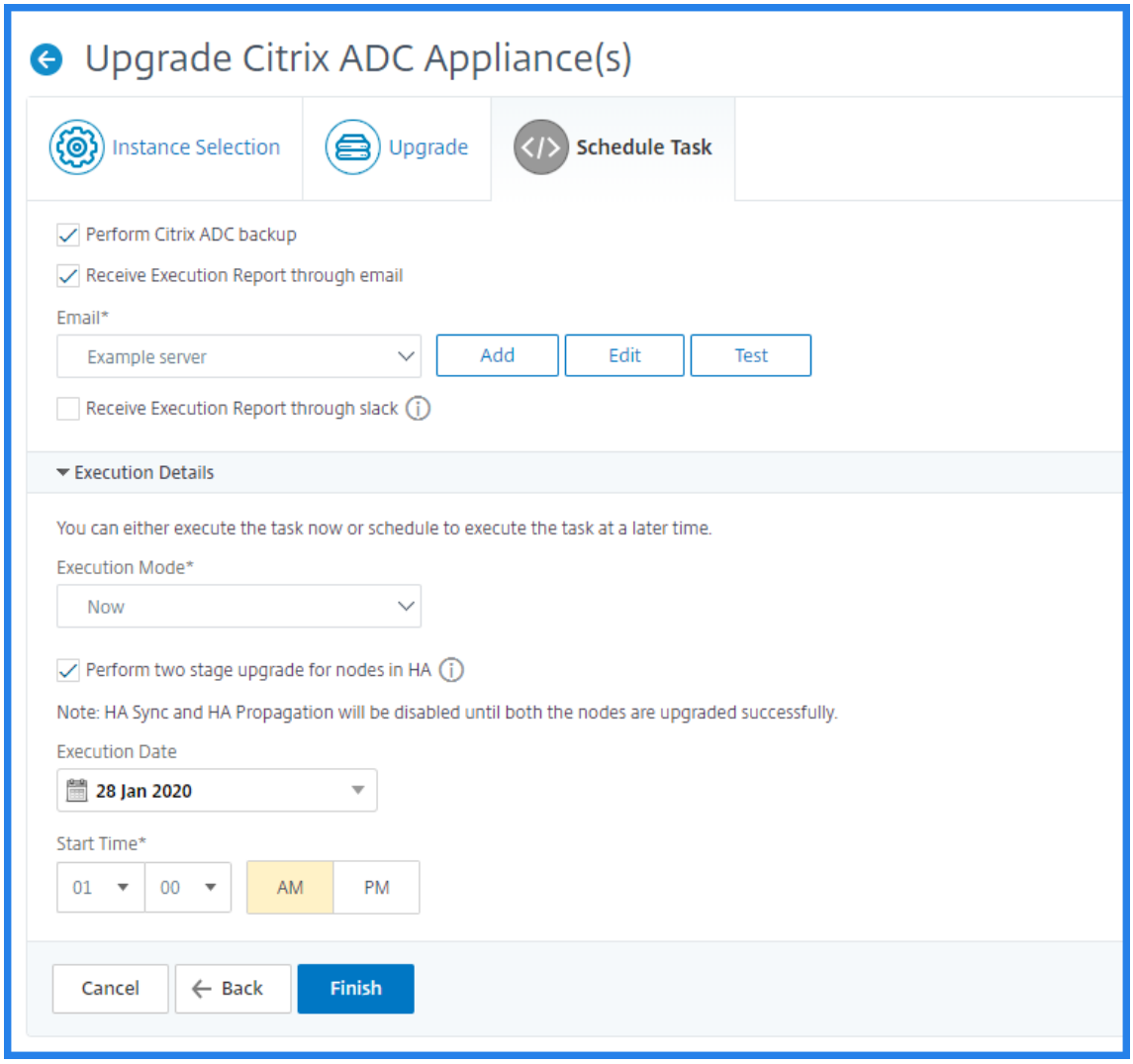
3. 在“升级 Citrix ADC 设备”页面的“实例选择”选项卡中，添加要运行升级过程的 Citrix ADC 实例。单击 下一步 开始对所选实例进行升级前验证。



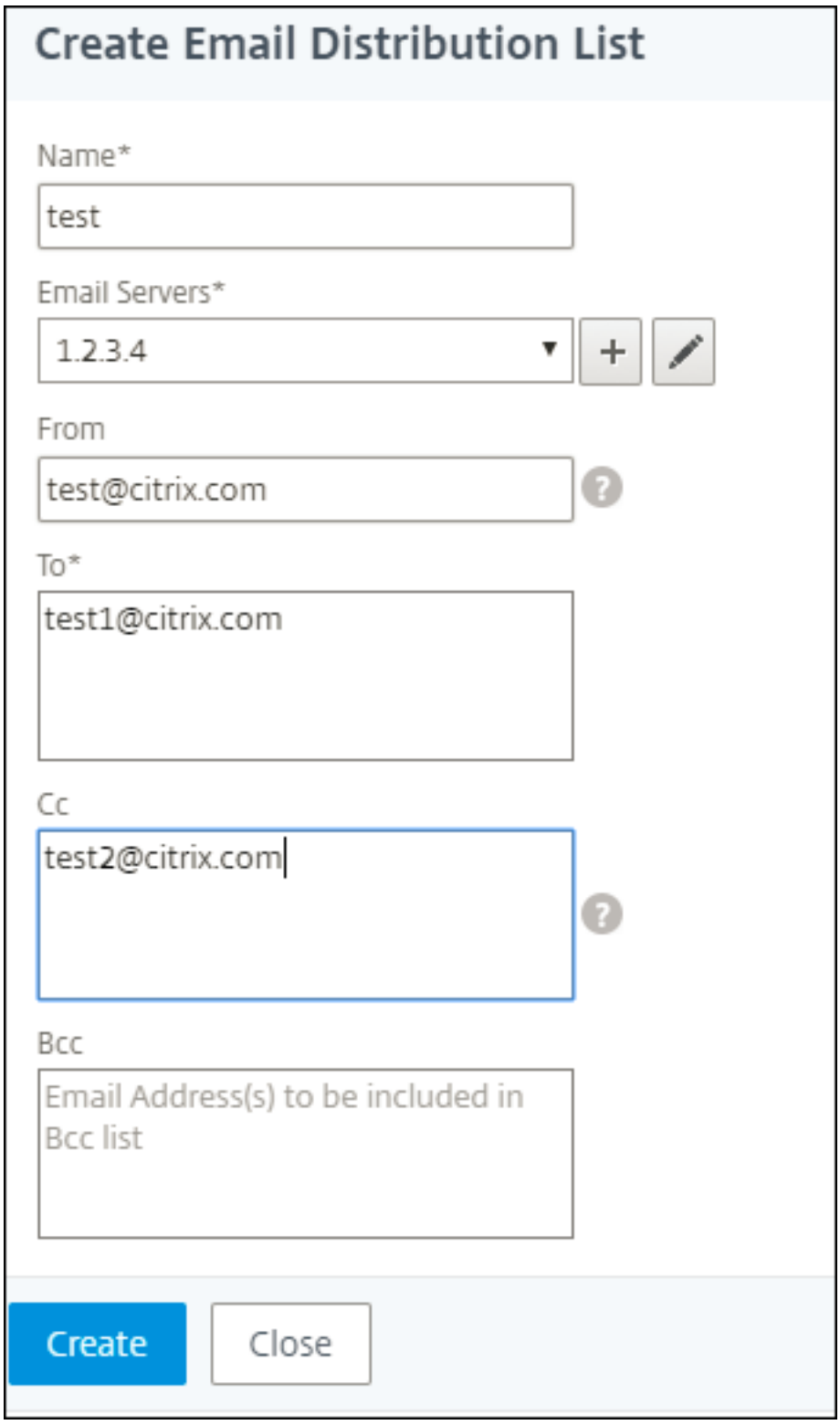
4. 在“升级”选项卡上，从“软件映像”列表中选择本地（您的本地计算机）或设备（编译文件必须存在于 Citrix ADM 虚拟设备上）。



5. 您可以启用电子邮件通知以接收升级 Citrix ADC 实例的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
6. 选择“+”图标以创建电子邮件通讯组列表。
7. 要立即升级 Citrix ADC 实例，请从“执行模式”列表中选择“现在”。
8. 要稍后升级 Citrix ADC 实例，请从“执行模式”列表中选择“稍后”。然后，您可以选择升级 Citrix ADC 实例的执行日期和开始时间。

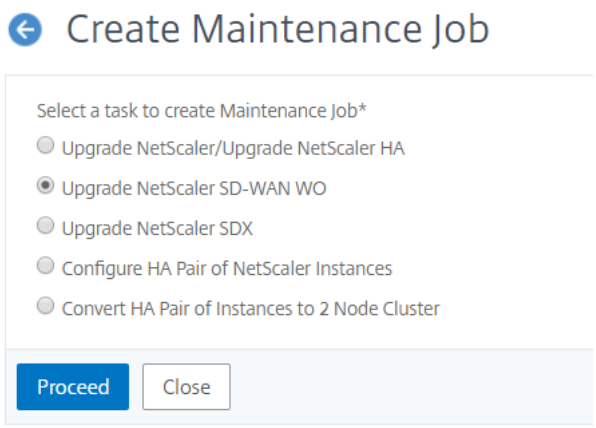


9. 在“创建电子邮件通讯组列表”页面上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。

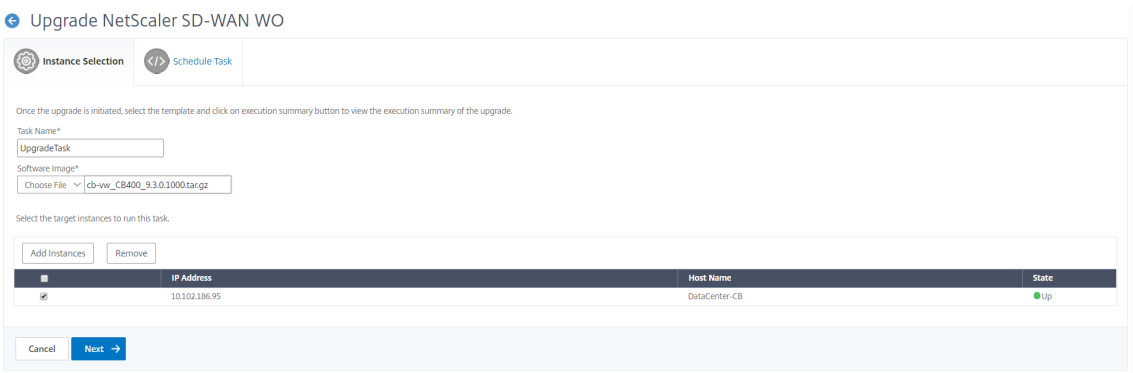


计划升级 **Citrix SD-WAN WO** 实例

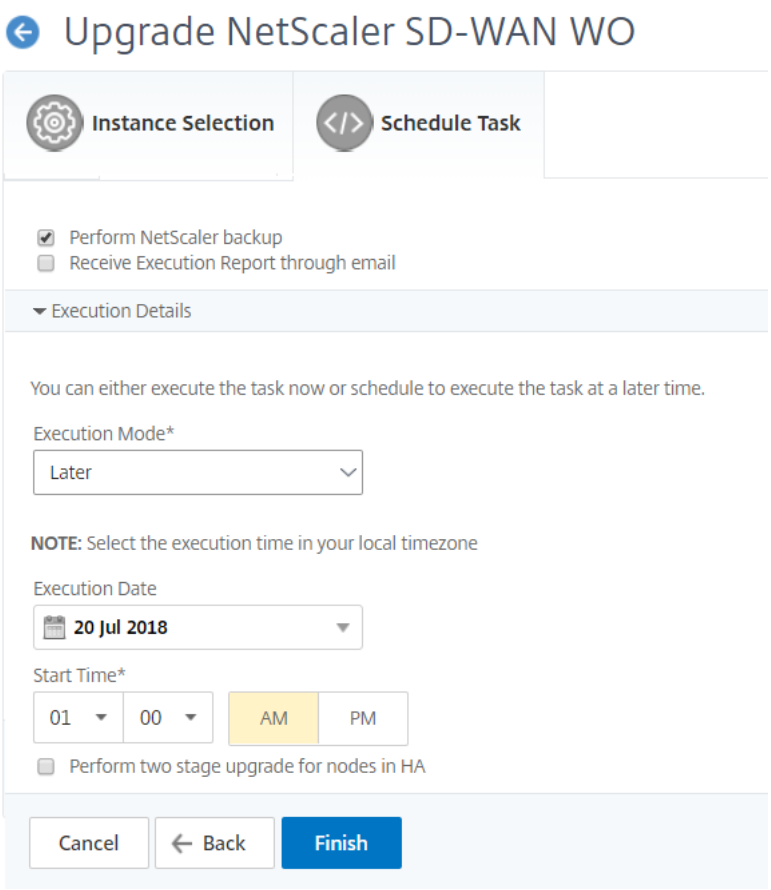
1. 在 Citrix ADM 中，导航到网络 > 配置作业 > 维护作业。单击“创建作业”按钮。
2. 在创建维护作业页上，选择升级 **Citrix SD-WAN WO**，然后单击继续。



3. 在升级 **Citrix SD-WAN WO** 页面的实例选择选项卡中，添加任务名称。从“软件映像”列表中，选择“本地”（您的本地计算机）或“设备”（编译文件必须存在于 Citrix MAS 虚拟设备上）。添加要在其上运行升级过程的 Citrix SD-WAN WO 实例。单击下一步。



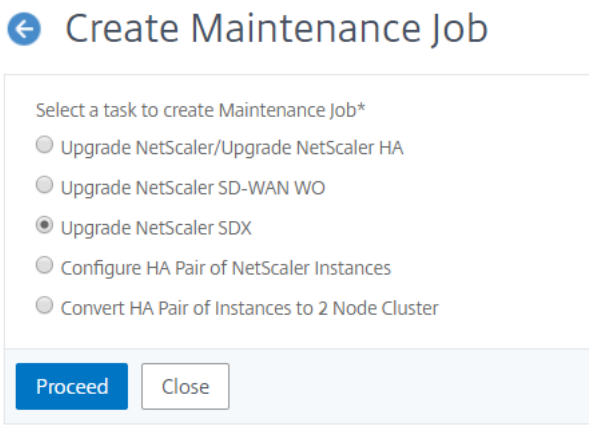
4. 要立即升级 Citrix SD-WAN WO 实例，请从执行模式列表中选择现在。单击完成。
5. 要稍后升级 Citrix SD-WAN WO 实例，请从执行模式列表中选择稍后。然后，您可以选择升级 Citrix SD-WAN WO 实例的执行日期和开始时间。
6. 您可以启用电子邮件通知以接收升级 Citrix SD-WAN WO 实例的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
7. 选择 **+** 图标以创建电子邮件通讯组列表。



8. 在“创建电子邮件通讯组列表”页面上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。

计划升级 **Citrix ADC SDX** 实例

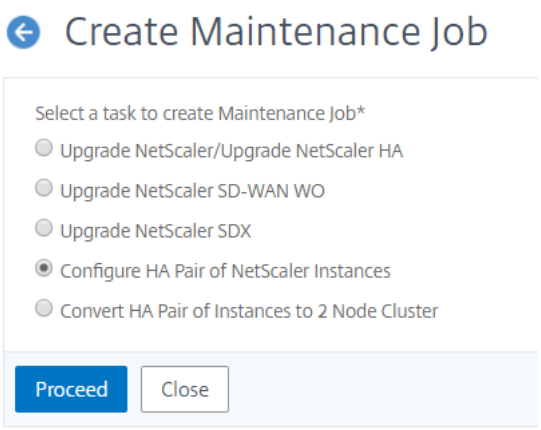
1. 在 Citrix ADM 中，导航到网络 > 配置作业 > 维护作业。单击“创建作业”按钮。
2. 在创建维护作业页面上，选择升级 **Citrix ADC SDX**，然后单击继续。



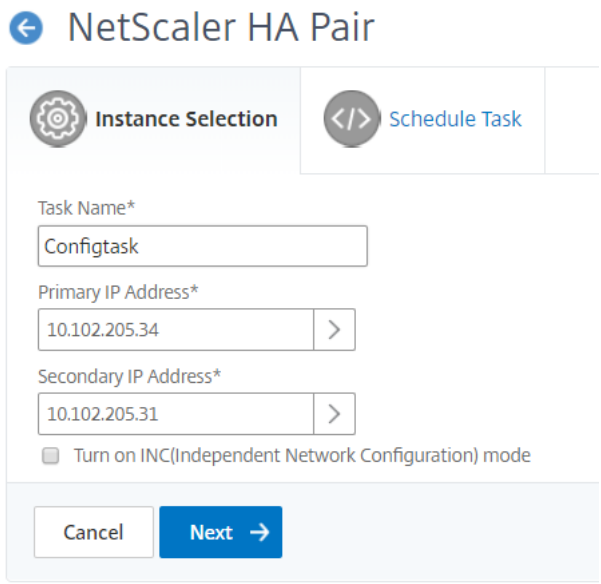
3. 在“升级 **Citrix ADC SDX** 装置”页上的“实例选择”选 项卡中，添加 任务名称。从“软件映像”列表中，选择“本 地”（您的本地计算机）或“设备”（编译文件必须存在于 Citrix ADM 虚拟设备上）。添加要在其上运行升级过程的 Citrix ADC SDX 实例。单击下一步。
4. 您可以启用电子邮件通知，以接收升级 Citrix ADC SDX 实例的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
5. 选择 **+** 图标以创建电子邮件通讯组列表。
6. 要立即升级 Citrix ADC SDX 实例，请从执行模式列表中选择现在。单击完成。
7. 要稍后升级 Citrix ADC SDX 实例，请从执行模式列表中选择稍后。然后，您可以选择用于升级 Citrix ADC SDX 实例的执行日期和开始时间。
8. 在“创建电子邮件通讯组列表”页面上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。

计划配置 **Citrix ADC** 实例的高可用性对

1. 导航到网络 > 配置作业 > 维护作业。单击“创建作业”按钮。
2. 在创建维护作业页面上，选择配置 **Citrix ADC** 实例的高可用性对，然后单击继续。



3. 在 **Citrix ADC HA** 对 页面上的“实例选择”选 项卡中，添加 任务名称。输入主 IP 地址和辅助地址，然后单击下一步。

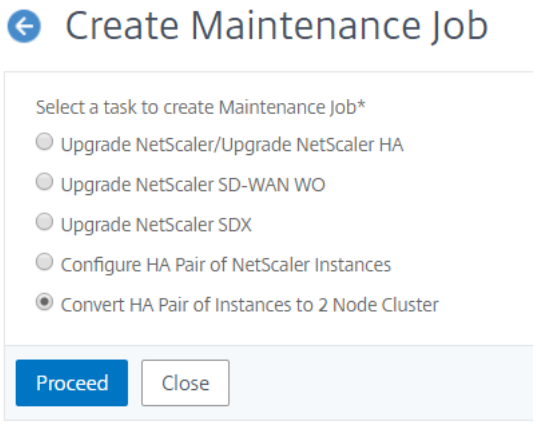


4. 在“计 划任务”选项卡上，您可以选择现在或稍后配置 Citrix ADC HA 对。
5. 要立即配置 Citrix ADC HA 对，请从执行模式列表中选择现在。您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
6. 要稍后配置 Citrix ADC 高可用性对，请从“执行模式”列表中选择“稍后”。然后，您可以选择电子执行日期和开始时间。您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
7. 选择 **+** 图标以创建电子邮件通讯组列表。
8. 在“创建电子邮件通讯组列表”页面上，指定电子邮件分发列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在

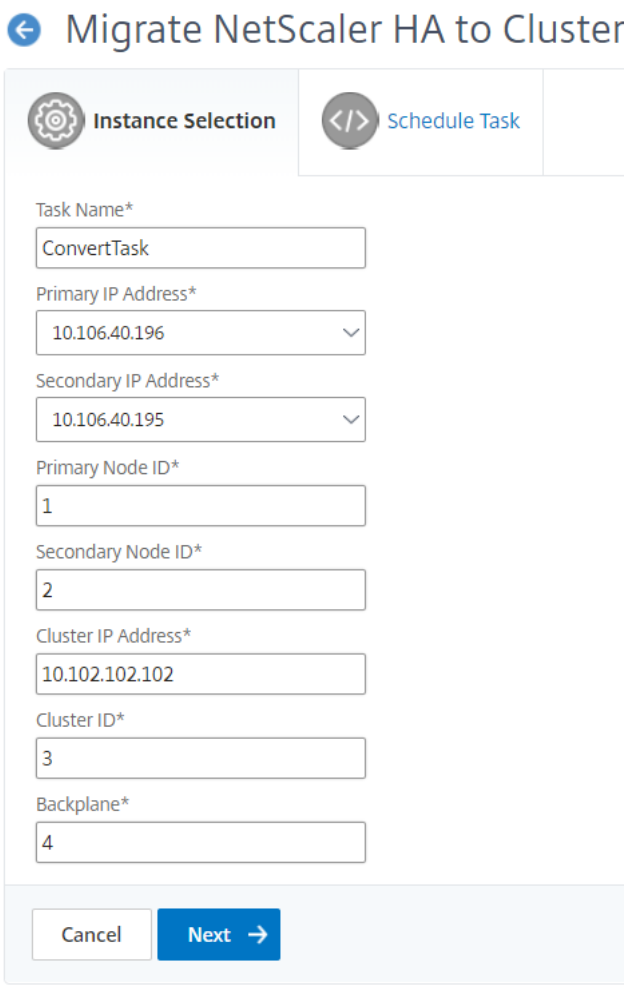
邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。

计划将 **HA** 实例对转换为群集

1. 导航到网络 > 配置作业 > 维护作业。单击“创建作业”按钮。
2. 在创建维护作业页面上，选择将高可用性实例对转换为 **2** 节点群集，然后单击继续。



3. 在“将 **Citrix ADC HA** 迁移到群集”页上的“实例选择”选 项卡中，添加 任务名称。指定主 IP 地址、辅助地址、主节点 ID、辅助节点 ID、群集 IP 地址、群集 ID 和背板。单击下一步。



4. 在“计 划任务”选项卡上，您可以选择立即或稍后将 Citrix ADC HA 迁移到群集。
5. 要稍后配置 Citrix ADC 高可用性对，请从“执行模式”列表中选择“稍后”。然后，您可以选择执行日期和开始时间。您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击“通过电子邮件接收执行报告”复选框以启用电子邮件通知。
6. 选择 **+** 图标以创建电子邮件通讯组列表。
7. 在“创建电子邮件通讯组列表”页面上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在发件人框中，添加要从中发送邮件的电子邮件地址。在收件人框中，添加要向其发送消息的一个或多个电子邮件地址。您还可以添加一个或多个电子邮件地址以发送邮件副本和副本，而无需在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成 配置过程。

配置审核

February 6, 2024

本文档包括：

创建审核模板

February 6, 2024

您希望确保某些配置运行在特定实例上以获得网络的最佳性能。您还希望监视跨托管 Citrix Application Delivery Controller (ADC) 实例的配置更改，排除配置错误，并在系统突然关闭后恢复未保存的配置。您可以使用要在某些实例上审核的特定配置创建审核模板。Citrix Application Delivery Management (Citrix ADM) 将这些实例与审核模板进行比较，并报告配置是否不匹配。每当出现配置不匹配时，Citrix ADM 都会生成配置差异报告，使您能够进行故障排除和纠正不需要的配置更改。

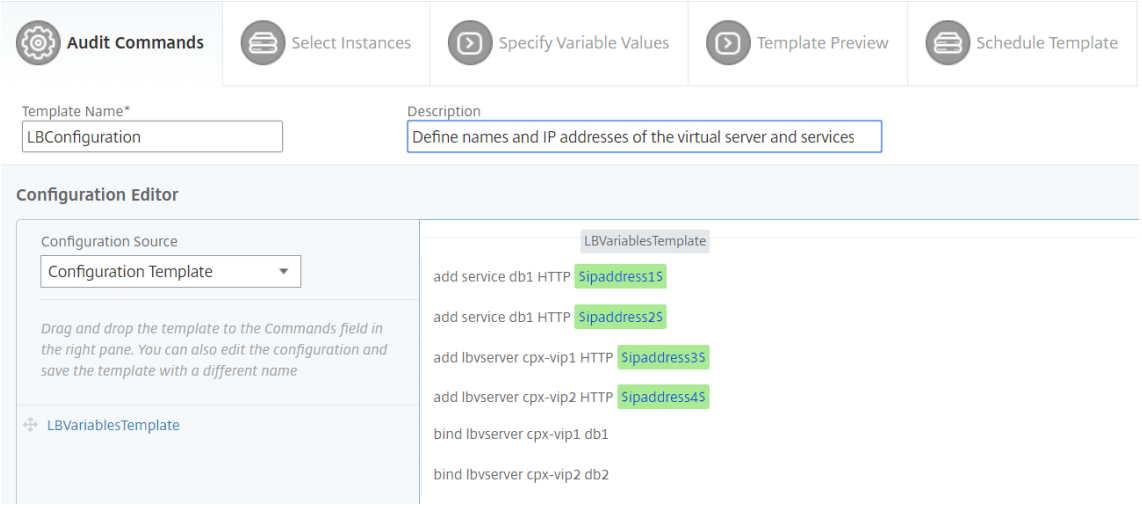
您可以通过以下方式自动运行审核模板：

- 计划应运行模板的时间
- 设置 Citrix ADM 运行模板的频率。您可以每天、在一周中的特定日期或在一个月中的特定日期运行模板。

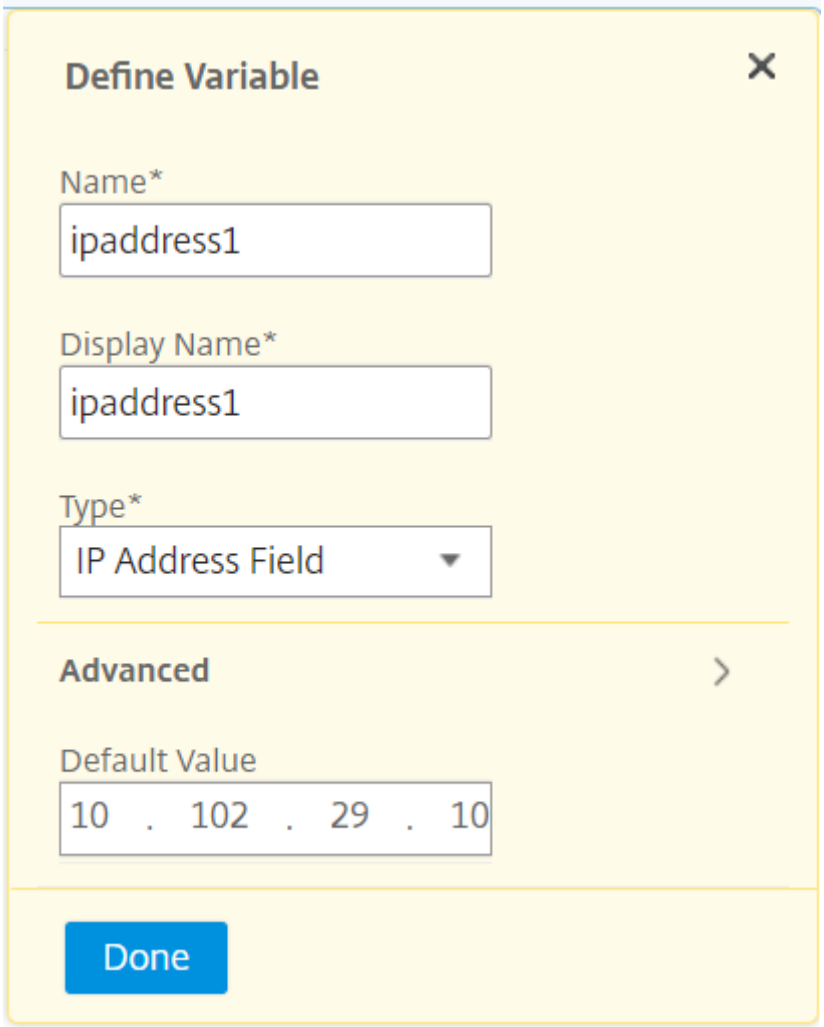
此外，您可以选择将 Citrix ADM 生成的差异报告发送到您可以配置的指定电子邮件地址。通过此选项，您的用户可以将报告作为邮件附件接收，并且用户无需登录到 Citrix ADM 即可手动导出报告。

要创建审核模板，请执行以下操作：

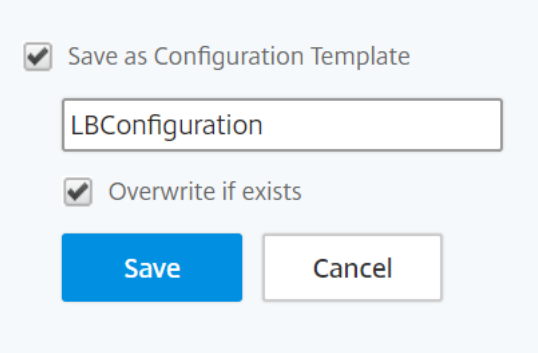
1. 导航到“网络”>“配置审核”>“审核模板”，然后单击“添加”。
2. 在“创建模板”页和“审核命令”选项卡中，指定模板名称及其说明。
3. 在 配置编辑器 页面中，键入您的命令并将命令保存为配置模板。您也可以将现有模板从左窗格拖动到编辑器。
4. 选择要转换为变量的值，然后单击转换为变量。例如，选择负载平衡服务器“ipaddress1”的 IP 地址，然后单击“转换为变量”。该变量现在用“$”括起来，如下图所示。



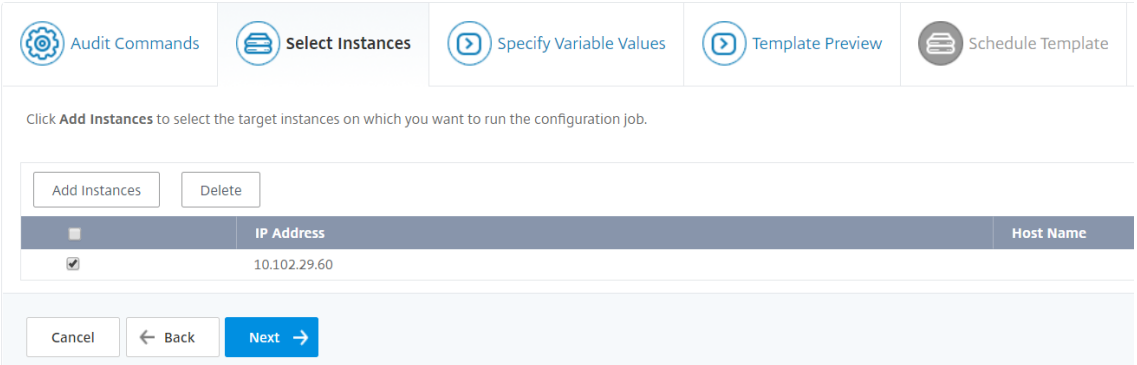
在定义变量窗口中，设置此变量的属性-名称、显示名称和变量的类型。如果要进一步指定变量的默认值，请单击“高 级”选项。



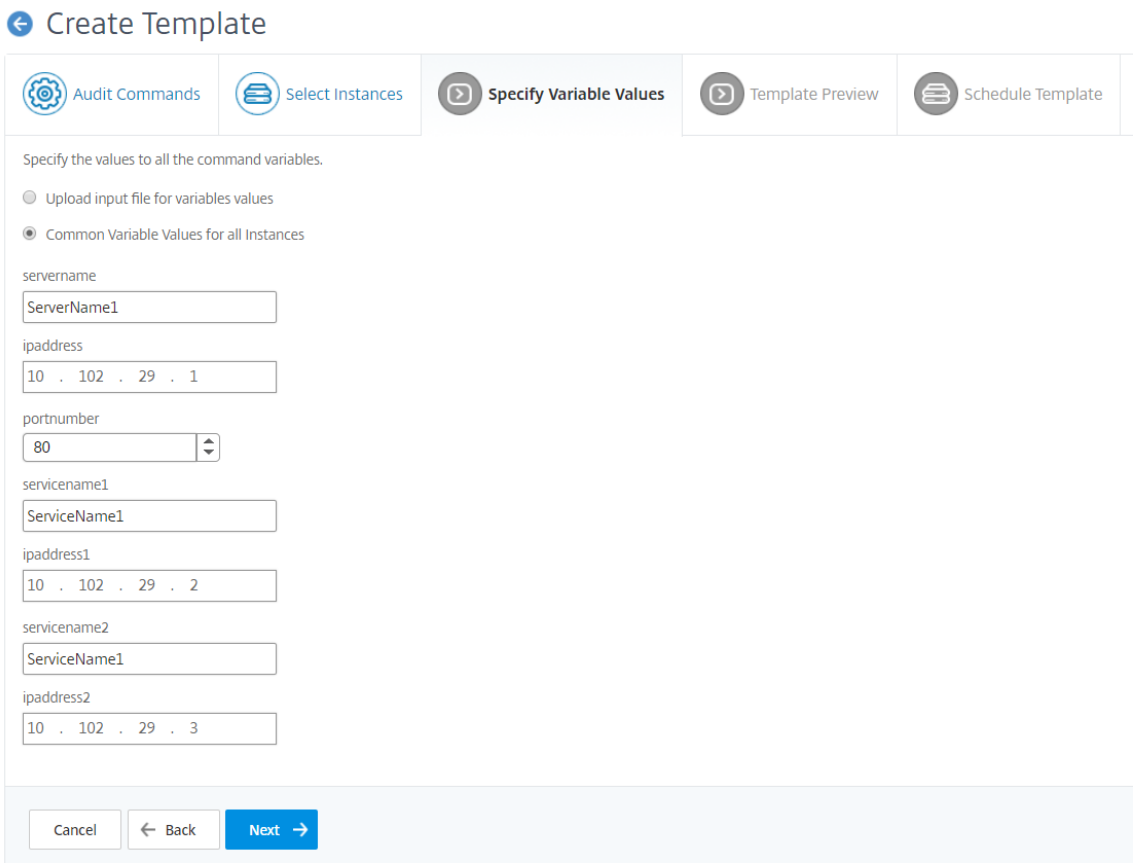
您还可以将命令另存为配置模板。



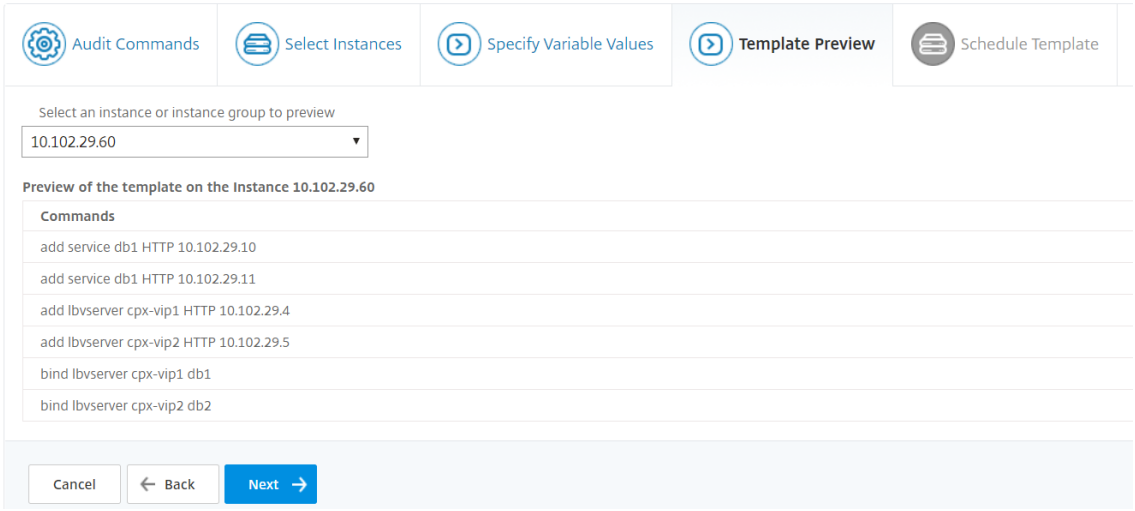
5. 单击保存，然后单击下一步。
6. 在“选择实例”选项卡中，选择要对其运行配置审核的实例，然后单击“下一步”。



7. 在“指定变量值”选项卡中，有两个选项：
   a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器
   b) 输入您为所有实例定义的变量的通用值
8. 单击下一步。



9. 在“模板预览”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令。单击下一步。



10. 在计划模板选项卡中，您有以下选项来计划模板的运行并配置邮件地址以发送差异报告。

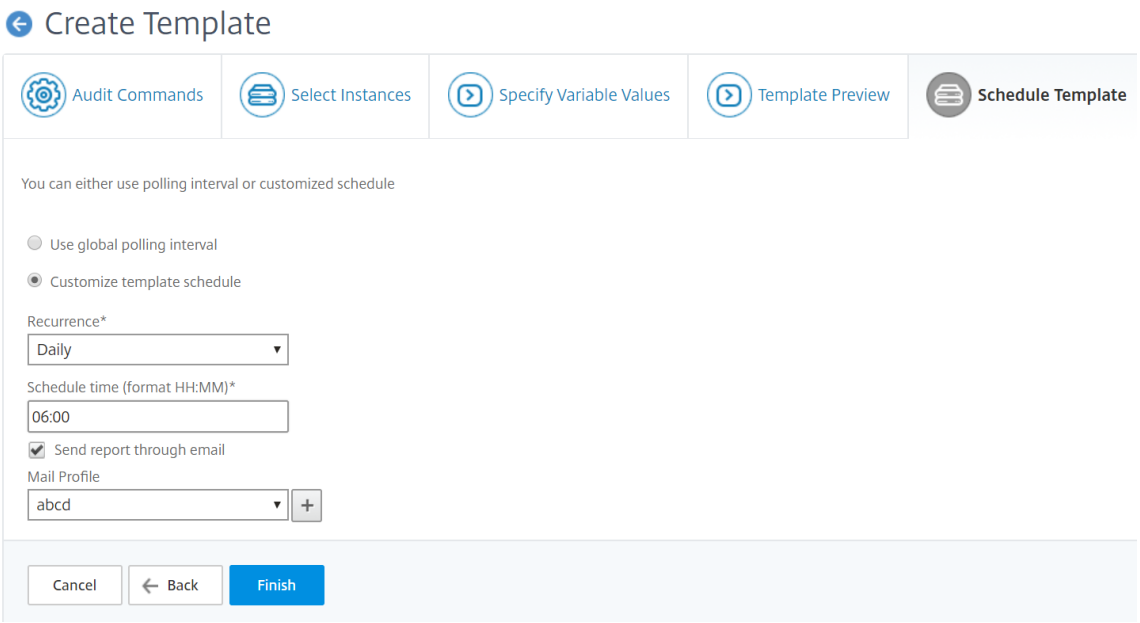
    - 使用全局轮询间隔。选择此选项可在 Citrix ADM 上全局配置的时间在实例上运行模板。

      > 注意
      >
      > 要在 Citrix ADM 中配置全局轮询间隔，请导航到网络 > 配置审核 > 审核模板，然后单击全局轮询

> 时间间隔。在“轮询间隔”字段中，输入 Citrix ADM 应全局轮询实例的分钟数。

- 自定义模板计划。使用此选项可配置需要运行模板的时间和频率
- 通过电子邮件发送报告。使用此选项可以配置差异报告应作为邮件附件发送到的邮件配置文件。

11. 单击完成。



审核模板将显示在 审核模板 列表中，并在计划时间针对指定实例中的配置运行。

查看审核报告

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 允许您在配置审核部分查看和下载配置审核差异报告。配置审核部分允许您导出所有实例和每个实例的摘要报告，还允许您导出每个实例模板对的精细差异报告。

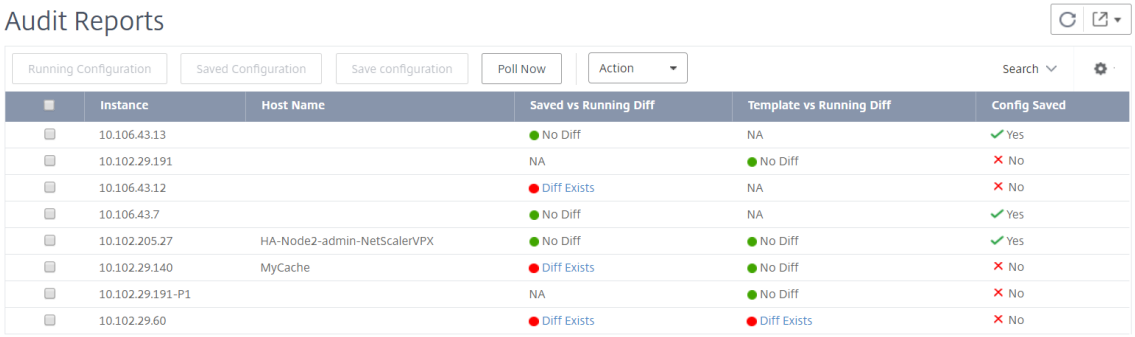
“审核模板”列表中显示的审核模板将在计划时间针对指定实例中的配置运行。“配置审核”控制板上的 NetScaler 配置偏移 图表显示了有关保存的配置更改与未保存的配置相比的高级详细信息。当您单击 **NetScaler** 配置偏差图表时，随后的审核报告页面会显示一个实例列表，其中显示“差异存在”和“无差异”。您可以下载 Citrix ADM 显示的差异报告。

Citrix ADM 还提供了一个选项，用于计划将差异报告自动导出为邮件附件。有关如何计划报告导出的详细信息，请参阅创建审核模板。

要导出配置审核报告，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“配置审核”。

2. 在“配置审核”页面上，单击 **NetScaler** 配置偏移 图表内部。
3. 审核报告 页面列出了存在差异的实例。此页面还显示其运行配置没有任何区别的实例列表。



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

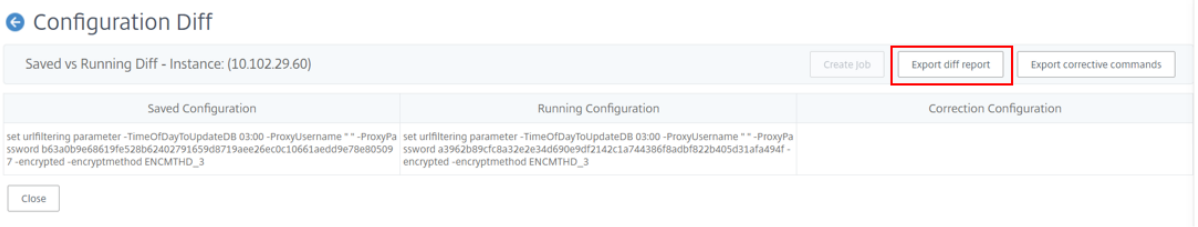
在图像中，您可以看到对于某些实例，差异仅存在于“保存与运行比较”中，对于某些实例，差异仅存在于“模板与运行比较”中。在某些情况下，保存的与正在运行的差异以及模板与正在运行的差异中都存在差异。

已保存与正在运行的比较

您可以查看实例上保存的配置与该实例上当前运行的配置之间的差异报告。例如，单击“已保存与运行差异”下的实例的差异存在。

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

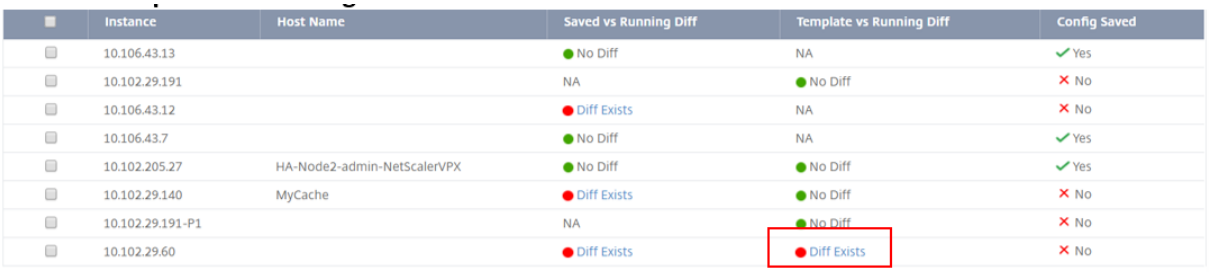
在这里，您可以看到针对该实例运行配置差异的已保存配置的报告。



单击 导出差异报告 可下载差异报告的.csv 文件。也可以单击“导出更正命令”将命令导出到.txt 文件中。然后，您可以从配置作业对关联的 Citrix ADM 实例运行命令，以更正该实例中的配置。

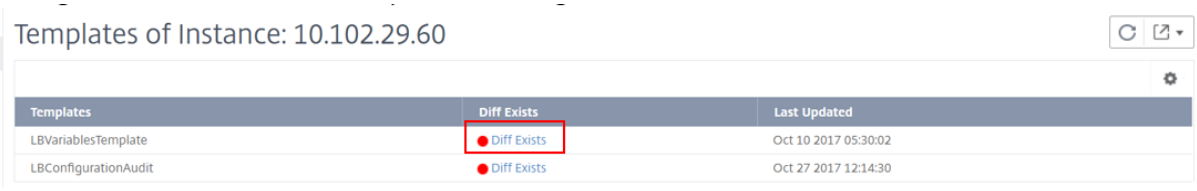
模板与运行比较

“模板与运行比较”包括所有模板，而“保存与运行比较”是默认模板。您可以查看模板和运行配置之间存在的差异。例如，单击“模板与运行比较”下的其中一个实例的比较存在。

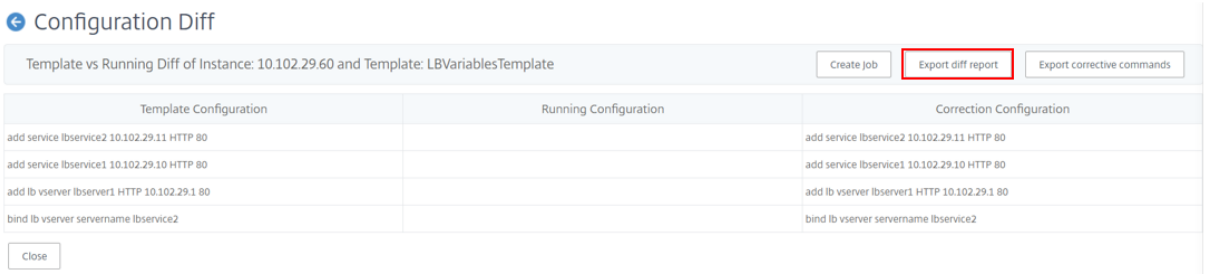


Instance	Host Name	Saved vs Running Diff	Template vs Running Diff	Config Saved
10.106.43.13		No Diff	NA	Yes
10.102.29.191		NA	No Diff	No
10.106.43.12		Diff Exists	NA	No
10.106.43.7		No Diff	NA	Yes
10.102.205.27	HA-Node2-admin-NetScalerVPX	No Diff	No Diff	Yes
10.102.29.140	MyCache	Diff Exists	No Diff	No
10.102.29.191-P1		NA	No Diff	No
10.102.29.60		Diff Exists	Diff Exists	No

现在，您可以看到两个模板显示差异，Citrix ADM 实例的配置与模板正在查找的配置不同。



再次单击“比较存在”。下图显示了模板要查找的配置以及空白的运行配置，因为尚未配置或删除此类命令。您还可以查看更正配置或要运行的命令来更正配置。



单击 导出差异报告 可下载差异报告的.csv 文件。也可以单击“导出更正命令”将命令导出到.txt 文件中。然后，您可以在 CLI 中运行命令来更正该实例中的配置。

下图显示了下载到系统的.csv diff 示例文件：

#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

跨实例审核配置更改

February 6, 2024

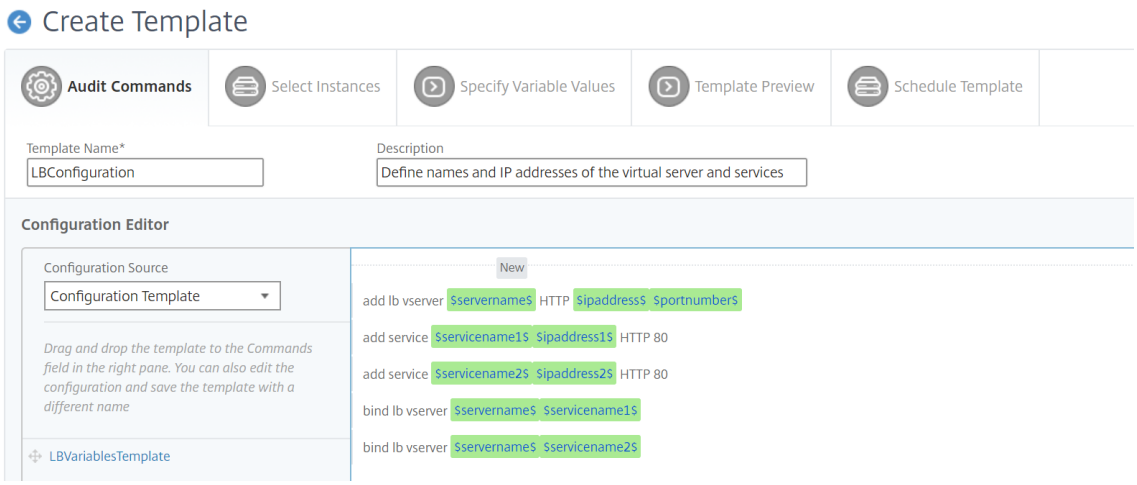
您希望确保某些配置运行在特定实例上以获得网络的最佳性能。您还希望监视跨托管 Citrix Application Delivery Controller (ADC) 实例的配置更改，排除配置错误，并在系统突然关闭后恢复未保存的配置。您可以使用希望运行在

某些实例上的特定配置来创建审核模板。Citrix Application Delivery Management (Citrix ADM) 将这些实例与审核模板进行比较，并报告配置中存在不匹配的情况。这样，就可以对错误进行故障排除并纠正。

您可以通过安排模板的运行时间来自动运行审核模板。您还可以设置 Citrix ADM 运行模板的频率。您可以每天、在一周中的特定日期或在一个月中的特定日期运行模板。您还可以选择将 Citrix ADM 生成的差异报告发送到可配置的指定电子邮件地址。通过此选项，您的用户将以邮件附件形式收到报告，并且用户无需登录到 Citrix ADM 手动检查报告。

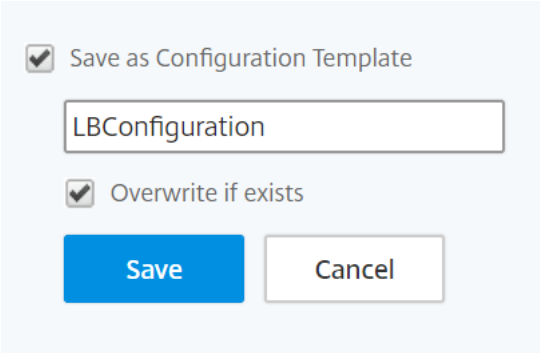
要创建审核模板，请执行以下操作：

1. 导航到 “网络” > “配置审 计” > “审核模板”，然后单击 “添加”。
2. 在“创建模板”页和“审核命令”选项卡中，指定模板名称及其说明。
3. 在 配置编辑器中，键入命令并将命令另存为配置模板。您还可以从编辑器的左侧窗格中拖放现有模板。
4. 选择要转换为变量的值，然后单击转换为变量。例如，选择负载平衡服 务器的 IP 地址“ipaddress”，然后单击“转换为变 量”，如下图所示。



如果要进一步指定变量的默认值，请单击“高 级”选项。

您还可以将命令另存为配置模板。

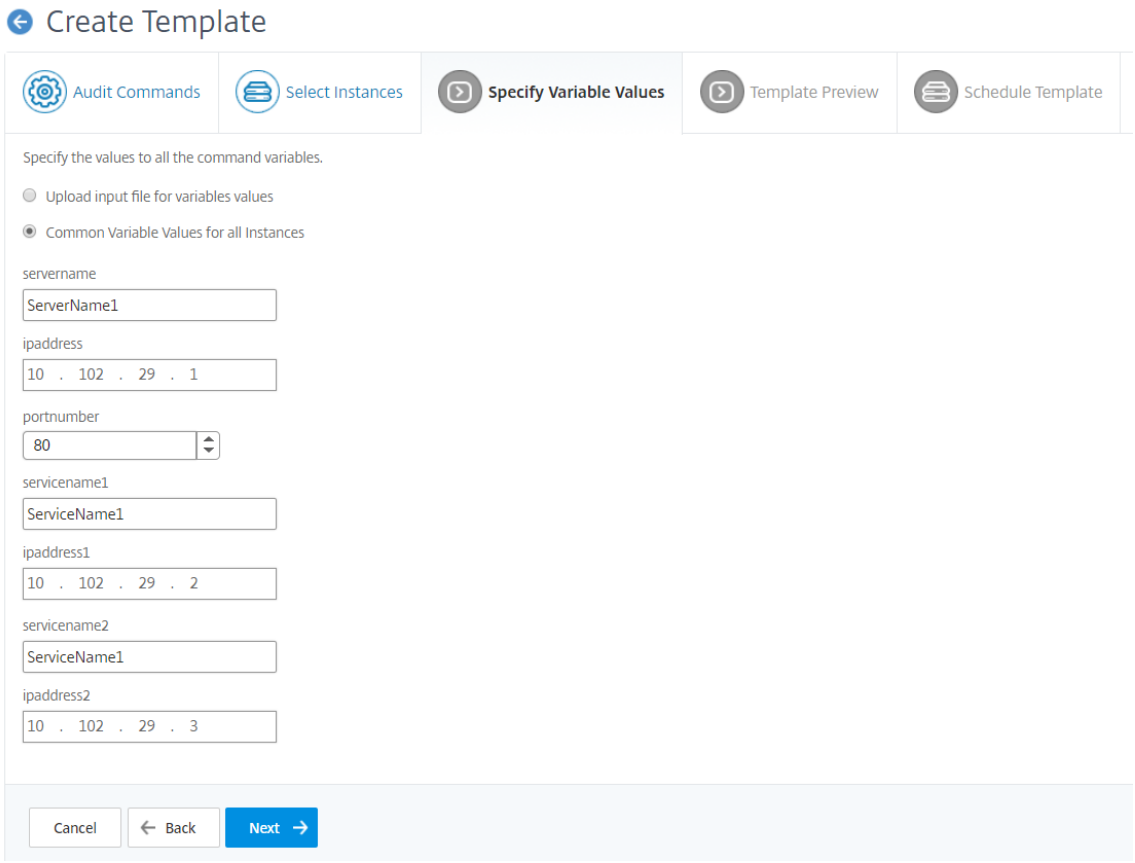


5. 单击保存，然后单击下一步。
6. 在“选择实例”选项卡中，选择要对其运行配置审核的实例。
7. 在“指定变量值”选项卡中，有两个选项：

a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器

b) 输入您为所有实例定义的变量的通用值

8. 单击下一步。

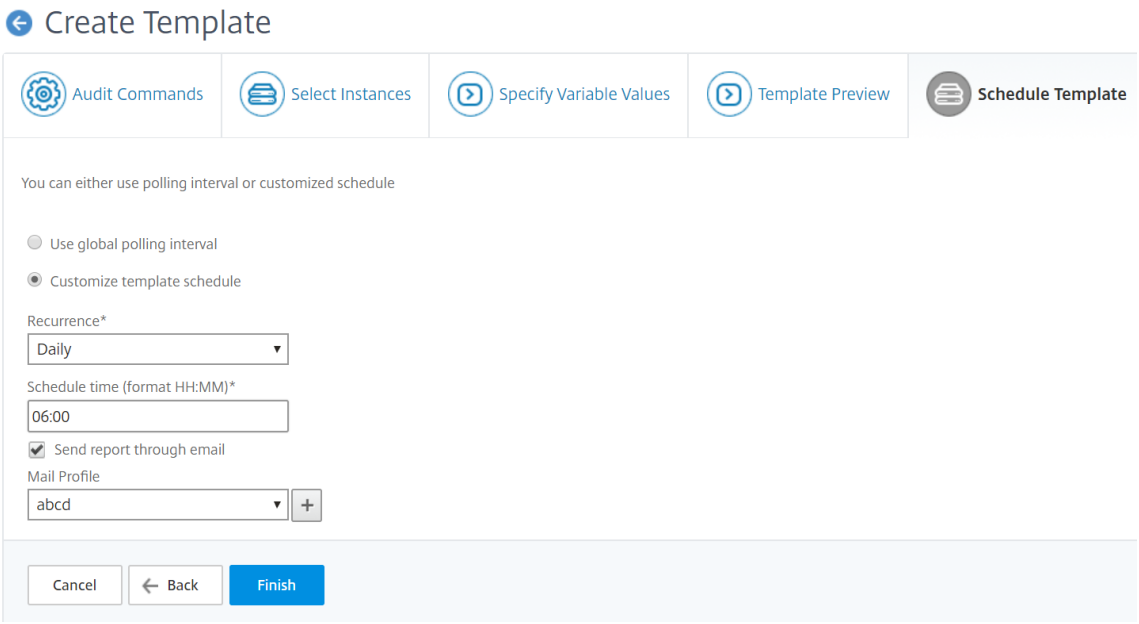


9. 在“模板预览”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令。单击下一步。

10. 在“计划模板”选项卡中，有三个选项可以自动运行模板和发送差异报告的邮件地址。

- 使用全局轮询间隔。选择此选项可在 Citrix ADM 上按全局配置的时间在实例上运行模板
- 自定义模板计划。使用此选项可配置需要运行模板的时间和频率
- 通过电子邮件发送报告。使用此选项可以配置差异报告应作为邮件附件发送到的邮件配置文件。

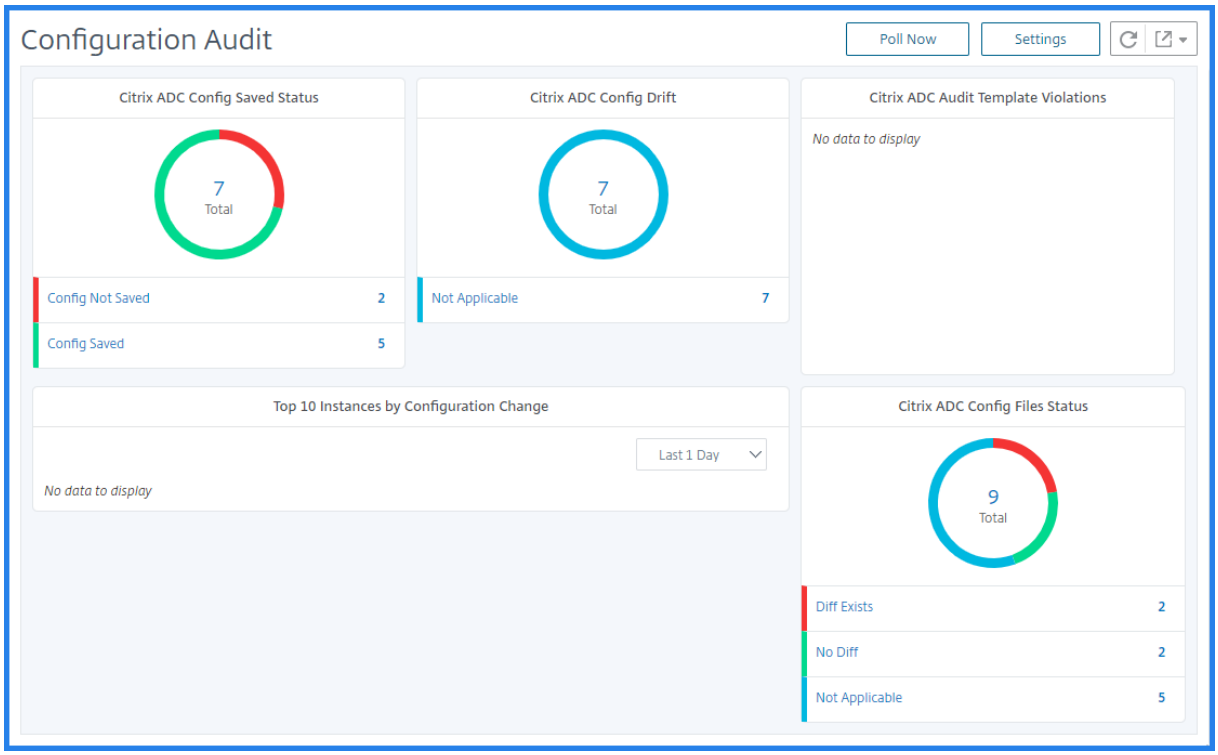
11. 单击完成。



审核模板将显示在 审核模板 列表中，并在计划时间针对指定实例中的配置运行。

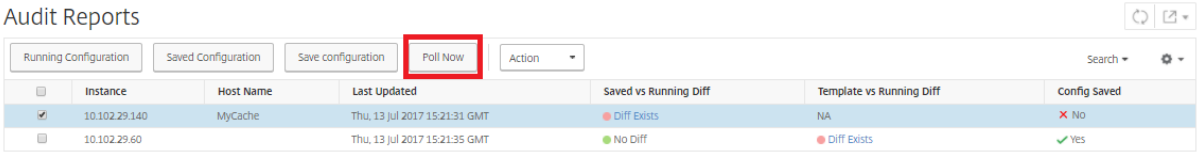
查看配置更改的详细信息

还可以使用“Configuration Audit”（配置审核）控制板查看有关配置更改的高级详细信息，例如按配置更改排在前十位的实例或保存和未保存的配置数。



Citrix ADM 还允许您手动轮询配置审核，并立即将实例的所有配置审核添加到 Citrix ADM 中。为此，请导航到 N 网络 > 配置审核，单击“立即投票”，弹出页面“立即投票”为您提供轮询网络中所有 Citrix ADC 实例或轮询所选实例的选项。

还可以对实例强制执行审核。为此，请单击 **NetScaler Config Saved Status**（NetScaler 配置保存状态）图表或 **NetScaler Config Drift**（NetScaler 配置偏差）图表。在“审核报告”页面上，选择实例，然后在操作 列表中选择 P **poll Now**。



要设置配置审核通知，请执行以下操作：

1. 导航到“网络”>“配置审核”。
2. 在配置审核页上，单击设置。
3. 在 **Notification Settings**（通知设置）页面上，单击 **Edit**（编辑）图标以启用通知设置。
4. 选中 **Enabled**（已启用）复选框，然后从下拉列表中选择电子邮件通讯组列表。还可以单击 **+** 图标并指定电子邮件服务器详细信息来创建电子邮件通讯组列表。

获取有关网络配置的配置建议

February 6, 2024

您可以使用最佳配置设置 Citrix Application Delivery Controller (ADC) 实例，以便在应用程序上实现最佳性能。但是，可能存在有些配置可能不是标准配置，这可能会影响您的应用程序的性能。

为了帮助您优化应用程序性能，Citrix Application Delivery Management (Citrix ADM) 会分析 Citrix ADC 实例配置并为您提供建议。您可以应用 Citrix ADM 中的推荐配置。

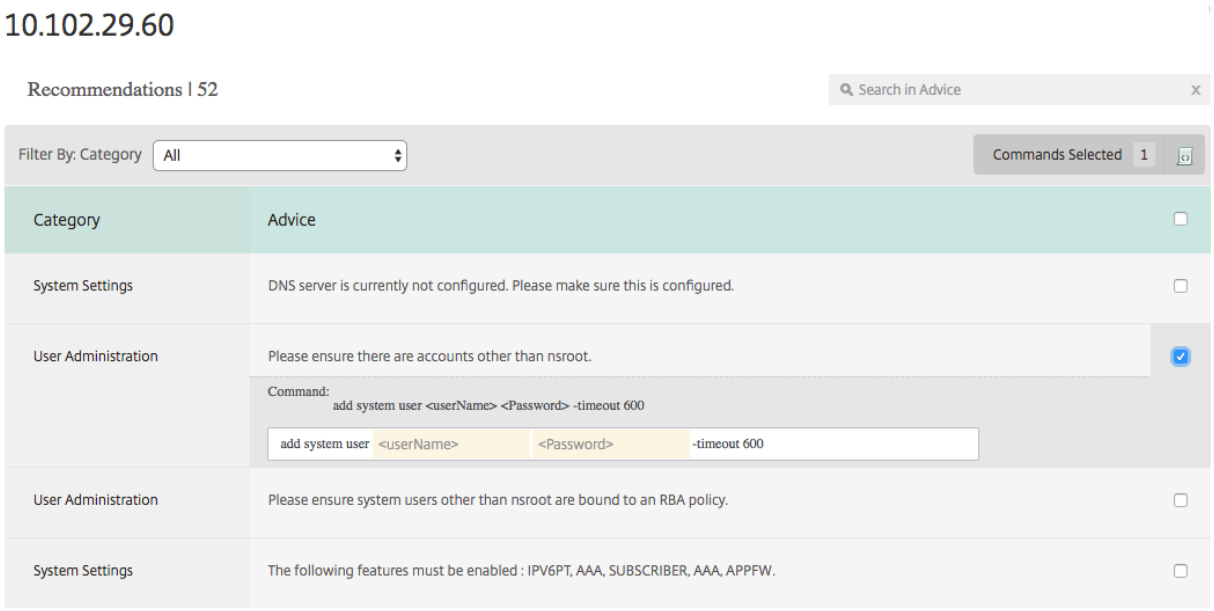
要分析 **Citrix ADC** 实例，请执行以下操作：

1. 导航到 网络 > 配置审核 > 配置建议。
2. 执行以下操作之一：

   - 单击 **Upload Configuration File**（上载配置文件）并上载网络实例的配置文件。

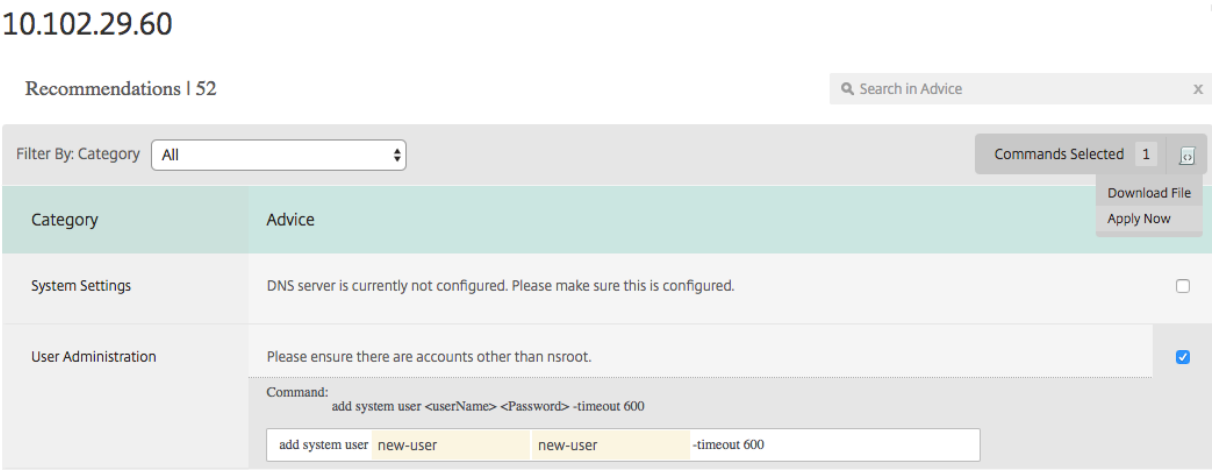
   -单击“选择设备”，然后选择要分析的 Citrix ADC 实例。

Citrix ADM 分析实例上的配置，并提供配置建议列表，如下图所示。单击配置建议旁边的复选框可以查看更正命令。

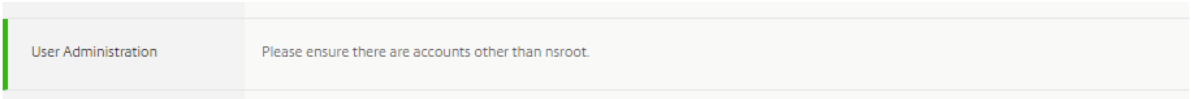


如果要更新配置，请在更正命令中指定变量的值，并单击 **Apply Now**（立即应用），如下图所示。

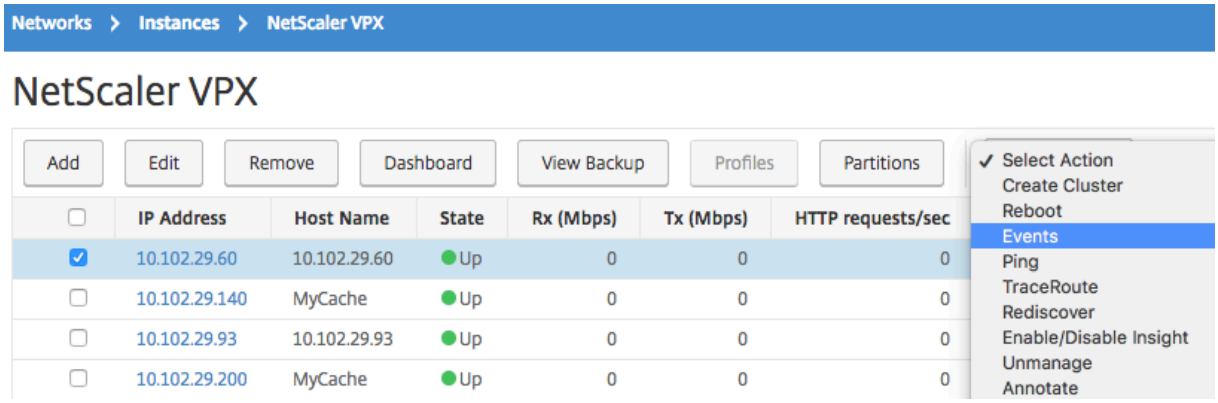
> 注意此处列出
>
> 的命令只是建议。具有读写权限的用户或许能够使用此功能编辑任何命令。确保向您认为不应编辑命令的用户授予有限的特权访问权限。



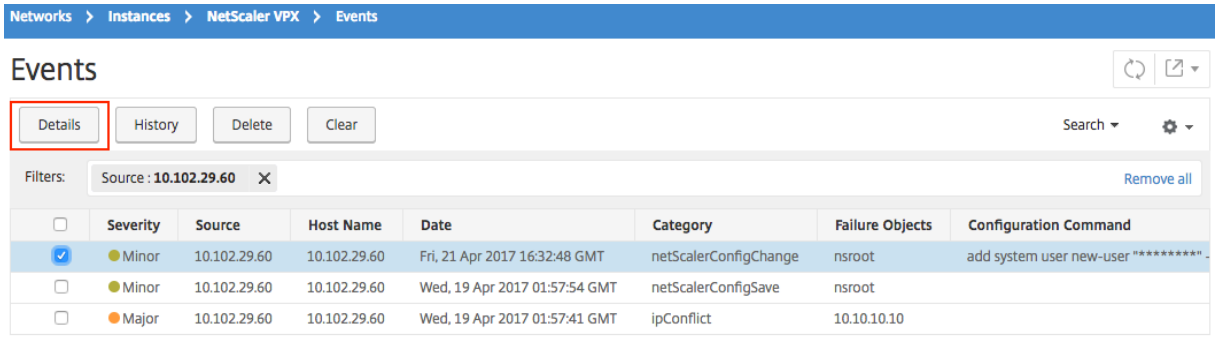
在网络实例上成功运行了命令后，建议旁边的复选框会消失。



如果要查看在网络实例上运行的命令的详细信息，请导航到“网络”>“实例”>“**<Instance_Type>**”，选择实例的 IP 地址，然后从“操作”下拉列表中单击“事件”列表。



在事件页面上，您可以查看配置更改的详细信息。



对 **Citrix ADC** 实例的轮询配置审核

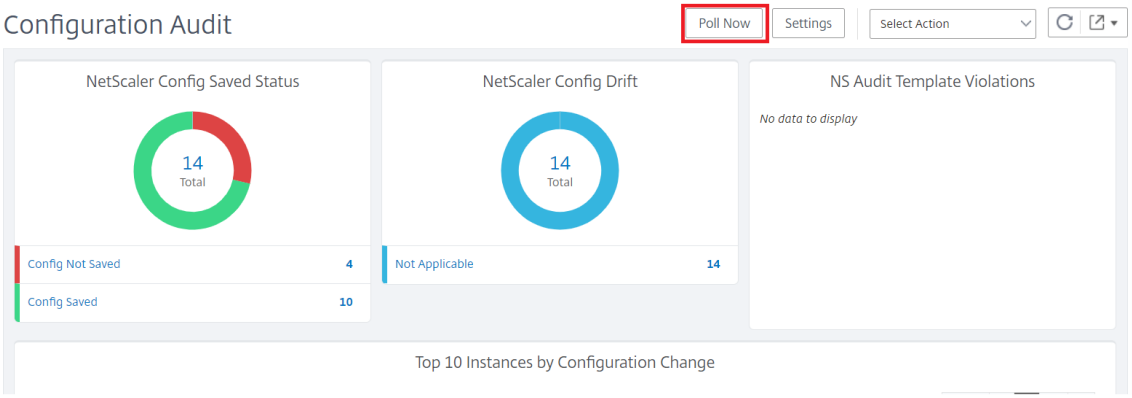
February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 每 10 小时自动轮询配置审核，以查找 Citrix Application Delivery Controller (ADC) 实例上发生的配置更改。您还可以手动轮询配置审核以发现最近的更改，但轮询所有 Citrix ADC 实例配置会给网络带来沉重负载。

您可以仅手动轮询一个或多个选定实例的配置审核，而不是轮询整个 Citrix ADC 实例的配置审核。

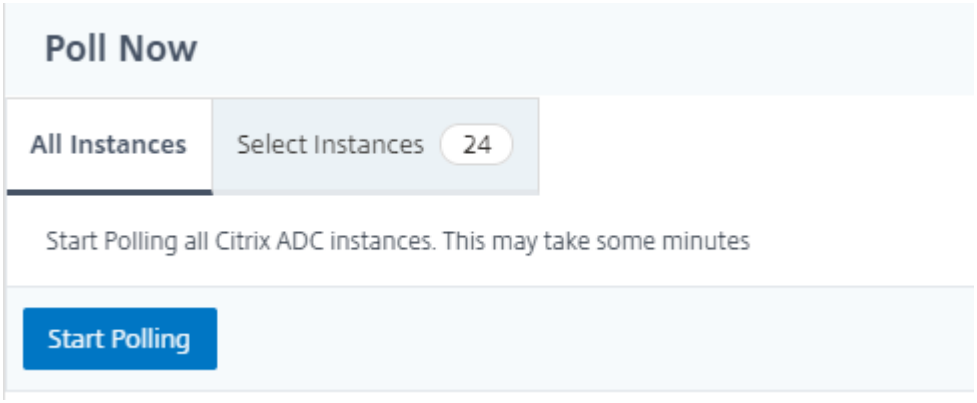
轮询 **Citrix ADC** 实例的配置审核：

1. 在 Citrix ADM 中，导航到“网络”>“配置审核”。
2. 在 配置审核 页上的右上角，单击 立即轮询。

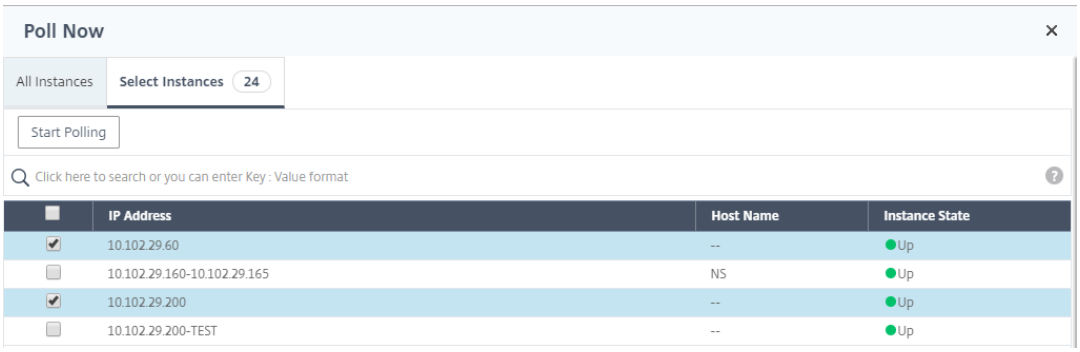


3. 此时会弹出立即轮询页面，您可以选择轮询网络中的所有 Citrix ADC 实例或轮询选定实例。

   a) 要轮询所有 Citrix ADC 实例，请选择 所有实例 选项卡，然后单击 开始轮询。



   b) 要轮询特定实例，请选择 选择实例选项卡，从列表中选择实例，然后单击立即轮询。



为 **ConfigChange SNMP** 陷阱生成配置审核差异

February 6, 2024

每当网络中 Citrix Application Delivery Controller (ADC) 实例的配置发生更改时，配置文件就会更新。实例会将配置更改 SNMP 陷阱发送到 Citrix Application Delivery Management (Citrix ADM)。当实例发送 ConfigChange SNMP 陷阱时，您可以启用 Citrix ADM 对该实例执行配置审核。

如果审核模板配置和正在运行的配置之间存在任何差异，则“审核报告”页面上将显示“差异存在”状态消息。单击 差异退出 链接将转到 配置差异 页面，您可以在其中查看纠正命令。您可以使用这些纠正命令创建配置作业，并在特定 Citrix ADC 实例上执行该作业。运行配置作业时，实例将返回到所需的配置。有关如何通过更正命令创建配置作业的详细信息，请参阅 如何通过 Citrix ADM 上的更正命令创建配置作业。

要在接收 **ConfigChange SNMP** 陷阱时运行配置审核模板，请执行以下操作：

Citrix ADM 允许您启用在 Citrix ADM 中运行配置审核模板的选项。

1. 在 Citrix ADM 中，导航到“网络”>“配置审核”。
2. 在“配 置审核”页面上单击“设置”。
3. 单击“配置更改审核设置”部分中的编辑图标。
4. 选中“收到 **netScalerConfigChange** 事件时进行配置审核”复选框。

> 注意
>
> 这是所有实例的全局设置。Citrix ADM 会对将来收到 netScalerConfigChange SNMP 陷阱的每个实例进行配置审核。

1. 在“运行审核模板的延迟（以 分钟为单位）”字段中，键入分钟。Citrix ADM 在 Citrix ADC 实例收到 Citrix ADC 实例的 ConfigChange SNMP 陷阱时，会在这段时间延迟之后在该实例上运行配置审核模板。

网络功能

February 6, 2024

使用网络功能功能，您可以监视在托管 Citrix 应用程序 Delivery Controller (ADC) 实例上配置的实体的状态。您可以查看统计信息，例如，事务详细信息、连接详细信息以及负载平衡虚拟服务器的吞吐量。您还可以在计划维护时启用或禁用实体。

“Network Functions”（网络功能）控制板为您提供以下图形：

- 客户端连接数最高的前 5 位虚拟服务器
- 服务器连接数最高的前 5 位虚拟服务器
- 吞吐量（MB/秒）最大的前 5 位虚拟服务器
- 吞吐量（MB/秒）最小的前 5 位虚拟服务器
- 虚拟服务器最多的前 5 位实例

- 虚拟服务器的状态
- 负载平衡虚拟服务器的运行状况
- 协议

生成负载平衡实体的报告

February 6, 2024

Citrix Application Delivery Management (ADM) 允许您查看所有级别的 Citrix Application Delivery Controller (ADC) 实例实体的报告。您可以在 Citrix ADM > 网络功能 中下载两种类型的报告：合并报告和单个报告。

合并报告：您可以下载和查看在 Citrix ADC 实例上管理的所有实体的合并报告或汇总报告。

此报告允许您大致了解 Citrix ADC 实例、分区和网络中存在的相应负载平衡实体（虚拟服务器、服务组和服务）之间的映射。

下图显示了一个汇总报告示例。

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				

合并报告的格式为 CSV 格式。每列中的条目说明如下：

- **NetScaler IP** 地址：报告中显示了 Citrix ADC 实例的 IP 地址
- **NetScaler** 主机名：主机名显示在报告中。
- 分区：显示管理分区的 IP 地址
- 虚拟服务器：<name_of_the_virtual_server>#virtual_IP_address :port_number
- 服务：<name_of_the_service>#service-IP_address:port_number
- 服务组:<name_of_service_group>#server_member1_IP_address:port,server_member2_IP_address:port,se ……..,server_membern_IP_address:port

> 注意
>
> - 如果没有主机名，则显示对应的 IP 地址。
> - 空列表示未为该 Citrix ADC 实例配置相应的实体。

个人报告：您还可以下载和查看所有实例和实体的独立报告。例如，您可以仅下载负载平衡虚拟服务器、负载平衡服务或负载平衡服务组的报告。

Citrix ADM 允许您立即下载报告。您还可以计划在每天、每周或每月的某个固定时间生成报告。

生成组合负载平衡报告

1. 在 Citrix ADM 中，导航到网 络 > 网络功能 > 负载平衡。
2. 在“负载平衡”页面上，单击“  ”。
3. 在打开的“导出”页面上，您有两个选项可以查看报告：
   a) 选择“立即导出”选项卡，然后单击“确定”。

      合并报告将下载到您的系统上。

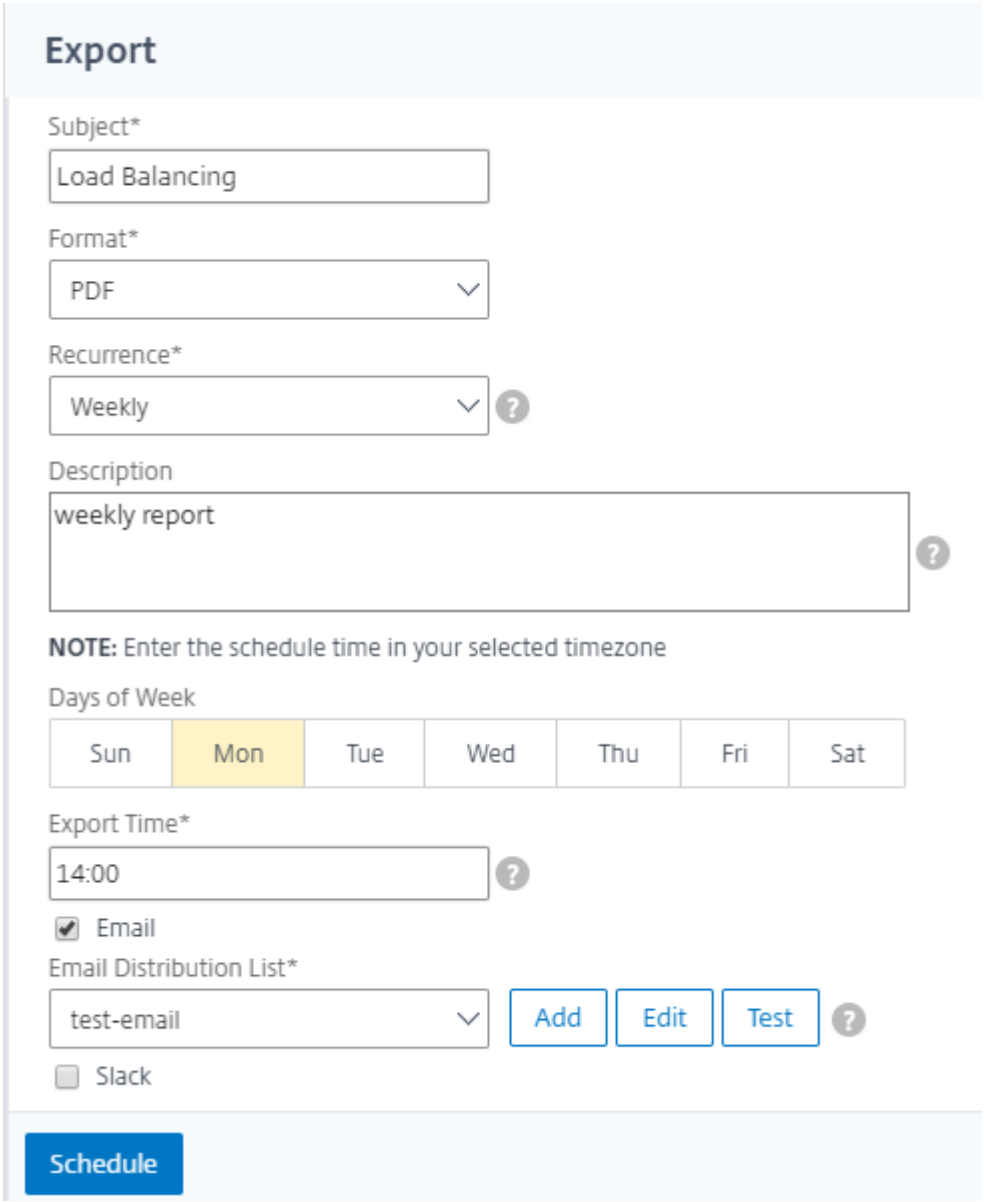
   b) 选择“计划报告”选项卡，计划定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

      i. 重复 -从下拉列表框中选择“每日”、“每周”或“每 月”。

      ii. 重复时间-以 24 小时格式将时间输入为 Hour: minute。

      iii. 电子邮件配置文件 -从下拉列表框中选择一个配置文件，或单击 **+** 创建电子邮件配置文件。

> 注意
>
> 如果您选择每周定期，请确保您选择要计划报表的工作日。

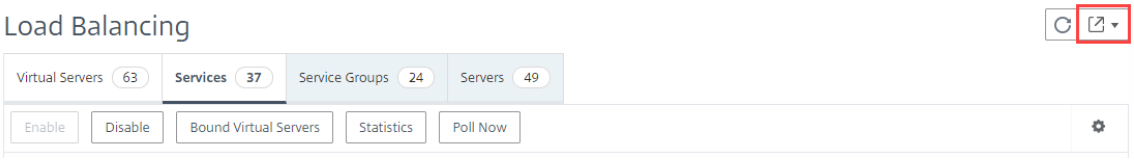


> 注意
>
> 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

生成单个负载平衡实体报告

您可以为与实例关联的特定类型的实体生成并导出单个报告。例如，假定这样一个场景：您要查看网络中所有负载平衡服务的列表。

1. 在 Citrix ADM 中，导航到 网络 > 网络功能 > 负载平衡 **>** 服务。
2. 在 服务 页面上，单击右上角的 导出 按钮。



a) 如果要 在此时生成和查看报告，请选择“立即导出”选项卡。

b) 选择“计划导出”以计划定期生成和导出报告。

> 注意
>
> 只能以邮件附件形式下载报告或导出报告。您无法在 Citrix ADM GUI 上查看报告。

导出或计划网络功能报告的导出

February 6, 2024

您可以为 Citrix Application Delivery Management (ADM) 中的选定网络功能生成综合报告，例如负载平衡、内容交换、缓存重定向、全局服务器负载平衡 (GSLB)、身份验证和 Citrix Gateway。此报告允许您全面了解 Citrix ADC 实例、分区和网络中存在的相应绑定实体（虚拟服务器、服务组和服务）之间的映射。您可以以.csv 文件格式导出这些报告。

报告显示以下虚拟服务器数据：

- NetScaler IP 地址
- 主机名
- 分区数据
- 虚拟服务器名称
- 虚拟服务器的类型
- 虚拟服务器
- 目标 LB 虚拟服务器

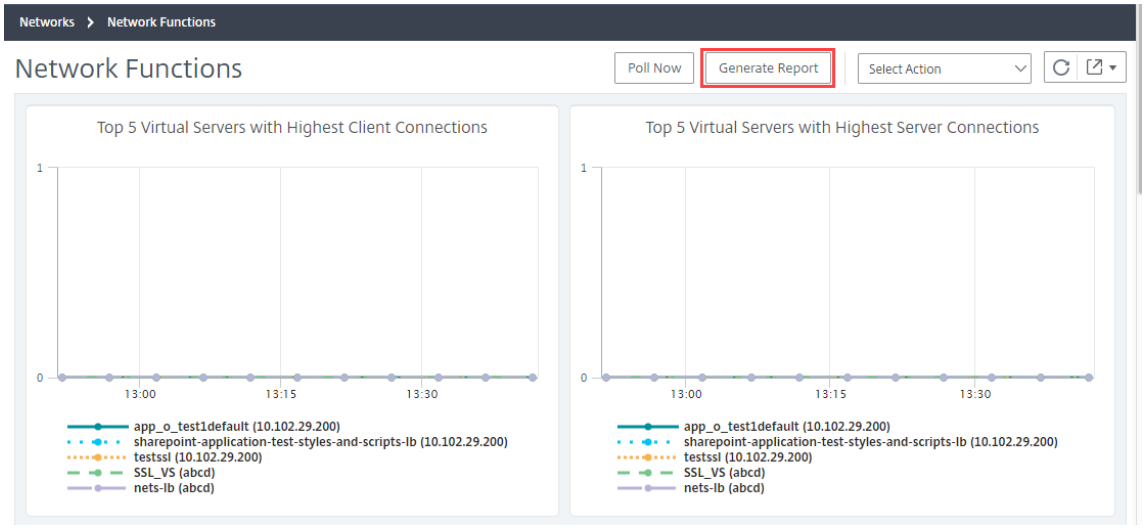
> 注意：
>
> 对于内容交换和缓存重定向虚拟服务器，Target LB 虚拟服务器列列出了所有 LB 服务器，即默认服务器和基于策略的服务器。
>
> - 服务名称
> - 服务组名称

您可以计划按不同的间隔将这些报告导出到指定的电子邮件地址。

> 注意
>
> - 对于 GSLB 虚拟服务器，网络功能报告仅显示 GSLB 虚拟服务器和关联服务。
> - 对于内容切换和缓存重定向虚拟服务器，报告仅显示与关联负载平衡服务器的绑定。
> - 此报告中未列出 SSL 虚拟服务器，因为 Citrix ADM 上未维护单独的 SSL 虚拟服务器列表。
> - 生成新报告时，旧报告将自动从您的帐户中清除。
> - 您无法为 HAProxy 生成网络函数报告。

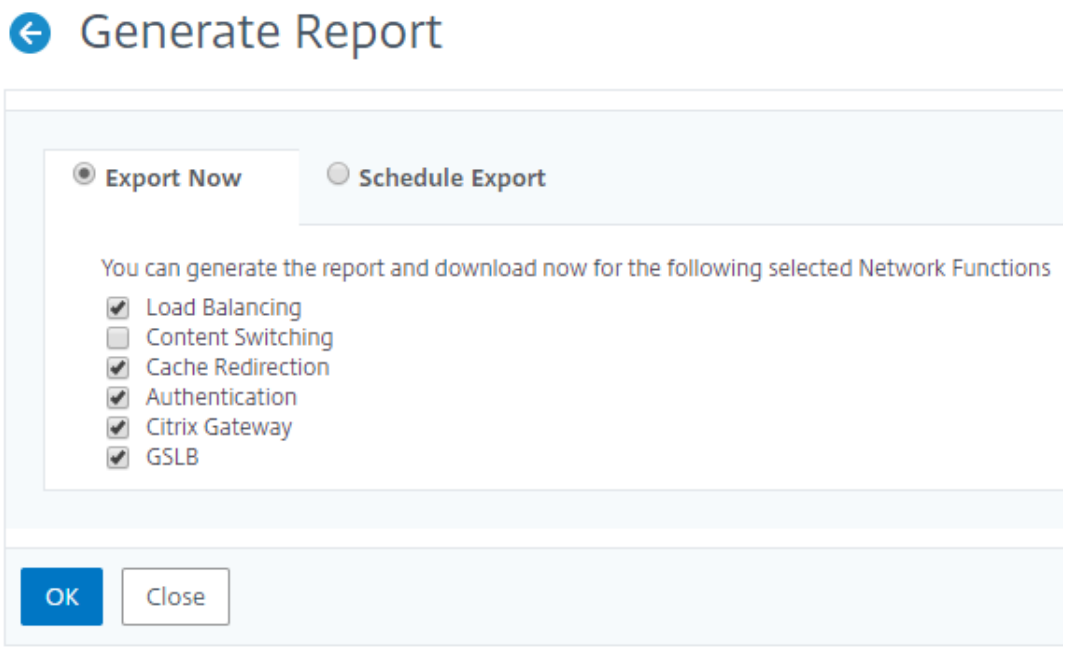
要导出和计划网络函数报告，请执行以下操作：

1. 导航到网络 **>** 网络功能。
2. 在“网络功能”页面的右窗格中，单击页面右上角的“生成报告”。



3. 在 生成报告 页面上，您有以下 2 个选项：

   a) 选择“立即导出”选项卡，然后单击“确定”。报告将下载到您的系统。



下图显示了网络函数报告的示例。

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			

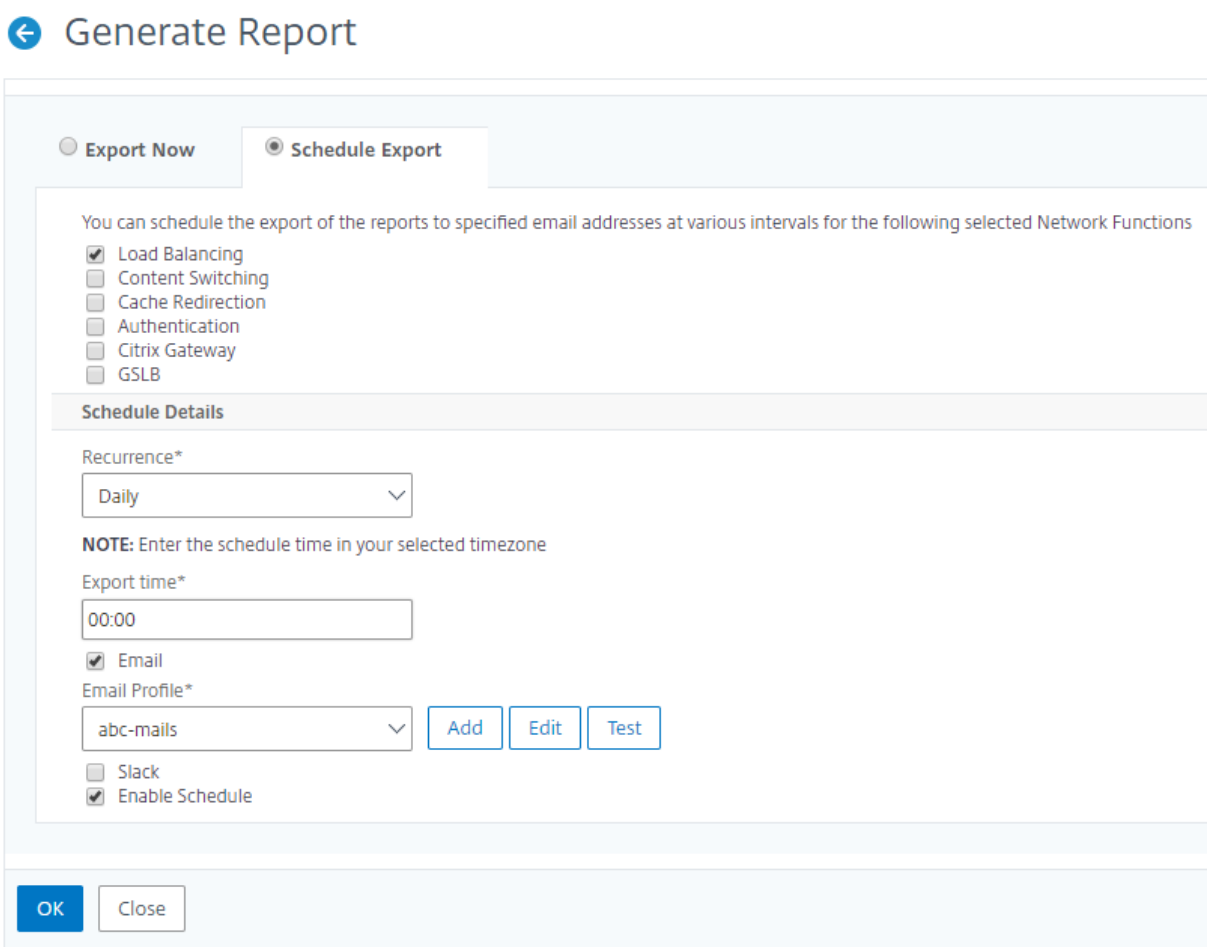
b) 选择“计划报告”选项卡，以计划定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

   i. 重复-从下拉列表框中选择“每日”、“每周”或“每月”。

   ii. 循环时间-以 24 小时格式输入时间为小时：分钟。

   iii. 电子邮件配置文件-从下拉列表框中选择一个配置文件，或单击 **+** 创建电子邮件配置文件。

单击 启用计划 以计划您的报告，然后单击 确定。通过单击“启用计划”复选框，您可以生成选定的报告。



网络报告

February 6, 2024

您可以通过监视 Citrix Application Delivery Management (ADM) 上的网络报告来优化资源使用。您可能有包含许多部署在多个位置的应用程序的分布式部署。为了确保应用程序的最佳性能，您还部署了多个 Citrix Application Delivery Controller (ADC) 实例来平衡负载、切换内容或压缩流量。网络性能会影响应用程序性能。要继续保持应用程序的性能，必须定期监视网络性能并确保所有资源均以最佳方式使用。

现在，Citrix ADM 不仅可以为全局级别的实例生成报告，还可以为虚拟服务器和网络接口等实体生成报告。实例系列由 Citrix ADC 和 SD-WAN 实例组成。您可以为其生成报告的虚拟服务器如下所示：

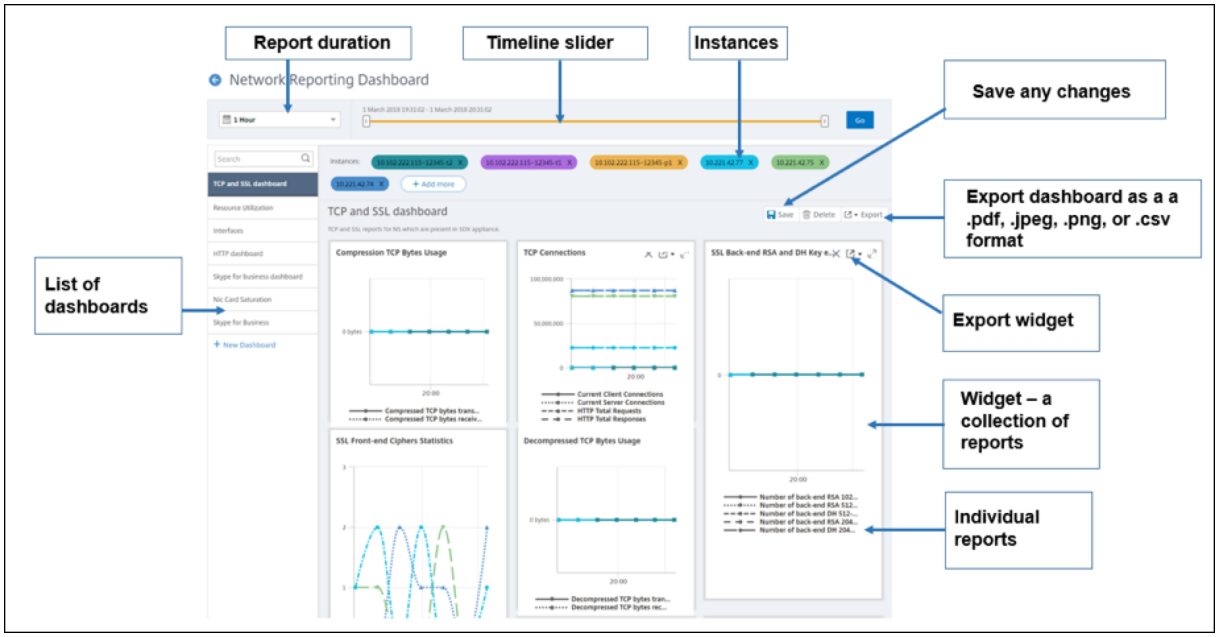
- 负载平衡服务器
- 内容交换服务器
- 缓存重定向
- 全局服务负载平衡 (GSLB)

- 身份验证
- Citrix Gateway

Citrix ADM 中的网络报告控制板是高度可定制的。现在，您可以为各种实例、虚拟服务器和其他实体创建多个控制板。

网络报告控制板

下图显示了控制板中的各种功能：

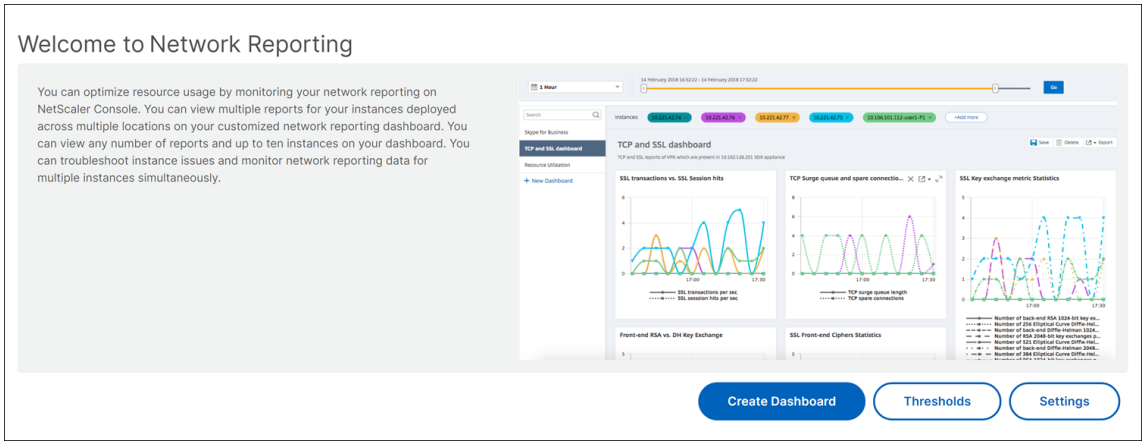


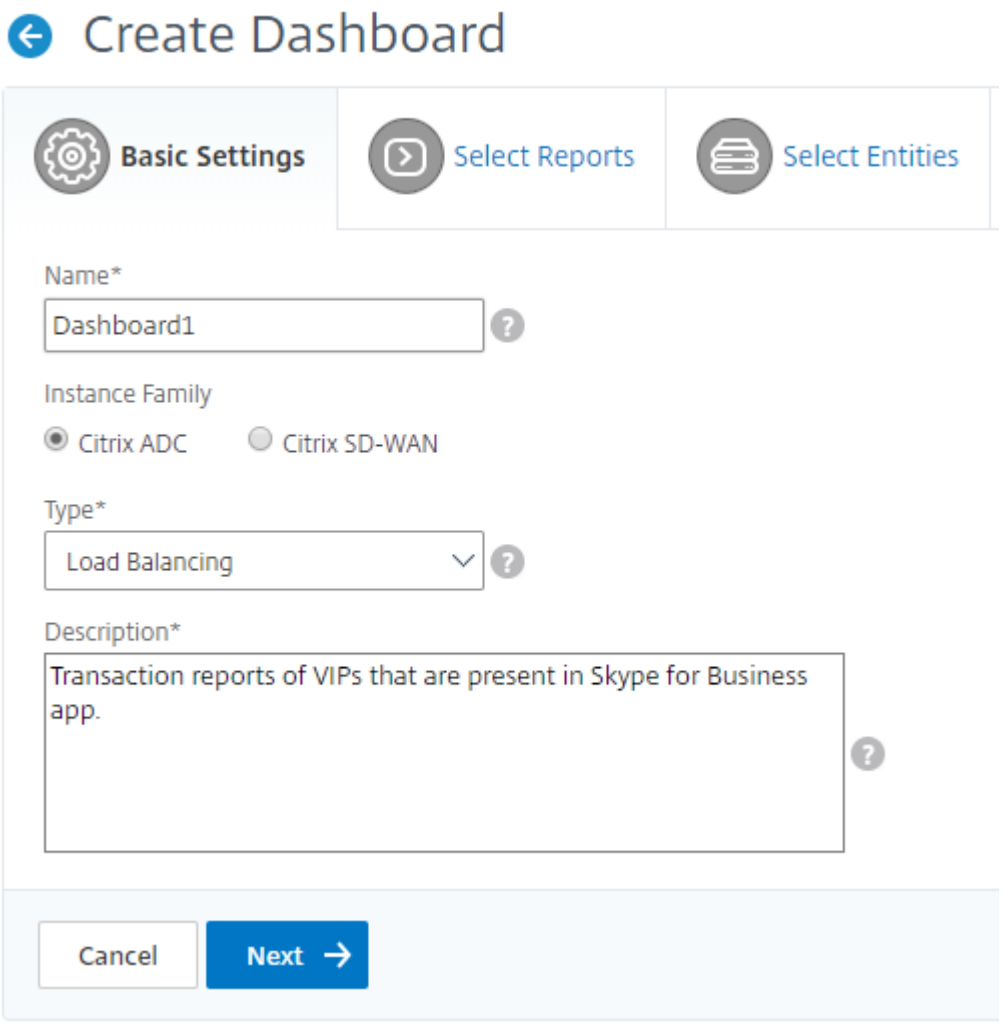
- 左侧面板列出了在 Citrix ADM 中创建的所有自定义控制板。您可以单击其中一个来查看控制板所包含的各种报告。例如，TCP 和 SSL 控制板包含与 TCP 和 SSL 协议相关的各种报告。
- 您可以使用多个控件自定义每个控制板，以显示各种报告。小组件表示控制板上的报表，即更多相关报表的集合。例如，压缩 TCP 字节使用情况报告包含每秒传输和接收的压缩 TCP 字节的报告。
- 您可以显示一小时、一天、一周或一个月的报告。此外，您现在可以使用时间轴滑块选项来自定义 Citrix ADM 上生成报告的持续时间。
- 您可以通过单击“X”删除报告。您也可以将报告导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。您还可以计划生成报告的时间和重复。您还可以配置应将报告发送到的电子邮件分发列表。
- 控制板顶部的“实例”部分列出了生成报告的所有实例的 IP 地址。
- 您可以通过单击“X”删除实例，也可以向报告添加更多实例。但是，目前 Citrix ADM 允许您查看十个实例的报告。
- 您还可以将整个控制板导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。必须保存对控制板所做的任何更改。单击保存保存更改。

以下部分详细介绍了创建控制板、生成报表和导出报表的任务。

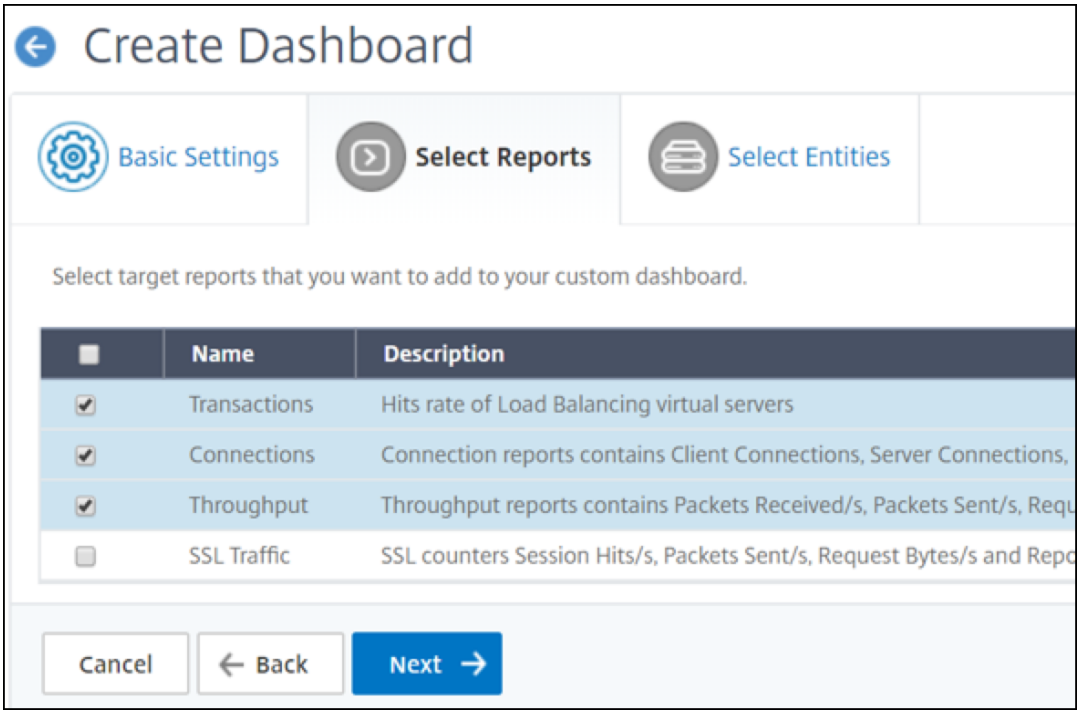
查看或创建控制板

1. 在 Citrix ADM 中，导航到“网 络”>“网络报告”。

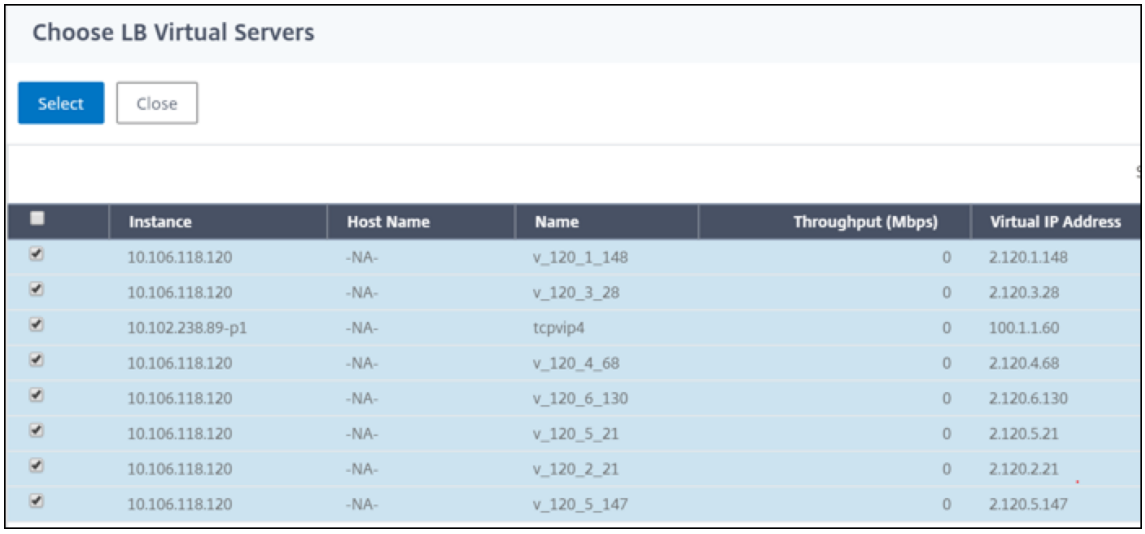




2. 在 选择报告 选项卡中，选择所需的报告。在此示例中，您可以选择事务、连接和吞吐量。单击下一步。
3. 要查看现有控制板，请单击 查看控制板。“网络报表仪表 板 页将打开，您可以在其中查看所有控制板和报表小组件。
4. 要创建控制板，请单击“创建控制板”。
5. “创建控制面板”页面打开。
6. 在“基本设置”选项卡中，输入以下详细信息：
    a) 名称。键入控制板的名称。
    b) 实例系列。选择实例类型-Citrix ADC 或 Citrix SD-WAN
    c) 类型。选择要为其生成报告的实体类型。在此示例中，选择负载平衡虚拟服务器。
    d) 说明。为控制板键入有意义的描述。
    e) 单击下一步。



7. 在“选择实体”选项卡中，单击“添加”。
8. 在滑动的“选择 **LB** 虚拟服务器”窗口中，选择任意数量的要监视的虚拟服务器。



> 注意
>
> 根据您在基本设置选项卡中选择的实体类型，实体选项卡将填充相应的实体。例如，如果您选择全局，则可以添加实例。

9. 单击“创建”。

将创建 **TCP** 和 **SSL** 控制面板，显示您选择的所有报告。

> 注意
>
> 目前，无法保存您对图例或筛选器所做的任何更改。

导出网络报告

虽然您可以以.pdf、.png、.jpeg 或.csv 格式导出小组件报告，但只能以.pdf、.jpeg 或.png 格式导出整个控制板。

> 注意
>
> 如果您具有只读权限，则无法在 Citrix ADM 中导出报告。您需要编辑权限才能在 Citrix ADM 中创建文件并导出该文件。

要导出控制板报告，请执行以下操作：

1. 导航到“网络”>“网络报告”
2. 单击 查看控制板 以查看您已创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，单击“控制板 **1**”。
4. 点击页面右上角的导出按钮。
5. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。

安排网络报告时，您可以通过在“主题”字段中输入文本字符串来自定义报告的标 题。在计划时间创建的报表将以此字符串作为其名称。

例如，对于来自特定虚拟服务器的网络报告，可以键入主题为“身份验证报告-10.106.118.120”，其中 10.106.118.120 是被监视虚拟服务器的 IP 地址。

> 注意
>
> 当前，此选项仅在您计划导出报告时可用。立即导出标题时，无法将标题添加到报表中。

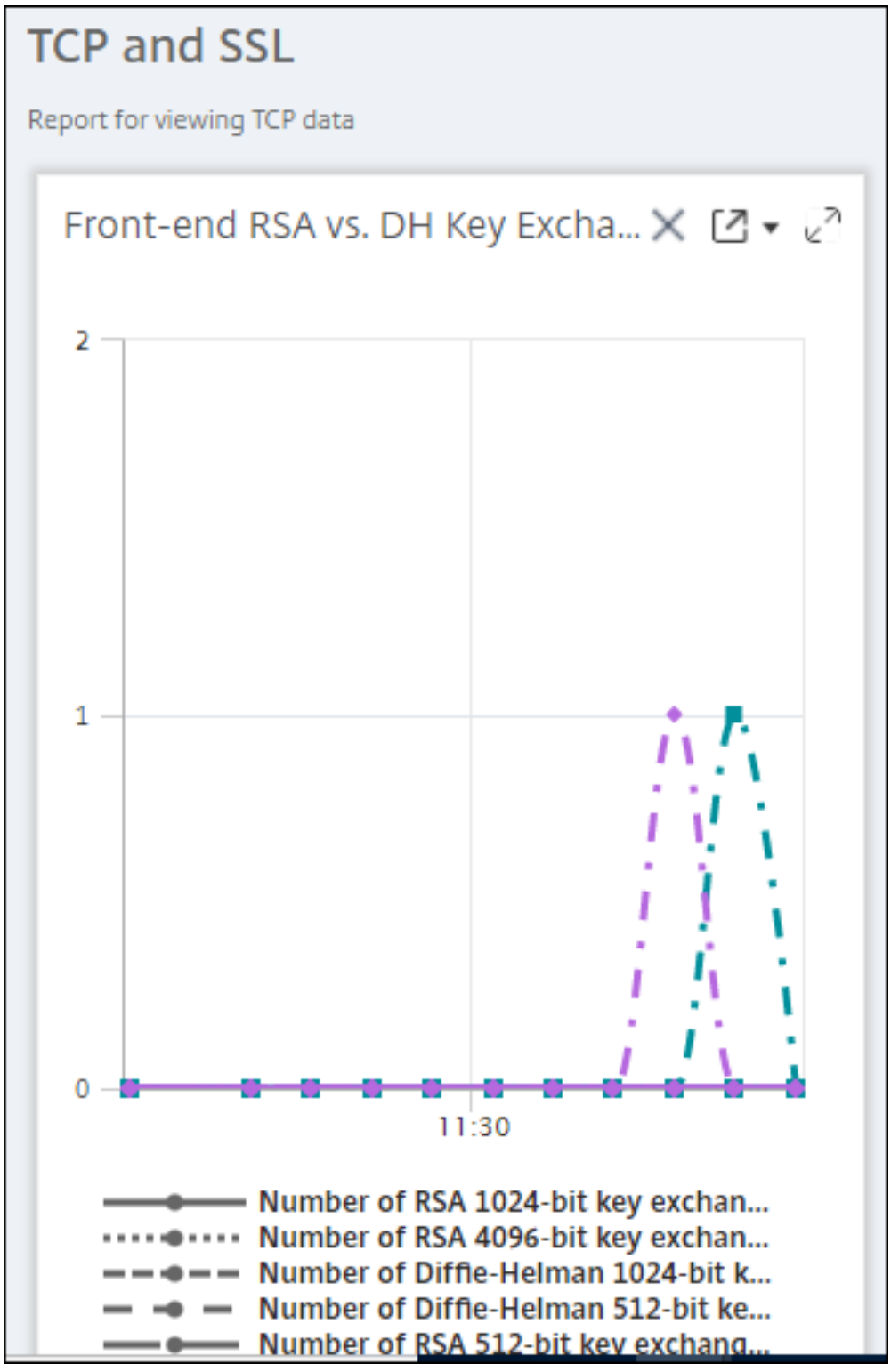
要导出控制板报告，请执行以下操作：

1. 导航到“网络”>“网络报告”
2. 单击 查看控制板 以查看您已创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，单击“控制板 **1**”。
4. 点击页面右上角的导出按钮。
5. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。**

要导出小组件报表，请执行以下操作：

1. 导航到网 络 > 网络报告。
2. 单击 查看控制板 以查看您已创建的所有控制板。

3. 在左窗格中，单击控制板。在此示例中，还单击 **TCP** 和 **SSL**。
4. 选择一个小组件。例如，选择前端 **RSA** 与 **DH** 密钥交换。
5. 单击页面右上角的导出按钮
6. 在“立即导出”选项卡下，选择所需的格式，然后单击“导出”。



如何在 **Citrix ADM** 上管理网络报告的阈值

要监视 Citrix ADC 实例的状态，可以在计数器上设置阈值并在超过阈值时接收通知。在 Citrix ADM 上，您可以配置阈值并查看、编辑和删除它们。

例如，当内容交换虚拟服务器的连接计数器达到指定值时，您可以收到电子邮件通知。您可以为特定实例类型定义阈值。您还可以从所选实例中选择要为特定计数器指标生成的报告。

当计数器的值超过或低于（由规则指定）阈值时，将生成具有指定严重性的事件以表示性能相关问题。计数器值恢复到您认为正常的值时，将清除事件。导航到“网络”>“事件”>“** 报告”可以查看这些 事件。在“报告”页面上，您可以单击“按严重性划 ** 分的事件”圆环以按严重性查看事件。

您还可以将操作与阈值关联，例如在超过阈值时发送电子邮件或 SMS 消息。

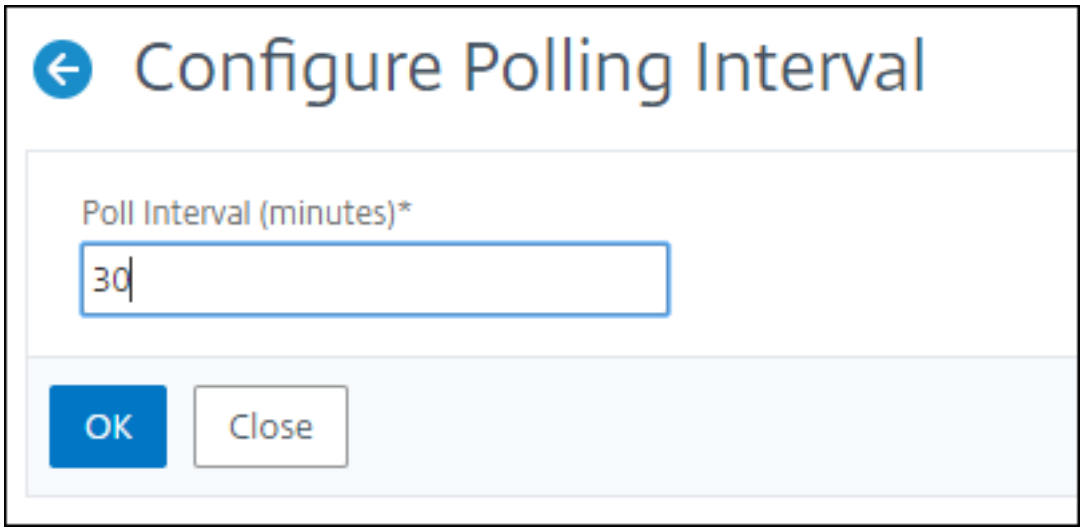
创建阈值

1. 在 Citrix ADM 中，导航到 网络 > 网络报告 > 阈值。在 **Thresholds**（阈值）下方单击 **Add**（添加）。
    1. 在“创建 阈值”页面上，指定以下详细信息：
        - 阈值名称。阈值的名称。
        - 实例类型。选择 Citrix ADC 或 Citrix SD-WAN WO。
        - 报告名称。提供有关此阈值的信息的性能报告的名称。
    2. 您还可以设置规则来指定何时生成或清除事件。您可以在“配置规则”部分下指定以下详细信息：
        - 指标。选择要为其设置阈值的指标。
        - 比较器。选择比较器以检查监视值是否大于或等于或小于或等于阈值。
        - 阈值。键入用于计算事件严重性的值。例如，您可能希望在当前客户端连接的监视值达到 80% 时生成事件严重性为严重的事件。在此情况下，键入 80 作为阈值。您可以导航到“网络”>“事件”>“报告”来查看“严重程度”事件。在“报告”页面上，您可以单击“按严重性划分的事件”圆环以按严重性查看事件。
        - 清除值。键入指示何时清除该值的值。例如，您可能希望在监视的值达到 50% 时清除当前客户端连接阈值。在此情况下，键入 50 作为清除值。
        - 事件严重性。选择要为阈值设置的安全级别。
    3. 选择要为其设置阈值的一个或多个实例的 IP 地址。
    4. 您还可以添加 事件消息。键入您希望在达到阈值时显示的消息。Citrix ADM 将监视值和阈值附加到此消息中。
    5. 选择启用启用阈值以生成警报。
    6. 或者，您可以配置诸如电子邮件和/或短信通知之类的 操作。
    7. 单击创建。

为网络报告设置性能轮询时间间隔

默认情况下，每 5 分钟 NITRO 调用收集一次性能数据用于网络报告。此操作检索实例统计信息（例如，计数器信息），并按每分钟、每小时、每天或每周对其进行汇总。可以在预定义的报告中查看此汇总数据。

要设置性能轮询间隔，请导航到“网 络”>“网络报告”，然后单击“配置轮询间隔”。轮询时间间隔不能低于 5 分钟，也不能超过 60 分钟。



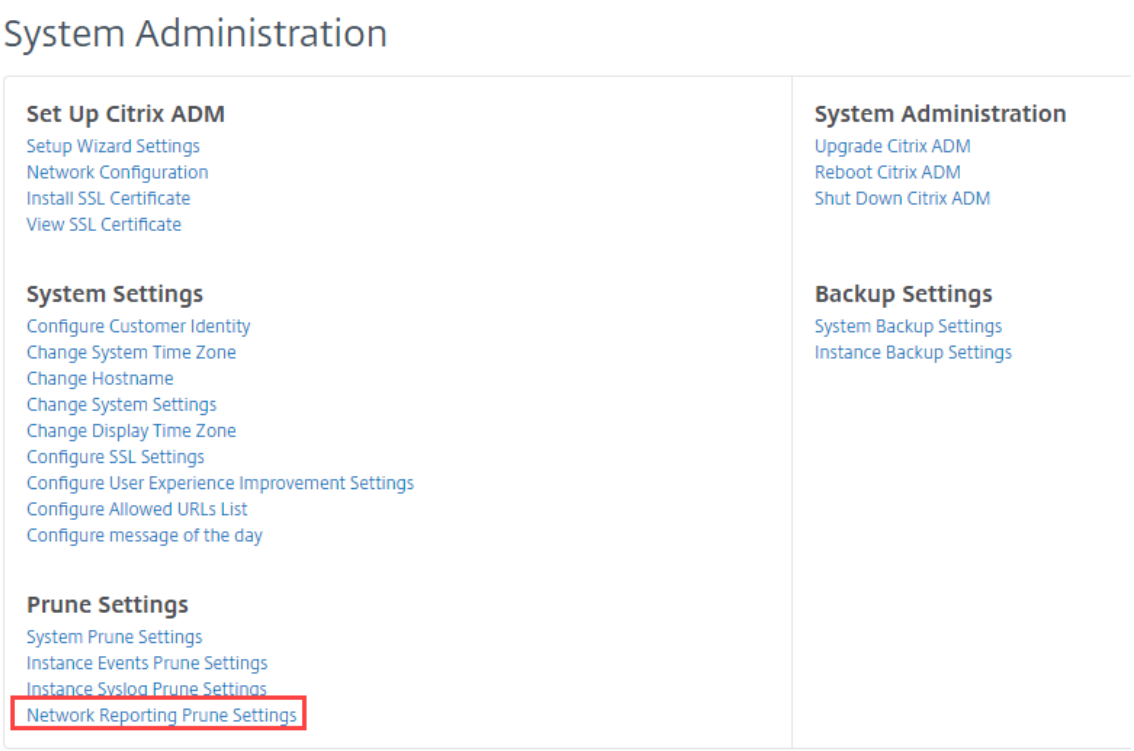
配置网络报告修剪设置

您可以在 Citrix ADM 中配置网络报告数据的清除间隔。这将限制存储在 Citrix ADM 服务器数据库中的网络报告数据量。默认情况下，每 24 小时（01.00 小时）对报告历史数据的网络进行修剪。

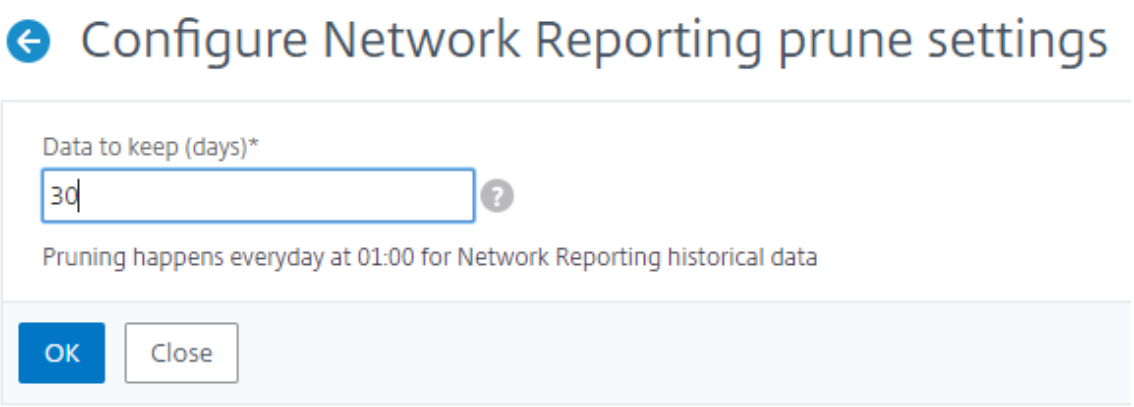
> 注意
>
> 您可以指定的值不能超过 90 天或小于 1 天。

要配置网络报告删除设置，请执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。在“删除设置”下，单击“网络报告删除设置”。



2. 在“配置网络报告删除设置”页面中，指定保留数据的天数，然后单击“** 确定”。



所有网络报告性能数据将在所选天数内保留在 Citrix ADM 数据库中。

分析

February 6, 2024

Citrix ADM 分析功能提供了一种简单且可扩展的方式来查看各种 Citrix ADC 见解，以分析和提高应用程序性能。您可以在 Citrix ADM 中使用一个分析功能或同时使用多个分析功能。

下表介绍了 Citrix ADM 支持的各种分析功能：

分析功能	说明
Web Insight	Web Insight 支持对企业 Web 应用程序的可见性，并允许您监视 Citrix ADC 中的所有 Web 应用程序。作为管理员，您可以看到对应用程序的集成和实时监视。
HDX Insight	HDX Insight 为通过 Citrix ADC 的 ICA 流量提供端到端的可见性。通过 HDX Insight，您可以查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。
Gateway Insight	通过 Gateway Insight 可以查看所有用户登录 Citrix Gateway 时遇到的失败，而无论访问模式为何。
Security Insight	Security Insight 提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。
SSL Insight	SSL Insight 提供对安全 Web 事务 (HTTPS) 的可见性，并允许您监视 Citrix ADC 中的所有安全 Web 应用程序。作为管理员，您可以看到对安全 Web 事务的集成、实时和历史监视。
TCP Insight	TCP Insight 提供了一种简单且可扩展的解决方案，用于监视 Citrix ADC 实例中使用的优化技术和拥堵控制策略（或算法）的指标，以避免在数据传输中发生网络拥堵。
Video Insight	Video Insight 功能提供了一种简单且可扩展的解决方案，用于监视 Citrix ADC 设备使用的视频优化技术的指标，以改进客户体验和提高操作效率。
WAN Insight	通过 WAN Insight 分析，管理员可以轻松监视数据中心与分支 WAN 优化设备之间传输的加速和未加速 WAN 流量。WAN Insight 还提供了网络上的客户端、应用程序和分支机构的可见性，以帮助有效地排除网络问题。

许可证要求

February 6, 2024

下表描述了 Citrix ADC 实例的许可要求，以便在 Citrix ADM 上查看各种分析报告：

Citrix ADM 分析功能	Citrix ADC 许可证要求
Web Insight	所有 Citrix ADC 许可版本 (Standard/Enterprise/Platinum). 均支持关于 Citrix ADM 的 Web Insight 报告。
HDX Insight	以下 Citrix ADC 许可均支持关于 Citrix ADM 的 HDX Insight 报告：Enterprise Edition（用于报告 < 1 小时）或 Platinum Edition（用于无限量报告）。注意 不支持标准许可证版本。
Security Insight	持有 App Firewall 许可的 Platinum Edition 或 Enterprise Edition 支持关于 Citrix ADM 的 Security Insight 报告。注意 不支持标准许可证版本和独立应用防火墙许可证。
SSL Insight	所有 Citrix ADC 许可版本 (Standard/Enterprise/Platinum) 均支持 Citrix ADM 上的 SSL Insight 报告。
Gateway Insight	以下 Citrix ADC 许可均支持关于 Citrix ADM 的 Gateway Insight 报告：Enterprise Edition（用于报告 < 1 小时）或 Platinum Edition（用于无限量报告）。注意 不支持标准许可证版本。
TCP Insight	所有 Citrix ADC 许可版本 (Standard/Enterprise/Platinum) 均支持 TCP Insight 报告。
Video Insight	Citrix ADM 的 Video Insight 报告受到 Citrix ADC Premium（VPX-T 1000 系列，VPX-T）支持。
WAN Insight	Citrix SD-WAN WO Edition（广域网优化版）支持 Citrix ADM 的 WAN Insight 报告。

Logstream 概述

February 6, 2024

Citrix ADC 实例生成 AppFlow 记录，是数据中心所有应用程序流量的中心控制点。IPFIX 和 Logstream 是将这些 AppFlow 记录从 Citrix ADC 实例传输到 Citrix ADM 的协议。有关详细信息，请参阅 AppFlow。

- IPFIX 是 RFC 5101 中定义的一个打开式互联网工程任务组 (IETF) 标准。IPFIX 使用 UDP 协议，这是不可靠的传输协议，用于在一个方向上的数据流。由于 IPFIX 使用 UDP 协议，因此遵守 IPFIX 标准会在 Citrix ADM 中处理更多资源。

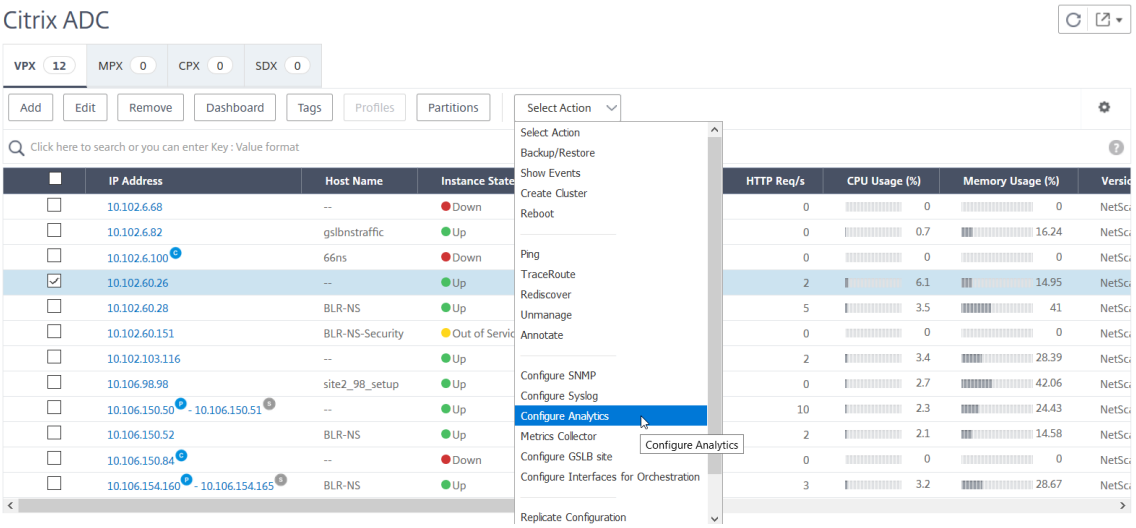
- Logstream 是 Citrix 拥有的协议，用作将分析日志数据从 Citrix ADC 实例高效传输到 Citrix ADM 的传输模式之一。Logstream 使用可靠的 TCP 协议，处理数据所需的资源较少。

对于 11.1 版本 **47.14** 和 **11.1** 版本 **62.8** 之间的 Citrix ADC，Logstream 是启用 Web 见解 (HTTP) 的默认传输模式，IPFIX 是启用其他见解的唯一传输模式。对于从 **12.0** 到最新版本的 Citrix ADC 版本，您可以选择 Logstream 或 IPFIX 作为传输模式。

> 注意
>
> Citrix ADM 版本和内部版本应 等于或高 于 Citrix ADC 版本和内部版本。例如，如果您安装了 Citrix ADC 12.1 版本 50.28/50.31 或更早版本，请确保您已安装了 Citrix ADM 12.1 版本 50.39。

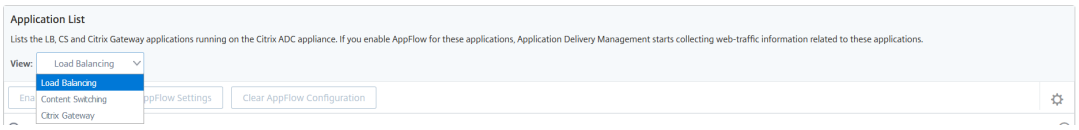
要在 **Citrix ADM** 上启用分析时使用 **Logstream** 作为通信模式，请执行以下操作：

1. 导航到网络 > 实例 > **Citrix ADC**，然后选择要在其上启用分析的 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。

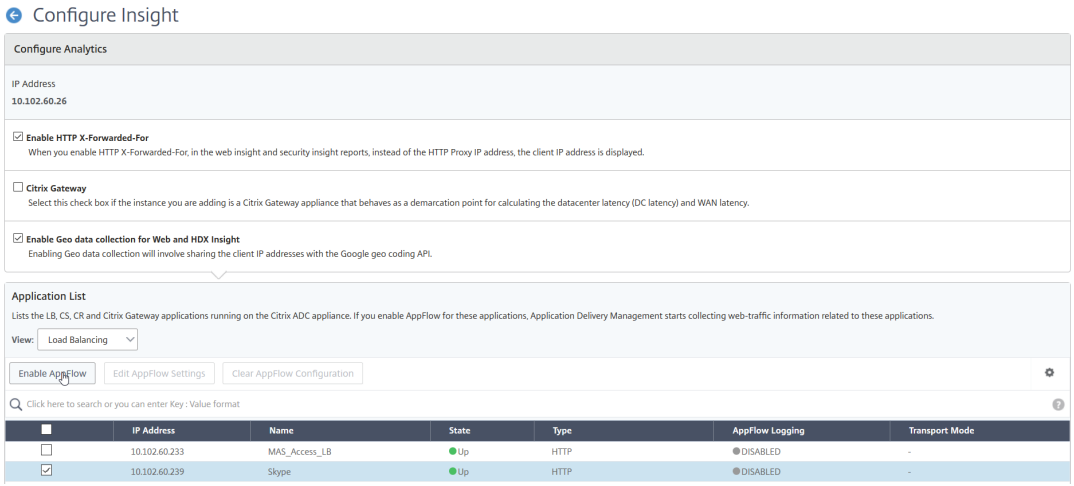


3. 在“配置智能分析”页上：

   a) 为负载平衡或内容切换选择 应用程序列表。



   b) 选择虚拟服务器，然后单击 启用 **AppFlow**。

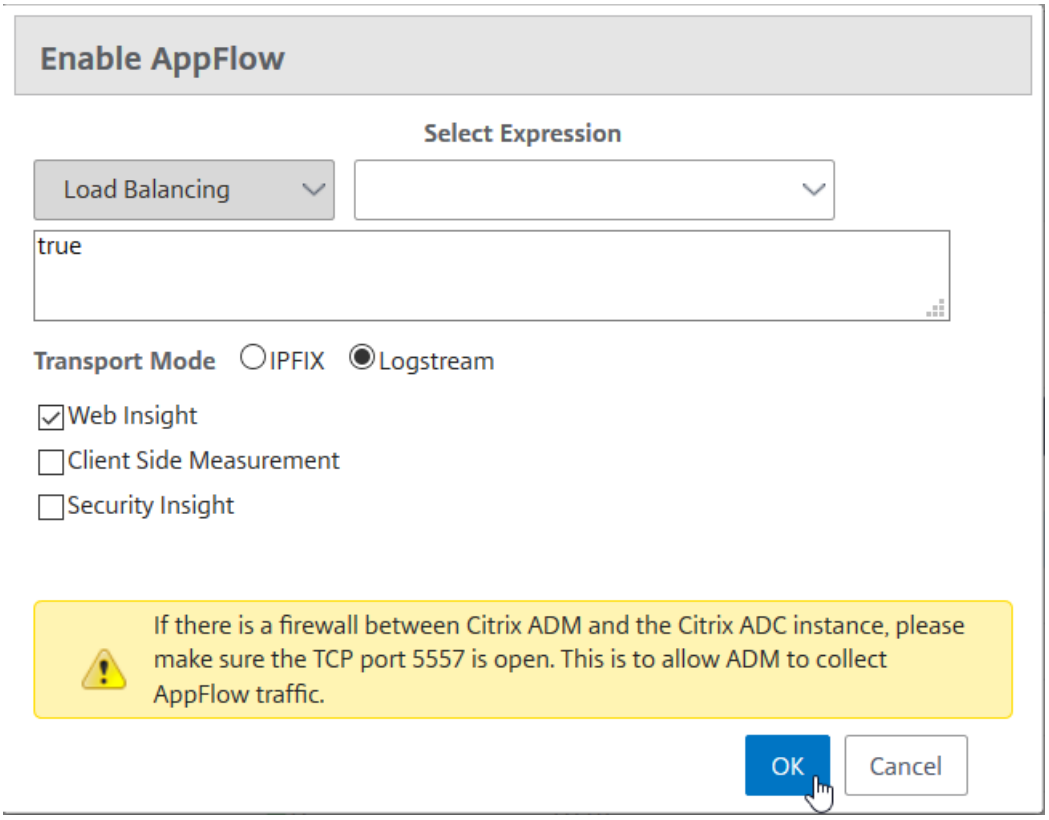


4. 在“启用 AppFlow”对话框中：

   - 在文本框中输入 **true**
   - 选择 **Logstream** 作为传输模式

     > 注意
     >
     > Citrix 建议您选择 Logstream 作为传输模式。

   - 选择洞察类型，然后单击“确定”。



下表描述了支持 Logstream 作为传输 模式的 Citrix ADM 的功能：

功能	IPFIX	Logstream
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

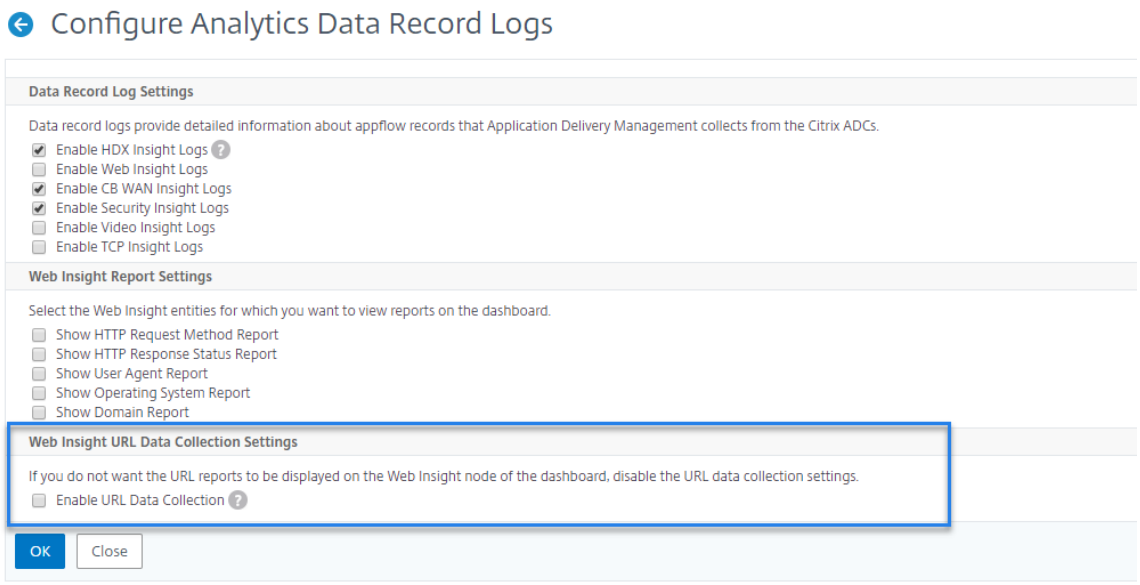
禁用 **URL** 数据收集

February 6, 2024

如果您不希望在 Citrix Application Delivery Management (ADM) 中控制板的 Web 智能分析节点上显示 URL 报告，则可以禁用 URL 数据收集。

禁用来自 **Citrix ADM** 的 **URL** 数据收集的步骤

1. 在 Citrix ADM 中，导航到“分析”>“设置”，然后单击“配置分析数据记录日志”。
2. 在 **Web Insight URL Data Collection Settings**（Web 洞察 URL 数据收集设置）部分，如果 **Enable URL Data Collection**（启用 URL 数据收集）选项已选中，请清除该复选框。
3. 单击确定。



创建阈值和警报

February 6, 2024

您可以设置阈值和警报来监视 Citrix ADC 实例的状态。可以设置计数器阈值以及监视实例和托管实例上的实体。

当计数器的值超过阈值时，Citrix Application Delivery Management (ADM) 会生成一个事件来表示与性能相关的问题。如果计数器值符合在阈值中指定的清除值，即会清除事件，这意味着特定阈值已回到其正常状态。

还可以为阈值关联操作。操作包括发送警报、电子邮件或 SMS 通知。当超过阈值时，Citrix ADM 会自动执行您定义的操作，例如启用警报和发送电子邮件或 SMS 通知。

使用 **Citrix ADM** 创建阈值和警报

1. 在 Citrix ADM 中，导航到分析 > 设置 > 阈值。在 **Thresholds**（阈值）下方单击 **Add**（添加）。
2. 在“创建阈值”页上，指定以下详细信息：
   - **Name**（名称）- 用于配置阈值的名称。
   - 流量类型 -要为其配置阈值的流量类型。
   - **Entity**（实体）- 要为其配置阈值的类别或资源类型。
   - **Reference Key**（引用键）- 根据选择的流量类型和实体自动生成的值。

- **Duration**（持续时间）- 要为其配置阈值的时间间隔。
- 配置规 则—要为其配置阈值的度量的规则。
- 通知设置 -启用阈值并在超过阈值时通过各种渠道（如电子邮件、松弛或短信）接收通知。

3. 单击创建。

对于 HDX Insight，还可以设置多个阈值，以便仅当违反了配置的阈值中的所有实体时才生成警报。

配置自适应阈值

February 6, 2024

自适应阈值功能为每个 URL 的最大命中数设置阈值。如果 URL 的最大命中数大于为该 URL 设置的阈值，则会向外部 syslog 服务器发送 syslog 消息。阈值时间间隔可以是天或周。

阈值计算方式如下：

阈值 = 最大命中次数 ***** 阈值乘数

其中：

- 最大命中数是 URL 的最大命中数。
- 阈值系数是您定义的整数值（默认值：2）。

使用 **Citrix ADM** 创建自适应阈值

1. 在 Citrix ADM 中，导航到分析 > 设置 > 自适应阈值，然后单击“添加”。
2. 在“自适应阈值”页面上，指定以下参数：
   - **Name**（名称）- 阈值名称
   - **Entity**（实体）- URL
   - **Duration**（持续时间）- 阈值的持续时间（天或周）
   - 阈值乘 数-用户定义的整数，该整数与指定 URL 的最大命中计数相乘，以获取 URL 的自适应阈值。

配置数据库持久性

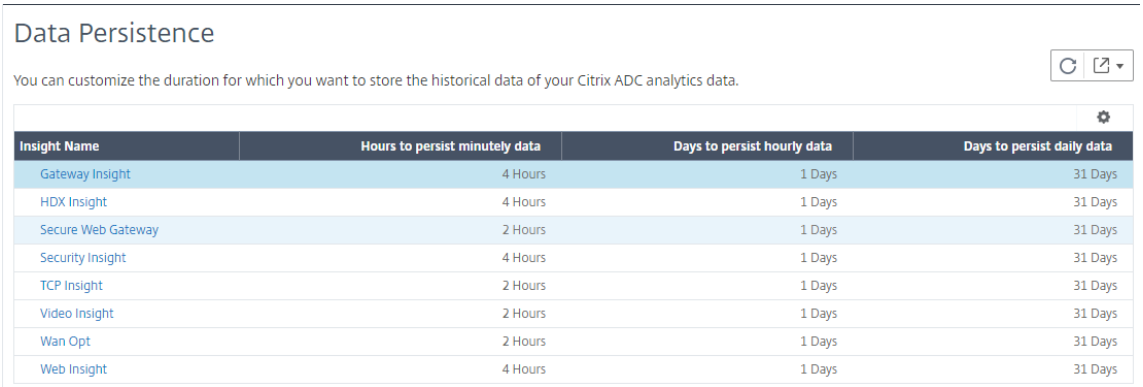
February 6, 2024

在 Citrix Application Delivery Management (ADM) 中配置数据库持久性允许您自定义要存储 Citrix ADC 分析数据的历史数据的持续时间。您可以为分析的历史数据选择以下数据库持久性类型：

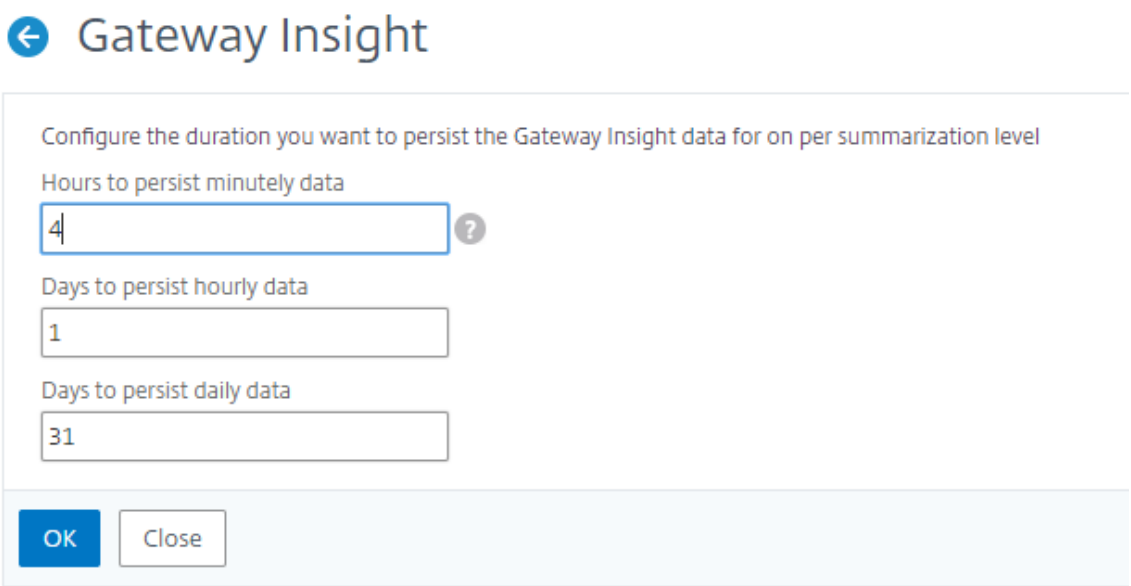
- Hours to persist minutely data（保持每分钟数据的小时数）
- Days to persist hourly data（保持每小时数据的天数）
- Days to persist daily data（保持每日数据的天数）

配置数据库持久性

1. 导航到 > 分析 > 设置 > 数据库持久性。
2. 单击要配置数据库持久性的 Insight 类型。



3. 指定要在 Citrix ADM 上保留智能分析数据的持续时间。例如，对于 Gateway Insight，可以将分析的每分钟历史数据存储 2 小时，或将每小时数据存储 1 天。



针对分析的自助诊断

February 6, 2024

Citrix Application Delivery Management (ADM) 执行自助诊断，以确定托管实例上的许可证和配置问题，以满足以下分析功能：

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- Secure Web Gateway 分析

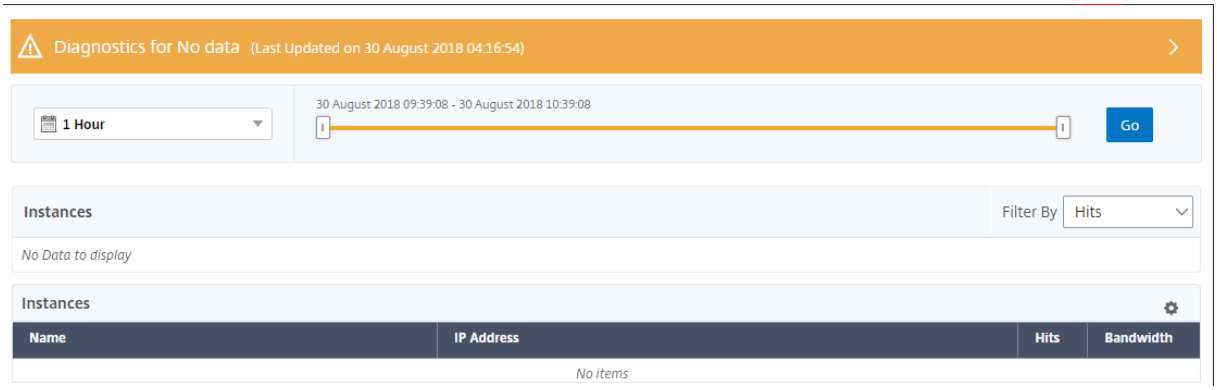
自助诊断程序每 12 小时运行一次，如果发现每个指定分析功能的问题，则会生成一份诊断报告。诊断报告提供了问题的来源、问题类型以及解决问题的纠正措施。自助诊断可帮助您更快地识别和解决问题。

例如，如果 AppFlow 策略未绑定到虚拟服务器或虚拟服务器未获得许可，则 Citrix ADM 将无法获得 Web Insight 监视所需的数据。自助诊断可识别问题并生成诊断报告。您可以查看诊断报告以检查问题并执行纠正措施。

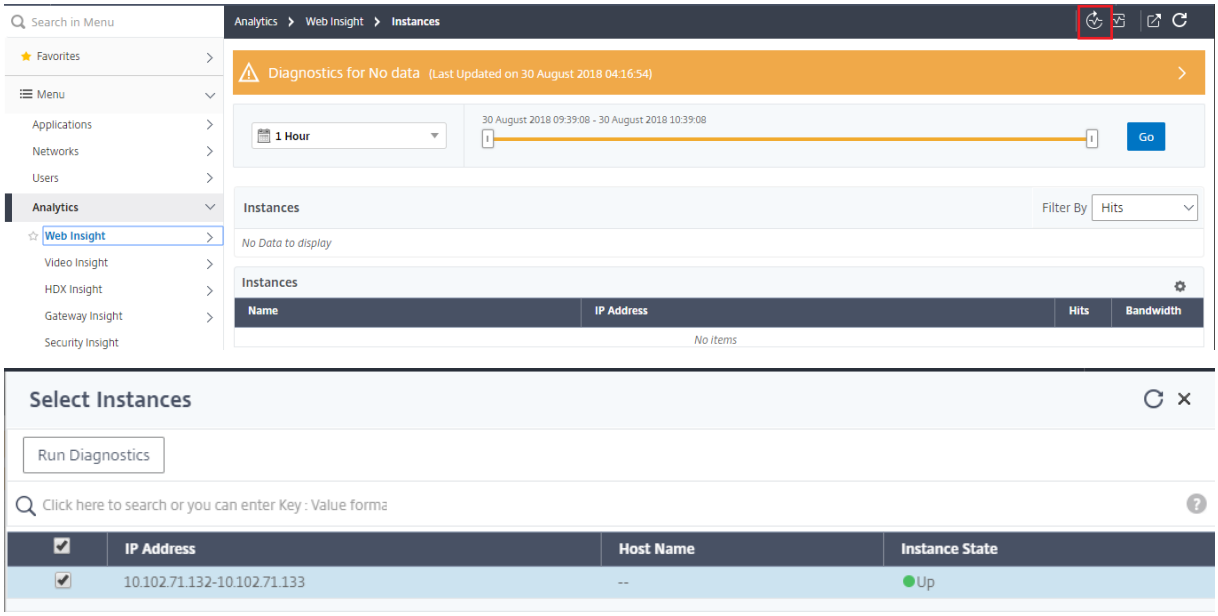
查看诊断报告

要查看指定分析功能的诊断报告，您需要转到 Citrix ADM 控制板中的相应分析节点。

例如，要查看 Web 智能分析的诊断报告，请导航到“分析”**>**“**Web** 智能分析”。在“Web Insight”页面上，选择“显示诊断”图标。



如果要检查问题，也可以运行即时诊断程序。单击“运行诊断”。选择实例并选择 运行诊断程序。



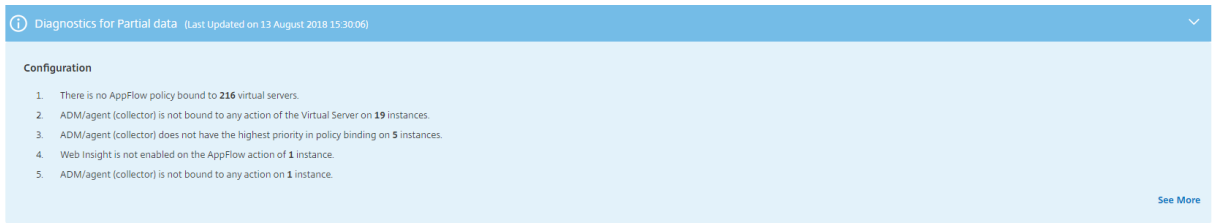
分析诊断报告

自助诊断根据问题的严重程度以橙色或蓝色背景显示诊断报告。

橙色背景的诊断报告表示比蓝色背景更严重。

例如，在您的 Citrix ADC 实例上配置了五台虚拟服务器。如果您尚未在任何虚拟服务器上启用 AppFlow 参数，则 Citrix ADM 不会收到用于分析的 Web Insight 和 Security Insight 流量。自助诊断程序将配置问题确定为严重问题。您可以在 Web Insight 和 Security Insight 功能中看到橙色背景诊断报告。

如果您在其中一台虚拟服务器上启用了 AppFlow，则 Citrix ADM 会收到数据进行分析。您可以在蓝色背景下看到诊断报告，因为至少有一个虚拟服务器正在发送流量进行分析。

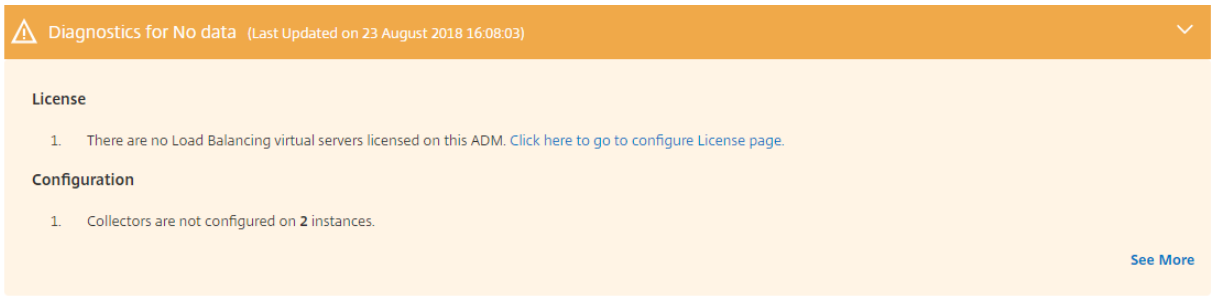


> 重要：自助诊断程序不检查流量。它只检查与托管实例上的指定分析功能相关联的许可证或配置问题。有时，您看不到任何分析数据，因为没有活动流量流经虚拟服务器。

诊断报告包含摘要页面和详细信息页面。

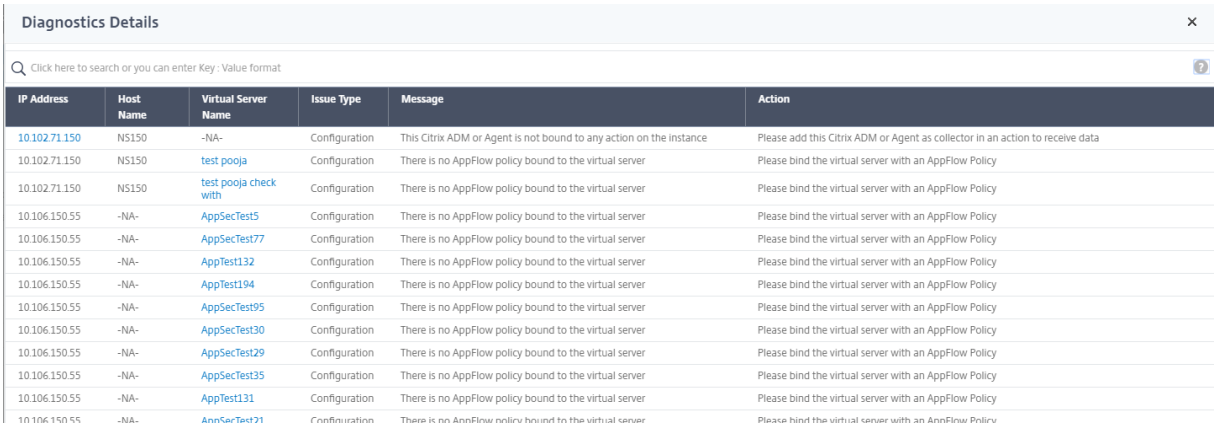
摘要页面概述了问题类型（许可证或配置）。该页面可能包含指向相关配置页的超链接。

例如，如果 Citrix ADM 上没有许可的负载平衡虚拟服务器，则摘要页面将提供一个超链接，用于指向“系统许可证”页面。



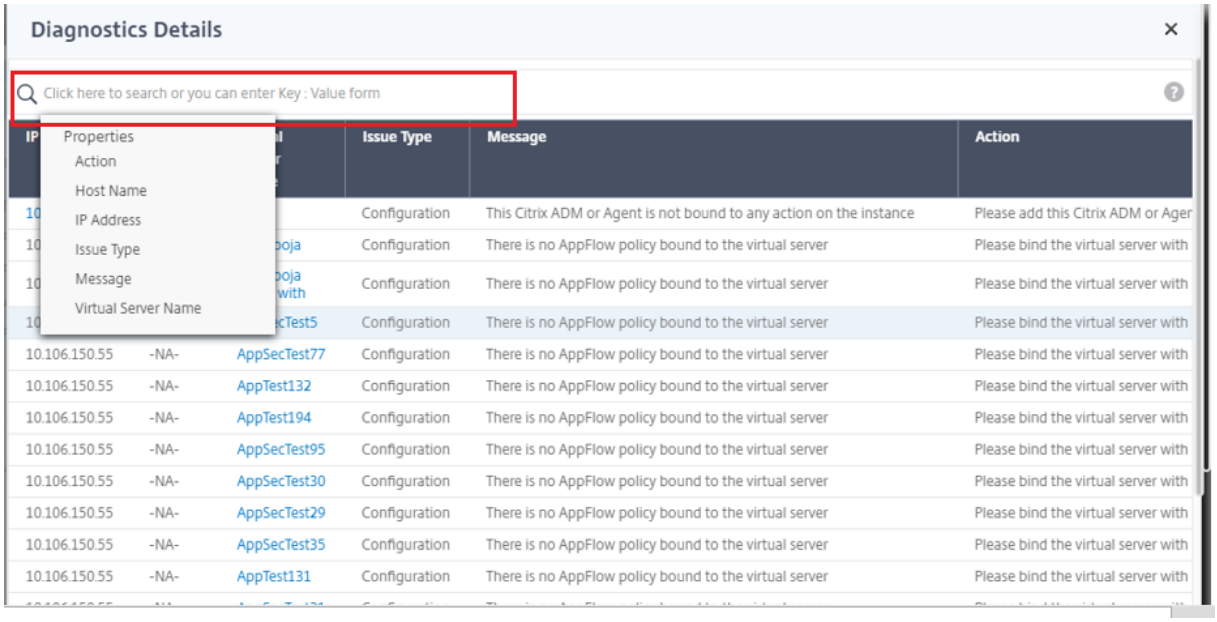
要查看有关问题的详细信息，请单击摘要页面上的查看详 细信息。

详细信息页面提供有关问题的完整信息，并建议您需要执行的操作。您可以单击针对每个问题的超链接来配置托管实例或虚拟服务器。



IP Address	Host Name	Virtual Server Name	Issue Type	Message	Action
10.102.71.150	NS150	-NA-	Configuration	This Citrix ADM or Agent is not bound to any action on the instance	Please add this Citrix ADM or Agent as collector in an action to receive data
10.102.71.150	NS150	test pooja	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.102.71.150	NS150	test pooja check with	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest5	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest77	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest132	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest194	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest95	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest30	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest29	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest35	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppTest131	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy
10.106.150.55	-NA-	AppSecTest21	Configuration	There is no AppFlow policy bound to the virtual server	Please bind the virtual server with an AppFlow Policy

您还可以根据操作、主机名、IP 地址和问题类型等搜索问题。



解决问题后，您需要运行即时诊断以生成最新的诊断报告。

Web Insight

February 6, 2024

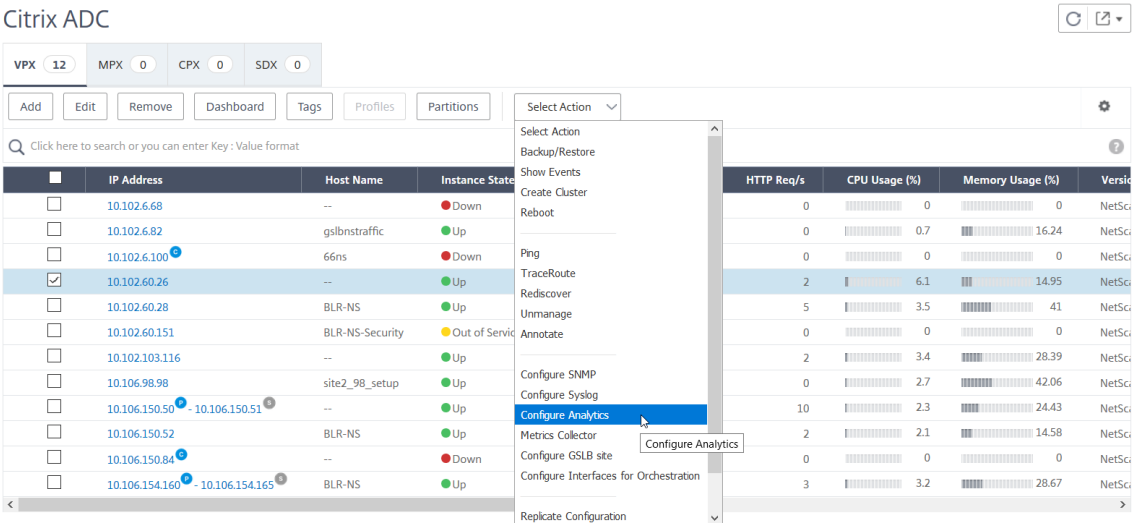
通过 Web Insight，管理员可以监视 Citrix ADC 实例提供的所有 Web 应用程序。作为管理员，您可以从 Citrix ADC 实例获得对应用程序的集成实时监视。Web Insight 提供客户端网络延迟和服务器响应时间等关键信息，确保监视和改善应用性能。从 Citrix ADC 实例处理的每个 HTTP HTTPS 事务捕获用于分析的数据。分析数据使您能够分析环境中 Citrix ADC 实例、应用程序、URL、客户端和服务器的性能。

以下是您可以使用 Web 智能分析查看数据的一些使用案例：

- 访问 SharePoint 等应用程序时遇到高延迟的客户端列表
- 一个小时内点击最多的顶级应用程序
- 从客户端访问的应用程序和 URL 列表
- 特定客户端使用的操作系统和浏览器
- 发送错误相关响应最多的应用程序或服务器
- 一个特定客户端的可访问性问题
- 来自特定客户端的少数或所有应用程序的可访问性问题
- 从特定客户端和后端服务器，应用程序的几页很慢
- 从特定客户端和后端服务器访问应用程序时速度很慢

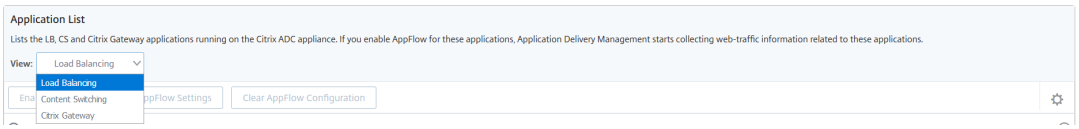
您可以为选定实例上的特定虚拟服务器启用 Web Insight，以监视 Web 应用程序上的流量。然后，Web 见解功能提供 Citrix ADM 中虚拟服务器的统计信息。要启用 Web 见解功能，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到网络 > 实例 > **Citrix ADC**，然后选择要在其上启用分析的 Citrix ADC 实例。
3. 从选择操作列表中，选择配置分析。

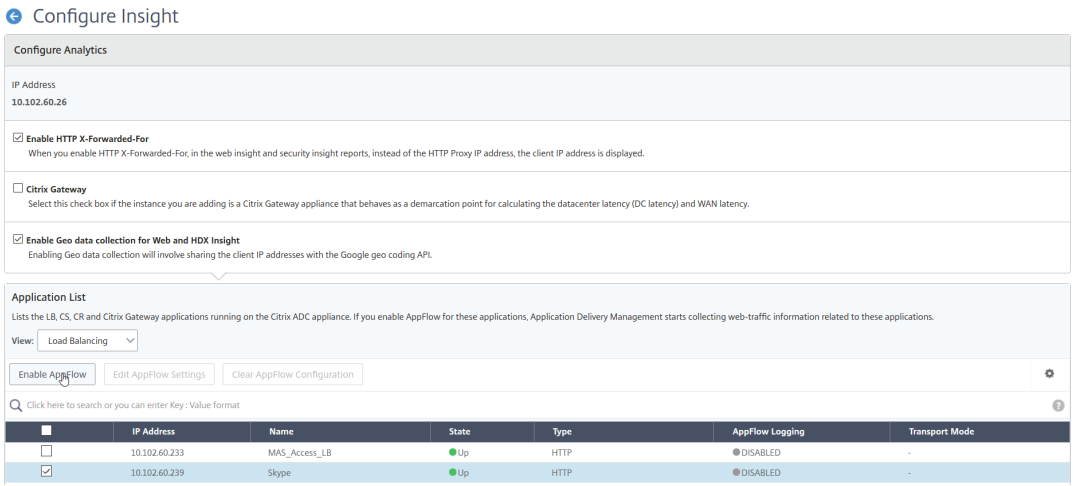


4. 在“配置智能分析”页上：

   a) 为负载平衡或内容切换选择 应用程序列表。



   b) 选择虚拟服务器，然后单击 启用 **AppFlow**。

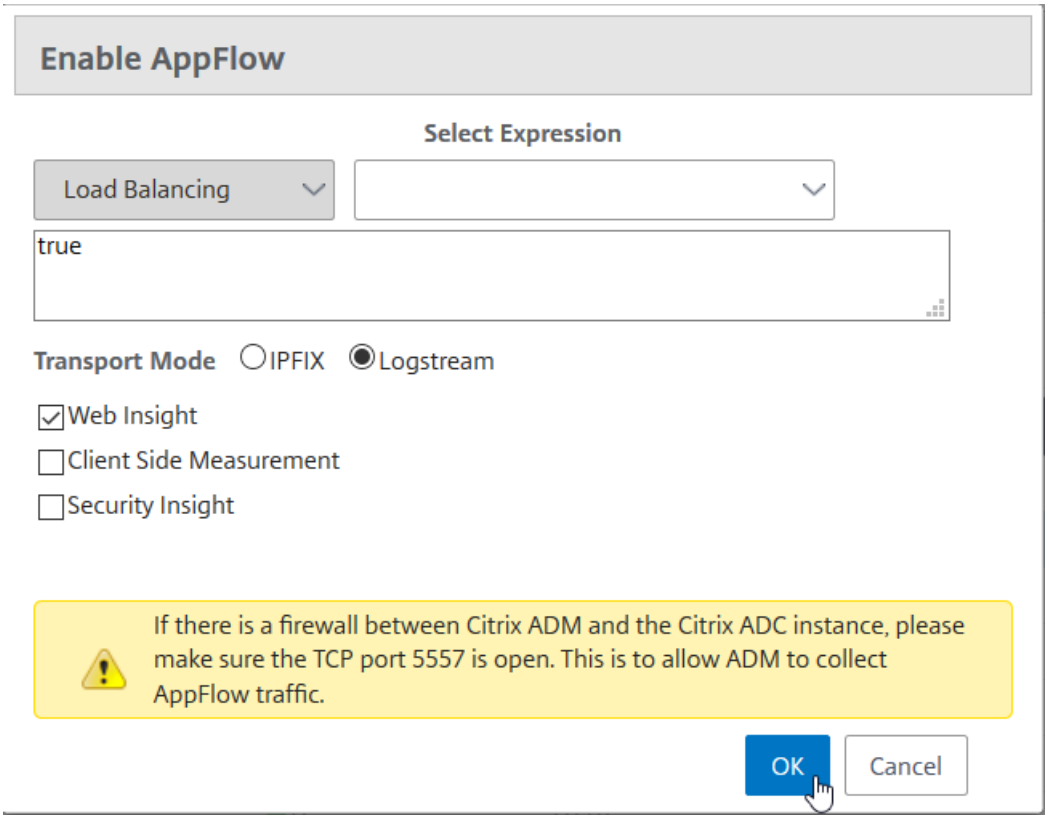


5. 在“启用 AppFlow”对话框中：

- 在文本框中输入 **true**
- 选择 **Logstream** 作为传输模式

> 注意：Citrix 建议您选择 Logstream 作为传输模式。

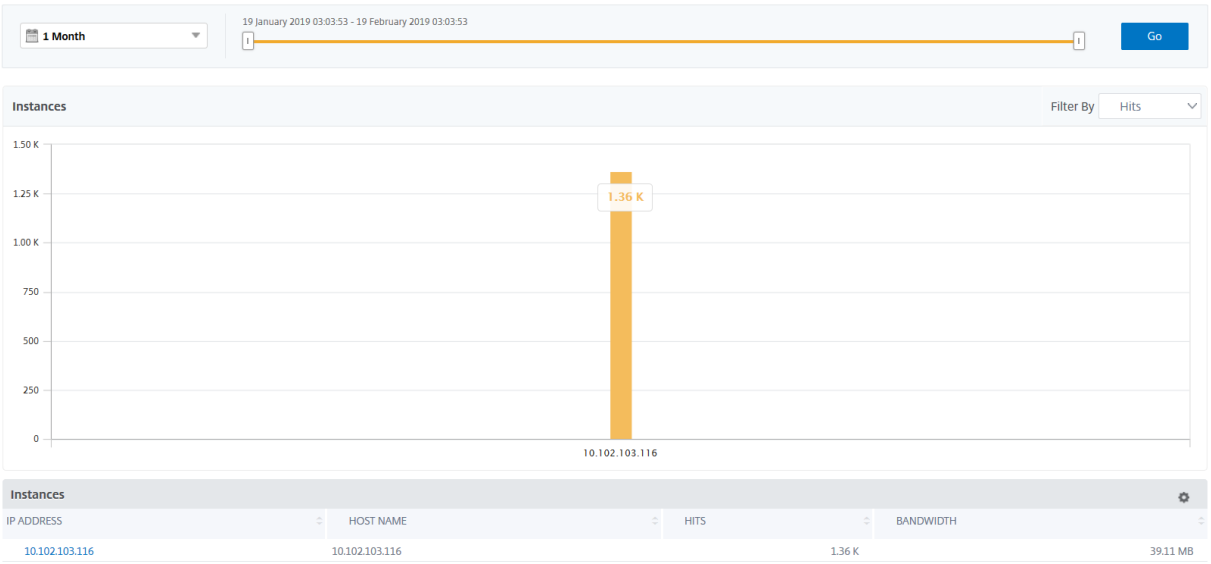
- 选择“**Web** 智能分析”，然后单击“确定”。



分析 **Web** 应用程序问题

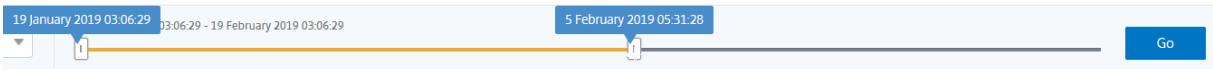
管理员需要识别的常见问题之一是延迟问题。作为管理员，您需要查找延迟问题是来自服务器网络、客户端网络还是服务器响应时间。使用 Citrix ADM，您可以通过导航到分析 > **Web Insight** 来识别这些信息。

导航到分析 > **Web Insight** 时，它会显示通过 Web 智能分析启用的 Citrix ADC 实例。您可以查看实例的详细信息，例如 IP 地址、主机名、总点击次数和带宽。



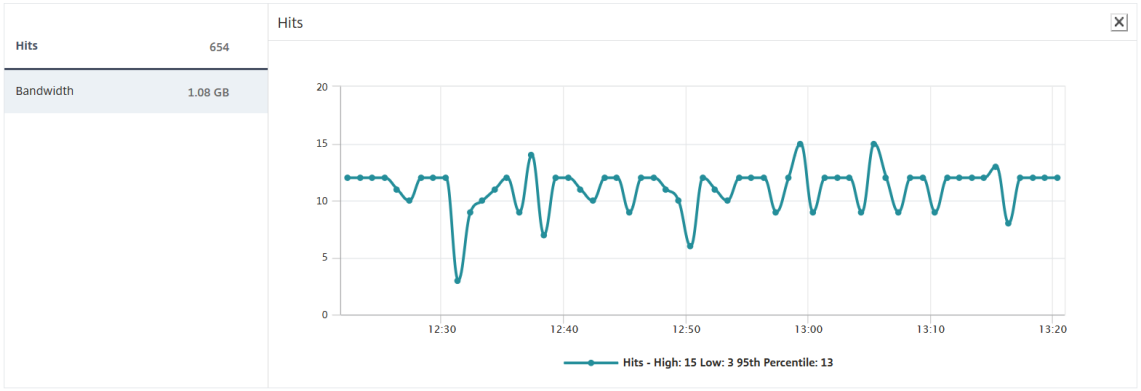
使用列表，您可以选择时间持续时间以查看实例的见解。

您还可以使用滑块自定义时间持续时间，然后单击 转到 以显示结果。

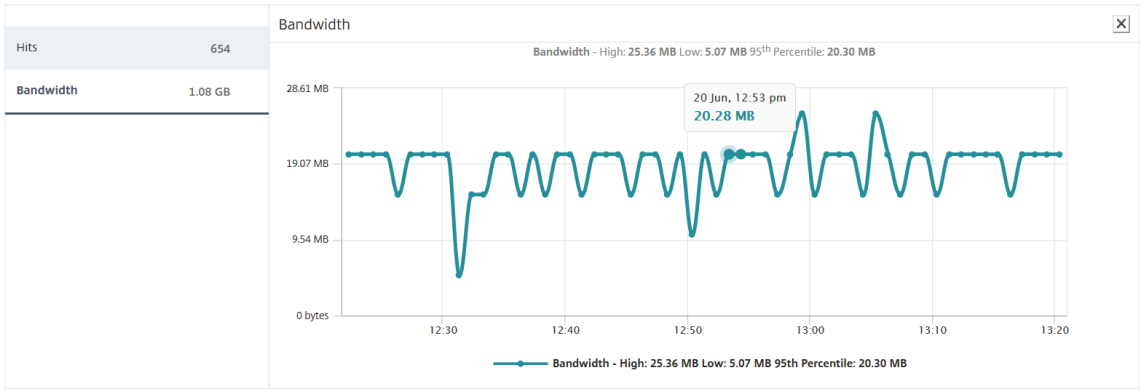


当您单击实例的图形或 IP 地址时，将显示有关实例的详细信息。您可以查看以下内容的见解：

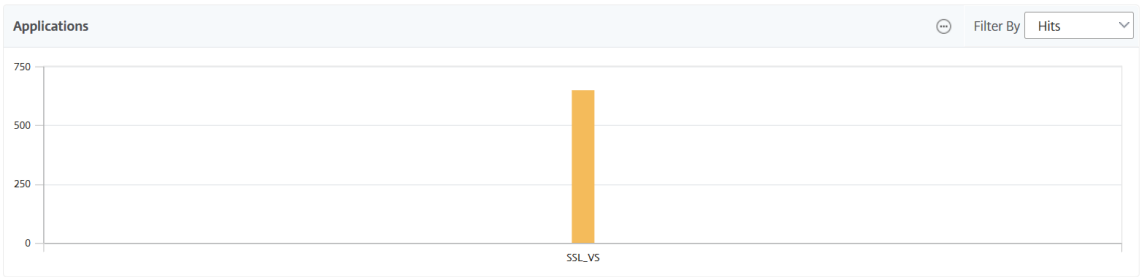
- 点击总数



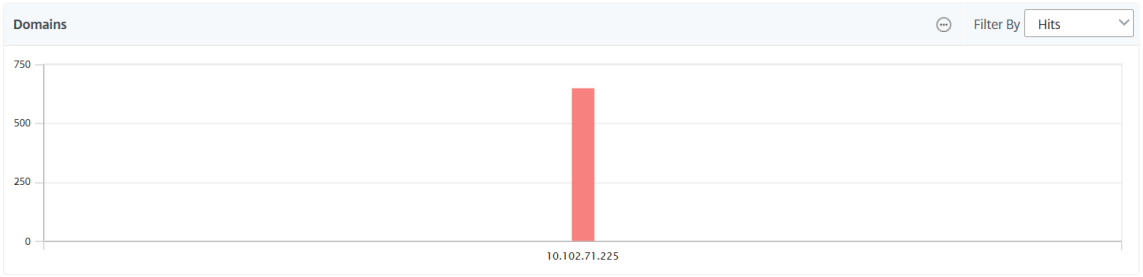
- 带宽



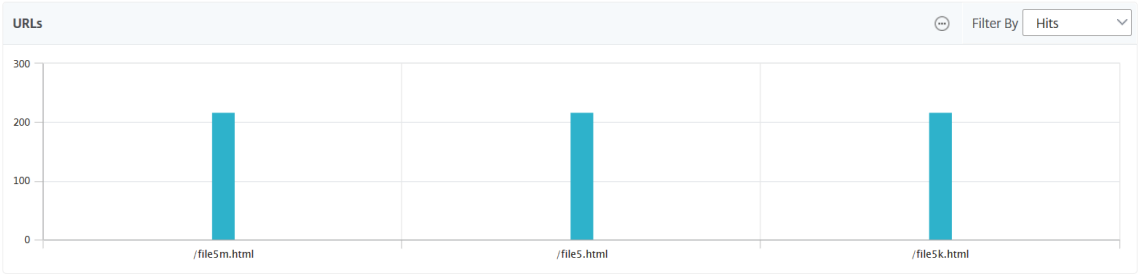
- 应用程序



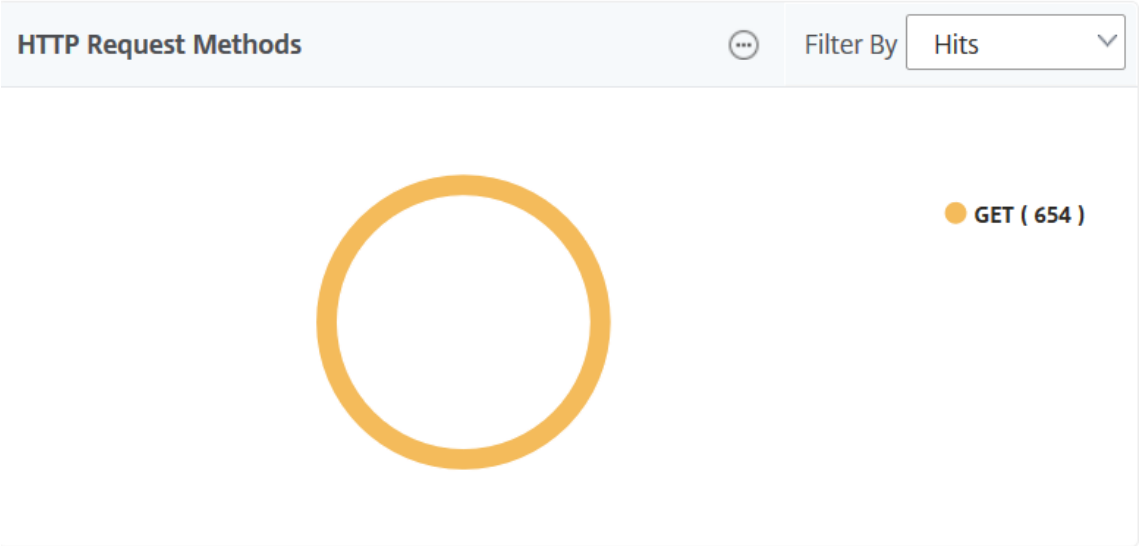
- 域



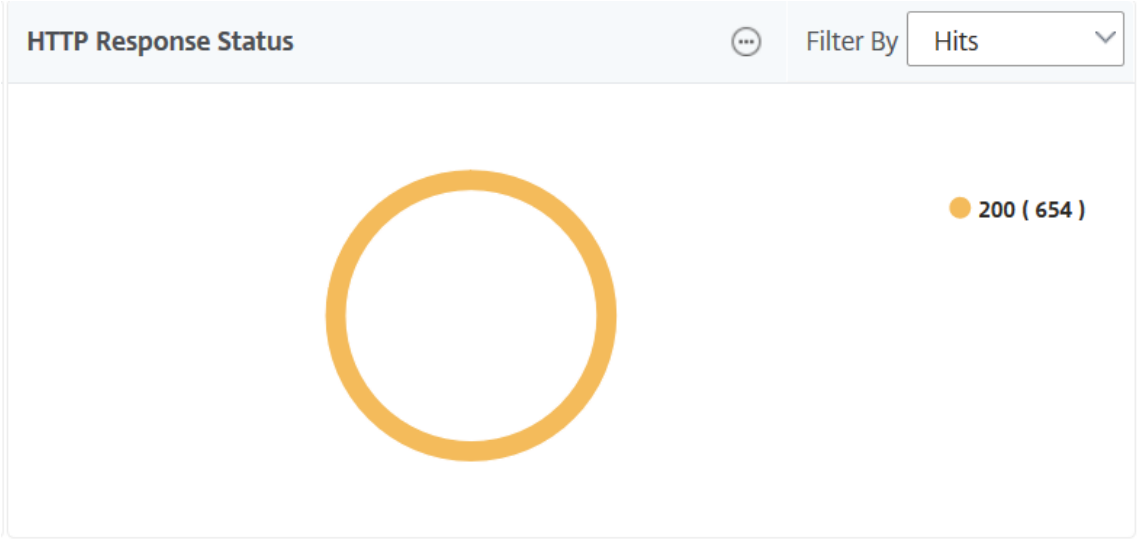
- **URL**



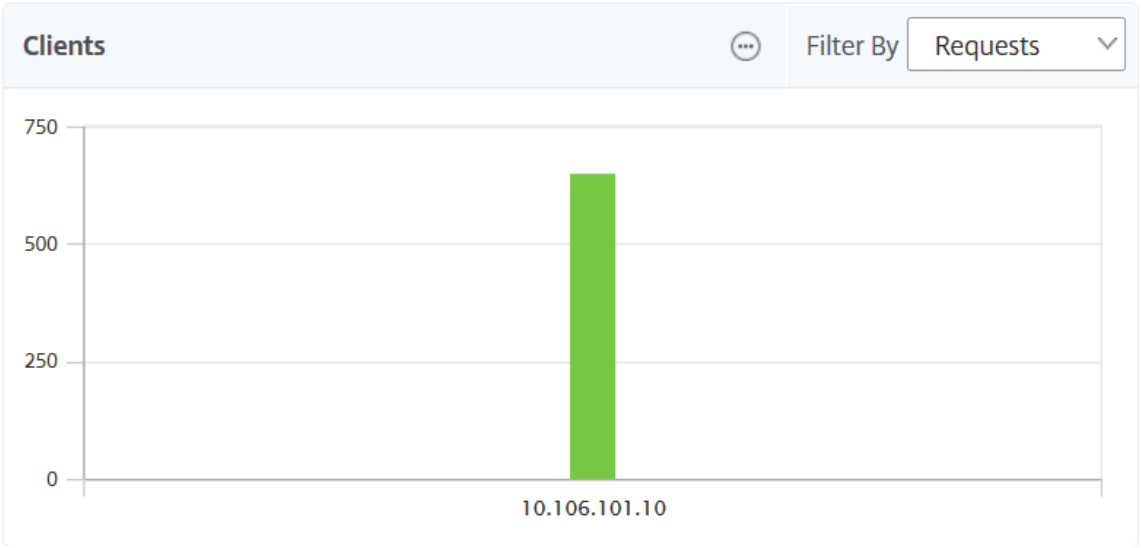
- **HTTP** 请求方法



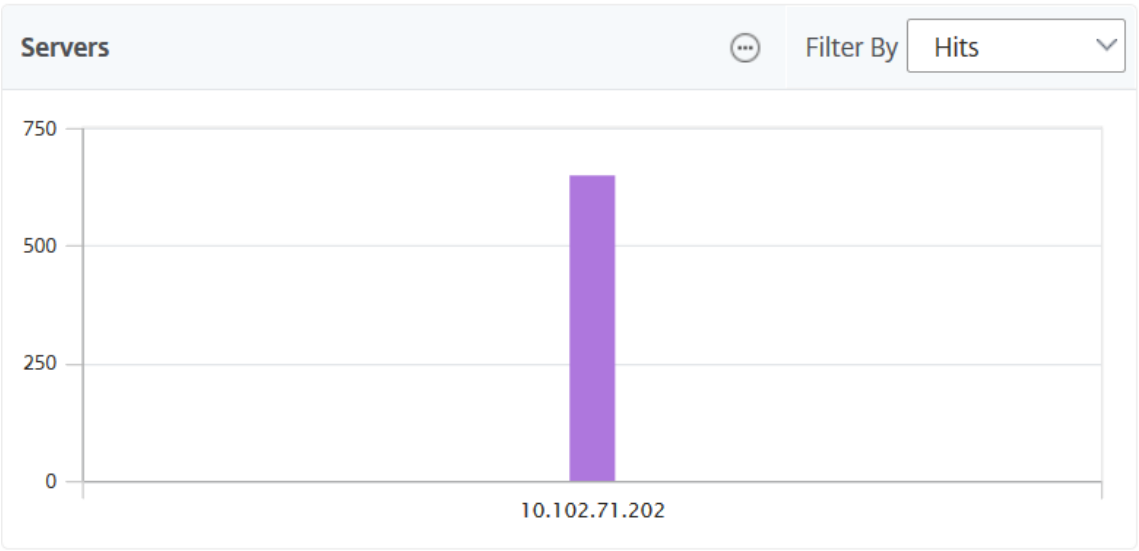
- **HTTP** 响应状态



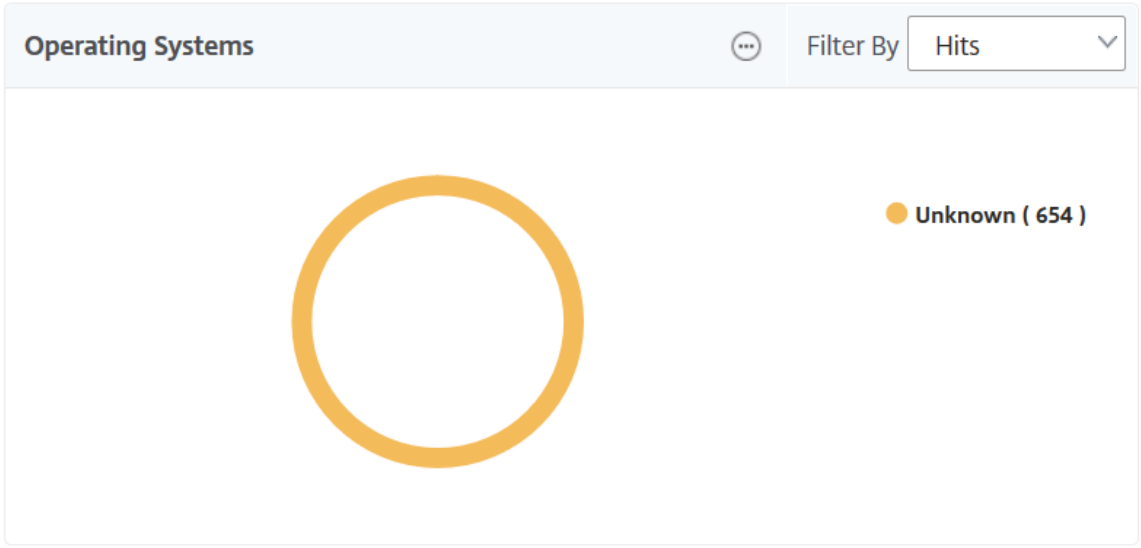
- 客户端



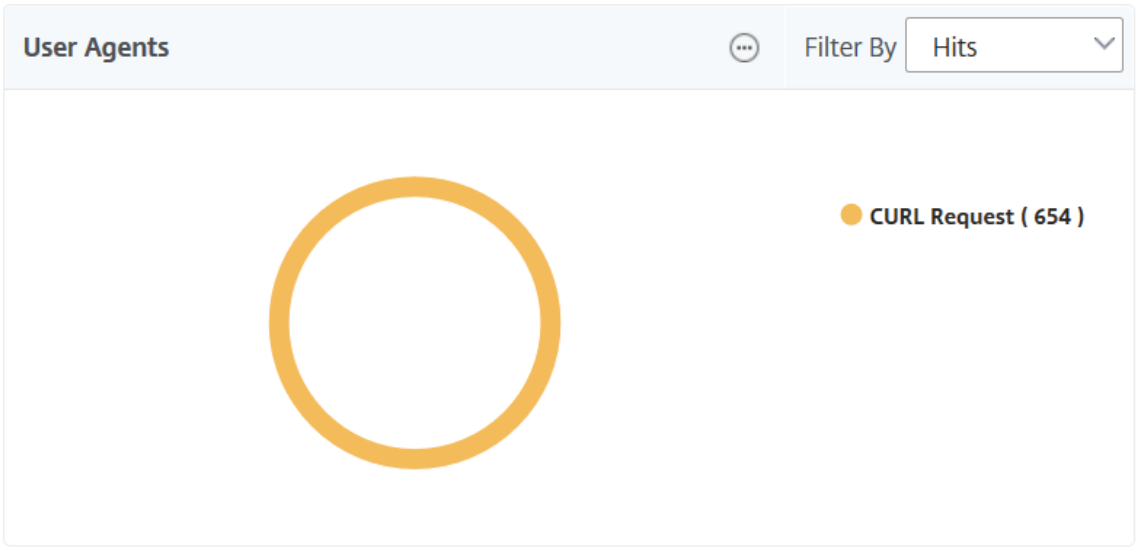
- 服务器



- 操作系统

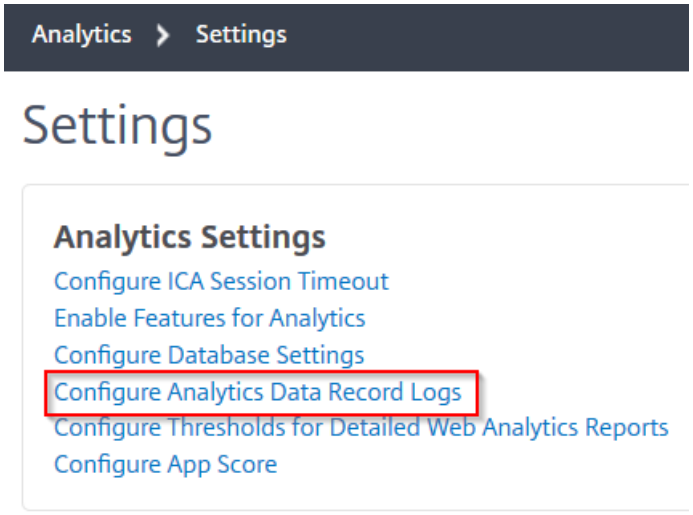


- 用户代理

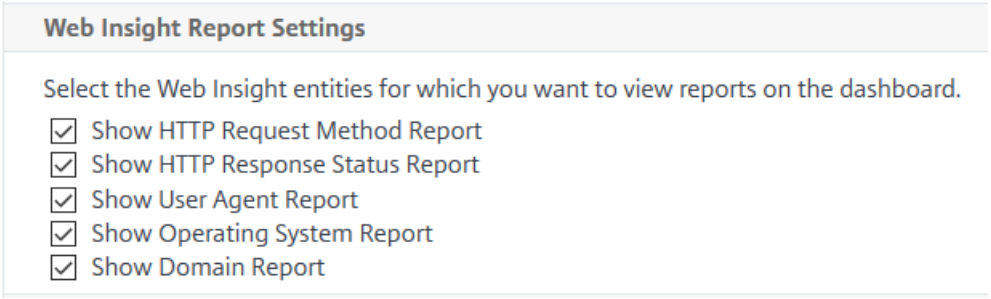


您还可以选择要在 GUI 上查看其报表的 **Web** 智能分析实体。

1. 导航到分析 > **Web Insight** > 设置。
2. 单击配置分析数据记录日志。



3. 在 **Web Insight** 报告设置下，选择要在 GUI 上查看报表的实体。



4. 单击确定。

要深入钻取以进一步分析，您可以在 GUI 中的 Web 见解分析下单击每个见解分类。例如，如果要检查已配置服务器的问题：

1. 导航到分析 > **Web Insight** > 服务器。
2. 将显示“服务器”页面，其中包含所有已配置的服务器。
3. 单击图表中的 IP 地址。您也可以单击表中的 IP 地址。

此时将显示所选服务器的详细分析视图。从此视图中，您可以检查多个见解，例如：

- 服务器接收的总点击次数
- Bandwidth（带宽）
- 服务器处理时间
- 服务器网络延迟
- 为服务器配置的虚拟服务器
- 访问服务器的客户端总数
- 服务器提供的响应代码总数

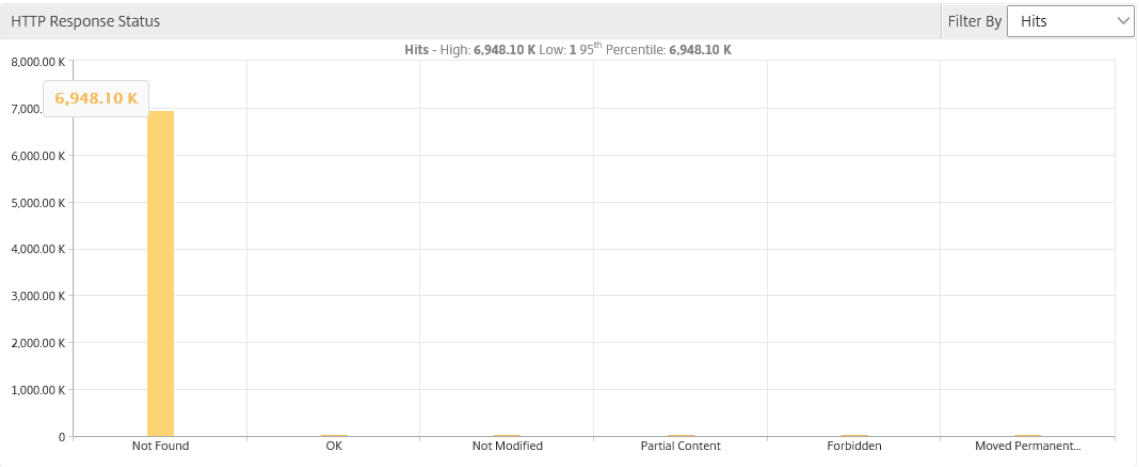
使用案例 **1-**内部服务器错误

考虑您的用户遇到 Web 应用程序的无法访问错误 500 的情况。错误 500（未找到）是 HTTP 响应状态错误，指示 Web 服务器上的问题，但服务器没有明确说明问题。要识别并深入到实际问题，请执行以下操作：

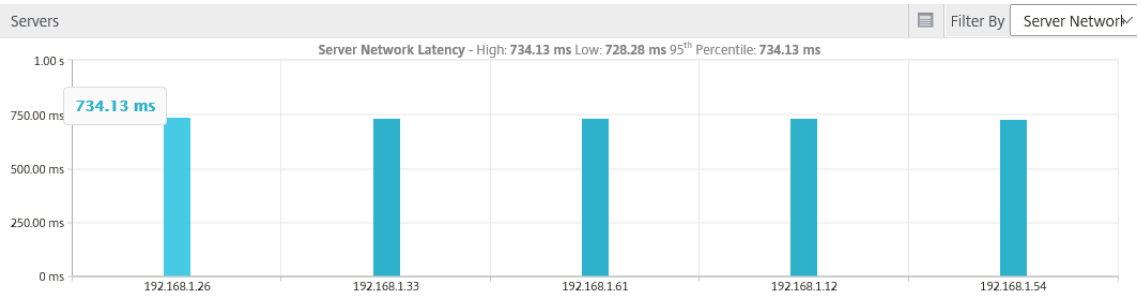
1. 导航到分析 > **Web Insight** > 响应状态。

   将显示控制板页面。控制板为您提供了可用于分析所处理 HTTP 事务的成功和失败的指标。

2. 单击图表上的未找到。



3. 向下滚动以查看服务器图形，然后从筛选方式列表中选择服务器网络延迟。



该图表表明每个应用程序服务器在检索 Web 应用程序时都存在问题，因此 Web 服务器的响应时间会增加。问题可能是 Web 服务器没有响应来自任何服务器的任何请求。

用例 **2-**用户在访问 **Web** 应用程序时遇到缓慢

考虑您的 Web 应用程序通过 10 个不同的 Web 服务器托管的情况。当多个用户同时访问应用程序时，一个或多个用户可能会遇到应用程序缓慢。作为管理员，您必须分析以下场景以了解问题的根本原因：

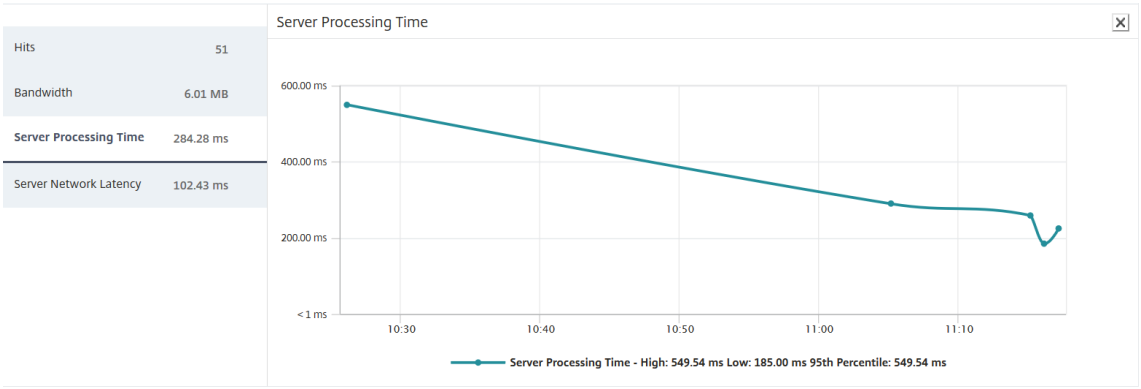
方案 **1-**服务器处理时间：

当多个请求同时击中 10 个 Web 服务器时，加载请求所花费的时间取决于：

- 队列中的请求数。
- 每个请求用于处理 HTTP 事务的带宽。

  服务器图形可帮助您了解服务器处理的请求的每个服务器的处理时间。同样，应用程序图表显示每个 HTTP 事务消耗的点击量、响应时间和带宽。

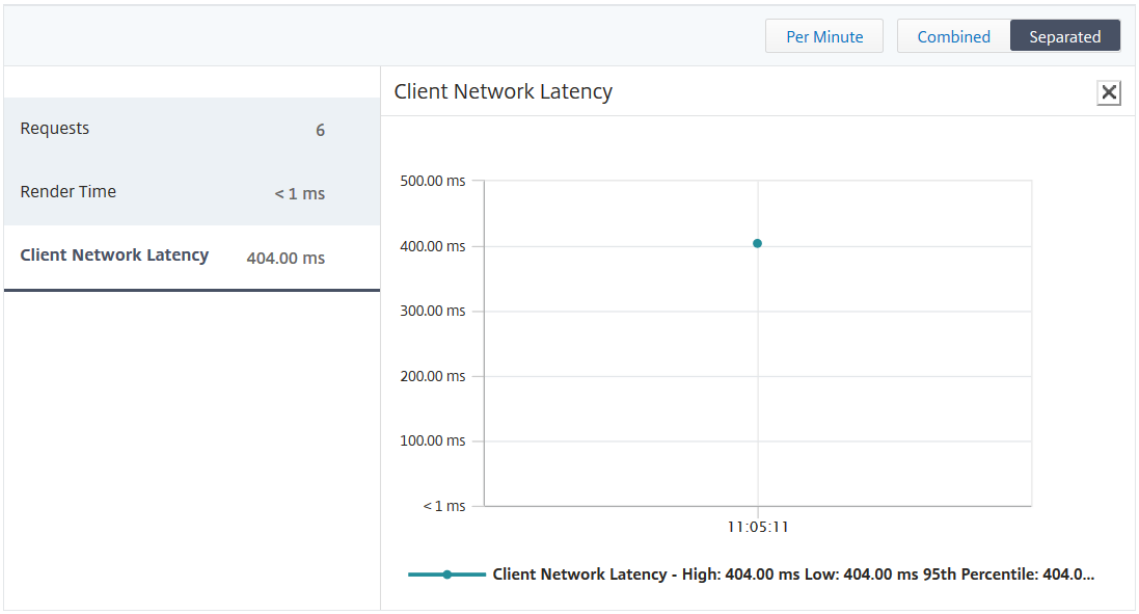
1. 导航到分析 > **Web Insight** > 服务器。
2. 从图表中选择服务器。
3. 单击服务器处理时间以分析服务器的处理时间。



场景 **2-**客户端延迟：

应用程序的响应时间和总点击次数可能是应用程序访问缓慢的原因。您可以检查客户端网络延迟并分析客户端网络延迟的衡量指标。要分析根本原因：

1. 导航到分析 > **Web Insight** > 客户端。
2. 从图表中选择客户端。
3. 单击客户端网络延迟分析高延迟。



在此示例中，作为管理员，您可以看到问题的根本原因来自客户端网络，因为客户端网络延迟表示高。

用例 **3-**访问 **Web** 应用程序的缓慢

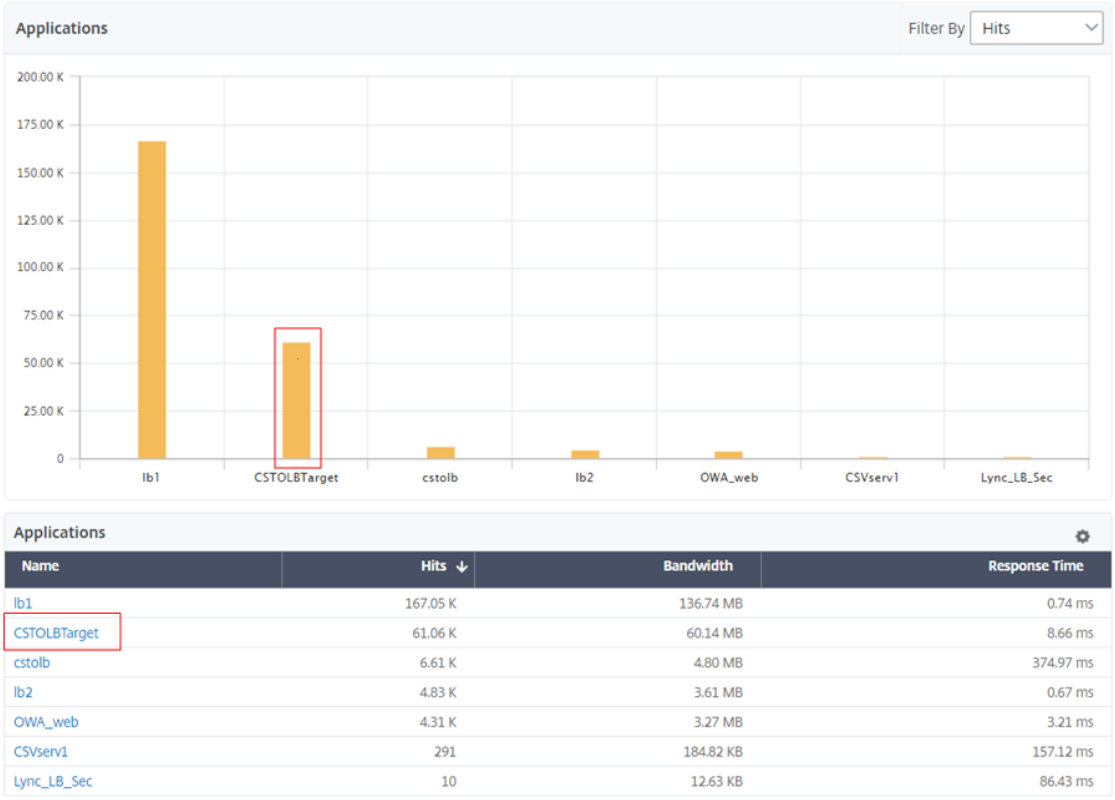
考虑以下情况：您有适用于 Windows 用户的 Web 服务器和适用于 Mac 用户的 Web 服务器，并且您的用户报告访问 Web 应用程序的速度缓慢。作为管理员，您知道您有：

- 为 Windows 用户配置了内容交换虚拟服务器。

- 为 Mac 用户配置了内容交换虚拟服务器。
- 将绑定到虚拟服务器的关联服务配置为基于 Windows 和 Mac 用户重定向请求。

要分析 Web 应用程序缓慢问题的根本原因：

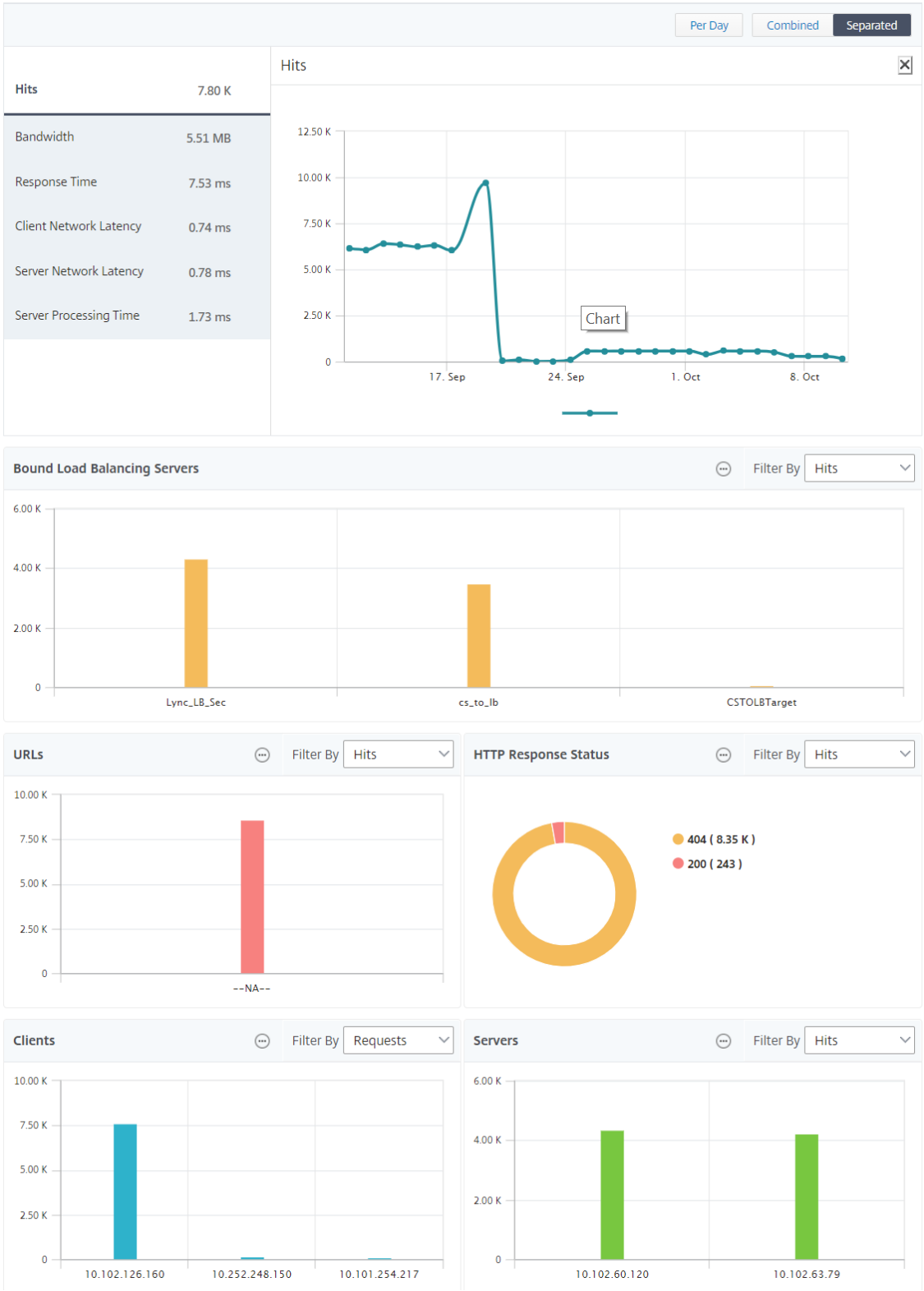
1. 导航到分析 > **Web Insight** > 应用程序
2. 选择内容交换虚拟服务器。
   例如，映像中的“CstolbTarget”应用程序是绑定到其他负载平衡虚拟服务器的内容交换虚拟服务器



Applications

Name	Hits ↓	Bandwidth	Response Time
lb1	167.05 K	136.74 MB	0.74 ms
CSTOLBTarget	61.06 K	60.14 MB	8.66 ms
cstolb	6.61 K	4.80 MB	374.97 ms
lb2	4.83 K	3.61 MB	0.67 ms
OWA_web	4.31 K	3.27 MB	3.21 ms
CSVserv1	291	184.82 KB	157.12 ms
Lync_LB_Sec	10	12.63 KB	86.43 ms

3. 单击内容交换虚拟服务器以查看其他负载平衡虚拟服务器。也可以单击表中的应用程序名称。



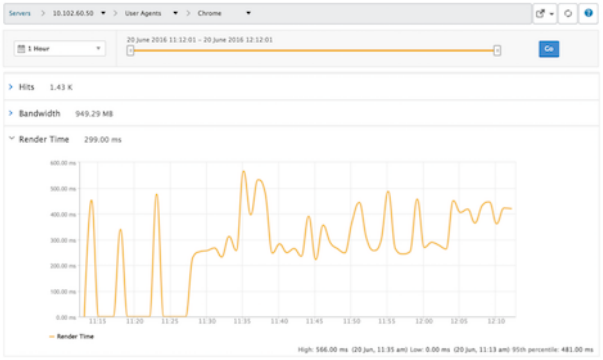
您可以进一步单击绑定的负载平衡服务器以查看这些应用程序的 Web 智能分析详细信息。

分析浏览器和操作系统的见解

可以使用 Web Insight 来帮助您区分 L7 延迟问题，并了解移动设备使用情况。作为管理员，见解可以帮助您了解整个用户群的不同操作系统使用情况。

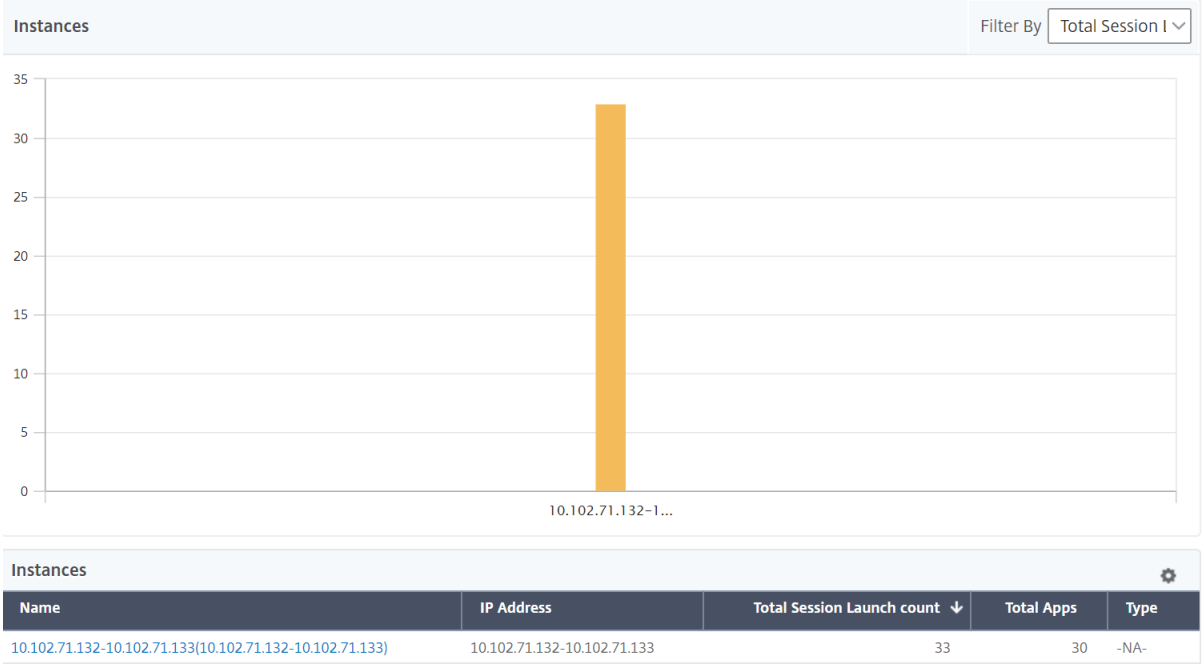
导航到“分析”>“**Web Insight**”>“操作系统”，了解用户访问速度缓慢的原因以及这是否是由于某些浏览器不兼容所致。还可以查看某些客户端上在使用哪些操作系统，以及在访问哪些浏览器。可以比较不同浏览器上的呈现时间，进一步深入查看特定浏览器，以找出哪些应用程序页面与该浏览器的最长呈现时间关联。

例如，可以选择 Google Chrome，查看对于特定应用程序的不同 URL 页面的相应呈现时间。

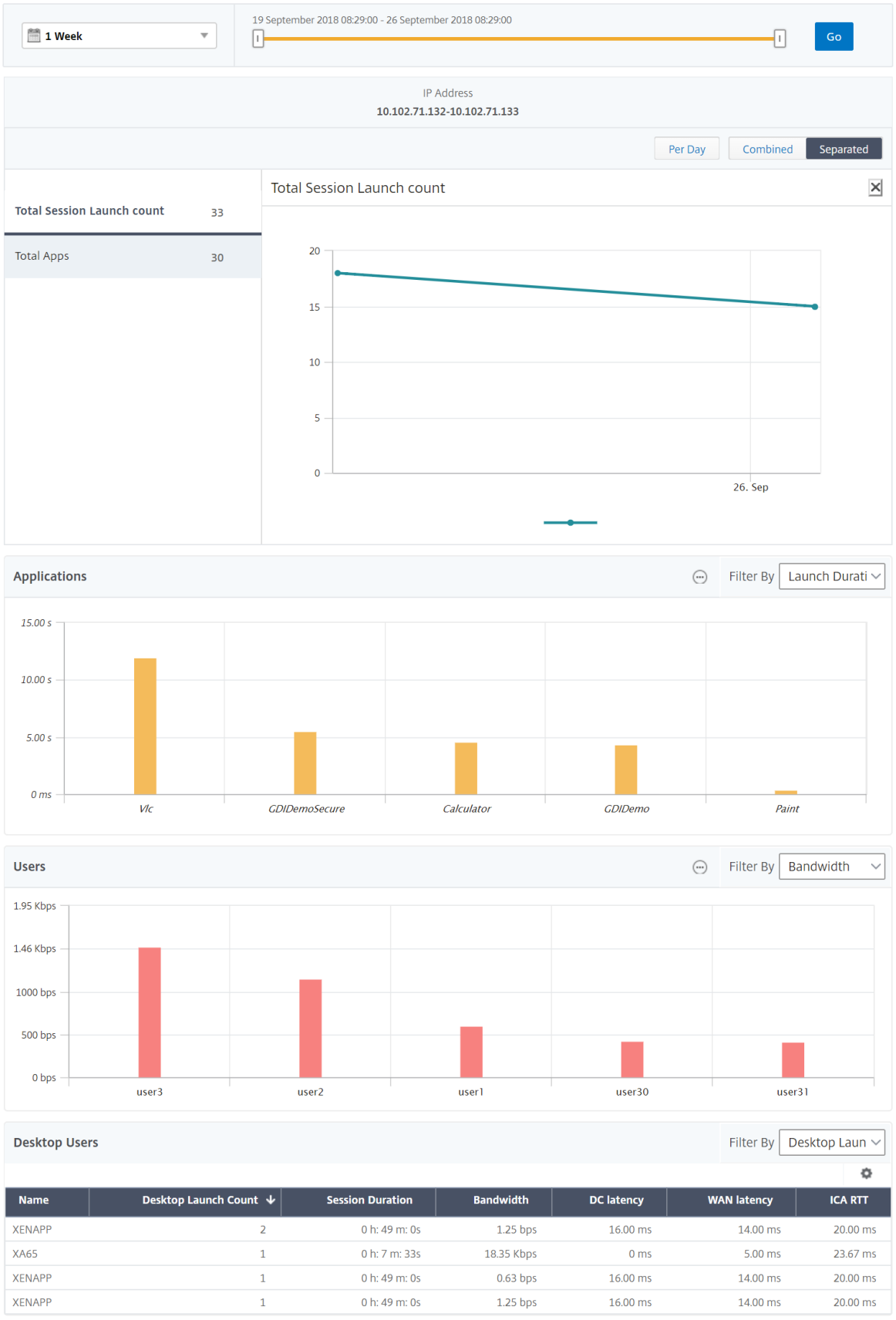


在高可用性模式下部署的 **Citrix ADC** 实例

Citrix ADM 为部署在高可用性模式下的 ADC 实例提供报告。所有分析都支持高可用性模式下实例的汇总报告。



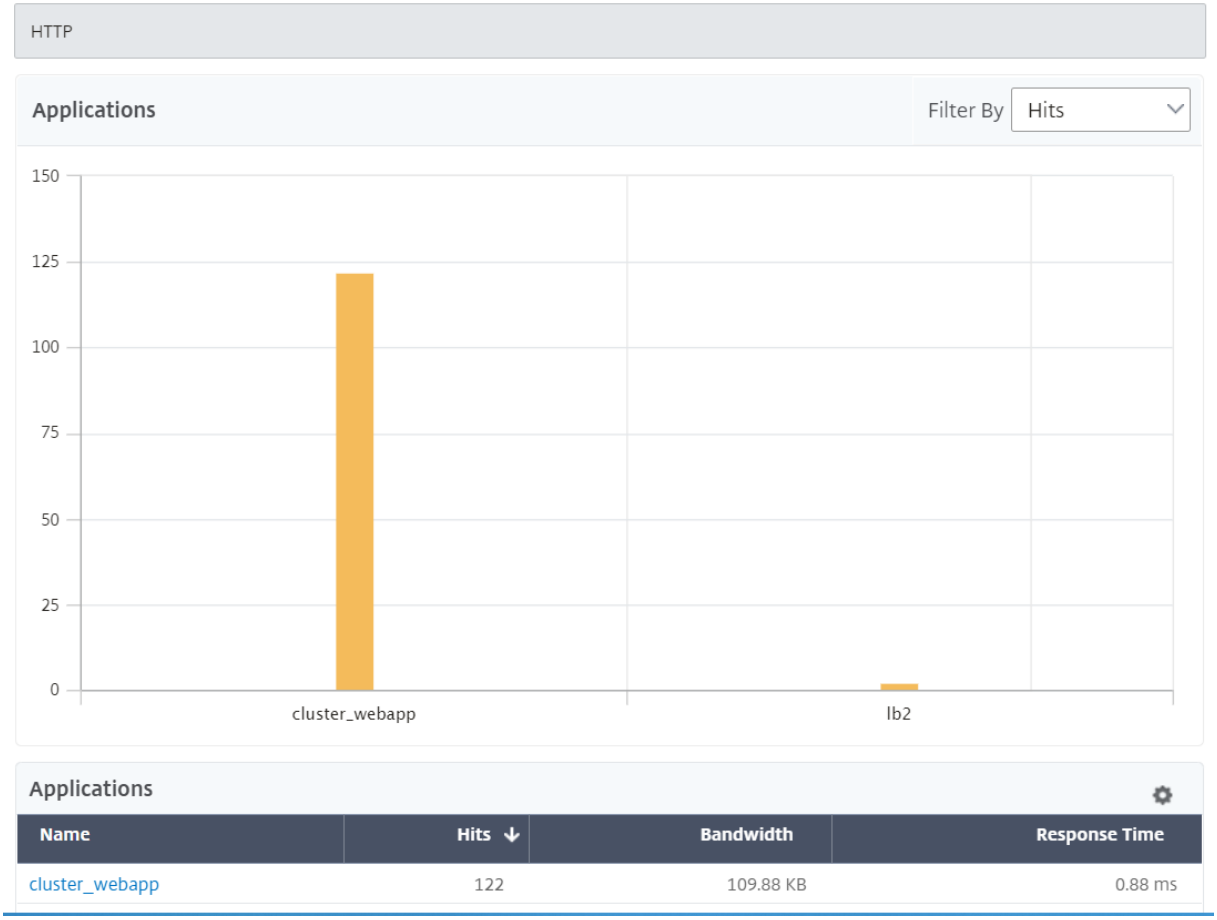
您可以单击高可用性实例的名称以查看更多详细信息。



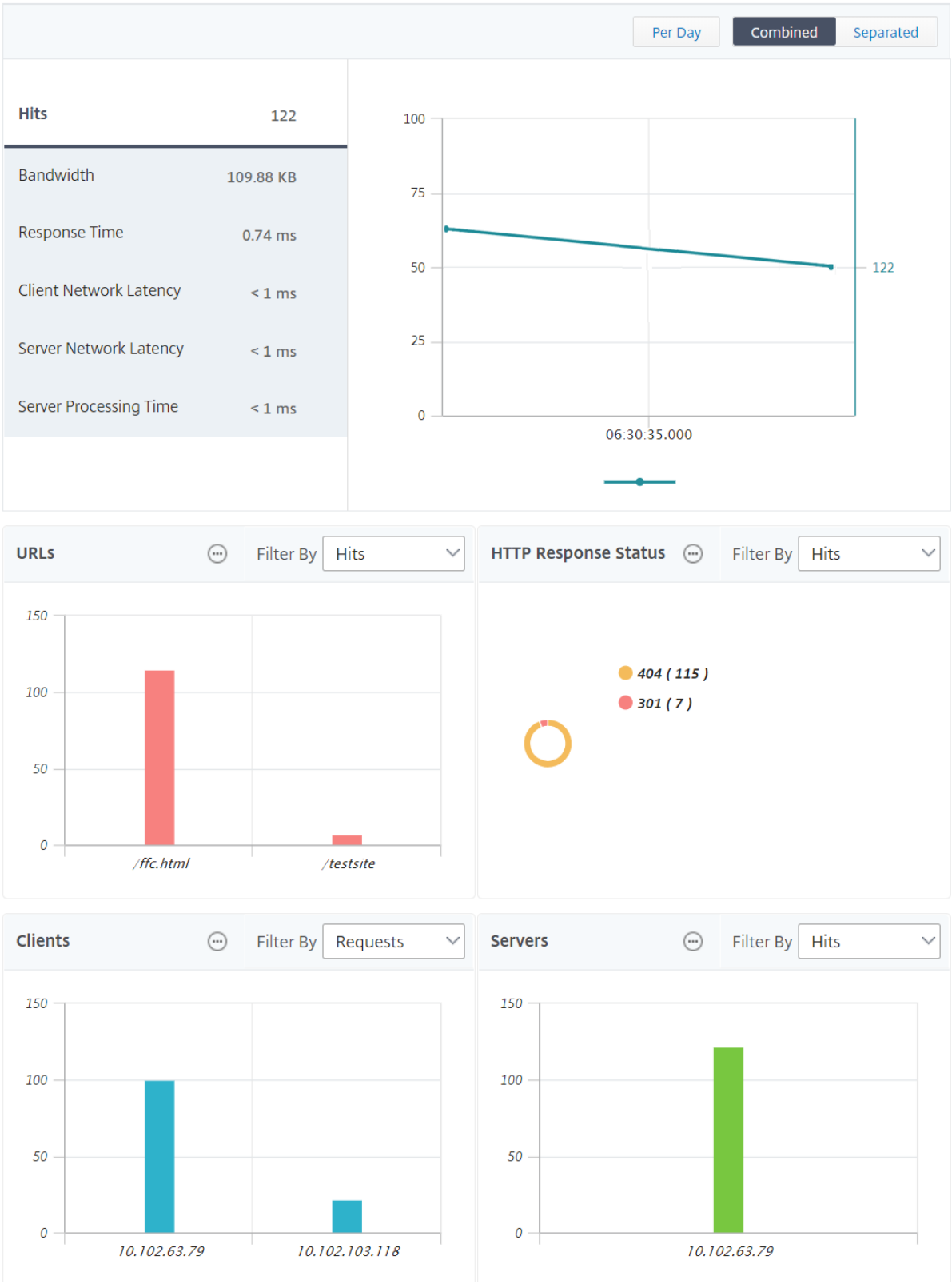
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

以群集模式部署的 **Citrix ADC** 实例

Citrix ADM 为以群集模式部署的 ADC 实例提供报告。所有分析都支持群集模式下的实例的聚合报告。



您还可以单击 CLIP 主机名以查看有关在群集模式下部署的 ADC 实例的所有详细信息。



> 注意
>
> - 之前在升级到 Citrix ADM 12.1 版本 503.x 之前收集的所有数据将继续显示为独立报告，直到数据保留为止。
> - 对于在群集模式下部署的 ADC 实例，观察域 ID/ 观察域名将替换为 CLIP 主机名和 CLIP。以前收集的所有数据都将继续报告观察域 ID/观察域名。

Web 见解地理测量配置

Citrix ADM 中的地理地图功能显示了地图上不同地理位置的 Web 应用程序的使用情况。管理员可以使用此信息了解应用程序使用趋势和容量规划。

Geomap 提供有关特定于国家/地区、州和城市的以下指标的信息：

- 点击总数：访问应用程序的总次数。
- 带宽：服务客户端请求时消耗的总带宽
- 响应时间：向客户端请求发送响应所用的平均时间。

Geomaps 提供的信息可用于解决以下几个用例：

- 访问应用程序的客户端数最大的区域
- 响应时间最长的区域
- 消耗最多带宽的区域

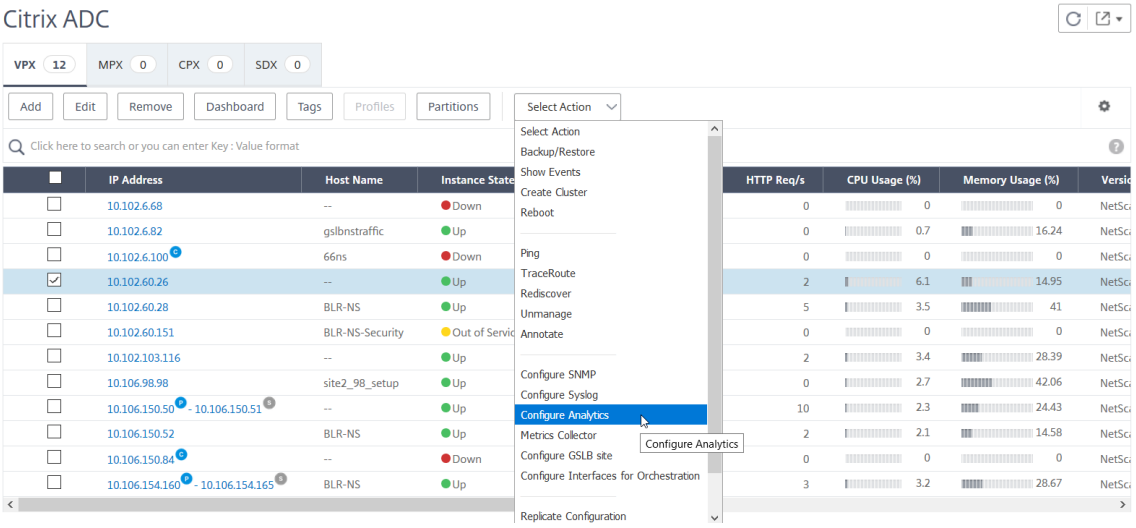
Citrix ADM 为您提供了为专用 IP 地址或公用 IP 地址配置地理地图的选项。

为专用 **IP** 地址配置地理地图

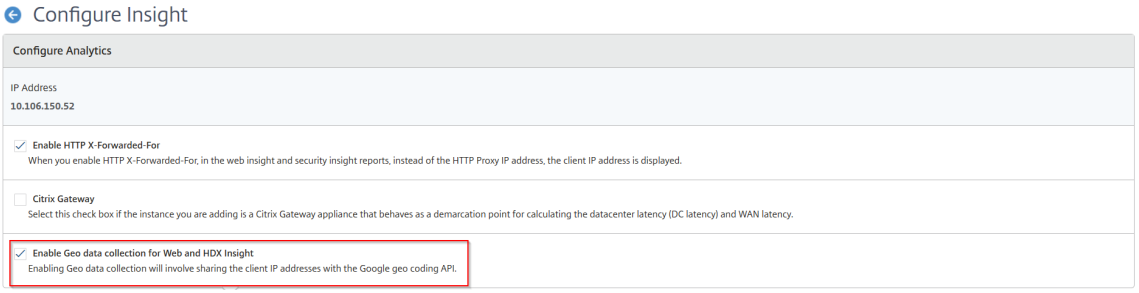
要查看来自地理位置上专用 IP 地址的 Web 应用程序流量，必须首先创建专用 IP 地址块，然后启用地理数据收集。

要启用地理数据收集，请执行以下操作：

1. 导航到网络 > 实例 > **Citrix ADC**，然后选择 Citrix ADC 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。



3. 在配置 **Insight** 页面上，选择为 **Web** 和 **HDX Insight** 启用地理数据收集。

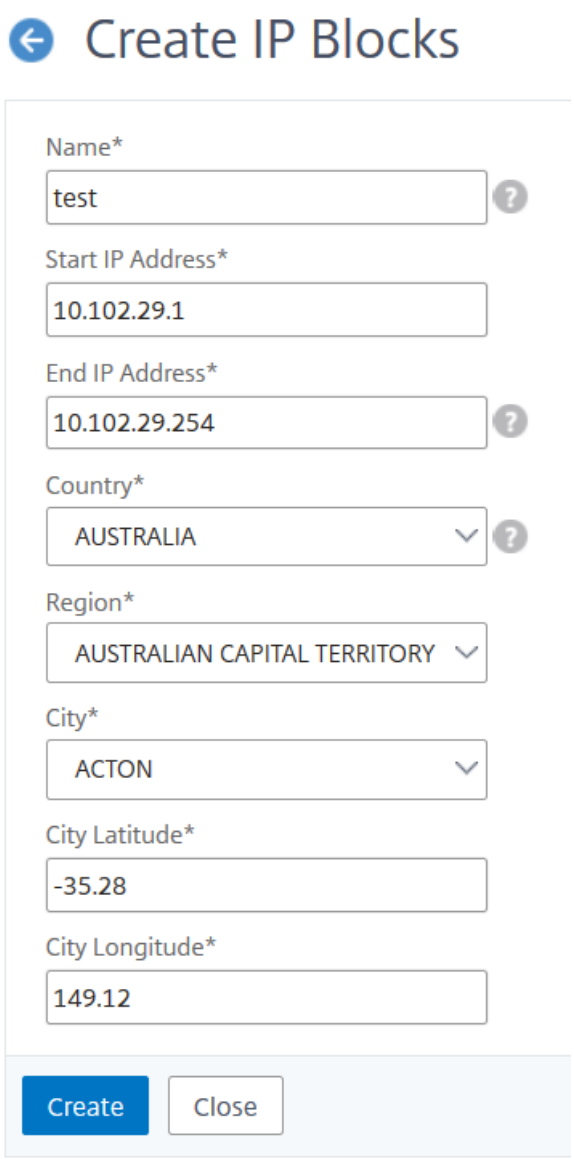


创建专用 **IP** 块　将客户端专用 IP 地址添加到 Citrix ADM 服务器后，Citrix ADM 可以识别客户端的位置。例如，如果客户端的 IP 地址属于与 A 城市相关联的专用 IP 地址块的范围内，Citrix ADM 会识别此客户端的流量来自 A 城市。

要创建 IP 块，请执行以下操作：

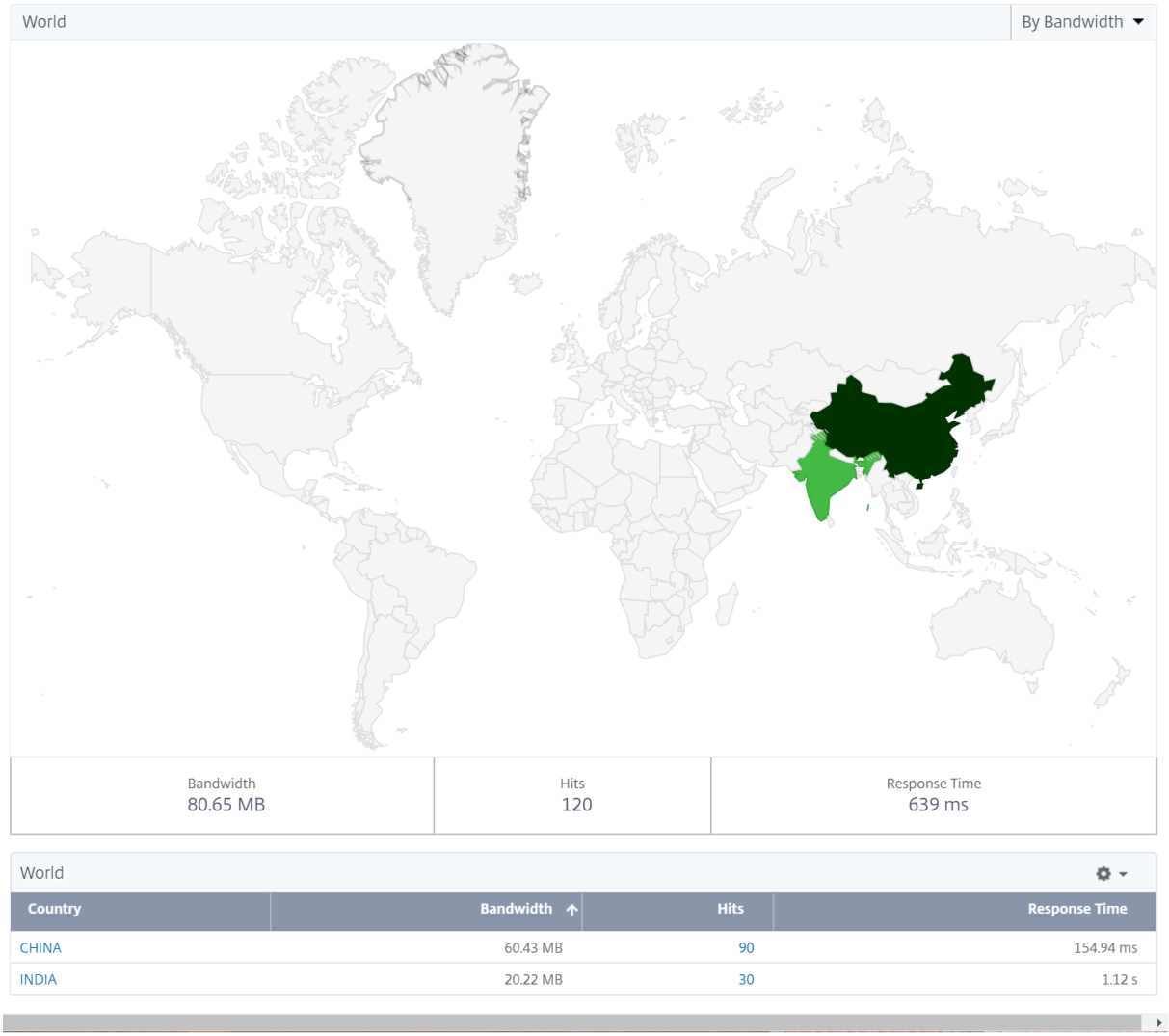
1. 在 Citrix ADM 中，导航到分析 > 设置 > **IP** 封锁，然后单击“添加”。
2. 在创建 **IP** 块页面中，指定以下参数：
    - 名称。为专用 IP 块指定一个名称
    - 起始 **IP** 地址。指定 IP 块的最低 IP 地址范围。
    - 结束 **IP** 地址。指定 IP 块的最大 IP 地址范围。
    - 国家。从列表中选择国家。
    - 区域。根据国家/地区，该区域会自动填充，但您可以选择您的区域。
    - 城市。根据地区，城市会自动填充，但您可以选择您的城市。
    - 城市纬度和城市经度。根据您选择的城市，纬度和经度会自动填充。

3. 单击 **Create**（创建）完成。



公共 **IP** 块　如果客户端使用公用 IP 地址，Citrix ADM 还可以识别客户端的位置。Citrix ADM 具有其内置位置 CSV 文件，该文件与基于客户端 IP 地址范围的位置匹配。对于使用公用 IP 块，唯一的要求是必须从“配置智能分析”页面启用“启用地理数据收集”。

> 注意
>
> Citrix ADM 需要互联网连接才能显示特定地理位置的地理地图。还需要 Internet 连接才能以.pdf、.png 或.jpg 格式导出 GeoMap。



要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出 图标。在 导出 页面上，您可以执行以下操作之一：

1. 选择“立即导出”选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出 选项卡。安排每天、每周或每月发送报告，并通过电子邮件或 Slack 消息发送报告。

> 注意
>
> - 如果您选择每周定期，请确保您选择要计划报表的工作日。
> - 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

配置阈值

您可以创建阈值，并在阈值突破时收到通知。在典型部署中，您可以将阈值设置为：

- 跟踪各种应用程序指标
- 促进规划
- 每当应用程序的指标值超过设定的阈值时都会收到通知

要配置阈值：

1. 导航到分析 > 设置 > 阈值。
2. 在“阈值”页上，单击“添加”。

   屏幕上将显示“创建阈值”页面。
3. 指定以下详细信息：

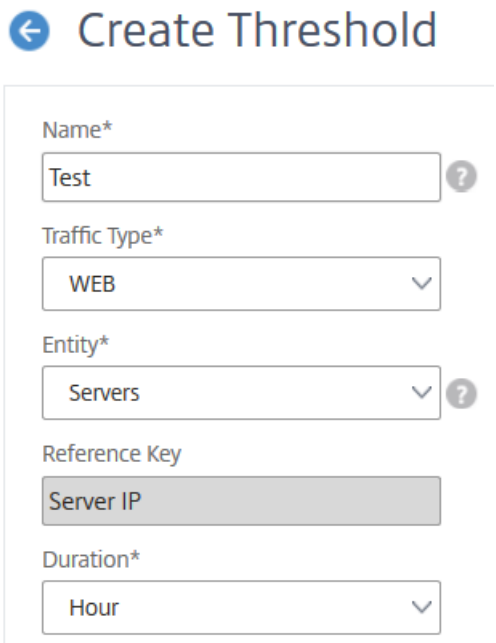
   a) 名称 -指定用于创建事件的名称。

   b) 流量类型 -从列表中选择 WEB。

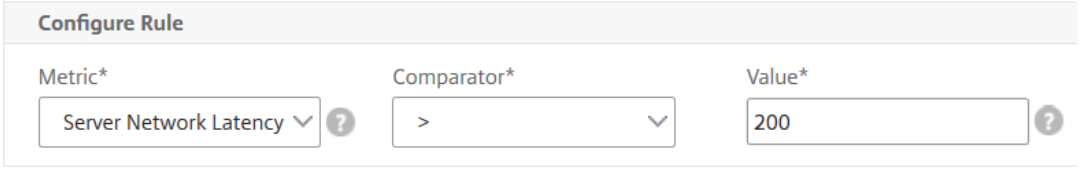
   c) 实体 -从列表中选择类别或资源类型。默认情况下，选择“应用程序”作为实体。

   d) 引用键 -根据您选择的流量类型和实体自动生成引用键。

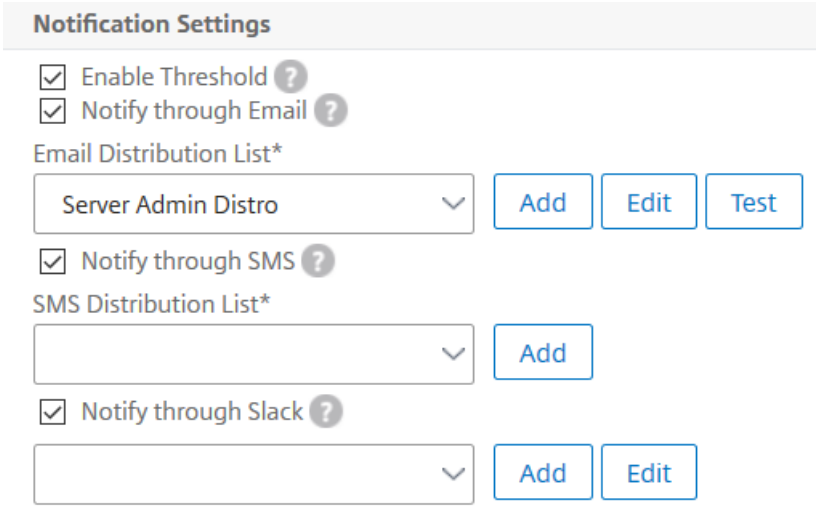
   e) 持续时间-从列表中选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。



   f) 在配置规则部分，通过选择指标和所需的比较器来创建规则，并提供阈值。



g) 在通知设置部分中，选择启用阈值和要获取警报的警报模式。



4. 单击创建。

HDX Insight

February 6, 2024

HDX Insight 为通过 Citrix ADC 流向 Citrix Virtual Apps and Desktops 的 HDX 流量提供端到端可见性。它还让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。实时和历史可见性数据的可用性使 Citrix Application Delivery Management (ADM) 能够支持各种使用案例。

要显示任何数据，您需要在您的 Citrix Gateway 虚拟服务器上启用 AppFlow。AppFlow 可以通过 IPFIX 协议或 Logstream 方法传递。

> 注意 要允许记录 ICA 往返时间计算，请启用以下策略设置：

- ICA 往返行程计算
- ICA 往返行程计算间隔
- 空闲连接的 ICA 往返行程计算

如果单击单个用户，则可以看到该用户在所选时间段内创建的每个 HDX 会话，无论是处于活动状态还是已终止状态。其他信息包括会话期间消耗的几个延迟统计信息和带宽。您还可以从单个虚拟通道（如音频、打印机映射和客户端驱动器映射）获取带宽信息。

您还可以导航到 **HDX Insight** > 应用 程序，然后单击 启动持续时间以查看应用程序启动所花费的时间。您还可以通过导航到 **HDX Insight -** 用户来查看所有连接的用户的用户代理。

> 注意 HDX 分析支持在软件版本 12.0 上运行的 Citrix ADC 实例中配置的管理分区。

下列瘦客户端支持 HDX Insight：

- WYSE 基于 Windows 的瘦客户端
- WYSE 基于 Linux 的瘦客户端
- WYSE 基于 ThinOS 的瘦客户端
- 10Zig 基于 Ubuntu 的瘦客户端

找出低性能问题的根本原因

场景 **1**

用户在访问 Citrix Virtual Apps and Desktops 时遇到延迟。

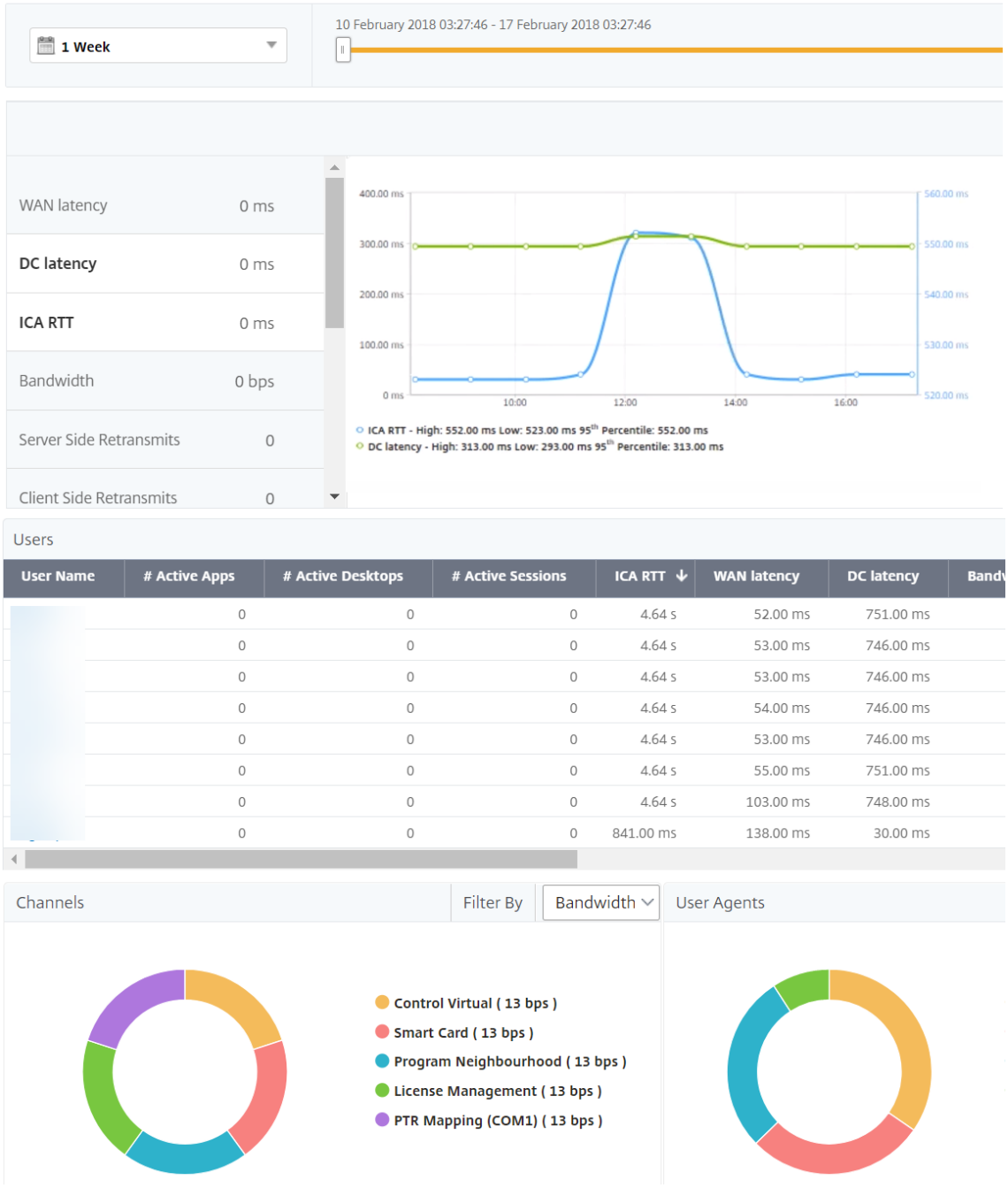
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟或客户端网络延迟造成。

为了找出问题的根本原因，请分析下列指标：

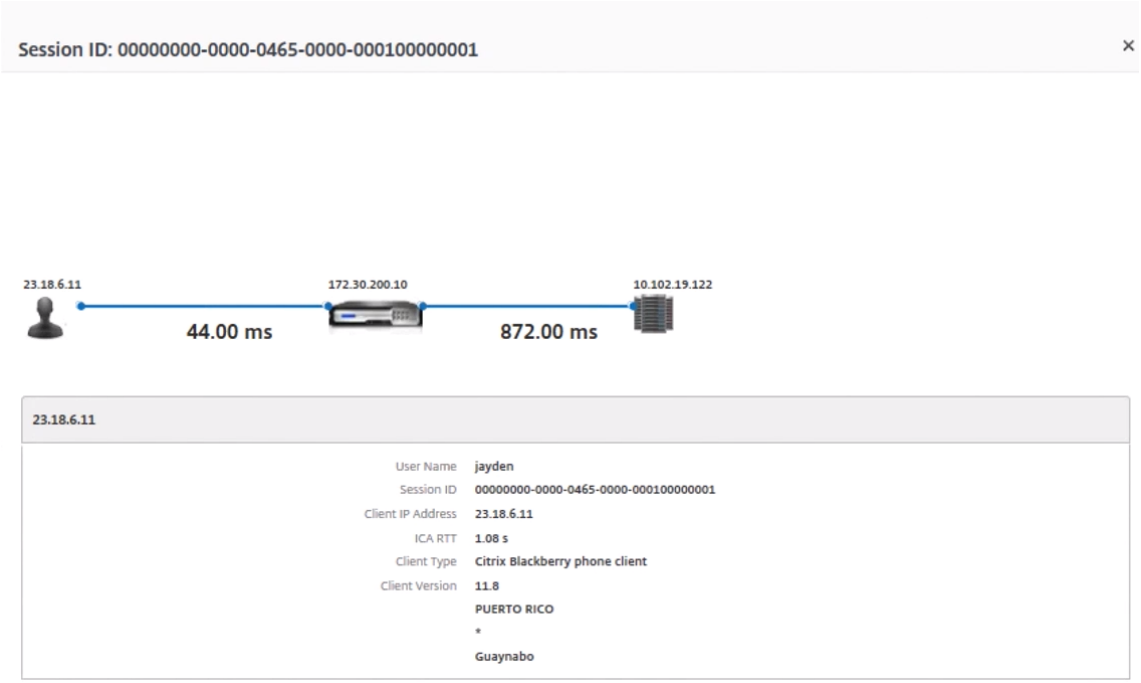
- WAN 延迟
- DC 延迟
- 主机延迟

要查看客户端度量，请执行以下操作：

1. 在“分析”选项卡上，导航到“**HDX Insight** 能分析”>“用户”。
2. 向下滚动并选择用户名，然后从列表中选择时段。期间可以是一天、一周、一个月，甚至可以自定义要查看数据的期间。
3. 图表以图形形式显示用户在指定时间段内的 ICA RTT 和 DC 延迟值。



4. 在“当前会话”表中，将鼠标悬停在 **RTT** 值上，并记下主机延迟、DC 延迟和 WAN 延迟值。
5. 在“当前会话”表中，单击跳图符号以显示有关客户端与服务器之间连接的信息，包括延迟值。



总结　在此示例中，**DC** 延迟为 751 毫秒，**WAN** 延迟为 52 毫秒，主机延迟为 6 秒。这表示由于服务器网络导致的平均延迟，用户正在遇到延迟。

方案 **2**

用户在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上启动应用程序时遇到延迟

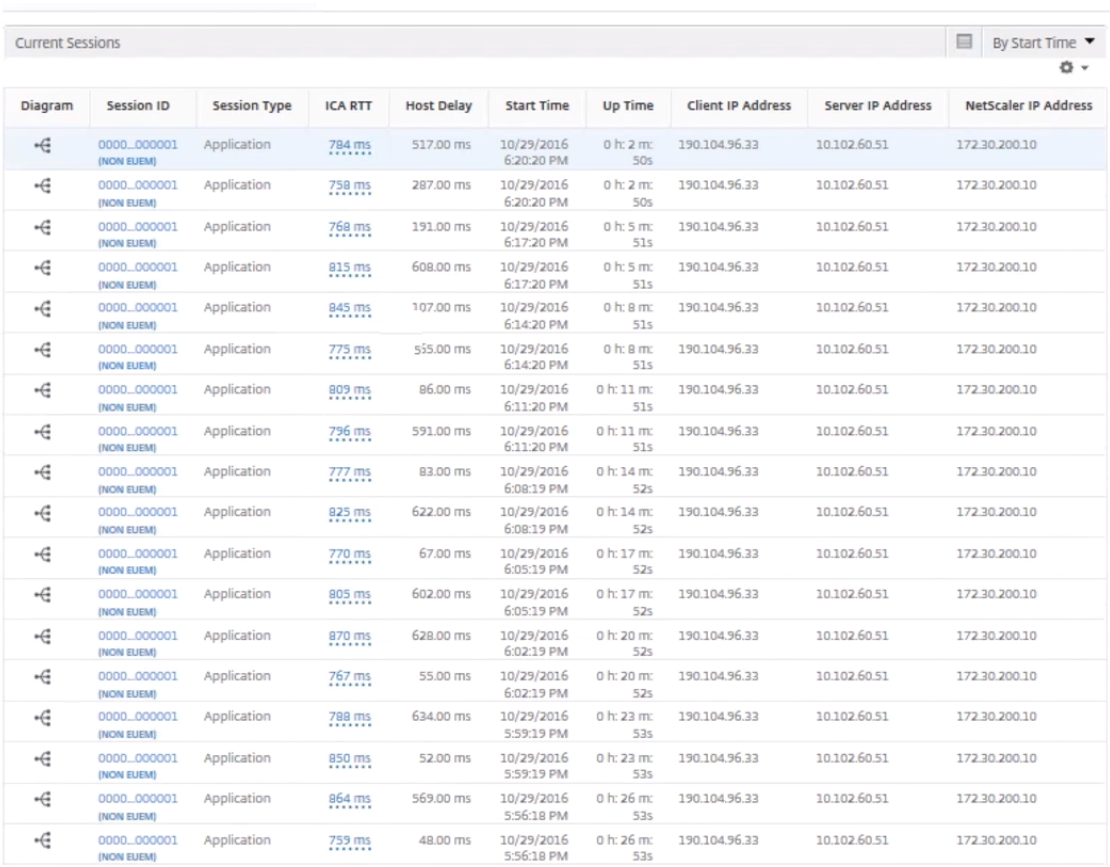
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟、客户端网络延迟或应用程序启动所用时间造成。

为了找出问题的根本原因，请分析下列指标：

- WAN 延迟
- DC 延迟
- 主机延迟

要查看用户指标，请执行以下操作：

1. 在“分析”选项卡上，导航到 **HDX Insight** > 用户。
2. 向下滚动并单击用户名。
3. 在图形表示方式中，注意观察特定会话的 WAN 延迟、DC 延迟以及 RTT 值。
4. 在“当 前会话”表中，请注意主机延迟很高。



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

总结　在此示例中，直流延迟为 1 毫秒，**WAN** 延迟 为 12 毫秒，但主机延迟 为 517 毫秒。高 RTT 且直流和 WAN 延迟较低，表示主机服务器上出现应用程序错误。

> 注意：如果您使用的是 Citrix ADM 运行软件 11.1 版本 51.21 或更高版本，HDX Insight 还会显示其他用户指标，例如广域网抖动和服务器端重传次数。要查看这些指标，请导航到分析 > **HDX Insight** > 用户，然后选择一个用户名。用户指标将显示在图旁边的表中。

用于 **HDX Insight** 的地理图

Citrix ADM 地理地图功能在地图上显示应用程序在不同地理位置的使用情况。管理员可以使用此信息来了解应用程序在各地理位置使用情况的趋势。

您可以通过指定特定地理位置的专用 IP 范围（起始和结束 IP 地址），将 Citrix ADM 配置为显示特定地理位置或局域网的地理地图。

您还可以在 HDX Insight 中查看地理位置地图中的历史和活动用户的详细信息。导航到分析 > **HDX Insight**，然后在地图的“世界”部分，单击要查看详细信息的国家或地区。您可以按城市和省/自治区进一步深入查看信息。

要为数据中心配置地理图，请执行以下操作：

在“分析”选项卡上，导航到“设 置”>“**IP** 块”以配置特定位置的地理地图。

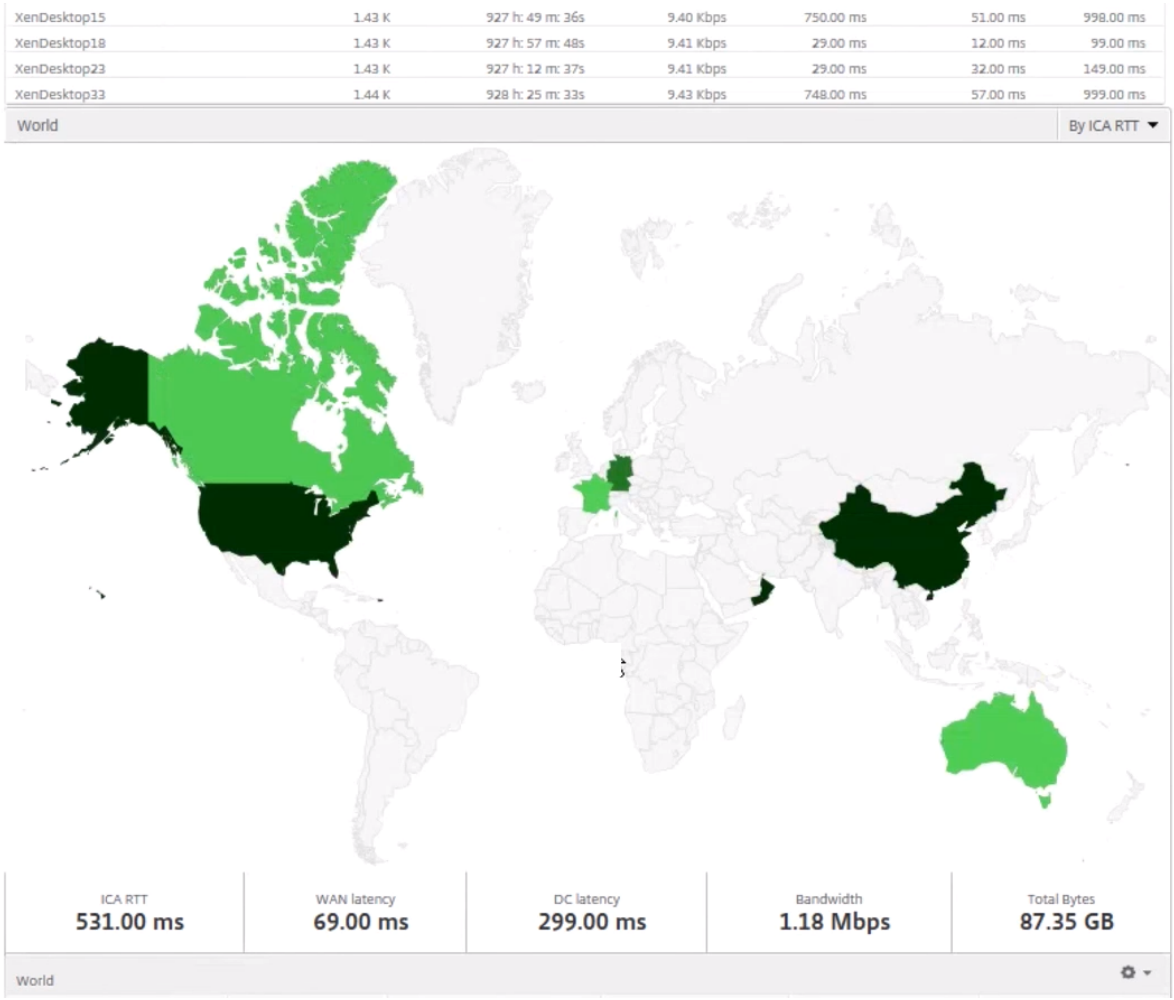
用例

假设这样一个场景：组织 ABC 有 2 个分支机构：一个在圣克拉拉，另一个在印度。

圣克拉拉用户使用 SClara.x.com 上的 Citrix Gateway 设备来访问 VPN 流量。印度用户使用 India.x.com 上的 Citrix Gateway 设备来访问 VPN 流量。

在一个特殊的时间间隔（例如 10 AM 到 5 PM），圣克拉拉的用户连接到 SClara.x.com 来访问 VPN 流量。大多数用户访问相同的 Citrix Gateway，从而导致连接到 VPN 的延迟，因此某些用户连接到 India.x.com 而不是 SClara.x.com。

分析流量的 Citrix ADC 管理员可以使用地理映射功能显示圣克拉拉办公室中的流量。该地图显示圣克拉拉办事处的响应时间非常长，因为圣塔克拉拉办事处只有一台 Citrix Gateway 设备，用户可以通过该设备访问 VPN 流量。因此，管理员可能会决定安装另一个 Citrix Gateway，以便用户有两个本地 Citrix Gateway 设备来访问 VPN。



限制

如果 Citrix ADC 实例拥有企业版许可，则不会触发在 Citrix ADM 上为 HDX Insight 设置的阈值，因为分析数据仅收集 1 小时。

启用 **HDX Insight** 数据收集

February 6, 2024

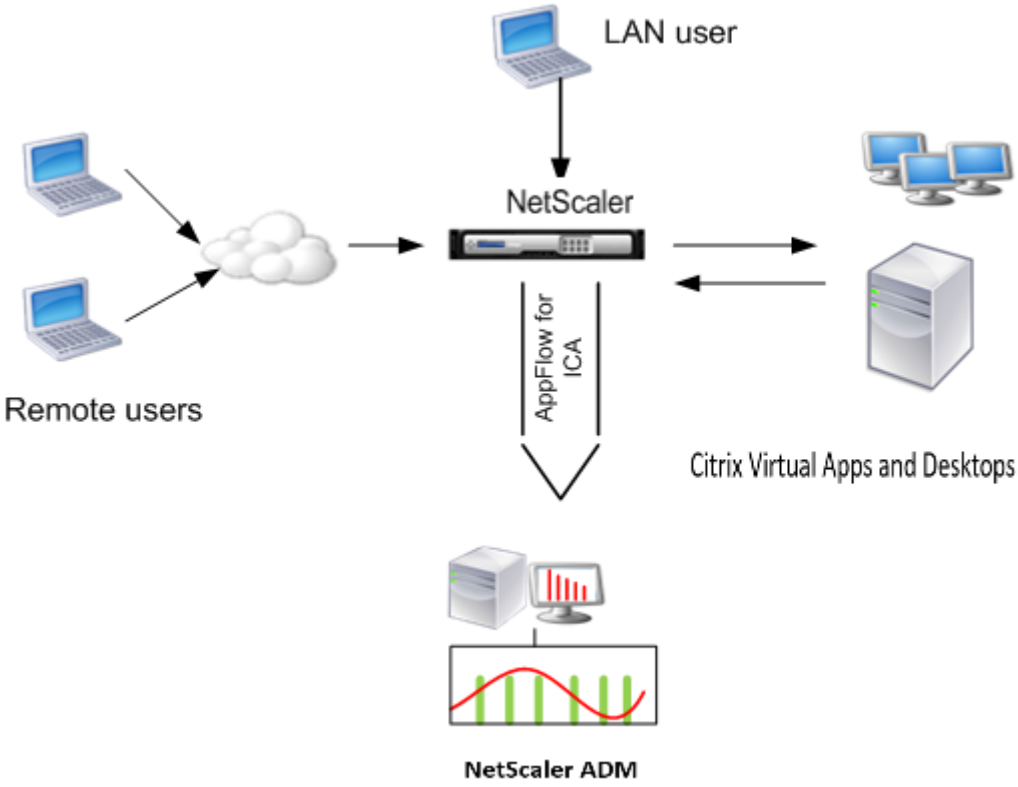
HDX Insight 通过 Citrix ADC 实例或 Citrix SD-WAN 设备传递的 ICA 流量提供前所未有的端到端可见性，使 IT 部门能够提供卓越的用户体验，并且是 Citrix Application Delivery Management (ADM) 分析的一部分。HDX Insight 针对网络、虚拟桌面、应用程序及应用程序结构提供令人信服的强大业务智能和故障分析功能。HDX Insight 可以即时鉴别分类用户问题、收集有关虚拟桌面连接的数据、生成 AppFlow 记录并将其呈现为可视报告。

在 Citrix ADC 中启用数据收集的配置因设备在部署拓扑中的位置而异。

启用数据收集以监视在局域网用户模式下部署的 **Citrix ADC**

访问 Citrix Virtual Apps and Desktops 应用程序的外部用户必须在 Citrix Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 Citrix Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便将请求重定向到 Citrix ADC 设备。

要克服这些挑战，并让局域网用户直接连接到 Citrix Virtual Apps and Desktops 应用程序，您可以通过配置缓存重定向虚拟服务器（该服务器充当 Citrix Gateway 设备上的 SOCKS 代理）以 LAN 用户模式部署 Citrix ADC 设备。



> 注意： Citrix ADM 和 Citrix Gateway 设备位于同一子网中。

要监视在此模式下部署的 Citrix ADC 设备，请先将 Citrix ADC 设备添加到 NetScaler Insight 清单，启用 AppFlow，然后在控制面板上查看报告。

将 Citrix ADC 装置添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。

> 注意
>
> - 在 ADC 实例上，您可以导航到“系统”>“**AppFlow**”>“收集器”，以检查收集器（即 Citrix ADM）是否启动。Citrix ADC 实例使用 NSIP 将 AppFlow 记录发送到 Citrix ADM。但是该实例使用其 SNIP 来验证与 Citrix ADM 的连接。因此，请确保在实例上配置 SNIP。
> - 无法使用 Citrix ADM 配置实用程序在局域网用户模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。

> • 有关策略表达式的信息，请参阅策略和表达式。

要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 添加转发代理缓存重定向虚拟服务器并提供代理 IP 和端口，指定服务类型为 HDX。

   add cr vserver <name> <servicetype> [<ipaddress> <port>] [-cacheType <cachetype>] [- cltTimeout <secs>]

   示例

   ```
   add cr vserver cr1 HDX 10.12.2.2 443  -cacheType FORWARD  -
       cltTimeout 180
   <!--NeedCopy-->
   ```

   > 注意：如果您使用 Citrix Gateway 设备访问 LAN 网络，请添加要由匹配 VPN 流量的策略应用的操作。

   add vpn trafficAction <name> <qual> [-HDX (ON or OFF)]

   add vpn trafficPolicy <name> <rule> <action>

   示例

   ```
   add vpn trafficAction act1 tcp -HDX ON

   add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
   <!--NeedCopy-->
   ```

3. 将 Citrix ADM 添加为 Citrix ADC 设备上的 AppFlow 收集器。

   add appflow collector <name> **-IPAddress** <ip_addr>

   示例：

   ```
   add appflow collector MyInsight -IPAddress 192.168.1.101
   <!--NeedCopy-->
   ```

4. 创建 AppFlow 操作，并将收集器与该操作关联。

   add appflow action <name> **-collectors** <string> …

   示例：

   ```
   add appflow action act -collectors MyInsight
   <!--NeedCopy-->
   ```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

   add appflow policy <policyname> <rule> <action>

   示例：


```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。

   bind appflow global <policyname> <priority> **-type** <type>

   示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

   > 注意 要应用于 ICA 流量，类型的值应为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

   set appflow param -flowRecordInterval 60

   示例：

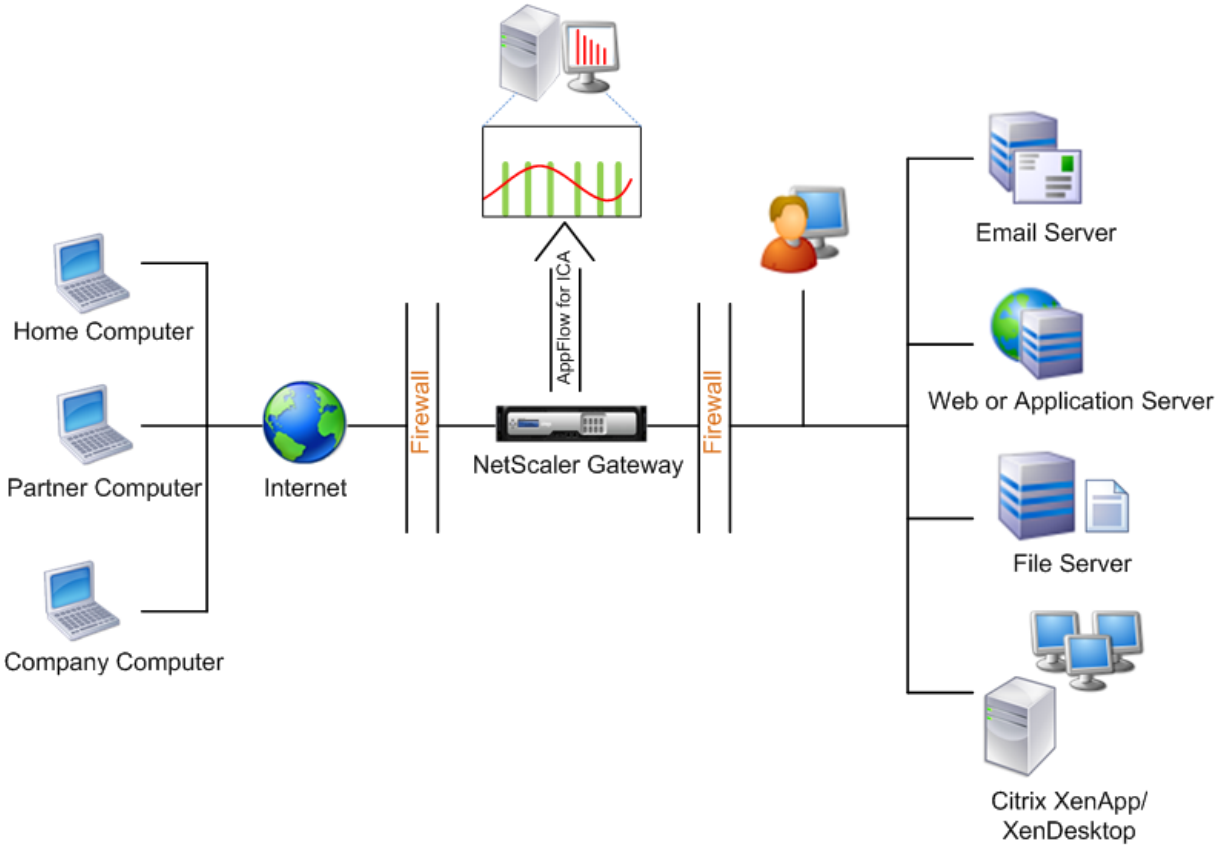
```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 保存配置。类型：`save ns config`

为在单跃点模式下部署的 **Citrix Gateway** 设备启用数据收集

在单跃点模式下部署 Citrix Gateway 时，它位于网络的边缘。网关实例提供与桌面交付基础架构的代理 ICA 连接。单跃点是最简单、最常见的部署。如果外部用户尝试访问组织中的内部网络，单跃点模式可提供安全性。
在单跃点模式下，用户通过虚拟专用网络 (VPN) 访问 Citrix ADC 设备。

要开始收集报告，必须将 Citrix Gateway 设备添加到 Citrix Application Delivery Management (ADM) 清单中，并在 ADM 上启用 AppFlow。



要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到“网络”>“实例”，然后选择要启用分析的 Citrix ADC 实例。
4. 从选择操作下拉列表中，选择配置分析。
5. 选择 VPN 虚拟服务器，然后单击启用 **AppFlow**。
6. 在“启用 **AppFlow**”字段中，键入 **true**，然后选择 **ICA**。
7. 单击确定。

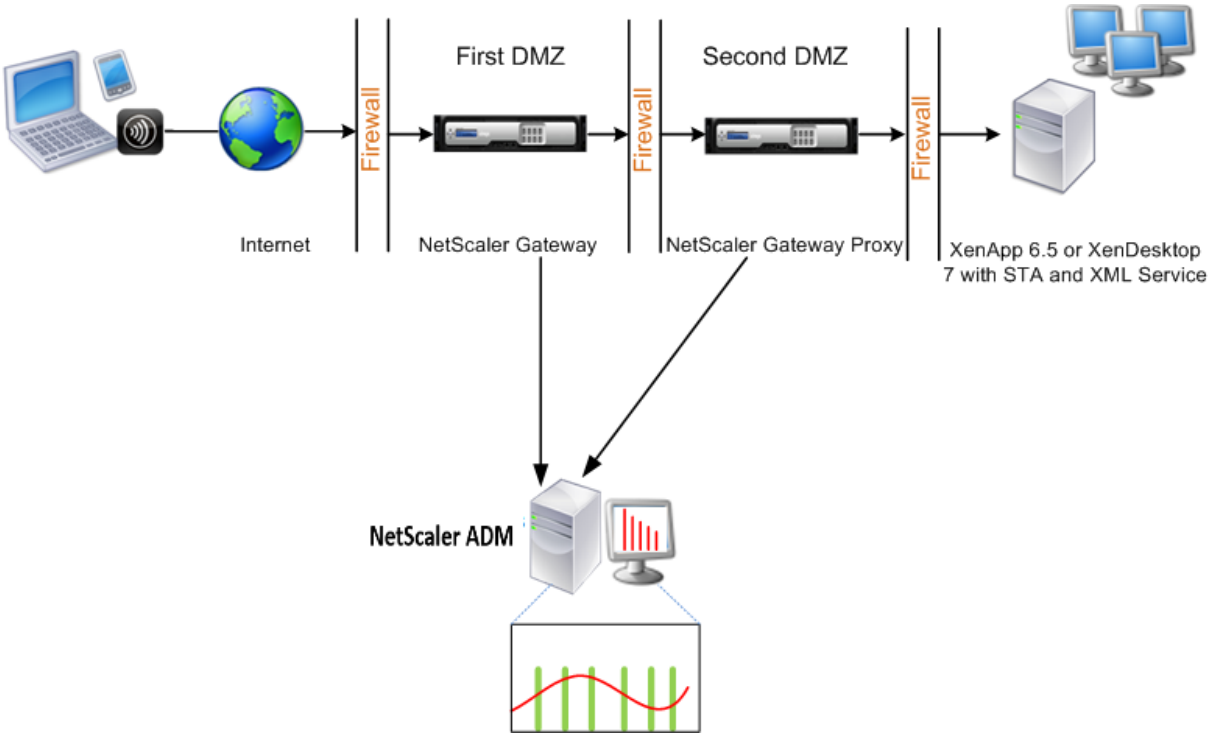
> 注意：在单跃点模式下启用 AppFlow 时，以下命令在后台执行。此处显式指定这些命令是为了进行故障排除。
>
> - add appflow collector <name> -IPAddress <ip_addr>
> - add appflow action <name> -collectors <string>
> - set appflow param -flowRecordInterval <secs>
> - disable ns feature AppFlow
> - enable ns feature AppFlow
> - add appflow policy <name> <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

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则 Citrix ADM 上仍会显示剩余的 HDX Insight 数据。

为在双跃点模式下部署的 **Citrix Gateway** 设备启用数据收集

Citrix Gateway 双跳模式为组织的内部网络提供额外的保护，因为攻击者需要穿透多个安全区域或非军事区域 (DMZ) 才能访问安全网络中的服务器。如果要分析 ICA 连接通过的跃点数（Citrix Gateway 装置），以及有关每个 TCP 连接上延迟的详细信息，以及它如何与客户端感知到的总 ICA 延迟展开，则必须安装 Citrix ADM，以便 Citrix Gateway 设备报告这些生命统计数据。



第一个 DMZ 中的 Citrix Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 Citrix Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 Citrix Gateway 充当 Citrix Gateway 代理设备。此 Citrix Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。

Citrix ADM 可以部署在属于第一个 DMZ 中 Citrix Gateway 设备的子网中，也可以部署在属于 Citrix Gateway 设备的第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 Citrix ADM 和 Citrix Gateway 部署在同一个子网中。

在双跃点模式下，Citrix ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 Citrix Gateway 设备添加到 Citrix ADM 清单并启用数据收集后，每台设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 Citrix ADM 识别哪个装置正在导出记录，每个装置都会使用跳数指定，并使用连接链 ID 指定每个连接。跃点数表示流量从客户端流向服务器的 Citrix Gateway 设备的数量。连接链 ID 表示客户端与服务器之间的端到端连接。

Citrix ADM 使用跳数和连接链 ID 来关联来自两个 Citrix Gateway 设备的数据并生成报告。

要监视在此模式下部署的 Citrix Gateway 设备，必须先将 Citrix Gateway 添加到 Citrix ADM 清单，在 Citrix ADM 上启用 AppFlow，然后在 Citrix ADM 控制面板上查看报告。

在 **Citrix ADM** 上启用数据收集

如果启用 Citrix ADM 开始从两个装置收集 ICA 详细信息，则收集的详细信息将是冗余的。即两个设备报告相同的指标。要克服这种情况，您必须在第一台 Citrix Gateway 设备上启用适用于 ICA 的 AppFlow，然后在第二台设备上启用适用于 TCP 的 AppFlow。这样做，其中一个设备导出 ICA AppFlow 记录，另一个设备导出 TCP AppFlow 记录。这还节省解析 ICA 通信的处理时间。

要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到“网络”>“实例”，然后选择要启用分析的 Citrix ADC 实例。
4. 从选择操作下拉列表中，选择配置分析。
5. 选择 VPN 虚拟服务器，然后单击启用 **AppFlow**。
6. 在启用 **AppFlow** 字段中，键入 **true** ，然后分别为 ICA 流量和 TCP 流量选择 **ICA/TCP**。

   > 注意 如果未在 Citrix ADC 设备上为相应的服务或服务组启用 AppFlow 日志记录，则即使“洞察”列显示已启用，Citrix ADM 控制面板也不会显示记录。

7. 单击确定。

配置 **Citrix Gateway** 设备以导出数据

安装 Citrix Gateway 设备后，必须在 Citrix Gateway 设备上配置以下设置，以便将报告导出到 Citrix ADM：

- 在第一个和第二个 DMZ 中配置 Citrix Gateway 设备的虚拟服务器以相互通信。
- 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。
- 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
- 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。
- 允许其中一个 Citrix Gateway 设备导出 ICA 记录

- 允许其他 Citrix Gateway 设备导出 TCP 记录：
- 在两个 Citrix Gateway 设备上启用连接链接。

使用命令行界面配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 虚拟服务器配置为与第二个 DMZ 中的 Citrix Gateway 虚拟服务器进行通信。

   add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [**-secure**(ON or OFF)] [**-imgGifToPng**] …

   add vpn nextHopServer nh1 10.102.2.33 8443 –secure ON

2. 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。在第一个 DMZ 中的 Citrix Gateway 上运行以下命令：

   bind vpn vserver <name> **-nextHopServer** <name>

   bind vpn vserver vs1 -nextHopServer nh1

3. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点和 AppFlow。

   set vpn vserver <name> [**- doubleHop** (ENABLED or DISABLED)] [**- appflowLog** (ENABLED or DISABLED)]

   set vpn vserver vpnhop2 –doubleHop ENABLED –appFlowLog ENABLED

4. 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。

   set vpn vserver<name> [**-authentication** (ON or OFF)]

   set vpn vserver vs -authentication OFF

5. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。

   bind vpn vserver<name> [**-policy**<string>**-priority**<positive_integer>] [**-type**<type>]

   bind vpn vserver vpn1 -policy appflowpol1 -priority 101 –type OTHERTCP_REQUEST

6. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

   bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type ICA_REQUEST

7. 在两个 Citrix Gateway 设备上启用连接链接：

   set appFlow param [**-connectionChaining** (ENABLED or DISABLED)]

   set appflow param -connectionChaining ENABLED

使用配置实用程序配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix Gateway 绑定到第一个 DMZ 中的 Citrix Gateway。

a) 在“配置”选项卡上展开 **Citrix Gateway** ，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，并在“Advanced”（高级）组中，展开 **Published Applications**（发布的应用程序）。

c) 单击下一跳服务器 并将下一跳服务器绑定到第二个 Citrix Gateway 设备。

2. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。

a) 在“配置”选项卡上展开 **Citrix Gateway** ，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展开 **More**（更多），选择 **Double Hop**（双跃点）并单击 **OK**（确定）。

3. 在第二个 DMZ 中的 Citrix Gateway 上禁用虚拟服务器上的身份验证。

a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展开 **More**（更多），并取消选中 **Enable Authentication**（启用身份验证）。

4. 启用其中一个 Citrix Gateway 设备导出 TCP 记录。

a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，在“Advanced”（高级）组中，展开“Policies”（策略）。

c) 单击 + 图标，然后在“选择策略”下拉列表中选择 **AppFlow**，然后从“选择类型”下拉列表中选择“其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

5. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，然后在高级组中
展开策略。

c) 单击 + 图标，然后在“选择策略”下拉列表中选择 **AppFlow** ，然后从“选择类型”下拉列表中选择“其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

6. 在两个 Citrix Gateway 设备上启用连接链接。

a) 在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Appflow**。

b) 在右侧窗格的“设置”组中，单击“更改 **AppFlow** 设置”。

c) 选择 **Connection Chaining**（连接链）并单击 **OK**（确定）。

7. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix Gateway 绑定到第一个 DMZ 中的 Citrix Gateway。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在“高级”组中展开“已发布的应用程序”。

c) 单击下一跳服务器，然后将下一跳服务器绑定到第二台 Citrix Gateway 设备。

8. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展 开“更多 ”，选 择“双跳 ”，然后单击“** 确定”。

9. 在第二个 DMZ 中的 Citrix Gateway 上禁用虚拟服务器上的身份验证。

a) 在“配置”选项卡上，展开 Citrix Gateway，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展开 **More**（更多），并取消选中 **Enable Authentication**（启用身份验证）。

10. 启用其中一个 Citrix Gateway 设备导出 TCP 记录。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右侧窗格中，双击虚拟服务器，然后在高 级 组中展 开策略。

c) 单击 **+** 图标，然后在“选择策略”下拉列表中选择 **AppFlow**，然后从“选择类型”下拉列表中选择“其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

11. 允许其他 Citrix Gateway 设备导出 ICA 记录。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 **+** 图标，然后在“选择策略”下拉列表中选择 **AppFlow**，然后从“选择类型”下拉列表中选 择“其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

12. 在两个 Citrix Gateway 设备上启用连接链接。

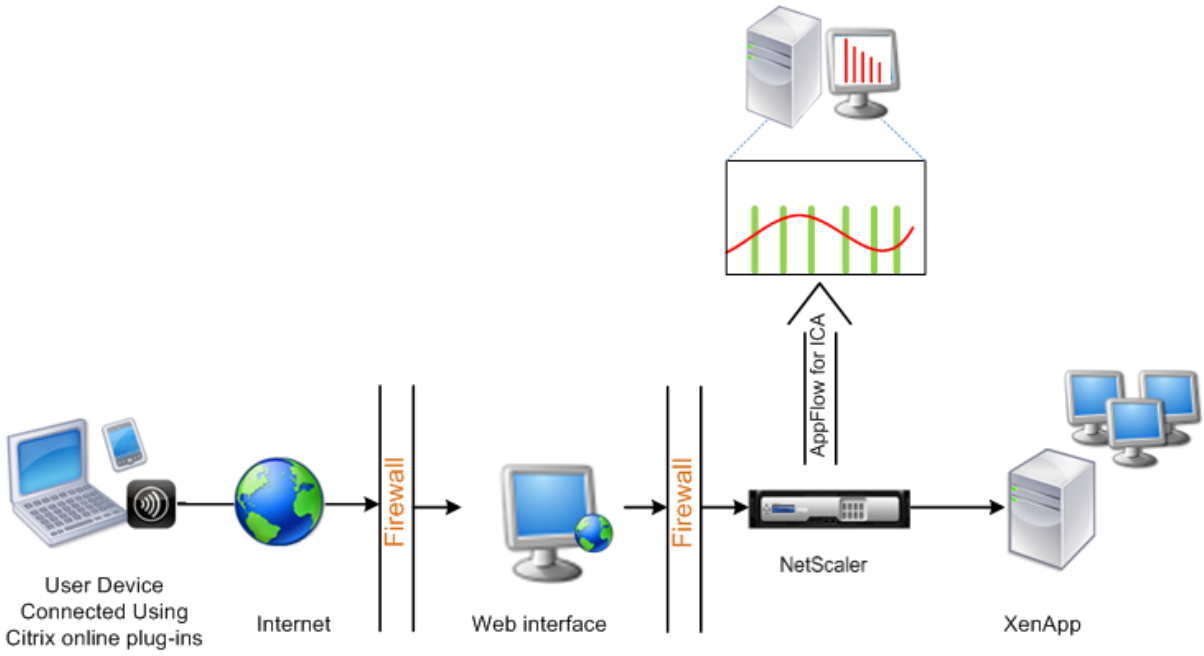
启用数据收集以监视在透明模式下部署的 **Citrix ADC**

当以透明模式部署 Citrix ADC 时，客户端可以直接访问服务器，而无需干预虚拟服务器。如果 Citrix ADC 设备在 Citrix Virtual Apps and Desktops 环境中以透明模式部署，ICA 流量不会通过 VPN 传输。

将 Citrix ADC 添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。启用数据收集依赖于设备和模式。在这种情况下，您必须在每台 Citrix ADC 设备上将 Citrix ADM 作为 AppFlow 收集器添加，并且必须配置 AppFlow 策略以收集流经该设备的全部或特定 ICA 流量。

> 注意
>
> - 无法使用 Citrix ADM 配置实用程序在透明模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。
> - 有关策略表达式的信息，请参阅策略和表达式。

下图显示了在透明模式下部署 Citrix ADC 时，Citrix ADM 的网络部署情况：



要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 指定 Citrix ADC 设备监听流量的 ICA 端口。

```
1 set ns param --icaPorts <port>...
2 <!--NeedCopy-->
```


示例：

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> 注意
>
> - 可以使用此命令最多指定 10 个端口。
> - 默认端口号为 2598。可以根据需要修改端口号。

3. 在 Citrix ADC 设备上添加 NetScaler Insight Center 作为 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> 注意要查看在 Citrix ADC 设备上配置的 AppFlow 收集器，请使用 **show appflow collector** 命令。

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

示例：

add appflow action act -collectors MyInsight

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

示例：

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```


> 注意要应用于 ICA 流量，**type** 的值应为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

示例：

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

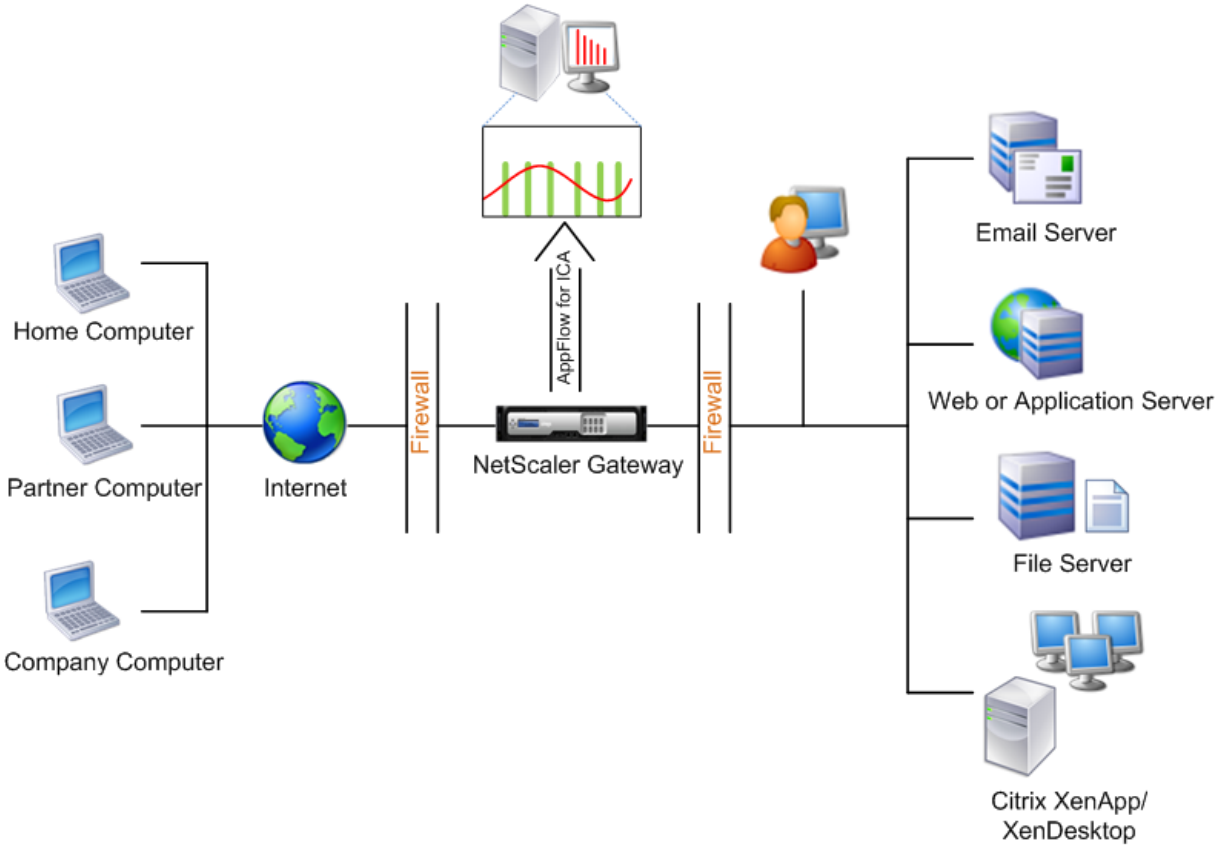
8. 保存配置。类型：`save ns config`

为在单跃点模式下部署的 **Citrix Gateway** 设备启用数据收集

February 6, 2024

在单跃点模式下部署 Citrix Gateway 时，它位于网络的边缘。网关实例提供与桌面交付基础架构的代理 ICA 连接。单跃点是最简单、最常见的部署。如果外部用户尝试访问组织中的内部网络，单跃点模式可提供安全性。
在单跃点模式下，用户通过虚拟专用网络 (VPN) 访问 Citrix ADC 设备。

要开始收集报告，必须将 Citrix Gateway 设备添加到 Citrix Application Delivery Management (ADM) 清单中，并在 ADM 上启用 AppFlow。



要从 **ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到基础架构 > 实例，然后选择要启用分析的 NetScaler 实例。
4. 从操作下拉列表中，选择启用/禁用 **Insight**。
5. 选择 **VPN** 虚拟服务器，然后单击启用 **AppFlow**。
6. 在“启用 **AppFlow**”字段中，键入 **true**，然后选择 **ICA**。
7. 单击确定。

> 注意 在单跃点模式下启用 AppFlow 时，以下命令将在后台执行。此处显式指定这些命令是为了进行故障排除。
>
> - 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

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则 Citrix ADM 上仍会显示剩余的 HDX Insight 数据。

启用数据收集以监视在透明模式下部署的 NetScaler ADC

February 6, 2024

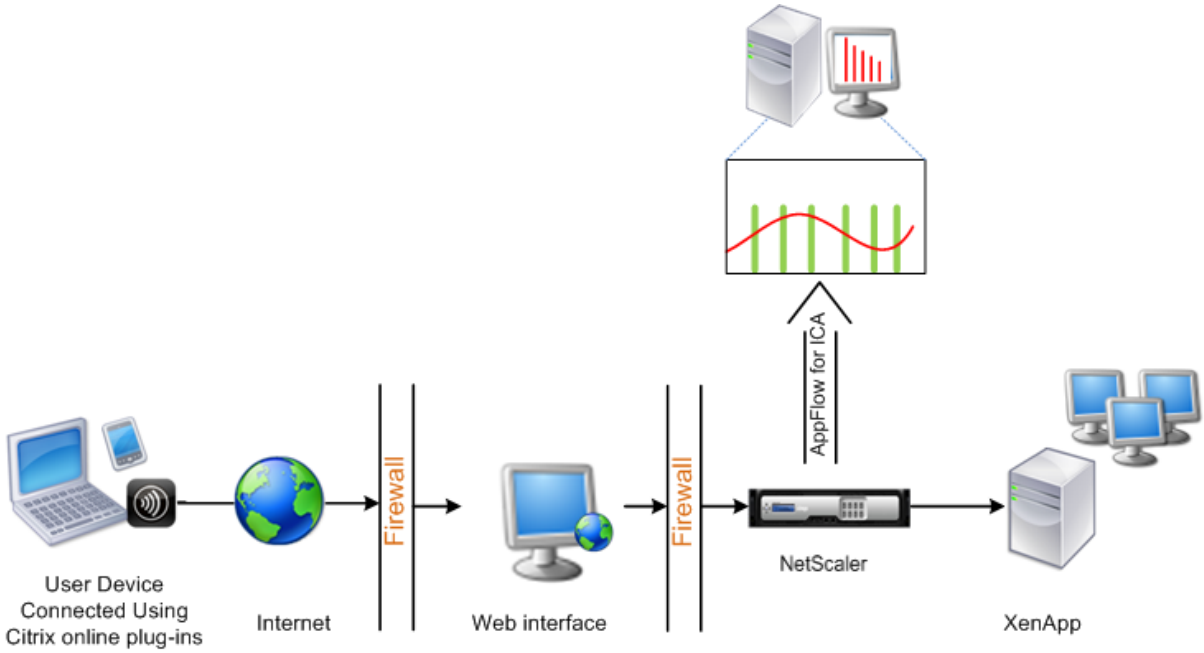
NetScaler ADC 以透明模式部署时，客户端可以直接访问服务器，不会干扰虚拟服务器。如果 NetScaler 设备在 Citrix Virtual Apps and Desktops 环境中以透明模式部署，则 ICA 流量不会通过 VPN 传输。

将 Citrix ADC 添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。启用数据收集依赖于设备和模式。在这种情况下，您必须将 Citrix ADM 作为 AppFlow 收集器添加到每台 NetScaler 设备上，并且必须配置 Appflow 策略以收集流经该设备的全部或特定 ICA 流量。

注意

- 使用 Citrix ADM 配置实用程序无法在以透明模式部署的 NetScaler ADC 上启用数据收集。
- 有关命令及其用法的详细信息，请参阅命令参考。
- 有关策略表达式的信息，请参阅策略和表达式。

下图显示了在透明模式下部署 NetScaler ADC 时 Citrix ADM 的网络部署：



要使用命令行界面在 **NetScaler** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 指定 NetScaler 设备侦听流量所用的 ICA 端口。

```
set ns param --icaPorts \<port\>...
<!--NeedCopy-->
```

示例：

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```

> 注意
>
> - 可以使用此命令最多指定 10 个端口。
> - 默认端口号为 2598。可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 NetScaler 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

示例：


```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> 注意 要查看在 NetScaler 设备上配置的 appflow 收集器，请使用 **show appflow collector** 命令。

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

示例：

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

示例：

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

注意要应用于 ICA 流量，类型的值应为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 保存配置。

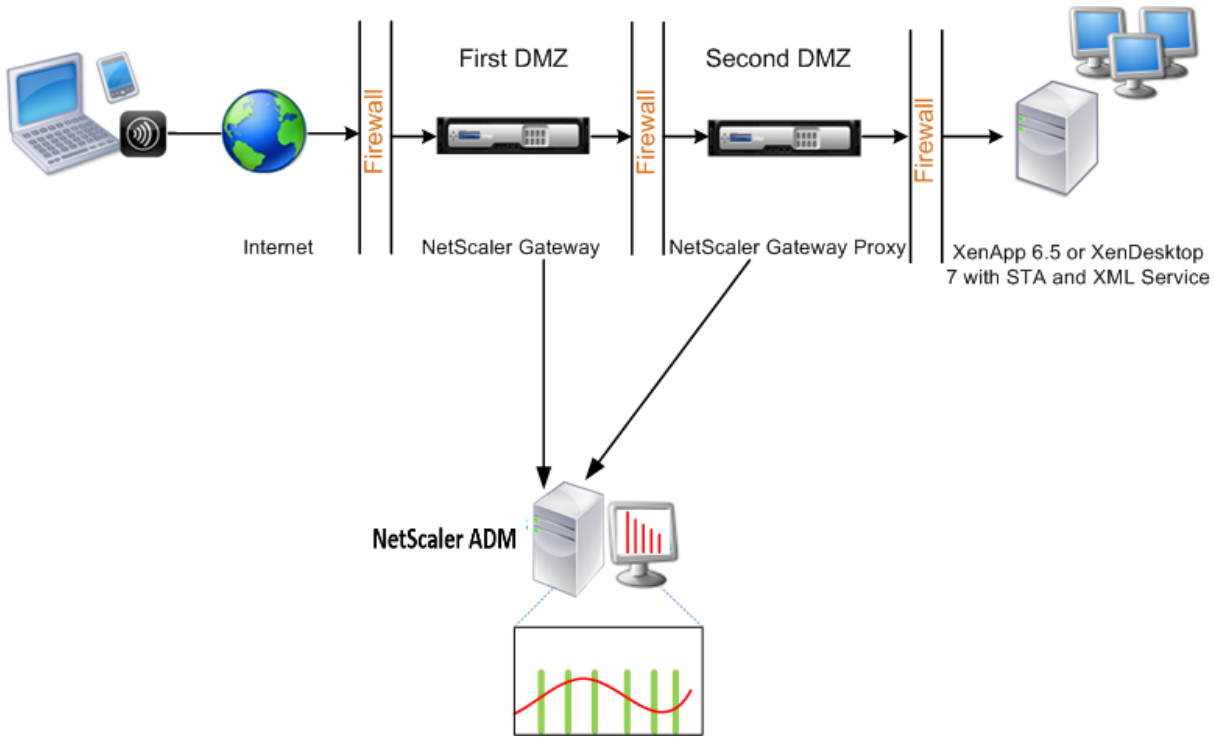
```
save ns config
<!--NeedCopy-->
```


为在双跃点模式下部署的 **Citrix Gateway** 设备启用数据收集

February 6, 2024

Citrix Gateway 双跳模式为组织的内部网络提供额外的保护，因为攻击者需要穿透多个安全区域或非军事区域 (DMZ) 才能访问安全网络中的服务器。如果要分析 ICA 连接通过的跃点数（Citrix Gateway 装置），以及有关每个 TCP 连接上延迟的详细信息，以及它如何与客户端感知到的总 ICA 延迟展开，则必须安装 Citrix ADM，以便 Citrix Gateway 设备报告这些生命统计数据。

图 3. Citrix ADM 在双跃点模式下部署



第一个 DMZ 中的 Citrix Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 Citrix Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 Citrix Gateway 充当 Citrix Gateway 代理设备。此 Citrix Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。

Citrix ADM 可以部署在属于第一个 DMZ 中 Citrix Gateway 设备的子网中，也可以部署在属于 Citrix Gateway 设备的第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 Citrix ADM 和 Citrix Gateway 部署在同一个子网中。

在双跃点模式下，Citrix ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 Citrix Gateway 设备添加到 Citrix ADM 清单并启用数据收集后，每台设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 Citrix ADM 识别哪个装置正在导出记录，每个装置都会使用跳数指定，并使用连接链 ID 指定每个连接。跃点数表示流量从客户端流向服务器的 Citrix Gateway 设备的数量。连接链 ID 表示客户端与服务器之间的端到端连接。

Citrix ADM 使用跳数和连接链 ID 来关联来自两个 Citrix Gateway 设备的数据并生成报告。

要监视在此模式下部署的 Citrix Gateway 设备，必须先将 Citrix Gateway 添加到 Citrix ADM 清单，在 Citrix ADM 上启用 AppFlow，然后在 Citrix ADM 控制面板上查看报告。

在 **Citrix ADM** 上启用数据收集

如果启用 Citrix ADM 开始从两个装置收集 ICA 详细信息，则收集的详细信息将是冗余的。即两个设备报告相同的指标。要克服这种情况，必须在第一台 Citrix Gateway 设备之一上启用适用于 TCP 的 AppFlow，然后在第二台设备上启用适用于 ICA 的 AppFlow。这样做，其中一个设备导出 ICA AppFlow 记录，另一个设备导出 TCP AppFlow 记录。这还节省解析 ICA 通信的处理时间。

要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到基础架构 > 实例，然后选择要启用分析的 NetScaler 实例。
2. 从操作下拉列表中，选择启用/禁用 **Insight**。
3. 选择 VPN 虚拟服务器，然后单击启用 **AppFlow**。
4. 在启用 **AppFlow** 字段中，键入 **true** ，然后分别为 ICA 流量和 TCP 流量选择 **ICA/TCP**。

   > 注意：如果未为 NetScaler 设备上的相应服务或服务组启用 AppFlow 日志记录，即使 Insight 列显示为已启用，Citrix ADM 控制板也不会显示记录。

5. 单击确定。

配置 **Citrix Gateway** 设备以导出数据

安装 Citrix Gateway 设备后，必须在 Citrix Gateway 设备上配置以下设置，以便将报告导出到 Citrix ADM：

- 在第一个和第二个 DMZ 中配置 Citrix Gateway 设备的虚拟服务器以相互通信。
- 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。
- 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
- 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。
- 允许其中一个 Citrix Gateway 设备导出 ICA 记录
- 允许其他 Citrix Gateway 设备导出 TCP 记录：
- 在两个 Citrix Gateway 设备上启用连接链接。

使用命令行界面配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 虚拟服务器配置为与第二个 DMZ 中的 Citrix Gateway 虚拟服务器进行通信。

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
<!--NeedCopy-->
```

2. 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。在第一个 DMZ 中的 Citrix Gateway 上运行以下命令：

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点和 AppFlow。

set vpn vserver [**- doubleHop** (ENABLED	DISABLED)] [**- appflowLog** (ENABLED	DISABLED)]

```
set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
<!--NeedCopy-->
```

4. 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。

set vpn vserver [**-authentication** (ON	OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

   bind vpn vserver<name> [**-policy**<string> **-priority**<positive_integer>] [**-type**<type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. 在两个 Citrix Gateway 设备上启用连接链接：

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

使用配置实用程序配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix Gateway 绑定到第一个 DMZ 中的 Citrix Gateway。
   a) 在配置选项卡上，展开 **Citrix Gateway**，然后单击虚拟服务器。
   b) 在右侧窗格中，双击虚拟服务器，并在“Advanced”（高级）组中，展开 **Published Applications**（发布的应用程序）。
   c) 单击下一跃点服务器，然后将下一跃点服务器绑定到第二个 Citrix Gateway 设备。
2. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
   a) 在“配置”选项卡上展开 **Citrix Gateway** ，然后单击“虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。
   c) 展开 **More**（更多），选择 **Double Hop**（双跃点）并单击 **OK**（确定）。
3. 在第二个 DMZ 中的 Citrix Gateway 上禁用虚拟服务器上的身份验证。
   a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在基本设置 组中单击编辑图标。
   c) 展开 **More**（更多），并取消选中 **Enable Authentication**（启用身份验证）。
4. 启用其中一个 Citrix Gateway 设备导出 TCP 记录。
   a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。
   b) 在右侧窗格中，双击虚拟服务器，在“Advanced”（高级）组中，展开“Policies”（策略）。
   c) 单击 + 图标，然后从“选择策略”列表中选择 **AppFlow**，然后从“选择类型”列表中选择“其他 **TCP** 请求”。
   d) 单击 继续。
   e) 添加策略绑定，并单击 **Close**（关闭）。
5. 启用其他 Citrix Gateway 设备以导出 ICA 记录：
   a) 在“配置”选项卡上，展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 + 图标，然后从“选择策略”下拉列表中选择 **AppFlow**，然后从“选择类型”列表中选择“其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

6. 在两个 Citrix Gateway 设备上启用连接链接。

a) 在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Appflow**。

b) 在右侧窗格的“设置”组中，单击“更改 **AppFlow** 设置”。

c) 选择 **Connection Chaining**（连接链）并单击 **OK**（确定）。

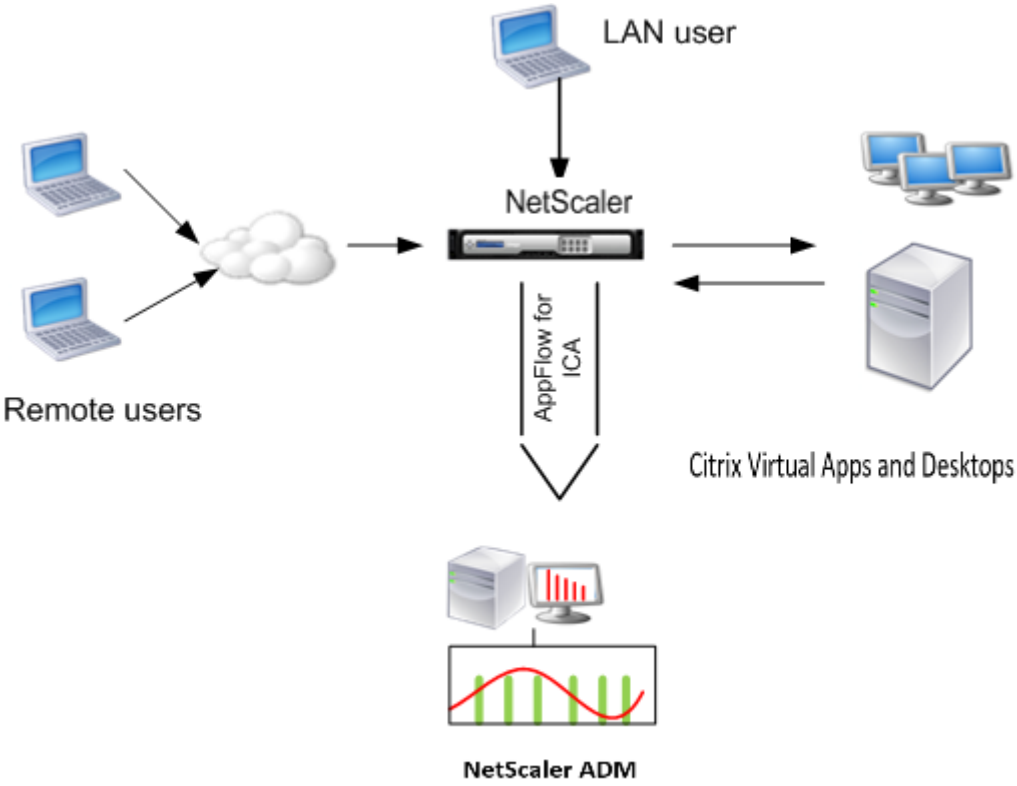
启用数据收集以监视在局域网用户模式下部署的 NetScaler ADC

February 6, 2024

访问 Citrix Virtual Apps and Desktops 应用程序的外部用户必须在 Citrix Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 Citrix Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便请求重定向至 NetScaler 设备。

要克服这些挑战，并让局域网用户直接连接到 Citrix Virtual Apps and Desktops 应用程序，您可以通过配置缓存重定向虚拟服务器（该服务器充当 Citrix Gateway 设备上的 SOCKS 代理）以 LAN 用户模式部署 NetScaler 设备。

图 4. 在局域网用户模式下部署的 Citrix ADM



> 注意
>
> Citrix ADM 和 Citrix Gateway 设备位于同一个子网中。

要监视在此模式下部署的 Citrix 设备，请先将 Citrix 设备添加到 NetScaler Insight 清单中，启用 AppFlow，然后在控制面板上查看报告。

将 Citrix 设备添加到 Citrix ADM 清单后，必须启用 AppFlow 进行数据收集。

> 注意
>
> - 使用 NetScaler ADC 配置实用程序无法在局域网用户模式下部署的 Citrix ADM 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅“命令参考”。
> - 有关策略表达式的信息，请参阅“策略和表达式”。

要使用命令行界面在 **NetScaler** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 添加转发代理缓存重定向虚拟服务器并提供代理 IP 和端口，指定服务类型为 HDX。

```
1 add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
     cacheType <cachetype>] [ - cltTimeout <secs>]
2 <!--NeedCopy-->
```


示例：

```
add cr vserver cr1 HDX 10.12.2.2 443  -cacheType FORWARD  -
    cltTimeout 180
<!--NeedCopy-->
```

> 注意：如果您使用 Citrix Gateway 设备访问 LAN 网络，请添加要由匹配 VPN 流量的策略应用的操作。

```
add vpn trafficAction** \<name\> \<qual\> \[-HDX ( ON | OFF )\]

add vpn trafficPolicy** \<name\> \<rule\> \<action\>
<!--NeedCopy-->
```

示例：

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. 将 Citrix ADM 添加为 Citrix ADC 设备上的 AppFlow 收集器。

```
add appflow collector** \<name\> \*\*-IPAddress\*\* \\<ip\\_addr
    \\>
<!--NeedCopy-->
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action** \<name\> \*\*-collectors\*\* \<string\> ...
<!--NeedCopy-->
```

示例：

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy** \<policyname\> \<rule\> \<action\>
<!--NeedCopy-->
```

示例：

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。


```
bind appflow global** \<policyname\> \<priority\> \*\*-type\*\* \<
    type\>
<!--NeedCopy-->
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> 注意 要应用于 ICA 流量，类型的值应为 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

示例：

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 保存配置。

```
save ns config
<!--NeedCopy-->
```

为 **HDX Insight** 创建阈值并配置警报

February 6, 2024

Citrix Application Delivery Management (ADM) 上的 HDX Insight 允许您监视通过 Citrix ADC 实例的 HDX 流量。Citrix ADM 允许您在用于监视智能分析通信量的各种计数器上设置阈值。您还可以在 Citrix ADM 中配置规则和创建警报。

HDX 流量类型与各种实体（如应用程序、桌面、网关、许可证和用户）相关联。每个实体都可以包含与其关联的不同指标。例如，应用程序实体与命中次数、应用程序消耗的带宽和服务器的响应时间相关联。用户实体可以与用户使用的 WAN 延迟、DC 延迟、ICA RTT 和带宽相关联。

Citrix ADM 中的 HDX Insight 阈值管理允许您在突破设置的阈值时主动创建规则和配置警报。现在，此阈值管理已扩展到配置一组阈值规则。现在，您可以监视组而不是单个规则。阈值规则组由从用户、应用程序和桌面等实体中选择的指标的一个或多个用户定义的阈值规则组成。每个规则都会根据您在创建规则时输入的预期值进行监视。对于用户实体，阈值组也可以与地理位置相关联。

仅当违反了配置的阈值组中的所有规则时，才会在 Citrix ADM 上生成警报。例如，您可以根据会话启动总数监视应用程序，也可以将应用程序启动计数作为一个阈值组进行监视。只有在违反两条规则时才会生成警报。这允许您在实体上设置更真实的阈值。

下面列出了几个示例：

- 阈值规则 1：用户（实体）的 ICA RTT（指标）应小于 100 毫秒
- 阈值规则 2：用户（实体）的 WAN 延迟（指标）应小于 100 毫秒

阈值组的示例可以是：{阈值规则 1 + 阈值规则 2}

要创建规则，应首先选择要监视的实体。然后在创建规则时选择指标。例如，您可以选择应用程序实体，然后选择会话启动总计数或应用程序启动计数。您可以为实体和指标的每种组合创建一条规则。使用提供的比较器（>、<、>= 和 <=），键入每个指标的阈值。

> 注意
>
> 如果您不想监视单个组中的多个实体，则必须为每个实体创建一个单独的阈值规则组。

当计数器的值超过阈值时，Citrix ADM 会生成一个事件以表示违反阈值，并为每个事件创建警报。

您必须配置接收警报的方式。您可以允许警报在 Citrix ADM 上显示和/或通过电子邮件或短信在移动设备上接收警报。对于最后两个操作，您必须在 Citrix ADM 上配置电子邮件服务器或 SMS 服务器。

阈值组也可以绑定到地理位置，以便对用户实体进行特定地理监视。

用例示例

ABC Inc. 是一家全球性的公司，在 50 多个国家设有办事处。该公司有两个数据中心，一个位于新加坡，另一个位于加利福尼亚州，负责托管 Citrix Virtual Apps and Desktops。公司的员工使用 Citrix Gateway 和基于 Citrix GSLB 的重定向访问全球各地的 Citrix Virtual Apps and Desktops。ABC Inc. 的 Citrix Virtual Apps and Desktops 管理员 Eric 希望跟踪其所有办公室的用户体验，以便优化应用程序和桌面交付，以便随时随地访问。Eric 还希望检查用户体验指标，如 ICA RTT，延迟，并主动提出任何偏差。

ABC Inc. 的用户有一个分布式的存在。有些用户位于数据中心附近，而另一些用户则位于离数据中心更远的地方。随着用户群的分布广泛，指标和相应的阈值也因这些位置而异。例如，数据中心附近位置的 ICA RTT 可能为 5-10 毫秒，而远程位置的 ICA RTT 可能约为 100 毫秒。

借助 HDX Insight 的阈值规则组管理，Eric 可以为每个位置设置特定于地理位置的阈值规则组，并通过电子邮件或短信收到每个区域的违规警报。Eric 还能够将对阈值规则组中多个指标的跟踪结合起来，并将根本原因缩小到容量问题（如果有）。Eric 现在能够主动跟踪任何偏差，而不必担心手动查看所有 Citrix Virtual Apps and Desktops 产品组合指标的复杂性。

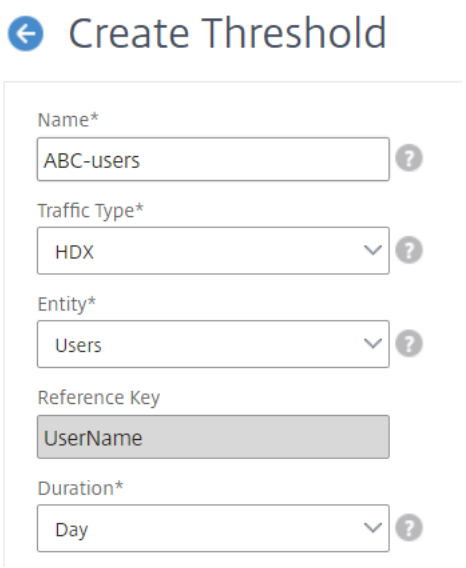
要使用 **Citrix ADM** 创建阈值规则组并为 **HDX Insight** 配置警报，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 > 设置 > 阈值。在打开的阈值页面上，单击添加。
2. 在 **Create Thresholds and Alerts**（创建阈值和警报）页面上，指定以下详细信息：
    a) 名称。键入用于创建 Citrix ADM 生成警报的事件的名称。
    b) 流量类型。从下拉列表框中选择 HDX。

c) 实体。从下拉列表框中选择类别或资源类型。您之前选择的每种流量类型的实体不同。

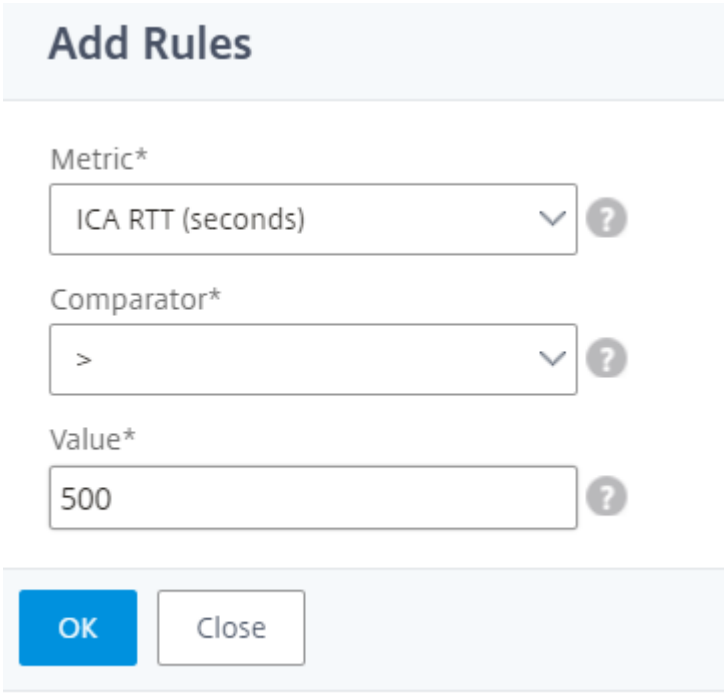
d) 参考键。参考密钥是根据您选择的流量类型和实体自动生成的。

e) 持续时间。从下拉列表框中，选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。



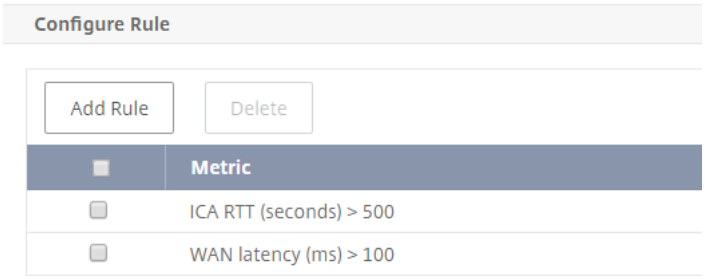
3. 为所有实体创建阈值规则组：

对于 HDX 流量，必须通过单击“添加规则”来创建规则。在打开的“添加规则”弹出窗口中输入值。



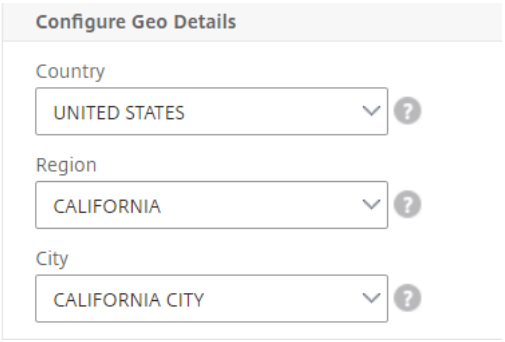
您可以创建多个规则来监视每个实体。在一个组中创建多个规则允许您将实体作为一组阈值规则而不是单个规则

进行监视。单击确定关闭窗口。



4. 配置用户实体的地理位置标记

   或者，您可以在“配置地理详细信息”部分中为用户实体创建基于位置的警报。下图显示了创建基于地理位置的标记以监视美国西海岸用户 WAN 延迟性能的示例。



5. 单击启用阈值以允许 Citrix ADM 开始监视实体。
6. （可选）配置操作，如电子邮件通知和 SMS 通知。
7. 单击创建以创建阈值规则组。

查看 **HDX Insight** 报告和指标

February 6, 2024

HDX Insight 提供与 Citrix ADC 实例上的 HDX 流量相关的报告和指标的完整可见性。

您可以查看任何选定实体的 HDX 指标。视图中包括以下类别的实体：

- 用户：显示在选定时间间隔内访问 Citrix Virtual Apps and Desktops 的所有用户的报告。
- 应用程序：显示应用程序总数的报告以及所有相关信息，例如在指定时间间隔内启动应用程序的总次数。
- 实例：显示用作传入流量网关的 Citrix ADC 实例的报告。
- 桌面：显示在选定时间范围内使用的桌面的报告。
- 许可证：显示指定时段内使用的 SSL VPN 许可证总数的报告。

> 注意
>
> “许可证”值不适用于 Citrix SD-WAN 设备。

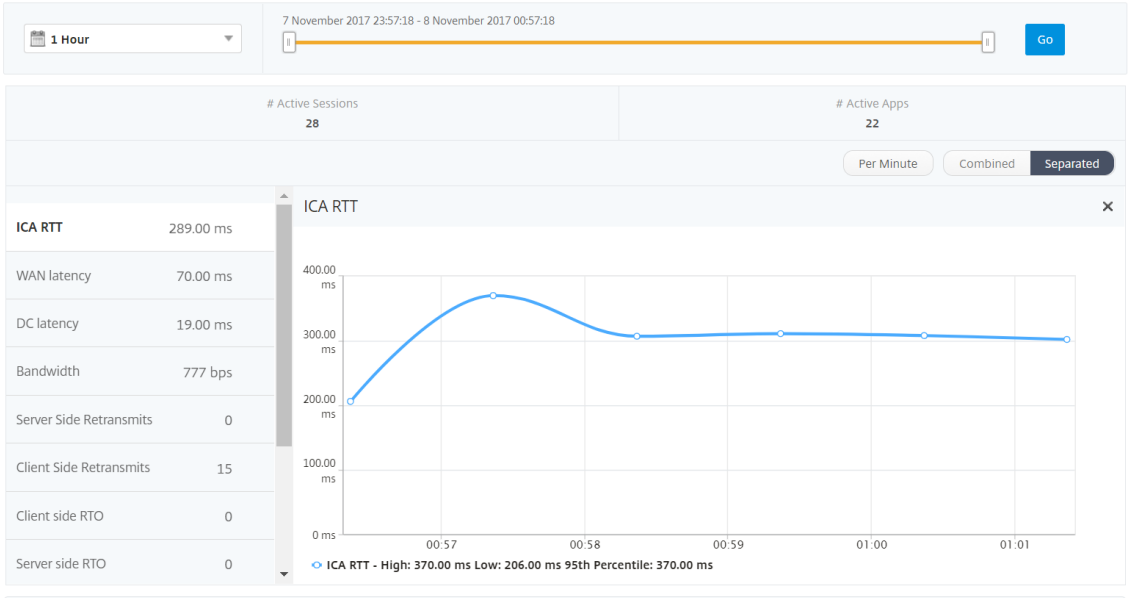
用户视图报告和指标

2017 年 11 月 6 日

此视图中的报告和衡量指标按照 Citrix Virtual Apps and Desktops 用户显示。

要导航到“用户”视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户



“User”（用户）视图报告和指标包括以下部分：

- Summary View（摘要视图）
- Per User View（每个用户视图）
- Per User Session View（每个用户会话视图）

Summary View（摘要视图）

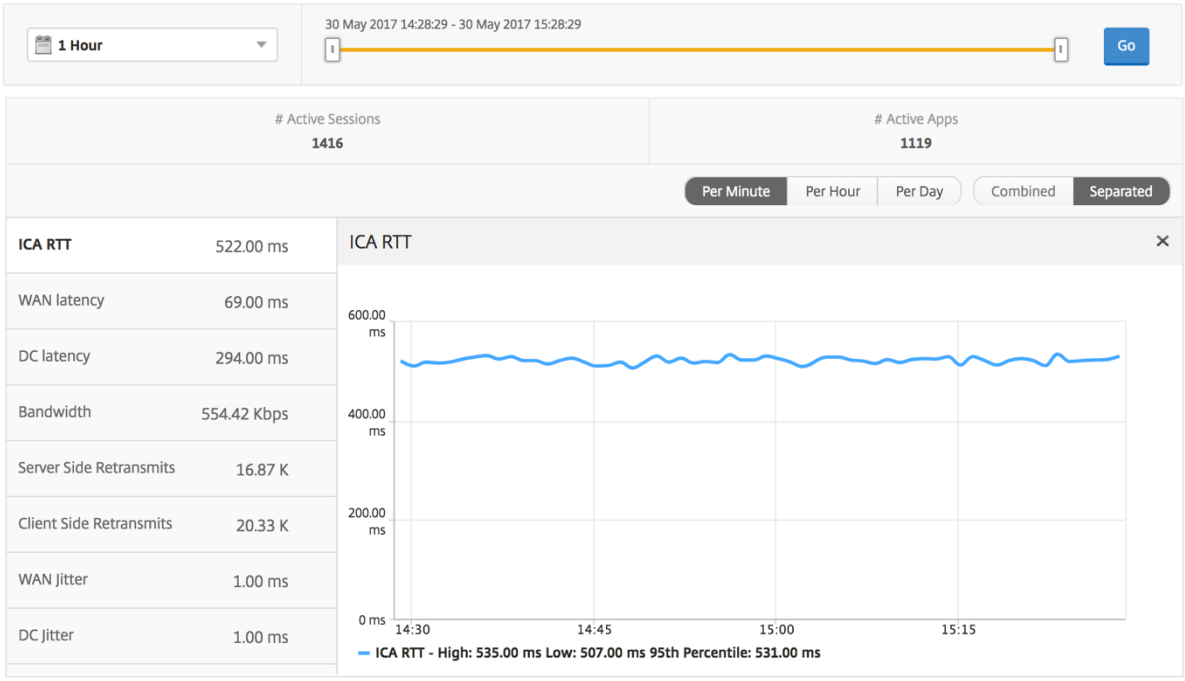
“Summary View”（摘要视图）显示在选定时间线内登录的所有用户的报告。除非另有说明，否则此视图中的所有指标/报告均显示选定时间段内与这些用户对应的值。

要更改选定时间段，请执行以下操作：

1. 使用时间段列表或时间滑块设置所需的时间间隔。
2. 单击转到。

折线图

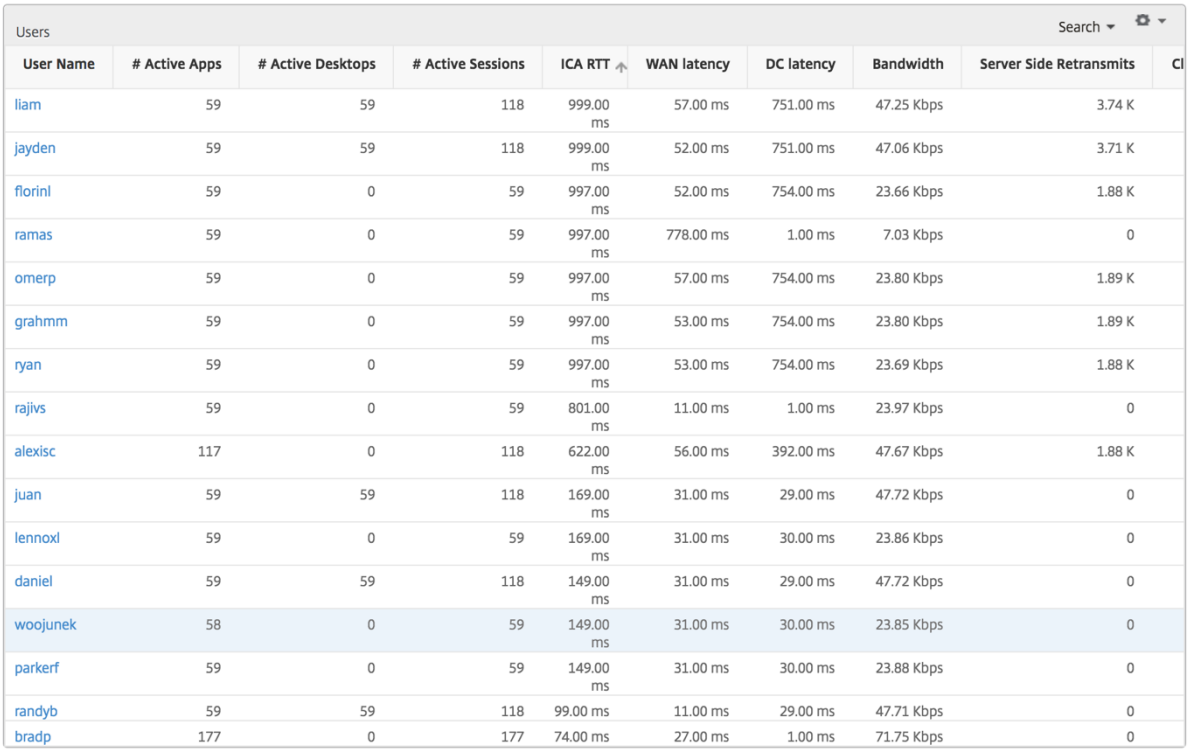
指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



用户摘要报告　下面是与此报告特定相关的指标。

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Total App Launch Count（应用程序启动总数）	在选定的时间段内用户启动的应用程序总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。

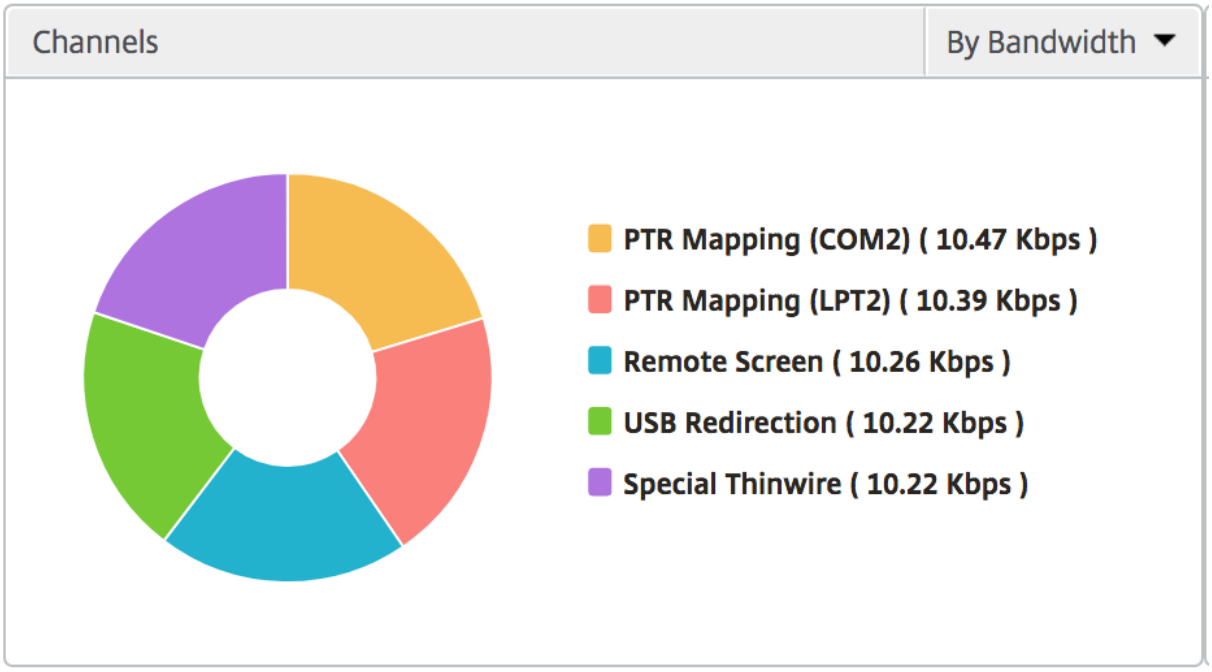


Users

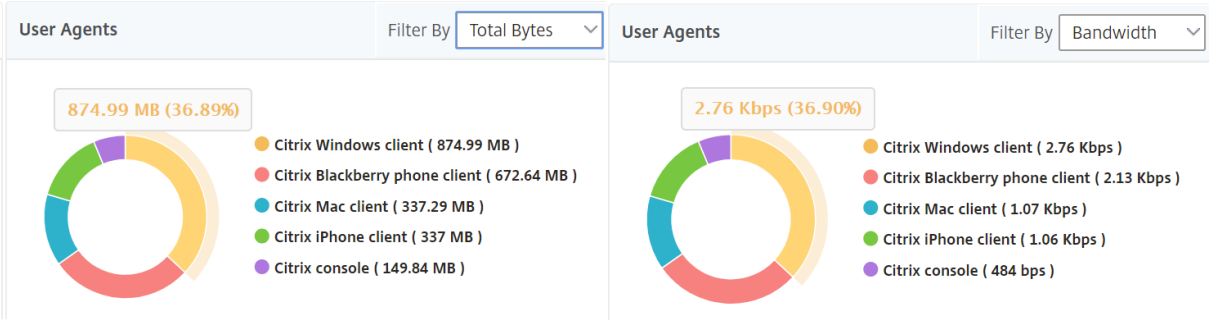
Search

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	

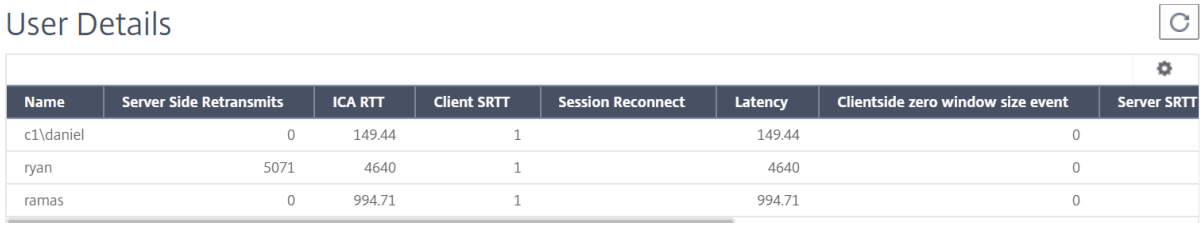
Channels（通道） “Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



User Agents（用户代理） 用户代理以甜圈图表的形式表示每个 Receiver 客户端使用的总带宽/总字节。图表中的每个彩色段代表一个 Receiver 客户端。分段的长度取决于在该接收方客户端上启动其应用程序的用户数量。您还可以按带宽或总字节对指标进行排序。



单击每个区段以查看使用该 Receiver 客户端的用户的详细信息。

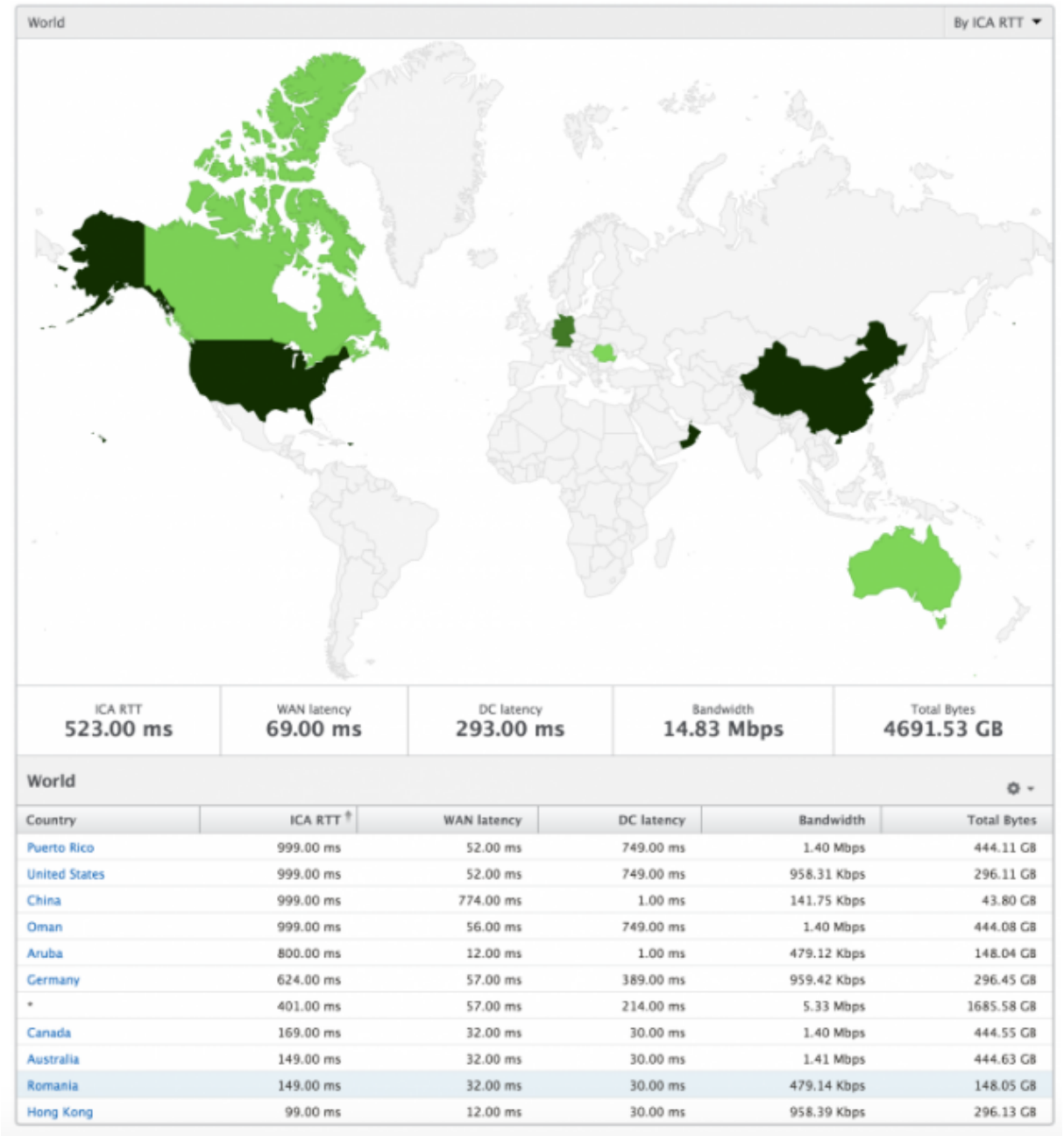


阈值违规计数 阈值违反计数指标表示在选定时间段内违反的阈值计数。

世界地图　通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市以及通过单击区域。管理员可以进一步向下钻取以按城市和州查看信息。从 Citrix ADM 12.0 及更高版本中，您可以深入查看从地理位置连接的用户。

以下详细信息可以在 HDX Insight 的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



每用户视图

“Per User View”（每个实例视图）提供任何特定的选定用户的详细最终用户体验报告。

要导航到特定用户的度量，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户。
3. 从“User Summary Report”（用户摘要报告）部分中选择特定用户。

折线图　折线图显示在选定时间段内特定的选定用户的所有指标摘要。

当前/已终止会话报告　此报告与选定用户的所有当前/已终止用户会话有关。这些指标可以按开始时间、会话重新连接和 ACR 计数进行排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致通过 Citrix ADC 传输的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。

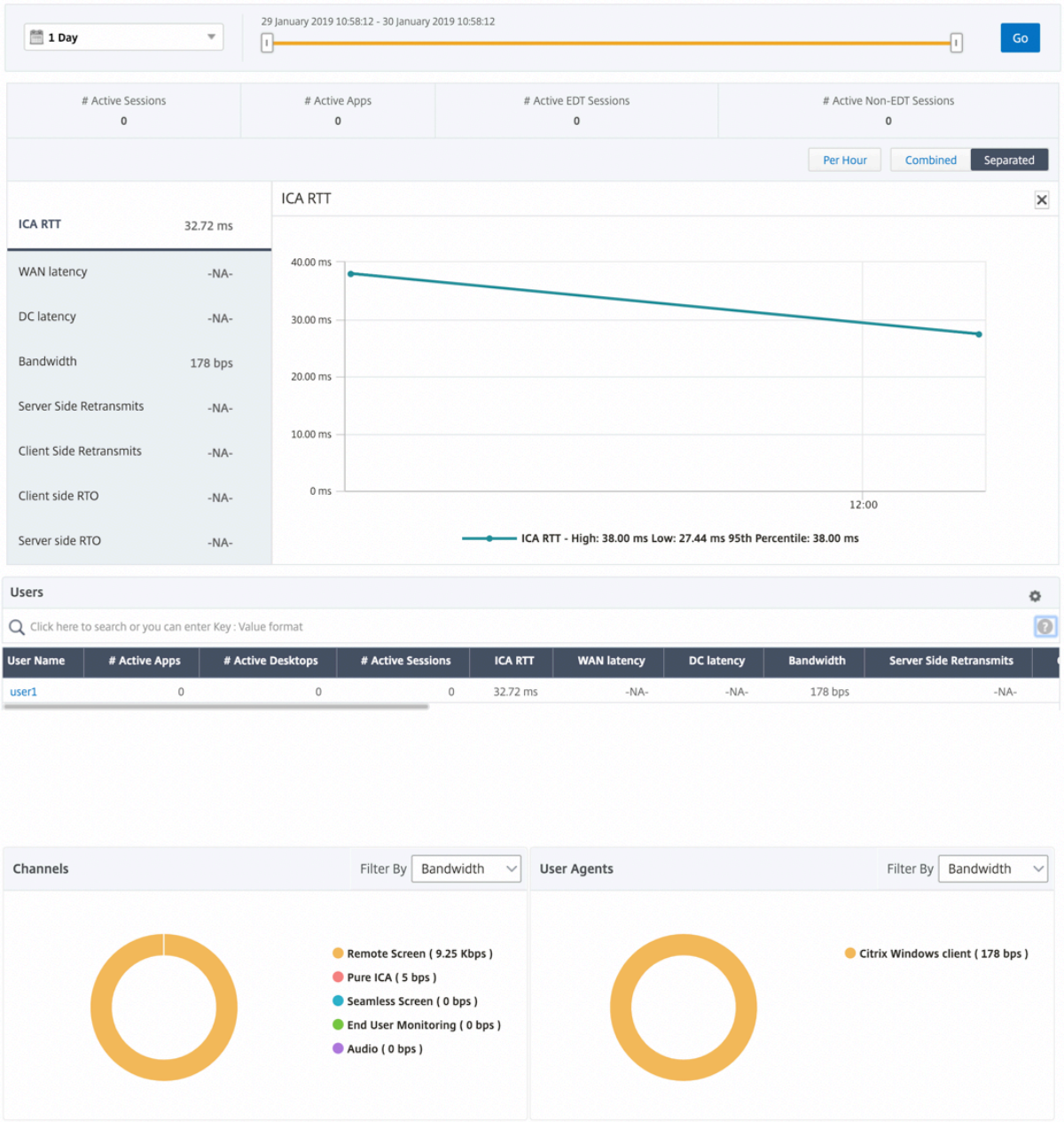
指标	说明
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。

支持 **HDX Insight** 中的 **EDT**

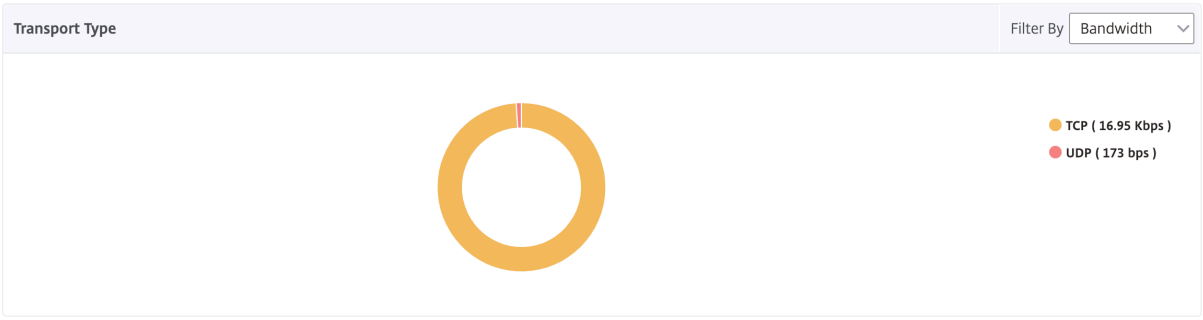
Citrix Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示 HDX Insight 的分析信息。也就是说, ADM 现在同时支持 UDP 和 TCP 协议。对 Citrix Gateway 的 EDT 支持可确保运行 Citrix Receiver 的用户在虚拟桌面中获得高清晰度的会话中用户体验。

HDX Insight 现在在活动会话报告中显示 EDT 会话和非 EDT 会话的数量。“用户”(Users) 表格显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传、RTO 等衡量指标，以及当前从 TCP 堆栈计算时确实具有 EDT

会话的用户不可用。因此，它们将显示为“NA”。



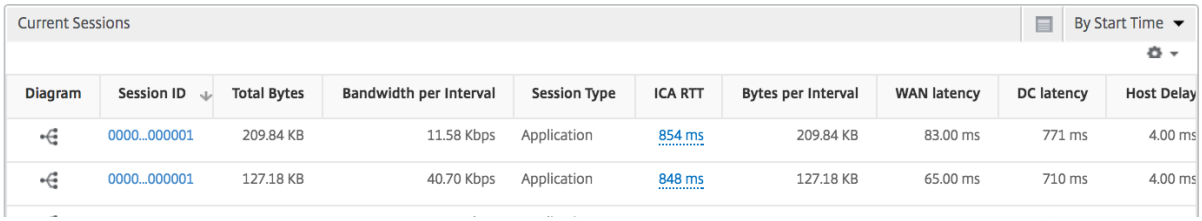
引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。

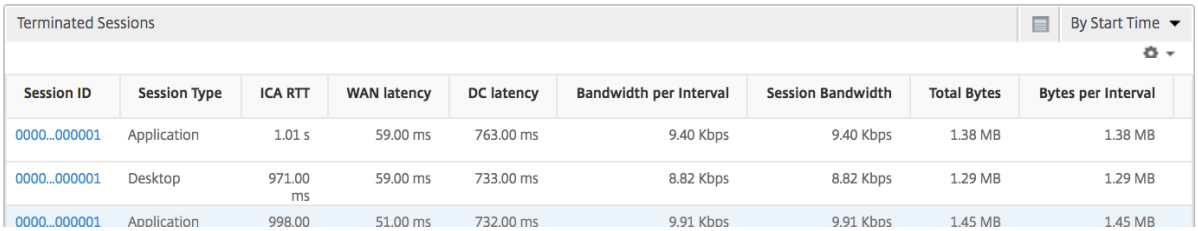


> 注意：从版本 12.1 版本 50.28 开始的 Citrix ADM 支持 HDX Insight 能分析中的 EDT，并且在版本 12.1 版本 49.23 开始的 ADC 实例上可用。

Citrix ADM 12.0 及更高版本中提供的 **HDX Insight** 分析指标：

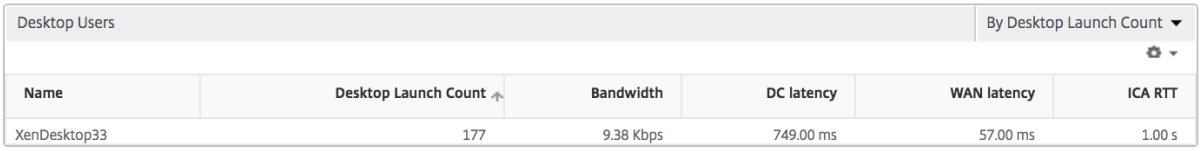
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。
L7 Server-side Latency（L7 服务器端延迟）	Citrix ADC 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。



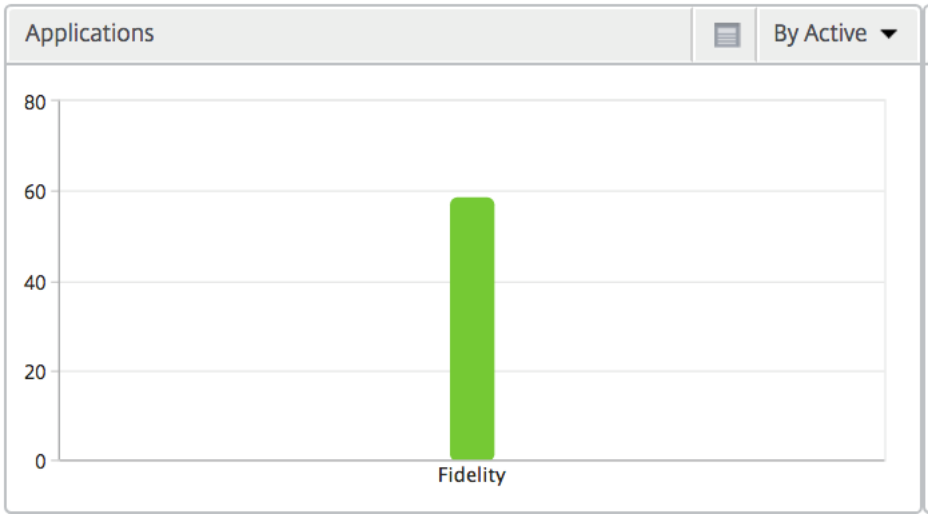


桌面用户　此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

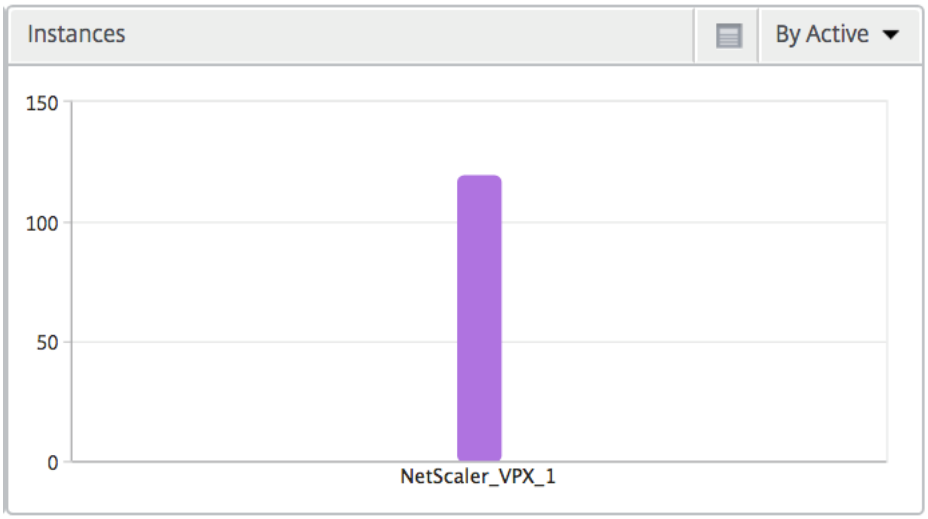
指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。



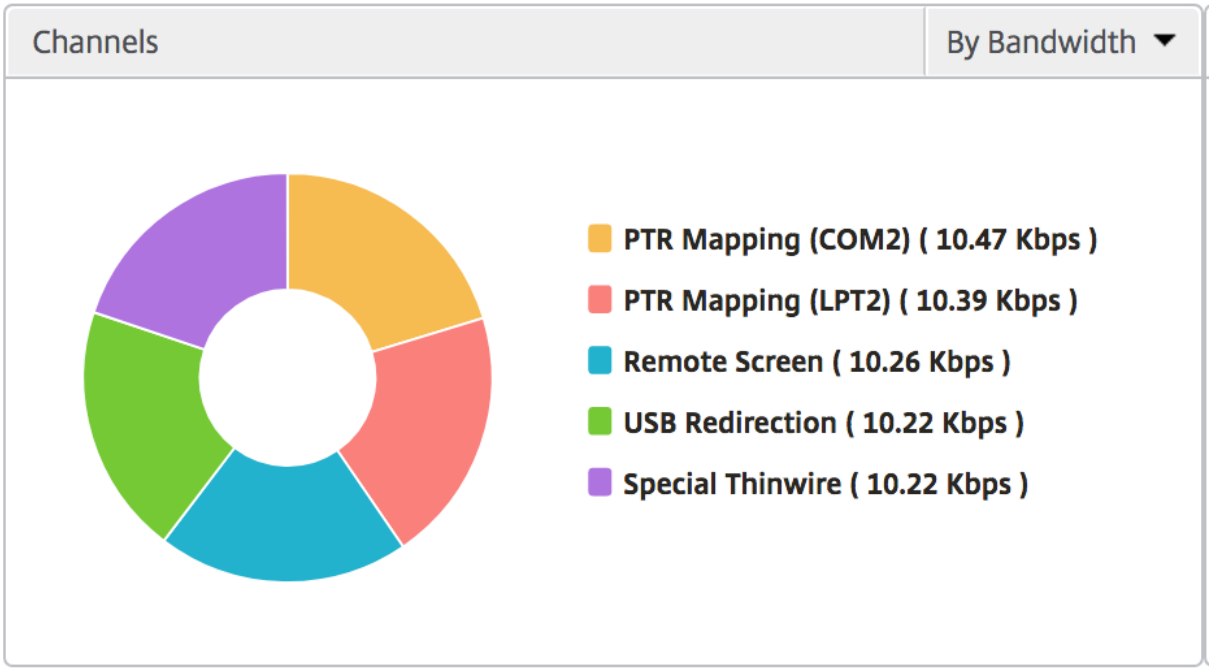
应用程序　表示按活动、会话启动总数、应用程序启动总数和启动持续时间排序的应用程序的条形图。



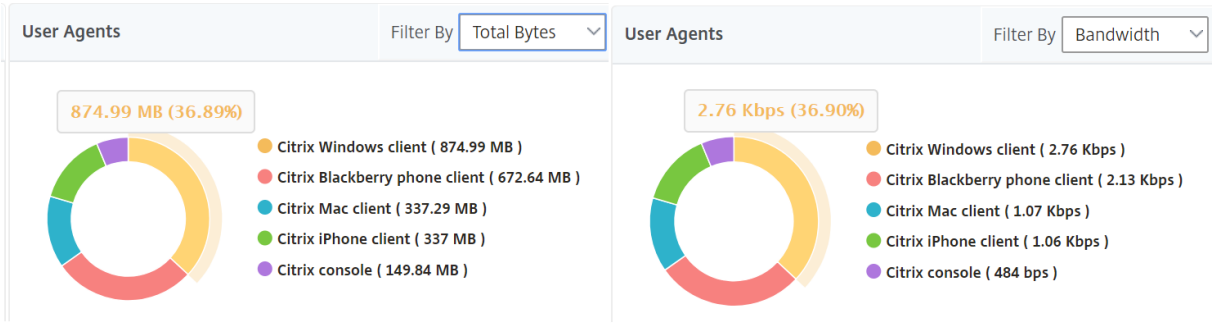
实例　表示按活动应用程序和总应用程序排序的 Citrix ADC 实例的条形图



Channels（通道） “Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



User Agents（用户代理） “User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



每用户会话视图 “Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

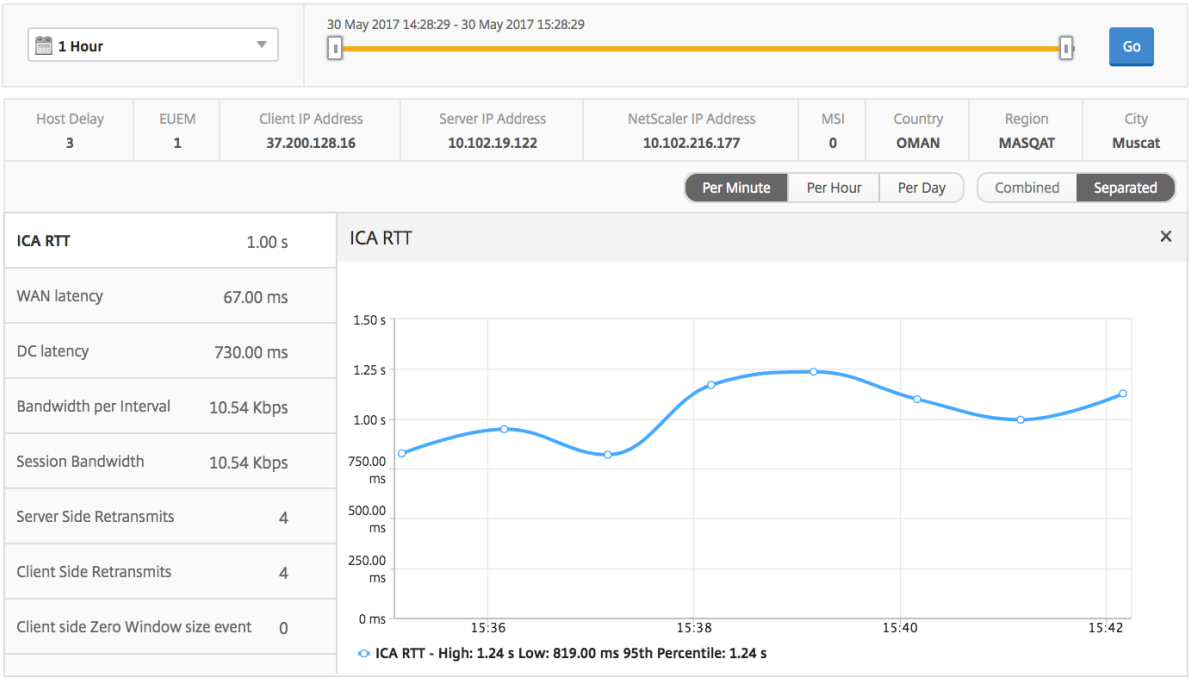
要查看选定用户会话的度量，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户。
3. 从用户摘要报告部分选择特定用户。
4. 从当前会话或已终止的会话列中选择一个会话。

时间线图

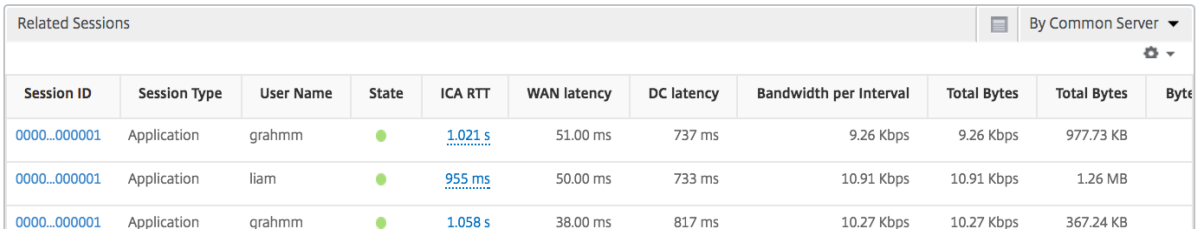
指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



活动应用程序　活动应用程序部分显示选定用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间排序。

Related Sessions（相关会话）　“Related Sessions”（相关会话）部分显示选定用户的会话的相关会话。可以选择该关系作为公用服务器或通用 Citrix ADC。



应用程序视图报告和指标

此视图中的报告和衡量指标侧重于 Citrix Virtual Apps。

要导航到“应用程序”视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到“分析”> “**HDX Insight**”> “应用程序”。

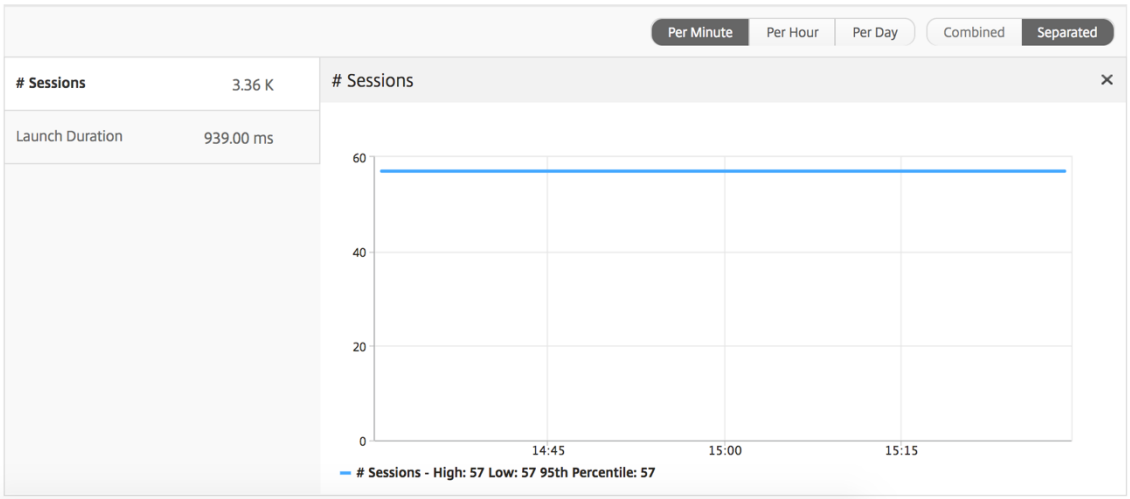
Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有应用程序的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

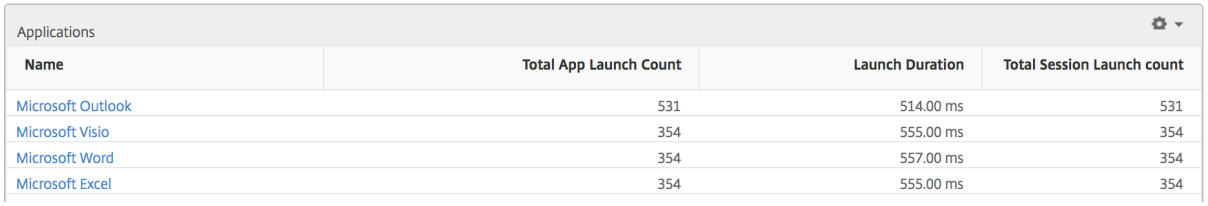
折线图

指标	说明
Sessions（会话数）	在给定时间间隔内的会话总数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。



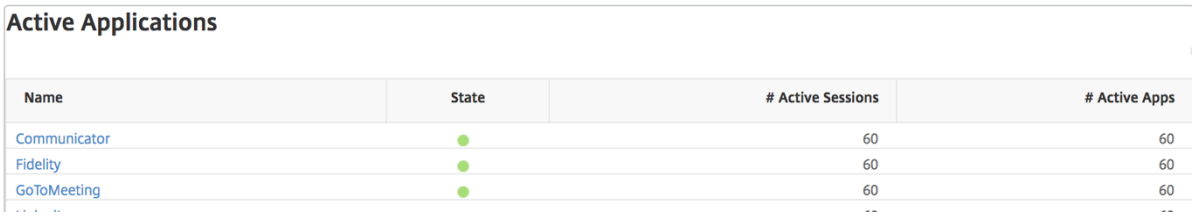
应用程序摘要报告

指标	说明
名称	Citrix Virtual Apps 的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix Virtual Apps 总数。
Launch Duration（启动持续时间）	启动 Citrix 虚拟应用程序所需的平均时间。



活动应用程序报告

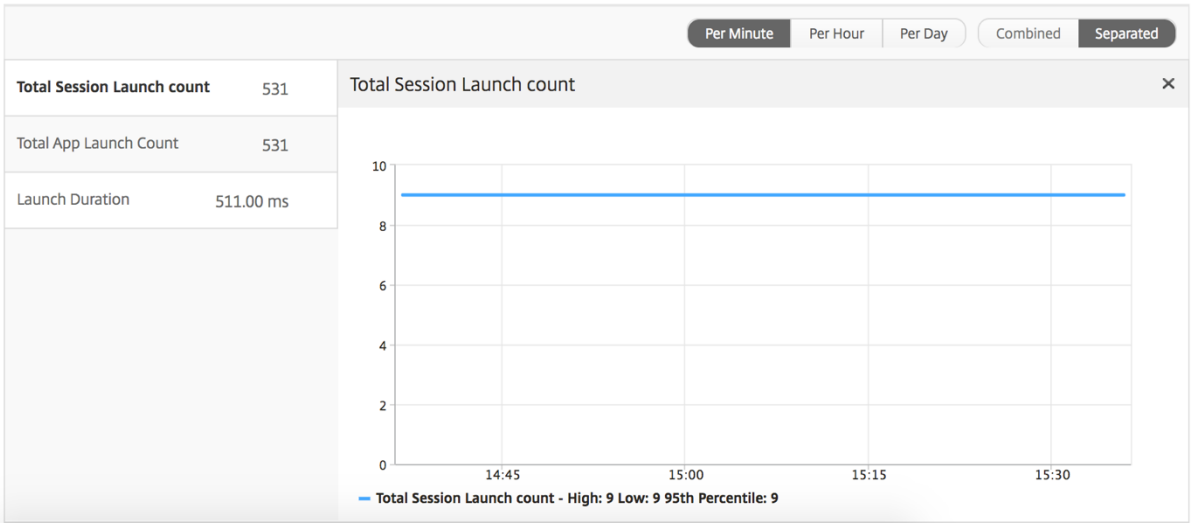
指标	说明
名称	Citrix Virtual Apps 的名称。
状态	显示应用程序的状态：绿色 - 活动、红色 - 不活动
Active Sessions（活动会话数）	在给定时间间隔内使用此应用程序的活动用户会话数。
Active Apps（活动应用程序数）	此应用程序的活动会话数。



阈值报告　阈值报告表示选定时段内实体被选为应用程序时突破阈值的次数。有关详细信息，请参阅 如何创建阈值。

折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。

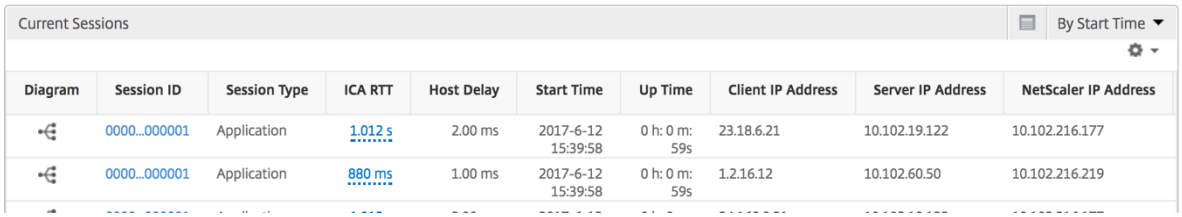


“当前会话”报告

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致通过 Citrix ADC 传输的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。

指标	说明
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

指标	说明
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
用户名	访问此特定 Citrix Virtual Apps 的用户的用户名。
会话 ID	Citrix Virtual Apps 会话的唯一标识符。
会话类型	将为“Application”（应用程序）。
状态	会话状态：绿色表示活动，红色表示不活动。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。
L7 Server-side Latency（L7 服务器端延迟）	在 Citrix ADC 设备和 Citrix Virtual Apps 之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。



“每个应用程序会话”视图

“Per Application Session View”（每个应用程序会话视图）显示特定的选定应用程序会话的报告。

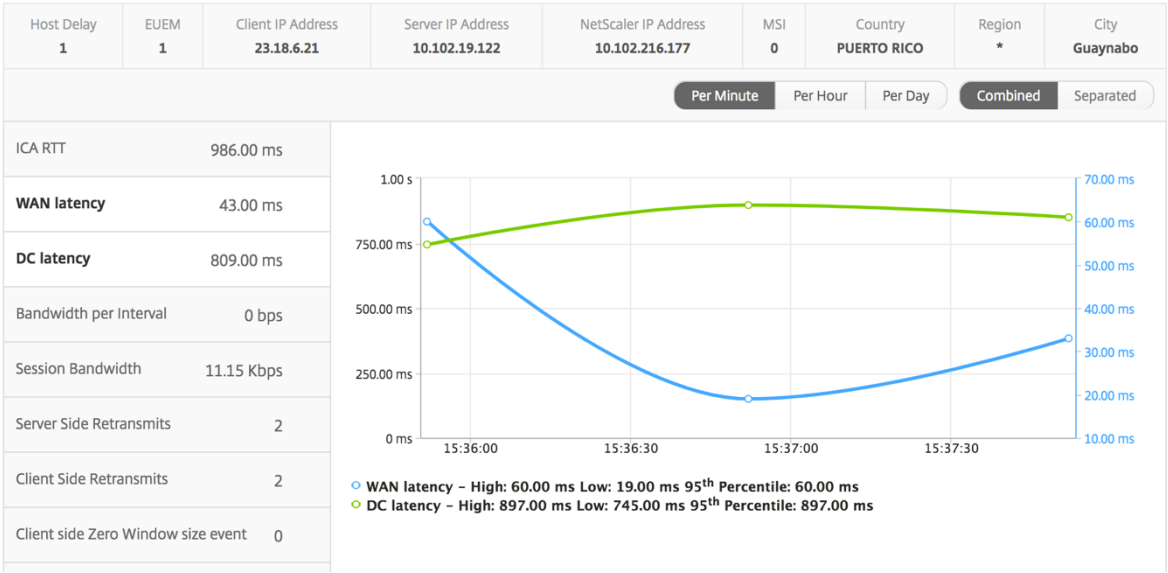
要查看会话报告，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到“分析”>“**HDX Insight**”>“应用程序”。
3. 从“Application Summary Report”（应用程序摘要报告）中选择特定用户。
4. 从当前会话报告中选择会话。

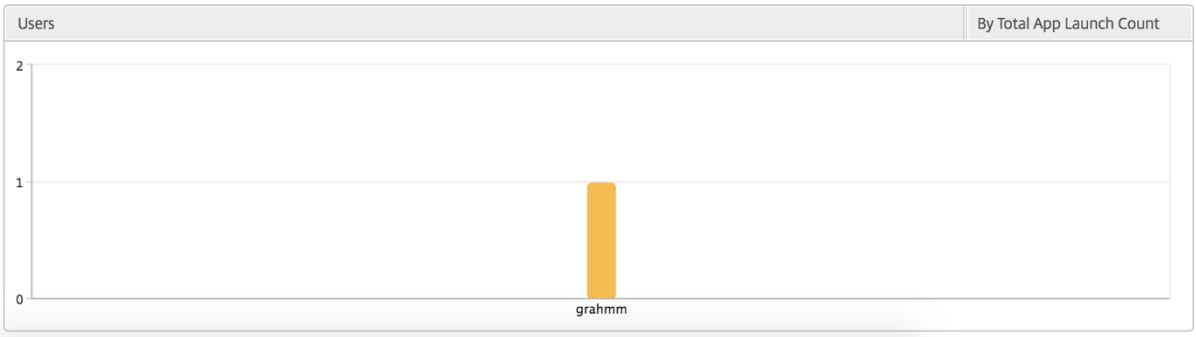
折线图

指标	说明
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
Server side Zero Window size event（服务器端零窗口大小事件）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。

指标	说明
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



用户条形图　用户条形图表示登录此特定应用程序的用户。



桌面视图报表和指标

此视图中的报告和衡量指标集中在 Citrix Virtual Desktops 上。

要导航到桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 桌面。

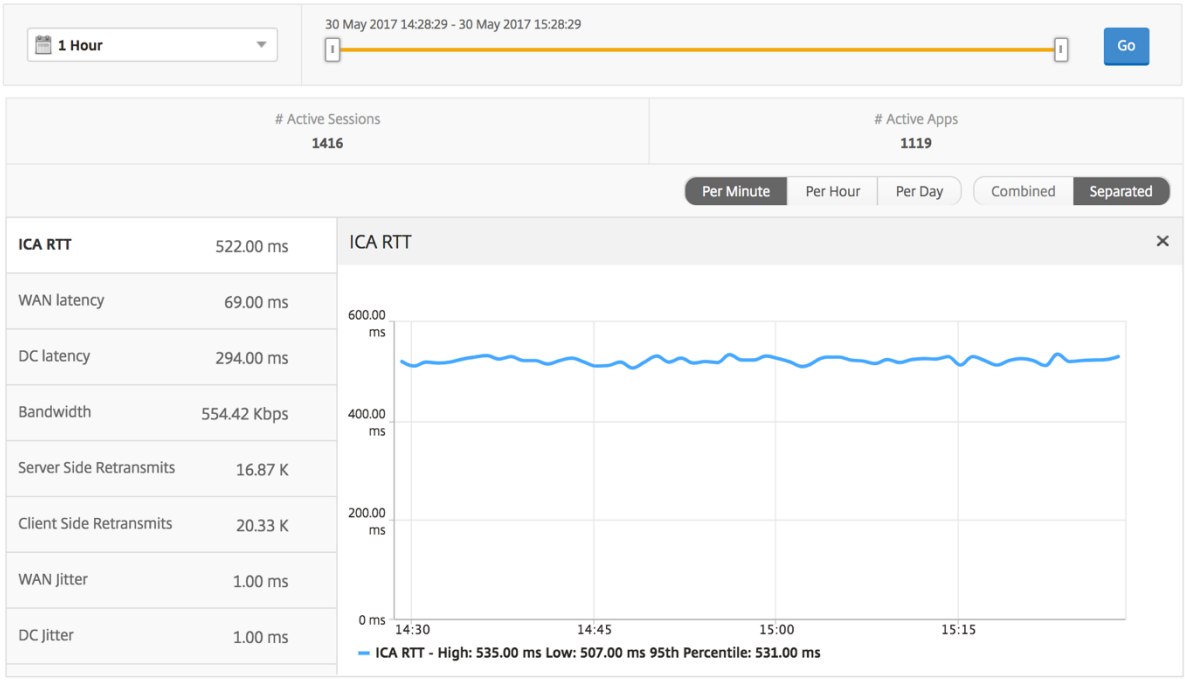
Summary View（摘要视图）

摘要视图显示在选定时间轴内登录的所有 Citrix Virtual Desktops 的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

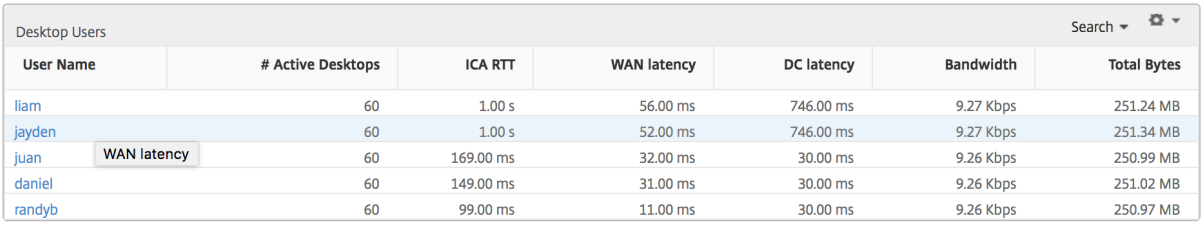
折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



台式机摘要报告

指标	说明
活动会话	在给定时间间隔内活动 Citrix Virtual Desktops 会话的总数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。



阈值报告　阈值报告表示在选定期间内将 实体 选为桌面时所超过的阈值计数。有关详细信息，请参阅 如何创建阈值。

每个桌面视图

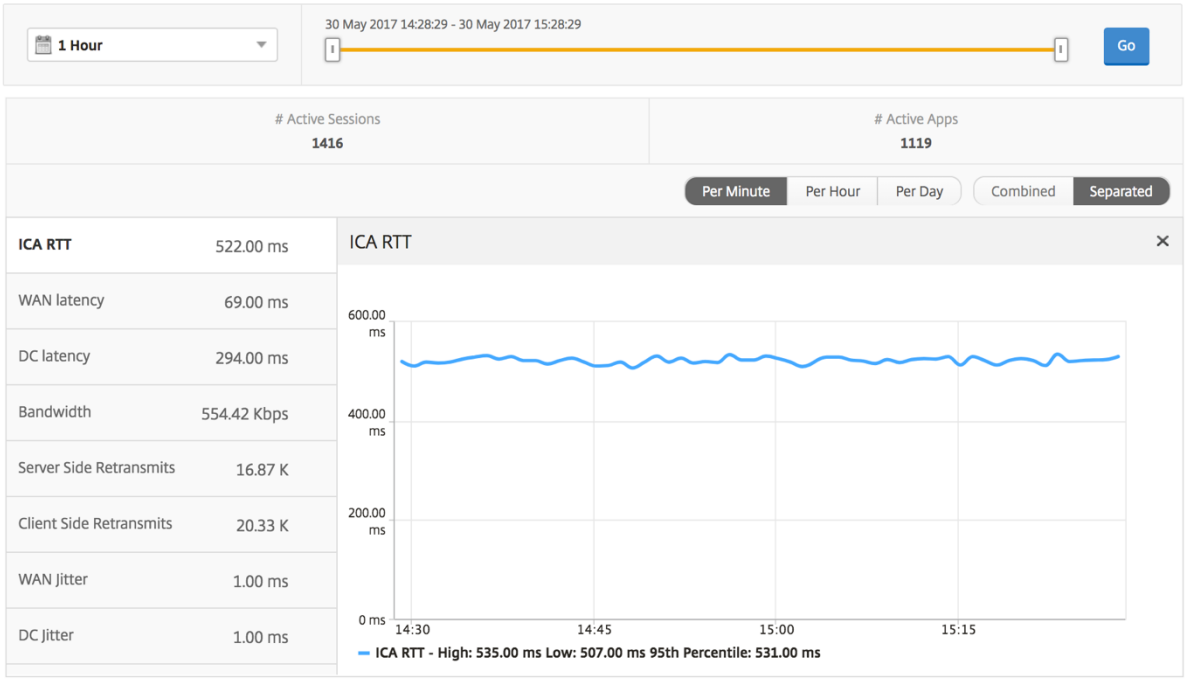
每个桌面视图提供了选定 Citrix 虚拟桌面的详细最终用户体验报告。

要导航到特定的桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 分析 **> HDX Insight >** 桌面。
3. 从桌面摘要报告中选择特定桌面。

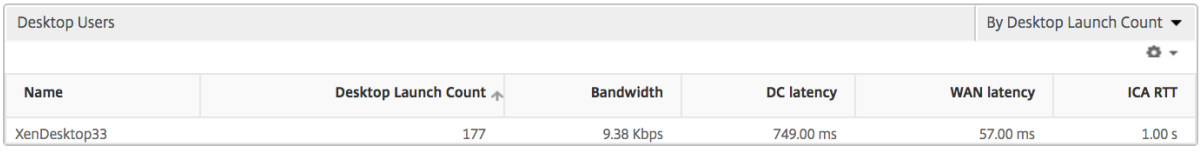
折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



桌面用户报告　此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

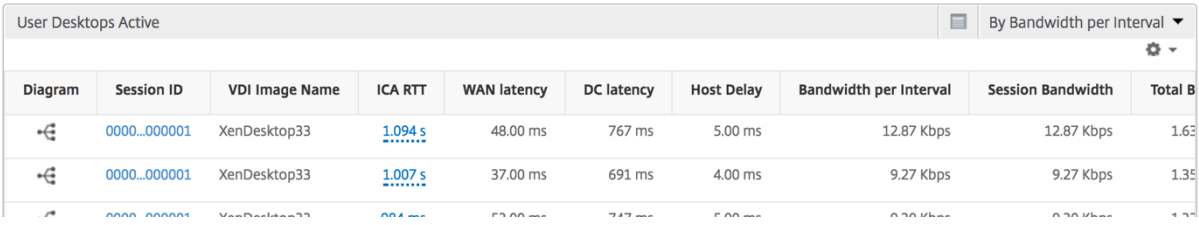
指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。



用户桌面活动/非活动报告　以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致通过 Citrix ADC 传输的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。

指标	说明
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称
Diagram（示意图）	



每个桌面会话视图

每个桌面会话视图提供特定选定 Citrix 虚拟桌面会话的报告。

要导航到桌面会话视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 分析 **> HDX Insight >** 桌面。
3. 从桌面摘要报告中选择特定桌面。
4. 从当前会话报告中选择会话。

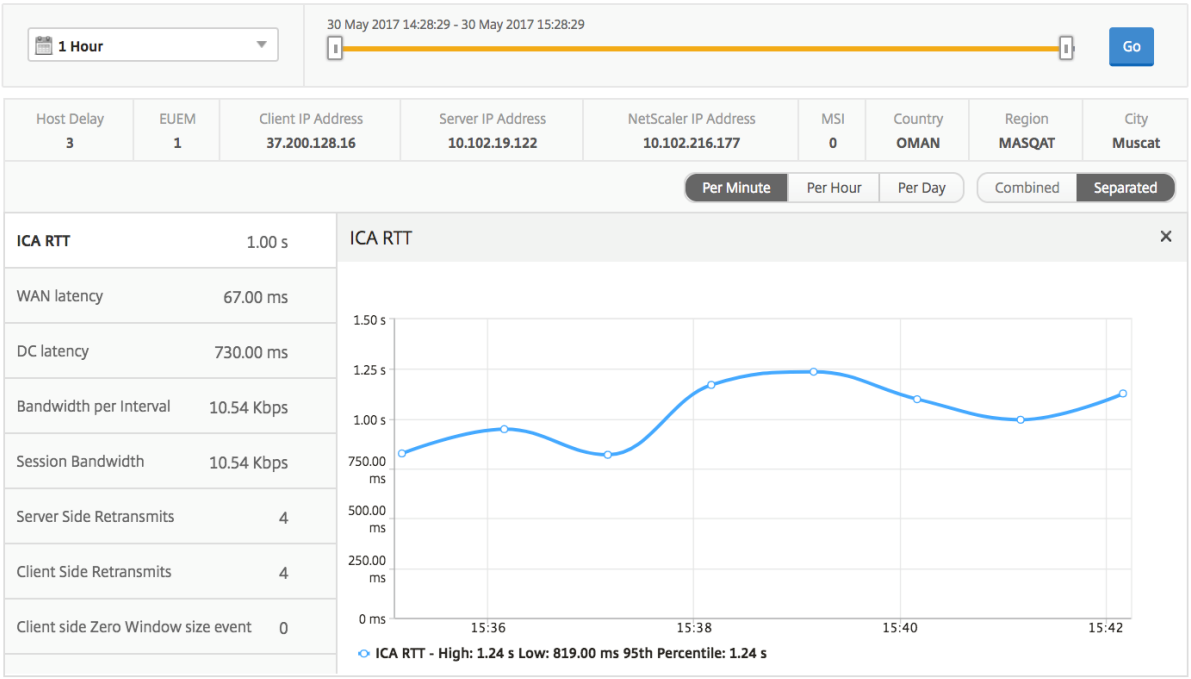
时间线图 “Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

要查看选定用户会话的度量，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户。
3. 从用户摘要报告部分选择特定用户。
4. 从当前会话或已终止的会话列中选择一个会话。

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。

指标	说明
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。

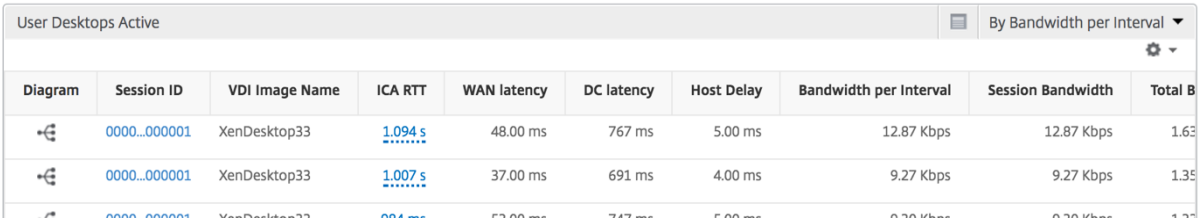


相关桌面会话报告　以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致通过 Citrix ADC 传输的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。

指标	说明
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。

指标	说明
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。



实例视图报告和指标

实例视图中的报告和指标集中在 Citrix ADC 实例上。

要导航到“实例”视图，请执行以下操作：

1. 使用受支持的 Web 浏览器登录到 Citrix ADM。
2. 导航到“分析”**>**“**HDX Insight**”**>**“实例”。

“Instance”（实例）视图报告和指标包括以下部分：

- Instance Summary View（实例摘要视图）
- Per Instance View（每个实例视图）

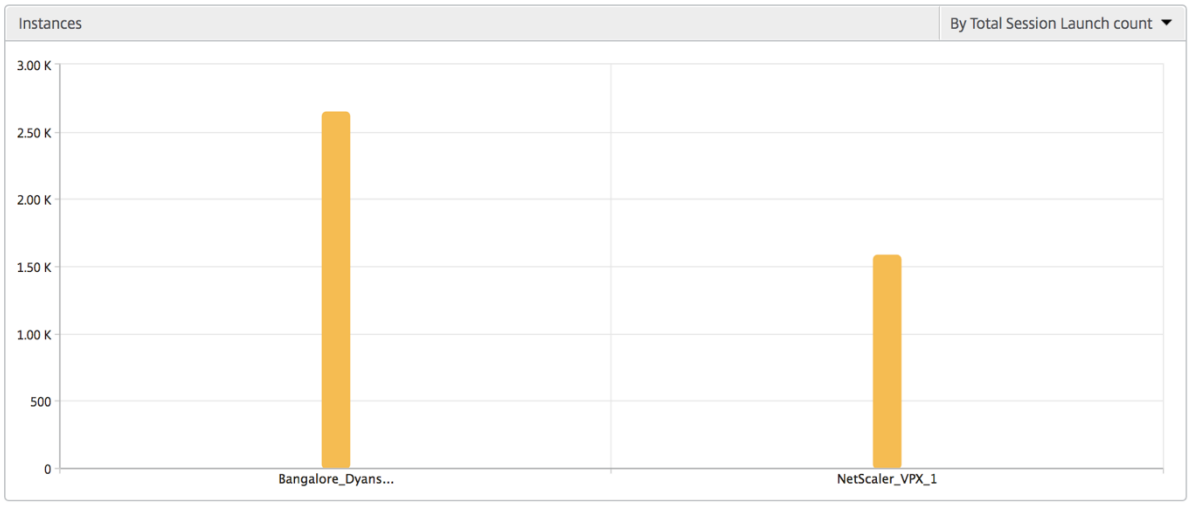
“实例摘要”视图

此视图称为摘要视图，因为它显示了添加到 Citrix ADM 的所有 Citrix ADC 实例的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

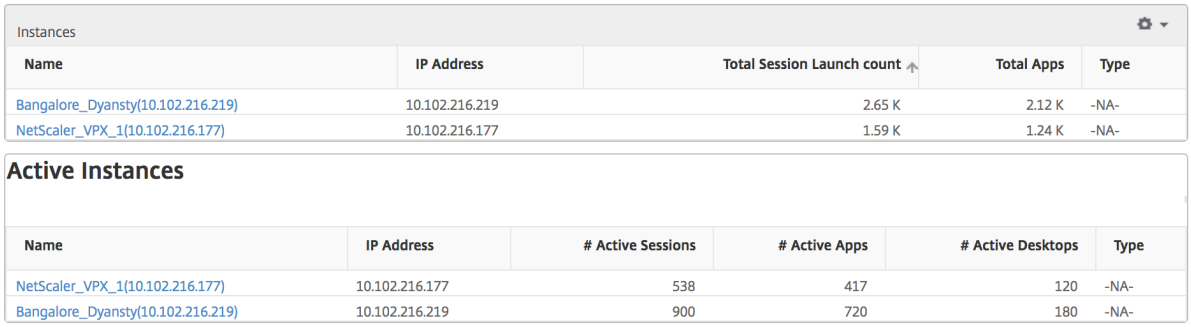
实例条形图

此图形显示实例与总会话启动计数的比较	应用程序总数，可从图表画布右上角的下拉列表中选择。



实例/活动实例摘要报告

指标	说明
名称	Citrix ADC 实例的主机名。
IP 地址	NetScaler IP 地址。
Total Session Launch Count（会话启动总数）	在给定时间间隔内创建的唯一用户会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用


Instances

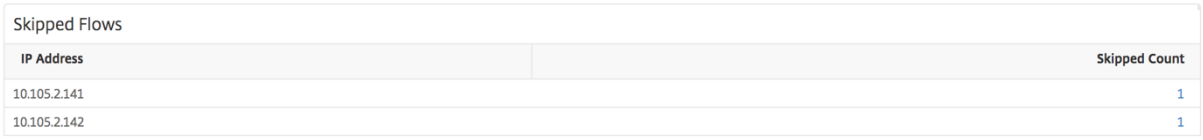
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

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-

阈值报告　阈值报告表示在选定时间段内将实体选为实例的违反阈值计数。有关详细信息，请参阅 如何创建阈值。

跳过的流　跳过的流是跳过解析 ICA 连接的记录。这可能是由于多种原因造成的，例如使用不受支持的 Citrix Virtual Apps and Desktops 版本、Receiver 或 Receiver 类型不受支持的版本等。此表显示 IP 地址和跳过的流计数。这些 Receiver 可能不属于列入白名单的 Receiver；因此，监视时跳过了这些会话。



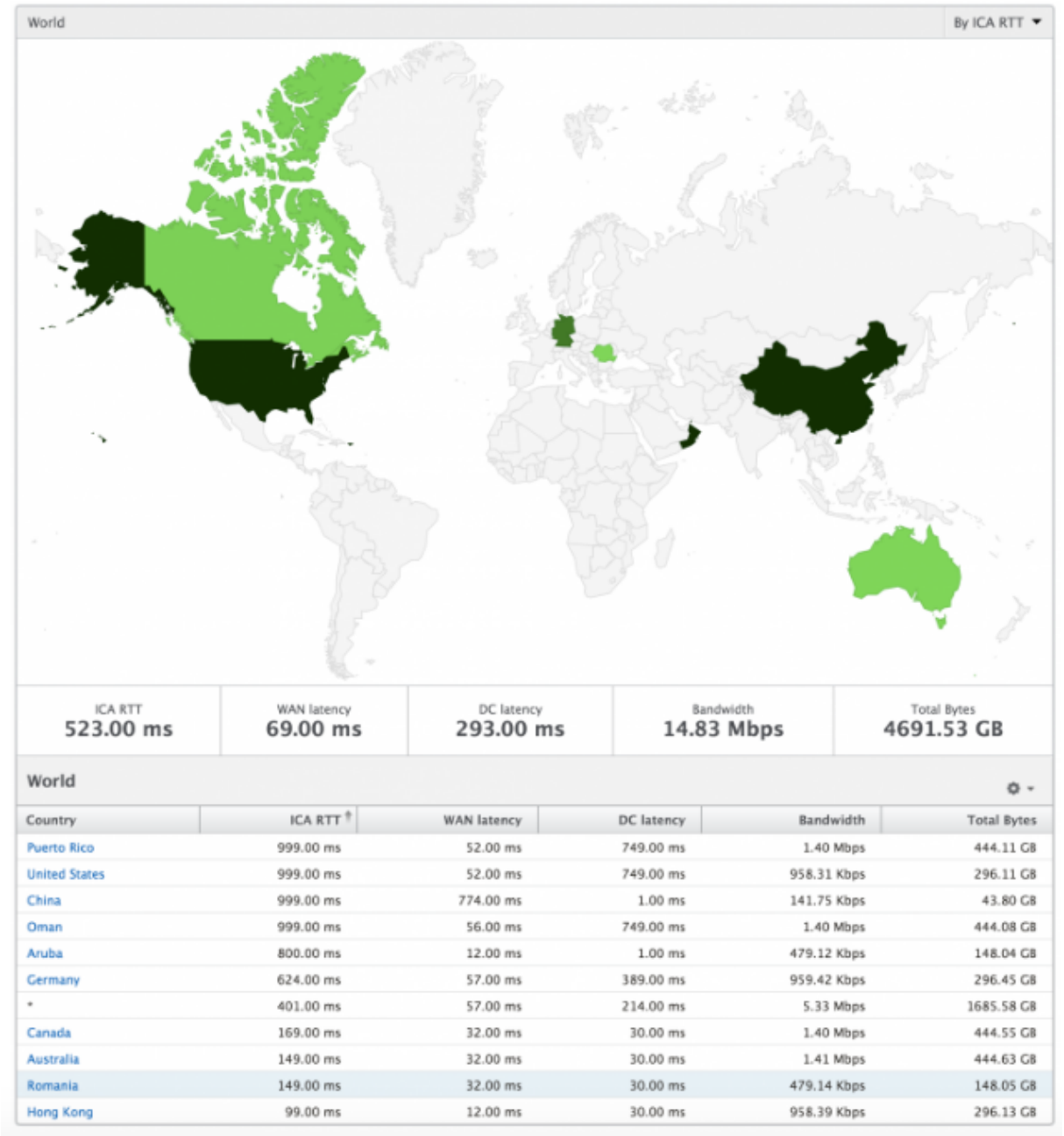
Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

“**World**”（世界）视图　通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以使用系统的“World”（世界）视图，只需单击区域即可深入查看特定国家/地区以及进一步深入到城市。管理员可以按城市和省/自治区进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

可以在 HDX Insight 中的世界地图上查看以下详细信息，每个指标的密度以热度地图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



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

每实例视图

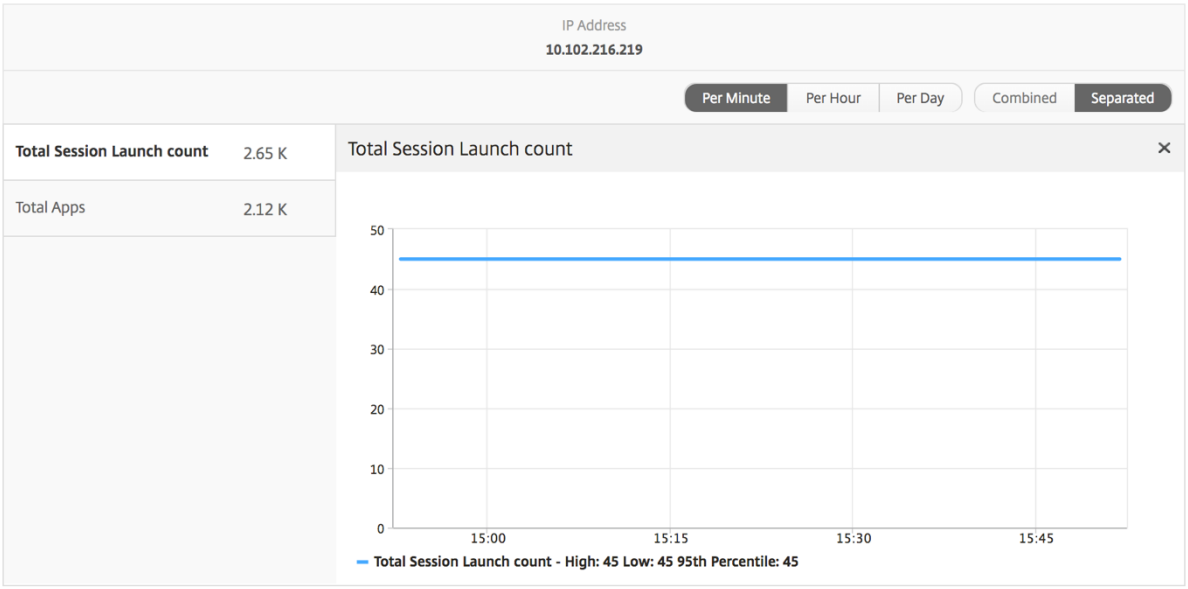
每个实例视图为特定选定的 Citrix ADC 实例提供详细的最终用户体验报告。

要导航到“实例”视图，请执行以下操作：

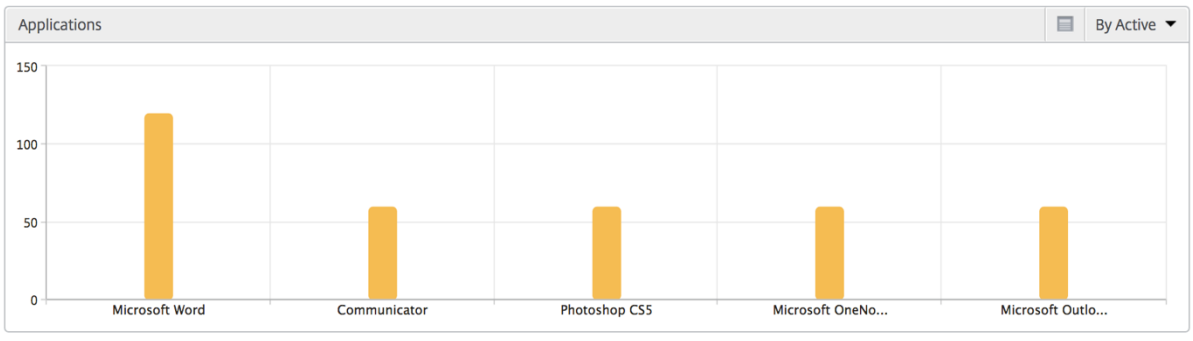
1. 使用受支持的 Web 浏览器登录到 Citrix ADM。
2. 导航到“分析” **>** “**HDX Insight**” **>** “实例”。
3. 从实例摘要报告中选择特定实例。

折线图

指标	说明
IP 地址	此项表示选定实例的 NetScaler IP 地址。
Total Session Launch count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。



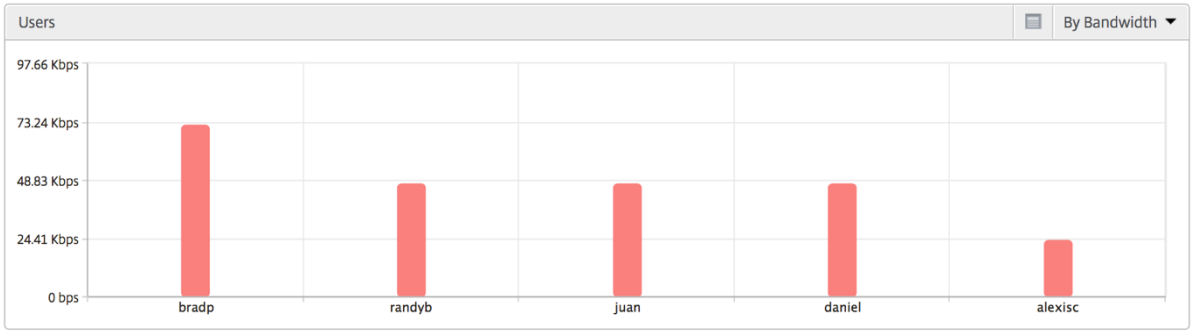
“**Applications**”（应用程序）条形图　基于以下条件显示排在前 5 位的应用程序 - 按活动应用程序数、会话启动总数、应用程序启动总数或启动持续时间。



“**Users**”（用户）条形图　“Users”（用户）条形图基于以下条件显示排在前 5 位的用户

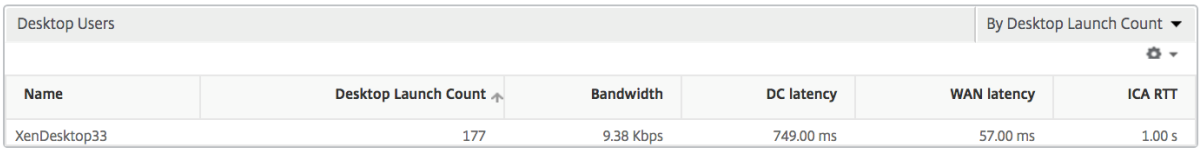
- Bandwidth（带宽）
- WAN 延迟

- DC 延迟
- ICA RTT



桌面用户报告　此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 Citrix Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

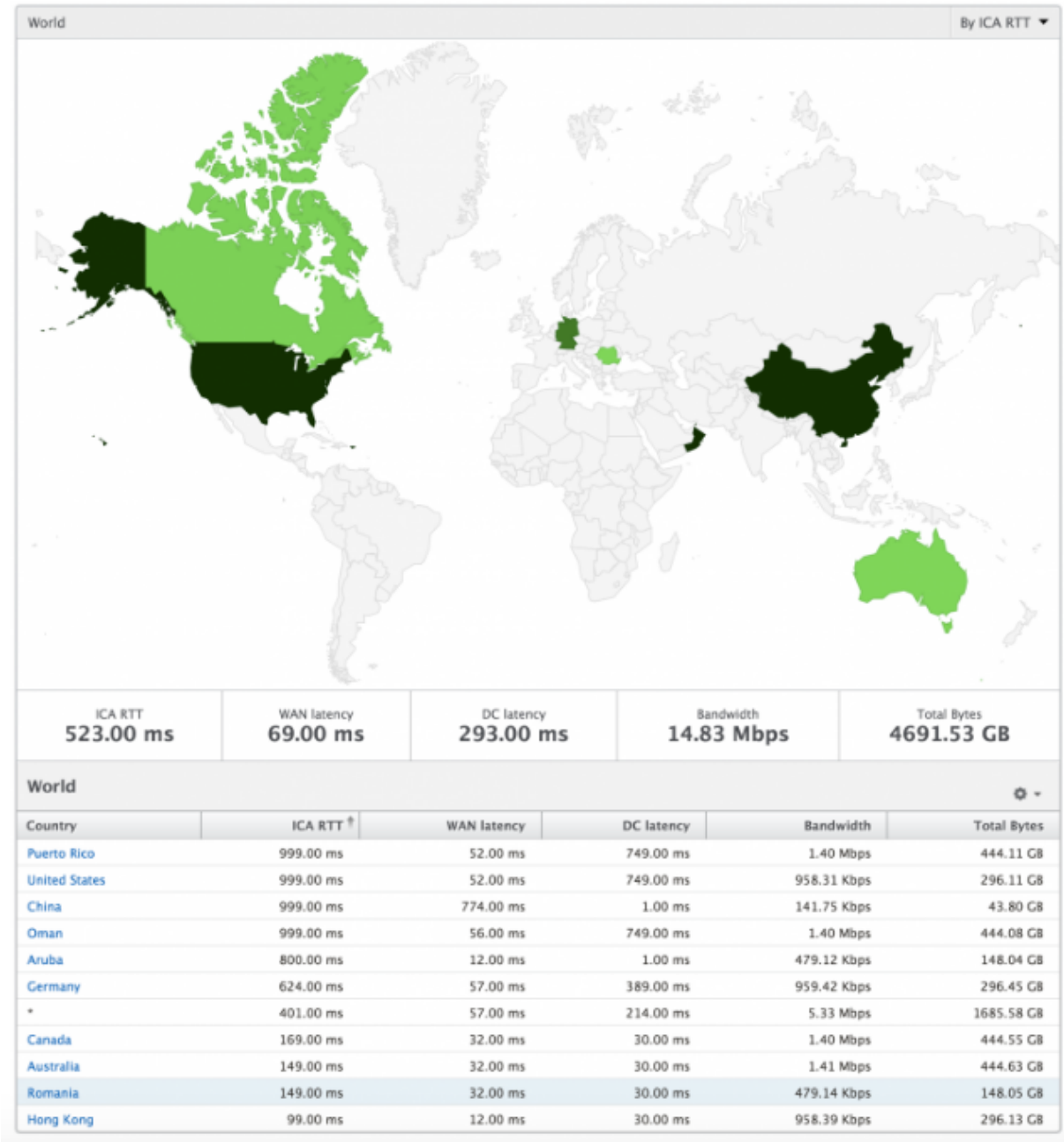


“**World**”（世界）视图　通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以使用系统的“World”（世界）视图，只需单击区域即可深入查看特定国家/地区以及进一步深入到城市。管理员可以按城市和省/自治区进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

可以在 HDX Insight 中的世界地图上查看以下详细信息，每个指标的密度以热度地图的形式显示：

- ICA RTT

- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



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

许可证视图报告和指标

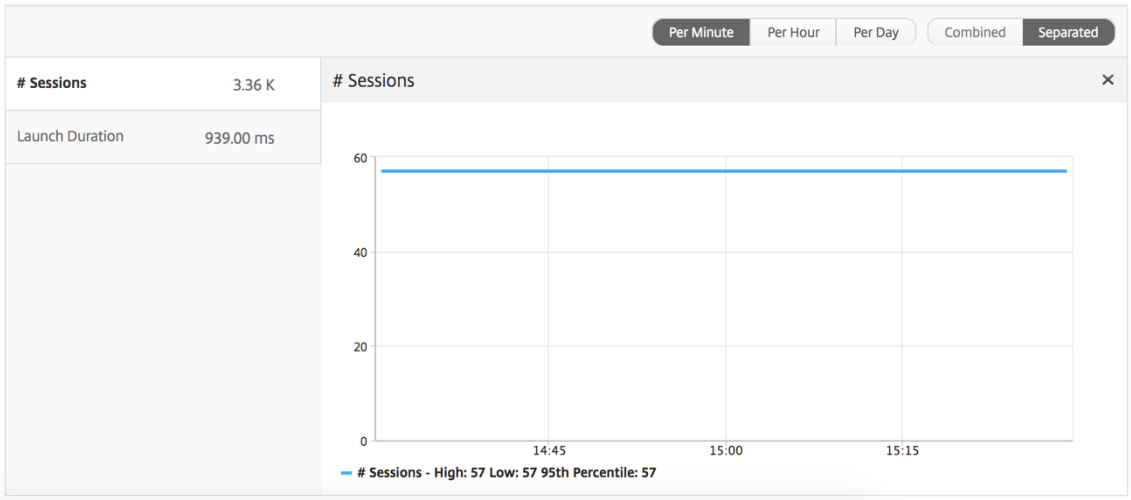
许可证视图提供了有 Citrix Gateway 许可证信息的详细信息。

要导航到“许可证”视图，请执行以下操作：

1. 使用受支持的 Web 浏览器登录到 Citrix ADM。
2. 导航到 分析 **> HDX Insight >** 许可证。

折线图

指标	说明
正在使用的许可证	在选定的时间轴内使用的 Citrix Gateway CCU 许可证。每个计数均表示用户会话数。这与用户启动的应用程序和桌面会话无关。
Total licenses（许可证总数）	可供客户使用的 Citrix Gateway CCU 许可证总数。



阈值报告　阈值报告表示在选定期间内将实体选为许可证的违反阈值计数。有关详细信息，请参阅 如何创建阈值。

“**Application**”（应用程序）视图报告和指标

February 6, 2024

此视图中的报表和衡量指标集中在 Citrix Virtual Apps 上。

要导航到“应用程序”视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到“分析”>“**HDX Insight**”>“应用程序”。

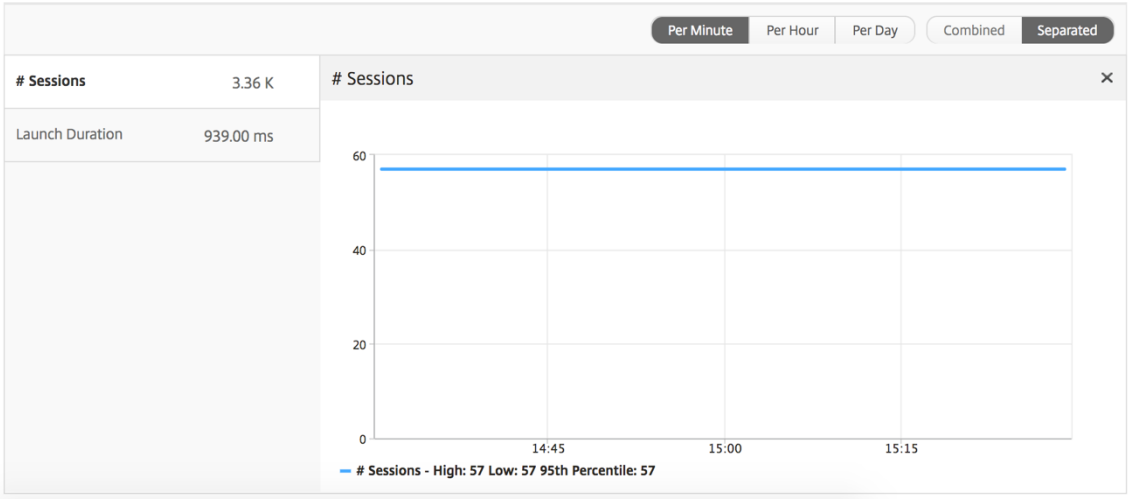
Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有应用程序的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

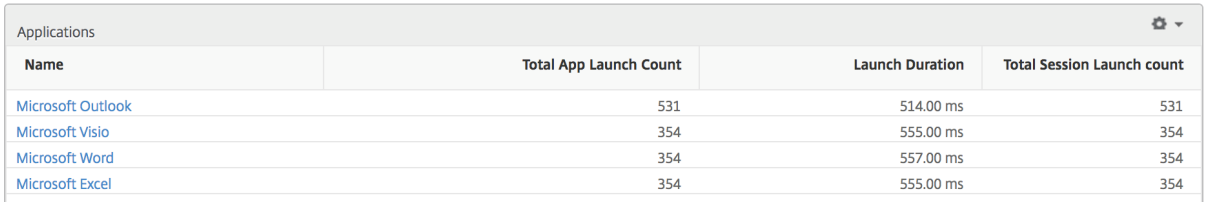
折线图

指标	说明
Sessions（会话数）	在给定时间间隔内的会话总数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。



Applications Summary Report（应用程序摘要报告）

指标	说明
名称	Citrix Virtual Apps 的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix Virtual Apps 总数。
Launch Duration（启动持续时间）	启动 Citrix Virtual Apps 所花费的平均时间。

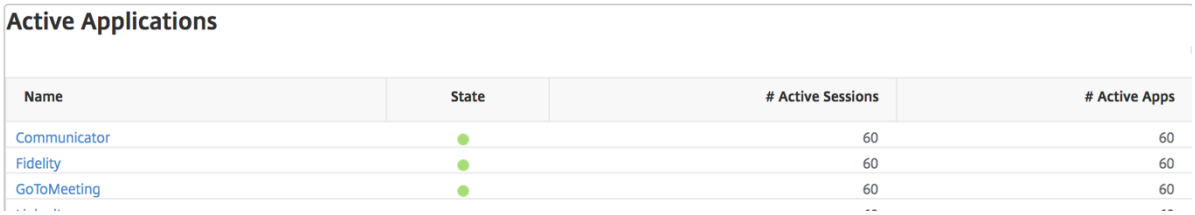


Applications

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

“活动应用程序”报告

指标	说明
名称	Citrix Virtual Apps 的名称。
状态	显示应用程序的状态：绿色 - 活动、红色 - 不活动
Active Sessions（活动会话数）	在给定时间间隔内使用此应用程序的活动用户会话数。
Active Apps（活动应用程序数）	此应用程序的活动会话数。



Active Applications

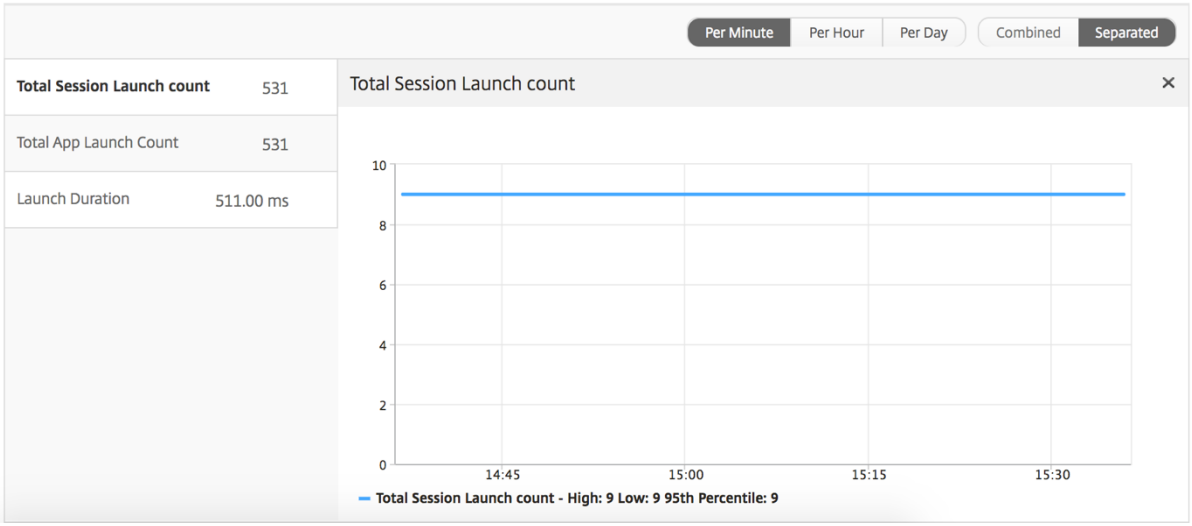
Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

阈值报告

阈值报告表示在选定期间内将实体选为应用程序的违反阈值计数。有关更多信息，请参阅如何创建阈值和警报。

折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。

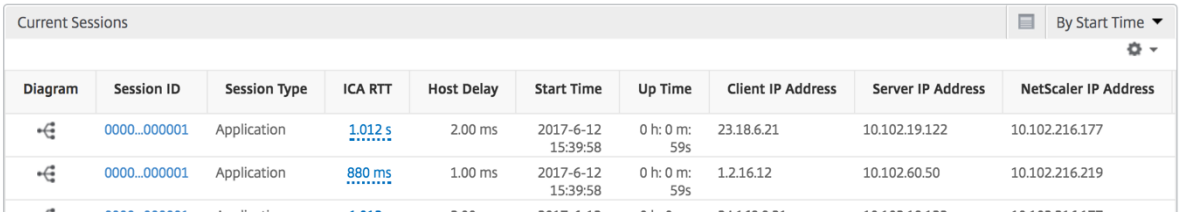


当前会话报告

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致的通过 NetScaler ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端等。
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。

指标	说明
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
用户名	访问此特定 Citrix Virtual Apps 的用户的用户名。
会话 ID	Citrix Virtual Apps 会话的唯一标识符。
会话类型	将为“Application”（应用程序）。
状态	会话状态：绿色表示活动，红色表示不活动。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。交付路径中存在非 Citrix 设备的情况下，此指标很有用。
L7 Server-side Latency（L7 服务器端延迟）	在 NetScaler 设备和 Citrix Virtual Apps 之间观察到的平均 L7 延迟。交付路径中存在非 Citrix 设备的情况下，此指标很有用。



Per Application Session View（每个应用程序会话视图）

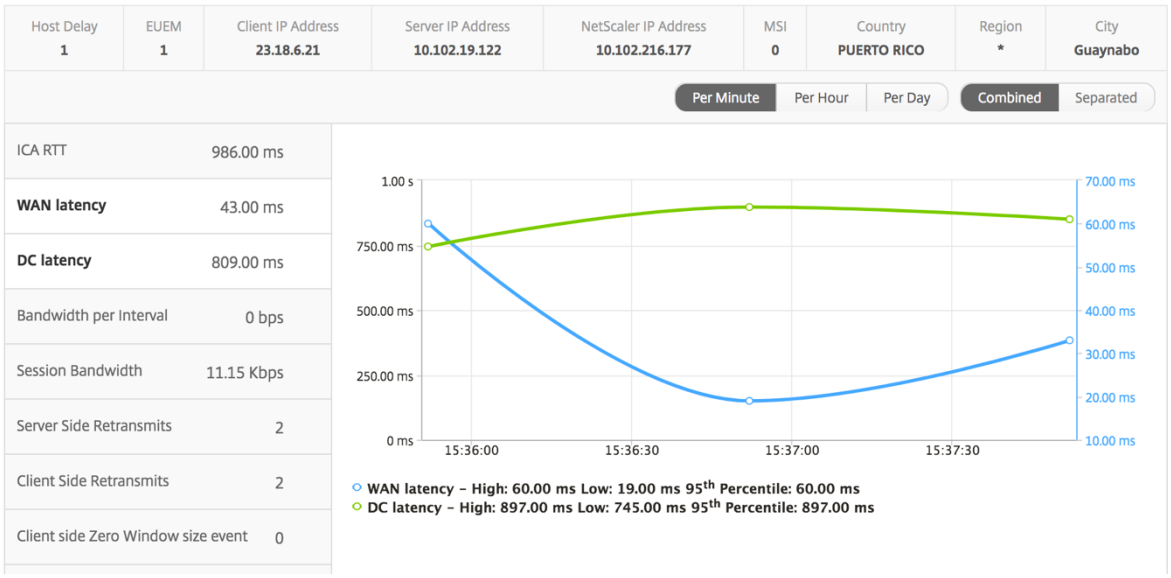
“Per Application Session View”（每个应用程序会话视图）显示特定的选定应用程序会话的报告。

要查看会话报告，请执行以下操作：

1. 导航到“分析”>“**HDX Insight**”>“应用程序”。
2. 从“Application Summary Report”（应用程序摘要报告）中选择特定用户。
3. 从当前会话报告中选择会话。

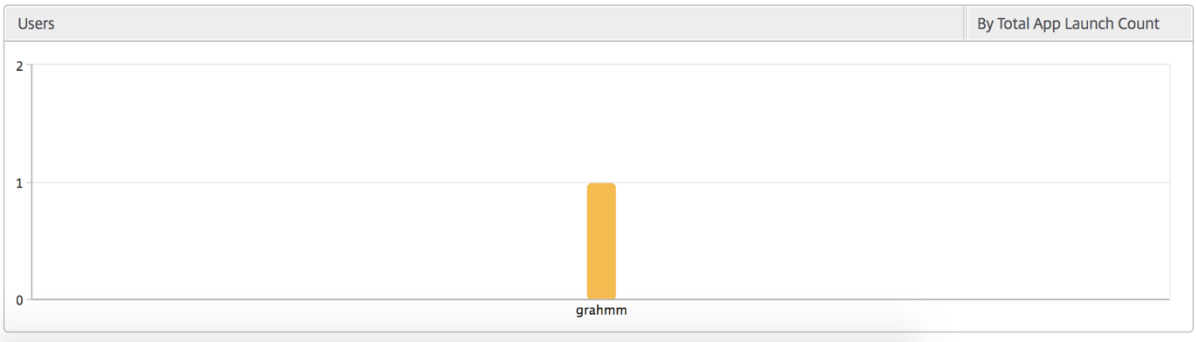
折线图

指标	说明
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
Server side Zero Window size event（服务器端零窗口大小事件）	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



用户条形图

用户条形图表示登录此特定应用程序的用户。



“**Desktop**”（桌面）视图报告和指标

February 6, 2024

此视图中的报告和指标侧重于 Citrix Virtual Desktops Virtual Desktops。

要导航到桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 桌面。

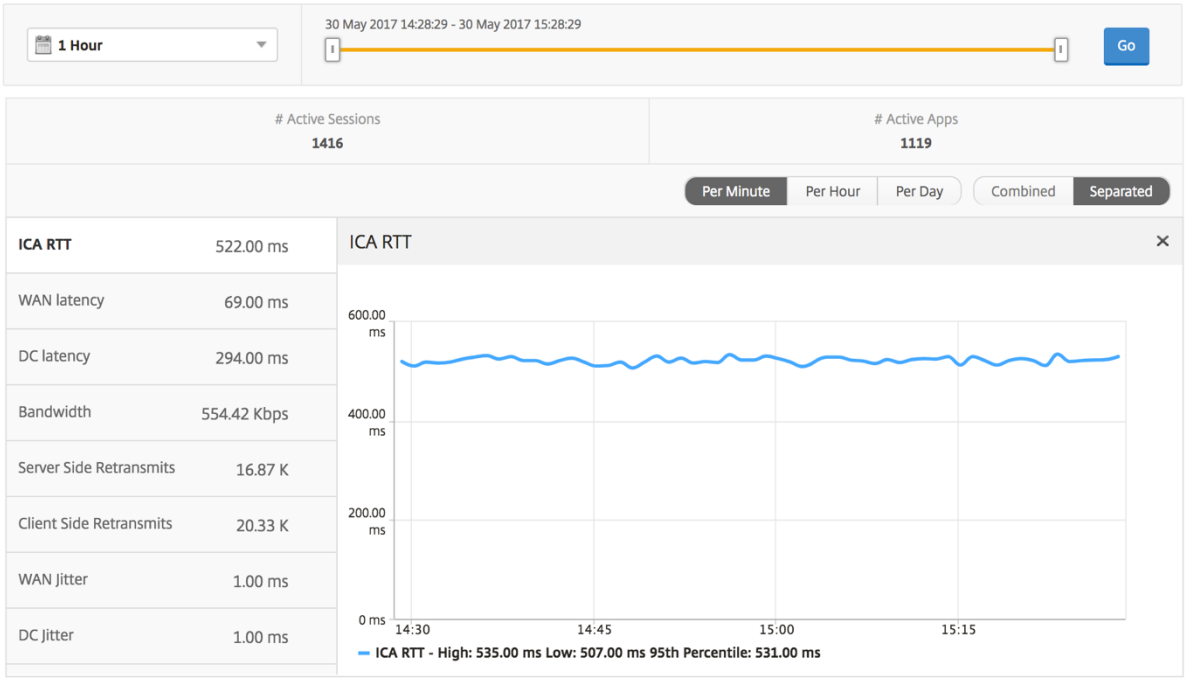
Summary View（摘要视图）

摘要视图显示在选定时间轴内登录的所有 Citrix Virtual Desktops 的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

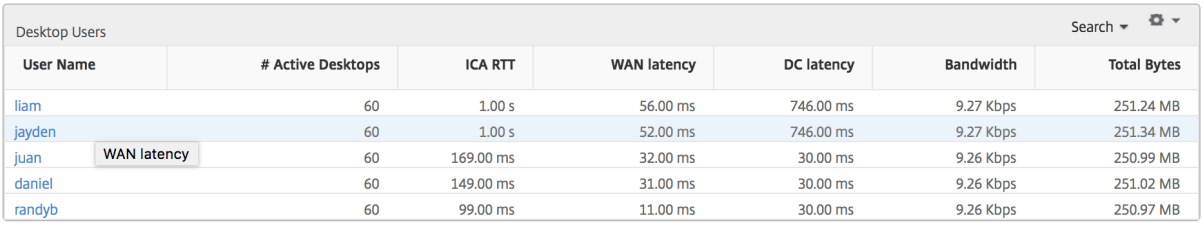
折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



Desktop Summary Report（桌面摘要报告）

指标	说明
活动会话	在给定时间间隔内活动 Citrix Virtual Desktops 会话的总数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。



阈值报告

阈值报告表示在选定期间内将 实体 选为桌面时所超过的阈值计数。有关更多信息，请参阅如何创建阈值和警报。

Per Desktop View（每个桌面视图）

每个桌面视图提供了选定 Citrix 虚拟桌面的详细最终用户体验报告。

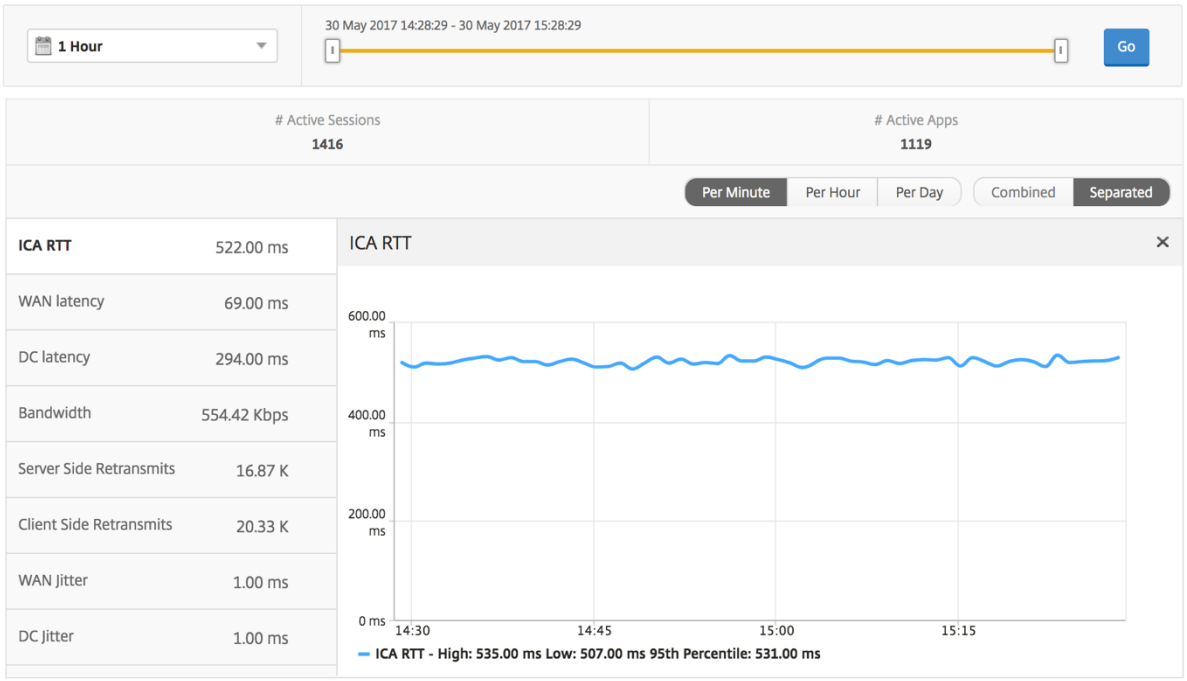
要导航到特定的桌面视图，请执行以下操作：

1. 导航到 分析 **> HDX Insight >** 桌面。
2. 从桌面摘要报告中选择特定桌面。

折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。

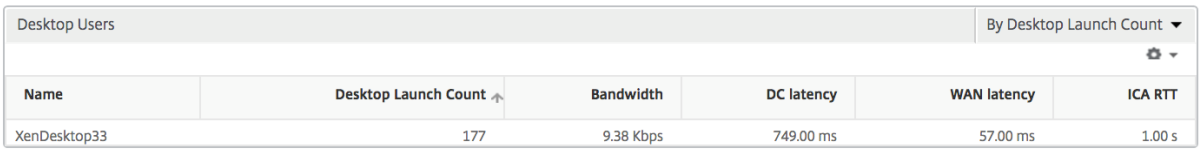


“**Desktop Users**”（桌面用户）报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。

指标	说明
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。



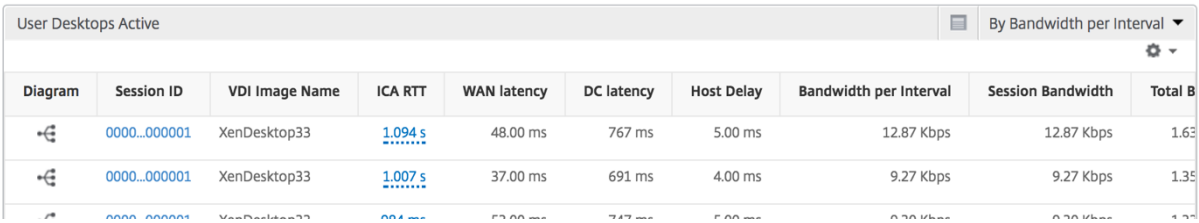
“**User Desktops Active**”（活动用户桌面）/ “**User Desktops Inactive**”（非活动用户桌面）报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致的通过 NetScaler ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端等。
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。

指标	说明
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称
Diagram（示意图）	



Per Desktop Session View（每个桌面会话视图）

每个桌面会话视图提供特定选定 Citrix 虚拟桌面会话的报告。

要导航到桌面会话视图，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 桌面。
2. 从桌面摘要报告中选择特定桌面。
3. 从当前会话报告中选择会话。

时间线图

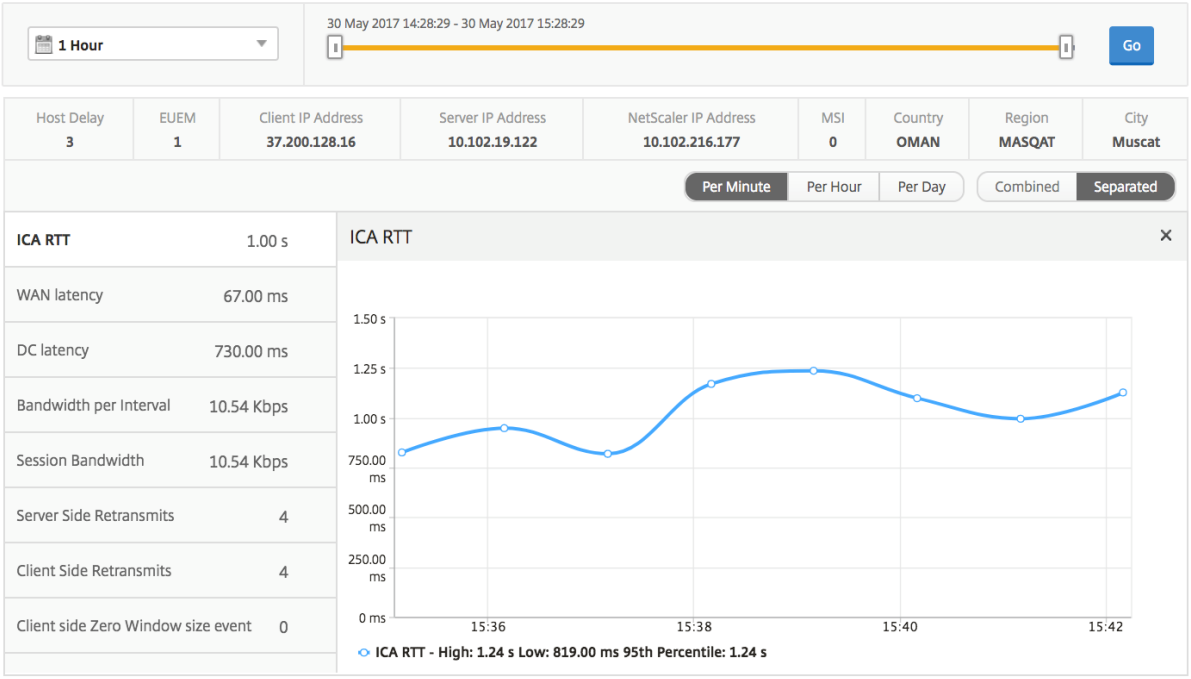
“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

要查看选定用户会话的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或已终止的会话列中选择一个会话。

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。

指标	说明
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



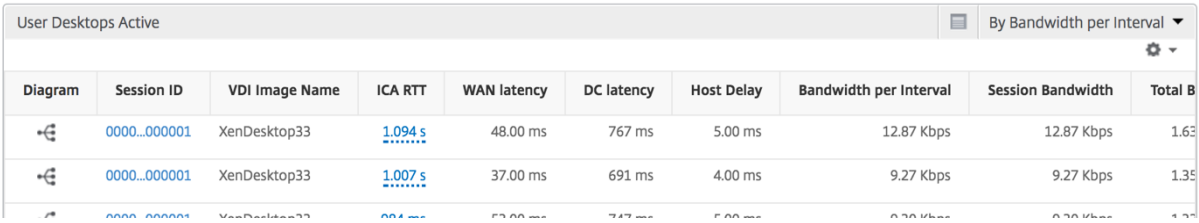
相关桌面会话报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致的通过 NetScaler ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。

指标	说明
客户端类型	Receiver 类型 - Citrix Windows 客户端等。
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称



“**User**”（用户）视图报告和指标

February 6, 2024

此视图中的报告和衡量指标按照 Citrix Virtual Apps and Desktops 用户显示。

要导航到“用户”视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户

Summary View（摘要视图）

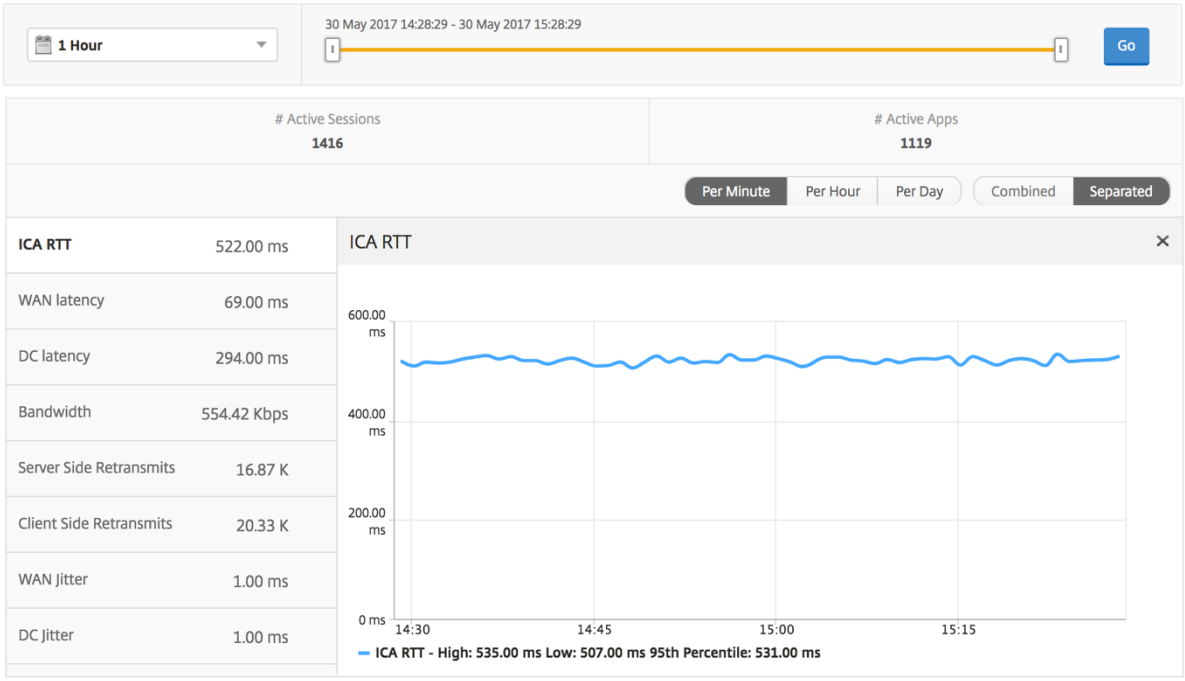
“Summary View”（摘要视图）显示在选定时间线内登录的所有用户的报告。除非另有说明，否则此视图中的所有指标/报告均显示选定时间段内与这些用户对应的值。

要更改选定时间段，请执行以下操作：

1. 使用时间段下拉框或时间滑块设置所需的时间间隔。
2. 单击转到。

折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。

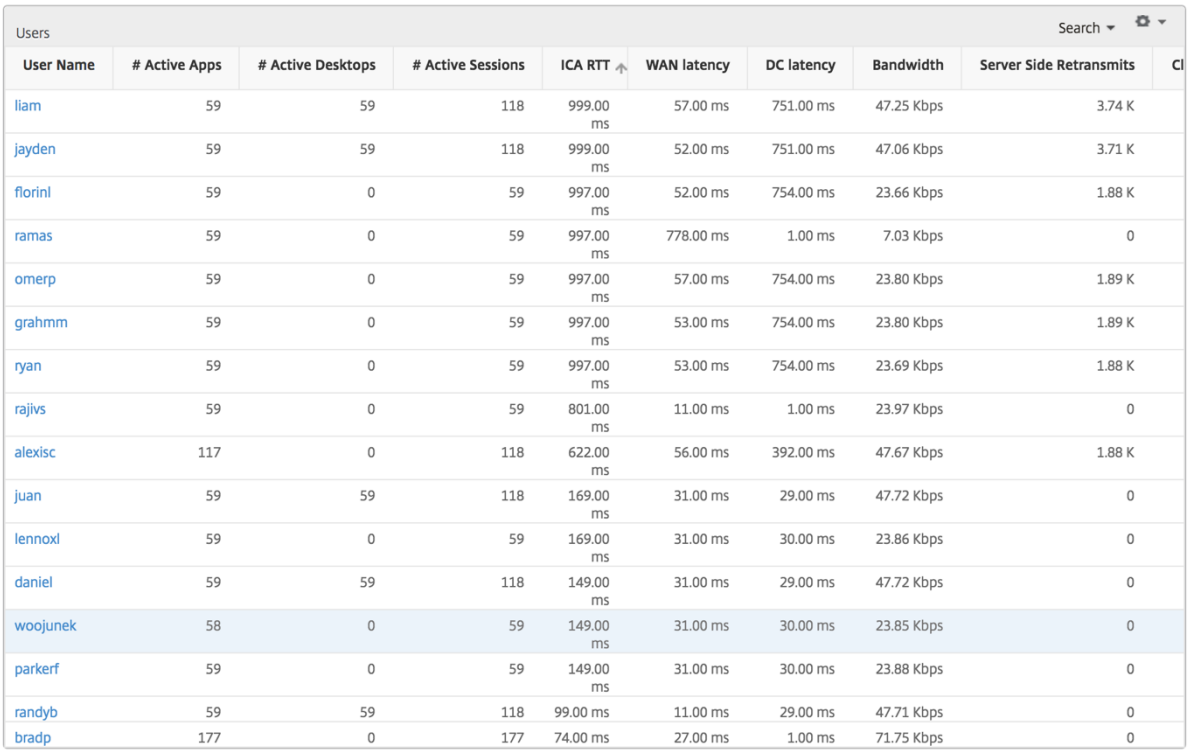


User Summary Report（用户摘要报告）

下面是与此报告特定相关的指标。

指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps and Desktops 上托管的应用程序或桌面进行交互时遇到的屏幕延迟。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Total App Launch Count（应用程序启动总数）	在选定的时间段内用户启动的应用程序总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。



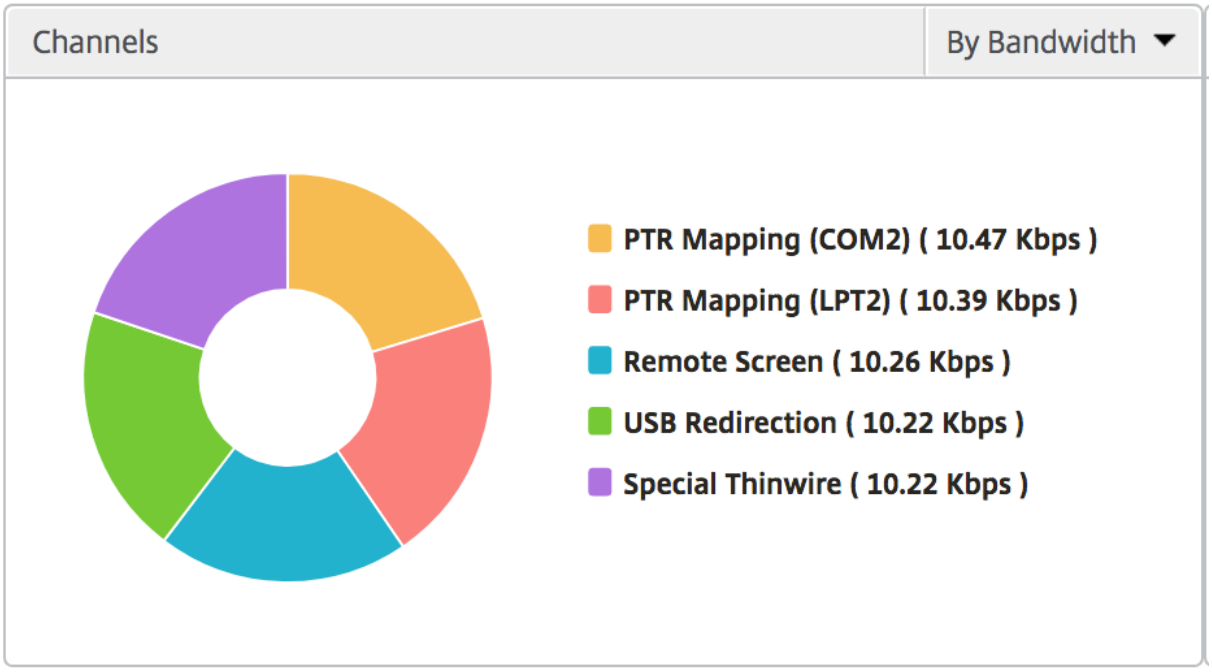
Users

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	

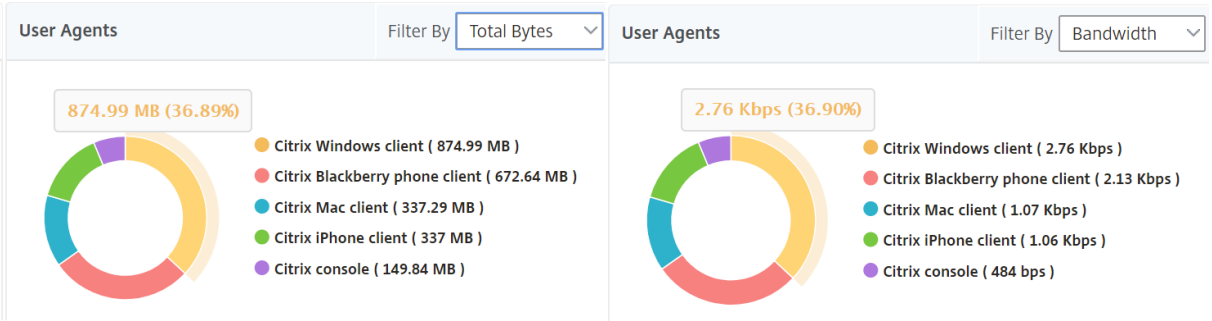
Channels（通道）

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



User Agents（用户代理）

“User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



阈值违反计数

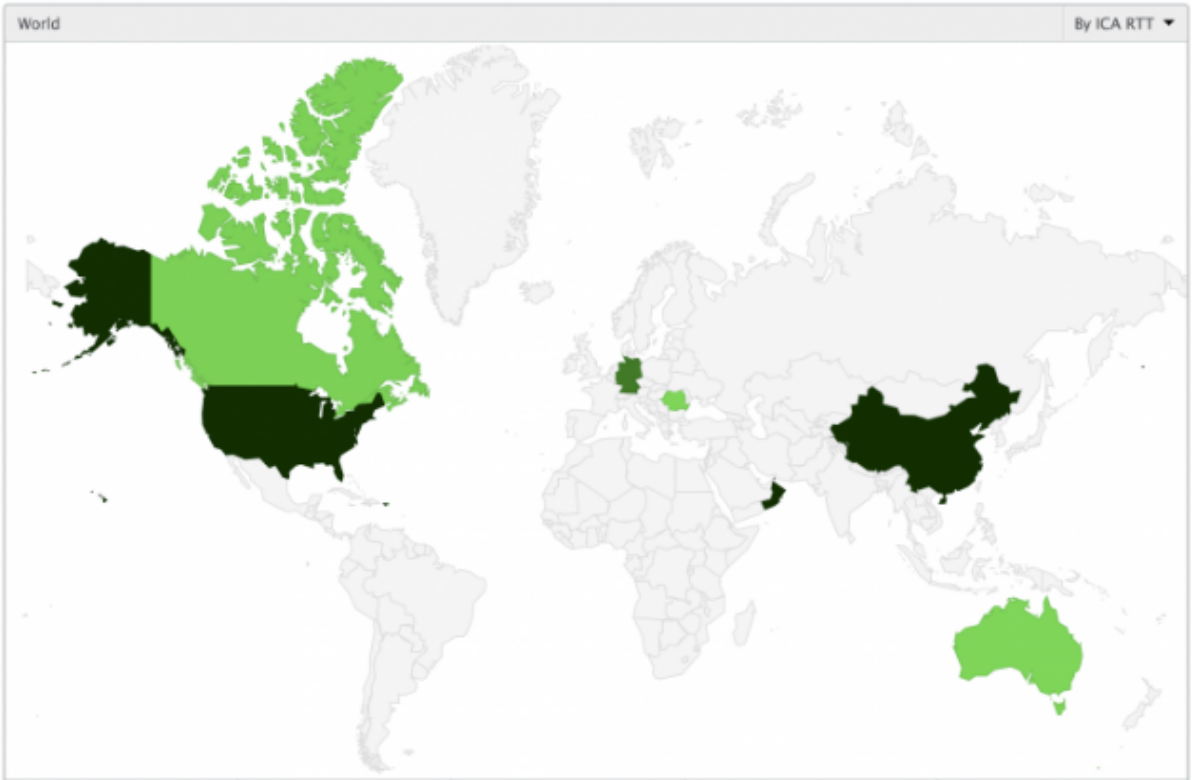
阈值违反计数指标表示在选定时间段内违反的阈值计数。有关更多信息，请参阅 如何创建阈值和警报。

世界地图

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以使用系统的“World”（世界）视图，只需单击区域即可深入查看特定国家/地区以及进一步深入到城市。管理员可以按城市和省/自治区进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

可以在 HDX Insight 中的世界地图上查看以下详细信息，每个指标的密度以热度地图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
523.00 ms	69.00 ms	293.00 ms	14.83 Mbps	4691.53 GB

World

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

Per User View（每个用户视图）

“Per User View”（每个实例视图）提供任何特定的选定用户的详细最终用户体验报告。

要导航到特定用户的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从“User Summary Report”（用户摘要报告）部分中选择特定用户。

折线图

折线图显示在选定时间段内特定的选定用户的所有指标摘要。

“**Current Sessions**”（当前会话）**/** “**Terminated Sessions**”（终止的会话）报告

此报告与选定用户的所有当前/已终止用户会话有关。这些指标可以按开始时间、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络导致的通过 NetScaler ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	Receiver 类型 - Citrix Windows 客户端等。
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。

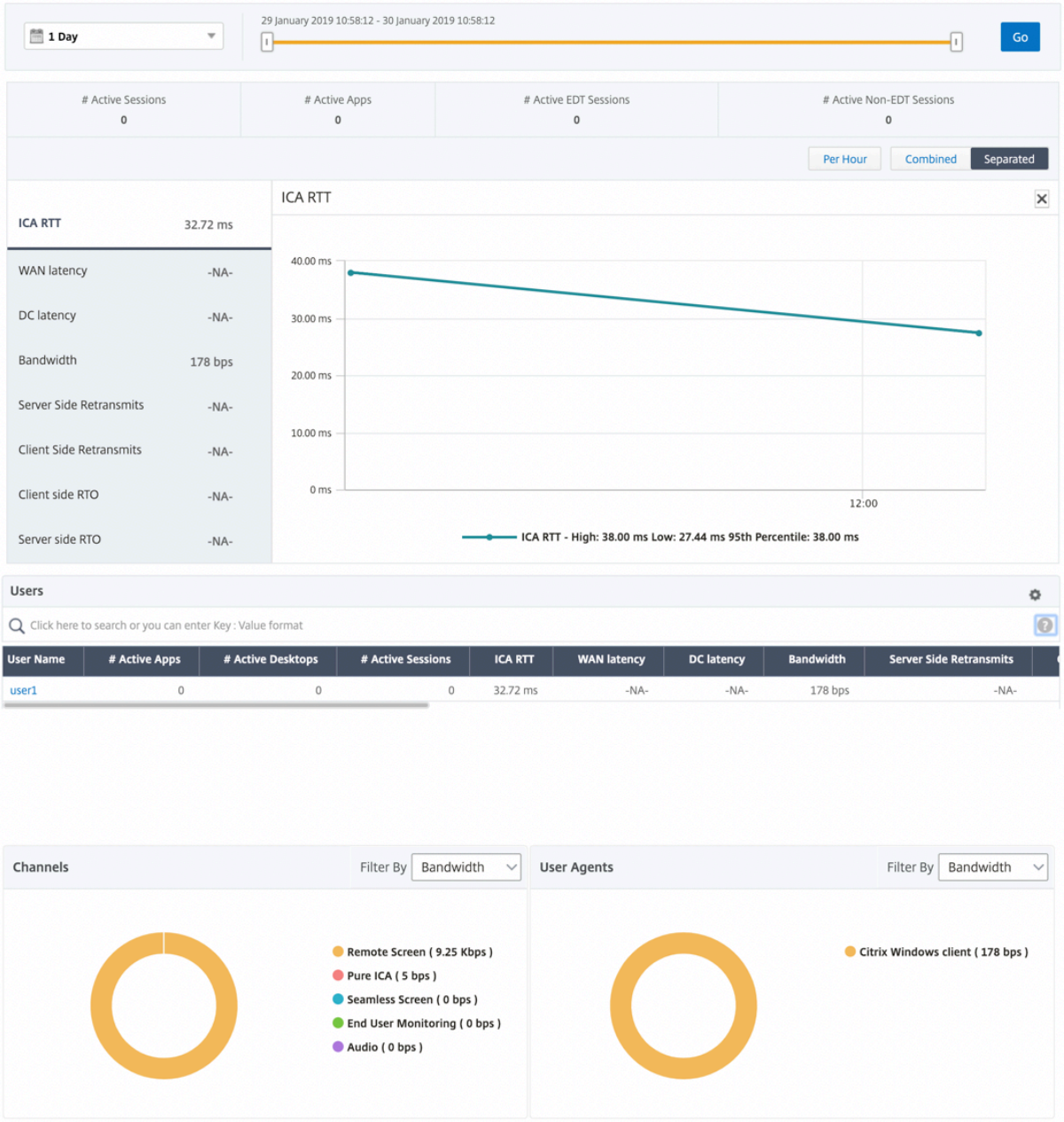
指标	说明
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。

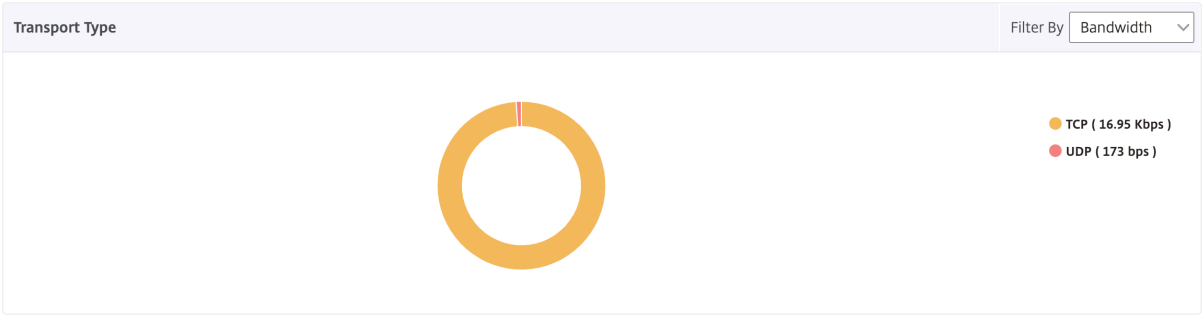
支持 **HDX Insight** 中的 **EDT**

Citrix Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示 HDX Insight 的分析信息。也就是说, ADM 现在同时支持 UDP 和 TCP 协议。对 Citrix Gateway 的 EDT 支持可确保运行 Citrix Receiver 的用户在虚拟桌面中获得高清晰度的会话中用户体验。

HDX Insight 现在在活动会话报告中显示 EDT 会话和非 EDT 会话的数量。“用户”(Users) 表格显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传、RTO 等衡量指标，以及当前从 TCP 堆栈计算时确实具有 EDT 会话的用户不可用。因此，它们将显示为“NA”。

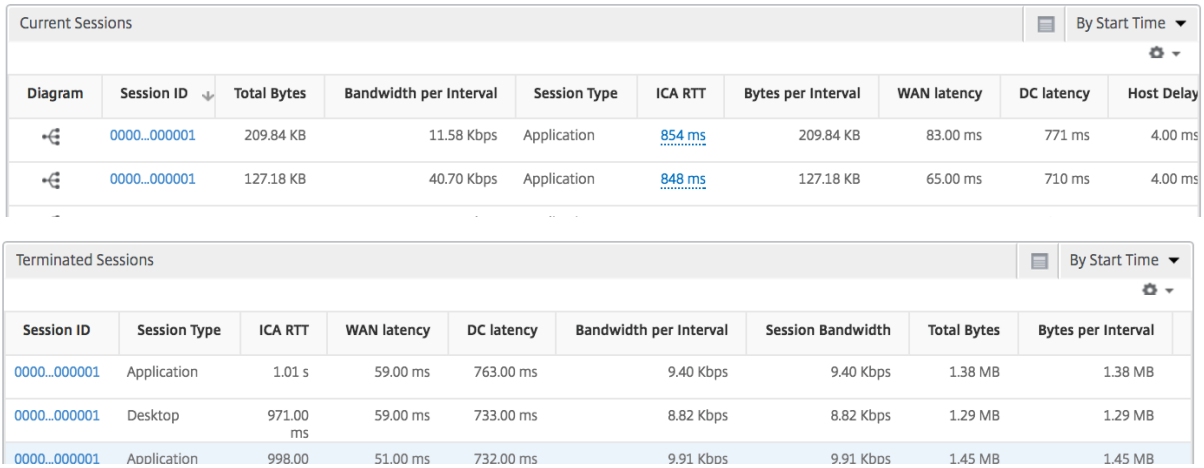


引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。



Citrix ADM 12.0 及更高版本中提供的 **HDX Insight** 分析指标：

L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。交付路径中存在非 Citrix 设备的情况下，此指标很有用。
L7 Server-side Latency（L7 服务器端延迟）	NetScaler 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。交付路径中存在非 Citrix 设备的情况下，此指标很有用。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。

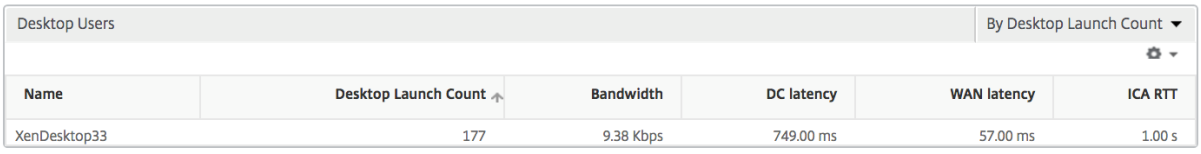


Desktop Users（桌面用户）

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

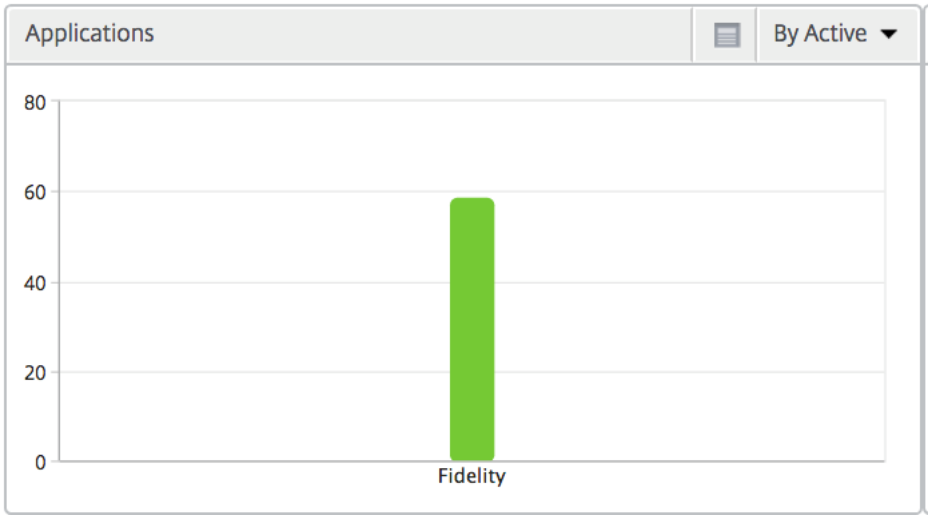
指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。

指标	说明
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。



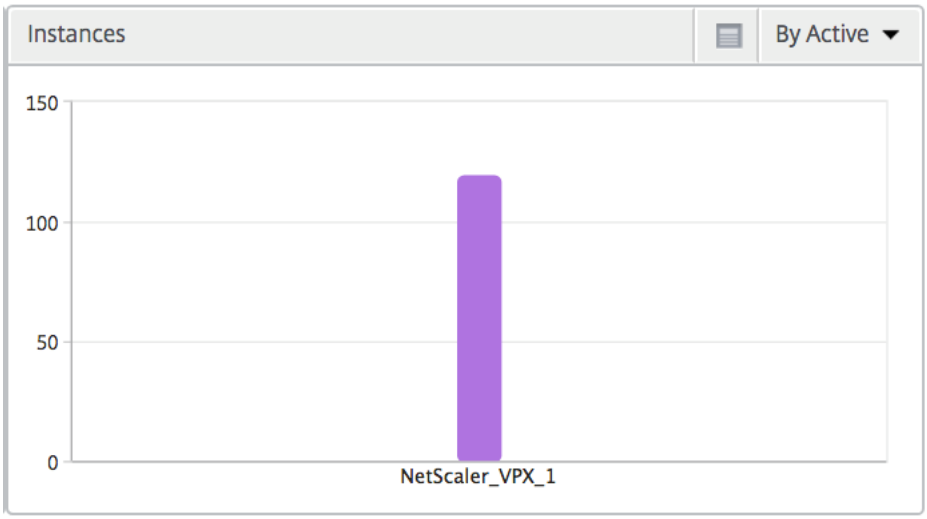
应用程序

表示按活动、会话启动总数、应用程序启动总数和启动持续时间排序的应用程序的条形图。



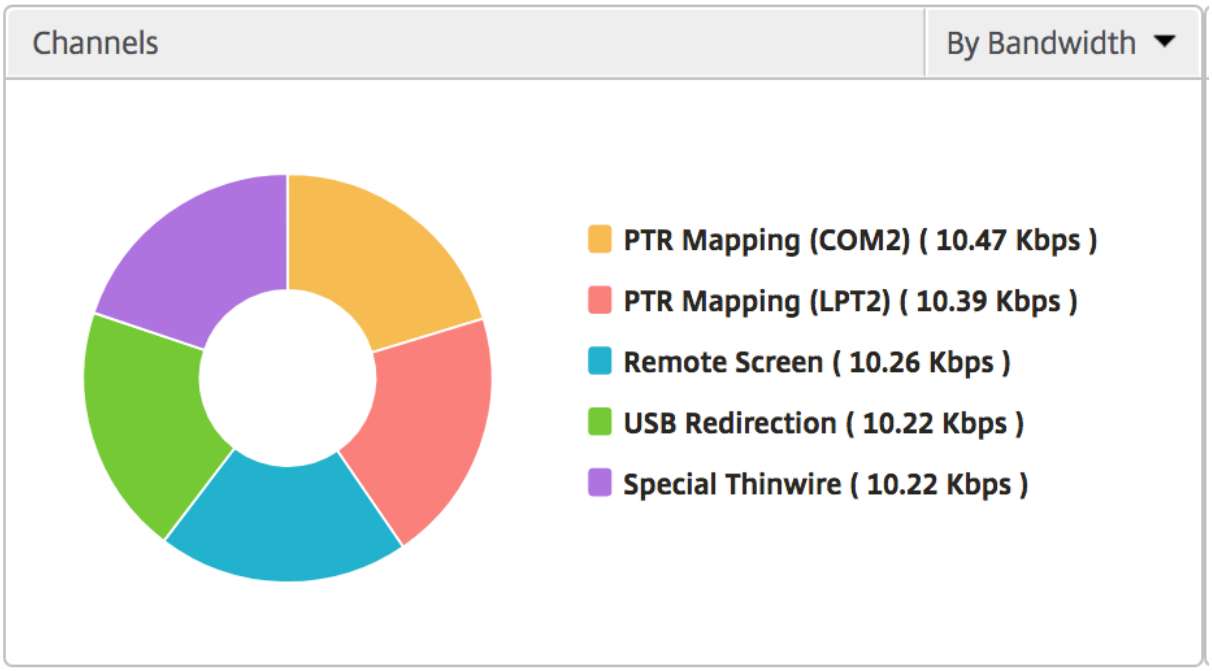
实例

表示按活动应用程序和总应用程序排序的 NetScaler 实例的条形图



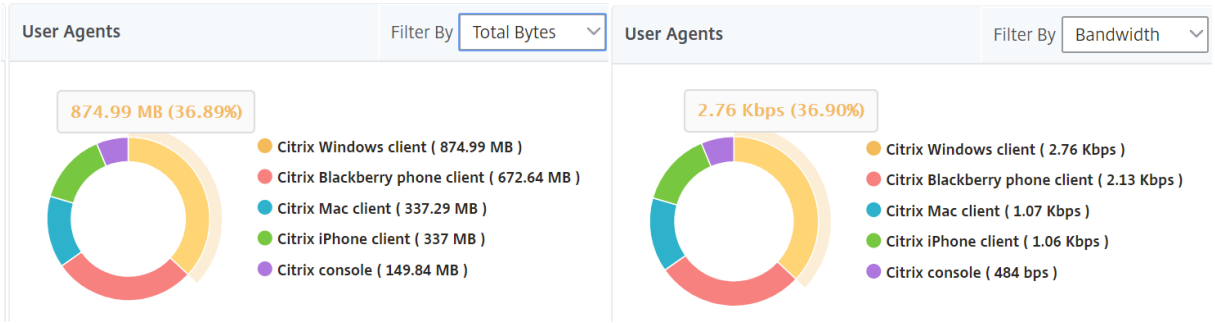
Channels（通道）

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



User Agents（用户代理）

“User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



Per User Session View（每个用户会话视图）

“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

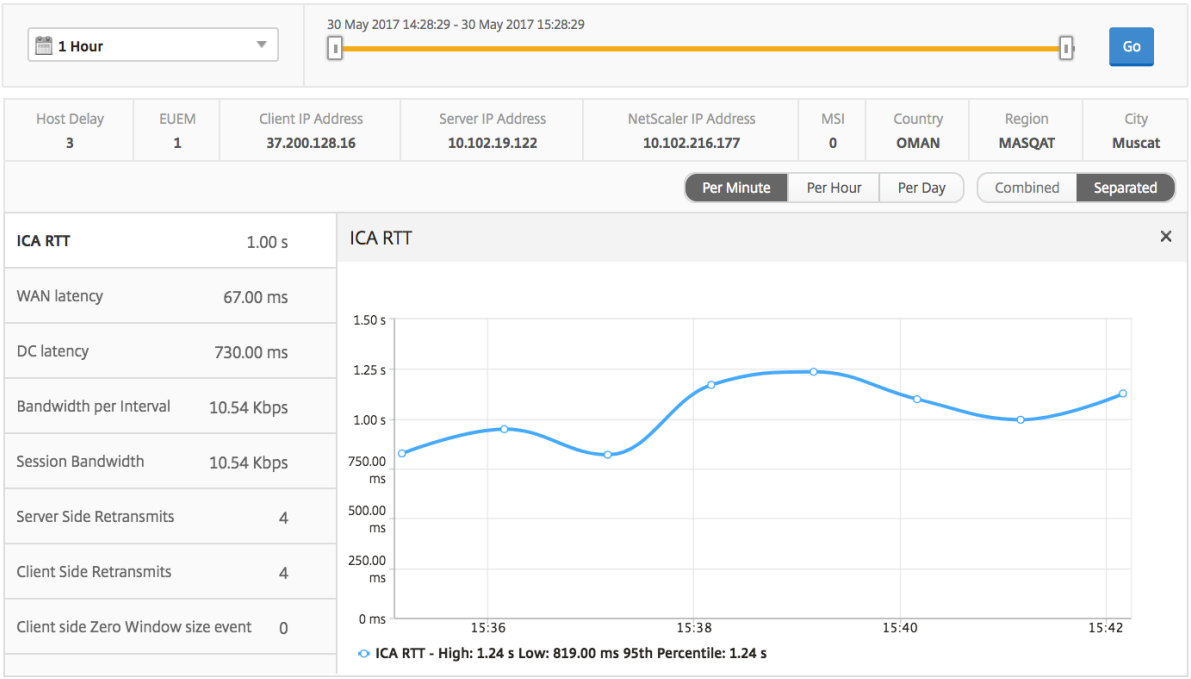
要查看选定用户会话的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或已终止的会话列中选择一个会话。

时间线图

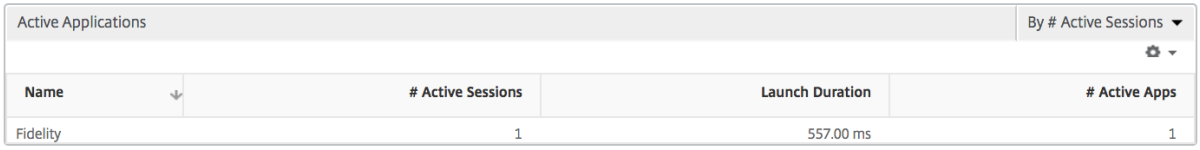
指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	在 NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接上发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



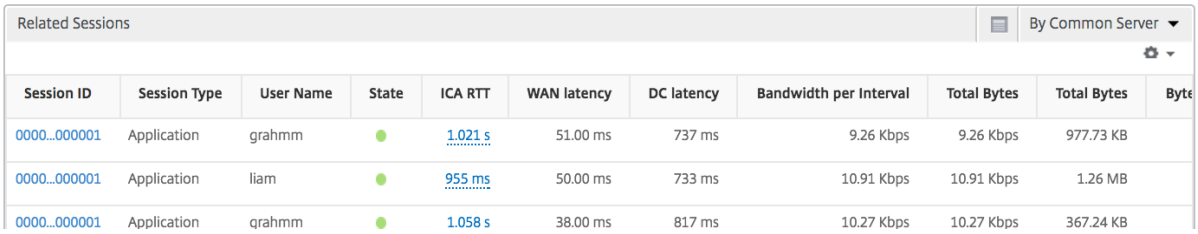
活动应用程序

“Active Applications”（活动应用程序）部分显示选定用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间排序。



Related Sessions（相关会话）

“Related Sessions”（相关会话）部分显示选定用户的会话的相关会话。可以选择该关系作为公用服务器或通用 NetScaler。



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	

“**Instance**”（实例）视图报告和指标

February 6, 2024

“Instance”（实例）视图中的报告和指标针对的是 NetScaler s 实例。

要导航到“实例”视图，请执行以下操作：

1. 使用受支持的 Web 浏览器登录到 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 实例。

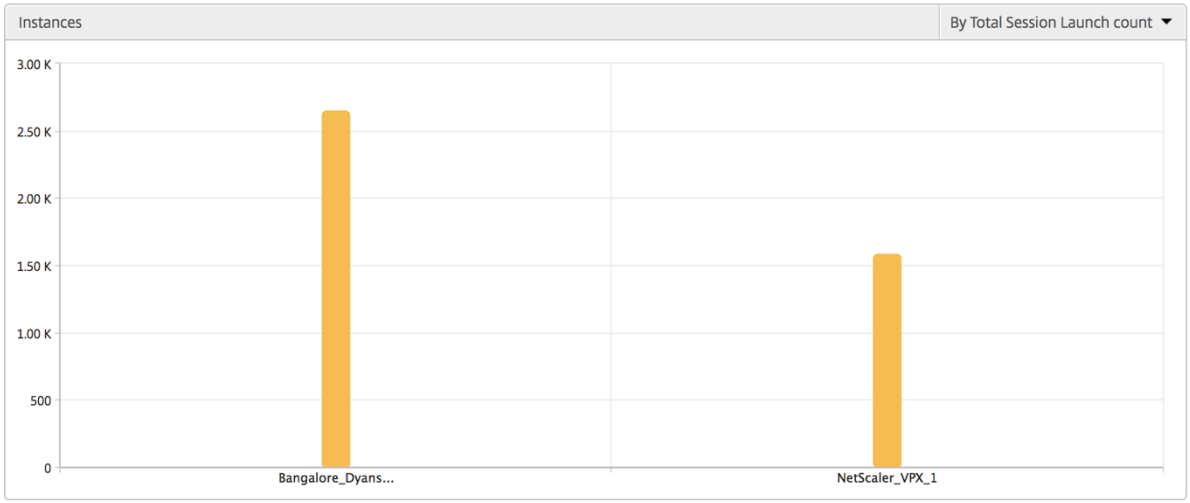
Instance Summary View（实例摘要视图）

此视图称为摘要视图，因为它显示了添加到 Citrix ADM 的所有 NetScaler 实例的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

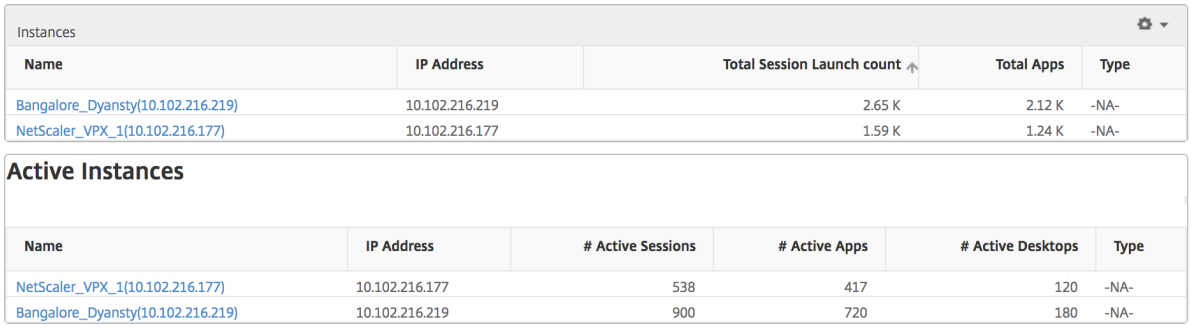
“**Instances**”（实例）条形图

此图表显示实例与会话总启动次数和应用总数，可从图表画布右上角的下拉菜单中选择。



实例/活动实例摘要报告

指标	说明
名称	NetScaler 实例的主机名。
IP 地址	NetScaler IP 地址。
Total Session Launch Count（会话启动总数）	在给定时间间隔内创建的唯一用户会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用


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-

阈值报告

阈值报告表示在选定时间段内将实体选为实例的违反阈值计数。有关更多信息，请参阅如何创建阈值和警报。

跳过的流

跳过的流是跳过解析 ICA 连接的记录。这可能是由于多种原因造成的，例如使用不支持的 Citrix Virtual Apps and Desktops 版本、接收器或接收方类型不支持的版本等。此表显示 IP 地址和跳过的流计数。这些 Receiver 可能不属于列入白名单的 Receiver；因此，监视时跳过了这些会话。

请参阅 **Error! Hyperlink reference not valid.**（错误! 超链接引用无效。）了解与 ICA 解析有关的问题的更多详细信息。

Skipped Flows

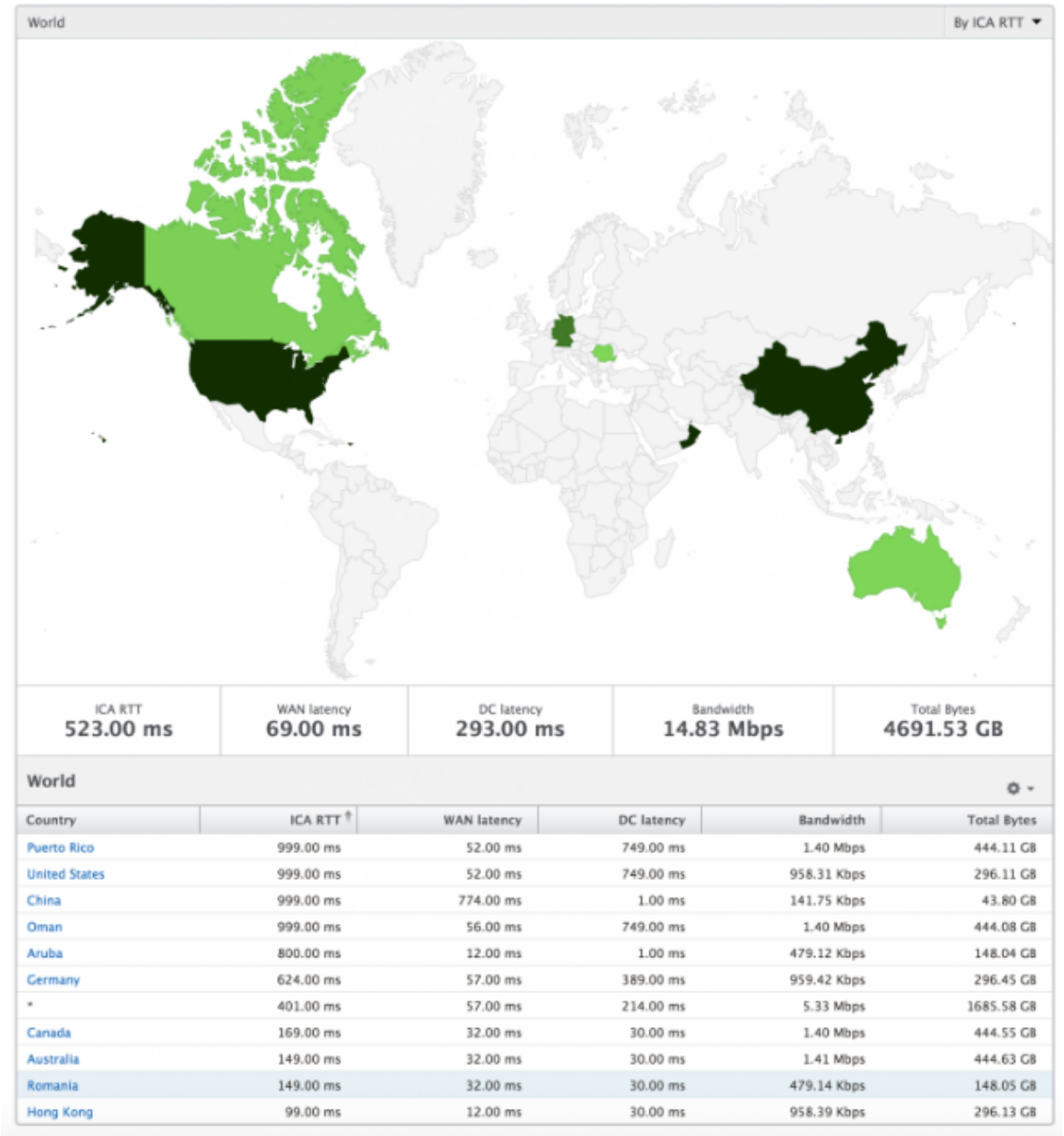
IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

“**World**”（世界）视图

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以使用系统的“World”（世界）视图，只需单击区域即可深入查看特定国家/地区以及进一步深入到城市。管理员可以按城市和省/自治区进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

可以在 HDX Insight 中的世界地图上查看以下详细信息，每个指标的密度以热度地图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



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

Per Instance View（每个实例视图）

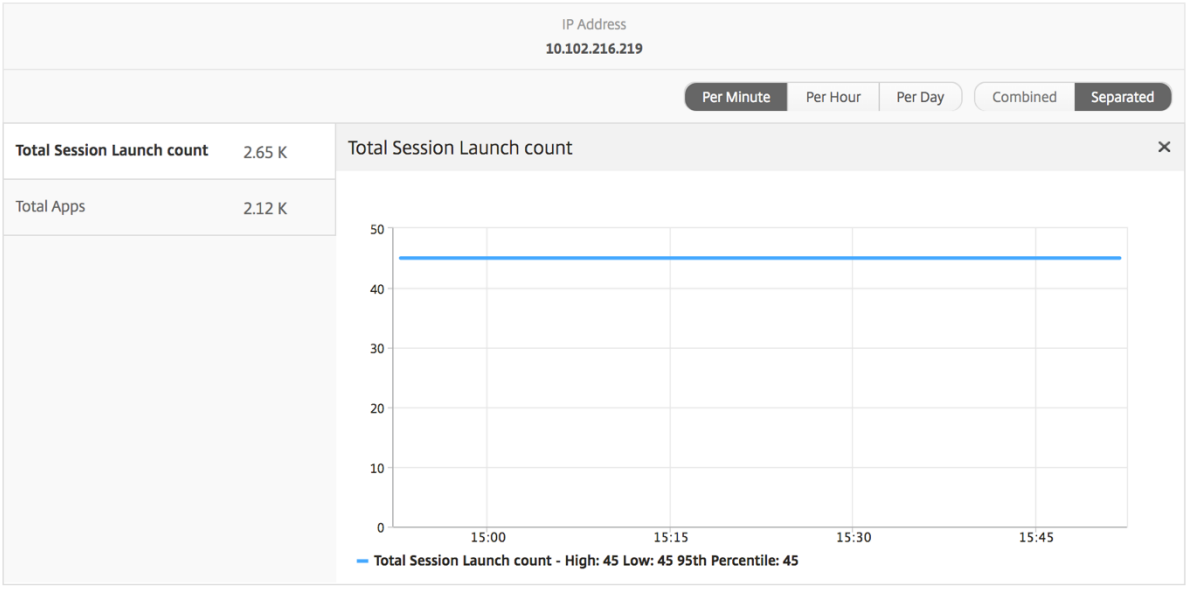
每个实例视图为特定选定的 NetScaler 实例提供详细的最终用户体验报告。

要导航到“实例”视图，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 实例。
2. 从实例摘要报告中选择特定实例。

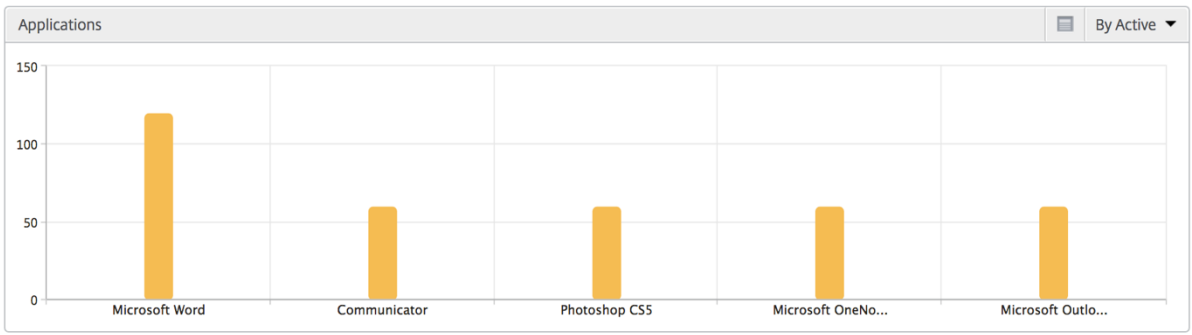
折线图

指标	说明
IP 地址	此项表示选定实例的 NetScaler IP 地址。
Total Session Launch count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。



“应用程序”条形图

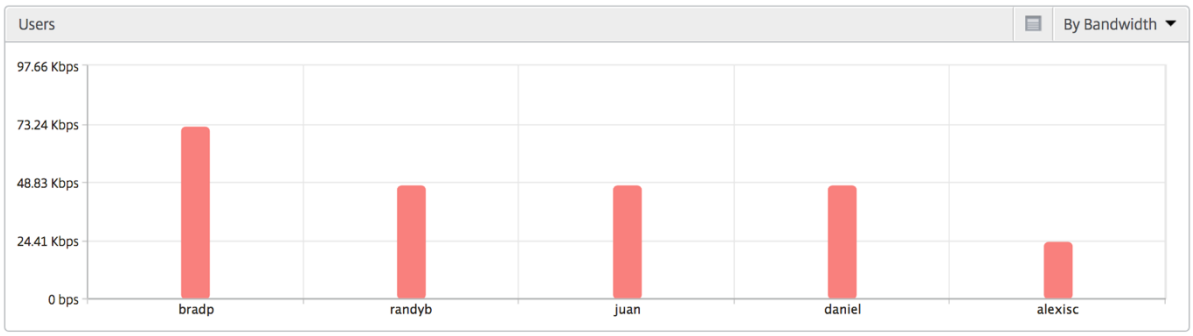
基于以下条件显示排在前 5 位的应用程序 - 按活动应用程序数、会话启动总数、应用程序启动总数或启动持续时间。



“**Users**”（用户）条形图

“Users”（用户）条形图基于以下条件显示排在前 5 位的用户

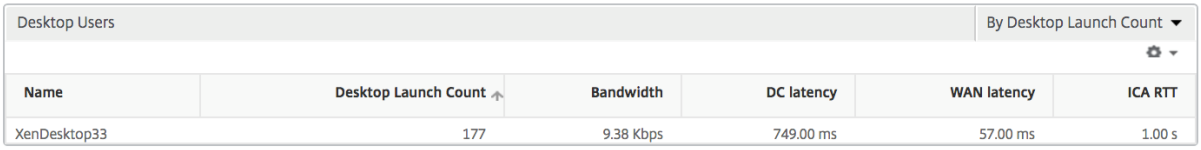
- Bandwidth（带宽）
- WAN 延迟
- DC 延迟
- ICA RTT



“**Desktop Users**”（桌面用户）报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC 延迟	网络的服务器端导致的延迟。即从 NetScaler 到后端服务器。
WAN 延迟	网络的客户端导致的延迟。即从 NetScaler 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

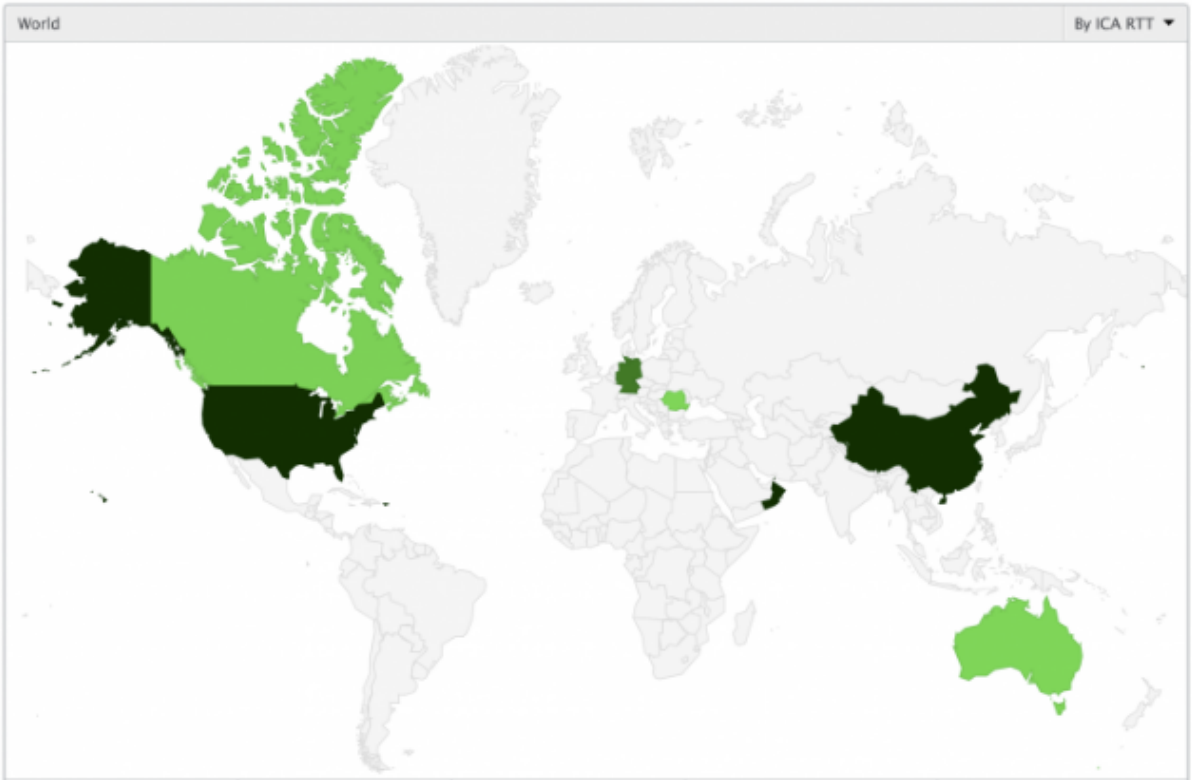


“**World**”（世界）视图

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以使用系统的“World”（世界）视图，只需单击区域即可深入查看特定国家/地区以及进一步深入到城市。管理员可以按城市和省/自治区进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

可以在 HDX Insight 中的世界地图上查看以下详细信息，每个指标的密度以热度地图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
523.00 ms	69.00 ms	293.00 ms	14.83 Mbps	4691.53 GB

World

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

“**License**”（许可证）视图报告和指标

February 6, 2024

许可证视图提供了有 Citrix Gateway 许可证信息的详细信息。

要导航到“许可证”视图，请执行以下操作：

1. 使用支持的网络浏览器登录到您的 NetScaler MA Service。
2. 导航到 分析 > **HDX Insight** > 许可证。

折线图

指标	说明
正在使用的许可证	在选定的时间轴内使用的 Citrix Gateway CCU 许可证。每个计数均表示用户会话数。这与用户启动的应用程序和桌面会话无关。
Total licenses（许可证总数）	可供客户使用的 Citrix Gateway CCU 许可证总数。

!本地化后的图片

阈值报告

阈值报告表示在选定期间内将实体选为许可证的违反阈值计数。有关更多信息，请参阅如何创建阈值和警报。

对 **HDX Insight** 问题进行故障排除

February 6, 2024

如果 HDX Insight 解决方案未按预期运行，则问题可能出在以下情况之一。有关故障排除，请参阅相应部分中的清单。

- HDX Insight 配置。
- Citrix ADC 和 Citrix ADM 之间的连接。
- 在 Citrix ADC 中生成 HDX/ICA 流量的记录。
- Citrix ADM 中的记录总量。

HDX Insight 配置清单

- 确保在 Citrix ADC 中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 Citrix ADC 运行配置中的 HDX Insight 配置。

  执行 `show running | grep -i <appflow_policy>` 命令以检查 HDX Insight 配置。确保绑定类型为 ICA 请求。例如;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  对于透明模式，绑定类型必须为 ICA_REQ_DEFAULT。例如;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- 对于单跃点/Access Gateway 或双跃点部署，请确保 HDX Insight AppFlow 策略绑定到 VPN 虚拟服务器，HDX/ICA 流量正在流动。
- 对于透明模式或局域网用户模式，请确保设置 ICA 端口 1494 和 2598。
- 检查 Citrix Gateway 或 VPN 虚拟服务器中的“appflowlog”参数启用了 Access Gateway 或双跳部署。有关详细信息，请参阅 为虚拟服务器启用 AppFlow。
- 选中双跃点 Citrix ADC 中已启用“连接链接”。有关详细信息，请参阅 配置 Citrix Gateway 设备以导出数据。
- HA 故障转移后，如果 HDX Insight 详细信息被跳过解析，请检查 ICA 参数“enableSRonHAFailover”是否已启用。有关详细信息，请参阅 Citrix ADC 高可用性对上的会话可靠性。

Citrix ADC 与 **Citrix ADM** 之间的连接检查表

- 检查 Citrix ADC 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 Citrix ADC 和 AppFlow Collector 之间的连接状态。
- 检查 HDX Insight AppFlow 策略命中。

  执行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中率。

  您还可以导航到 GUI 中的“系统”**>**“**AppFlow**”**>**“策略”，以检查 AppFlow 策略命中。
- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

在 **Citrix ADC** 核对表中为 **HDX/ICA** 流量生成记录

执行日志验证命令 `tail -f /var/log/ns.log | grep -i "default ICA Message"`。根据生成的日志，您可以使用此信息进行故障排除。

- 日志：跳过解析 **ICA** 连接 **-** 此主机不支持 **HDX Insight**

  原因：Citrix Virtual Apps and Desktops 版本不受支持

  解决办法：将 Citrix Virtual Apps and Desktops 服务器升级到受支持的版本。

- 日志：**Client type received 0x53, NOT SUPPORTED**

  原因：Citrix Workspace 应用程序不受支持的版本

  解决方案：将 Citrix Workspace 应用程序升级到受支持的版本。有关详细信息，请参阅 Citrix Workspace 应用程序。

- 日志：来自扩展数据包的错误-跳过此流的所有 **hdx** 处理

  原因：解压缩 ICA 流量时出现问题

  解决方案：在建立新会话之前，此 ICA 会话没有可用的报告。

- 日志：无效过渡：**NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_ST_UNINIT**”

  原因：解析 ICA 握手时出现问题

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：缺少 **EUEM ICA RTT**

  原因：无法解析最终用户体验监视通道数据

  解决方案：确保在 Citrix Virtual Apps and Desktops 服务器上启动了最终用户体验监视服务。确保您使用的是受支持的 Citrix Workspace 应用程序版本。

- 日志：通道标头无效

  原因：无法识别通道头

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：跳过代码

  如果您看到以下任何跳过代码值，则会跳过解析 Insight 详细信息。

  > 跳过代码 0 表示记录已成功从 Citrix ADC 导出。

跳过代码	错误消息	错误原因
100	NS_ICA_ERR_NULL_FRAG	处理 ICA 碎片时出错，可能是内存状况造成的
101	NS_ICA_ERR_INVALID_HS_CMD	收到的握手命令无效
102	NS_ICA_ERR_REDUC_PARAM_CNT	为 V3 扩展器初始化指定的参数无效
103	NS_ICA_ERR_REDUC_INIT	无法正确初始化 V3 扩展器
104	NS_ICA_ERR_REDUC_PARAM_BYTES	字节不足，无法将编码器分配给通道
105	NS_ICA_ERR_INVALID_CHANNEL	ICA 通道号无效
106	NS_ICA_ERR_INVALID_DECODER	为通道指定的解码器无效

跳过代码	错误消息	错误原因
107	NS_ICA_ERR_INVALID_TW_PARAM	在 Thinwire 通道上指定的参数计数无效
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwire 通道的解码器无效
109	NS_ICA_ERR_REDUC_NO_DECODER	没有为通道定义解码器
110	NS_ICA_ERR_REDUC_V3_EXPANDER	无法扩展通道数据
111	NS_ICA_ERR_REDUC_BYTES_V3_COR	扩展器错误：消耗的字节多于可用字节
112	NS_ICA_ERR_REDUC_BYTES_OOR	错误：未压缩的数据溢出
113	NS_ICA_ERR_REDUC_INVALID_CMD	未定义的扩展器命令
114	NS_ICA_ERR_CGP_FILL_HOLE	处理拆分 CGP 帧时出错
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB 分配错误—由于内存不足
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	扩展器上下文的内存分配错误
117	NS_ICA_ERR_ICA_OLD_SERVER	旧服务器，不支持功能块
118	NS_ICA_ERR_PIR_MANY_FRAG	数据包初始化请求被分段，无法处理
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 功能初始化错误
120	NS_ICA_ERR_NO_MSI_SUPPORT	主机不支持 MSI 功能。表示低于 6.5 的 XenApp 版本或低于 5.0 的 XenDesktop 版本
121	NS_ICA_ERR_CGP_INVALID_CMD	遇到无效的 CGP 命令
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	通道上的字节数不足
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL 或 SEAMLESS 通道上的数据不正确
124	NS_ICA_ERR_INVALID_PURE_CMD	处理 PURE ICA 通道数据时收到无效命令
125	NS_ICA_ERR_INVALID_PURE_LEN0	处理 PURE ICA 通道数据时遇到无效长度
126	NS_ICA_ERR_INVALID_PURE_LEN	处理 PURE ICA 通道数据时遇到无效长度
127	NS_ICA_ERR_INVALID_CLNT_DATA	从客户端接收到的数据长度无效
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID 大小错误
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	检测到无效的通道头
130	NS_ICA_ERR_CGP_PARSE_RECONNECT	尝试重新连接的会话失败

跳过代码	错误消息	错误原因
131	NS_ICA_ERR_DISABLE_SR_NON_NS_RECONNECT	禁用 SR 时出错
132	NS_ICA_ERR_REDUC_NOT_V3	不支持的 ICA Reducer 版本
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	已禁用压缩，主机不支持压缩
134	NS_ICA_ERR_IDENT_PROTO	无法识别 ICA 或 CGP 协议，接收器不正确
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 签名或幻字符串不正确
136	NS_ICA_ERR_PARSE_RAW	解析 ICA 握手数据包时出错
137	NS_ICA_ERR_INCOMPLETE_PKT	握手时收到的数据包不完整
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA 帧太大，超过 1460 字节
139	NS_ICA_ERR_FORWARD	转发 ICA 数据时出错
140	NS_ICA_ERR_MAX_HOLES	无法处理 CGP 命令，因为它被拆分超出了支持的限制
141	NS_ICA_ERR_ASSEMBLE_FRAME	无法正确重组 ICA 框架
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	已跳过此接收器（客户端）的 ICA 解析，因为它不在白名单中
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	无法检测客户端重新连接 Cookie 的解析状态
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	客户端重新连接后检测到的重新连接 Cookie 长度无效
145	NS_ICA_ERR_INVALID_RECONNECT_ID	客户端重新连接 cookie 错过了所需的约束
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	从客户端接收到的 Receiver 版本字符串无效
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	从客户端收到的产品编码无效
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	扩展后的通道长度无效
149	NS_ICA_ERR_SPECIAL_THINWIRE	解压缩错误
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	遇到无法执行无缝命令的字节不足的问题
151	NS_ICA_ERR_EUEM_INSUFFBYTE	遇到 EUEM 命令的字节不足
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	无缝通道解析的事件无效
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL 通道解析的事件无效
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEM 通道解析的事件无效
155	NS_ICA_ERR_USB_INVALID_EVENT	USB 通道解析的事件无效

跳过代码	错误消息	错误原因
156	NS_ICA_ERR_PURE_INVALID_EVENT	纯通道解析的事件无效
157	NS_ICA_ERR_VCP_INVALID_EVENT	虚拟通道解析的事件无效
158	NS_ICA_ERR_ICAP_INVALID_EVENT	ICA 数据解析的事件无效
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGP 数据解析的事件无效
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	基本加密中 crypt 命令的状态无效
161	NS_ICA_ERR_BASICCRYPT_INVALIDCMD	基本加密中的 crypt 命令无效
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	RC5 加密中 crypt 命令的状态无效
163	NS_ICA_ERR_ADVCRYPT_INVALIDCMD	RC5 加密中的 crypt 命令无效
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5 加密/解密时出错
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5 加密/解密时出错
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA 不支持 Reducer 版本 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	接收器不支持 Reducer 版本 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA 握手中出现意外的字节数
169	NS_ICA_ERR_HIGHER_RECONSEQ	从对等后重新连接获得更高的 CGP 恢复序列号
170	NS_ICA_ERR_DESCSRINFO_ABSENT	重新连接后无法恢复 ICA 解析状态
171	NS_ICA_ERR_NSAP_PARSING	解析 Insight 通道数据时出错
172	NS_ICA_ERR_NSAP_APP	从 Insight 渠道数据解析应用详细信息时出错
173	NS_ICA_ERR_NSAP_ACR	解析 Insight 通道数据中的 ACR 详细信息时出错
174	NS_ICA_ERR_NSAP_SESSION_END	从 Insight 通道数据解析会话结束详细信息时出错
175	NS_ICA_ERR_NON_NSAP_SN	由于缺少 Insight 渠道支持，跳过了服务节点上的 ICA 解析
176	NS_ICA_ERR_NON_NSAP_CLIENT	客户端不支持 NSAP
177	NS_ICA_ERR_NON_NSAP_SERVER	VDA 不支持 NSAP
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAP 数据协商时出错
179	NS_ICA_ERR_SN_RECONNECT_TKT_FETCH	在服务节点中获取服务重新连接票证时出错
180	NS_ICA_ERR_SN_HIGHER_RECONSEQ	在服务节点中接收更高的重新连接序列号时出错

跳过代码	错误消息	错误原因
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_FOR_NONSSL	禁用非 SSL 连接的 HDXinsight 时出错

示例日志：

```
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]"
```

```
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]"
```

错误计数器

ICA 解析时会捕获各种计数器。下表列出了用于 ICA 解析的各种计数器。
执行查看计数器详细信息 `nsconmsg -g hdx -d statswt0`的命令。

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_tot_ica_conn	指示 NS 检测到的纯 ICA 连接的总数。每当检测到基于客户端 PCB 上的 ICA 签名的 ICA 连接时，就会递增。	统计信息
hdx_tot_cgp_conn	指示 NS 检测到的 CGP 连接总数（会话可靠性开启）。每当检测到基于客户端 PCB 上的 CGP 签名的 CGP 连接时，就会递增。	统计信息
hdx_dbg_tot_udt_conn	表示 NS 检测到的 UDP ICA 连接总数	统计信息

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_dbg_tot_nsap_conn	表示 NS 检测到的支持 NSAP 的连接总数	统计信息
hdx_tot_skip_conn	表示由于 ICA 或 CGP 签名无效，解析器跳过了多少个 ICA 连接。	统计信息
hdx_dbg_active_conn	当时活跃的 EDT/CGP/ICA 连接总数。	统计信息
hdx_dbg_active_nsap_conn	当时活跃的 EDT/CGP/ICA NSAP 连接总数。	统计信息
hdx_dbg_skip_appflow_disabled	由于禁用 AppFlow 而将 AppFlow 从会话中分离的实例总数	统计/诊断
hdx_dbg_transparent_user	透明用户访问的总数	统计/诊断
hdx_dbg_ag_user	Access Gateway 用户访问总数	统计/诊断
hdx_dbg_lan_user	局域网用户模式访问总数	统计/诊断
hdx_basic_enc	指示使用基本加密的 ICA 连接数	统计/诊断
hdx_advanced_enc	表示使用基于 RC5 的高级加密的 ICA 连接数	统计/诊断
dx_dbg_wanscaler_on_clientside	客户端上有 Citrix SD-WAN 的 CGP/ICA 连接总数	统计/诊断
hdx_dbg_wanscaler_on_serversid	具有 Citrix SD-WAN 服务器端的 CGP/ICA 连接总数	统计/诊断
hdx_dbg_reconnected_session	来自客户端的未出现任何 Citrix ADC 错误的重新连接请求总数	统计/诊断
被拒绝的主机重新连接	客户端拒绝的重新连接请求的主机总数	统计/诊断
hdx_euem_available	指示具有“最终用户体验监视”通道可用的连接数。需要使用最终用户体验监视通道来收集 ICA RTT 等统计信息。	统计/诊断
已禁用的高清错误	使用 nsapimgr 旋钮禁用会话可靠性。会话不适用于此会话。	错误
hdx_err_skip_no_msi	XA/XD 服务器缺少 MSI 功能。这表示服务器版本较旧，HDX Insight 会跳过此连接。	错误
hdx_err_skip_old_server	不支持的旧服务器版本	错误
高清错误白名单	客户端接收器不在白名单中，HDX Insight 将跳过此连接	错误

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_sm_ica_cam_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CAM_CHANNEL 总数	诊断
hdx_sm_ica_usb_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_USB_CHANNEL 总数	诊断
hdx_sm_ica_clip_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CLIP_CHANNEL 总数	诊断
hdx_sm_ica_ccm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CCM_CHANNEL 总数	诊断
hdx_sm_ica_cdm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CDM_CHANNEL 总数	诊断
hdx_sm_ica_com1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM1_CHANNEL 总数	诊断
hdx_sm_ica_com2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM2_CHANNEL 总数	诊断
hdx_sm_ica_cpm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CPM_CHANNEL 总数	诊断
hdx_sm_ica_lpt1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT1_CHANNEL 总数	诊断
hdx_sm_ica_lpt2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT2_CHANNEL 总数	诊断
dx_dbg_sm_ica_msi_disabled	通过 SmartAccess 策略禁用 MSI 的案例总数	诊断
hdx_sm_ica_file_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_FILE_CHANNEL 总数	诊断
hdx_dbg_usb_accept_device	接受的 USB 设备总数	诊断
hdx_dbg_usb_reject_device	拒绝的 USB 设备总数	诊断
hdx_dbg_usb_reset_endpoint	重置的 USB 端点总数	诊断
hdx_dbg_usb_reset_device	重置的 USB 设备总数	诊断
hdx_dbg_usb_stop_device	已停止的 USB 设备总数	诊断
hdx_dbg_usb_stop_device_response	来自已停止的 USB 设备的响应总数	诊断
hdx_dbg_usb_device_gone	消失的 USB 设备总数	诊断
hdx_dbg_usb_device_stopped	已停止的 USB 设备总数	诊断

nstrace validation

检查 CFLOW 协议以查看 Citrix ADC 中的所有 AppFlow 记录。

Citrix ADM 核对表中的记录填写

- 执行命令 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"`并检查日志以确认 Citrix ADM 正在接收 AppFlow 记录。
- 确认已将 Citrix ADC 实例添加到 Citrix ADM 中。
- 验证 Citrix Gateway/VPN 虚拟服务器是否已在 Citrix ADM 中获得许可。
- 确保为双跃点启用了多跳参数设置。
- 确保 Citrix Gateway 在双跃点部署中已获得第二跃点许可。

在联系 Citrix 技术支持之前

要快速解决问题，请确保在联系 Citrix 技术支持之前已掌握以下信息：

- 部署和网络拓扑的详细信息。
- Citrix ADC 和 Citrix ADM 版本。
- Citrix Virtual Apps and Desktops 服务器版本。
- 客户端 Receiver 版本。
- 发生问题时的活动 ICA 会话数。
- 通过在 Citrix ADC `show techsupport` 命令提示符下执行命令捕获的技术支持包。
- 为 Citrix ADM 捕获的技术支持包。
- 在所有 Citrix ADC 上捕获的数据包跟踪。
  要启动数据包跟踪，请键入，`start nstrace -size 0'`
  要停止数据包跟踪，请键入、`stop nstrace`
- 通过执行 `show arp` 命令收集系统 ARP 表中的条目。

已知问题

有关 HDX Insight 的已知问题，请参阅 Citrix ADC 发行说明。

Gateway Insight

February 6, 2024

在 Citrix Gateway 部署中，查看用户的访问详细信息对于解决访问失败问题至关重要。作为网络管理员，您希望知道用户何时无法登录 Citrix Gateway，并且希望了解用户活动和登录失败的原因，但除非用户发送解析请求，否则该信息通常不可用。

通过 Gateway Insight 可以查看所有用户登录 Citrix Gateway 时遇到的失败，而无论访问模式为何。可以查看所有可用用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。可以查看某个用户的端点分析 (EPA)、身份验证、单点登录 (SSO) 及应用程序启动失败。还可以查看某个用户的活动会话和已终止会话的详细信息。

通过 Gateway Insight 还可以查看虚拟应用程序的应用程序启动失败的原因。这可提高您对任何登录或应用程序启动失败问题进行故障排除的能力。您可以查看已启动的应用程序数量、总会话数和活动会话数、应用程序占用的总字节数和带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

您可以在任何给定时间查看与 Citrix Gateway 设备关联的所有网关的网关数量、活动会话数、总字节数和使用的带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活动的详细信息。

所有日志消息都存储在 Citrix ADM 数据库中，因此您可以查看任何时间段的错误详细信息。还可以查看登录失败摘要，并确定在登录过程的什么阶段发生了失败。

需要注意的事项

- 以下部署支持 Gateway Insight：
  - Access Gateway
  - Unified Gateway
- Citrix ADM 的版本和版本必须与 Citrix Gateway 设备的版本相同或更晚。
- 对于具有企业许可证的 Citrix ADC 实例，可以查看一小时的 Gateway Insight 报告。查看超过一小时的 Gateway Insight 报告需要白金许可证。

限制

- 当身份验证方法配置为基于证书的身份验证时，Citrix Gateway 网关不支持 Gateway Insight。
- 对于 Gateway Insight 报告，Citrix ADC 设备不会提供地理位置信息。
- 在 HDX Insight“Users”（用户）控制板上只能看到虚拟 ICA 应用程序和桌面的成功用户登录、延迟及应用程序级别详细信息。

- 在双跃点模式下，无法查看第二个 DMZ 中的 Citrix Gateway 设备上的故障。
- 远程桌面协议 (RDP) 桌面访问问题不会报告。
- 以下身份验证类型支持 Gateway Insight。如果使用其他身份验证类型，您可能会在 Gateway Insight 中看到一些差异。
  - 本地
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - 本机 OTP

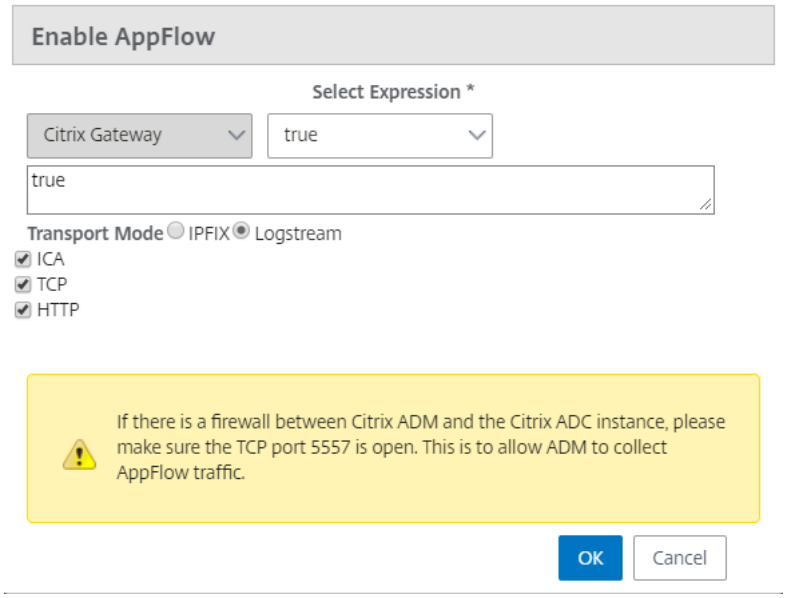
启用 **Gateway Insight**

要为您的 Citrix Gateway 设备启用 Gateway Insight，必须首先将 Citrix Gateway 设备添加到 Citrix ADM 中。然后必须为表示 VPN 应用程序的虚拟服务器启用 AppFlow。有关向 Citrix ADM 添加设备的信息，请参阅“添加设备”。

> 注意
>
> 要查看 Citrix ADM 中的端点分析 (EPA) 故障，必须在 CitCitrix Gateway 设备上启用 AppFlow 身份验证、授权和审核用户名记录。

在 **Citrix ADM** 中为虚拟服务器启用 **AppFlow**

1. 登录到 Citrix ADM。
2. 导航到“网络”**>**“实例”，然后选择要为其启用 **AppFlow** 的实例。
3. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。
4. 在“配置智能分析”页的“配置分析”下，选择 **Citrix Gateway**。
5. 选择要为其启用 AppFlow 的虚拟服务器，然后单击 启用 **AppFlow**。
6. 在启用 **AppFlow** 屏幕上的选择表达式列表中，单击“真”。
7. 在 传输模式旁边，选中 **Logstream** 复选框。



> 注意
>
> 您可以选择 IPFIX 或 `Logstream` 作为传输模式。

8. 单击确定。

使用 **GUI** 在 **Citrix Gateway** 设备上启用 **AppFlow** 身份验证、授权和审核用户名日志记录

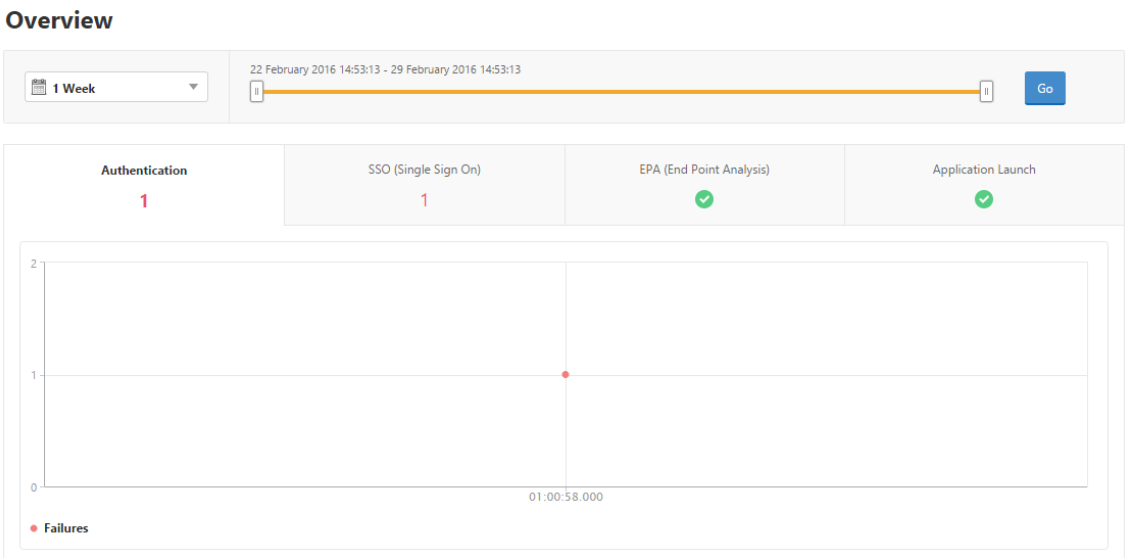
1. 导航到配置 **>** 系统 **> AppFlow >** 设置，然后单击更改 **AppFlow** 设置。
2. 在“配置 **AppFlow** 设置”屏幕中，选择 **AAA** 用户名，然后单击“确定”。

查看 **Gateway Insight** 报告

在 Citrix ADM 中，您可以查看与 Citrix Gateway 设备关联的所有用户、应用程序和网关的报告，也可以查看特定用户、应用程序或网关的详细信息。在“概 述”部分，您可以查看 EPA、SSO、身份验证和应用程序启动失败。还可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。

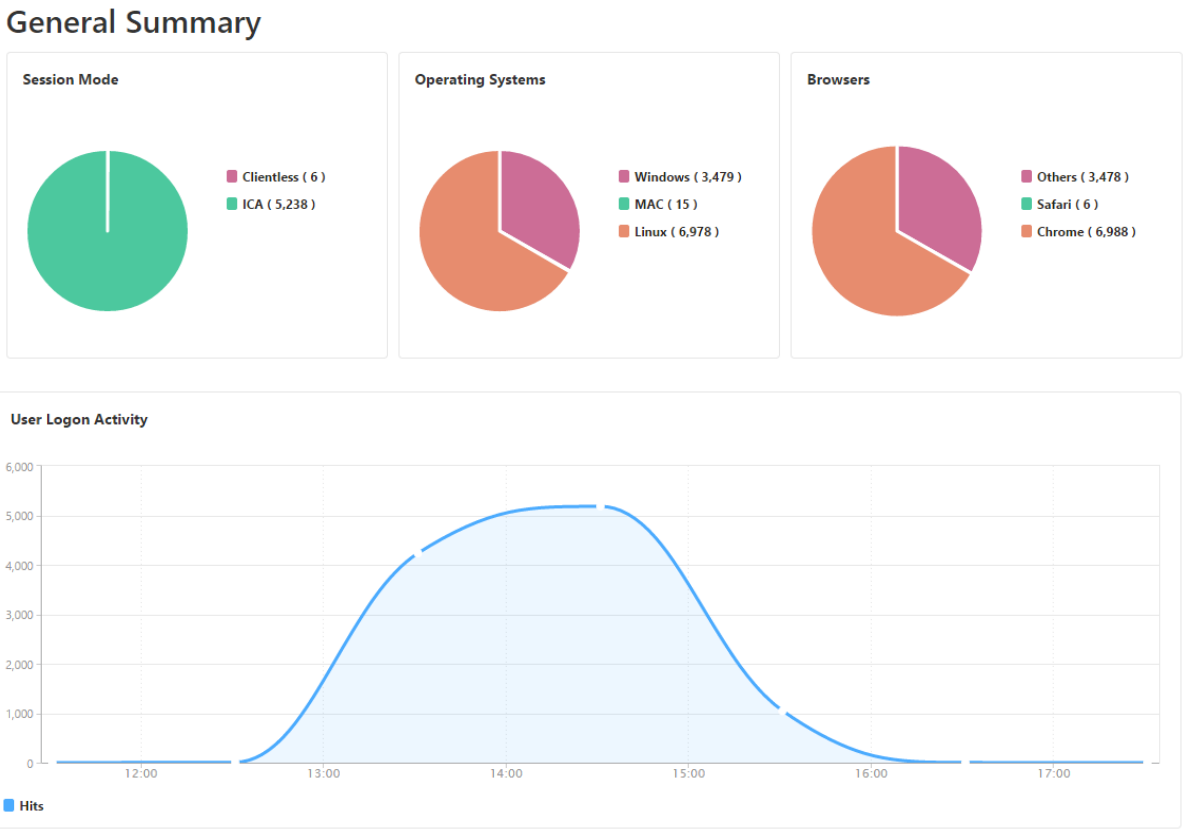
查看 **EPA**、**SSO**、身份验证、授权和应用程序启动失败

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 单击 “EPA (End Point Analysis)”（EPA(端点分析)）、“Authentication”（身份验证）、“Authorization”（授权）、“SSO (Single Sign On)”（SSO(单点登录)）或“Application Launch”（应用程序启动）选项卡以显示失败详细信息。



查看会话模式、客户端及用户数摘要

在 Citrix ADM 中，导航到分析 **> Gateway Insight**，向下滚动以查看报告。

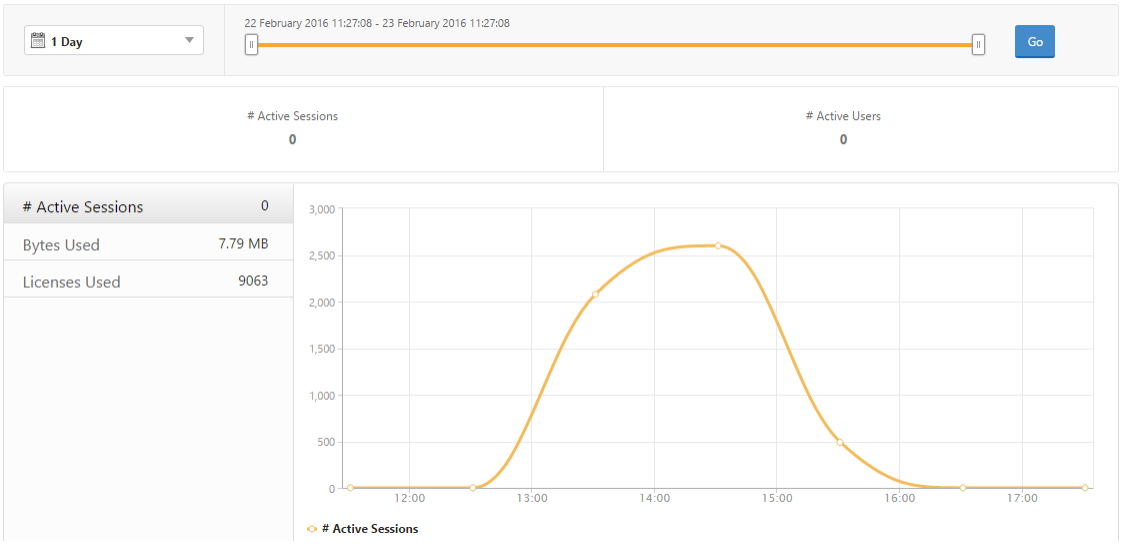


查看用户的 **Gateway Insight** 报告

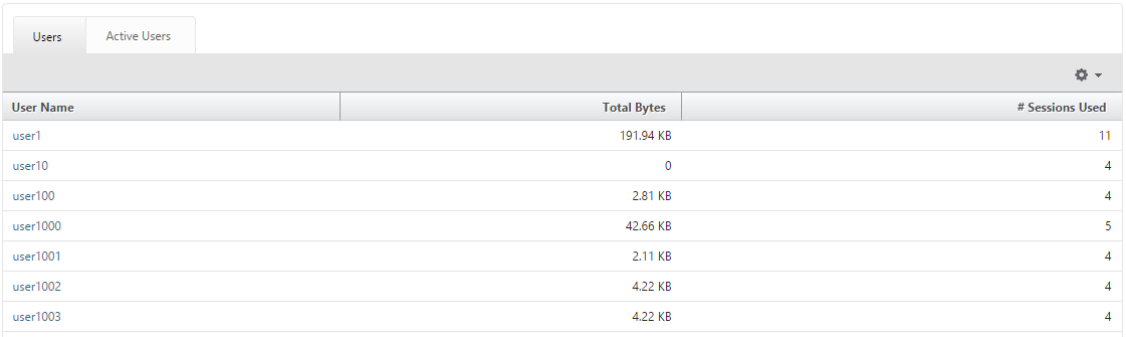
您可以查看与 Citrix Gateway 设备关联的所有用户的报告。可以查看某个用户的 EPA、身份验证、SSO 及应用程序启动失败。还可以查看某个用户的活动会话和已终止会话的详细信息。

查看用户详细信息

1. 在 Citrix ADM 中，导航到“分析”**>**“**Gateway Insight**”**>**“用户”。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 您现在可以查看活动用户数、活动会话数、字节数和所有用户在此期间使用的许可证。



向下滚动可查看可用用户和活动用户列表。



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

在“用 户”或“活动用户”选项卡上，可以单击“用户 名”列中的用户以显示该用户的 EPA、身份验证、SSO 和应用程序启动失败以及其他详细信息。

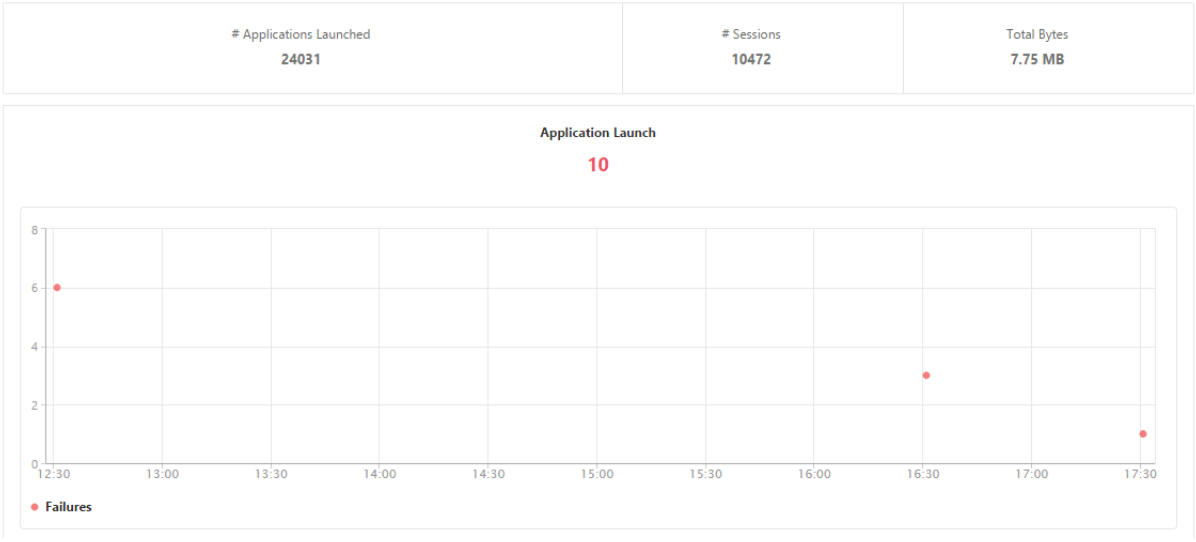
查看应用程序的 **Gateway Insight** 报告

您可以查看已启动的应用程序数量、总会话数和活动会话数、应用程序占用的总字节数和带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

查看应用程序详细信息

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight >** 应用程序。
2. 选择要查看应用程序详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在，您可以查看已启动的应用程序数量、总会话数和活动会话数、应用程序占用的总字节数和带宽。



向下滚动可查看 ICA 和其他应用程序使用的会话数、带宽及总字节数。

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

在其他应用程序选项卡上，您可以单击名称列中的应用程序以显示该应用程序的详细信息。

查看网关的 **Gateway Insight** 报告

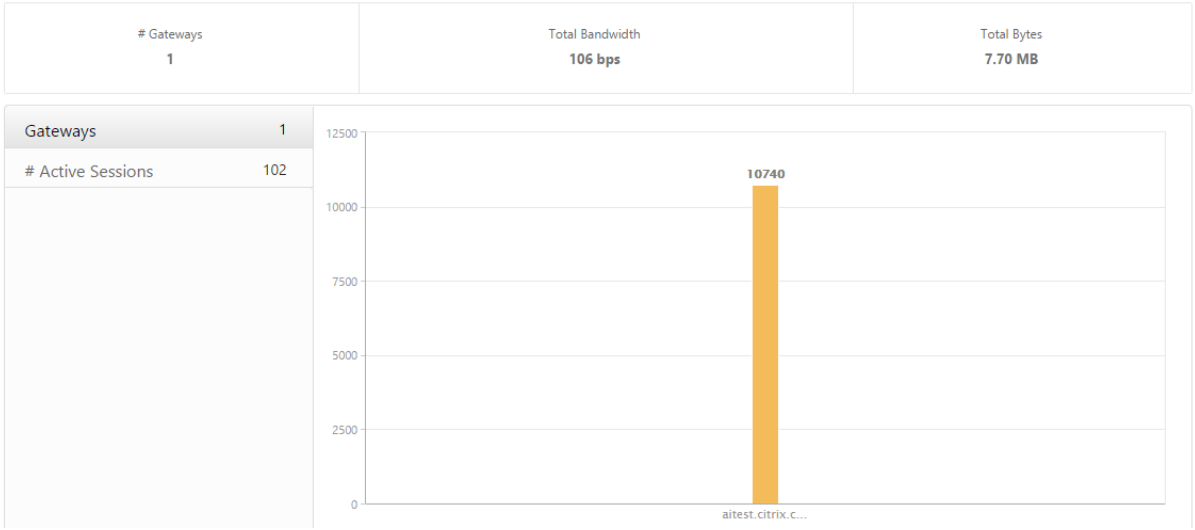
您可以在任何给定时间查看与 Citrix Gateway 设备关联的所有网关使用的网关数、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活

动的详细信息。

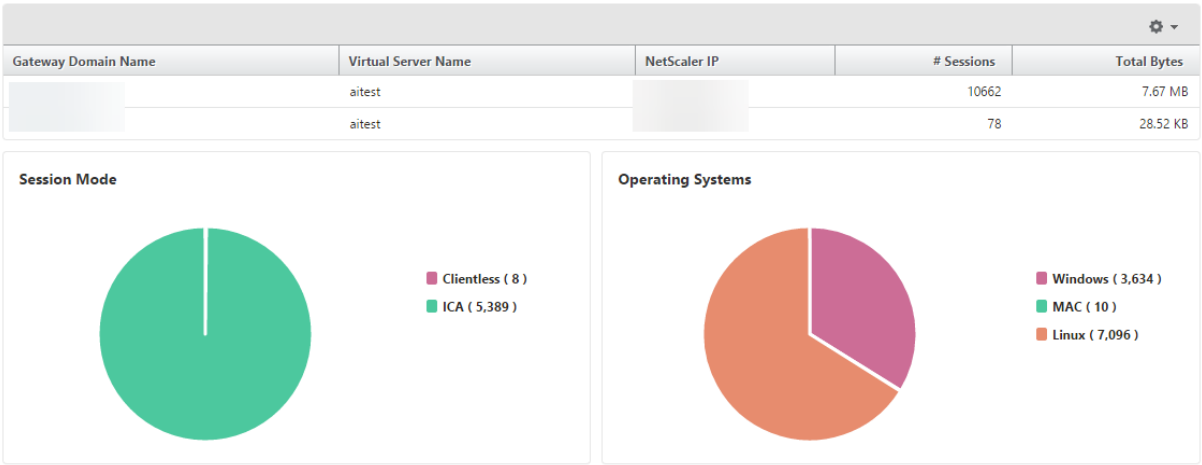
查看网关详细信息

1. 在 **Citrix ADM** 中，导航到分析 **> Gateway Insight >** 网关。
2. 选择要查看网关详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在，您可以查看与 Citrix Gateway 设备关联的所有网关在任何给定时间使用的网关数、活动会话数、总字节数和带宽。



向下滚动可查看网关详细信息，例如，“Gateway Domain Name”（网关域名）、“Virtual Server Name”（虚拟服务器名称）、NetScaler IP 地址、会话模式及“Total Bytes”（总字节数）。



您可以单击 Gateway 域名列中的 **Gateway** ，以显示网关的 EPA、身份验证、单点登录和应用程序启动失败以及其他详细信息。

导出报告

您可以在本地计算机上以 PDF、JPEG、PNG 或 CSV 格式将 GUI 中显示的所有详细信息保存 Gateway Insight 报告。您还可以计划以各种时间间隔将报告导出到指定的电子邮件地址。

> 注意
>
> - 具有只读访问权限的用户不能导出报告。
> - 仅当 Citrix ADM 具有互联网连接时，才会导出地理地图报告。

导出报告

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“立即导出”下，选择所需的格式，然后单击“导出”。

要计划导出：

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“计划导出”下，指定详细信息并单击“计划”。

要添加电子邮件服务器或电子邮件通讯组列表，请执行以下操作：

1. 在“配置”选项卡上，导航到“系统”>“通知”>“电子邮件”。
2. 在右窗格中，选择“电子邮件服务器”以添加电子邮件服务器，或选择“电子邮件通讯组列表”以创建电子邮件通讯组列表。
3. 指定详细信息，然后单击“创建”。

要导出整个 **Gateway Insight** 控制板：

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“立即导出”下，选择 **PDF** 格式，然后单击“导出”。

Gateway Insight 用例

以下使用案例展示了如何使用 Gateway Insight 在 Citrix Gateway 设备上查看用户的访问详细信息、应用程序和网关。

用户无法登录到 **Citrix Gateway** 设备或内部 **Web** 服务器

您是 Citrix Gateway 管理员，通过 Citrix ADM 监视 Citrix Gateway 设备，您想了解用户无法登录的原因，或者失败发生在登录过程的哪个阶段。

Citrix ADM 使您能够在登录过程的以下阶段查看用户登录错误的详细信息：

- 身份验证
- 端点分析 (EPA)
- 单点登录

在 Citrix ADM 中，您可以搜索特定用户，然后查看该用户的所有详细信息。

要搜索用户，请执行以下操作：

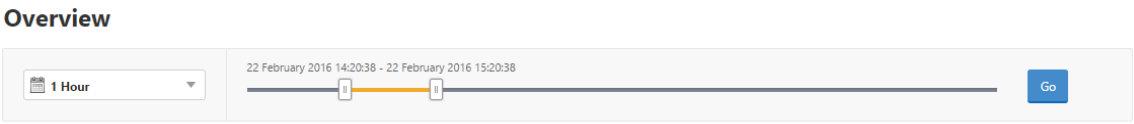
在 Citrix ADM 中，导航到分析 **> Gateway Insight**，然后在“搜索用户”文本框中指定要搜索的用户。

身份验证失败

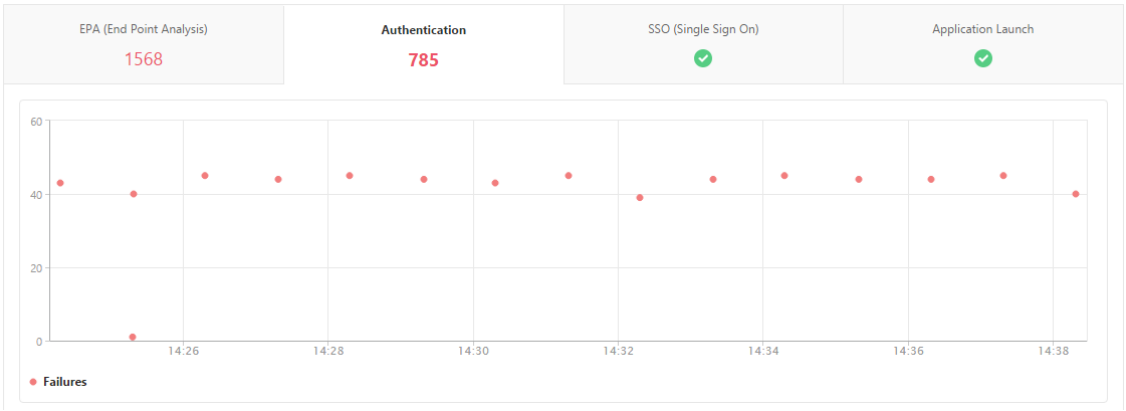
可以查看身份验证错误，例如，凭据错误或身份验证服务器没有响应。如果设置了两个阶段的身份验证，可以查看是身份验证的主阶段、次阶段还是两个阶段失败。

要查看验证失败的详细信息，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在概述部分中，选择要查看身份验证错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击身份验证选项卡。您可以在故障图中查看任何给定时间的身份验证错误数量。

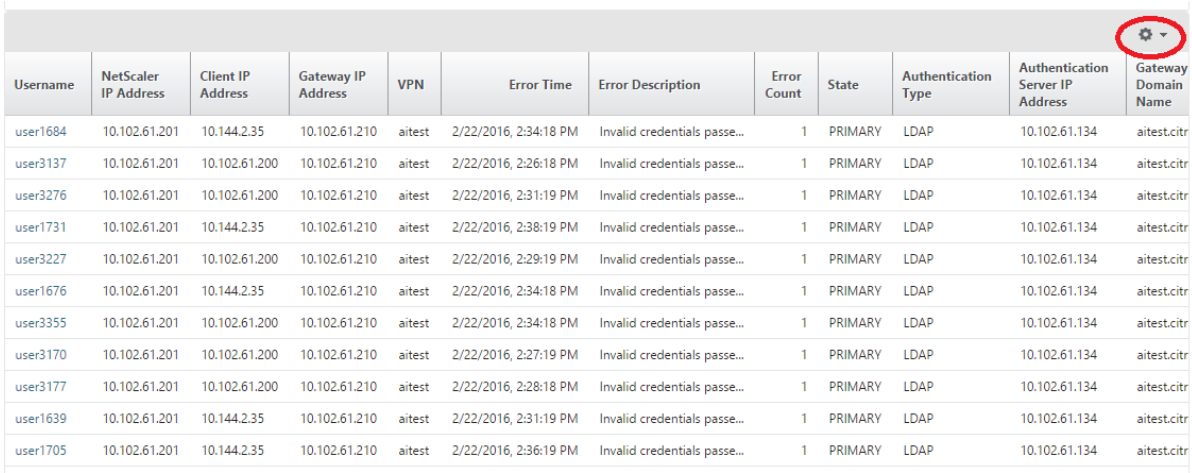


在同一选项卡上的表中向下滚动可查看每个身份验证错误的详细信息，例如，**Username**（用户名）、**Client IP Address**（客户端 **IP** 地址）、**Error Time**（错误时间）、**Authentication Type**（身份验证类型）、**Authentication Server IP Address**（身份验证服务器 **IP** 地址）及其他信息。表中的错误描述列显示登录失败的原因，状态列显示在两阶段身份验证的哪个阶段发生失败。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

您可以单击“用户 名”列中的用户以显示该用户的身份验证错误和其他详细信息。

您可以使用下面的屏幕截图中所示的向下箭头自定义表以添加或删除列。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	State	Authentication Type	Authentication Server IP Address	Gateway Domain Name
user1684	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3137	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:26:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3276	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1731	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:38:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3227	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:29:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1676	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3355	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:34:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3170	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:27:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user3177	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:28:18 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1639	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:31:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr
user1705	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:36:19 PM	Invalid credentials passe...	1	PRIMARY	LDAP	10.102.61.134	aitest.citr

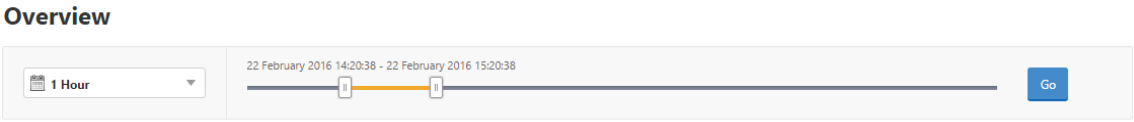
环保局失败

您可以在身份验证前或身份验证后阶段查看 EPA 失败。

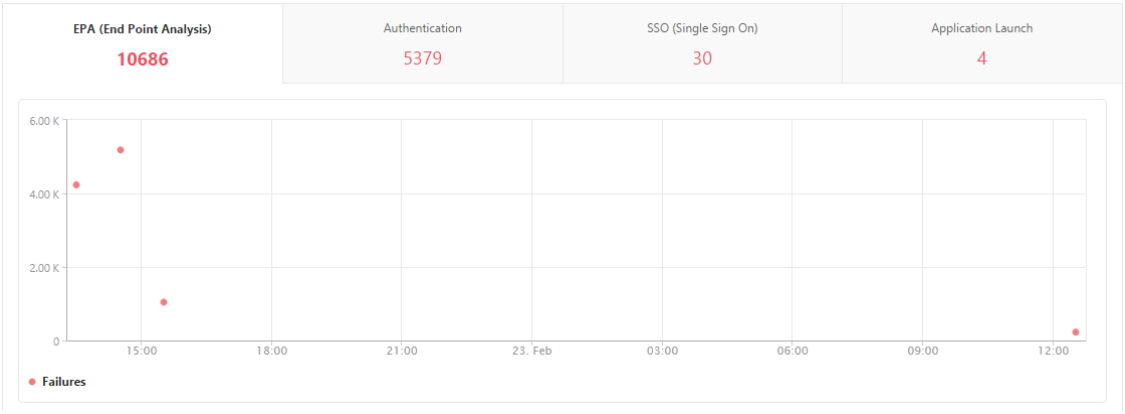
> 重要：
>
> - 仅当配置了经典表达式时，才会报告 EPA 失败。
> - 如果在身份验证前或身份验证后策略中配置了高级表达式，则不会报告 EPA 失败。
> - 如果将 EPA 配置为 nFactor 身份验证流程中的一个因素，则不会报告 EPA 失败。

要查看 **EPA** 失败详细信息，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在“Overview”（概述）部分中，选择要查看 EPA 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击 **EPA**（终点分析）选项卡。您可以在故障图中查看任何给定时间的 EPA 错误数。



在同一选项卡上的表中向下滚动可查看每个 EPA 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Gateway IP Address**（网关 **IP** 地址）、**VPN**、**Error Time**（错误时间）、**Policy Name**（策略名称）、**Gateway Domain Name**（网关域名）及其他信息。表中 **Error Description**（错误说明）列显示 EPA 失败的原因，**Policy Name**（策略名称）列显示导致失败的策略。

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

您可以单击“用户 名”列中的用户以显示该用户的 EPA 错误和其他详细信息。

您可以使用向下箭头自定义表格以添加或删除列。

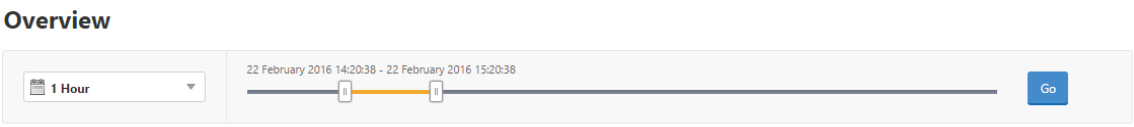
> 注意
>
> 将“clientSecurity”表达式配置为 VPN 会话策略规则时，Citrix Gateway 不会报告 EPA 故障。

SSO 故障

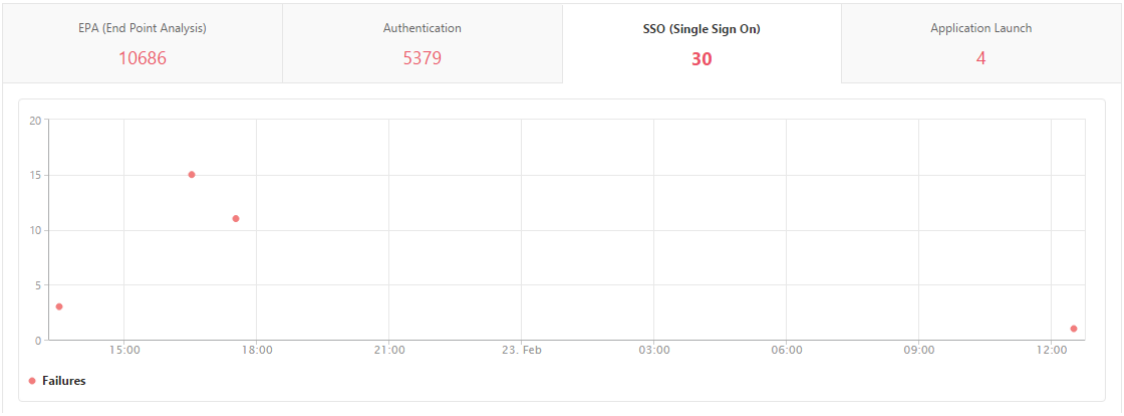
您可以查看通过 Citrix Gateway 设备访问任何应用程序的用户在任何阶段的所有 SSO 故障。

要查看 **SSO** 故障详细信息，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在“Overview”（概览）部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击 **SSO**（单次登录）选项卡。可以在“Failures”（失败）图中查看任何给定时间的 SSO 错误数。



在同一选项卡上的表中向下滚动可查看每个 SSO 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）及其他信息。

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

您可以单击“用户 名”列中的用户以显示该用户的 SSO 错误和其他详细信息。

您可以使用向下箭头自定义表格以添加或删除列。

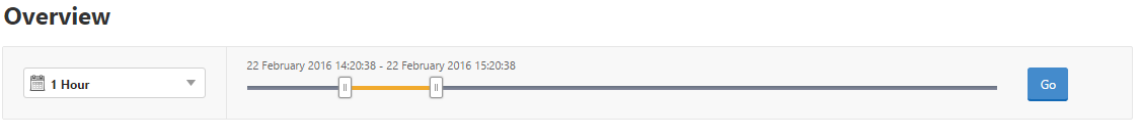
成功登录到 **Citrix Gateway** 后，用户将无法启动任何虚拟应用程序

对于应用程序启动失败，您可以查看原因，例如无法访问 Secure Ticket Authority (STA) 或 Citrix Virtual Apps 服务器，或无效的 STA 票证。可以查看错误发生的时间、错误的详细信息以及 STA 验证失败的资源。

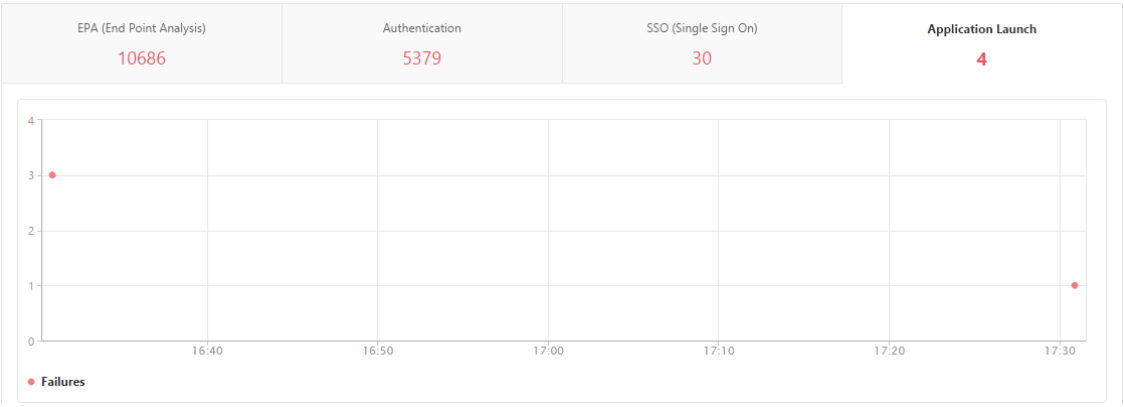
查看应用程序启动失败的详细信息：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。

2. 在概述部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击应用程序启动选项卡。您可以在失败图表中查看任何给定时间的应用程序启动失败次数。



在同一选项卡上的表中向下滚动可查看每个应用程序启动错误的详细信息，例如，**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）、**Gateway Domain Name**（网关域名）及其他信息。表中的 **Error Description**（错误说明）列显示 STA 服务器的 IP 地址，**Resource Name**（资源名称）列显示 STA 验证失败的资源的详细信息。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

您可以单击“用户 名”列中的用户以显示该用户的应用程序启动错误和其他详细信息。

您可以使用向下箭头自定义表格以添加或删除列。

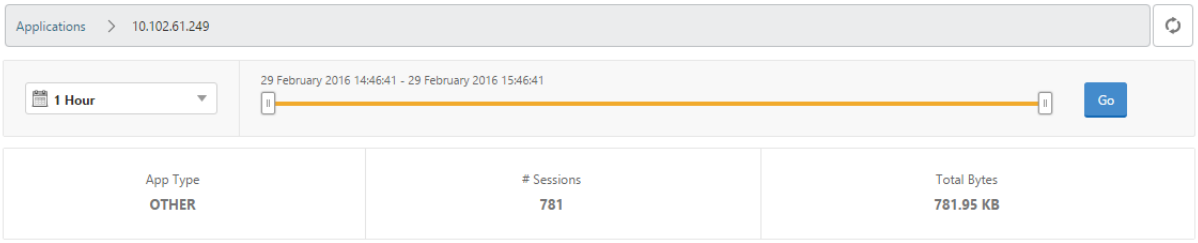
成功启动新应用程序后，用户希望查看该应用程序占用的总字节和带宽

成功启动新应用程序后，可以在 Citrix ADM 中查看该应用程序占用的总字节和带宽。

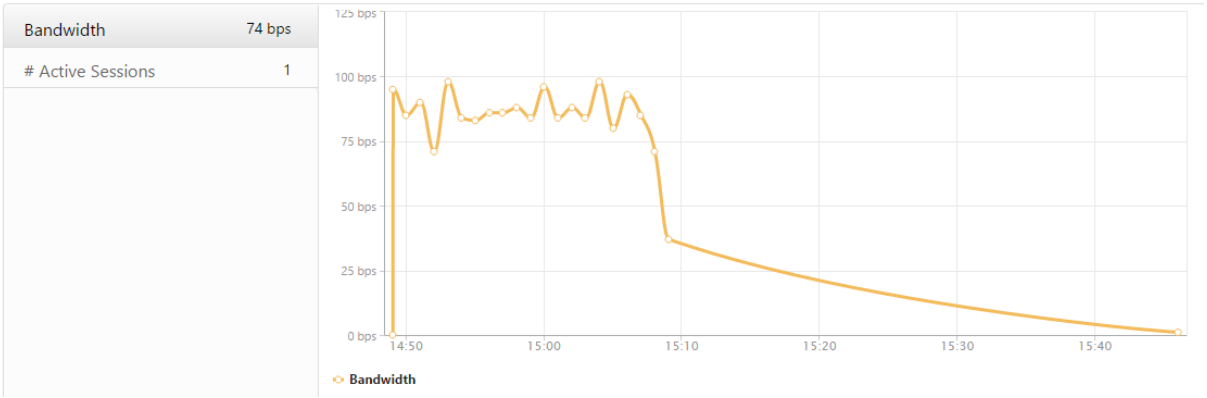
要查看应用程序消耗的总字节和带宽，请执行以下操作：

在 Citrix ADM 中，导航到分析 **> Gateway Insight >** 应用程序，向下滚动，然后在其他应用程序选项卡上单击要查看详细信息的应用程序。

可以查看该应用程序使用的会话数和总字节数。



还可以查看该应用程序使用的带宽。

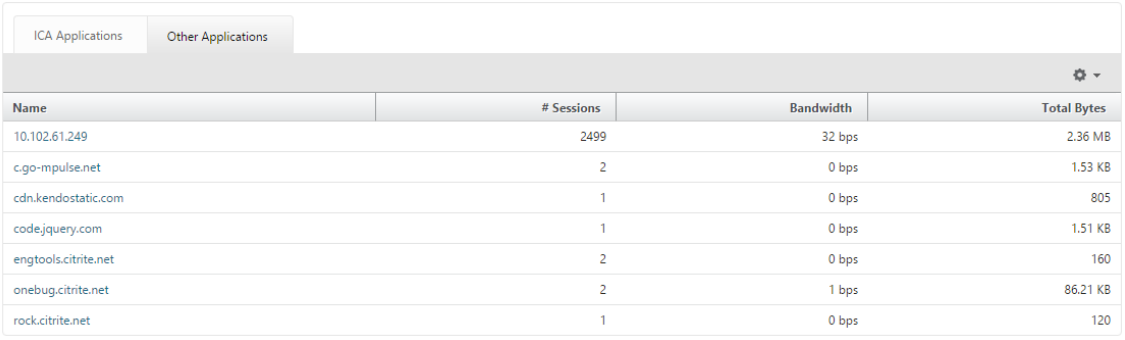


用户已成功登录到 **Citrix Gateway**，但无法访问内部网络中的某些网络资源

通过 Gateway Insight，可以确定用户是否有权访问网络资源。还可以查看导致失败的策略的名称。

要查看资源的用户访问权限，请执行以下操作：

1. 在 Citrix ADM 中，导航到“分析” **>** “网关洞察” **>** “应用程序”。
2. 在出现的屏幕上，向下滚动，然后在 其他应用程序 选项卡上，选择用户无法登录的应用程序。



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

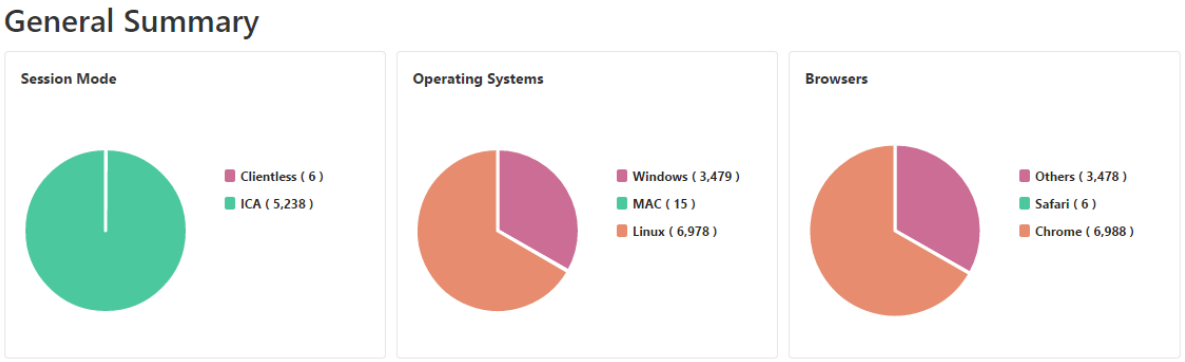
3. 向下滚动，在“用户”表中，将显示所有有权访问该应用程序的用户。

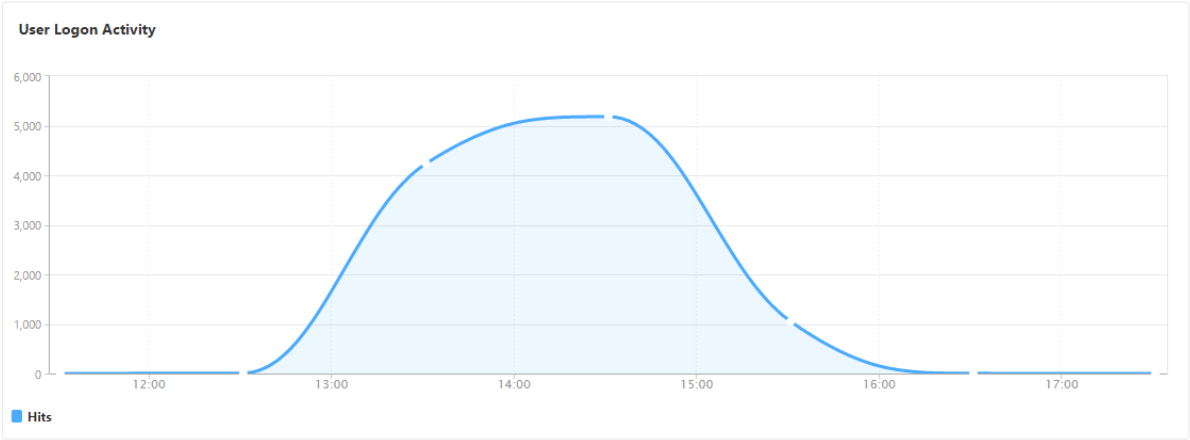
不同的用户可能正在使用不同的 **Citrix Gateway** 部署，也可能通过不同的访问模式登录到 **Citrix Gateway**。管理员必须能够查看有关部署类型和访问模式的详细信息

通过 Gateway Insight，可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。您还可以确定用户的部署是统一网关还是经典 Citrix Gateway 部署。对于 Unified Gateway 部署，可以查看内容交换虚拟服务器名称和 IP 地址及 VPN 虚拟服务器名称。

要查看会话模式、客户端类型和登录用户数量的摘要，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在概述部分中，向下滚动以查看会话模式、操作系统、浏览器和用户登录活动图表显示用户用于登录的不同会话模式、客户端类型以及每小时登录的用户数。





对 **Gateway Insight** 问题进行故障排除

February 6, 2024

如果 Gateway Insight 解决方案无法按预期运行，则问题可能出在以下任一方面。有关故障排除，请参阅相应部分中的清单。

- Gateway Insight 配置。
- Citrix ADC 和 Citrix ADM 之间的连接问题。
- 在 Citrix ADC 中生成记录。
- 在 Citrix ADM 中进行验证。

Gateway Insight 配置清单

- 确保在 Citrix ADC 中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 Citrix ADC 运行配置中的网关智能分析配置。

  执行 `show running | grep -i <appflow_policy>` 命令以检查 Gateway Insight 配置。确保绑定类型为请求。例如;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

- 对于单跳、接入网关或 Unified Gateway 部署，请确保 Gateway Insight AppFlow 策略绑定到 VPN 虚拟服务器，其中 VPN 流量正在流动。有关详细信息，请参阅 启用 HDX Insight 数据收集。
- 检查 Citrix Gateway/VPN 虚拟服务器中的“appflowlog”参数。有关详细信息，请参阅 为虚拟服务器启用 AppFlow。

Citrix ADC 与 **Citrix ADM** 之间的连接检查表

- 检查 Citrix ADC 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 Citrix ADC 和 AppFlow Collector 之间的连接状态。
- 检查 Gateway Insight AppFlow 策略命中。

  执行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中率。

  您还可以导航到 GUI 中的“系统”**>**“**AppFlow**”**>**“策略”，以检查 AppFlow 策略命中。
- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

Citrix ADC 核对清单中的记录生成

- 执行 `nsconmsg -d stats -g ai_tot` 命令并检查 Citrix ADC 中的统计信息增量。
- 捕获无记录日志并检查 CFLOW 数据包，以确认 Citrix ADC 导出 AppFlow 记录。

Citrix ADM 中的验证

- 执行 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` 命令以检查日志以确认 Citrix ADM 正在接收 AppFlow 记录。
- 确保已将 Citrix ADC 实例添加到 Citrix ADM 中。
- 确保 Citrix Gateway/VPN 虚拟服务器已在 Citrix ADM 中获得许可。

Gateway Insight 统计数据

以下 Gateway Insight 统计数据可用。

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_Export
- ai_tot_postauth_epa_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_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_mismatch
- ai_tot_appflow_disabled

联系 **Citrix** 技术支持

要快速解决问题，请确保在联系 Citrix 技术支持之前已掌握以下信息：

- 部署和网络拓扑的详细信息。
- Citrix ADC 和 Citrix ADM 版本。
- 适用于 Citrix ADC 和 Citrix ADM 的技术支持包。
- 在问题过程中无法捕获。

已知问题

有关 Gateway Insight 的已知问题，请参阅 Citrix ADC 发行说明。

Security Insight

February 6, 2024

面向 Internet 的 Web 和 Web 服务应用程序越来越易受攻击。要保护应用程序免受攻击，您必须了解威胁、实时可操作的攻击数据以及对策建议。Security Insight 提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。

> 注意
>
> 在 Citrix Application Delivery Management (ADM) 上运行版本 11.0 Build 65.31 及更高版本的 Citrix ADC 设备支持 Security Insight。

Security Insight 的工作原理

Security Insight 是基于控制板的直观安全分析解决方案，让您可以完全了解与应用程序关联的威胁环境。Security Insight 包含在 Citrix ADM 中，它会根据您的应用程序防火墙和 Citrix ADC 系统安全配置定期生成报告。报告包含每个应用程序的以下信息：

- 威胁指数。一个单位数评级系统，指示应用程序攻击的严重程度，无论应用程序是否受到 Citrix ADC 设备的保护。应用程序上的攻击越严重，该应用程序的威胁指数越高。值的范围是 1 到 7。

  威胁指数基于攻击信息。攻击相关的信息（例如，违反类型、攻击类别、位置和客户端详细信息）让您可以了解应用程序上的攻击。只有在发生违规或攻击时，才会向 Citrix ADM 发送违规信息。大量违反和漏洞会导致较高的威胁指数值。

- 安全指数。一个单位数评级系统，用于指示您配置 Citrix ADC 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数越高。值的范围是 1 到 7。

安全指标同时考虑应用程序防火墙配置和 Citrix ADC 系统安全配置。为了获得较高的安全指数值，两个配置都必须强健。例如，如果进行了严格的应用程序防火墙检查，但尚未采用 Citrix ADC 系统安全措施（如 nsroot 用户的强密码），则会为应用程序分配一个较低的安全指数值。

- 可操作信息。降低威胁指数及提高安全指数所需的信息，可显著提高应用程序安全性。例如，可以查看有关违反、应用程序防火墙和其他安全功能的现有和缺少的安全配置以及应用程序被攻击速率等的信息。

配置安全智能分析

Citrix ADM 支持来自所有已配置应用程序防火墙的 Citrix ADC 实例的安全智能分析。

要在 ADC 实例上配置 Security Insight，请首先配置应用程序防火墙配置文件和应用程序防火墙策略。尽管随后可以在全局范围内绑定应用程序防火墙策略，但 Citrix 建议将该策略绑定到虚拟服务器。

要查看 Citrix ADM 上的分析，请在实例上启用 AppFlow 功能，配置 AppFlow 收集器、操作和策略，并在全局范围内绑定策略。此外，尽管您随后可以在全局范围内绑定应用程序防火墙策略，但 Citrix 建议将该策略绑定到虚拟服务器。Citrix 还建议您使用 Citrix ADM 在 ADC 实例上部署 AppFlow 配置。配置收集器时，必须指定要监视报告的 Citrix ADM 服务器的 IP 地址。

要在 **Citrix ADC** 实例上配置 **Security Insight**，请执行以下操作：

1. 运行以下命令来配置应用程序防火墙配置文件和策略，并全局绑定应用程序防火墙策略，或将应用程序防火墙策略绑定到负载平衡虚拟服务器。

---

add appfw profile [**-defaults** (basic 高级）]

---

set appfw profile <name> [**-startURLAction** <startURLAction> …]

add appfw policy <name> <rule> <profileName>

bind appfw global <policyName> <priority>

或者，

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,
bind lb vserver outlook  - policyName pr_appfw_pol  - priority  “20
   ”
<!--NeedCopy-->
```


2. 运行以下命令来启用 AppFlow 功能、配置 AppFlow 收集器、操作及策略，并全局绑定策略，或将策略绑定到负载平衡虚拟服务器：

   add appflow collector <name> **-IPAddress** <ipaddress>

---

set appflow param DISABLED)]
[**-SecurityInsightRecordInterval**]
[**-SecurityInsightTraffic** (ENABLED

---

   add appflow action <name> **-collectors** <string>

   add appflow policy <name> <rule> <action>

   bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

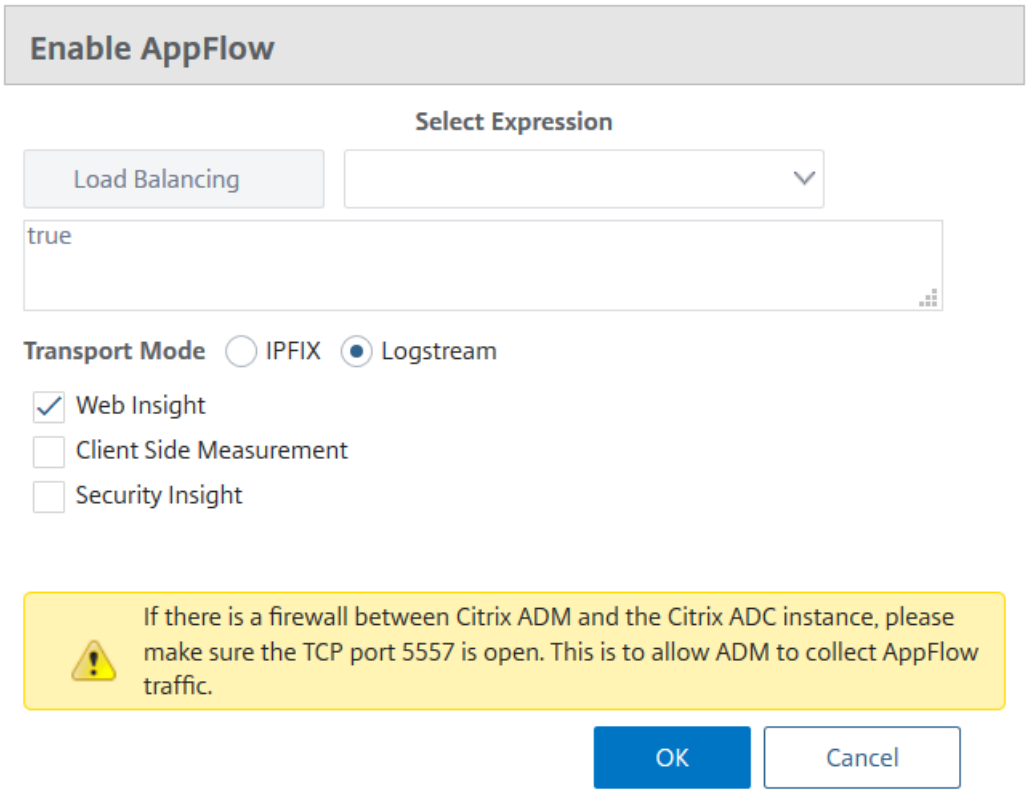
   或者，

   bind lb vserver <vserver> **-policyName** <policy> **-priority** <priority>

```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
   SecurityInsightTraffic ENABLED
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
add appflow policy af_policy_Sap_10.102.63.85 true
   af_action_Sap_10.102.63.85
bind appflow global pol1 1 END -type REQ_DEFAULT
or,
bind lb vserver Sap  - policyName af_action_Sap_10.102.63.85  -
   priority  “20”
<!--NeedCopy-->
```

要从 **Citrix ADM** 启用 **AppFlow**，请执行以下操作：

1. 在 Web 浏览器中，键入 **Citrix ADM** 的 IP 地址（例如 http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到“网络”>“实例”，然后选择要启用 AppFlow 的 Citrix ADC 实例。
4. 从选择操作列表中，选择配置分析。
5. 选择虚拟服务器，然后单击“启用 **AppFlow**”。
6. 在“启用 **AppFlow**”字段中，键入 **true**，然后选择 **Security Insight**。
7. 单击确定。



查看安全智能分析报告的地理位置

安全智能分析报告包括客户端请求源自的确切地理位置。您可以查看 Citrix ADM 中的地理位置。Citrix ADC 中内置的地理数据库文件包含大部分公用 IP 地址。该文件位于 Citrix ADC 中的 **/var/netscaler/inbuilt_db** 位置。

要启用地理位置，请执行以下操作：

运行以下命令以启用地理位置日志记录及采用 CEF 格式的日志记录：

- **add locationFile** <Complete path with the DB filename>
- **set appfw settings -geoLocationLogging ON**
- **set appfw settings -CEFLogging ON**

如果地理数据库文件中没有任何 IP 地址，则可以添加该地理位置的 IP 地址。除了 IP 地址外，您还可以添加城市/州/国家名称以及每个位置的纬度和经度坐标。

使用文本编辑器（如 vi 编辑器）打开 geo 数据库文件，并为每个位置添加一个条目。

该条目必须采用以下格式：

```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,
latitude
```

例如，


```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

IP 信誉

可以使用 NetScaler Insight Center 来监视和管理您的传入流量的 IP 信誉。可以配置策略以将更多 IP 添加为恶意 IP，并创建自定义的阻止列表。

要了解如何配置和使用 IP 信誉，请参阅 IP 信誉。

监视 IP 信誉

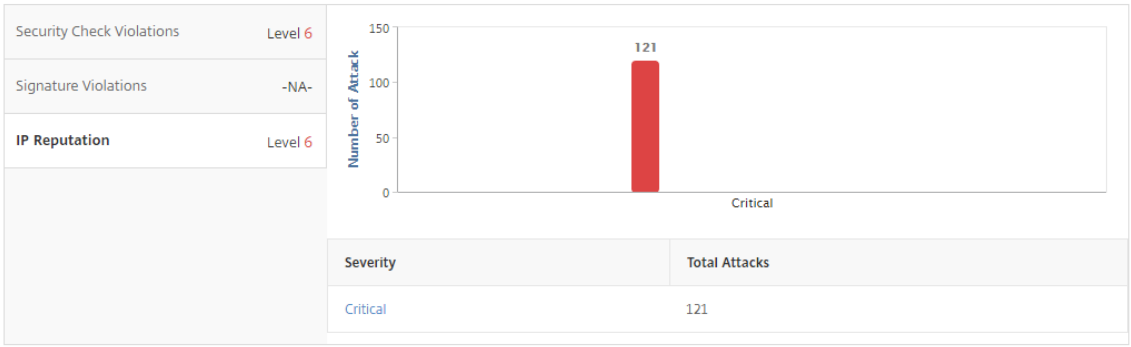
IP 信誉功能提供有关恶意 IP 地址的攻击相关信息。例如，它报告有关客户端 IP 地址的 IP 信誉得分、IP 信誉类别、IP 信誉攻击时间、设备 IP 及详细信息。

IP 信誉分数指示与 IP 地址关联的风险。该分数范围如下：

IP 信誉得分	风险级别
1–20	高风险
21–40	可疑
41–60	中等风险
61–80	低风险
81–100	可信

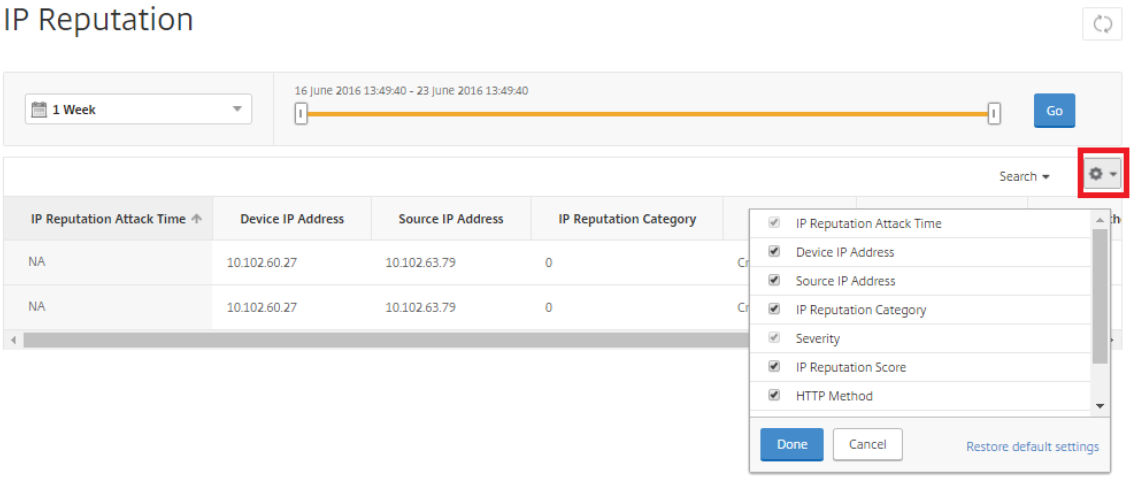
要监视 **IP** 信誉，请执行以下操作：

1. 导航到分析 > **Security Insight**，然后选择要监视的应用程序。
2. 在威胁索引选项卡中，选择 **IP** 信誉。



3. 选择严重性以显示该级别的攻击的更多详细信息。您可以单击条形图或图表下方的表格中。
4. 选择要查看详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。然后，单击 **Go**（继续）。

5. 要自定义显示，请单击设置按钮。



阈值

您可以设置应用程序的安全指数和威胁指数的阈值，以及在 Security Insight 中查看这些阈值。

要设置阈值，请执行以下操作：

1. 导航到分析 > 设置 > 阈值，然后选择添加。
2. 在“流量类型”字段中选择流量类型为“安全”，然后在其他相应的字段中输入必填信息，例如名称、持续时间和实体。
3. 在“配置规则”部分中，使用“指标”、“比较器”和“值”字段来设置阈值。

   例如，“Threat Index”（威胁指数）“>”“5”
4. 在“通知设置”中，选择通知类型。
5. 单击创建。

要查看阈值违反，请执行以下操作：

1. 导航到分析 > **Security Insight** > 设备，然后选择 Citrix ADC 实例。
2. 在“应用程序”部分中，您可以在“阈值违规”列中查看每个虚拟服务器发生的 阈值违规 数。

Security Insight 用例

以下用例说明了如何使用 Security Insight 来评估应用程序面临的威胁以及改进安全措施。

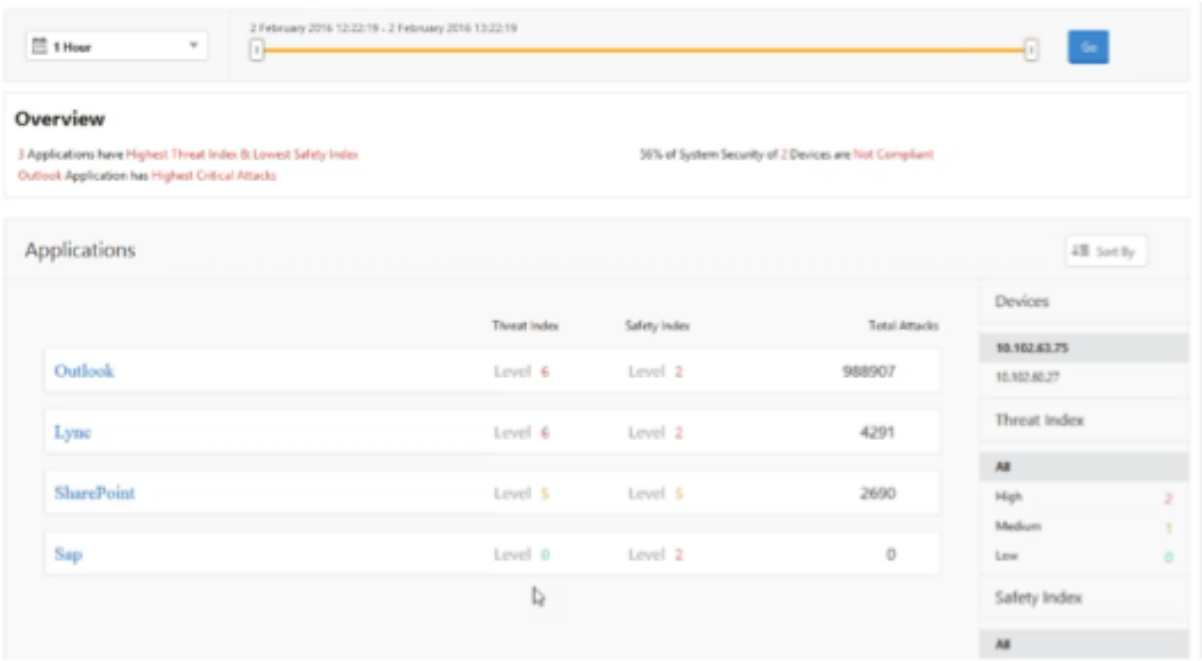
获取威胁环境的概述

在此使用案例中，您有一组可能遭受攻击的应用程序，并且您已将 Citrix ADM 配置为监视威胁环境。您必须经常查看威胁指数、安全指数以及应用程序可能遇到的攻击类型和严重程度。此审查 使您能够首先将注意力集中在最需要关注的应用程序上。Security Insight 控制板提供了应用程序在您选择的一段时间内以及所选 Citrix ADC 设备所遇到的威胁的摘要。它显示应用程序列表、它们的威胁指数和安全指数以及在所选时间段的攻击总数。

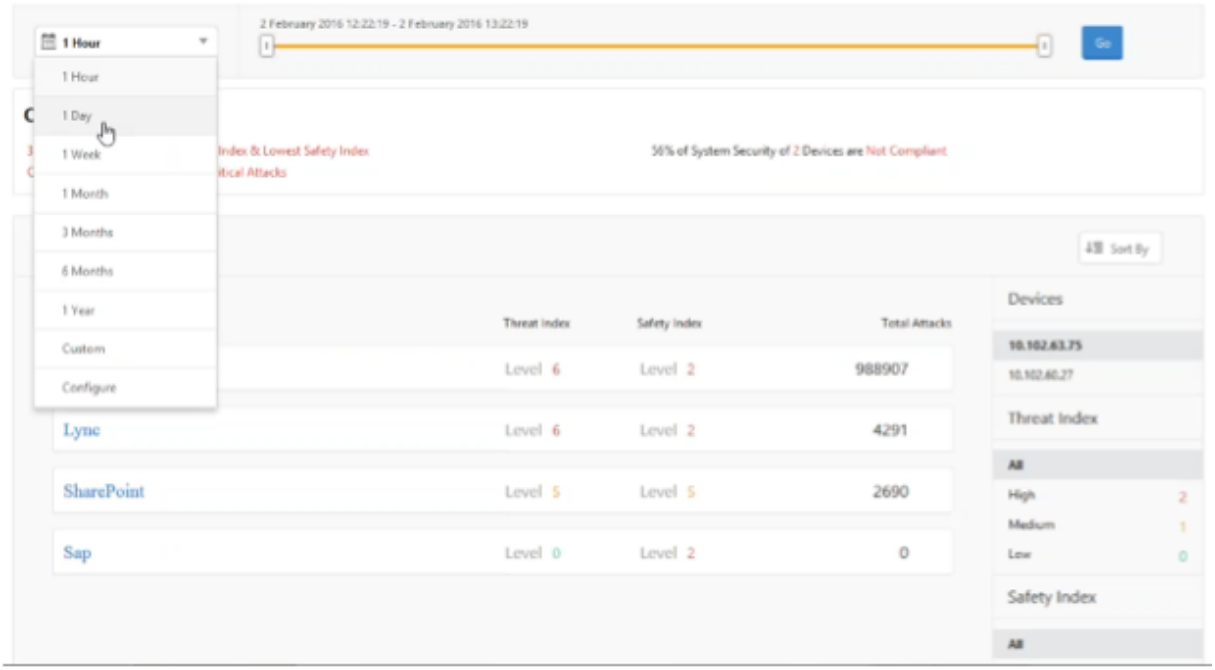
例如，您可能在监视 Microsoft Outlook、Microsoft Lync、SharePoint 和 SAP 应用程序，您可能希望查看这些应用程序的威胁环境的摘要。

要获取威胁环境的摘要，请登录到 **Citrix ADM**，然后导航到“分析” **>** “安全智能分析”。

此时将显示每个应用程序的主要信息。默认时间段是 1 小时。



要查看不同时段的信息，请从左上角的列表中选择一个时段。



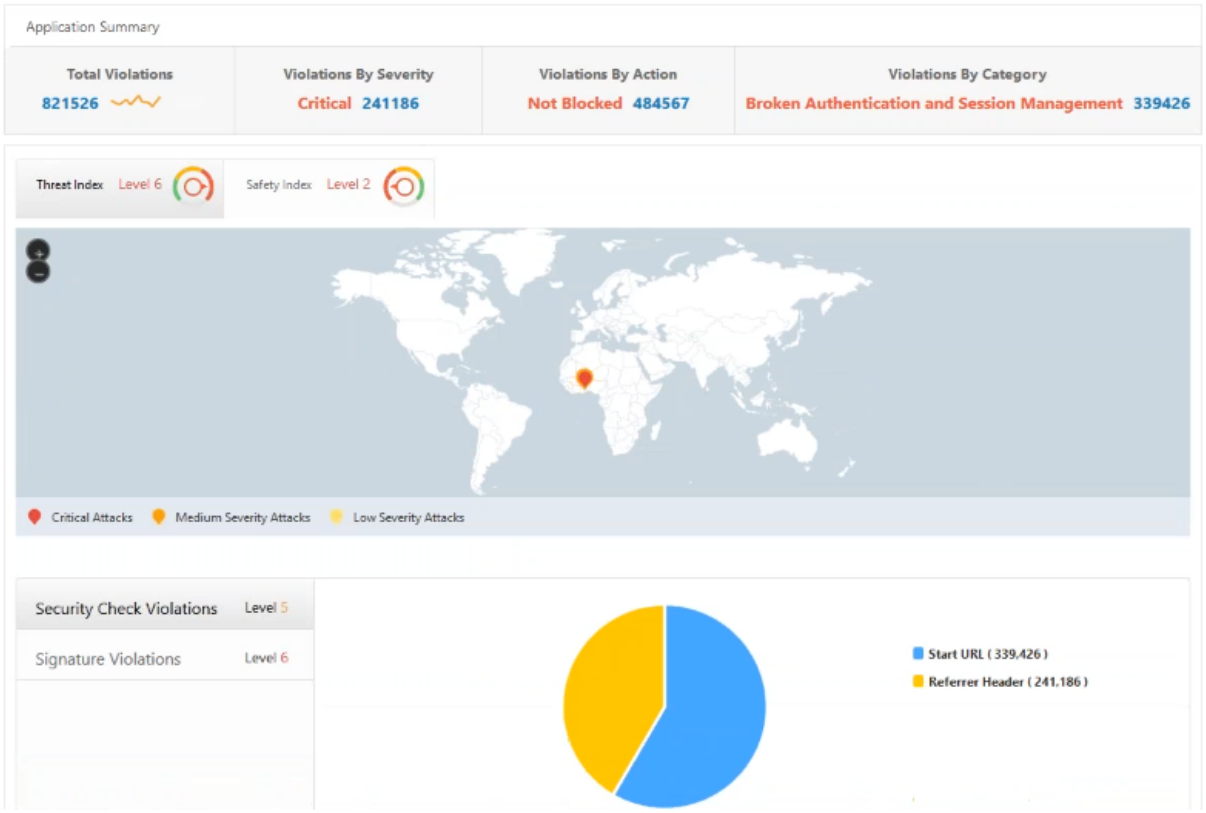
要查看其他 Citrix ADC 实例的摘要，请在“设备”下单击 Citrix ADC 实例的 IP 地址。要按给定列对应用程序列表排序，请单击列标题。

确定应用程序的威胁风险

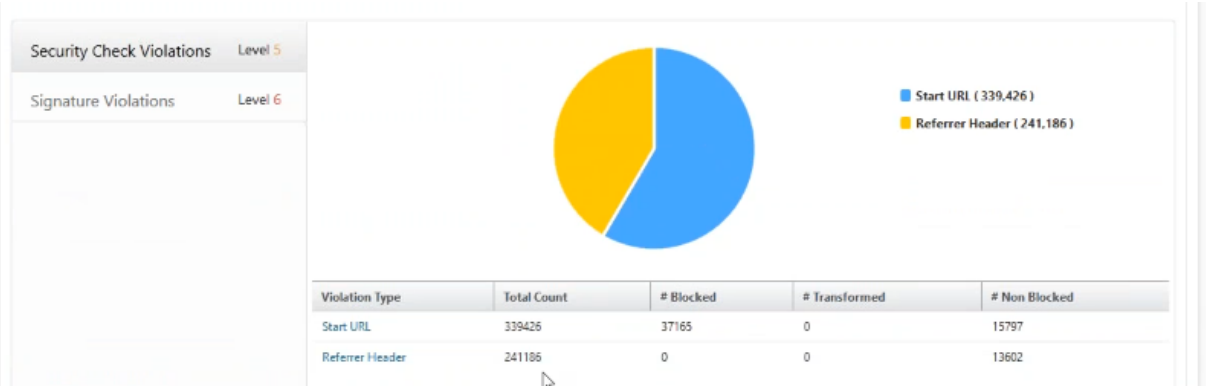
要在“安全智能分析”控制板上识别具有高威胁指数和低安全指数的应用程序，您希望在决定保护这些威胁风险之前确定威胁风险。即，您希望确定降低了其指数值的攻击的类型和严重性。可以通过查看应用程序摘要来确定应用程序面临的威胁。

在此示例中，Microsoft Outlook 的威胁指数值是 6，您希望知道哪些因素导致此高威胁指数。

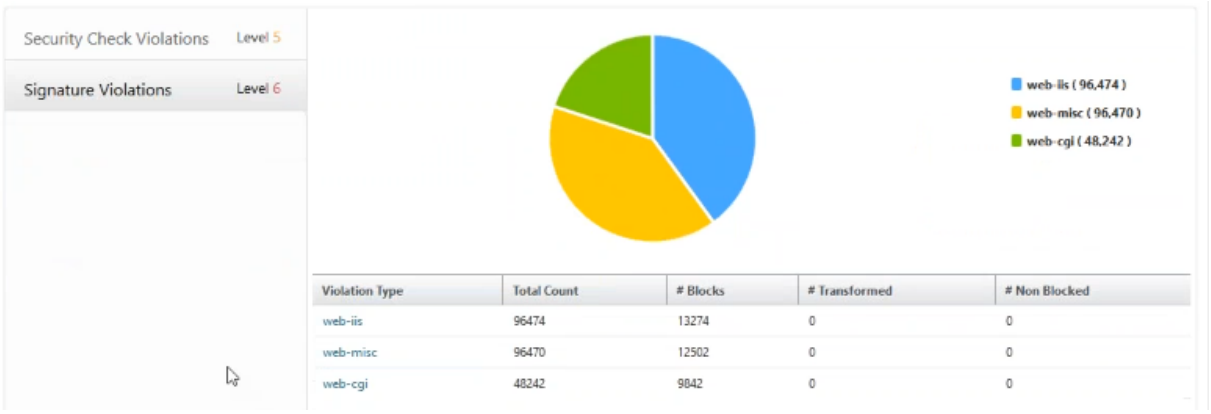
要确定 Microsoft Outlook 面临的威胁，请在 **Security Insight** 控制板上，单击 **Outlook**。应用程序摘要包含标识服务器地理位置的地图。



单击 **Threat Index**（威胁指数）**> Security Check Violations**（安全检查违反），并查看显示的违反信息。



单击 签名违 规并查看显示的违规信息。

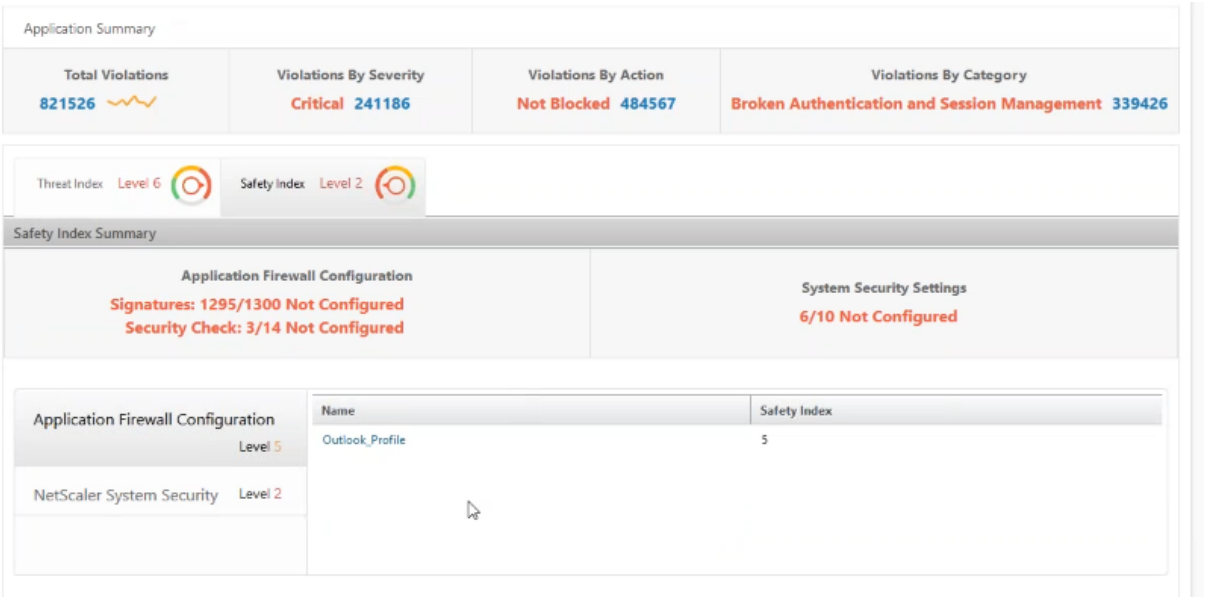


确定应用程序的现有和缺少的安全配置

查看了应用程序面临的威胁后，您希望确定哪些应用程序安全配置正在实施，以及该应用程序缺少哪些配置。可以深度查看应用程序的安全指数摘要来获取此信息。

安全指数摘要为您提供有关以下安全配置的有效性：

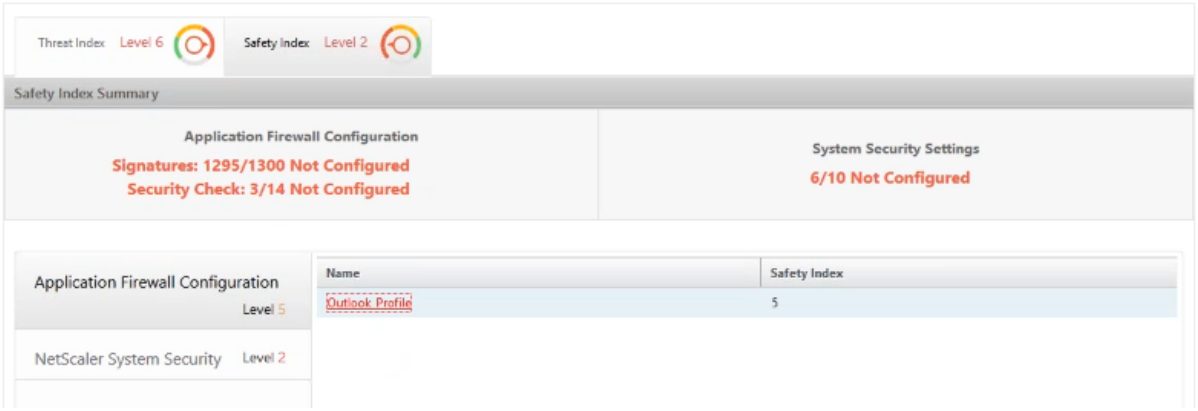
- 应用程序防火墙配置。显示多少签名和安全实体未配置。
- **NetScaler** 系统安全。显示多少系统安全设置未配置。



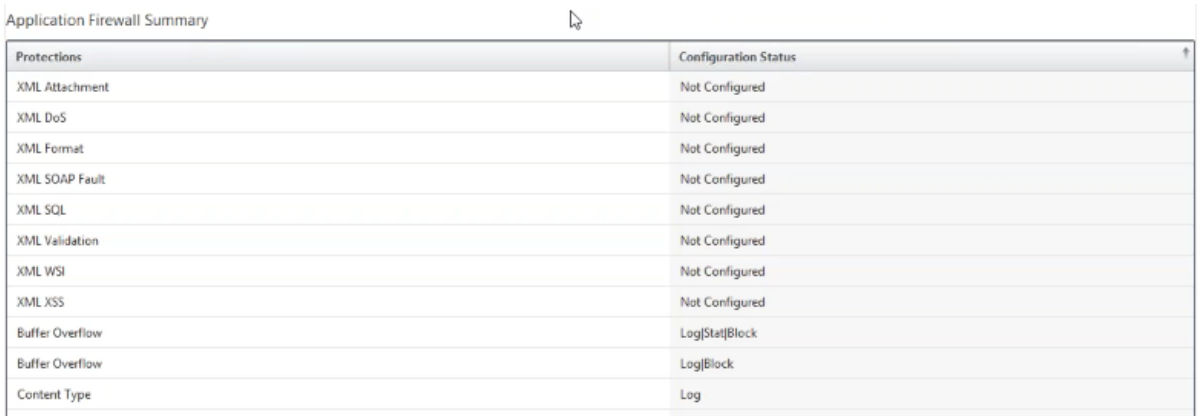
在之前的用例中，您查看了 Microsoft Outlook 面临的威胁，它的威胁指数值为 6。现在，您希望知道 Outlook 有哪些安全配置正在实施，以及可以添加哪些配置来改进其威胁指数。

在 **Security Insight** 控制板上，单击 **Outlook**，然后单击 **Safety Index**（安全指数）选项卡。查看 **Safety Index Summary**（安全指数摘要）区域提供的信息。

在 **Application Firewall Configuration**（应用程序防火墙配置）节点上，单击 **Outlook_Profile** 并查看饼图中的安全检查和签名违反信息。



查看应用程序防火墙摘要表中每个保护类型的配置状态。要按列对表排序，请单击列标题。

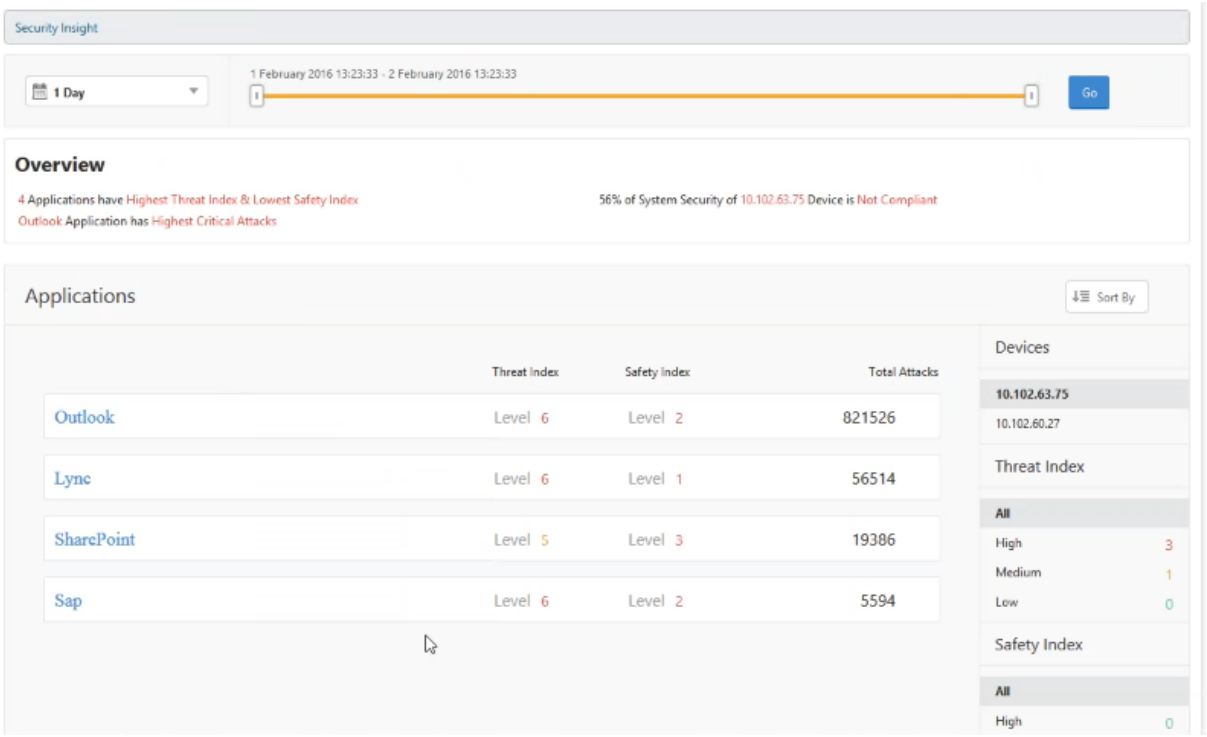


单击 **NetScaler System Security**（NetScaler 系统安全）节点，并查看系统安全设置和 Citrix 建议以改进应用程序安全指数。

确定需要立即关注的应用程序

需要立即注意的应用程序是那些具有较高威胁指数和较低安全指数的应用程序。

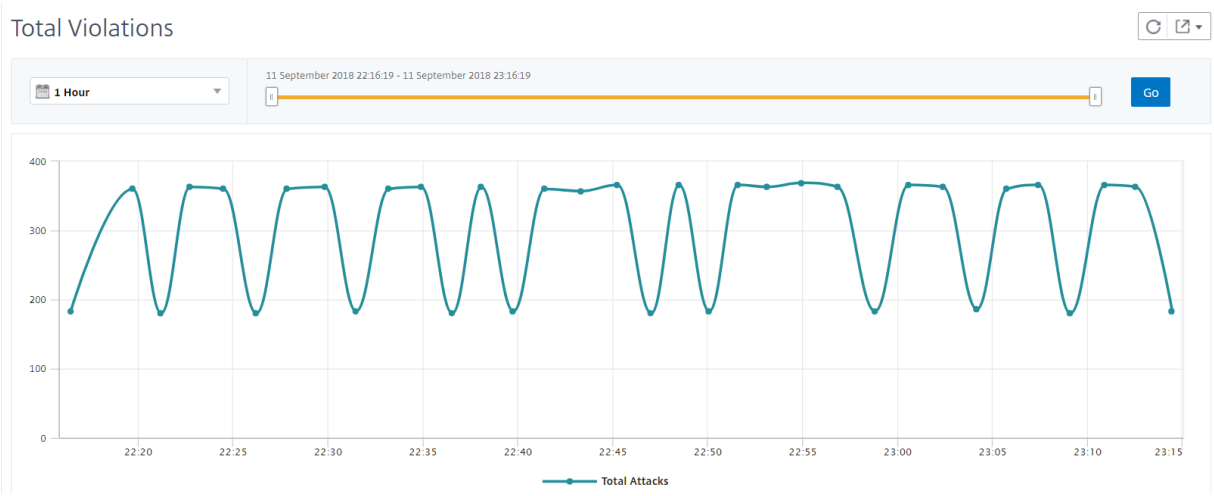
在此示例中，Microsoft Outlook 和 Microsoft Lync 都具有较高威胁指数值 6，但在两个安全指数中，Lync 的安全指数较低。因此，可能必须先将注意力放在 Lync 上，然后再改进 Outlook 的威胁环境。



确定给定时间段内的攻击次数

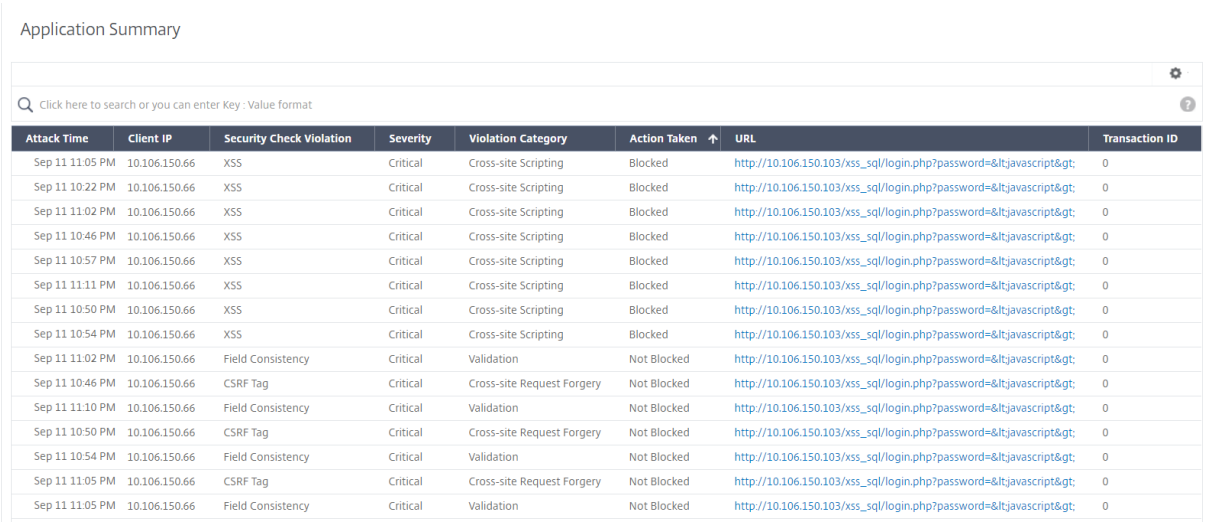
您可能希望确定在给定时间点给定应用程序上发生了多少攻击，或者您可能希望研究特定时间段的攻击速率。

在 Security Insight 页面上，单击任意应用程序，然后在“应用程序摘要”中单击违规次数。“违规总数”页面以图形方式显示攻击时间为 1 小时、1 天、1 周和 1 个月。



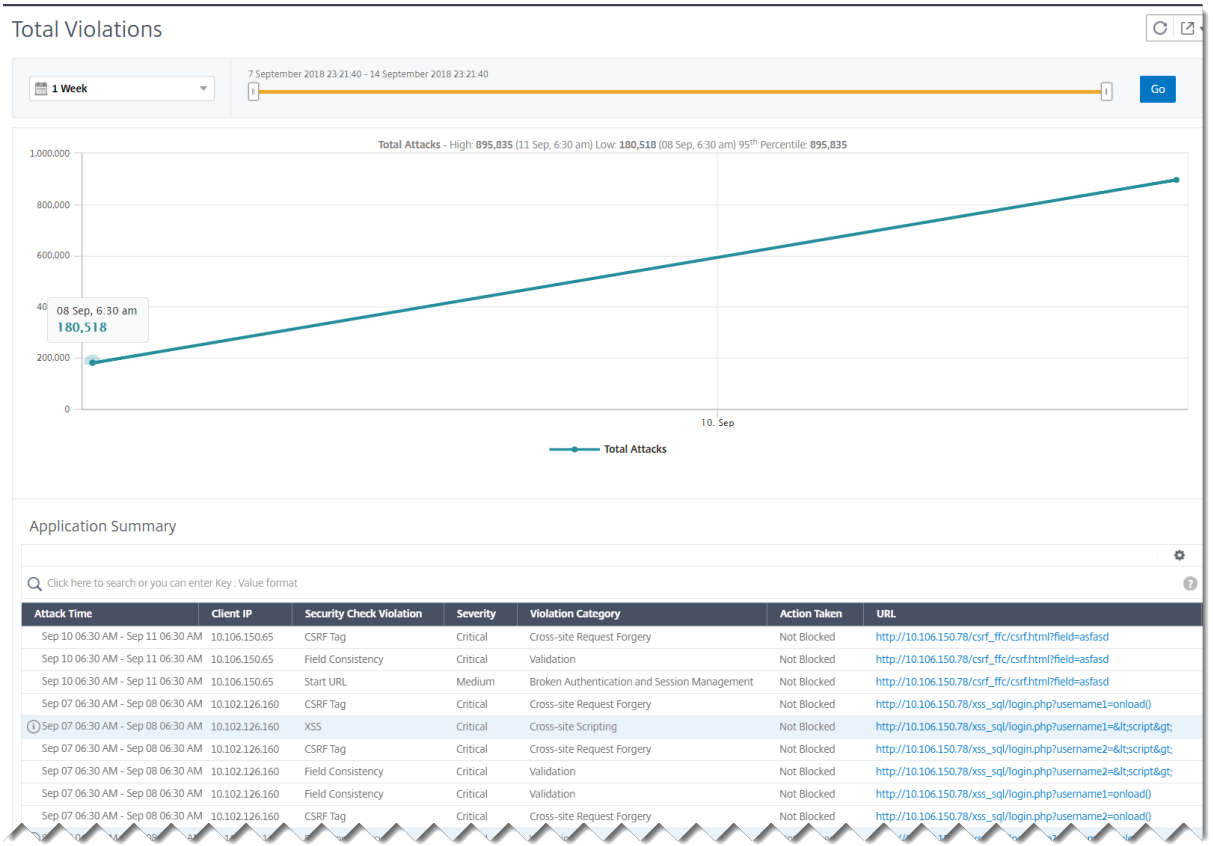
“应用程序摘要”表提供了有关攻击的详细信息。其中一些内容如下：

- 攻击时间
- 发生攻击的客户端的 IP 地址
- 严重性
- 违规类别
- 攻击起源的 URL 以及其他详细信息。



Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0

虽然您始终可以在每小时报告中查看攻击时间（如图所示），但现在您可以查看聚合报告的攻击时间范围，即使是每日或每周报告也是如此。如果您从时段列表中选择“1 天”，Security Insight 报告将显示汇总的所有攻击，攻击时间将显示在一小时内。如果您选择“1 周”或“1 个月”，则所有攻击将被汇总，攻击时间显示在一天范围内。

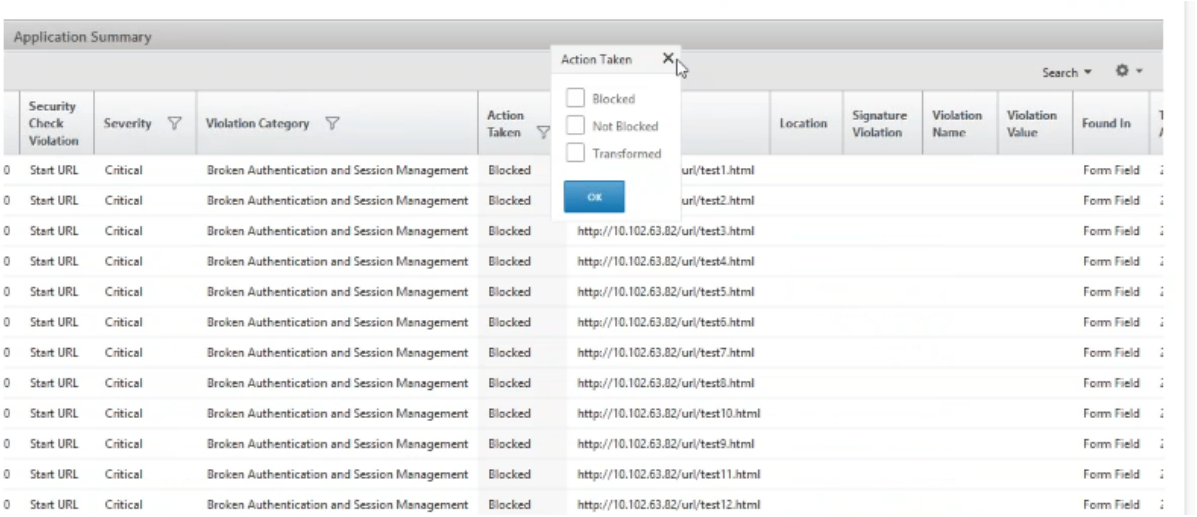


获取有关安全漏洞的详细信息

您可能希望查看应用程序攻击的列表，并深入了解攻击的类型和严重性、Citrix ADC 实例采取的操作、请求的资源以及攻击的来源。

例如，您可能希望确定 Microsoft Lync 上多少攻击被阻止了、请求了什么资源以及来源的 IP 地址。

在“Secur **ity Insight**”控制板上，单击 **Lync >** 违规总数。在表中，单击 **Action Taken**（采取的操作）列标题中的过滤器图标，然后选择 **Blocked**（被阻止）。



有关请求的资源的信息，请查看 **URL** 列。有关攻击来源的信息，请查看 **Client IP**（客户端 IP）列。

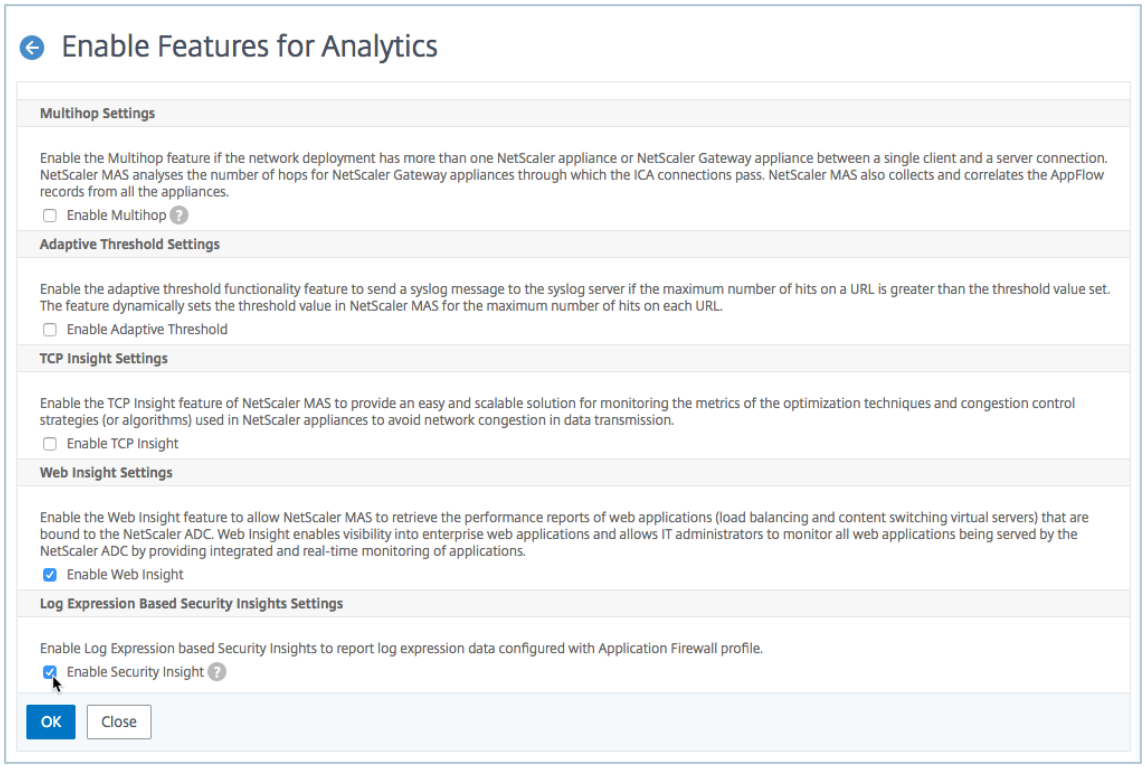
查看日志表达式详细信息

Citrix ADC 实例使用使用应用程序防火墙配置文件配置的日志表达式对企业中的应用程序的攻击采取措施。在安全智能分析中，您可以查看为 Citrix ADC 实例使用的日志表达式返回的值。这些值包括请求标头、请求正文等。除了日志表达式值之外，您还可以查看日志表达式名称和在应用程序防火墙配置文件中定义的日志表达式的注释，Citrix ADC 实例用于对攻击执行操作。

必备条件　确保您：

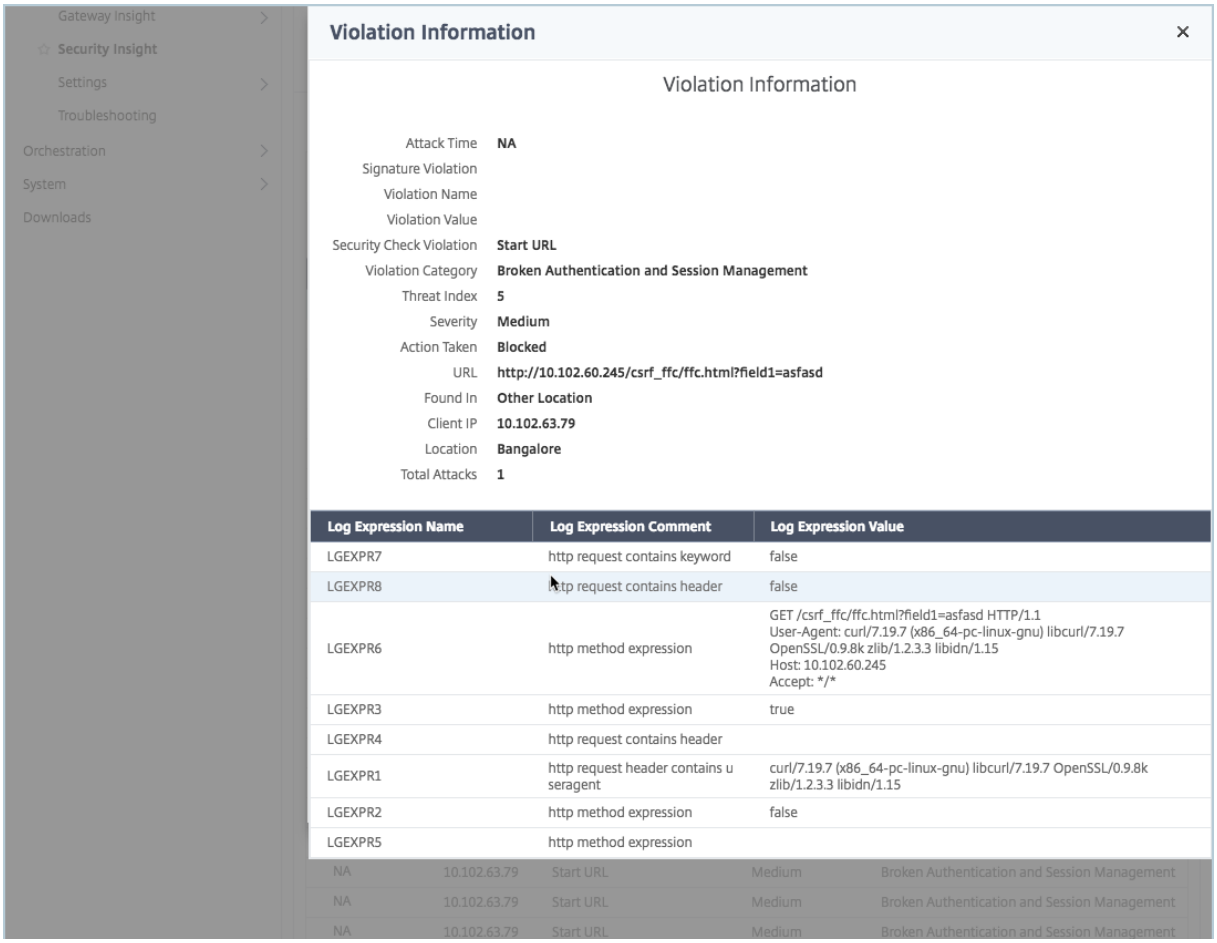
- 在应用程序防火墙配置文件中配置日志表达式。有关详细信息，请参阅应用程序防火墙。
- 在 Citrix ADM 中启用基于日志表达式的安全见解设置。请执行以下操作：

  1. 导航到 分析 **>** 设置，然后单击 启用分析功能。
  2. 在“启用分析功能”页中，选择“基于日志表达式的安全智能分析设置”部分下的“启用安全智 能分析”，然后单 击“确定”。



例如，您可能希望查看由 Citrix ADC 实例返回的日志表达式的值，用于针对企业中的 Microsoft Lync 攻击采取的操作。

在 Security Insight 控制面板上，导航到 **Lync >** 全部违规行为。在“应用程序摘要”表中，单击 URL 可在“违规信息”页中查看 违规的完整详细信息，包括日志表达式名称、注释以及 Citrix ADC 实例为操作返回的值。

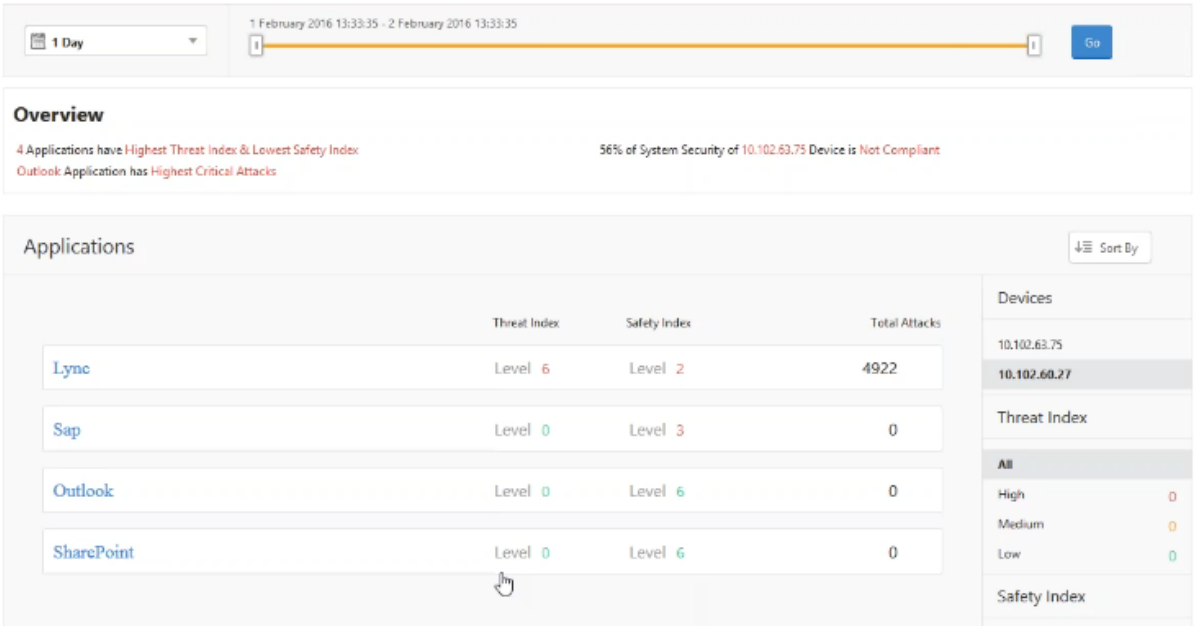


在部署配置之前确定安全指数

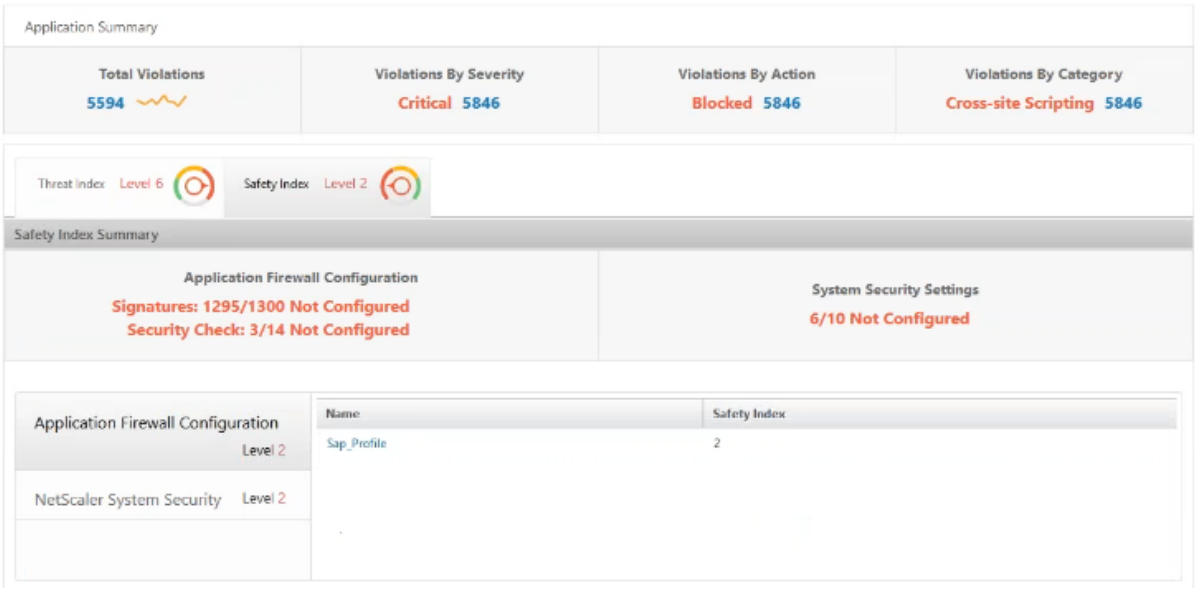
在 Citrix ADC 实例上部署安全配置后，会发生安全漏洞，但您可能希望在部署安全配置之前评估安全配置的有效性。

例如，您可能需要评估具有 10.102.60.27 IP 地址的 Citrix ADC 实例上 SAP 应用程序配置的安全索引。

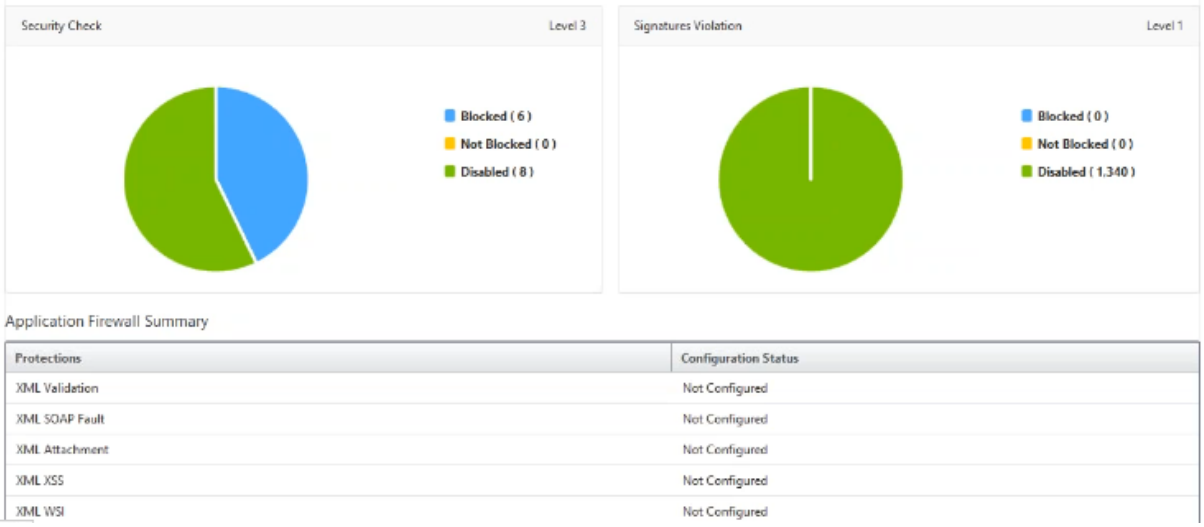
在 **Security Insight** 控制面板的设备下，单击您配置的 Citrix ADC 实例的 IP 地址。可以看到威胁指数和攻击总数都是 0。威胁指数直接反映应用程序上攻击的数量和类型。攻击数为零表示应用程序没有面临任何威胁。



单击 **Sap > Safety Index**（安全指数）**> SAP_Profile**，并评估显示的安全指数信息。



在应用程序防火墙摘要中，可以查看不同保护设置的配置状态。如果一个设置被设置为日志或如果一个设置未配置，则为应用程序分配较低的安全指数。



SSL Insight

February 6, 2024

SSL Insight 提供安全 Web 事务 (HTTPS) 的可见性，并允许 IT 管理员通过对安全 Web 事务提供集成、实时和历史监视，监视 Citrix ADC 提供的所有安全 Web 应用程序。通过此功能，管理员可以评估以下内容：

- 确定配置更改对客户使用情况的影响：管理员可以了解更改配置（例如关闭 SSLv3 或移除 RC4-MD5 等密码）对客户端的影响。这可以通过评估此协议和密码的历史事务数据来完成。
- 量化客户端性能：管理员可以根据使用的 SSL 密码/协议或协商的证书了解对应用程序响应时间的影响。
- 应用程序安全：评估是否有任何应用程序在低安全协议、密码或弱密钥强度下运行事务。

如果在 Citrix ADC 实例上启用 SSL 分析，则会记录和记录每个 SSL 事务的 SSL 统计信息。这些统计信息显示 SSL 流的详细信息。此外，每个成功的连接都会由 Citrix Application Delivery Management (ADM) 分析记录和显示。

SSL Insight 提供以下关键信息，这些信息由 Citrix ADM Analytics 显示：

- SSL 协议版本已协商
- 协商的密码和密码强度
- 使用的证书的签名哈希算法
- 证书类型和大小
- SSL 前端和后端错误

> 注意
>
> 对于成功的 SSL 连接，SSL AppFlow 日志记录会在每笔事务结束时进行。

必备条件

- 您打算配置 SSL Insight 的 Citrix ADC 实例必须运行 Citrix ADC 软件版本 11.1 51.21 及更高版本。在运行 11.1 51.21 的 ADC 实例上运行以下命令，以启用 Logstream 作为 SSL Insight 的传输类型。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   对于运行版本 12.0 及更高版本的 ADC 实例，在从 ADM 启用 AppFlow 的同时，选择 Logstream 作为传 输类型。

- Citrix ADM 版本和版本必须等于或高于 Citrix ADC 版本和内部版本。例如，如果您安装了 Citrix ADM 11.1 版本 61.7，请确保已安装了 Citrix ADC 11.1 版本 60.14 或更早版本。

配置 **SSL Insight**

如果您启用了以下元素，则 SSL Insight 指标包含在 Web Insight 报告中：

- 在每个 Citrix ADC 实例上启用 Web 智能分析的 AppFlow。
- 在每个 Citrix ADC 实例上启用 ULFD 模式。
- 在每个 Citrix ADC 实例上启用所需的 AppFlow 参数。

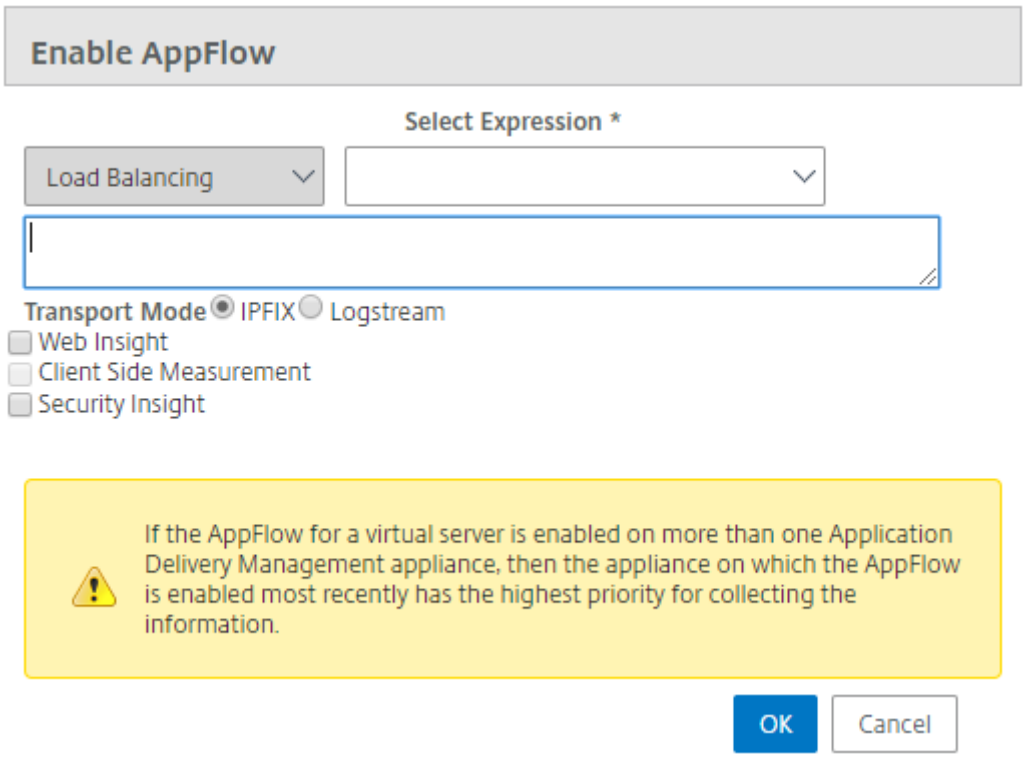
启用 **AppFlow** 功能

> 注意
>
> 您可以从 Citrix ADM 或每个 Citrix ADC 实例启用 AppFlow 功能。

要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到“网络”**>**“实例”，然后选择要启用分析的 **Citrix ADC** 实例。
2. 从选择操作列表中，选择配置分析。
3. 选择虚拟服务器，然后单击“启用 **AppFlow**”。
4. 在“启用 AppFlow”字段中，键入 **true**，然后选择 **WebInsight**。
5. 在每个 Citrix ADC 实例上重复步骤 3 到步骤 6。

6. 单击确定。



> 注意
>
> 如果虚拟服务器的运行状态不是“UP”（运行），则无法在虚拟服务器上启用数据收集。

要使用 **Citrix ADC GUI** 启用 **AppFlow** 功能，请执行以下操作：

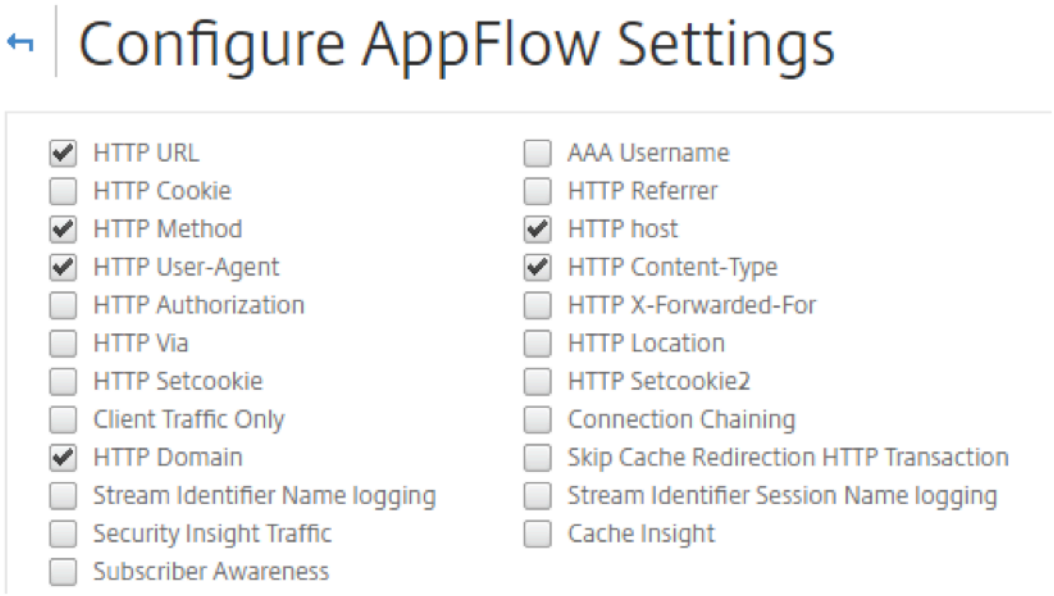
在 Citrix ADC 实例的 GUI 中，导航到“配置”**>**“系统”**>**“设置”，单击“配 置高级功能”，然后选择“**AppFlow**”。

启用 **SSL** 智能分析参数

在每个 Citrix ADC 实例上，您必须启用某些 HTTP 参数才能在 Citrix ADM 中显示 SSL 智能分析记录。

要从 **Citrix ADC** 配置实用程序启用 **SSL** 智能分析参数，请执行以下操作：

1. 导航到 配置 > 系统 > **AppFlow**，然后单击“更改 **AppFlow** 设置”。
2. 选中以下复选框：**HTTP** 域、**HTTP** 主机、**HTTP** 方法、**HTTP URL**、**HTTP** 用户代理、**HTTP** 内容类型。
3. 单击确定。



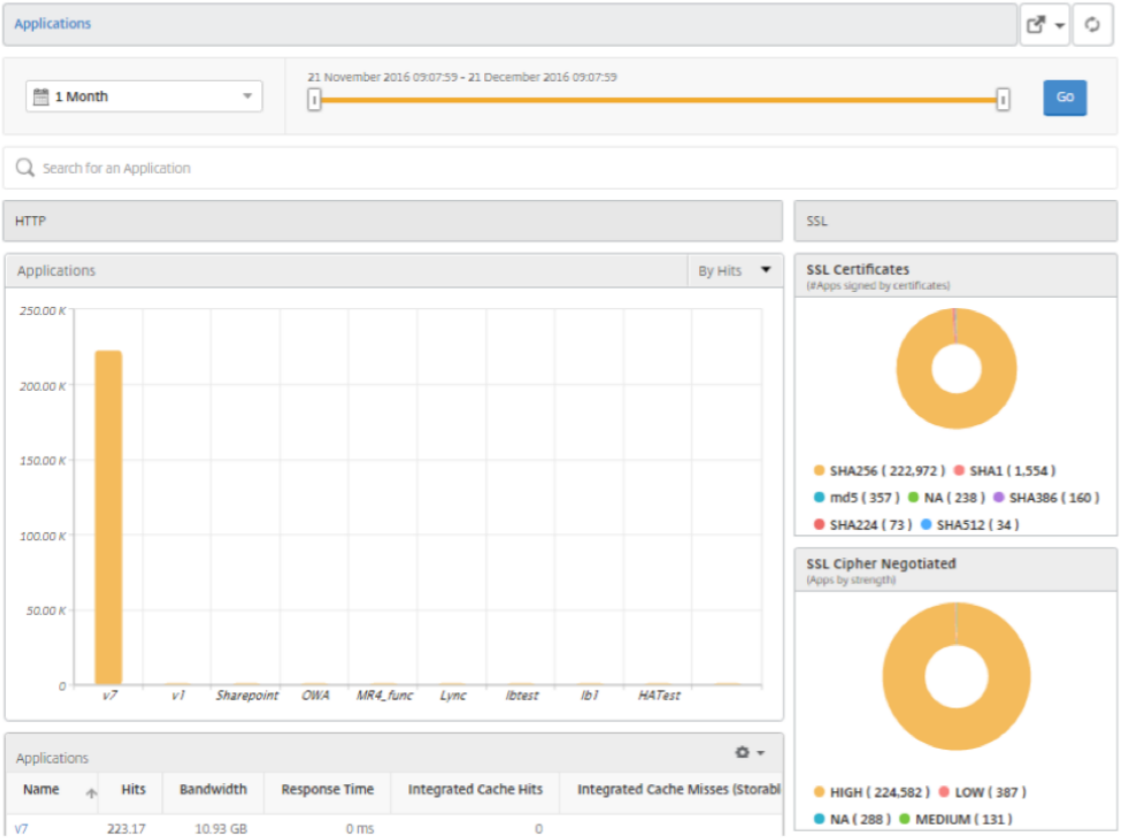
查看 **SSL** 智能分析度量

Citrix ADM 中的 SSL 智能分析度量提供了 Citrix ADC 实例所服务的 SSL 事务性能的详细视图。您可以在客户端、服务器或应用程序级别查看 SSL Insight 指标，以及查看 SSL 成功和失败事务的指标。借助这些指标，您可以分析和优化您的 Citrix ADC HTTPS 设置和 SSL 证书设置，并跟踪性能问题。

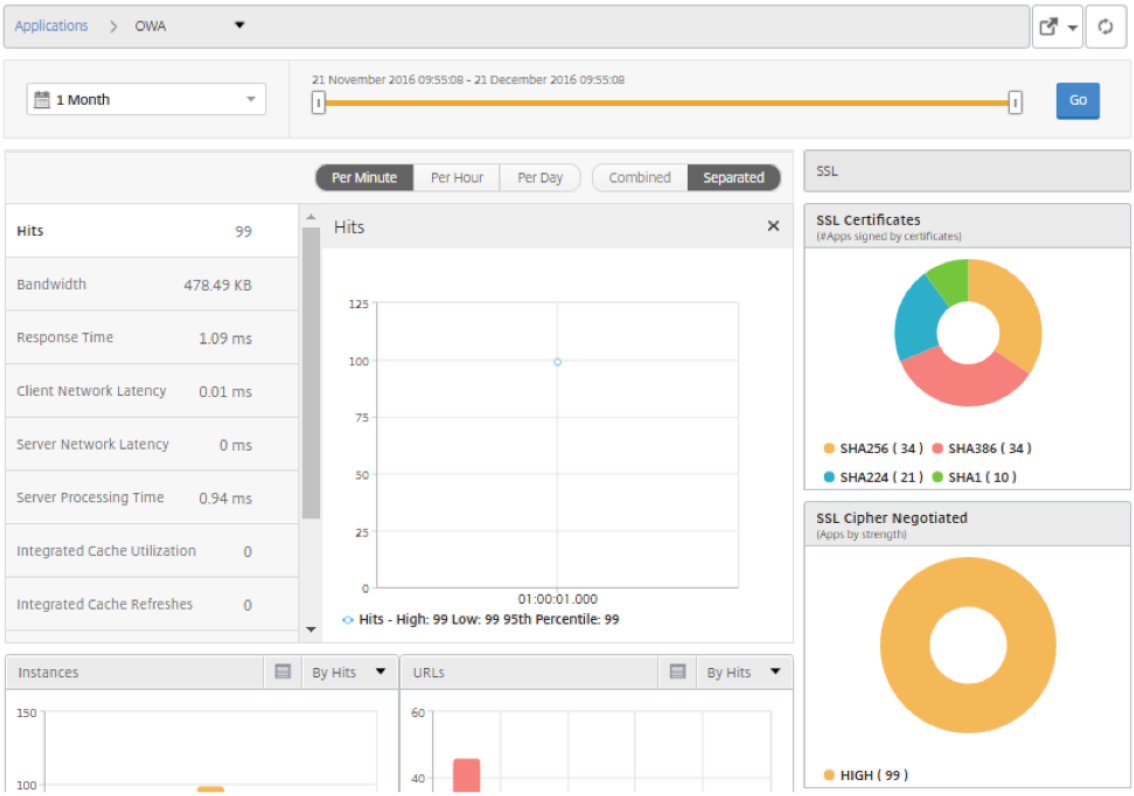
要在 **Citrix ADM** 中监视 **SSL** 智能分析度量，请执行以下操作：

1. 在“**** 分析”选项卡上，导航到 **Web Insight** ，然后单击“客户端”、“服务 ** 器”或“应用程序”节点，分别显示有关客户端、服务器或应用程序的指标。
2. 在左上角窗格中，从期间列表中选择要显示其指标的时间范围。可以使用时间范围滑块自定义时间范围。单击转到。
3. SSL Insight 指标将以饼图形式显示，您可以单击这些图表以了解更多详细信息。

> 注意
>
> 饼图显示所有应用程序、客户端或服务器的度量。



4. 要显示特定应用程序、客户端或服务器的详细信息，请单击条形图上的相应值。



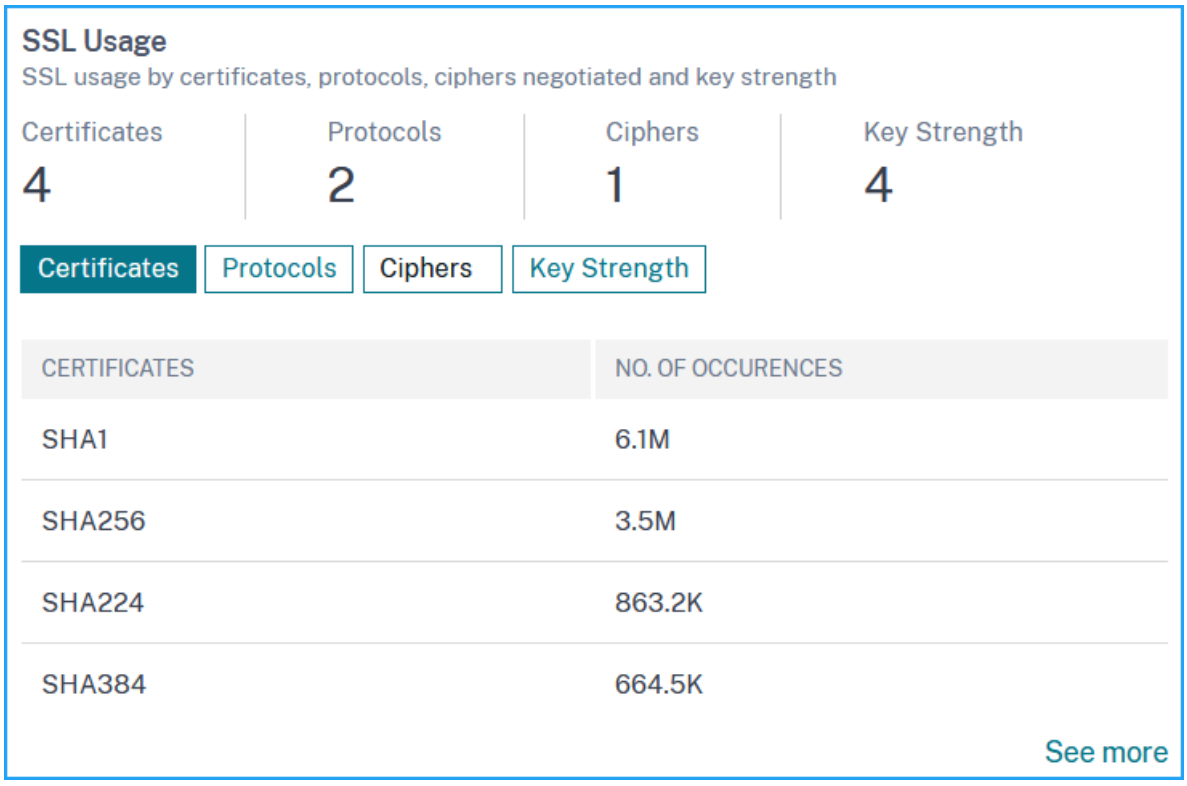
5. 要查看失败的 SSL 事务，请在“SSL”部分中选择单选按钮。

使用案例：获取应用程序、客户端或服务器的 **SSL** 事务概述

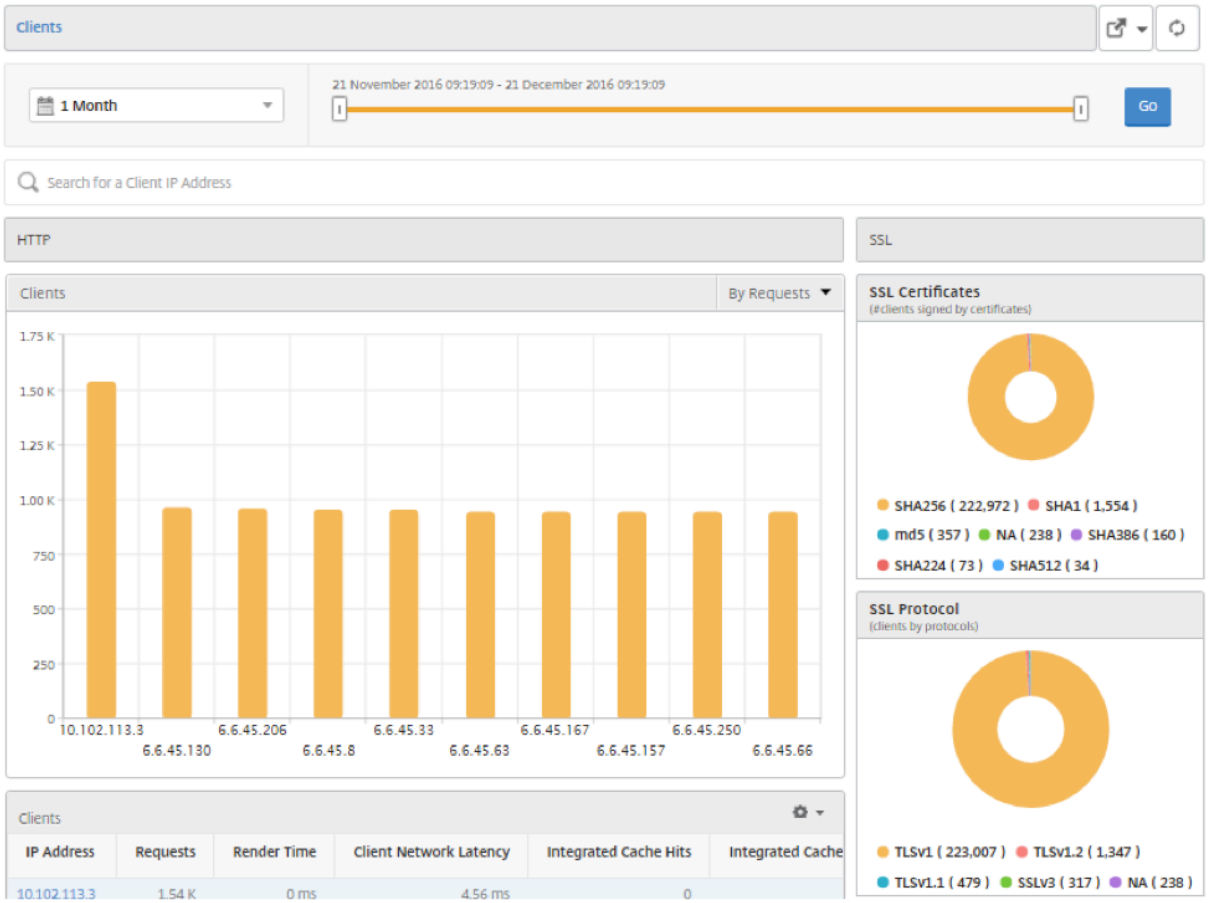
以下用例说明了如何使用 SSL Insight 来评估应用程序、客户端和服务器中的各种 SSL 参数的使用情况，以及改进安全措施。

请考虑您有一组使用 SSL 事务 (HTTPS) 进行通信的应用程序，并且您已将 Citrix ADM 配置为监视 SSL 组件。您可能需要频繁查看应用程序，以便可以首先关注最需要注意的应用程序。SSL 见解控制板提供了应用程序在您选择的一段时间内以及针对所选 Citrix ADC 设备使用的各种 SSL 参数的摘要。具体如下：

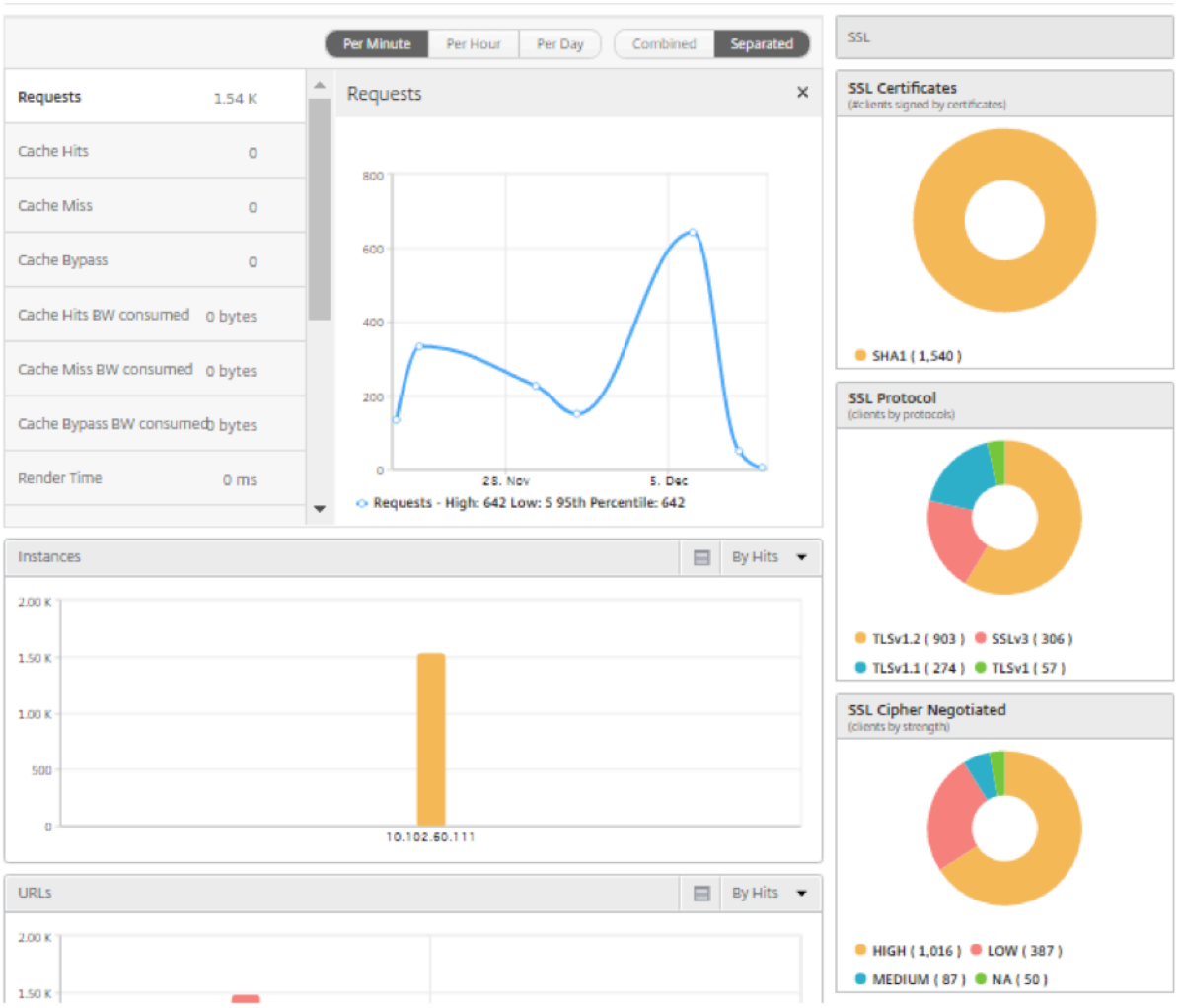
- SSL Certificates（SSL 证书）
- SSL Protocols（SSL 协议）
- SSL Cipher Negotiated（协商的 SSL 密码）
- SSL Key Strength（SSL 密钥强度）
- SSL Failure - Frontend（SSL 失败 - 前端）
- SSL Failure - Backend（SSL 失败 - 后端）



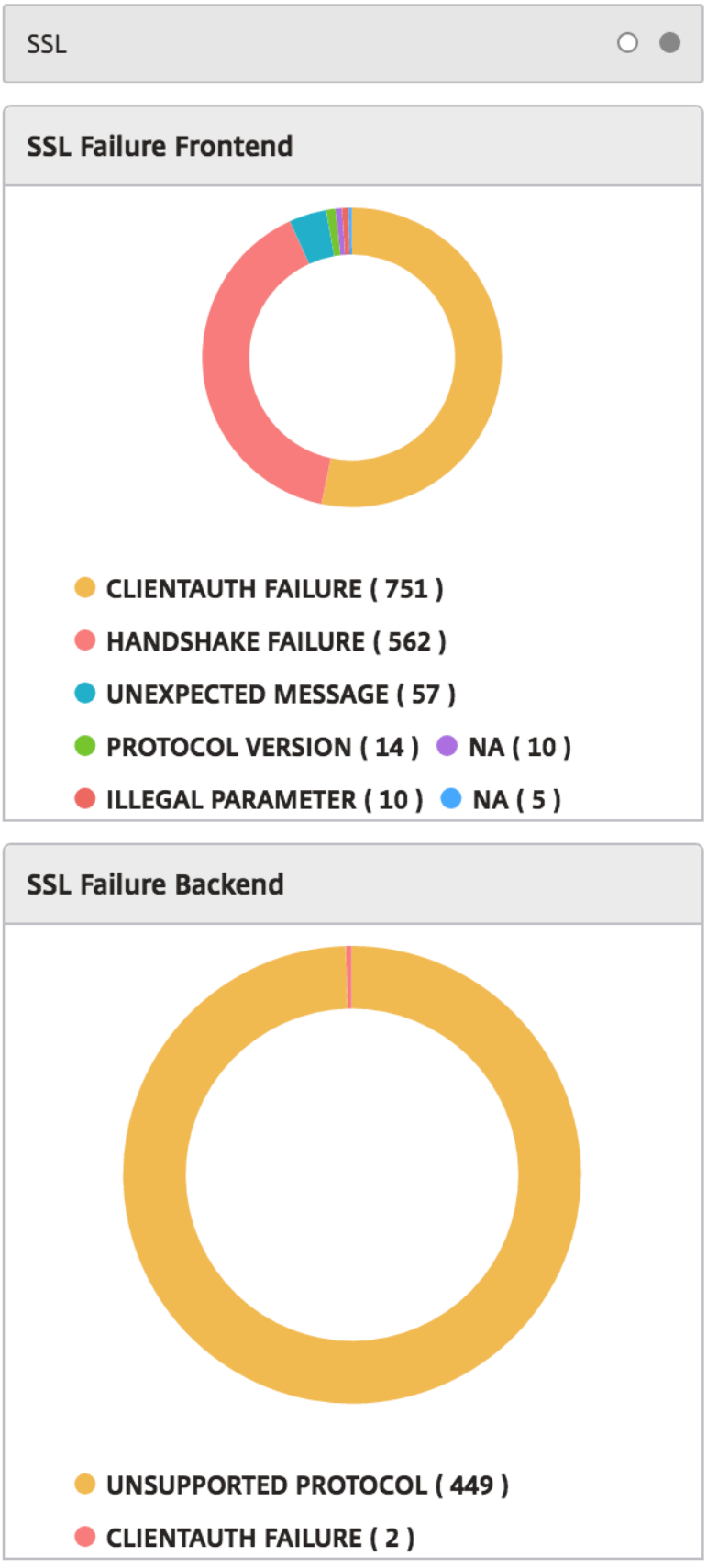
在以下示例中，您可以看到客户端列表（按其 IP 地址标识）和每个客户端的 SSL 命中数。此外，在右侧，可以看到所有客户端的 SSL 参数。



要显示某个客户端的 SSL 详细信息，请在条形图中或在图形下面的表中选择该客户端。在以下示例中，选定客户端的事务使用 SHA1 SSL 证书和四个主要协议：TSLv1.2、TSLv1.1、TSLv1 和 SSLv3。您还可以看到协商了各种强度的密码。颜色编码指示 SSL 协议的强度，为您提供有关弱密码和强密码的信息。



同样，要查看有关失败的 SSL 事务的信息，请选择 **SSL** 部分上的单选按钮。SSL 前端和后端故障分别显示在两个饼图中。在以下示例中，您可以查看主要的后端 SSL 错误是握手失败和主要前端 SSL 错误是非法参数。



TCP Insight

February 6, 2024

Citrix Application Delivery Management (ADM) 的 TCP Insight 功能提供了一种简单且可扩展的解决方案，用于监视 Citrix ADC 设备中使用的优化技术和拥塞控制策略（或算法）的指标，以避免数据传输中的网络拥塞。此功能使用“TCP 速度报告”功能，即衡量在采用和不采用 TCP 优化的情况下的 TCP 文件下载或上载性能。

您可以查看关键的传输层指标（如数据量、吞吐量和速度），并使用该信息测量 Citrix ADC 实例提供的流量，并验证 TCP 优化的优势。指标按流方向（从客户端到 Citrix ADC，从 Citrix ADC 到源服务器）、TCP 端口和虚拟局域网进行了细分。

必备条件

在开始配置 TCP Insight 功能之前，请务必满足以下必备条件：

- Citrix ADC 实例在软件版本 11.1 build 51.21 或更高版本上运行。
- 您已经安装了在软件版本 11.1 build 51.21 或更高版本上运行的 Citrix ADM。
- 为应用程序配置的所有虚拟服务器都已获得许可，以便在 Citrix ADM 上进行管理和监视。
  有关 Citrix ADM 许可的信息，请参阅许可。

Citrix ADM 的硬件要求：

组件	要求
RAM	8 GB
虚拟 CPU	4 注意 Citrix 建议您使用 8 个 CPU 以获得更好的性能。
存储空间	120 GB 注意 Citrix 建议您使用 500 GB 以获得更好的性能。

启用 **TCP Insight**

在查看 TCP Insight 指标之前，必须在 Citrix ADM 上启用该功能。

要启用 **TCP** 见解：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到分析 > 设置，然后单击启用分析功能。

3. 在启用分析功能页面上，选择启用 **TCP Insight**。
4. 在确认窗口中，单击确定。

在 **Citrix ADM** 中查看 **TCP Insight** 指标

在 Citrix ADM 中启用 TCP Insight 后，您可以查看关键传输层信息，如流量模式（Internet 或移动数据）、数据量、吞吐量、接口、端口、平均上载速度、平均下载速度。

要在 **Citrix ADM** 中显示 **TCP** 智能分析指标，请执行以下操作：

导航到分析 > **TCP Insight**。

您可以将鼠标指针悬停在条形图上，以查看相应传输技术的数据量。此外，您还可以在图形下面的表中查看数据量和其他指标。

> 注意
>
> 您可以使用表格上的设置图标自定义图表中显示的指标。您还可以选择指标所属的时间段，以及使用时间滑块调整时间段。

您还可以从 TCP Insigh t 列表中进行选择，查看接口、端口和比特率等指标。

用例

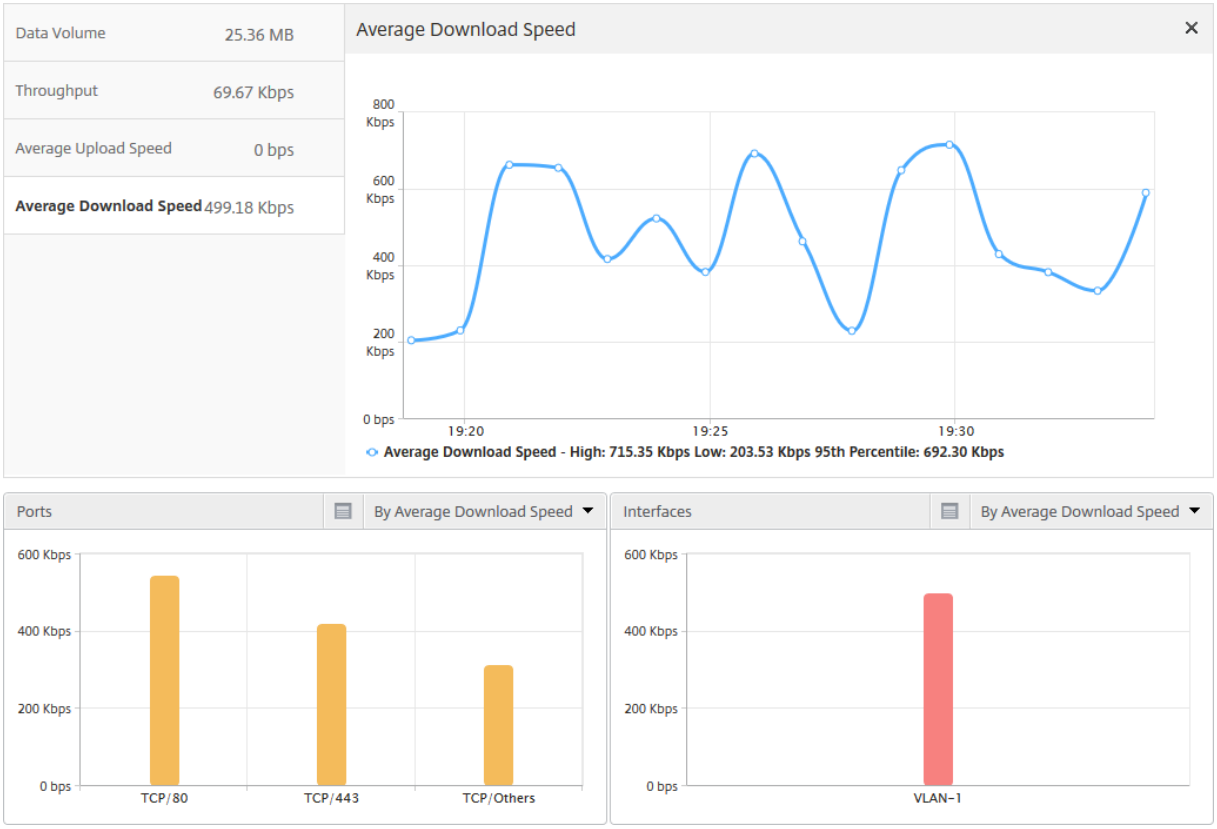
以下用例说明了在 Citrix ADC 设备上使用 TCP Insight 的一些方法：

- 评估 TCP 优化的好处
- 调整 TCP 参数
- 衡量 TCP 优化对流量的影响

评估 **TCP** 优化的好处

Citrix ADC TCP 优化实际上对移动（无线电）或企业网络（互联网）有多大好处。您可以查看通过 TCP 进行的数据传输的速度，以及比较未优化性能和优化性能。这些衡量指标按下载和上载方向（始终在无线/客户端上）以及按不同的目标端口（HTTP (80) 和 HTTPS (443)）单独显示。
通过检查 TCP 洞察力指标，您可以量化优化 TCP 流量所获得的速度提升。

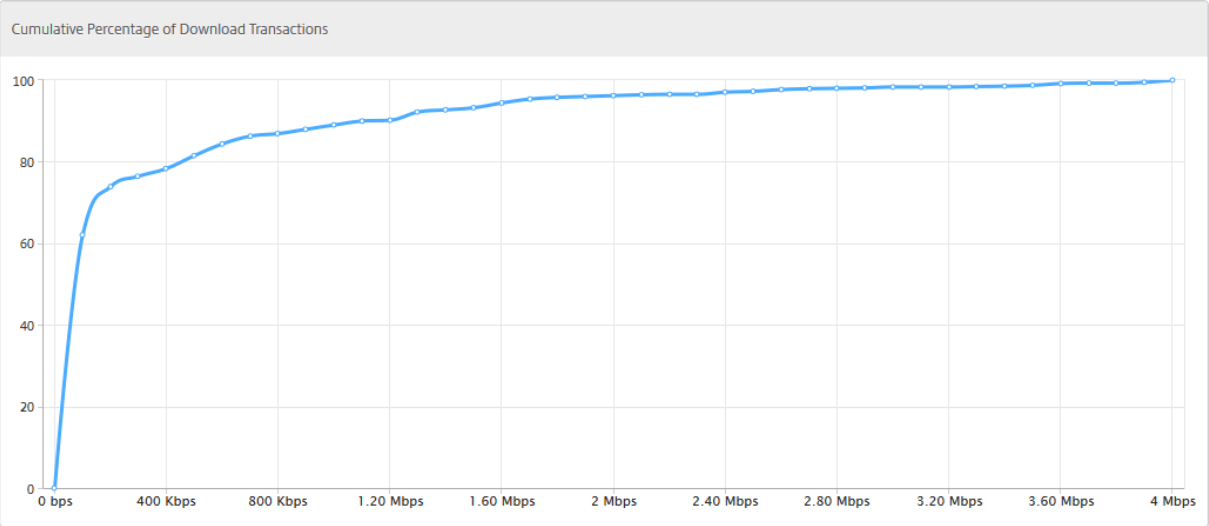
要查看这些参数的摘要，请登录 Citrix ADM 并单击 **TCP Insight** 选项卡。然后单击 **Sides**（端）并从条形图或图形下面的表中选择 **Internet** 或 **Radio**（无线）。



调整 **TCP** 参数

使用不同的 TCP 配置文件对同一流量可能会产生不同的输出。在这种情况下，您可能需要查看和比较 Citrix ADC 运行不同 TCP 优化配置文件的时段的速度测量值。您可以使用结果来调整 TCP 参数以提高传输速度，以及创建用于在特定的客户网络中实现最佳的用户感受体验的 TCP 配置文件。

要查看报告，请登录到 Citrix ADM。然后，在 **TCP Insight** 选项卡上，单击“比特率”，然后从条形图或图表下方的表格中选择所需的比特率。

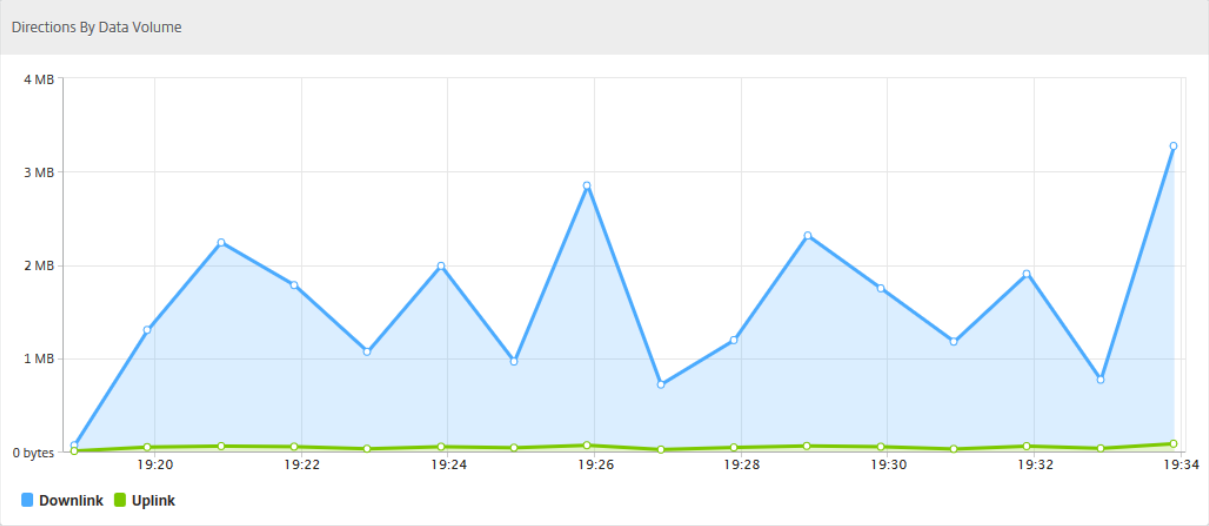


衡量 **TCP** 优化对流量的影响

可以在不同时间段之间比较 Citrix ADC 实例处理的 IP 层数据量/吞吐量的测量结果，以评估 TCP 优化对订阅者数据消耗的影响。可以按网络的各端（无线端和 Internet 端）、不同的流量段（按不同的接口或虚拟 LAN 区分）、每个方向（下行链路和上行链路）以及不同的目标端口（HTTP 和 HTTPS）单独应用衡量指标。可以使用比较来确认 TCP 优化是否促使订阅方使用更多数据。

要获取测量摘要，请登录 Citrix ADM，在 TC **P Insight** 选项卡上单击 S **id**es，然后从条形图或图表下方的表格中选择 **Internet** 或 **Radio** 。

您也可以从时间列表中选择不同的时间范围。可以使用时间范围滑块自定义时间范围。

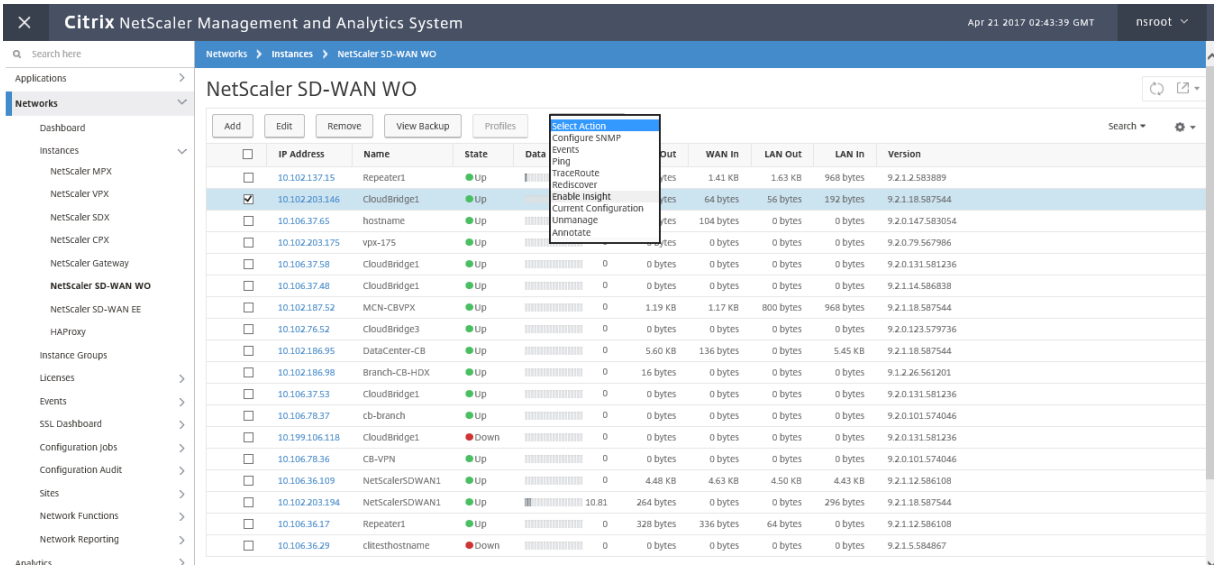


WAN Insight

February 6, 2024

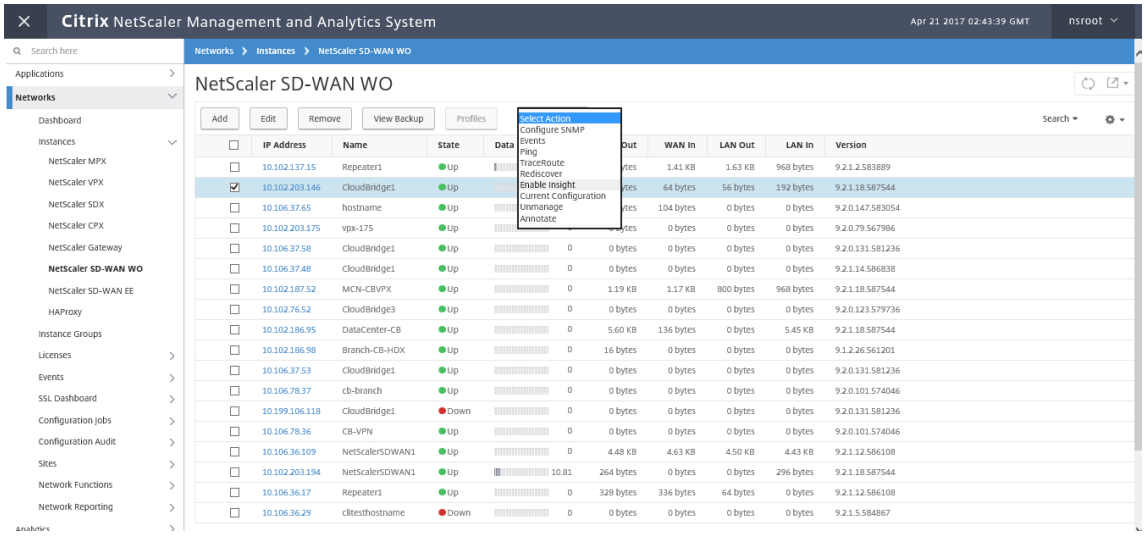
Citrix SD-WAN 优化 (WO) 设备通过提高数据中心和分支站点之间的网络数据流的效率，优化了通过 WAN 交付大量应用程序。通过 WAN Insight 分析，管理员可以轻松监视数据中心与分支 WAN 优化设备之间传输的加速和未加速 WAN 流量。通过 WAN Insight 可以查看网络上的客户端、应用程序和分支，从而有助于有效地对网络问题进行故障排除。通过实时和历史报告，您可以主动解决问题（如果有）

通过对数据中心 WAN 优化设备启用分析，Citrix Application Delivery Management (ADM) 可以收集数据并提供数据中心和分支 WAN 优化设备的报告和统计信息。



要在 **WAN** 优化设备上启用分析：

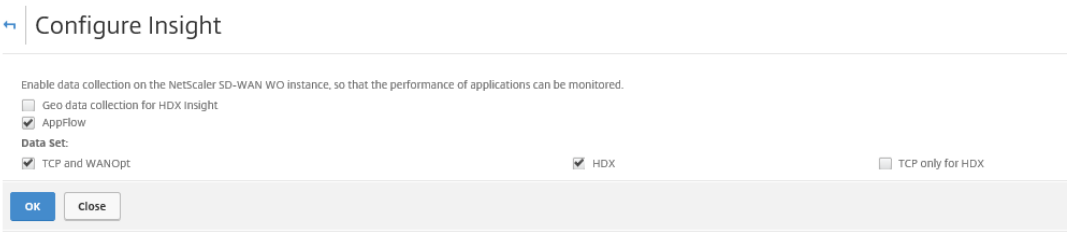
1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如 http://192.168.100.1）。
2. 在“用户名”和“密码”字段中，输入管理员凭据。
3. 导航到 网络 > 实例 > **Citrix SD-WAN**，然后选择 SD-WAN 实例。



4. 从“选择 操作”下拉列表中，选 择“配置分析”。
5. 根据需要选择以下参数：

   - 为 **HDX Insight** 收集地理数据：与 Google Geo API 共享客户端 IP 地址。
   - **AppFlow**：开始从广域网优化实例收集数据。

     - **TCP** 和 **WANOpt**：提供 TCP 和网站见解报告。
     - **HDX**：提供 HDX Insight 报告。
     - **TCP** 仅适用于 **HDX**：仅为 HDX Insight 报告提供 TCP。



6. 单击确定。

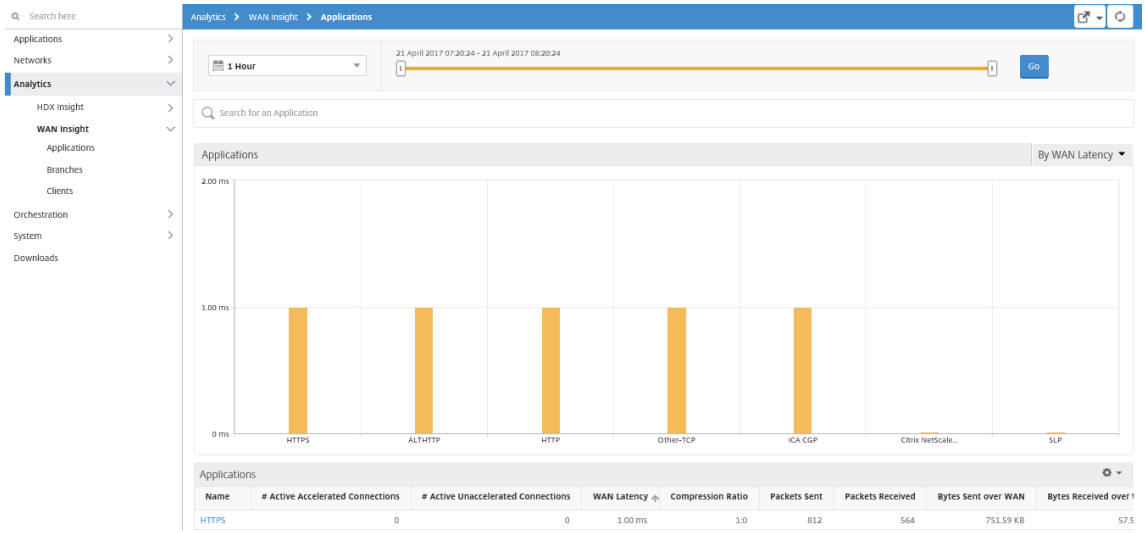
要查看 **WAN Insight** 报告，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如 http://192.168.100.1）。
2. 在“用户名”和“密码”字段中，输入管理员凭据。
3. 导航到分析 > **WAN** 见解。

> 注意
>
> 只有在将 SD-WO 实例添加到 Citrix ADM 后，WAN Insight 选项才可见。

您可以查看以下报告：

- 应用程序 -显示选定持续时间内所有应用程序的使用情况和性能统计信息。
- 分支机构 -显示所有 WAN 优化分支设备的使用情况和性能统计信息。
- 客户端 -显示每个分支中访问 WAN 优化设备的所有客户端的使用情况和性能统计信息。



显示以下指标：

指标	说明
Active Accelerated Connections（活动加速连接）	加速的活动 WAN 连接数。
Active Unaccelerated Connections（活动未加速连接）	未加速的活动 WAN 连接数。
WAN 延迟	用户与应用程序交互时遇到的延迟（以毫秒为单位）。
Compression Ratio（压缩比）	在选定的持续时间内分支机构与数据中心设备之间的数据压缩比率。
Packets Sent（发送的数据包数）	在选定的持续时间内 WAN 优化设备通过网络发送的数据包数。
Packets Received（接收的数据包数）	在选定的持续时间内 WAN 优化设备从网络接收的数据包数。
Bytes Sent over WAN（通过 WAN 发送的字节数）	Citrix WAN 优化设备在选定持续时间内通过 WAN 发送的字节数。
Bytes Received over WAN（通过 WAN 接收的字节数）	在选定的持续时间内 WAN 优化设备从 WAN 接收的字节数。
LAN RTO	在选定的持续时间内 WAN 优化设备向 LAN 重新传输超时的次数。

指标	说明
WAN RTO	在选定的持续时间内 WAN 优化设备向 WAN 重新传输超时的次数。
Retransmit Packets (LAN)（重新传输数据包 (LAN)）	在选定的持续时间内 WAN 优化设备向 LAN 网络重新传输的数据包数。
Retransmit Packets (WAN)（重新传输数据包 (WAN)）	在选定的持续时间内 WAN 优化设备向 WAN 网络重新传输的数据包数。

Video Insight

February 6, 2024

Video Insight 功能提供了一种简单且可扩展的解决方案，用于监视 Citrix ADC 设备使用的视频优化技术的指标，以改善客户体验和运营效率，其优点包括：

- 在高峰时段出现拥堵时管理网络。
- 改进视频播放连贯性并降低视频停顿。
- 支持新的视频服务方案（例如 Binge-on 视频服务）。
- 支持客户选择持续性最佳的视频质量。
- 为订阅方提供一致的用户体验。

在优化视频流量的同时，Citrix ADC 设备使用特殊机制来动态调节视频比特率，并采用随机采样技术来估计优化技术节省的成本。有关 Citrix ADC 视频优化功能的详细信息，请参阅 视频优化。将 Citrix ADC 装置与 Citrix Application Delivery Management (ADM) 集成后，它会从通过 Citrix ADC 装置流动的视频数据中收集关键信息。您可以使用此信息比较 ABR 视频流量的优化性能和未优化性能，以及确定由于优化产生的节省等。

> 注意
>
> Citrix ADM 中提供的未优化会话的统计信息与您在 Citrix ADC 设备中选择的随机采样会话相对应。有关随机采样的更多信息，请参阅视频优化。

Citrix ADM 中的 Video Insight 提供了以下类型的视频流量的指标：

- 通过 HTTP 进行的渐进式下载 (PD) 视频
- 通过 HTTP 进行的 ABR 视频
- 通过 HTTPS 进行的 ABR 视频
- 通过 QUIC 进行的 YouTube ABR 视频

配置 **Video Insight**

> 注意
>
> 使用 Citrix ADC Premium 许可证的 Citrix ADC 实例支持 Video Insight。Citrix ADC Premium 许可证受到 Citrix ADC 电信平台（VPX T1000 和 VPX-T）的支持。

要在 Citrix ADC 实例上配置 Video Insight，请首先启用 AppFlow 功能，配置 AppFlow 收集器、操作和策略，然后全局绑定策略。配置收集器时，必须指定要监视报告的 Citrix ADM 服务器的 IP 地址。

要在 Citrix ADC 实例上配置 Video Insight，请运行以下命令来配置 AppFlow 配置文件和策略，并在全局范围内绑定 AppFlow 策略。

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

示例

```
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
<!--NeedCopy-->
```

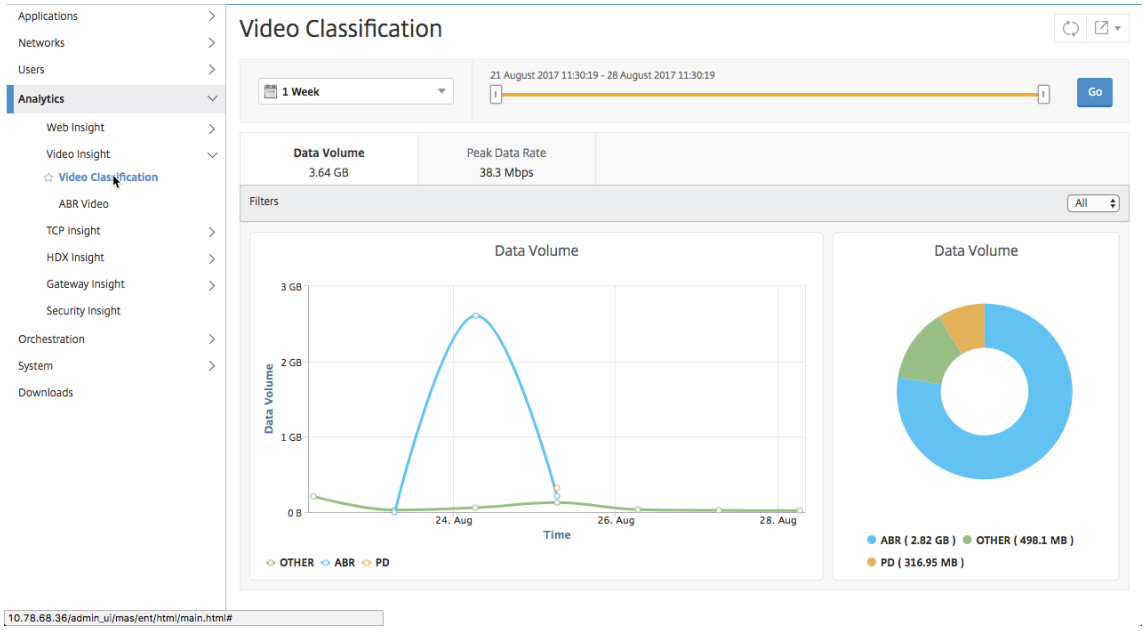
在 **Citrix ADM** 中查看 **Video Insight** 指标

在 Citrix ADM 中启用 Video Insight 后，您可以查看视频优化指标，如视频分类、数据量、峰值数据速率和 ABR 视频播放。这些指标可帮助您分析您的网络和优化视频，以改进订阅方体验、操作效率及其他性能条件。

要在 **Citrix ADM** 中查看 **Video Insight** 指标，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 虚拟设备的 IP 地址（例如 http://192.168.100.1）。

2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到 **Analytics**（分析）**> Video Insight**。



> 注意
>
> 图表中图例 **OTHER** 提供的值表示视频流量中的非 ABR 和非 PD 数据，具体取决于您选择的过滤器：
>
> - 全 部—视频流量中非 ABR（HTTP、HTTPS 和 QUIC）和非 PD（HTTP）数据的总和。
> - **HTTP** —视频流量中非 ABR 和非 PD 数据的总和。
> - **HTTPS** —视频流量中非 ABR 视频数据的总和。
> - **QUIC** —视频流量中非 ABR 视频数据的总和。

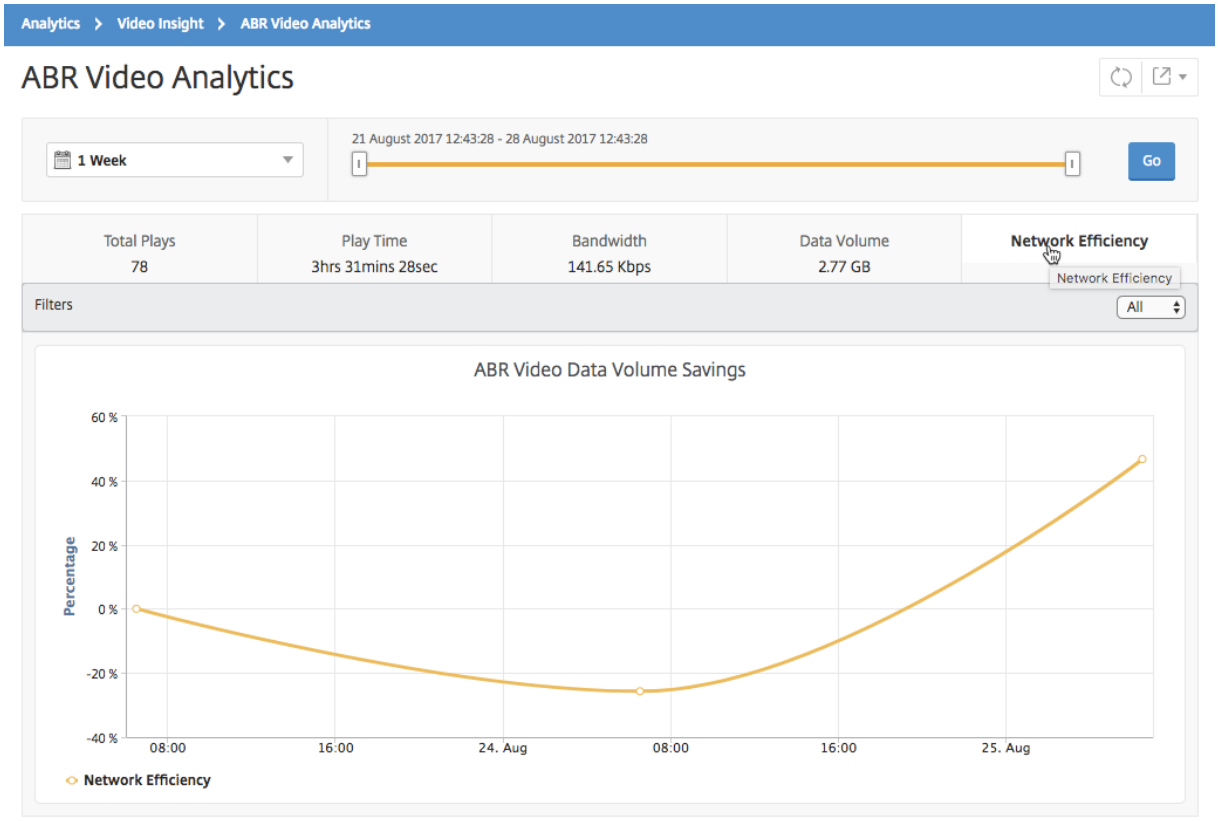
查看网络效率

February 6, 2024

对于给定时间范围，Citrix Application Delivery Management (ADM) 提供了一个图形，显示时间范围内优化的视频会话与未优化的视频会话的比率。它还显示通过优化节省的带宽百分比。节省的带宽百分比的计算公式如下：

节省的带宽百分比 = 优化 **ABR** 视频数据量平均值 **/** 未优化 **ABR** 视频数据量平均值。

要查看优化节省的带宽百分比，请登录 Citrix ADM，导航到分析 **> Video Insight**，然后单击 **ABR** 视频。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（继续），并选择 **Network Efficiency**（网络效率）选项卡。



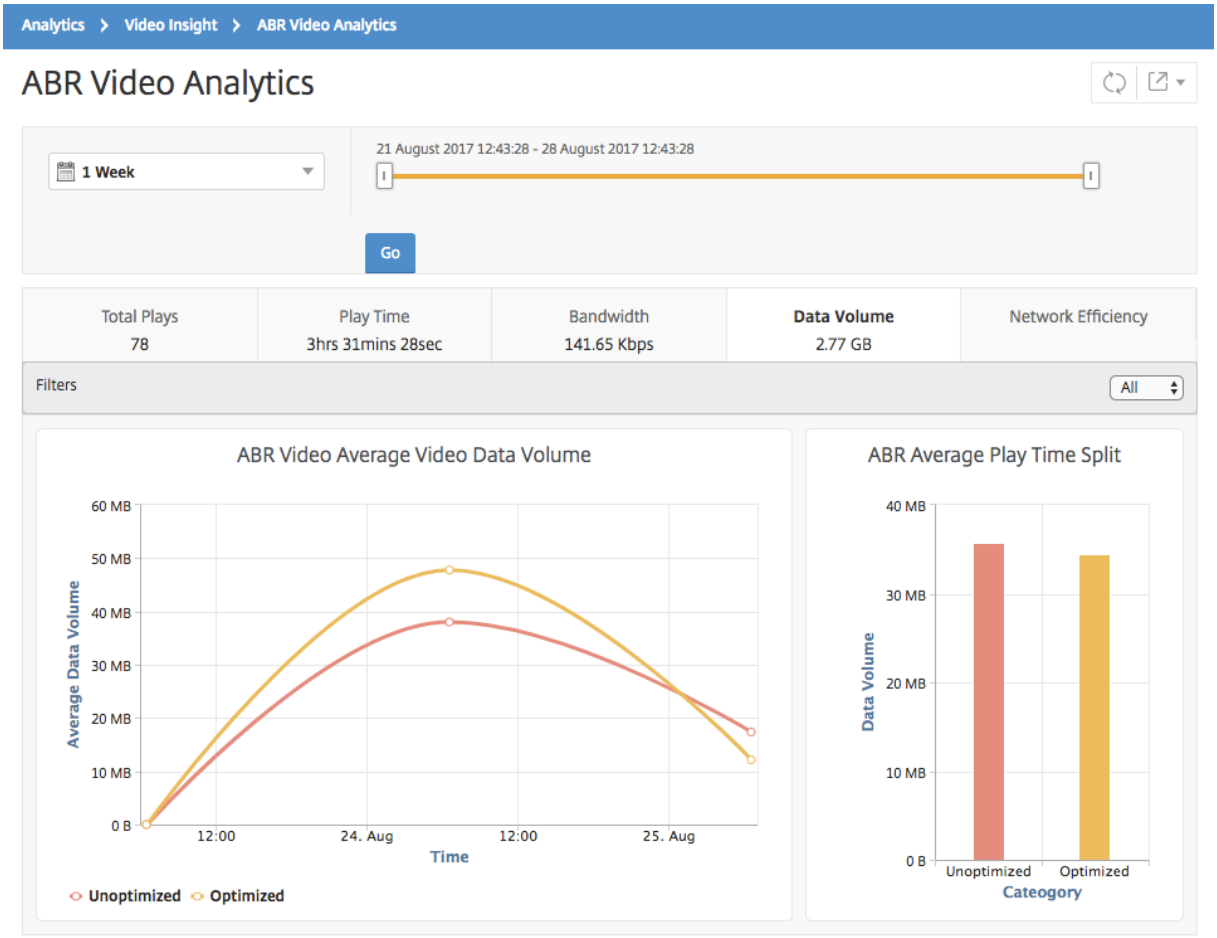
比较优化和未优化的 **ABR** 视频使用的数据量

February 6, 2024

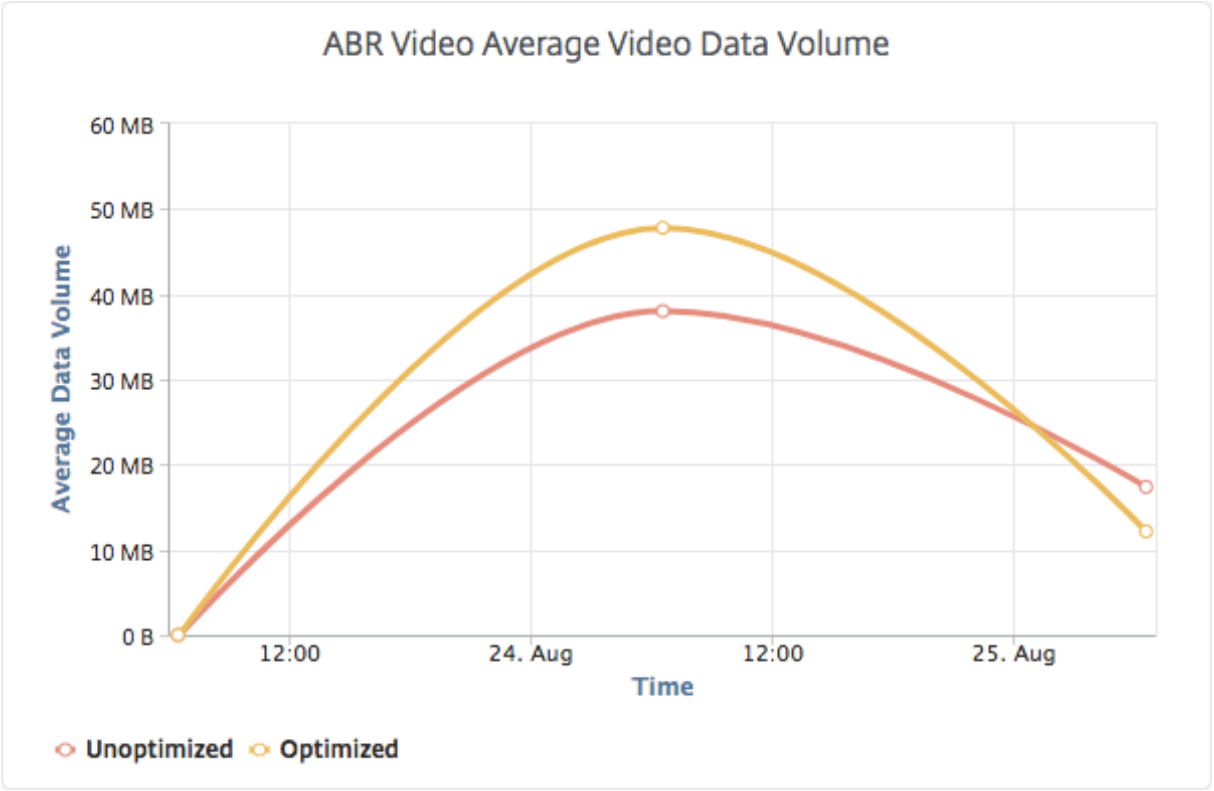
在给定的时间范围内，Citrix Application Delivery Management（ADM）显示优化和未优化的 ABR 视频使用的数据量。，以便您可以比较这两个体积。

要查看 ABR 视频使用的数据量，请登录 Citrix ADM，导航到分析 **> Video Insight**，然后单击 **ABR** 视频。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（继续），并选择 **Data Volume**（数据量）选项卡。

您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC ABR 视频。



Data Volume（数据量）选项卡提供折线图和饼图，描述 ABR 视频使用的平均数据量，以及在选定的时间范围内在您的网络中优化和未优化 ABR 视频占用的数据量。您可以将鼠标指针悬停在折线图上以查看特定时间范围内使用的平均数据量：



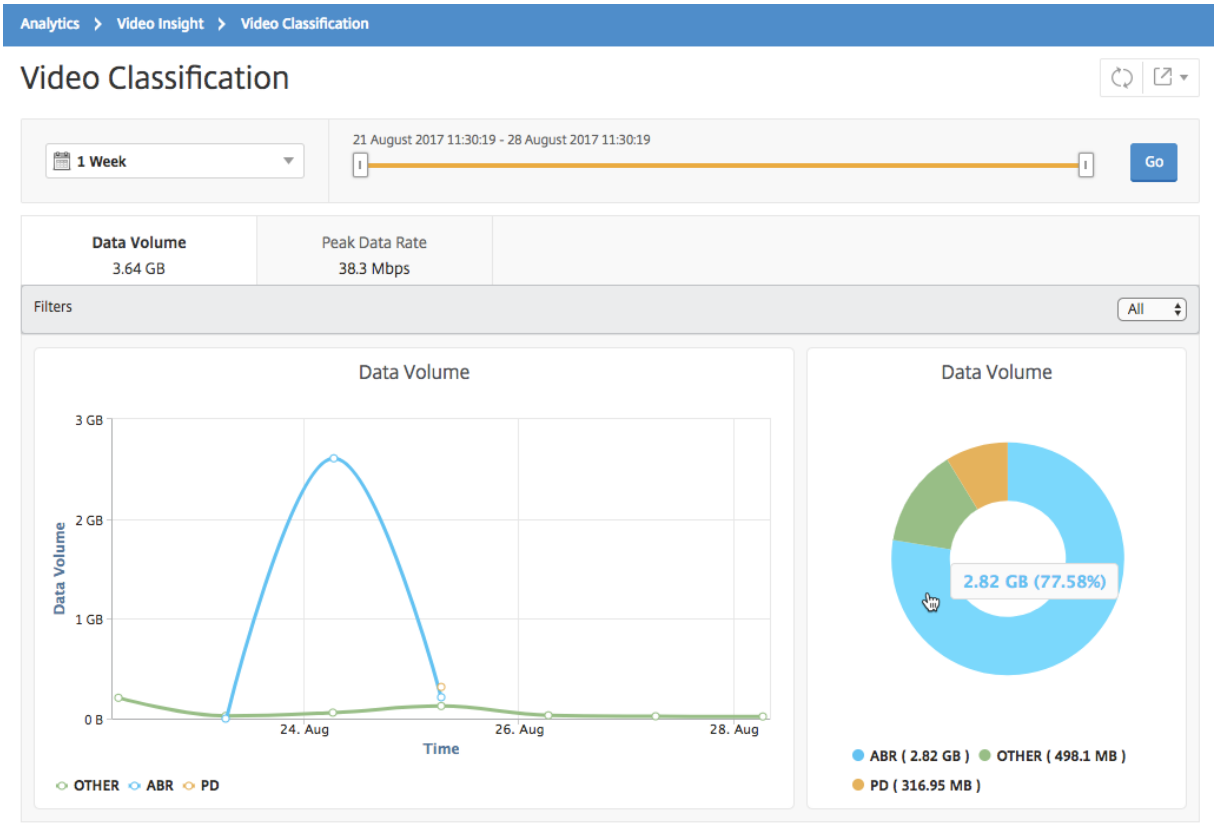
查看您的网络中通过流技术推送的视频类型和使用的数据量

February 6, 2024

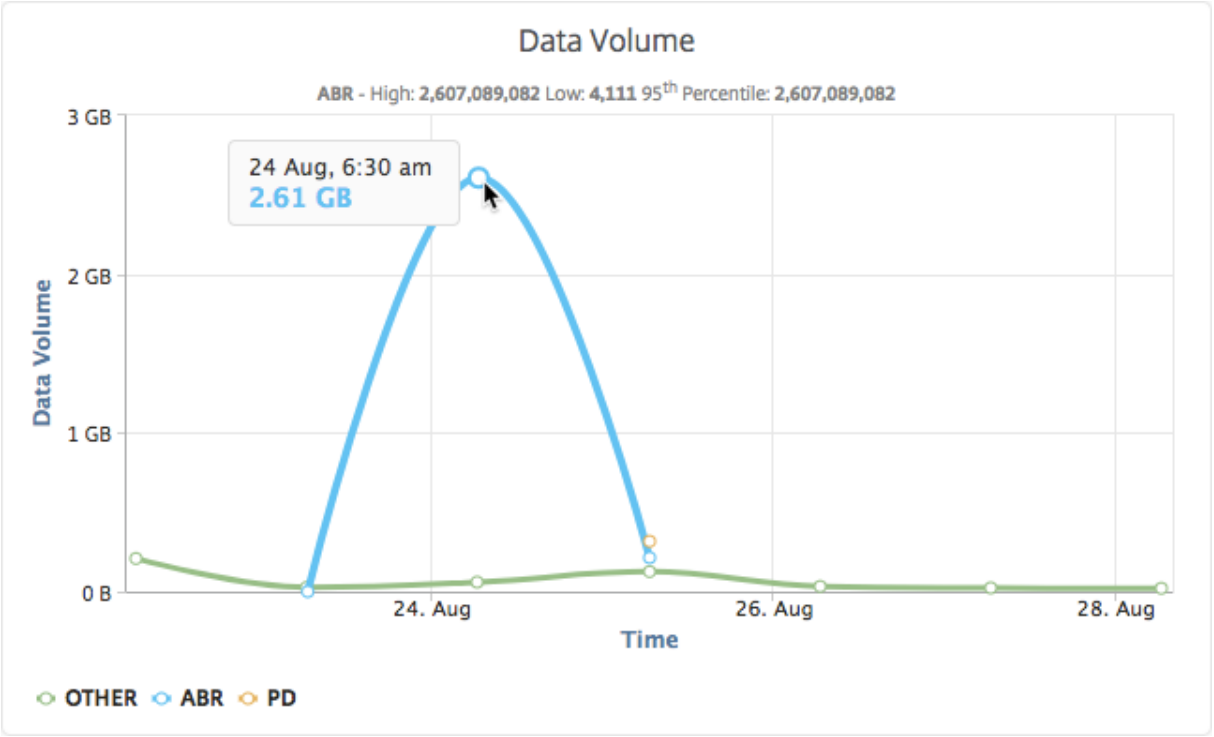
Citrix ADC 设备可检测您的网络中的加密或未加密视频流量以及视频流的类型（PD 或 ABR）。Citrix Application Delivery Management (ADM) 显示这些指标以及视频流量在定义的时间范围内消耗的数据量。

要查看视频类型和消耗的数据量，请登录 Citrix ADM，导航到 **Analytics > Video Insight**，然后单击“视频分类”。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击转到。

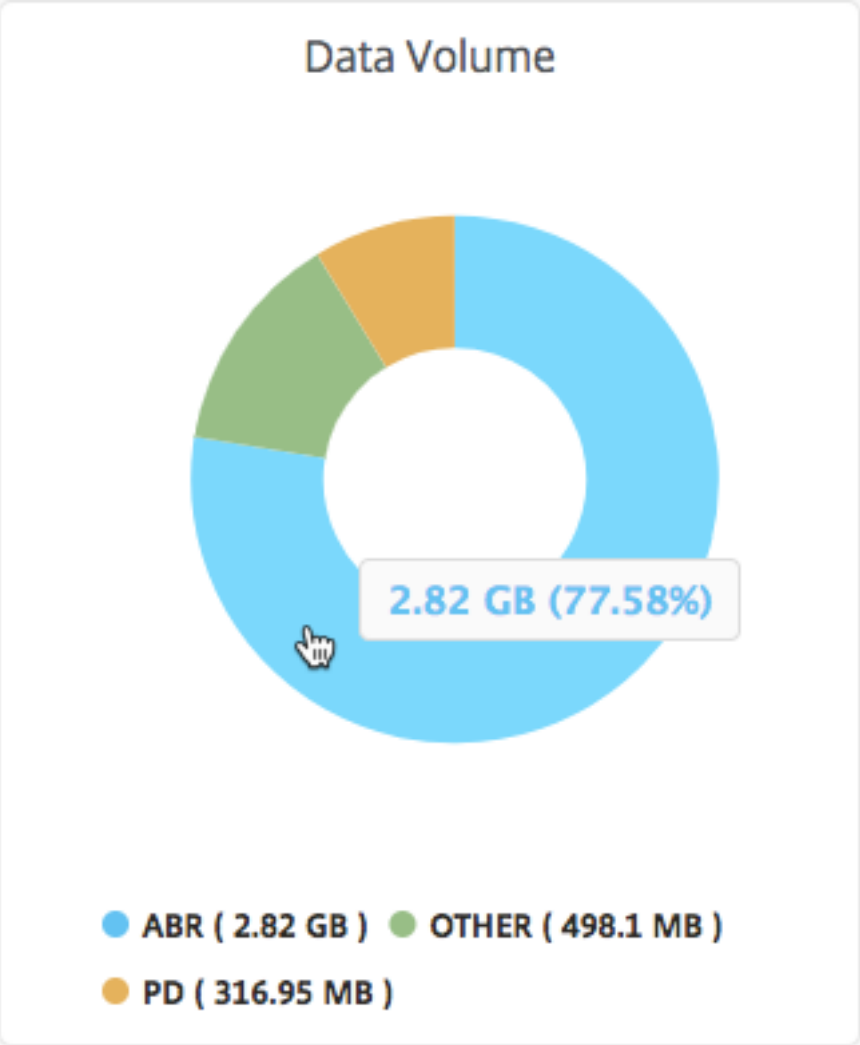
您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC 流量。



Data Volume（数据量）选项卡提供折线图和饼图，显示从您的网络中通过流技术推送的视频流量类型，以及您的网络使用的数据量。您可以将鼠标指针悬停在折线图上以查看特定时间范围内使用的数据：



此外，您还可以将鼠标指针悬停在饼图上以查看特定类型的视频流量使用的数据量的百分比。



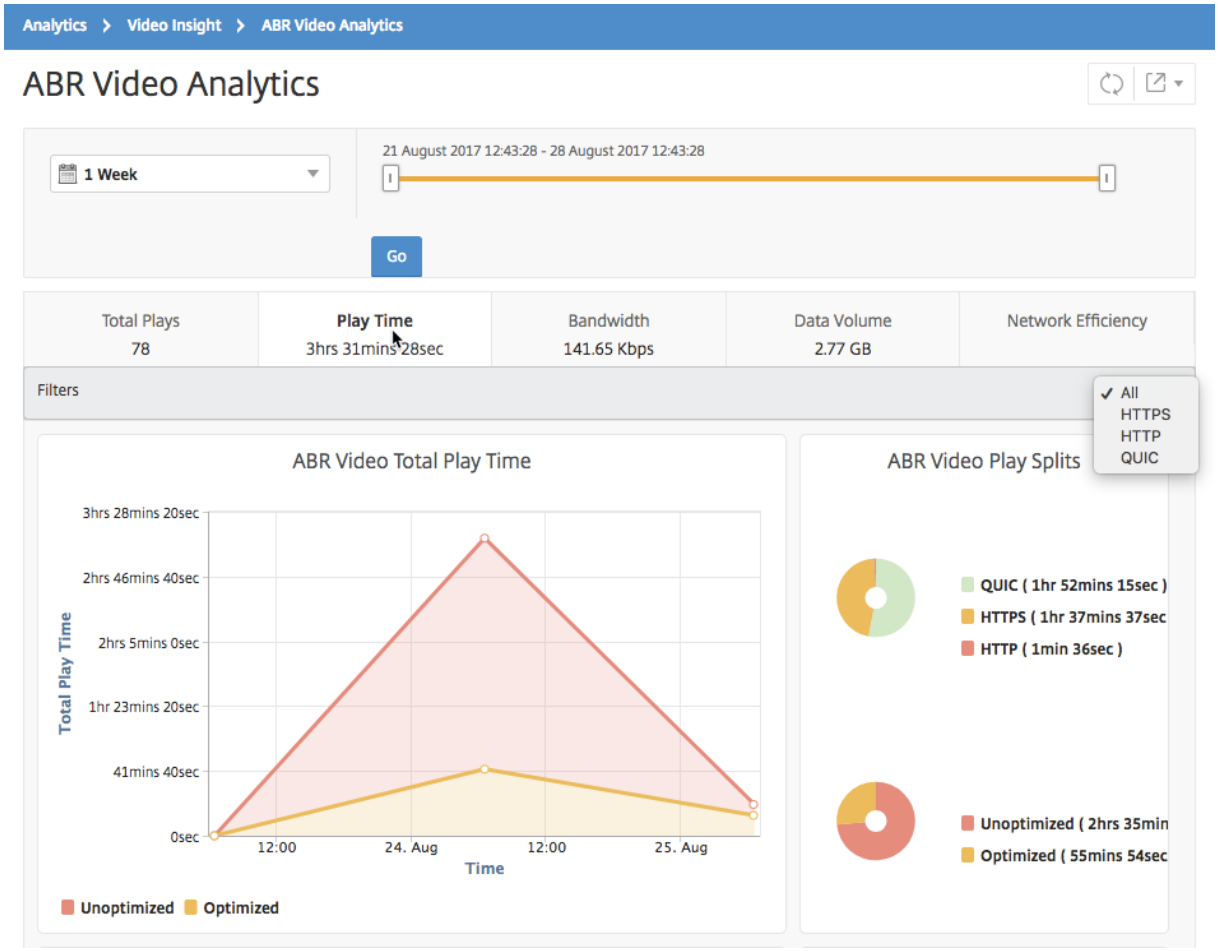
比较 **ABR** 视频的优化和未优化的播放时间

February 6, 2024

在给定的时间范围内，Citrix Application Delivery Management (ADM) 提供 ABR 视频的播放时间，还允许您比较网络中优化和未优化 ABR 视频的播放时间。

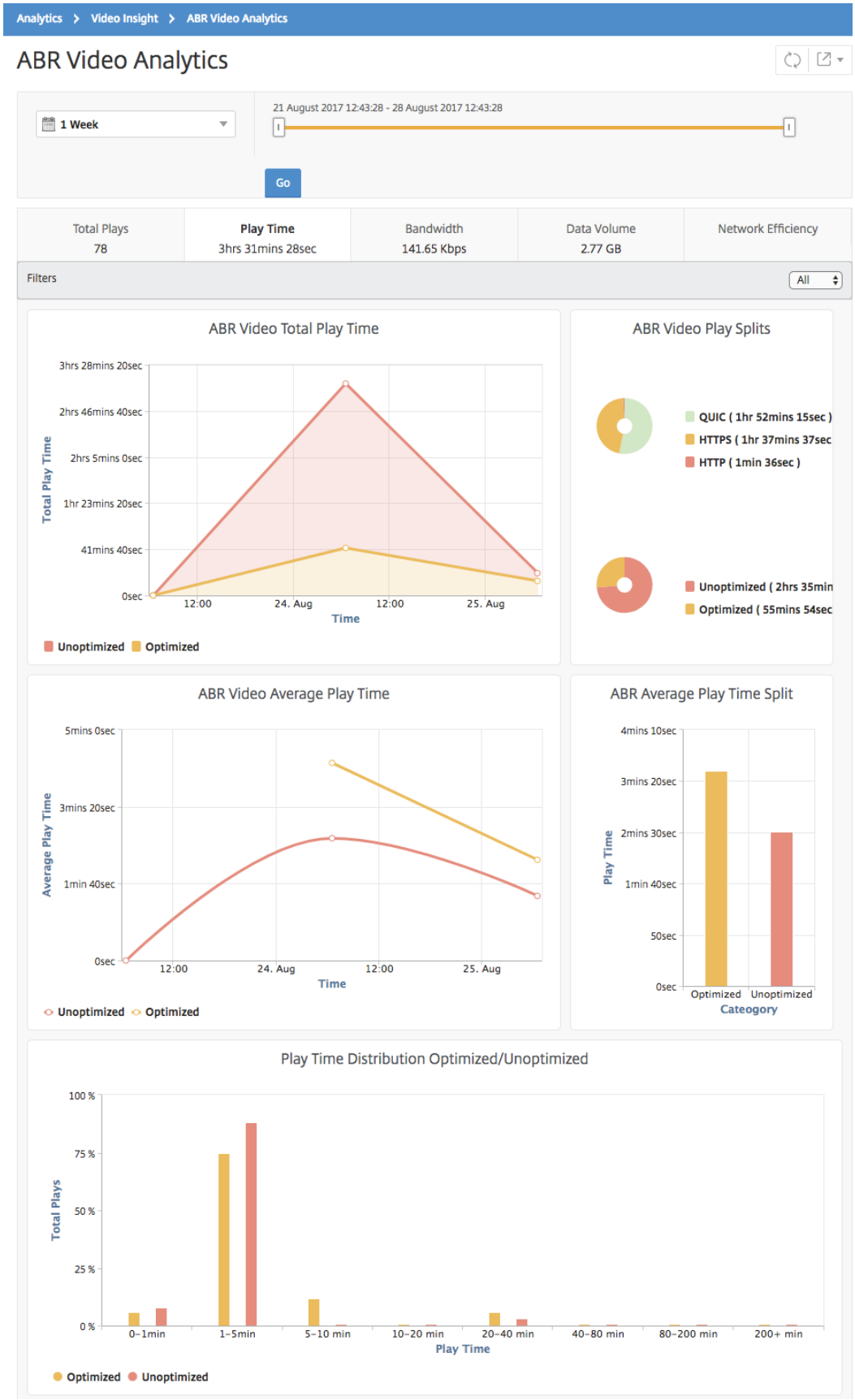
要查看播放时间，请登录 Citrix ADM，导航到分析 **> Video Insight**，然后单击 **ABR** 视频。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（转到），并选择 **Play Time**（播放时间）选项卡。

您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC ABR 视频。



对于选定的时间范围，**Play Time**（播放时间）选项卡提供折线图和饼图，描述以下内容：

- 在您的网络中 ABR 视频的总播放时间
- 在选定的时间范围内，在您的网络中 ABR 视频的优化播放和未优化播放的总播放时间。
- 加密和未加密 ABR 视频的总播放时间。
- ABR 视频的平均播放时间
- ABR 视频的优化播放和未优化播放的平均播放时间
- 加密和未加密 ABR 视频的平均播放时间
- 优化和未优化 ABR 视频之间的播放时间分布



比较优化和未优化的 **ABR** 视频的带宽占用量

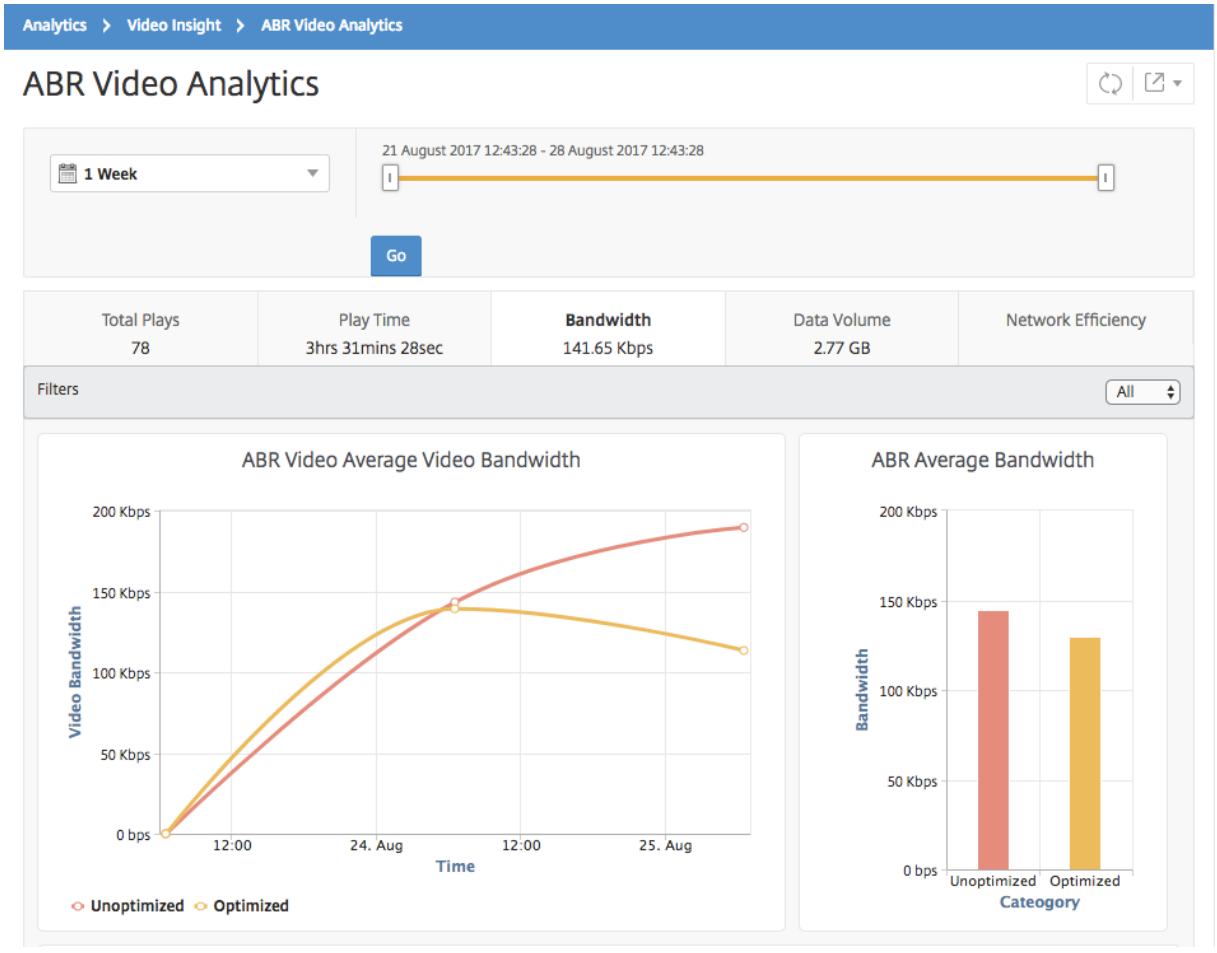
February 6, 2024

在给定时间范围内，Citrix Application Delivery Management (ADM) 提供了优化和未优化 ABR 视频所消耗的带宽，还可以根据以下情况比较网络中优化和未优化 ABR 视频所消耗的带宽：

- Play Time（播放时间）
- Data Volume（数据量）

要查看带宽消耗，请登录 Citrix ADM，导航到分析 **> Video Insight**，然后单击 **ABR** 视频分析。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（转到），并选择 **Bandwidth**（带宽）选项卡。

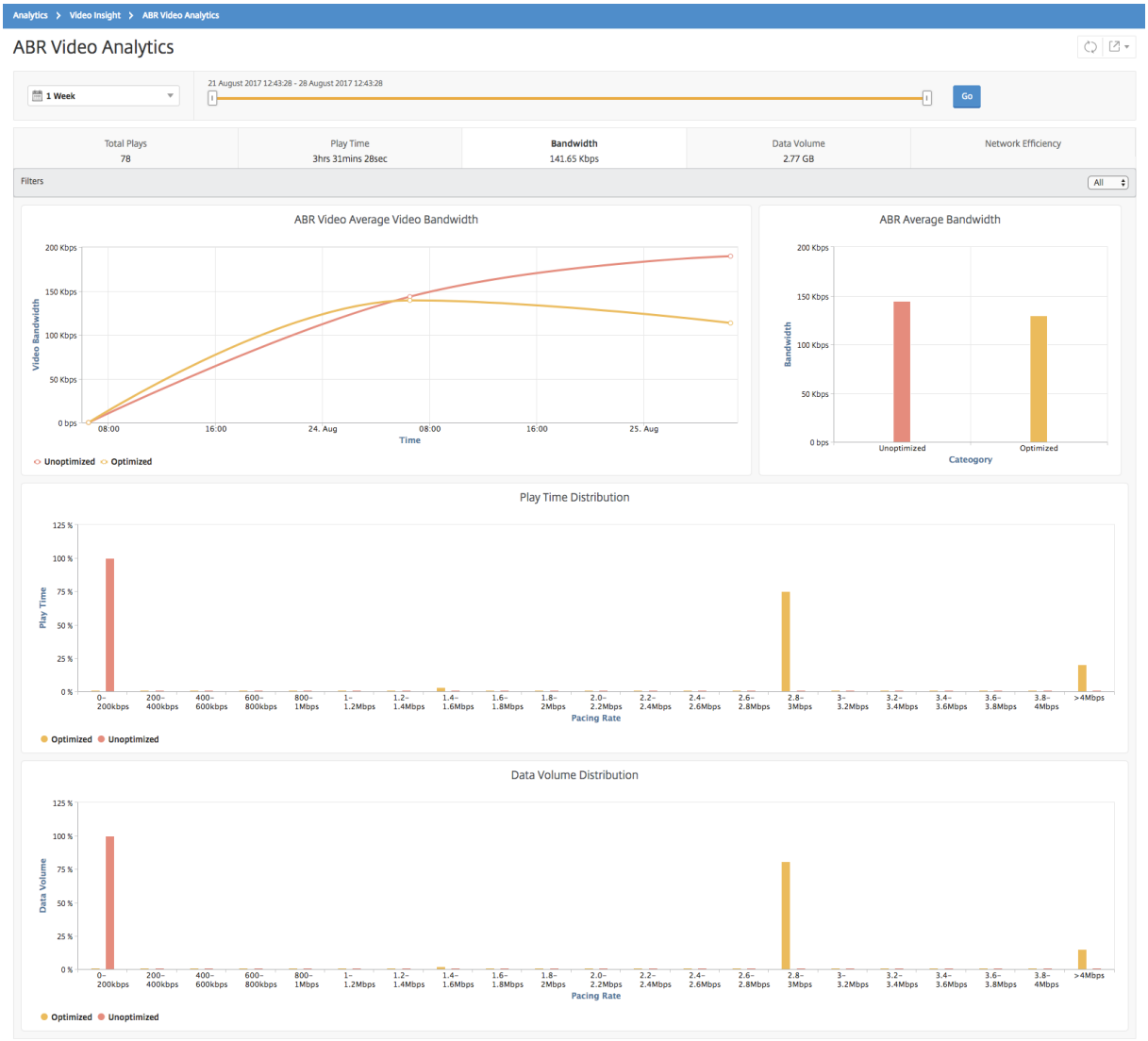
您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC ABR 视频。



对于选定的时间范围，Bandwidth（带宽）选项卡提供折线图和饼图，描述以下内容：

- 优化和未优化 ABR 视频占用的平均带宽。

- 基于优化和未优化 ABR 视频之间的播放时间分布占用的带宽。
- 基于优化和未优化 ABR 视频之间分布的数据量占用的带宽。



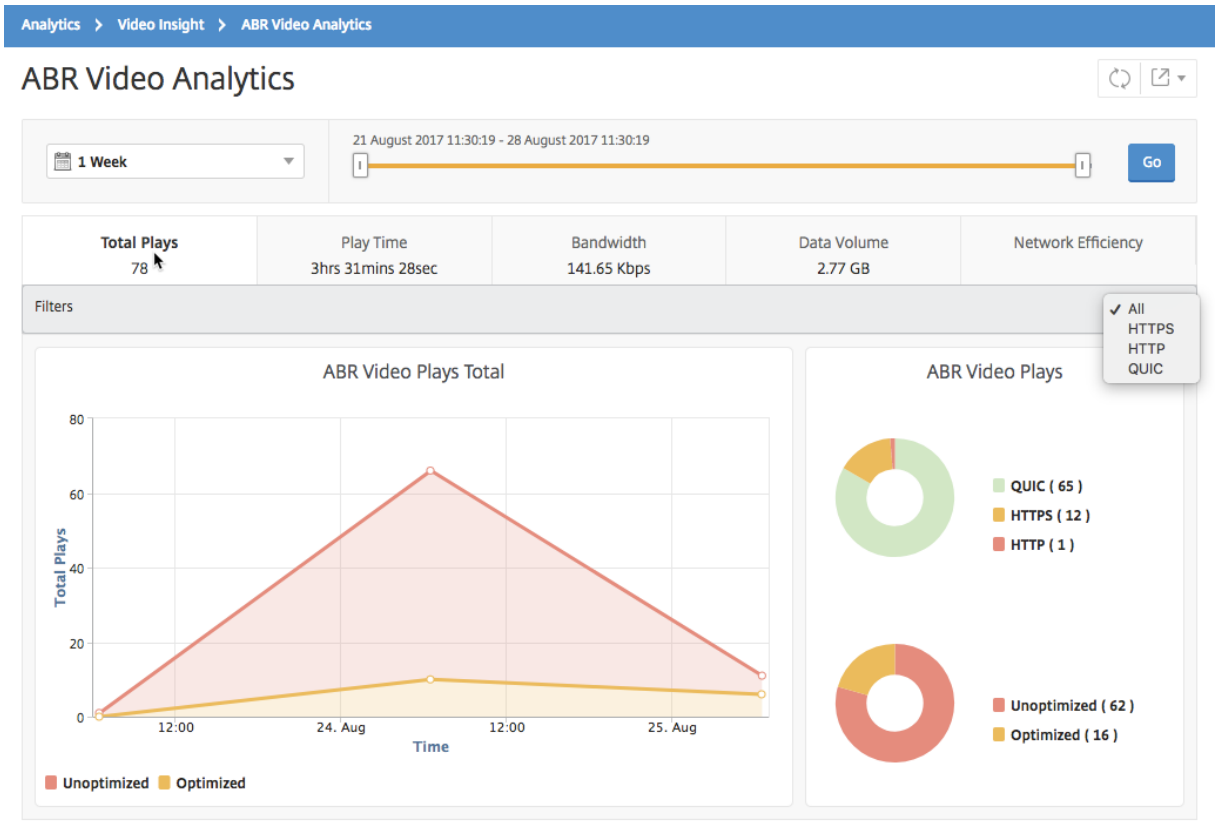
比较 **ABR** 视频的优化和未优化的播放数

February 6, 2024

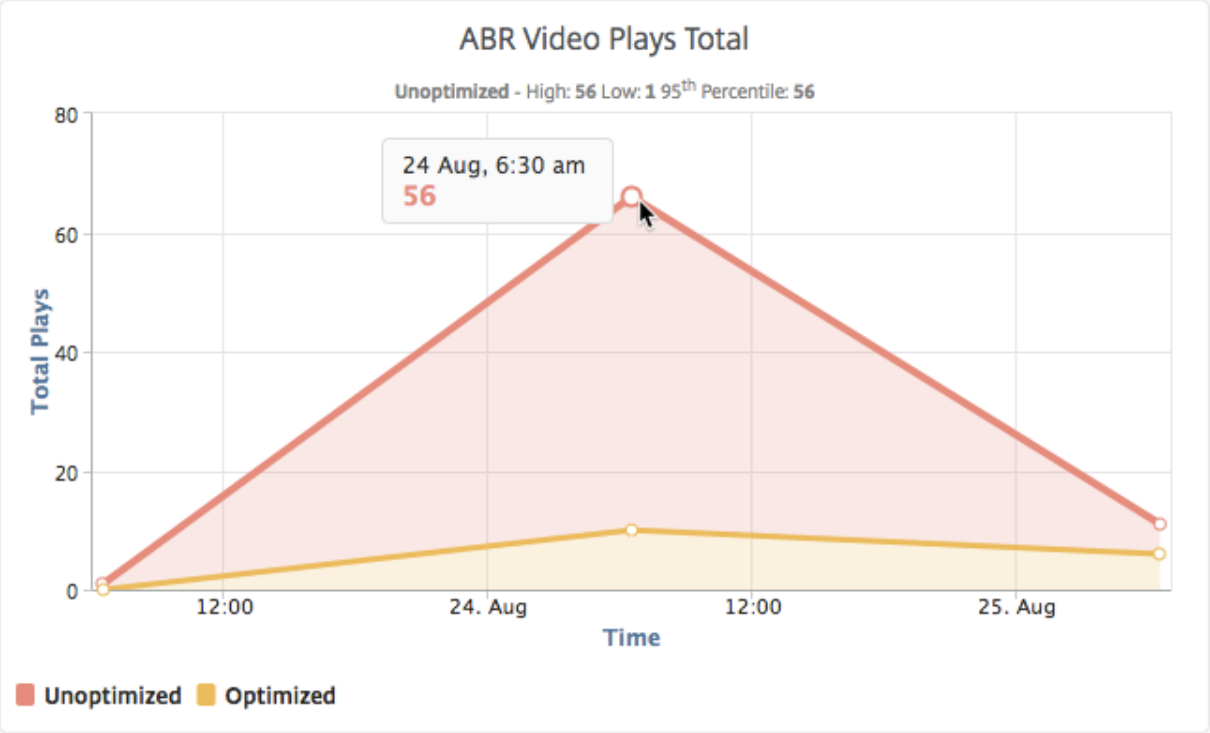
在给定时间范围内，Citrix Application Delivery Management (ADM) 会显示 ABR 视频的播放次数，并使您能够比较网络中优化和未优化播放次数。

要查看播放次数，请登录 Citrix ADM，导航到分析 **> Video Insight**，然后单击 **ABR** 视频分析。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（转到），并选择 **# of Plays**（播放数）选项卡。

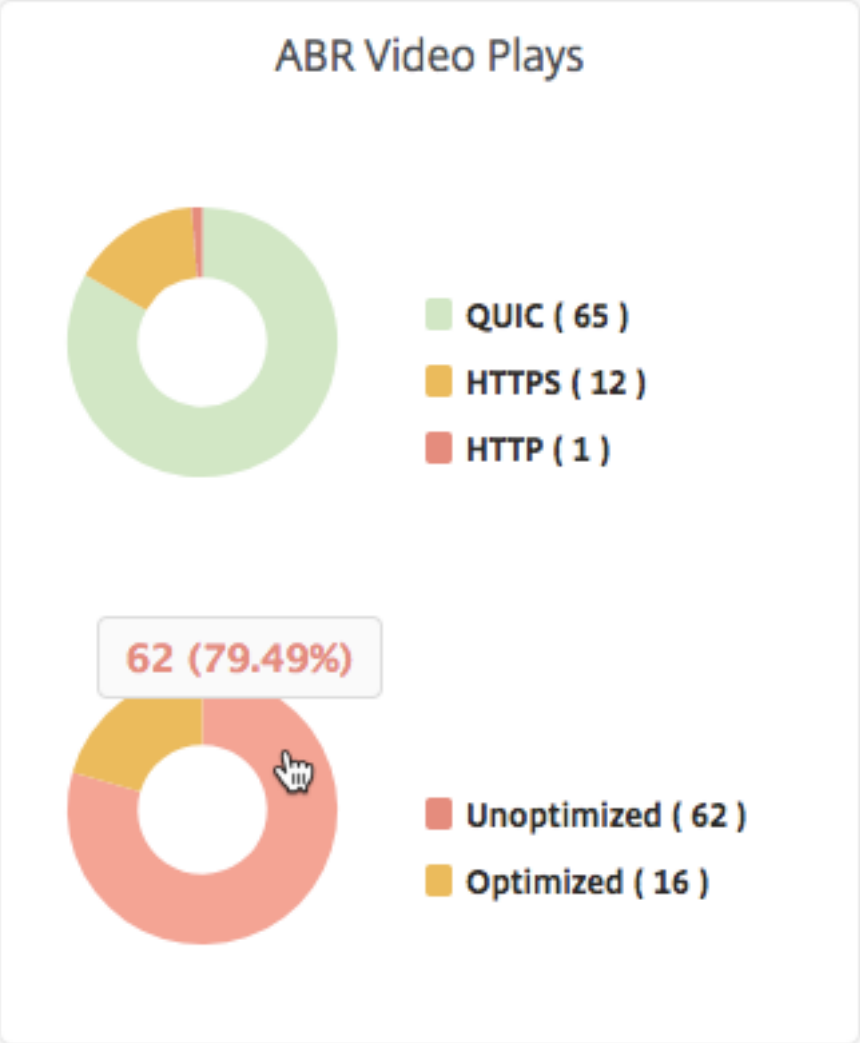
您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC ABR 视频。



# of Plays（播放数）选项卡提供折线图和饼图，描述在您的网络中 ABR 视频的播放数，以及在选定的时间范围内在您的网络中 ABR 视频的优化和未优化播放数。您可以将鼠标指针悬停在折线图上以查看特定时间范围内的播放数：



此外，您还可以将鼠标指针悬停在饼图上以显示在选定的时间范围内优化和未优化播放的百分比以及加密和未加密 ABR 视频的百分比。



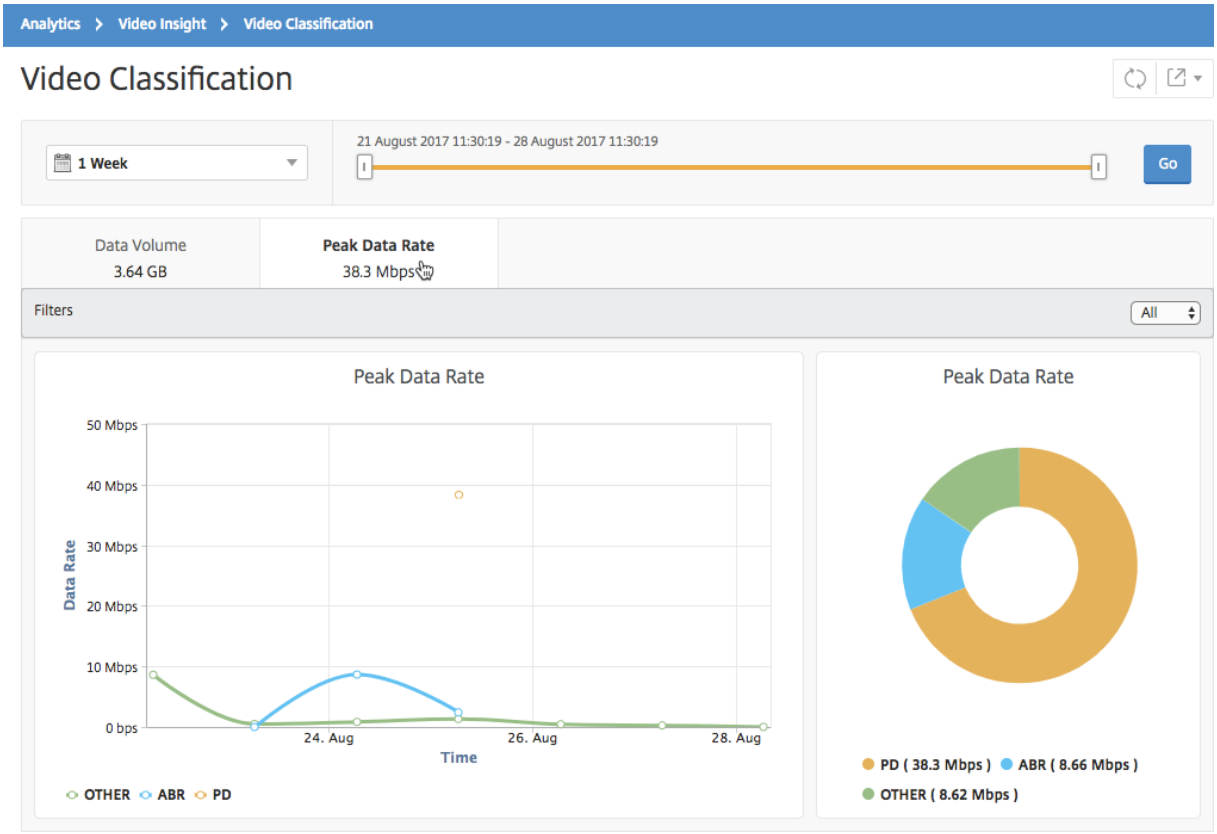
查看特定时间范围内的峰值数据速率

February 6, 2024

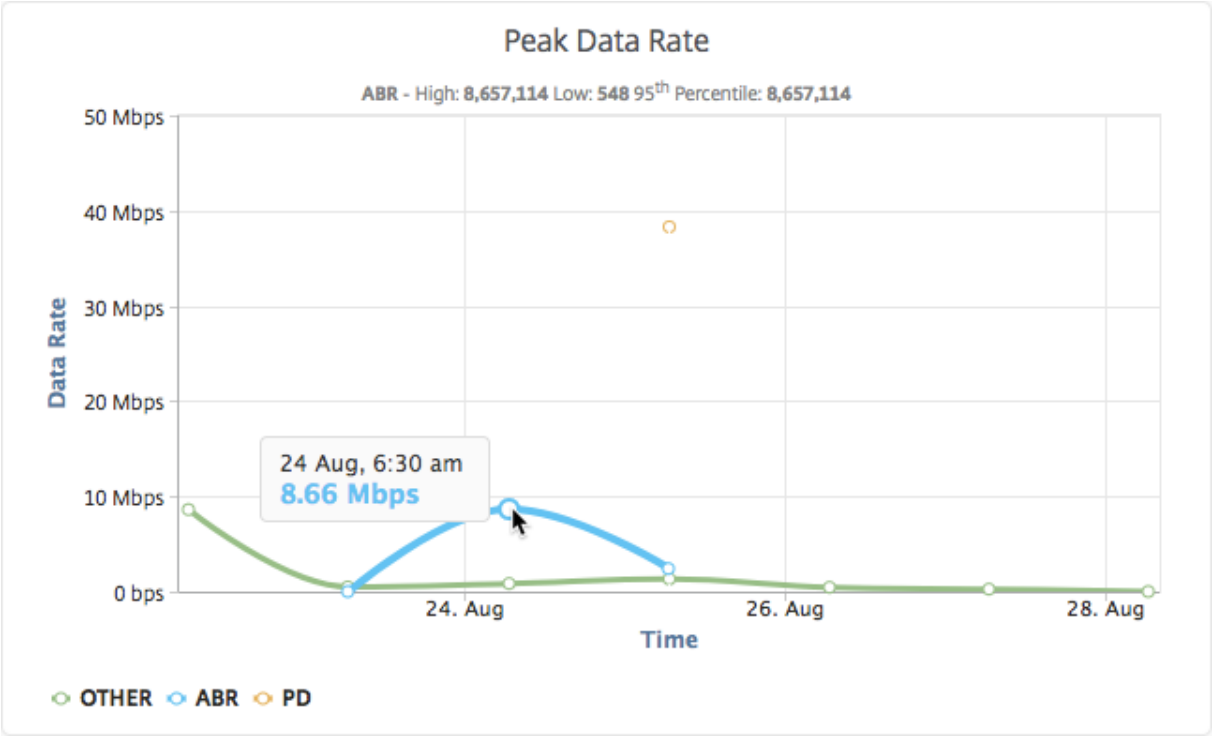
Citrix Application Delivery Management (ADM) 显示网络中视频流量的峰值吞吐量或数据速率。

要查看视频流量的峰值数据速率，请登录 Citrix ADM，导航到 **Analytics > Video Insight**，然后单击“视频分类”。然后，在右侧窗格中，从下拉列表中选择时间范围。可以使用时间范围滑块进一步自定义时间范围。单击 **Go**（继续），并选择 **Peak Data Rate**（高峰数据速率）选项卡。

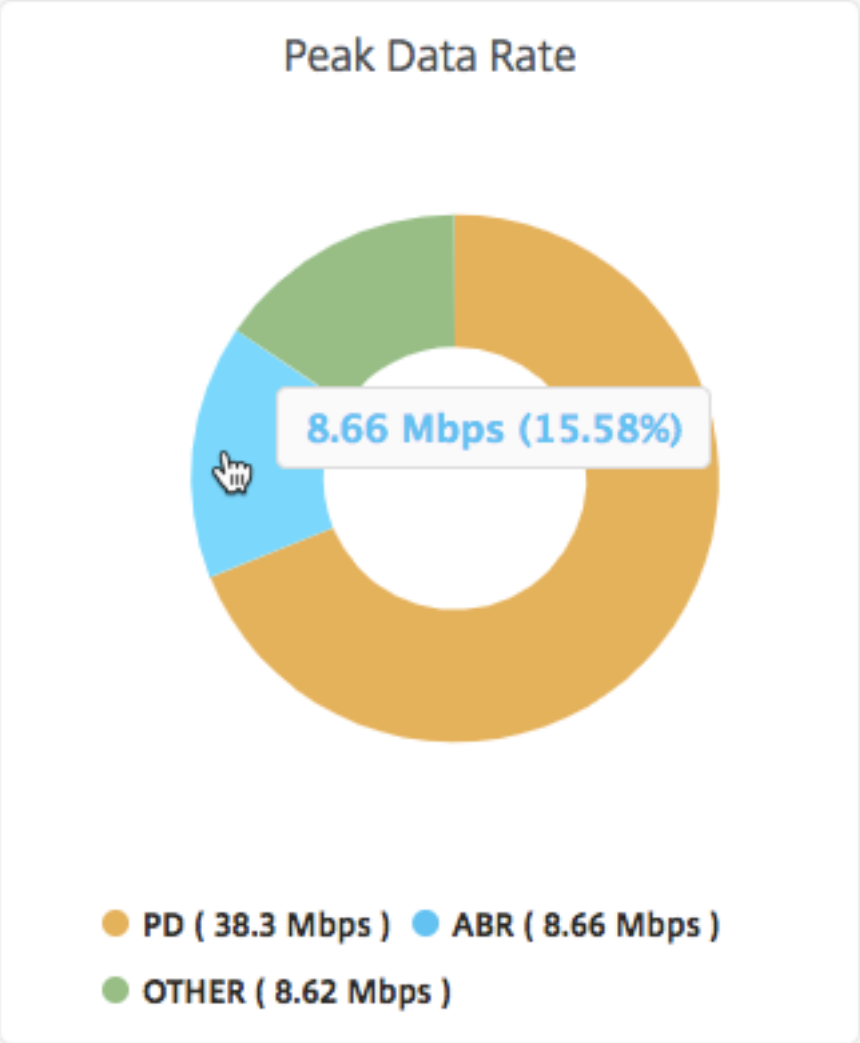
您可以使用过滤器下拉列表来选择 HTTP、HTTPS 或 QUIC 流量。



Peak Data Rate（高峰数据速率）选项卡提供折线图和饼图，显示选定时间范围内从您的网络中通过流技术推送的视频流量类型的高峰数据速率，以及您的网络中视频流量的高峰数据速率。您可以将鼠标指针悬停在折线图上以显示特定时间范围内的高峰数据速率。



此外，您还可以将鼠标指针悬停在饼图上以显示选定时间范围内通过流技术推送的视频流量类型使用的高峰数据速率的百分比。



Secure Web Gateway 分析

February 6, 2024

位于企业网络边缘的 Citrix Secure Web Gateway (SWG) 设备充当互联网代理。该设备可以在透明代理模式或显式代理模式下操作，提供拦截 Internet 流量（包括 HTTPS）的控制功能。拦截、跳过或阻止任何请求的决定是基于设备上配置的策略做出的。用户在登录企业网络之前会进行身份验证。所有请求和响应都会标记到用户，且用户活动会记录在设备中。有关更多信息，请参阅 Citrix Secure Web Gateway。

当您将 Citrix Application Delivery Management (ADM) 与 Citrix SWG 设备集成时，设备上记录的用户活动和后续记录将使用 Logstream 导出到 Citrix ADM。Citrix ADM 会整理和提供有关用户活动的信息，例如，所访问的 Web 站点和所占用的带宽。它还报告带宽使用和检测到的威胁，例如，恶意软件和钓鱼网站。您可以使用这些关键指标监视您的网络，并对 Citrix SWG 设备采取纠正措施。

要将 **Citrix SWG** 设备与 **Citrix ADM** 集成，请执行以下操作：

1. 在 Citrix SWG 设备上，在配置 Secure Web Gateway 时，启用分析并提供要用于分析的 Citrix ADM 实例的详细信息。
2. 在 Citrix ADM 中，将 Citrix SWG 设备作为实例添加到 Citrix ADM。有关更多信息，请参阅 将实例添加到 Citrix ADM。

控制板

February 6, 2024

May 24, 2018

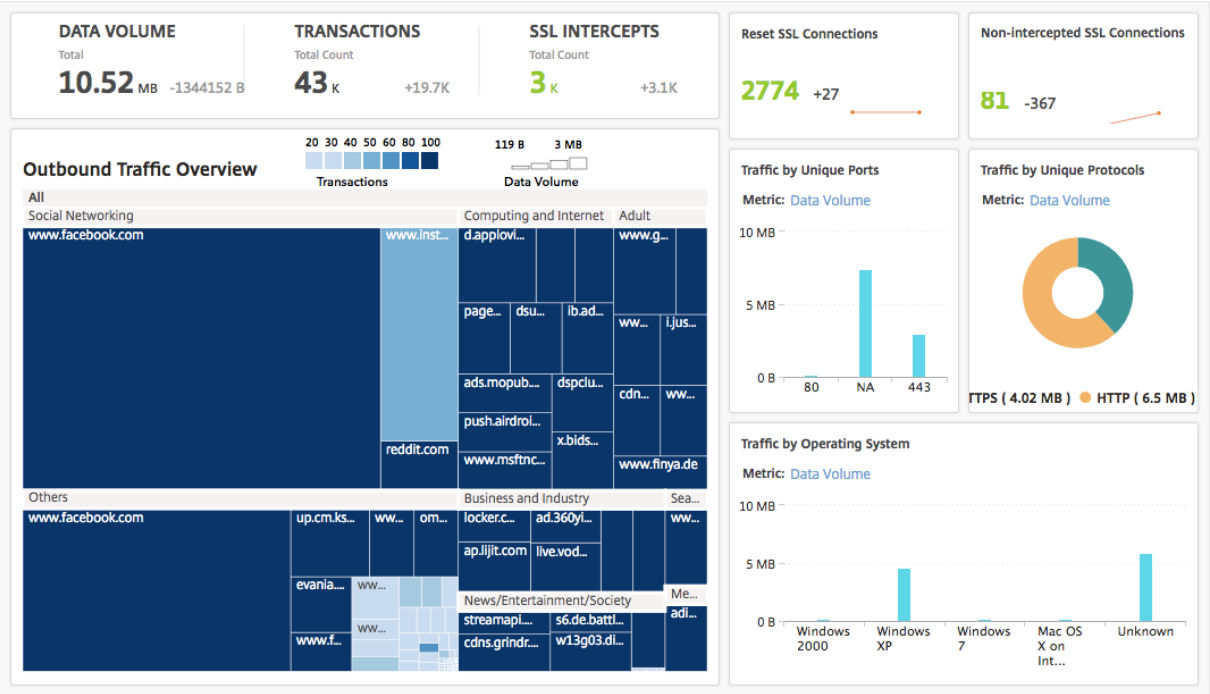
Citrix Application Delivery Management (ADM) 提供两个控制板，即出 站流量控制板 和 用户控制板。这些控制板显示多个图表，这些图表汇总了从企业网络访问的 Web 站点或应用程序，以及您的网络中的用户执行的活动。

Outbound Traffic Dashboard（出站流量控制板）

出 站流量控制面板 提供从网络访问的 URL 或域的摘要。它按事务数或 URL 或域使用的数据量提供所有 URL 或域的历史视图。
它还提供了以下详细信息：

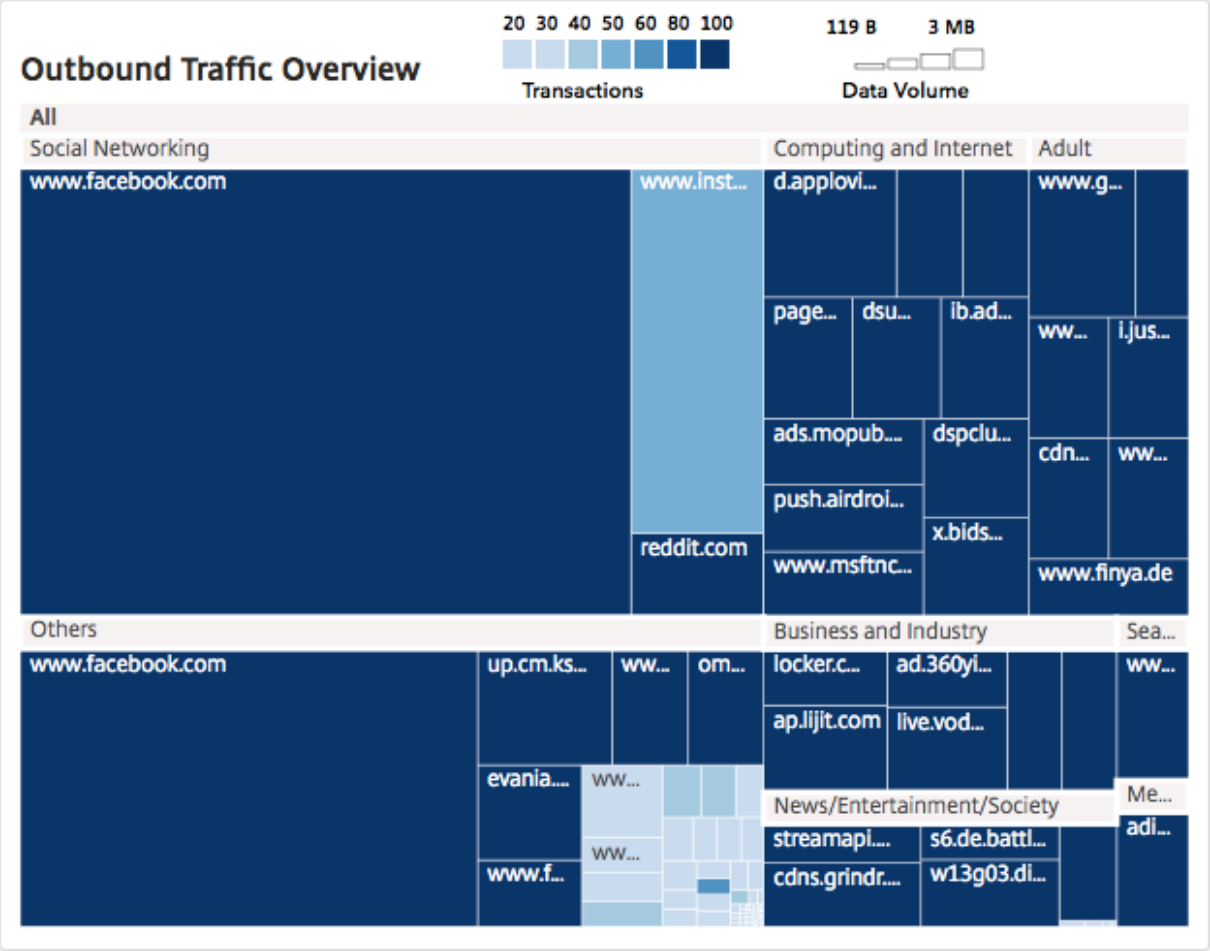
1. 从您的网络访问的 URL 或域占用的带宽量。
2. 从您的网络访问 URL 和域时发生的事务数。
3. 事务期间被 Citrix SWG 设备截获的 SSL 连接数量。
4. 事务期间未被 Citrix SWG 设备截获的 SSL 连接的数量。
5. 事务期间由 Citrix SWG 设备重置的 SSL 连接数量。
6. 传输的 Web 流量，基于用于传输流量的端口、Web 流量使用的协议以及用于传输流量的客户端操作系统。

要访问出站流量控制面板，请导航到应用程序 **>** 出站流量控制面板。



查看来自网络的出站流量

出站流量控制面板包括出站流量概述窗格。在“出站流量概览”窗格中，Citrix ADM 将访问的 URL 或域分为几类，例如购物、新闻、社交网络等。出 站流量概述 窗格将从您的网络访问的 URL 或域显示为 URL 类别中的节点。节点的大小对应于访问 URL 或域时使用的数据量。节点的颜色指示访问 URL 或域时发生的事务数。



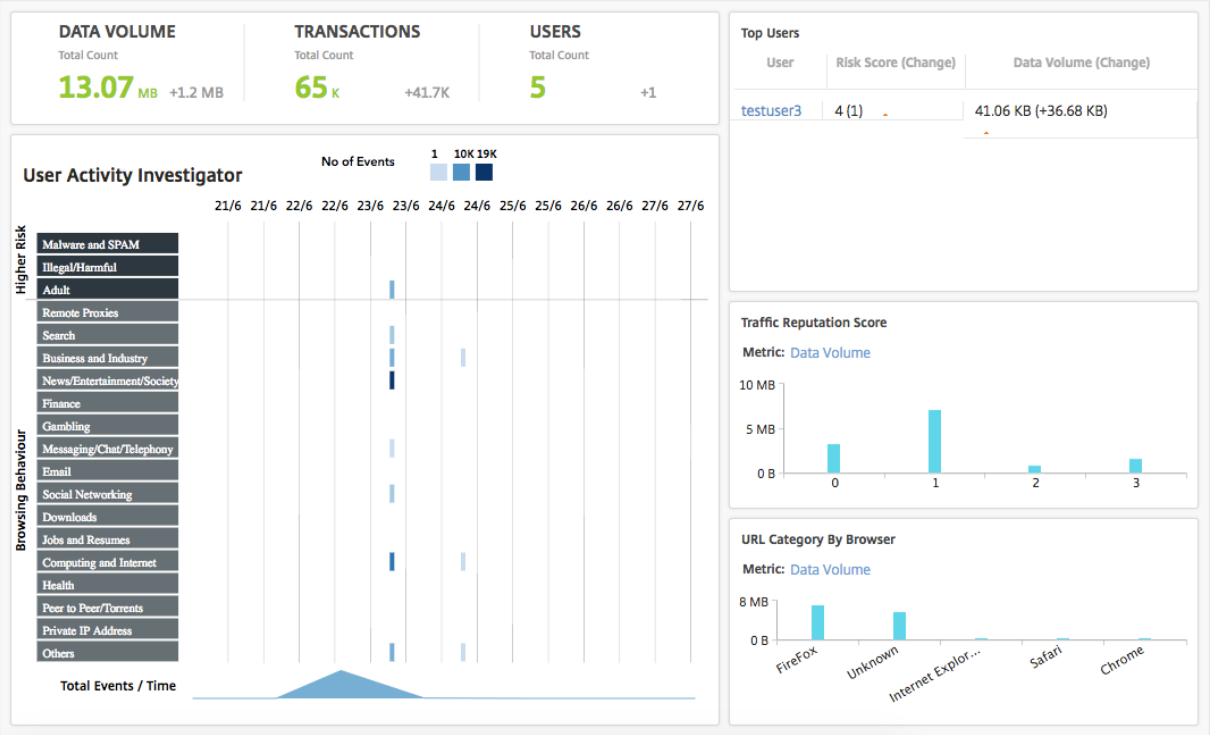
您可以单击某个类别来过滤图表，以显示指定时间范围内与该类别相关的详细信息。

User Dashboard（用户控制板）

用户控制板显示企业中用户执行的活动的摘要。它提供一些主要指标，可以用来确定以下内容：

1. 您企业中的用户的浏览行为。
2. 您企业中的用户访问的 URL 类别。
3. 排名前五位的用户，基于其风险得分和其占用的带宽。有关风险评分的详细信息，请参阅“风险评分”。
4. 用于访问 URL 或域的浏览器。
5. 用户生成的 Web 流量，基于流量信誉得分。

要访问用户控制板，请导航到用户 **>** 控制板。

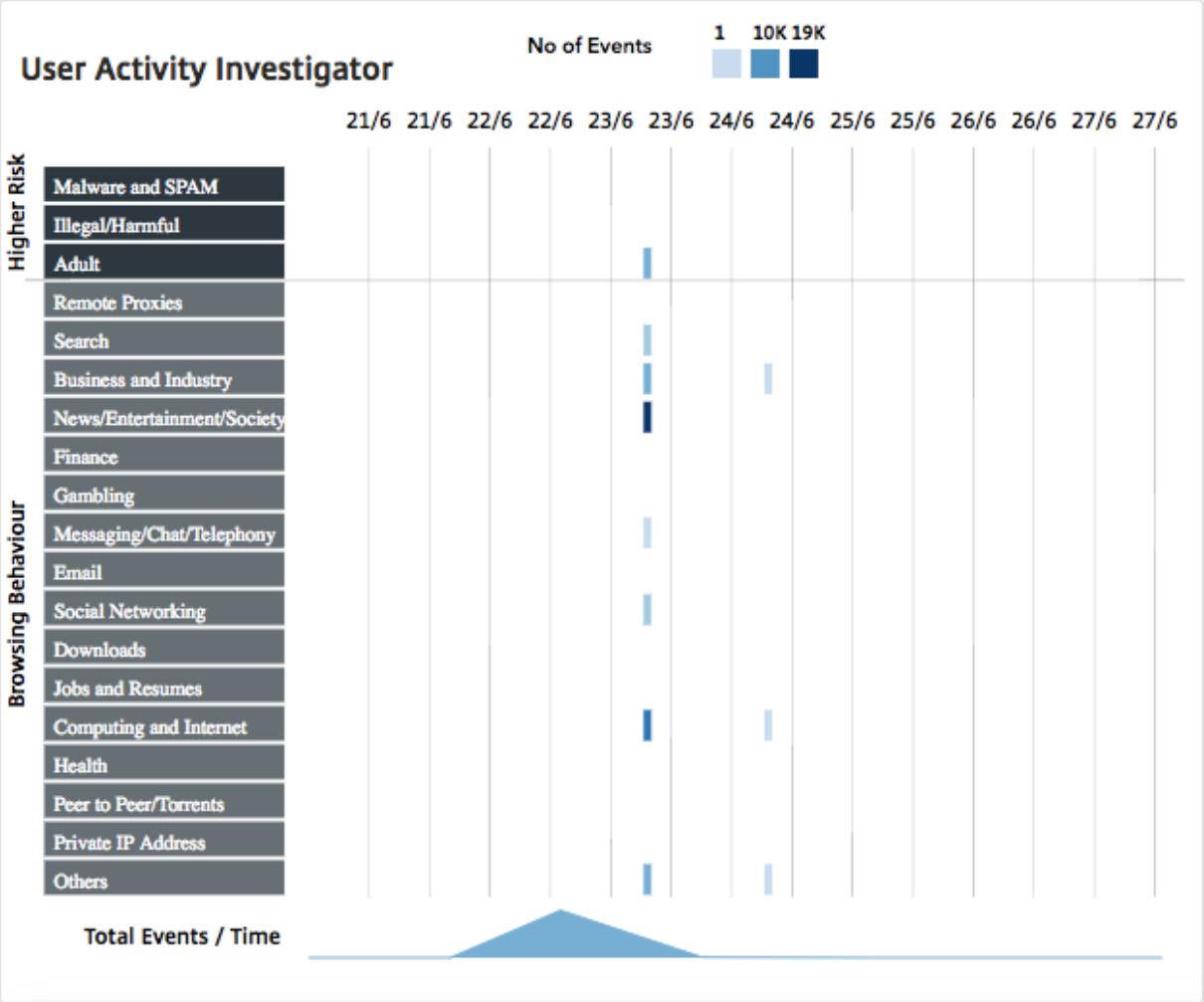


您可以在“顶级用户”窗格中单击某个用户 来筛选图表，以显示该用户在指定时间范围内执行的 Web 活动的详细信息。

User Activity Investigator（用户活动调查器）

用户控制板包括一个用户活动调查器窗格，显示用户执行的各种 Web 活动。它显示在选定的时间范围内用户访问的 URL 类别，以及每个 URL 类别触发的各种事件。您可以单击事件获取事务级别详细信息。

用户活动调查器按 URL 类别显示关键信息，例如用户的浏览行为、用户的高风险活动以及触发的事件。事件以矩形图形式显示在图表中。如果选定的持续时间是一小时，则每个图例以一分钟的时间间隔进行汇总，如果选定的持续时间是一天，则每个图例以一小时的时间间隔进行汇总。



这些图例会进行汇总，并按照发生的事件数进行颜色编码。可以将鼠标指针悬停在图例上来显示选定图例的详细信息，例如，时间和汇总的事件数。可以从时间段下拉框中选择时间来自定义图的时间段。

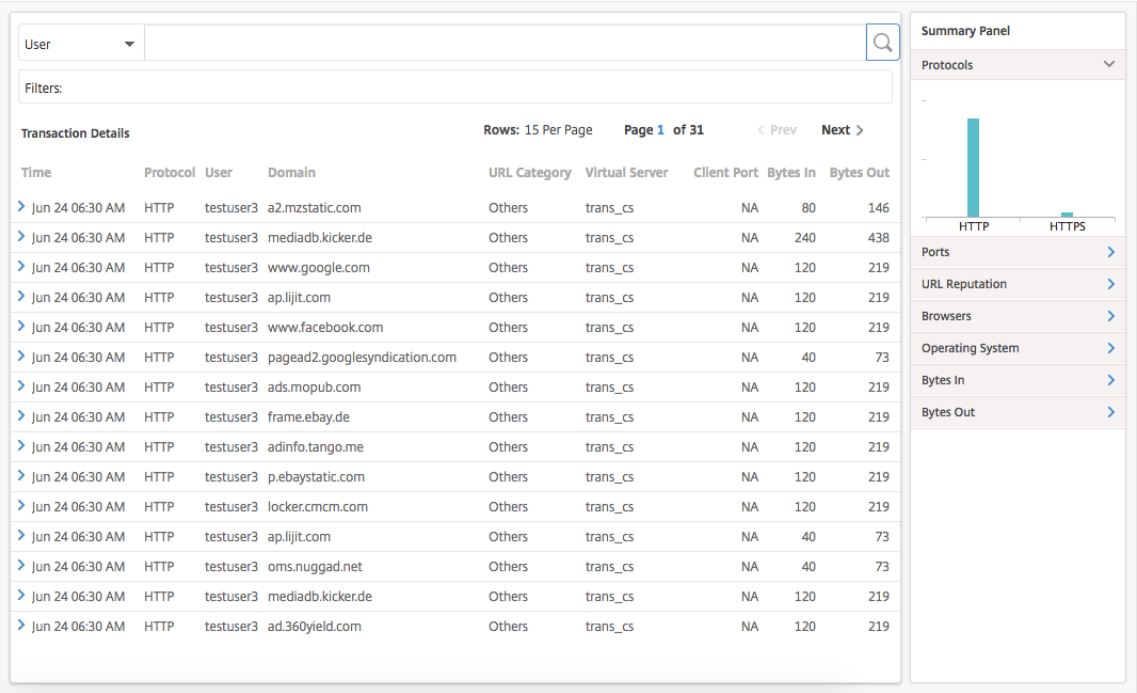
您可以单击事件以进一步深入查看，了解事务的详细信息。

User Transactions（用户事务）

“User Transactions”（用户事务）页面显示您网络中的用户事务的详细信息。它提供事务级别详细信息，例如：

1. 事务的发生时间
2. 用于事务的协议
3. 用户名
4. 用户访问的域
5. URL 类别
6. 用于拦截事务的代理服务器

7. 客户端端口详细信息
8. 输入字节数
9. 输出字节数



Summary Panel（摘要面板） 摘要面板 显示事务 详细信息窗格中显示的所有事务 指标。此面板允许您通过选择或取消选择指标在“事务详情”窗格中对事务进行排序和查看。摘要面板 显示以下指标：

指标	说明
协议	事务中使用的协议
端口	用于事务的端口
URL 信誉	URL 信誉评分
浏览器	用于事务的浏览器
操作系统	用于事务的操作系统
输入字节数	通过 Citrix SWG 设备接收的数据量。
输出字节数	通过 Citrix SWG 设备发送的数据量。

风险评分

风险评分是 Citrix ADM 中用于确定与企业中用户相关的风险的评分系统。Citrix ADM 根据 Citrix SWG 设备为网络中用户访问的 URL 分配的 URL 信誉分数分配风险分数。有关 URL 信誉评分的信息，请参阅 URL 信誉得分。下表描述了 Citrix ADM 分配的风险评分。

风险评分	说明
1	用户的 Web 活动没有发现威胁或没有异常。
2	用户的 Web 活动没有发现威胁或没有异常，但用户正在访问没有 URL 信誉分数的“未知站点”。
3	在用户的 Web 活动未检测到威胁，但用户尝试访问的站点潜在易受攻击或与潜在易受攻击的站点关联。
4	潜在易受害的用户。
5	用户的 Web 活动异常，用户已访问已知的恶意站点。

用例

February 6, 2024

监视 **SSL** 拦截

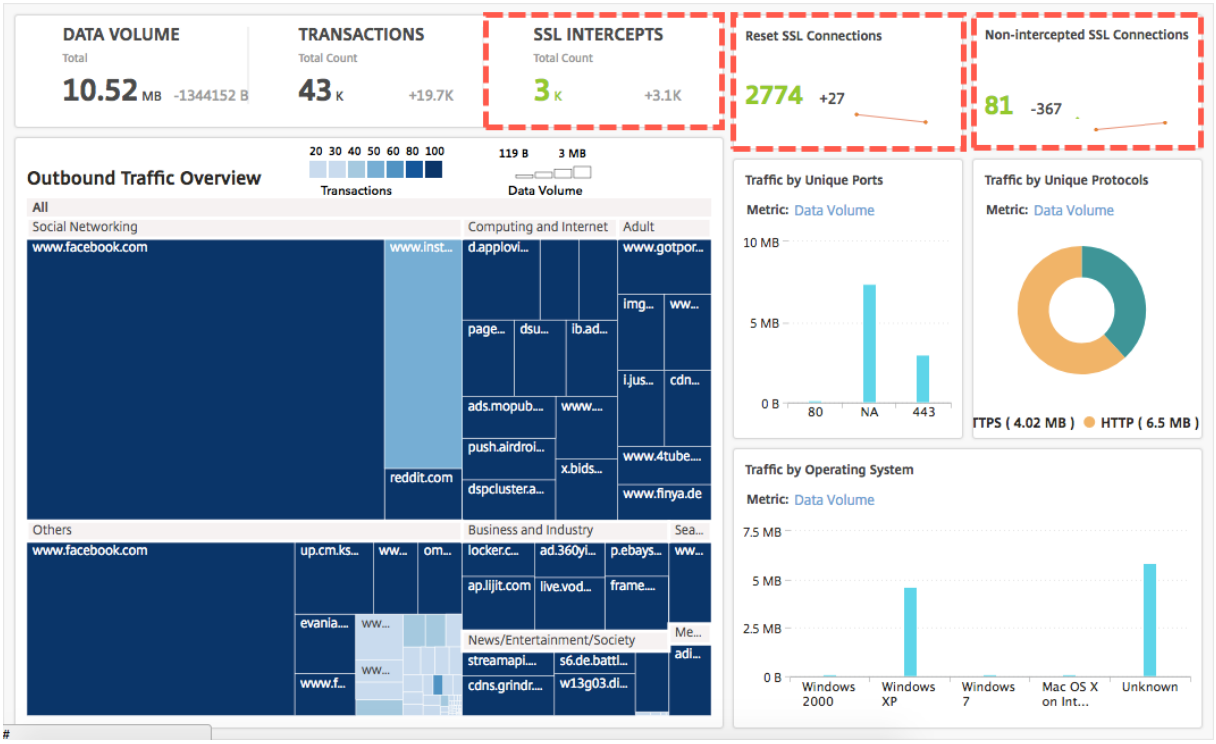
Citrix SWG 设备使您能够检查加密的出站流量。您可以根据设备上配置的策略拦截、跳过或阻止任何 HTTPS 请求。Citrix Application Delivery Management (ADM) 提供了有关所选时间范围内 出站流量控制板 中 SSL 连接的以下详细信息：

- Citrix SWG 设备拦截、未拦截和重置的 SSL 连接的数量
- SSL 连接的事务详细信息

使用这些详细信息，您可以进一步微调 Citrix SWG 设备上的策略，以有效地检查加密的出站流量。有关更多信息，请参阅 Citrix Secure Web Gateway。

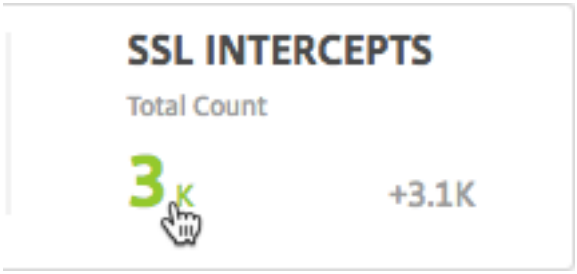
要显示拦截、未拦截和重置的 **SSL** 连接数，请执行以下操作：

导航到应用程序 **>** 出站流量控制面板。“Outboard Traffic Dashboard”（出站流量控制板）将显示拦截、未拦截和重置的 SSL 连接数。

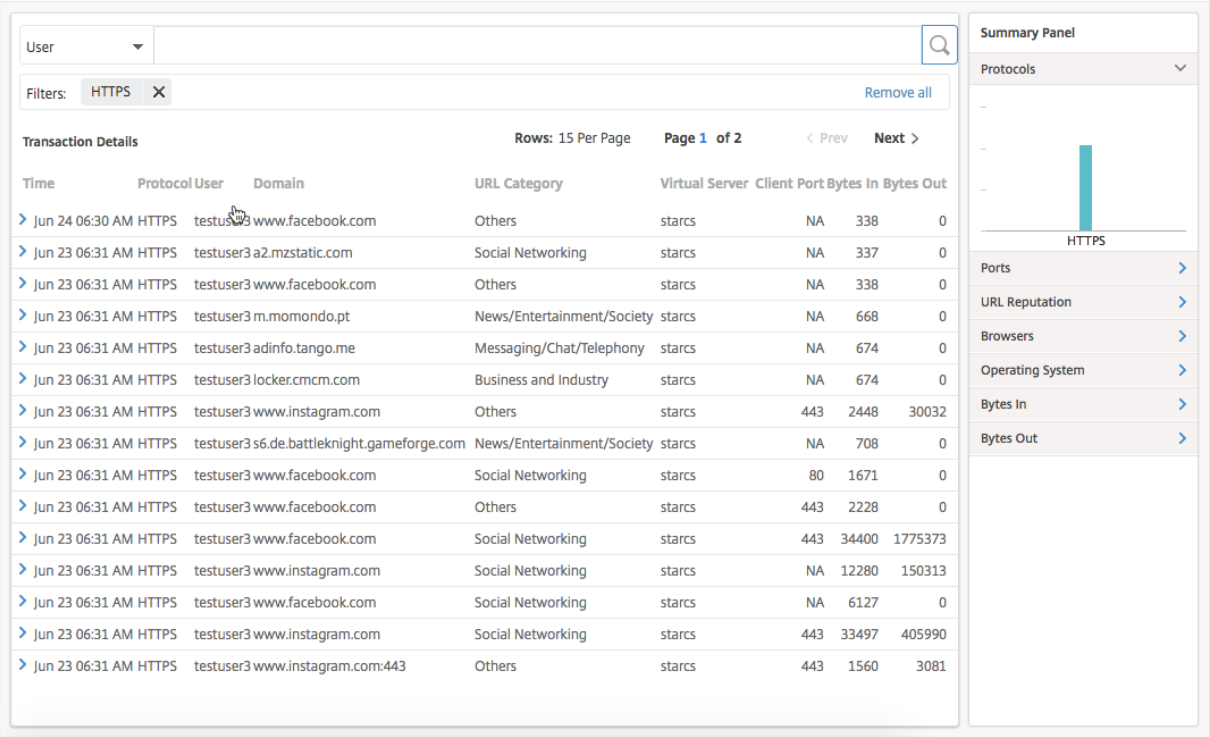


要显示拦截的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **SSL INTERCEPTS**（SSL 拦截）部分中的总计数。



在选定时间范围内拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。

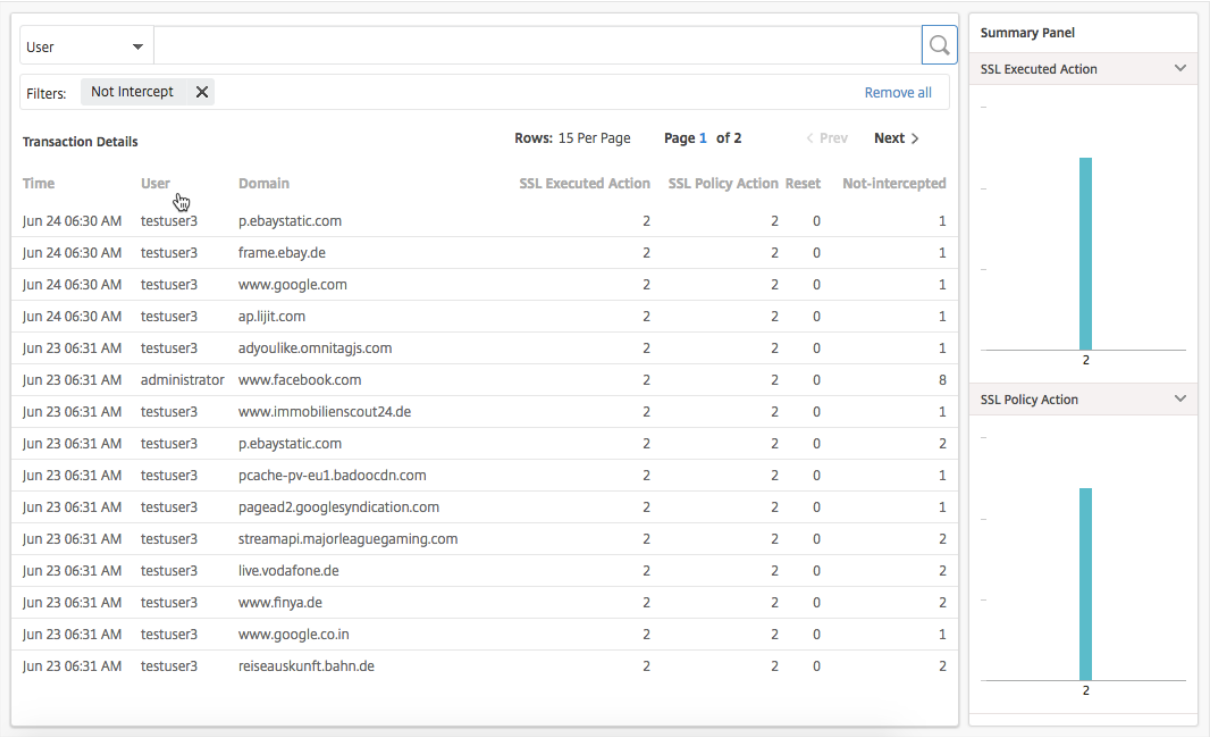


您可以进一步按用户和 URL 类别过滤事务详细信息。

要查看未拦截流量的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **Not-intercepted SSL Connections**（未拦截 SSL 连接）部分中的总计数。

在选定时间范围内流量未被拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。

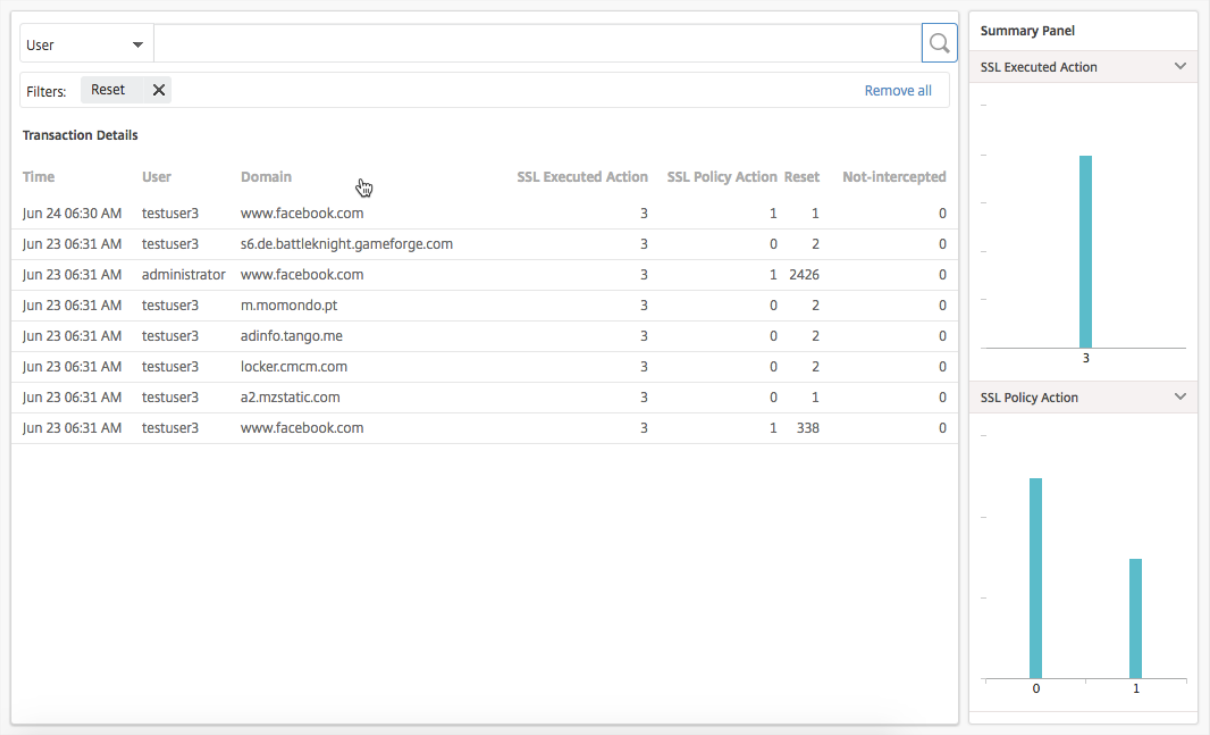


您可以进一步按用户和 URL 类别过滤事务详细信息。

要显示已重置的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **Reset SSL Connections**（重置 SSL 连接）部分中的总计数。

在选定时间范围内流量未被拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。



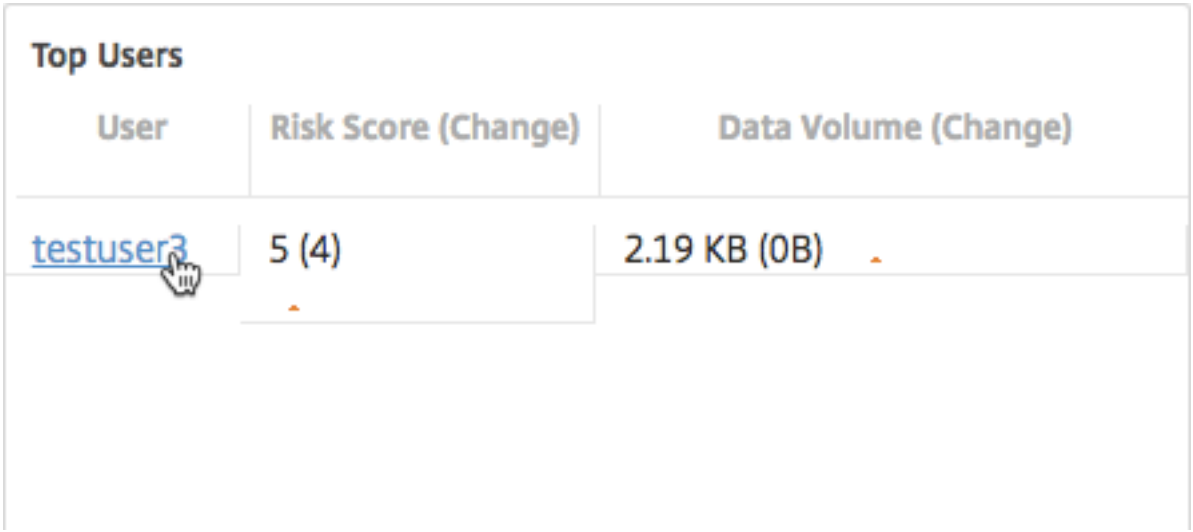
您可以进一步按用户和 URL 类别过滤事务详细信息。

检查端点

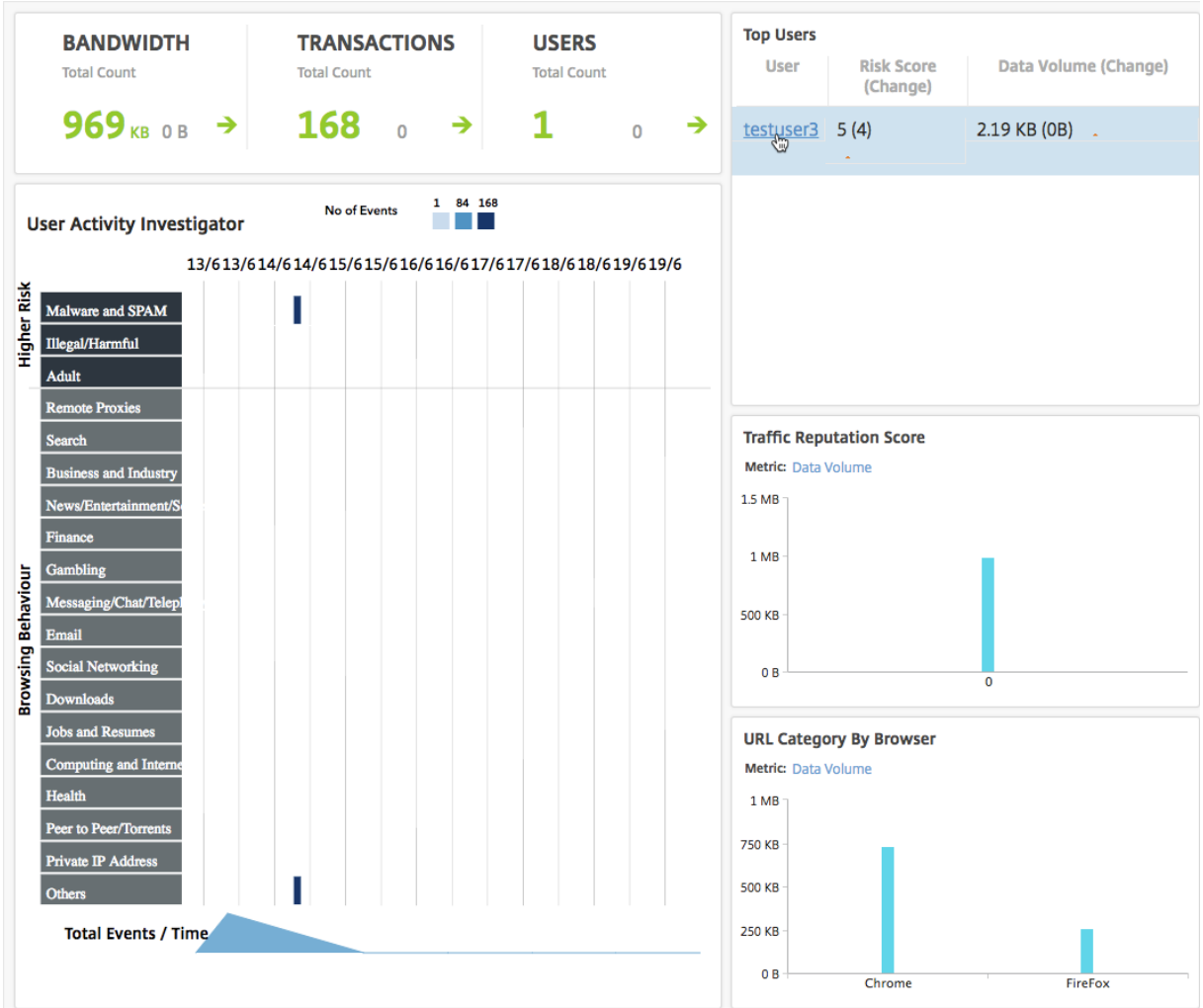
您在 Citrix SWG 设备上配置的策略指定设备如何记录企业中执行的所有用户活动。Citrix ADM 提供了关键指标，可用于确定：

1. 您企业中的用户的浏览行为。
2. 您企业中的用户访问的 URL 类别。
3. 排名前五位的用户，基于其风险得分和其占用的带宽。有关风险评分的更多信息，请参阅 风险评分。
4. 用于访问 URL 或域的浏览器。
5. 用户生成的 Web 流量，基于流量信誉得分。

例如，如果用户 ID 为 testuser3 的用户经常访问企业中与恶意软件相关的站点，则 Citrix ADM 会将该用户识别为高风险活动用户并分配更高的风险得分。testuser3 信息显示在 用户控制板的顶级用户 部分。



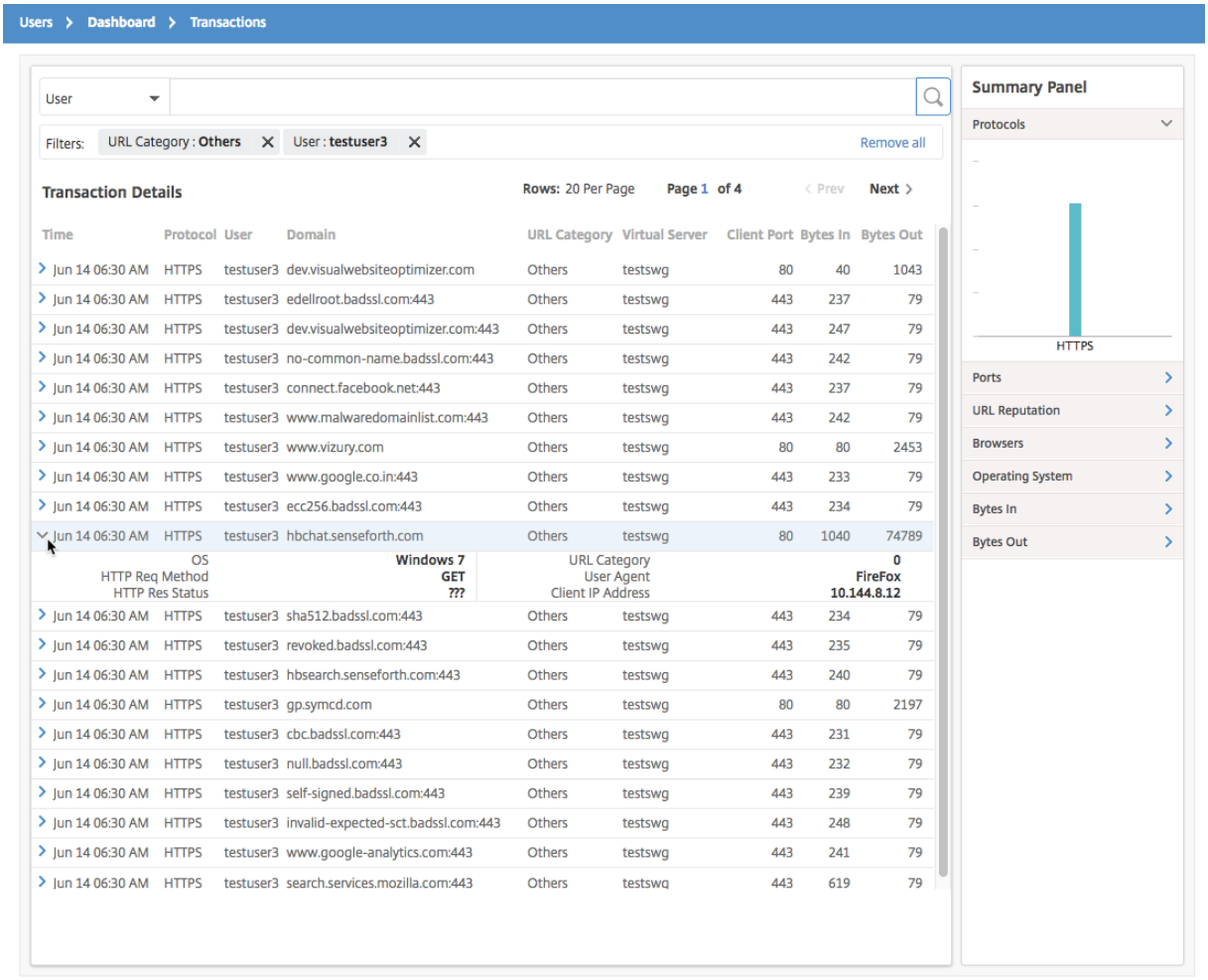
您可以单击 testuser3 来筛选用户控制面板，以显示与 testuser3 相关的所有关键指标。



在 **User Activity Investigator**（用户活动调查器）窗格中，testuser3 的高风险活动以各自 URL 类别中的事件形

式显示。

您可以悬停在事件上以显示事件数，并且您可以单击事件以调查在出现事件期间发生的事务。

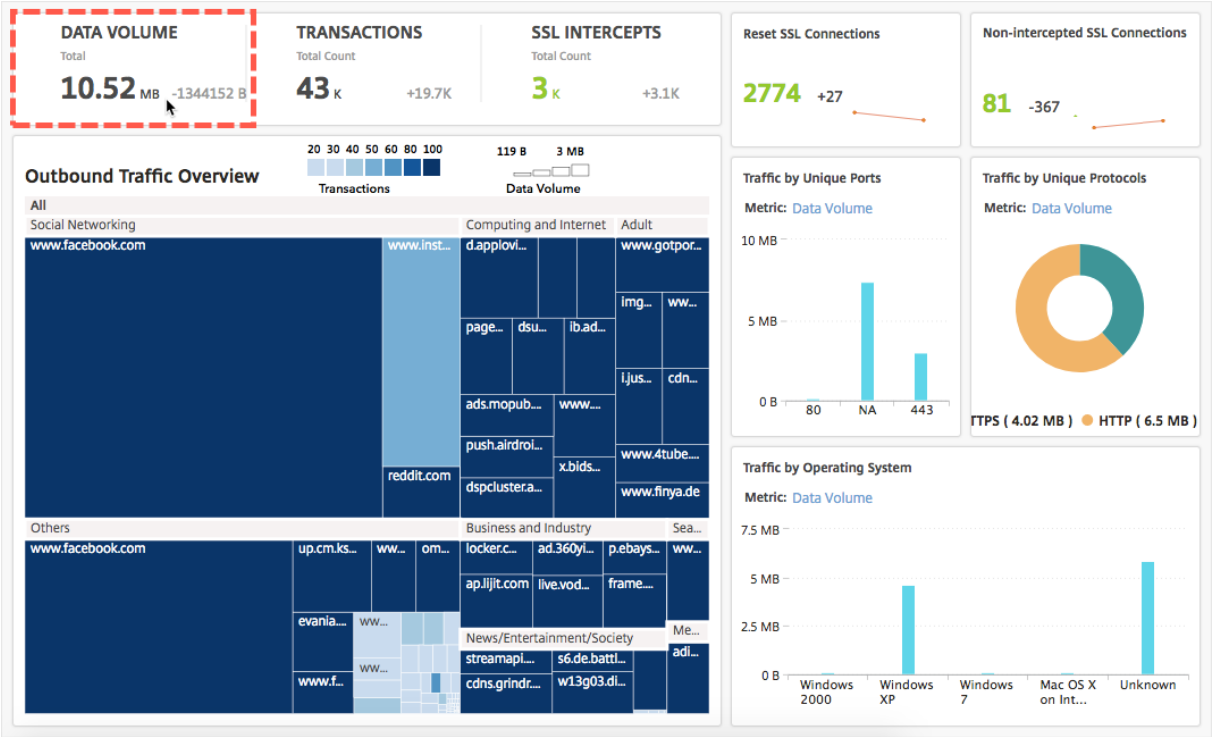


利用这些信息，您可以确定用户的系统是否受恶意软件感染，也可以了解用户的带宽消耗模式并微调您的 Citrix SWG 策略。有关更多信息，请参阅 Citrix Secure Web Gateway 文档。

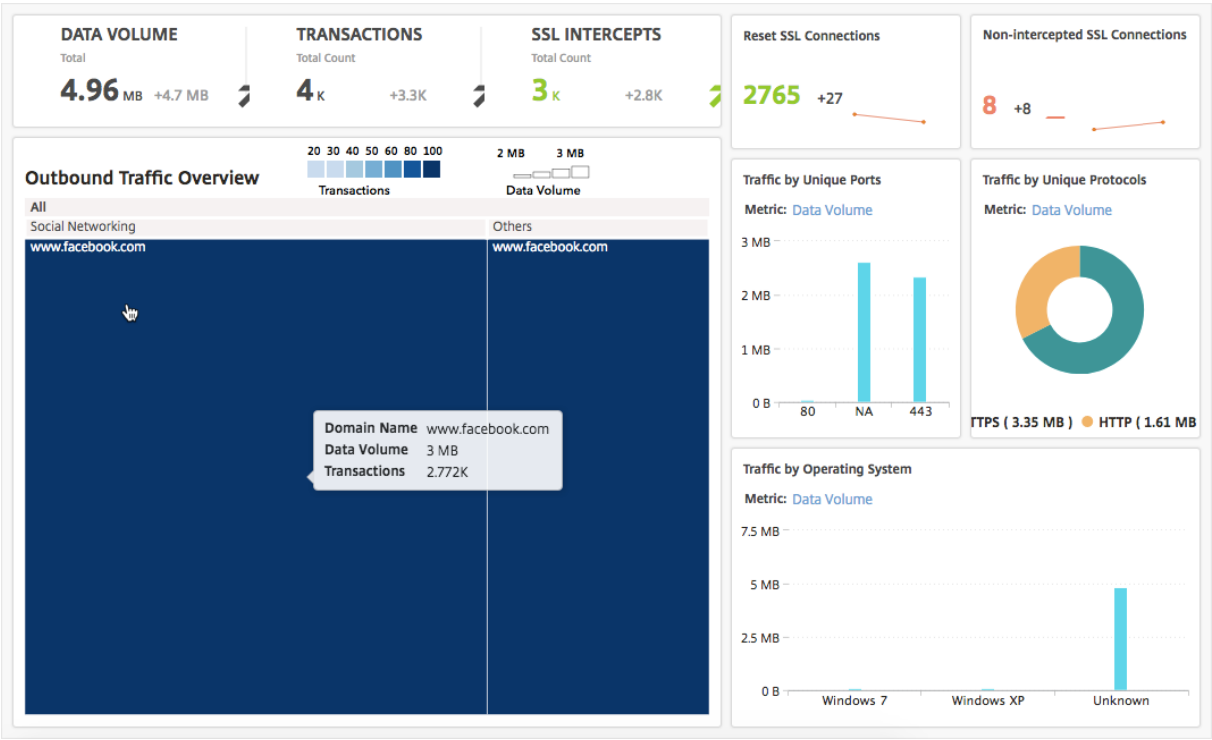
报告带宽占用量

Outbound Traffic Dashboard（出站流量控制板）和 **User Dashboard**（用户控制板）显示多个图表，这些图表汇总了从企业网络访问的 Web 站点或应用程序，以及您的网络中的用户执行的活动。

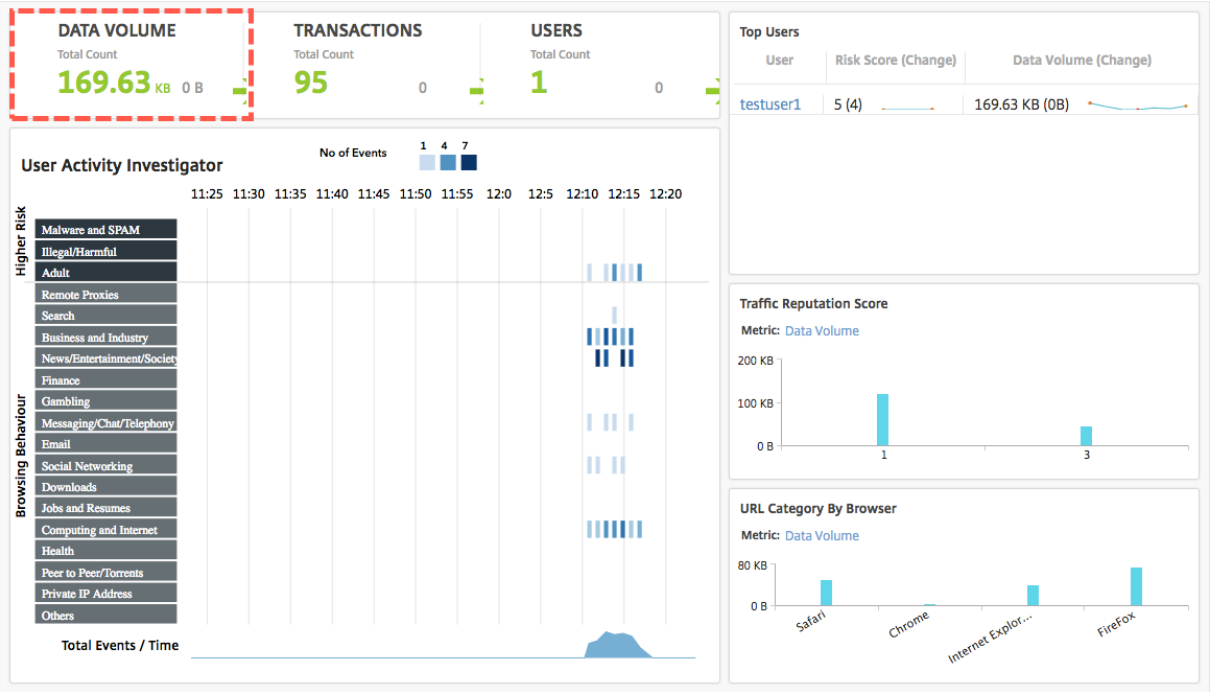
出 站流量控制面板 提供从您的网络访问的 URL 或域名的数据量消耗的详细信息。导航到 **Applications**（应用程序）**> Outbound Traffic Dashboard**（出站流量控制板），其中数据量详细信息显示在 **Data Volume**（数据量）部分中。



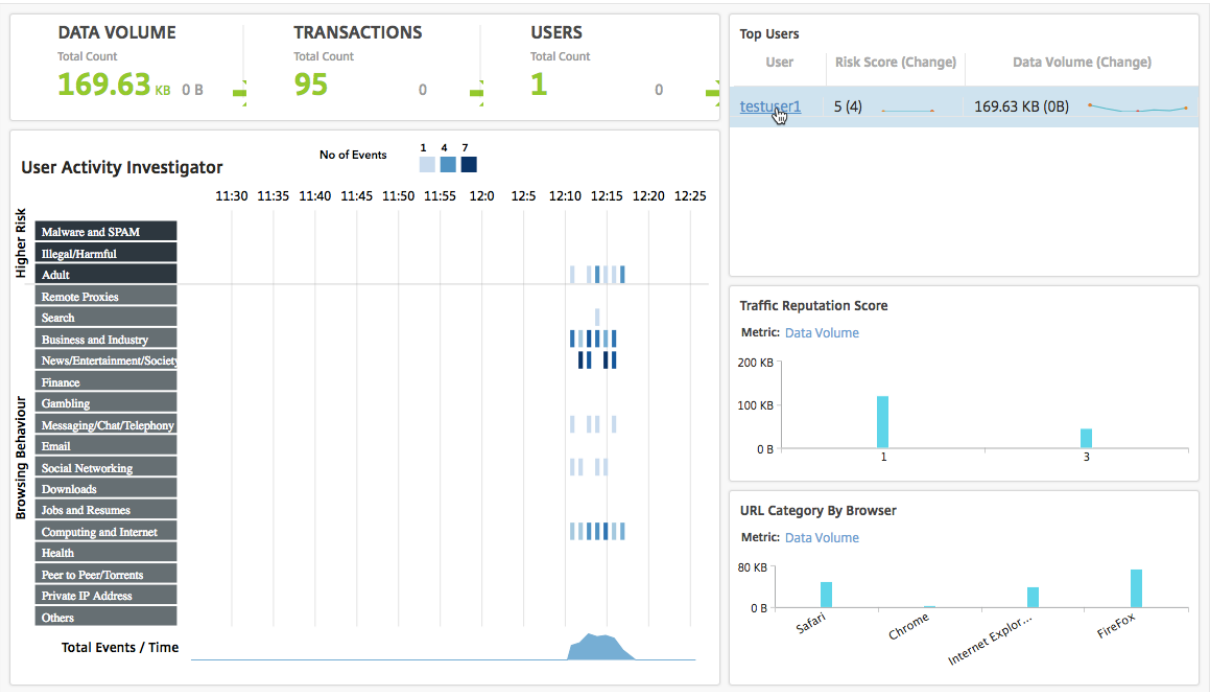
在“出站流量概览”窗格中，您可以单击域或 URL 来显示该域或 URL 消耗的数据量的详细信息。



User Dashboard（用户控制板）提供了有关您网络中的用户占用的带宽的详细信息。导航到 **Users**（用户）> **Dashboard**（控制板）以在 **User Dashboard**（用户控制板）的 **DATA VOLUME**（数据量）部分中显示用户占用的带宽的详细信息。



您可以从 **Top Users**（排名前几位的用户）部分选择用户来查看该用户占用的带宽的详细信息。**DATA VOLUME**（数据量）部分和图表中的其他主要指标将按选定用户过滤。



通过使用这些详细信息，您可以了解带宽占用量和占用的原因。例如，如果用户正在访问社交网站并且这造成了大量带宽消耗，则管理员可以访问 Citrix SWG 设备并配置 URL 列表功能来控制对网站的访问。有关更多信息，请参阅 使用案例：使用自定义 URL 集筛选 URL 主题。

查看出站流量分布

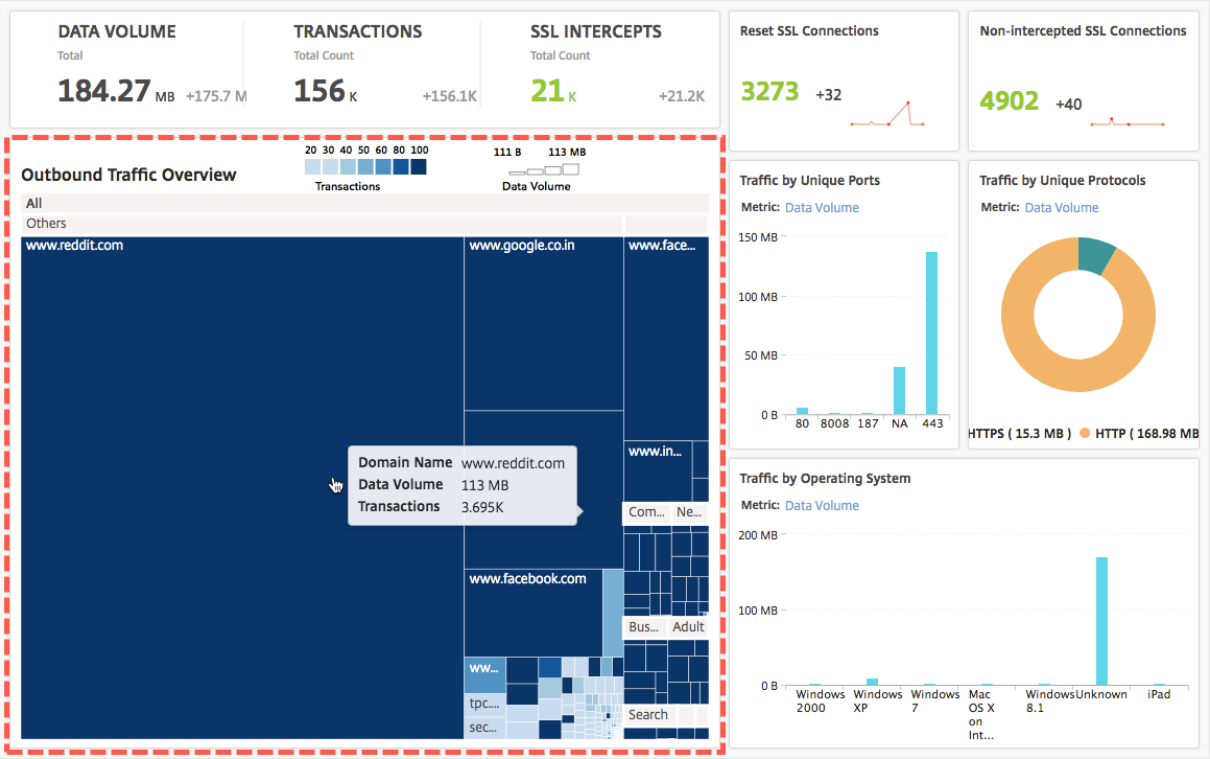
Citrix SWG 设备提供 URL 分类和筛选功能，您可以使用这些功能对从您的网络访问的 URL 进行分类。在 Citrix ADM 中，出站流量控制面板包括出站流量概览窗格。在 **Outbound Traffic Overview**（出站流量概览）窗格中，Citrix ADM 将访问的 URL 或域分组为不同类别（例如，Shopping（购物）、News（新闻）、Mobile（移动）等）以显示您网络中的出站流量分布。对于选定的时间范围，您可以单击 URL 以了解：

1. 访问该 URL 占用的带宽
2. 访问该 URL 时发生的事务
3. 访问该 URL 时拦截、未拦截和重置的 SSL 连接数

通过此信息，您可以了解出站流量模式并制定更正决策，例如，是否阻止特定 URL。

要查看出站流量分布：

导航到应用程序 **>** 出站流量控制面板。外部流量控制面板 在“出站流量概览”窗格中显示 URL：



如果您要查看特定 URL 的详细信息，请选择该 URL。

通过使用此信息，您可以了解出站流量模式，以及使用在您的 SWG 设备上配置的 URL 过滤器控制您的网络流量。有关更多信息，请参阅 URL 过滤。

调配

February 6, 2024

在软件定义网络连接 (SDN) 中，软件应用程序控制器管理网络及其活动，而不是管理支持网络的硬件。也就是说，SDN 允许网络管理员使用基于软件的集中式管理工具将物理网络连接虚拟化为逻辑网络连接并管理网络服务。SDN 让网络工程师和管理员可以快速响应不断变化的业务要求。

SDN 比较有名的优势是流量可编程性、更大的灵活性、创建策略驱动的网络监督能力以及实施网络自动化，下面列出了 SDN 一些特别的优势：

- 集中式网络置备
- 将网络安全性提高到粒度级
- 降低了运行成本
- 提高了云提取的级别
- 保证了内容交付
- 缩短了网络停机时间

Citrix Application Delivery Management (ADM) 通过集成不同供应商的 SDN 控制器，支持在企业网络中使用 SDN。Citrix ADM 支持 VMware NSX Manager 和 Cisco 应用程序策略基础结构控制器 (APIC)。

VMware NSX Manager

Citrix ADM 与 VMware 网络虚拟化平台集成，以实现 Citrix ADC 服务的部署、配置和管理的自动化。此集成消除了与物理网络拓扑关联的传统复杂性，从而让 vSphere/vCenter 管理员能够以程序化方式更快地部署 Citrix ADC 服务。

VMware NSX Manager 呈现逻辑防火墙、交换机、路由器、端口及其他网络连接元素，从而能够在各种虚拟机管理程序、云管理系统和关联的网络硬件之间构成虚拟网络连接。此外，它还支持外部网络连接和安全服务。

通过 Citrix ADM 的云调配功能可以将 Citrix ADC 产品与 VMware NSX 集成，并提供以下功能：

- 能够在服务插入过程中将预置备的 VPX 按需分配给特定 Edge 网关。
- 能够通过在 NSX 环境内运行的实例上的应用程序模板配置 Citrix ADC 的高级功能（如 SSL 和 CS）以及基本负载平衡。
- 能够在服务删除过程中从特定 Edge 网关取消分配 VPX，并为另一个 Edge 网关重新分配同一 VPX。
- 能够从 vCenter 控制台快速部署 Citrix ADC 功能，作为应用程序所需的所有基础架构的部署工作流程的一部分。

优势：

- 在应用程序部署工作流中，自动按需分配新 ADC 服务
- 通过应用程序模板，简化了应用程序特定的高级 ADC 功能的配置
- 多租户职责分离和自助服务使用模型，同时为云管理员提供单一控制点
- 更轻松地与 Citrix ADM API 集成，这有助于支持意外的未来使用。

有关如何在 Citrix ADM 上配置 VMware NSX Manager 的更多信息，请参阅 将 Citrix ADC 设备与 VMware NSX Manager集成。

Cisco ACI 混合模式

Cisco ACI 1.3 版 (2f) 中引入了混合模式支持。在混合模式下，可以通过应用程序策略基础结构控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委派给 Citrix ADM，它在 APIC 中充当设备管理器。

Citrix ADC 混合模式解决方案由混合模式设备包和 Citrix ADM 支持。需要在 APIC 中上载混合模式设备包。有关更多信息，请参阅在 Cisco ACI 的混合模式下使用 Citrix ADM 进行 Citrix ADC 自动化。

OpenStack：集成 Citrix ADC 实例

February 6, 2024

Citrix Application Delivery Management (ADM) 的云编排功能使 Citrix ADC 产品与 OpenStack 平台集成。通过将此功能与 OpenStack 平台结合使用，OpenStack 用户可以使用 Citrix ADC 的负载平衡功能 (LBaaS)。之后，OpenStack 用户可以在 Citrix ADC 实例中从 OpenStack 部署负载平衡器配置。

以下各节简要介绍了 Citrix ADM 和 OpenStack 集成工作流中的功能。

Citrix ADC 驱动器用于开放式堆栈中子 LBA

OpenStack 中子 LBaaS 插件包含一个 Citrix ADC 驱动程序，使 OpenStack 能够与 Citrix ADM 进行通信。OpenStack 使用此驱动程序将通过 LBaaS API 完成的任何负载平衡配置转发到 Citrix ADM，Citrix ADM 将在所需的 Citrix ADC 实例上创建负载平衡器配置。OpenStack 还使用驱动程序定期调用 Citrix ADM，以从 Citrix ADC 检索所有负载平衡配置的不同实体（如 VIP 和池）的状态。用于 OpenStack 平台的 Citrix ADC 驱动程序软件与 Citrix ADM 捆绑在一起。要下载并安装驱动程序，必须首先安装 Citrix ADM 并启动应用程序。

相互注册 Citrix ADM 和 OpenStack

您必须首先在 Citrix ADM 上注册 OpenStack 信息。指定 OpenStack 控制器 IP 地址和云管理用户凭据，以及 OpenStack Citrix ADC 驱动用户凭据。稍后可以在中子配置文件 (中子.conf) 的 Citrix ADC_ 驱动程序部分指定相同的登录凭据，以便 OpenStack 中的 Citrix ADC 驱动程序可以在 LB 配置期间连接到 Citrix ADM。

在 OpenStack 和 Citrix ADM 相互注册后，两者都可以相互通信。此外，OpenStack 用户可以使用其在 OpenStack 中的现有凭据登录到 Citrix ADM 用户界面，以检查其 LB 配置在 Citrix ADC 中的执行情况。

OpenStack 中的租户

在 OpenStack 中，租户也称为项目。租户是一组用户；租户或项目也可以定义为一组分配给隔离用户组的资源（计算、网络和存储等）。

放置策略

放置策略使您可以灵活地决定用户创建的每个负载平衡器配置中使用的 Citrix ADC 实例。或者，Citrix ADM 还提供了一个基于 OpenStack 租户分配 Citrix ADC 实例的选项。

服务包

服务包是将策略/SLA、设备或自动置备配置规范及租户/放置策略关联在一起的捆绑包。服务包通常是以提供给租户的隔离策略进行定义。

下面是与服务包相关的一些要点：

- 租户不能属于多个服务包。
- 多个租户可以与相同的服务包关联。
- 在设置为自动配置的服务包中，只能从一种平台类型（在 SDX 平台上或 OpenStack 计算平台上）创建虚拟 Citrix ADC 实例。

LBaaS V1 和 **LBaaS V2** 支持的功能

虽然 OpenStack 中的 LBaaS V1 驱动程序支持从 OpenStack Horizon 用户界面进行操作，但 LBaaS V2 驱动程序仅支持命令行操作。

下面的列表显示了 OpenStack 上 LBaaS V1 和 LBaaS V2 支持的功能：

- LBaaS V1
  - 负载平衡
- LBaaS V2
  - 负载平衡
  - 使用 OpenStack 中主要管理器 Barbican 管理的证书进行 SSL 卸载
  - 证书捆绑包（包括中间证书颁发机构）

- SNI 支持

本文档提供关于以下内容的信息：

- 用例场景
- Citrix ADM 集成与 OpenStack 工作流程
- Prerequisites
- Citrix ADM 和 OpenStack 中的预配置任务
- 使用 Horizon 对 LBaaS V1 进行配置的步骤
- 使用命令行对 LBaaS V2 进行配置的步骤
- 在 OpenStack 上手动配置 Citrix ADC VPX 实例
- 将 Citrix ADM 与 OpenStack 加热服务集成
- 监视 Citrix ADM 中的 OpenStack 应用程序

用例场景

以下用例场景介绍了将 Citrix ADM 与 OpenStack 平台整合的工作流程：

企业 Example-Cloud-Provider 已使用 OpenStack 组件来设置一个云，为其租户提供基础结构。Steve 是此云提供商的管理员，而 Tom 是 Example-Cloud-Provider 的云基础结构的租户。汤姆的组织，例如，Sportsonline.com，需要两个服务器 S1 和 S1，而汤姆还需要一个专用的 Citrix ADC 设备来平衡 OpenStack 平台上的服务器 S1 和 S2 之间的流量。

为了满足这一要求，史蒂夫必须安装和配置 OpenStack 和 Citrix ADM，并准备好相互协作。Steve 必须在 OpenStack 中创建名为 Example-SportsOnline 的租户帐户，然后为该租户帐户分配资源。Steve 还必须为 Example-SportsOnline 创建不同的登录凭据（用户）用于管理器其资源和配置。Tom 现在可以在 OpenStack 上创建两个服务器 S1 和 S2 以管理其组织中的流量。

史蒂夫必须注册 OpenStack 的详细信息与 Citrix ADM, 并在 OpenStack 网络组件中配置 Citrix ADC LBaaS 驱动程序, 中子. 注册完成后，Citrix ADM 将显示 OpenStack 中所有租户的详细信息。Steve 可以从想要 Citrix ADC LBaaS 功能的列表中选择 Example-sportsOnline，然后配置 Tom 在 Citrix ADM 中为其负载平衡器配置分配专用 Citrix ADC。

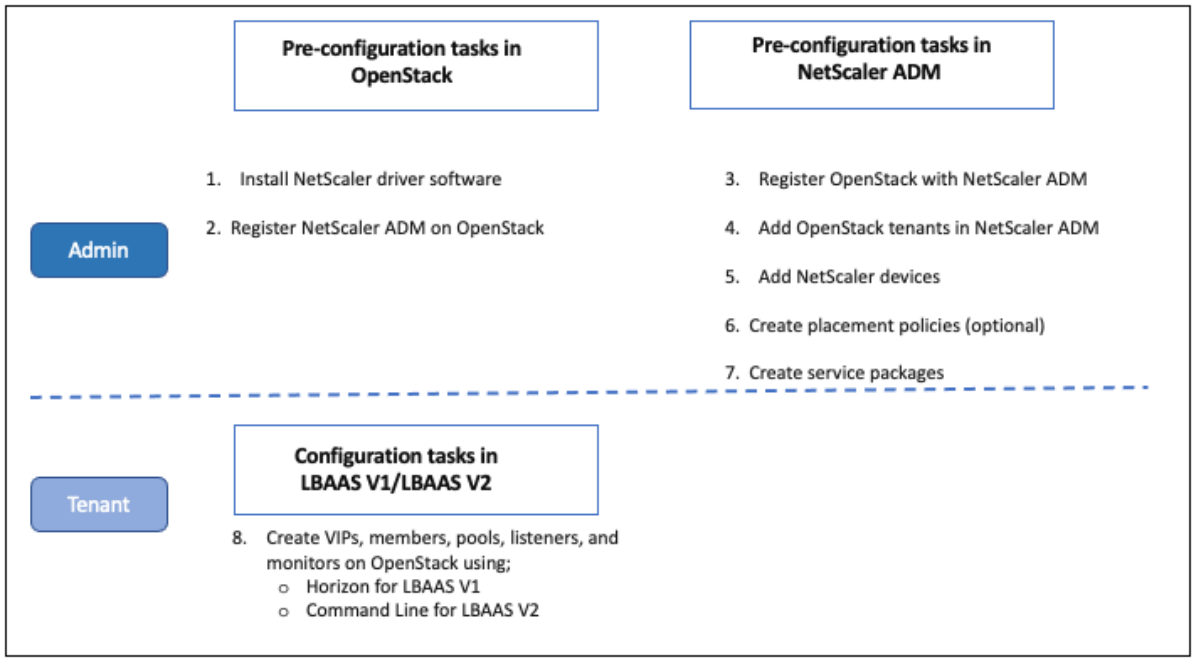
为此，Steve 可以使用 Citrix ADM 用户界面在 OpenStack 的计算层（Nova）上配置 Citrix ADC VPX 实例，也可以使 MAS 按需自动配置 Citrix ADC VPX 实例，当 Tom 在 OpenStack 中进行 LB 配置时。在任何一种情况下，Citrix ADM 都会管理 VPX 实例。为了实现这一目标，Steve 在 Citrix ADM 中创建了一个服务包，并定义了 SLA 中与 Tom 商定的服务包中的条件。例如，Steve 选择“专用”隔离策略来提供专用实例用于为 Tom 提供负载平衡器配置。即，Steve 在服务包中为 Tom 选择非共享实例。然后，他将许多 Citrix ADC VPX 实例分配给服务包，并将示例体育联机以及需要专用 Citrix ADC 和服务包的其他租户关联起来。因此，当 Tom 执行他的第一个负载平衡器配置时，Citrix ADM 会将服务包中的一个 Citrix ADC VPX 实例分配给 Example-SportsOnline，并将他的配置部署到该 Citrix ADC 中。

Tom 现在可以通过使用 OpenStack LBaaS/UI 创建池、虚拟 IP (VIP) 及运行状况监视器来创建负载平衡配置。OpenStack 中的池和 VIP 在 Citrix ADC 实例上作为服务组和虚拟服务器进行部署。Tom 还可以创建运行状况监视器来监视服务器，并仅向那些在任何时间点处于运行状态且可从 Citrix ADC 访问的服务器发送应用程序流量。

在 OpenStack 中创建的负载平衡配置现在已在 Citrix ADC 实例上实施。完全配置后，Citrix ADC VPX 实例接管负载平衡功能，并开始接受应用程序流量并平衡 Tom 创建的服务器 S1 和 S2 之间的流量。

Citrix ADM 与 OpenStack 工作流程的集成

下面的流程图说明了在配置 LBaaS V1 和 LBaaS V2 时需要遵循的工作流。



必备条件

February 6, 2024

在将 Citrix ADC 虚拟实例与 OpenStack 平台集成之前，请确保满足以下要求：

Citrix ADM 和 OpenStack 软件要求

- Citrix ADM 12.1 安装在受支持的 Hypervisor 工作站上，该工作站符合最低硬件要求系统。
- OpenStack 组件已安装并正在运行。
- Citrix ADM 12.1 支持以下 OpenStack 版本 - Newton、Ocata 和 Pike。

Citrix ADM 硬件要求

下表列出了在 OpenStack 服务器上安装 Citrix ADC 虚拟实例时应拥有的虚拟计算资源。

组件	要求
RAM	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

> 注意
>
> 考虑到主机上没有其他虚拟机运行，上面指定的内存和硬盘要求适用于在 OpenStack 平台上部署 Citrix ADM。对 OpenStack 的硬件要求取决于在其中运行的虚拟机数。

Citrix ADM 和 OpenStack 中的预配置任务

February 6, 2024

本节将帮助您在配置 Citrix Application Delivery Management (ADM) 和 OpenStack 之前执行预配置任务。

安装 Citrix ADM

在受支持的 Hypervisor 上安装 Citrix ADM。有关如何下载和安装 Citrix ADM 的更多信息，请参阅 部署 Citrix ADM。

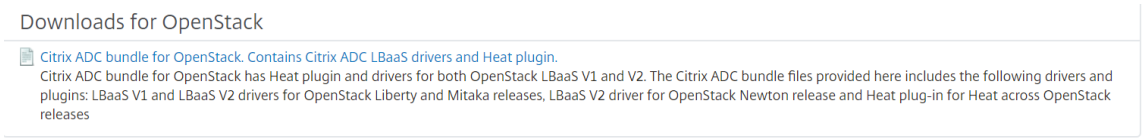
安装 Citrix ADC 驱动程序软件并在 OpenStack 上注册 Citrix ADM

从 Citrix ADM 下载页面下载适用于 OpenStack 的 Citrix ADC 捆绑包。

要使用 **Citrix ADM GUI** 在 **OpenStack** 平台上安装 **Citrix ADC** 驱动程序，请执行以下操作：

1. 在 Citrix ADM 中，单击“下载”。Citrix ADM 中的“下载”页面提供了下载适用于 Newton、Ocata 和 Pike OpenStack 版本所需的适用于 **OpenStack** 的 **Citrix ADC** 捆绑包软件的链接。

2. 将最新的 Citrix ADC 捆绑 tar 文件下载到 OpenStack 控制器中的临时目录（例如 /tmp）。该捆绑包包括适用于所有 OpenStack 版本的 LBaaas V2 驱动程序和热插件。



3. 运行以下命令，从 Citrix ADC 驱动程序 tar 文件中提取文件：

```
tar -xvzf <name_of_tar_file>
```

4. 如果您有 OpenStack <Release Name> 设置，请在提示符下键入以下命令：

```
cd <Release Name>
```

示例：

```
cd Newton
```

5. 运行以下命令来安装驱动程序并指定 Citrix ADM IP 地址、在向 Citrix ADM 注册 OpenStack 时配置的 Citrix ADC 驱动程序密码以及协议：

```
./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
```

单节点 **OpenStack** 设置示例：

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
```

多节点 **OpenStack** 设置示例：

```
./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
```

> 注意
>
> 提供系统的 neutron-lbaas 目录的路径是可选的。提供该路径可以帮助脚本找到驱动程序。
>
> 在 OpenStack 上成功注册 Citrix ADM 后，您还可以使用 OpenStack 用户凭据登录到 Citrix ADM。
>
> 在 OpenStack 上成功注册 Citrix ADM 后，重新启动 OpenStack 中子服务。

在 **Citrix ADM** 中注册 **OpenStack**

要使用 **Citrix ADM GUI** 将 **OpenStack** 注册到 **Citrix ADM**，请执行以下操作：

1. 在 Citrix ADM 中，导航到“编排”>“云编排”>“**OpenStack**”。
2. 单击“配置 **OpenStack** 设置”。

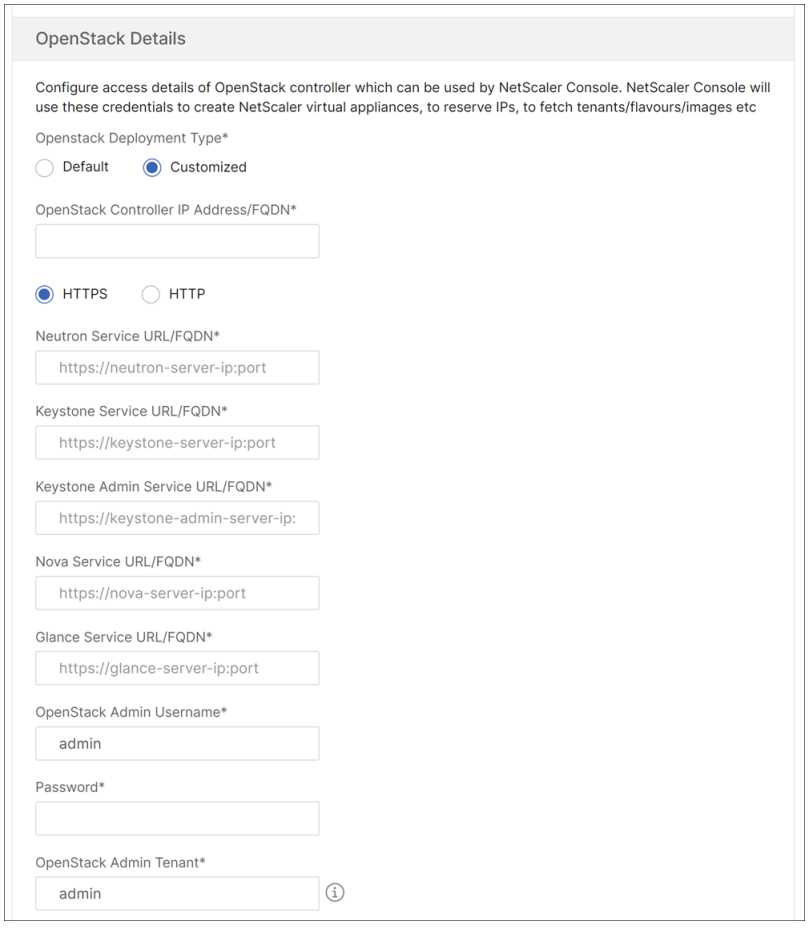
3. 在“配置 **OpenStack** 设置”页面中，您可以设置参数以在 Citrix ADM 中配置 OpenStack。此处有两个选项 - “Default”（默认）和“Customized”（自定义）。

   对于 OpenStack 的 Newton 和 Ocata 版本，您可以使用默认或自定义部署类型。但是，对于 Pike 版本，您必须使用自定义部署类型向 Citrix ADM 注册 OpenStack。

- 默认部署类型

  如果 OpenStack 服务正在默认端口上运行，请选择默认值。例如，Neutron 服务的默认端口是 9696，Keystone 服务的默认端口是 5000。

1. OpenStack Controller IP Address（OpenStack 控制器 IP 地址）- OpenStack 控制器的 IP 地址（应该可以使用此 IP 地址访问 KeyStone 服务和 Neutron 服务）。例如，输入 IP 地址 10.102.205.23。
2. OpenStack 管理员用户名-OpenStack Controller 的管理员用户名。例如，输入 admin1。
3. Password（密码）- OpenStack 控制器的管理用户的密码。
4. OpenStack 管理租户-OpenStack 上管理租户的名称。例如，输入 admin。



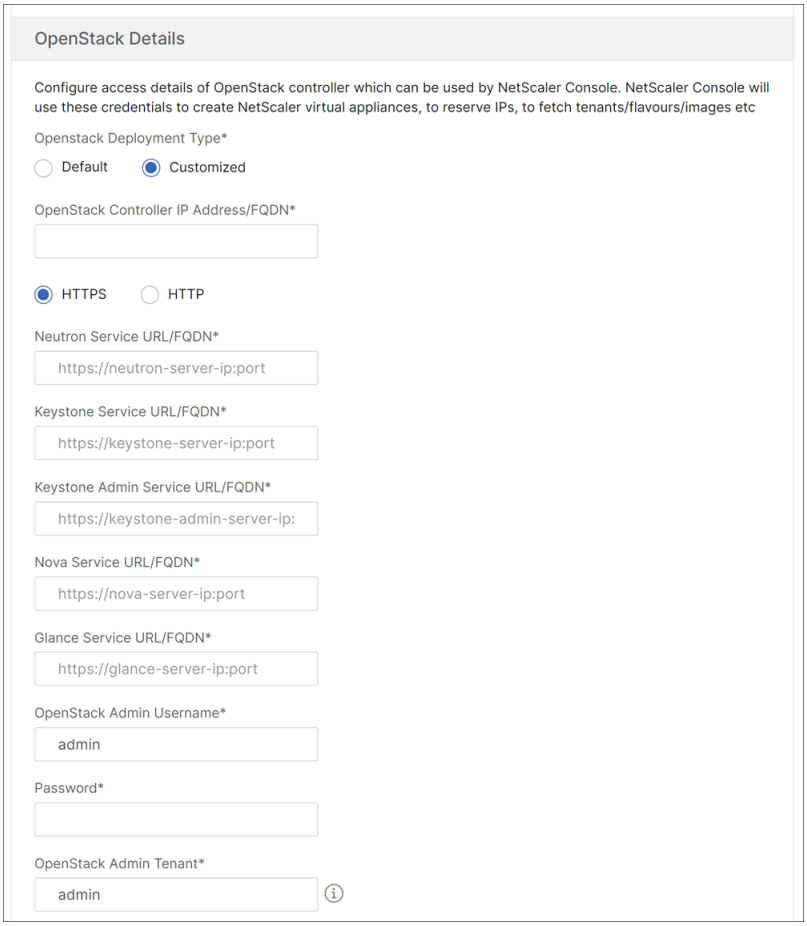
- 自定义部署类型

  如果 OpenStack 服务在不同于默认端口的端口上运行，请将部署类型选择为自定义。如果这些服务在不同的端

口上运行，请在此处指定它们。在 Citrix ADM 中注册 OpenStack Newton 和 Ocata 版本与注册 OpenStack Pike 版本不同。

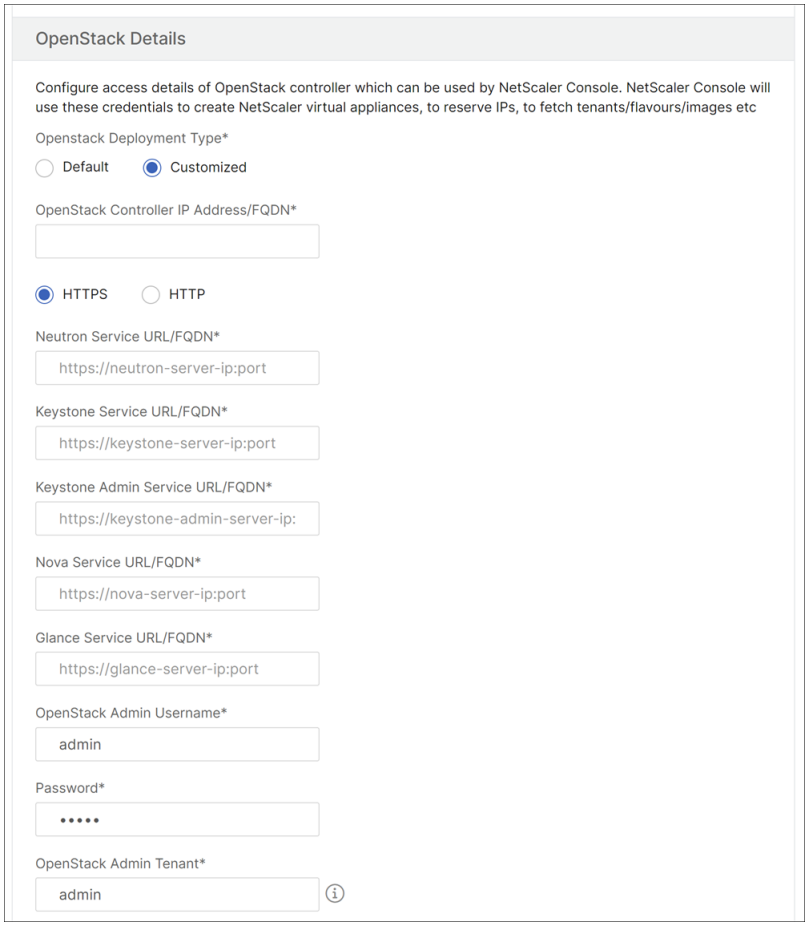
OpenStack 的 **Newton** 和 **Ocata** 版本：

1. 如果您正在注册 OpenStack 的 Newton 版本，请指定各种 OpenStack 服务的端口号。
2. 指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名，如您之前在 默认 设置中指定的那样。

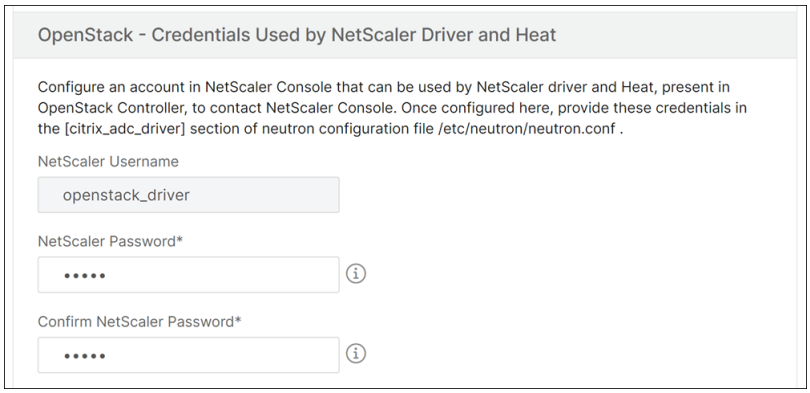


OpenStack 的 **Pike** 版本：

如果您正在注册 OpenStack 的 Pike 版本，请输入 OpenStack 服务的详细信息，如下图所示。您还必须在默认设置中指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名。



1. 在 **OpenStack** 中子 **LBaaS-Citrix ADC** 驱动程序使用的凭据部分中，为 OpenStack Citrix ADC 驱动程序用户帐户设置 Citrix ADC 驱动程序密码。Citrix ADM 使用这些凭据对来自 OpenStack Citrix ADC 驱动程序的调用进行身份验证。在 OpenStack Controller 中执行 Citrix ADC 驱动程序安装脚本时，必须指定相同的密码。



2. 单击确定。

在 **OpenStack** 上创建租户

在 OpenStack 中创建项目或租户，将用户添加到项目或租户，并为所有用户分配角色。OpenStack 中的身份服务 KeyStone 为每个 OpenStack 服务提供身份验证服务。身份验证服务使用域、项目（租户）、用户和角色组合。

有关如何在 OpenStack 中创建项目和执行其他任务的更多信息，请参阅 OpenStack 文档，网址为 http://docs.openstack.org/。

添加 **OpenStack** 租户

1. 在 Citrix ADM 中，导航到编排 > 云编排 > **OpenStack** >**OpenStack** 租户，然后单击添加。
2. 在 **Add OpenStack Tenants**（添加 OpenStack 租户）页面上，单击 **+Add**（+ 添加），然后选择 OpenStack 租户。
3. 单击确定。

根据在集成 OpenStack 时是使用预置备的实例还是自动置备实例，执行以下两个任务之一：

- 预置 Citrix ADC 设备
- 在 OpenStack 上自动配置净缩放器 VP X 设备

预配 **Citrix ADC** 设备

根据在集成 OpenStack 时是使用预置备的实例还是自动置备实例，执行以下两个任务之一：

- 预置 Citrix ADC 设备
- 在 OpenStack 上自动配置净缩放器 VP X 设备

预配置 **Citrix ADC** 设备

在任何虚拟机管理程序平台（如 Citrix Hypervisor、KVM 或 ESX）上安装 Citrix ADC 设备，并将该实例添加到 Citrix ADM。然后，Citrix ADM 管理此设备，该设备负载平衡服务器中的流量。

要在 **Citrix ADM** 中添加现有的 **Citrix ADC VPX** 实例，请执行以下操作：

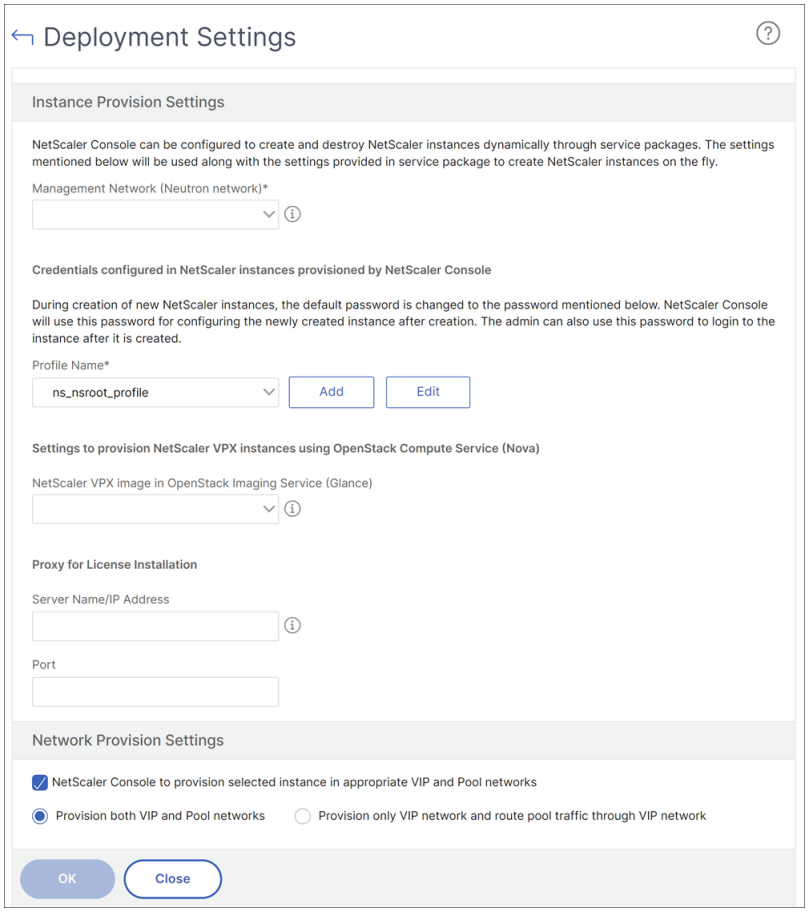
1. 在 Citrix ADM 中，导航到“基础架构”>“实例”>“**Citrix ADC VPX**”，然后单击“添加”。
2. 在“添加 **Citrix ADC VPX**”页上，指定 Citrix ADC VPX 实例的 IP 地址，然后从“配置文件名称”列表中选择一个实例配置文件。实例配置文件包含用于登录到 Citrix ADC VPX 的凭据。还可以单击 + 图标创建新实例配置文件。单击确定。

自动配置 **Citrix ADC** 设备

从 Citrix 下载页面下载所需的 Citrix ADC 实例映像，然后将其上载到 OpenStack Imaging 服务 Glance 上。在将实例分配给租户时，使您可以按需配置 Citrix ADC 实例。

要在 **OpenStack** 上自动置备 **Citrix ADC VPX** 设备，请执行以下操作：

1. 在 Citrix ADM 中，导航到“编排”>“云编排”>“**OpenStack**”。
2. 单击“部署设置”。
3. 设置以下参数：
    a) 管理网络-选择 OpenStack 上的管理网络，自动配置的 Citrix ADC VPX 连接到该网络。
    b) Profile Name（配置文件名称）- 从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
    c) 许可证 - 提供用于许可新的自动预配的 Citrix ADC 实例的 Citrix ADM 许可证激活代码 (LAC)。Citrix ADM 在管理网络中的 OpenStack 计算上配置 Citrix ADC 实例，然后使用指定的许可证代码在这些实例上触发许可证安装。然后，Citrix ADC 实例使用此处指定的 LAC 从 Citrix 网站下载许可证文件。
    d) Citrix ADC VPX 映像概览-选择用于创建 Citrix ADC VPX 实例的 OpenStack 概览中可用的 Citrix ADC VPX 映像。
    e) 代理设置-提供用于安装许可证的 Citrix ADC 代理服务器的详细信息。如果 Citrix ADC 无法通过管理网络直接访问互联网，则可能需要这样做。
4. 单击确定。



在 **Citrix ADM** 中创建服务包

要在 **Citrix ADM** 中为租户创建服务包，请执行以下操作：

1. 在 Citrix ADM 中，导航到 编排 > 云 编排 > **OpenStack** > 服务包，然后单击“添加”。
2. 在“服务包”页面上，指定以下参数：
   a) Name（名称）- 服务包的名称。例如，输入 SVC-PKG-GOLD。
   b) Citrix ADC 实例分配-在服务包中定义的实例分配类型，Citrix ADC 实例资源分配给租户。选择 专用。有关策略的更多信息，请参阅 服务包隔离策略。
   c) Citrix ADC 实例预配-选择 现有实例以将现有 Citrix ADC 实例分配给租户。如果要在配置期间创建 Citrix ADC 实例，请选择“按需创建实例”。
   d) Citrix ADC 实例类型-选择 **Citrix ADC VPX**。

   > 注意：
   >
   > 选择 Citrix ADC VPX 以分配在 SDX 平台上托管的预配置 Citrix ADC 实例。

3. 单击“继续”将租户与服务包相关联。

> 注意：如果要在 ** 高可用性模式下部署 Citrix ADC 实例，则
>
> 启用预配 ** 置 Citrix ADC 实例对以实现高可用性。

4. 在“分配实例”部分，单击“添加”，然后选择要分配给租户的 Citrix ADC 实例，然后单击“继续”。
5. 在“分配 **OpenStack** 租户/安置政策”部分的 **OpenStack** 租户下，单击“添加”，然后选择 租户。
6. 单击 **Continue**（继续），然后单击 **Done**（完成）。

> 注意：
>
> 如果未找到策略，则会恢复回退机制，并且 Citrix ADM 会根据租户分配 Citrix ADC 实例。如果租户不是任何服务包的一部分，Citrix ADM 将显示一条错误消息：“Tenant <admin> 不是任何服务包的一部分，也没有默认的服务包。”

创建放置策略（可选）

隔离策略不仅仅基于租户。可以创建灵活的放置策略，这些策略不仅基于租户名称或 ID，而且也基于其他自定义属性。

要在 **Citrix ADM** 中为租户创建放置策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 编排 > 云 编排 **>**OpenStack**>** 放置策略，然后单击“添加”。
2. 在 **Add Placement Policy**（添加放置策略）页面上，设置以下参数：
   a) Name（名称）- 键入放置策略的名称
   b) Sample Expressions（示例表达式）- 从列表中选择示例表达式。这些示例有助于构建放置策略。
   c) Expression（表达式）- 根据在前面的字段中选择的示例表达式，在此字段中填充一个布尔表达式。根据需要编辑字段名称。
3. 单击确定。

通过客户端网络启用从 **Citrix ADC** 实例到后端服务器的流量

默认情况下，在 OpenStack 编排工作流中，Citrix ADC 实例会动态绑定到负载平衡器或客户端网络以及成员或服务器网络。

在某些部署中，也可以通过客户端网络访问服务器，并且可以通过客户端网关进行路由。在这种情况下，Citrix ADC 实例无需绑定到服务器网络，而只需要绑定到客户端网络。

执行以下设置以配置通过客户端网关的流量。

导航到“调配”>“云调配”>“**OpenStack**”>“部署设置”，然后选择“仅配置 **VIP** 网络和通过 **VIP** 网络路由池流量”选项。

然后，Citrix ADM 通过在客户网络中添加 SNIP 来将 Citrix ADC 实例配置到该网络，并将进一步向客户端网络网关添加默认路由。这使实例能够通过客户端网关到达服务器。

Citrix ADC SDX 平台上部署的自动配置 **Citrix ADC VPX** 设备

在 Citrix ADM 中添加 Citrix ADC SDX 平台，以便 Citrix ADM 按需在此平台上配置实例。

要自动监视部署在 **Citrix ADC SDX** 平台上的 **Citrix ADC** 实例，请执行以下操作：

1. 在 Citrix ADM GUI 中，导航到 网络 > 实例 > **Citrix ADC SDX**，然后单击 “添加” 以添加 Citrix ADC SDX 平台。
2. 导航到 调配 > 云调配 > **OpenStack** > 部署设置。
3. 在 “管理网络 ” 部分，在 OpenStack 上选择自动配置的 Citrix ADC SDX 所连接的管理网络。
    a) 在配置文件名称中，从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
    b) 单击确定。
4. 要在 OpenStack 中配置 Citrix ADC SDX 平台，请导航到编排 > 云编排 >**OpenStack**> 服务包。
    a) 单击“添加”创建新的服务包。
    b) 输入服务包的名称。
    c) 在 **Citrix ADC** 实例分配字段中，选择专用。
    d) 在 **Citrix ADC** 实例置备字段中，选择按需创建实例，然后在自动配置平台字段中，选择 **Citrix ADC SDX**。
    e) 默认情况下，仅在 Citrix ADC SDX 平台上预配 Citrix ADC VPX 实例。
    f) 单击 继续。
    g) 在“自动配置设置”部分中，设置资源 属性。
        i. 吞吐量 字段。输入 1000 Mbps。
        ii. **Citrix ADC** 版本 字段。从列表中，选择 Citrix ADC SDX 平台上存在的正确版本的 Citrix ADC VPX 映像。使用命令行配置 LBaaS V2
    h) 在 **Citrix ADC SDX** 平台部分中，单击添加 以将 SDX 平台添加到服务包中。
    i) 单击 继续。
    j) 在“配置 **OpenStack** 租户”部分，单击“添加”以添加租户。您也可以通过单击“新建”来添加新租户。
    k) 单击完成。
5. LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端，并执行配置任务。有关如何执行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

使用地平线配置 **LBaaS V1**

February 6, 2024

Tom 现在可以登录 OpenStack Horizon 门户，创建 LBaaS 池，并选择此池的所有成员所在的子网。Tom 必须添加虚拟 IP (VIP) 地址并将此 VIP 分配给他创建的池。Tom 还可以在命令行上或通过 API 执行此操作。Tom 服务器的外部客户端可以连接到此 VIP 地址，该地址托管在分配的 Citrix ADC 上，Citrix ADC 通过配置的端口将所有请求分发给池成员。

LBaaS 池成员是添加到所选池的已负载平衡的服务器。Tom 可以为其中每个成员分配权重和端口。

运行状况监视器用于观察池的所有成员的运行状况和良好运行状态。Tom 可以在 OpenStack 中指定延迟、超时和重试限制来创建运行状况监视模板，此外还可以指定方法、URL 路径以及成功时的预期 HTTP 代码。创建监视器后，Tom 必须将监视器与之前创建的池关联。

有关如何在 OpenStack 中创建池以及其他 LBaaS 配置任务的更多信息，请参阅 OpenStack 文档。

> 重要
>
> OpenStack 的 Liberty 版本不支持 LBaaS V1。有关更多信息，请参阅 OpenStack 发行说明。

使用命令行配置 **LBaaS V2**

February 6, 2024

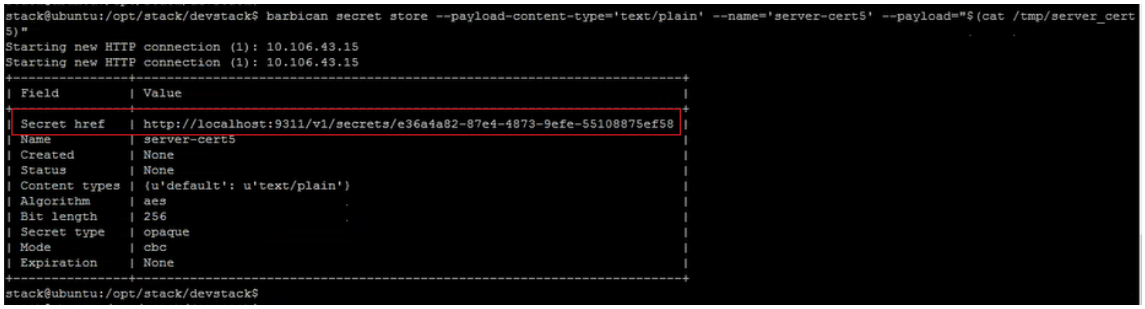
LBaaS V2 支持使用 Barbican 管理的证书进行 SSL 卸载、证书捆绑包（包括中间证书颁发机构）、SNI 支持以及常规负载平衡功能。LBaaS V2 仅支持使用命令行接口执行配置任务。LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。

> 注意
>
> 要求使用 SSL 卸载功能时，请将证书和密钥上载到 Barbican 服务。如果支持 SSL 卸载，请执行步骤 1、2 和 3，否则请从步骤 4 继续以创建负载平衡器、侦听器、池和成员。

1. 使用以下命令将证书上载到巴比肯服务：

   barbican secret store –payload-content-type <content_type> –name <certificate_name> –payload<certificate_location>

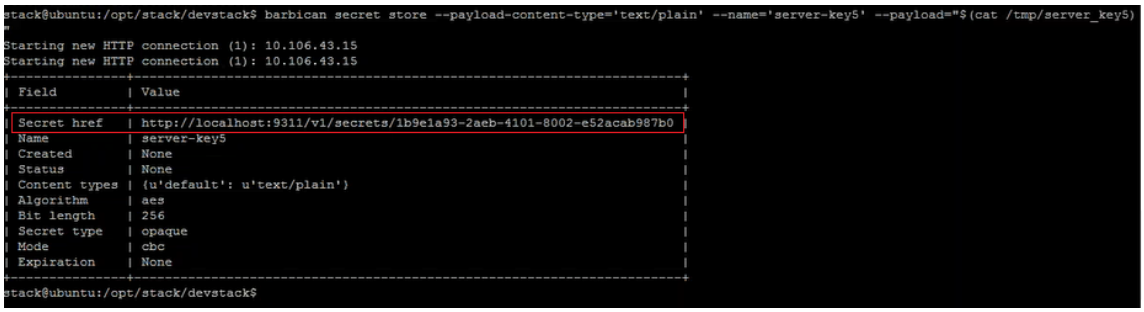
   示例：barbican secret store –payload-content-type=’ text/plain’–name=’ hp_server_certificate’–payload=” hp_server/tmp/server_certificate”



2. 使用以下命令将密钥上载至 Barbican 服务：

   barbican secret store –payload-content-type <content_type> –name <key_name> –payload<key_location>

   示例：barbican secret store –payload-content-type=’ text/plain’ –name=’ shp_server_key’ –payload=” hp-server/tmp/server_key”



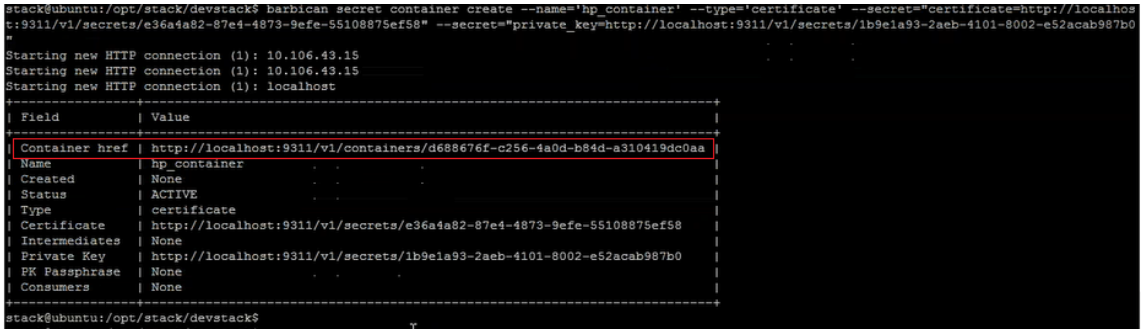
> 注意
>
> 在执行这两个 Barbican 命令加载证书和密钥时，“Secret href”字段提供位置或 url。这是安装了 OpenStack 的系统上存储证书和密钥的位置。复制这些链接，在步骤 3 中在 Barbican 服务中创建容器时，将这些链接作为参数提供。

3. 使用以下命令在 Barbican 服务中创建容器以存储证书和密钥：

   在命令中，将 <certificate_url> 替换为在上载证书时从“Secret href”字段获得的 url。同样，将 <key_url> 替换为在上载密钥时从“Secret href”字段获得的 url。

   barbican secret container create –name<container_name> –type<container_type> –secret<certificate_url> –secret<key_url>

   示例：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”



请复制容器 href 值。在步骤 6 中创建侦听器时必须提供指向容器的链接。

4. 在 OpenStack 中设置环境变量。通过这些变量，OpenStack 客户端命令可以与 OpenStack 服务通信。

   示例：

   export OS_PASSWORD-hp

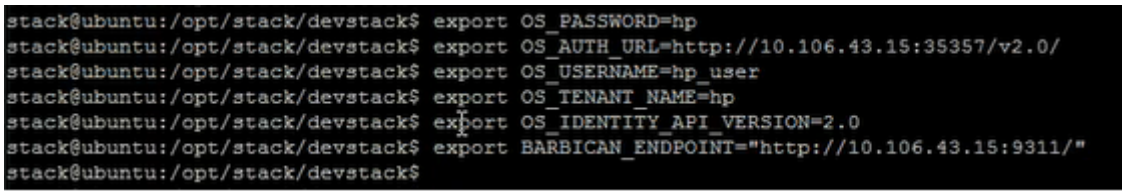
   导出 OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   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/"



> 注意
>
> 在运行其他命令之前为每个 SSH 会话设置这些变量。有关 OpenStack 环境变量的详细信息，请参阅 OpenStack 环境变量。

5. 使用以下命令创建负载平衡器：

   neutron lbaas-loadbalancer-create –name <loadbalancer-name> <subnet-name> –provider <netscaler>

   示例：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$
```

成功创建负载平衡器后，状态从 PENDING_CREATE 变为 ACTIVE。

```
+--------------------------------------+------------+-------------+---------------------+-----------+
| 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. 使用以下命令创建监听程序：

   neutron lbaas-listener-create –loadbalancer <loadbalancer-name> –name <listener-name> –protocol <protocol_type> –protocol-port <port_number> –default-tls-container-id<container_url>

   示例：中子监听器创建—名称 hp-lb 测试列表—负载平衡器 hp-lb 测试—协议终止 _HTTPS —协议端口 443 —默认 TLS 容器 ID `http://10.106.43.15:9311/v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`

   > 注意
   >
   > 如果要在没有 SSL 卸载支持的情况下创建侦听器，请执行以下命令而不提供容器位置：
   >
   > 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. 使用以下命令创建池：

neutron lbaas-pool-create –lb-algorithm <algorithm_type> –listener <listener-name> –protocol <protocol_type> –name <pool-name>

示例：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. 使用以下命令创建成员：

   neutron lbaas-member-create –subnet <subnet-name> –address <ip-address of the web server> –protocol-port <port_number> <pool-name>

   示例：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$
```

监视 **Citrix ADM** 中的 **OpenStack** 应用程序

您的租户可以使用其 OpenStack 凭据登录到 Citrix Application Delivery Management (ADM)，以监视从任何浏览器从 OpenStack 创建的 VIP 和池。URL 的格式应如下所示：

http://\<mas_ip\>/\<admin_ui\>/mas/ent/html/cc_tenant_main.html

其中，<mas-ip-address>，是在 OpenStack 中注册的 Citrix ADM IP 地址。

> 注意
>
> - OpenStack VIP 对应于 Citrix ADM 中的虚拟服务器。
> - OpenStack 池对应于 Citrix ADM 中的服务组。
> - OpenStack 池成员对应于 Citrix ADM 中的服务组成员。

配置第 7 层内容交换

February 6, 2024

Citrix Application Delivery Management (ADM) 与 OpenStack 协调，在 Citrix ADC 实例上配置第 7 层 (L7) 交换或基于内容的交换功能。内容交换与简单的负载平衡不同，因为特定类型的请求可以导向到特定服务器。在 OpenStack 中使用 Citrix ADC 实例作为提供程序创建 L7 配置时，Citrix ADM 会分配一个 Citrix ADC 实例，并部署与 L7 配置对应的内容交换和响应器配置。然后，Citrix ADC 实例可以根据请求的应用层特征分发和负载平衡用户请求。

OpenStack 7 层 (L7) 负载平衡功能组合了负载平衡和内容交换，可针对特定类型内容提供优化交付。因此，由于仅执行适用于内容的策略，从而提高了负载平衡器的性能。7 层负载平衡还有利于提高应用程序基础结构的效率。由于能够根据类型、URI 或数据分开内容，因此能够在应用程序基础结构中优化物理资源的分配。例如，浏览到的最终用户 `http://example-sports.com/about-us` 应由托管有关公司和服务的内容的服务器池提供服务，而浏览的用户则 `http://example-sports.com/shopping-cart-football` 应由其他服务器池提供服务。允许用户进行在线购买。

在 L7 交换中，负载平衡器实现为内容交换虚拟服务器，该服务器接受来自用户的 HTTP 请求，并将请求分发到应用程序服务器。L7 交换或内容交换允许您通过单点进入来访问各种后端服务（例如，不仅有 Web 应用程序、Web 服务门户、Web 邮件，而且有移动管理、不同语言的内容等）。即，您可以为您向用户提供的所有服务提供一个公用 IP 地址。

与较低级别的负载平衡不同，7 层交换不要求池中的所有服务器具有相同的内容。使用 L7 交换的负载平衡器配置假定不同池中的应用程序或后端服务器具有不同的内容。L7 交换可以根据 URI、主机、HTTP 标头或应用程序消息中的任何其他内容导向请求。应用程序服务器实际上应该能够为特定类型的内容提供服务。例如，一个服务器可能只为图片提供服务，一个服务器可能执行服务器端脚本语言（例如 PHP 和 ASP），另一个服务器可能为静态内容（例如 HTML、CSS 和 JavaScript）提供服务。

L7 规则

以下属性在规则中定义，用于评估流量，它们将与规则中定义的值进行比较：

- hostname：HTTP 请求中的主机名将与规则中的值参数进行比较。例如 www.example-sports.com。
- path：HTTP URI 的路径部分将与规则中的值参数进行比较。例如，“www.example-sports.com/shopping-cart/football_pump.
- file_type：URI 的最后一部分将与规则中的值参数进行比较。例如 txt、html、jpg、png、xls 等。
- header：主要参数中定义的标头将与规则中的值参数进行比较。
- cookie：主要参数指定的 cookie 将与规则中的值参数进行比较。cookie request-header 字段值包含存储的 URL 信息的名称和值对；常规语法如下 - Cookie: name=value。例如，一个正在寻找名为“stores”且值以“football-”开头的 Cookie 的规则将如下所示：type = Cookie, compare_type=StartsWith, key = stores value = football-。

比较类型

评估流量时，L7 策略将以下表达式与规则中定义的属性进行比较。

- regex：Perl 类型正则表达式匹配
- starts_with：字符串开头
- ends_with：字符串结尾
- contains：字符串包含
- equal_to：字符串等于

> 注意
>
> 主机名、路径、标头和 cookie 属性支持所有比较类型，但 file_type 属性仅支持正则表达式和 equal_te。

L7 策略

L7 策略处理传入 HTTP 流量，当匹配策略中定义的所有规则时返回“true”值。

在任何 L7 策略中，所有规则都通过 AND 运算符以逻辑方式连接在一起。请求必须匹配所有规则，策略才会返回“true”值。负载平衡器采取的操作基于策略返回的值。您可以创建具有相同操作的另一个策略，在规则之间实现逻辑 OR 运算。

例如，您可以创建一个策略，在此策略中，传入 HTTP 请求可以包含词语“EXAMPLE-SPORTS”、“SPORTS-FOOTBALL”或“EXAMPLE-FOOTBALL”，以便负载平衡器可以采取合适的操作将这些请求转发到 Example-sports ecommerce 公司的服务器池，从而为请求的内容提供服务。您可以创建另一个策略，它采取相同操作但匹配“example-sports”、“example-sports-football”或“example-football”。如果用户发送的 HTTP 请求包含这六个关键字中的任何一个，负载平衡器都将请求转发到 Example-Sports 服务器。

根据策略中定义的规则，L7 策略可以采取以下任何操作：

- 重定向到池 - 将请求转发到与 L7 策略关联的规则标识的应用程序服务器。即，您可以创建一个应用程序规则以根据域名将请求定向到特定负载平衡器池。例如，您可以创建一个规则，将针对 example-football.com 的一些请求定向到 pool_1，将针对 example-sports-online_purchase.com 的其他请求定向到 pool_2。
- 重定向到 URL - 向客户端发送位置响应头包含新位置的重定向 HTTP 响应。浏览器使用新位置更新地址栏并发出新请求。用例很多。例如，如果 Web 站点地址发生变化，您可以将请求重定向到新地址，而不是丢弃。或者，在 Web 站点维护期间，您可以将用户重定向到只读站点。
- 拒绝 - 拒绝请求且不采取任何进一步操作。例如，您可以返回“401 Unauthorized”（401 未经授权）响应以拒绝用户对受限制 Web 页面的访问。

内容交换配置包括内容交换虚拟服务器、负载平衡设置（包括负载平衡服务器和服务）以及内容交换策略。创建内容交换虚拟服务器和策略后，应将每个策略绑定到内容交换虚拟服务器。将策略绑定到内容交换虚拟服务器时，应指定目标

负载平衡虚拟服务器。请求到达内容交换虚拟服务器时，该虚拟服务器将关联的内容交换策略应用于该请求。策略的优先级定义绑定到内容交换虚拟服务器的策略的评估顺序。

可以将具有侦听器 ID 的任何池分配为流量转移到的默认虚拟服务器池。池与侦听器松散绑定在一起，仅通过实现 L7 策略与侦听器关联。还可以直接在负载平衡器下创建池，无需绑定到侦听器。在这种情况下，池创建时处于“pending_create”状态。由于 L7 策略与侦听器紧密绑定在一起，因此必须创建并实现包含池 ID 的 L7 策略，池才能处于“active”状态并开始接收流量请求。

一个池可以由多个 L7 策略提供服务，但在至少附加了一个策略时保持“active”状态。删除最后一个策略后，池返回到“pending_create”状态，直到创建了另一个策略并与之关联。如果删除池本身，则原本由它接收的所有 HTTP 请求都重定向到默认池。

OpenStack L7 策略和 **Citrix ADC** 实体之间的映射

OpenStack	Citrix ADC 实体	说明
操作为 REDIRECT_TO_POOL 的 L7 策略	内容交换策略 > 内容交换操作	Citrix ADM 创建一个内容交换策略，该策略绑定到内容交换虚拟服务器，并与内容交换操作相关联，该操作指定应用程序服务器的目标池，以便检索内容并向用户呈现。
操作为 REDIRECT_TO_URL 的 L7 策略	响应方策略 > 响应方操作	Citrix ADM 创建一个响应程序策略，该策略绑定到内容交换虚拟服务器，并与响应程序操作关联，该操作指定要向用户显示的目标 URL。
操作为 REJECT 的 L7 策略	响应方策略 > 丢弃请求	Citrix ADM 创建一个响应程序策略，该策略绑定到内容交换虚拟服务器，并与删除请求的响应程序操作相关联。

如果评估结果为“真”的 L7 策略的操作将流量重定向到处于“create_pending”状态的池，则 Citrix ADM 将实现指定的池以及负载平衡虚拟服务器。Citrix ADM 从 L7 策略中创建内容交换策略，并使用相应的内容交换操作将请求重定向到与该池关联的负载平衡虚拟服务器。如果第二个 L7 策略重定向到同一池，Citrix ADM 将创建内容交换策略和内容交换操作，以将流量重定向到与池关联的现有负载平衡虚拟服务器。

策略定位

OpenStack 中对 L7 策略的评估由其优先级确定。在 OpenStack 中，默认情况下，按策略的创建顺序为其分配优先级。第一个创建的策略编号为 1，后续创建的策略连续编号。但您可以更改策略的优先级，为其分配不同的优先级。策略始终按其优先级顺序进行评估。始终首先执行匹配特定请求的第一个策略。

创建策略时，应注意以下事项：

- 如果为新策略分配的优先级与某个现有策略相同，则新策略采用该优先级。现有策略的优先级将会降低。如有必要，还可以降低其他策略的优先级以保持策略的评估顺序。
- 如果创建新策略时未指定位置，则新策略将只是附加到列表中。
- 如果创建新策略时为其分配的位置大于列表中已有的策略数，则新策略将附加到列表中，即，新策略的优先级将始终为下一个可用优先级。例如，假定有三个策略 A、B 和 C，优先级为 1、2 和 3，如果创建一个策略并为其分配优先级 8，则新策略的优先级将变为 4。
- 如果向列表添加策略或从列表中删除策略，则策略位置值将从 1 重新排序，而不会跳过数字。例如，假定策略 A、B、C 和 D 的位置值为 1、2、3 和 4，如果从列表中删除策略 B，则策略 C 现在排在第二个位置，策略 D 排在第三个位置。

在 Citrix ADM 中，始终存在与优先级为 1 的 csvServer 相关联的默认策略。此默认策略指定在任何给定时间点 lbvserver 应处理的 TCP 连接数。因此，当在 Citrix ADC 中创建相应的响应程序策略和内容交换策略时，它们的优先级总是高于相应 L7 策略的优先级 1。例如，如果 L7 策略的优先级为 1，则创建的内容交换策略的优先级为 2。同样，如果 L7 策略的优先级为 2，则创建的响应方策略的优先级为 3。

在 OpenStack 中，首先评估“reject”和/或“redirect_to_url”策略，然后评估“redirect_to_pool”策略。在 Citrix ADC 实例中，始终首先评估响应程序策略，以删除请求或向用户提供重定向的 Web 地址，最后评估内容切换策略。如果内容交换策略和响应方策略相互排斥，则此评估顺序通常不会导致出现任何冲突。即，两个 L7 策略不应有相同的表达式。应该在响应方策略和内容交换策略中添加派生表达式以避免此类冲突。例如，编写一个表达式用于拒绝发送到“sports-football.com”的所有请求，编写另一个表达式用于允许发送到“example-sports-football.com”的请求。创建 L7 策略以使拒绝请求的所有响应方策略排列在评估列表顶部，后面依次接着用于 Web 定向的响应方策略和内容交换策略。

在 Citrix ADM 中，始终存在与优先级为 1 的 csvServer 相关联的默认策略。此默认策略指定在任何给定时间点 lbvserver 应处理的 TCP 连接数。因此，当在 Citrix ADC 中创建相应的响应程序策略和内容交换策略时，它们的优先级总是高于相应 L7 策略的优先级 1。例如，如果 L7 策略的优先级为 1，则创建的内容交换策略的优先级为 2。同样，如果 L7 策略的优先级为 2，则创建的响应方策略的优先级为 3。

在 OpenStack 中，首先评估“reject”和/或“redirect_to_url”策略，然后评估“redirect_to_pool”策略。在 Citrix ADC 中，始终首先评估响应程序策略，以删除请求或向用户提供重定向的 Web 地址，最后评估内容切换策略。如果内容交换策略和响应方策略相互排斥，则此评估顺序通常不会导致出现任何冲突。即，任何两个 L7 策略不应有相似的表达式。应该在响应方策略和内容交换策略中添加相似的派生表达式以避免此类冲突。例如，编写一个表达式用于拒绝发送到“sports-football.com”的所有请求，编写另一个表达式用于允许发送到“example-sports-football.com”的请求。创建 L7 策略以使拒绝请求的所有响应方策略排列在评估列表顶部，后面依次接着用于 Web 定向的响应方策略和内容交换策略。

配置任务

通过 Neutron LBaaS 命令执行 L7 策略和操作实现。

在 OpenStack 中设置环境变量并创建负载平衡器（例如 LB1）。成功创建负载平衡器后，创建侦听器和池（例如 L1、P1 和 P2），并向池添加成员和监视器。例如，P1 是 L1 的默认池，P2 是绑定到 LB1 的池并管理应用程序服务器。

有关如何使用命令行配置 LBaaS V2 的更多信息，请参阅使用命令行 配置 LBaaS V2。

以下命令创建策略并定义特定操作：

创建用于丢弃请求的 **L7** 策略

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action<action-name>
```

示例：

neutron lbaas-l7policy-create -name policy11 -action REJECT -listener L1

上述命令创建响应方策略 policy11 并将其绑定到内容交换服务器以拒绝请求。由于没有为此策略创建规则，因此策略的评估结果为“false”并拒绝请求。

创建用于将请求重定向到特定 **URL** 的 **L7** 策略

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-url <redirect-url>
```

示例：

neutron lbaas-l7policy-create -name policy12 -action REDIRECT_TO_URL -listener admin-list1 -redirect-url http://example-sports/about-us.html

上述命令创建响应方操作以将请求重定向到 URL、创建具有操作的响应方策略以及将此策略绑定到内容交换虚拟服务器。

```
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>
```

可以使用 AND 运算符连接上述两个规则为响应方策略派生表达式。

创建用于将请求重定向到池的 **L7** 策略

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <
    listener name> --action <action-name> --redirect-pool <redirect-pool
    >
```

示例：

neutron lbaas-l7policy-create -name policy13 -action REDIRECT_TO_POOL -listener admin-list1 -redirect-pool admin-pool2

如果这是第一个 L7 策略，则上述命令将 P2 与 LB1 一起实现、创建内容交换重定向操作以及将请求重定向到 LB1。如果 P2 已存在，则该命令将创建内容交换重定向操作以及将请求重定向到 LB1。

在 **OpenStack** 上手动预配 **Citrix ADC VPX** 实例

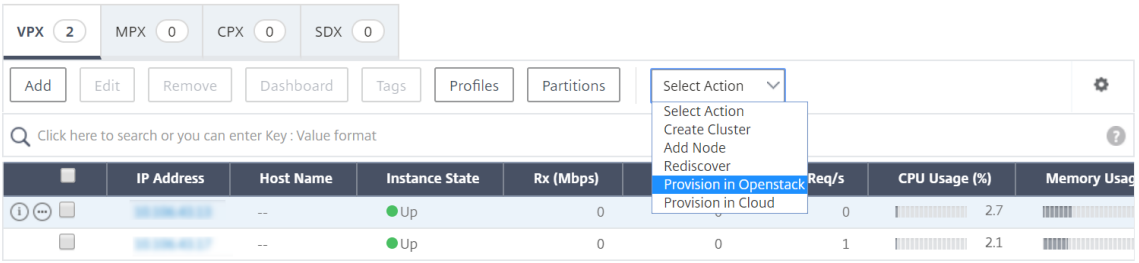
February 6, 2024

在少数企业网络中，出于安全原因，Citrix ADC VPX 实例无法连接到 Citrix 许可证服务器以自动下载许可证。在这种情况下，您需要在 OpenStack 平台上手动部署 Citrix ADC VPX 实例。使用您从 Citrix 收到的许可证激活码 (LAC)，下载相应的 Citrix ADC VPX 许可证并将其保存在本地系统中。

要在 **OpenStack** 上手动置备 **Citrix ADC VPX** 实例，请执行以下操作：

1. 在 OpenStack 上安装 Citrix ADC 驱动程序软件并注册 Citrix Application Delivery Management (ADM)
    a) 在 Citrix ADM 中，导航到“编排”>“云编排”>“**OpenStack**”。
    b) 单击“配置 **OpenStack** 设置”。在“配置 **OpenStack** 设置”页面中，您可以设置参数以在 Citrix ADM 中配置 OpenStack。这里有两个选项 - 默认和自定义。
    c) 如果 OpenStack 服务在默认端口上运行，选择 **Default**（默认）。
2. 导航到“调配”**>**“云 ****** 调配”>“**OpenStack**”，然后单击“部署设置”。******
    a) 管理网络 -选择 OpenStack 上的管理网络，自动配置的 Citrix ADC VPX 连接到该网络。
    b) 配置文件名称 -从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
    c) Citrix ADC VPX 映像概览-选择用于创建 Citrix ADC VPX 实例的 OpenStack 概览中可用的 Citrix ADC VPX 映像。该下拉列表将仅显示 OpenStack Glance 中已有的那些映像。
3. 在 Citrix ADM 中，导航到 编排 > 云 编排 > **OpenStack** > 服务包，然后单击“添加”。
4. 在“服务包”页面上，指定以下参数：
    a) 名称 -服务包的名称。例如，输入 SVC-PKG-GOLD。
    b) **Citrix ADC** 实例分配 -选择 专用 或 分区 作为服务包中定义的实例分配类型。
    c) **Citrix ADC** 实例预配 -选择 按需创建实例 以在配置期间创建 Citrix ADC 实例。
    d) 自动配置平台 -选择 **OpenStack** 计算。默认情况下，将选择 Citrix ADC VPX 作为实例类型。
    e) 分配 **OpenStack** 租户**/**安置政策-部分的 OpenStack 租户下方，单击“添加”，然后选择租户。
    f) 单击 **Continue**（继续），然后单击 **Done**（完成）。
5. 导航到“系统”>“系统管理”>“更改系统设置”，然后从下拉列表中选择 **http** 。
6. 导航到“网络”>“实例”>“**Citrix ADC VPX**”。

7. 在 **Citrix ADC VPX** 页中，单击 管理 下拉列表，然后选择 预配设备。



   a) 在“设备预配”页面上，输入设备的名称，然后选择您在上一步中创建的服务包。

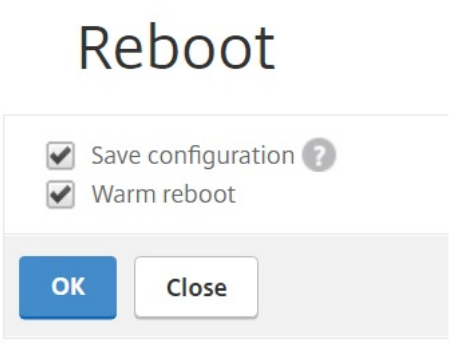
   b) 单击确定。

8. 导航到“调配”>“云调配”>“**OpenStack**”>“请求”选项卡。选择请求并单击“任务”以查看任务。当任务的状态更改为“已完成”时，这意味着 Citrix ADC VPX 是在 Citrix ADM 中置备的。

9. 导航到“网络”>“实例”>“**Citrix ADC VPX**”，检查 Citrix ADC VPX 实例是否显示在 Citrix ADC VPX 页中。

10. 单击 Citrix ADC VPX 实例。当 Citrix ADC VPX 系统在浏览器窗口中打开时，请登录到该实例。导航到“配置”>“系统”>“许可证”，然后手动添加新许可证。有关如何添加新许可证的详细信息，请参阅Citrix ADC 许可概述。

11. 重新启动 Citrix ADC VPX 实例。



12. 几分钟后，您可以登录到 OpenStack，并在系统 > 实例中，您可以看到 Citrix ADC VPX 实例部署在 OpenStack 上。

13. LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端，并执行配置任务。有关如何执行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

使用样书在 **OpenStack** 上预配 **Citrix ADC VPX** 实例

February 6, 2024

在 OpenStack 编排工作流程中，Citrix Application Delivery Management (ADM) 现在使用“os-cs-lb-mon”样本在分配给 OpenStack 租户的 Citrix ADC 实例上部署 LBaaS 配置。将为 OpenStack 用户创建的每个负载平衡器创建一个配置包。

在 OpenStack 工作流中使用样书进行配置可提供以下好处：

- 通过查看所有配置对象，更好地可视化。
- 通过回滚实现可靠性。
- 支持各种 Citrix ADC 实例类型（Citrix ADC HA、分区、VPX、CPX 和其他）。
- 通过使用自己的样书为 OpenStack 租户部署配置进行自定义。

作为 **Citrix ADM** 管理员，导航到“应用程序”**>**“配置”以查看在 **Citrix ADC** 实例上部署的配置包。
您可以执行以下任务：

- 滚动查看为负载平衡器部署的“os-cs-lb-mon”配置包。
- 在“os-cs-lb-mon”样书面板上单击“查看定义”以检查部署在实例上的配置。
- 单击 查看对象 可查看在实例上部署的 Citrix ADC 对象或实体的列表。

使用样书 **Provisioning** 实例之前的注意事项

从 Citrix ADM 12.1 版本 49.23 起，OpenStack 调配工作流程的架构已更新。该工作流程现在使用 Citrix ADM 样书来配置 Citrix ADC 实例。如果要从版本 12.0 或版本 12.1 版本 48.18 升级到 Citrix ADM 12.1 版本 49.23，则必须运行以下迁移脚本：

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- 运行迁移脚本会创建与现有 OpenStack 配置相对应的“os-cs-lb-mon”样本的配置包。
- 如果您从这些早期版本中部署了 OpenStack 配置，则必须运行此迁移脚本。
- 只有在运行版本 12.1 版本 49.23 的迁移脚本后，才能使用“os-cs-lb-mon”样书在实例上部署新配置。
- 在运行迁移脚本之前，从 OpenStack 尝试的所有配置都将失败。

> 注意
>
> - 运行迁移脚本后，无法降级到 Citrix ADM 的先前版本。
> - 确保您已将用于 OpenStack LBaaas V2 的 Citrix ADC 驱动程序升级到最新版本。使用与最新 Citrix ADM 12.1 版本 49.23 一起提供的 Citrix ADC 捆绑文件。

LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并执行配置任务。有关如何执行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

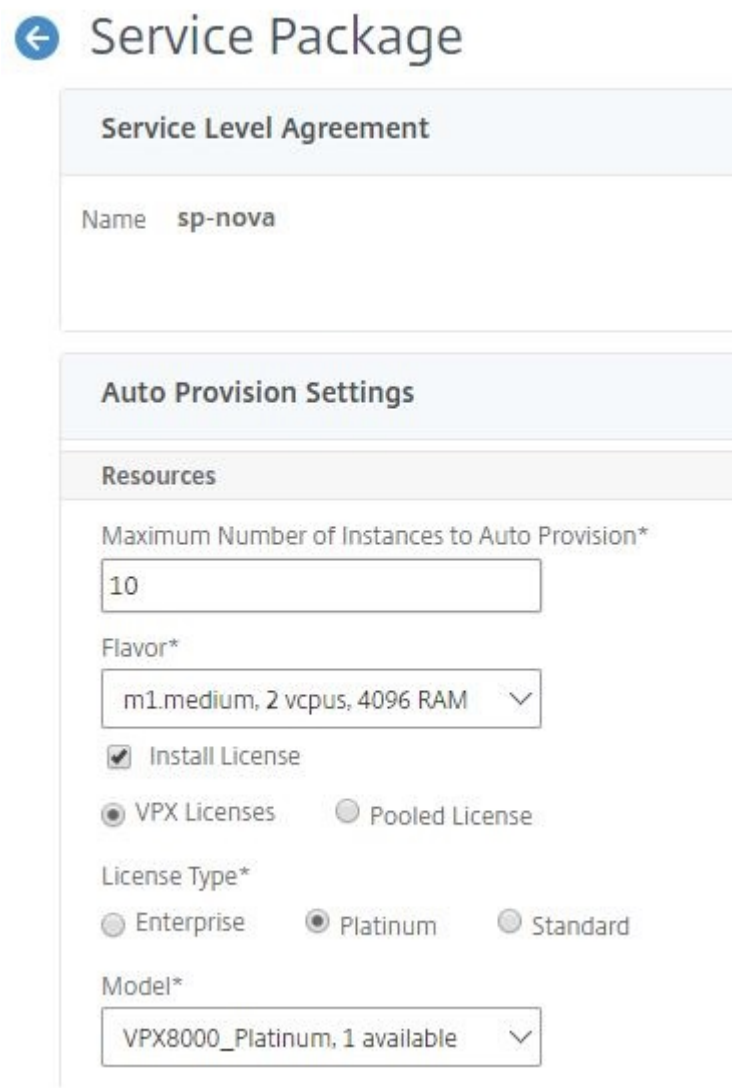
VPX 签入和签出许可证以及 OpenStack 环境的池许可证支持

February 6, 2024

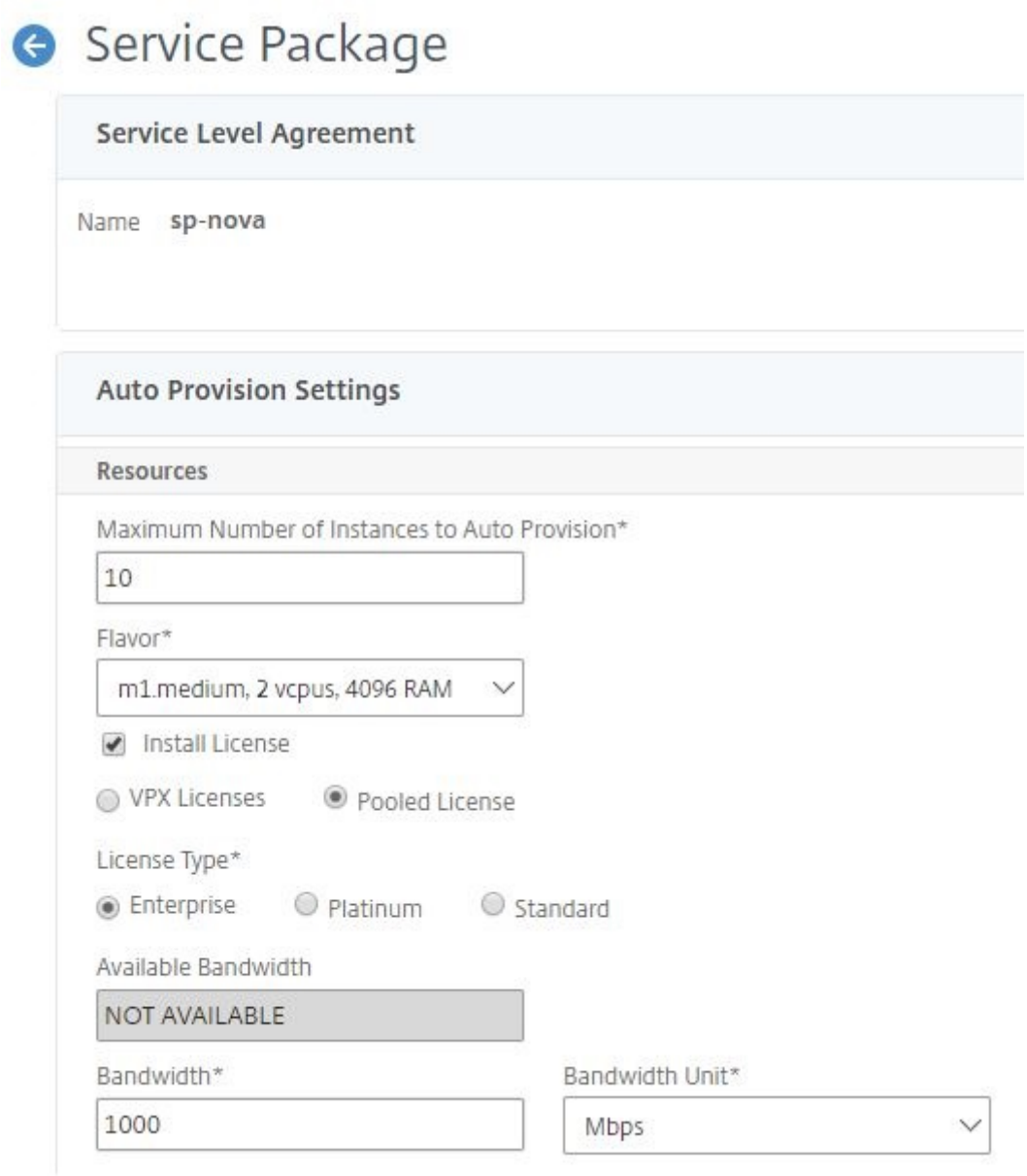
在 OpenStack 编排工作流中，当您选择使用 **OpenStack** 计算的服务包时，Citrix Application Delivery Management (ADM) 会根据需要创建 Citrix ADC VPX 实例。现在，Citrix ADM 中业务流程功能中的服务包页面得到了增强，以提供在按需创建的 Citrix ADC VPX 实例上安装所需的许可证。提供的许可证可以是 VPX 办理登机手续和签出许可证，也可以是共用许可证。

要使用此功能，必须先在 Citrix ADM 中上载许可，然后创建使用 OpenStack 计算的服务包。

- 如果是签入和签出许可证，则可以从各种可用许可证中选择要安装的许可证。



- 如果是池许可证，则可以同时选择要安装的带宽和许可证版本的类型。



每当您以 Citrix ADM 作为提供程序部署第一个负载平衡器时，Citrix ADM 都会创建 Citrix ADC VPX 实例，并将服务包中指定的许可证安装到新创建的实例。

此外，当您删除现有的负载平衡实例时，不再需要该实例。实例已停用，并将许可证返回到 Citrix ADM。这样可以优化使用 Citrix ADM 中提供的许可证。

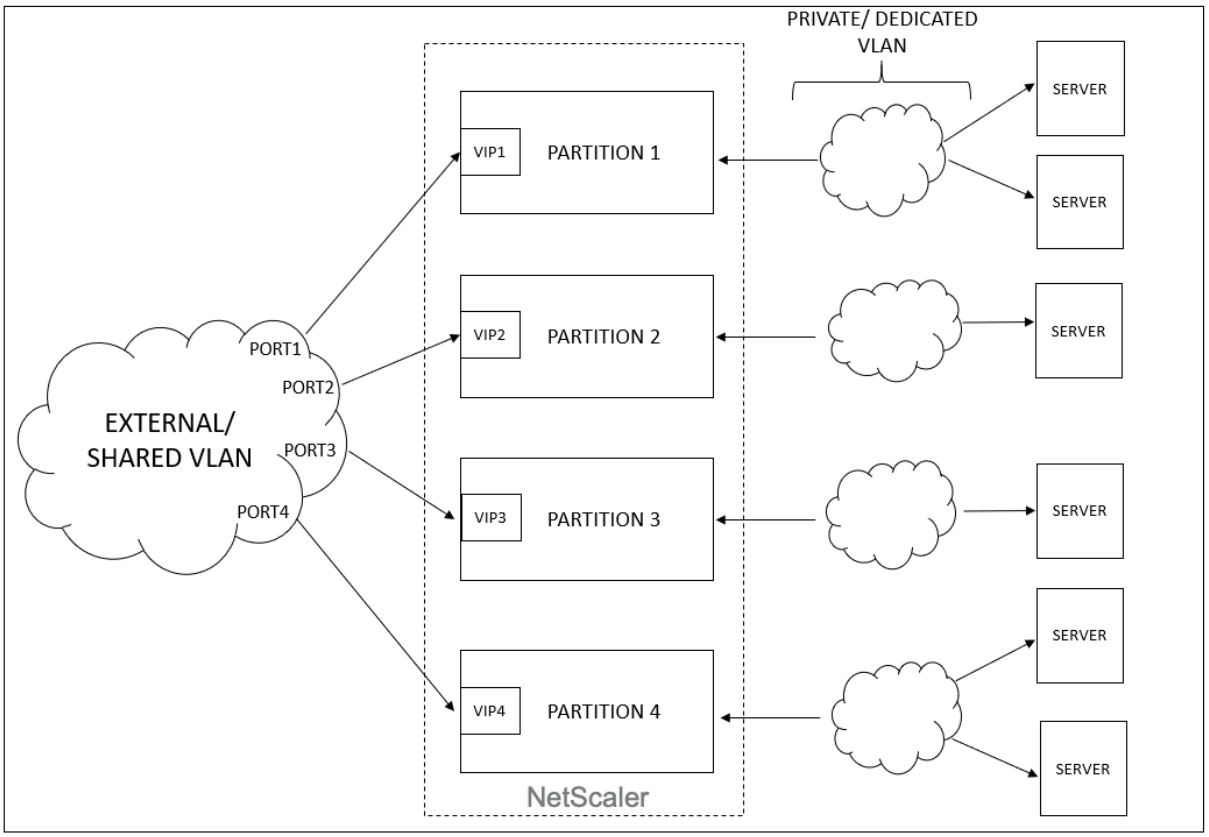
> 注
>
> 意当以高可用性模式部署 Citrix ADM 时，请考虑将许可证上载到当前处于活动状态或主要的 Citrix ADM MAS-HA-1。当您部署第一个请求并且 Citrix ADM 创建 Citrix ADC VPX 实例时，该实例将从 MAS-HA-1 中签出所需的许可证。在稍后的时间点，假定没有许可证的辅助 Citrix ADM MAS-HA-2 现在处于活动状态。ADC VPX 实例现在无法从 MAS-HA-2 签出许可证，因此无法为新用户创建该实例。

> 在这种情况下，确保 MAS-HA-1 已启动并且现在是当前的主节点。也就是说，手动故障切换 Citrix ADM 从 MAS-HA-2 到 MAS-HA-1。之后，您必须重新尝试从 OpenStack 进行配置，并使用适当的许可证重新创建实例。有关 Citrix ADM 高可用性部署中许可证支持的详细信息，请参阅 高可用性。

对管理分区的共享 **VLAN** 支持

February 6, 2024

对于通过专用网络连接的租户，Citrix Application Delivery Management (ADM) 支持隔离策略，因此每个租户都有自己的专用分区、专用 VLAN 和专用服务器。对于从公用网络连接的租户，专用虚拟 LAN 会要求使用太多的 IP 地址。共享虚拟 LAN 通过在每个分区上创建一个虚拟 IP 地址，由此创建一个单一 IP 子网，避免了此问题

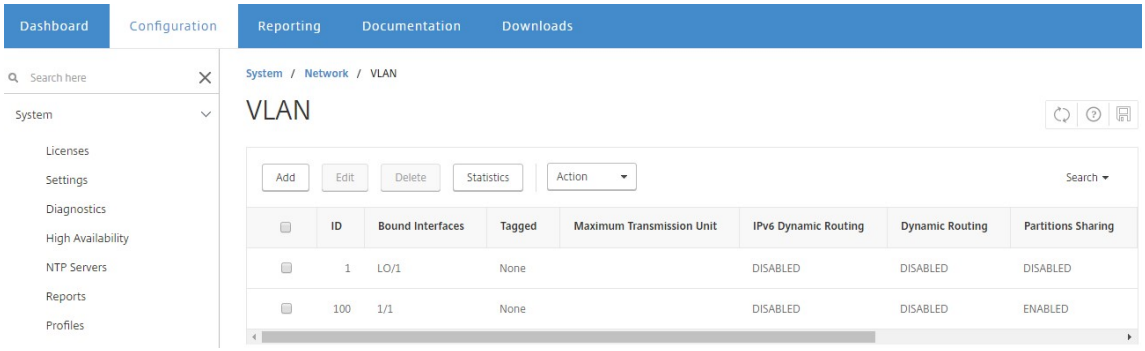


租户配置 VIP 或侦听程序时，系统会在 Citrix ADC 设备中为该租户创建管理分区。所有负载平衡器配置都会被推送到创建的管理分区。如果租户使用共享网络或外部网络创建负载平衡器，那么将会添加该网络的虚拟 LAN，并启用共享功能。当不同的租户使用同一个共享网络创建其负载平衡器时，VLAN 不会再次添加到 Citrix ADC，但该 VLAN 也会绑定到第二个分区。因此，使用相同共享网络的任何租户都将获得绑定到相同虚拟 LAN 的分区。

Citrix ADM 支持虚拟目标 MAC 地址。租户共享 VLAN 时，Citrix ADM 会为 Citrix ADC 设备上的分区分配不同的 MAC 地址。这样就可以在多个分区之间或所有租户和所有通信域之间共享虚拟 LAN。

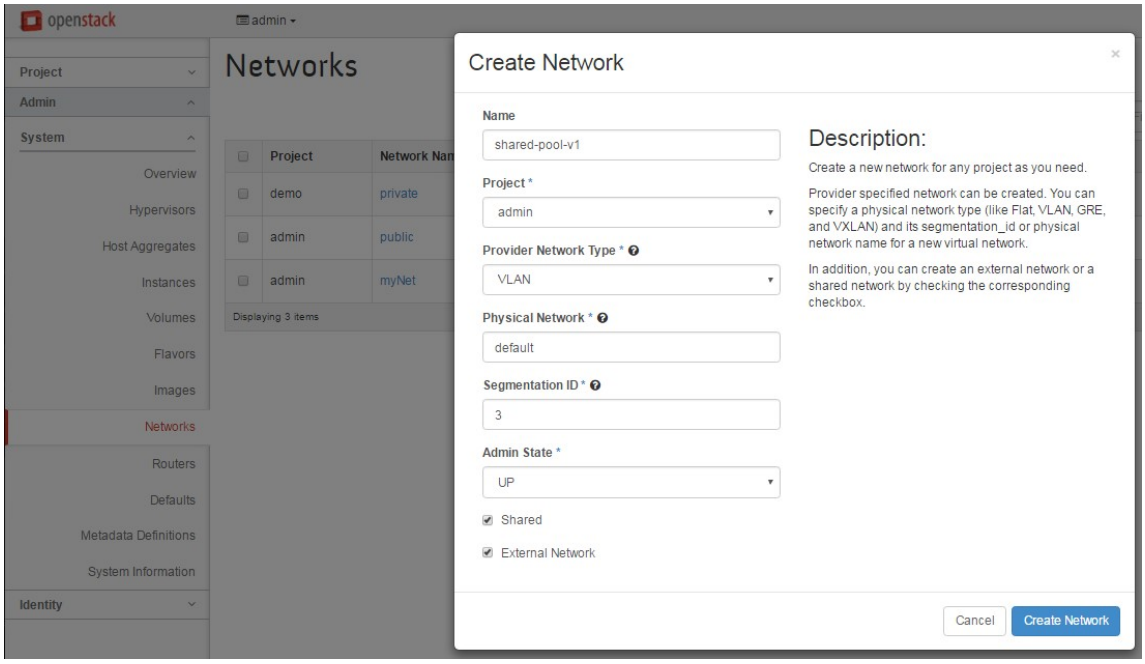
从 **Citrix ADC** 实例配置共享 **VLAN**

1. 在 Citrix ADC 实例中，导航到 配置 > 系统 > 网络 > **VLAN**，选择 VLAN 配置文件，然后单击“** 编辑”以设置分区共享参数。
2. 在 配置 **VLAN** 页面上，选中“分区共享”复选框。
3. 单击确定。



从 **OpenStack** 调配配置共享虚拟 **LAN**

1. 在 OpenStack 中，导航到“管理员”>“系统”>“网络”，然后单击“创建网络”。
2. 在 **Create Network**（创建网络）中，设置以下参数：
   a) Name（名称）- 输入网络的名称
   b) Project（项目）- 从下拉列表中选择项目
   c) 提供商网络类型-从下拉列表中选择 **VLAN** 。这定义虚拟网络建立为虚拟 LAN。
   d) Physical Network（物理网络）- 此处选择默认物理网络。可以编辑此项。
   e) Admin State（管理状态）- 默认情况下，网络的管理状态是“UP”（运行）
   f) 选择 **Shared**（共享）和 **External Network**（外部网络）定义共享虚拟 LAN 且虚拟 LAN 使用外部网络。
3. 单击 **Create Network**（创建网络）。



试用许可工作流程

February 6, 2024

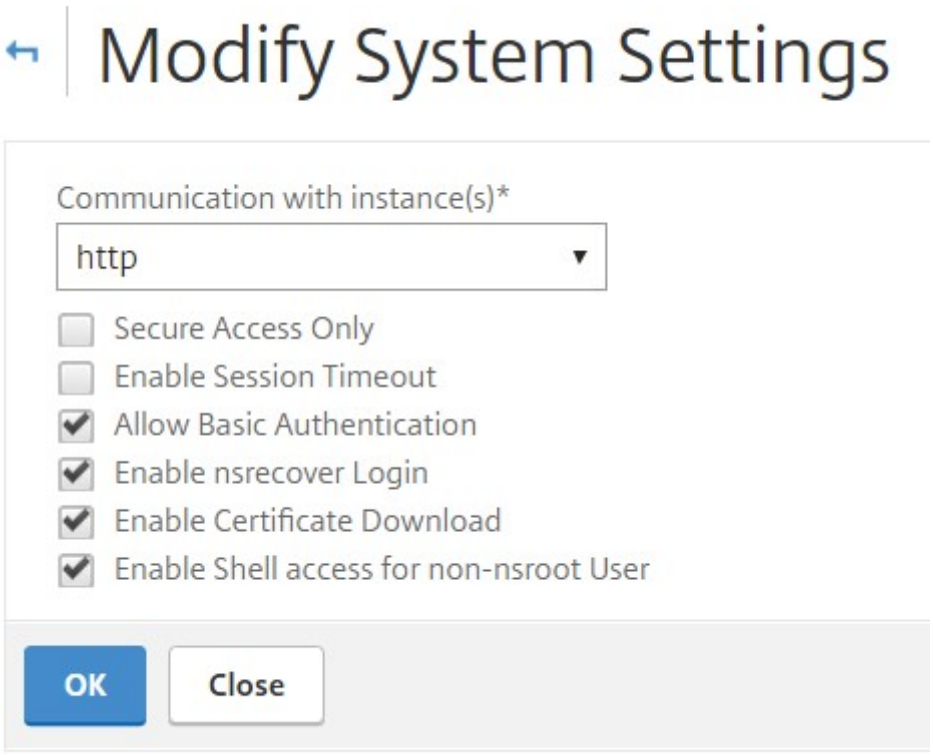
在使用 OpenStack 编排自动置备 Citrix ADC VPX 实例期间，Citrix Application Delivery Management (ADM) 使用 OpenStack 计算启动 Citrix ADC VPX 实例。新配置的 Citrix ADC VPX 实例在设置期间与 Citrix 许可门户联系，并使用许可证激活码 (LAC) 自动下载并安装许可证文件。

试用版许可证

技术支持人员在现场安装 Citrix ADM 和 Citrix ADC VPX 设备时使用试用许可证。适用于 Citrix ADC VPX 的试用或评估许可证的有效期为 90 天。如果需要评估多个 Citrix ADC 或在 90 天后延长测试，则需要申请新的评估许可证。Citrix ADM 为您提供了替代解决方案，而不是自动安装试用许可证文件。您可以手动下载许可证文件并将其安装到 Citrix ADC VPX 上，以完成实例的安装。

如果 Citrix ADC VPX 无法连接到互联网，请将 Citrix ADM 配置为充当 Citrix 许可门户的代理服务器，然后安装许可证文件。

具有试用许可证的 Citrix ADC VPX 实例只能在 HTTP 上与 Citrix ADM 进行通信。要在 Citrix ADM 中配置 HTTP 通信，请导航到 “系统” > “系统管理”，然后单击 “更改系统设置”。从下拉列表中选择 **http** 以设置通信方法，然后单击确定。



与 **OpenStack Heat** 服务集成

February 6, 2024

OpenStack Neutron LBaaS 面向应用程序支持核心负载平衡服务，例如，负载平衡、SSL 卸载和内容交换。LBaaS 通过 RESTful API 进行管理，租户可以使用该 API 进行创建、更新和删除 LBaaS 对象的 REST 调用。由于 LBaaS 提供负载平衡服务，因此在编排过程中不允许使用更高级的 Citrix ADC 功能。Citrix ADC 加热插件克服了这一限制。

Heat 调配服务

通过 OpenStack Heat 调配服务可以基于模板部署复杂的云应用程序。Heat 调配模板 (HOT) 以文本文件方式描述云应用程序的基础结构，用户可读写这些文件，且版本控制工具可以管理这些文件。编写这些模板使用的是结构化语言 YAML。HOT 模板允许您创建大多数的 OpenStack 资源类型，以及指定在其中定义的资源之间的关系。借助 Citrix ADC 热插件，您可以在任何 Citrix ADC 实例上配置高级应用程序交付 Controller (ADC) 功能。

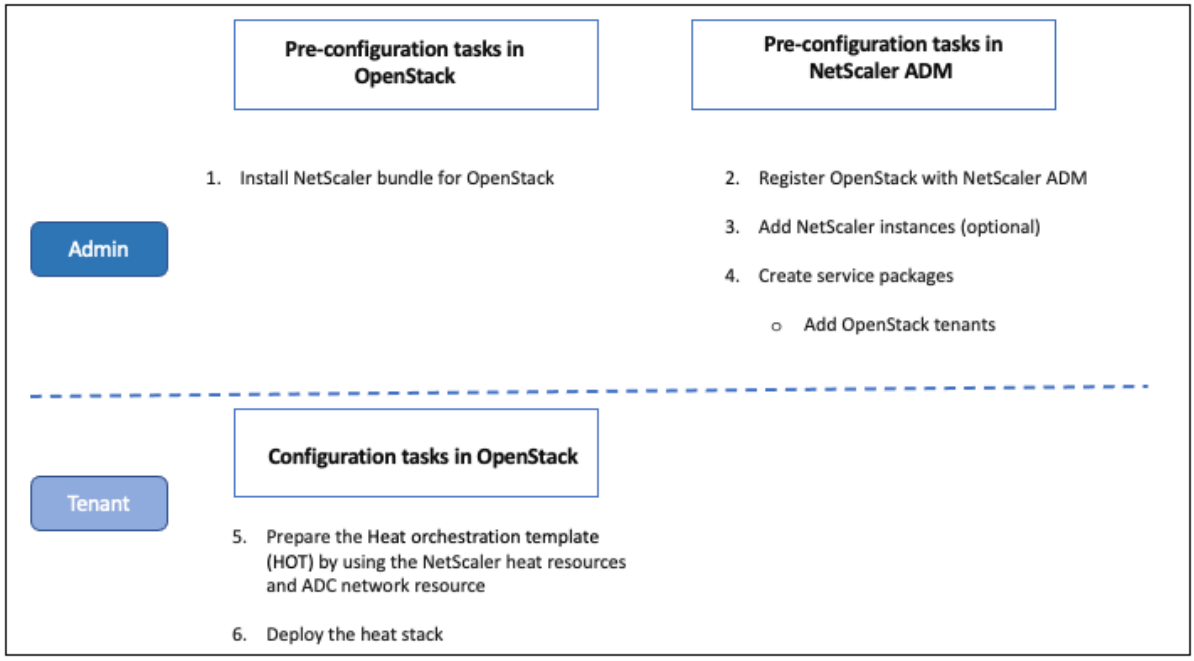
Citrix ADC 样书

Citrix Application Delivery Management (ADM) 样书可用于创建和配置 Citrix ADC 功能。与 Heat 模板一样，样书也是使用 YAML 编写的。可以为每个功能创建单独的样书，并且可以使用单个样书在多个 Citrix ADC 实例上部署配置。

在 Citrix ADC 与 OpenStack 集成期间，Citrix ADM 将所有 Citrix ADM 样书作为加热服务中的资源发布。这包括 Citrix ADM 附带的样书和用户在稍后时间点创建的样书。“热量”模板允许您使用这些样书资源配置 Citrix ADC 的高级功能。

使用热配置 Citrix ADC 实例的工作流

以下流程图说明了部署 Heat 堆栈的工作流：



以云管理员身份执行以下任务：

要在 **OpenStack** 中配置 **Heat** 服务：

1. 下载适用于 OpenStack 的 Citrix ADC 软件包

   在 OpenStack 中安装 Citrix ADC 软件包。在 Citrix ADM 中，导航到“下载”并下载 Citrix ADC 驱动程序包，解压缩捆绑包，然后将捆绑包中 Heat 文件夹的内容复制到 OpenStack 中的 Heat 引擎 资源 目录中。目录路径如下所示：

   /opt/stack/heat/heat/engine/resources/netscaler_resources

2. 在 heat.conf 文件中创建一个“netscaler_plugin”部分，然后更新该部分中的以下参数：

   [netscaler_plugin]

a) 如果通信为 http，则参数更新如下：

NMAS_BASE_URI=<http://10.146.103.45:80>

NMAS_USERNAME=

NMAS_PASSWORD=

b) 当通信为 https 时，参数更新如下：

NMAS_BASE_URI=https://common_name_used_in_certificate

NMAS_USERNAME=<openstack_driver_username

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH=<path_of_the_certificate_file>

如果用户将 ssl_cert_verify 设置为“假”，则 Citrix ADM 会在请求调用中发送 verify=False，这将禁用 SSL 证书验证。如果将 SSL_cert_ 验证设置为“True”并且存在证件路径条目，则 Citrix ADM 会在请求的验证参数中发送此路径，否则 Citrix ADM 会发送“验证”= True。

> 注意
>
> 要在“高可用性”模式下部署 Citrix ADM，请更新 heat.conf 文件中的以下参数：
>
> NMAS_BASE_URI=<ip address of the front-end virtual server>

3. 在 OpenStack 中重新启动加热服务。

   在 OpenStack 中重新启动 Citrix ADC 加热服务时，所有定义的 Citrix ADM 样书都将作为资源导入到热量中。此外，Citrix ADC 网络资源和证书资源将作为 Citrix ADC 热量资源导入 OpenStack。

4. 注册 Citrix ADM 与 OpenStack.

   a) 在 Citrix ADM 中，导航到 编排 > 云编排 > **OpenStack**，然后单击“配置 **OpenStack** 设置”。

   b) 在 配置 **OpenStack** 设置 页面中，您可以设置用于配置 OpenStack 的参数。此处有两个选项：“Default”（默认）和“Customized”（自定义）。

   c) 如果 **OpenStack** 服务在默认端口上运行，请选择默认。输入以下参数：

      i. OpenStack 控制器 IP 地址

      ii. 管理员用户名

      iii. 密码

      iv. 开放式堆栈管理租户

      v. Citrix ADC 驱动程序和热密码

> 注意
>
> 这与您在 heat.conf 文件中输入的密码 (NMAS_PASSWORD) 相同。

5. 创建服务包并与租户定义 SLA。

   在 OpenStack 注册期间，在 Citrix ADM 中为每个用户创建租户，并且租户信息由 LBaaS 驱动程序和热插件使用。“热量”插件使用此信息与 Citrix ADM 联系，将样书作为热量资源导入 OpenStack 中。

   > 注意
   >
   > 有关在 Citrix ADM 和 OpenStack 中创建服务包和其他预配置任务的更多信息，请参阅 将 Citrix ADM 与 OpenStack 平台集成。

6. 观察到 Citrix ADM 中的所有相关样书都作为资源导入到 OpenStack 热量中。此外，请观察 Citrix ADC 网络资源和 Citrix ADC 证书资源已作为资源导入 OpenStack 热量。

   > 注意
   >
   > 目前，您只能使用 Citrix ADM 附带的样书。

   您的租户现在可以在 OpenStack 中创建 Heat 模板、输入所需 Heat 参数的值以及部署 Heat 堆栈。部署热量堆栈后，配置将推送到 Citrix ADM，并配置所需的 Citrix ADC 实例。

要准备热火模板并启动 **Heat** 堆栈，请执行以下操作：

1. 在 OpenStack 中，租户可以使用 Heat 资源创建 Heat 调配模板 (HOT)。
2. 在 OpenStack Horizon 中，租户管理员可以导航到项目 > 调配 > 堆栈 来创建 Heat 模板并启动 Heat Stack。创建 HOT 的方法有两种：

   - 文件 -从本地目录中选择更新的模板
   - 直接输入 -将模板中的 YAML 内容复制并粘贴到窗口中

   > 注意
   >
   > 成功部署堆栈后，租户可以使用更改堆栈模板更新堆栈。但不能修改创建堆栈时最初提供的子网信息和虚拟 IP 地址 (VIP)。

   租户部署堆栈后，导航到“编排”>“云编排”>“**OpenStack**”>“**Citrix ADM** 中的请求”，以观察任务列表。此外，在 Citrix ADM 中导航到 “应用程序”> “配置”，观察是否已成功以样书配置包的形式配置 Citrix ADC 实例。

Citrix ADM 样书的示例：

下图显示了如何构建 Citrix ADM 样书的示例，并简要说明了这些组件。有关 Citrix ADM 样书以及如何使用附带的样书的详细信息，请参阅 样书。


```
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

热模板示例：

下图显示了 YAML 中定义的“热量”模板的结构，并指向作为“热量”资源导入的样书资源和 Citrix ADC 网络资源。

```
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

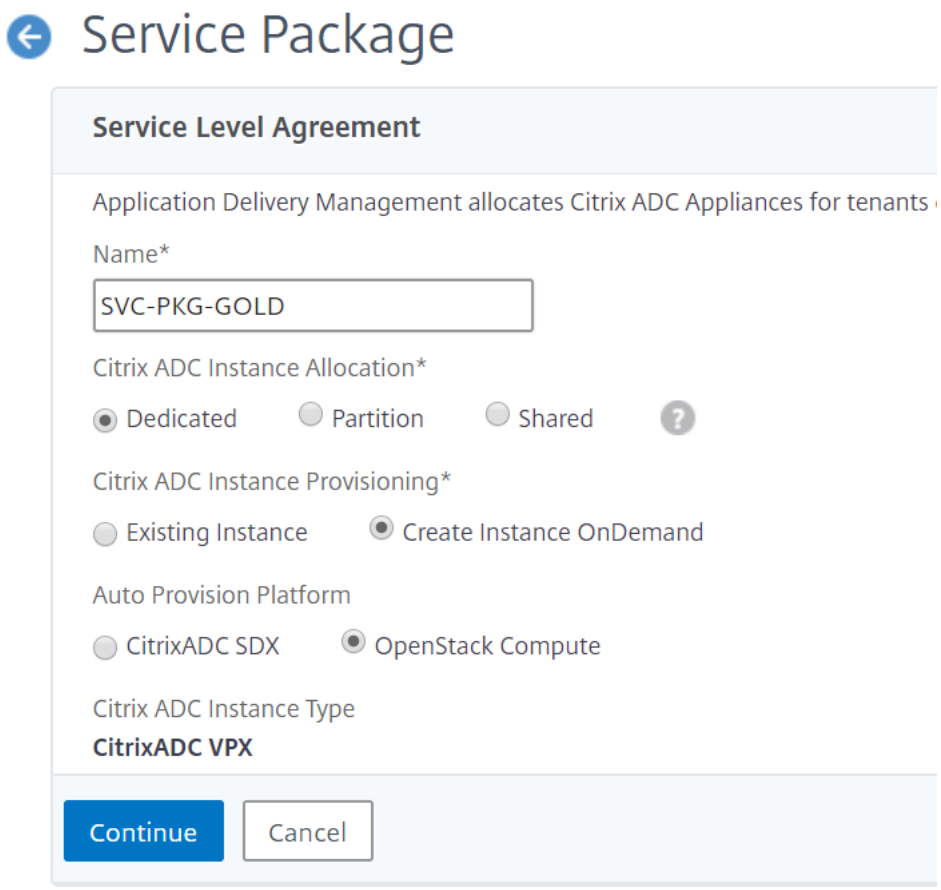
有关 Heat 服务以及如何创建模板的更多信息，请参阅OpenStack Heat 文档。

服务包隔离策略

February 6, 2024

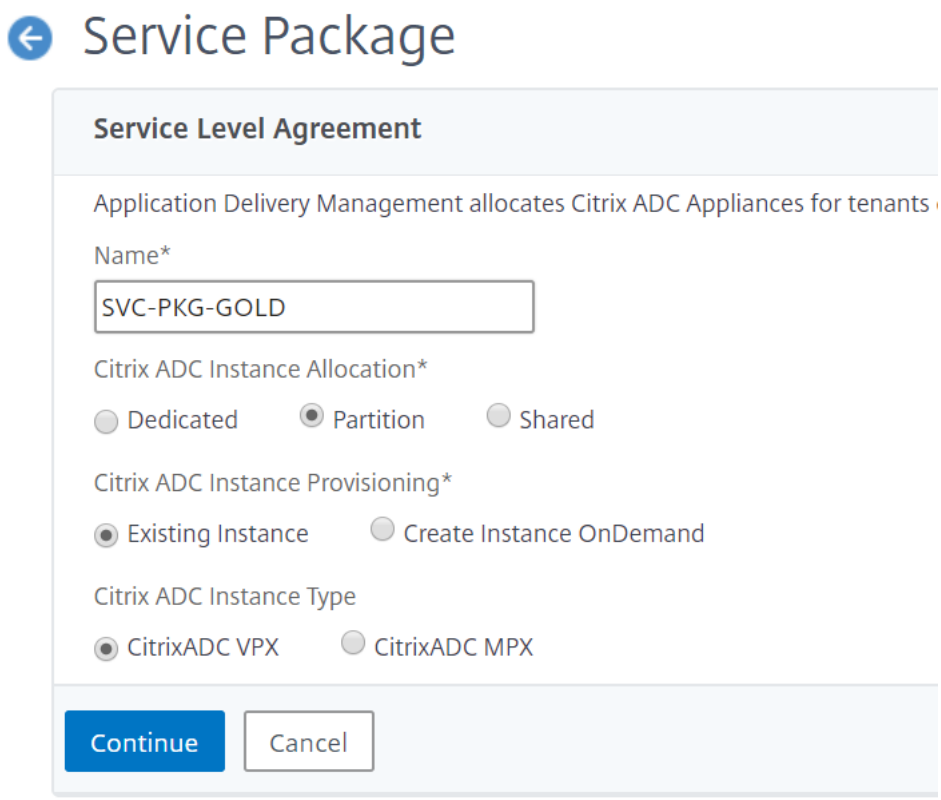
专用隔离策略

与专用策略的 Citrix Application Delivery Management (ADM) 服务包关联的每个租户都会从属于此服务包的实例中分配一个 Citrix ADC 实例。此分配的 Citrix ADC 实例不与其他租户共享。



分区隔离策略

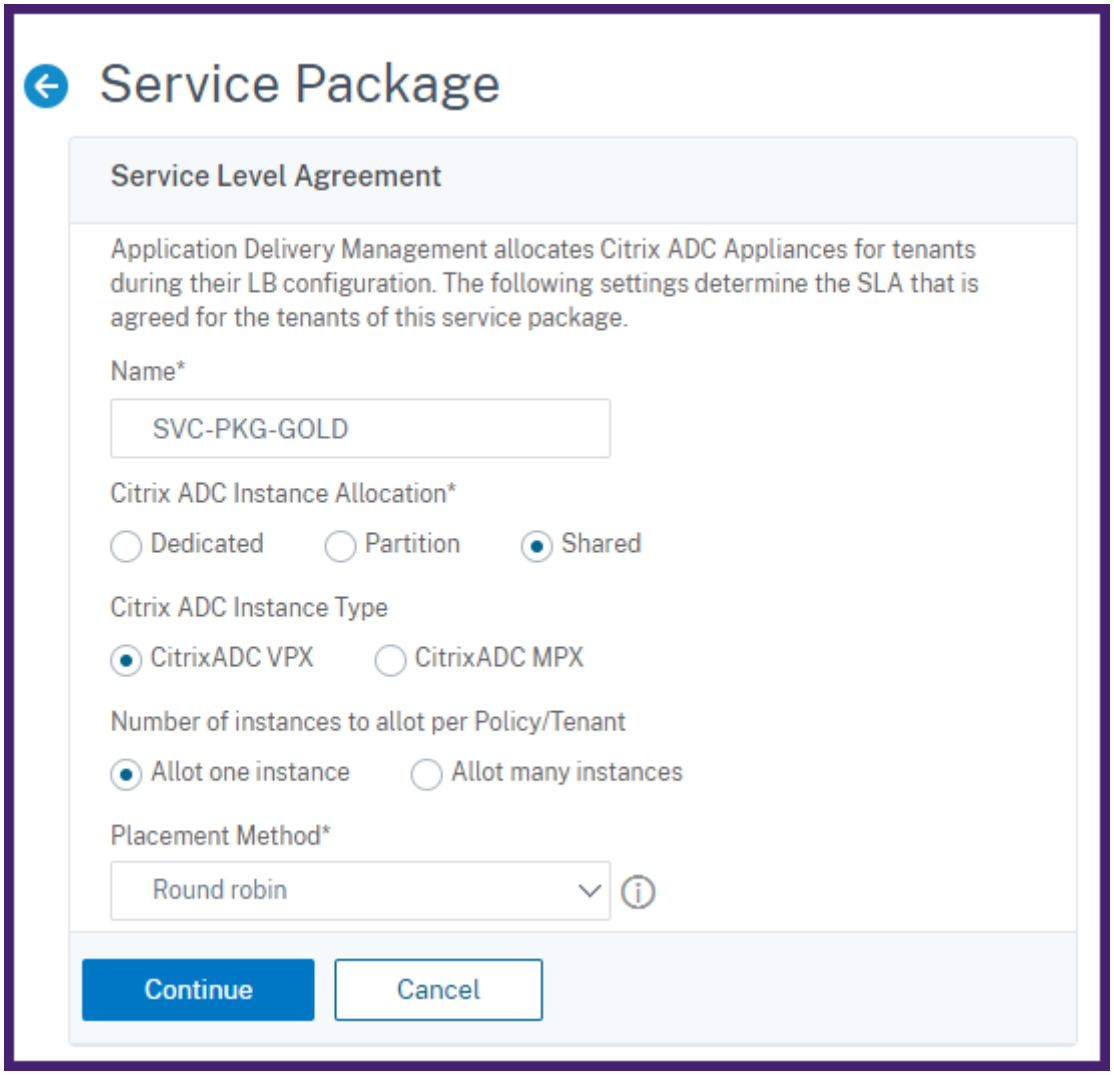
与分区策略的服务包关联的每个租户都会分配一个属于服务包的 Citrix ADC 实例的专用逻辑管理分区。



共享隔离策略

与服务包关联的租户共享作为服务包一部分的 Citrix ADC 实例。租户的所有配置都分配给一个 Citrix ADC 实例。在此模式下，多个租户的配置可以托管在同一 Citrix ADC 实例上。您可以选择 **Citrix ADC VPX** 或 **Citrix ADC MPX** 作为设备类型。您可以选择仅为服务包分配一个 Citrix ADC 实例或多个实例。也就是说，多个租户可以共享 Citrix ADC 设备的一个或多个虚拟实例。

> 注意：
>
> 将服务包中的 Citrix ADC SDX 实例仅作为 Citrix ADC VPX 实例添加为 Citrix ADC SDX 实例，因为 Citrix ADC SDX 具有预配置的 Citrix ADC VPX。



> 注意
>
> 还可以创建灵活的放置策略，这些策略不仅基于租户名称或 ID，而且基于其他自定义属性。有关灵活的放置策略的详细信息，请参阅基于策略的灵活设备分配。

灵活的基于策略的设备分配

February 6, 2024

Citrix Application Delivery Management (ADM) 会根据与租户商定的 SLA 将 Citrix ADC 虚拟实例分配给租户。为租户分配虚拟实例会在实例和租户之间建立一对一的关系，此时只能为租户分配数据中心里的一个服务包。

有些情况下，租户可能需要多个实例，或者实例分配可能不是基于作为条件的租户，而是基于其他因素，例如，网络 ID 或应用程序。在这种情况下，Citrix ADM 允许您根据用户定义的表达式精确定义放置策略，以便为其中一个托管实例分

配负载平衡器配置。

放置策略使您可以灵活地决定用户创建的每个负载平衡器配置中使用的 Citrix ADC 实例。Citrix ADM 中的灵活放置策略为基于租户分配 Citrix ADC 实例的现有方法提供了一个附加选项。

> 注意
>
> 您可以手动为租户分配实例，也可以基于创建的表达式使用放置策略来分配实例。不能对单个服务包同步使用这两个方法。

放置策略是基于对主要 LBaaS 配置对象（例如池和负载平衡器）的属性定义布尔表达式。Citrix ADM 中的放置策略用户界面提供了预定义的表达式，您可以从中进行选择，以定义自定义策略。可以针对不同的表达式创建多个放置策略。因此，每个租户可以有多个按租户要求定义的设备。

必须先选择表达式以匹配以后必须配置的根对象。对于 LBaaS V1，根对象可以是池对象；对于 LBaaS V2，根对象可以是负载平衡器对象。因此，LBaaas V1 和 V2 API 都支持基于 Citrix ADM 策略的放置。之后这些放置策略与服务包关联。根对象放置在实例中后，模型中连续的对象都会添加在该实例中。

例如，池配置对象可以有以下属性：

- tenant_id
- name
- description
- protocol
- lb_method
- subnet_id
- subname_name
- admin_state_up
- status
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

下面的示例中显示了一些使用池属性为策略定义表达式的表达式：

1. 基于池名称的策略表达式

   配置 [“池”] [“名称”] ==“高端池”

2. 基于池子网名称的策略表达式

   配置 [“池”] [“子网名称”] == “us-west-payment-subnet1”

3. 基于负载平衡器子网名称的策略表达式

   配置 [“负载平衡器”] [“子网名称”] == “mas-subnet”

添加放置策略

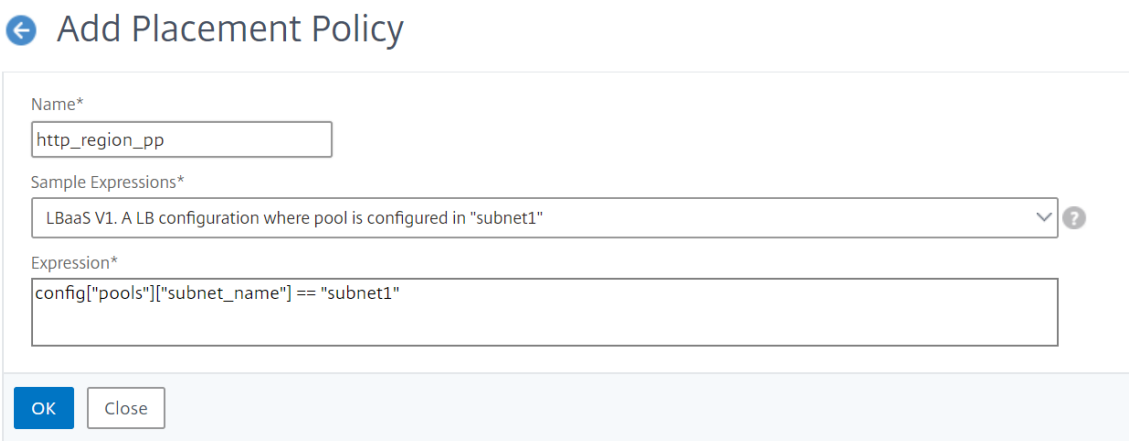
1. 在 Citrix ADM 主页上，导航到 “** 编排” > “云 ** 编排 ” > “放置策略”，然后单击 “添加”。
2. 在 **Add Placement Policy**（添加放置策略）页面上，设置以下参数：

   a) Name（名称）- 键入放置策略的名称

   b) Frequently Used Expressions（常用表达式）- 从下拉列表中选择表达式。

   c) Expression（表达式）- 根据在前面的字段中选择的表达式，在此字段中填充一个逻辑（布尔）表达式。根据需要编辑字段名称。

> 注意：创建多个策略
>
> 时，请确保这些策略彼此独占。



3. 单击确定。
4. 导航到 “调配” > “云调配” > “OpenStack” > “服务包”，然后单击 “添加”。
5. 在 服务包 页面上，设置以下参数：

   a) 名称-键入服务包的名称

   b) 隔离策略-选择 共享 策略

   在共享隔离策略中，租户的负载平衡器配置与分配给该租户的设备中其他租户的负载平衡器配置共存。

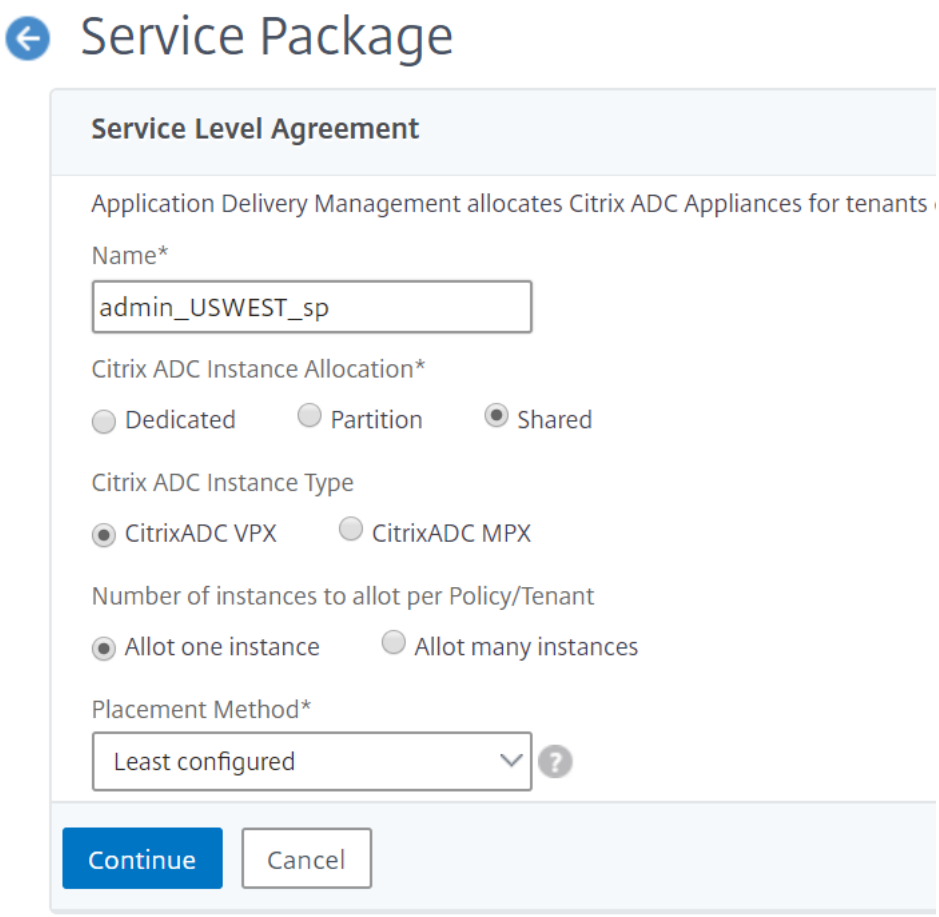
c) 设备类型-选择预置备的 **Citrix ADC VPX** 或 **Citrix ADC MPX**

如果希望租户的所有负载平衡器配置绑定到一个设备，请选择 **Allot one device**（分配一个设备）。如果希望租户的每个负载平衡器配置根据放置策略分发在数个设备上，请选择 **Allot many devices**（分配多个设备）。

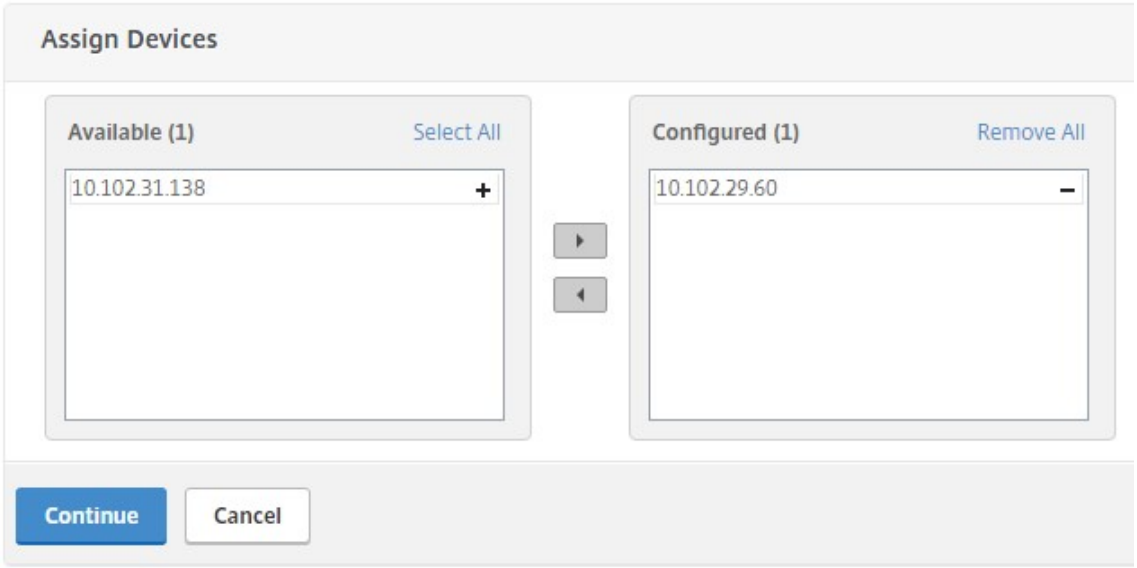
> 注意：必须将
>
> Citrix ADC SDX 作为仅在服务包中添加为 Citrix ADC VPX 实例，因为 Citrix ADC SDX 在其上配置了 Citrix ADC VPX。

d) 放置方法-选择 最低配置

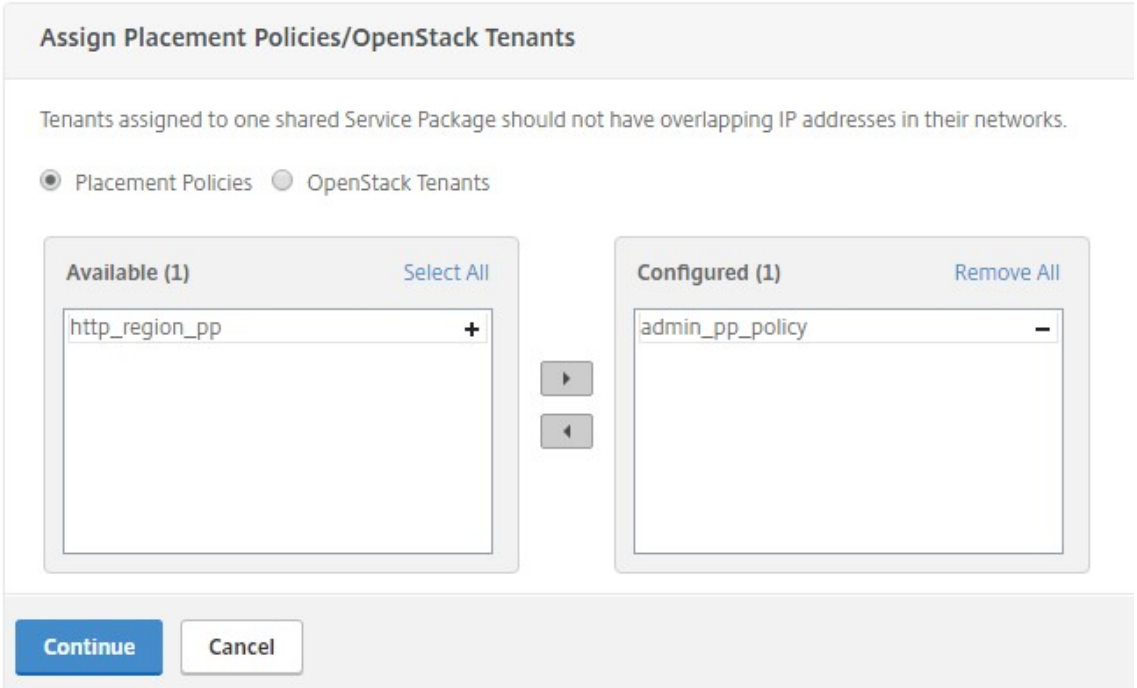
选择“最少配置”时，将选择在该时间点配置的池成员数量最少的 Citrix ADC 实例作为租户的设备。



6. 单击继续。
7. 在“分配设备”部分，将可用的 Citrix ADC 设备添加到已配置的设备列表中。



8. 单击继续。
9. 在 分配置放置策略/**OpenStack** 租户 部分中，添加您之前创建的放置策略。



> 注意：
>
> 如果未找到策略，则会恢复回退机制，并且 Citrix ADM 会根据租户分配 Citrix ADC 实例。如果租户不是任何服务包的一部分，Citrix ADM 将显示一条错误消息：“Tenant <admin> 不是任何服务包的一部分，也没有默认的服务包。”

10. 单击 **Continue**（继续），然后单击 **Done**（完成）。

NSX 管理器：手动预配 Citrix ADC 实例

February 6, 2024

Citrix Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动执行 Citrix ADC 服务的部署、配置和管理。此集成抽象出了与物理网络拓扑相关的传统复杂性，使 vSPhere/vCenter 管理员能够更快地以编程方式部署 Citrix ADC 服务。

本文提供了必须在 VMware NSX 管理器和 Citrix ADM 上执行的任务列表。

> 注意
>
> 确保已安装和配置适用于 vSphere 6.2 及更高版本的 VMware NSX，并且已经创建了必须进行负载平衡的边缘网关、DLR 和虚拟机。

必备条件

- 在满足最低要求的硬件上安装 VMware ESXi 4.1 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 在满足最低系统要求的管理工作站上安装 VMware 开放式虚拟化格式工具（VMware ESXi 4.1 版需要）。
- 在任何支持的虚拟机管理程序上安装 Citrix ADM。

  有关在任何受支持的虚拟机管理程序上安装 Citrix ADM build 12.1 的任务，请参阅 部署 Citrix ADM。

VMware ESXi 硬件要求

下表列出了 VMware ESXi 服务器上安装 Citrix ADM 虚拟设备所需的虚拟计算资源。

组件	要求
RAM	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 Gbps

> 注意：
>
> 上面指定的内存和硬盘要求用于在 VMware ESXi 服务器上部署 Citrix ADM（考虑到主机上没有其他虚拟机）。对 VMware ESXi 服务器的硬件要求取决于在其中运行的虚拟机数。

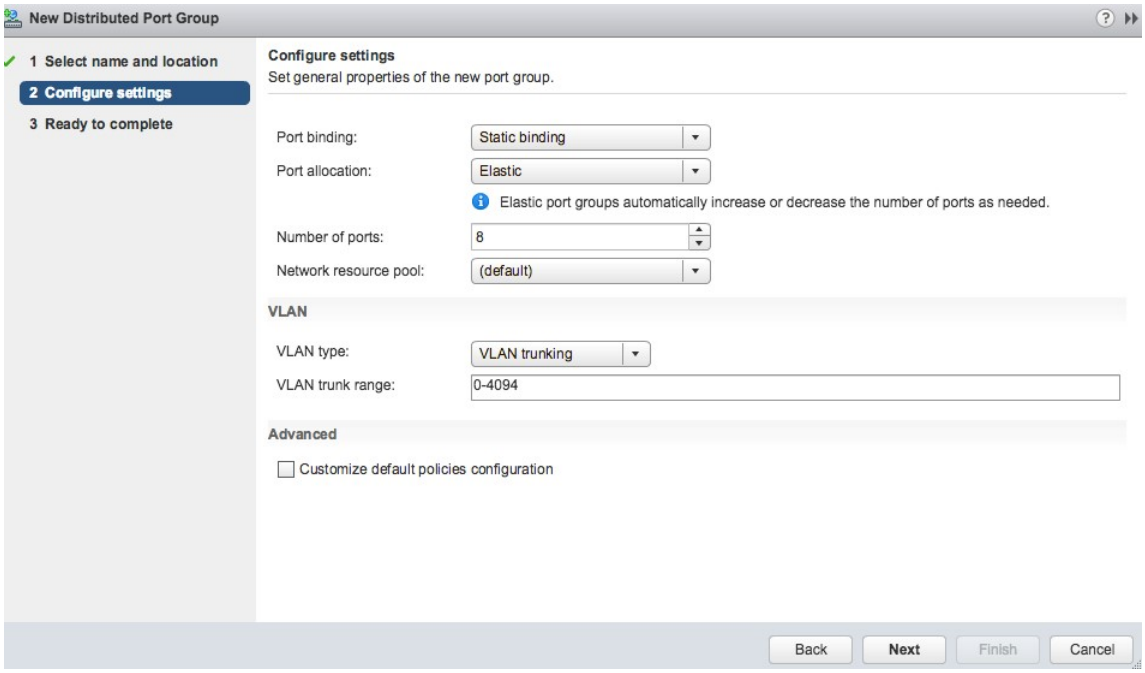
配置 **VMware NSX**

- 创建具有不同容量的 Citrix ADC VPX 实例池，这些实例将添加到不同服务包中。

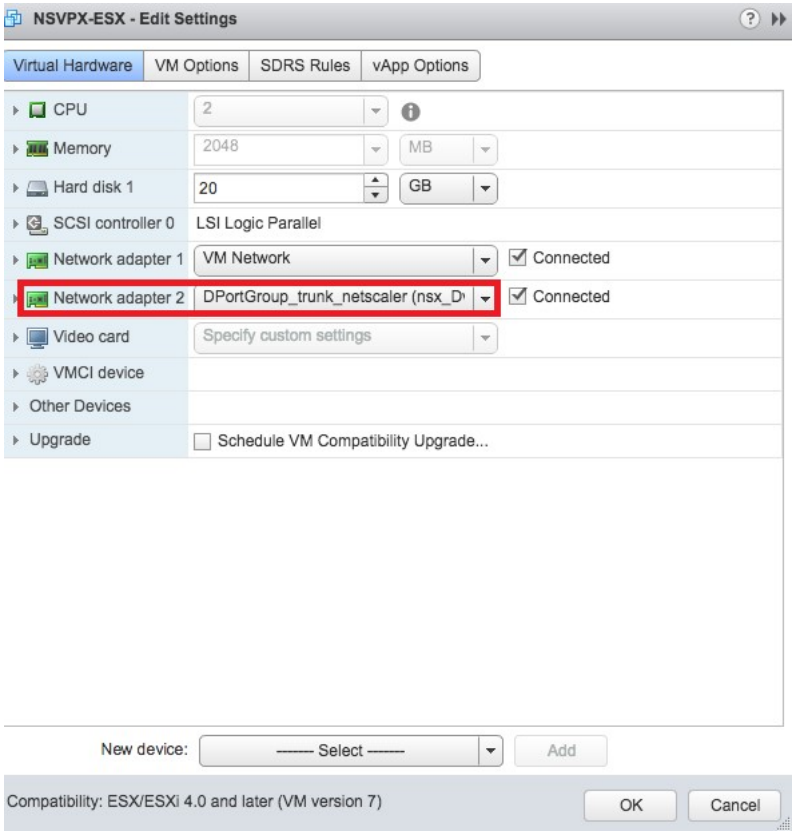
例如：

- 创建五个 VPX1000（1 Gbps）的 Citrix ADC VPX 实例。这些实例添加到金牌级服务包。
- 创建五个 VPX10（10 Mbps）的 Citrix ADC VPX 实例。这些实例添加到铜牌级服务包。

1. 在 vSphere Client 中，导航到 **Networking**（网络连接），创建类型为虚拟 LAN 的 Trunk 端口组，且设定范围（例如 101-105）（甚至可以提供全范围，但仅为所需的虚拟 LAN 创建类型为虚拟 LAN 的端口组）。

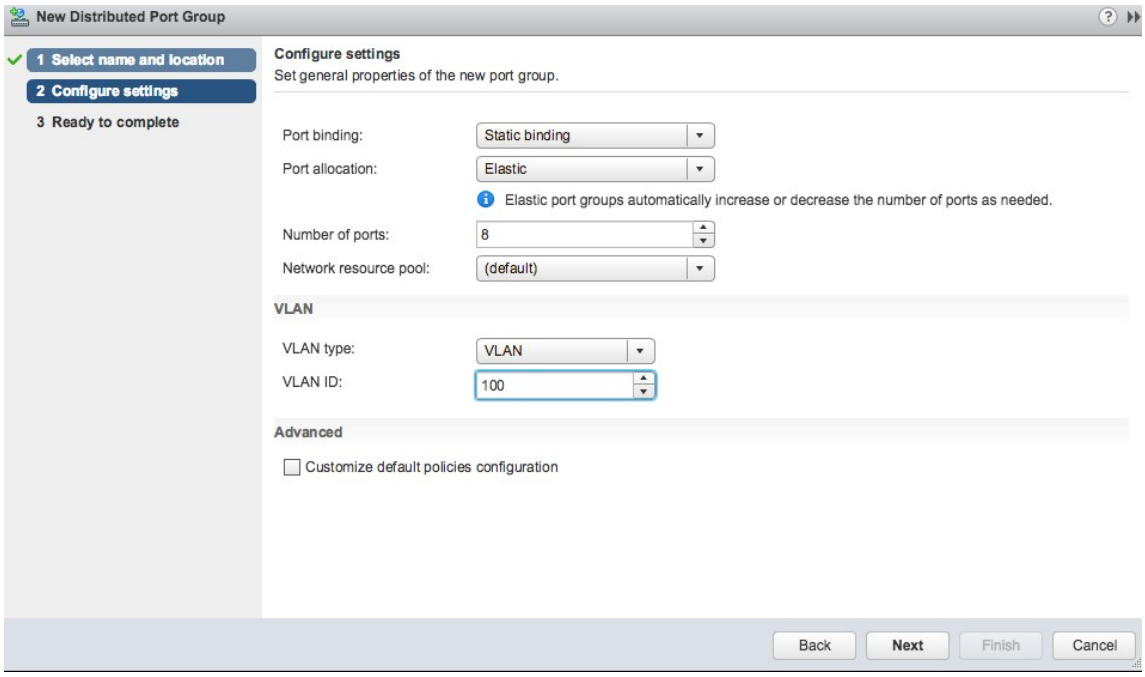


2. 为每个 Citrix ADC VPX 实例创建一个新接口，并将其连接到上面创建的 VLAN 范围中继端口组。



3. 在 vSphere Client 中，导航到 **Networking**（网络连接），创建类型为虚拟 LAN 的端口组。

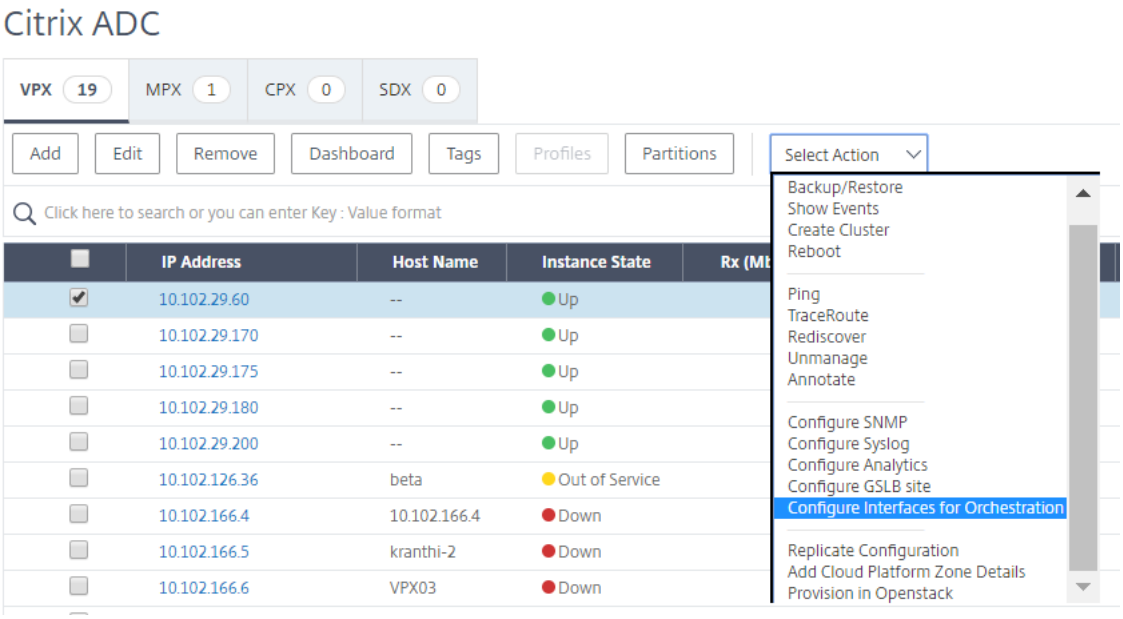
   例如，如果创建了范围是 101-105 的初始 Trunk 端口组，则创建五个虚拟 LAN 端口组（每个虚拟 LAN 一个端口组），即虚拟 LAN 101 一个端口组，虚拟 LAN 102 另一个端口组，依次类推，直至虚拟 LAN 105。



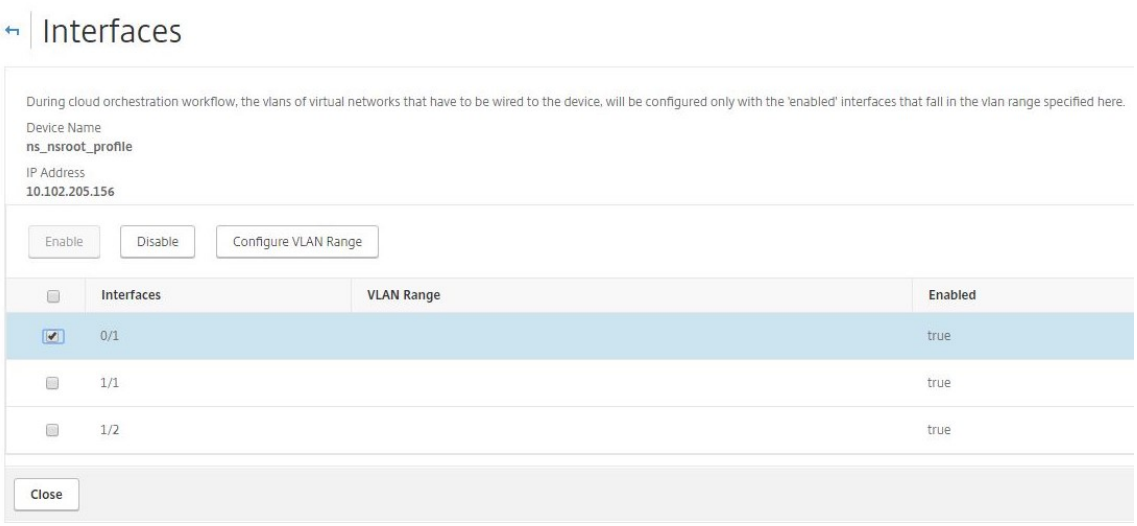
在 **Citrix ADM** 中添加 **Citrix ADC VPX** 实例

在 Citrix ADM 中添加 Citrix ADC VPX 实例，并为每个设备指定中继组的 VLAN 范围。

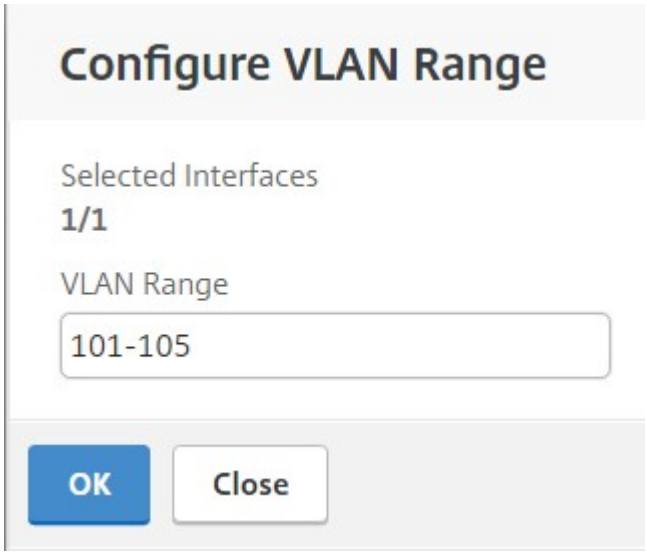
1. 在 Citrix ADM 中，导航到基础架构 > 实例 > **Citrix ADC VPX**，然后单击“添加”。
2. 在“添加 **Citrix ADC VPX**”页上，指定实例的主机名、每个实例的 IP 地址或 IP 地址范围，然后从“P**rofile** 名称”列表中选择实例配置文件。还可以单击 + 图标创建新实例配置文件。
3. 单击确定。
4. 从 Citrix ADC VPX 页面的列表中选择新添加的 **Citrix ADC VPX** 实例，然后单击“操作”字段中的向下箭头按钮 **。选择 ****Configure Interfaces for Orchestration**（为调配配置接口）。



5. 在“接口”页面上，选择管理接口，然后单击“禁用”以禁止 VLAN 绑定到管理接口。



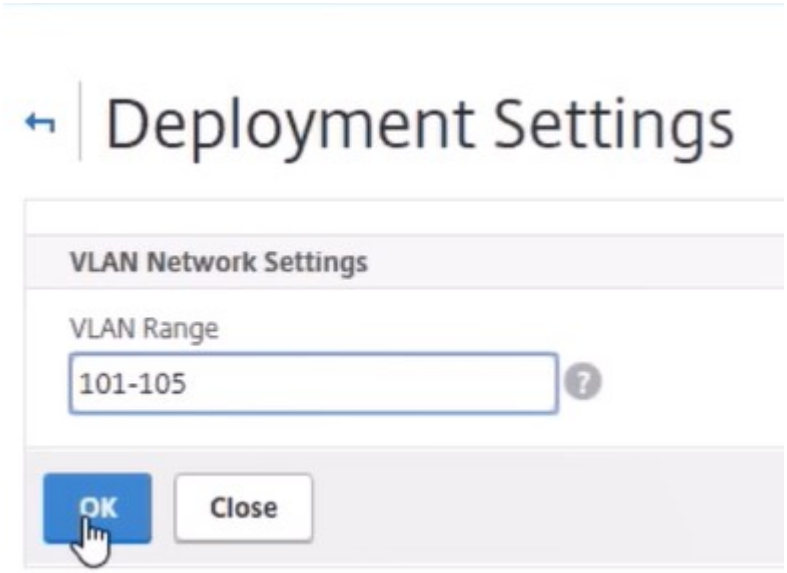
6. 在“接口”页面上，选择所需的接口，然后单击“配置 **VLAN** 范围”。
7. 输入 NSX Manager 中配置的 VLAN 范围，单 击确定，然后单击 关闭。



在 **Citrix ADM** 中注册 **VMware NSX** 管理器

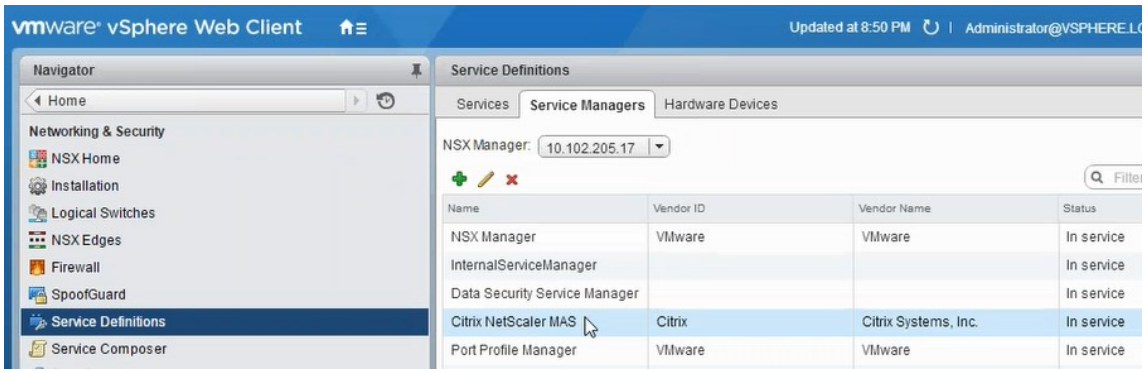
在 Citrix ADM 中注册 VMware NSX 管理器，以便在它们之间创建通信通道。

1. 在 **Citrix ADM** 中，从下拉列表中导航到“编排”>“SDN 编排”**>**“VMware NSX 管理器”，然后单击“配置 NSX 管理器设置”。
2. 在 配置 **NSX Manager** 设置 页面上，设置以下参数：
   a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
   b) NSX Manager Username（NSX Manager 用户名）- NSX Manager 的管理用户名。
   c) Password（密码）- NSX Manager 的管理用户的密码。
3. 在 NSX 管理器 使用的 **Citrix ADM** 帐户部分中，设置 **NSX** 管理器 的 Citrix ADC 驱动程序用户名和密码。Citrix ADM 使用这些登录凭据对来自 NSX 管理器的负载平衡器配置请求进行身份验证。
4. 单击确定。
5. 导航到“调配”>“系统”>“部署设置”。提供在 Trunk 端口组中配置的虚拟 LAN 范围。



6. 登录到 vSphere Web 客户端上的 NSX 管理器，然后导航到“服务定义”>“服务管理器”。

   您可以将 Citrix Citrix ADM 作为服务管理器之一进行查看。这表示注册成功，并在 NSX 管理器和 Citrix ADM 之间建立了通信通道。



在 **Citrix ADM** 中创建服务包

1. 在 Citrix ADM 中，导航到 **Orchestration** > **SDN** 编排 > **VMware NSX ManagerService Packages**，然后单击“添加”以添加新的服务包。
2. 在“服务包”页面的“基本设置”部分中，设置以下参数：

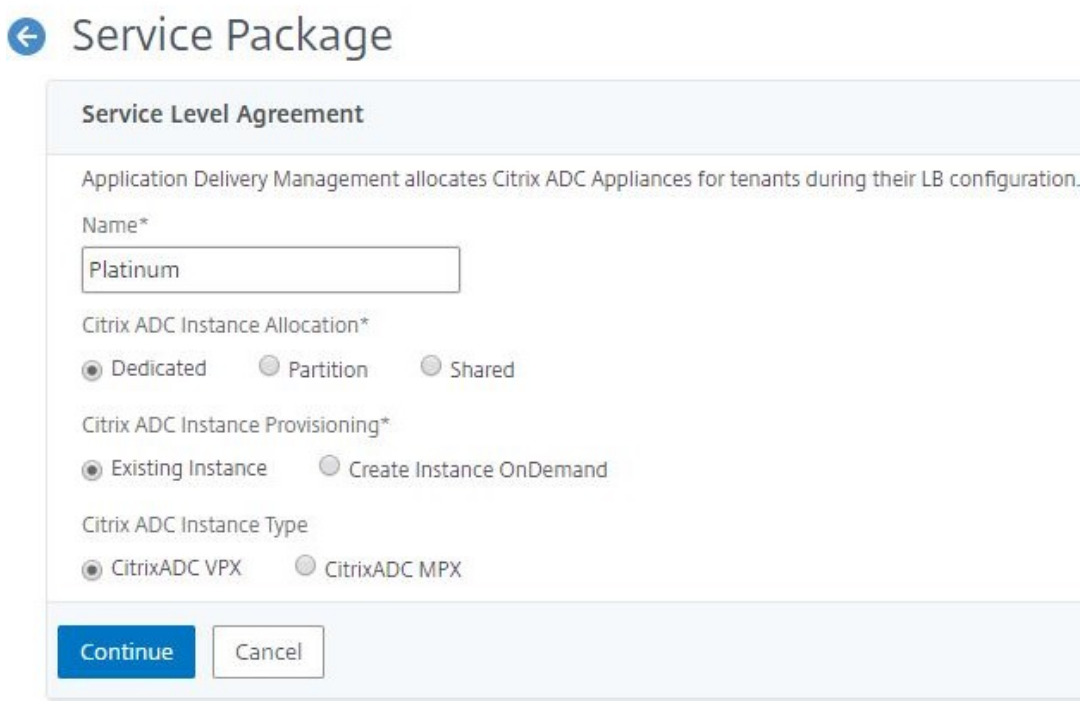
   a) Name（名称）- 键入服务包的名称

   b) Isolation Policy（隔离策略）- 默认情况下，隔离策略设置为“Dedicated”（专用）

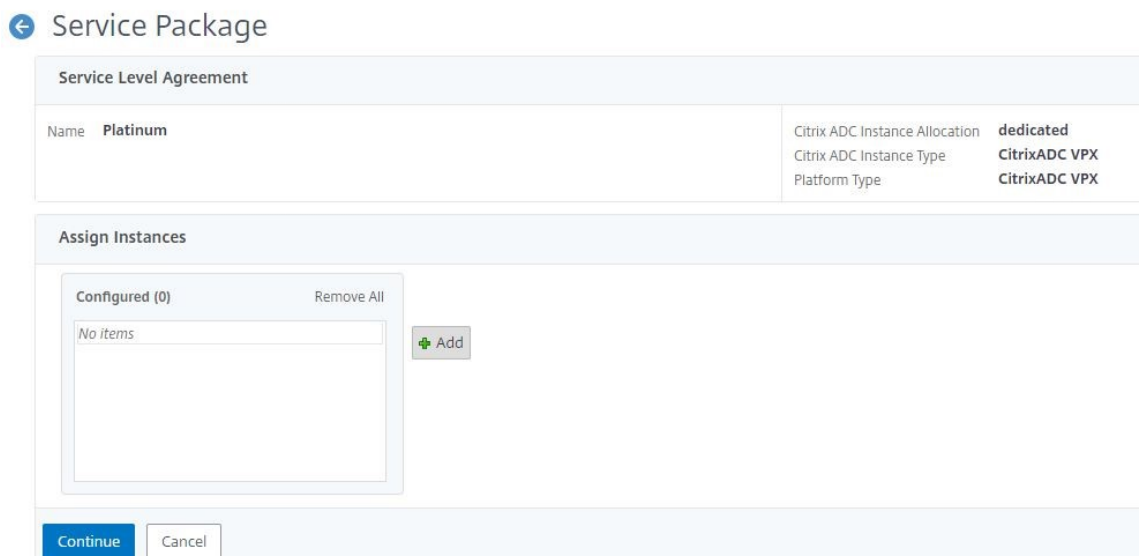
   c) 设备类型—默认情况下，设备类型设置为 Citrix ADC VPX

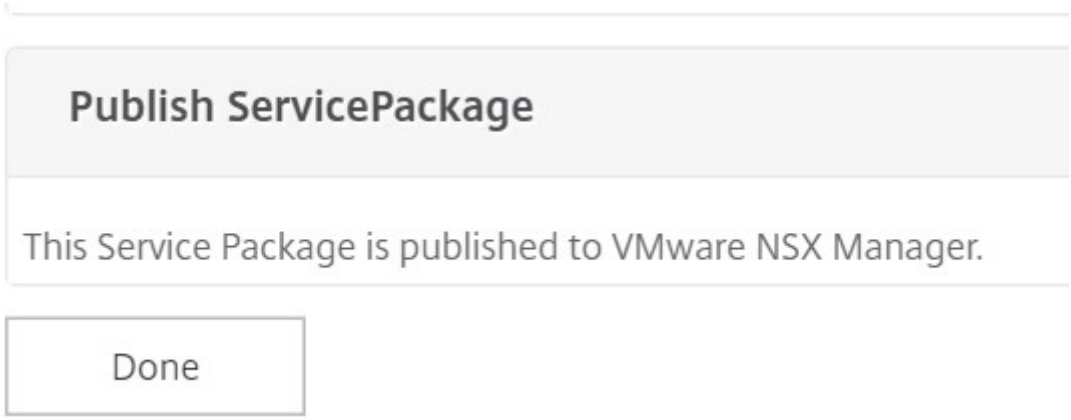
> 注意
>
> 这些值在此版本中是默认设置的，您无法对其进行修改。

d) 单击继续。



3. 在“分配设备”部分，选择此程序包的预置 VPX，然后单击“继续”。
4. 在“发布服务包”部分中，单击“继续”以将服务包发布到 VMware NSX，然后单击“完成”。





此过程在 NSX Manager 中配置服务包。服务可以添加多个设备，并且多个边缘可以使用相同的服务包将 Citrix ADC VPX 实例卸载到 Citrix ADM。

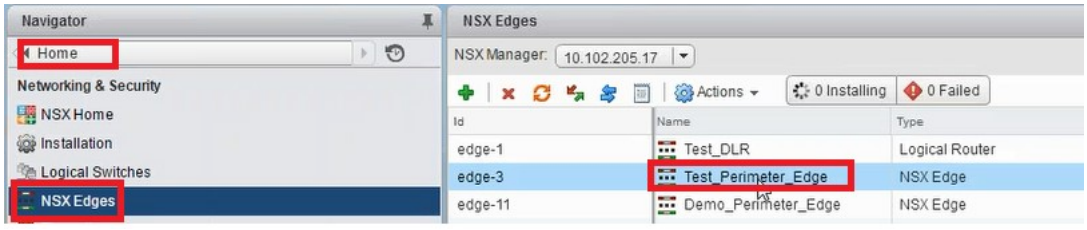
5. 登录 vSphere Web Client 上的 NSX Manager，然后导航到服务定义 > 服务。

   您可以看到 Citrix ADM 服务包已注册。

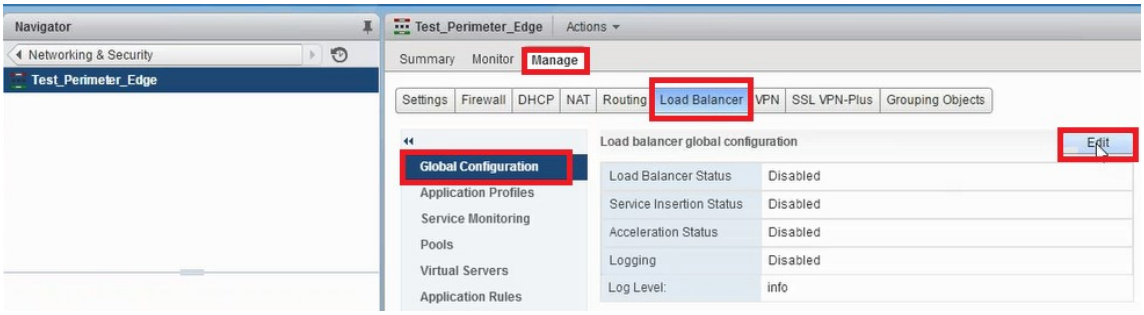
为边界执行负载平衡器服务插入

在先前创建的 NSX Edge Gateway 上执行负载平衡器服务插入（将负载平衡功能从 NSX LB 卸载到 Citrix ADC）。

1. 在 NSX Manager 中，导航到“主页”>“**NSX** 边缘”，然后选择已配置的边缘 Gateway。

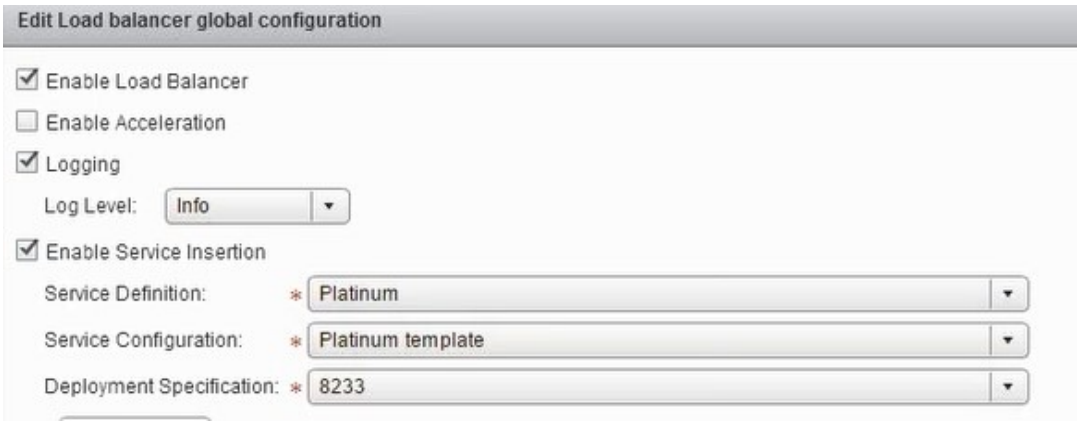


2. 单击 管理，然后在 负载平衡器 选项卡上，选择 全局配置，然后单击 编辑。

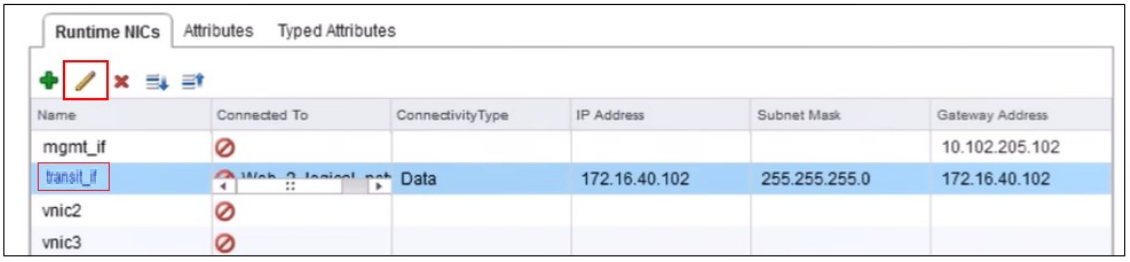


3. 选择 启用负载平衡器、日志记录、启用服务插入 以启用它们。

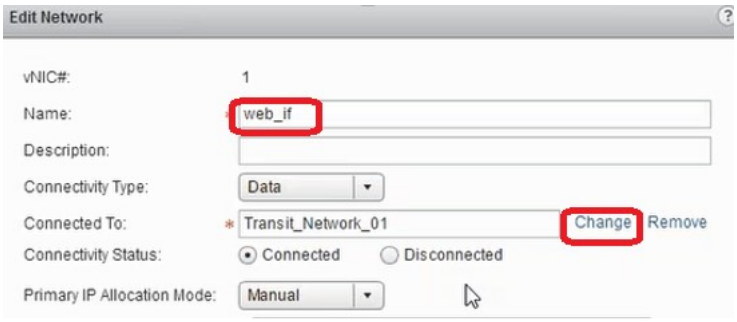
   a) 在 服务定义中，选择在 Citrix ADM 中创建并发布到 NSX 管理器的服务包。



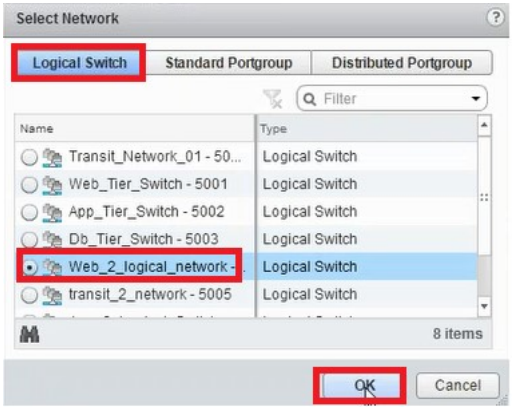
4. 选择现有的运行时网卡，然后单击“编辑”图标以编辑在分配 Citrix ADC VPX 时必须连接的运行时 NIC。



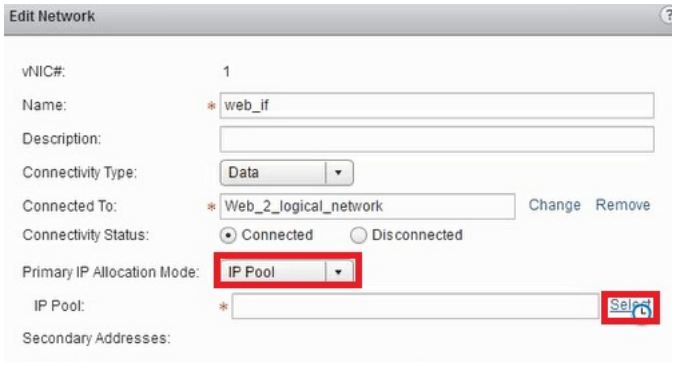
5. 编辑 NIC 的名称，将连接类型指定为 数据，然后单击 更改。



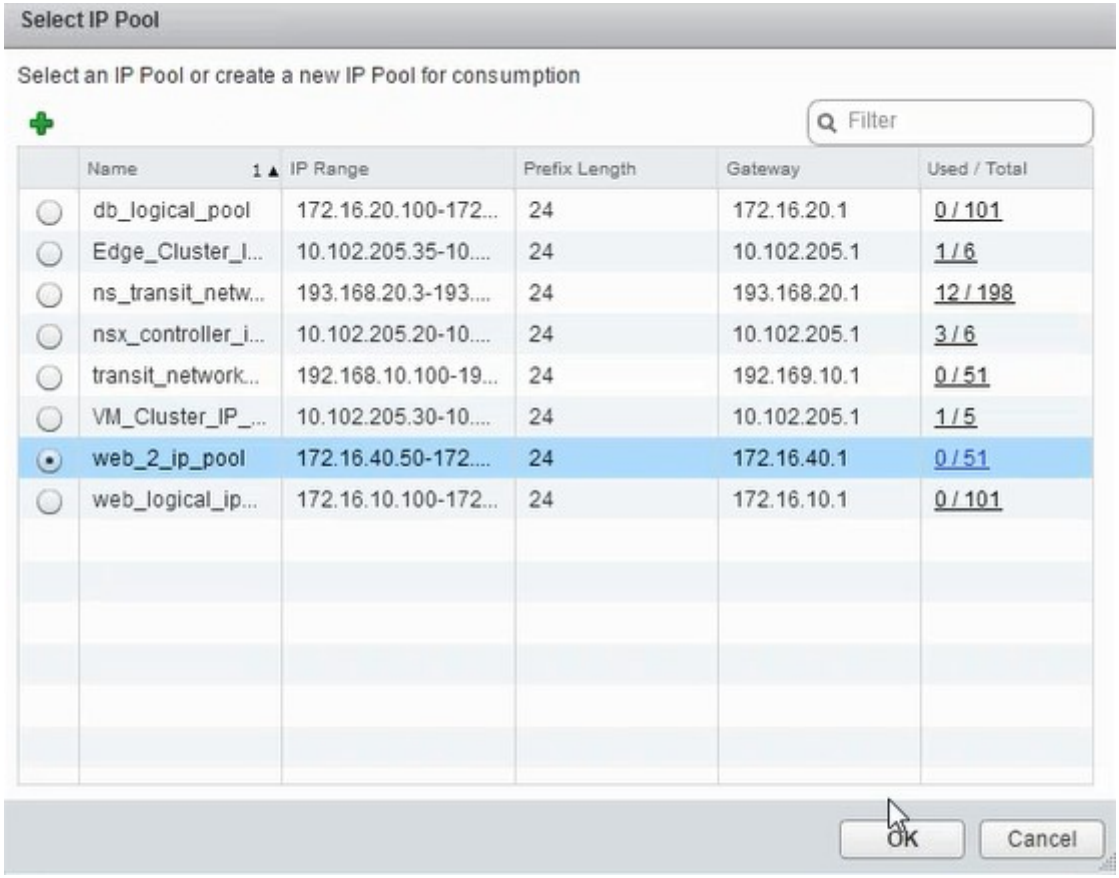
6. 选择适当的 Web 逻辑交换机。



7. 在 主 **IP** 分配模式下，从下拉列表中选择 IP 池，然后单击 IP 池字段上的向下箭头按钮。



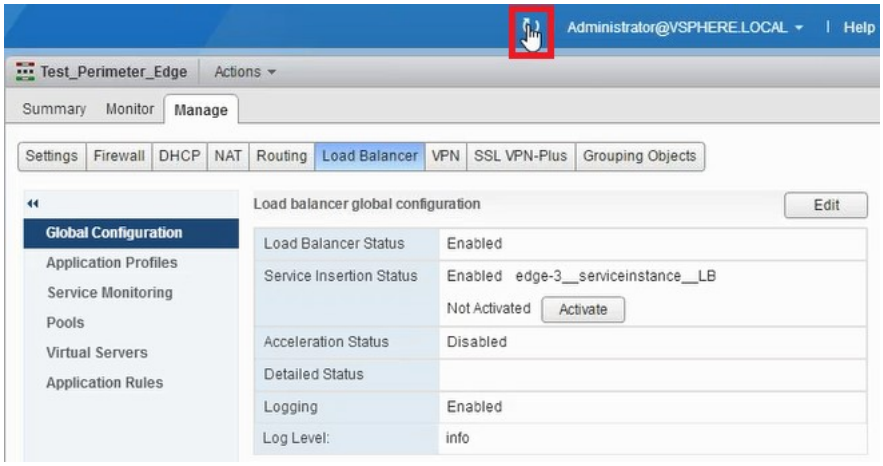
8. 在“选 择 **IP** 池”窗口中，选择相应的 IP 池，然后单击“确定”。

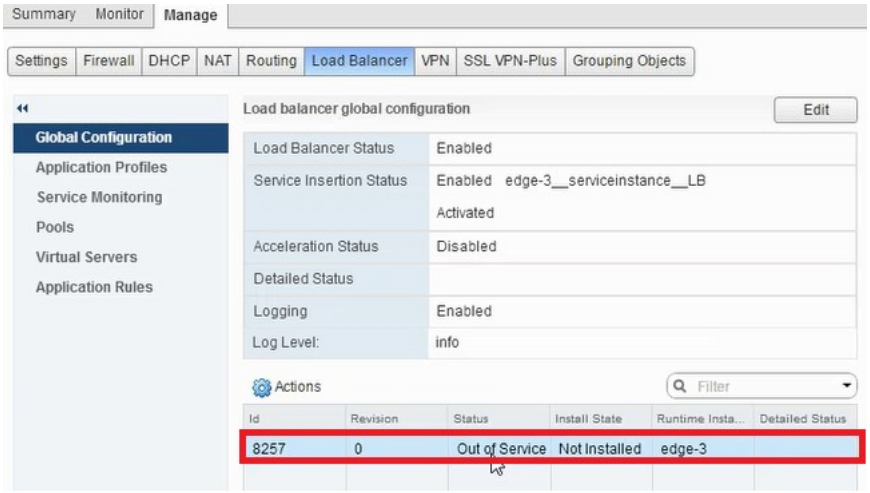


在 Citrix ADC VPX 装置中获取 IP 地址并将其设置为源净 IP 地址。在 NSX Manager 中创建一个 L2 网关以将 VXLAN 映射到虚拟 LAN。

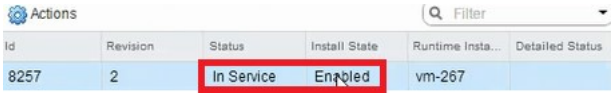
> 注意
>
> 所有数据接口都作为运行时 NIC 连接，它们应该是 DLR 接口的一部分。

9. 刷新视图以查看运行时间的创建。





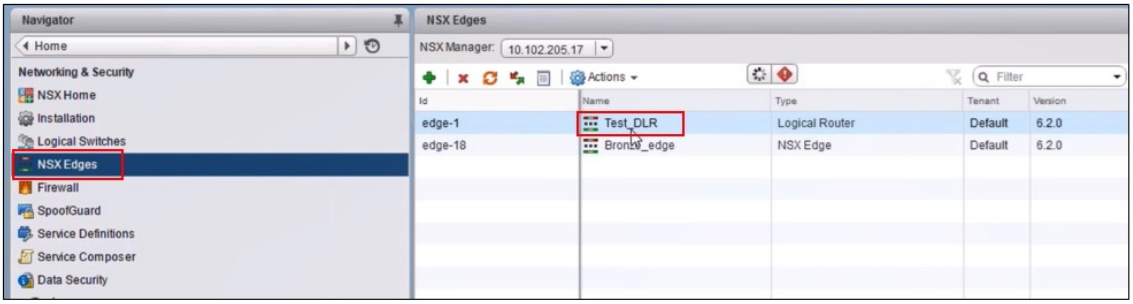
10. VM 启动后，“状态”的值将更改为“正 在服务”，“安装状态”的值更改为“已启用”。



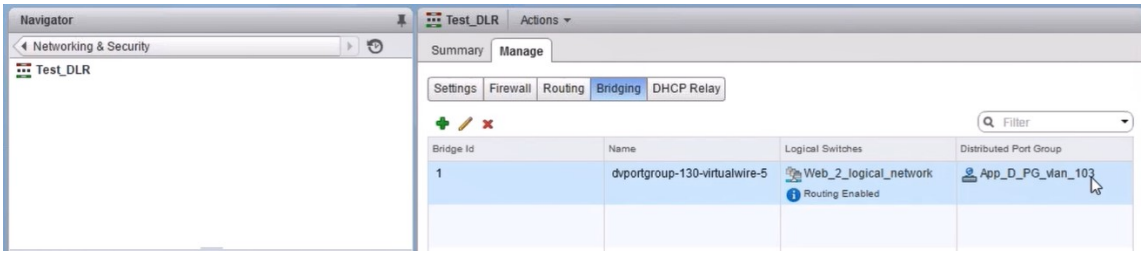
> 注意：
>
> 在 Citrix ADM 中，导航到“业务 流程”>“请求”以查看 LB 服务插入完成的进度详细信息。

在 **NSX Manager** 中查看 **L2** 网关

1. 登录到 vSphere Web 客户端上的 NSX 管理器，导航到 **NSX** 边缘，然后选择已创建的 DLR。



2. 在 DLR 页面中，导航到“管理”>“桥接”。可以看到列表中显示的 L2 网关。



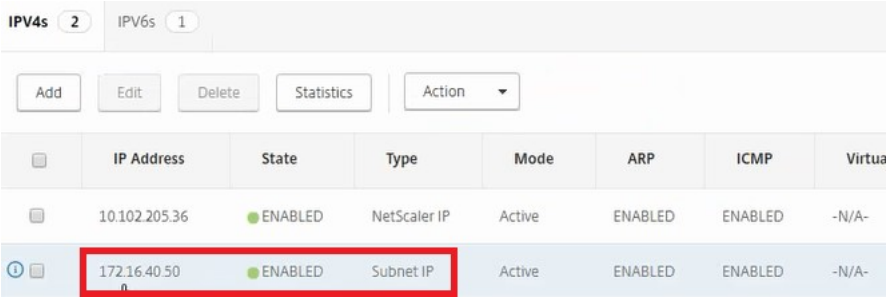
> 注意为每个数据接口创建
>
> 一个 L2 Gateway。

查看分配的 **Citrix ADC**

1. 使用 Citrix ADM 中显示的 IP 地址登录到 Citrix ADC VPX 实例。然后，导航到“配置”>“系统”>“网络”。在右侧窗格中，可以看到添加了两个 IP 地址。单击 IP 地址超链接可以查看详细信息。

   子网 IP 地址与 NSX 中添加的 Web Interface 的 IP 地址相同。

2. 导航到“配置”>“系统”>“许可 证”以查看应用于此实例的许可证。

使用样书配置 **Citrix ADC VPX** 实例

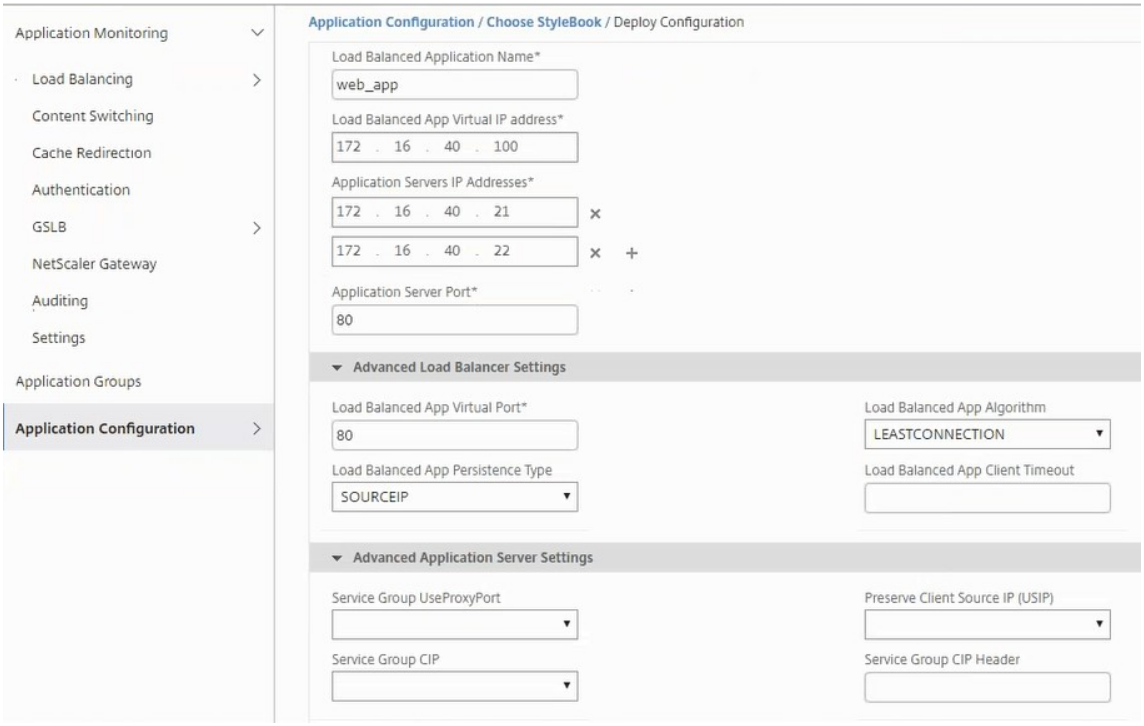
1. 在 Citrix ADM 中，导航到“编排”>“**SDN** 编排”>“配置 **NSX** 管理器”>“边缘网关”。

   记下分配给必须通过样书应用负载平衡配置的相应边缘网关的 Citrix ADC 实例 IP。

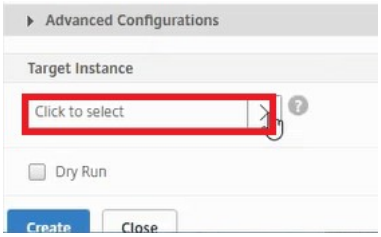
2. 创建新样书。导航到“****** 应用程序”**>** “** 配置”，导入样书，然后从列表中选择样本。

   要创建新样书，请参阅创建您自己的样书。

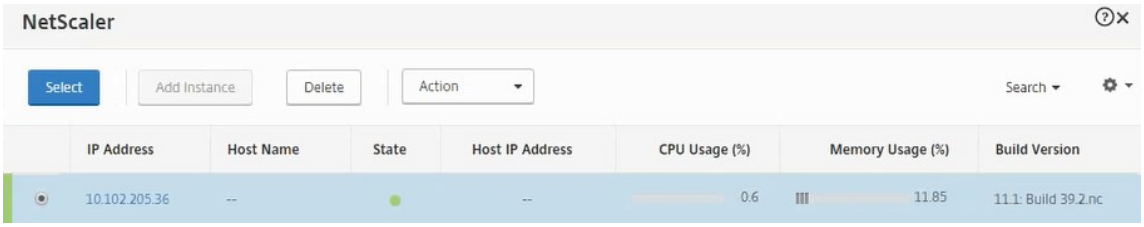
3. 为所有所需参数指定值。



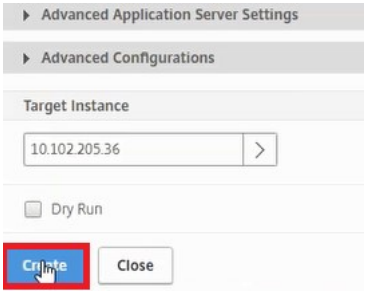
4. 指定要在其上运行这些配置设置的 Citrix ADC VPX 实例。



5. 选择前面说明的 IP 实例，然后单击“选择”。

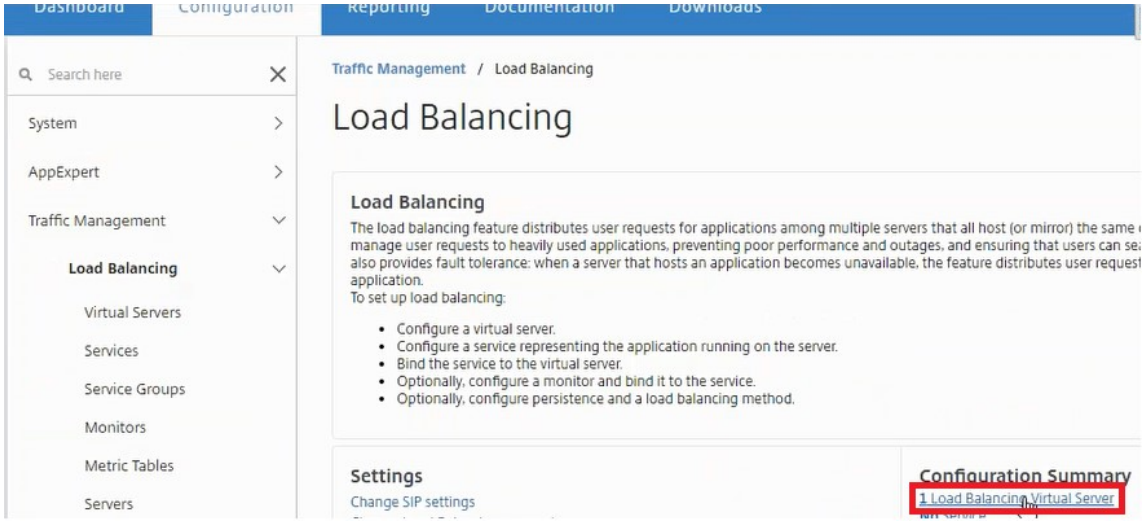


6. 单击 创建 可在选定的设备上应用配置。

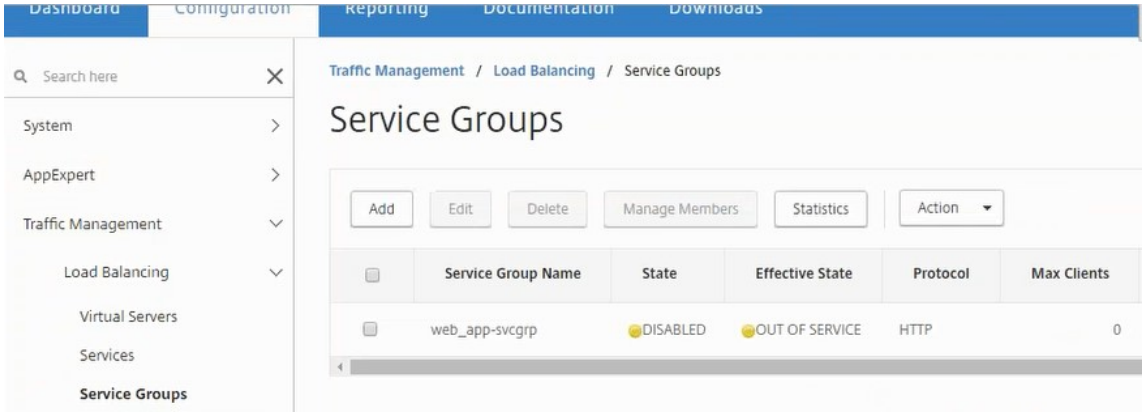


查看负载平衡器配置

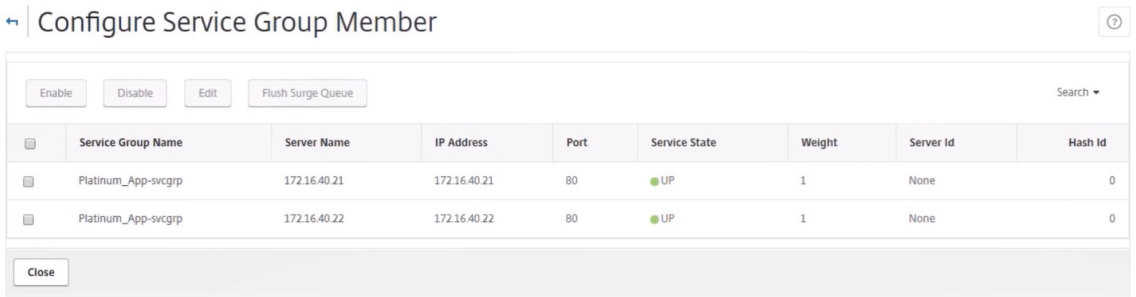
1. 登录到 Citrix ADC VPX 实例，导航到“配置”>“流量管理”>“负载平衡”以查看创建的负载平衡虚拟服务器。



还可以查看创建的服务组。



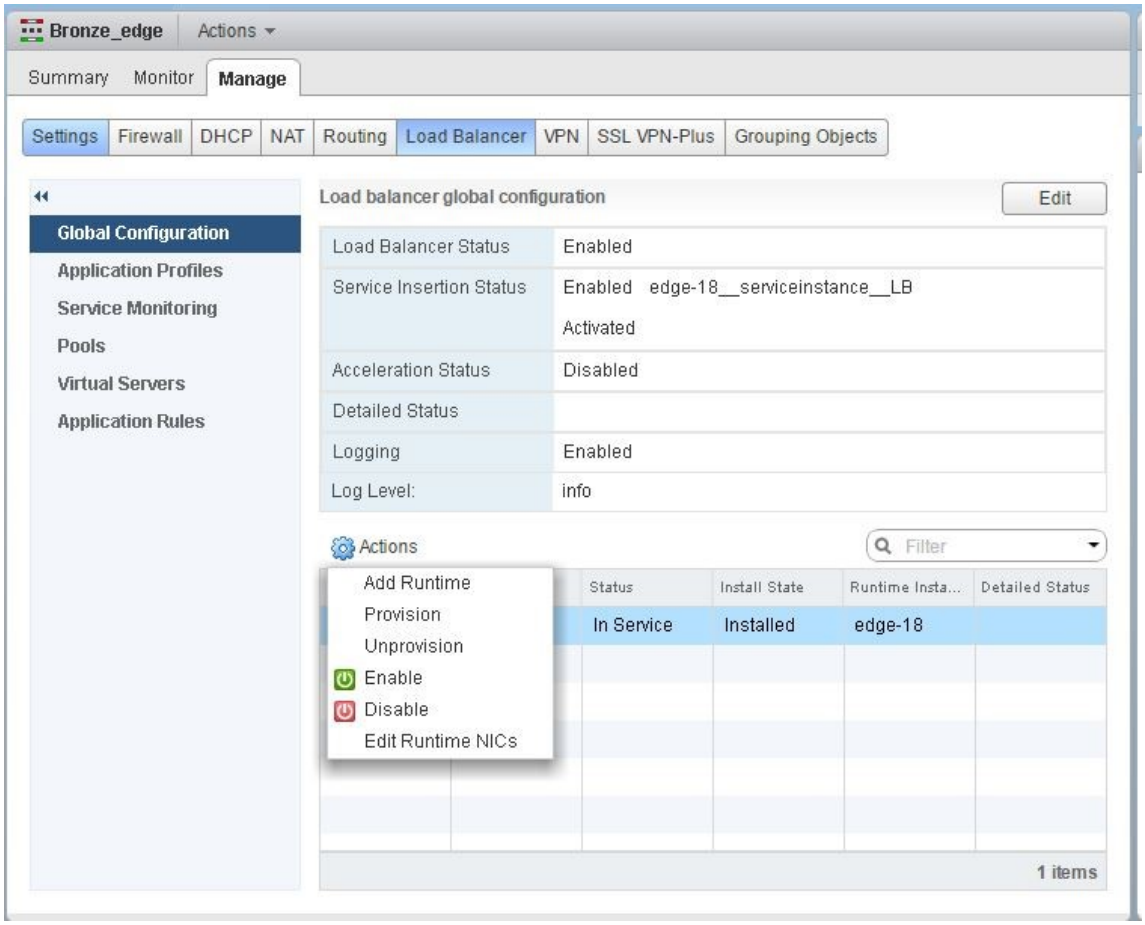
2. 选择服务组，然后单击 管理成员。**Configure Service Group Member**（配置服务组成员）页面显示与服务组关联的成员。



删除负载平衡器服务

1. 在 Citrix ADM 中，导航到“应用程 序”>“配置”，然后单击“**X**”图标以删除应用程序配置。
2. 登录到 vSphere Web 客户端上的 NSX 管理器，然后导航到 Citrix ADC VPX 实例所连接的边缘 Gateway。
3. 导航到“管 理”>“负载平衡器”>“全局配置”，右键单击运行时条目，然后单击“取消置备”。

   > 注意 NetScler MAS 中的
   >
   > 边缘网关对应于 NSX 管理器中的运行时条目。



   Citrix ADC VPX 实例已停止服务。

4. 在 Citrix ADM 中，导航到“编排”>“**SDN** 编排”>“配置 **NSX** 管理器”>“边缘网关”。确认 Edge 网关与所删除实例的各个映射是否不存在。

NSX 管理器：自动预配 **Citrix ADC** 实例

February 6, 2024

概述

Citrix Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动执行 Citrix ADC 服务的部署、配置和管理。此集成抽象出了与物理网络拓扑相关的传统复杂性，使 vSPhere/vCenter 管理员能够更快地以编程方式部署 Citrix ADC 服务。

在 VMware NSX 管理器上插入和删除负载平衡服务期间，Citrix ADM 会动态配置和销毁 Citrix ADC 实例。此动态 Provisioning 要求在 Citrix ADM 中自动分配 Citrix ADC VPX 许可证。当 Citrix ADC 许可上载到 Citrix ADM 时，Citrix ADM 将扮演许可服务器的角色。

必备条件

> 注意
>
> 仅适用于 **vSphere 6.1** 或更早版本的 **VMware NSX** 支持此集成。

- Citrix ADM, 版本 12.1 设置在高可用性和安装在 ESX 上.
- Citrix ADC VPX，版本 12.1
- 适用于 Citrix ADC VPX 实例的 Citrix ADC VPX 许可证，版本 12.1
- 在满足最低要求的硬件上安装 VMware ESXi 4.1 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 在满足最低系统要求的管理工作站上安装 VMware 开放式虚拟化格式工具（VMware ESXi 4.1 版需要）。

Citrix ADM 和 **Citrix ADC** 实例的高可用性部署

要置备 Citrix ADM HA 设置，请安装从 Citrix 下载站点下载的 Citrix ADM 映像文件。有关如何配置 Citrix ADM HA 设置的详细信息，请参阅 在高可用性中部署 Citrix ADM。

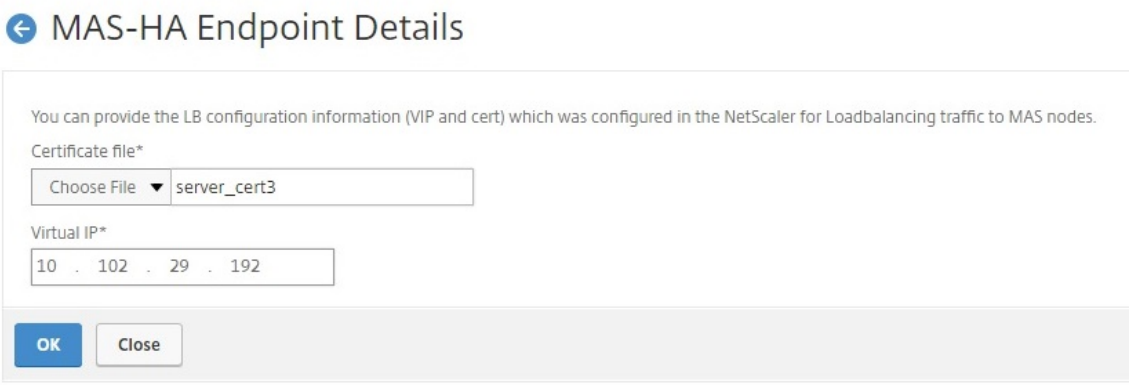
设置 **Citrix ADM HA** 端点详细信息

要将 VMware NSX 管理器与在 HA 模式下部署的 Citrix ADM 集成，必须首先输入负载平衡 Citrix ADC 实例的虚拟 IP 地址。您还必须将 Citrix ADC 负载平衡虚拟服务器上存在的证书文件上载到 Citrix ADM 文件系统。

要在 **Citrix ADM** 中提供负载平衡配置信息，请执行以下操作：

1. 在 Citrix ADM HA 节点中，导航到“系统”>“部署”。
2. 单击右上角的 **HA** 设置，然后在 **MAS-HA** 设置 页面中，单击 **MAS-HA** 端点详细信息。

3. 在 **MAS-HA** 端点详细信息 页面上，上载负载平衡 Citrix ADC 实例上已存在的相同证书。
4. 输入负载平衡 Citrix ADC 实例的虚拟 IP 地址，然后单 击确定。



在 **Citrix ADM** 中注册 **VMware NSX** 管理器

在设置两个 Citrix ADM 服务器以高可用性时，这两个服务器节点处于主动-被动模式。登录到主 Citrix ADM 服务器节点，将 VMware NSX 管理器注册到 HA 中的 Citrix ADM，以便在它们之间创建通信通道。

要将 **VMware NSX** 管理器注册到 **HA** 中的 **Citrix ADM**，请执行以下操作：

1. 在主 Citrix ADM 服务器节点中，导航到“编排”>“**SDN** 编排”>“**VMware NSX** 管理器”。
2. 单击“配置 **NSX** 管理器设置”。
3. 在 配置 **NSX Manager** 设置 页面上，设置以下参数：
   a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
   b) NSX Manager Username（NSX Manager 用户名）- NSX Manager 的管理用户名。
   c) Password（密码）- NSX Manager 的管理用户的密码。
4. 在 NSX 管理器使用的 Citrix ADM 帐户部分中，设置 NSX 管理器的 Citrix ADC 驱动程序密码。
5. 单击确定。

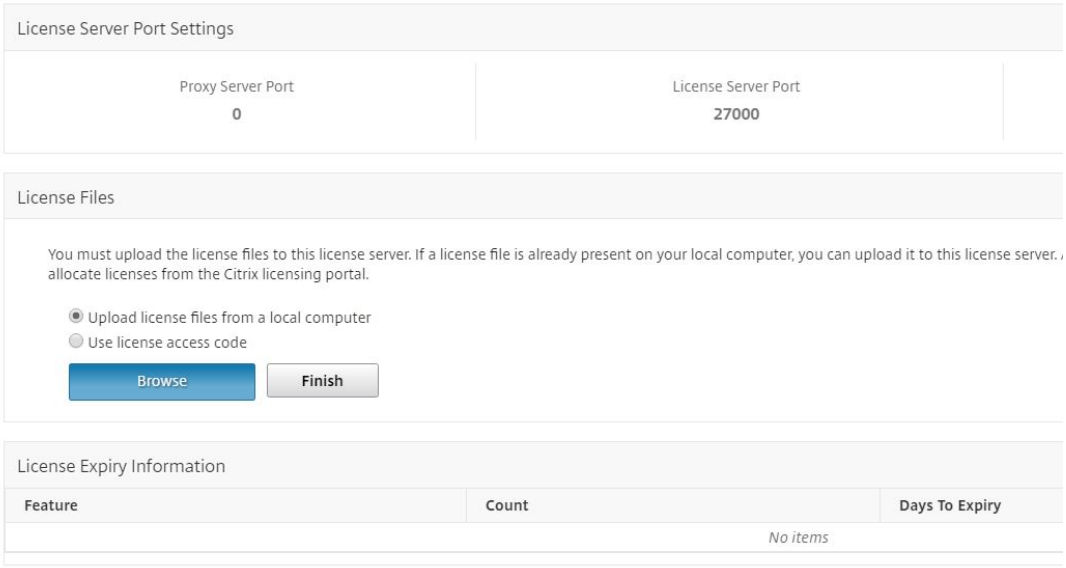
在 **Citrix ADM** 中上载许可证

将 Citrix ADC VPX 许可证上载到 Citrix ADM，以便 Citrix ADM 能够在与 NSX 进行协调期间自动为实例分配许可证。

要在 **Citrix ADM** 上安装许可证文件，请执行以下操作：

1. 在 Citrix ADM 中，导航到网络 > 许可证。
2. 在“许可证文件”部分，选择以下选项之一：
   a) 从本地电脑上载许可文件-如果本地电脑 上已经存在许可文件，则可以将其上载到 Citrix ADM。要添加许可证文件，请单击“浏览”，然后选择要添加的许可证文件 (.lic)。然后单击“完成”。
   b) 使用许可访问代码 -Citrix 通过电子邮件发送您购买的许可的许可访问代码 (LAC)。要添加许可证文件，请在文本框中输入 LAC，然后单击“获取许可证”。

> 注意：您可以随
>
> 时从许可证设置向 Citrix ADM 添加更多许可证。



在 **Citrix ADM** 中上载 **Citrix ADC VPX** 镜像

将 Citrix ADC 映像添加到 Citrix ADM 中，以便 Citrix ADM 使用服务包中定义的这些映像。

要在 **Citrix ADM** 中上载 **Citrix ADC VPX** 图像，请执行以下操作：

1. 在 Citrix ADM 中，导航到“编排”>“**SDN** 编排”>“**VMware NSX** 管理器”>“**ESX NSVPX** 映像”。
2. 单击“上载”，然后从本地存储文件夹中选择 Citrix ADC VPX zip 包。

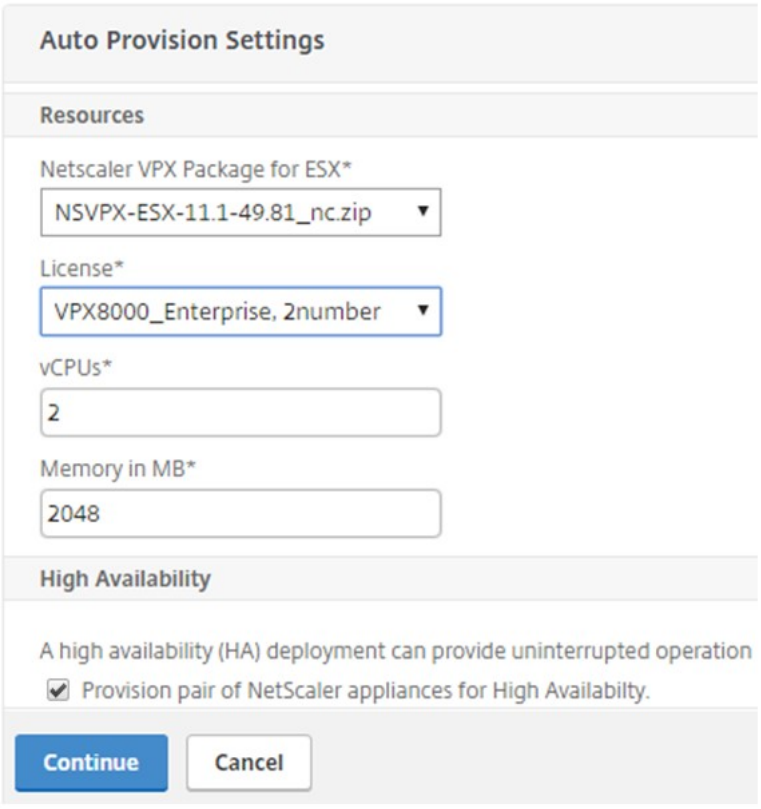
在 **Citrix ADM** 中创建服务包

在 Citrix ADM 中创建服务包以定义 SLA 集，该集指示如何分配 Citrix ADC 资源。

要在 **Citrix ADM** 中创建服务包，请执行以下操作：

1. 在 Citrix ADM 中，导航到 **Orchestration** > **SDN** 编排 > **VMware NSX ManagerService**Packag es，然后单击“添加”以添加新的服务包。
2. 在“服务包”页面的“基本设置”部分中，设置以下参数：
   a) Name（名称）- 服务包的名称
   b) 隔离策略-选择 专用
   c) Citrix ADC 实例预配-选择 按需创建实例
   d) 自动配置平台-选择 思特利 **xADC SDX**
   e) 单击继续
3. 在“自动配置设置”部分，选择最近上载的用于在 NSX 平台上部署的 Citrix ADC VPX zip 包，选择相应的许可，然后单击“继续”。

> 注意：
>
> 在“高可用性”部分中，选中该复选框以为 HA 置备 Citrix ADC 实例。



> 注意
>
> 上图所示列表框中显示的许可证名称 VPX8000_Enterprise，2number 就是一个示例，解释如下：
>
> - VPX-许可证是部署 Citrix ADC VPX 实例
> - 8000-消耗带宽为 8 GB
> - Enterprise - Citrix 提供三种类型的许可证 - Standard、Enterprise 和 Platinum
> - 2 号-使用此许可证可以部署两个 Citrix ADC VPX 实例
>
> “许可证”列表框中显示的许可证 名称取决于您从 Citrix 购买的许可证。

4. 单击继续。
5. 该服务包已发布到 NSX Manager。在 NSX Manager 中，导航到 “服务定义” > “服务管理器”。您可以将 Citrix ADM 作为服务管理器之一进行查看。这表示注册成功，并在 NSX 管理器和 Citrix ADM 之间建立了双向通信。

> 注
>
> 意：对于处于高可用性部署的 Citrix ADM，许可证只能在 Citrix ADM 许可服务器节点中上载。Citrix ADM 节点处于主动-被动模式。

为 **Edge** 执行负载平衡器服务插入

在现有 NSX Edge 网关上执行负载平衡器服务插入，即将负载平衡功能从 NSX 负载平衡器卸载到 Citrix ADC。

要在 **NSX Edge** 网关上插入负载平衡服务，请执行以下操作：

1. 在 NSX Manager 中，导航到 主页 > 网络和安全 > **NSX E**dges，然后双击选择已配置的 Edge 网关。
2. 单击 管理，然后在 负载平衡器 选项卡上，选择 全局配置，然后单击 编辑。
3. 选择“启用负载平衡器和启用服务插入”以启用它们。
4. 在 服务定义中，选择发布到 NSX Manager 的服务包。
5. 为管理接口配置一个虚拟 NIC，为数据接口配置一个或多个虚拟 NIC。相应地为管理和数据选择网络。

> 注意：
>
> 在主 IP 分配模式下选择 IP 池选项。Citrix ADM 不支持手动或 DHCP 分配 IP 地址。

6. 单击“刷新”图标查看运行时的创建情况。

> 注意：
>
> 由于您要在 HA 部署中部署两个 Citrix ADC VPX 实例，因此在 NSX 管理器中会创建两个运行时间。
>
> 您可能需要刷新屏幕才能查看屏幕上显示的运行时间。

7. 选择运行时间，单击“操作”，然后从弹出式菜单中选择“安装”。如果是 HA，则还对另一个运行时重复此操作。
8. 当两台虚拟机启动时，状态的值更改为“服务中”，安装状态的值更改为“已启用”。

   > 注意
   >
   > 您可能需要刷新屏幕才能查看状态的变化。

9. 在 Citrix ADM 中，导航到“**** 编排”**>**“请求”以查看完成服务插入的进度详情。您可以看到 **Citrix ADM** 发出了创建和更新运行时间的请求。更新运行时间后，选择请求并单击“** 任务”按钮，查看 Citrix ADM 是否已添加到 NSX Manager 中。

   对于 HA，在 Citrix ADM 中将有两个请求创建和更新两个运行时间。更新两个运行时间后，选择两个请求并单击“** 任务”按钮，查看是否已在 NSX Manager 中添加了两个 Citrix ADM HA 节点。

10. 在 Citrix ADM 中，导航到“编排”>“**SDN** 编排”>“**VMware NSX** 管理器”>“边缘网关”。在右侧面板中，您可以查看是否已将 Citrix ADC VPX 添加到 NSX 边缘网关中。

    对于高可用性，您可以看到在 NSX 边缘网关中添加了两个处于高可用性模式的 Citrix ADC VPX 实例。

11. 在 Citrix ADM 中，导航到“网络”>“许可证”>“**VPX** 许可证”。选择 Citrix ADC VPX 许可证和您已安装的版本。

    处于 HA 模式的 Citrix ADC VPX 实例使用两个许可证，状态将显示在屏幕上，如下所示。

服务插入完成后，您可以使用样书通过以下两种方法之一配置 Citrix ADC 实例：

- 在 VMware NSX Manager GUI 中在 Citrix ADC VPX 上配置负载平衡服务

- 在 Citrix ADM GUI 中在 Citrix ADC VPX 上配置负载平衡服务

在 **VMware NSX Manager GUI** 中在 **Citrix ADC VPX** 上配置负载平衡服务

执行以下任务以使用内置样书在 NSX Edge 网关设备上启用负载平衡服务的配置。

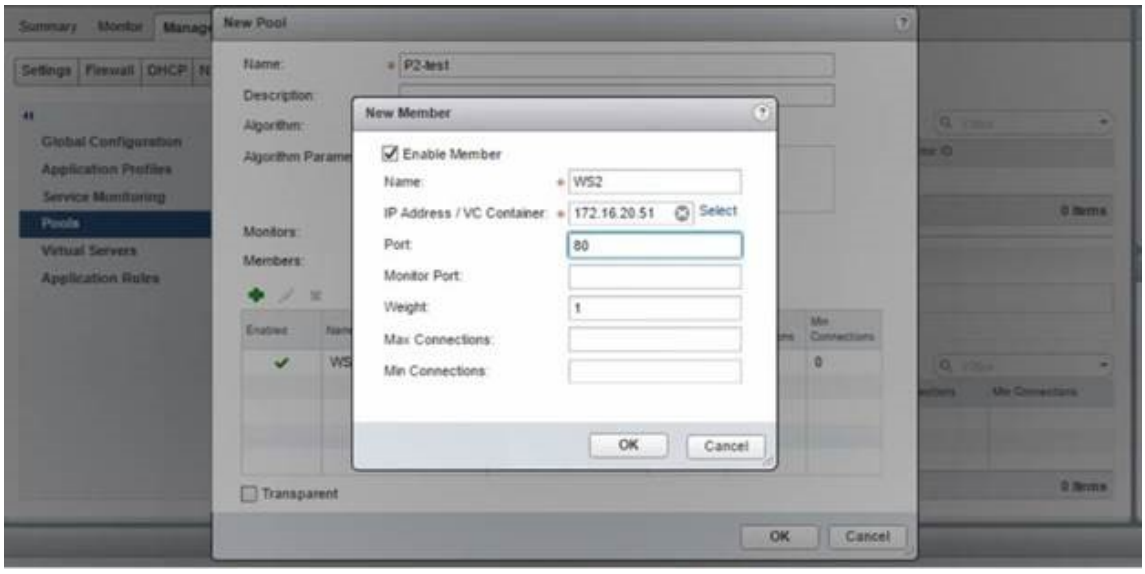
在 NSX Manager 中，导航到 主页 > 网络和安全 > **NSX E**dges，然后双击选择已配置的 Edge 网关。

创建池和池成员

创建服务器池和不同容量的成员。

1. 单击“管理”，然后在“负载平衡器”选项卡上选择“池”，然后单击“**+**”图标添加新池，然后设置以下参数：
   a) Name（名称）- 新池的名称
   b) Algorithm（算法）- 从下拉列表中选择算法，将基于该算法选择池。
   c) Monitors（监视器）- 确保服务监视器设置为 default_http_monitor
   d) Members（成员）- 单击“+”以向池添加成员，并在“New Member”（新成员）窗口中输入必要的参数。
      i. Name（名称）- 成员的名称
      ii. IP Address/ VC Container（IP 地址/VC 容器）- 单击“Select”（选择）以从可用列表中选择对象或输入对象的 IP 地址。
2. 单击确定。

   根据需要添加任意数量的成员。



创建虚拟服务器

创建一组虚拟服务器，并为每个虚拟服务器分配一个池。

1. 单击“管理”，然后在“负载平衡器”选项卡上，选择“虚拟服务器”，然后单击“**+**”图标添加虚拟服务器，然后设置以下参数：

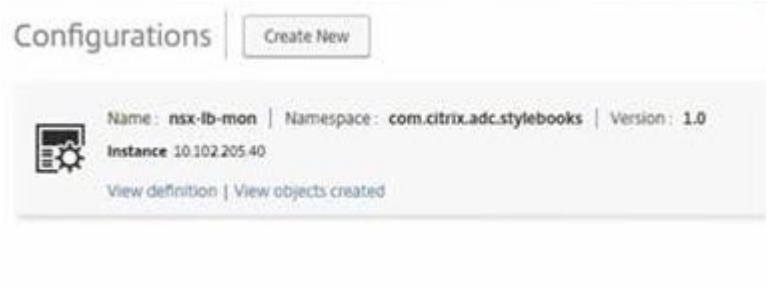
   a) 应用程序配置文件-默认情况下，显示在 Citrix ADM 中创建的服务配置文件。

   b) Name（名称）- 虚拟服务器的名称。

   c) IP Address（IP 地址）- 单击“Select”（选择）以选择现有的 IP 地址池或创建新的 IP 地址池。

   d) Default pool（默认池）- 从下拉列表中选择默认池。

2. 单击确定。
3. 在 Citrix ADM 中，导航到“业务 流 程”>“请求”，以查看在一个或多个选定 Citrix ADC 实例上完成服务创建的进度详细信息。
4. 在 Citrix ADM 中，导航到 应用程序 > 配置，然后检查“nsx-lb-mon”配置包是否已创建。



在 **Citrix ADM GUI** 中在 **Citrix ADC VPX** 上配置负载平衡服务

使用 Citrix ADM 样书在 Citrix ADC 实例上部署负载平衡器配置。对于 HA，配置部署在 HA 中的两个 Citrix ADC 实例上。

要通过样书创建配置包，请执行以下操作：

1. 在 Citrix ADM 中，导航到“应用程序”>“配置”>“创建新”，然后从列表中选择 **HTTP/SSL** 负载平衡（带监视器）样书。样书将以用户界面页面形式打开，您在此为此样书中定义的所有参数输入值。
2. 为所有所需参数指定值。
3. 选择在 NSX 环境中配置的目标 Citrix ADC VPX 实例，然后单击“创建”将配置应用到所选设备上。对于 HA 部署，请选择处于 HA 模式的实例。

验证在 **Citrix ADC VPX** 实例中创建的虚拟服务器和服务组

您可以查看服务组和虚拟服务器是通过登录 Citrix ADC VPX 实例创建的。

要查看服务组和虚拟服务器，请执行以下操作：

1. 登录到 Citrix ADC VPX 实例。对于 HA 部署，您必须登录到处于 HA 状态的两个 Citrix ADC 实例。
2. 导航到“配置”>“系统”>“网络”。在右侧窗格中，可以查看添加的 IP 地址。单击 IP 地址超链接可以查看详细信息。您可以看到子网 IP 地址与在 NSX 中添加的 Web Interface 的 IP 地址相同。
3. 接下来，导航到 流量管理 > 负载平衡 > 虚拟服务器 并查看虚拟服务器的详细信息。
4. 接下来，导航到 服务组 并查看服务组的详细信息。
5. 最后，导航到“配置”>“系统”>“许可 证”以查看应用于此实例的许可证。

删除负载平衡服务

如果在 NSX 管理器上部署的 Citrix ADC VPX 实例上不再需要负载平衡服务，则可以删除之前执行的服务插入。

要删除配置和服务插入，请执行以下操作：

1. 在 Citrix ADM 中，导航到 应用程序 > 配置，选择创建的应用程序配置，然后单击“X”图标删除配置。
2. 在 NSX 管理器中，导航到 Citrix ADC VPX 实例所连接的边缘 Gateway。导航到 管理 > 负载平衡器 > G 全局配置，右键单击运行时条目，然后单击“取消配置”。将是虚拟机停止工作。
3. 在 Citrix ADM 中，导航到“编排”>“云编排”>“边缘网关”。确认不应存在 Edge 网关与所删除实例的各个映射。

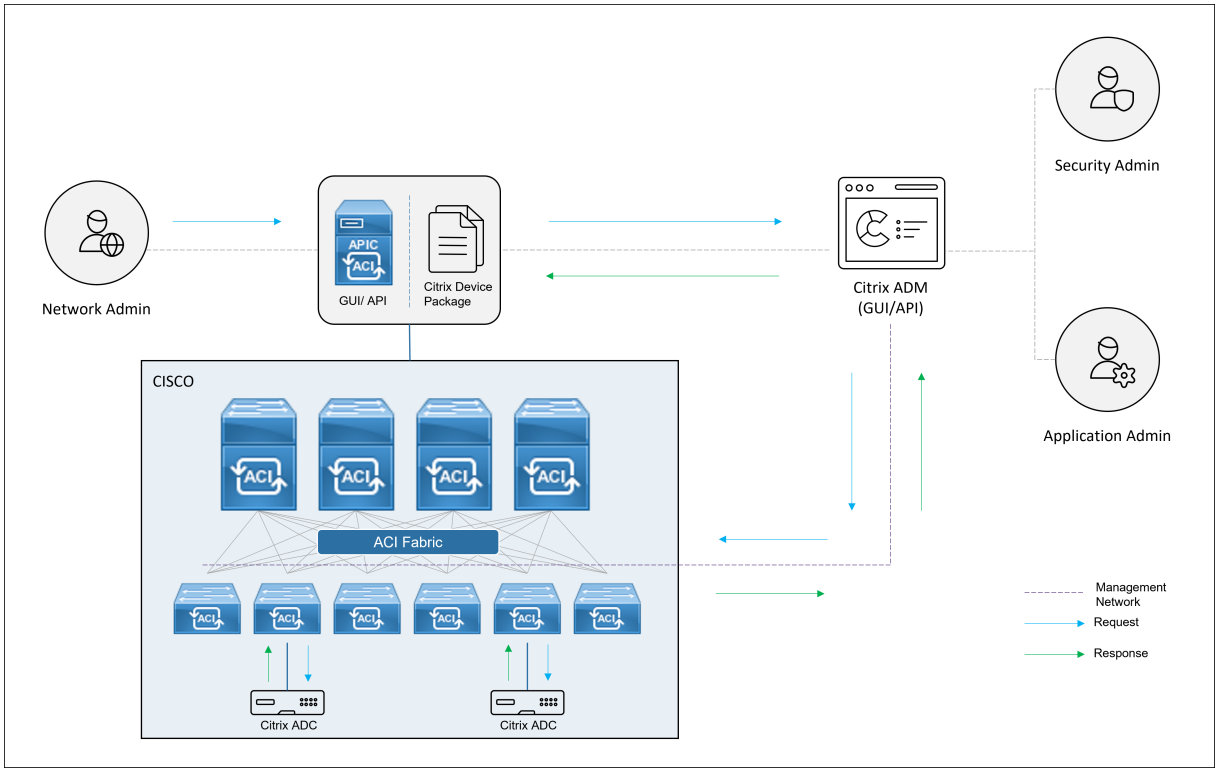
在 **Cisco ACI** 混合模式下使用 **Citrix ADC** 实现的 **Citrix ADM** 自动化

February 6, 2024

Cisco ACI 1.3 版 (2f) 中引入了混合模式支持。在混合模式下，您可以通过应用程序策略基础设施控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委托给 Citrix Application Delivery Management (ADM)，后者在 APIC 中充当设备管理器。

Citrix ADC 混合模式解决方案由混合模式设备包和 Citrix ADM 支持。需要在 APIC 中上载混合模式设备包。该软件包提供来自 Citrix ADC 的所有网络 L2-L3 可配置实体。应用程序奇偶校验由样书从 Citrix ADM 映射到 APIC。也就是说，样书充当给定应用程序的 L2-L3 配置和 L4-L7 配置之间的引用。在 APIC 中为 Citrix ADC 配置网络实体时，必须提供样书名称。

下图概述了混合模式解决方案中的 Citrix ADC：

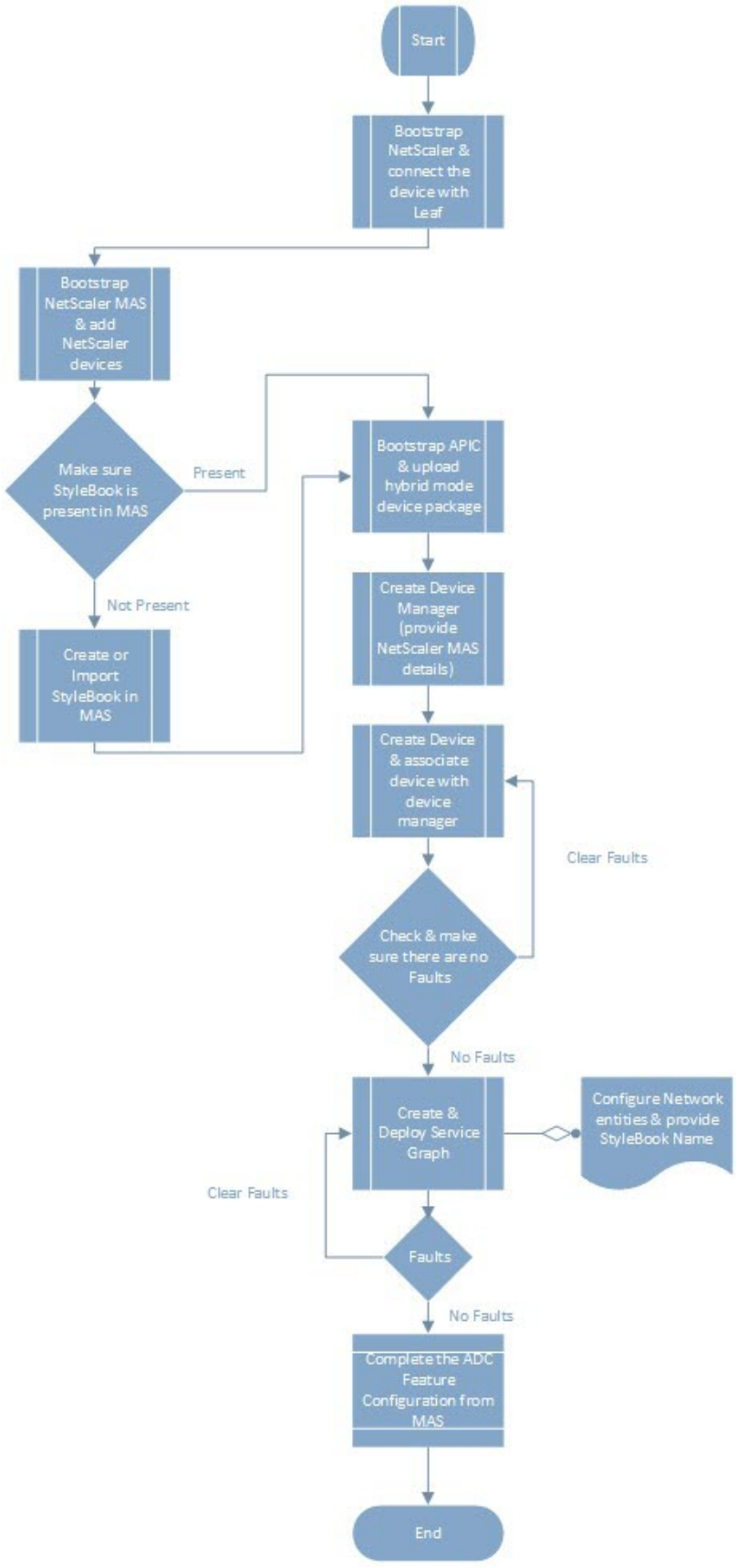


在混合模式下，Citrix ADC 配置分两个阶段执行：

1. 从 Cisco APIC 进行网络交换
2. 配置通过 Citrix ADM 完成

对于任何给定的应用程序，在 Cisco APIC 中进行服务图创建和部署过程中，网络管理员必须提供网络特定的详细信息，例如 IP 地址、端口、虚拟 LAN（自动）等。然后，这些配置详细信息通过设备包推送到 Citrix ADM，Citrix ADM 在内部对其进行处理并配置 Citrix ADC。应用程序管理员在 Citrix ADM 中使用样书创建应用程序的 ADC 相关配置，然后将这些配置从 Citrix ADM 推送到 Citrix ADC。Cisco APIC 和 Citrix ADM 通过管理网络与 ADC 通信。

下图显示了混合解决方案中的 Citrix ADC 工作流：



必备条件

February 6, 2024

请确保：

- 您拥有 Cisco ACI 组件和 Citrix ADC 的概念知识。
  - 有关 Cisco ACI 及其组件的更多信息，请参阅产品文档，网址为：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html。
  - 有关 Citrix ADC 的更多信息，请参阅 Citrix ADC 产品文档，网址为：http://docs.citrix.com/。
- 已设置并配置所有所需的 Cisco ACI 组件，包括数据中心里的 Cisco APIC。有关 Cisco ACI 及其组件的更多信息，请参阅产品文档，网址为：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html。
- 您已安装 Citrix ADC 11.1 或更高版本。
- 您已在思科 ACI 中配置了 Citrix ADC，以便可以使用思科 APIC 对它们进行管理。
- 您已在您的环境中部署了 Citrix Application Delivery Management (ADM)。有关更多信息，请参阅 Citrix ADM 12.1。
- 建立了从 APIC 到 Citrix ADM 和 ADC 的管理连接。
- 请记录：
  - 用于管理和数据路径连接的连接接口和 IP 地址。
  - 叶交换机详细信息：Citrix ADC IP 地址、端口、接口等。

> 注意
>
> 在此版本中，混合模式解决方案在单一上下文中支持 Citrix ADC，即不支持管理分区。

使用 **Cisco APIC** 和 **Citrix ADM** 在混合模式下配置 **Citrix ADC**

February 6, 2024

执行以下任务，通过使用 Cisco APIC 和 Citrix Application Delivery Management (ADM) 在混合模式下配置 Citrix ADC：

1. 将结构中的 Citrix ADC 实例添加到 Citrix ADM 中。有关说明，请参阅 向 Citrix ADM 添加实例。

2. 使用 Citrix ADM 为应用程序创建样书。有关说明，请参阅 使用 Citrix ADM 为应用程序创建样书。
3. 将 Citrix ADC 混合模式设备包导入思科 APIC。有关说明，请参阅 将 Citrix ADC 混合模式设备包导入思科 APIC
4. 在思科 APIC 中将 Citrix ADM 添加为设备管理器。有关说明，请参阅 在思科 APIC 中将 Citrix ADM 添加为设备管理器
5. 使用思科 APIC 在思科 ACI 中添加 Citrix ADC 设备。有关说明，请参阅 在思科 ACI 中将 Citrix ADC 作为设备添加
6. 创建和部署服务图模板。有关说明，请参阅 创建和部署服务图
7. 在 Citrix ADM 中使用样书配置 L4-L7 参数。有关说明，请参阅 使用 Citrix ADM 中的样书配置 L4-L7 参数
8. Cisco APIC 中的附加或分离端点事件。有关更多信息，请参阅 从 APIC 附加或分离终端节点事件

使用 **Citrix ADM** 为应用程序创建样书

February 6, 2024

样书是一种配置模板，您可以使用它为任何应用程序创建和管理 Citrix ADC 配置。您可以创建用于配置特定 Citrix ADC 功能的样书，例如负载平衡、SSL 卸载或内容切换。可以设计样书以创建针对企业应用程序部署（例如 Microsoft Exchange 或 Lync）的配置。有关详细信息，请参阅样书。

您可以为您的应用程序创建自己的样书，也可以修改和使用随 Citrix Application Delivery Management (ADM) 附带的 APIC-HTTP-LB 样书。

要在 Citrix ADM 中为应用程序创建自己的样书，请参阅 如何创建自己的样书。

创建样书时，请务必遵循样书中的 APIC 服务图模型。也就是说，适用于任何应用程序的 APIC 服务图遵循通过 ADC 功能连接的使用者和提供商模型。使用者和提供商以端点组 (EPG) 表示，是一对一的关系。在样书中也必须遵循相同的模型，其中提供商 EPG 必须以服务组表示，每个端点以服务组的成员表示。ADC 功能节点必须由虚拟服务器（例如，负载平衡虚拟服务器）表示，虚拟服务器与服务组之前必须是一对一的关系。

这基本上体现了服务图的本质，让您可以处理来自 APIC 的附加或分离事件，其中附加事件是将端点绑定到对应的服务组，分离事件是对其取消绑定。必须确保服务图和样书是对等的，以实现从网络 L2-L3 到 ADC 功能 L4-l7 配置的无缝自动化。

将 **Citrix ADC** 混合模式设备封装导入 **Cisco APIC**

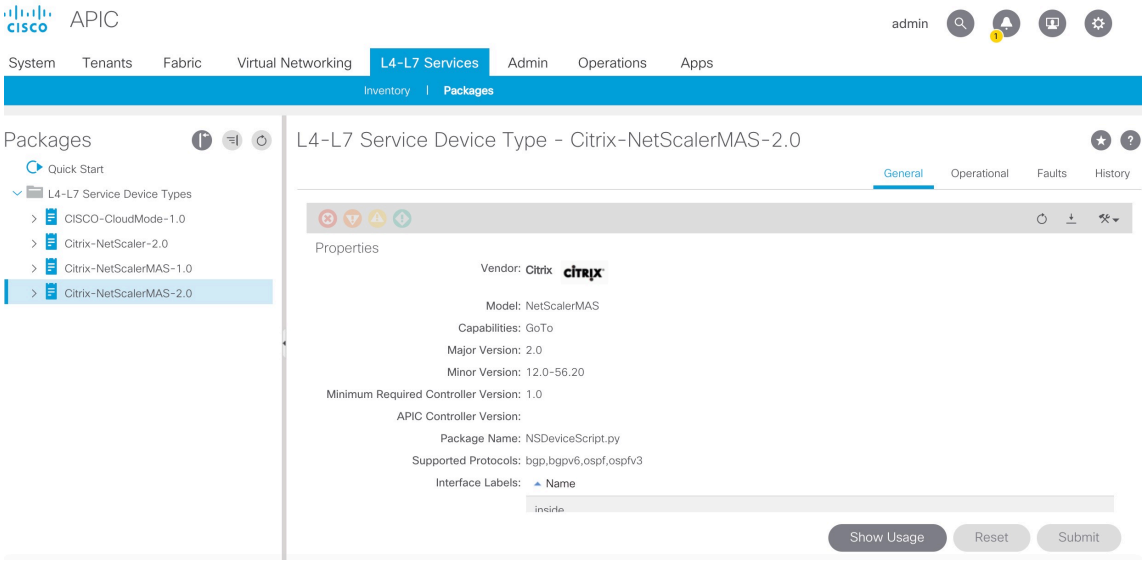
February 6, 2024

与完全托管模式相比，混合模式设备包是轻型包。通过设备型号只能提供 L2-L3 网络参数。器件型号中只定义了一个通用 ADC 功能，以及基于结构中 Citrix ADC 部署的四个功能配置文件（例如，单臂和双臂，RHI 相同）。混合模式设备包名称是 **NetScaler** 混合模式设备包 **12.0** 版本 **56.20**。在 Citrix 下载站点中搜索混合模式设备包，下载该软件包，然后将设备包导入到 APIC。

> 注意
>
> 混合模式设备包可以与完全托管模式设备包共存。

要使用 **APIC GUI** 将混合模式设备包导入 **APIC**，请执行以下操作：

1. 在菜单栏上，单击 **L4-L7** 服务 选项卡，然后选择 包 面板。
2. 在 导航 窗格中，右键单击 **L4-L7** 设备类型 并选择 导入设备包。
3. 在“导入设备包”对话框中，单击“浏览”选择下载的 Citrix ADC 混合模式设备包。
4. 单击 **Submit**（提交）。
   成功将设备包导入 APIC 后，在 导航 窗格中，您可以通过单击设备名称来查看设备包的详细信息。



> 重要
>
> 导入设备包后，请确保 APIC 中没有故障。可以单击“Device Types”（设备类型）窗口中的 **Faults**（故障）选项卡查看故障。

在 **Cisco APIC** 中将 **Citrix ADM** 添加为设备管理器

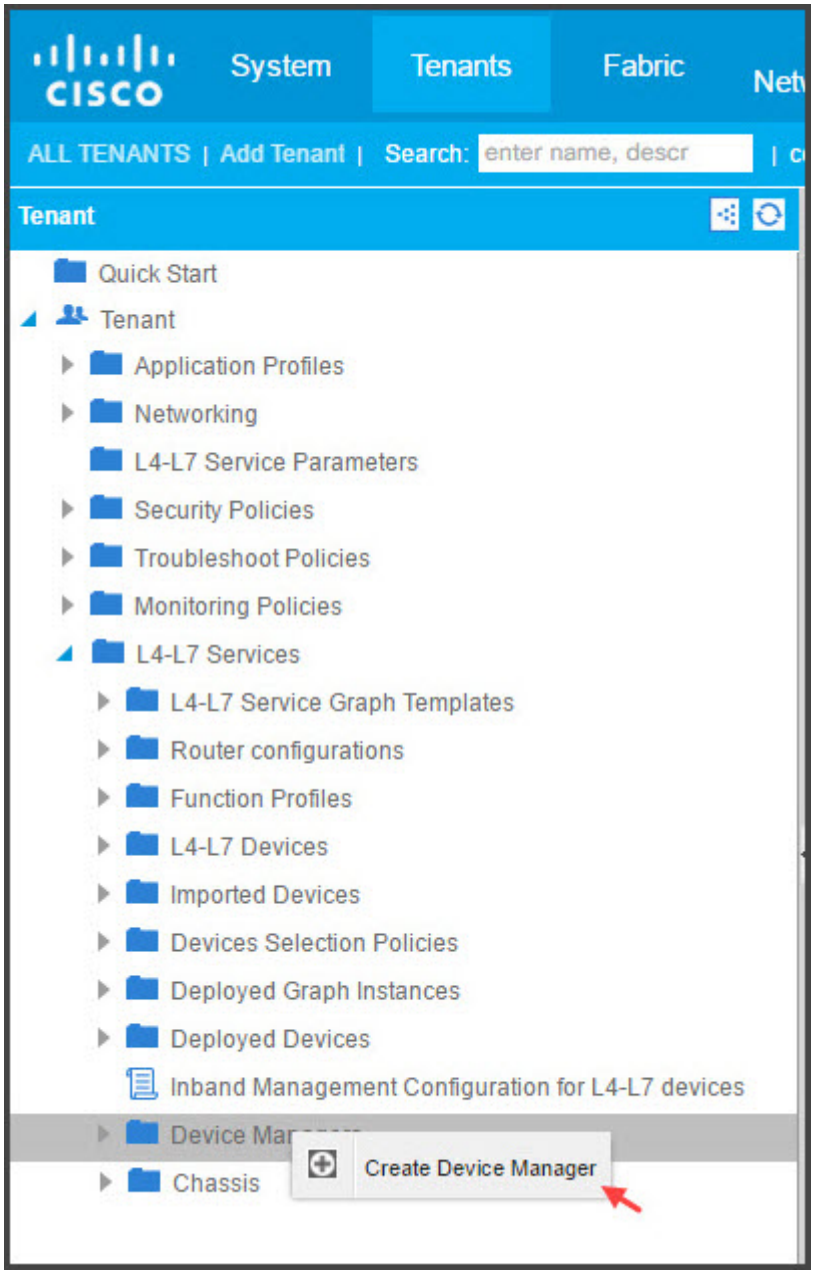
February 6, 2024

May 24, 2018

Citrix Application Delivery Management (ADM) 充当 Cisrix ACI 上部署的 Citrix ADC 的集中设备管理器。您需要在 Cisco APIC 中将 Citrix ADM 添加为设备管理器。

要使用 **APIC GUI** 将 **Citrix ADM** 添加为设备管理器，请执行以下操作：

1. 在菜单栏上，转到 租户 **>** 所有租户。
2. 在“工作”窗格中，双击租户的名称。
3. 在 导航 窗格中，选择 ***tenant_name* > L4-L7** 服务。
4. 右键单击“设备管理 器”，然后单击“创建设备管理器”。



5. 在“创建设备管理器”对话框中，执行以下操作：

a) 在“设备管理器名称”字段中，输入要注册为设备管理员的 Citrix ADM 部署的名称。

b) 在 **Management EPG**（管理 EPG）下拉列表中，选择管理 EPG。

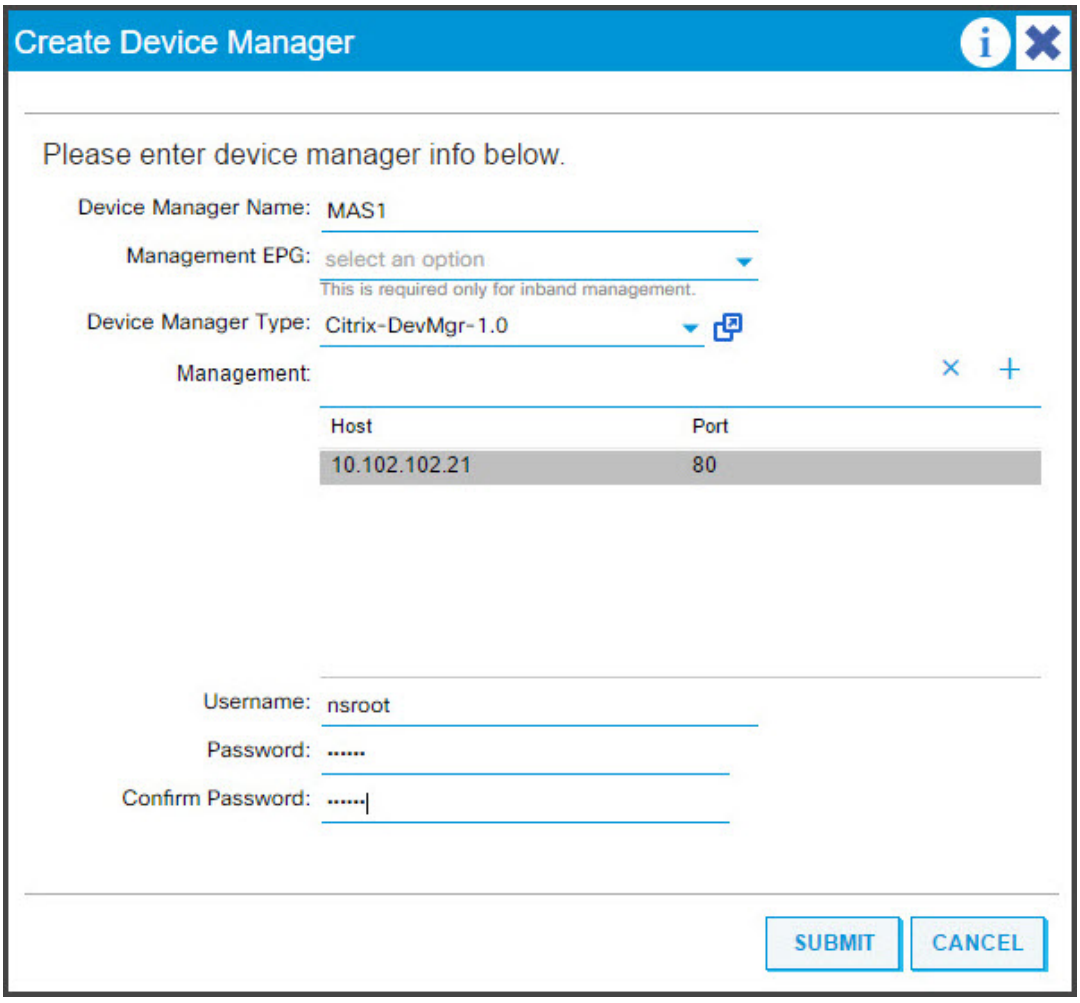
c) 在 **Device Manager Type**（设备管理器类型）下拉列表中，选择 **Citrix-DevMgr-1.0**。

d) 在“管理”字段中，单击 **+** 并添加 Citrix ADM 部署的 IP 地址和端口详细信息。

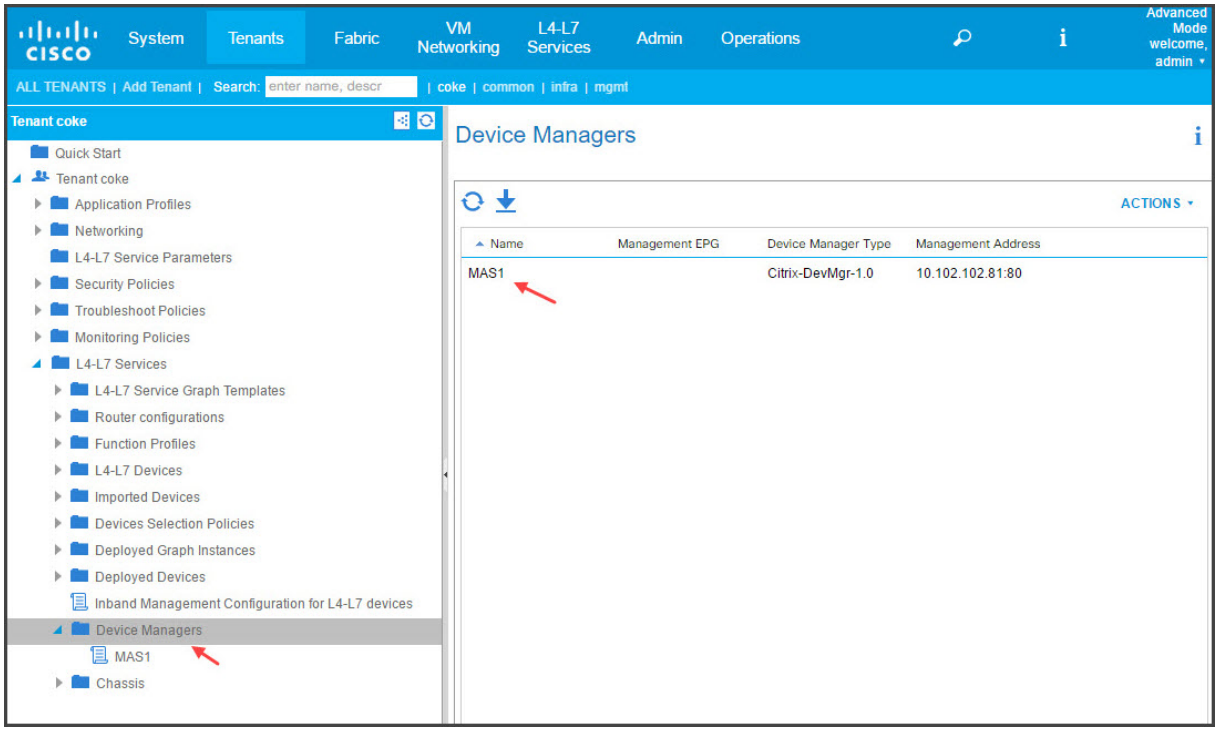
e) 在“用户名”字段中，输入用于访问 Citrix ADM 的用户名。

f) 在“密码”和“确认密码”字段中，输入访问 Citrix ADM 的密码。

g) 单击 **SUBMIT**（提交）。



一旦 Citrix ADM 在 APIC 中成功注册为设备管理器，便会添加设备管理器并显示在“导航”窗格中。要查看已注册的设备管理器，请在导航窗格中转到 ***tenant_name* > L4-L7** 服务 **>** 设备管理器。



> 注意
>
> 确保 Cisco APIC 和 Citrix ADM 之间没有连接问题，并且您提供的凭据与用于访问 Citrix ADM 的相同。还需确保帐户具有管理员权限。
>
> 重要
>
> 导入设备包后，请确保 APIC 中没有故障。可以单击“Device Types”（设备类型）窗口中的 **Faults**（故障）选项卡查看故障。

您还可以使用 API 将 Citrix ADM 注册为设备管理器。以下是示例 XML 有效负载，展示了如何使用 API 将 Citrix ADM 添加为设备管理器。

```
<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>
</polUni>
```


使用 **APIC** 将 **Citrix ADC** 添加为 **Cisco ACI** 中的设备

February 6, 2024

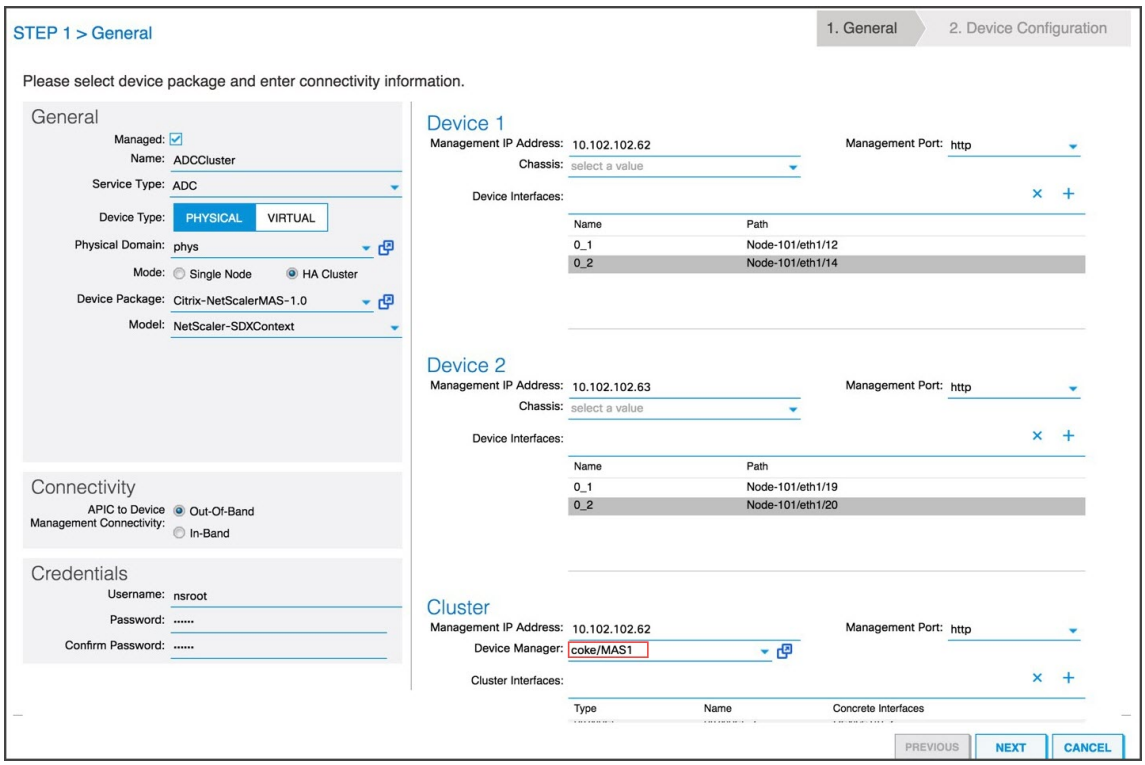
为了实现网络自动化，您需要将 Citrix ADC 作为 L4-L7 设备添加到 APIC 中。APIC 根据部署的服务图，在 Leaf 和 Citrix ADC 设备之间执行网络拼接。需要配置设备配置的基本设置，例如配置管理 IP 地址、设备管理器和凭据。

要使用 **APIC GUI** 将 **Citrix ADC** 注册为 **APIC** 中的设备，请执行以下操作：

1. 在菜单栏上，转到 租户 **>** 所有租户。
2. 在“工作”窗格中，双击租户的名称。
3. 在 导航 窗格中，选择 ***tenant_name* > L4-L7** 服务 **> L4-L7** 设备。
4. 在“工作”窗格中，选择“操作”**>**“创建 **L4-L7** 设备”。
5. 在“创建 **L4-L7** 设备”对话框的“常规”部分中，执行以下操作：
   a) 选中“托管”复选框。
   b) 在“名称”字段中，输入设备的名称。
   c) 在 **Service Type**（服务类型）下拉列表中，选择 **ADC**。
   d) 在 **Device Type**（设备类型）字段中，选择 **Physical**（物理）。

      > 注意：
      >
      > 对于 VMware ESX，请确保选择虚拟并关联相应的虚拟机管理器 (VMM) 域。

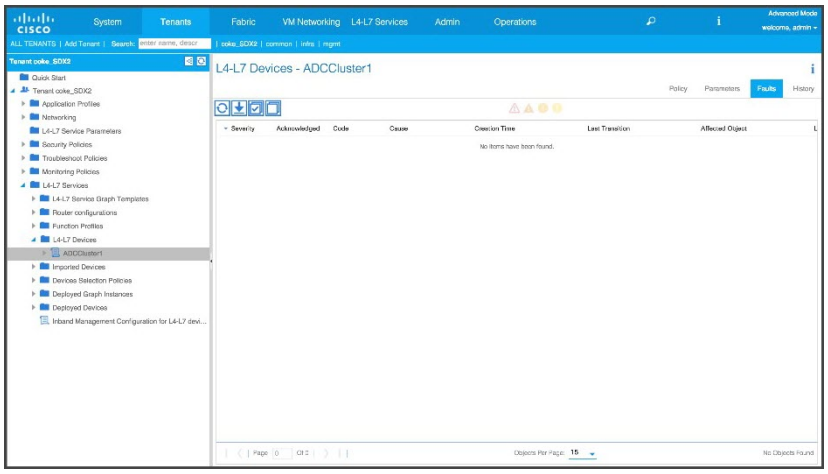
   e) 在 **Physical Domain**（物理域）下拉列表中，选择物理域。
   f) 在 模式 字段中，根据您的要求选择 单节点 或 **HA** 群集。
   g) 在 设备包 下拉列表中，选择 **Citrix-NetScalerMAS-1.0**。
   h) 在 型号 下拉列表中，选择设备型号。例如，Citrix ADC-MPX 或 Citrix ADC-VPX。
6. 在“连接”部分，在“**APIC** 到设备管理连接”字段中选择“带外”或“带内”，具体取决于架构中 Citrix ADC 的配置方式。
7. 在“凭据”部分中，指定用于访问设备的用户名和密码。
8. 分别在 设备 **1** 和 设备 **2** 部分中完成与管理相关的配置。
9. 在“群集”部分中，完成群集的管理相关配置。确保在 设备管理器 下拉列表中，选择在 C isco APIC 中将 Citrix ADM 添加为设备管理器中创建的设备管理器



10. 单击“下一步”。此时将显示“Device Configuration”（设备配置）页面。混合模式设备包不提供设备和群集特定的配置详细信息，例如高可用性、启用/禁用功能和模式以及有关 NTP、SNMP 和 SNMP 警报等的配置。这些配置必须通过使用 Citrix ADM 完成。

11. 单击“完成”。成功在 APIC 中注册了设备后，设备会添加并显示在“Navigation”（导航）窗格中。要查看注册的设备，请在导航窗格中转到 ***tenant_name* > L4-L7** 服务 **> L4-L7** 设备 **> device_name**。

> 重要
>
> 注册设备后，请确保 APIC 中没有故障。您可以通过单击“工作”窗格中的“错误”选项卡来查看故障。



您还可以使用 API 注册 Citrix ADC 设备。下面是添加 L4-L7 设备的示例 XML 有效负载：


```
<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]"/>

     </vnsCIf>

     <vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>

     <vnsCCred name="username" value="nsroot"/>

     <vnsCCredSecret name="password" value="****"/>

     </vnsCDev>

     <vnsCDev name="ADC2" devCtxLbl="C1">

     <vnsCIf name="1_1">

     <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1
        /34]"/>

     </vnsCIf>

     <vnsCIf name="1_2">

```



```
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/
              cIf-1_2"/>
78
79        <vnsRsCIfAtt tDn="uni/tn-coke/lDevVip-ADCCluster1/cDev-ADC2/
              cIf-1_2"/>
80
81        </vnsLIf>
82
83        </vnsLDevV
84
85        </fvTenant>
86
87        </polUni>
```

创建和部署服务图

February 6, 2024

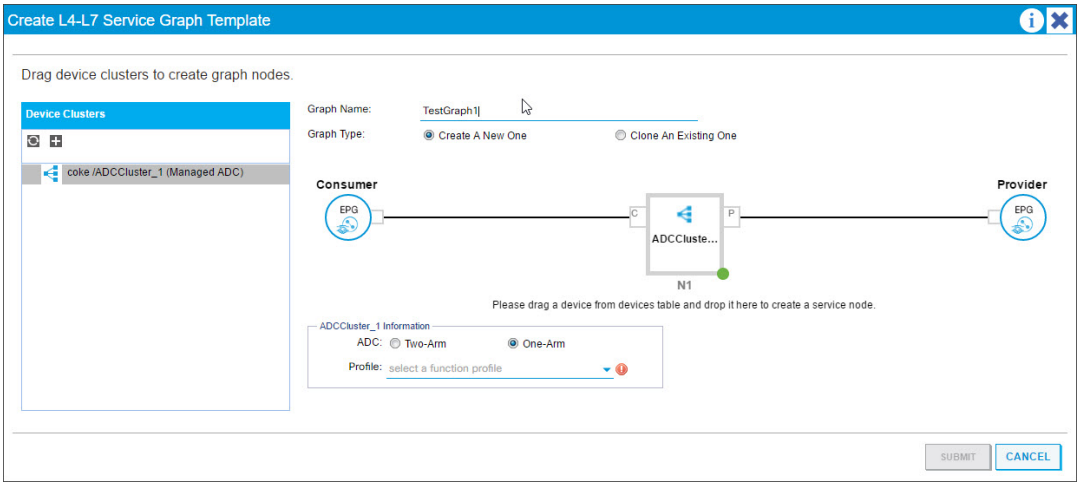
您必须在 APIC 中使用思科 APIC 服务图模板来创建和部署 Citrix ADC。请务必在创建和部署服务图时使用 ADC 功能配置文件。

在 APIC 中配置图形后，APIC 根据功能定义、与结构的设备连接以及配置为图形部署一部分的实体来自动完成设备配置。作为创建服务图的一部分，APIC 还自动完成网络配置（例如虚拟 LAN 分配及其绑定），在您从 APIC 删除图形后，该配置会立即被删除。

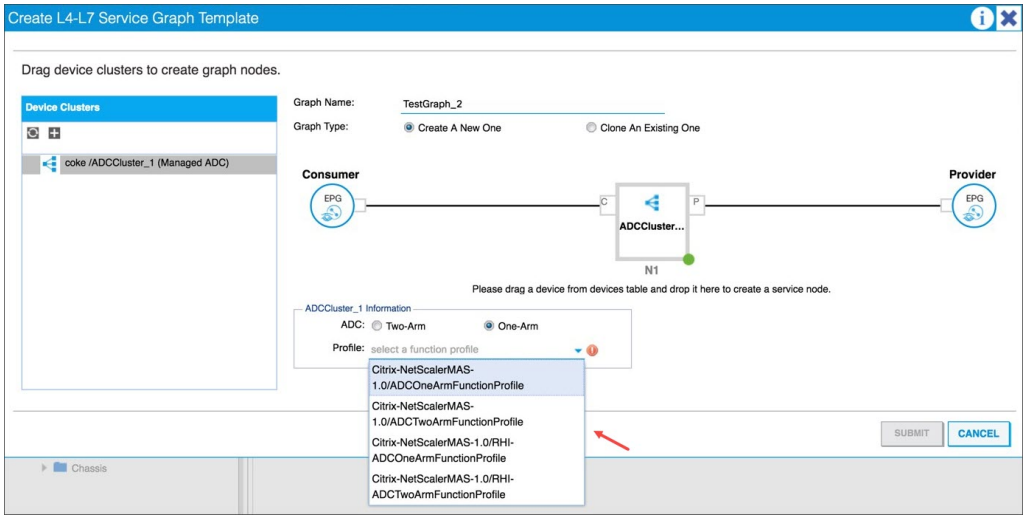
服务图以两层或多层应用程序表示，它们之间插入适当的服务功能。按照合同，在源和目标 EPG 之间插入服务图。

要使用 **APIC GUI** 创建服务图，请执行以下操作：

1. 在菜单栏上，转到 租户 **>** 所有租户。
2. 在“工作”窗格中，双击租户的名称。
3. 在 导航 窗格中，选择 ***tenant_name*** **> L4-L7** 服务 **> L4-L7** 服务图模板。
4. 在 工作 窗格中，选择 操作 **>** 创建 **L4-L7** 服务图模板。
5. 在“创建 **L4-L7** 服务图模板”对话框的“设备群集”部分中，选择设备群集并执行以下操作：
   a) 在 **Graph Name**（图形名称）字段中，输入服务图模板的名称。
   b) 在 **Graph Type**（图形类型）字段中，选择 **Create A New One**（创建一个新图）。
   c) 在 **Device Cluster**（设备群集）部分，将设备拖放在使用者端点组和提供商端点组之间以创建服务节点。



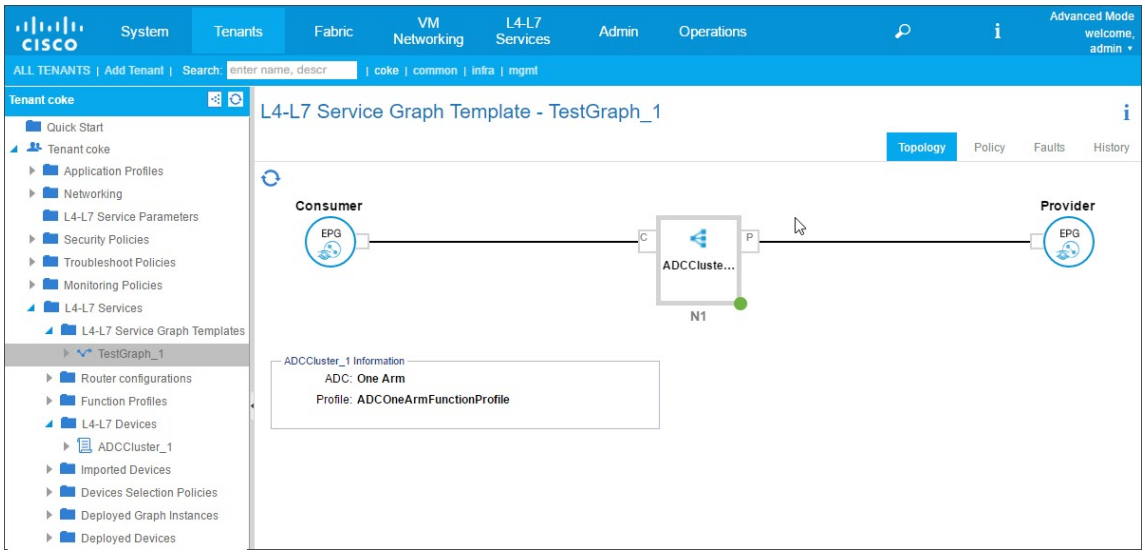
   d) 在 <***L4-L7device_name information***> 部分，执行以下操作：
      i. 在 **ADC** 字段中，选择“单臂”或“双臂”，具体取决于 Citrix ADC 在架构中的部署方式。
      ii. 在 配置文件 下拉列表中，选择设备包中提供的功能配置文件。



iii. 单击 **SUBMIT**（提交）。

6. 在 导航 窗格中，单击服务图模板。屏幕上将显示服务图模板的图形拓扑。

> 注意
>
> Cisco APIC 支持连接器的概念，这些连接器在 ADC 群集节点中可见。连接器定义网络流量方向和设备脚本，该脚本根据连接是外部还是内部，动态将分配的虚拟 LAN 绑定到虚拟 IP (VIP) 或子网 IP (SNIP) 地址。此外，虚拟 LAN 还绑定到用于入站流量和出站流量的特定接口。

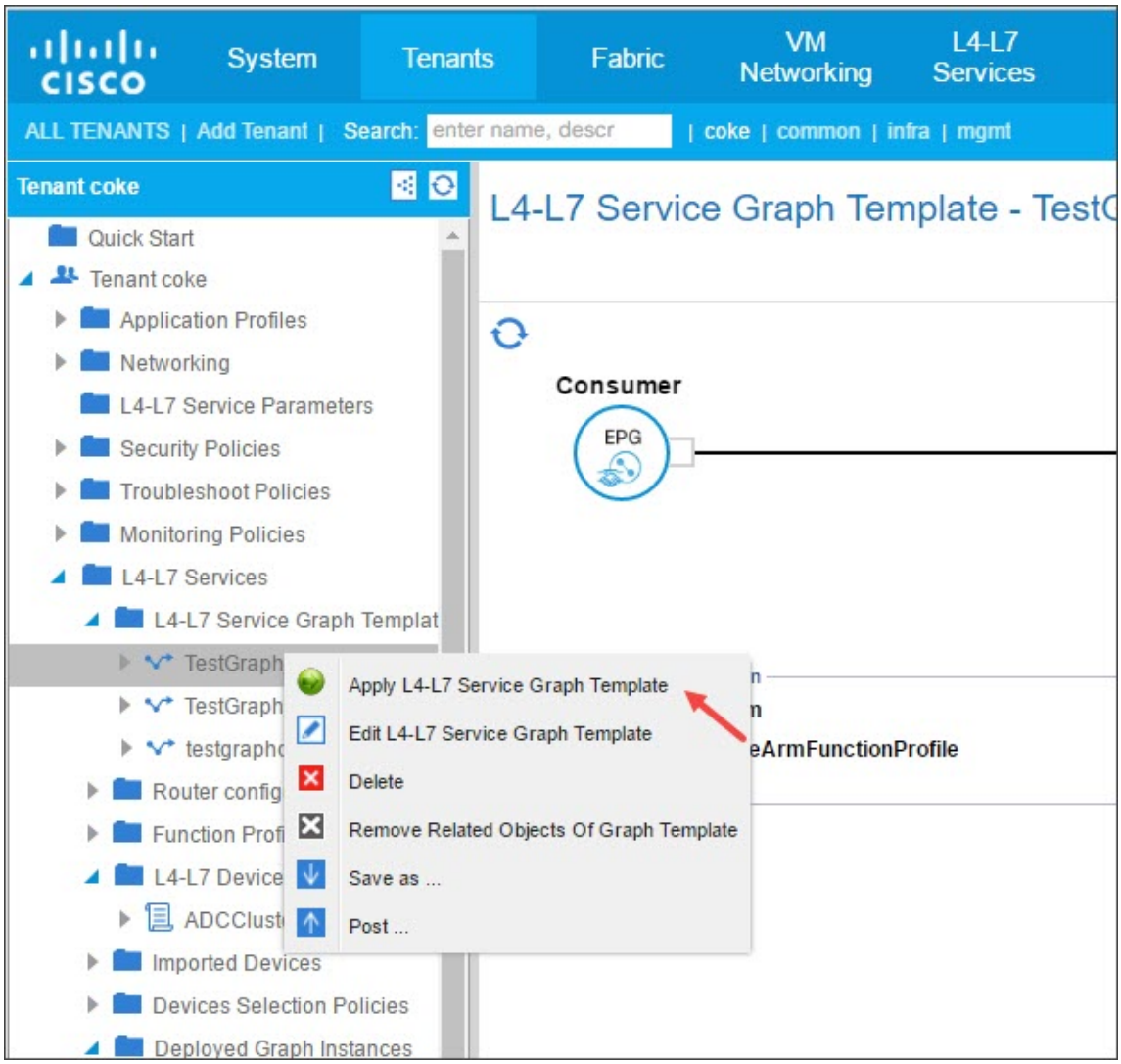


将服务图模板应用于端点组

创建了服务图模板后，需要使用 APIC GUI 来应用创建的服务图模板。

要应用服务图模板，请执行以下操作：

1. 在菜单栏上，转到 租户 **>** 所有租户。
2. 在“工作”窗格中，双击租户的姓名。
3. 在导航窗格中，选择 ***tenant_name*** **> L4-L7** 服务 **> L4-L7** 服务图模板。
4. 右键单击 ***template_name*** ，然后单击“应用 **L4-L7** 服务图形模板”。

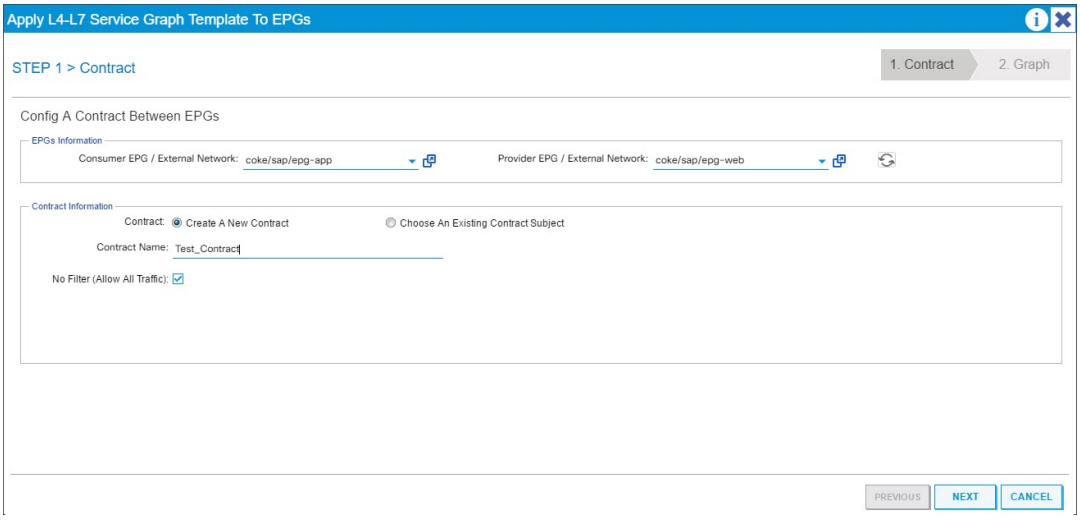


5. 在“将 **L4-L7** 服务图模板应用于 **EPG**”对话框的“**EPG** 信息”部分中，填写以下字段：

   a) 在 **Consumer EPG/External Network**（使用者 EPG/外部网络）下拉列表中，选择使用者端点组。

   b) 在 **Provider EPG/External Network**（提供商 EPG/外部网络）下拉列表中，选择提供商端点组。

   c) 在 **Contract Information**（合同信息）部分，完成适当的字段。合同信息与 Cisco APIC 特定相关，并作为与 EPG 关联的安全策略的一部分进行配置。



d) 单击下一步。

e) 在 图表模板 下拉列表中，选择您创建的服务图形模板。

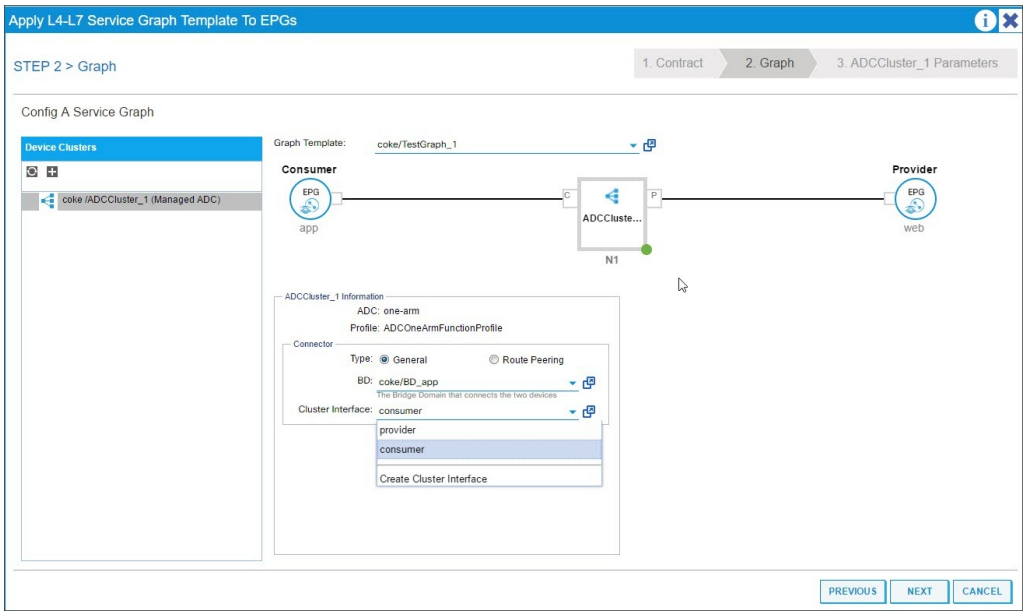
f) 在“连接器”部分中，执行以下操作：

i. 在“类型”字段中，选择“常规”。

ii. 在 **BD** 下拉列表中，选择网桥域。连接器详细信息属于包含在 Cisco APIC 基础结构模型中的桥接域的一部分。

iii. 在 **Cluster Interface**（群集接口）下拉列表中，为所选桥接域选择适当的群集接口。

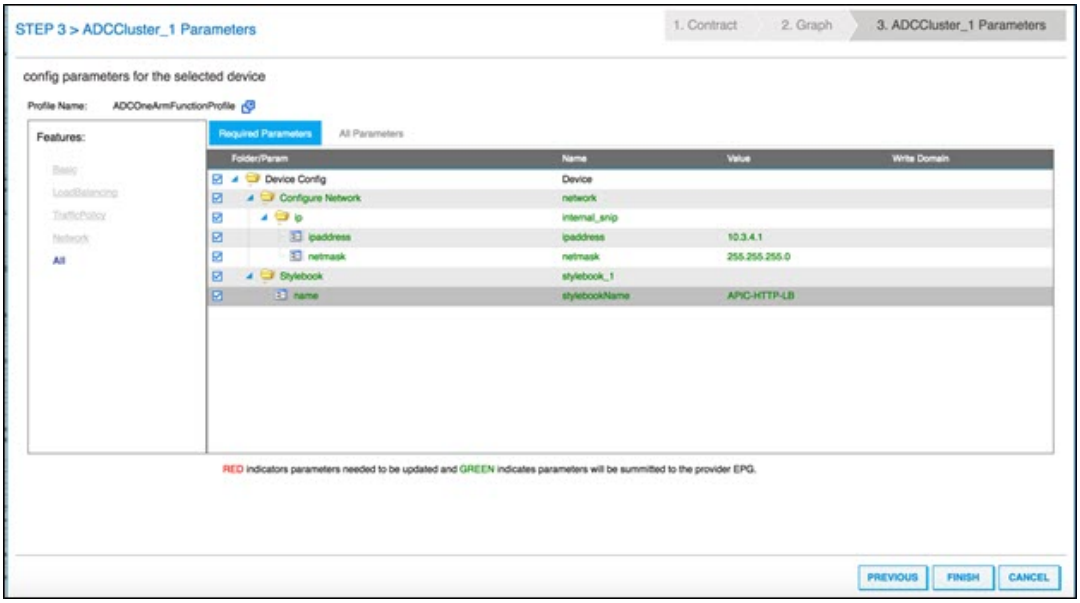
Cisco APIC 根据所选服务图模板的要求，将选定的网桥域用于 Citrix ADC 设备与结构之间的数据路径流量。



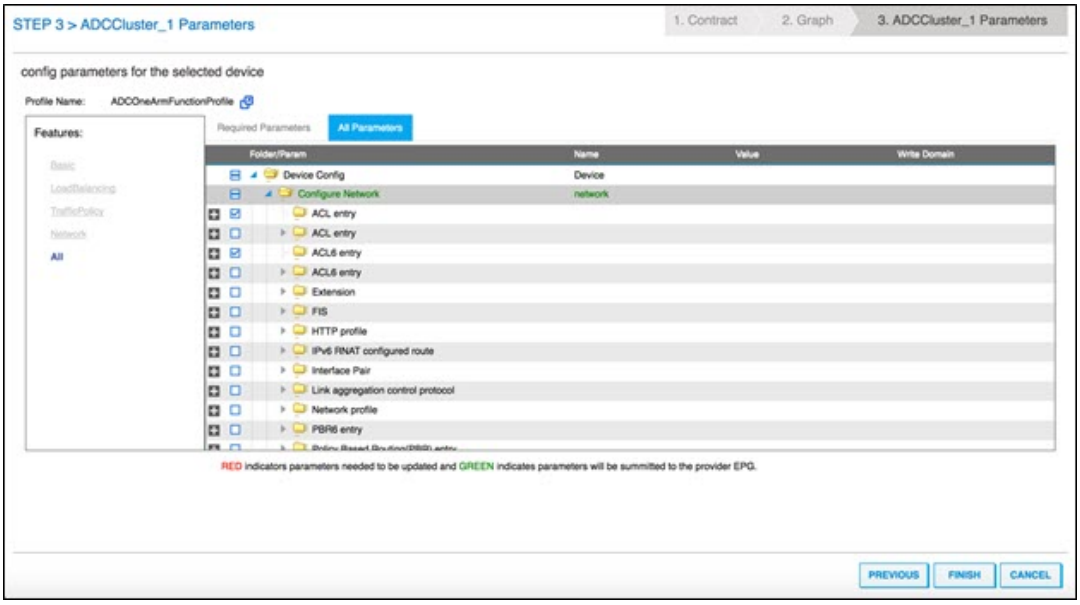
iv. 单击下一步。

在 参数 屏幕的 必填参数 选项卡上，输入 L2-L3 的特定详细信息，例如配置文件规定的 IP 地址。其他主要参数是样书名称。它可以是 Citrix Application Delivery Management (ADM) 中提供的内置样书 **APIC-HTTP-LB**，也可以提供在 使用 Citrix ADM 为应用程序创建样书中创建的样书的名称

> 注意
>
> 样书名称将服务图形详细信息与使用 Citrix ADM 为给定应用程序创建的 L4-L7 配置链接起来。



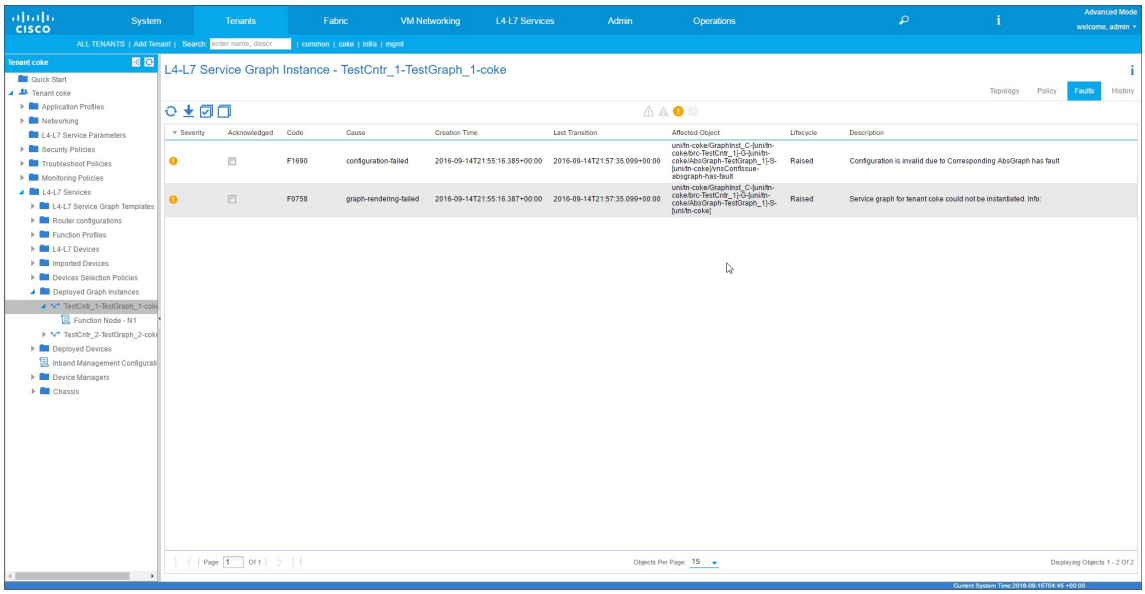
Cisco APIC GUI 允许根据功能（例如负载平衡）过滤参数。可以在 **Required Parameters**（所需参数）选项卡中查看和设置所有必要参数，可以在 **All Parameters**（所有参数）选项卡中查看和设置与功能有关的所有其他参数。



> 注意
>
> 默认情况下，内置单臂配置文件要求提供 SNIP 详细信息，例如 IP 地址和网络掩码。可以在 Cisco APIC GUI 中单击 **All Parameters**（所有参数）并展开 **Configure Network**（配置网络）树来查看其他网络连接参数。这将列出 Citrix ADC 支持的所有网络参数。可以从 Cisco APIC GUI 实例化任何实体，并为列出的属性提供值。

6. 单击完成。

> 重要
>
> 应用服务图模板后，请确保部署的图形中没有故障。您可以通过单击“工作”窗格中的“错误”选项卡来查看故障。



作为服务图形部署的一部分，混合模式设备包将配置详细信息从 Cisco APIC 推送到 Citrix ADM。Citrix ADM 在内部将这些配置处理到相应的 Citrix ADC，并将响应返回到 APIC。成功的图形部署将没有任何故障，并且 Citrix ADC 已成功地与相应图形的结构联网。

APIC 支持使用 API 以不同的方法来配置和部署图形，图形部署包括对 APIC 特定的一些构造的依赖项，例如租户、合同、虚拟 LAN 和命名空间。

下面的示例方法说明了其中一个方法，即利用 APIC 的 API 来创建和部署 L4-L7 图，假定已在 APIC 中配置 APIC 特定的工件。

> 重要
>
> 请务必将这些 XML 有效负载用作参考，并在您的环境中使用 XML 之前对其进行适当的更改。

下面是一个使用 API 创建和部署服务图的示例：

a) 创建 AppProfile

b) 创建服务图详细信息

c) 将服务图附加到合同

下面是一个用于创建 AppProfile 的示例 XML 有效负载。应用程序配置文件包含 EPG，提供程序 EPG 包含 Citrix ADC 特定的实体、属性及其值。在以下示例 XML 有效负载中，使用一组属性和样书名称创建 Citrix ADC 特定的网络实体（如 NSIP）。

```
<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>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
                    <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
```



```
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
                    <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    external_network" name="external_network">
                    <vnsCfgRelInst name="external_network_key" key
    ="external_network_key" targetName="Network/snip2"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
    " name="mFCngStylebook_1">
                    <vnsCfgRelInst name="Stylebook_key" key="
    Stylebook_key" targetName="stylebook_1"/>
                </vnsFolderInst>
                <!-- ------- END CONFIG PAYLOAD -------------- -->
                <fvSubnet ip="110.110.110.110/24" scope="shared"/>
                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
                <fvRsDomAtt tDn="uni/phys-sepg" />
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
            </fvAEPg>
            <!-- EPG 2 -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
                <fvRsCons tnVzBrCPName="Ctrct1"/>
                <fvRsBd tnFvBDName="BD_app" />
                <fvSubnet ip="220.220.220.220/24" scope="shared"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
                <fvRsDomAtt tDn="uni/phys-sepg" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

下面是一个用于创建服务图详细信息的示例 XML 有效负载：

```
<polUni>
    <fvTenant name="coke">
        <vnsAbsGraph name = "Graph1">
            <vnsAbsTermNodeProv name = "Input1">
                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
            </vnsAbsTermNodeProv>
            <vnsAbsNode name="ADC" funcType="GoTo">
                <vnsAbsFuncConn name = "outside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
                </vnsAbsFuncConn>
```



```
                <vnsAbsFuncConn name = "inside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
                </vnsAbsFuncConn>
                <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-
    NetScalerMAS-1.0/mFunc-ADCFunction"/>
                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/outtmnl"/>
                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix
    -NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-
    ADCOneArmServiceProfileGroup/absFuncProf-A
DCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-
    ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph
    -Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

下面是一个用于将服务图附加到合同的示例 XML 有效负载：

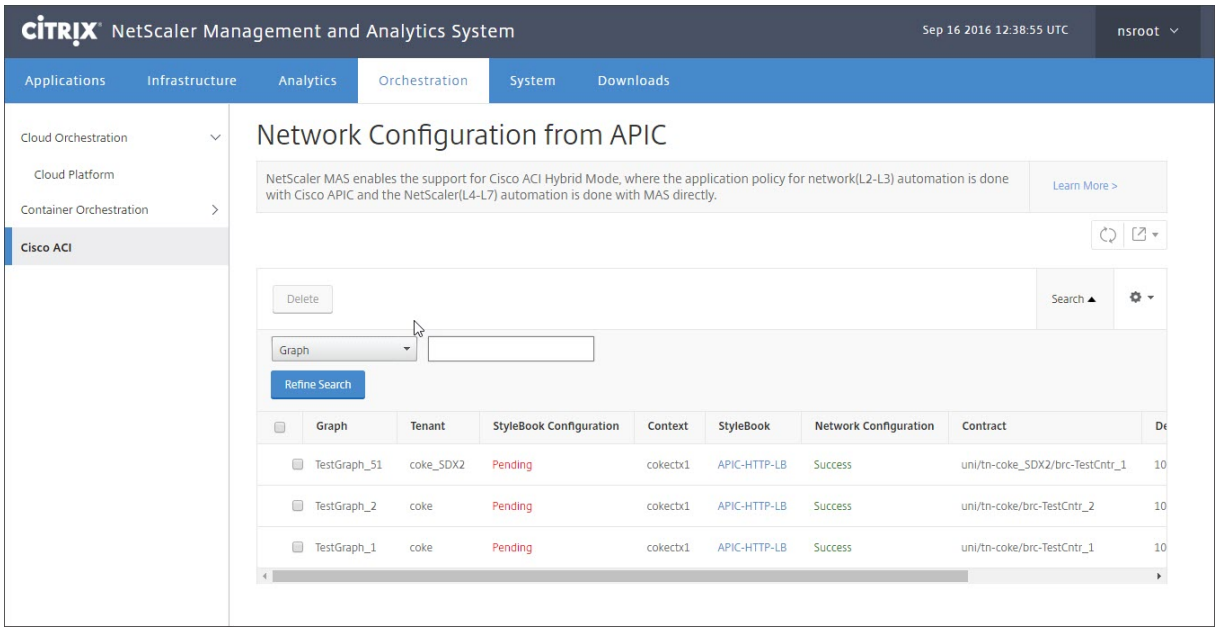
```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```


使用样书配置来自 **Citrix ADM** 的 **L4-L7** 参数

February 6, 2024

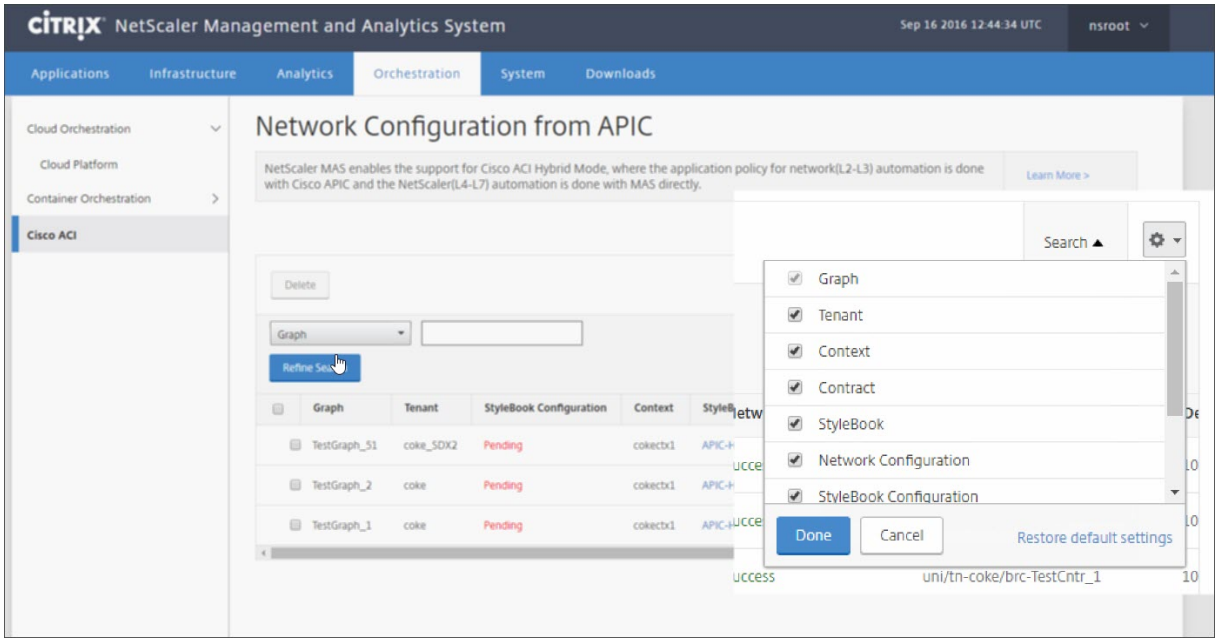
May 24, 2018

在 Citrix Application Delivery Management (ADM) 中，您可以在“业务 流 程”选项卡上的 C **isco ACI** 下查看已部署的服务图表详细信息。表格视图中显示服务图详细信息，例如图形名称、租户名称、上下文、样书名称及网络配置状态。



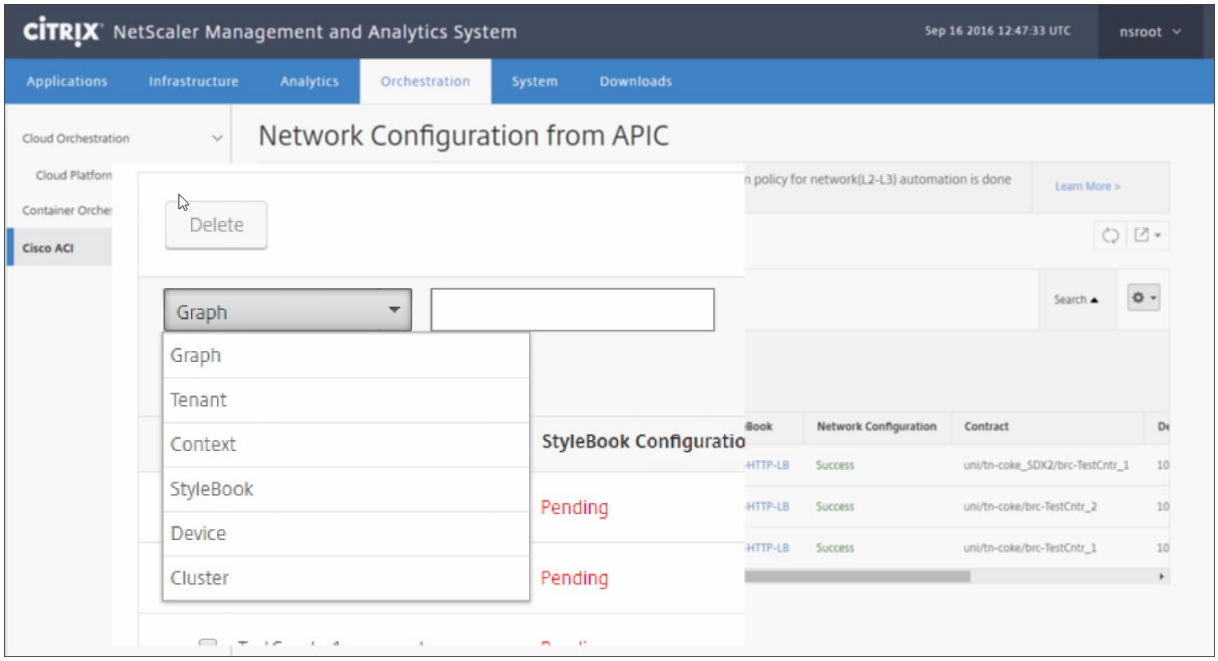
> 注意
>
> 如果从 Cisco APIC 删除了图形，对应的配置将从设备中删除，包括 L4-L7 配置。

此外，表格视图允许您对表中显示的任何列进行排序，以及使用“Search”（搜素）选项过滤数据。还可以从列的下拉列表中选择或取消选择列名来自定义列详细信息：



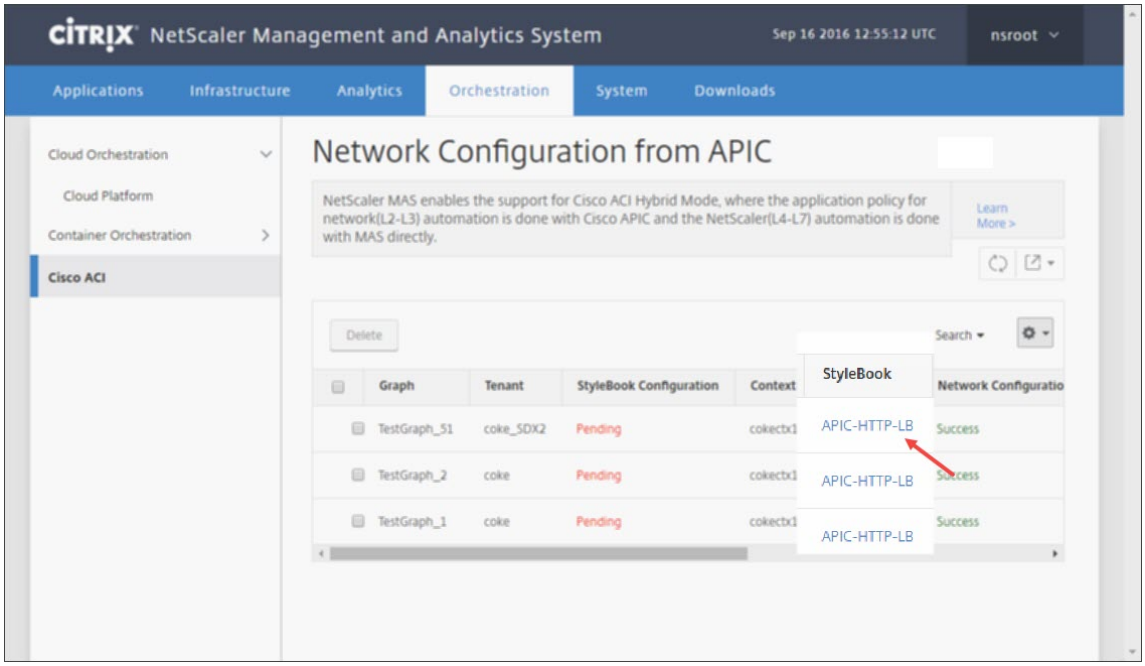
此外，可以单击 **Search**（搜索）按钮并使用搜索选项来过滤数据。可以从下拉框中选择任何列并输入对应的值来过滤表中显示的数据。

> 注意
>
> 搜索功能区分大小写，您必须提供精确的搜索条件。

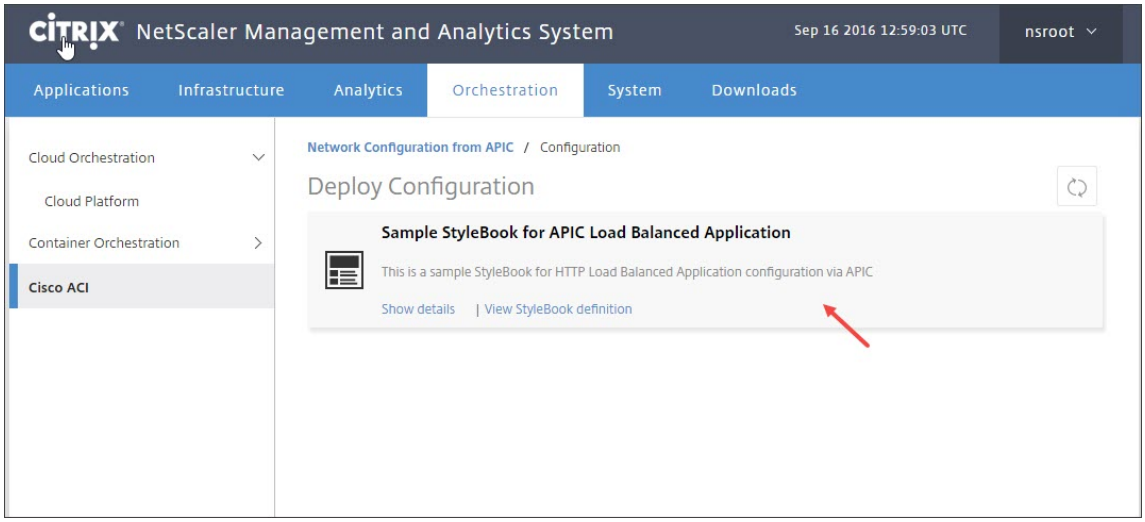


要在 Citrix ADM 中使用样书部署 L4-L7 配置，请执行以下操作：

1. 单击在表格视图中显示为 URL 的样书名称。



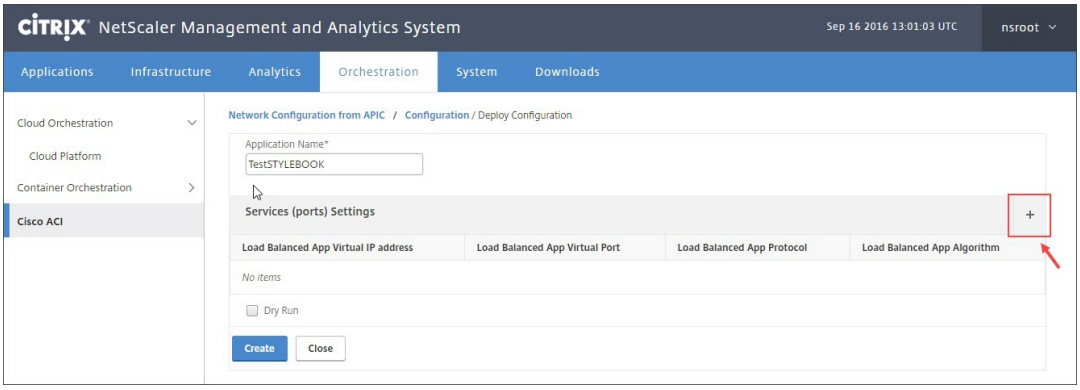
2. 在“配置”窗口中，双击样书。



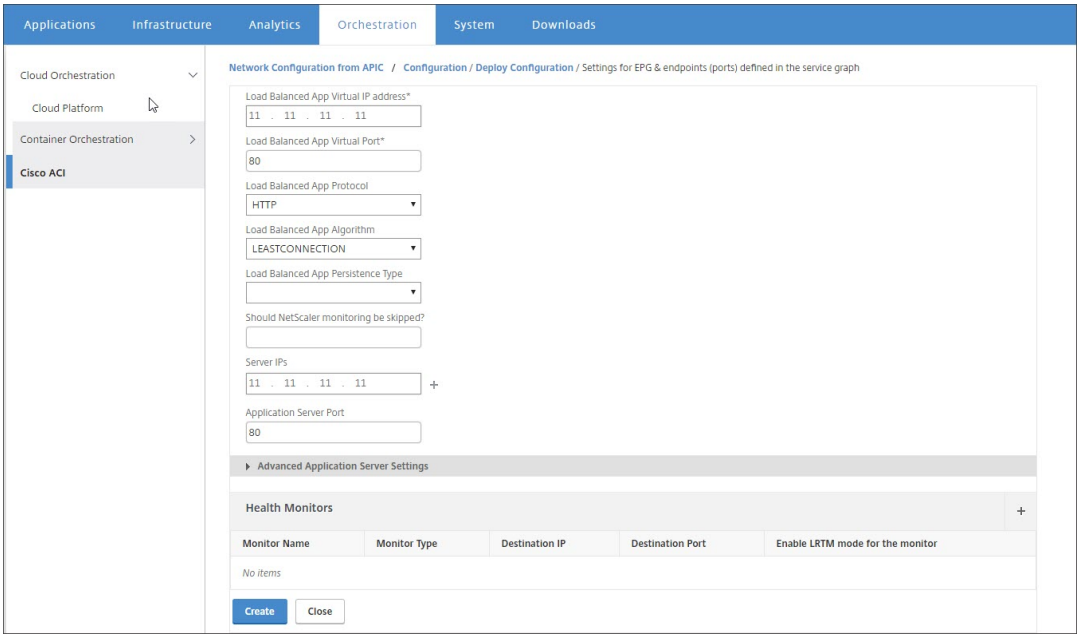
3. 在“Deploy Configuration”（部署配置）窗口中，执行以下操作：

   a) 在 **Application Name**（应用程序名称）字段中，输入与 APIC 中应用程序的服务图对应的 ADC 功能配置的名称。

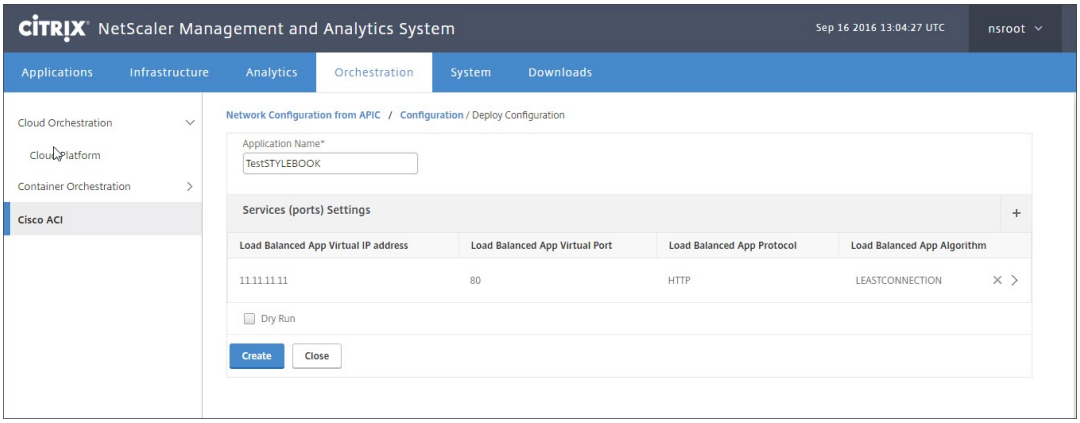
   b) 在“Service (ports) Settings”（服务 (端口) 设置）部分，单击 **+**。



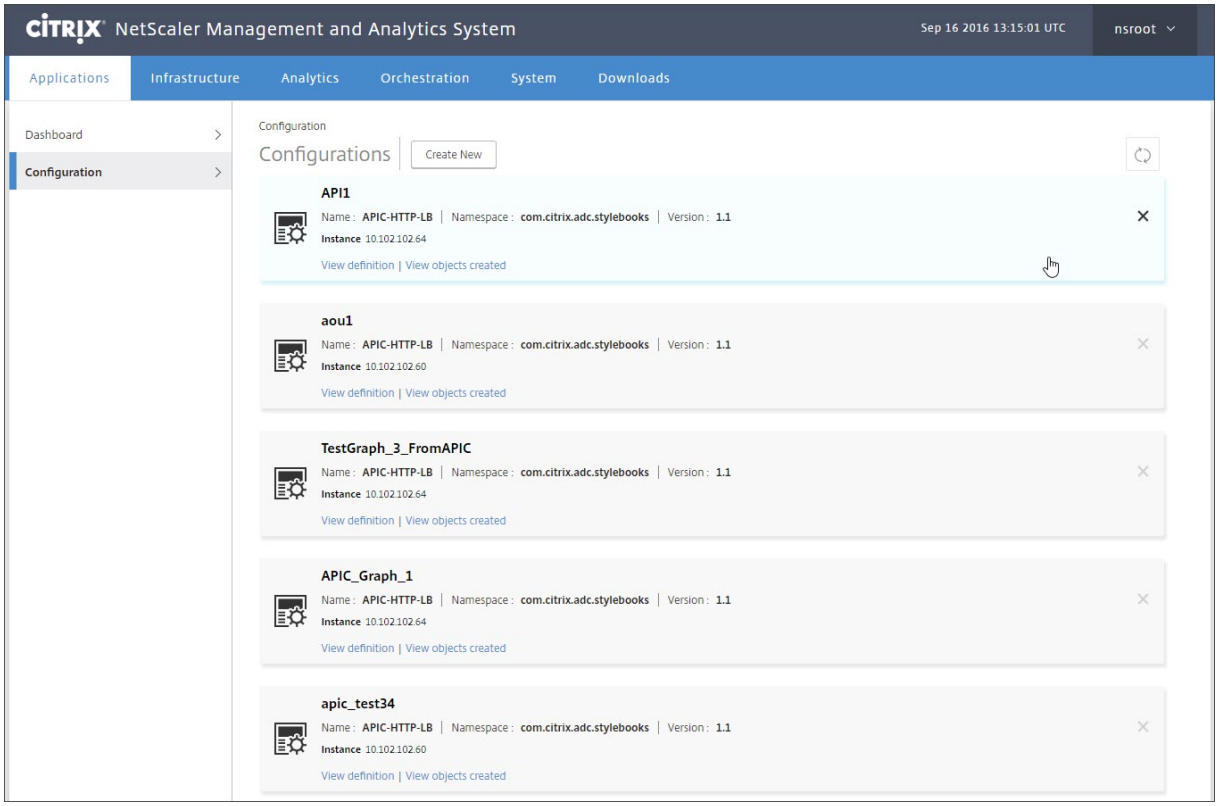
c) 在服务图窗口中定义的 **EPG** 和端点（端口）的设置中，输入从样书填充的参数的值，然后单击“创建”。



d) 单击创建。



在 Citrix ADM 中部署样书中指定的 L4-L7 配置。可以导航到 **Application**（应用程序）**> Configuration**（配置），在 **Application**（应用程序）选项卡中查看样书配置。



从 **APIC** 附加和分离端点事件

February 6, 2024

混合模式解决方案隐式处理 Cisco APIC 中的附加或分离端点事件。当 Cisco APIC 触发连接终端节点事件时，Citrix Application Delivery Management (ADM) 中的样书会自动触发服务组服务组成员绑定，并且在分离终端节点事件期间解除绑定。

此外，如果在 Cisco APIC 中触发连接或分离终端节点事件之前尚未在 Cisco ADM 中部署 L4-L7 配置，则解决方案将在数据库中保留连接 IP 地址。在通过样书创建了服务组后，这些 IP 地址被绑定到对应的服务组。

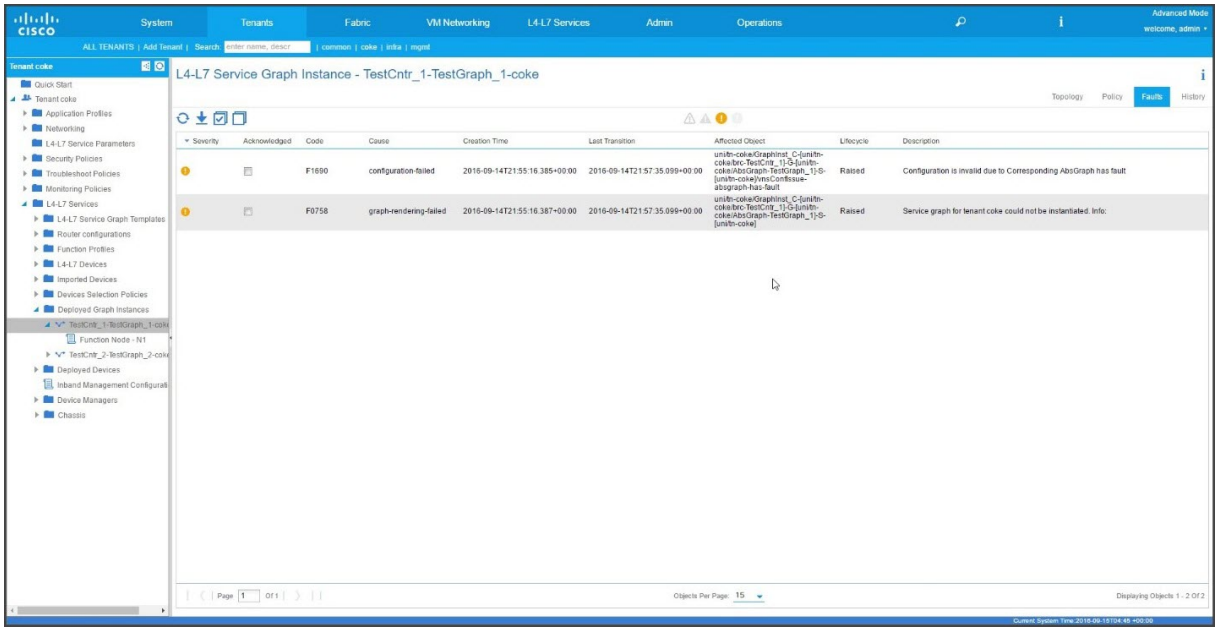
APIC 故障报告

February 6, 2024

在 Cisco ACI 中部署 Citrix ADC 设备包时，思科 APIC 会报告任何故障。可以查看 APIC 任何级别（例如，设备、租户、EPG 或服务图）的故障报告。下面的屏幕截图显示了设备级别的故障报告。有关故障的更多信息，请参见

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。

选择任何 APIC 实体并单击 **Faults**（故障）选项卡可显示 APIC 针对该实体报告的故障。



由 **Citrix ADM** 生成的日志

February 6, 2024

Citrix Application Delivery Management (ADM) 提供了大量的日志记录，可帮助解决问题。生成的日志 (**admin.log**) 位于：**/var/controlcenter/log/**

您可以登录到 Citrix ADM，然后使用命令行管理程序导航到 Citrix ADM 目录结构。以下是用于 APIC 图形部署的 Citrix ADM 日志的示例片段。

```
    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 }
 }
 }
 }
 }
 }
, '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]]' }
, (4, 'Network', 'network'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'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
            Details  = 10.102.102.62 +++++++++++++++++
88      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89      2016-06-29 10:58:33,867 DEBUG Host name from device =
           ADCHybridMode_1
90      "InProgress","message":null,"replication_status":"","target":"
           10.102.102.81","operation":"POST","entity_type":"apic","
           entity_id":null }
91    }
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
```



```
          Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
          }
100    ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102    }
103    collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
          0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
       (3, 'ADCFunction', 'N1')], 0) }
109    }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
          []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
       : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116    "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
       D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764

118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
120   '10.102.102.62': {
121   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
       u'NONE', 'operation_name': 'add_op' }
122    }
123   , (7, '', '2129920_32778'): {
124   'vlan': {
125   u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
       u'NONE', 'operation_name': 'add_op' }
126    }
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 = {
161   0: [], 1: [], 3: [] }
162
163      2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList
           = []
164      2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps
          attachIpList = [] dettachIpList = []
165      2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
166   '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 }
167
168 <!--NeedCopy-->
```

混合模式设备包生成的日志

February 6, 2024

Citrix ADC 混合模式设备包生成与配置相关的日志和监视相关的日志。生成的日志位于 **/data/devicescript/Citrix.NetScalerMAS.1.0/logs**。

下面是 Cisco APIC 的 **debug.log** 的示例代码段：

```
1     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
2     2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
         24063] +++++++++++++++ serviceAudit  request ++++++++++++++++++
3     2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
         24063] ++++++++++ getStyleBookObjects ++++++++++++
4     2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
         24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
          {
5   'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
6   (5, 'name', 'stylebookName'): {
7   'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
       }
8    }
9    }
10
11    2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
         24063] NMAS collection styleBookName= APIC-HTTP-LB
12    2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
         24063] NMAS collection retCol= {
13  'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
       'stylebook_1')) }
14
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
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
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: []
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
89 <!--NeedCopy-->
```

Cisco ACI 云管协调程序模式下的 Citrix ADC 设备包

February 6, 2024

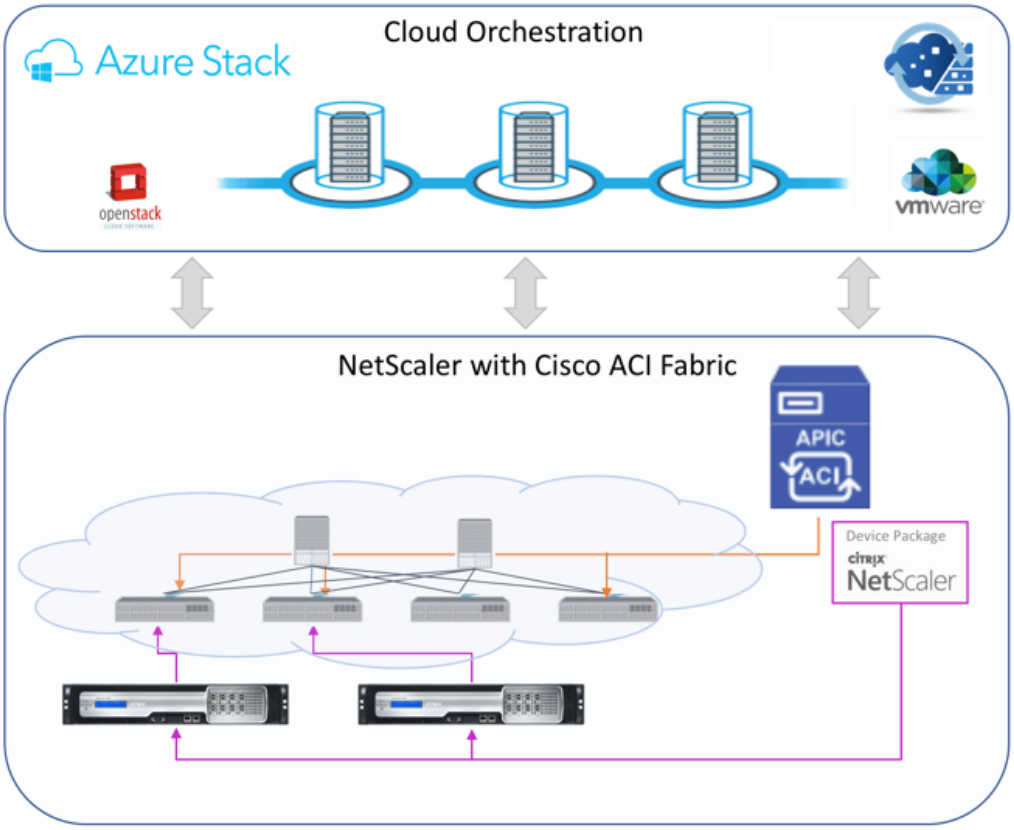
借助 Application Policy Infrastructure Controller (APIC) 3.1 版，Citrix ADC 和 Cisco ACI 扩展了联合集成产品组合，以提供满足客户需求的新解决方案。新的集成模式 ACI 云调配程序模式 ** 通过标准化参数抽象配置复杂性，简化了 L4-L7 的集成。该解决方案无缝协作以使 L4-L7 服务自动化，从而实现敏捷应用程序部署、运营灵活性和简便性的目标。

使用 Citrix ADC 解决方案的 Cisco ACI 云协调程序模式具有以下优势：

- L4-L7 服务的自动化减少了人为错误。
- Cisco ACI 解决方案的预构建集成可帮助您缩短部署时间，并提高 Web 应用程序、虚拟机和 SQL 等应用程序的性能。
- 跨物理和虚拟网络组件全面集成对应用程序（例如 Web 应用程序、虚拟机和 SQL）的运行状况的可见性。

ACI 云调配程序模式现在为您提供了更多选择，可以直接使用新的简化的 APIC GUI，或者根据自己的喜好选择任何云调配程序，例如 Cisco Cloud Center、Windows Azure Pack、OpenStack、vRealize 或任何其他云调配程序这一新变化是通过将一组 ADC 属性公开为 ADC 架构来实现的。这些属性映射到设备包函数配置文件中。您可以在云调配程序（Cisco Cloud Center 或无线应用协议 (WAP)）配置 ADC 服务时为这些属性提供值。

下图概述了云编排解决方案中的 Citrix ADC：



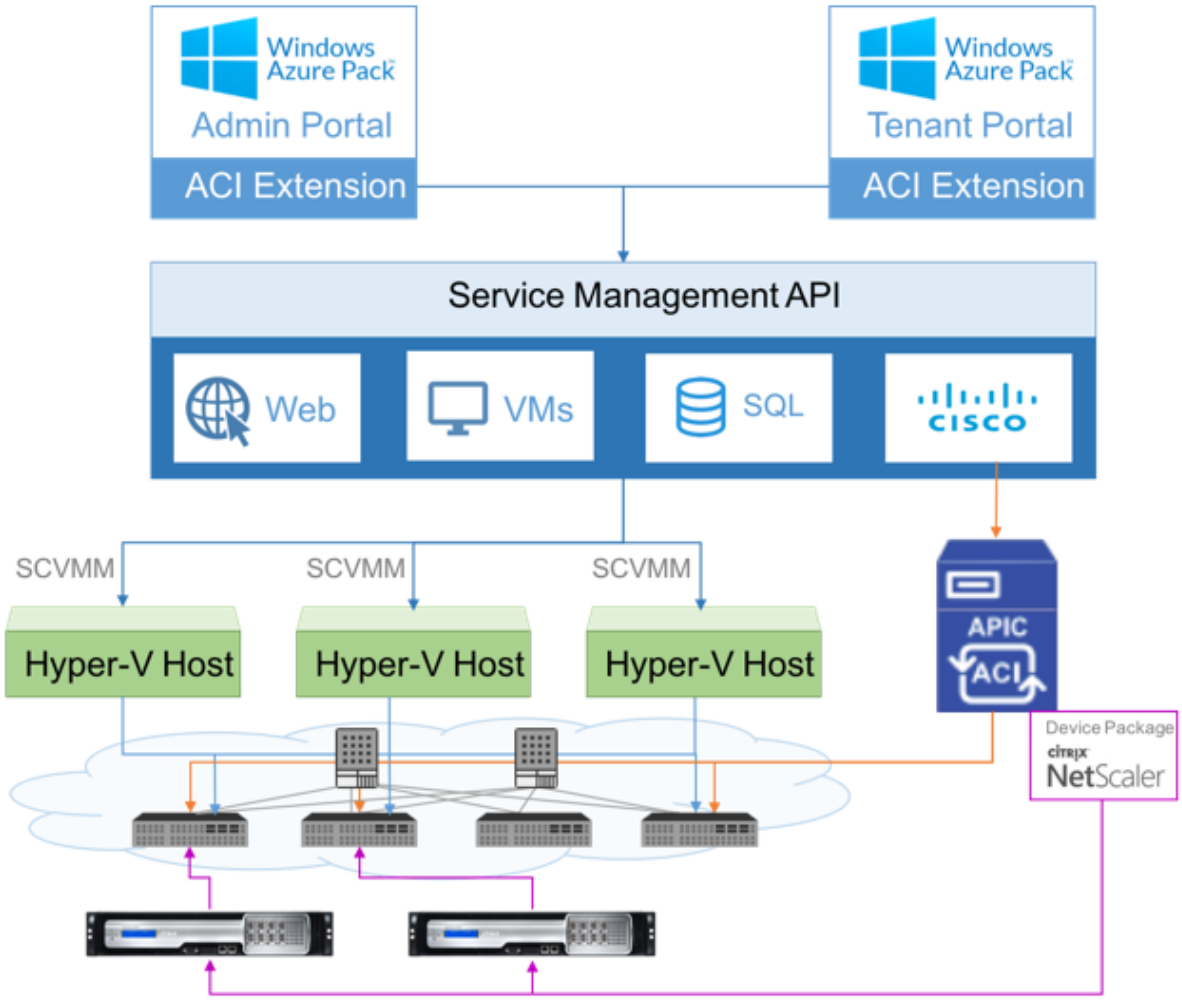
使用 Microsoft Azure 包的云协调程序模式解决方案涉及许多集成点，例如 Azure 包到 Cisco APIC、Cisco APIC 到系统中心虚拟机管理器 (SCVMM)，Cisco APIC 到 Citrix ADC。作为私有云中的租户，您可以启用 NAT、配置网络服

务以及添加负载平衡器。

Azure Pack 支持租户和管理员门户，每个门户都有自己的一组可执行的操作。

- 作为管理员，您可以执行管理任务，例如 ACI 注册、VIP 范围、Citrix ADC 设备与虚拟机云的关联以及租户用户帐户创建。
- 作为租户，您可以执行诸如登录 Azure Pack 租户门户和配置网络、桥接域和虚拟路由和转发 (VRF) 等任务，还可以使用 Citrix ADC 负载平衡和 RNAT 功能。

下图概述了云模式解决方案中的 Azure 包：



> 重要
>
> - 云管理员可以协助使用 APIC 支持的 L4-L7 架构，任何其他更改都可以由 APIC 管理员直接在 APIC 中完成。这样，您就可以配置和部署 Citrix ADC，使其与受支持的功能集相同。
> - 租户可以为同一网络部署具有不同端口的多个 VIP 地址。必须确保 IP 和端口组合是唯一的。

> - Citrix ADC 设备包仅支持单上下文部署。每个租户都将获得一个专用的 Citrix ADC 实例。
> - 无线应用程序协议 (WAP) 支持 Citrix ADC MPX 设备和 Citrix ADC VPX 设备（包括部署在 Citrix ADC SDX 平台上的 Citrix ADC VPX 实例）。

云调配程序模式设备包同时支持完全托管模式和服务管理器模式。完全托管模式包支持各种功能配置文件，例如简单负载平衡、内容交换、SSL 卸载和其他配置文件。这些功能配置文件涵盖了 Citrix ADC 的完整功能集和部署模式。同样，服务管理器模式设备包支持单臂和双臂配置以及使用 APIC 部署 Citrix ADC。Citrix Application Delivery Management (ADM) 充当 APIC 的服务管理器，您可以使用 Citrix ADM 配置 Citrix ADC L4-L7 参数。

> 注意
>
> 在服务管理器模式（混合模式）下，您无法重复使用或重新分配相同的服务器 IP 地址，该地址已存在于 Citrix ADC 设备中。

云调配程序模式功能配置文件有一组映射到 APIC ADC 架构的参数，并且调配程序将使用这些参数。云协调程序提供 ADC 参数的值（VIP，同时通过 APIC 预配 Citrix ADC）。调配程序与 APIC 的 API 进行通信，并将 ADC 的特定详细信息作为特定功能配置文件的有效负载的一部分进行传递。在内部，APIC 提取值并将其传递给在内部配置 Citrix ADC 的设备包。

有关 Cisco APIC 支持的 ADC 架构的完整列表的详细信息，请参阅 Cisco APIC 第 4 层至第 7 层服务部署指南，版本 3.x 及更高版本）。

完全托管模式设备包支持以下功能配置文件：

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
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

服务管理模式设备包支持以下云模式功能配置文件：

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

Citrix ADC 支持上述功能配置文件。APIC 在 ADC 架构中支持这些参数的子集。如果功能配置文件中存在 Cisco ACI 不支持的属性，则必须克隆云调配程序模式功能配置文件，并由 APIC 为所有不受支持的属性提供值，并且必须保存这些属性。稍后，调配程序可以使用新克隆的功能配置文件。

Citrix Cloud 模式设备包支持 Citrix ADC 12.0，服务管理器模式也使用 Citrix ADM 12.0。设备包已将模型版本从 1.0 更改为 2.0，可以用作新安装。云调配模式模式设备包无法从以前的设备包版本升级，因为模型版本已更改。

云调配程序模式设备包也可以在常规部署中使用。该包不强制用户通过任何云协调程序预配 Citrix ADC。该设备包仅与 APIC 兼容，而 APIC 与云调配程序兼容。

Citrix ADC 池容量

February 6, 2024

Citrix ADC 池容量允许您跨不同 ADC 外形共享带宽或实例许可证。对于基于虚拟 CPU 订阅的实例，您可以跨实例共享虚拟 CPU 许可证。将此池容量用于位于数据中心或公有云中的实例。当实例不再需要资源时，它会将分配的容量重新检查到公用池中。将释放的容量重用于需要资源的其他 ADC 实例。

您可以使用池化许可，通过确保为实例分配必要的带宽而不是超出其需要的带宽来最大限度地提高带宽利用率。在不影响流量的情况下，增加或减少在运行时分配给实例的带宽。使用池容量许可证，您可以自动执行实例 Provisioning。

Citrix ADC 池容量许可的工作原理

Citrix ADC 池容量包含以下组件：

- Citrix ADC 实例，可以分为以下几类：
  - 零容量硬件
  - 独立 VPX 实例或 CPX 实例
- 带宽池
- 实例池
- Citrix ADM 配置为许可服务器

零容量硬件

当通过 Citrix ADC 池容量进行管理时，MPX 和 SDX 实例称为“零容量硬件”，因为这些实例在从带宽和实例池中检出资源之前无法正常工作。因此，这些平台也被称为 MPX-Z 和 SDX-Z 设备。

零容量硬件需要平台许可证才能从公共池中检出带宽和实例许可证。但是，您不能将 Citrix ADC 池容量用于另一个 Citrix ADC 硬件实例。

管理和安装平台许可证。您必须通过使用硬件序列号或许可证访问代码手动安装平台许可证。安装平台许可证后，它将锁定到硬件，无法按需在 Citrix ADC 硬件实例之间共享。但是，您可以手动将平台许可证移动到另一个 Citrix ADC 硬件实例。

运行 ADC 软件版本 11.1 的 ADC MPX 实例构建 54.14 或更高版本，运行 11.1 的 ADC SDX 实例构建 58.13 或更高版本支持 ADC 池容量。有关详细信息，请参阅 表 **1**。**MPX** 和 **SDX** 实例支持的池容量。

独立 **Citrix ADC VPX** 实例

在以下虚拟机管理程序上运行 Citrix ADC 软件版本 11.1 Build 54.14 及更高版本的 Citrix ADC VPX 实例支持池容量：

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

在以下虚拟机管理程序和云平台上运行 Citrix ADC 软件版本 12.0 Build 51.24 及更高版本的 Citrix ADC VPX 实例支持池容量

- Microsoft Hyper-V
- AWS
- Microsoft Azure

> 注意
>
> 要启用 Citrix ADM 与 Microsoft Azure 或 AWS 之间的通信，必须配置 IPSEC 隧道。 有关更多信息，请参阅将部署在云端的 Citrix ADC VPX 实例添加到 Citrix ADM。
> 与零容量硬件不同，VPX 不需要平台许可证。为了处理流量，它必须从池中签出带宽和实例许可证。

独立的 **Citrix ADC CPX** 实例

部署在 Docker 主机上的 Citrix ADC CPX 实例支持集容量。与零容量硬件不同，CPX 不需要平台许可证。为了处理流量，它必须从池中签出实例许可证。

带宽池

带宽池是 Citrix ADC 实例（物理和虚拟）可共享的总带宽。带宽池包含用于每个软件版本（标准版、企业版和铂金版）的单独池。给定的 Citrix ADC 实例不能同时检出来自不同池的带宽。可从其签出带宽的带宽池取决于为其许可的软件版本。

实例池

实例池定义了可通过 Citrix ADC 池容量管理的 VPX 实例或 CPX 实例的数量，或 SDX-Z 实例中的 VPX 实例数量。

从池中签出许可证时，该许可证解锁 MPX-Z、SDX-Z、VPX 和 CPX 实例的资源，包括 CPU/PE、SSL 核心、每秒数据包以及带宽。

> 注意
>
> SDX-Z 的管理服务不使用实例。

Citrix ADM 许可证服务器

Citrix ADC 池容量使用配置为许可服务器的 Citrix ADM 软件来管理池容量许可：带宽池许可和实例池许可。您无需获得 ADM 许可即可使用 Citrix ADM 管理池容量许可。

从带宽和实例池中签出许可证时，零容量硬件上的 Citrix ADC 外形规格和硬件型号决定

- Citrix ADC 实例在正常运行之前必须签出的最小带宽和实例数。

- Citrix ADC 可以签出的最大带宽和实例数。
- 每个带宽签出的最低带宽单位。最小带宽单位是 Citrix ADC 必须从池中签出的最小带宽单位。任何签出都必须是最低带宽单位的整数倍数。例如，如果 Citrix ADC 的最小带宽单位为 1 Gbps，则可以检出 100 Gbps，但不能检出 200 Mbps 或 150.5 Gbps。最低带宽单位与最低带宽要求不同。Citrix ADC 实例只有在获得至少最小带宽许可后才能运行。一旦达到最低带宽，实例可以使用最小带宽单位检查更多带宽。

表 1、2 和 3 汇总了所有支持的 NetScaler 实例的最大带宽/实例、最小带宽/实例和最小带宽单位。表 4 总结了不同外形规格的许可证要求。对于所有支持的 Citrix ADC 实例：

表 **1. MPX** 和 **SDX** 实例支持的池容量

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
MPX 5900Z	10	1	不适用	不适用	1 Gbps
MPX 8005Z	15	5	不适用	不适用	1 Gbps
MPX 8900Z	33	5	不适用	不适用	1 Gbps
MPX-14000Z 系列	100	20	不适用	不适用	1 Gbps
MPX-15000Z 系列	100	20	不适用	不适用	1 Gbps
MPX-25000Z-40G	200	100	不适用	不适用	1 Gbps
MPX-24000Z 系列	150	100	40	80	1 Gbps
SDX 8015Z	15	2	1	5	1 Gbps
SDX 89XX 系列	33	10	2	7	1 Gbps
SDX-115XX 系列	42	7	2	20	1 Gbps
SDX-14000Z 系列	100	10	2	25	1 Gbps
SDX 15000Z-50G	100	10（注意：低于 12.1 54.x 的版本为 20 Gbps）	2（注意：低于 12.1 54.x 的版本为 5 个实例）	55	1 Gbps

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
SDX-15000Z	100	10（注意：低于 12.1 54.x 的版本为 20 Gbps）	2（注意：低于 12.1 54.x 的版本为 5 个实例）	55	1 Gbps
SDX-22XXX 系列	120	20	10	80	1 Gbps
SDX-25000Z-40G	200	50	10	115	1 Gbps
SDX 26000Z-100G	200	50	10	115	1 Gbps
SDX 26000Z	200	50	10	115	1 Gbps
SDX 26000Z-50S	200	50	10	115	1 Gbps
SDX 8005Z	15	2	1	2	1 Gbps
SDX-24000Z 系列	150	50	10	80	1 Gbps

> 注意
>
> 最低带宽和实例适用于运行以下版本及更高版本的 SDX 实例：11.1 64.x、12.0 63.x 和 12.1 54.x。
>
> 最低购买数量与最低系统要求不同。

表 **2. CPX** 实例支持的池容量

	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
CPX	10	1	1	1	10 Mbps

表 **3.** 虚拟机管理程序和云服务上的 **VPX** 实例支持的池容量

虚拟机管理程序/云服务	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例数	最大实例数	最低带宽单位
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	5 Gbps	10 Mbps	1	1	10 Mbps
Azure	3 Gbps	10 Mbps	1	1	10 Mbps

> 注意：
>
> 最小采购数量不同于最低系统要求。

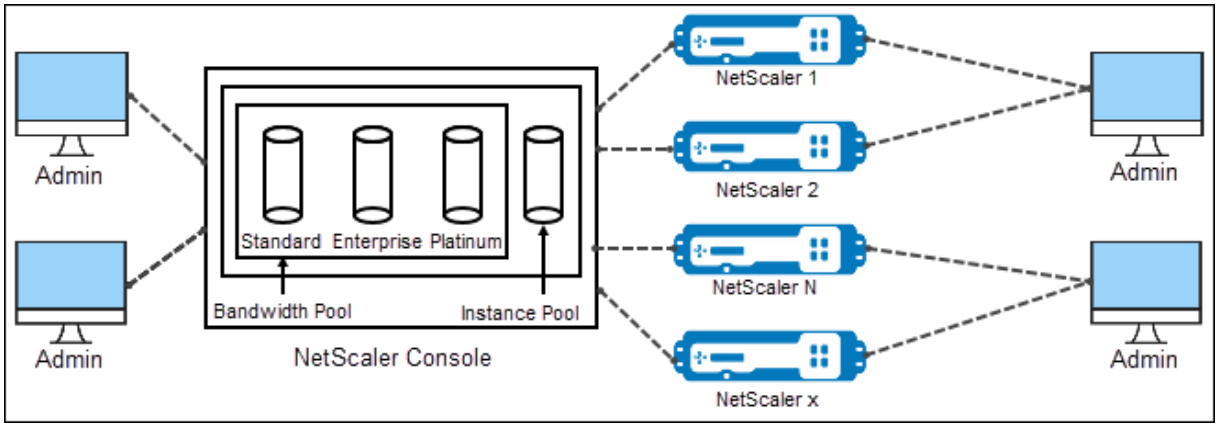
表 **4.** 不同外形规格的许可证要求

产品系列	零容量硬件购买	带宽和版本订阅	实例订阅
MPX	需要许可证	需要许可证	-
SDX	需要许可证	需要许可证	需要许可证
VPX	-	需要许可证	需要许可证
CPX	-	-	需要许可证

配置 **Citrix ADC** 池容量

February 6, 2024

Citrix Application Delivery Management (ADM) 是所有添加到 ADM 的 Citrix ADC 实例的许可服务器。您可以将池容量许可证文件（带宽池或实例池）上载到许可证服务器。您可以根据需要将许可池中的许可分配给 Citrix ADC 实例。您可以从 Citrix ADM 分配许可，也可以根据实例的最小和最大容量从 Citrix ADC 实例（MPX-Z/SDX-Z/VPX/VPX/CPX）签出许可。



支持的硬件和软件版本

Citrix ADC 软件版本	Citrix ADC MPX 零容量硬件	Citrix ADC SDX 零容量硬件	适用于 Citrix ADC VPX 的支持虚拟机管理程序
11.1 版本 54.14 及更高版本 12.0 版本 51.24 及更高版本	MPX-14000Z, MPX-14000Z-40G, MPX-25000Z-40G	SDX-14000Z, SDX-14000Z-40G, SDX-25000Z-40G	VMware ESX 6.0、Citrix Hypervisor、Linux KVM Microsoft Hyper-V、Amazon AWS、Microsoft Azure

将 **Citrix ADM** 配置为许可服务器

您可以将 Citrix ADM 配置为 Citrix ADC 池容量的许可服务器。Citrix ADC 实例可以通过两种方式获得带宽或实例许可，或两者兼而有之：

- Citrix ADC 实例可以向 Citrix ADM 发起签出请求，以获取其带宽和/或实例许可。
- 许可可以通过 Citrix ADM 分配给 Citrix ADC 实例。

> 注意
>
> 只有将池化许可添加到 Citrix ADM 后，才会在 Citrix ADM 上显示池容量。

以下是使用 Citrix ADC 池化容量的 Citrix ADC 实例的运行模式：

- 最佳—实例以适当的许可证容量运行。
- 容量不匹配—实例运行时容量小于用户配置的容量。
- 宽限 - 实例在宽限许可下运行。
- 宽限与不匹配—实例按宽限运行，但容量小于用户配置的容量。

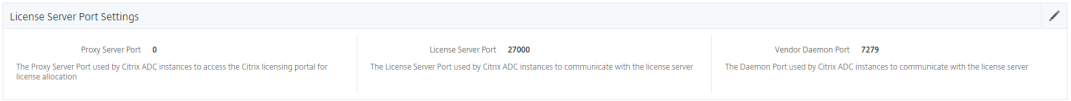
- 不可用—实例未在 Citrix ADM 中注册以进行管理，或者从 Citrix ADM 到实例的 Nitro 通信无法运行。
- 未分配 -实例中未分配许可证。

要在 **Citrix ADM** 上安装许可证文件，请执行以下操作：

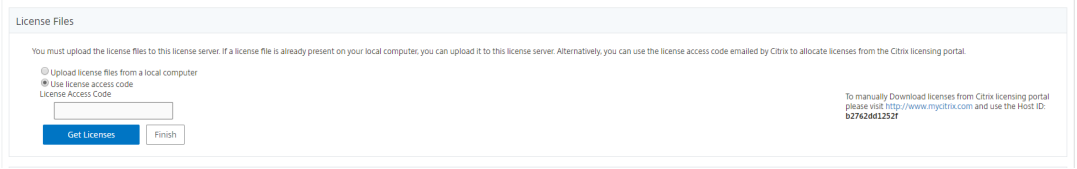
1. 在 Web 浏览器中，键入 **Citrix ADM** 的 IP 地址（例如 http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到“网络 ” **>** “许可证”。
4. 在“许可证文件”部分中，选择以下选项之一：

   - 从本地电脑上载许可文件-如果本地电脑 上已经存在许可文件，则可以将其上载到 Citrix ADM。要添加许可证文件，请单击“浏览”，然后选择要添加的许可证文件 (.lic)。然后单击“完成”。

     > 注意
     >
     > 如果上载的许可文件未在 Citrix ADC 池容量中添加许可，则可以选择许可文件并单击“应用许可”将许可添加到池中。

   - 使用许可证访问代码 -Citrix 通过电子邮件向您购买的许可证访问代码 (LAC) 发送电子邮件。要添加许可证文件，请在文本框中输入 LAC，然后单击“获取许可证”。

     > 注意
     >
     > 您可以随时通过许可设置向 Citrix ADM 添加更多许可。

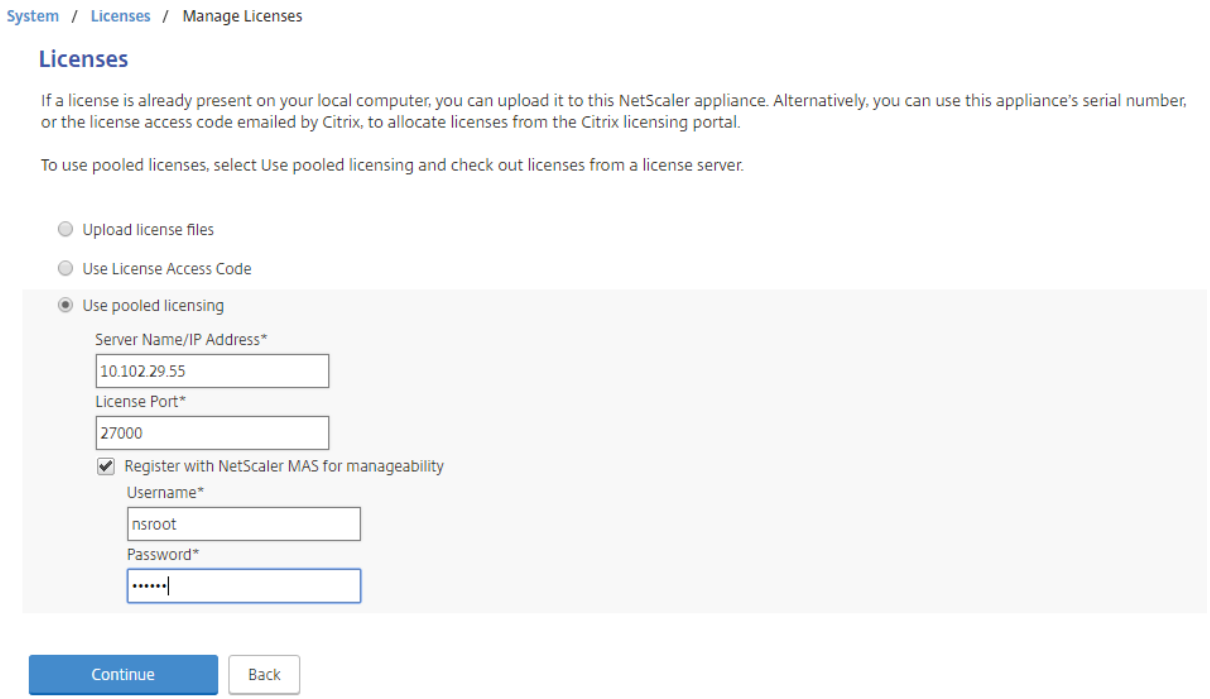
要从 **Citrix ADM** 分配 **Citrix ADC** 池容量许可证，请执行以下操作：

> 注意
>
> 如果您尚未向 Citrix ADM 注册 Citrix ADC 实例，则可以从 Citrix ADM 签出许可证，但无法从 Citrix ADM 向启用 Citrix ADC 池容量的实例分配许可证。

在向 ADC 实例分配池容量许可证之前，请确保满足以下先决条件。

> 先决条件在通过 Citrix ADM 管理实例的池许可证之前，必须先向 Citrix ADM 注册 Citrix ADC 实例。在 Citrix

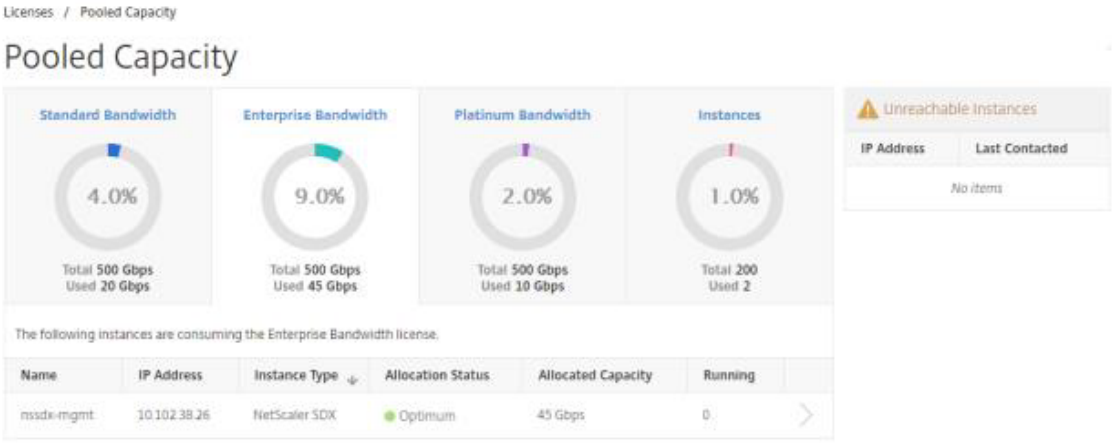
> ADC GUI 中，导航到“系统”>“许可证”>“管理许可”，然后在添加 **Citrix ADM IP** 时选中“向 **Citrix ADM** 注册以实现可管理性”复选框。



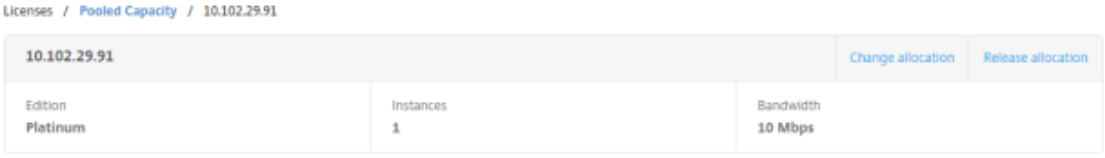
> 注意
>
> 在上面屏幕的 用户名 和 密码 字段中，输入 Citrix ADM 凭据。

向许可证服务器注册实例后，按如下所示分配许可证：

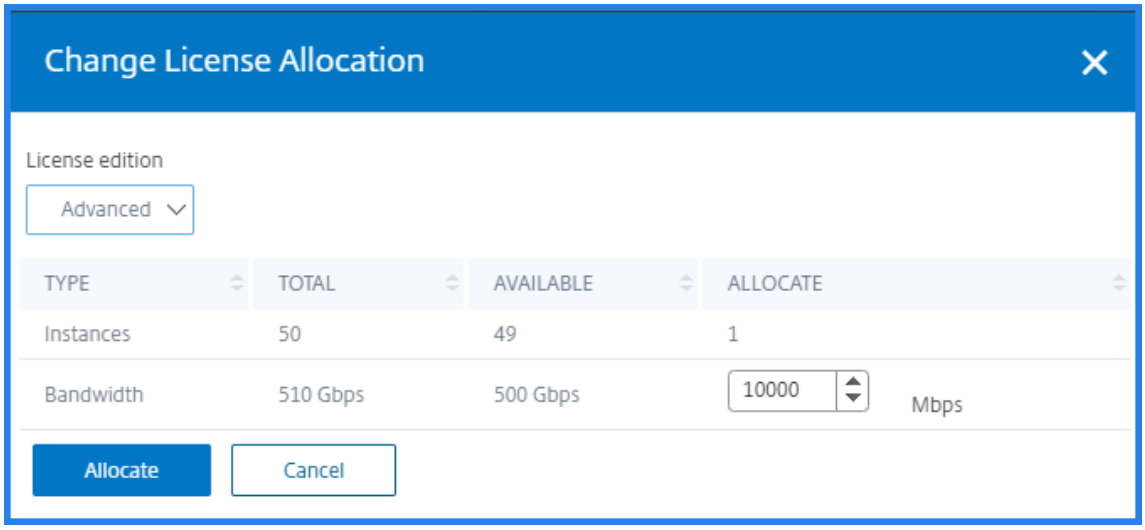
1. 在 Web 浏览器中，键入 **Citrix ADM** 的 IP 地址（例如 http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 在配置选项卡上，导航到 网络 **>** 许可证 **>** 池化容量。
4. 单击要管理的许可证池。
5. 单击 **>** 按钮，从可用实例列表中选择 Citrix ADC 实例。



6. 如果要更改或发放许可证分配，请单击“更改 分配”或“发布分配”。



7. 如果单击“更改分配”，则会出现一个弹出窗口，其中包含许可证服务器中的可用许可证。



8. 您可以通过设置分配下拉选项来选择分配给 Citrix ADC 实例的带宽或实例。做出选择后，单击“分配”。
9. 您也可以从“更改许可证分配”窗口的下拉选项中更改分配的许可证版本。

在 **MPX-Z** 上配置 **Citrix ADC** 池容量

MPX-Z 是支持 Citrix ADC 池容量的 Citrix ADC MPX 设备。MPX-Z 支持铂金版、企业版或标准版许可证的带宽池。

MPX-Z 需要其平台许可证，才能连接到许可证服务器。您可以通过从本地计算机上载许可文件或使用实例的硬件序列号或 Citrix ADC 实例 GUI 的“系统”>“** 许可”部分的 许可 访问代码来安装 MPX-Z 平台许可。如果删除 MPX-Z 平

台许可证，则会禁用池容量功能，且所有签出的许可证都签入许可证服务器中。

您可以动态修改 MPX-Z 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

> 注意
>
> 重新启动实例时，它将自动签出其配置的容量所需的池许可证。

在 **Citrix ADC VPX** 实例上配置 **Citrix ADC** 池容量

启用池容量的 Citrix ADC VPX 实例可以从带宽池（白金版/企业版/标准版）中签出许可。您可以使用 Citrix ADC GUI 从许可服务器签出许可。

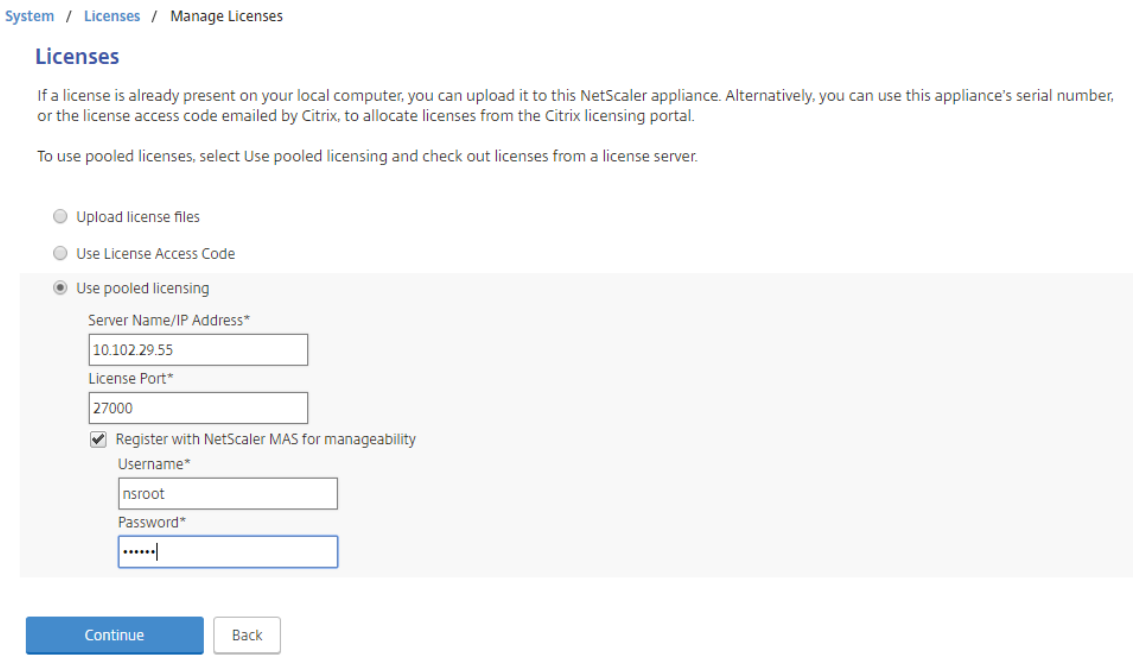
您可以动态修改 VPX 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

> 注意
>
> 重新启动实例时，它将自动签出其配置的容量所需的池许可证。

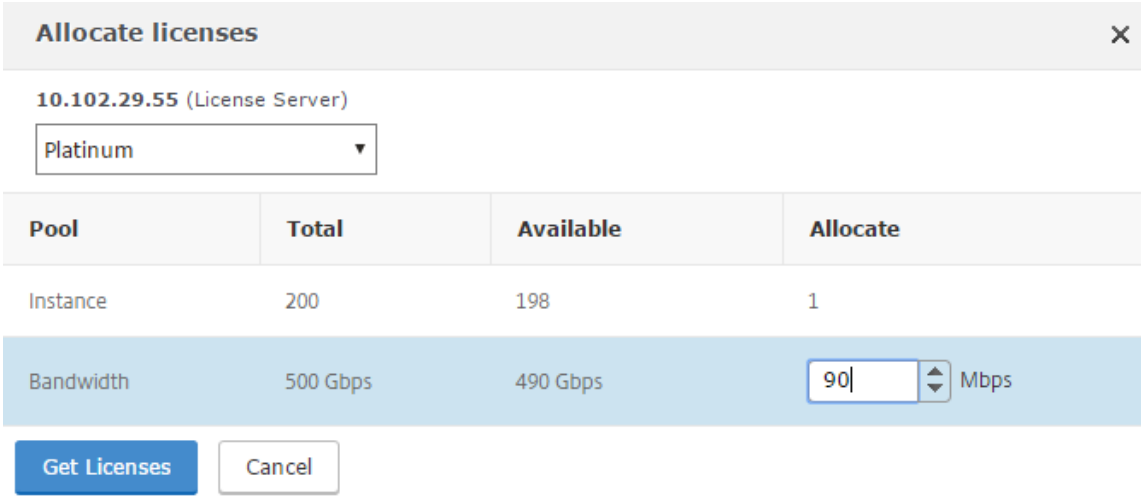
向 **Citrix ADC MPX-Z** 或 **Citrix ADC VPX** 实例分配池许可证

要分配许可证，请执行以下操作：

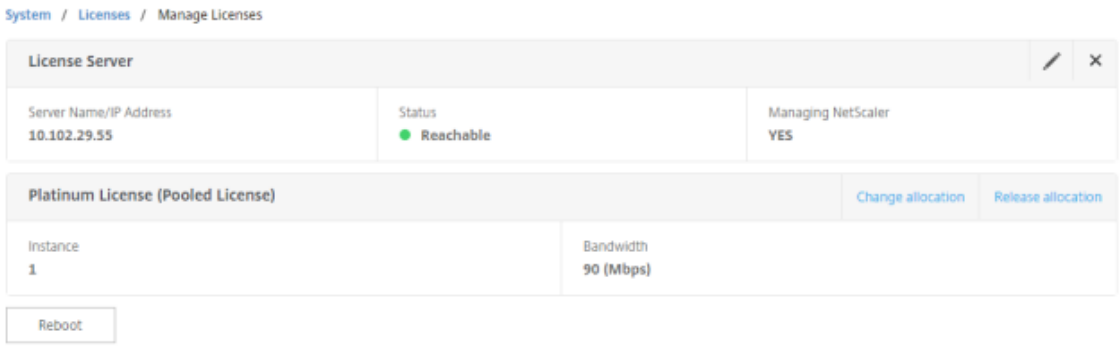
1. 在 Web 浏览器中，键入 Citrix ADC 实例的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“系统”**>**“许可证”**>**“管理许可证”，单击“添加新许可证”，然后选择“使用共享许可”。



4. 在“服务器名称/**IP** 地址”字段中输入许可证服务器 的详细信息。
5. 如果您想通过 Citrix ADM 管理实例的池许可，请选中“向 **Citrix ADM** 注册以实现可管理性”复选框并输入 ADM 凭 据。
6. 选择许可证版本和所需的带宽，单击“获取许可证”。

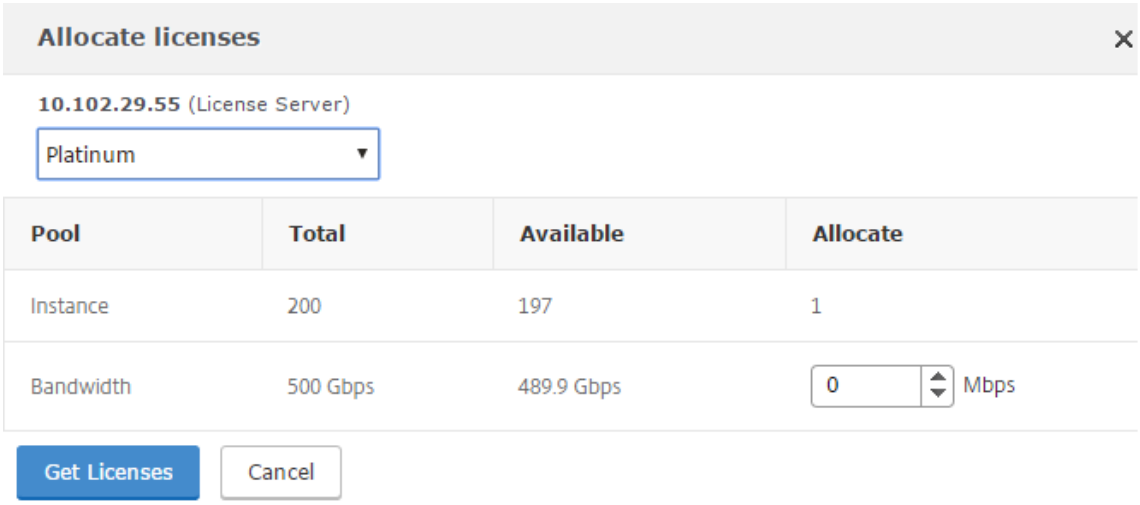


7. 您可以通过选择“更改分配”或“发布分配”来 更改 或 释放许可证分配。



8. 如果单击更改分配，弹出窗口将显示许可证服务器上可用的许可证。

> 注意
>
> 如果更改带宽分配，则不需要重新启动，但如果更改许可证版本，则需要热重新启动。



9. 您可以从“分配”下拉列表中为 Citrix ADC 实例分 配 带宽或实例。然后单击“获取许可证”。
10. 您可以从弹出窗口中的下拉列表中选择许可证版本和所需的带宽。

> 注意
>
> 带宽分配应该是最低带宽单位的倍数。

在 **SDX-Z** 上配置 **Citrix ADC** 池容量

SDX-Z 实例是启用池容量的 Citrix ADC SDX 实例。SDX-Z 支持实例池以及用于铂金版、企业版和标准版的带宽池。申请 SDX-Z 平台许可后，管理服务提供选项，
用于将许可签出和签回许可服务器，以及为在 SDX-Z 平台上运行的 Citrix ADC 实例分配带宽容量。

> 注意
>
> 在 SDX-Z 上运行的 Citrix ADC VPX 实例无法直接将许可证从许可证服务器签出或签入许可证服务器。这可以由 SDX 中的管理服务完成。

您可以安装 SDX-Z 平台许可证，方法是从本地计算机上载许可证文件，或使用实例的硬件序列号或许可证访问代码。

如果删除 SDX-Z 平台许可证，则会禁用池容量功能，且所有许可证都重新签入许可服务器中。

> 注意
>
> 如果重新启动实例，它将签出其配置的容量所需的池许可证。

Citrix ADC SDX 上的池容量

实例池：

SDX 设备可以置备 SDX 设备的实例池中可用的相同数量的实例。

带宽池：

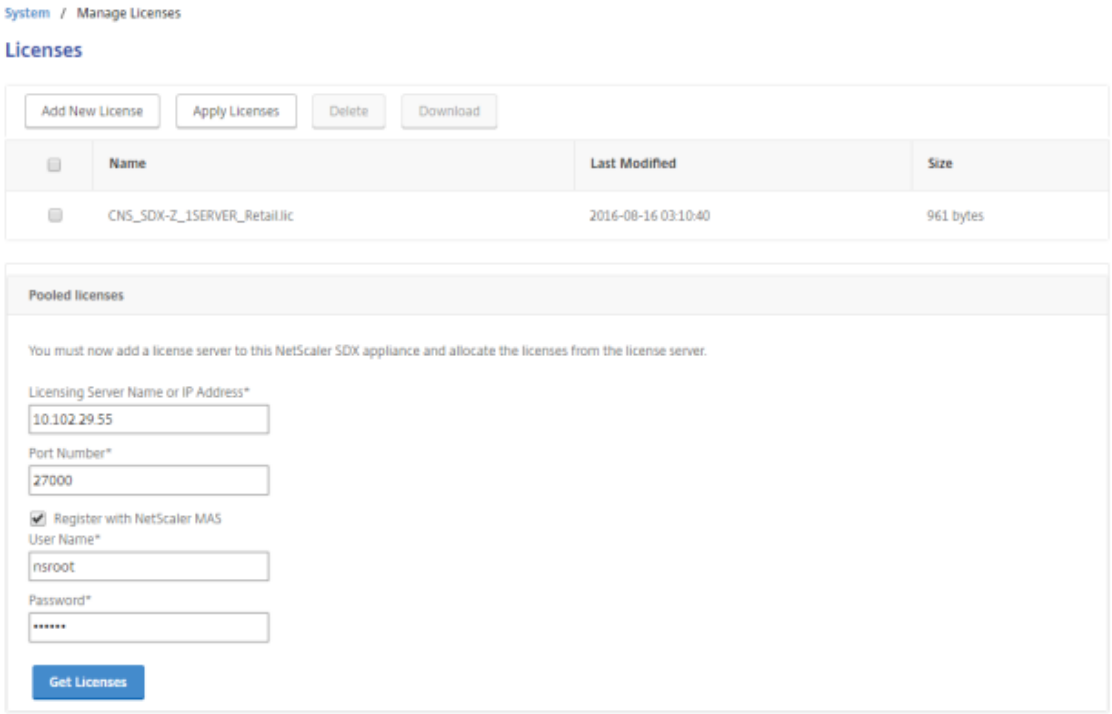
在 Citrix ADC 实例配置期间，将为该实例分配带宽。您可以选择版本和所需的带宽来配置虚拟 Citrix ADC 实例。仅当实例具有适用于所请求版本的足够带宽时，管理服务才允许继续进行置备。如果带宽不足，您会收到通知。

> 注意
>
> 修改带宽不需要重新启动实例。

向 **Citrix ADC SDX-Z** 实例分配池许可证

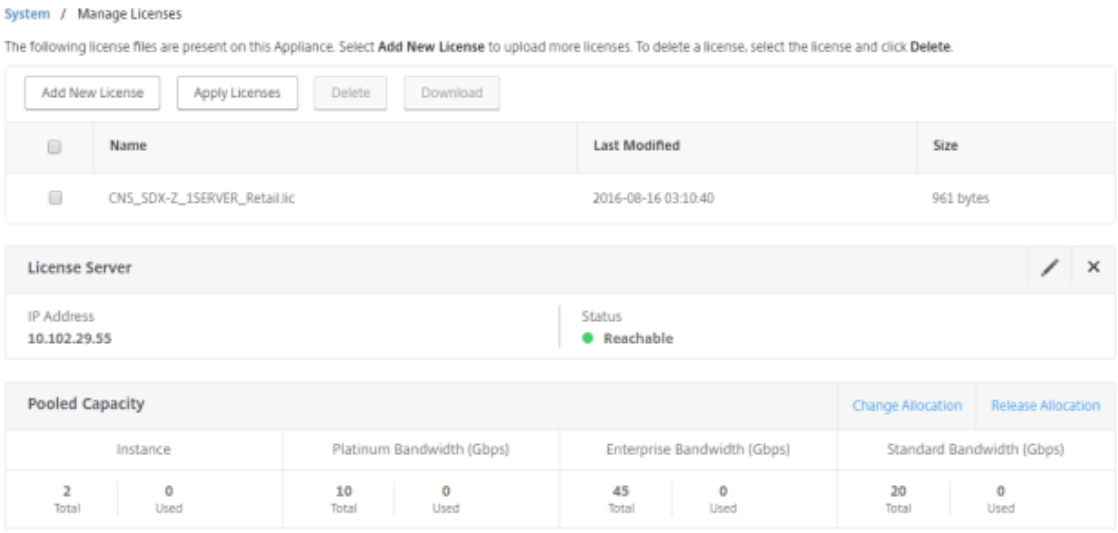
要分配许可证，请执行以下操作：

1. 在网络浏览器中，键入您的 Citrix ADC SDX-Z 实例的 IP 地址（例如 http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在配置选项卡上，导航到 系统 **>** 许可证，然后转到 池化容量。

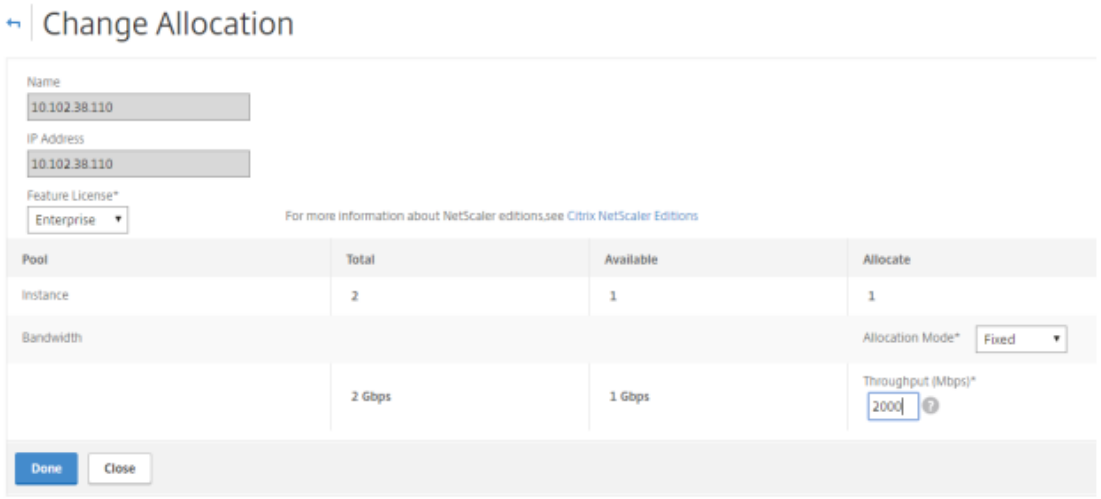


4. 在“服务器名称/**IP** 地址”字段中输入许可证服务器 的详细信息。
5. 如果要通过 Citrix ADM 管理实例的池许可证，请选中“向 **Citrix ADM** 注册”复选框，然后输入 ADM 凭据。
6. 您可以通过选择“更改分配”或“发布分配”来 更改 或 释放许可证分配。

> 注意
>
> 签出的许可证由 ADM 存储在单独的池中。



7. 要更改 SDX-Z 实例中特定 VPX 实例的许可证分配，请从“实例”部分选择该实 例，然后单击“更改分配”。将出现一个新窗口，显示可用的许可证。



8. 您可以从 功能许可证 下拉列表中更改实例的带宽版本，并在 吞吐量 **(mbps)** 字段中更改所需的带宽。然后单击 **Done**（完成）。

> 注意
>
> 带宽分配应该是对应尺寸规格的最低带宽单位的整数倍数。

在 **Citrix ADC CPX** 实例上配置 **Citrix ADC** 池容量

在配置 Citrix ADC CPX 实例时，您可以将 Citrix ADC CPX 实例配置为使用 Citrix ADC 池容量。在 ***docker run*** 命令中，您需要提供 Citrix ADC 许可服务器的详细信息。Citrix ADC CPX 实例从实例池中签出许可。

> 注意
>
> 默认情况下，Citrix ADC CPX 实例会从实例池中签出实例许可，吞吐量自动设置为 1000 Mbps。您不能修改分配给实例的 1000 Mbps 带宽。

您可以从 Docker 应用商店下载 Citrix ADC CPX。在 Docker 主机上，要下载 Citrix ADC CPX，请运行以下命令：

```
docker pull store/citrix/netscalercpx: <version>

<!--NeedCopy-->
```

要在配置 **Citrix ADC CPX** 实例时配置 **Citrix ADC** 池容量，请执行以下操作：

在配置 Citrix ADC CPX 实例时，在 ***docker run*** 命令中将 Citrix Licensing Server 定义为环境变量，如下所示：

```
docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name
    <container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --
    cap-add=NET_ADMIN <REPOSITORY>:<TAG>

<!--NeedCopy-->
```

其中：

- <LS_IPADDRESS> 是 Citrix 许可服务器的 IP 地址。
- <LS_PORT> 是 Citrix 许可服务器的端口。默认情况下，端口为 27000。

将 **Citrix ADC MPX** 中的永久许可升级到 **Citrix ADC** 池容量

February 6, 2024

具有永久许可证的 Citrix ADC MPX 装置可升级到 Citrix ADC 池容量许可证。升级到 Citrix ADC 池容量许可证允许您按需将许可证池中的许可证分配给 Citrix ADC 设备。您还可以为在高可用性模式下配置的 Citrix ADC 实例配置 Citrix ADC 池容量许可证。要在高可用模式下为 Citrix ADC MPX 实例配置 Citrix ADC 池容量许可，请参阅 将 Citrix ADC MPX 高可用性对中的永久许可升级为 Citrix ADC 池容量。

> 重要
>
> 要将 Citrix ADC MPX 装置升级到 Citrix ADC 池容量许可证，您需要将 MPX-Z 许可证上载到该装置。

要升级到 **Citrix ADC** 池容量，请执行以下操作：

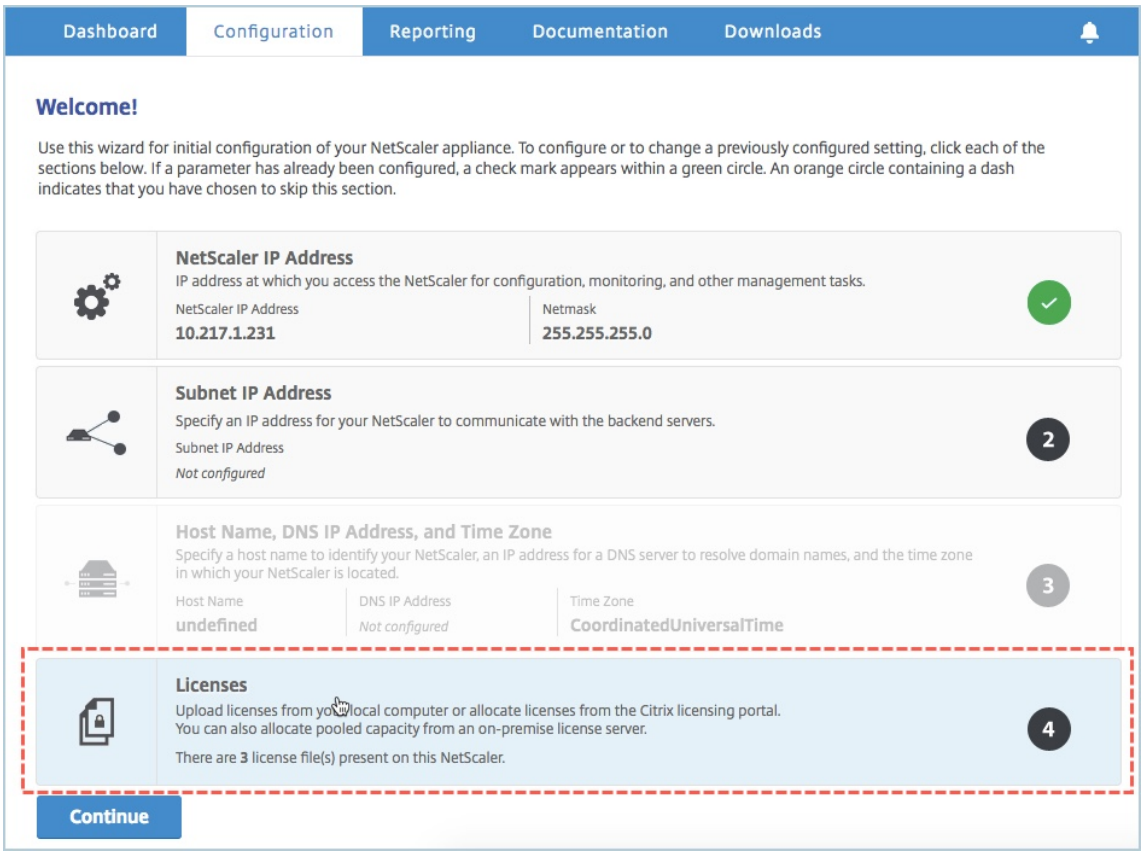
1. 在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。

4. 上载零容量许可证（MPX-Z 许可证）。在配置选项卡上，导航到 系统 > 许可证。
5. 在详细信息窗格中，单击“管理许可证”，单击“添加 新许可证”。
6. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”以从本地计算机中选择零容量许可证。
7. 上载许可证后，单击 重新启动 以重新启动设备。

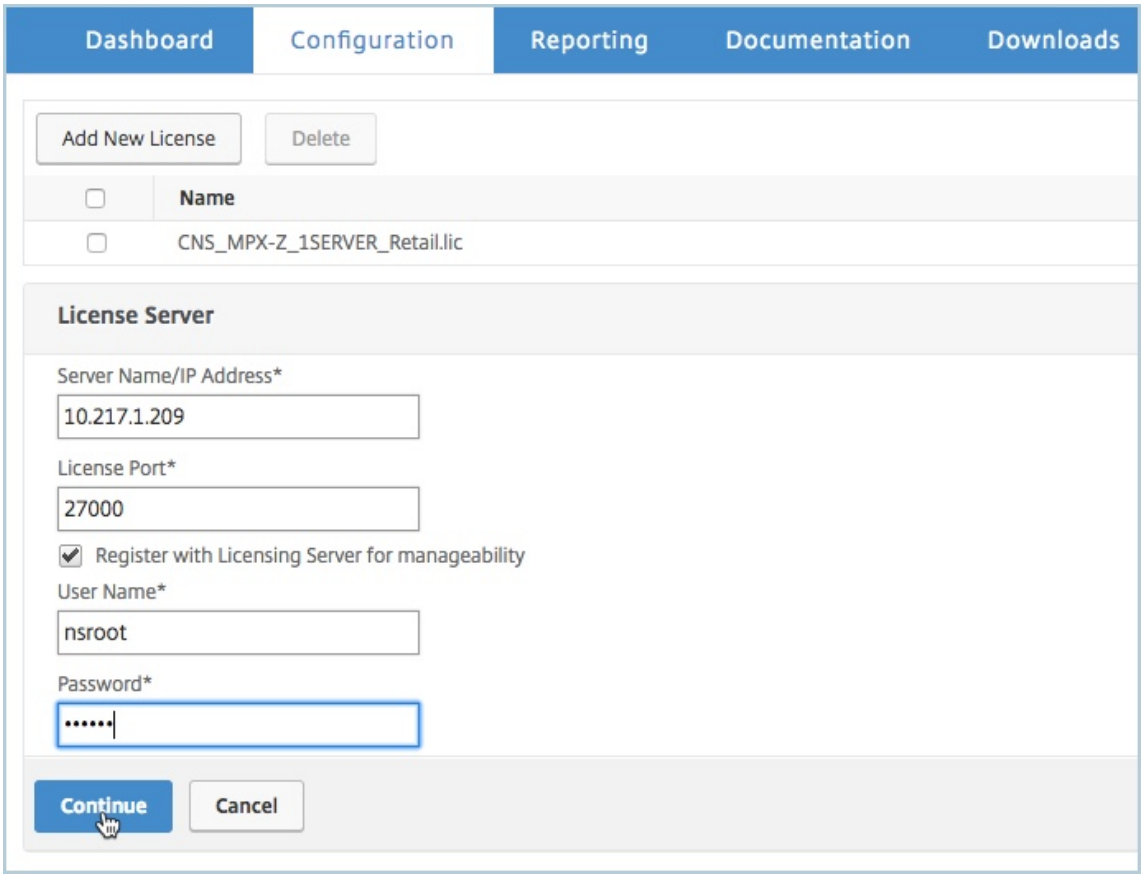
   在重新启动设备之前，请确保未保存任何配置。

   > 警告应用 MPX-Z 许可证
   >
   > 后，装置上包括 SSL 卸载在内的功能将变为未授权。设备停止处理 HTTPS 请求。
   >
   > 如果在升级之前在装置上启用了“仅安全访问”选项，则无法使用 HTTPS 通过 Citrix ADM GUI 连接到装置。

8. 在“确 认”页面上，单击“是”。
9. 装置重新启动后，登录到装置。
10. 在“欢迎”页面上，单击“许可证”部分。



11. 在“许可证服务器”部分中，执行以下操作：



a) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器详细信息。

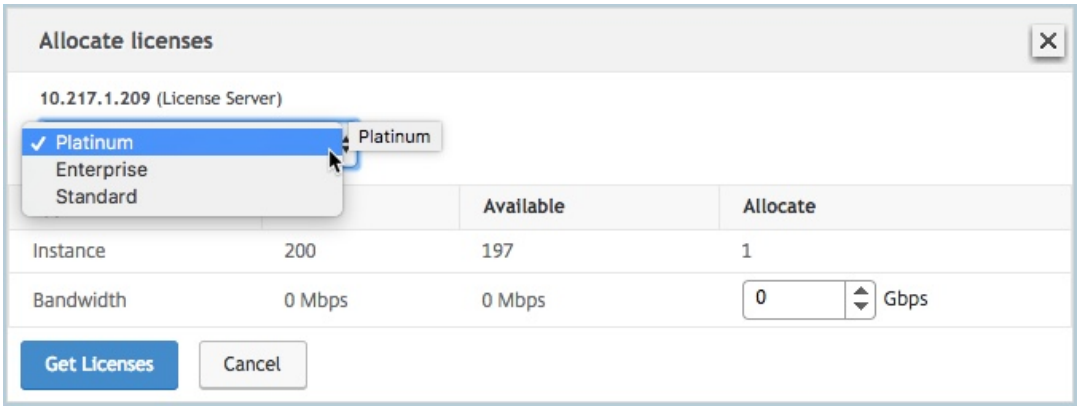
b) 在“许可证端口”字段中，输入许可证服务器端口。默认值：27000。

c) 如果您想通过 Citrix ADM 管理实例的池许可，请选中“向 许可服务器注册以实现可管理性”复选框并输入 ADM 凭 据。

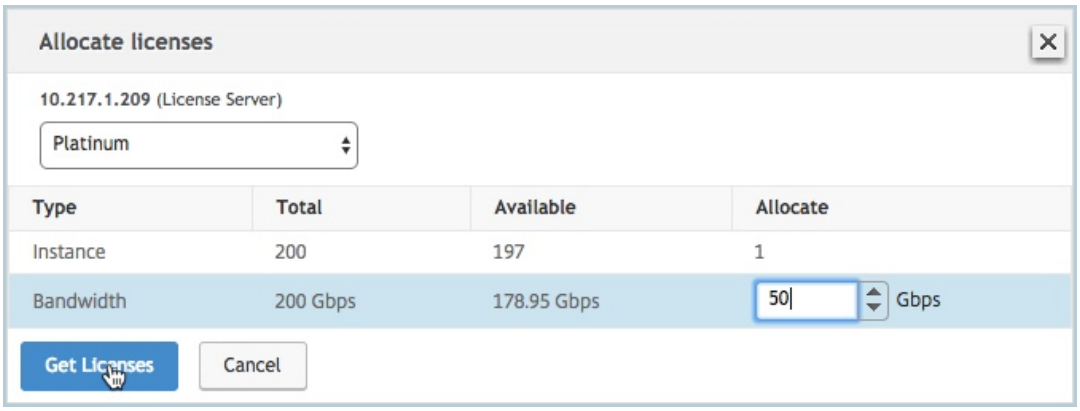
d) 单击继续。

12. 在“分配许可证”窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。



b) 从“分配”菜单将带宽分配 给 Citrix ADC 装置，然后单击“获取许可证”。



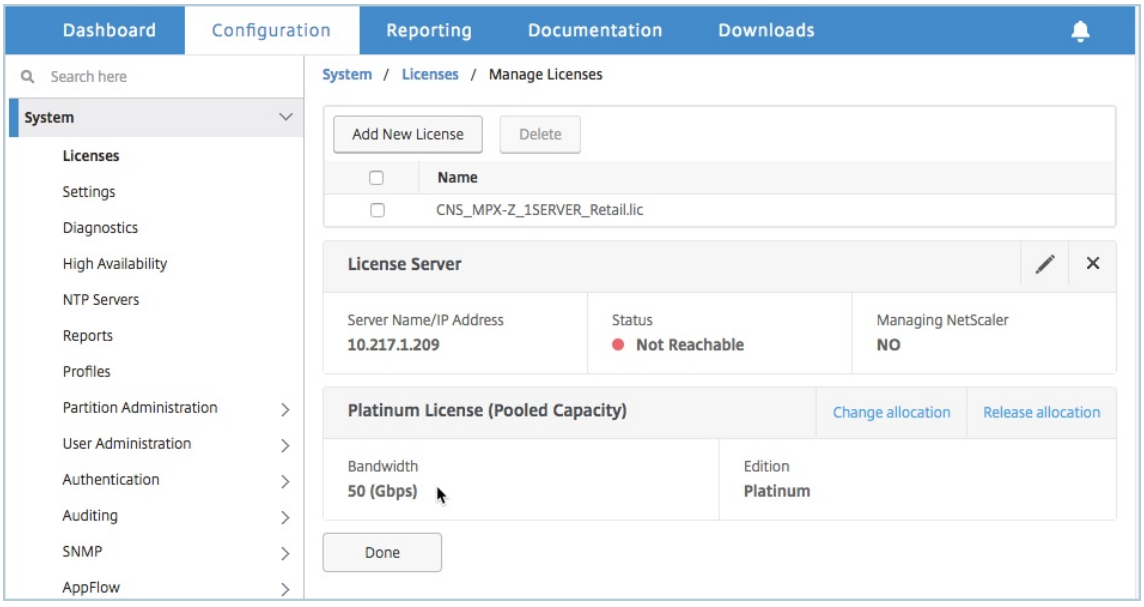
c) 出现提示时，单击 重新启动 以重新启动装置。

13. Citrix ADC MPX 设备重新启动后，登录 Citrix ADC MPX 设备。在“欢迎 使用”页面上，单击“继续”。

“许可证”页面列出了所有已许可的功能。

14. 导航到“系统”**>**“许可证”，然后单击“管理许可证”。

在“管理许可证”页面上，可以查看许可证服务器、许可证版本和分配带宽的详细信息。



将 **Citrix ADC MPX** 高可用性对中的永久许可升级到 **Citrix ADC** 池容量

对于在高可用性模式下配置的 Citrix ADC MPX 装置，您必须在 HA 对中的主要和辅助 Citrix ADC 实例上配置 Citrix ADC 池容量。您需要将相同容量的许可证分配给 HA 对中的主 Citrix ADC 实例和辅助实例。例如，如果您想让 HA 对中的每个实例获得 1 Gbps 的容量，则需要从公用池中分配 2 Gbps 的容量，这样您就可以为 HA 对中的主和辅助 Citrix ADC 实例各分配 1 Gbps 的容量。

> 重要
>
> 要升级 Citrix ADC MPX 设备以使用 Citrix ADC 池容量许可证，您需要将 MPX-Z 上载到该设备。

必备条件

确保将 MPX-Z 许可证上载到 HA 对中的主实例和辅助实例。

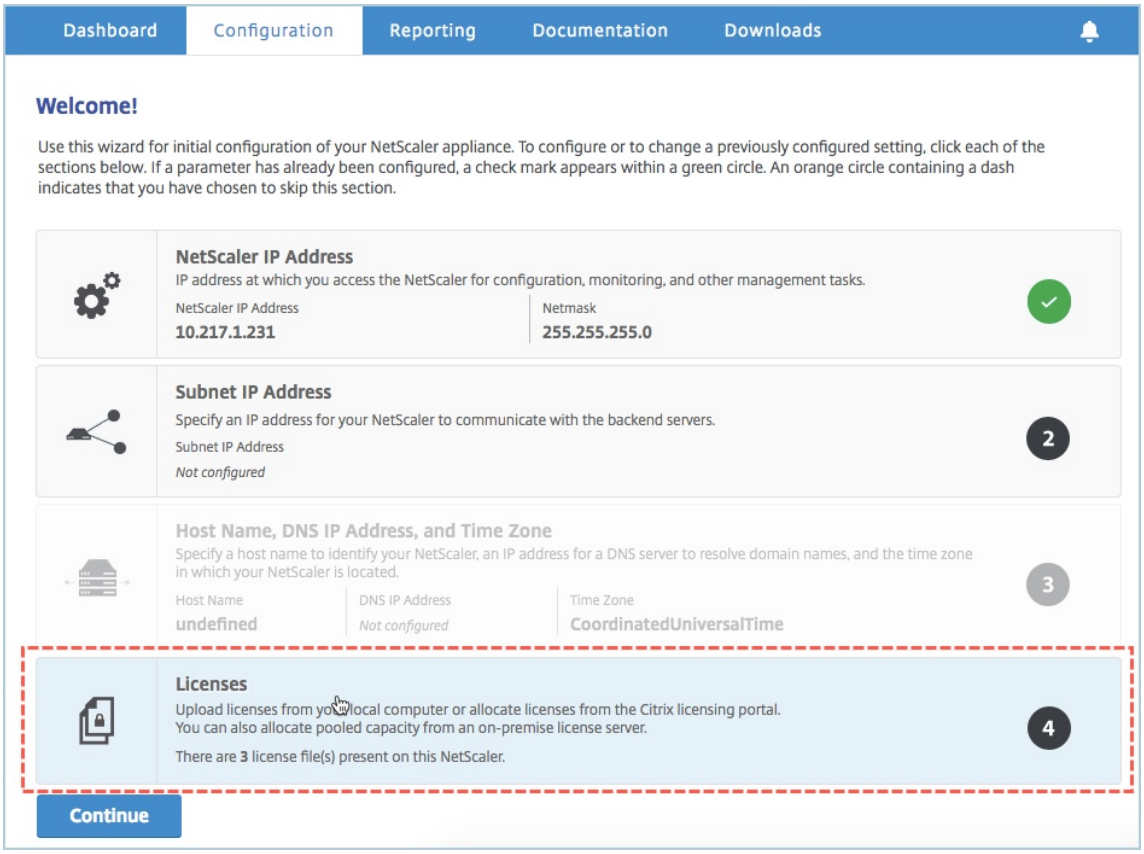
要将 **MPX-Z** 许可证上载到 **HA** 对中的 **Citrix ADC MPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证（MPX-Z 许可证）。在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Licenses**（许可证）。
5. 在详细信息窗格中，单击 管理许可证，单击 添加新许可证。
6. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”以从本地计算机中选择零容量许可证。

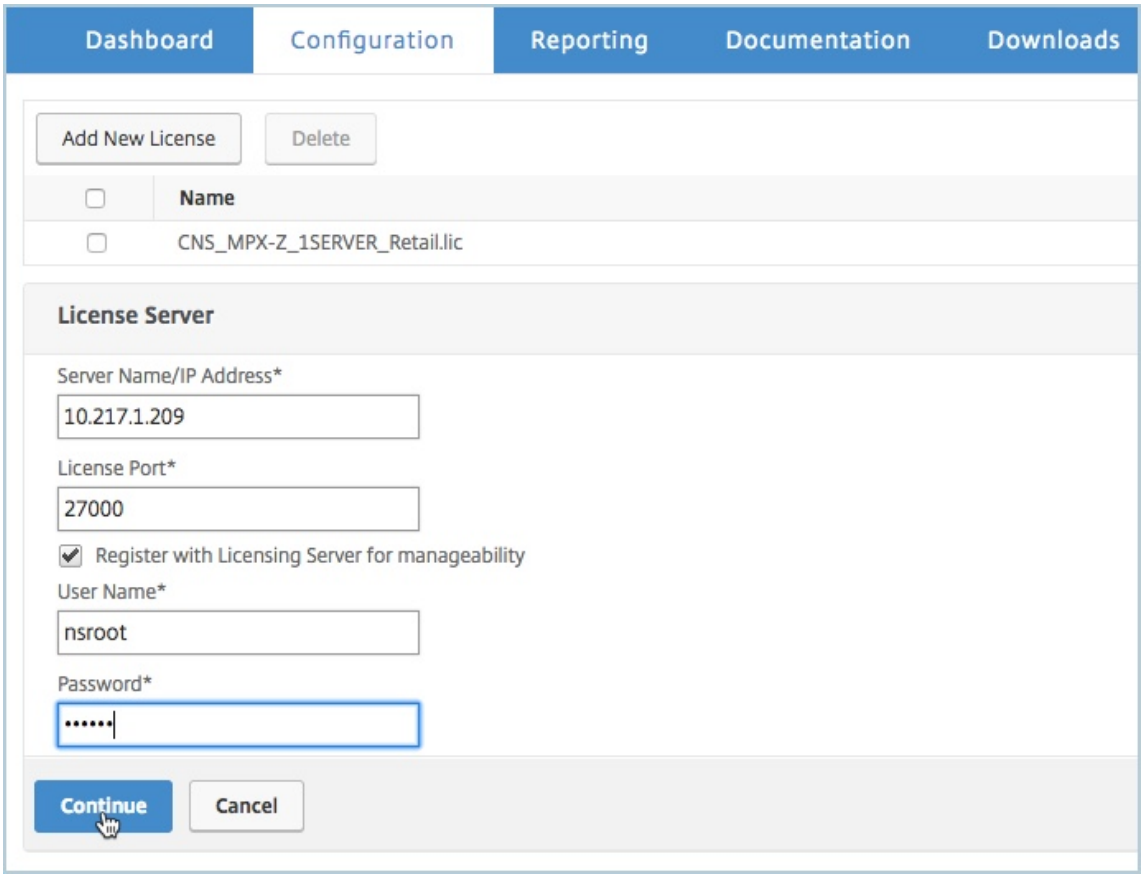
   上载许可证后，系统会提示您重新启动设备。
7. 单击“重新启 动”以重新启动装置。
8. 在“确 认”页面上，单击“是”。

要将现有的 **HA** 设置升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 登录到辅助 Citrix ADC MPX 实例。在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎”页面上，单击“许可证”部分。



4. 在“许可证服务器”部分中，执行以下操作：



a) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器详细信息。

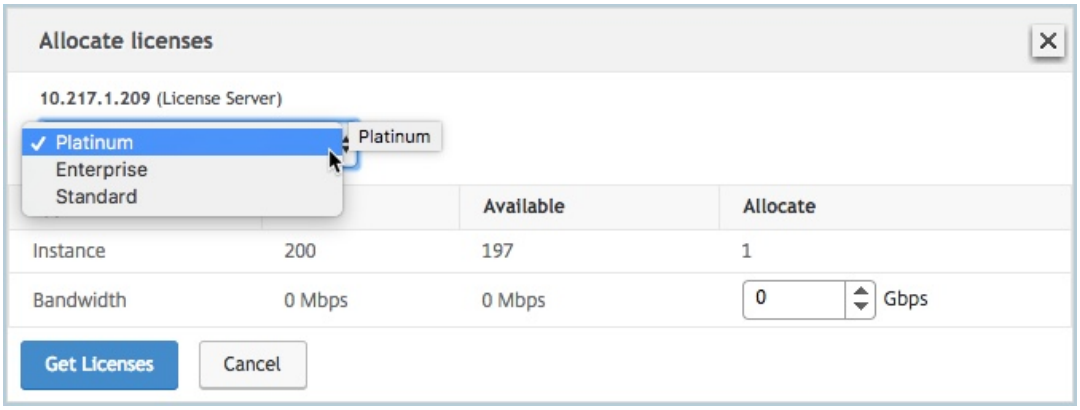
b) 在“许可证端口”字段中，输入许可证服务器端口。默认值：27000。

c) 如果您想通过 Citrix ADM 管理实例的池许可，请选中“向 许可服务器注册以实现可管理性”复选框并输入 ADM 凭 据。

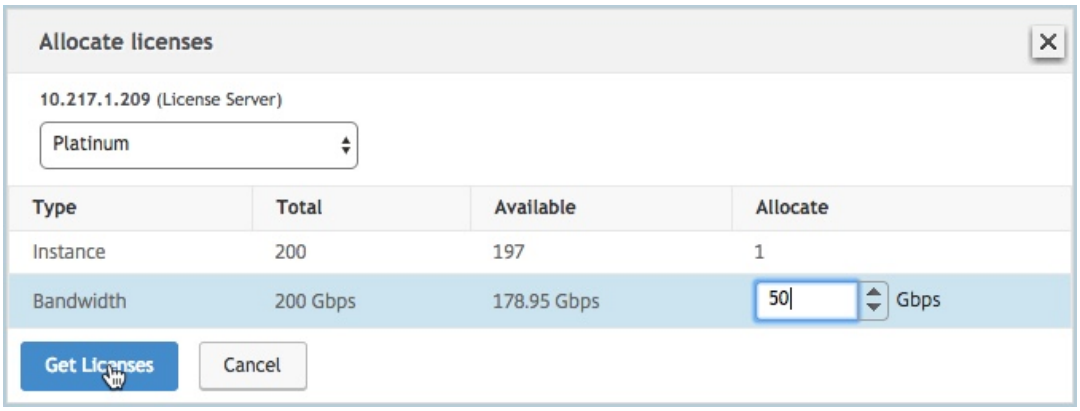
d) 单击继续。

5. 在“分配许可证”窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。



b) 从“分配”菜单将带宽分配 给 Citrix ADC 装置，然后单击“获取许可证”。



c) 出现提示时，单击 重新启动 以重新启动装置。

辅助 Citrix ADC MPX 装置重新启动后，它将成为 HA 对中的主 Citrix ADC MPX 装置。

6. 登录到现有的主 Citrix ADC MPX 装置，然后重新启动装置。执行以下操作：

a) 在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，例如 http://192.168.100.1。

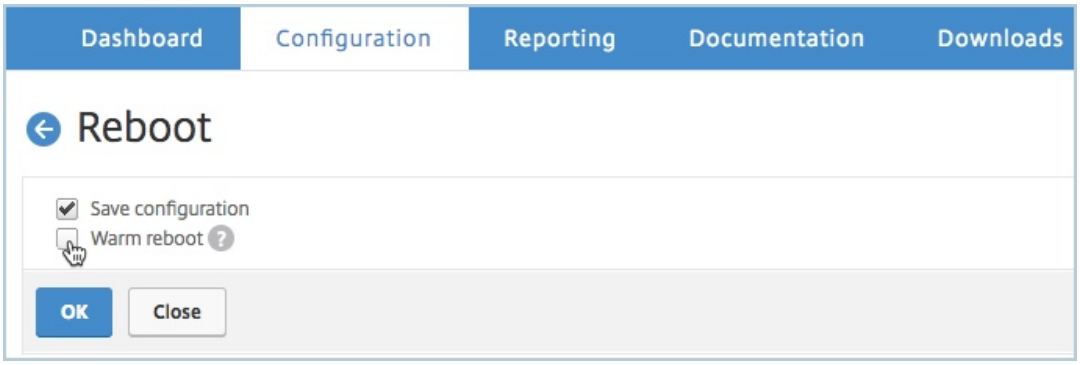
b) 在“用户名”和“密码”字段中，键入管理员凭据。

c) 在“欢迎 使用”页面上，单击“继续”。

d) 在“配置”选项卡上，单击“系统”。

e) 在“系统”页面上，单击“重新启动”。

f) 在“重新启动”页面上，选择“热重新启动”，然后单击“确定”。



主 Citrix ADC MPX 装置重新启动后，它将成为 HA 对中的辅助 Citrix ADC MPX 装置。如果需要，您可以在 HA 对中的任何实例上使用以下命令，将 HA 对中的主实例和辅助实例更改为原始 HA 对配置：

```
1 > force ha failover
2 <!--NeedCopy-->
```


将 **Citrix ADC SDX** 中的永久许可证升级到 **Citrix ADC** 池容量

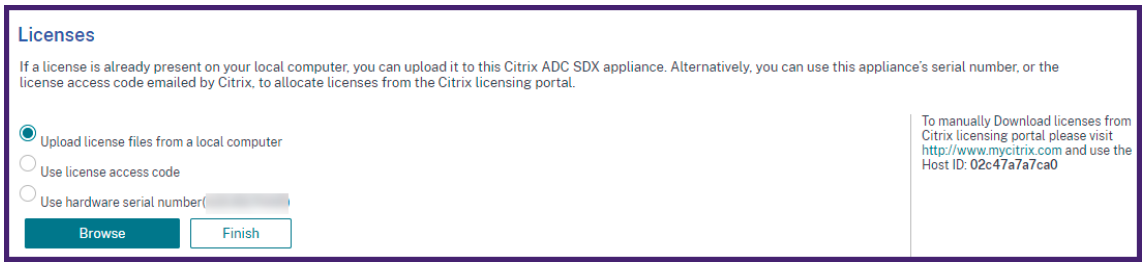
February 6, 2024

具有永久许可证的 Citrix ADC SDX 设备可以升级到 Citrix ADC 池容量许可证。升级到 Citrix ADC 池容量许可后，您可以根据需要将许可池中的许可分配给 Citrix ADC 设备。您还可以为在高可用性模式下配置的 Citrix ADC 实例配置 Citrix ADC 池容量许可证。

> 重要
>
> 要将 SDX 设备升级到 Citrix ADC 池容量许可，需要将 SDX-Z 许可上载到该设备。

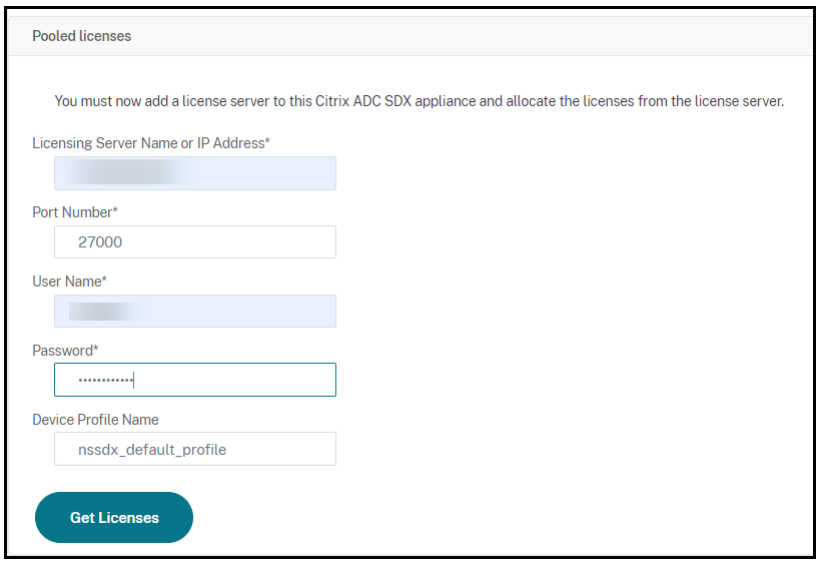
要升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 SDX ADC 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证。在配置选项卡上，导航到 系统 > 许可证。
5. 导航到 系统 > 许可证。
6. 在“许可证”页面中，单击“管理许可证”，然后单击“添加新许可证”。
7. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”以从本地计算机中选择零容量许可证。然后，单击“完成”。



成功应用零容量许可 证后，“许可证”页面上将显示“池许可证”部分。

8. 在 池许可证部 分中，执行以下操作：



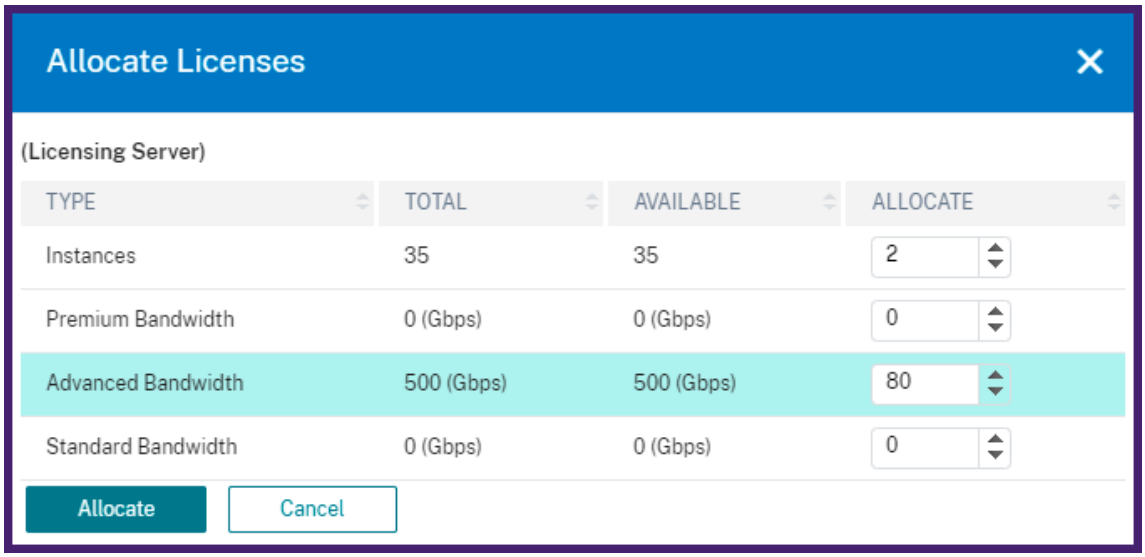
a) 在 授权服务器名称或 **IP** 地址 字段中，输入许可证服务器详细信息。

b) 在 端口号 字段中，输入许可证服务器端口。默认值：27000。

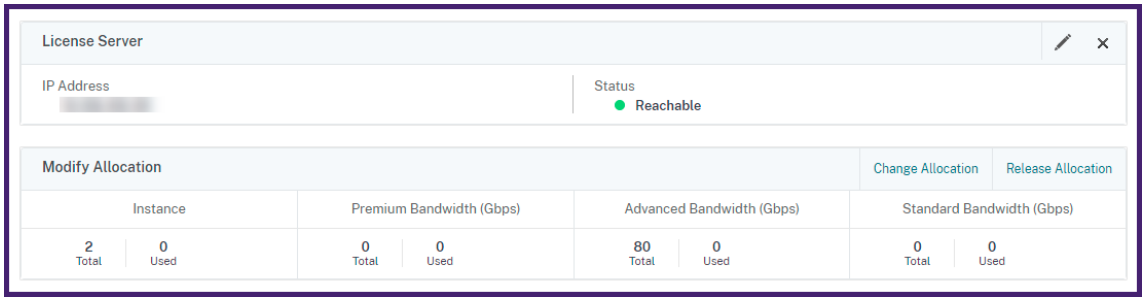
c) 如果要通过 Citrix ADM 管理实例的池许可证，请选中“向 **Citrix ADM** 注册”复选框，然后输入 ADM 凭据。

d) 单击 **Get Licenses**（获取许可证）。

9. 在“分配许可证”窗口中，指定所需的实例和带宽，然后单击“分配”。



在“管理许可证”页面上，可以查看许可证服务器、许可证版本以及池中分配的实例和带宽的详细信息。



Citrix ADC 群集模式下的 Citrix ADC 池容量

February 6, 2024

您可以在配置为群集的 Citrix ADC 实例上配置 Citrix ADC 池容量。以下是在群集模式下在 Citrix ADC 实例上配置池容量的先决条件：

- 实例应单独以池容量许可证模式运行以组成群集。
- 所有实例运行时应使用相同的带宽。
- 所有实例都应从同一 Citrix Application Delivery Management (ADM) 中检出池容量。
- 除非新实例的容量和 Citrix ADM 配置与群集中现有实例的容量和 Citrix ADM 配置相同，否则无法将新实例添加到现有 Citrix ADC 群集中。

从 Citrix ADC 群集签出的任何容量都将为所有群集节点分配相同的容量，签出带宽 = 提供的带宽 * 节点数量。

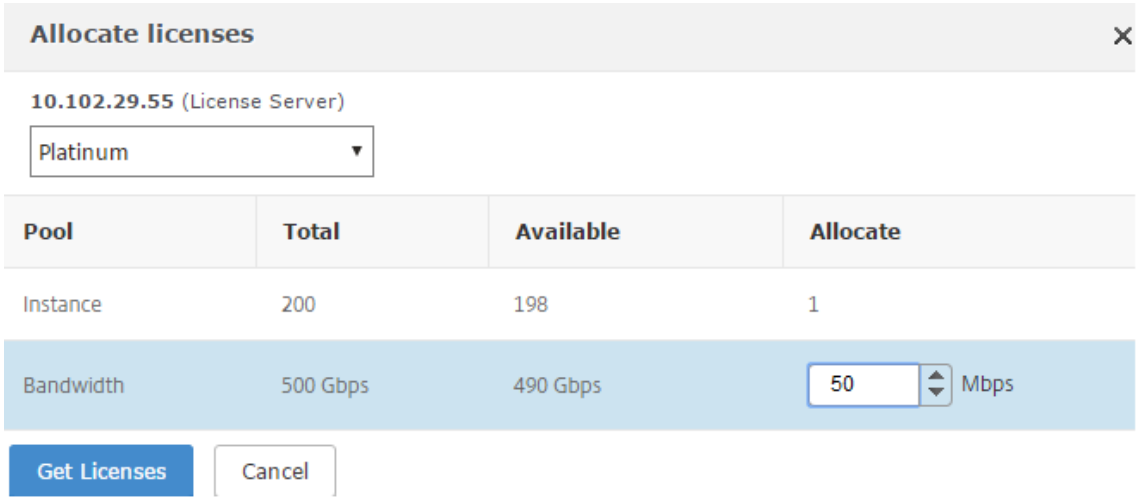
例如，如果您从 Citrix ADC 群集中签出 50 Mbps 的带宽，并且该群集包含 12 个实例，则每个实例将自动接收 50 Mbps；并且 600 mbps 将从池中签出。

> 注意
>
> 如果群集中的一个或多个实例无响应，则群集继续使用其余实例的容量。

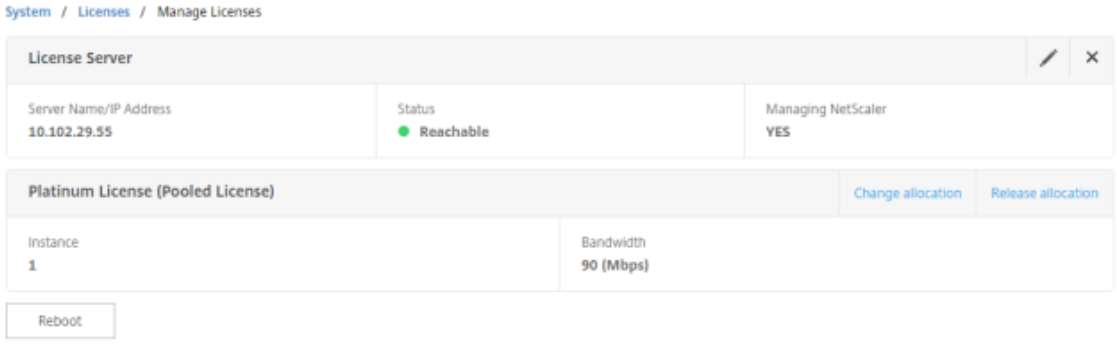
要在群集模式下在 **Citrix ADC** 实例上分配 **Citrix ADC** 池化容量，请执行以下操作：

1. 在 Web 浏览器中，键入 群集 IP (CLIP) 地址的 **IP** 地址（例如，http://192.168.100.1)。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“系统”**>**“许可证”**>**“管理许可证”，单击“添加新许可证”，然后选择“使用池化许可”。
4. 在“服务器名称 **/IP** 地址”字段中输入许可证服务器的名称或地址。
5. 如果您想通过 Citrix ADM 管理实例的池许可，请选中“向 **Citrix ADM** 注册以实现可管理性”复选框并输入 ADM 凭 据。

6. 选择许可证版本和所需的带宽，然后单击 获取许可证。

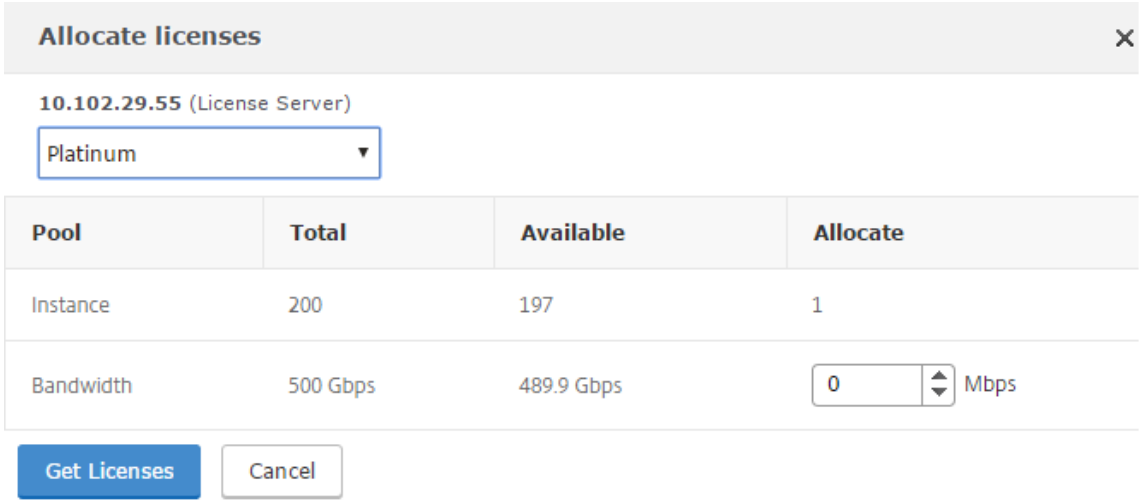


7. 您可以通过选择“更改分配”或“发布分配”来 更改 或 释放许可证分配。



8. 如果单击更改分配，弹出窗口将显示许可证服务器上可用的许可证。

> 注意
>
> 带宽分配必须是对应尺寸规格的最低带宽单位的整数倍数。



9. 您可以从“分配”下拉列表中为 Citrix ADC 实例分 配 带宽或实例。然后单击“获取许可证”。
10. 您可以从弹出窗口中的下拉列表中选择许可证版本和所需的带宽。

> 注意
>
> 如果更改带宽分配，则不需要重新启动，但如果更改许可证版本，则需要热重新启动。

运行状况监视

February 6, 2024

许可服务器持续监视启用 Citrix ADC 池容量的实例的运行状况。实例定期向许可证服务器发送消息。如果连续几次未收到消息，则许可证服务器报告失去了连接。

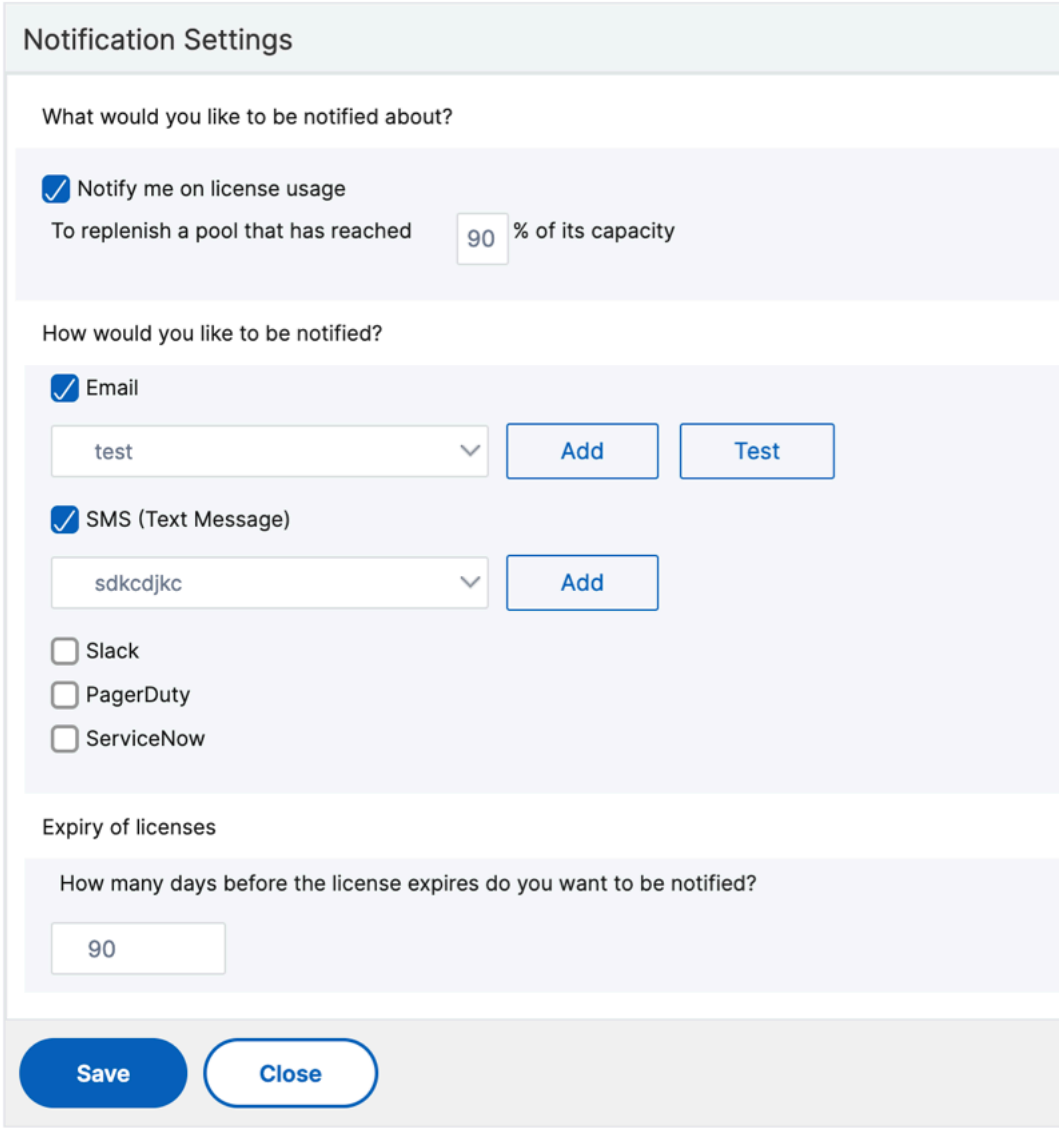
您可以创建自定义通知以补充默认的警报。

宽限期

当启用了 Citrix ADC 集容量的实例处于正常状态并且许可证服务器停止响应时，该实例将继续以当前容量运行 30 天。如果 30 天后没有恢复与许可证服务器的连接，则实例将失去其容量并停止处理流量。

通知和警报

可以通过 Citrix Application Delivery Management (ADM) 为对实例执行的任何操作启用通知。除了自定义通知设置外，默认情况下会配置以下警报。例如：要配置补充已耗尽一定百分比容量的池的警报，请导航到“基础架构”>“许可证”>“设置”>“通知设置”，然后单击“编辑”按钮。



发生问题时的预期行为

February 6, 2024

以下是许可证服务器和 Citrix ADC 实例遇到所述问题时的预期行为：

许可证服务器停止响应

> 警告
>
> 许可证服务器没有响应。Citrix ADC 将继续以当前容量运行 30 天。30 天后，如果未恢复到许可证服务器的连接，Citrix ADC 将失去其当前容量并停止处理流量。

如果许可证服务器停止响应，Citrix ADC 实例将进入宽限期，直到连接恢复为止。

启用 **Citrix ADC** 集容量的实例停止响应

如果启用了 Citrix ADC 集容量的实例停止响应，并且许可证服务器处于正常状态，则许可证服务器将在 10 分钟后检查所有 Citrix ADC 实例的许可证。实例重新启动后，它将发送请求以从许可服务器签出所有许可证。

许可证服务器和启用 **Citrix ADC** 集容量的实例都停止响应

如果许可证服务器和启用 Citrix ADC 池容量的实例都重新启动并重新建立连接，则许可证服务器会在 10 分钟后签入所有许可证，并且启用 Citrix ADC 池容量的实例会在重新启动完成后自动签出许可证。

启用 **Citrix ADC** 集容量的实例可以正常地关闭

在正常关闭过程中，您可以选择签入许可证或保留在正常关闭之前分配的许可证。如果您选择签入许可证，则启用 Citrix ADC 集容量的实例在重新启动后将取消许可证。如果您选择保留许可证，则在实例关闭时将这些许可证签入许可服务器。实例重新启动后，它将与许可服务器重新建立连接，并签出保存的配置中指定的许可证。

如果系统重新启动并且由于池中没有可用容量而导致检出失败，Citrix ADC 将检查 Citrix Application Delivery Management (ADM) 池许可证的清单，并检出任何可用容量。如果 Citrix ADC 未按照配置以满容量运行，则会引发 SNMP 警报以通知用户此情况。如果带宽池中没有可用容量，则启用了池容量的实例将处于未获许可状态。

网络失去连接

> 错误消息（系统日志）
>
> 许可证服务器未响应。

如果许可证服务器和启用 Citrix ADC 集容量的实例处于正常状态，但网络连接丢失，则这些实例将继续以其当前容量运行 30 天。30 天后，如果没有恢复与许可证服务器的连接，则实例将失去其容量并停止处理流量，且许可证服务器将签入其所有许可证。许可证服务器重新建立与 Citrix ADC 实例的连接后，这些实例将再次签出许可证。

配置池容量许可证的过期检查

February 6, 2024

现在，您可以为 Citrix ADC 池容量许可证配置许可证到期阈值。通过设置阈值，Citrix Application Delivery Management (ADM) 在许可证即将过期时通过电子邮件或 SMS 发送通知。当 Citrix ADM 上的许可证过期时，还会发送 SNMP 陷阱和通知。

当发送许可证到期通知并且可以在 Citrix ADM 上查看此事件时，将生成一个事件。

要配置许可证到期检查，请执行以下操作：

1. 导航到 “网络” > “许可证”。
2. 在“许可证设置”页面的“许可证到期信息”部分下，您可以找到即将到期的许可证的详细信息：
    - 功能：即将过期的许可证类型。
    - 数量：将 受影响的虚拟服务器或实例的数量。
    - 到期天数：许可证到期前的天数。
3. 在“通知设置”部分，单击“编辑”图标并指定警报阈值。您可以设置用于通知管理员的池许可证容量的百分比。
4. 通过选中相应的复选框来选择要发送的通知类型。通知类型如下：
    a) 电子邮件配置文件：指定邮件服务器和配置文件详细信息。当您的许可证即将过期时，将触发电子邮件。
    b) **SMS** 配置文件：指定短信服务 (SMS) 服务器和配置文件详细信息。当您的许可证即将过期时，会触发 SMS 消息。
5. 然后，根据许可证到期前的天数指定要发送通知的时间。
6. 单击保存。

> 注意
>
> 向池中添加新许可证时，Citrix ADC 实例将在其现有许可证到期时使用新许可证。

Citrix ADC VPX 签入和签出许可

February 6, 2024

您可以通过 Citrix Application Delivery Management (ADM) 按需将 VPX 许可证分配给 Citrix ADC VPX 实例。许可证由 Citrix ADM 存储和管理，其许可框架可提供可扩展的自动许可证配置。在配置 Citrix ADC VPX 实例时，Citrix ADC VPX 实例可以从 Citrix ADM 中检出许可证，或者在删除或销毁实例时，将其许可证重新检查到 Citrix ADM。

必备条件

请务必满足以下必备条件：

- 您正在使用运行软件版本 12.0 的 Citrix ADC VPX 映像。
  例如：NSVPX-ESX-12.0-xx.xx_nc.zip
- 您已安装运行版本 12.0 的 Citrix ADM。
  例如：MAS-ESX-12.0-xx.xx.zip

> 注意
>
> 要通过 Citrix ADM 管理现有 VPX 许可证，您需要将许可证重新托管到 Citrix ADM。

在 **Citrix ADM** 中安装许可证

> 注意：
>
> 在安装许可证之前，如果您更改了软件版本或带宽，请重新启动 Citrix ADM 虚拟设备。

要在 **Citrix ADM** 上安装许可证文件，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 User Name（用户名）和 Password（密码）中，输入管理员凭据。
3. 导航到“网络”>“许可证”。
4. 在“许可证文件”部分中，选择以下选项之一：
   - 从本地电脑上载许可文件-如果本地电脑 上已经存在许可文件，则可以将其上载到 Citrix ADM。
     要添加许可证文件，请单击“浏览”，然后选择要添加的许可证文件 (.lic)。然后单击“完成”。
   - 使用许可证访问代码 -Citrix 通过电子邮件向您购买的许可证访问代码 (LAC) 发送电子邮件。
     要添加许可证文件，请在文本框中输入 LAC，然后单击“获取许可证”。

   > 注意：
   >
   > 在使用 LAC 代码安装许可证之前，请确保您已连接到互联网。

   您可以随时从许可证设置向 Citrix ADM 添加更多许可证。

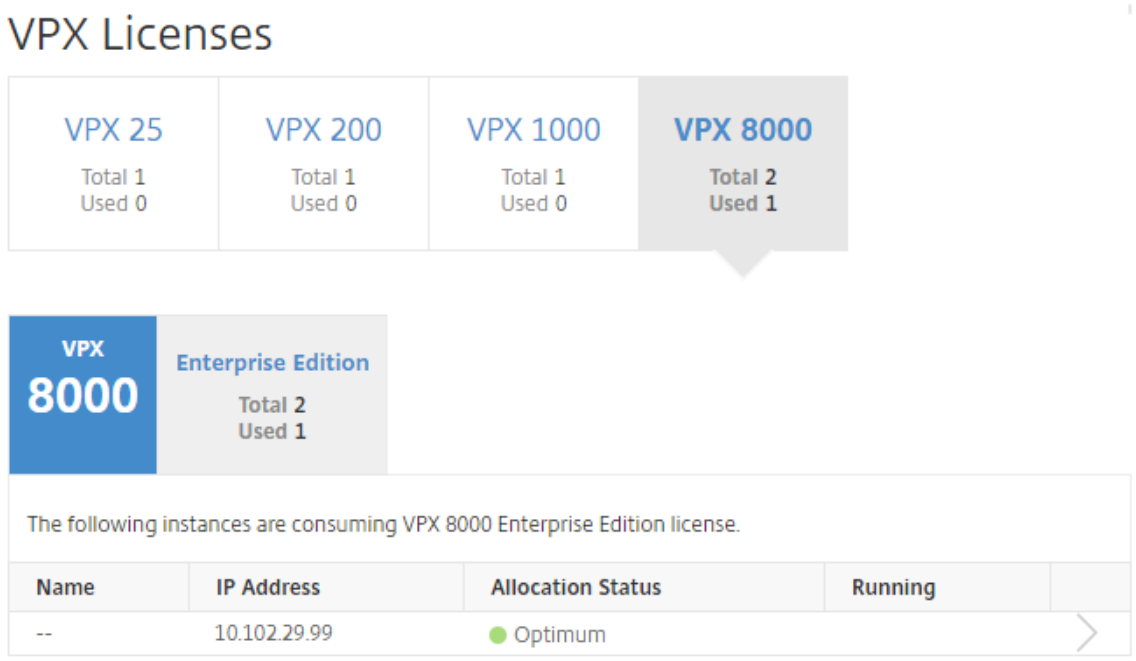
验证

您可以在 Citrix ADM GUI 中查看可用和已分配的许可证。

要显示许可证，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。

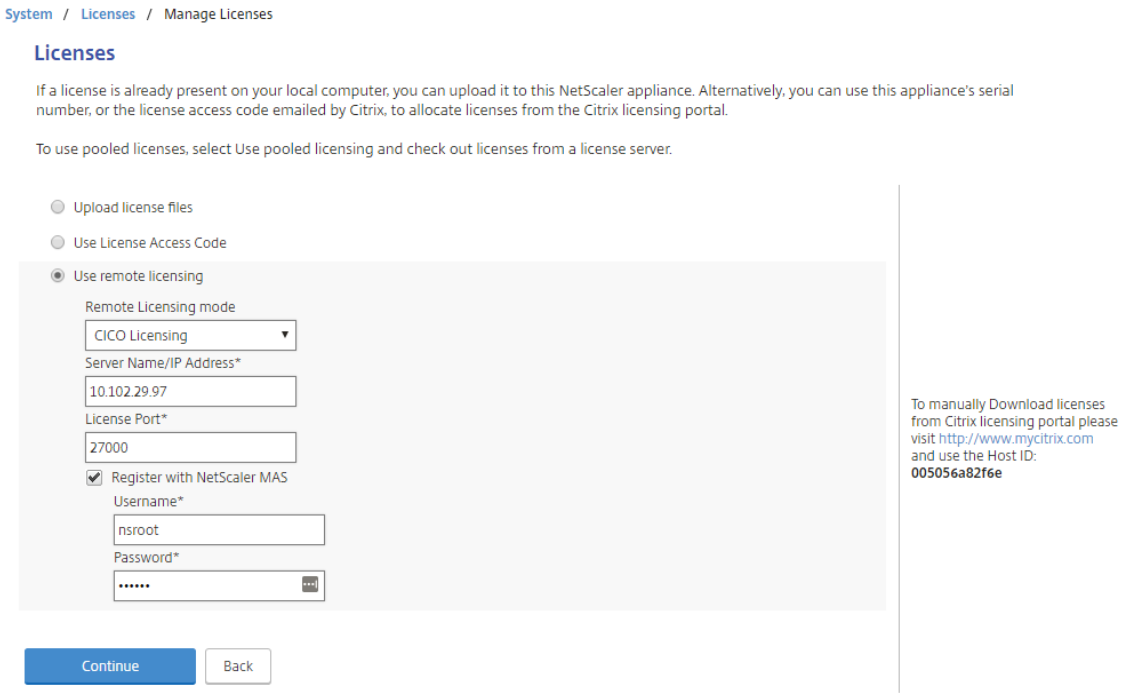
3. 在“配置”选项卡上，导航到“网络”>“许可证”>“**VPX** 许可证”。



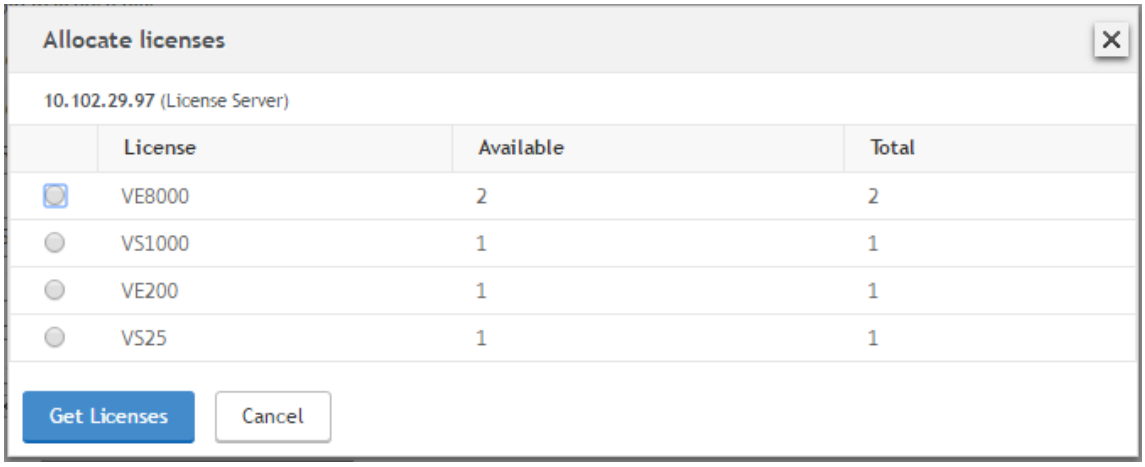
4. 您可以在可用许可证部分下的表中查看分配的许可证。

使用 **Citrix ADC GUI** 将 **VPX** 许可证分配到 **Citrix ADC VPX** 实例

1. 在 Web 浏览器中，键入 Citrix ADC 实例的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“系统”>“许可证”>“管理许可证”，单击“添加新许可证”，然后选择“使用远程许可”。
4. 在“服务器 名称/**IP** 地址”字段中输入许可证服务器的详细信息。
5. 如果您想通过 Citrix ADM 管理实例的 VPX 许可，请选中“向 **Citrix ADM** 注册”复选框并输入 Citrix ADM 凭据。

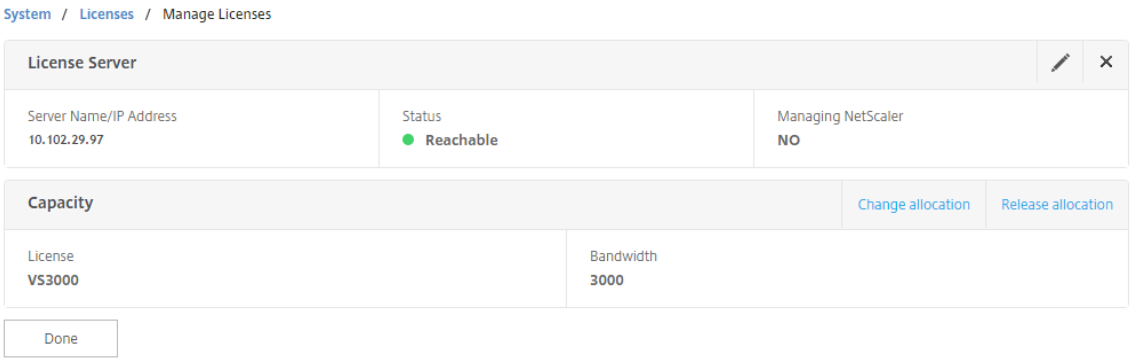


6. 选择具有所需带宽的许可证版本，单击 获取许可证。



7. 单击“重启”，您的 Citrix ADC VPX 实例将重启。

8. 您可以通过导航到“系统”>“许可证”**>**“管理许可证”，然后选择“更改分配”或“发布 ** 分配”来更改或释放许 ** 可证分配。



9. 如果单击更改分配，弹出窗口将显示许可证服务器上可用的许可证。选择所需的许可证，单击 获取许可证。

使用 **Citrix ADC CLI** 将 **VPX** 许可证分配到 **Citrix ADC VPX** 实例

1. 在 SSH 客户端中，输入 Citrix ADC 实例的 IP 地址，然后使用管理员凭据登录。
2. 要添加许可服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. 要显示许可服务器上的可用许可证，请输入以下命令：

```
sh licenseserverpool
<!--NeedCopy-->
```



```
> 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. 要为 Citrix ADC VPX 装置分配许可证，请输入以下命令：

```
set capacity  -platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

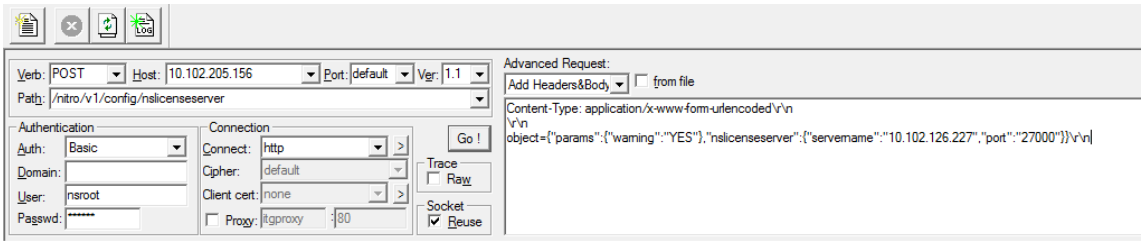
通过使用 **API** 将 **VPX** 许可证分配给 **Citrix ADC VPX** 实例

在 Web 浏览器或 API 客户端中，使用管理员凭据登录到 Citrix ADC VPX 实例。

要添加许可服务器，请执行以下操作：

1. 将请求类型设置为“过 帐”。
2. 将路径设置为 /nitro/v1/config/nslicensingserver。
3. 按如下方式设置有效载荷：

```
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
<!--NeedCopy-->
```

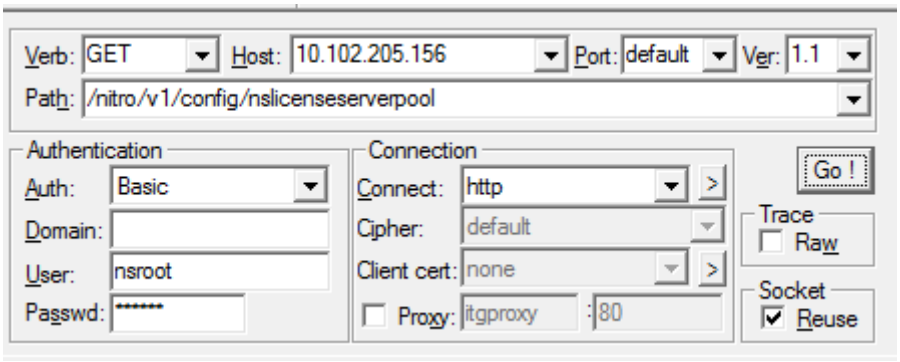



Citrix ADM 响应请求。以下示例响应显示成功。

```
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.
```

要查看许可服务器上的可用许可证，请执行以下操作：

1. 将请求类型设置为 **Get**。
2. 将路径设置为 /nitro/v1/config/nslicenseserverpool



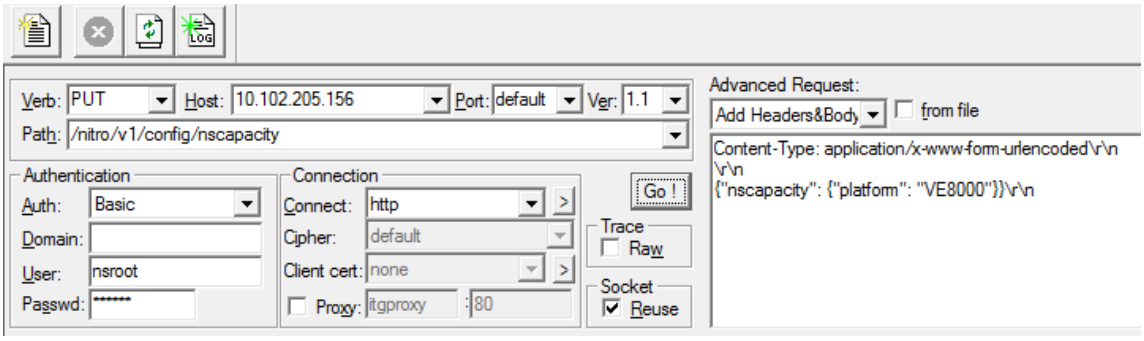
Citrix ADM 响应请求。以下示例响应显示成功，以及许可证服务器上的可用许可证列表。

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.

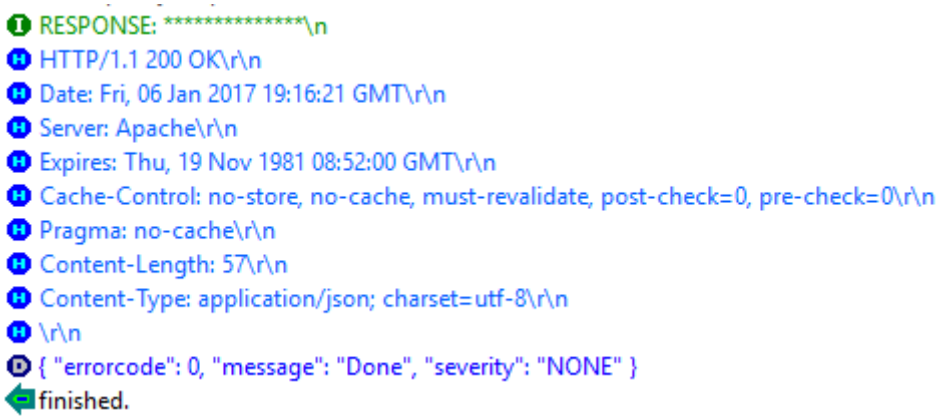
要将许可证分配给 **Citrix ADC VPX** 装置，请执行以下操作：

1. 将请求类型设置为“过 帐”。
2. 将路径设置为 /nitro/v1/config/nscapacity。
3. 按如下方式设置有效载荷：

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  “nscapacity:{
  “platform” :” VE8000”  }
  }
 \r\n
<!--NeedCopy-->
```



Citrix ADM 响应请求。以下示例响应显示成功。



为 **Citrix ADC VPX** 登入/退出许可证配置过期检查

现在，您可以为 Citrix ADC VPX 许可证配置许可证到期阈值。通过设置阈值，Citrix ADM 在许可证即将到期时通过电子邮件或 SMS 发送通知。当 Citrix ADM 上的许可证过期时，还会发送 SNMP 陷阱和通知。

当发送许可证到期通知并且可以在 Citrix ADM 上查看此事件时，将生成一个事件。

要配置许可证到期检查，请执行以下操作：

1. 导航到 “网络”> “许可证”。
2. 在“许可证设 置”页面的 “许可证到期 信息”部分下，您可以找到即将到期的许可证的详细信息：
   - 功能：即将过期的许可证类型。
   - 数量：将受到影响的虚拟服务器或实例的数量。
   - 到期天数：许可证到期前的天数。
3. 在“通知设置”部分，单击“编辑”图标并指定警报阈值。您可以设置用于通知管理员的池许可证容量的百分比。
4. 通过选中相应的复选框来选择要发送的通知类型。通知类型如下：
   a) 电子邮件配置文件：指定邮件服务器和配置文件详细信息。当您的许可证即将过期时，将触发电子邮件。
   b) **SMS** 配置文件：指定短信服务 (SMS) 服务器和配置文件详细信息。当您的许可证即将过期时，会触发 SMS 消息。
5. 然后，根据许可证到期前的天数指定要发送通知的时间。
6. 单击保存。

Citrix ADC 虚拟 **CPU** 许可

February 6, 2024

像您这样的数据中心管理员正在转向更新的技术，这些技术可以简化网络功能，同时提供更低的成本和更大的可扩展性。较新的数据中心架构必须至少包含以下功能：

- 软件定义网络 (SDN)
- 网络功能虚拟化 (NFV)
- 网络虚拟化 (NV)
- 微型服务

这种运动还要求软件要求具有动态性、灵活性和敏捷性，以满足不断变化的业务需求。许可证还将由一个中央管理工具管理，并充分了解使用情况。

Citrix ADC VPX 的虚拟 **CPU** 许可

早些时候，Citrix ADC VPX 许可证是根据实例的带宽消耗分配的。Citrix ADC VPX 仅限使用基于其绑定许可证版本的特定带宽和其他性能指标。要增加可用带宽，必须升级到提供更多带宽的许可证版本。在某些情况下，带宽要求可能较低，但对其他 L7 性能（例如 SSL TPS、压缩吞吐量等）的要求更高。在这种情况下，升级 Citrix ADC VPX 许可证可能不合适。但是，您可能仍然需要购买带宽较大的许可证，以解锁 CPU 密集处理所需的系统资源。Citrix ADM 现在支持根据虚拟 CPU 要求向 Citrix ADC 实例分配许可证。

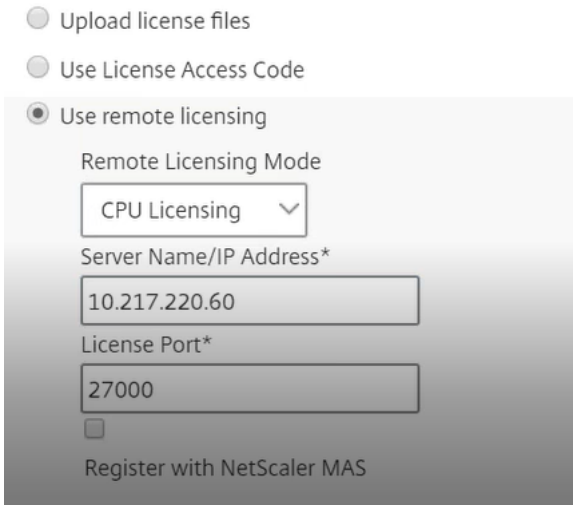
在基于 CPU 使用情况的虚拟许可功能中，许可证指定特定 Citrix ADC VPX 有权使用的 CPU 数量。因此，Citrix ADC VPX 只能从许可证服务器检出其上运行的虚拟 CPU 数量的许可证。Citrix ADC VPX 会根据系统中运行的 CPU 数量签出许可证。Citrix ADC VPX 在签出许可证时不考虑空闲 CPU。

与池许可证容量和 CICO 许可证功能类似，Citrix ADM 许可证服务器管理一组单独的虚拟 CPU 许可证。此外，为虚拟 CPU 许可证管理的三个版本是标准版、企业版和白金版。这些版本解锁了与带宽许可证版本解锁的功能集相同。

虚拟 CPU 的数量可能会发生变化，或者许可证版本有变化时。在这种情况下，您必须始终关闭实例，然后再发起新许可证集的请求。签出许可证后，必须重新启动 Citrix ADC VPX。

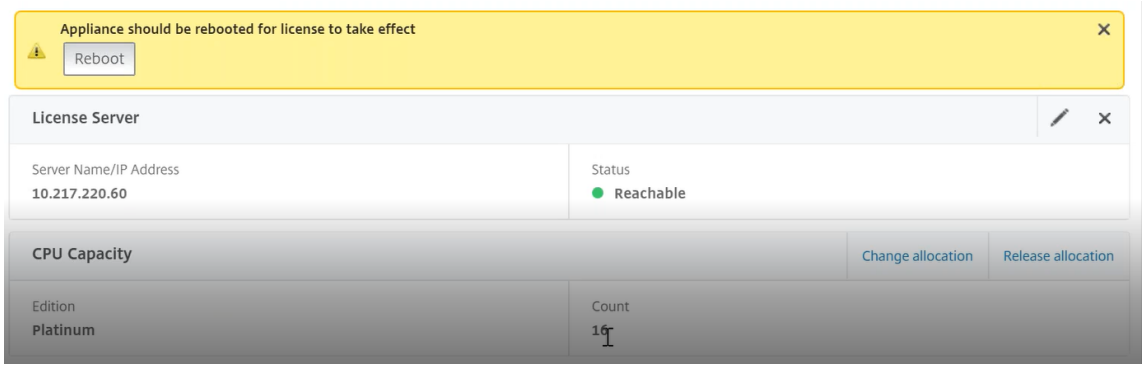
要使用 **GUI** 在 **Citrix ADC VPX** 中配置许可服务器，请执行以下操作：

1. 在 Citrix ADC VPX 中，导航到“系统”>“许可证”，然后单击“管理许可证”。
2. 在“许可证”页面上，单击“添加新许可证”。
3. 在“许可证”页面上，选择“使用远程许可”选项。
4. 从“远程许可模式”列表中选择 CPU 许可。
5. 键入许可证服务器的 IP 地址和端口号。
6. 单击继续。



> 注意
>
> 您必须始终在 Citrix ADM 中注册 Citrix ADC VPX 实例。如果尚未完成，请启用向 **Citrix ADM** 注册 并键入 Citrix ADM 登录凭据。

7. 在“分配许可证”窗口中，选择许可证类型。该窗口显示总数和可用的虚拟 CPU 以及可以分配的 CPU。单击 **Get Licenses**（获取许可证）。
8. 单击下一页上的 重新启动 以申请许可证。



> 注意
>
> 您还可以释放当前许可证并从其他版本签出。例如，您已经在实例上运行标准版许可证。您可以发布该许可证，然后从企业版中退出。

使用 **CLI** 在 **Citrix ADC VPX** 许可证中配置许可服务器

在 Citrix ADC VPX 控制台中，为以下两个任务键入以下命令：

1. 要将许可服务器添加到 Citrix ADC VPX，请执行以下操作：

```
1 add licenseserver <IP address of the license server>
```



```
<!--NeedCopy-->
```

2. 要申请许可证，请执行以下操作：

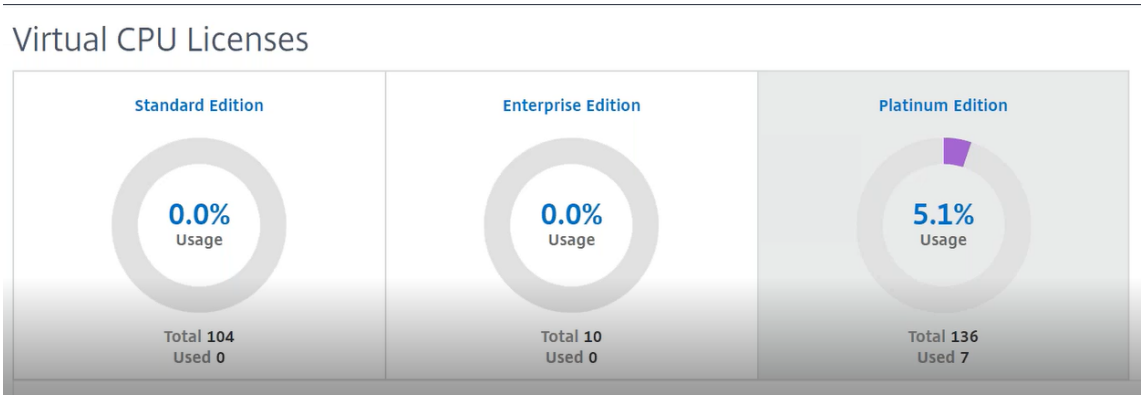
```
set capacity -vcpu - edition platinum
<!--NeedCopy-->
```

出现提示时，键入以下命令重新启动实例：

```
reboot -w
<!--NeedCopy-->
```

在 **Citrix ADM** 上管理虚拟 **CPU** 许可证

1. 在 Citrix ADM 中，导航到“网络”>“许可证”>“虚拟 **CPU** 许可证”。
2. 此页面显示为每种类型的许可证版本分配的许可证。
3. 单击每个甜甜圈中的数字可查看使用此许可的 Citrix ADC 实例。



适用于 **Citrix ADC CPX** 的虚拟 **CPU** 许可

在配置 Citrix ADC CPX 实例时，您可以将 Citrix ADC CPX 实例配置为根据实例的 CPU 使用情况从许可证服务器签出许可证。

Citrix ADC CPX 依靠在 Citrix ADM 上运行的许可证服务器来管理许可证。Citrix ADC CPX 在启动时从许可证服务器签出许可证。当 Citrix ADC CPX 关闭时，许可证将签回许可证服务器。

您可以从 Docker 应用商店下载 Citrix ADC CPX。在 Docker 主机上，要下载 Citrix ADC CPX，请运行以下命令：

```
docker pull store/citrix/netscalercpx:<version>
<!--NeedCopy-->
```

CPX 许可证有三种许可证类型：

1. CPX 和 VPX 支持虚拟 CPU 订阅许可证

2. 池容量许可证
3. CP1000 许可证仅支持 CPX 的单到多个 vCPU

要在置备 **Citrix ADC CPX** 实例的同时 **Provisioning vCPU** 订阅许可证，请执行以下操作：

您需要指定 Citrix ADC CPX 实例使用的 vCPU 许可数量。

- 此值通过 Docker、Kubernetes 或中索斯/马拉松作为环境变量输入。
- 目标变量是“CPX_CORES”。CPX 可以支持 1 到 7 个内核。

要指定 2 个内核，您可以执行 docker 运行命令，如下所示：

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2
<!--NeedCopy-->
```

在配置 Citrix ADC CPX 实例时，在 **docker run** 命令中将 Citrix ADC 许可服务器定义为环境变量，如下所示：

```
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
<!--NeedCopy-->
```

其中，

- *<LS_IP_ADDRESS>* 是 Citrix ADC 许可服务器的 IP 地址。
- *<LS_PORT>* 是 Citrix ADC 许可服务器的端口。默认情况下，端口为 27000。

> 注意
>
> 默认情况下，Citrix ADC CPX 实例会从 vCPU 订阅池中签出许可证。如果实例使用“n”CPU 运行，则 CPX 实例会检出“n”许可证数量。

要在预配 **Citrix ADC CPX** 实例时 **Provisioning Citrix ADC** 池容量或 **CP1000** 许可证，请执行以下操作：

如果您想使用池化许可（基于带宽）或 CPX 私有池（CP1000 或基于专用池）查看 CPX 实例的许可证，则必须相应地提供环境变量。

例如，

```
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
<!--NeedCopy-->
```

CP1000. 此命令触发从 CP1000 池（CPX 专用池）检出。然后，Citrix ADC CPX 实例检索为 CPX_CORES 指定的“n”个内核数量的“n”个实例。最常见的用例是为单个实例的检出指定 n = 1。多核 CPX 用例会检查“n”个 vCPU（其中“n”表示从 1 到 7）。


```
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
<!--NeedCopy-->
```

集合容量。此命令从实例池中签出一个许可证，消耗白金带宽池中的 1000 Mbps 带宽，但使 CPX 的运行速度高达 2000 Mbps。在池许可中，不收费前 1000 Mbps 的费用。

> 注意
>
> 从带宽池中取出时，为所需目标带宽指定相应的 vCPU 数量，如下表所示：

内核数量 (vCPU)	最大带宽
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

管理 **Citrix SD-WAN** 实例

February 6, 2024

使用 Citrix ADM 可以监视、管理和查看您的网络中的 Citrix SD-WAN 设备的分析数据。以下互操作性表提供了有关其中每个 Citrix SD-WAN 平台版本当前支持的 Citrix ADM 功能的信息。

Citrix SD-WAN 平台版本和 **Citrix ADM** 功能的互操作性矩阵

平台版本	发现	配置	监视	报告（网络报告）	事件管理	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	是	是	是	是	是	是	是

平台版本	发现	配置	监视	报告（网络报告）	事件管理	HDX Insight	WAN Insight
Citrix SD-WAN SE	是	否	否	否	否	否	否
Citrix SD-WAN PE	是	否	否	否	否	是	否

Citrix ADM 支持的 **Citrix SD-WAN** 版本

平台版本	Citrix SD-WAN 版本	Citrix ADM 版本
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 及更高版本	Citrix ADM 11.0 及更高版本
Citrix SD-WAN SE	Citrix SD-WAN 9.3.0 及更高版本	Citrix ADM 12.0.53.8 及更高版本
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 及更高版本	Citrix ADM 12.0.53.8 及更高版本

您可以将 Citrix SD-WAN WANOP 设备添加为 Citrix ADM 上的托管实例。有关更多信息，请参阅 将实例添加到 Citrix ADM。您可以查看 Citrix SD-WAN WANOP 实例的 WAN Insight、HDX Insight、网络报告和事件报告。

Citrix ADM 允许 Citrix SD-WAN 标准版 (SE) 和企业版 (EE) 设备将自身注册为 Citrix ADM 上的托管实例。

要将 Citrix SD-WAN SE/PE/AE 设备添加到 Citrix ADM，请在 Citrix SD-WAN SE/PE/AE 设备上将 Citrix ADM 配置为 AppFlow 收集器。Citrix SD-WAN SE/PE/AE 设备将自己添加为 Citrix ADM 上的托管实例。然后，SD-WAN SE/PE/AE 设备将分析数据发送到 Citrix ADM。

您可以在每个 SD-WAN SE/PE/AE 设备上单独将 Citrix ADM 设置为 AppFlow 收集器，也可以使用 Citrix SD-WAN 中心将配置导出到受控装置。

有关更多信息，请参阅 在 Citrix ADM 中添加 Citrix SD-WAN SE/PE/AE 实例。

对于 Citrix SD-WAN PE 装置，您可以查看 HDX 数据记录或多跳数据，具体取决于 AppFlow 配置。Citrix SD-WAN SE 设备仅提供多跳数据。有关更多信息，请参阅 查看 HDX Insight 报告和指标 和 查看多跃点部署的分析数据。

此页提供了一些主题的快速访问链接，您可以参考这些主题，以便使用 Citrix ADM 设备来管理 SD-WAN WANOP 设备。

Citrix ADM 概述

关于 Citrix ADM

Architecture

Citrix ADM 如何发现实例

Citrix ADM 如何与托管实例进行通信

Citrix ADM 部署

使用 Citrix Hypervisor 部署 Citrix ADM

使用 Microsoft Hyper-V 部署 Citrix ADM

使用 VMware ESXi 部署 Citrix ADM

使用 Linux KVM 服务器部署 Citrix ADM

在高可用性模式下部署 Citrix ADM

从 NetScaler Insight Center 迁移到 Citrix ADM

将 Citrix ADM 与 Director 集成

实例管理

如何向 Citrix ADM 中添加实例

如何在 Citrix ADM 上创建实例组

如何使用 Citrix ADM 备份和还原实例

配置管理

如何在 Citrix ADM 上使用纠正命令创建配置作业

如何在 Citrix ADM 中安排使用内置模板创建的作业

如何在 Citrix ADM 中重新安排使用内置模板配置的作业

如何重用执行的配置作业

分析

WAN Insight

HDX Insight

如何查看 Citrix SD-WAN WANOP 实例的网络报告

如何配置自适应阈值

如何为分析配置数据库汇总

如何使用 Citrix ADM 创建阈值和警报

事件管理

如何在 Citrix ADM 上设置事件的事件期限

如何使用 Citrix ADM 安排事件过滤器

如何在 Citrix ADM 中设置事件的重复电子邮件通知

如何使用 Citrix ADM 禁止显示事件

如何查看 Citrix SD-WAN WANOP 实例的事件报告

如何修改 NetScaler 实例上发生的事件的报告严重性

如何在 Citrix ADM 中查看事件摘要

如何在 Citrix ADM 的“Infrastructure”（基础结构）控制板上显示事件严重性和 SNMP 陷阱的偏差

身份验证

如何级联外部身份验证服务器

如何添加 RADIUS 身份验证服务器

如何添加 LDAP 身份验证服务器

如何添加 TACACS 身份验证服务器

如何在 Citrix ADM 中提取身份验证服务器组

如何启用回退本地身份验证

Citrix ADM 系统

管理 Citrix ADM 系统

如何升级 Citrix ADM

如何为 Citrix ADM 生成技术支持文件

如何在单服务器部署中备份和还原您的 Citrix ADM 服务器

如何备份和还原高可用性对中的 Citrix ADM 配置

如何在 Citrix ADM 中为非默认用户启用 shell 访问权限

如何在 Citrix ADM 上配置 NTP 服务器

如何为 Citrix ADM 配置 SSL 设置

如何为 Citrix ADM 配置 syslog 清除时间间隔

如何查看 Citrix ADM 的审核信息

如何配置 Citrix ADM 的系统通知设置

如何监视 Citrix ADM 的 CPU、内存和磁盘使用情况

如何为 Citrix ADM 配置密码组

如何在 Citrix ADM 上创建 SNMP 陷阱、管理员和用户

如何为 Citrix ADM 服务器分配主机名

如何为 Citrix ADM 配置系统修剪设置

如何使用 Citrix ADM 配置系统备份设置

如何在 Citrix ADM 上配置和查看系统警报

添加 **Citrix SD-WAN** 实例

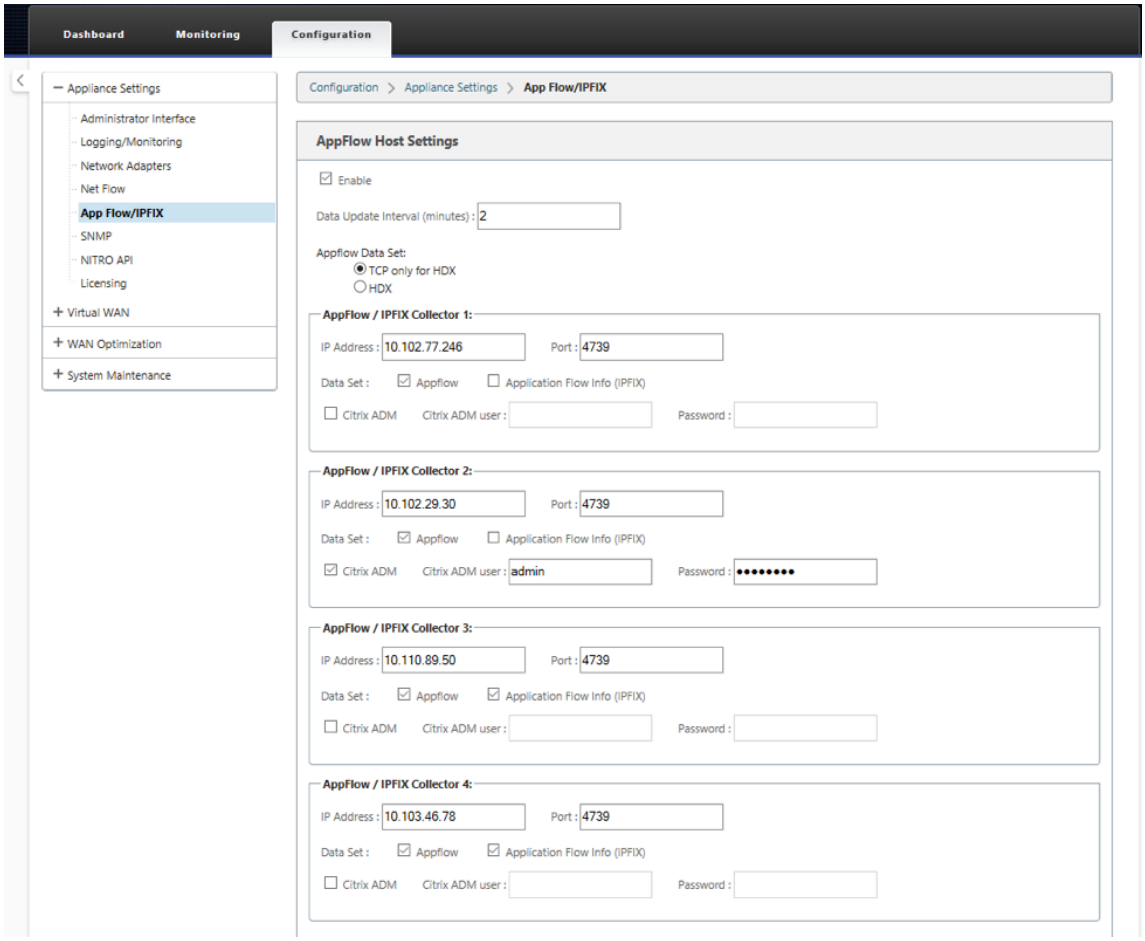
February 6, 2024

将 Citrix ADM 配置为 Citrix SD-WAN SE/PE 装置上的 AppFlow 收集器，以便在 Citrix ADM 中添加这些实例。Citrix SD-WAN SE/PE 装置在 Citrix ADM 上注册为托管实例，并收集其 AppFlow 记录。对于 Citrix SD-WAN PE 装置，您可以 仅为 **HDX** 模板启用 **TCP** ，也可以启用 **HDX** 模板。仅适用于 **HDX** 模板的 **TCP** 提供多跳数据。**HDX** 模板提供 HDX 数据，应仅在数据中心设备上启用该模板。

您可以在单个 SD-WAN SE/PE/AE 设备上将 Citrix ADM 配置为 AppFlow 收集器，也可以使用 SD-WAN Center 将 Citrix ADM 配置为 AppFlow 收集器，然后将配置导出到由其管理的设备。

要将 **Citrix ADM** 配置为 **Citrix SD-WAN SE/PE/AE** 设备上的 **AppFlow** 收集器，请执行以下操作：

1. 在 SD-WAN SE/PE/AE Web 界面中，导航到 配置 > **AppFlow/IPFix**
2. 选择“启用”。



3. 在“数据更新间隔”字段中，指定 AppFlow 报告导出到 AppFlow 收集器的时间间隔（以分钟为单位）。

> 注意
>
> 如果 Citrix ADM 是 AppFlow 收集器，则数据更新间隔应为 1 分钟。

4. 执行以下操作之一：

   - 选择 **HDX**，将 HDX 见解数据发送到 AppFlow 收集器。应该在分支设备上启用此选项。
   - 选择“仅适用于 **HDX** 的 **TCP**”，将多跳数据发送到 AppFlow 收集器。

> 注意
>
> **HDX** 模板选项仅适用于 Citrix SD-WAN PE 装置，应在数据中心设备上启用该选项

5. 在“**IP** 地址”字段中，键入外部 AppFlow 收集器系统（Citrix ADM 服务器）的 IP 地址。
6. 在“端口 ”字段中，键入外部 AppFlow 收集器系统监听的端口号。默认值为 4739。
7. 选中“**Citrix ADM**”复选框，以指定 Citrix ADM 是 AppFlow 收集器。

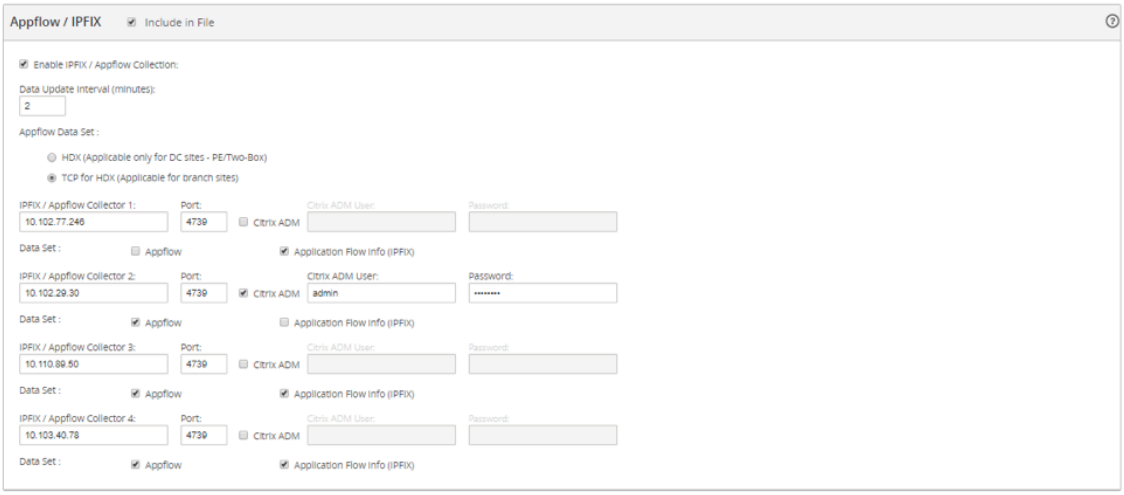
> 注意
>
> - Citrix ADM 目前不支持 IPFIX 集合。
> - 最多可以添加 4 个 AppFlow 收集器。Citrix ADM 或任何支持 IPFIX 协议的 AppFlow 收集器。

8. 输入 Citrix ADM 服务器的凭据
9. 单击 应用设置。

在 Citrix ADM 上发现并列出了 Citrix SD-WAN SE/PE 装置。Citrix SD-WAN SE/PE 装置将分析数据发送到 Citrix ADM。有关更多信息，请参阅 AppFlow 和 IPFIX。

要使用 **Citrix SD-WAN** 中心将 **Citrix ADM** 配置为 **AppFlow** 收集器，请执行以下操作：

1. 在 Citrix SD-WAN 中心管理用户界面中，导航到“配置”>“装置设置”。
2. 导航到 **AppFlow/IPFIX** 部分，然后选 择“包含在文件中”。
3. 选择启用 **IPFIX/AppFlow** 集合。



4. 在“数据 更新 间隔”字段中，指定 AppFlow 报告导出到 AppFlow 收集器的时间间隔（以分钟为单位）。

> 注意
>
> 如果 Citrix ADM 是 AppFlow 收集器，则数据更新间隔应为 1 分钟。

5. 执行以下操作之一：
   - 选择 **HDX**，将 HDX 见解数据发送到 AppFlow 收集器。
   - 为 **HDX** 选择 **TCP**，将多跳见解数据发送到 AppFlow 收集器。应该在分支设备上启用此选项。

> 注意
>
> **HDX** 模板选项仅适用于 Citrix SD-WAN PE 装置，应在数据中心装置上启用该选项。

6. 在 **IPFIX AppFlow** 收集 器字段中，键入外部 AppFlow 收集器系统（Citrix ADM 服务器）的 IP 地址。
7. 在“端口 ”字段中，键入外部 AppFlow 收集器系统监听的端口号。默认值为 4739。
8. 选中“**Citrix ADM**”复选框以指定 Citrix ADM 是 AppFlow 收集器。
9. 输入 Citrix ADM 服务器的凭据。

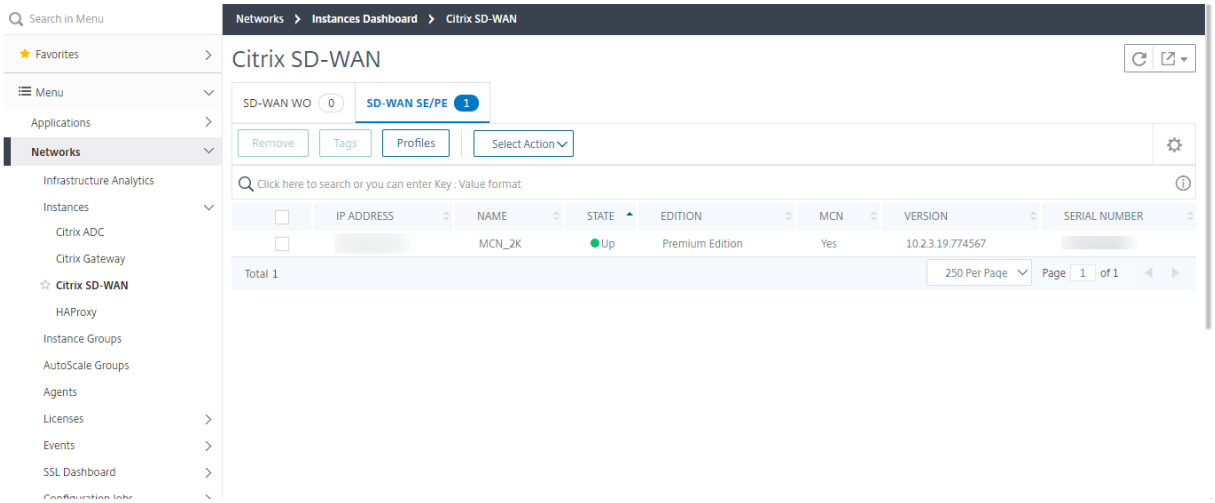
   > 注意
   >
   > 最多可以添加 4 个 AppFlow 收集器。Citrix ADM 或任何支持 IPFIX 协议的 AppFlow 收集器。

10. 保存配置并将其导出到托管设备中。

    有关详细信息，请参阅 如何配置装置设置并将其导出到受控装置。

有关使用 Citrix SD-WAN Center、AppFlow 和 IPFIX 将 Citrix ADM 配置为 AppFlow收集器的更多信息。

Citrix SD-WAN SE/PE 装置由 Citrix ADM 发现并列出。在 Citrix ADM 中发现并列出了 Citrix SD-WAN SE/PE 设备。要查看发现的 Citrix SD-WAN SE/PE 设备，请在 Citrix ADM Web 界面中导航到 网络 > 实例 > **Citrix SD-WAN** ，然后选择 **SD-WAN SE/PE/AE**。



您可以查看发现的设备的 IP 地址、名称、当前状态、软件版本和自身版本。还可以查看设备是否是主控制器节点 (MCN)。

您可以执行以下操作：

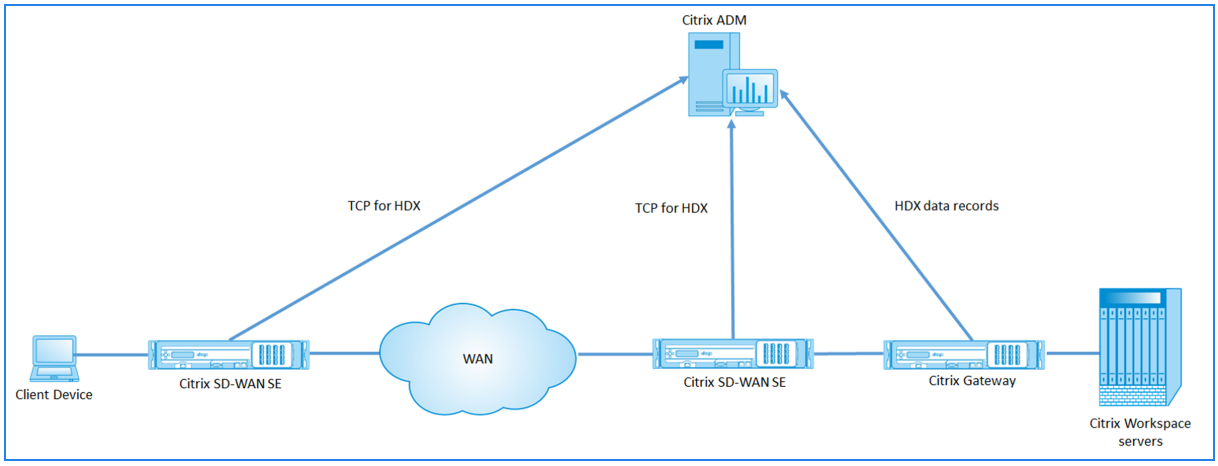
- 查看和删除实例配置文件。
- 从 Citrix ADM 中删除实例。
- 重新发现实例。

对于 Citrix SD-WAN PE 装置，您可以查看 HDX 数据记录或多跳数据，具体取决于 AppFlow 配置。Citrix SD-WAN SE 设备仅提供多跳数据。有关更多信息，请参阅 查看 HDX Insight 报告和指标 和 查看多跃点部署的 Citrix SD-WAN 分析数据。

查看用于多跃点部署的 **Citrix SD-WAN** 分析数据

February 6, 2024

在多跃点网络部署中，客户端与服务器之间有多个设备，如下图所示。在这种类型的部署中，Citrix SD-WAN SE 设备和 Citrix Gateway 将添加到 Citrix ADM 中，并启用 AppFlow。



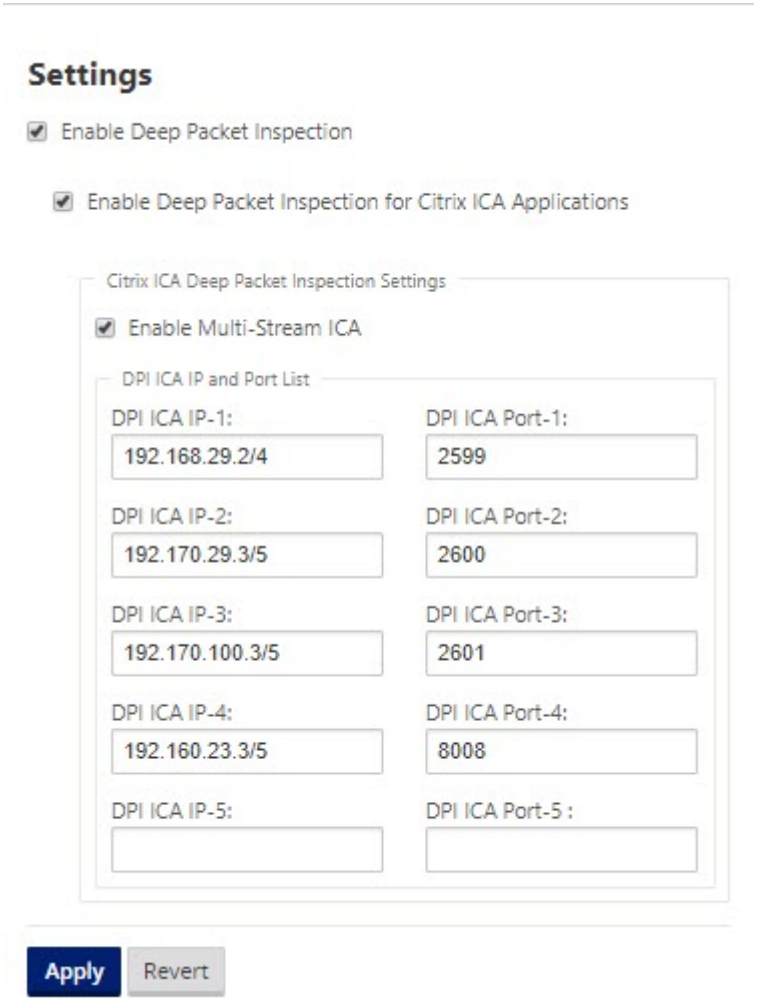
Citrix ADM 根据跳数和连接链 ID 识别从哪个设备接收数据。跃点计数表示流量从客户端传输到服务器通过的设备数。连接链 ID 表示客户端与服务器之间的端到端连接。

Citrix ADM 使用跳数和连接链 ID 来关联来自设备的数据，并生成报告。

要让 Citrix SD-WAN SE 设备将分析数据发送到 Citrix ADM，您应该将 Citrix Gateway 的虚拟 IP 地址配置为 DPI ICA IP，并将 DPI ICA 端口号设置为 443。

要配置 **ICA DPI** 设置，请执行以下操作：

1. 在 Citrix SD-WAN SE 设备用户界面中，导航到配置编辑器 > 高级 > 全局 > 应用程序 > 设置
2. 选择“启用深度包检测”>“为 **Citrix ICA** 应用程序启用深度包检测”>“启用多流 **ICA**”



3. 在 **DPI ICA IP-1** 字段中，输入 Citrix Gateway 虚拟 IP 地址和前缀。
4. 在 **DPI ICA** 端口 **1** 字段中，输入端口号 443。
5. 单击“应用”，然后使用更改管理流程将配置导出到设备。

在 Citrix ADM 中，对于每个活跃的 ICA 会话，您都可以在 HDX Insight 中查看会话图。会话图提供有关连接路径中的设备的详细信息。通过它们还可以深入了解网络设备与其紧邻的下一个跃点之间的客户端/服务器端延迟。通过此信息可以找出延迟的根本原因以及对性能问题进行故障排除。

Citrix SD-WAN SE 不发送 HDX 数据记录。它仅提供“适用于 HDX 的 TCP”信息。HDX 分析数据由网络中启用 HDX 分析的设备（例如，Citrix ADC 或 Citrix Gateway）提供。

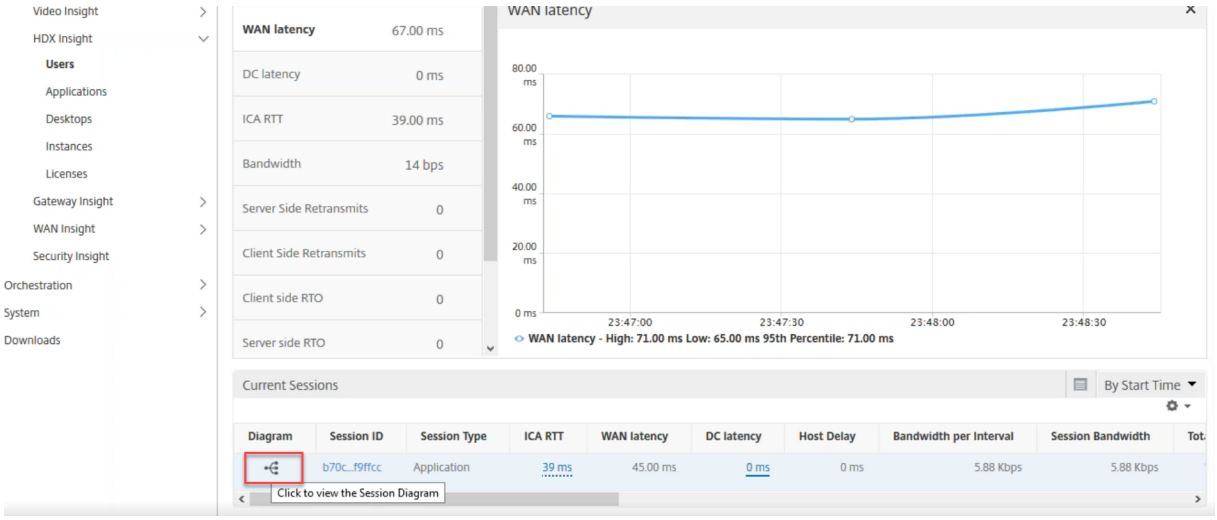
Citrix SD-WAN PE 设备可以为 HDX 数据或 HDX 洞察数据发送 TCP，具体取决于设备的 AppFlow 配置。应在数据中心设备上启用 HDX 模板。

> 注意
>
> 在多跃点部署中，请确保仅其中一个网络设备发送 HDX Insight 数据。其余网络设备可以发送“适用于 HDX 的

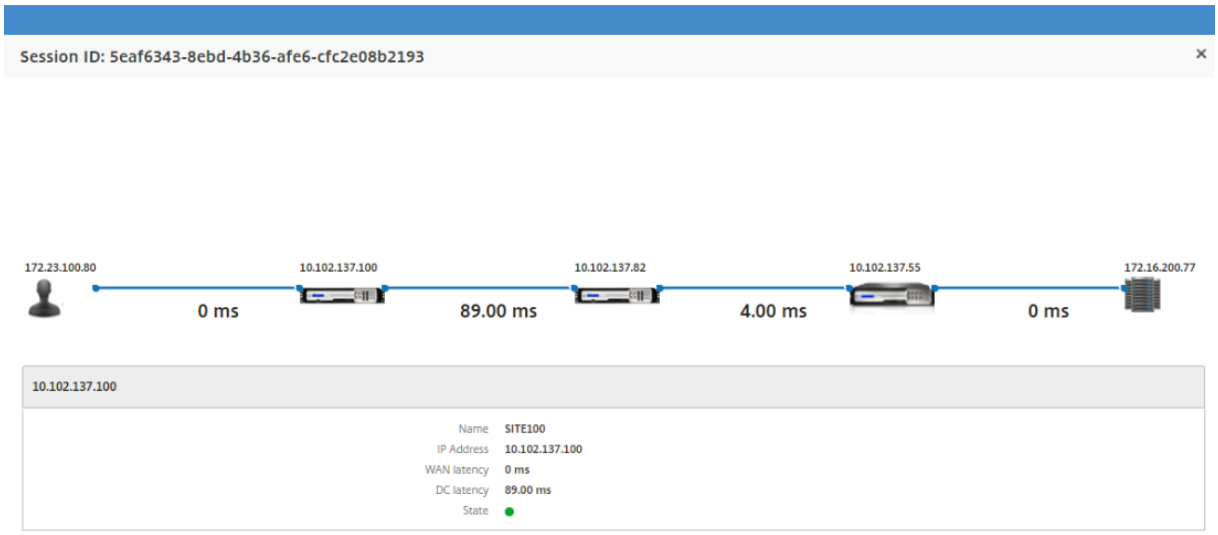
> TCP”数据。

要查看多跳数据，请执行以下操作：

在 Citrix ADM Web 界面中，导航到 **HDX Insight** > 用户 > 当前会话或 **HDX Insight** > 应用程序 > 当前会话，然后单击图表图标。



将显示网络拓扑图。



单击任何网络元素可显示详细信息。

> 注意
>
> 显示的信息取决于选定的网络元素。

Citrix 设备会显示以下参数：

- 名称：Citrix 设备的名称。
- **IP** 地址：设备的 IP 地址。

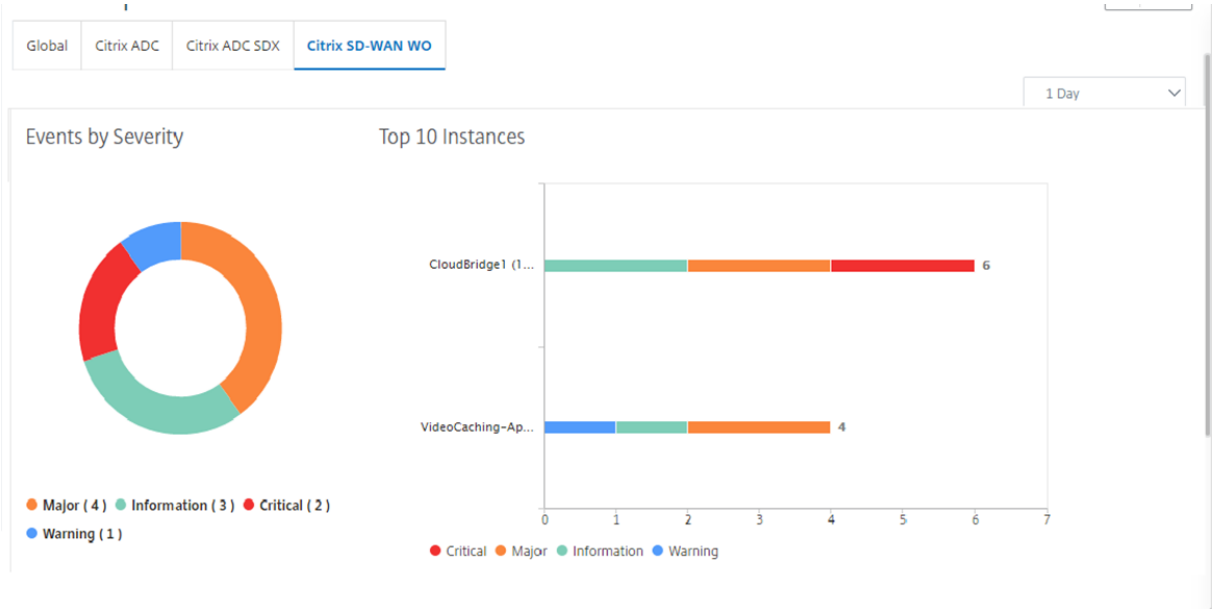
- 广域网延迟：由网络客户端引起的延迟。也就是说，从 Citrix 设备到最终用户。
- **DC** 延迟：由网络服务器端引起的延迟。也就是说，从 Citrix 设备到后端服务器。
- 状态：设备可达性状态。

查看 **Citrix SD-WAN WANOP** 实例的事件报告

February 6, 2024

您可以通过导航到 “网络” > “事件” > “报告”，然后选择 **Citrix SD-WAN WO**，以图形表示形式查看前 10 个 SD-WAN WANOP 实例的事件。

每个实例的事件根据其严重性进行显示，您可以单击每个严重性来了解有关事件数、事件发生时间以及事件所属类别的详细信息。



查看 **Citrix SD-WAN WANOP** 实例的网络报告

February 6, 2024

您可以在 Citrix ADM 中查看与 WAN 优化网络相关的报告，使用这些数据可以排除网络问题或分析 Citrix SD-WAN WANOP 设备的行为。您可以查看过去一小时、一天、一周或一个月内 WAN 优化设备的网络统计信息的报告。

您可以查看以下报告：

报告	说明
加速	使用此报告可以分析加速流量的模式（按服务类别的 KBPS）和通过 WAN 优化设备的 加速 TCP 连接数。这包括通过 WAN 优化设备进行加速的 TCP 连接数、已选择进行加速的开放和 半闭合连接数以及候选半开放连接 数加速度。
Pass through Connection（通过连接传送）	使用此报告可查看 WAN 优化设备的非加速连接。
Service Class（服务类别）	使用此报告可以查看基于为 WAN 优化设备 定义的服务类型的发送和接收带宽节省。
应用程序	使用此报告可以查看在 WAN 优化设备上 运行的应用程序的发送和接收数据卷（以每秒比特为单位）。
CPU 使用率	使用此报告可查看以百分比表示的 WAN 优化设备的 CPU 使用率。
Capacity Increase（容量增加）	使用此报告可查看 WAN 优化设备的累计发送压缩比。
Data reduction（数据减少）	使用此报告可查看以百分比表示的传输和接收带宽节省量。您还可以分别分析 WAN 优化设备的 传输带宽和接收带宽节省值。
Link Utilization（链路利用率）	使用此报告可以查看 WAN 优化的传输链路利用率和接收链路利用率的百分比。
Plugin Usage（插件使用情况）	使用此报告可查看连接到 WAN 优化设备的插件数。
Packet Loss（数据包丢失）	使用此报告可查看 WAN 优化设备中 定义的链路丢弃的已发送数据包和链路丢弃的接收数据包。
吞吐量	使用此报告可以查看 WAN 优化设备的链路发送卷和链路接收卷（以比特为单位）。
QoS	使用此报告可以查看 WAN 优化设备的 QOS 已发送和 QOS 接收卷（以位/秒为单位）。

要查看 **Citrix SD-WAN WANOP** 网络报告，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“网络报告”>“**Citrix SD-WAN WO**”。
2. 从“报 告名称”下拉列表中选择要查看的报告。
3. 从“实例”下拉列表中，选择要查看其报告的 Citrix SD-WAN WANOP 实例。
4. 从持续时 间 下拉列表中，选择时间间隔。
5. 单击运行。

备份 **Citrix SD-WAN WANOP** 实例

February 6, 2024

您可以备份实例的当前状态，稍后使用备份的文件将实例恢复到相同状态。在升级实例之前或出于预防原因备份实例是一种很好的做法。稳定系统的备份使您能够将系统恢复到稳定点，以防系统变得不稳定。有多种方法可以在 Citrix SD-WAN WANOP 实例上执行备份和恢复。您可以使用 GUI、CLI 进行临时备份和还原实例，也可以使用 Citrix ADM 执行备份。Citrix ADM 使用 NITRO 调用、安全外壳 (SSH) 协议和安全复制 (SCP) 协议复制托管 Citrix SD-WAN WANOP 实例的当前状态。

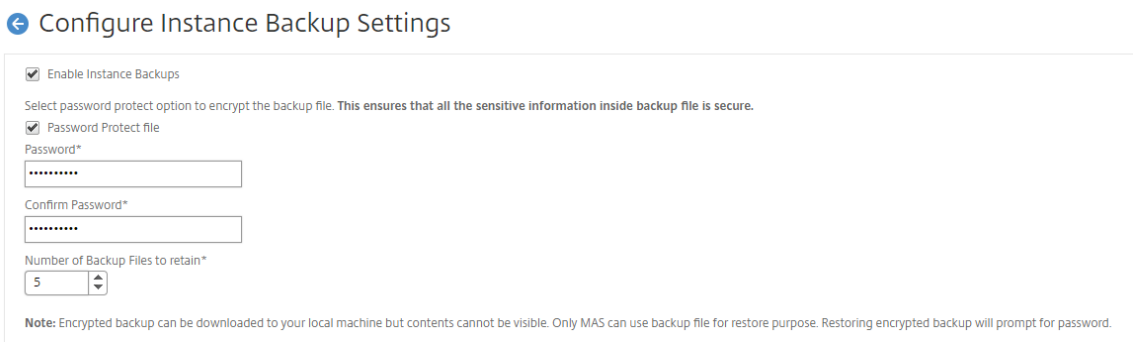
配置实例备份设置

在 Citrix ADM 中备份 Citrix SD-WAN WANOP 实例之前，必须在 Citrix ADM 上配置实例备份设置。

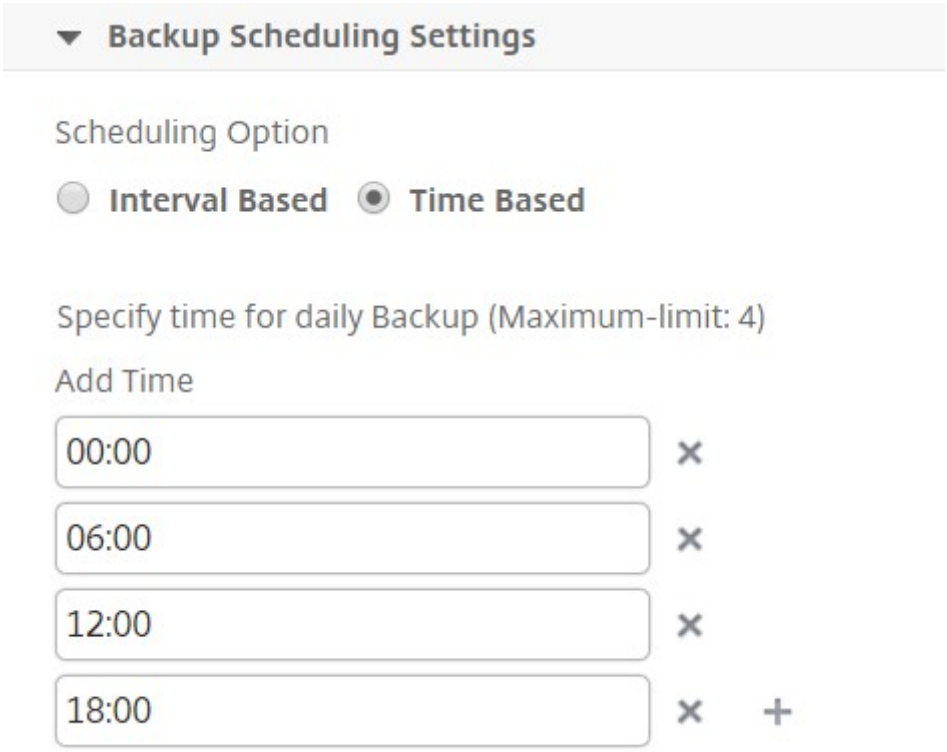
要配置实例备份设置，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“系统管理”。在右侧窗格的“备份设置”下，选择“实例备份设置”。
2. 选择“启用实例备份”。默认情况下启用此选项。
3. 选择“密码保护文件”以加密备份文件。加密备份文件可确保备份文件中的敏感信息是安全的。
4. 在“要保留的备份文件数量”字段中，指定要在 Citrix ADM 中保留的备份文件数量。您最多可以保留 50 个备份文件。

   > 注意
   >
   > 每个备份文件都需要一些存储要求。Citrix 建议您根据您的要求在 Citrix ADM 上存储最佳数量的备份文件。

5. 设置备份计划设置。选择以下选项之一：
   - 基于时间间隔 -在指定的时间间隔过后，在 Citrix ADM 中创建备份文件。默认备份时间间隔是 12 小时。
   - 基于时间 -您可以以“小时: 分钟”格式指定备份的时间。Citrix ADM 允许在实例上进行最多四次每日备份。

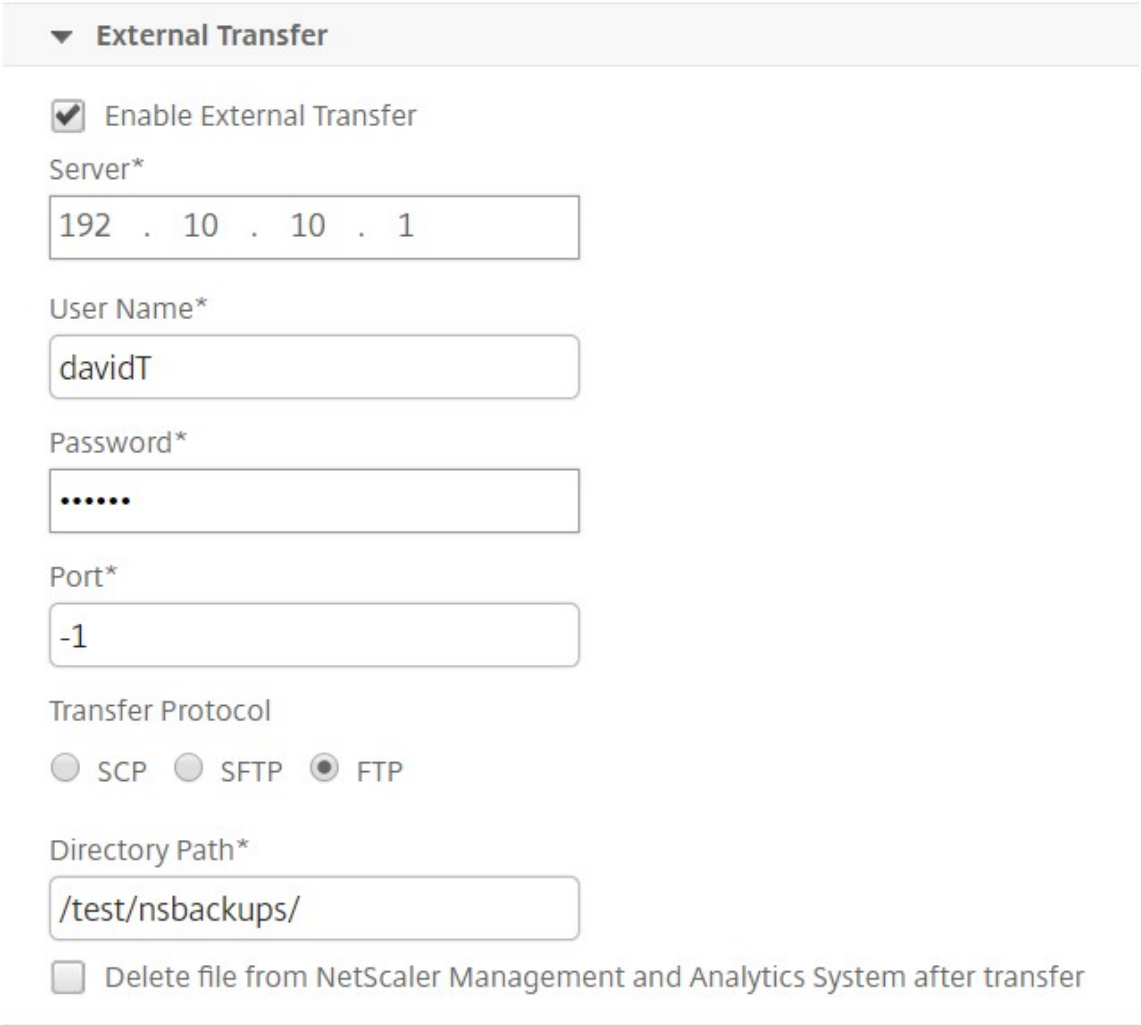


> 注意
>
> 忽略 **Citrix ADC** 设置 部分；这些设置不适用于 Citrix SD-WAN WANOP 实例。

6. 选择 启用外部传输 以将实例备份文件传输到外部位置。输入以下字段的值：

   - 服务器：外部服务器的 IP 地址。
   - 用户名：外部服务器的用户名
   - 密码：外部服务器的密码。
   - 端口：用于与外部服务器通信的端口号。
   - 传输协议：用于将备份文件从 Citrix ADM 传输到外部服务器的协议。

   还可以在将备份文件传输到外部服务器后从 Citrix ADM 中删除备份文件。



7. 单击确定。

> 注意
>
> 当任何选定的 Citrix SD-WAN WANOP 实例出现备份失败时，Citrix ADM 会向自身发送 SNMP 陷阱或系统日志通知。

创建 **Citrix SD-WAN WANOP** 实例的备份

为 Citrix SD-WAN WANOP 实例创建备份的过程适用于使用默认 nsroot 配置文件的管理员用户。

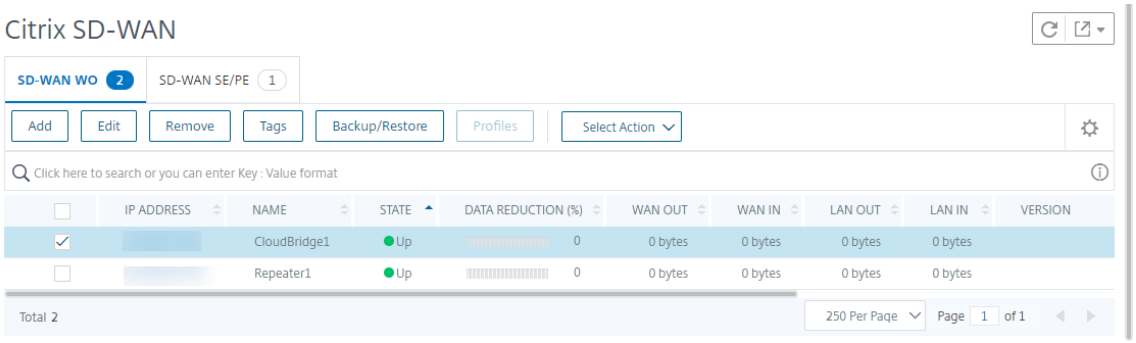
有关自定义用户如何备份 Citrix SD-WAN WANOP 实例的信息，请参阅本主题中的“为自定义用户创建 Citrix SD-WAN WANOP 实例的备份”部分。

有关更多信息，请确保已将 Citrix SD-WAN WANOP 实例添加到 Citrix ADM 中，请参阅 将实例添加到 Citrix ADM。

要为 **Citrix SD-WAN WANOP** 实例创建备份，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“实例”>“**Citrix SD-WAN**”。

2. 在 **SD-WAN WO** 中，选择要备份的 Citrix SD-WAN WANOP 实例，然后单击备份/还原。



3. 在“备份文件”页面上，单击“备份”。
4. 使用以下任一选项对备份文件进行加密：
   - 选择“受密码保护的文件”，然后输入密码以加密备份文件。
   - 选择 使用全局密码 以使用您在实例备份设置页面上指定的全局密码。
5. 单击“创建
   备份”

为自定义用户创建 **Citrix SD-WAN WANOP** 实例的备份

如果您已在 Citrix SD-WAN WANOP 实例中创建了具有管理员权限的自定义用户，请使用以下过程添加实例并使用 Citrix ADM 备份该实例。

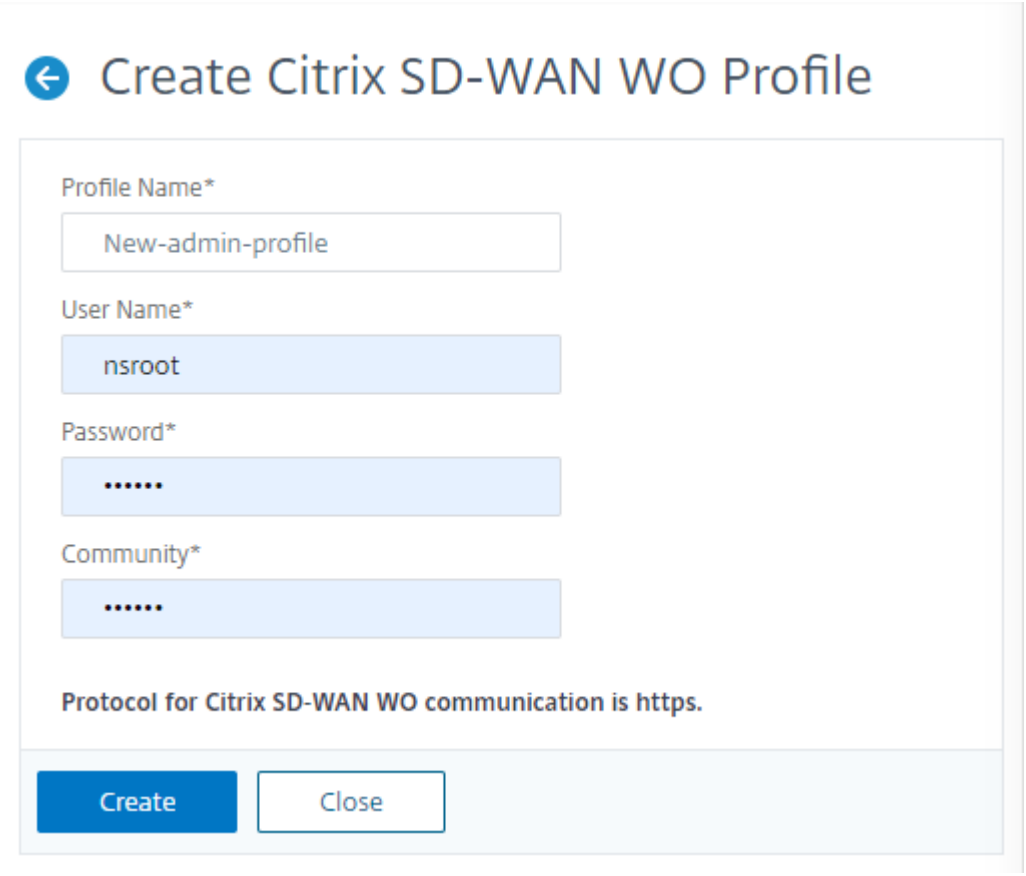
自定义用户的备份操作在 400/800/1000WS/2000/2000WS/3000/4000/5000/4100/5100 SD-WAN WANOP 平台上不受支持。

> 注意
>
> Citrix 建议您在 Citrix ADM 中创建 Citrix SD-WAN 高级平台的备份时使用默认 nsroot 配置文件。

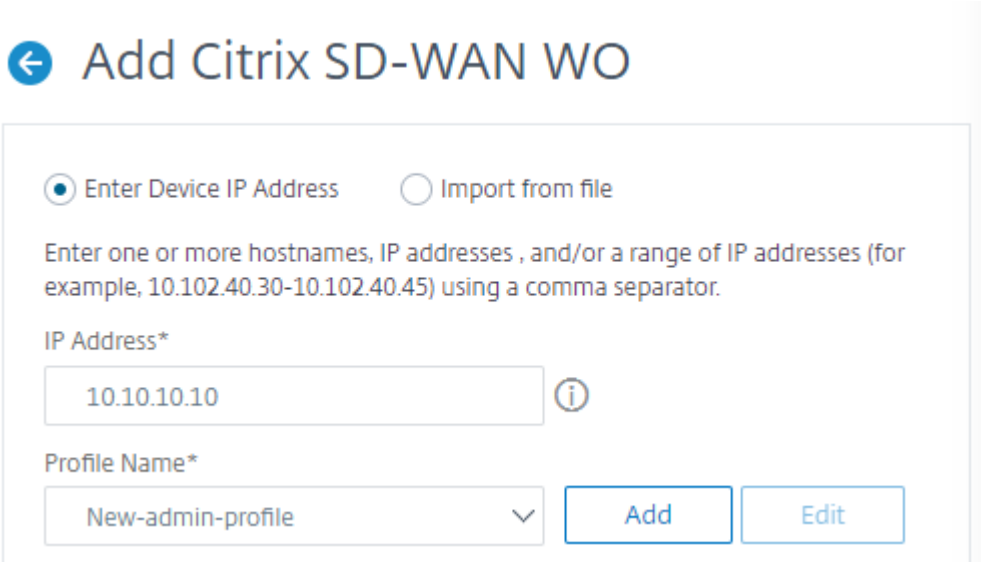
要添加 **Citrix SD-WAN WANOP** 实例并为自定义用户执行备份，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“实例”>“**Citrix SD-WAN**”，然后选择“**SD** 广域网”。
2. 单击添加。
3. 在 **IP** 地址 字段中，输入 Citrix SD-WAN WANOP 实例的 IP 地址。

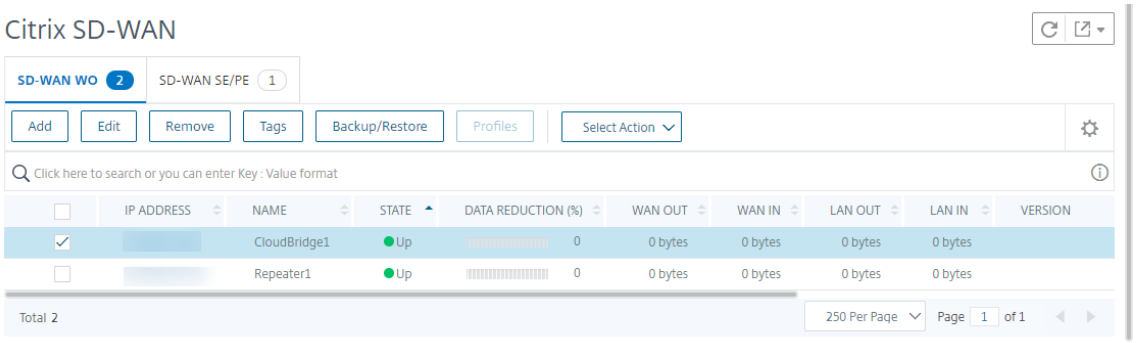
4. 单击“** 配置文件名称”字段旁边的“添加”以创建新的配置文件。将出现“创建 Citrix SD-WAN WO** 配置文件”窗口。



5. 在“配置文件名称”字段中，输入配置文件的名称。
6. 在“用户名”字段中，输入您在 SD-WAN WANOP 实例上创建的定制用户的用户名。
7. 在“密码”字段中，输入您在 SD-WAN WANOP 实例中为定制用户设置的密码。
8. 在“社区”字段中，输入在 SD-WAN WANOP 设备上配置的 SNMP 通信字符串。（例如：公共）
9. 单击创建。
10. 在“配置文件名称”字段中，选择新创建的配置文件并单击“确定”。



11. 导航至“网络”>“实例”>“**Citrix SD-WAN**”。
12. 在 **SD-WAN WO** 中，选择刚刚添加的 Citrix SD-WAN WANOP 实例，然后单击备份/还原。



13. 在“备份文件”页面上，单击“备份”。
14. 使用以下任一选项对备份文件进行加密：
    - 选择“受密码保护的文件”，然后输入密码以加密备份文件。
    - 选择“使用全局密码”以使用您在实例备份设置页面上指定的全局密码。

> 注意
>
> 您可以将加密的备份文件下载到本地计算机，但无法查看其内容。只有 Citrix ADM 可以将这些备份文件用于还原目的。恢复加密备份将提示输入密码。

15. 单击“创建备份”。

重要

```
1. 对于 Citrix SD-WAN WANOP VPX 装置，Citrix ADM 仅备份 CB 代理配置文件。
```

a) 对于高级 Citrix SD-WAN WANOP 平台，Citrix ADM 备份 以下内容：·

- CB 代理配置文件
- NTP 配置文件
- DNS
- SNMPD 配置文件
- 系统日志配置文件
- SSL 证书、密钥和策略
- SVM 数据库文件
- 组件（XML 格式）
- 资源（XML 格式）

下表中列出了各个文件夹中备份的文件。请注意，如果文件夹名称后接“*”，则备份该文件夹中的所有文件夹。

目录	子目录或文件
/br_broker/	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/*
/var/	mps/policy/、*mps/ssl_certs/sdx_default_ssl_cert*、*mps/ssl_keys/sdx_default_ssl_key*、*mps/tenants/*

管理 **HAProxy** 实例

February 6, 2024

HAProxy 是开放源负载平衡器，可以对任何 TCP 或 HTTP 服务进行负载平衡。有关 HAProxy 的详细信息，请参阅 http://www.haproxy.org/。

Citrix Application Delivery Management (Citrix ADM) 支持 HAProxy 1.4.24 或更高版本。在您向 Citrix ADM 中添加已在其中预配了 HAProxy 实例的主机时，Citrix ADM 会发现该主机上的 HAProxy 实例并允许您对其进行监视。它将向您显示有关实例上 HAProxy 配置的以下类型信息：

- 前端 - 请求应该如何转发到后端。
- 后端 - 接收转发的请求的一组服务器。
- 服务器 - HAProxy 用于对流量进行负载平衡的服务器。

有关详细信息，请参阅 http://www.haproxy.org/download/1.7/doc/configuration.txt。

此外，Citrix ADM 还提供了 HAProxy 应用程序控制板，您可以在其上实时监视前端。有关更多信息，请参阅HAProxy 应用程序控制面板。

将 **HAProxy** 实例添加到 **Citrix ADM**

February 6, 2024

在 Citrix Application Delivery Management (Citrix ADM) 中，您需要手动添加配置 HAProxy 实例的主机的详细信息。添加这些详细信息后，Citrix ADM 会自动发现在主机上置备的 HAProxy 实例并将其添加到 Citrix ADM 清单中。它还会发现 HAProxy 实例上配置的所有前端、后端和服务器，并将前端视为发现的应用程序。

必备条件

请务必执行以下操作：

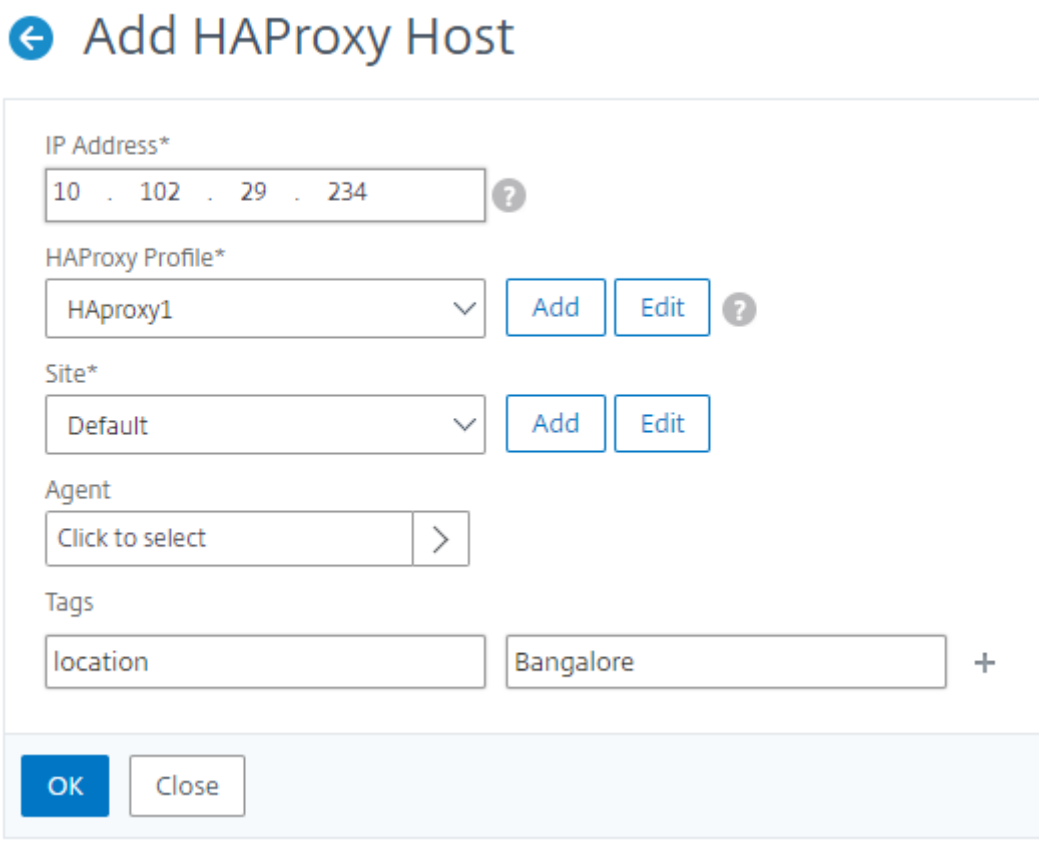
- 在您的部署中的主机上部署了 HAProxy 实例。有关详细信息，请参阅 http://www.haproxy.org/#docs。
- 识别并确定要在“HAProxy App Dashboard”（HAProxy 应用程序控制板）上查看其应用程序统计信息的前端的数量。默认情况下，“HAProxy App Dashboard”（HAProxy 应用程序控制板）显示 30 个发现的应用程序的统计信息。有关 HAProxy 应用程序控制面板的更多信息，请参阅 HAProxy 应用程序控制面板。如果要查看 30 个以上发现的应用程序的统计信息，需要购买单独的许可证。有关详细信息，请参阅 第三方许可。

> 重要
>
> Citrix ADM 需要访问主机才能发现其中的 HAProxy 实例。您可以通过提供主机的 SSH 密钥对或使用主机密码来提供对 Citrix ADM 的访问。如果您要使用 SSH 密钥对提供访问权限，请务必在主机中生成 SSH 私钥和公钥对，并将公钥添加到主机上的授权密钥。此外，SSH 用户帐户必须具有超级用户权限。

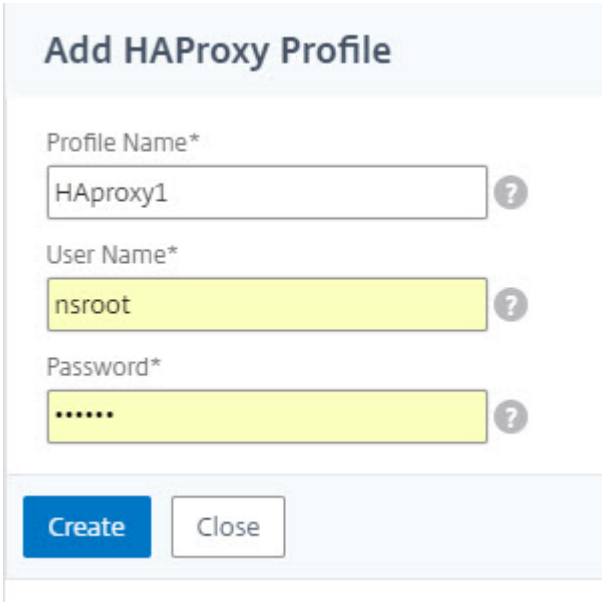
要将 **HAProxy** 实例添加到 **Citrix ADM**，请执行以下操作：

1. 在 Web 浏览器中，键入 **Citrix Application Delivery Management** 的 IP 地址（例如 http://192.168.100.1）。
2. 在“用户名”和“密码”字段中，输入管理员 凭据。默认的管理员凭据是“nsroot”和“nsroot”。

3. 导航到 网络 > 实例。在“实例”下，选择 **HAProxy** ，然后单击“添加”。
4. 在“添加 **HAProxy** 主机”对话框中，执行以下操作：



1. 在 **IP** 地址字段中，输入已置备 HAProxy 实例的主机的 IP 地址。
   a) 在 **HAProxy** 配置文件 菜单中，选择一个现有的 HAProxy 配置文件，或者创建并选择一个新的 HAProxy 配置文件。要创建 HAProxy 配置文件，请单击“添加”。
      i. 在添加 **HAProxy** 配置文件对话框中，执行以下操作：



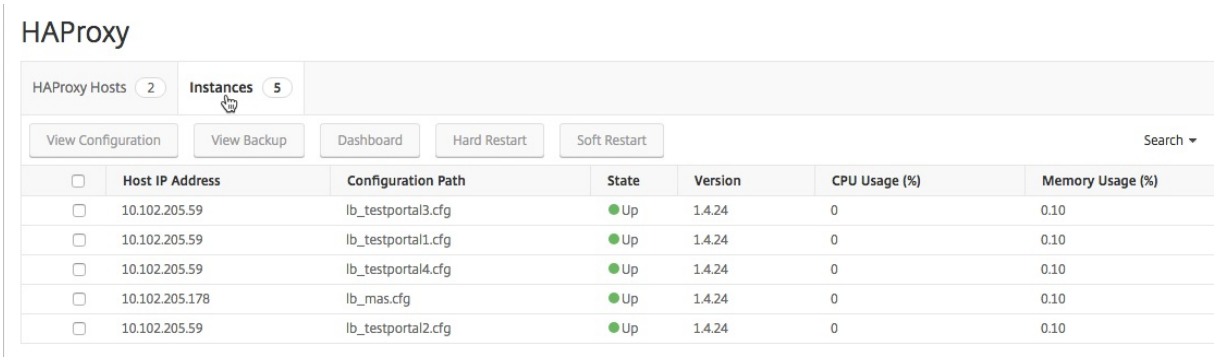
i. 在“配置文件名称”字段中，输入配置文件名称。

ii. 在“用户名”和“密码”字段中，输入主机的用户凭据。

iii. 单击创建。

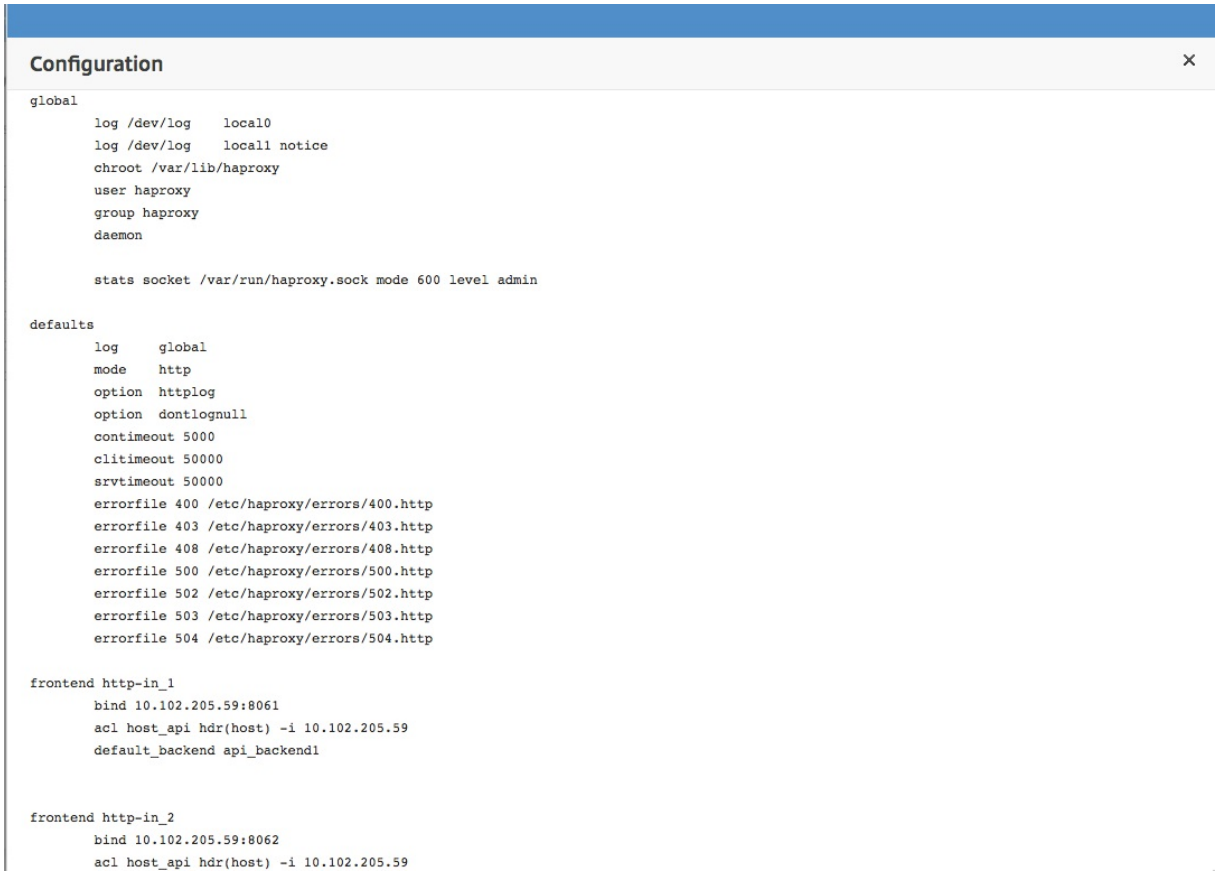
2. 从“站点”菜单中选择 HAProxy 站点。要创建新站点并将其添加到菜单中，请单击“添加”。
3. 从“** 代理”菜单中，选择一个代理。
4. 在“标签”字段中，相应地输入值。
5. 单击确定。

Citrix ADM 会发现在主机上预配置的 HAProxy 实例，您可以在“实例”选项卡上查看所有 HAProxy 实例。



查看 **HAProxy** 实例的配置

要查看 Citrix ADM 中 HAProxy 实例的配置，请导航到“网络”>“实 例”>“**HAProxy**”，然后在“实 例”选项卡上，选择 HAProxy 实例，然后单击“查看配置”。



HAProxy 应用程序控制板

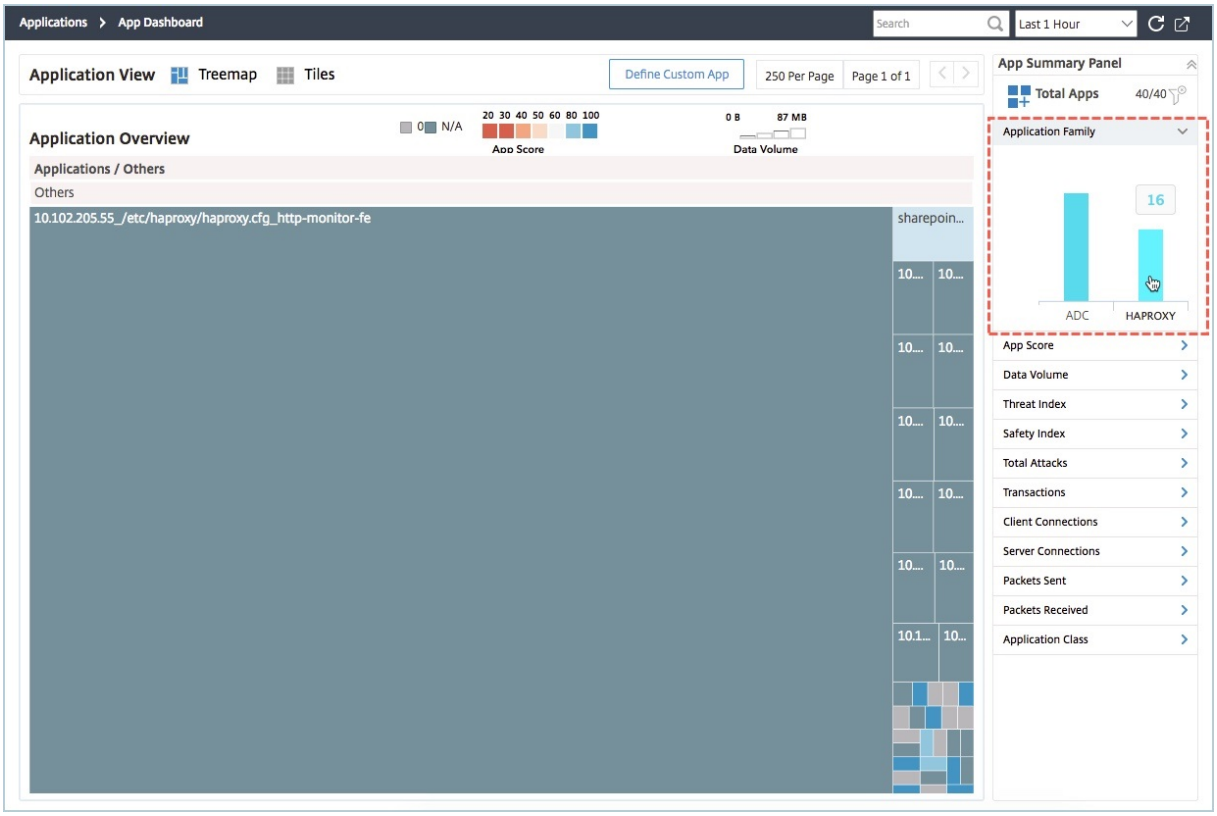
February 6, 2024

应用程序控制面板提供由 Citrix Application Delivery Management (Citrix ADM) 监视的所有 HAProxy 前端的实时统计信息。它将前端作为离散应用程序列出，并提供有关应用程序的事务、吞吐量和会话信息。

> 重要
>
> 确保在 HAProxy 实例配置文件中启用了 统计 信息。要启用 统计信息，请编辑 HAProxy 配置文件，然后在默认值部分之后添加一个类似于以下示例中的条目：

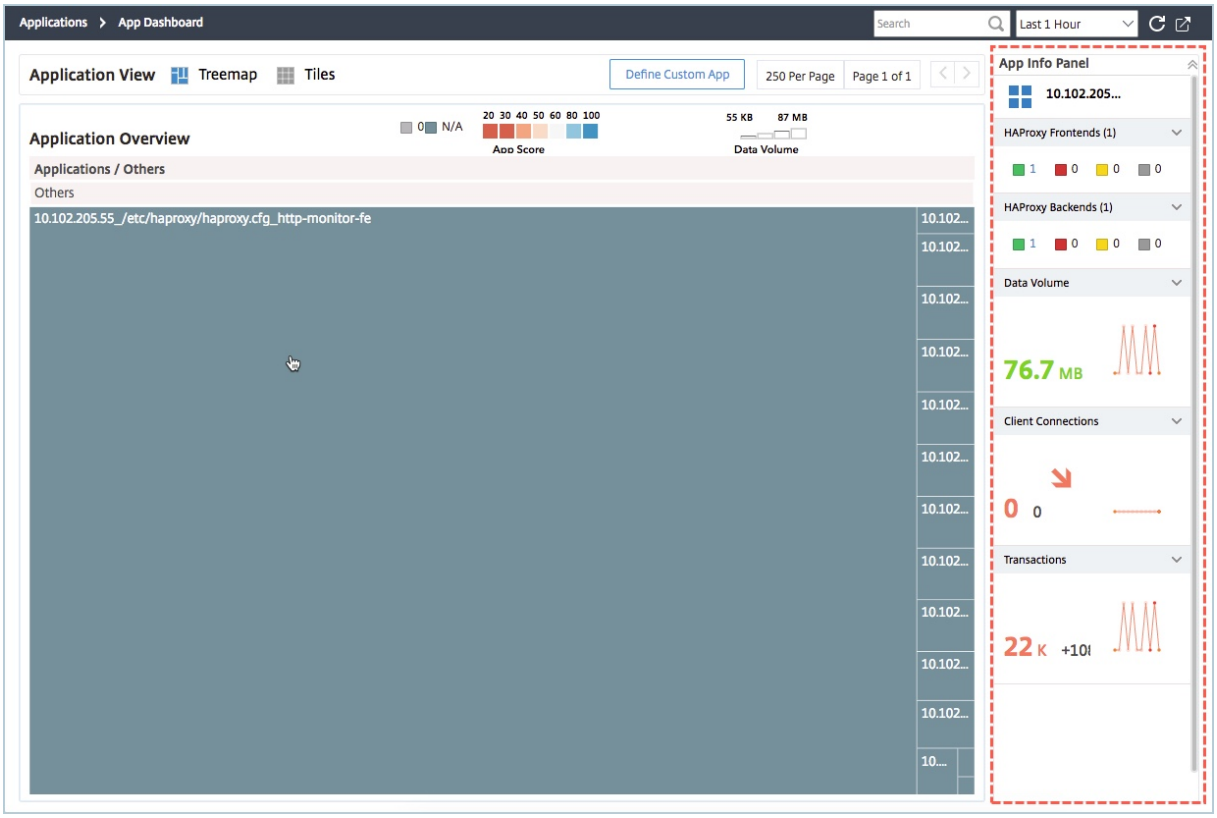
```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```


要访问 Citrix ADM 中应用程序控制板上的 HAProxy 应用程序，在将 HAProxy 实例添加到 Citrix ADM 后，请导航“应用程 序”>“控制板”。您可以筛选控制板以仅显示 HAProxy 应用程序，要筛选控制板，请选择“应用程序摘要信息面板”的“应用程 序系列”部分下显示的 **HAPROX** Y。



查看 **HAProxy** 应用程序的关键指标

向下钻取 HAProxy 应用程序时，“应用程序信息”面板位于第一级。该面板显示应用程序的主要指标和组件，以及其状态。例如，对于任何选定的 HAProxy 应用程序，“应用程序信息”面板会显示 HAProxy 前端总数、HAProxy 后端总数、数据量、客户端连接趋势以及事务记录。要查看 HAProxy 应用程序的关键指标，请单击应用程序控制板上的 HAProxy 应用程序图块。“App Info Panel”（应用程序信息面板）随后将替换“App Summary Panel”（应用程序摘要面板）。

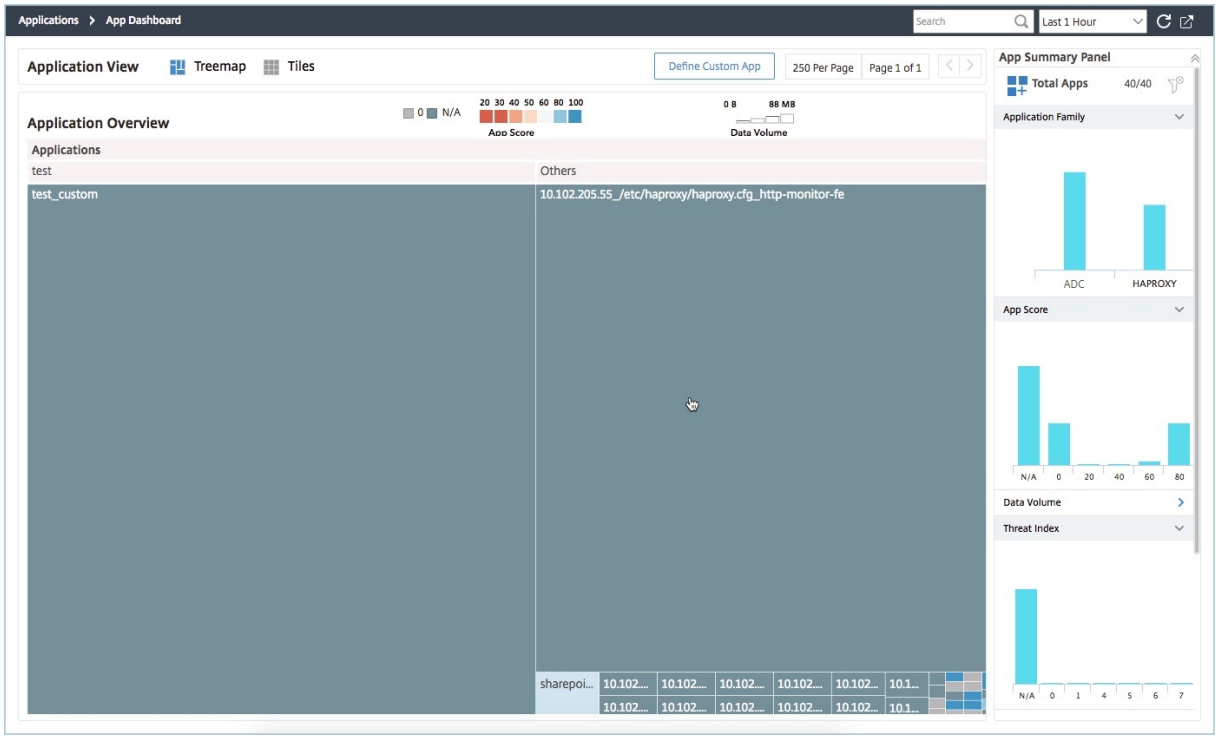


查看 **HAProxy** 应用程序的实时性能

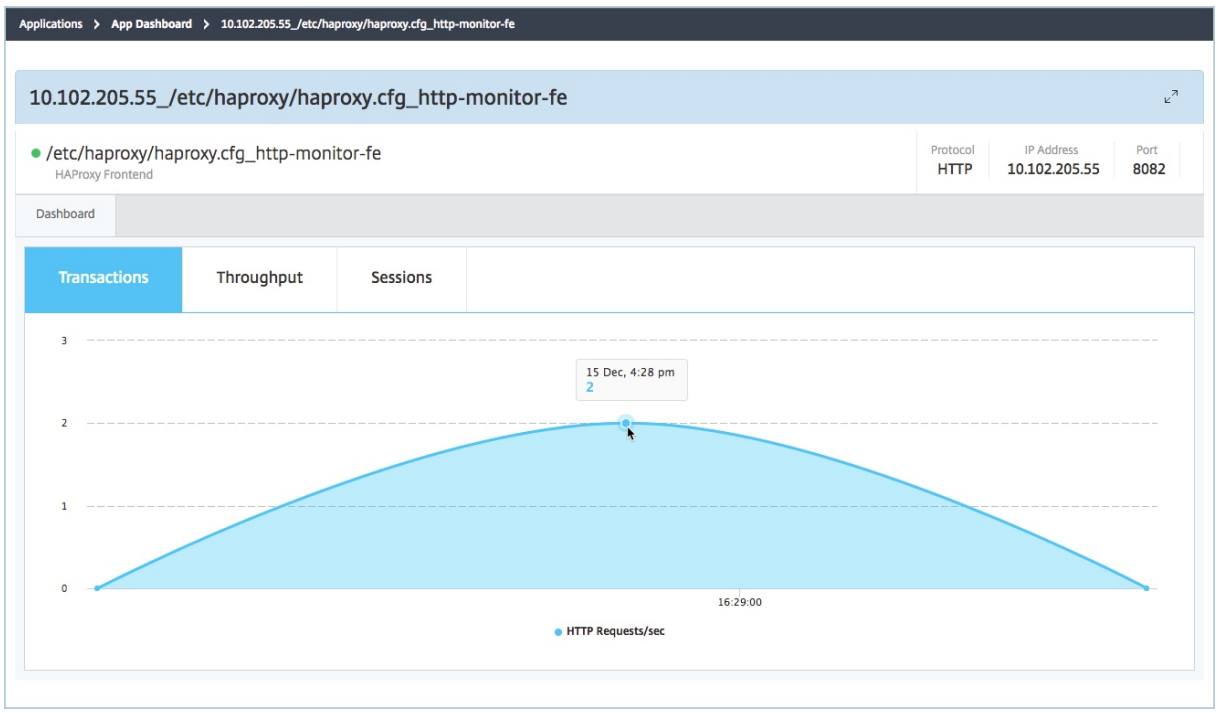
通过 Citrix ADM，您可以查看 HAProxy 应用程序的实时性能。它提供了所选 HAProxy 应用程序的以下实时详细信息：

- 事务。应用程序执行的事务。
- 吞吐量。应用程序的吞吐量。
- 会话。应用程序建立的会话数。

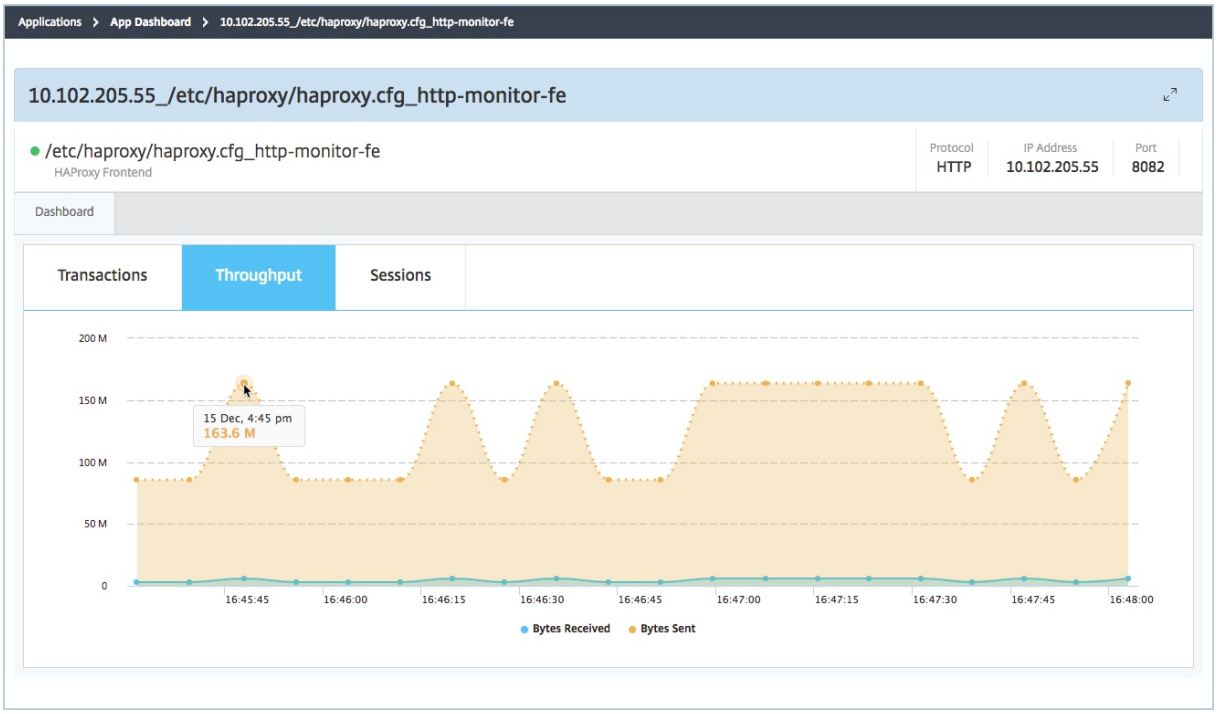
要查看 HAProxy 应用程序的实时性能，请在应 用程序控制板上双击 HAProxy 应用程序磁贴。



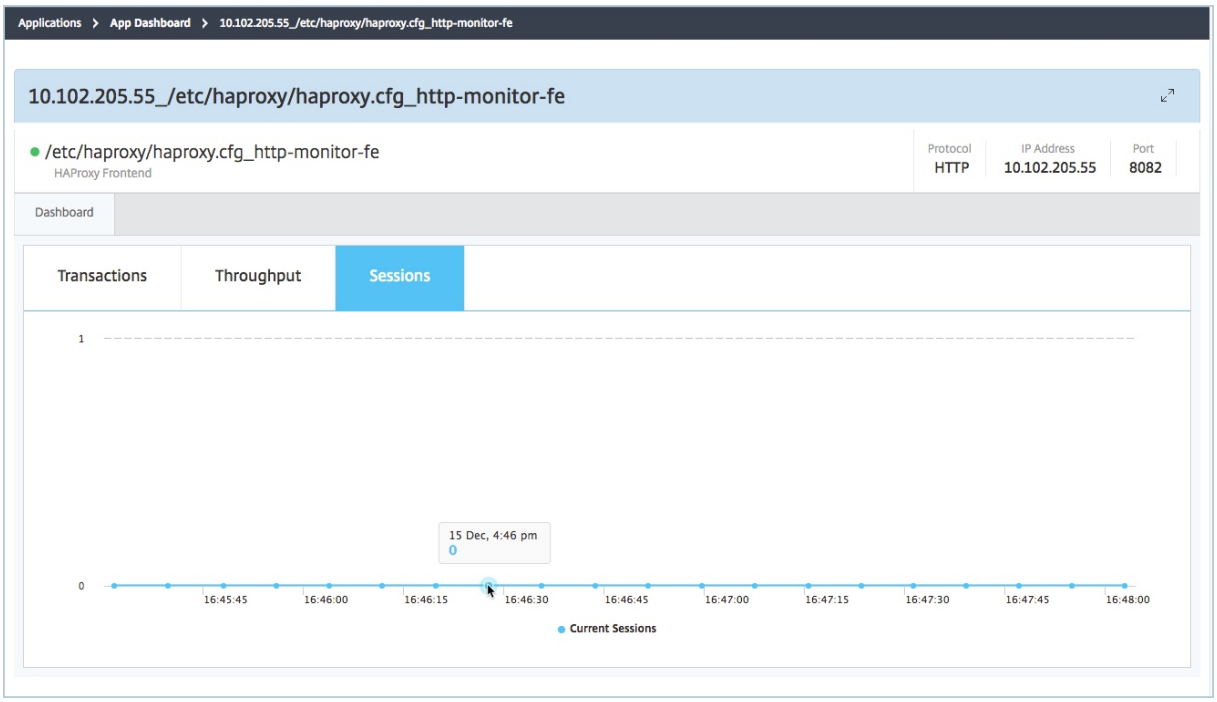
默认情况下，“事 务处理”选项卡处 于选中状态，并显示应用程序执行的实时事务处理。



要查看应用程序的实时吞吐量，请单击 吞吐量 选项卡。



您可以单击“会 话”选项卡以查看应用程序实时建立的会话数。

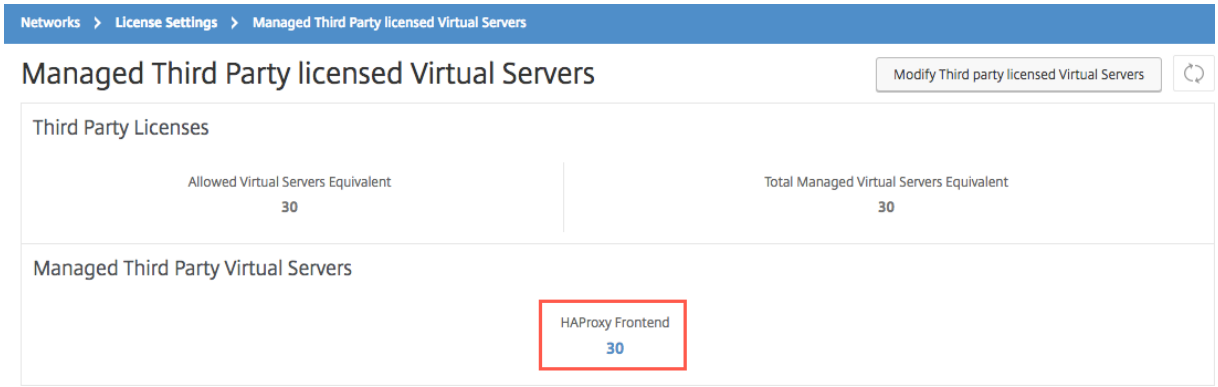


第三方许可

February 6, 2024

将主机添加到 Citrix Application Delivery Management (Citrix ADM) 后，Citrix ADM 会自动发现在主机上置备的 HAProxy 实例并将其添加到 Citrix ADM 清单中。它还会发现 HAProxy 实例上配置的所有前端、后端和服务器，并将前端视为发现的应用程序。

您可以管理和监视所有发现的应用程序，但默认情况下，“HAProxy App Dashboard”（HAProxy 应用程序控制板）显示 30 个发现的应用程序的应用程序统计信息。有关“HAProxy App Dashboard”（HAProxy 应用程序控制板）的详细信息，请参阅“HAProxy App Dashboard（HAProxy 应用程序控制板）”。如果要查看 30 个以上发现的应用程序的应用程序统计信息，需要购买单独的许可证。



在数量为 100 的虚拟服务器包中提供用于额外前端的许可证。您可以使用 Citrix ADM GUI 获取有效的许可证并安装许可证。

安装第三方许可证

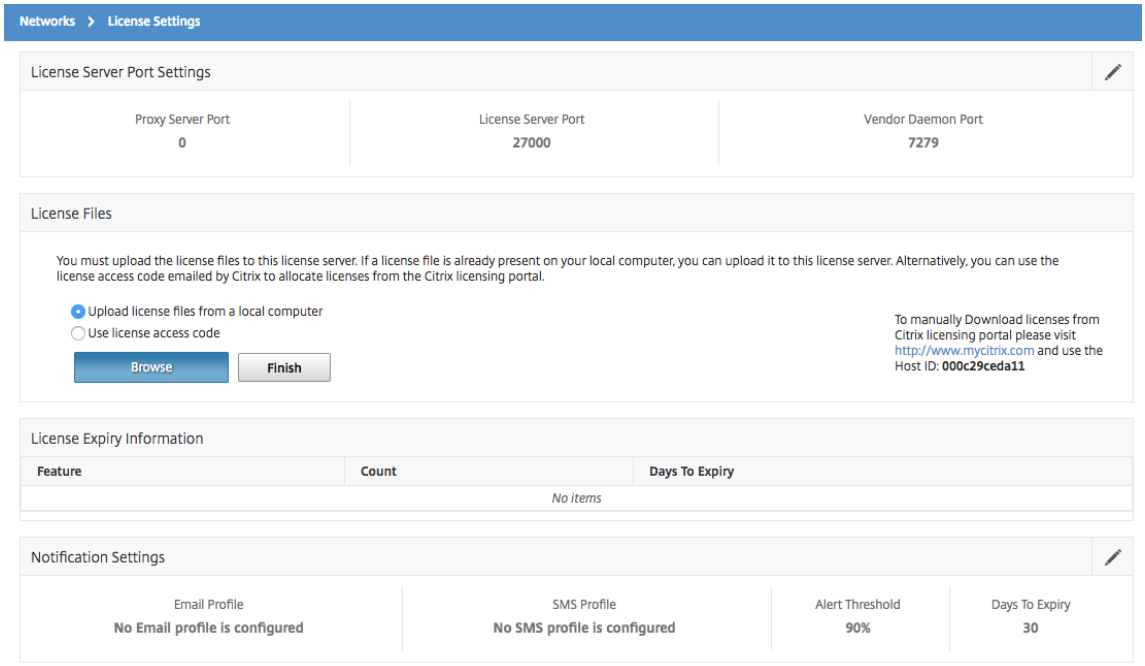
您可以在 Citrix ADM 上安装许可证，以查看 30 多个发现的应用程序的应用程序统计信息。

要安装许可证，请执行以下操作：

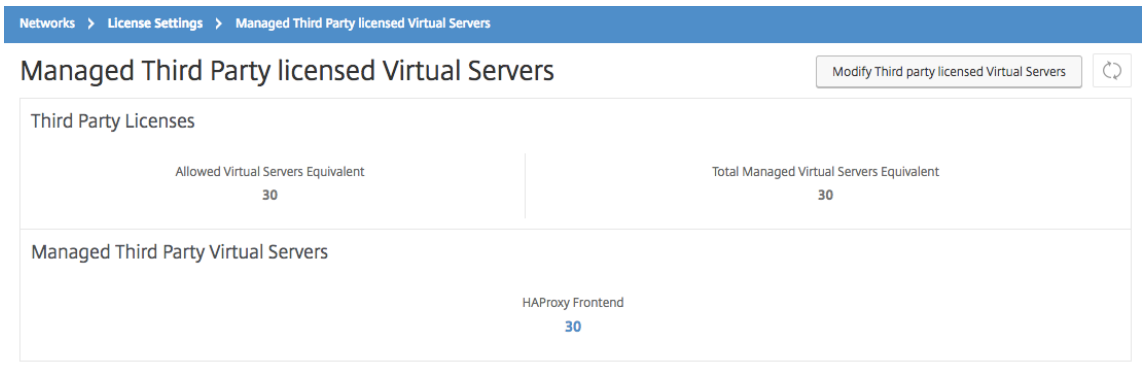
1. 在 Web 浏览器中，键入 **NetScaler Management and Analytics System** 的 IP 地址（例如 http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到“网络”>“许可证”。
4. 在“许可证文件”部分中，选择以下选项之一：
    - 从本地计算机上载许可证文件。如果您的本地计算机上已经有许可证，请单击“Browse”（浏览）并选择要用于分配您的许可证的许可证文件 (.lic)。单击完成。

- **Use License Activation Code**（使用许可证激活代码）- Citrix 将通过电子邮件发送您购买的许可证的 LAC。在文本框中输入 LAC，然后单击 **Get Licenses**（获取许可证）。

> 注意
>
> 如果选择此选项，NetScaler Management and Analytics System 必须连接到 Internet，或者必须有代理服务器。



您可以通过导航到“网络”>“许可证”>“第三方许可证”来验证 **Citrix ADM** 上安装的许可证。

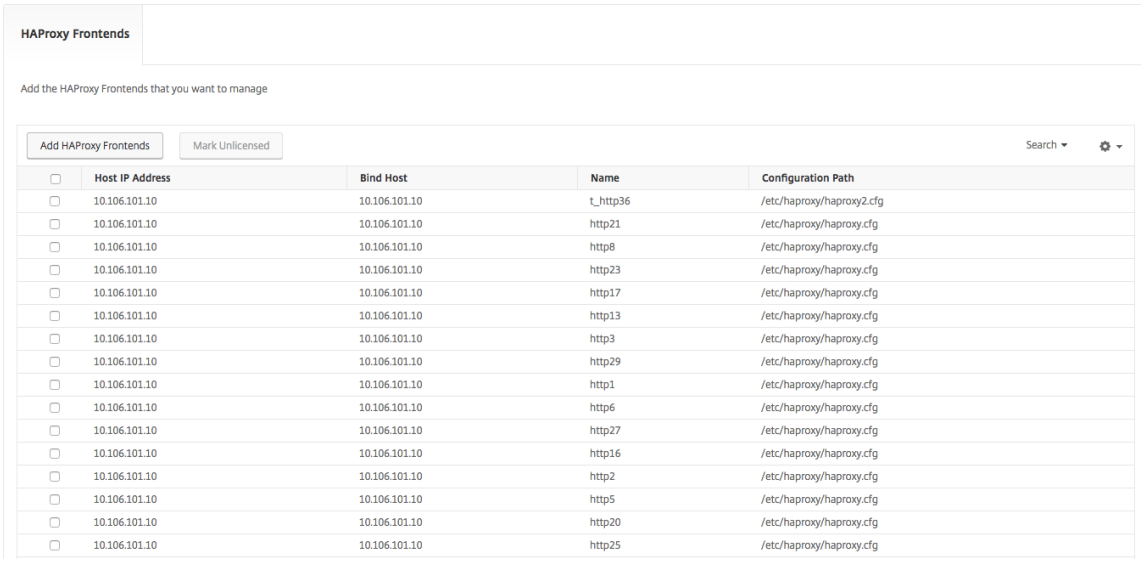


管理第三方许可证

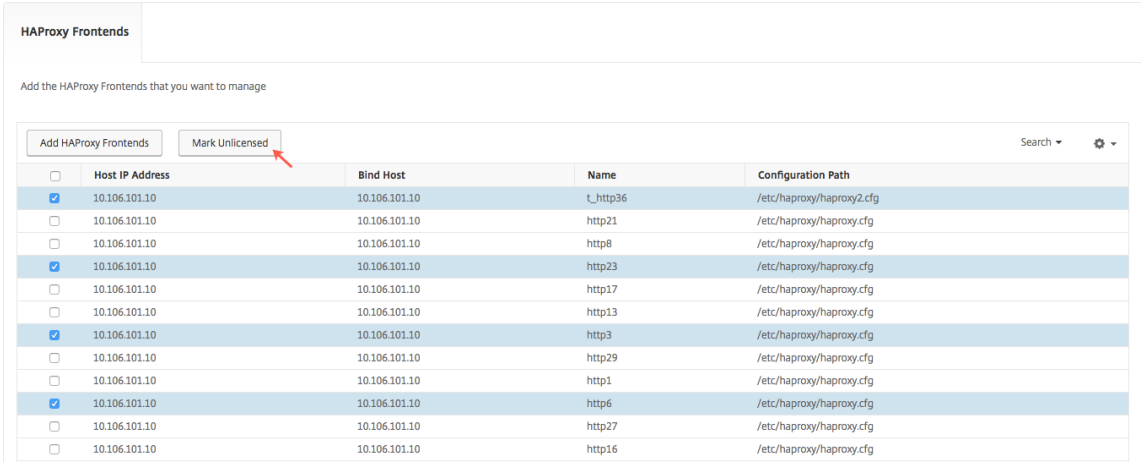
Citrix ADM 会随机选择 HAProxy 实例中发现的应用程序，并自动对其进行许可。如果您要更改选定的发现应用程序，您需要手动取消许可已许可的发现应用程序，然后将许可证分配给您要许可的发现应用程序。

要管理第三方许可证，请执行以下操作：

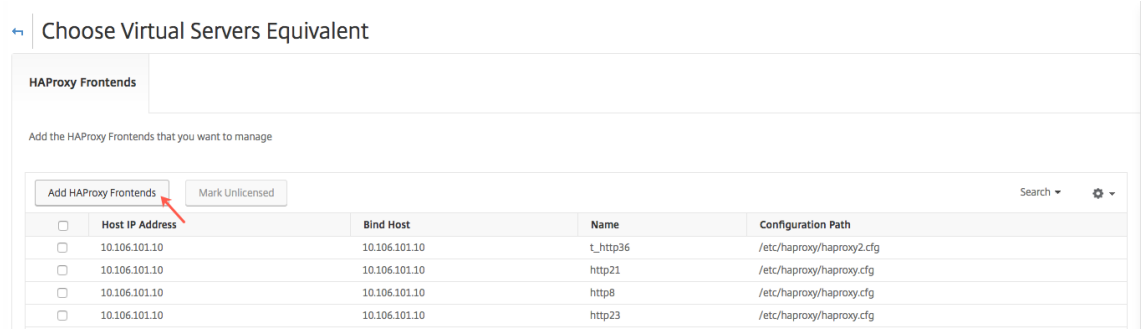
1. 导航到 网络 > 许可证 > 第三方许可证，然后单击 修改第三方许可证的虚拟服务器。控制板将显示托管的前端。



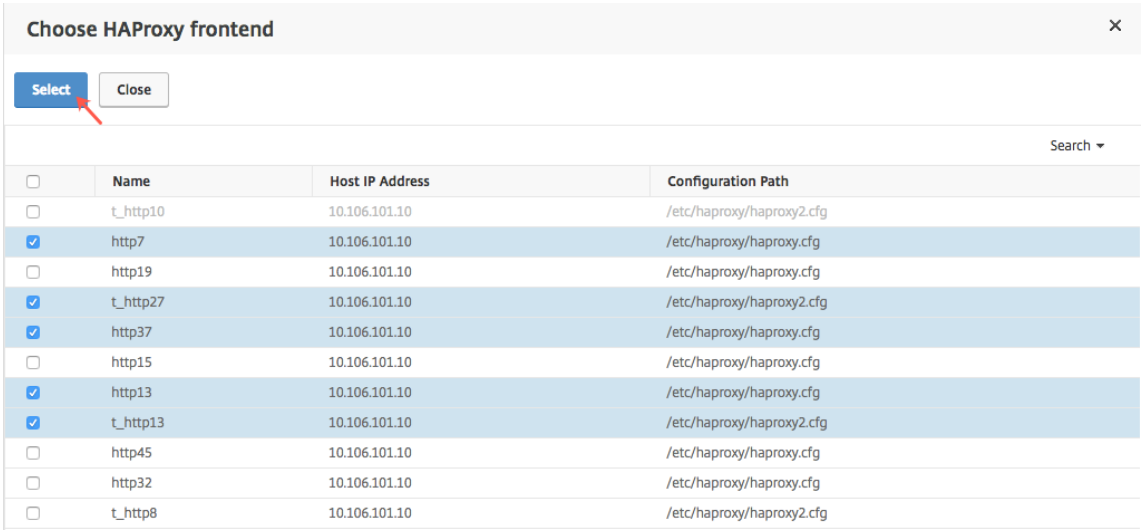
2. 从列表中选择前端，标记为未许可，然后单击“完成”以释放许可证。



3. 释放许可证后，或者如果您已有可用的许可证，请单击 添加 **HAProxy** 前端。



4. 在“选择 **HAProxy** 前端”对话框中，从列表中选择未经许可的前端，然后单击“选择”。



5. 单击“立即完成”。

HAProxy 实例的基于角色的访问控制

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 使用精细的基于角色的访问控制 (RBAC) 来控制对配置对象的访问。例如，您可以创建用户并为其提供对特定 HAProxy 实例的访问权限，以及可以指定针对“HAProxy App Dashboard”（HAProxy 应用程序控制板）的查看/只读权限。有关详细信息，请参阅 Citrix ADM 中的基于角色的访问控制。

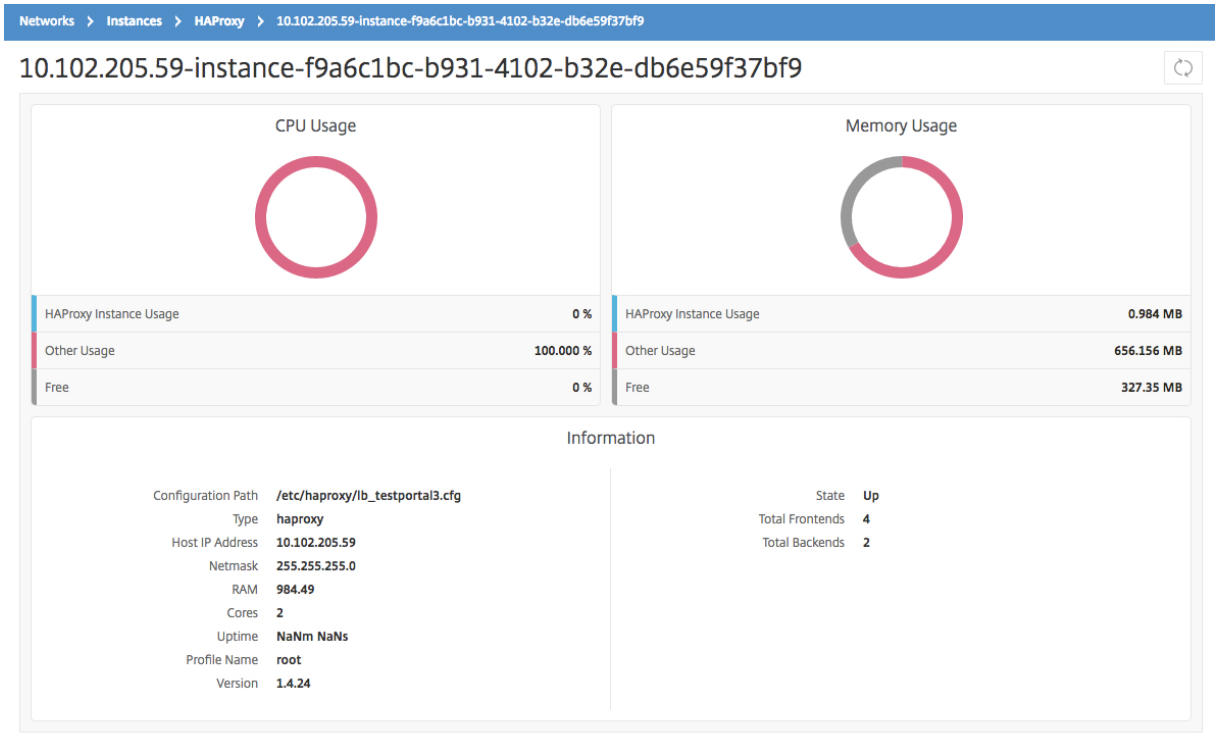
监视 HAProxy 实例

February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 中的 HAProxy 控制板显示有助于跟踪 HAProxy 实例的 CPU 和内存使用情况的图形。该控制板还显示指示以下信息的图形：

- 主机上的 HAProxy 实例使用的 CPU 的百分比。
- 主机上的其他实体使用的 CPU 的百分比。
- 主机上剩余的 CPU 的百分比。
- 主机上的 HAProxy 实例使用的内存的百分比。
- 主机上的其他实体使用的内存的百分比。
- 主机上剩余的内存的百分比。

要监视 Citrix ADM 中的 HAProxy 实例，请导航到 网络 > 实 例 > **HAProxy** > 实 例 选项卡，选择 HAProxy 实例，然后单击 控制板。



查看在 **HAProxy** 实例上配置的前端的详细信息

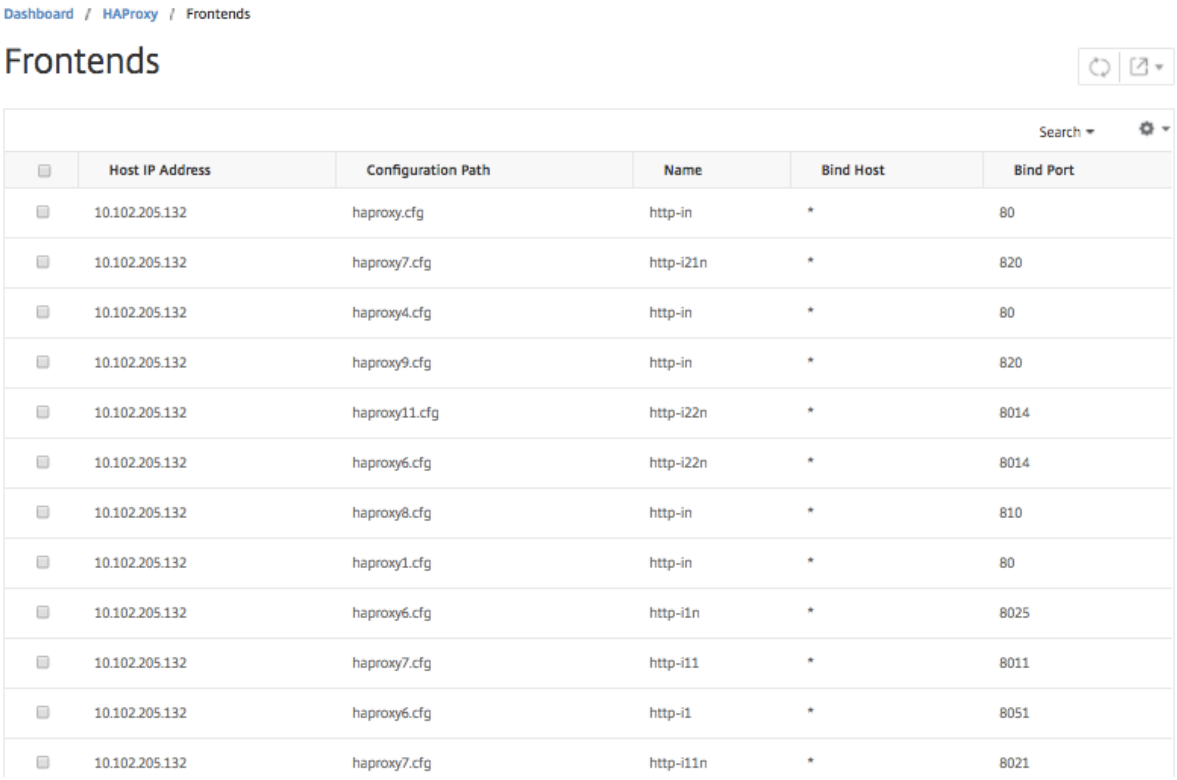
February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的前端的以下详细信息：

- 主机 **IP** 地址。主机的 IP 地址
- 配置路径。主机上 HAProxy 实例的绝对配置路径。
- 名称。处理传入流量的前端的名称。
- 绑定主机。前端绑定到的 IP 地址。
- 绑定端口。前端绑定到的端口。

要查看 **HAProxy** 实例上配置的前端，请执行以下操作：

在 Citrix ADM 中，导航到“网 络” **>** “网络功能” **>** “**HAProxy**” **>** “前端”。



查看在 **HAProxy** 实例上配置的后端的详细信息

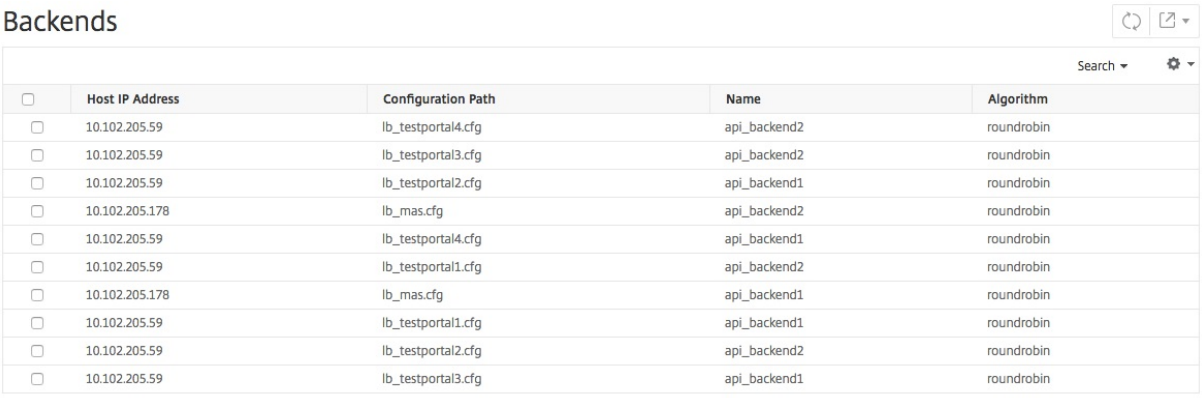
February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的后端应用程序的以下详细信息：

- 主机 **IP** 地址。主机的 IP 地址。
- 配置路径。主机上的 HAProxy 实例路径。
- 名称。流量转发到的后端的名称。
- 算法。用于平衡流量的负载平衡算法。

要查看 **HAProxy** 实例上配置的后端，请执行以下操作：

在 Citrix ADM 中，导航到“网 络”>“网络功能”>“**HAProxy**”>“后端”。



查看在 **HAProxy** 实例上配置的服务器的详细信息

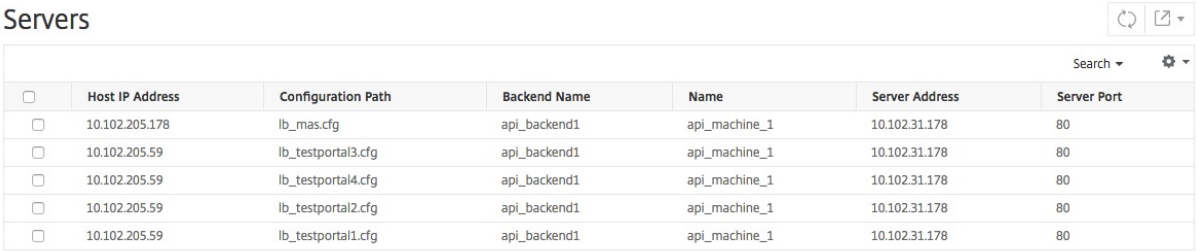
February 6, 2024

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的服务器的以下详细信息：

- 主机 **IP** 地址。主机的名称。
- 配置路径。主机上的 HAProxy 实例配置文件的绝对路径。
- 后端名称。HAProxy 配置中后端的名称。
- 名称。HAProxy 配置中服务器的名称。
- 服务器地址。服务器的 IP 地址。
- 服务器端口。服务器所使用的端口。

要查看 **HAProxy** 实例上配置的服务器，请执行以下操作：

在 Citrix ADM 中，导航到“网 络” **>** “网络功能” > “**HAProxy**” > “服务器”。

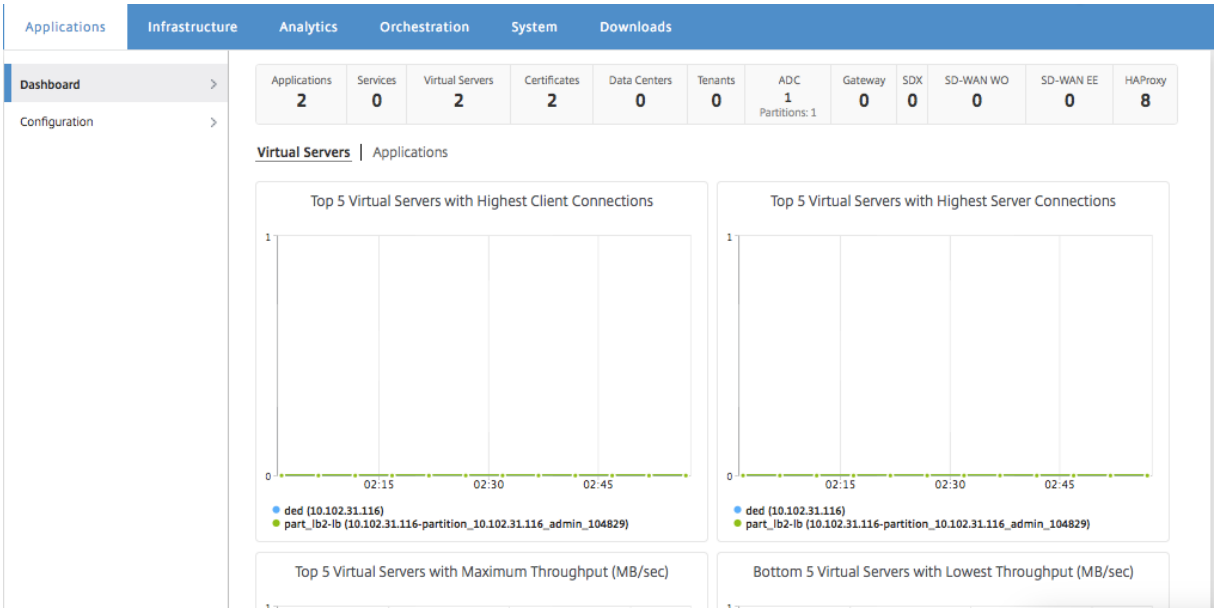


查看具有最多前端或服务器数量的 **HAProxy** 实例

February 6, 2024

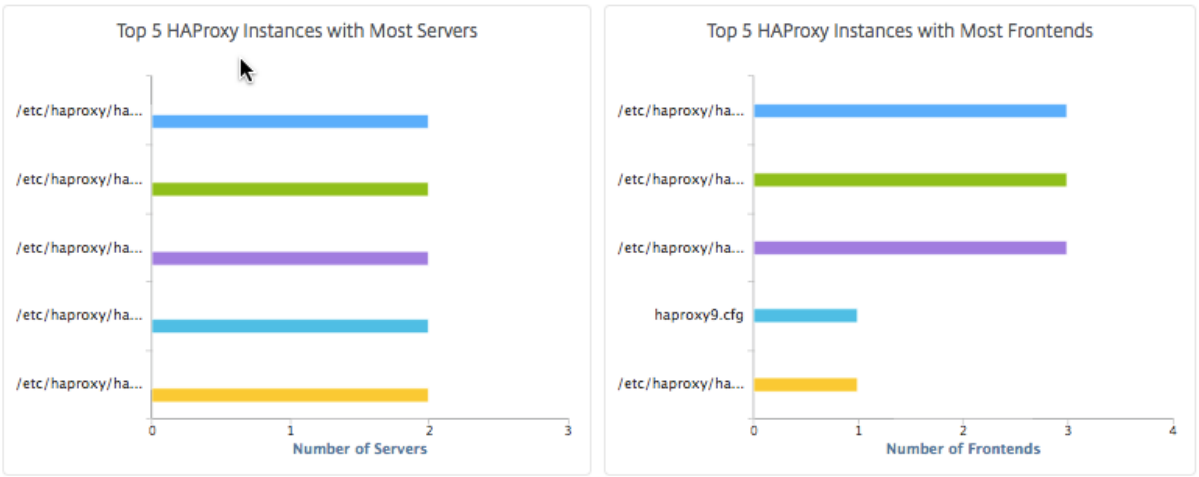
在应用程序控制板上，Citrix Application Delivery Management (Citrix ADM) 显示它发现的 HAProxy 实例数，并列出了配置了最多前端或服务器数量的前五个 HAProxy 实例。

要查看应用程序控制板，请在 Citrix ADM 中导航至“应用程 序”>“控制板”。



Citrix ADM 发现的 HAProxy 实例数显示在顶行中，如下所示：

要查看配置的前端数或服务器数排在前五位的 HAProxy 实例列表，请向下滚动控制板：



重新启动 **HAProxy** 实例

February 6, 2024

要从 Citrix Application Delivery Management (Citrix ADM) GUI 重新启动 HAProxy 实例，可以选择硬重新启动或软重新启动。

硬重启

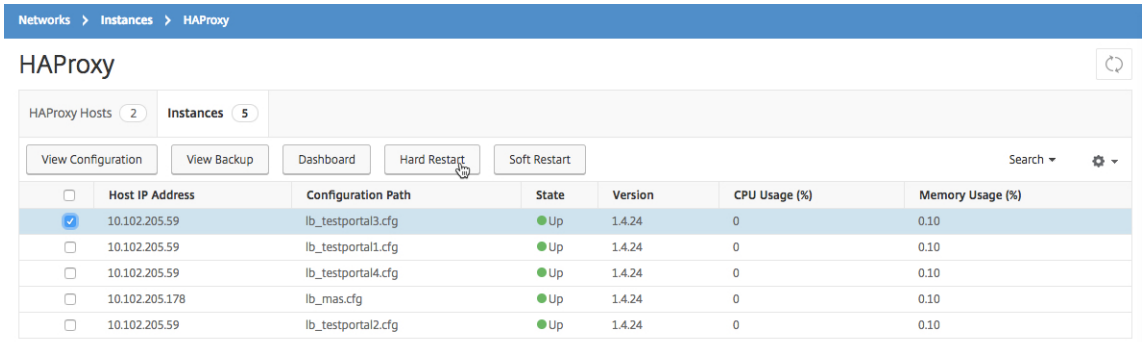
硬重新启动将终止实例上的 HAProxy 进程并关闭所有已建立的连接。重新启动后，将建立新 HAProxy 进程，且后续新连接由新 HAProxy 进程处理。

软重启

软重新启动将取消 HAProxy 进程与侦听端口的绑定，但 HAProxy 进程会继续处理现有连接直到其关闭。将创建新 HAProxy 进程来处理新连接。

要重新启动 **HAProxy** 实例，请执行以下操作：

1. 导航到“网络”>“实例”>“**HAProxy**”，然后单击“实例”选项卡。
2. 在 实例 选项卡上，选择要重新启动的 HAProxy 实例。
3. 单击 硬重新启动 硬重新启动 HAProxy 实例，或单击 软重新启动 软重新启动 HAProxy 实例。



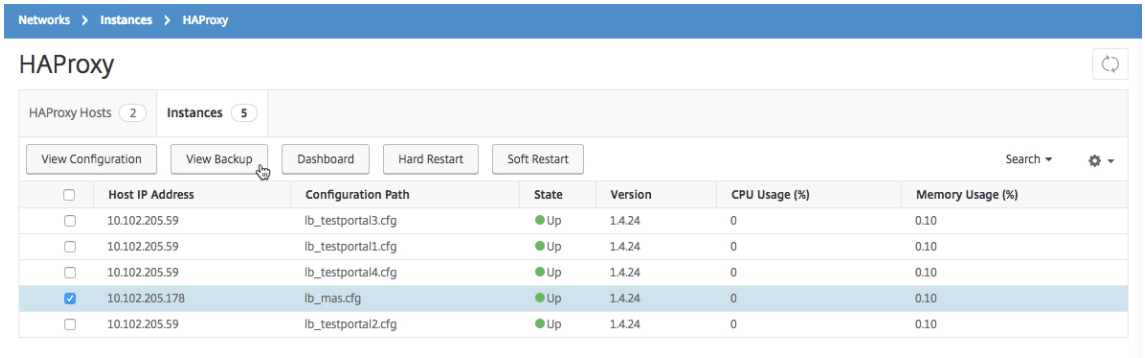
备份和还原 **HAProxy** 实例

February 6, 2024

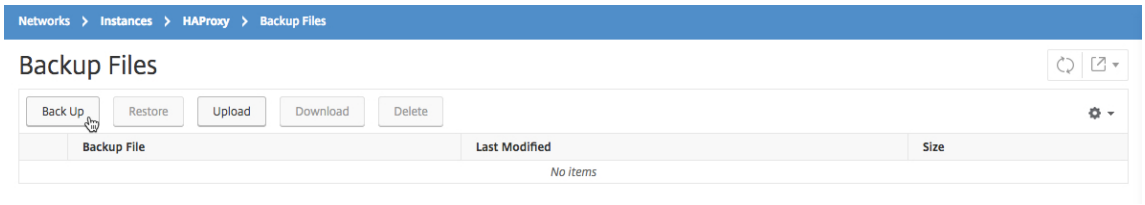
可以在 HAProxy 配置文件中备份 HAProxy 实例的当前状态。如果实例变得不稳定，可以使用备份文件将实例还原到稳定状态。

要使用 **Citrix ADM** 备份 **HAProxy** 实例，请执行以下操作：

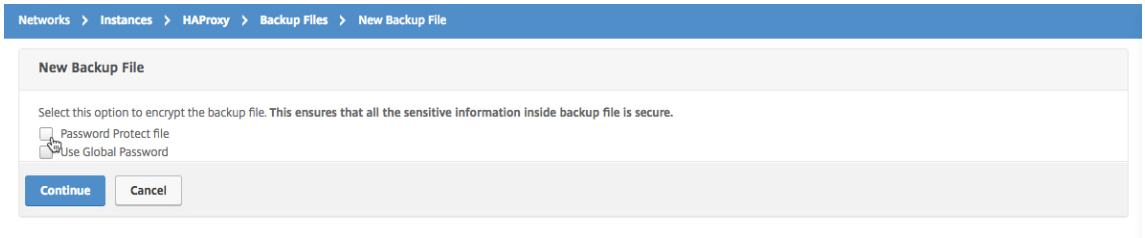
1. 在 Citrix Application Delivery Management (Citrix ADM) 中，导航到“网络” **>** “实例” **>** “**HAProxy**”。
2. 在 **HAProxy** 页面中，单击实 例 选项卡。
3. 选择要备份的 HAProxy 实例，然后单击 查看备份。



4. 在“备份文件”页面上，单击“备 份”。



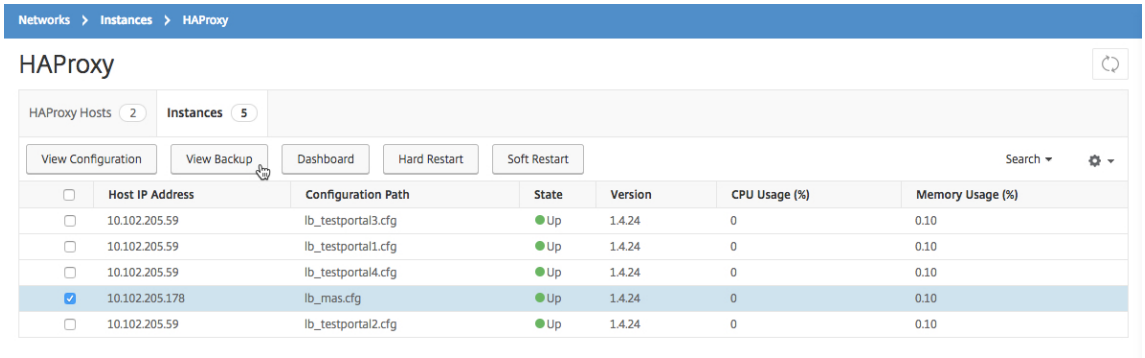
5. 可以选择为备份文件加密以增加安全性。



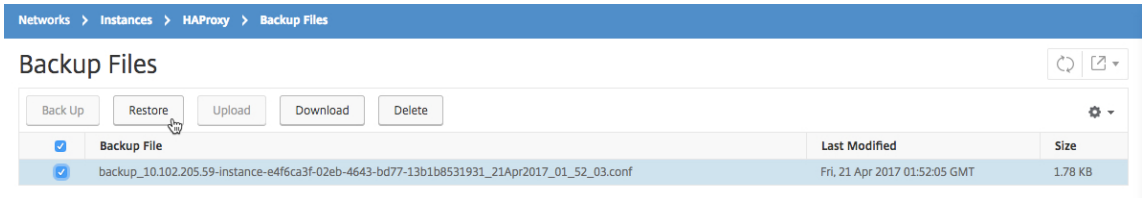
6. 单击继续。

要使用 **Citrix ADM** 还原实例，请执行以下操作：

1. 导航到“网络” > “实例” > “**HAProxy**”。
2. 在 **HAProxy** 页面上，单击实 例 选项卡。
3. 选择要还原的实例，然后单击 查看备份。



4. 在 **Backup Files**（备份文件）页面上，选择要还原的备份文件，然后单击 **Restore**（还原）。



> 注意
>
> 恢复实例时，Citrix ADM 软重新启动 HAProxy 实例。

编辑 **HAProxy** 配置文件

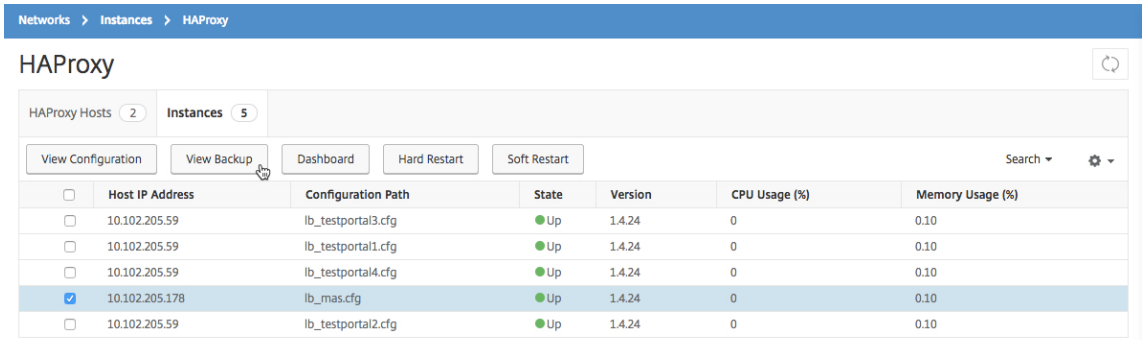
February 6, 2024

您可以在现有 HAProxy 配置文件中更新前端、后端、服务器及其他设置。要编辑 HAProxy 配置文件，请执行以下操作：

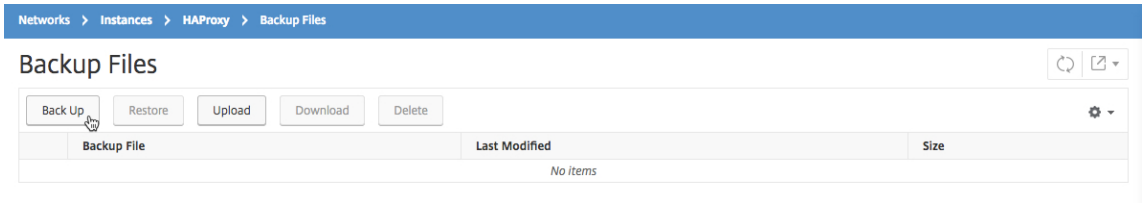
- 备份 HAProxy 配置文件。
- 下载备份 HAProxy 配置文件，然后对其进行脱机编辑。
- 将更新后的 HAProxy 配置文件上载到 Citrix Application Delivery Management (Citrix ADM)
- 使用更新的备份文件还原 HAProxy 实例。

要使用 **Citrix ADM** 编辑 **HAProxy** 配置文件，请执行以下操作：

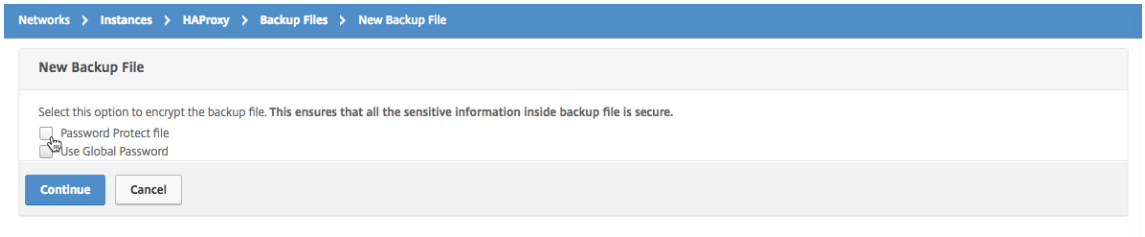
1. 在 Citrix ADM 中，导航到“网络”>“实例”>“**HAProxy**”。
2. 在 **HAProxy** 页面上，单击实 例 选项卡。
3. 选择要备份的 HAProxy 实例，然后单击 查看备份。



4. 在 **Backup Files**（备份文件）页面上，单击 **Back Up**（备份）。

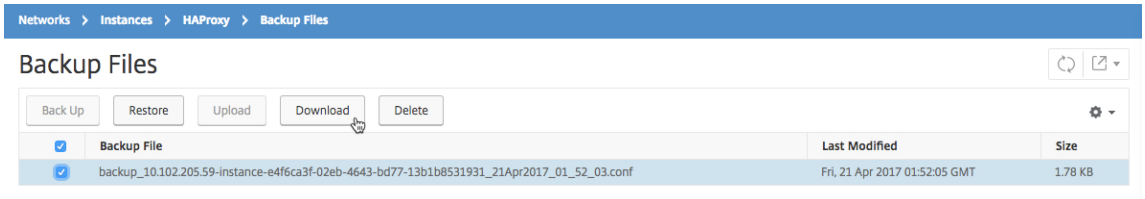


5. 单击继续。

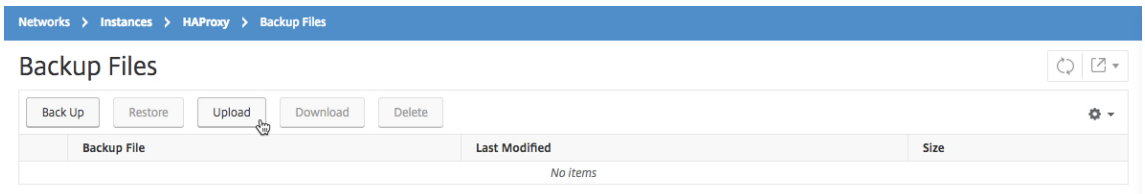


> 注意
>
> 请勿加密备份文件。

6. 在“备份文件”页面上，选择备份文件，然后单击“下载”。



7. 使用文本编辑器，编辑 HAProxy 配置文件。
8. 在“备份文件”页面上，单击“上载”浏览并选择更新后的 HAProxy 配置文件。



上载更新的 HAProxy 配置文件后，它将列在“备份文件”页面上。

9. 选择更新后的 HAProxy 配置文件，然后单击 恢复。

管理系统设置

February 6, 2024

下表描述了如何在 Citrix ADM 上配置系统设置。

| 如果您想…| 做这个…|
|————————————————————————————————|————————————————————————————————————
-|
| 配置当日消息 | 现在，您可以在 Citrix ADM 中创建欢迎消息。您可以使用此功能为自己或登录到 Citrix ADM 的用户设置提醒消息。导航到“系 ** 统 **” > “系 ** 统设 ** 置”，然后单击“配置 ** 当日 ** 消息”。单击“启 ** 用消息 **”，在消息框中键入消息，然后单击“**** 确定”。|
| 关闭 Citrix ADM| 导航到 **System**（系统）> **System Administration**（系统管理）。您可以单击“关 ** 闭 Citrix ADM**”以完全关闭 Citrix ADM。** 注 ** 意 关闭 Citrix ADM 后，只能从安装了 Citrix ADM 的虚拟机管理程序重新启动 Citrix ADM。|
| 配置设置向导设置 | 导航到 **System**（系统）> **System Administration**（系统管理）。在“** 设置 Citrix ADM**”下，选择安 ** 装向导设 ** 置。您可以选择 **Citrix ADM 网络 ** 选项来修改网络设置，例如 Citrix ADM 的 IP 地址及其密码。您可以单击“系 ** 统 ** 设置”来修改主机名、与实例的通信模式或本地时区。|
| 配置网络设置 | 导航到 **System**（系统）> **System Administration**（系统管理）。在“** 设置 Citrix ADM**”下，选择“网 ** 络 ** 配置”。GUI 显示安装在 Citrix ADM 上的 SSL 证书和密钥。|
| 查看 SSL 证书 | 导航到 **System**（系统）> **System Administration**（系统管理）。在“** 设置 Citrix ADM**”下，选择 查 ** 看 SSL 证 ** 书。GUI 显示安装在 Citrix ADM 上的 SSL 证书和密钥。|
| 更改时区 | 导航到“系 ** 统 **” > “系 ** 统 ** 管理”。在“系 ** 统设 ** 置”下，选择“更 ** 改时区 **”。从 时 ** 区 ** 下拉列表中，选择您的 Citrix ADM 设备时钟的时区。|
| 更改主机名 | 导航到 **System**（系统）> **System Administration**（系统管理）。在 **System Settings**（系统设置）下方，选择 **Change Hostname**（更改主机名）。输入用于识别您的 Citrix ADM 的主机名，这样，当您为 Citrix ADM Gateway 生成通用许可时，该主机名就会显示在许可中。|
| 更改系统设置 | 导航到“系 ** 统 **” > “系 ** 统 ** 管理”。在“系 ** 统设 ** 置”下，选择“更 ** 改系统设 ** 置”。然后，选中或清除复选框以启用或禁用以下功能- 仅限 Secure Access、启用会话超时、允许基本身份验证、启用 nsrecover 登录、启用证书下载、为非 nsroot 用户启用 Shell 访问权限、提示用户提供实例登录凭据 |
| 配置 SSL 设置 | 导航到 **System**（系统）> **System Administration**（系统管理）。在“系 ** 统设 ** 置”下，选择“配置 **SSL** 设置”以显示当前协议设置和应用的密码套件。如果要修改任何设置，请在“编辑设置”下选择“协议 **** 设 **** 置”或“密 ** 码 ** 套件”。|
| 启用用户体验改善设置功能 | 导航到 **System**（系统）> **System Administration**（系统管理）。在“系 ** 统设 ** 置”下，选择“配置用 ** 户体验改善设 ** 置”，然后选中“启用 **CUXIP**”复选框。如果选中此复选框，则

收集使用情况统计信息的唯一目的是 改善图形用户界面。接收到的数据仅供 Citrix 工程师使用，不与任何人共享。|
升级 Citrix ADM	导航到 **System**（系统）> **System Administration**（系统管理）。在“** 系统管理 **”副标题下，选择“** 升级 Citrix ADM**”，然后选择新的映像文件。您可以选择 Citrix ADM 虚 拟 设备上已有的文件，也可以从本地计算机上载文件。
重启 Citrix ADM	导航到 **System**（系统）> **System Administration**（系统管理）。在“系 ** 统 ** 管理”副标题下，选择重 ** 启 Citrix ADM**。此时将显示一个要求您确认操作的对话框。单击 ** 是 **。
配置系统删除设置（用于删除旧数据）	导航到 **System**（系统）> **System Administration**（系统管理）。在“** 删除设 ** 置”下，选择“系 ** 统清理设 ** 置”。在 Data to keep (days)（保留数据 (天数)）字段中，输入数据在系统中保留的天数。
配置系统备份设置	导航到 **System**（系统）> **System Administration**（系统管理）。在“备份 ** 设 ** 置”下，选择“系 ** 统备份设 ** 置”，然后输入 要在 Citrix ADM 设备上保留的系统备 份数量。您也可以选择加密备份文件，也可以指定将它们传输到的外部位置。可以在系统上保留或删除传输的备份文件。
配置实例备份设置	导航到 **System**（系统）> **System Administration**（系统管理）。在“备份 ** 设 ** 置”下，选择 实例备份 ** 设 ** 置，然后输入创建备份 Citrix ADM 管理的所有实例的备份文件的时间间隔（以小时为单位）。您可以指定要保留的备份文件数量，以及是否对 其进行加密，这样没有密码就无法访问 它们。
查看系统统计信息	导航到“** 系统”> “统 **** 计信息 **”。一个折线图显示 CPU 使用情况、内存使用情况及磁盘使用情况之类的信息。
查看和管理会话	导航到“系 ** 统 **” > “**** 会话”。之后可以查看所有活动会话及详细信息。要终止会话，请选中其复选框并单击“** 取 ** 消会话”。
添加或修改租户	导航到“系 ** 统 **” > “** 租 ** 户”，然后添加新租户或编辑现有租户的设置。可以提供其他信息，例如，租户的组织单位名称、部门和 URL。
更改用户锁定策略	导航到“系 ** 统 **” > “用 ** 户管 ** 理”。在“用 ** 户 ** 配置”下，选择“用户 ** 锁 ** 定配置”，然后选中“启用用 ** 户锁 ** 定”复选框。您可以指定用户在禁用其帐户 之前可以 进行的无效尝试次数，以及用户锁定政策的有效期限。
更改密码复杂性	导航到“系 ** 统 **” > “用 ** 户管 ** 理”。在“用 ** 户 ** 配置”下，选择“密 ** 码策 ** 略”，然后选中“启用密码复 ** 杂 ** 性”复 选框。在“最小密码 ** 长 ** 度”字段中，输入 Citrix ADM 密码所需的最小 字符数。
添加或修改用户	导航到“系 ** 统 **” > “用 ** 户管 ** 理” > “用户”。在“用户”下，添加新用户或编辑现有用户的设置。添加用户时，您可以启用外部 身 份验证、会话超时以及将用户分配到特定组等选项。
添加或修改用户组	导航到“系 ** 统 **” > “用 ** 户管 ** 理” > “组 ****”。在“组 ****” 下，添加新组或 编辑现有组的设置。添加组时，您可以启用诸如为组分配权限、配置会话超时、向组分配用户以及允许访问 Citrix ADM 上的 特定 或所有应用程序等选项。
更改身份验证配置	导航到“系 ** 统 **” > “身份验 ** 证 **” > “身份验 ** 证 **”。在“身份验 ** 证 **” 下，选择“身份验 ** 证 ** 配置”，然 后 选择身份验证服务器的类型。
添加或修改 RADIUS 服务器	导航到 系 ** 统 ** > 身份验 ** 证 ** > **RADIUS**。在 **RADIUS** 下，添加新的 RADIUS 服务器或通过输入 或修改网络参数来编辑现有 RADIUS 服务器的设置。
添加或修改 LDAP 服务器	导航到 System（系统）> Authentication（身份验证）> LDAP。在 LDAP 下，通过输入或修改网络参数来添加新的 LDAP 服务器 或编辑 现有 LDAP 服务器的设置。
添加或修改 TACACS 服务器	导航到 系 ** 统 ** > 身份验 ** 证 ** > **TACACS**。在 **TACACS** 下，添加新的

TACACS 服务器或通过输入或 修改网络参数来编辑 现有 TACACS 服务器的设置。|
添加或修改 syslog 服务器	导航到“系 ** 统 **” > “** 审核 **” > “系统日志服务 ** 器 **”。在 **Syslog** 服务器下，添加新的 syslog 服务器或通过输入或修改网络参数来编辑现有 syslog 服务器的设 置。可以选择要监视的日志级别种类来提供其他信息。
读取 syslog 消息	导航到“系 ** 统 **” > “** 审核 **”。在 **Audit Messages**（审核消息）下方，选择 **Syslog Messages**（Syslog 消息）。所有系统日志文件的汇总都显示在“Syslog Viewer”（Syslog 查看器）中。您可以从“文件”下拉选项中选择要查看的 syslog 文件。此外，可以按模块、事件类型和严重性进一步筛选 syslog 文件。
配置 syslog 清除设置	导航到“系 ** 统 **” > “** 审核 **”。在“** 设 ** 置”下，选择“系统日志清除 ** 设 ** 置”，然后输入在 Citrix ADM 中删除系统日志数据 之前保留该数据的 天数。
查看系统事件	导航到“系 ** 统 **” > “** 事 ** 件”。之后可以查看所有当前事件及详细信息。
添加或修改 NTP 服务器	导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。添加新的 NTP 服务器或编辑现有 NTP 服务器的设置。
配置 NTP 参数	导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。单击 **NTP Parameters**（NTP 参数）并在提供的给定字段中输入服务器的配置详细信息。
启用 NTP 同步	导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。要将 NTP 服务器上显示的时间与本地时钟同步，请选中“启用 **NTP** 同步”复选框。
添加或修改密码组	导航到“系 ** 统 **” > “密码 ** 组 **” 以添加新的密 码组或编辑现有密码组 的设置。必须输入密码组的说明，并将其分配给密码套件。
配置通知设置	定位至“** 系统 **” > “** 通知 **”。在 **Settings**（设置）下方，选择 **Change Notification Settings**（更改通知设置）。选择要发送通知的操作，然后选 ** 择 ** 电子邮件、短 ** 信 ** 或两者。
配置事件摘要设置	定位至“** 系统 **” > “** 通知 **”。在 **Settings**（设置）下方，选择 **Configure Event Digest Settings**（配置事件摘要设置）。清除“禁用事件摘要”复选框后 **，您可 ** 以设置重复周期，并 选择用 于发送事件摘要通知的电子邮件通讯组列表。
添加或修改电子邮件服务器	导航到“系 ** 统 **” > “**** 通知” > “电子 ** 邮 ** 件”。在“电子 ** 邮 ** 件”下，选 择“电子 ** 邮件服务器 **” 选项卡以添加新的电子邮件服务器或编辑现有电子邮件服务器的设置。您可以启用其他检查，以确保访问 电子邮件服务器需要身 份验证，或者指定您的电子邮件服务器支持 SSL 身份验证。
添加或修改电子邮件通讯组列表	导航到“系 ** 统 **” > “**** 通知” > “电子 ** 邮 ** 件”。在“电子 ** 邮 ** 件”下，选择 “** 电子邮件分发列 ** 表”选项卡以添加新 的 电子邮件分发列表或编辑现有电子邮件分发列表的设置。
添加或修改 SMS 服务器	导航到“系 ** 统 **” > “**** 通知” > “短 ** 信 **”。在 **SMS** 下，选择 **SMS 服务器 ** 选项卡以添加新的 SMS 服务器或编辑 现有 SMS 服务器的设置。
添加或修改 SMS 通讯组列表	导航到“系 ** 统 **” > “**** 通知” > “短 ** 信 **”。在 **SMS** 下，选择 **SMS 分发列 ** 表 选项卡以添加 新的 SMS 分发列表或编辑现有 SMS 分发列表的设置。
配置 SNMP 引擎 ID	导航到“系 ** 统 **” > “**SNMP**”。在“** 设 ** 置”下，选择“配置引擎 **ID**” 并指定引擎 ID。
配置 SNMP MIB	导航到“系 ** 统 **” > “**SNMP**”。在“** 设 ** 置”下，选择“配置 **SNMP MIB**”，然后输入 SNMP MIB 详细信息。
配置 SNMP 陷阱	导航到 **System**（系统）> **SNMP** > **Trap Destinations**（陷阱目标）。在 **SNMP 陷阱 ** 下，添加新的 SNMP 陷阱目标或编辑现有 SNMP 陷阱目标的设置。
添加或修改 SNMP 管理器	导航到 **System**（系统）> **SNMP** > **Managers**（管理器）。在 **SNMP**

管理器下，添加新的 SNMP 管理器或 编辑现有 SNMP 管理器的设置。|
添加或修改 SNMP 用户	导航到 **System**（系统）> **SNMP** > **Users**（用户）。在 **SNMP Users**（SNMP 用户）下方，添加新 SNMP 用户或编辑现有 SNMP 用户的设置。
添加或修改 SNMP 视图	导航到“系 ** 统 **” > “**SNMP**” > “视 ** 图 **”。在 **SNMP View**（SNMP 视图）下方，添加新 SNMP 视图或编辑现有 SNMP 视图的设置。
修改警报	导航到“系 ** 统 **” > “** 警 ** 报”，然后选择要修改其设置的警报。警报可帮助您监视 Citrix ADM 服务器的运行状况。
查看任务日志	导航到“系 ** 统 **” > “** 诊 ** 断” > “任 ** 务 ** 日志”。然后，您可以查看所有任务日志 以及详细信息。您可以通过选择任务日志并查看其 设备日志来查看其 他信息，然后查看所选设备日志的命令日志。
生成技术支持文件	导航到“系 ** 统 **” > “** 诊 ** 断” > “** 技术支持 **”。在 “** 技 ** 术支持”下，单击“生成 ** 技 ** 术支持文件”以 生成 Citrix ADM 数据和统计信息的存档（TAR 文件），您可 以 将其发送给 Citrix 支持部门以获取调试问题的帮助。
配置控制板 报告时区设置	导航到“系 ** 统 **” > “分析 ** 设 ** 置”。在 **Analytics 设 ** 置下，选择 配 置控制板 ** 报告时区 ** 设置，将您的本地时间或 GMT 时区设 置为控制板上显示的报告的默认时区。
配置 ICA 会话超时	导航到“系 ** 统 **” > “分析 ** 设 ** 置”。在 “分析 ** 设 ** 置” 下，选择 “配置 **ICA** 会话超时”，然后输入 ICA 会话在终止之前可以保持空 闲状态的 时间长度。
配置分析功能	导航到“系 ** 统 **” > “分析 ** 设 ** 置”。在 “分析 ** 设 ** 置” 下，选 ** 择 “** 配置功能”以启用多跳设置和自适应阈值设置。如果选中 “** 启 ** 用多跳”复选框，Citrix ADM 会收集并关联在客户端与 服务器之间部署了多个 Citrix ADC 实例的所有设备的 AppFlow 记录。如果选中“启用自 ** 适应阈 ** 值”复选框，则每当 URL 的点击次数高于 其阈值时，系统就会向 syslog 服务器发 送一条 syslog 消息。
配置数据库设置	导航到“系 ** 统 **” > “分析 ** 设 ** 置”。在 ** 分析设置 ** 下，选择 ** 配置功能 ** 以启用数据库索引设置和数据库清理设置。通过选中“启用数据 ** 库 ** 索引”复选框，可以简 化对 Citrix ADM 数据库的有效 查询。如果选中“启用数据 ** 库 ** 清理”复 选框，则如果 Citrix ADM 负载过重，无法在定期安排的时间进行清理，则会重复尝试清理数据库。
配置数据库缓存设置	导航到“系 ** 统 **” > “分析 ** 设 ** 置”。在 **Analytics 设 ** 置下，选择 配置数据 ** 库 ** 缓存设 置，将数据库内容 本地存储在缓存中，这样您无需访 问数据库服务器即可查看此 内容。
配置数据记录设置	在“分析 ** 设 ** 置” 中，选择“配置数 ** 据记录设 ** 置”。您可以为以下设置启用功能：数据记录日志设置、数据 持续时间持续性设置、Web Insight 报告 设置、Web Insight SLA 数据收集设置、Web Insight URL 数据收集设置、URL 参数设置
为特定的 Citrix ADC IP 地址配置 SLA 管理	导航到 “** 系统 **” > “** 分析设置 **” > “**SLA 管理 **”。从显示的列表中，选择要在服务器响应时间、点击/秒和带宽使用量上管理 SLA 的 设备的 Citrix ADC IP 地 址。
配置每个 Insight 摘要 级别的数据库记录的 保留期限	导航到 “** 系统 **” > “** 分析设置 **” > “** 数据库汇总 **”。指定要在 Citrix ADM 上保留 Insight 数据 的期限。可以选择按每小时、每天或每分钟存储数据。
添加或修改自适应阈值	导航到“系 ** 统 **” > “分析 ** 设 ** 置” > “自 ** 适应阈 ** 值”。在 “自 ** 适应阈 ** 值”下，添加新的自适应阈值或编辑现有自适应阈值的设置。自适应阈值功能为每个 URL 的最 大点击 量设置阈值。如果 URL 的最大命中次数高 于为该 URL 设置的阈值，则系统会向 外部 syslog 服务器发送一条 syslog 消息。阈值时间间隔可以是天或周。
添加或修改阈值和警报	导航到 “** 系统 **” > “** 分析设置 **” > “** 阈值 **”。在 “** 阈 ** 值”下，添加新限制或编辑现有阈值的设置。您可以在创建或修改阈值时提供其他操作 项目，例如启用 阈值、通过电子邮件或短信发送通知

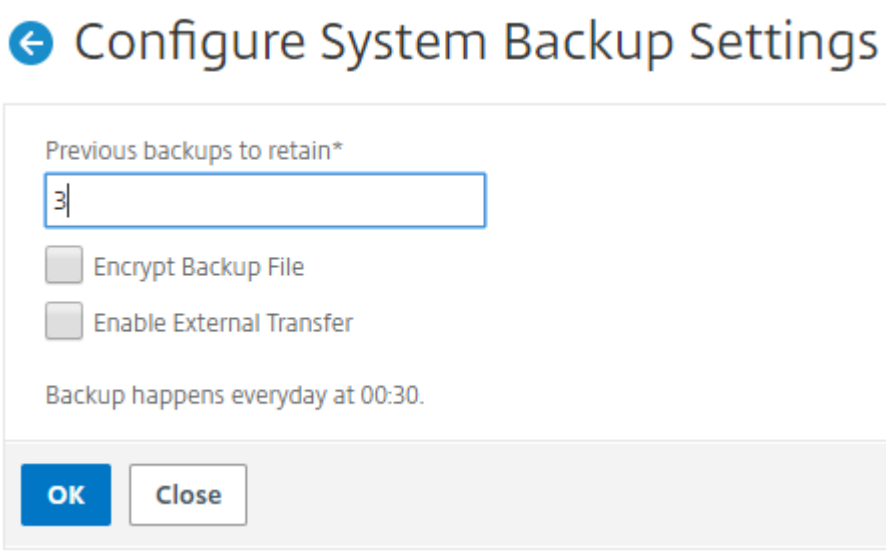
或 为阈值 配置规则。|
上载 SSL 证书文件和 SSL 密钥	导航到“系 ** 统 **” > “高 ** 级设 ** 置” > “**SSL 证 ** 书文件”。在 **SSL 证 ** 书文件下，选择 **SSL 证 ** 书 选项卡上载新的 SSL 证书。同样，在 **SSL 证 ** 书文件下，选择 **SSL 密钥 ** 选项卡来上载新的 SSL 密钥。
查看或编辑报告导出计划	导航到“系 ** 统 **” > “高 ** 级设 ** 置” > “** 导 ** 出计划”。之后可以查看所有导出计划及详细信息。您可以编辑此处 显示的列表中的任何导出 时间表。
计划报告导出	导航到“系 ** 统 **” > “高 ** 级设 ** 置” > “** 导 ** 出计划”。要添加新计划，请单击最右边的按钮，然后选 择“** 计 ** 划导出”选项卡。指定详细信息并单击 **Schedule**（计划）。
使用备份和还原功能	导航到“系 ** 统 **” > “** 高 ** 级设 ** 置” **> “备份文件”，创建 Citrix ADM 当前设置的备份。稍后您可 以使用这些备份的文件将 Citrix ADM 恢复到您备份的状态。Citrix 建议在执行升级之前使用此功能，通常 作为预防措施。
安装 SSL 证书	导航到 **System**（系统）> **System Administration**（系统管理）。在“** 设置 Citrix ADM**”下，选择安 ** 装 SSL 证 ** 书。您可以选择 Citrix ADM 虚拟设备上 已有的 证书文件和 SSL 密钥文件，也可以从本地 计算机上载这 些文件。必须在“密码”字段中输入 Citrix ADM 密码才能成 功 安装 SSL 证书。
Prompt Credentials for Instance Login（进行实例登录时提示提供凭据）	导航到“系 ** 统 **” > “更 ** 改系统设 ** 置”。启用“提示实 ** 例登录凭 ** 据”以提示用户 在 Citrix ADC 实例上的任何配置操作中输入实例凭据。
Enable Automatic Data Purge（启用自动数据清除）	导航到 **System**（系统）> **System Administration**（系统管理）。在“** 删除设 ** 置”下，选择“系 ** 统清理设 ** 置”。选 ** 中“启用 ** 自动数据清除”复选框，允许 Citrix ADM 在 磁盘使用量达到设定的阈值时清除数据。启用 此功能后，Citrix ADM 会清除与 事件、系统日志、性能报告和分析相关的数据，直到磁盘使用量低 于设定的阈值为止。单击“编辑”图标修改磁盘使用率的 阈值。

配置系统备份设置

February 6, 2024

在需要备份和还原 Citrix Application Delivery Management (ADM) 系统之前，应设置初始系统备份设置。

1. 导航到“系统”>“系统管理”。在“备份设置”下，单击“系统备份设置”。
2. 在“配置系统备份设置”页面上，指定以下内容：
   - 要保留的备份数。最多只能保留 10 个备份。
   - 加密备份文件。
   - 启用外部传输。可以将备份文件副本传输到另一个系统上作为预防措施。要恢复配置时，必须先将文件上载到 Citrix ADM 服务器，然后执行还原操作。指定服务器、用户名和密码、端口、要使用的传输协议以及目录路径。要了解有关外部传输的更多信息，请参阅 将 Citrix ADM 备份文件传输到外部系统。
3. 单击确定。



配置 NTP 服务器

February 6, 2024

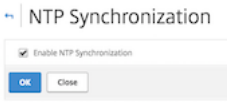
您可以在 Citrix Application Delivery Management (ADM) 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

要在 **Citrix ADM** 上配置 **NTP** 服务器，请执行以下操作：

1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器），然后单击 **Add**（添加）。
2. 在 **Create NTP Server**（创建 NTP 服务器）页面上，输入以下详细信息：
   - **Server Name/IP Address**（服务器名称/IP 地址）–输入 NTP 服务器的域名或 IP 地址。添加了 NTP 服务器后无法更改名称或 IP 地址。
   - **Minimum Poll Interval**（最小轮询时间间隔）–指定传输的 NTP 消息之间的最小时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最小轮询时间间隔是 64 秒（可以表示为 2^6），则输入 6。
   - **Maximum Poll Interval**（最大轮询时间间隔）–指定传输的 NTP 消息之间的最大时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最大轮询时间间隔是 256 秒（可以表示为 2^8），则输入 8。
   - **Key Identifier**（密钥标识符）- 输入可以用于 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择“Autokey”（自动密钥），请勿添加密钥标识符。
   - **Autokey**（自动密钥）- 如果希望 NTP 服务器使用公钥身份验证，请选择 **Autokey**（自动密钥）。如果要添加密钥标识符，请勿选择。
   - **Preferred**（首选）–如果希望将此 NTP 服务器指定为进行时钟同步的首选服务器，请选择此选项。这仅在配置多个服务器时适用。
3. 单击创建。

要在 **Citrix ADM** 上启用 **NTP** 同步，请执行以下操作：

1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。
2. 单击 **NTP** 同步，然后选中 启用 **NTP** 同步 复选框。
3. 单击确定。



> 注意：
>
> 您可以在文件 `/var/log/ntpd.log` 文件的 /var/log 目录中找到 NTP 日志消息。

升级 **Citrix ADM**

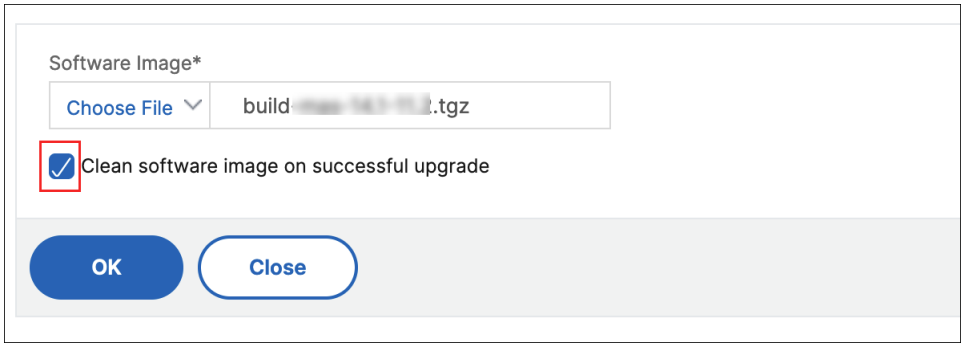
February 6, 2024

每个 Citrix Application Delivery Management (ADM) 版本都提供了新的和更新的功能以及更多的功能。增强功能的完整列表在版本发布时附带的发行说明中提供。升级软件前，请花一些时间阅读发行说明。在开始升级软件前了解许可框架及许可证类型，这很重要。

要升级 **Citrix ADM**，请执行以下操作：

1. 导航到 **System**（系统）> **System Administrations**（系统管理）。在“系统管理”子标题下，单击“升级 **Citrix ADM**”。
2. 在升级 Citrix ADM 页面上，选择本 地（您的本地 计算机）或 ** 设 ** 备（证书文件必须存在于 Citrix ADM 虚拟设备 上），上载新的映像文件。
   默认情况下，软件映像在成功升级后被清理。

3. 单击确定。



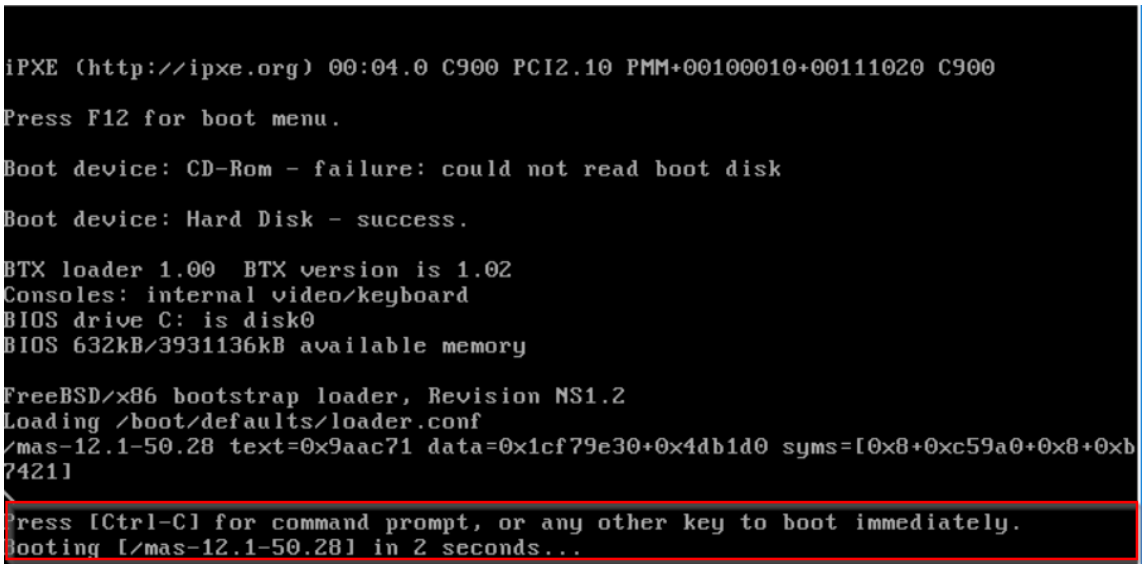
如何重置 **Citrix ADM** 的密码

February 6, 2024

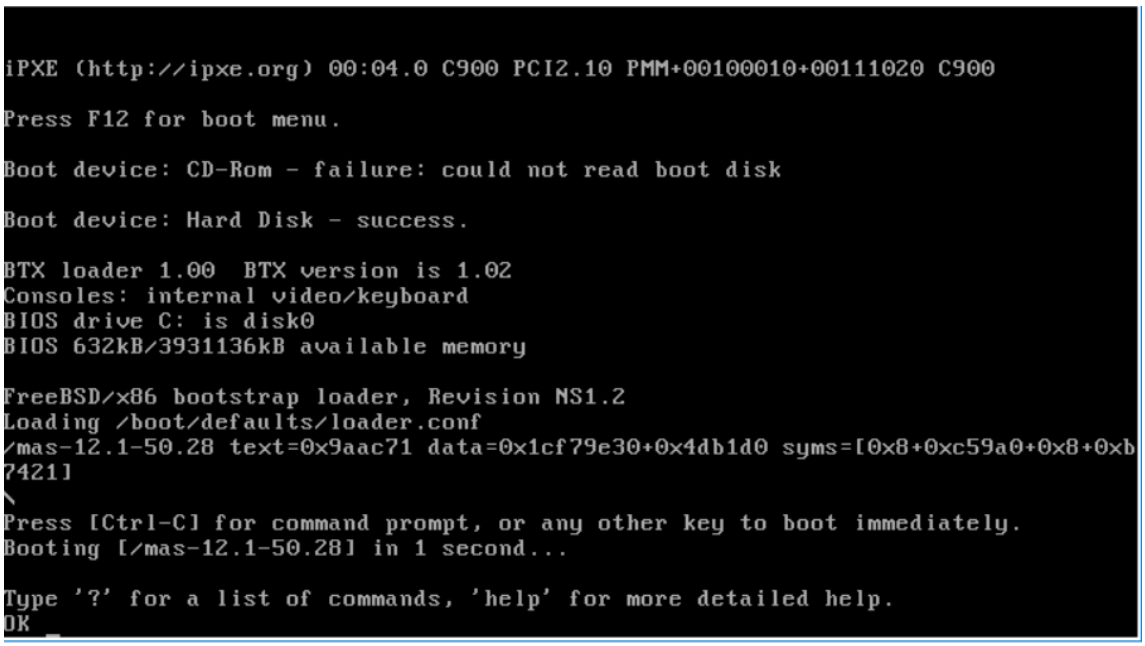
在托管 Citrix ADM 的虚拟机管理程序上，重置 Citrix ADM 密码的过程可能有所不同。如果您已更改默认密码并想要重置为默认密码，则可以通过重新启动 Citrix ADM 节点来重置密码。

使用 **XenCenter** 的 **Citrix Hypervisor**:

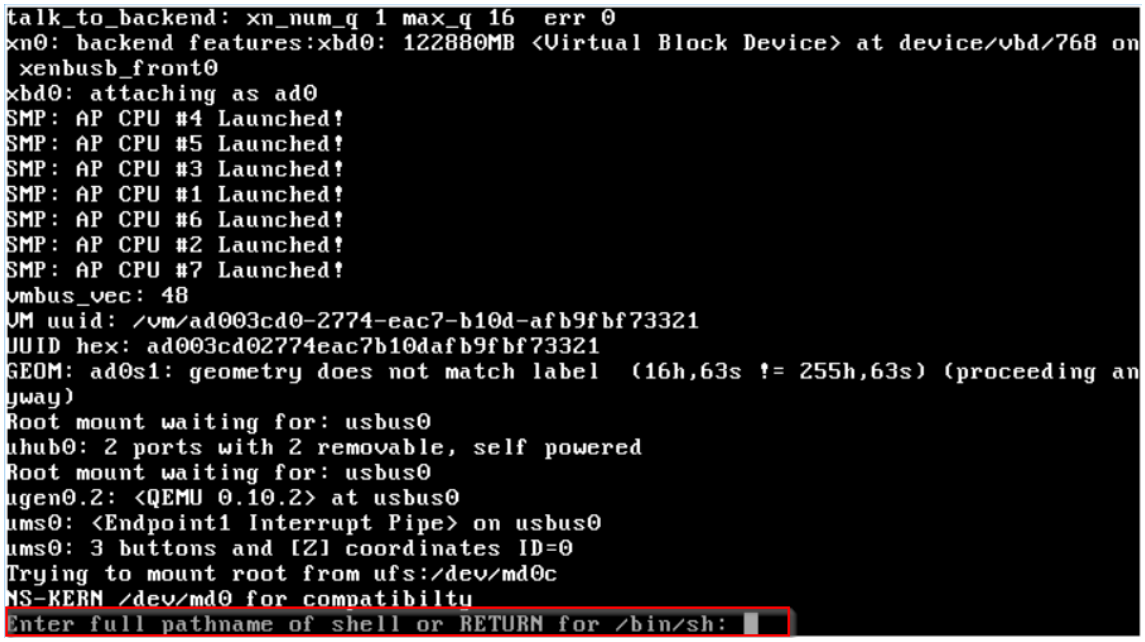
1. 使用 XenCenter 登录 Citrix Hypervisor。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台 选项卡上，按 **CTL + C** 中断启动顺序。



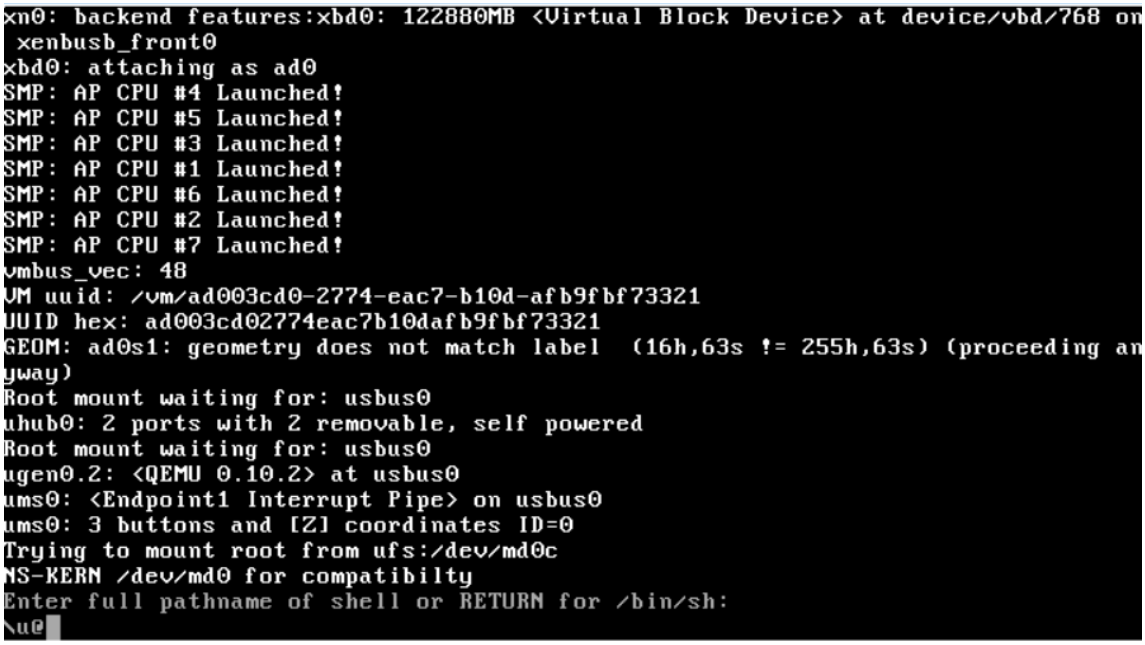
4. 在 OK 提示符下运行 **boot-s** 命令。



Citrix ADM 重新启动并显示以下消息：

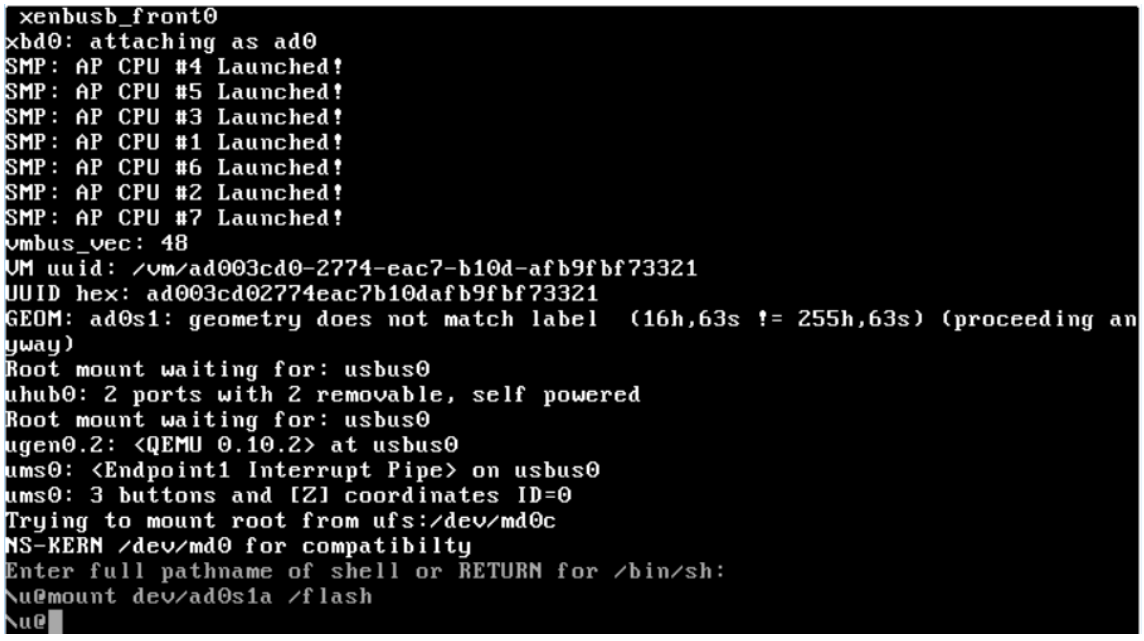


5. 按 **Enter** 获取 /u @ 提示符。



6. 使用以下命令装载闪存分区：

   ```
   mount dev/ad0s1a /flash
   ```



7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：

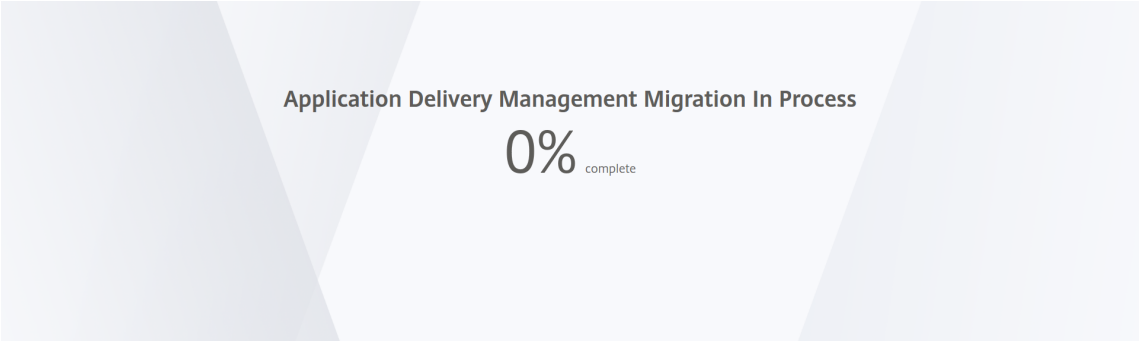
   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

10. 运行 重启 命令以重新启动 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
```

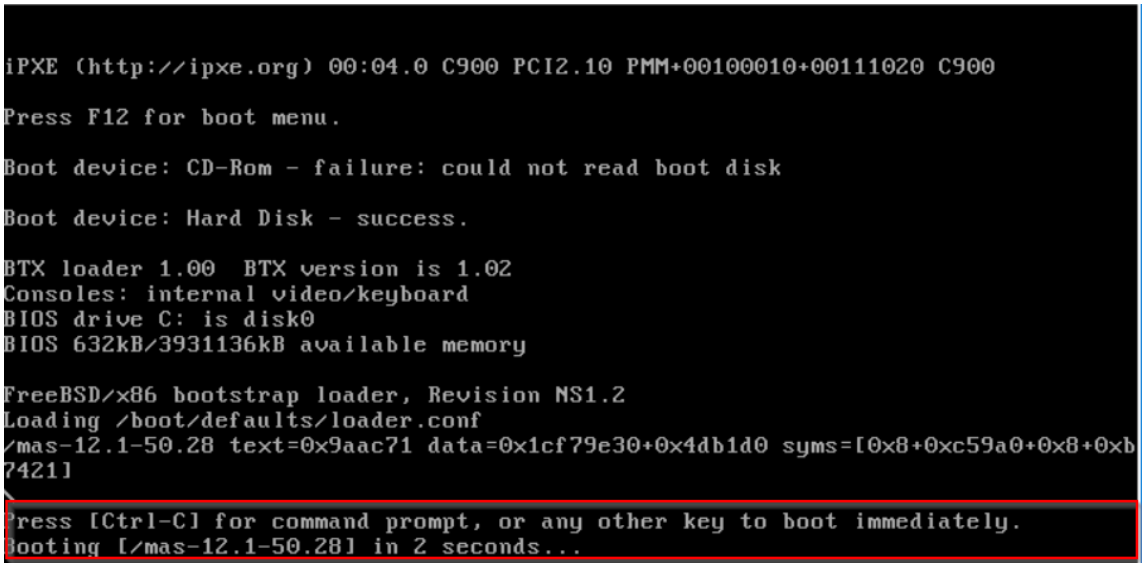
11. 访问 Citrix ADM GUI，然后等待重新启动完成。



现在，您可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsroot/nsroot* 从 Hypervisor 登录。

使用 **vSphere** 的 **ESX**:

1. 使用 vSphere 登录 ESX。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台 选项卡上，按 **CTL + C** 中断启动顺序。



4. 在 OK 提示符下运行 **boot-s** 命令。

   Citrix ADM 将重新启动。

5. 按 **Enter** 获取 /u @ 提示符。
6. 使用以下命令装载闪存分区：

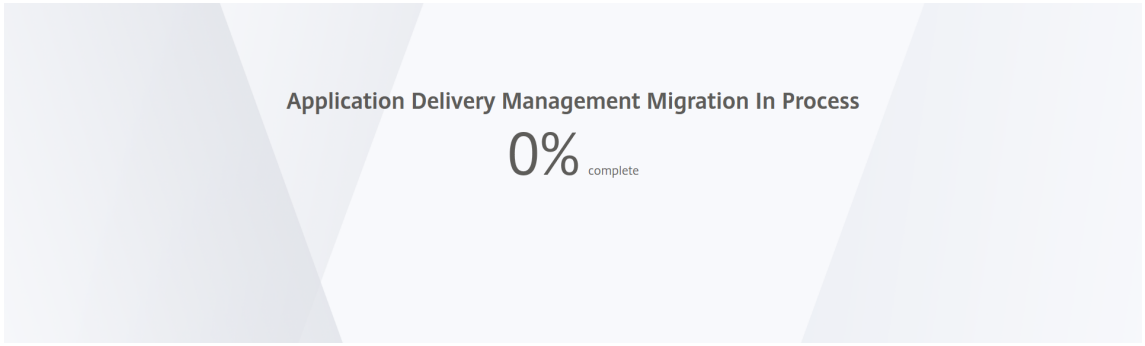
   ```
   mount dev/da0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：

   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

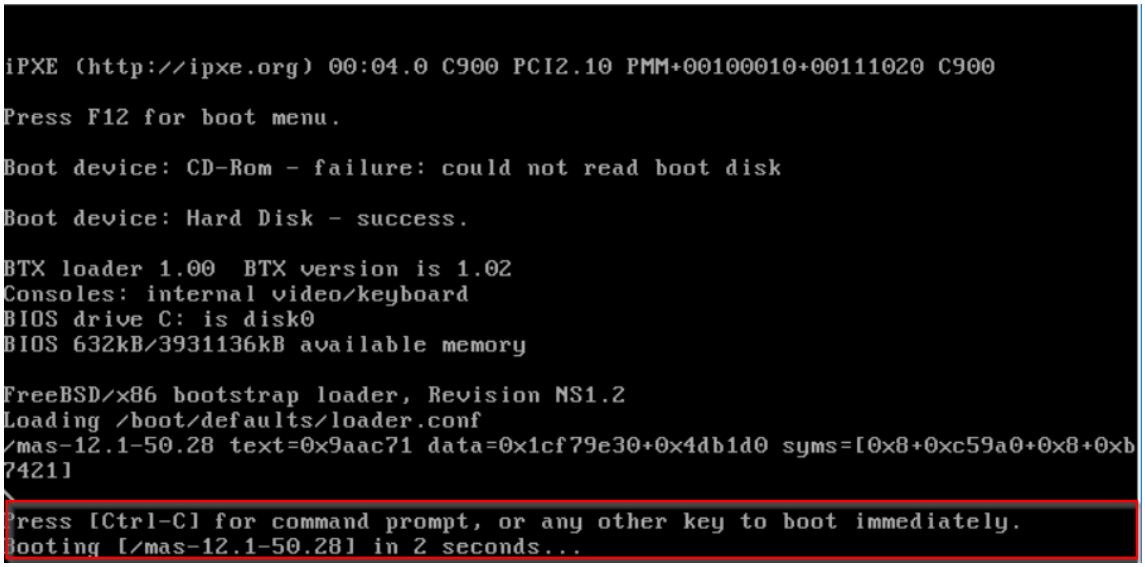
10. 运行 重启 命令以重新启动 Citrix ADM。
11. 访问 Citrix ADM GUI，然后等待重新启动完成。



您现在可以使用 nsroot/nsroot 凭据从图形用户界面登录，从 *ESX* 服务器登录。

使用 **Hyper-V** 管理器的 **Hyper-V**：

1. 使用 Hyper-v 管理器登录 hyper-v。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台 选项卡上，按 **CTL + C** 中断启动顺序。



4. 在 OK 提示符下运行 **boot-s** 命令。

   Citrix ADM 将重新启动。

5. 按 **Enter** 获取 /u @ 提示符。
6. 使用以下命令装载闪存分区：

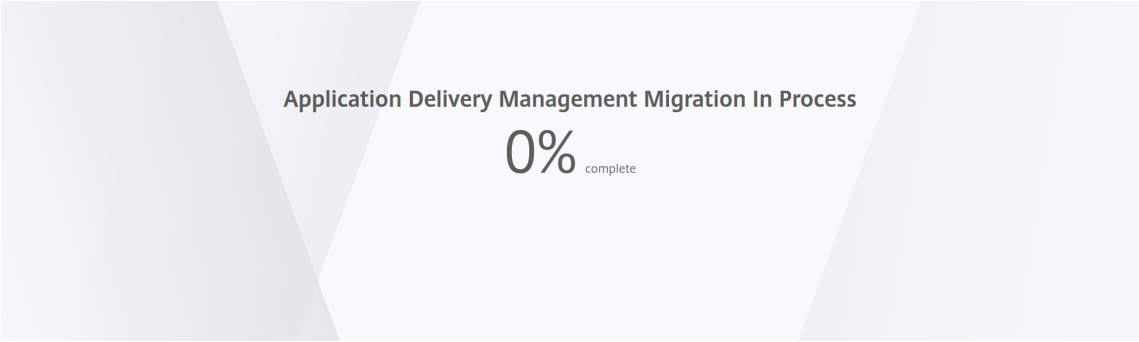
   ```
   mount dev/ad0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：

   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

10. 运行 重启 命令以重新启动 Citrix ADM。
11. 访问 Citrix ADM GUI，然后等待重新启动完成。



您现在可以使用 *nsroot/nsroot* 凭据从图形用户界面登录，并使用 *nsroot/nsroot* 从超级 v 管理器登录。

Linux KVM 服务器（**SSH** 到 **KVM** 服务器通过使用任何 **SSH** 客户端）：

1. 使用 SSH 客户端登录 Citrix ADM 到 KVM 服务器。
2. 重启 Citrix ADM。
3. 在显示加载/启动/ 默认**/**装载器**.conf** 消息后不久，按 **CTL + C** 中断启动序列。
4. 在 OK 提示符下，运行以下命令：

   ```
   set console='comconsole,vidconsole'
   ```

5. 运行 引导**-s** 命令以重新启动 Citrix ADM。
6. 显示输入 **shell** 的完整路径或 **/bin/sh** 的 **RETURN** 消息后，按 **Enter** 获取 /u@ 提示符。
7. 使用以下命令装载闪存分区：

   ```
   mount dev/vtbd0s1a /flash
   ```

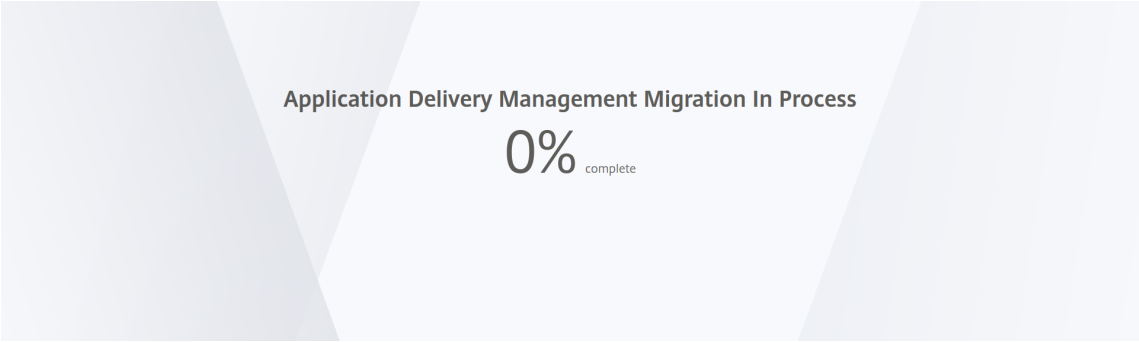
8. ```
   Delete /flash/mpsconfig/master.passwd
   ```

9. ```
   Delete rm -rf /etc/passwd
   ```

10. 使用以下命令创建文件：

    ```
    touch /flash/mpsconfig/.recover
    ```

    密码现在重置为默认密码。
11. 运行 重启 命令以重新启动 Citrix ADM。
12. 访问 Citrix ADM GUI，然后等待重新启动完成。



您现在可以使用 nsroot/nsroot 凭据从图形用户界面登录，并从 *SSH* 控制台登录。

配置 **syslog** 删除时间间隔

February 6, 2024

Syslog 是日志记录标准协议。它有两个组件：在 Citrix Application Delivery Controller (ADC) 实例上运行的 Syslog 审核模块，以及 Syslog 服务器，它可以在 Citrix ADC 实例的底层 FreeBSD 操作系统 (OS) 上运行，也可以在远程系统上运行。SYSLOG 使用用户数据报协议 (UDP) 进行数据传输。

通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

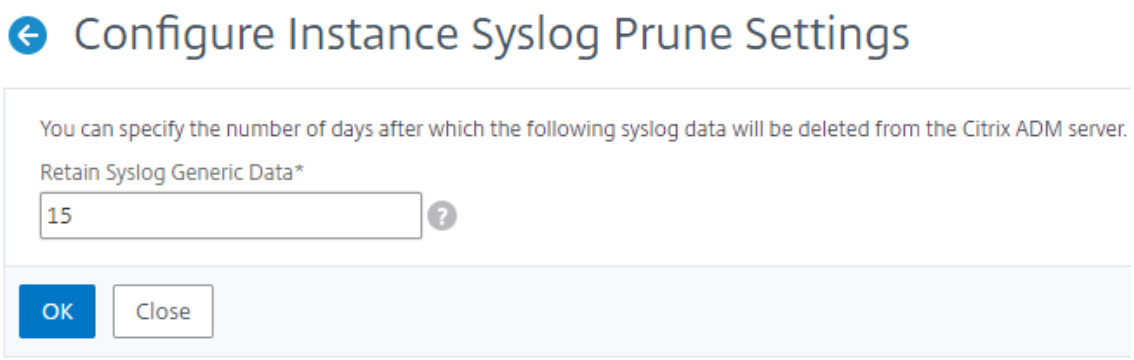
要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定从 Citrix Application Delivery Management (ADM) 中删除以下 syslog 数据的天数：

- 一般 Syslog 数据
- AppFirewall 数据
- Citrix Gateway 数据

您还可以按系统日志类型配置 Citrix Gateway 清除间隔。此清除间隔优先于为保留 Citrix Gateway 数据而配置的清除间隔。

要配置 **Citrix ADM** 的系统日志清除间隔设置，请执行以下操作：

1. 导航到 **System**（系统）> **System Administration**（系统管理）。在“删除 设置”下，单击“实例 **Syslog** 删除设置”。
2. 在“配置实例 **Syslog** 清除设置”页面中，指定“保留 **Syslog** 通用数据”。键入 Citrix ADM 保留通用系统日志消息的天数。



配置系统删除设置

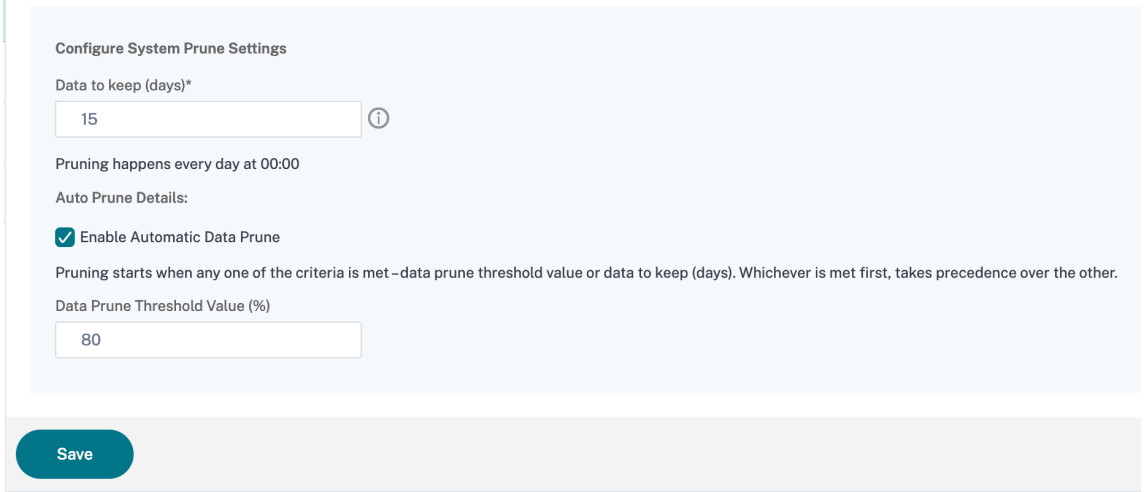
February 6, 2024

要限制存储在 Citrix Application Delivery Management (ADM) 软件数据库中的报告数据量，可以对其进行修剪。您可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时修剪一次（在 00.00 点）。

> 注意
>
> 您指定的值不能超过 30 天或少于 15 天。

要使用 **Citrix ADM** 为性能报告配置系统修剪设置，请执行以下操作：

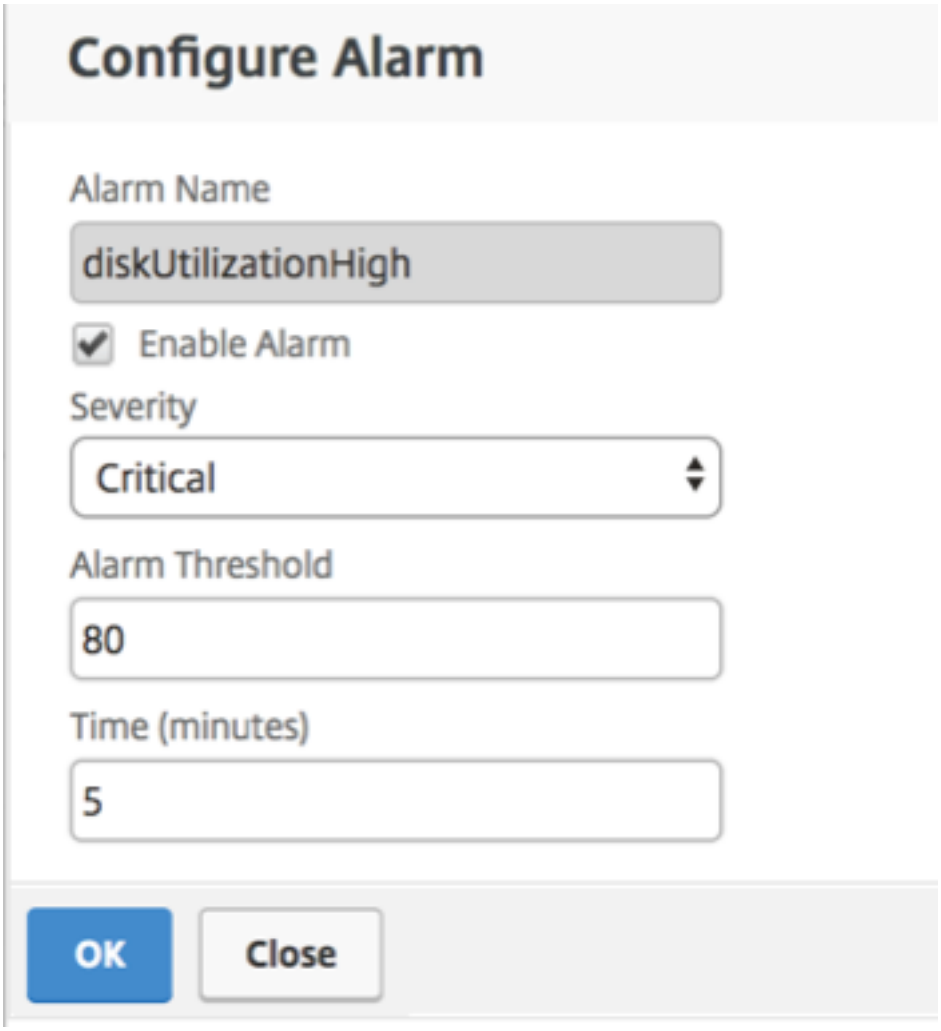
1. 导航到“系统”>“系统管理”。在 “删除设置”下，单击 “系统清理设置”。
2. 在“配置系统修剪设置”页中，指定保留数据的天数，然后单击“确定”。



您可以通过选中 “启用自动数据清除”复选框来启用自动清除。当磁盘使用量超过配置的数 据清除阈值时，将触发警报。

您可以配置和启用磁盘高警报（默认情况下）并指定以下内容：

- 严重性， 例如“严重”。
- 警报阈值。键入用于计算事件严重性的值。
- 时间。要触发警报的时间长度（以分钟为单位）。



为非默认用户启用 **shell** 访问权限

February 6, 2024

您可以在 Citrix Application Delivery Management (ADM) 中为非默认用户启用 shell 访问。可以使用此功能启用和设置与实例的通信模式。

> 注意
>
> 默认情况下，对非默认用户禁用 shell 访问。

要在 **Citrix ADM** 中为非默认用户启用 **shell** 访问，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“系统管理”。
2. 在 **System Settings**（系统设置）中，单击 **Change System Settings**（更改系统设置）。
3. 在 **Modify System Settings**（修改系统设置）页面上，配置以下参数：
   - **Communication with instances**（与实例通信）- 选择通信协议。
   - 安全访问 -启用 Citrix ADM 的安全访问。
   - **Enable Session Timeout**（启用会话超时）- 指定保留非活动会话的时间段。
   - **Allow Basic Authentication**（允许基本身份验证）- 允许管理服务接受使用基本身份验证协议提供的凭据。
   - **Enable nsrecover Login**（启用 nsrecover 登录）- 对管理服务启用 nsrecover 登录。
   - 启用证书下载 -使您能够从添加的 Citrix ADC 下载证书。
   - 为非 **nsroot** 用户启用命令行管理程序访问—为 Citrix ADM 中的非默认用户启用 shell 访问。
   - 提示用户凭据进行实例登录 -允许用户在从 Citrix ADM 登录到实例时输入其用户凭据。
4. 单击确定。

恢复无法访问的 **Citrix ADM** 服务器

February 6, 2024

Citrix Application Delivery Management (ADM) 现在提供了一个用于执行系统数据库清理的数据库维护工具。现在，您可以启动 Citrix ADM 实用程序工具以连接到文件系统、删除一些组件并使数据库可访问。Citrix ADM 恢复脚本是一种工具，可通过清除旧的或未使用的数据库表和文件来帮助恢复文件系统中的空间。该工具可帮助您按连续步骤浏览数据库表和文件，并显示相应项目在文件系统上占用的当前空间。选择要删除的数据库表和文件后，该工具将在确认后从文件系统中删除这些表和文件。

如何将 **Citrix ADM** 数据库恢复脚本用于 **Citrix ADM** 独立部署

在单个服务器 Citrix ADM 部署中使用以下过程连接到文件系统、删除一些组件并使数据库可访问，然后执行恢复操作。

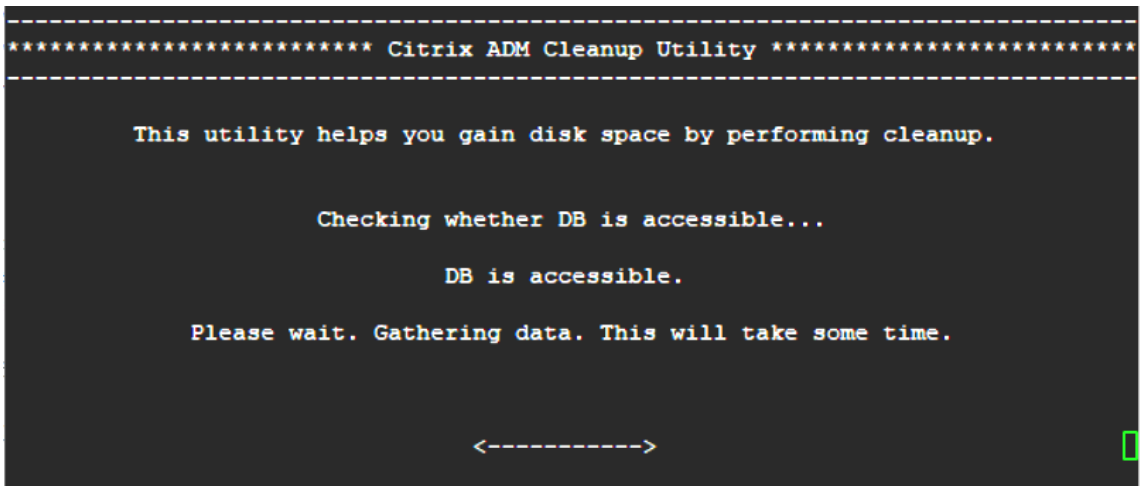
1. 使用 SSH 客户端或虚拟机管理程序控制台登录 Citrix ADM 并键入以下命令：数据

```
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
```

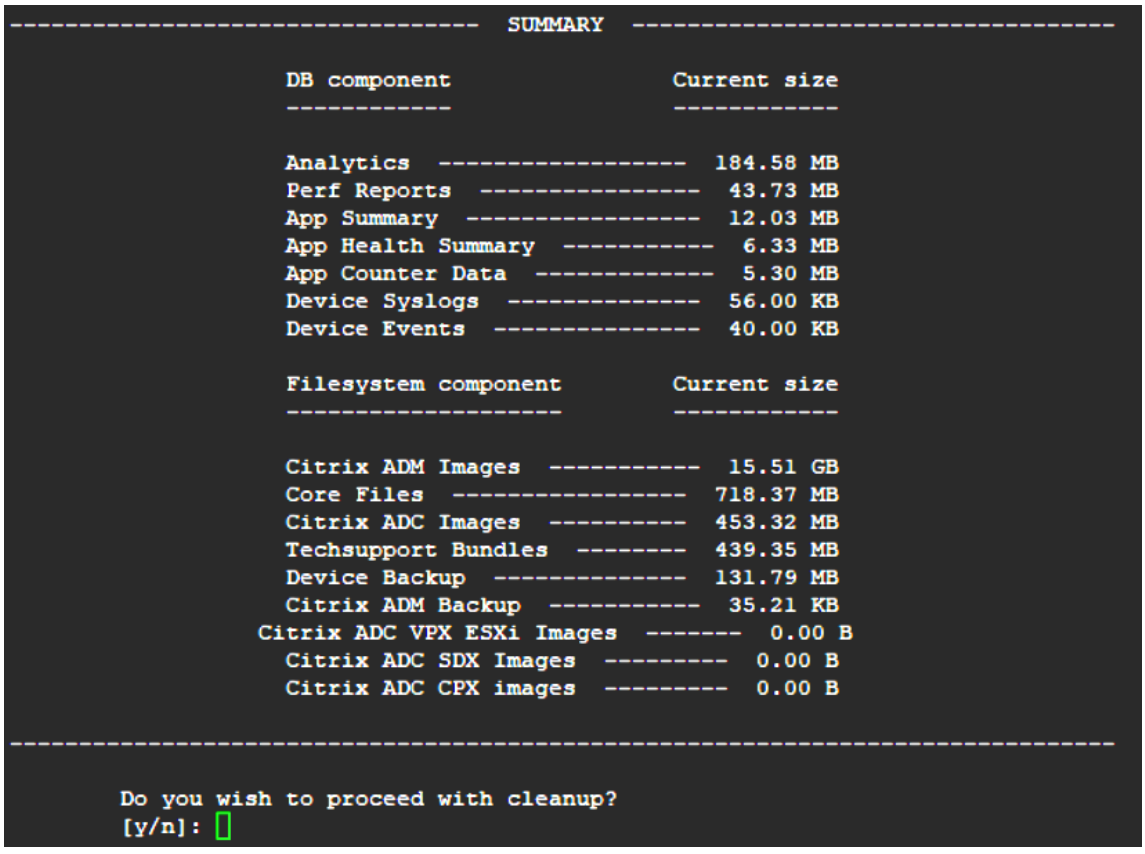
工具

2. 当屏幕显示停止一些 Citrix ADM 进程的警告消息时，键入“y”并按 **Enter** 键。

   当系统确定可以删除数据库的哪些组件而不影响系统的核心文件时，将出现以下屏幕。



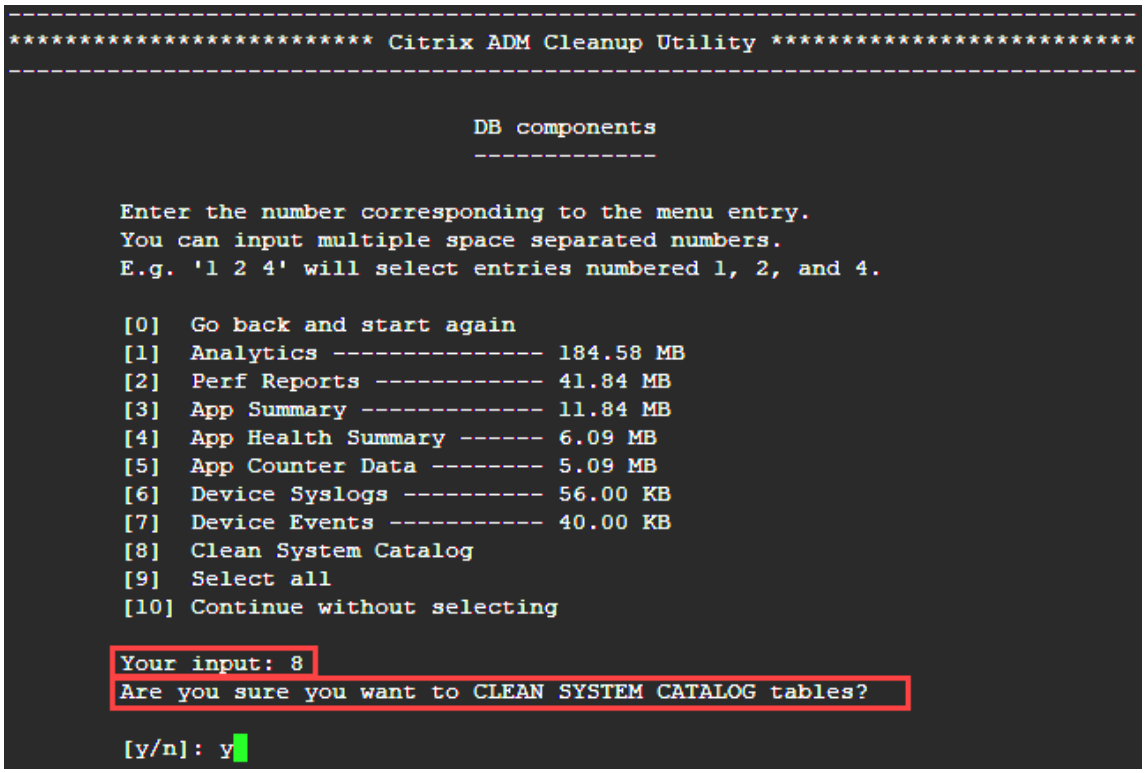
3. 屏幕显示数据库中的文件列表。键入“y”，然后按 Enter 键开始清理过程。



4. 您可以选择需要清理的特定数据库组件，然后键入相应的数字。按下 回车 键。

   例如，要执行系统目录清理，请在 数据库组件 选择菜单中选择选项 8，然后键入“y”，然后按 **Enter** 键继续清理系统目录。

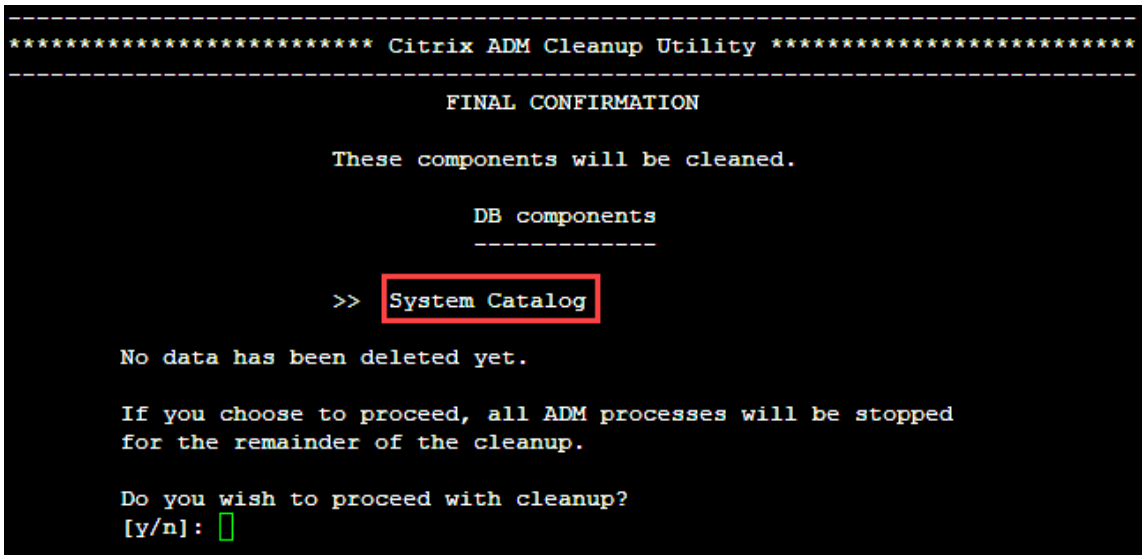
> 注意：
>
> Citrix ADM 包括称为系统目录的用户表。系统目录是 Citrix ADM 数据库中的一个位置，关系数据库管理系统在其中存储架构元数据，例如有关表和列以及内部记录的信息。系统目录中的表就像常规表一样，随着时间的推移，它们会累积膨胀行和死行，因此需要定期清理以获得最佳性能。定期维护这些表是一种很好的做法。该活动不仅释放了磁盘空间，而且还提高了数据库的整体性能，从而提高了 Citrix ADM 的性能。



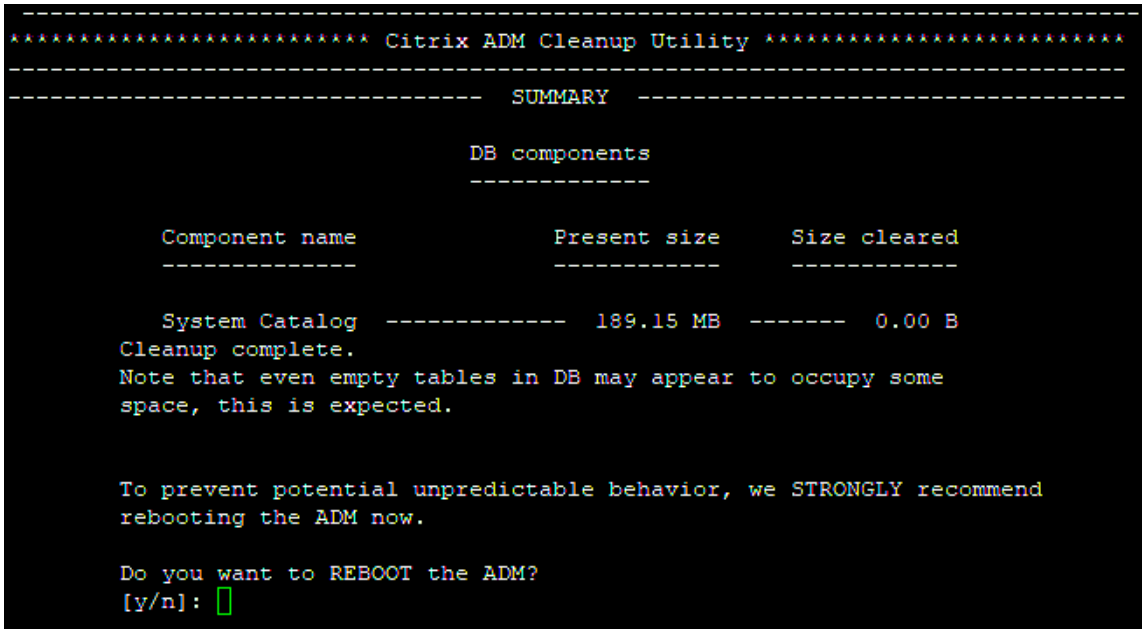
清理实用程序为您提供了清理数据库组件和文件组件的选项。您可以通过键入“1”和“9”之间的数字来选择任何文件组件，或者键入“11”并按 Enter 键清理数据库组件。

> 注意
>
> 数字“11”表示您尚未选择任何要清理的文件组件，正在清理先前选择的早期数据库组件。在此示例中，它是“系统目录”。

5. 键 入 “**y**”，然后在最终确认屏幕中再次按下 **Enter** 键。



系统目录已清理，这可能需要一些时间，具体取决于系统目录中表格的大小。该过程完成后，将显示摘要屏幕。



6. 键入“y”并按 Ent **er** 键重启 Citrix ADM。

   确保在系统清理后重新启动 Citrix ADM。在 Citrix ADM 重新启动后，请等待大约 30 分钟以完成内部数据库操作。然后，您必须能够连接到 Citrix ADM 数据库。如果没有，请再次运行恢复脚本以释放更多空间。当 Citrix ADM 启动并运行时，它必须按预期运行。

   > ** 注
   >
   > 意：** 清理后，系统目录表的当前大小永远不会等于零。这是因为只有空行会从表中删除，即使清理了表中也可能有一些有效的条目。

如何将 **Citrix ADM** 数据库恢复脚本用于 **Citrix ADM** 高可用性部署

高可用性部署中的 Citrix ADM 服务器的数据库系统处于连续同步模式。使用新的数据库恢复工具时，不需要在两个 Citrix ADM 服务器上复制该过程。

1. 使用 SSH 客户端或虚拟机管理程序的控制台登录到主节点。
2. 请运行以下命令：

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. 按照适用于 Citrix ADM 独立部署恢复脚本的步骤 2 中的过程进行操作

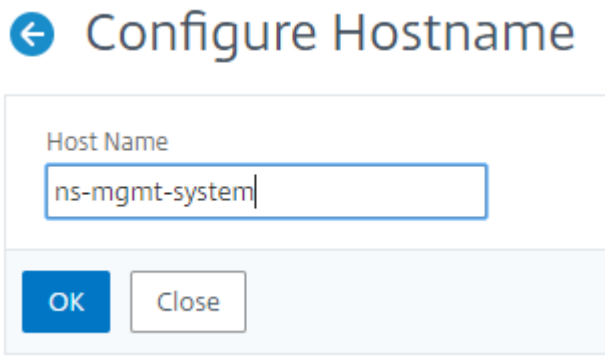
为 **Citrix ADM** 服务器分配主机名

February 6, 2024

要标识 Citrix Application Delivery Management (ADM) 服务器，可以为该服务器分配主机名。主机名将显示在 Citrix ADM 的通用许可证上。

要为 **Citrix ADM** 服务器分配主机名，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“系统管理”。
2. 在 **System Settings**（系统设置）下方，单击 **Change Hostname**（更改主机名）。
3. 在“配置主机名”页上，输入主机名，然后单击“确定”。



备份和还原您的 **Citrix ADM** 服务器

February 6, 2024

您可以对 Citrix ADM 服务器进行定期备份。您可以备份和还原配置文件、实例详细信息、系统数据等。在升级之前，请出于预防原因备份 ADM 服务器配置文件。

备份包括以下组件：

- Citrix ADM 配置文件：
  - SNMP
  - Syslog 服务器配置文件
  - NTP 文件
  - SSL 证书
  - 控制中心文件
- Citrix ADM 服务器管理的 Citrix ADC 实例的备份。
- 配置审核模板。
- 存储在数据库中的系统数据：

  - 创建的租户和用户列表。
  - 外部身份验证服务器配置（LDAP、RADIUS 及其他）。
  - 创建的配置作业和作业模板。

- 存储在数据库中的基础结构和应用程序数据：
  - 来自添加和托管的 Citrix ADC 实例的数据。
  - 实例配置文件详细信息、版本详细信息和实例组详细信息等。
  - 管理员创建的静态应用程序（虚拟服务器组）。
- SNMP 设置。

> 注意：
>
> 分析数据、事件和系统日志消息将从备份中排除。

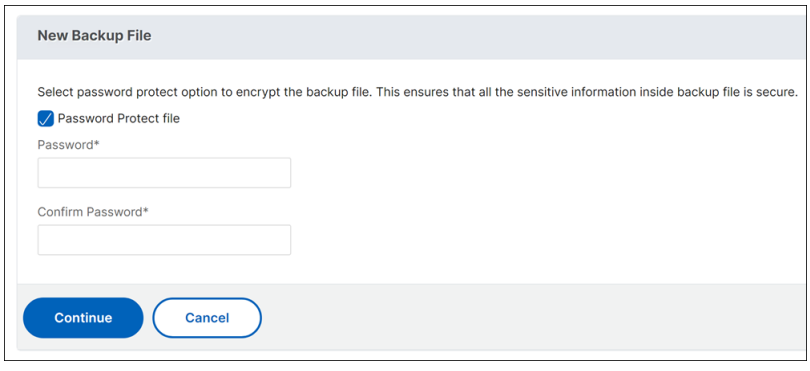
备份 **Citrix ADM** 配置

默认情况下，Citrix ADM 服务器每 24 小时（00.30 小时）备份一次配置。您也可以安排和选择备份时间。此外，您可以将备份文件的副本移动到另一个系统。

备份以还可加密的压缩 TAR 文件进行存储。默认情况下，在服务器中保留三个备份文件。为避免任何磁盘空间不足问题，您最多可以在 Citrix ADM 服务器上存储 10 个备份文件。但是，作为预防措施，Citrix 建议您在服务器上存储备份文件的一些副本或 将文件传输到另一个系统 。

要备份 **Citrix ADM** 配置，请执行以下操作：

1. 导航到 **System**（系统）> **Advanced Settings**（高级设置）> **Backup Files**（备份文件），然后单击 **Back Up**（备份）。
2. 若要加密备份文件，请选中 密码保护文件 复选框，然后提供加密文件的密码。



> 注意
>
> 您也可以通过导航到“系统”>“系统 备份 设置”，然后选择“加密备份文件”来设置 备份文件进行加密。

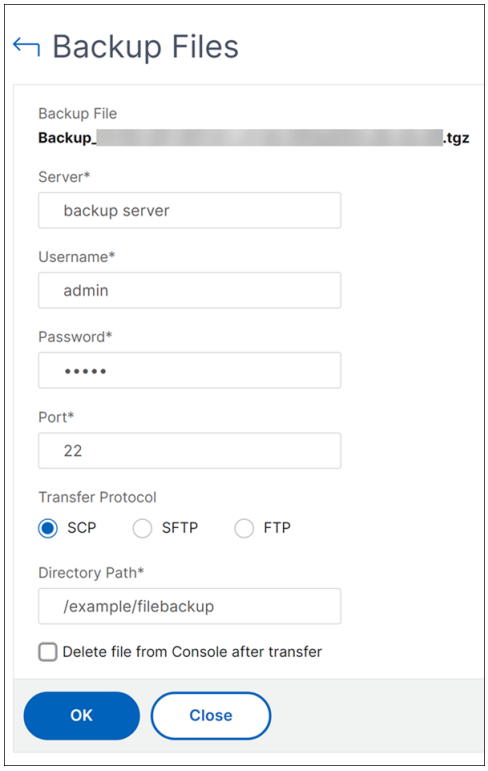
将 **Citrix ADM** 备份文件传输到外部系统

可以将备份文件副本传输到另一个系统上作为预防措施。要还原配置时，请先将文件上载到 Citrix ADM 服务器，然后执行 还原操作。

要传输 **Citrix ADM** 备份文件，请执行以下操作：

1. 导航到 “系统” > “高级设置” > “备份文件”。
2. 选择要移动到另一个系统的备份文件，然后单击“传输”。
3. 在“备份文件”页面上，指定以下参数：
   - 服务器 -您要传输备份文件的系统的 IP 地址。
   - 用户名和密码 -复制备份文件的新系统的用户凭据。
   - **Port**（端口）- 文件要传输到的系统的端口号。
   - **Transfer Protocol**（传输协议）- 进行备份文件传输要使用的协议。可以选择 SCP、SFTP 或 FTP 协议来传输备份文件。
   - 目录路径 -在新系统上将备份文件传输到的位置。

   或者，您也可以通过导航到“系统”>“系统 备份设置”来
   设置外部系统的 详细信息。
4. 通过选中“传输后从 应用程序交付管理中删除文件”复选框，可以在传输后从 Citrix ADM 中删除备份文件。
5. 单击“确定”进行传输。



> 注意
>
> 要将备份文件的副本保存在本地系统中，请导航到“系统”>“高级设置”>“备份文件”，选择要复制的文件，然后单击“下载”。

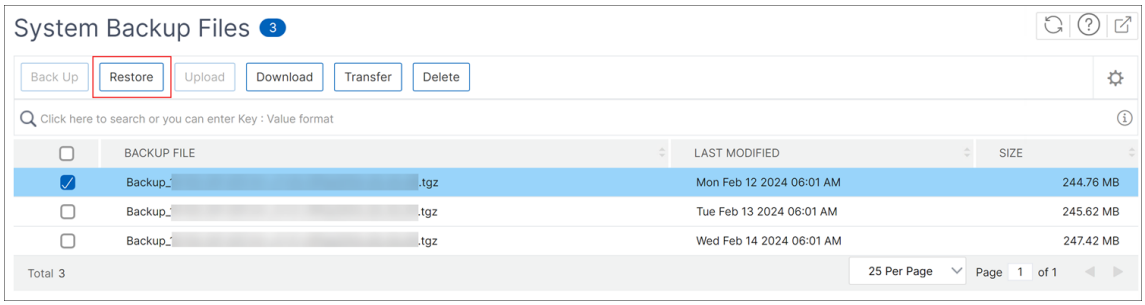
从备份文件还原 **Citrix ADM** 配置

从以前备份的文件还原 Citrix ADM 配置时，还原操作将取消备份文件的修改，然后恢复配置。还原操作会删除现有配置并将其替换为备份文件中的配置。

> 注意
>
> 如果重命名备份文件或修改了备份文件内容，则还原操作将失败。

要从备份文件还原 **Citrix ADM** 配置，请执行以下操作：

1. 导航到 **System**（系统）> **Advanced Settings**（高级设置）> **Backup Files**（备份文件）。
2. 选择要还原的备份文件，然后单击 **Restore**（还原）。
3. 在确认对话框中，单击 **Yes**（是）。



> 注意
>
> 要从存储在外部系统中的备份文件恢复配置，请在执行还原操作之前将备份文件上载到 ADM 服务器。要上载文件，请导航到“系统”>“高级设置”>“备份文件”，然后单击“上载”。

查看审核信息

January 29, 2024

Syslog 是日志记录标准协议。它有两个组件：在 Citrix Application Delivery Controller (ADC) 实例上运行的 Syslog 审核模块，以及 Syslog 服务器，它可以在 Citrix ADC 实例的底层 FreeBSD 操作系统 (OS) 上运行，也可以在远程系统上运行。SYSLOG 使用用户数据报协议 (UDP) 进行数据传输。

通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

如果您将 Citrix ADC 设备配置为将 syslog 消息重定向到 Citrix Application Delivery Management (ADM)，则可以监视 Citrix ADC 设备生成的 syslog 消息。您可以使用 Citrix ADM 中的内置模板功能安排作业，创建生成不同类型 syslog 数据的 syslog 服务器。

首先，配置实例可以向其发送日志信息的 syslog 服务器。然后，指定用于记录日志消息的日期和时间格式。

要在 **Citrix ADM** 上配置 **syslog** 服务器，请执行以下操作：

1. 导航到“系统”>“审核”。在“配置摘要”下，选择 **Syslog** 服务器。或者您可以导航到“系统”>“审核”>“**syslog** 服务器”。
2. 在 **Syslog** 服务器 页面中，单击“添加”。
3. 在 **Create Syslog Server**（创建 Syslog 服务器）页面上，输入以下值：
    - **Name**（名称）- syslog 服务器的名称。
    - **IP Address**（IP 地址）- syslog 服务器的 IP 地址。
    - **Port**（端口）- Syslog 服务器端口。
4. 选择日志级别（All（全部）、None（无）或 Custom（自定义））。相应地选择严重级别。
5. 单击创建。

要在 **Citrix ADM** 上配置 **syslog** 日期和时间格式，请执行以下操作：

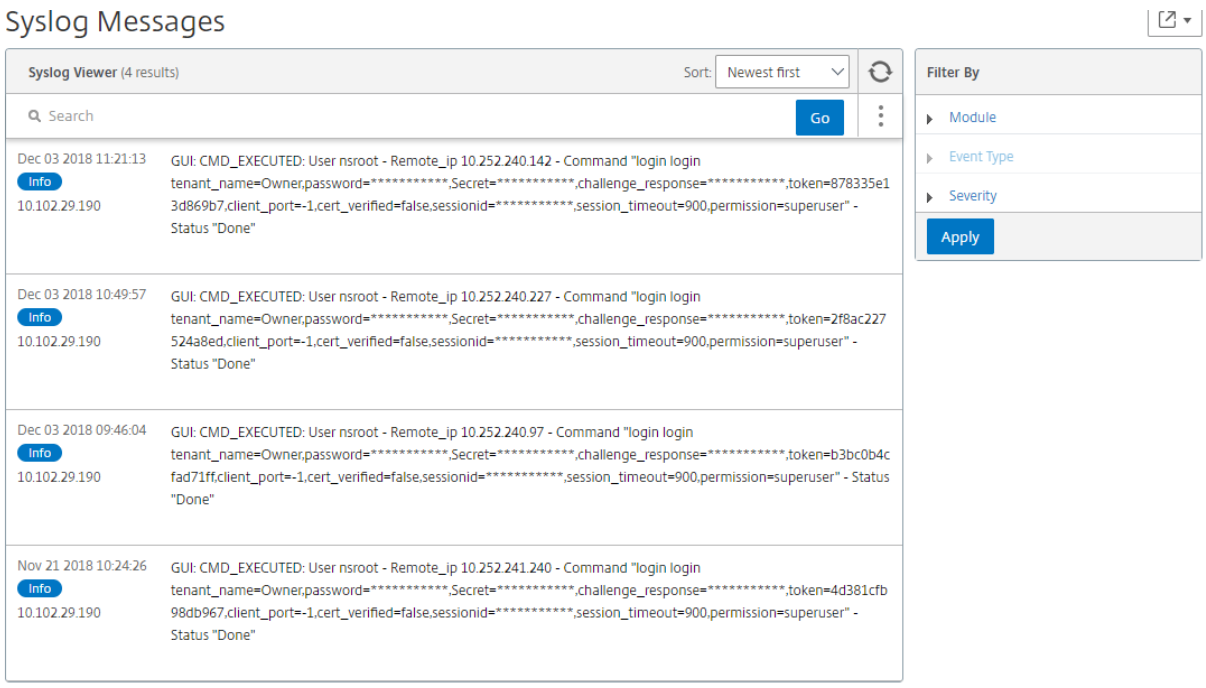
1. 导航到“系统”>“审核”。在“配置摘要”下，选择 **Syslog** 服务器。
2. 在 **Syslog** 服务器页面中，选择一个 syslog 服务器，然后单击 S**yslog** 参数。
3. 在 **Configure Syslog Parameters**（配置 Syslog 参数）页面上，指定日期和时间格式。
4. 单击确定。

要在 **Citrix ADM** 上查看 **syslog** 消息，请执行以下操作：

如果您已将实例配置为将 syslog 消息重定向到 Citrix ADM 服务器，则现在可以查看在托管 Citrix ADC 实例上生成的所有 syslog 消息。syslog 消息集中存储在 Citrix ADM 服务器的数据库中，并将在 Syslog Viewer 上提供这些消息以供审核。可以合并此日志记录信息，并基于收集的数据得出分析报告。

您可以按模块、事件类型和严重性过滤此信息。还可以配置 syslog 来记录不同类型的事件。

要查看 **Syslog** 查看器，请导航到“系统”>“审核”。在“审核”页面的“审核消息”下，选择 **Syslog** 消息。选择合适的过滤器以查看您的 syslog 消息。



配置 **SSL** 设置

February 6, 2024

SSL（安全套接字层）和 TLS（传输层安全性）是常用的安全网络连接协议，它们在用户和服务器之前提供加密通信。您可以在 Citrix Application Delivery Management (ADM) 上配置 SSL 设置，并指定连接到系统的客户端类型。

要为 **Citrix ADM** 配置 **SSL** 设置，请执行以下操作：

1. 导航到 **System**（系统）> **System Administration**（系统管理）。在 **System Settings**（系统设置）下方，单击 **Configure SSL Settings**（配置 SSL 设置）。
2. 在 **SSL** 设置 页面上，查看当前的协议设置和应用于系统的密码套件。
3. 要修改协议设置，请导航到 **Edit Settings**（编辑设置）> **Protocol Settings**（协议设置），进行所需更改。
4. 要修改应用的密码套件，请导航到 **Edit Settings**（编辑设置）> **Cipher Suites**（密码套件），进行所需更改。
5. 单击 “** 确定”，然后单击 “关闭 **”。

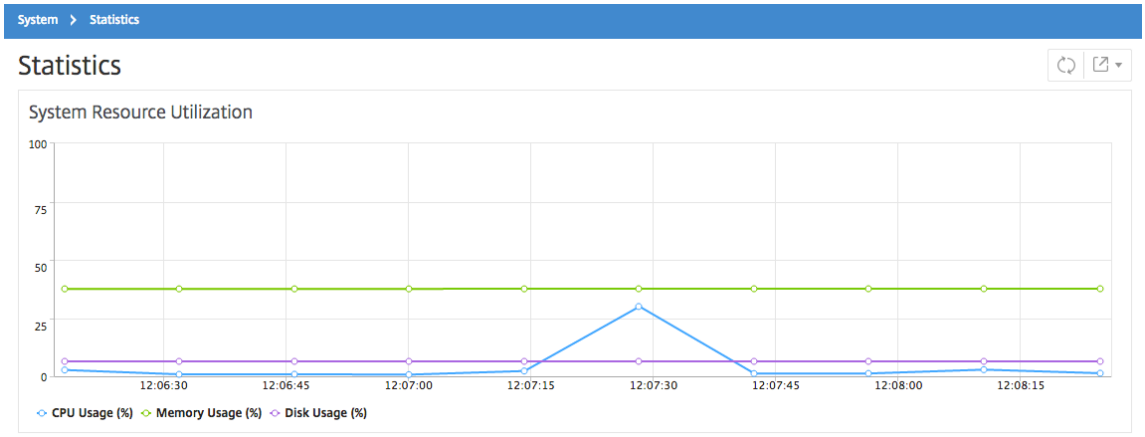
监视 **CPU**、内存和磁盘使用情况

January 29, 2024

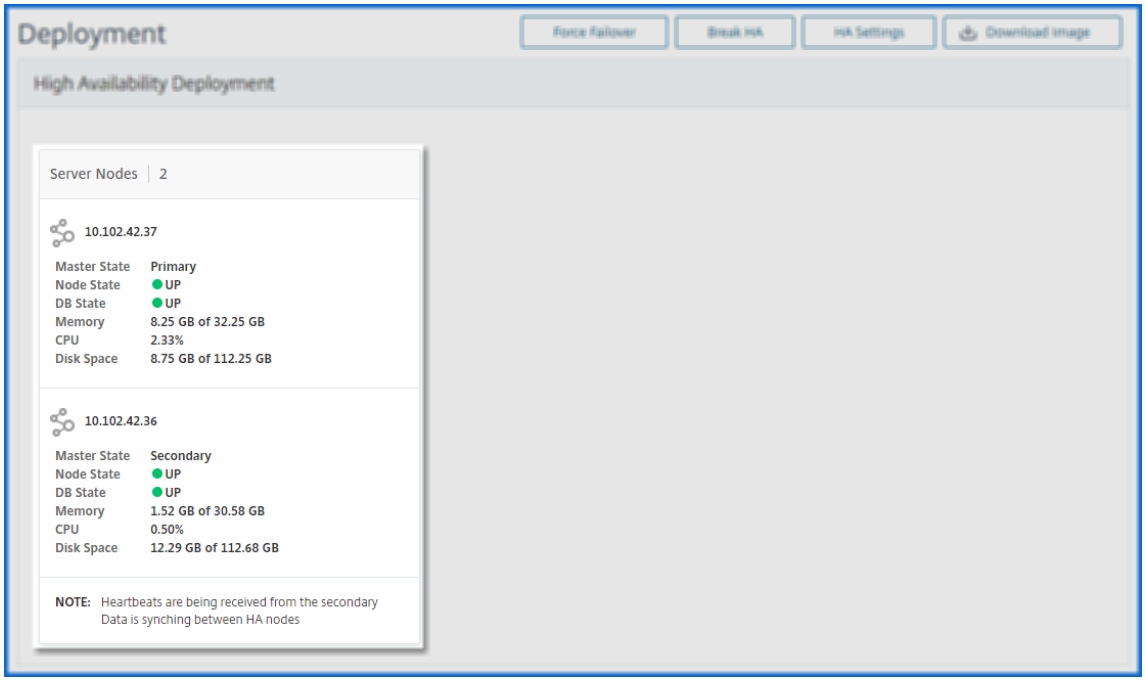
您可以使用日志和统计信息中保存的信息。此信息还显示在帮助您配置和维护 Citrix Application Delivery Management (ADM) 的报告中。

要监视 CPU、内存和磁盘使用情况，

- 独立部署。导航到“系统”**>**“统计信息”。可以查看实时 CPU、内存及磁盘利用率图表。



- 高可用性部署。导航到“系统”>“部署”。内存、CPU、磁盘空间和托管实例的统计信息以数字方式显示，如下图所示：



配置系统通知设置

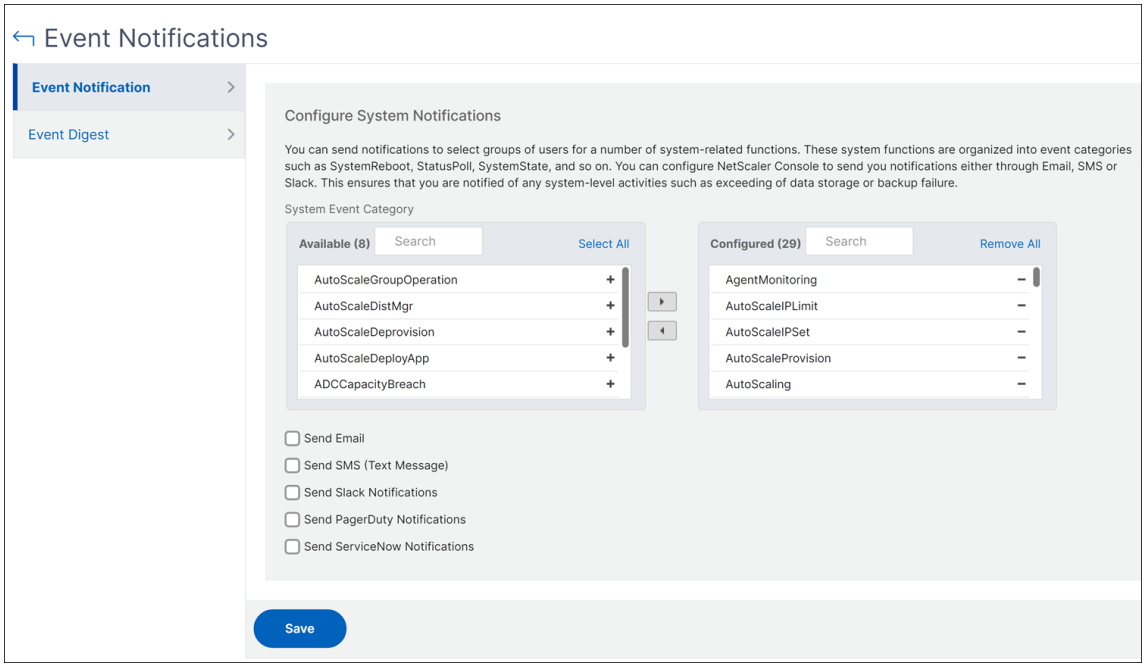
February 6, 2024

可以发送通知来为一些系统相关的功能选择用户组。这些系统功能按事件类别（例如 SystemReboot、StatusPoll、SystemState 等）划分。您可以将 Citrix Application Delivery Management (ADM) 配置为通过电子邮件或 SMS 向您发送通知。必须配置电子邮件服务器和/或短信服务 (SMS) 网关服务器，才能向用户发送电子邮件和文本通知。这可确保您将收到任何系统级活动（例如，用户登录或系统重新启动）通知。

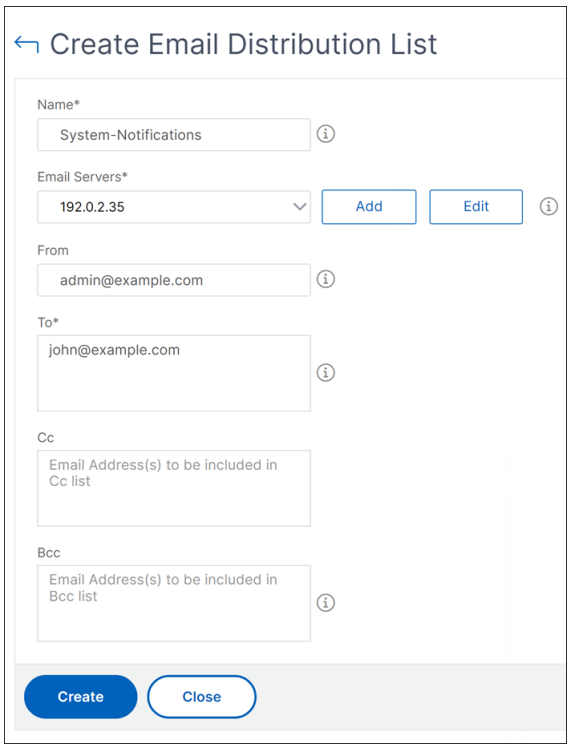
例如，当有人尝试使用 CLI 登录到 Citrix ADM 时，您可能希望向两个用户发送电子邮件通知，并且登录尝试失败。您必须选择 UserLogin 类别来配置系统通知，并且创建电子邮件通知服务器或选择要向其发送通知的现有电子邮件通讯组列表。

要在 **Citrix ADM** 上配置系统通知设置，请执行以下操作：

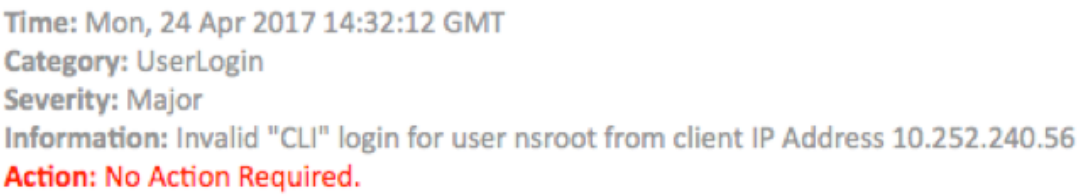
1. 定位至“系统”>“通知”。在“设置”下，单击“更改通知设置”。
2. 在“配置系统通知设置”页的“类别”下，选择一个类别，如“用户登录”。



3. 选择“发送电子邮件”，然后从下拉列表中选择电子邮件分发或单击“**+**”图标创建新的电子邮件通讯组列表，如下图所示。如果要 发送短信通知，请选择发送 **SMS**（短信），然后通过单击“**+**”图标并指定 SMS 服务器详细信息来创建 SMS 分发列表。



为特定事件类别设置通知后，每当发生属于该类别的事件时，都会使用电子邮件或 SMS 向收件人发送通知。在此示例中，当用户无法使用 CLI 登录到 Citrix ADM 时，您可以看到电子邮件通知。



将针对以下事件发送系统通知：

类别	原因
BackupFailure	系统备份失败
DataStorageExceeded	数据库存储超过许可证中指定的限制
DeviceBackupFailure	实例备份失败
哈蒙	发生系统 HA 故障切换，没有来自对等节点的检测信号，并发生数据库同步失败
HealthMontoring	CPU、RAM 或磁盘利用率超过阈值
LicensePool	许可证池超过阈值

类别	原因
许可证	许可证在申请时失败
PasswordRecovery	密码恢复失败或成功
PerfCounterThresholdHigh	性能计数器值超过限制
PerfCounterThresholdNormal	性能计数器的值正常
PolicyFailed	任何系统策略均失败
RemoteDeviceBackupFailure	远程实例备份失败
RemoteSystemBackupFailure	远程系统备份失败
RemoteSystemBackupNormal	远程系统备份成功
SSLCertThreshold	已突破证书的阈值
StatusPoll	实例状态的任何变化
SubSystemState	子系统状态的任何变化
SystemReboot	系统已重新启动
SystemState	系统状态的任何变化
TrapConfigFailure	在实例上添加 SNMP 陷阱时出现故障
UserLogin	用户身份验证失败

生成技术支持文件

February 6, 2024

Citrix 建议您在联系技术支持人员调试问题之前，先生成 Citrix Application Delivery Management (ADM) 数据和统计数据的存档。存档是可以发送给技术支持团队的 TAR 文件。

> 注意
>
> 对于高可用性模式下的 Citrix ADM 服务器，您可以从任 一服务器生成技术支持文件。Citrix 建议您不要使用负载平衡虚拟服务器 IP 地址来生成技术支持文件。

要配置和发送来自 **Citrix ADM** 的技术支持文件，请执行以下操作：

1. 导航到“系统”>“诊断”>“技术支持”，然后单击“生成技术支持文件”。
2. 在“生成支持文件”页上，选择以下选项：

- **Collect Debug Logs**（收集调试日志）- 选择此选项以收集 afdecoder 日志。
- **Duration**（持续时间）- 输入应收集调试日志的持续时间。如果启用了“收集调试日志”选项，您将只会看到此选项。
- **Collect Data Distribution**（收集数据分发）- 选择此选项以从数据库中收集各种各样的日志。

```
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. 您可以通过两种方式将技术支持文件发送给支持团队：

   a) 您可以将文件从 ADM GUI 下载到本地存储，然后使用 Web 浏览器上载到 CIS。

   b) 您还可以通过在 ADM 控制台上运行脚本将技术支持文件上载到 Citrix Insight Services (CIS) 网站。

      i. 使用 SSH 登录 ADM 控制台。

      ii. 切换到命令行管理程序提示符并键入：

      /mps/collector_upload.pl

下面给出了完整的命令，其中包含您需要提供的属性：

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr <sr>] [-description <description>] [-debug] <file>
<!--NeedCopy-->
```

运行 Perl 脚本的好处是您不必将技术支持文件从 ADM 下载到本地系统，然后将其上载到 CIS。作为一个选项，您可以使用 ADM 控制台的代理直接将文件上载 到 CIS。

确保您在 CIS 上有一个帐户。您可以使用您的 Citrix 帐户凭据将文件上载到 CIS。

如果您没有代理服务器怎么办？或者，如果您在使用 SSL 转发代理时遇到了一些问题怎么办？（如果 Perl 脚本不信任代理服务器的根证书，则可能会发生这种情况。）
您仍然可以直接从 ADM shell 将文件上载到 CIS。

> 注意
>
> 在 ADM 无法从控制台将文件上载到 CIS 的情况下，您仍然可以下载文件并通过电子邮件将其发送给 Citrix 技术支持团队。或者，您可以将文件从 ADM 下载到本地存储，然后使用 Web 浏览器上载到 CIS。

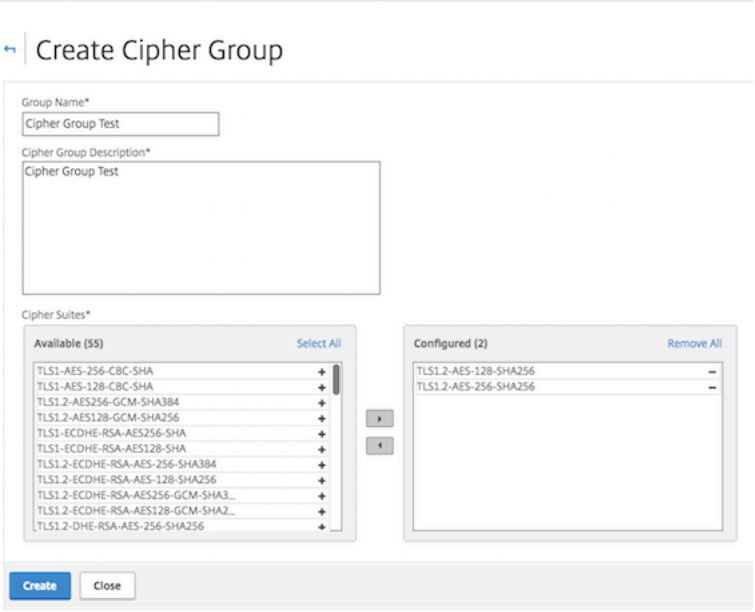
配置密码组

January 29, 2024

密码组是绑定到 Citrix Application Delivery Controller (ADC) 实例上的 SSL 虚拟服务器、服务或服务组的一组密码套件。密码套件包括协议、密钥交换 (Kx) 算法、身份验证 (Au) 算法、加密 (Enc) 算法及消息身份验证代码 (Mac) 算法。

要在 **Citrix ADM** 上添加密码组，请执行以下操作：

1. 导航到 **System**（系统）> **Cipher Groups**（密码组），然后单击 **Add**（添加）。
2. 在 **Create Cipher Group**（创建密码组）页面上，输入以下详细信息：
   - **Group Name**（组名）- 密码组的名称。
   - **Cipher Group Description**（密码组说明）–提供密码组的说明。
   - **Cipher Suites**（密码套件）–单击“Add”（添加）从“Available”（可用）列表中选择密码套件，然后将所选（或全部）密码套件移至“Configured”（已配置）列表。
3. 单击创建。



创建 **SNMP** 陷阱目标、管理者社区和用户

February 6, 2024

每当 Citrix ADM 出现异常情况时，都会生成 SNMP 陷阱。然后将陷阱发送到称为陷阱目标服务器的远程设备或 *SNMP* 陷阱目标。您可以从名为 SNMP 管理器的远程设备查询 *SNMP* 代理以获取特定于系统的信息。该代理随后会在管理信息库 (MIB) 搜索请求的数据，并将其发送到 SNMP 管理器。

要在 **Citrix ADM** 上创建 **SNMP** 陷阱目标，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Trap Destinations**（陷阱目标）。

2. 在 **SNMP** 陷阱下，单击“添加”创建 SNMP 陷阱，然后指定以下详细信息：
    - 版本。选择要使用的 SNMP 版本。
    - 目标服务器。陷阱目的地的名称或 IP 地址。
    - **Port**（端口）。输入陷阱目的地的端口。该端口默认设置为 162。
    - 社区。指定向陷阱侦听器发送陷阱时要使用的社区字符串。
3. 单击创建。

> 注意
>
> 如果您正在创建 SNMP v3 陷阱目的地，请指定要将陷阱绑定到的 SNMP 用户凭据。要添加 SNMP 用户凭据，请单击“插入”，然后从可用 SNMP 用户列表中添加用户。

要创建 **SNMP** 管理员社区，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Managers**（管理器）。
2. 在 **SNMP** 管理器下，单击“添加”创建 SNMP 管理器社区，然后指定以下详细信息：
    - **SNMP** 管理器。输入 SNMP 管理器的名称或 IP 地址。
    - 社区。指定向陷阱侦听器发送陷阱时要使用的社区字符串。
3. 或者，您可以选中“启用管理网络”复选框来指定网络 掩码，即 SNMP 管理器网络的子网掩码。
4. 单击创建。

要创建 **SNMP** 用户，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Users**（用户）。
2. 在 **SNMP** 用户下，单击“添加”。
3. 输入用户名并从菜单为用户分配安全级别。
4. 根据您分配给用户的安全级别，提供额外的身份验证协议，如身份验证协议、隐私密码和分配 SNMP 视图。

配置和查看系统警报

February 6, 2024

您可以启用和配置一组警报，以监视 Citrix Application Delivery Management (ADM) 服务器的运行状况。您应该配置系统警报，以确保您可以了解任何严重或重大系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。对于有些警报类别（例如 cpuUsageHigh 或 memoryUsageHigh），您可以为每项设置阈值并定义严重性（例如“Critical”（严重）或“Major”（重大））。对于有些类别（例如 inventoryFailed 或 loginFailure），

只能定义严重性。当警报类别（例如 MemoryUsageHigh）超出阈值时，或发生与警报类别对应的事件（例如 登录失败）时，系统中将记录一条消息，您可以将该消息作为 syslog 消息查看。可以进一步设置通知以接收对应于警报设置的电子邮件或 SMS。

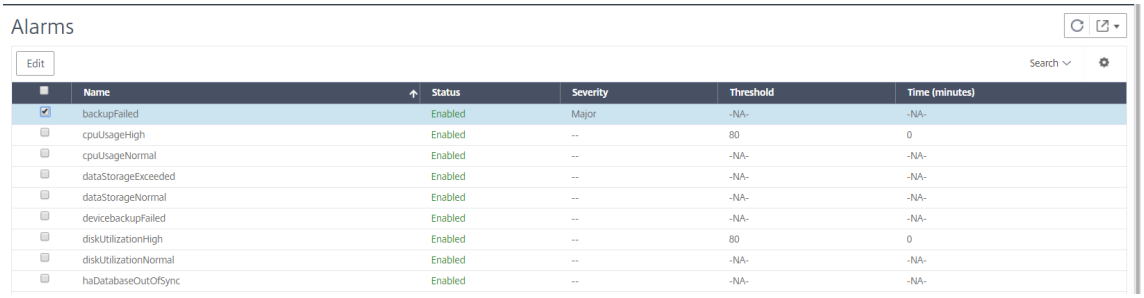
可以分配或修改警报的严重性。您可以分配的严重性级别为“严重”、“严重”、“次要”、“警告”和“信息”。

考虑一种情况，您希望在备份尝试失败时监视。您可以启用 BackupFailed 警报并为其分配严重性，例如“严重”。每当 Citrix ADM 尝试备份系统文件以及尝试失败时，都会触发警报。您可以在 Citrix ADM 上查看消息，也可以通过电子邮件或短信获取通知。

要配置警报，必须选择 BackupFailed 警报并将严重性级别指定为“主要”。默认情况下，启用警报。

要使用 **Citrix ADM** 配置和查看系统警报，请执行以下操作：

1. 导航到“系统”>“警报”。

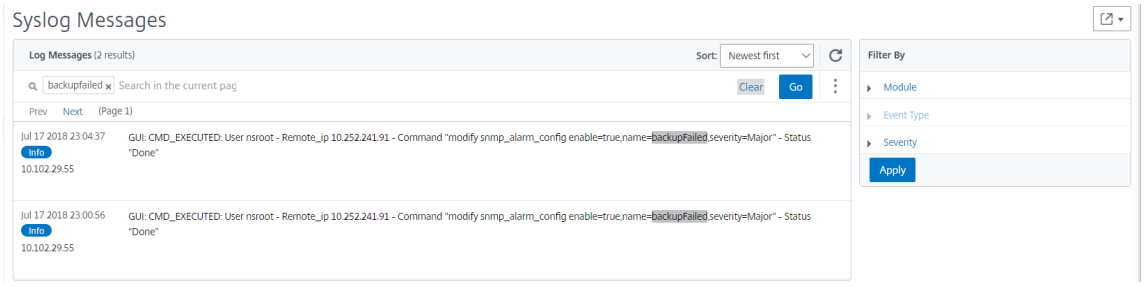


2. 选择要配置的警报（例如，备份失败），然后单击“编辑”修改其设置。
3. 默认情况下，启用警报。分配严重性级别（例如：主要），然后单击“确定”。

> 注意
>
> 对于少数警报，您无法设置阈值。
> 触发警报后，可以查看以 syslog 消息形式存在的生成事件。

要使用 **Citrix ADM** 查看由备份失败警报生成的事件，请执行以下操作：

1. 导航到“系统”>“审核”。
2. 在“审核”页面的“审核消息”下，选择 **Syslog** 消息。
3. 在搜索字段中，键入警报的名称。
   在此示例中，您可以看到为失败的备份尝试生成了一个事件。



您还可以设置通知以在触发警报时向您发送电子邮件或 SMS（短信服务）文本。有关如何配置系统通知的信息，请参阅 如何配置 Citrix ADM 的系统通知设置。

作为 **API** 代理服务器的 **Citrix ADM**

February 6, 2024

除了由于自身的管理和分析功能而能够接收 NITRO REST API 请求外，Citrix Application Delivery Management (Citrix ADM) 还可以充当其托管实例的 REST API 代理服务器。REST API 客户端可以将 API 请求发送到 Citrix ADM，而不是将 API 请求直接发送到托管实例。Citrix ADM 可以区分它其须响应的 API 请求与其必须原样转发至托管实例的 API 请求。

作为 API 代理服务器，Citrix ADM 具有以下优势：

- 验证 **API** 请求。Citrix ADM 按照配置的安全策略和基于角色的访问控制 (RBAC) 策略来验证所有 API 请求。Citrix ADM 还可以识别租户，确保 API 活动不会跨越租户边界。
- 集中审核。Citrix ADM 维护与其托管实例有关的所有 API 活动的审核日志。
- 会话管理。Citrix ADM 使 API 客户端不必维护与托管实例的会话的任务。

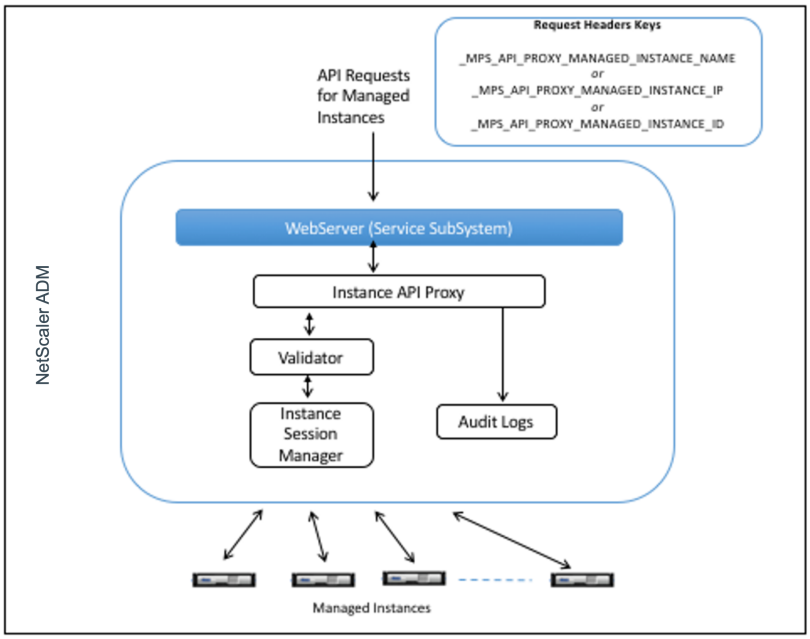
Citrix ADM 如何作为 **API** 代理服务器运行

如果希望 Citrix ADM 将请求转发到托管实例，则可以将 API 客户端配置为在 API 请求中包含以下任何一个 HTTP 标头：

- _MPS_API_PROXY_MANAGED_INSTANCE_NAME。托管实例的名称。
- _MPS_API_PROXY_MANAGED_INSTANCE_IP。托管实例的 IP 地址。
- _MPS_API_PROXY_MANAGED_INSTANCE_ID。托管实例的 ID。

存在这些 HTTP 标头中的任何一个可帮助 Citrix ADM 将 API 请求识别为它必须转发给托管实例的 API 请求。标头值帮助 Citrix ADM 确定必须将请求转发到的托管实例。

下图中说明了此流程：



如上图所示，当请求中出现其中一个 HTTP 标头时，Citrix ADM 按如下方式处理请求：

1. 在不修改请求的情况下，Citrix ADM 将请求转发到实例 API 代理引擎。
2. 实例 API 代理引擎将 API 请求转发至验证程序，并将 API 请求的详细信息记录在审核日志中。
3. 验证程序确保请求没有违反配置的安全策略、RBAC 策略、租赁边界等。它会执行额外的检查，例如检查以确定托管实例是否可用。

如果 API 请求有效且可以转发到托管实例，Citrix ADM 会识别由实例会话管理器维护的会话，然后将请求发送到托管实例。

如何将 **Citrix ADM** 用作 **API** 代理服务器

以下示例显示了一个 API 客户端向 IP 地址为 192.0.2.5 的 Citrix ADM 服务器发送的 REST API 请求。Citrix ADM 需要将请求原样转发到 IP 地址为 192.0.2.10 的托管实例。所有示例都使用 _MPS_API_PROXY_MANAGED_INSTANCE_IP 标头。

在向 Citrix ADM 发送 API 请求之前，API 客户端必须：

- 登录 Citrix ADM
- 获取会话 ID
- 在后续的 API 请求中包含会话 ID。

登录 API 请求的形式如下：

```
1    POST /nitro/v2/config/login HTTP/1.1
```



```
    Host: 192.0.2.5
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {

        "login":
        {

            "username":"******",
            "password":"*******"
         }

     }

<!--NeedCopy-->
```

Citrix ADM 响应登录请求，显示包括会话 ID 的响应信息。以下示例响应正文显示了会话 ID：

```
{


  "errorcode": 0,
  "message": "Done",
  "operation": "add",
  "resourceType": "login",
  "username": "***********",
  "tenant_name": "Owner",
  "resourceName": "******",
  "login": [
    {

      "tenant_name": "Owner",
      "permission": "superuser",
      "session_timeout": "36000",
      "challenge_token": "",
      "username": "",
      "login_type": "",
      "challenge": "",
      "client_ip": "",
      "client_port": "-1",
      "cert_verified": "false",
      "sessionid": "##
    D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
      "token": "b2f3f935e93db6a"
     }

  ]

 }

<!--NeedCopy-->
```


示例 **1**：检索负载平衡虚拟服务器统计信息

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
    GET /nitro/v1/stat/lbvserver HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    Accept: application/json
    Cache-Control: no-cache
<!--NeedCopy-->
```

示例 **2**：创建负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
    POST /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
    Host: 192.0.2.5
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {
 "lbvserver":{
 "name":"sample_lbvserver","servicetype":"HTTP","ipv46":"10.102.1.11","
    port":"80" }
  }

<!--NeedCopy-->
```

示例 **3**：修改负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
    PUT /nitro/v1/config/lbvserver HTTP/1.1
    Host: 192.0.2.5
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Content-Type: application/json
    Accept: application/json
    Cache-Control: no-cache

    {
 "lbvserver":{
```



```
 "name":"sample_lbvserver","appflowlog":"DISABLED" }
  }

<!--NeedCopy-->
```

示例 **4**：删除负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
    DELETE /nitro/v1/config/lbvserver/sample_lbvserver HTTP/1.1
    Host: 192.0.2.5
    Cookie: SESSID=##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    Cache-Control: no-cache

<!--NeedCopy-->
```

常见问题解答

February 6, 2024

本部分内容提供了有关以下 Citrix Application Delivery Management (Citrix ADM) 功能的常见问题解答。单击下表中的功能名称可以查看该功能的常见问题解答列表。

分析	身份验证	配置管理
证书管理	部署	部署（灾难恢复）
事件管理	实例管理	样书
系统管理		

分析

我是否要在以单跳模式部署的 **Citrix Gateway** 实例上启用 **EUEM** 虚拟通道

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则 Citrix ADM 上仍会显示剩余的 HDX Insight 数据。

EUEM 虚拟通道是在 Citrix Virtual Desktops 应用程序 (VDA) 上运行的默认服务。如果未运行，请在 VDA 服务中启动“Citrix 最终用户体验监视”过程。

我如何使 **Citrix ADM** 能够监视 **Web** 应用程序和虚拟桌面流量**?**

1. 导航到基础架构 > 实例，然后选择要启用分析的 Citrix Application Delivery Controller (Citrix ADC) 实例。
2. 从“操作”下拉列表中选择“启用/禁用 **Insight**”。
3. 在打开的 **Configure Insight**（配置洞察）页面上，选择要在其上启用分析的所有虚拟服务器，并单击 **Enable AppFlow**（启用 AppFlow）。有关更多详细信息，请参阅如何在实例上启用分析。

> 注意
>
> 对于 11.0 版本、65.30 版本及更高版本的 Citrix ADC 实例，Citrix ADM 上没有显式启用安全智能分析的选项。确保在 Citrix ADC 实例上配置 AppFlow 参数，以便 Citrix ADM 开始接收安全智能分析通信以及 Web 智能分析通信。有关如何在 Citrix ADC 实例上设置 AppFlow 参数的详细信息，请参阅使用配置实用程序设置 AppFlow 参数。

添加 **Citrix ADC** 实例后，**Citrix ADM** 是否会自动开始收集分析信息**?**

否。您必须首先对由 Citrix ADM 管理的 Citrix ADC 实例中托管的虚拟服务器启用分析。有关更多详细信息，请参阅如何在实例上启用分析。

我是否需要访问各个 **Citrix ADC** 设备才能启用分析

否。所有配置都通过 Citrix ADM 用户界面完成，该界面列出了特定 Citrix ADC 实例上托管的虚拟服务器。有关更多详细信息，请参阅如何对实例启用分析。

可以在 **Citrix ADC** 实例上列出哪些虚拟服务器类型以启用分析**?**

当前 Citrix ADM 用户界面上列出以下虚拟服务器以便启用分析：

- 负载平衡虚拟服务器
- 内容交换虚拟服务器
- VPN 虚拟服务器
- 缓存重定向虚拟服务器

如何将额外的磁盘连接到 **Citrix ADM?**

要将额外的磁盘连接到 Citrix ADM，请执行以下操作：

1. 关闭 Citrix ADM 虚拟机。

2. 在 Hypervisor 中，将所需磁盘大小的额外磁盘连接到 Citrix ADM 虚拟机。

   例如，让我们考虑您希望将磁盘空间增加到 200 GB, 在 Citrix ADM 虚拟机 120 GB. 在这种情况下，您需要连接 200 GB 而不是 80 GB 的磁盘空间。新附加的 200 GB 磁盘空间将用于存储数据库数据、Citrix ADM 日志文件。现有的 120 GB 磁盘空间将用于存储核心文件、操作系统日志文件等。

3. 启动 Citrix ADM 虚拟机。

您所说的收集器未在 **Citrix ADC** 实例上配置是什么意思**?**

收集器接收由 Citrix ADC 设备生成的 AppFlow 记录。

启用 AppFlow 功能后，Citrix ADM 会从 Citrix ADC 实例接收 Security Insight 和 Web Insight 流量。在 Citrix ADC 实例上启用 AppFlow 功能时，必须至少指定一个将 AppFlow 记录发送到的收集器。如果未在 Citrix ADC 实例上配置收集器，Citrix ADM 不会接收来自这些实例的流量。

例如，将五个 Citrix ADC 实例添加到 Citrix ADM 中。如果没有为两个实例指定收集器，则不会有流量流向 Citrix ADM。自助诊断程序检测到问题，并将问题显示为“未在 2 个实例上配置收集器。”

有关如何配置 AppFlow 功能的更多信息，请参阅 配置 AppFlow 功能。

身份验证

身份验证请求的负载平衡是什么

通过身份验证服务器负载平衡功能，Citrix ADM 可以对定向至外部身份验证服务器的身份验证请求执行负载平衡。对身份验证服务器执行负载平衡可确保在多个身份验证服务器之间分摊身份验证负载，从而避免某个身份验证服务器过载。可以创建身份验证服务以使用身份验证协议（例如，LDAP、RADIUS 或 TACACS）与现有外部身份验证服务器连接，并从其获取用户信息。

是否需要级联外部身份验证服务器

级联外部身份验证服务器提供不间断的身份验证处理，从而在某个身份验证服务器发生故障时允许对合法用户进行访问。可以级联的身份验证服务器的类型没有限制。可以全是 RADIUS 服务器或全是 LDAP 服务器，也可以是 RADIUS 服务器和 LDAP 服务器组合。

可以级联多少个外部身份验证服务器

在 Citrix ADM 中，最多可以级联 32 个外部身份验证服务器。

外部身份验证失败时，是否有备用方法

在某些情况下，即使您级联了多台服务器，外部身份验证也可能完全失败。例如，外部服务器可能无法访问，或者可能没有在任何外部身份验证服务器中输入新用户的凭据。为了防止在此类情况下锁定用户，可以启用回退本地身份验证。有关更多详细信息，请参阅回退本地身份验证。

什么是回退本地身份验证

回退本地身份验证是当外部身份验证失败时可以在本地对用户进行身份验证的一种方式。如果外部身份验证失败，Citrix ADM 将访问本地用户数据库以对用户进行身份验证。

在 Citrix ADM 中，导航到“系统”>“身份验证”>“身份验证 配置”。在此页面上，可以将多个外部身份验证服务器添加到一个级联中，并可以选择 **Enable fallback local authentication**（启用回退本地身份验证）选项。

什么是提取外部用户组

如果添加了用于验证用户的外部服务器，则可以将现有用户组导入（提取）到 Citrix ADM 中。必须导入一次用户组，并向用户组提供组权限，而不是导入各个用户并为其提供单独的权限。不必在 Citrix ADM 上重新创建用户。

为什么需要指定组权限

使用 Citrix ADC 的负载平衡功能时，可以将 Citrix ADM 与外部身份验证服务器集成，并从身份验证服务器导入用户组信息。登录 Citrix ADM，在 Citrix ADM 中手动创建相同的组信息，并为这些组分配权限。用户和用户组权限在 Citrix ADM 中进行管理，而不是在外部服务器中进行管理。用户在外部服务器上有基于角色的不同访问权限。还应在 Citrix ADM 中为用户配置相同的权限。不是为每个用户单独配置权限，而是可以配置组级别权限，以便用户组成员可以在负载平衡的虚拟服务器上访问特定服务。可以分配的典型权限是管理 Citrix ADC 实例、Citrix SDX 实例、虚拟服务器等权限，以便该组的用户只能管理那些实例或虚拟服务器。可以在以后编辑指定给用户的组级别权限。甚至可以删除一个或多个用户组；其他组用户仍可以在 Citrix ADM 中操作。

配置管理

我是否可以使用 **Citrix ADM** 同时跨多个 **Citrix ADC** 实例执行配置**?**

是，可以使用配置作业在多个 Citrix ADC 实例之间执行配置。

Citrix ADM 上的配置作业是什么**?**

作业是可以在一个或多个托管实例上创建并运行的一组配置命令。可以使用 Citrix ADM GUI 创建作业以在实例上进行配置更改、在网络中多个实例上复制配置以及录制和播放配置任务。还可以将录制的任务转换为 CLI 命令。

可以使用 Citrix ADM 的配置作业功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

我是否可以在 **Citrix ADM** 中使用内置模板计划作业**?**

是的！可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，可以使用内置模板选项计划作业来配置 syslog 服务器。您可以选择立即运行作业，也可以选择将作业安排在以后运行。

可以保存以前创建的一个作业的配置，在修改命令、参数、配置来源和目标实例后重新运行该作业。当必须在不同的实例上运行同一组命令或作业遇到错误并停止进一步执行时，这很有用。

证书管理

从 **Citrix ADM** 中删除 **SSL** 证书是否会导致从 **Citrix ADC** 实例中删除证书**?**

否

部署

默认用户名和密码是什么**?**

- 完成初始网络配置后，可以使用默认用户名和密码 (nsrecover/nsroot) 从虚拟机管理程序或 SSH 控制台登录 Citrix ADM。
- 用于从 GUI 登录的默认用户名和密码为 *nsroot/nsroot*。

如何更改默认密码**?**

要更改密码，请执行以下操作：

1. 在 Citrix ADM 中，导航到“系统”>“用户管理”>“用 户”。

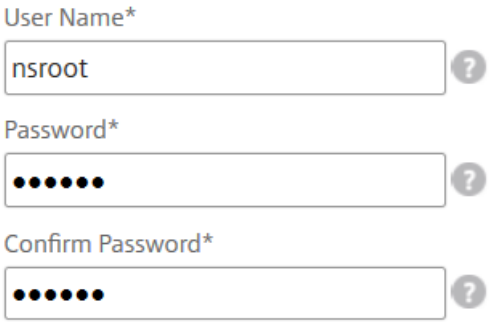
   此时将显示“用户”页。

2. 选择用户名 **nsroot** ，然后单击 编辑。

   此时将显示“配置系统用户”页。

3. 选择“更改密码”并创建您选择的密码。



4. 单击确定。

   现在，您可以使用新密码从 GUI 和 Hypervisor 或 SSH 控制台登录。

   > 注意
   >
   > 不能修改用户名。

如何重置密码**?**

您可以查看此 文档 来重置密码。

在 **HA** 对中，如果在主节点中更改了密码，并且稍后选择了“中 断 **HA** 对”选项，则会出现什么行为

您可以使用新密码登录到两个独立节点。

如果两台独立服务器的密码不同，在高可用性对中部署这两台服务器会有什么影响**?**

当您将两台独立服务器部署到高可用性对时，建议两台服务器都使用默认密码。

高可用性配置已完成，但无法访问主节点 **GUI**。可能的原因是什么**?**

配置需要几分钟时间才能生效。您可以在几分钟后再次尝试访问。

高可用性配置已完成，但无法访问浮动 **IP** 地址 **GUI**。可能的原因是什么**?**

完成 HA 配置后，您需要首先访问主节点 GUI 并完成部署。有关更多信息，请参阅 将主节点和辅助节点部署为高可用性对。部署完成后，服务器将重新启动并准备好进行高可用性部署。然后，您可以访问浮动 IP 地址 GUI。

Citrix ADM 独立版和 **Citrix ADM** 高可用性支持哪些数据库**?**

Citrix ADM 独立版和 Citrix ADM HA 都支持 PostgreSQL。

辅助节点可能会丢失哪些数据**?**

辅助节点侦听主节点通过 Citrix ADM 数据库发送的检测信号消息。如果辅助节点未收到检测信号的时间超过 180 秒，辅助节点将在主节点上执行基于 SSH 的检查。如果检测信号和基于 SSH 的检查失败，则认为主节点已关闭。

在这种情况下，辅助节点将接管成为主节点，180 秒的时间范围可以被视为辅助节点可能丢失的数据。

如果主节点关闭，会发生什么情况**?**

辅助节点将接管并成为主节点。

如何重新安装出现故障的节点**?**

建议安装全新的 VM 版本。要重新安装，请执行以下操作：

1. 打破 HA 对。导航到“系统”>“部署”

   此时将显示部署页面。单击 **Break HA**（中断高可用性）
2. 从 Hypervisor 中删除故障节点。
3. 将.xva 映像文件导入虚拟机管理程序。
4. 在“Console”（控制台）选项卡中，使用初始网络配置配置 Citrix ADM。有关详细信息，请参阅 注册并部署第一台服务器（主节点） 和 注册并部署第二台服务器（辅助节点）。
5. 重新部署 HA 对。

Citrix ADM 是否支持 **SAN** 存储**?**

Citrix 建议您在本地存储上托管 Citrix ADM VHD。当托管在 SAN 中的存储设备上时，Citrix ADM 可能无法按预期工作。

Citrix ADM 是否支持其他磁盘**?**

是。默认情况下，Citrix ADM HA 对的新安装会分配 120 GB 的存储空间。对于超过 120 GB 的存储空间，您可以再添加一个磁盘，最大存储空间为 3 TB。不支持再添加多个磁盘。

禁用高可用性对后，配置的浮动 **IP** 地址会发生什么**?**

浮动 IP 地址将无法再访问，您需要重新部署高可用性对。

我是否可以在重新部署时提供不同的浮动 **IP** 地址**?**

是。可以配置新的浮动 IP 地址。

为什么辅助节点 **GUI** 无法访问**?**

辅助节点只是一个只读副本服务器，并且仅在主节点因任何原因关闭时才充当主节点。Citrix 建议访问主节点 GUI 或浮动 IP 地址 GUI。

如果主节点长时间关闭，是否仍然可以使用浮动 **IP** 地址 **GUI** 完成配置**?**

是。您仍然可以继续进行配置，并且配置将保存在辅助节点中。主节点恢复后，将同步所有配置。

如果将来有必要更改主节点 **IP** 地址或辅助节点 **IP** 地址或浮动 **IP** 地址（例如，将其更改为 **IPv6**），建议执行哪些解决方案**?**

如果不中断高可用性对，则不支持更改高可用性对中的 IP 地址。

要更新主节点或辅助节点 IP 地址，请执行以下操作：

1. 打破 HA 对。导航到“系统”>“部署”。

   此时将显示“部署”页。单击 **Break HA**（中断高可用性）

   a) 使用 SSH 客户端或从虚拟机管理程序登录到主节点。

   b) 使用 `nsrecover` 作为用户名并输入您设置的密码。

   c) 输入 网络配置。执行 Regi ster 中提供的 步骤 **3** 中的步骤，然后部署第一台服务器（主节点）。

      在初始网络配置期间，您可以提供不同的 IP 地址。

   d) 对辅助节点执行相同的过程，然后继续执行 注册和部署第二台服务器（辅助节点）中提供的 步骤 **3** 中的过程。

要更新浮动 IP 地址，请执行以下操作：

1. 导航到“系统”>“部署”。

   此时将显示“部署”页。

   a) 单击 **HA Settings**（高可用性设置）。

   b) 单击 **Configure Floating IP Address for High Availability Mode**（为高可用性模式配置浮动 IP 地址）。

   c) 输入浮动 IP 地址，然后单击“确定”。

ADM 是否支持 **AMD** 处理器**?**

不是。ADM 不支持 AMD 处理器

部署（灾难恢复）

主站点与灾难恢复站点之间的复制频率有多高**?**

主站点与灾难恢复站点之间的复制是实时的。

在灾难恢复站点启动备份脚本后，在主站点恢复并完全运行之前，灾难恢复站点是否会成为临时主站点**?**

否。灾难恢复站点现在将成为主站点。

如果选择了“中断 **HA** 对”选项，则两个节点将作为独立服务器运行。由于 **DR** 支持不适用于独立服务器，如果选择“**Break HA pair**”（断开高可用性对），灾难恢复站点会发生什么情况**?**

如果选择“Break HA pair”（断开高可用性对）选项，主站点与灾难恢复站点之间的复制将终止。作为重新部署高可用性对的一部分，您需要重新配置 DR 站点。

事件管理

我如何使用 **Citrix ADM** 跟踪在我的托管 **Citrix ADC** 实例上生成的所有事件**?**

作为网络管理员，您可以查看一些详细信息，例如，您的 Citrix ADC 实例上的配置更改、登录情况、硬件故障、阈值违反和实体状态变化，以及特定实例上的事件及其严重性。可以使用 Citrix ADM 事件控制板查看您的所有 Citrix ADC 实例上生成的报告，了解严重事件严重性详细信息。

什么是事件规则

使用 Citrix ADM，您可以配置规则来监视特定事件。事件规则使监视在 Citrix ADM 基础架构中生成的大量事件变得更加容易。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。

您可以创建筛选器的条件包括严重性、Citrix ADC 实例、类别和故障对象。可以分配给事件的操作包括发送电子邮件通知、将来自托管 Citrix ADC 实例的 SNMP 陷阱转发到 Citrix ADM 以及发送 SMS 通知。

实例管理

Citrix ADM 中的数据中心是什么**?**

Citrix ADM 数据中心是位于特定地理位置的 Citrix ADC 实例的逻辑分组。每台服务器都可以监视和管理数据中心内的多个 Citrix ADC 实例。您可以使用 Citrix ADM 服务器来管理来自托管实例的系统日志、应用程序流量和 SNMP 陷阱等数据。有关配置数据中心的详细信息，请参阅如何在 Citrix ADM 中为地理地图配置数据中心。

Citrix ADM 支持哪些不同的 **Citrix** 设备**?**

实例是要从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备。必须将这些实例添加到 Citrix ADM 服务器中。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 中：

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN WO
- Citrix SD-WAN PE

您可以在首次设置 Citrix ADM 服务器时添加实例，也可以在以后添加实例。

什么是实例配置文件**?**

Citrix ADM 使用实例配置文件来访问特定实例。

实例配置文件包含用于访问一个或多个实例的用户名和密码。每个实例类型都有一个默认配置文件。例如，ns-root-profile 是 Citrix ADC 实例的默认配置文件。它包含默认的 Citrix ADC 管理员凭据。更改访问实例所需的凭据时，可以为那些实例定义自定义实例配置文件。

我们是否可以在 **Citrix ADM** 中添加无限数量的 **SD-WAN** 实例**? Citrix ADM** 是否可以处理 **SD-WAN** 的所有标量计数器和矢量计数器**?**

目前，可以添加到 Citrix ADM 的 SD-WAN 实例没有许可证限制。Citrix ADM 有一组内置报告，可在内部轮询标量计数器和矢量计数器。

我是否可以在 **Citrix ADM** 中重新发现多个 **Citrix VPX** 实例**?**

可以，您可以在 Citrix ADM 中重新发现多个 Citrix **VPX** 实例，以了解实例的最新状态和配置。

导航到“网络”>“实例”>“**NetScaler VPX**”，选择要重新发现的实例，然后在“操作”下拉列表中单击“重新发现”。有关更多信息，请参阅 如何重新发现多个 VPX 实例。

是否可以在 **Citrix SDX** 上安装 **Citrix ADM?**

否

样书

样书可以用于配置在不同版本的 **Citrix ADC** 软件上运行的不同 **Citrix ADC** 实例吗

是的，如果不同版本的命令之间没有差异，则可以使用样书来配置在不同版本上运行的不同 Citrix ADC 实例。

如果使用样书同时配置多个 **Citrix ADC** 实例，并且一个 **Citrix ADC** 实例的配置失败，会发生什么情况**?**

如果将配置应用于 Citrix ADC 实例失败，则不会应用配置，而不会再应用任何实例，并回滚已应用的配置。

通过 **Citrix ADC** 进行的 **Citrix ADC** 备份是否包括通过样书应用的配置

是

系统管理

是否可以将主机名分配给我的 **Citrix ADC** 服务器**?**

可以，您可以分配主机名来标识您的 Citrix ADM 服务器。要指定主机名，请导航至 **System**（系统）> **System Administration**（系统管理）> **System Settings**（系统设置），并单击 **Change Hostname**（更改主机名）。

主机名将显示在 Citrix ADM 的通用许可证上。有关详细信息，请参阅如何将主机名分配给 Citrix ADM 服务器。

是否可以备份和还原我的 **Citrix ADM** 配置**?**

是，可以备份配置文件（NTP 文件和 SSL 证书）、系统数据、基础结构和应用程序数据以及所有 SNMP 设置。如果您的 Citrix ADM 变得不稳定，您可以使用备份的文件将 Citrix ADM 恢复到稳定状态。

要备份和恢复 Citrix ADM 的配置，请导航到 “系统”>“高级设置”> “备份文件”，然后视情况单击 “备 份”或 “还原”。有关详细信息，请 参阅如何在 Citrix ADM 上备份和恢复配置。

Citrix 建议在执行升级之前或出于防范性措施的原因，使用此功能。

Citrix ADM 上的阈值和警报是什么**?**

可以设置阈值和警报来监视 Citrix ADC 实例的状态及监视托管实例上的实体。

如果计数器值超过阈值，Citrix ADM 将生成警报来表示发生了性能相关的问题。在计数器值回到阈值中指定的清除值时，事件将被清除。

我是否可以为 **Citrix ADM** 生成技术支持文件**?**

是。Citrix 建议您在联系技术支持人员以解决问题之前，先生成一份 Citrix ADM 数据和统计信息的存档。存档是可以发送给技术支持团队的 TAR 文件。

您可以生成一个技术支持文件，其中包含调试日志、收集调试日志的持续时间以及 Citrix ADM 数据库中不同且不同的日志。

要配置和发送技术支持文件，请导航到 “系统” > “诊断” > “技术支持”，然后单击 “生成技术支持文件”。有关详细信息，请参阅如何为 Citrix ADM 生成技术支持文件。

什么是 **syslog** 清除

Syslog 是日志记录标准协议。通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定在天数之后将从 Citrix ADM 中删除所有通用系统日志数据、AppFirewall 数据和 CitCitrix Gateway 数据。

我可以在 **Citrix ADM** 上配置 **NTP** 服务器吗**?**

可以在 Citrix ADM 中配置网络时间协议 (NTP) 服务器以将 Citrix ADM 时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

要配置 NTP 服务器，请导航到 “系统” > “**NTP** 服务器”，然后单击 “添加”。有关详细信息，请参阅如何在 Citrix ADM 上配置 NTP 服务器。

从哪个版本支持 **Citrix ADM** 主动**-**被动 **HA** 部署**?**

自 Citrix ADM 12.0 Build 51.24 起支持 Citrix ADM 主动-被动高可用性部署模式。

我已有 **Citrix ADM** 主动**-**被动高可用性设置并在 **Citrix ADC** 设备上配置了负载平衡虚拟服务器以实现统一的 **GUI** 访问。如何更新此配置

将 Citrix ADM 高可用性对升级到主动-被动模式后，必须在 Citrix ADC 设备上运行以下命令来更新负载平衡配置：

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** “**{**“**statuscode** “**:0, ** “**is_passive** “**:0}**” **-LRTM DISABLED**

我是否可以使用端口 **443** 在 **Citrix ADC** 实例上配置 **Citrix ADM** 高可用性对的负载平衡**?**

否，您不能使用端口 443 在 Citrix ADC 实例上配置 Citrix ADM HA 对的负载平衡。

在 Citrix ADC 上配置 `http-ecv` 和 `https-ecv` 监视器时，它无法正确监视 Citrix ADM HA 节点。

是否可以使用 **Citrix ADM** 服务器备份文件还原另一台 **Citrix ADM** 服务器的配置**?**

是

Citrix ADM 备份 **Citrix ADC** 实例后，是否可以使用该备份文件通过 **Citrix ADM** 还原另一个 **Citrix ADC** 实例的配置**?**

是。下载 Citrix ADM 备份文件，将其上载到另一个 Citrix ADC 实例的备份存储库中，然后恢复该实例。确保网络信息和身份验证信息不冲突。例如，检查 IP 地址或端口冲突、不匹配的密码配置文件。还要确保还原的 VPX 实例具有与备份的实例相同的 NSIP 地址和 Citrix ADC 许可证。

在恢复高可用性对中的实例之前，请确保备份文件中存储的 IP 地址和状态（主或辅助）与原始 HA 配置的 IP 地址和状态相匹配。还要验证新的主要和辅助服务是否具有相同类型的 Citrix ADC 许可证。

我们能否强制 **Citrix ADM** 使用 **SNIP** 地址与 **Citrix ADC** 实例进行通信，而不是使用 **Citrix ADM** 服务器的 **NSIP** 地址**?**

可以，您可以在 Citrix ADM 中添加 SNIP 地址（启用了管理功能），以便与 Citrix ADC 实例进行通信。

当我在 **Citrix ADM** 中备份 **Citrix ADC** 实例时，结果是完全备份还是基本备份**?**

Citrix ADM 对 Citrix ADC 实例的备份是完全备份。

是否有针对 **Citrix ADM** 的故障排除指南**?**

是。请参阅 https://support.citrix.com/article/CTX224502。

发生 **Citrix ADM** 高可用性故障转移时，如何管理 **Citrix ADC** 实例**?**

如果检测信号和基于 SSH 的检查失败，则认为主节点关闭，辅助节点将作为主节点接管工作。默认情况下，所有 Citrix ADC 实例都会使用最新的主节点详细信息作为其 SNMP 陷阱目标进行更新。

新的主（活动）Citrix ADM 节点将检查以确定以前的活动节点是否配置为 AppFlow 收集器还是 syslog 服务器。如果配置为，则新的主节点将 AppFlow 收集器或 syslog 服务器详细信息添加到发送到实例的信息中。

对于 syslog，它替换旧的服务器详细信息。

出现故障的 **Citrix ADM** 高可用性节点重新启动时会发生什么情况**?**

返回到服务后，除非主动节点进行故障转移，否则 Citrix ADM 节点将保持被动

Citrix ADC 实例如何在 **Citrix ADM** 高可用性节点之间分布**?**

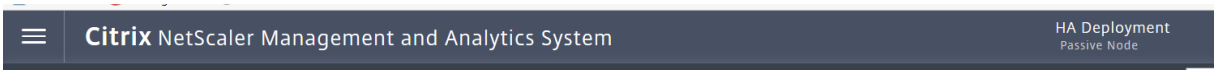
所有 Citrix ADC 实例都由主 Citrix ADM 节点进行管理。

在 **Citrix ADM HA** 故障转移的情况下，如何管理虚拟服务器许可证**?**

如果应用虚拟服务器许可证的 Citrix ADM 主节点出现故障，则新的主节点将在 30 天的宽限期内管理虚拟服务器许可证。在宽限期结束之前，必须在新的主服务器上重新申请许可证。有关替代品，请联系 Citrix 支持部门。

Citrix ADM 高可用性设置是否必须使用负载平衡器**?**

否，但如果没有负载平衡器，则必须通过其自己的 IP 地址访问 Citrix ADM 节点。被动节点标记为“被动”，Citrix 建议不要在被动节点上创建任何配置。



Citrix ADM 是否支持外部数据库**?**

否

由 **Citrix ADM** 管理的 **Citrix ADC** 实例是否可以用作 **Citrix ADM** 高可用性的负载平衡器**?**

是

在 **Citrix ADM** 高可用性节点之间同步哪些数据**?**

同步完整的 Citrix ADM 数据库，并同步以下文件夹：

- /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/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/