Citrix SD-WAN Center 11.4

Machine translated content

Disclaimer

Contents

Requisitos e instalación del sistema

February 16, 2022

Antes de instalar Citrix SD-WAN Center en una máquina virtual, asegúrese de que debe comprender los requisitos de hardware y software y cumplir los requisitos previos.

> **Nota**
>
> Los requisitos del sistema son comunes tanto para la red de una sola región como para la red de varias regiones.

Requisitos de hardware

Citrix SD-WAN Center tiene los siguientes requisitos de hardware.

Procesador

- Procesador de 4 núcleos, 3 GHz (o equivalente) o superior para un servidor que gestiona hasta 64 sitios.
- Procesador de 8 núcleos, 3 GHz (o equivalente) o superior para un servidor que gestiona hasta 128 sitios.
- Procesador de 16 núcleos, 3 GHz (o equivalente) o superior para un servidor que gestiona hasta 256 sitios.
- Procesador de 32 núcleos, 3 GHz (o equivalente) o superior para un servidor que gestiona hasta 550 sitios.

Memoria

- Se recomienda encarecidamente un mínimo de 8 GB de RAM para una máquina virtual que administre hasta 64 sitios.
- Se recomienda encarecidamente un mínimo de 16 GB de RAM para una máquina virtual que administre hasta 128 sitios.
- Se recomienda encarecidamente un mínimo de 32 GB de RAM para una máquina virtual que administre hasta 256 sitios.
- Se recomienda encarecidamente un mínimo de 32 GB de RAM para una máquina virtual que administre hasta 550 sitios.

Requisitos de espacio en disco

La siguiente tabla proporciona algunas pautas para determinar los requisitos de espacio en disco para el almacenamiento de datos de Citrix SD-WAN Center. Use almacenamiento de acceso directo con SSD que tengan de 5000 a 10000 IOPS.

Requisitos estimados de espacio en disco

# Sitios de cliente	Número promedio de enlaces WAN por sitio	Número promedio de servicios de Intranet/Internet por sitio	Número medio de rutas virtuales por sitio	Tamaño de la base de datos (TB) durante 1 año
32	2	2	2	1.2T
32	4	4	4	1.8T
32	8	8	8	5.3T
64	2	2	2	1.5T
64	4	4	4	2.6T
64	8	8	8	9.6T
96	2	2	2	1.8T
96	4	4	4	3.3T
96	8	8	8	14.0T
128	2	2	2	2.0T
128	4	4	4	4.1T
128	8	8	8	18.0T
192	2	2	2	2.6T
192	4	4	4	5.6T
192	8	8	8	27.0T
256	2	2	2	3.0T
256	4	4	4	7.2T
256	8	8	8	35.0T
550	2	2	2	15.9T
550	4	4	4	41.9T
550	8	8	8	195.6T

Ancho de banda

La siguiente tabla proporciona algunas pautas para determinar los requisitos de ancho de banda de red para la máquina virtual Citrix SD-WAN Center.

Requisitos estimados de ancho de banda

# Sitios de cliente	Número promedio de enlaces WAN	Número medio de rutas virtuales por sitio	Total de datos de VWAN por encuesta de 5 minutos (MB)	Velocidad de ancho de banda para configurar por sondeo de 5 minutos (Kbps)
32	2	2	1.2	Predeterminado 1000
32	4	4	3.6	Predeterminado 1000
32	8	8	20.0	Predeterminado 1000
64	2	2	2.3	Predeterminado 1000
64	4	4	7.2	Predeterminado 1000
64	8	8	40.0	2000
96	2	2	3,5	Predeterminado 1000
96	4	4	10.8	Predeterminado 1000
96	8	8	60.0	3000
128	2	2	4,6	Predeterminado 1000
128	4	4	14.4	Predeterminado 1000
128	8	8	80.0	4000
192	2	2	6.9	Predeterminado 1000
192	4	4	21,6	2000
192	8	8	120.0	6000
256	2	2	9.2	Predeterminado 1000

# Sitios de cliente	Número promedio de enlaces WAN	Número medio de rutas virtuales por sitio	Total de datos de VWAN por encuesta de 5 minutos (MB)	Velocidad de ancho de banda para configurar por sondeo de 5 minutos (Kbps)
256	4	4	28,8	2000
256	8	8	160	10000
550	2	2	34,0	2000
550	4	4	89,3	6000
550	8	8	415.7	24000

Software

Citrix SD-WAN Center VPX se puede configurar en las siguientes plataformas:

Hipervisor

- Servidor VMware ESXi, versión 6.5.
- Citrix XenServer 6.5 o superior.
- Microsoft Hyper-V 2012 R2 o superior.

Plataforma en la nube

- Microsoft Azure
- Amazon Web Services

Los exploradores deben tener habilitadas las cookies y JavaScript instalado y habilitado.

La interfaz web Citrix SD-WAN Center es compatible con estos exploradores web:

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- Mozilla Firefox 41.0+

Requisitos previos

A continuación se indican los requisitos previos para instalar e implementar Citrix SD-WAN Center:

- El nodo de control maestro (MCN) de SD-WAN y los nodos de cliente existentes deben actualizarse a la versión más reciente del software Citrix SD-WAN.
- Se recomienda tener un servidor DHCP disponible y configurado en la red SD-WAN.

- Debe tener los archivos de instalación de Citrix SD-WAN Center.

> **Nota**
>
> No puede personalizar ni instalar ningún software de terceros en Citrix SD-WAN Center. Sin embargo, puede modificar la configuración de vCPU, memoria y almacenamiento.

Descargue el software Citrix SD-WAN Center

Descargue los archivos de instalación del software Citrix SD-WAN Center Management Console, para la versión y la plataforma requeridas, en la página Descargas.

Los archivos de instalación de Citrix SD-WAN Center utilizan la siguiente convención de nomenclatura:

ctx-sdwc-version_number-platform.extension

- *version_number* es la versión de Citrix SD-WAN Center.
- *platform* es el tipo de plataforma, el hipervisor o el nombre de la plataforma de la nube.
- *extension* es la extensión del archivo de instalación.

Platform	Extensión de archivo
Citrix XenServer	.xva
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-azure.vhd.zip

Recopilar la información de instalación y configuración de Citrix SD-WAN Center

Esta sección proporciona una lista de comprobación con la información que necesitará para completar la instalación e implementación de Citrix SD-WAN Center.

Recopilar o determinar la siguiente información:

- Dirección IP del servidor ESXi, XenServer, servidor Hyper-V o Azure que aloja la máquina virtual (VM) Citrix SD-WAN Center.
- Un nombre único para asignar a la máquina virtual Citrix SD-WAN Center.
- La cantidad de memoria que se debe asignar para la máquina virtual Citrix SD-WAN Center.
- La cantidad de capacidad de disco que se asignará para el disco virtual de la máquina virtual.
- Dirección IP de puerta de enlace que Citrix SD-WAN Center utilizará para comunicarse con redes externas.

- Máscara de subred para la red en la que se instalará la máquina virtual Citrix SD-WAN Center.

Instalar y configurar Citrix SD-WAN Center en un servidor ESXi

April 13, 2021

Instalar el cliente VMware vSphere

Las siguientes son las instrucciones básicas para descargar e instalar el cliente VMware vSphere que utilizará para crear e implementar la máquina virtual Citrix SD-WAN Center. Para obtener más información, consulte la documentación de VMware vSphere Client.

Para descargar e instalar VMware vSphere Client, haga lo siguiente:

1. Abra un explorador y navegue hasta el servidor ESXi que aloja la instancia de vSphere Client y Citrix SD-WAN Center Virtual Machine (VM).

   Aparecerá la página de bienvenida de VMware ESXi.

2. Haga clic en el vínculo **Descargar vSphere Client** para descargar el archivo de instalación de vSphere Client.

3. Instale vSphere Client.

   Ejecute el archivo de instalación de vSphere Client que ha descargado y acepte cada una de las opciones predeterminadas cuando se le solicite.

4. Una vez completada la instalación, inicie el programa vSphere Client.

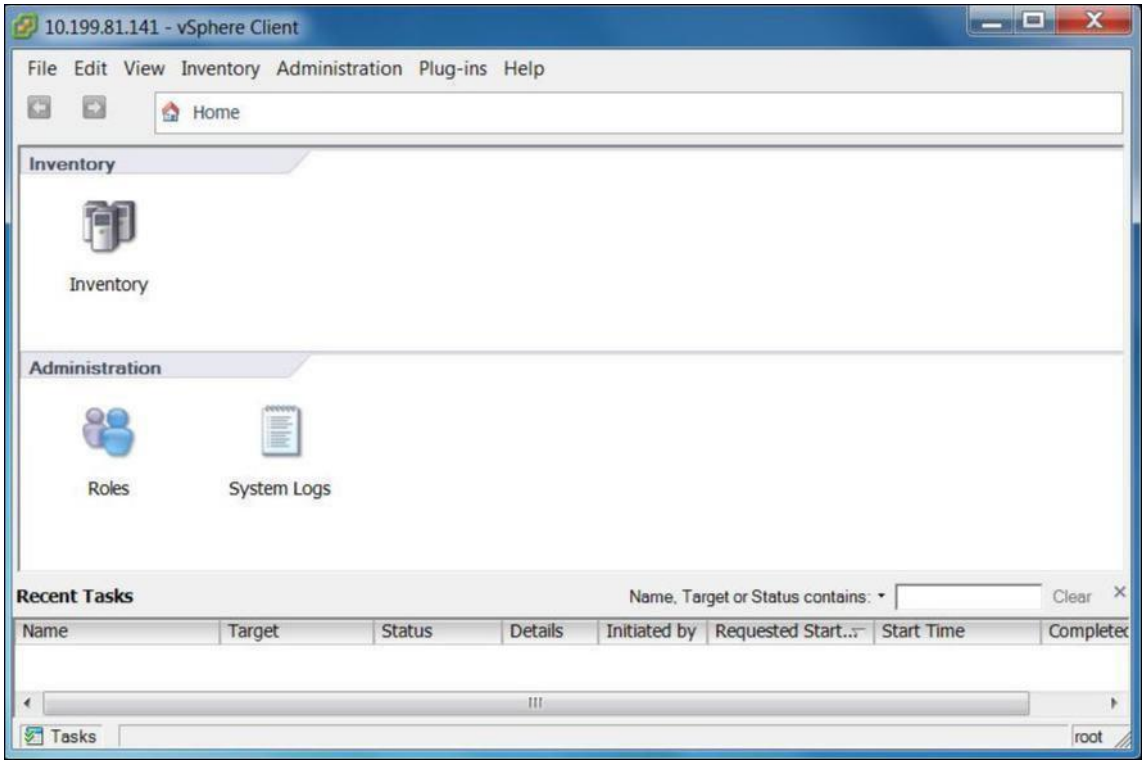
   Aparecerá la página de inicio de sesión de VMware vSphere Client, que le solicita las credenciales de inicio de sesión del servidor ESXi.

5. Introduzca las credenciales de inicio de sesión del servidor ESXi:

   - **Dirección IP/ Nombre**: Introduzca la dirección IP o el nombre de dominio completo (FQDN) para el servidor ESXi que aloja la instancia de Citrix SD-WAN Center VM.
   - **Nombre de usuario**: Introduzca el nombre de cuenta del administrador del servidor. El valor predeterminado es raíz.
   - **Contraseña**: Introduzca la contraseña asociada a esta cuenta de administrador.

6. Haga clic en **Login**.

   Aparecerá la página principal de vSphere Client.



Creación de la VM de Citrix SD-WAN Center mediante la plantilla OVF

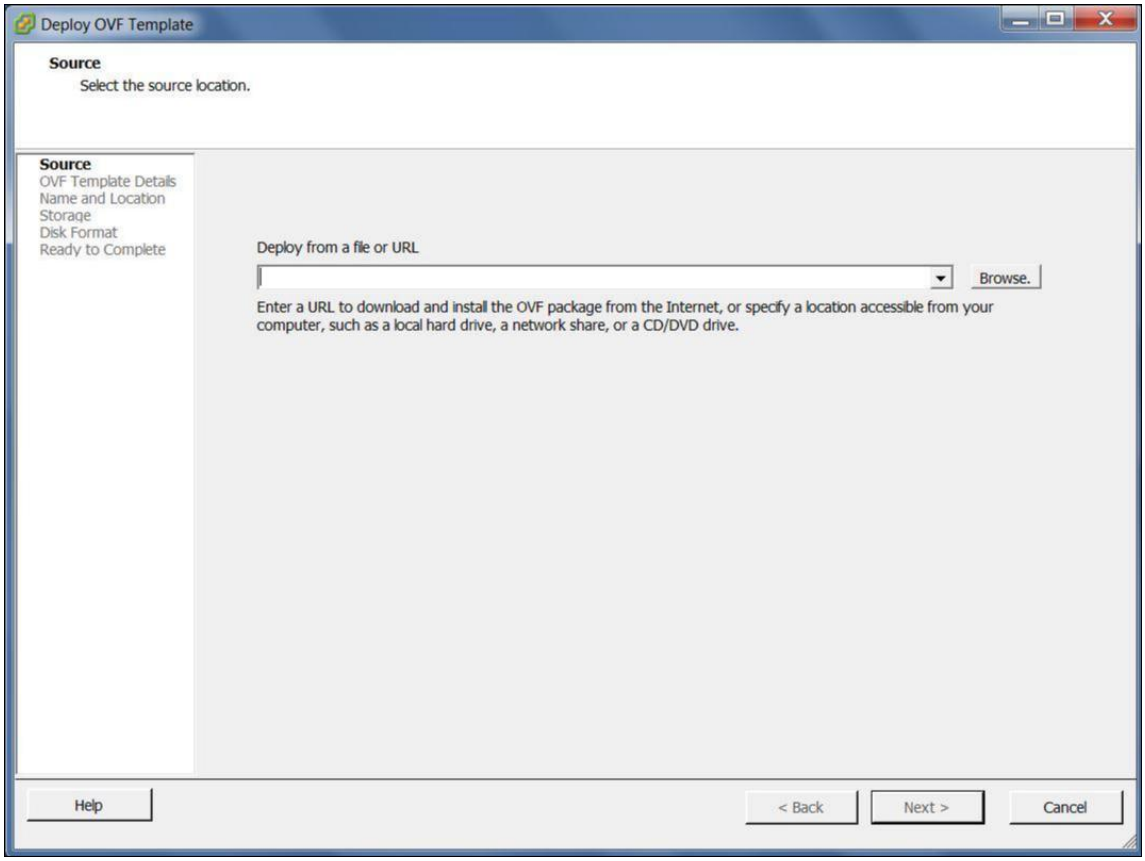
Después de instalar el cliente VMware vSphere, cree la máquina virtual Citrix SD-WAN Center.

1. Si aún no lo ha hecho, descargue el archivo de plantilla OVF de Citrix SD-WAN Center (archivo.ova) de Citrix SD-WAN Center en el equipo local.

   Para obtener más información, consulte Requisitos e instalación del sistema.

2. En vSphere Client, haga clic en **Archivo**y, a continuación, seleccione **Implementar plantilla OVF** en el menú desplegable.

   Aparecerá el asistente **Implementar plantilla OVF**.

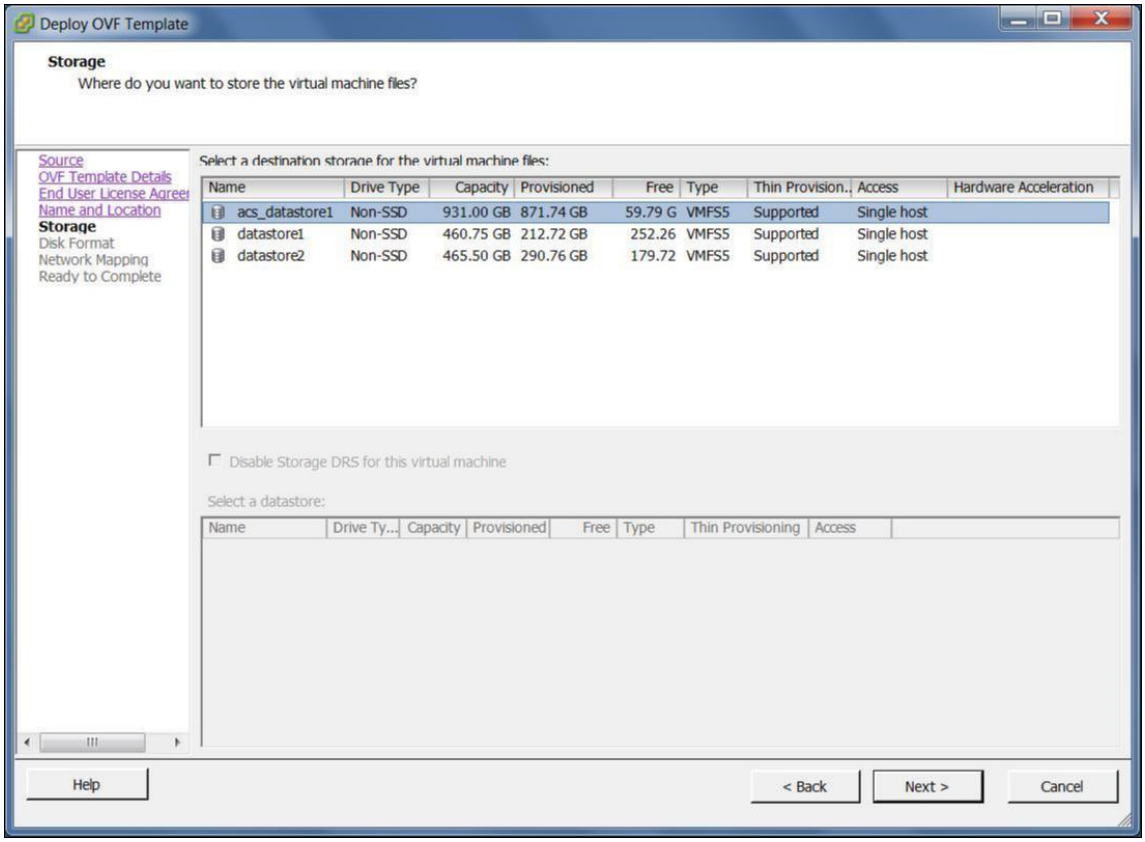


3. Haga clic en **Examinar** y seleccione la plantilla OVF de Citrix SD-WAN Center (archivo.ova) que quiere instalar.
4. Haga clic en **Siguiente**.

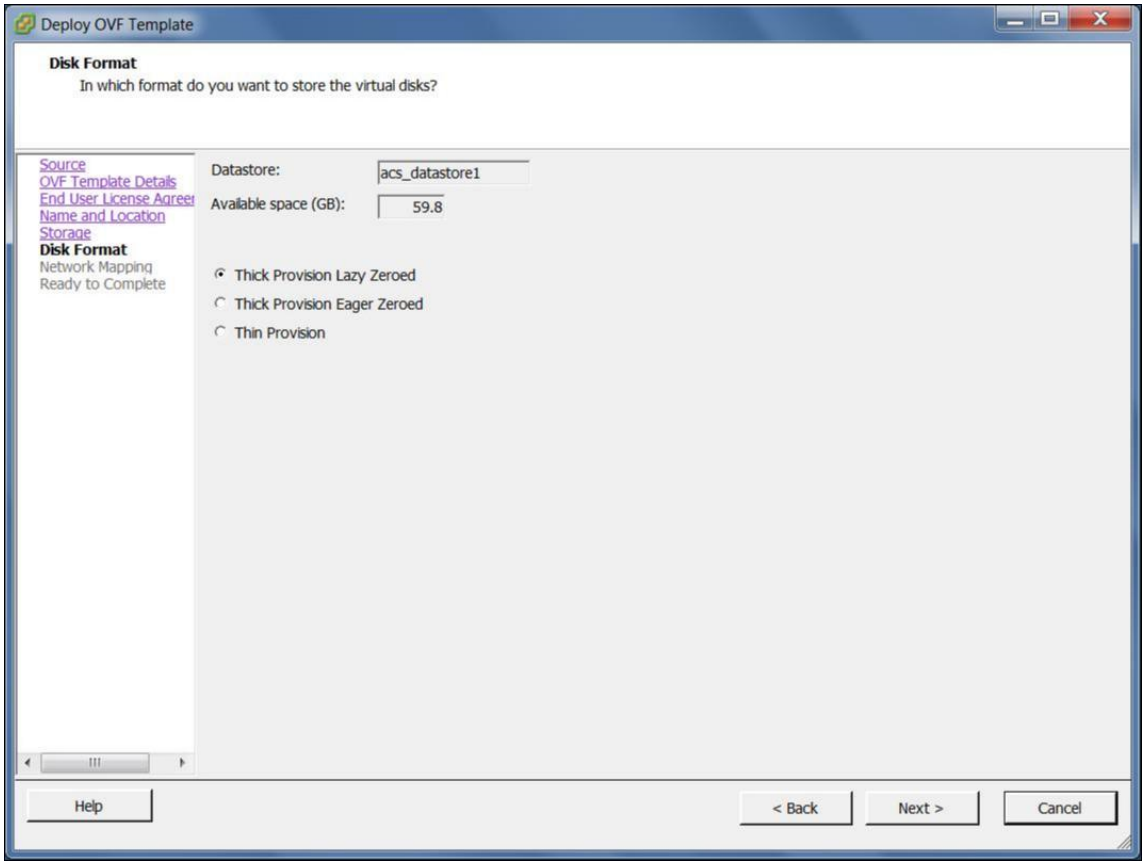
   Se importa el archivo ova y aparece la página Detalles de Plantilla OVF.
5. Haga clic en **Siguiente**.
6. En la página Contrato de licencia de usuario final, haga clic en **Aceptar**y, a continuación, haga clic en **Siguiente**.
7. En la página Nombre y ubicación, escriba un nombre único para la nueva máquina virtual (o acepte el valor predeterminado).

   El nombre debe ser único dentro de la carpeta **Inventario** actual y puede tener hasta 80 caracteres de longitud.
8. Haga clic en **Siguiente**.

   Aparecerá la página Almacenamiento.



9. Por ahora, acepte el recurso de almacenamiento predeterminado haciendo clic en **Siguiente**. También puede configurar el almacén de datos. Para obtener más información, consulte Agregar y configurar el almacén de datos en el servidor ESXi.



10. En la página Formato de disco, acepte la configuración predeterminada y haga clic en **Siguiente**.
11. En la página Asignación de red, acepte el valor predeterminado (Red de VM) y haga clic en **Siguiente**.
12. En la página Listo para completar, haga clic en **Finalizar** para crear la máquina virtual.

    > **Nota**: La
    >
    > descompresión de la imagen del disco en el servidor puede tardar varios minutos.

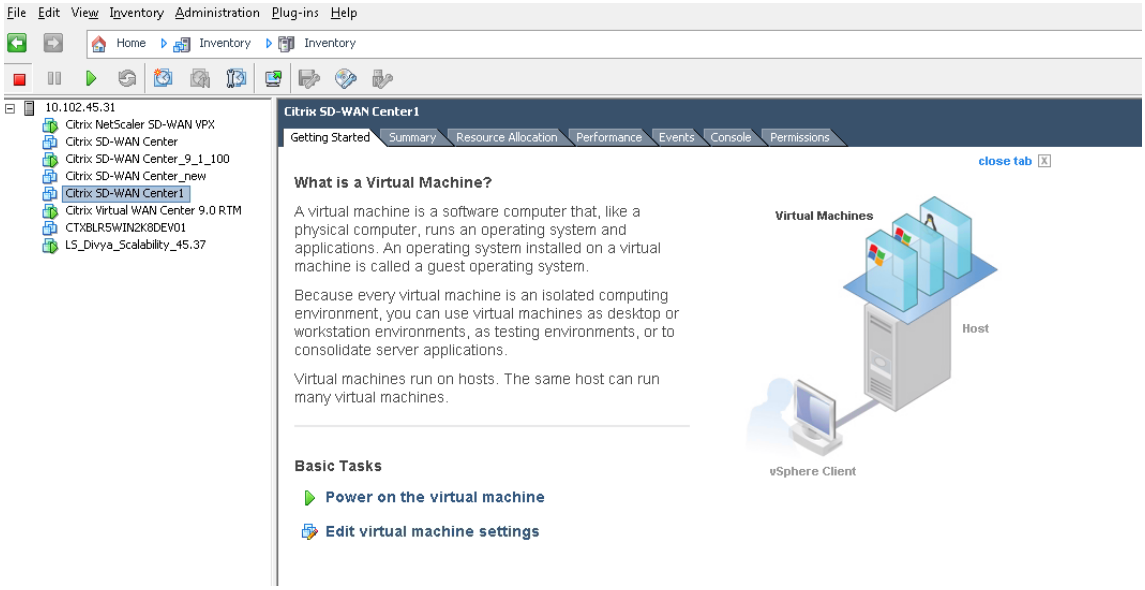
13. Haga clic en **Cerrar**.

Ver y registrar la dirección IP de administración en el servidor ESXi

La dirección IP de administración es la dirección IP de la máquina virtual de SD-WAN Center, utilice esta dirección IP para iniciar sesión en la interfaz de usuario web de Citrix SD-WAN Center.

Para mostrar la dirección IP de administración, haga lo siguiente:

1. En la página Inventario de cliente de vSphere, seleccione la nueva máquina virtual Citrix SD-WAN Center en el árbol de **inventario** (panel izquierdo).

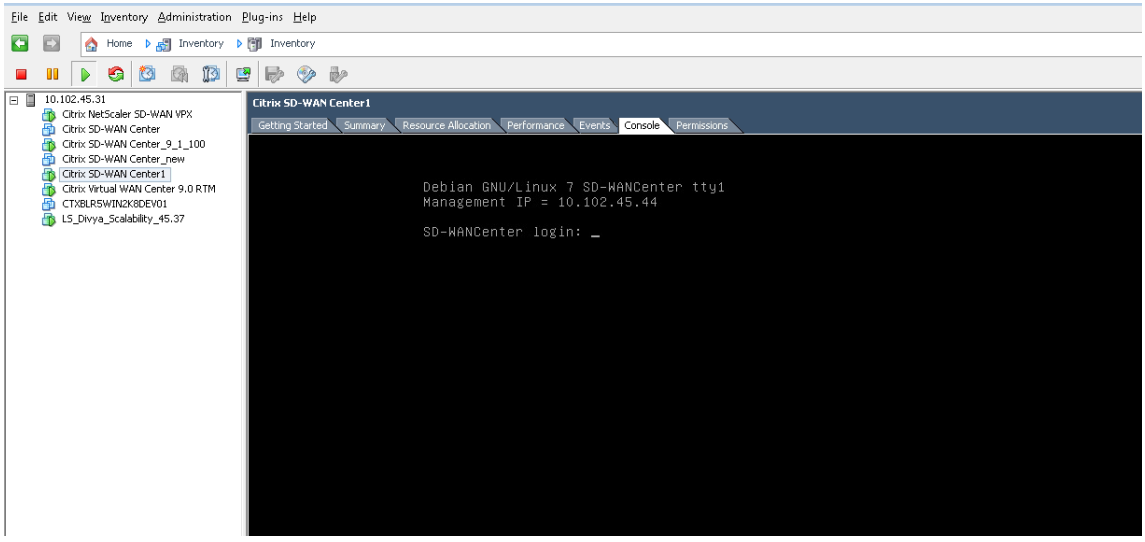


2. En la página Citrix SD-WAN Center, en Tareas básicas, haga clic en **Encender en la máquina virtual**.
3. Seleccione la ficha **Consola** y, a continuación, haga clic en cualquier lugar dentro del área de la consola para entrar en el modo de consola.

   Esto convierte el control del cursor del mouse sobre la consola de la máquina virtual.

   > **Nota**
   >
   > Para liberar el control de consola del cursor, presione las teclas <Ctrl> y <Alt> simultáneamente.

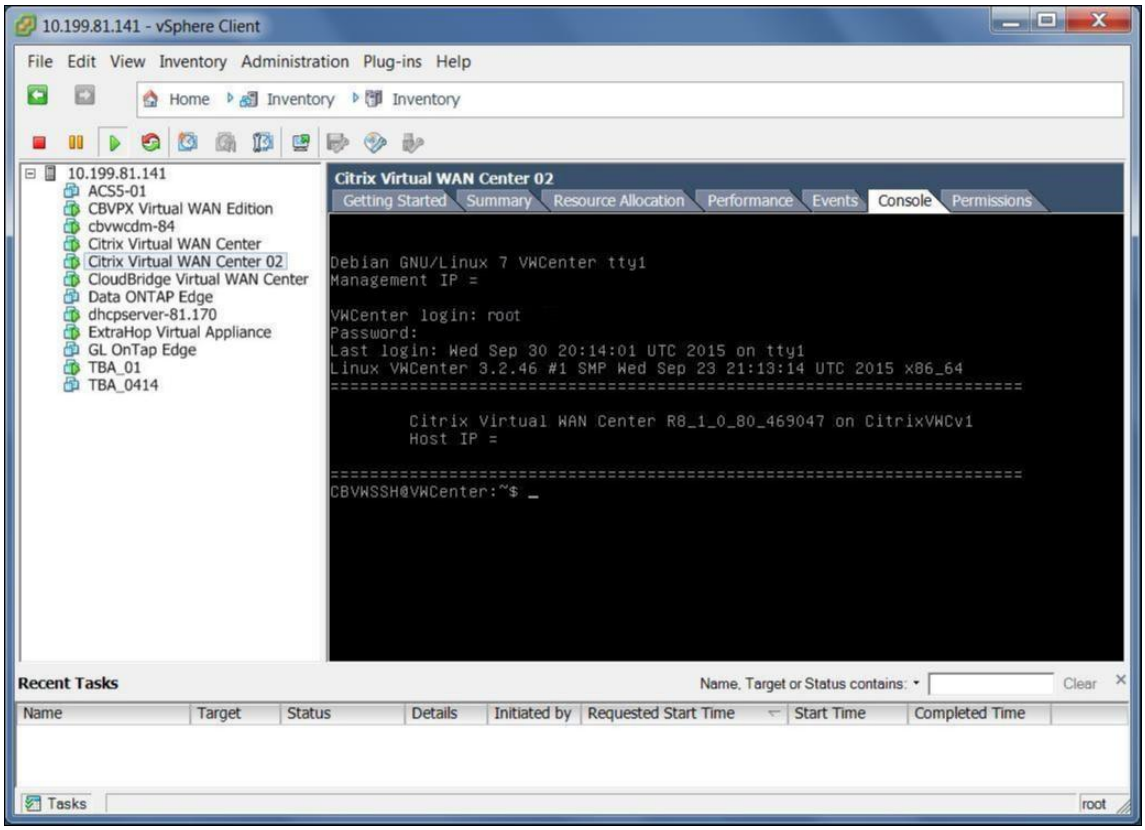
4. Pulse **Intro** para mostrar el mensaje de inicio de sesión de la consola.



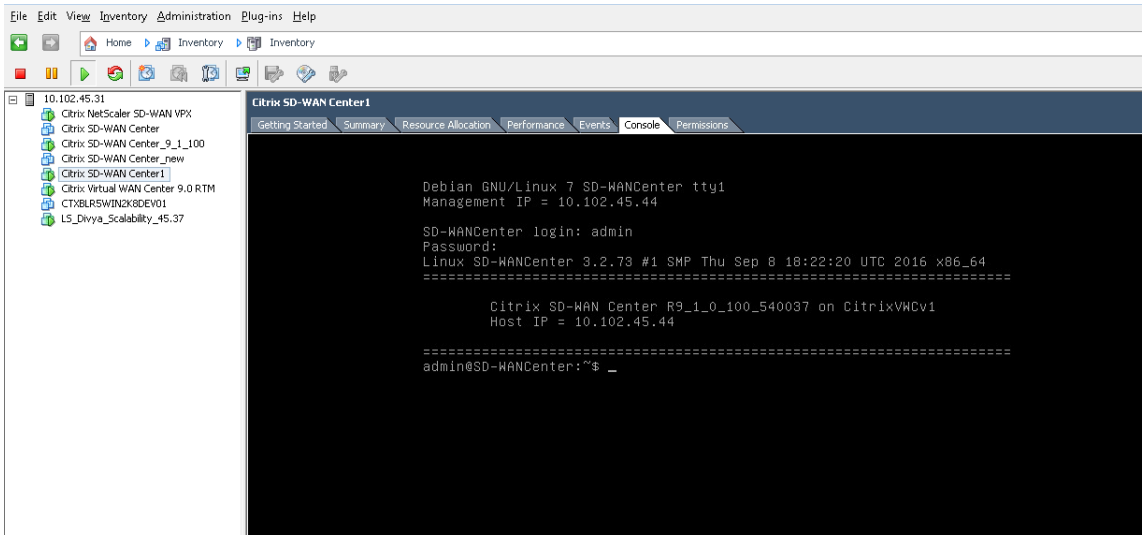
5. Inicie sesión en la consola de la máquina virtual.

Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Center son las siguientes:

- Inicio de sesión: admin
- Contraseña: contraseña



6. Registre la dirección IP de administración de la VM de Citrix SD-WAN Center, que se muestra como la dirección IP del host en un mensaje de bienvenida que aparece al iniciar sesión.



> **Nota**
>
> El servidor DHCP debe estar presente y disponible en la red SD-WAN, o este paso no se puede completar.

Si el servidor DHCP no está configurado en la red SD-WAN, debe introducir manualmente una dirección IP estática.

Para configurar una dirección IP estática como dirección IP de administración:

1. Cuando se inicie la máquina virtual, haga clic en la ficha **Consola**.
2. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Center son las siguientes:

   Inicio de sesión: admin

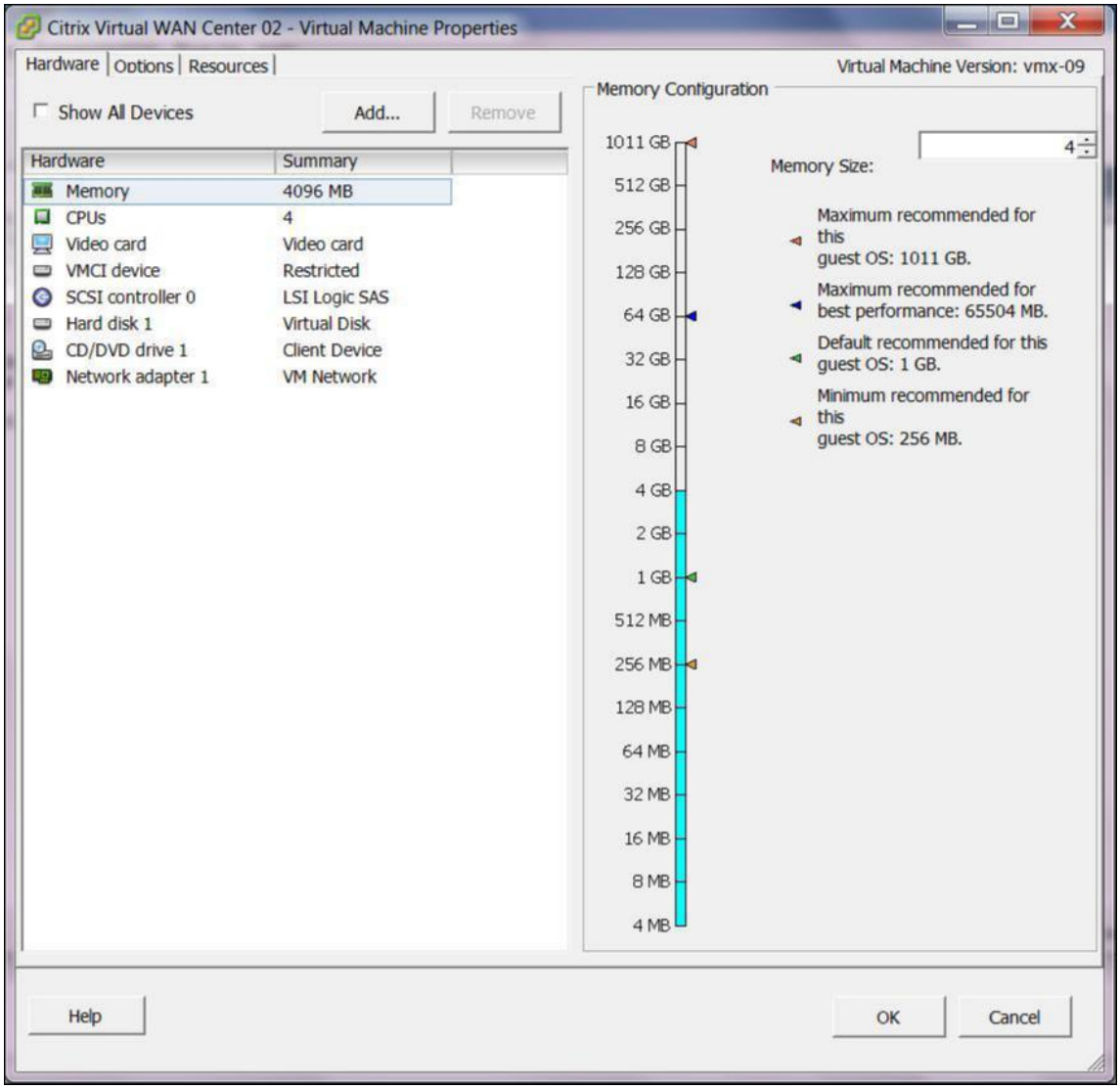
   Contraseña: contraseña
3. En la consola, introduzca el comando CLI **management_ip**.
4. Introduzca la **interfaz de conjunto de comandos <ipaddress> <subnetmask> <gateway>**, para configurar la dirección IP de administración.

Agregar y configurar el almacén de datos en un servidor ESXi

Puede agregar y configurar el almacén de datos para almacenar estadísticas desde Citrix SD-WAN Center.

Para agregar y configurar el almacén de datos:

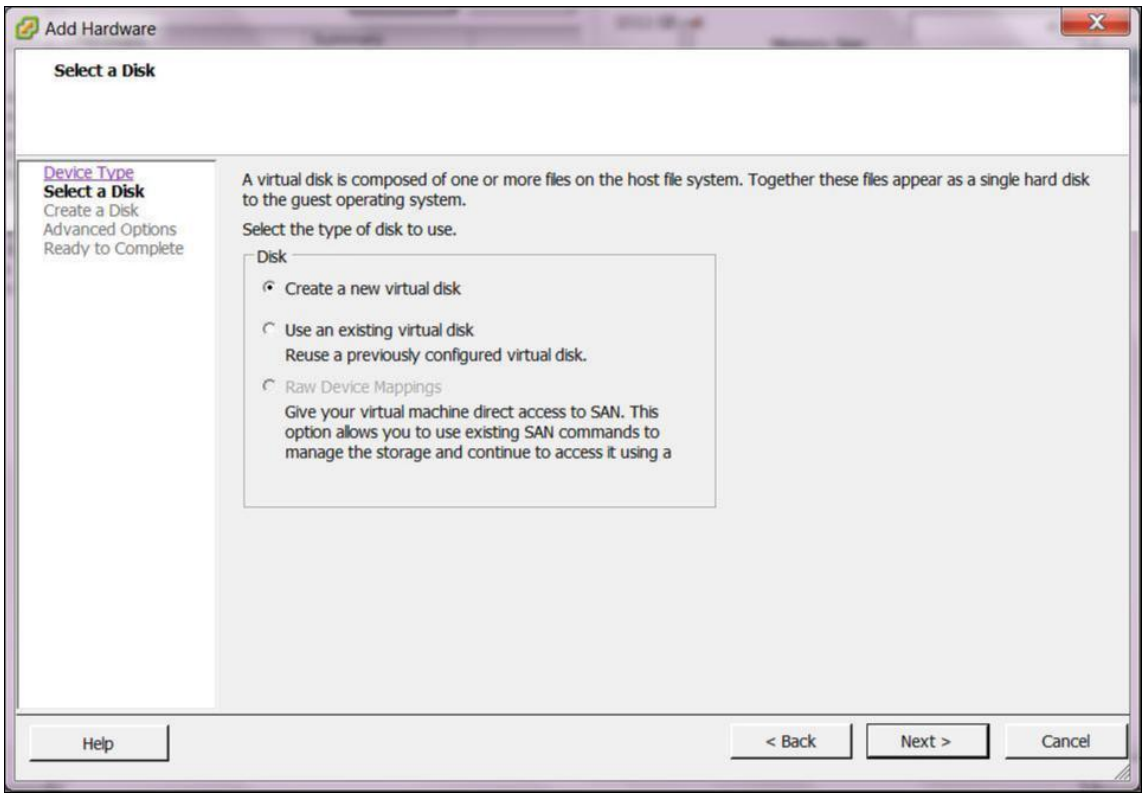
1. En el cliente de vSphere, haga clic en el icono **Inventario** para abrir la página Inventario.
2. Expanda la rama Árbol de **inventario** para el servidor host de VM Citrix SD-WAN Center.
3. En el panel izquierdo, haga clic en **+** junto a la dirección IP del servidor que aloja la máquina virtual Citrix SD-WAN Center que creó.
4. Abra la nueva máquina virtual Citrix SD-WAN Center para modificarla.
5. En el árbol **de inventario**, haga clic con el botón derecho en el nombre de la máquina virtual Citrix SD-WAN Center que creó y seleccione **Modificar configuración** en el menú desplegable.



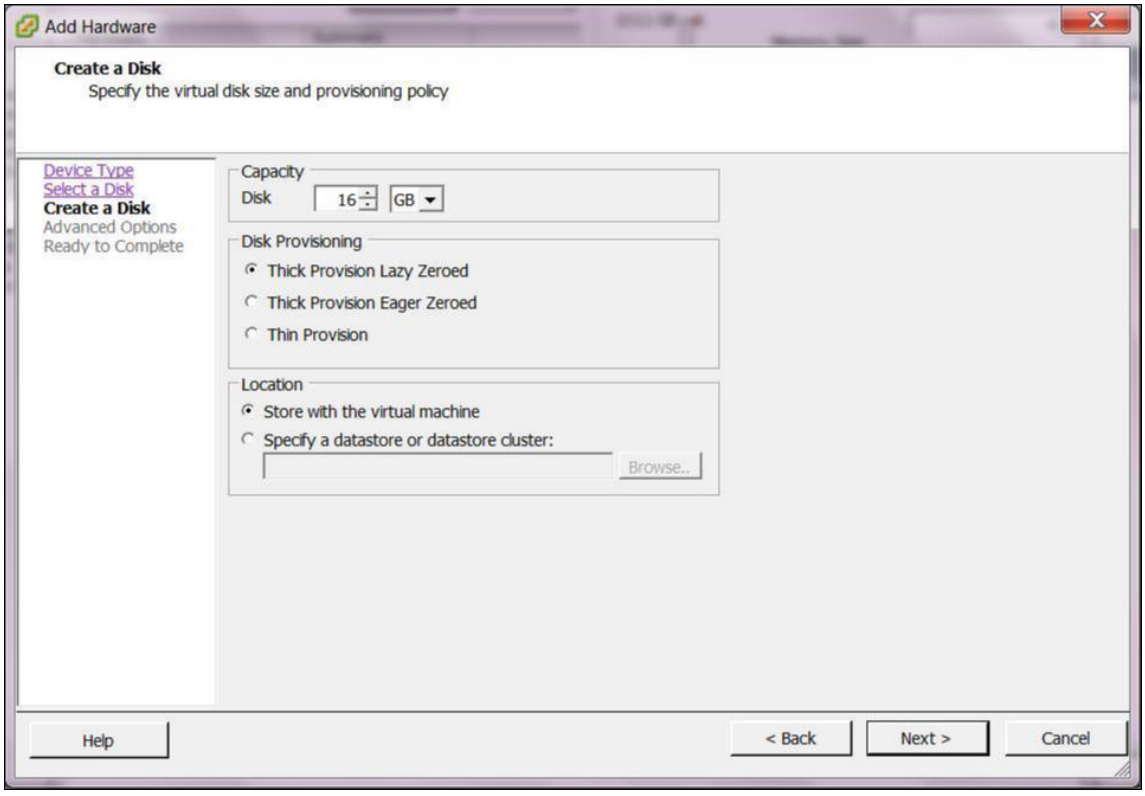
6. En el campo Tamaño de memoria, introduzca la cantidad de memoria que desea asignar a esta máquina virtual.

   Para obtener más información, consulte Requisitos de memoria.

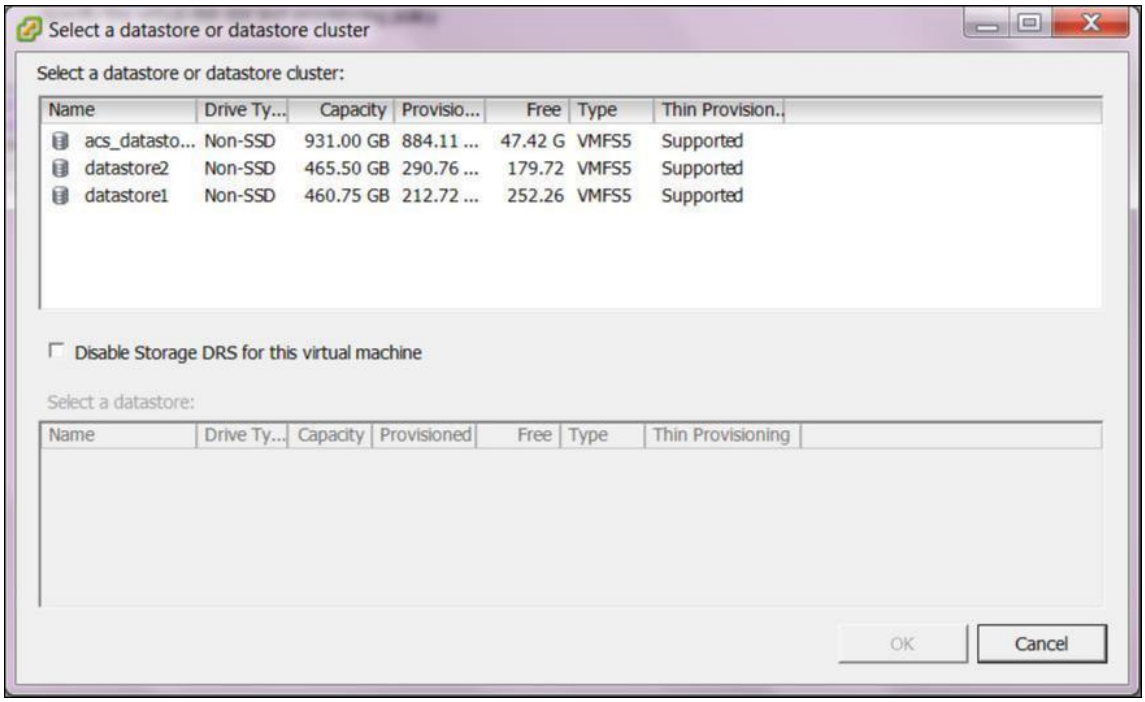
7. Haga clic en **Agregar**.
8. En la página Tipo de dispositivo del Asistente para agregar hardware, seleccione **Disco duro** y, a continuación, haga clic en **Siguiente**.



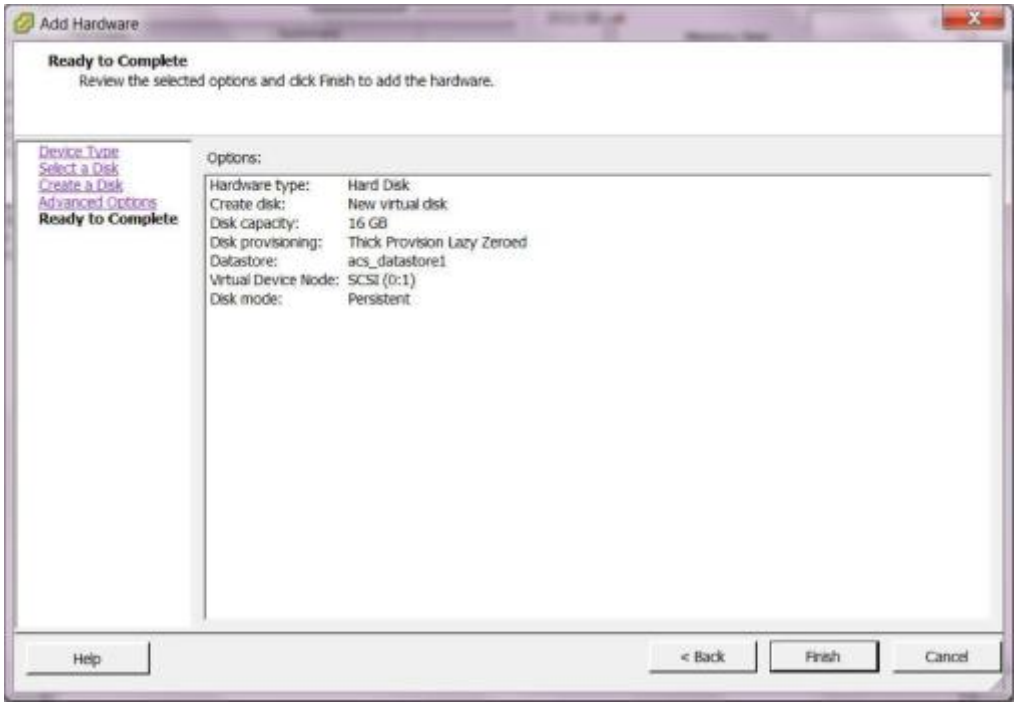
9. En la página Seleccionar un disco, seleccione **Crear un disco virtual nuevo** y haga clic en **Siguiente**.



10. En la página Crear un disco, en la sección **Capacidad**, seleccione la capacidad del disco para el nuevo disco virtual.
11. En la sección Aprovisionamiento de discos, seleccione **Thick Provisioning Lazy Zeroed** (valor predeterminado).
12. En la sección Ubicación, seleccione **Especificar un almacén de datos o un clúster de almacenes**de datos.
13. Haga clic en **Examinar**.



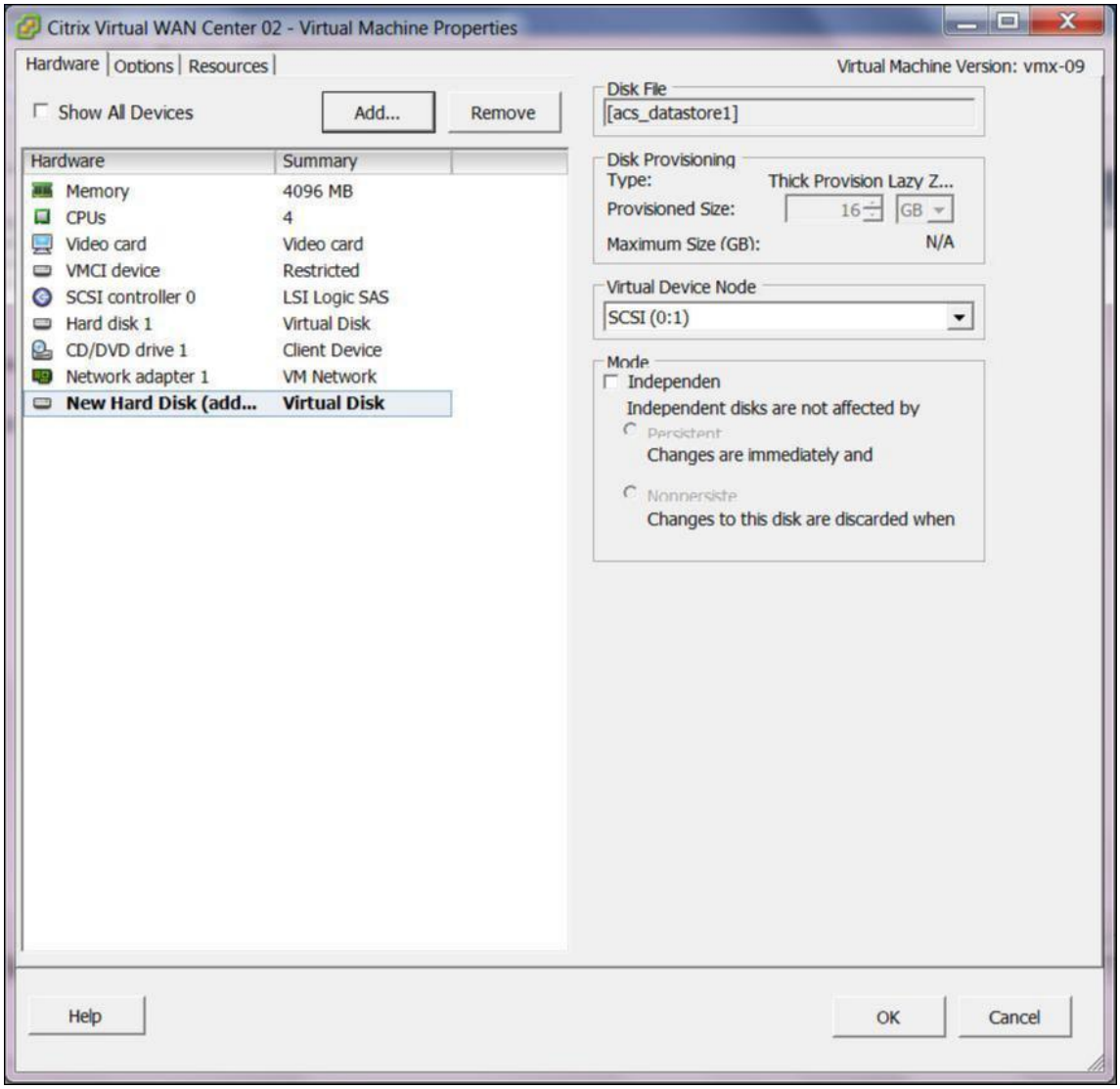
14. Seleccione un almacén de datos con suficiente espacio disponible y haga clic en **Aceptar**.
15. Haga clic en **Siguiente**.
16. En la página Opciones avanzadas, acepte la configuración predeterminada de **Opciones avanzadas** y haga clic en **Siguiente**.



17. Haga clic en **Finalizar**.

    Esto agrega el nuevo disco virtual, descarta el Asistente para agregar hardware y le devuelve a la página Propiedades de la máquina virtual.

18. Haga clic en **Aceptar**.



Instalar y configurar Citrix SD-WAN Center en XenServer

April 13, 2021

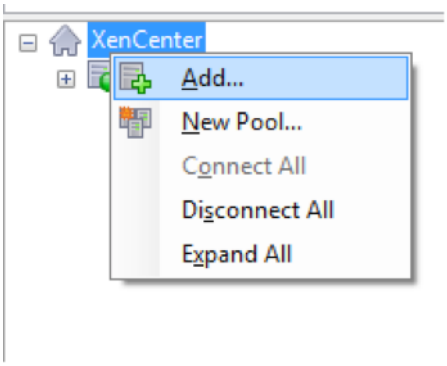
Antes de instalar la máquina virtual de Citrix SD-WAN Center en un servidor XenServer, recopile la información necesaria tal como se describe en Recopilación de información de configuración e instalación de Citrix SD-WAN Center.

Instalar el servidor XenServer

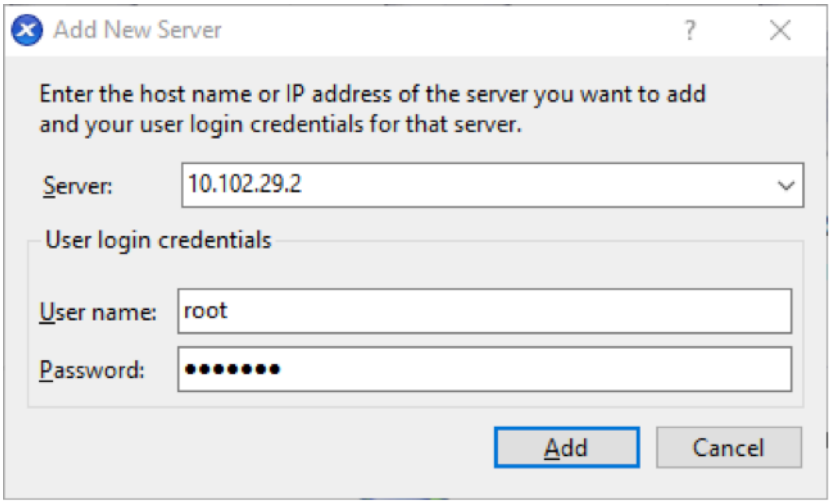
Para instalar el servidor Citrix XenServer en el que implementará la máquina virtual Citrix SD-WAN Center, debe tener XenCenter instalado en el equipo. Si aún no lo ha hecho, descargue e instale XenCenter.

Para instalar un servidor XenServer:

1. Abra la aplicación XenCenter en el equipo.
2. En el panel de árbol izquierdo, haga clic con el botón derecho en **XenCenter** y seleccione **Agregar**.



3. En la ventana **Agregar nuevo servidor**, introduzca la información necesaria en los siguientes campos:
   - **Servidor**: introduzca la dirección IP o el nombre de dominio completo (FQDN) del servidor XenServer que alojará la instancia de VM de Citrix SD-WAN Center.
   - **Nombre de usuario**: Introduzca el nombre de cuenta del administrador del servidor. El valor predeterminado es raíz.
   - **Contraseña**: Introduzca la contraseña asociada a esta cuenta de administrador.



4. Haga clic en **Agregar**.

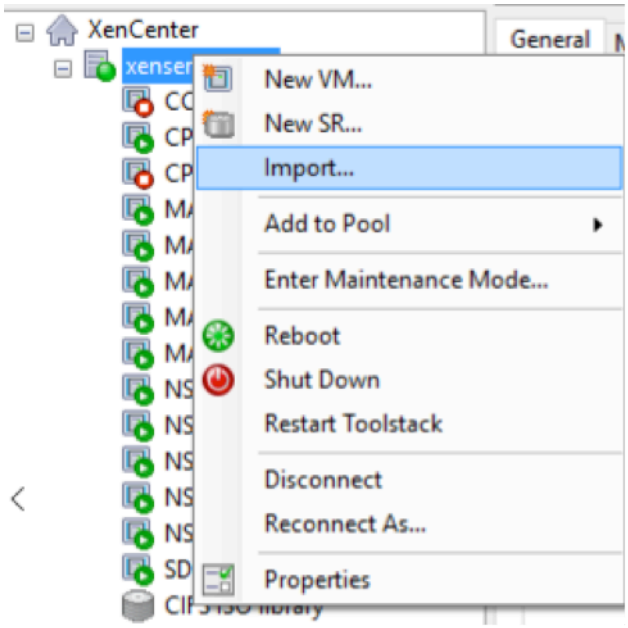
   La dirección IP del nuevo servidor aparece en el panel izquierdo.

Cree la máquina virtual de Citrix SD-WAN Center mediante el archivo XVA

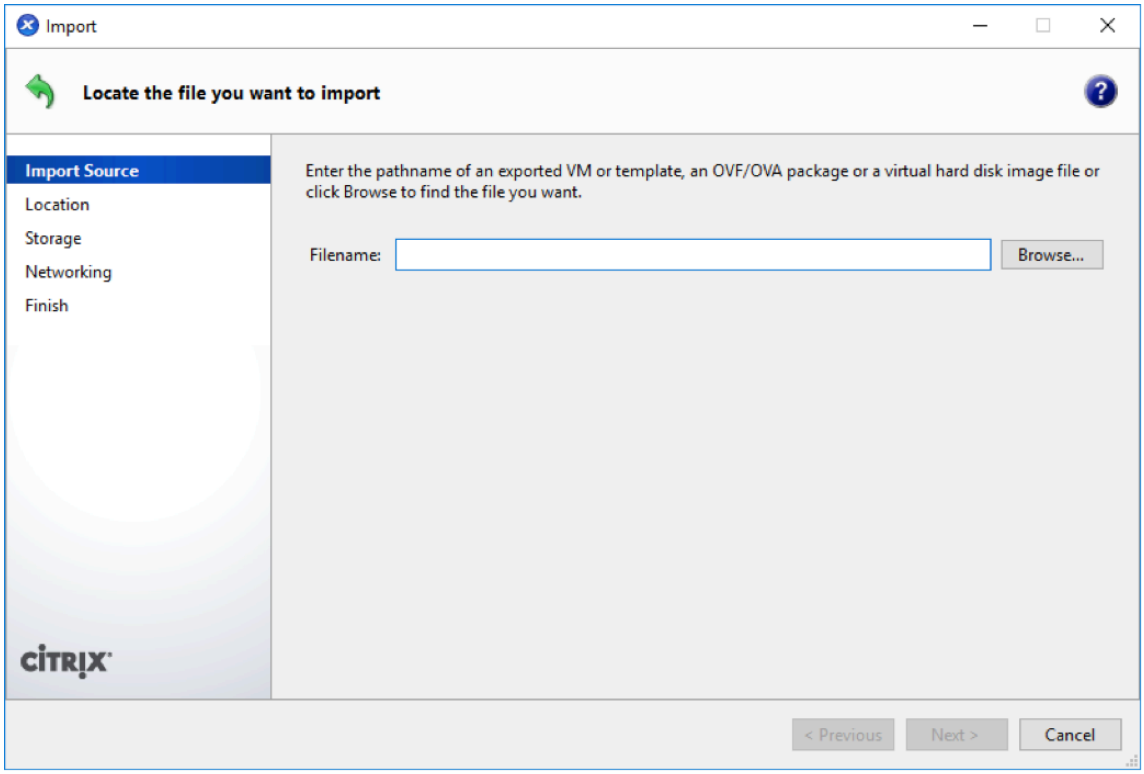
El software de máquina virtual Citrix SD-WAN Center se distribuye como un archivo XVA. Si aún no lo ha hecho, descargue el archivo.xva. Para obtener más información, consulte Requisitos e instalación del sistema.

Para crear la máquina virtual Citrix SD-WAN Center:

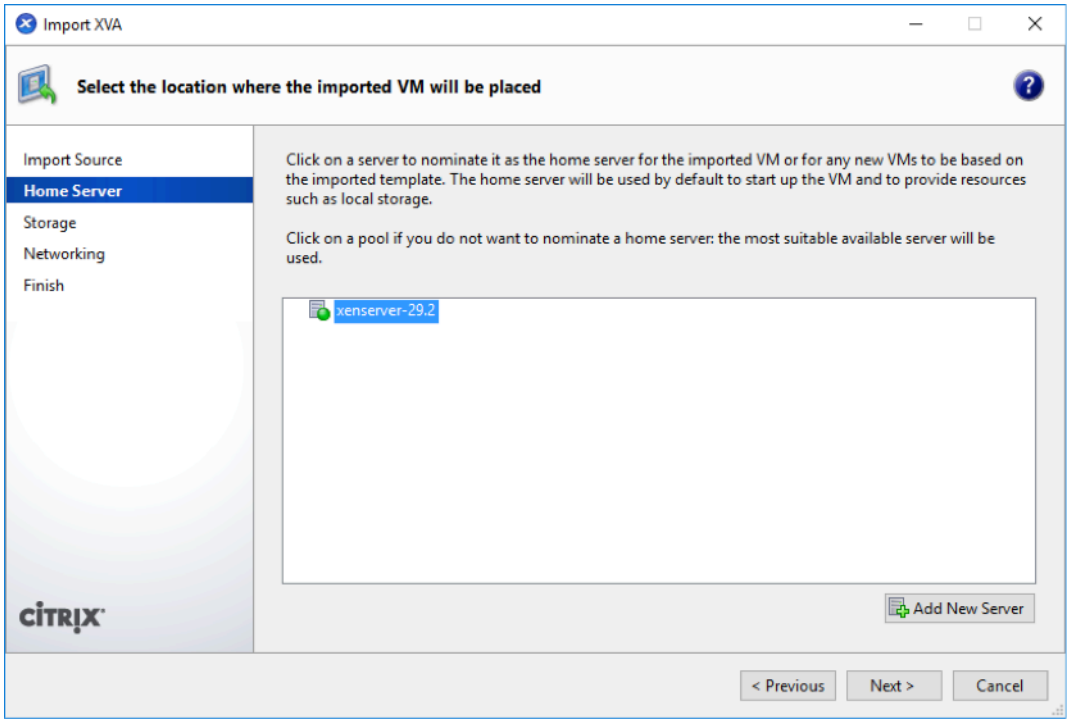
1. En XenCenter, haga clic con el botón secundario en **XenServer** y haga clic en **Importar**.



2. Busque el archivo.xva descargado, selecciónelo y haga clic en **Siguiente**.

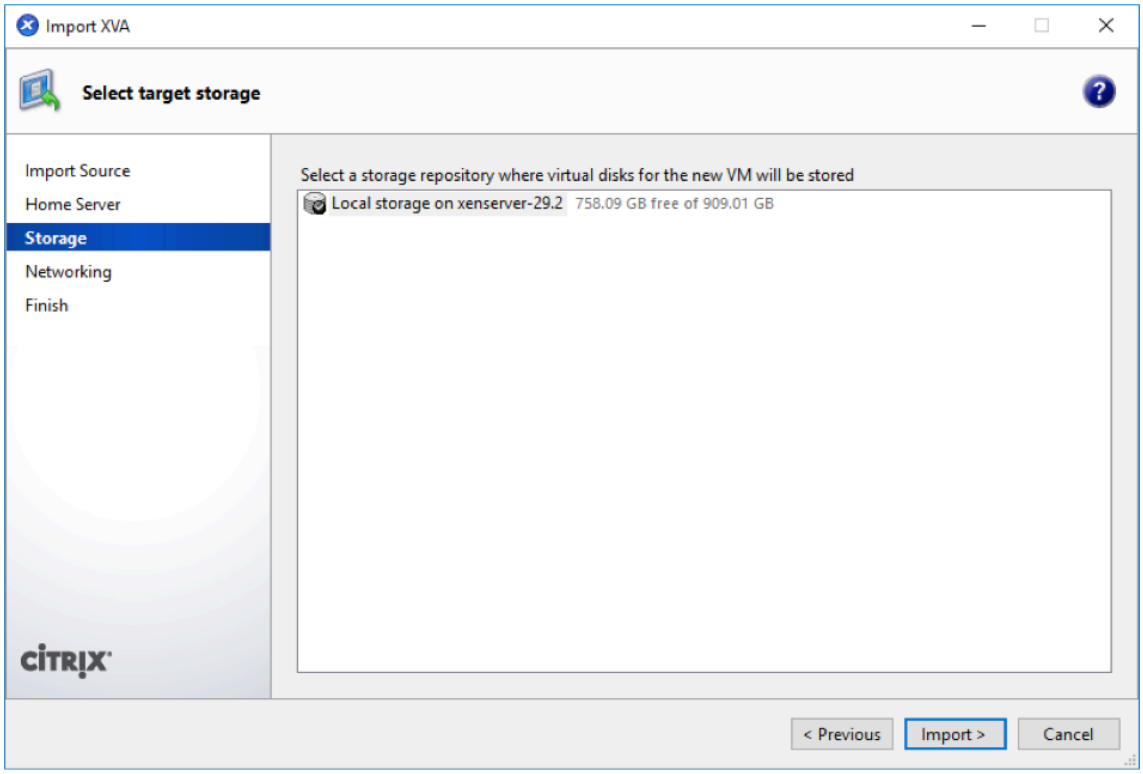


3. Seleccione un servidor XenServer creado anteriormente como la ubicación a la que quiere importar la máquina virtual y haga clic en **Siguiente**.



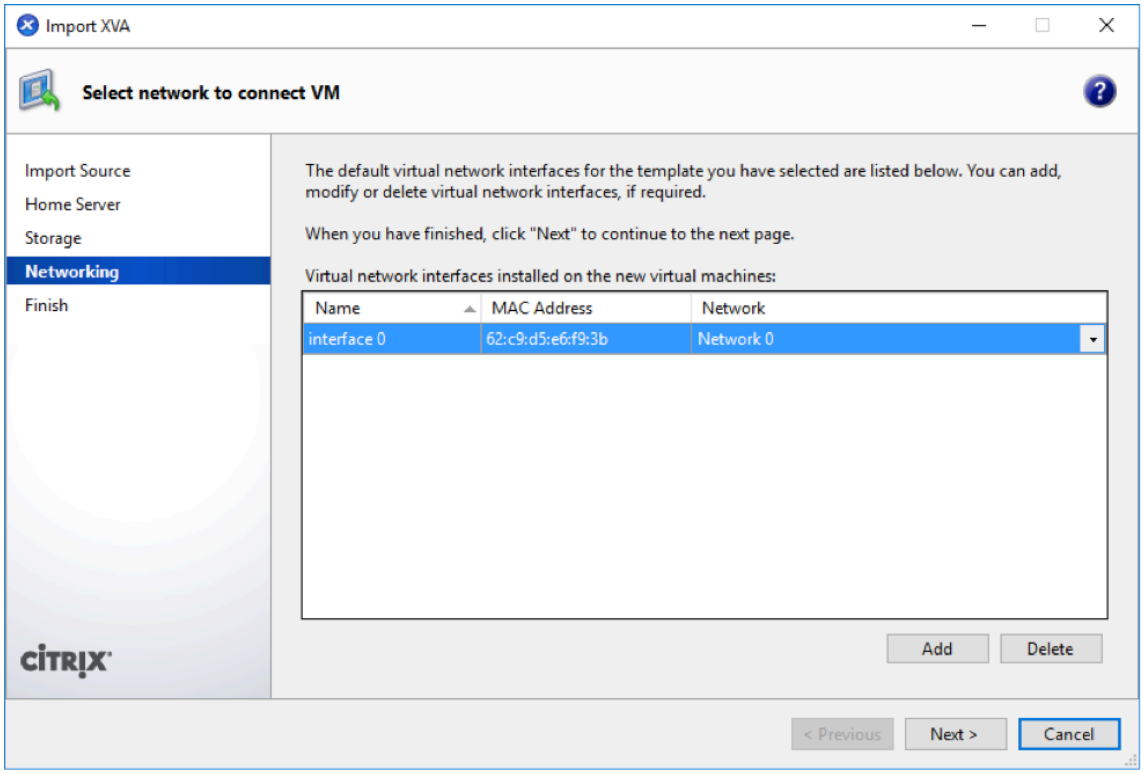
4. Seleccione un repositorio de almacenamiento donde se almacenará el disco virtual de la nueva máquina virtual y haga clic en **Importar.**

Por ahora, puede aceptar el recurso de almacenamiento predeterminado. O puede configurar el almacén de datos. Para obtener más información, vea la sección **Agregar y configurar el almacén de datos en XenServer**.



La máquina virtual importada de Citrix SD-WAN Center aparece en el panel izquierdo.

5. Seleccione una red a la que quiere conectar la VM y haga clic en **Siguiente**.



6. Haga clic en **Finalizar**.

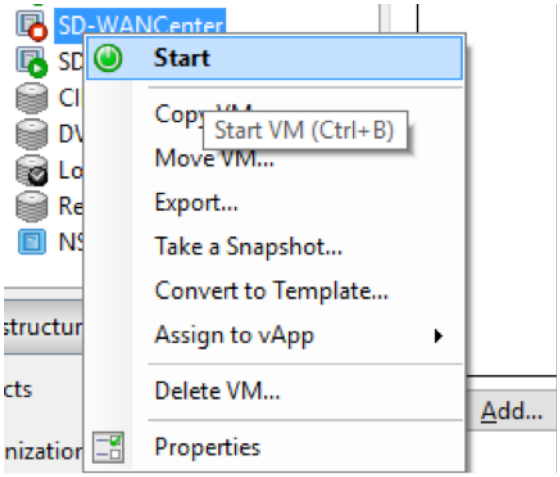
Ver y registrar la dirección IP de administración en XenServer

La dirección IP de administración es la dirección IP de la máquina virtual Citrix SD-WAN Center, utilice esta dirección IP para iniciar sesión en la interfaz de usuario web de Citrix SD-WAN Center.

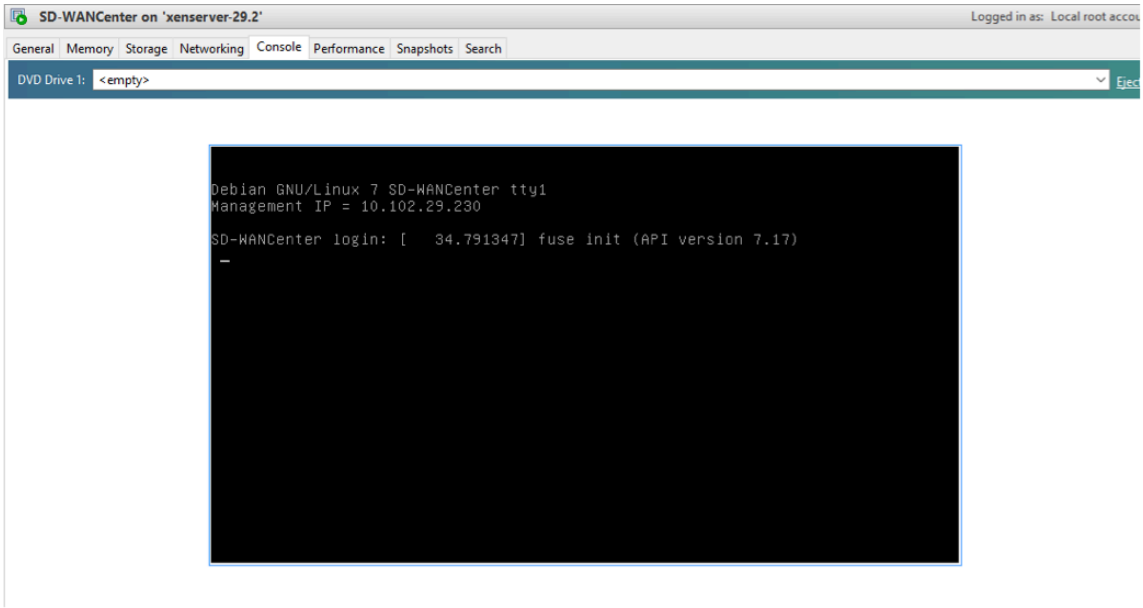
> **Nota**
>
> El servidor DHCP debe estar presente y disponible en la red SD-WAN.

Para mostrar la dirección IP de administración:

1. En la interfaz XenCenter, en el panel izquierdo, haga clic con el botón derecho en la nueva máquina virtual Citrix SD-WAN Center y seleccione **Inicio**.



2. Cuando se inicie la máquina virtual, haga clic en la ficha **Consola**.



3. Tome nota de la dirección IP de administración.

> **Nota**
>
> El servidor DHCP debe estar presente y disponible en la red SD-WAN, o este paso no se puede completar.

4. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Center son las siguientes:

   Inicio de sesión: admin

   Contraseña: contraseña

   Si el servidor DHCP no está configurado en la red Citrix SD-WAN, debe introducir manualmente una dirección IP estática.

Para configurar una dirección IP estática como dirección IP de administración:

1. Cuando se inicie la máquina virtual, haga clic en la ficha **Consola**.
2. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual Citrix SD-WAN Center son las siguientes:

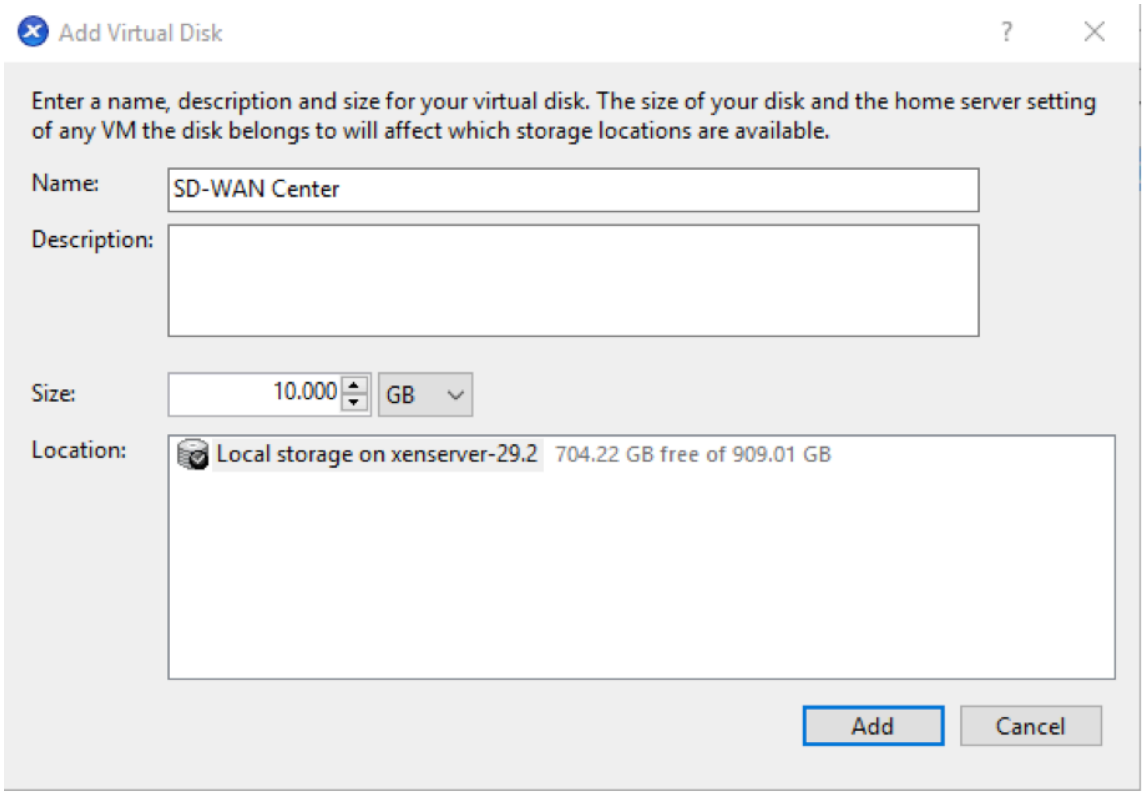
   Inicio de sesión: admin
   ; **Contraseña**: password
3. En la consola, introduzca el comando de CLI **management_ip.**
4. Introduzca el comando **set interface <ipaddress> <subnetmask> <gateway>**, para configurar la dirección IP de administración.

Agregar y configurar el almacenamiento de datos para un servidor XenServer

Puede agregar y configurar el almacenamiento de datos para almacenar estadísticas desde el centro Citrix SD-WAN.

Para agregar y configurar el almacenamiento de datos:

1. En XenCenter, cierre la máquina virtual Citrix SD-WAN Center.
2. En la ficha **Almacenamiento**, haga clic en **Agregar**.



3. En el campo **Nombre**, escriba un nombre para el disco virtual.
4. En el campo **Descripción**, escriba una descripción del disco virtual.
5. En el campo **Tamaño**, seleccione el tamaño requerido.
6. En el campo **Ubicación**, seleccione el almacenamiento local.
7. Haga clic en **Agregar**.

Instalar y configurar Citrix SD-WAN Center en Microsoft Hyper-V

April 13, 2021

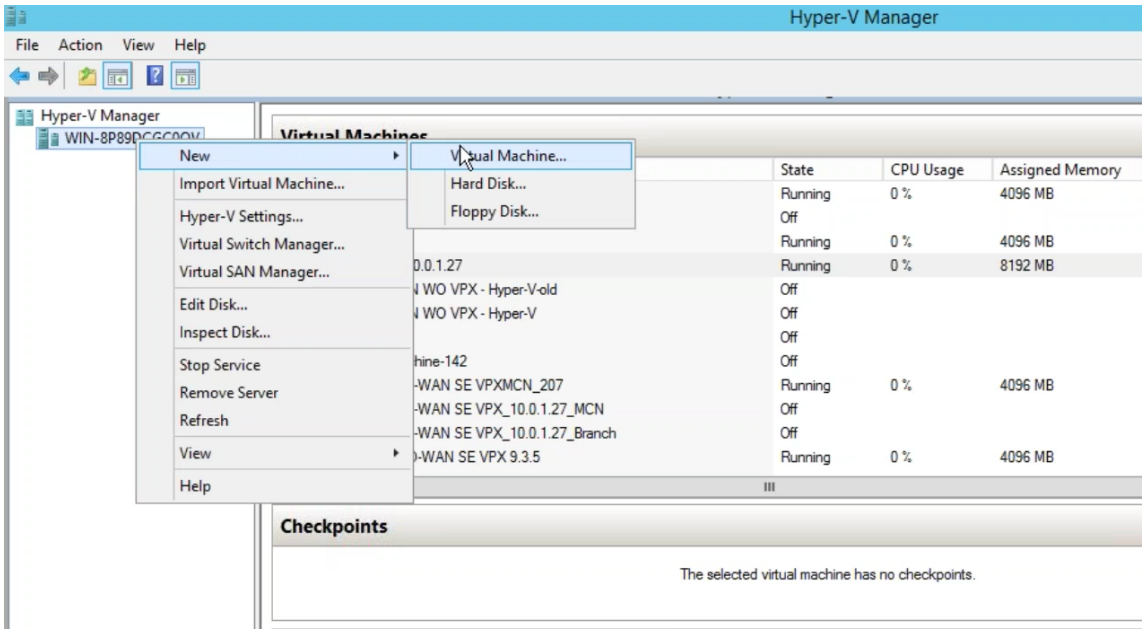
Antes de instalar la máquina virtual (VM) Citrix SD-WAN Center en el servidor Microsoft Hyper-V, recopile la información necesaria tal como se describe en Requisitos e instalación del sistema.

Descargue el software SD-WAN Center para Hyper-V, como se describe en la sección Descarga del software Citrix SD-WAN Center de Requisitos e instalación del sistema.

Asegúrese de que la función Hyper-V y la herramienta de administración están habilitadas en el servidor Windows.

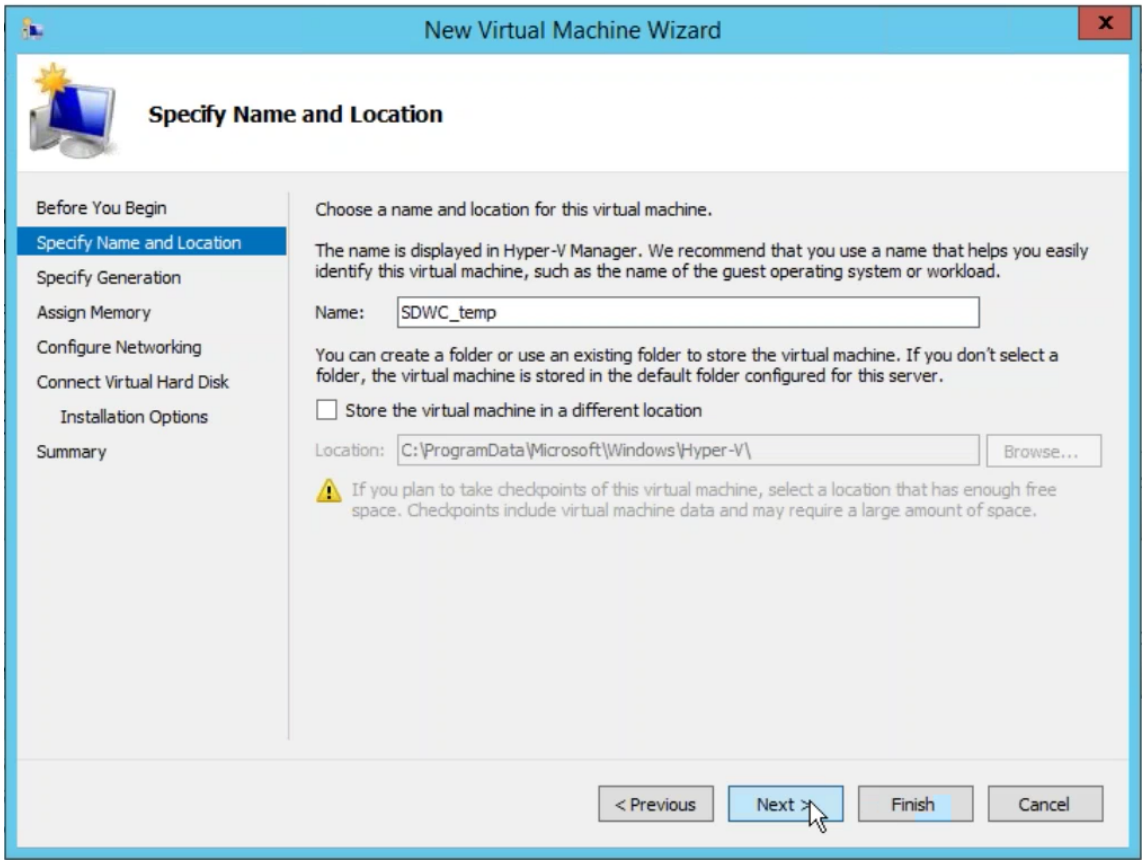
Para crear la máquina virtual SD-WAN Center en el servidor Hyper-V:

1. En el Administrador de Hyper-V, haga clic con el botón secundario en el servidor de Hyper-V y seleccione **Nuevo** > **Máquina virtual**.



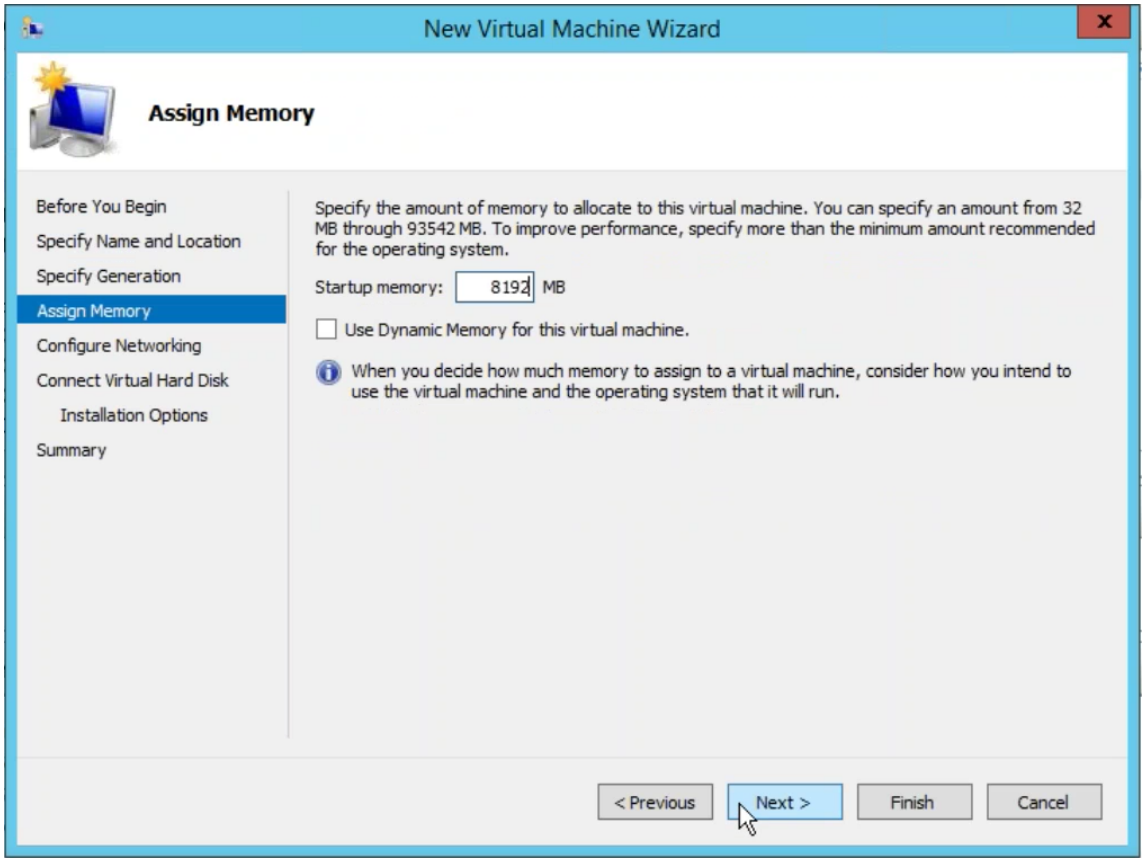
Aparecerá el **Asistente para nueva máquina virtual**. Haga clic en **Siguiente**.

2. Especifique un nombre para la máquina virtual central de SD-WAN y cambie la ubicación de almacenamiento de la máquina virtual, si es necesario.Haga clic en **Siguiente**.

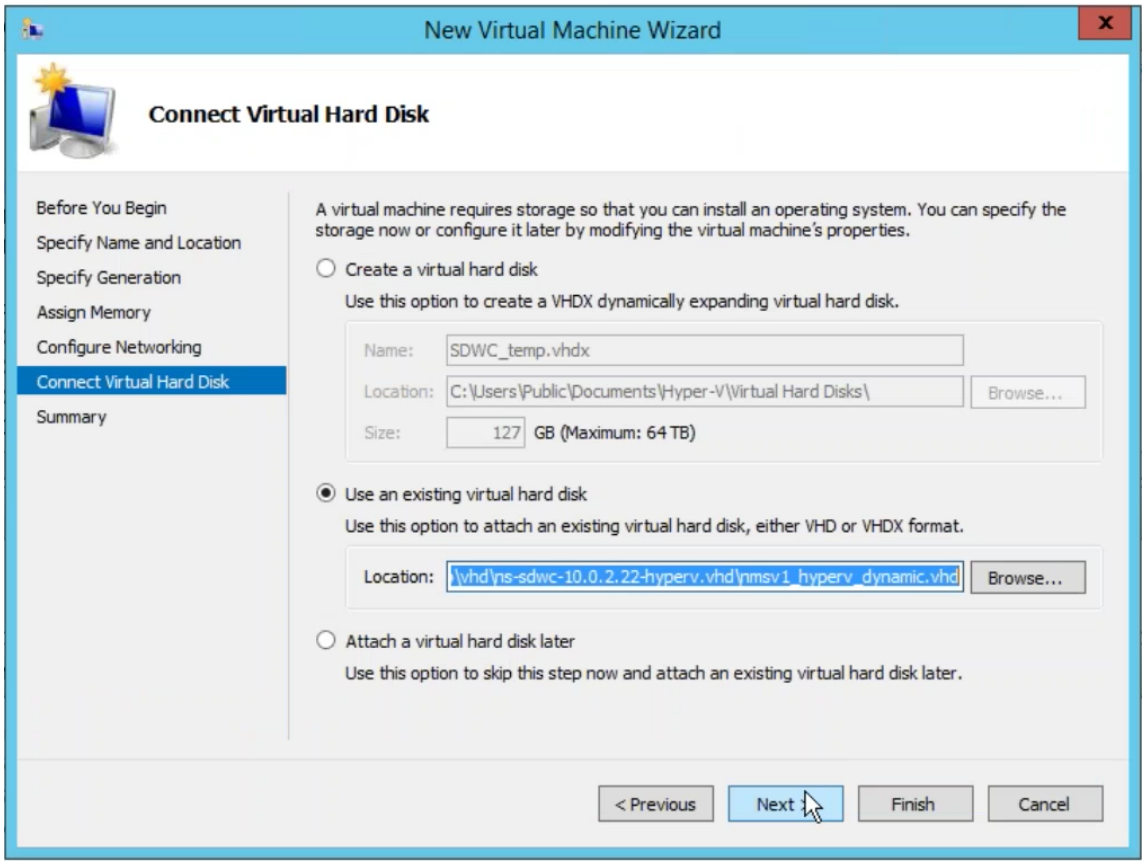


3. Elija la generación de VM requerida. Haga clic en **Siguiente**.
4. Asigne una memoria de 8 GB a la máquina virtual. Haga clic en **Siguiente**.

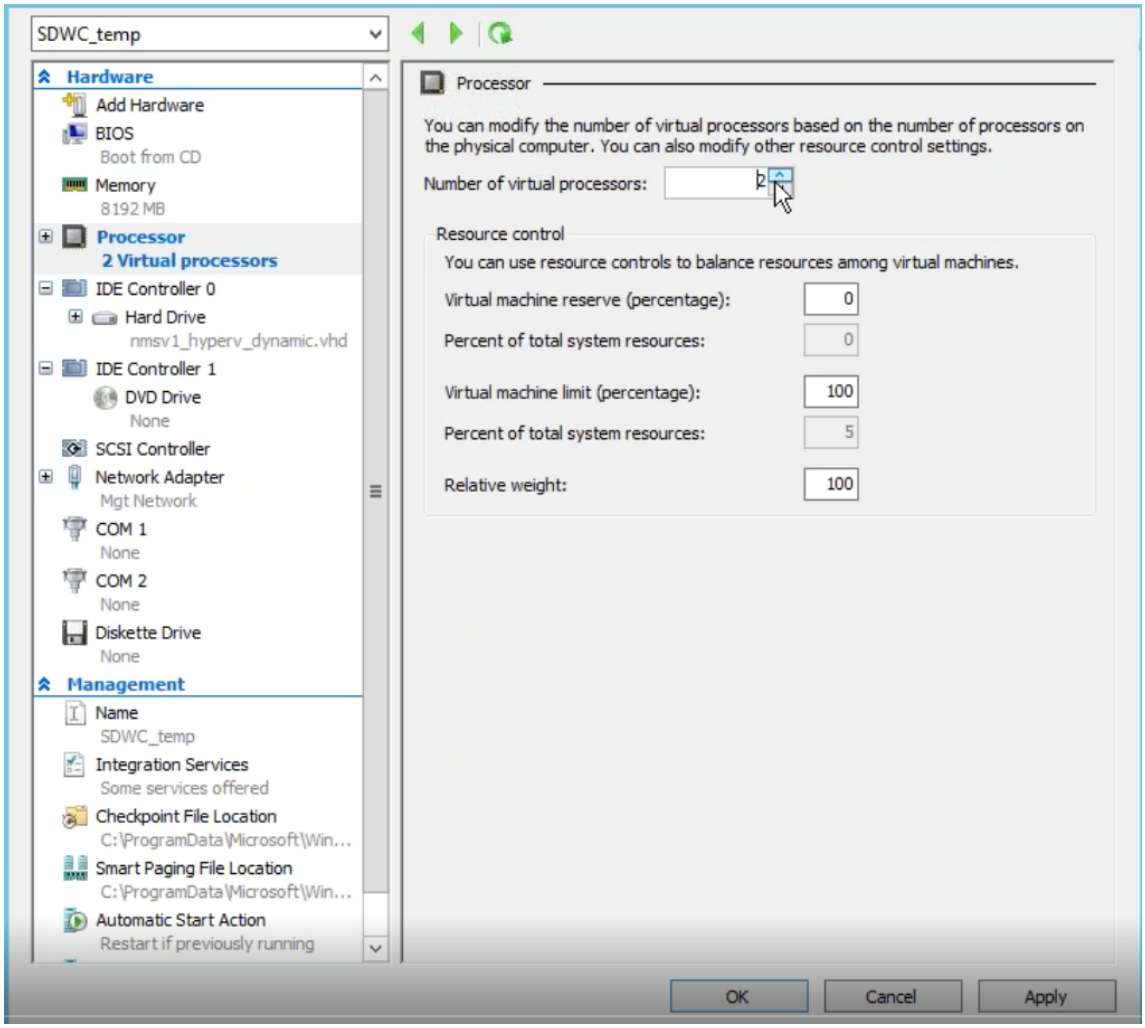
> **Nota**
>
> La máquina virtual Citrix SD-WAN Center requiere un mínimo de 8 GB de memoria para administrar hasta 64 sitios.Para obtener más información acerca de la memoria al número de sitios que se asignan, consulte Requisitos e instalación del sistema.



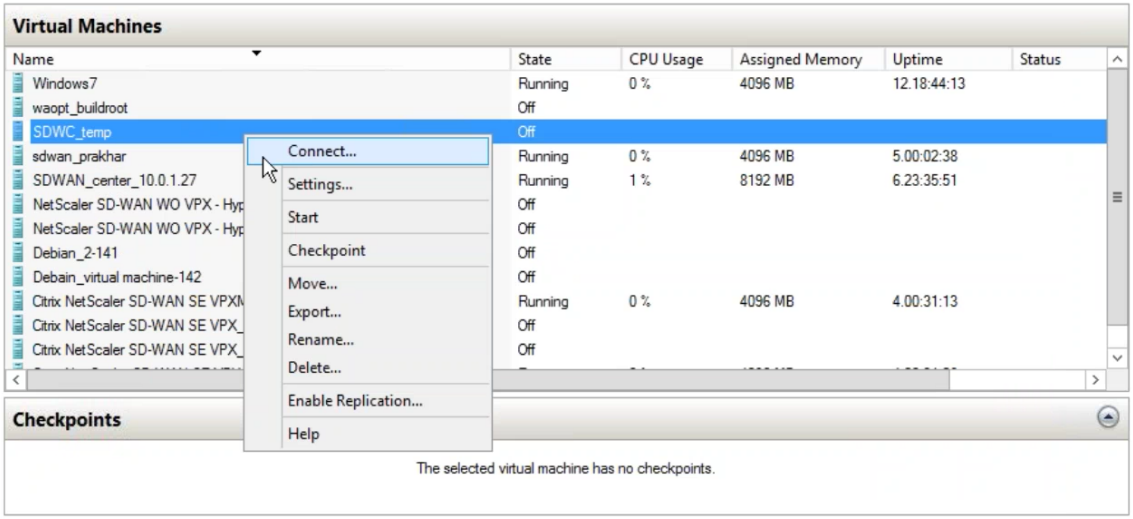
5. Elija el conmutador virtual que va a utilizar el adaptador de red de la máquina virtual, haga clic en **Siguiente**.
6. Seleccione **Usar un disco duro virtual existente**, busque y seleccione el archivo SD-WAN Center VHD que ha descargado. Haga clic en **Siguiente**.



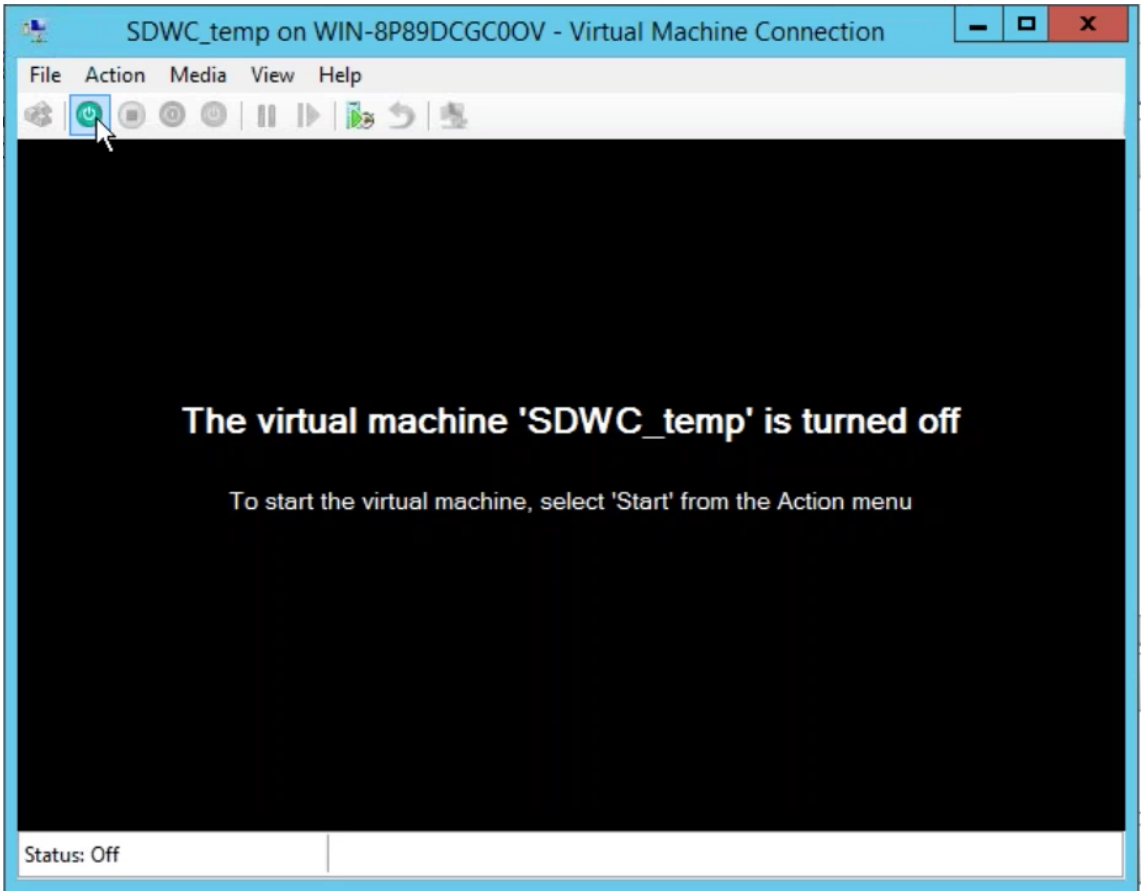
7. Revise el resumen de la máquina virtual y cambie la configuración si es necesario; de lo contrario, haga clic en **Finalizar**.La máquina virtual SD-WAN Center se crea y se muestra en la sección **Máquinas virtuales**.
8. Haga clic con el botón derecho en la máquina virtual SD-WAN Center y seleccione **Configuración**. Establezca el número de procesadores virtuales en cuatro y haga clic en **Aplicar**.



9. Haga clic con el botón derecho en la máquina virtual SD-WAN Center y seleccione **Conectar**.

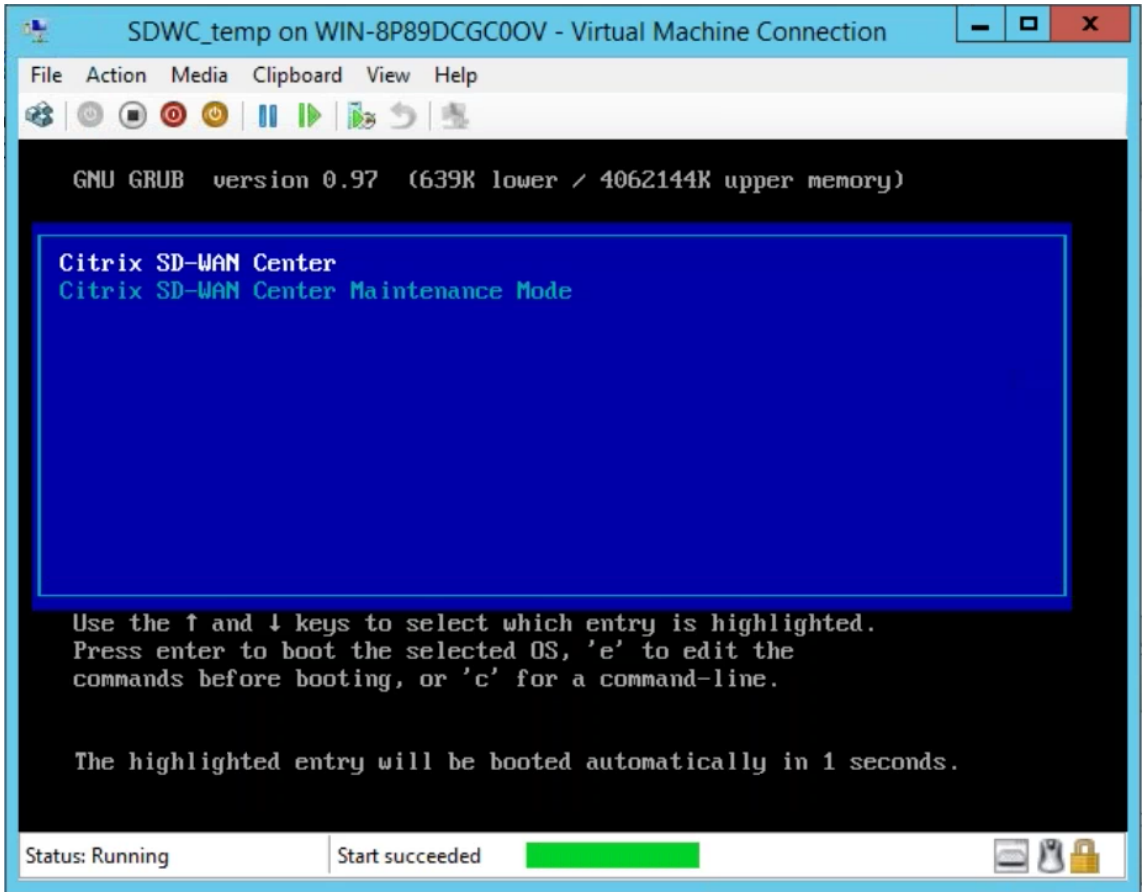


10. Haga clic en el botón **Inicio**.



> **Nota**
>
> La instalación inicial puede tardar hasta 50 minutos, dependiendo del número de CPU y RAM que haya configurado.

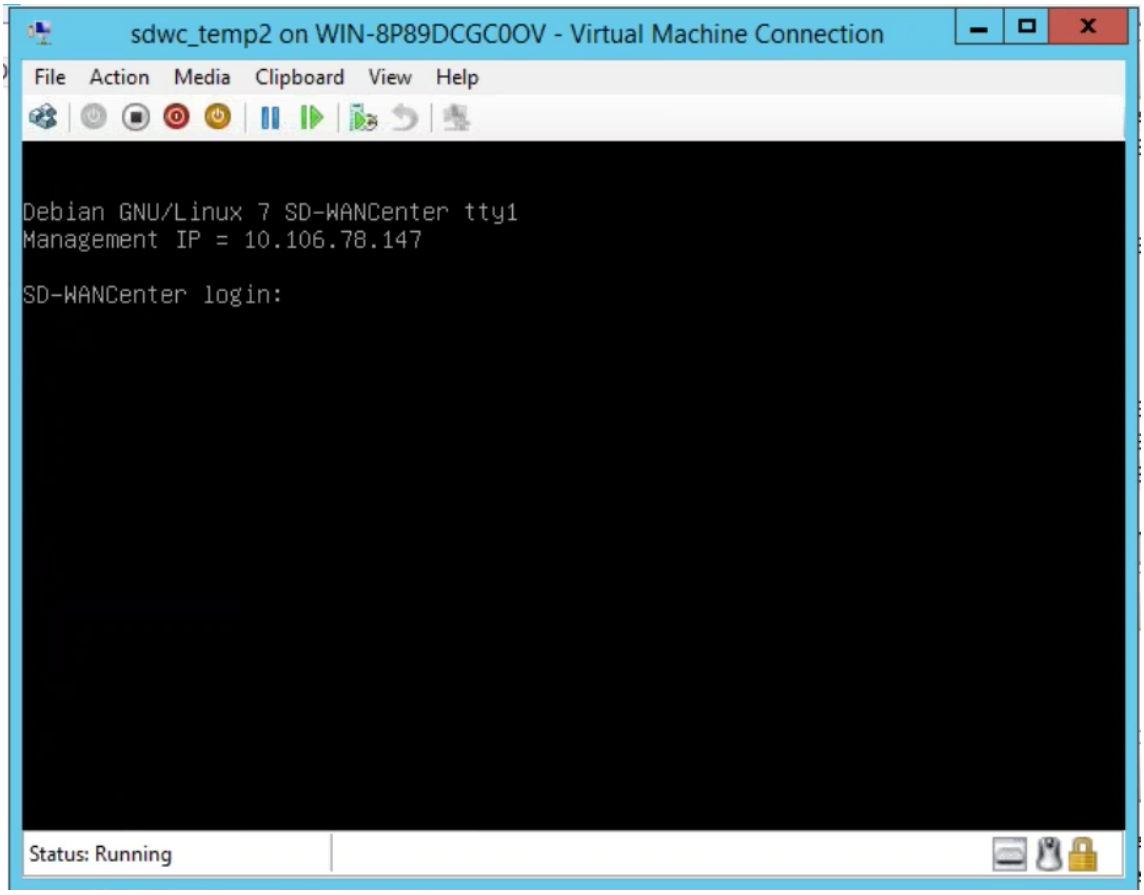
11. Una vez iniciada la máquina virtual, seleccione Citrix SD-WAN Center y pulse Entrar.



12. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual de SD-WAN Center son las siguientes:

    Inicio de sesión: admin

    Contraseña: contraseña



La dirección IP de administración se muestra en la consola. Utilice esta IP para acceder a la interfaz web de SD-WAN Center.

> **Nota**
>
> Si DHCP no está configurado en la red SD-WAN, debe introducir manualmente una dirección IP estática.

Para configurar una dirección IP estática como dirección IP de administración:

1. Inicie sesión en la máquina virtual. Las credenciales de inicio de sesión predeterminadas para la nueva máquina virtual de SD-WAN Center son las siguientes:

   Inicio de sesión: admin

   Contraseña: contraseña

2. En la consola, introduzca el comando CLI ***management_ip***.
3. Introduzca el comando **set interface <ipaddress> <subnetmask> <gateway>**, para configurar la dirección IP de administración.

Utilice la dirección IP de administración para acceder a la interfaz web de Citrix SD-WAN Center.

Citrix SD-WAN Center en Azure Marketplace mediante la plantilla de solución

April 13, 2021

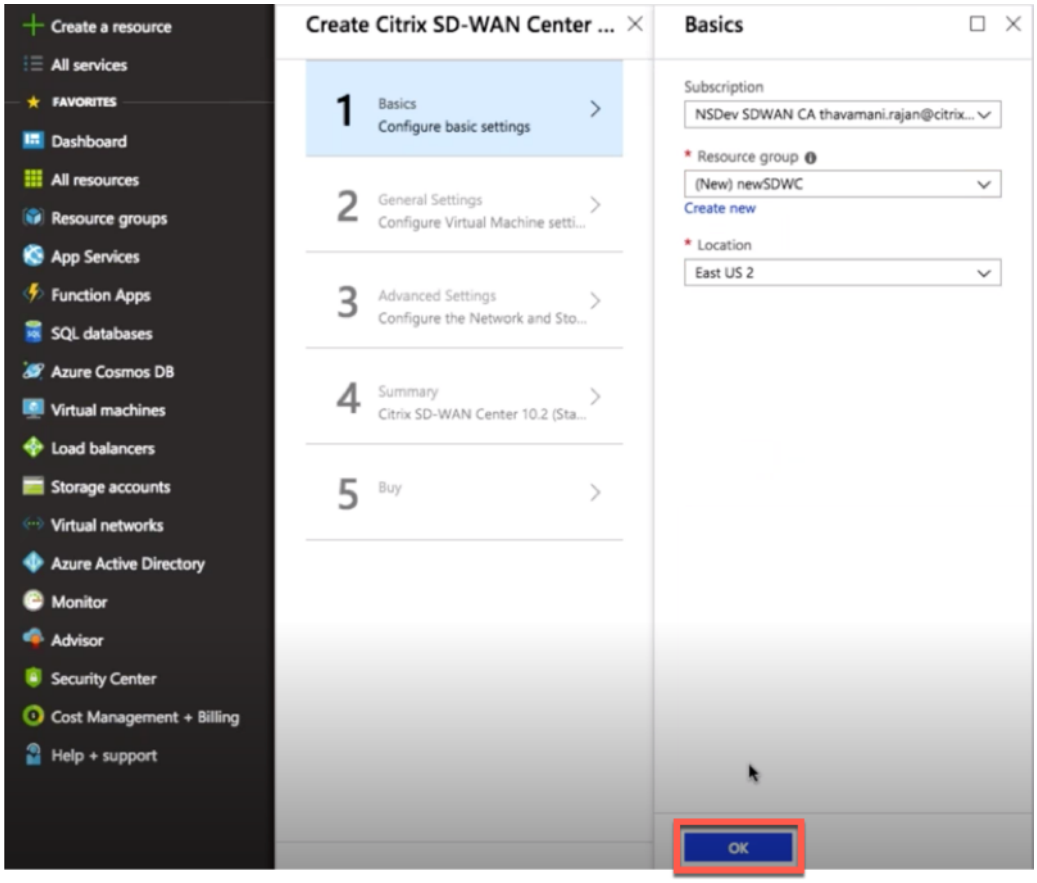
Citrix SD-WAN Center ya está disponible en Azure Marketplace. Puede implementar Citrix SD-WAN Center como máquina virtual (VM) en Azure Cloud mediante la plantilla de solución.

Antes de instalar la máquina virtual (VM) Citrix SD-WAN Center en Microsoft Azure, recopile la información necesaria tal como se describe en Requisitos e instalación del sistema.

Asegúrese de tener acceso a Microsoft Azure.

Para implementar Citrix SD-WAN Center VPX en Microsoft Azure:

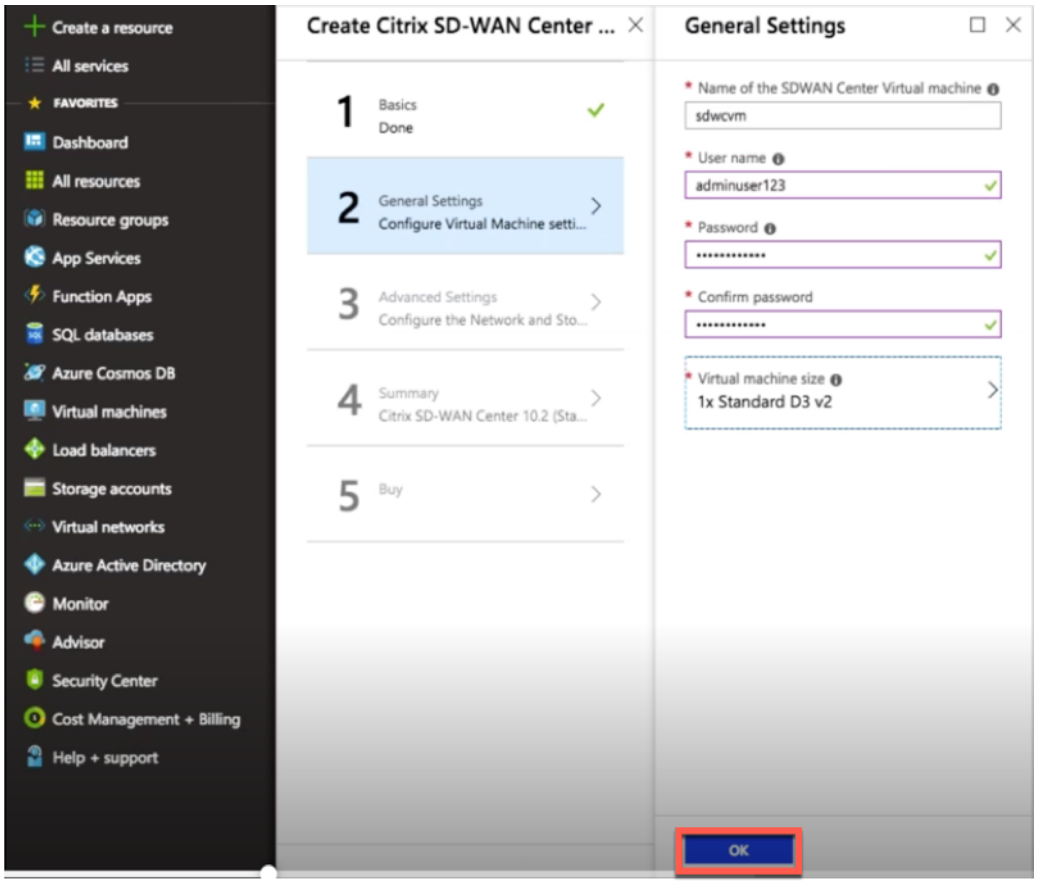
1. En Microsoft Azure, vaya a **Inicio > Marketplace**. Busque y seleccione **Citrix SD-WAN Center**.
2. Haga clic en **Crear** en la página **Centro de Citrix SD-WAN**. Aparecerá la página **Crear Centro Citrix SD-WAN**.
3. En la sección **Básicos**, seleccione el tipo de suscripción, el grupo de recursos y la ubicación. Haga clic en **Aceptar**.



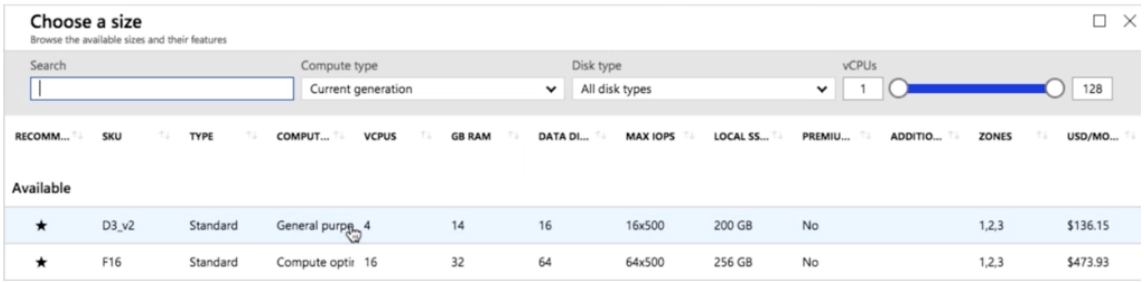
> **NOTA:**
>
> Un grupo de recursos es un contenedor que contiene recursos relacionados para una solución de Azure. El grupo de recursos puede incluir todos los recursos de la solución o solo los recursos que quiera administrar como grupo. Puede decidir cómo quiere asignar recursos a grupos de recursos en función de su implementación.

4. En la sección **Configuración general**, escriba el nombre y las credenciales que proporcionan acceso a nivel de administrador o privilegios para la máquina virtual Citrix SD-WAN Center.

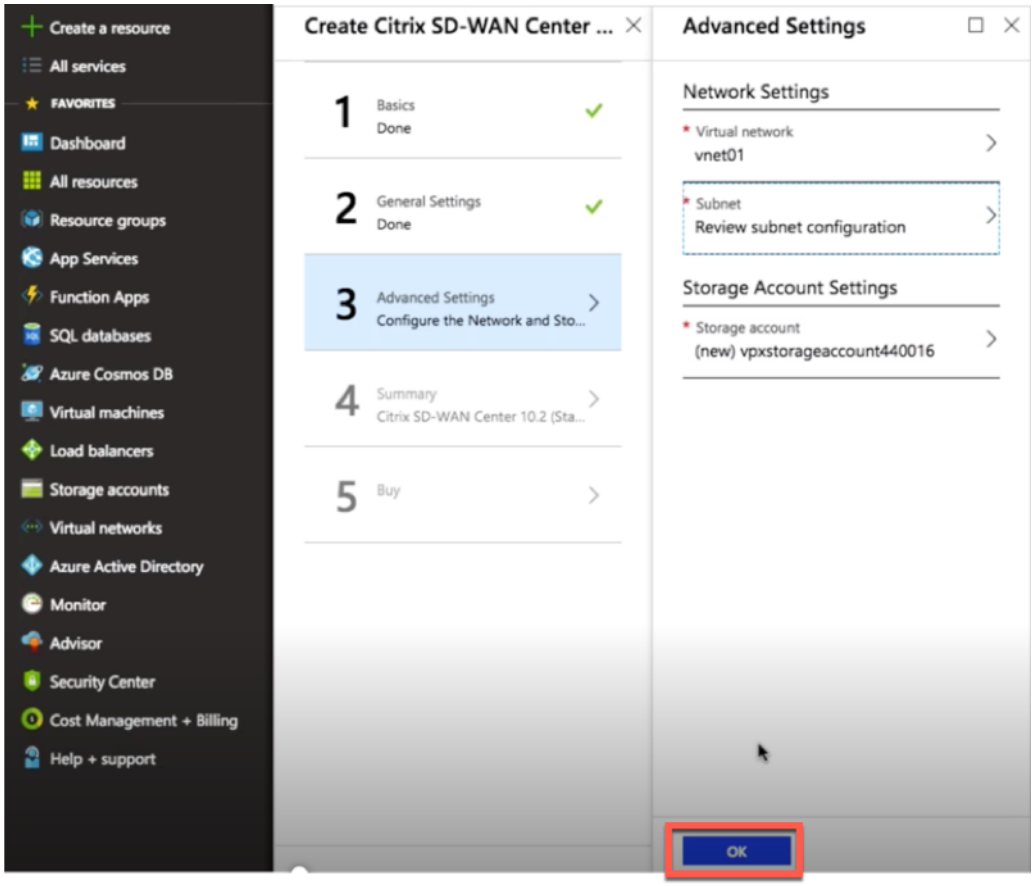
   Las credenciales que se proporcionan en este paso 4, también se usarían para establecer la contraseña para la cuenta de inicio de sesión del usuario **administrador** (la contraseña predeterminada de la cuenta de administrador se puede modificar con esta credencial de contraseña). Haga clic en **Aceptar**.



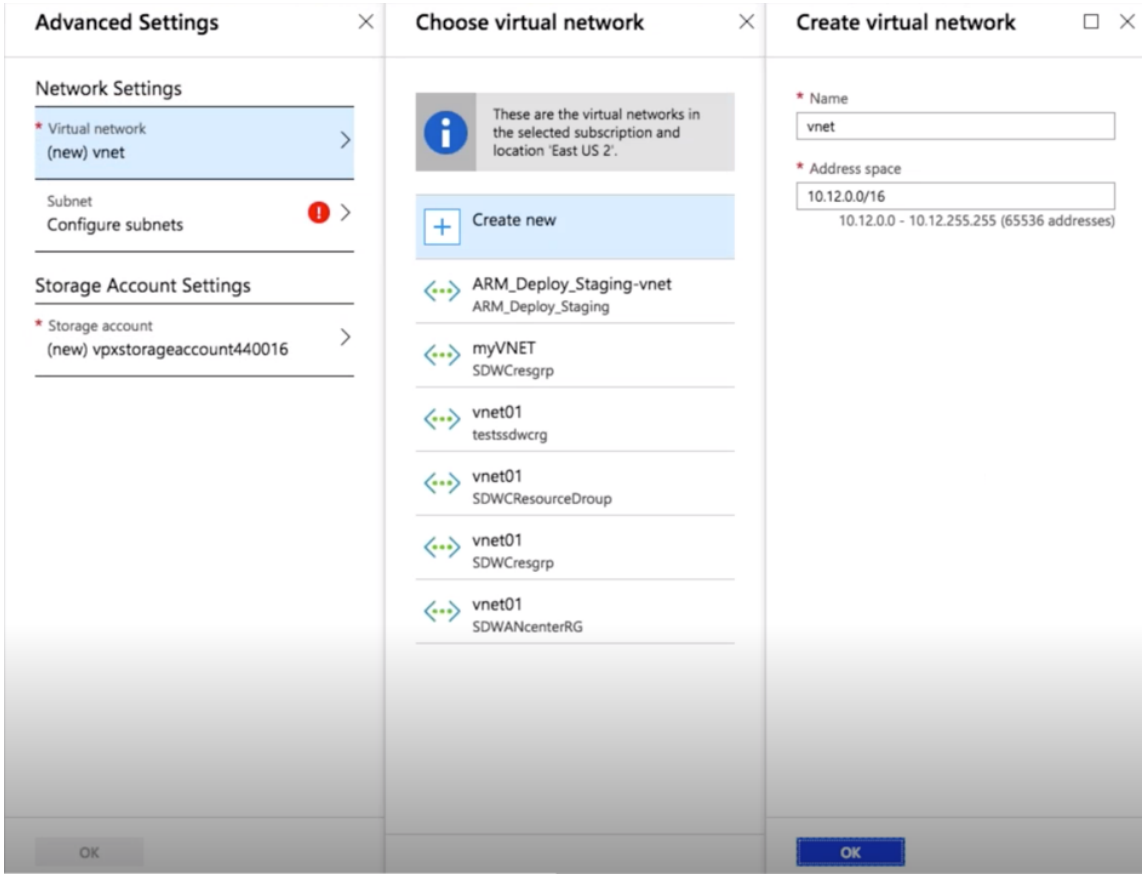
> **NOTA:**
>
> Actualmente hay dos tamaños disponibles tipos de instancia: **Standard_D3_v2** y **Standard_F16**. La instancia D3_v2 se puede utilizar para supervisar la red que tiene hasta 64 sitios. La instancia F16 es útil para supervisar la red que tiene hasta 128 sitios. También puede buscar y elegir un tamaño de máquina virtual disponible.



5. En la sección **Configuración avanzada**, configure la configuración de la **cuenta de red y almacenamiento** para **Citrix SD-WAN Center VPX** en función del número de sitios que se van a supervisar.

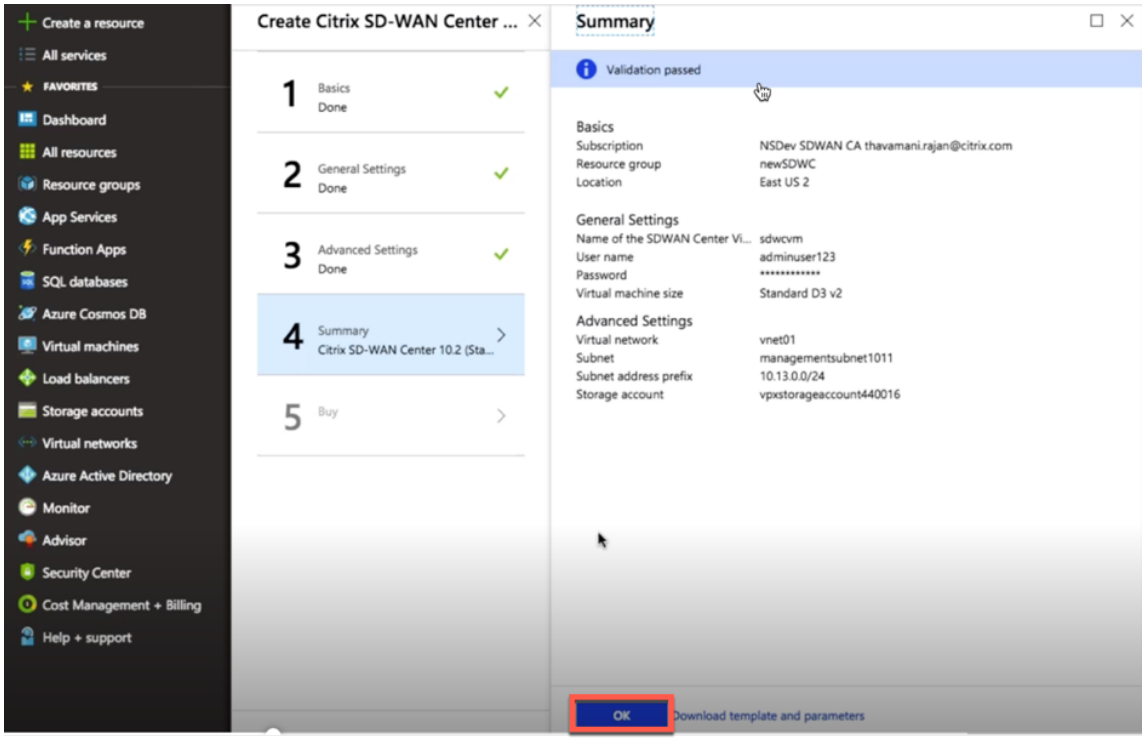


Seleccione la red virtual de la lista disponible o puede crear una nueva red virtual dando un **espacio de nombre** y un **espacio de dirección**.

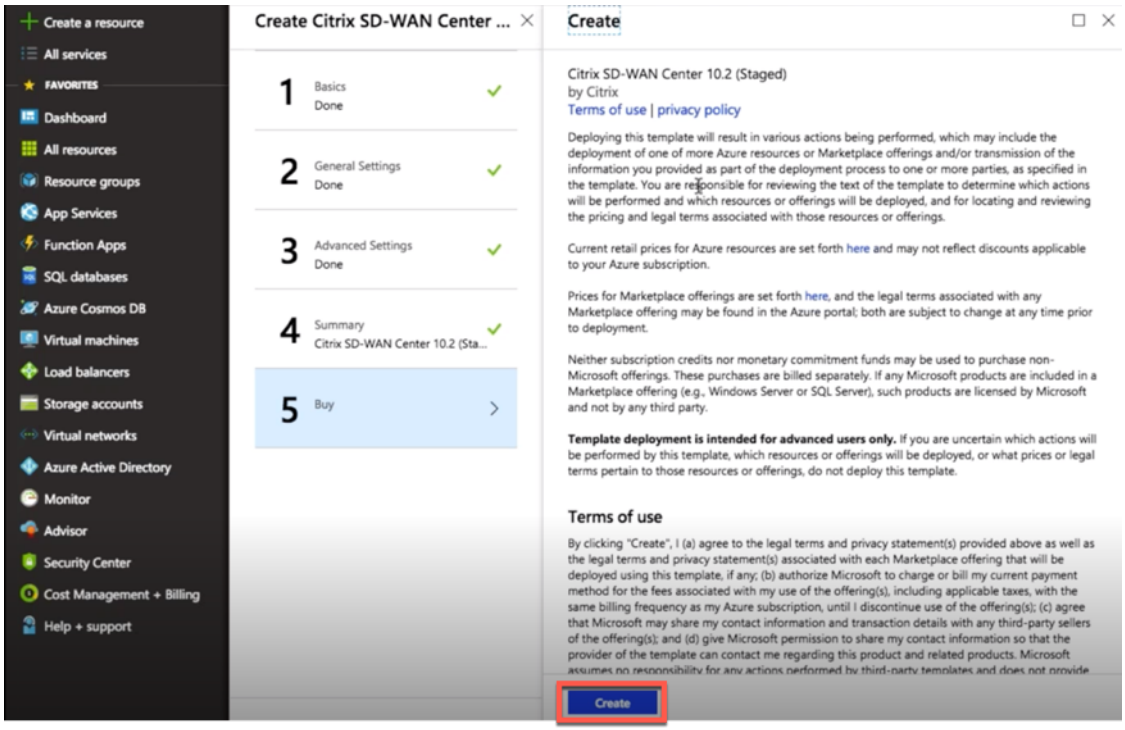


Seleccione **Subred** en la lista desplegable. Cree una **cuenta de almacenamiento** y haga clic en **Aceptar**.

6. La configuración proporcionada en los pasos anteriores se valida y aplica. Si ha configurado correctamente, aparecerá el mensaje de validación pasada. Haga clic en **Aceptar**.



7. Después de la implementación correcta, aparece la página **Crear**. Lea atentamente las **Condiciones de uso y la Directiva de privacidad** y haga clic en **Crear**.



Espere a que se complete el aprovisionamiento de VM y, a continuación, inicie sesión con la IP asignada a esa máquina virtual (verificando la sección de redes y mediante las credenciales de admin-

istrador (que se establecieron en el paso 4) y siga las directrices generales de implementación de SD-WAN Center.

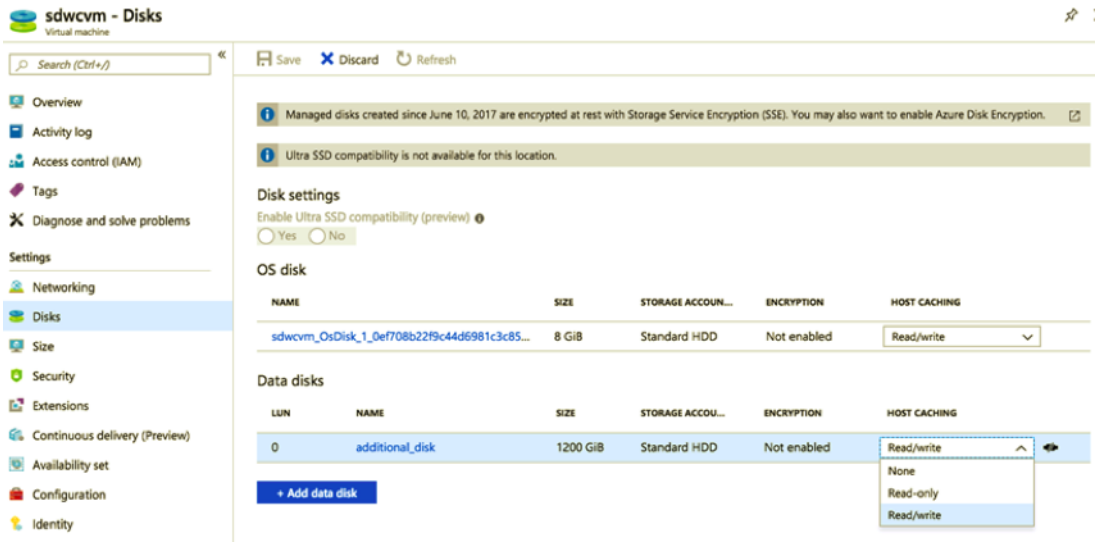
Agregar disco de datos

En esta sección se describe cómo adjuntar un nuevo disco de datos administrado a una máquina virtual (VM) mediante portal de Azure. El tamaño de la máquina virtual determina cuántos discos de datos puede adjuntar.

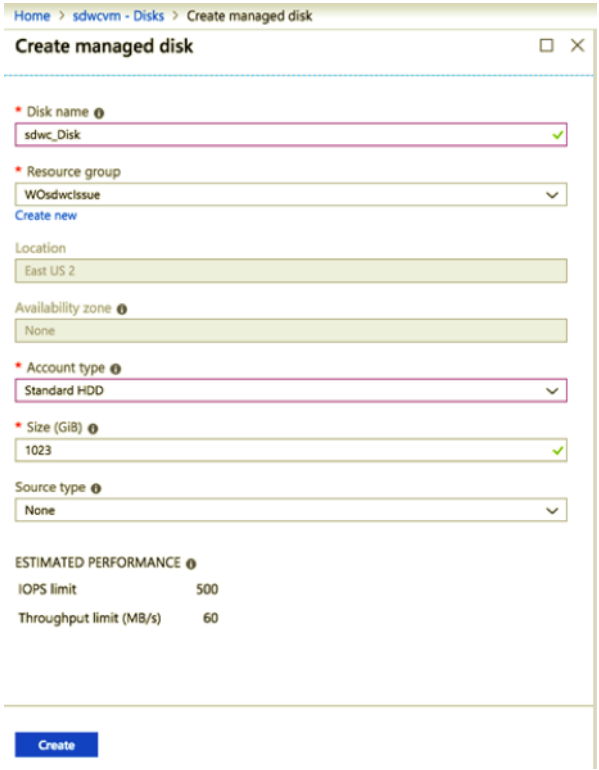
En el portal de Azure, en el menú de la izquierda, seleccione **Máquinas virtuales** y seleccione una máquina virtual de la lista.

Realice las siguientes acciones para agregar disco de datos adicional en Azure SD-WAN Center:

1. Apague la VM.
2. En el panel de VM, seleccione **Discos** en la sección **Configuración**.



3. Haga clic en **+ Agregar disco de datos** y cree un nuevo disco de datos con permiso de lectura y escritura.



Adjunte un disco rellenando los siguientes detalles obligatorios:

- **Nombre del disco**: Proporcione un nombre para el disco de datos SD-WAN Center.
- **Grupo de recursos**: Seleccione un grupo de recursos de la lista desplegable.
- **Tipo de cuenta**: Seleccione un tipo de cuenta en la lista desplegable.
- **Tamaño (GIB)**: Proporciona un tamaño en gibibyte.
- **Tipo de almacenamiento**: Seleccione un tipo de origen en la lista desplegable.

4. Una vez que haya terminado, haga clic en **Aceptar**.

Para activar la máquina virtual, consulte el Cambiar el almacenamiento activo al nuevo almacenamiento de datos tema.

Citrix SD-WAN Center en AWS en formato de imagen importable de VM

April 13, 2021

Citrix SD-WAN Center es un sistema de administración centralizado o una solución de administración de vidrio único que permite a las empresas configurar, supervisar y analizar todos los dispositivos Citrix SD-WAN en su WAN.

Crear instancias de un dispositivo virtual (AMI) SD-WAN Center en AWS

Necesita una cuenta de AWS para instalar un dispositivo virtual SD-WAN Center en una VPC de AWS. Puede crear una cuenta de AWS aquí. El Centro SD-WAN está disponible como una Amazon Machine Image (AMI) en AWS Marketplace.

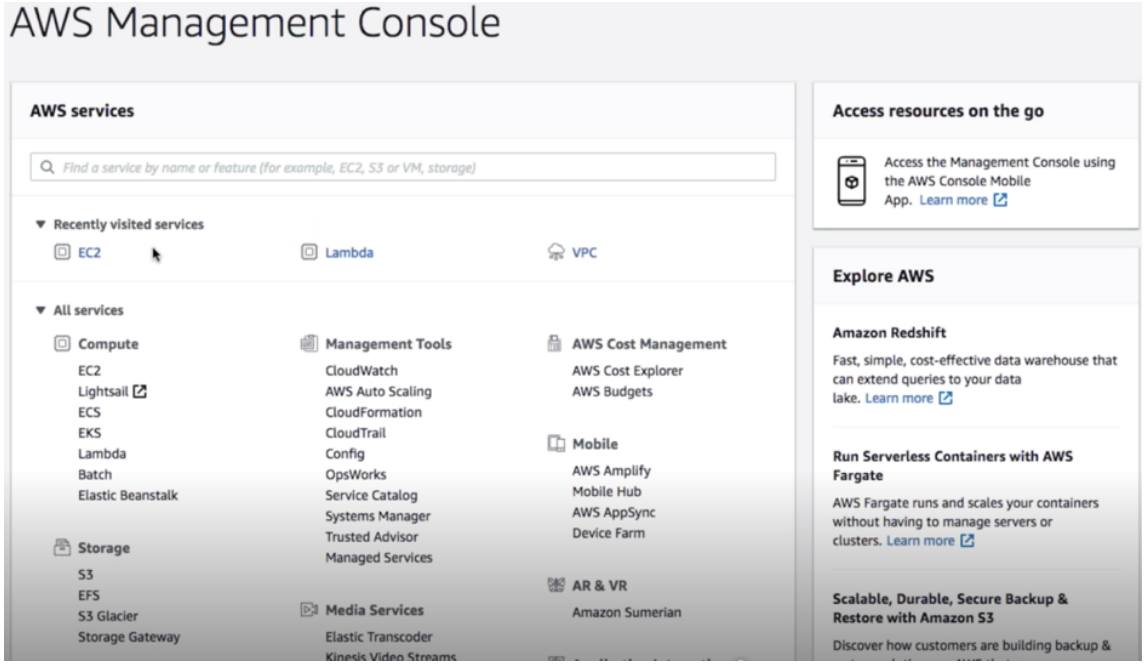
> **Nota**
>
> :
>
> Amazon realiza cambios frecuentes en sus páginas de AWS, por lo que es posible que las siguientes instrucciones no estén actualizadas.

Existen dos enfoques para crear instancias de un dispositivo virtual (AMI) de SD-WAN Center en AWS:

1. **Primer enfoque:** en un explorador web, escribahttp://aws.amazon.com/. Seleccione AWS Management Console en My Account para abrir Amazon Web Services (AWS).

   Segundo enfoque:
   en un explorador web, escribahttp://console.aws.amazon.compara abrir **Amazon Web Services**.

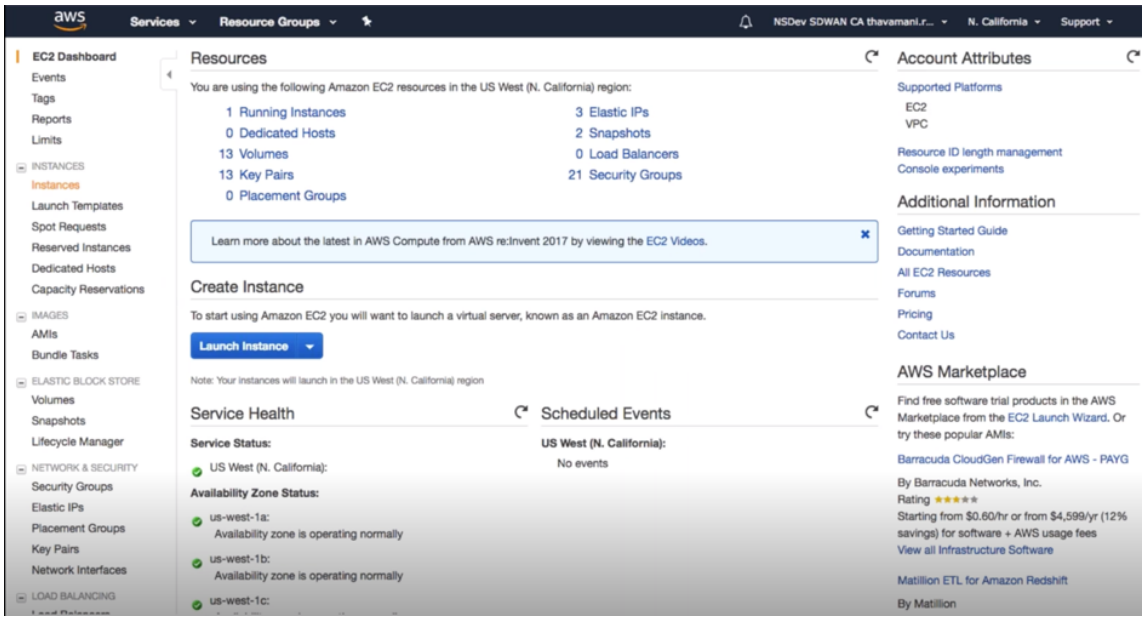
2. Utilice las credenciales de su cuenta de AWS para iniciar sesión. Esto le llevará a la página de **Amazon Web Services**. Puede ver la lista **Servicios visitados recientemente** junto con todos los demás servicios.

   Los dispositivos Citrix SD-WAN Center ofrecen EC2 como instancias de servicio de AWS.

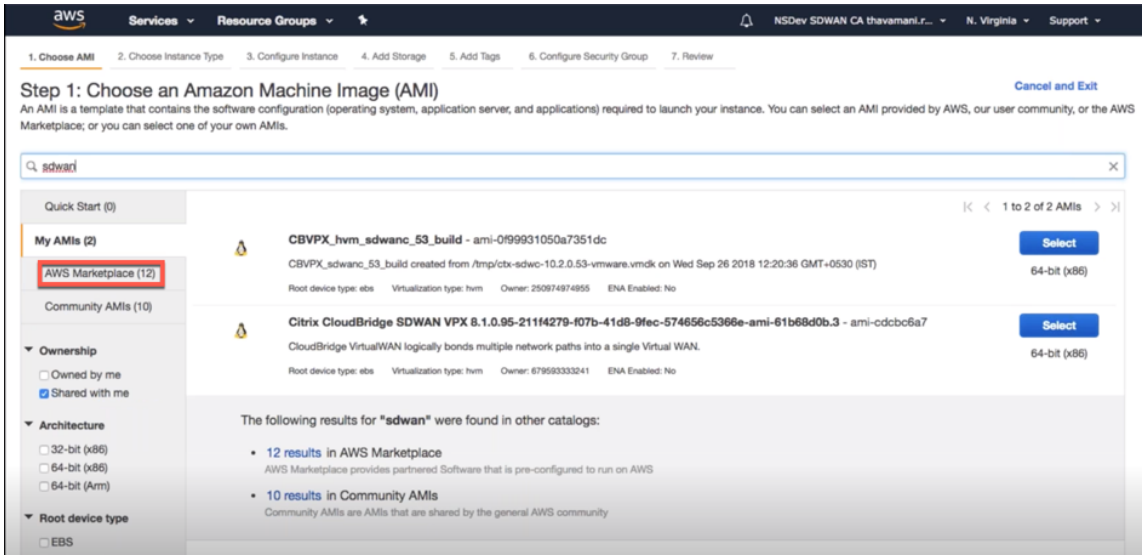
   - **EC2 Dashboard** : nube informática elástica, servicios e instancias virtuales de tamaño variable

3. Haga clic en **EC2** en la sección **Compute** y, a continuación, seleccione **Launch Instance**.



Puede seleccionar la opción **Iniciar instancia** o acceder manualmente a la pantalla **Instancia** seleccionando la ubicación de la opción **Instancias** en el lado izquierdo en **INSTANCIAS** (consulte la captura de pantalla anterior).

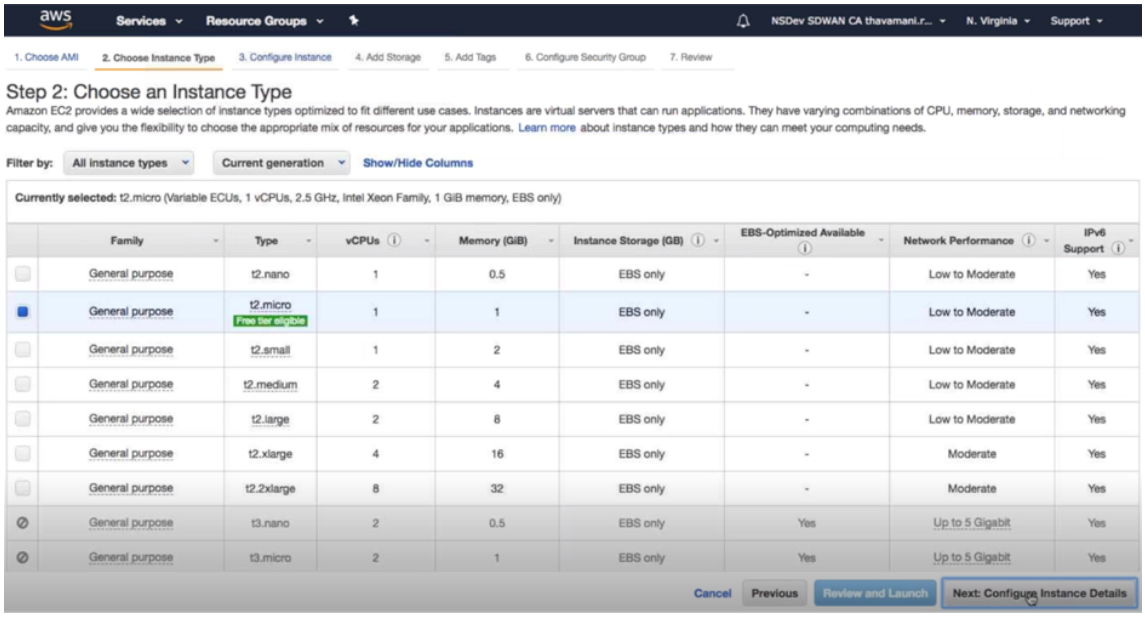
4. En la página **Elegir AMI**, haga clic en la ficha **AWS Marketplace**.
5. En el campo Texto Buscar, escriba SD-WAN para buscar la AMI de SD-WAN y haga clic en **Buscar**.



En la página de resultados de búsqueda, seleccione una de las AMI de Citrix SD-WAN Center con la versión más reciente, haga clic en **Seleccionar**.

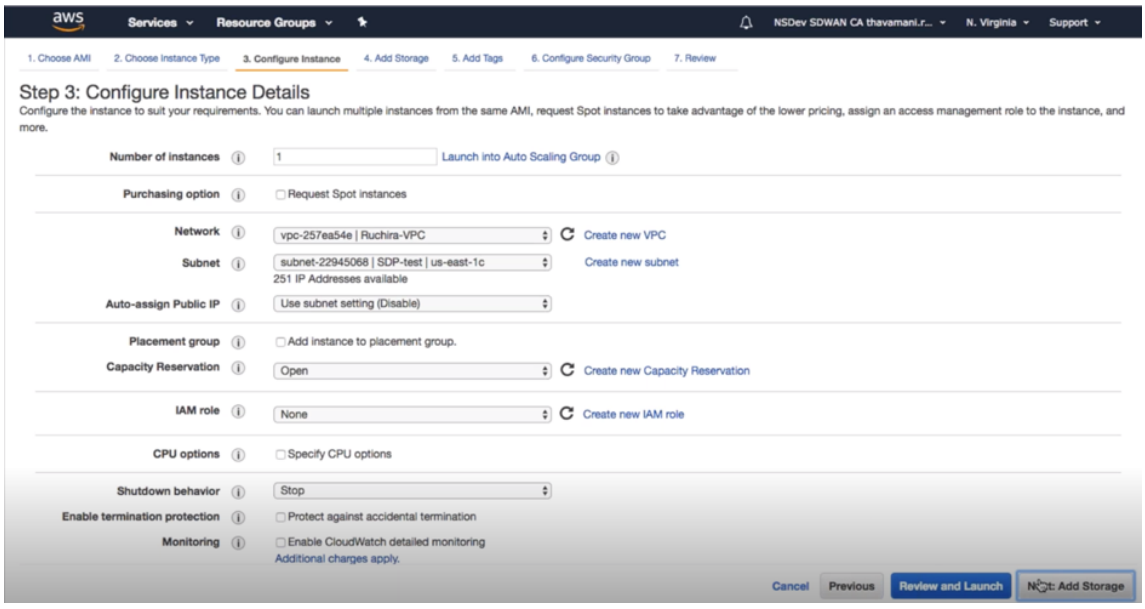
Una plantilla **AMI** contiene la configuración del software, incluido el sistema operativo, el servidor de aplicaciones y las aplicaciones. Esta plantilla es necesaria para iniciar instancias.

6. Elija un tipo de instancia y seleccione **Siguiente: Configurar Detalle de Instancia**. Puede filtrar la búsqueda seleccionando un tipo de instancia específico o todo tipo de instancia con la generación actual.



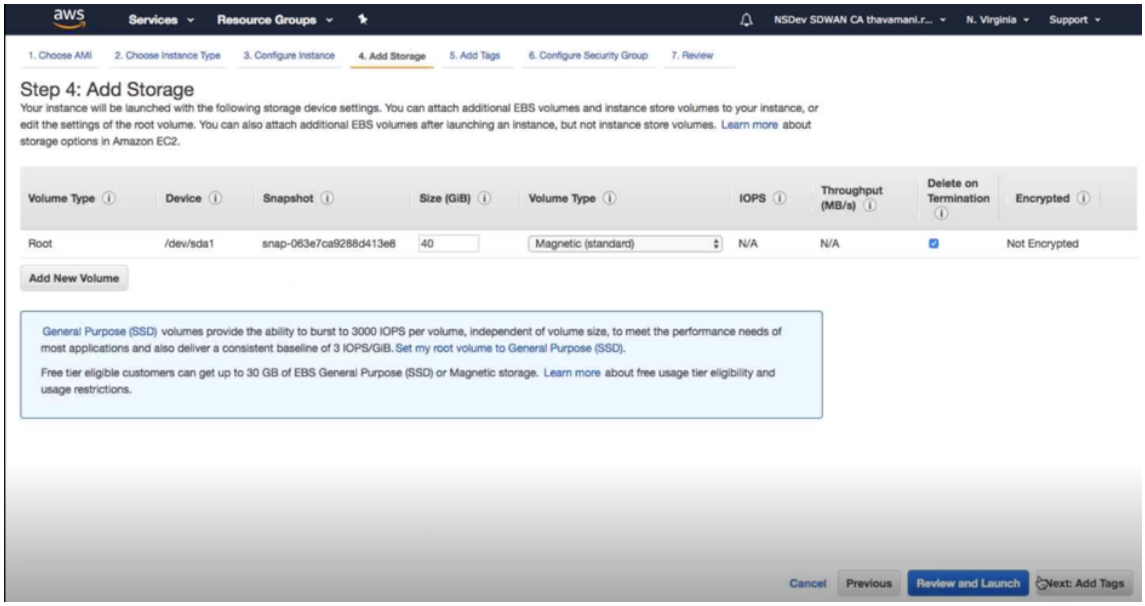
Amazon EC2 ofrece una amplia selección de tipos de instancias optimizados para adaptarse a diferentes casos de uso. Las instancias son servidores virtuales que pueden ejecutar aplicaciones.

7. En la página **Configurar instancia**, escriba 1 en el cuadro **de texto Número de instancias** y rellene los demás detalles, como Red, Subred, etc., para una instancia específica, según sea necesario. Haga clic en **Siguiente: Agregar almacenamiento**.

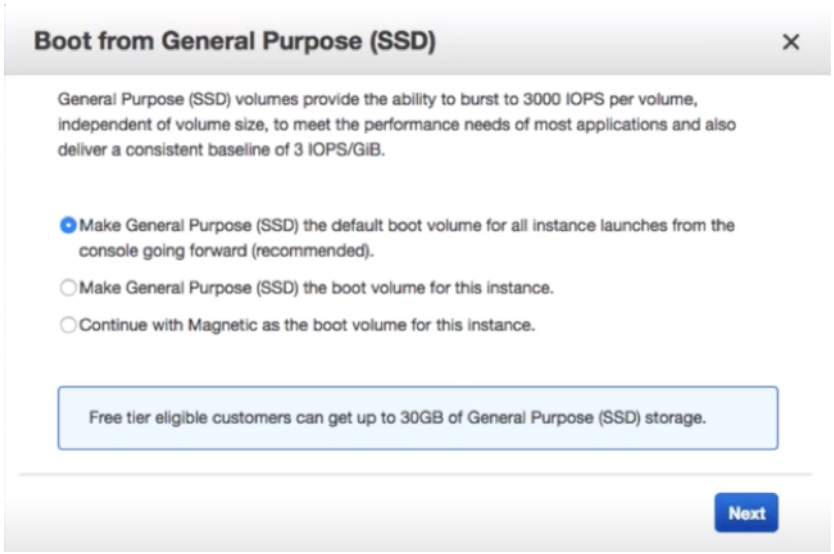


8. La instancia se inicia con la configuración del dispositivo de almacenamiento. Puede agregar

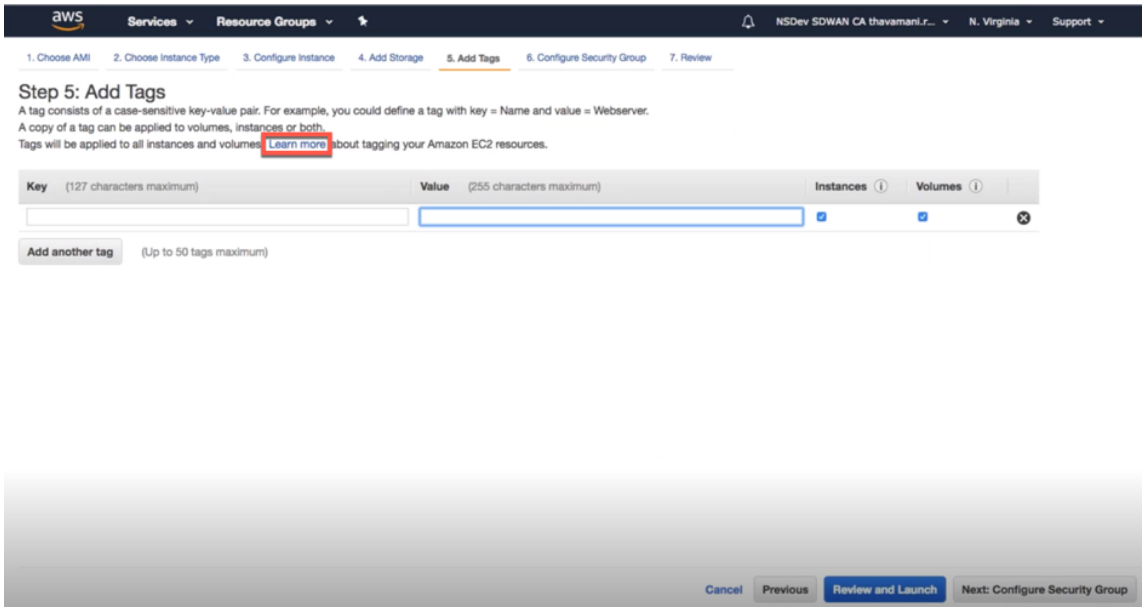
un nuevo volumen por separado una vez aprovisionada la instancia.



9. Haga clic en **Revisar y lanzar** para seleccionar la opción de volumen de arranque según sus requisitos. Haga clic en **Siguiente**.



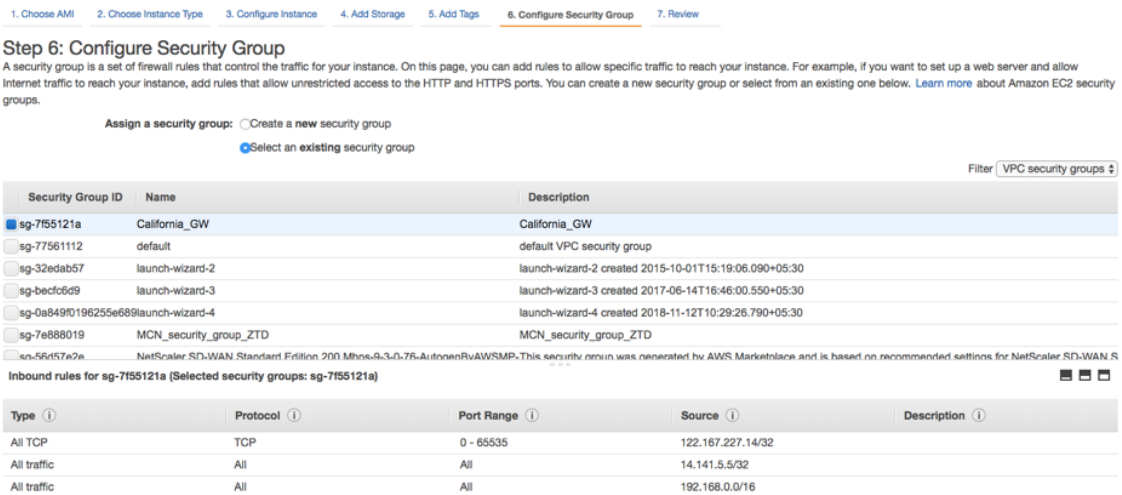
10. Agregue o defina una etiqueta con un **nombre clave** y un **valor**. Haga clic en **Más** información para obtener más información sobre el etiquetado. Puede agregar hasta 50 etiquetas como máximo. Haga clic en **Siguiente: Configurar grupo de seguridad**.



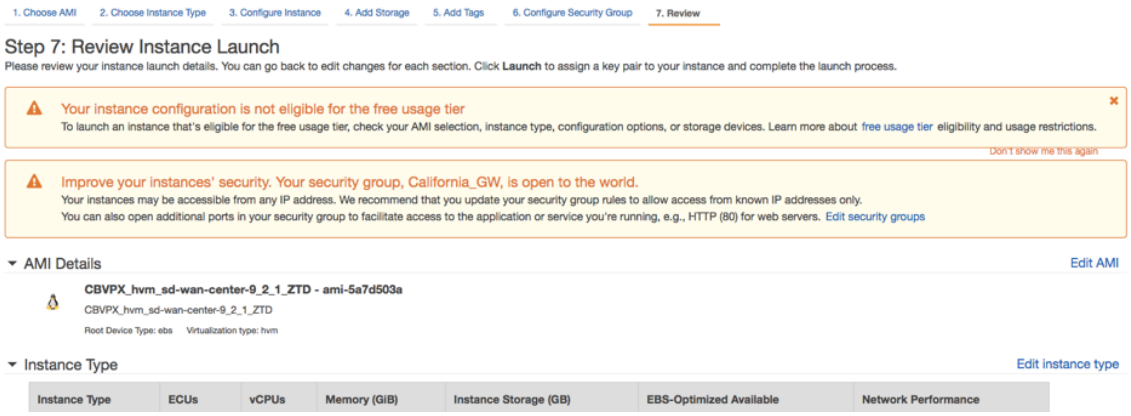
> **Nota**:
>
> NOTA: La longitud de una clave de etiqueta debe tener entre 1 y 127 caracteres.

11. Puede crear un grupo de seguridad general que ayude a controlar el tráfico de la instancia. Puede crear un nuevo grupo de seguridad o seleccionar un grupo de seguridad existente en la lista.

> **Nota**:
>
> Asegúrese de que el grupo de seguridad permita que las conexiones entrantes a través del puerto 2156 recopile datos de los dispositivos Citrix SD-WAN.



12. Revise los detalles del inicio de la instancia y haga clic en **Iniciar**. Aparece un cuadro emergente para solicitar la creación de un par de claves. Es obligatorio crear un par de claves para la instancia.



Autenticación de dos factores

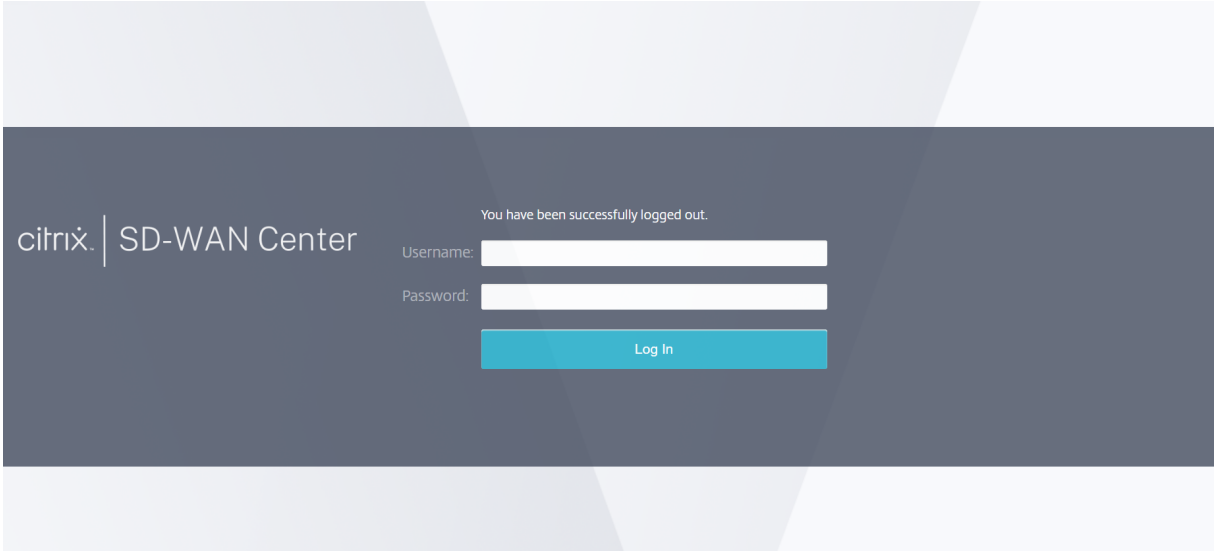
April 13, 2021

La autenticación de dos factores (TFA) presenta dos factores de autenticación para obtener acceso a Citrix SD-WAN Center para cuentas de usuario locales y remotas. Introduce una capa adicional de seguridad en la secuencia de inicio de sesión de Citrix SD-WAN Center.

El primer nivel de autenticación para una cuenta de usuario local se logra mediante la contraseña configurada en Citrix SD-WAN Center. Para obtener más información, consulte Cuentas de usuario.

El primer nivel de autenticación para una cuenta de usuario remoto se logra mediante el servidor de autenticación RADIUS o TACACS+ principal. Para obtener más información, consulte Autentificación principal.

Se puede configurar un servidor de autenticación RADIUS o TACACS+ secundario adicional para cuentas de usuario locales y remotas para habilitar la autenticación de dos factores. Para obtener más información, consulte Autentificación secundaria.



Credenciales de inicio de sesión de Citrix SD-WAN Center:

- **Nombre de usuario**: nombre de usuario configurado en SD-WAN Center o en el servidor de autenticación principal.
- Contraseña :**contraseña**configurada en SD-WAN Center o en el servidor de autenticación principal.
- **Contraseña secundaria**: contraseña configurada en el servidor de autenticación secundario.

> **Nota**
>
> La opción **Contraseña secundaria** solo aparece cuando se configura el servidor de autenticación secundario.

Autentificación principal

April 13, 2021

Puede configurar servidores de autenticación como RADIUS o TACACS+ para autenticar a los usuarios remotos que inician sesión en Citrix SD-WAN Center. La autenticación primaria es el primer factor de autenticación para usuarios remotos cuando la autenticación de dos factores está habilitada. Para obtener más información, consulte Autenticación de dos factores.

> **Nota**
>
> Asegúrese de que las cuentas de usuario se crean en los servidores de autenticación necesarios.

Servidor de autenticación RADIUS

Para utilizar la autenticación RADIUS, debe especificar y configurar al menos un servidor RADIUS. Opcionalmente, puede configurar servidores de copia de seguridad redundantes, hasta un máximo de tres servidores RADIUS. Los servidores se comprueban secuencialmente, comenzando por el servidor que aparece primero en la sección **Servidores**. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación RADIUS.

Para habilitar y configurar la autenticación RADIUS:

1. En la interfaz web de Citrix SD-WAN Center, vaya a **Administración** > **Configuración de usuario/autenticación**.
2. En la sección **Autenticación principal** > **Autenticación RADIUS**, active la casilla de verificación **Habilitar autenticación RADIUS**.

   > **Nota**
   >
   > Si la autenticación TACACS+ ya está habilitada, se inhabilita.

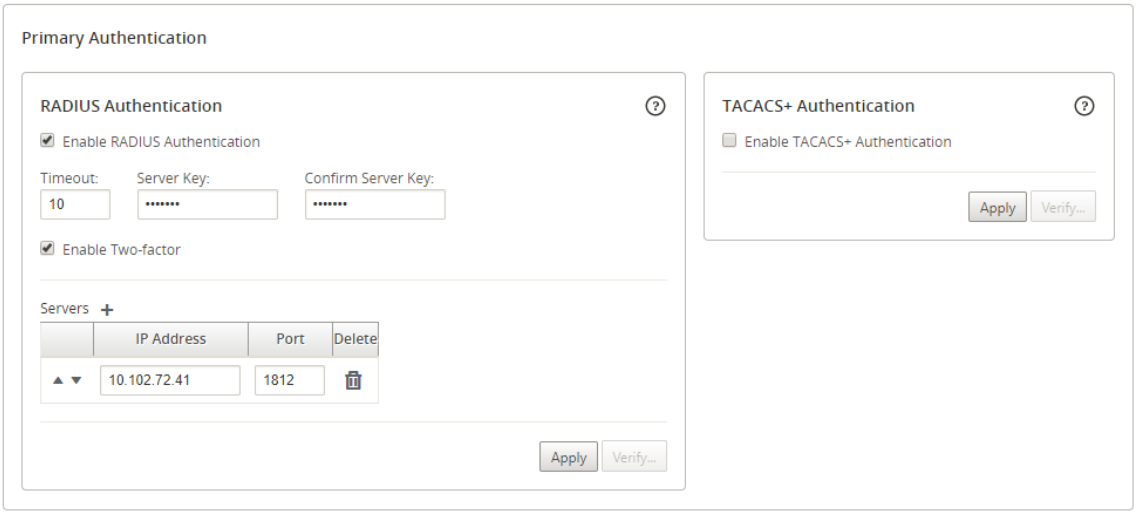
3. En el campo **Tiempo de espera**, introduzca el intervalo de tiempo (en segundos) para esperar una respuesta de autenticación del servidor RADIUS.

   El valor de tiempo de espera debe ser menor o igual a 60 segundos.
4. En el campo **Clave del servidor**, escriba una clave secreta para utilizarla cuando se conecte a los servidores RADIUS.
5. En los campos **Confirmar clave del servidor**, vuelva a introducir la clave secreta.

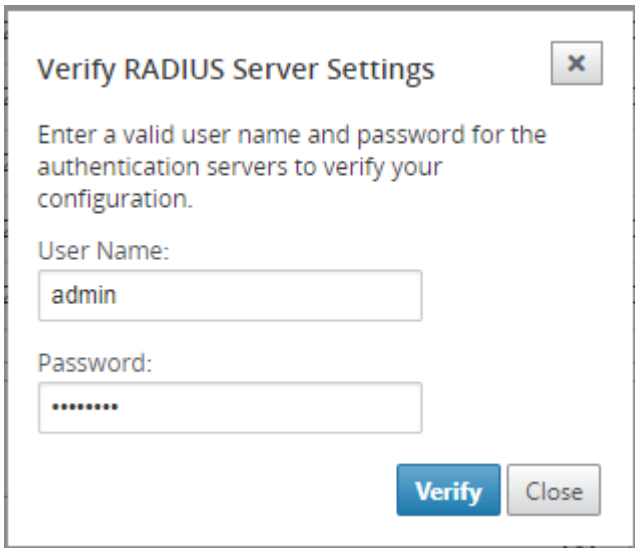
   > **Nota**
   >
   > Las opciones de**Timeout**y**Clave de servidor**se aplican a todos los servidores configurados**.**
6. Seleccione **Activar dos factores** para habilitar la autenticación de dos factores.

   > **Nota**
   >
   > La opción **Habilitar dos factores** aparece solo cuando se configura el servidor de autenticación secundario.
   >
   > Configure un servidor de autenticación secundario, ya sea RADIUS o TACAS+. Para obtener más información, consulte Autentificación secundaria.
7. Haga clic en el icono más (+) situado junto a **Servidores** para agregar un servidor RADIUS.
8. En el campo **Dirección IP**, introduzca la dirección IP del host para el servidor RADIUS.

9. En el campo **Puerto**, introduzca el número de puerto para el servidor RADIUS. El número de puerto predeterminado es 1812.



10. Haga clic en **Aplicar**.
11. Haga clic en **Verificar** para verificar la conexión con el servidor RADIUS. Aparece el cuadro de diálogo **Verificar configuración del servidor RADIUS**.



12. Introduzca un nombre de usuario y una contraseña válidos para los servidores de autenticación y haga clic en**Verificar**.

Para configurar más servidores, repita los pasos 7 a 12.

Servidor de autenticación TACACS+

Para utilizar TACACS+, debe especificar y configurar al menos un servidor TACACS+. Opcionalmente, puede configurar servidores de copia de seguridad redundantes, hasta un máximo de tres servidores

TACACS+. Los servidores se comprueban secuencialmente, comenzando por el servidor que aparece primero en la sección **Servidores**. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación TACACS+.

Para habilitar y configurar la autenticación TACACS+:

1. En la interfaz web de Citrix SD-WAN Center, vaya a **Administración** > **Configuración de usuario/autenticación**.
2. En la sección **Autenticación primaria** > **Autenticación TACACS+**, active la casilla **Habilitar autenticación TACACS+**.

   > **Nota**
   >
   > Si la autenticación RADIUS ya está habilitada, se inhabilita.

3. En el campo **Tiempo de espera**, introduzca el intervalo de tiempo (en segundos) para esperar una respuesta de autenticación del servidor TACACS+.

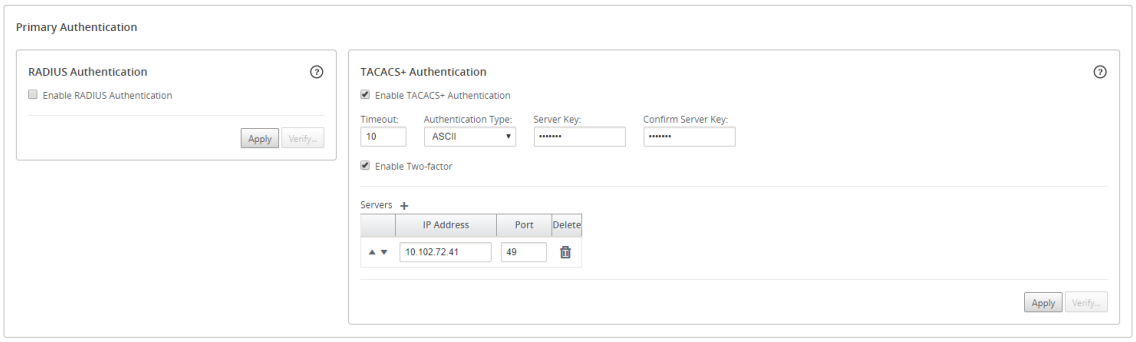
   El valor de tiempo de espera debe ser menor o igual a 60 segundos.
4. En el campo **Tipo de autenticación**, seleccione el método de cifrado que se utilizará para enviar el nombre de usuario y la contraseña al servidor TACACS+.
5. En el campo **Clave del servidor**, escriba una clave secreta para usarla cuando se conecte a los servidores TACACS+.
6. En los campos **Confirmar clave del servidor**, vuelva a introducir la clave secreta.

   > **Nota**
   >
   > Los valores de **Tiempo de espera**, **Tipo de autenticación** y **Clave de servidor** se aplican a todos los servidores configurados.

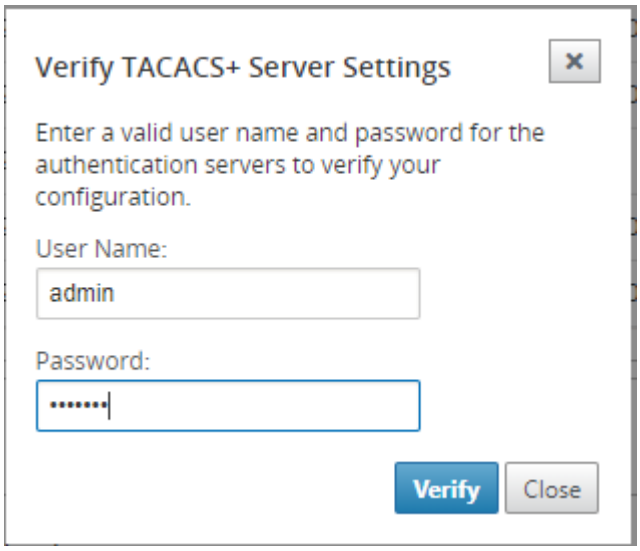
7. Seleccione **Activar dos factores** para habilitar la autenticación de dos factores.

   > **Nota**
   >
   > La opción **Habilitar dos factores** aparece solo cuando se configura el servidor de autenticación secundario.
   >
   > Configure un servidor de autenticación secundario, ya sea RADIUS o TACAS+. Para obtener más información, consulte Autentificación secundaria.

8. Haga clic en el icono más (+) situado junto a **Servidores** para agregar un servidor TACACS+.
9. En el campo **Dirección IP**, introduzca la dirección IP del host para el servidor TACACS+.
10. En el campo **Puerto**, introduzca el número de puerto para el servidor TACACS+. El número de puerto predeterminado es 49.



11. Haga clic en **Aplicar**.
12. Haga clic en **Verificar** para verificar la conexión con el servidor RADIUS. Aparece el cuadro de diálogo **Verificar configuración del servidor TACACS+**.



13. Introduzca un nombre de usuario y una contraseña válidos para los servidores de autenticación y haga clic en**Verificar**.

    Para configurar más servidores, repita los pasos 8 a 13.

Autentificación secundaria

April 13, 2021

La autenticación secundaria está configurada para habilitar la autenticación de dos factores para cuentas de usuario locales y remotas. Puede configurar el servidor de autenticación RADIUS o TACACS+ como el servicio de autenticación secundario. Para obtener más información, consulte Autenticación de dos factores.

> **Nota**
>
> Asegúrese de que las cuentas de usuario se crean en los servidores de autenticación necesarios. La contraseña de la cuenta de usuario debe utilizarse como segundo factor en la secuencia de inicio de sesión de Citrix SD-WAN Center.

Servidor de autenticación RADIUS secundario

Para utilizar la autenticación RADIUS, debe especificar y configurar al menos un servidor RADIUS. Opcionalmente, puede configurar servidores de copia de seguridad redundantes, hasta un máximo de tres servidores RADIUS. Los servidores se comprueban secuencialmente, comenzando por el servidor que aparece primero en la sección **Servidores**. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación RADIUS.

Para habilitar y configurar la autenticación RADIUS:

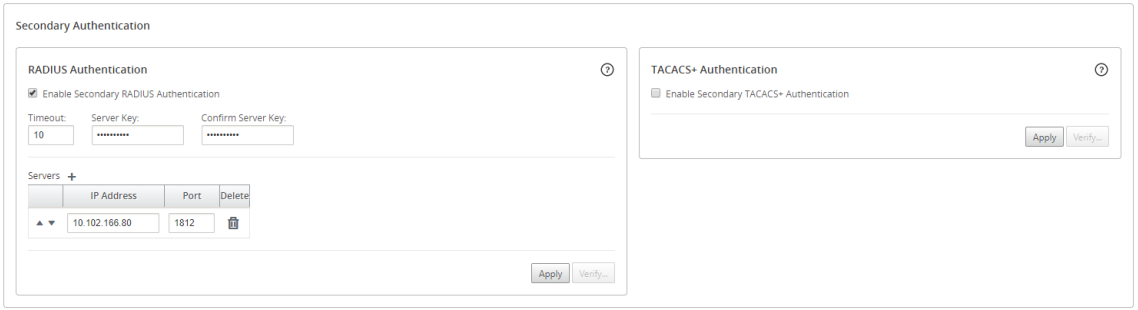
1. En la interfaz web de Citrix SD-WAN Center, vaya a **Administración** > **Configuración de usuario/autenticación**.
2. En la sección **Autenticación secundaria** > **Autenticación RADIUS**, active la casilla de verificación **Habilitar autenticación RADIUS secundaria**.

   > **Nota**
   >
   > Si la autenticación TACACS+ ya está habilitada, se inhabilita.

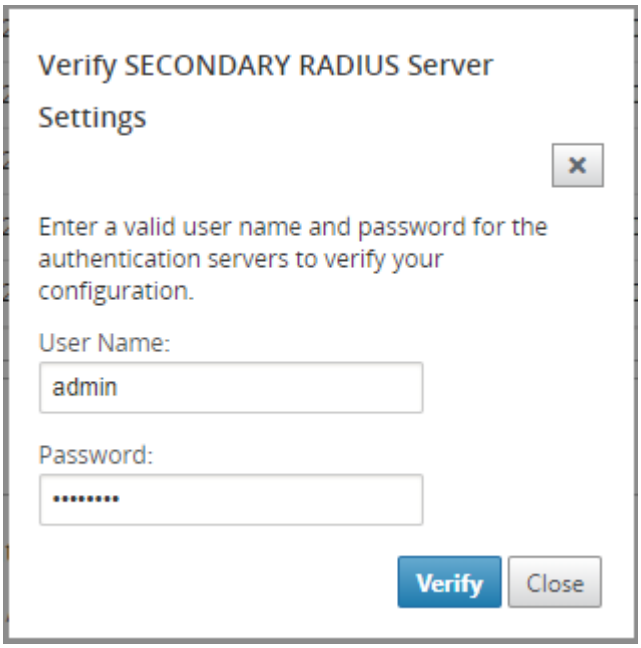
3. En el campo **Tiempo de espera**, introduzca el intervalo de tiempo (en segundos) para esperar una respuesta de autenticación del servidor RADIUS.

   El valor de tiempo de espera debe ser menor o igual a 60 segundos.
4. En el campo **Clave del servidor**, escriba una clave secreta para utilizarla cuando se conecte a los servidores RADIUS.
5. En los campos **Confirmar clave del servidor**, vuelva a introducir la clave secreta.

   > **Nota**
   >
   > Las opciones de**Timeout**y**Clave de servidor**se aplican a todos los servidores configurados**.**
6. Haga clic en el icono más (+) situado junto a **Servidores** para agregar un servidor RADIUS.
7. En el campo **Dirección IP**, introduzca la dirección IP del host para el servidor RADIUS.
8. En el campo **Puerto**, introduzca el número de puerto para el servidor RADIUS. El número de puerto predeterminado es 1812.



9. Haga clic en **Aplicar**.
10. Haga clic en **Verificar** para verificar la conexión con el servidor RADIUS. Aparece el cuadro de diálogo **Verificar configuración del servidor RADIUS secundario**.



11. Introduzca un nombre de usuario y una contraseña válidos para los servidores de autenticación y haga clic en**Verificar**.

Para configurar más servidores, repita los pasos 6 a 11.

Servidor de autenticación TACACS+ secundario

Para utilizar TACACS+, debe especificar y configurar al menos un servidor TACACS+. Opcionalmente, puede configurar servidores de copia de seguridad redundantes, hasta un máximo de tres servidores TACACS+. Los servidores se comprueban secuencialmente, comenzando por el servidor que aparece primero en la sección **Servidores**. Asegúrese de que las cuentas de usuario necesarias se crean en el servidor de autenticación TACACS+.

Para habilitar y configurar la autenticación TACACS+:

1. En la interfaz web de SD-WAN Center, vaya a **Administración** > **Configuración de usuario/autenticación**.
2. En la sección **Autenticación secundaria** > **Autenticación TACACS+**, active la casilla de verificación **Habilitar autenticación TACACS+ secundaria**.

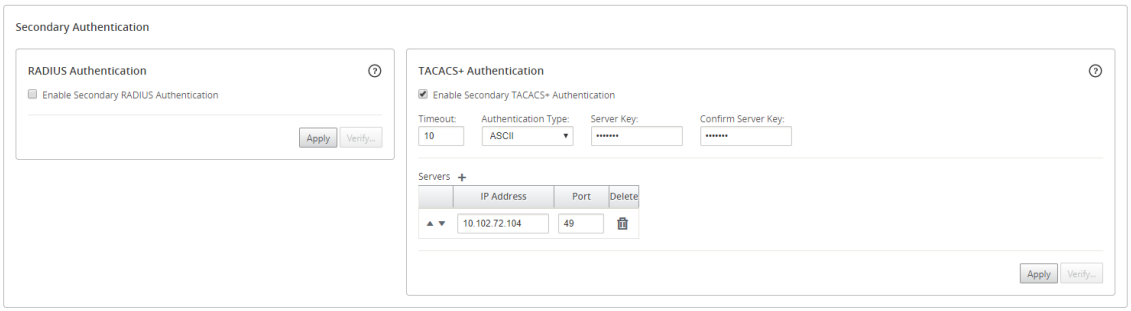
   > **Nota**
   >
   > Si la autenticación RADIUS ya está habilitada, se inhabilita.

3. En el campo **Tiempo de espera**, introduzca el intervalo de tiempo (en segundos) para esperar una respuesta de autenticación del servidor TACACS+.

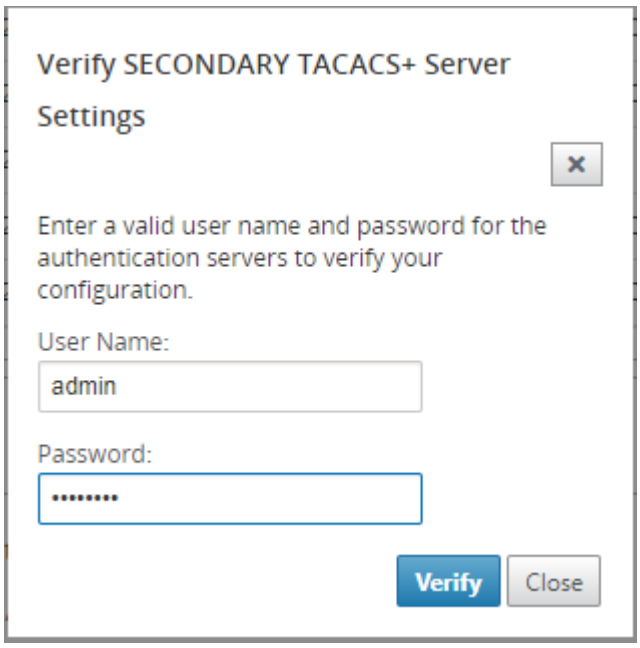
   El valor de tiempo de espera debe ser menor o igual a 60 segundos.
4. En el campo **Tipo de autenticación**, seleccione el método de cifrado que se utilizará para enviar el nombre de usuario y la contraseña al servidor TACACS+.
5. En el campo **Clave del servidor**, escriba una clave secreta para usarla cuando se conecte a los servidores TACACS+.
6. En los campos **Confirmar clave del servidor**, vuelva a introducir la clave secreta.

   > **Nota**
   >
   > Los valores de **Tiempo de espera**, **Tipo de autenticación** y **Clave de servidor** se aplican a todos los servidores configurados.

7. Haga clic en el icono más (+) situado junto a **Servidores** para agregar un servidor TACACS+.
8. En el campo **Dirección IP**, introduzca la dirección IP del host para el servidor TACACS+.
9. En el campo **Puerto**, introduzca el número de puerto para el servidor TACACS+. El número de puerto predeterminado es 49



10. Haga clic en **Aplicar**.
11. Haga clic en **Verificar** para verificar la conexión con el servidor RADIUS. Aparece el cuadro de diálogo **Verificar configuración del servidor TACACS+**.



12. Introduzca un nombre de usuario y una contraseña válidos para los servidores de autenticación y haga clic en**Verificar**.

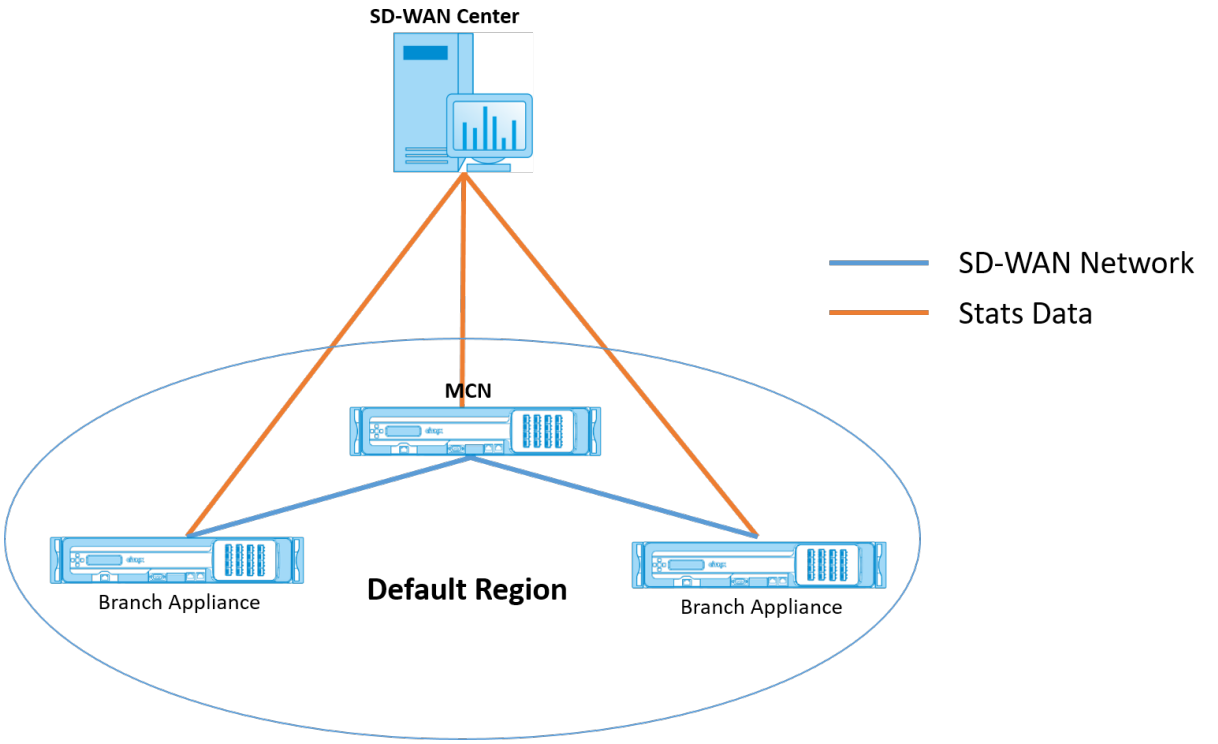
    Para configurar más servidores, repita los pasos 7 a 12.

Implementación de red en una región

April 13, 2021

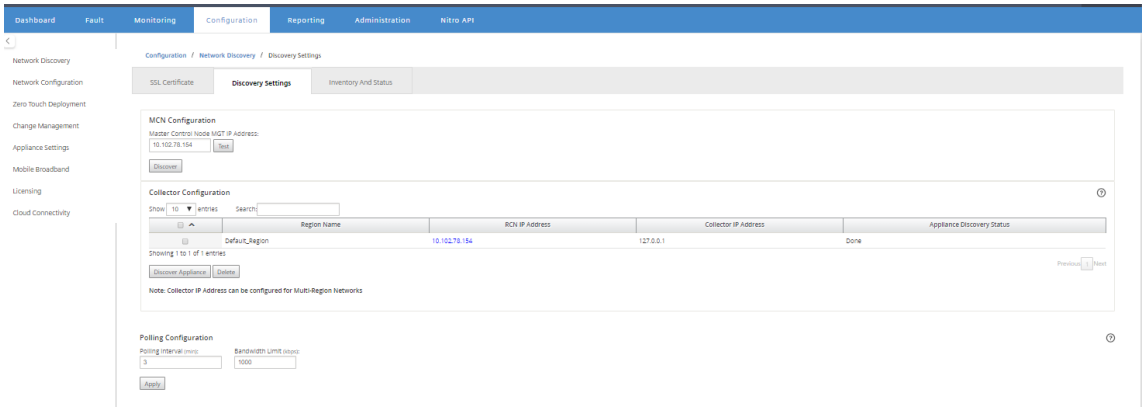
Si su organización tiene una red pequeña que abarca un único límite administrativo (o geográfico), puede usar Citrix SD-WAN Center en el modo predeterminado (con una única "región predeterminada"). Una región puede admitir un máximo de 550 sitios.

Una red de región única tiene un nodo de control maestro (MCN) para el control centralizado y Citrix SD-WAN Center para la administración centralizada. La región asociada y controlada por el MCN se denomina región predeterminada. Citrix SD-WAN Center sondea el MCN y todos los dispositivos de sucursal de la región predeterminada.



Para implementar Citrix SD-WAN Center para una sola región:

1. Descargue el software Citrix SD-WAN Center. Para obtener más información, consulte Requisitos del sistema e instalación.
2. Instale Citrix SD-WAN Center en Servidor ESXi, XenServer, Hyper-V o Azure.
3. Configuración de los ajustes de la interfaz de administración. Para obtener más información, consulte Configurar los parámetros de la interfaz de administración.
4. Genere, descargue e instale el Certificado SSL SD-WAN MCN en SD-WAN Center. Para obtener más información, consulte Instalar el certificado SSL de Citrix SD-WAN.
5. Genere, descargue e instale el certificado SSL de SD-WAN Center en el dispositivo MCN. Para obtener más información, consulte Instalar el certificado SSL de Citrix SD-WAN Center.
6. En la GUI de Citrix SD-WAN Center, vaya a **Configuración** > **Detección de redes** > **Configuración de detección.**
7. En el campo **Dirección IP MGT del nodo de controlador principal, introduzca la dirección** IP de MCN y haga clic en **Probar**. Esto establece una conexión entre el MCN y Citrix SD-WAN Center.



8. Haga clic en **Detectar**. Si ya ha descubierto un MCN, esta opción cambia a **Redetección**.

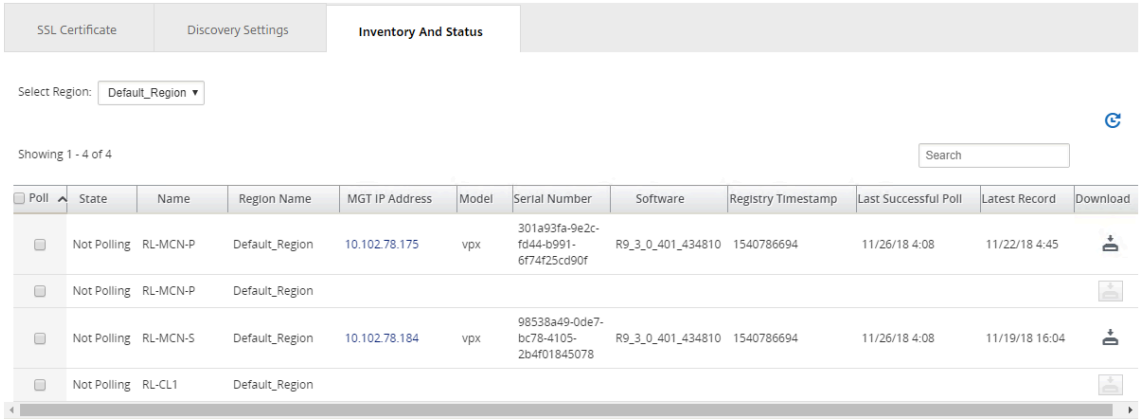
   > **Nota**
   >
   > El MCN debe estar activo y el servicio SD-WAN debe estar habilitado. Para obtener más información, consulte Activación del servicio SD-WAN.

9. Una vez finalizada la operación de detección, haga clic en la ficha **Inventario y estado**.

   La tabla **Inventario y Estado** muestra la información de estado de todos los dispositivos Citrix SD-WAN detectados.

10. Active la casilla **de verificación Encuesta** en la esquina superior izquierda del encabezado de la tabla.

    Esto activa la casilla de verificación **Sondeo** para cada dispositivo que se muestra en la tabla. Para excluir un dispositivo de la lista de sondeo, desactive su casilla de verificación.



11. Haga clic en **Aplicar**.

    > **Sugerencia**
    >
    > Puede aumentar el tamaño de almacenamiento de Citrix SD-WAN Center creando un data store en su máquina virtual y cambiando el data store. Para obtener más información,

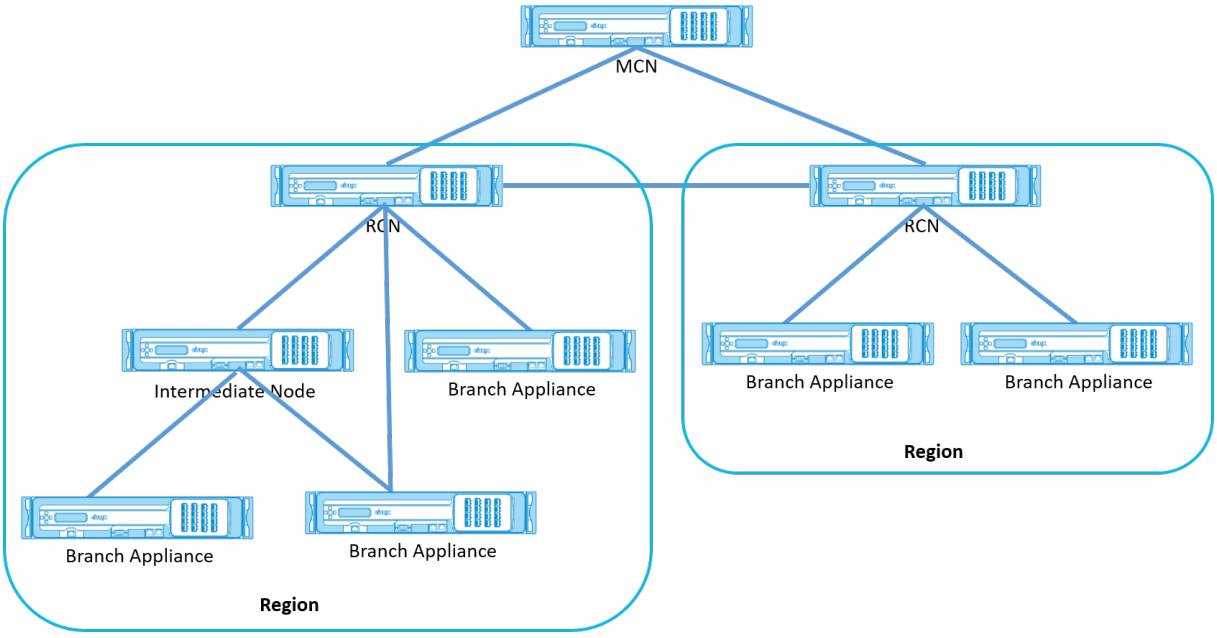
> consulte Cambiar el almacenamiento activo al nuevo almacenamiento de datos.

Implementación de red en varias regiones

April 13, 2021

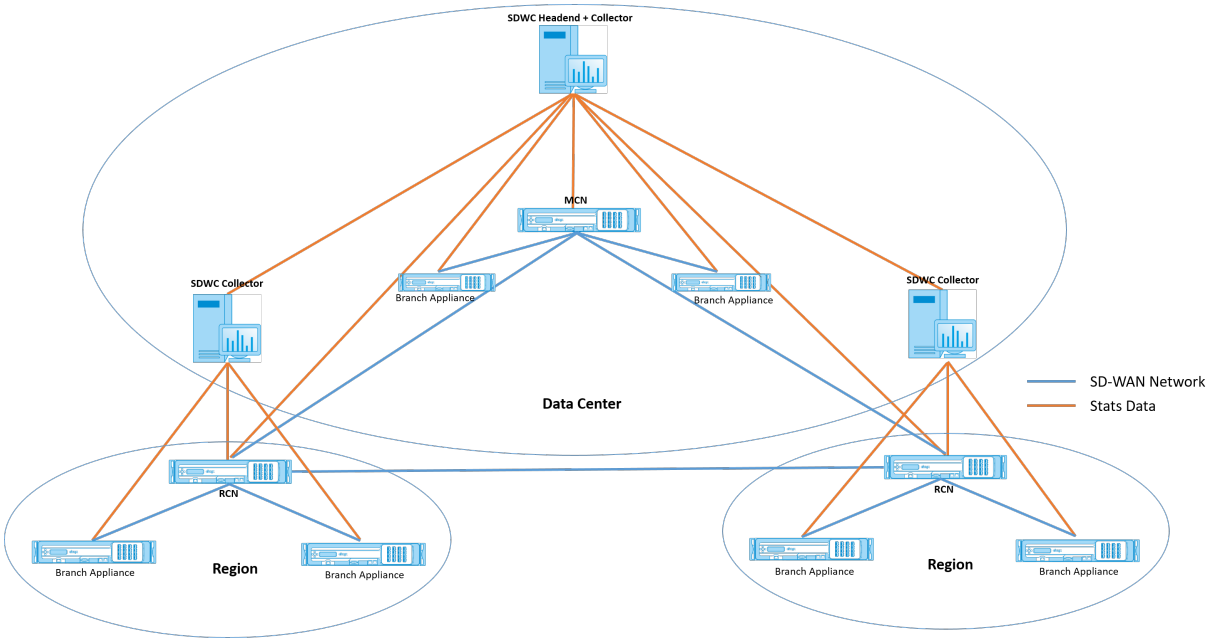
Si su organización tiene una red grande que abarca varios límites administrativos (o geográficos), puede utilizar Citrix SD-WAN Center en modo multirregión, con cada región admite un máximo de 550 sitios.

La red multiregión admite una arquitectura jerárquica con un nodo de control maestro (MCN) que controla varios nodos de control regionales (RCNs). Cada RCN, a su vez, controla varios sitios cliente. El MCN también se puede utilizar opcionalmente para controlar algunos sitios cliente directamente como parte de la "región predeterminada". Esta arquitectura jerárquica y distribuida permite una mayor escala y una delegación efectiva de la administración regional.



El Citrix SD-WAN Center sondea el MCN, los RCNs y todos los dispositivos de sucursal asociados.

La arquitectura multiregión Citrix SD-WAN Center requiere la adición de un recopilador por región para recopilar y almacenar datos y estadísticas a nivel de región. Esta arquitectura distribuida permite una mayor escala en varias regiones, al tiempo que conserva la vista de "panel único de cristal"para administrar toda la red.



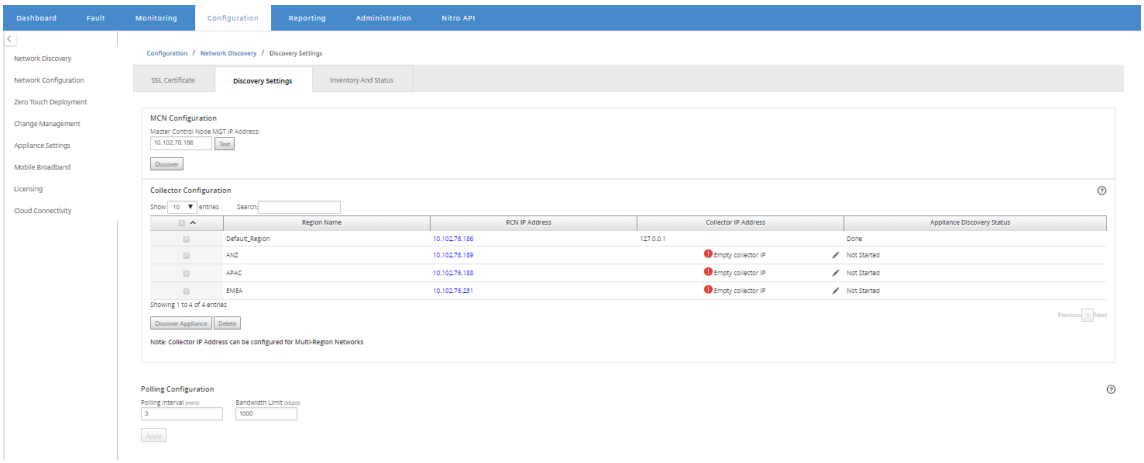
> **Nota**
>
> Para una implementación multiregión, las estadísticas de región predeterminadas incluyen estadísticas de todos los sitios administrados por el MCN y el RCN. Sin embargo, los datos de RCN no se almacenan en el recopilador SD-WAN Center. El colector SD-WAN Center obtiene los datos del sitio RCN de los respectivos colectores regionales.

Para implementar Citrix SD-WAN Center para varias regiones:

1. Descargue el software Citrix SD-WAN Center. Para obtener más información, consulte Requisitos del sistema e instalación.
2. Instale Citrix SD-WAN Center en Servidor ESXi, XenServer, Hyper-V o Azure.
3. Configuración de los ajustes de la interfaz de administración. Para obtener más información, consulte Configurar los parámetros de la interfaz de administración.
4. Genere, descargue e instale el Certificado SSL SD-WAN MCN en SD-WAN Center. Para obtener más información, consulte Instalar el certificado SSL de Citrix SD-WAN.
5. Genere, descargue e instale el certificado SSL de SD-WAN Center en el dispositivo MCN. Para obtener más información, consulte Instalar el certificado SSL de Citrix SD-WAN Center.
6. En la GUI de Citrix SD-WAN Center, vaya a **Configuración** > **Detección de redes** > **Configuración de detección.**
7. En el campo **Dirección IP MGT del nodo de controlador principal, introduzca la dirección** IP de MCN y haga clic en **Probar**. Esto establece una conexión entre el MCN y Citrix SD-WAN Center.

8. Haga clic en **Detectar**. En la sección **Configuración del recopilador** aparece una lista de todos los RCNs conectados al MCN. Para descubrir los sitios de región no predeterminados, debe tener un RCN activo con rutas activas a MCN.

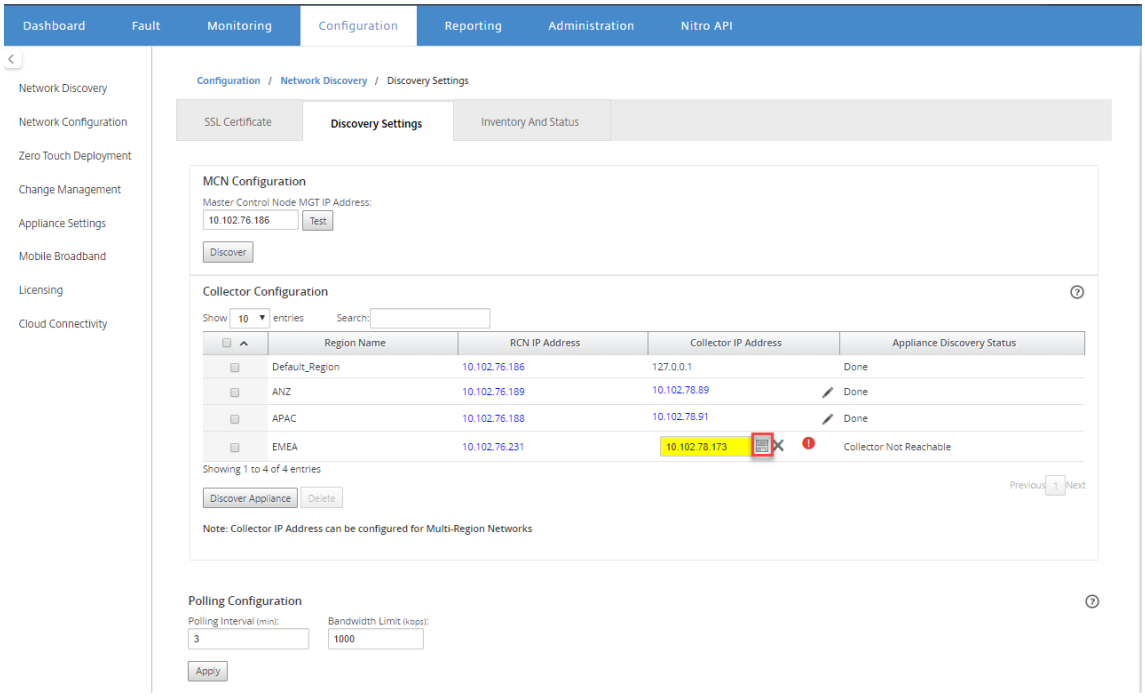
   > **Nota**
   >
   > Citrix SD-WAN Center actúa como un selector de la región predeterminada.



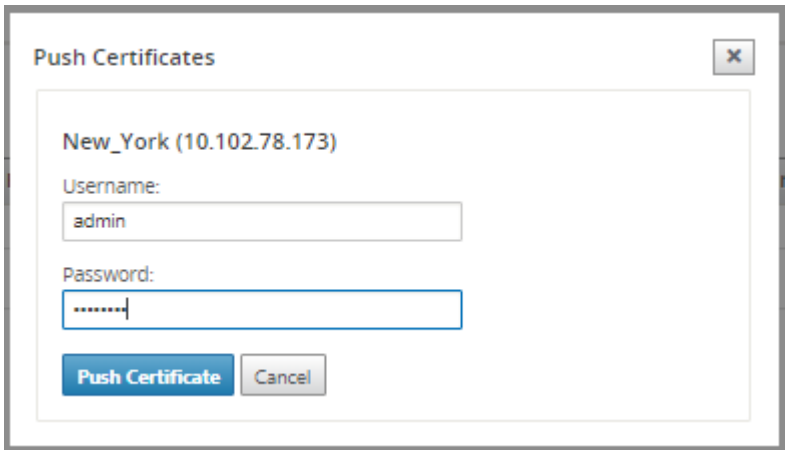
9. Haga clic en el icono de edición y, en el campo **IP del recopilador**, escriba la dirección IP del Citrix SD-WAN Center que quiere configurar como recopilador para una región.

   > **Nota**
   >
   > Para configurar un recopilador, instale una máquina virtual Citrix SD-WAN Center y configure la dirección IP de administración. La dirección IP de administración de ese Citrix SD-WAN Center es la dirección IP del recopilador.

10. Haga clic en el icono Guardar para guardar la dirección IP del recopilador y presione el par Certificate-Key en el RCN.

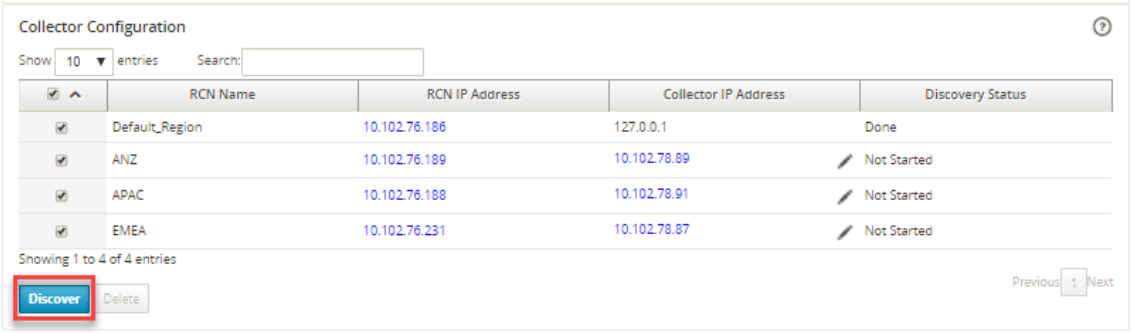


11. Introduzca las credenciales del RCN y haga clic en **Certificado Push**.

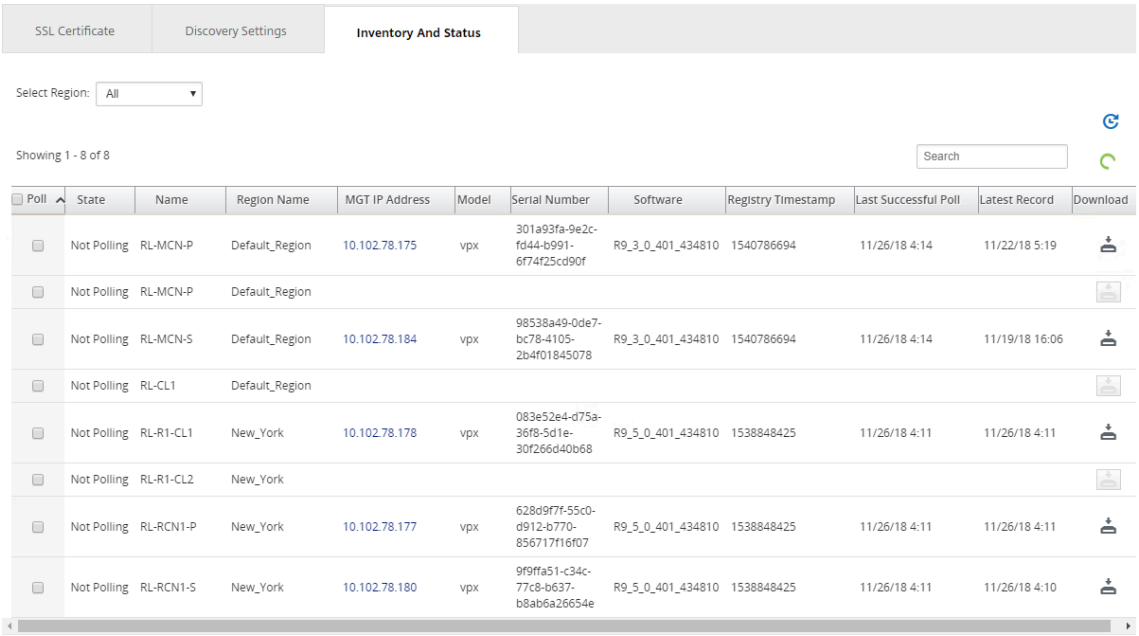


12. Del mismo modo, configure la dirección IP del recopilador para todos los RCNs.

> **Nota**
>
> Los dispositivos se descubren automáticamente cada 30 minutos. Si se agregan nuevos RCNs a la red y se realiza una administración de cambios, puede seleccionar el dispositivo y hacer clic en **Discover Appliance** para descubrir el dispositivo inmediatamente.



Después de que el **estado de detección** cambie a **Listo**, puede ver los sitios detectados en la página **Inventario y estado**.



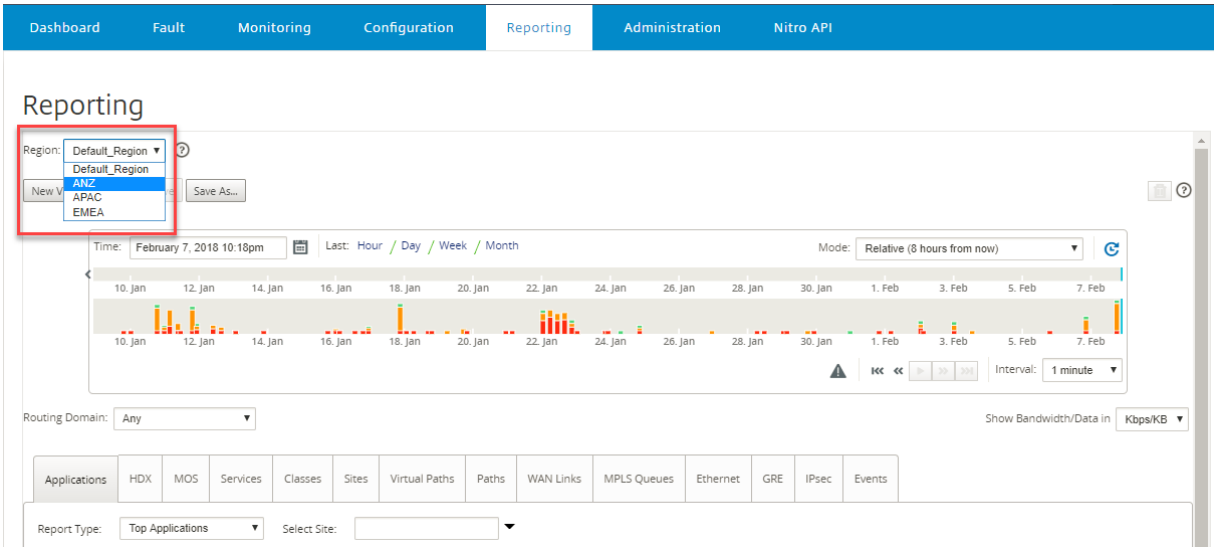
> **Sugerencia**
>
> Puede filtrar los sitios en función del nombre de la región. En el campo **Seleccionar región**, seleccione la región.

13. En la página **Inventario y estado**, seleccione los sitios que quiere iniciar la encuesta y haga clic en **Aplicar**.

> **Sugerencia**
>
> Puede aumentar el tamaño de almacenamiento del recopilador creando un data store en su máquina virtual. Para obtener más información, consulte Cambiar el almacenamiento activo al nuevo almacenamiento de datos.

Puede seleccionar regiones específicas para ver los informes de eventos y estadísticos.

Los datos de eventos e informes estadísticos se obtienen del recopilador de la región respectiva.



Configuración

April 13, 2021

Los pocos pasos iniciales para configurar Citrix SD-WAN Center son comunes tanto para la red de una región como para la red multiregión. A continuación se muestra una lista de los procedimientos de configuración comunes:

- Configurar los parámetros de la interfaz de administración
- Instale los certificados de Citrix SD-WAN Center.
- Cambiar el almacenamiento activo a un nuevo almacenamiento de datos.

Configurar los parámetros de la interfaz de administración

April 9, 2021

Puede utilizar la interfaz web de Citrix SD-WAN Center para configurar los parámetros de la interfaz de administración.

La configuración de la interfaz de administración incluye lo siguiente:

- Dirección IP de administración del centro de Citrix SD-WAN
- Dirección IP de la puerta de enlace
- Máscara de subred
- DNS principal

- DNS secundario

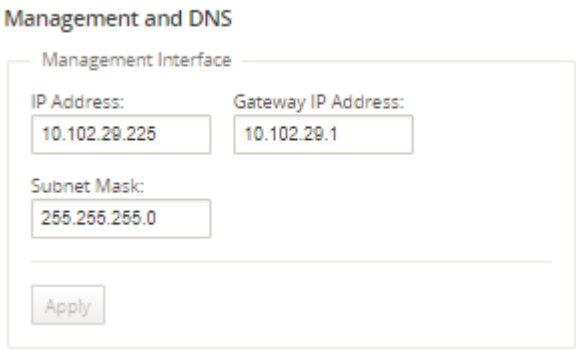
Para configurar las opciones de la interfaz de administración:

1. En la interfaz web de Citrix SD-WAN Center, seleccione la ficha **Administración**.

   De forma predeterminada, aparece la página **Configuración de usuario/autenticación**.
2. En el árbol de navegación, seleccione **Configuración global**.
3. Configure las opciones de administración y DNS.

   En la sección **Administración y DNS**, agregue la información necesaria a los siguientes campos:

   - **Dirección IP**: Introduzca la dirección IP para Citirx SD-WAN Center.
   - **Dirección IP de puerta**de enlace: introduzca la dirección IP de puerta de enlace que la VM Citrix SD-WAN Center utilizará para comunicarse con redes externas.
   - **Máscara de subred**: Introduzca la máscara de subred para definir la red en la que reside la máquina virtual Citrix SD-WAN Center.



4. Haga clic en **Aplicar**.

> **Nota**
>
> La conectividad con Citrix SD-WAN Center finalizará cuando se apliquen los cambios.

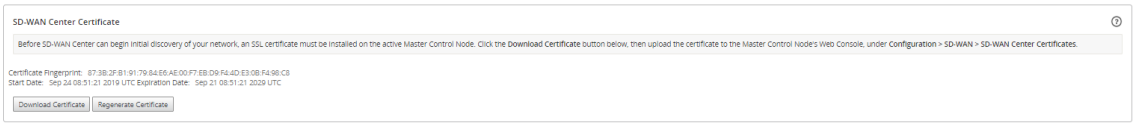
Instalar el certificado SSL de SD-WAN Center

April 9, 2021

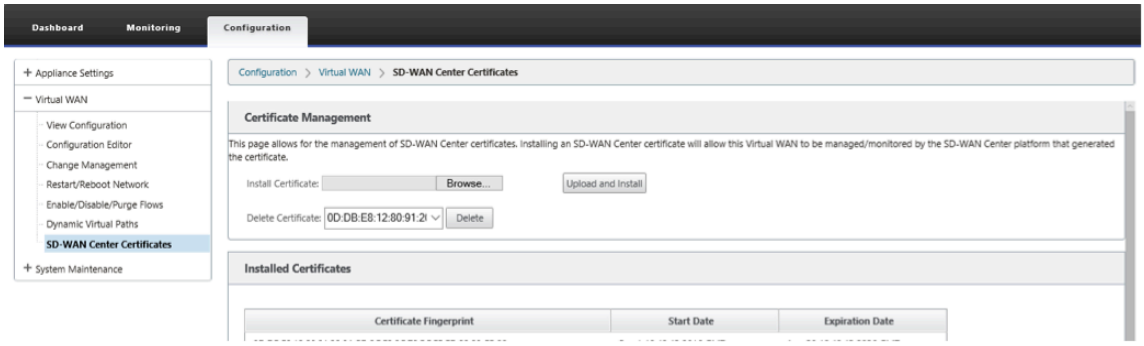
Para establecer una conexión entre Citrix SD-WAN Center y el nodo de control maestro (MCN) de Citrix SD-WAN, descargue el certificado SSL del SD-WAN Center e instálelo en el MCN.

Para generar e instalar el certificado Citrix SD-WAN Center:

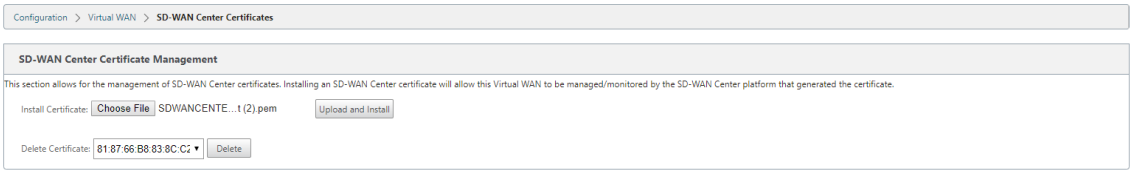
1. En la interfaz web de Citrix SD-WAN Center, vaya a **Configuración** > **Detección de redes** > **Certificado SSL > CertificadoSD-WAN Center Certificate**.
2. Haga clic en **Regenerar certificado** para generar un nuevo certificado SSL para establecer la comunicación con el MCN.



3. Haga clic en **Descargar certificado**. Desplácese hasta la ubicación deseada y guarde el certificado.
4. En la interfaz web de MCN de Citrix SD-WAN, vaya a **Configuración** > **Virtual WAN** > **SD-WAN Center Certificates** > **SD-WAN Center Certificate Management**.



5. Haga clic en **Elegir archivo**, busque y seleccione el certificado SSL de SD-WAN Center descargado.



6. Haga clic en **Cargar e instalar**, carga el certificado SSL de SD-WAN Center al MCN y muestra un mensaje de éxito cuando se complete la instalación.

Instalar el certificado SSL de Citrix SD-WAN

April 13, 2021

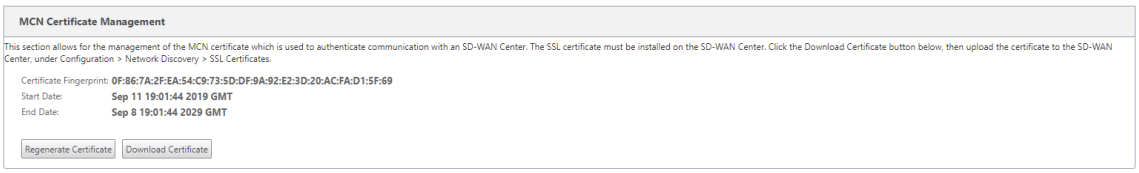
Para establecer la conexión entre Citrix SD-WAN MCN y Citrix SD-WAN Center, descargue el certificado SSL del dispositivo MCN SD-WAN e instálelo en SD-WAN Center.

Puede volver a generar el certificado del dispositivo en el MCN que reemplaza al certificado predefinido y, a continuación, instalarlo en SD-WAN Center.

La instalación del certificado del dispositivo en el Centro de SD-WAN es obligatoria para las nuevas implementaciones y para que la comunicación SSL funcione. MCN genera un certificado de red y distribuye el certificado con una clave privada a través del administrador de certificados a todos los nodos. Cada sucursal utiliza los certificados para autenticar SD-WAN Center.

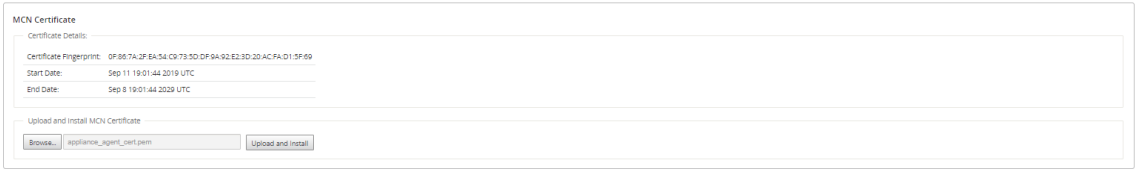
Para generar e instalar el certificado de SD-WAN:

1. En el dispositivo SD-WAN de MCN, vaya a **Configuration** > **Virtual WAN** > **SD-WAN Center Certificates** > **MCN Certificate Management**.
2. Haga clic en **Regenerar certificado** para generar un nuevo certificado SSL para establecer la comunicación con SD-WAN Center.

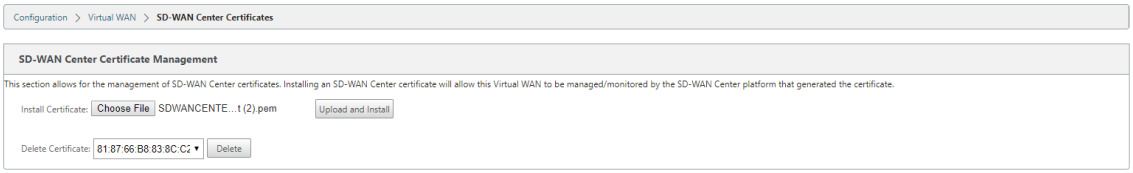


> **Nota**
>
> :
>
> Al volver a generar el certificado SSL, el dispositivo SD-WAN utiliza el nuevo certificado inmediatamente para comunicarse con el Centro SD-WAN descubierto. Sin embargo, la comunicación con los dispositivos no se establece hasta que descargue e instale el certificado recién generado en SD-WAN Center.

3. Haga clic en **Descargar certificado**. Desplácese hasta la ubicación deseada y guarde el certificado.
4. En la interfaz web de Citrix SD-WAN Center, vaya a **Configuración** > **Certificado SSL** > **Certificado MCN**.



5. Haga clic en **Examinar** y seleccione el certificado SSL MCN descargado.



6. Haga clic en **Cargar e instalar**, cargará el certificado SSL MCN al Centro SD-WAN.

Cambiar el almacenamiento activo al nuevo almacenamiento de datos

April 13, 2021

En Citrix SD-WAN Center, puede cambiar el almacenamiento activo al almacén de datos que creó en el servidor virtual. Esto le permite almacenar más datos estadísticos obtenidos sondeando todos los dispositivos Citrix SD-WAN en la WAN. Para obtener información sobre cómo crear un almacén de datos en el servidor ESXi, consulte Agregar y configurar el almacén de datos en ESXi Server. Para obtener información sobre cómo crear un almacén de datos en XenServer, consulte Agregar y configurar el almacenamiento de datos en XenServer.

Para especificar el almacenamiento activo para la máquina virtual Citrix SD-WAN Center:

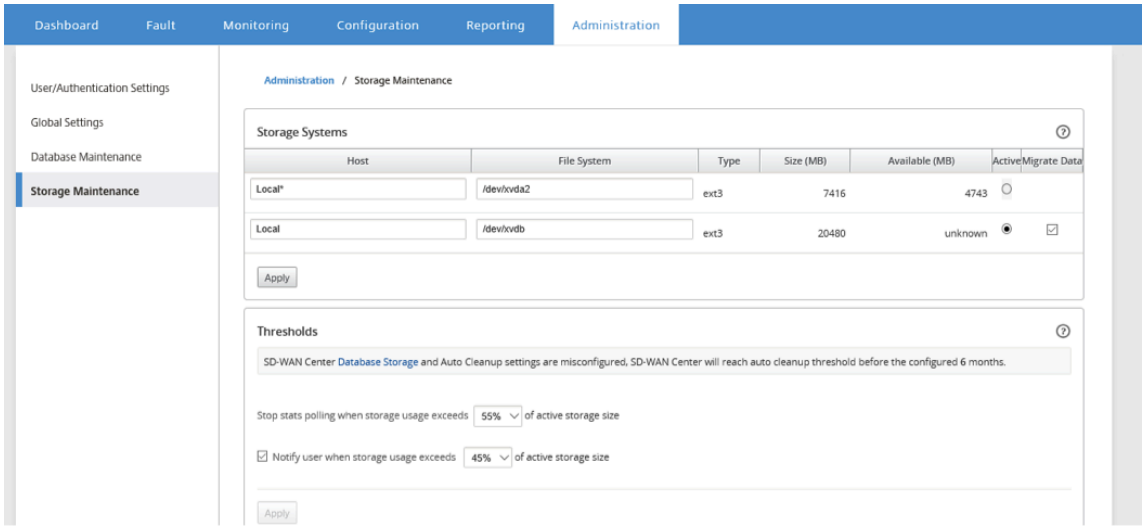
1. Inicie sesión en Citrix SD-WAN Center VM.

   Las credenciales de inicio de sesión predeterminadas para Citrix SD-WAN Center son las siguientes:

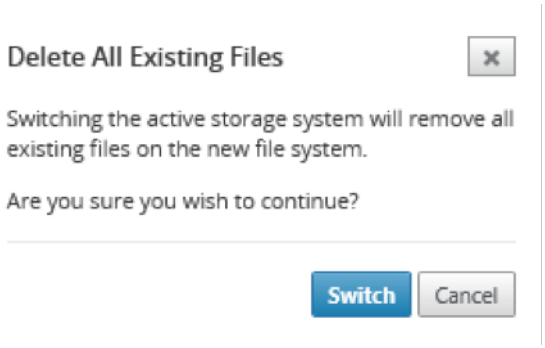
   Inicio de sesión: admin

   Contraseña: contraseña

2. Haga clic en la ficha **Administración** y, a continuación, haga clic en **Mantenimiento de almacenamiento**.



3. En la columna **Activo** de la tabla Sistemas de almacenamiento, seleccione el almacenamiento que ha creado.
4. Seleccione **Migrar datos** y haga clic en **Aplicar**.
5. Aparecerá el mensaje **Eliminar todos los archivos existentes**, haga clic en **Cambiar**.



Esto coloca Citrix SD-WAN Center en **modo de mantenimiento** y muestra una barra de progreso en el área de la página principal.

6. Cuando finalice la activación, haga clic en **Continuar**.

   Esto descarta la barra de progreso y vuelve a la página principal **Mantenimiento de almacenamiento**.

Implementación del dispositivo Citrix SD-WAN

April 13, 2021

Puede utilizar Citrix SD-WAN Center para crear el archivo de configuración del dispositivo o configuración del dispositivo y utilizar el asistente de administración de cambios para enviar la configuración a los dispositivos de la red. Para obtener más información, consulte Configurar dispositivos Citrix SD-WAN.

Puede configurar Citrix SD-WAN Center para que actúe como el servidor central de licencias y proporcione servicios de licencias a todos los nodos de la red. Esto elimina la necesidad de instalar licencias en nodos individuales localmente. Para obtener más información, consulte Citrix SD-WAN Center como servidor de licencias.

Puede utilizar Citrix SD-WAN Center para optimizar el proceso de implementación de los dispositivos de SD-WAN en sucursales mediante la función Zero Touch Deployment. Para obtener más información, consulte Implementación de Zero Touch.

Configurar dispositivos Citrix SD-WAN

April 13, 2021

Utilice el Editor de configuración para modificar los valores de configuración y exportar el paquete de configuración al MCN. Para obtener más información, consulte Editor de configuración.

Puede utilizar el asistente de administración de cambios del dispositivo MCN a través de Citrix SD-WAN Center. Para obtener más información, consulte Asistente para administración de cambios.

Puede configurar la configuración del dispositivo en Citrix SD-WAN Center y exportarlo a un conjunto de dispositivos Citrix SD-WAN administrados en su red SD-WAN.Para obtener más información, consulte Configuración del dispositivo.

Editor de configuración

April 13, 2021

El Editor de configuración está disponible como un componente de la interfaz web Citrix SD-WAN Center y en la Interfaz Web de administración de Citrix SD-WAN que se ejecuta en el nodo de control maestro (MCN) de la red SD-WAN.

> **Nota**
>
> No puede enviar configuraciones a los dispositivos detectados directamente desde Citrix SD-WAN Center. Puede utilizar el Editor de configuración para modificar los valores de configuración y crear un paquete de configuración. Una vez creado el paquete de configuración, puede exportarlo al MCN e instalarlo. Los cambios se reflejan entonces en el MCN.
>
> Tiene que iniciar sesión con derechos administrativos en el dispositivo Citrix SD-WAN Center y el MCN, modificar las configuraciones en SD-WAN Center de Citrix y exportar e instalar las configuraciones en el MCN.

Para obtener instrucciones detalladas sobre el uso del Editor de configuración para configurar Citrix SD-WAN, consulteCitrix SD-WAN 10.1la documentación.

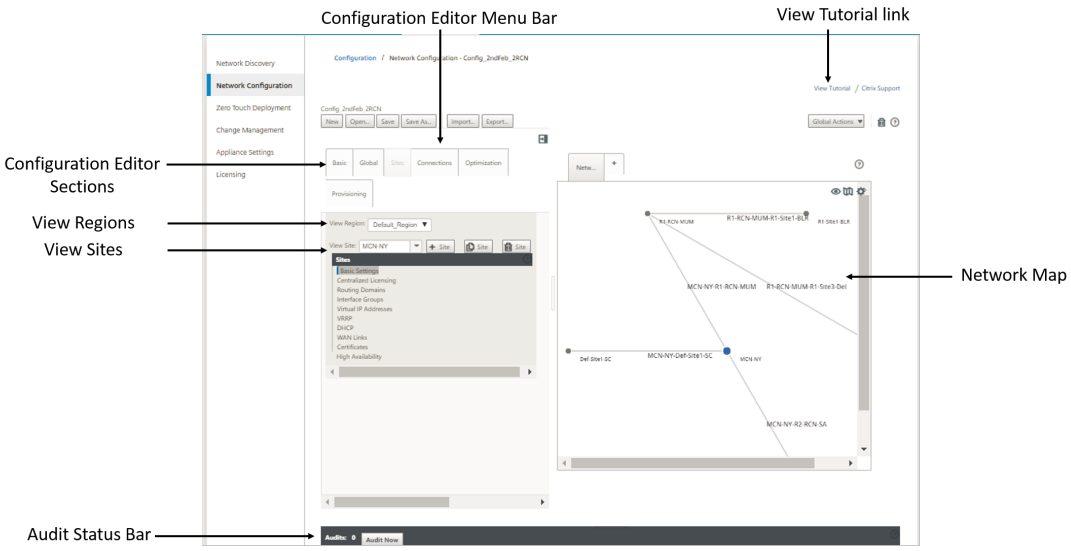
El Editor de configuración le permite hacer lo siguiente:

- Agregue y configure sitios y conexiones de Citrix SD-WAN Appliance.
- Aprovisione el dispositivo Citrix SD-WAN.
- Cree y defina la configuración de Citrix SD-WAN.
- Defina y visualice mapas de red de su sistema SD-WAN.

Para abrir el Editor de configuración:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Configuración**.
2. Haga clic en **Configuración de red**.

La siguiente ilustración describe los elementos básicos de navegación y página del **Editor de configuración**, así como la terminología utilizada en esta guía para identificarlos.



La pantalla principal del Editor de configuración tiene los siguientes elementos de navegación:

- **Barra de menús del Editor de Configuración**: contiene los botones de actividad principales para las operaciones del Editor de configuración Además, en el extremo derecho de la barra de menús se encuentra el botón de enlace **Ver tutorial** para iniciar el tutorial del Editor de configuración. El tutorial le guiará a través de una serie de descripciones de burbujas para cada elemento de la visualización del Editor de configuración.
- **Secciones del Editor de configuración**: Cada ficha representa una sección de nivel superior. Hay seis secciones: **Básico**,**Global**, **Sitios**, **Conexiones**, **Optimización** y **Provisioning**. Haga clic en una ficha de sección para mostrar el árbol de configuración de esa sección.
- **Ver región**: para la implementación de varias regiones, muestra todas las regiones configuradas. Para el implementación de una sola región, la región predeterminada se muestra de forma predeterminada. Para ver los sitios de una región, seleccione una región en la lista desplegable.
- **Ver Sitios:**Muestra los nodos de sitio que se han agregado a la configuración y que están abiertos actualmente en el Editor de configuración. Para ver la configuración del sitio, seleccione un sitio de la lista desplegable.
- **Mapa de red:** proporciona una vista esquemática de la red SD-WAN.Pase el cursor del ratón sobre los sitios o la ruta para ver más detalles. Haga clic en los sitios para ver las opciones del informe.
- Barra de**estado de auditoría: barra**gris oscura situada en la parte inferior de la página Editor de Configuración, que abarca todo el ancho de la página Editor de Configuración. La barra de estado **Auditorías** solo está disponible cuando el **Editor de configuración** está abierto. Un icono de alerta de auditoría (punto rojo o delta de vara dorada) en el extremo izquierdo de la

barra de estado indica uno o más errores presentes en la configuración abierta actualmente. Haga clic en la barra de estado para mostrar una lista completa de todas las alertas de auditoría sin resolver para esa configuración.

Asistente para administración de cambios

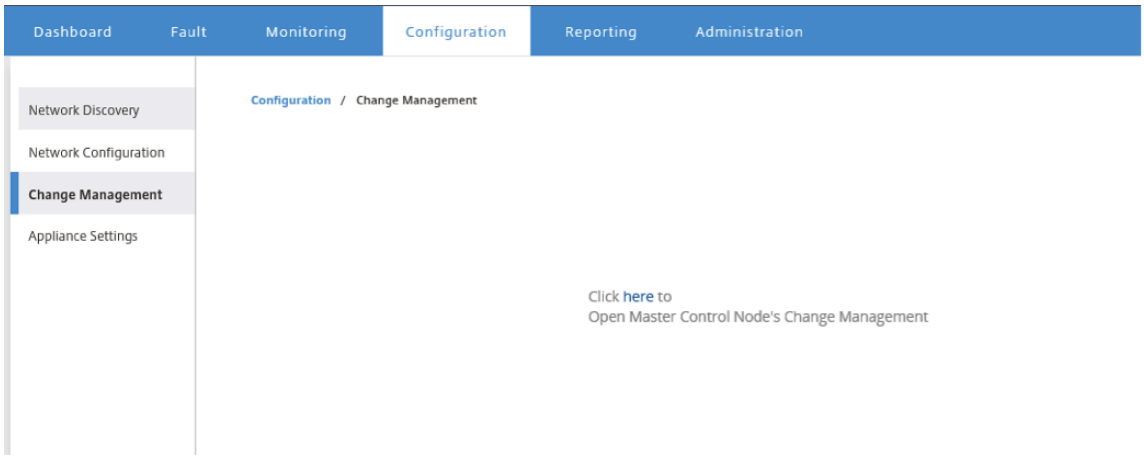
April 9, 2021

El asistente Administración de cambios le guía a través del proceso de carga, descarga, almacenamiento provisional y activación del software y la configuración de Citrix SD-WAN en el dispositivo Master Control Node (MCN) y los dispositivos cliente.

El asistente de administración de cambios es un componente de la interfaz web de administración de Citrix SD-WAN que se ejecuta en el MCN y no forma parte de Citrix SD-WAN Center. Sin embargo, puede utilizar Citrix SD-WAN Center para conectarse al MCN especificado y acceder al asistente de administración de cambios.

Para abrir el Asistente para administración de cambios:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Configuración**.
2. Haga clic en **Administración de cambios**.



3. En el mensaje **Haga clic aquí para abrir la administración de cambios del nodo principal de control**, haga clic en el vínculo **aquí**.

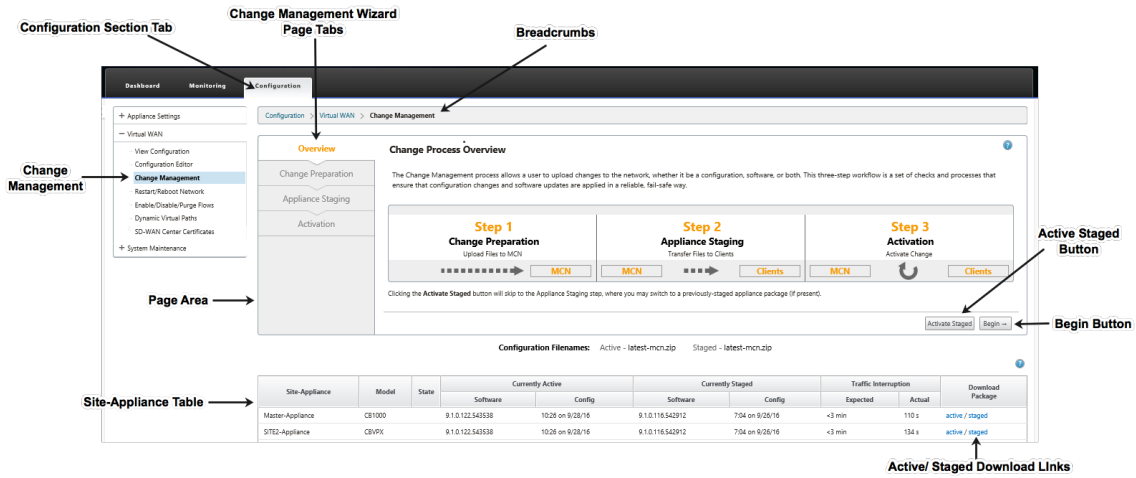
   Se iniciará sesión automáticamente en la GUI de MCN.

   > **Nota**

> No es necesario que inicie sesión en la GUI de MCN mediante las credenciales de MCN, la función de inicio de sesión automático permite Single Sign-On.

4. En la interfaz web de administración de MCN, haga clic en la ficha **Configuración**.
5. En el árbol de navegación (panel izquierdo), haga clic en **+** junto a la rama **Virtual WAN** para expandir esa rama.
6. Haga clic en **Administración de cambios**.

   Muestra la primera página del asistente de **administración de cambios**, la página **Visión General del Proceso de Cambios**, tal como se muestra en la ilustración siguiente.



7. Para iniciar el asistente, haga clic en **Iniciar**.

> **Nota**
>
> Para obtener instrucciones completas sobre el uso del asistente para cargar, organizar y activar el software y la configuración de SD-WAN en los dispositivos, consulte la Guía del usuario de SD-WAN 9.1.0.

El asistente **de administración de cambios** tiene los siguientes elementos de navegación:

- **Área de página**: muestra los formularios, tablas y botones de actividad de cada página del asistente de **administración de cambios** .
- **Fichas de página del asistente Administración de cambios**: En el lado izquierdo del área de página, en cada página del asistente, las fichas aparecen en el orden en que se producen los pasos correspondientes en el proceso del asistente. Cuando una ficha está activa, puede hacer clic en ella para volver a una página anterior del asistente. Una ficha activa muestra su nombre se muestra en una fuente azul. Una fuente gris indica una ficha inactiva. Las fichas están inactivas hasta que todas las dependencias (pasos anteriores) se han completado sin error.

- **Tabla Appliance-Site**: en la parte inferior del área de la página del asistente, esta tabla contiene información sobre cada sitio de dispositivo configurado y vínculos para descargar los paquetes de dispositivos activos o en etapas para ese sitio y modelo de dispositivo. Un paquete en este contexto es un paquete de archivos zip que contiene el paquete de software SD-WAN apropiado para ese modelo de dispositivo y el paquete de configuración especificado. La sección Nombres de archivos de configuración situada encima de la tabla muestra el nombre del paquete para los paquetes activos y en etapas actuales del dispositivo local.
- **Vínculos de descarga activo/por etapas**: en el campo **Descargar paquete** (columna de la derecha) de cada entrada de la tabla **Appliance-Site**, puede hacer clic en un vínculo de una entrada para descargar el paquete activo o por etapas del sitio de ese dispositivo.
- **Botón Iniciar**: Haga clic en Iniciar para **iniciar** el proceso del asistente **de Gestión de Cambios** y vaya a la página de separador **Preparación de Cambios** .
- **Botón Activar por etapas**: Si no se trata de una implementación inicial y quiere activar la configuración por etapas actualmente, tiene la opción de continuar directamente con el paso **Activación**. Haga clic en **Activar por etapas** para pasar directamente a la página **Activación** e iniciar la activación de la configuración en fase interactiva.

Configuración del dispositivo

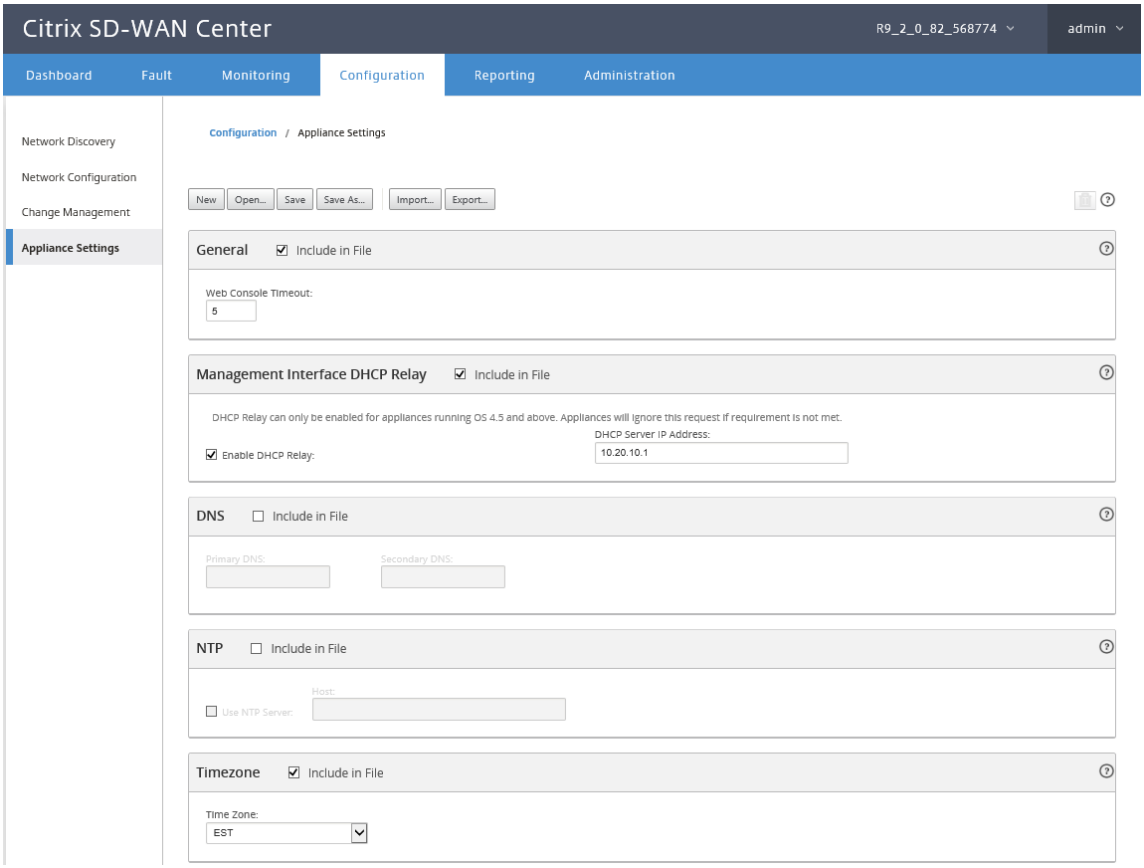
April 9, 2021

Puede configurar la configuración del dispositivo en Citrix SD-WAN Center y exportarlo a un conjunto de dispositivos Citrix SD-WAN administrados en su red SD-WAN.La página **Configuración del dispositivo** permite realizar las siguientes acciones:

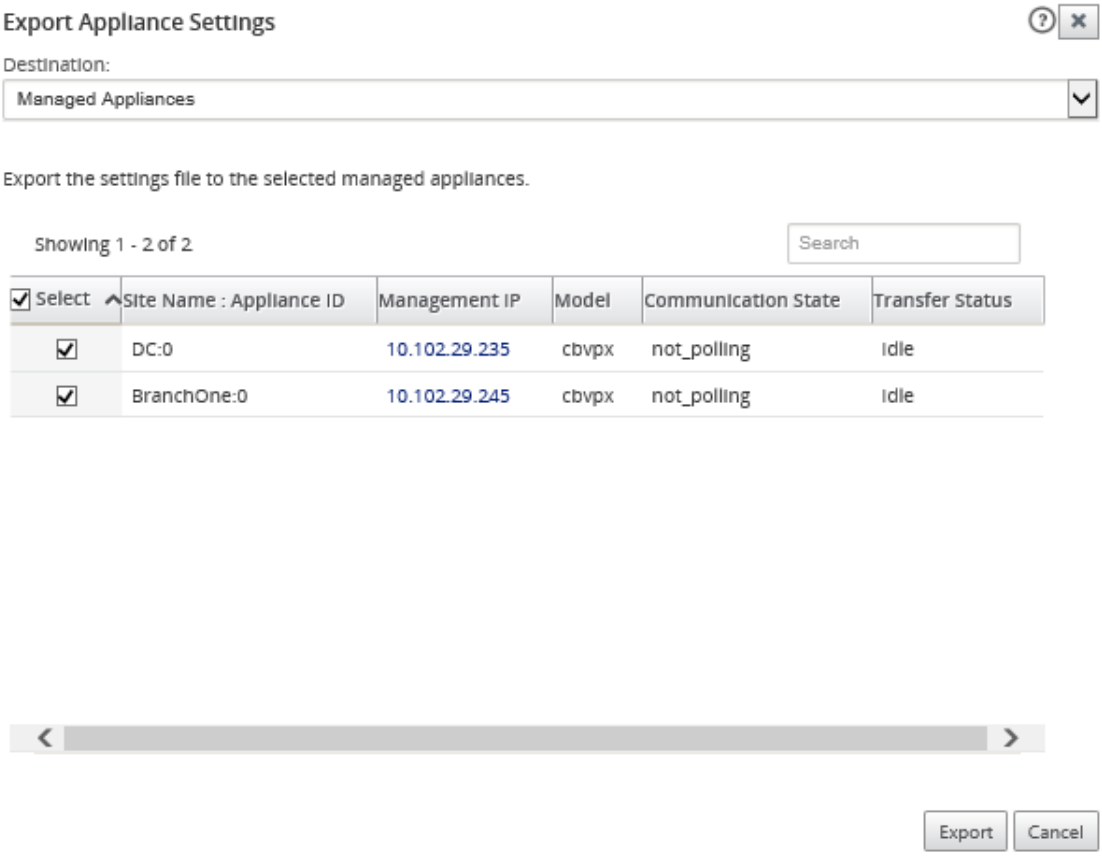
- Cree un archivo de configuración del dispositivo.
- Abra y modifique un archivo de configuración de dispositivo existente.
- Importe un archivo de configuración del dispositivo desde el equipo local.
- Descargue un archivo de configuración del dispositivo en el equipo local.
- Exporte un archivo de configuración de dispositivo a los dispositivos administrados.

Para crear un archivo de configuración del dispositivo y exportarlo a dispositivos administrados:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Configuración**.
2. Haga clic en **Configuración del dispositivo** y, a continuación, haga clic en **Nuevo**.



3. Seleccione **Incluir en archivo** para la configuración requerida y especifique los valores de parámetro para la configuración. Para obtener más información, consulte tabla de configuración del dispositivo.
4. Haga clic en **Exportar**. En el cuadro de diálogo **Guardar como**, escriba un nombre para el archivo de configuración del dispositivo y haga clic en **Guardar**. Aparecerá el cuadro de diálogo **Exportar configuración del equipo**.
5. En el campo **Destino**, seleccione **Dispositivos administrados** y seleccione los dispositivos a los que quiere exportar la configuración del dispositivo.



> **Nota**
>
> Para descargar la configuración del dispositivo en el equipo local, seleccione **Descarga de archivos** en el campo **Destino**.

6. Haga clic en **Exportar**.

Administración remota de sitios LTE

February 16, 2022

Citrix SD-WAN Center le permite ver y administrar de forma remota todos los sitios LTE de su red. Incluye dispositivos conectados a través de un módem LTE interno o un módem USB LTE externo.

Los dispositivos Citrix SD-WAN, como Citrix SD-WAN 210 SE LTE y 110 LTE Wi-Fi, tienen un módem LTE interno integrado. También puede conectar un módem USB 3G/4G externo en los siguientes dispositivos Citrix SD-WAN.

- Citrix SD-WAN 210 SE

- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wifi SE

CDC Ethernet, MBIM y NCM son los tres tipos de módems USB externos soportados. Puede configurar los parámetros de APN y habilitar/inhabilitar el módem a través de la nueva GUI de Citrix SD-WAN y Citrix SD-WAN Center. Las operaciones de banda ancha móvil no son compatibles con los módems USB CDC Ethernet.

Requisitos previos para módem LTE externo:

- Utilice los dongles USB LTE compatibles. Los modelos de hardware de dongle compatibles son Verizon USB730L y AT&T USB800.
- Asegúrese de que se inserta una tarjeta SIM en el dongle USB LTE. Los dongles CDC Ethernet LTE están preconfigurados con una dirección IP estática, esto interfiere con la configuración y causa un fallo de conexión o una conexión intermitente, si no se inserta la tarjeta SIM.
- Antes de insertar un dongle CDC Ethernet LTE en el dispositivo SD-WAN, conecte la memoria USB externa a una máquina Windows/Linux y asegúrese de que Internet funciona correctamente con la configuración adecuada de APN y Mobile Data Roaming. Asegúrese de que el modo de conexión del dongle USB cambia del valor predeterminado Manual a Auto.

> **Nota**
>
> - Los dispositivos Citrix SD-WAN solo admiten un dongle USB LTE a la vez. Si hay más de un dongle USB enchufado, desenchufe todos los dongles y enchufe solo un dongle.
> - Los dispositivos Citrix SD-WAN no admiten el nombre de usuario y la contraseña para módems USB. Asegúrese de que la función de nombre de usuario y contraseña esté inhabilitada en el módem durante la instalación.
> - Desconectar o reiniciar un dongle MBIM externo afecta a la sesión de datos interna del módem LTE. Este es un comportamiento esperado.
> - Cuando se conecta un módem LTE externo, el dispositivo SD-WAN tarda unos 3 minutos en reconocerlo.

Operaciones compatibles con módems internos y externos:

Operaciones	Módem interno	Módem externo - CDC Ethernet	Módem externo - MBIM y NCM
Preferencia de SIM	Sí - Para dispositivos compatibles con doble SIM	No	No
PIN SIM	Sí	No	No

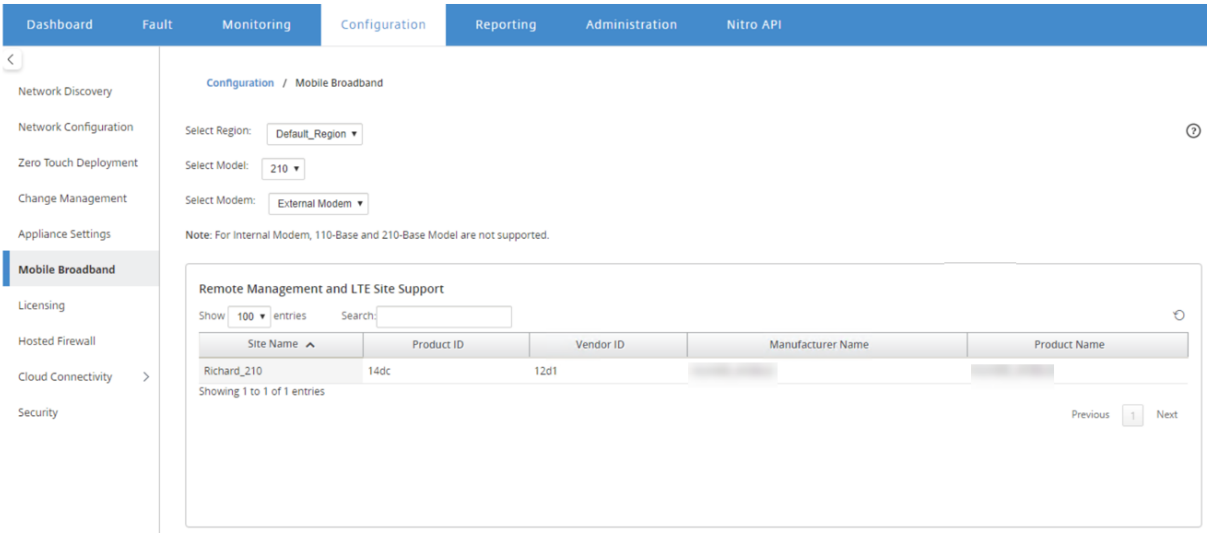
Operaciones	Módem interno	Módem externo - CDC Ethernet	Módem externo - MBIM y NCM
Configuración de APN	Sí	No	Sí
Configuración de la red	Sí	No	No
Itinerancia	Sí	No	No
Administrar firmware	Sí	No	No
Activar/desactivar módem	Sí	No	Sí
Reiniciar el módem	Sí	No	No
Actualizar SIM	Sí	No	No

Para administrar de forma remota los sitios LTE de la red, en la interfaz de usuario de SD-WAN Center, vaya a **Configuración > Banda ancha móvil**. Todos los dispositivos LTE, entre sitios, administrados por el Centro SD-WAN se enumeran aquí.

Para una implementación de varias regiones, puede seleccionar una región para la que quiere administrar los sitios LTE. La opción Default_Region está seleccionada de forma predeterminada.

También puede seleccionar el modelo de dispositivo LTE y el tipo de módem.

Para enumerar los dispositivos que utilizan un módem externo, vaya a **Configuración** > **Banda ancha móvil**. Seleccione **Módem externo** como tipo de módem.

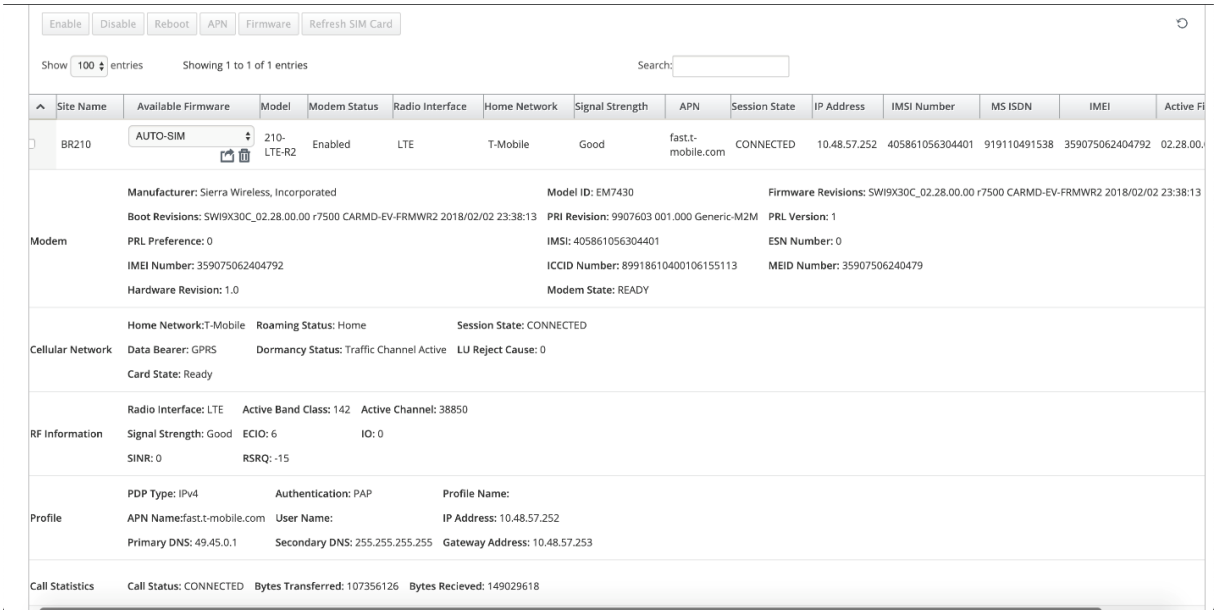


> **Nota**
>
> El PIN SIM y otras configuraciones de módem LTE no son compatibles actualmente con módems

> externos.

Para enumerar los dispositivos que utilizan un módem interno, vaya a **Configuración** > **Banda ancha móvil**. Seleccione **Módem interno** como tipo de módem.

> **Nota**
>
> Las operaciones LTE son diferentes para diferentes modelos LTE.



Puede seleccionar un único dispositivo o varios dispositivos para realizar la siguiente operación de módem LTE:

- **Habilitar**: Habilite el módem en los sitios seleccionados.
- **Inhabilitar**: Inhabilite el módem en los sitios seleccionados.
- **Reiniciar**: Reinicie el módem en los sitios seleccionados.
- **APN**: Configure la configuración de APN para los sitios seleccionados. Para obtener más información, consulte Configurar los parámetros de APN.
- **Firmware**: Esta opción es aplicable únicamente para el dispositivo 210 LTE. Busque y seleccione el firmware requerido. Puede optar por cargar solo o cargar y aplicar el archivo de firmware en los sitios seleccionados. En la lista de firmware disponible puede optar por aplicarlo o eliminarlo.

  > **Nota**
  >
  > En la implementación de varias regiones, las operaciones de firmware para sitios de región no predeterminados no se pueden realizar desde el encabezado SD-WAN Center. Puede realizar operaciones de firmware desde el Centro SD-WAN de Collector de la región especí-

> fica.

- **Actualizar tarjeta SIM**: Actualice la tarjeta SIM desactivándola y activándola de nuevo en los sitios seleccionados. Esta operación se realiza para detectar la nueva tarjeta SIM insertada en el módem 210 SE LTE.
- **Preferencia SIM**: esta opción solo se aplica al dispositivo 110 LTE. El dispositivo 110 LTE admite SIM dual y puede establecer las preferencias de SIM.
- **Modo de red**: puede seleccionar la red móvil en los dispositivos Citrix SD-WAN que admiten módem LTE interno. Las redes admitidas son 3G, 4G o ambas. Para dispositivos LTE 110, seleccione la SIM en la que desea aplicar los cambios.
- **Itinerancia**: La opción de roaming está habilitada de forma predeterminada en los dispositivos LTE, puede optar por inhabilitarla. Para dispositivos LTE 110, seleccione la SIM en la que desea aplicar los cambios.

También puede configurar la funcionalidad LTE en dispositivos LTE individuales. Para obtener más información, consulte Configurar la funcionalidad LTE en 210 SE LTE.

Para obtener información sobre la configuración de un dispositivo 110-LTE-WIFI, consulte Configurar la funcionalidad LTE en 110 LTE Wi-Fi.

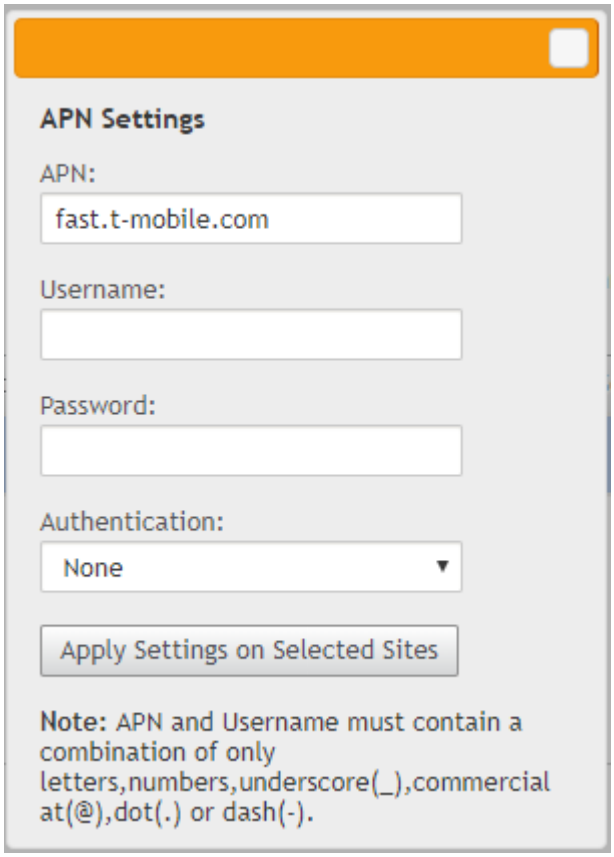
Configuración de APN

APN es el nombre de la configuración que lee el dispositivo para configurar una conexión a la puerta de enlace entre la red celular del operador y la Internet pública. Puede obtener la información de APN del operador y configurar de forma remota los ajustes de **APN** en uno o varios dispositivos LTE.

> **Nota**
>
> La configuración de APN varía de un transportista a otro.

Para configurar los valores de APN:

1. En la interfaz de usuario de SD-WAN Center, vaya a **Configuración > Banda ancha móvil**. Seleccione los sitios LTE para los que quiere configurar la configuración de APN y haga clic en **APN**.



2. Para un dispositivo 110 LTE, seleccione la SIM en la que se aplica la configuración de APN.
3. Introduzca el **nombre de APN**, el nombre de **usuario**, la **contraseña**y la **autenticación** proporcionados por el operador. Puede elegir entre los protocolos de autenticación PAP, CHAP y PAPCHAP. Si el transportista no ha proporcionado ningún tipo de autenticación, establezca en **Ninguno**.
4. Haga clic en **Aplicar configuración en sitios seleccionados**.

Citrix SD-WAN Center como servidor de licencias

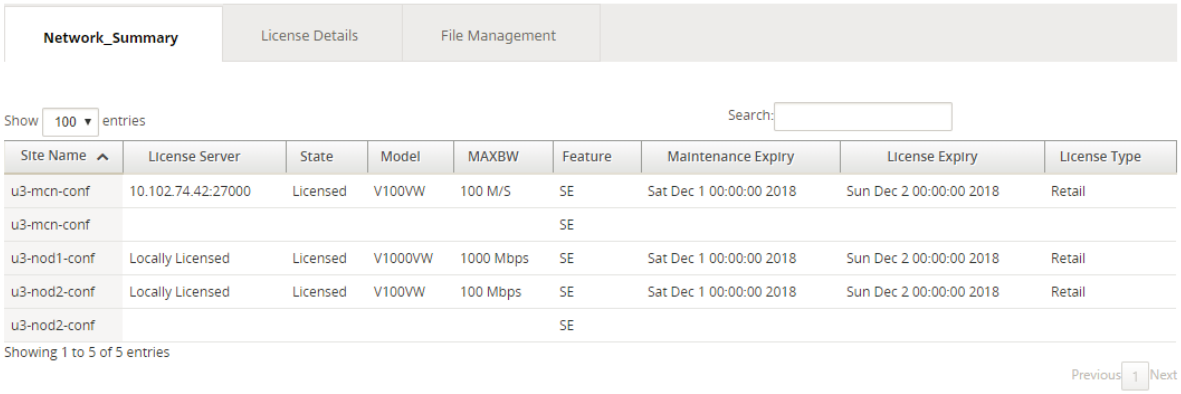
April 13, 2021

Puede adquirir las licencias para los dispositivos de su red, cargarlas e instalarlas en SD-WAN Center. Para utilizar SD-WAN Center como servidor de licencias remoto, configure la dirección IP de SD-WAN Center como servidor remoto para la administración centralizada de licencias. Para obtener más información, consulte Administración centralizada de licencias.

Después de insertar la configuración de red a los sitios a través del proceso de administración de cambios y una vez activada la configuración, los dispositivos de sucursal obtienen automáticamente las

licencias del SD-WAN Center.
Para que estas licencias se utilicen, se debe asignar las licencias al host del propio SD-WAN Center.

Para ver los detalles de licencia de todos los dispositivos detectados por SD-WAN Center, vaya a **Configuración** > **Licencias** > **Resumen de red.**



Se muestran los siguientes parámetros:

- **Nombre del sitio**: Nombre del sitio.
- **Servidor de licencias**: la dirección IP y el número de puerto del servidor de licencias. Si la licencia se instaló localmente en el dispositivo, se muestra como "Licencia local".
- **Estado**: El estado actual de la licencia del dispositivo, con licencia o sin licencia.
- **Modelo**: Modelo de dispositivo compatible con la licencia.
- **MAXBW**: El ancho de banda máximo permitido por la licencia.
- **Función**: La edición de Citrix SD-WAN que admite la licencia.
- **Caducidad de mantenimiento**: La fecha de caducidad de Citrix Subscription Advantage.

  > **Nota**
  >
  > Durante la actualización del software, si la fecha de compilación del software es superior a la fecha de caducidad del mantenimiento, la actualización del software no está permitida.

- **Caducidad de la licencia**: La fecha de caducidad de la licencia.
- **Tipo de licencia**: El tipo de licencia.

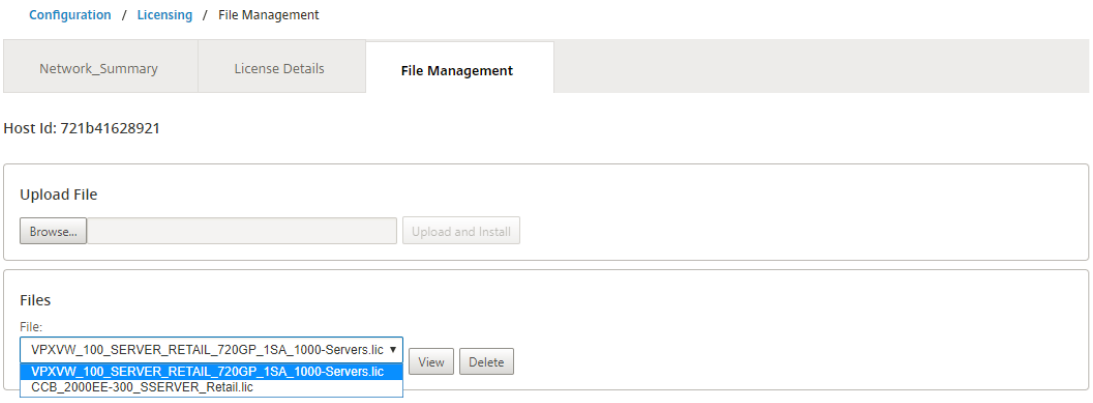
Para cargar e instalar archivos de licencia en SD-WAN Center:

1. Obtenga la licencia para los dispositivos Citrix SD-WAN y guárdela en su equipo local.

> **Nota**
>
> Para obtener instrucciones sobre cómo obtener una licencia de software Citrix SD-WAN, póngase en contacto con el servicio de atención al cliente de Citrix SD-WAN.

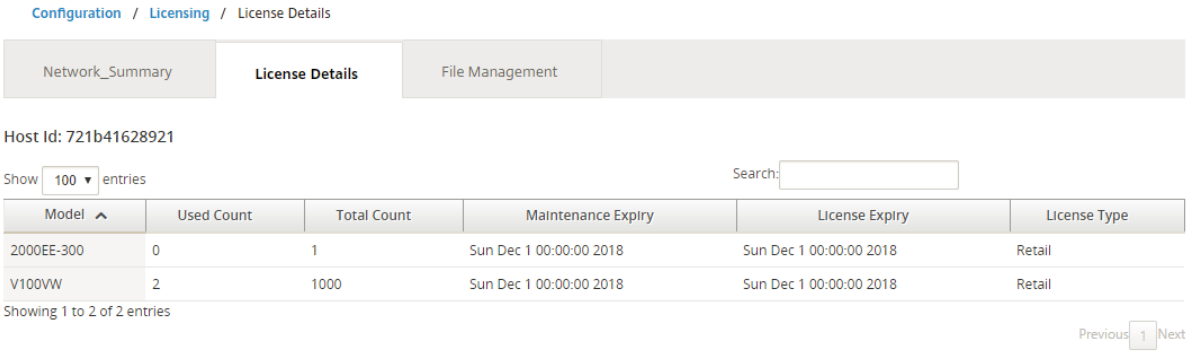
2. En la GUI de SD-WAN Center, vaya a **Licencias** > **Administración de archivos**.
3. En la sección **Cargar archivo**, haga clic en **Examinar**. Seleccione el archivo de licencia del equipo local y haga clic en **Cargar e instalar**.

   Los archivos de licencia instalados aparecen en el menú desplegable **Archivos**, puede elegir ver o eliminar los archivos de licencia.



> **Nota**
>
> El ID de host es el ID de host de SD-WAN Center, que se utiliza para generar los archivos de licencia. Los archivos de licencia generados con un identificador de host diferente no se pueden cargar e instalar en Citrix SD-WAN Center.

Puede ver los detalles de todos los archivos de licencia cargados e instalados en Citrix SD-WAN Center, de un vistazo, navegando a **Configuración** > **Licencias** > **Detalles de licencia.**



Se muestran los siguientes parámetros:

- **Modelo: modelo** de dispositivo compatible con la licencia.
- **Recuento usado:** el número de dispositivos en los que está instalada esta licencia.
- **Recuento total:** Número total de dispositivos en los que se puede instalar esta licencia.
- **Caducidad de mantenimiento**: La fecha de caducidad de Citrix Subscription Advantage.
- **Caducidad de la licencia**: La fecha de caducidad de la licencia.
- **Tipo de licencia**: El tipo de licencia.

Implementar Citrix SD-WAN en Azure desde Citrix SD-WAN Center

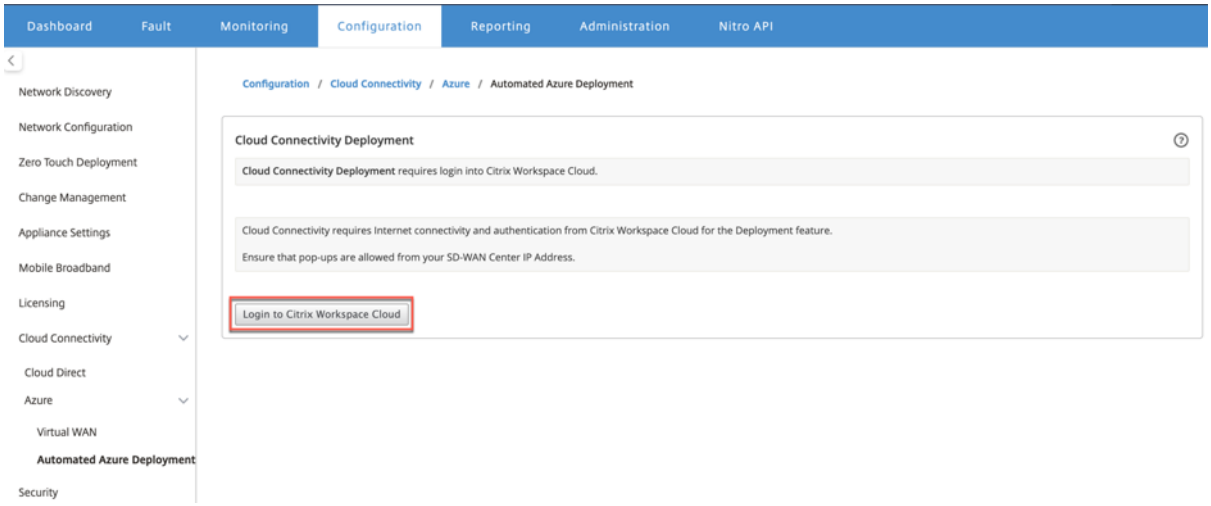
April 13, 2021

Citrix SD-WAN para Azure permite a las organizaciones tener una conexión segura directa desde cada sucursal a las aplicaciones alojadas en Azure, lo que elimina la necesidad de realizar backhaul tráfico vinculado a la nube a través de un centro de datos.

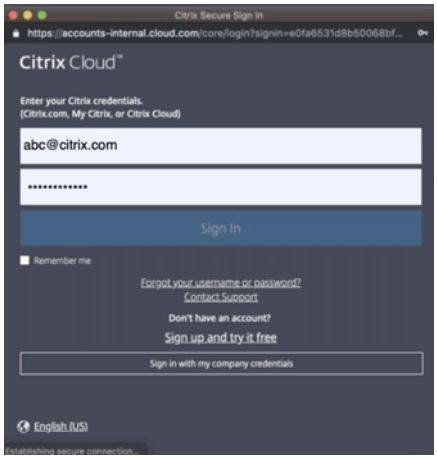
Requisitos previos

- Credenciales de Citrix Workspace Cloud.
- credenciales de suscripción de Azure
- Aplicación y entidad de servicio de Azure con el control de acceso basado en roles, consulte Cómo: Usar el portal para crear una aplicación de Azure AD y un principal de servicio que pueda tener acceso a los recursos.
- Una vez creada la entidad de servicio, tome nota de los siguientes detalles:
  - Identificador de suscriptor de Azure
  - ID de arrendatario
  - ID de aplicación
  - Clave secreta
- Realice la administración de cambios en el Centro MCN/SD-WAN mediante ctx-sdw-sw-xxxxxxx.zip.
- Desde Citrix SD-WAN Center, descubra el MCN y extraiga la configuración activa.

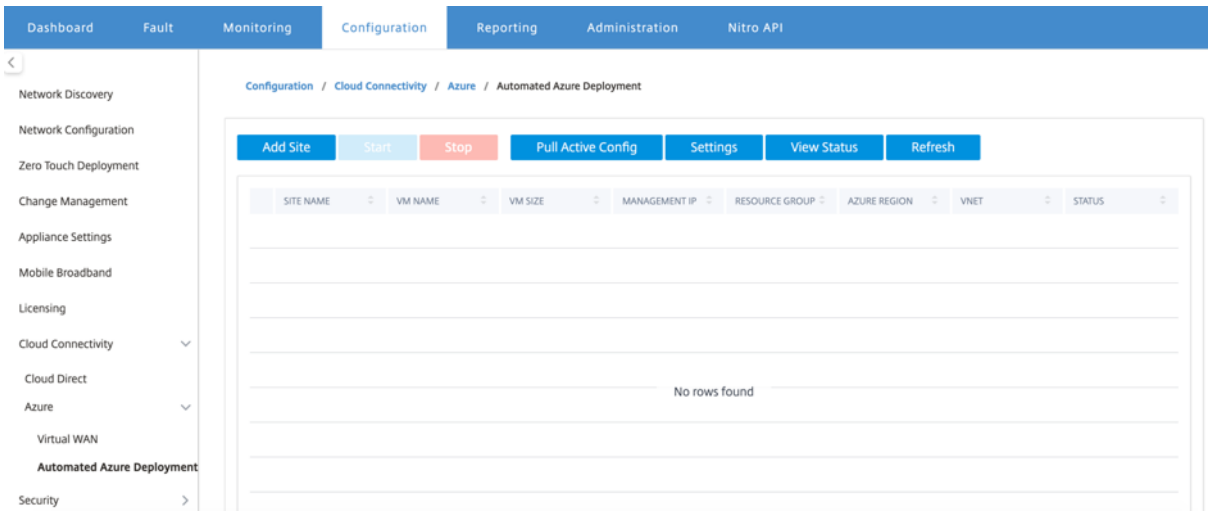
Para implementar Citrix SD-WAN en Azure desde SD-WAN Center, vaya a **Configuración > Conectividad en la nube > Azure > Implementación automatizada de Azure**.



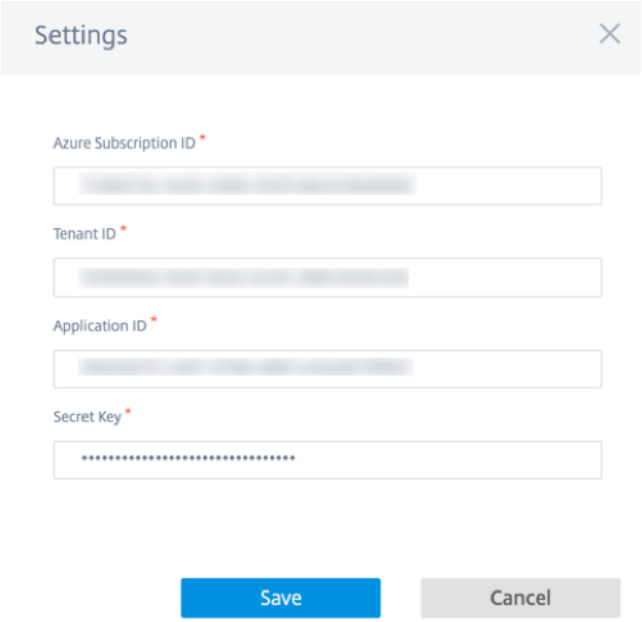
Inicie sesión con las credenciales de Citrix Cloud.



Implementación automática de Azure



Haga clic en **la opción Configuración** y proporcione los detalles de la suscripción de Azure. Haga clic en la opción Extraer configuración activa para recuperar la configuración activa en ejecución del MCN.



Implementación de Citrix SD-WAN en Azure

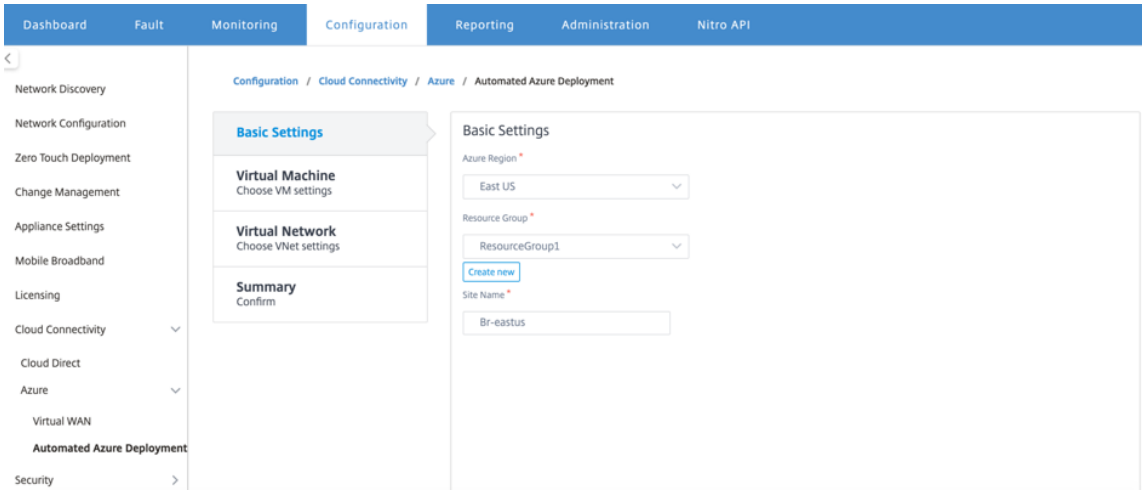
Para implementar Citrix SD-WAN en Microsoft Azure:

1. Haga clic en **Agregar un sitio** para agregar una nueva instancia de SD-WAN. Inicia la creación de una máquina virtual SD-WAN en Azure bajo su suscripción actual.

   Como parte de esta implementación, también:

   - Agrega automáticamente la configuración SD-WAN para el sitio recién agregado a la configuración activa actual en MCN.
   - Realiza la administración de cambios.
   - Aplique la versión y configuración del software de MCN a este nuevo sitio.

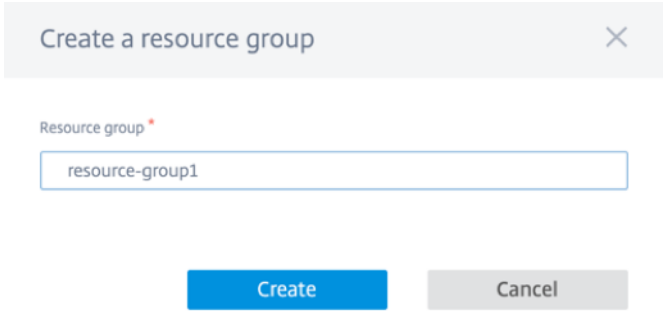
   Complete la **configuración básica, la máquina virtual** y la configuración **de red virtual**.



En Configuración básica, seleccione la región y el grupo de recursos en la lista desplegable. Una vez seleccionada la región, la lista desplegable del grupo de recursos muestra todos los grupos de recursos existentes en esta región bajo esta suscripción.

> **NOTA:**
>
> Para agregar un sitio, el grupo de recursos debe estar vacío.

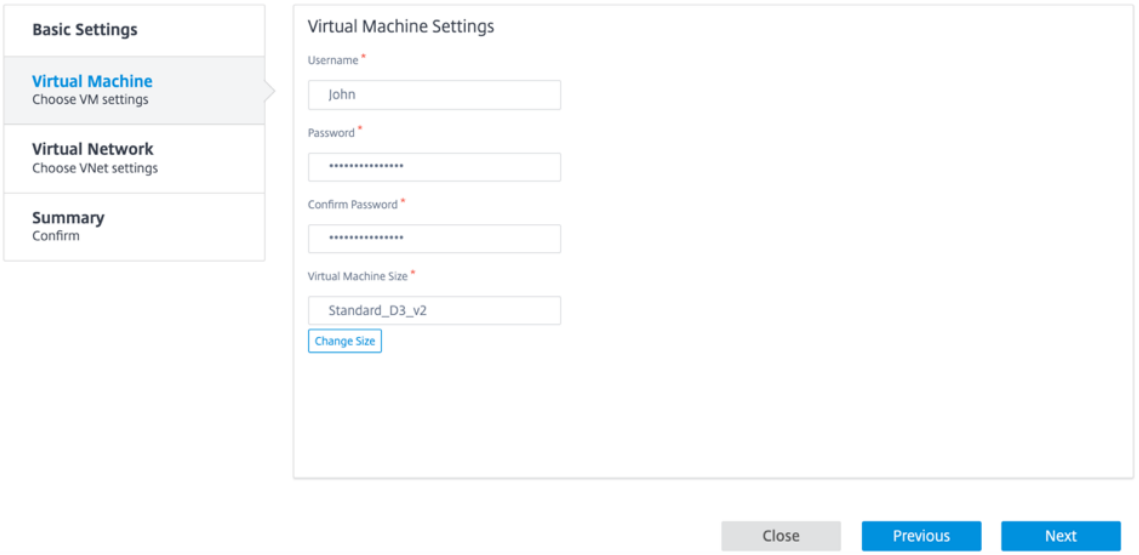
Puede elegir un grupo de recursos vacío existente o hacer clic en la opción **Crear nuevo** para crear uno nuevo.



2. El nombre del sitio se genera automáticamente con el nombre de la región. Aún puede modificar el nombre del sitio según sea necesario.

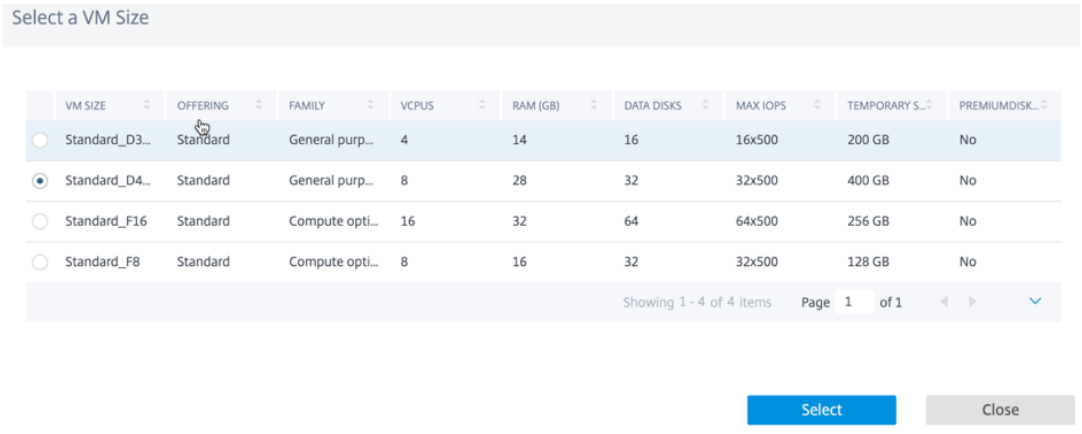
   > **NOTA:**
   >
   > Asegúrese de que el nombre del sitio mantiene los requisitos de nombre de sitio SD-WAN y es único en la red SD-WAN.
   >
   > El nombre de máquina virtual de Azure se genera a partir del nombre del sitio en formato **AZ-Regionname-SiteName**.

3. Haga clic en **Siguiente** para configurar la máquina virtual.

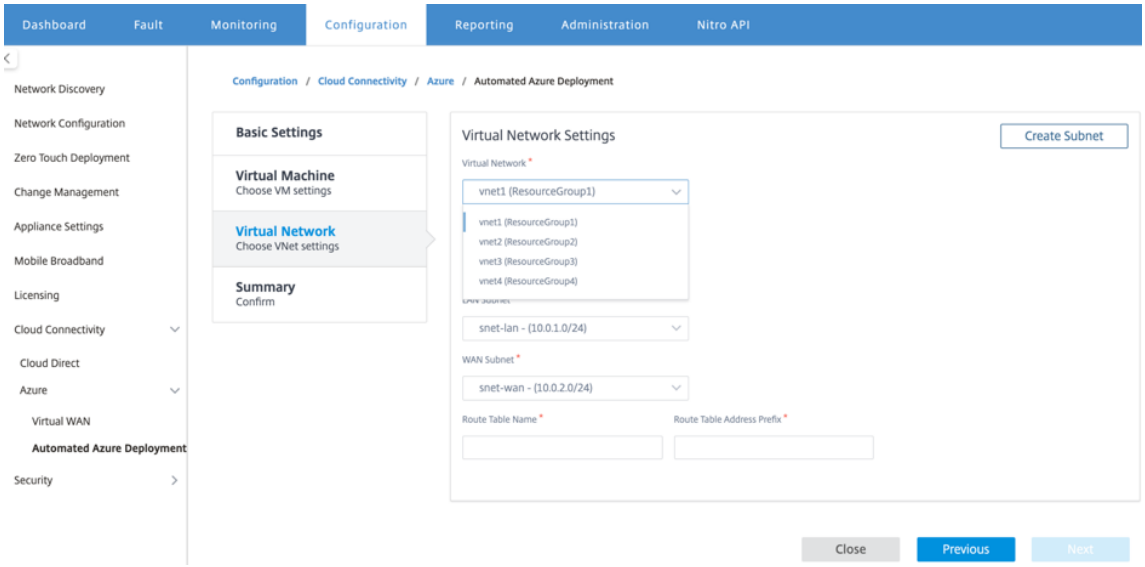


Proporcione un nombre de usuario, contraseña y Confirmar contraseña. De forma predeterminada, el tamaño de la máquina virtual se rellena automáticamente con el tamaño estándar. Haga clic en **Cambiar tamaño** para seleccionar un tamaño de máquina virtual diferente si es necesario.

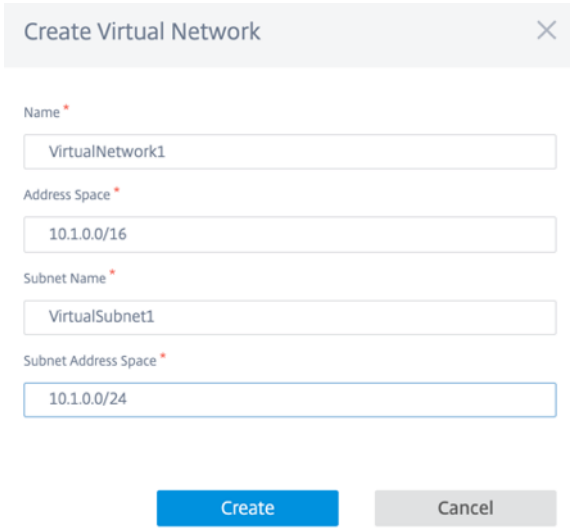
> **NOTA:**
>
> Esta credencial de usuario proporcionada durante la implementación tiene acceso de solo lectura a Azure SD-WAN. Para privilegios administrativos, utilice credenciales de administrador.



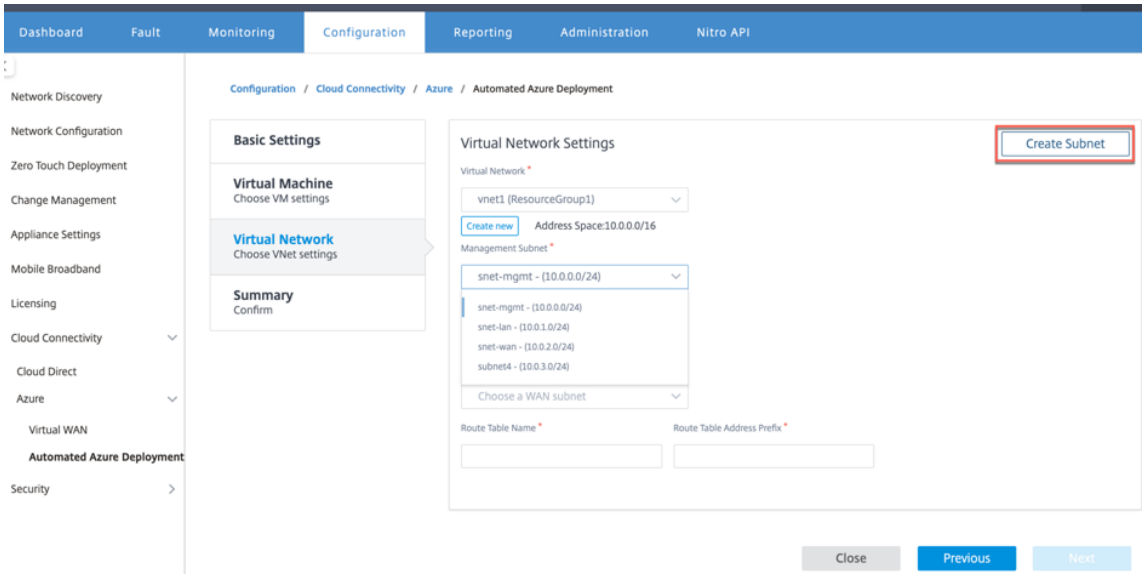
4. Haga clic en **Siguiente** para realizar la configuración de red virtual.
5. Seleccione la red virtual en la lista desplegable. La lista contiene toda la red virtual en la región de Azure elegida.



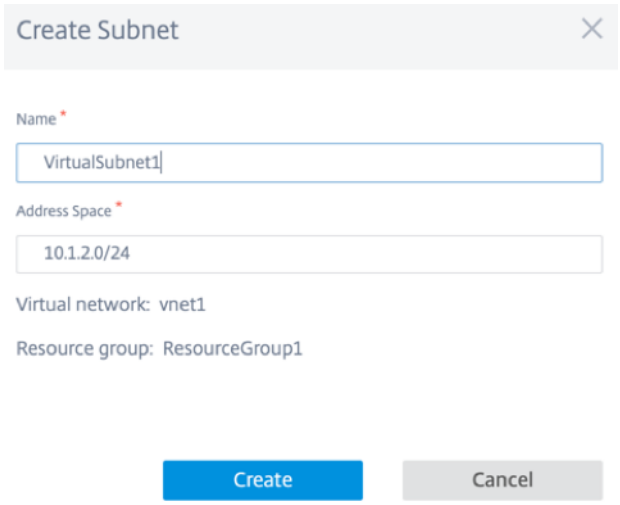
Puede implementar el sitio en una red virtual existente o crear una nueva red virtual. Haga clic en **Crear nuevo** para crear una nueva red virtual. Proporcione el nombre de red virtual, el espacio de direcciones (especifique un espacio de direcciones IP privado personalizado), el nombre de subred y el espacio de direcciones de subred.



6. Seleccione una subred para la administración.



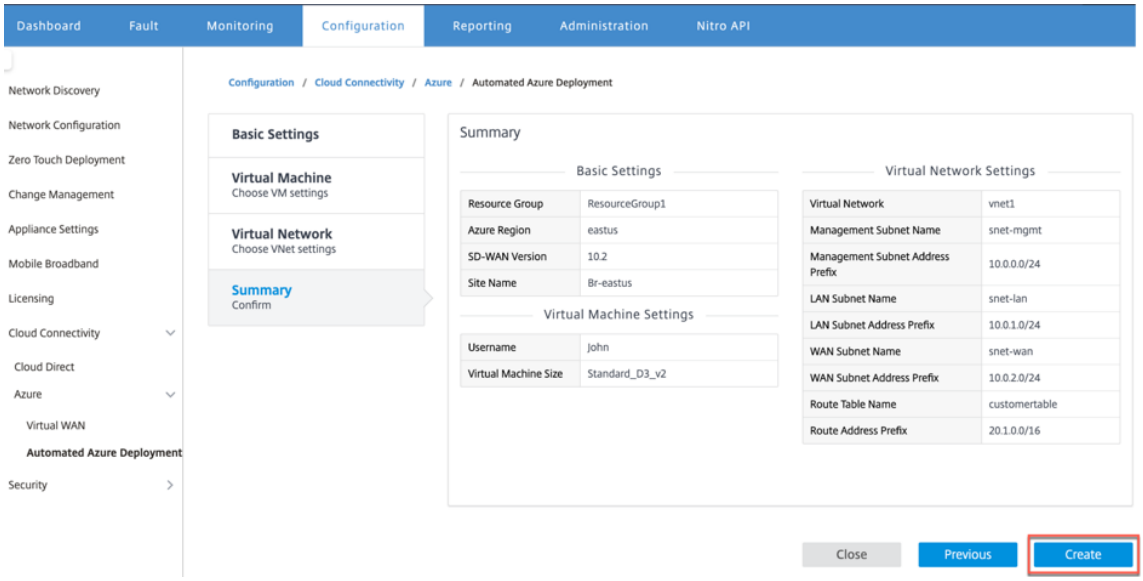
7. También puede crear una subred mediante la opción **Crear una subred** (desde la esquina superior derecha).



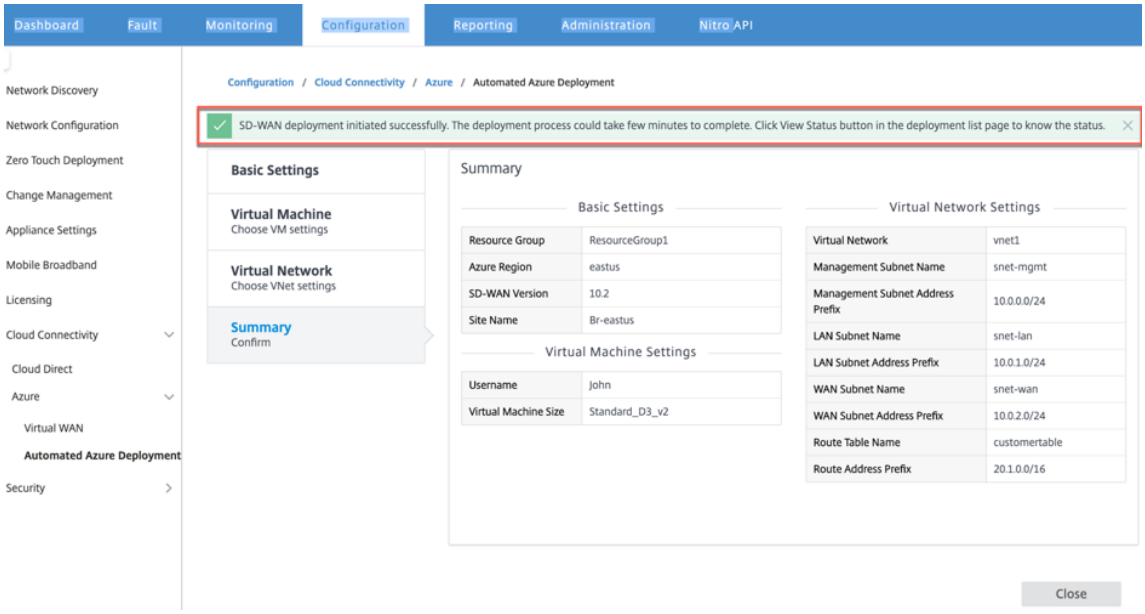
8. En la lista desplegable, elija una subred diferente para LAN y WAN y proporcione el **nombre de la tabla de enrutamiento** junto con el **prefijo de dirección de tabla de enrutamiento**. El **prefijo de dirección de tabla de enrutamiento** es el espacio de direcciones de destino que se redirige a este dispositivo SD-WAN. El enrutamiento de Azure redirigirá otra dirección de destino.

> **NOTA:**
>
> La tabla de enrutamiento está asociada a la subred LAN. Si la subred LAN seleccionada ya tiene una tabla de enrutamiento asociada, esa tabla de ruta se mostrará y no se puede modificar. De lo contrario, puede especificar el nombre de la tabla de enrutamiento.

9. Haga clic en **Siguiente** para revisar y confirmar los detalles de configuración y haga clic en **Crear**.



Aparece un mensaje de estado en la parte superior indicando que la implementación se inició correctamente.



La implementación puede tardar tiempo en completarse, por lo que se recomienda hacer clic en **Ver estado** para obtener la última actualización sobre el estado de la implementación.

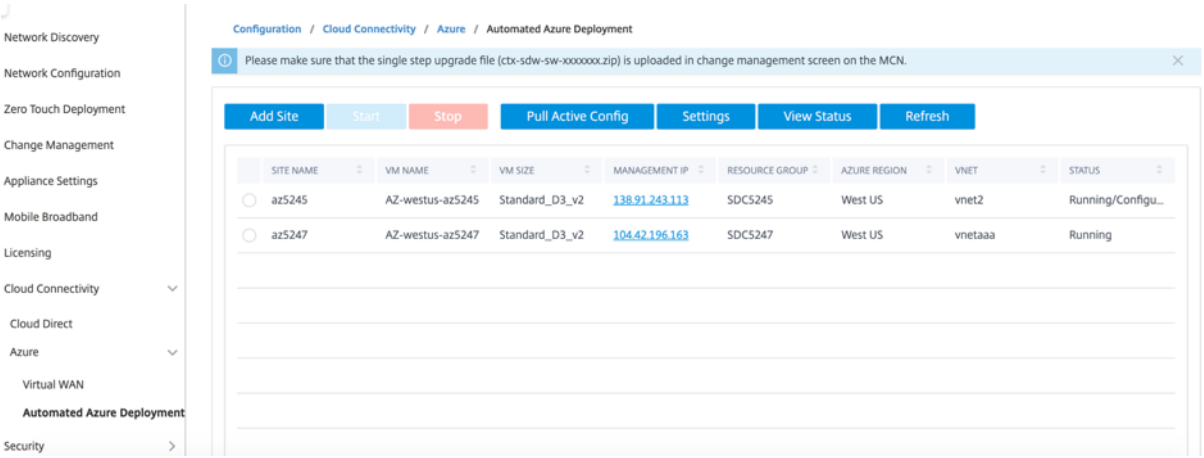
Como parte de la implementación:

- La máquina virtual se crea en la región de Azure seleccionada.
- Un sitio se agrega automáticamente a la configuración activa de SD-WAN en la SD-WAN.
- La administración de cambios se realiza en la máquina virtual de Azure recién aprovisionada.

Una vez que la implementación se realiza correctamente, las rutas virtuales se forman entre el sitio de MCN y Azure. Si la implementación encuentra un error, el proceso se deshace y se revierten todos

los recursos creados automáticamente.

De forma predeterminada, el sitio se coloca como parte del dominio de enrutamiento predeterminado. Pertenece a la región predeterminada mediante el grupo de rutas automáticas predeterminado.



- **Nombre del sitio**: Nombre del sitio de Citrix SD-WAN. Este nombre de sitio se utiliza en la configuración de Citrix SD-WAN.
- **Nombre de máquina virtual**: nombre de la máquina virtual (VM) aprovisionada en Azure.
- **Tamaño de máquina virtual**: el tamaño de máquina virtual que se seleccionó al crear el sitio.
- Dirección**IP**de administración: dirección IP de administración asignada a la máquina virtual SD-WAN recién creada.
- **Grupo de Recursos**: Los grupos de recursos son construcciones lógicas y el intercambio de datos entre grupos de recursos siempre es posible. La máquina virtual de Azure pertenece a este grupo de recursos. Los nuevos recursos creados durante la implementación de Citrix SD-WAN se agrupan en este grupo de recursos. Si se produce algún error durante la implementación, se eliminarán los recursos creados en este grupo de recursos.
- **Región de Azure**: representa la ubicación del grupo de recursos y sus recursos.
- **VNet**: Red virtual que está siendo utilizada por el sitio.
- **Estado**: proporciona el estado de la máquina virtual.

Haga clic en el botón **Actualizar** para obtener el estado más reciente del sitio. Puede **iniciar** o **detener** la máquina virtual en cualquier momento para el sitio seleccionado. Solo puede seleccionar un sitio a la vez.

Cuando finalice la implementación, inicie sesión en MCN o Citrix SD-WAN Center para ver el estado de las rutas virtuales.

Implementación de Zero Touch

January 10, 2022

> **Nota**
>
> El servicio Zero Touch Deployment se admite en determinados dispositivos Citrix SD-WAN:
>
> - SD-WAN 110 Standard Edition
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition (se requiere reimagen)
> - SD-WAN 1000 Enterprise Edition (Premium Edition) (se requiere reimagen)
> - SD-WAN 1100 Standard Edition
> - Edición SD-WAN 1100 Premium (Enterprise)
> - SD-WAN 2000 Standard Edition (se requiere reimagen)
> - SD-WAN 2000 Enterprise Edition (Premium Edition (se requiere reimagen)
> - Instancia de AWS VPX de SD-WAN

El servicio Zero Touch Deployment (ZTD) es un servicio en la nube gestionado y gestionado por Citrix que permite descubrir nuevos dispositivos en la red Citrix SD-WAN y automatiza el proceso de implementación de sucursales. El servicio ZTD Cloud Service es accesible desde cualquier nodo de la red a través de Internet y a través del protocolo Secure Socket Layer (SSL).

ZTD Cloud Service se comunica de forma segura con los servicios de back-end de Citrix Network que almacenan la identificación de los clientes que han adquirido dispositivos compatibles con Zero Touch (por ejemplo, SD-WAN 410-SE, 2100-SE).Los servicios de back-end están disponibles para autenticar cualquier solicitud de implementación de Zero Touch, validando correctamente la asociación entre la cuenta del cliente y los números de serie de los dispositivos Citrix SD-WAN.

Arquitectura y flujo de trabajo de ZTD

Sitio del centro de datos

Citrix SD-WAN Administrator: Usuario con derechos de administración del entorno SD-WAN con las siguientes responsabilidades principales:

- Creación de la configuración mediante la herramienta de configuración de red de Citrix SD-WAN Center o importación de la configuración desde el dispositivo SD-WAN de nodo de control maestro (MCN)

- Citrix Cloud Login para iniciar el servicio Zero Touch Deployment Service para la implementación de nuevos nodos de sitio.

> **Nota**
>
> Si su SD-WAN Center está conectado a Internet a través de un servidor proxy, debe configurar la configuración del servidor proxy en SD-WAN Center. Para obtener más información, consulte Configuración del servidor proxy para la implementación de Zero Touch.

Administrador de red: Un usuario responsable de la administración de redes empresariales (DHCP, DNS, Internet, firewall, etc.)

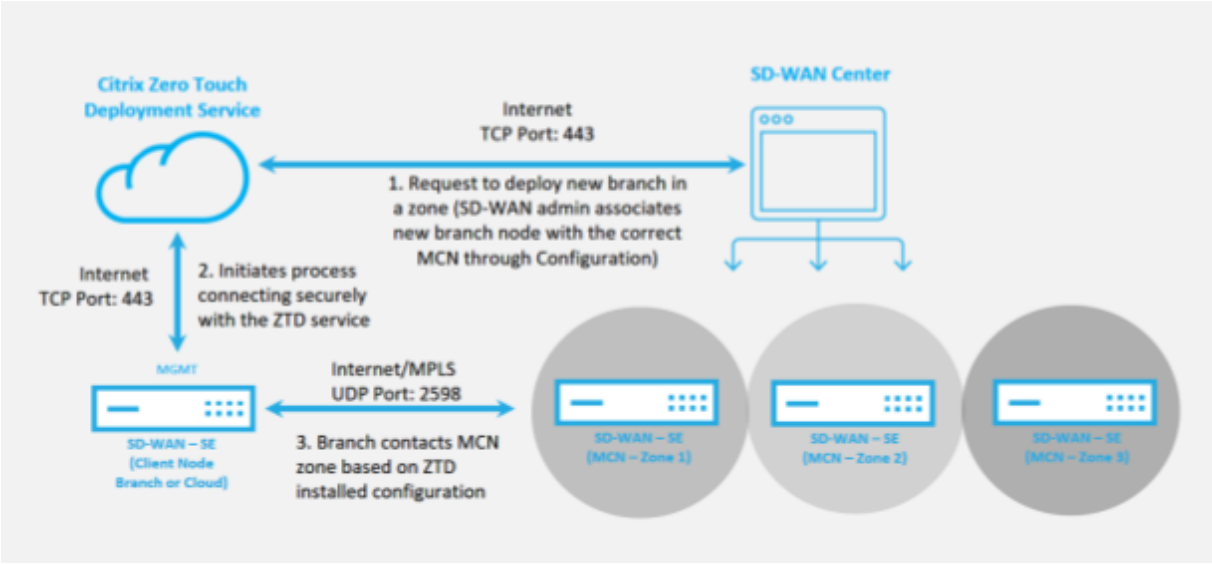
- Si es necesario, configure firewalls para la comunicación saliente con FQDN ***sdwanzt.citrixnetworkapi.net*** desde SD-WAN Center.

Sitio remoto

Instalador in situ: Un contacto local o un instalador contratado para actividades in situ con las siguientes responsabilidades principales:

- Desempaquete físicamente el dispositivo Citrix SD-WAN.
- Reimagen de dispositivos listos para ZTD.
  - Necesario para: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - No se requiere para: SD-WAN 410-SE, 2100-SE
- Cable de alimentación del dispositivo.
- Cable el dispositivo para la conectividad a Internet en la interfaz de administración (por ejemplo, MGMT o 0/1).
- Cable del dispositivo para la conectividad de enlace WAN en las interfaces de datos (por ejemplo, apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc.).

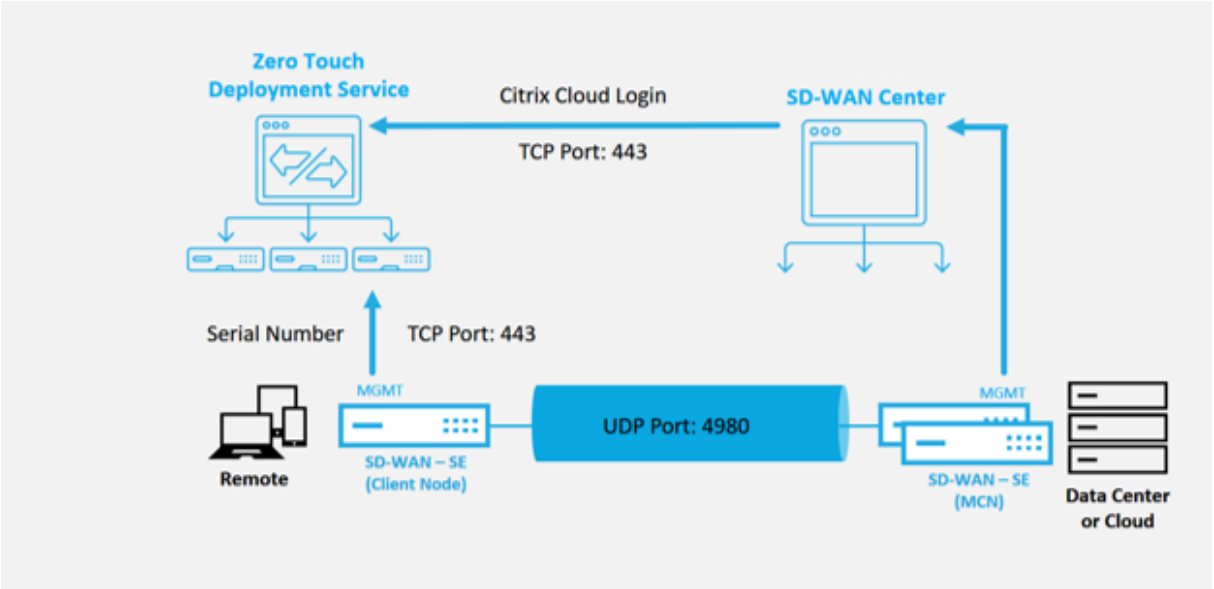
> **Nota**
>
> El diseño de la interfaz es diferente en cada modelo, así que consulte la documentación para la identificación de datos y puertos de administración.



Se requieren los siguientes requisitos previos antes de iniciar cualquier servicio Zero Touch Deployment:

- Ejecución activa de SD-WAN promovida a Master Control Nodo (MCN).
- Ejecución activa de SD-WAN Center con conectividad al MCN a través de Virtual Path.
- Credenciales de inicio de sesión de Citrix Cloud creadas en https://onboarding.cloud.com (consulta las instrucciones que se indican a continuación sobre la creación de la cuenta).
- Conectividad de red de administración (SD-WAN Center y SD-WAN Appliance) a Internet en el puerto 443, ya sea directamente o a través de un servidor proxy.
- Conectividad a Internet en el puerto 443 para acceder al portal web de SD-WAN Center para la configuración inicial de ZTD.
- (opcional) Al menos un dispositivo SD-WAN que se ejecuta activamente en una sucursal en modo cliente con conectividad de ruta virtual válida a MCN para ayudar a validar el establecimiento de rutas correctas en la red subyacente existente.

El último requisito previo no es un requisito, pero permite al administrador de SD-WAN validar que la red de calco subyacente permite que se establezcan rutas virtuales cuando se complete la implementación de Zero Touch con cualquier sitio recién agregado.Principalmente, esto valida que las directivas de firewall y ruta adecuadas estén en vigor para el tráfico NAT en consecuencia o confirmar la capacidad para que el puerto UDP 4980 pueda penetrar correctamente en la red para llegar al MCN.



Descripción general del servicio de implementación de cero toque

El servicio Zero Touch Deployment Service funciona en conjunto con el SD-WAN Center para facilitar la implementación de los dispositivos SD-WAN de sucursales. SD-WAN Center se configura y utiliza como herramienta de administración central para los dispositivos SD-WAN Standard y Enterprise (Premium) Edition.Para utilizar Zero Touch Deployment Service (o ZTD Cloud Service), un administrador debe comenzar por implementar el primer dispositivo SD-WAN en el entorno y, a continuación, configurar e implementar SD-WAN Center como punto central de administración.Cuando el SD-WAN Center, versión 9.1 o posterior, está instalado con conectividad a Internet pública en el puerto 443, SD-WAN Center inicia automáticamente el servicio en la nube e instala los componentes necesarios para desbloquear las funciones de implementación de Zero Touch y hacer que la opción de implementación de Zero Touch esté disponible en la interfaz gráfica de usuario de SD-WAN Center.Zero Touch Deployment no está disponible de forma predeterminada en el software SD-WAN Center.Esto está diseñado a propósito para asegurarse de que los componentes preliminares adecuados de la red de calco subyacente estén presentes antes de permitir que un administrador inicie cualquier actividad in situ que implique la implementación Zero Touch.

Después de un entorno SD-WAN en funcionamiento, el registro en Zero Touch Deployment Service se realiza mediante la creación de un inicio de sesión en la cuenta de Citrix Cloud.Con SD-WAN Center capaz de comunicarse con el servicio ZTD, la GUI expone las opciones de implementación Zero Touch en la ficha Configuración.Al iniciar sesión en el servicio Zero Touch se autentica el ID de cliente asociado al entorno SD-WAN concreto y se registra SD-WAN Center, además de desbloquear la cuenta para una mayor autenticación de las implementaciones de dispositivos ZTD.

Mediante la herramienta de configuración de red en SD-WAN Center, el administrador de SD-WAN necesitará utilizar las plantillas o la capacidad de clonar sitio para crear la configuración de SD-WAN

para agregar nuevos sitios.SD-WAN Center utiliza la nueva configuración para iniciar la implementación de ZTD para los sitios recién agregados.Cuando el administrador de SD-WAN inicia un sitio para la implementación mediante el proceso ZTD, tiene la opción de autenticar previamente el dispositivo que se va a utilizar para ZTD rellenando previamente el número de serie e iniciando la comunicación por correo electrónico con el instalador in situ para iniciar la actividad in situ.

El instalador in situ recibe una comunicación por correo electrónico en la que se indica que el sitio está listo para la implementación de Zero Touch y que puede iniciar el procedimiento de instalación de encendido y cableado del dispositivo para la asignación de direcciones IP DHCP y el acceso a Internet en el puerto MGMT.Además, cableado en cualquier puerto LAN y WAN.Todo lo demás es iniciado por el servicio ZTD y el progreso es supervisado por el uso de la URL de activación. En caso de que el nodo remoto que se va a instalar sea una instancia en la nube, al abrir la URL de activación se inicia el flujo de trabajo para instalar automáticamente la instancia en el entorno de nube designado, ningún instalador local necesita ninguna acción.

Zero Touch Deployment Cloud Service automatiza las siguientes acciones:

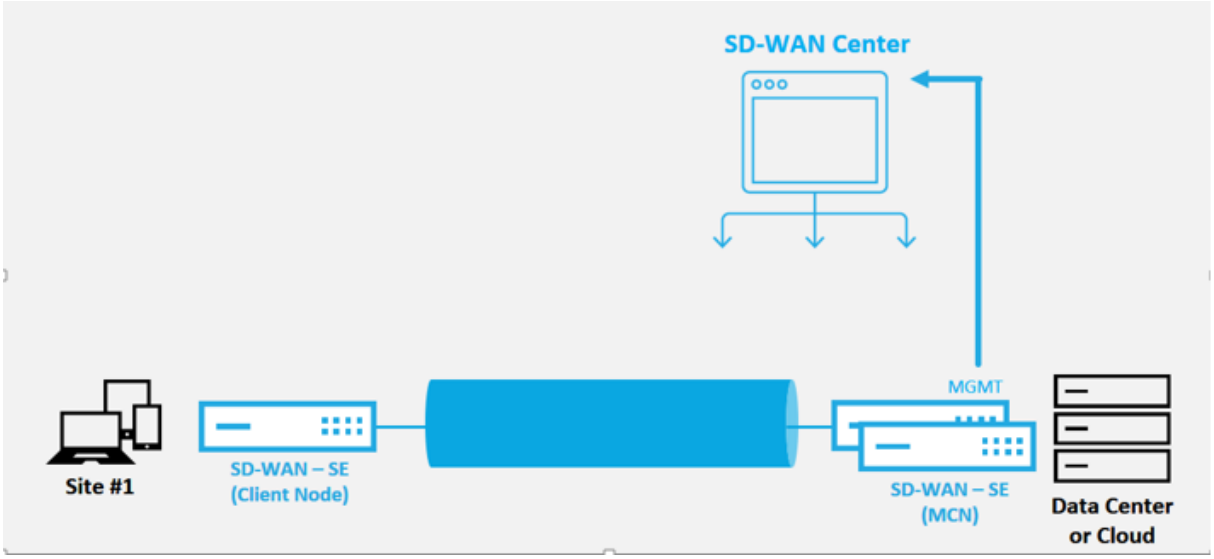
Descargue y actualice el Agente ZTD si hay nuevas funciones disponibles en el dispositivo de sucursal.

- Autenticar el dispositivo de sucursal validando el número de serie.
- Autenticar que el Administrador de SD-WAN aceptó el sitio para ZTD mediante SD-WAN Center.
- Extraiga el archivo de configuración específico para el dispositivo de destino del SD-WAN Center.
- Inserte el archivo de configuración específico para el dispositivo de destino en el dispositivo de sucursal.
- Instale el archivo de configuración en el dispositivo de sucursal.
- Inserte los componentes de software SD-WAN que falten o las actualizaciones necesarias en el dispositivo de sucursal.
- Inserte un archivo de licencia temporal de 10 Mbps para confirmar el establecimiento de la ruta virtual en el dispositivo de sucursal.
- Habilite el servicio SD-WAN en el dispositivo de sucursal.

Se requieren más pasos del Administrador de SD-WAN para instalar un archivo de licencia permanente en el dispositivo.

Procedimiento del servicio de implementación de Zero Touch

En el siguiente procedimiento se detallan los pasos necesarios para implementar un nuevo sitio mediante el servicio de implementación Zero Touch.Tener un MCN en ejecución y un nodo cliente ya trabajando con la comunicación adecuada con SD-WAN Center, así como rutas virtuales establecidas que confirmen la conectividad a través de la red subyacente. Se requieren los siguientes pasos del Administrador de SD-WAN para iniciar la implementación de Zero Touch:



Cómo configurar el servicio de implementación Zero Touch

El SD-WAN Center tiene la funcionalidad de aceptar solicitudes de dispositivos recién conectados para unirse a la red SD-WAN Enterprise. La solicitud se reenvía a la interfaz web a través del servicio de implementación de Zero Touch. Una vez que el dispositivo se conecta al servicio, se descargan los paquetes de configuración y actualización de software.

Flujo de trabajo de configuración:

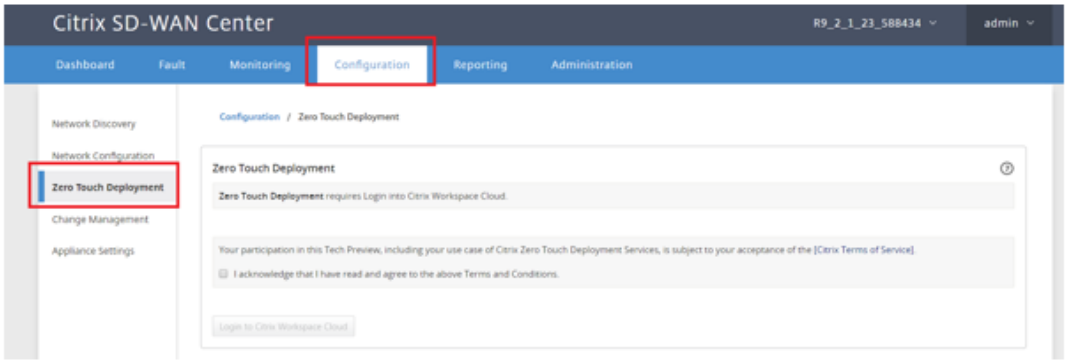
- Acceda a **SD-WAN Center** > **Crear nueva configuración de sitio** o Importar configuración existente y guárdela.
- Inicie sesión en Citrix Workspace Cloud para habilitar el servicio ZTD. La opción de menú Deployment Zero Touch ahora se muestra en la interfaz de administración web de SD-WAN Center.
- En SD-WAN Center, vaya a **Configuración** > **Implementación de Zero Touch** > **Implementar nuevo sitio**.
- Seleccione un dispositivo, haga clic en Habilitar y haga clic en**Implementar**.
- El instalador recibe un correo electrónico de activación > Introduzca el número de serie > **Activar** > El dispositivo se implementa correctamente.

Para configurar el servicio Zero Touch Deployment:

1. Instale SD-WAN Center con capacidades de implementación de Zero Touch habilitadas.
    a) Instale SD-WAN Center con la dirección IP asignada a DHCP.
    b) Verifique que SD-WAN Center asigne una dirección IP de administración adecuada y una dirección DNS de red con conectividad a Internet pública a través de la red de administración.

c) Actualice el SD-WAN Center a la versión más reciente del software SD-WAN.

d) Con una conectividad adecuada a Internet, el SD-WAN Center inicia el servicio en la nube Zero Touch Deployment (ZTD) y descarga e instala automáticamente cualquier actualización de firmware específica para ZTD, si este procedimiento de llamada home falla, la siguiente opción Zero Touch Deployment no estará disponible en la GUI.



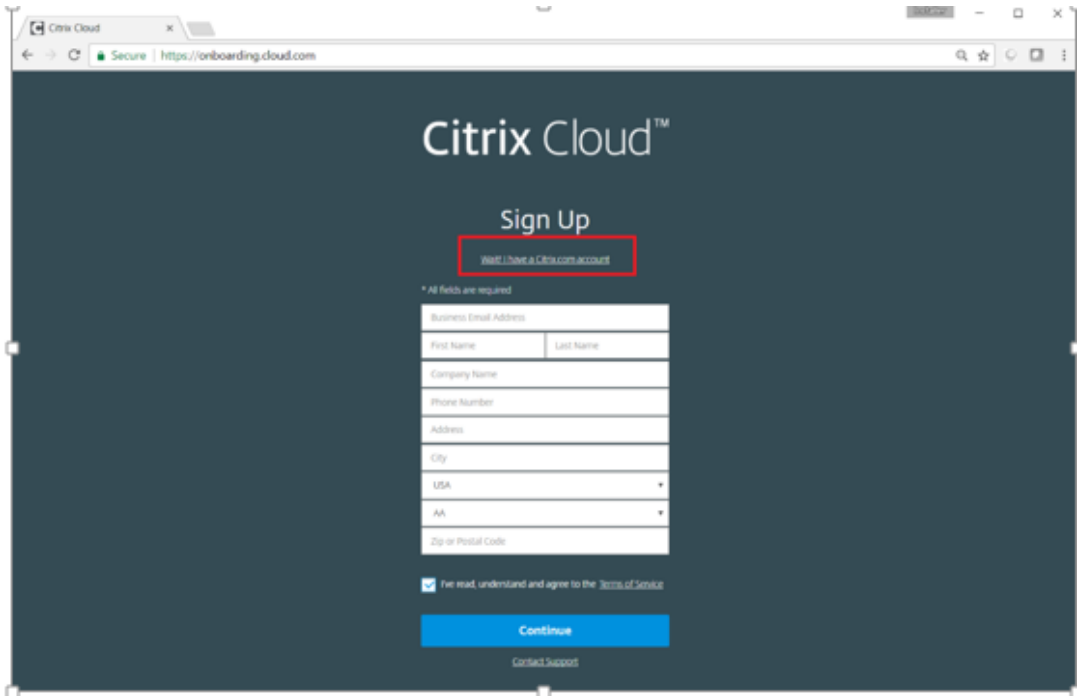
e) Lea los Términos y Condiciones y, a continuación, seleccione **Reconozco que he leído y acepto los Términos y Condiciones anteriores**.

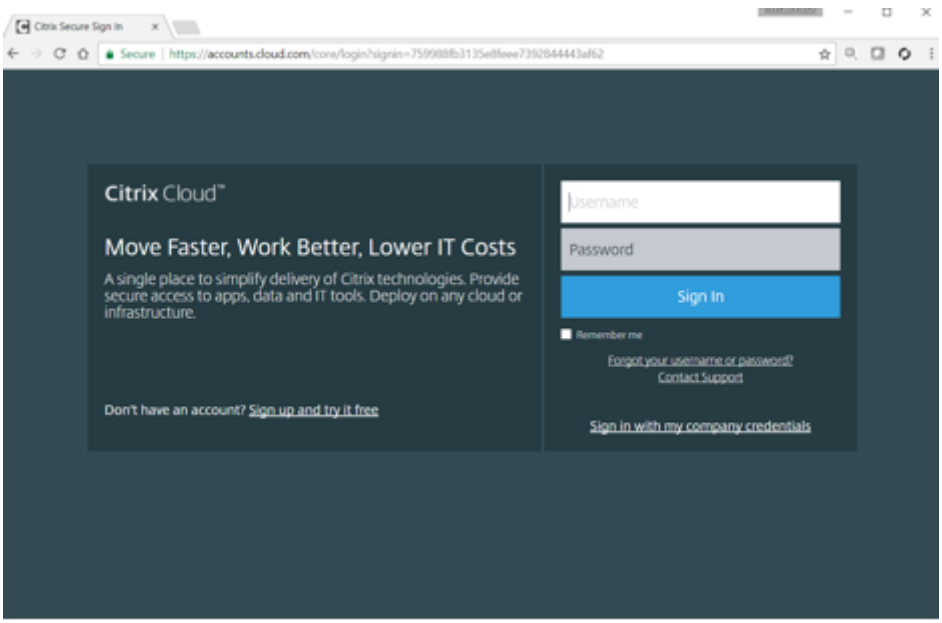
f) Haga clic en el botón **Iniciar sesión en Citrix Workspace Cloud** si ya se ha creado una cuenta de Citrix Cloud.

g) Inicie sesión en la cuenta de Citrix Cloud y, al recibir el siguiente mensaje de inicio de sesión correcto, **NO CERRAR ESTA VENTANA, EL PROCESO REQUIERE OTROS 20 SEGUNDOS APROXIMADAMENTE PARA QUE LA GUI DE SD-WAN CENTER SE ACTUALICE.** La ventana debe cerrarse sola cuando esté completa.**

h) Para crear una cuenta de Cloud Login siga el siguiente procedimiento:

- Abra un explorador web y vaya a https://onboarding.cloud.com.
- Haga clic en el enlace para **Espere, tengo una cuenta de Citrix.com**.





i) Inicie sesión con una cuenta de Citrix existente.

j) Una vez iniciada la sesión en la página SD-WAN Center Zero Touch Deployment, puede observar que no hay sitios disponibles para la implementación de ZTD debido a las siguientes razones:

- La configuración activa no se ha seleccionado en el menú desplegable Configuración
- Todos los sitios para la configuración activa actual ya se han implementado
- La configuración no se creó mediante SD-WAN Center, sino el Editor de configuración disponible en el MCN

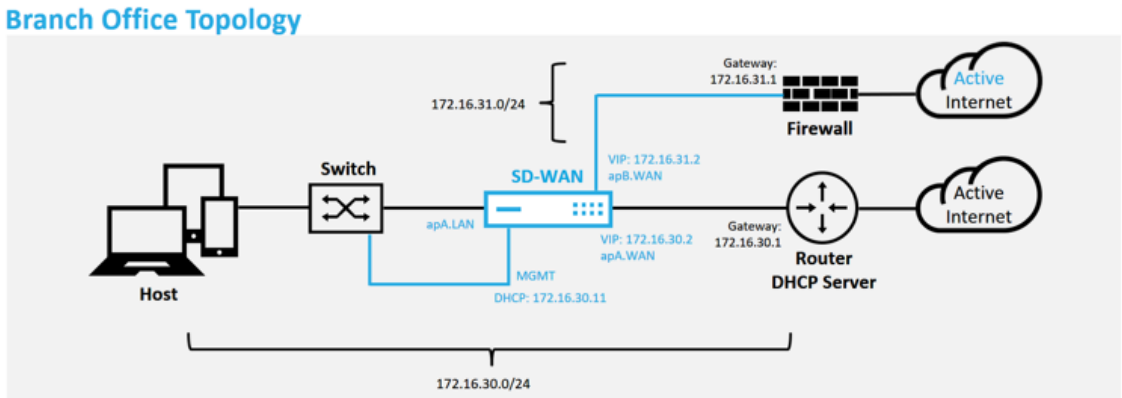
- Los sitios no se crearon en la configuración que hace referencia a dispositivos con prestaciones Zero Touch (por ejemplo, 410-SE, 2100-SE, Cloud VPX)

2. Actualice la configuración para agregar un **nuevo sitio remoto** con un **dispositivo SD-WAN compatible con ZTD** mediante SD-WAN Center Network Configuration.

   Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center.Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center.Se debe utilizar el siguiente procedimiento para agregar un nuevo sitio destinado a la implementación de Zero Touch.

   Diseñe el nuevo sitio para la implementación del dispositivo SD-WAN describiendo primero los detalles del nuevo sitio (es decir, el modelo del dispositivo, el uso de grupos de interfaz, las direcciones IP virtuales, los enlaces WAN con ancho de banda y sus puertas de enlace respectivas).

   > **Importante**
   >
   > Puede observar que cualquier nodo de sitio que tenga VPX seleccionado como modelo también aparece en la lista, pero actualmente la compatibilidad con ZTD solo está disponible para la instancia de AWS VPX.
   >
   > **Nota**
   >
   > - Asegúrese de que utiliza un explorador web compatible con Citrix SD-WAN Center
   > - Asegúrese de que el explorador web no bloquee ninguna ventana emergente durante el inicio de sesión de Citrix Workspace

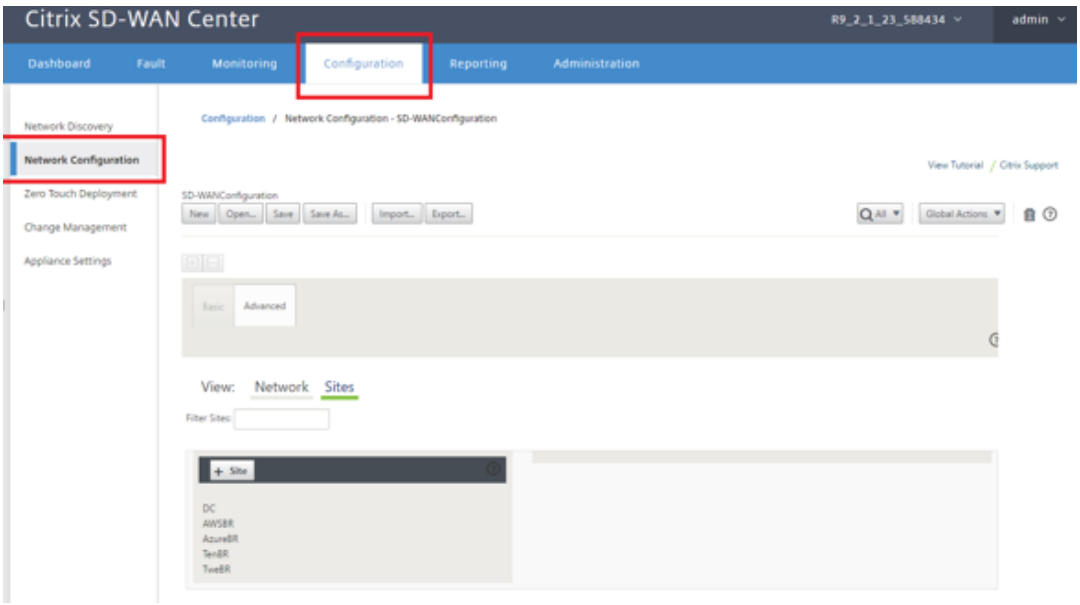
   Se trata de un ejemplo de implementación de un sitio de sucursal, el dispositivo SD-WAN se implementa físicamente en la ruta de acceso del enlace WAN MPLS existente a través de una red 172.16.30.0/24 y mediante un vínculo de copia de seguridad existente habilitándolo en un estado activo y finalizando ese segundo enlace WAN directamente en el dispositivo SD-WAN en una subred diferente 172.16.31.0/24.

Nota

Los dispositivos SD-WAN asignan automáticamente una dirección IP predeterminada 192.168.100.1/16.Con DHCP habilitado de forma predeterminada, el servidor DHCP de la red puede proporcionar al dispositivo una segunda dirección IP en una subred que se superponga a la predeterminada.Esto puede provocar un problema de redirección en el dispositivo en el que el dispositivo puede no conectarse a ZTD Cloud Service. Configure el servidor DHCP para asignar direcciones IP fuera del rango 192.168.0.0/16.

Hay varios modos de implementación disponibles para la colocación de productos SD-WAN en una red. En el ejemplo anterior, SD-WAN se está implementando como una superposición sobre la infraestructura de red existente.Para los nuevos sitios, los administradores de SD-WAN pueden optar por implementar la SD-WAN en la implementación del modo Edge o Gateway, eliminando la necesidad de un enrutador perimetral WAN y un firewall, y consolidando las necesidades de red de enrutamiento perimetral y firewall en la solución SD-WAN.

a) Abra la **interfaz de administración web de SD-WAN Center** y vaya a la página **Configuración** > **Configuración de red**.

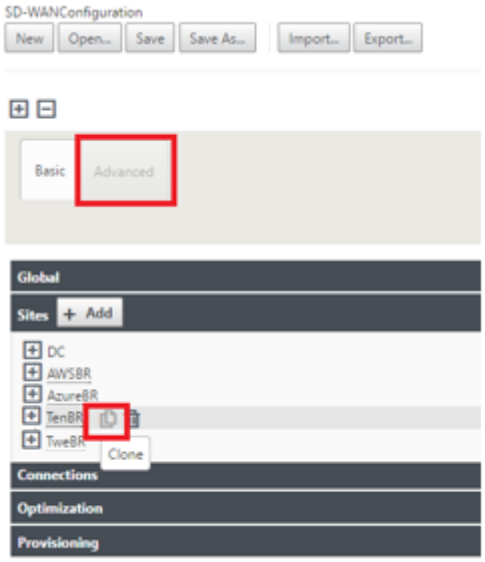


b) Asegúrese de que ya hay una configuración en funcionamiento o importe la configuración desde el MCN.

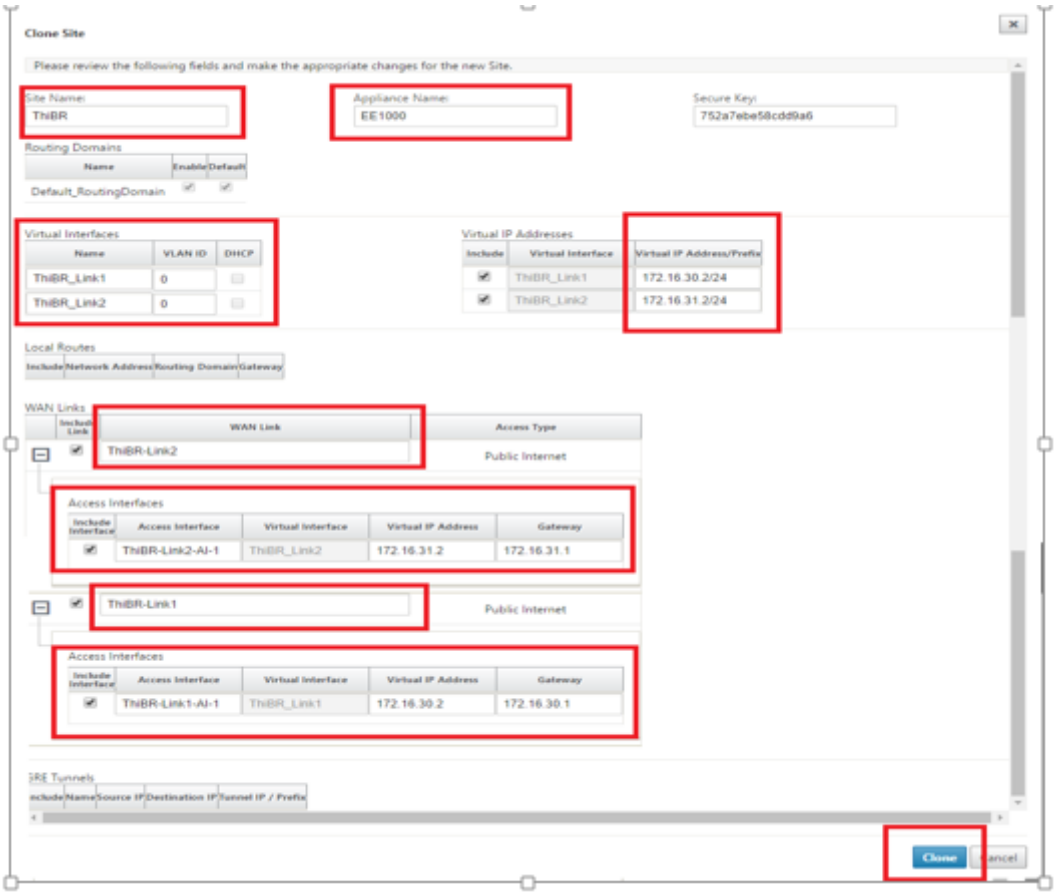
c) Acceda a la ficha Avanzadas para crear un sitio.

d) Abra el icono Sitios para mostrar los sitios configurados actualmente.

e) Creó rápidamente la configuración para el nuevo sitio mediante la función de clonación de cualquier sitio existente.

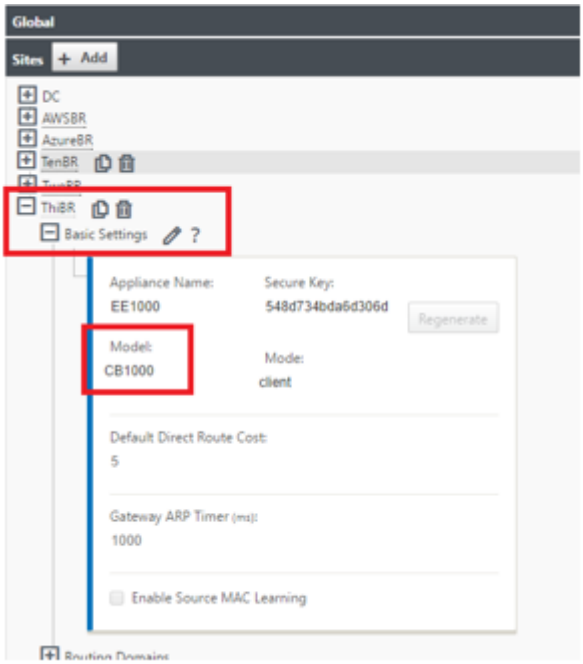


f) Rellene todos los campos requeridos de la topología diseñada para este nuevo sitio de sucursal



g) Después de clonar un sitio nuevo, desplácese hasta la **Configuración básica** del sitio y verifique que el Modelo de SD-WAN esté seleccionado correctamente, lo que soportaría el

servicio Zero Touch.



h) El modelo SD-WAN para el sitio se puede actualizar, pero tenga en cuenta que es posible que deba redefinirse los grupos de interfaz, ya que el dispositivo actualizado puede tener un nuevo diseño de interfaz que se utilizó para clonar.

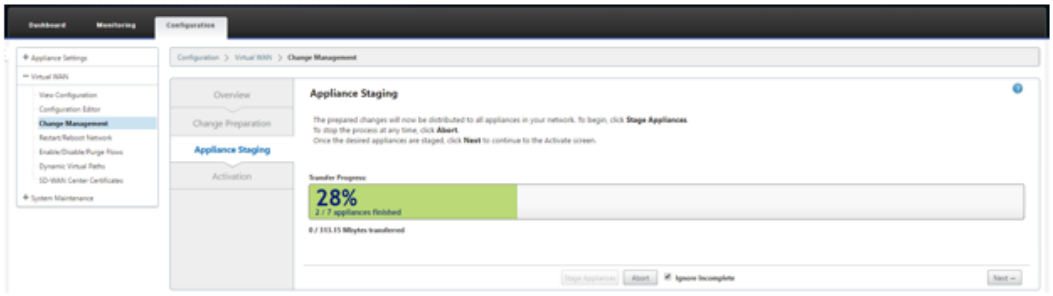
i) Guarde la nueva configuración en SD-WAN Center y use la exportación a la opción **Bandeja de entrada de administración de cambios** para insertar la configuración mediante Administración de cambios.

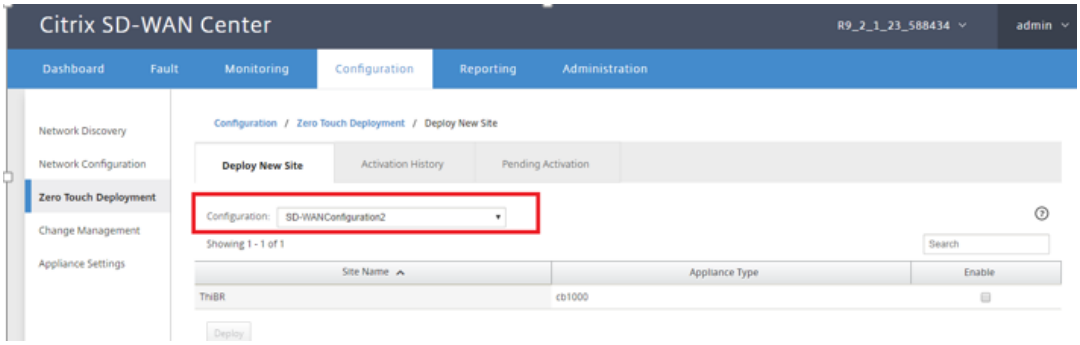
j) Siga el procedimiento de administración de cambios para organizar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar mediante Zero Touch, debe utilizar la opción Ignorar incompleta para omitir el intento de insertar la configuración en el nuevo sitio que aún necesita ir a través del flujo de trabajo ZTD.

3. Vuelva a la página SD-WAN Center Zero Touch Deployment y, con la nueva configuración activa en ejecución, el nuevo sitio estará disponible para su implementación.

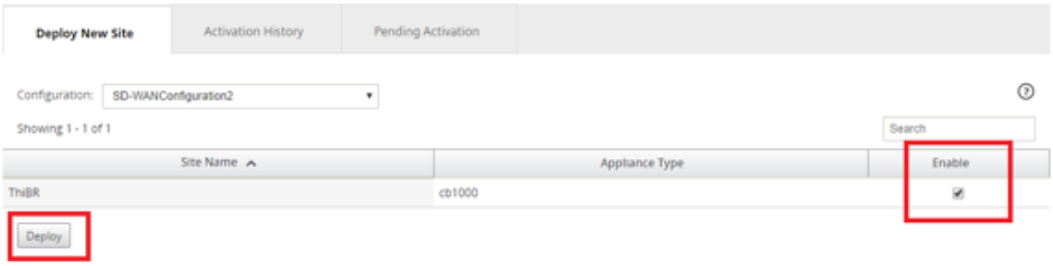
   a) En la página Deployment Zero Touch, en la ficha **Implementar nuevo sitio**, seleccione el archivo de configuración de red en ejecución

   b) Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos SD-WAN no implementados que son compatibles con Zero Touch

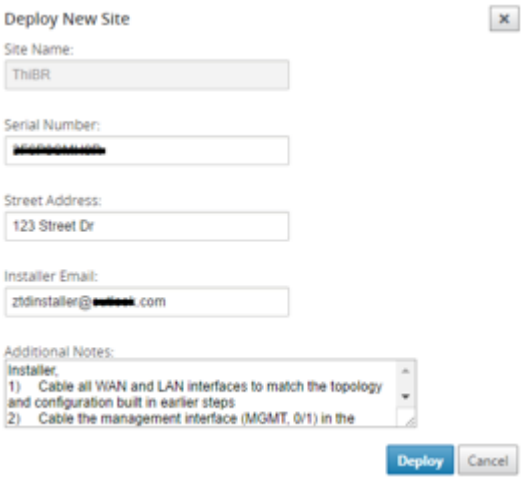




c) Seleccione los sitios de sucursal que quiere configurar para el servicio Zero Touch, haga clic en **Habilitar** y, a continuación, en **Implementar**.



d) Aparece una ventana emergente Implementar nuevo sitio, en la que el administrador puede proporcionar el número de serie, la dirección de calle del sitio de la sucursal, la dirección de correo electrónico del instalador y más notas, si es necesario.

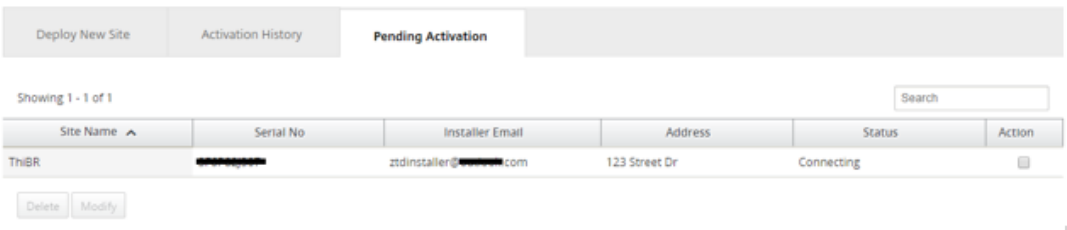


> **Nota**
>
> El campo de entrada Número de serie es opcional y, dependiendo de si se rellena o no, dará lugar a un cambio en la actividad in situ de la que es responsable el instalador.
>
> - Si se rellena el campo Número de serie: no es necesario que el instalador introduzca el número de serie en la URL de activación generada con el comando deploy site
> - Si el campo Número de serie se deja en negro: el instalador será responsable de introducir el número de serie correcto del dispositivo en la URL de activación generada con el comando deploy site

a) Después de hacer clic en el botón **Implementar**, aparecerá un mensaje que indica que "La configuración del sitio se ha implementado".

b) Esta acción activa el SD-WAN Center, que se registró previamente con ZTD Cloud Service, para compartir la configuración de este sitio en particular para que sea temporal almacenada en ZTD Cloud Service.

c) Acceda a la ficha Activación pendiente para confirmar que la información del sitio de la sucursal se rellenó correctamente y se puso en un estado de actividad del instalador pendiente.

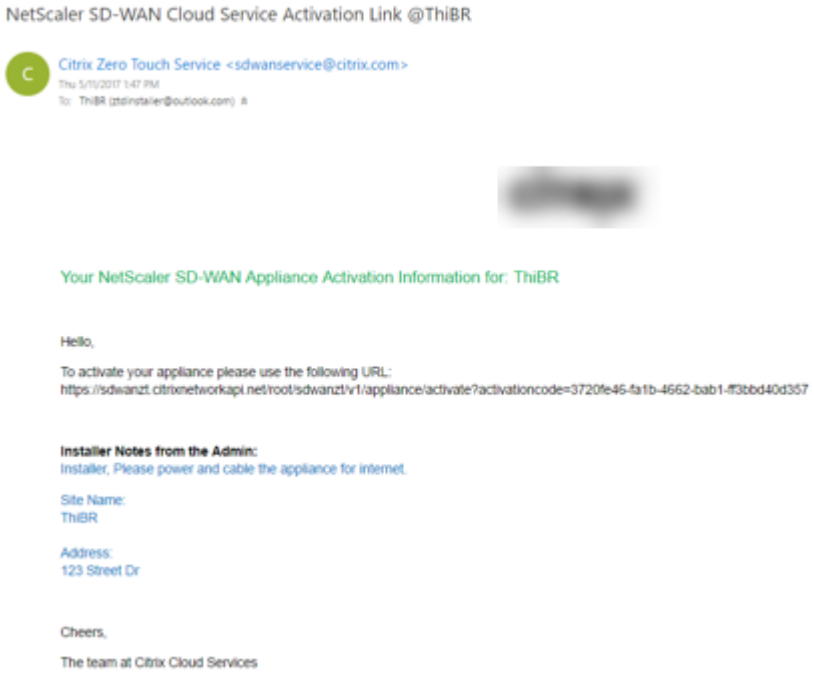


> **Nota**
>
> Si la información es incorrecta, se puede seleccionar una implementación de Zero Touch

> en el estado de activación pendiente. Si se elimina un sitio de la página de activación pendiente, estará disponible para su implementación en la página de ficha Implementar nuevo sitio. Una vez que elija eliminar el sitio de la sucursal de Activación pendiente, el enlace de activación enviado al instalador se convierte en inválido.
>
> Si el administrador de SD-WAN no rellenó el campo Número de serie, el campo de estado indica Esperando el instalador en lugar de Conectando.

4. La siguiente serie de actividades es realizada por el instalador in situ.

   a) El instalador comprueba en el buzón la dirección de correo electrónico que utilizó el Administrador de SD-WAN al implementar el sitio.



   b) Abra la URL de activación de implementación de Zero Touch en una ventana del explorador de Internet.

   c) Si el administrador de SD-WAN no rellenó previamente el número de serie en el paso del sitio de implementación, el instalador será responsable de localizar el número de serie en el dispositivo físico e introducir el número de serie manualmente en la URL de activación y, a continuación, haga clic en el botón **Activar**.

d) Si el administrador rellenando previamente la información del número de serie, la URL de activación ya habrá progresado al siguiente paso.

e) El instalador debe estar físicamente in situ para realizar las siguientes acciones:

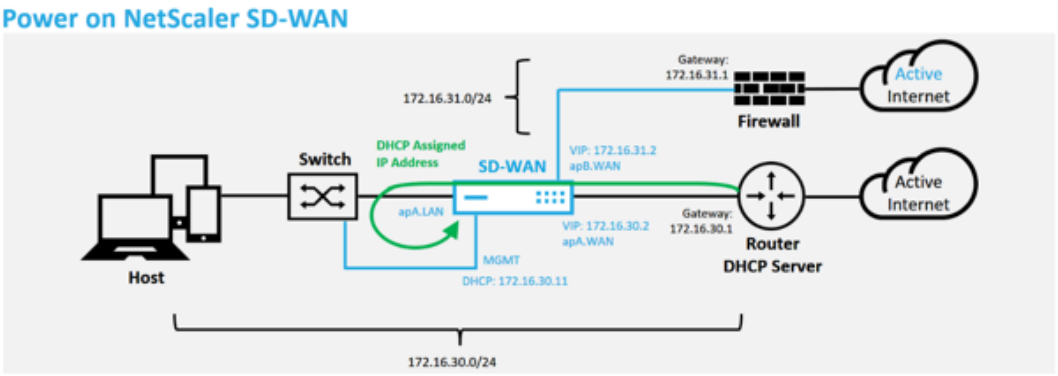
- Cable todas las interfaces WAN y LAN para que coincidan con la topología y la configuración incorporadas en los pasos anteriores.
- Cable de la interfaz de administración (MGMT, 0/1) en el segmento de la red que proporciona la dirección IP DHCP y conectividad a Internet con DNS y FQDN a la resolución de direcciones IP.
- Cable de alimentación del dispositivo SD-WAN.
- Encienda el interruptor de alimentación del dispositivo.

> **Nota**
>
> La mayoría de los dispositivos se encenderán automáticamente cuando el cable de alimentación esté conectado.Es posible que algunos dispositivos tengan que encenderlo con el interruptor de encendido situado en la parte frontal del dispositivo, mientras que otros pueden tener el interruptor de encendido en la parte posterior del dispositivo.Algunos interruptores de encendido requieren mantener pulsado el botón de encendido hasta que la unidad se encienda.

5. La siguiente serie de pasos se automatizan con la ayuda del servicio Zero Touch Deployment, pero requiere que estén disponibles los siguientes requisitos previos.

   - El dispositivo de sucursal debe estar encendido
   - DHCP debe estar disponible en la red existente para asignar la administración y la dirección IP DNS
   - Cualquier dirección IP asignada DHCP requiere conectividad a Internet con capacidad para resolver FQDN
   - La asignación de IP se puede configurar manualmente, siempre y cuando se cumplan los demás requisitos previos

   a) El dispositivo obtiene una dirección IP del servidor DHCP de redes, en este ejemplo topología esto se logra a través de las interfaces de datos omitidas de un dispositivo de estado predeterminado de fábrica.

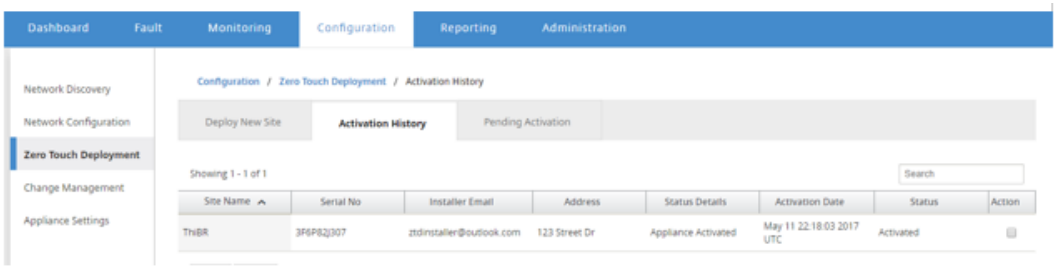


b) A medida que el dispositivo obtiene la administración web y las direcciones IP DNS del servidor DHCP de red subyacente, el dispositivo inicia el servicio Zero Touch Deployment Service y descarga las actualizaciones de software relacionadas con ZTD.

c) Con una conectividad correcta con ZTD Cloud Service, el proceso de implementación realiza automáticamente lo siguiente:

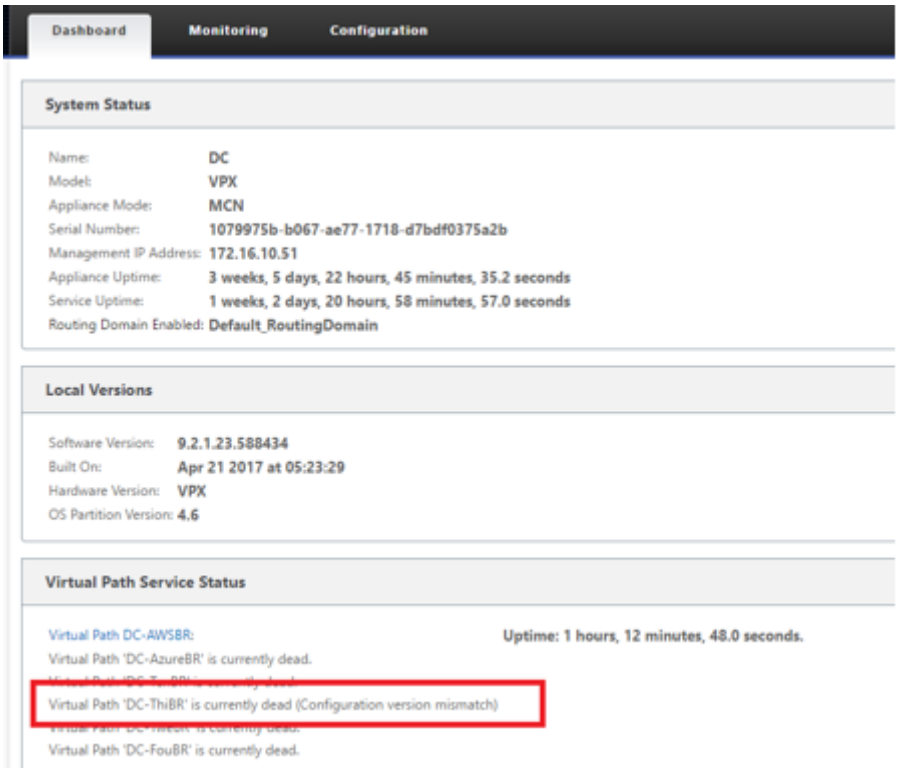
- Descargue el archivo de configuración almacenado anteriormente por el SD-WAN Center
- Aplicación de la configuración al dispositivo local
- Descargar e instalar un archivo de licencia temporal de 10 MB
- Descargar e instalar cualquier actualización de software si es necesario
- Activar el servicio SD-WAN

d) Se puede realizar una confirmación adicional en la interfaz de administración web de SD-WAN Center; en el menú Implementación táctil se muestran los dispositivos activados correctamente en la ficha **Historial de activación**.

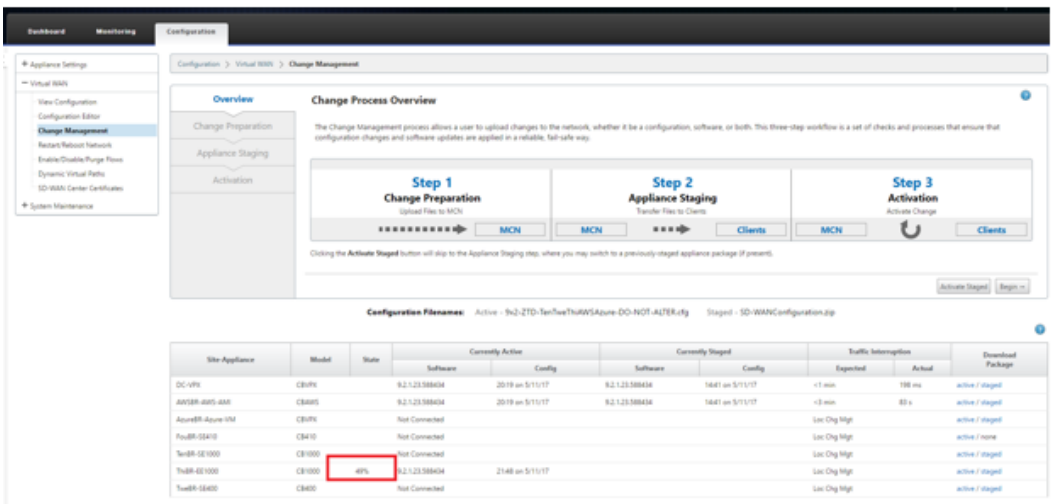


e) Es posible que las rutas virtuales no se muestren inmediatamente en un estado conectado

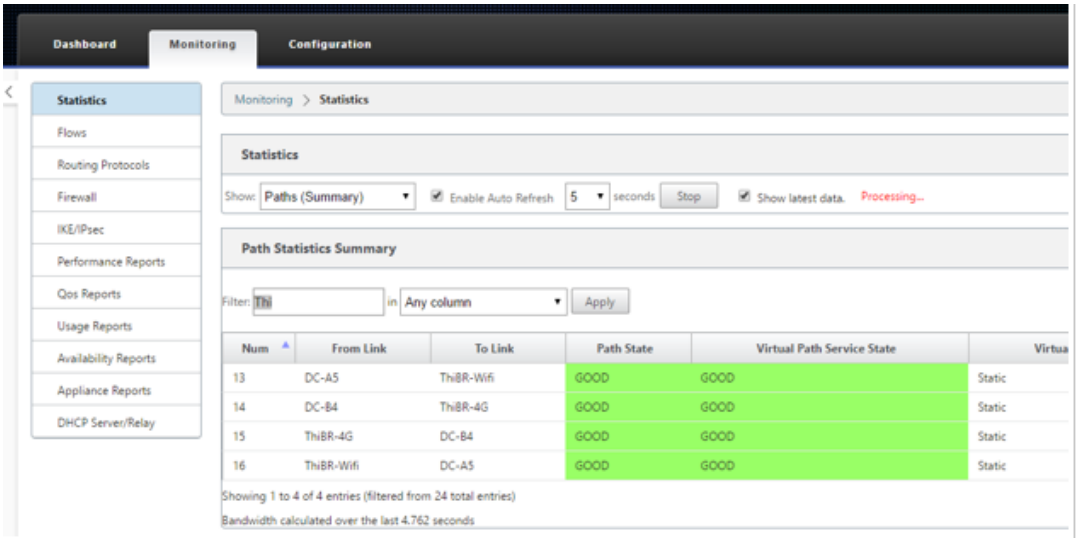
porque es posible que el MCN no confíe en la configuración transmitida desde ZTD Cloud Service e informe No coincide la versión de configuración en el panel de MCN.



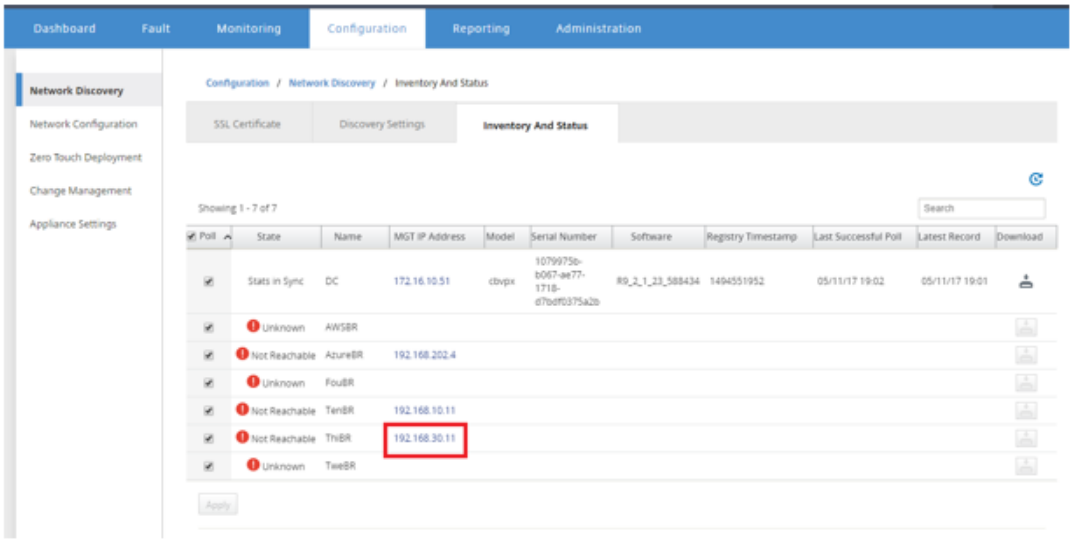
f) La configuración se vuelve a entregar al dispositivo de sucursal recién instalado y el estado se supervisa en la página **MCN** > **Configuración** > **WAN virtual** > **Administración de cambios** (este proceso puede tardar varios minutos en completarse).



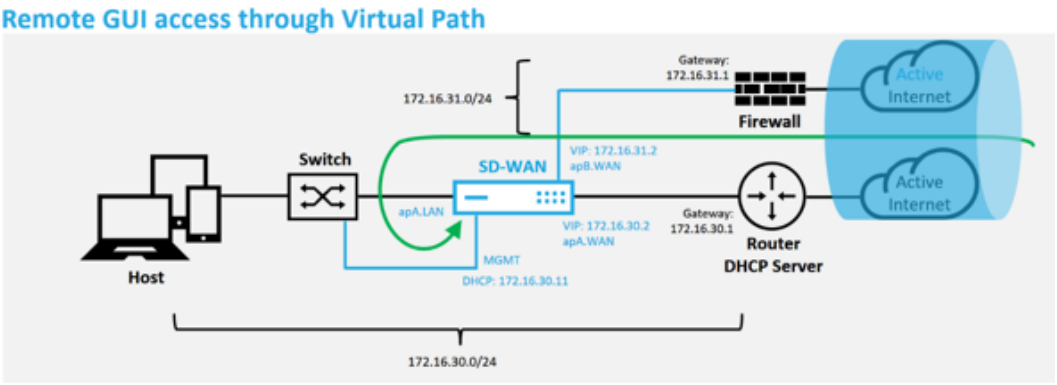
g) El Administrador de SD-WAN puede supervisar la página de administración web de MCN de cabecera para las rutas virtuales establecidas del sitio remoto.



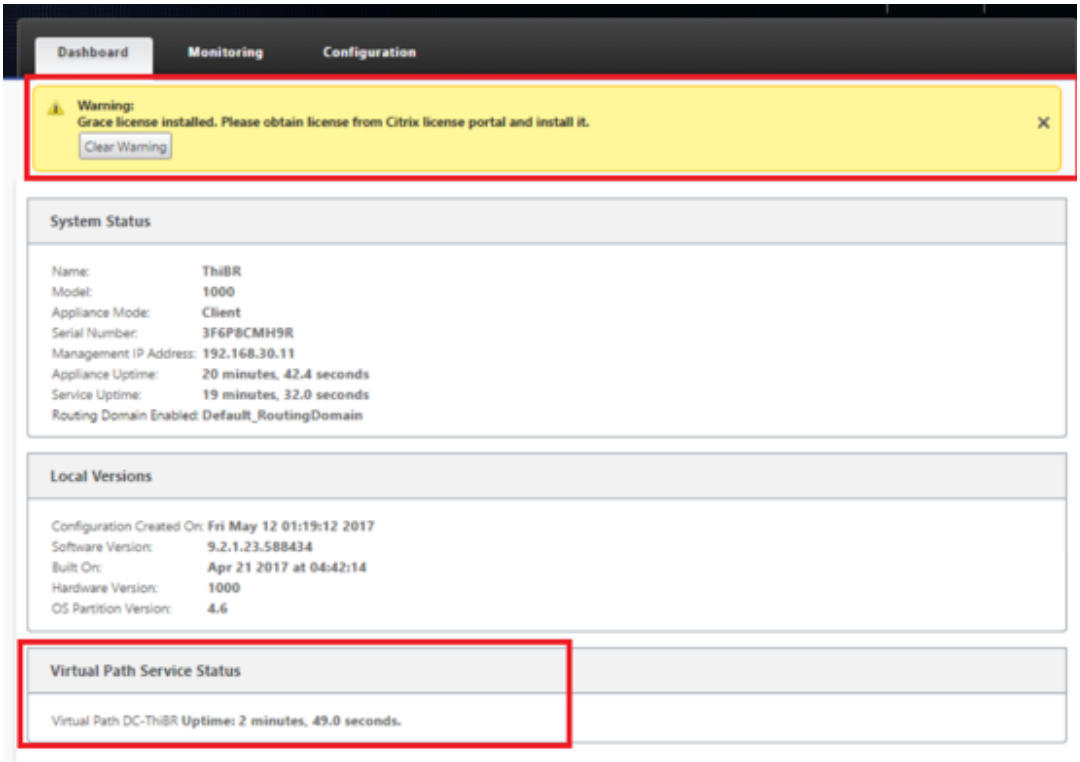
h) SD-WAN Center también se puede utilizar para identificar la dirección IP asignada por DHCP del dispositivo in situ desde la página **Configuración** > **Detección de red** > **Inventario y estado**.



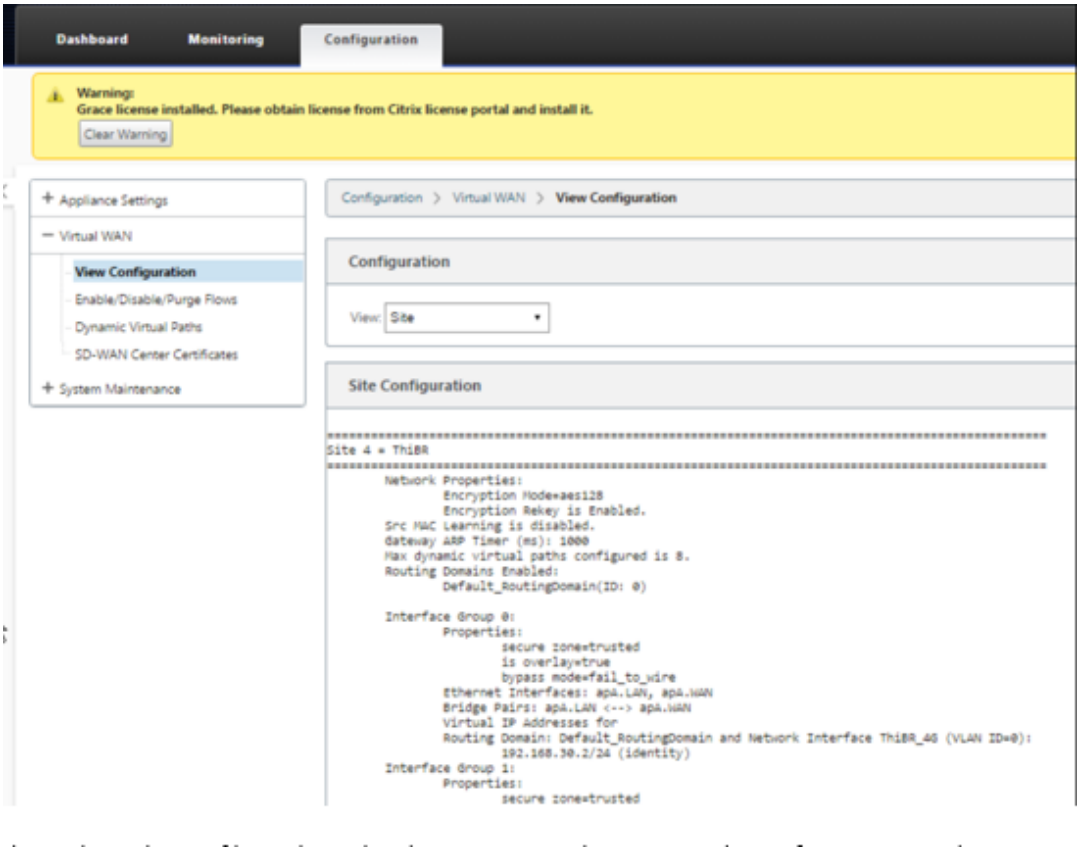
i) En este punto, el Administrador de red SD-WAN puede obtener acceso de administración web al dispositivo in situ mediante la red de superposición SD-WAN.



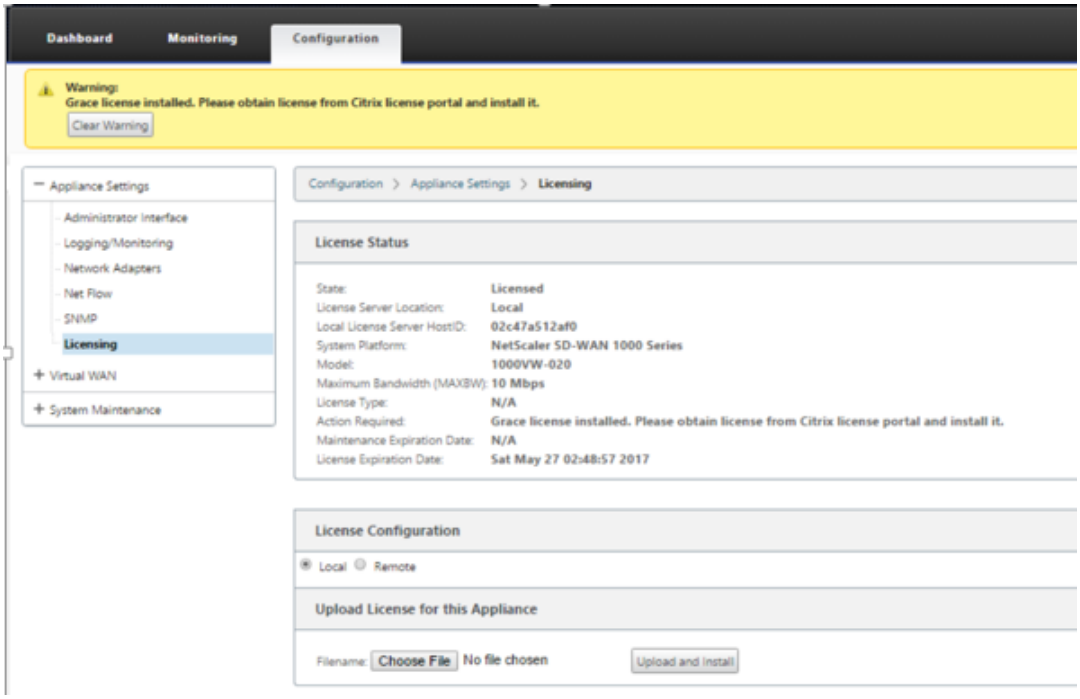
j) El acceso de administración web al dispositivo de sitio remoto indica que el dispositivo se ha instalado con una licencia Grace temporal a 10 Mbps, lo que permite que el estado del servicio de ruta virtual se informe como activo.



k) La configuración del dispositivo se puede validar mediante la página **Configuración** > **WAN virtual** > **Ver configuración**.



l) El archivo de licencia del dispositivo se puede actualizar a una licencia permanente mediante la página **Configuración** > **Configuración del equipo** > **Licencias**.



m) Después de cargar e instalar el archivo de licencia permanente, el banner de advertencia

de licencia Grace desaparece y durante el proceso de instalación de la licencia no se producirá ninguna pérdida de conectividad con el sitio remoto (se eliminan cero pings).

Zero Touch local

April 13, 2021

Para obtener instrucciones acerca de cómo implementar un dispositivo SD-WAN con servicio Zero Touch, consulte el tema Cómo configurar el servicio de implementación Zero Touch.

AWS

April 9, 2021

Implementación en AWS

Con la versión 9.3 de SD-WAN, las capacidades de implementación de Zero Touch se han extendido a las instancias de la nube.El procedimiento para implementar el proceso de implementación de Zero Touch cuatro instancias en la nube es ligeramente diferente de la implementación del dispositivo para el servicio Zero Touch.

1. Actualice la configuración para agregar un nuevo sitio remoto con un dispositivo en la nube SD-WAN compatible con ZTD mediante SD-WAN Center Network Configuration.

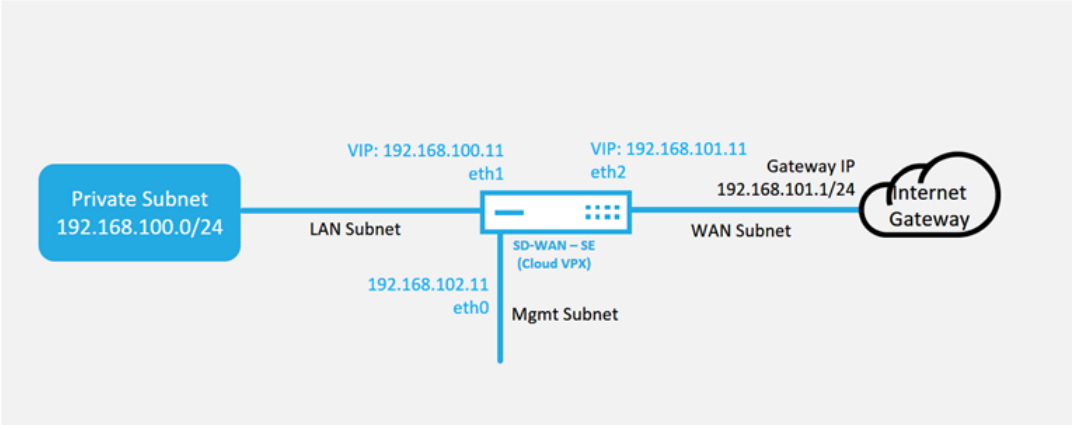
   Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center.Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center.Se debe utilizar el siguiente procedimiento para agregar un nuevo nodo en la nube destinado a la implementación de Zero Touch.

   a) Diseñar el nuevo sitio para la implementación en la nube SD-WAN esbozando primero los detalles del nuevo sitio (es decir, tamaño VPX, uso de grupos de interfaz, direcciones IP virtuales, enlaces WAN con ancho de banda y sus respectivas puertas de enlace).

      > **Nota**
      >
      > • Las instancias SD-WAN implementadas en la nube deben implementarse en

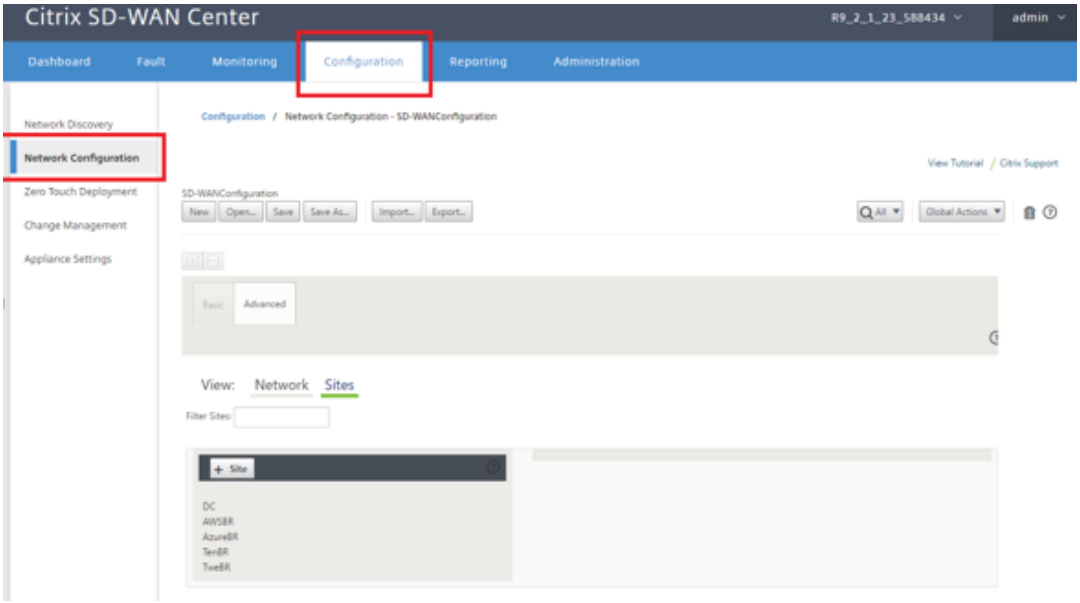
> modo Edge/Gateway.
> - La plantilla para la instancia en la nube está limitada a tres interfaces: Administración, LAN y WAN (en ese orden).
> - Las plantillas de nube disponibles para SD-WAN VPX están actualmente configuradas para obtener la dirección IP #.#.#.11 de las subredes disponibles en la VPC.

Cloud Topology with NetScaler SD-WAN



Este es un ejemplo de implementación de un sitio implementado en la nube SD-WAN, el dispositivo Citrix SD-WAN se implementa como el dispositivo perimetral que presta servicio a un único enlace WAN de Internet en esta red en la nube.Los sitios remotos podrán aprovechar varios enlaces WAN de Internet distintos que se conectan a esta misma puerta de enlace de Internet para la nube, proporcionando resiliencia y conectividad de ancho de banda agregada desde cualquier sitio de implementación de SD-WAN a la infraestructura de la nube.Esto proporciona conectividad rentable y altamente confiable a la nube.

b) Abra la interfaz de administración web de SD-WAN Center y vaya a la página **Configuración** > **Configuración de red**.

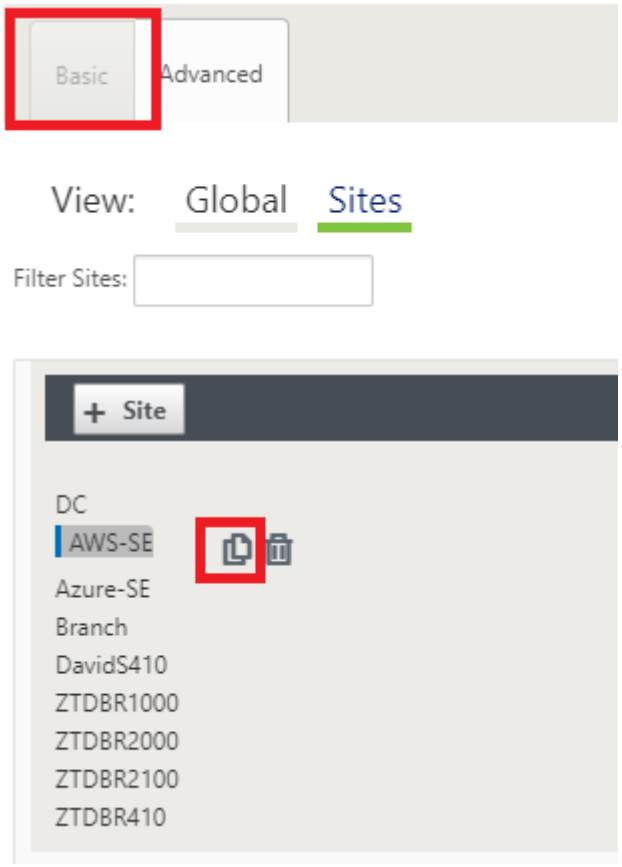


c) Asegúrese de que ya hay una configuración en funcionamiento o importe la configuración desde el MCN.

d) Acceda a la ficha Básico para crear un nuevo sitio.

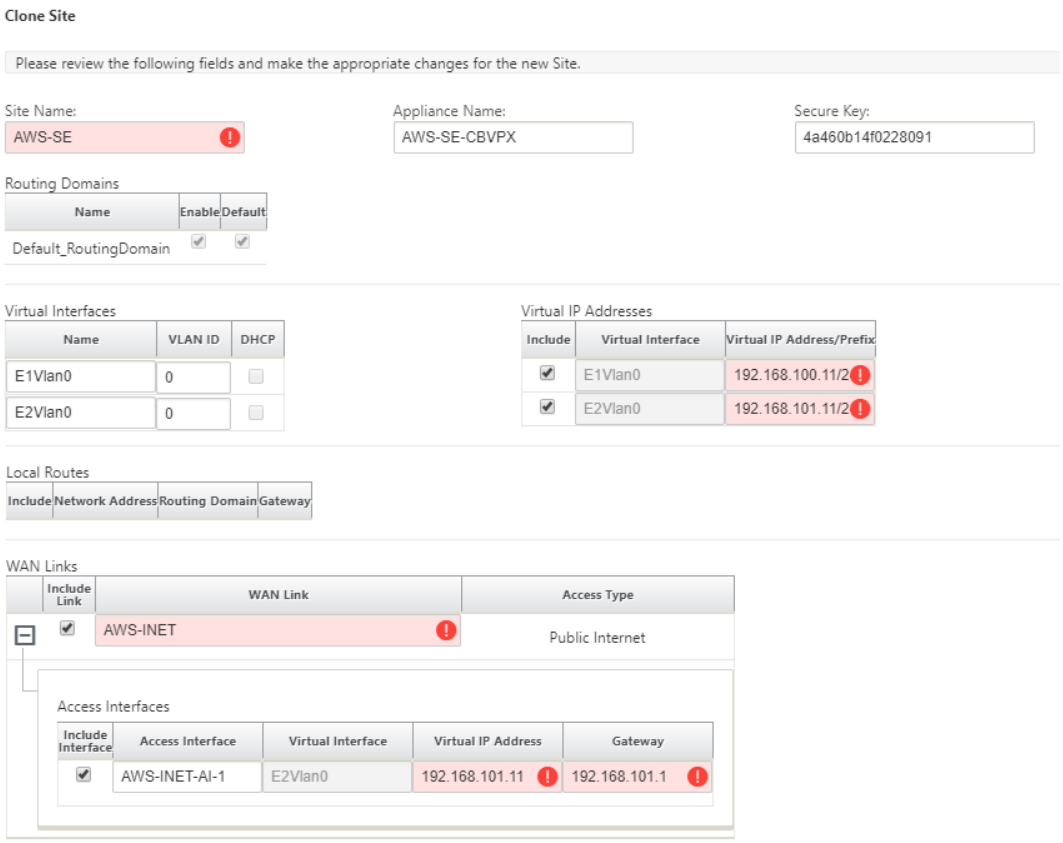
e) Abra el icono Sitios para mostrar los sitios configurados actualmente.

f) Cree rápidamente la configuración para el nuevo sitio en la nube mediante la función de clonación de cualquier sitio existente o cree manualmente un nuevo sitio.

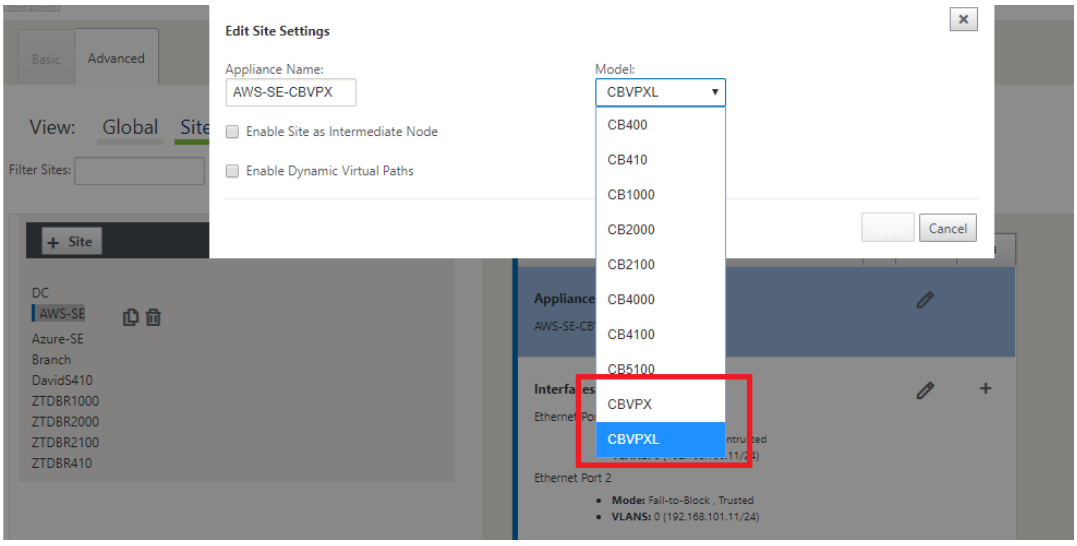


g) Rellene todos los campos requeridos de la topología diseñada anteriormente para este nuevo sitio en la nube

Tenga en cuenta que la plantilla disponible para implementaciones de ZTD en la nube es difícil utilizar la dirección IP #.#.#.11 para las subredes de administración, LAN y WAN.Si la configuración no está configurada para que coincida con la dirección de host IP .11 esperada para cada interfaz, el dispositivo no podrá establecer correctamente ARP a las puertas de enlace del entorno de nube y conectividad IP a la ruta virtual del MCN.

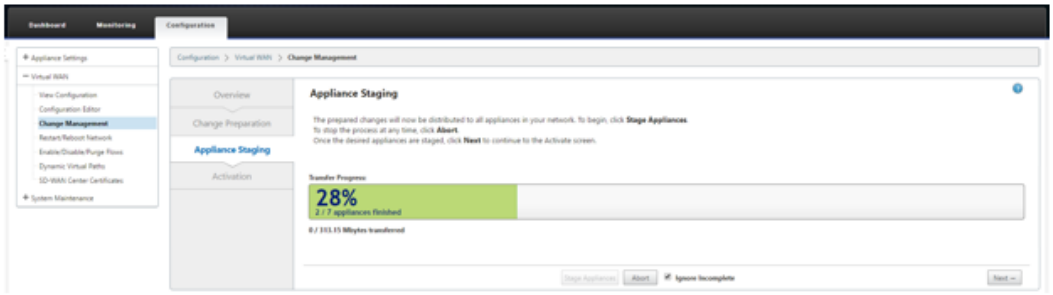


h) Después de clonar un sitio nuevo, desplácese hasta la **Configuración básica** del sitio y verifique que el Modelo de SD-WAN esté seleccionado correctamente, lo que soportaría el servicio Zero Touch.



i) Guarde la nueva configuración en SD-WAN Center y use la exportación a la opción **Bandeja de entrada de administración de cambios** para insertar la configuración mediante Administración de cambios.

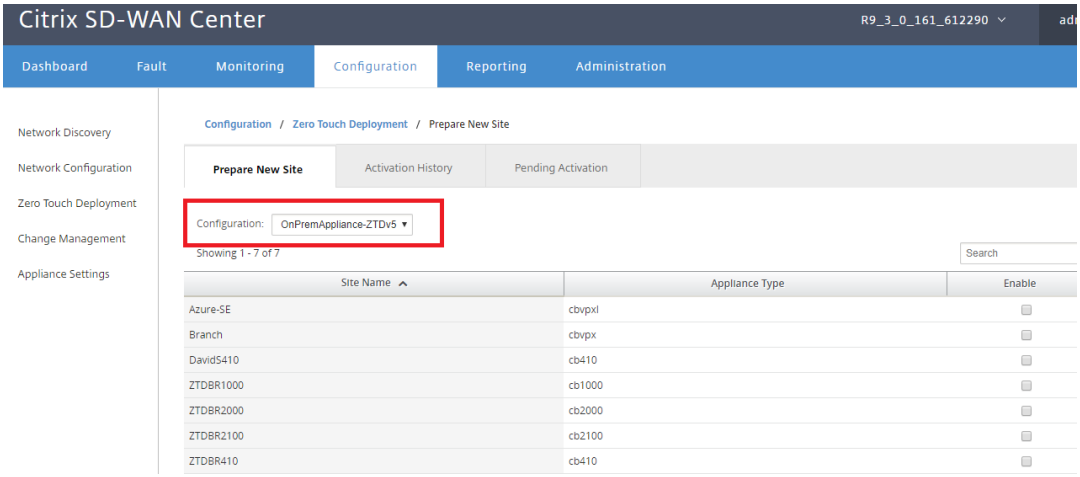
j) Siga el procedimiento de administración de cambios para organizar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar mediante Zero Touch, deberá utilizar la opción *Ignorar incompleto* para omitir el intento de insertar la configuración en el nuevo sitio que todavía necesita pasar por el flujo de trabajo ZTD.



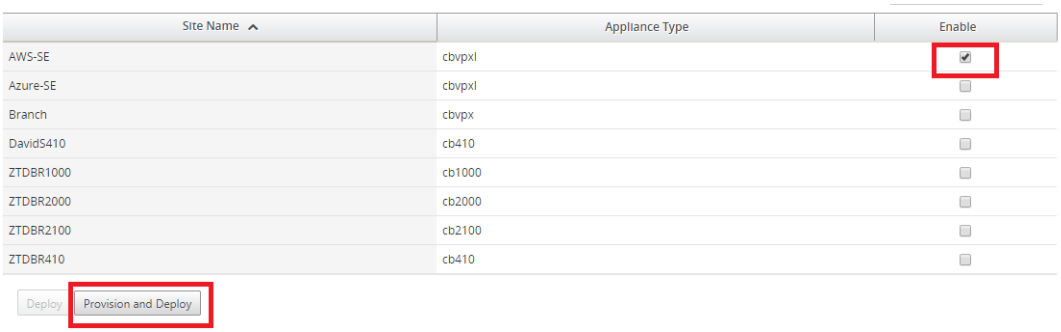
2. Vuelva a la página SD-WAN Center Zero Touch Deployment y, con la nueva configuración activa ejecutándose, el nuevo sitio estará disponible para su implementación.

   a) En la página Deployment Zero Touch, en la ficha **Implementar nuevo sitio**, seleccione el archivo de configuración de red en ejecución.

   b) Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos Citrix SD-WAN no implementados que son compatibles con Zero Touch.

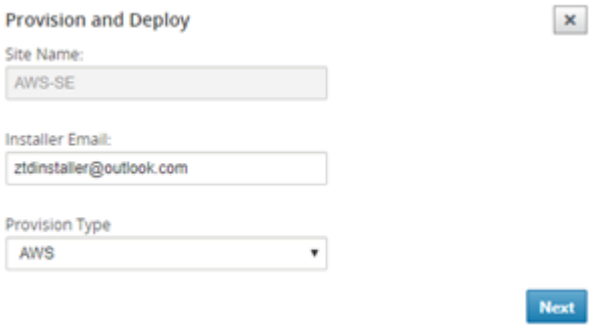


   c) Seleccione el sitio de nube de destino que quiere implementar mediante el servicio Zero Touch, haga clic en **Habilitar**y, a continuación, en **Aprovisionar e implementar**.

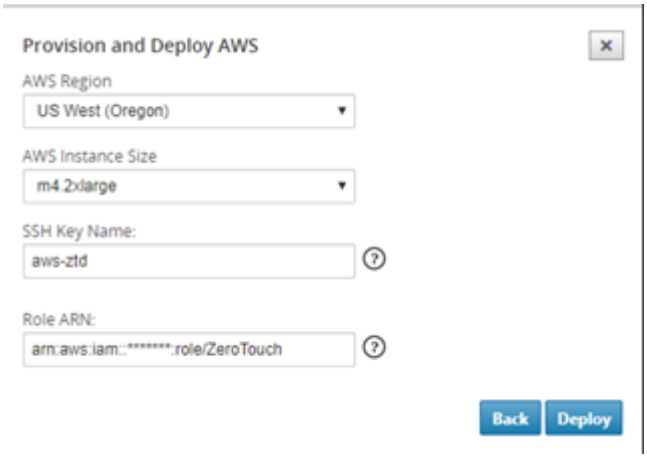


d) Aparecerá una ventana emergente en la que el administrador de Citrix SD-WAN puede iniciar la implementación de Zero Touch.

Rellene una dirección de correo electrónico donde se puede entregar la URL de activación y seleccione el **tipo de provisión** para la nube deseada.



e) Después de hacer clic en **Siguiente**, seleccione la región adecuada, tamaño de instancia, rellene correctamente los campos Nombre de clave SSH y ARN de rol.

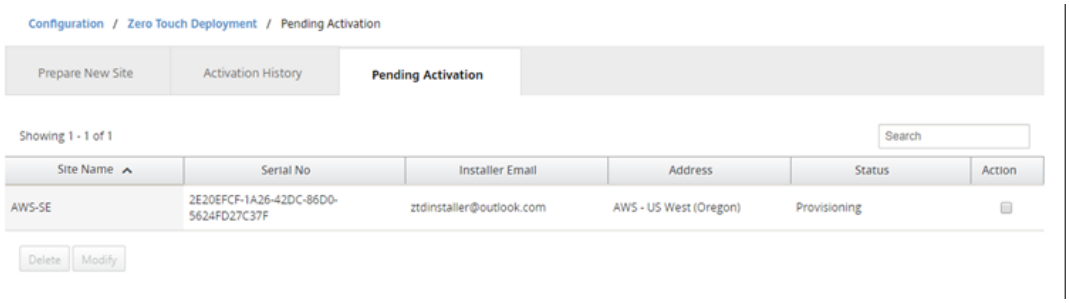


> **Nota**
>
> Utilice los enlaces de ayuda para obtener orientación sobre cómo configurar la clave SSH y el ARN de rol en la cuenta Cloud.Asegúrese también de que la región de selección coincida con lo que está disponible en la cuenta y de que el tamaño de instancia

> seleccionado coincida con VPX o VPXL como el modelo seleccionado en la configuración de SD-WAN.

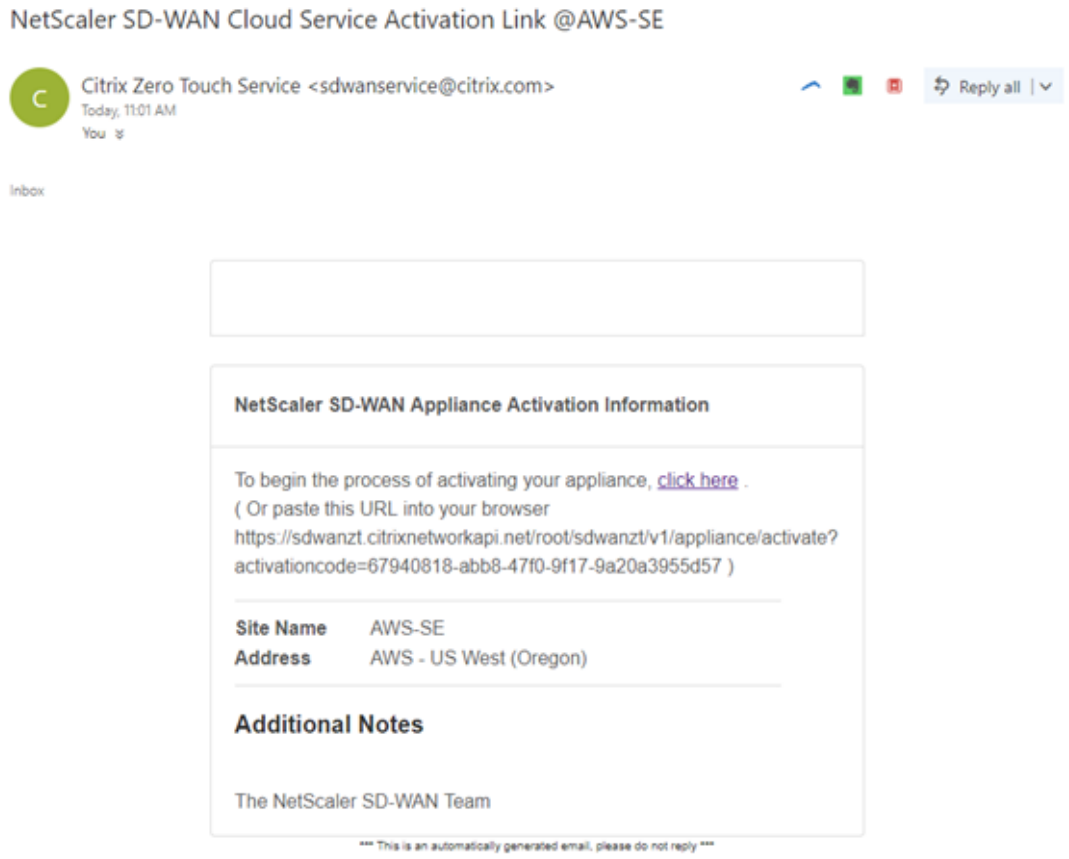
f) Haga clic en **Implementar**, activando el SD-WAN Center, que se había registrado previamente con ZTD Cloud Service, para compartir la configuración de este sitio para que sea temporal almacenada en ZTD Cloud Service.

g) Acceda a la ficha **Activación pendiente** para confirmar que la información del sitio se rellenó correctamente y se puso en un estado de Provisioning.



3. Inicie el proceso de implementación Zero Touch como administrador de la nube.

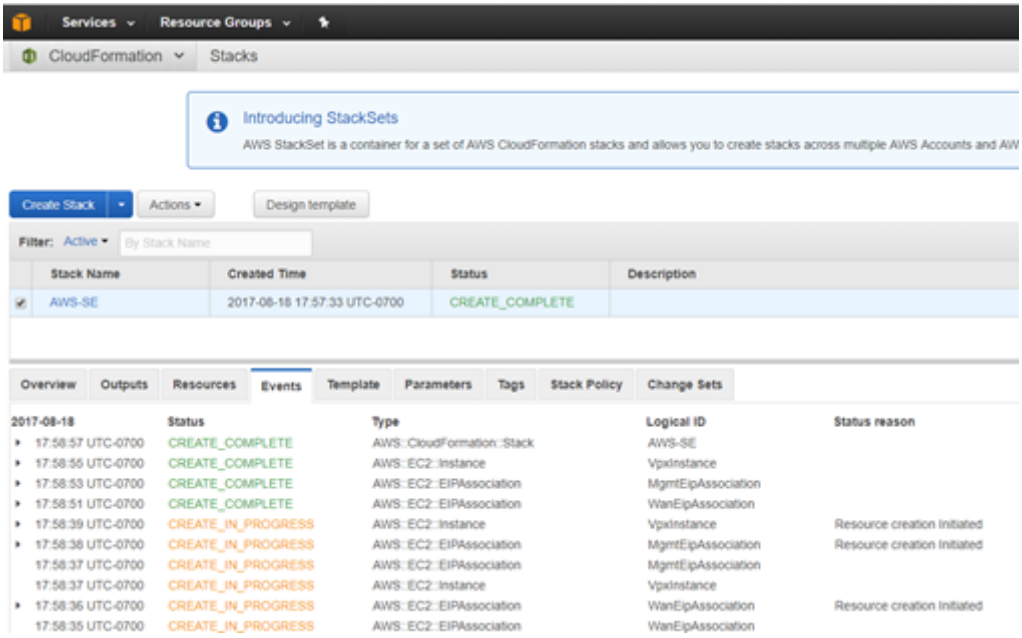
a) El instalador deberá comprobar el buzón de correo de la dirección de correo electrónico que el Administrador de SD-WAN utilizó al implementar el sitio.



b) Abra la URL de activación que se encuentra en el correo electrónico en una ventana del explorador de Internet.

c) Si la clave SSH y el ARN de rol se introducen correctamente, el servicio de implementación Zero Touch comenzará inmediatamente a Provisioning la instancia SD-WAN; de lo contrario, los errores de conexión se mostrarán inmediatamente.

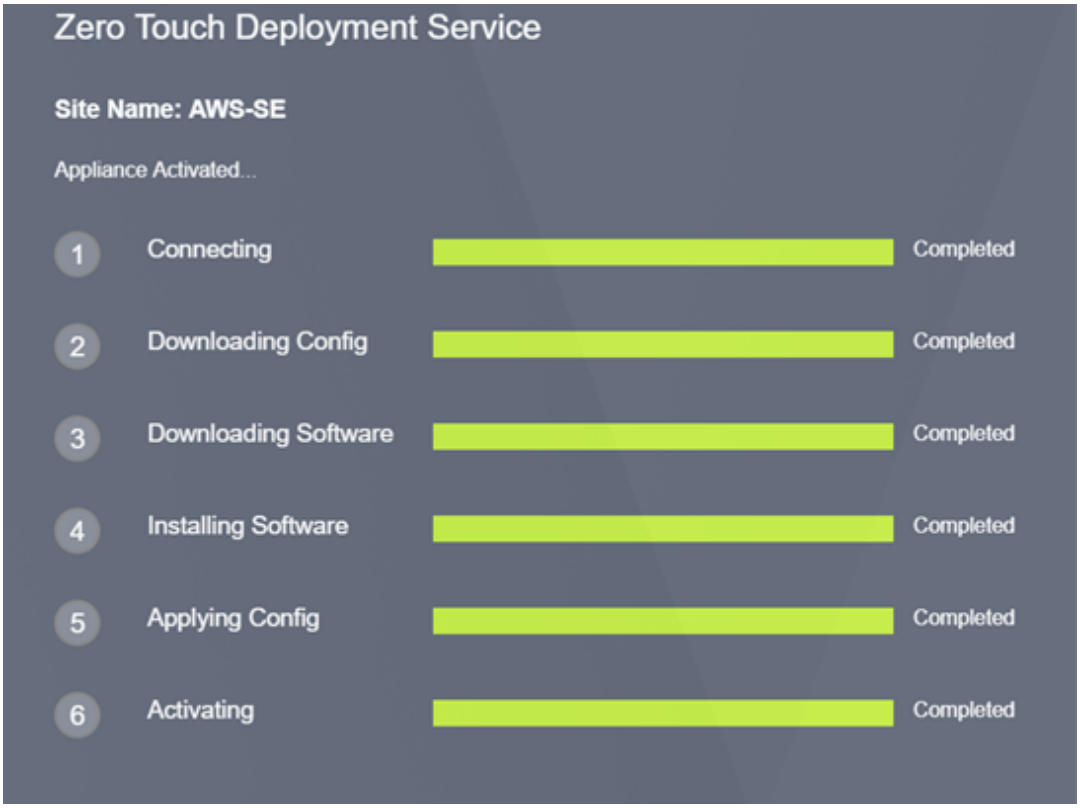
d) Para solucionar problemas adicionales en la consola de AWS, el servicio Cloud Formation se puede utilizar para detectar cualquier evento que se produzca durante el proceso de Provisioning.



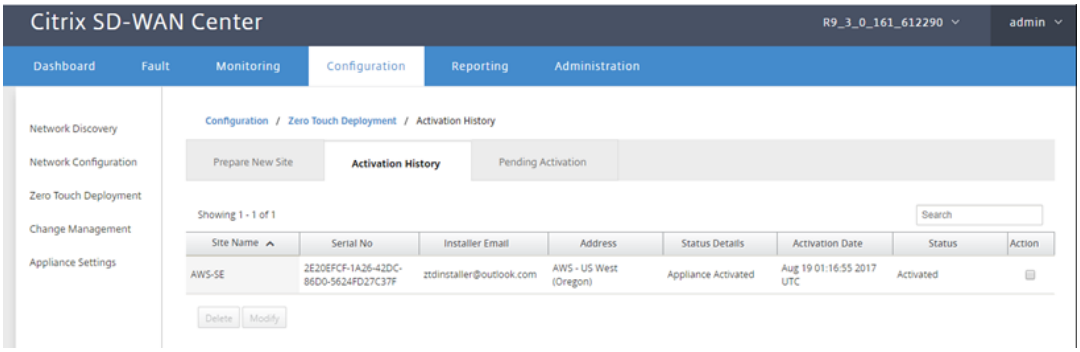
e) Permitir que el proceso de Provisioning entre 8 y 10 minutos y la activación entre 3 y 5 minutos se complete por completo.

f) Con una conectividad correcta de la instancia de nube SD-WAN al servicio de nube ZTD, el servicio realizará automáticamente lo siguiente:

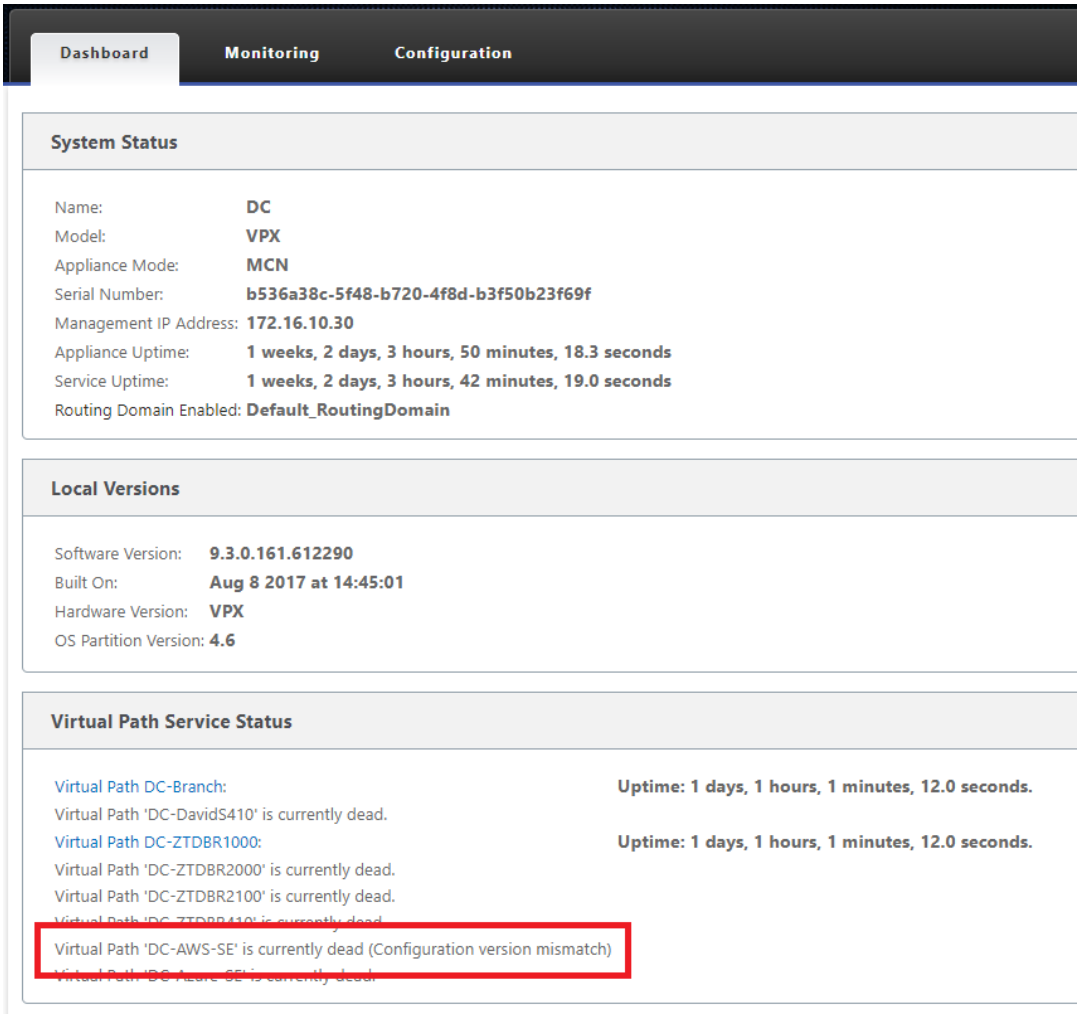
- Descargue el archivo de configuración específico del sitio almacenado anteriormente por SD-WAN Center
- Aplicación de la configuración a la instancia local
- Descargar e instalar un archivo de licencia temporal de 10 MB
- Descargar e instalar cualquier actualización de software si es necesario
- Activar el servicio SD-WAN



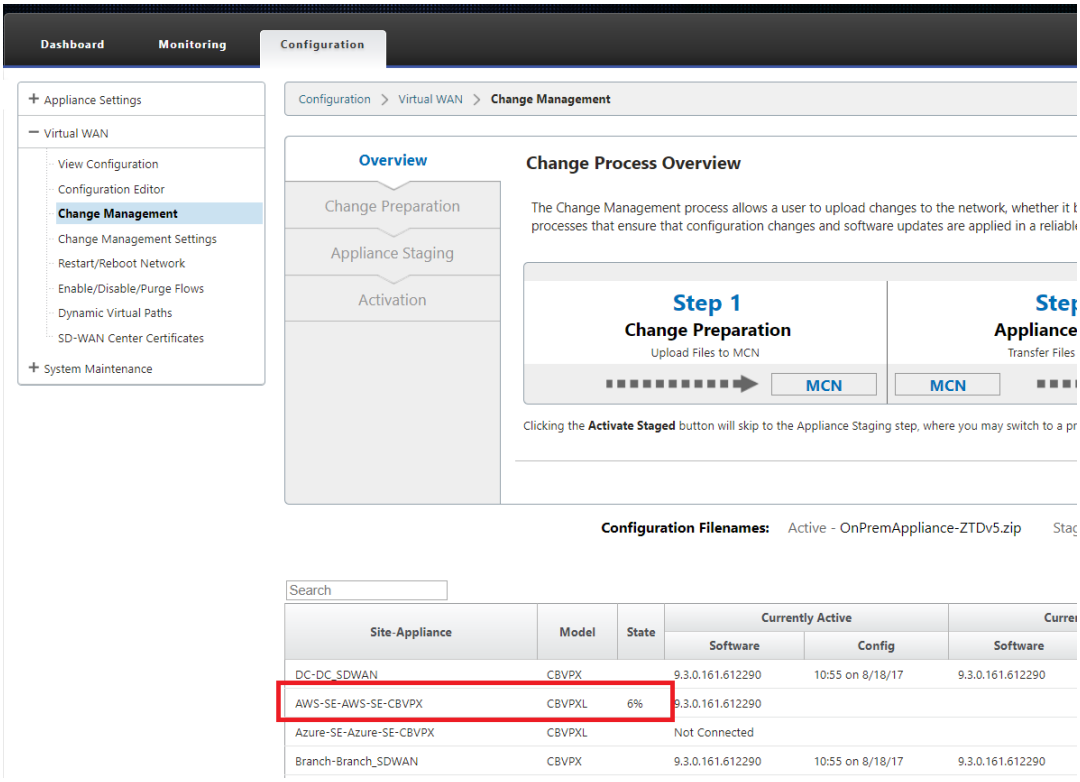
g) Se puede realizar una confirmación adicional en la interfaz de administración web de SD-WAN Center; el menú Deployment Zero Touch mostrará los dispositivos activados correctamente en la ficha **Historial de activación**.



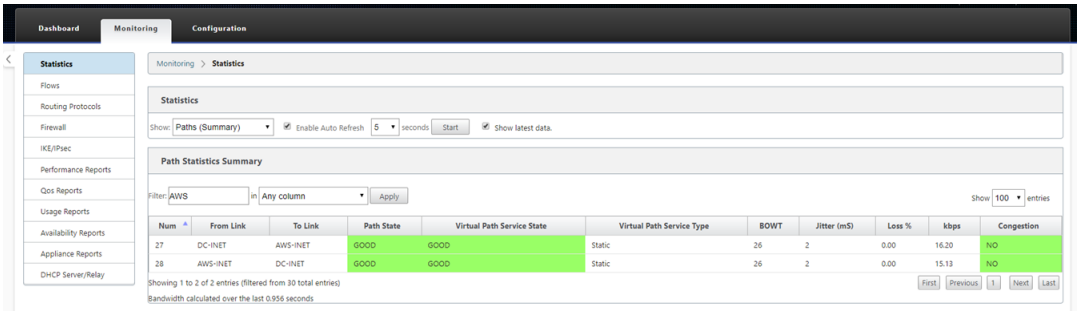
h) Es posible que las rutas virtuales no se muestren inmediatamente en un estado conectado, esto se debe a que el MCN puede no confiar en la configuración transmitida desde ZTD Cloud Service, e informará No*coincide la versión de configuración* en el panel de MCN.



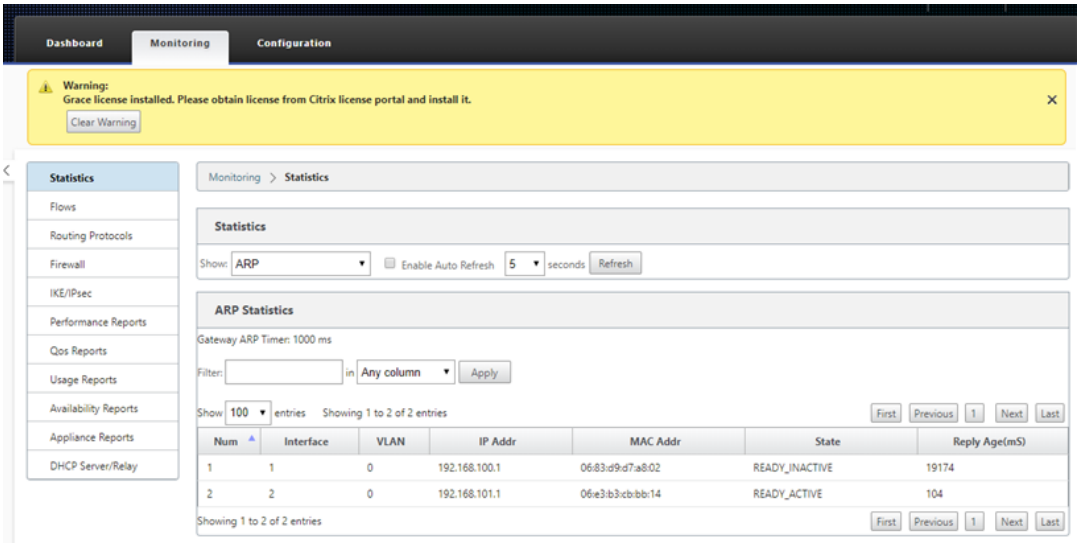
i) La configuración se volverá a entregar automáticamente al dispositivo de sucursal recién instalado, el estado de esto puede ser supervisado en la página **MCN** > **Configuración** > **WAN virtual** > **Administración de cambios** (dependiendo de la conectividad, este puede tardar varios minutos en completarse).



j) El Administrador de SD-WAN puede supervisar la página de administración web de MCN de cabecera para las rutas virtuales establecidas del sitio de nube recién agregado.



k) Si es necesario solucionar problemas, abra la interfaz de usuario de instancias SD-WAN mediante la IP pública asignada por el entorno de nube durante el Provisioning y utilice la tabla ARP de la página **Monitoring** > **Statistics** para identificar cualquier problema relacionado con las puertas de enlace previstas, o utilizan las opciones de ruta de seguimiento y captura de paquetes en diagnósticos.



Azure

April 13, 2021

Con la versión 9.3 de SD-WAN, las capacidades de implementación de Zero Touch se han extendido a las instancias de la nube. El procedimiento para implementar el proceso de implementación de Zero Touch para las instancias en la nube es ligeramente diferente al de la implementación del dispositivo para el servicio táctil cero.

Actualización de la configuración para agregar un nuevo sitio remoto con un dispositivo en la nube SD-WAN compatible con ZTD mediante la configuración de red de SD-WAN Center

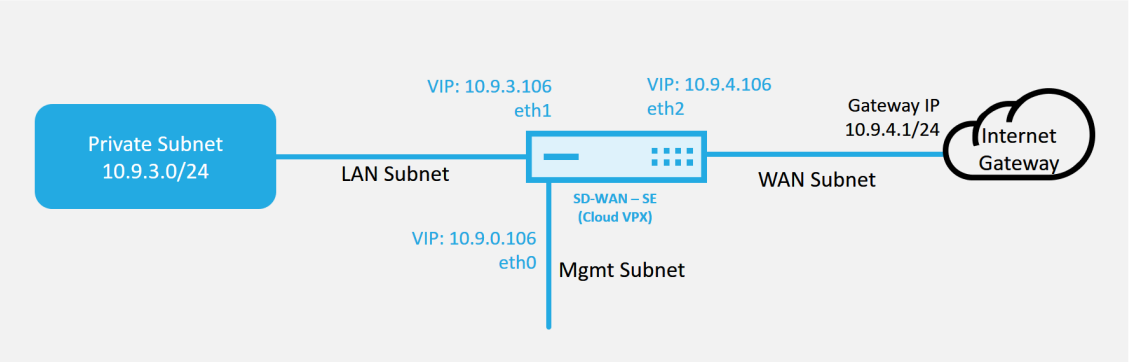
Si la configuración de SD-WAN no se creó mediante la configuración de red de SD-WAN Center, importe la configuración activa desde el MCN y comience a modificar la configuración mediante SD-WAN Center. Para la capacidad de implementación de Zero Touch, el administrador de SD-WAN debe crear la configuración mediante SD-WAN Center. Se debe utilizar el siguiente procedimiento para agregar un nuevo nodo en la nube destinado a la implementación de Zero Touch.

1. Diseñar el nuevo sitio para la implementación en la nube SD-WAN esbozando primero los detalles del nuevo sitio (es decir, tamaño VPX, uso de grupos de interfaz, direcciones IP virtuales, enlaces WAN con ancho de banda y sus respectivas puertas de enlace).

Nota

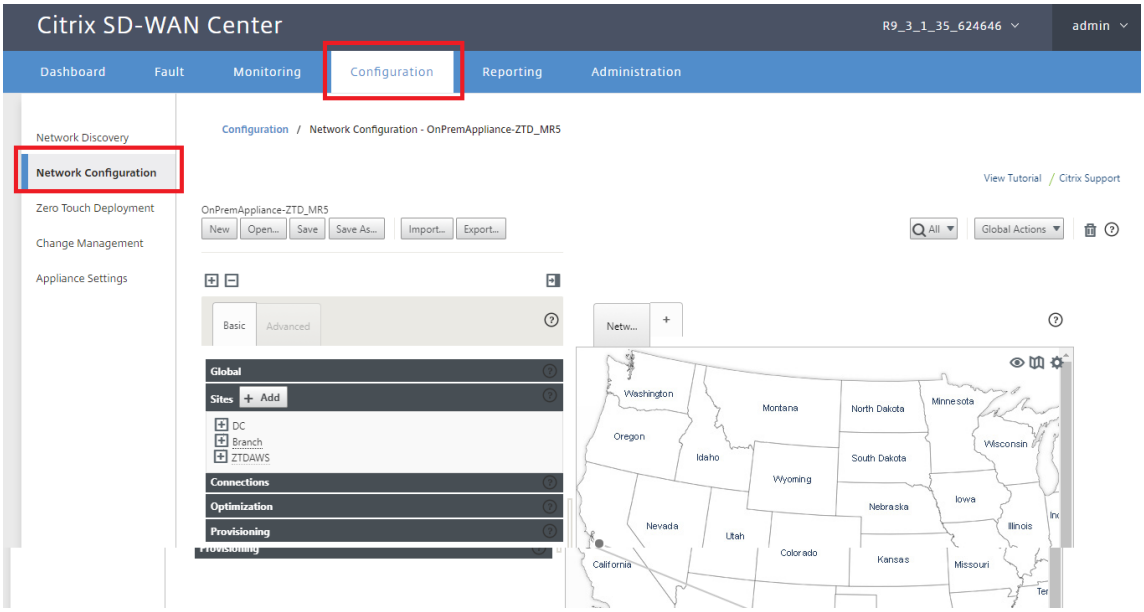
- Las instancias SD-WAN implementadas en la nube deben implementarse en modo Edge/Gateway.
- La plantilla para la instancia en la nube está limitada a tres interfaces: Administración, LAN y WAN (en ese orden).
- Las plantillas disponibles en la nube de Azure para SD-WAN VPX están actualmente configuradas para obtener la IP 10.9.4.106 para la WAN, la IP 10.9.3.106 para la LAN y la IP 10.9.0.16 para la dirección de administración.La configuración de SD-WAN para el nodo de Azure destinado a Zero Touch debe coincidir con este diseño.
- El nombre del sitio de Azure en la configuración debe estar en minúsculas sin caracteres especiales (por ejemplo, ztdazure).

Azure Cloud Topology with NetScaler SD-WAN

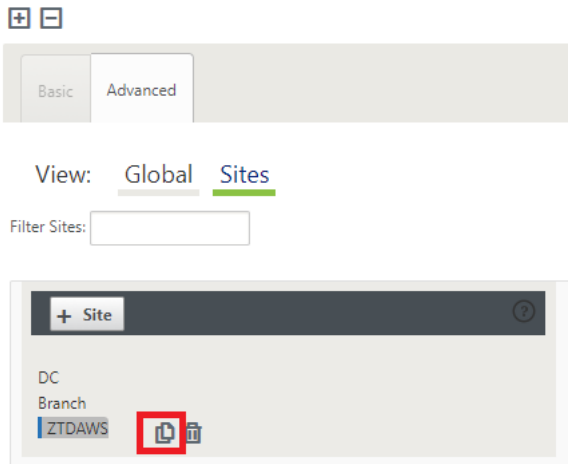


Este es un ejemplo de implementación de un sitio implementado en la nube SD-WAN, el dispositivo Citrix SD-WAN se implementa como el dispositivo perimetral que presta servicio a un único enlace WAN de Internet en esta red en la nube.Los sitios remotos podrán aprovechar varios enlaces WAN de Internet distintos que se conectan a esta misma puerta de enlace de Internet para la nube, proporcionando resiliencia y conectividad de ancho de banda agregada desde cualquier sitio de implementación de SD-WAN a la infraestructura de la nube.Esto proporciona conectividad rentable y altamente confiable a la nube.

2. Abra la interfaz de administración web de SD-WAN Center y vaya a la página **Configuración** > **Configuración de red**.



3. Asegúrese de que ya hay una configuración en funcionamiento o importe la configuración desde el MCN.
4. Acceda a la ficha Básico para crear un nuevo sitio.
5. Abra el icono Sitios para mostrar los sitios configurados actualmente.
6. Cree rápidamente la configuración para el nuevo sitio en la nube mediante la función de clonación de cualquier sitio existente o cree manualmente un nuevo sitio.

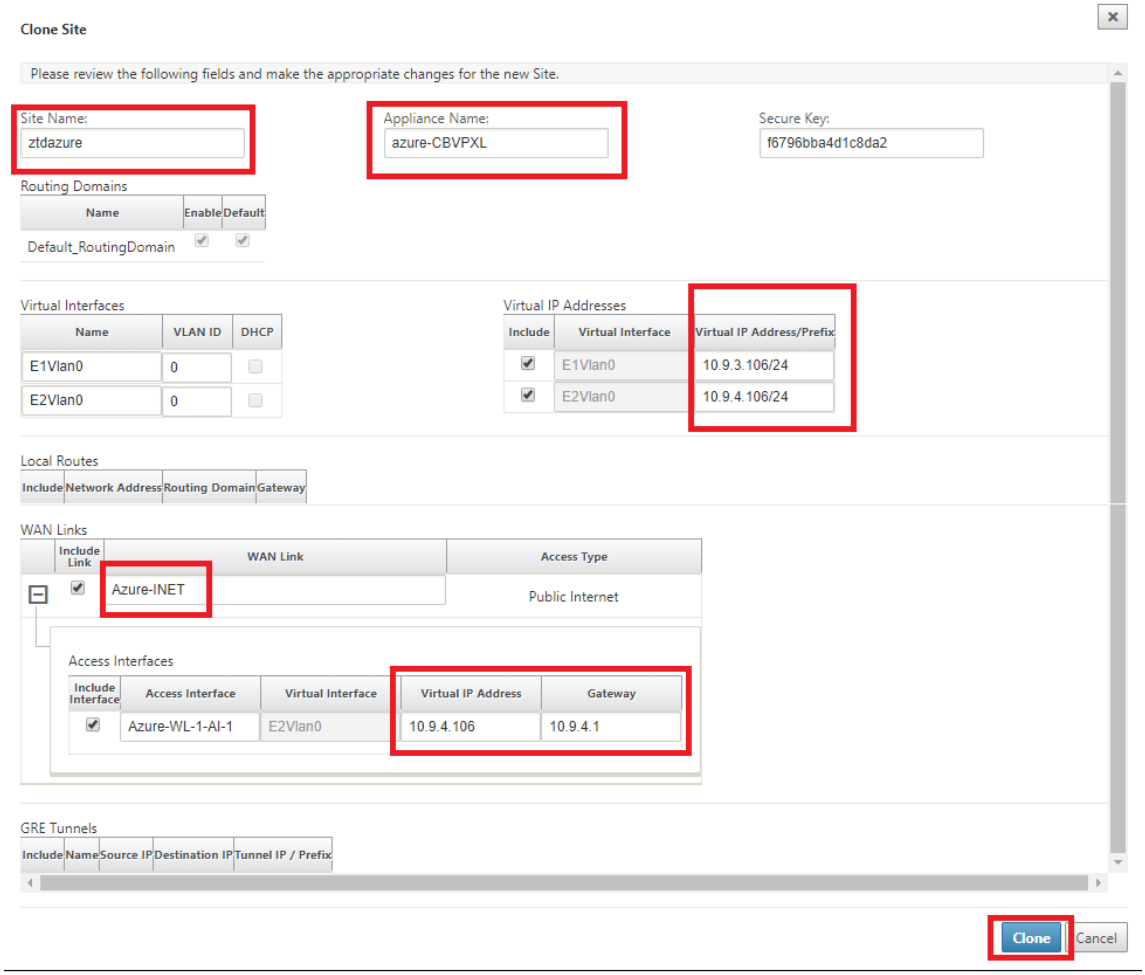


7. Rellene todos los campos necesarios de la topología diseñada anteriormente para este nuevo sitio en la nube.

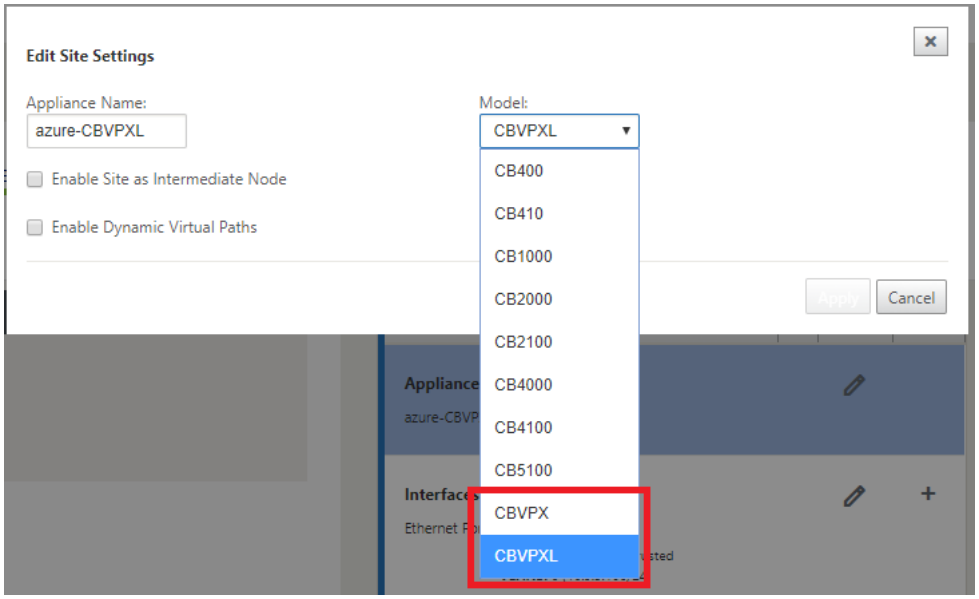
   Tenga en cuenta que la plantilla disponible para las implementaciones de ZTD en la nube de Azure está actualmente configurada para obtener la IP 10.9.4.106 para la WAN, la IP 10.9.3.106 para la LAN y la IP 10.9.0.16 para la dirección de administración. Si la configuración no está definida para que coincida con la dirección VIP esperada para cada interfaz, el dispositivo no

podrá establecer correctamente ARP en las puertas de enlace del entorno de nube y conectividad IP con la ruta virtual del MCN.

Es importar que el nombre del sitio sea compatible con lo que Azure espera.El nombre del sitio debe estar en minúsculas, al menos 6 caracteres, sin caracteres especiales, debe confirmar a la siguiente expresión regular **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $.**

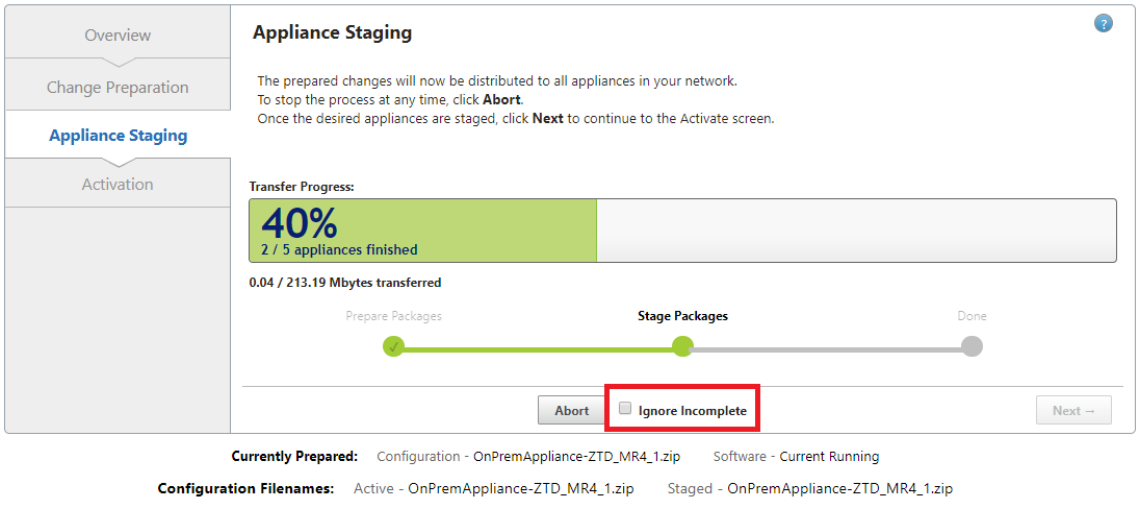


8. Después de clonar un sitio nuevo, desplácese hasta la **Configuración básica** del sitio y verifique que el Modelo de SD-WAN esté seleccionado correctamente, lo que soportaría el servicio Zero Touch.



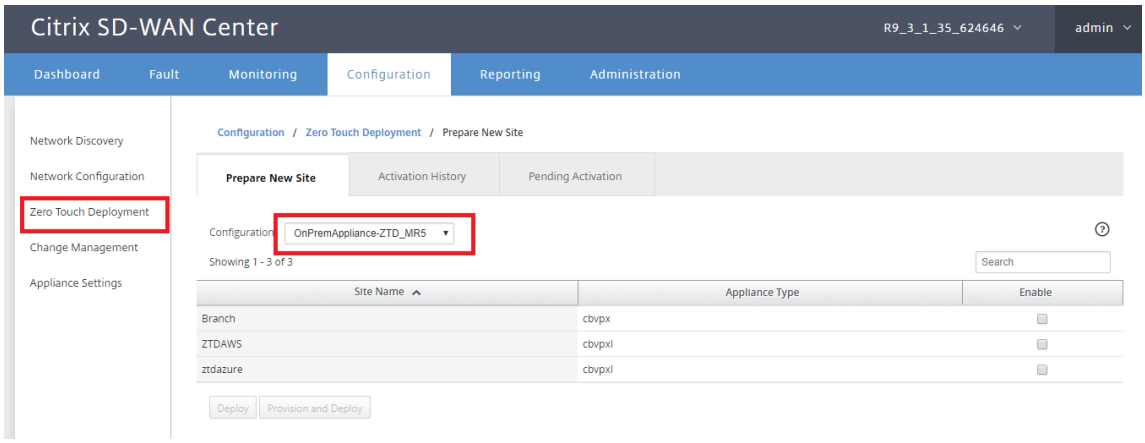
9. Guarde la nueva configuración en SD-WAN Center y use la exportación a la opción **Bandeja de entrada de administración de cambios** para insertar la configuración mediante Administración de cambios.

10. Siga el procedimiento de administración de cambios para organizar correctamente la nueva configuración, lo que hace que los dispositivos SD-WAN existentes conozcan el nuevo sitio que se va a implementar mediante Zero Touch, deberá utilizar la opción *Ignorar incompleto* para omitir el intento de insertar la configuración en el nuevo sitio que todavía necesita pasar por el flujo de trabajo ZTD.

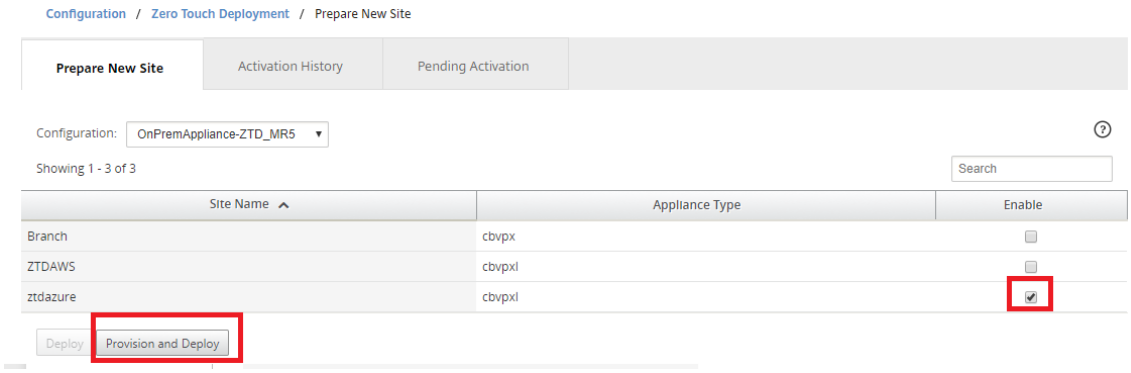


Vaya a la página de implementación de Zero Touch de SD-WAN Center y, con la nueva configuración activa en ejecución, el nuevo sitio estará disponible para SD-WAN Center Provision and Deploy Azure (paso 1 de 2)

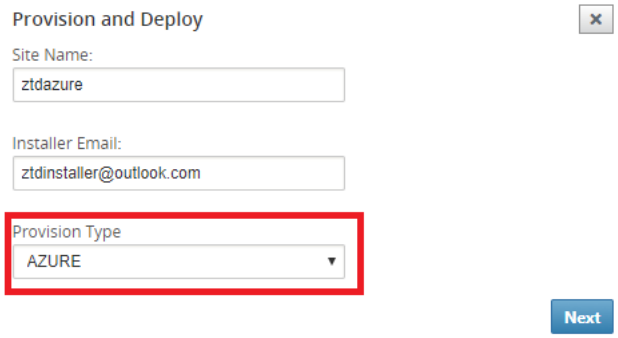
1. En la página Deployment Zero Touch, inicie sesión con las credenciales de su cuenta de Citrix. En la ficha **Implementar nuevo sitio**, seleccione el archivo de configuración de red en ejecución.
2. Después de seleccionar el archivo de configuración en ejecución, se mostrará la lista de todos los sitios de sucursales con dispositivos Citrix SD-WAN compatibles con ZTD.



3. Seleccione el sitio de nube de destino que desea implementar mediante el servicio Zero Touch, haga clic en**Habilitar**y, a continuación, haga clic en **Aprovisionar e implementar**.

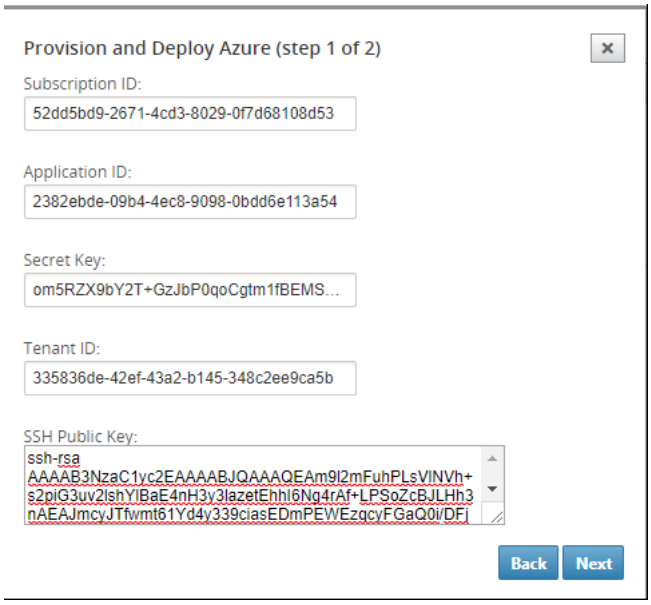


4. Aparecerá una ventana emergente en la que el administrador de Citrix SD-WAN puede iniciar la implementación de Zero Touch. Valide que el nombre del sitio cumpla con los requisitos de Azure (minúsculas sin caracteres especiales). Rellene una dirección de correo electrónico en la que se pueda entregar la URL de activación y seleccione Azure como **Tipo de aprovisionamiento** para la nube deseada, antes de hacer clic en **Siguiente**.

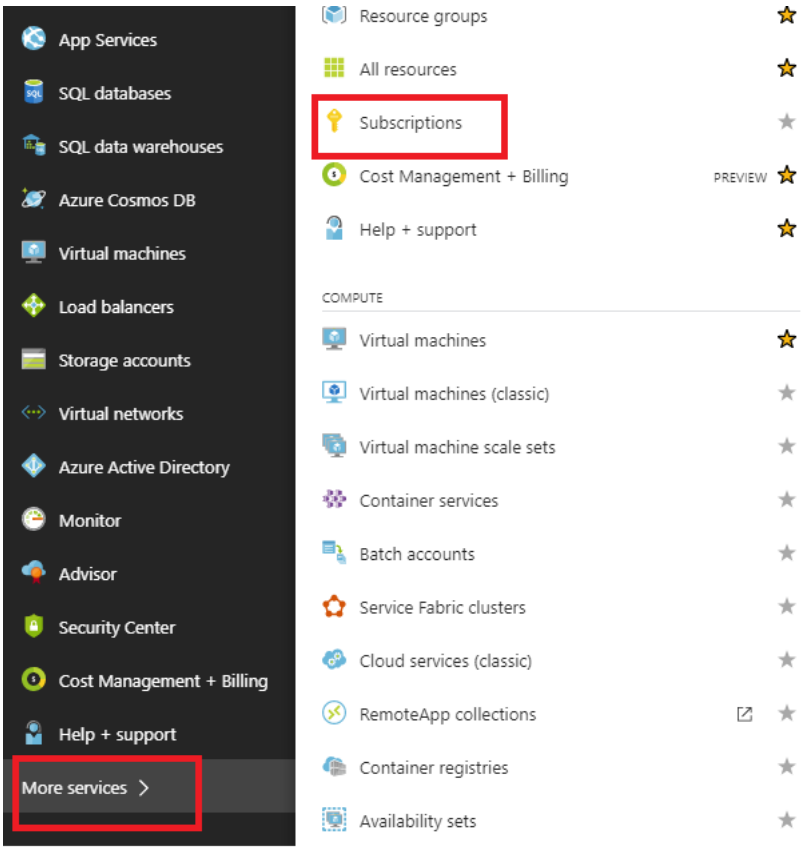


5. Después de hacer clic en **Siguiente**, la ventana Aprovisionar e implementar Azure (paso 1 de 2) requerirá la entrada de obtenida de la cuenta de Azure.

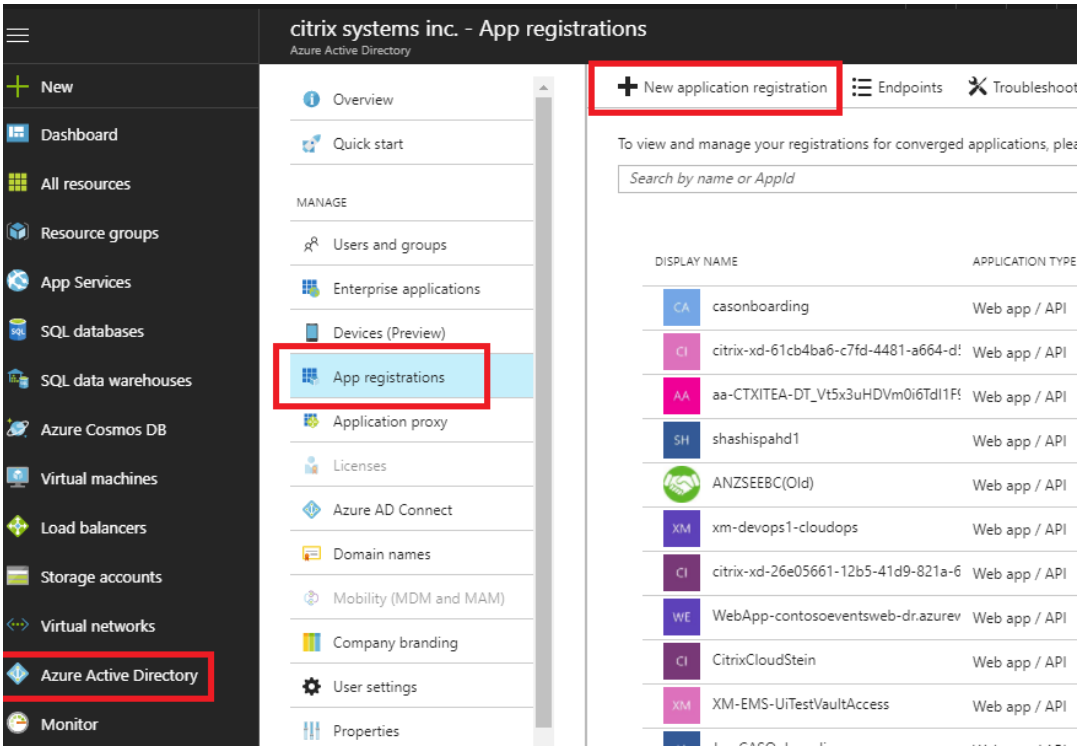
   Copie y pegue cada campo requerido después de obtener la información de su cuenta de Azure.En los pasos siguientes se describe cómo obtener el ID de suscripción, el ID de aplicación, la clave secreta y el ID de arrendatario necesarios desde su cuenta de Azure y, a continuación, haga clic en **Siguiente**.



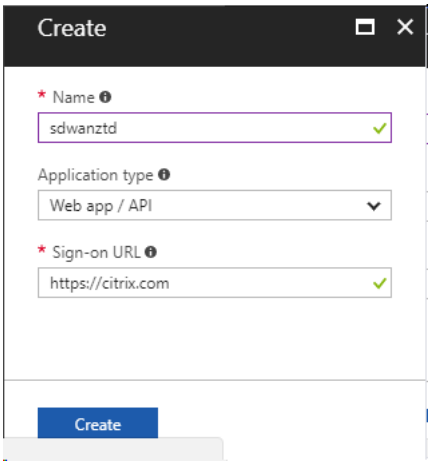
   a) En la cuenta de Azure, podemos identificar el ***ID de suscripción*** requerido navegando a "Más servicios"y seleccionar **Suscripciones.**



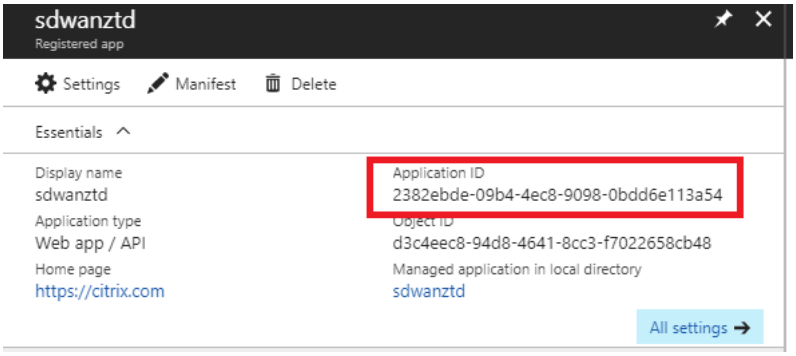
b) Para identificar el ***ID de aplicación***necesario, vaya a Azure Active Directory, Registros de aplicaciones y haga clic en N**nuevo registro de aplicaciones.**



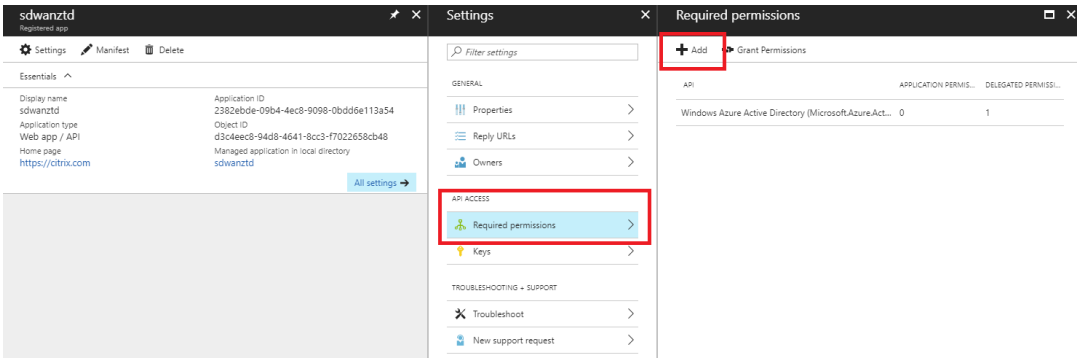
c) En el menú Crear registro de aplicaciones, introduzca un nombre y una URL de inicio de sesión (puede ser cualquier URL, el único requisito es que debe ser válida) y, a continuación, haga clic en **Crear**.



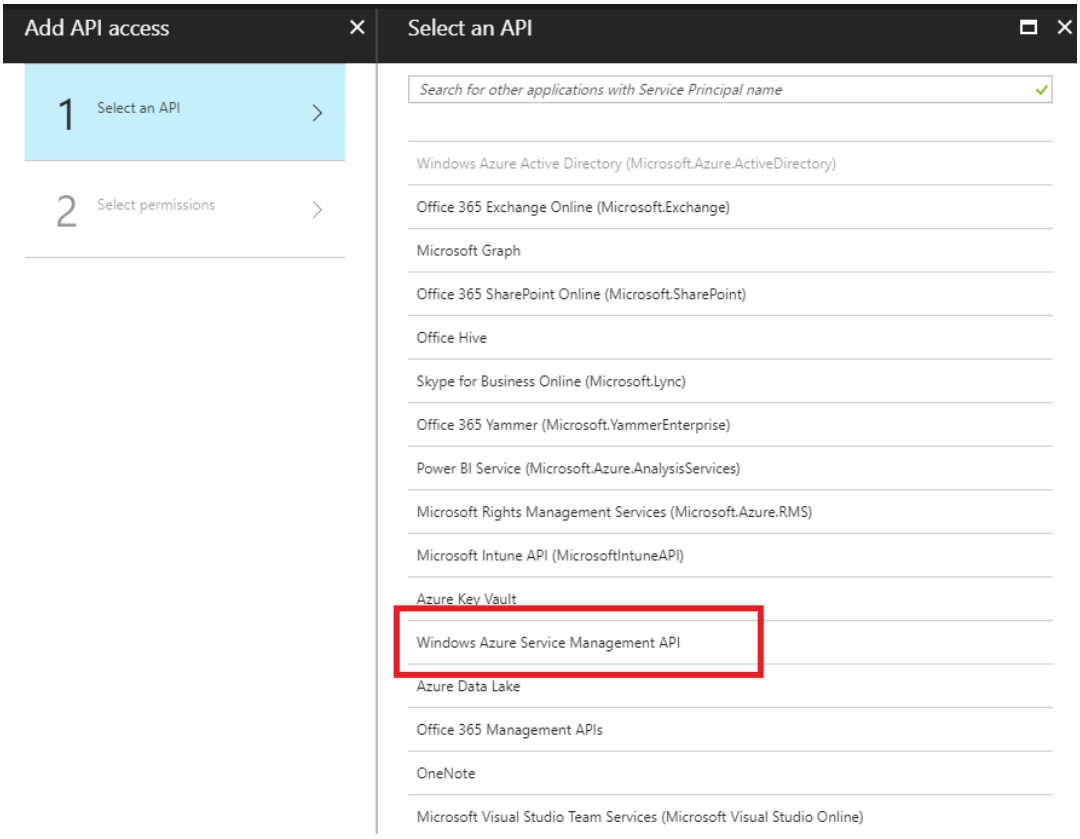
d) Busque y abra la aplicación registrada recién creada y anote el ID de aplicación.



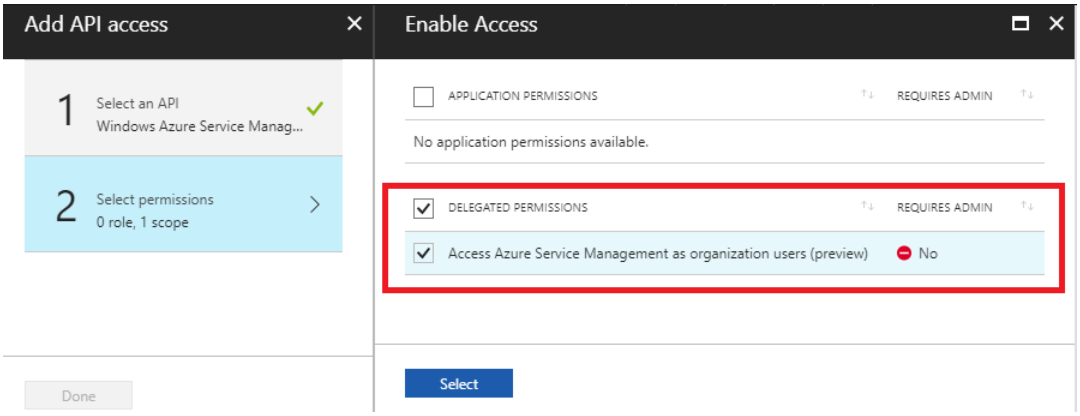
e) Vuelva a abrir la aplicación de registro recién creada e identificar la *clave de seguridad*requerida, en Acceso a API, seleccione **Permisos requeridos**, para permitir que un tercero aprovisionamiento e instancia. A continuación, seleccione **Agregar**.



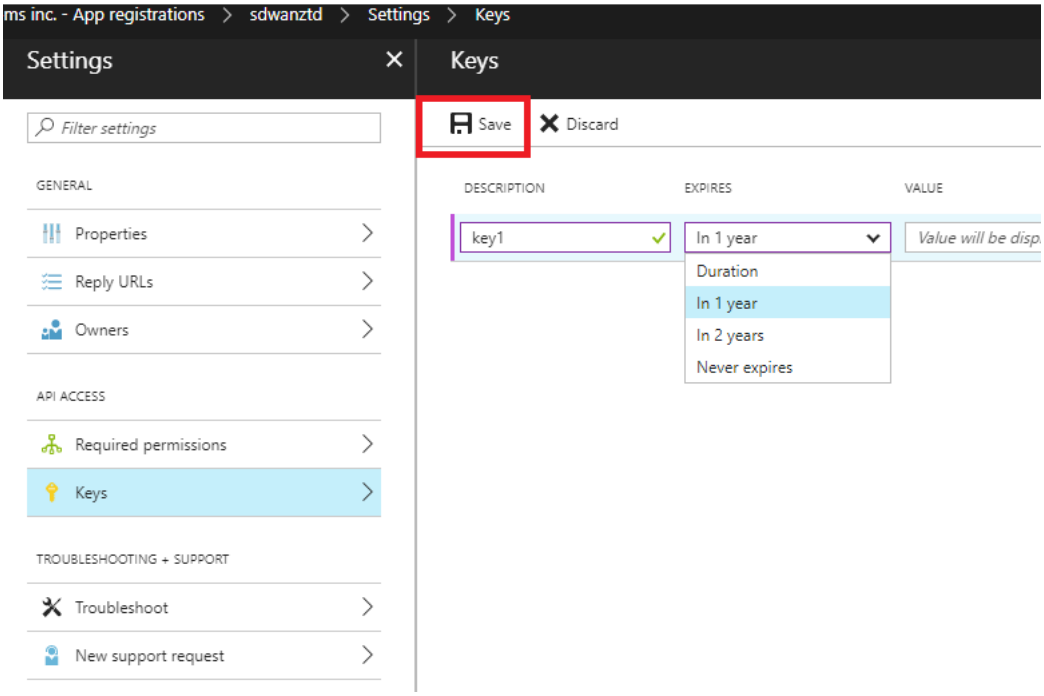
f) Al agregar los permisos necesarios, **seleccione una API y, a continuación,** resalte la **API de administración de servicios de Windows Azure.**



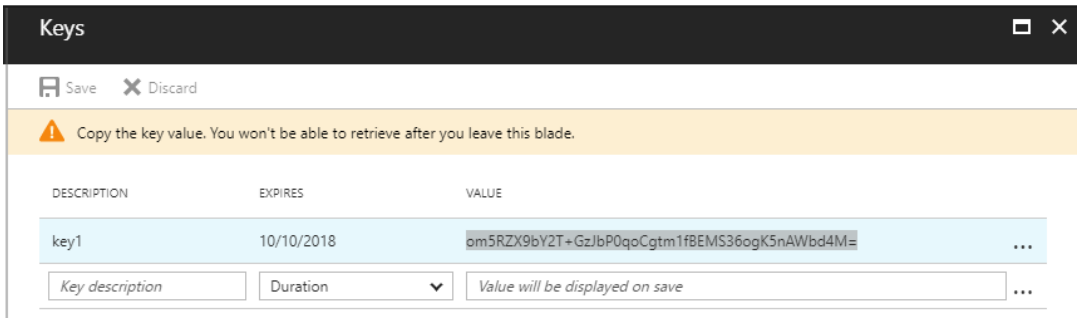
g) Active **Delegate Permissions** para aprovisionar instancias y, a continuación, haga clic en **Seleccionar** y **Terminar**.



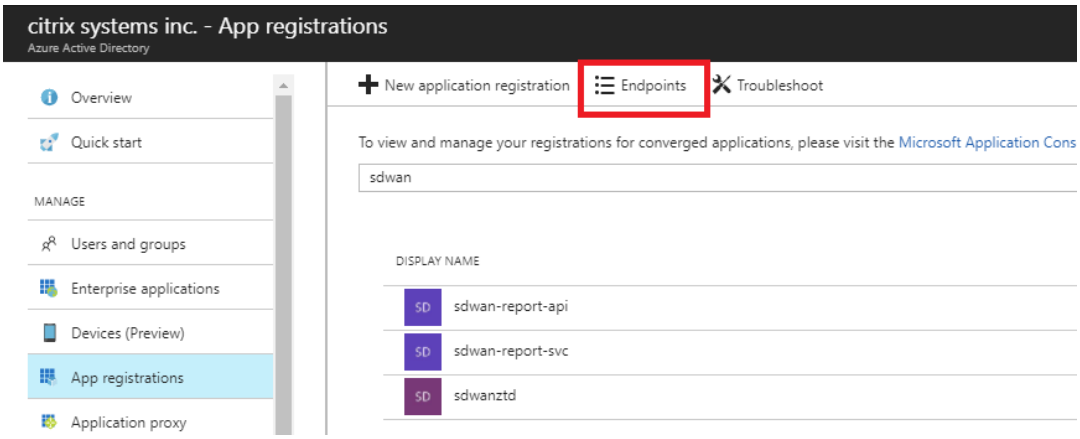
h) Para esta aplicación registrada, en Acceso API, seleccione **Claves** y cree una **descripción de clave** secreta y la **duración** deseada para que la clave sea válida.A continuación, haga clic en **Guardar**, **que** producirá una **clave secreta** (la clave solo es necesaria para el proceso de Provisioning, se puede eliminar después de que la instancia esté disponible).



i) Copie y guarde la clave secreta (tenga en cuenta que no podrá recuperarla más adelante).

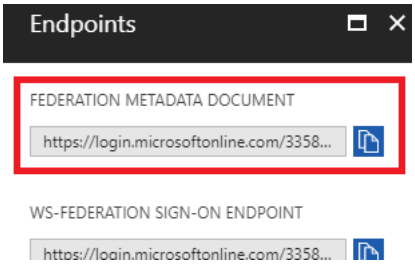


j) Para identificar el **ID de arrendatario** requerido, vuelva al panel de registro de la aplicación y seleccione **Puntos finales**.

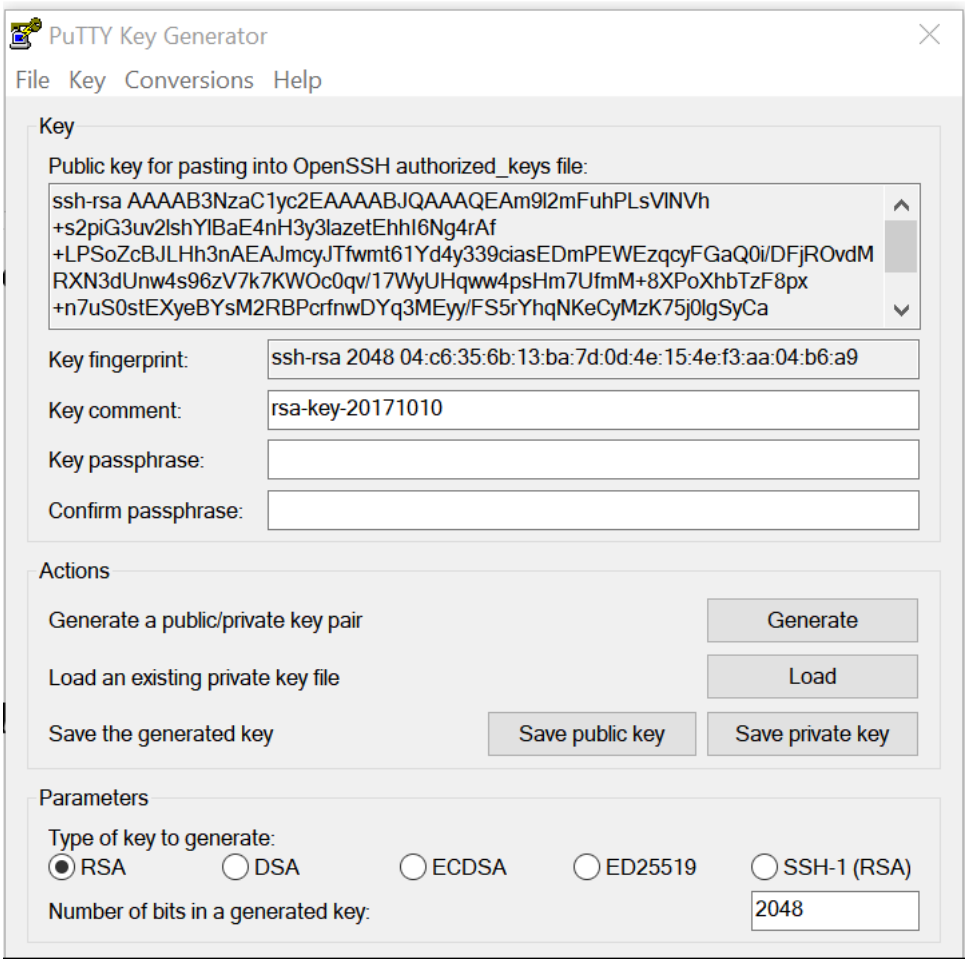


k) Copie el **documento de metadatos de federación** para identificar su ID de arrendatario

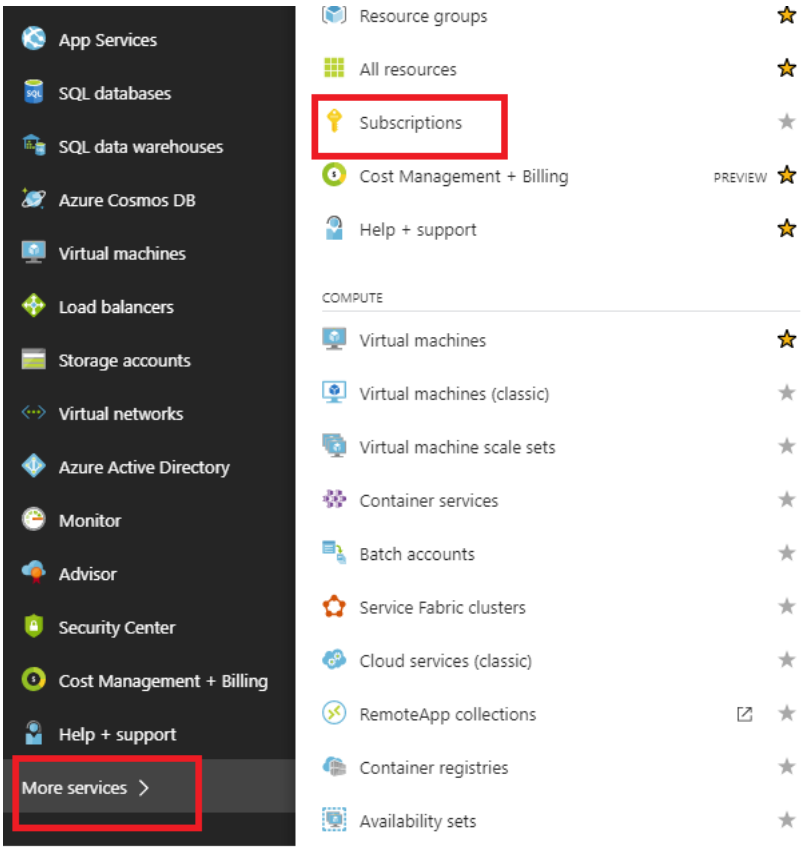
(tenga en cuenta que el ID de arrendatario es una cadena de 36 caracteres situada entre "online.com/"y "/federation"en la URL).



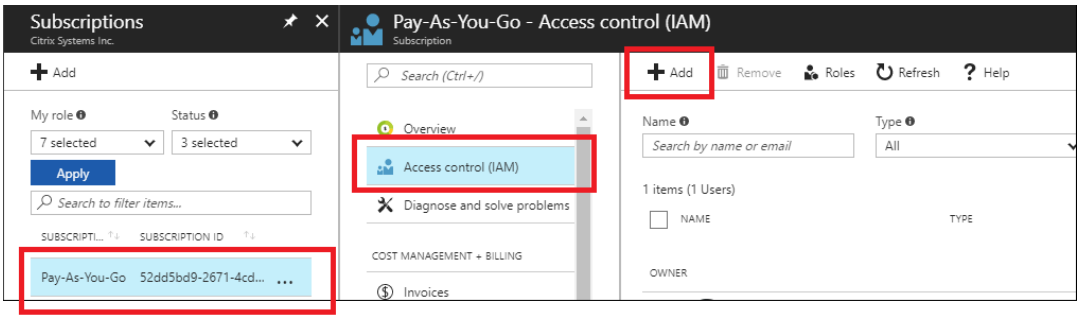
l) El último elemento requerido es la ***clave pública SSH***.Esto se puede crear mediante Putty Key Generator o ssh-keygen y se utilizará para la autenticación, eliminando la necesidad de contraseñas para iniciar sesión.La clave pública SSH se puede copiar (incluidos el encabezado ssh-rsa y las cadenas de clave rsa finales).Esta clave pública se compartirá a través de la entrada de SD-WAN Center en Citrix Zero Touch Deployment Service.



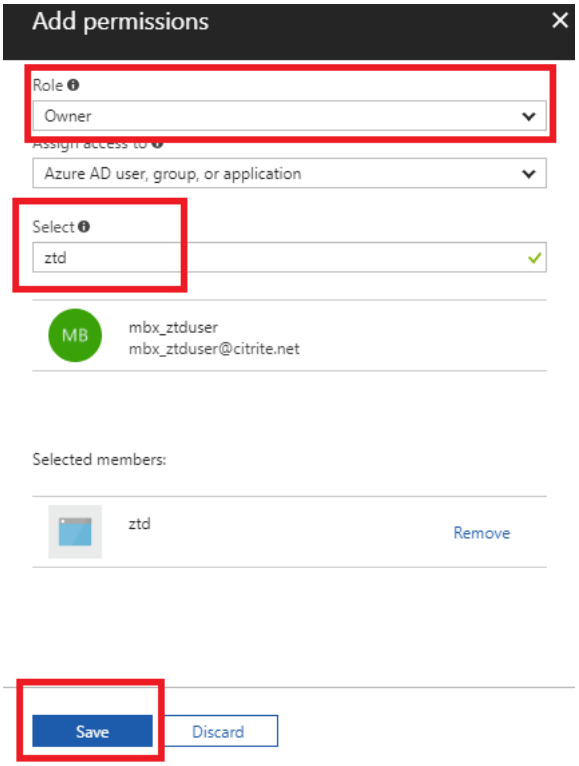
m) Se requieren pasos adicionales para asignar a la aplicación un rol.Vuelva a Más servicios y, a continuación, a Suscripciones.



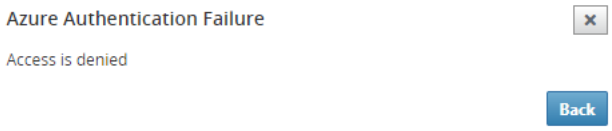
n) Seleccione la suscripción activa, luego **Control de acceso (AIM)**y, a continuación, haga clic en **Agregar.**



o) En el panel de agregar permisos, seleccione el rol "**Propietario**", asigne acceso a **"Usuario, grupo o aplicación de Azure AD"**y busque la aplicación registrada en el **campo Seleccionar**para permitir que el servicio de nube de implementación de Zero Touch cree y configure la instancia en Azure suscripción.Una vez identificada la aplicación, selecciónela y asegúrese de que se rellena como miembro seleccionado antes de hacer clic en **Guardar**.

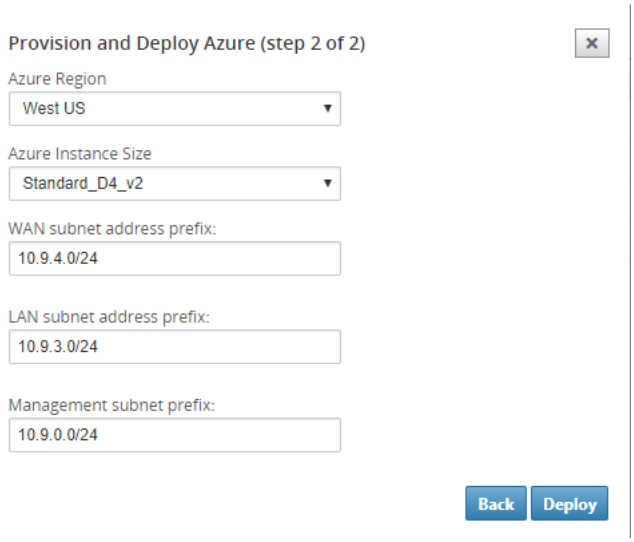


p) Después de recopilar las entradas necesarias e introducirlas en SD-WAN Center, haga clic en **Siguiente**.Si las entradas no son correctas, se producirá un error de autenticación.

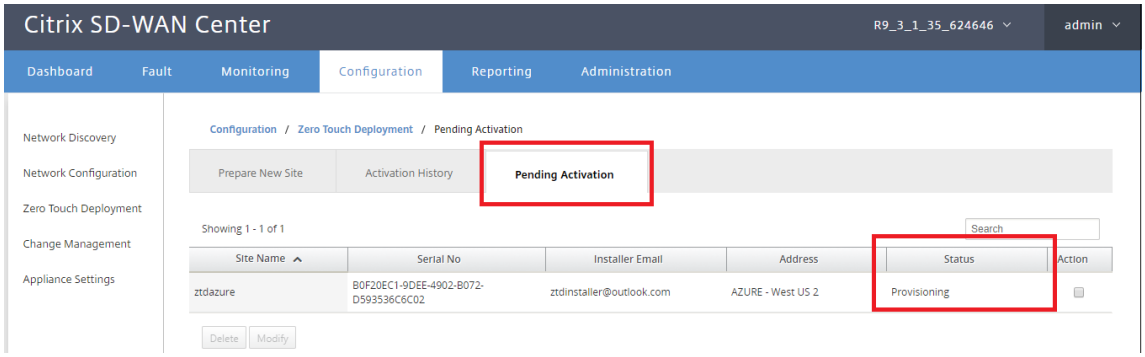


Aprovisionamiento e implementación de Azure del centro de SD-WAN (paso 2 de 2)

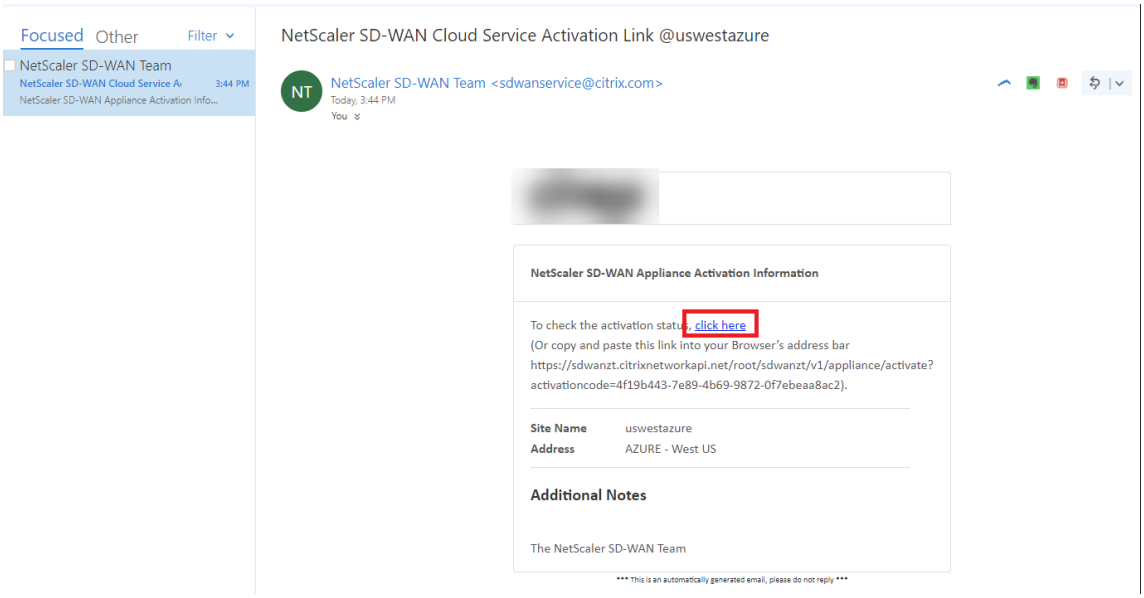
1. Una vez que la autenticación de Azure se haya realizado correctamente, rellene los campos apropiados para seleccionar la región de Azure deseada y el tamaño de instancia adecuado y, a continuación, haga clic en **Implementar**.



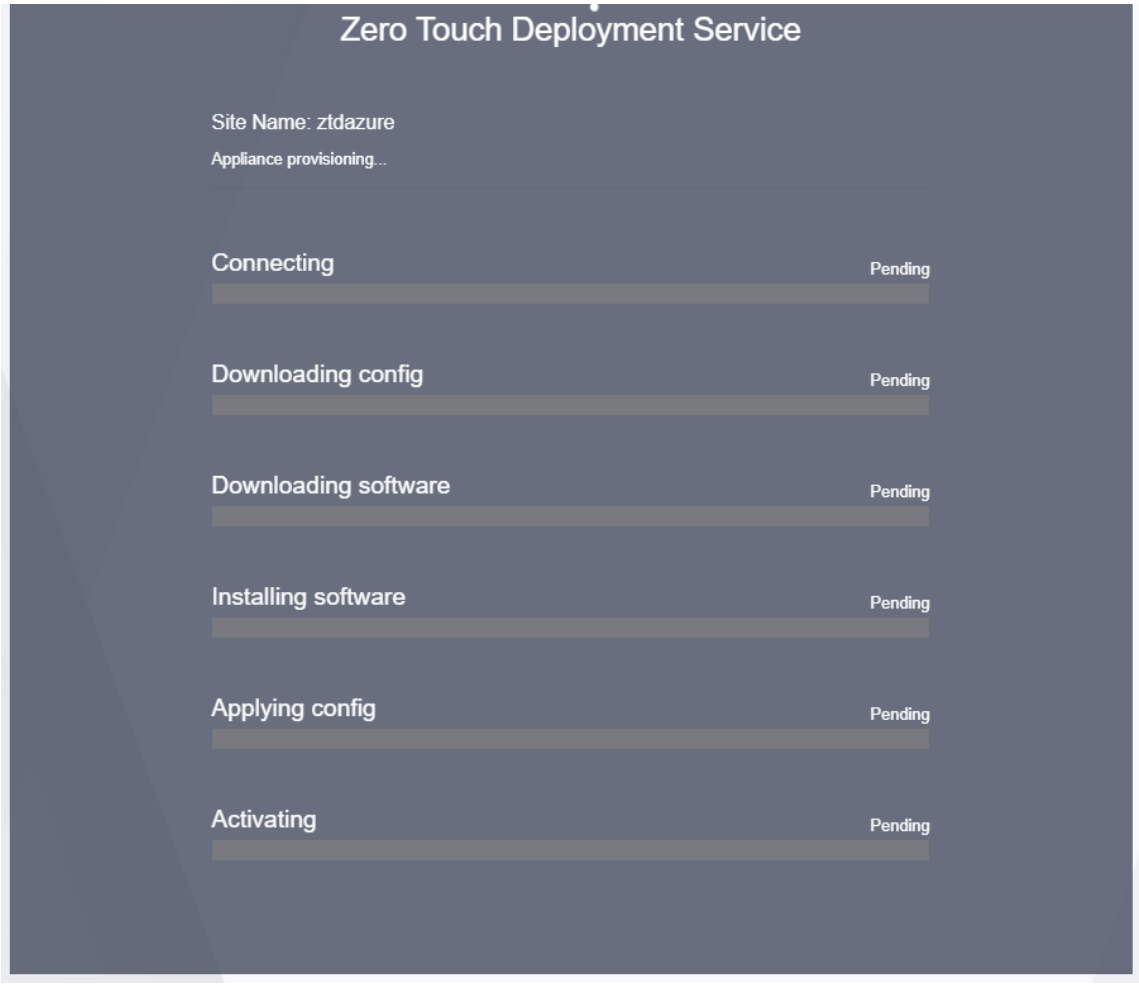
2. Si se desplaza a la ficha **Activación pendiente** en SD-WAN Center, podrá realizar un seguimiento del estado actual de la implementación.



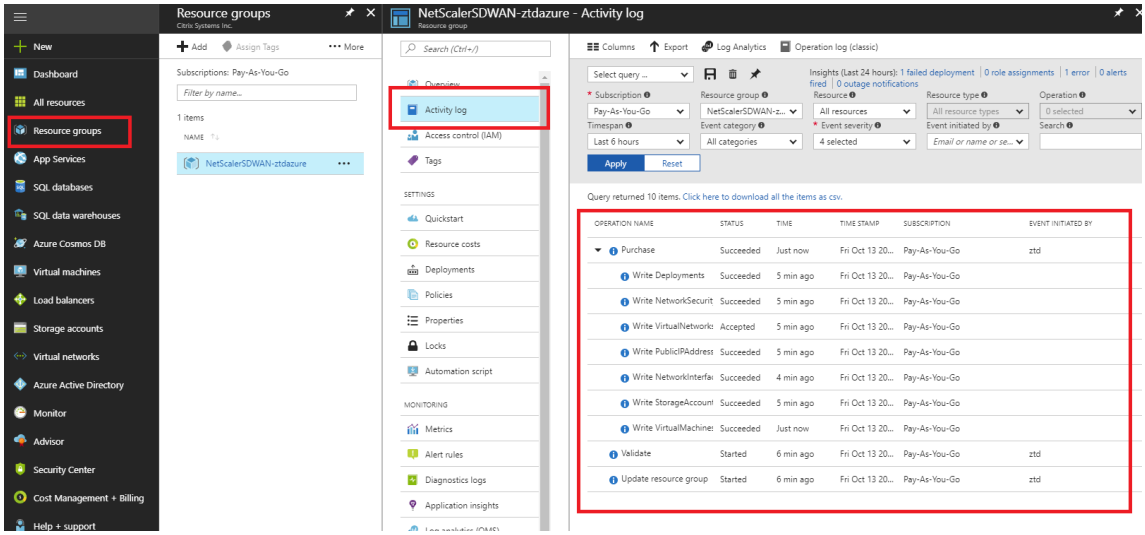
3. Un correo electrónico con un código de activación será entregado a la dirección de correo electrónico introducida en el paso 1, obtener el correo electrónico y abrir la **URL de activación** para activar el proceso y comprobar el estado de la activación.



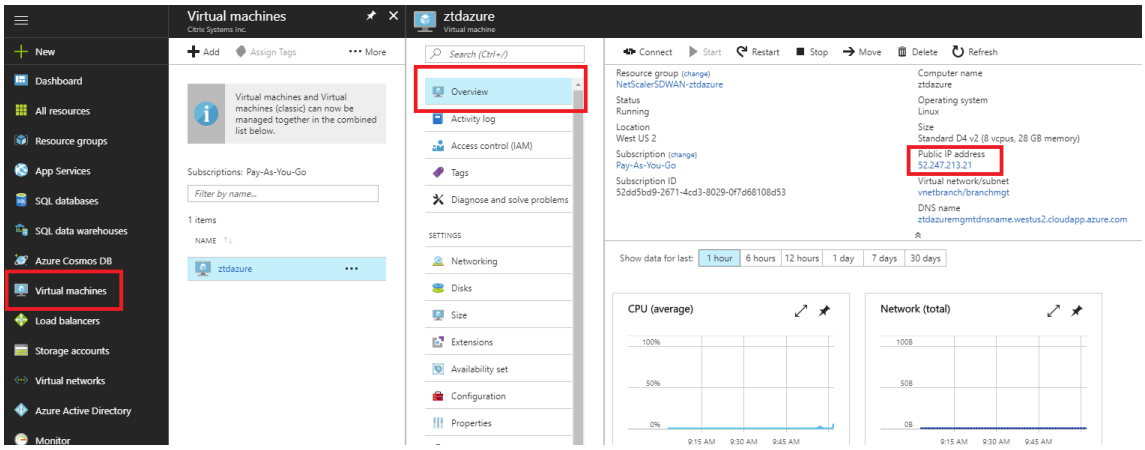
4. Se enviará un correo electrónico con una URL de activación a la dirección de correo electrónico introducida en el paso 1.Obtenga el correo electrónico y abra la **URL de activación** para activar el proceso y comprobar el estado de activación.



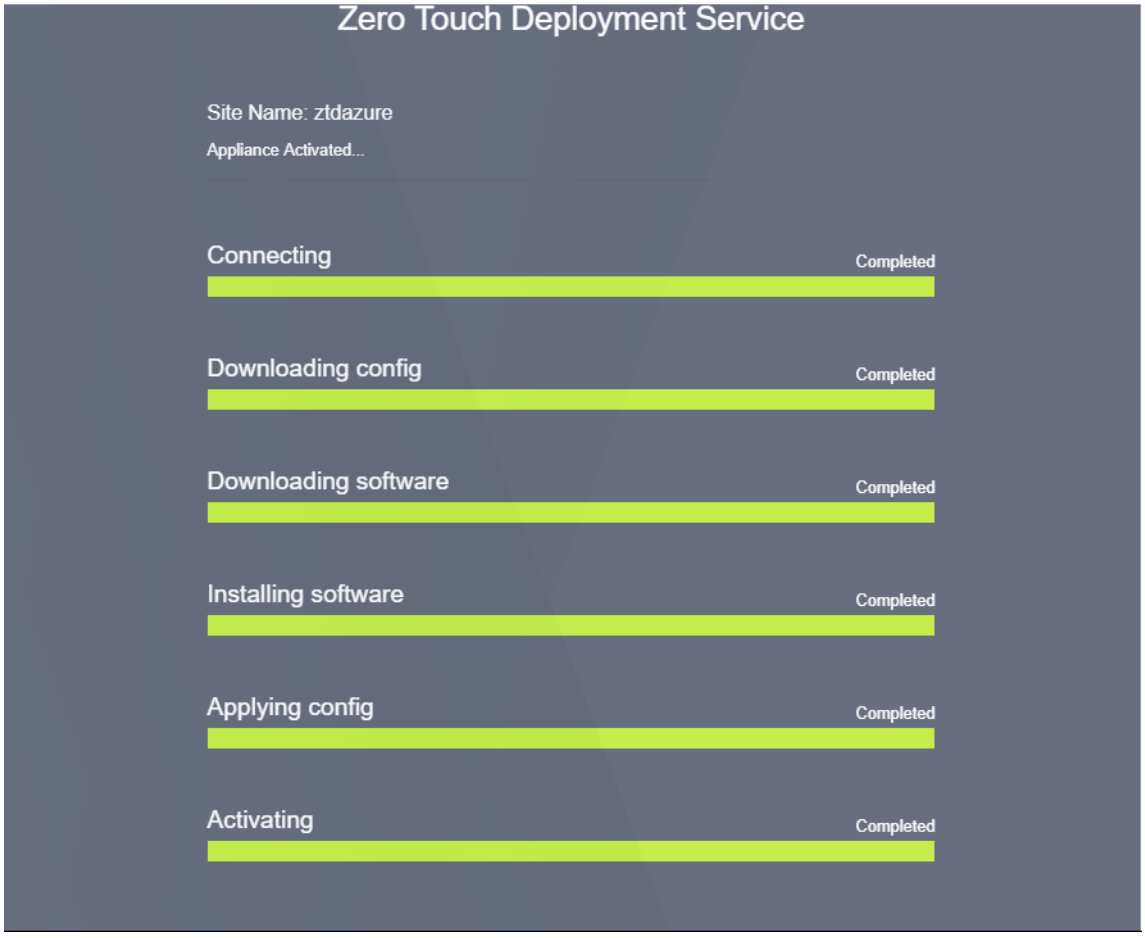
5. El servicio en la nube de SD-WAN tardará unos minutos en aprovisionar la instancia.Puede supervisar la actividad en el portal de Azure, en **Registro de actividad** para el **grupo de recursos** que se crea automáticamente.Cualquier problema o error con el aprovisionamiento se rellenará aquí y se replicará en SD-WAN Center en el Estado de activación.



6. En el portal de Azure, la instancia iniciada correctamente estará disponible en **Máquinas virtuales.** Para obtener la dirección IP pública asignada, vaya a Visión General de la instancia.

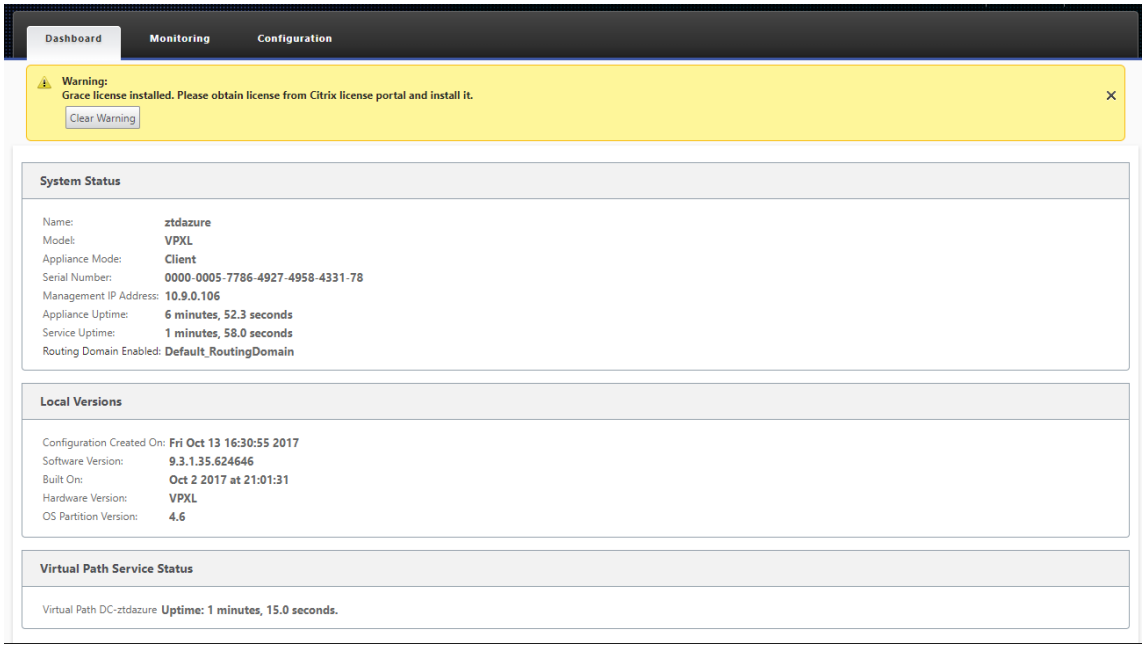


7. Después de que la máquina virtual esté en estado de ejecución, dele un minuto antes de que el servicio se ponga en contacto e inicie el proceso de descarga de la configuración, el software y la licencia.

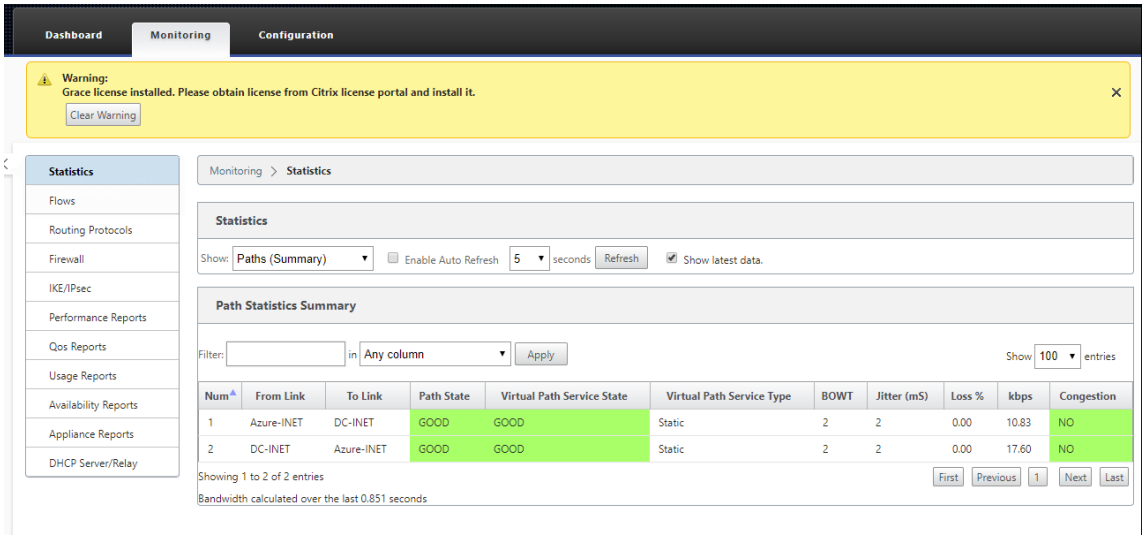


8. Después de que cada uno de los pasos del servicio SD-WAN Cloud se complica automática-

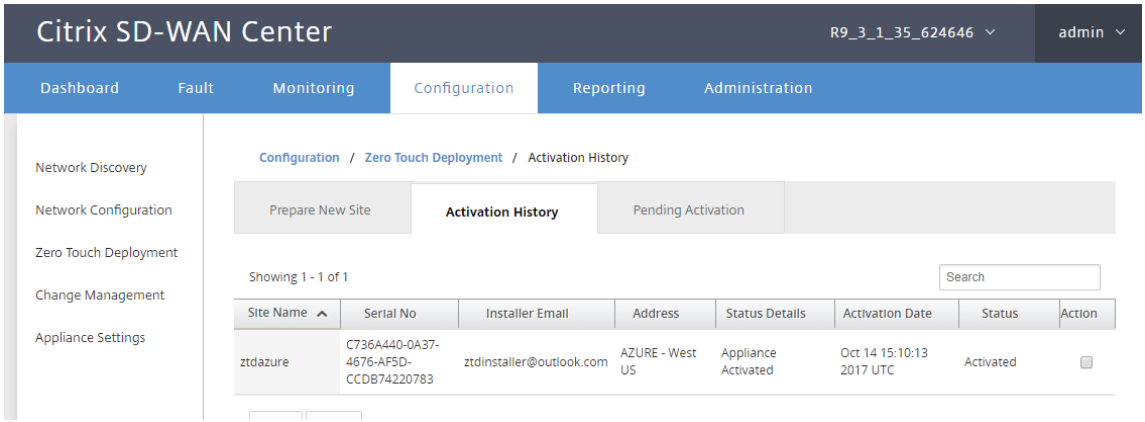
mente, inicie sesión en la interfaz web de instancias SD-WAN mediante la IP pública obtenida del portal de Azure.



9. La página Estadísticas de supervisión de Citrix SD-WAN identificará la conectividad correcta desde el MCN a la instancia de SD-WAN en Azure.



10. Además, el intento de Provisioning correcto (o incorrecto) se registrará en la página Historial de activación de SD-WAN Center.



Configuración del servidor proxy para la implementación de Zero Touch

April 9, 2021

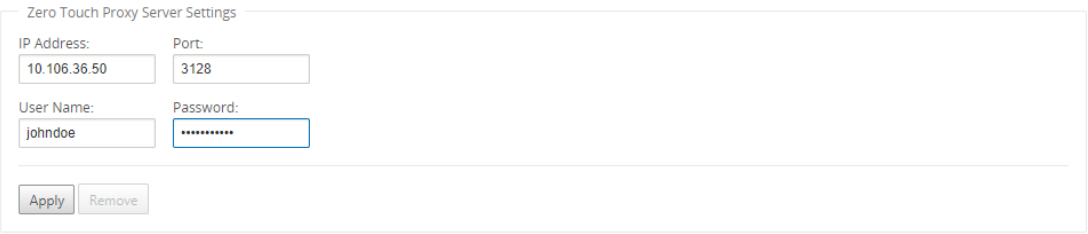
Como requisito previo para la implementación Zero Touch, Citrix SD-WAN Center debe estar conectado a Internet. Si su Citrix SD-WAN Center está conectado a Internet a través de un servidor proxy, debe configurar la configuración del servidor proxy en Citrix SD-WAN Center.

> **Nota**
>
> Esta configuración del servidor proxy se utiliza solo para la implementación de Zero Touch.

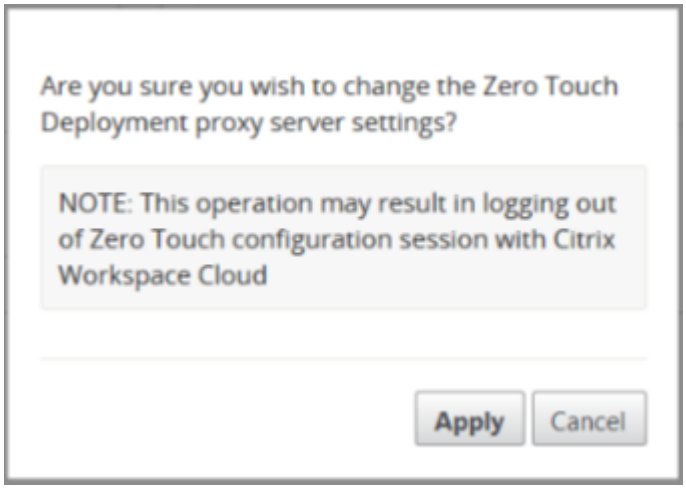
Para configurar la configuración del servidor proxy de cero contacto:

1. En la interfaz web de SD-WAN Center, vaya a **Administración** > **Configuración global** > **Interfaz de administración**.
2. En la sección **Configuración del servidor proxy cero táctil**, introduzca valores para los siguientes campos:
   - **Dirección IP**: La dirección IP del servidor proxy.
   - **Puerto**: el número de puerto de red en el que el servidor proxy acepta conexiones.
   - **Nombre de usuario**: El nombre de usuario del servidor proxy
   - **Contraseña**: La contraseña del servidor proxy.

   > **Nota**
   >
   > Puede dejar el campo **Nombre de usuario** y **contraseña** en blanco si no hay autenticación configurada en el servidor proxy.



3. Haga clic en **Aplicar**, aparecerá un cuadro de diálogo de confirmación.

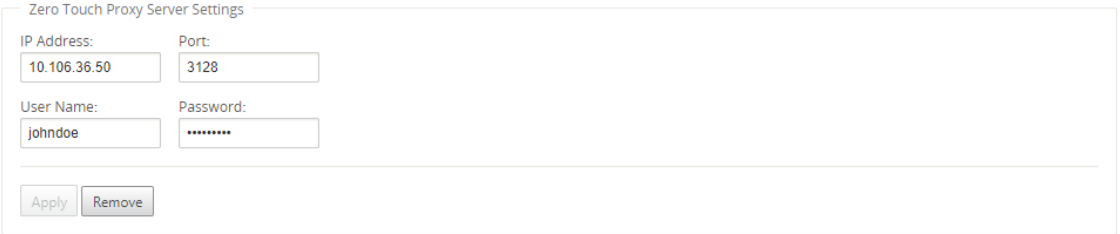


4. Haga clic en **Aplicar**.

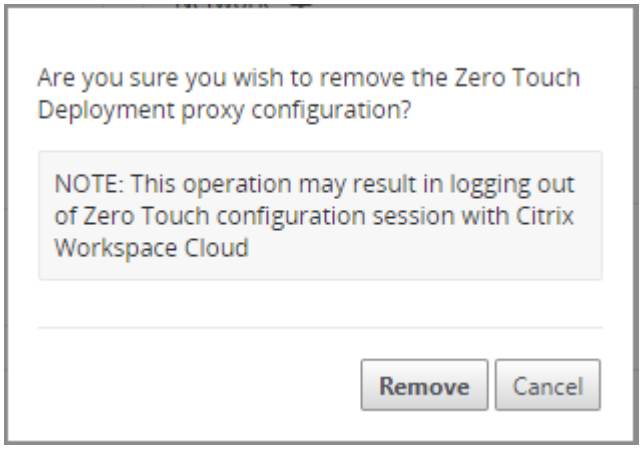
> **Nota**
>
> Puede quitar la configuración del servidor proxy por completo, si Citrix SD-WAN Center está conectado directamente a Internet. También puede quitar la configuración del servidor proxy y configurar otro servidor proxy, si es necesario.

Para quitar la configuración del servidor proxy:

1. En la interfaz web de Citrix SD-WAN Center, vaya a **Administración** > **Configuración global** > **Interfaz de administración**.
2. En la sección **Configuración del servidor proxy Zero Touch**, haga clic en **Quitar**.



3. Haga clic en **Quitar**, aparecerá un cuadro de diálogo de confirmación.



4. Haga clic en **Quitar**.

Integración de redes Palo Alto

April 13, 2021

Las redes Palo Alto ofrecen una infraestructura de seguridad basada en la nube para proteger redes remotas. Proporciona seguridad al permitir a las organizaciones configurar firewalls regionales basados en la nube que protegen la estructura SD-WAN.

El servicio Prisma Access para redes remotas le permite conectar ubicaciones de red remotas y ofrecer seguridad a los usuarios. Elimina la complejidad de configurar y administrar dispositivos en cada ubicación remota. El servicio proporciona una forma eficiente de agregar fácilmente nuevas ubicaciones de red remotas y minimizar los desafíos operativos al garantizar que los usuarios de estas ubicaciones estén siempre conectados y seguros, y le permite administrar las directivas de forma centralizada desde Panorama para lograr una seguridad uniforme y optimizada para su sistema remoto ubicaciones de red.

Para conectar sus ubicaciones de red remotas al servicio Prisma Access, puede usar el firewall de última generación de Palo Alto Networks o un dispositivo compatible con IPsec de terceros, incluido SD-WAN, que puede establecer un túnel IPsec para el servicio.

- Planificar el servicio Prisma Access para redes remotas
- Configurar el servicio Prisma Access para redes remotas
- Redes remotas integradas con importación de configuración

La solución Citrix SD-WAN ya ofrecía la capacidad de eliminar el tráfico de Internet de la sucursal. Esto es fundamental para ofrecer una experiencia de usuario más confiable y de baja latencia, a la vez que se evita la introducción de una costosa pila de seguridad en cada sucursal. Citrix SD-WAN y Palo Alto

Networks ahora ofrecen a las empresas distribuidas una forma más confiable y segura de conectar a los usuarios de sucursales con aplicaciones en la nube.

Los dispositivos Citrix SD-WAN pueden conectarse a la red del servicio en la nube de Palo Alto (Prisma Access Service) a través de túneles IPSec desde ubicaciones de dispositivos SD-WAN con una configuración mínima. Puede configurar la red Palo Alto en Citrix SD-WAN Center.

Antes de comenzar a configurar Prisma Access Service para redes remotas, asegúrese de que tiene la siguiente configuración preparada para asegurarse de que puede habilitar correctamente el servicio y aplicar la directiva para los usuarios de las ubicaciones de red remotas:

1. **Conexión de servicio**: Si sus ubicaciones de red remotas requieren acceso a la infraestructura de su sede corporativa para autenticar usuarios o para habilitar el acceso a activos de red críticos, debe configurar el acceso a su red corporativa para que las oficinas centrales y las ubicaciones de red remotas sean conectado.

Si la ubicación de red remota es autónoma y no necesita acceder a la infraestructura en otras ubicaciones, no es necesario configurar la conexión de servicio (a menos que los usuarios móviles necesiten acceso).

1. **Plantilla**: El servicio Prisma Access crea automáticamente una pila de plantillas (Remote_Network_Template_Stack) y una plantilla de nivel superior (Remote_Network_Template) para el servicio Prisma Access para redes remotas. Para configurar Prisma Access Service for Remote Networks, configure la plantilla de nivel superior desde cero o aproveche su configuración existente, si ya está ejecutando un firewall de redes Palo Alto en las instalaciones.

   La plantilla requiere la configuración para establecer el túnel IPSec y la configuración de Intercambio de claves de Internet (IKE) para la negociación de protocolos entre la ubicación de red remota y el servicio Prisma Access para redes remotas, zonas a las que puede hacer referencia en la directiva de seguridad y un perfil de reenvío de registros para que puede reenviar registros desde el servicio Prisma Access para redes remotas al servicio de registro.

2. **Grupo de dispositivos principal**: El servicio Prisma Access para redes remotas requiere que especifique un grupo de dispositivos principal que incluya la directiva de seguridad, los perfiles de seguridad y otros objetos de directiva (como grupos y objetos de aplicaciones y grupos de direcciones), así como la directiva de autenticación para que el servicio Prisma Access para redes remotas puede aplicar sistemáticamente directivas para el tráfico que se enruta a través del túnel IPSec al servicio Prisma Access para redes remotas. Debe definir reglas y objetos de directiva en Panorama o utilizar un grupo de dispositivos existente para proteger a los usuarios en la ubicación de red remota.

   > **Nota:**
   >
   > Si utiliza un grupo de dispositivos existente que hace referencia a zonas, asegúrese de agre-

> gar la plantilla correspondiente que define las zonas a Remote_Network_Template_Stack.

Esto le permite completar la asignación de zonas al configurar Prisma Access Service for Remote Networks.

3. **Subredes IP**: Para que el servicio Prisma Access enrute el tráfico a las redes remotas, debe proporcionar información de enrutamiento para las subredes que quiere proteger mediante el servicio Prisma Access. Puede definir una ruta estática a cada subred en la ubicación de red remota o configurar BGP entre las ubicaciones de conexión de servicio y el servicio Prisma Access, o utilizar una combinación de ambos métodos.

   Si configura ambas rutas estáticas y habilita BGP, las rutas estáticas tienen prioridad. Si bien puede ser conveniente utilizar rutas estáticas si tiene unas pocas subredes en sus ubicaciones de red remotas, en una implementación grande con muchas redes remotas con subredes superpuestas, BGP le permitirá escalar más fácilmente.

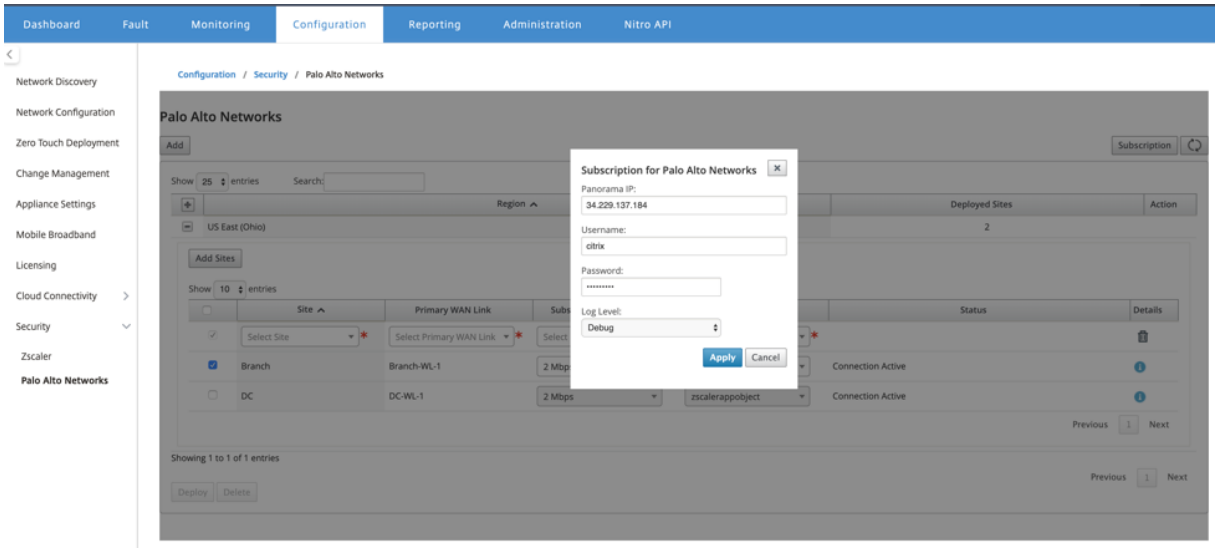
Red Palo Alto en SD-WAN Center

Asegúrese de que se cumplen los siguientes requisitos previos:

- Obtener la dirección IP panorámica del servicio PRISMA ACCESS.
- Obtener nombre de usuario y contraseña de usuario en el servicio PRISMA ACCESS.
- Configure los túneles IPSec en la GUI del dispositivo SD-WAN.
- Asegúrese de que el sitio no está incorporado a una región, que ya tiene un sitio diferente configurado con perfiles ike/ipsec distintos de Citrix-ike-crypto-default/Citrix-ipsec-crypto-default.
- Asegúrese de que la configuración de Prisma Access no se cambie manualmente cuando SD-WAN Center actualice la configuración.

En la GUI de Citrix SD-WAN Center, proporcione información de suscripción a Palo Alto.

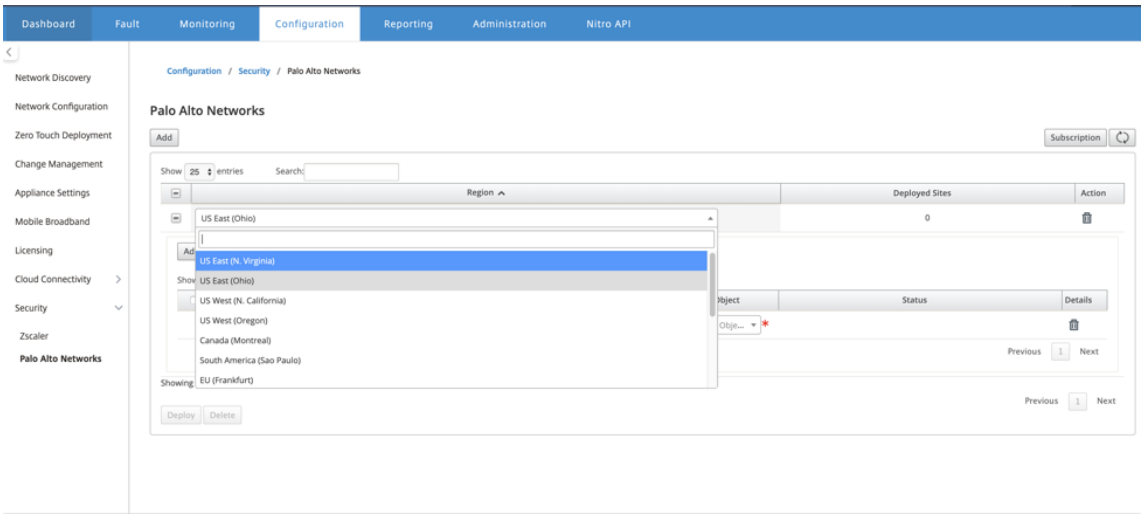
- Configure la dirección IP panorámica. Puede obtener esta dirección IP de Palo Alto (servicio PRISMA ACCESS).
- Configure el nombre de usuario y la contraseña utilizados en el servicio PRISMA ACCESS.

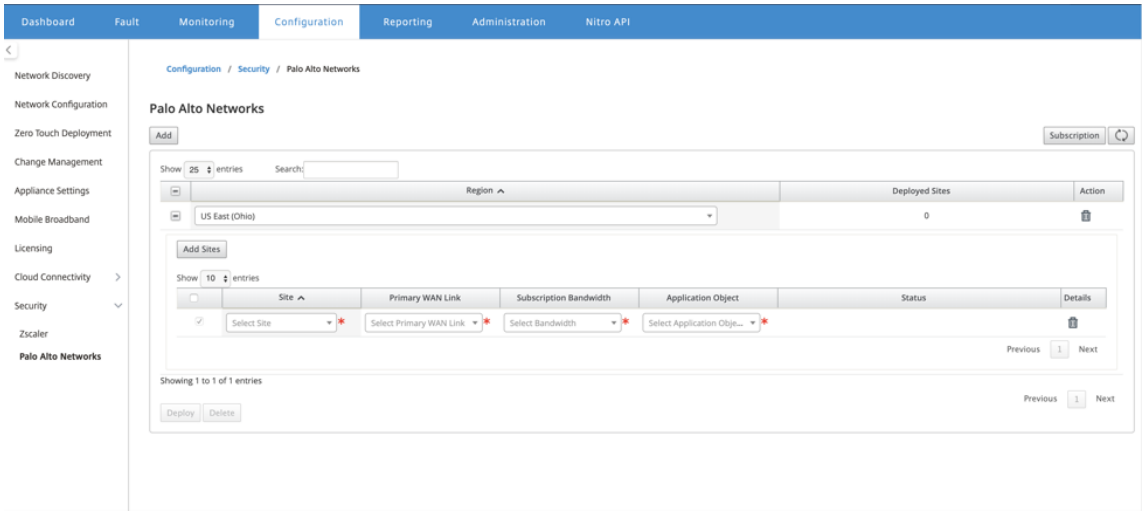


Agregar e implementar sitios

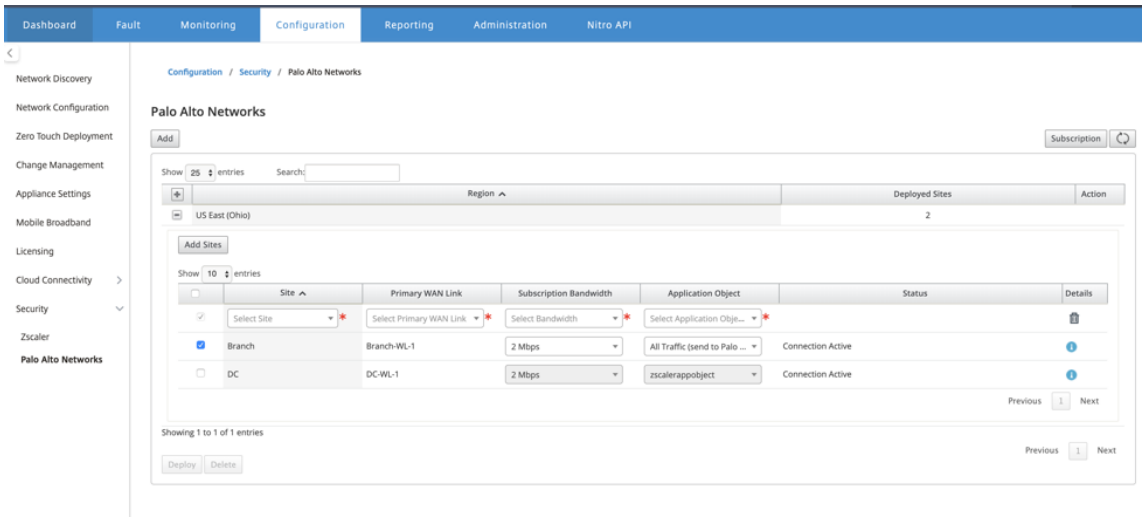
1. Para implementar los sitios, elija la región de red PRISMA ACCESS y el sitio SD-WAN que se configurará para la región Prisma Access y, a continuación, seleccione el enlace WAN del sitio, el ancho de banda y el objeto de aplicación para la selección del tráfico.

   > **Nota**
   >
   > :
   >
   > El flujo de tráfico se ve afectado si el ancho de banda seleccionado supera el rango de ancho de banda disponible.
   >
   > Puede optar por redirigir todo el tráfico enlazado a Internet al servicio PRISMA ACCESS seleccionando la opción **Todo el tráfico** en la selección Objeto Aplicación.

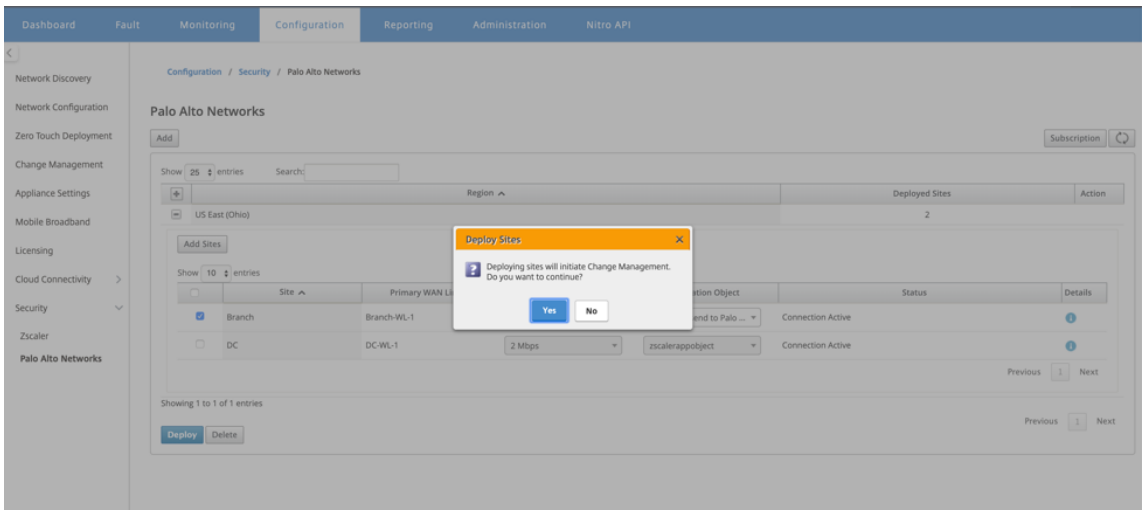




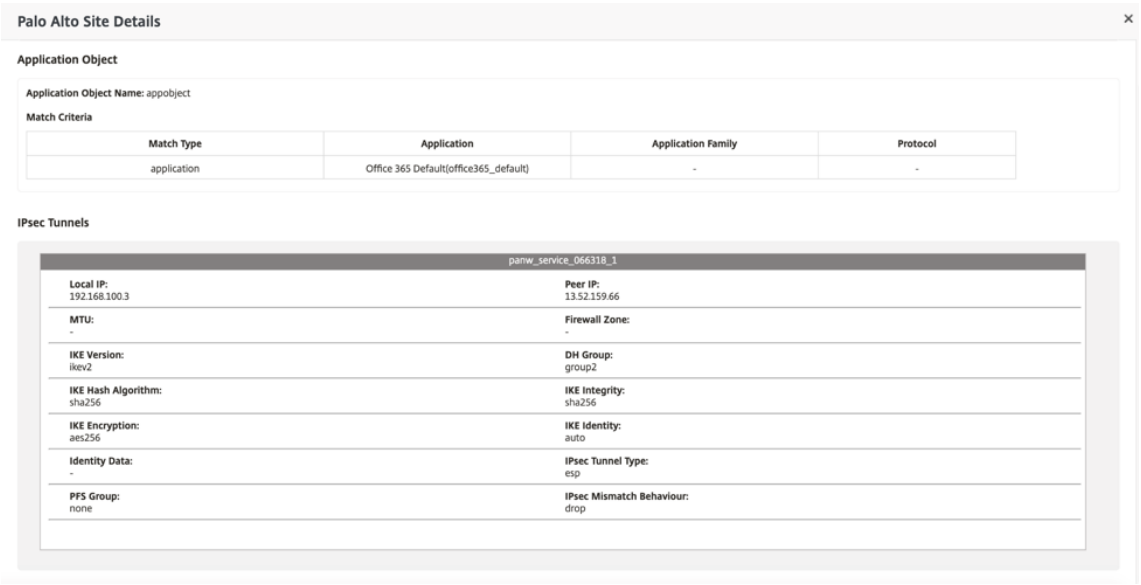
2. Puede continuar agregando más sitios de sucursales SD-WAN según sea necesario.



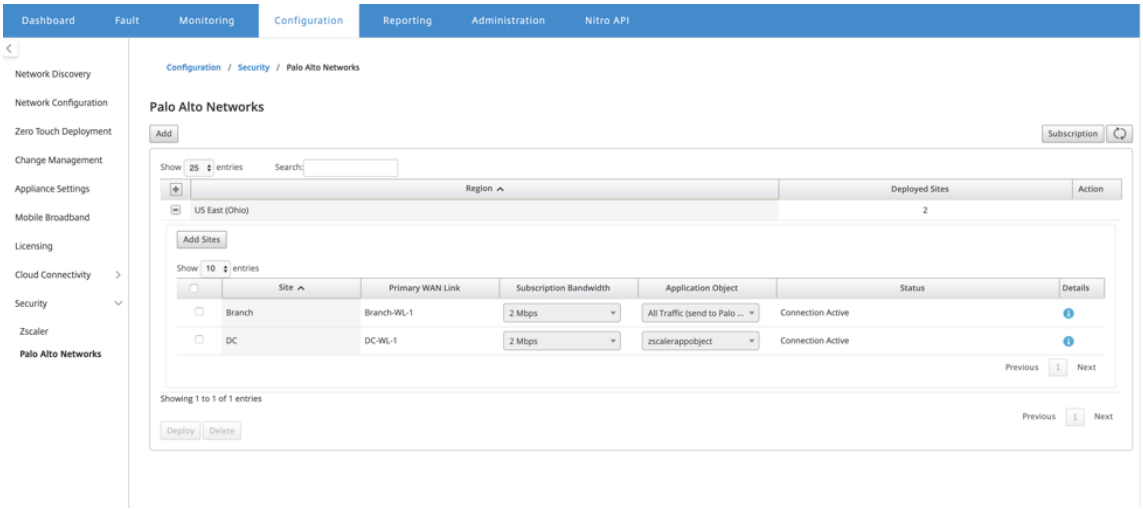
3. Haga clic en **Implementar**. Se inicia el proceso de gestión de cambios. Haga clic en **Sí** para continuar.



Después de la implementación, la configuración del túnel IPSec utilizada para establecer los túneles es la siguiente.



La página de destino muestra la lista de todos los sitios configurados y agrupados en diferentes regiones SD-WAN.



Verificar la conexión de tráfico de extremo a extremo:

- Desde la subred LAN de la sucursal, acceda a los recursos de Internet.
- Compruebe que el tráfico pasa a través del túnel IPSec de Citrix SD-WAN hasta Palo Alto Prisma Access.
- Compruebe que la directiva de seguridad de Palo Alto se aplica al tráfico en la ficha Supervisión.
- Verifique que la respuesta de Internet al host en una sucursal llegue a través.

WAN virtual de Microsoft Azure

April 13, 2021

Microsoft Azure Virtual WAN y Citrix SD-WAN proporcionan conectividad de red simplificada y administración centralizada en cargas de trabajo de nube híbrida. Puede automatizar la configuración de los dispositivos de sucursal para conectarse a la WAN de Azure y configurar directivas de administración del tráfico de sucursales de acuerdo con los requisitos de su empresa. La interfaz de panel integrada proporciona información sobre la solución de problemas instantánea que puede ahorrar tiempo y proporciona visibilidad para conectividad de sitio a sitio a gran escala.

Microsoft Azure Virtual WAN le permite habilitar la conectividad simplificada a las cargas de trabajo de Azure Cloud y enrutar el tráfico a través de la red troncal de Azure y más allá. Azure proporciona más de 54 regiones y varios puntos de presencia en todo el mundo Las regiones de Azure sirven como concentradores que puede elegir conectarse a las sucursales. Una vez conectadas las sucursales, utilice el servicio en la nube de Azure a través de la conectividad de concentrador a concentrador. Puede simplificar la conectividad mediante la aplicación de varios servicios de Azure, incluido el emparejamiento de concentradores con redes virtuales de Azure. Los concentradores sirven de puertas de enlace de tráfico para las sucursales.

Microsoft Azure Virtual WAN ofrece las siguientes ventajas:

- Soluciones de conectividad integradas en concentradores y radiales: automatice la conectividad y la configuración de sitio a sitio entre las instalaciones y el concentrador de Azure desde diversos orígenes, incluidas las soluciones de partners conectados.
- Configuración e instalación automatizadas: Conecte sus redes virtuales al concentrador de Azure sin problemas.
- Solución de problemas intuitiva: Puede ver el flujo de extremo a extremo dentro de Azure y usar esta información para realizar las acciones necesarias.

Comunicación de concentrador a concentrador

A partir de la versión 11.1.0, la WAN virtual de Azure es compatible con la comunicación de concentrador a concentrador mediante el método de tipo **estándar**.

Los clientes de Azure Virtual WAN ahora pueden aprovechar la red troncal global de Microsoft para la comunicación entre regiones concentrador (arquitectura de red de tránsito global). Esto permite la comunicación de bifurcación a Azure, de rama a rama sobre la estructura troncal de Azure y de rama a centro (en todas las regiones de Azure).

Puede aprovechar la estructura troncal de Azure para la comunicación entre regiones solo cuando adquiera el SKU estándar para la WAN virtual de Azure. Para obtener más información sobre precios,

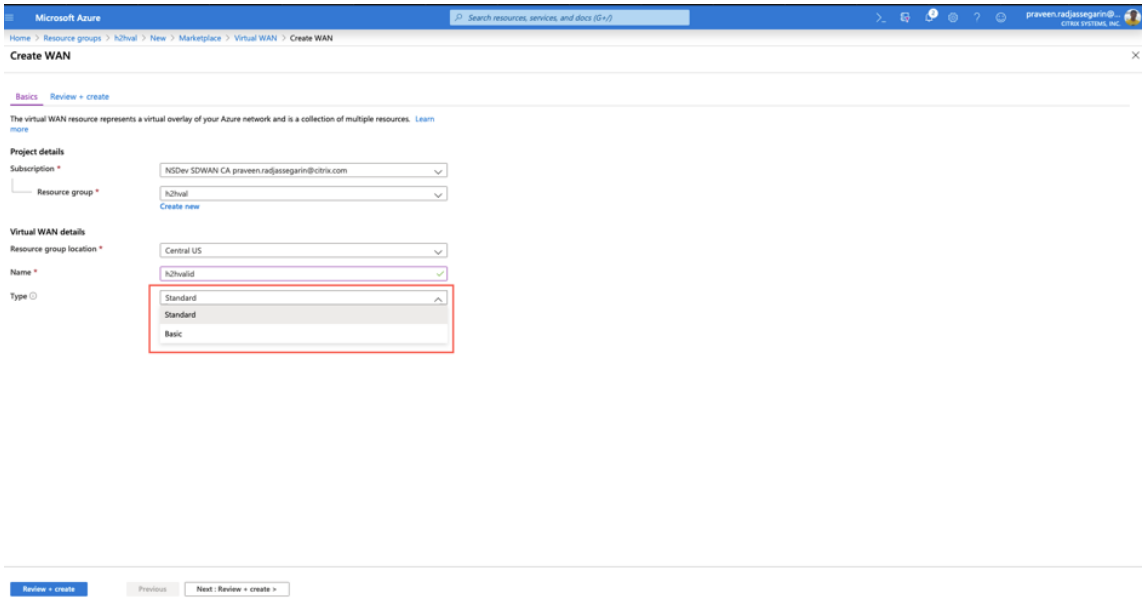
consulte Precios de la WAN virtual. Con el SKU básico, no puede usar la estructura troncal de Azure para la comunicación entre regiones de centro a centro. Para obtener más información detallada, consulte Arquitectura de red de tránsito global y WAN.

Los concentradores están conectados entre sí en una WAN virtual. Esto implica que una rama, usuario o vNet conectada a un concentrador local puede comunicarse con otra rama o vNet mediante la arquitectura de malla completa de los concentradores conectados.

También puede conectar VNET dentro de un concentrador que transita a través del concentrador virtual, y vNET a través del concentrador, mediante el marco conectado de concentrador a concentrador.

Hay dos tipos de WAN virtual:

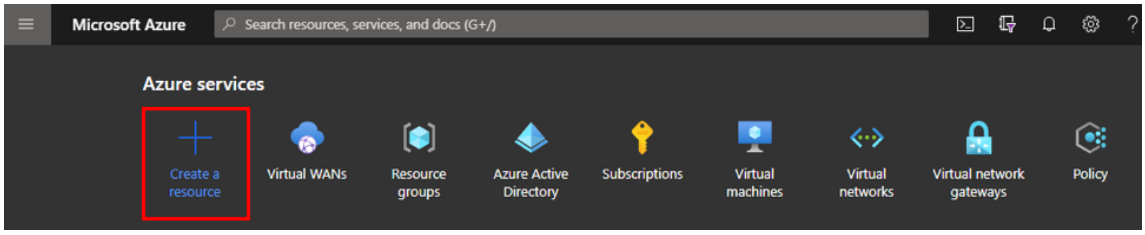
- **Básico**: Mediante el método **Basic**, las comunicaciones de centro a centro se producen dentro de una región. El tipo de WAN **básica** ayuda a crear un hub básico (SKU = Basic). Los concentradores básicos se limitan a la funcionalidad VPN de sitio a sitio.
- **Estándar**: Mediante el método **Estándar**, las comunicaciones de centro a concentrador se producen entre diferentes regiones. Una WAN **estándar** ayuda a crear concentrador estándar (SKU = Estándar). Los concentradores**estándar** contienen ExpressRoute, VPN de usuario (P2S), concentrador de malla completo y tránsito de VNET a VNet a través de los concentradores.



Crear servicio WAN virtual de Azure en Microsoft Azure

Para crear el recurso de Azure Virtual WAN, realice los siguientes pasos:

1. Inicie sesión en Azure Portal y haga clic en **Crear un recurso**.

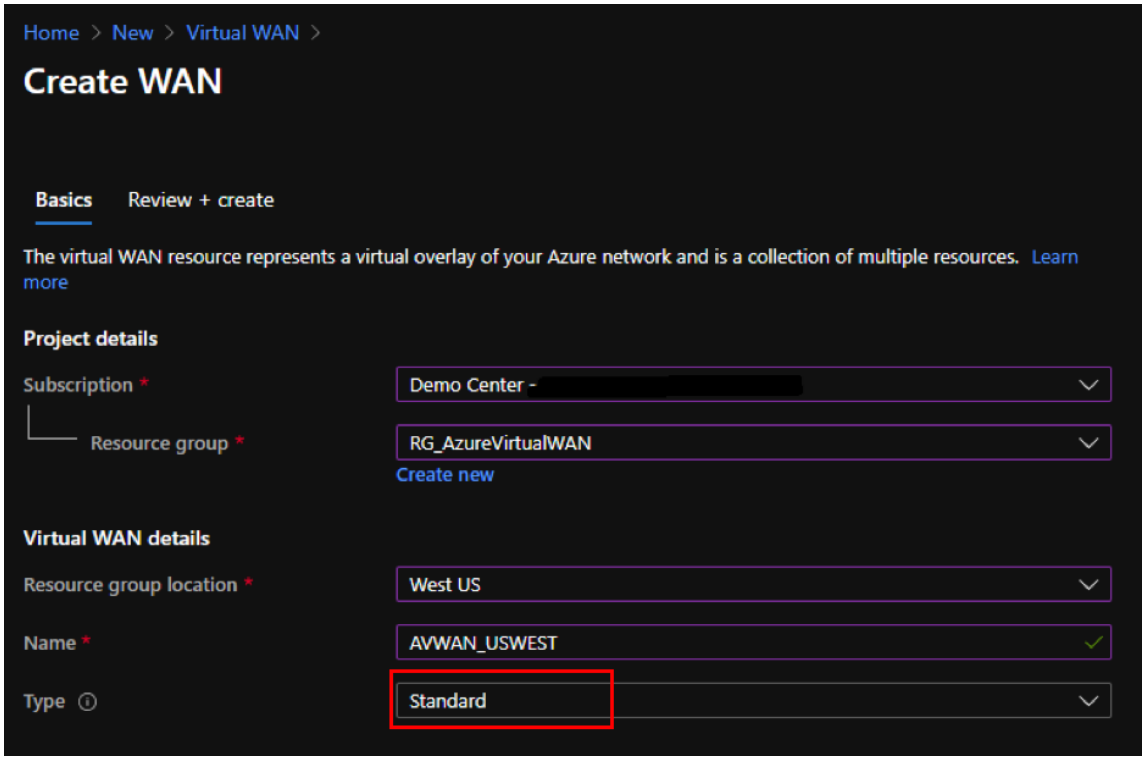


2. Busque **WAN virtual** y haga clic en **Crear**.
3. En **Básico**, proporcione los valores de los siguientes campos:

    - **Suscripción**: seleccione y proporcione los detalles de la suscripción en la lista desplegable.
    - **Grupo de recursos**: seleccione un grupo de recursos existente o cree uno nuevo.

        > **Nota**
        >
        > Al crear la entidad de servicio para permitir la comunicación con la API de Azure, asegúrese de utilizar el mismo grupo de recursos que contiene la WAN virtual. De lo contrario, SD-WAN Orchestrator no tendrá permisos suficientes para autenticarse en las API de Azure Virtual WAN que habilitan la conectividad automatizada.

    - **Ubicación del grupo de recursos**: seleccione la región de Azure en la lista desplegable.
    - **Nombre**: proporcione el nombre de la nueva WAN virtual.
    - **Tipo**: seleccione Tipo **estándar** si desea utilizar la comunicación de concentrador a centro entre diferentes regiones; de lo contrario, seleccione **Básico**.



4. Haga clic en **Revisar + crear**.
5. Revise los detalles que ha introducido para crear la Wan virtual y haga clic en **Crear** para finalizar la creación de WAN virtual.

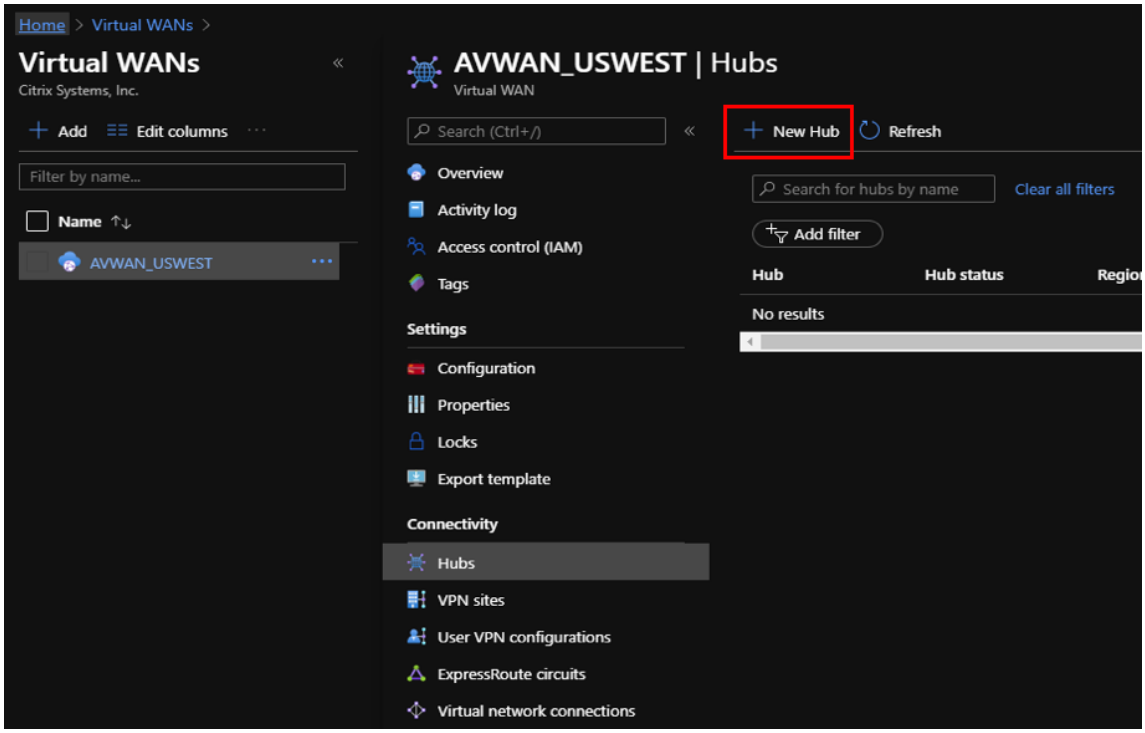
La implementación del recurso tarda menos de un minuto.

> **Nota**
>
> Puede actualizar de Básico a Estándar, pero no puede volver de Estándar a Básico. Para obtener información sobre los pasos para actualizar una WAN virtual, consulte Actualizar una WAN virtual de Básica a Estándar.

Crear un centro en la WAN virtual de Azure

Realice los siguientes pasos para crear un concentrador que permita la conectividad desde varios puntos finales diferentes (por ejemplo, dispositivos VPN locales o dispositivos SD-WAN):

1. Seleccione la WAN virtual de Azure creada anteriormente.
2. Seleccione **Hubs** en la sección **Conectividad** y haga clic en **+ Nuevo concentrador**.

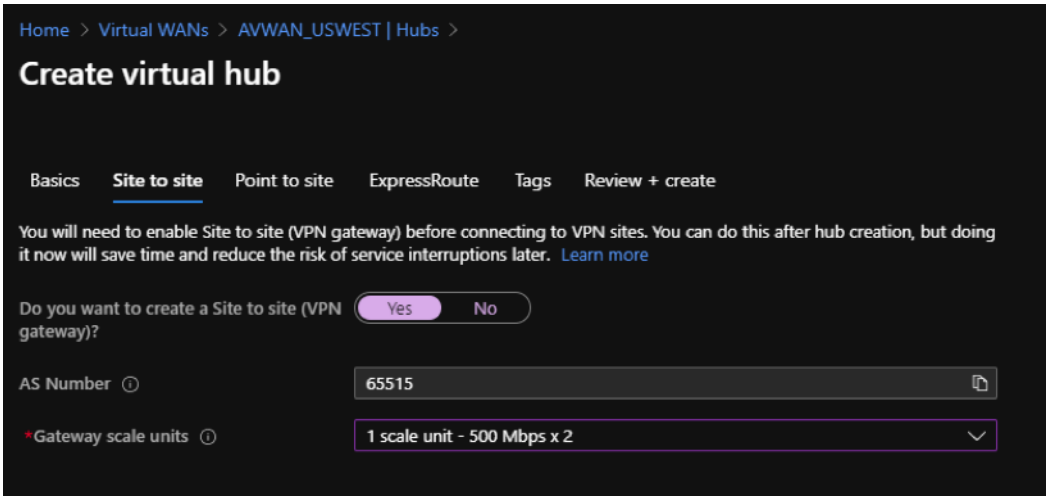


3. En **Básico**, proporcione los valores de los siguientes campos:

   - **Región** : seleccione la región de Azure en la lista desplegable.
   - **Nombre** : introduzca el nombre del nuevo Hub.
   - **Espacio de direcciones privado del hub** : introduzca el rango de direcciones en CIDR. Seleccione una red única que esté dedicada únicamente al concentrador.

4. Haga clic en **Siguiente: Site to Site** y proporcione los valores de los siguientes campos:

   - **¿ Desea crear un sitio a sitio (puerta de enlace VPN)?** —Seleccione **Sí**.
   - **Unidades de escala de puerta** de enlace: seleccione las unidades de escala de la lista desplegable según sea necesario.



5. Haga clic en **Revisar + crear**.
6. Revise la configuración y haga clic en **Crear** para iniciar la creación del concentrador virtual.

La implementación del recurso puede tardar hasta 30 minutos.

Cree una entidad de servicio para Azure Virtual WAN e identifique los identificadores

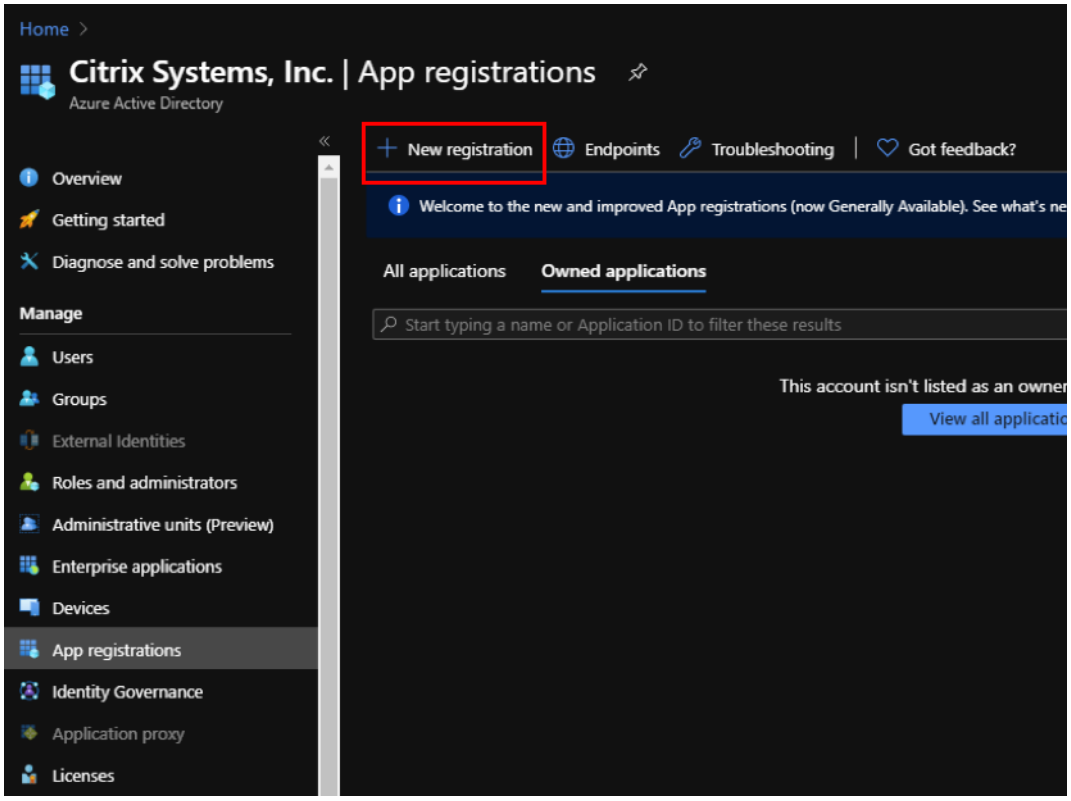
Para que SD-WAN Orchestrator se autentique a través de las API de Azure Virtual WAN y habilite la conectividad automatizada, se debe crear una aplicación registrada e identificarse con las siguientes credenciales de autenticación:

- ID de suscripción
- ID de cliente
- Secreto del cliente
- ID de arrendatario

> **Nota**
>
> Al crear la entidad de servicio para permitir la comunicación con la API de Azure, asegúrese de utilizar el mismo grupo de recursos que contiene la WAN virtual. De lo contrario, SD-WAN Orchestrator no tendrá permisos suficientes para autenticarse en las API de Azure Virtual WAN que habilitan la conectividad automatizada.

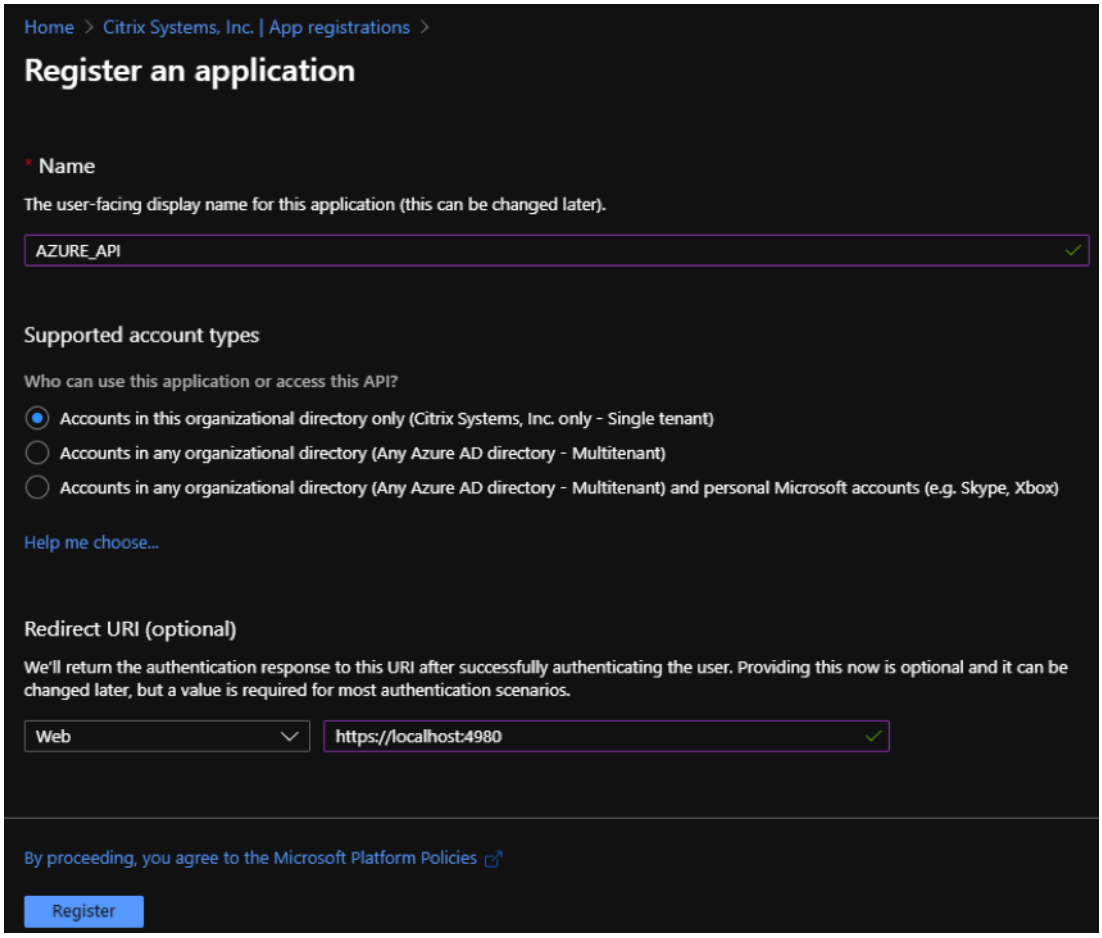
Realice los siguientes pasos para crear un nuevo registro de aplicación:

1. En el portal de Azure, vaya a **Azure Active Directory**.
2. En Administrar, selecciona **Registro de aplicaciones**.
3. Haga clic en **+ Nuevo registro**.

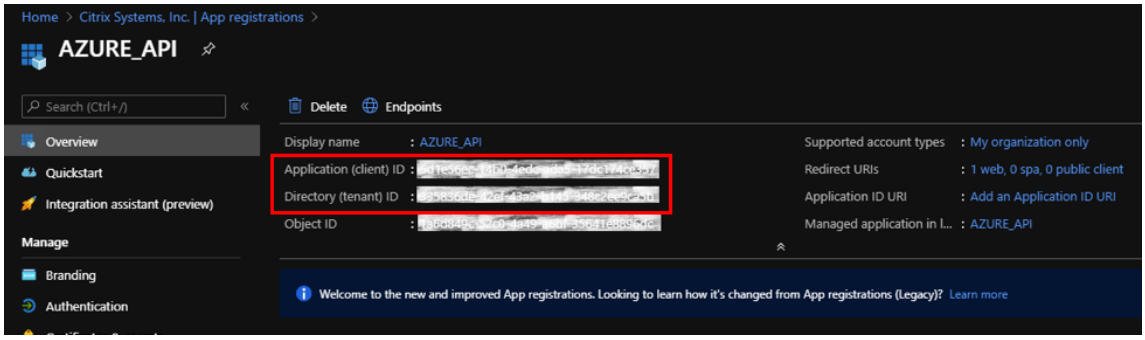


4. Proporcione valores para los siguientes campos para registrar una aplicación:

   - **Nombre**: Proporcione el nombre para el registro de la solicitud.
   - **Tipos de cuenta admitidos**: Seleccione Cuentas en este directorio organizativo solo opción (* - Arrendatario único).
   - **URI de redirección (opcional)**: Seleccione Web en la lista desplegable e introduzca una URL aleatoria única (por ejemplo, https://localhost: 4980)
   - Haga clic en **Registrar**.



Puede copiar y almacenar el ID de **aplicación (cliente) y el ID** de **directorio (arrendatario)** que se pueden usar en SD-WAN Orchestrator para la autenticación en la suscripción de Azure para el uso de API.



El siguiente paso para el registro de la aplicación, crear una clave principal de servicio para fines de autenticación.

Para crear la clave principal de servicio, realice los siguientes pasos:

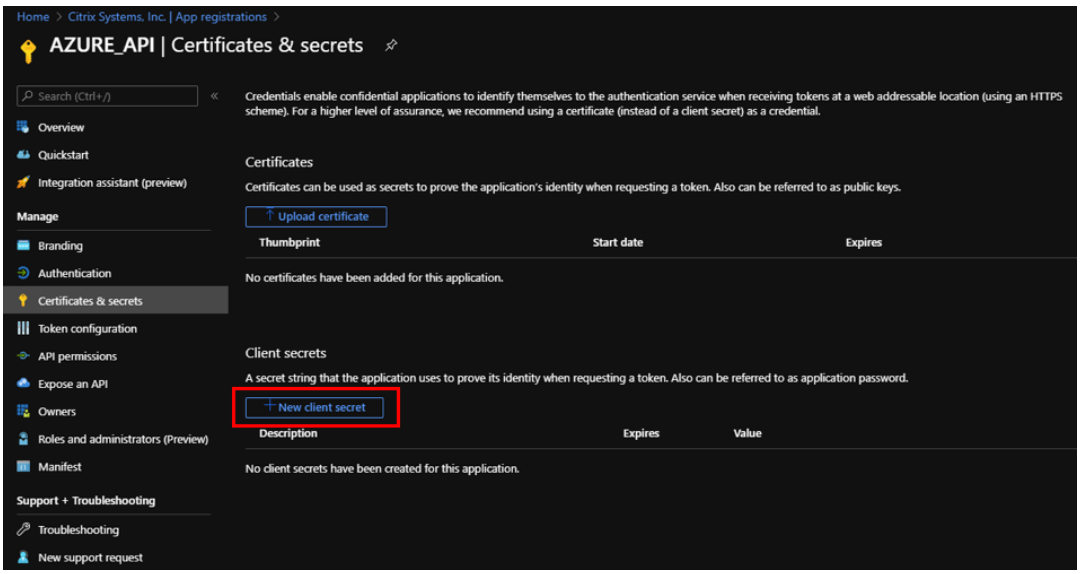
a) En el portal de Azure, vaya a **Azure Active Directory**.

b) En **Administrar**, vaya a **Registro de aplicaciones**.

c) Seleccione la aplicación registrada (creada anteriormente).

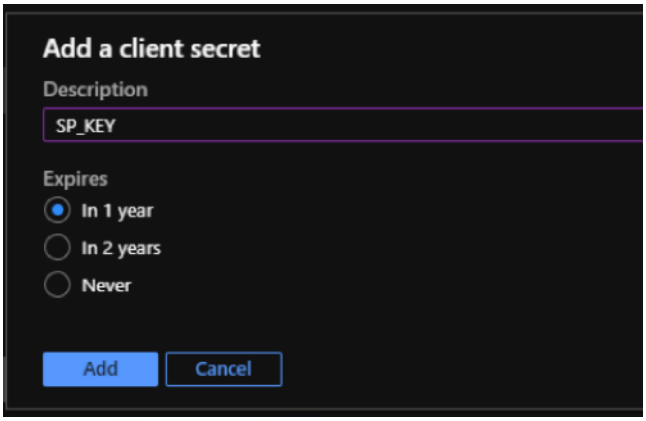
d) En **Administrar**, seleccione **Certificados y secretos**.

e) En **Secretos de cliente**, haga clic en **+ Nuevo secreto de cliente**.



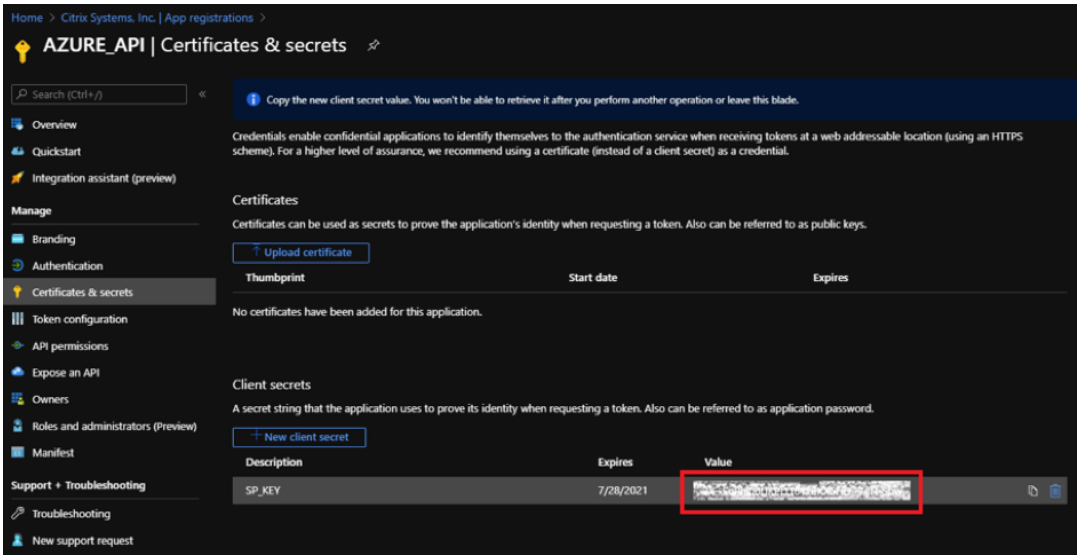
f) Para agregar un secreto de cliente, proporcione valores para los siguientes campos:

- **Descripción**: Proporcione un nombre para la clave principal del servicio.
- **Caduca**: seleccione la duración de caducidad según sea necesario.



g) Haga clic en **Agregar**.

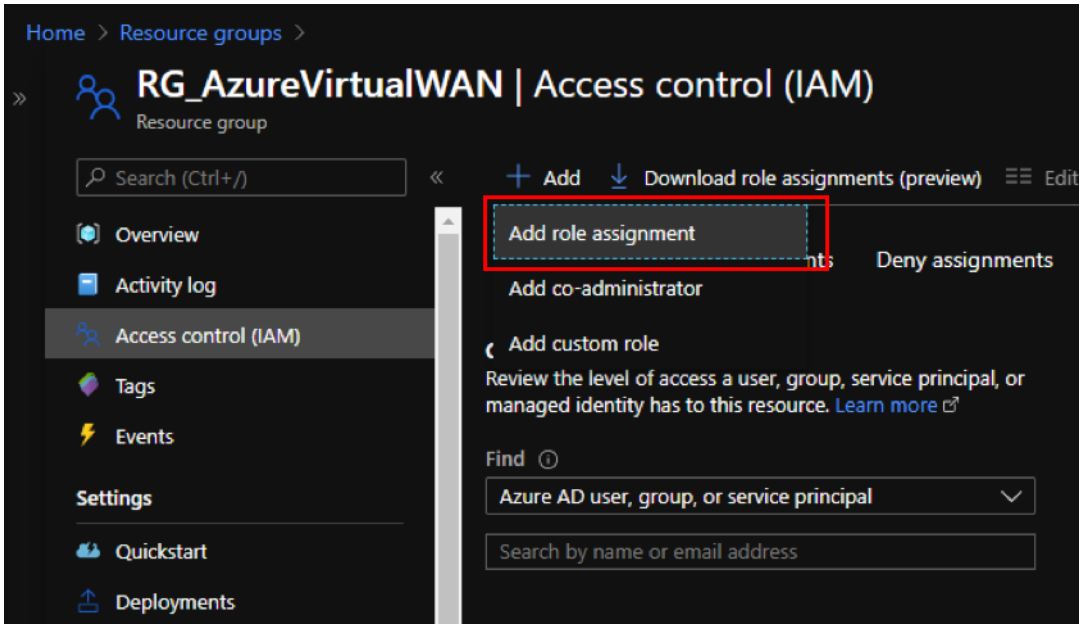
h) El secreto de cliente está inhabilitado en la columna **Valor**. Copie la clave en el portapapeles. Este es el secreto del cliente que debe introducir en SD-WAN Orchestrator.



> **Nota**
>
> Debe copiar y almacenar el valor de clave secreta antes de volver a cargar la página porque, ya no se mostrará después.

Realice los siguientes pasos para asignar los roles adecuados con fines de autenticación:

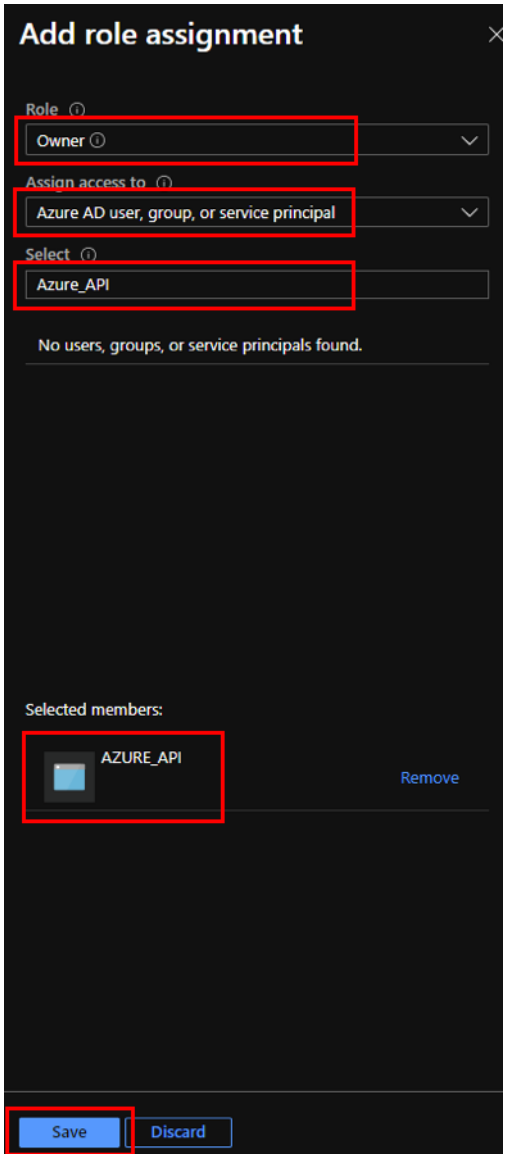
1. En el portal de Azure, vaya al **grupo de recursos** donde se creó la WAN virtual.
2. Desplácese hasta **Control de acceso (IAM)**.
3. Haga clic en **+ Agregar** y seleccione **Agregar asignación de rol**.



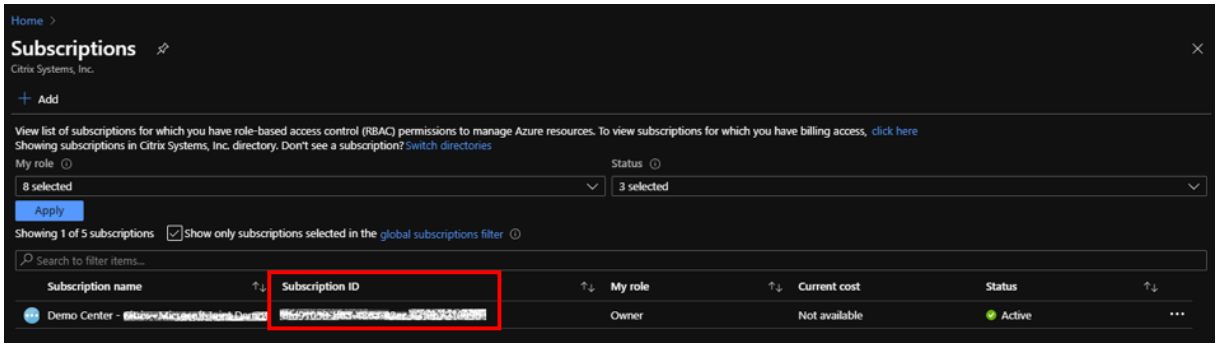
4. Para agregar la asignación de roles, proporcione valores para los siguientes campos:

- **Rol**: Seleccione Propietario en la lista desplegable. Este rol permite la gestión de todo, incluido el acceso a los recursos.
- **Asignar acceso a**: Seleccione **Usuario, grupo** o **entidad de servicio de** Azure AD.
- **Seleccionar**: Proporcione el nombre de la aplicación registrada creada anteriormente y seleccione la entrada correspondiente cuando aparezca.

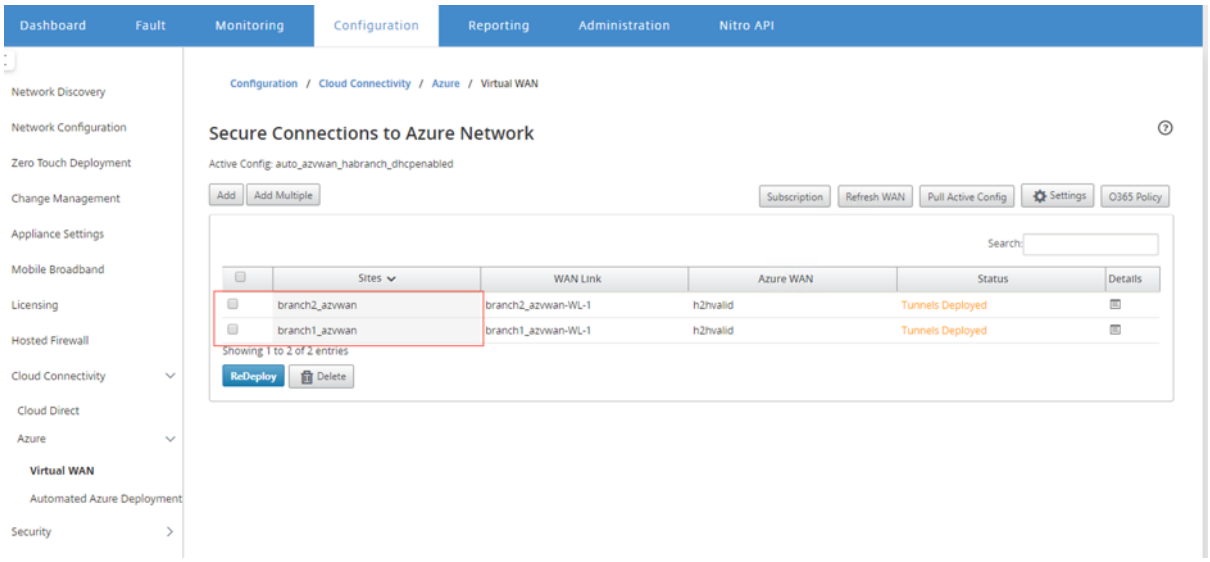
5. Haga clic en **Guardar**.



Por último, debe obtener el identificador de suscripción para la cuenta de Azure. Puede identificar su **ID de suscripción** buscando suscripciones en Azure Portal.



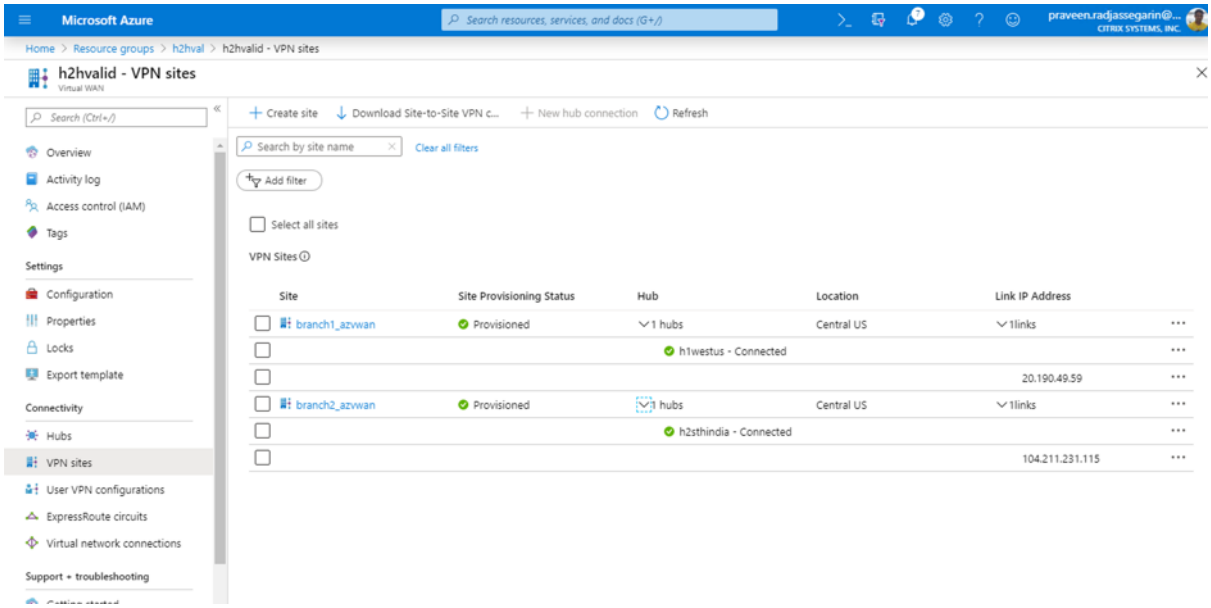
Una vez creada la WAN virtual, inicie sesión en la **interfaz de usuario de SD-WAN Center > Configuración > Azure > Virtual WAN**.



Seleccione dos sitios diferentes e inicie la implementación. Una vez implementados los sitios, puede asociar ambos sitios a dos concentradores diferentes.

> **NOTA**
> De forma predeterminada de rama a rama y BGP está inhabilitado. Puede crear una ruta estática o habilitar BGP (en Configuración) y la conectividad de rama a rama.

Habilite la casilla de verificación BGP y de rama a rama e implemente los túneles. Una vez implementados correctamente los túneles, puede verificar el estado en **Microsoft Azure > Grupos de recursos** seleccionar el **grupo de recursos** que creó y haga clic en **Sitios VPN**.



Uso de Citrix SD-WAN para conectarse a Microsoft Azure Virtual WAN

February 16, 2022

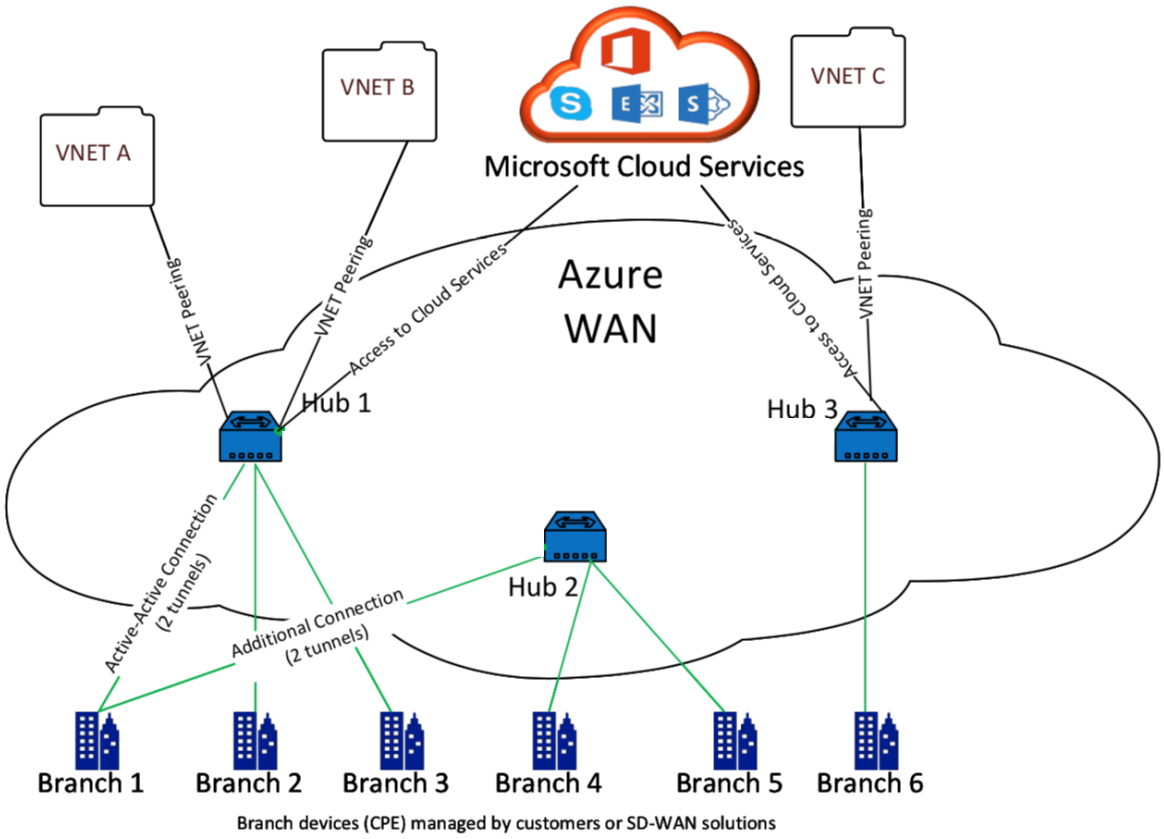
Para que los dispositivos locales se conecten a Azure se requiere un controlador. Un controlador ingiere las API de Azure para establecer la conectividad de sitio a sitio con la WAN de Azure y un Hub.

La WAN virtual de Microsoft Azure incluye los siguientes componentes y recursos:

- WAN: representa toda la red en Microsoft Azure. Contiene enlaces a todos los Hubs que le gustaría tener dentro de esta WAN. Las WAN están aisladas entre sí y no pueden contener un concentrador común ni conexiones entre dos concentradores en WAN diferentes.
- Sitio: Representa su dispositivo VPN local y su configuración. Un sitio puede conectarse a varios concentradores. Mediante Citrix SD-WAN, puede tener una solución integrada para exportar automáticamente esta información a Azure.
- Hub: representa el núcleo de la red en una región específica. El Hub contiene varios puntos finales de servicio para habilitar la conectividad y otras soluciones a la red local. Las conexiones de sitio a sitio se establecen entre los sitios a un extremo VPN de Hubs.
- Conexión de red virtual del concentrador: la red de concentradores conecta Azure Virtual WAN Hub sin problemas a su red virtual. Actualmente, está disponible la conectividad a redes virtuales que se encuentran dentro de la misma región de concentrador virtual.
- Rama: Las ramas son los dispositivos Citrix SD-WAN locales, que existen en las ubicaciones de las oficinas del cliente. Un controlador SD-WAN administra las ramas de forma centralizada. La

conexión se origina desde detrás de estas ramas y termina en Azure. El controlador SD-WAN es responsable de aplicar la configuración requerida a estas ramas y a Azure Hubs.

En la siguiente ilustración se describen los componentes de Virtual WAN:



Cómo funciona Microsoft Azure Virtual WAN

1. SD-WAN Center se autentica mediante la funcionalidad de acceso basado en funciones, principal o principal de servicio, que está habilitada en la GUI de Azure.
2. SD-WAN Center obtiene la configuración de conectividad de Azure y actualiza el dispositivo local. Esto automatiza la descarga, edición y actualización de la configuración del dispositivo in situ.
3. Después de que el dispositivo tenga la configuración correcta de Azure, se establece una conexión de sitio a sitio (dos túneles IPSec activos) a la WAN de Azure. Azure requiere el conector de dispositivo de rama para admitir la configuración de IKEv2. La configuración BGP es opcional.

   Nota: Los parámetros IPSec para establecer túneles IPSec están estandarizados.

IPSec (propiedad)	Parámetro
Algoritmo de cifrado Ike	AES 256
Algoritmo de integridad Ike	SHA 256
Grupo Dh	DH2
Algoritmo de cifrado IPSec	GCM AES 256
Algoritmo de integridad IPsec	GCM AES 256
Grupo PFS	None (Ninguno)

Azure Virtual WAN automatiza la conectividad entre la red virtual de carga de trabajo y el concentrador. Cuando se crea una conexión de red virtual de concentrador, establece la configuración adecuada entre el concentrador aprovisionado y la red virtual de cargas de trabajo (VNET).

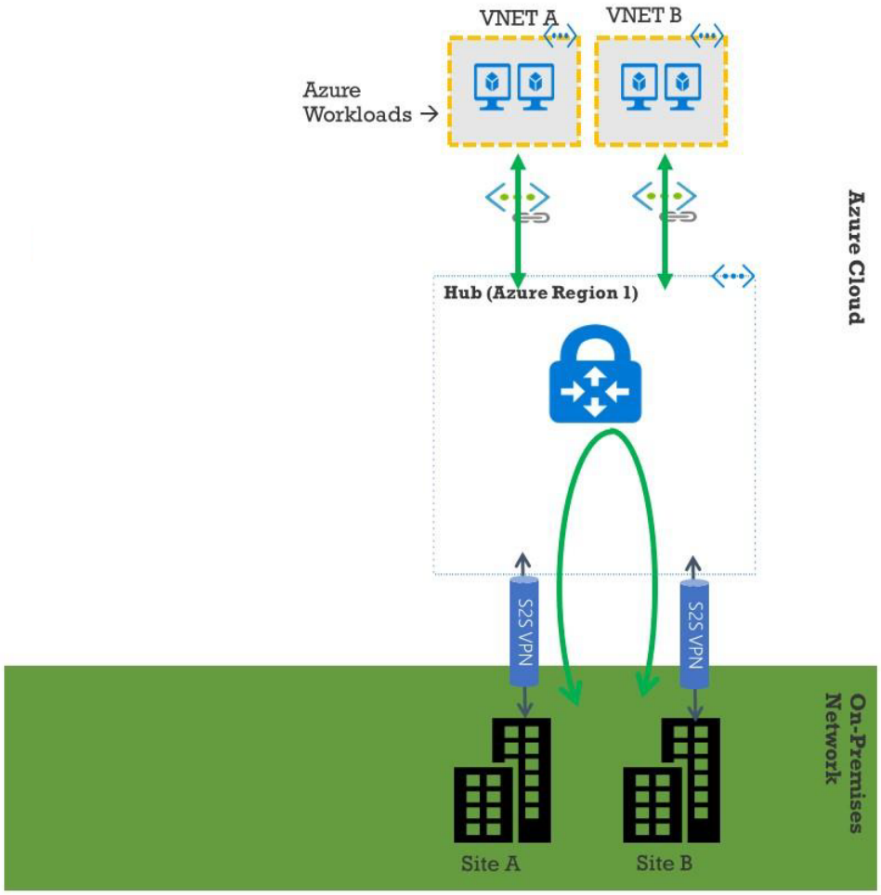
Requisitos previos y requisitos

Lea los siguientes requisitos antes de continuar con la configuración de Azure y SD-WAN para administrar sitios de ramas que se conectan a concentradores de Azure.

1. Tener una suscripción a Azure en la lista de permitidos para Virtual WAN.
2. Disponer de un dispositivo local como, por ejemplo, un dispositivo SD-WAN para establecer IPSec en recursos de Azure.
3. Tener enlaces a Internet con direcciones IP públicas. Aunque un único vínculo a Internet es suficiente para establecer la conectividad con Azure, necesita dos túneles IPSec para utilizar el mismo vínculo WAN.
4. Controlador SD-WAN: un controlador es la interfaz responsable de configurar los dispositivos SD-WAN para conectarse a Azure.
5. Una VNET en Azure que tiene al menos una carga de trabajo. Por ejemplo, una máquina virtual, que aloja un servicio. Tenga en cuenta los siguientes puntos:

    a) La red virtual no debe tener una puerta de enlace VPN o Express Route de Azure, ni un dispositivo virtual de red.
    b) La red virtual no debe tener una ruta definida por el usuario, que enruta el tráfico a una red virtual WAN no virtual para la carga de trabajo a la que se accede desde la rama local.
    c) Deben configurarse los permisos adecuados para acceder a la carga de trabajo. Por ejemplo, acceso SSH del puerto 22 para una máquina virtual ubuntu.

El siguiente diagrama ilustra una red con dos sitios y dos redes virtuales en Microsoft Azure.



Configurar Microsoft Azure Virtual WAN

Para que las ramas SD-WAN locales se conecten a Azure y tengan acceso a los recursos a través de túneles IPSec, deben completarse los siguientes pasos.

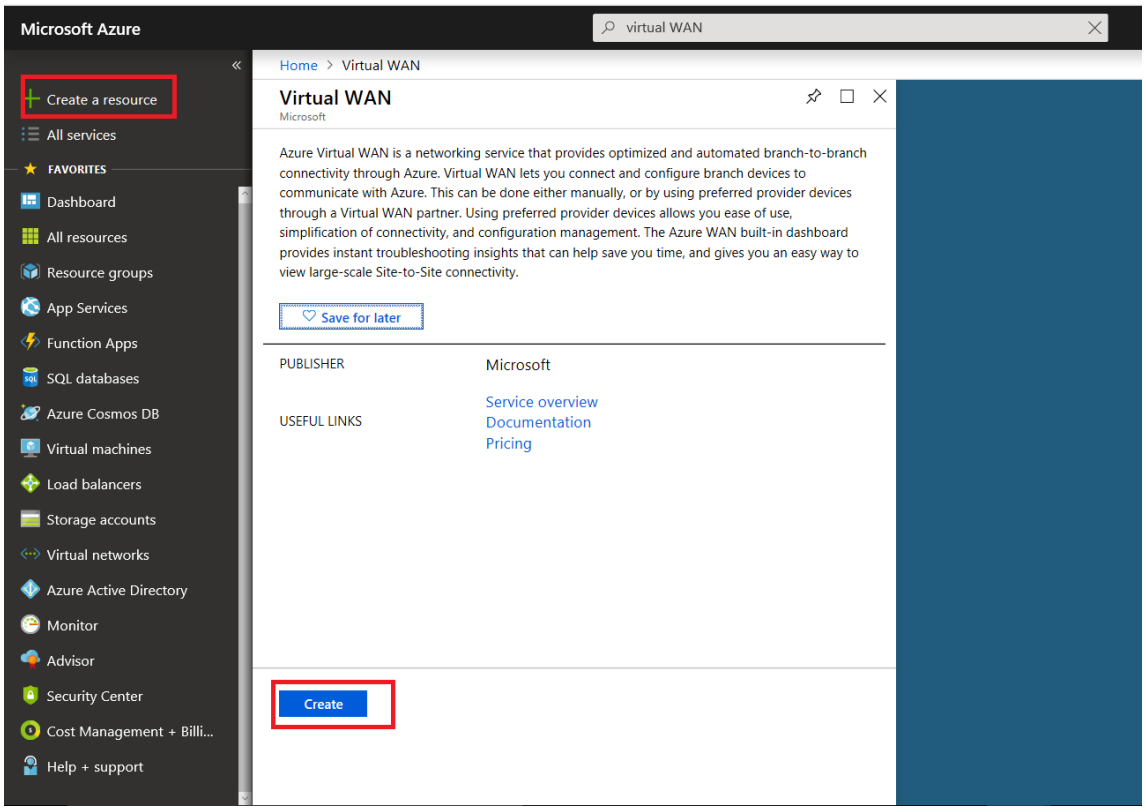
1. Configuración de recursos WAN.
2. Habilitar las ramas SD-WAN para conectarse a Azure mediante túneles IPSec.

Configure la red de Azure antes de configurar la red SD-WAN, ya que los recursos de Azure necesarios para conectarse a dispositivos SD-WAN deben estar disponibles de antemano. Sin embargo, puede configurar la configuración de SD-WAN antes de configurar los recursos de Azure, si lo prefiere. En este tema se analiza la configuración de la red Azure Virtual WAN antes de configurar los dispositivos SD-WAN. https://microsoft.com Azure virtual-wan.

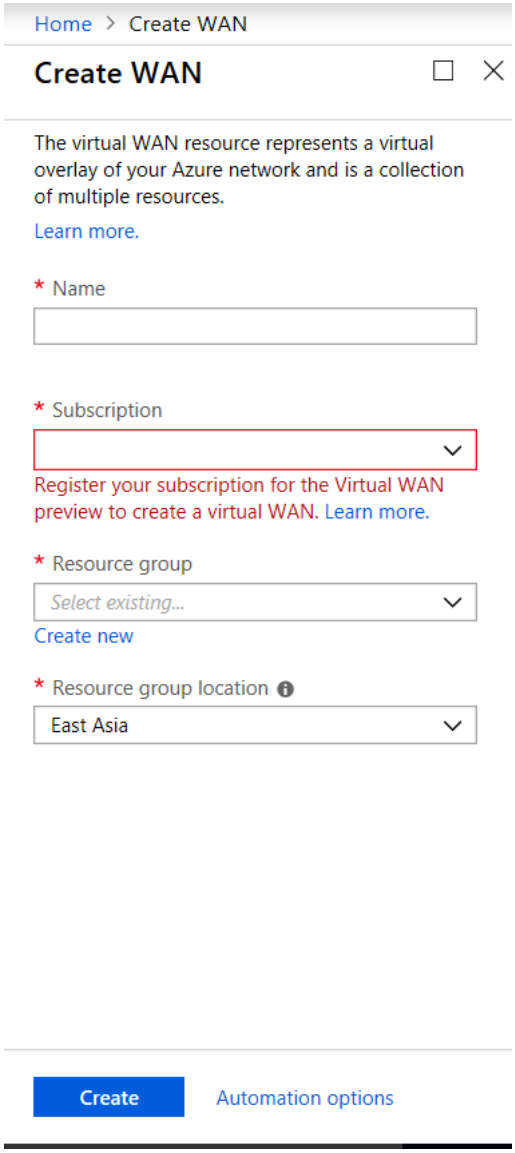
Crear un recurso WAN

Para utilizar las funciones de WAN virtual y conectar el dispositivo de rama local en Azure:

1. Inicie sesión en Azure Marketplace, vaya a la aplicación WAN virtual y seleccione **Crear WAN**.



2. Introduzca un nombre para la WAN y seleccione la suscripción que desea utilizar para WAN.



3. Seleccione un grupo de recursos existente o cree un nuevo grupo de recursos. Los grupos de recursos son construcciones lógicas y el intercambio de datos entre grupos de recursos siempre es posible.
4. Seleccione la ubicación donde quiere que resida el grupo de recursos. WAN es un recurso global que no tiene una ubicación. Sin embargo, debe especificar una ubicación para el grupo de recursos que contenga metadatos para el recurso WAN.
5. Haga clic en **Crear**. Esto inicia el proceso para validar e implementar la configuración.

Crear sitio

Puede crear un sitio mediante un proveedor preferido. El proveedor preferido envía la información sobre su dispositivo y sitio a Azure o puede decidir administrar el dispositivo usted mismo. Si quiere

administrar el dispositivo, debe crear el sitio en Azure Portal.

Red SD-WAN y flujo de trabajo WAN virtual de Microsoft Azure

Configurar el dispositivo SD-WAN:

1. Aprovisionamiento de un dispositivo Citrix SD-WAN
    - Conecte el dispositivo de rama SD-WAN al dispositivo MCN.
2. Configurar el dispositivo SD-WAN
    - Configure los Servicios de Intranet para la conexión Active-Active.

Configurar el Centro de SD-WAN:

- Configure SD-WAN Center para conectarse a Microsoft Azure.

Configurar la configuración de Azure:

- Proporcione ID de arrendatario, ID de cliente, clave segura, ID de suscriptor y grupo de recursos.

Configurar asociación de sitio de rama a WAN:

1. Asocie un recurso WAN a una rama. El mismo sitio no se puede conectar a varias WAN.
2. Haga clic en **Nuevo** para configurar la asociación Site-WAN.
3. Seleccione **Recursos WAN de Azure**.
4. Seleccione **Servicios** (Intranet) para el sitio. Seleccione dos servicios para la compatibilidad con Active-Standby.
5. Seleccione **Nombres de sitio** que quiere asociar a los recursos de WAN.
6. Haga clic en **Implementar** para confirmar la asociación.
7. Espere a que el estado cambie a **Túneles implementados** para ver la configuración del **túnel IPSec**.
8. Utilice la vista Informes de SD-WAN Center para comprobar el estado de los respectivos túneles IPSec.

Configurar la red de Citrix SD-WAN

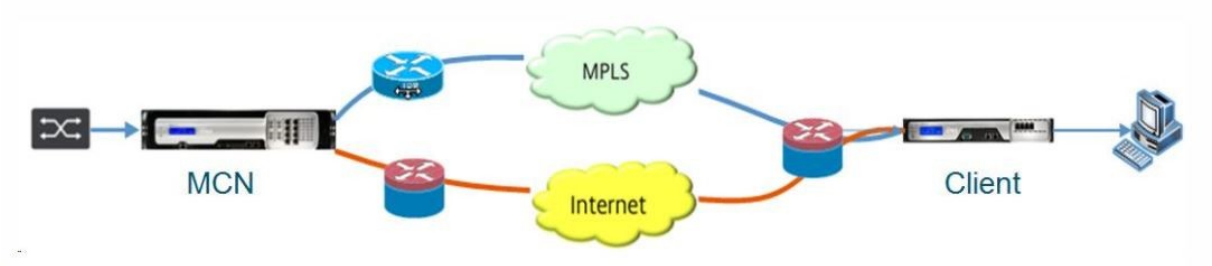
MCN:

El MCN sirve como punto de distribución para la configuración inicial del sistema y los cambios de configuración posteriores. Solo puede haber un MCN activo en una WAN virtual.
De forma predeterminada, los dispositivos tienen la función de cliente asignada previamente. Para establecer un dispositivo como MCN, primero debe agregar y configurar el sitio como MCN. La interfaz gráfica de usuario de configuración de red está disponible después de configurar un sitio como MCN.

Las actualizaciones y los cambios de configuración deben realizarse únicamente desde el centro MCN o SD-WAN.

Función del MCN:

El MCN es el nodo central que actúa como el controlador de una red SD-WAN y el punto de administración central de los nodos cliente. Todas las actividades de configuración, además de la preparación de paquetes de firmware y su distribución a los clientes, se configuran en el MCN. Además, la información de supervisión solo está disponible en el MCN. El MCN puede supervisar toda la red SD-WAN, mientras que los nodos de cliente solo pueden supervisar las Intranets locales y cierta información para esos clientes, a los que están conectados. El objetivo principal del MCN es establecer conexiones superpuestas (rutas virtuales) con uno o más nodos de cliente ubicados en la red SD-WAN para la comunicación de sitio a sitio empresarial. Un MCN puede administrar y tener rutas virtuales a varios nodos cliente. Puede haber más de un MCN, pero solo uno puede estar activo en un momento dado. La siguiente ilustración ilustra el diagrama básico de los dispositivos MCN y cliente (nodo de rama) para una red pequeña de dos sitios.



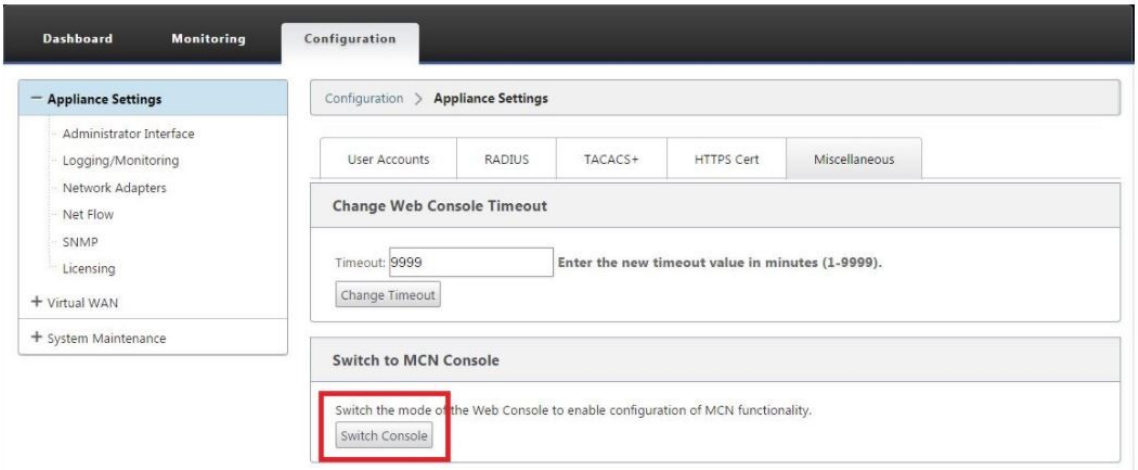
Configurar el dispositivo SD-WAN como MCN

Para agregar y configurar el MCN, primero debe iniciar sesión en la Interfaz Web de administración del dispositivo que está designando como MCN y cambiar la Interfaz Web de administración al modo de consola de MCN. El modo Consola de MCN permite el acceso al Editor de configuración en la Interfaz Web de administración a la que está conectado actualmente. A continuación, puede utilizar el Editor de configuración para agregar y configurar el sitio MCN.

Para cambiar la Interfaz Web de administración al modo Consola MCN, haga lo siguiente:

1. Inicie sesión en la interfaz web de administración de SD-WAN del dispositivo que quiere configurar como MCN.
2. Haga clic en **Configuración** en la barra de menú principal de la pantalla principal de la interfaz web de administración (barra azul en la parte superior de la página).
3. En el árbol de navegación (panel izquierdo), abra la **rama Configuración del equipo** y haga clic en **Interfaz de administrador**.

4. Selecciona la ficha **Miscellaneous (Miscellaneous**). Se abrirá la página de configuración administrativa de varios.



   En la parte inferior de la ficha **Varios** se encuentra la sección **Cambiar a [cliente, Consola de MCN]**. Esta sección contiene el botón **Conmutador de consola** para alternar entre los modos de consola del dispositivo.

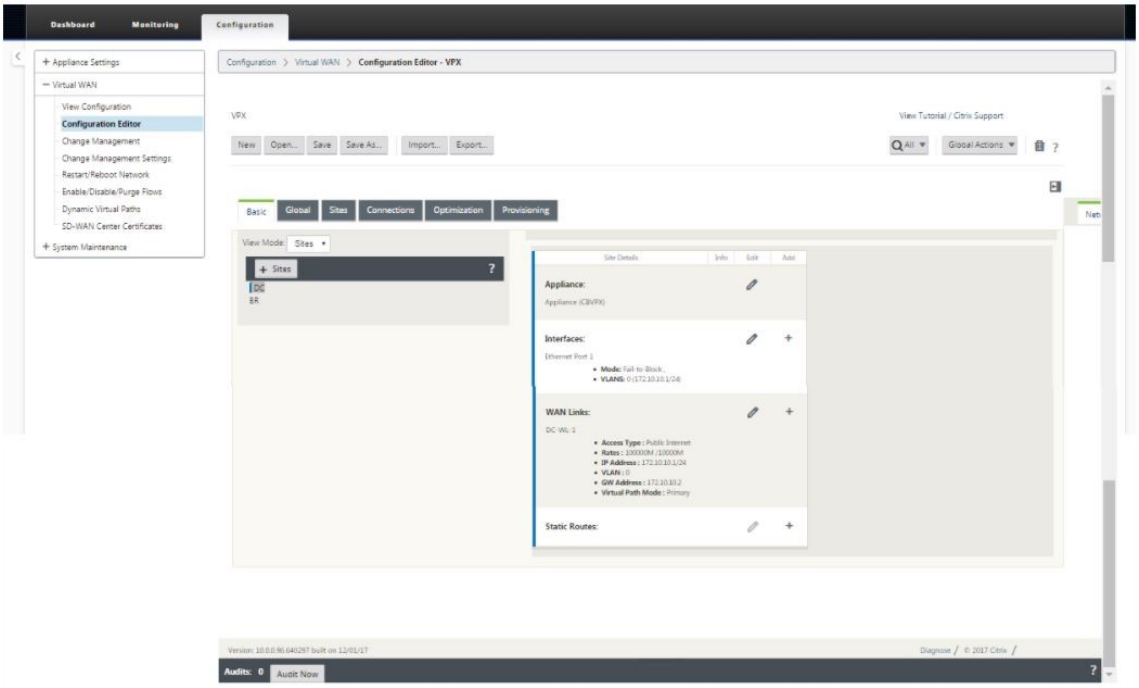
El encabezado de la sección indica el modo de consola actual, de la siguiente manera:

- En el modo Consola de cliente (predeterminado), el encabezado de la sección es Cambiar a consola MCN.
- En el modo Consola MCN, el encabezado de la sección es Cambiar a consola cliente.

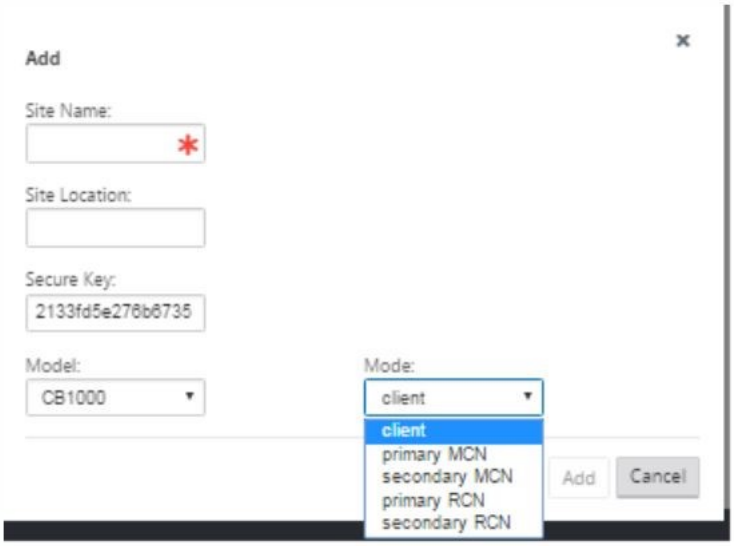
De forma predeterminada, un nuevo dispositivo se encuentra en el modo Consola de cliente. El modo Consola MCN habilita la vista Editor de configuración en el árbol de navegación. El Editor de configuración solo está disponible en el dispositivo MCN.

Configurar MCN Para agregar y comenzar a configurar el sitio del dispositivo MCN, haga lo siguiente:

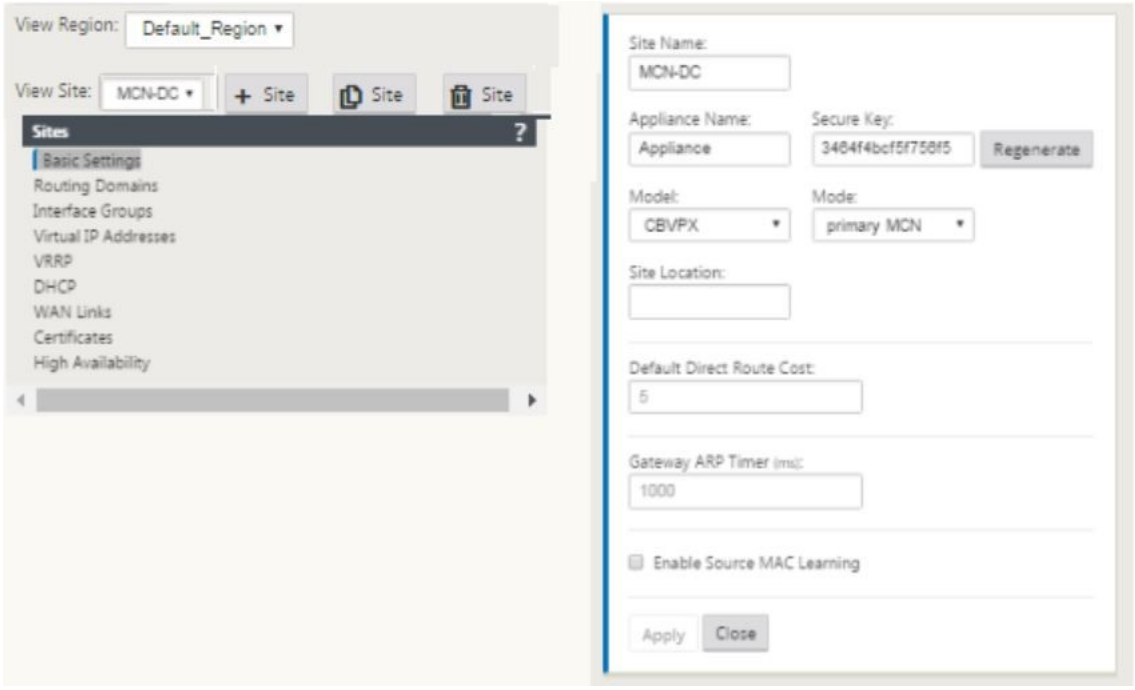
1. En la GUI del dispositivo SD-WAN, vaya a **Virtual WAN** > **Configuration Editor**.



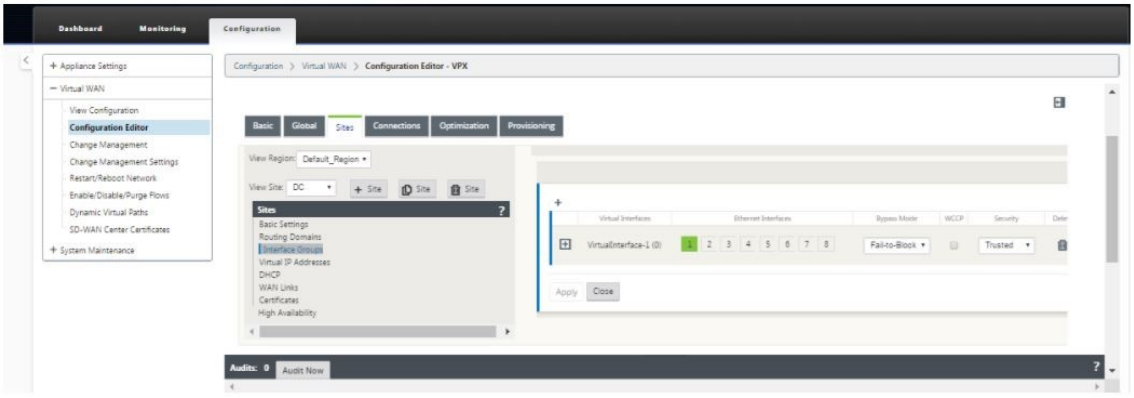
2. Haga clic en **+ Sitios** en la barra Sitios para comenzar a agregar y configurar el sitio MCN. Aparece el cuadro de diálogo **Agregar sitio**.



3. Escriba un nombre de sitio que le permita determinar la ubicación geográfica y la función del dispositivo (DC o DC secundario). Seleccione el modelo de dispositivo correcto. La selección del dispositivo correcto es crucial, ya que las plataformas de hardware difieren entre sí en términos de potencia de procesamiento y licencias. Dado que estamos configurando este dispositivo como el dispositivo final principal, elija el modo como MCN principal y haga clic en **Agregar**.
4. Esto agrega el nuevo sitio al árbol de sitios y la vista predeterminada muestra la página de configuración de configuración básica como se muestra a continuación:

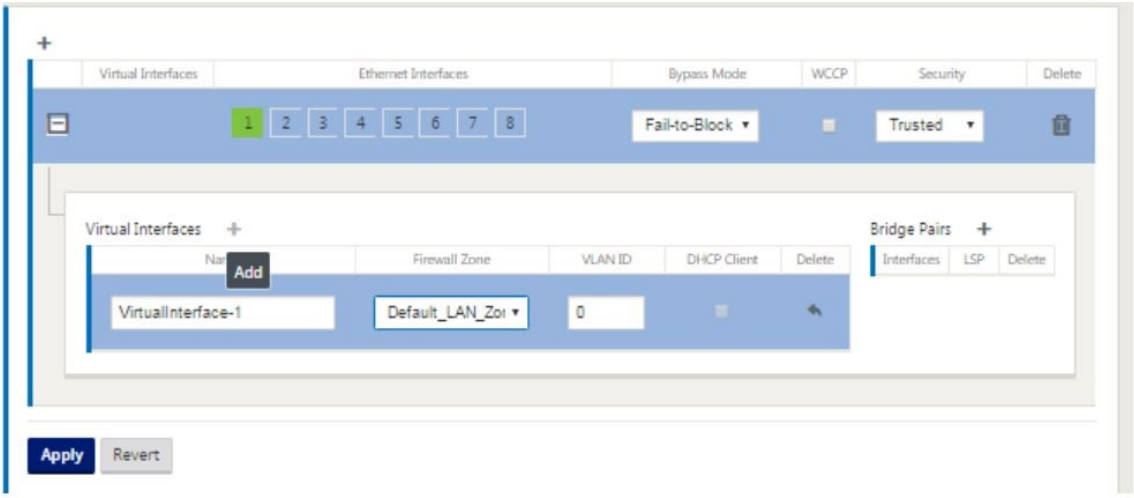


5. Introduzca la configuración básica, como la ubicación, el nombre del sitio.
6. Configure el dispositivo para que pueda aceptar tráfico de Internet/MPLS/banda ancha. Defina las interfaces donde terminan los enlaces. Esto depende de si el dispositivo está en modo superposición o calco subyacente.
7. Haga clic en **Grupos de interfaces** para comenzar a definir las interfaces.

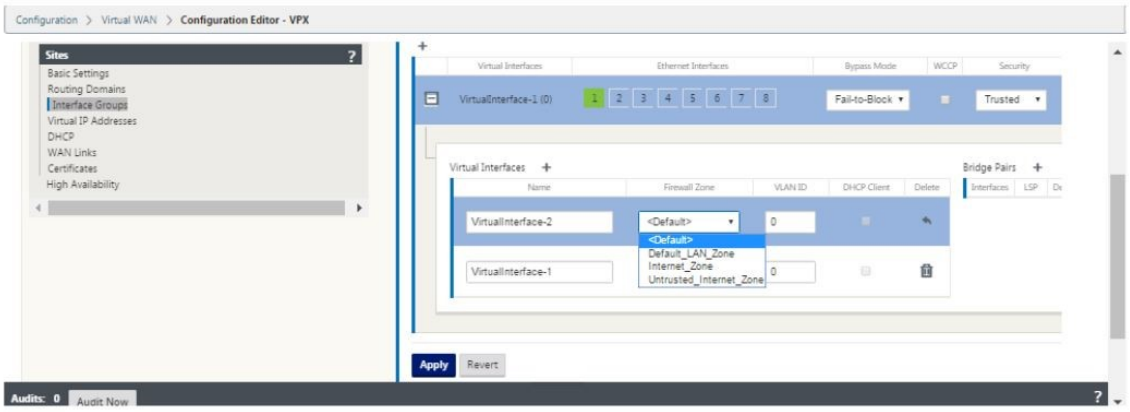


8. Haga clic en + para agregar grupos de interfaces virtuales. Esto agrega un nuevo grupo de interfaces virtuales, el número de interfaces virtuales depende de los vínculos que quiera que gestione el dispositivo. El número de vínculos que puede manejar un dispositivo varía de un modelo a otro y el número máximo de vínculos puede ser de hasta ocho.

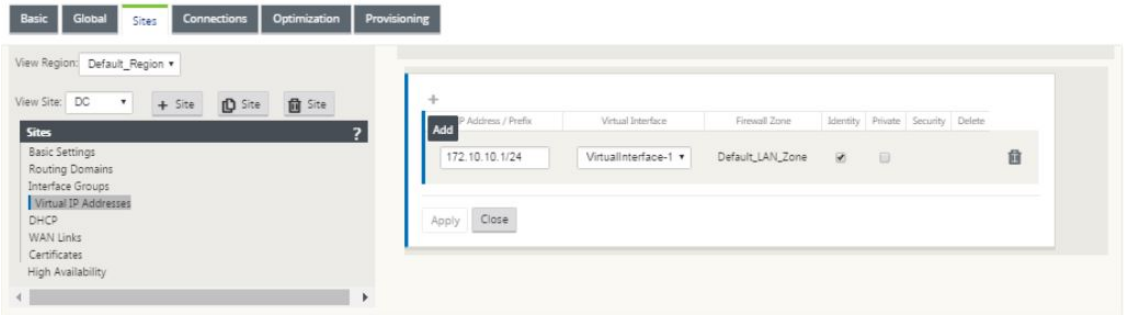
9. Haga clic en + a la derecha de las interfaces virtuales para ver la pantalla como se muestra a continuación.

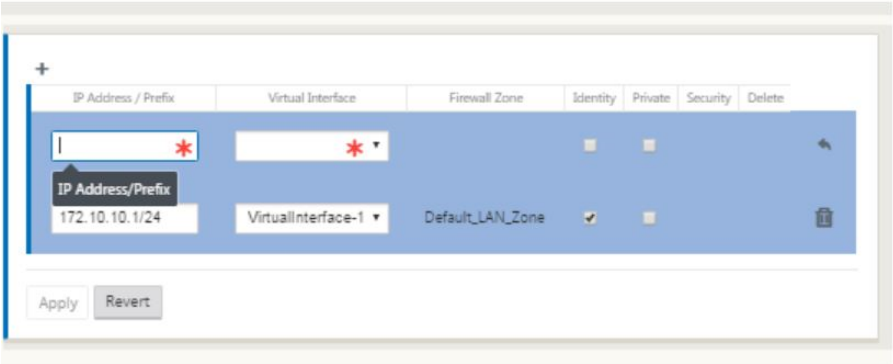


10. Seleccione las **interfaces Ethernet**, que forman parte de esta interfaz virtual. Dependiendo del modelo de plataforma, los dispositivos tienen un par preconfigurado de interfaces de error a cable. Si quiere habilitar la conmutación por error en los dispositivos, asegúrese de que está eligiendo el par correcto de interfaces y asegúrese de elegir la conmutación por error en la columna **Modo de derivación**.
11. Seleccione el nivel de seguridad en la lista desplegable. Se elige el modo de confianza, si la interfaz sirve enlaces MPLS y no fiable se elige cuando se utilizan vínculos de Internet en las interfaces respectivas.
12. Haga clic en + a la derecha de la etiqueta denominada interfaces virtuales. Esto muestra el nombre, la zona del firewall y los ID de VLAN. Introduzca el **nombre y el ID de VLAN** para este grupo de interfaces virtuales. El ID de VLAN se utiliza para identificar y marcar el tráfico hacia y desde la interfaz virtual, utilice 0 (cero) para el tráfico nativo/no etiquetado.

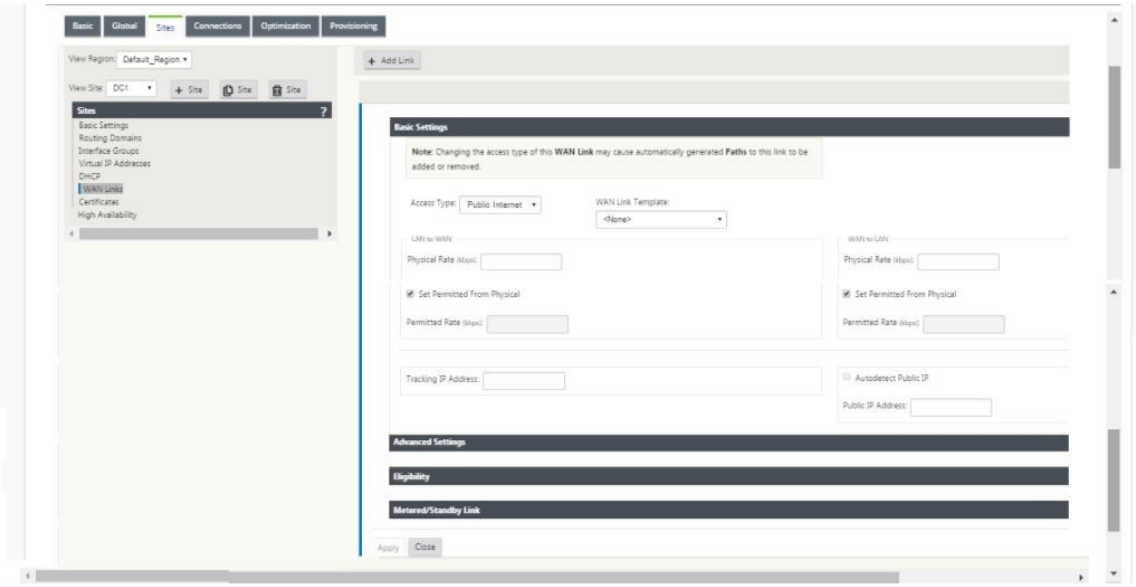


13. Para configurar las interfaces en error de cableado, haga clic en Pares de puente. Esto agrega un nuevo par de puentes y permite la edición. Haga clic en **Aplicar** para confirmar esta configuración.
14. Para agregar más grupos de interfaces virtuales, haga clic en + a la derecha de la rama de grupos de interfaz y continúe como se indica anteriormente.
15. Una vez elegidas las interfaces, el siguiente paso es configurar las direcciones IP en estas interfaces. En la terminología Citrix SD-WAN, esto se conoce como VIP (IP virtual).
16. Continúe en la vista de sitios y haga clic en la dirección IP virtual para ver las interfaces para configurar VIP.

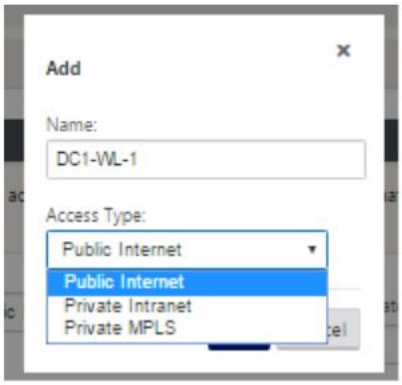




17. Introduzca la información Dirección IP/ Prefijo y seleccione la **Interfaz Virtual** con la que está asociada la dirección. La dirección IP virtual debe incluir la dirección de host completa y la máscara de red. Seleccione la configuración deseada para la dirección IP virtual, como Zona de firewall, Identidad, Privada y Seguridad. Haga clic en **Aplicar**. Esto agrega la información de dirección al sitio y la incluye en la tabla Direcciones IP virtuales del sitio. Para agregar más direcciones IP virtuales, haga clic en + a la derecha de las Direcciones IP virtuales y continúe como se indica anteriormente.
18. Continúe en la sección Sitios para configurar vínculos WAN para el sitio.

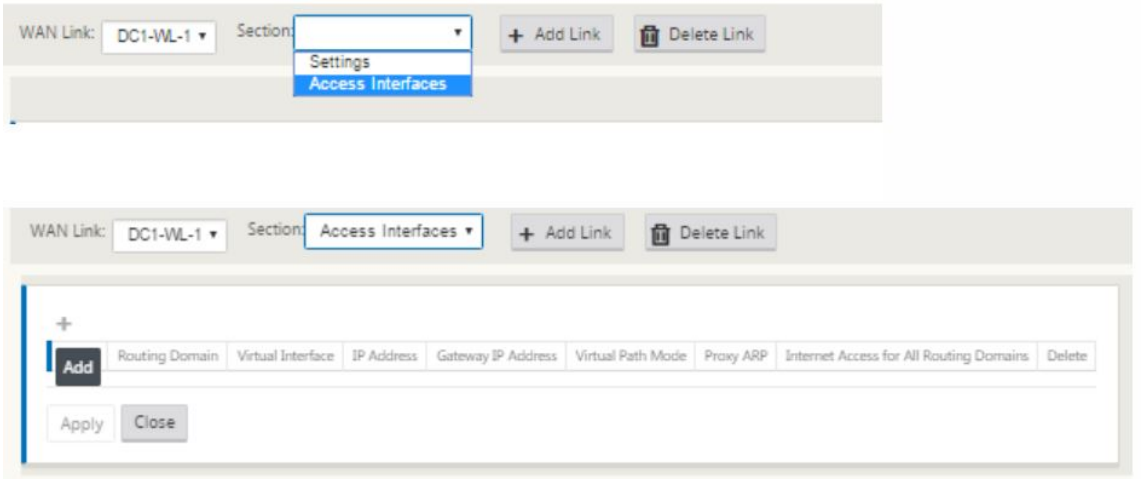


19. Haga clic en **Agregar vínculo**, en la parte superior del panel a la derecha. Esto abre un cuadro de diálogo, que le permite elegir el tipo de vínculo que se va a configurar.



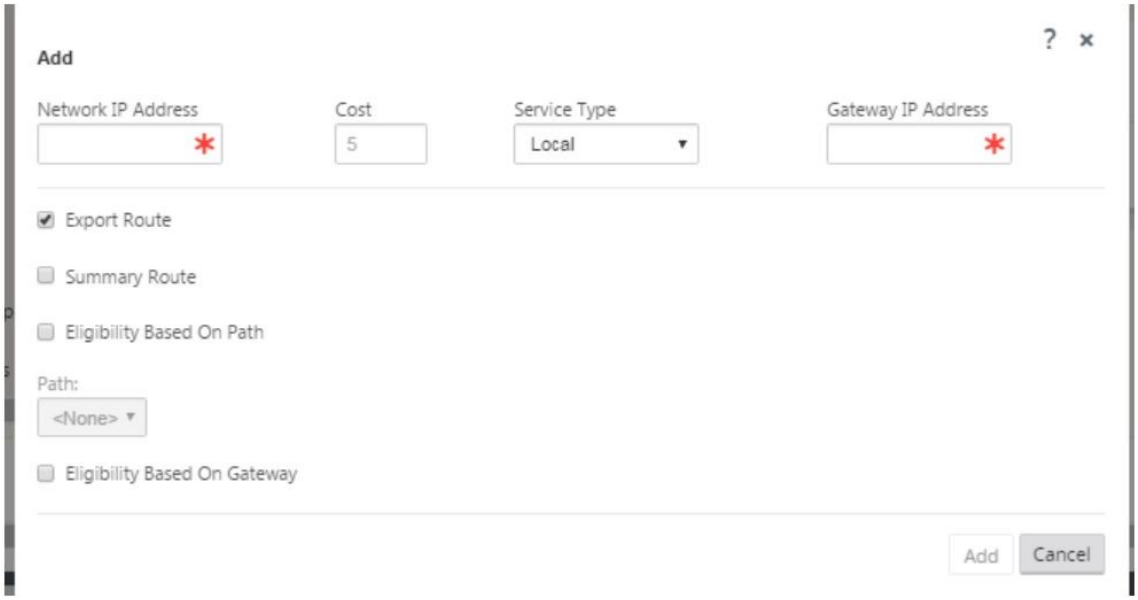
20. Internet público es para enlaces de Internet/gran ancho de banda/DSL/ADSL, mientras que MPLS privado es para enlaces MPLS. Intranet privada también es para enlaces MPLS. La diferencia entre MPLS privados y los vínculos de Intranet privados es que MPLS privados permite preservar las directivas de QoS de los enlaces MPLS.

21. Si elige Internet público y las IP se asignan a través de DHCP, elija la opción de detección automática de IP.
22. Seleccione **Interfaces de Acceso** en la página de configuración de vínculos WAN. Esto abre la vista Interfaces de acceso para el sitio. Agregue y configure el VIP y la IP de la puerta de enlace para cada uno de los enlaces como se muestra a continuación.



23. Haga clic en **+** para agregar una interfaz. Esto agrega una entrada en blanco a la tabla y la abre para modificarla.
24. Introduzca el nombre que quiere asignar a esta interfaz. Puede elegir asignarle un nombre según el tipo de vínculo y la ubicación. Mantenga el dominio de enrutamiento como predeterminado si no quiere segregar redes y asignar una IP a la interfaz.
25. Asegúrese de proporcionar una dirección IP de puerta de enlace accesible públicamente si el enlace es un enlace a Internet o una IP privada si el enlace es un enlace MPLS. Mantenga el modo de ruta virtual como principal, ya que necesita este vínculo para formar la ruta virtual.

    Nota: Habilite el ARP proxy a medida que el dispositivo responda a las solicitudes ARP para la dirección IP de la puerta de enlace cuando no se pueda acceder a la puerta de enlace.
26. Haga clic en **Aplicar** para finalizar la configuración del vínculo WAN. Si quiere configurar más vínculos WAN, repita los pasos para otro vínculo.
27. Configurar rutas para el sitio. Haga clic en Vista Conexiones y seleccione rutas.
28. Haga clic en + para agregar rutas, se abrirá un cuadro de diálogo como se muestra a continuación.

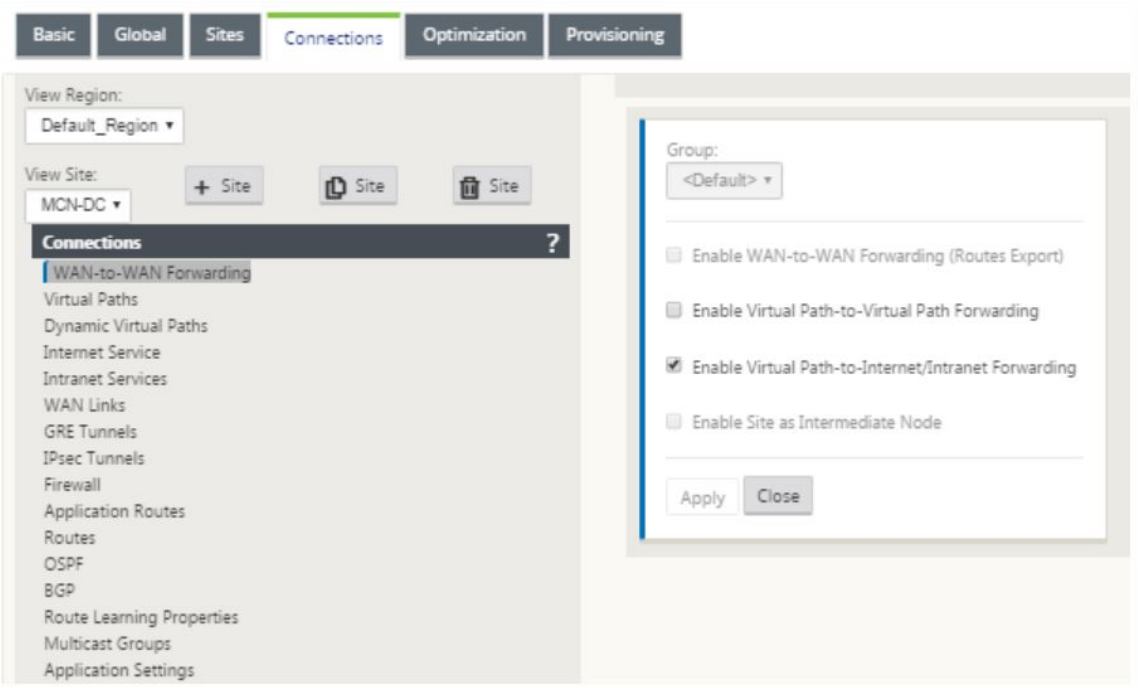


29. Introduzca la siguiente información disponible para la nueva ruta:
    - Dirección IP de red
    - Coste: el coste determina qué ruta tiene prioridad sobre la otra. Las rutas con costes más bajos tienen prioridad sobre las rutas de mayor coste. El valor predeterminado es cinco.
    - Tipo de servicio: seleccione el servicio, un servicio puede ser cualquiera de los siguientes:
        - Ruta virtual
        - Intranet
        - Internet
        - Paso a través
        - Locales
        - Túnel GRE
        - Túnel IPsec LAN
30. Haga clic en **Aplicar**.

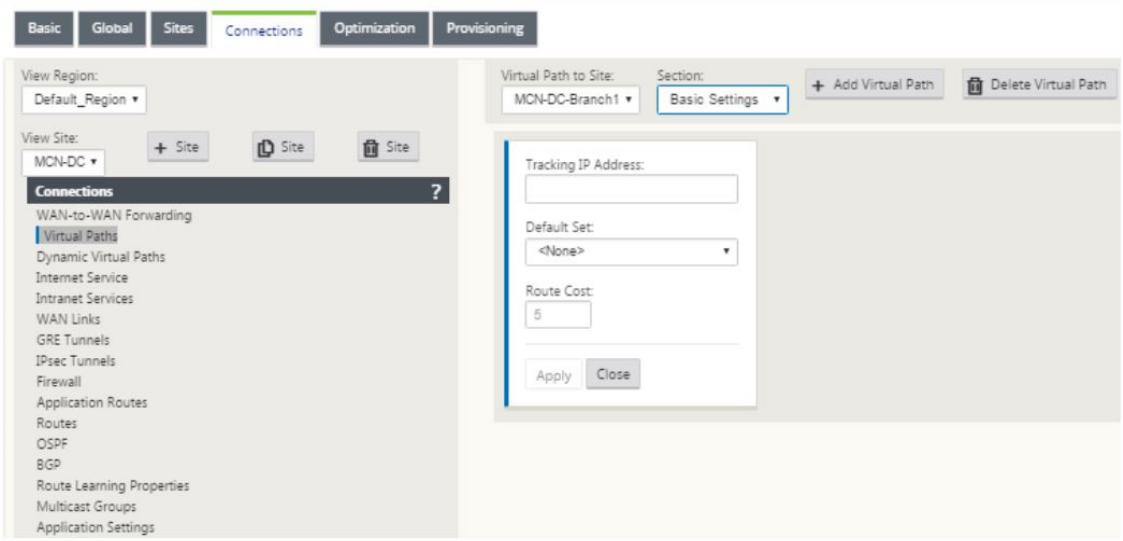
Para agregar más rutas para el sitio haga clic en + a la derecha de la rama de rutas y proceda como arriba. Para obtener más información, consulte Configurar MCN.

Configurar ruta virtual entre MCN y sitios de rama Establezca conectividad entre el MCN y el nodo de rama. Puede hacerlo configurando una ruta virtual entre estos dos sitios. Vaya a la ficha **Conexiones** en el árbol de configuración del editor de configuración.

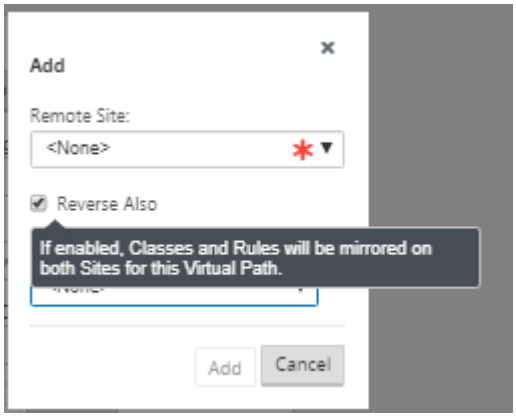
1. Haga clic en la ficha **Conexiones** en la sección de configuración. Esto muestra la sección de conexiones del árbol de configuración.
2. Seleccione el **MCN** desde el menú desplegable del sitio de vista en la página de sección de **conexiones**.



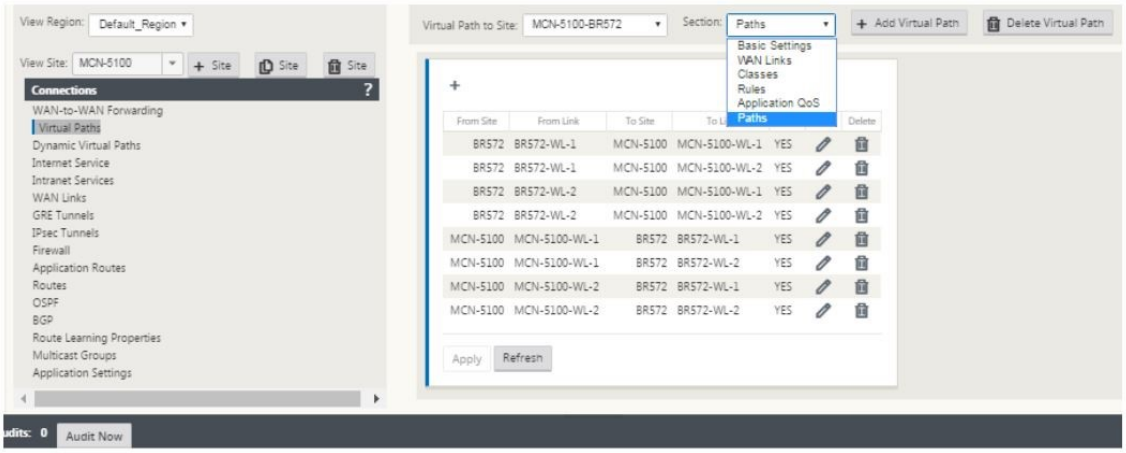
3. Seleccione la ruta virtual en la ficha Conexiones para crear la ruta virtual entre los sitios de MCN y rama.



4. Haga clic en **Agregar ruta virtual** junto al nombre de la ruta virtual estática en la sección Rutas virtuales. Esto abre un cuadro de diálogo como se muestra a continuación. Elija la rama para la que quiere configurar la ruta de acceso virtual. Debe configurarlo bajo la etiqueta denominada sitio remoto. Seleccione el nodo de bifurcación en esta lista desplegable y haga clic en la casilla de verificación **Invertir también**.



La clasificación y la dirección del tráfico se reflejan en ambos sitios de la ruta virtual. Una vez completado esto, seleccione rutas en el menú desplegable debajo de la etiqueta llamada sección como se muestra a continuación.



5. Haga clic en **+ Agregar** encima de la tabla de rutas, que muestra el cuadro de diálogo Agregar ruta. Especifique los puntos finales dentro de los cuales se debe configurar la ruta virtual. Ahora, haga clic en **Agregar** para crear la ruta y haga clic en la **casilla Invertir también**.

   Nota: Citrix SD-WAN mide la calidad del enlace en ambas direcciones. Esto significa que el punto A al punto B es una ruta y el punto B al punto A es otro ruta. Con la ayuda de la medición unidireccional de las condiciones de enlace, la SD-WAN es capaz de elegir la mejor ruta para enviar tráfico. Esto es diferente de medidas como RTT, que es una métrica bidireccional para medir la latencia. Por ejemplo, una conexión entre el punto A y el punto B se muestra como dos rutas y para cada una de ellas las métricas de rendimiento del vínculo se calculan de forma independiente.

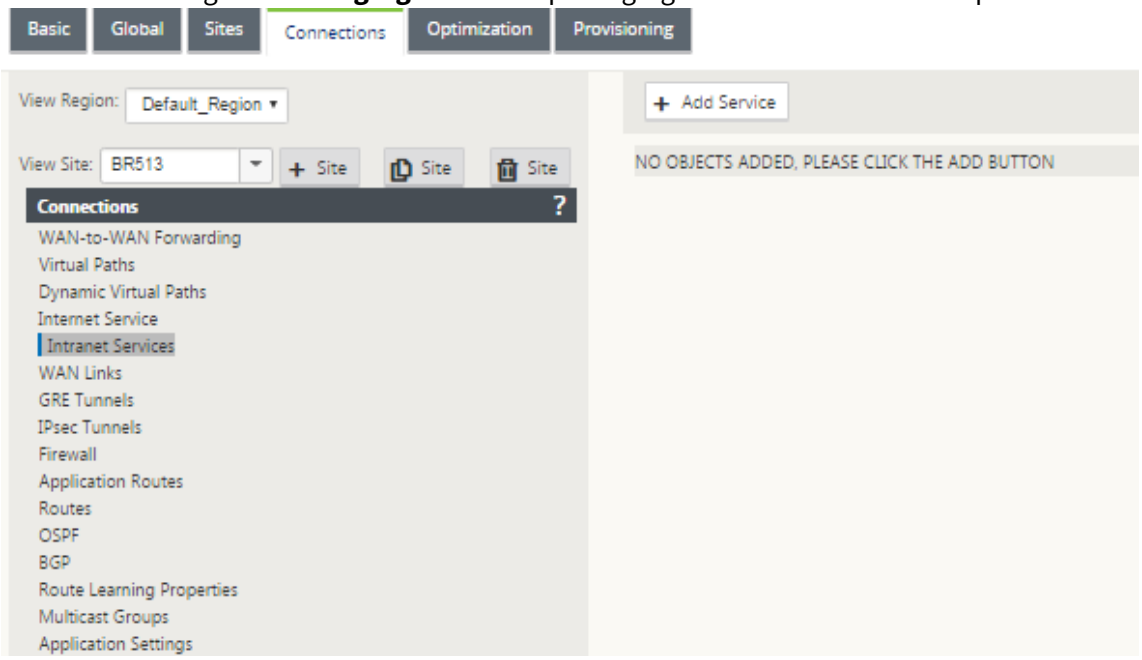
Esta configuración es suficiente para subir las rutas virtuales entre el MCN y la rama, otras opciones de configuración también están disponibles. Para obtener más información, consulte Configurar el servicio de rutas virtuales entre sitios de MCN y clientes.

Implementar configuración de MCN El siguiente paso es implementar la configuración. Esto implica los dos pasos siguientes:

1. Exporte el paquete de configuración de SD-WAN a Change Management.
    - Antes de generar los paquetes del dispositivo, primero debe exportar el paquete de configuración completo del **Editor de configuración** a la bandeja de entrada provisional de **administración de cambios** global del MCN. Consulte los pasos proporcionados en la sección Realizar la administración de cambios.
2. Generar y organizar los paquetes del dispositivo.
    - Después de agregar el nuevo paquete de configuración a la bandeja de entrada de Administración de cambios, puede generar y poner en escena los paquetes del dispositivo en los sitios de rama. Para ello, utilice el Asistente para administración de cambios en la interfaz web de administración en el MCN. Consulte los pasos proporcionados en la sección Poner paquetes de dispositivos en el entorno de ensayo.

Configurar servicios de intranet para conectarse con recursos WAN de Azure

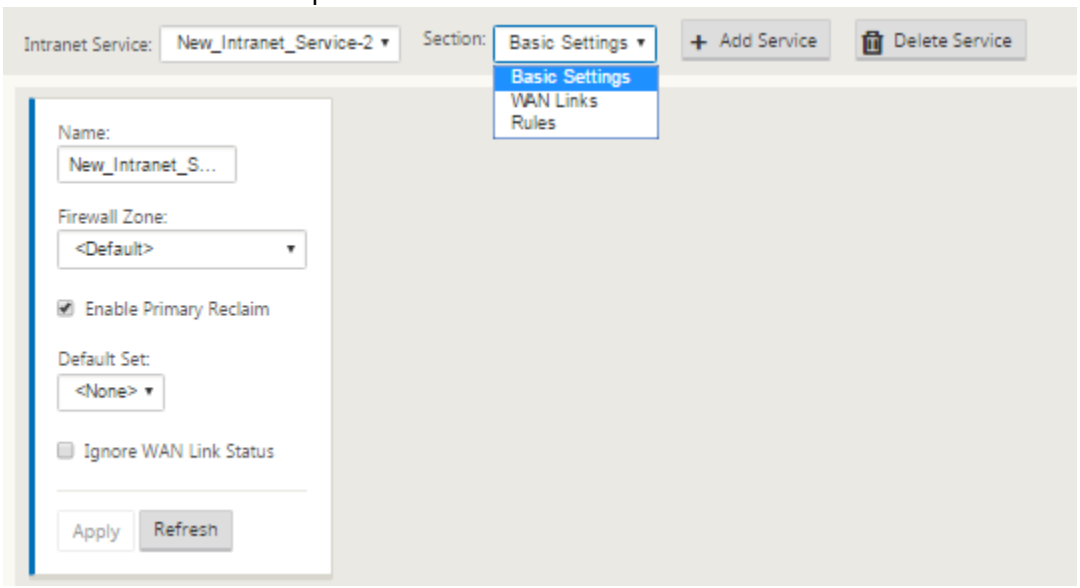
1. En la GUI del dispositivo SD-WAN, vaya al **Editor de configuración**y desplácese hasta el icono **Conexiones** . Haga clic en **+ Agregar servicio** para agregar un servicio de intranet para ese sitio.



2. En **Configuración básica** del servicio de intranet, hay varias opciones sobre cómo quiere que el servicio de intranet se comporte durante la falta de disponibilidad de vínculos WAN.
    - **Habilitar recuperación primaria**: Marque esta casilla si quiere que el enlace principal elegido se haga cargo cuando aparezca después de fallar. Sin embargo, si elige no marcar

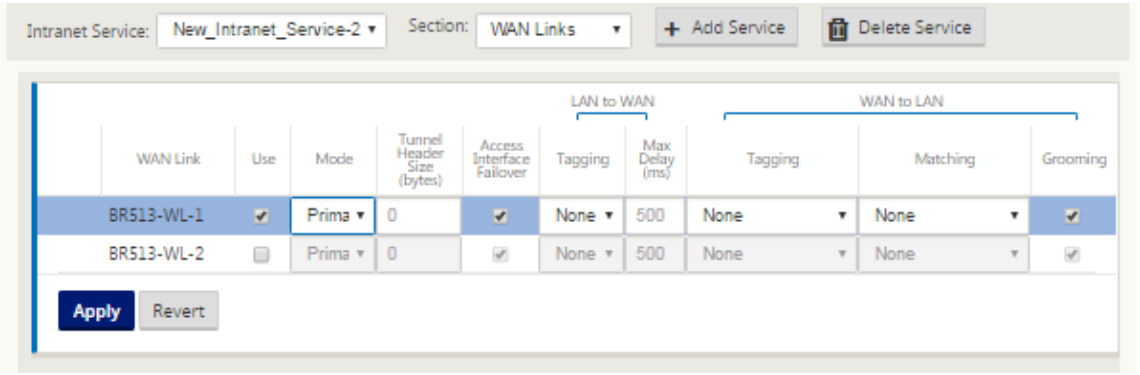
esta opción, el enlace secundario continuará enviando tráfico.

- **Ignorar estado del vínculo WAN**: Si esta opción está habilitada, los paquetes destinados a este servicio de intranet seguirán mediante este servicio aunque los vínculos WAN constitutivos no estén disponibles.



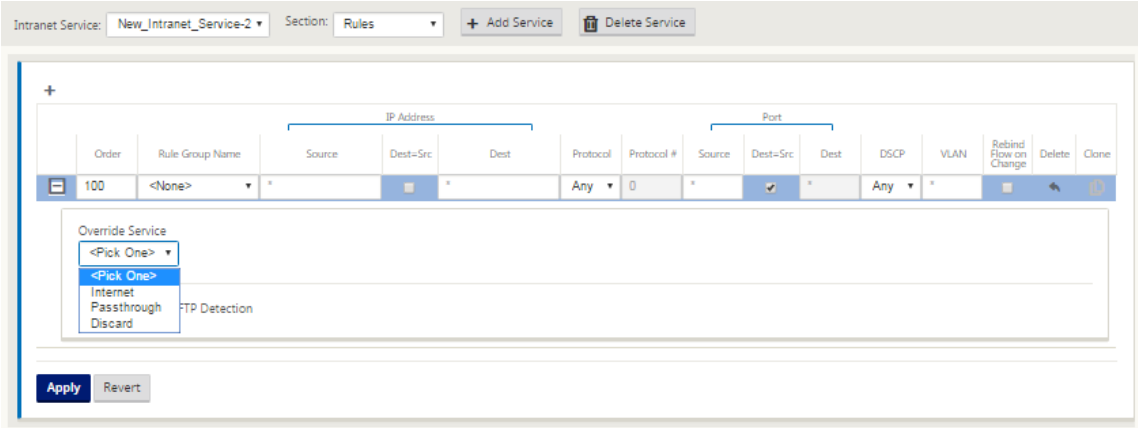
3. Después de configurar los parámetros básicos, el siguiente paso es elegir los vínculos WAN constitutivos para este servicio. Se eligen dos enlaces como máximo para un servicio de Intranet. Para elegir los vínculos WAN, seleccione la opción Vínculos WAN de la lista desplegable denominada Sección. Los vínculos WAN funcionan en modo primario y secundario y solo se elige un vínculo WAN principal.

   Nota: Cuando se crea un segundo servicio de intranet, debe tener la asignación de enlace wan-link primario y secundario.

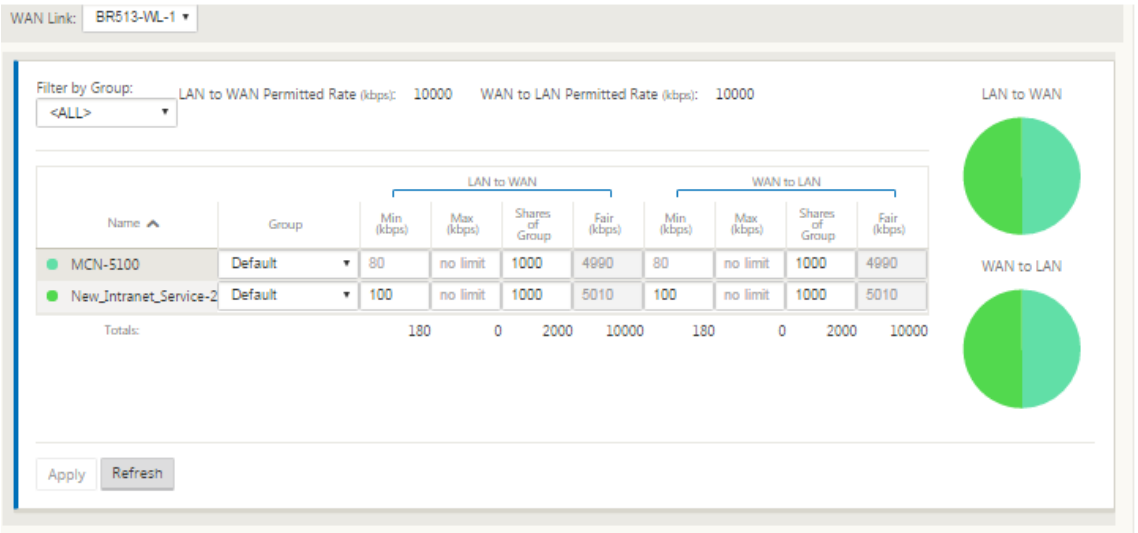


4. Las reglas específicas del sitio de rama están disponibles, lo que permite personalizar cada sitio de rama sobrescribiendo de forma única cualquier configuración general configurada en el conjunto predeterminado global. Los modos incluyen la entrega deseada a través de un enlace WAN específico o como un servicio de anulación que permite pasar o descartar el tráfico filtrado. Por ejemplo, si hay algo de tráfico, que no desea pasar por el servicio de intranet, puede escribir

una regla para descartar ese tráfico o enviarlo a través de un servicio diferente (Internet o pasar a través).

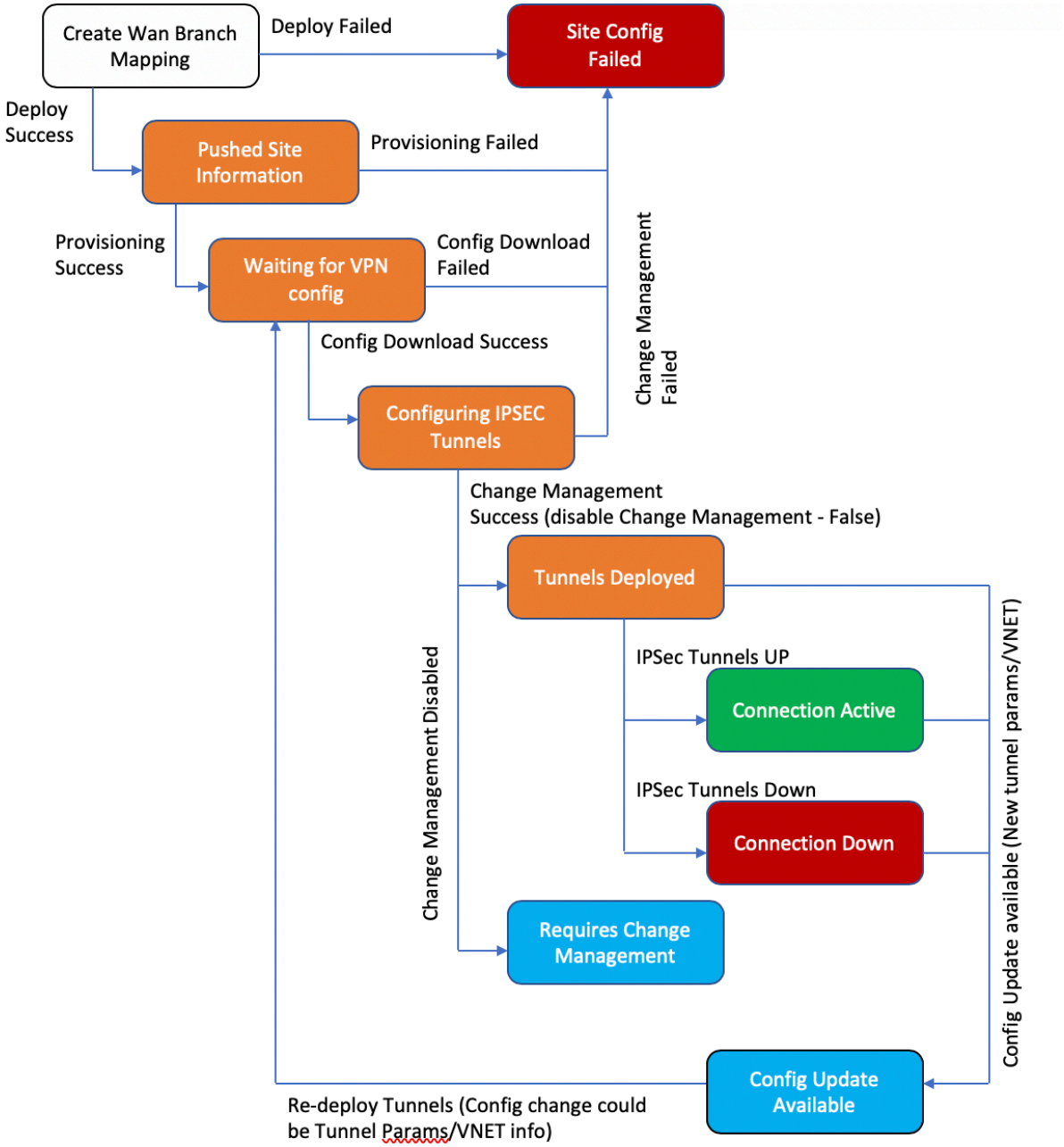


5. Con el Servicio de Intranet habilitado para un sitio, el mosaico **Provisioning** está disponible para permitir la distribución bidireccional (LAN a WAN/WAN a LAN) del ancho de banda para un enlace WAN entre los diversos servicios que utilizan el enlace WAN. La sección **Servicios** le permite ajustar aún más la asignación de ancho de banda. Además, se puede habilitar el reparto justo, permitiendo que los servicios reciban su ancho de banda mínimo reservado antes de que se promulguen las distribuciones justas.



Configurar el centro de SD-WAN

El siguiente diagrama describe el flujo de trabajo de alto nivel de SD-WAN Center y la conexión de Azure Virtual WAN y las transiciones de estado correspondientes de la implementación.



Configurar la configuración de Azure:

- Proporcione ID de arrendatario de Azure, ID de aplicación, clave secreta e identificador de

suscripción (también conocido como principal de servicio).

Configurar asociación de sitio de rama a WAN:

- Asociar un sitio de rama a un recurso WAN. El mismo sitio no se puede conectar a varias WAN.
- Haga clic en **Nuevo** para configurar la asociación Site-WAN.
- Seleccione **Recursos WAN de Azure**.
- Seleccione **Nombres de sitio** que desea asociar a los recursos WAN.
- Haga clic en **Implementar** para confirmar la asociación. Los vínculos WAN que se utilizarán para la implementación de túneles se rellenan automáticamente con el que tiene la mejor capacidad de enlace.
- Espere a que el estado cambie a"Túneles implementados'para ver la configuración del **túnel IPSec**.
- Utilice la vista Informes de SD-WAN Center para comprobar el estado de los respectivos túneles IPSec. El estado del túnel IPSec debe ser VERDE para que fluya el tráfico de datos, lo que indica que la conexión está activa.

Aprovisione SD-WAN Center:

El centro SD-WAN es la herramienta de gestión y generación de informes para Citrix SD-WAN. La configuración requerida para Virtual WAN se realiza en SD-WAN Center. El centro SD-WAN solo está disponible como factor de forma virtual (VPX) y debe instalarse en un hipervisor VMware ESXi o XenServer. Los recursos mínimos necesarios para configurar un dispositivo de SD-WAN Center son 8 GB de RAM y 4 núcleos de CPU. Estos son los pasos para instalar y configurar una máquina virtual de SD-WAN Center.

Configurar SD-WAN Center para conectividad de Azure

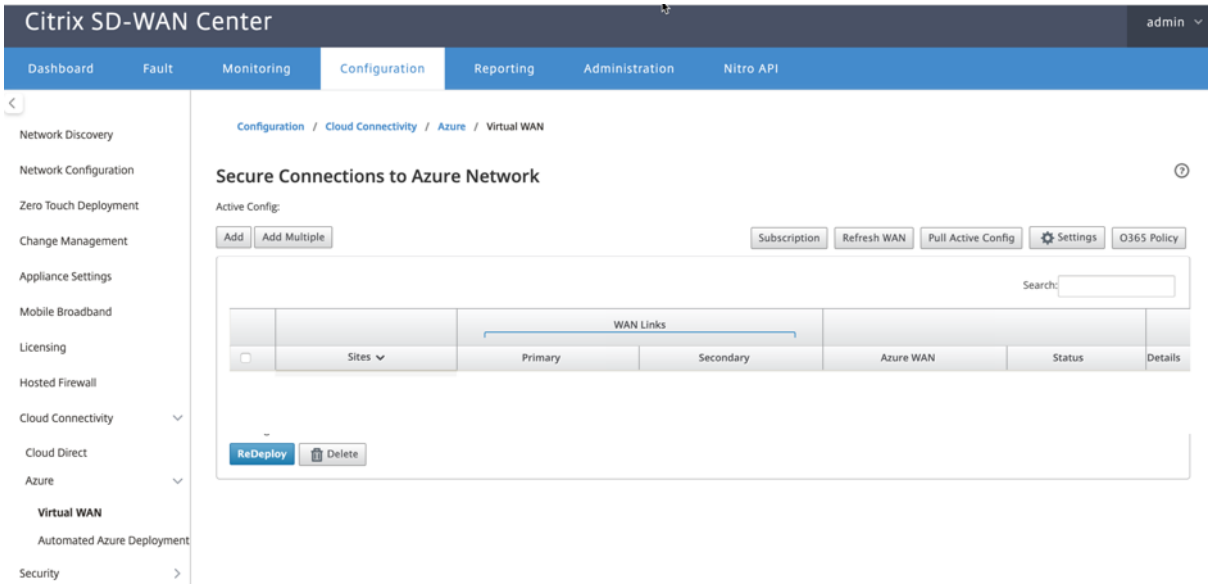
Consulte Crear una entidad de servicio para obtener más información.

Para autenticar correctamente el centro SD-WAN con Azure, deben estar disponibles los siguientes parámetros:

- Directorio (ID de arrendatario)
- Aplicación (ID de cliente)
- Clave segura (Secreto del cliente)
- ID de suscriptor

Autenticar SD-WAN Center:

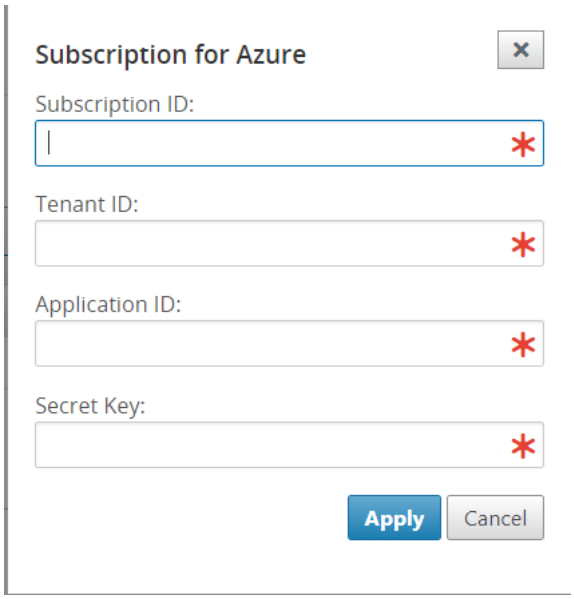
En la interfaz de usuario de SD-WAN Center, vaya a **Configuración** > **Conectividad en la nube** > **Azure** > **WAN virtual**. Configurar la configuración de conexión de Azure. Consulte el siguiente enlace para obtener más información sobre la configuración de la conexión VPN de Azure,
Azure Resource Manager.



Con la versión 11.1.0 y superior, se admite la configuración de vínculos WAN principal y secundaria para la integración de Azure Virtual WAN. La razón principal de agregar un vínculo WAN secundario es tener redundancia desde el sitio Citrix SD-WAN.

Con la implementación anterior, la falla del vínculo WAN podría provocar una interrupción del tráfico y la pérdida de conectividad a Azure Virtual WAN. Con la implementación actual, la conectividad de WAN virtual de sitio a Azure se mantiene activa incluso si el vínculo WAN principal está inactivo.

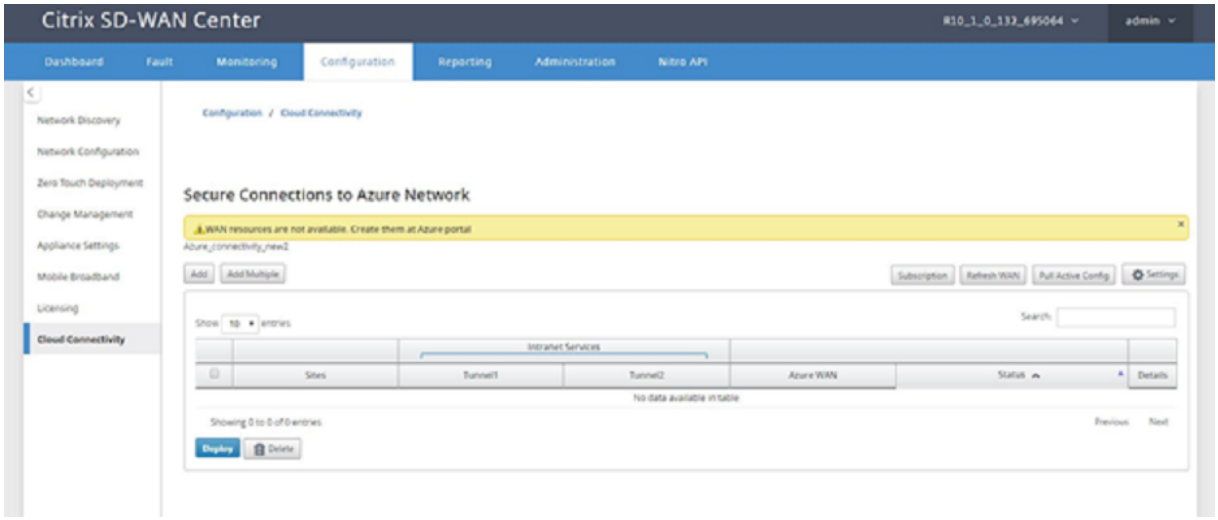
Introduzca el ID de **suscripción, el ID**de **arrendatario**, el **ID de aplicación**y **la clave segura**. Este paso es necesario para autenticar SD-WAN Center con Azure. Si las credenciales introducidas anteriormente no son correctas, se produce un error en la autenticación y no se permiten otras acciones. Haga clic en **Aplicar**.



El campo **Cuenta de almacenamiento** hace referencia a la cuenta de almacenamiento que ha creado en Azure. Si no creó una cuenta de almacenamiento, se creará automáticamente una nueva cuenta de almacenamiento en su suscripción al hacer clic en **Aplicar**.

Obtenga recursos de Azure Virtual WAN:

Una vez que la autenticación se realiza correctamente, Citrix SD-WAN sondea Azure para obtener una lista de recursos WAN virtuales de Azure, que creó en el primer paso después de iniciar sesión en Azure Portal. Los recursos WAN representan toda la red en Azure. Contiene enlaces a todos los Hubs que le gustaría tener dentro de esta WAN. Las WAN están aisladas entre sí y no pueden contener un concentrador común o conexiones entre dos concentradores diferentes en diferentes recursos WAN.



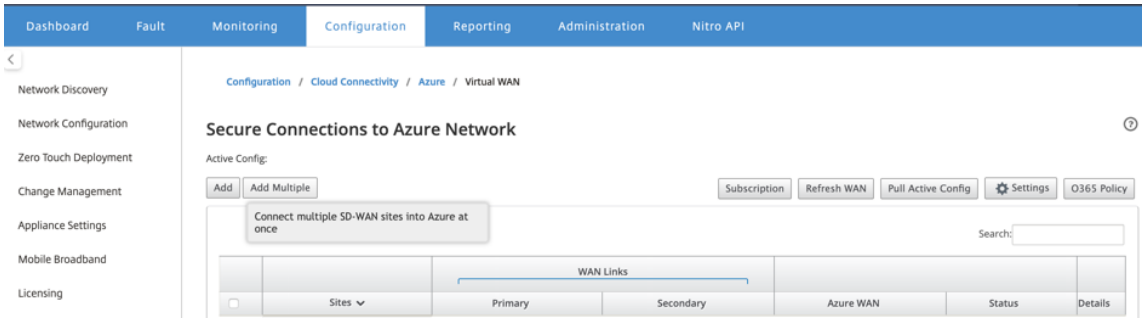
Para asociar sitios de ramas y recursos WAN de Azure:

Un sitio de rama debe estar asociado a recursos de Azure WAN para establecer túneles IPSec. Una rama se puede conectar a varios concentradores dentro de un recurso WAN virtual de Azure y un recurso WAN virtual de Azure se puede conectar con varios sitios de ramas locales. Cree filas individuales para cada rama a implementaciones de recursos de WAN Virtual de Azure.

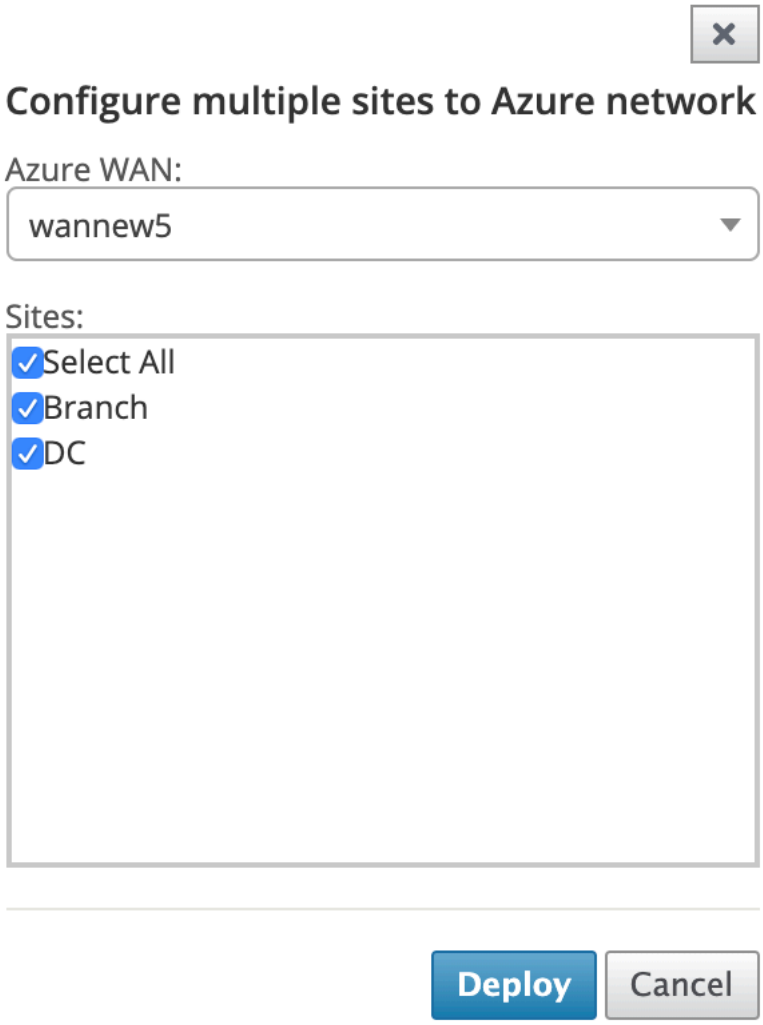
Para agregar varios sitios:

Puede optar por agregar todos los sitios respectivos y asociarlos con los recursos WAN únicos elegidos.

1. Haga clic en **Agregar varios** para agregar todos los sitios que se deben asociar a los recursos WAN seleccionados.



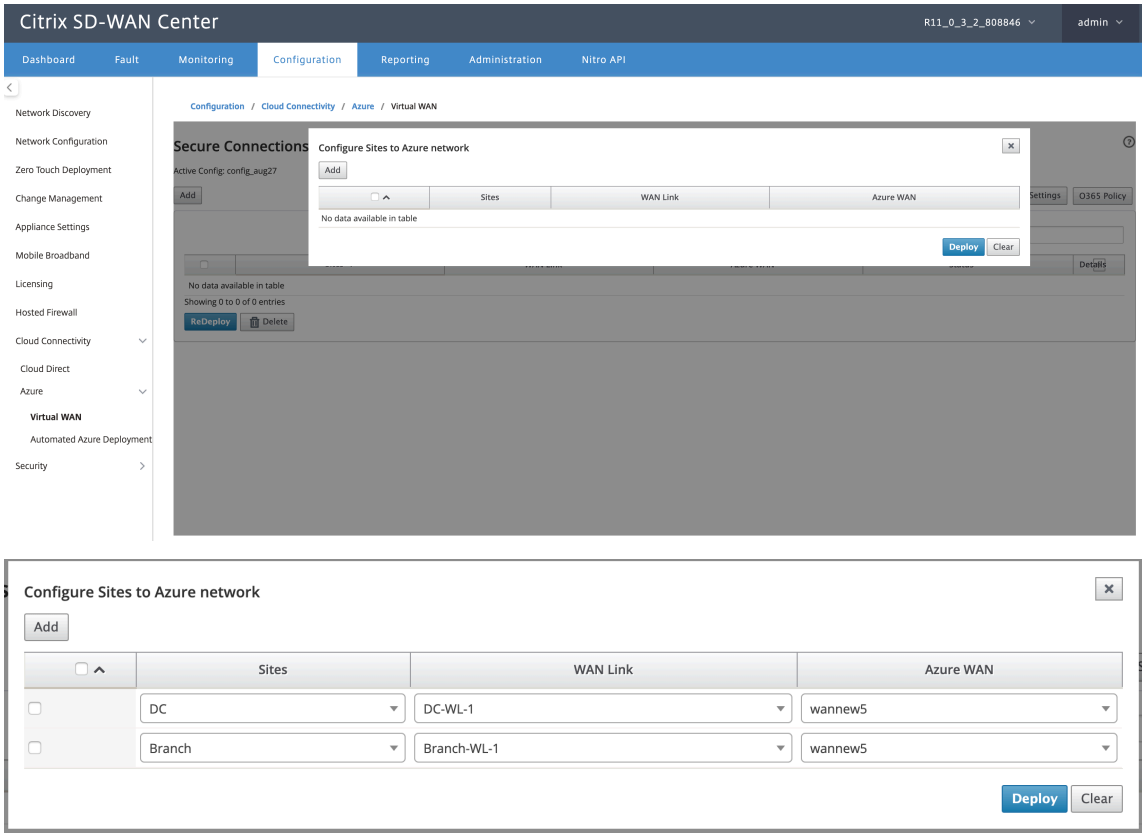
2. La lista desplegable Recursos WAN de Azure (que se muestra a continuación) se rellena previamente con los recursos que pertenecen a su cuenta de Azure. Si no se han creado recursos WAN, esta lista está vacía y debe desplazarse al portal de Azure para crear los recursos. Si la lista se rellena con recursos WAN, elija el **recurso WAN de Azure** al que necesita los sitios de rama para conectarse.
3. Elija uno o todos los sitios de bifurcación para iniciar el proceso de establecimiento de túneles IPSec. Los vínculos WAN de Internet pública de mejor capacidad de sitios se eligen automáticamente para establecer los túneles IPSec a las puertas de enlace VPN de Azure.



Para agregar un solo sitio:

También puede optar por agregar sitios uno por uno (uno) y a medida que crece la red, o si está realizando una implementación sitio por sitio, puede optar por agregar varios sitios como se describe anteriormente.

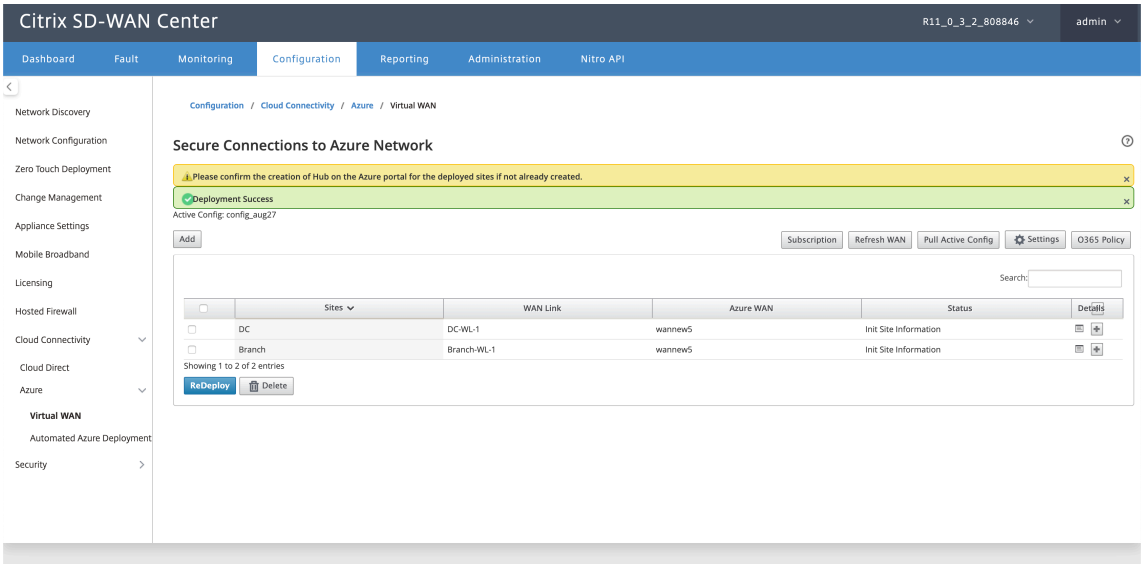
1. Haga clic en **Agregar nueva entrada** para seleccionar un nombre de sitio para la asociación Site-Wan. Agregue sitios en el cuadro de diálogo Configurar sitios en **red de Azure**.



2. Seleccione el sitio de rama que quiere configurar para la red WAN virtual de Azure.
3. Seleccione el vínculo WAN asociado al sitio (los vínculos de tipo Internet público se muestran en el orden de mejor capacidad de vínculo físico)
4. Seleccione el recurso WAN al que debe asociarse el sitio en el menú desplegable **WAN Virtual de Azure**.
5. Haga clic en **Implementar** para confirmar la asociación. El estado (“Información del sitio de inicio”, “Información del sitio empujado”y “Esperando la configuración de VPN”) se actualiza para notificarle sobre el proceso.

El proceso de implementación incluye el siguiente estado:

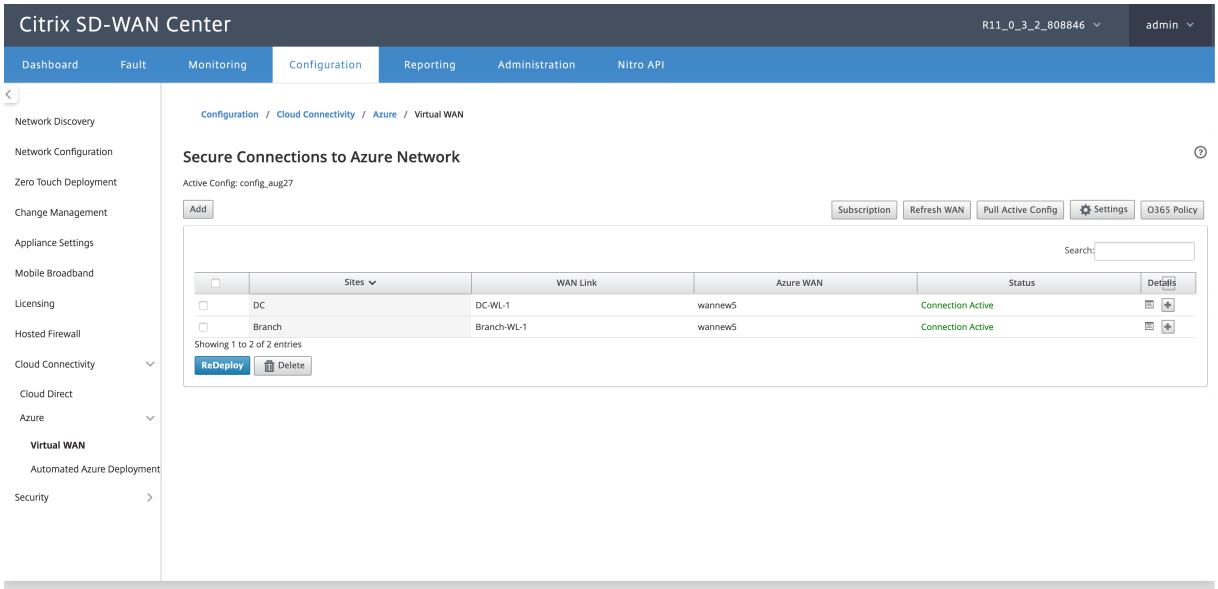
- Información del sitio Push
- Esperando la configuración de VPN
- Túneles implementados
- Conexión activa (el túnel IPsec está activo) o Conexión inactiva (el túnel IPsec está inactivo)

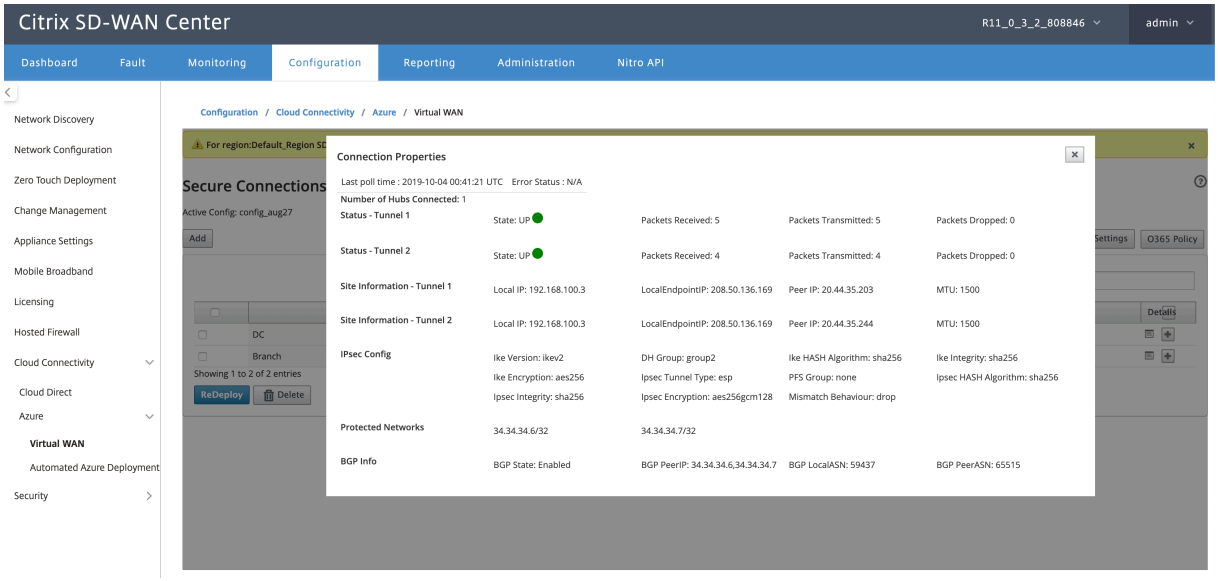


Asociar asignaciones de recursos Wan del sitio (Portal de Azure):

Asocie los sitios implementados en Azure Portal a los concentradores virtuales creados en el recurso de Azure Virtual WAN. Uno o varios centros virtuales pueden asociarse con el sitio de rama. Cada concentrador virtual se crea en una región específica y cargas de trabajo específicas se pueden asociar a los concentradores virtuales mediante la creación de Conexiones de red virtuales. Solo después de que la asociación de sitio de rama a Virtual Hub se realiza correctamente, las configuraciones VPN se descargan y se establecen los túneles IPSec respectivos desde el sitio hasta las puertas de enlace VPN.

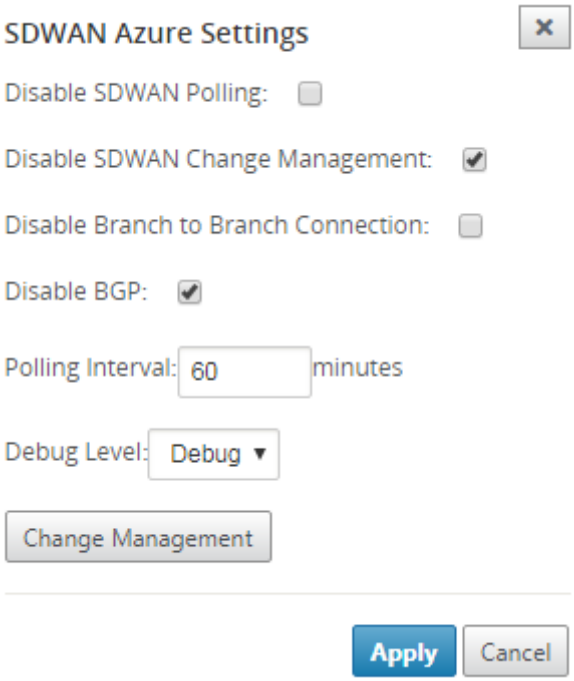
Espere a que el estado cambie a Túneles implementados o Conexión activa para ver la configuración del **túnel IPSec**. Ver la configuración de IPSec asociada a los servicios seleccionados.





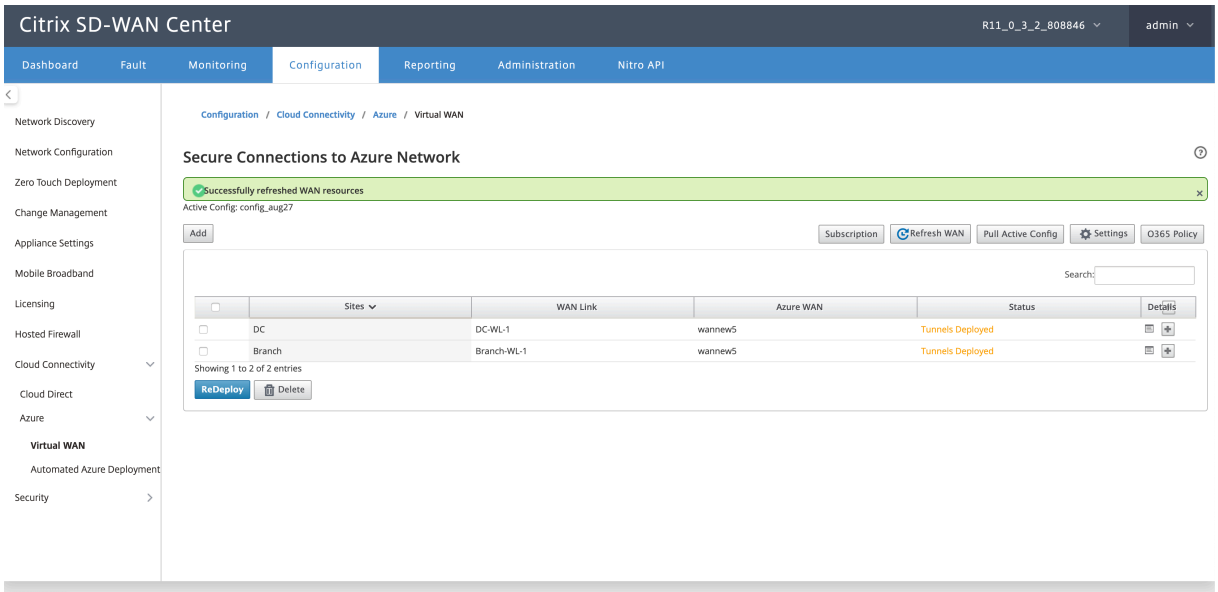
Configuración de Azure de SD-WAN:

- **Inhabilitar la administración de cambios SD-WAN**: De forma predeterminada, el proceso de administración de cambios está automatizado. Esto significa que cada vez que una nueva configuración está disponible en la infraestructura de Azure Virtual WAN, SD-WAN Center la obtiene y comienza a aplicarla a las ramas automáticamente. Sin embargo, este comportamiento se controla, si desea controlar cuándo se debe aplicar una configuración a las ramas. Una ventaja de inhabilitar la administración automática de cambios es que la configuración de esta función y otras funciones de SD-WAN se administra de forma independiente.
- **Inhabilitar sondeo SDWAN:** Inhabilita todas las nuevas implementaciones y sondeos de SD-WAN Azure en implementaciones existentes.
- **Intervalo de sondeo**: La opción Intervalo de sondeo controla el intervalo de búsqueda de actualizaciones de configuración en la infraestructura de Azure Virtual WAN, el tiempo recomendado para el intervalo de sondeo es de 1 hora.
- **Inhabilitar la conexión de rama a rama**: Inhabilita la comunicación de rama a rama a través de la infraestructura WAN virtual de Azure. De forma predeterminada, esta opción está inhabilitada. Una vez habilitado esto, significa que las ramas locales pueden comunicarse entre sí y con los recursos detrás de las ramas a través de IPSec a través de Virtual WAN Infra de Azure. Esto no tiene ningún efecto en la comunicación de rama a rama a través de la ruta virtual SD-WAN, las ramas pueden comunicarse entre sí y sus respectivos recursos/puntos finales a través de la ruta virtual incluso si esta opción está inhabilitada.
- **Inhabilitar BGP**: Inhabilita BGP sobre IP, de forma predeterminada está inhabilitado. Una vez habilitada, las rutas del sitio se anuncian a través de BGP.
- **Nivel de depuración**: Permite capturar registros para depurar si hay algún problema de conectividad.



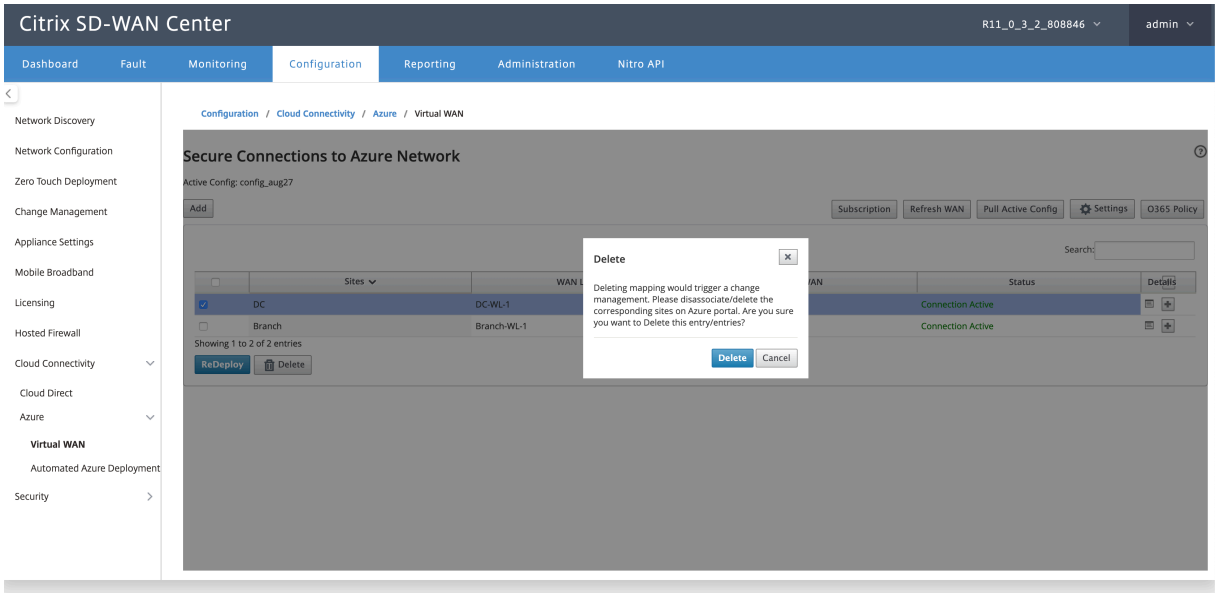
Actualizar recursos WAN:

Haga clic en el icono **Actualizar** para recuperar el conjunto más reciente de recursos WAN que actualizó en Azure Portal. Se muestra un mensaje que indica "recursos WAN actualizados correctamente" una vez finalizado el proceso de actualización.

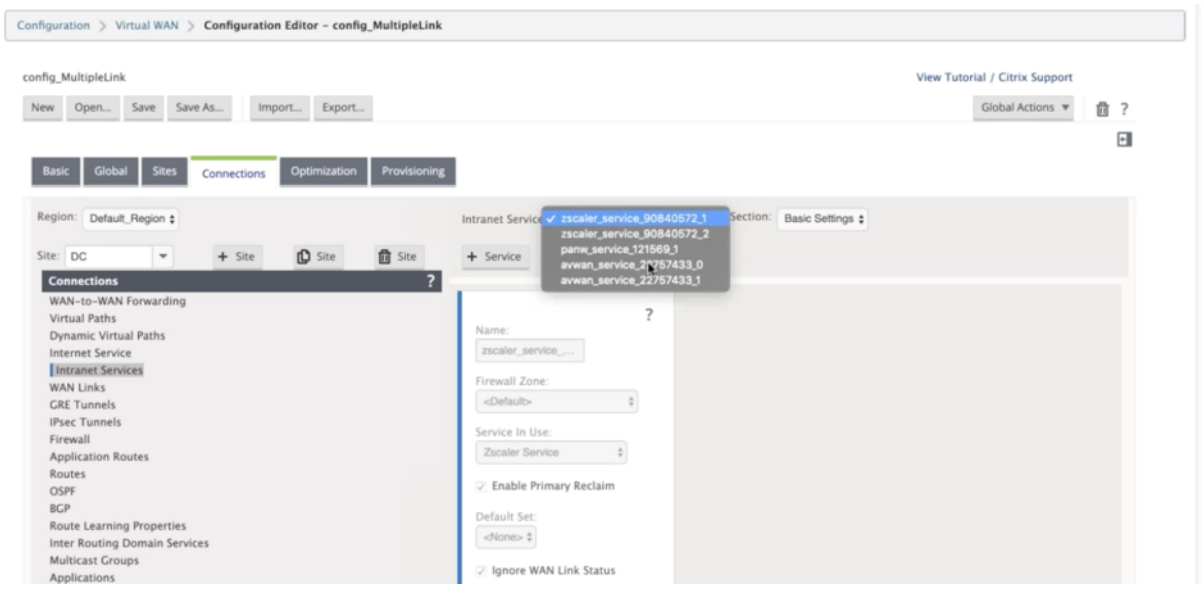


Quitar asociación de recursos WAN del sitio Seleccione una o varias asignaciones para realizar la eliminación. Internamente, se activa el proceso de administración de cambios del dispositivo SD-WAN y, hasta que se realice correctamente, se inhabilita la opción Eliminar para evitar que se realicen

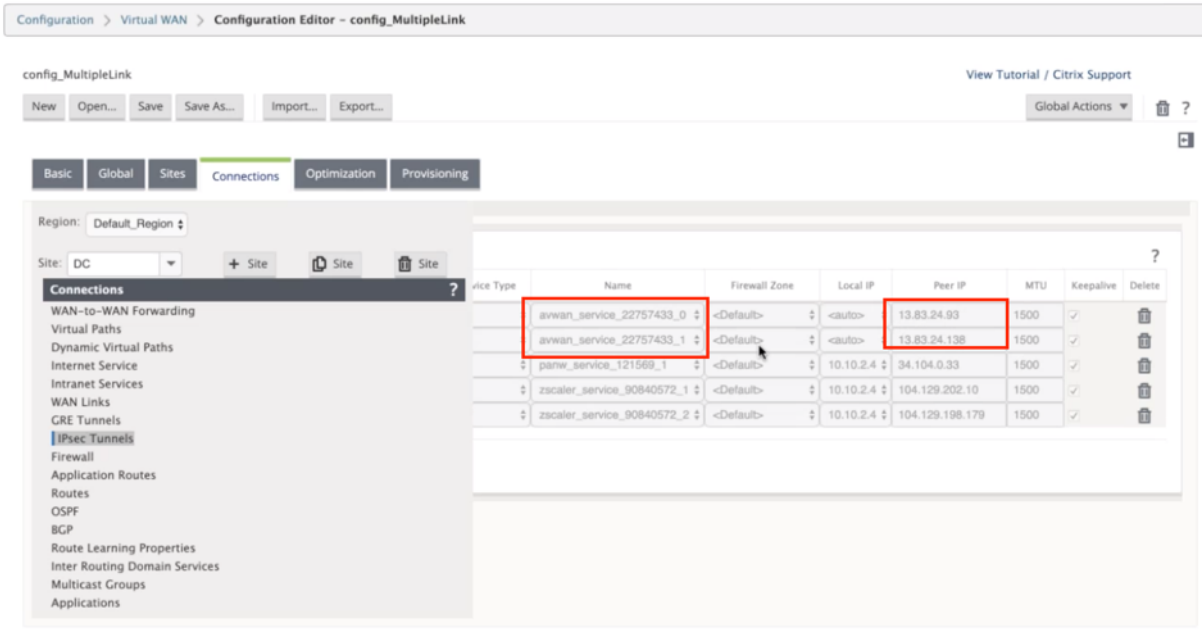
más eliminaciones. Para eliminar la asignación, debe desasociar o eliminar los sitios correspondientes en Azure Portal. El usuario tiene que realizar esta operación manualmente.



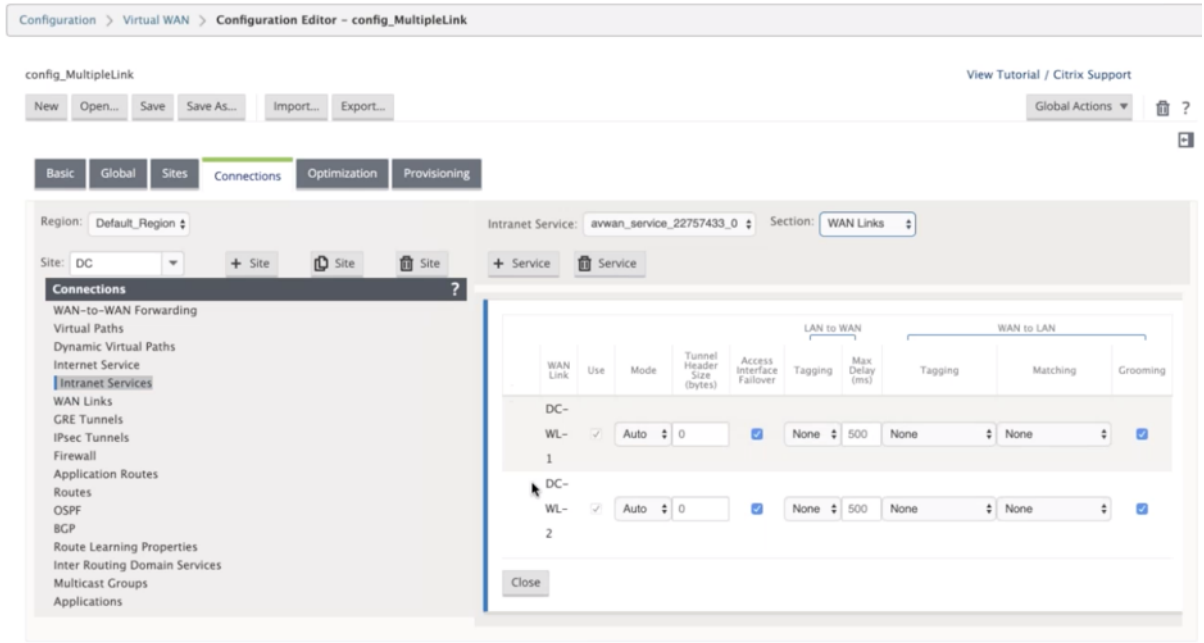
Una vez creados los túneles, puede ver dos servicios de intranet creados en su MCN.



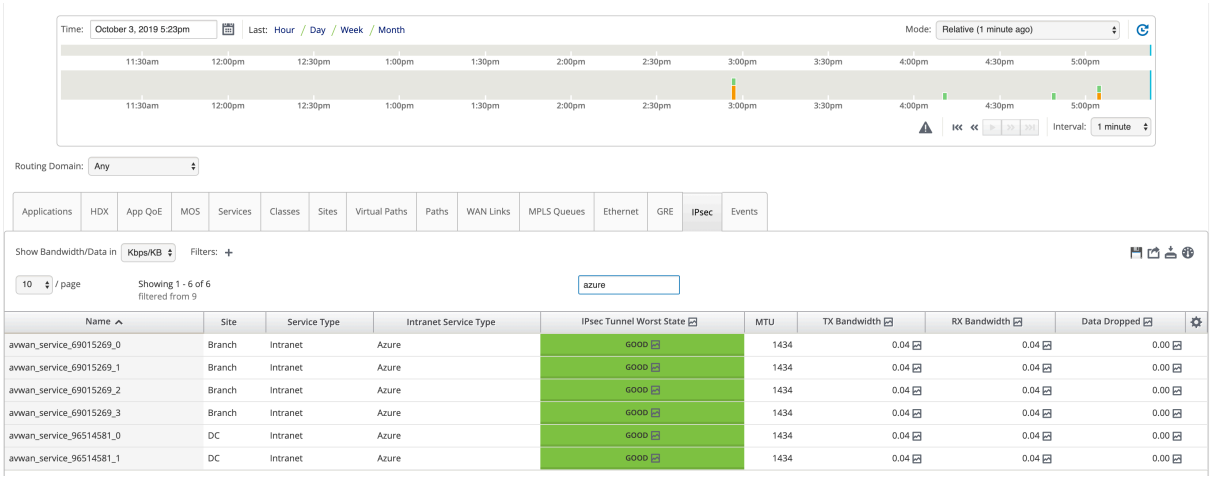
Cada servicio de Intranet corresponde a túneles IPSec creados con IPs del mismo nivel (IPs de punto final de WAN Virtual de Azure).



En **Servicios de Intranet**, si selecciona **Vínculos WAN** en la lista desplegable **Sección**, puede ver el vínculo WAN principal y secundario especificado por usted. De forma predeterminada, el modo se establece en **Automático**.



Supervisar túneles IPsec En la interfaz de usuario de SD-WAN Center, vaya a **Informes** > **IPSec** para comprobar el estado de los túneles IPSec. El estado del túnel debe ser VERDE para que fluya el tráfico de datos.



Servicio Cloud Direct

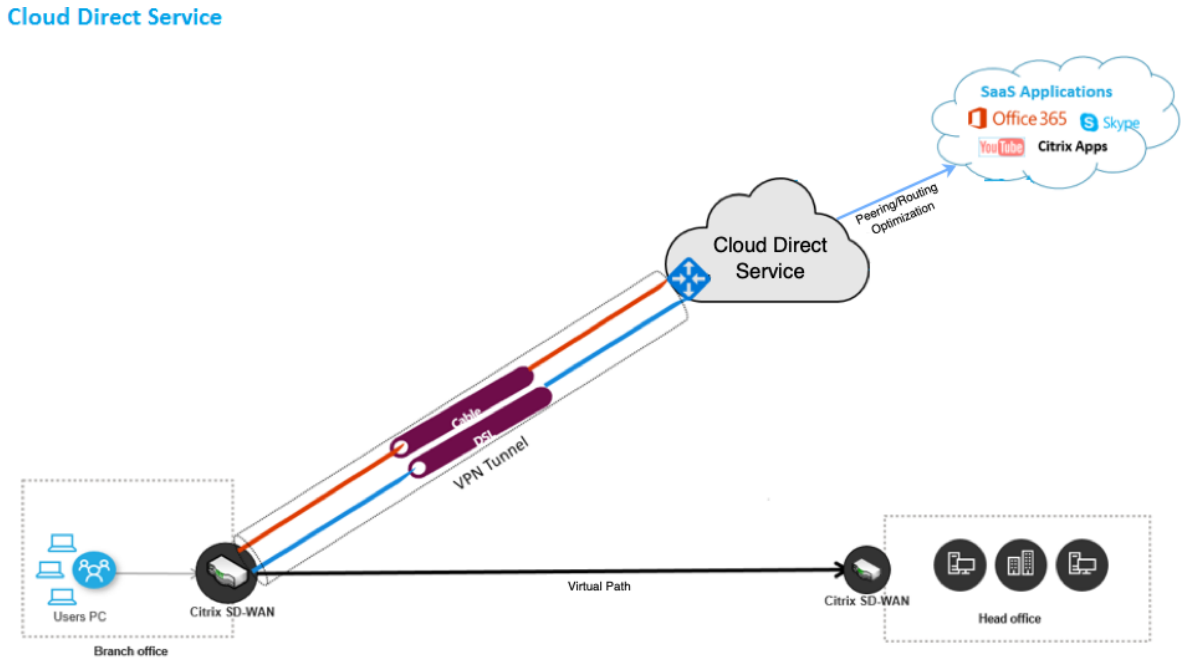
April 13, 2021

El servicio Cloud Direct ofrece funcionalidades SD-WAN como un servicio en la nube a través de una entrega fiable y segura para todo el tráfico enlazado a Internet independientemente del entorno host (centro de datos, nube e Internet). Mejora la visibilidad y la gestión de la red. Permite a los socios ofrecer servicios gestionados de SD-WAN para aplicaciones SaaS críticas para el negocio a sus clientes finales.

El servicio directo en la nube ofrece las siguientes ventajas:

- **Redundancia** : utiliza varios vínculos WAN de Internet y proporciona conmutación por error sin interrupciones.
- **Agregación de vínculos** : utiliza todos los enlaces WAN de Internet al mismo tiempo.
- Equilibrio de carga inteligente en conexiones WAN de diferentes proveedores:
  - Medición de la pérdida de paquetes, la fluctuación y el rendimiento.
  - Identificación de aplicaciones personalizadas.
  - Requisitos de aplicación y adecuación del rendimiento del circuito (adaptarse a las condiciones de red en tiempo real).
- Capacidad de QoS dinámica de grado SLA-grado para circuito de Internet:
  - Se adapta dinámicamente a los diferentes niveles de rendimiento del circuito.
  - Adaptación a través del túnel en los puntos finales de entrada y salida.
- Redireccionar llamadas VOIP entre circuitos sin soltar la llamada.
- Monitorización y visibilidad de extremo a extremo.

Flujo de trabajo de servicio directo en



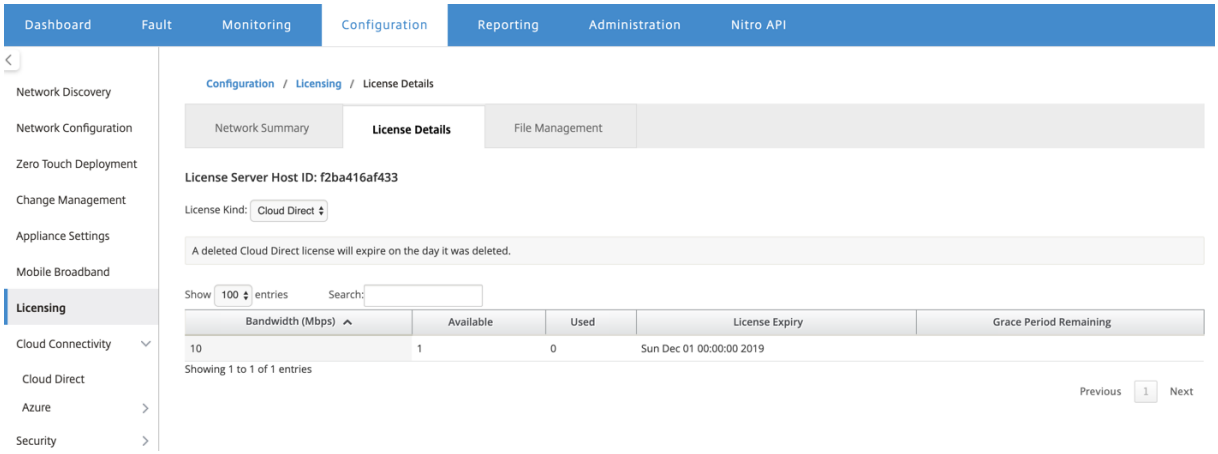
Antes de comenzar a implementar el servicio Cloud Direct, asegúrese de que se han completado los siguientes pasos:

1. Dispón de un dispositivo de edición 410-SE, 210-SE o 1100-SE/PE. Si la versión SD-WAN enviada de fábrica del dispositivo es anterior a la 9.3.5, debe seguir el procedimiento de reimagen de USB para actualizar el dispositivo a la imagen de base de envío más reciente.
2. Realice actualización de un solo paso el procedimiento para instalar la versión de software compatible con Cloud Direct Service.
3. Configure el dispositivo MCN y establezca las rutas virtuales con sus sucursales:
    - Configurar sitio de sucursal. Consulte Configurar sucursal para obtener más información.
    - Cree objetos de aplicación para rutas basadas en aplicaciones.
        - Si tiene la intención de dirigir selectivamente las aplicaciones a través del servicio Cloud direct, cree los objetos de aplicación incluyendo las aplicaciones correspondientes, vea cómo crear Objetos de aplicación, que se enrutan a través del servicio Cloud direct. Para administrar el tráfico enlazado a Internet, el servicio Internet debe crearse desde el editor de configuración del dispositivo. Para obtener más información, consulte Servicio de Internet.
        - Si tiene la intención de dirigir todo el tráfico vinculado a Internet a través del servicio directo de Citrix Cloud, puede omitir la creación de objetos específicos de la aplicación.

Licencias

La función de servicio Cloud Direct tiene licencia independientemente de las licencias básicas de SD-WAN. Asegúrese de haber instalado las licencias necesarias para el servicio Cloud Direct en SD-WAN Center. Para obtener más información, consulte Citrix SD-WAN Center como servidor de licencias.sd-wan-center-as-license-server.

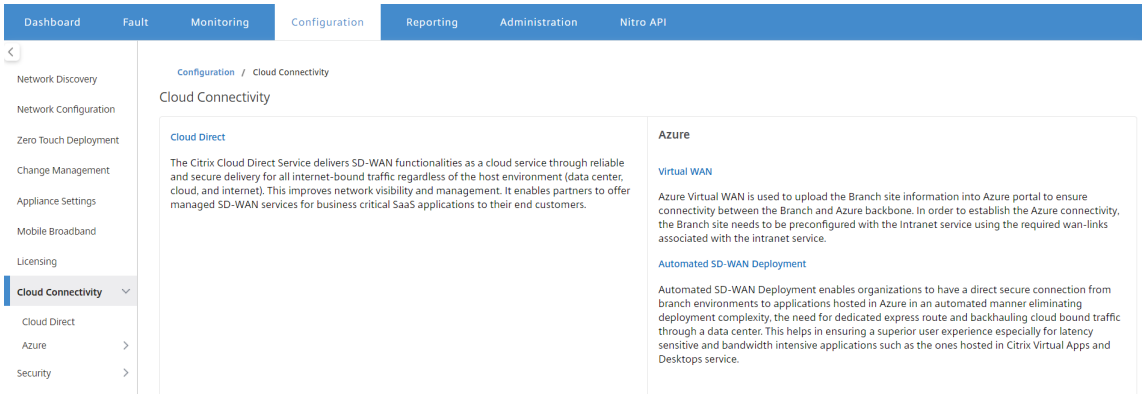
La página Licencias proporciona detalles sobre la información de licencia del servicio Cloud Direct instalada.



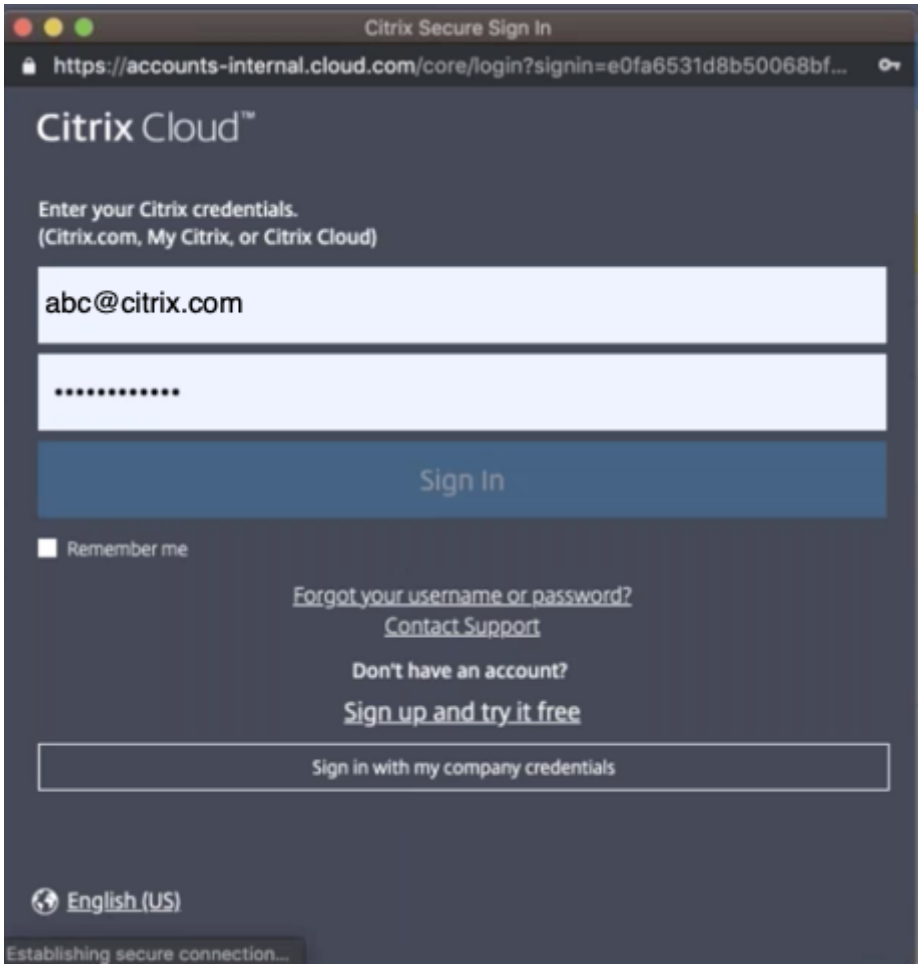
> **Nota**
>
> Hay un período de gracia de 30 días para que las licencias de Cloud Direct caducadas o eliminadas, antes del cual debe instalar las licencias válidas para que los sitios de Cloud Direct implementados funcionen. Si no se instalan licencias válidas antes de que expire el período de gracia, SD-WAN Center inhabilita el servicio Cloud Direct in situ con la licencia caducada.

Configurar el servicio directo en la nube en el Centro de SD-WAN

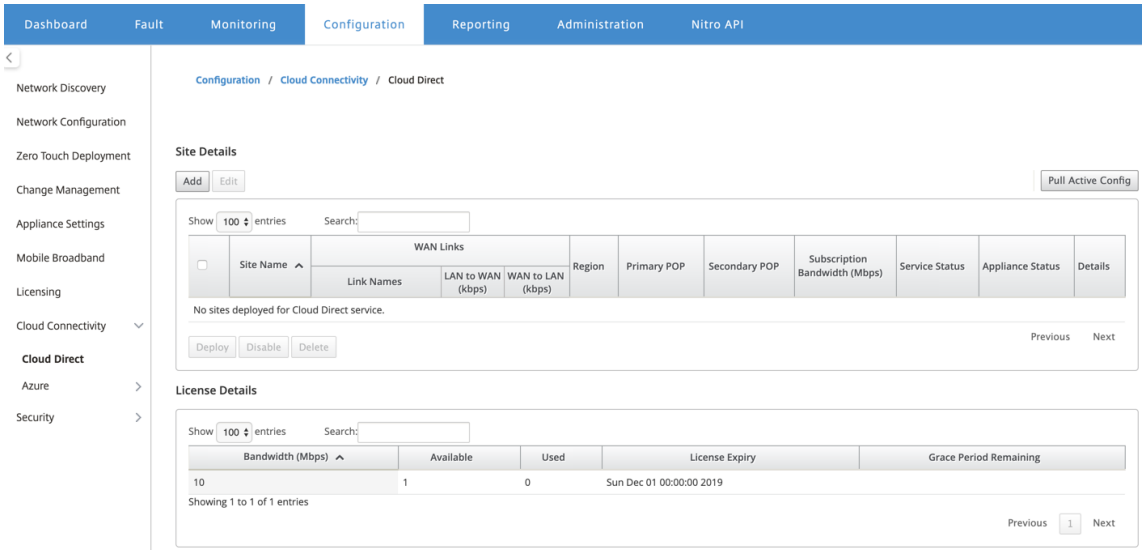
1. En la GUI de SD-WAN Center, vaya a **Configuración** > **Conectividad en la nube** > **Cloud Direct**.



2. Inicie sesión con las credenciales de Citrix Cloud.

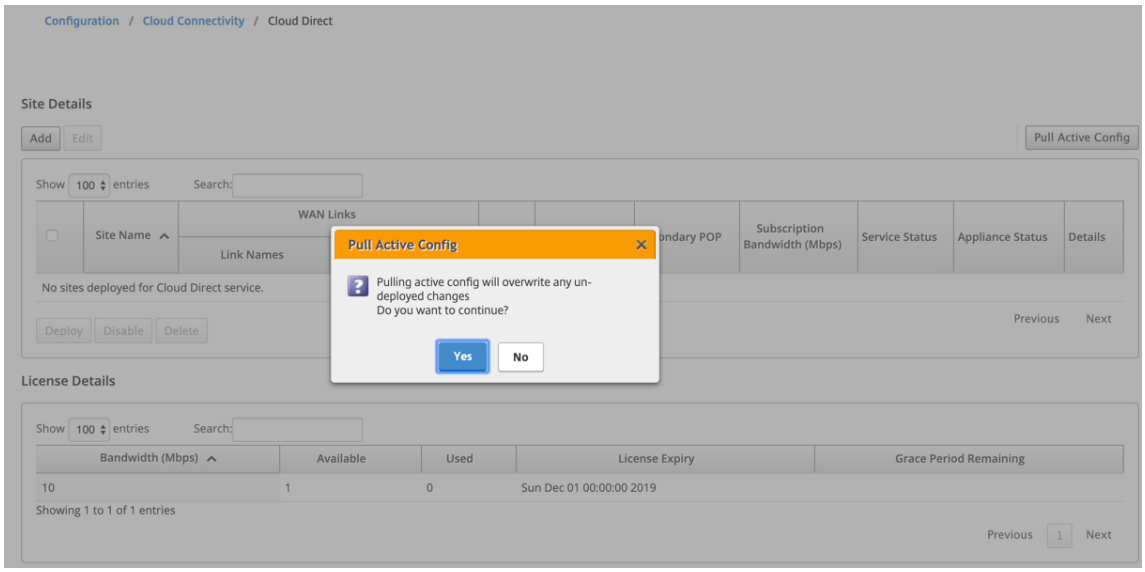


La página principal de Cloud Direct aparece después de iniciar sesión correctamente en Citrix Cloud Service.



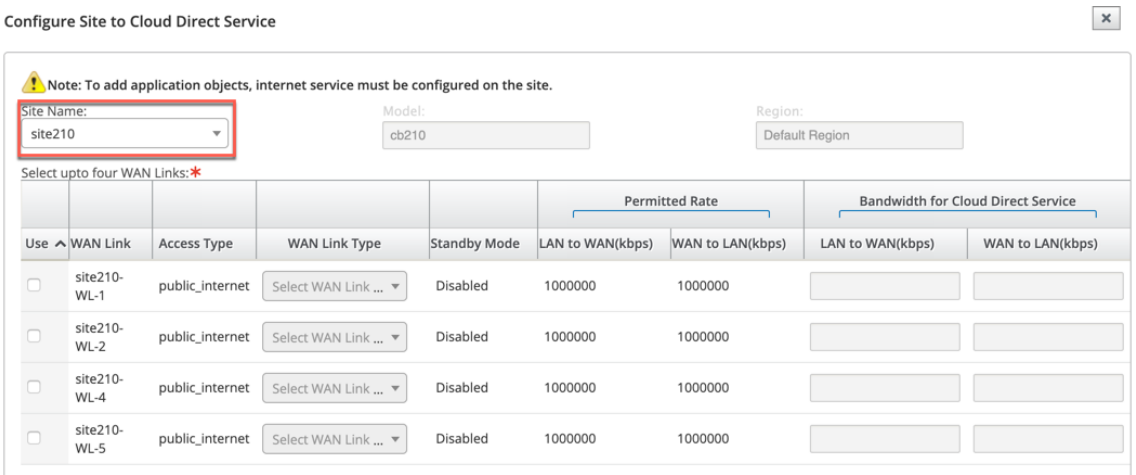
3. Haga clic en **Extraer configuración activa** para recuperar la configuración de MCN activa más

reciente.



4. Haga clic en **Agregar un nuevo sitio**. Los sitios que son elegibles para la implementación del servicio Cloud Direct se muestran en el menú.

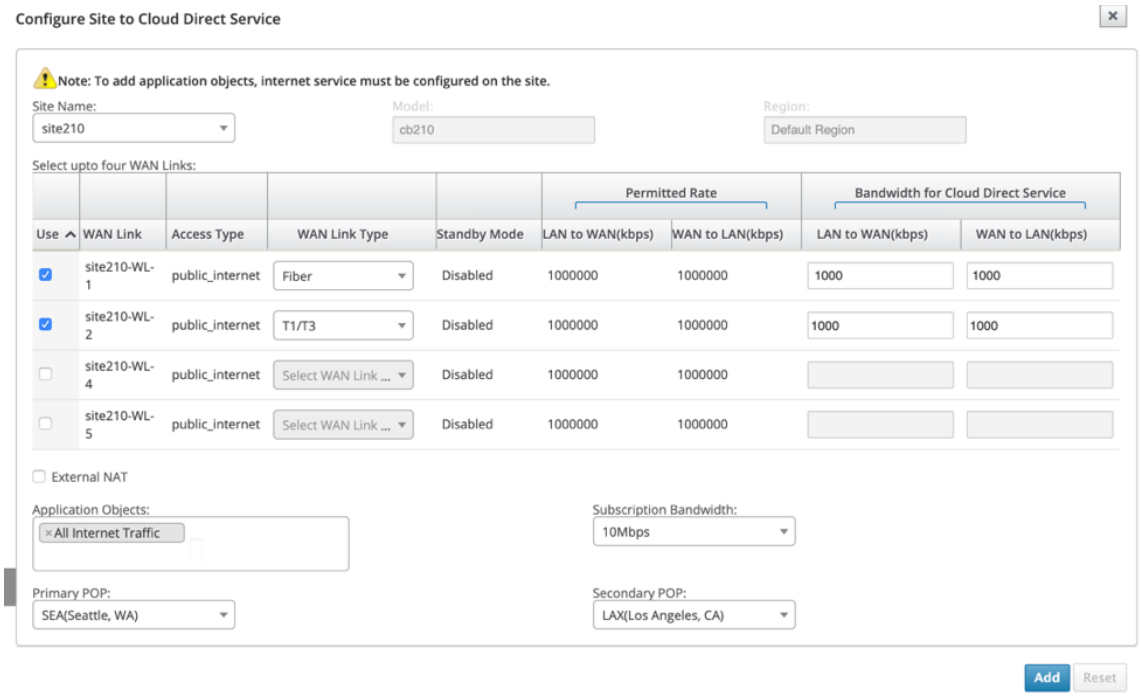
> **Nota**
>
> - La función de servicio Cloud Direct es compatible con los dispositivos de hardware 210, 410 y 1100.
> - A partir de la versión 11.2, el servicio Cloud Direct es compatible con los dispositivos SD-WAN 2100, 4100 y 6100. Tanto SD-WAN Center como Orchestrator permiten implementar la función de servicio Cloud Direct en dispositivos SD-WAN 2100, 4100 y 6100. SD-WAN Center admite licencias de suscripción de hasta 250 Mbps para Cloud Direct.



5. Cuando se selecciona un sitio, se muestran los vínculos WAN públicos de Internet asociados al sitio seleccionado, junto con la información del modelo del dispositivo y la región en la que se implementa el dispositivo.

6. Seleccione los vínculos WAN que desea utilizar para el tráfico del servicio Cloud Direct, junto con las opciones **Tipo de vínculo WAN**, **Objetos de aplicación**, Ancho de **banda de suscripción**, **POP principal**y **POP secundario** .

> **Nota**
>
> - Se admiten hasta cuatro enlaces WAN para el servicio Cloud Direct.
> - Ya no es necesario reservar un ancho de banda de enlace WAN exclusivamente para el servicio Cloud Direct. Si el servicio Cloud Direct no está activo, los demás servicios como rutas virtuales, Internet o servicios de intranet configurados en ese vínculo WAN pueden utilizar el ancho de banda según los recursos compartidos configurados.



- **Nombre del sitio**: muestra los sitios que son elegibles para la implementación de funciones de Cloud Direct.
- **Modelo**: para el sitio seleccionado, el nombre del modelo de dispositivo correspondiente se rellena automáticamente.
- **Región**: Para el sitio seleccionado, los detalles de la región implementada específica del dispositivo se rellenan automáticamente.
- **Vínculo WAN**: Para el sitio seleccionado, se muestran los vínculos WAN de Internet públicos asociados.
- **Tipo de vínculo WAN**: seleccione el tipo de vínculo WAN en el menú.
- **Modo de espera**: modo de espera se recupera de la configuración del enlace WAN.

- **Ancho de banda para Cloud Direct Service**: Introduzca el ancho de banda que Cloud Direct Service puede utilizar exclusivamente. El ancho de banda seleccionado debe ser menor que el ancho de banda permitido configurado y no estaría disponible para su uso por los servicios Virtual Path, Internet e Intranet.
- **NAT externo**: se requiere que el tráfico público de Internet originado desde la red LAN de sucursal sea NAT de origen de una dirección IP específica. De forma predeterminada, esto se realiza automáticamente y se realiza como parte de la configuración de red SD-WAN. Si quiere configurar la IP NAT (Red LAN) fuera del dispositivo SD-WAN (por ejemplo, en un firewall externo), puede elegir la opción NAT externa al implementar sitios. La IP a la que el tráfico LAN debe ser el NAT de origen está disponible en la página **Detalles** del sitio implementado de Cloud Direct.
- **Objetos de aplicación**: puede elegir objetos de aplicación específicos o seleccionar "Todo el tráfico de Internet"para ser redirigido a través del servicio Cloud Direct. En caso de que se seleccionen los objetos específicos de la aplicación, el tráfico de esas aplicaciones se envía a través del servicio Cloud Direct y el resto del tráfico se dirige mediante el servicio de Internet configurado en el dispositivo.
- **Ancho de banda**de suscripción: el ancho de banda de suscripción está asociado a la licencia para el servicio directo en la nube.
- **Modo de facturación**: cuando un cliente planea implementar un sitio de Cloud Direct como parte de la validación de prueba de concepto (POC), el campo **Modo de facturación** debe establecerse como **demostración**. Para todos los demás casos, establezca el modo de facturación como **Producción**.

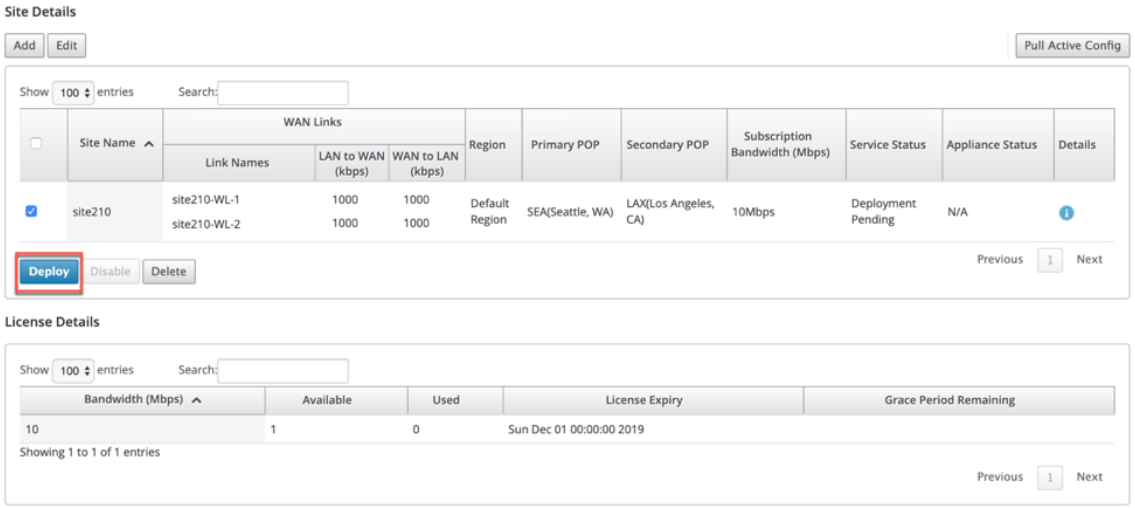
> **NOTA:** Se produce la siguiente situación, si el **modo de facturación** está seleccionado como **demostración** o **producción**:
>
> - Si se crea un sitio de Cloud Direct con el **modo de facturacióncomo demostración**, la configuración se puede modificar en Producción.
> - Si se crea un sitio de Cloud Direct con el **Modo de facturación** como **Producción**, la configuración no se puede modificar en **Demo**.

La opción **Modo de facturación** permite el uso de licencias de evaluación o prueba de Cloud Direct, que pueden proporcionarlas las ventas de Citrix o los socios autorizados. Los sitios que operan con licencias de evaluación de Cloud Direct deben estar configurados en la opción **Modo de facturación de demostración**. Los sitios que se actualizan a licencias de suscripción completas de Cloud Direct deben estar configurados en la opción **Modo de facturación de producción**.

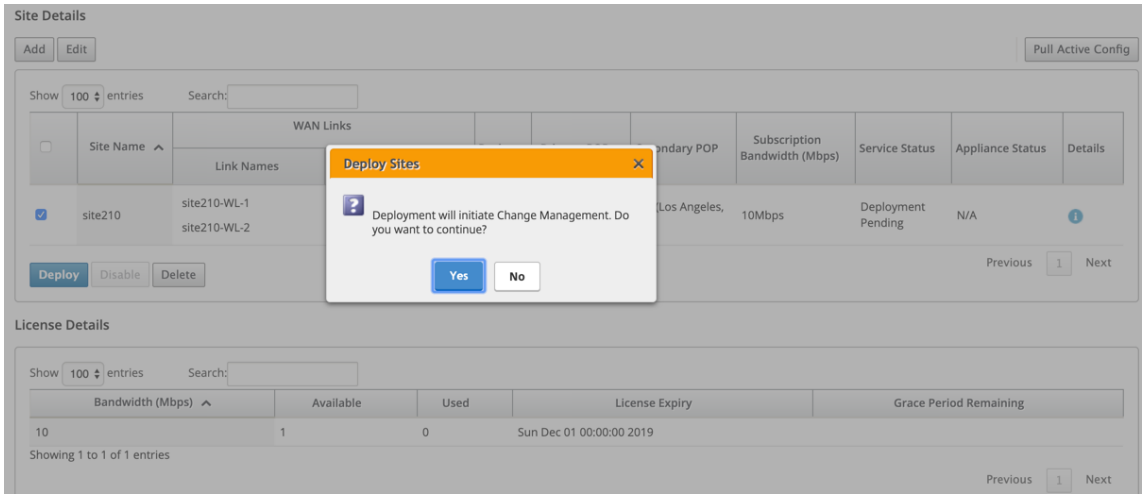
- **POP primario/secundario**: Asegúrese de que el POP primario y secundario no sea el mismo. Seleccione los POP en función de la proximidad de la ubicación. Haga clic en

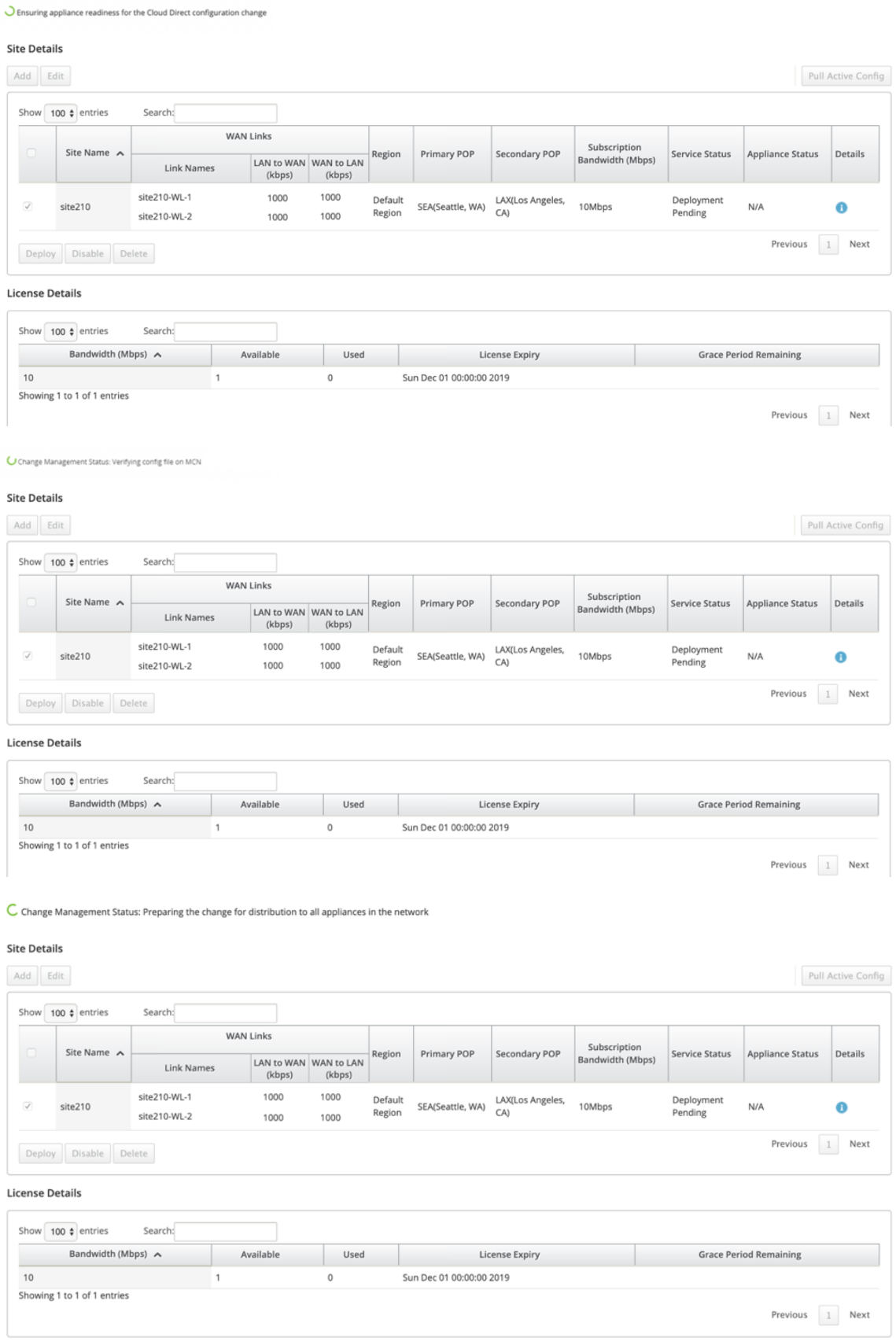
Agregar.

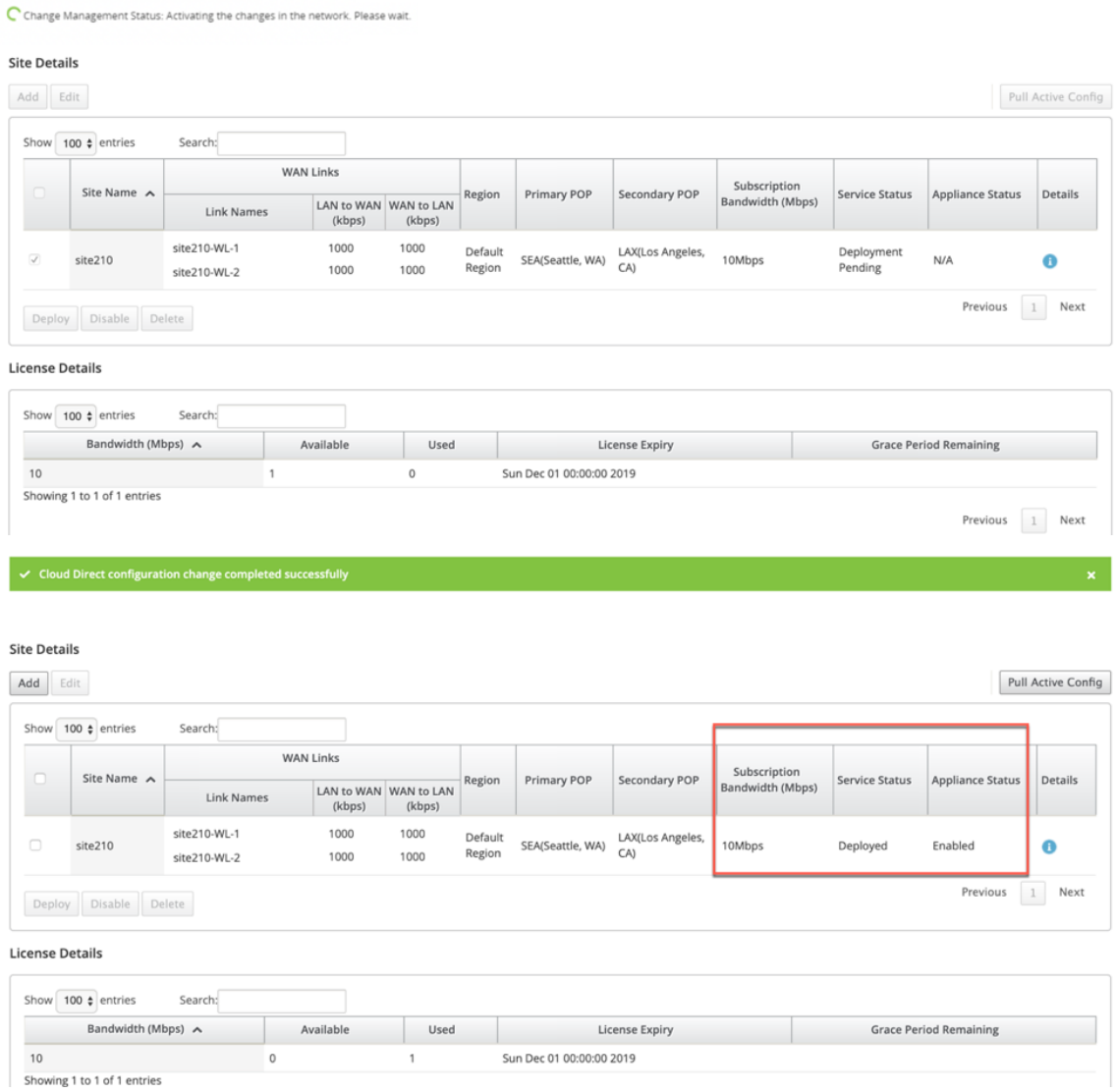
7. Después de agregar los sitios, el estado del servicio se muestra como **Deployment es Pendiente**. Seleccione el sitio para el que quiere implementar el servicio Cloud Direct y haga clic en **Implementar**.



Se muestra una notificación que indica que la operación de implementación inicia una administración de cambios en el dispositivo MCN. Puede hacer clic en **Sí** o **No**.







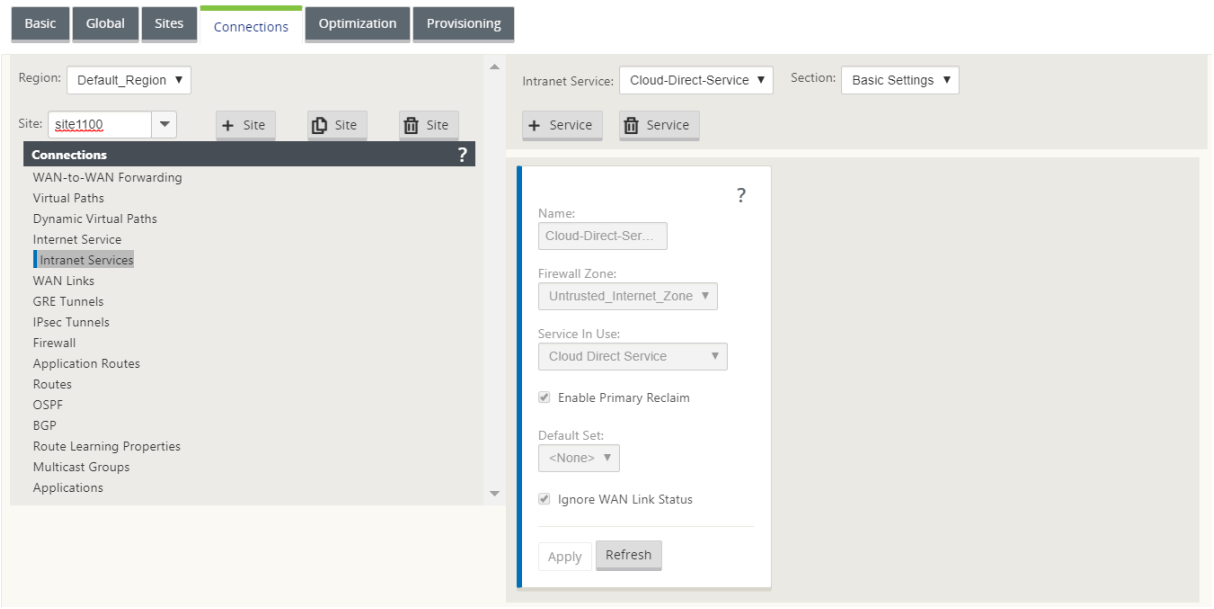
Después de implementar correctamente los sitios, la página de servicio directo en la nube muestra lo siguiente:

- **Estado del servicio**: Implementada
- **Estado del dispositivo**: Activado
- **Ancho de banda de suscripción (Mbps)**: 10 Mbps
- **Se consumió la licencia instalada**

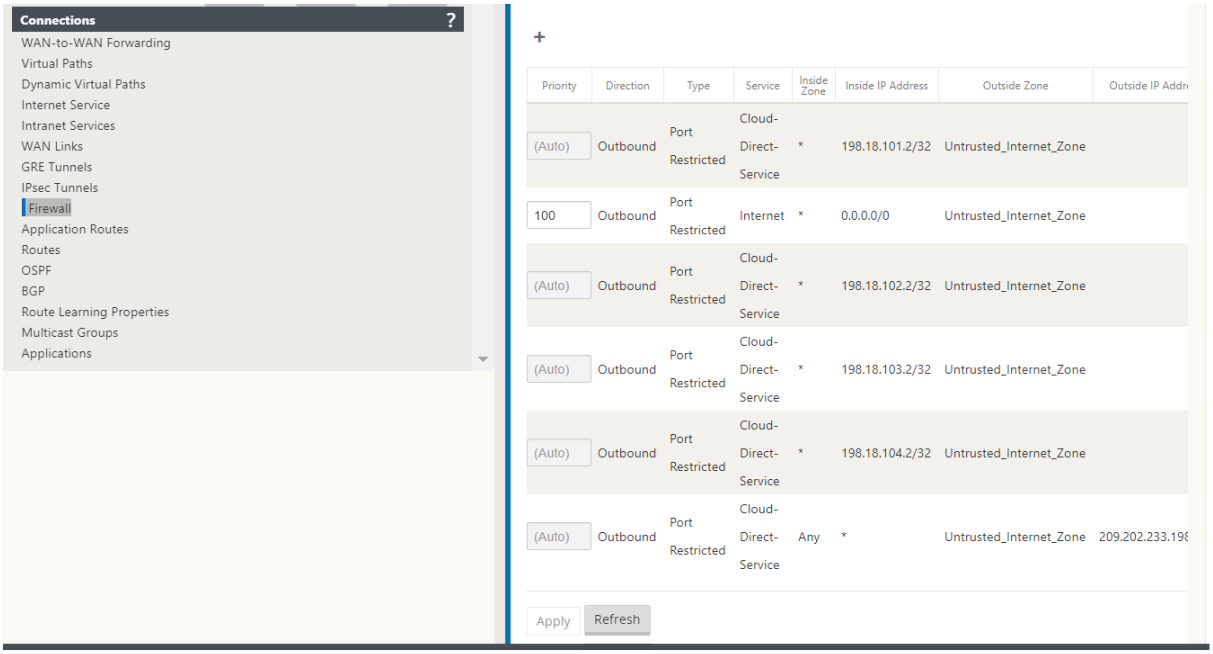
El paso de administración de cambios anterior genera automáticamente y agregue las configuraciones de servicio Cloud Direct necesarias a la configuración en ejecución.

> **Nota**

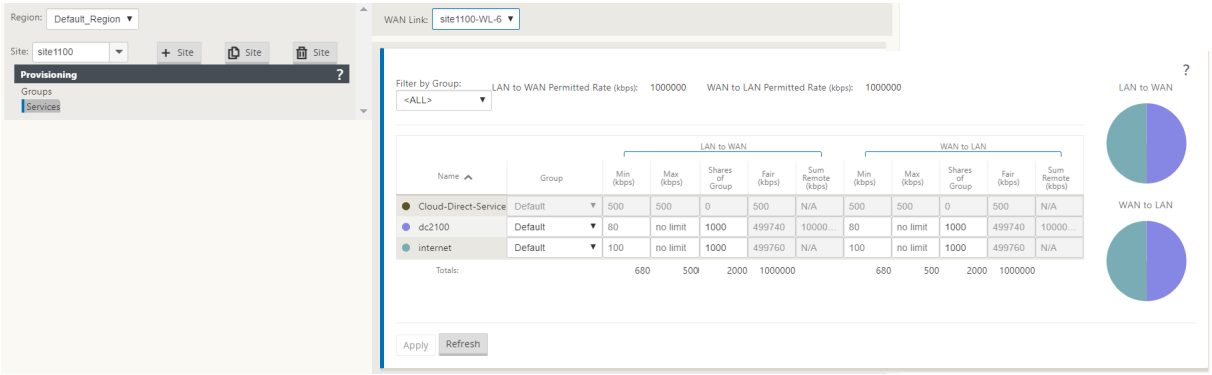
> El servicio **Cloud Direct (servicio** de intranet) creado automáticamente está asociado con Default_RoutingDomain.



Configuración de conexiones de seguridad

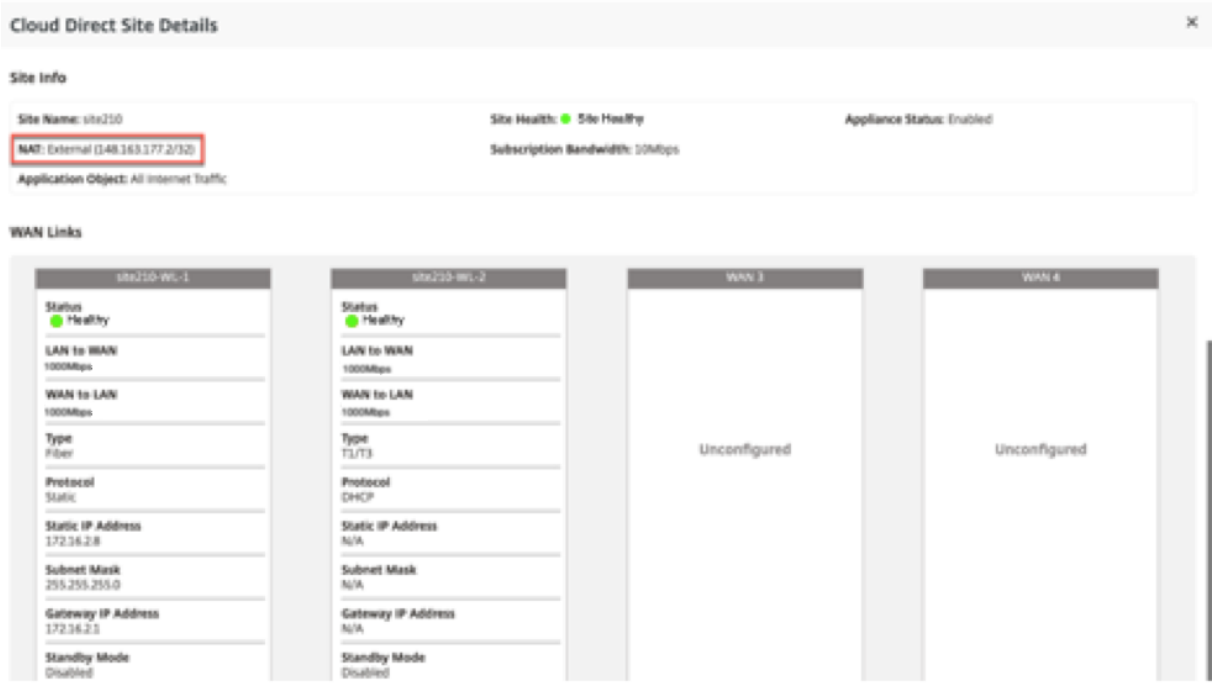


Sitios de aprovisionamiento en la GUI de la aplicación SD-WAN

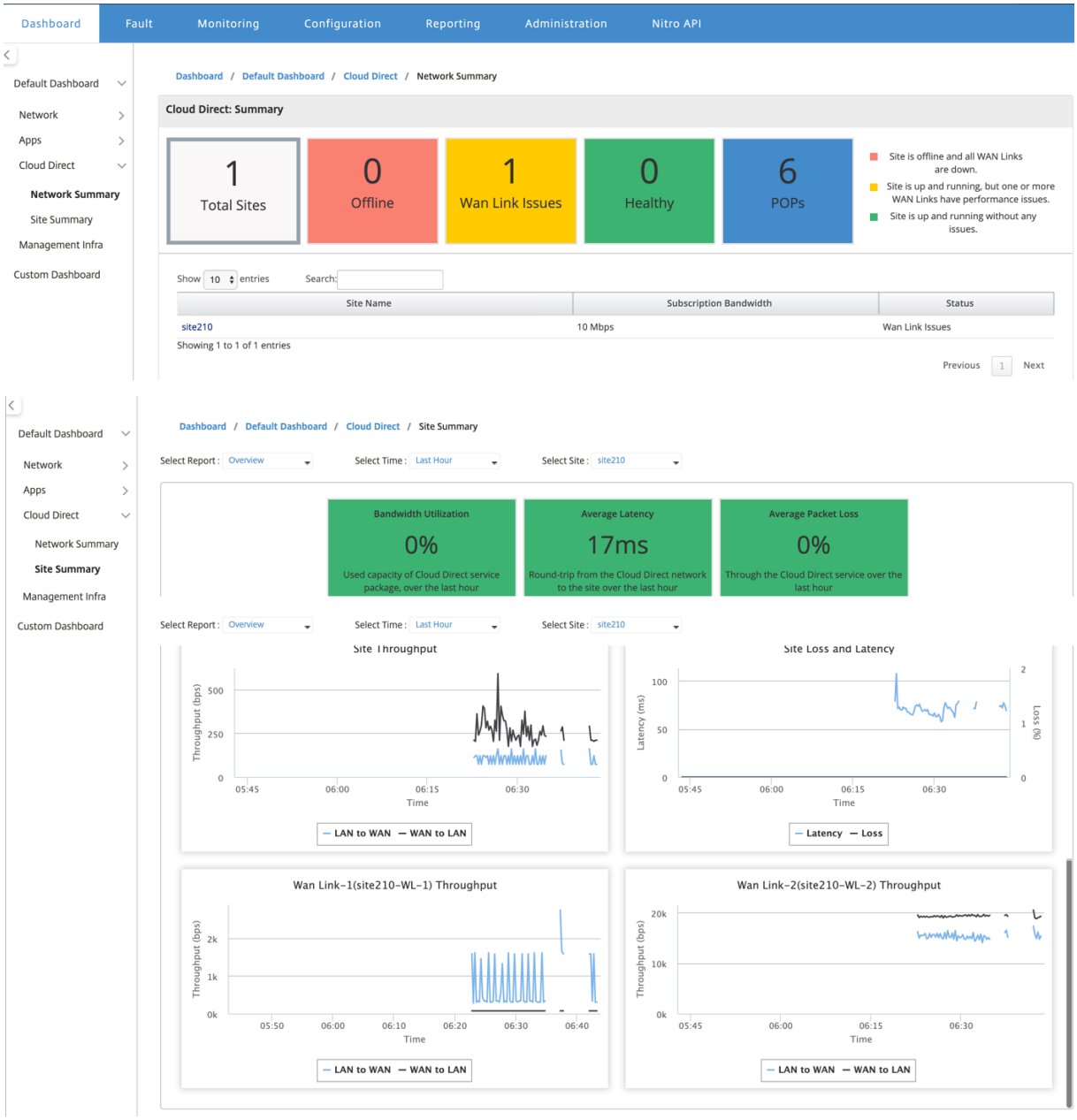


Supervisión del servicio Cloud Direct

Puede ver el servicio Cloud Direct configurado una vez implementados y habilitados los sitios. Haga clic en el icono de exclamación de la columna **Detalles** para ver los detalles del sitio.



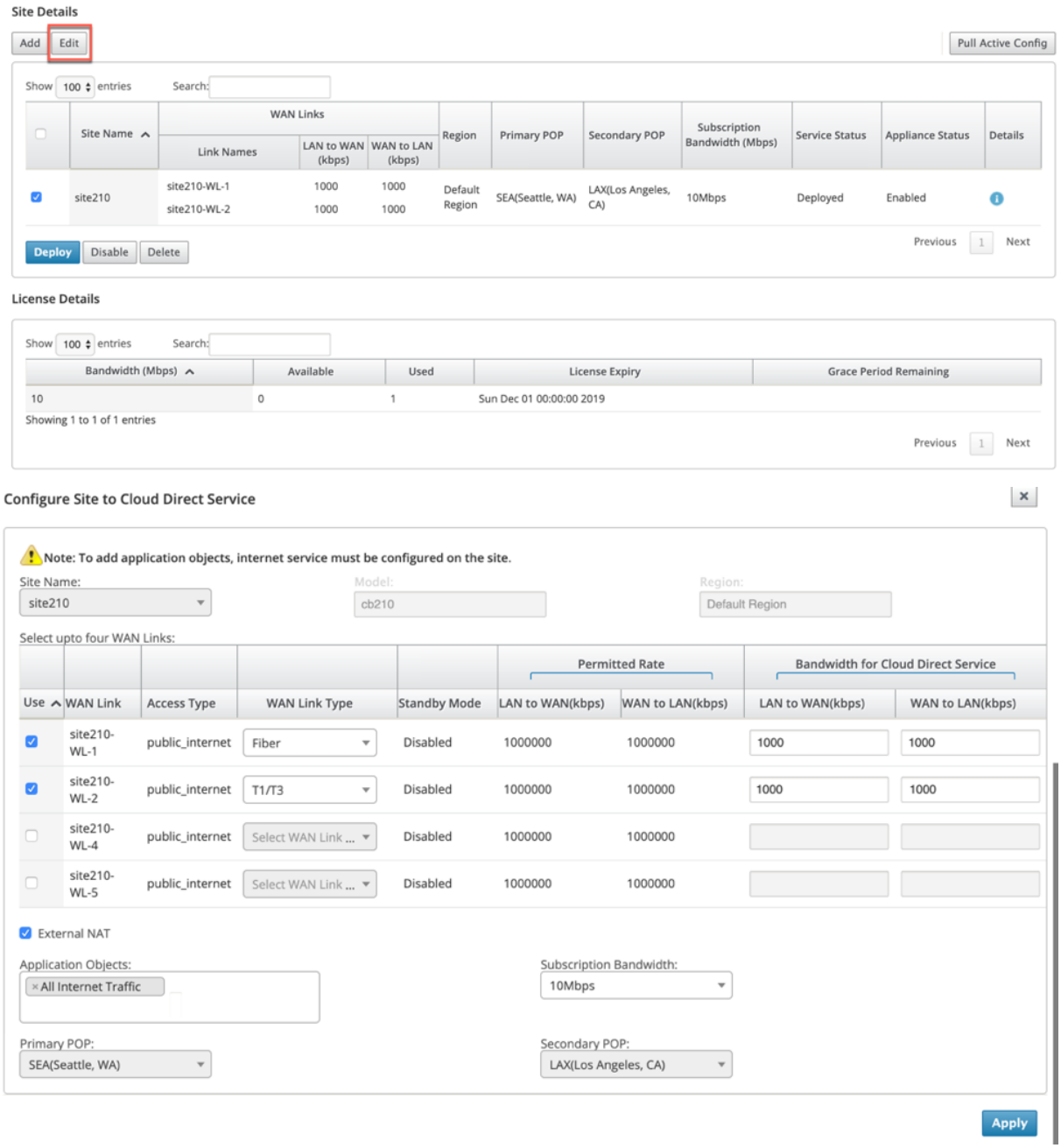
Puede ver los gráficos de resumen del sitio navegando a **Panel** > **Cloud Direct** > Resumen de **red y Resumendel sitio**.

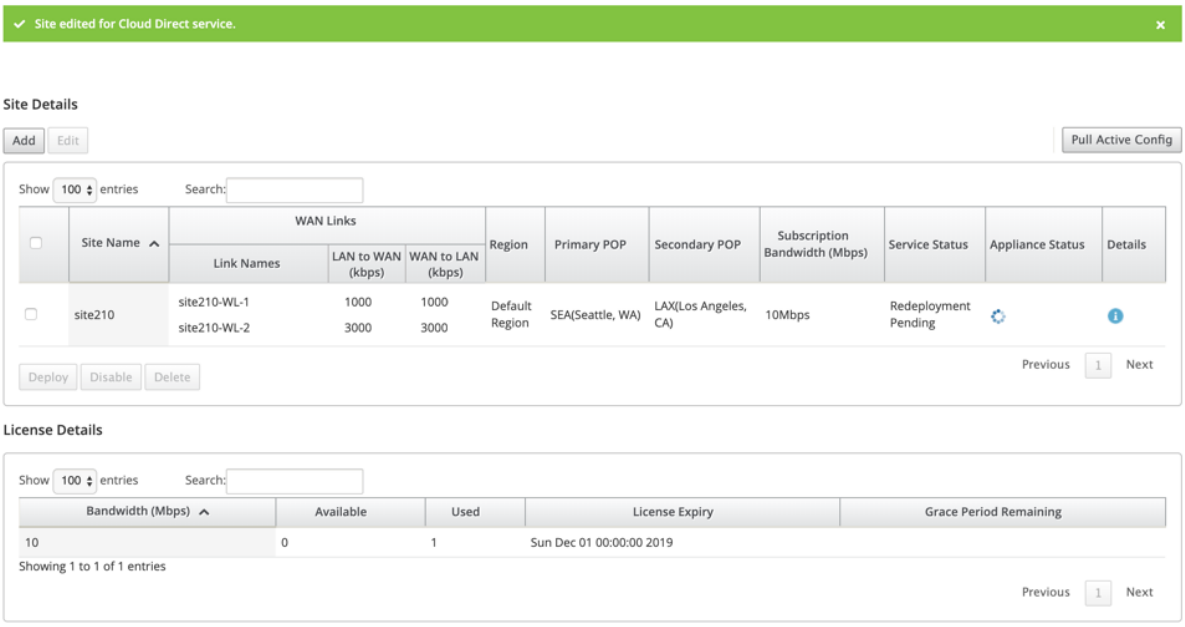


Modificar sitio en SD-WAN Center

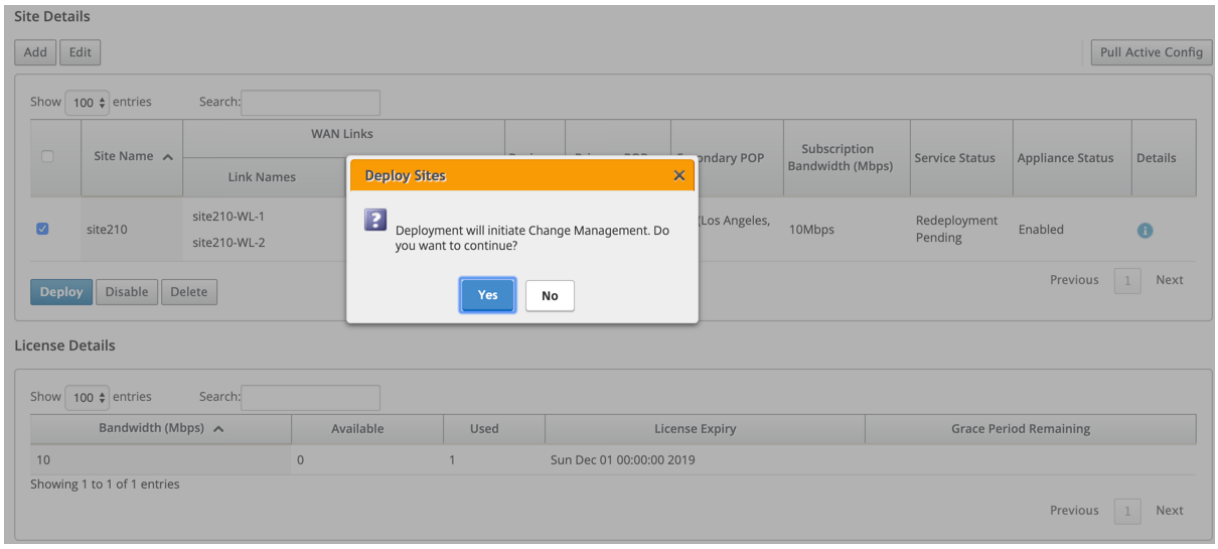
Puede elegir modificar los sitios para modificar el ancho de banda y el tipo de enlace wan.

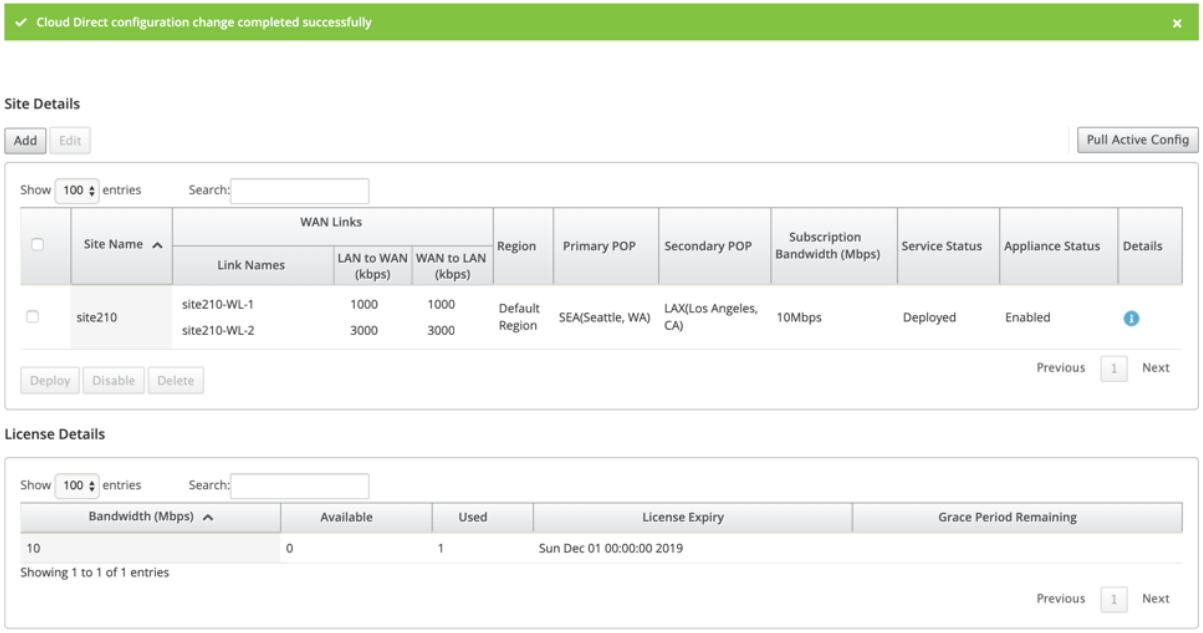
> **Nota**
>
> Las selecciones POP no se pueden modificar.





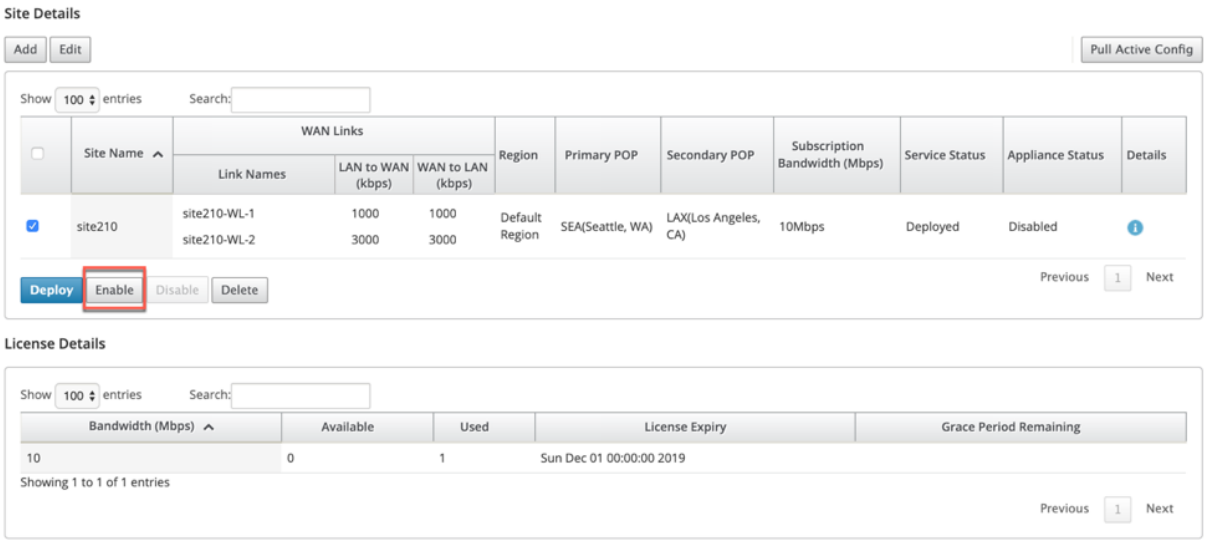
El estado del servicio se muestra como reimplementación pendiente. Implementación el sitio. El proceso de implementación se ha completado para el sitio modificado.

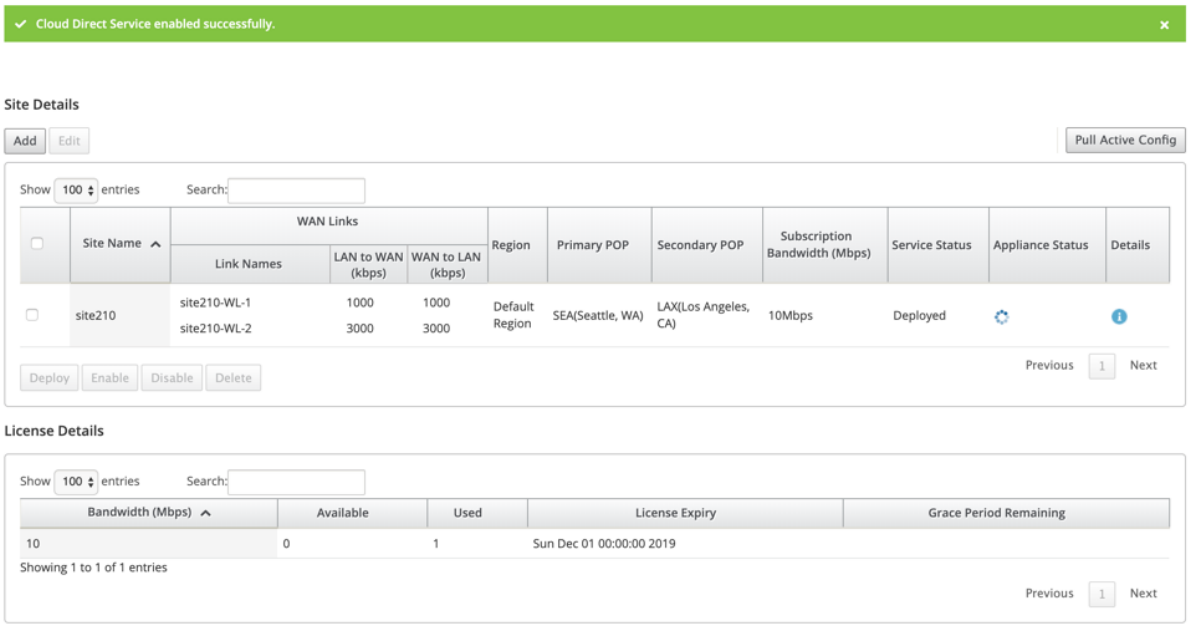




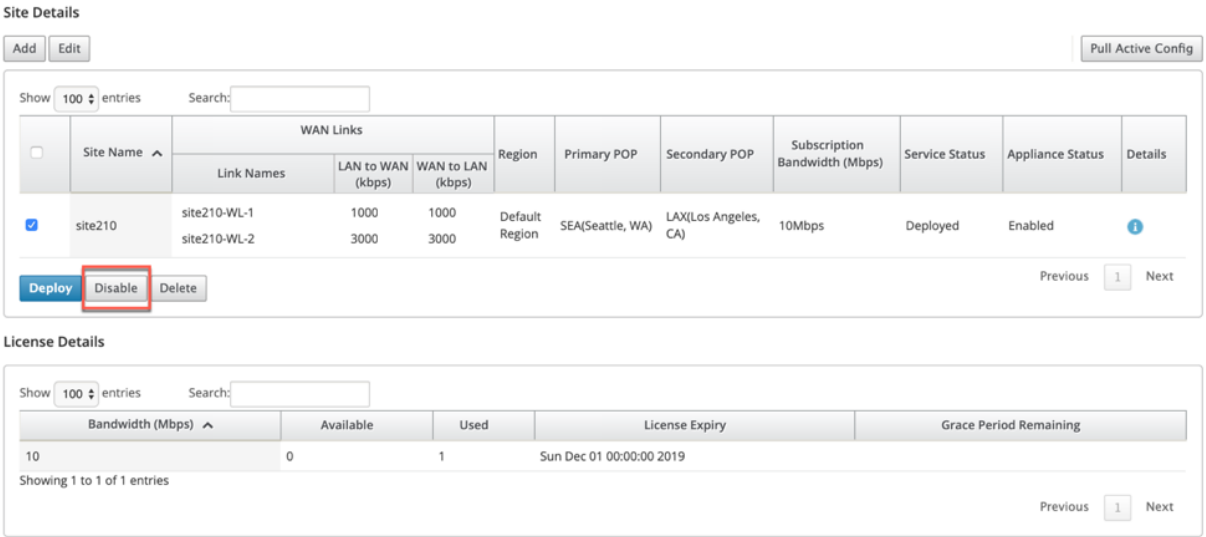
Habilitar e inhabilitar el sitio

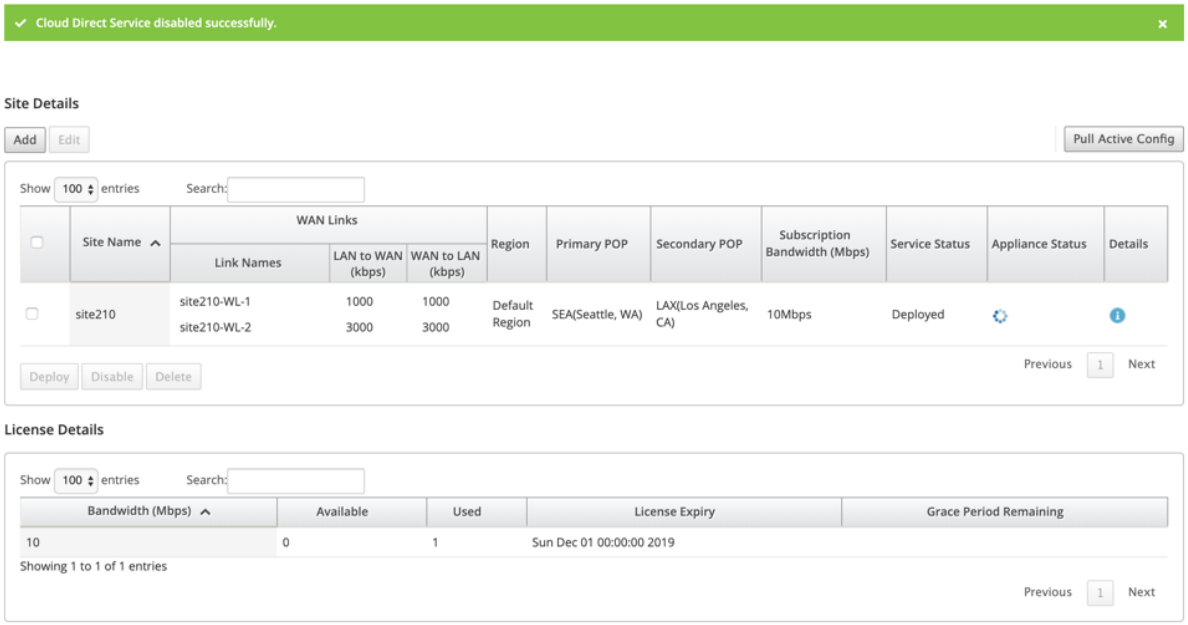
Puede habilitar un sitio implementado que tenga un estado de dispositivo como inhabilitado. Para habilitar un sitio, haga clic en **Habilitar**.





Haga clic en **Inhabilitar** para inhabilitar un sitio implementado. Inhabilitar el sitio ya no usaría el servicio directo en la nube para dirigir el tráfico de Internet. Todo el tráfico se redirige a través del servicio Internet, si está configurado en el dispositivo.

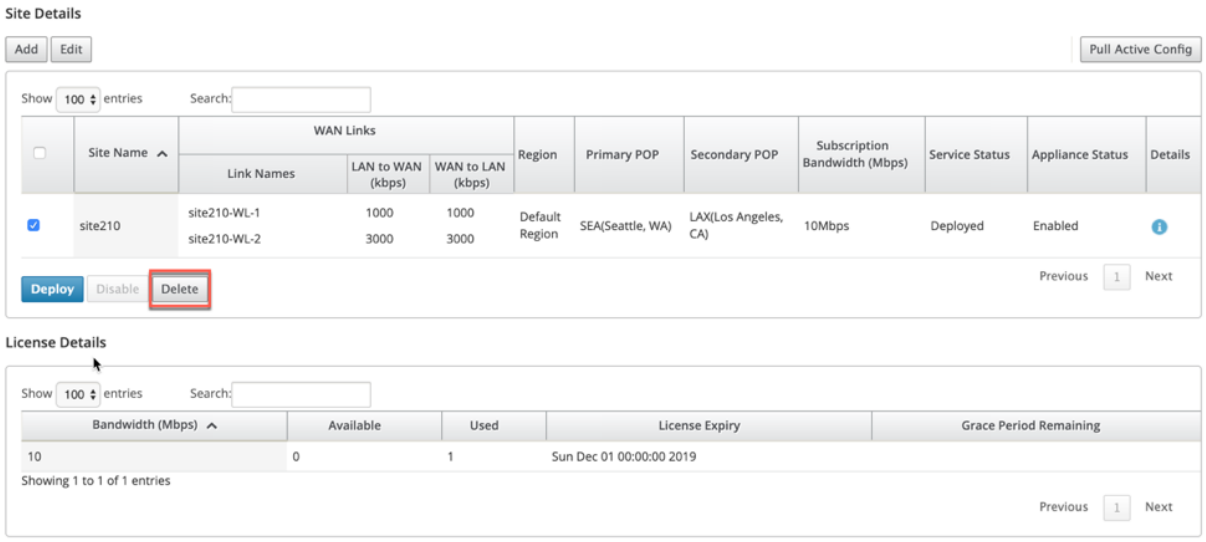


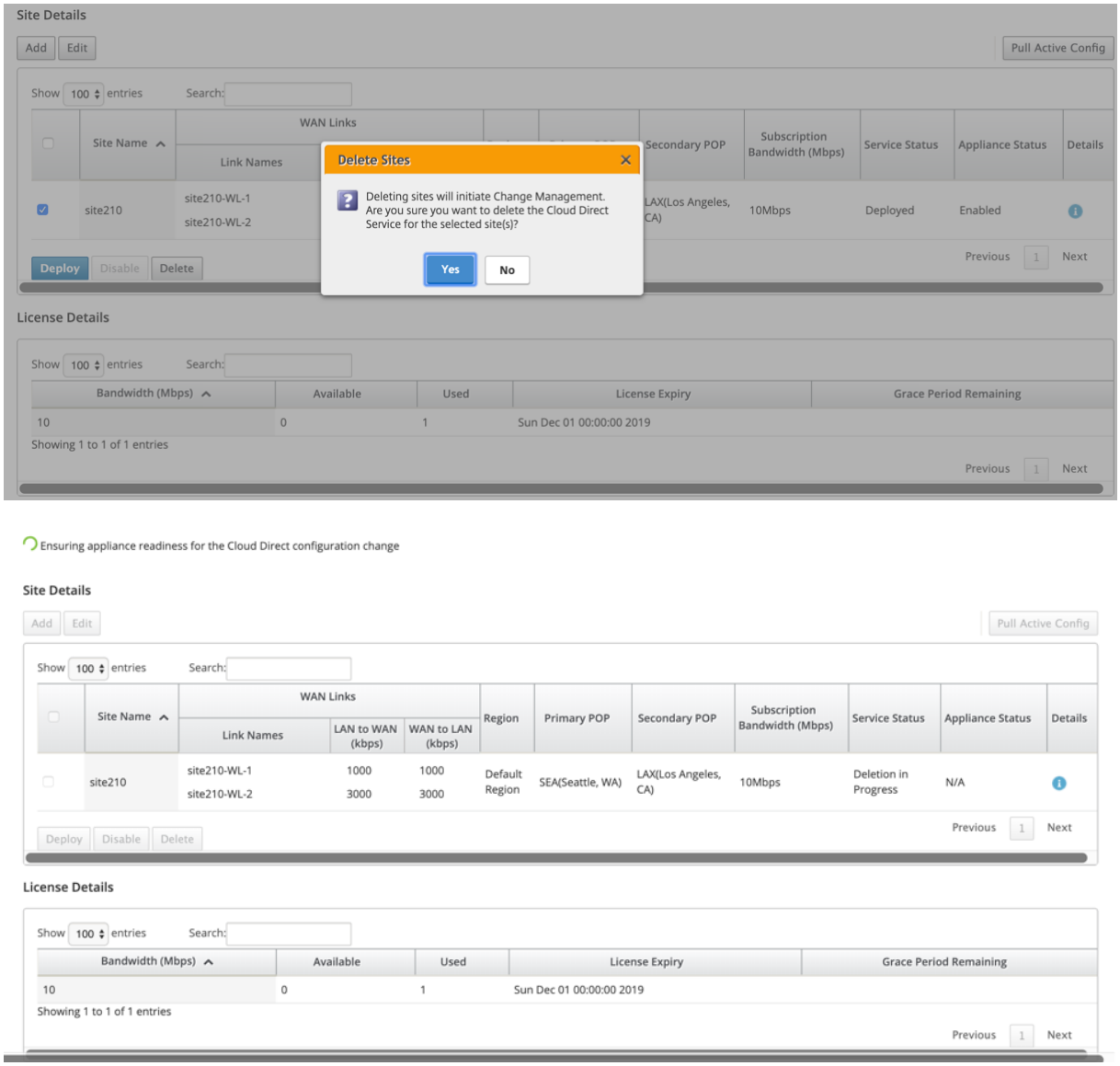


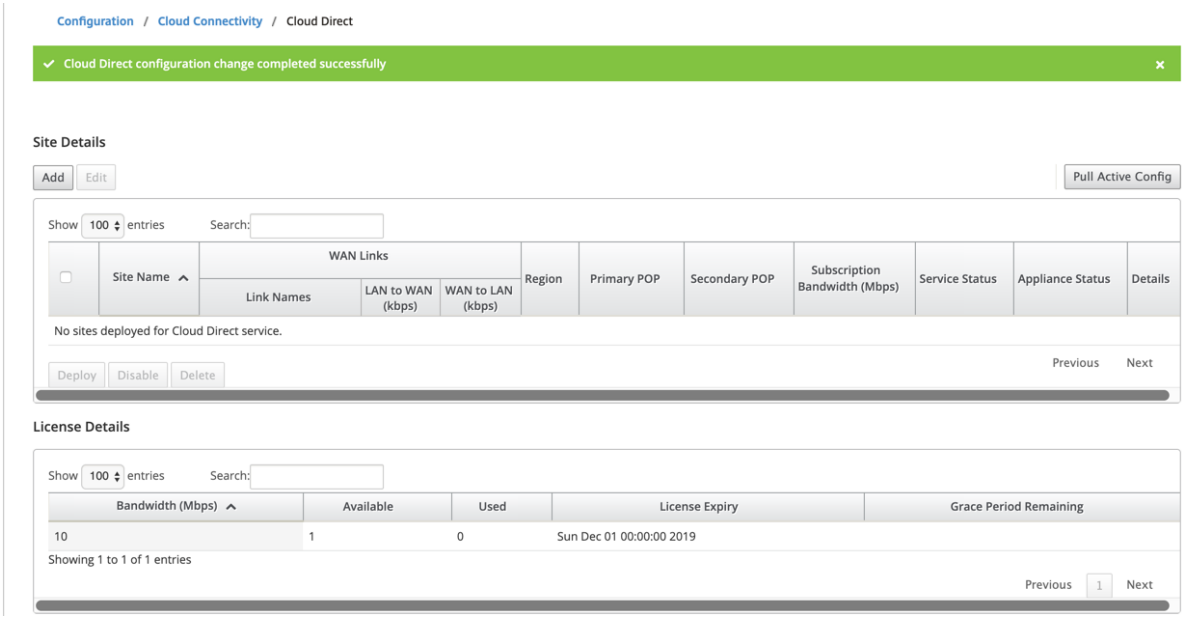
Eliminación del sitio

Puede optar por eliminar los sitios que ya no requieren conectividad de Cloud Direct. Para eliminar sitios, seleccione el sitio y haga clic en **Eliminar**. Aparece un mensaje de confirmación para eliminar sitios.

Toda la configuración del servicio directo en la nube se elimina mediante el proceso de gestión de cambios.



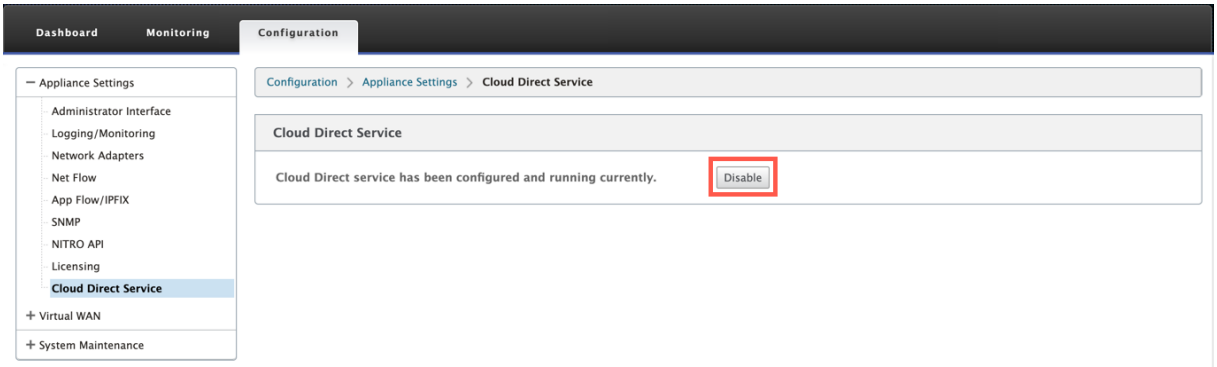




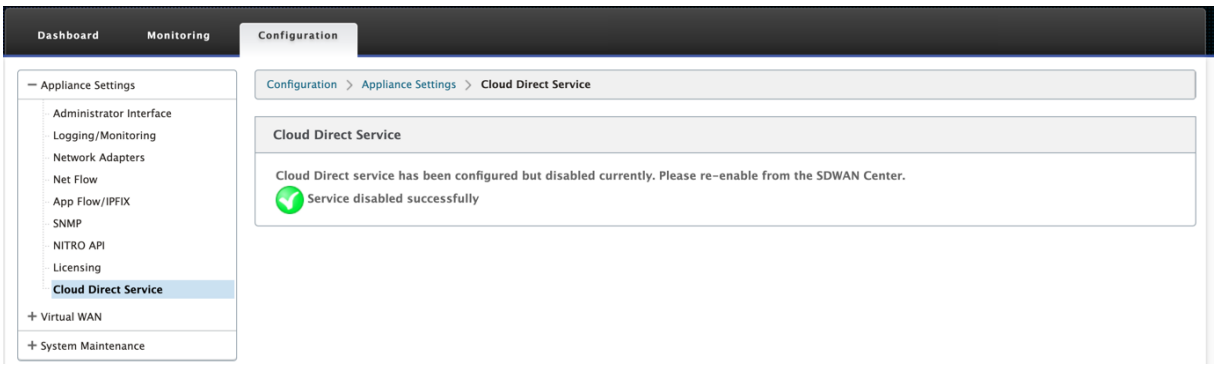
Estado del servicio Cloud Direct en Citrix SD-WAN

Puede verificar el estado del servicio Cloud Direct en un dispositivo SD-WAN local.

Vaya a la GUI de Citrix SD-WAN, vaya a **Configuración** > expanda **Configuración del dispositivo** > seleccione **Cloud Direct Service**.



Haga clic en la opción Inhabilitar para inhabilitar el servicio Cloud Direct.



Solución de problemas

Los mensajes de error más comunes que pueden producirse en SD-WAN Center al implementar el servicio Cloud Direct son los siguientes.

Los mensajes de error/estado se muestran en SDW-AN Center en **Configuración** > **Cloud Connectivity** > **Cloud Direct**.

"Error de licencia de Cloud Direct. Cargue una licencia adicional para el ancho de banda {bandwidth} Mbps"

- Cargue una licencia válida de Cloud Direct en SD-WAN Center navegando a **Configuración** > **Licencias** > **Administración de archivos** y, a continuación, continúe con la implementación de esta función

"HA de configuración de Cloud Direct debido al problema de inicio de sesión de Citrix Cloud Workspace"

- Vuelva a introducir las credenciales para el inicio de sesión de Citrix Cloud Workspace en SD-WAN Center navegando a **Configuración** > **Cloud Connectivity** opción.

"Error de procesamiento de configuración de Cloud Direct. Sitio: {site_name} (IP: {mgmt_ip}) no es accesible o falta soporte de Cloud Direct"

- Compruebe si el dispositivo o los dispositivos SD-WAN (en caso de implementación de HA) son accesibles en el puerto de administración.

"Error de comprobación de configuración de HA de configuración de Cloud Direct para el sitio: {site_name}"

- Compruebe la conectividad de ambos dispositivos en el par HA correspondiente al sitio que se está implementando.

"Tanto los dispositivos HA Pair deben ser accesibles para realizar la configuración Cloud Direct"

- Al implementar el servicio Cloud Direct en dispositivos SD-WAN en el par HA, los dispositivos secundarios y primarios deben estar accesibles en el puerto de administración.

"Error de procesamiento de configuración de Cloud Direct. Sitio: {site_name} (IP: {mgmt_ip}) tiene un problema de inicio de sesión SSO"

- Compruebe si el dispositivo SD-WAN está en funcionamiento y se puede acceder a él en el puerto de administración. Este error se muestra cuando SD-WAN Center no puede realizar el inicio de sesión único en el dispositivo SD-WAN.

"Error interno encontrado durante el procesamiento de configuración de Cloud Direct"

- Esto puede ocurrir debido a varias condiciones de error durante la comprobación de configuración o el resto del procesamiento. Es posible que un usuario tenga que revisar los registros y realizar la operación de nuevo.

"Se ha cancelado el procesamiento de configuración de Cloud Direct. MCN no está preparado para la gestión del cambio"

- Compruebe si MCN está accesible y en funcionamiento y que su estado de administración de cambios es "network_staging".

"Error de procesamiento de configuración de Cloud Direct. Sitio: {site_name} (IP: {mgmt_ip}) no tiene soporte para Cloud Direct. Realice una actualización de un solo paso para tener un soporte de Cloud Direct"

- Realice una actualización de software de un solo paso en el dispositivo SD-WAN a través de **MCN** > **Administración de cambios**. Después de este procedimiento, vuelva a intentar implementar el servicio Cloud Direct para este sitio.

"Error de procesamiento de configuración de Cloud Direct. Error en la operación de administración de cambios de WAN SD"

- La operación de administración de cambios de alguna manera no tuvo éxito. Compruebe los registros del Centro de SD-WAN para obtener más detalles.

"Error de procesamiento de configuración de Cloud Direct. Error al habilitar el servicio en el sitio: {site_name}"

- No se puede habilitar el servicio Cloud Direct en el dispositivo SD-WAN. Compruebe si hay conectividad de un dispositivo específico o de aquellos en el par HA o si hay algún problema al realizar

el inicio de sesión único. Compruebe los registros en el Centro y el dispositivo SD-WAN para obtener más detalles.

"Error de procesamiento de configuración de Cloud Direct. Error al inhabilitar el servicio en el sitio: {site_name}"

- No se puede inhabilitar el servicio Cloud Direct en el dispositivo SD-WAN. Compruebe si hay conectividad de un dispositivo específico o de aquellos en el par HA o si hay algún problema al realizar el inicio de sesión único. Compruebe los registros en el Centro y el dispositivo SD-WAN para obtener más detalles.

"Error de procesamiento de configuración de Cloud Direct. Configuración de la inserción de imagen en el sitio: {site_name} falló"

- No se puede cargar la imagen específica del servicio en el dispositivo a través de la API REST o no se puede acceder a ambos dispositivos en el par HA.

"Cloud Direct Service encontró un error durante el procesamiento de la configuración. Errores de auditoría encontrados en la configuración de SD-WAN"

- Se encontraron errores de auditoría al intentar compilar la configuración de SD-WAN. Compruebe los registros del Centro de SD-WAN para obtener más detalles.

"Error de procesamiento de configuración de Cloud Direct. Error al crear sitio para el sitio: {site_name}"

- Error del lado del servicio al intentar crear un sitio para el dispositivo SD-WAN correspondiente. Revise los registros del Centro SD-WAN para obtener más detalles.

"Error de procesamiento de configuración de Cloud Direct. Error al actualizar el sitio para el sitio: {site_name}"

- Error del lado del servicio al intentar modificar la configuración relacionada con el sitio para el dispositivo SD-WAN correspondiente. Revise los registros del Centro SD-WAN para obtener más detalles.

Mensajes de error observados en los registros (SDWAN_common.log)

A continuación se presentan algunos escenarios en los que el servicio Cloud Direct se implementa en el dispositivo SD-WAN, pero es posible que no funcione como se esperaba. Puede descargar y revisar los registros del dispositivo SD-WAN local mediante SDWAN_common.log para obtener más detalles.

Caso 1

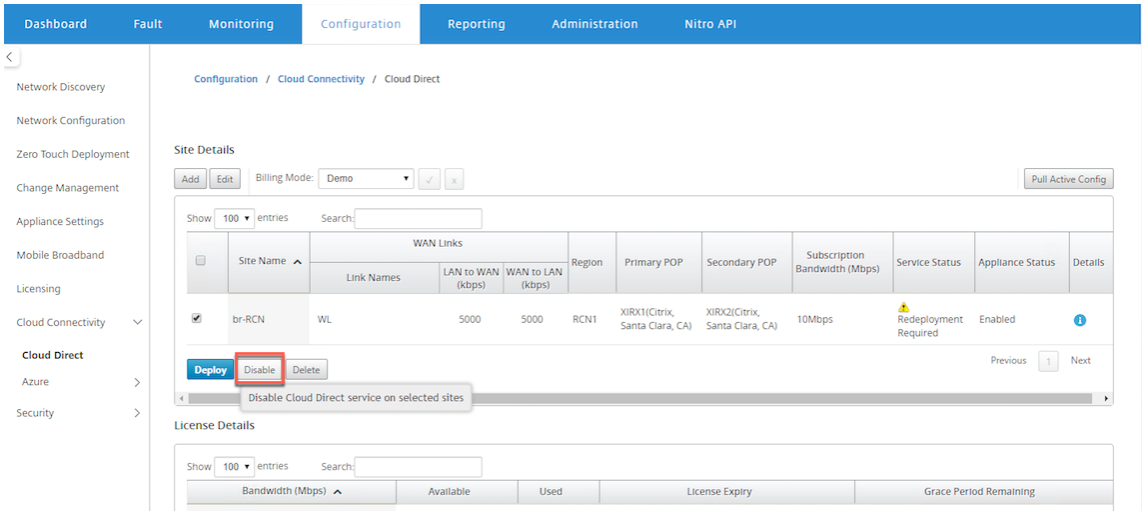
"La VM detectada de Cloud Direct no responde…Inhabilite Cloud Direct Service". "El servicio Cloud Direct ha sido inhabilitado." El KVM subyacente que se ejecuta en el dispositivo SD-WAN local no funciona de la manera esperada. En tal caso, la funcionalidad del servicio Cloud Direct está inhabilitada en el dispositivo.

Caso 2

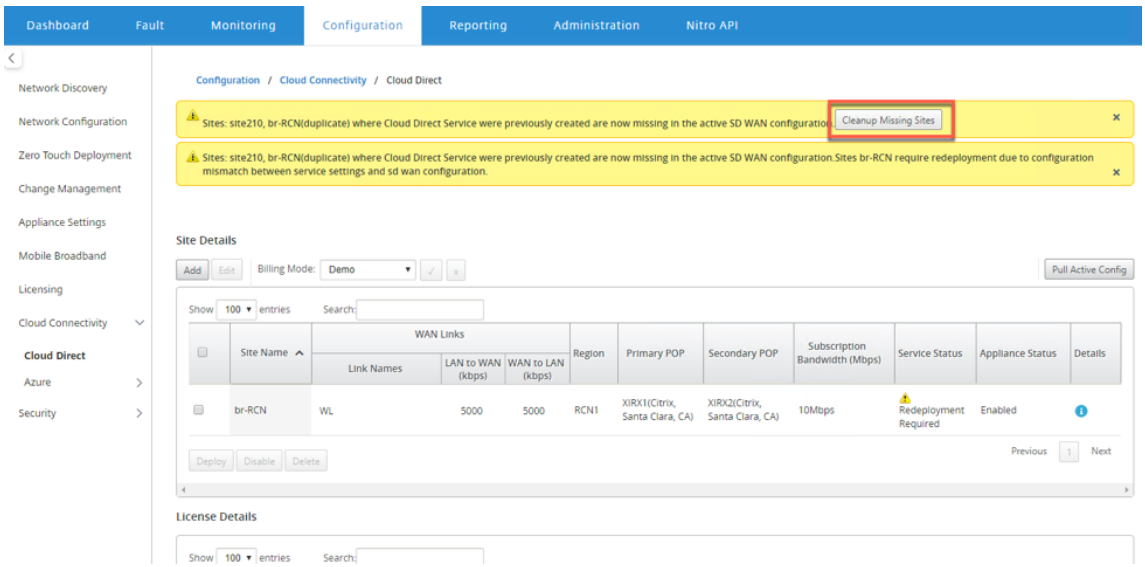
"No se han visto paquetes de túnel durante los últimos 5 minutos…Inhabilite Cloud Direct Service". "El servicio Cloud Direct ha sido inhabilitado." No hay ningún túnel establecido entre el dispositivo SD-WAN y el extremo de túnel en uso para el servicio Cloud Direct. Esto puede deberse a una configuración incorrecta de wan-link, falta de conectividad a Internet a través de wan-link configurado, imagen de datos o configuración incompatible o no válida enviada al dispositivo o a cualquier regla de firewall que pueda estar dejando caer paquetes de túnel UDP cuando se reciben a través de wan-link. En tal caso, la funcionalidad del servicio Cloud Direct está inhabilitada en el dispositivo.

Cuando activa una configuración en MCN con diferente configuración de Cloud Direct (Por ejemplo: la configuración de NAT se cambia para Cloud Direct) y podría provocar la interrupción permanente del tráfico. Para superar este bloque, puede seguir uno de los siguientes pasos para seleccionar las diferentes rutas presentes en el dispositivo:

1. En la GUI de SD-WAN Center, vaya a **Configuración** > **Conectividad en la nube** > **Cloud Direct**. Seleccione el dispositivo directo en la nube y haga clic en la opción **Inhabilitar** para inhabilitar el servicio directo en la nube.



2. Vaya a **Configuración** > **Cloud Connectivity** > **Cloud Direct** y extraiga la configuración activa para obtener la notificación de limpieza. Puede hacer clic en el botón de notificación **Limpiar sitios faltantes** que se muestra para el dispositivo cloud direct afectado. Esta operación inhabilita el servicio Cloud Direct que se ejecuta en el dispositivo.



3. Redespliegue el servicio Cloud Direct en SD-WAN Center para utilizar el servicio Cloud Direct para los dispositivos afectados.

Integre Citrix SD-WAN y Zscaler mediante Citrix SD-WAN Center

April 13, 2021

Citrix SD-WAN y Zscaler ayudan a las empresas a transformar su WAN para la migración a la nube

al proporcionar interrupciones locales seguras a aplicaciones y recursos alojados en Internet. Las nuevas tecnologías de infraestructura WAN, como SD-WAN, aumentan la agilidad y la escalabilidad de la red, al tiempo que reducen los costes y la complejidad para mejorar la experiencia del usuario en las organizaciones distribuidas.

Las soluciones SD-WAN simplifican el enrutamiento al permitir que el tráfico destinado a la nube se desconecte a Internet localmente. SD-WAN proporciona flexibilidad para enrutar el tráfico a Internet (eliminar el entorno de CC central) mediante el uso de funciones de dirección de aplicaciones. Sin embargo, exponer la red a Internet plantea riesgos significativos para la seguridad. Un enfoque centralizado para proteger la ruptura local a través de un servicio en la nube elimina la sobrecarga de mantenimiento de la infraestructura de seguridad en las sucursales. Todo el tráfico se enruta de forma fiable y segura a Zscaler (plataforma de seguridad basada en la nube) con Citrix SD-WAN en la red de sucursales. Puede eliminar la costosa infraestructura y proteger su red de amenazas y vulnerabilidades.

Citrix SD-WAN

Citrix SD-WAN ayuda a las empresas a trasladarse a la nube al habilitar de forma segura las rupturas locales de ramificación a Internet con un firewall con estado integrado para crear directivas que permitan o denieguen el acceso a Internet directamente desde la sucursal. Citrix SD-WAN identifica aplicaciones mediante una combinación de una base de datos integrada de más de 4.000 aplicaciones, incluidas aplicaciones SaaS individuales, y utiliza tecnología de inspección profunda de paquetes para detectar y clasificar aplicaciones en tiempo real. Utiliza este conocimiento de aplicación para dirigir el tráfico de la sucursal a Internet, nube o SaaS.

Zscaler

Zscaler es la plataforma de seguridad basada en la nube líder, que ofrece una seguridad superior sin necesidad de hardware, dispositivos o software locales. Zscaler pone un perímetro alrededor de Internet, de modo que las empresas no necesitan poner un perímetro de seguridad alrededor de cada oficina. Zscaler Cloud Security Platform actúa como una serie de puestos de comprobación de seguridad en más de 100 centros de datos en todo el mundo. Al redirigir el tráfico de Internet a Zscaler, las empresas pueden proteger instantáneamente almacenes, sucursales y ubicaciones remotos. Zscaler conecta usuarios e Internet, inspeccionando cada byte de tráfico, incluso si está cifrado o comprimido, para que los usuarios estén seguros y todas las amenazas ocultas se identifiquen antes de que puedan infiltrarse en la red empresarial.

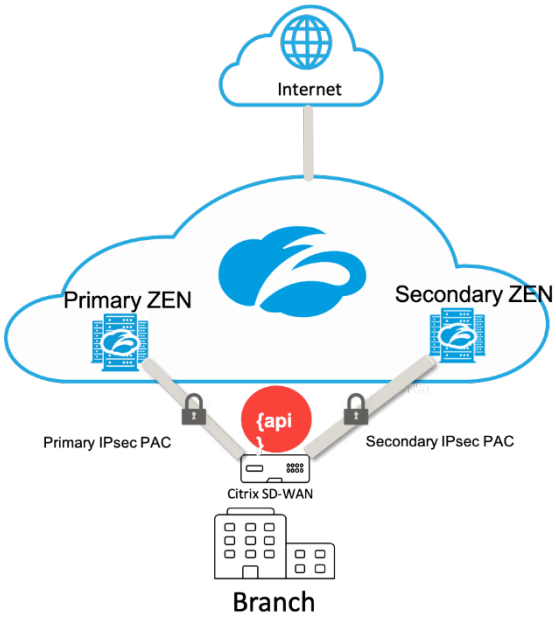
Citrix SD-WAN permite crear directivas que permiten la separación directa de Internet desde la sucursal y la plataforma de seguridad en la nube de Zscaler garantiza la seguridad de TI mediante la inspección de todo el tráfico enlazado a Internet en un servicio en la nube cercano a donde se conectan los usuarios.

Nodos de aplicación de Zscaler (ZENs)

Citrix SD-WAN admite las API de Zscaler para automatizar la creación de túneles IPSec entre Citrix SD-WAN y Zscaler Enforcement Nodes (ZENs) en la red en la nube de Zscaler. Las ZENs son puertas de enlace de seguridad de Internet en línea con todas las funciones que inspeccionan todo el tráfico de Internet de forma bidireccional en busca de malware y aplican directivas de seguridad y cumplimiento.

La API de Zscaler proporciona las dos ubicaciones de centro de datos más cercanas a cada sucursal, lo que permite a SD-WAN dirigir el tráfico con eficacia. Las organizaciones pueden permitir que Zscaler elija automáticamente el ZEN más cercano a la sucursal haciendo que ZEN observe las direcciones IP de los enlaces WAN configurados en Citrix SD-WAN o puede seleccionar manualmente las **ZENs**.

> **NOTA**
>
> Ambas rutas siempre estarán en modo activo si el túnel es UP. Si algún túnel desciende, la ruta correspondiente se vuelve inalcanzable y la otra ruta se mantenga ARRIBA en ese caso.



Ventajas

Las ventajas de integrar Citrix SD-WAN y Zscaler incluyen:

- Adopción más rápida de SaaS y nube en una empresa distribuida.
  - Centralizar la seguridad como servicio en la nube elimina la necesidad de tenerla en cada sucursal.

  - Eliminar la necesidad de devolver el tráfico destinado a Internet, lo que permite la ruptura local de Internet en la sucursal.

- Administración de TI simplificada con conectividad automatizada a un Secure Web Gateway.
  - La compatibilidad con API automatiza la configuración de túneles seguros a Zscaler
- Experiencia mejorada del usuario al reducir la latencia del tráfico SaaS de backhauling.
  - Elimina la dependencia del modelo de hub-and-radial por motivos de seguridad
- Eliminación de costosas pilas de seguridad en sucursales
  - Reduzca la sobrecarga de tener que implementar y administrar firewalls en las sucursales.
- Garantía de que el tráfico vinculado a Internet siempre es seguro.
  - Las directivas de seguridad no vinculan a los usuarios a una ubicación física.
  - Proporciona espacio aislado, inspección de todos los puertos y protocolos, incluido SSL, filtrado de URL, protección avanzada contra amenazas y mucho más para protegerse contra ataques de día cero.

Funcionalidad compatible

Una implementación de Zscaler que utiliza dispositivos SD-WAN admite la siguiente funcionalidad:

- Reenviar tráfico de Internet definido por el usuario a Zscaler, permitiendo así la interrupción directa de Internet.
- Acceso directo a Internet (DIA) mediante Zscaler en base a un sitio por cliente.
  - En algunos sitios, es posible que quiera proporcionar a DIA equipo de seguridad local y no utilizar Zscaler.
  - En algunos sitios, puede optar por realizar una copia de seguridad del tráfico a otro sitio del cliente para acceder a Internet.
- Implementaciones de redirección y reenvío virtuales.
- Un enlace WAN como parte de los servicios de Internet.

Zscaler es un servicio en la nube. Debe configurarlo como un servicio y definir los enlaces WAN subyacentes:

- Configure un vínculo WAN de Internet público de confianza en el centro de datos y en los sitios de sucursal.
- Configuración automática de túneles IPSec para servicios de intranet.

Implementación de Zscaler en el flujo de trabajo de Citrix SD-WAN Center

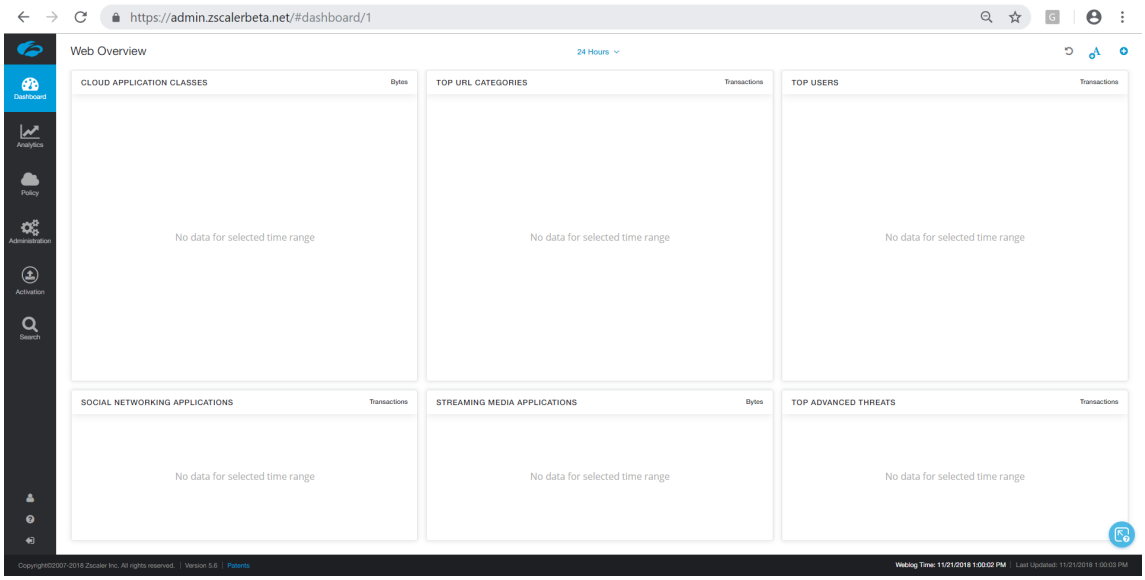
Los siguientes son los pasos de alto nivel que definen el flujo de trabajo para implementar Zscaler en SD-WAN Center.

1. Configure la suscripción de Zscaler a SD-WAN Center (una sola vez). Inicie sesión en el Zscaler sitio para obtener información de suscripción.
2. Seleccione **Implementar** en la GUI de Citrix SD-WAN Center.
    - Implementar la configuración para el sitio mediante Internet wan-link y objeto de aplicación preconfigurado.
    - Establecer conectividad.
    - Obtener/Actualizar el estado IPSec.

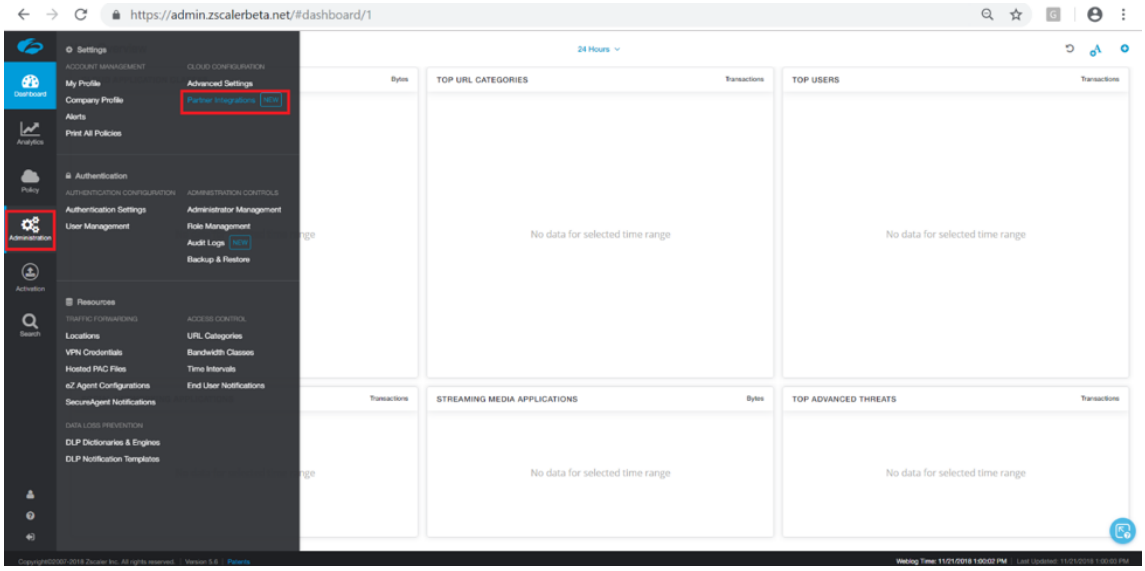
Suscripción a Zscaler

Antes de continuar con la configuración de Zscaler en SD-WAN Center, debe iniciar sesión en el portal de Zscaler.

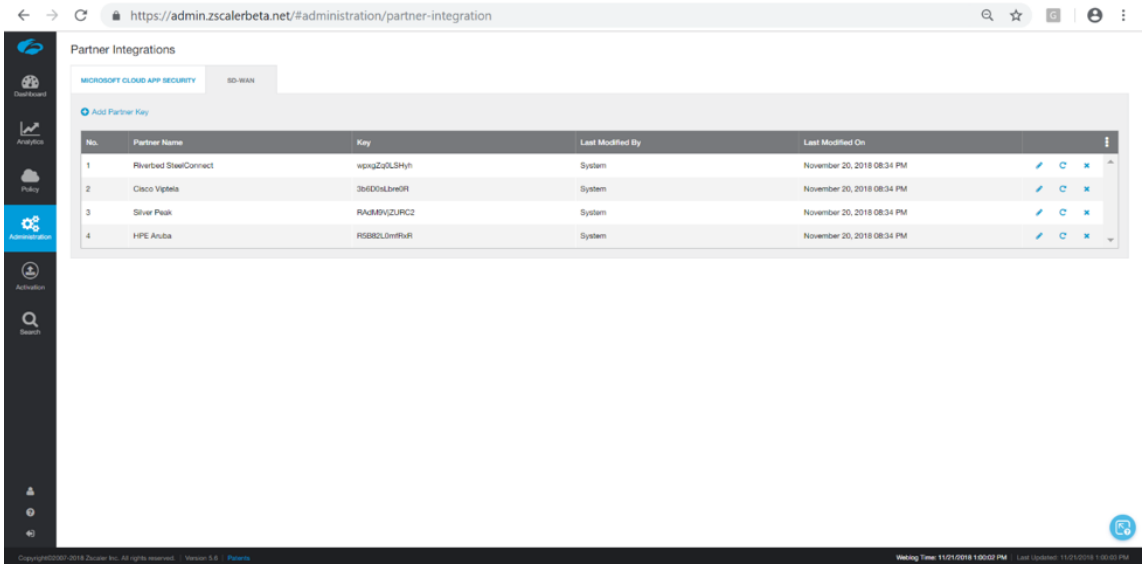
1. Inicie sesión en el Zscaler sitio para obtener información de suscripción. Se abrirá la página Panel de control.

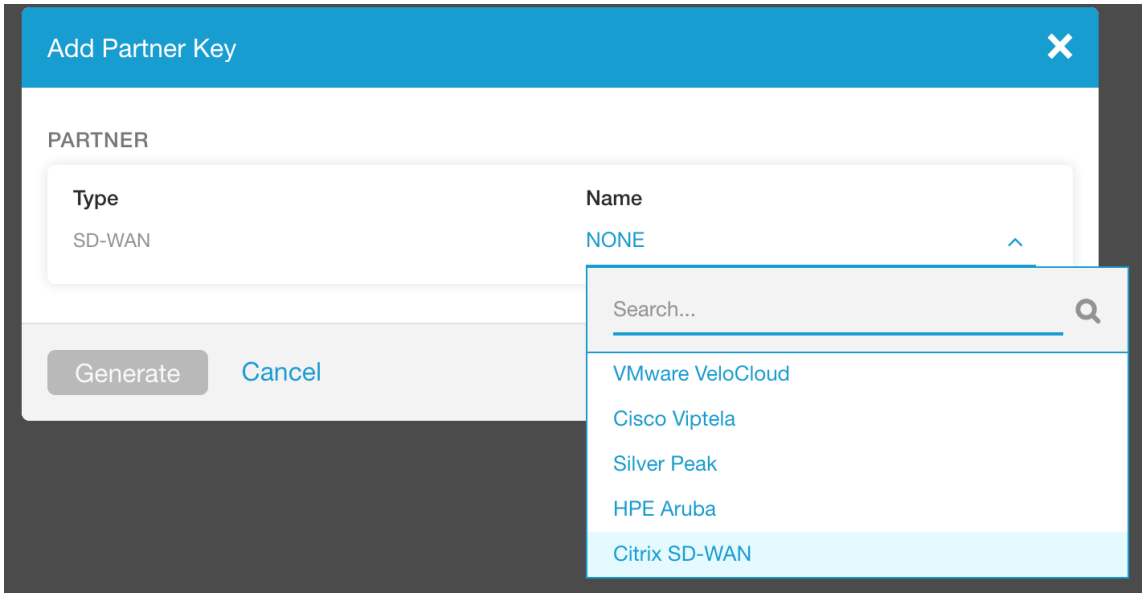


2. Haga clic en **Administración > Integraciones de socios**.



3. Seleccione **SD-WAN** en la página **Integraciones de partners**. Haga clic en **Agregar clave de socio**.

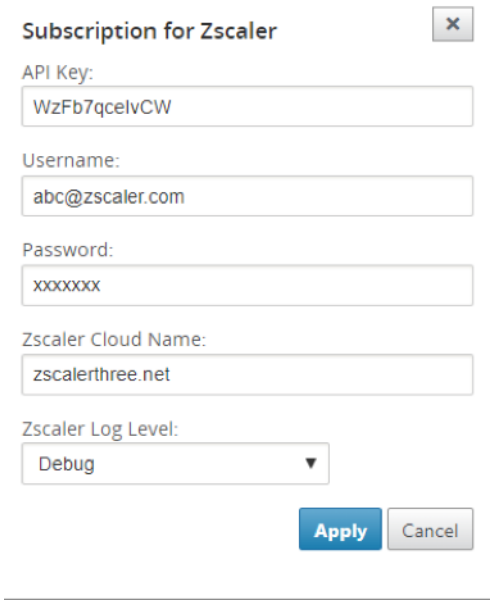




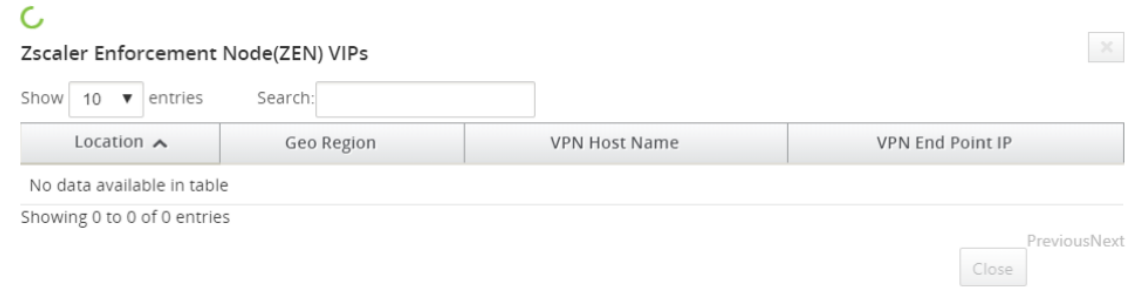
4. Elija **Citrix SDWAN** para la clave de socio y haga clic en **Generar**. Guarde la llave.

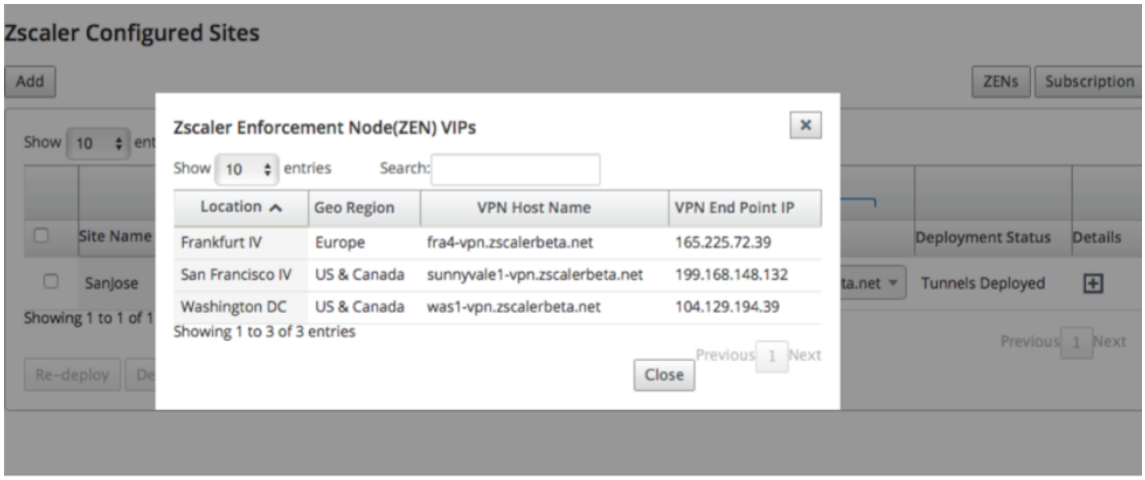
Configurar Zscaler en Citrix SD-WAN Center

1. En la GUI de Citrix SD-WAN Center, vaya a la página **Configuración > Seguridad**. Se abrirá la página **Sitios configurados de Zscaler**.
2. Haga clic en **Suscripción**. Introduzca la API de Zscaler (clave de socio) creada en los pasos anteriores. Proporcione su nombre de **usuario** y **contraseña**de Zscaler. Seleccione **Zscaler Cloud Name**, **Zscaler Log Level**y haga clic en **Aplicar**.

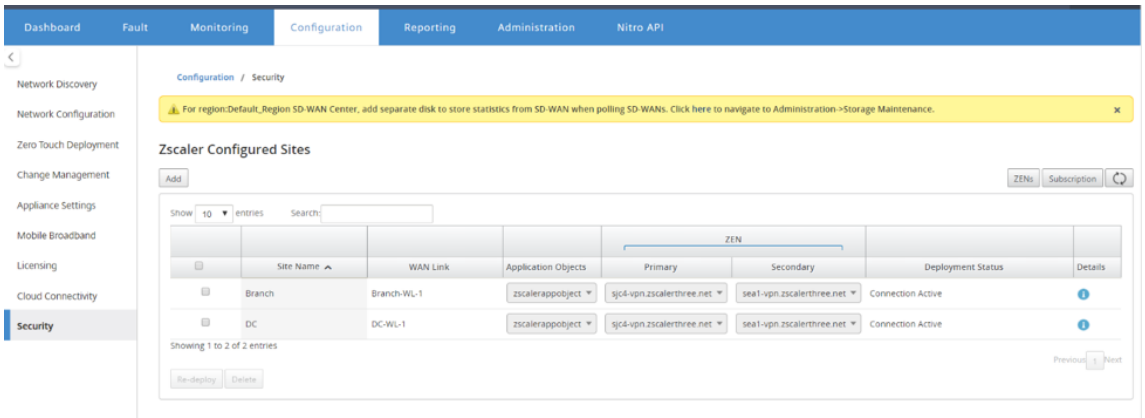


3. Zens proporciona la lista de endpoints VPN disponibles para esta suscripción a la nube de Zscaler.

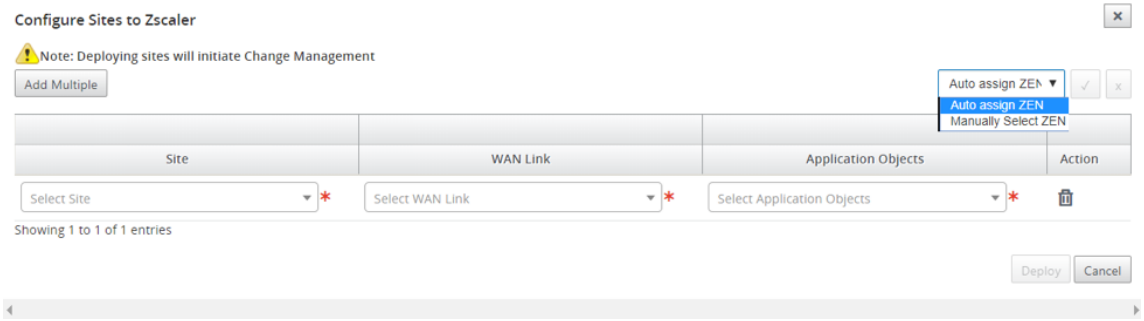




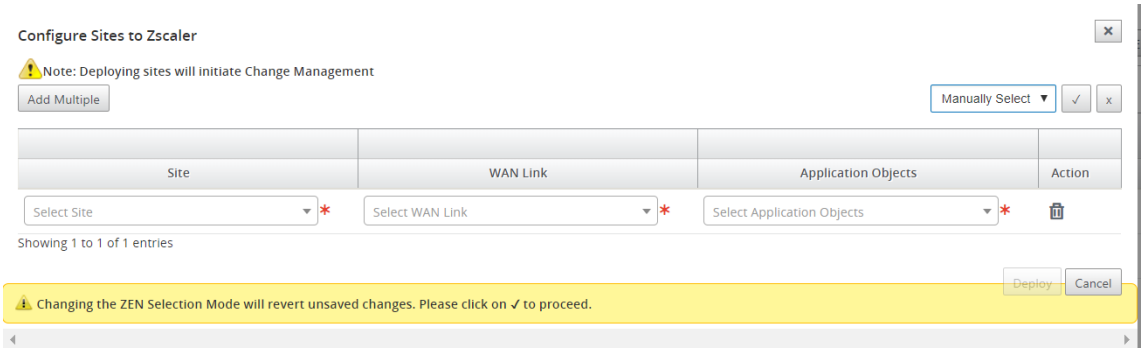
4. Después de introducir la suscripción a Zscaler y los detalles del ZEN, puede comenzar a agregar sitios a Zscaler. Haga clic en **Agregar**.



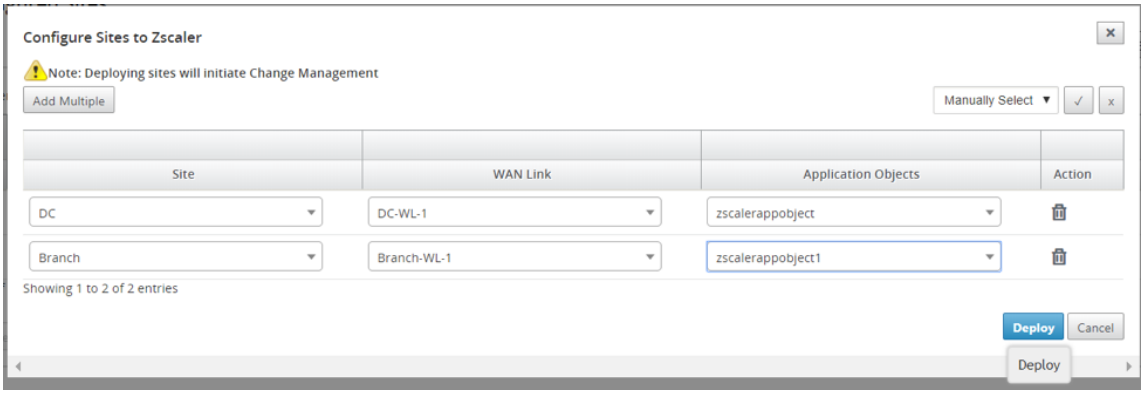
5. En el cuadro de diálogo **Configurar sitios en Zscaler**, agregue **Sitio, Enlace WAN** y **Objetos de aplicación**. De forma predeterminada, se selecciona la opción **Asignar ZEN automáticamente**.

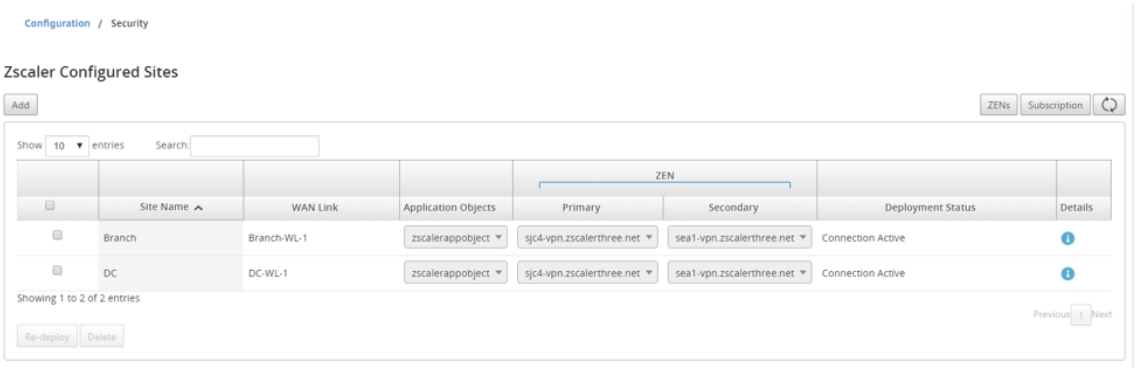


Puede **seleccionar manualmente el ZEN**. Sin embargo, aparece el siguiente mensaje notificando que se pierden los cambios no guardados.



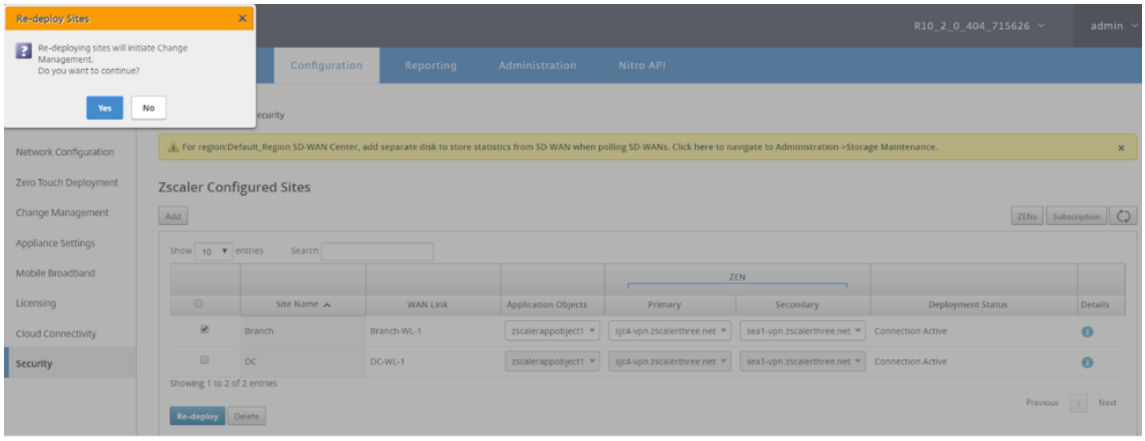
6. Seleccione los sitios necesarios y haga clic en **Implementar**. Puede optar por agregar varios sitios seleccionando **Agregar varios**. Los sitios seleccionados se implementan y se muestra la página de configuración.



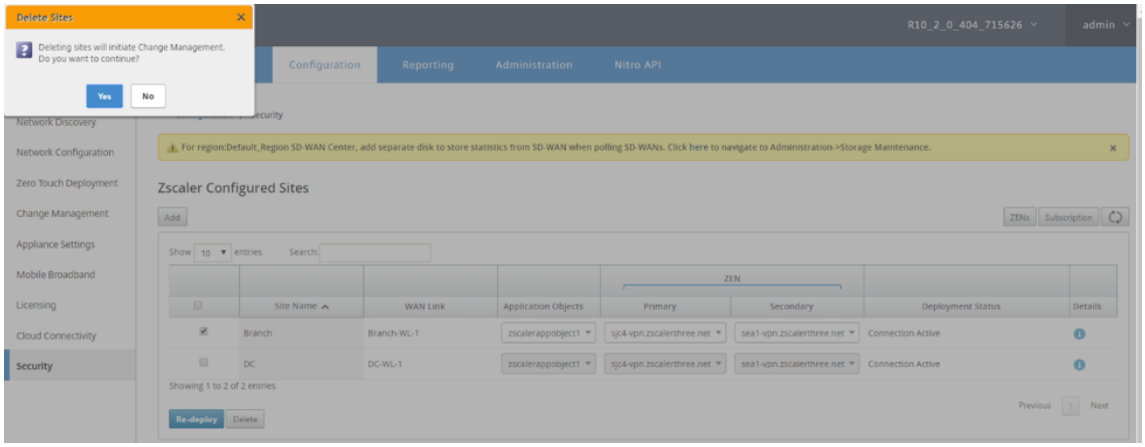


Observe que las direcciones IP ZEN primarias y secundarias están rellenadas y que el estado de implementación es **Conexión activa**.

7. Haga clic en **Reimplementar** si realiza cambios en los extremos de VPN u objetos de aplicación del sitio configurado. Cualquier cambio en los sitios configurados en el Centro de SD-WAN desencadena un proceso de **administración de cambios** en los dispositivos configurados en los sitios de sucursal y los sitios de DC.

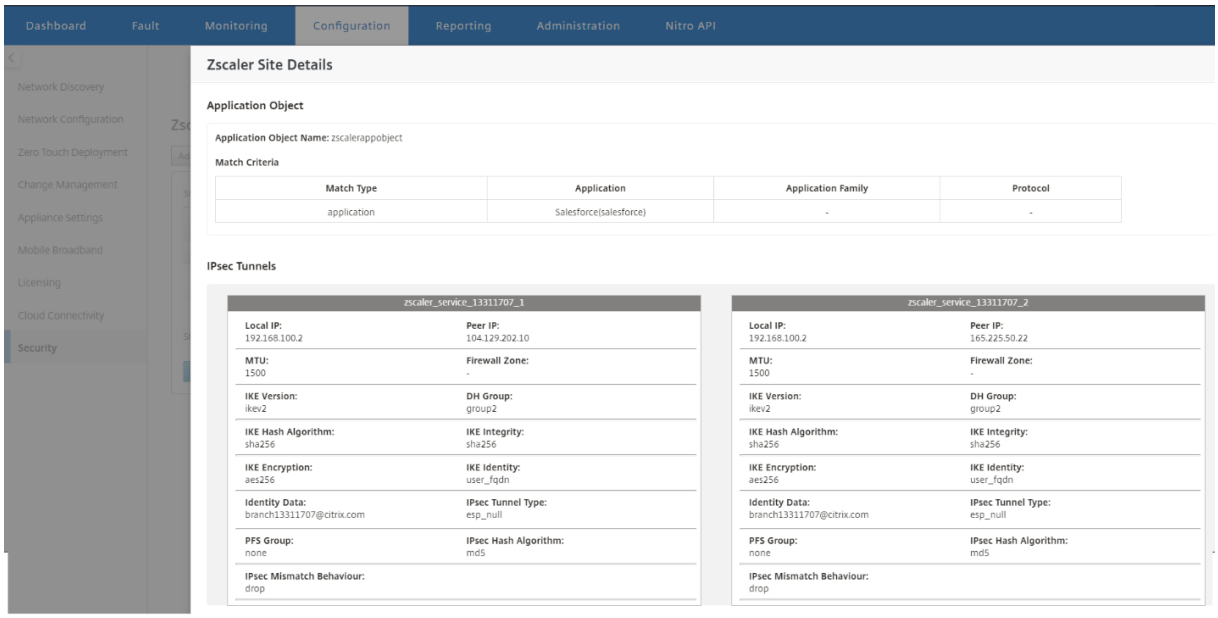


La eliminación de sitios también desencadena el proceso de administración de cambios.



Supervisión y solución de problemas

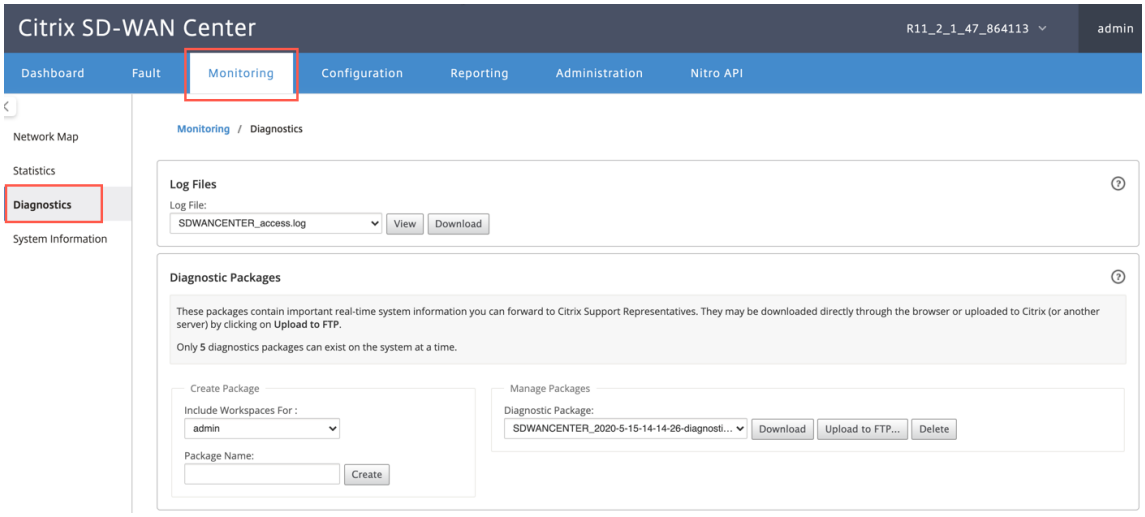
Seleccione sitios configurados para ver más información sobre Objetos de aplicación y direcciones IP primario/secundarias. Puede hacer clic en el icono **Detalles** para ver información completa sobre los sitios configurados.



Puede ver y descargar los registros de Zscaler que se pueden utilizar para solucionar problemas en Citrix SD-WAN Center.

Para ver los archivos de registro de Zscaler:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Supervisión** > **Diagnósticos**.

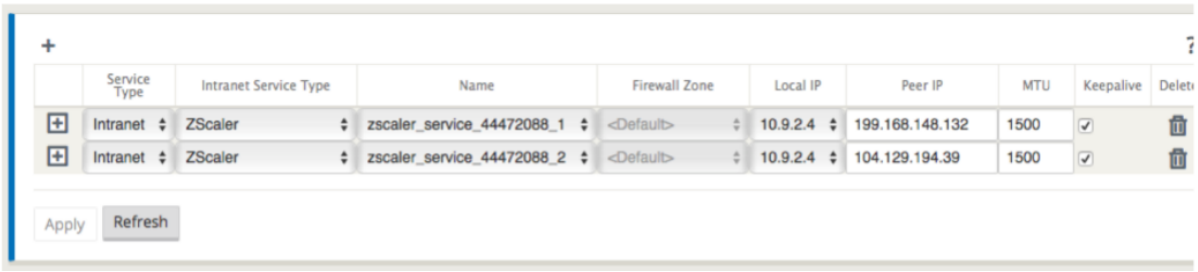


2. En la lista desplegable **Archivo de registro**, seleccione el archivo de registro de Zscaler que desea ver. Haga clic en **Ver**.

3. Si quiere descargar los archivos de registro en el equipo, haga clic en **Descargar**.

Configuración del túnel IPSec

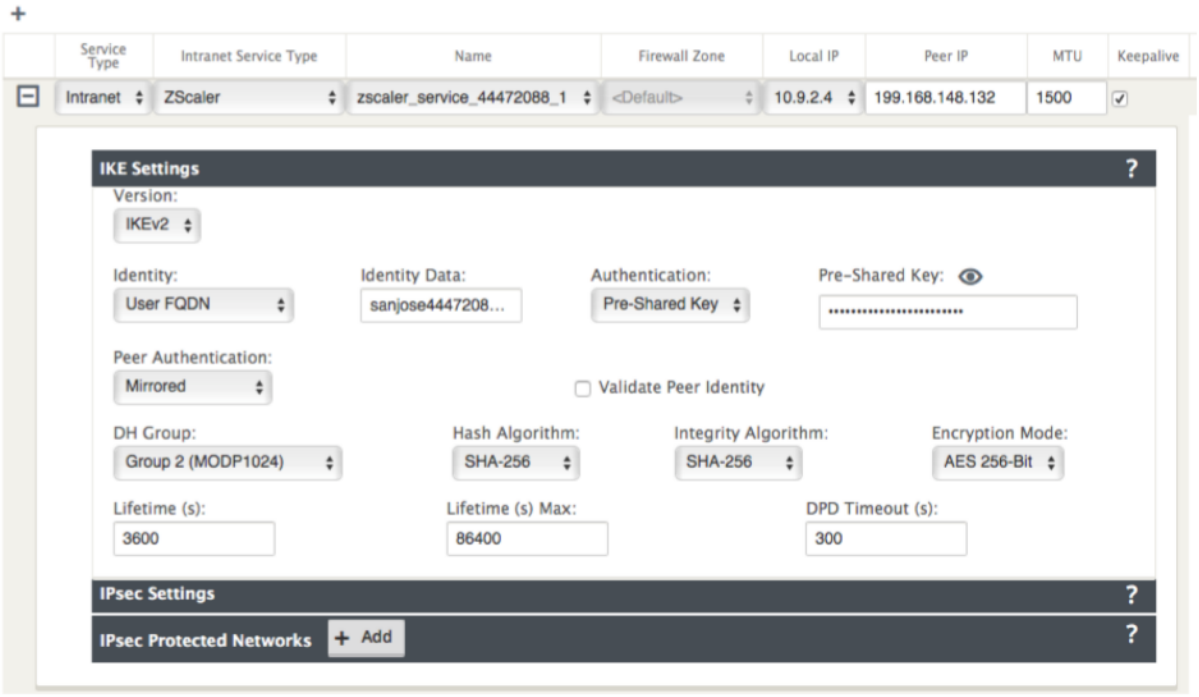
La página Detalles de la GUI de SD-WAN Center proporciona información sobre la configuración del túnel IPSec para los extremos primario y secundario. La IP del mismo par se obtiene de Zscaler. Compruebe la configuración del túnel IPSec en el editor de configuración de GUI del dispositivo SD-WAN.



Configuración IKE

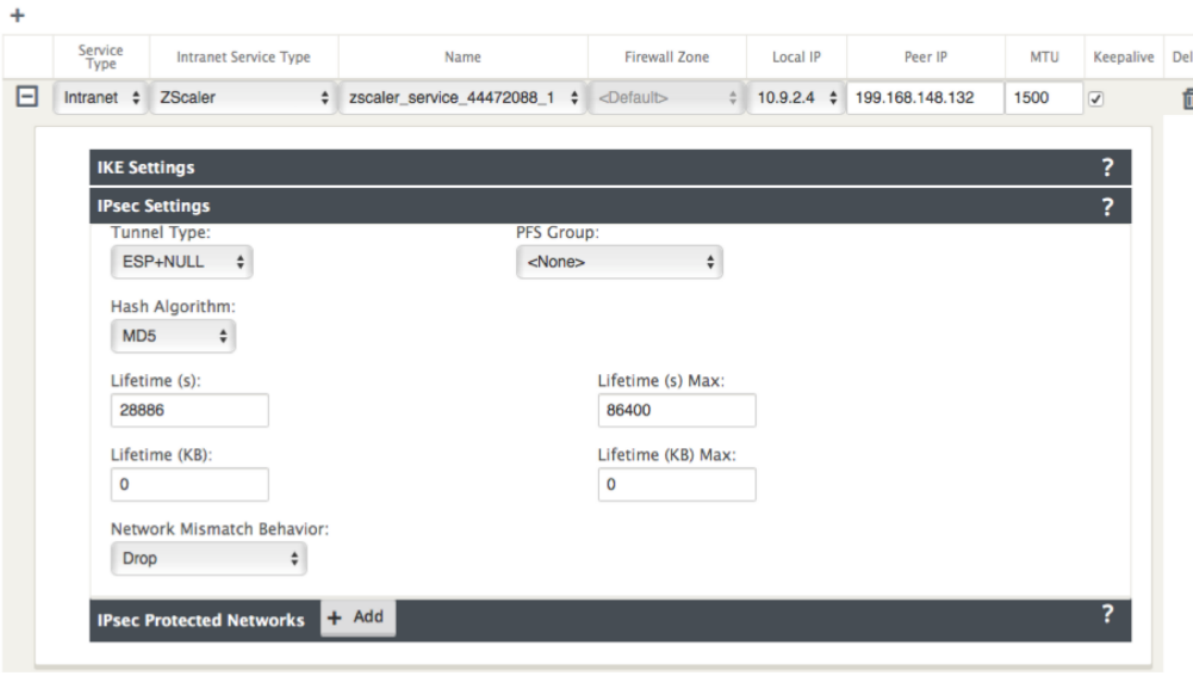
Se eligen las siguientes opciones de IKE/IPsec para la configuración del túnel IPSec en el dispositivo SD-WAN. Para obtener más información acerca de la configuración de túnel IPSec —IKE, consulte; Cómo configurar túneles IPSec entre dispositivos SD-WAN y de terceros tema.

- Versión IKE: IKEv2
- Identidad IKE: FQDN del usuario
- Algoritmo hash: SHA-256
- Algoritmo de integridad —SHA-256
- Modo de cifrado: AES 256 Bits
- IPSec —Modo de túnel
- Cifrado IPSec: Null



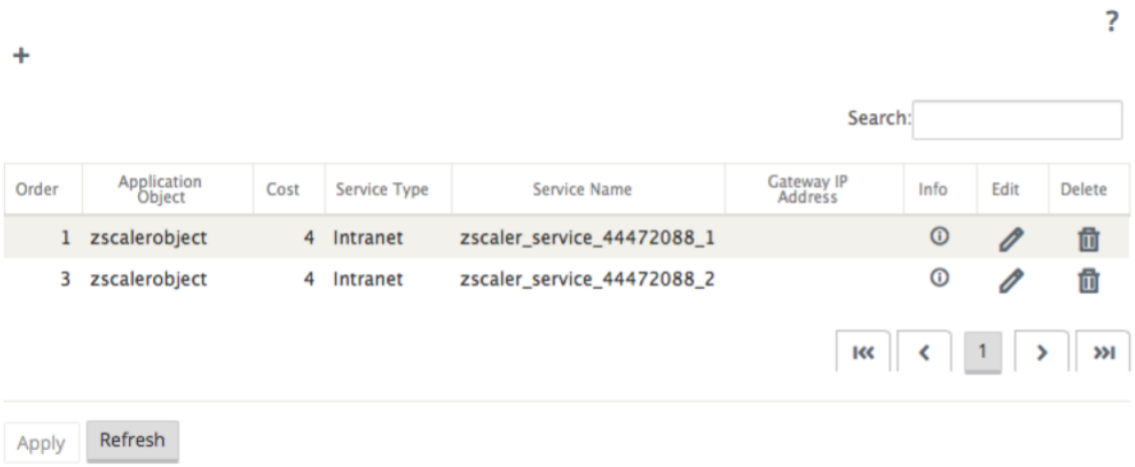
Configuración de IPSec

Para obtener más información acerca de la configuración del túnel IPSec, vea el Cómo configurar túneles IPSec entre dispositivos SD-WAN y de terceros tema.



Objetos de aplicación

Asegúrese de que los objetos de aplicación estén configurados. Para obtener más información acerca de la configuración de rutas de aplicación, consulte Clasificación de aplicaciones el tema.



> **Nota**
>
> La configuración del túnel GRE no se admite como parte del flujo de trabajo automatizado. Sin embargo, la configuración manual todavía está permitida. Para obtener más información, consulte Integración de Zscaler mediante túneles GRE y túneles IPSec.

Supervisión

April 13, 2021

Citrix SD-WAN Center Dashboard le permite ver las estadísticas y gráficos de la red SD-WAN en un único panel. Para obtener más información, consulte Panel de mandos.

También puede ver los Eventos y los Informes de la red SD-WAN en Citrix SD-WAN Center.

Seguimiento de artículos relacionados:

Paquetes diagnóstico

Notificaciones de eventos

Archivos de registros

Volcados de memoria

Intervalo de sondeo

Estadísticas

Información del sistema

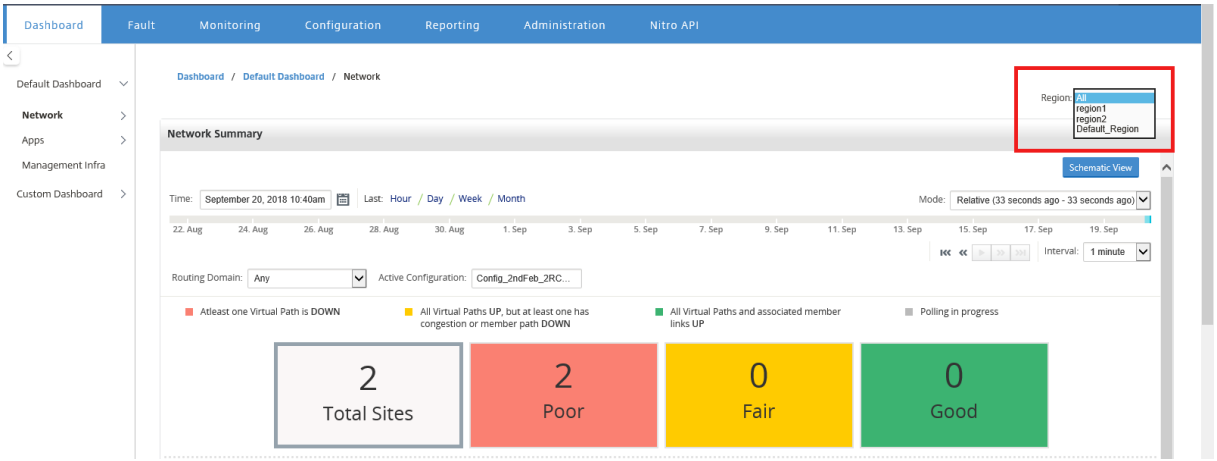
Panel de mandos

February 16, 2022

Citrix SD-WAN Center Dashboard muestra un subconjunto de las estadísticas comunes de un vistazo. Para una implementación de una sola región, las estadísticas se obtienen del MCN detectado en Citrix SD-WAN Center. Para una implementación de varias regiones, las estadísticas se obtienen de todos los recopiladores regionales de Citrix SD-WAN Center para el intervalo de tiempo seleccionado. Puede ver las siguientes estadísticas:

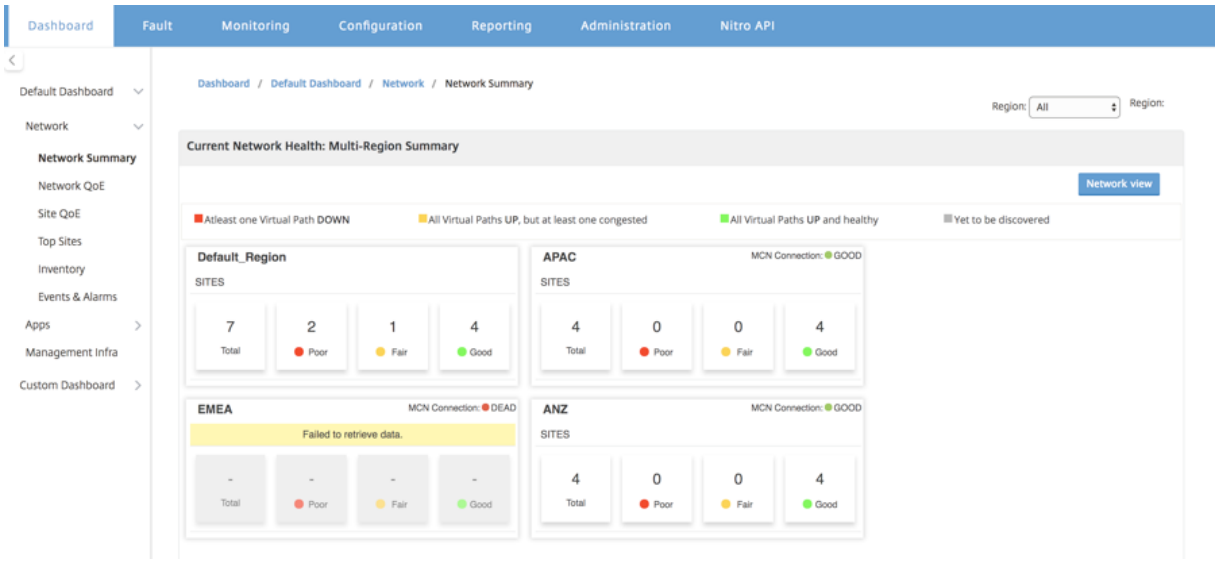
- Resumen de la red
- QoE de red
- Sitios principales
- Inventory
- Eventos y Alarmas
- Principales aplicaciones
- HDX QoE
- Infraestructura de gestión

Para una implementación de una sola región, las estadísticas de región predeterminadas se muestran en el tablero de mandos. Para una implementación de varias regiones, puede elegir ver el panel de varias regiones o el panel regional. Para ver el panel de control de varias regiones, en el menú **Región** seleccione **Todo**. Sin embargo, no puede ver el panel de resumen de varias regiones cuando se configuran más de 300 sitios.



Puede ver el estado de conexión de MCN en cada icono de región. El estado de conexión de MCN es el estado de la ruta virtual entre un RCN y el MCN.

> **Nota**
>
> Para una implementación de varias regiones, las estadísticas de región predeterminadas incluyen estadísticas de todos los sitios administrados por el MCN. También podría incluir estadísticas de RCN ya que los RCNs tienen rutas virtuales al MCN.
>
> El menú desplegable **Región** no está disponible en Citrix SD-WAN Center Collectors.



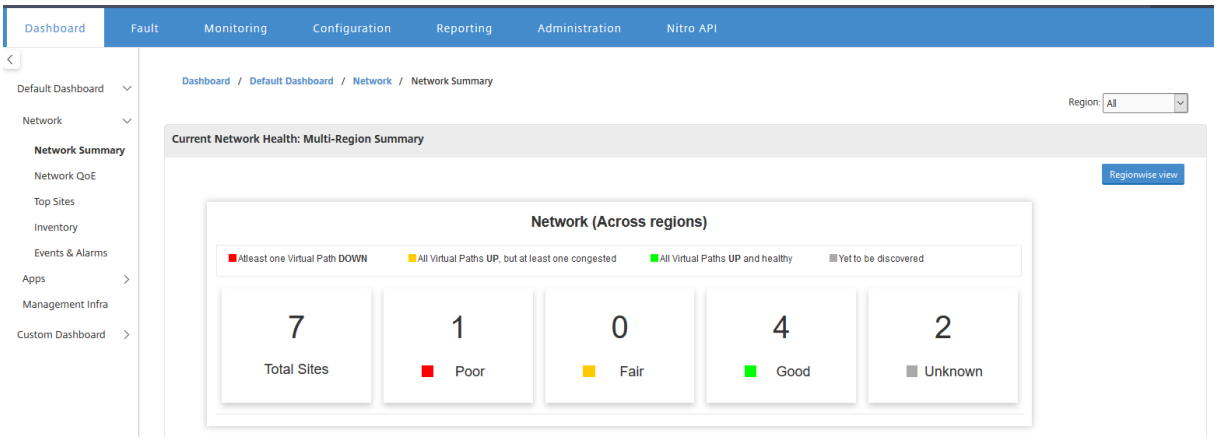
Citrix SD-WAN Center Dashboard se actualiza en función del intervalo de sondeo configurado. El intervalo de sondeo predeterminado es de cinco minutos. Para obtener más información, consulte Intervalo de sondeo.

Resumen de la red

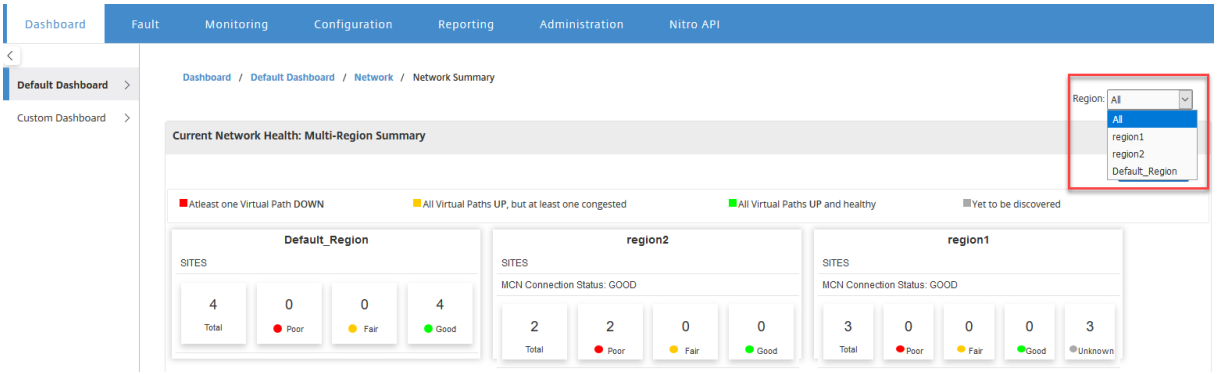
Para una implementación de varias regiones, el widget **Resumen de red** proporciona una visión general del estado de la red en todas las regiones. Se muestra una tarjeta de región para cada región de la red con la siguiente información:

- El número total de sitios en la región.
- El número de sitios en el estado Pobre. Un sitio se encuentra en el estado Poor cuando al menos una ruta virtual está INACTIVA.
- El número de sitios en el estado Fair. Un sitio está en estado Justo cuando todas las rutas virtuales del sitio están ACTIVAS, pero al menos una ruta tiene un problema de congestión o una ruta de miembro está INACTIVA.
- El número de sitios en el buen estado. Un sitio está en el estado Bueno cuando todas las rutas virtuales y las rutas de miembro asociadas están UP.
- El número de sitios en el estado Desconocido. Un sitio se encuentra en el estado Desconocido cuando la encuesta está en curso.

Para ver el resumen de red de varias regiones, vaya a **Panel** > **Panel predeterminado** > **Red** > **Resumen de red** y, en el menú desplegable **Región**, seleccione **Todo**.



De forma predeterminada, la pantalla aparece en **la vista Red**. Puede ver el estado actual de la red del resumen de la red multiregión haciendo clic en la **vista de región**. También puede ver el estado de conexión de MCN en cada icono de región.



Haga clic en una tarjeta de región para profundizar en el panel regional.

Para una región individual, el widget **Resumen de red** proporciona una visión general del estado de la red de la región seleccionada.

Para ver el resumen de red regional, vaya a **Panel** > **Panel predeterminado** > **Red** > **Resumen de red** y, en el menú desplegable **Región**, seleccione **una región**.

Puede ver el resumen de la red regional en la vista de teselas o en la vista esquemática.

Puede utilizar el control de línea temporal para ver el resumen del estado de la red para un período seleccionado. También puede reproducir o pausar el estado de la red a lo largo de un intervalo de tiempo.

El modo ayuda a ver el tiempo como un concepto relativo o absoluto.

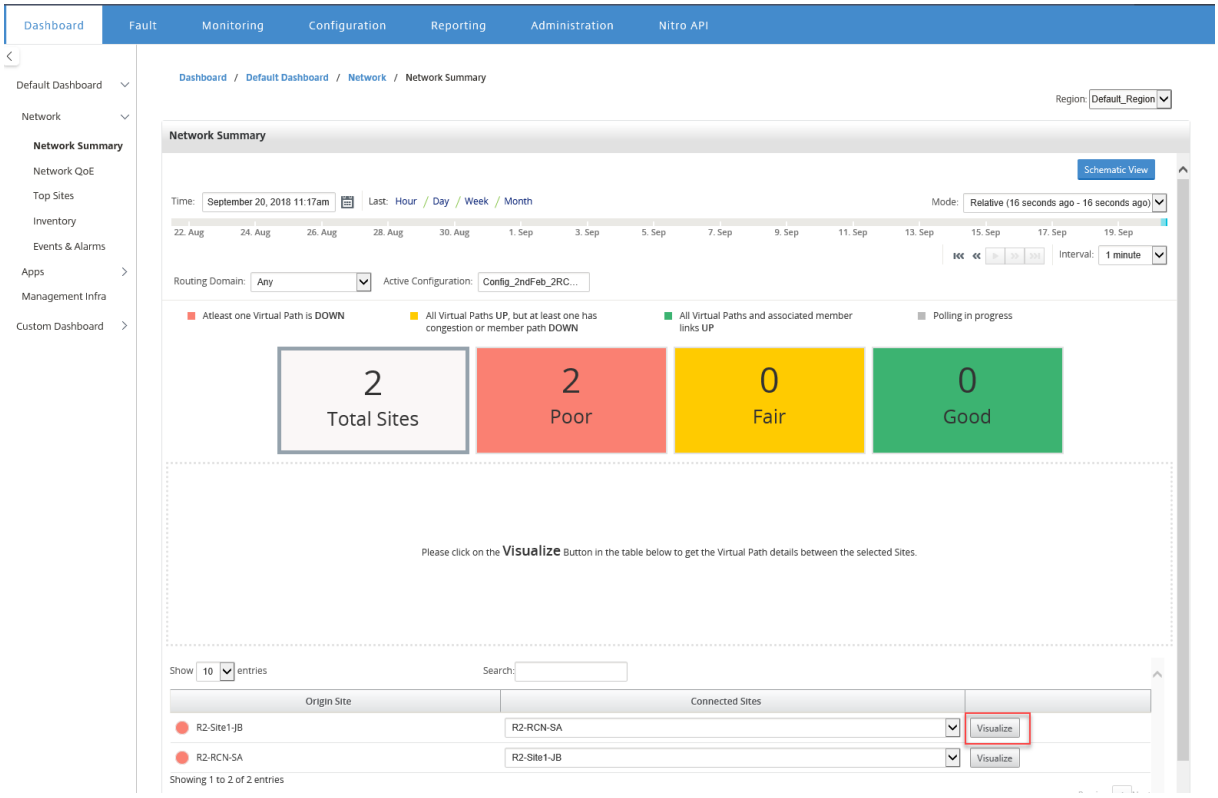
Para obtener más información sobre la línea temporal y el modo, consulte Controles de la línea temporal.

Vista de teselas

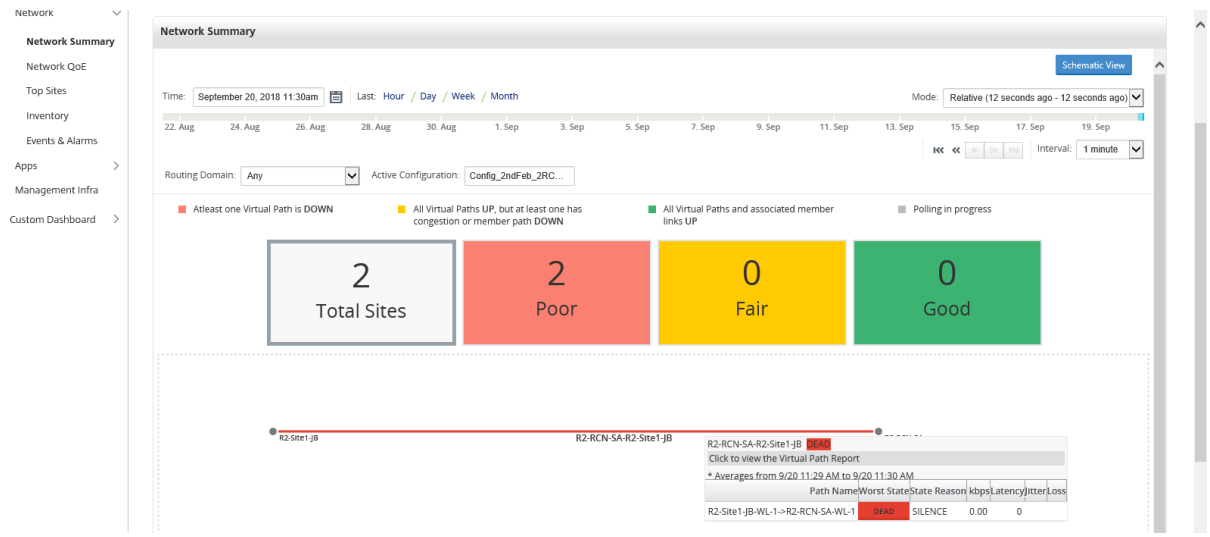
La vista de mosaico proporciona la siguiente información:

- El número total de sitios en la región.
- El número de sitios en el estado Pobre. Un sitio se encuentra en el estado Poor cuando al menos una ruta virtual está INACTIVA.
- El número de sitios en el estado Fair. Un sitio está en estado Justo cuando todas las rutas virtuales del sitio están ACTIVAS, pero al menos una ruta tiene un problema de congestión o una ruta de miembro está INACTIVA.
- El número de sitios en el buen estado. Un sitio está en el estado Bueno cuando todas las rutas virtuales y las rutas de miembro asociadas están UP.
- El número de sitios en el estado Desconocido. Un sitio se encuentra en el estado Desconocido cuando la encuesta está en curso.

Para ver una representación gráfica de un trazado entre dos sitios, seleccione la ruta y haga clic en **Visualizar**.



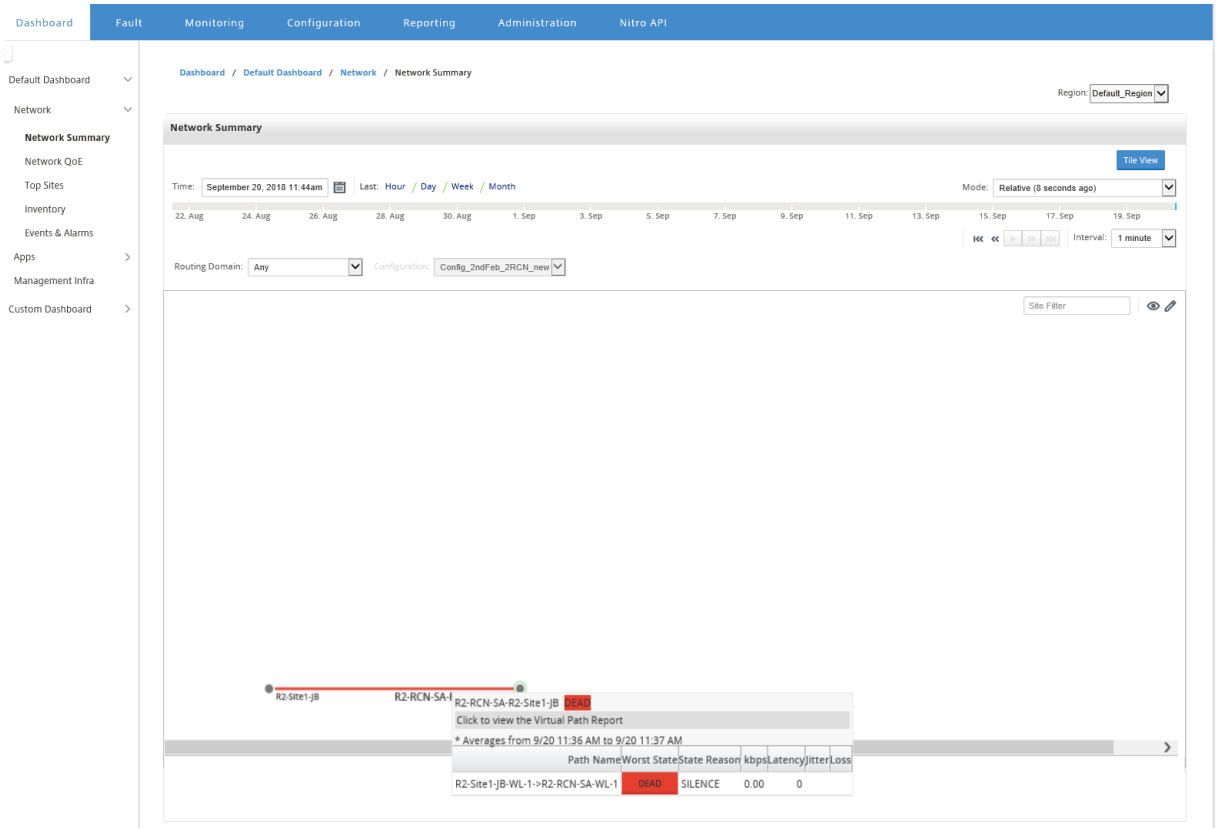
Pase el cursor del ratón sobre los sitios o la ruta para ver más detalles. Haga clic en los sitios para ver y seleccionar las opciones de informe.



Vista Esquema

La vista esquemática proporciona una vista gráfica de la red SD-WAN. La información mostrada en esta sección se actualiza en función del dominio de configuración y enrutamiento seleccionado. Para ver aquí un mapa de red, debe importar la configuración de red y los mapas de red desde el nodo controlador maestro (MCN). Para obtener más información, consulte Importar configuración de MCN.

Pase el cursor del ratón sobre los sitios o la ruta para ver más detalles. Haga clic en los sitios para ver las opciones del informe.

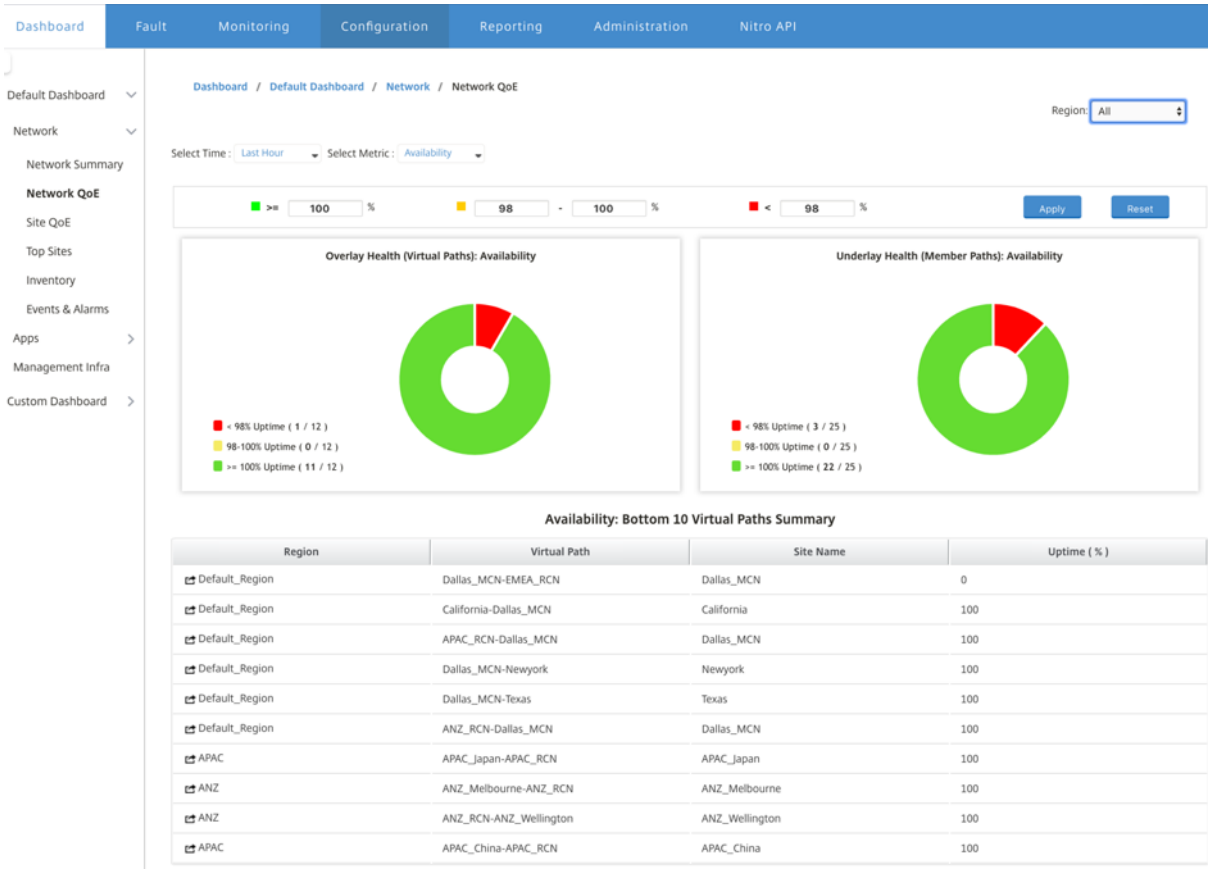


QoE de red

El widget **QoE de red** proporciona una representación gráfica de los parámetros de disponibilidad, pérdida, latencia y fluctuación de una ruta virtual. Proporciona las estadísticas para la ruta virtual de superposición y las rutas de miembro del calco subyacente.

Para una implementación de varias regiones, puede ver una lista de las 10 rutas virtuales inferiores en función de la métrica seleccionada. Los datos de ruta virtual se recopilan de todos los recopiladores regionales para el intervalo de tiempo seleccionado. Puede ver los detalles de ancho de banda, fluctuación, pérdida y congestión de las rutas virtuales que más necesitan su atención.

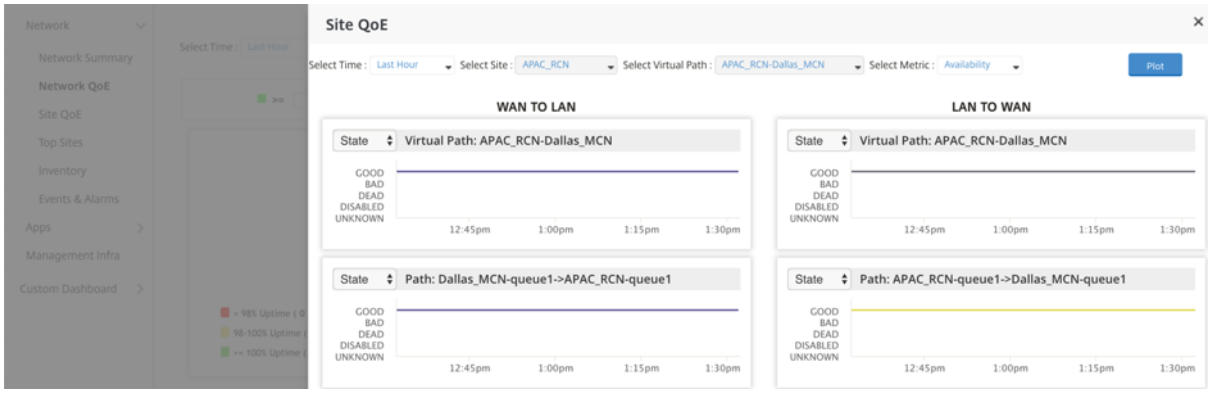
Para ver el estado de la ruta virtual de varias regiones, vaya a **Panel** > **Panel predeterminado** > **Red** > **QoE de red** y, en el menú desplegable **Región**, seleccione **Todo.**



Para una región individual, puede ver una lista de las 10 rutas virtuales inferiores en función de la métrica seleccionada. Las estadísticas se recopilan para el intervalo de tiempo seleccionado. Puede ver los detalles de ancho de banda, fluctuación, pérdida y congestión de las rutas virtuales que más necesitan su atención.

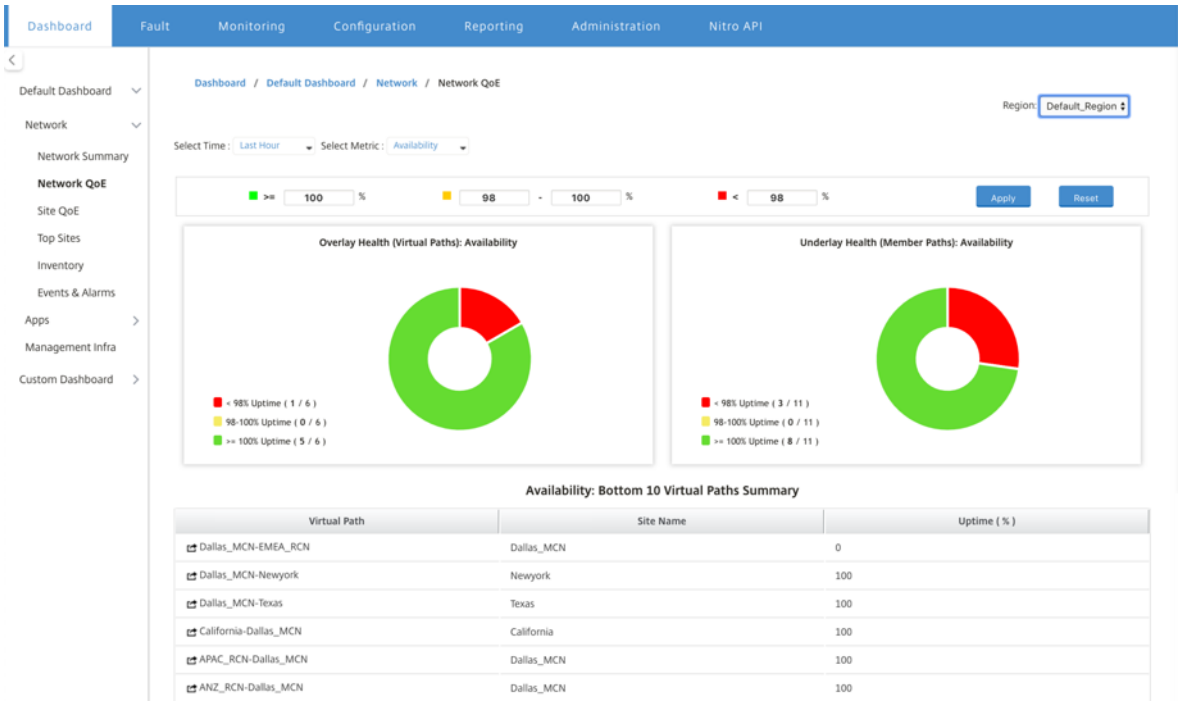
Puede comparar las rutas de superposición y calco subyacente para la métrica seleccionada (disponibilidad, pérdida, fluctuación, latencia) a lo largo del intervalo de tiempo seleccionado. También puede establecer umbrales personalizados para las métricas y guardarlos al hacer clic en **Aplicar**. Haga clic en **Restablecer** para almacenar los umbrales predeterminados.

El usuario también puede profundizar en cualquier ruta virtual de la tabla mediante el botón de **profundización** situado a la izquierda de cada fila. Aparece un **QoE del sitio** con la comparación detallada entre el conducto y sus rutas de miembro subyacentes.



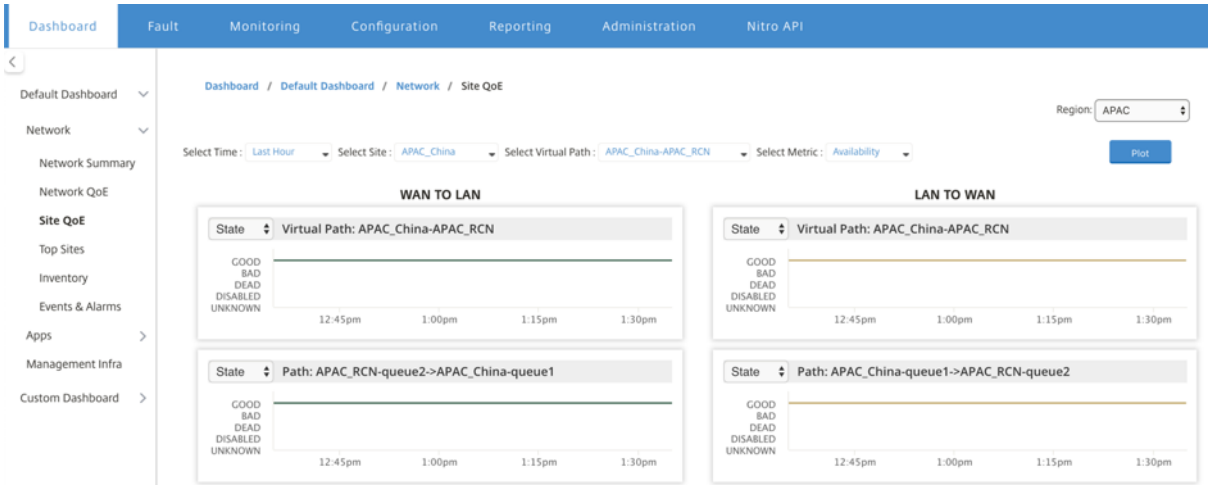
En el control deslizante, el nombre del sitio y la ruta virtual se seleccionan de forma predeterminada en función de la fila en la que haya hecho clic y se inhabilitará. **Sin embargo, el usuario puede seleccionar un intervalo de tiempo y una métrica diferentes y hacer clic en la opción Trazar para trazar los nuevos gráficos.**

Para ver las estadísticas de mantenimiento de rutas virtuales regionales, vaya a **Panel** > **Panel predeterminado** > **Red** > **QoE de red** y, en el menú desplegable **Región**, seleccione una región.



QoE del sitio

Puede utilizar QoE del sitio como herramienta para comparar la ruta virtual y las rutas de los miembros subyacentes. Debe seleccionar un sitio y cualquier ruta virtual de este sitio y métrica. Haga clic en **Trazar**.

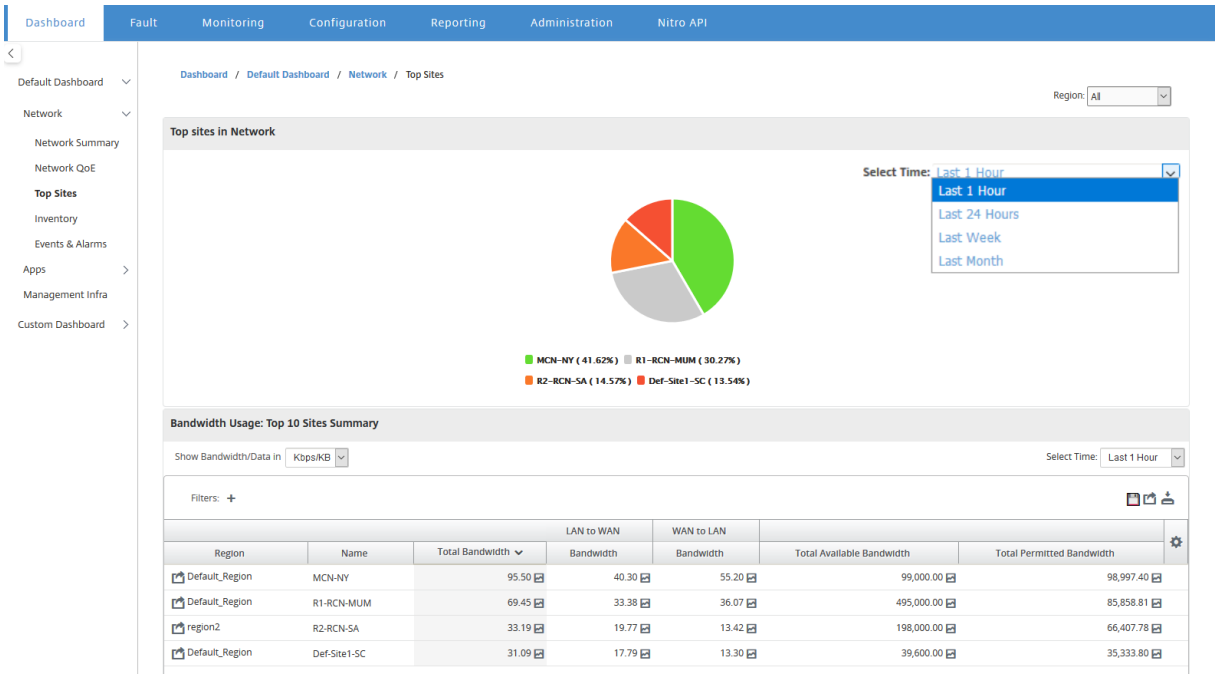


En la primera sección, traza las estadísticas de rutas virtuales en dirección **WAN a LAN** y **LAN a WAN**. Debajo de la sección traza todos los gráficos de rutas de miembro subyacentes. Ambas cosas están presentes tanto a nivel regional como de red.

Sitios principales

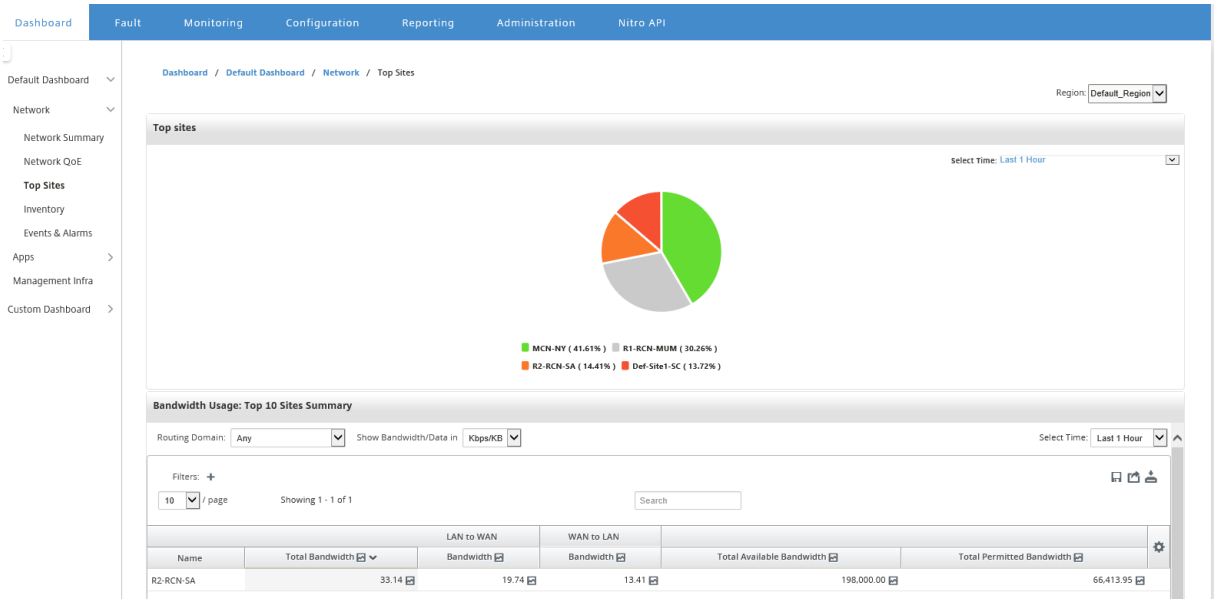
Para una implementación de varias regiones, el widget **Sitios principales** enumera los 10 sitios principales de todas las regiones, que tienen el mayor uso de ancho de banda, en el intervalo de tiempo seleccionado.

Para ver los sitios principales de todas las regiones, vaya a **Panel** > **Panel predeterminado** > **Red** > **Sitios principales** y, en el menú desplegable **Región**, seleccione **Todo.**



Haga clic en un sitio o métrica para ver informes y estadísticas detallados.

Para una región individual, el widget Sitios principales muestra las estadísticas de uso de ancho de banda para todos los sitios de la región. Las estadísticas se recopilan para el intervalo de tiempo seleccionado. Puede filtrar los sitios en función del dominio de enrutamiento.



Inventory

Cada 30 minutos, el administrador de inventario recopila la información de hardware de todos los dispositivos Citrix SD-WAN descubiertos en Citrix SD-WAN Center.

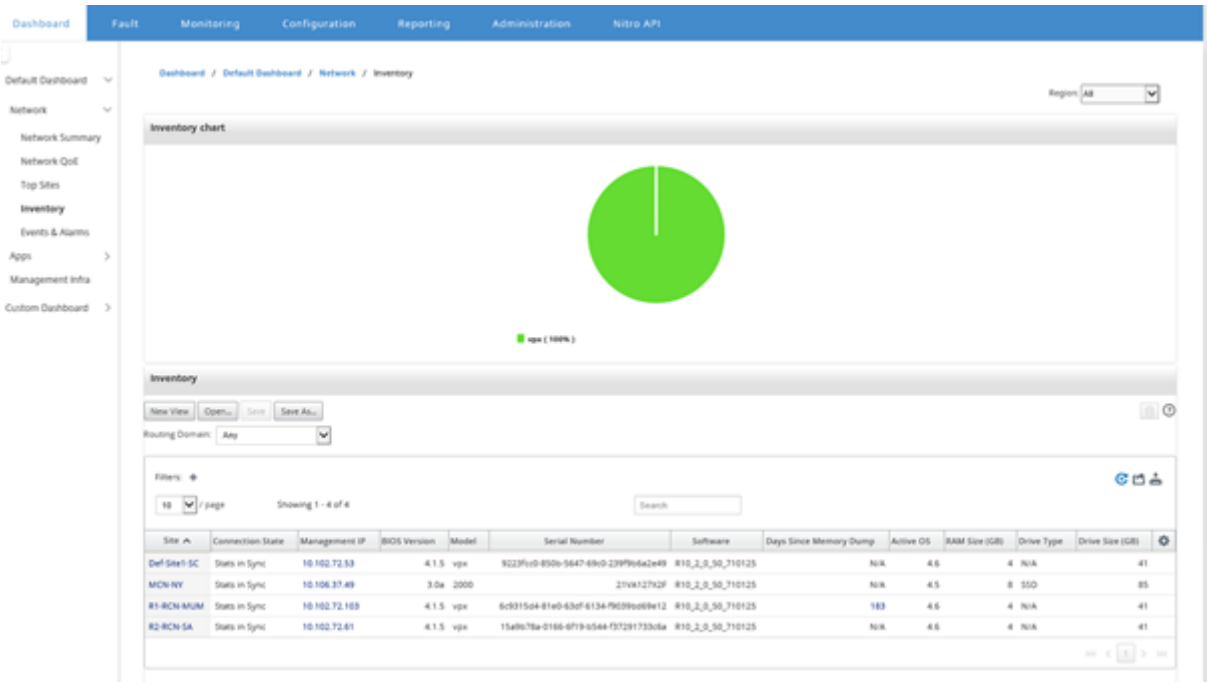
Para ver las estadísticas de inventario de varias regiones, vaya a **Panel > Panel** de **control predeterminado** > **Red** > **Inventario** y, en el menú desplegable **Región**, seleccione.

Para ver las estadísticas de inventario de una región específica, seleccione la **región** en el menú desplegable Región.

Puede ver las siguientes estadísticas de inventario:

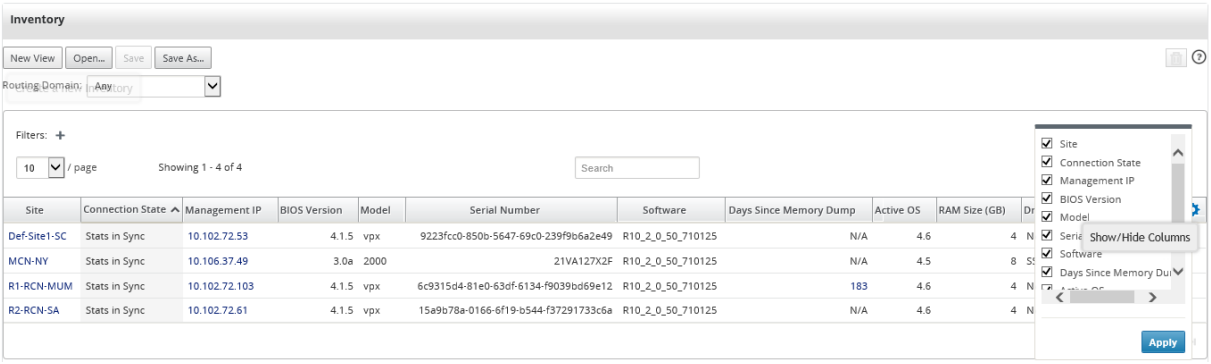
- **Sitio**: Nombre del sitio encontrado en la configuración que se ejecuta en el MCN. Si el dispositivo es un MCN secundario, aparece "(secundario)"junto al nombre. Puede hacer clic en el nombre para acceder a la consola web del dispositivo.
- **Estado de conexión**: estado de conectividad al dispositivo. Aparece un icono rojo cuando no se puede acceder a la conexión o no se autentica.
- **Dirección IP de**administración: dirección IP de administración del dispositivo. Puede hacer clic en la dirección IP para acceder a la consola web del dispositivo.
- **Versión del**BIOS: versión del BIOS del dispositivo.
- **Modelo**: Modelo de hardware del dispositivo.

- **Número de serie**: Número de serie del dispositivo.
- **Software**; número de versión del software SD-WAN.
- **Días desde el volcado de memoria**: tiempo desde el último volcado de memoria de error del sistema. Si el dispositivo volcó su memoria en los últimos cuatro días, aparecerá un icono de error junto a la hora. Si el volcado de memoria se produjo entre 5 y 10 días atrás, aparece un icono de advertencia. N/A aparece si no hay ningún volcado disponible. Al hacer clic en la hora se abre la página de registro de la SD-WAN.
- **Sistema operativo activo**: el sistema operativo que se está ejecutando actualmente en el dispositivo.
- **Tamaño de RAM (GB)**: cantidad de RAM instalada actualmente en el dispositivo en GB.
- **Tipo de unidad**: tipo de unidad de almacenamiento de datos instalada en el dispositivo. El valor puede ser SSD (unidad de estado sólido) o HDD (unidad de disco duro).
- **Tamaño de unidad (GB)**: tamaño de la unidad de almacenamiento de datos instalada actualmente en el dispositivo en GB.



Nota

Puede organizar las columnas de la tabla de estadísticas de inventario mediante la opción **Mostrar/Ocultar columnas**.



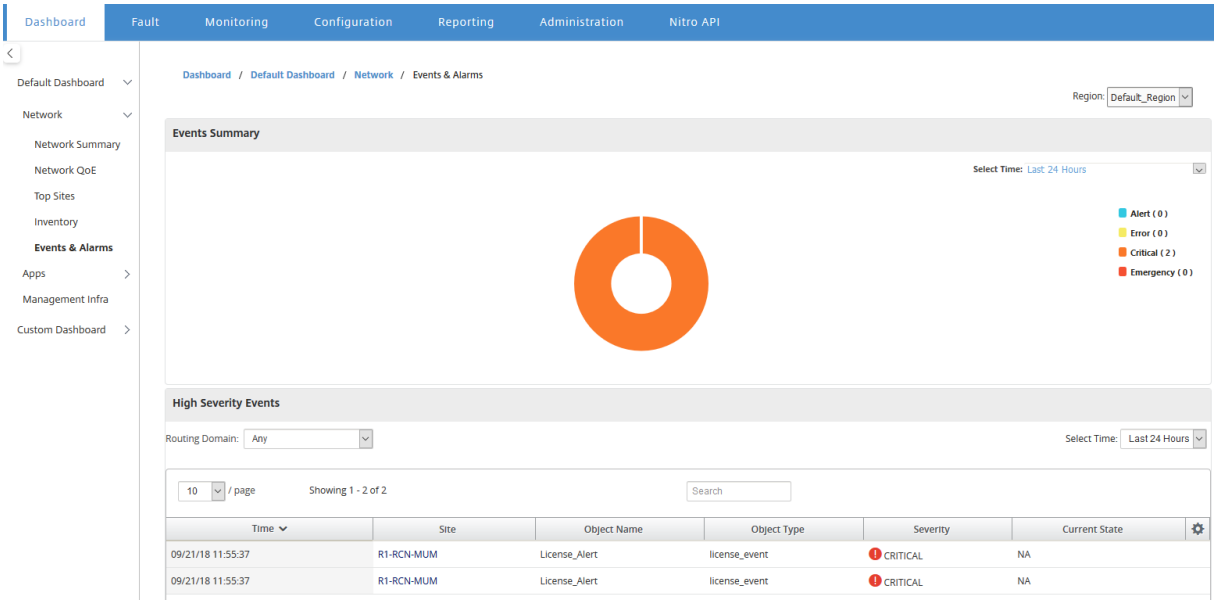
Eventos y alarmas

Para una implementación de varias regiones, puede ver los eventos y las alarmas de todas las regiones de la red. Esta información se recopila para el intervalo de tiempo seleccionado. Para ver los eventos y las estadísticas de varias regiones, vaya a **Panel** > **Panel predeterminado** > **Red** > **Eventos y alarmas** y, en el menú desplegable **Región**, seleccione **Todo**.

También puede ver todos los eventos y alarmas de una región individual. Esta información se recopila para el intervalo de tiempo seleccionado. Para ver los eventos y las estadísticas de alarmas, vaya a **Panel** > **Panel predeterminado** > **Red** > **Eventos y alarmas** y, en el menú desplegable **Región**, seleccione una región.

La sección **Resumen de eventos** proporciona una descripción gráfica del tipo de evento y la cantidad de eventos. Puede hacer clic en el gráfico para ver los eventos en la página **Falla**. La pantalla también describe cuántos eventos hay en cada categoría. Los disparadores de alarma se pueden configurar en los dispositivos SD-WAN individuales. Para obtener más información, consulte Notificaciones de eventos.

La sección **Eventos de alta gravedad** muestra una lista de los eventos graves. Puede filtrar los eventos en función del dominio de enrutamiento. La información que se muestra en esta sección se recopila en la ficha **Falla**. Para obtener más información, consulte Eventos.

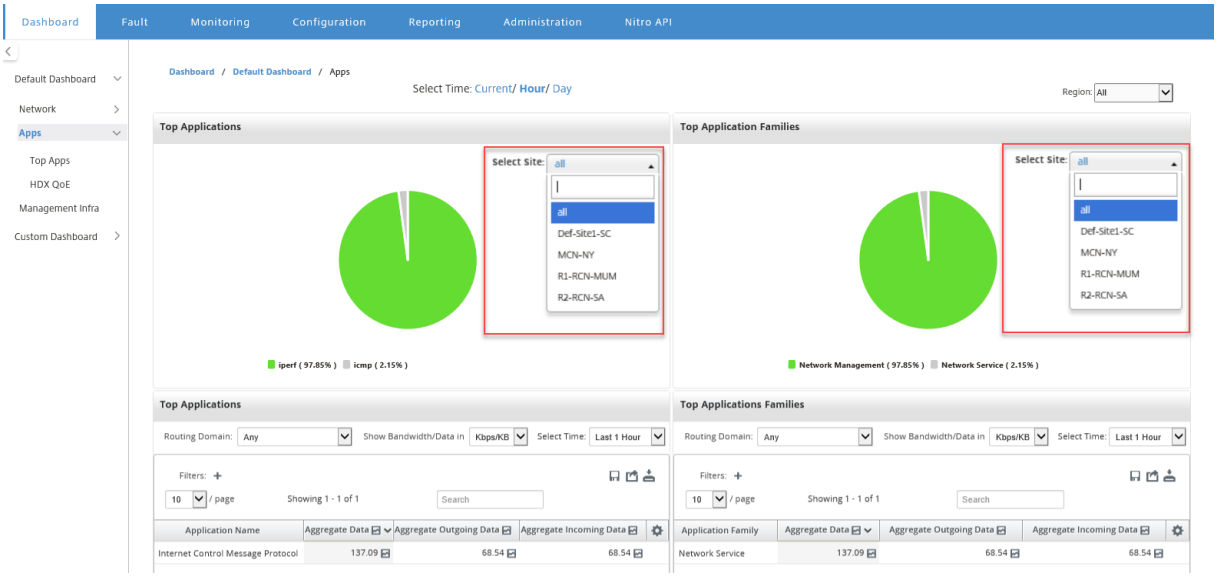


Aplicaciones

Aplicaciones principales

La inspección profunda de paquetes (DPI) permite al dispositivo SD-WAN analizar el tráfico que pasa a través de él e identificar los tipos de aplicación y familia de aplicaciones. Para una implementación de varias regiones, puede ver las aplicaciones principales y las familias de aplicaciones principales de todas las regiones de la red. Esta información se recopila para el intervalo de tiempo seleccionado.

Para ver las estadísticas de aplicaciones principales en todas las regiones de la red, vaya a **Panel** > **Panel predeterminado** > **Aplicaciones > Aplicaciones principales y,** en el menú desplegable **Región**, seleccione **Todo.**

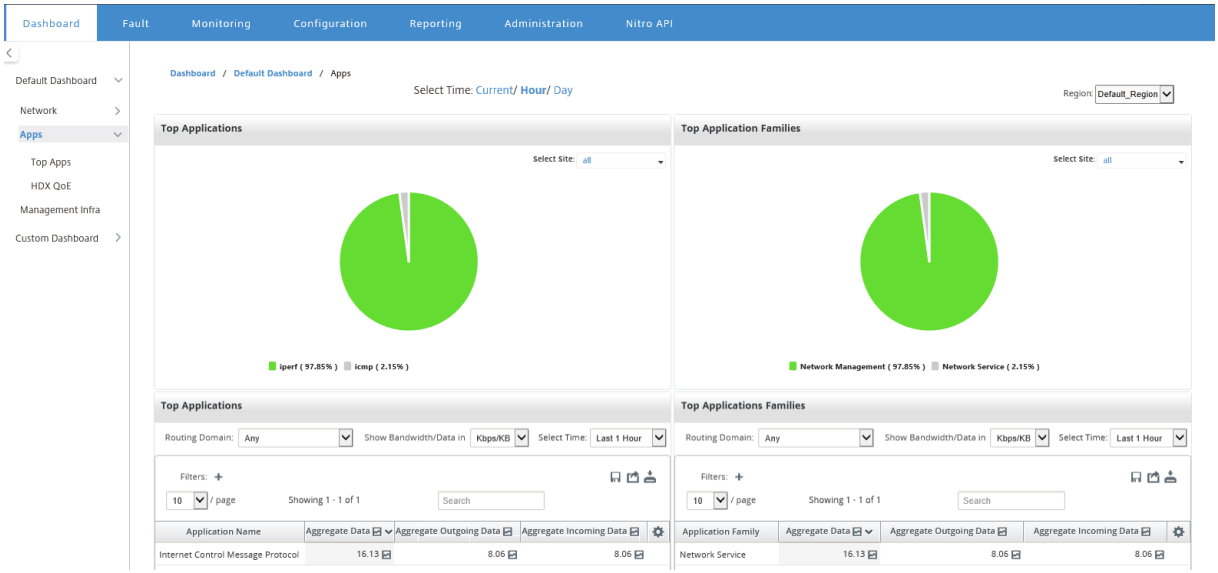


Puede ver la lista desplegable en la que se puede buscar la selección de emplazamiento para la **aplicación principal** y las **familias de aplicaciones principales**.

También puede ver las aplicaciones principales y las familias de aplicaciones superiores de una región determinada.

Para ver las estadísticas de la aplicación de una región, vaya a **Panel** > **Panel predeterminado** > **Aplicaciones > Aplicaciones principales** y, en el menú desplegable **Región**, seleccione una región**.**

Puede seleccionar el sitio y el intervalo de tiempo como las últimas 24 horas, última hora o actual.

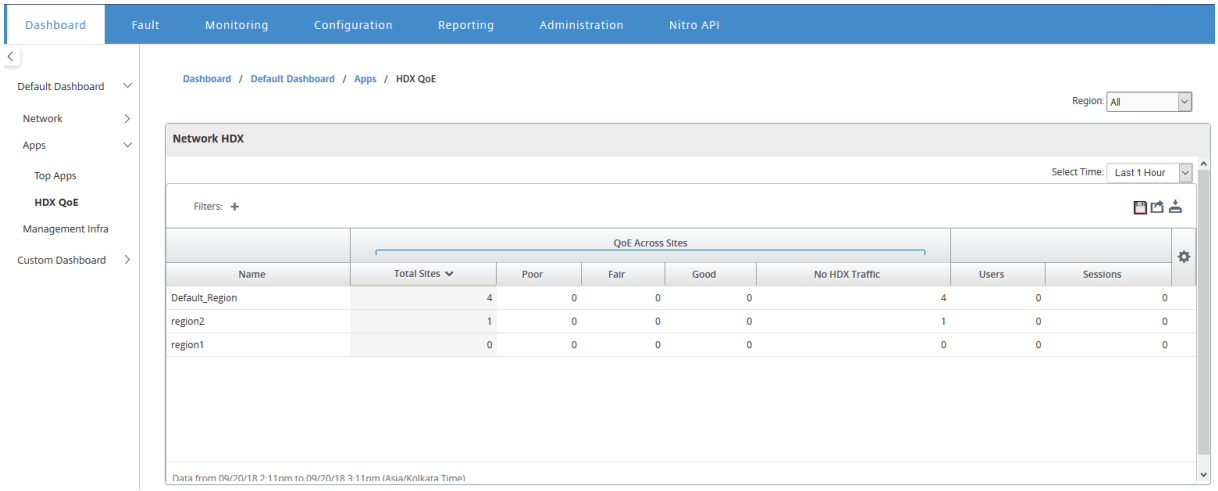


HDX QoE

Quality of Experience (QoE) es un índice calculado que le ayuda a comprender la calidad de su experiencia ICA. Este índice se calcula para todo el tráfico de aplicaciones ICA atravesado desde la WAN hasta el sitio. Las estadísticas de caída de paquetes, fluctuaciones y latencia se utilizan en el cálculo de QoE. El QoE es un número entero entre [0, 100], cuanto mayor sea el número, mejor será la experiencia del usuario.Las estadísticas de fluctuación, latencia y caída de paquetes se realizan un seguimiento en las rutas de datos durante el procesamiento de paquetes.

Los sitios de toda la red se clasifican como buenos, justos, deficientes o sin tráfico HDX en función de la QoE del tráfico HDX. Para obtener más información, consulte HDX QoE.

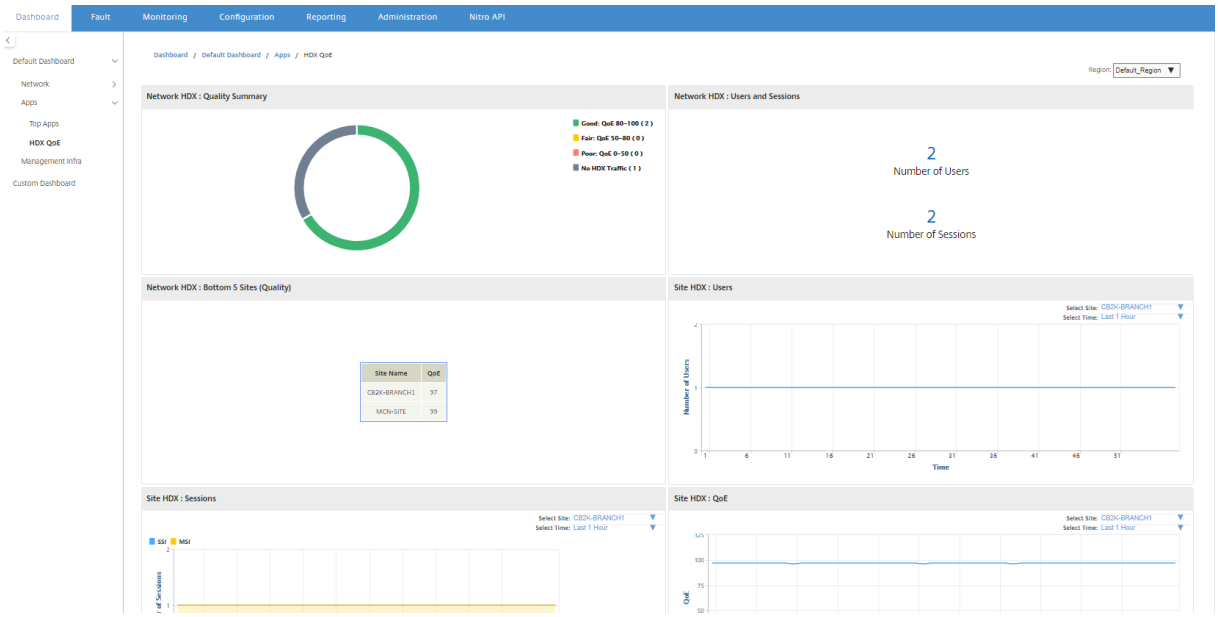
Para ver HDX QoE, de sitios, en todas las regiones de la red, vaya a **Panel** > **Panel predeterminado** > **Aplicaciones > HDX QoE** y, en el menú desplegable **Región**, seleccione **Todo**.



Puede ver las siguientes métricas HDX QoE para las regiones individuales.

- HDX de red: Resumen de calidad
- HDX de red: Usuarios y Sesiones
- HDX de red: Los cinco sitios inferiores (calidad)
- Sitio HDX: Usuarios
- Site HDX: Sesiones
- Sitio HDX: Calidad de Experiencia

Para ver las estadísticas de HDX QoE, vaya a **Panel** > **Panel predeterminado** > **Aplicaciones > HDX QoE** y, en el menú desplegable **Región**, seleccione una región.



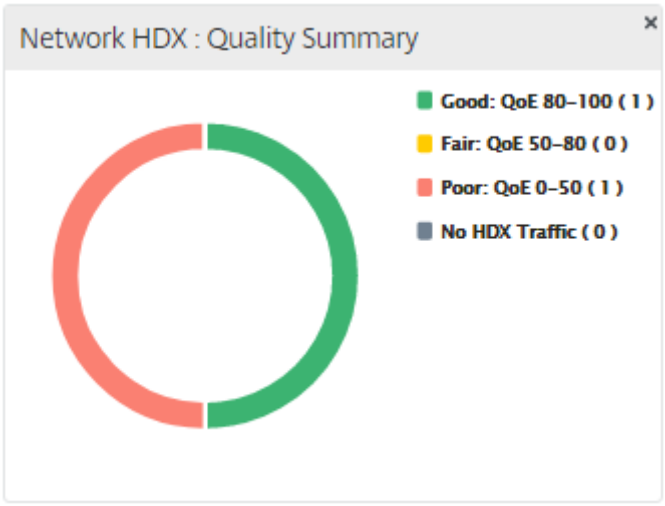
> **Nota**
>
> A veces, es posible que los datos del panel HDX y los informes HDX de diferentes sitios no parez-

> can estar sincronizados porque cada estadística de sitio se sondea de forma independiente.
>
> En los widgets de panel de HDX, es posible que vea un sitio sin tráfico HDX, pero puede haber un número distinto de cero de sesiones y usuarios HDX. Sucede cuando las sesiones HDX permanecen inactivas durante ese período de sondeo y aún permanecen en estado abierto.

HDX de red: Resumen de calidad

El tráfico HDX se clasifica en las siguientes categorías de calidad:

Calidad	Rango QoE
Bueno	80–100
Normal	50–80
Mala	0–50
Sin tráfico HDX	N/D

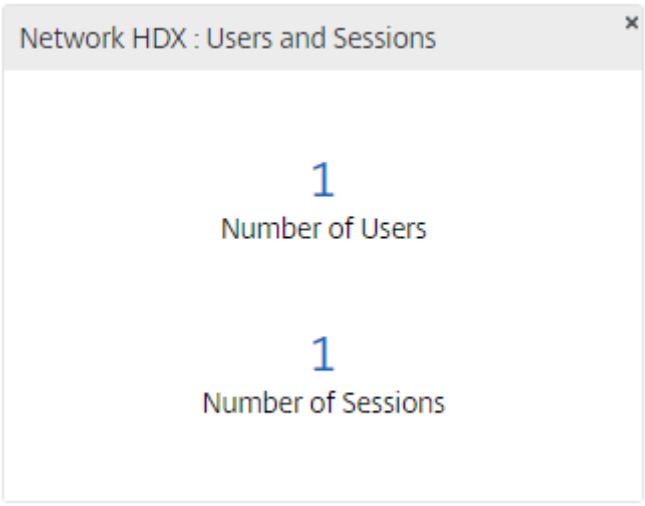


Puede hacer clic en el gráfico para ver los informes HDX por sitio. Para obtener más información, consulte How to View HDX Reports.

HDX de red: Usuarios y Sesiones

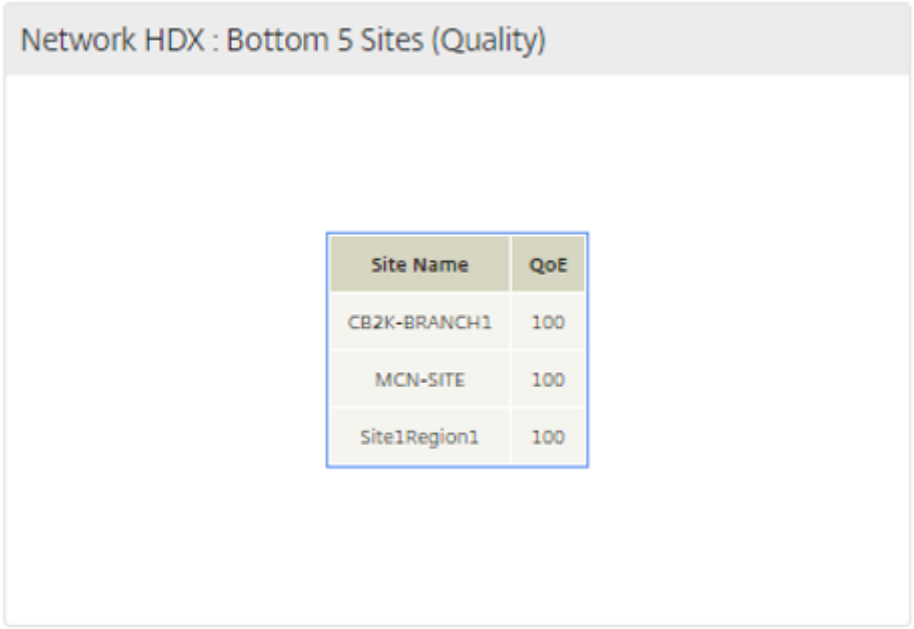
Este widget proporciona información sobre el número de usuarios y sesiones HDX activos. El número de sesiones es el número total de sesiones ICA (SSI) y ICA de varias sesiones activas de sesión única (MSI).

> **Nota**
>
> En la versión actual, el número de usuarios no se basa en nombres de usuario distintos. Es decir, dos sesiones iniciadas por un solo usuario en dos máquinas diferentes se cuentan como dos usuarios.



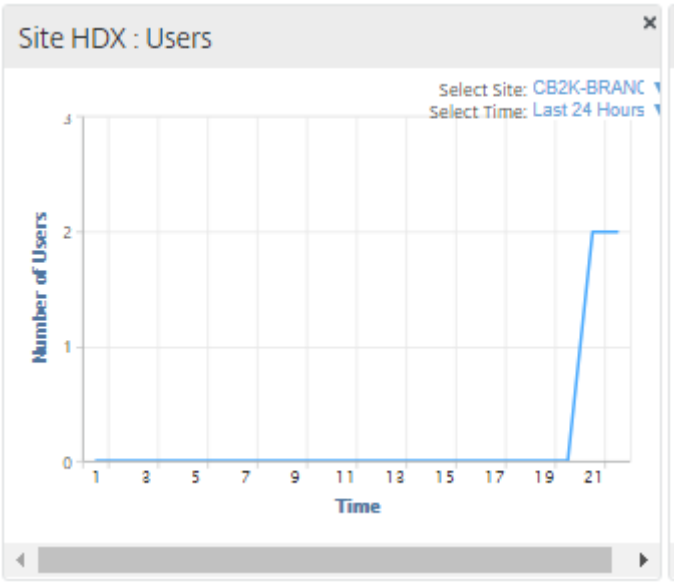
Red HDX: 5 sitios inferiores (calidad)

Este widget proporciona una lista de los 5 sitios inferiores que tienen la menor puntuación QoE. Ayuda a impulsar mejores iniciativas de experiencia de usuario final.



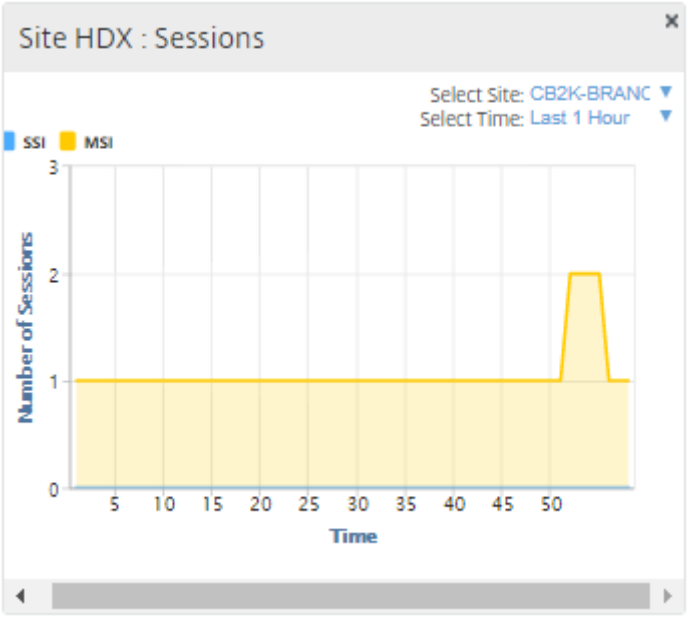
Sitio HDX: Usuarios

Este widget proporciona una representación gráfica del número de usuarios que estuvieron activos en un sitio determinado durante el intervalo de tiempo seleccionado.Puede seleccionar el sitio y el intervalo de tiempo como las últimas 24 horas, la última 1 hora o los últimos 5 minutos.



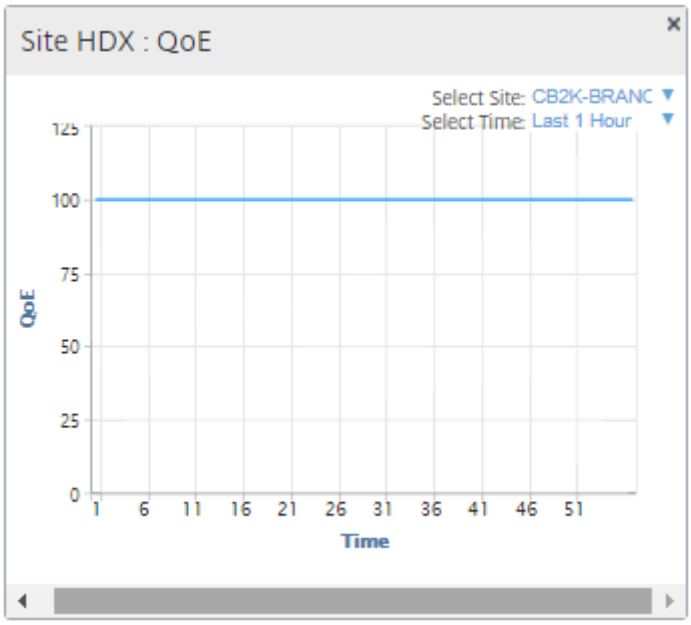
Site HDX: Sesiones

Este widget proporciona una representación gráfica del número de sesiones MSI y SSI activas en un sitio determinado durante el intervalo de tiempo seleccionado.Puede seleccionar el sitio y el intervalo de tiempo como las últimas 24 horas, la última 1 hora o los últimos 5 minutos.



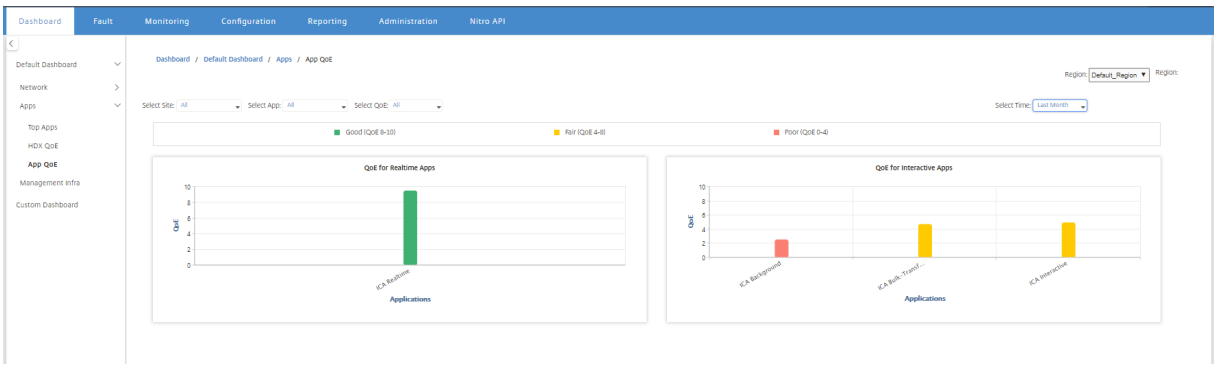
Sitio HDX: Calidad de la experiencia

Este widget proporciona una representación gráfica de la QoE general en un sitio determinado durante el intervalo de tiempo seleccionado.Puede seleccionar el sitio y el intervalo de tiempo como las últimas 24 horas, la última 1 hora o los últimos 5 minutos.



QoE de aplicaciones

La QoE de la aplicación es una medida de calidad de experiencia para una aplicación. El rango de puntuación QoE de la aplicación es 0-10, donde 10 representa una calidad excelente y 0 representa mala calidad. Para obtener más información, consulte QoE de aplicaciones. Puede ver la puntuación QoE de la aplicación para el tráfico interactivo y en tiempo real.

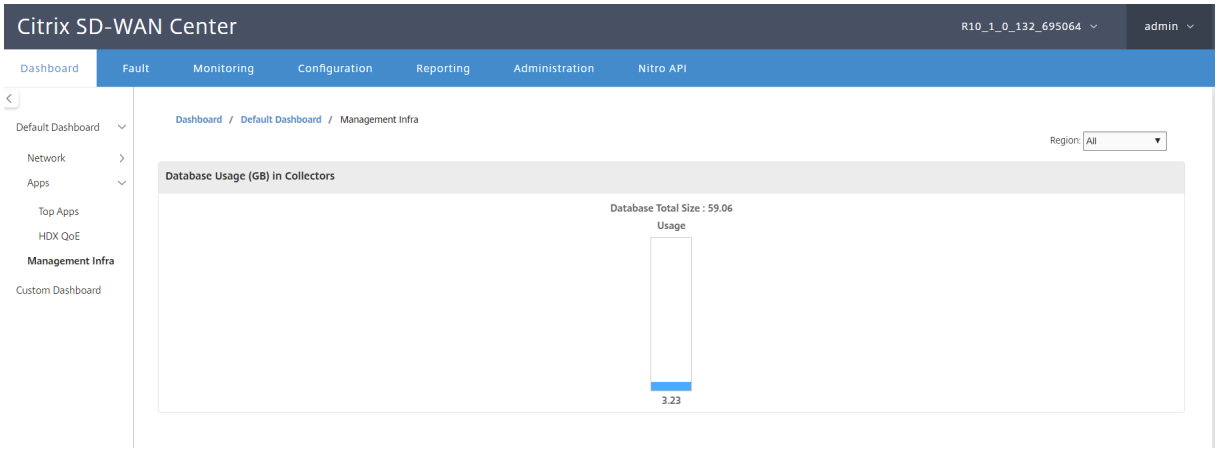


Puede filtrar las estadísticas de QoE de la aplicación por sitio, aplicación o tipo de QoE.

Infraestructura de gestión

La página Gestión de Infraestructura permite ver las estadísticas de almacenamiento y uso de la base de datos de Citrix SD-WAN Center.

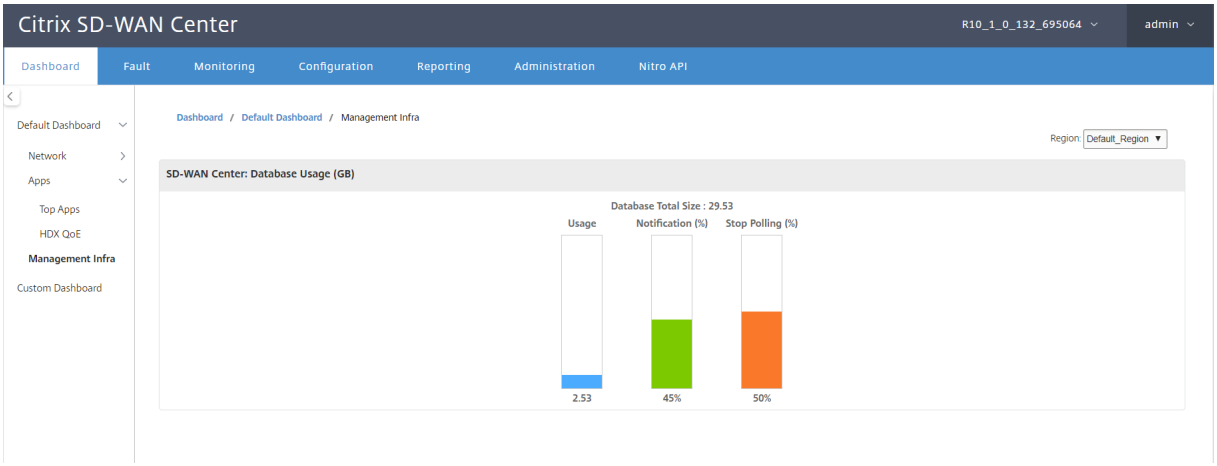
Para una implementación de varias regiones, puede ver el uso de la base de datos de todos los recopiladores de la red. Para ver las estadísticas de la base de datos de varias regiones, vaya a **Panel** > **Panel predeterminado** > **Infraestructura de administración** y, en el menú desplegable **Región**, seleccione **Todo**.



Para ver las estadísticas de la base de datos de Citrix SD-WAN Center para una región determinada, vaya a **Panel** > **Panel predeterminado** > **Administración Infra** y, en el menú desplegable **Región**, seleccione una región.

La sección **Uso de Base** de Datos muestra una visión general gráfica del uso de recursos de base de datos y los umbrales para enviar notificaciones o detener la recopilación de datos. Puede hacer clic en el gráfico para ver los detalles en la página Mantenimiento de la Base de Datos.

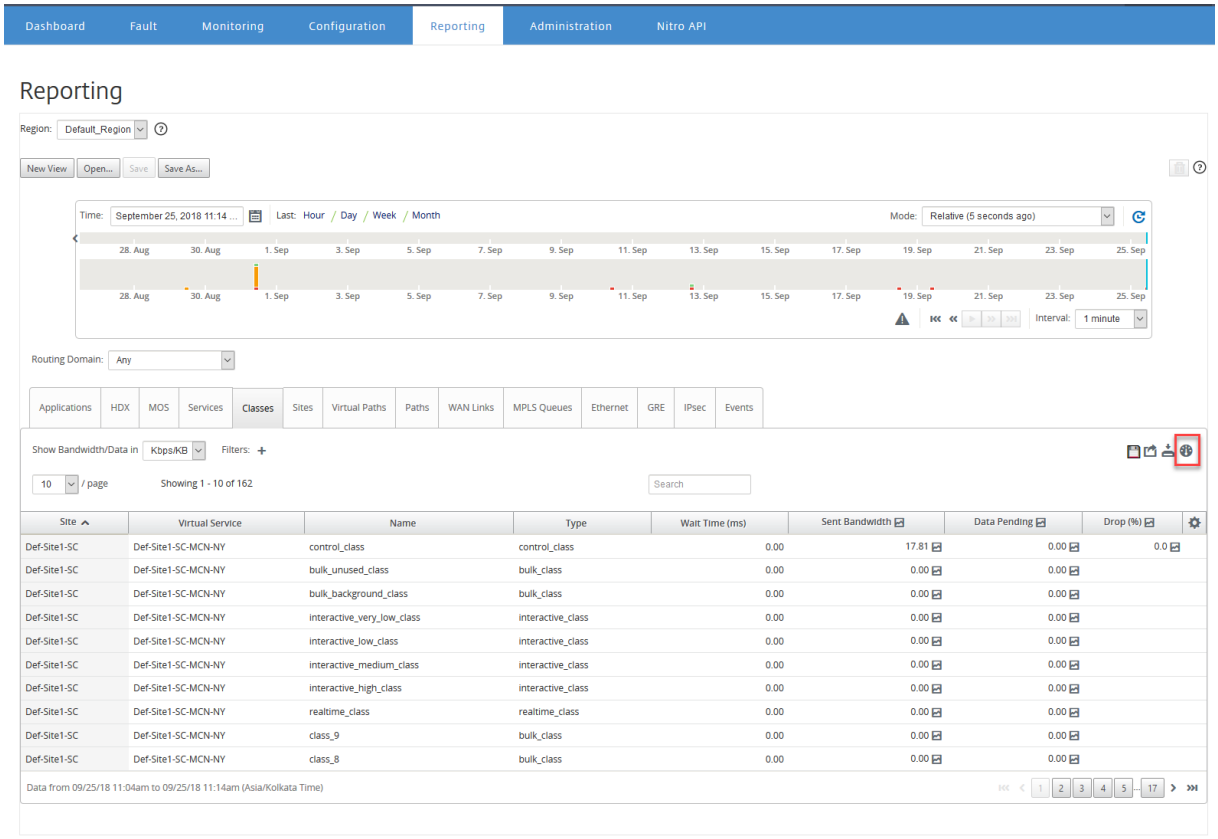
- **Uso**: Capacidad de base de datos que se está utilizando actualmente, en GB.
- **Notificación**: Umbral para generar una notificación de uso de base de datos. El umbral es un porcentaje del tamaño máximo de la base de datos. Si se configura una alerta de correo electrónico, se envía una notificación por correo electrónico cuando el tamaño de la base de datos supera este umbral. Para obtener más información, consulte Notificaciones de eventos.
- **Detener sondeo**: Umbral para detener el sondeo de estadísticas. El umbral es un porcentaje del tamaño máximo de la base de datos. El sondeo se detiene cuando el tamaño de la base de datos supera este umbral. Para obtener más información, consulte Administrar base de datos.



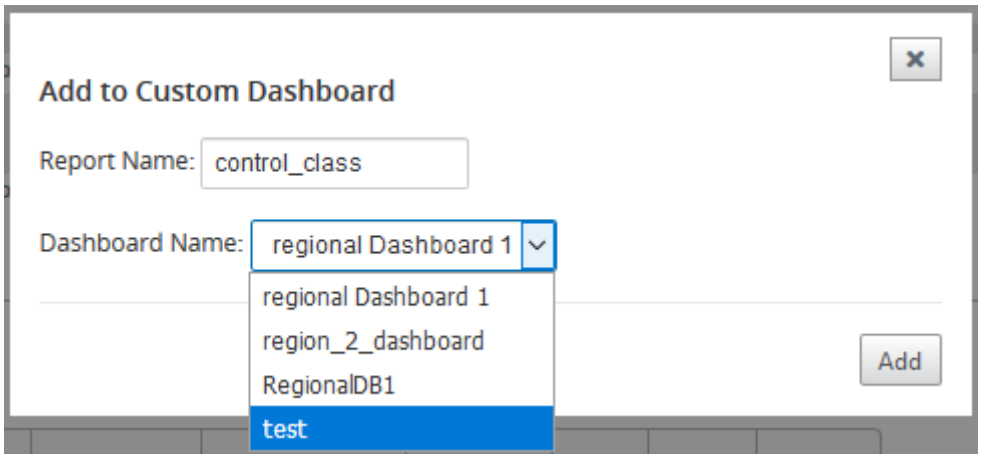
Panel de control personalizado

Puede personalizar el panel de Citrix SD-WAN Center y elegir las estadísticas que quiere ver en el panel en función de sus necesidades analíticas. Cree un panel personalizado de detalles regionales o un resumen global. También puede personalizar un informe existente.

> **Nota**
>
> Ahora puede anclar un informe como widget al panel personalizado mediante la opción **Agregar al panel** de control de la página Informes.



Introduzca el nombre del informe y seleccione el panel personalizado.



Para el panel personalizado Detalles regionales, puede elegir entre los siguientes widgets de nivel de región:

- Resumen del sitio
- Ruta virtual
- Eventos de la región
- Resumen de alarma de región
- Gestor de inventario (por región)

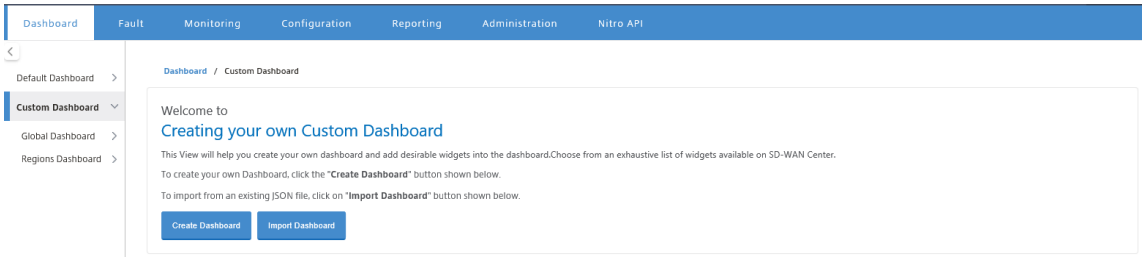
- Principales sitios por región
- Rutas
- Colas MPLS
- Ethernet
- Túneles LAN GRE
- Túneles IPsec
- Resumen del servicio
- Clases
- Eventos del sitio
- Aplicaciones Principales por Región
- Familia de aplicaciones superior por región
- Sitio HDX: Usuarios
- Site HDX: Sesiones
- Sitio HDX: QoE
- Aplicaciones MOS
- Uso de la base

Para un panel personalizado Resumen global, puede elegir entre los siguientes widgets de nivel de red:

- Resumen de varias regiones
- Estado de la ruta virtual en la red
- Eventos
- Resumen de alarmas
- Administrador de inventario
- Mejores sitios de la red
- HDX de red
- Uso de bases de datos en recopiladores
- Aplicaciones Principales
- Familias de aplicaciones principales

Para crear un panel personalizado:

1. Vaya a **Panel de control** > **Panel de control personalizado** y haga clic en **Crear panel de control**.

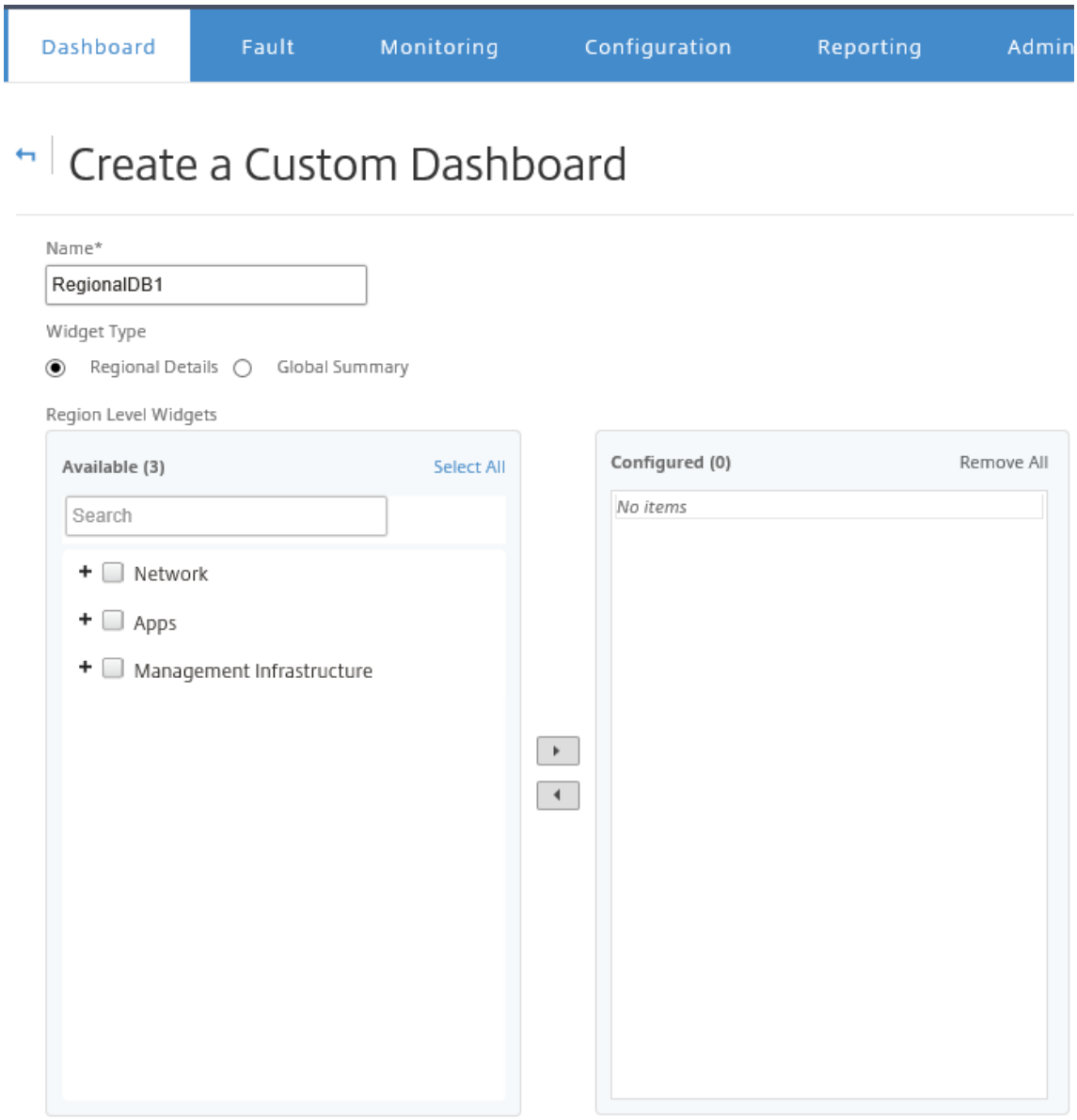


> **Nota**
>
> También puede importar un panel existente en formato JSON haciendo clic en **Importar panel**.

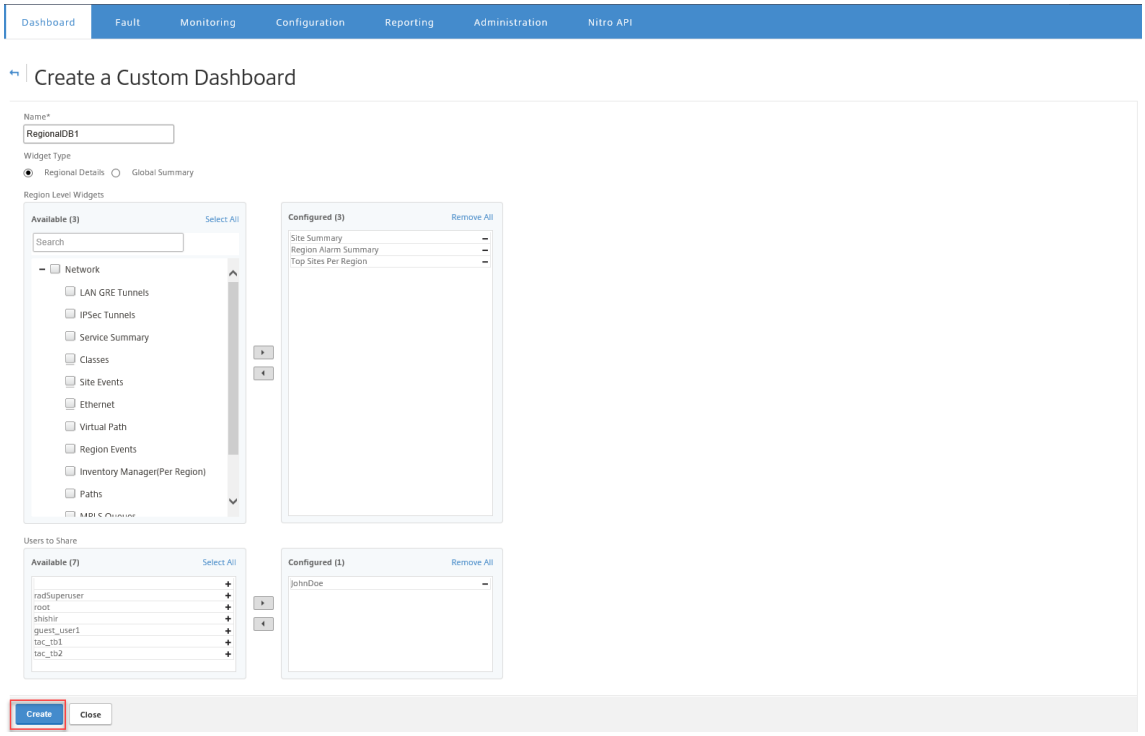
2. En el campo **Nombre**, escriba un nombre para el panel personalizado.
3. Seleccione el tipo de widget. Seleccione **Resumen global** para ver los widgets de nivel de red, seleccione **Detalles regionales** para ver los widgets de nivel regional.

4. Haga clic en **Agregar** y seleccione los widgets necesarios.

   Los widgets se clasifican en tres niveles: Red, Aplicaciones e Infraestructura de administración.



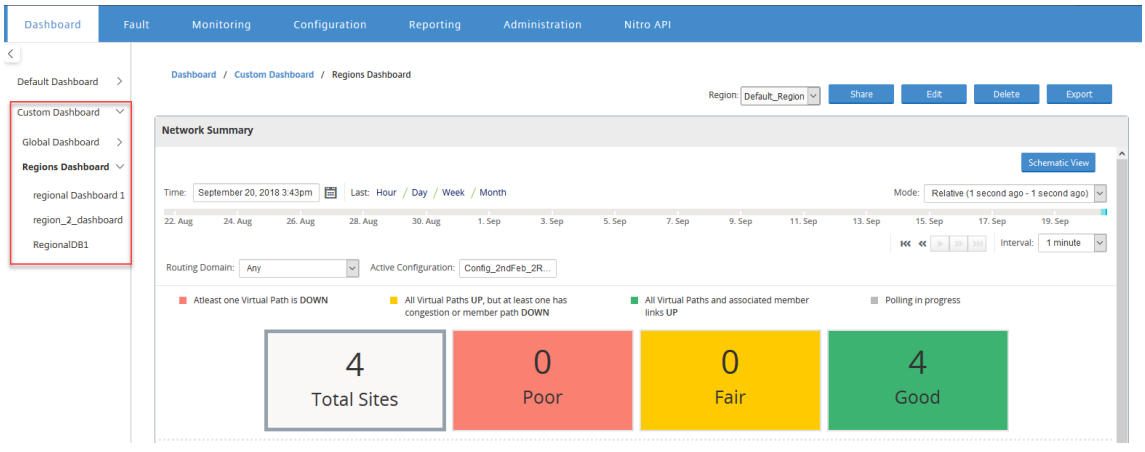
> Nota
>
> En la implementación de una sola región, solo están disponibles los **Widgets de nivel de región**.



También puede compartir el panel personalizado con varios usuarios. Para obtener más información sobre los usuarios, consulte Cuentas de usuario.

5. Haga clic en **Crear**. El panel personalizado recién creado aparece en **Panel personalizado**.

> **Sugerencia**
>
> Puede modificar o eliminar el panel personalizado.



Paquetes diagnóstico

April 13, 2021

Un paquete de diagnóstico consta de todos los archivos de registro del sistema, información del sistema y otros detalles necesarios que ayudarán al equipo de soporte de Citrix SD-WAN a diagnosticar y resolver problemas con el sistema.

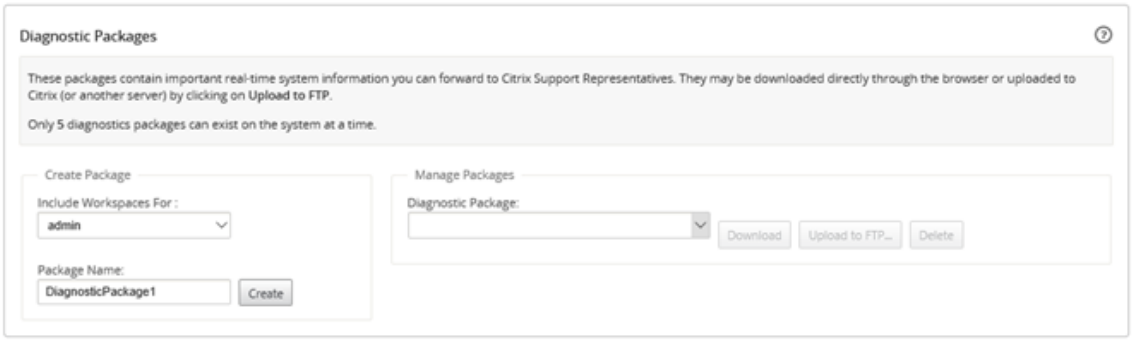
Después de crear el paquete, puede descargarlo en su equipo y, a continuación, enviar el paquete de diagnóstico al servicio de atención al cliente de Citrix o puede cargarlo directamente en el servidor de Soporte al cliente de Citrix (u otro servidor).

> **Nota**
>
> Citrix SD-WAN Center puede almacenar un máximo de cinco paquetes de diagnóstico a la vez.

Para crear un paquete de diagnóstico:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Supervisión** y, a continuación, haga clic en **Diagnósticos**.
2. En la sección **Paquetes de diagnóstico**, en **Crear paquete**, en la lista desplegable **Incluir áreas de trabajo para** seleccione un usuario cuyos espacios de trabajo se copiarán en los diagnósticos.

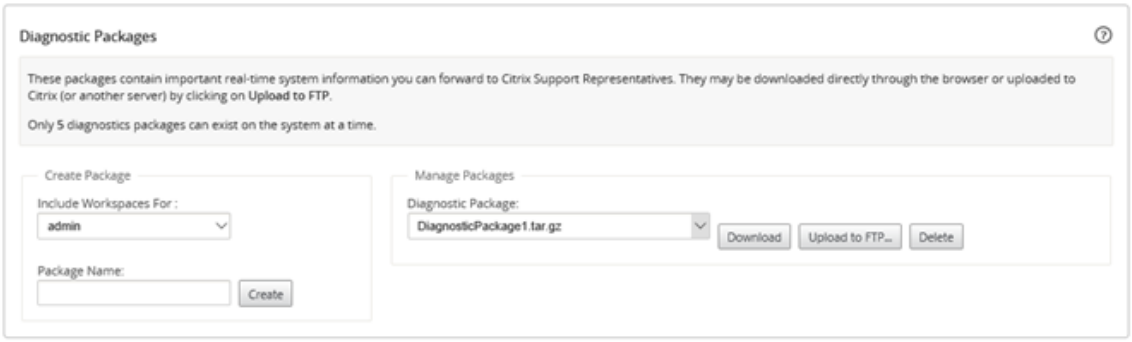
   > **Nota**
   >
   > El paquete de diagnósticos incluirá las cinco configuraciones modificadas más recientemente por el usuario seleccionado.

3. En el campo **Nombre del paquete**, introduzca un nombre para el paquete de diagnóstico.
4. Haga clic en **Crear**. Esto ejecuta un diagnóstico del sistema y genera un paquete de diagnóstico.

Para descargar un paquete de diagnóstico:

1. En la sección **Paquetes de diagnóstico**, en **Administrar paquete**, en la lista desplegable **Paquetes de diagnóstico** seleccione el paquete que quiere descargar.



2. Haga clic en **Download**. El paquete de diagnóstico se descarga en el equipo local.

Para cargar un paquete de diagnóstico en un servidor FTP:

1. En la sección **Paquetes de diagnóstico**, en **Administrar paquete**, en la lista desplegable **Paquetes de diagnóstico** seleccione el paquete que quiera cargar.
2. Haga clic en **Cargar a FTP**. Esto abre el cuadro de diálogo **Cargar al servidor FTP** para especificar la información de autenticación FTP y cargar el paquete en el servidor FTP de Soporte al cliente de Citrix o a otro host FTP.

3. En el campo **Nombre del cliente**, escriba un nombre para ayudar a Citrix SD-WAN Support a identificar los paquetes de diagnóstico.
   Se creará un directorio con este nombre en el servidor FTP de Citrix y sus archivos se cargarán en esa ubicación.

4. En el campo **Host FTP**, introduzca la dirección IP o el nombre de host (si DNS está configurado) del servidor FTP.
5. En el campo **Nombre de usuario**, introduzca un nombre de usuario que se utilizará para iniciar sesión en el servidor FTP.
6. En el campo **Contraseña**, introduzca la contraseña asociada al nombre de usuario.
7. Haga clic en **Cargar**.

> **Nota**
>
> Se recomienda eliminar periódicamente paquetes de diagnóstico antiguos, para evitar exceder el límite para los paquetes máximos permitidos. Para eliminar un paquete de diagnóstico existente, seleccione un paquete de diagnóstico en la lista desplegable **Paquete de diagnóstico** y, a continuación, haga clic en **Eliminar**.

Eventos

April 13, 2021

Citrix SD-WAN Center recopila información de eventos de todos los dispositivos detectados en la red. Esta información de evento se puede filtrar y ver en la página **Visor de eventos**.

Los detalles del evento incluyen la siguiente información.

- **Hora:** la hora en que se generó el evento.
- **Sitio:** El nombre del sitio en el que se originó el evento.
- **Id. de dispositivo:** muestra si el dispositivo desde el que se originó el evento es un dispositivo primario (**0**) o secundario (**1**).

  > **Nota**
  >
  > La columna ID del dispositivo está oculta de forma predeterminada. Para mostrar la columna, haga clic en **Mostrar/Ocultar** (icono de engranaje) y seleccione la casilla de verificación **ID del dispositivo** en el menú desplegable

- **Nombre de Objeto:** El nombre del objeto que genera el evento.
- **Tipo de Objeto:** El tipo de objeto que genera el evento.
- **Severidad:** el nivel de gravedad del evento.
- **Estado anterior:** el estado del objeto antes del evento. El estado aparecerá como **desconocido** si no es aplicable.

- **Estado actual:** el estado del objeto en el momento del evento.
- **Descripción:** Una descripción de texto del evento.

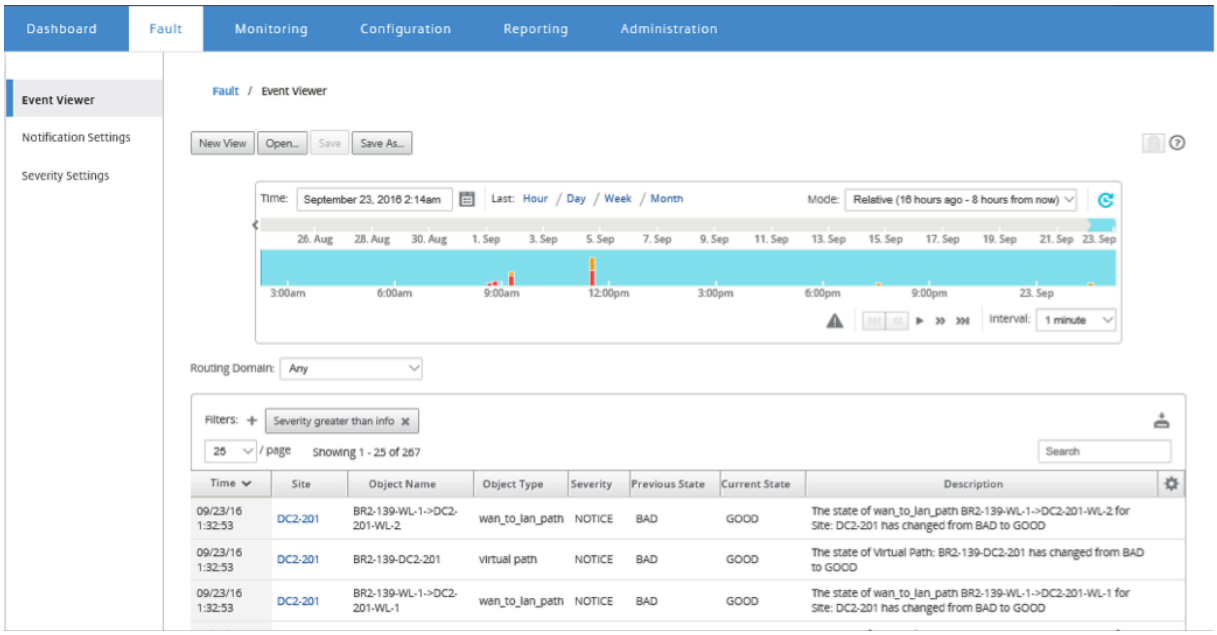
Visualización de eventos

Puede ver los eventos, filtrarlos y descargarlos desde la página Visor de eventos.

Para acceder a la página del visor de eventos.

En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Falla**.

La página Visor de sucesos aparece de forma predeterminada.



Puede seleccionar y ver informes de un período determinado mediante los controles de línea de tiempo. Para obtener más información, consulte, Controles de cronología.

> **Nota**
>
> Puede ver los datos de eventos de los últimos 30 días. Cualquier dato más allá de este período se elimina automáticamente del recopilador SD-WAN Center y de los recopiladores regionales respectivos.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.

Uso de filtros

Puede crear filtros personalizados para restringir los resultados de la tabla Eventos.

Para crear y aplicar un filtro:

1. Haga clic en el icono **+** situado a la derecha de la etiqueta de la sección **Filtros**.
2. Seleccione una categoría en el menú desplegable.

   Las opciones disponibles son:

   - Tamaño
   - Nombre del objeto
   - Tipo de objeto
   - Gravedad
   - Estado anterior
   - Estado actual

3. Seleccione un operador en el menú desplegable central.

   Opciones disponibles:

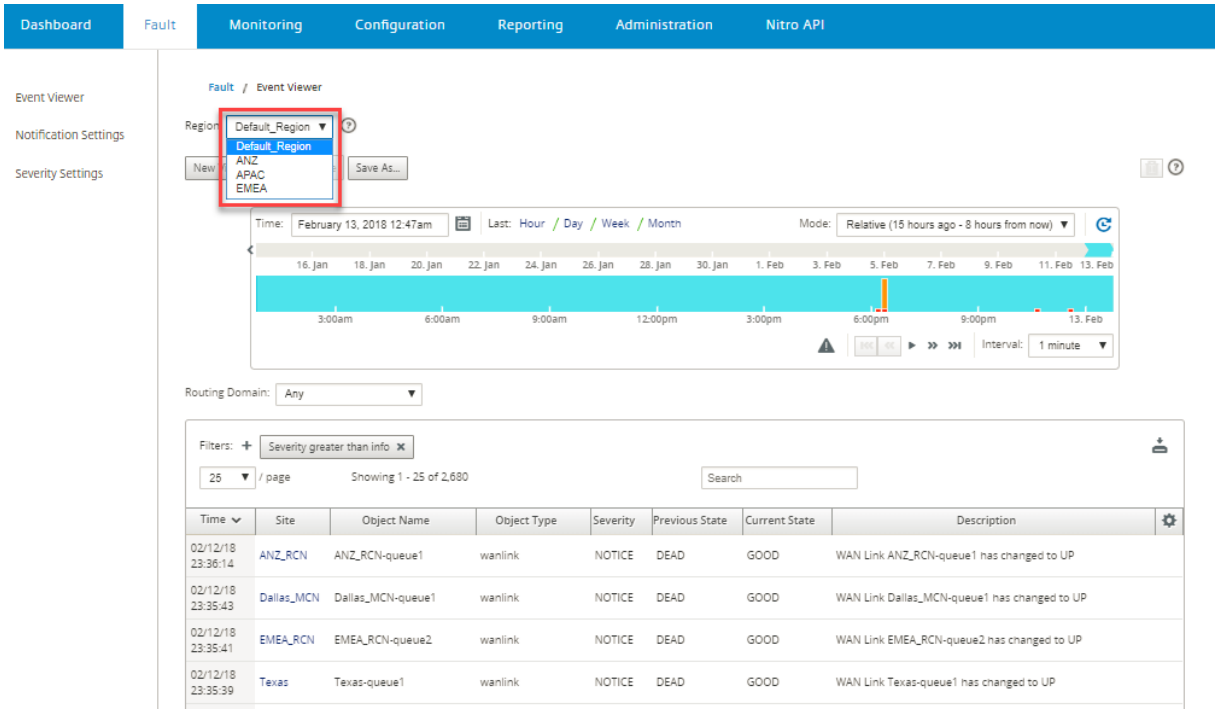
   - es
   - no es
   - es uno de
   - contiene
   - no contiene
   - menos de
   - menor o igual a
   - más de
   - igual o mayor que

4. Introduzca la cadena o el valor por el que desea delimitar el filtro.

> **Nota**
>
> Este campo distingue mayúsculas y minúsculas.

> **Nota**
>
> Puede crear y aplicar varios filtros.
> En Red de varias regiones, puede seleccionar regiones específicas para ver el evento.

Los datos de eventos se obtienen del recopilador de la región respectiva.



> **Nota**
>
> En la implementación de red de una sola **región, la lista desplegable Región** no está disponible.

Para descargar la tabla de eventos como un archivo CSV:

Haga clic en el icono Descargar en la esquina superior derecha de la tabla de eventos.

Para obtener más información sobre las estadísticas de eventos, consulte Informe de eventos.

Puede configurar Citrix SD-WAN Center para que envíe notificaciones de eventos externos para diferentes tipos de eventos como correo electrónico, capturas SNMP o mensajes syslog. Para obtener más información, consulte Notificaciones de eventos.

Notificaciones de eventos

April 13, 2021

Puede configurar Citrix SD-WAN Center para que envíe notificaciones de eventos para diferentes tipos de eventos como correo electrónico, capturas SNMP o mensajes syslog. Una vez que haya configurado la configuración de notificación de correo electrónico, SNMP y syslog, puede seleccionar la gravedad para diferentes tipos de eventos y seleccionar el modo (correo electrónico, SNMP, syslog) para enviar notificaciones de eventos. Se generan notificaciones para eventos iguales o superiores al nivel de gravedad especificado para el tipo de evento.

Los niveles de gravedad disponibles son los siguientes, en orden descendente de gravedad:

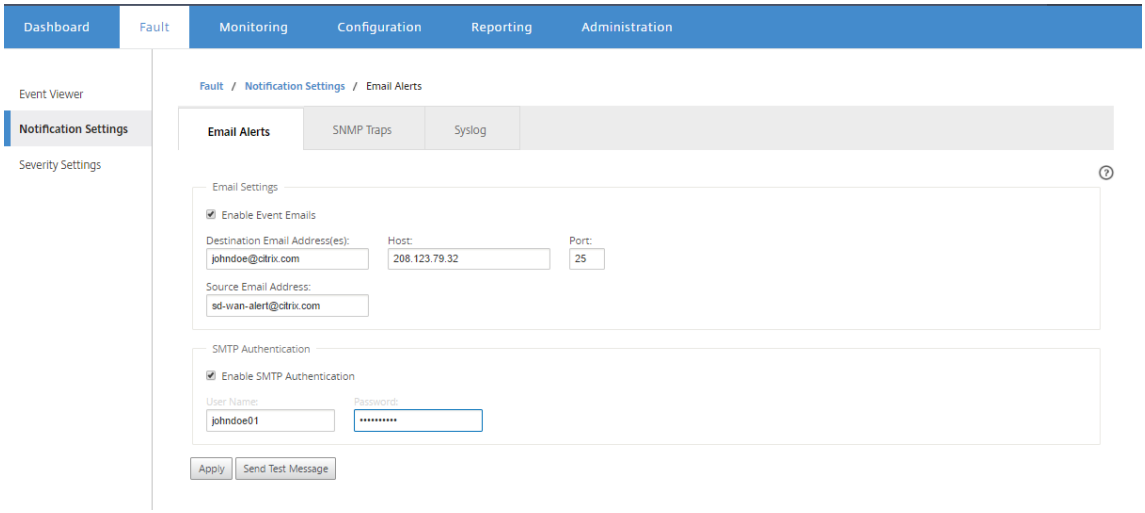
- EMERGENCIA
- ALERTA
- CRÍTICO
- ERROR
- ADVERTENCIA
- AVISO
- INFORMATIVO
- DEPURACIÓN

> **Sugerencia**
>
> Puede configurar las opciones de notificación para recibir alertas de eventos por correo electrónico, capturas SNMP o mensajes Syslog tanto en Citrix SD-WAN Center como en los dispositivos Citrix SD-WAN individuales de la red.
>
> Sin embargo, habilitar las notificaciones en Citrix SD-WAN Center le permite recibir notificaciones de eventos para toda la red de Citrix SD-WAN (es decir, MCN y todos los sitios). Si bien, habilitar las notificaciones en los dispositivos Citrix SD-WAN le permite recibir notificaciones solo de los dispositivos individuales.
>
> Se recomienda habilitar las notificaciones solo en Citrix SD-WAN Center, para evitar las notificaciones redundantes de los demás dispositivos Citrix SD-WAN de la red.

Configuración de las opciones de notificación de correo electrónico

Para configurar las opciones de notificación por correo electrónico:

1. En la interfaz de administración web de Citrix SD-WAN Center, vaya a **Falla** > **Configuración de notificaciones** > **Alertas de correo electrónico.**



2. Seleccione **Activar correos electrónicos de eventos**.
3. En el campo **Dirección de correo electrónico de destino**, introduzca la dirección de correo electrónico a la que se van a enviar las notificaciones de alerta.

   > **Nota**
   >
   > Puede introducir varias direcciones de correo electrónico separadas por punto y coma.

4. En el campo **Host**, introduzca la dirección IP o el nombre de host de un servidor SMTP externo para retransmitir mensajes de correo electrónico a Internet.
5. En el campo **Puerto**, introduzca el número de puerto que se utilizará para la conexión SMTP. El puerto predeterminado es 25.
6. En el campo **Dirección de correo electrónico de origen**, introduzca la dirección de correo electrónico desde la que se envían las alertas de correo electrónico.
7. Seleccione **Habilitar autenticación SMTP**.
8. En el campo **Nombre de usuario**, escriba un nombre de usuario para el servidor SMTP utilizado para la autenticación.
9. En el campo **Contraseña**, introduzca la contraseña asociada al nombre de usuario del servidor SMTP utilizado para la autenticación.

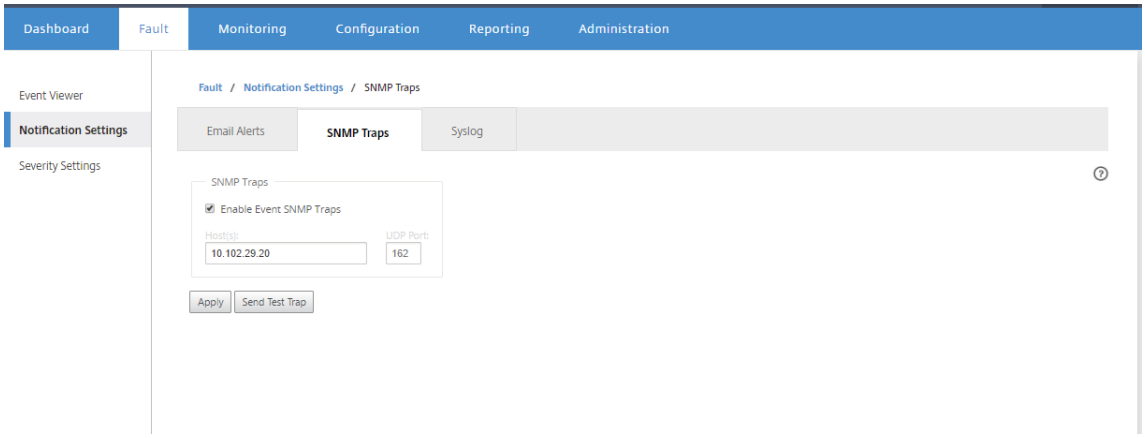
   > **Nota**
   >
   > Haga clic en **Enviar mensaje de prueba** para enviar una alerta de correo electrónico de ejemplo a los destinatarios configurados.

10. Haga clic en **Aplicar**.

Configuración de las opciones de notificación de captura SNMP

Para configurar las opciones de notificación de captura SNMP:

1. En la interfaz de administración web de Citrix SD-WAN Center, vaya a **Falla** > **Configuración de notificaciones** > **Trampas SNMP**.
2. Seleccione **Activar capturas SNMP de eventos.**



3. En el campo **Host (s)**, introduzca la dirección IP o el nombre de host de un sistema SNMP externo. Este host recibirá los eventos como capturas SNMP.

   > **Nota**
   >
   > Puede introducir varias direcciones IP o nombres de host separados por punto y coma.

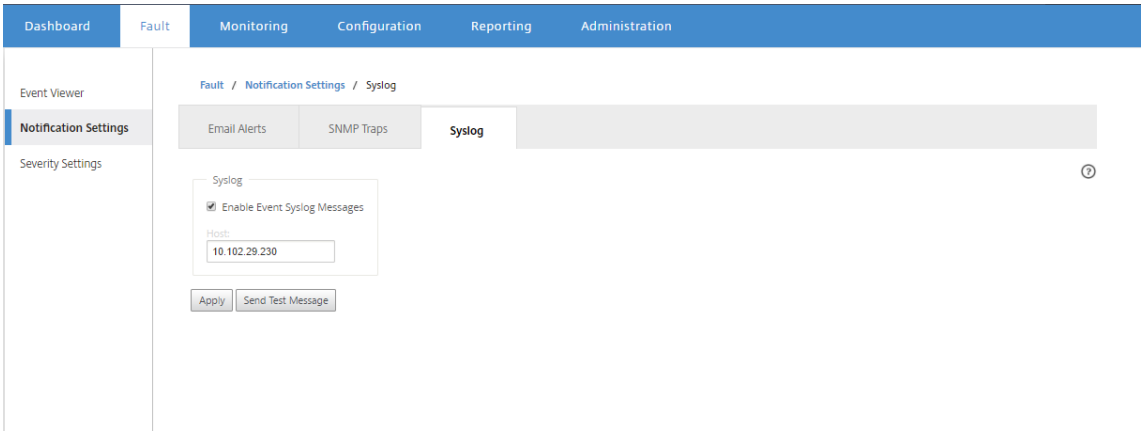
4. En el campo **Puerto UDP**, introduzca el puerto UDP que se utilizará para enviar las capturas SNMP. De forma predeterminada, el puerto UDP se establece en 162.
5. Haga clic en **Aplicar** para aplicar la configuración de notificación de capturas SNMP.

   > **Nota**
   >
   > Como alternativa, haga clic en **Enviar captura de prueba** para comprobar si el sistema puede enviar una captura SNMP al destino configurado.

Configuración de las opciones de notificación de syslog

Para configurar las opciones de notificación de Syslog:

1. En la interfaz de administración web de Citrix SD-WAN Center, vaya a **Falla** > **Configuración de notificación** > **Syslog**.
2. Seleccione **Habilitar mensajes de Syslog de eventos.**



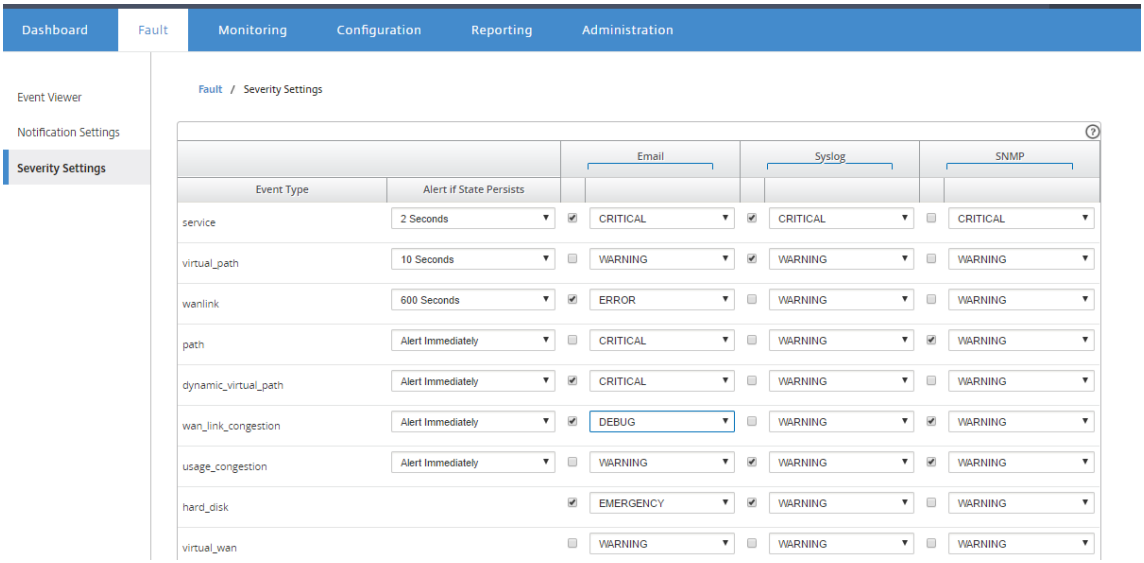
3. En el campo **Host**, introduzca la dirección IP o el nombre de host de un servidor syslog externo, que se utilizará para recibir eventos como mensajes syslog.
4. Haga clic en **Aplicar** para aplicar la configuración de notificación de syslog.

> **Nota**
>
> Como alternativa, haga clic en **Enviar mensaje de prueba** para comprobar si el sistema puede enviar un mensaje syslog al host configurado.

Configuración de notificaciones de eventos

Para configurar las notificaciones de eventos:

1. En la interfaz de administración web de Citrix SD-WAN Center, vaya a **Falla** > **Configuración de gravedad**.
2. En el campo **Alerta si el estado persiste**, seleccione la duración tras la cual, si el evento persiste, se enviará una notificación.



3. Para cada tipo de evento, seleccione la opción de notificación y seleccione la gravedad.

> **Nota**
>
> Las opciones de notificación de correo electrónico, Syslog y SNMP solo se habilitarán después de configurar las respectivas opciones de notificación.

4. Haga clic en **Aplicar**.

Configuración de alarmas

También puede configurar alarmas en Citrix SD-WAN Center y enviarlas a dispositivos individuales.

Para configurar la alarma en Citrix SD-WAN Center, vaya a **Configuración** > **Configuracióndel dispositivo** > **Configuración de notificación** > **Configuración de alarma** y haga clic en **+**.

Seleccione o introduzca valores para los siguientes campos:

- **Tipo de evento**: El dispositivo Citrix SD-WAN puede desencadenar alarmas para subsistemas u objetos concretos de la red, que se denominan tipos de evento. Los tipos de evento disponibles son SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL e IPSEC_TUNNEL.
- **Estado del desencadenador**: Estado del evento que activa una alarma para un tipo de evento. Las opciones de estado de activación disponibles dependen del tipo de evento elegido.
- **Duración del desencadenador**: La duración en segundos determina la rapidez con que el dispositivo desencadena una alarma. Introduzca”0”para recibir alertas inmediatas o introduzca un valor entre 15-7200 segundos.Las alarmas no se activan si se producen eventos adicionales en el mismo objeto dentro del período de duración del disparador. Las alarmas adicionales se activan solo si un evento persiste más tiempo que el período de duración del desencadenador.
- **Borrar estado: Estado**del evento que borra una alarma para un tipo de evento después de que se activa la alarma. Las opciones de Borrar estado disponibles dependen del estado de activación elegido.
- **Duración clara:** La duración en segundos determina cuánto tiempo se debe esperar antes de borrar una alarma.Introduzca”0”para borrar inmediatamente la alarma o introduzca un valor entre 15-7200 segundos. La alarma no se borra si se produce otro evento de estado claro en el mismo objeto dentro del tiempo especificado.

- **Gravedad**: Campo definido por el usuario que determina la urgencia de una alarma. La gravedad se muestra en las alertas enviadas cuando se activa o borra la alarma y en el resumen de la alarma activada.
- **Correo electrónico**: El activador de alarma y las alertas claras para el tipo de evento se envían por correo electrónico.
- **Syslog**: El activador de alarma y las alertas claras para el tipo de evento se envían a través de Syslog.
- **SNMP**: El disparador de alarma y las alertas claras para el tipo de evento se envían a través de la captura SNMP.

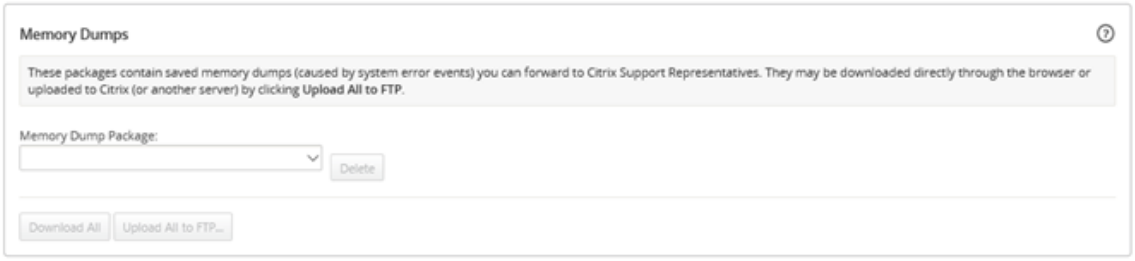
Volcados de memoria

April 9, 2021

Se genera un volcado de memoria cuando se bloquea un proceso. Todos los volcados de memoria actualmente en el sistema se pueden descargar en un paquete combinado y cargarlos en un servidor FTP para su examen por el equipo de soporte de Citrix. Sin embargo, puede eliminar volcados de memoria individuales.

Para descargar volcados de memoria:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Supervisión** y, a continuación, haga clic en **Diagnósticos**.
2. En la sección **Volcados de memoria**, en la lista desplegable **Paquete de volcado de memoria** seleccione un paquete de volcado de memoria.



3. Haga clic en **Descargar todo**. Guarde el paquete de volcado de memoria en el equipo local.

Para cargar un paquete de volcado de memoria en un servidor FTP:

1. En la sección **Volcados de memoria**, en la lista desplegable **Paquete de volcado de memoria** seleccione un paquete de volcado de memoria.

2. Haga clic en **Cargar al servidor FTP**. Esto abre el cuadro de diálogo **Cargar todo en FTP** para especificar la información de autenticación FTP y cargar el paquete en el servidor FTP de Soporte al cliente de Citrix o a otro host FTP.

3. En el campo **Nombre del cliente**, escriba un nombre para ayudar a Citrix SD-WAN Support a identificar los paquetes de diagnóstico.

   Se creará un directorio con este nombre en el servidor FTP de Citrix y sus archivos se cargarán en esa ubicación.

4. En el campo **Host FTP**, introduzca la dirección IP o el nombre de host (si DNS está configurado) del servidor FTP.
5. En el campo **Nombre de usuario**, introduzca un nombre de usuario que se utilizará para iniciar sesión en el servidor FTP.
6. En el campo **Contraseña**, introduzca la contraseña asociada al nombre de usuario.
7. Haga clic en **Cargar**.

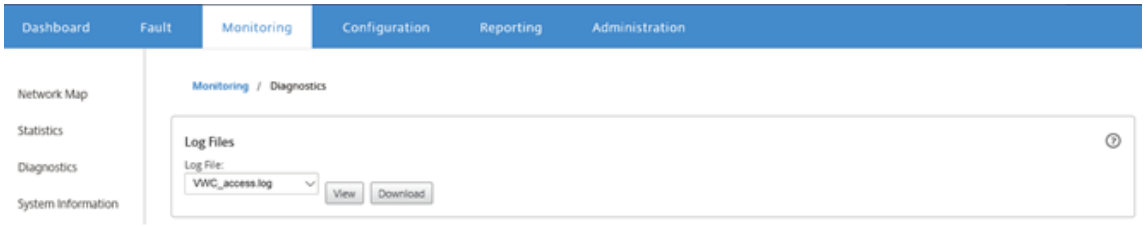
Archivos de registros

April 9, 2021

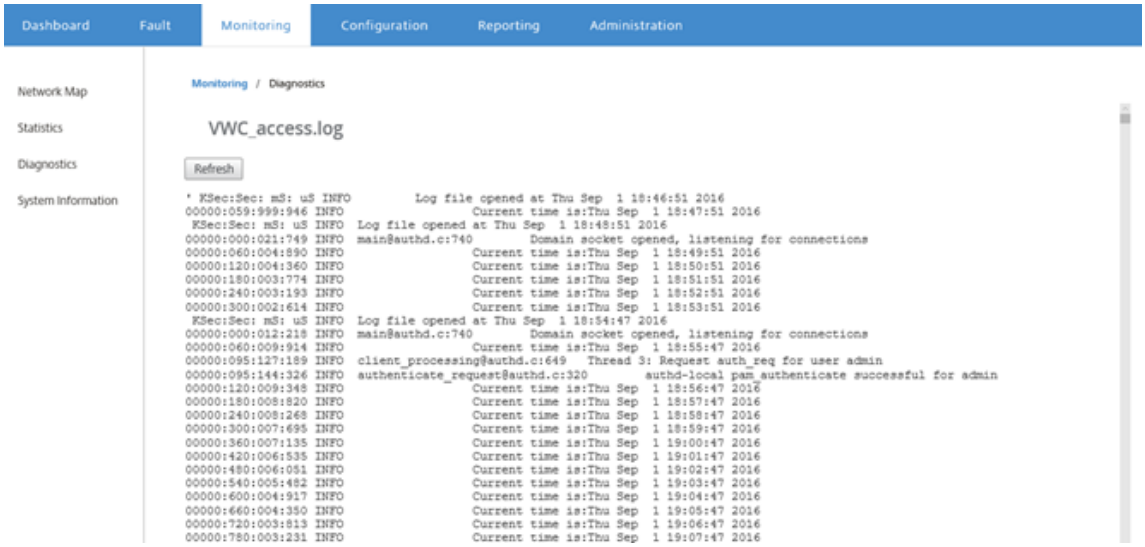
Los archivos de registro recopilan información relacionada con la consola web, excepciones de interfaz de usuario, bloqueos internos, etc. Estos registros se pueden utilizar para solucionar problemas en Citrix SD-WAN Center.

Para ver archivos de registro:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Supervisión**.
2. Haga clic en **Diagnósticos**.
3. En la lista desplegable **Archivo de registro**, seleccione el archivo de registro que quiere ver.



4. Haga clic en **Ver**. Se muestra el contenido del archivo de registro.



5. Si quiere descargar los archivos de registro en el equipo, haga clic en **Descargar**.

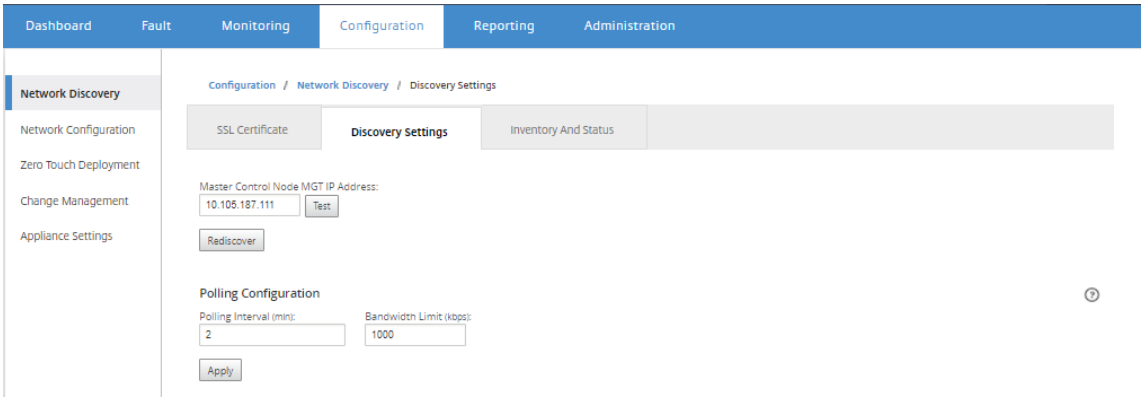
Intervalo de sondeos

April 13, 2021

La encuesta se refiere al proceso de recopilación de estadísticas del dispositivo descubierto. Puede configurar el intervalo y el límite de ancho de banda para las operaciones de sondeo después de descubrir los dispositivos. Para obtener información sobre cómo descubrir el dispositivo, consulte Implementación de red en una región o Implementación de red en varias regiones.

Para realizar la configuración de sondeo:

1. En la interfaz web de Citrix SD-WAN Center, vaya a **Configuración** > **Detección de redes** > **Configuración de detección**.



2. En el campo **Intervalo de sondeo**, introduzca la frecuencia de sondeo en minutos. El rango es de 2 a 60 minutos. El valor predeterminado es 5 minutos.
3. En el campo **Límite de ancho de banda**, introduzca el límite de ancho de banda de sondeo en kbps. El MCN limitará el ancho de banda al valor especificado al transferir estadísticas de sondeo desde el dispositivo a Citrix SD-WAN Center. El rango es de 100 Kbp —1 Gbps. El valor predeterminado es 1 Mbps.
4. Haga clic en **Aplicar**.

Estadísticas

April 13, 2021

Puede ver las estadísticas recopiladas por Citrix SD-WAN Center como gráficos. Estos gráficos se trazan como línea de tiempo frente al uso, lo que le permite comprender las tendencias de uso de varias propiedades de objetos de red. Puede ver gráficos para estadísticas de aplicaciones de toda la red. Para cada sitio de la red SD-WAN, puede ver gráficos para los siguientes parámetros de red:

- Ancho de banda
- QoS
- Ruta virtual
- Servicios de Internet
- Servicios de Intranet
- Servicios PassThrough
- Enlaces WAN
- Interfaces Ethernet
- Túneles GRE

- Túneles IPSec
- Aplicaciones
- Familias de aplicaciones

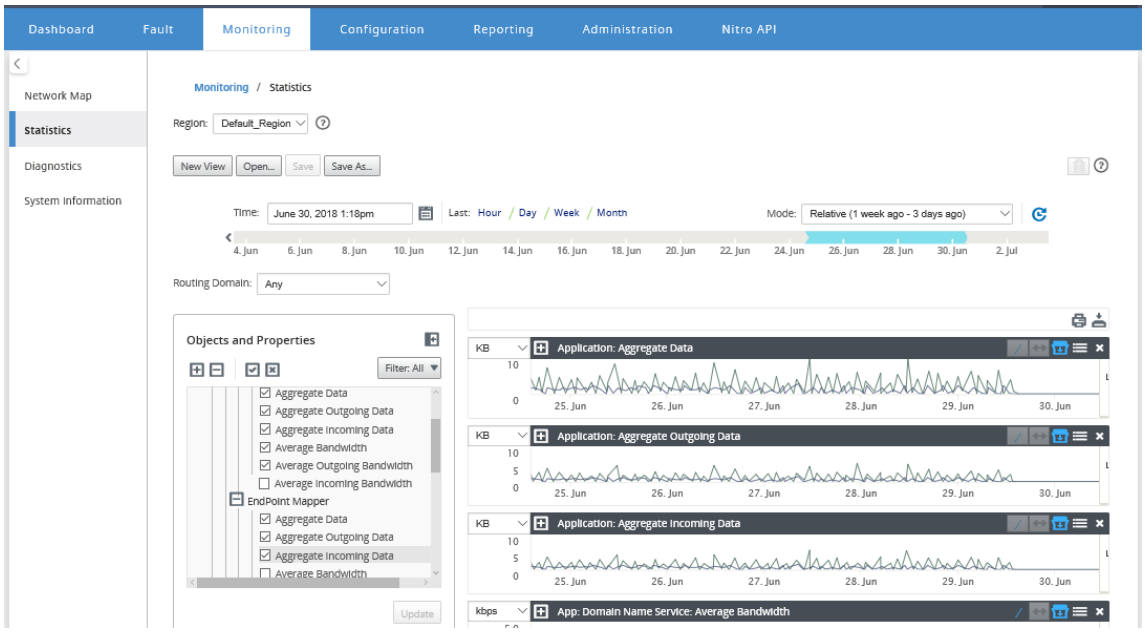
> **Sugerencia**
>
> Puede crear vistas según sus necesidades, guardarlas y abrir vistas existentes.

Para ver gráficos estadísticos:

1. En la interfaz de usuario web de Citrix SD-WAN Center, vaya a **Supervisión** > **Estadísticas**.
2. Seleccione una región y un dominio de enrutamiento.
3. En el árbol jerárquico **Objetos y propiedades**, busque y seleccione las propiedades de interés.

   > **Sugerencia**
   >
   > También puede utilizar el menú desplegable **Filtro** y el menú **Presets** para simplificar el proceso de búsqueda y selección de propiedades.

4. Haga clic en **Actualizar** para mostrar los gráficos de las propiedades seleccionadas.

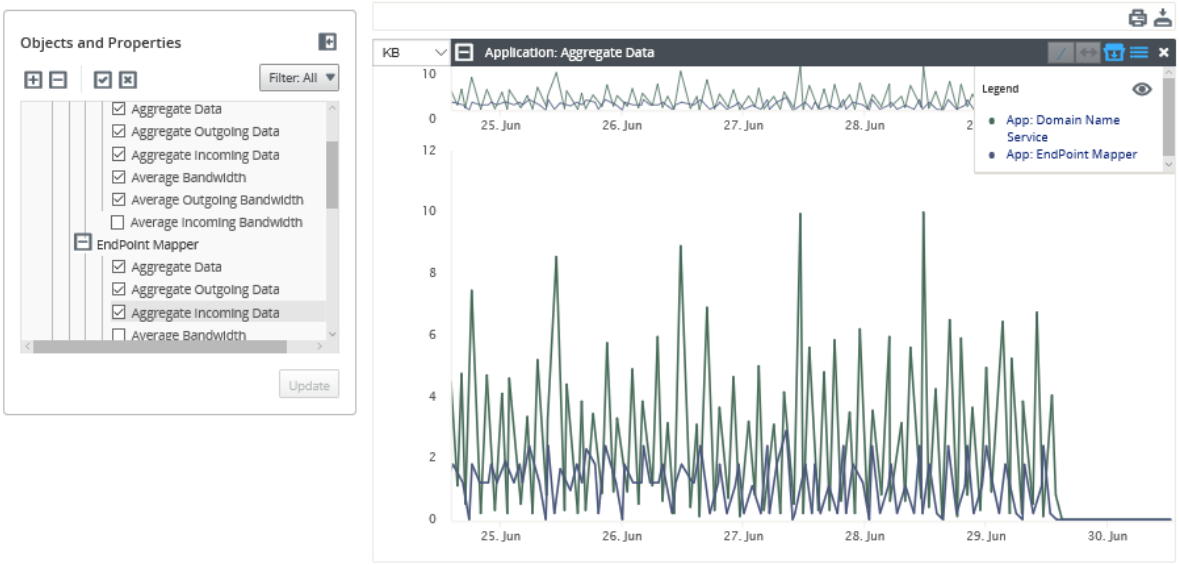


> **Sugerencia**
>
> Anule la selección de una propiedad y haga clic en **Actualizar** para quitar el gráfico de esa propiedad del área Visualización de gráficos.

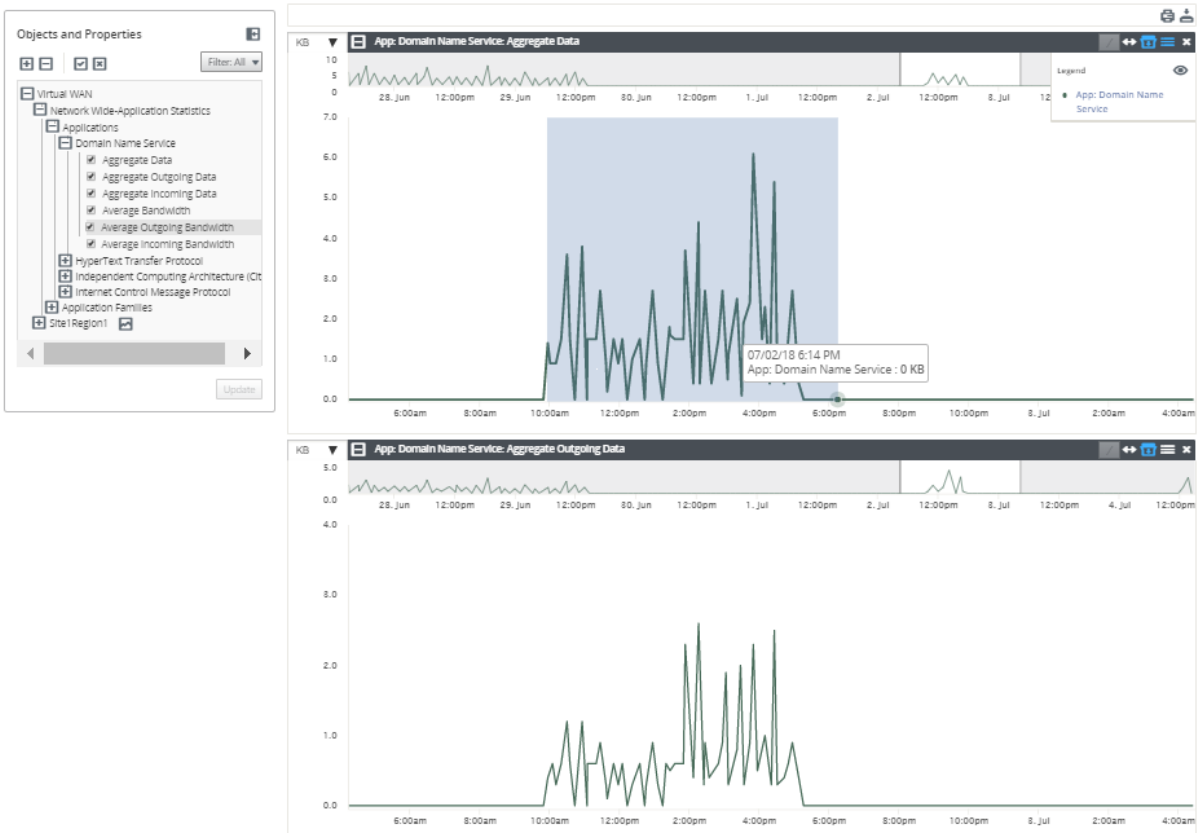
5. Seleccione un período para la vista actual. Para obtener más información, consulte Controles de cronología

   Los gráficos se muestran en función de las propiedades seleccionadas.

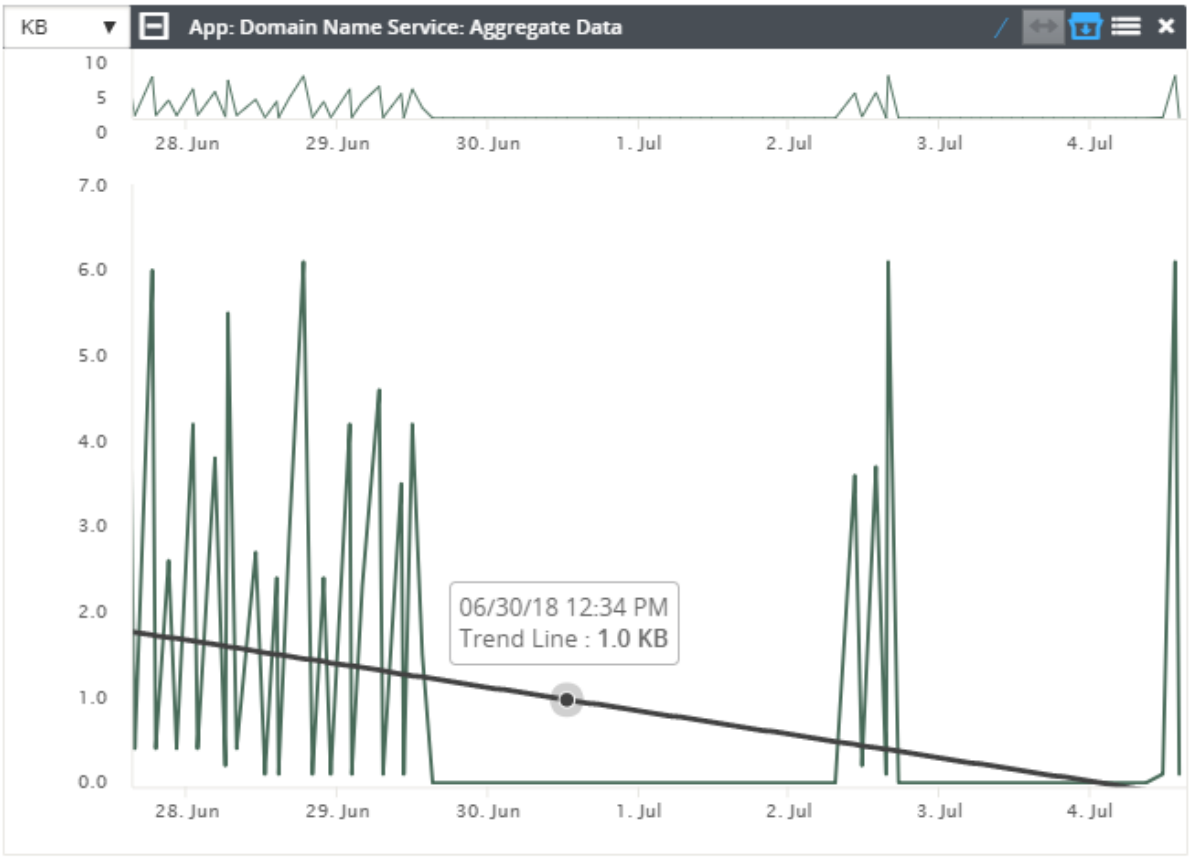
> **Sugerencia**
>
> Si selecciona más de una propiedad, los gráficos se mostrarán en modo **Vista de tendencia** para ahorrar espacio vertical. Haga clic en el encabezado de un gráfico para mostrar y ocultar el gráfico completamente expandido. También puede mostrar y ocultar la vista de tendencia y las leyendas en los gráficos.



> **Sugerencia**
>
> Para ampliar un gráfico, haga clic y arrastre el área de trazado del gráfico. El zoom en un gráfico amplía todos los gráficos, hasta el tiempo seleccionado, para mantener una vista coherente. Haga clic en el icono de restablecimiento (↔) para restablecer el zoom.



> **Sugerencia**
>
> Puede mostrar y ocultar la línea de tendencia haciendo clic en el icono (/).



> **Nota**
>
> Puede imprimir los gráficos o descargar el conjunto de gráficos como un archivo CSV.

Información del sistema

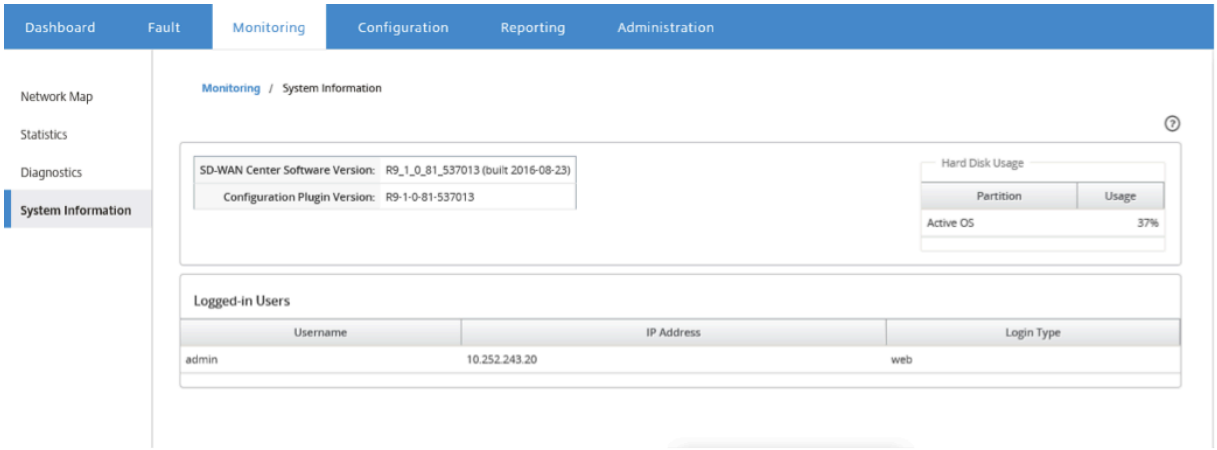
April 9, 2021

La siguiente información se muestra en la página de información del sistema:

- **Versión del software Citrix SD-WAN Center**: La versión del software Citrix SD-WAN Center instalada y ejecutándose en esta máquina virtual.
- **Versión del plugin de configuración**: La versión del plugin del editor de configuración actualmente instalada y ejecutándose en esta máquina virtual de Citrix SD-WAN Center.
- **Uso del disco duro**: Cantidad de espacio en disco duro utilizado por el sistema operativo y las particiones de datos.
- **Usuarios conectados**: Nombre de usuario, dirección IP y tipo de inicio de sesión de cada usuario que haya iniciado sesión en esta máquina virtual de Citrix SD-WAN Center.

Para mostrar la información del sistema:

En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Supervisión** y, a continuación, haga clic en **Información del sistema**.



Informes

April 13, 2021

Citrix SD-WAN Center proporciona los siguientes informes:

- **Aplicaciones:** muestra detalles sobre el tráfico entrante, el tráfico saliente y el tráfico total de las aplicaciones, sitios y familias de aplicaciones principales.
- **HDX**: Muestra datos HDX detallados para cada sitio.
- **Sitios:** muestra las estadísticas de nivel de sitio para cada sitio de la WAN virtual. Las filas Sitios se expanden para mostrar la tabla **Servicios** filtrada para el sitio.
- **Servicio:** Muestra estadísticas de resumen por tipo de servicio (Ruta virtual, Internet, Intranet y PassThrough) para cada sitio de la WAN virtual. Las filas Servicios se expanden para mostrar los Servicios individuales para el tipo de servicio.
- **Rutas virtuales:** muestra las estadísticas de nivel de ruta virtual para cada ruta virtual de la SD-WAN. Las filas Rutas virtuales se expanden para mostrar las rutas contenidas en la ruta virtual.

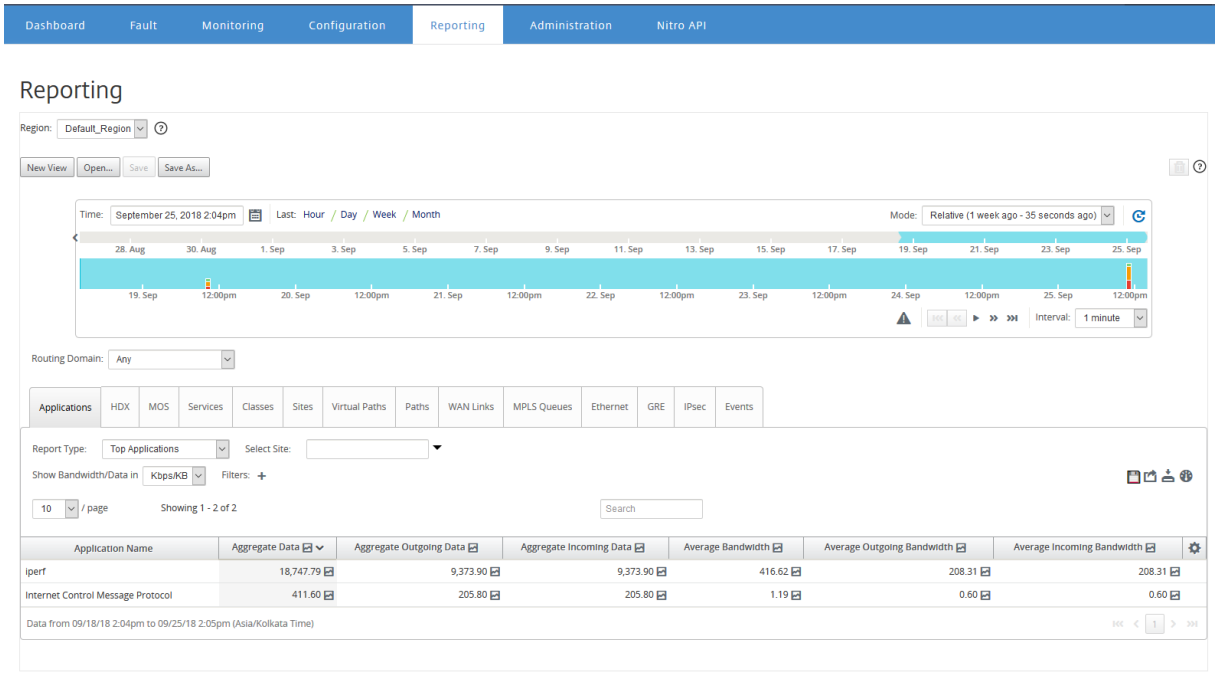
> **Nota**
>
> Los datos de ruta virtual se registran desde la perspectiva de ambos endpoints, como tal, cada ruta virtual puede tener dos filas identificadas por el sitio que registró las estadísticas.

- **Rutas de acceso:** muestra las estadísticas de nivel de ruta de cada ruta de la WAN virtual.
- **Vínculos WAN:** Muestra las estadísticas de nivel de vínculo WAN para cada vínculo WAN en cada sitio de la WAN virtual. Las filas Vínculos WAN se expanden para mostrar un resumen de uso

para cada tipo de servicio para ese vínculo WAN. A continuación, cada fila de tipo de servicio se expandirá para mostrar los usos de cada servicio de ese tipo. Si el enlace WAN es un vínculo MPLS privado, se mostrará una segunda tabla que muestra las colas MPLS para el vínculo WAN.

- **Colas MPLS:** Las filas Colas MPLS se expanden para mostrar un resumen de uso para cada tipo de servicio de esa cola. A continuación, cada fila de tipo de servicio se expandirá para mostrar los usos de cada servicio de ese tipo.
- **Clases:** Muestra las estadísticas de nivel de clase para cada clase de cada ruta virtual en la WAN virtual.
- **Score MOS**: La puntuación media de opinión (MOS) proporciona una medida numérica de la calidad de la experiencia que una aplicación ofrece a los usuarios finales.
- **Interfaces Ethernet:** Muestra estadísticas de nivel de interfaz Ethernet para cada interfaz en cada sitio de la WAN virtual.
- **Túneles GRE:** muestra estadísticas de cada túnel LAN GRE en cada sitio de la WAN.
- **Túneles IPSec:** muestra estadísticas de cada túnel de seguridad IP en cada sitio de la WAN.
- **Eventos:** Muestra los recuentos resumidos de los eventos que ocurren en cada sitio de la WAN virtual. Las filas**Eventos** se expanden para mostrar los recuentos de resumen por tipo de objeto para ese sitio. A continuación, cada tipo de objeto se expandirá para mostrar los recuentos de resumen de cada objeto de ese tipo.

En la ficha **Informes** de la interfaz web de Citrix SD-WAN Center, puede ver todos los informes o informes seleccionados. También puede descargar informes.

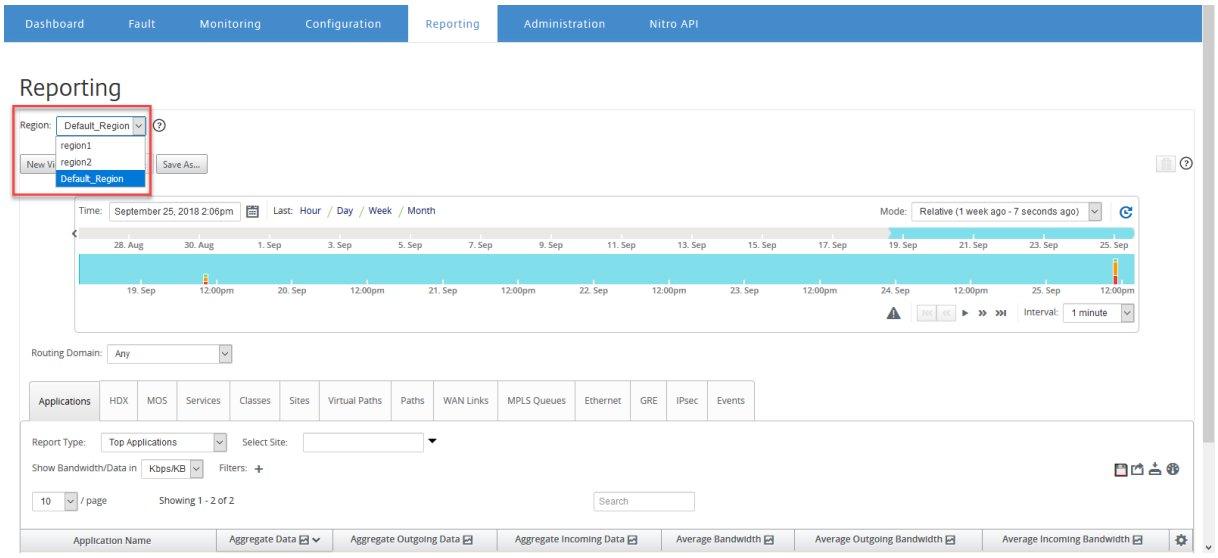


Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.

En Red multiregión, puede seleccionar regiones específicas para ver los informes estadísticos.

Los datos de los informes se obtiene del recopilador de la región respectiva.



> **Nota**
>
> En la implementación de red de una sola **región, la lista desplegable Región** no está disponible.

Para obtener más información sobre cómo ver diferentes informes, consulte los siguientes temas:

Informe de solicitud

Informe de Ancho

Informe de clase

Informe de interfaz Ethernet

Informe de eventos

Informe del túnel GRE

Informe HDX

Informe de túnel IPSec

Vincular informe de rendimiento

MOS para aplicaciones

Informe de colas MPLS

Informe de aplicación

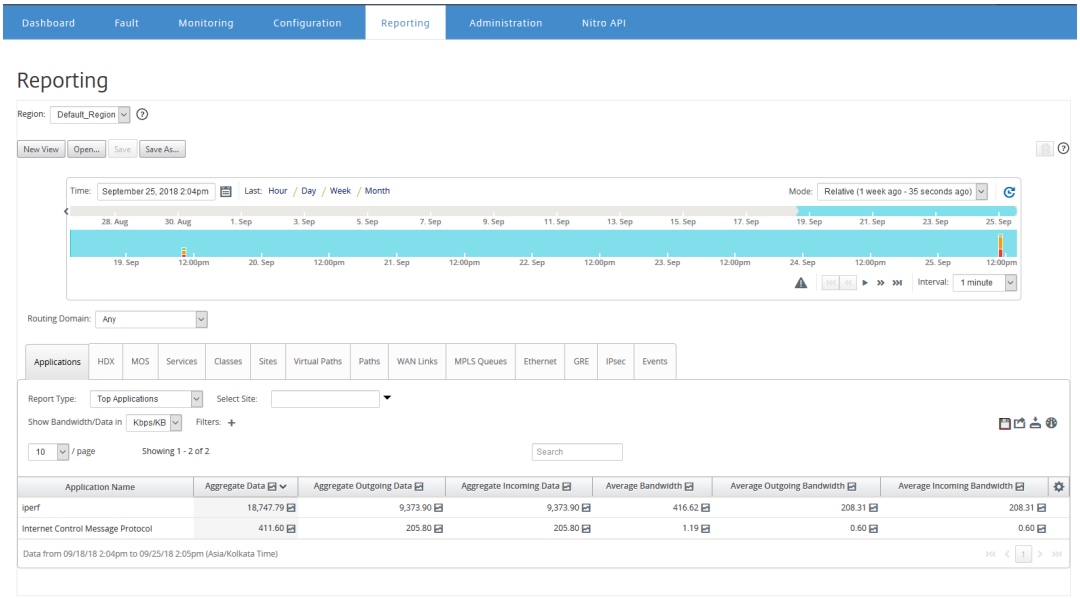
April 13, 2021

La inspección profunda de paquetes (DPI) permite al dispositivo SD-WAN analizar el tráfico que pasa a través de él e identificar los tipos de aplicación y familia de aplicaciones. El dispositivo Citrix SD-WAN registra el número de bytes y el ancho de banda del tráfico entrante y saliente de cada aplicación. SD-WAN Center sondea el dispositivo SD-WAN en el intervalo de sondeo definido, obtiene estos datos y los muestra en el panel y como informes.

Puede ver las aplicaciones principales, los sitios principales y los informes de la familia de aplicaciones principales. Estos informes proporcionan detalles sobre el ancho de banda y los datos totales, entrantes y salientes.

Para ver informes de aplicaciones en Citrix SD-WAN Center:

1. En la interfaz de usuario web de Citrix SD-WAN Center, vaya a **Informes** > **Aplicaciones**.
2. En el control de línea de tiempo, seleccione el intervalo de tiempo. Para obtener más información, consulte Controles de cronología.
3. Seleccione la unidad para mostrar los datos. Puede elegir ver los datos del informe en unidades de Kbps, Mbps o Gbps.
4. En la lista desplegable **Tipo de informe**, seleccione uno de los siguientes tipos de informe:
    - **Aplicaciones principales: Las**aplicaciones principales utilizadas en la red para el intervalo de tiempo seleccionado. Puede filtrar la aplicación superior por nombre de sitio. De forma predeterminada, se muestran las aplicaciones principales de todos los sitios.
    - **Familias de aplicaciones principales**: familias de aplicaciones principales utilizadas en la red. Puede filtrar las familias de aplicaciones principales por nombre de sitio. De forma predeterminada, se muestran las familias de aplicaciones principales de todos los sitios.
    - **Sitios principales**: tráfico en los sitios superiores para el intervalo de tiempo seleccionado. Puede filtrar los sitios principales por aplicación o nombre de familia de la aplicación.



Para cada tipo de informe, puede ver los datos siguientes:

- **Datos entrantes agregados: datos**de aplicación que llegan al sitio desde la WAN.
- Datos**salientes agregados: datos**de aplicación enviados desde el sitio a la WAN.
- **Datos agregados**: suma del tráfico entrante y saliente.
- Ancho de**banda entrante medio**: ancho de banda del tráfico entrante de aplicaciones.
- Ancho de**banda saliente medio**: ancho de banda del tráfico saliente de aplicaciones.
- **Ancho de banda medio**: ancho de banda total consumido por el tráfico de aplicaciones entrante y saliente.

> **Sugerencia**
>
> Para cada valor, puede pasar el cursor del ratón sobre el icono del gráfico para ver un mini-gráfico o hacer clic para abrir la vista gráfica en otra ventana. Para obtener más información, consulte Estadísticas.

Informe QoE de la aplicación

April 13, 2021

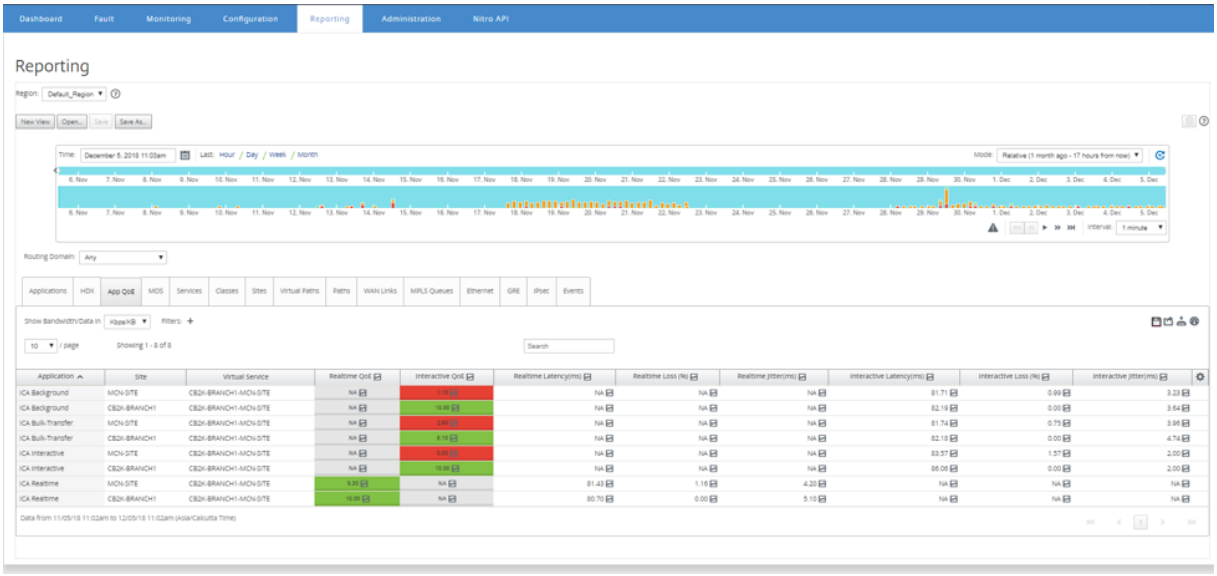
La QoE de la aplicación es una medida de calidad de experiencia para una aplicación. El rango de puntuación QoE de la aplicación es 0-10, donde 10 representa una calidad excelente y 0 representa mala calidad. Para obtener más información, consulte **la sección QoE de la aplicación**.

Para ver el informe QoE de la aplicación:

En Citrix SD-WAN Center, vaya a **Informes > QoE de la aplicación**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período determinado mediante los controles de línea de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Aplicación**: Nombre de aplicación u objeto de aplicación.
- **Sitio**: El nombre del sitio.
- **Servicio virtual**: el servicio de ruta virtual utilizado.
- **QoE en tiempo real**: la puntuación QoE para el tráfico en tiempo real.
- **QoE interactiva**: La puntuación QoE para el tráfico interactivo.
- **Latencia en tiempo real**: latencia en milisegundos para el tráfico en tiempo real.
- **Pérdida en tiempo real**: El porcentaje de pérdida del tráfico en tiempo real.
- **Jitter en tiempo real**: la fluctuación observada en milisegundos para el tráfico en tiempo real.
- **Latencia interactiva**: latencia en milisegundos para el tráfico interactivo.
- **Pérdida interactiva**: El porcentaje de pérdida para el tráfico interactivo.
- **Interactive Jitter**: La fluctuación observada en milisegundos para el tráfico interactivo.

> **Sugerencia**
>
> Para cada valor, puede pasar el cursor del ratón sobre el icono del gráfico para ver un minigráfico o hacer clic para abrir la vista gráfica en otra ventana.

Para obtener más información, consulte Estadísticas.

Informe de Ancho

April 13, 2021

Citrix SD-WAN Center proporciona una vista central de los datos estadísticos de ancho de banda sondeados desde diferentes sitios de la red SD-WAN.

En la configuración de Citrix SD-WAN, el tráfico que fluye a través de las rutas virtuales se clasifica como perteneciente a tipos de clase en tiempo real, interactivo o masivo. Las clases están predefinidas, pero puede personalizar estas clases y aplicarles reglas. Para obtener más información, consulte Personalización de Classe y Reglas por IP Addess y número de puerto.

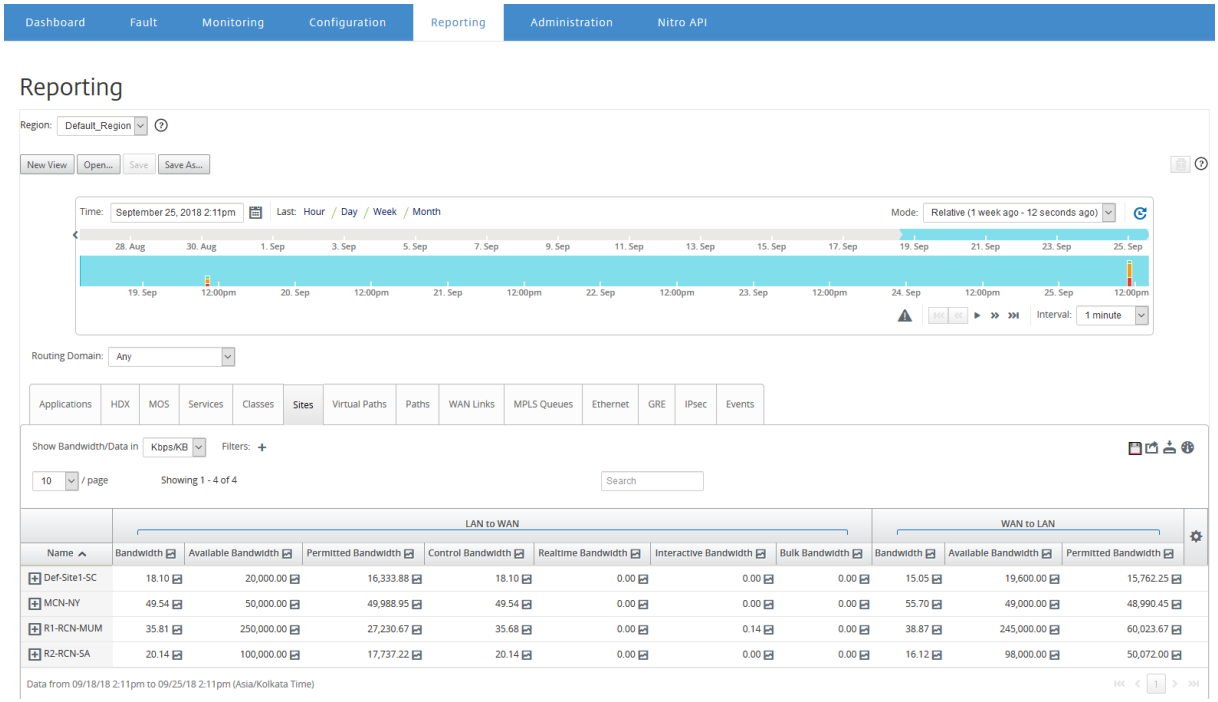
Mediante Citrix SD-WAN Center, puede ver, junto con las estadísticas básicas de ancho de banda, el ancho de banda consumido por las aplicaciones que pertenecen a estos tipos de clase en cada sitio, ruta o nivel de vínculo WAN.

Para ver las estadísticas de anchode banda:

En Citrix SD-WAN Center, vaya a **Informes** > **Sitios**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Ancho de banda**: Ancho de banda total consumido por todos los tipos de paquetes. Ancho de banda = Controla el ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva Por ejemplo, en la captura de pantalla anterior, en el SITE2, Ancho de banda = 1120.99+166.61+117.21+810.78+26.40
- **Ancho de banda disponible**: ancho de banda total asignado a todos los enlaces WAN de un sitio.
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información estadística de redirección, programación y enlace.
- **Ancho de banda permitido**: Ancho de banda disponible para transmitir información.
- Ancho de**banda en tiempo real**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de Citrix SD-WAN. El rendimiento de dichas aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- Ancho de**banda interactivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de Citrix SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase masiva en la configuración de Citrix SD-WAN. Estas aplicaciones implican muy poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).

Informe de clase

April 13, 2021

Los servicios virtuales se pueden asignar a clases de QoS particulares, y se pueden aplicar restricciones de ancho de banda diferentes a diferentes clases. Una clase puede ser uno de los tres tipos básicos:

- **Clases en tiempo real**: Servir flujos de tráfico que exigen un servicio rápido hasta un cierto límite de ancho de banda. Se prefiere una latencia baja sobre el rendimiento agregado.
- **Clases interactivas**: sirve flujos de tráfico sensibles a la pérdida y la latencia. Las clases interactivas tienen menor prioridad que en tiempo real, pero tienen prioridad absoluta sobre el tráfico masivo.
- **Clases masivas**: sirve flujos de tráfico que requieren un alto ancho de banda y son sensibles a las pérdidas. Las clases masivas tienen la prioridad más baja.

La especificación de diferentes requisitos de ancho de banda para diferentes clases permite al programador de rutas virtuales arbitrar solicitudes de ancho de banda competidoras de varias clases del mismo tipo. El programador utiliza el algoritmo Hierarchical Fair Service Curve (HFSC) para lograr la equidad entre las clases.

Para obtener más información sobre cómo personalizar clases, consulte Personalización de clases.

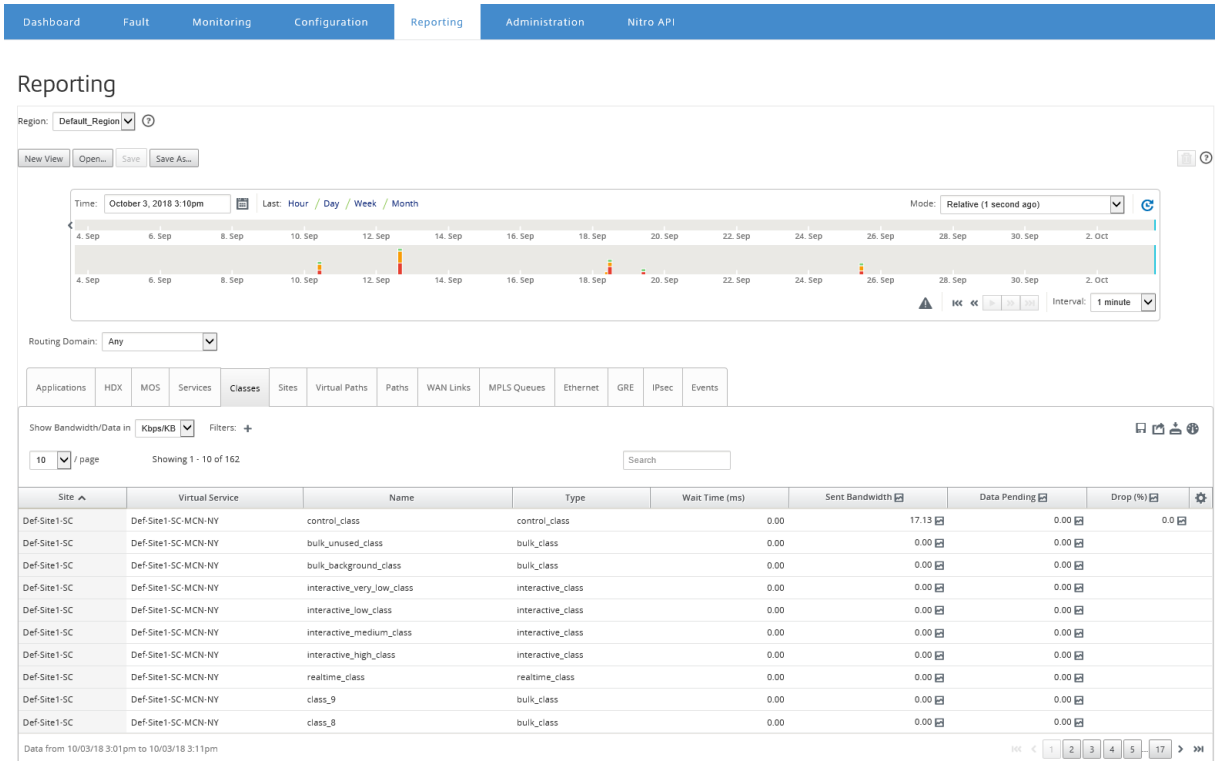
Para ver las estadísticas de clase:

En Citrix SD-WAN Center, vaya a **Informes** > **Clases**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período determinado mediante los controles de línea de tiempo. Para obtener más información, consulte, Controles de cronología.

> **Nota**
>
> Puede ver los datos de clase de los últimos 30 días. Cualquier dato más allá de este período se elimina automáticamente del recopilador SD-WAN Center y de los recopiladores regionales respectivos.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Nombre: Nombre**de la clase
- **Tipo**: Tipo de clase. En tiempo real, interactivo o masivo.
- **Tiempo de espera**: El intervalo de tiempo entre la transmisión de paquetes en milisegundos.
- **Ancho de banda enviado**: Ancho de banda transmitido
- **Datos enviados**: Datos enviados, en Kbps.
- **Paquetes enviados**: Número de paquetes enviados.
- **Datos pendientes**: Datos a enviar, en Kbps.
- **Paquetes Pendientes**: Número de paquetes que se van a enviar.
- **Suelta**: Porcentaje de datos eliminados.
- **Datos eliminados**: Datos eliminados, en Kbps.
- **Paquetes descartados**: Número de paquetes descartados debido a la congestión de la red.
- **Cobertura de datos**: Porcentaje del período seleccionado para el que se dispone de datos.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

Informe de interfaz Ethernet

April 13, 2021

Citrix SD-WAN Center proporciona una vista central de todas las interfaces Ethernet de los diferentes dispositivos Citrix SD-WAN de su red SD-WAN. Esto le ayuda durante la solución de problemas a ver rápidamente si alguno de los puertos está inactivo. También puede ver el ancho de banda transmitido y recibido o los detalles del paquete en cada puerto. También puede ver el número de errores que se produjeron en estas interfaces durante un período de tiempo determinado.

Las interfaces Ethernet se configuran en cada dispositivo Citrix SD-WAN durante la configuración de la red SD-WAN.

Para obtener información acerca de la configuración de grupos de interfaz para sitios de MCN, consulte Configurar MCN.

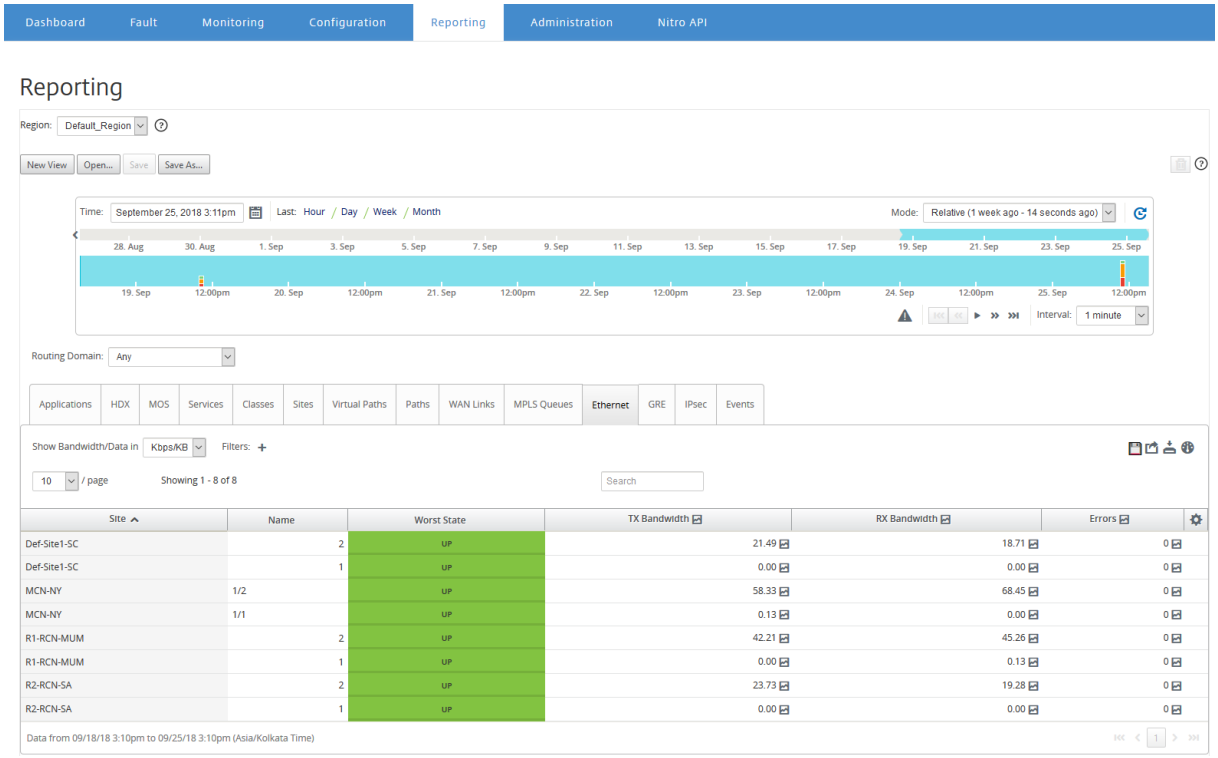
Para obtener información acerca de la configuración de grupos de interfaz para sitios de sucursales, consulte Configurar nodo de rama.

Para ver las estadísticas de la interfaz Ethernet:

En Citrix SD-WAN Center, vaya a **Informes** > **Ethernet**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Nombre**: Nombre de la interfaz Ethernet.
- **Peor estado**: Peor estado observado durante el período de tiempo seleccionado.
- **Ancho de banda TX**: Ancho de banda
- Ancho de**banda RX**: ancho de banda recibido.
- **Paquetes TX**: Número de paquetes transmitidos.
- **Paquetes RX**: Número de paquetes recibidos.
- **Errores**: Número de errores observados durante el período de tiempo seleccionado.
- **Cobertura de datos**: Porcentaje del período de tiempo seleccionado para el que se dispone de datos.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

Informe de eventos

April 13, 2021

Puede ver recuentos de diferentes eventos que ocurren en cada sitio de la red SD-WAN.

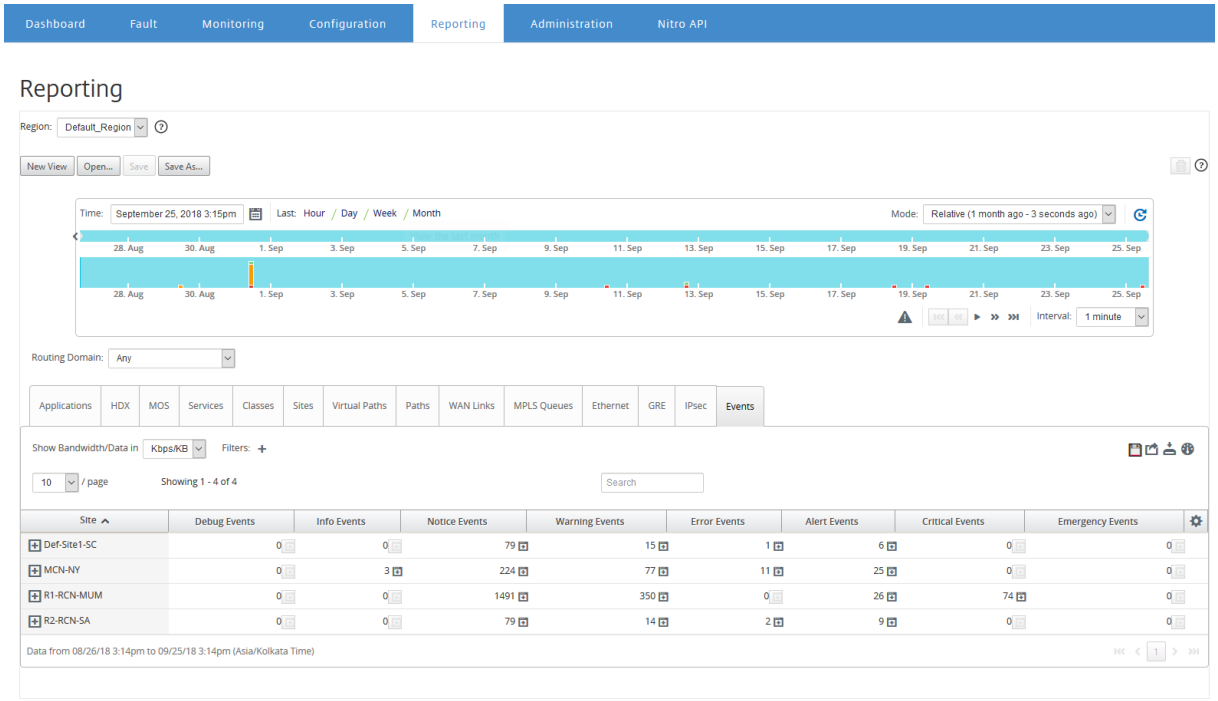
Para obtener más información acerca de los eventos, consulte Eventos.

Para ver estadísticas de eventos:

En Citrix SD-WAN Center, vaya a **Informes** > **Eventos**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Eventos de información**: número de eventos de información que se produjeron durante el período de tiempo seleccionado. Estos son eventos de bajo nivel.
- **Eventos de Aviso**: Número de eventos de aviso que se produjeron durante el período de tiempo seleccionado. Estos son eventos que el administrador debe conocer.
- **Eventos de Advertencia**: Número de eventos de advertencia que se produjeron durante el período de tiempo seleccionado. Estos son eventos que requieren acción en un futuro próximo.
- **Eventos de error**: número de eventos de error ocurridos durante el período de tiempo seleccionado. Estos son eventos que indican algún tipo de error.
- **Eventos de Alerta**: Número de eventos de alerta que se produjeron durante el período de tiempo seleccionado. Estos son eventos que pueden requerir acción.

- **Eventos Críticos**: Número de eventos críticos ocurridos durante el período de tiempo seleccionado. Son acontecimientos que indican una crisis inminente.
- **Eventos de emergencia**: número de eventos de emergencia ocurridos durante el período de tiempo seleccionado. Estos son eventos que indican una crisis inmediata (por ejemplo, falla en la fuente de alimentación, falla del ventilador, umbral del disco duro superado, servicio inhabilitado).
- **Eventos de depuración**: número de eventos de depuración que se produjeron durante el período de tiempo seleccionado. Los eventos de depuración se generan cuando se utilizan las opciones Test Email o Test Syslog en los dispositivos Citrix SD-WAN.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

En la tabla siguiente se enumeran algunos ejemplos de los cambios de estado de los objetos para los que se informa de eventos.

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

Puede configurar Citrix SD-WAN Center para que envíe notificaciones de eventos externos para diferentes tipos de eventos como correo electrónico, capturas SNMP o mensajes syslog. Para obtener más información, consulte Notificaciones de eventos.

Informe del túnel GRE

February 16, 2022

Puede utilizar un mecanismo de túnel para transportar paquetes de un protocolo dentro de otro protocolo. El protocolo que lleva el otro protocolo se denomina protocolo de transporte, y el protocolo transportado se denomina protocolo de pasajeros. La encapsulación de redirección genérica (GRE) es un mecanismo de túnel que utiliza IP como protocolo de transporte y puede transportar muchos protocolos de pasajeros diferentes.

La dirección de origen del túnel y la dirección de destino se utilizan para identificar los dos extremos de los vínculos punto a punto virtuales en el túnel.

Para obtener más información acerca de la configuración de túneles GRE en dispositivos Citrix SD-WAN, consulte Túnel GRE.

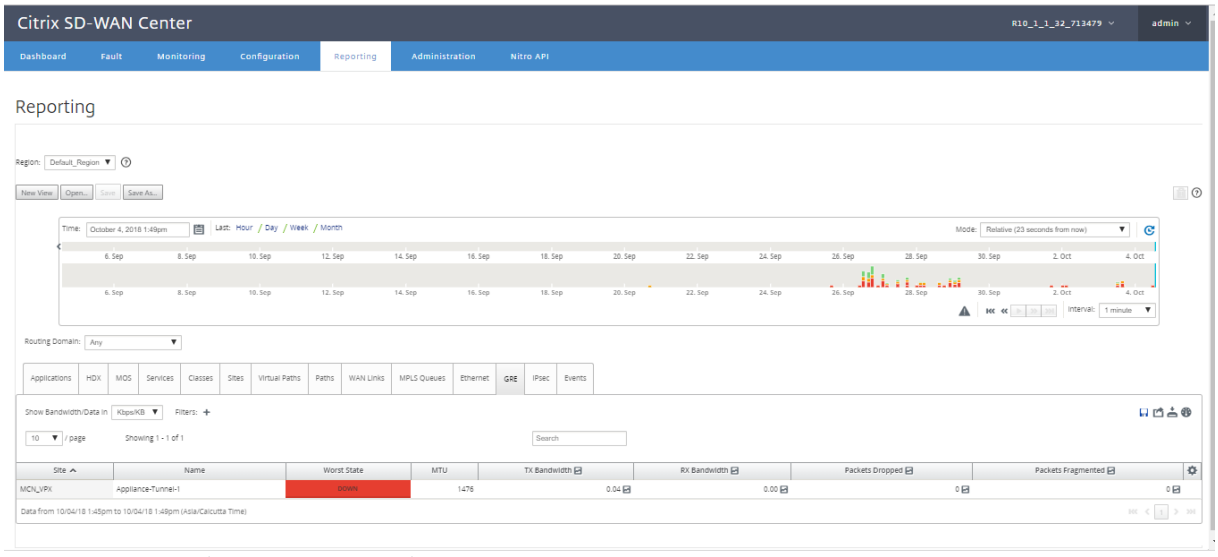
Citrix SD-WAN Center puede mostrarle el estado de todos los túneles GRE configurados en su red Citrix SD-WAN.

Para ver las estadísticas del túnel GRE:

En Citrix SD-WAN Center, vaya a **Informes** > **GRE**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Peor estado**: Peor estado observado durante el período de tiempo seleccionado.
- **MTU**: Unidad de transmisión máxima: el tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico.
- **Ancho de banda TX**: Ancho de banda
- Ancho de**banda RX**: ancho de banda recibido.
- **Paquetes TX**: Número de paquetes transmitidos.
- **Paquetes RX**: Número de paquetes recibidos.
- **Paquetes descartados**: Número de paquetes descartados debido a la congestión de la red.
- **Paquetes Fragmentados**: Número de paquetes fragmentados. Los paquetes se fragmentan para crear paquetes más pequeños que pueden pasar a través de un enlace con una MTU más pequeña que el datagrama original. Los fragmentos son reensamblados por el anfitrión receptor.
- **Cobertura de datos**: Porcentaje del período de tiempo seleccionado para el que se dispone de datos.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

Informe HDX

April 13, 2021

Seleccione uno de los siguientes tipos de informe de la lista desplegable:

- Estadísticas del sitio HDX
- Resumen de HDX (aplicable tanto para el canal de información HDX disponible como para las sesiones no disponibles)
- Sesiones de usuario HDX (aplicable para sesiones disponibles del canal de información HDX)
- Aplicaciones HDX (solo aplicable para sesiones disponibles del canal de información HDX)

Estadísticas del sitio HDX

El informe HDX proporciona datos HDX detallados por sitio.Los datos de cada sitio se muestran en dos vistas.

Vista de resumen

La vista Resumen muestra los siguientes datos de un sitio:

- **Índice QoE** - La calidad de la experiencia (QoE) es un valor numérico entre 0 y 100. Cuanto mayor sea el valor, mejor será la experiencia del usuario.
- **Usuarios**: El número de usuarios activos en el sitio.
- **Flujos TCP** : el número de sesiones HDX activas en el sitio que utilizan el protocolo TCP.
- **Flujos UDP**: Número de sesiones HDX activas en el sitio que utilizan protocolos UDP.
- **Sesiones** : el número total de sesiones HDX activas en el sitio que incluye sesiones de integración a pequeña escala (SSI) e Integración de mediana escala (MSI).

Vista de detalle

Puede hacer clic en un sitio individual para ver detalles sobre todas las variables que afectan a QoE.Cada par de filas muestra los factores QoE para los datos calculados en los lados local y remoto para una ruta virtual determinada.

Las variables de latencia, fluctuación y caída de paquetes que afectan a QoE son los números efectivos que está midiendo el dispositivo Citrix SD-WAN. Por ejemplo, puede haber un porcentaje mayor de caída de paquetes en la red, ya que Citrix SD-WAN corrige las caídas de paquetes a través de su propio protocolo, la pérdida efectiva de paquetes observada por la aplicación sería mucho menor, por lo que mejora la QoE para las aplicaciones HDX.

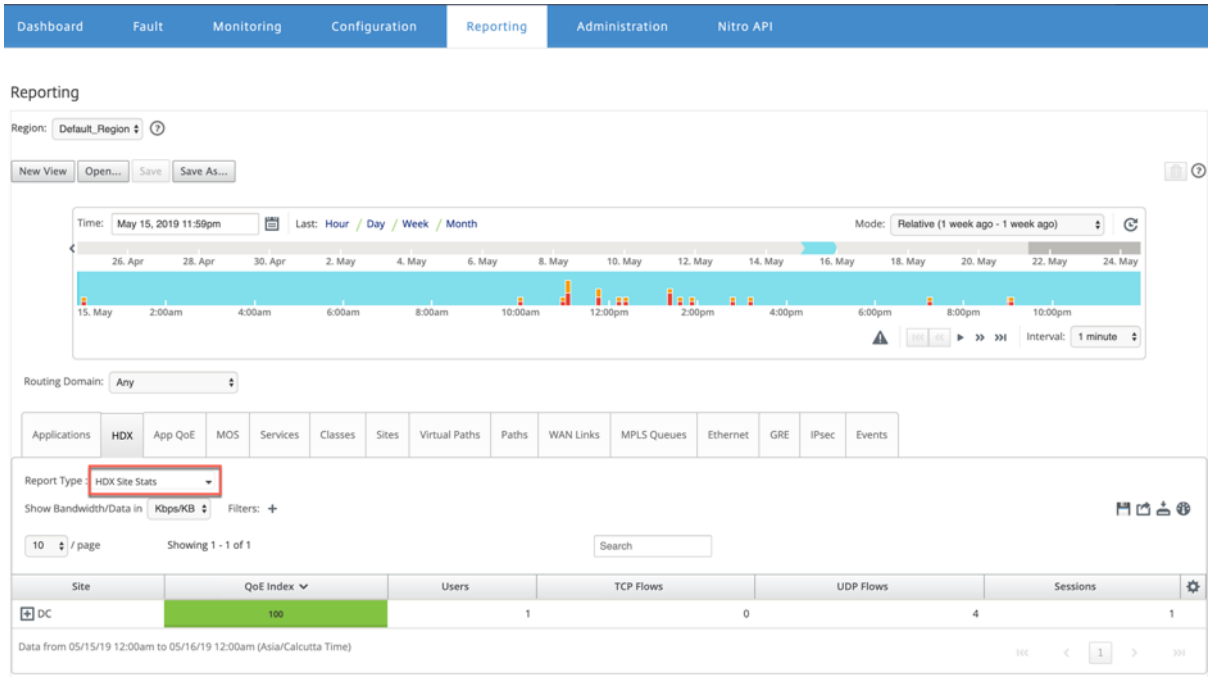
Del mismo modo, la mejora de la latencia mediante la duplicación de paquetes también mejora la QoE para aplicaciones HDX. En otras palabras, Citrix SD-WAN mejora la QoE para el tráfico HDX mejorando los factores que afectan a la QoE. Para obtener más información, consulte HDX QoE.

Para ver informes HDX:

En Citrix SD-WAN Center, vaya a **Informes** > **HDX**y, en el control de línea de tiempo, seleccione un punto.

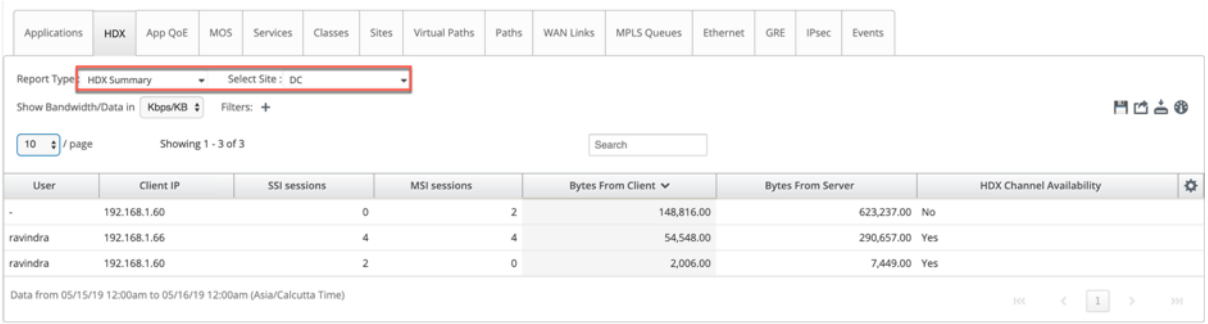
Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Resumen HDX

Seleccione el informe **Resumen de HDX** y el sitio en la lista desplegable. El informe de resumen HDX muestra el informe de cada usuario que ha iniciado sesión durante el período de tiempo seleccionado.



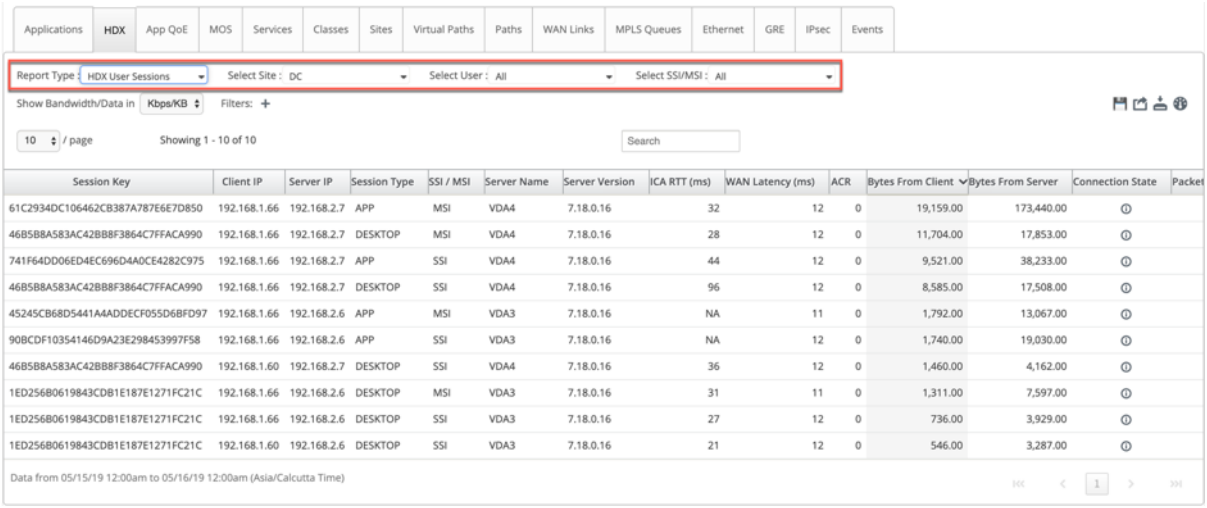
En el informe de resumen HDX, puede ver los siguientes parámetros:

- **Usuario**: Nombre del usuario.

- **IP del cliente**: Dirección IP del cliente.
- Sesiones**SSI: Número de sesiones**de ICA de transmisión única (SSI) activas.
- Sesiones**MSI: Número de sesiones**de ICA (MSI) de múltiples secuencias activas.
- **Bytes del cliente**: Tamaño en bytes del cliente.
- **Bytes del servidor**: Tamaño en bytes desde el servidor.
- **Disponibilidad del canal HDX**: Proporciona el estado de disponibilidad del canal de información HDX como **Sí/No**. Si el canal no está disponible, el nombre de usuario se muestra como un guión (-).

Sesiones de usuario HDX

En el informe Sesiones de usuario HDX, puede ver todos los detalles de las sesiones que utiliza cada usuario. Seleccione el sitio, el usuario y SSI o MSI en la lista desplegable. De forma predeterminada, los campos **Seleccionar usuario** y **Seleccionar SSI/MSI** muestran **TODOS**.



Puede utilizar las opciones **Buscar** o **Filtrar: +** para averiguar la información de sesión requerida según sus requisitos.

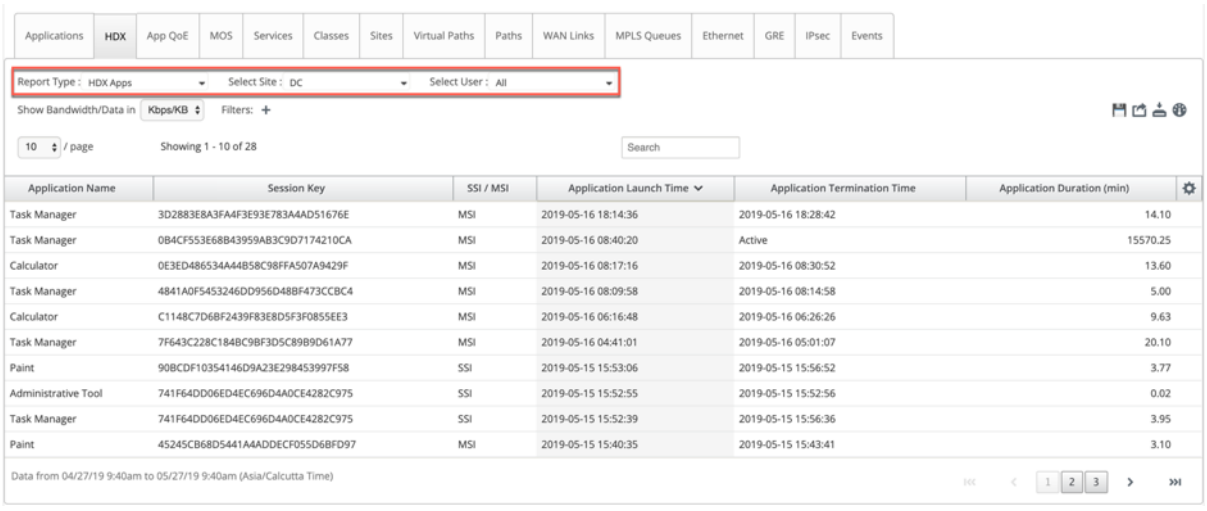
- **Clave**de sesión: La clave de sesión representa la identidad única para una sesión ICA.
- **IP del cliente**: dirección IP del cliente para cada sesión.
- **IP del servidor**: dirección IP del servidor para cada sesión.
- **Tipo de sesión**: Tipo de sesiones (Escritorio, App).
- **SSI/MSI**: muestra si se trata de una sesión SSI o MSI.
- **Nombre del servidor**: muestra el nombre del servidor.
- **Versión del servidor**: muestra la versión del servidor.
- **ICA RTT (ms)**: muestra el tiempo de ida y vuelta (RTT) ICA en milisegundos. Este es un tiempo de ida y vuelta de extremo a extremo entre el cliente y el servidor.

- **Latencia WAN**: Latencia sobre la WAN, es decir, entre las dos SD-WAN sobre la ruta virtual. Esta latencia no incluye latencia de red del lado del cliente o del lado del servidor.
- **ACR**: muestra los recuentos de reconexión automática del cliente.
- **Bytes del cliente**: Tamaño en bytes del cliente.
- **Bytes del servidor**: Tamaño en bytes desde el servidor.
- **Estado de conexión**: Pase el ratón para ver el estado de la conexión.
  - Para MSI, hay cuatro conexiones. Estas conexiones son de nivel L4 (estado TCP/UDP).
  - Para SSI, solo hay una conexión.

- **Packet from Client**: Número de paquetes del cliente.
- **Paquetes del servidor**: Número de paquetes del servidor.

Aplicaciones HDX

Puede ver toda la aplicación utilizada por un usuario específico o por todos los usuarios. Seleccione el **Sitio** y el **Usuario** para ver los detalles de las aplicaciones.



- **Nombre de la aplicación**: proporciona el nombre de la aplicación HDX.
- **Clave de sesión**: proporciona la clave de sesión única que se utiliza para esa aplicación en particular.
- **SSI/MSI**: muestra si se trata de una sesión SSI o MSI.

- **Hora de inicio**de la aplicación: proporciona la hora de inicio de la aplicación con fecha.
- **Hora de terminación**de la aplicación: Proporciona la hora de finalización de la aplicación con fecha. Si una aplicación está activa, se muestra activa en lugar de la hora de finalización.
- **Duración de la aplicación (min)**: proporciona la duración del tiempo de aplicación en minutos.

> **Nota**
>
> - Si se produce algún error no deseado, por ejemplo, si la información de sesión HDX no está disponible en el dispositivo, los informes basados en usuarios HDX no se muestran incluso si **HDX User Reporting** está habilitado. Algunos de los campos como el nombre de usuario, el nombre del servidor, la versión del servidor, ICA RTT en los informes pueden mostrarse como **NA**.
> - El tiempo de finalización de la aplicación en el informe de **HDX Apps** solo se muestra si SD-WAN recibe el **tiempo de finalización de la aplicación** de Xen Application/Xen Desktop Server. De lo contrario, se informa de que algunas de las aplicaciones están activas incluso si están cerradas.

Informe de túnel IPSec

April 13, 2021

Los protocolos de seguridad IP (IPSec) proporcionan servicios de seguridad como el cifrado de datos confidenciales, la autenticación, la protección contra la reproducción y la confidencialidad de los datos para paquetes IP.La carga útil de seguridad encapsulada (ESP) y el encabezado de autenticación (AH) son los dos protocolos de seguridad IPSec utilizados para proporcionar estos servicios de seguridad.

En el modo de túnel IPSec, todo el paquete IP original está protegido por IPSec. El paquete IP original se envuelve y encripta, y se agrega un nuevo encabezado IP antes de transmitir el paquete a través del túnel VPN.

Para obtener más información acerca de la configuración de túneles IPSec en dispositivos Citrix SD-WAN, consulte Terminación del túnel IPSec.

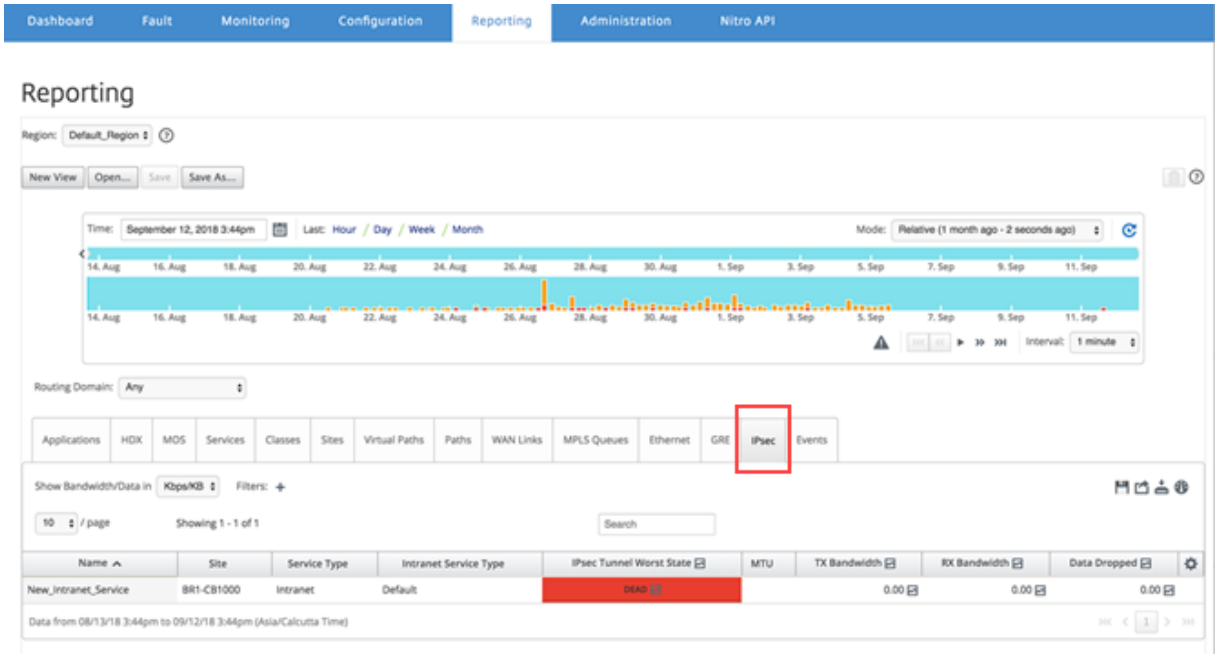
Citrix SD-WAN Center puede mostrarle el estado de todos los túneles IPSec configurados en la red Citrix SD-WAN.

Para ver las estadísticas del túnel IPSec:

En Citrix SD-WAN Center, vaya a **Informes** > **Túneles IPSec**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Nombre: Nombre**de la aplicación.
- **Sitio**: Nombre del sitio.
- **Tipo de Servicio**: Tipo del servicio.
- Tipo de**servicio de intranet: tipo**de servicio de intranet asociado al túnel IPSec. Los siguientes son los tipos de servicios de intranet:
  - Predeterminado
  - WAN virtual de Microsoft Azure
  - Zscaler
  - Citrix SaaS Gateway
- **Peor estado IPSec**: Peor estado observado durante el período de tiempo seleccionado.
- **MTU**: Unidad de transmisión máxima: tamaño del datagrama IP más grande que se puede transferir a través de un enlace específico.
- **Ancho de banda TX**: Ancho de banda
- Ancho de**banda RX**: ancho de banda recibido.
- **Paquetes TX**: Número de paquetes transmitidos.
- **Paquetes RX**: Número de paquetes recibidos.
- **Datos eliminados**: Datos eliminados, en Kbps.

- **Paquetes descartados**: Número de paquetes descartados.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

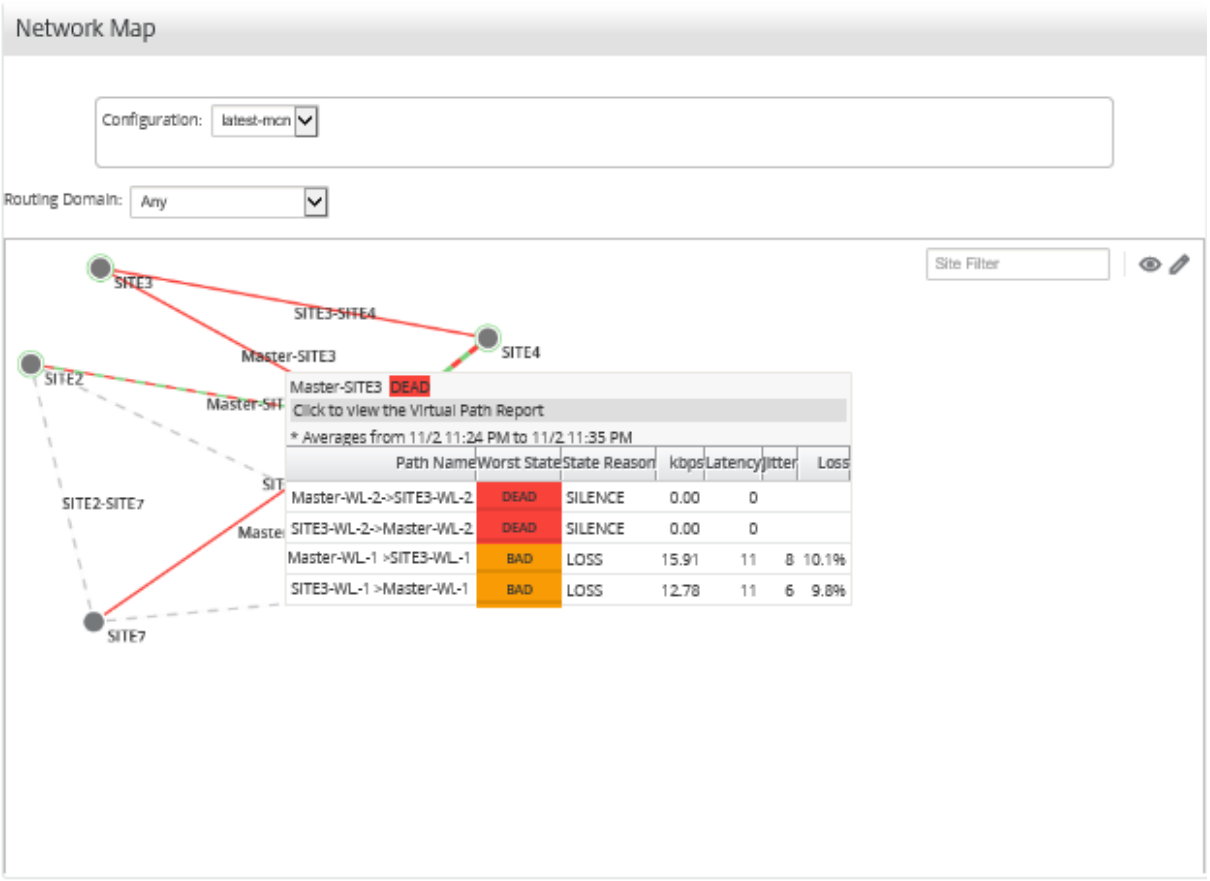
Vincular informe de rendimiento

April 13, 2021

Citrix SD-WAN Center puede mostrar estadísticas de rendimiento a nivel de sitio, servicio, ruta virtual o WAN Link.

Considere una red en la que la organización ABC tiene cuatro sucursales. Se han reportado interrupciones en el SITE3. Es decir, a veces los empleados no pueden ver las páginas de la intranet. Sospecha que es debido al rendimiento de los enlaces subyacentes.

Puede obtener una vista de alto nivel de las estadísticas de vínculos pasando el cursor del mouse sobre la ruta entre un sitio y el centro de datos en el Mapa de red en el panel.



La captura de pantalla anterior muestra que hay dos enlaces WAN (WL-1 y WL-2) entre SITE 3 y el nodo controlador maestro (MCN), y muestra estadísticas de los 10 minutos más recientes.

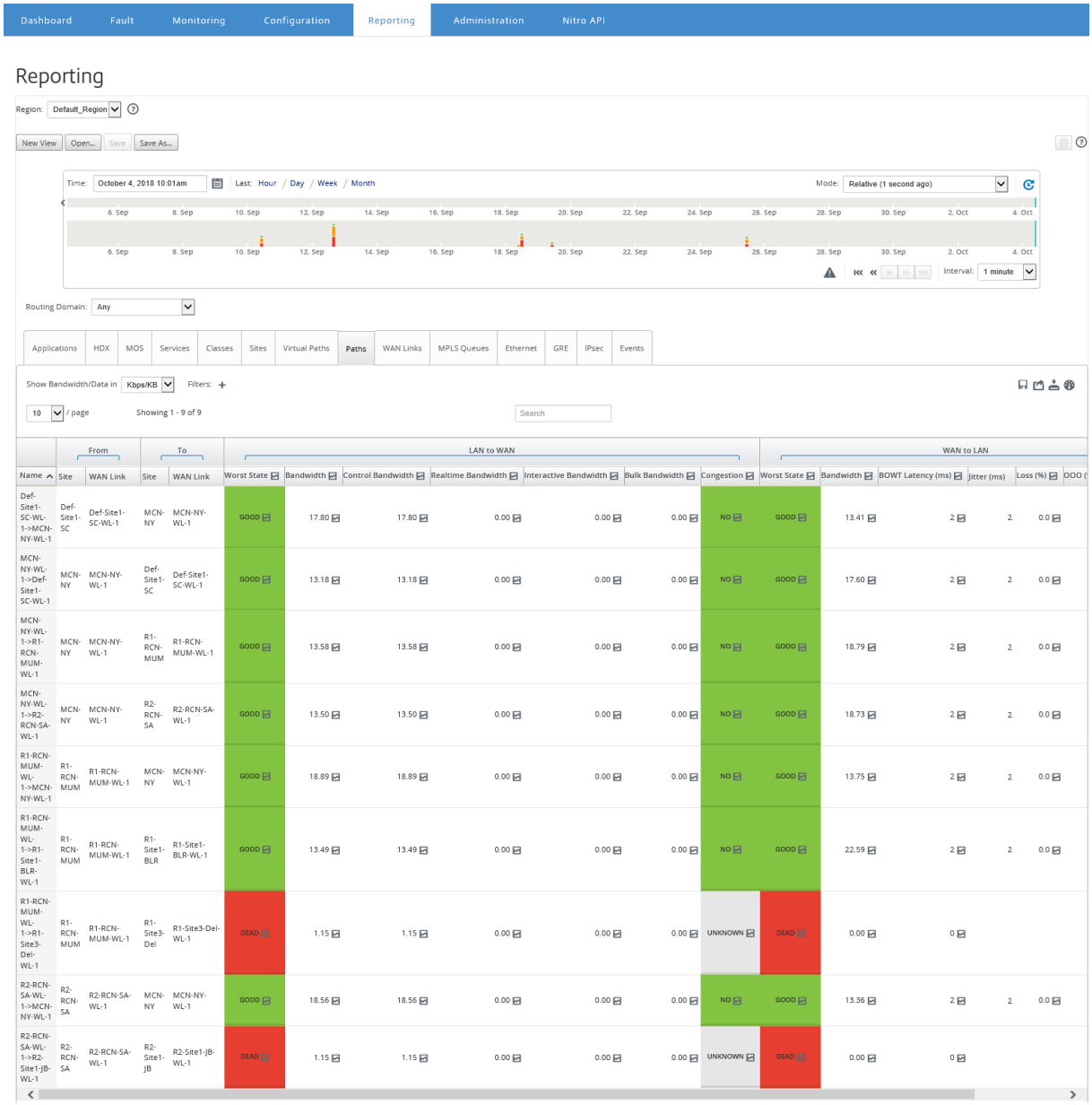
Las rutas virtuales Master-WL2->SITE3-WL2 y SITE3-WL2 ->Master-WL2 no funcionan, y las rutas alternativas Master-WL1->SITE3-WL1 y SITE3-WL1 ->Master-WL1 están en mal estado, perdiendo un porcentaje significativo de los datos transmitidos. Esa es la causa probable del problema de la pérdida de tiempo en el SITE3.

También puede ver las estadísticas de vínculos navegando a **Informes** >**Rutas**.

En el control de línea de tiempo seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Nombre**: El nombre de la ruta.
- **De (Site and WAN Link)**: El sitio de origen y el enlace WAN.
- **A (Sitio y enlace WAN)**: el sitio de destino y el vínculo WAN.
- **LAN a WAN**
  - **Estado de trabajo**:
  - **Ancho de banda**: Ancho de banda total consumido por todos los tipos de paquetes. Ancho de banda = Control de ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva + ancho de banda
  - **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control

que contienen información estadística de redirección, programación y enlace.
  - Ancho de**banda en tiempo real**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de SD-WAN. El rendimiento de dichas aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
  - Ancho de**banda interactivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de SD-WAN. El rendimiento de dichas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
  - Ancho de**banda masivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase masiva en la configuración de SD-WAN. Estas aplicaciones implican muy poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
  - **Congestión**: congestión debido al aumento del tráfico o a un retraso inesperado en el flujo de paquetes en la WAN.

- **WAN a LAN**:
  - **Peor estado**: el peor estado de WAN a LAN observado durante el período de tiempo.
  - **Ancho de banda**
  - **Latencia BOWT (ms)**: Mejor tiempo unidireccional (BOWT) tomado para que un paquete se mueva de un punto a otro, en milisegundos.
  - **Jitter (ms)**: Variación en el retraso de los paquetes recibidos, en milisegundos.
  - **Pérdida (%)**: Porcentaje de paquetes perdidos.
  - **OOO (%)**: Porcentaje de paquetes que no están en el orden correcto o fuera de servicio (OOO).
  - **Congestión**: congestión debido al aumento del tráfico o a un retraso inesperado en el flujo de paquetes en la WAN.

Haga clic en el icono **Configuración** y seleccione los parámetros que quiere ver en los informes.

MOS para aplicaciones

February 16, 2022

La puntuación media de opinión (MOS) proporciona una medida numérica de la calidad de la experiencia que una aplicación ofrece a los usuarios finales. Se utiliza principalmente para aplicaciones VoIP. En Citrix SD-WAN, MOS también se utiliza para evaluar la calidad de las aplicaciones que no son VoIP juzgando el tráfico como si se tratara de una llamada VoIP.

Citrix SD-WAN Center calcula y muestra MOS para el tráfico que pasa a través de la ruta virtual. Active la opción **Estimar MOS** para cada aplicación en cada dispositivo Citrix SD-WAN para mostrar las puntuaciones MOS de estas aplicaciones en Citrix SD-WAN Center.

Para obtener más información sobre cómo habilitar MOS para aplicaciones en Citrix SD-WAN, consulte Agregar grupos de reglas y habilitar MOS.

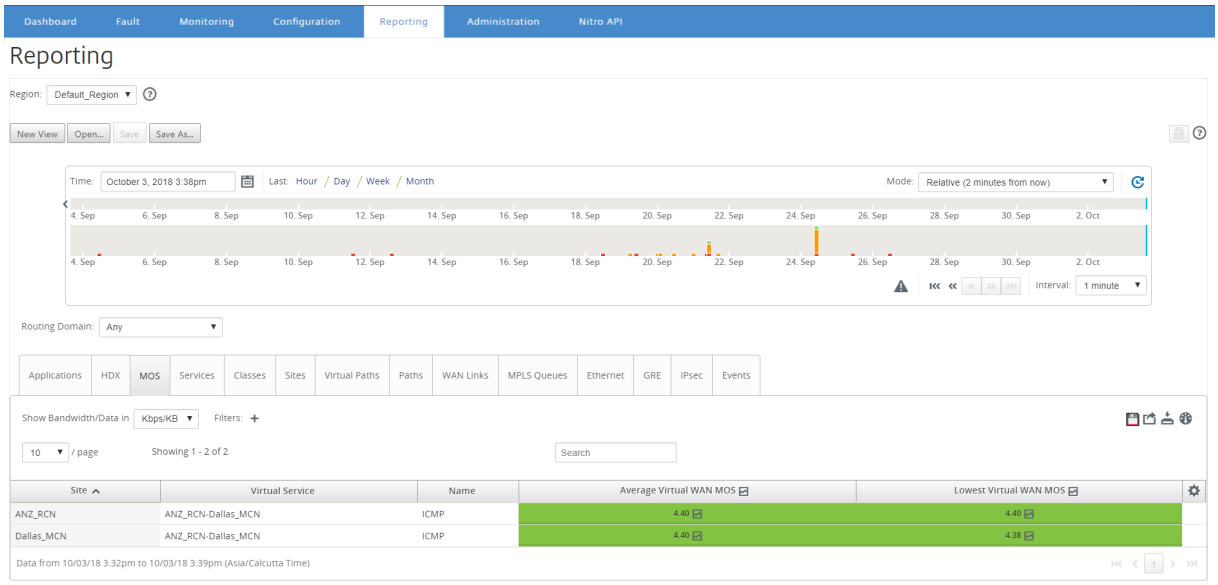
> **Nota**
>
> Active la opción Seguimiento del rendimiento, en Reglas para calcular MOS para aplicaciones y mostrarlo en Citrix SD-WAN Center. Para obtener más información sobre las reglas, consulte Reglas por dirección IP y número de puerto.

Para ver MOS para aplicaciones:

En Citrix SD-WAN Center, vaya a **Informes** > **Aplicaciones**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Nombre**: Nombre de la aplicación.
- **Promedio Virtual WAN MOS**: Puntuación de calidad media calculada durante el período de tiempo seleccionado.
- **Virtual WAN MOS**más bajo: la puntuación de calidad más baja calculada dentro del período de tiempo seleccionado.

Las puntuaciones se clasifican de la siguiente manera:

- 5 —Los usuarios están muy satisfechos.
- 4 —Los usuarios están satisfechos.
- 3 —Los usuarios no están satisfechos.
- 2 —Los usuarios están muy insatisfechos.
- 1 —No recomendado.

Informe de colas MPLS

April 13, 2021

Las colas MPLS proporcionan colas de servicios controladas por etiquetas de punto de código (DSCP) estándar de servicios diferenciados. Las etiquetas controlan la calidad del servicio entre dos sitios en la WAN virtual.

Las colas MPLS permiten a los proveedores de MPLS identificar el tráfico sobre la base de los marcadores DSCP, de modo que el proveedor pueda aplicar la clase de servicio.

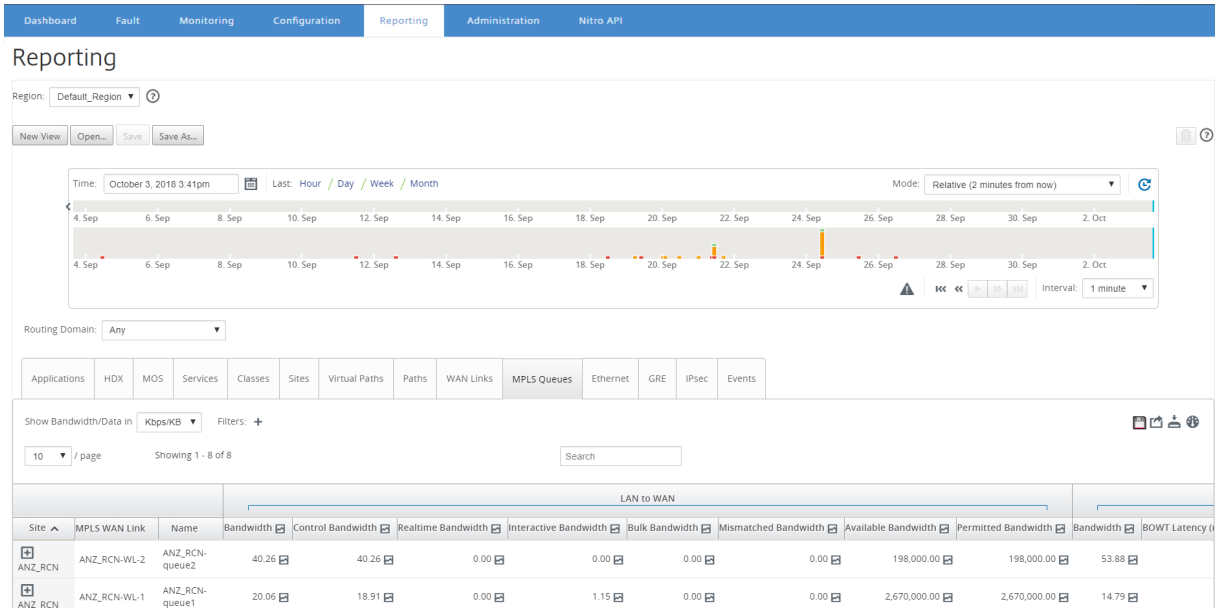
Para obtener más información acerca de la configuración de vínculos WAN MPLS privados en dispositivos Citrix SD-WAN, consulte Colas MPLS.

Para ver las estadísticas de colas MPLS:

En Citrix SD-WAN Center, vaya a **Informes** > **Colas MPLS**y, en el control de línea de tiempo, seleccione un período de tiempo.

Puede seleccionar y ver informes de un período de tiempo determinado mediante los controles de escala de tiempo. Para obtener más información, consulte, Controles de cronología.

También puede crear, guardar y abrir vistas de informe. Para obtener más información, consulte, Administrar vistas.



Puede ver las siguientes métricas:

- **Vínculo WAN**de MPLS: nombre del vínculo WAN de MPLS al que pertenece la cola MPLS.
- **Nombre**: El nombre de la etiqueta DSCP.
- **Ancho de banda**: Ancho de banda total consumido por todos los tipos de paquetes. Ancho de banda = Controla el ancho de banda + ancho de banda en tiempo real + ancho de banda interactiva
- **Ancho de banda de control**: Ancho de banda utilizado para transferir paquetes de control que contienen información estadística de redirección, programación y enlace.
- Ancho de**banda en tiempo real**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase en tiempo real en la configuración de Citrix SD-WAN. El rendimiento de dichas aplicaciones depende en gran medida de la latencia de la red. Un paquete retrasado es peor que un paquete perdido (por ejemplo, VoIP, Skype for Business).
- Ancho de**banda interactivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase interactiva en la configuración de Citrix SD-WAN. El rendimiento de estas aplicaciones depende en gran medida de la latencia de la red y de la pérdida de paquetes (por ejemplo, XenDesktop, XenApp).
- Ancho de**banda masivo**: ancho de banda consumido por las aplicaciones que pertenecen al tipo de clase masiva en la configuración de Citrix SD-WAN. Estas aplicaciones implican muy poca intervención humana y son manejadas principalmente por los propios sistemas (por ejemplo, FTP, operaciones de copia de seguridad).
- Ancho de**banda no coincidente**: Las tramas que no coinciden con las etiquetas DSCP definidas se asignan a una cola predeterminada designada para el ancho de banda no coincidente.
- Ancho de**banda disponible**: la suma del ancho de banda asignado a todos los enlaces WAN de un sitio.

- **Ancho de banda permitido**: Ancho de banda disponible para transmitir información.
- **Latencia BOWT**: El mejor tiempo unidireccional que se tarda un paquete en moverse de un punto a otro, en milisegundos.
- **Fluctuación**: Variación en el retraso de los paquetes recibidos, en milisegundos.
- **Paquetes perdidos**: Número de paquetes perdidos.
- **Pérdida**: Porcentaje de paquetes perdidos.
- **OOO**: Porcentaje de paquetes que no están en el orden correcto.
- **Congestión**: congestión debido al aumento del tráfico o a un retraso inesperado en el flujo de paquetes en la WAN.

> **Nota**
>
> Haga clic en el icono de configuración para seleccionar las métricas que quiere ver.

Administración

April 13, 2021

Puede administrar y mantener su Citrix SD-WAN Center VPX mediante las siguientes opciones administrativas.

Configurar fecha y hora

Certificados HTTPS

Importar configuración de MCN

Administrar la base

Vistas a Mangae

Actualización de software

Controles de cronología

Cuentas de usuario

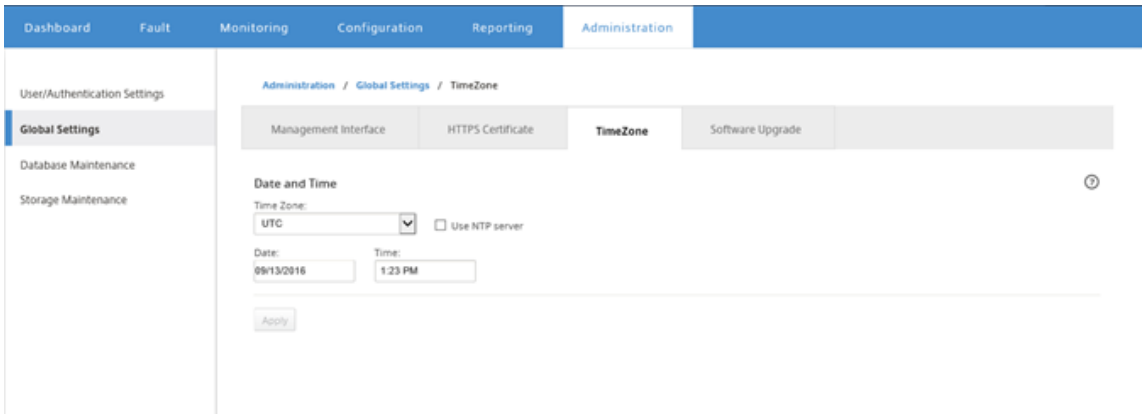
Configurar fecha y hora

April 9, 2021

Puede cambiar la fecha y hora del sistema de administración de Citrix SD-WAN Center manualmente o mediante un servidor NTP.Si selecciona la opción **Usar servidor NTP**, no podrá introducir manualmente una fecha y hora actuales.

Para establecer manualmente la fecha y la hora:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global**y, a continuación, haga clic en **Zona horaria**.



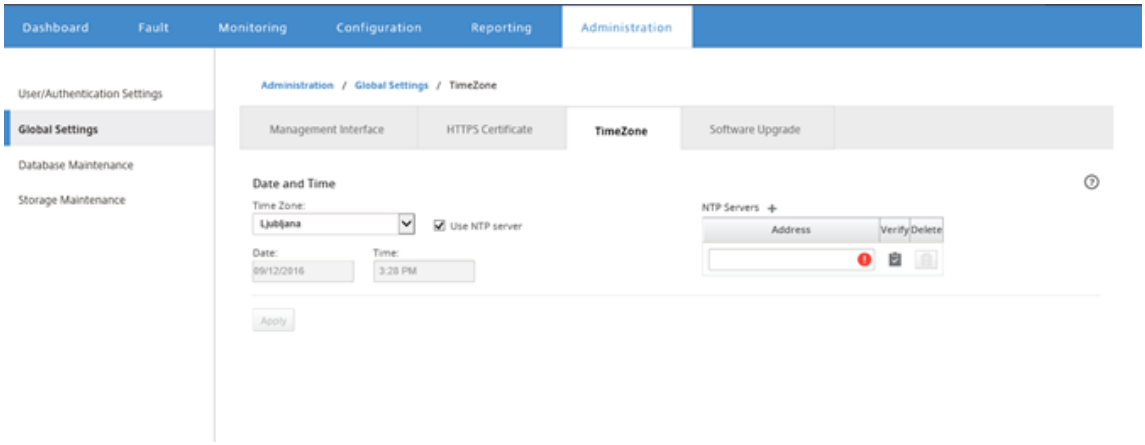
3. En el campo **Zona horaria**, seleccione una **ciudad** en la zona horaria actual. También puede introducir la fecha y hora actuales de la zona horaria.
4. Haga clic en **Aplicar**.

Puede sincronizar el reloj Citrix SD-WAN Center con un servidor NTP externo.

Para establecer la fecha y la hora mediante un servidor NTP:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global** y, a continuación, haga clic en **Zona horaria**.
3. Seleccione **Usar servidor NTP**.

   Esto inhabilita los campos Fecha y Hora y muestra la tabla Servidores NTP.



4. Para agregar un nuevo servidor NTP, haga clic en el icono **+** junto a Servidor NTP.
5. En el campo **Dirección**, introduzca la **dirección IP** del servidor NTP.

   Puede especificar hasta tres servidores NTP, pero debe especificar al menos uno. Estos actúan como servidores NTP de respaldo, si un servidor está inactivo, Citrix SD-WAN Center se sincroniza automáticamente con el otro servidor NTP.

   Si especifica un nombre de dominio para un servidor NTP, también debe configurar un servidor DNS a menos que ya lo haya hecho.Para quitar una entrada de servidor de la tabla, haga clic en el icono **Eliminar** de la columna Eliminar de la entrada.
6. Haga clic en **Verificar** para comprobar que el servidor es accesible antes de aplicar la configuración.
7. Haga clic en **Aplicar**.

Certificados HTTPS

April 9, 2021

El certificado HTTPS es necesario para establecer una conexión HTTPS de administración segura con Citrix SD-WAN Center.

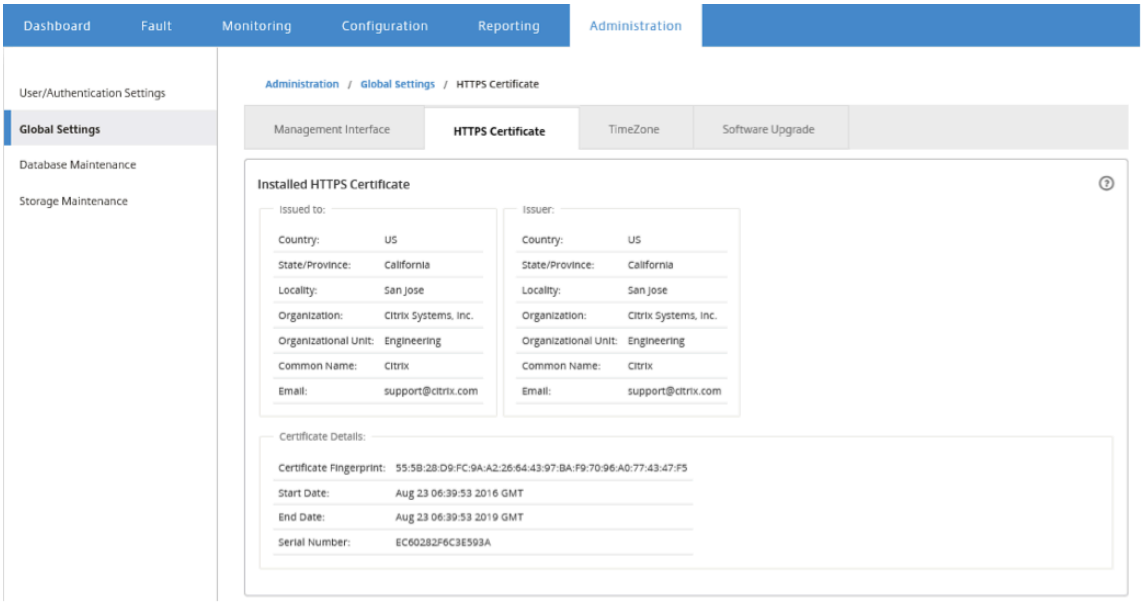
Ver los detalles del certificado HTTPS instalado

Para evaluar el certificado actual, puede mostrar los detalles del certificado.

Para mostrar los detalles del certificado HTTPS ya instalado en Citrix SD-WAN Center:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global** y, a continuación, haga clic en **Certificado HTTPS**.

   Los detalles del certificado HTTPS aparecen en la sección **Certificado HTTPS instalado**.

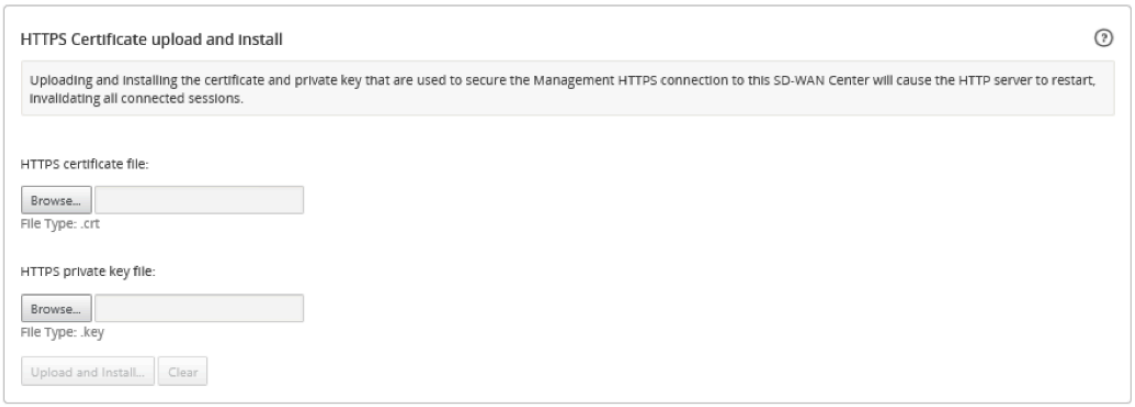


Cargar e instalar un certificado HTTPS

Al instalar un certificado HTTPS, Citrix SD-WAN Center se pone en modo de mantenimiento hasta que se complete la operación. Cuando se completa la operación, se reinicia el servidor web, invalidando todas las sesiones conectadas. Si la conexión con el servidor se pierde cuando se reinicia el servidor web, la pantalla de modo de mantenimiento vuelve a cargar automáticamente la página anterior y muestra un aviso de seguridad del explorador. Si la pantalla no se vuelve a cargar, haga clic en **Continuar** para volver a cargar la página anterior.

Para cargar e instalar el certificado HTTPS:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global** y, a continuación, haga clic en **Certificados HTTPS**.
3. En la sección **Carga e instalación de certificados HTTPS**, en el campo **Archivo de certificado HTTPS**, haga clic en **Examinar** y seleccione un certificado HTTPS.
4. Para el campo **Archivo de clave privada HTTPS**, haga clic en **Examinar** y seleccione un archivo de clave privada HTTPS.
5. Haga clic en **Cargar e instalar**.



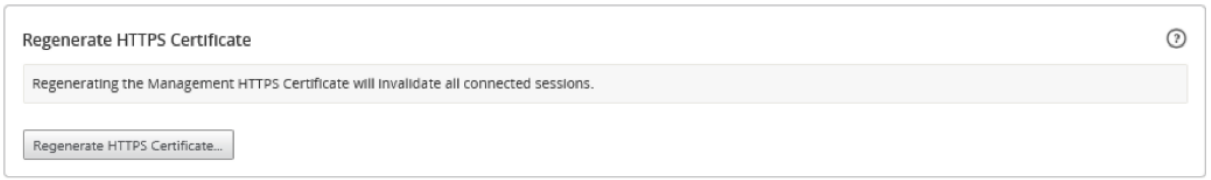
Volver a generar el certificado HTTPS

Puede volver a generar un certificado autofirmado que proteja la conexión HTTPS de administración a Citrix SD-WAN Center. Al regenerar el certificado HTTPS, Citrix SD-WAN Center se encuentra en modo de mantenimiento hasta que se complete la operación. Cuando se completa la operación, se reinicia el servidor web, invalidando todas las sesiones conectadas.

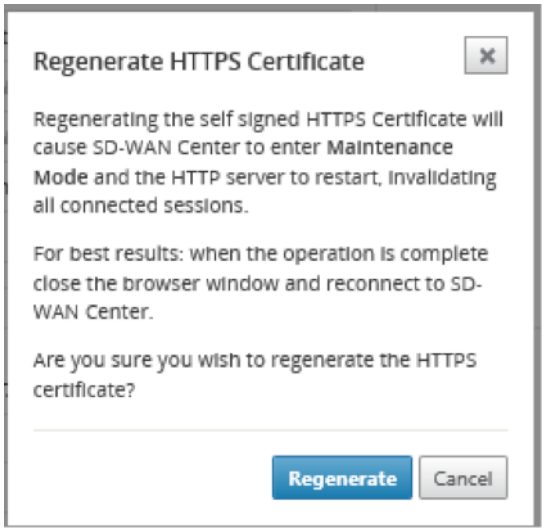
Si la conexión con el servidor se pierde cuando se reinicia el servidor web, la pantalla de modo de mantenimiento vuelve a cargar automáticamente la página anterior y muestra un aviso de seguridad del explorador. Si la pantalla no aparece, haga clic en **Continuar** para volver a cargar la página anterior.

Para regenerar el certificado HTTPS:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global** y, a continuación, haga clic en **Certificados HTTPS**.
3. En la sección **Regenerar certificado HTTPS**, haga clic en **Regenerar certificado HTTPS**.



Aparecerá el mensaje Regenerar certificado HTTPS. Haga clic en **Regenerar**.



Importar configuración de MCN

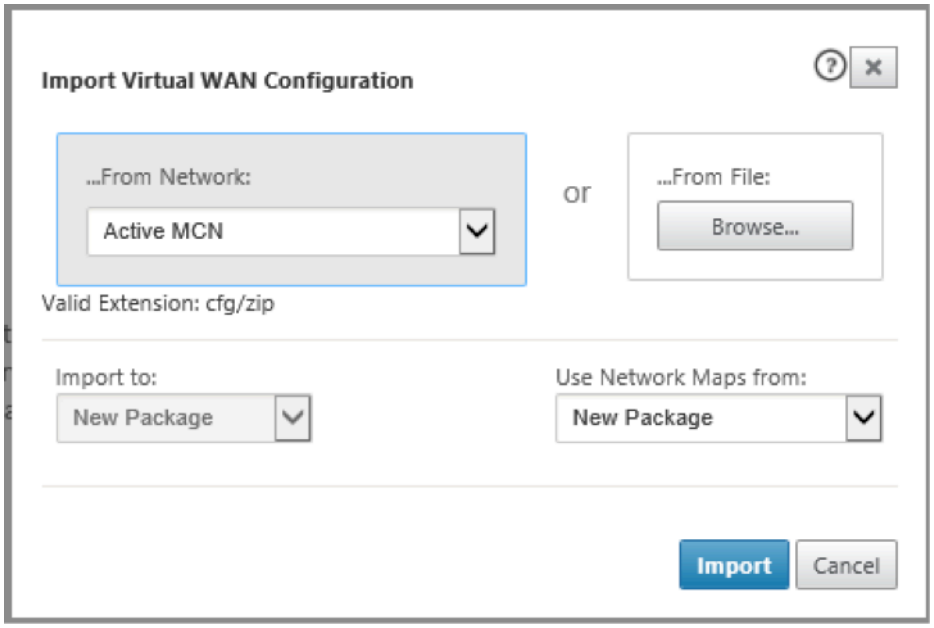
April 13, 2021

Cuando se configura Citrix SD-WAN Center y se establece una conexión entre el nodo de control maestro (MCN) y Citrix SD-WAN Center, puede importar la configuración de MCN a Citrix SD-WAN Center y ver los mapas de red.

La función Importar importa una configuración en una configuración maestra abierta o nueva de Citrix SD-WAN. Si se abre una configuración maestra de Citrix SD-WAN cuando se utiliza la función de importación, ésta y sus mapas se sobrescriben con la nueva configuración maestra de Citrix SD-WAN. Si no hay ninguna configuración maestra de Citrix SD-WAN abierta, se crea un paquete sin título.

Para importar la configuración de MCN a Citrix SD-WAN Center:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Configuración**.
2. Haga clic en **Configuración de red** y, a continuación, haga clic en **Importar**.



3. En el campo **De red**, seleccione una de las siguientes opciones:

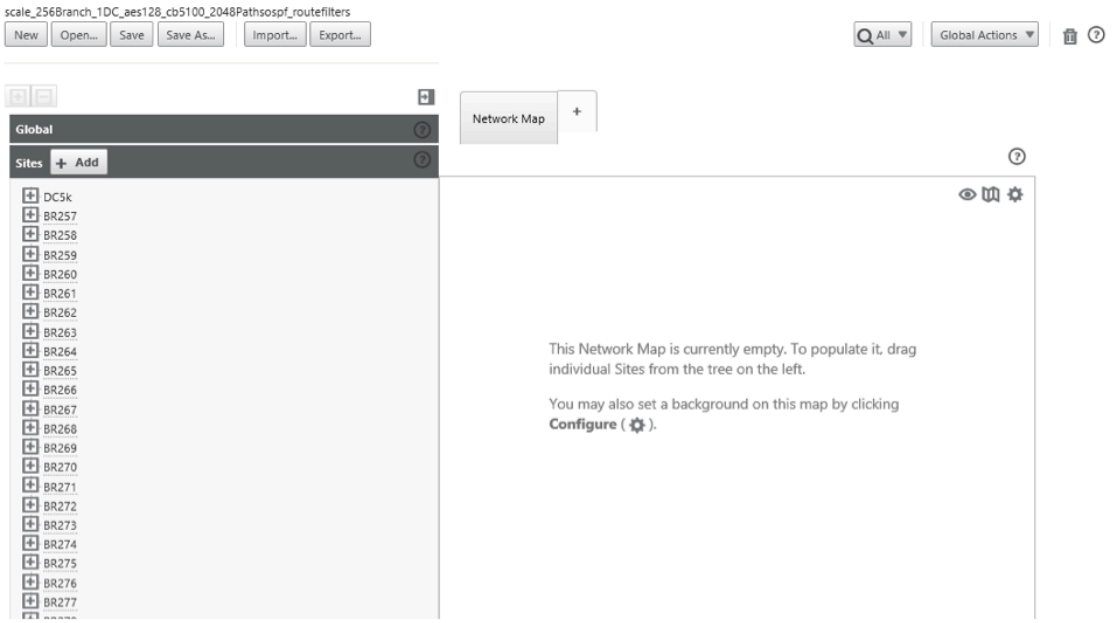
   - **MCN activo**: conéctese al MCN activo y descargue la configuración actual.
   - **Otro**: Conéctese a una dirección IP de un MCN diferente y descargue la configuración actual. Es posible que tenga que instalar el certificado de seguridad desde este Citrix SD-WAN Center en el MCN antes de poder importar la configuración.

   Para obtener más información, consulte, Instalar el certificado Citrix SD-WAN Center.

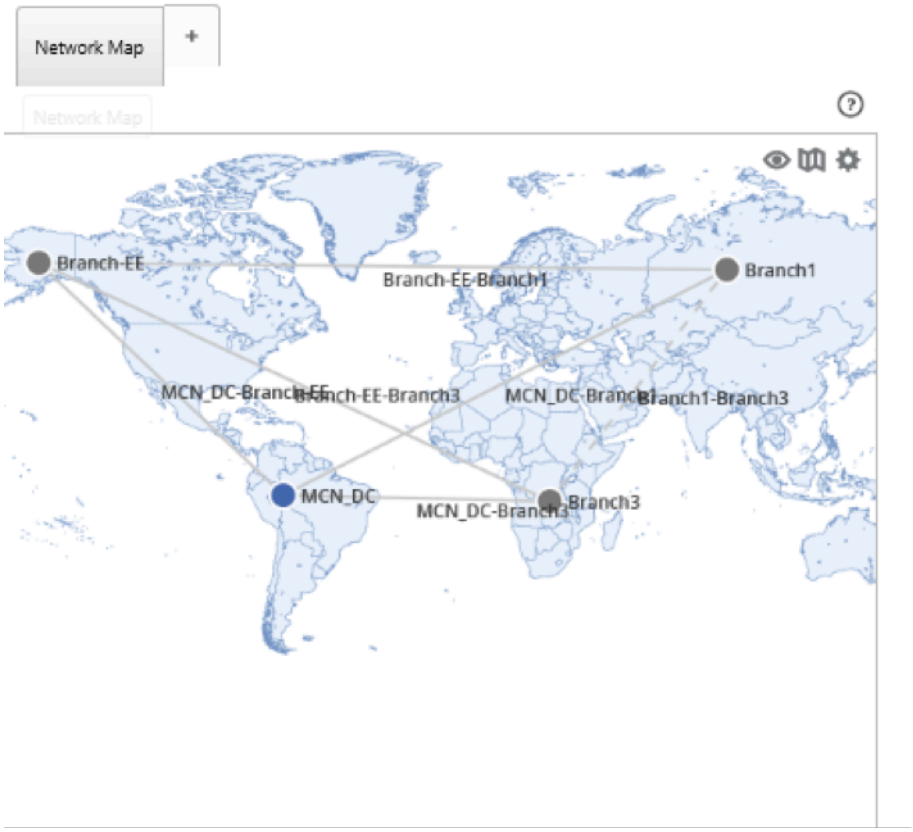
4. Alternativamente, en la sección **Desde archivo**, haga clic en **Examinar** y seleccione una configuración para cargar desde el equipo.
5. En el campo **Importar** a, seleccione **Paquete actual** para importar el contenido del archivo seleccionado en el paquete abierto actual.
6. En el campo **Usar mapas de red de**, seleccione una de las siguientes opciones.

   - **Paquete actual**: conserva el conjunto de mapas de red guardado actualmente después de la importación.
   - **Nuevo paquete**: utilice los mapas de red del paquete importado y descarte el conjunto actual de mapas.
   - **Ambos paquetes**: utilice los mapas importados además de los mapas guardados actualmente.

7. Haga clic en **Importar**. Se importa la configuración.



8. En la sección **Mapa de red**. Haga clic en el icono de configuración y seleccione **Rellenar** automáticamente para agregar y organizar automáticamente cada sitio de la configuración al mapa.



Administrar la base

April 9, 2021

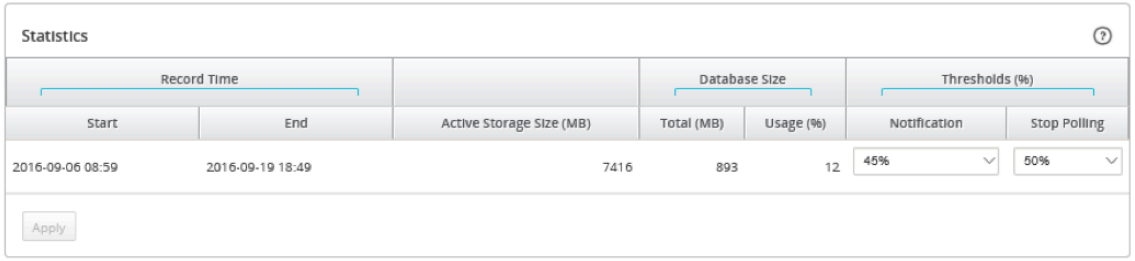
Puede supervisar y administrar la base de datos para asegurarse de que hay suficiente espacio disponible en disco para almacenar los datos de sondeo de todos los dispositivos detectados en la red.

Ver estadísticas de base de datos

La tabla **Estadísticas** muestra las estadísticas de base de datos disponibles e incluye campos de entrada para especificar los umbrales de uso del disco de base de datos para notificaciones y sondeos.

Para ver estadísticas de base de datos:

1. En la interfaz de usuario web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Mantenimiento de base de datos** En la sección **Estadísticas** se muestra la siguiente información.
    - **Hora de Registro:** Muestra la fecha y la marca de hora de los registros más antiguos y más recientes de la base de datos. Esta columna contiene la siguiente información:
        - **Inicio:** muestra la fecha y hora del registro más antiguo de la base de datos.
        - **Fin**: Muestra la fecha y hora del registro más reciente de la base de datos.
    - **Tamaño de almacenamiento activo (MB)**: muestra el espacio en disco del almacenamiento activo actual.
    - **Tamaño de la base de datos (MB)**: muestra el tamaño actual de la base de datos y la información de uso. Esta columna contiene la siguiente información:
        - **Total (MB)**: muestra el tamaño total en MB de la base de datos.
        - **Uso (%)**: muestra el porcentaje de uso del disco de base de datos en el espacio en disco del almacenamiento activo actual.



Para establecer el umbral de notificación y sondeo:

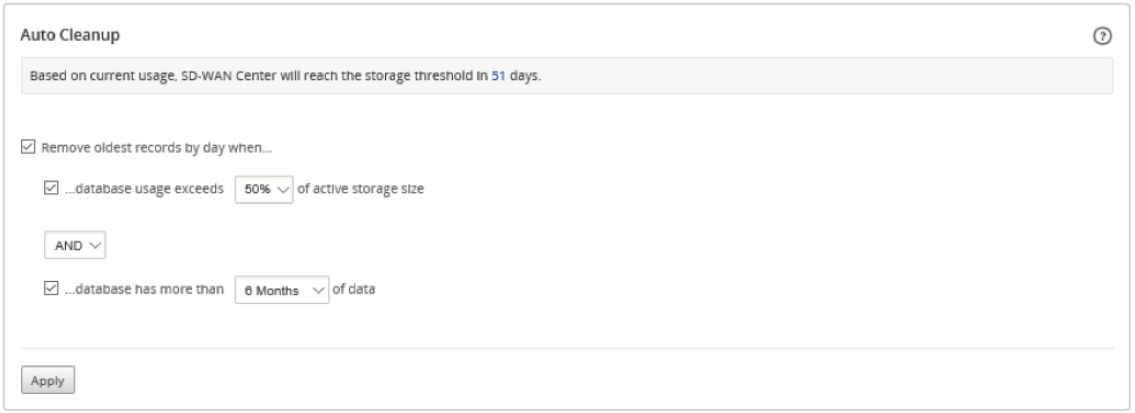
1. En el campo **Notificación**, introduzca el porcentaje del tamaño de la base de datos o del tamaño de almacenamiento activo que se utilizará como umbral para generar una notificación de uso de la base de datos. Se enviará una notificación por correo electrónico cuando el uso de la base de datos supere este umbral.
2. En el campo **Detener sondeo**, introduzca el umbral de uso del disco de base de datos (porcentaje) en el que quiere detener el sondeo de estadísticas. Seleccione un valor del **10%** al **50%** en el menú desplegable. El valor predeterminado es **50%**.
3. Haga clic en **Aplicar**.

Configuración de limpieza automática

Para mantener bajo control el uso del disco de la base de datos, puede especificar umbrales que, cuando se superan, activan la eliminación de registros antiguos de la base de datos.

Para habilitar la limpieza de bases de datos y configurar los umbrales:

1. En la interfaz de usuario web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Mantenimiento de base de datos**
3. En la sección **Limpieza automática**, seleccione **Quitar registros más antiguos por día cuando ...** para habilitar la limpieza de la base de datos.



Cuando está habilitada, la base de datos se comprueba automáticamente a las 2:00 AM todos los días. La comprobación inicia una limpieza de base de datos si se cumplen o superan los umbrales especificados. De forma predeterminada, esto no está habilitado.

Anteriormente, la configuración predeterminada para la limpieza automática de la base de datos de SD-WAN Center era la siguiente:

- Elimine los registros más antiguos por día cuando:
  - …el uso de la base de datos supera el 50% del tamaño de almacenamiento activo

- El operador debe seleccionarse como AND
- …base de datos tiene más de 6 meses de datos

Con la versión 11.1.1 y superior, la configuración predeterminada para la limpieza automática de la base de datos de SD-WAN Center ahora ha cambiado a lo siguiente:

- Elimine los registros más antiguos por día cuando:
  - …el uso de la base de datos supera el 50% del tamaño de almacenamiento activo
  - El operador debe seleccionarse como OR
  - …base de datos tiene más de 1 mes de datos

> **Nota**
>
> El cambio en la configuración no afectará a los sistemas SD-WAN Center ya aprovisionados que se actualizan a la versión 11.1.1. Solo es aplicable a los sistemas SD-WAN Center recién aprovisionados de la versión 11.1.1 o superior.

4. Seleccione**…el uso de la base de datos supera el (%) del tamaño de almacenamiento activo** y, a continuación, seleccione un porcentaje en el menú desplegable para especificar el umbral para una limpieza de la base de datos. Las opciones son del **10%** al **50%** en incrementos del **5%**.
5. Seleccione **AND** u**OR**, un operador en el menú desplegable entre los umbrales «…uso de base de datos excede…» y «…base de datos tiene más de…» para especificar a un operador cómo aplicar esta regla. El valor predeterminado es **OR** desde la versión 11.1.1.
6. **La base de datos Select…tiene más** de [# meses] **meses de datos** y, a continuación, seleccione el número de meses en el menú desplegable para especificar el umbral de intervalo de tiempo para una limpieza de base de datos para la que desea conservar los datos en la base de datos. Las opciones son de **1 mes** a **12 meses** en incrementos de un mes.
7. Haga clic en **Aplicar**.

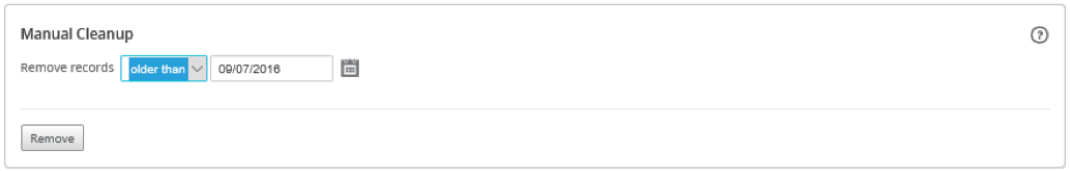
Configuración de limpieza manual

Puede quitar manualmente los registros de estadísticas y eventos de la base de datos, en función de los criterios especificados.

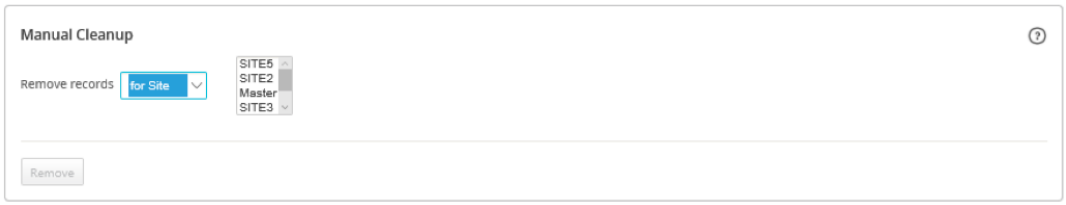
Para realizar una limpieza manual de la base de datos:

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Mantenimiento de base de datos**
3. En **la sección Limpieza manual**, seleccione un filtro en el menú desplegable **Eliminar registros**. Las opciones de filtro son:

- **anterior a:** Quite los registros recopilados antes de una fecha especificada. Al seleccionar este filtro, aparecerá un campo de fecha y un botón de selección de calendario. Haga clic en el botón del calendario para seleccionar una fecha. Se eliminarán todos los registros anteriores a la fecha especificada.



- **para sitio:** elimine los registros recopilados antes de una fecha especificada. Al seleccionar este filtro, aparecerá un campo de fecha y un botón de selección de calendario. Haga clic en el botón del calendario para seleccionar una fecha. Se eliminarán todos los registros anteriores a la fecha especificada.



4. Haga clic en **Quitar**.

Administrar vistas

April 9, 2021

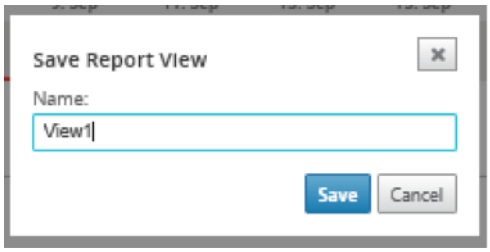
La página Fallo, Informes, Mapa de Red y Estadísticas le permite crear, mostrar, modificar y eliminar las vistas respectivas.

> **Nota**
>
> Las capturas de pantalla utilizadas en el procedimiento pueden variar de la interfaz de usuario real dependiendo del tipo de vista.

Para crear una vista nueva:

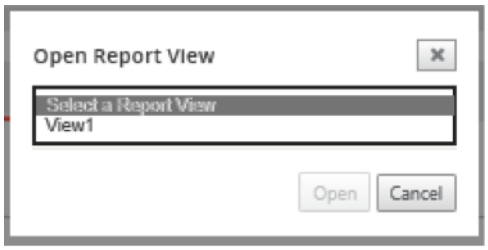
1. Haga clic en **Nueva vista**, esto crea una nueva vista sin nombre y restablece la especificación de tiempo a la hora actual.
2. Cree y aplique filtros o realice los cambios necesarios.
3. Haga clic en **Guardar como**.

4. En el cuadro de diálogo **Guardar vista**, escriba un nombre para la vista.
5. Haga clic en **Guardar**.



Para abrir y modificar una vista existente:

1. Haga clic en **Abrir**.
2. En el cuadro de diálogo **Abrir vista**, seleccione una vista de informe en la lista desplegable.
3. Haga clic en **Abrir**. Se abrirá la vista de eventos.
4. Realice la modificación necesaria según sea necesario.
5. Haga clic en **Guardar**.



Para eliminar una vista, abra la vista y haga clic en el icono de eliminación.

Actualización de software

April 9, 2021

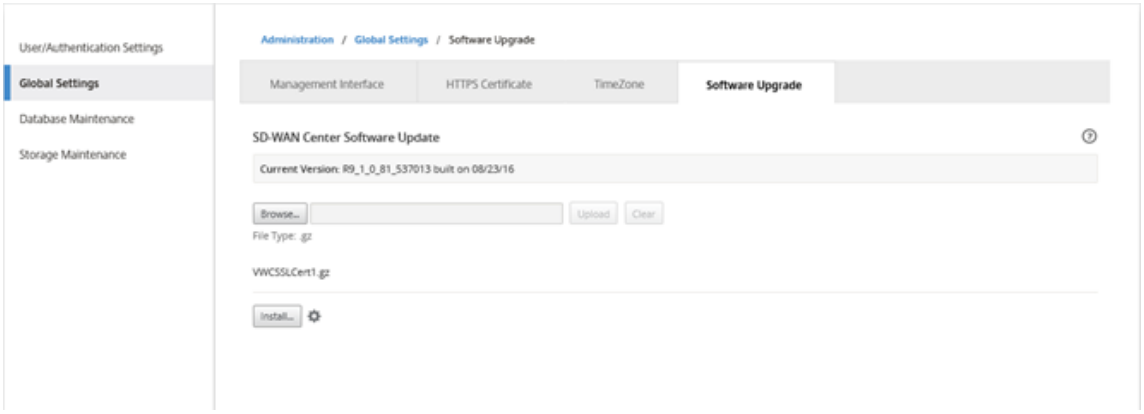
Puede utilizar la opción Actualización de software para actualizar el software Citrix SD-WAN Center a la versión más reciente. El proceso de actualización de software coloca Citrix SD-WAN Center en modo de mantenimiento. Si se requiere una migración de base de datos, este proceso puede tardar varias horas. Durante este tiempo, no se recopilarán datos estadísticos de la WAN virtual y todas las funciones de Citrix SD-WAN Center no estarán disponibles.

> **Importante**
>
> Se recomienda ejecutar la actualización durante las horas de mantenimiento.

> **Nota**
>
> Descargue el paquete de software adecuado de Citrix SD-WAN Center en su equipo local. Puede descargar este paquete desde la Descargas página.

Para cargar e instalar una nueva versión del software Citrix SD-WAN Center

1. En la interfaz web de Citrix SD-WAN Center, haga clic en la ficha **Administración**.
2. Haga clic en **Configuración global** y, a continuación, en **Actualización de software**.



3. Haga clic en **Examinar** para abrir un explorador de archivos y seleccione el paquete de software que quiere cargar.
4. Haga clic en Cargar para **cargar** el paquete de software seleccionado en la máquina virtual Citrix SD-WAN Center actual.
5. Una vez completada la carga, haga clic en **Instalar**.
6. Cuando se le pida que confirme, haga clic en **Instalar**.
7. En el cuadro de diálogo que aparece, active la casilla **Acepto el Contrato de licencia de usuario final** y, a continuación, haga clic en **Instalar**.

Controles de cronología

April 9, 2021

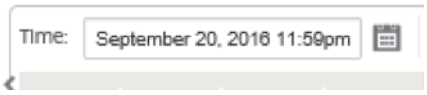
La línea de tiempo situada en la parte superior de la página Fallo, Informes, Mapa de Red y Estadísticas proporciona controles para restringir el período de tiempo de la Vista actual. Puede ver un período de tiempo de hasta 30 días de datos de la base de datos actual.

> **Nota**
>
> En función del período de tiempo seleccionado, puede ver los datos históricos independientemente de la configuración actual de la red de Citrix SD-WAN.

Hora

Puede utilizar los siguientes elementos para especificar un período de tiempo para la vista actual:

- **Hora** : introduzca una fecha y una hora en el campo **Hora** para limitar los resultados del gráfico a una fecha y hora específicas. El formato puede ser cualquiera de los siguientes:
  - ***Mes Día, Año Hora:Minutos*** [**am** / **pm**] Por ejemplo: 7 de septiembre de 2015 2:00pm.
  - ***MM/DD/AAAA HH:MM*** [**am** / **pm**] Por ejemplo: 09/07/2015 8:36am.
  - ***M/D/AA H:MM*** [**am** / **pm**] Por ejemplo: 9/7/15 10:14pm
- **Calendario**: (Icono Calendario) Haga clic en el icono de calendario situado a la derecha del campo Hora y seleccione una fecha para restringir los resultados de la vista a esa fecha.



- **Línea de tiempo**: Haga clic y arrastre a otro punto de una línea de tiempo para seleccionar un marco de tiempo de al menos 30 minutos.

- **Último: Hora/Día/Semana/Mes**. Haga clic en una opción (**Hora**, **Día**, **Semana** o **Mes**) para restringir los resultados de la vista a ese período de tiempo.

Modo

El modo Línea de tiempo determina cómo interpreta la escala de tiempo las selecciones de marco temporal y cómo se reflejan las actualizaciones automáticas en la vista actual y en el panel. Hay dos opciones de modo, **Relativo** (*marco de tiempo seleccionado*) y **Absoluto** (*marco de tiempo seleccionado*), donde el marco de tiempo seleccionado es el período de tiempo especificado en el campo **Tiempo**.

Para cambiar el modo Línea de tiempo, seleccione **Relativa** o **Absoluta** en el menú desplegable **Modo** situado en la esquina superior derecha de la Línea de tiempo.

Modo relativo

Si selecciona Modo **relativo**, la Línea de tiempo tratará el período de **tiempo especificado para Tiempo** como un tiempo relativo al ahora. Si guarda la vista y la abre más tarde, la información representada en la vista será relativa a la hora en que se abrió la vista. Si ha habilitado las actualizaciones automáticas y se detecta una actualización de estadísticas, la vista se actualiza en relación con la última hora registrada en la base de datos.

El período de tiempo especificado actualmente se muestra entre paréntesis como parte de la opción de menú **Relativo**. Por ejemplo, si seleccionó **Último: Día** como marco de tiempo, la opción **Relativo** aparece como Relativo (hace 1 día - 1 minuto a partir de ahora).

Modo absoluto

Si selecciona el modo **Absoluto**, la Línea de tiempo tratará el período de tiempo especificado para **Tiempo**: como puntos absolutos (estáticos) en el tiempo. La vista siempre representará la hora seleccionada, incluso si guarda la vista y la abre posteriormente, o si habilita las actualizaciones automáticas. El período de tiempo especificado actualmente se muestra entre paréntesis como parte de la opción de menú **Absoluto**, mediante el siguiente formato:

Absoluto (*start_date start_time-fin_date fin_time*)

Por ejemplo, si seleccionó **Último: Día** como marco de tiempo y la fecha y hora actuales son 9/7 4:43 PM, la opción **Absoluto** aparece como **Absoluto (9/6 4:43 PM - 9/7 4:43 PM)**.

Cuentas de usuario

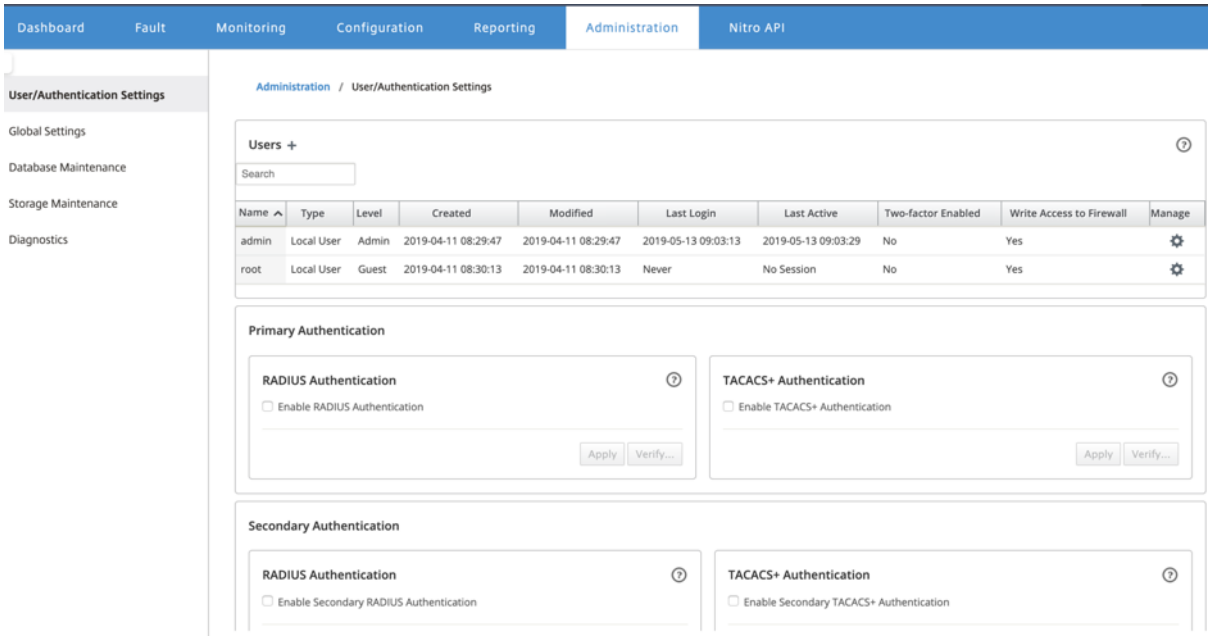
April 13, 2021

Puede ver una lista de todas las cuentas de usuario locales y remotas que han iniciado sesión en la máquina virtual Citrix SD-WAN Center al menos una vez. Las cuentas de usuario remoto se autentican a través de los servidores de autenticación RADIUS o TACACS+. También puede agregar una nueva cuenta de usuario local a Citrix SD-WAN Center.

> **Nota**
>
> Si una cuenta de usuario está disponible en un servidor de autenticación remoto pero nunca se usa para iniciar sesión en Citrix SD-WAN Center, no se muestra en la lista **Usuarios**.

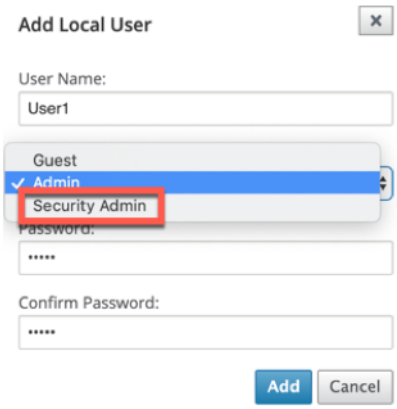
Para ver cuentas de usuario en la interfaz web de SD-WAN Center, vaya a **Administración > Configuración de usuario/autenticación**.

Aparecerá una lista de cuentas de usuario en la sección **Usuarios**.



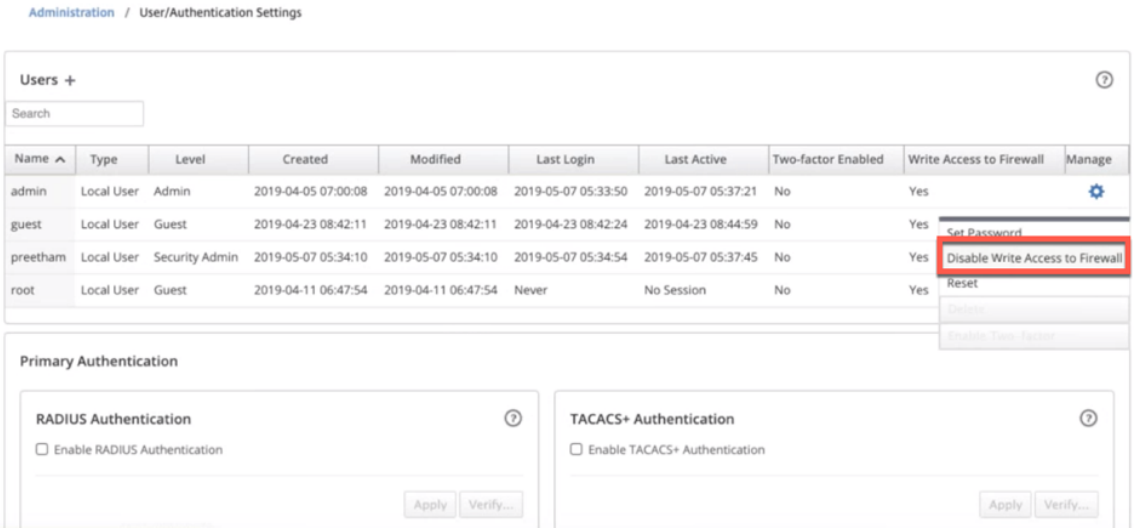
Se muestra la siguiente información:

- **Nombre:** El nombre de usuario.
- **Tipo**: El tipo de cuenta de usuario, puede ser uno de los siguientes:
  - **Local: cuentas de**usuario creadas y administradas localmente mediante la interfaz SD-WAN Center.
  - **RADIUS**: cuentas de usuario remotas autenticadas por el servidor RADIUS.
  - **TACACS+**: cuentas de usuario remotas autenticadas por el servidor TACACS+.
- **Nivel:** Los siguientes son tres niveles de privilegio de cuenta:
  - **Admin**: La cuenta de administrador tiene privilegios administrativos. Tiene acceso de lectura-escritura a todas las secciones.
  - **Invitado**: Cuenta de invitado es una cuenta de solo lectura con acceso a la página **Panel**, **Informes**y **Supervisión**.
  - Administrador de**seguridad**: un **administrador de seguridad**tiene acceso de lectura y escritura solo para el firewall y la configuración relacionada con la seguridad en el **Editor de configuración**, mientras que tiene acceso de solo lectura a las secciones restantes.

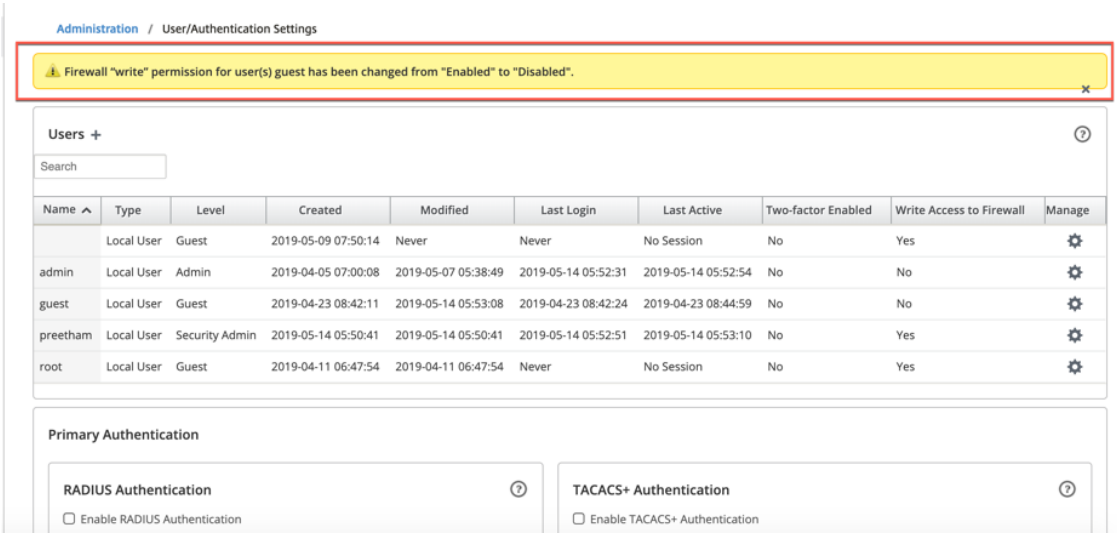


NOTA

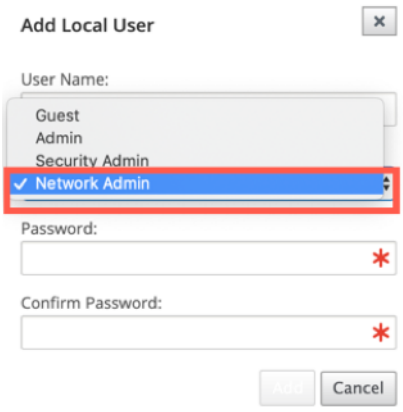
* Solo el administrador y el administrador de seguridad pueden cambiar o modificar la configuración de la función de seguridad.
* El administrador de seguridad puede habilitar o inhabilitar el acceso de escritura al firewall para todas las cuentas de usuario excepto el superadministrador.



Aparece una barra de notificaciones a todos los usuarios después de que el administrador de seguridad cambie el permiso de escritura del firewall para un usuario específico. Esta notificación se muestra por usuario y, por lo tanto, cada usuario que haya iniciado sesión debe reconocer la advertencia para que se elimine.



- Administrador de**red**: un **administrador de red** tiene permisos de lectura y escritura para todas las secciones y puede aprovisionar completamente una rama, excepto la configuración relacionada con el firewall y la seguridad en el Editor de configuración.



El nodo de firewall alojado no está disponible para el administrador de red. En este caso, el administrador de red debe importar una nueva configuración. Tanto la configuración relacionada con la red como la seguridad son mantenidas por el superadministrador (Admin).

El administrador de red y el administrador de seguridad pueden realizar cambios en la configuración y también implementarla en la red.

> **NOTA**
>
> El administrador de red y el administrador de seguridad no pueden agregar o eliminar cuentas de usuario. Solo pueden modificar sus propias contraseñas de cuenta.

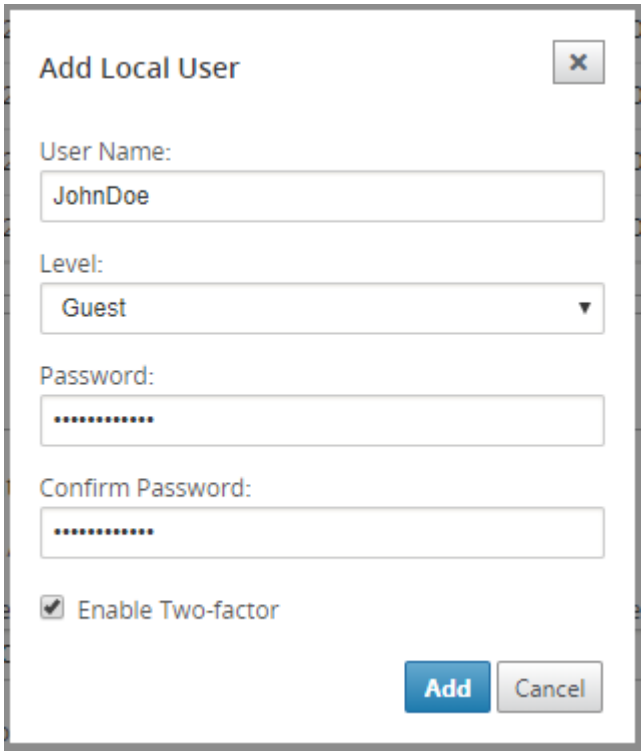
- **Creado**: para las cuentas de usuario locales, la fecha en que se creó la cuenta de usuario. Para una cuenta de usuario remota, la fecha de la primera sesión de inicio de sesión.
- **Modificado**: para las cuentas de usuario locales, la fecha en que se cambió la contraseña por última vez. Para usuarios remotos, la fecha de la primera sesión de inicio de sesión.

- **Último inicio de sesión**: la fecha en la que el usuario inició sesión correctamente por última vez. Una información sobre herramientas muestra la dirección IP del dispositivo utilizado para iniciar sesión.
- **Último activo**: la fecha en que se realizó la última solicitud al servidor. Una información sobre herramientas muestra la dirección IP del dispositivo utilizado para iniciar sesión.
- **Administrar:** Haga clic en el icono de engranaje para ver un menú que contiene las siguientes opciones:
  - **Establecer contraseña**: cambie la contraseña de la cuenta de usuario local. La contraseña raíz actual es necesaria para cambiar la contraseña raíz. No se pueden cambiar las contraseñas de las cuentas de usuario remotas.
  - **Restablecer**: elimina los espacios de trabajo y las preferencias de esta cuenta de usuario.
  - **Eliminar**: elimine la cuenta de usuario local, los espacios de trabajo y las preferencias de SD-WAN Center. No puede eliminar cuentas remotas y administrativas.
  - **Activado de dos factores:** Habilite la autenticación de dos factores para la cuenta de usuario local y remota. Para obtener más información, consulte autenticación de dos factores.
- **Acceso de escritura al firewall**: muestra que el acceso de escritura al firewall está habilitado o inhabilitado.

Para agregar una nueva cuenta de usuario local al Citrix SD-WAN Center:

> **Nota**
>
> Las cuentas de usuario creadas localmente en Citrix SD-WAN Center no tienen el privilegio de modificar y exportar el paquete de configuración de red al MCN.

1. Haga clic en el icono Agregar + situado junto a **Usuarios**. Aparecerá**el cuadro de diálogo Agregar usuario local**.



2. Introduzca valores para los siguientes parámetros:

   - **Nombre de usuario**: nombre de usuario de la cuenta de usuario local.
   - **Nivel**: Privilegio de cuenta. Una cuenta de usuario invitado es una cuenta de solo lectura limitada a la visualización de paneles, informes y estadísticas. La cuenta de usuario invitado no tiene el privilegio de modificar y exportar el paquete de configuración de red al MCN.
   - **Contraseña**: Contraseña de la cuenta de usuario.
   - **Confirmar contraseña**: vuelva a introducir la contraseña para la confirmación.

3. Seleccione **Habilitar dos factores** para habilitar la autenticación de dos factores para la cuenta de usuario local.

   > **Nota**
   >
   > La opción **Habilitar dos factores** aparece solo cuando se configura el servidor de autenticación secundario.
   >
   > Configure un servidor de autenticación secundario, ya sea RADIUS o TACAS+. Asegúrese de que la cuenta de usuario está configurada en el servidor de autenticación secundario. Para obtener más información, consulte Autentificación secundaria.

4. Haga clic en **Agregar**.Se crea la nueva cuenta de usuario y la información de la cuenta se agrega a la tabla **Usuarios**.

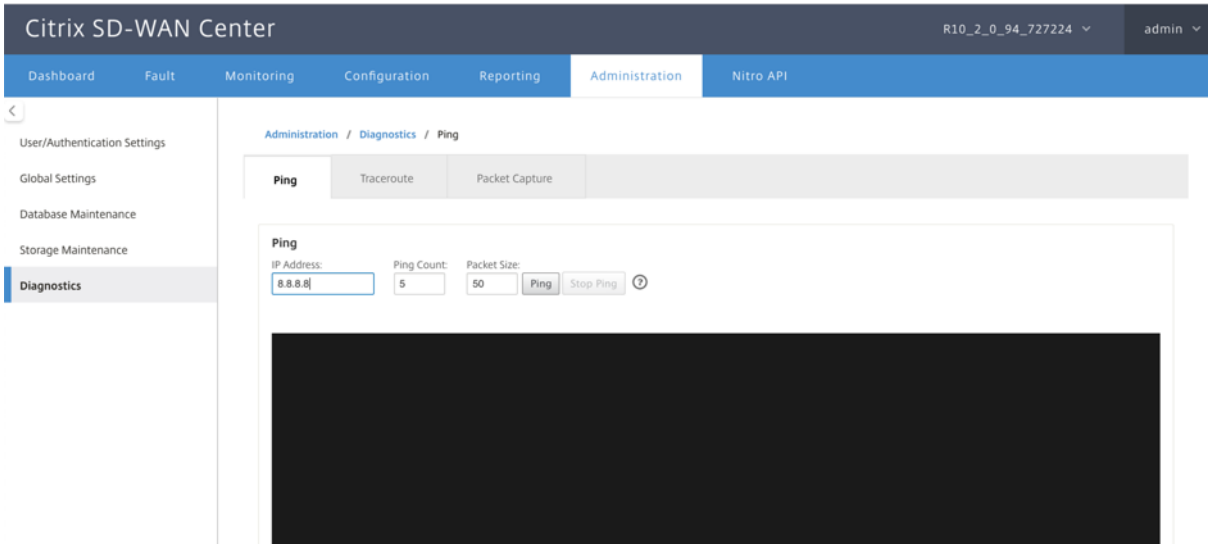
> **Nota**
>
> Citrix SD-WAN Center puede tener hasta 600 usuarios locales.

Diagnóstico

April 13, 2021

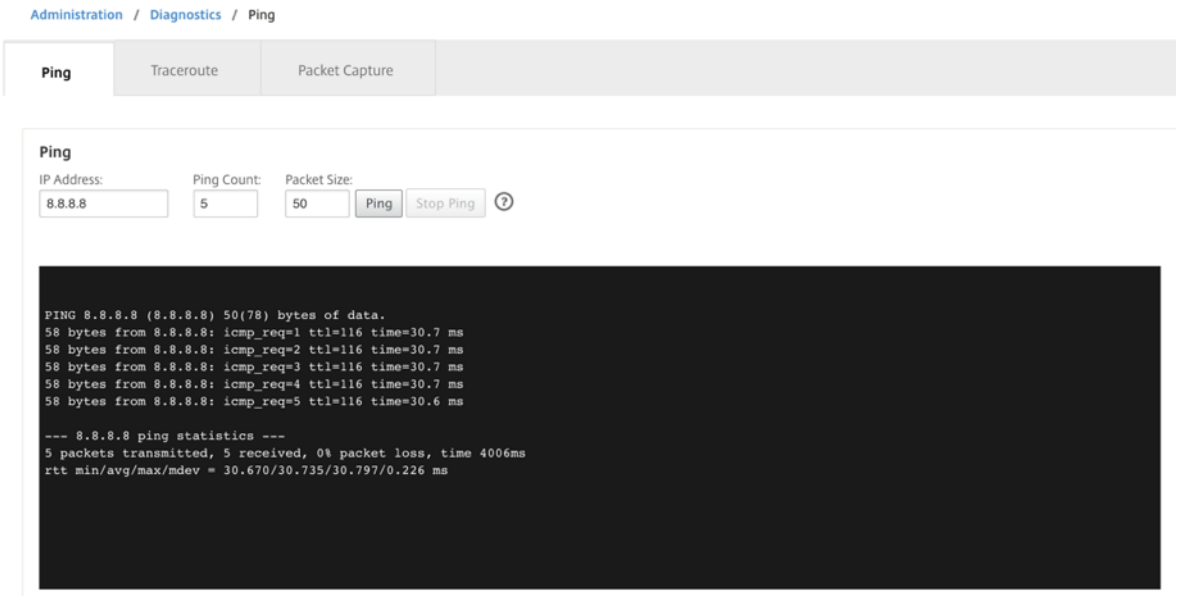
Las utilidades de**diagnóstico de Citrix SD-WAN Center** ofrecen funciones de Ping, Traceroute y Packet Capture para probar e investigar problemas de conectividad en el dispositivo Citrix SD-WAN Center. Las opciones de diagnóstico en el **panel de control de Citrix SD-WAN Center controlan la recopilación de datos**.

Para utilizar la herramienta Diagnósticos, vaya a **Administración > Diagnósticos**.



Ping

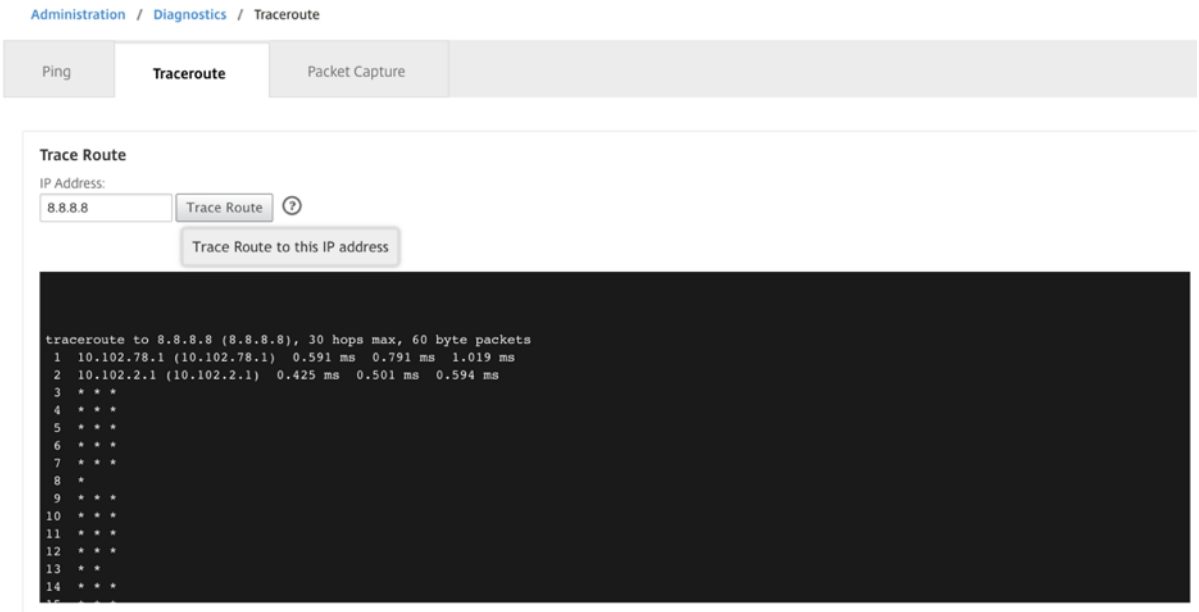
Puede hacer ping a cualquier dirección IP de administración en la red SD-WAN Center mediante la opción **Ping**.



Proporcione una dirección IP válida junto con el número de recuentos de ping (cantidad de veces para enviar la solicitud de ping) y el tamaño del paquete (número de bytes de datos). Haga clic en **Detener ping** para detener una búsqueda de ping continua.

Traceroute

Utilice la opción **Traceroute** para asegurarse de que se pueda acceder a las direcciones IP. Puede rastrear cualquier dirección IP de administración en la red mostrando la ruta y midiendo los retrasos en tránsito de los paquetes.



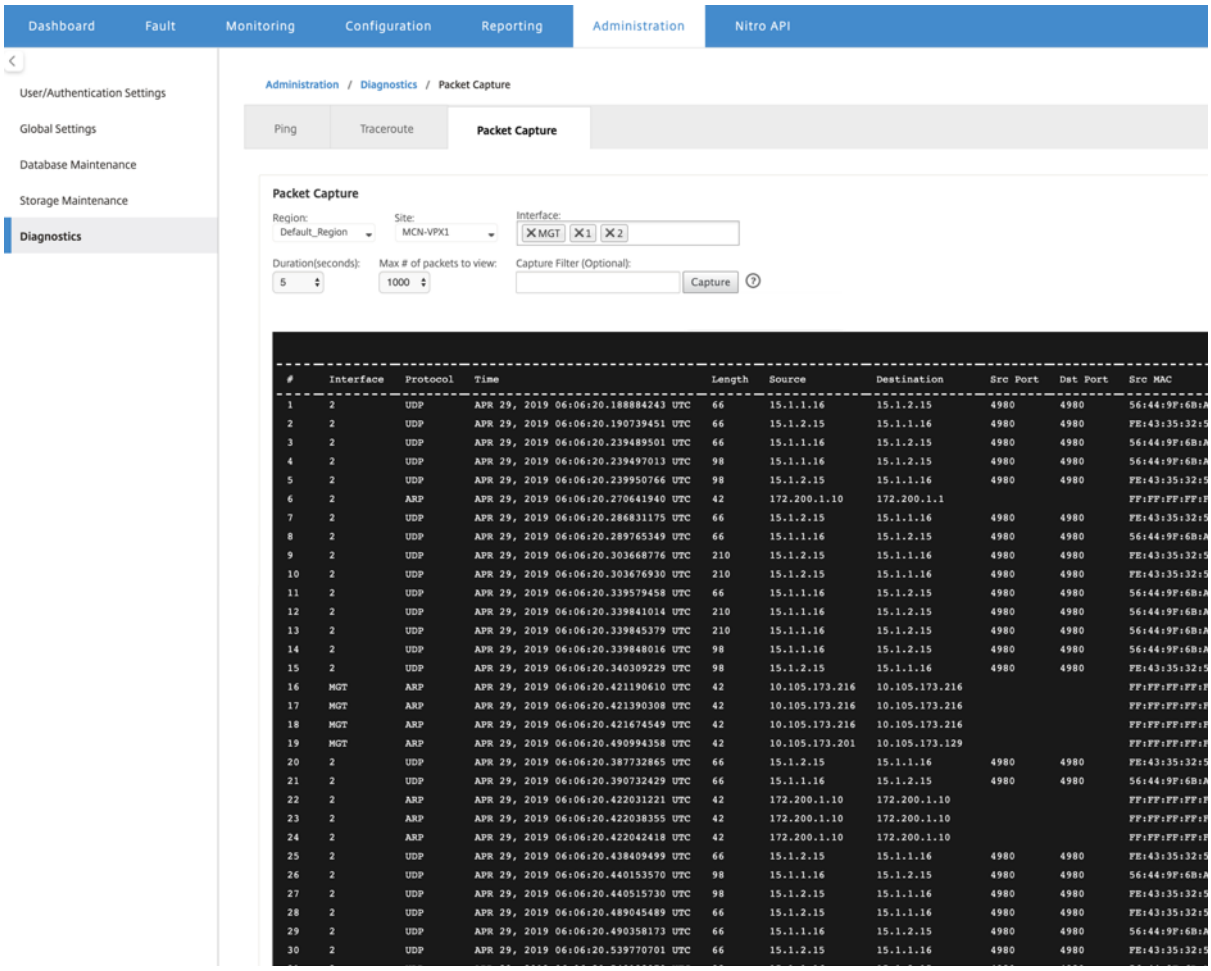
Introduzca una dirección IP de administración válida para rastrear la ruta. Haga clic en **Rastrear**

ruta.

> **NOTA:**
>
> El resultado de traceroute muestra un máximo de 30 saltos.

Captura de paquetes

Utilice la opción **Captura de paquetes** para interceptar el paquete de datos que atraviesa sobre la interfaz activa seleccionada presente en el sitio seleccionado.



Proporcione las siguientes entradas para la operación de captura de paquetes:

- **Región**: Seleccione una región administrada por SD-WAN Center de la lista desplegable.
- **Sitio**: Sitios disponibles en la región seleccionada. Seleccione un sitio de la lista desplegable.
- **Interfaz**: Las interfaces activas están disponibles para la captura de paquetes en el sitio seleccionado. Seleccione una interfaz o agregue interfaces en la lista desplegable. Al menos seleccione una interfaz para activar una captura de paquetes.

> **NOTA:**
>
> La capacidad de ejecutar la captura de paquetes en todas las interfaces a la vez ayuda a acelerar la tarea de solución de problemas.

- **Duración (segundos)**: Duración (en segundos) de cuánto tiempo deben capturarse los datos.
- **Número máximo de paquetes a ver**: Límite máximo de paquetes a ver en el resultado de captura de paquetes.
- **Filtro de captura (opcional)**: El campo **Filtro de captura** opcional acepta una cadena de filtro que se utiliza para determinar qué paquetes se capturan. Los paquetes se comparan con la cadena de filtro y si el resultado de la comparación es verdadero, entonces se captura el paquete. Si el filtro está vacío, se capturan todos los paquetes. Para obtener más información, consulte Filtros de captura.

  A continuación se presentan algunos ejemplos de este filtro de captura:

  - **Ether proto\ARP**: Captura paquetes ARP
  - **Ether proto\IP**: Captura paquetes IPv4
  - **VLAN 100**: Captura paquetes con una VLAN de 100\
  - **Host 10.40.10.20**: Captura paquetes IPv4 hacia o desde el host con la dirección 10.40.10.20
  - **Net 10.40.10.0 Mask 255.255.255.0**: Captura paquetes IPv4 en la subred 10.40.10.0/24
  - **IP proto\TCP**: Captura paquetes IPv4/TCP
  - **Puerto 80**: Captura paquetes IP hacia o desde el puerto 80
  - **Intervalo de puertos 20-30**: Captura paquetes IP hacia o desde los puertos 20 a 30
  - **Host 10.40.10.20 y Puerto 80 y TCP**: Captura solo paquetes IP hacia o desde el puerto TCP 80 en el host 10.40.10.20

> **Nota**:
>
> El límite máximo de tamaño de archivo de captura es de hasta 575 MB. Una vez que el archivo de captura de paquetes alcanza este tamaño, la captura de paquetes se detiene.

Haga clic en **Capturar** para ver el resultado de la captura de paquetes.