Citrix SD-WAN Center 11

Machine translated content

Disclaimer

Contents

系统要求和安装

February 18, 2022

在 VM 上安装 Citrix SD-WAN Center 之前，请确保您必须了解硬件和软件要求，并且已满足必备条件。

> 注意
>
> 对于单区域网络和 mutli 区域网络，系统要求相同。

硬件要求

Citrix SD-WAN Center 具有以下硬件要求。

处理器

- 4 核、3 GHz（或等效）处理器或更好地管理最多 64 站点的服务器。
- 8 核、3 GHz（或等效）处理器或更好地管理最多 128 站点的服务器。
- 16 核、3 GHz（或等效）处理器或更好地管理最多 256 站点的服务器。
- 32 核、酷睿 3 GHz（或等效处理器）或者更适用于管理最多 550 个站点的服务器。

内存

- 对于管理多达 64 个站点的虚拟机，强烈建议至少使用 8GB 的 RAM。
- 对于管理最多 128 个站点的 VM，强烈建议最少使用 16 GB RAM。
- 对于管理最多 256 个站点的 VM，强烈建议最少使用 32 GB RAM。
- 对于管理最多 550 个站点的 VM，强烈建议最少使用 32 GB RAM。

磁盘空间要求

下表提供了有关确定 Citrix SD-WAN Center 数据存储的磁盘空间要求的一些指导原则。将直接存取存储与具有 5000 到 10000 IOPS 的固态硬盘配合使用。

估计的磁盘空间需求

# 客户端网站	每个站点的平均 **WAN** 链接数	每个网站的平均数内联网/互联网服务	每个站点的平均虚拟路径数	**1** 年的数据库大小 **(TB)**
32	2	2	2	1.2T
32	4	4	4	1.8T

# 客户端网站	每个站点的平均 WAN 链接数	每个网站的平均数内联网/互联网服务	每个站点的平均虚拟路径数	1 年的数据库大小 (TB)
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

网络带宽

下表提供了确定 Citrix SD-WAN Center VM 的网络带宽要求的一些指导原则。

估计的网络带宽需求

# 客户端网站	平均数 WAN 链接	每个站点的平均虚拟路径数	每 5 分钟轮询 VWAN 数据总量 (MB)	按 5 分钟轮询配置的带宽速率 (Kbps)
32	2	2	1.2	默认值 1000
32	4	4	3.6	默认值 1000

# 客户端网站	平均数 **WAN** 链接	每个站点的平均虚拟路径数	每 **5** 分钟轮询 **VWAN** 数据总量 **(MB)**	按 **5** 分钟轮询配置的带宽速率 **(Kbps)**
32	8	8	20.0	默认值 1000
64	2	2	2.3	默认值 1000
64	4	4	7.2	默认值 1000
64	8	8	40.0	2000
96	2	2	3.5	默认值 1000
96	4	4	10.8	默认值 1000
96	8	8	60.0	3000
128	2	2	4.6	默认值 1000
128	4	4	14.4	默认值 1000
128	8	8	80.0	4000
192	2	2	6.9	默认值 1000
192	4	4	21.6	2000
192	8	8	120.0	6000
256	2	2	9.2	默认值 1000
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

软件

可以在以下平台上配置 Citrix SD-WAN Center VPX：

Hypervisor

- VMware ESXi 服务器，版本 6.5。
- Citrix XenServer 6.5 或更高版本。
- Microsoft Hyper-V 2012 R2 或更高版本。

云平台

- Microsoft Azure
- Amazon Web Services

浏览器必须启用 cookie，并且已安装并启用了 JavaScript。

Citrix SD-WAN Center Web 界面在以下浏览器上受支持：

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- 火狐火狐 41.0+

必备条件

下面是安装和部署 Citrix SD-WAN Center 的必备条件：

- SD-WAN 主控制节点 (MCN) 和现有客户端节点必须升级到最新的 Citrix SD-WAN 软件版本。
- 建议在 SD-WAN 网络中提供并配置 DHCP 服务器。
- 您必须具有 Citrix SD-WAN Center 安装文件。

> 注意
>
> 您不能在 Citrix SD-WAN Center 上自定义或安装任何第三方软件。但是，您可以修改 vCPU、内存和存储设置。

下载 **Citrix SD-WAN Center** 软件

从下载页面下载所需版本和平台的 Citrix SD-WAN Center 管理控制台软件安装文件。

Citrix SD-WAN Center 安装文件使用以下命名约定：

ctx-sdwc-版本 _ 数字平台. 扩展名

- *version_number* 是 Citrix SD-WAN Center 版本编号。
- 平台 是平台类型、虚拟机管理程序或云平台名称。
- 扩展名 是安装文件扩展名。

平台	文件扩展名
Citrix XenServer	.xva
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-Azure.vhd.zip

收集 **Citrix SD-WAN Center** 安装和配置信息

本部分提供了完成 Citrix SD-WAN Center 安装和部署所需的信息的核对表。

收集或确定以下信息：

- 托管 Citrix SD-WAN Center 虚拟机 (VM) 的 ESXi 服务器、XenServer、Hyper-V 服务器或 Azure 的 IP 地址。
- 要分配给 Citrix SD-WAN Center VM 的唯一名称。
- 为 Citrix SD-WAN Center VM 分配的内存量。
- 要为虚拟机分配给虚拟磁盘的磁盘容量。
- Citrix SD-WAN Center 将用来与外部网络进行通信的网关 IP 地址。
- 将在其中安装 Citrix SD-WAN Center VM 的网络的子网掩码。

在 **ESXi** 服务器上安装并配置 **Citrix SD-WAN Center**

April 13, 2021

安装 **VMware vSphere** 客户端

以下是下载和安装用于创建和部署 Citrix SD-WAN Center 虚拟机的 VMware vSphere 客户端的基本说明。有关详细信息，请参阅 VMware vSphere 客户端文档。

要下载并安装 VMware vSphere 客户端，请执行以下操作：

1. 打开浏览器并导航到托管 vSphere Client 和 Citrix SD-WAN Center 虚拟机 (VM) 实例的 ESXi 服务器。

   此时将显示 VMware ESXi 欢迎页面。

2. 单击下载 **vSphere** 客户端链接以下载 vSphere 客户端安装文件。
3. 安装 vSphere Client。

   运行您下载的 vSphere Client 安装程序文件，并在出现提示时接受每个默认选项。

4. 安装完成后，启动 vSphere Client 程序。

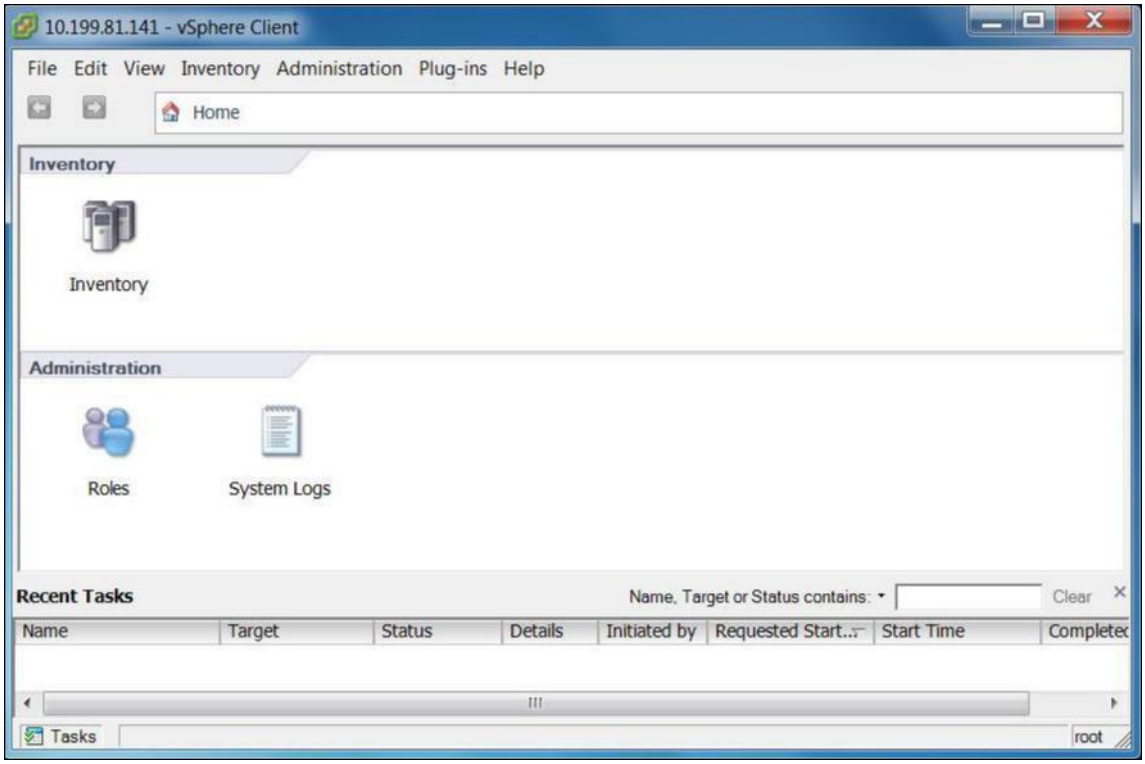
   此时将显示 VMware vSphere 客户端登录页面，提示您输入 ESXi 服务器登录凭据。

5. 输入 ESXi 服务器登录凭据：

   - **IP** 地址**/**名称：输入托管 Citrix SD-WAN Center 虚拟机实例的 ESXi 服务器的 IP 地址或完全限定域名 (FQDN)。
   - 用户名：输入服务器管理员帐户名称。默认值为根。
   - 密码：输入与此管理员帐户关联的密码。

6. 点击 登录。

   此时将显示 vSphere Client 主页。



使用 **OVF** 模板创建 **Citrix SD-WAN Center VM**

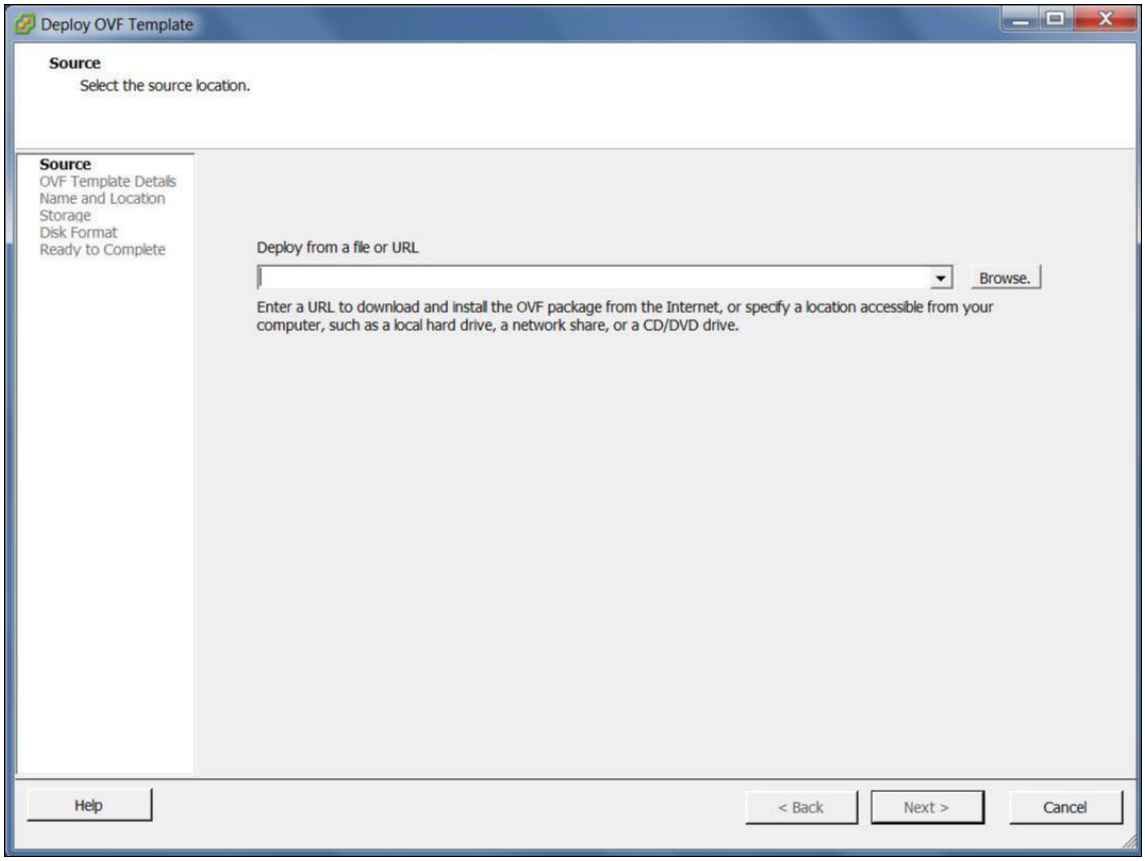
安装 VMware VSphere 客户端后，创建 Citrix SD-WAN Center 虚拟机。

1. 如果尚未将 Citrix SD-WAN Center OVF 模板文件（ova 文件）下载到本地 PC，请将其下载到本地 PC。

   有关详细信息，请参阅系统要求和安装。

2. 在 vSphere 客户端中，单击文件，然后从下拉菜单中选择部署 **OVF** 模板。

   此时将显示部署 **OVF** 模板向导。

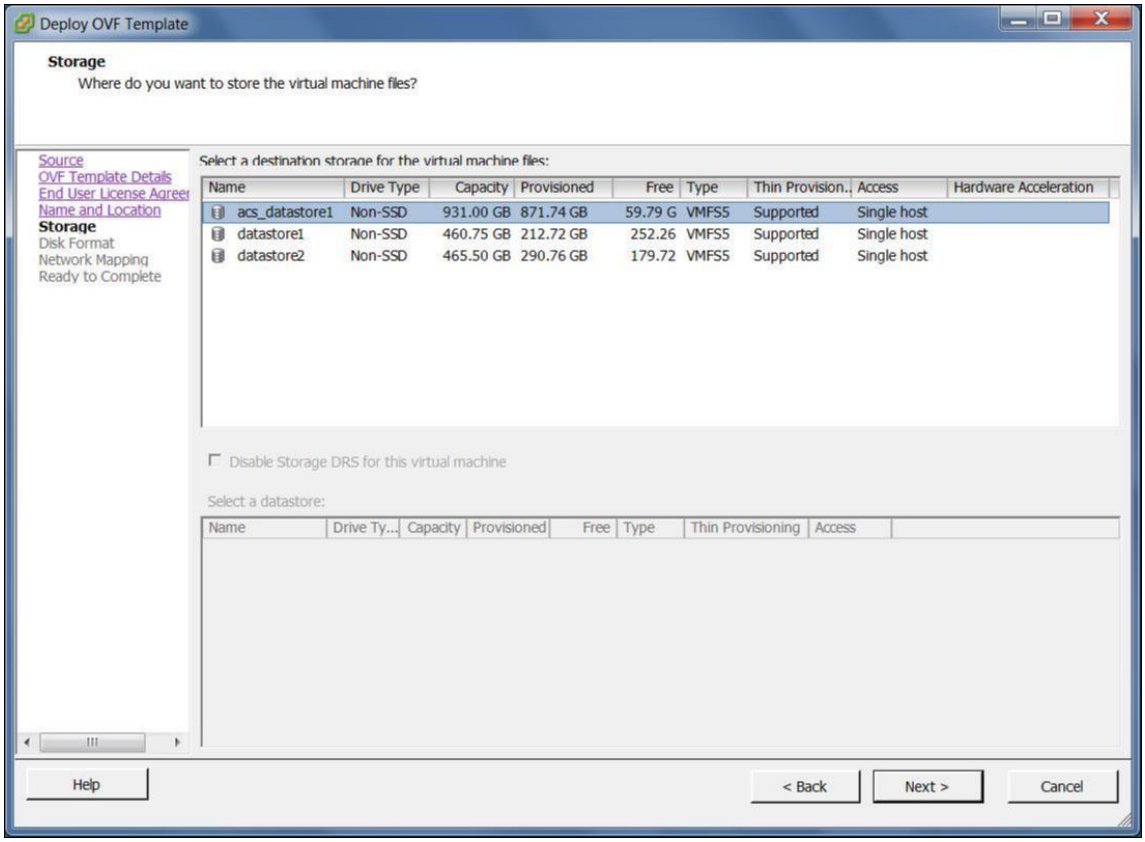


3. 单击浏览并选择要安装的 Citrix SD-WAN Center OVF 模板（ova 文件)。
4. 单击下一步。

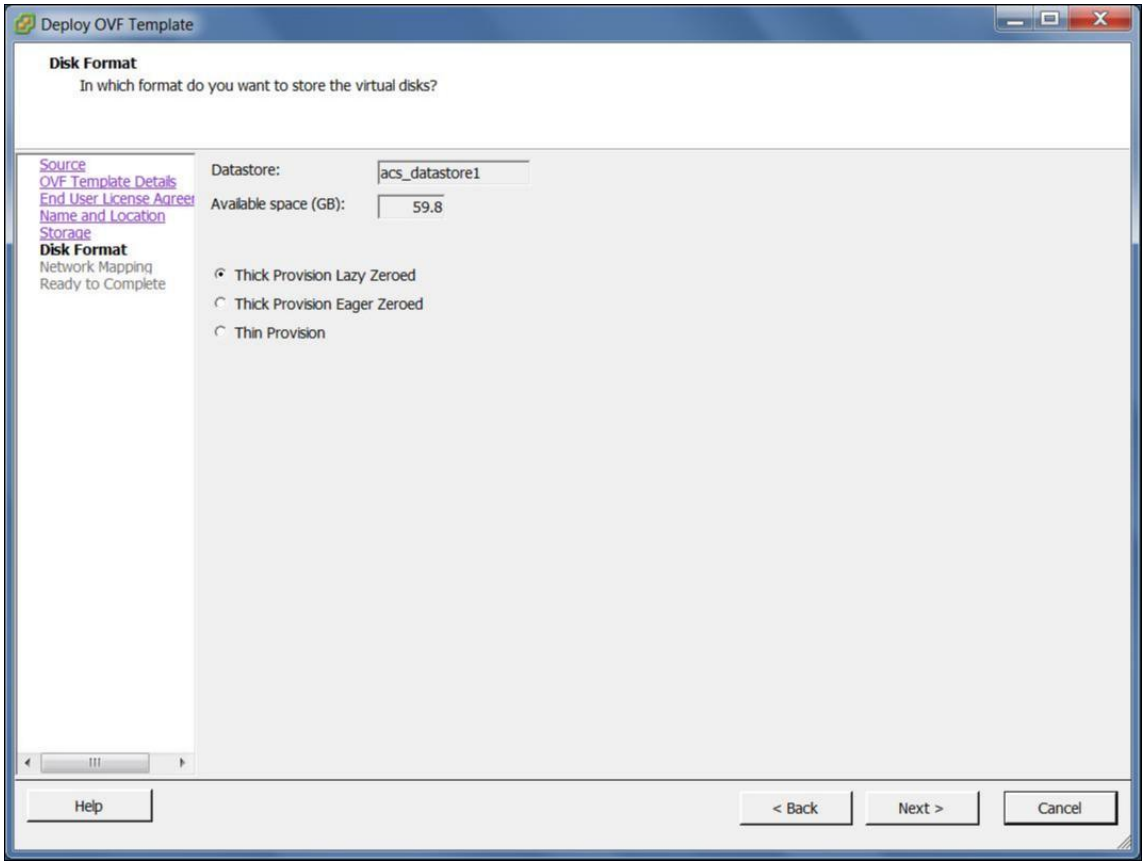
   将导入 ova 文件，并显示 OVF 模板详细信息页面。
5. 单击下一步。
6. 在最终用户许可协议页面上，单击接受，然后单击下一步。
7. 在“名称和位置”页面上，输入新 VM 的唯一名称（或接受默认值)。

   名称在当前 库存 文件夹中必须唯一，长度最多可达 80 个字符。
8. 单击下一步。

   此时将显示“存储”页面。



9. 现在，单击下一步接受默认存储资源。您还可以配置数据存储。有关详细信息，请参阅在 ESXi 服务器 上添加和配置数据存储。



10. 在“磁盘格式”页面上，接受默认设置，然后单击下一步。
11. 在“网络映射”页面上，接受默认值（VM 网络），然后单击下一步。
12. 在“完成准备就绪”页面上，单击完成以创建 VM。

    > 注意：将磁盘映像
    >
    > 解压到服务器可能需要几分钟的时间。

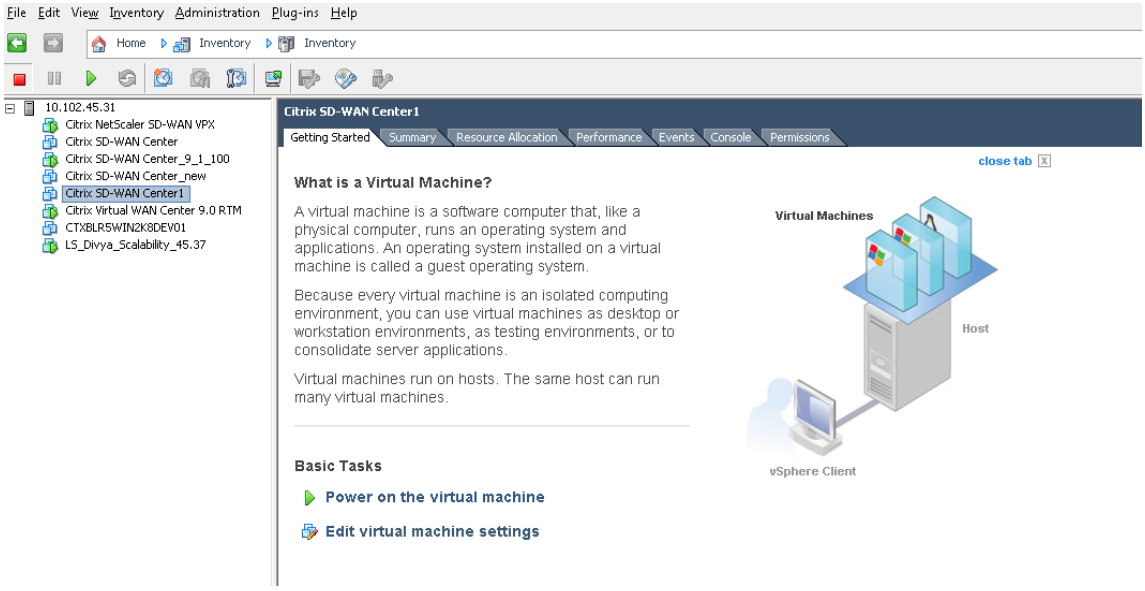
13. 单击关闭。

在 **ESXi** 服务器上查看并记录管理 **IP** 地址

管理 IP 地址是 SD-WAN Center VM 的 IP 地址，使用此 IP 地址登录 Citrix SD-WAN Center Web UI。

要显示管理 IP 地址，请执行以下操作：

1. 在 vSphere 客户端清单页面上，在清单树状结构（左侧窗格）中选择新 Citrix SD-WAN Center VM。

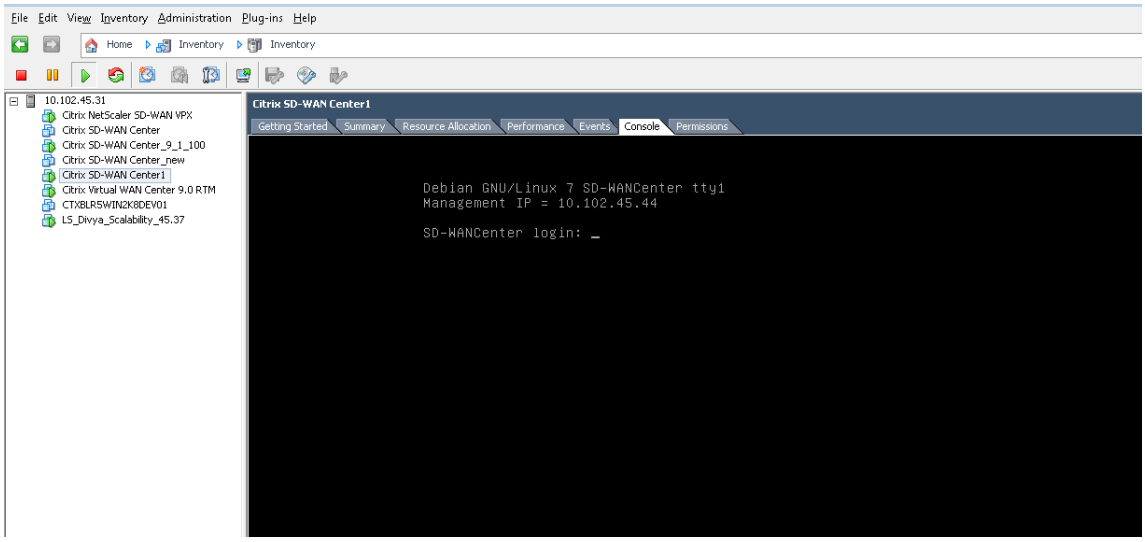


2. 在 Citrix SD-WAN Center 页面上，在基本任务下，单击虚拟机上的电源。
3. 选择控制台选项卡，然后单击控制台区域内的任意位置以进入控制台模式。

   这会将鼠标光标的控制权转移到虚拟机控制台。

   > 注意
   >
   > 要释放光标的控制台控制，请同时按下 <Ctrl> 和 <Alt> 键。

4. 按 **Enter** 键显示控制台登录提示。

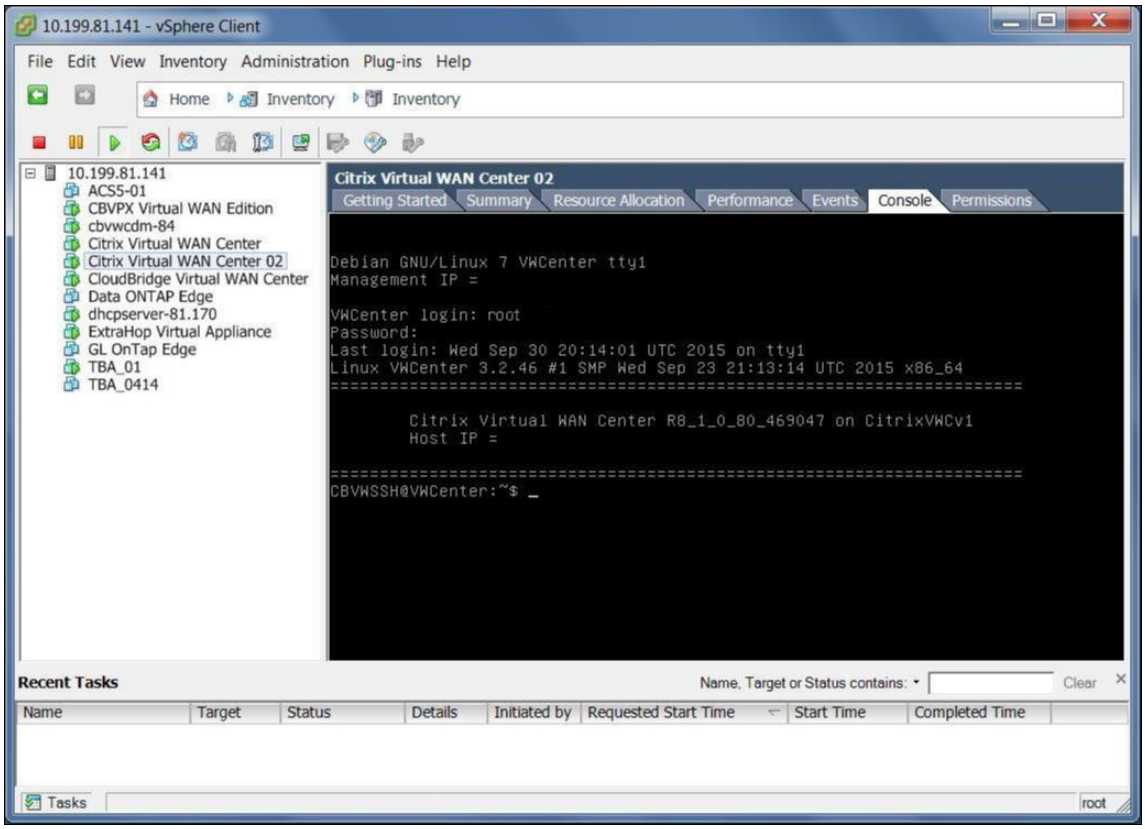


5. 登录 VM 控制台。

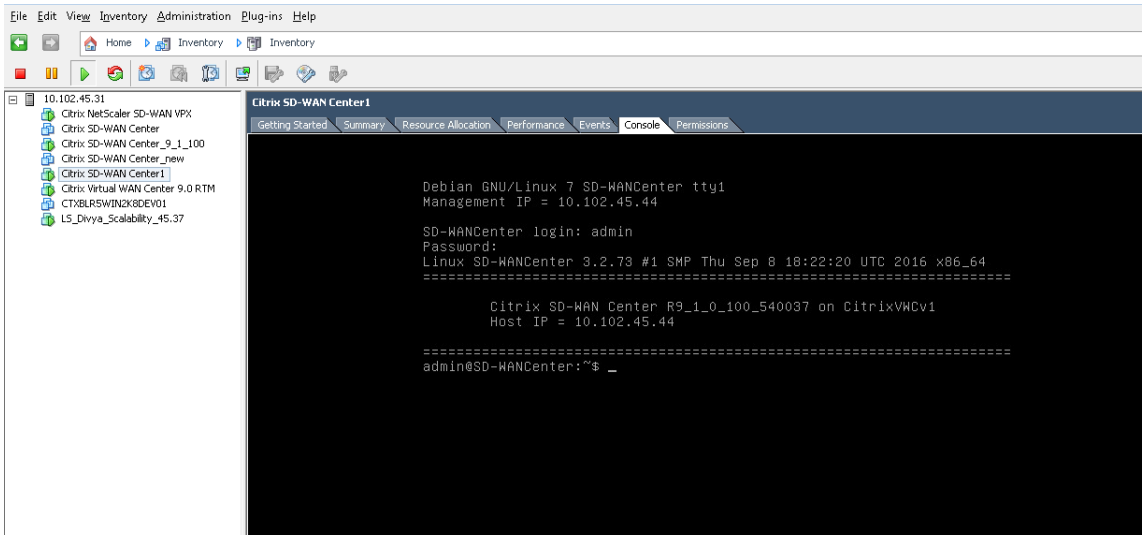
   新 Citrix SD-WAN Center 虚拟机的默认登录凭据如下所示：

   - 登录：admin

- 密码：password



6. 记录 Citrix SD-WAN Center VM 的管理 IP 地址，该地址显示为在登录时显示的欢迎消息中的主机 IP 地址。



> 注意
>
> DHCP 服务器必须存在并在 SD-WAN 网络中可用，否则无法完成此步骤。

如果未在 SD-WAN 网络中配置 DHCP 服务器，您必须手动输入静态 IP 地址。

要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

1. VM 启动时，单击控制台选项卡。
2. 登录虚拟机。新 Citrix SD-WAN Center 虚拟机的默认登录凭据如下所示：

   登录：admin

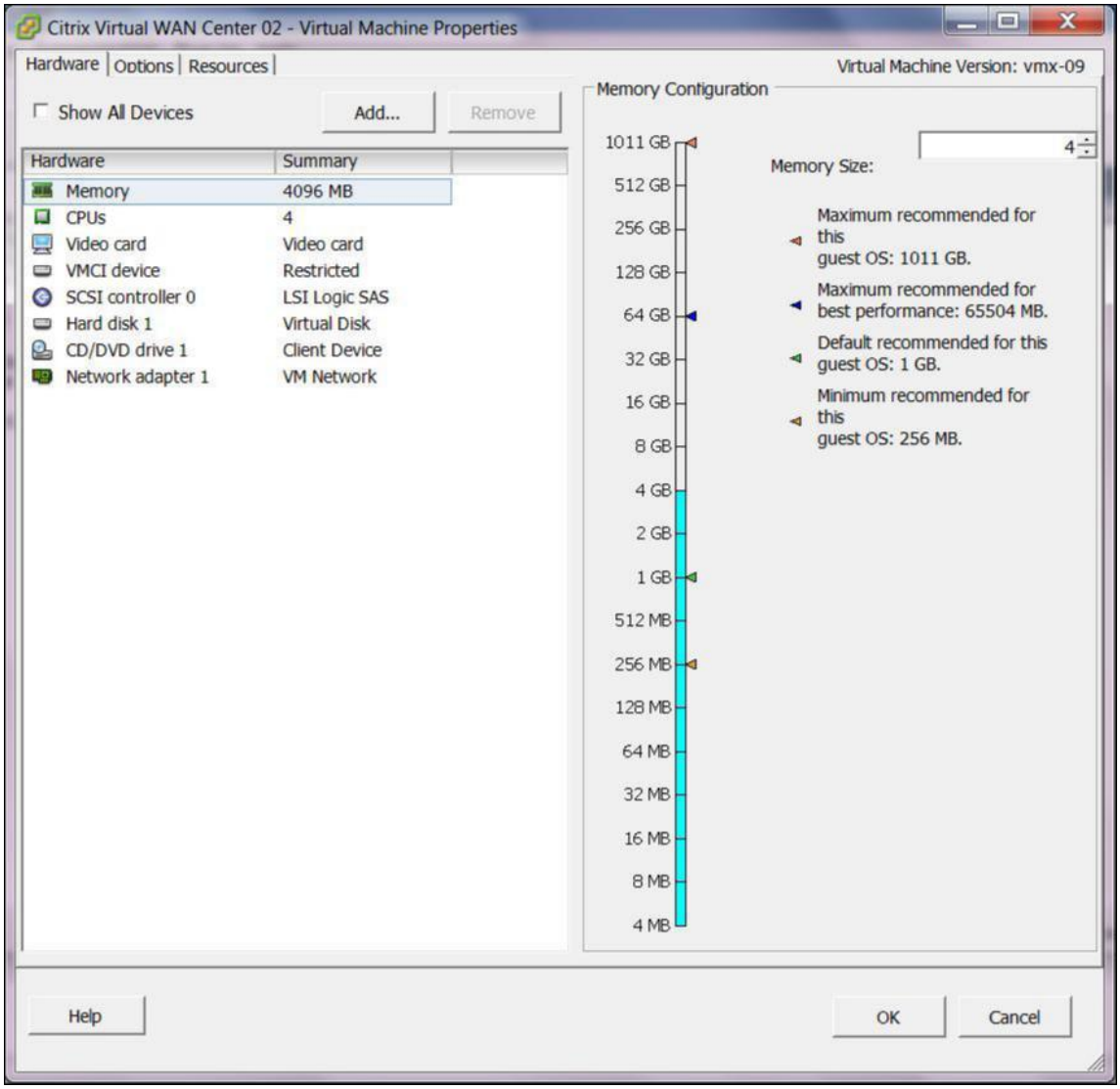
   Password（密码）：password
3. 在控制台中，输入 CLI 命令 **management_IP**。
4. 输入命令 **set interface <ipaddress> <subnetmask> <gateway>**，以配置管理 IP。

在 **ESXi** 服务器上添加和配置数据存储

您可以添加和配置数据存储，以存储 Citrix SD-WAN Center 中的统计信息。

要添加和配置数据存储，请执行以下操作：

1. 在 vSphere 客户端中，单击清单图标以打开清单页面。
2. 展开 Citrix SD-WAN Center VM 主机服务器的清单树状分支。
3. 在左窗格中，单击托管您创建的 Citrix SD-WAN Center VM 的服务器的 IP 地址旁边的 **+** 。
4. 打开新 Citrix SD-WAN Center VM 以进行编辑。
5. 在 清 单树中，右键单击您创建的 Citrix SD-WAN Center VM 的名称，然后从下拉菜单中选择 编辑设置。

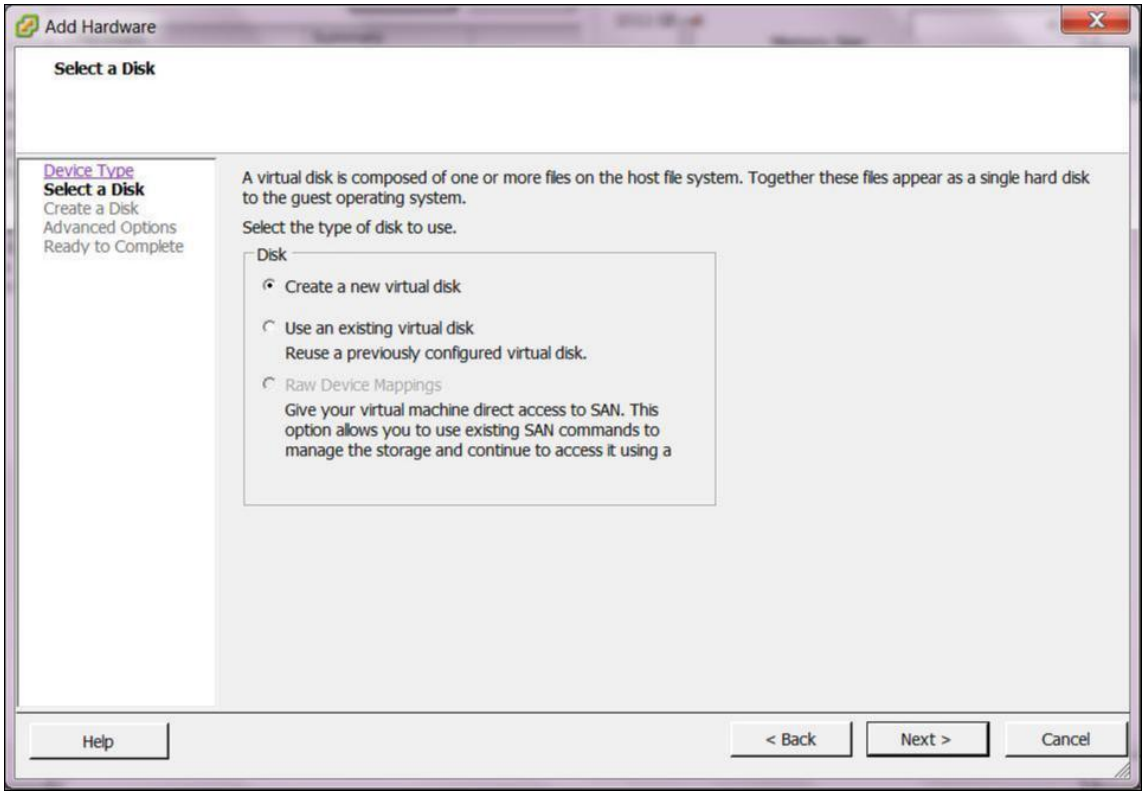


6. 在“内存大小”字段中，输入要为此 VM 分配的内存量。

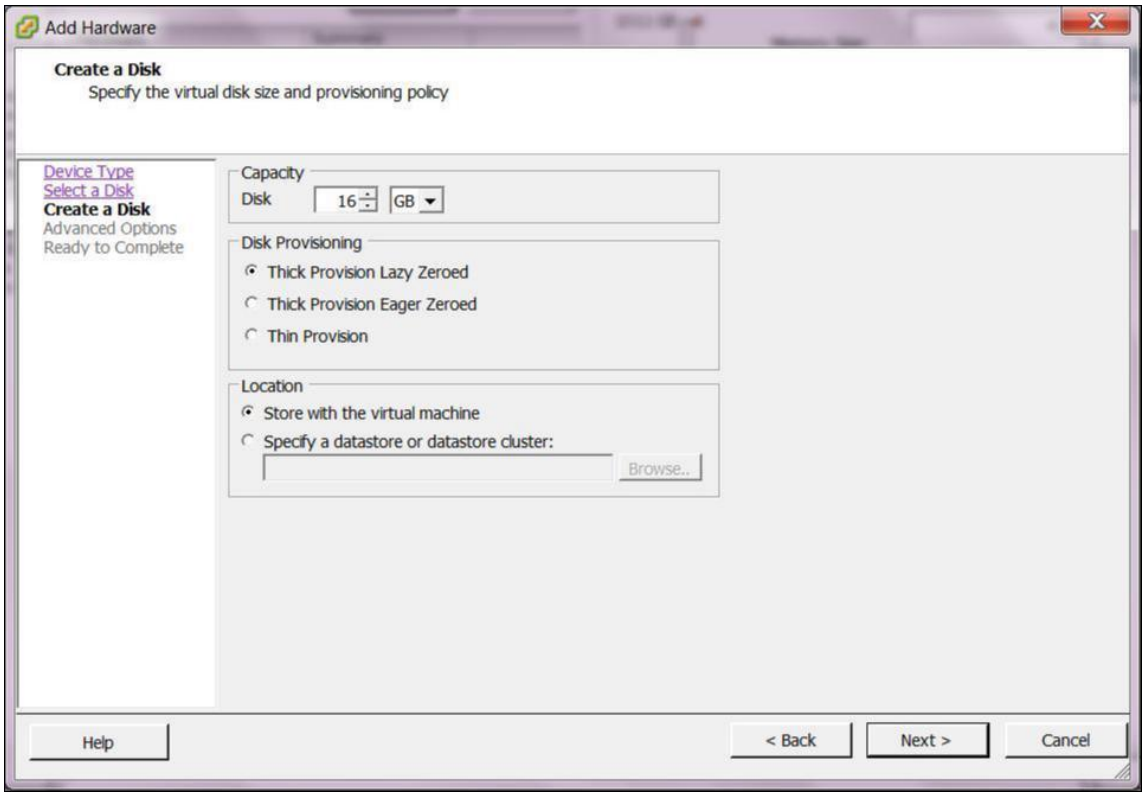
   有关详细信息，请参阅内存要求。

7. 单击添加。

8. 在“添加硬件”向导的“设备类型”页面上，选择硬盘，然后单击下一步。

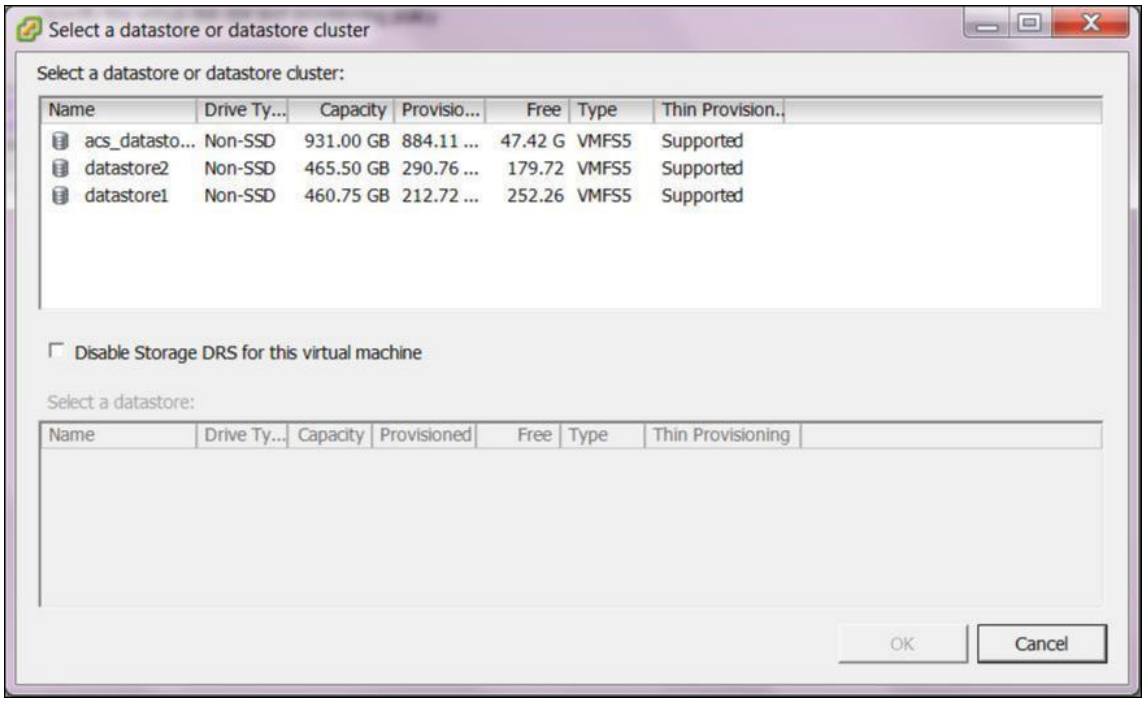


9. 在“选择磁盘”页面上，选择创建新虚拟磁盘，然后单击下一步。

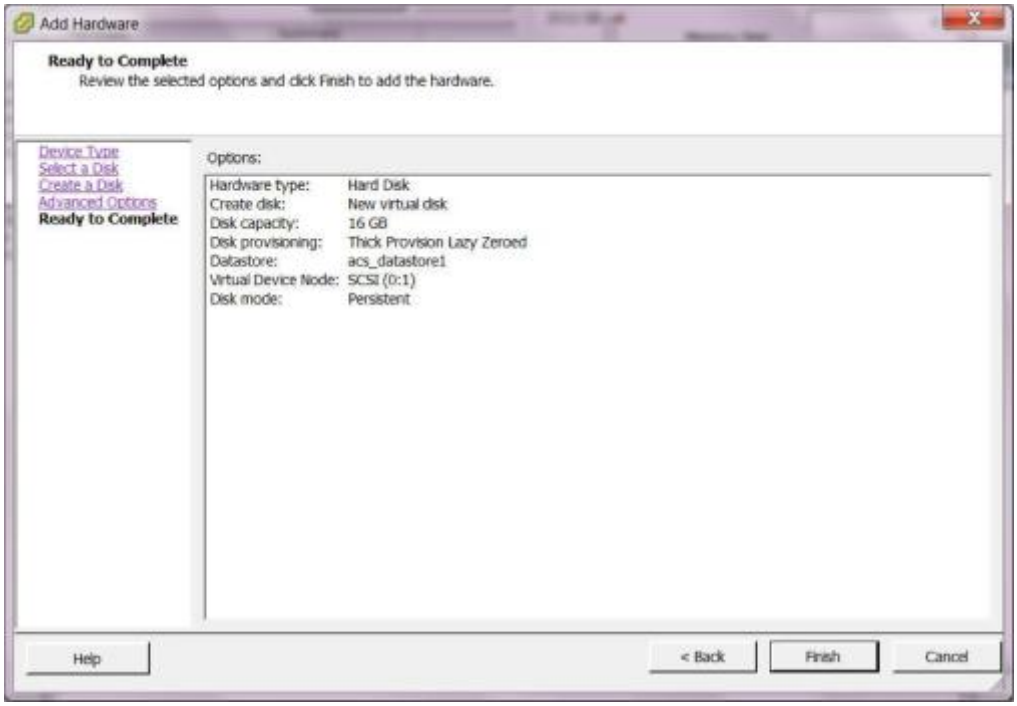


10. 在“创建磁盘”页面上的容量部分中，选择新虚拟磁盘的磁盘容量。

11. 在“磁盘预配”部分中，选择厚预配延迟零（默认设置）。
12. 在“位置”部分中，选择指定数据存储或数据存储群集。
13. 单击浏览。



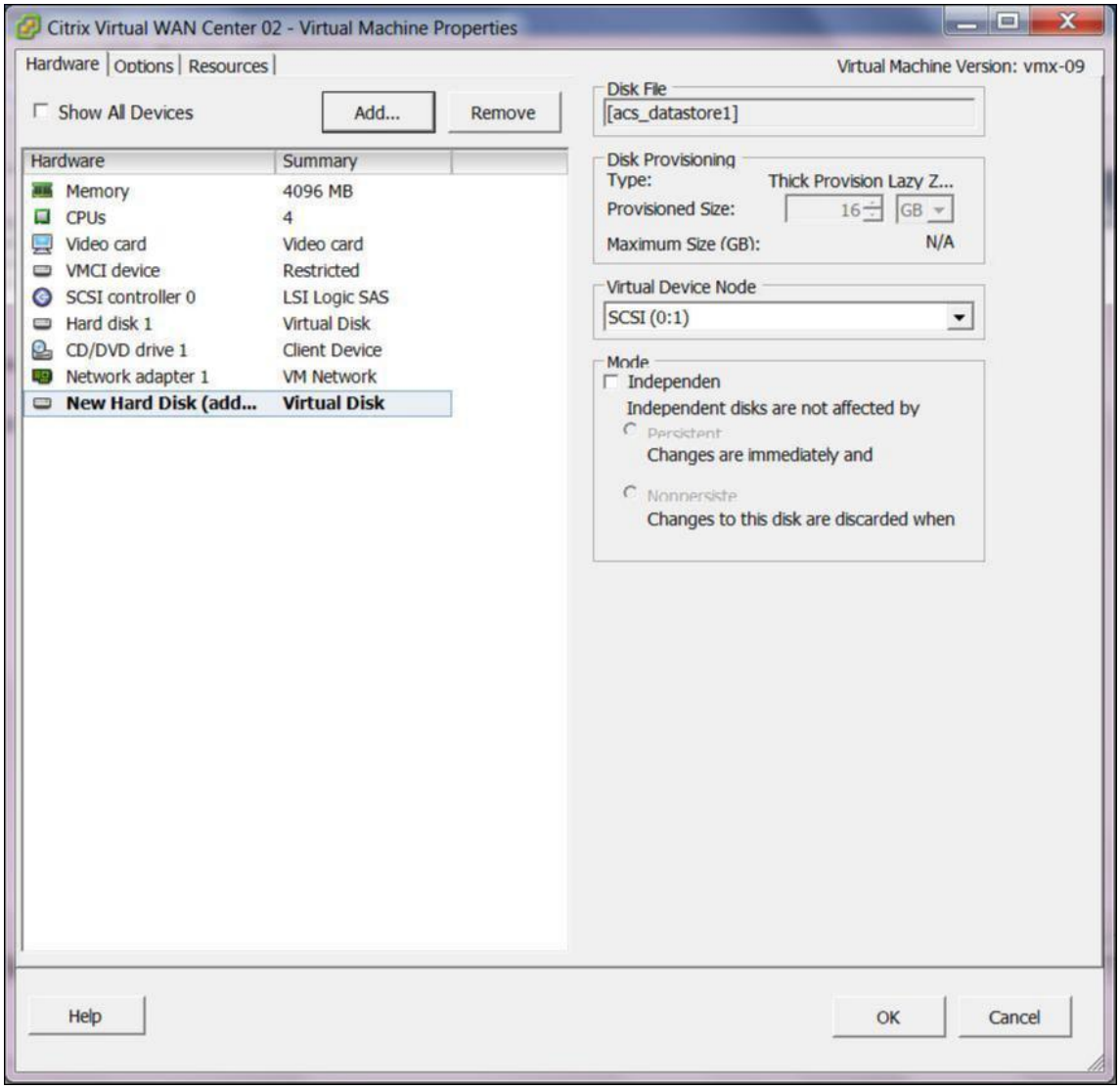
14. 选择一个具有足够可用空间的数据存储，然后单击确定。
15. 单击下一步。
16. 在“高级选项”页面上，接受高级选项默认设置，然后单击下一步。



17. 单击完成。

    这将添加新虚拟磁盘，使“添加硬件”向导无法关闭，并返回到虚拟机属性页面。

18. 单击 **OK**（确定）。



在 **XenServer** 上安装并配置 **Citrix SD-WAN Center**

April 13, 2021

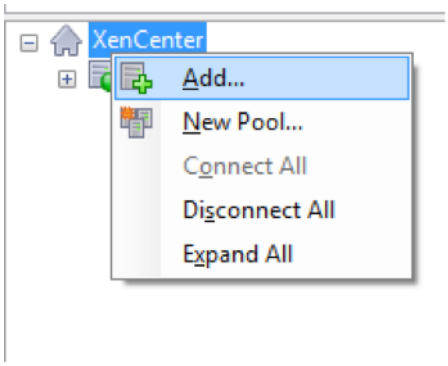
在 XenServer 服务器上安装 Citrix SD-WAN Center 虚拟机之前，请按收集 Citrix SD-WAN Center 安装和配置信息中所述收集必要的信息。

安装 **XenServer** 服务器

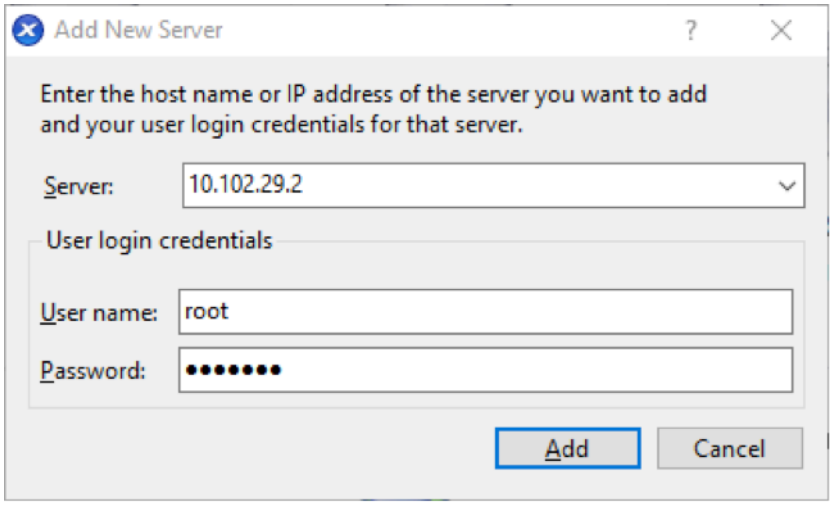
要安装要在其上部署 Citrix SD-WAN Center 虚拟机的 Citrix XenServer 服务器，必须在您的计算机上安装 XenCenter。如果尚未下载并安装 XenCenter，请执行下载并安装。

要安装 XenServer 服务器，请执行以下操作：

1. 在计算机上打开 XenCenter 应用程序。
2. 在左侧树结构窗格中的 **XenCenter** 上单击鼠标右键，然后选择添加。



3. 在添加新服务器窗口中，在以下字段中输入所需的信息：
   - 服务器：输入将托管您的 Citrix SD-WAN Center VM 实例的 XenServer 服务器的 IP 地址或完全限定的域名 (FQDN)。
   - 用户名：输入服务器管理员帐户名称。默认值为根。
   - 密码：输入与此管理员帐户关联的密码。



4. 单击添加。

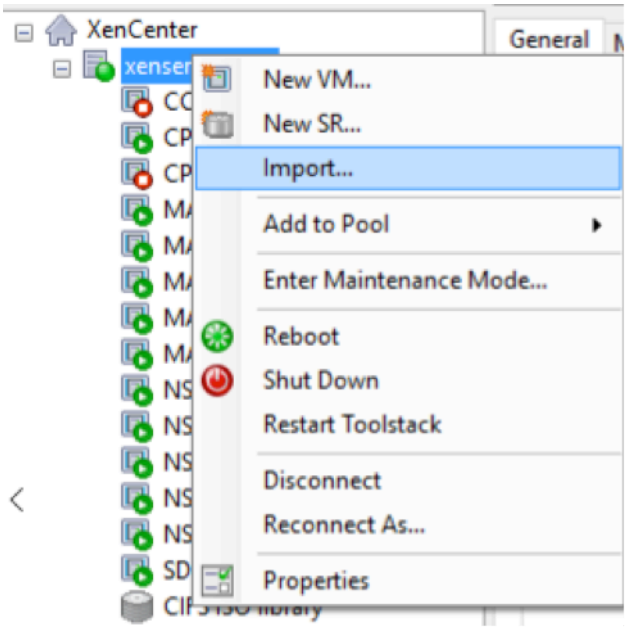
   新服务器的 IP 地址将显示在左窗格中。

使用 **XVA** 文件创建 **Citrix SD-WAN Center VM**

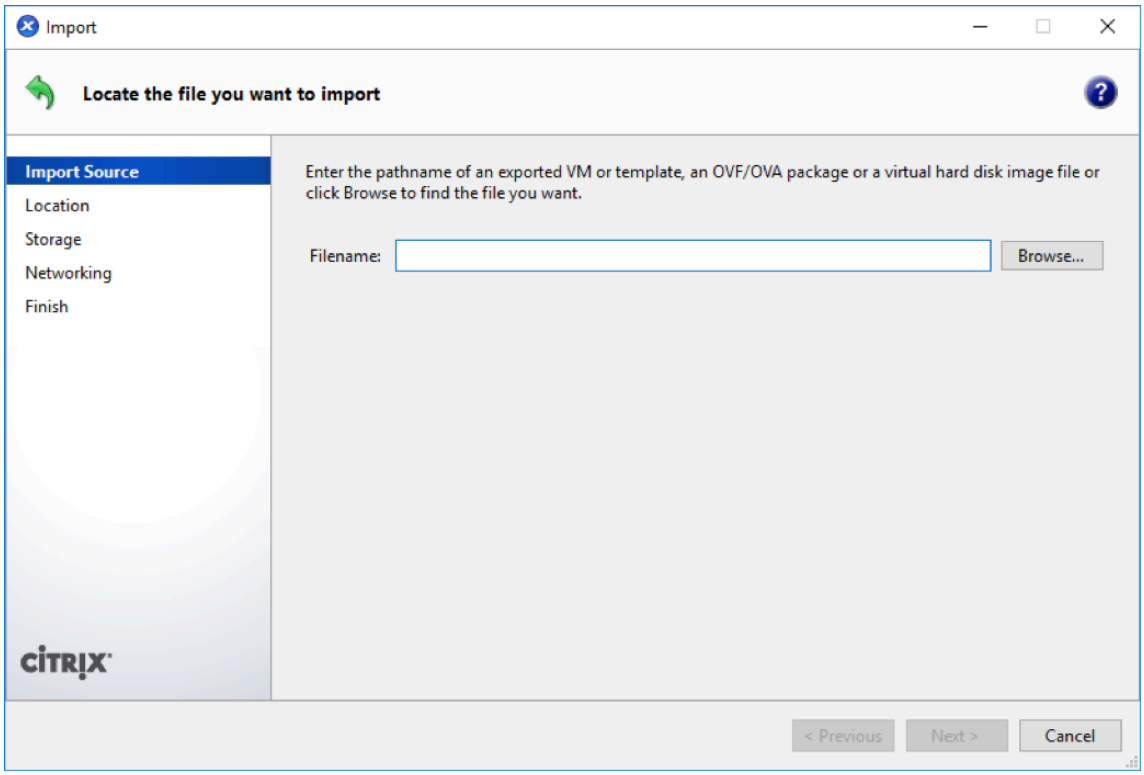
Citrix SD-WAN Center 虚拟机软件以 XVA 文件的形式分发。如果您尚未下载.xva 文件，请下载该文件。有关详细信息，请参阅系统要求和安装。

要创建 Citrix SD-WAN Center VM，请执行以下操作：

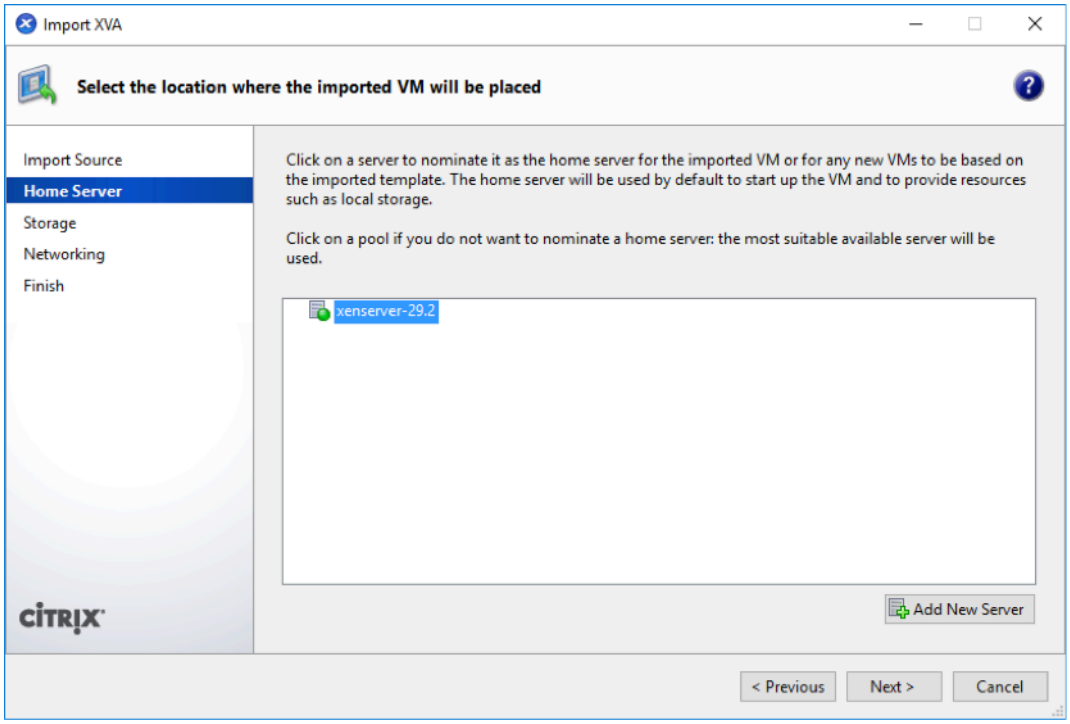
1. 在 XenCenter 中，在 **XenServer** 上单击鼠标右键，然后单击导入。



2. 浏览到下载的 xva 文件，将其选中，然后单击下一步。

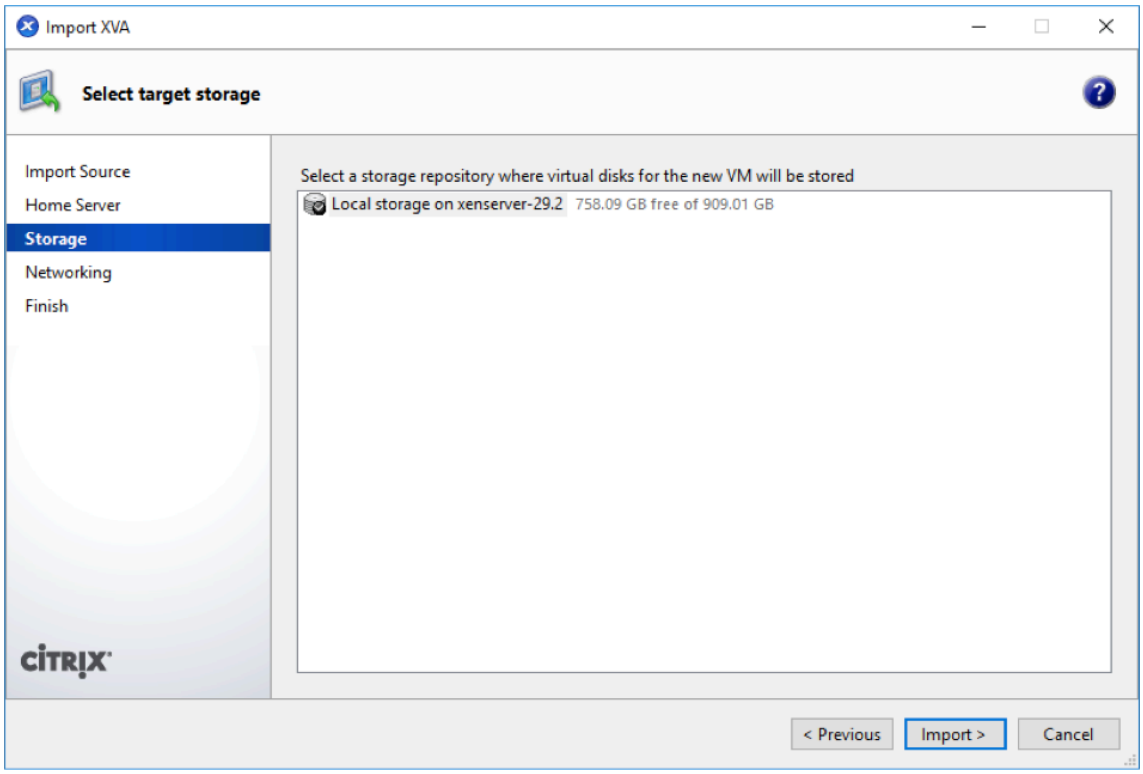


3. 选择之前创建的 XenServer 服务器作为导入 VM 的位置，然后单击下一步。



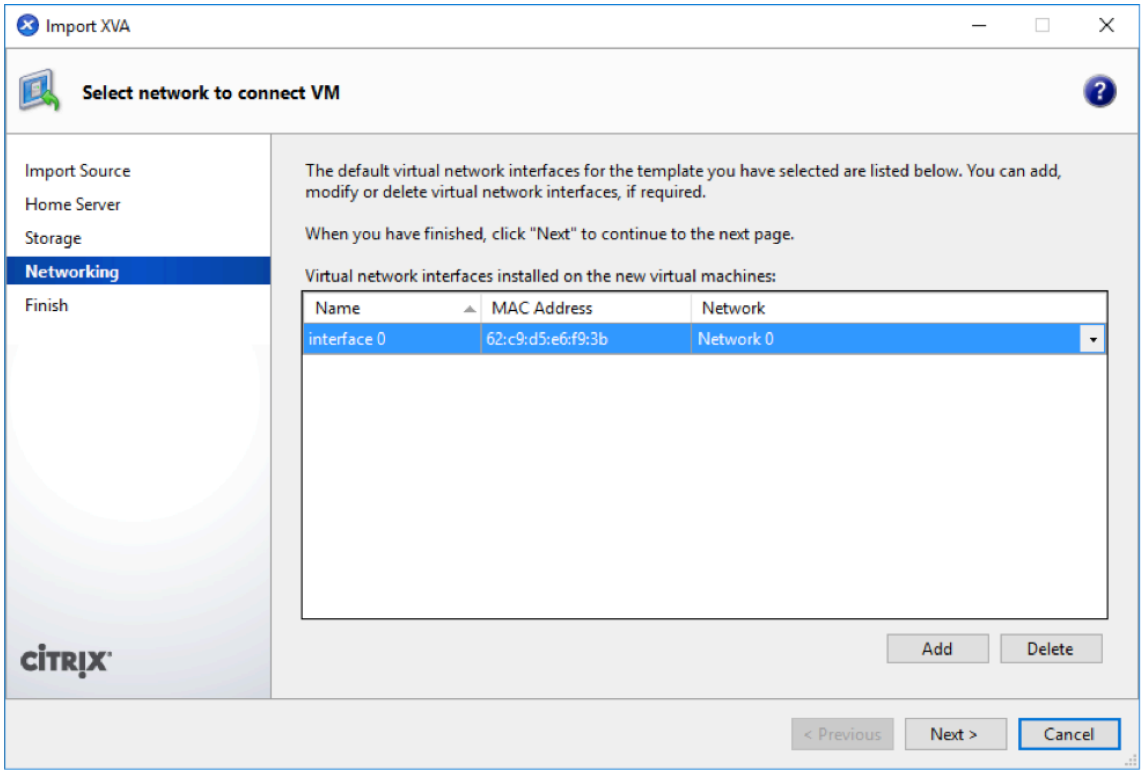
4. 选择将存储新 VM 的虚拟磁盘的存储库，然后单击 导入。

   现在，您可以接受默认存储资源。或者，您可以配置数据存储。有关详细信息，请参阅 在 **XenServer** 上添加和配置数据存储部分。



   导入的 Citrix SD-WAN Center VM 将显示在左侧窗格中。

5. 选择要将 VM 连接到的网络，然后单击下一步。



6. 单击完成。

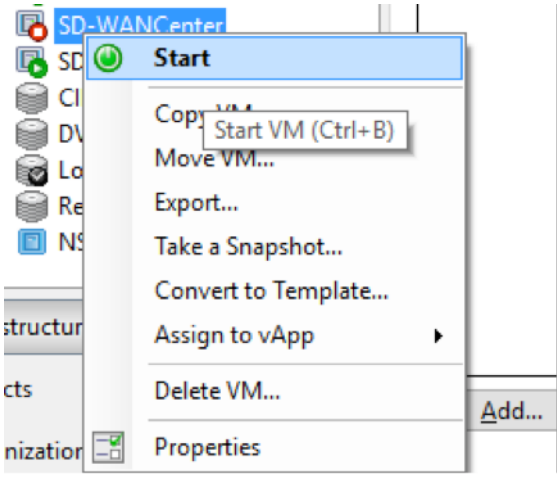
在 **XenServer** 上查看并记录管理 **IP** 地址

管理 IP 地址是 Citrix SD-WAN Center VM 的 IP 地址，使用此 IP 地址登录到 Citrix SD-WAN Center Web UI。

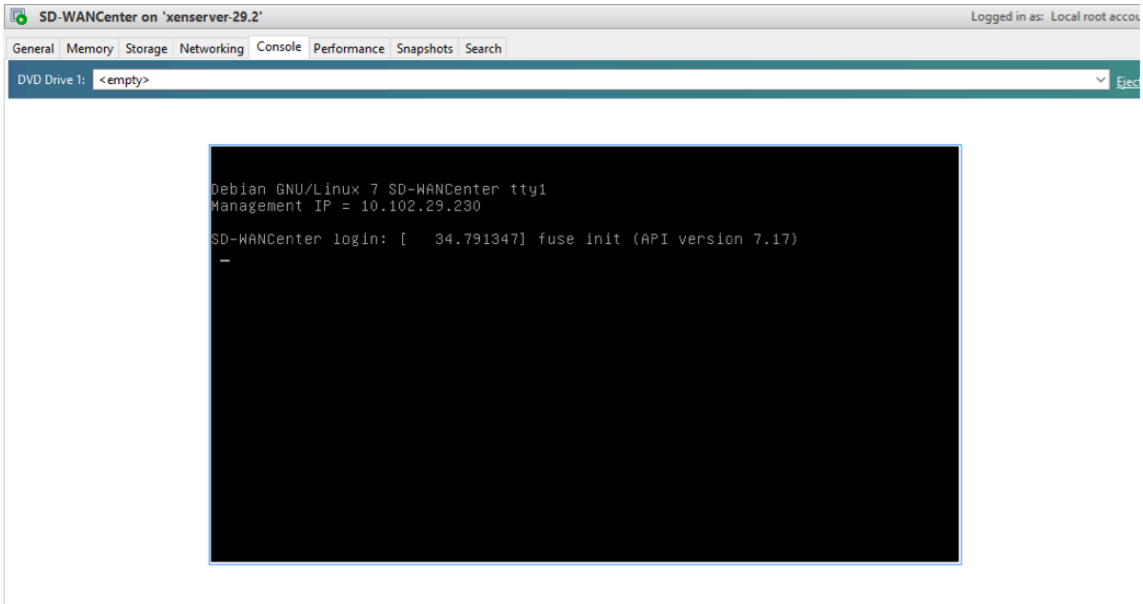
> 注意
>
> DHCP 服务器必须在 SD-WAN 网络中存在并可用。

要显示管理 IP 地址，请执行以下操作：

1. 在 XenCenter 界面中，在左侧窗格中，右键单击新的 Citrix SD-WAN Center VM，然后选择启动。



2. VM 启动时，单击控制台选项卡。



3. 记下管理 IP 地址。

> 注意
>
> DHCP 服务器必须存在并在 SD-WAN 网络中可用，否则无法完成此步骤。

4. 登录虚拟机。新 Citrix SD-WAN Center 虚拟机的默认登录凭据如下所示：

   登录：admin

   Password（密码）：password

   如果未在 Citrix SD-WAN 网络中配置 DHCP 服务器，则必须手动输入静态 IP 地址。

要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

1. VM 启动时，单击控制台选项卡。

2. 登录虚拟机。新 Citrix SD-WAN Center 虚拟机的默认登录凭据如下所示：

   登录：admin
   ，密码：password

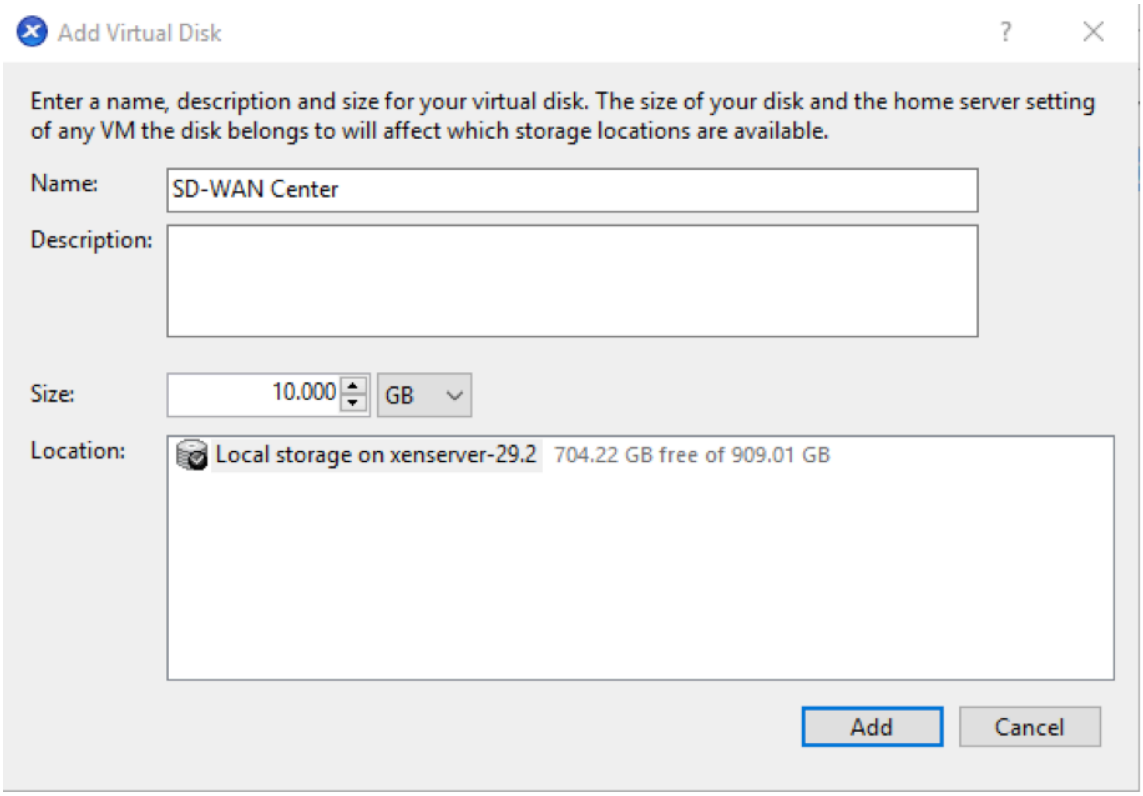
3. 在控制台中输入 CLI 命令 **Management_ip**。
4. 输入命令 **set interface <ipaddress> <subnetmask> <gateway>**，以配置管理 IP。

为 **XenServer** 服务器添加和配置数据存储

您可以添加和配置数据存储，以存储 Citrix SD-WAN Center 中的统计信息。

要添加和配置数据存储，请执行以下操作：

1. 在 XenCenter 中，关闭 Citrix SD-WAN Center VM。
2. 在存储选项卡上，单击添加。



3. 在名称字段中，输入虚拟磁盘的名称。
4. 在说明字段中，输入虚拟磁盘的说明。
5. 在大小字段中，选择所需的大小。
6. 在位置字段中，选择本地存储。
7. 单击添加。

在 Microsoft Hyper-V 上安装并配置 Citrix SD-WAN Center

April 13, 2021

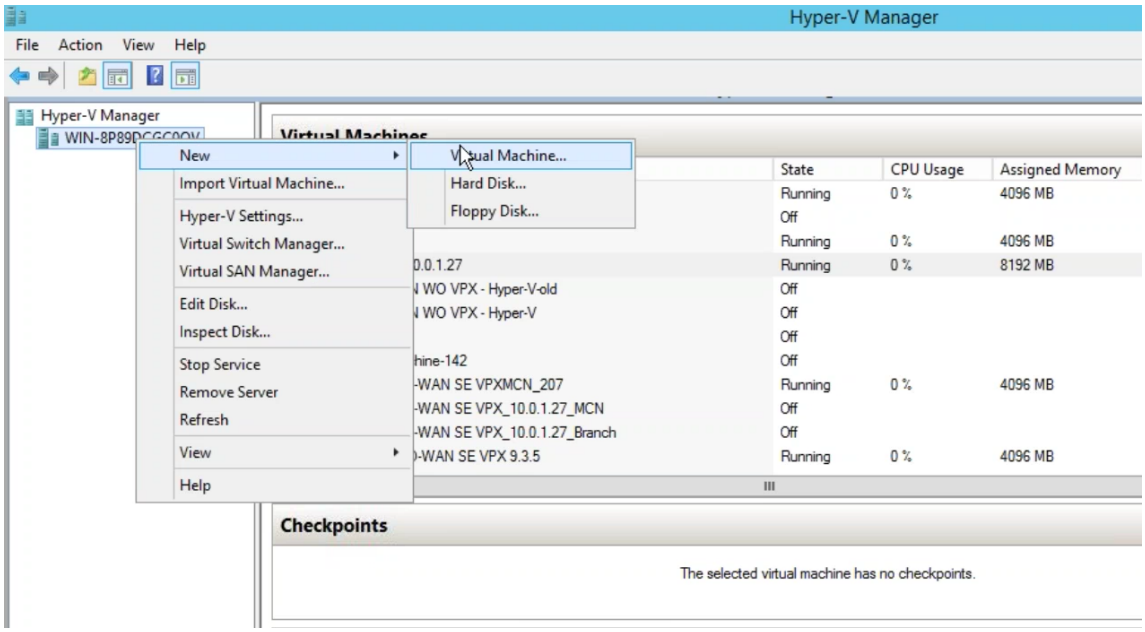
在 Microsoft Hyper-V 服务器上安装 Citrix SD-WAN Center 虚拟机 (VM) 之前，请收集必要的信息，如系统要求和安装中所述。

下载适用于 Hyper-V 的 SD-WAN Center 软件，如系统要求和安装的“下载 Citrix SD-WAN Center 软件”部分中所述。

确保 Hyper-V 功能和管理工具在您的 Windows 服务器上处于启用状态。

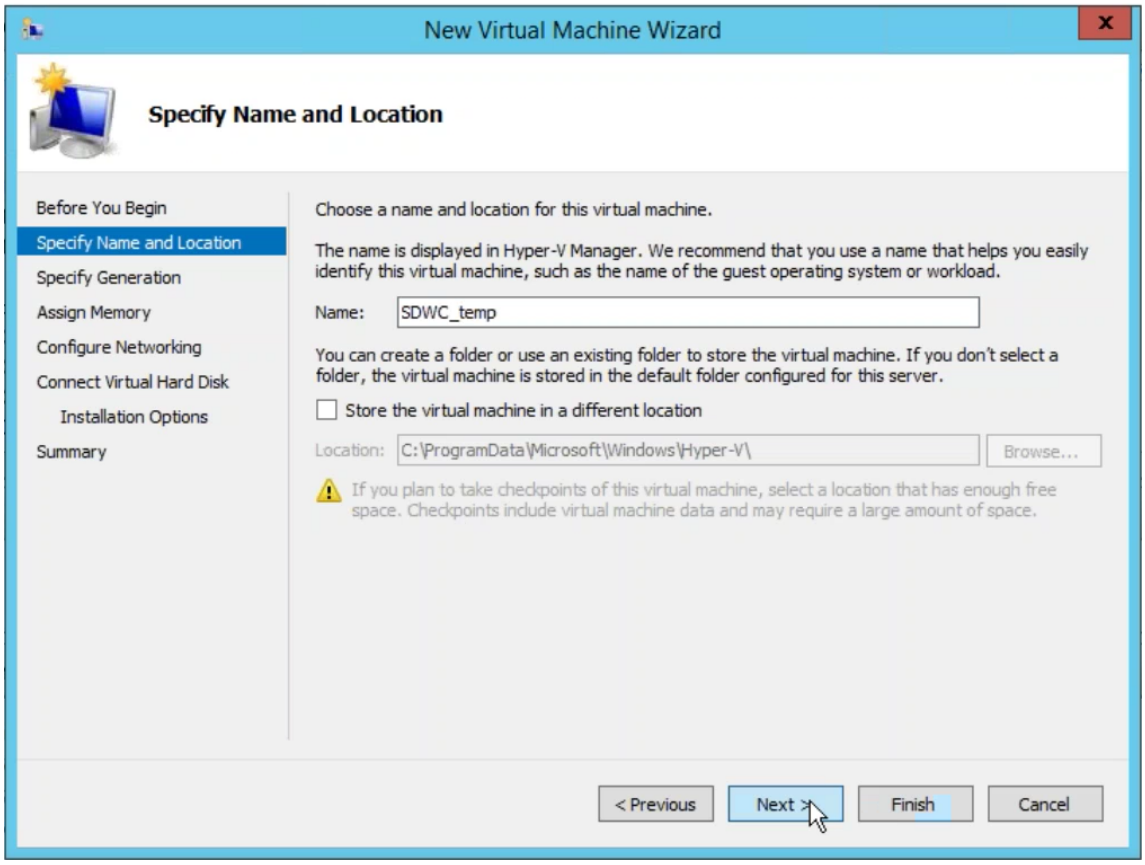
要在 Hyper-V 服务器上创建 SD-WAN Center VM，请执行以下操作：

1. 在 Hyper-V 管理器中，在 Hyper-V 服务器上单击鼠标右键，然后选择新建 > 虚拟机。



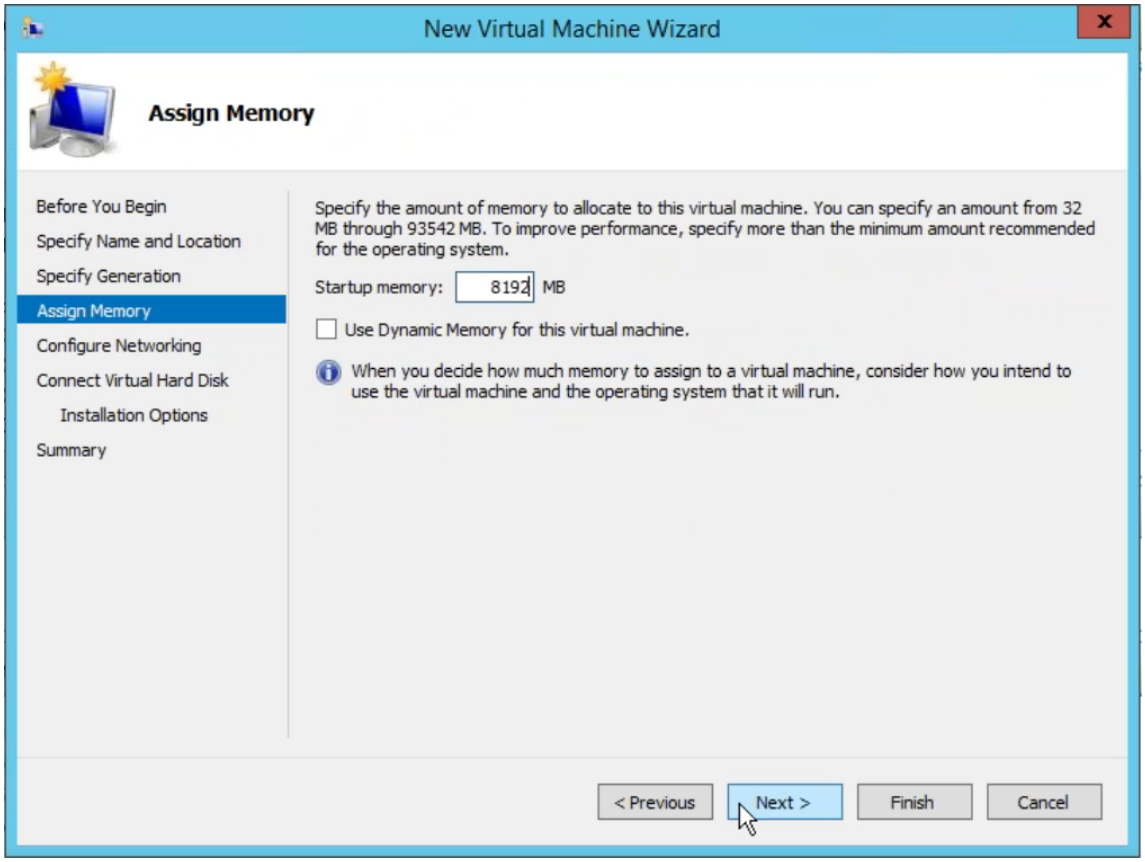
   此时将显示新建虚拟机向导。单击下一步。

2. 指定 SD-WAN Center VM 的名称，并更改 VM 存储位置（如有必要）。单击下一步。

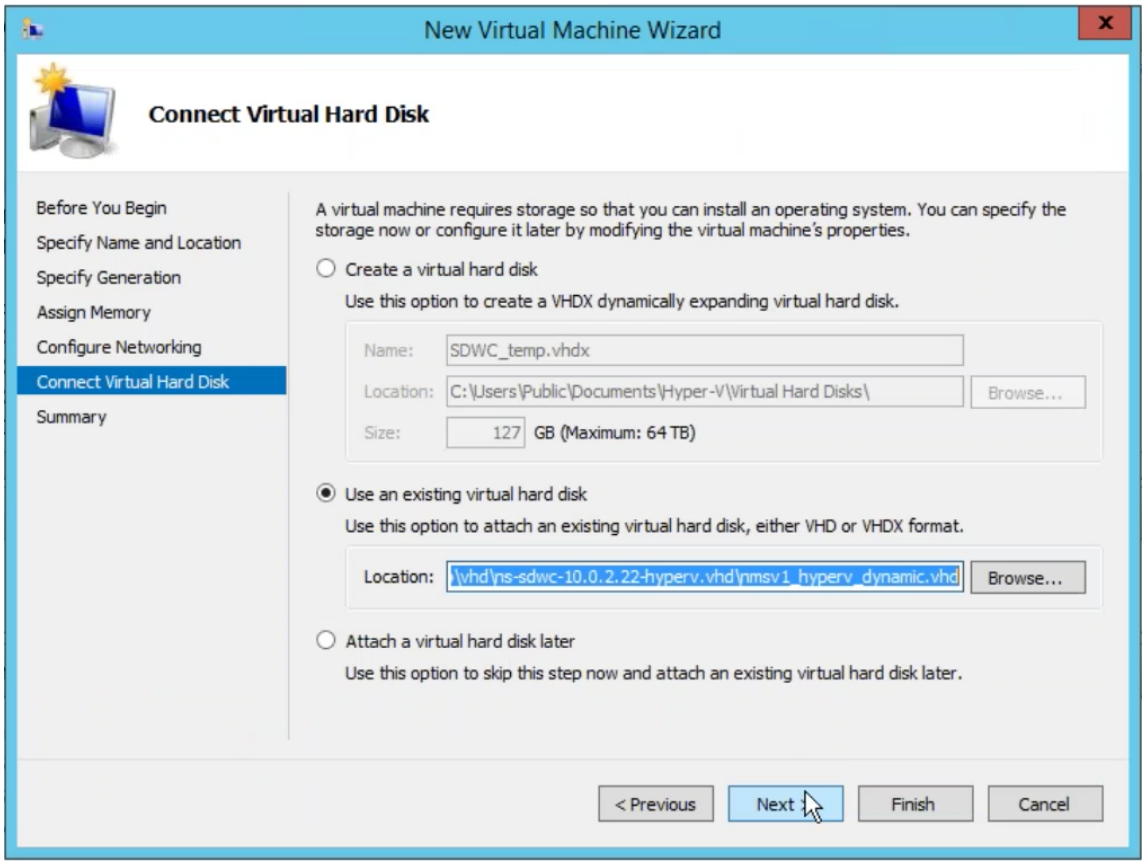


3. 选择所需的虚拟机生成。单击下一步。
4. 为虚拟机分配 8 GB 的内存。单击下一步。

> 注意
>
> Citrix SD-WAN Center VM 至少需要 8 GB 内存才能管理最多 64 个站点。有关内存与站点映射数量的详细信息，请参阅系统要求和安装。

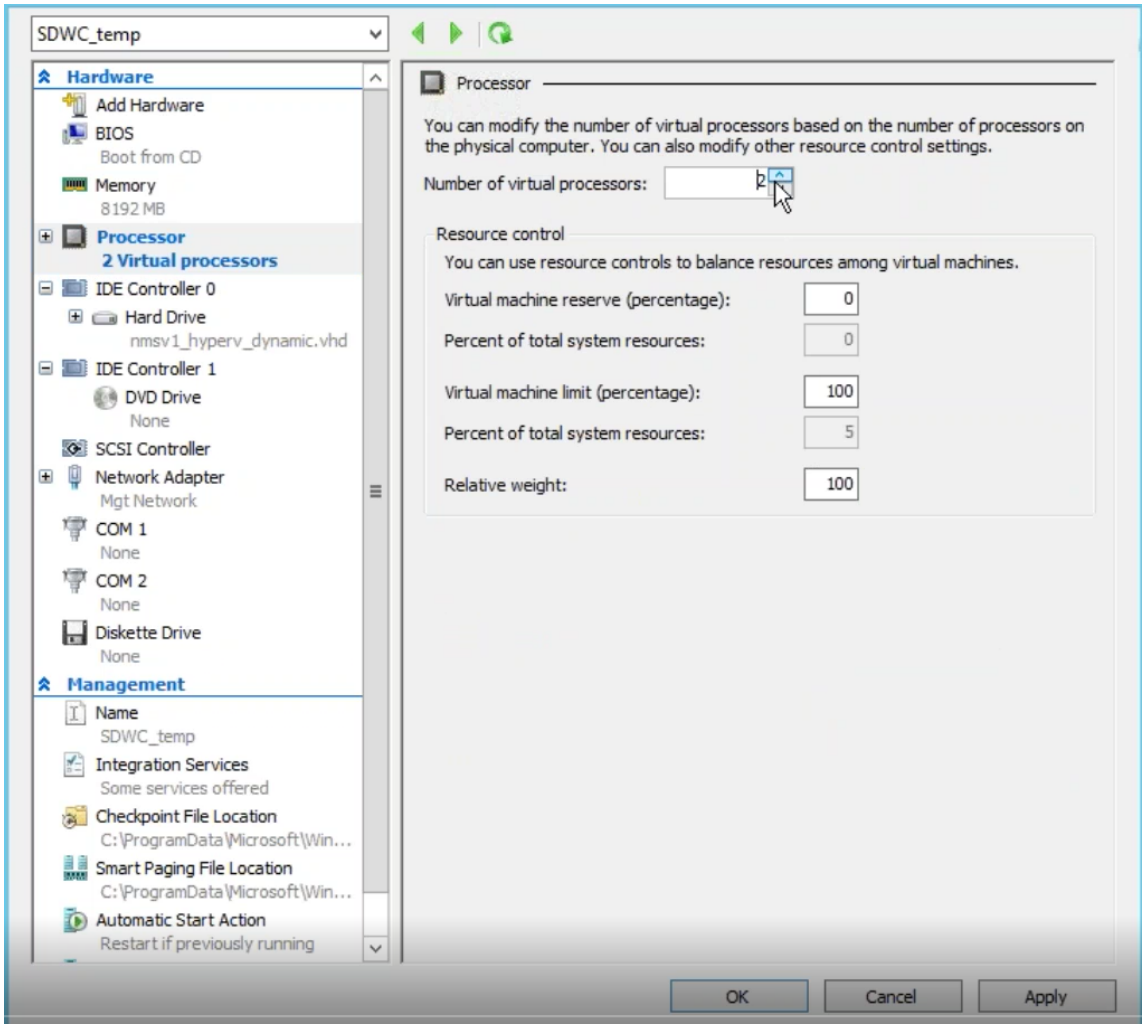


5. 选择要由 VM 的网络适配器使用的虚拟交换机，单击下一步。
6. 选择使用现有虚拟硬盘，浏览并选择您下载的 SD-WAN Center VHD 文件。单击下一步。

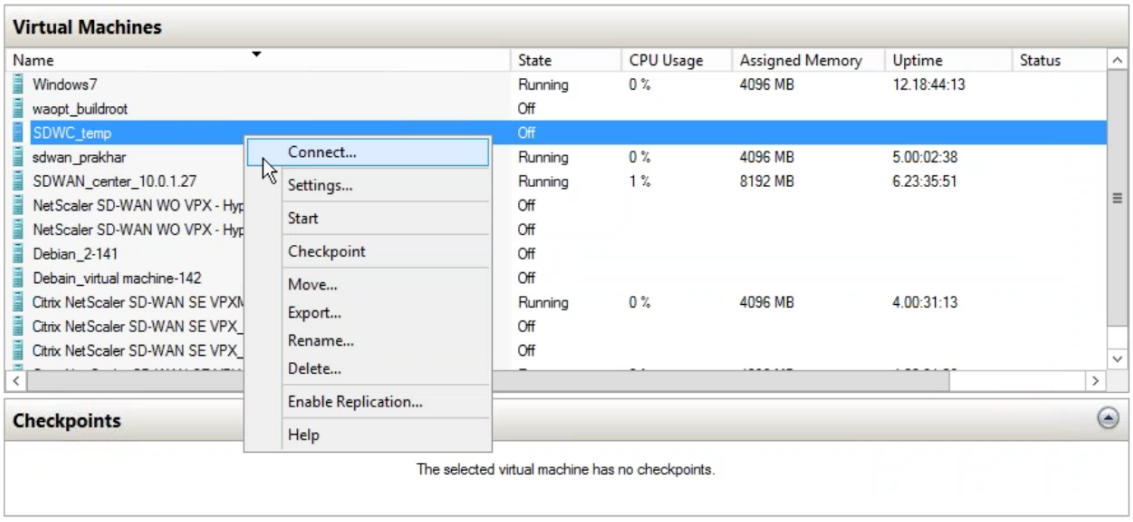


7. 检查 VM 摘要并更改设置（如有必要），或者单击完成。此时将创建 SD-WAN Center VM，该 VM 将在虚拟机部分中列出。

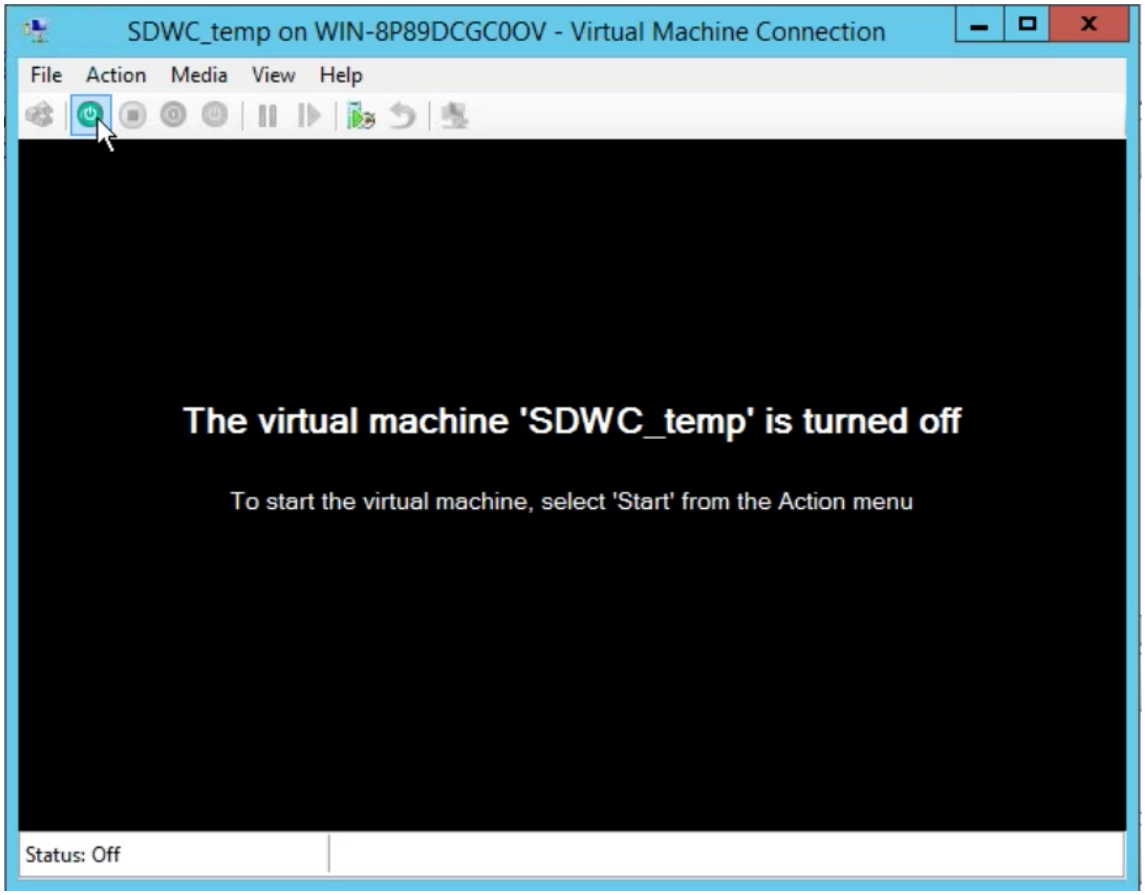
8. 在 SD-WAN Center VM 上单击鼠标右键，然后选择设置。将虚拟处理器的数量设置为 4，然后单击应用。



9. 在 SD-WAN Center VM 上单击鼠标右键，然后单击连接。

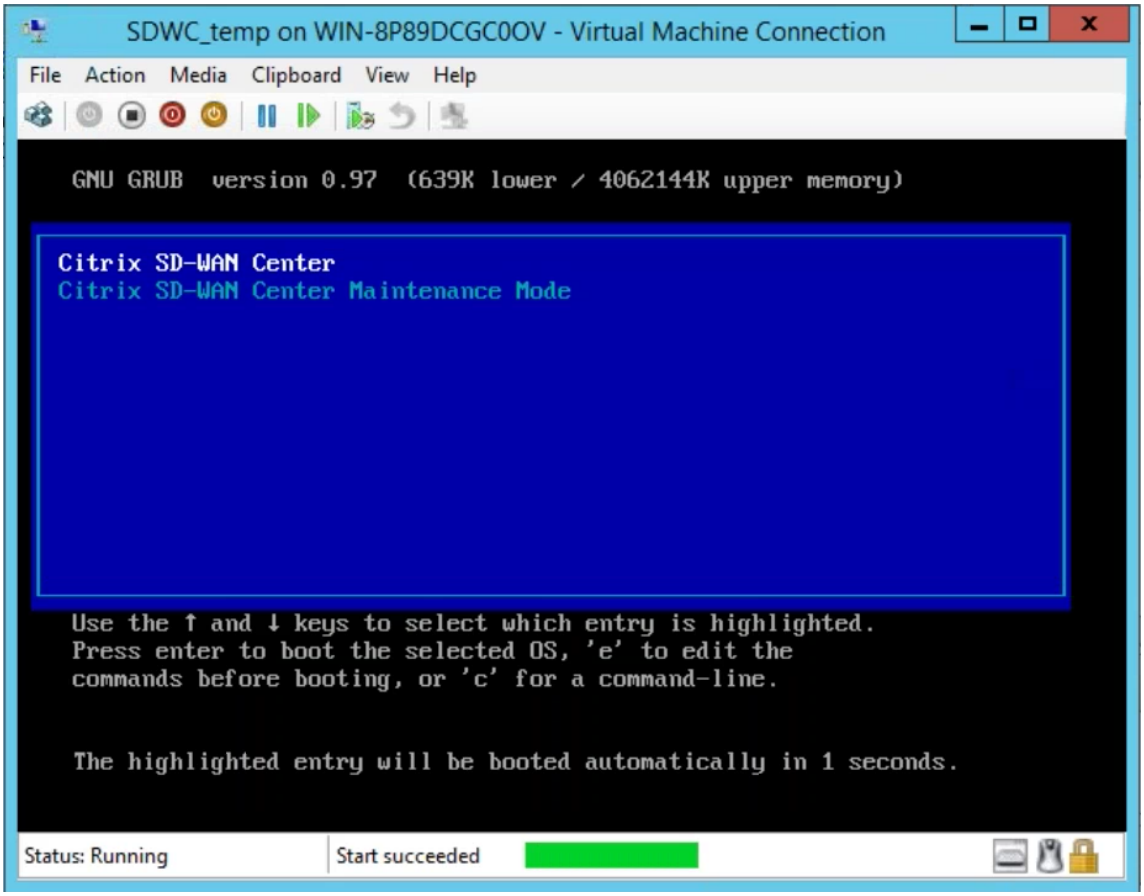


10. 单击开始按钮。



> 注意
>
> 初始安装可能最多需要 50 分钟，具体取决于您配置的 CPU 和 RAM 的数量。

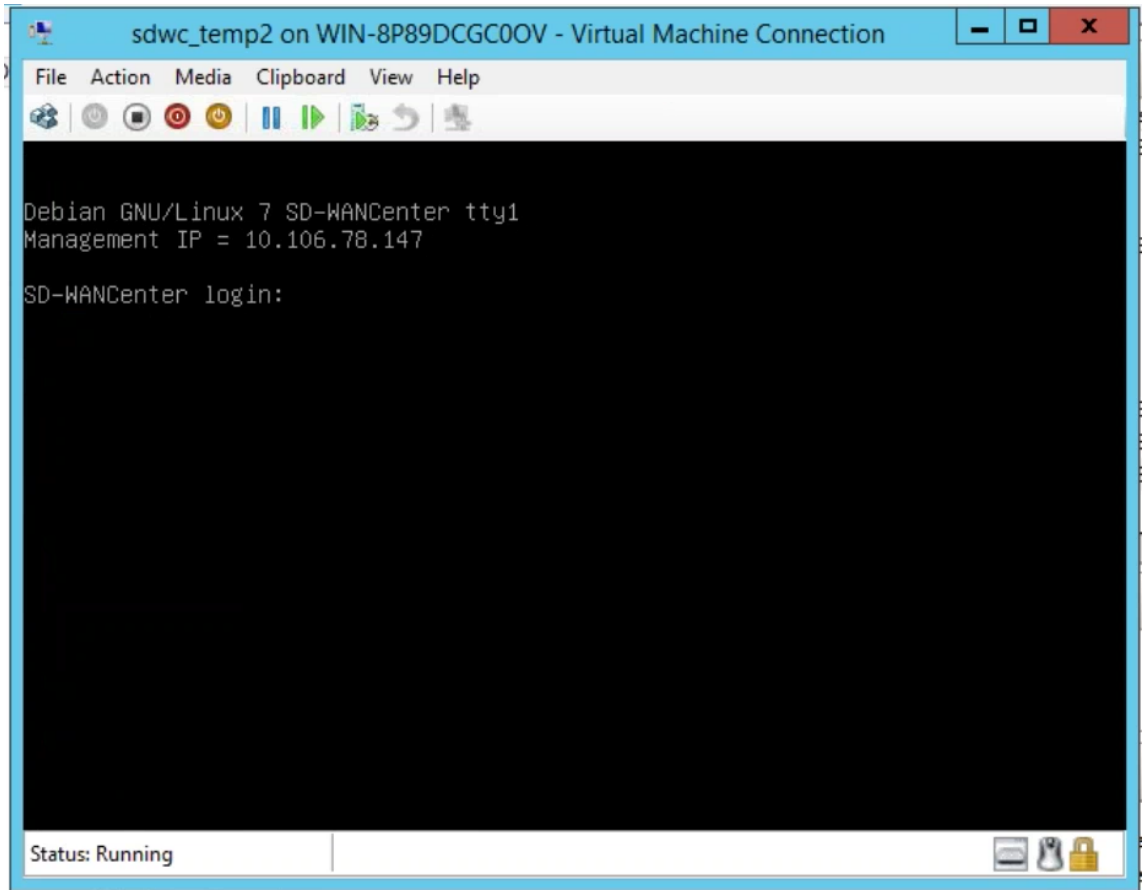
11. 启动 VM 后，选中 Citrix SD-WAN Center 并按 Enter 键。



12. 登录到虚拟机。新 SD-WAN Center VM 的默认登录凭据如下所示：

    登录：admin

    Password（密码）：password



管理 IP 地址在控制台中显示使用此 IP 访问 SD-WAN Center Web 界面。

> 注意
>
> 如果未在 SD-WAN 网络中配置 DHCP，则必须手动输入静态 IP 地址。

要将静态 IP 地址配置为管理 IP 地址，请执行以下操作：

1. 登录虚拟机。新 SD-WAN Center VM 的默认登录凭据如下所示：

   登录：admin

   Password（密码）：password

2. 在控制台中，输入 CLI 命令 ***management_IP***。
3. 输入命令 **set interface <ipaddress> <subnetmask> <gateway>**，以配置管理 IP。

使用管理 IP 访问 Citrix SD-WAN Center Web 界面。

Azure Marketplace 中使用解决方案模板的 Citrix SD-WAN Center

April 13, 2021

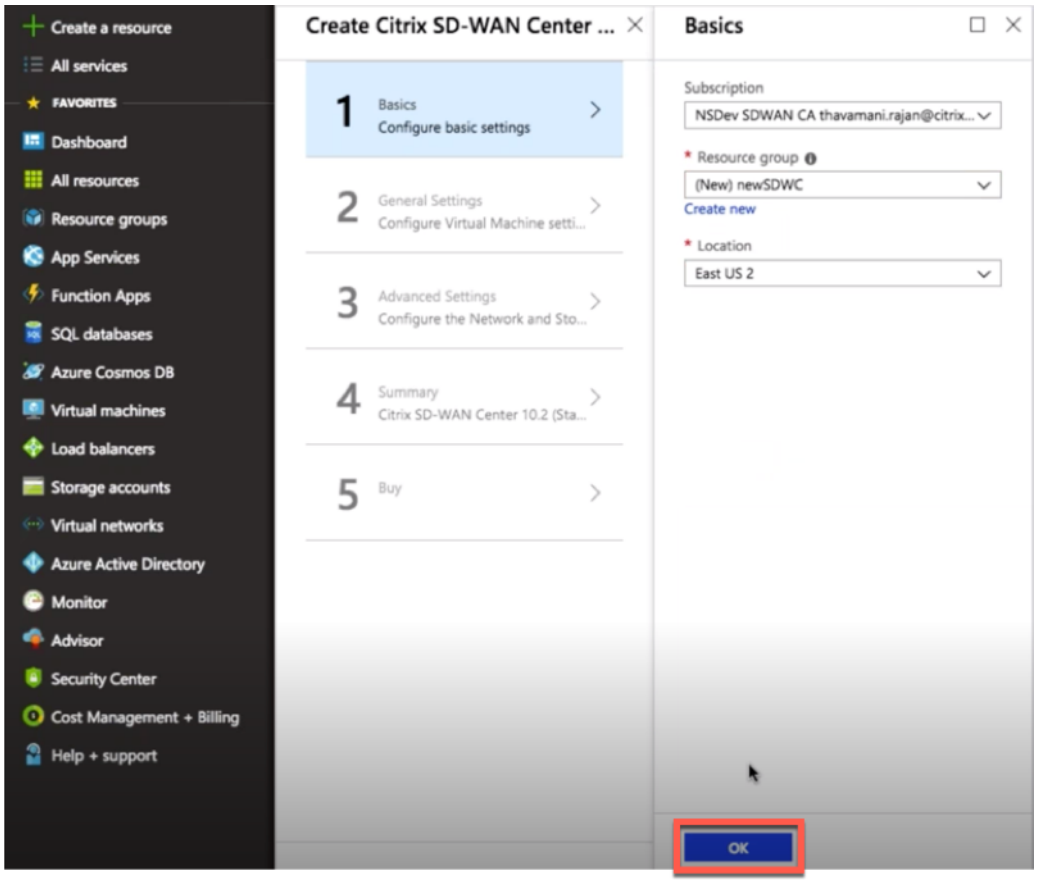
Citrix SD-WAN Center 现在可以在 Azure Marketplace 中使用。可以使用解决方案模板在 Azure 云中将 Citrix SD-WAN Center 部署为虚拟机 (VM)。

在 Microsoft Azure 上安装 Citrix SD-WAN Center 虚拟机 (VM) 之前，请收集必要的信息，如系统要求和安装中所述。

确保您有权访问 Microsoft Azure。

要在 Microsoft Azure 上部署 Citrix SD-WAN Center VPX，请执行以下操作：

1. 在 Microsoft Azure 中，导航到主页 **>** 商城。搜索并选择 **Citrix SD-WAN Center**。
2. 在 **Citrix SD-WAN Center** 页面上单击创建。此时将显示创建 **Citrix SD-WAN Center** 页面。
3. 在基础部分中，选择订阅类型、资源组和位置。单击确定。

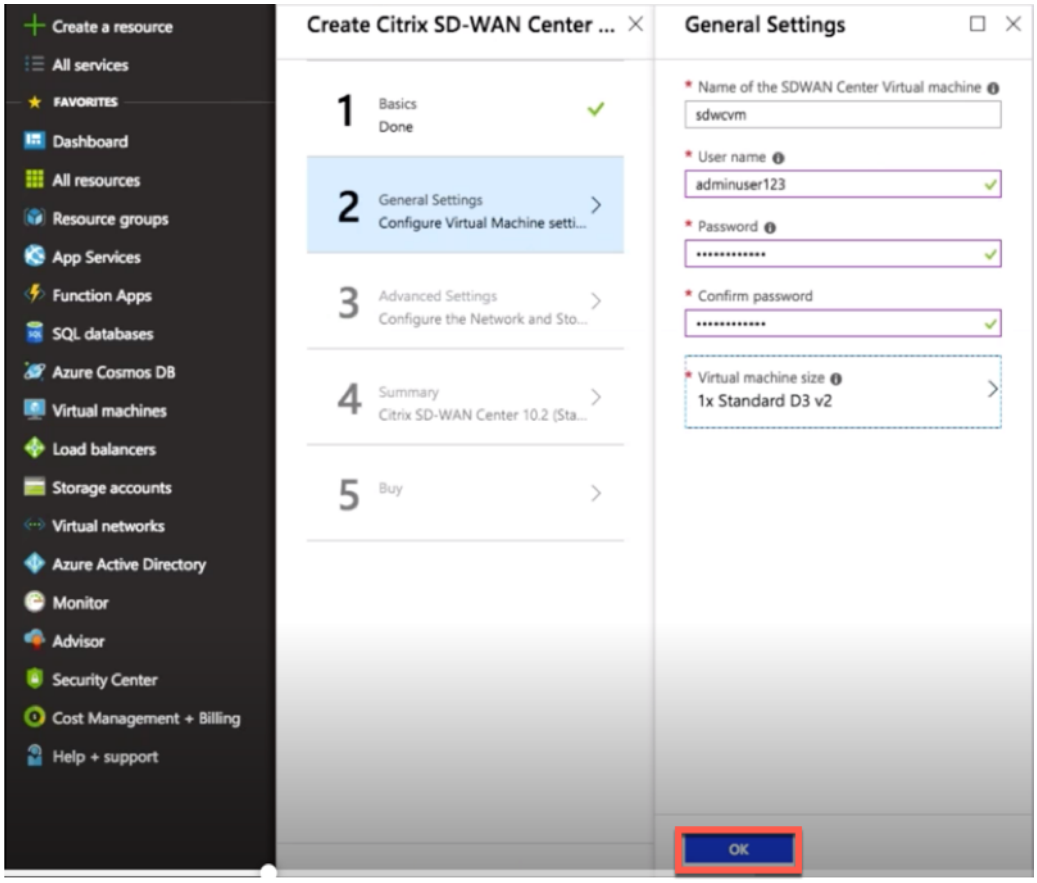


> 注意：
>
> 资源组是一个容器，用于保存 Azure 解决方案的相关资源。资源组可以包括解决方案的所有资源，或者仅

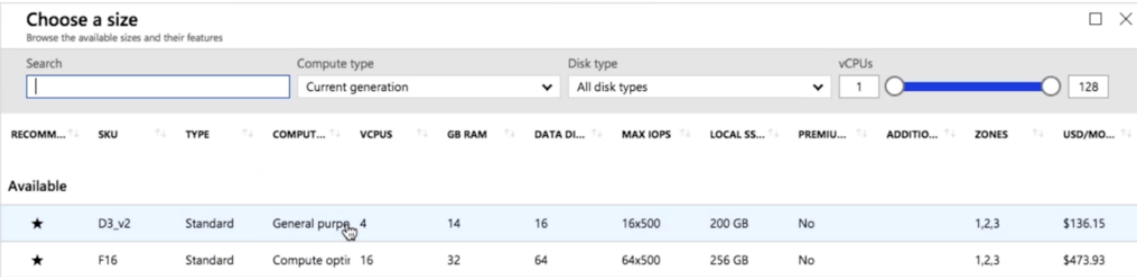
> 包括要作为一个组管理的资源。根据您的部署情况，您可以决定如何为资源组分配资源。

4. 在常规设置部分中，输入为 Citrix SD-WAN Center 虚拟机提供管理员级别访问或权限的名称和凭据。

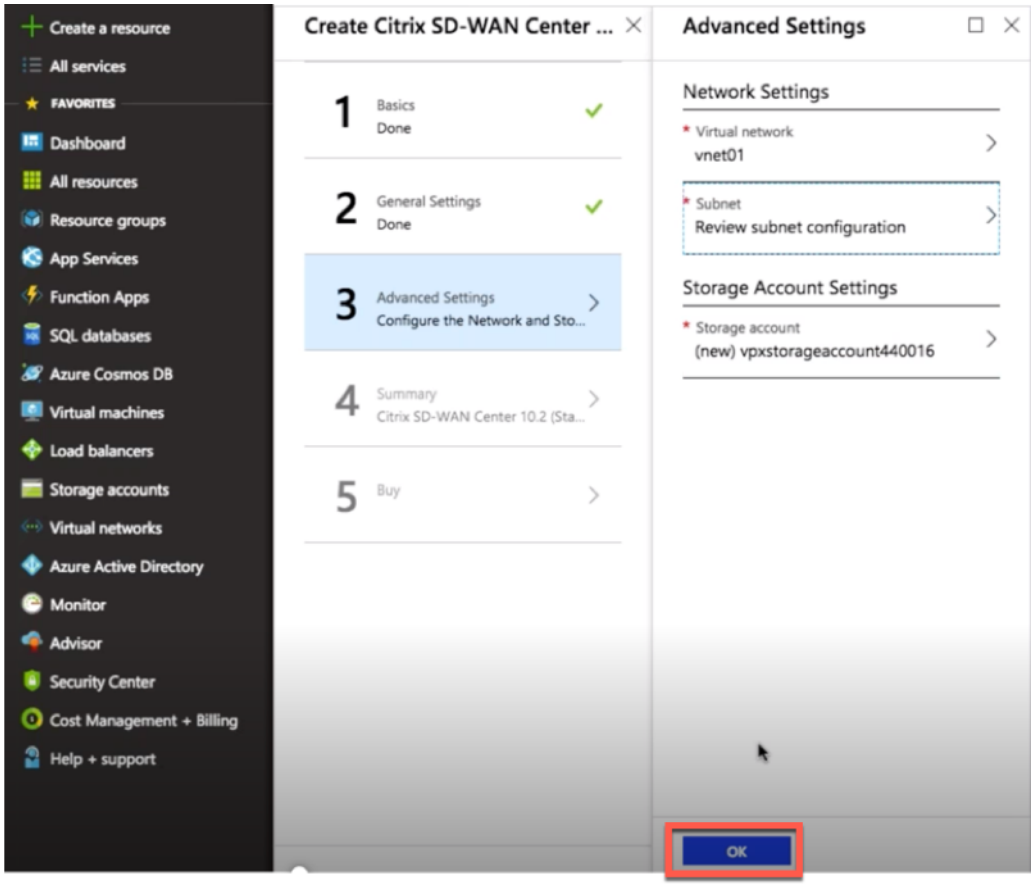
   在此步骤 4 中提供的凭据还将用于为管理员用户登录帐户设置密码（默认管理员帐户密码可以使用此密码凭据进行修改）。单击确定。



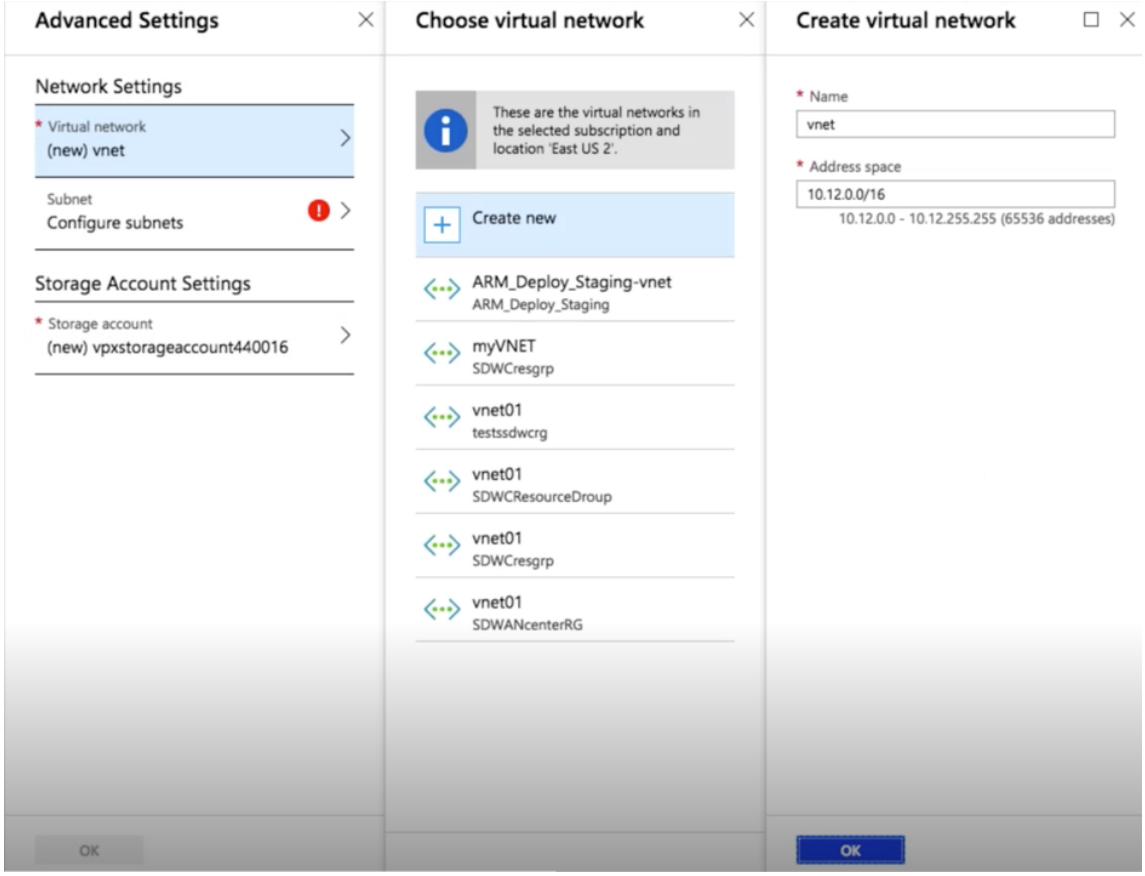
> 注意：
>
> 目前有两种大小的实例类型可用—**Standard_D3_v2** 和 **Standard_F16**。D3_v2 实例可用于监视最多具有 64 个站点的网络。要监视最多包含 128 站点的网络，F16 实例非常有用。您还可以搜索和选择可用的虚拟机大小。



5. 在高级设置部分中，根据要监视的站点数，为 **Citrix SD-WAN Center VPX** 配置网络和存储帐户设置。

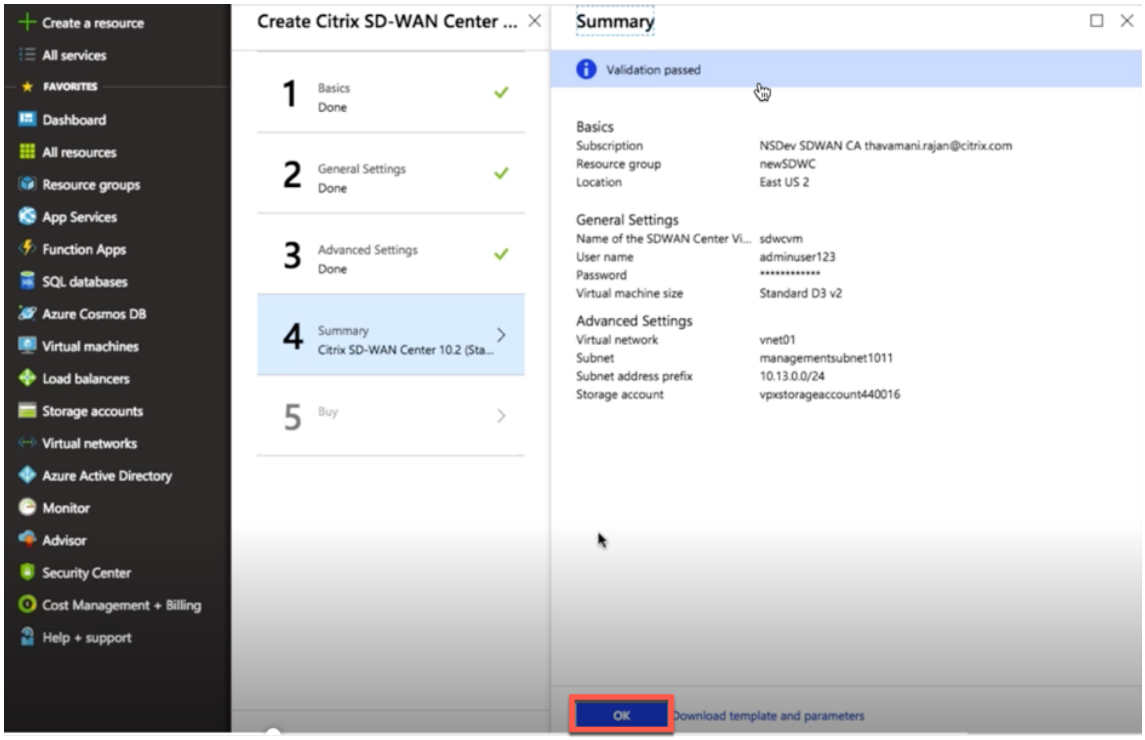


从可用列表中选择虚拟网络，或者通过提供名称和地址空间来创建新的虚拟网络。

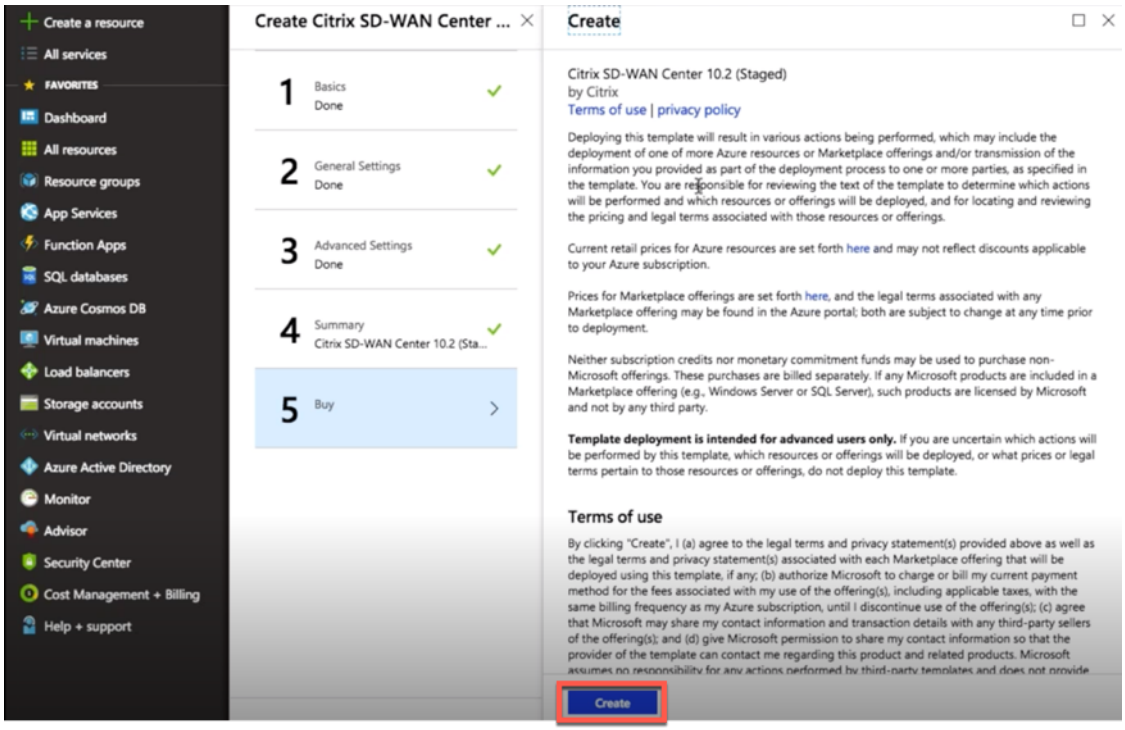


从下拉列表中选择子网。创建一个存储帐户并单击确定。

6. 验证并应用您在前面的步骤中提供的配置。如果配置正确，则将显示验证已通过消息。单击确定。



7. 成功部署后，将显示创建页面。仔细阅读使用条款和隐私政策策略，然后单击创建。



等待 VM 预配完成，然后使用已分配给该 VM 的 IP 登录（通过检查网络连接部分并使用管理员凭据（在步骤 4 中设置），然后按照通用 SD-WAN Center 部署指导方针进行登录。

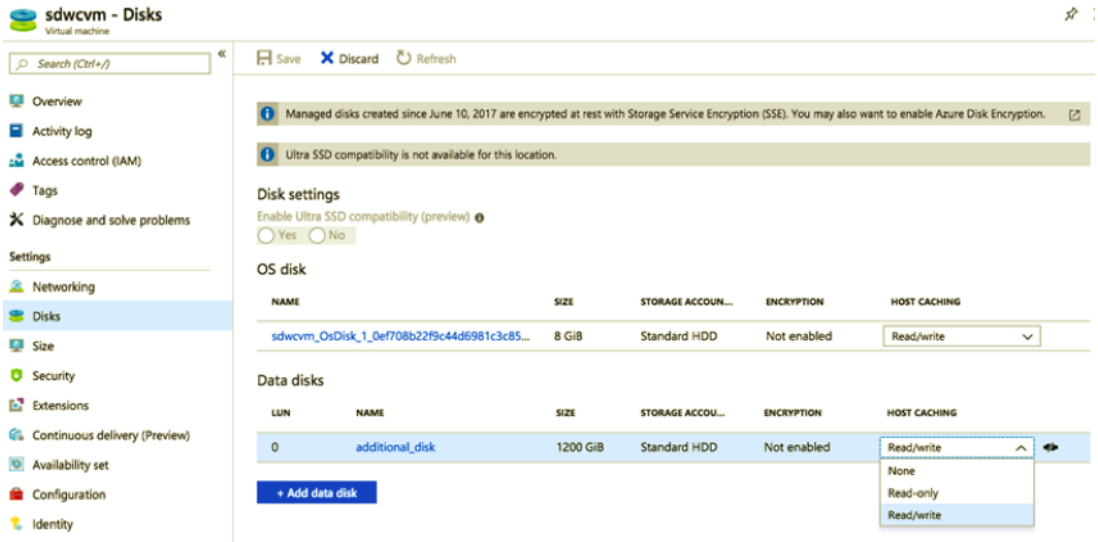
添加数据盘

本节介绍如何使用 Azure 门户将新的托管数据磁盘连接到虚拟机 (VM)。虚拟机大小决定了可以连接多少个数据磁盘。

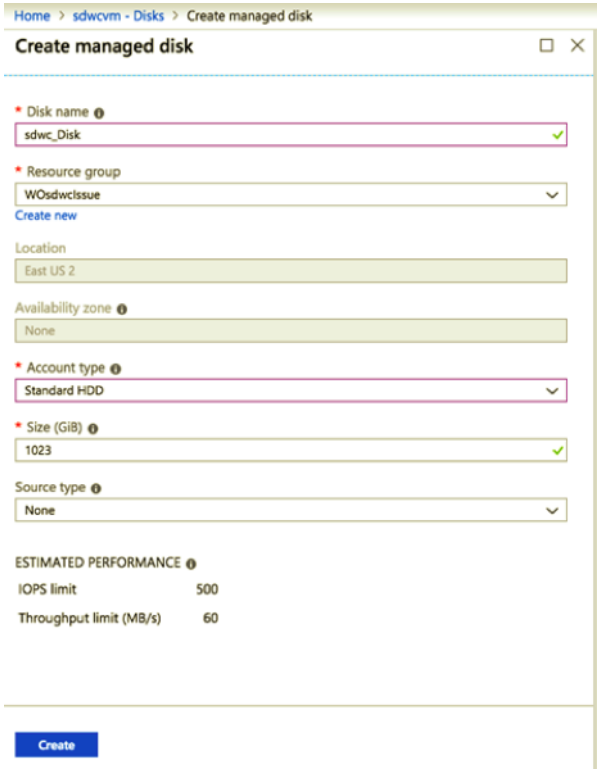
在 Azure 门户中，从左侧的菜单中选择虚拟机，然后从列表中选择虚拟机。

执行以下操作以在 Azure SD-WAN Center 中添加其他数据磁盘：

1. 关闭 VM。
2. 在 VM 控制板中，选择设置部分下的磁盘。



3. 单击 **+** 添加数据磁盘，然后创建具有读取和写入权限的新数据磁盘。



通过填写以下必需的详细信息来连接磁盘：

- 磁盘名称-提供 SD-WAN Center 数据磁盘的名称。
- 资源组–从下拉列表中选择资源组。
- 账户类型—从下拉列表中选择账户类型。
- 大小 **(GIB)**–以 GB 为单位提供大小。
- 存储类型 -从下拉列表中选择源类型。

4. 完成操作后，单击确定。

要打开 VM，请参阅将活动存储切换到新数据存储主题。

AWS 上 VM 可导入映像格式的 Citrix SD-WAN Center

April 13, 2021

Citrix SD-WAN Center 是一个集中式管理系统或一个透明的玻璃管理解决方案，使企业能够在其 WAN 上配置、监视和分析所有 Citrix SD-WAN 设备。

在 **AWS** 上实例化 **SD-WAN Center** 虚拟设备 **(AMI)**

要在 AWS VPC 中安装 SD-WAN Center 虚拟设备，需要使用 AWS 帐户。可以在此处创建一个 AWS 帐户。SD-WAN Center 在 AWS Marketplace 中以 Amazon 计算机映像 (AMI) 的形式提供。

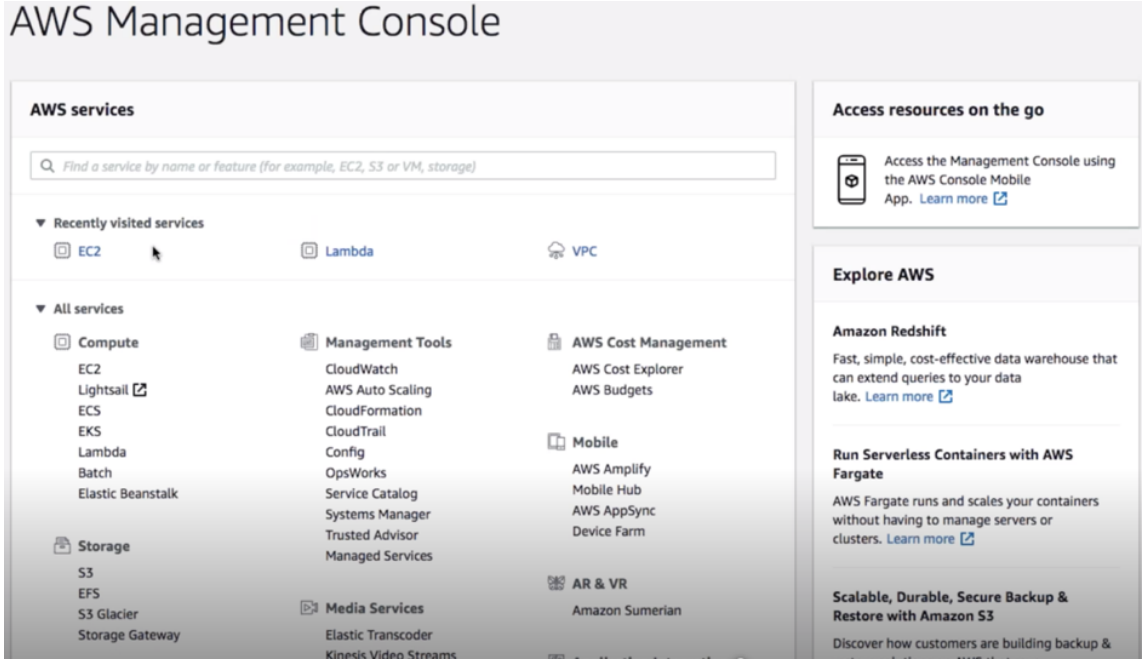
> 注意：
>
> Amazon 频繁更改其 AWS 页面，因此以下说明可能不是最新的。

可以通过两种方法在 AWS 上实例化 SD-WAN Center 虚拟设备 (AMI)：

1. 第一种方法：在 Web 浏览器中，键入 http://aws.amazon.com/。在“我的帐户”下选择 AWS 管理控制台，以打开 Amazon Web Services (AWS)。

   第二种方法：
   在 Web 浏览器中，键入 http://console.aws.amazon.com 以打开 **Amazon Web Services**。

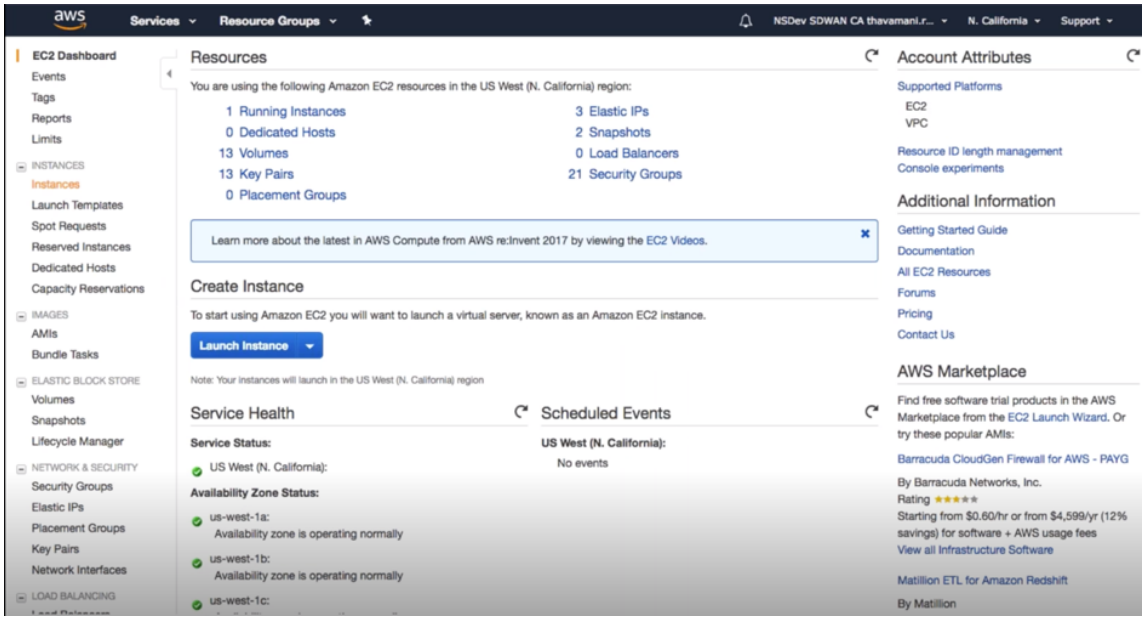
2. 使用您的 AWS 帐户证书登录。这将带您进入 **Amazon Web Services** 页面。您可以查看最 近访问过的服务列表以及所有其他服务。



   Citrix SD-WAN Center 设备将 EC2 作为 AWS 服务实例提供。

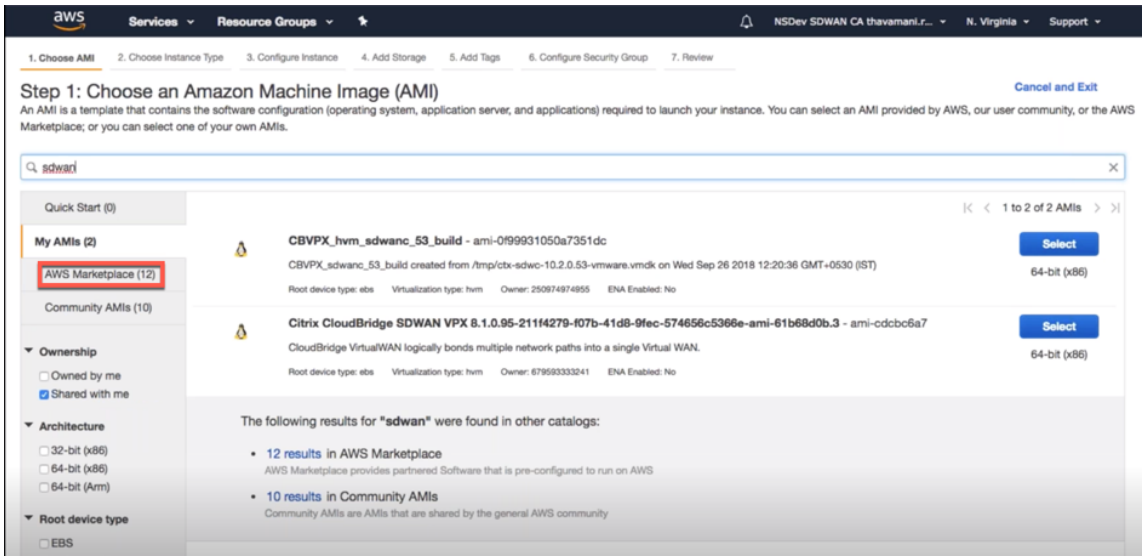
   - **EC2** 控制面板 -弹性计算云，可调整大小的虚拟服务/实例

3. 在计算部分单击 **EC2** ，然后选择启动实例。



您可以通过在左侧实例（实例）下方选择实例选项位置来选择启动实例选项或手动转至实例屏幕（请参阅以上屏幕截图）。

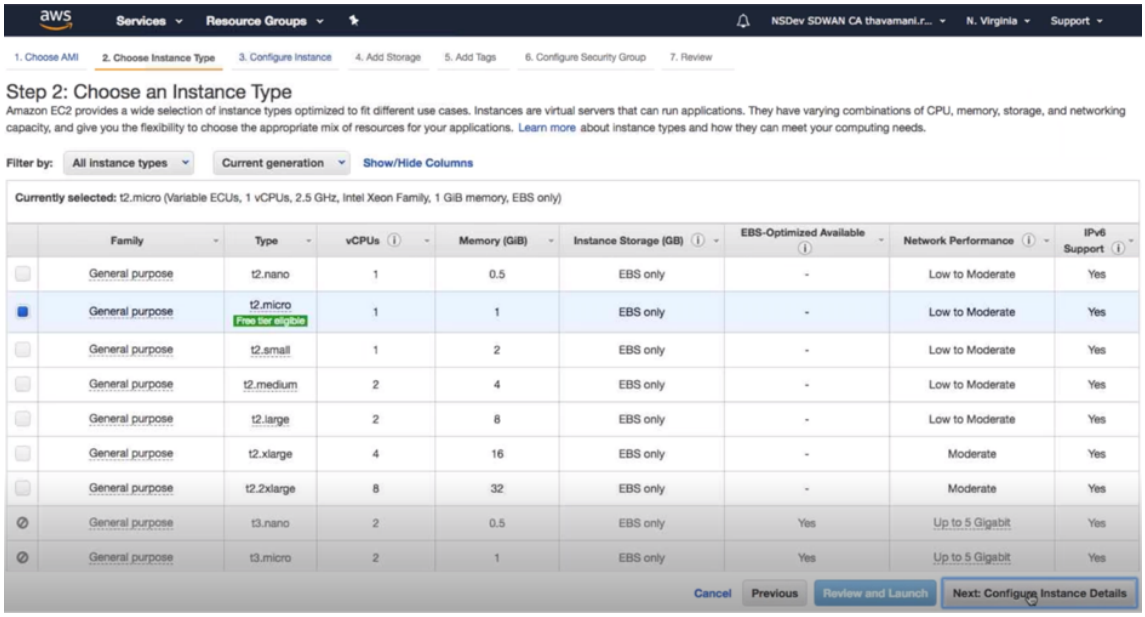
4. 在选择 **AMI** 页面上，单击 **AWS** 商城选项卡。
5. 在搜索文本字段中，键入 SD-WAN 以搜索 SD-WAN AMI，然后单击搜索。



在搜索结果页面上，从 AMI 的最新版本中选择一个 Citrix SD-WAN Center，然后单击选择。

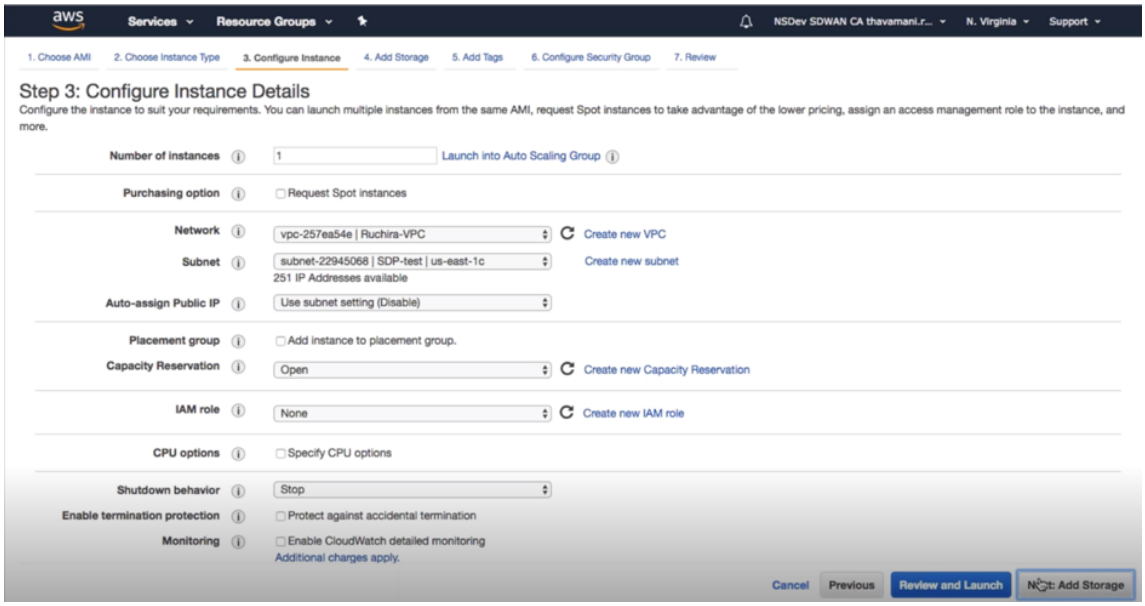
AMI 模板包含软件配置，包括操作系统、应用程序服务器和应用程序。要启动实例，此模板是必需的。

6. 选择实例类型，然后选择下一步**:** 配置实例详细信息。您可以通过选择特定实例类型或当前一代的所有实例类型来筛选搜索。

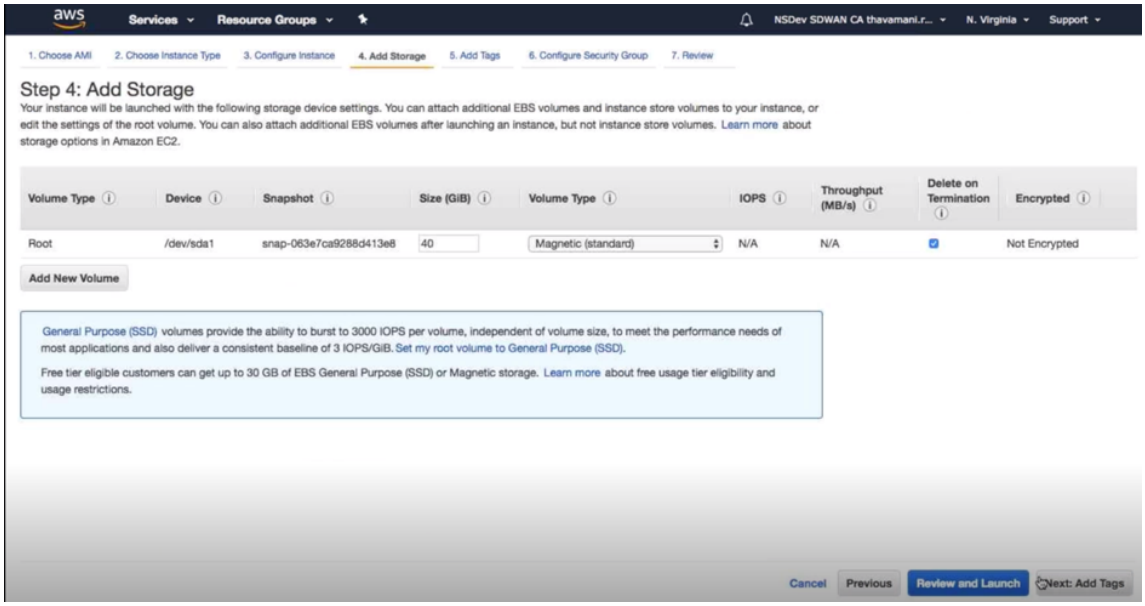


Amazon EC2 提供了多种针对不同使用案例而优化的实例类型。实例是可以运行应用程序的虚拟服务器。

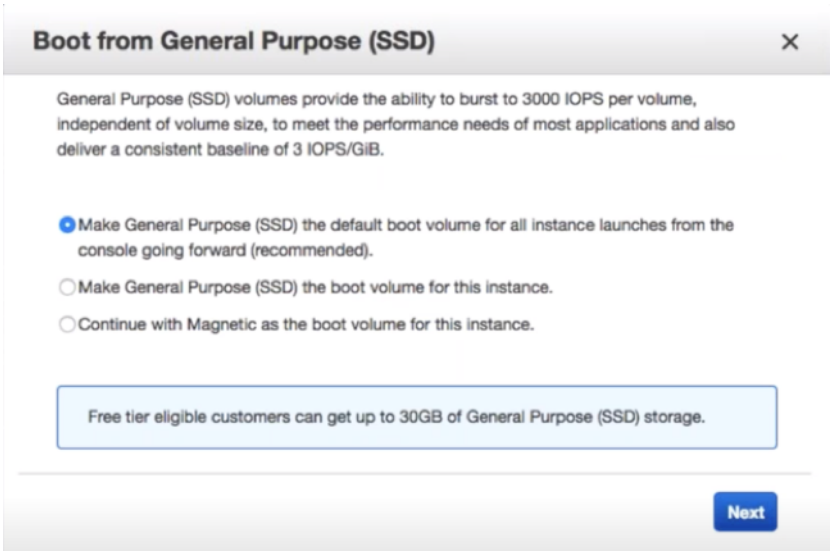
7. 在配置实例页面上，在实例数文本框中键入 1，然后根据需要填写特定实例的其他详细信息，例如“网络”、“子网”等。单击下一步**:** 添加存储。



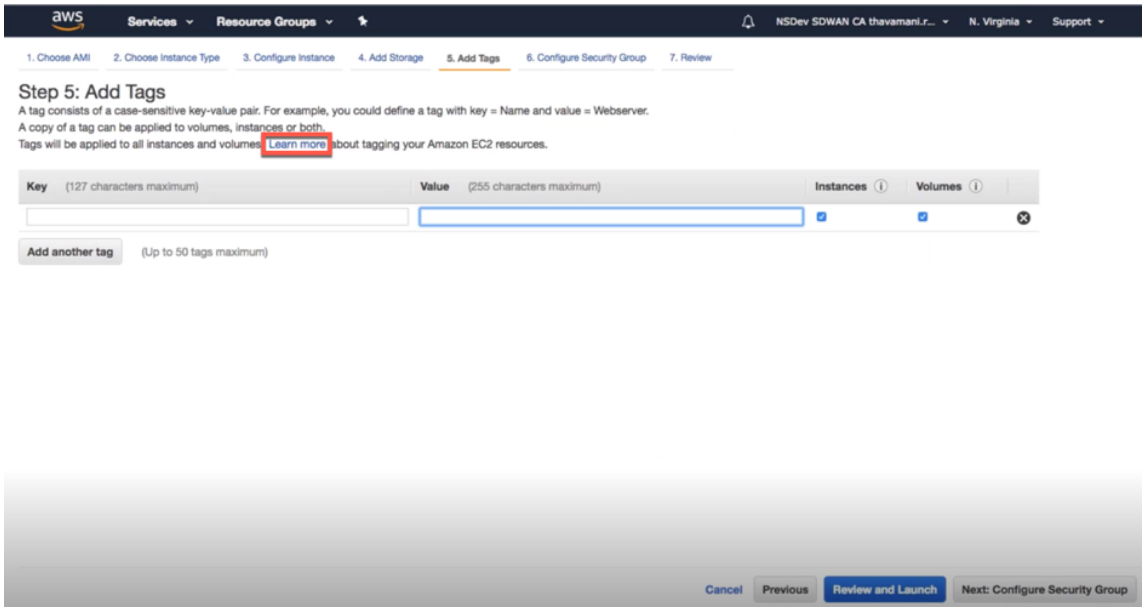
8. 实例使用存储设备设置启动。可以在预配实例后单独添加新的卷。



9. 根据您的要求，单击检查和启动以选择“引导卷”选项。单击下一步。



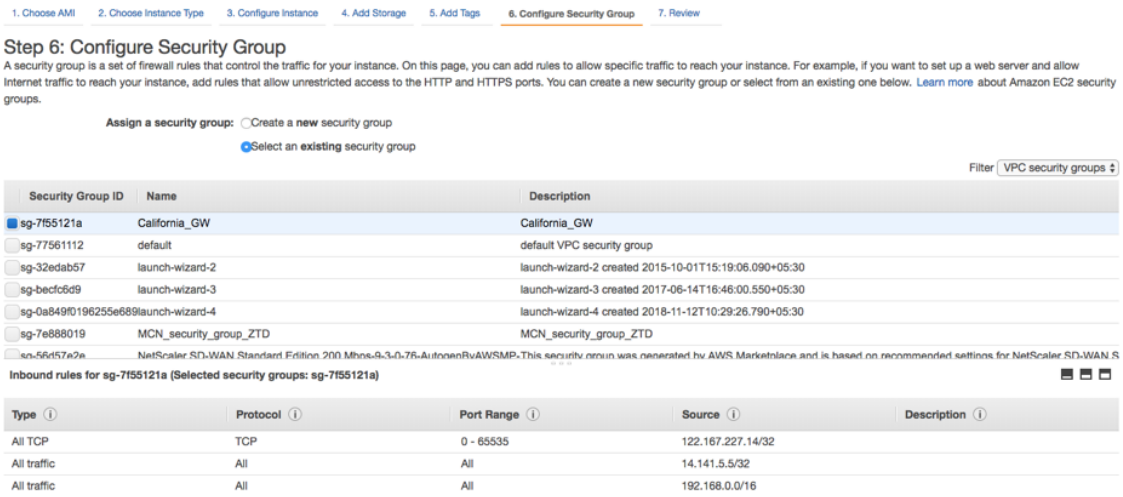
10. 添加或定义具有键名称和值的标签。单击了解详细信息以了解有关标记的详细信息。您最多可以添加 50 个标签。单击下一步：配置安全组。



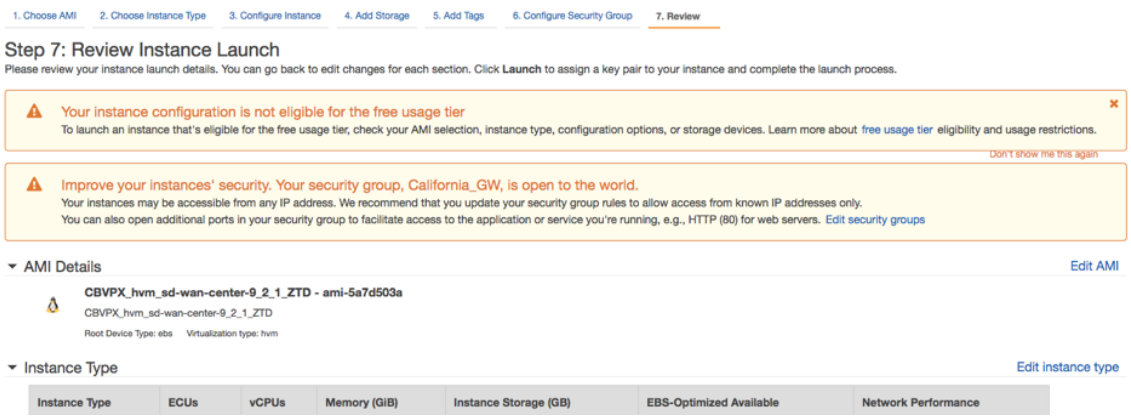
> 注意：
>
> 注意：标记密钥长度必须介于 1 到 127 个字符之间。

11. 您可以创建一个常规安全组来帮助控制实例的流量。可以创建新安全组，也可以从列表中选择现有安全组。

> 注意：
>
> 确保安全组允许通过 2156 端口的入站连接从 Citrix SD-WAN 设备收集数据。



12. 查看实例启动详细信息，然后单击启动。此时将显示一个弹出框，要求您创建密钥对。必须为实例创建密钥对。



双重身份验证

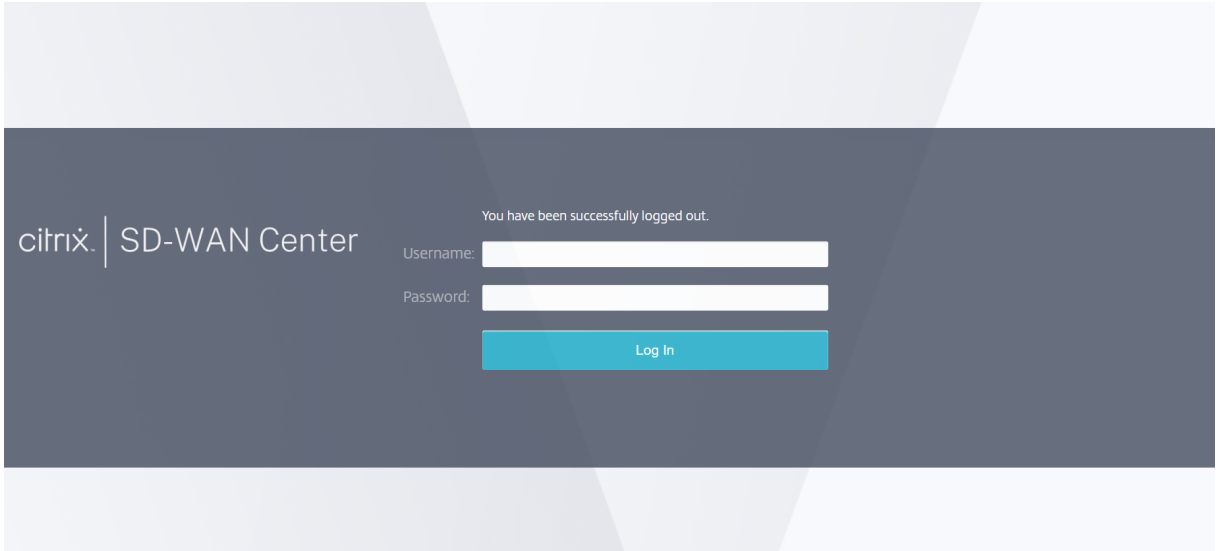
April 13, 2021

双重身份验证 (TFA) 提供了两种身份验证因素，以获取本地和远程用户帐户 Citrix SD-WAN Center 的访问权限。它在 Citrix SD-WAN Center 登录顺序中引入了一个额外的安全层。

通过使用 Citrix SD-WAN Center 上配置的密码完成本地用户帐户的第一层身份验证。有关详细信息，请参阅用户帐户。

通过使用主 RADIUS 或 TACACS+ 身份验证服务器，对远程用户帐户进行第一级身份验证。有关详细信息，请参阅主身份验证。

可以为本地和远程用户帐户配置额外的辅助 RADIUS 或 TACACS+ 身份验证服务器以启用双重身份验证。有关详细信息，请参阅二级身份验证。



Citrix SD-WAN Center 登录凭据：

- 用户名：在 SD-WAN Center 或主身份验证服务器上配置的用户名。
- 密码：在 SD-WAN Center 或主身份验证服务器上配置的密码。
- 二级密码：在辅助身份验证服务器上配置的密码。

> 注意
>
> 仅当配置了辅助身份验证服务器时，才会显示二级密码选项。

主身份验证

April 13, 2021

您可以配置诸如 RADIUS 或 TACACS+ 之类的身份验证服务器，对登录到 Citrix SD-WAN Center 的远程用户进行身份验证。在启用了双重身份验证的情况下，主要身份验证是远程用户的第一个身份验证系数。有关详细信息，请参阅双重身份验证。

> 注意
>
> 确保在所需的身份验证服务器上创建用户帐户。

RADIUS 身份验证服务器

要使用 RADIUS 身份验证，必须至少指定并配置一个 RADIUS 服务器。(可选）配置冗余备份服务器，最多包含三个 RADIUS 服务器。服务器将按顺序进行检查，首先从服务器部分列出的服务器开始。确保在 RADIUS 身份验证服务器上创建了所需的用户帐户。

要启用并配置 RADIUS 身份验证，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，导航到管理 > 用户/身份验证设置。
2. 在主身份验证 > **RADIUS** 身份验证部分中，选中启用 **RADIUS** 身份验证复选框。

   > 注意
   >
   > 如果 TACACS+ 身份验证已启用，则将处于禁用状态。

3. 在超时字段中，输入等待来自 RADIUS 服务器的身份验证响应的时间间隔（以秒为单位）。

   超时值应小于或等于 10 秒。

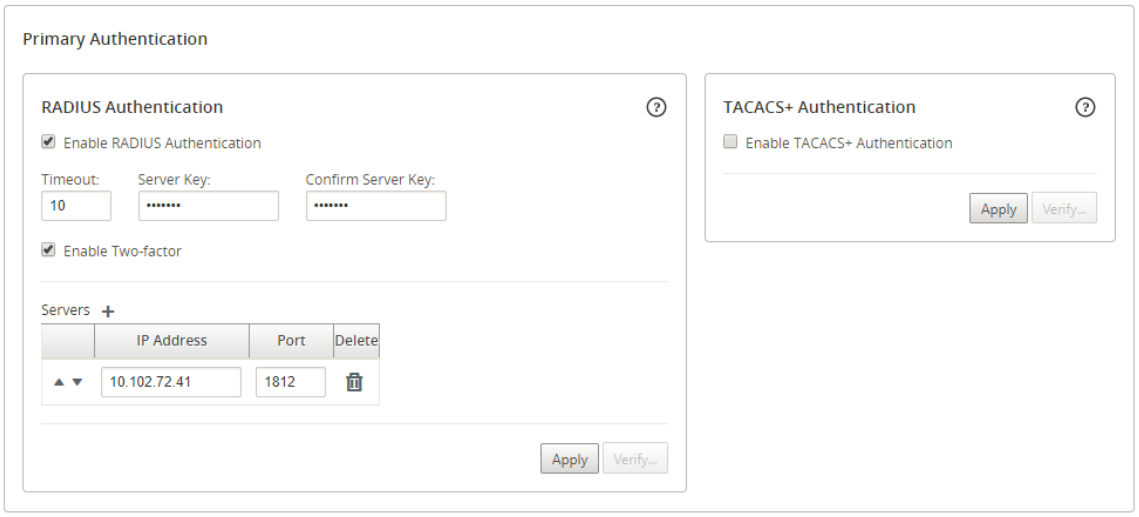
4. 在服务器密钥字段中，输入连接到 RADIUS 服务器时要使用的密钥。
5. 在确认服务器密钥字段中，重新输入密钥。

> 注意
>
> 超时和服务器密钥设置适用于所有已配置的服务器 **。**

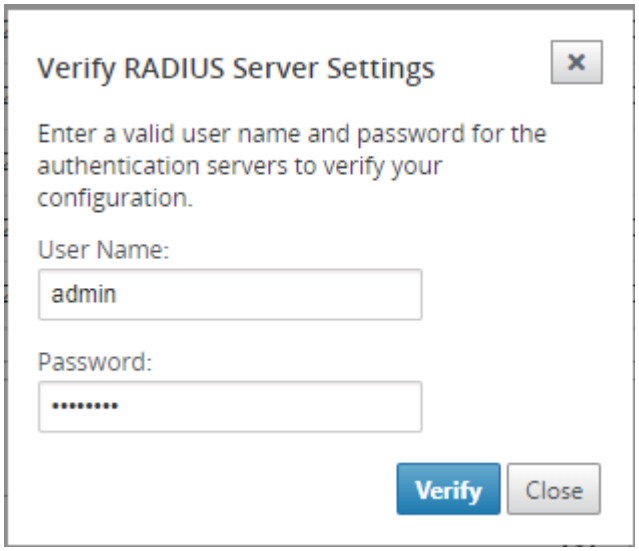
6. 选择启用双重身份验证以启用双重身份验证。

> 注意
>
> 仅当配置了辅助身份验证服务器时，才会显示启用双重选项。
>
> 配置辅助身份验证服务器（RADIUS 或 TACAS+）。有关详细信息，请参阅二级身份验证。

7. 单击服务器旁边的加号图标 (+) 以添加 RADIUS 服务器。
8. 在 **IP** 地址字段中，输入 RADIUS 服务器的主机 IP 地址。
9. 在端口字段中，输入 RADIUS 服务器的端口号。默认端口号为 1812。



10. 单击应用。
11. 单击验证以验证与 RADIUS 服务器的连接。此时将显示验证 **RADIUS** 服务器设置对话框。



12. 输入身份验证服务器的有效用户名和密码，然后单击验证。

要配置更多服务器，请重复步骤 7 到 12。

TACACS+ 身份验证服务器

要使用 TACACS+，必须至少指定并配置一个 TACACS+ 服务器。(可选）配置冗余备份服务器，最多可以包含三个 TACACS+ 服务器。服务器将按顺序进行检查，首先从服务器部分列出的服务器开始。确保在 TACACS+ 身份验证服务器上创建所需的用户帐户。

要启用和配置 TACACS+ 身份验证，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，导航到管理 > 用户/身份验证设置。
2. 在 主身份验证 > **TACACS+** 身份验证 部分，选中 启用 **TACACS+** 身份验证复选框。

   > 注意
   >
   > 如果已启用 RADIUS 身份验证，则将处于禁用状态。

3. 在超时字段中，输入等待来自 TACACS+ 服务器的身份验证响应的时间间隔（以秒为单位）。

   超时值应小于或等于 10 秒。

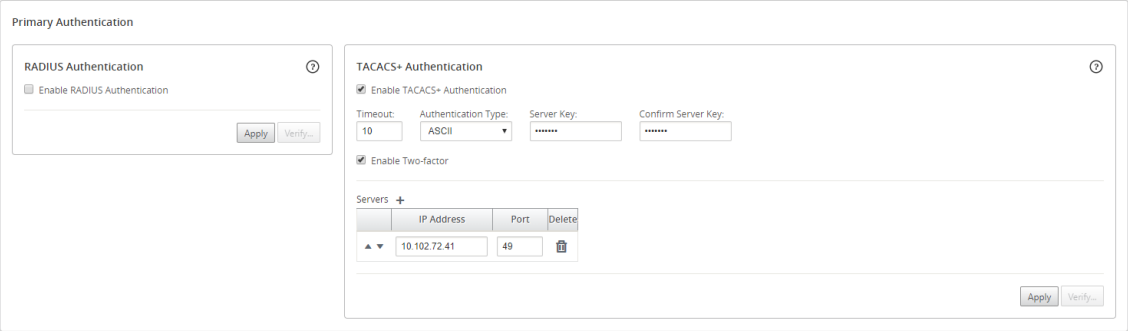
4. 在身份验证类型字段中，选择用于向 TACACS+ 服务器发送用户名和密码的加密方法。
5. 在服务器密钥字段中，输入连接 TACACS+ 服务器时要使用的密钥。
6. 在确认服务器密钥字段中，重新输入密钥。

   > 注意
   >
   > 超时、身份验证类型和服务器密钥设置将应用到所有已配置的服务器。

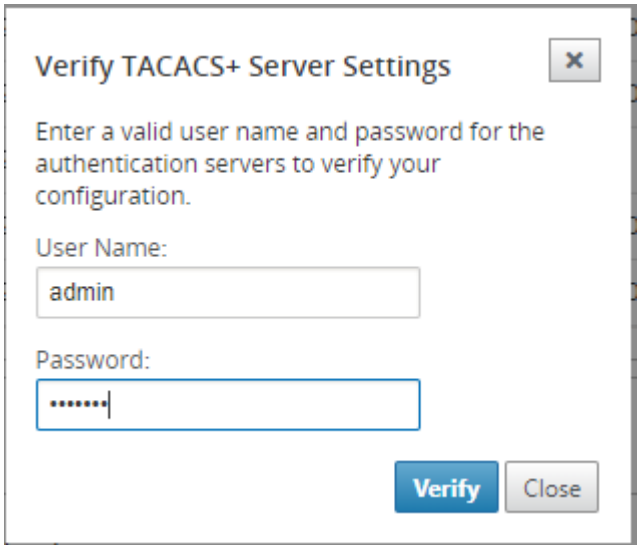
7. 选择启用双重身份验证以启用双重身份验证。

> 注意
>
> 仅当配置了辅助身份验证服务器时，才会显示启用双重选项。
>
> 配置辅助身份验证服务器（RADIUS 或 TACAS+）。有关详细信息，请参阅二级身份验证。

8. 单击服务器旁边的加号图标 (+) 以添加 TACACS+ 服务器。
9. 在 **IP** 地址字段中，输入 TACACS+ 服务器的主机 IP 地址。
10. 在端口字段中，输入 TACACS+ 服务器的端口号。默认端口号为 49。



11. 单击应用。
12. 单击验证以验证与 RADIUS 服务器的连接。此时将显示验证 **TACACS+** 服务器设置对话框。



13. 输入身份验证服务器的有效用户名和密码，然后单击验证。

    要配置更多服务器，请重复步骤 8 至 13。

二级身份验证

April 13, 2021

辅助身份验证配置为为本地和远程用户帐户启用双重身份验证。可以将 RADIUS 或 TACACS+ 身份验证服务器配置为辅助身份验证服务器。有关详细信息，请参阅双重身份验证。

> 注意
>
> 确保在所需的身份验证服务器上创建用户帐户。用户帐户密码将用作 Citrix SD-WAN Center 登录顺序中的第二个因素。

辅助 **RADIUS** 身份验证

要使用 RADIUS 身份验证，必须至少指定并配置一个 RADIUS 服务器。(可选）配置冗余备份服务器，最多包含三个 RADIUS 服务器。服务器将按顺序进行检查，首先从服务器部分列出的服务器开始。确保在 RADIUS 身份验证服务器上创建了所需的用户帐户。

要启用并配置 RADIUS 身份验证，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，导航到管理 > 用户/身份验证设置。
2. 在辅助身份验证 > **RADIUS** 身份验证部分中，选中启用辅助 **RADIUS** 身份验证复选框。

   > 注意
   >
   > 如果 TACACS+ 身份验证已启用，则将处于禁用状态。

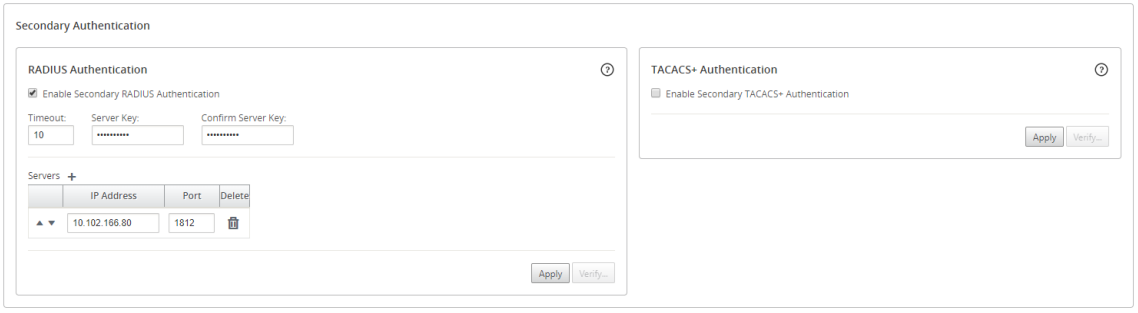
3. 在超时字段中，输入等待来自 RADIUS 服务器的身份验证响应的时间间隔（以秒为单位）。

   超时值应小于或等于 10 秒。

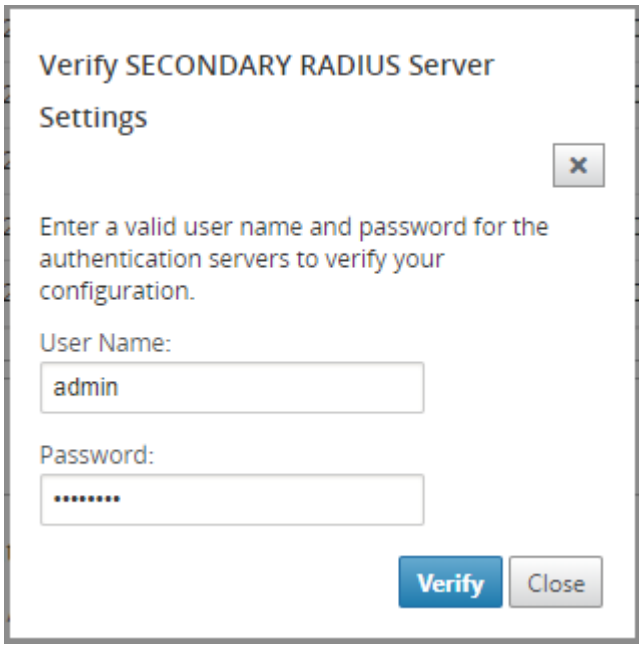
4. 在服务器密钥字段中，输入连接到 RADIUS 服务器时要使用的密钥。
5. 在确认服务器密钥字段中，重新输入密钥。

   > 注意
   >
   > 超时和服务器密钥设置适用于所有已配置的服务器 **。**

6. 单击服务器旁边的加号图标 (+) 以添加 RADIUS 服务器。
7. 在 **IP** 地址字段中，输入 RADIUS 服务器的主机 IP 地址。
8. 在端口字段中，输入 RADIUS 服务器的端口号。默认端口号为 1812。



9. 单击应用。
10. 单击验证以验证与 RADIUS 服务器的连接。此时将显示验证辅助 **RADIUS** 服务器设置对话框。



11. 输入身份验证服务器的有效用户名和密码，然后单击验证。

要配置更多服务器，请重复步骤 6 到 11。

辅助 **TACACS+** 身份验证服务器

要使用 TACACS+，必须至少指定并配置一个 TACACS+ 服务器。(可选）配置冗余备份服务器，最多可以包含三个 TACACS+ 服务器。服务器将按顺序进行检查，首先从服务器部分列出的服务器开始。确保在 TACACS+ 身份验证服务器上创建所需的用户帐户。

要启用和配置 TACACS+ 身份验证，请执行以下操作：

1. 在 SD-WAN Center Web 界面中，导航到管理 > 用户/身份验证设置。
2. 在 辅助身份验证 > **TACACS+** 身份验证 部分，选 中启用辅助 **TACACS+** 身份验证 复选框。

> 注意
>
> 如果已启用 RADIUS 身份验证，则将处于禁用状态。

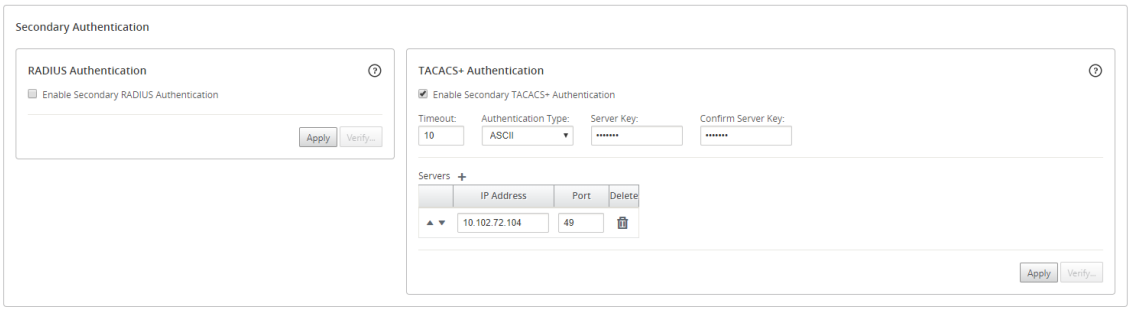
3. 在超时字段中，输入等待来自 TACACS+ 服务器的身份验证响应的时间间隔（以秒为单位）。

   超时值应小于或等于 10 秒。

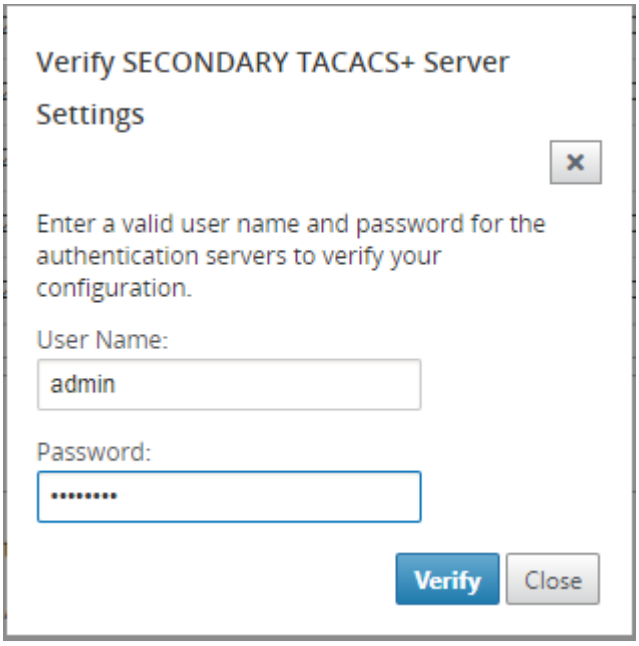
4. 在身份验证类型字段中，选择用于向 TACACS+ 服务器发送用户名和密码的加密方法。
5. 在服务器密钥字段中，输入连接 TACACS+ 服务器时要使用的密钥。
6. 在确认服务器密钥字段中，重新输入密钥。

> 注意
>
> 超时、身份验证类型和服务器密钥设置将应用到所有已配置的服务器。

7. 单击服务器旁边的加号图标 (+) 以添加 TACACS+ 服务器。
8. 在 **IP** 地址字段中，输入 TACACS+ 服务器的主机 IP 地址。
9. 在端口字段中，输入 TACACS+ 服务器的端口号。默认端口号为 49



10. 单击应用。
11. 单击验证以验证与 RADIUS 服务器的连接。此时将显示验证 **TACACS+** 服务器设置对话框。



12. 输入身份验证服务器的有效用户名和密码，然后单击验证。

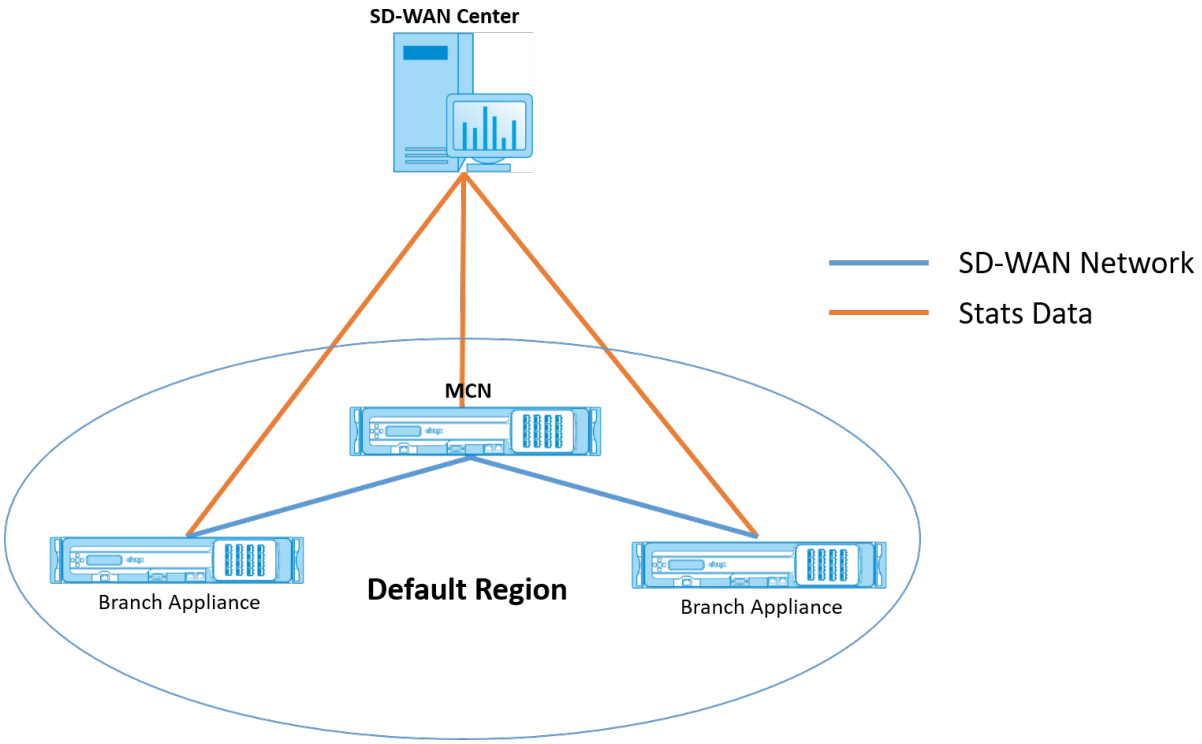
    要配置更多服务器，请重复步骤 7 到 12。

单区域网络部署

April 13, 2021

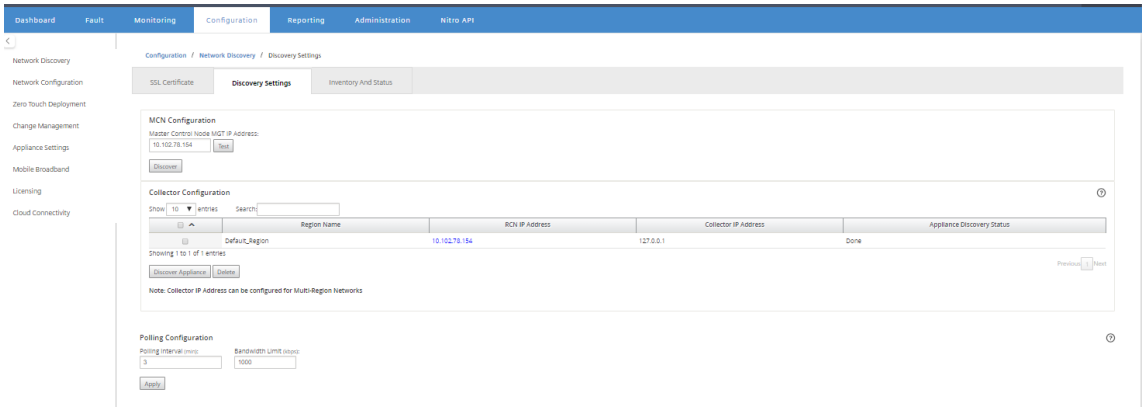
如果贵组织有一个小型网络跨越单个管理（或地理区域）界限，则可以在默认模式下使用 Citrix SD-WAN Center （带有一个“默认区域”）。一个区域最多可以支持 550 个站点。

一个区域网络具有一个用于集中控制的主控制节点 (MCN)，Citrix SD-WAN Center 来实现集中式管理。与 MCN 关联并受其控制的区域称为默认区域。Citrix SD-WAN Center 轮询 MCN 以及默认区域中的所有分支设备。



要为单区域部署 Citrix SD-WAN Center ，请执行以下操作：

1. 下载 Citrix SD-WAN Center 软件。有关详细信息，请参阅 [系统要求和安装。]。(/en-us/citrix-sd-wan-center/11/system-requirements-and-installation.html)
2. 在 ESXi 服务器、XenServer、Hyper-V 或 Azure 上安装 Citrix SD-WAN Center。
3. 配置管理界面设置。有关详细信息，请参阅配置管理界面设置。
4. 在 SD-WAN Center 生成、下载并安装 SD-WAN MCN SSL 证书。有关详细信息，请参阅安装 Citrix SD-WAN SSL 证书。
5. 在 MCN 设备上生成、下载并安装 SD-WAN Center SSL 证书。有关详细信息，请参阅安装 Citrix SD-WAN Center SSL 证书。
6. 在 Citrix SD-WAN Center GUI 中导航到配置 > 网络发现 > 发现设置。
7. 在主控制器节点的“插件 IP 地址”字段中，输入 MCN IP 地址，然后单击测试。这将在 MCN 与 Citrix SD-WAN Center 之间建立连接。



8. 单击发现。如果您已发现 MCN，此选项将更改为重新发现。

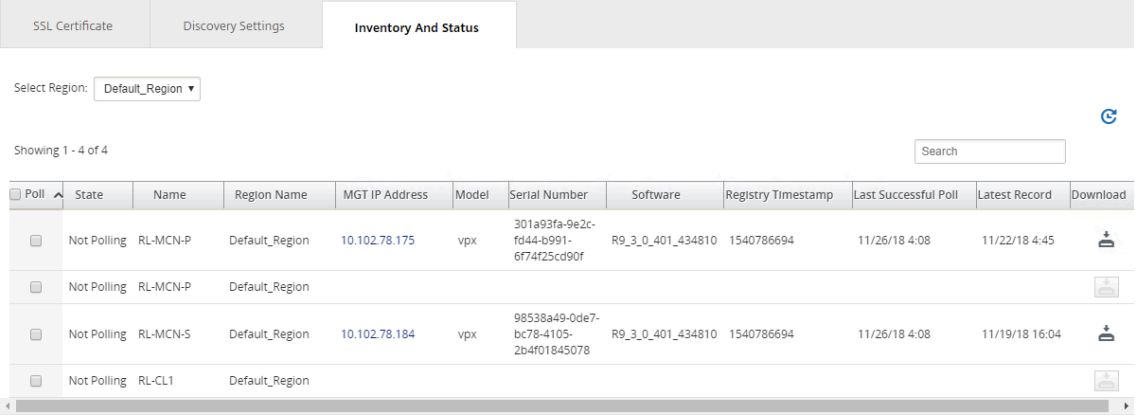
> 注意
>
> MCN 必须处于活动状态，并且应启用 SD-WAN 服务。有关详细信息，请参阅启用 SD-WAN 服务。

9. 在发现操作完成后，单击清单和状态选项卡。

   清单和状态表显示发现的所有 Citrix SD-WAN 设备的状态信息。

10. 选择表格标题左上角的轮询复选框。

    这将为表中列出的每个设备选中轮询复选框。要将设备从轮询列表中排除，请清除其复选框。



11. 单击应用。

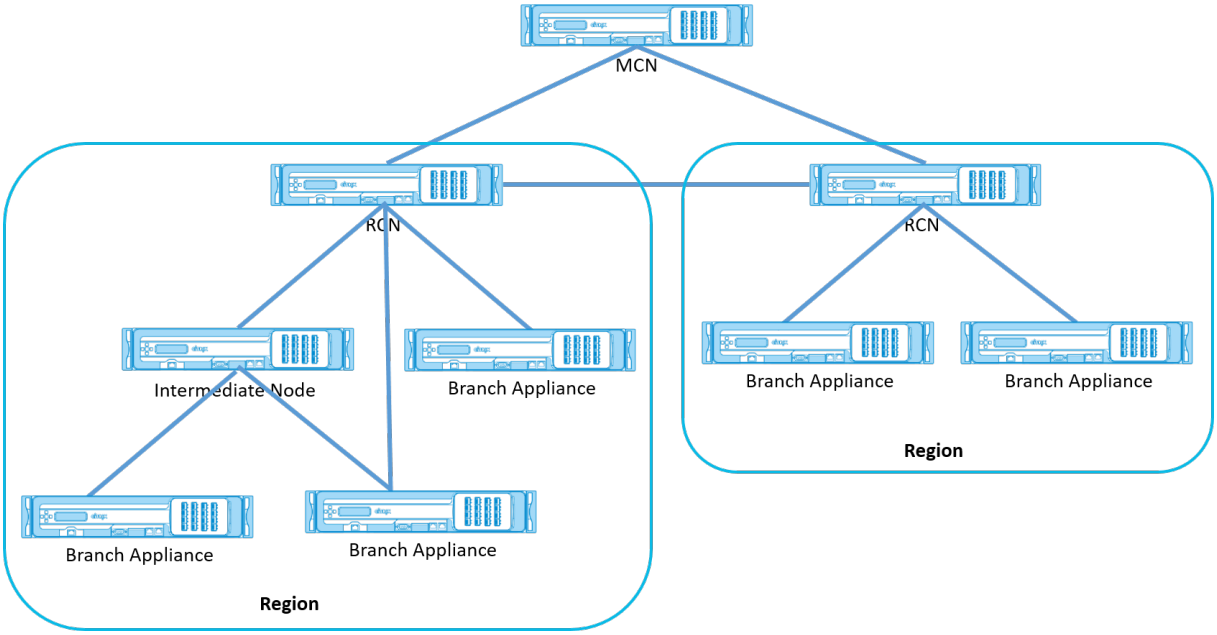
> 提示
>
> 可以通过在虚拟机上创建数据存储并切换数据存储来增加 Citrix SD-WAN Center 的存储大小。有关详细信息，请参阅将活动存储切换到新数据存储。

多区域网络部署

April 13, 2021

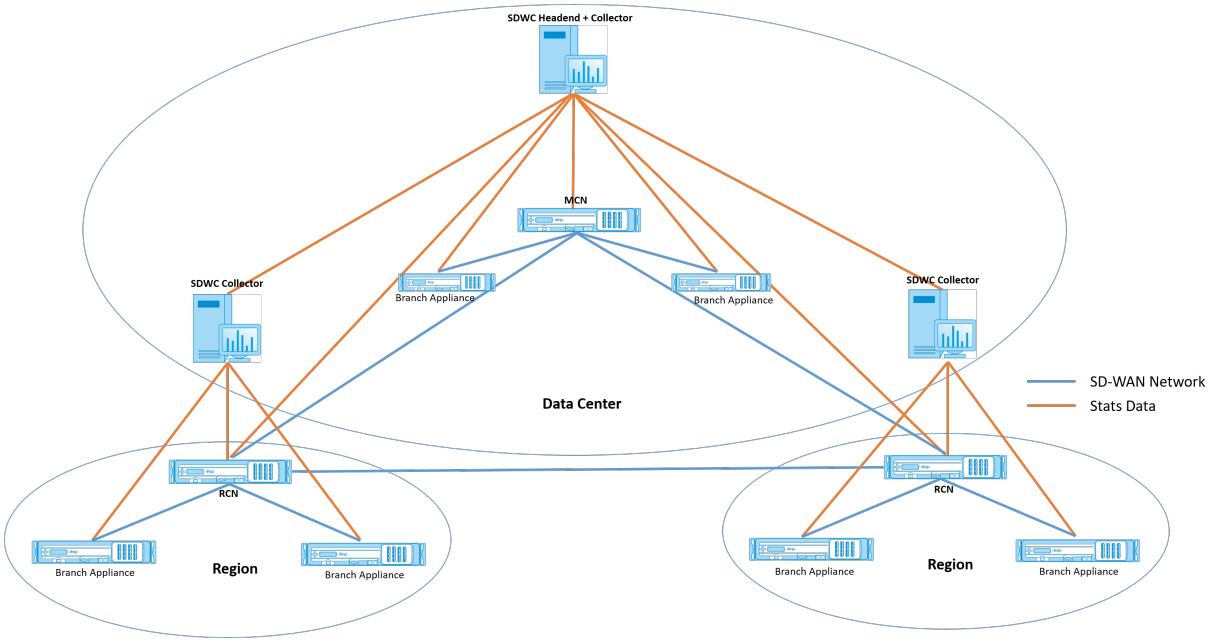
如果贵组织具有跨越多个管理（或地理）界限的大型网络，则可以在多区域模式下使用 Citrix SD-WAN Center ，每个区域最多支持最多 550 个站点。

多区域网络支持分层体系结构，并且主控制节点 (MCN) 控制多个区域控制节点 (RCN)。反过来，每个 RCN 控制多个客户端站点。MCN 还可以选择用于直接控制某些客户端站点，作为“默认区域”的一部分。这种分层和分布式结构可以实现更大规模的区域行政管理和有效的权力下放。



Citrix SD-WAN Center 轮询 MCN、RCN 和所有关联的分支设备。

多地区 Citrix SD-WAN Center 体系结构要求为每个地区添加收集器，以收集和存储地区级数据和统计信息。此分布式体系结构实现了跨多个区域的更高规模，同时保留了“单窗格玻璃”视图以管理整个网络。

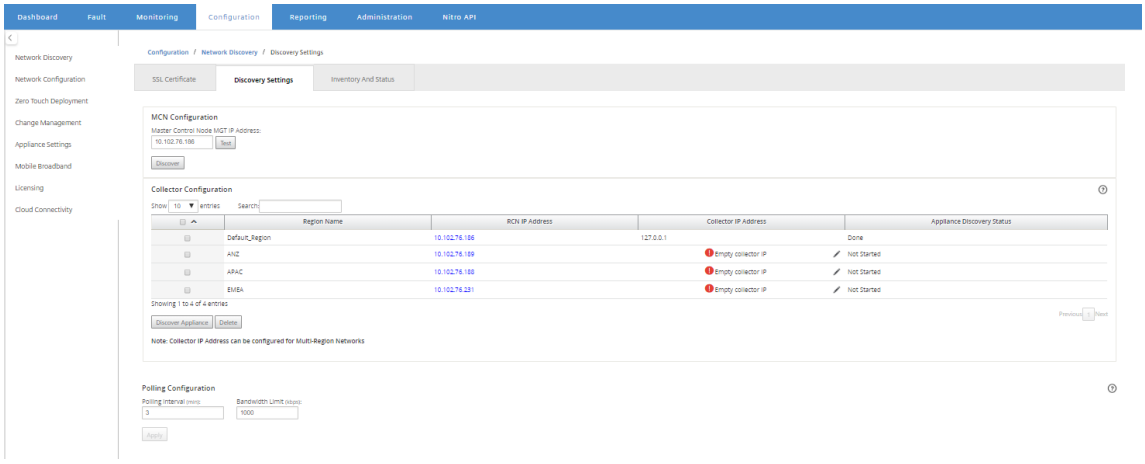


> 注意
>
> 对于多区域部署，默认的区域统计信息包括由 MCN 和 RCN 管理的所有站点的统计信息。但是，RCN 数据并不存储在 SD-WAN Center 收集器上。SD-WAN Center 收集器从各自的区域收集器获取 RCN 站点数据。

要为多地区部署 **Citrix SD-WAN Center**，请执行以下操作：

1. 下载 Citrix SD-WAN Center 软件。有关详细信息，请参阅 系统要求和安装。
2. 在 ESXi 服务器、XenServer、Hyper-V 或 Azure 上安装 Citrix SD-WAN Center。
3. 配置管理界面设置。有关详细信息，请参阅 配置管理界面设置。
4. 在 SD-WAN Center 生成、下载并安装 SD-WAN MCN SSL 证书。有关详细信息，请参阅安装 Citrix SD-WAN SSL 证书。
5. 在 MCN 设备上生成、下载并安装 SD-WAN Center SSL 证书。有关详细信息，请参阅安装 Citrix SD-WAN Center SSL 证书。
6. 在 Citrix SD-WAN Center GUI 中导航到配置 > 网络发现 > 发现设置。
7. 在主控制器节点的“插件 IP 地址”字段中，输入 MCN IP 地址，然后单击测试。这将在 MCN 与 Citrix SD-WAN Center 之间建立连接。
8. 单击发现。连接到 MCN 的所有 RCN 的列表将显示在收集器配置部分。要发现非默认区域站点，您需要有一个带有通往 MCN 的活动路径的 RCN。

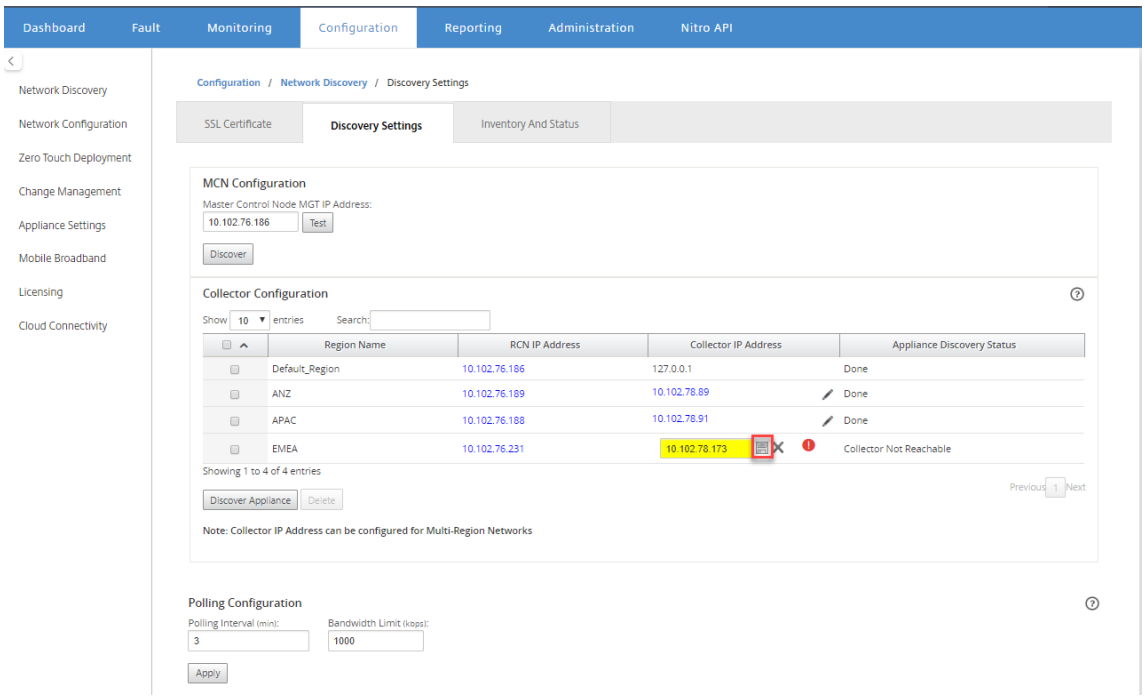
   > 注意
   >
   > Citrix SD-WAN Center 使用默认区域的收集器。



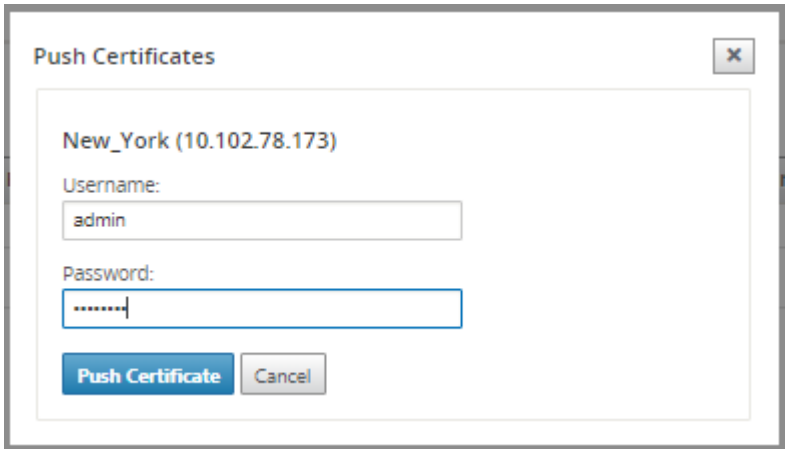
9. 单击“编辑”图标，然后在收集器 **IP** 字段中，输入要配置为区域收集器的 Citrix SD-WAN Center 的 IP 地址。

> 注意
>
> 要设置收集器，请安装一个 Citrix SD-WAN Center VM 并配置管理 IP 地址。Citrix SD-WAN Center 的管理 IP 地址是收集器 IP 地址。

10. 单击保存图标以保存收集器 IP 地址，并将证书-密钥对推送到 RCN。

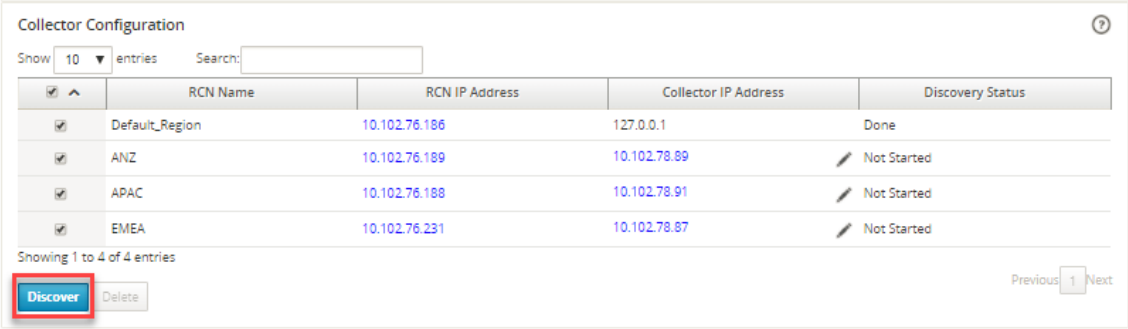


11. 输入 RCN 的凭据，然后单击推送证书。

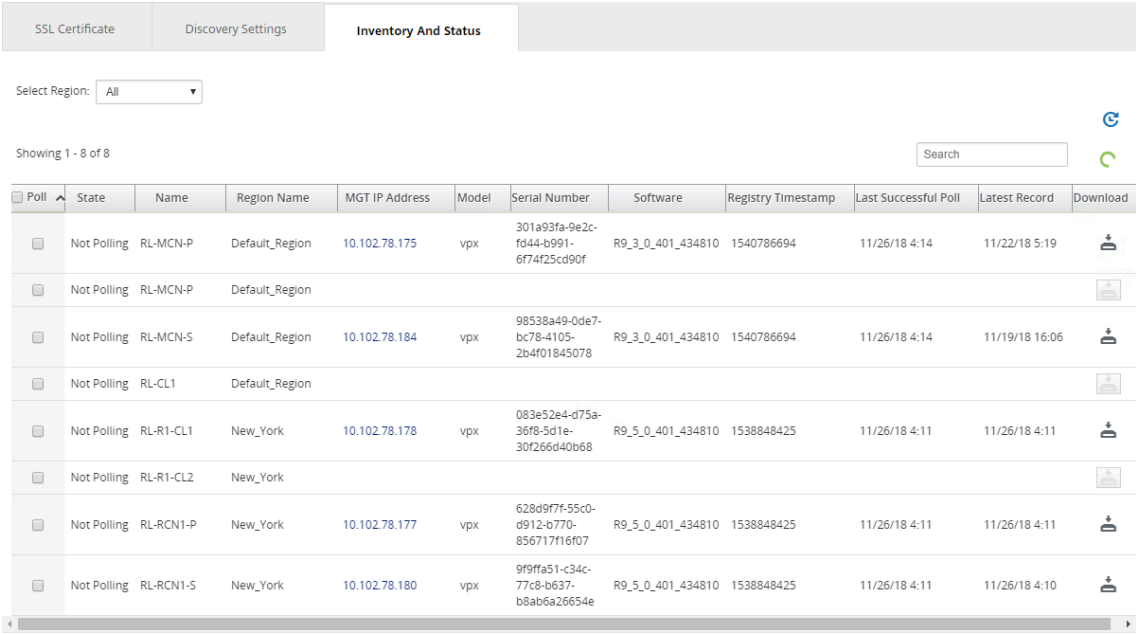


12. 同样，为所有 RCNs 配置收集器 IP 地址。

> 注意
>
> 这些设备每 30 分钟自动发现一次。如果在网络中添加了新 RCNs 并执行了更改管理，则可以选择该设备，然后单击发现设备以立即发现该设备。



发现状态更改为完成后，可以在“清单”和状态页面中查看发现的站点。



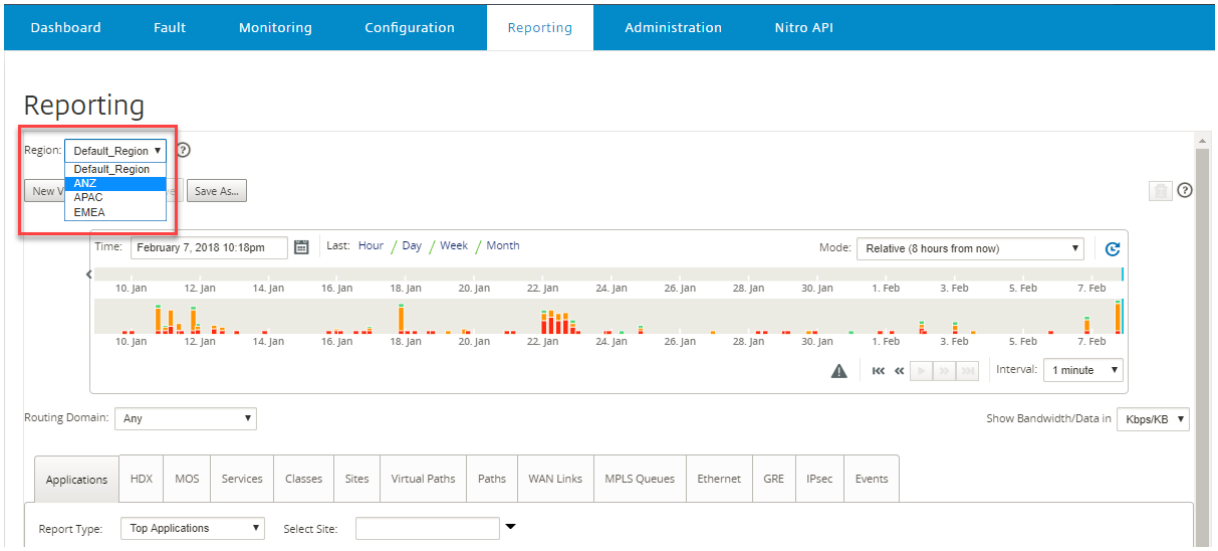
> 提示
>
> 您可以根据区域名称过滤站点。在选择地区字段中，选择区域。

13. 在清单和状态页面中，选择要启动轮询的站点，然后单击应用。

> 提示
>
> 您可以通过在虚拟机上创建数据存储来增加收集器的存储大小。有关详细信息，请参阅将活动存储切换到新的数据存储。

您可以选择特定地区以查看事件和统计报告。

事件和统计数据报告数据是从相应区域的收集器中获取的。



配置

April 13, 2021

配置 Citrix SD-WAN Center 的初始几个步骤通常适用于单区域网络和多区域网络。下面列出了通用配置过程：

- 配置管理界面设置
- 安装 Citrix SD-WAN Center 证书。
- 将激活存储切换到新的数据排序。

配置管理界面设置

April 13, 2021

可以使用 Citrix SD-WAN Center Web 界面配置管理接口设置。

管理接口设置包括以下各项：

- Citrix SD-WAN Center 管理 IP 地址
- 网关 IP 地址
- 子网掩码
- 主 DNS
- 二级 DNS

要配置管理接口设置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，选择管理选项卡。

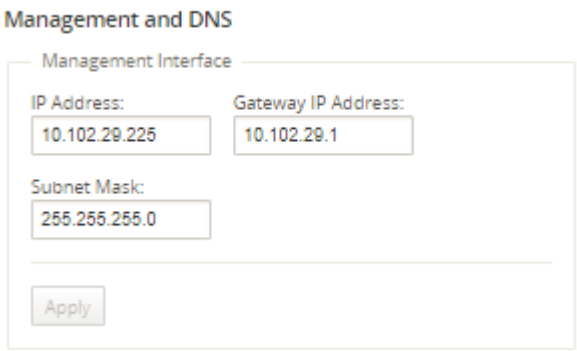
   默认情况下，将显示用户/身份验证设置页面。

2. 在导航树中，选择全局设置。

3. 配置管理和 DNS 设置。

   在管理和 **DNS** 部分中，将所需的信息添加到以下字段中：

   - **IP** 地址：输入 Citirx SD-WAN Center 的 IP 地址。
   - 网关 **IP** 地址：输入 Citrix SD-WAN Center VM 与外部网络进行通信时使用的网关 IP 地址。
   - 子网掩码：输入子网掩码以定义 Citrix SD-WAN Center VM 所在的网络。



4. 单击应用。

> 注意
>
> 应用您所做的更改时，与 Citrix SD-WAN Center 的连接将终止。

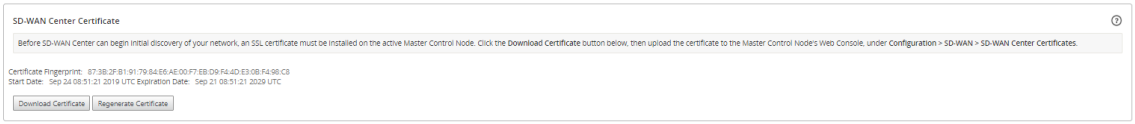
安装 **SD-WAN Center SSL** 证书

April 13, 2021

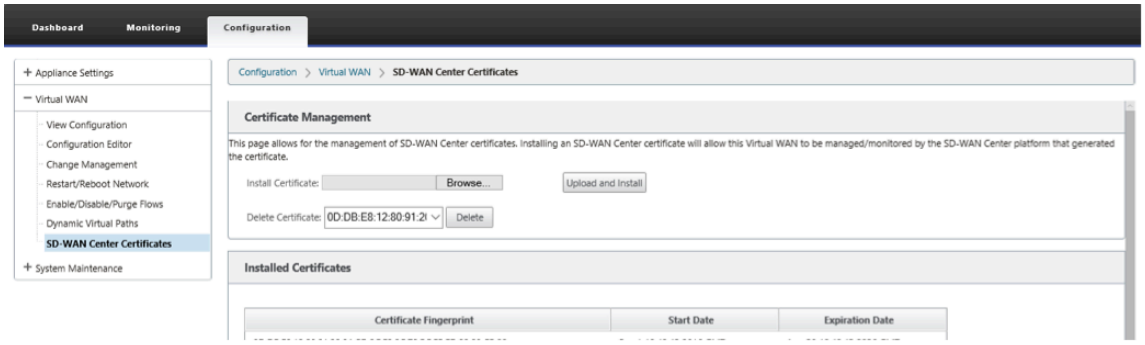
要在 Citrix SD-WAN Center 和 Citrix SD-WAN 主控制节点 (MCN) 之间建立连接，请从 SD-WAN Center 下载 SSL 证书并将其安装在 MCN 上。

要生成和安装 Citrix SD-WAN Center 证书，请执行以下操作：

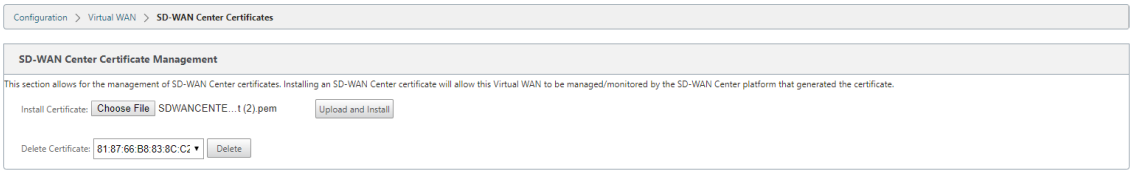
1. 在 Citrix SD-WAN Center Web 界面中，导航到配置 > 网络发现 > **SSL** 证书 > **SD-WAN Center** 证书。
2. 单击重新生成证书以生成新的 SSL 证书以建立与 MCN 的通信。



3. 单击下载证书。导航到所需的位置并保存证书。
4. 在 Citrix SD-WAN MCN Web 界面中，导航到配置 > 虚拟广域网 > **SD-WAN Center** 证书 > **SD-WAN Center** 证书管理。



5. 单击选择文件，浏览并选择下载的 SD-WAN Center SSL 证书。



6. 单击上载并安装，它会将 SD-WAN Center SSL 证书上载到 MCN，并在安装完成时显示成功消息。

安装 **Citrix SD-WAN SSL** 证书

April 13, 2021

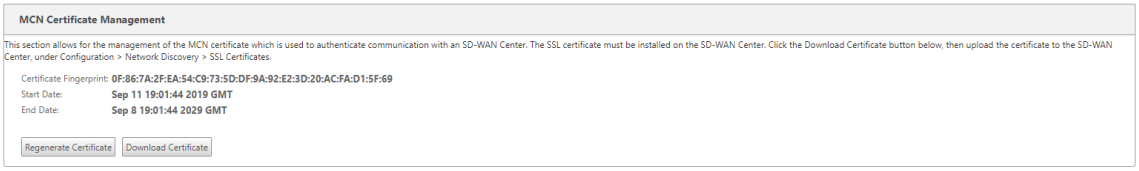
要在 Citrix SD-WAN MCN 和 Citrix SD-WAN Center 之间建立连接，请从 MCN SD-WAN 设备下载 SSL 证书并将其安装在 SD-WAN Center。

您可以在替换预定义证书的 MCN 上重新生成设备证书，然后将其安装在 SD-WAN Center 上。

要使新部署和 SSL 通信起作用，必须将设备证书安装到 SD-WAN Center。MCN 生成网络证书，并通过证书管理器向所有节点分发证书的私钥。每个分支使用证书来对 SD-WAN Center 进行身份验证。

要生成和安装 SD-WAN 证书，请执行以下操作：

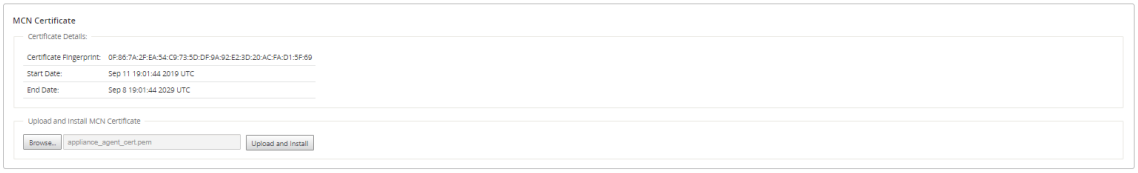
1. 在 MCN SD-WAN 设备中，导航到配置 > 虚拟 **WAN** > **SD-WAN Center** 证书 > **MCN** 证书管理。
2. 单击重新生成证书以生成新的 SSL 证书以建立与 SD-WAN Center 的通信。



> 注意：

> 重新生成 SSL 证书时，SD 设备会立即使用新证书来与发现的 SD-WAN Center 进行通信。但是，在 SD-WAN Center 上下载并安装新生成的证书之前，才能与设备建立通信。

3. 单击下载证书。导航到所需的位置并保存证书。
4. 在 Citrix SD-WAN Center Web 界面中，导航到配置 > **SSL** 证书 > **MCN** 证书。



5. 单击浏览并选择下载的 MCN SSL 证书。

6. 单击上载并安装，它将 MCN SSL 证书上载到 SD-WAN Center。

将活动存储切换到新数据存储

April 13, 2021

在 Citrix SD-WAN Center 中，可以将活动存储切换到在虚拟服务器上创建的数据存储。这样，您可以存储通过轮询 WAN 中的所有 Citrix SD-WAN 设备获得的更多统计数据。有关在 ESXi 服务器上创建数据存储的信息，请参阅 在 ESXi 服务器上添加和配置数据存储。有关在 XenServer 上创建数据存储的信息，请参阅在 XenServer 上添加和配置数据存储。

要为 Citrix SD-WAN Center VM 指定活动存储，请执行以下操作：

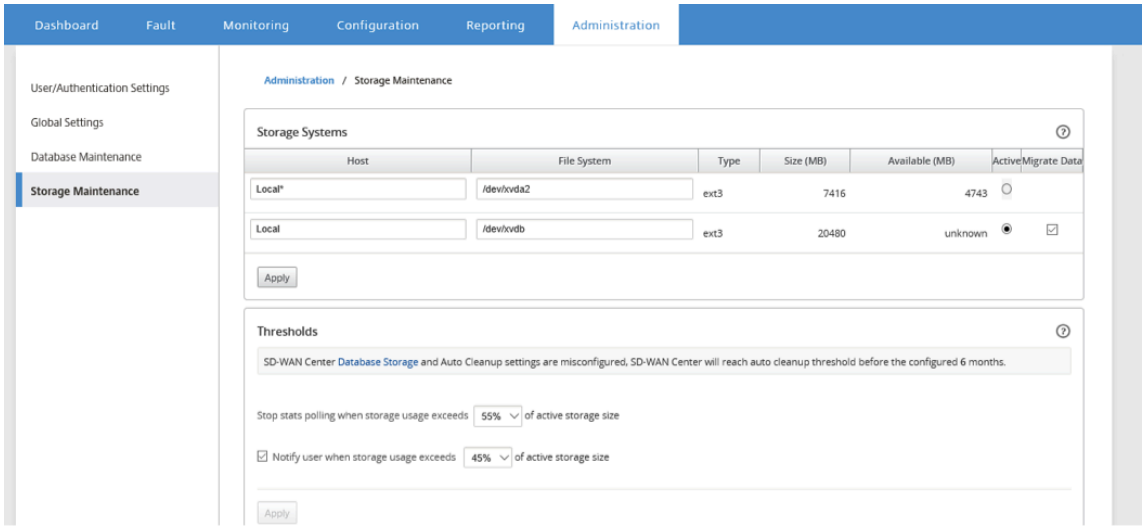
1. 登录 Citrix SD-WAN Center VM。

   Citrix SD-WAN Center 的默认登录凭据如下所示：

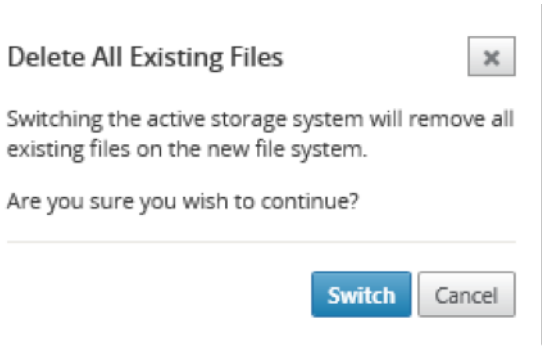
   登录：管理员

   密码：**password**

2. 单击管理选项卡，然后单击存储维护。



3. 在存储系统表的活动列中，选择您创建的存储。
4. 选择迁移数据并单击应用。
5. 此时将显示删除所有现有文件消息消息，然后单击切换。



这会将 Citrix SD-WAN Center 置于维护模式，并在主页面区域显示进度条。

6. 激活完成后，单击继续。

   这将取消进度条并返回到主存储维护页面。

部署 **Citrix SD-WAN** 设备

April 13, 2021

可以使用 Citrix SD-WAN Center 创建设备配置或设备设置文件，并使用更改管理向导将配置推送到网络中的设备。有关详细信息，请参阅配置 Citrix SD-WAN 设备。

可以将 Citrix SD-WAN Center 配置为用作中央许可服务器，并向网络中的所有节点提供许可服务。这样就无需在本地单个节点上安装许可证。有关详细信息，请参阅将 Citrix SD-WAN Center 作为许可证服务器。

可以使用 Citrix SD-WAN Center 在分支机构使用零触摸部署功能来优化部署 SD-WAN 设备的过程。有关详细信息，请参阅零接触部署。

配置 Citrix SD-WAN 设备

April 13, 2021

使用“配置编辑器”编辑配置设置，并将配置包导出到 MCN。有关详细信息，请参阅配置编辑器。

可以通过 Citrix SD-WAN Center 使用 MCN 设备的更改管理向导。有关详细信息，请参阅更改管理向导。

可以在 Citrix SD-WAN Center 上配置设备设置，并将其导出到 SD-WAN 网络中的一组托管 Citrix SD-WAN 设备上。有关详细信息，请参阅设备设置。

配置编辑器

April 13, 2021

配置编辑器以 Citrix SD-WAN Center Web 界面的组件形式提供，位于 SD-WAN 网络的主控制节点 (MCN) 上运行的 Citrix SD-WAN Management Web 界面中。

> 注意
>
> 您不能将配置直接从 Citrix SD-WAN Center 推送到发现的设备中。您可以使用“配置编辑器”来编辑配置设置以及创建配置包。创建配置包后，可以将其导出到 MCN 并进行安装。然后这些更改将反映在 MCN 中。
>
> 必须使用 Citrix SD-WAN Center 设备和 MCN 的管理权限登录，以编辑 Citrix SD-WAN Center 上的配置以及导出并在 MCN 上安装配置。

有关使用配置编辑器配置 Citrix SD-WAN 的详细说明，请参阅 Citrix SD-WAN 10.1 文档。

使用配置编辑器可以执行以下操作：

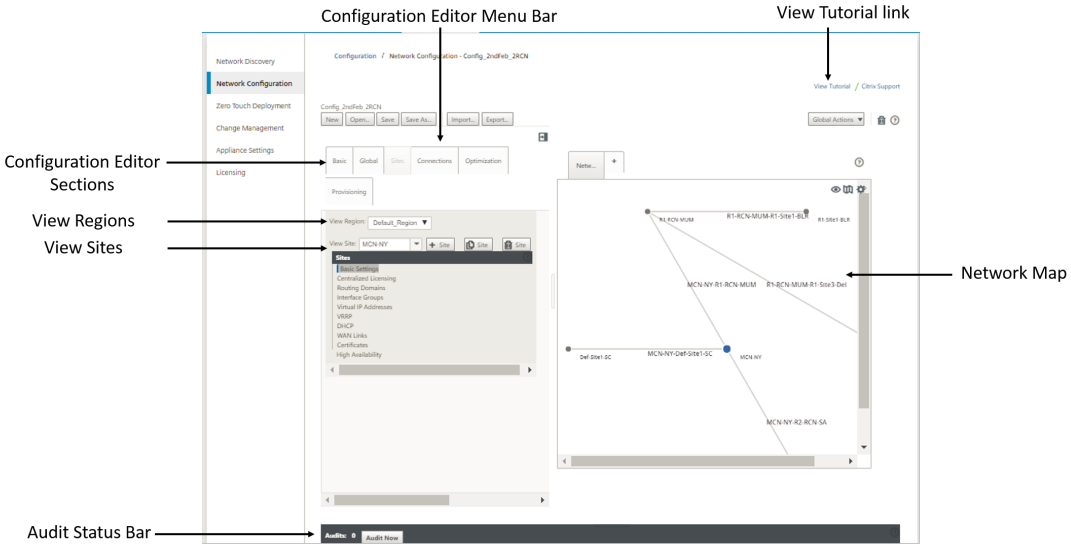
- 添加并配置 Citrix SD-WAN 设备站点和连接。
- 预配 Citrix SD-WAN 设备。
- 创建并定义 Citrix SD-WAN 配置。
- 定义并查看您的 SD-WAN 系统的网络映射。

要打开配置编辑器，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击配置选项卡。

2. 单击网络配置。

下图概述了配置编辑器的基本导航和页面元素，以及本指南中使用的术语，用于识别这些元素。



“配置编辑器”的主屏幕包含以下导航元素：

- 配置编辑器菜单栏：包含用于配置编辑器操作的主要活动按钮。此外，菜单栏最右侧的是用于启动配置编辑器教程的查看教程链接按钮。本教程将向您介绍配置编辑器显示的每个元素的一系列气泡说明。
- “配置编辑器”各部分：每个选项卡代表一个顶层区域。有六部分：基本、全局、站点、连接、优化和预配。单击部分选项卡可显示该部分的配置树。
- 视图区域：对于多区域部署，将列出所有已配置的区域。对于单区域部署，默认情况下将显示默认区域。要查看某个区域中的站点，请从下拉列表中选择一个区域。
- ** 查看站点：** 列出已添加到配置中并当前在配置编辑器中打开的站点节点。要查看站点配置，请从 frop 下拉列表中选择一个站点。
- 网络映射：提供 SD-WAN 网络的示意视图。将鼠标光标悬停在站点或路径上以查看更多详细信息。单击站点以查看报告选项。
- 审计状态栏：“配置编辑器”页面底部的深灰色条，并跨越“配置编辑器”页面的整体宽度。仅当配置编辑器打开时，审核状态栏才可用。状态栏最左侧的审核警报图标（红点或 goldenrod delta）表示当前打开的配置中存在一个或多个错误。单击状态栏可显示该配置的所有未解决审计警报的完整列表。

更改管理向导

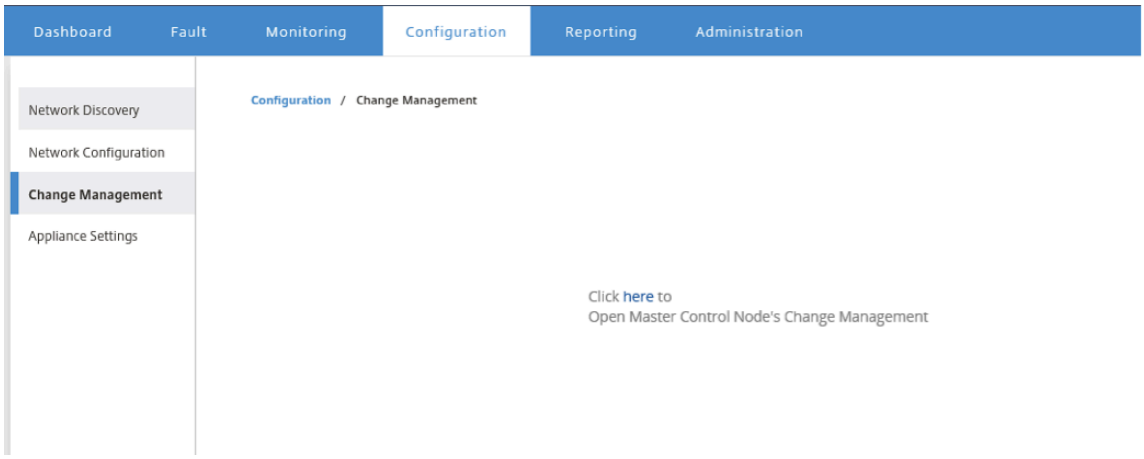
April 13, 2021

更改管理向导将引导您完成在主控制节点 (MCN) 设备和客户端设备上上载、下载、暂存和激活 Citrix SD-WAN 软件和配置的过程。

更改管理向导是 MCN 上运行的 Citrix SD-WAN 管理 Web 界面的一个组件，不属于 Citrix SD-WAN Center。但是，您可以使用 Citrix SD-WAN Center 连接到指定的 MCN，并访问更改管理向导。

要打开更改管理向导，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击配置选项卡。
2. 单击更改管理。



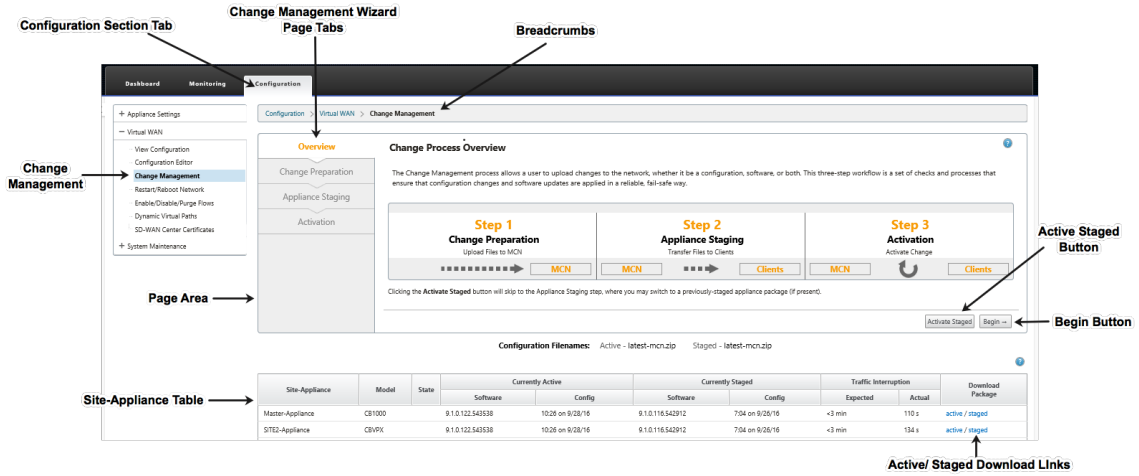
3. 在单击此处打开主控件节点的更改管理提示，单击此处链接。

   您将自动登录到 MCN GUI。

   > 注意
   >
   > 您无需使用 MCN 凭据登录 MCN GUI，自动登录功能可以启用单点登录。

4. 在 MCN management Web 界面中，单击配置选项卡。
5. 在导航树（左侧窗格）中，单击虚拟 **WAN** 分支旁边的 **+** 以展开该分支。
6. 单击更改管理。

   此时将显示更改管理向导的第一页（更改过程概述页面），如下图所示。



7. 要启动该向导，请单击开始。

> 注意
>
> 有关使用向导上载、暂存以及在设备上激活 SD-WAN 软件和配置的完整说明，请参阅《SD-WAN 9.1.0 用户指南》。

更改管理向导包含以下导航元素：

- 页面区域：显示更改管理向导各页面的表单、表格和活动按钮。
- 更改管理向导页选项卡：在页面区域的左侧，在向导的每一页上，按照在向导过程中执行相应步骤的顺序列出选项卡。当选项卡处于活动状态时，可以单击该选项卡以返回到向导中的上一个页面。活动选项卡显示其名称以蓝色字体显示。灰色字体表示不活动的选项卡。选项卡处于不活动状态，直至完成所有依赖项（之前的步骤），但未出现任何错误。
- 设备-站点表：在向导页面区域底部，此表包含有关每个已配置设备站点的信息，以及用于下载该设备型号和站点的活动或暂存设备软件包的链接。在此上下文中，软件包是一种 zip 文件包，其中包含适用于该设备型号以及指定配置包的相应 SD-WAN 软件包。表上方的配置文件名部分显示了本地设备上当前活动和暂存包的程序包名称。
- 主动/暂存下载链接：在下载软件包字段（最右侧栏）在设备-站点表中的每个条目中，可以单击某个条目中的链接以下载该设备站点的活动或暂存软件包。
- 开始按钮：单击开始以启动更改管理向导过程并转至更改准备选项卡页。
- 激活暂存按钮：如果这不是初始部署，而您想要激活当前的暂存配置，您可以选择直接继续执行激活步骤。单击激活分段直接进入激活页面并启动激活当前分段配置的激活。

设备设置

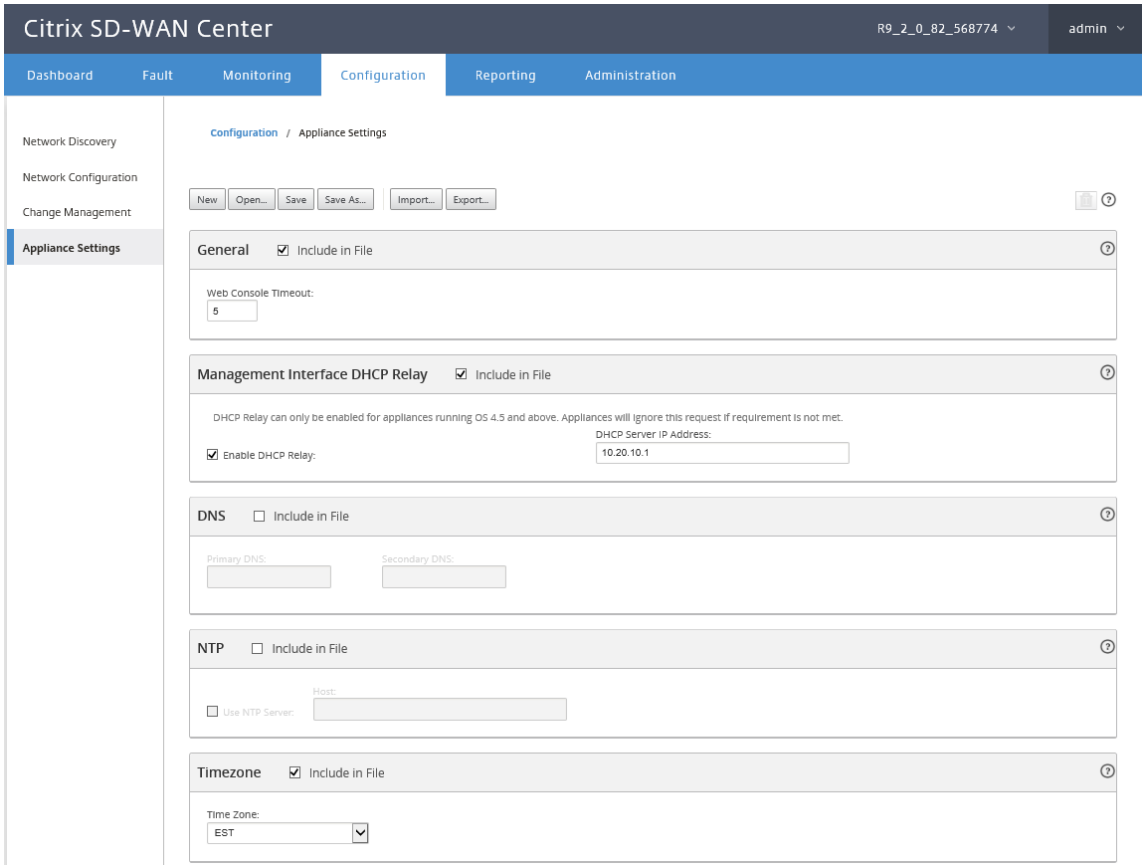
April 13, 2021

可以在 Citrix SD-WAN Center 上配置设备设置，并将其导出到 SD-WAN 网络中的一组托管 Citrix SD-WAN 设备上。在设备设置页面上，可以执行以下操作：

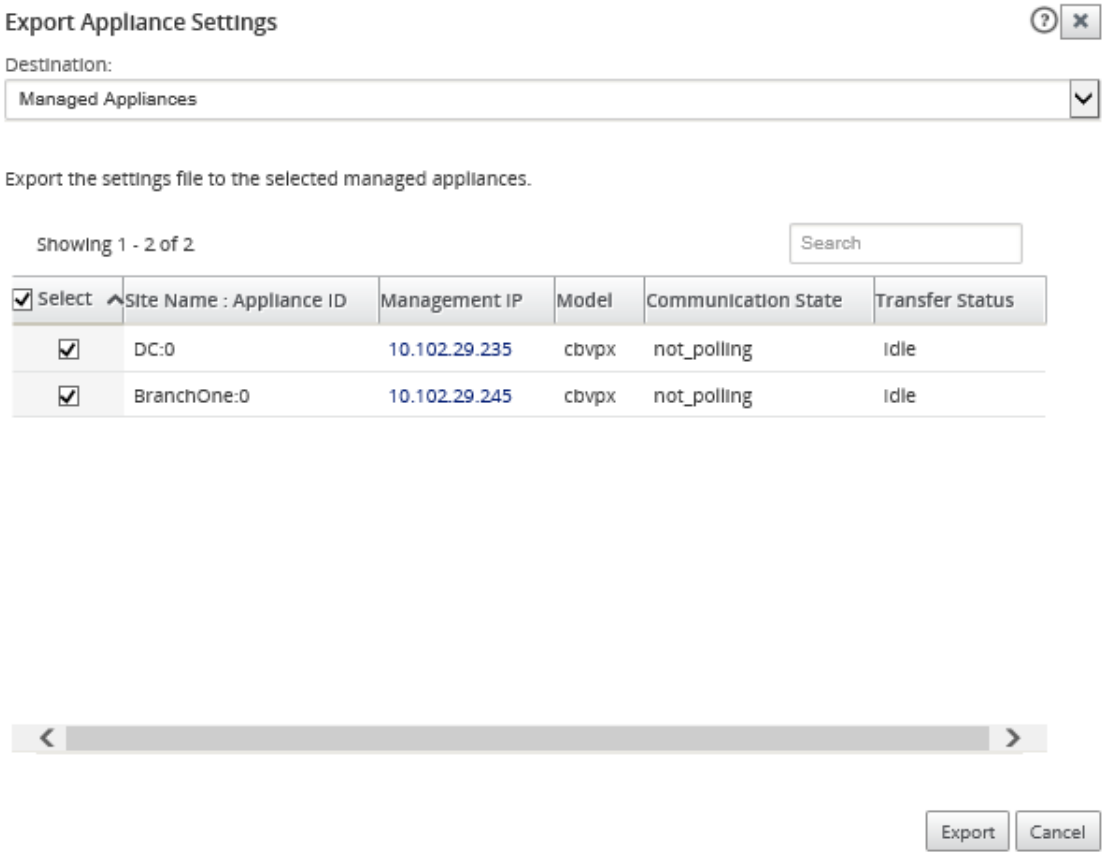
- 创建新的装置设置文件。
- 打开并编辑现有的装置设置文件。
- 从本地计算机导入装置设置文件。
- 将装置设置文件下载到本地计算机。
- 将装置设置文件导出到受控装置。

要创建设备设置文件并将其导出到托管设备，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击配置选项卡。
2. 单击设备设置，然后单击新建。



3. 为所需的设置选择包含在文件中，并为设置指定参数值。有关详细信息，请参阅装置设置表。
4. 单击导出。在另存为对话框中，输入设备设置文件的名称，然后单击保存。此时将显示导出设备设置对话框。
5. 在目标字段中，选择托管设备，然后选择要将设备设置导出到的设备。



> 注意
>
> 要将设备设置下载到本地计算机，请在目标字段中选择文件下载。

6. 单击导出。

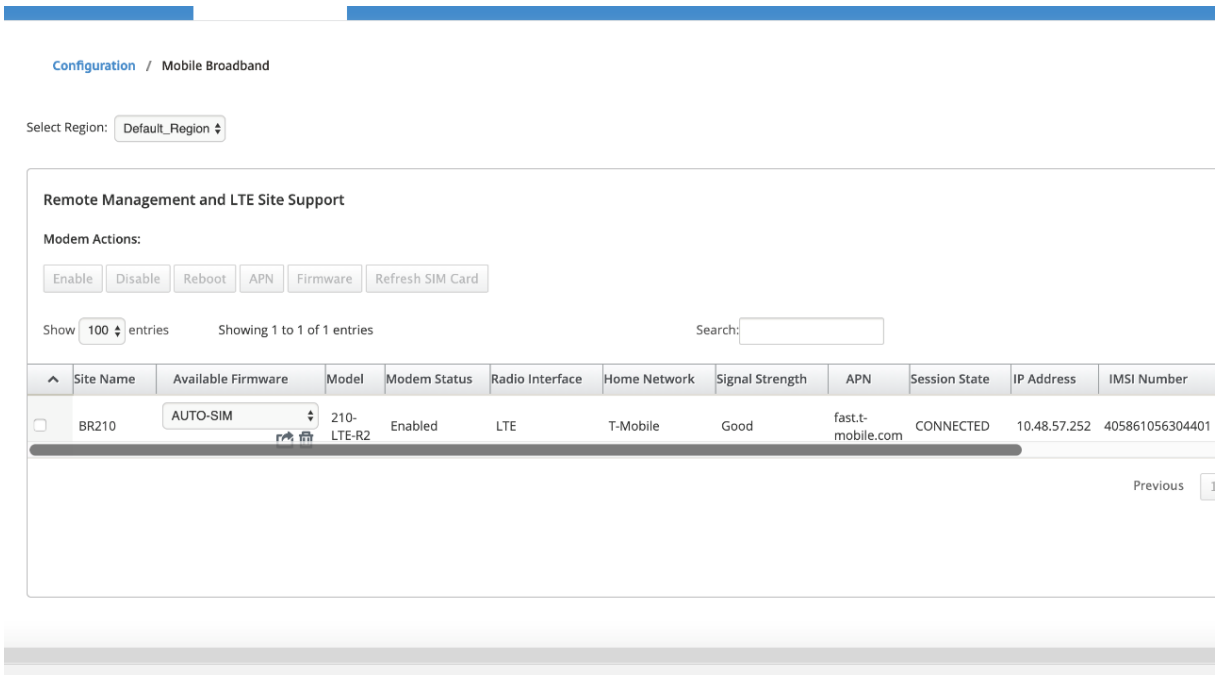
远程 **LTE** 站点管理

April 13, 2021

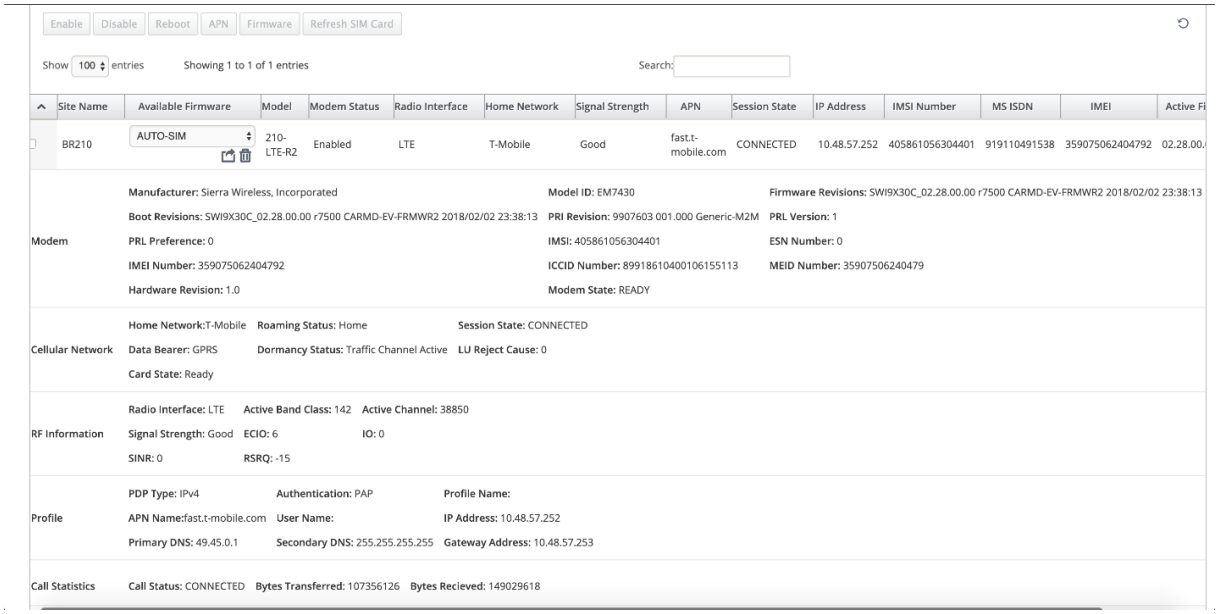
Citrix SD-WAN Center 允许您远程查看和管理网络中的所有 LTE 站点。LTE 摘要表列出了网络中使用的 Citrix SD-WAN 210-SE LTE 设备。

要远程管理网络中的 LTE 站点，请在 SD-WAN Center 用户界面中导航到配置 **>** 移动宽带。

对于多区域部署，您可以选择要管理 LTE 站点的区域。默认情况下，“默认”区域处于选中状态。



单击 **+** 查看详细信息。



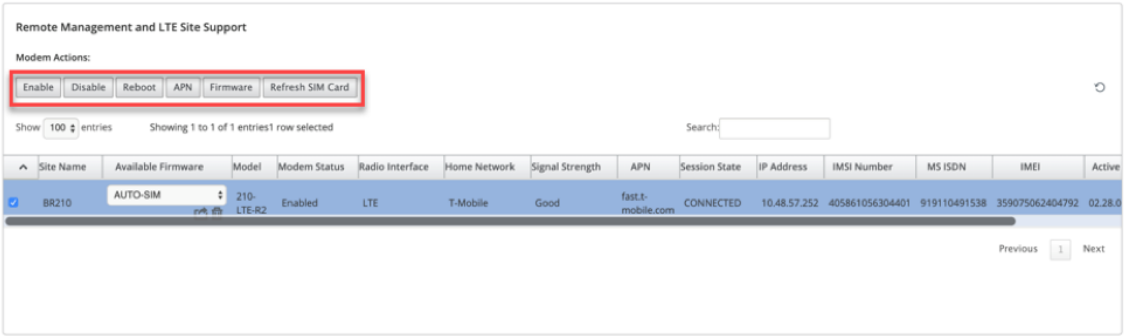
您可以选择单个设备或多个设备来执行以下 LTE 调制解调器操作：

- 启用：在选定站点启用调制解调器。
- 禁用：在选定站点禁用调制解调器。
- 重新启动：在选定站点重新启动调制解调器。
- **APN**：为所选站点配置 APN 设置。有关详细信息，请参阅配置 APN 设置。

- 固件：浏览并选择所需的固件。您可以选择仅上载或上载并应用所选站点上的固件文件。从可用固件列表中，您可以选择应用或删除它。

  > 注意
  >
  > 在多区域部署中，非默认区域站点的固件操作无法通过 SD-WAN Center Headend 完成。您可以从特定区域的 Collector SD-WAN Center 执行固件操作。

- 刷新 **SIM** 卡：通过将 SIM 卡关闭并在选定站点重新打开来刷新 SIM 卡。执行此操作是为了检测插入 210 SE LTE 调制解调器的新 SIM 卡。



您还可以在各个 LTE 设备上配置 LTE 功能。有关详细信息，请参阅在 210 SE LTE 上配置 LTE 功能。

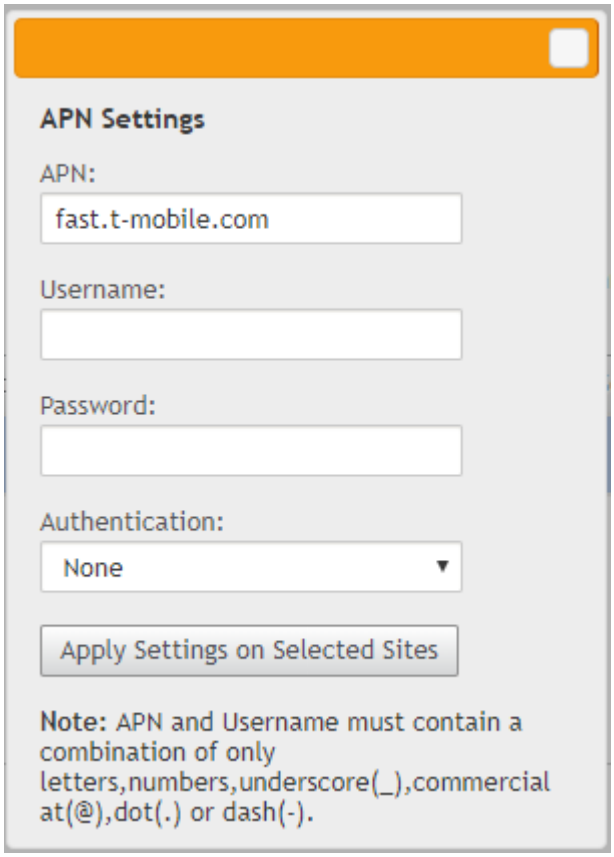
APN 设置

APN 是您的设备读取的设置的名称，用于在运营商的蜂窝网络和公共互联网之间建立与网关的连接。您可以从运营商处获取 APN 信息，并在一台或多台 LTE 设备上远程配置 **APN** 设置。

> 注意：
> APN 设置因承运人而异。

要配置 APN 设置：

1. 在 SD-WAN Center 用户界面中，导航到配置 **>** 移动宽带。选择要为其配置 APN 设置的 LTE 站点，然后单击 **APN**。



2. 输入运营商提供的 **APN** 名称、用户名、密码和 身份验证。您可以从 PAP、CHAP、PAPCHAP 身份验证协议中进行选择。如果运营商未提供任何身份验证类型，请将其设置为无。
3. 单击在所选站点上应用设置。

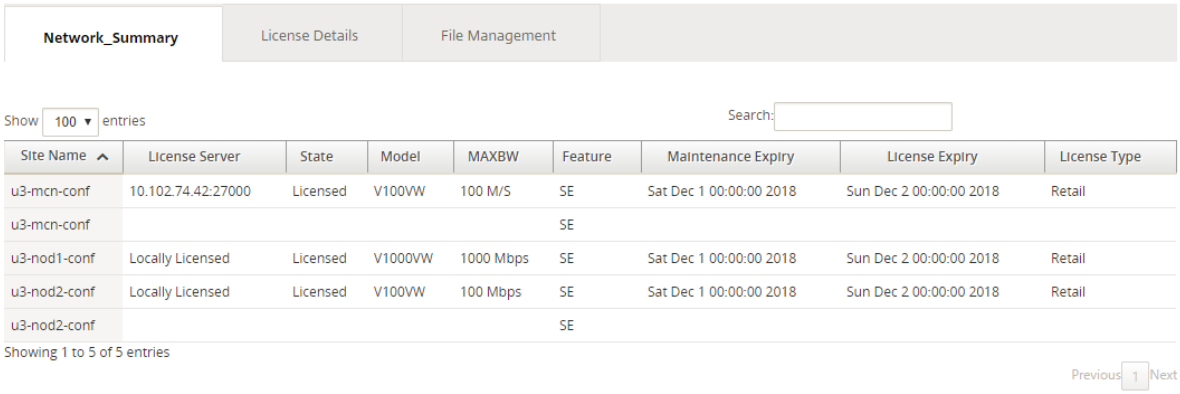
将 **Citrix SD-WAN Center** 作为许可证服务器

April 13, 2021

可以获取网络中设备的许可证，在 SD-WAN Center 中上载并安装。要将 SD-WAN Center 用作远程许可证服务器，请将 SD-WAN Center 的 IP 地址配置为用于集中式许可证管理的远程服务器。有关详细信息，请参阅集中许可证管理。

通过更改管理过程将网络配置推送到站点后，如果激活了配置，分支设备将自动从 SD-WAN Center 获取许可证。对于要使用的这些许可证，必须将许可证分配给 SD-WAN Center 自身的主机。

要查看 SD-WAN Center 发现的所有设备的许可证详细信息，请导航到配置 > 许可 > 网络摘要。



将显示以下参数：

- 站点名称：站点的名称。
- 许可证服务器：许可证服务器的 IP 地址和端口号。如果此许可证是在设备上本地安装的，则会显示为“本地许可”。
- 状态：设备的当前许可证状态，已获得许可或未获许可。
- 型号：许可证支持的设备型号。
- **MAXBW**：许可允许使用的最大带宽。
- 功能：许可证支持的 Citrix SD-WAN 版本。
- 维护过期：Citrix 专享升级服务的过期日期。

  > 注意
  >
  > 软件升级期间，如果软件生成日期高于维护过期日期，则不允许升级软件。

- 许可证过期：许可证的过期日期。
- 许可证类型：许可证的类型。

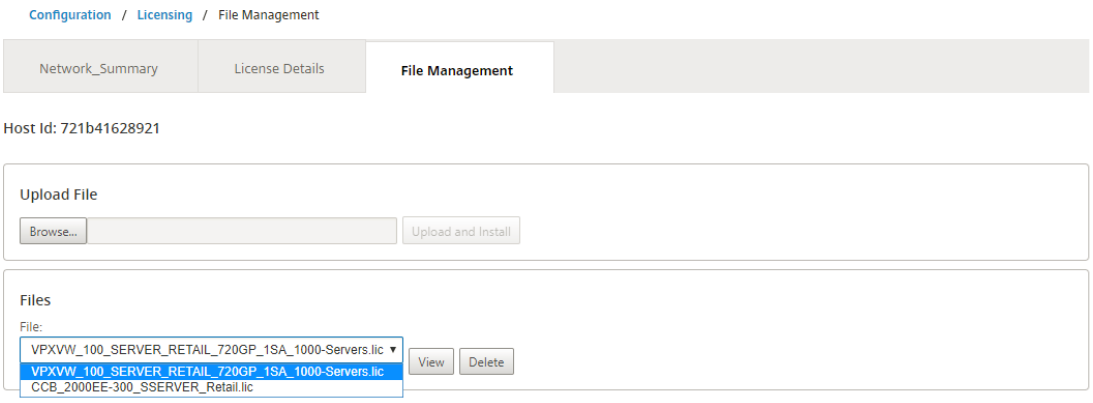
要上载并在 SD-WAN Center 中安装许可证文件，请执行以下操作：

1. 获取 Citrix SD-WAN 设备的许可证并将其保存在本地计算机上。

   > 注意
   >
   > 有关获取 Citrix SD-WAN 软件许可证的说明，请联系 Citrix SD-WAN 客户支持。

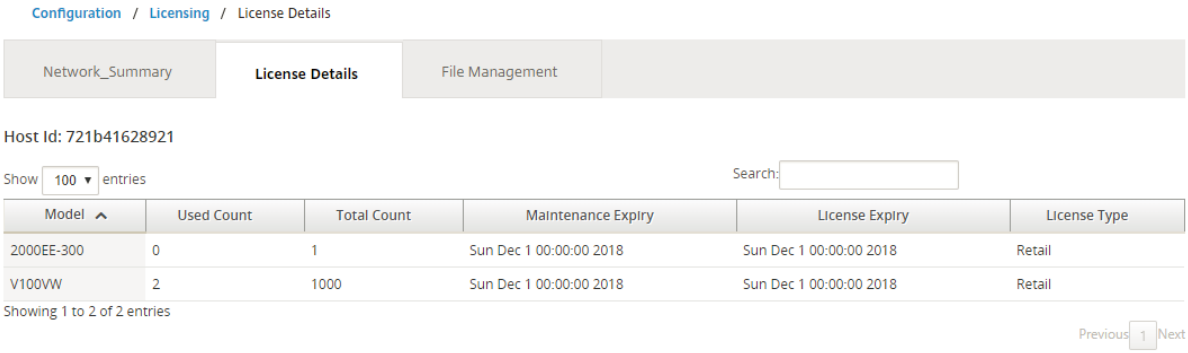
2. 在 SD-WAN Center GUI 中，导航到许可 > 文件管理。
3. 在上载文件部分中，单击浏览。从您的本地计算机中选择许可证文件，然后单击上载并安装。

   已安装的许可证文件将在文件下拉菜单中列出，您可以选择查看或删除许可证文件。



> 注意
>
> 主机 ID 为 SD-WAN Center 主机 ID，用于生成许可证文件。在 Citrix SD-WAN Center 上无法上载并安装使用不同主机 ID 生成的许可证文件。

您可以通过导航至配置 > 许可 > 许可证详细信息，来查看在 Citrix SD-WAN Center 上上载和安装的所有许可证文件的详细信息。



将显示以下参数：

- 型号：许可证支持的设备型号。
- 已用计数：安装了此许可证的设备数。
- 总计计数：可以安装此许可证的设备总数。
- 维护过期：Citrix 专享升级服务的过期日期。
- 许可证过期：许可证的过期日期。
- 许可证类型：许可证的类型。

从 Citrix SD-WAN Center 在 Azure 上部署 Citrix SD-WAN

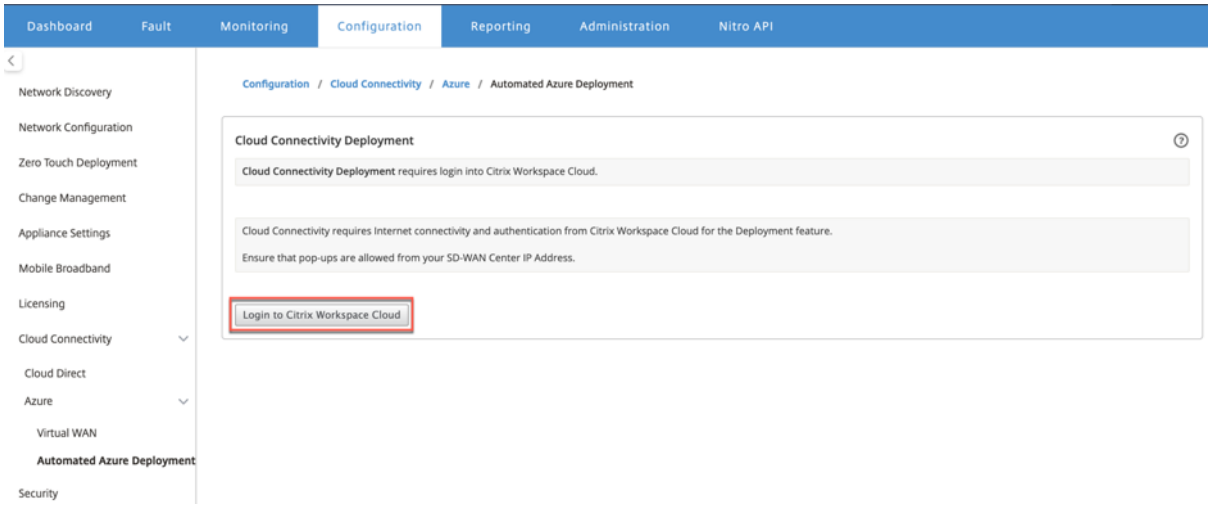
April 13, 2021

适用于 Azure 的 Citrix SD-WAN 使组织能够直接从每个分支到 Azure 中托管的应用程序建立直接安全的连接，而无需通过数据中心对云绑定流量进行回程处理。

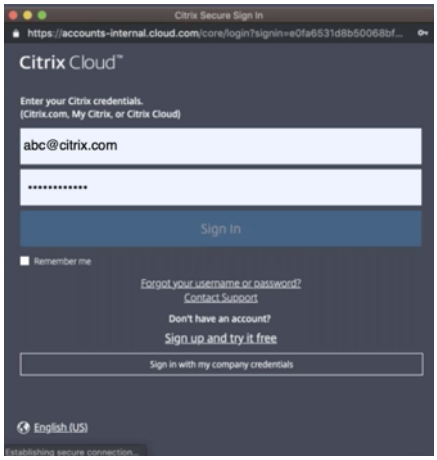
必备条件

- Citrix Workspace Cloud 凭据。
- Azure 订阅凭据
- Azure 应用程序和服务主体与基于角色的访问控制的访问权限，请参阅如何：使用门户创建可以访问资源的 Azure AD 应用程序和服务主体。
- 创建服务主体后，请记下以下详细信息：
  - Azure 订阅者 ID
  - 租户 ID
  - 应用程序 ID
  - 密钥
- 使用 ctx-sdw-sw-xxxxxxx 在 MCN/SD-WAN Center 上执行更改管理。
- 从 Citrix SD-WAN Center 中，发现 MCN 并拉取活动配置。

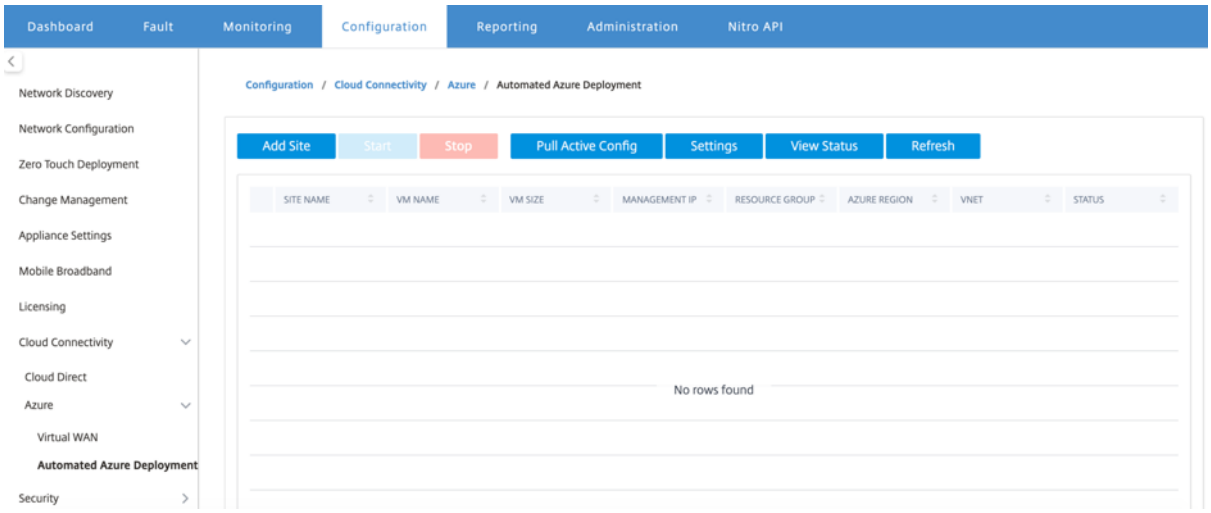
要在 Azure 上从 SD-WAN Center 部署 Citrix SD-WAN，请导航到配置 **>** 云连接 **> Azure >** 自动化 **Azure** 部署。



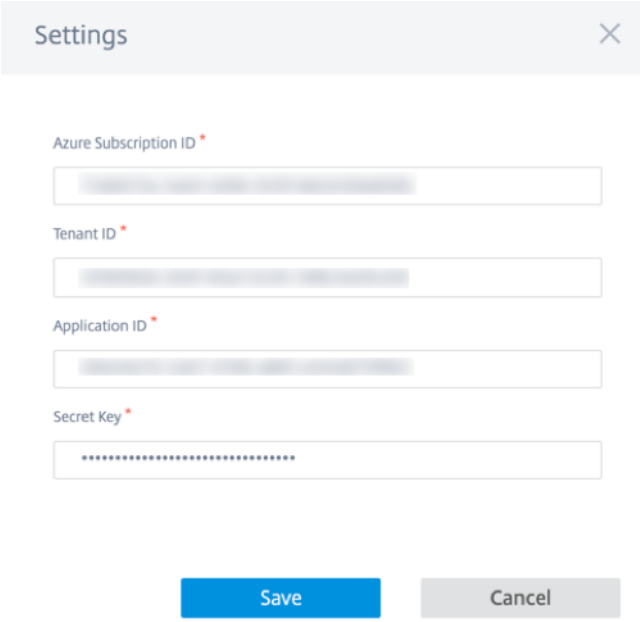
使用 Citrix Cloud 凭据登录。



自动化 **Azure** 部署



单击设置选项并提供 Azure 订阅的详细信息。单击“提取活动配置”选项可从 MCN 中检索活动的正在运行的配置。



在 **Azure** 中部署 **Citrix SD-WAN**

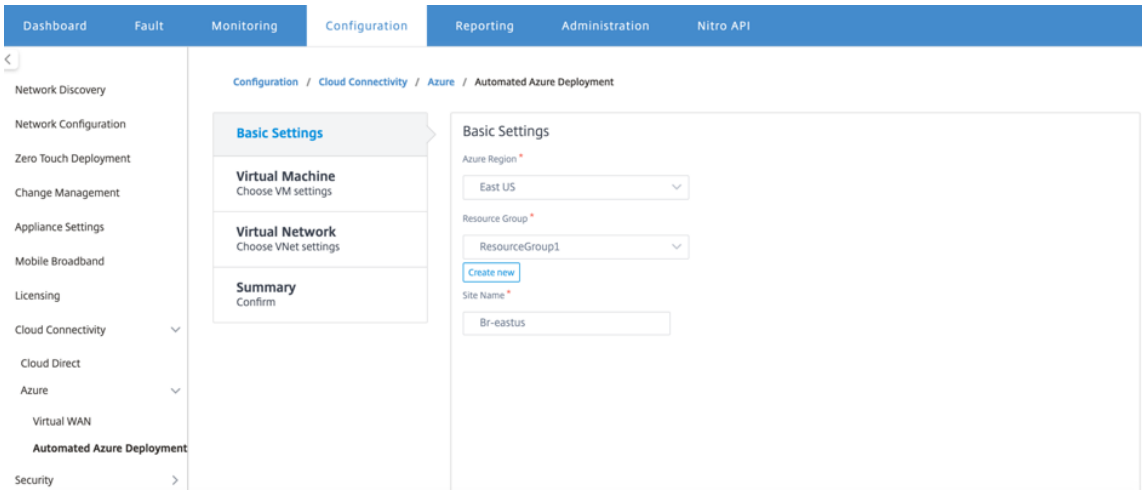
要在 Microsoft Azure 中部署 Citrix SD-WAN，请执行以下操作：

1. 单击添加站点以添加新的 SD-WAN 实例。它在 Azure 下启动在当前订阅下创建 SD-WAN 虚拟机。

   在此部署过程中，还可以执行以下操作：

   - 自动向 MCN 上的当前活动配置中添加新添加站点的 SD-WAN 配置。
   - 执行更改管理。
   - 将 MCN 的软件版本和配置应用于此新站点。

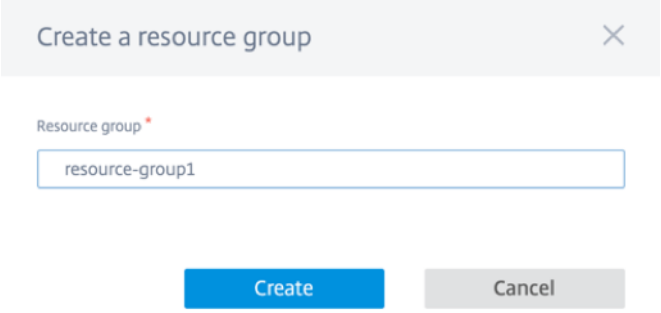
   完成基本设置、虚拟机和虚拟网络设置。



在“基本设置”下，从下拉列表中选择区域和资源组。选择区域后，资源组下拉列表将显示此订阅下此区域中的所有现有资源组。

> 注意：
>
> 要添加站点，资源组必须为空。

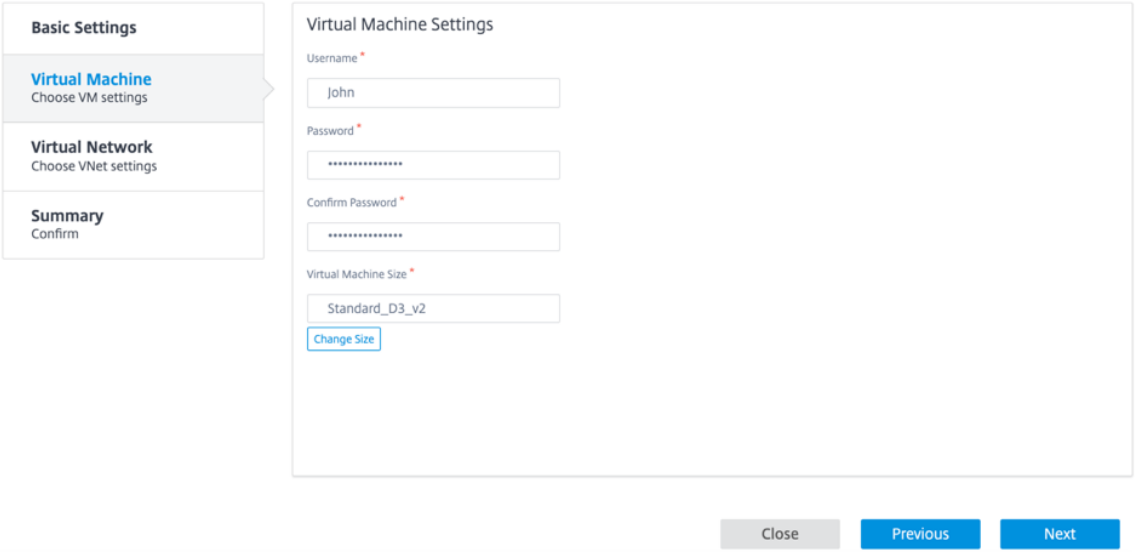
可以选择现有的空资源组，或单击 ** 新建选项以创建一个新的资源组。



2. 站点名称是使用区域名称自动生成的。您仍然可以根据需要编辑站点名称。

> 注意：
>
> 确保站点名称保持 SD-WAN 站点名称的要求，在 SD-WAN 网络中是唯一的。
>
> Azure 虚拟机名称是根据站点名称以 **AZ-regionname-sitename** 格式生成的。

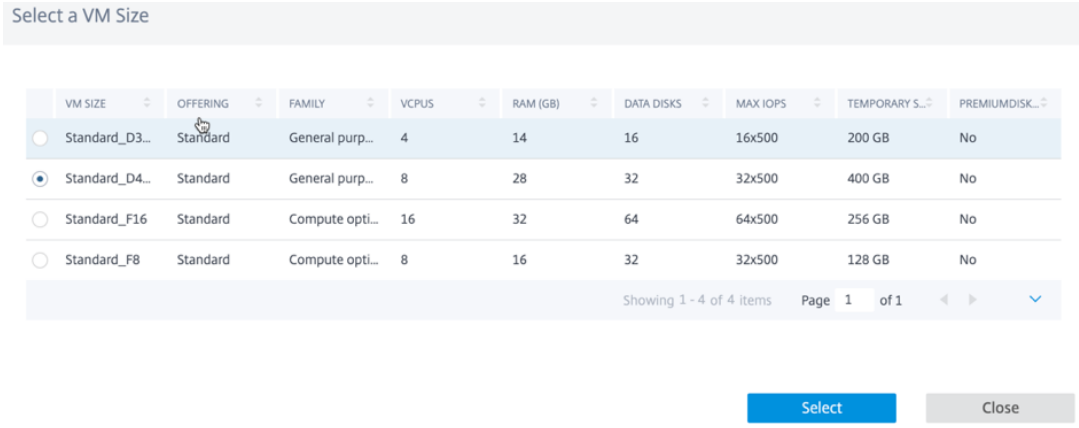
3. 单击 下一步 以配置虚拟机。



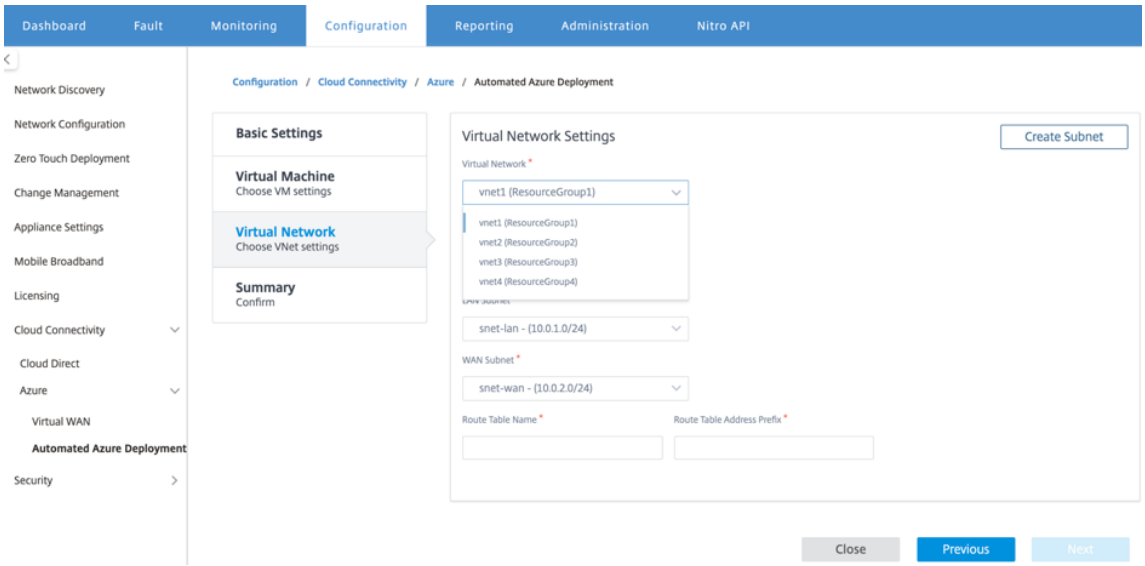
提供用户名、密码和确认密码。默认情况下，VM 的大小根据标准大小自动填充。如果需要，单击更改大小以选择不同的虚拟机大小。

注意：

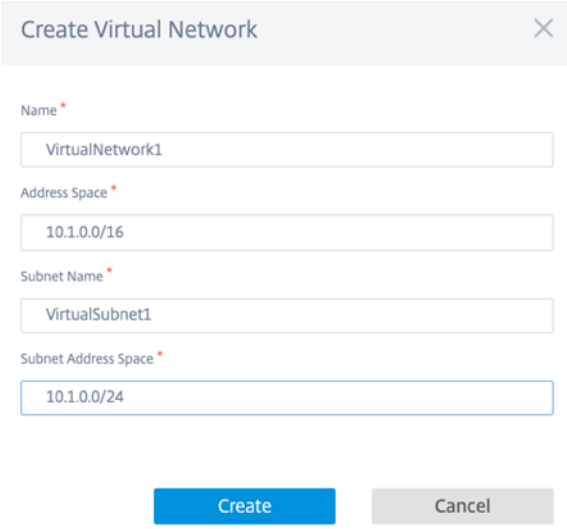
部署期间提供的此用户凭据具有对 Azure SD-WAN 的只读访问权限。要获得管理权限，请使用管理员凭据。



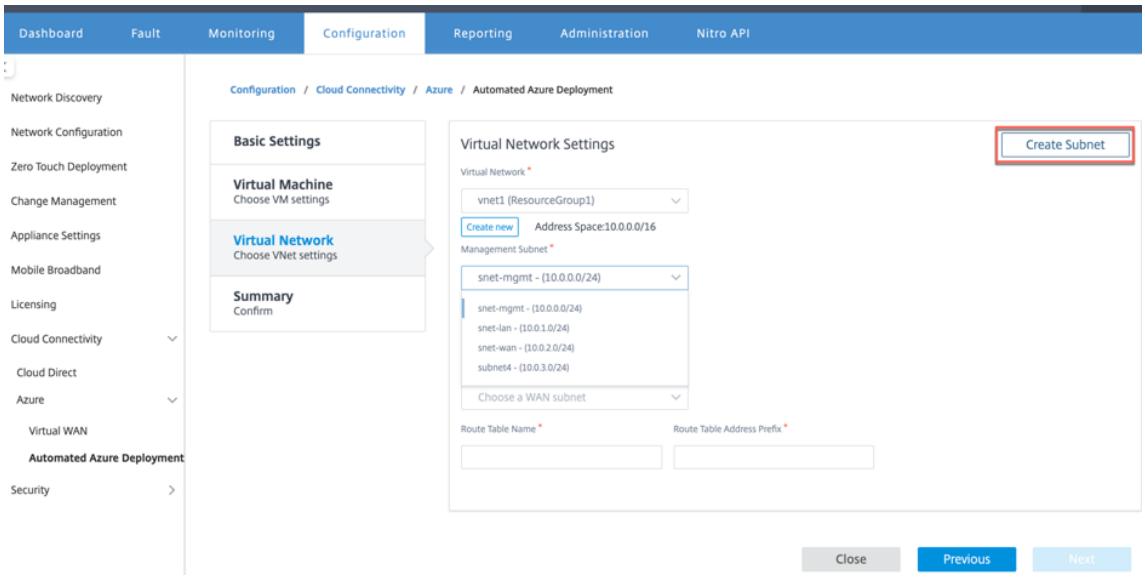
4. 单击下一步执行虚拟网络设置。
5. 从下拉列表中选择虚拟网络。该列表包含所选 Azure 区域中的所有虚拟网络。



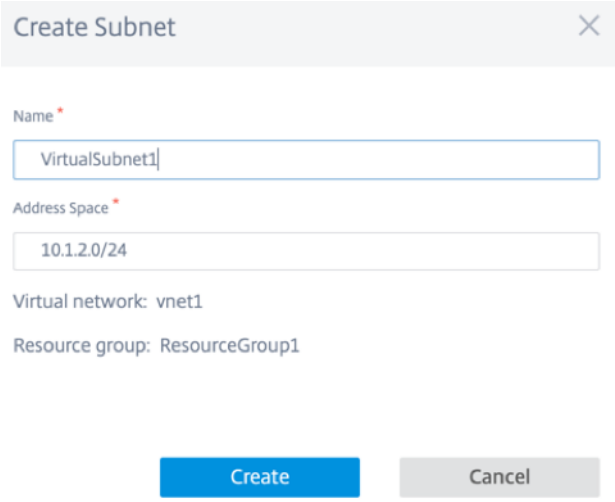
可以在现有虚拟网络上部署站点，也可以创建新的虚拟网络。单击新建创建新的虚拟网络。提供虚拟网络名称、地址空间（指定自定义专用 IP 地址空间)、子网名称和子网地址空间。



6. 选择一个子网进行管理。



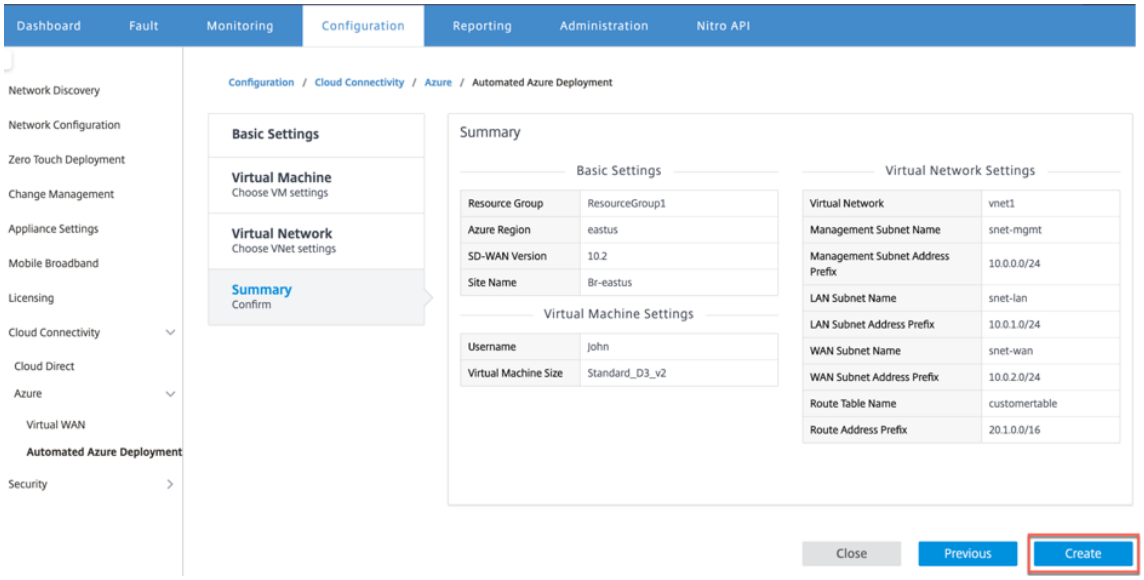
7. 还可以使用创建子网选项（从右上角开始）创建一个子网。



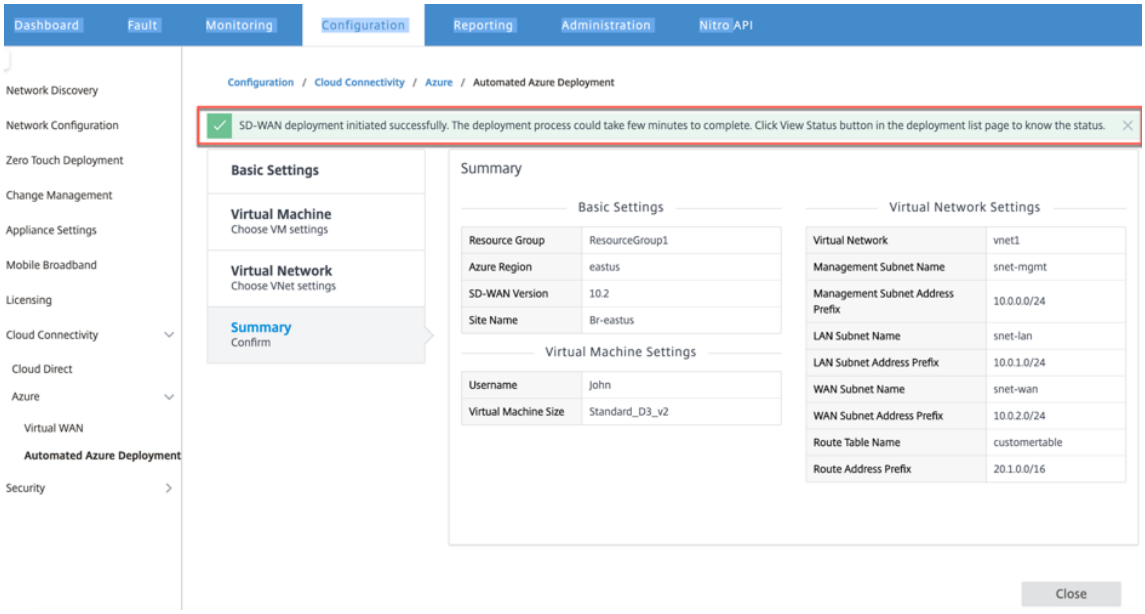
8. 从下拉列表中，选择适用于 LAN 和 WAN 的不同子网，并提供路由表名称以及路由表地址前缀。路由表地址前缀是重定向到此 SD-WAN 设备的目标地址空间。其他目标地址将通过 Azure 路由重定向。

> 注意：
>
> 路由表与 LAN 子网关联。如果选择的 LAN 子网已有关联的路由表，则将显示该路由表，并且无法对其进行修改。否则，您可以指定路由表名称。

9. 单击下一步查看并确认设置的详细信息，然后单击创建。



在顶部会显示一条状态消息，指出部署已成功启动。



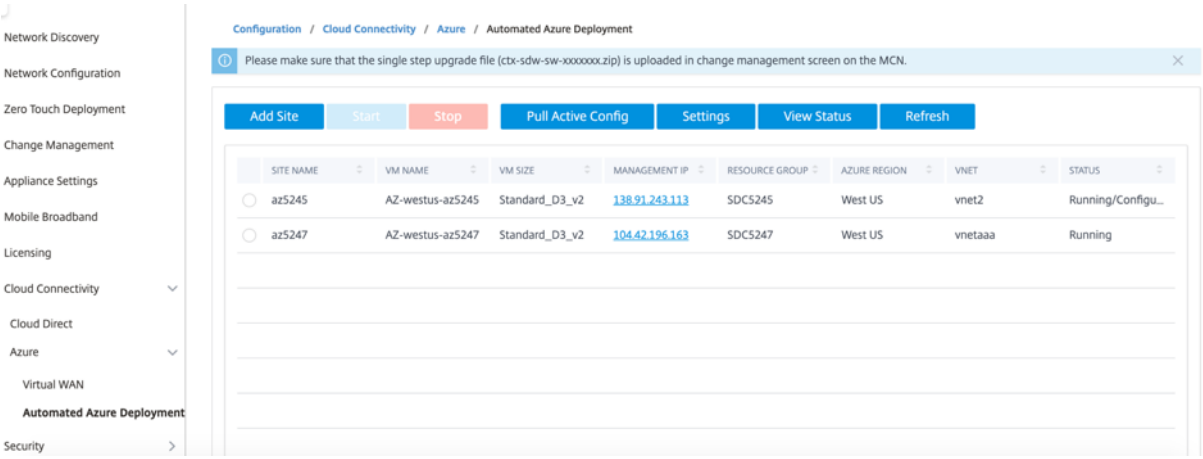
部署可能需要花费一些时间才能完成，建议您单击查看状态以获取有关部署状态的最新更新。

在部署过程中，请执行以下操作：

- 虚拟机将在选定的 Azure 区域中创建。
- 站点将自动添加到 SD-WAN 中的主动 SD-WAN 配置中。
- 在新置备的 Azure VM 上执行更改管理。

完成部署后，虚拟路径将在 MCN 与 Azure 站点之间建立。如果部署遇到错误，过程将回滚，所有自动创建的资源都将还原。

默认情况下，该站点作为默认路由域的一部分进行放置。它属于使用默认自动路径组的默认区域。



- 站点名称：Citrix SD-WAN 站点的名称。此站点名称在 Citrix SD-WAN 配置中使用。
- **VM** 名称：在 Azure 中预配的虚拟机 (VM) 的名称。
- **VM** 大小：在创建站点时选择的 vm 大小。

- 管理 **IP**：分配给新创建的 SD-WAN VM 的管理 IP 地址。
- 资源组：资源组为资源组之间的逻辑结构和数据交换始终可用。Azure 虚拟机属于此资源组。在 Citrix SD-WAN 部署期间创建的新资源在此资源组下进行分组。如果部署过程中出现任何错误，在此资源组中创建的资源将被删除。
- **Azure** 区域：表示资源组及其资源的位置。
- **VNet**：站点正在使用的虚拟网络。
- 状态：提供 VM 的状态。

单击刷新按钮以获取最新站点状态。您可以随时为所选站点启动或停止 VM。一次只能选择一个站点。

部署完成后，登录 MCN 或 Citrix SD-WAN Center 以查看虚拟路径的状态。

零接触部署

April 13, 2021

> 注意
>
> 仅在选择 Citrix SD-WAN 设备时支持零接触部署服务：
>
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition（需要重新创建映像）
> - SD-WAN 1000 Enterprise Edition（Premium Edition）（需要重新创建映像）
> - SD-WAN 1100 标准版
> - SD-WAN 1100 Premium (Enterprise) Edition
> - SD-WAN 2000 Standard Edition（需要重新创建映像）
> - SD-WAN 2000 Enterprise Edition（Premium Edition）（需要重新创建映像）
> - SD-WAN AWS VPX 实例

零接触部署 (ZTD) 服务是一种 Citrix 的受管理云服务，允许在 Citrix SD-WAN 网络中发现新设备，并自动完成分支机构的部署过程。可以从网络中的任何节点或通过安全套接字层 (SSL) 协议访问 ZTD 云服务。

ZTD 云服务可以与后端 Citrix 网络服务进行安全通信，以便为购买了零接触功能的设备（例如 SD-WAN 410-SE、2100-SE）进行身份验证。后端服务已就位，可以对任何零接触部署请求进行身份验证，从而正确验证客户帐户与 Citrix SD-WAN 设备的序列号之间的关联。

ZTD 高级架构和工作流

数据中心网站

Citrix SD-WAN 管理员–具有以下主要职责的 SD-WAN 环境的管理权限的用户：

- 使用 Citrix SD-WAN Center 网络配置工具创建配置，或从主控制节点 (MCN) SD-WAN 设备导入配置
- Citrix Cloud 登录为新站点节点部署启动零接触部署服务。

> 注意
>
> 如果您的 SD-WAN Center 通过代理服务器连接到 Internet，则必须在 SD-WAN Center 上配置代理服务器设置。有关详细信息，请参阅 零接触部署的代理服务器设置。

网络管理员–负责企业网络管理（DHCP、DNS、Internet、防火墙等）的用户

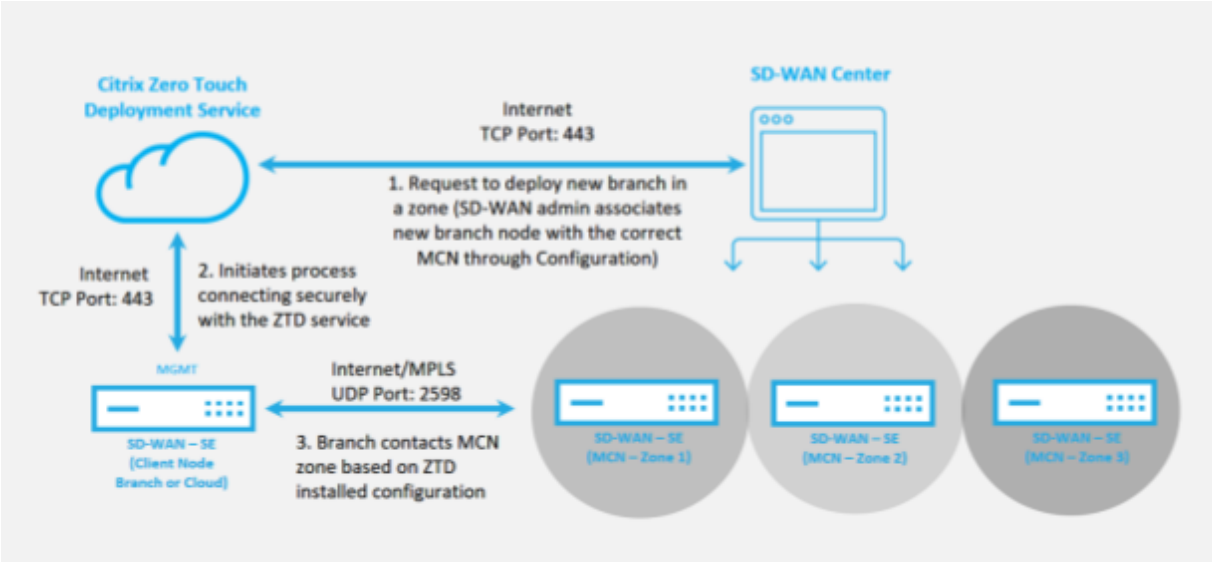
- 如有必要，请将防火墙设置为从 SD-WAN Center 向 FQDN ***sdwanzt.citrixnetworkapi.net*** 出站通信。

远程站点

现场安装程序–本地联系或使用以下主要职责的上门活动安装程序：

- 物理解压 Citrix SD-WAN 设备。
- 重新映像非 ZTD 就绪设备。
  - 所需的：SD-WAN 1000-SE、2000-SE、1000-EE、2000-EE
  - 不是必需的：SD-WAN 410-SE、2100-SE
- 电源线的设备。
- 在管理接口上连接设备的 Internet 连接（例如，MGMT 或 0/1)。
- 在数据接口（例如 apA.WAN、apB.WAN、apC.WAN、0/2、0/3、0/5 等）上连接设备以实现 WAN 链接连接。

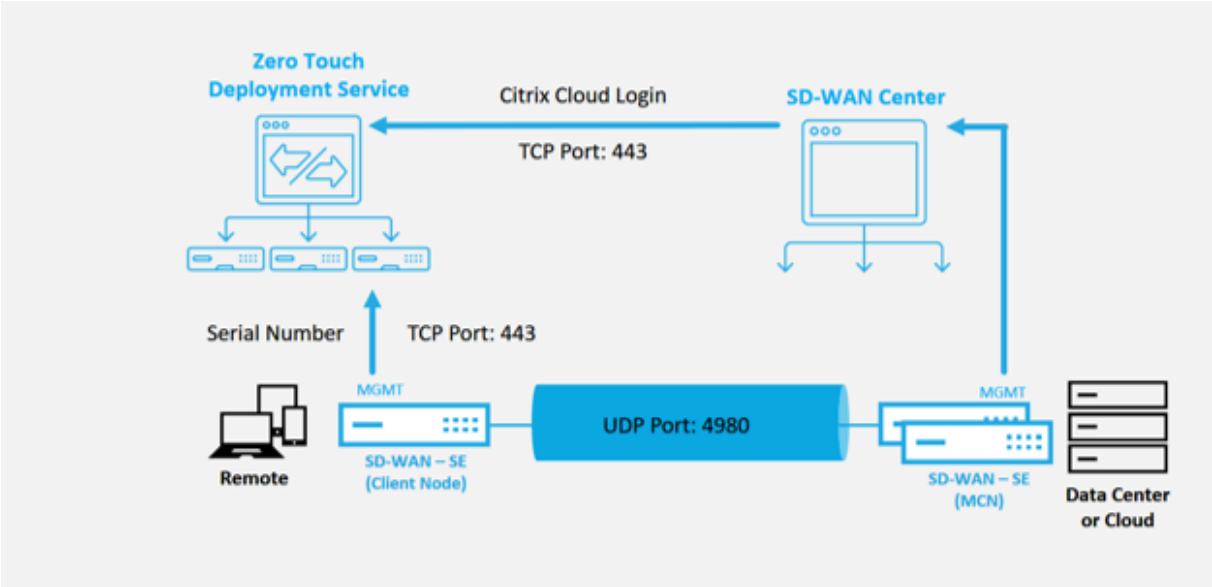
> 注意
>
> 每种模式的界面布局各不相同，因此，请参阅文档以了解数据和管理端口的标识。



需要满足以下必备条件，才能启动任何零接触部署服务：

- 主动运行 SD-WAN 提升到主控制节点 (MCN)。
- 主动运行 SD-WAN Center（通过虚拟路径连接到 MCN）。
- 在 https://onboarding.cloud.com 上创建 Citrix Cloud 登录凭据（在创建帐户时引用下面的说明）。
- 在端口 443 上直接管理或通过代理服务器管理到 Internet 网络连接（SD-WAN Center 和 SD-WAN 设备）。
- 在端口 443 上连接 Internet 以访问 SD-WAN Center Web 门户以进行 ZTD 初始设置。
- （可选）在客户端模式下，至少有一台主动运行在分支机构的 SD-WAN 设备，并且有效的虚拟路径可以连接到 MCN，以帮助验证在现有底层网络中成功建立的路径。

最后一个必备条件并不是必需的，但允许 SD-WAN 管理员验证 underlay 网络是否允许在使用任何新添加的站点完成零接触部署完成时建立虚拟路径。这主要是验证适当的防火墙和路由策略是否已在相应的 NAT 流量中使用，或者确认 UDP 端口 4980 是否能够成功进入网络以到达 MCN。



零接触部署服务概述

零接触部署服务与 SD-WAN Center 结合使用，以提供更易于部署的分支机构 SD-WAN 设备。SD-WAN Center 已配置为用于 SD-WAN Standard 和 Enterprise (Premium) Edition 设备的中央管理工具。要使用零接触部署服务(或 ZTD 云服务)，管理员必须先部署环境中的第一个 SD-WAN 设备，然后将 SD-WAN Center 配置和部署为中央管理点。当 SD-WAN Center（版本 9.1 或更高版本）与公共 Internet 连接到端口 443 时，SD-WAN Center 将自动启动云服务并安装必要的组件以解锁零接触部署功能，并使在 SD-WAN Center 的 GUI 中提供零接触部署选项。默认情况下，在 SD-WAN Center 软件中不提供零接触部署。这是为了在允许管理员启动任何涉及零接触部署的现场活动之前，确保底层网络中存在适当的初始组件。

正在运行的 SD-WAN 环境启动并向零接触部署服务中运行注册后，将通过创建 Citrix Cloud 帐户登录来完成。通过 SD-WAN Center 能够与 ZTD service 通信，GUI 会在“配置”选项卡下显示零接触部署选项。登录零接触服务会对与特定 SD-WAN 环境关联的客户 ID 进行身份验证，并注册 SD-WAN Center，以进一步对 ZTD 设备部署进行身份验证。

使用 SD-WAN Center 中的网络配置工具时，SD-WAN 管理员需要利用模板或克隆站点功能来构建 SD-WAN 配置以添加新站点。SD-WAN Center 使用新配置为新添加的站点启动 ZTD 部署。当 SD-WAN 管理员使用 ZTD 进程启动站点以进行部署时，他或她可以选择通过预填充序列号对设备进行预身份验证，从而在现场安装程序启动电子邮件以开始使用现场活动。

现场安装程序会接收电子邮件通信，表明该站点已准备就绪，可以进行零接触部署，并且可以开始执行安装过程，以便在 MGMT 端口上启动并连接设备，以实现 DHCP IP 地址分配以及访问 Internet。此外，还可以通过任何 LAN 和 WAN 端口布线。其他所有内容均由 ZTD Service 发起，并通过使用激活 URL 进行监视。如果要安装的远程节点是云实例，打开激活 URL 时，将开始执行工作流以自动在指定的云环境中安装实例，本地安装程序不需要执行任何操作。

零接触部署云服务可自动执行以下操作：

如果分支设备上提供了新功能，请下载并更新 ZTD 代理。

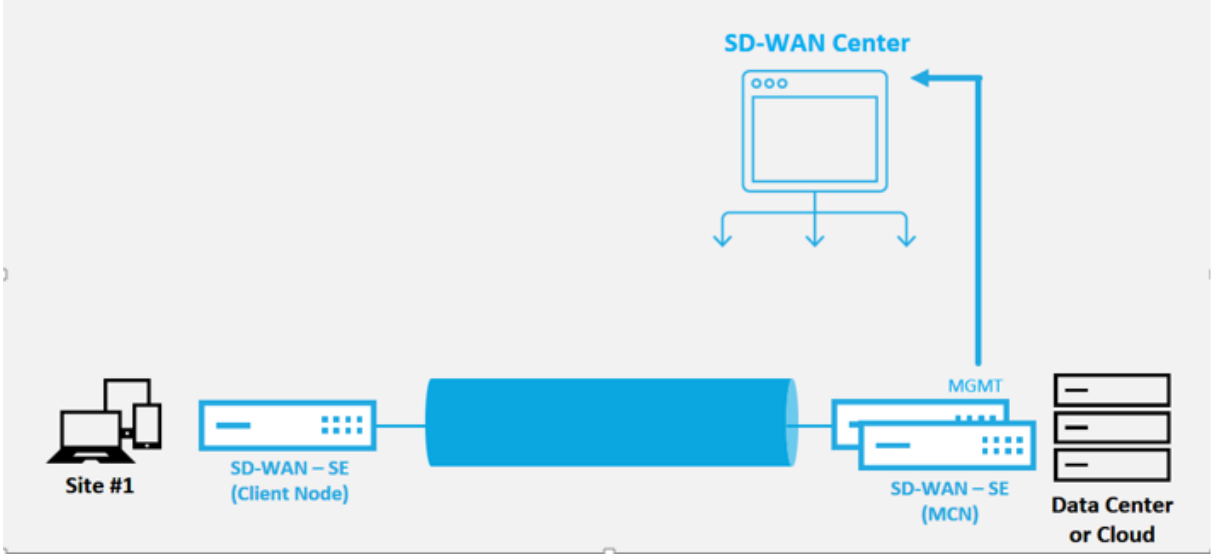
- 通过验证序列号对分支设备进行身份验证。
- 通过身份验证 SD-WAN 管理员是否已使用 SD-WAN Center 接受了用于 ZTD 的站点。
- 从 SD-WAN Center 拉出目标设备特定的配置文件。
- 将特定于目标设备的配置文件推送到分支设备。
- 在分支设备上安装配置文件。
- 将任何丢失的 SD-WAN 软件组件或所需更新推送到分支设备。
- 推送一个临时 10 Mbps 许可证文件，以确认与分支设备建立的虚拟路径。
- 在分支设备上启用 SD-WAN 服务。

要在设备上安装永久性许可证文件，SD-WAN 管理员需要执行更多步骤。

零接触部署服务程序

以下过程详细介绍了使用零接触部署服务部署新站点所需的步骤。有一个正在运行的 MCN 和一个客户端节点已使用与 SD-WAN Center 的正确通信，以及已建立的虚拟路径来确认跨基础网络的连接。要启动零接触部署，SD-WAN 管理

员需要执行以下步骤：



如何配置零接触部署服务

SD-WAN Center 可以接受来自新连接的设备的请求以加入 SD-WAN Enterprise 网络。请求通过零接触部署服务转发到 Web 界面。设备连接到服务后，将下载配置和软件升级软件包。

配置工作流：

- 访问 **SD-WAN Center** > 创建新站点配置或导入现有配置并保存。
- 登录 Citrix Workspace Cloud 以启用 ZTD 服务。“零接触部署”菜单选项现在显示在 SD-WAN center Web 管理界面中。
- 在 SD-WAN Center 中，导航到配置 > 零接触部署 > 部署新站点。
- 选择一个设备，单击启用，然后单击部署。
- 安装程序接收激活电子邮件 > 输入序列号 > 激活 > 设备已成功部署。

要配置零接触部署服务，请执行以下操作：

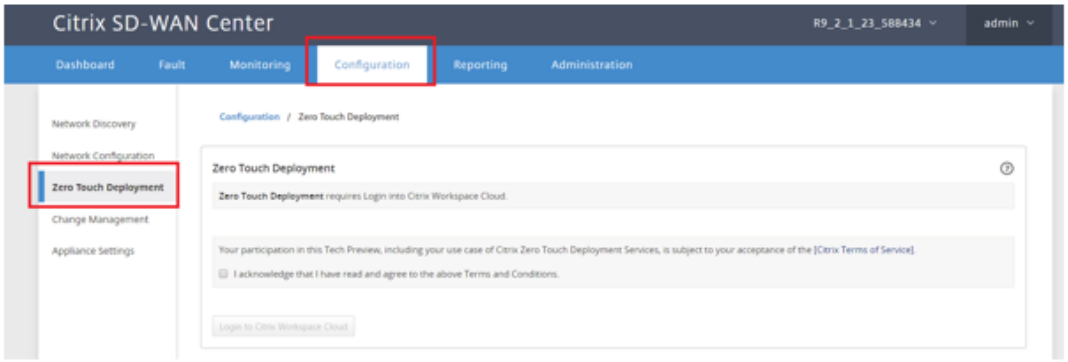
1. 安装 SD-WAN Center（启用了零接触部署功能)。

   a) 安装 SD-WAN Center（具有 DHCP 分配的 IP 地址)。

   b) 验证 SD-WAN Center 是否分配了正确的管理 IP 地址和网络 DNS 地址，并通过管理网络与公用 Internet 建立连接。

   c) 将 SD-WAN Center 升级到最新的 SD-WAN 软件发行版本。

   d) 在使用正确的 Internet 连接的情况下，SD-WAN Center 将启动零接触部署 (ZTD) 云服务，并自动下载并安装特定于 ZTD 的任何固件更新，如果此自动通报过程失败，则使用以下零接触部署选项在 GUI 中将不可用。



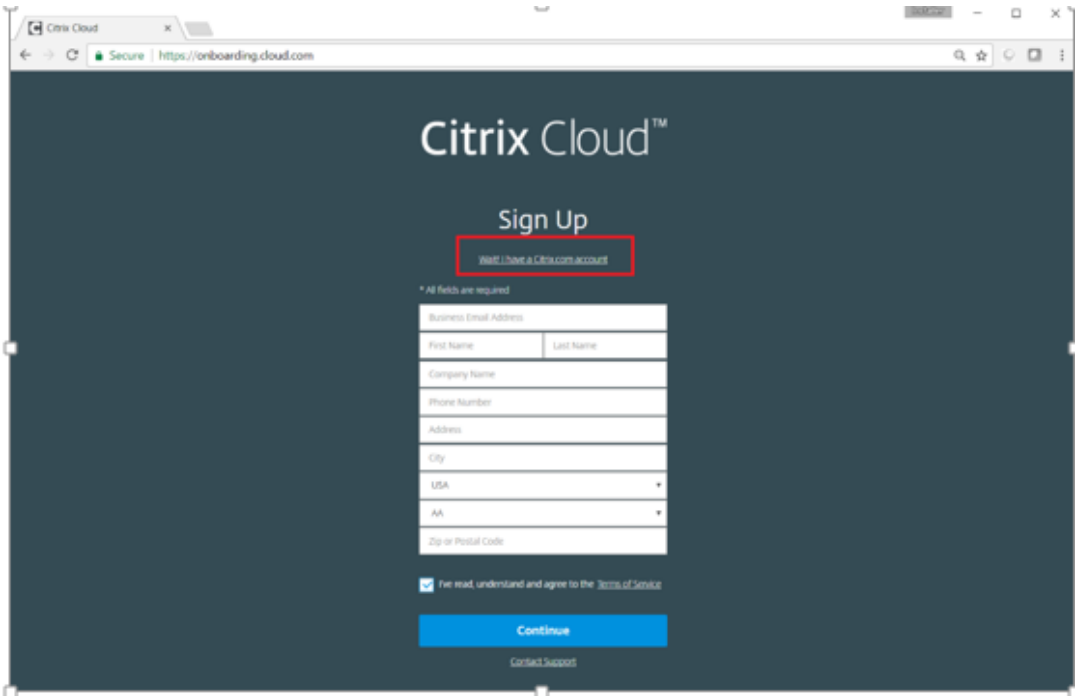
e) 阅读条款和条件，然后选择我已确认我已阅读并同意上述条款和条件。

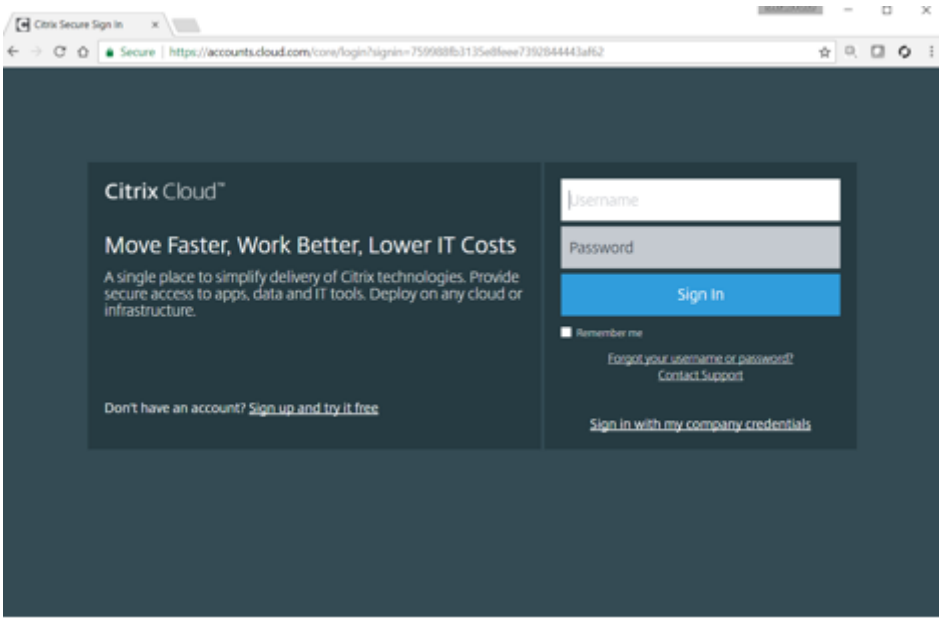
f) 如果已创建 Citrix Cloud 帐户，请单击登录 **Citrix Workspace Cloud** 按钮。

g) 登录到 Citrix Cloud 帐户，收到以下成功登录消息后，请不要关闭此窗口，该过程需要另外 **20** 秒钟才能刷新 **SD-WAN Center GUI**。窗口完成后应该自行关闭。**

h) 要创建云登录帐户，请执行以下操作：

- 打开 Web 浏览器以https://onboarding.cloud.com
- 单击请稍候，我有一个 **Citrix.com** 帐户链接。





i) 使用现有 Citrix 帐户登录。

j) 登录到 SD-WAN Center 零接触部署页面后，您可能会注意到 ZTD 部署中不存在任何站点，原因如下：

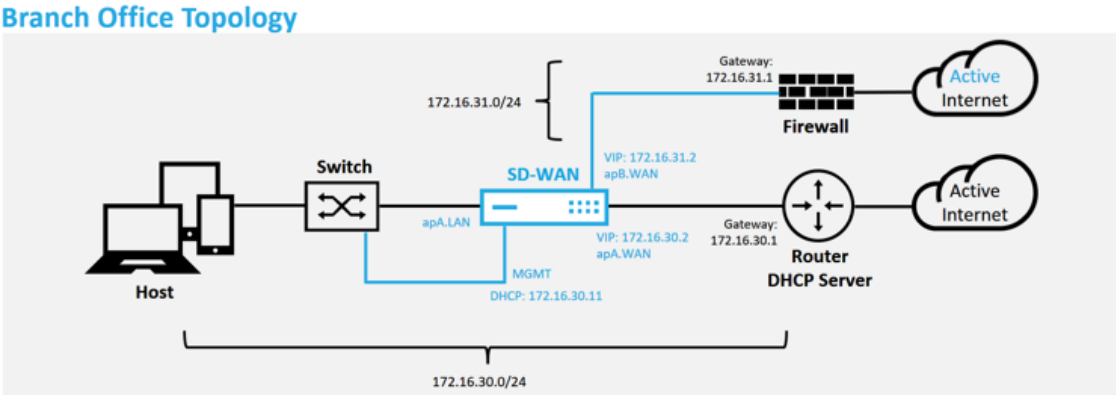
- 尚未从 配置 下拉菜单中选择活动配置
- 当前活动配置的所有站点都已部署
- 配置不是使用 SD-WAN Center 建立的，而是在 MCN 上可用的配置编辑器
- 站点未在配置中构建引用零个支持触摸的设备（例如 410-SE、2100-SE、Cloud VPX）

2. 更新配置，以使用 **ZTD** 功能的 **SD** 设备 (使用 SD-WAN Center 网络配置）添加新远程站点。

如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。应使用以下过程添加针对零接触部署的新站点。

通过首先列出新站点的详细信息（即设备型号、接口组使用情况、虚拟 IP 地址、带宽与带宽及其各自的网关），为 SD-WAN 设备部署设计新站点。

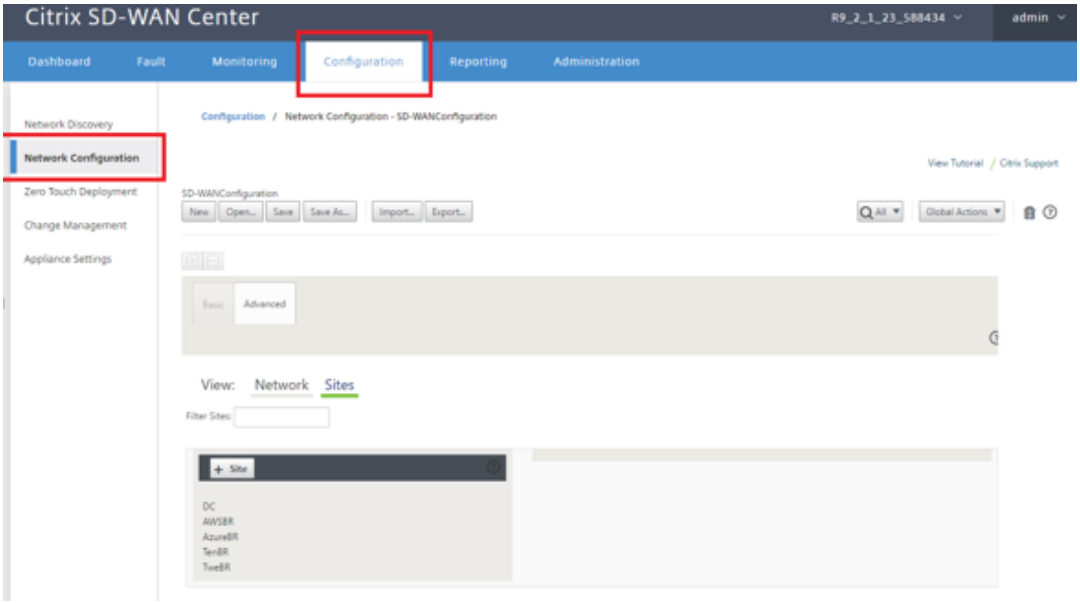
> 重要
>
> 您可能会注意到，还列出了已选中 VPX 的任何站点节点，但当前 ZTD 支持仅适用于 AWS VPX 实例。
>
> 注意
>
> - 请务必使用 Citrix SD-WAN Center 支持的 Web 浏览器
> - 确保 Web 浏览器在 Citrix Workspace 登录过程中不阻止任何弹出窗口



这是分支机构站点的部署示例，SD 设备物理上部署在 172.16.30.0/24 网络中的现有 MPLS WAN 链接的路径中，并通过将现有备份链接启用为“活动”状态并将其终止而使用现有备份链接。WAN 链接直接连接到不同子网 172.16.31.0/24 上的 SD-WAN 设备。

> 注意
>
> SD-WAN 设备 automatably 为默认 IP 地址 192.168.100.1/16 分配一个默认 IP 地址。默认情况下启用 DHCP 时，网络中的 DHCP 服务器可能会在与默认值重叠的子网中为设备提供第二个 IP 地址。这可能会导致设备上的路由问题，设备可能无法连接到 ZTD Cloud 服务。将 DHCP 服务器配置为分配在 192.168.0.0/16 范围内的 IP 地址。
>
> 有各种不同的部署模式可用于在网络中放置 SD-WAN 产品。在上面的示例中，将在现有网络基础结构的顶部将 SD-WAN 部署为覆盖。对于新站点，SD-WAN 管理员可以选择在边缘模式和网关模式部署中部署 SD-WAN，无需使用 WAN Edge 路由器和防火墙，也不需要将 Edge 路由和防火墙的网络需求整合到 SD-WAN 解决方案上。

a) 打开 **SD-WAN Center Web** 管理界 面，然后导航到 配置 > 网络配置 页面。



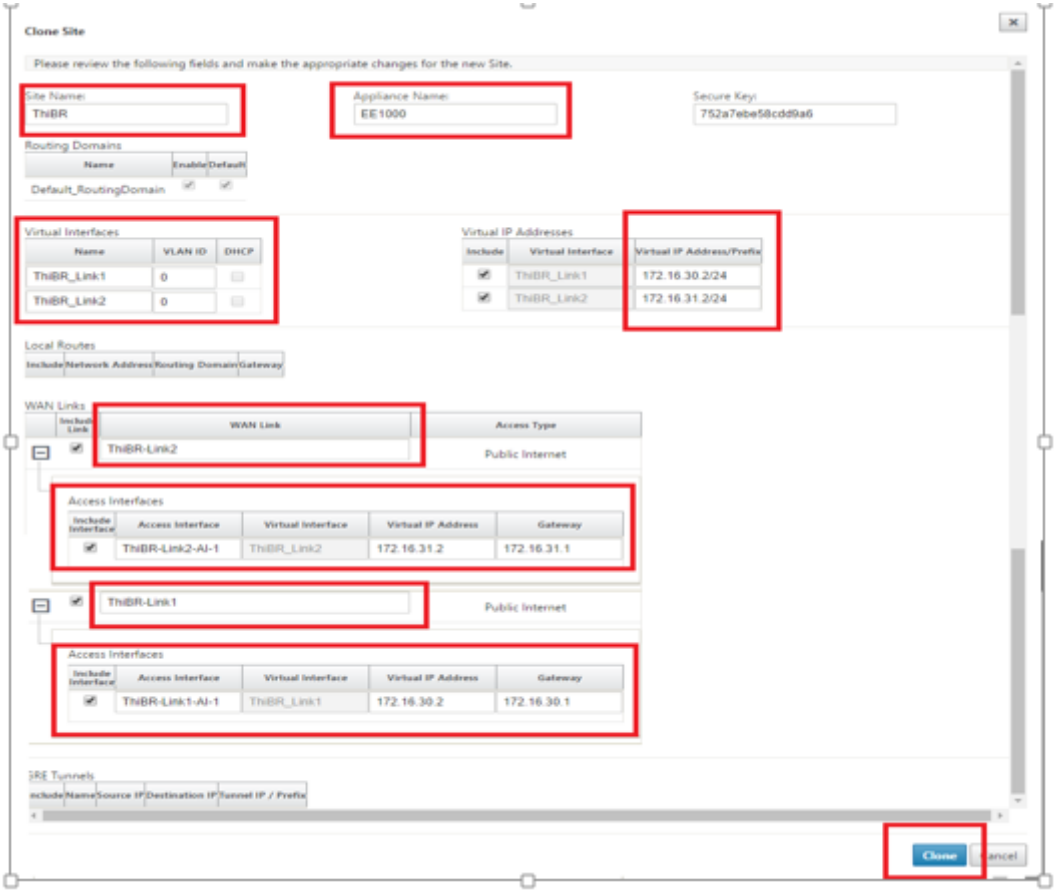
b) 确保已准备好正在运行的配置，或从 MCN 导入配置。

c) 导航到 高级 选项卡以创建站点。

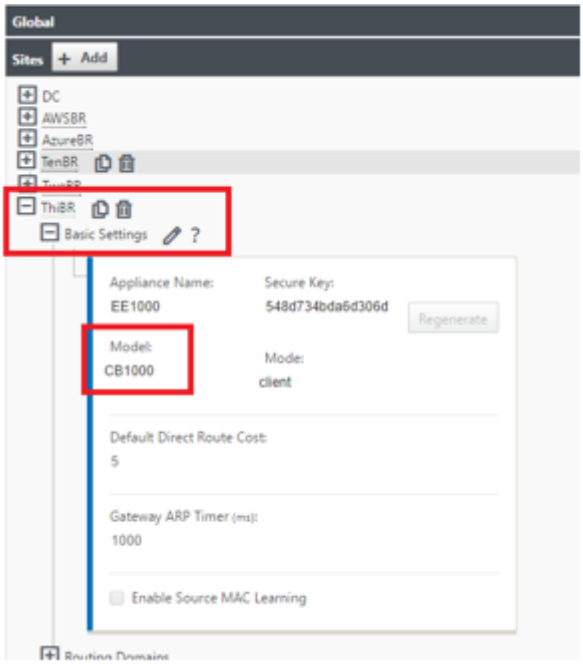
d) 打开 站点 磁贴以显示当前配置的站点。

e) 通过使用任何现有站点的克隆功能，快速构建新站点的配置。

f) 填充为此新分支站点 设计的拓扑中的所有必填字段



g) 克隆新站点后，导航到该站点的基本设置，并验证是否正确选择了要支持零接触服务的 SD-WAN 的型号。



h) 可以对站点的 SD-WAN 模型进行更新，但请注意，可能必须重新定义接口组，因为更新后的设备可能具

有新的界面布局，之后将使用克隆。

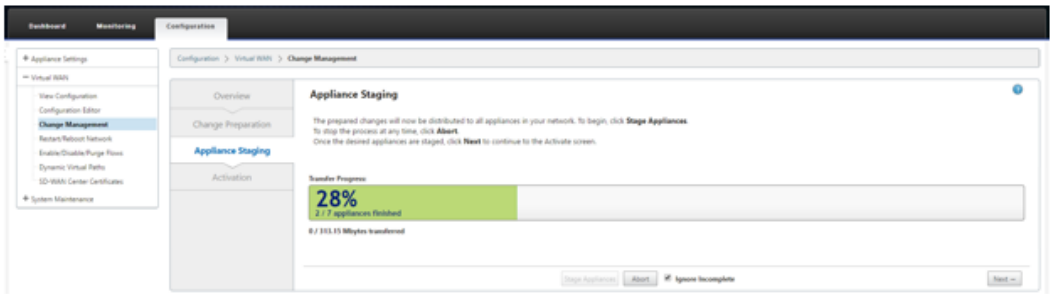
i) 在 SD-WAN Center 上保存新配置，并使用导出到更改管理收件箱选项，以使用更改管理推送配置。

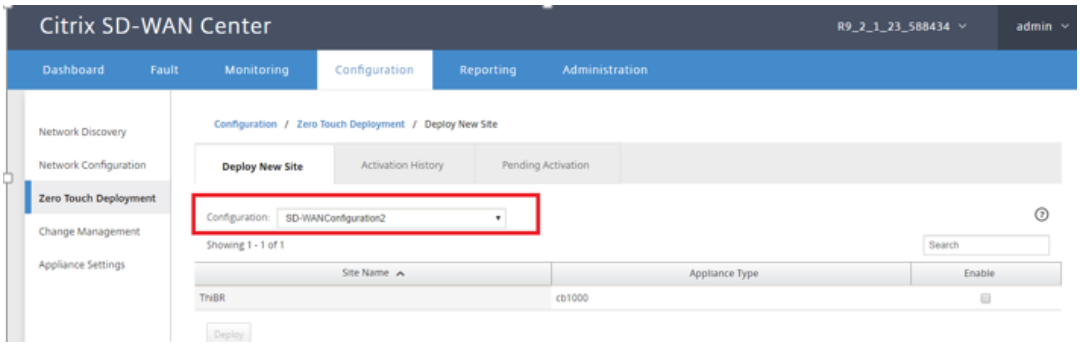
j) 按照更改管理过程来正确转移新配置，这样会导致现有 SD-WAN 设备知晓要通过零接触部署的新站点，您需要使用“忽略不完整”选项跳过尝试推送在新站点上配置，仍需要通过 ZTD 工作流。

3. 导航回 SD-WAN Center 零接触部署页面，在运行新的活动配置的情况下，将有新站点可供部署。

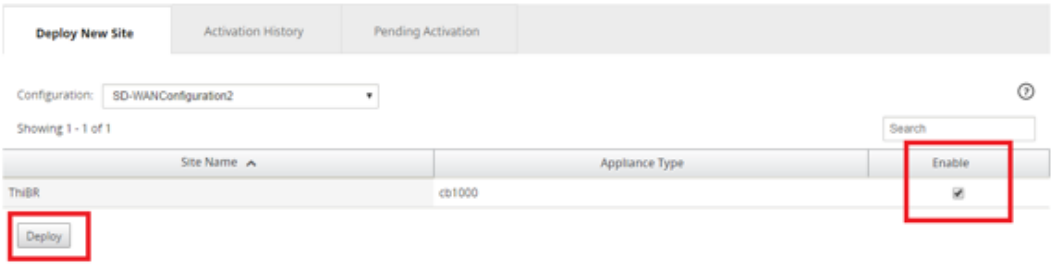
a) 在零接触部署页面的部署新站点选项卡下，选择正在运行的网络配置文件

b) 选择正在运行的配置文件后，将显示具有零接触支持的未部署 SD 设备的所有分支站点的列表。

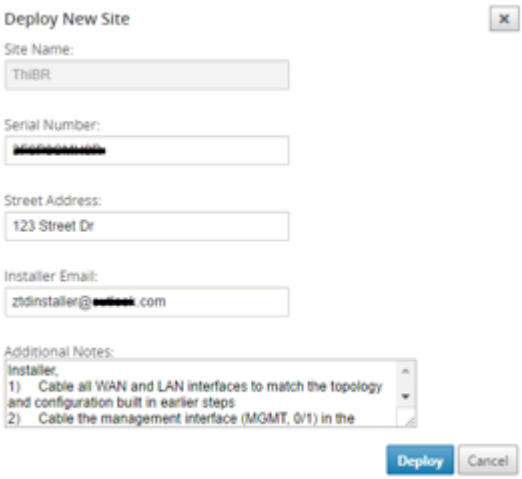




c) 选择要为零接触服务配置的分支站点，单击启用，然后再进行部署。



d) 此时将显示部署新站点弹出窗口，在此窗口中，管理员可以提供序列号、分支站点街道地址、安装程序电子邮件地址以及其他备忘录（如有必要）。

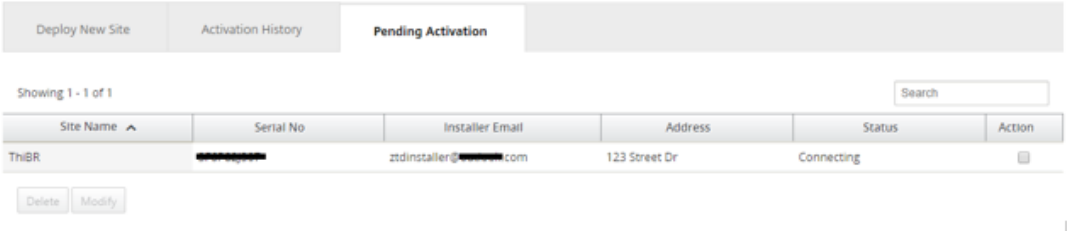


> 注意
>
> - “序列号”条目字段为可选字段，如果填充了此字段，则会导致安装程序负责在现场活动中进行更改。
> - 如果填充了“序列号”字段，则无需安装程序将序列号输入到使用“部署站点”命令生成的激活 URL 中。
> - 如果“序列号”字段为黑色，则安装程序将负责将设备的正确序列号输入到使用“部署站点”命令生成的激活 URL 中。

a) 单击部署按钮后，将显示一条消息，指出“站点配置已部署”。

b) 此操作将触发 SD-WAN Center（以前在 ZTD 云服务中注册），以将此特定站点的配置临时存储在 ZTD 云服务中。

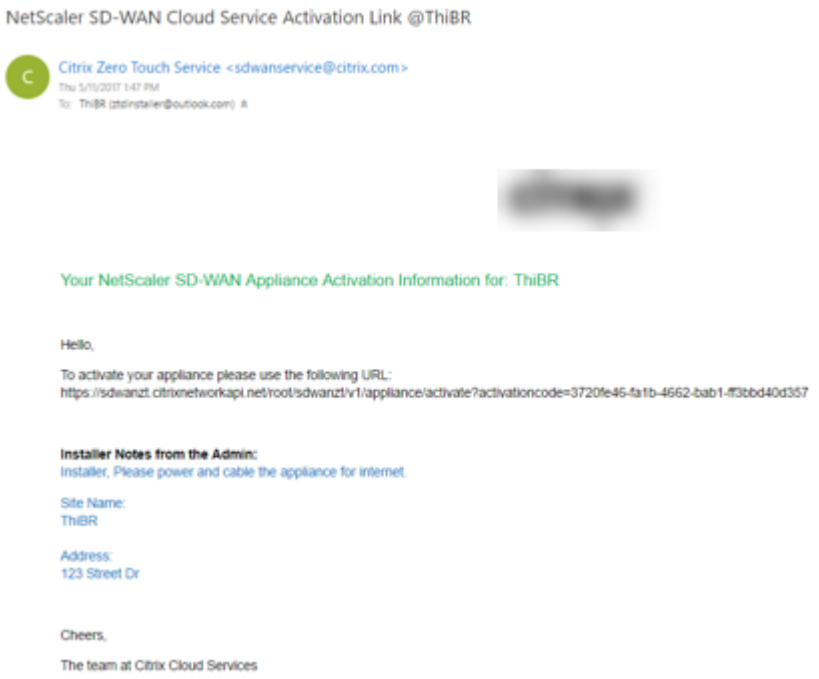
c) 导航到“挂起的激活”选项卡，确认已成功填充分支站点信息，并将其设置为待执行的安装程序活动状态。



> 注意
>
> 如果信息不正确，可以选择删除或修改挂起的激活状态的零接触部署。如果从“挂起的激活”页面中删除了一个站点，该站点将可以在部署新站点选项卡页面中部署。选择将分支站点从挂起的激活中删除后，发送到安装程序的激活链接将失效。
>
> 如果 SD-WAN 管理员未填充序列号字段，则状态字段将指示“正在等待安装程序”而非“正在连接”。

4. 下一系列活动由现场安装程序执行。

   a) 安装程序将验证邮箱中是否有 SD-WAN 管理员在部署站点时使用的电子邮件地址。



b) 在 Internet 浏览器窗口中打开零接触部署激活 URL。

c) 如果 SD-WAN 管理员未在部署站点步骤中预填充序列号，则安装程序将负责找到物理设备上的序列号，并手动将序列号输入到激活 URL 中，然后单击激活按钮。

d) 如果管理员预填充序列号信息，激活 URL 将一直准备执行下一个步骤。

e) 安装程序的物理位置必须在现场，以执行以下操作：

- 连接所有 WAN 和 LAN 接口，使其与之前步骤中构建的拓扑和配置相匹配。
- 在网络中提供 DHCP IP 地址和通过 DNS 将 FQDN 连接到 IP 地址解析的网络段中的管理接口（MGMT、0/1）电缆。

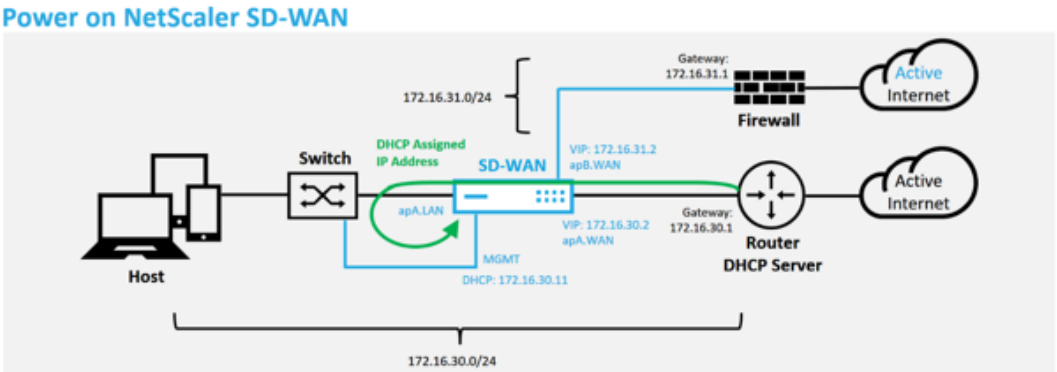
- 电源线 SD-WAN 设备。
- 打开设备的电源开关。

> 注意
>
> 连接电源线时，大多数设备将自动启动。某些设备可能必须使用设备前面的电源开关打开，而其他设备可能会在设备背面安装电源开关。某些电源开关需要按住电源按钮，直到设备启动。

5. 下一系列步骤通过零接触部署服务的帮助自动完成，但需要使用以下必备条件。

   - 分支设备应启动电源
   - DHCP 必须在现有网络中可用，以分配管理和 DNS IP 地址
   - 任何 DHCP 分配的 IP 地址都要求连接到 Internet，能够解析 FQDN
   - 只要其他先决条件满足以下条件，就可以手动配置 IP 分配。

   a) 设备从网络 DHCP 服务器获取 IP 地址，在此示例中，拓扑通过出厂默认状态设备的跳过数据接口实现。

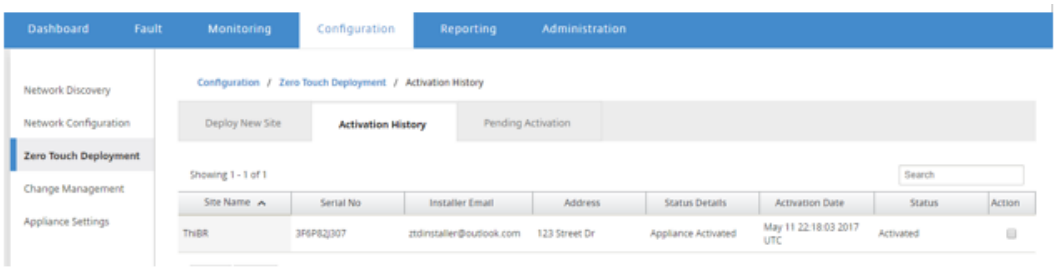


   b) 当设备从 underlay 网络 DHCP 服务器获取 Web 管理和 DNS IP 地址时，该设备将启动零接触部署服务并下载所有与 ZTD 有关的软件更新。

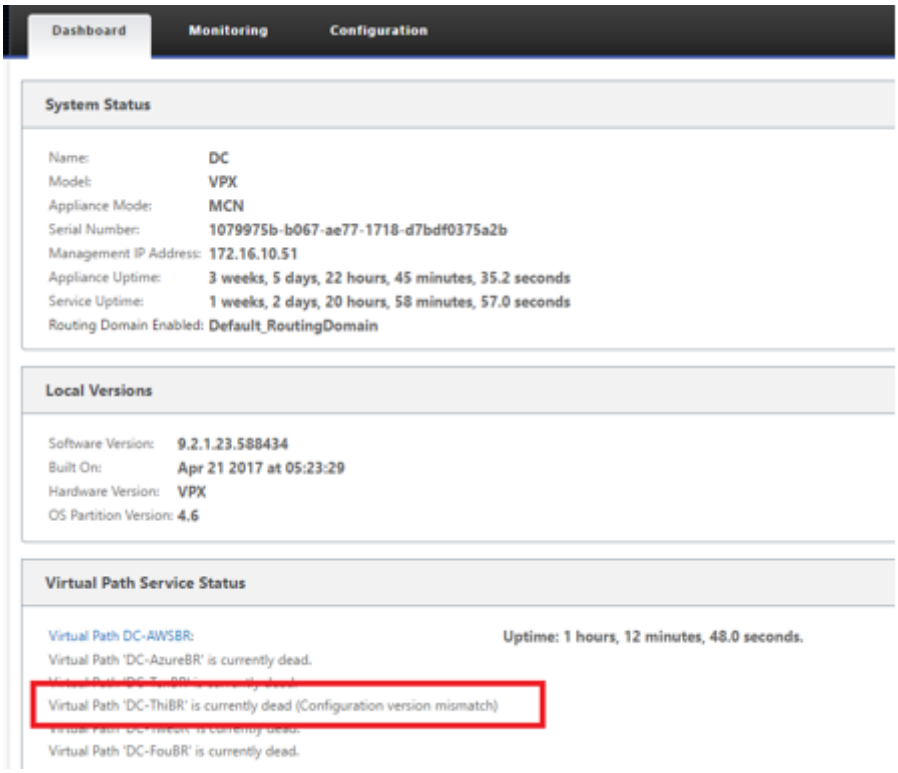
   c) 成功连接到 ZTD 云服务后，部署过程将自动执行以下操作：

      - 下载 SD-WAN Center 之前存储的配置文件
      - 将配置应用于本地设备
      - 下载并安装临时 10 MB 许可证文件
      - 下载并安装任何软件更新（如有需要）
      - 激活 SD-WAN 服务

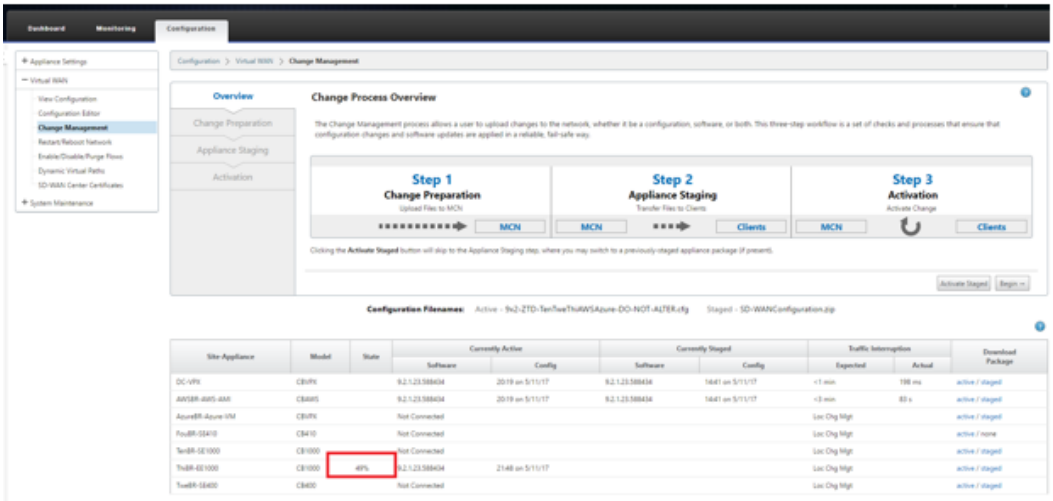
d) 进一步确认可以在 SD-WAN Center Web 管理界面中完成，在激活历史记录选项卡中，“零点触摸部署”菜单显示成功激活的设备。



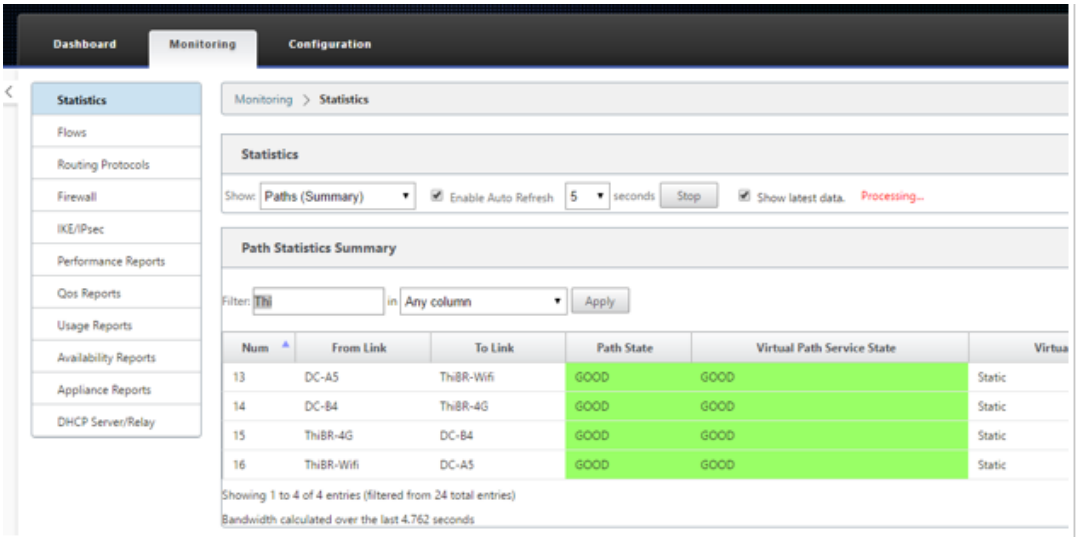
e) 虚拟路径可能不会立即以已连接的状态显示，因为 MCN 可能不信任从 ZTD 云服务中向下传递的配置，并在 MCN 控制板中报告“配置版本不匹配”。



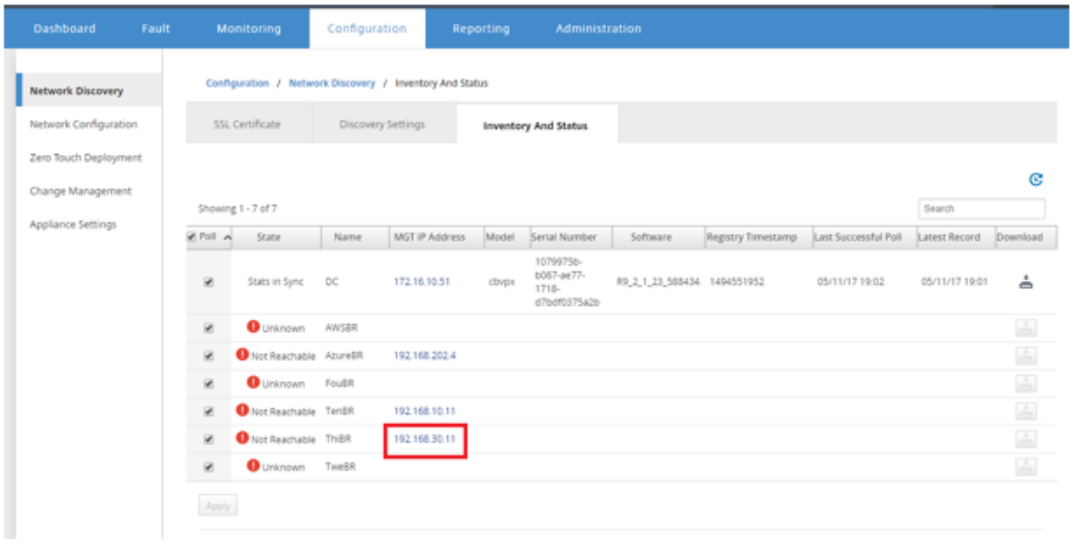
f) 该配置将重新传输到新安装的分支机构设备，并且状态将在 **MCN** > 配置 > 虚拟 **WAN** > 更改管理页面上进行监视（此过程可能需要几分钟时间才能完成）。



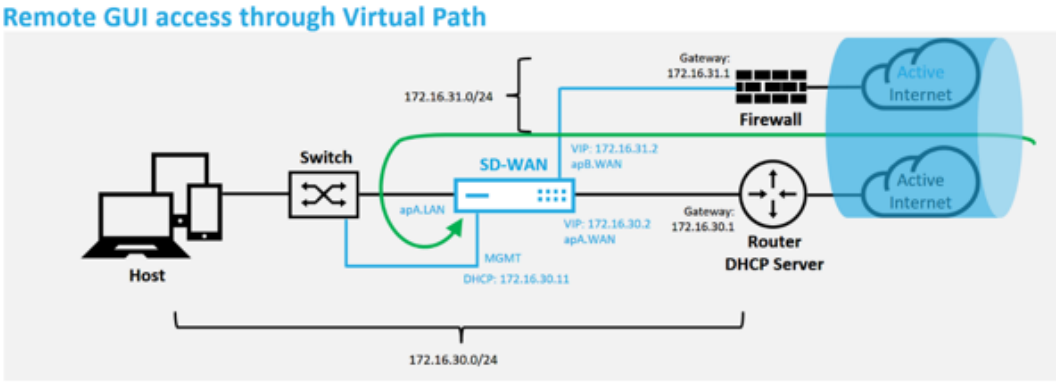
g) SD-WAN 管理员可以监视面向已建立的远程站点虚拟路径的头端 MCN Web 管理页面。



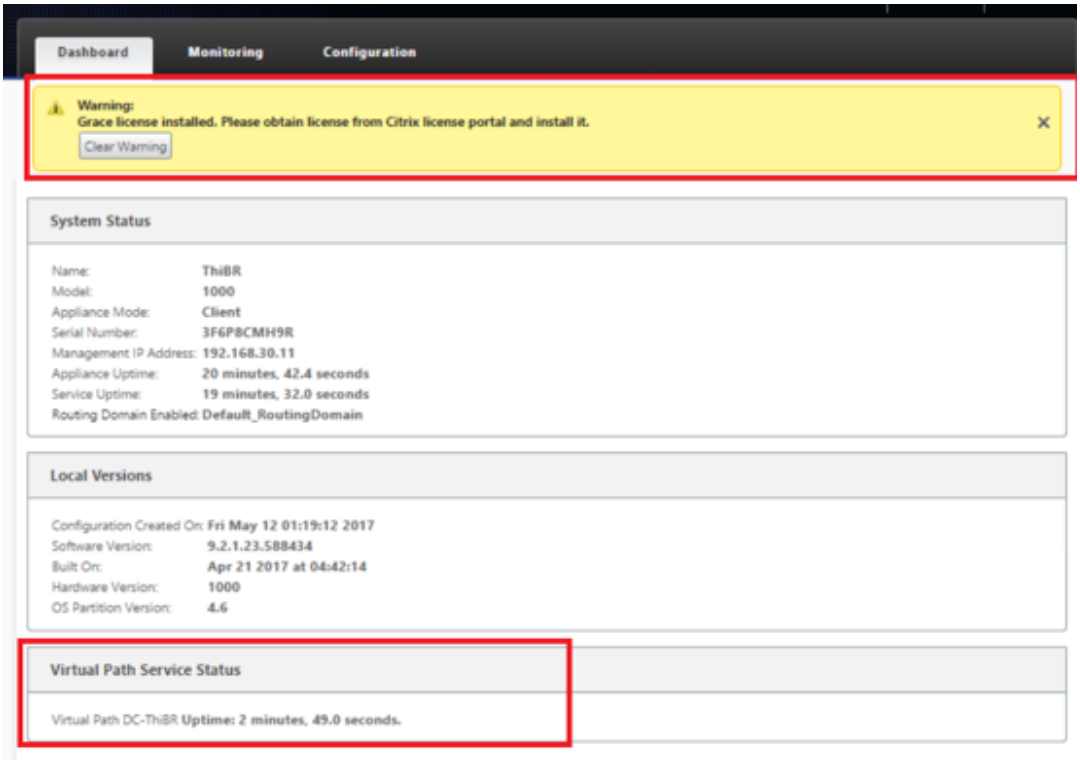
h) SD-WAN Center 还可用于从配置 > 网络发现 > 清单和状态页面识别现场设备的 DHCP 分配 IP 地址。



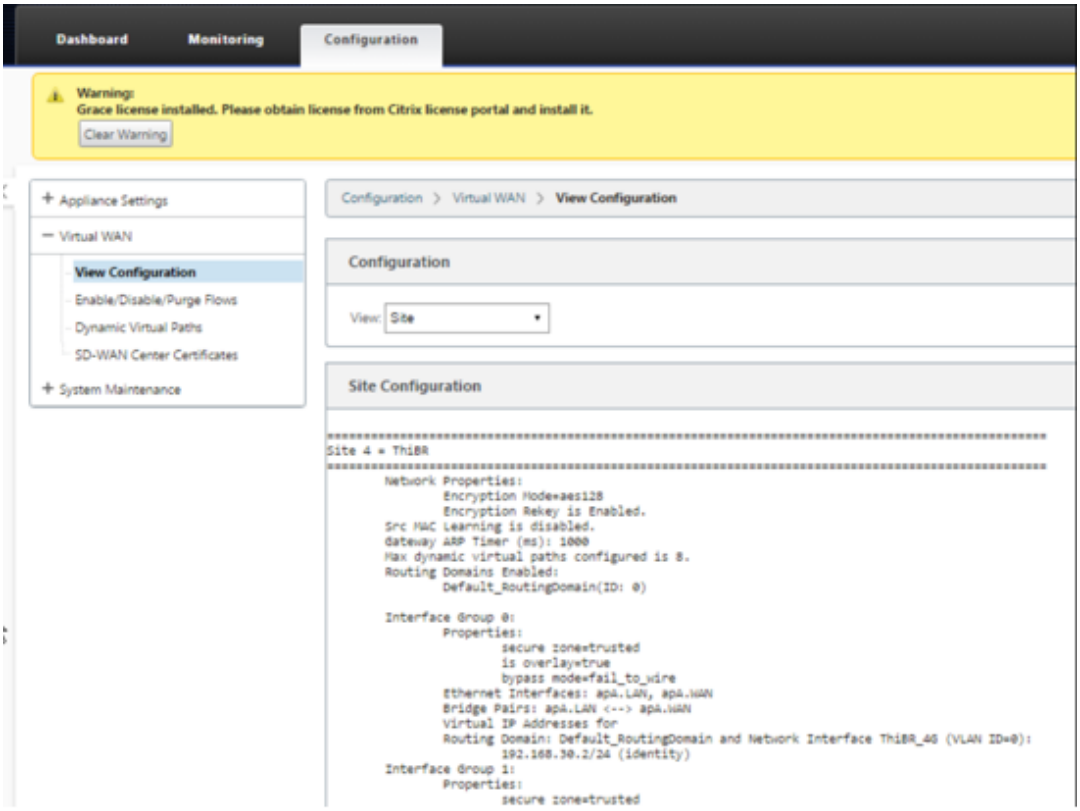
i) 此时，SD-WAN 网络管理员可以通过使用 SD-WAN 覆盖网络对现场设备进行 Web 管理访问。



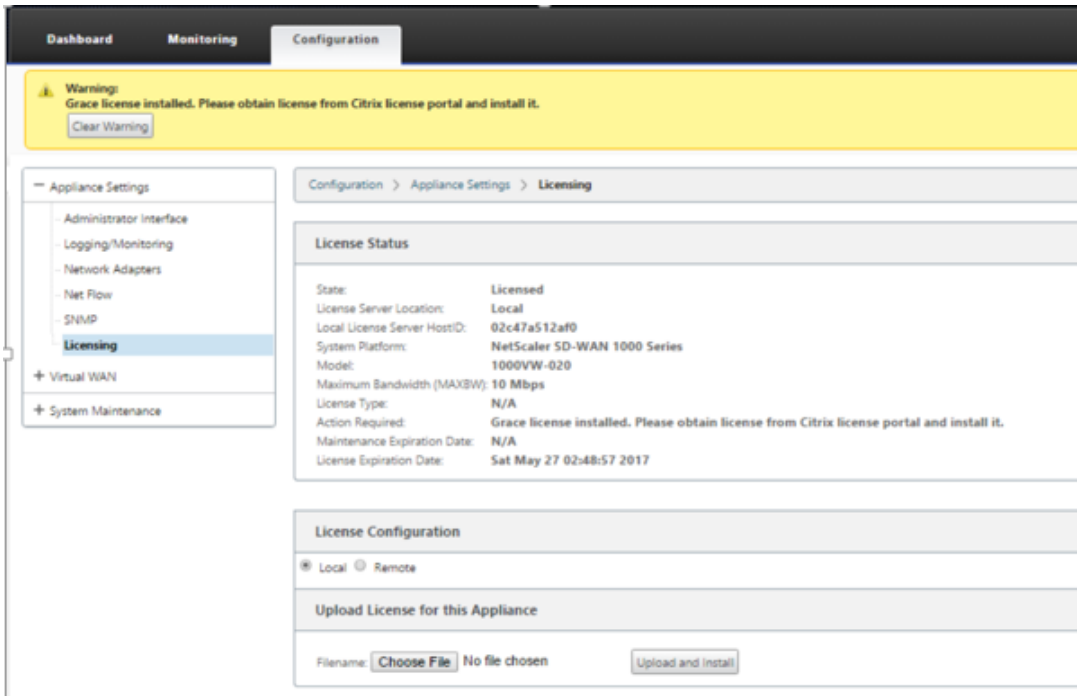
j) 对远程站点设备进行 Web 管理访问指示已使用临时宽限期 10 Mbps 来安装设备，这样可使虚拟路径服务状态报告为活动状态。



k) 可以使用配置 > 虚拟 **WAN**> 查看配置页面对设备配置进行验证。



l) 可以使用配置 > 设备设置 > 许可页面将设备许可证文件更新为永久许可证。



m) 上载并安装永久许可证文件后，宽限期许可证警告横幅会消失，并且在安装许可证过程中不会出现与远程站点的连接断开的情况（丢弃零个 ping）。

本地零接触

April 13, 2021

有关如何部署 SD-WAN 设备和零接触服务的说明，请参阅主题 如何配置零接触部署服务。

AWS

April 13, 2021

在 **AWS** 中部署

使用 SD-WAN 版本 9.3 时，零接触部署功能已扩展到云实例。部署零接触部署过程的过程中，四个云实例与设备部署的使用情况稍有不同，以实现零接触服务。

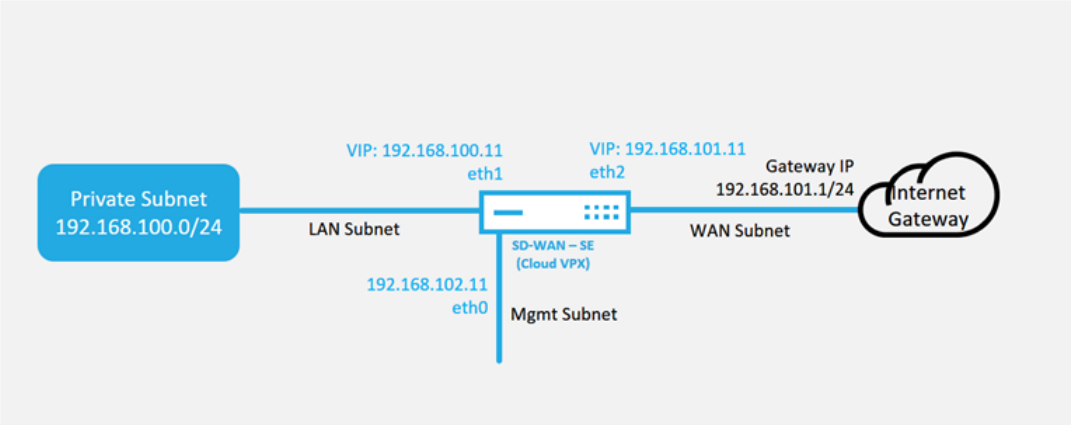
1. 通过使用 SD-WAN Center 网络配置，更新配置以添加具有 ZTD 功能的 SD-WAN 设备的新远程站点。

   如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。应使用以下过程添加针对零接触部署的新云节点。

   a) 通过首先列出新站点的详细信息（例如，VPX 大小、接口组使用情况、虚拟 IP 地址、WAN 链接以及带宽及其各自的网关），为 SD-WAN 部署设计新站点。

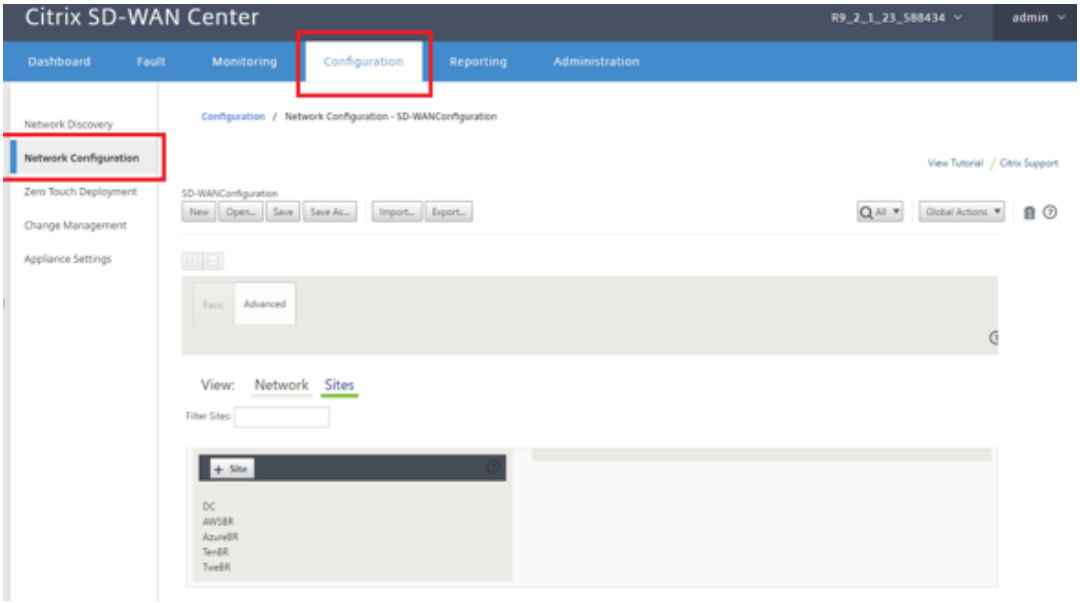
   > 注意
   >
   > - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
   > - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
   > - SD-WAN VPX 的可用云模板当前被硬设置为获取 VPC 中可用子网的 #.#.#.#.11 IP 地址。

   Cloud Topology with NetScaler SD-WAN

   这是已部署 SD-WAN 云的站点的部署示例，Citrix SD-WAN 设备部署为在此云网络中提供单一 Internet WAN 链接的边缘设备。远程站点将能够利用连接到此云中相同 Internet 网关的多个不同的 Internet WAN 链接，从而提供从任何 SD-WAN 部署站点到云基础结构的恢复能力和聚合带宽连接。这提供了经济高效且高度可靠的云连接。

   b) 打开 SD-WAN Center Web 管理接口，并导航到配置 > 网络配置页面。

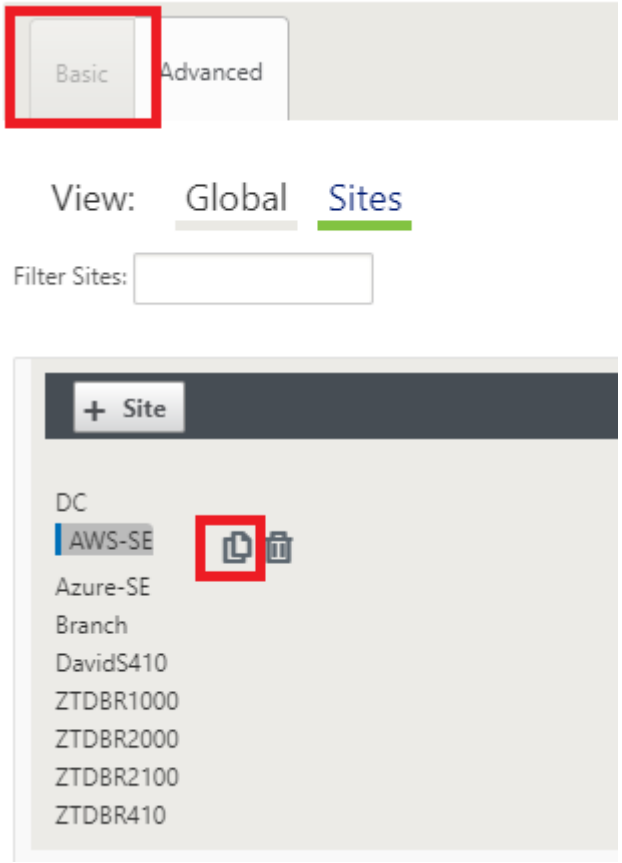


c) 确保已准备好正在运行的配置，或从 MCN 导入配置。

d) 导航到 基本 选项卡以创建新站点。

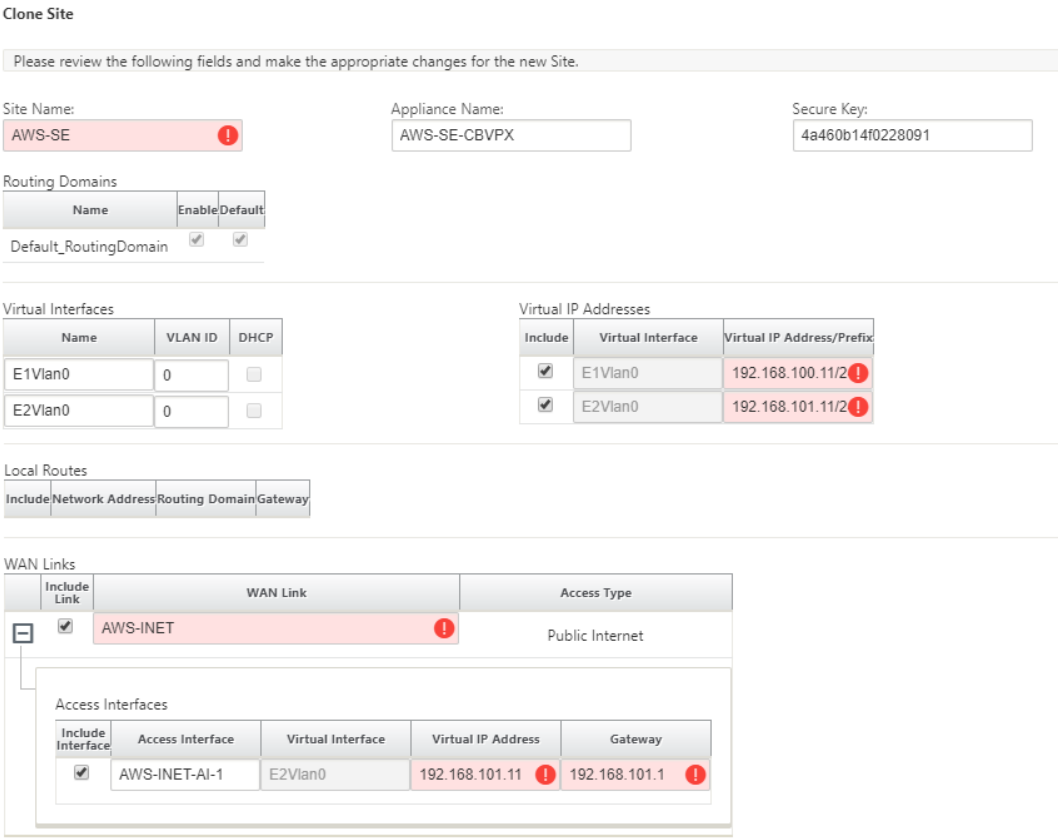
e) 打开 站点 磁贴以显示当前配置的站点。

f) 通过使用任何现有站点的克隆功能，或者手动构建新站点来快速构建新云站点的配置。

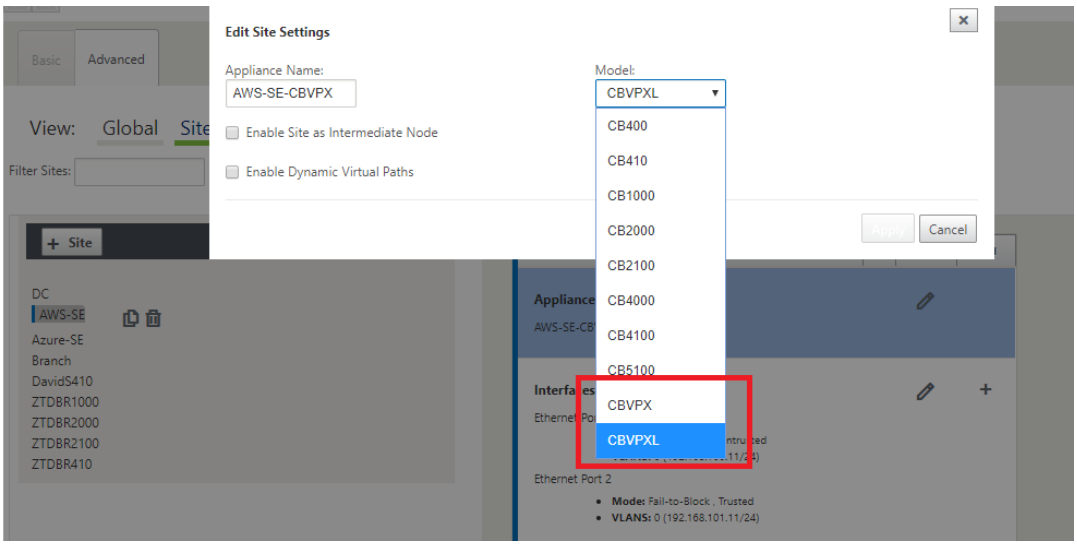


g) 填充之前为此新云站点设计的拓扑中的所有必填字段

请注意，可以将云 ZTD 部署的模板硬设置为对管理、LAN 和 WAN 子网使用 #.#.#.11 IP 地址。如果未将配置设置为与每个接口的预期.11 IP 主机地址相匹配，则该设备将无法正确地为云环境网关与 MCN 的虚拟路径建立 ARP 连接。

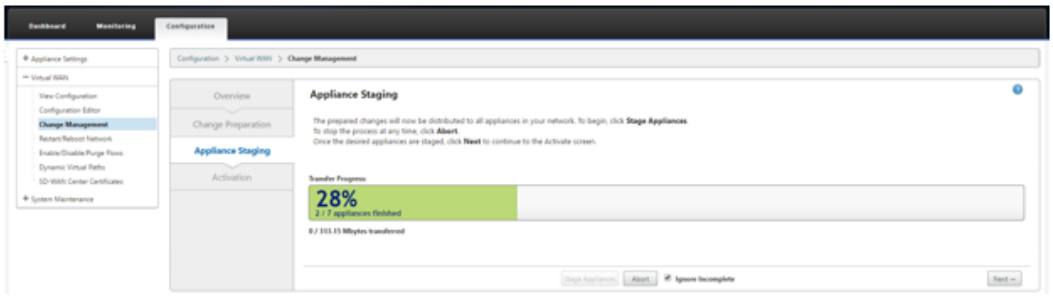


h) 克隆新站点后，导航到该站点的基本设置，并验证是否正确选择了要支持零接触服务的 SD-WAN 的型号。



i) 在 SD-WAN Center 上保存新配置，并使用导出到更改管理收件箱选项，以使用更改管理推送配置。

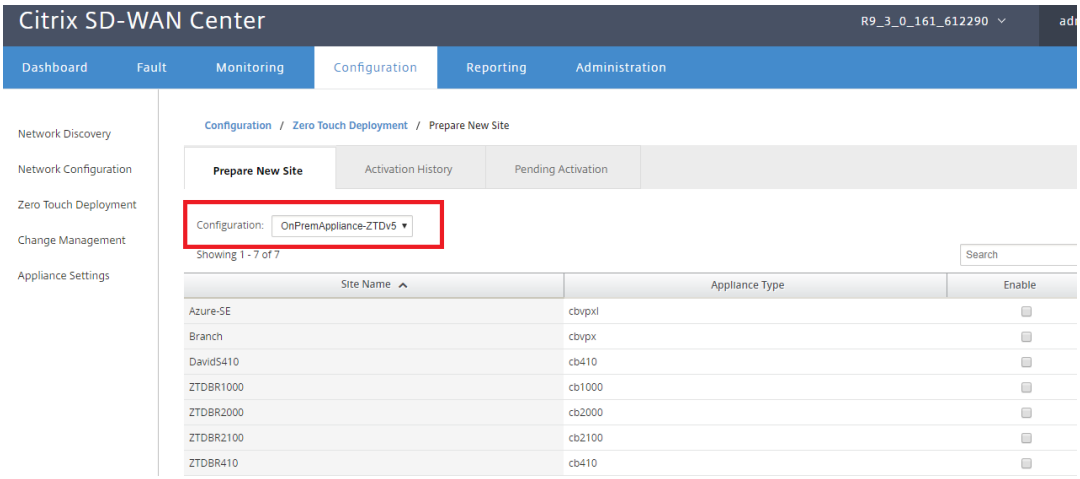
j) 按照更改管理过程来正确转移新配置，这样会导致现有 SD-WAN 设备知晓要通过零接触部署的新站点，您需要使用忽略不完整选项跳过尝试推送仍需要通过 ZTD 工作流的新站点配置。



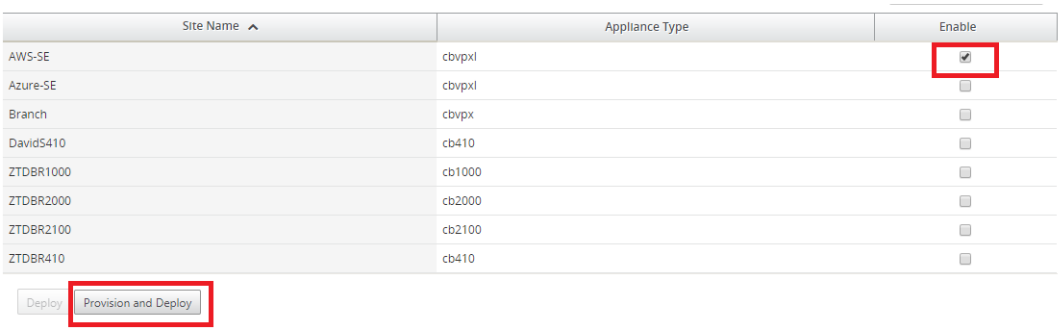
2. 导航回 SD-WAN Center 零接触部署页面，在运行新的活动配置的情况下，将有新站点可供部署。

a) 在零接触部署页面的部署新站点选项卡下，选择正在运行的网络配置文件。

b) 选择正在运行的配置文件后，将显示具有未部署的 Citrix SD-WAN 设备（支持零个触摸）的所有分支站点的列表。

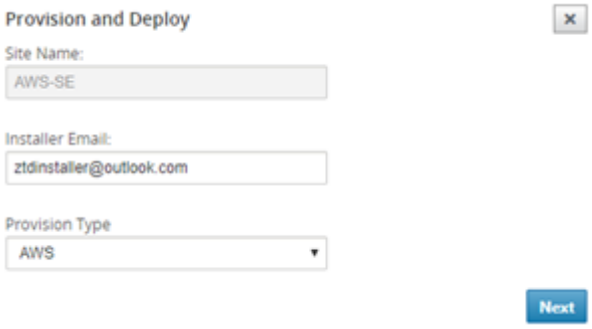


c) 选择要使用零接触服务部署的目标云站点，单击启用，然后单击 预配和部署。

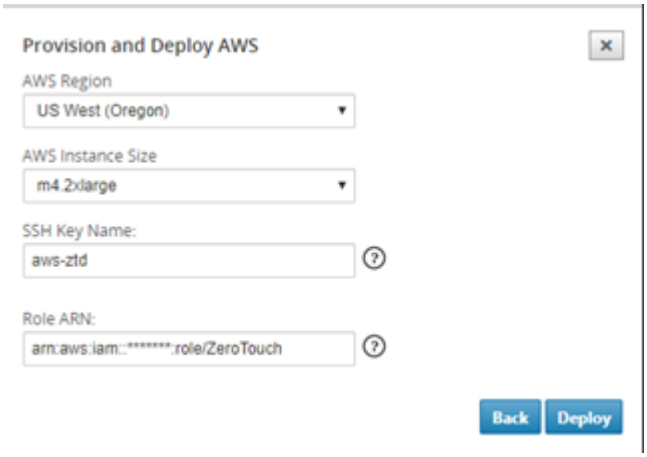


d) 此时将显示一个弹出窗口，其中 Citrix SD-WAN 管理员可以在零接触的情况下发起部署。

填写可以交付激活 URL 的电子邮件地址，然后选择所需云的提供类型。



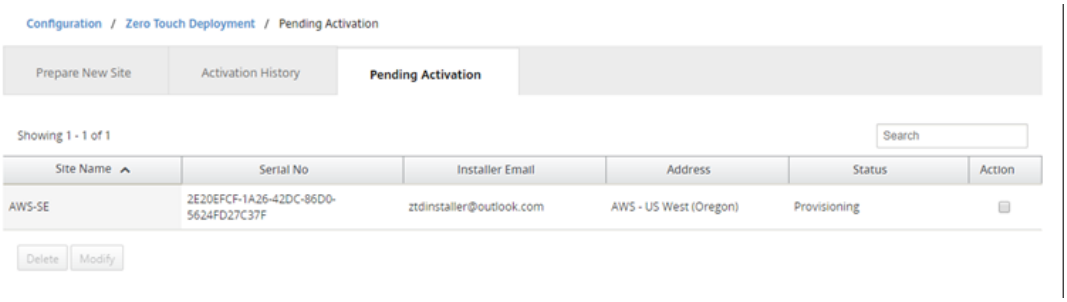
e) 单击下一步后，选择适当的区域（实例大小），相应地填充 SSH 密钥名称和角色 ARN 字段。



> 注意
>
> 请使用帮助链接获取有关如何在云帐户上设置 SSH 密钥和角色 ARN 的指导。此外，请确保所选区域与账户上的可用区域匹配，并且选定的实例大小与 SD-WAN 配置中选定型号的 VPX 或 VPXL 匹配。

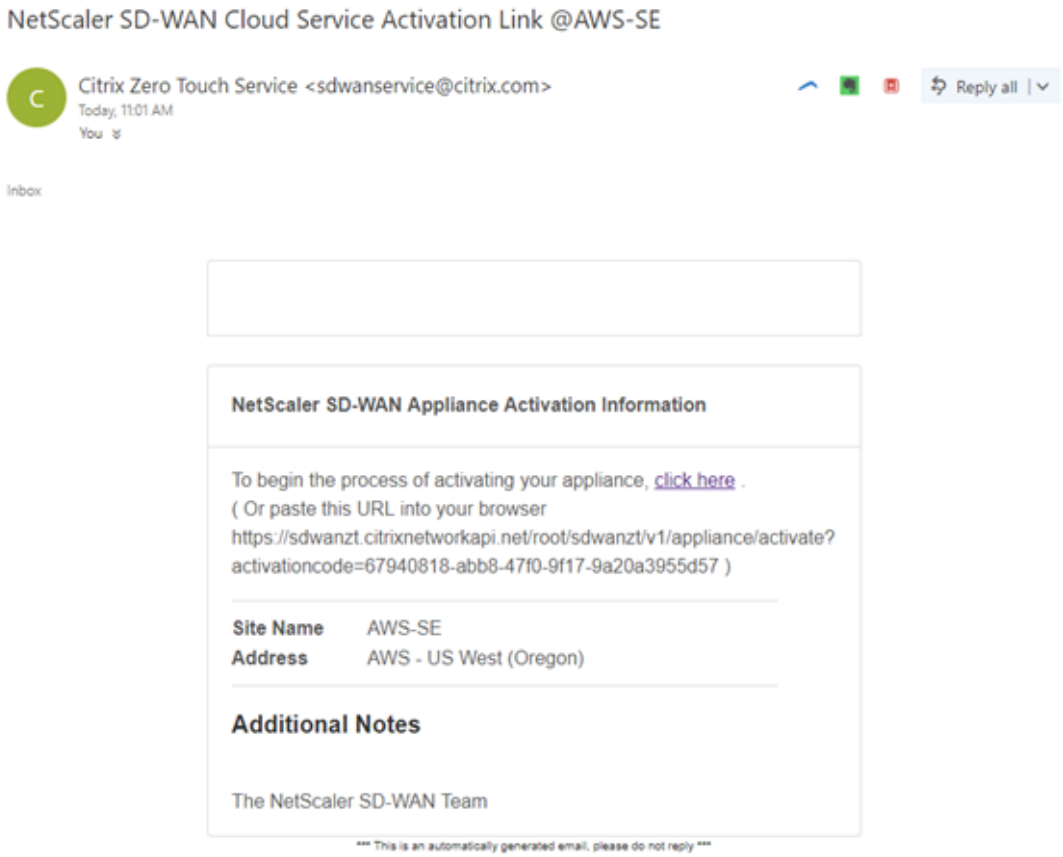
f) 单击部署，触发 SD-WAN Center（以前在 ZTD 云服务中注册），以将此站点的配置临时存储在 ZTD 云服务中。

g) 导航到挂起的激活选项卡，确认站点信息已成功填充并置于预配状态。



3. 以云管理员身份启动零接触部署过程。

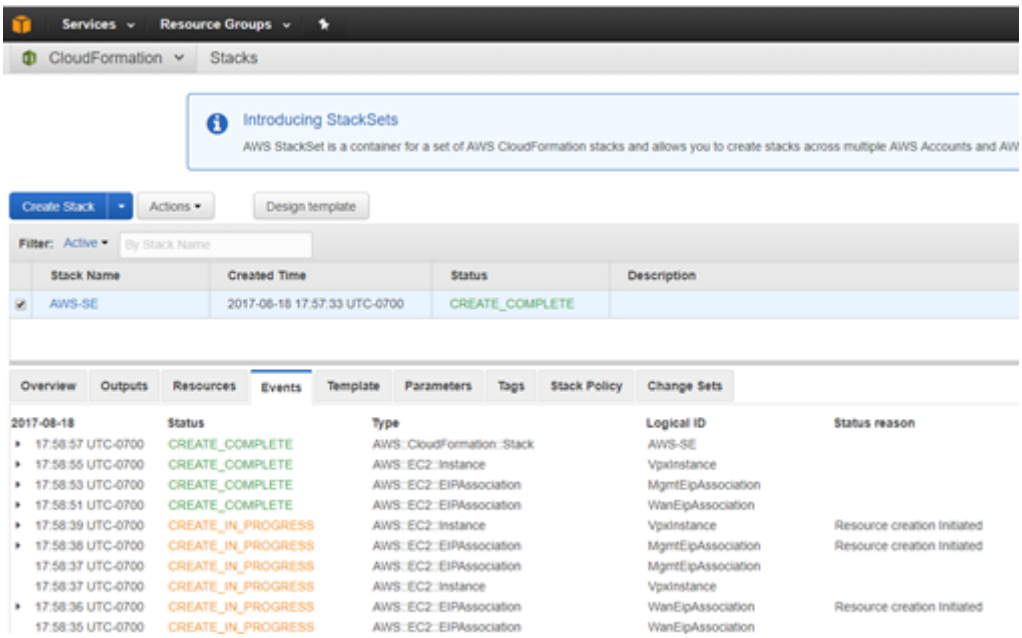
a) 安装程序将需要检查在部署站点时使用 SD-WAN 管理员的电子邮件地址的邮箱。



b) 在 Internet 浏览器窗口中打开在电子邮件中找到的激活 URL。

c) 如果正确输入了 SSH 密钥和角色 ARN，则“零接触部署”服务将立即开始预配 SD-WAN 实例，否则连接错误将立即显示出来。

d) 要在 AWS 控制台上执行其他故障排除，可以使用云组建服务来捕捉预配过程中发生的任何事件。

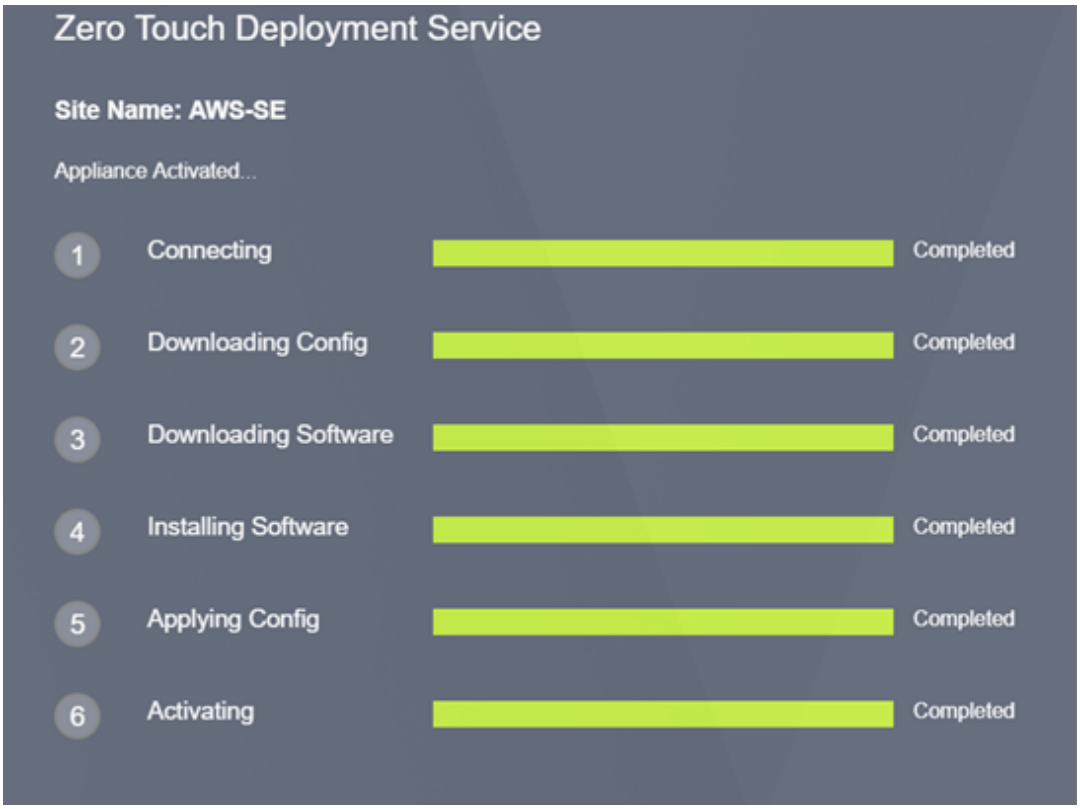


e) 允许预配过程 ~ 8-10 分钟，并在激活后约需要 3-5 分钟来完成。

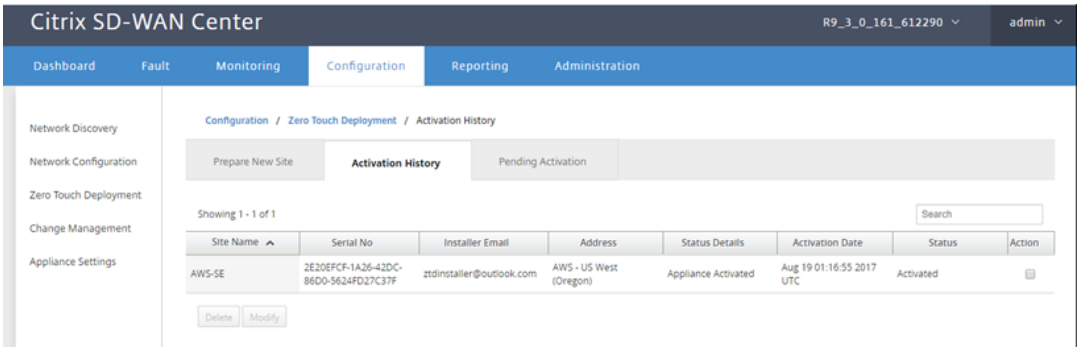
f) 通过将 SD-WAN 实例成功连接到 ZTD 云服务，该服务将自动执行以下操作：

- 下载 SD-WAN Center 之前存储的特定于站点的配置文件
- 将配置应用于本地实例
- 下载并安装临时 10 MB 许可证文件

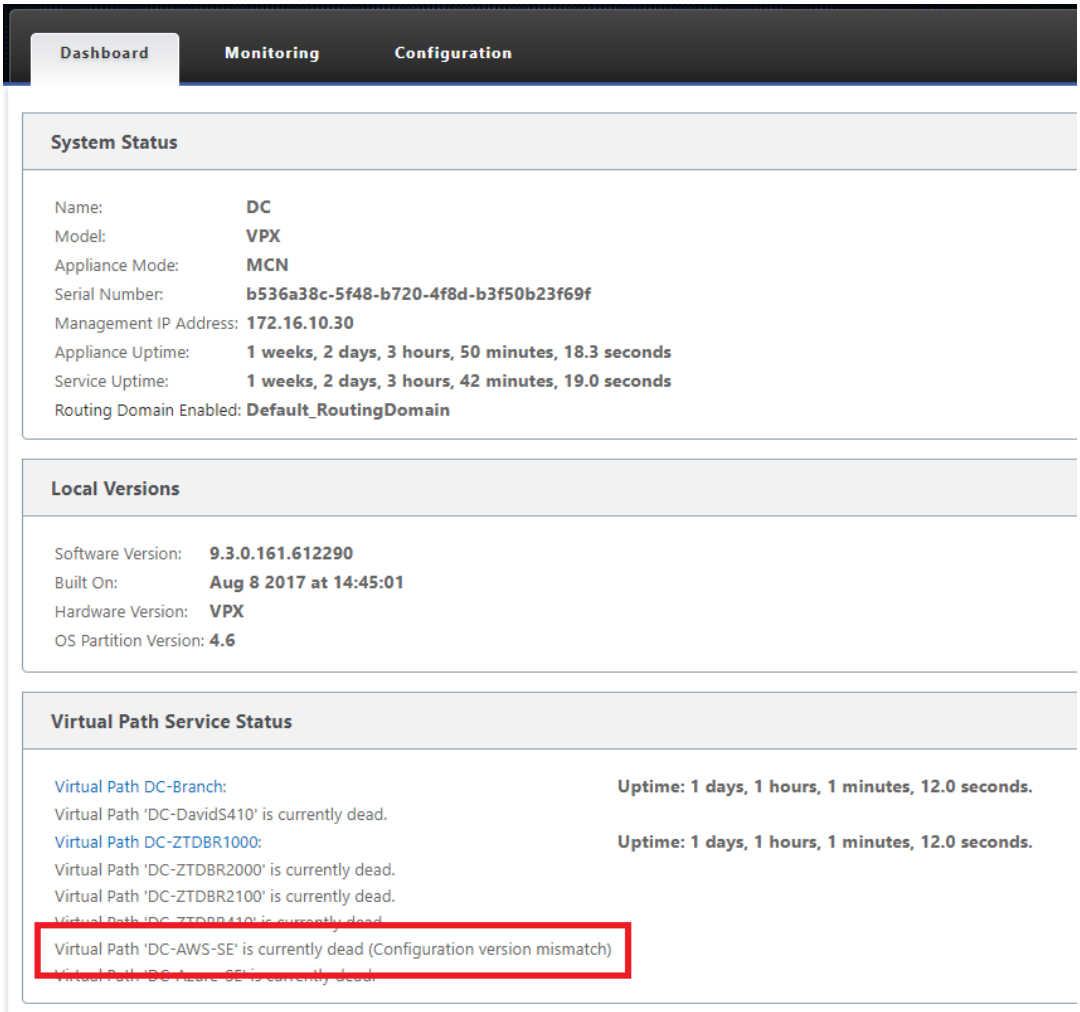
- 下载并安装任何软件更新（如有需要）
- 激活 SD-WAN 服务



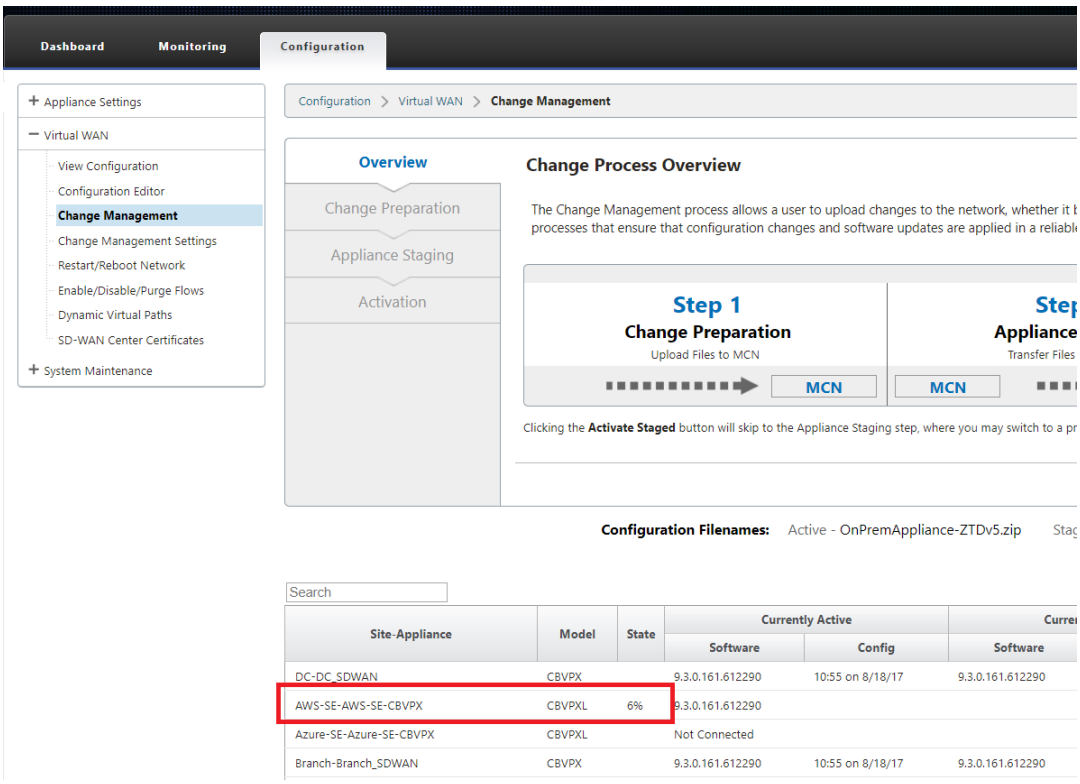
g) 可以在 SD-WAN Center Web 管理接口中执行进一步确认。零接触部署菜单将在激活历史记录选项卡中显示成功激活的设备。



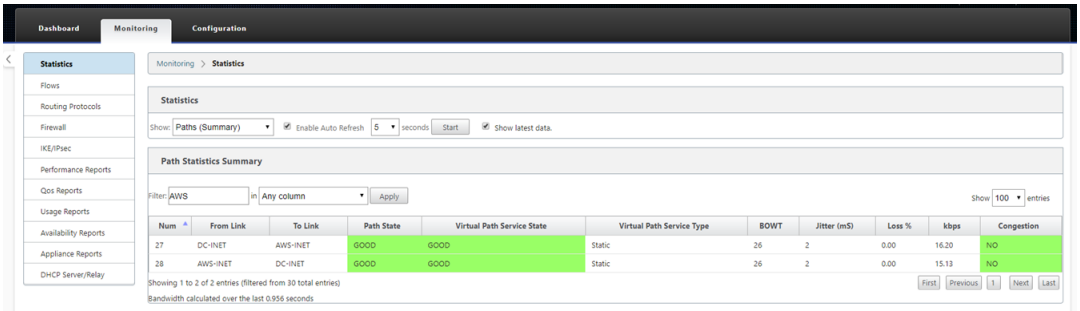
h) 虚拟路径可能不会立即以已连接状态显示，这是因为 MCN 可能不信任从 ZTD 云服务中向下传递的配置，并且将在 MCN 控制板中报告配置版本不匹配。



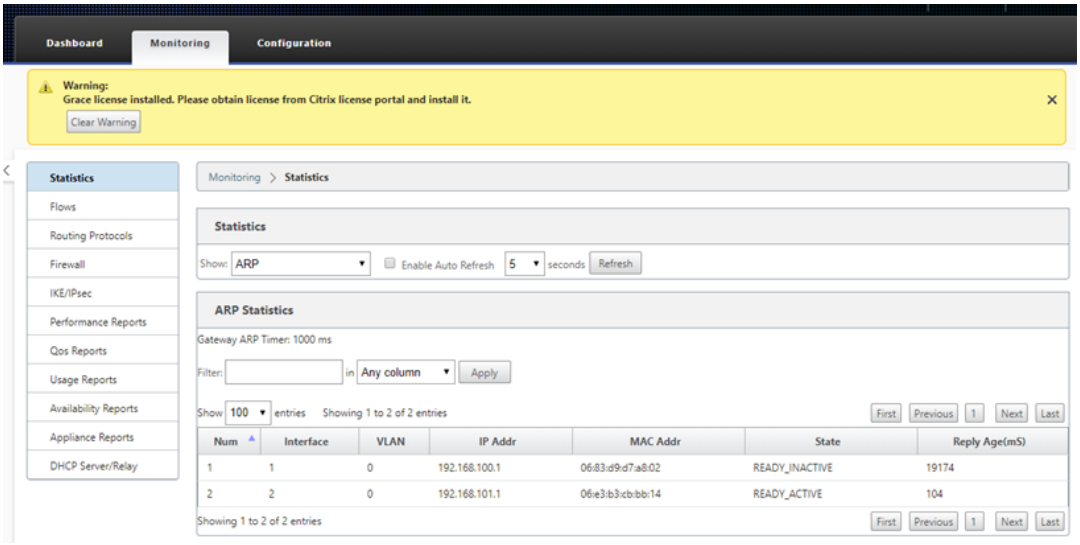
i) 此配置将自动重新传输到新安装的分支机构设备，这种状态可以在 **MCN** > 配置 > 虚拟 **WAN**> 更改管理页面上进行监视（具体取决于连接性，此过程可能需要几分钟时间才能完成）。



j) SD-WAN 管理员可以监视与新添加的云站点建立的虚拟路径有关的头端 MCN Web 管理页面。



k) 如果需要进行故障排除，请使用预配过程中云环境所分配的公用 IP 打开 SD-WAN 实例用户界面，并利用监视 > 统计信息页面中的 ARP 表来确定连接时遇到的任何问题到预期网关，或使用诊断中的跟踪路由和数据包捕获选项。



Azure

April 13, 2021

使用 SD-WAN 版本 9.3 时，零接触部署功能已扩展到云实例。部署面向云实例的零接触部署过程的过程与设备部署中的过程稍有不同，以实现零接触服务。

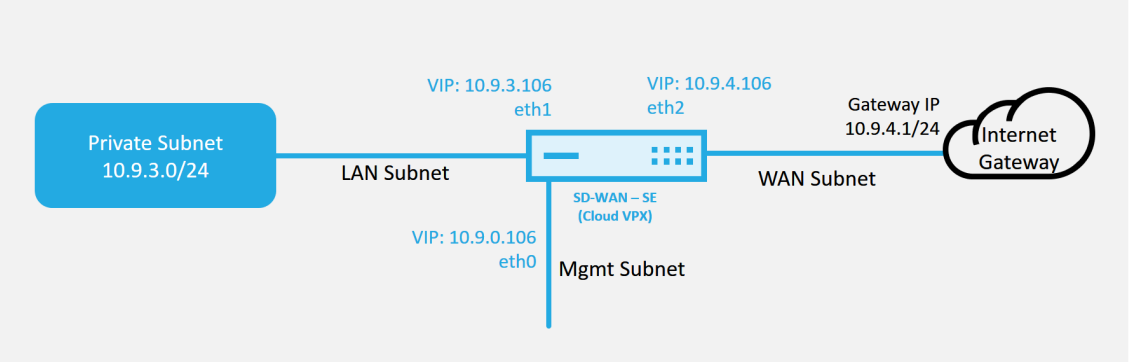
使用 **SD-WAN Center** 网络配置更新配置以添加具有 **ZTD** 功能的 **SD-WAN** 设备的新远程站点

如果 SD-WAN 配置不是使用 SD-WAN Center 网络配置构建的，则从 MCN 导入活动配置，然后开始使用 SD-WAN Center 修改配置。为实现零接触部署功能，SD-WAN 管理员必须使用 SD-WAN Center 构建配置。应使用以下过程添加针对零接触部署的新云节点。

1. 通过首先列出新站点的详细信息（例如，VPX 大小、接口组使用情况、虚拟 IP 地址、WAN 链接以及带宽及其各自的网关），为 SD-WAN 部署设计新站点。

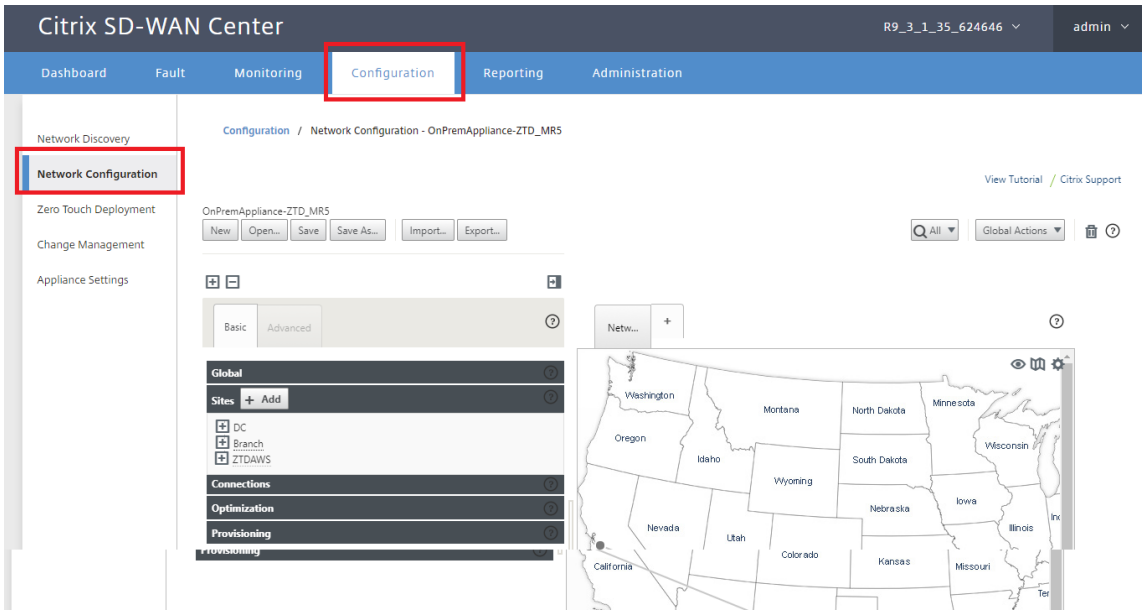
> 注意
>
> - 必须在边缘/网关模式下部署云部署 SD-WAN 实例。
> - 云实例的模板限制为三个接口：管理、LAN 和 WAN（以此顺序排列）。
> - 适用于 SD-WAN VPX 的 Azure 云模板当前被硬设置为获取 WAN 的 10.9.4.106 IP、适用于 LAN 的 10.9.3.106 IP 以及管理地址的 10.9.0.16 IP。面向零接触的 Azure 节点的 SD-WAN 配置必须与此布局匹配。
> - 配置中的 Azure 站点名称必须全小写且无特殊字符（例如 ztdazure）。

Azure Cloud Topology with NetScaler SD-WAN

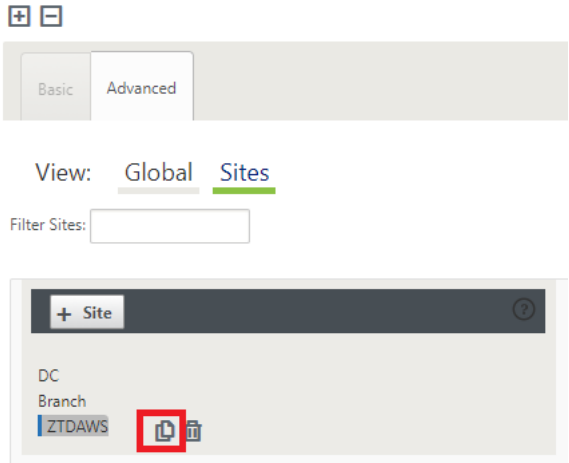


这是已部署 SD-WAN 云的站点的部署示例，Citrix SD-WAN 设备部署为在此云网络中提供单一 Internet WAN 链接的边缘设备。远程站点将能够利用连接到此云中相同 Internet 网关的多个不同的 Internet WAN 链接，从而提供从任何 SD-WAN 部署站点到云基础结构的恢复能力和聚合带宽连接。这提供了经济高效且高度可靠的云连接。

2. 打开 SD-WAN Center Web 管理接口，并导航到配置 > 网络配置页面。



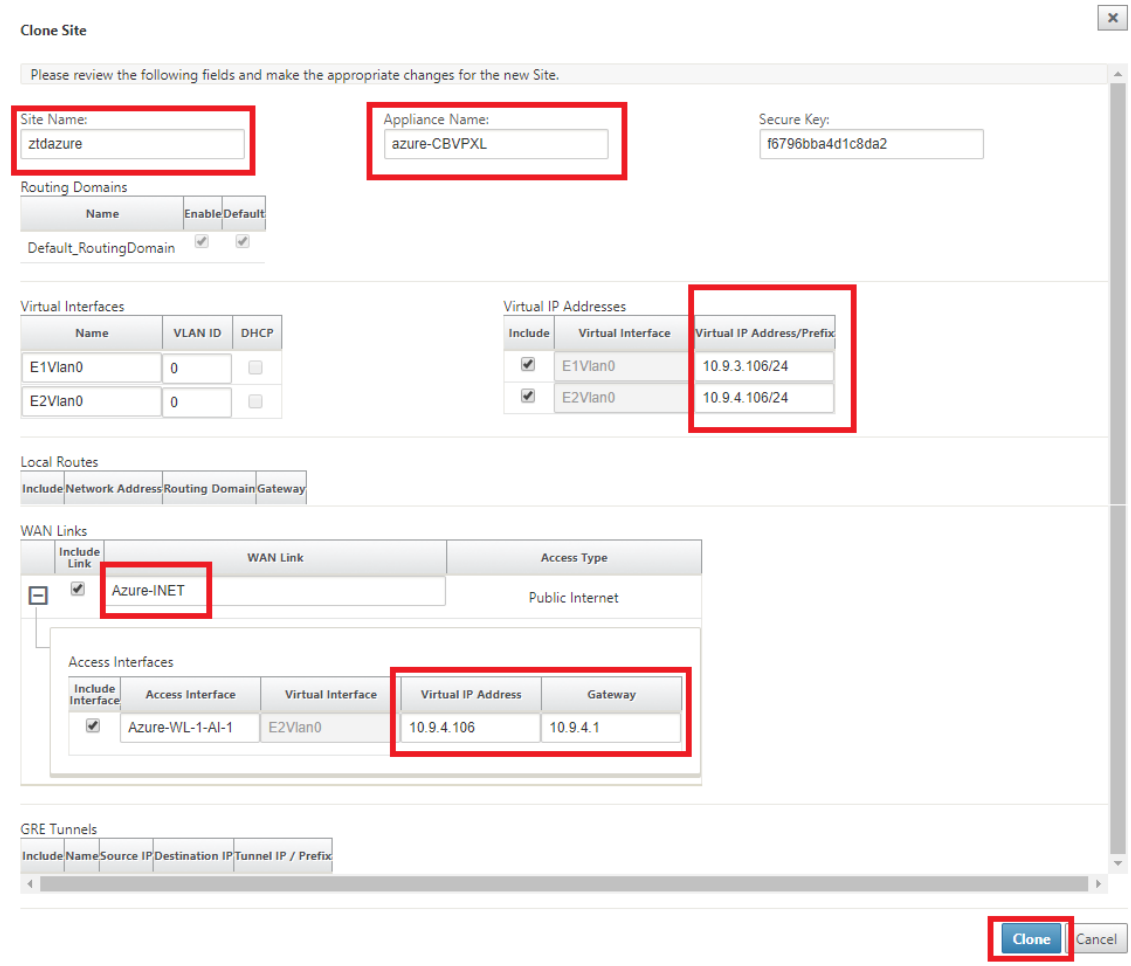
3. 确保已准备好正在运行的配置，或从 MCN 导入配置。
4. 导航到 基本 选项卡以创建新站点。
5. 打开 站点 磁贴以显示当前配置的站点。
6. 通过使用任何现有站点的克隆功能，或者手动构建新站点来快速构建新云站点的配置。



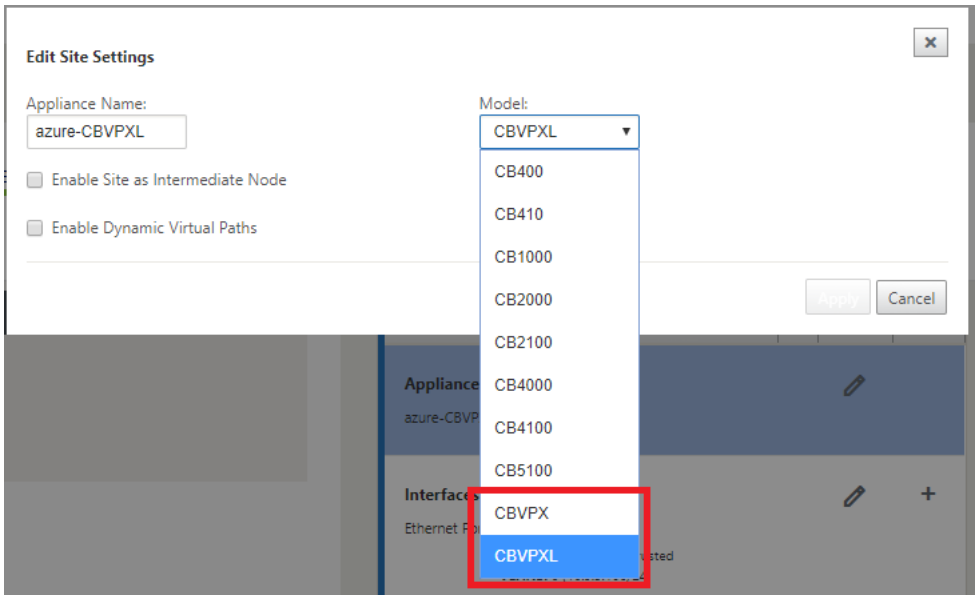
7. 填充之前为此新云站点设计的拓扑中的所有必填字段。

   请注意，适用于 Azure cloud ZTD 部署的模板当前被硬设置为获取 WAN 的 10.9.4.106 IP、适用于 LAN 的 10.9.3.106 IP 以及管理地址的 10.9.0.16 IP。如果未将配置设置为与每个接口的预期 VIP 地址相匹配，则该设备将无法正确地建立到云环境网关的 ARP 以及与 MCN 的虚拟路径的 IP 连接。

   将导入站点名称，使其符合 Azure 预期的要求。网站名称必须全部小写，至少 6 个字符，没有特殊字符，必须确认以下正则表达式 **^ [a-z] [a-z0-9-] {1,61} [a-z0-9] $**。

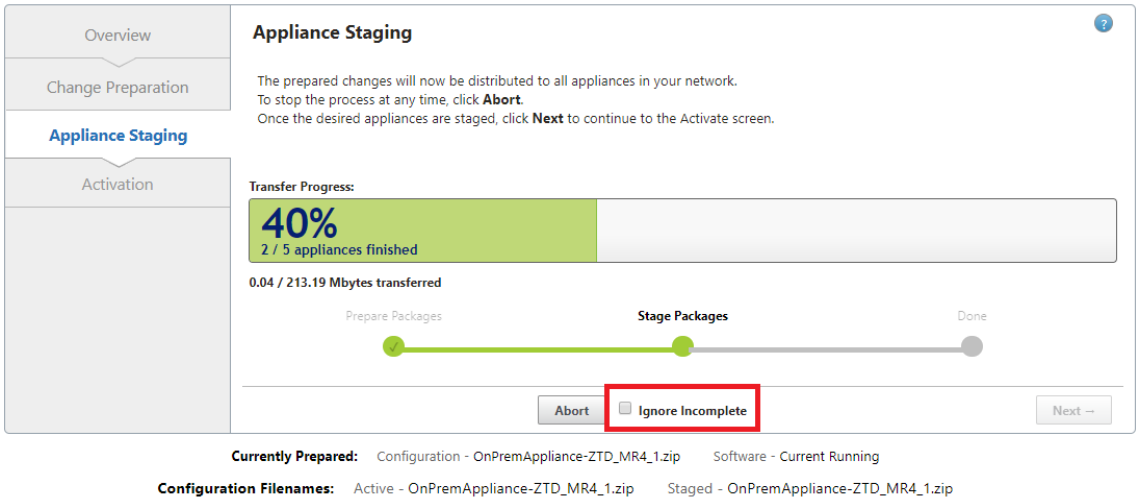


8. 克隆新站点后，导航到该站点的基本设置，并验证是否正确选择了要支持零接触服务的 SD-WAN 的型号。



9. 在 SD-WAN Center 上保存新配置，并使用导出到更改管理收件箱选项，以使用更改管理推送配置。

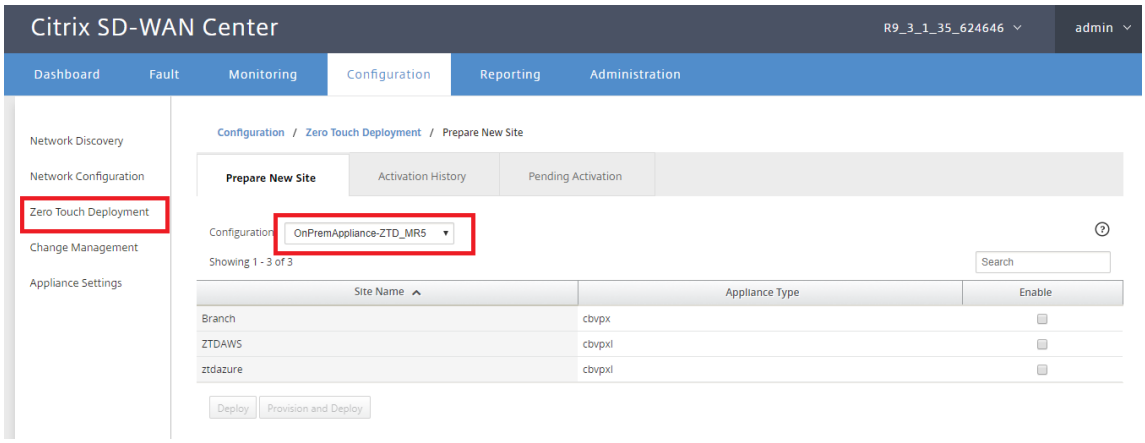
10. 按照更改管理过程来正确转移新配置，这样会导致现有 SD-WAN 设备知晓要通过零接触部署的新站点，您需要使用忽略不完整选项跳过尝试推送仍需要通过 ZTD 工作流的新站点配置。



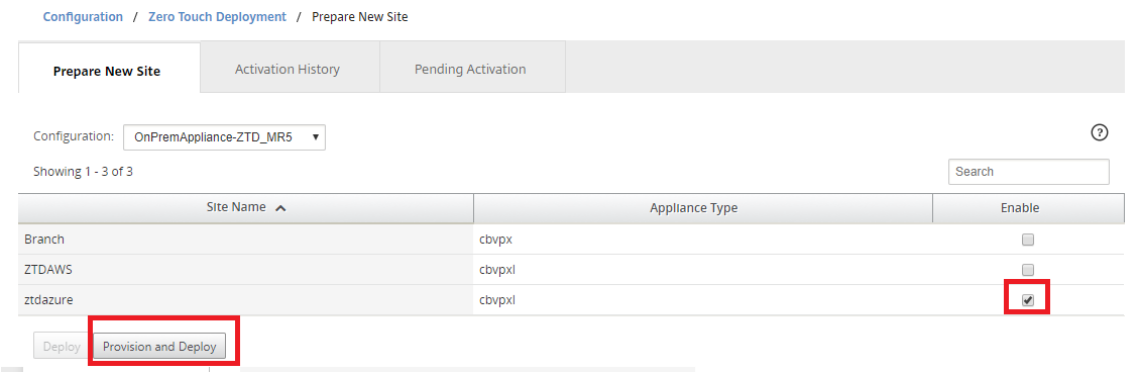
导航到 **SD-WAN Center** 的零接触部署页面，在运行新的活动配置的情况下，新站点将适用于 **SD-WAN Center** 预配和部署 **Azure**（第 **1** 步，共 **2** 步）

1. 在零轻点部署页面上，使用您的 Citrix 帐户凭据进行登录。在部署新站点选项卡下，选择正在运行的网络配置文件。

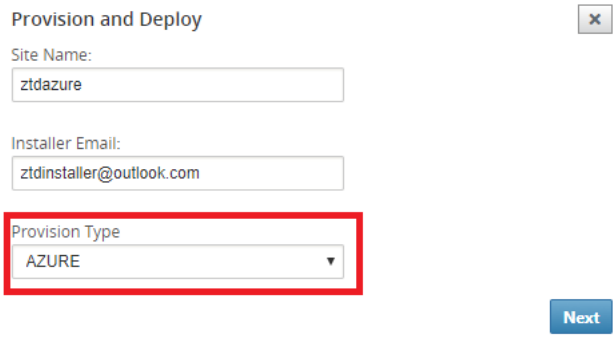
2. 选择正在运行的配置文件后，将显示具有 ZTD 功能的 Citrix SD-WAN 设备的所有分支站点的列表。



3. 选择要使用零接触服务部署的目标云站点，单击启用，然后单击 预配和部署。

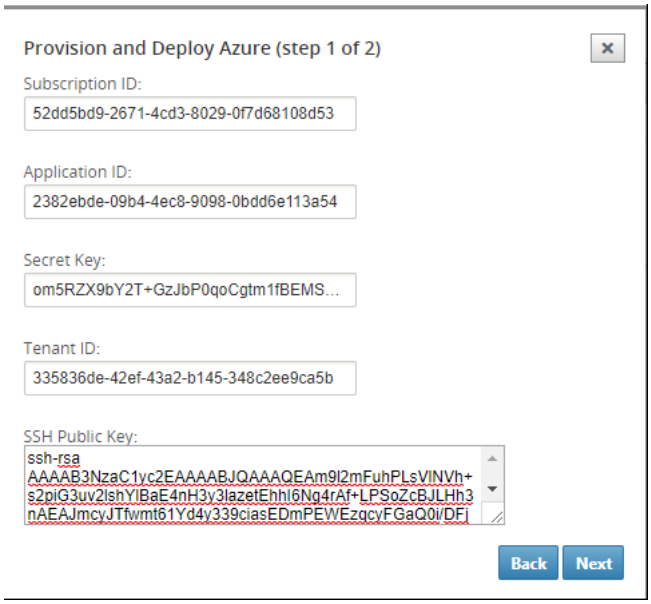


4. 此时将显示一个弹出窗口，其中 Citrix SD-WAN 管理员可以在零接触的情况下发起部署。验证站点名称是否符合 Azure 上的要求（小写，没有特殊字符）。填充可以传送激活 URL 的电子邮件地址，然后选择 Azure 作 为所需云的预配类型，然后单击 下一步。

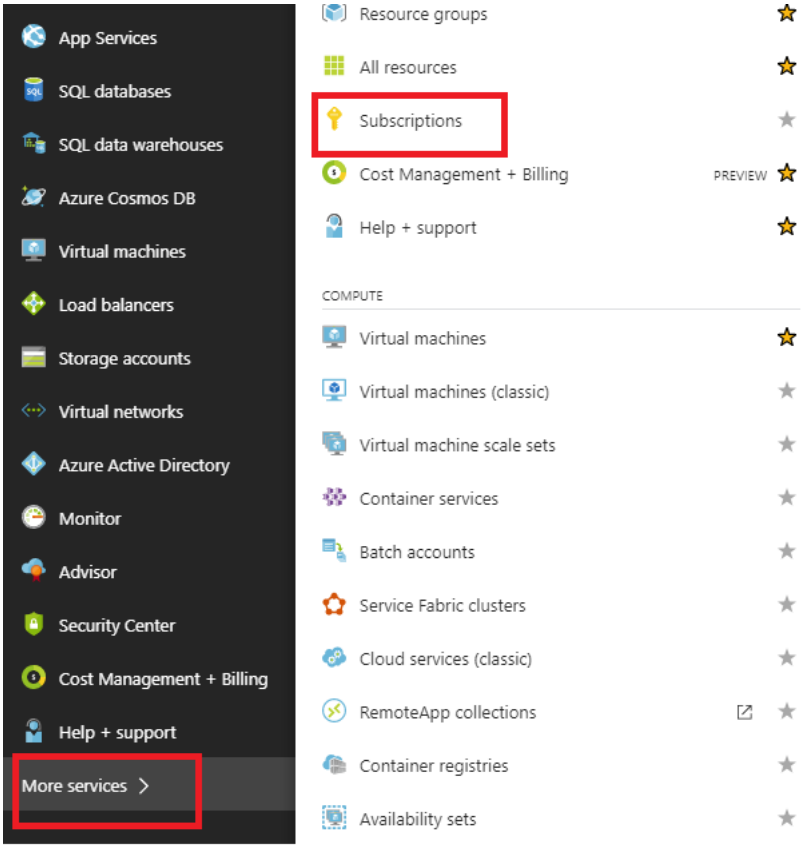


5. 单击下一步后，预配和部署 Azure（第 1 步，共 2 步）窗口将需要输入从 Azure 帐户获取的内容。

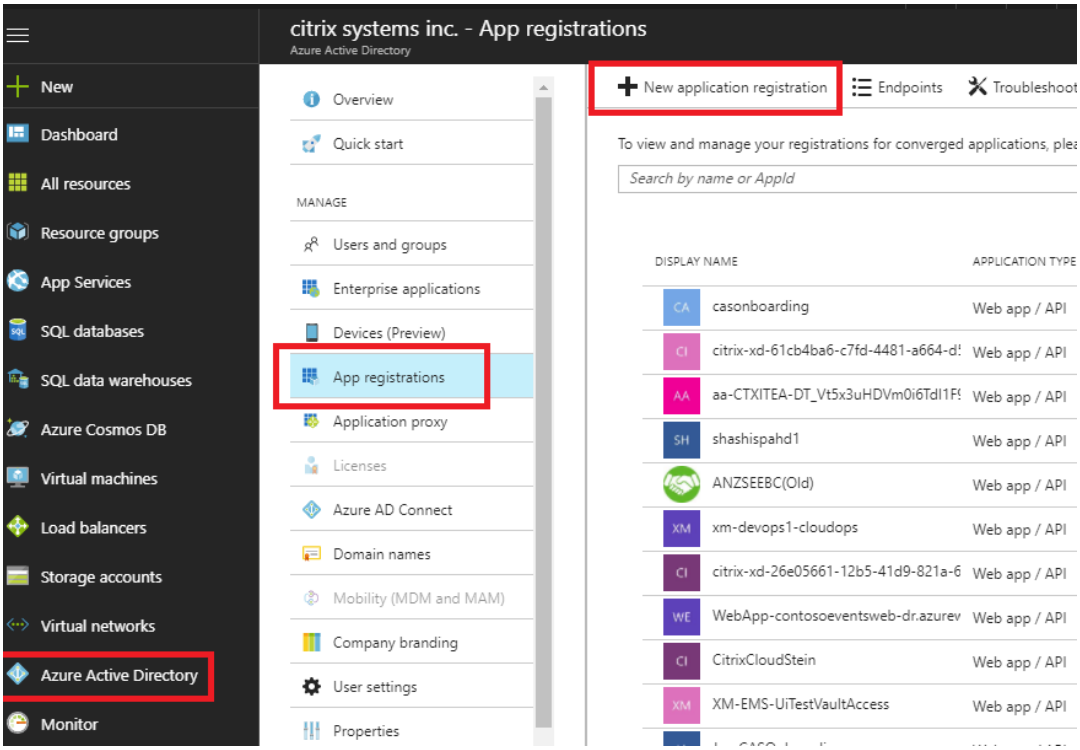
   从您的 Azure 帐户获取信息后，复制并粘贴每个必填字段。以下步骤概述了如何从 Azure 帐户获取所需的订阅 ID、应用程序 ID、密钥和租户 ID，然后单击 下一步继续。



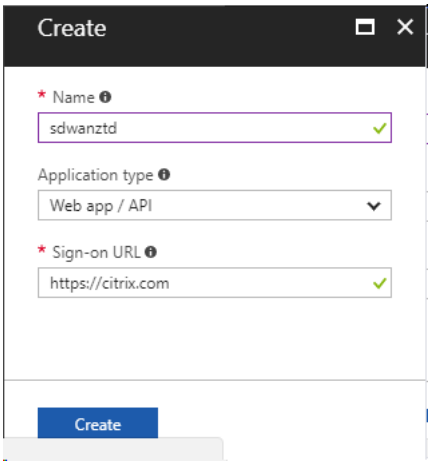
   a) 在 Azure 帐户上，我们可以通过导航到“更多服务”并选择订阅来识别所需的订阅 ***ID***。



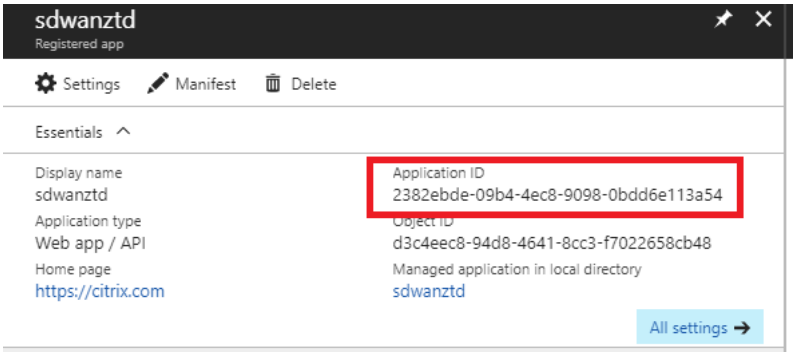
b) 要确定所需的应用程序 ***ID***，请导航到 Azure Active Directory、应用程序注册，然后单击新应用程序注册。



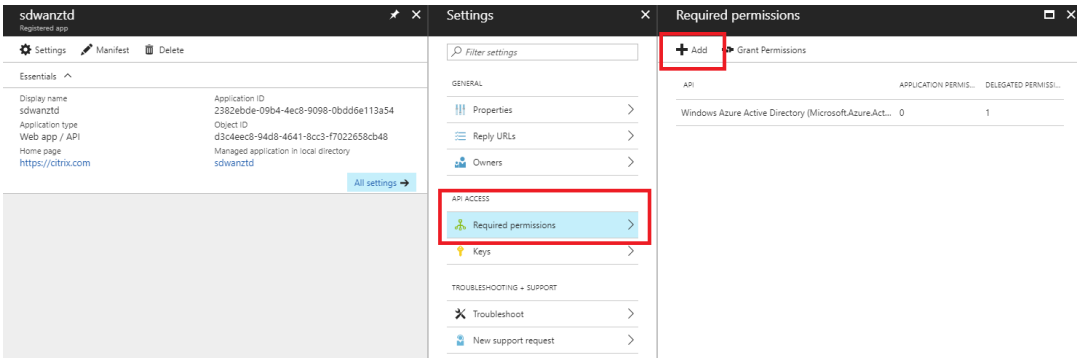
c) 在应用程序注册创建菜单中，输入名称和登录 URL（可以是任何 URL，唯一的要求是必须有效），然后单击创建。



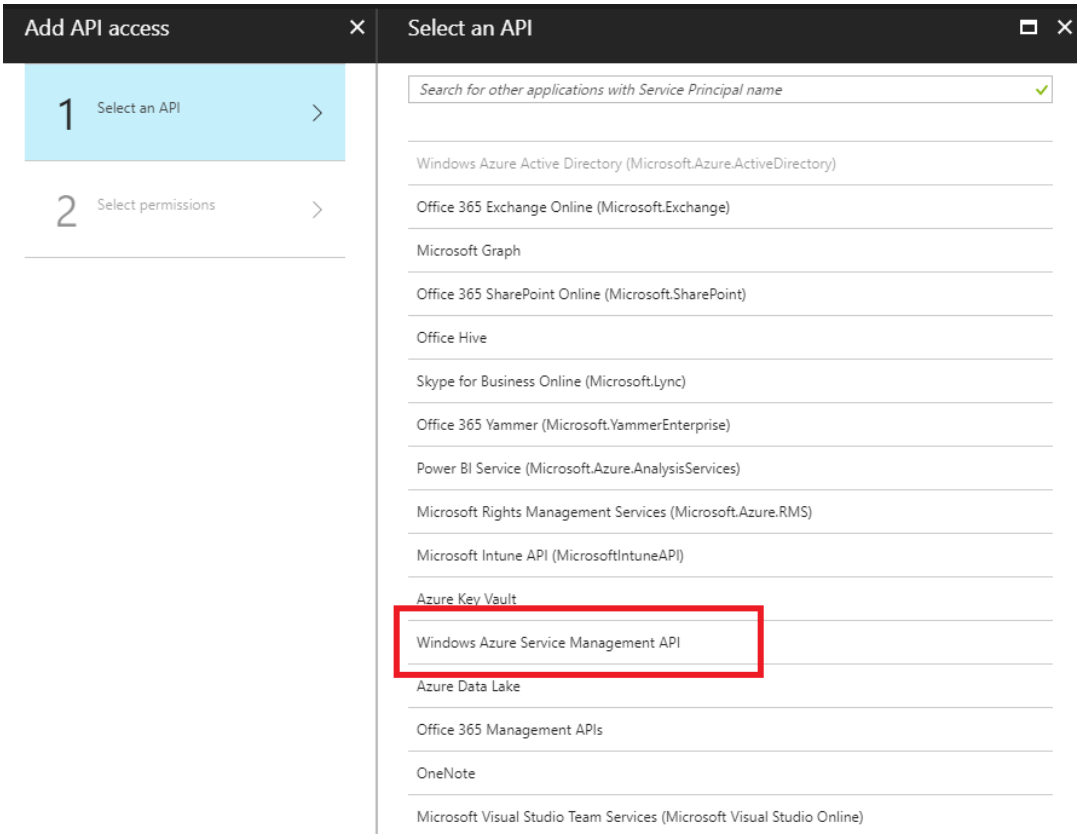
d) 搜索并打开新创建的注册应用程序，并记录应用程序 ID。



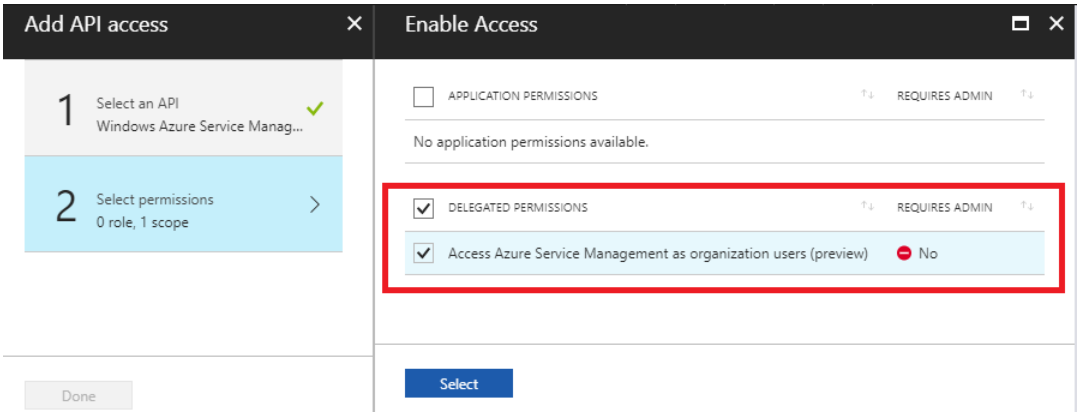
e) 再次打开新创建的注册应用程序，并确定所需的安全密钥，请在 API Access 下，选择必需的权限，以允许第三方配置和实例。然后选择添加。



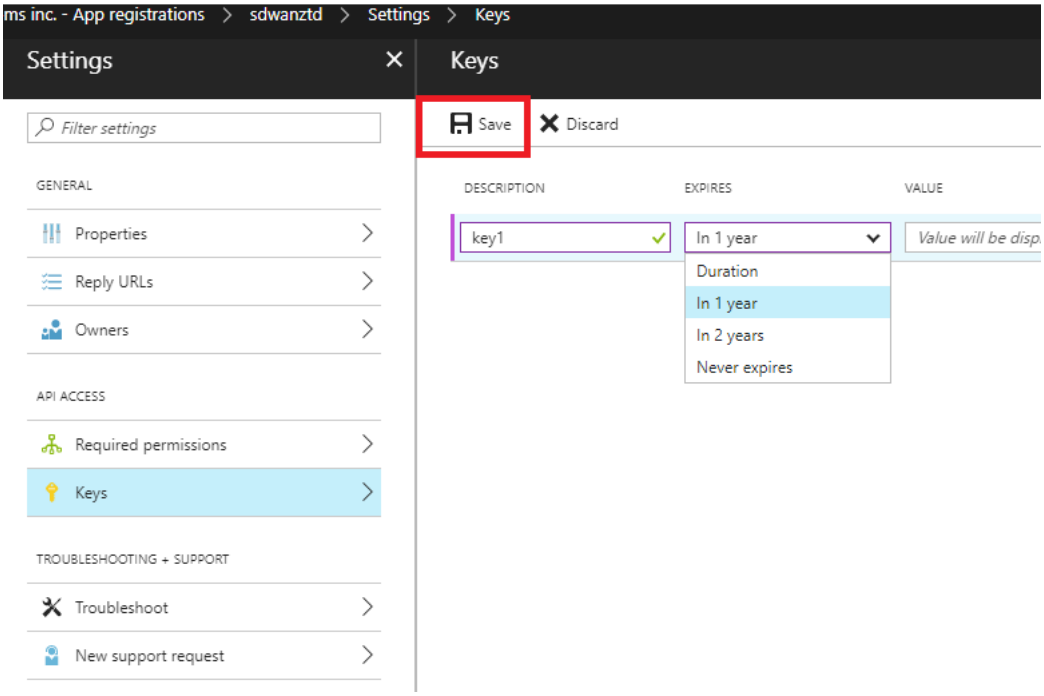
f) 添加所需权限时，选择一个 **API**，然后突出显示 **Windows Azure** 服务管理 **API**。



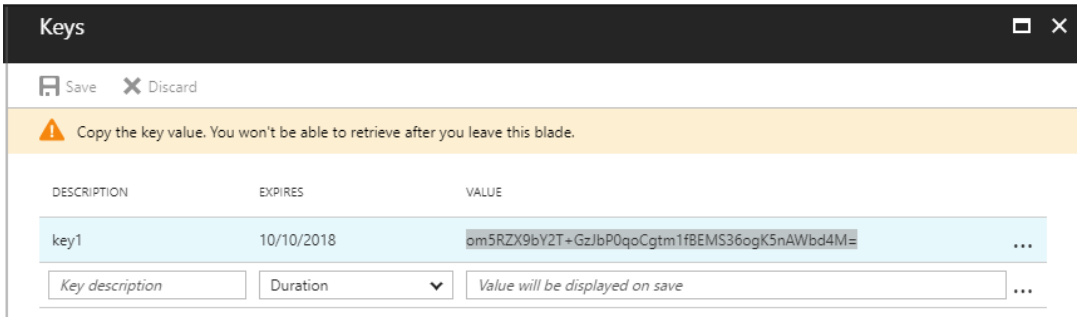
g) 启用委派权限以预配实例，然后单击选择和完成。



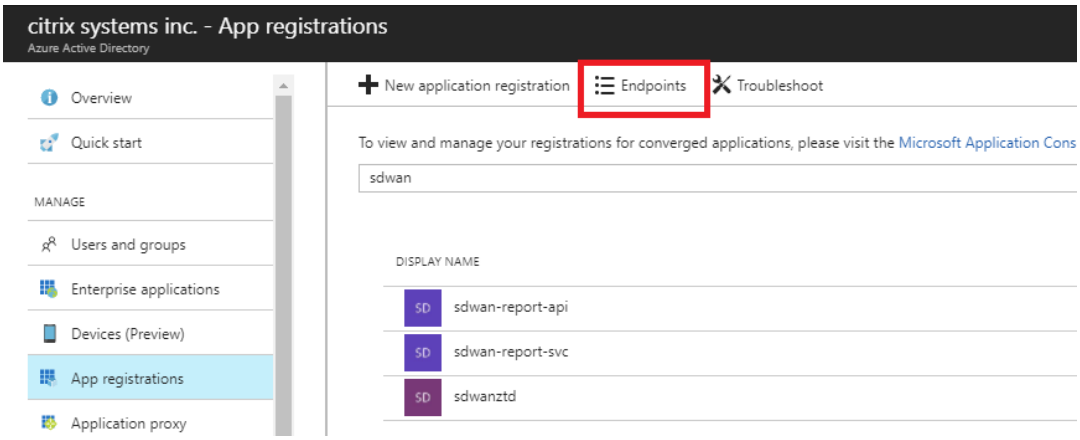
h) 对于此已注册应用程序，在 API Access 下，选择密钥，然后创建私有密钥描述和密钥有效的所需持续时间。然后单击保存，这将生成密钥，该密钥仅在预配过程中是必需的，可以在实例可用后将其删除。



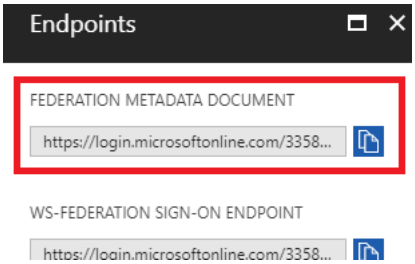
i) 复制并保存密钥（请注意，您以后将无法检索此密钥）。



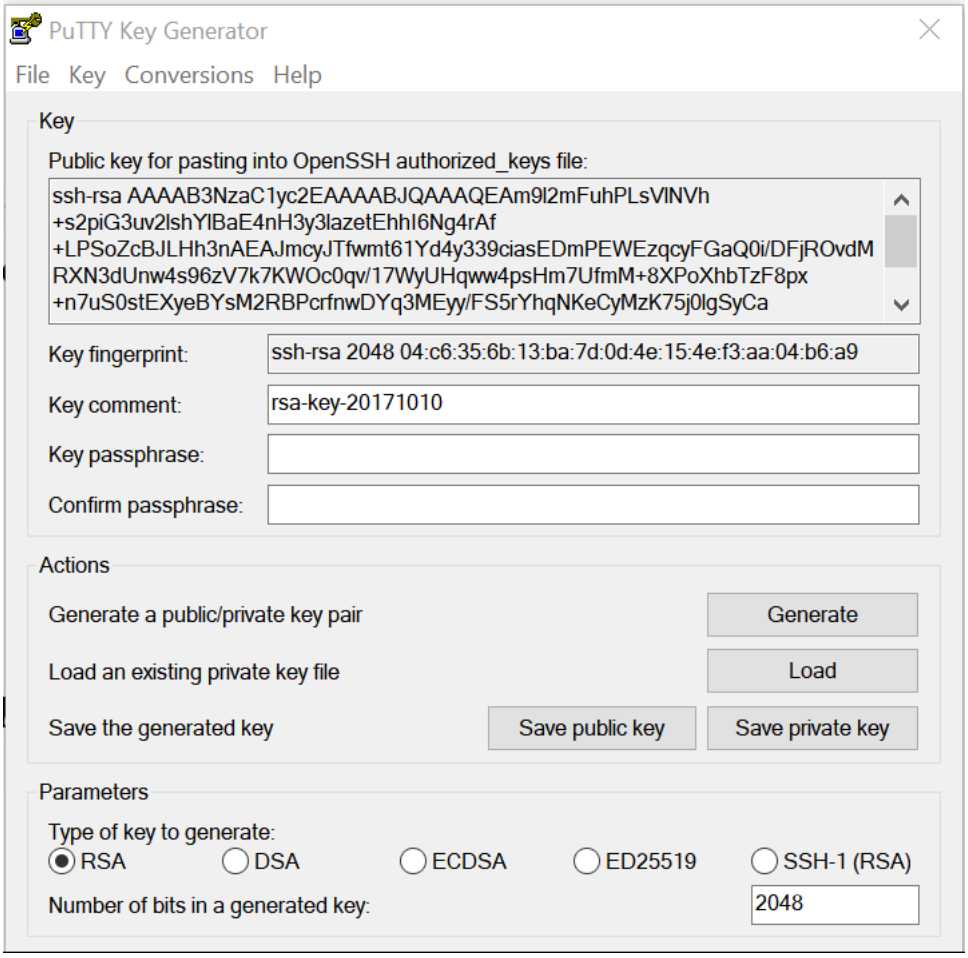
j) 要确定所需的 * 租户 **ID***, 导航回到“应用程序注册”窗格，然后选择端点。



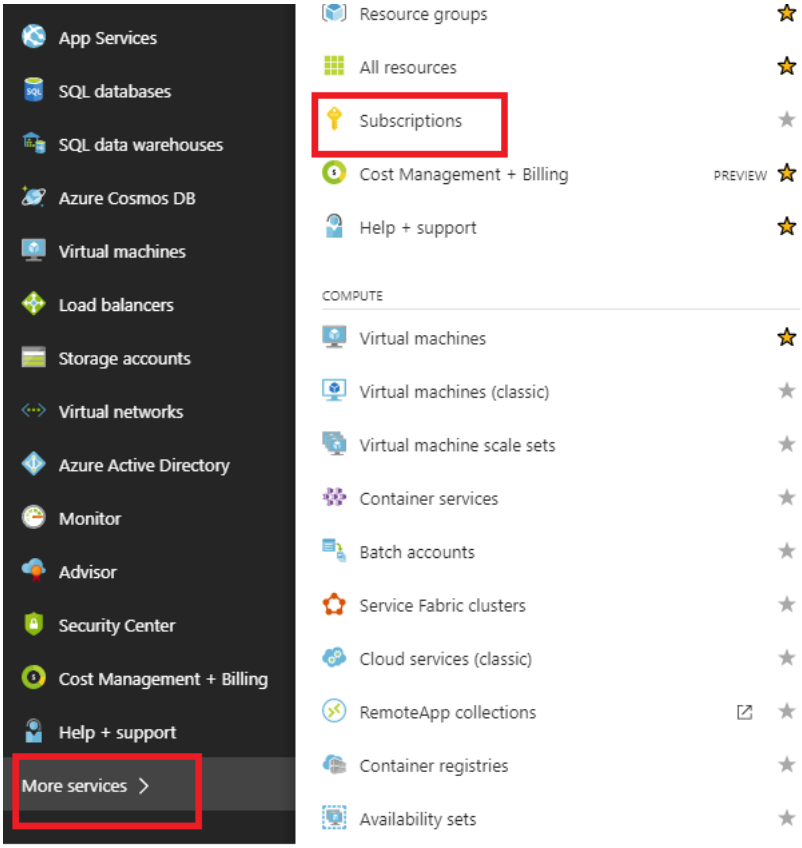
k) 复制联合元数据文档以标识您的租户 ID（注意租户 ID 为 36 字符的字符串，位于 URL 中的 online.com/与/federation 之间）。



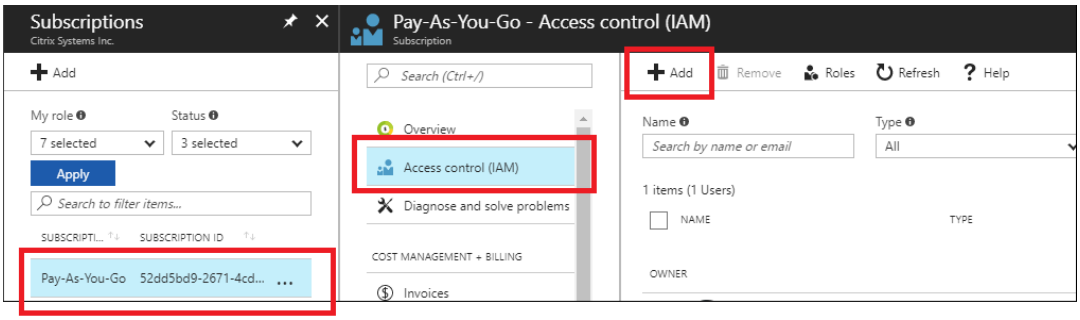
l) 所需的最后一项是 ***SSH*** 公钥。可以使用 Putty Key 发生器或 ssh keygen 创建此程序，并将其用于身份验证，从而不需要使用密码登录。可以复制 SSH 公钥（包括标头 ssh-rsa 和结尾的 rsa-key 字符串）。此公钥将通过 SD-WAN Center 输入共享到 Citrix 零接触部署服务。



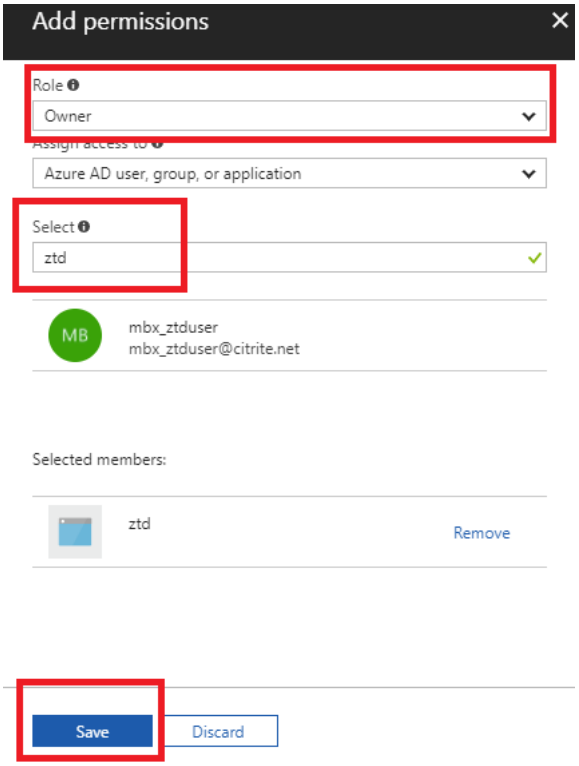
m) 为应用程序分配角色需要执行其他步骤。导航回“更多服务”，然后导航到“订阅”。



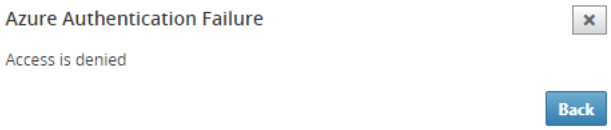
n) 选择活动订阅，然后选择访问控制 **(AIM)**，然后单击添加。



o) 在“添加权限”窗格中，选择所有者角色，分配对 **Azure AD** 用户、组或应用程序的访问权限，并在选择字段中搜索已注册的应用程序，以允许使用零轻点部署云服务来创建并配置在 Azure 订阅上实例。确定应用程序后，请选择该应用程序，并确保其在单击保存之前作为所选成员进行填充。

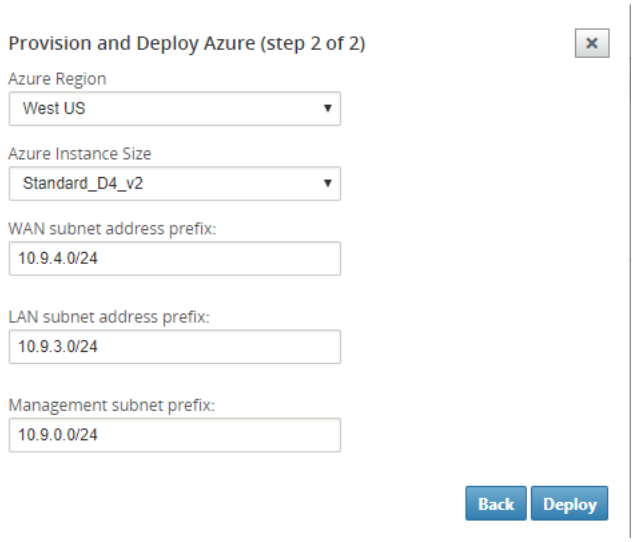


p) 收集所需输入并将其输入到 SD-WAN Center 后，单击下一步。如果输入不正确，则会出现身份验证失败。

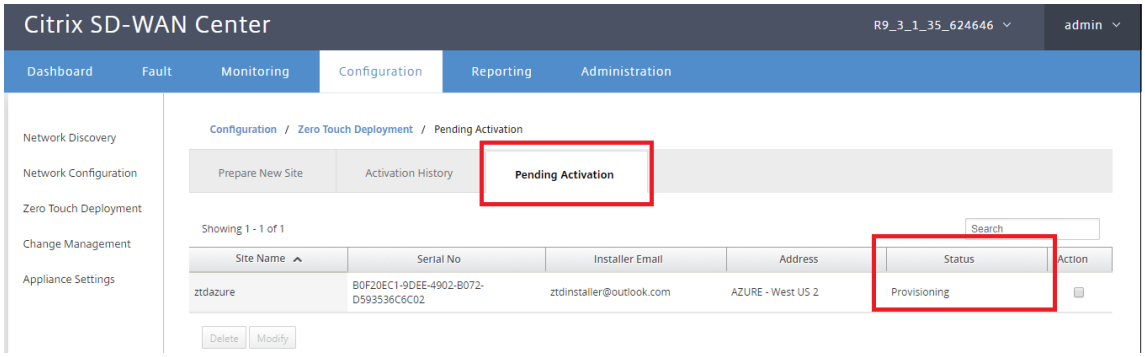


SD-WAN Center 预配和部署 Azure（第 2 步，共 2 步）

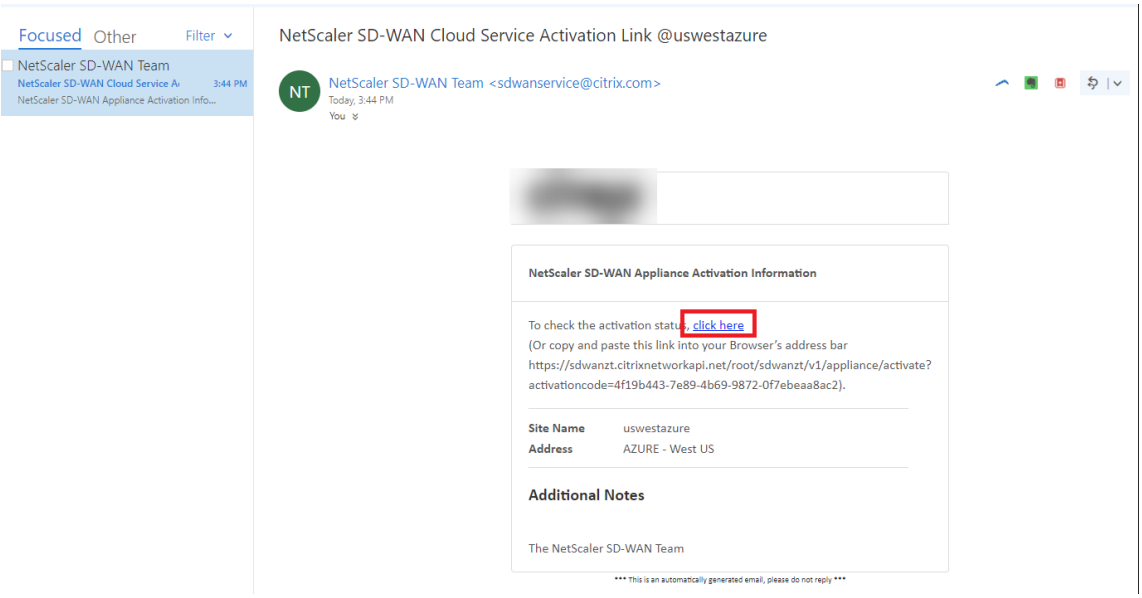
1. Azure 身份验证成功后，填充相应的字段以选择所需的 Azure 区域以及适当的实例大小，然后单击部署。



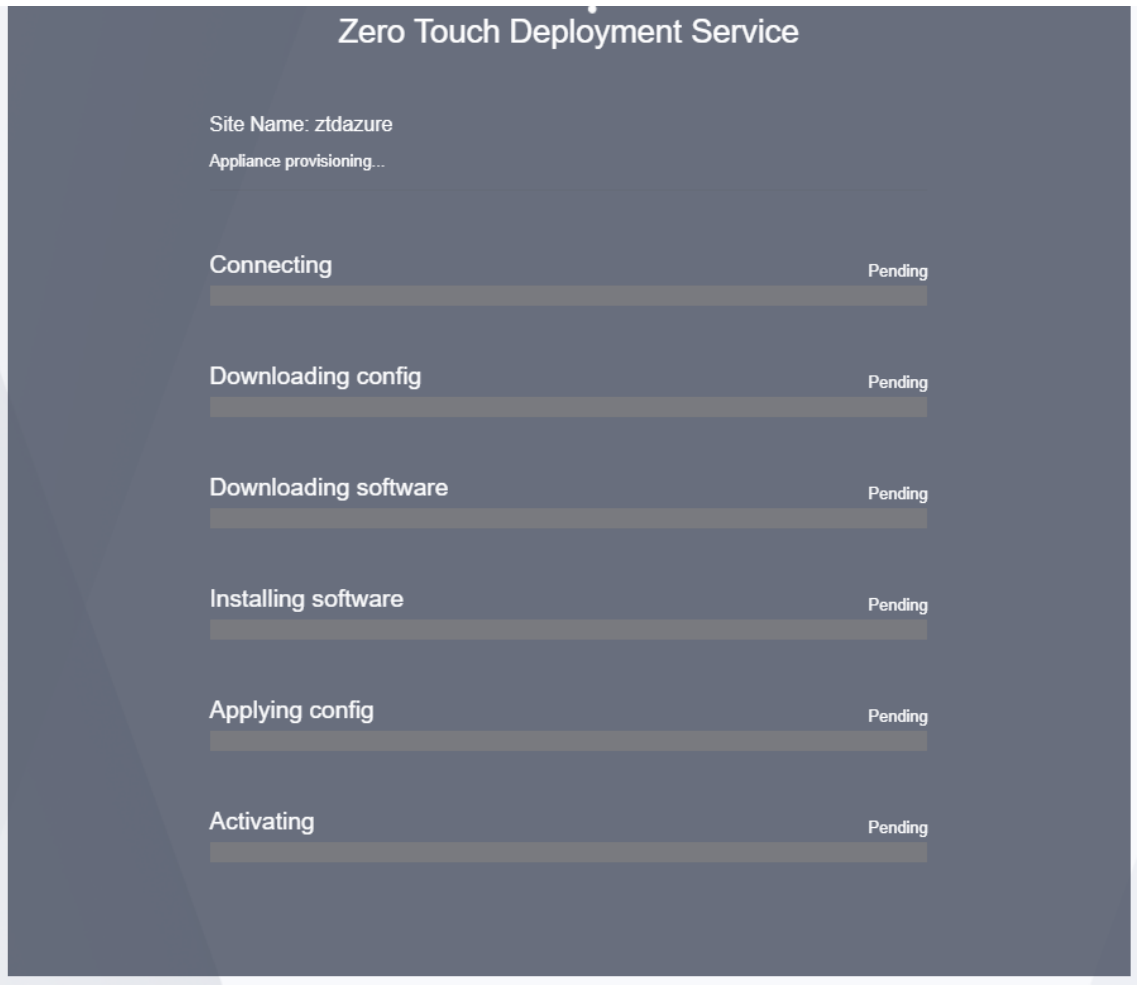
2. 导航到 SD-WAN Center 中的挂起的激活 选项卡可帮助跟踪部署的当前状态。



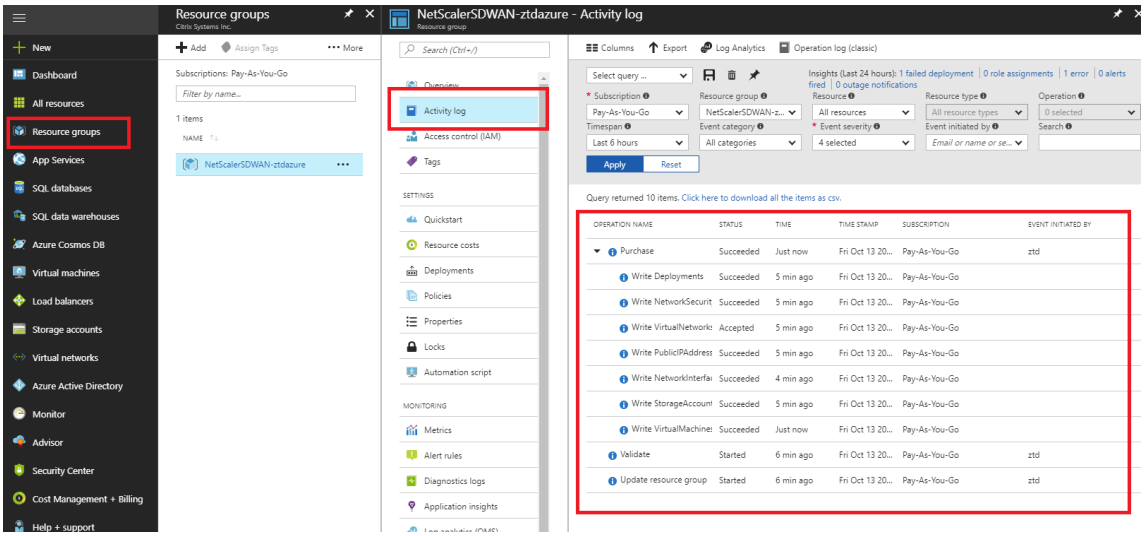
3. 在步骤 1 中，带有激活代码的电子邮件将传送到电子邮件地址输入项，获取电子邮件并打开激活 **URL** 以触发该过程并检查激活状态。



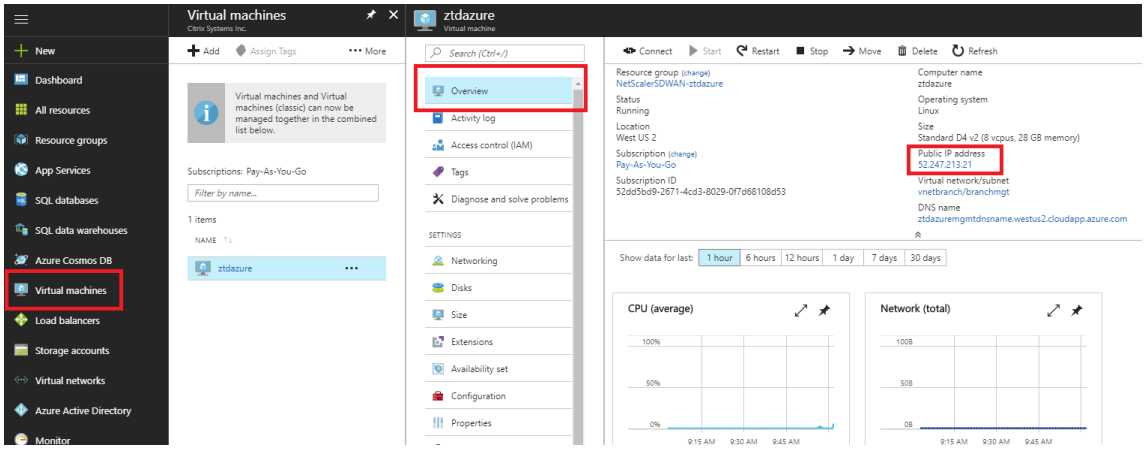
4. 带有激活 URL 的电子邮件将被发送到步骤 1 中输入的电子邮件地址。获取电子邮件并打开激活 **URL** 以触发流程并检查激活状态。



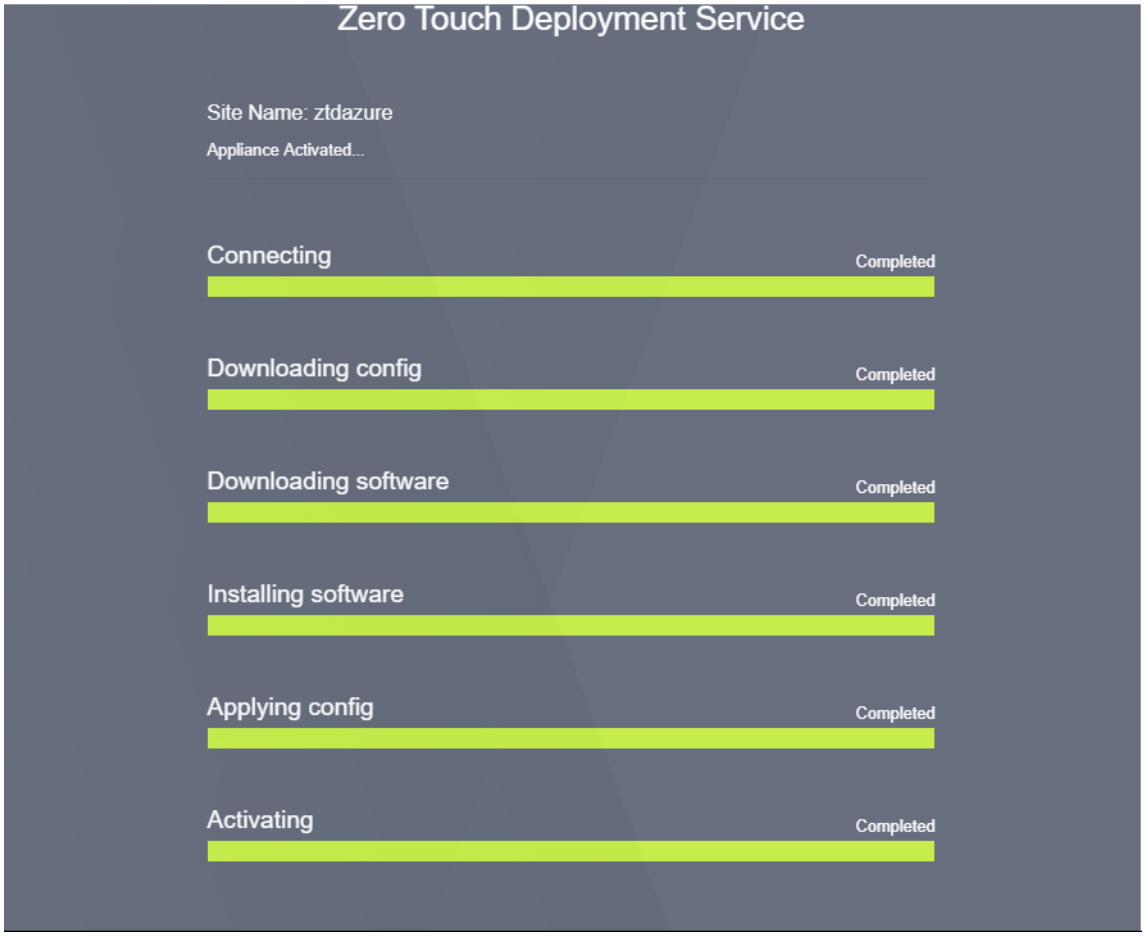
5. 使用 SD-WAN 云服务预配实例需要几分钟时间。您可以在 Azure 门户上，在自动创建的资源组下的活动日志下监视活动。此时将在此处填充预配的任何问题或错误，以及在激活状态下将其复制到 SD-WAN Center。



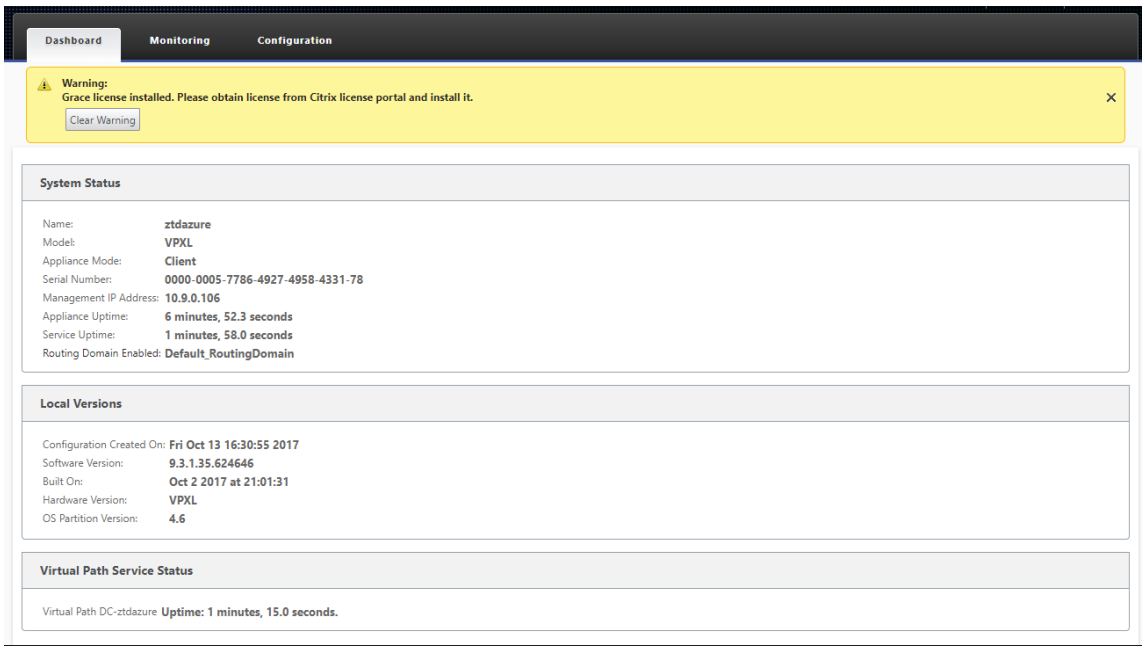
6. 在 Azure 门户中，成功启动的实例将在 虚拟机下提供。要获取分配的公用 IP，请导航至实例的概述。



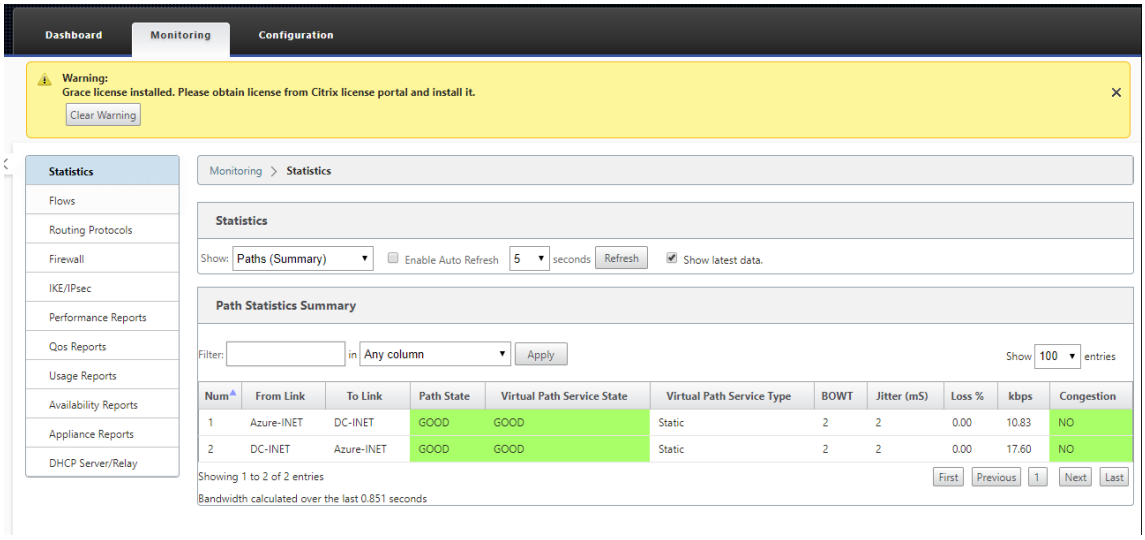
7. 当 VM 处于运行状态时，请在此时间后等待一分钟后，该服务才能完成，并启动下载配置、软件和许可证的过程。



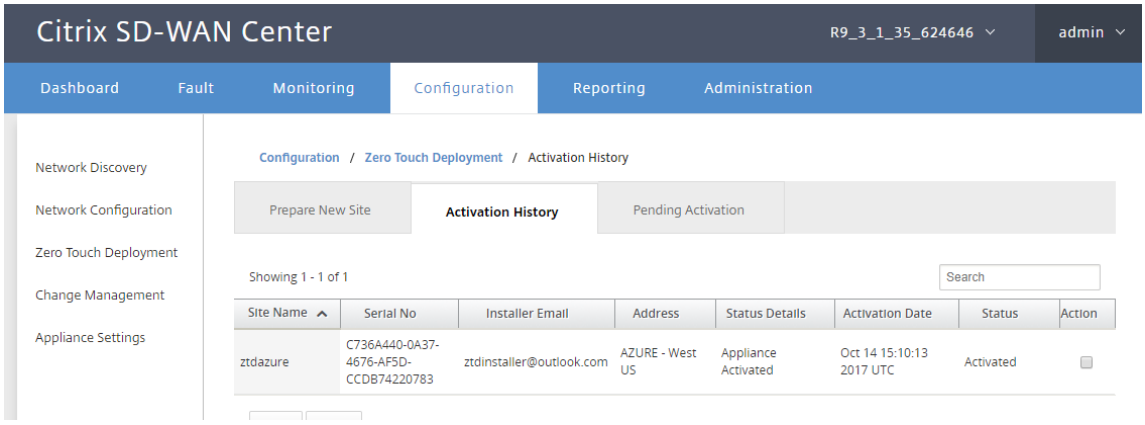
8. 每个 SD-WAN 云服务步骤自动完成后，使用从 Azure 门户获取的公用 IP 登录到 SD-WAN 实例 Web 界面。



9. Citrix SD-WAN 监视统计信息页面将在 Azure 中识别从 MCN 到 SD-WAN 实例的连接是否成功。



10. 此外，还会在 SD-WAN Center 的激活历史记录页面上记录成功的（或失败）预配尝试。



零接触部署的代理服务器设置

April 13, 2021

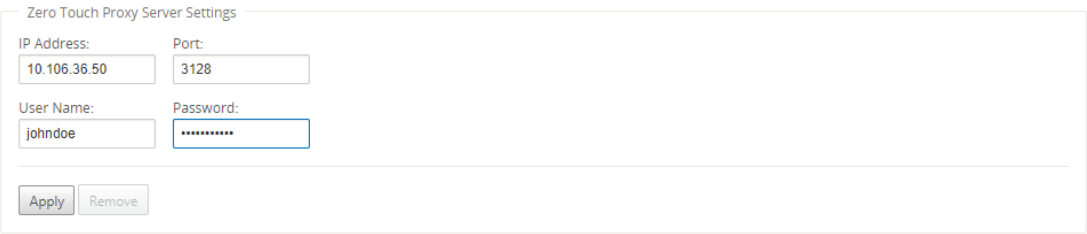
作为零接触部署的必备条件，应将 Citrix SD-WAN Center 连接到 Internet。如果 Citrix SD-WAN Center 通过代理服务器连接到 Internet，则必须在 Citrix SD-WAN Center 上配置代理服务器设置。

> 注意
>
> 此代理服务器设置仅用于零接触部署。

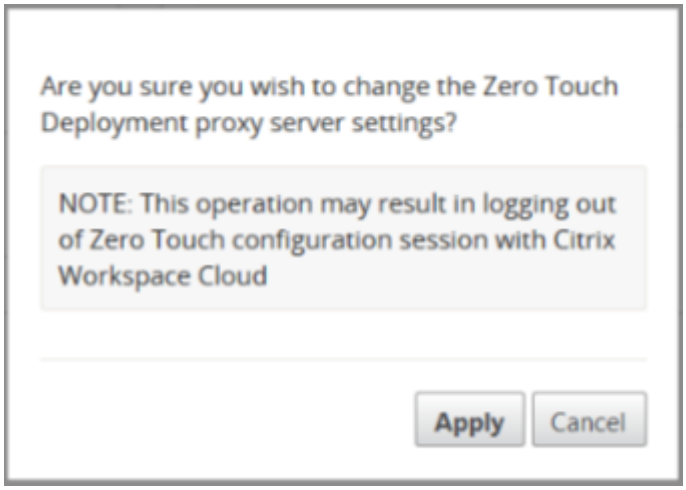
要配置零触摸代理服务器设置，请执行以下操作：

1. 在 SD-WAN Center Web 界面中，导航到管理 > 全局设置 > 管理接口。
2. 在零触摸代理服务器设置部分中，输入以下字段的值：
   - **IP** 地址：代理服务器的 IP 地址。
   - 端口：代理服务器用于接受连接的网络端口号。
   - 用户名：代理服务器用户名
   - 密码：代理服务器的密码。

> 注意
>
> 如果未在代理服务器上配置身份验证，则可以将用户名和密码字段留空。



3. 单击应用后，将显示确认对话框。

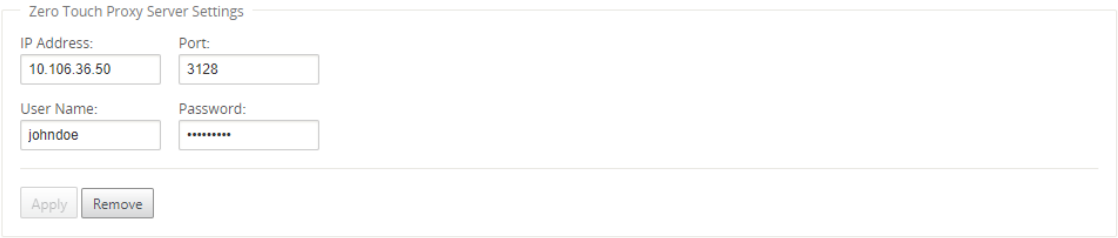


4. 单击应用。

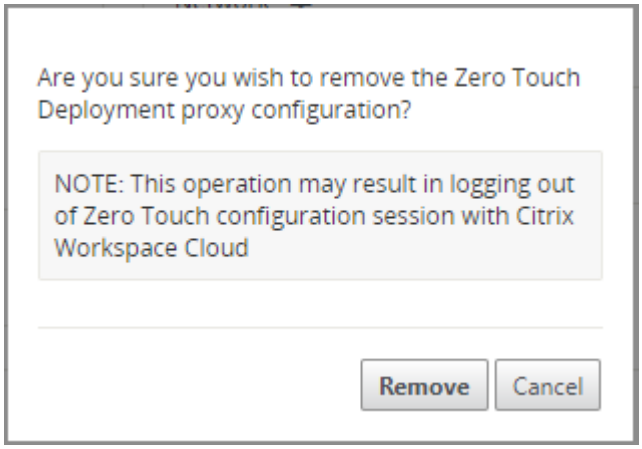
> 注意
>
> 如果 Citrix SD-WAN Center 直接连接到 Internet，则可以完全删除代理服务器设置。如有需要，还可以删除代理服务器设置，并配置其他代理服务器。

要删除代理服务器设置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，导航到管理 > 全局设置 > 管理接口。
2. 在零触摸代理服务器设置部分中，单击删除。



3. 单击删除时，将显示一个确认对话框。



4. 单击删除。

Palo Alto 网络集成

April 13, 2021

Palo Alto 网络提供基于云的安全基础设施，用于保护远程网络。它通过允许组织设置区域、基于云的防火墙来保护 SD-WAN 架构来提供安全性。

适用于远程网络的 Prisma Access 服务允许您登载远程网络位置，并为用户提供安全性。它消除了在每个远程位置配置和管理设备的复杂性。该服务提供了一种有效的方式，可以轻松添加新的远程网络位置，并通过确保这些位置的用户始终保持连接和安全，最大限度地减少运营挑战，并允许您从 Panorama 集中管理策略，为远程提供一致和简化的安全性网络位置。

要将远程网络位置连接到 Prisma Access 服务，可以使用 Palo Alto 网络下一代防火墙或符合 IPsec 标准的第三方设备（包括
SD-WAN），该设备可以建立到该服务的 IPsec 隧道。

- 规划远程网络的 Prisma Access 服务
- 配置远程网络的 Prisma Access 服务
- 带配置导入的板载远程网络

Citrix SD-WAN 解决方案已经提供了从分支中分离 Internet 流量的功能。这对于提供更可靠、低延迟的用户体验至关重要，同时避免在每个分支机构引入昂贵的安全堆栈。Citrix SD-WAN 和 Palo Alto 网络现在为分布式企业提供了一种更可靠和安全的方式，将分支机构中的用户连接到云中的应用程序。

Citrix SD-WAN 设备可以通过 IPsec 隧道从具有最低配置的 SD-WAN 设备位置连接到 Palo Alto 云服务（Prisma Access 服务）网络。可以在 Citrix SD-WAN Center 中配置 Palo Alto 网络。

在开始为远程网络配置 Prisma Access 服务之前，请确保已准备好以下配置，以确保您能够成功启用该服务并为远程网络位置中的用户强制执行策略：

1. 服务连接—如果您的远程网络位置需要访问公司总部的基础设施以验证用户身份或启用对关键网络资产的访问，则必须设置对您的企业网络的访问，以便总部和远程网络位置连接。

如果远程网络位置是自主的，并且不需要访问其他位置的基础设施，则无需设置服务连接（除非您的移动用户需要访问）。

1. 模板—Prisma Access 服务自动为远程网络的 Prisma Access 服务创建模板堆栈(Remote_Network_Template_Stack)和热门模板（Remote_Network_Template）。要为远程网络配置 Prisma Access 服务，请从头开始配置热门模板或利用现有配置（如果您已在本地运行 Palo Alto 网络防火墙）。

   该模板需要设置来建立 IPsec 隧道和 Internet 密钥交换 (IKE) 配置，用于远程网络位置与 Prisma Access 服务之间的协议协商，您可以在安全策略中引用的区域，以及日志转发配置文件，以便您可以将日志从远程网络的 Prisma Access 服务转发到日志记录服务。

2. 父设备组—远程网络的 Prisma Access 服务要求您指定包含安全策略、安全配置文件和其他策略对象（如应用程序组和对象以及地址组）的父设备组以及身份验证策略，以便远程网络的 Prisma Access 服务可以一致地对通过 IPSec 隧道路由到远程网络的 Prisma Access 服务的流量实施策略。您需要在 Panorama 上定义策略规则和对象，或使用现有设备组来保护远程网络位置中的用户的安全。

   > 注意：
   >
   > 如果您使用引用区域的现有设备组，请确保将定义区域的相应模板添加到远程网络 _ 模板 _ 堆栈中。

   这允许您在配置远程网络的 Prisma Access 服务时完成区域映射。

3. **IP** 子网—为了使 Prisma Access 服务将流量路由到您的远程网络，您必须为要使用 Prisma Access 服务保护的子网提供路由信息。您可以在远程网络位置定义指向每个子网的静态路由，或者在服务连接位置和 Prisma Access 服务之间配置 BGP，或者使用两种方法的组合。

   如果配置两个静态路由并启用 BGP，则静态路由优先。虽然如果远程网络位置只有几个子网，则使用静态路由可能会很方便，但在具有多个具有重叠子网的远程网络的大型部署中，BGP 可以让您更轻松地扩展。

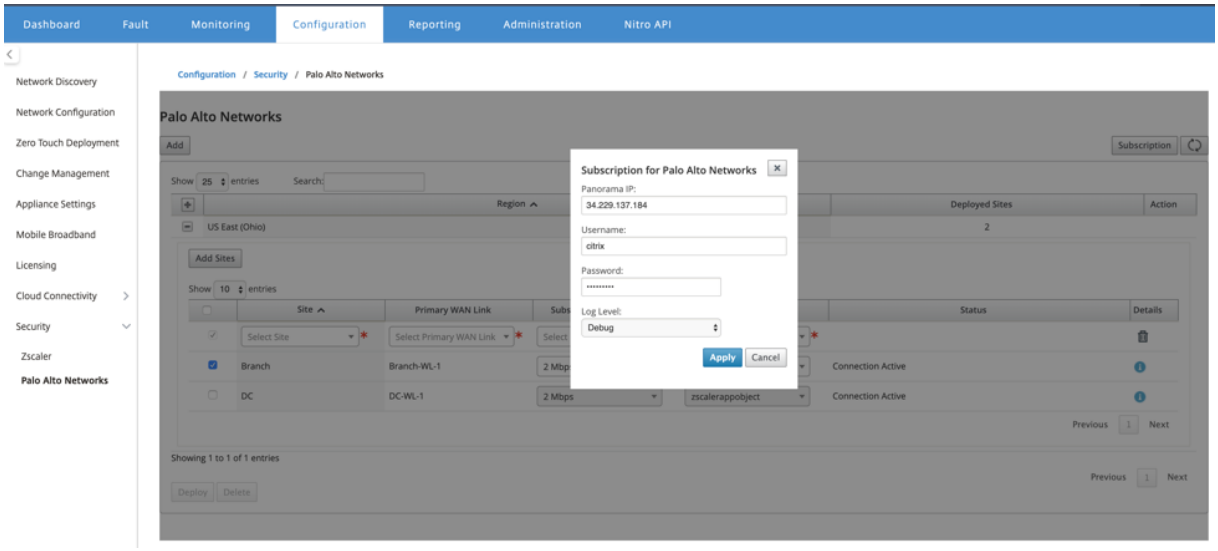
SD-WAN Center 中的 Palo Alto 网络

确保满足以下先决条件：

- 从 PRISMA ACCESS 服务获取全景 IP 地址。
- 在 PRISMA Access 服务中获取用户名和密码用户。
- 在 SD-WAN 设备 GUI 中配置 IPsec 隧道。
- 确保该网站没有登录到一个地区，该地区已经有一个不同的网站配置了不同的 IP/IPSec 配置文件，而不是 Citrix-IKE 加密默认值/Citrix-IPSec-加密默认值。
- 请确保 Prisma Access 配置不会手动更改配置时由 SD-WAN Center 更新。

在 Citrix SD-WAN Center GUI 中，提供 Palo Alto 订阅信息。

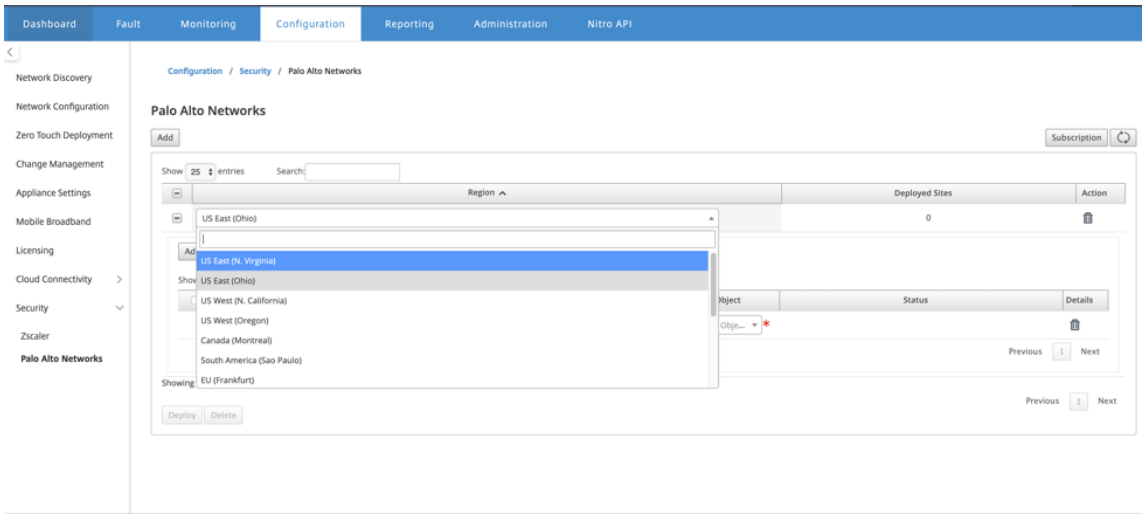
- 配置全景 IP 地址。您可以从 Palo Alto 获得此 IP 地址（PRISMA ACCESS 服务）。
- 配置 PRISMA ACCESS 服务中使用的用户名和密码。

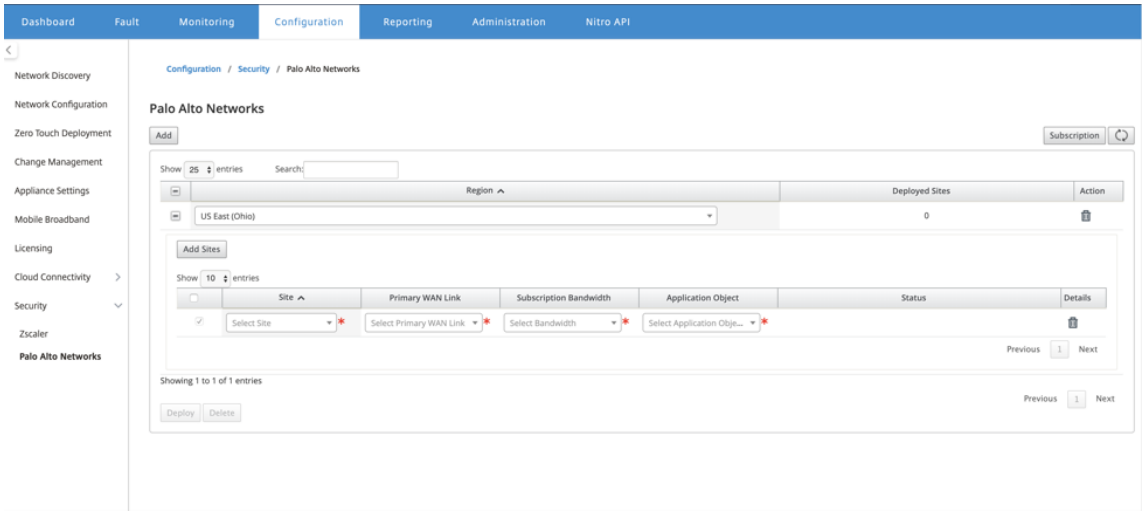


添加和部署站点

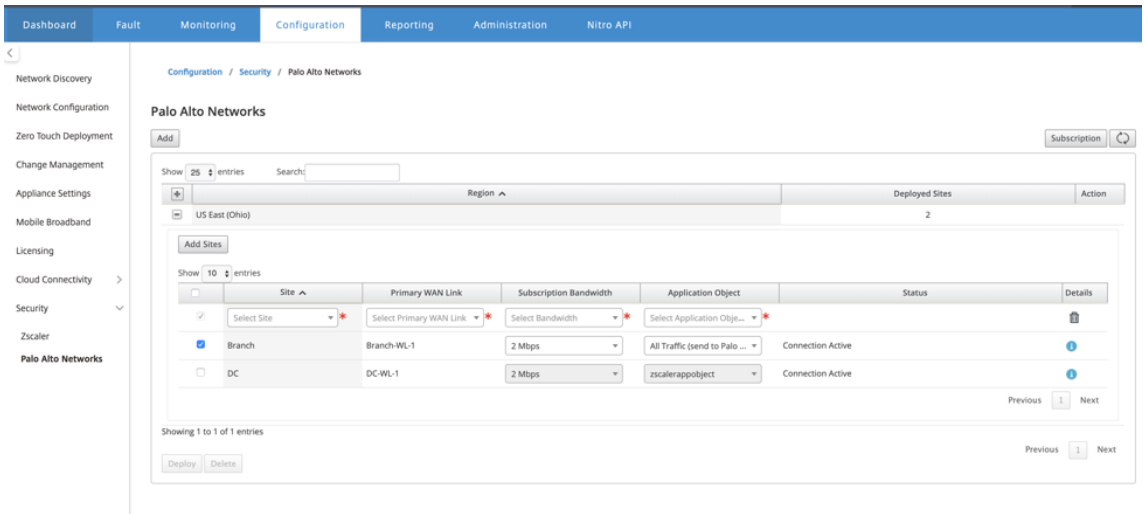
1. 若要部署站点，请选择要为 Prisma Access 区域配置的 PRISMA ACCESS 网络区域和 SD-WAN 站点，然后选择站点 WAN 链接、带宽和应用程序对象进行流量选择。

> 注意：
>
> 如果所选带宽超过可用带宽范围，则流量会受到影响。
>
> 通过选择 应用程序对象选择 下的 所有流量 选项，可以选择将 所有 **Internet** 绑定的流量 重定向到 PRISMA ACCESS 服务。

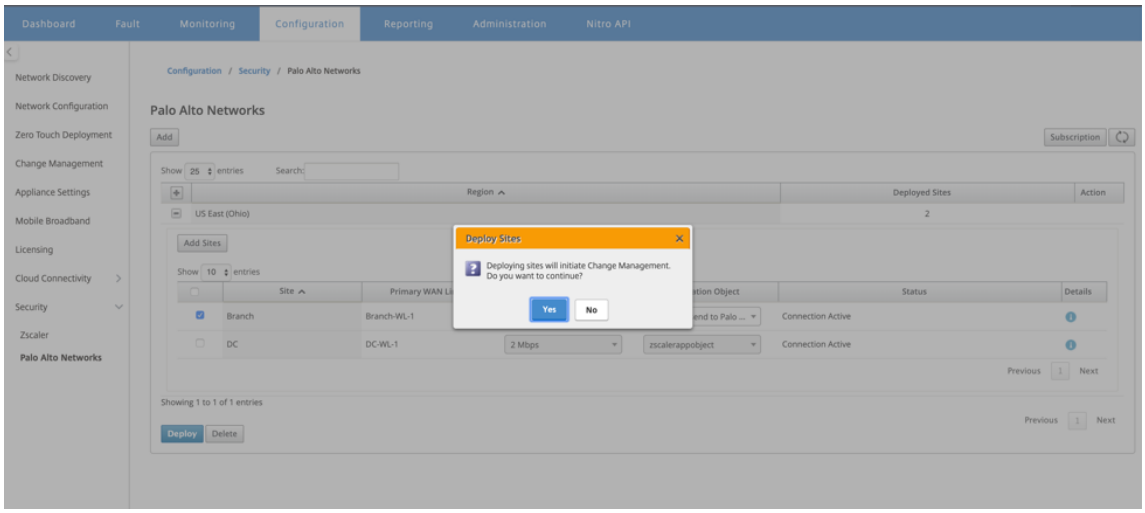




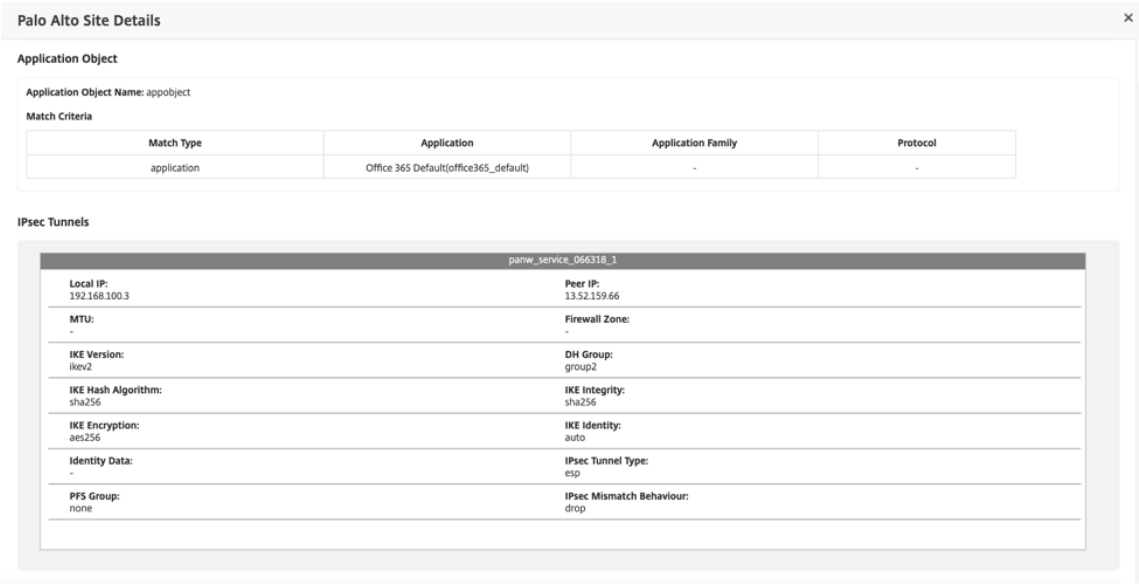
2. 您可以根据需要继续添加更多 SD-WAN 分支站点。



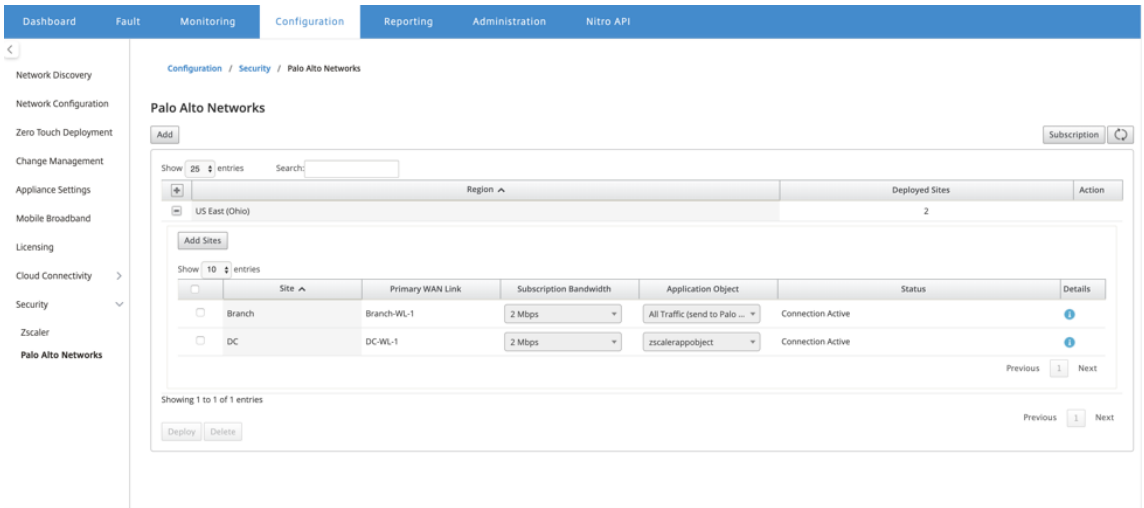
3. 单击部署。启动更改管理流程。单击“是”继续。



部署后，用于建立隧道的 IPsec 隧道配置如下。



登录页面显示在不同 SD-WAN 区域中配置和分组的所有站点的列表。



验证端到端流量连接：

- 从分支机构的 LAN 子网访问互联网资源。
- 验证流量是否通过 Citrix SD-WAN IPsec 隧道进入 Palo Alto Prisma Access。
- 验证是否在“监视”选项卡下对流量应用了 Palo Alto 安全策略。
- 验证从互联网到分支中的主机的响应是通过的。

Microsoft Azure 虚拟广域网

April 13, 2021

Microsoft Azure 虚拟 WAN 和 Citrix SD-WAN 可以在混合云工作负载中提供简化的网络连接和集中化的管理。可以自动执行分支设备的配置，以连接到 Azure WAN 并根据业务要求配置分支流量管理策略。内置控制板界面提供了即时故障排除见解，可以节省时间，并提供大规模的站点到站点间连接的可见性。

使用 Microsoft Azure 虚拟 WAN，可以简化与 Azure 云工作负载的连接，并可在 Azure 主干网之间路由流量。Azure 在地球 Azure 区域中提供了 54 个和多个存在点，用作可以选择连接到分支机构的集线器。连接分支后，请通过 hub 到 hub 连接使用 Azure 云服务。可以通过对 Azure VNETs 应用多个 Azure 服务（包括中枢对等）来简化连接。中心充当分支机构的流量网关。

Microsoft Azure 虚拟 WAN 具有以下优点：

- Hub 和分支中的集成连接解决方案-从各种来源（包括连接的合作伙伴解决方案）自动实现站点到站点的连接以及在本地与 Azure Hub 之间的配置。
- 自动设置和配置—将虚拟网络无缝连接到 Azure 中心。
- 直观的故障排除–您可以在 Azure 中看到端到端流，并使用此信息来执行所需的操作。

使用 Citrix SD-WAN 连接到微软 Azure 虚拟广域网

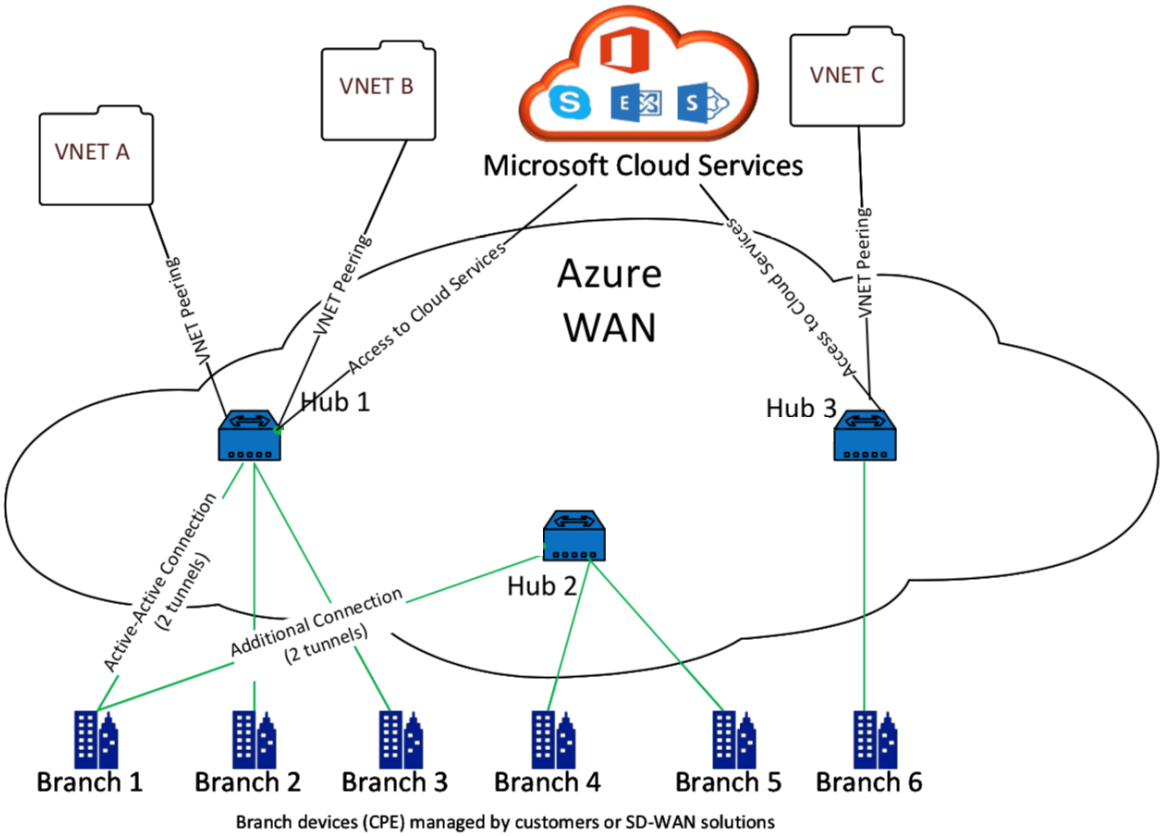
February 18, 2022

对于要连接到 Azure 的本地设备，需要使用控制器。控制器插入 Azure API，用于建立与 Azure WAN 和 Hub 的站点到站点的连接。

Microsoft Azure 虚拟 WAN 包括以下组件和资源：

- WAN：表示 Microsoft Azure 中的整个网络。它包含指向您希望在此广域网中拥有的所有中心的链接。WAN 彼此相互隔离，不能包含公用集线器，也不能包含在不同 WAN 中的两个 hub 之间的连接。
- 站点：表示本地 VPN 设备及其设置。一个站点可以连接到多个中心。通过 Citrix SD-WAN，可以使用内置解决方案自动将此信息导出到 Azure。
- Hub：表示您的网络在特定区域的核心。Hub 包含各种服务终端节点，可以实现与本地网络的连接和其他解决方案。在站点之间建立站点到站点的连接，然后再到 Hub VPN 端点。
- Hub 虚拟网络连接：Hub 网络可以将 Azure 虚拟 WAN Hub 无缝连接到您的虚拟网络。目前，连接到同一虚拟中心区域内的虚拟网络可用。
- 分支：分支是本地 Citrix SD-WAN 设备，存在于客户办公地点。SD-WAN 控制器集中管理分支。连接源于这些分支的后面，终止到 Azure。SD-WAN 控制器负责将所需的配置应用于这些分支和 Azure Hub。

下图介绍了虚拟 WAN 组件：



微软 **Azure** 虚拟广域网如何工作

1. SD-WAN Center 通过使用服务主体、主体或基于角色的访问功能进行身份验证，在 Azure GUI 中处于启用状态。
2. SD-WAN Center 获取 Azure 连接配置并更新本地设备。这会自动执行本地设备的配置下载、编辑和更新。
3. 在设备具有正确的 Azure 配置后，将向 Azure WAN 建立一个站点到站点连接（两个主动 IPsec 通道)。Azure 需要分支设备连接器才能支持 IKEv2 设置。BGP 配置是可选的。

   注意：建立 IPsec 通道的 IPsec 参数的标准化。

IPsec 属性	参数
IKE 加密算法	AES 256
IKE 完整性算法	SHA 256
Dh 集团	DH2
IPsec 加密算法	GCM AES 256

IPsec 属性	参数
IPsec 完整性算法	GCM AES 256
PFS 组	无

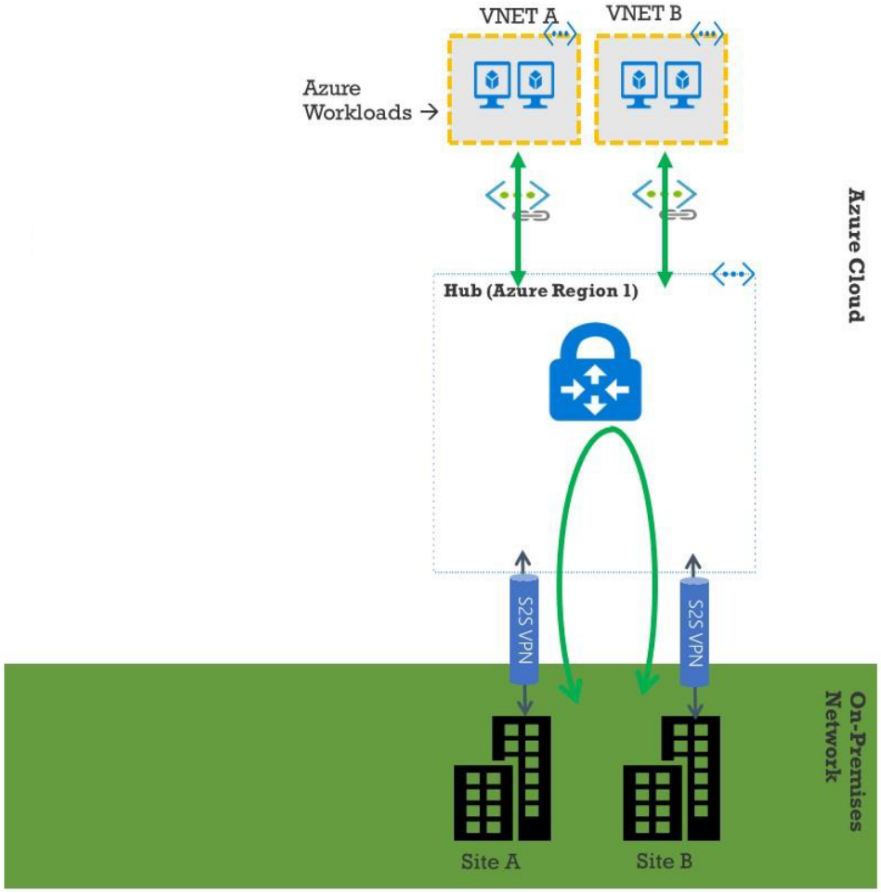
Azure 虚拟 WAN 可自动执行工作负载虚拟网络和中心之间的连接。创建中心虚拟网络连接时，它会在预配的 Hub 与工作负载虚拟网络 (VNET) 之间设置适当的配置。

先决条件和要求

请先阅读以下要求，然后再继续配置 Azure 和 SD-WAN 以管理连接到 Azure hub 的分支站点。

1. 已将虚拟广域网的 Azure 订阅列入白名单。
2. 使用软件定义广域网设备等本地设备在 Azure 资源中建立 IPsec。
3. 拥有带公共 IP 地址的互联网链接。虽然单个 Internet 链接足以建立连接到 Azure，但您需要两个 IPsec 通道才能使用相同的 WAN 链接。
4. SD-WAN controller-controller 是负责配置 SD-WAN 设备以连接到 Azure 的接口。
5. Azure 中至少有一个工作负载的 VNET。例如，负责托管服务的 VM。请注意以下几点：
   a) 虚拟网络不应具有 Azure VPN 或快速路由网关或网络虚拟设备。
   b) 虚拟网络不应具有用户定义的路由，该路由将流量路由到非虚拟 WAN 虚拟网络，以处理从内部分支机构访问的工作负载。
   c) 必须配置访问工作负载的适当权限。例如，对于 ubuntu VM，请使用端口 22 SSH 访问权限。

下图说明了 Microsoft Azure 中包含两个站点和两个虚拟网络的网络。



设置微软 **Azure** 虚拟 **WAN**

对于要连接到 Azure 并通过 IPsec 隧道访问资源的本地 SD-WAN 分支，应完成以下步骤。

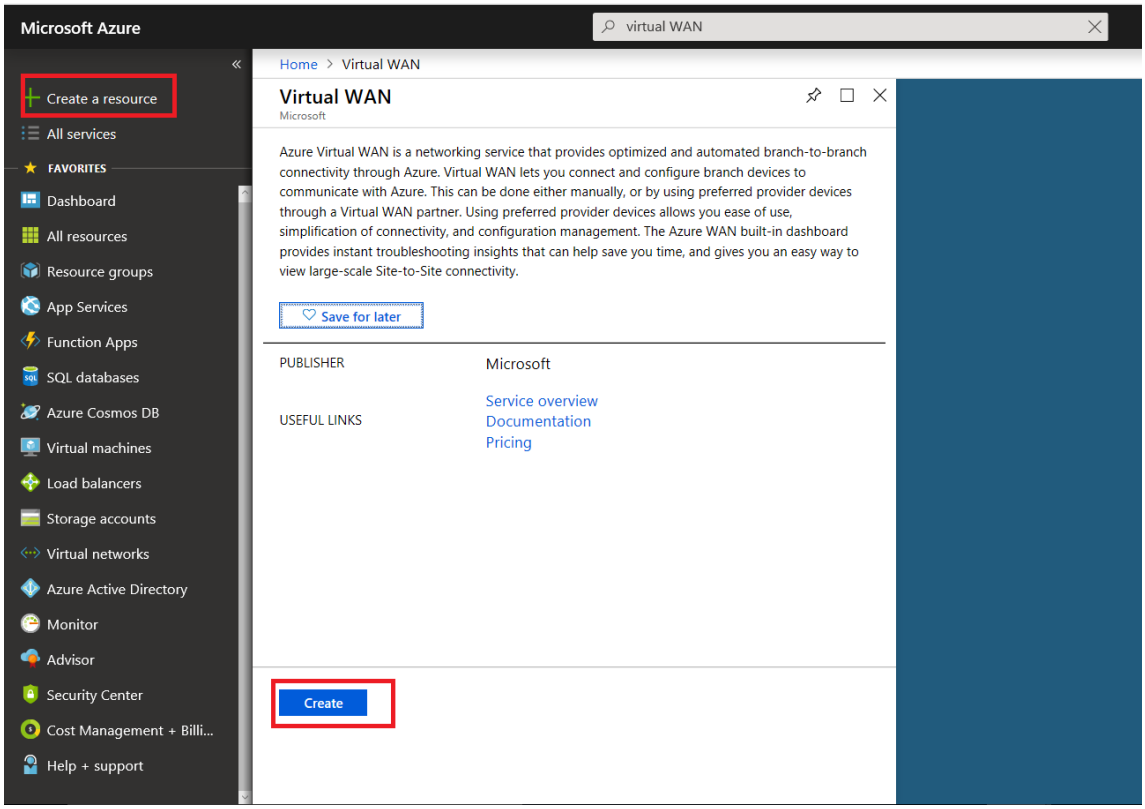
1. 配置 WAN 资源。
2. 启用 SD-WAN 分支以使用 IPsec 通道连接到 Azure。

配置 SD-WAN 网络之前，请配置 Azure 网络，因为连接到 SD-WAN 设备所需的 Azure 资源事先必须可用。但是，您可以在配置 Azure 资源之前配置 SD-WAN 配置（如果您首选)。本主题讨论在配置 SD-WAN 设备之前首先设置 Azure 虚拟 WAN 网络。https://microsoft.com azure virtual-wan。

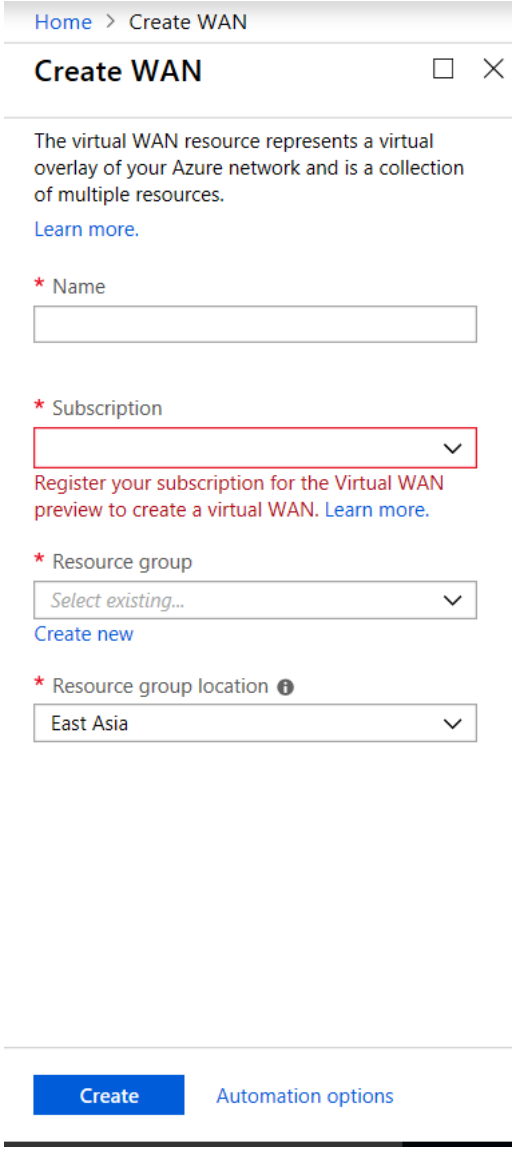
创建 **WAN** 资源

要使用虚拟 WAN 功能并将本地分支设备连接到 Azure，请执行以下操作：

1. 登录 Azure 应用商店，转到虚拟 WAN 应用程序，然后选择创建广域网。



2. 输入 WAN 的名称，然后选择要用于 WAN 的订阅。



3. 选择现有资源组或创建新资源组。资源组是逻辑构造，资源组之间的数据交换始终是可能的。
4. 选择您希望资源组驻留的位置。WAN 是一种没有位置的全球资源。但是，您必须为包含 WAN 资源元数据的资源组输入位置。
5. 单击“创建”。这将启动验证和部署设置的过程。

创建网站

您可以使用首选供应商创建站点。首选供应商将与您的设备和站点有关的信息发送至 Azure，或者您可以决定自己管理设备。如果要管理设备，需要在 Azure 门户中创建站点。

SD-WAN 网络和微软 **Azure** 虚拟 **WAN** 工作流

配置 SD-WAN 设备：

1. 预配 Citrix SD-WAN 设备
    - 将 SD-WAN 分支设备连接到 MCN 设备。
2. 配置 SD-WAN 设备
    - 为主动-主动连接配置 Intranet 服务。

配置 SD-WAN Center：

- 将 SD-WAN Center 配置为连接到 Microsoft Azure。

配置 Azure 设置：

- 提供租户 ID、客户端 ID、安全密钥、订阅者 ID 和资源组。

将分支站点配置为 WAN 关联：

1. 将一个 WAN 资源关联到分支机构。同一站点无法连接到多个 WAN。
2. 单击新建以配置站点 WAN 关联。
3. 选择 **Azure WAN** 资源。
4. 选择站点的服务（Intranet）。选择两项服务以获得活动-备用支持。
5. 选择要与 WAN 资源相关联的站点名称。
6. 单击部署以确认关联。
7. 等待状态更改为已部署的通道，以查看 **IPsec** 通道设置。
8. 使用 SD-WAN Center 报告视图检查相应 IPsec 隧道的状态。

配置 **Citrix SD-WAN** 网络

MCN：

MCN 充当初始系统配置和后续配置更改的分发点。虚拟 WAN 中只能有一个活动的 MCN。
默认情况下，设备具有客户端的预先分配的角色。要将设备建立为 MCN，必须首先添加站点并将其配置为 MCN。在将站点配置为 MCN 后，网络配置 GUI 变为可用。必须仅从 MCN 或 SD-WAN Center 执行升级和配置更改。

MCN 的角色：

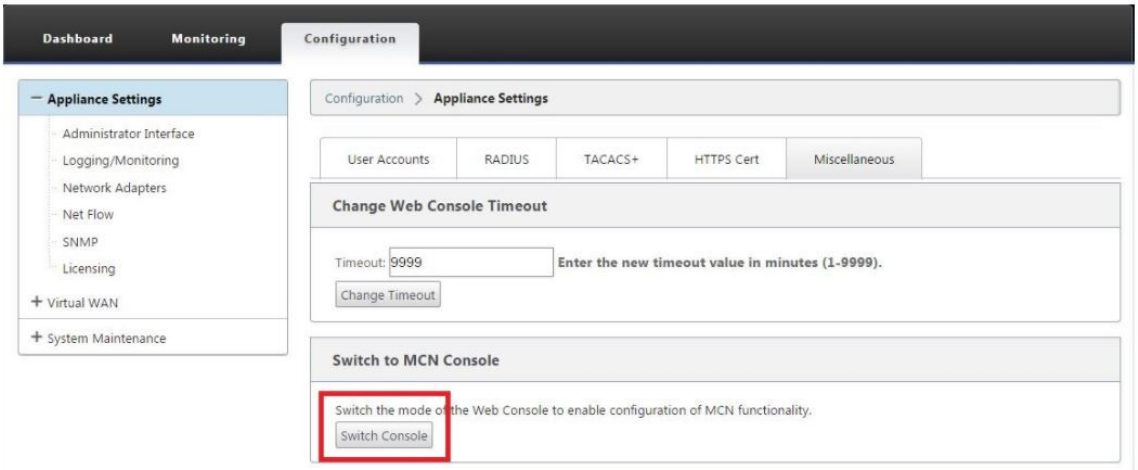
MCN 是指用作 SD-WAN 网络以及客户端节点的中央管理点的控制器的中心节点。所有配置活动、固件包的准备及其分发到客户端，都在 MCN 上进行配置。此外，监视信息仅在 MCN 上可用。MCN 可以监视整个 SD-WAN 网络，而客户端节点只能监视本地 Intranet 以及其所连接的客户端的某些信息。MCN 的主要用途是建立覆盖连接（虚拟路径），其包含一个或多个位于 SD-WAN 网络中的一个或多个客户端节点，用于实现企业站点到站点之间的通信。MCN 可以管理和拥有多个客户端节点的虚拟路径。可以有多个 MCN，但在任意给定时间只能激活一个。下图说明了一个小型两站点网络的 MCN 和客户端（分支节点）设备的基本示意图。

将 **SD-WAN** 设备配置为 **MCN**

要添加并配置 MCN，必须先在要指定为 MCN 的设备上登录到管理 Web 界面，然后将管理 Web 界面切换到 MCN 控制台模式。MCN 控制台 模式允许访问当前连接的管理 Web 界面中的配置编辑器。然后，您可以使用 配置编辑器 添加和配置 MCN 站点。

要将管理 Web 界面切换到 MCN 控制台 模式，请执行以下操作：

1. 在要配置为 MCN 的设备上登录到 SD-WAN 管理 Web 界面。
2. 在管理 Web 界面主屏幕（页面顶部的蓝色栏）的主菜单栏中单击 配置。
3. 在导航树（左窗格）中，打开设备设置分支，然后单击管理员界面。
4. 选择“其 他”选项 卡。此时将打开其他管理设置页面。



在杂项选项卡页面底部，切换到 **[客户端，MCN]** 控制台部分。本节包含切换控制台按钮，用于在设备控制台模式之间切换。

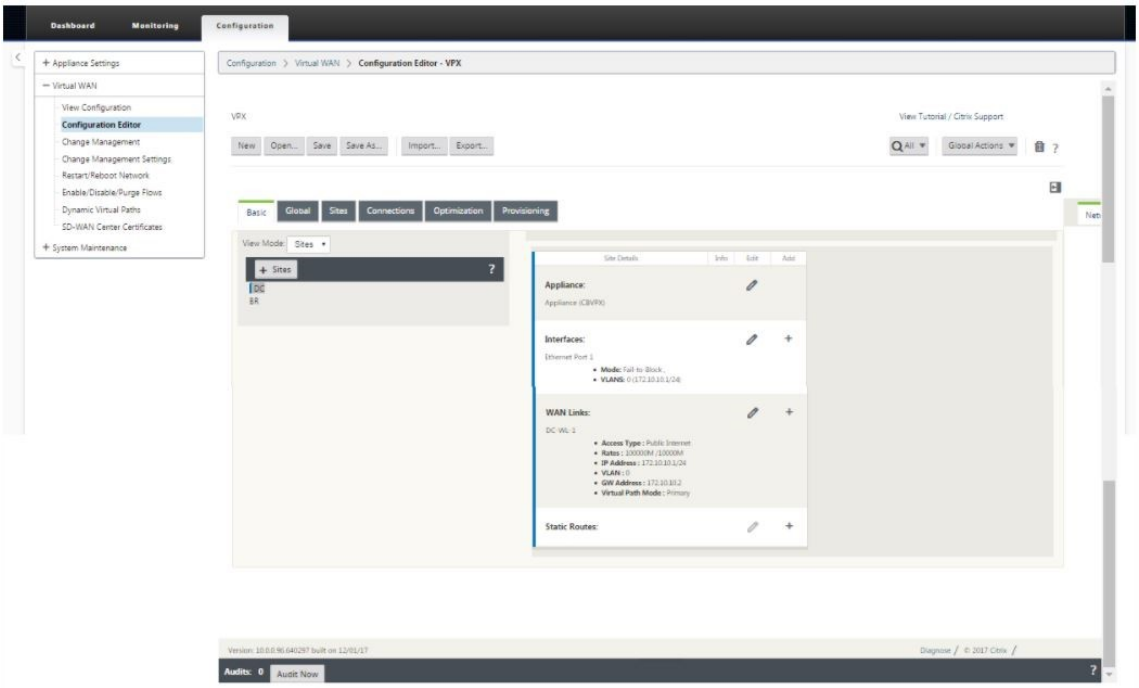
节标题指示当前控制台模式，如下所示：

- 处于 客户端控制台 模式（默认）时，部分标题为“切换到 MCN 控制台”。
- 处于 MCN 控制台 模式时，部分标题为“切换到客户端控制台”。

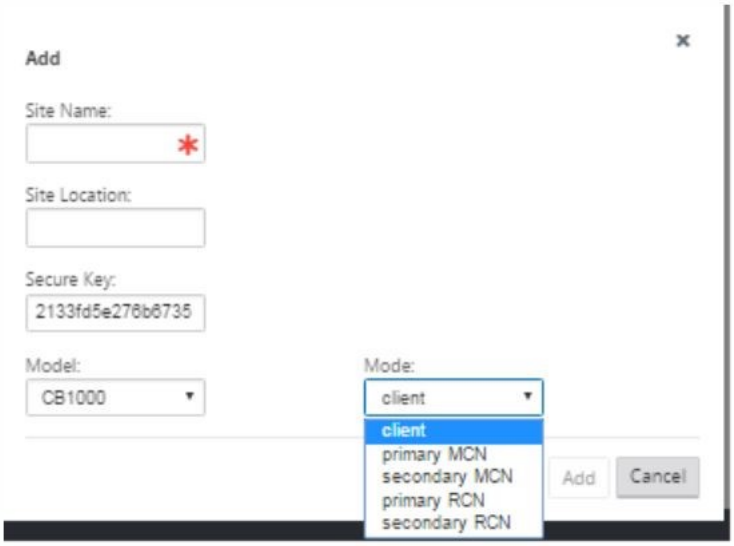
默认情况下，新设备在客户端控制台模式下显示。MCN 控制台模式在导航树结构中启用“配置编辑器”视图。配置编辑器 仅在 MCN 设备上可用。

配置 **MCN**　要添加和开始配置 MCN 设备站点，请执行以下操作：

1. 在 SD-WAN 设备 GUI 中，导航到虚拟 **WAN** > 配置编辑器。

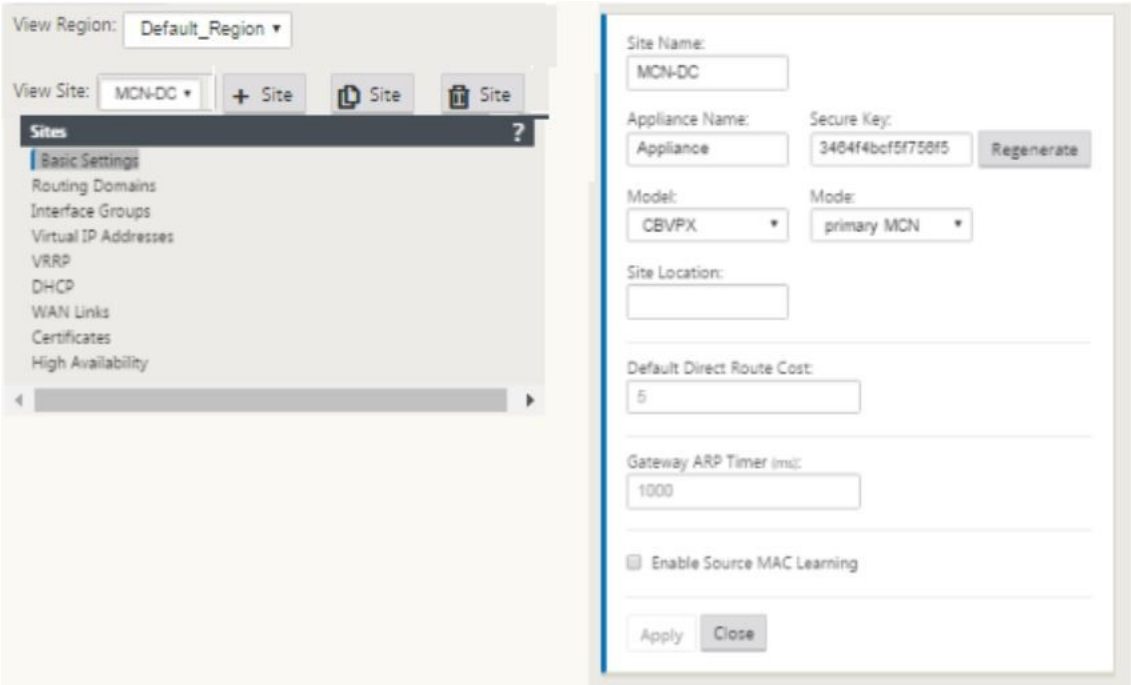


2. 单击“站点”栏中的 **+** 站点以开始添加和配置 MCN 站点。此时将显示添加站点对话框。

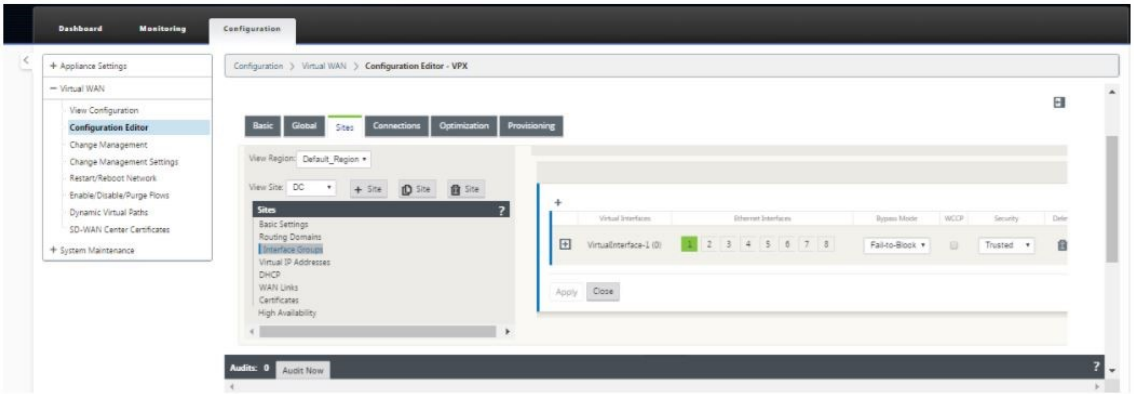


3. 输入一个站点名称，用于确定设备的地理位置和角色（DC/辅助 DC）。选择正确的设备型号。选择正确的设备是非常重要的，因为硬件平台在处理能力和许可方面互不相同。由于我们将此设备配置为主头端设备，请选择模式作为主 MCN，然后单击添加。

4. 这样会将新站点添加到站点树，默认视图将显示基本设置配置页面，如下所示：

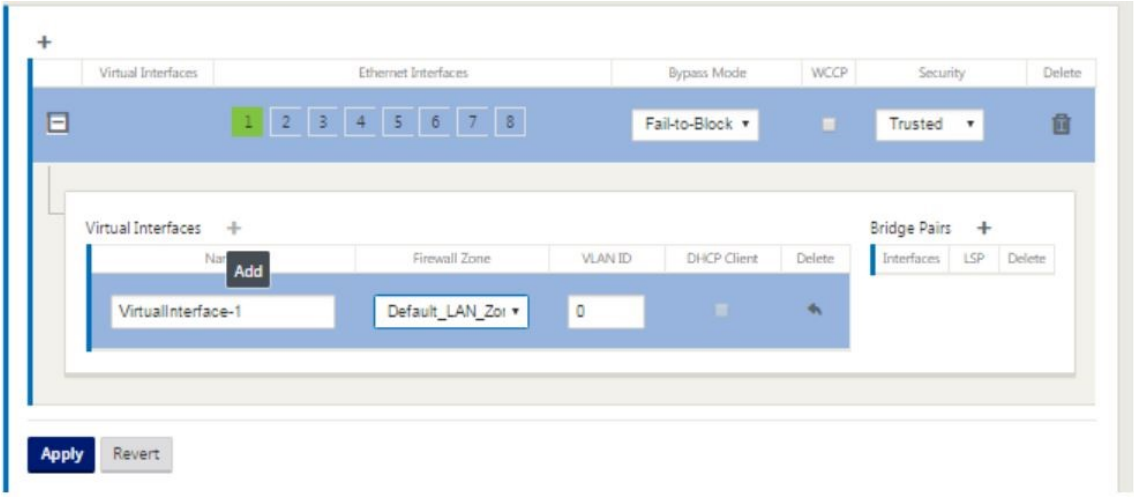


5. 输入基本设置，例如位置、站点名称。
6. 对设备进行配置，使其能够接受来自 Internet/MPLS/宽带的流量。定义链接终止的接口。这取决于设备处于叠加模式还是底层模式。
7. 单击接口组开始定义接口。



8. 单击 + 添加虚拟接口组。这将添加一个新的虚拟接口组。虚拟接口的数量取决于您希望设备处理的链接。设备可以处理的链接数因设备型号而异，最大链接数最多可以有八个。

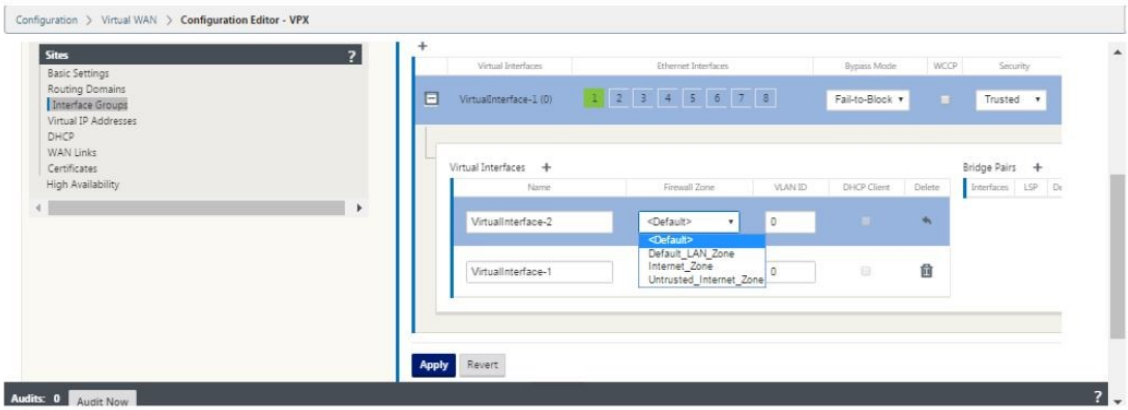
9. 单击虚拟接口右侧的 +，以按如下所示查看屏幕。



10. 选择构成此虚拟接口一部分的以太网接口。设备具有预配置的一对故障的故障到网络界面，具体取决于平台型号。如果要在设备上启用故障-有线，请确保选择正确的接口对，并确保在旁路模式列下选择“故障切换”。

11. 从下拉列表中选择安全级别。如果接口为在各接口上使用 Internet 链接，则选择“可信模式”（如果接口为“MPLS 链路”提供），将选择不受信任。

12. 在名为虚拟接口的标签右侧，单击 +。这将显示名称、防火墙区域和 VLAN ID。输入此虚拟接口组的名称和 **VLAN ID**。VLAN ID 用来识别进出虚拟接口的流量，并将其标记为从虚拟接口，对本机/未加标签的流量使用 0 (零)。



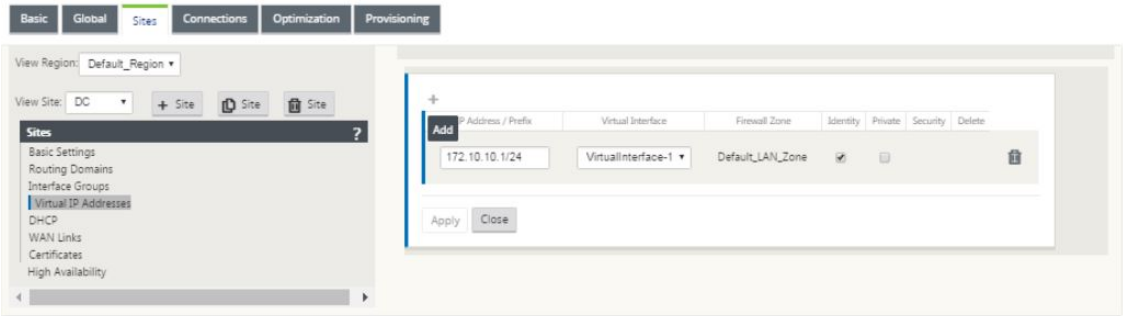
13. 要将接口配置为无法连接，请单击 Bridge 对。这会添加新的桥接对，并允许进行编辑。单击应用以确认这些设

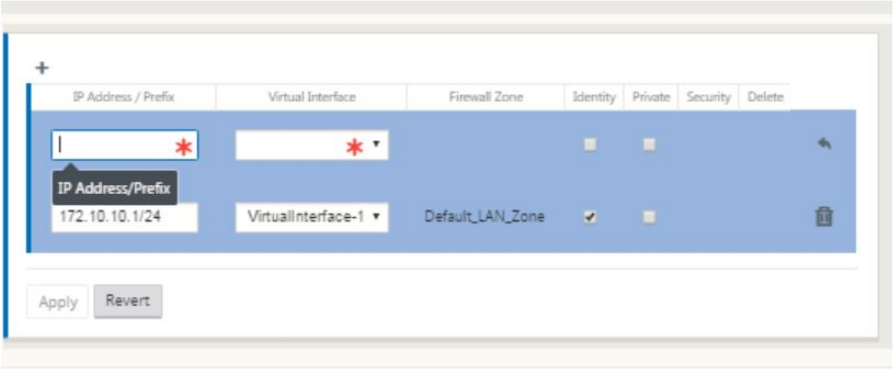
置。

14. 要添加更多虚拟接口组，请单击接口组分支右侧的 +，然后按如上所述操作。

15. 选择这些接口后，下一步是在这些接口上配置 IP 地址。在 Citrix SD-WAN 术语中，这称为 VIP（虚拟 IP）。

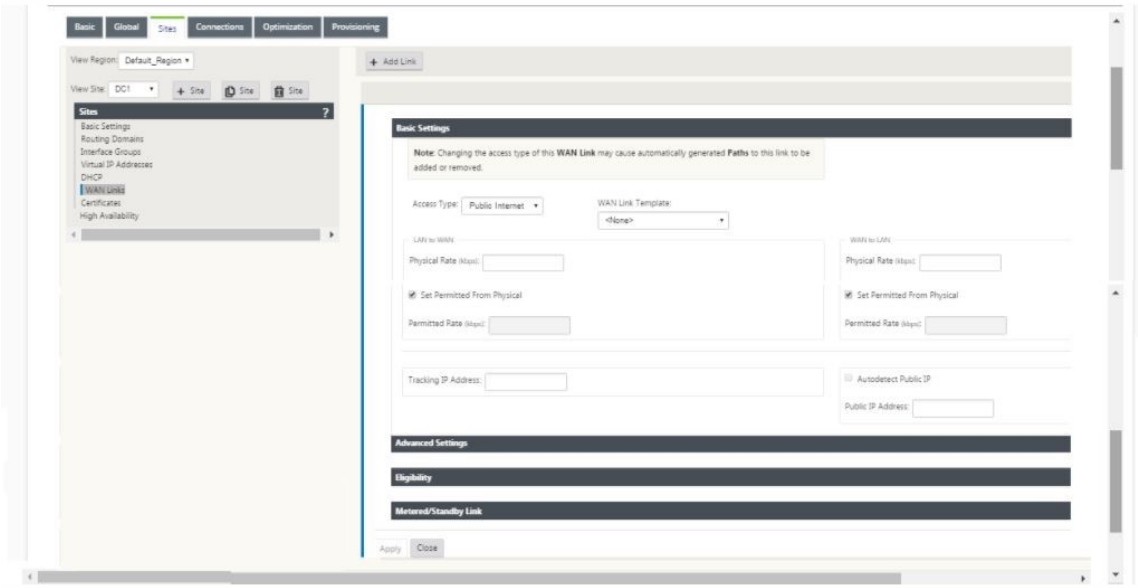
16. 继续在站点视图中，然后单击虚拟 IP 地址以查看用于配置 VIP 的接口。



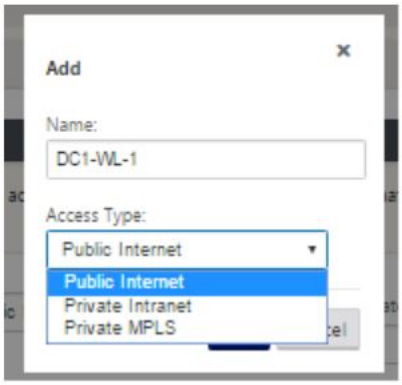


17. 输入 IP 地址/前缀信息，然后选择与该地址关联的虚拟接口。虚拟 IP 地址必须包含完整的主机地址和网络掩码。为虚拟 IP 地址选择所需的设置，例如防火墙区域、身份、专用和安全性。单击应用。这会将地址信息添加到站点中，并将其包含在站点 虚拟 IP 地址 表中。要添加更多虚拟 IP 地址，请单击 虚拟 IP 地址 右侧的 +，然后按照上述步骤继续操作。

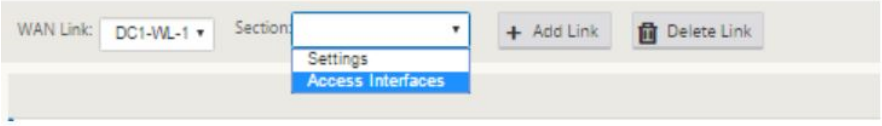
18. 继续在站点部分为站点配置 WAN 链接。

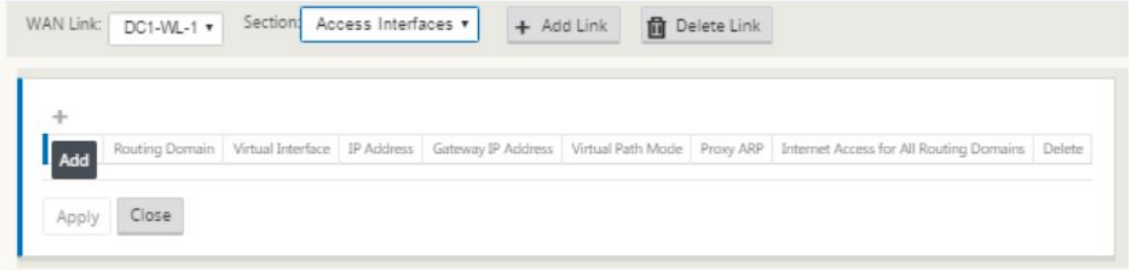


19. 在右侧面板的顶部，单击添加链接。此时将打开一个对话框，您可以在此对话框中选择要配置的链接类型。



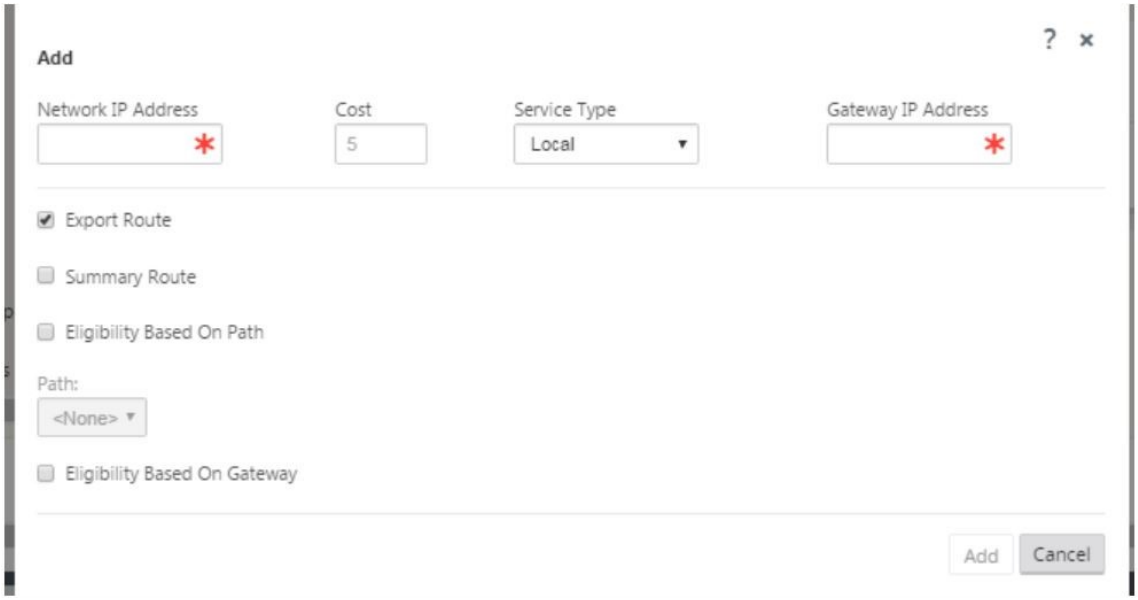
20. 公用 Internet 适用于 Internet/宽带/DSL/ADSL 链接，而专用 MPLS 则用于 MPLS 链路。私人内联网也用于 MPLS 链接。私有 MPLS 和私有内联网链接之间的区别在于，私有 MPLS 允许保留 MPLS 链路的 QoS 策略。
21. 如果您选择“公用 Internet”，并且通过 DHCP 分配 IP，请选择“自动检测 IP”选项。
22. 在 WAN 链接配置页面中，选择访问接口。这将打开站点的访问接口视图。添加并配置每个链接对应的 VIP 和网关 IP，如下所示。





23. 单击 **+** 以添加界面。这会向表格中添加一个空条目，并将其打开以进行编辑。
24. 输入要分配给此接口的名称。您可以根据链接类型和位置选择命名它。如果不希望将网络隔离，并为接口分配 IP，请将路由域保留为默认值。
25. 如果链接是互联网链接或私有 IP（如果链接是 MPLS 链接），请确保提供可公开访问的网关 IP 地址。将虚拟路径模式保持为主要模式，因为您需要使用此链接形成虚拟路径。

    注意：启用代理 ARP 时，当网关无法访问时，设备会回复网关 IP 地址的 ARP 请求。
26. 单击应用完成 WAN 链接的配置。如果要配置更多 WAN 链接，请对其他链接重复执行这些步骤。
27. 配置站点的路由。单击连接视图，然后选择路线。
28. 单击 + 以添加路由，这将打开一个对话框，如下所示。



29. 输入适用于新路由的以下信息：
    - 网络 IP 地址

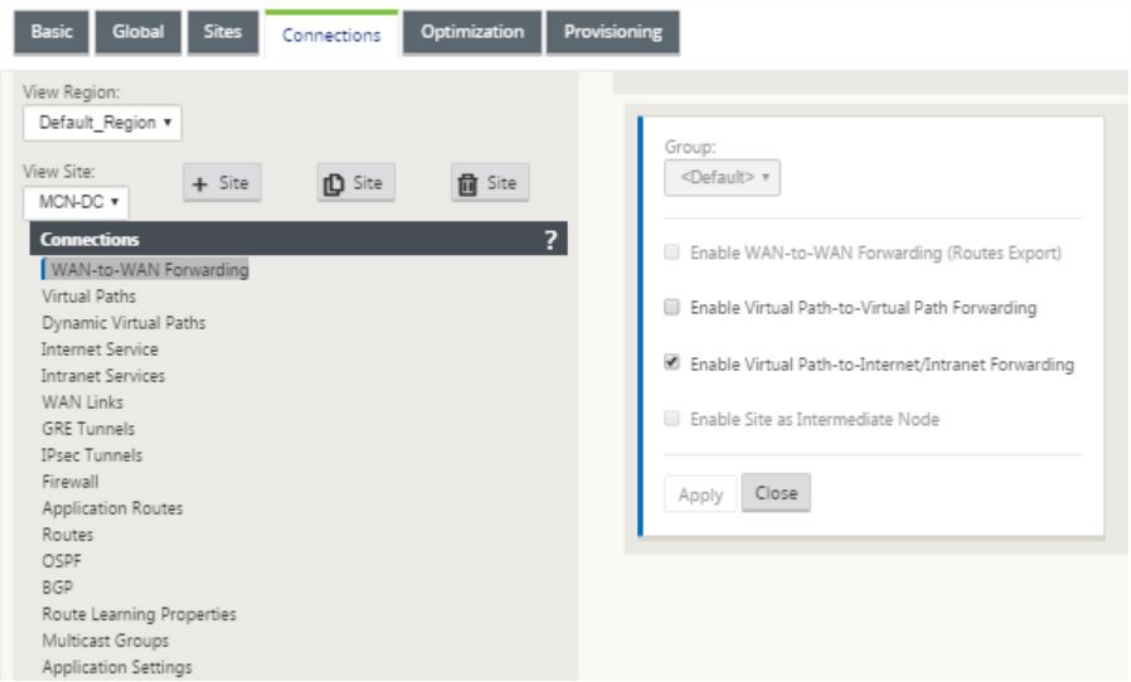
- 成本—成本决定哪条路线优先于另一条路线。成本较低的路径优先于成本较高的路线。默认值为 5。
- 服务类型 - 选择服务，一项服务可以是以下任意项：
  - 虚拟路径
  - 内联网
  - Internet
  - 直通
  - 本地
  - GRE 隧道
  - 局域网 IPsec 隧道

30. 单击应用。

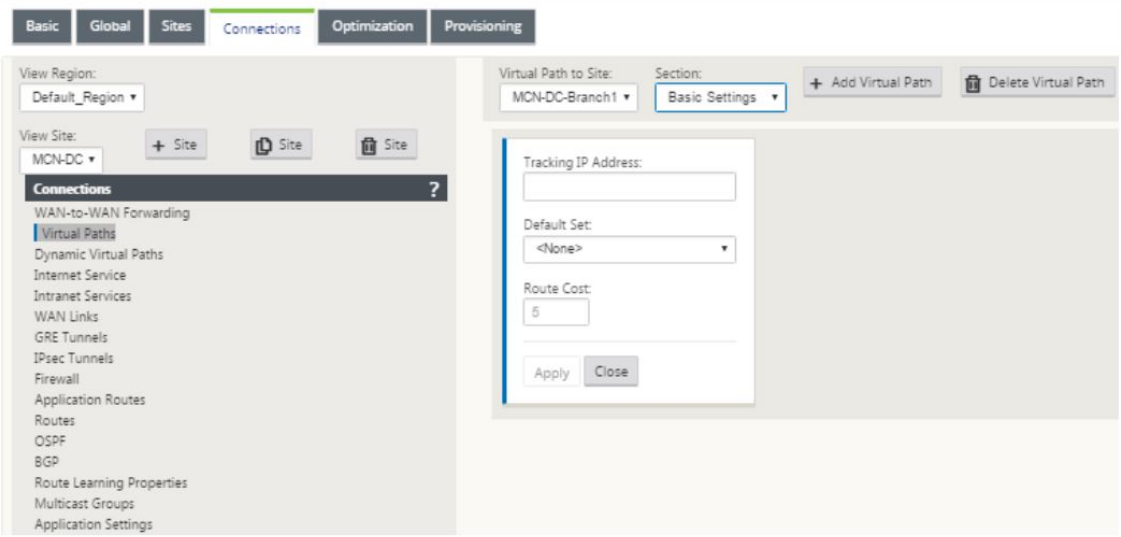
要为站点添加更多路由，请单击“路由”分支右侧的 +，然后按照上面的方式进行操作。有关更多信息，请参阅 配置 MCN。

配置 **MCN** 和分支站点之间的虚拟路径　在 MCN 和分支节点之间建立连接。您可以通过在这两个站点之间配置虚拟路径来实现此目的。导航到配置编辑器配置树中的连接选项卡。

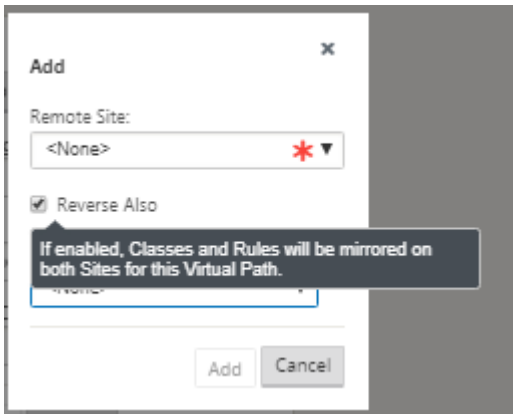
1. 在“配置”部分中，单击连接选项卡。这将显示配置树的连接部分。
2. 在连接部分页面中，从“查看站点”下拉菜单中选择 **MCN**。



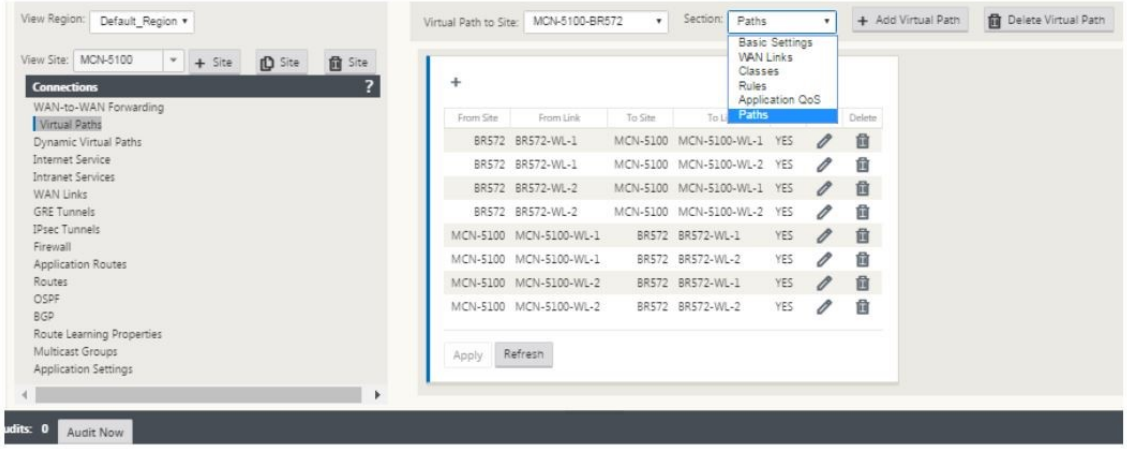
3. 从连接选项卡中选择虚拟路径，以在 MCN 和分支站点之间创建虚拟路径。



4. 在“虚拟路径”部分中，单击静态虚拟路径名称旁边的添加虚拟路径。此时将打开一个对话框，如下所示。选择要为其配置虚拟路径的分支。必须在名为远程站点的标签下进行配置。从此下拉列表中选择分支节点，然后单击同时反向复选框。



在虚拟路径的两个站点上镜像流量分类和转向。完成此操作后，请从名为“节”下的下拉菜单中选择路径，如下所示。



5. 在路径表格上方单击 **+** 添加，将显示“添加路径”对话框。指定必须在其中配置虚拟路径的端点。现在，单击添加以创建路径，然后单击反转复选框。

   注意：Citrix SD-WAN 在两个方向上测量链接质量。这意味着点 A 到点 B 是一条路径，点 B 到点 A 是另一个路径。通过单向度量链路条件的帮助，SD-WAN 可以选择发送流量的最佳路由。这与诸如 RTT 之类的度量值不同，后者是用来度量延迟的双向指标。例如，点 A 与点 B 之间的一个连接显示为两条路径，每个连接都分别计算链路性能指标。

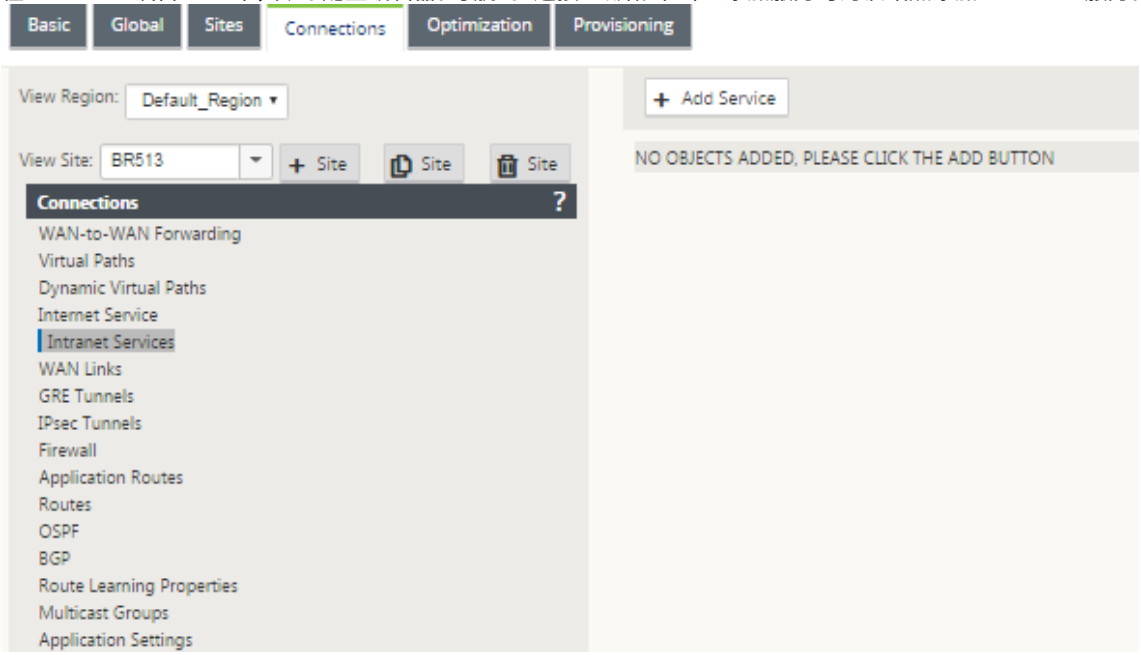
此设置足够用来将虚拟路径置于 MCN 与分支之间，其他配置选项也可用。有关详细信息，请参阅 在 MCN 和客户端站点之间配置虚拟路径服务。

部署 **MCN** 配置　下一步是部署配置。这包括以下两个步骤：

1. 将 SD-WAN 配置包导出到更改管理。
   - 在生成设备包之前，必须首先将完成的配置包从配 置编辑器 导出到 MCN 上的全局 变更管理 暂存收件箱。请参阅 执行变更管理一节中提供的步骤。
2. 生成并暂存设备软件包。
   - 将新配置包添加到更改管理收件箱后，可以在分支站点上生成并暂存设备包。要执行此操作，请使用 MCN 上的管理 Web 界面中的更改管理向导。请参阅 Stage 设备包一节中提供的步骤。

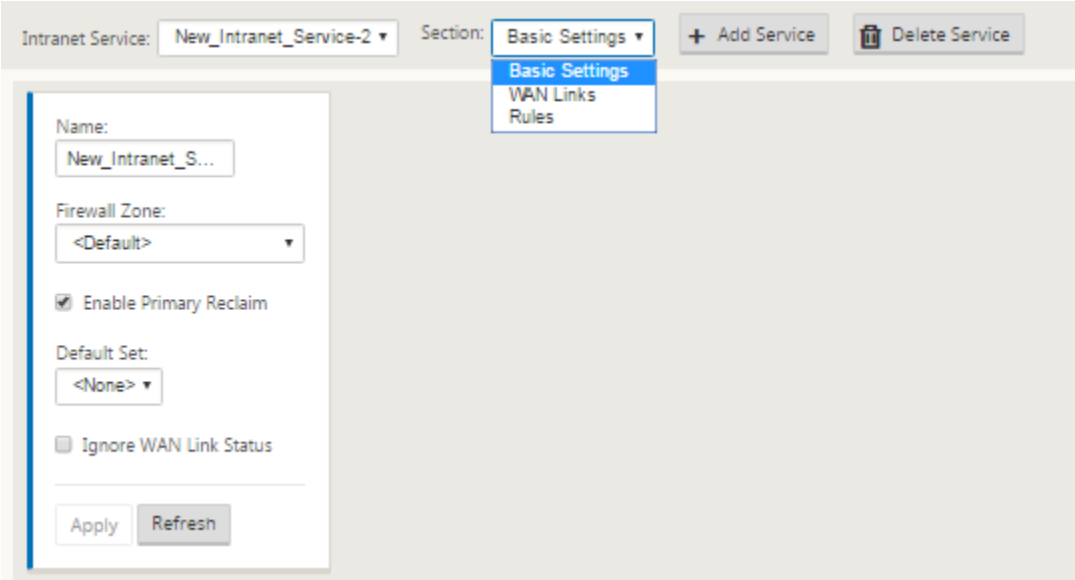
配置 **Intranet** 服务以连接 **Azure WAN** 资源

1. 在 SD-WAN 设备 GUI 中，转到 配置编辑器。导航到“连接”磁贴。单击 **+** 添加服务可为该站点添加 Intranet 服务。



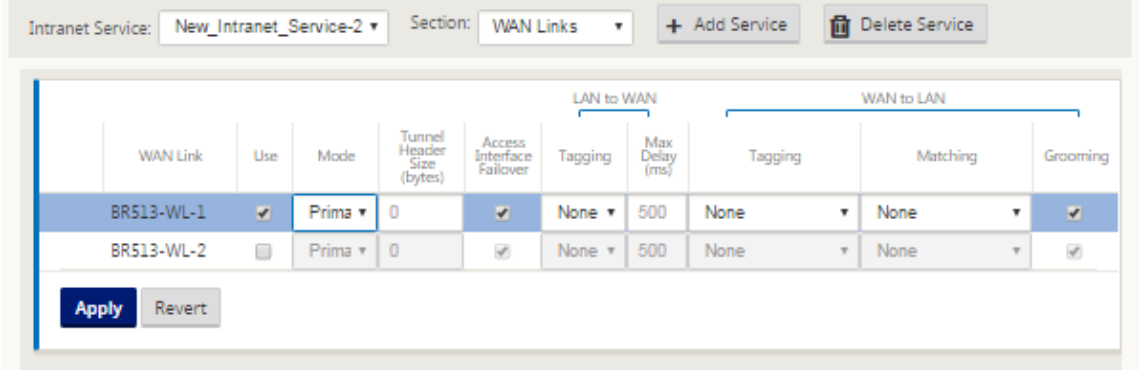
2. 在 Intranet 服务的基本设置中，您希望 Intranet 服务在 WAN 链接不可用期间的行为方式有几个选项。

- 启用主回收–如果希望选定的主链路在故障转移后接管，请选中此复选框。如果您选择不选中此选项，则辅助链路将继续发送流量。
- 忽略 **WAN** 链接状态 - 如果此选项处于启用状态，则发送给此 Intranet 服务的数据包将继续使用此服务，即使构成的 WAN 链接不可用也是如此。

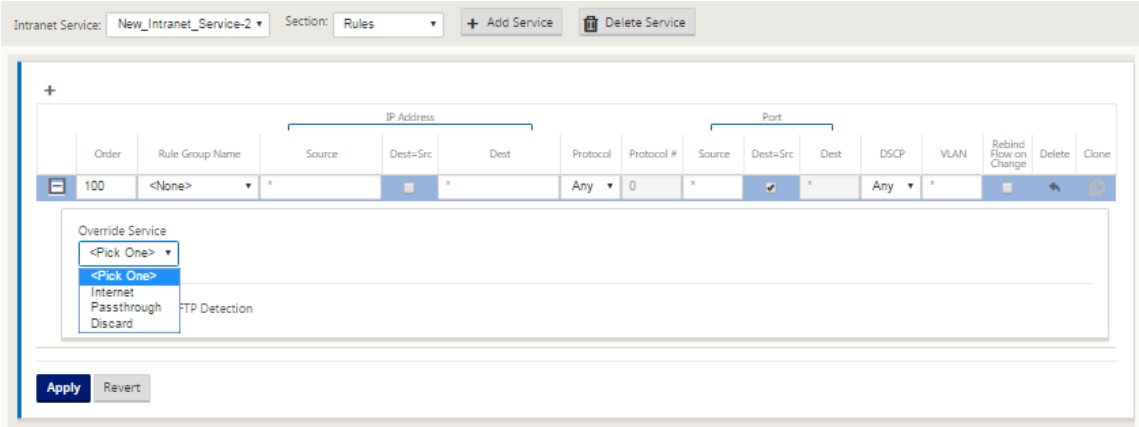


3. 配置基本设置后，下一步是为此服务选择组成 WAN 链接。一项内联网服务最多可选择两个链接。要选择 WAN 链接，请从标有“部分”的下拉列表中选择 WAN 链接选项。WAN link 功能在主模式和辅助模式下，只有一个链路被选为主要 WAN 链接。

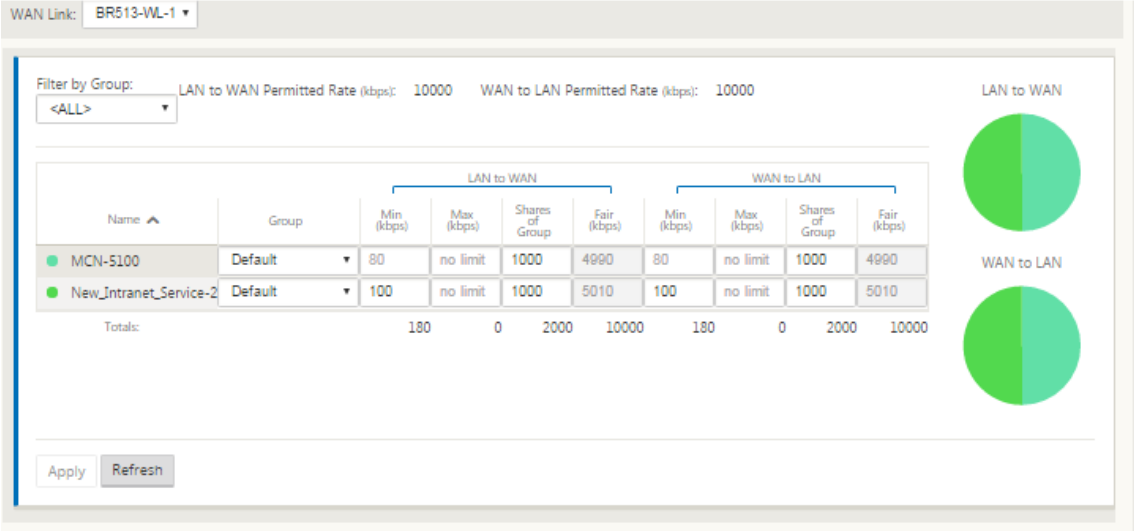
   注意：创建第二个 Intranet 服务时，必须具有主和辅助 WAN 链接映射。



4. 可以使用特定于分支站点的规则，从而使每个分支站点的自定义功能唯一覆盖在全局默认集中配置的任何常规设置。模式包括基于特定 WAN 链接的所需交付，或者用作覆盖服务，允许您经过过滤或放弃过滤的流量。例如，如果存在一些流量，即不希望通过 Intranet 服务，则可以编写一条规则，以丢弃该流量或通过其他服务（Internet 或直通）发送。

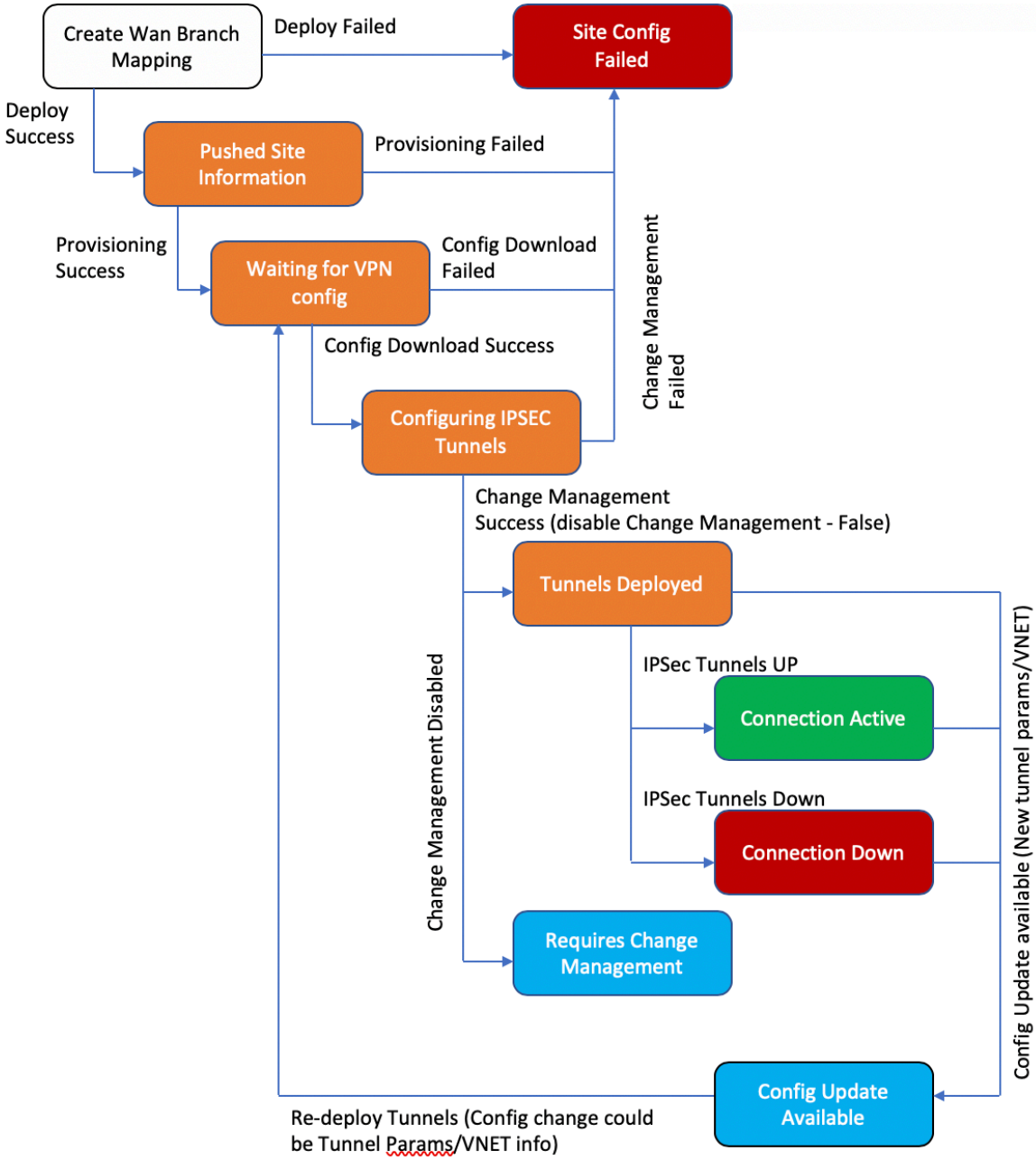


5. 如果为站点启用了 Intranet Service，则可以使用 Provisi **oning** 磁贴以允许在使用 WAN 链接的各种服务之间双向（LAN 到 WAN /WAN 到 LAN）分配 WAN 链路的带宽。服务部分允许您进一步微调带宽分配。此外，还可以启用公平共享，以允许服务在进行公平分发之前接收最低的保留带宽。



配置 **SD-WAN Center**

下图描述了 SD-WAN Center 和 Azure 虚拟 WAN 连接的高级工作流程以及部署的相应状态转换。



配置 **Azure** 设置：

- 提供 Azure 租户 ID、应用程序 ID、密钥和订阅 ID（也称为服务主体）。

将分支站点配置为 **WAN** 关联：

- 将分支站点关联到 WAN 资源。同一站点无法连接到多个 WAN。
- 单击新建以配置站点 WAN 关联。
- 选择 **Azure WAN** 资源。
- 选择要与 WAN 资源关联的站点名称。
- 单击部署以确认关联。用于隧道部署的 WAN 链接会自动填充具有最佳链接容量的 WAN 链接。
- 等待状态更改为“已部署隧道”以查看 **IPsec** 隧道 设置。
- 使用 SD-WAN Center 报告视图检查相应 IPsec 隧道的状态。IPsec 隧道状态应为绿色，以便数据流量流动，表示连接处于活动状态。

预配 **SD-WAN Center**：

SD-WAN Center 是用于 Citrix SD-WAN 的管理和报告工具。虚拟 WAN 的必需配置是在 SD-WAN Center 中执行的。SD-WAN Center 仅作为虚拟外形规格 (VPX) 提供，需要安装在 VMware ESXi 或 XenServer 虚拟机管理程序上。配置 SD-WAN Center 设备所需的最少资源包括 8 GB RAM 和 4 个 CPU 内核。以下是 安装 和 配置 SD-WAN 中心虚拟机的步骤。

为 **Azure** 连接配置 **SD-WAN Center**

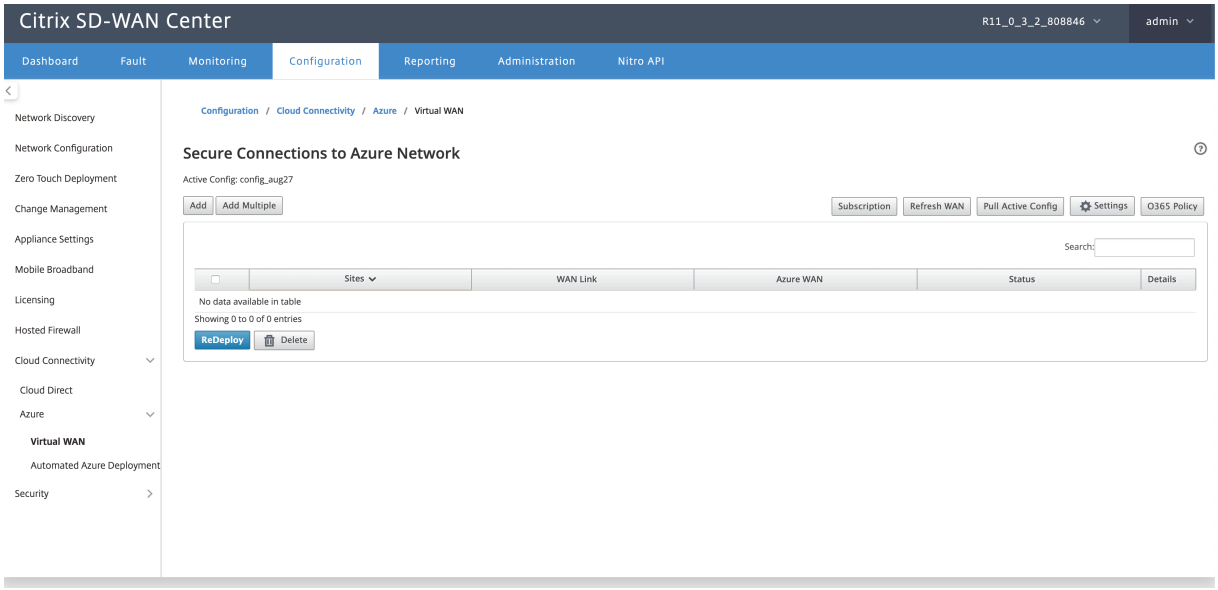
有关详细信息 ，请阅读创建服务主体 。

要成功通过 Azure 向 SD-WAN center 进行身份验证，应使用以下参数：

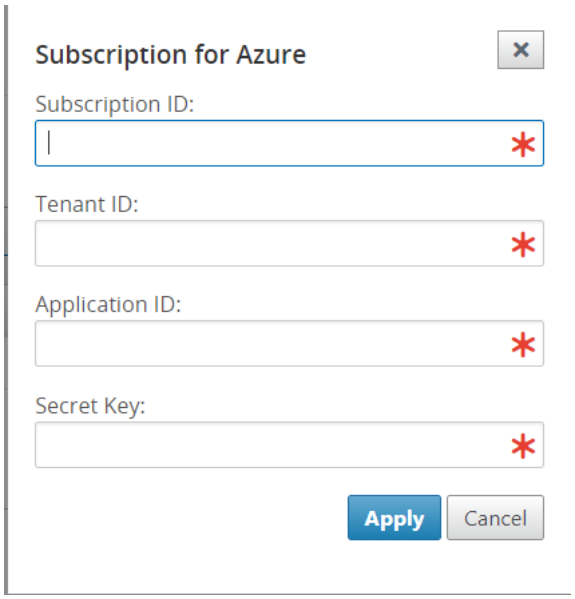
- 目录（租户 ID）
- 应用程序（客户端 ID）
- 安全密钥（客户端密钥）
- 订阅者 ID

对 **SD-WAN Center** 进行身份验证：

在 SD-WAN Center UI 中，导航到配置 > 云连接 > **Azure** > 虚拟广域网。配置 Azure 连接设置。有关配置 Azure VPN 连接的详细信息，请参阅以下链接：
Azure Resource Manager。



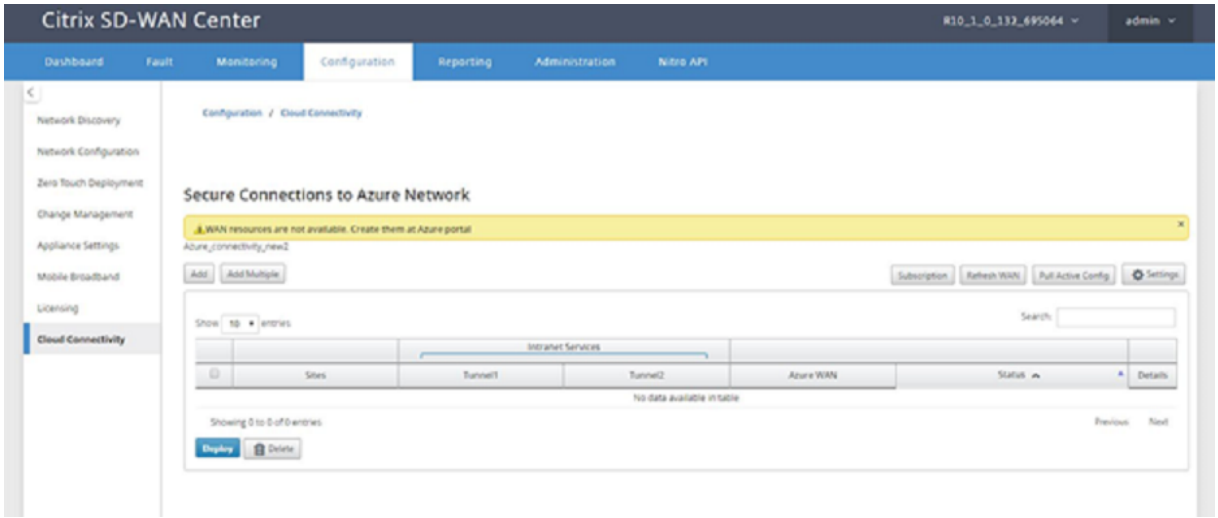
输入订阅 **ID**、租户 **ID**、应用程序 **ID** 和安全密钥。需要执行此步骤才能使用 Azure 对 SD-WAN Center 进行身份验证。如果在上面输入的凭据不正确，则身份验证将失败，并且不允许执行进一步操作。单击应用。



存储帐户字段引用您在 Azure 中创建的存储帐户。如果未创建存储帐户，单击应用后，将在您的订阅中自动创建一个新存储帐户。

获取 **Azure** 虚拟 **WAN** 资源：

成功完成身份验证后，Citrix SD-WAN 轮询 Azure 以获取 Azure 虚拟 WAN 资源的列表，在登录 Azure 门户后的第一个步骤中创建这些资源。WAN 资源代表您在 Azure 中的整个网络。它包含指向您希望在此广域网中拥有的所有中心的链接。WAN 彼此相互隔离，不能包含公用集线器，也不能包含不同 WAN 资源中的两个不同中枢之间的连接。



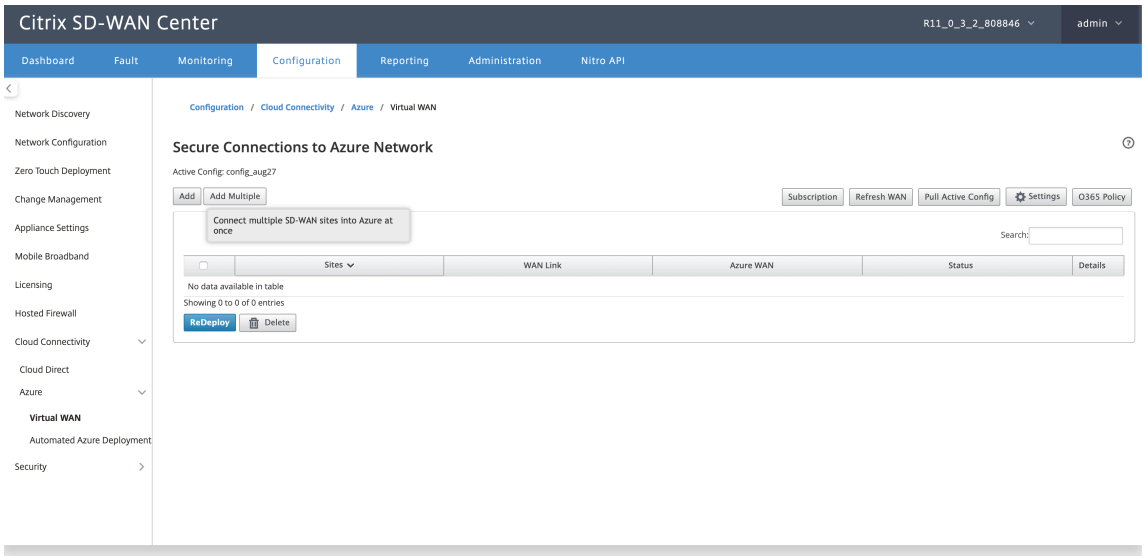
要关联分支站点和 Azure WAN 资源，请执行以下操作：

分支站点需要与 Azure WAN 资源相关联才能建立 IPsec 隧道。一个分支可以连接到一个 Azure 虚拟 WAN 资源中的多个中心，一个 Azure 虚拟 WAN 资源可以连接到多个本地分支站点。为每个分支到 Azure 虚拟 WAN 资源部署创建单行。

要添加多个站点，请执行以下操作：

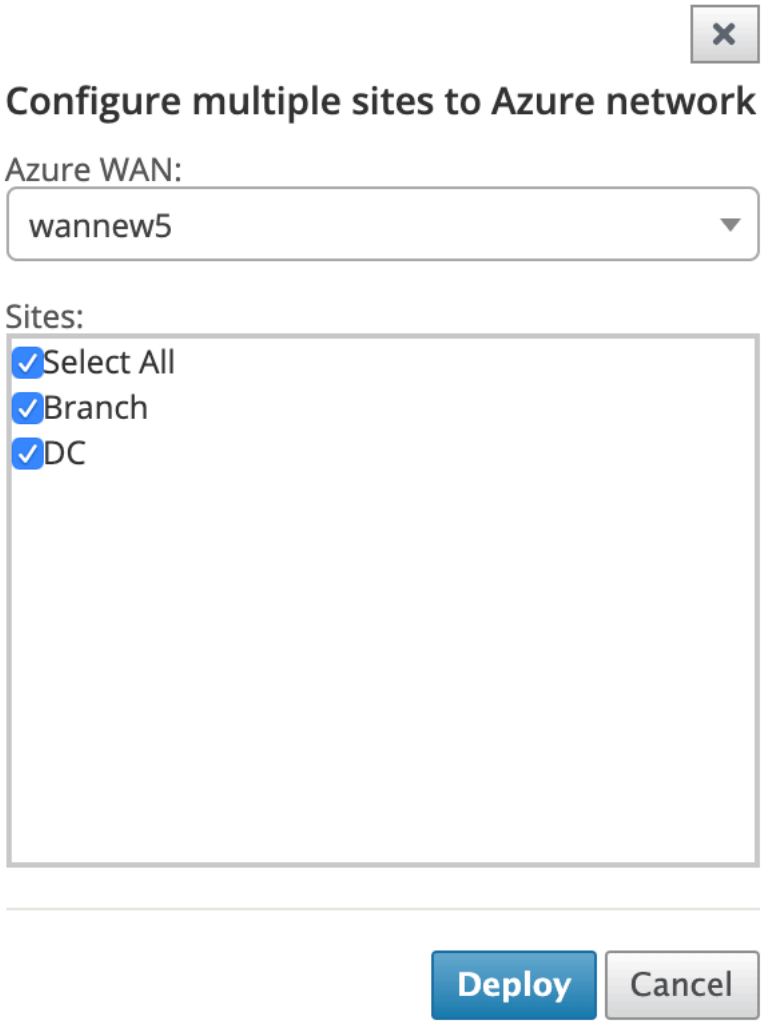
您可以选择添加所有相应的站点，然后将它们与选定的单个 WAN 资源相关联。

1. 单击添加多个以添加必须与所选 WAN 资源关联的所有站点。



2. Azure WAN 资源下拉列表（如下所示）已预先填充属于您的 Azure 帐户的资源。如果尚未创建 WAN 资源，则此列表为空，您必须导航到 Azure 门户才能创建资源。如果列表中填充了 WAN 资源，请选择您需要将分支站点连接到的 **Azure WAN** 资源。

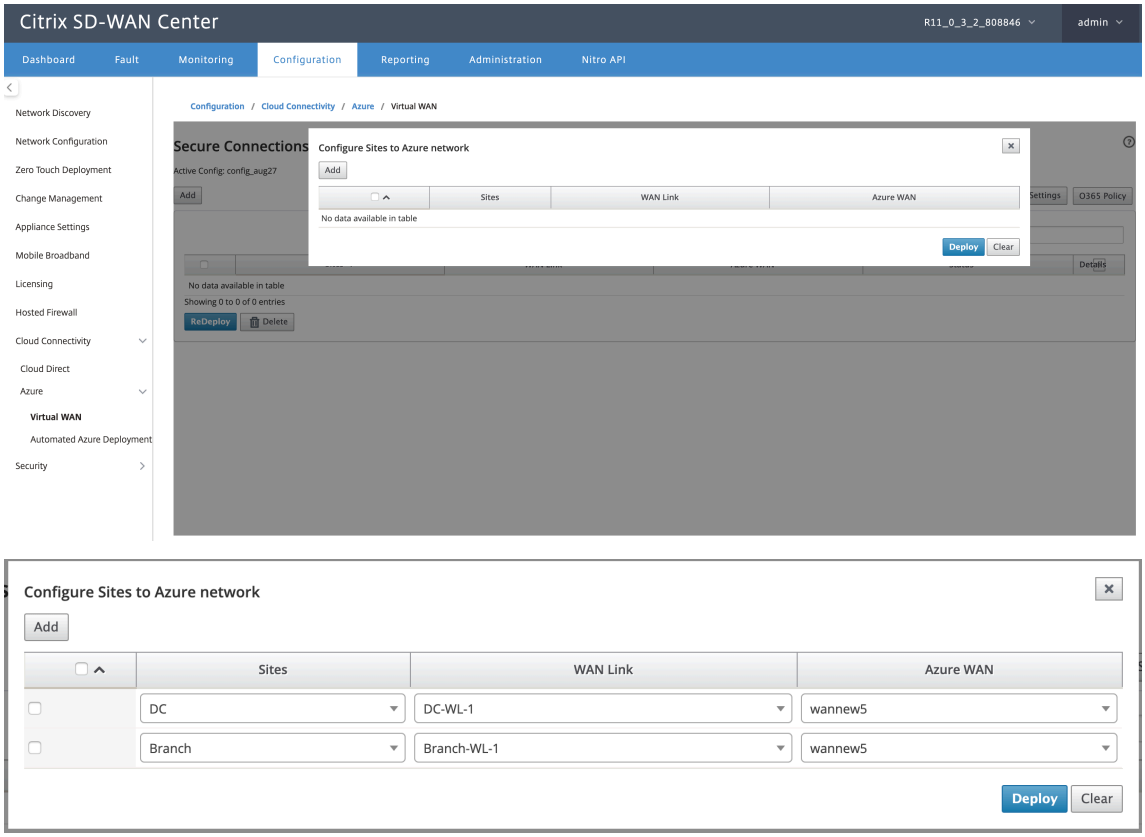
3. 选择一个或所有分支站点以启动 IPsec 隧道建立过程。自动选择站点最佳容量公共互联网 Wanlinks 来建立通往 Azure VPN 网关的 IPsec 隧道。



要添加单个站点，请执行以下操作：

您还可以选择一次性添加站点（单个），随着网络增长，或者如果正在执行站点间部署，可以选择添加多个站点（如上所述）。

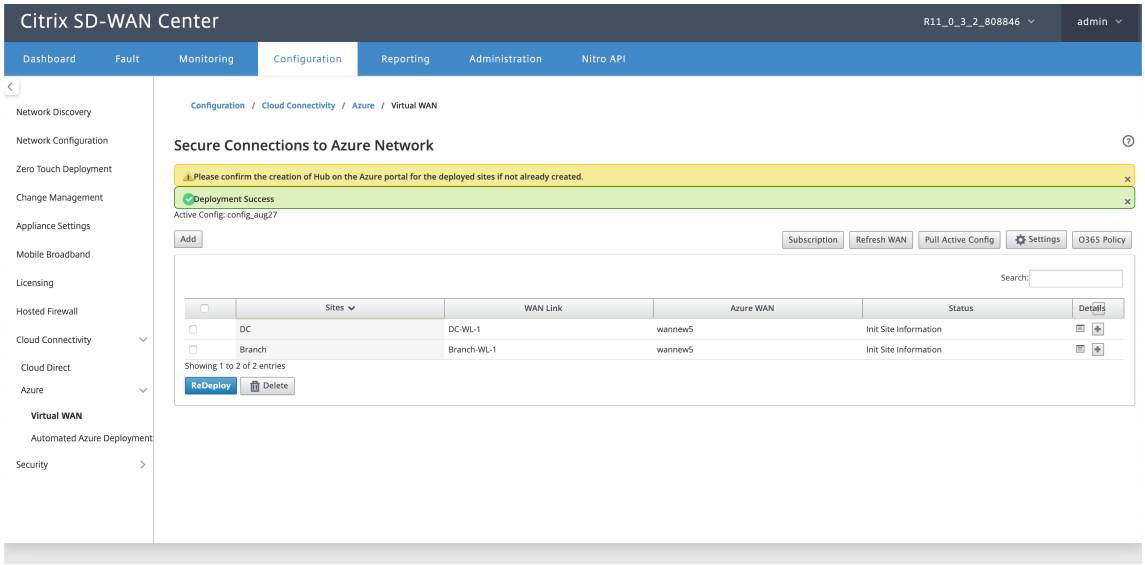
1. 单击新增为站点 WAN 关联选择一个站点名称。在“将站点配置到 **Azure** 网络”对话框中添加站点。



2. 选择要配置到 Azure 虚拟 WAN 网络的分支站点。
3. 选择与站点关联的 WAN 链接（公共互联网类型链接按最佳物理链路容量顺序列出）
4. 从 **Azure** 虚拟 **WAN** 下拉菜单中选择站点必须与之关联的 **WAN** 资源。
5. 单击部署以确认关联。状态（“初始化站点信息、已推送站点信息”和“正在等待 VPN 配置”）已更新，以通知您有关该过程的信息。

部署过程包括以下状态：

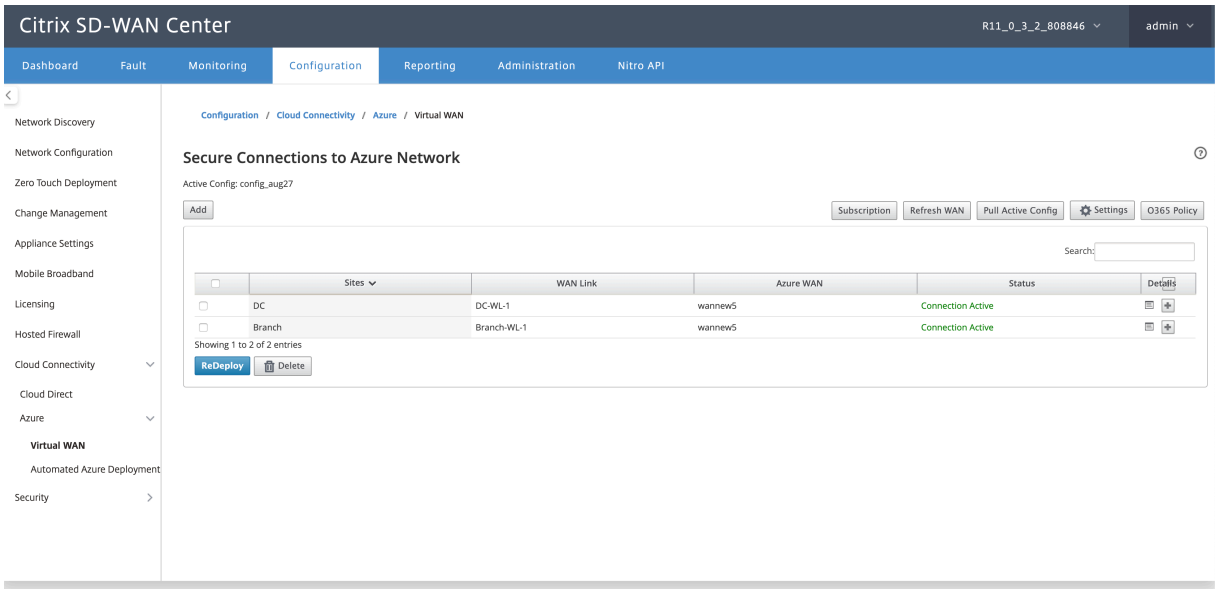
- 推送网站信息
- 等待 VPN 配置
- 已部署的隧道
- 连接处于活动状态（IPsec 通道已启动）或连接已关闭（IPsec 通道已关闭）

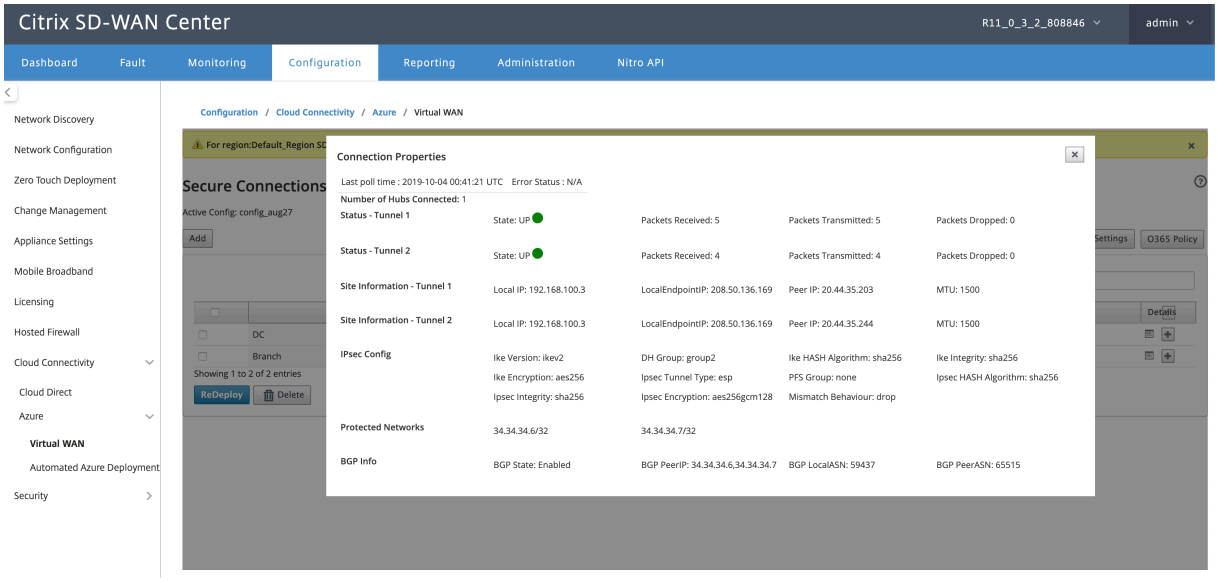


关联站点 **WAN** 资源映射（**Azure** 门户）：

将 Azure 门户上已部署的站点与在 Azure 虚拟 WAN 资源下创建的虚拟中心关联。一个或多个虚拟中心可以与分支机构站点关联。每个虚拟中心都是在特定区域创建的，并且可以通过创建虚拟网络连接将特定工作负载与虚拟中心关联。只有在分支站点到虚拟中心的关联成功后，才会下载 VPN 配置，并建立从站点到 VPN 网关的相应 IPsec 隧道。

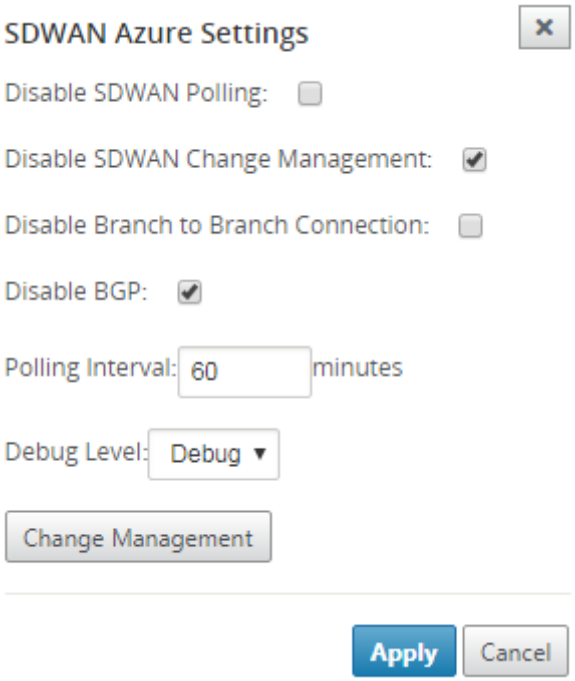
等待状态更改为已部署隧道或连接活动以查看 **IPsec** 隧道设置。查看与所选服务关联的 IPsec 设置。





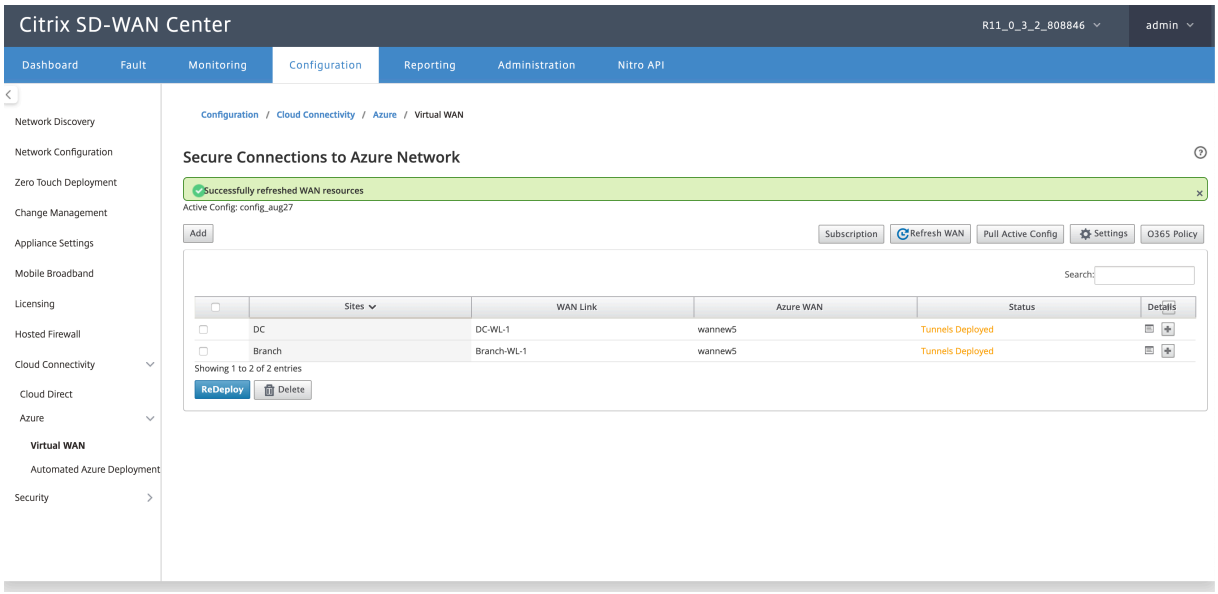
SD-WAN Azure 设置：

- 禁用 **SD-WAN** 更改管理—默认情况下，更改管理过程是自动化的。这意味着，只要可以在 Azure 虚拟 WAN 基础结构上提供新配置，SD-WAN Center 便会获得此配置，并开始将其自动应用于分支机构。但是，如果要控制何时必须将配置应用于分支，则可以控制此行为。禁用自动更改管理功能的一个优点是独立管理此功能和其他 SD-WAN 功能的配置。
- 禁用 **SDWAN** 轮询—禁用对现有部署的所有 SD-WAN Azure 新部署和轮询。
- 轮询间隔 - 轮询 间隔选项控制在 Azure 虚拟 WAN 基础结构中查找配置更新的时间间隔。建议的轮询间隔时间为 1 小时。
- 禁用分支到分支连接–禁用通过 Azure 虚拟 WAN 基础结构进行分支到分支通信。默认情况下，此选项处于禁用状态。启用此功能后，这意味着本地分支可以通过 Azure 的虚拟 WAN Infra 通过 IPsec 相互通信，也可以与分支后面的资源进行通信。这对通过 SD-WAN 虚拟路径进行分支到分支的通信没有任何影响，分支可以相互通信，并通过虚拟路径与它们各自的资源/端点通信，即使禁用此选项也是如此。
- 禁用 **BGP** —这将禁用 IP 上的 BGP，默认情况下它处于禁用状态。启用后，站点路由将通过 BGP 公布。
- 调试级别–如果存在任何连接问题，则可以启用捕获日志以进行调试。

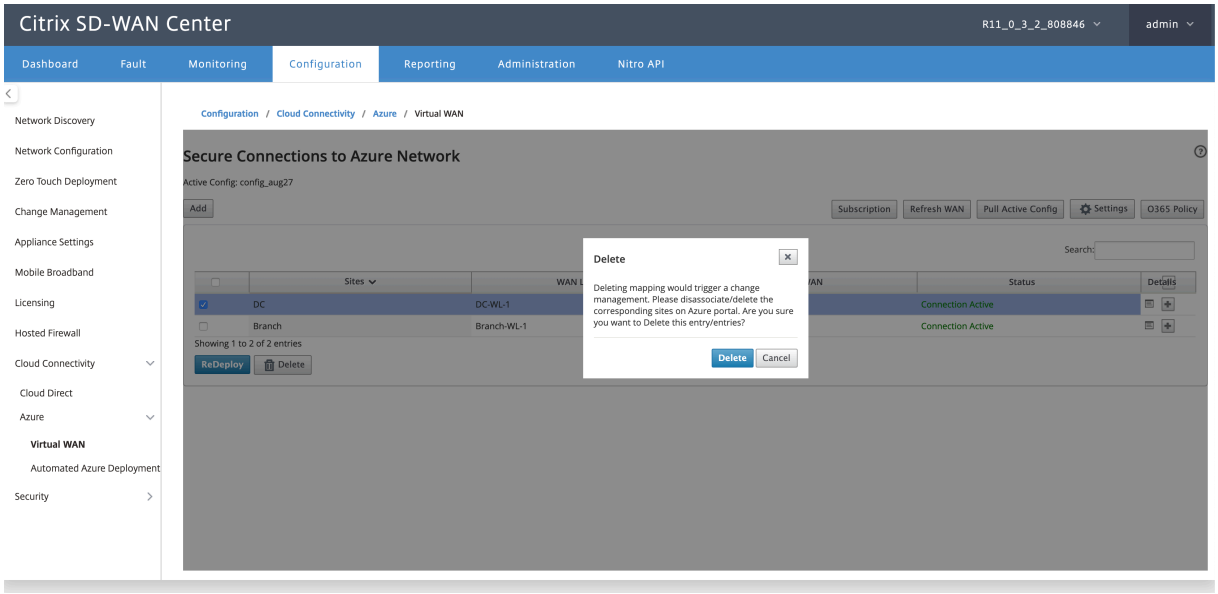


刷新 **WAN** 资源：

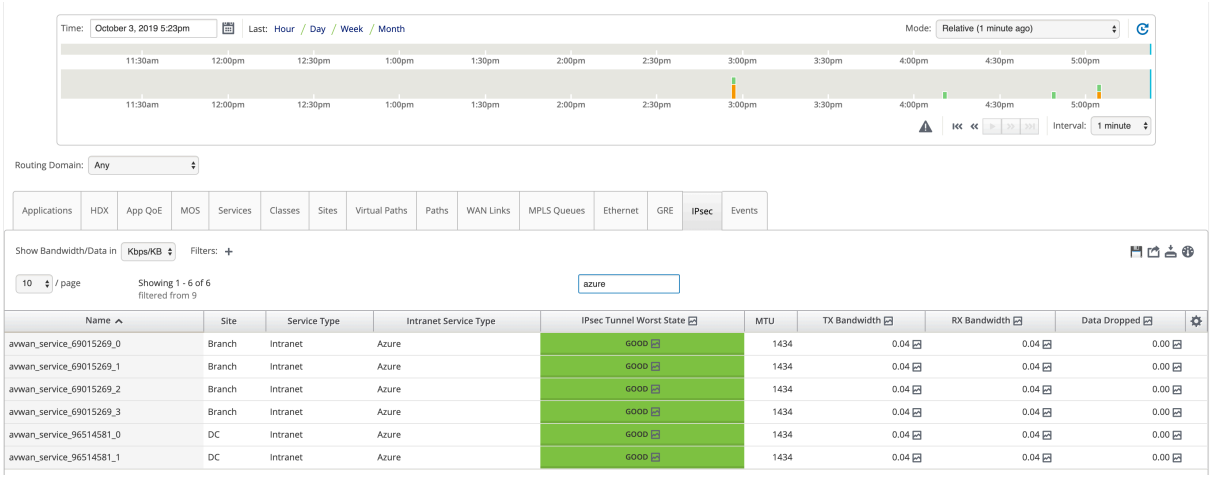
单击刷新图标可检索您在 Azure 门户上更新的最新 WAN 资源集。刷新过程完成后，将显示一条消息，指出“已成功刷新 WAN 资源”。



删除站点 **WAN** 资源关联　选择一个或多个映射以执行删除。在内部会触发 SD-WAN 设备更改管理过程，直至成功完成后，删除选项处于禁用状态，以防止进一步执行删除操作。要删除映射，需要取消关联或删除 Azure 门户中相应的站点。用户必须手动执行此操作。



监视 **IPsec** 隧道　在 SD-WAN Center 用户界面中，导航到报告 > **IPsec** 以检查 IPsec 隧道的状态。隧道状态应为绿色，数据流量才能流动。



云直接服务

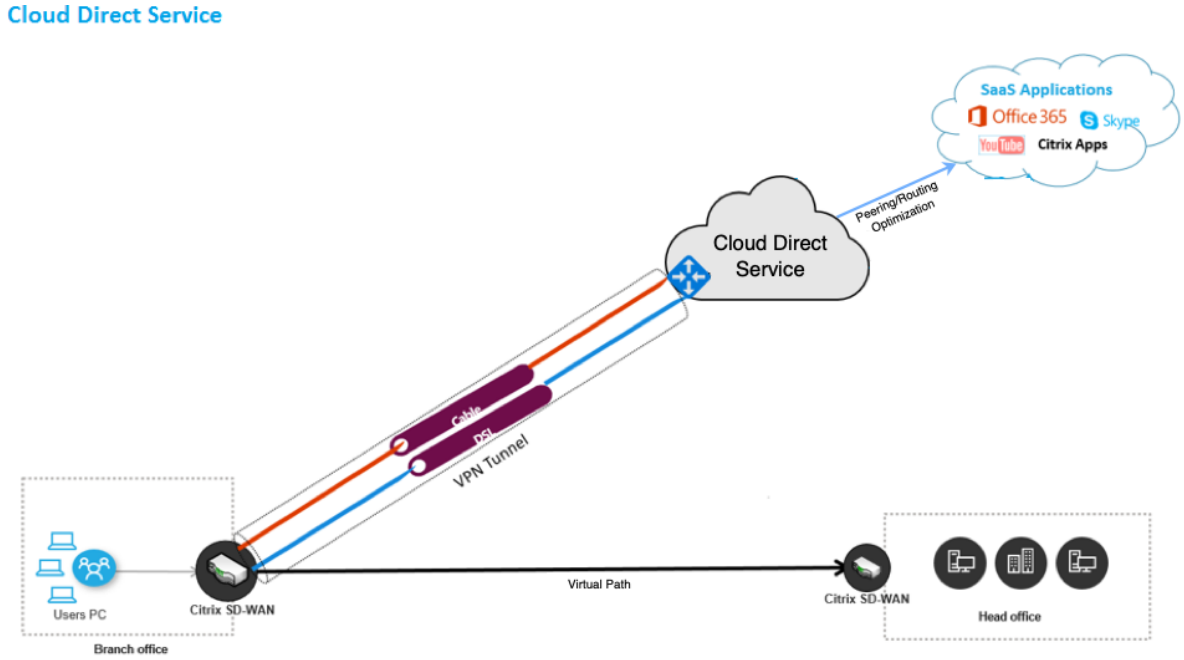
April 13, 2021

Cloud Direct 服务将 SD-WAN 作为云服务提供，无论主机环境（数据中心、云和互联网）为所有受 Internet 限制的流量提供可靠和安全的 SD-WAN 功能。它提高了网络可见性和管理。通过此软件，合作伙伴可以为业务关键型 SaaS 应用程序为其最终客户提供托管 SD 服务。

Cloud Direct 服务具有以下优势：

- 冗余 -使用多个 Internet WAN 链路并提供无缝故障切换。
- 链路聚合 -同时使用所有互联网 WAN 链接。
- 跨不同提供商的 WAN 连接进行智能负载平衡：
  - 测量数据包丢失、抖动和吞吐量。
  - 定制应用程序标识。
  - 应用要求和电路性能匹配（适应实时网络条件）。
- SLA 级动态 QoS 对 Internet 电路的访问能力：
  - 动态适应不同的电路吞吐量。
  - 通过入口和出口端点的隧道进行适应。
- 在不放弃呼叫的情况下在电路之间重新路由 VOIP 呼叫。
- 端到端监控和可见性。

云直接服务工作流



在开始部署 Cloud Direct 服务之前，请确保已完成以下步骤：

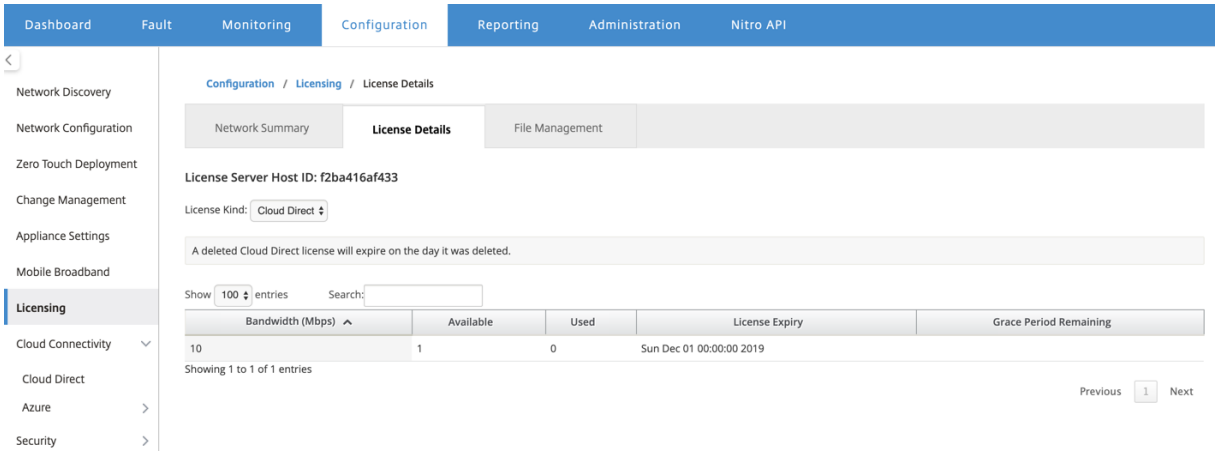
1. 拥有 410-SE、210-SE 或 1100-SE/PE 版本的设备。如果出厂发货的设备的 SD-WAN 版本早于 9.3.5，则需要按照 USB 映像过程将设备升级到最新的发货基础映像。
2. 执行单步升级过程以安装支持云直接服务的软件版本。
3. 配置 MCN 设备并使用其分支建立虚拟路径：
   - 配置分支站点。有关详细信息，请参阅配置分支。

- 为基于应用的路由创建应用程序对象。
  - 如果您打算通过 Cloud direct Service 有选择地引导应用程序，请通过包含通过 Cloud Direct 服务路由的相应应用程序（请参阅如何创建 应用程序对象）来创建应用程序对象。要管理 Internet 绑定的流量，需要从设备配置编辑器创建 Internet 服务。有关详细信息，请参阅互联网服务。
  - 如果您打算通过 Citrix Cloud 直接服务引导所有 Internet 绑定流量，则可以跳过创建特定应用程序对象。

许可

Cloud Direct 服务功能独立于 SD-WAN 的基本许可证获得许可。确保您已在 SD-WAN Center 上安装云直接服务所需的许可证。有关更多信息，请参阅 将 Citrix SD-WAN Center 作为许可证服务器.sd-wan-center-as-license-server。

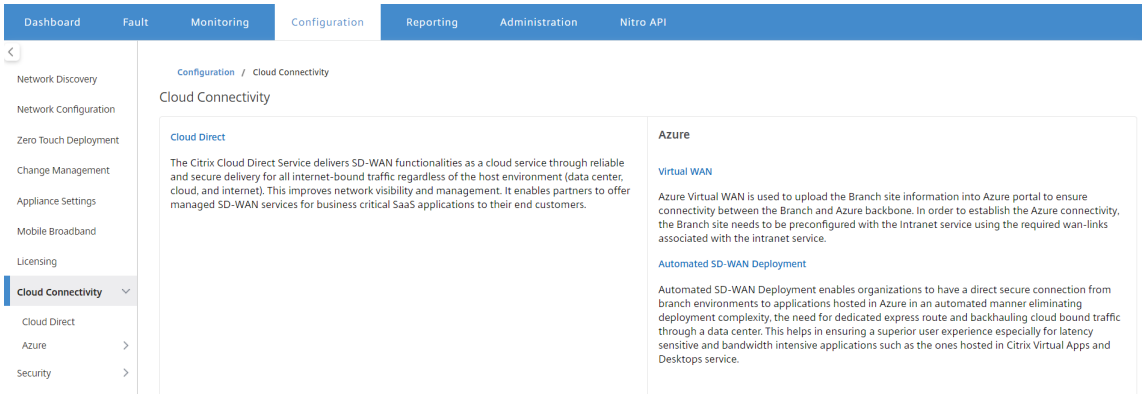
许可页面提供有关已安装 Cloud Direct 服务许可证信息的详细信息



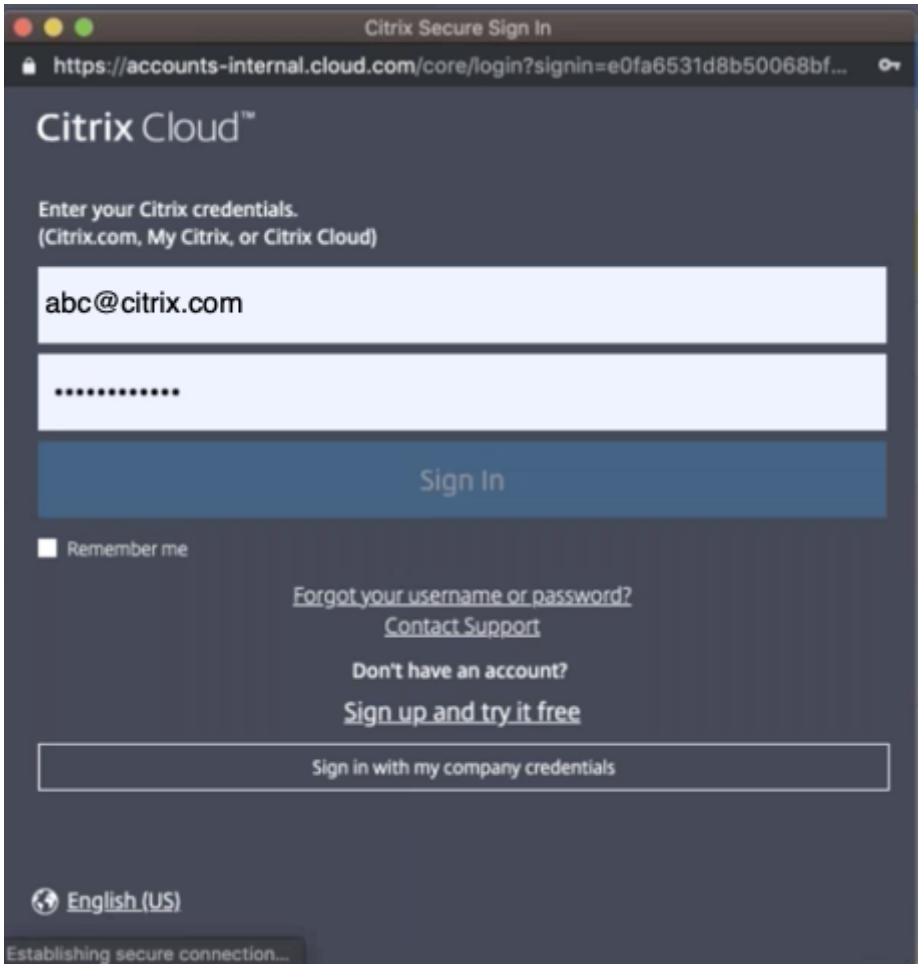
> 注意
> 过期或删除的 Cloud Direct 许可证有 30 天的宽限期，在此之前，您需要为已部署的 Cloud Direct 站点安装有效的许可证才能正常运行。如果在宽限期到期之前没有安装有效的许可证，SD-WAN Center 将使用过期的许可证在站点上禁用 Cloud Direct 服务。

在 **SD-WAN Center** 配置云直接服务

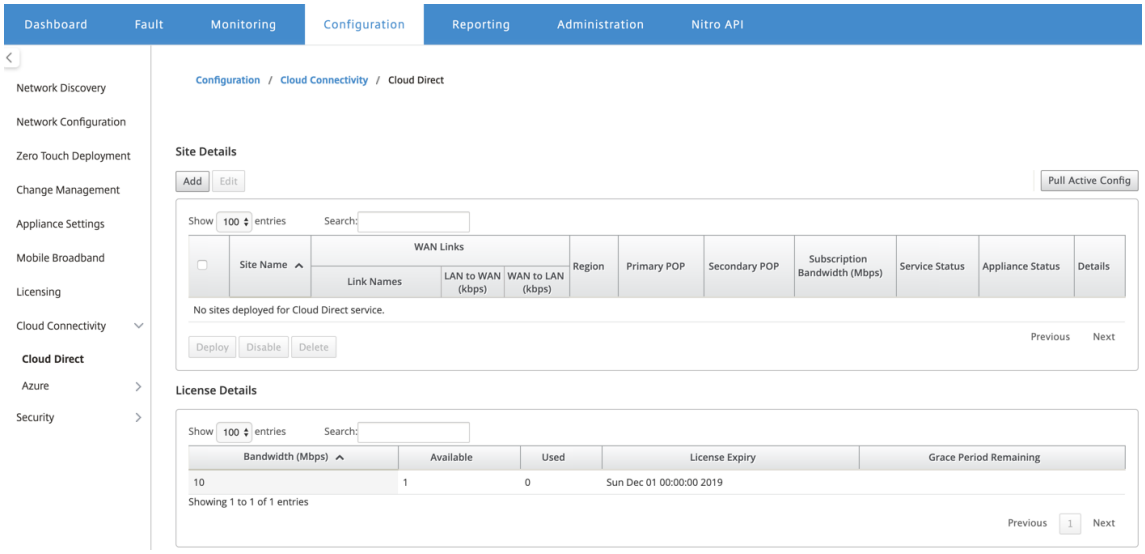
1. 在 SD-WAN Center GUI 中，导航到配置 > 云连接 > **Cloud Direct**。



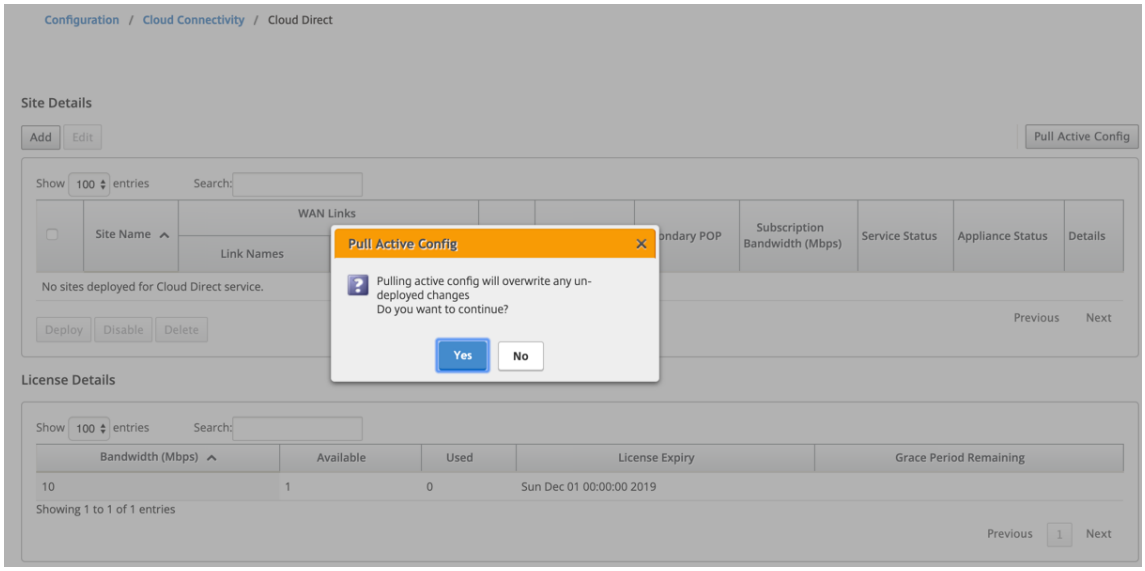
2. 使用 Citrix Cloud 凭据登录。



成功登录 Citrix Cloud 服务后，将显示云直接主页。

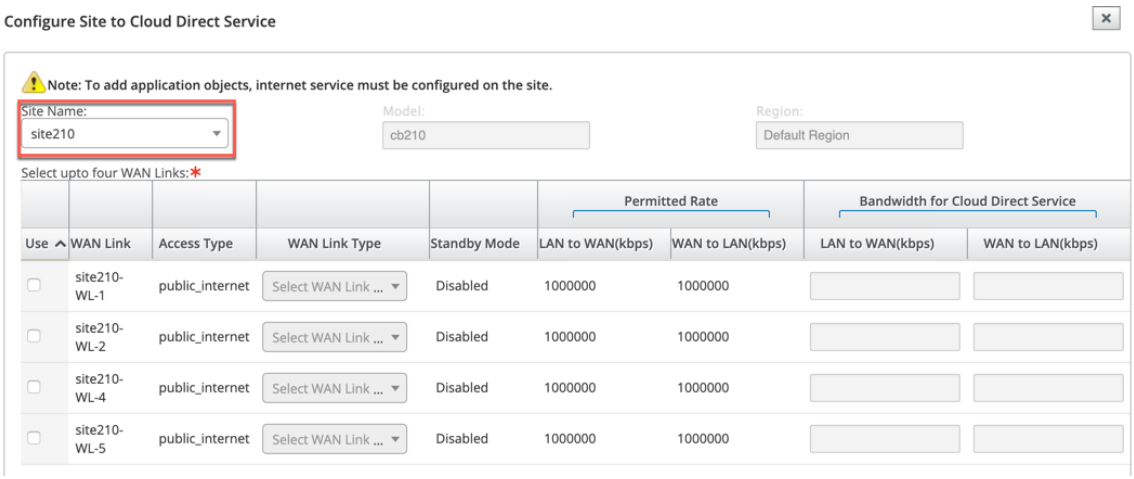


3. 单击 拉取活动配 置以检索最新的活动 MCN 配置。



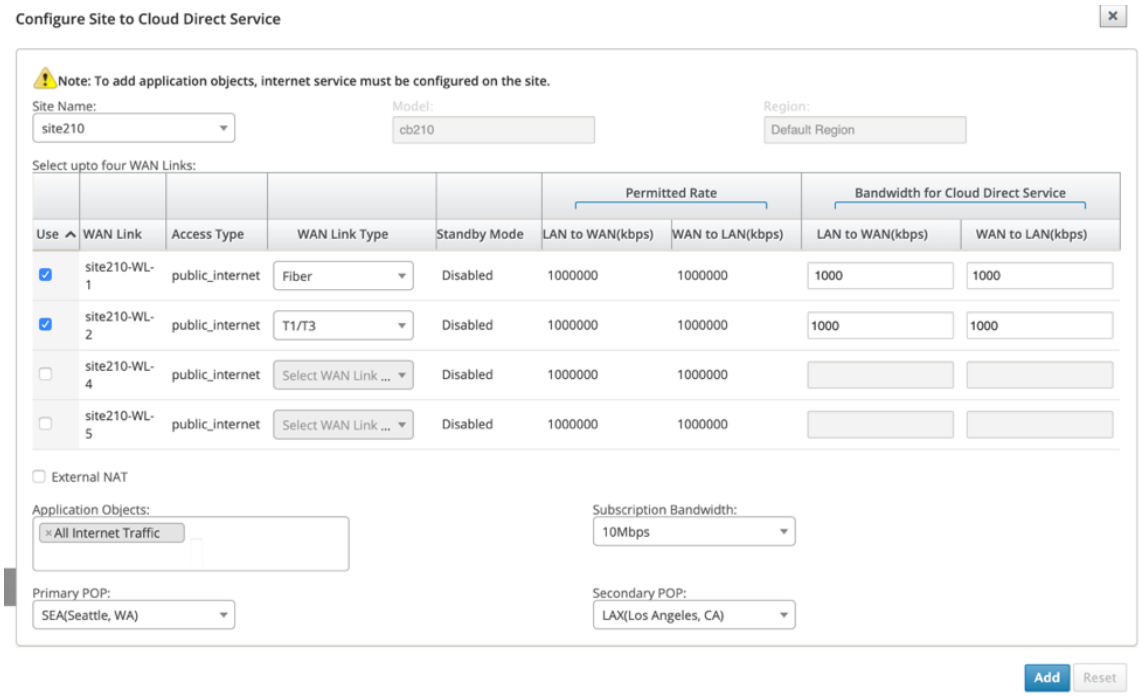
4. 单击添加新站点。菜单中将显示符合 Cloud Direct 服务部署条件的站点。

> 注意：
>
> 210、410 和 1100 个硬件设备支持云直接服务功能。



5. 选择站点后，将显示与所选站点关联的公共 Internet WAN 链接，以及设备型号信息和部署设备的区域。
6. 选择要用于云直接服务流量的 WAN 链接，以及 **WAN** 链接类型、应用程序对象、订阅带宽、主 **POP** 和辅助 **POP** 选项。

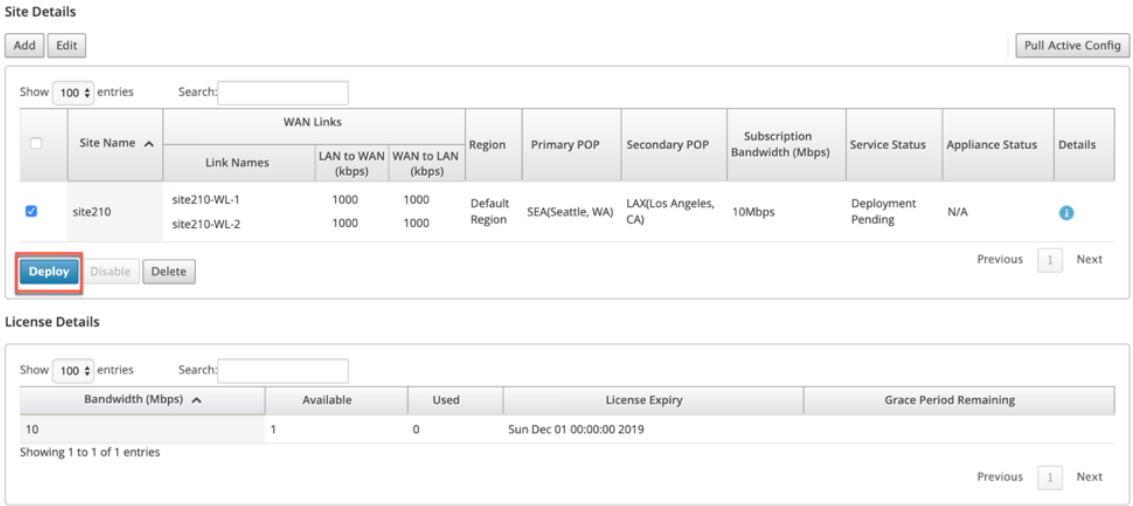
> 注意
>
> Cloud Direct 服务最多支持四个 WAN 链接。



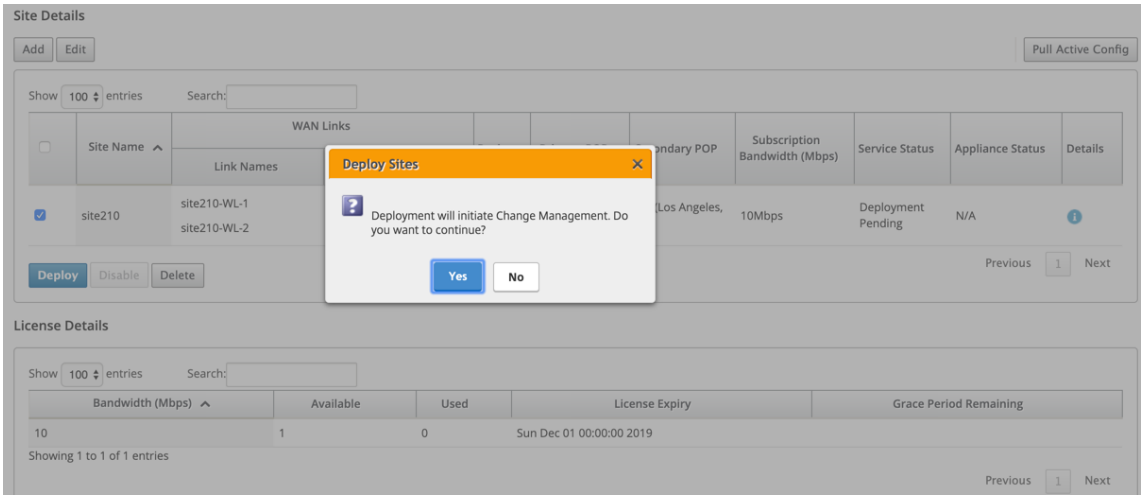
- 站点名称：显示符合 Cloud Direct 功能部署条件的站点。
- 型号：对于所选站点，将自动填充相应的装置型号名称。
- 区域：对于所选站点，将自动填充特定于设备的已部署区域详细信息。
- **WAN** 链接：对于所选站点，将显示关联的公共互联网 WAN 链接。

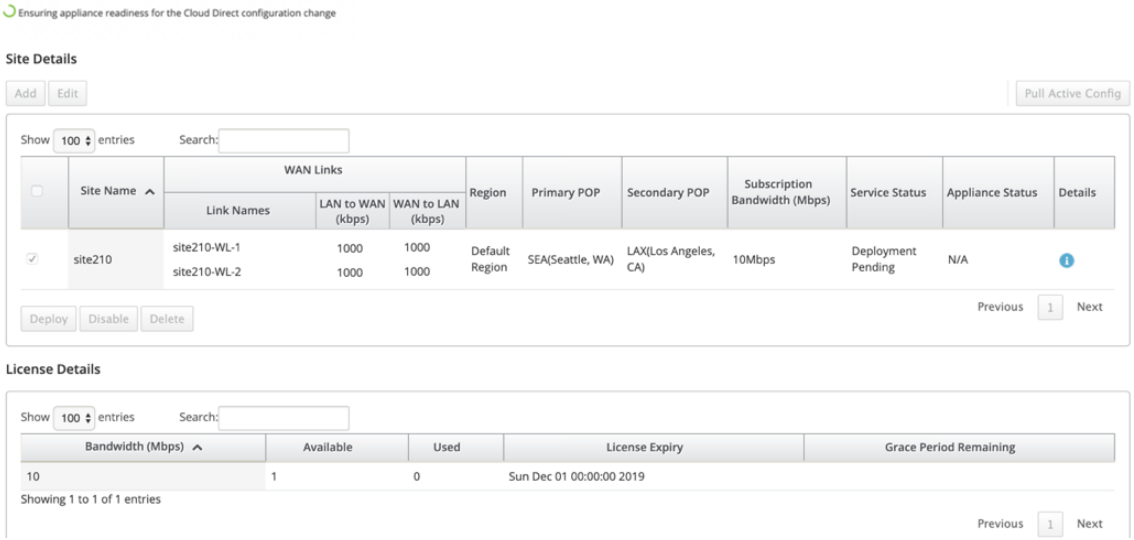
- **WAN** 链接类型：从菜单中选择 WAN 链接类型。
- 待机模式：从 WAN 链接配置中检索 待机模式。
- 云直接服务的带宽：输入云直接服务可独家使用的带宽。选定的带宽必须小于配置的允许带宽，且不能供虚拟路径、Internet 和 Intranet 服务使用。
- 外部 **NAT**：要求来自分支局域网网络的公共互联网流量是来自特定 IP 地址的来源 NAT。默认情况下，这将作为 SD-WAN 网络配置的一部分自动执行和处理。如果要在 SD-WAN 设备外（例如，在外部防火墙中）配置 NAT IP（LAN 网络），则可以在部署站点时选择“外部 NAT”选项。LAN 流量必须作为源 NAT 的 IP 在已部署 Cloud Direct 站点的详细信息页面中可用。
- 应用程序对象：您可以选择特定的应用程序对象或选择“所有互联网流量”以通过 Cloud Direct 服务重定向。如果选择了特定的应用程序对象，则这些应用程序的流量将通过 Cloud Direct 服务发送，其余流量将使用设备上配置的互联网服务进行引导。
- 订阅带宽：订阅带宽与云直接服务的许可相关联。
- 主/辅助 **POP**：确保主要和次要 POP 不相同。根据位置的邻近选择 POP。单击添加。

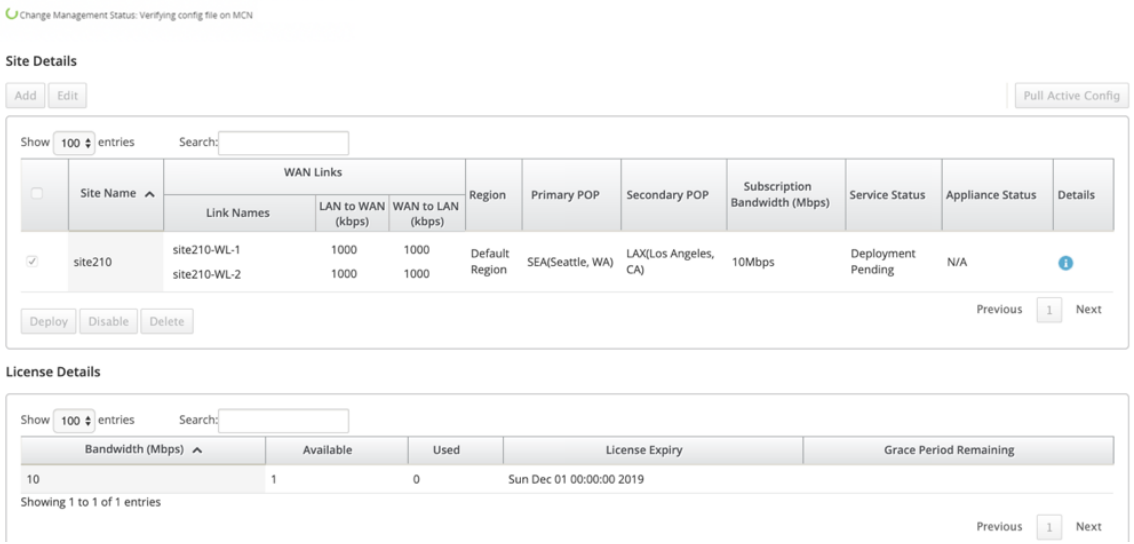
7. 添加站点后，服务状态将显示为“部署”为“挂起”。选择要为其部署云直接服务的站点，然后单击部署。



将显示一条通知，指出部署操作在 MCN 设备上启动更改管理。你可以单击“是”或“否”。







Change Management Status: Preparing the change for distribution to all appliances in the network

Site Details

Add Edit Pull Active Config

Show 100 entries Search:

	Site Name	WAN Links			Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
		Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)							
✓	site210	site210-WL-1 site210-WL-2	1000 1000	1000 1000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployment Pending	N/A	ℹ

Deploy Disable Delete Previous 1 Next

License Details

Show 100 entries Search:

Bandwidth (Mbps)	Available	Used	License Expiry	Grace Period Remaining
10	1	0	Sun Dec 01 00:00:00 2019	

Showing 1 to 1 of 1 entries

Previous 1 Next

Change Management Status: Activating the changes in the network. Please wait.

Site Details

Add Edit Pull Active Config

Show 100 entries Search:

	Site Name	WAN Links			Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
		Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)							
✓	site210	site210-WL-1 site210-WL-2	1000 1000	1000 1000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployment Pending	N/A	ℹ

Deploy Disable Delete Previous 1 Next

License Details

Show 100 entries Search:

Bandwidth (Mbps)	Available	Used	License Expiry	Grace Period Remaining
10	1	0	Sun Dec 01 00:00:00 2019	

Showing 1 to 1 of 1 entries

Previous 1 Next

✓ Cloud Direct configuration change completed successfully ×

Site Details

Add Edit Pull Active Config

Show 100 entries Search:

	Site Name	WAN Links			Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
		Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)							
☐	site210	site210-WL-1 site210-WL-2	1000 1000	1000 1000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployed	Enabled	ℹ

Deploy Disable Delete Previous 1 Next

License Details

Show 100 entries Search:

Bandwidth (Mbps)	Available	Used	License Expiry	Grace Period Remaining
10	0	1	Sun Dec 01 00:00:00 2019	

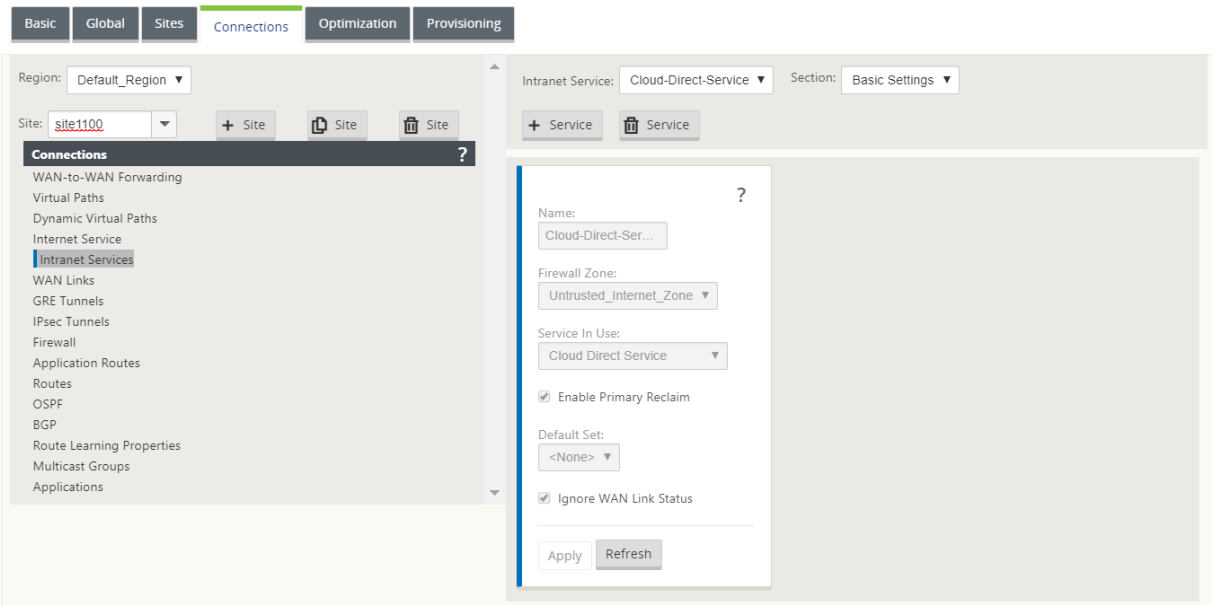
Showing 1 to 1 of 1 entries

成功部署站点后，云直接服务页面将显示以下内容：

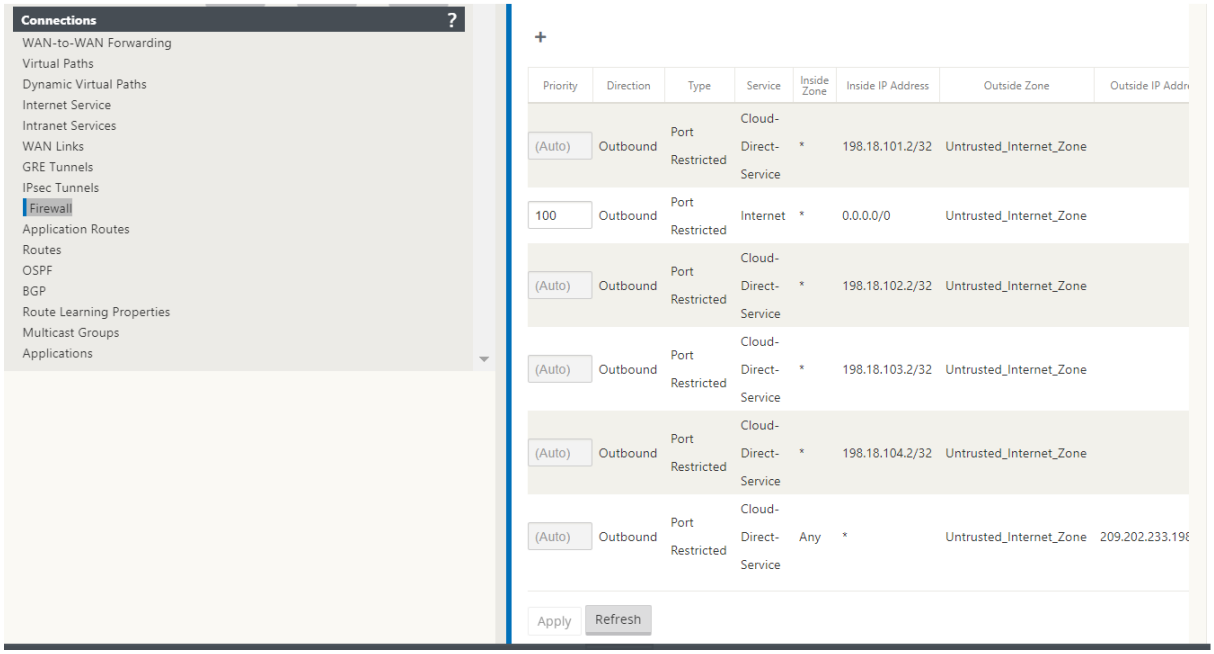
- 服务状态：已部署
- 装置状态：已启用
- 订阅带宽 **(Mbps)**：10 Mbps
- 已使用已安装的许可证

上述更改管理步骤自动生成所需的 Cloud Direct 服务配置并将其添加到正在运行的配置中。

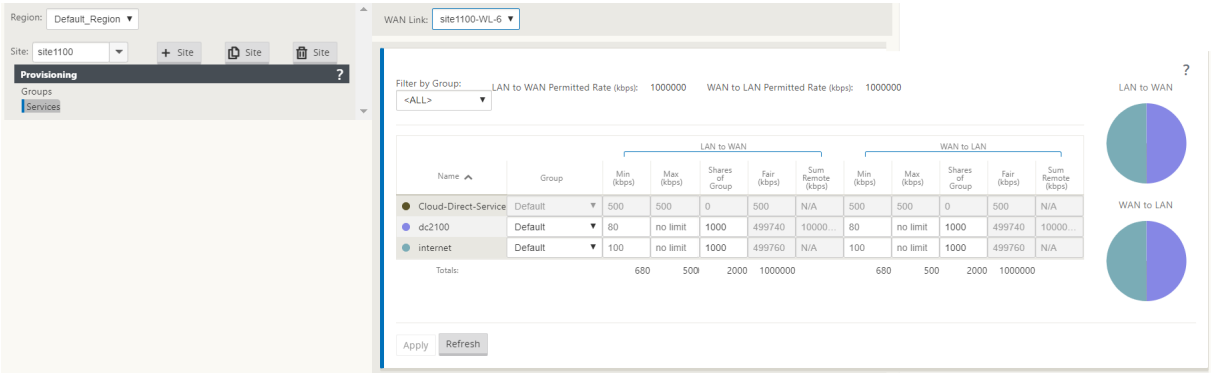
> 注意
>
> 自动创建的 **Cloud Direct Service**（Intranet 服务）与 Default_RoutingDomain 相关联。



防火墙设置

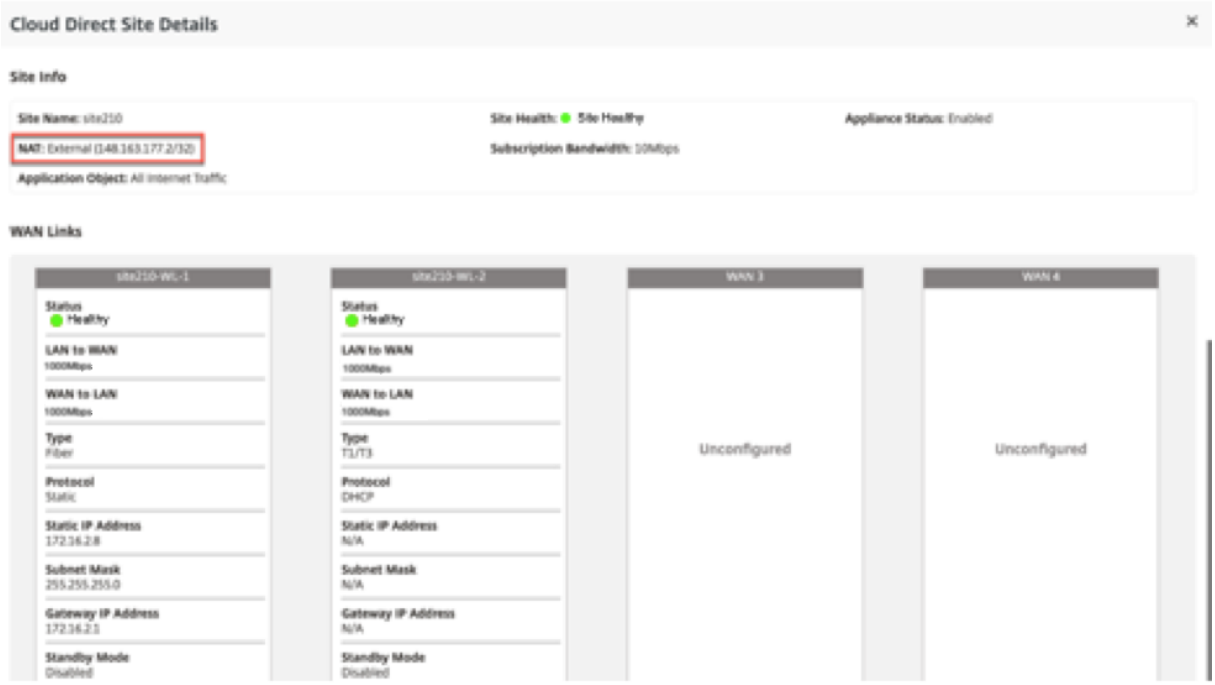


SD-WAN 应用程序 GUI 中的置备站点

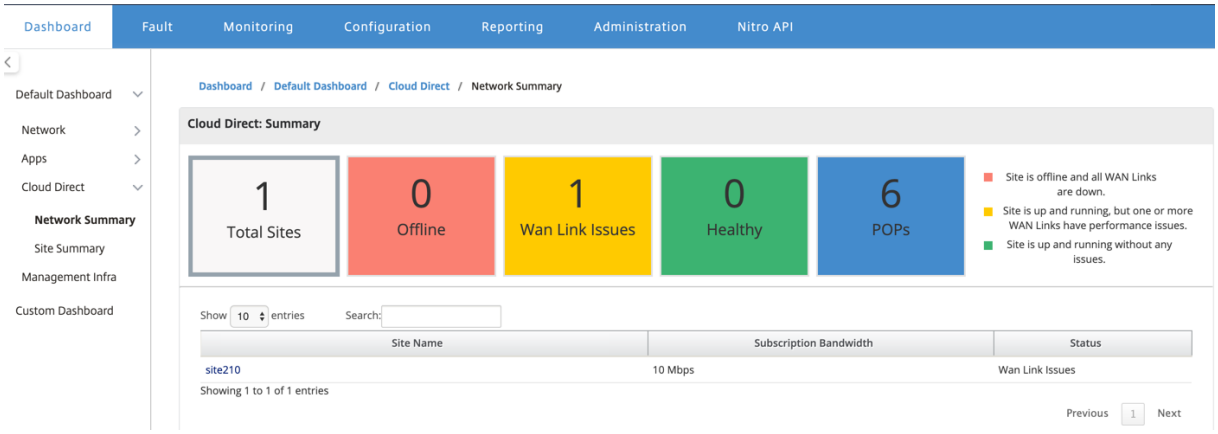


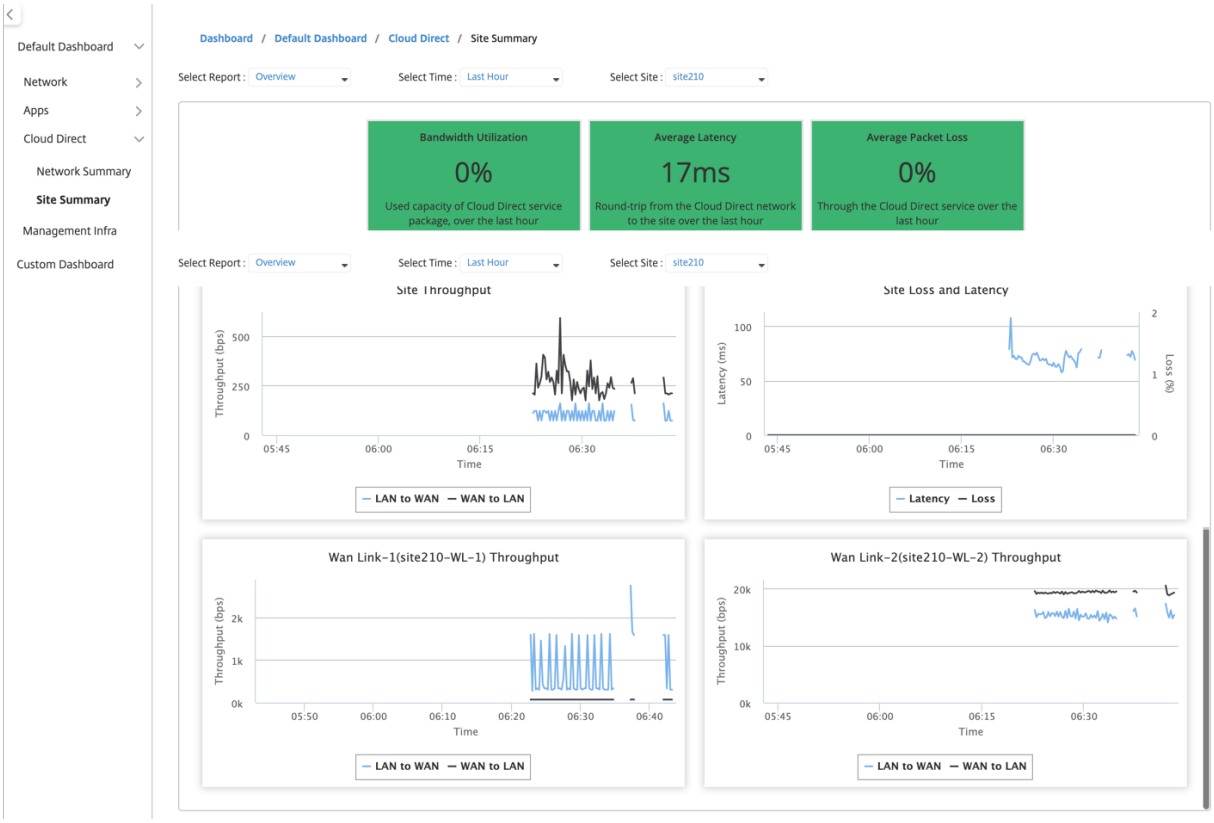
监控云直接服务

部署和启用站点后，您可以查看配置的 Cloud Direct 服务。单击 详细信息 列中的感叹号图标以查看站点详细信息。



您可以通过导航到控制面板 > **Cloud Direct** > 网络摘要和站点摘要来查看“站点摘要”图表。

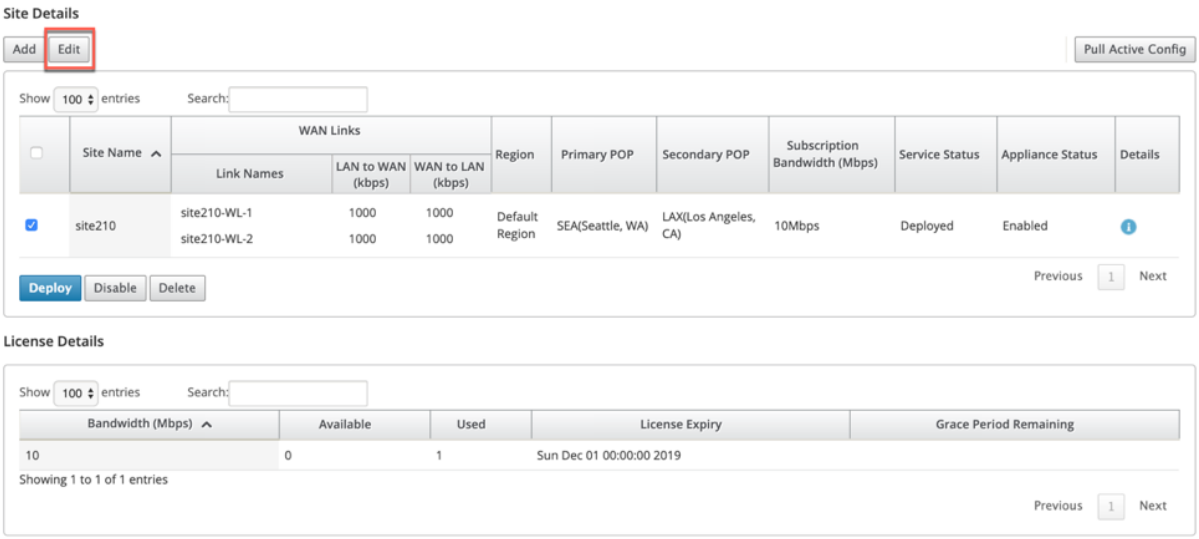


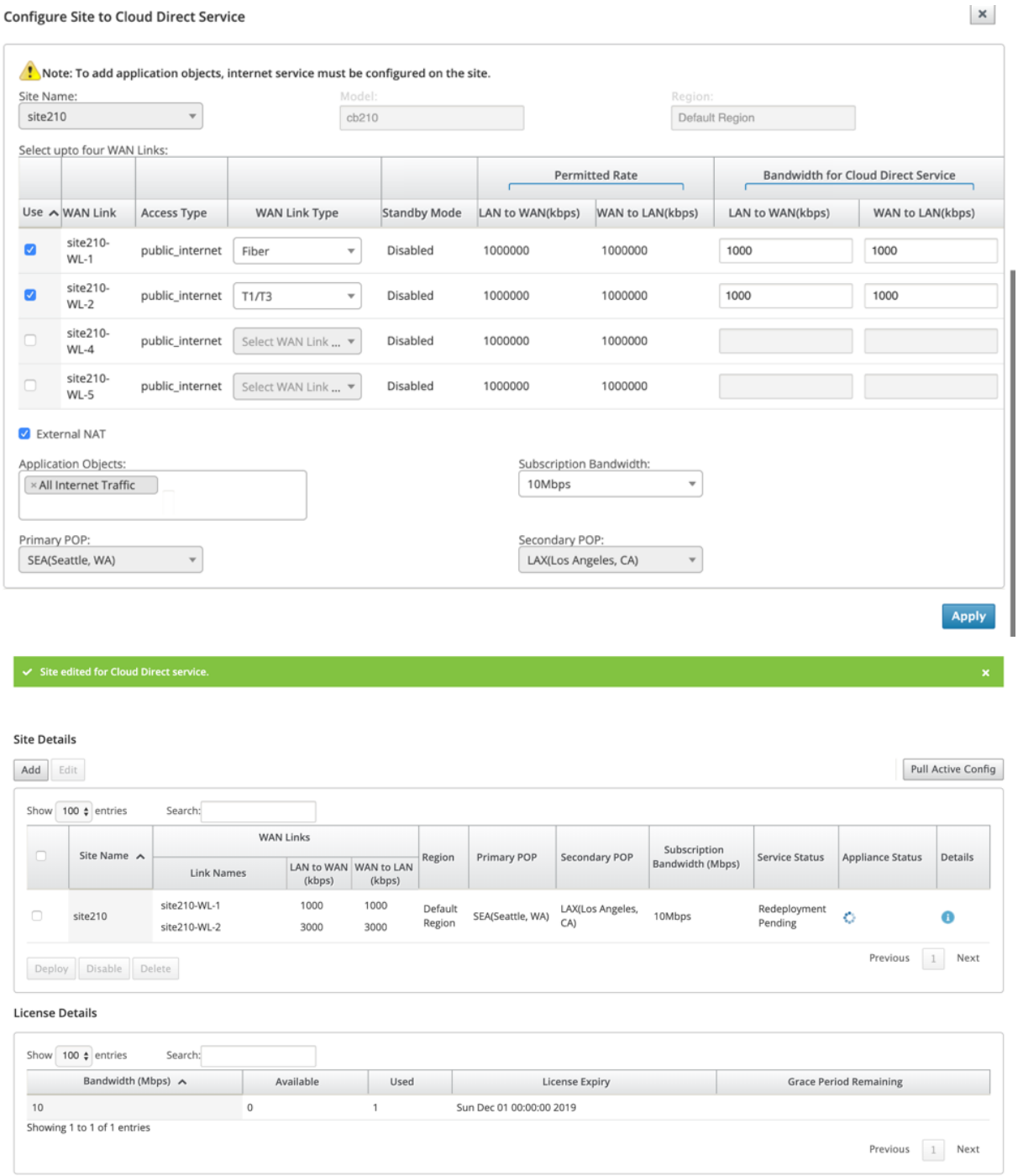


在 **SD-WAN Center** 中编辑站点

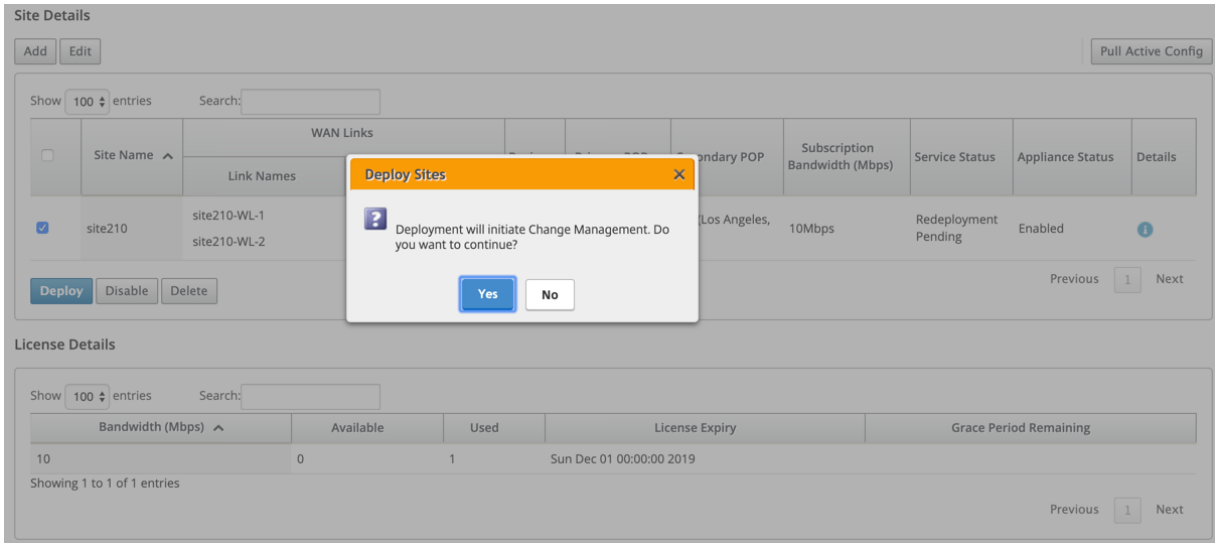
您可以选择编辑站点以修改带宽和 WAN 链接类型。

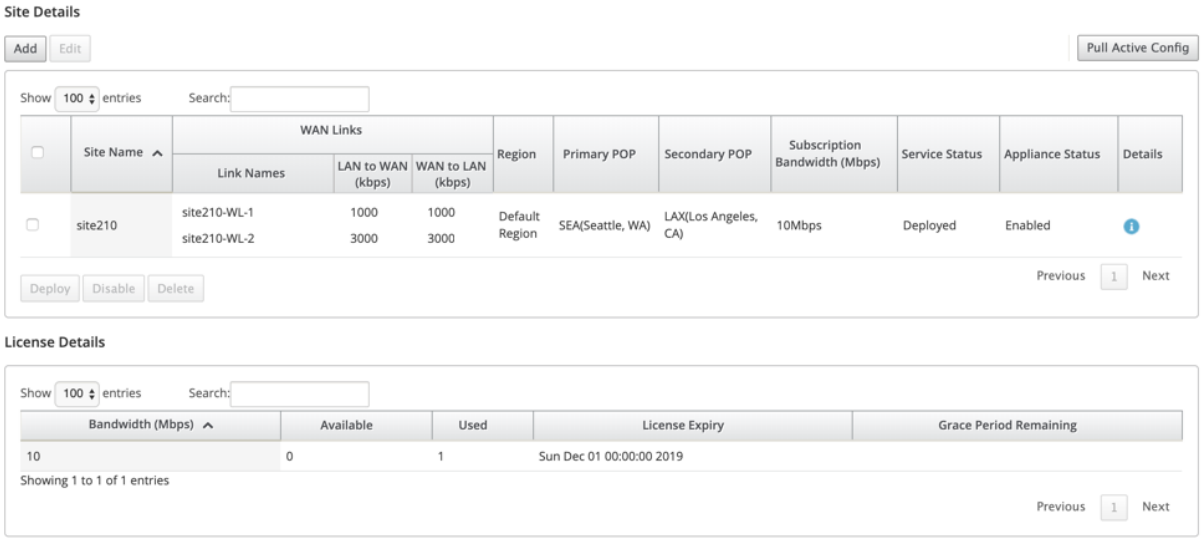
> 注意
>
> POP 选择无法编辑。





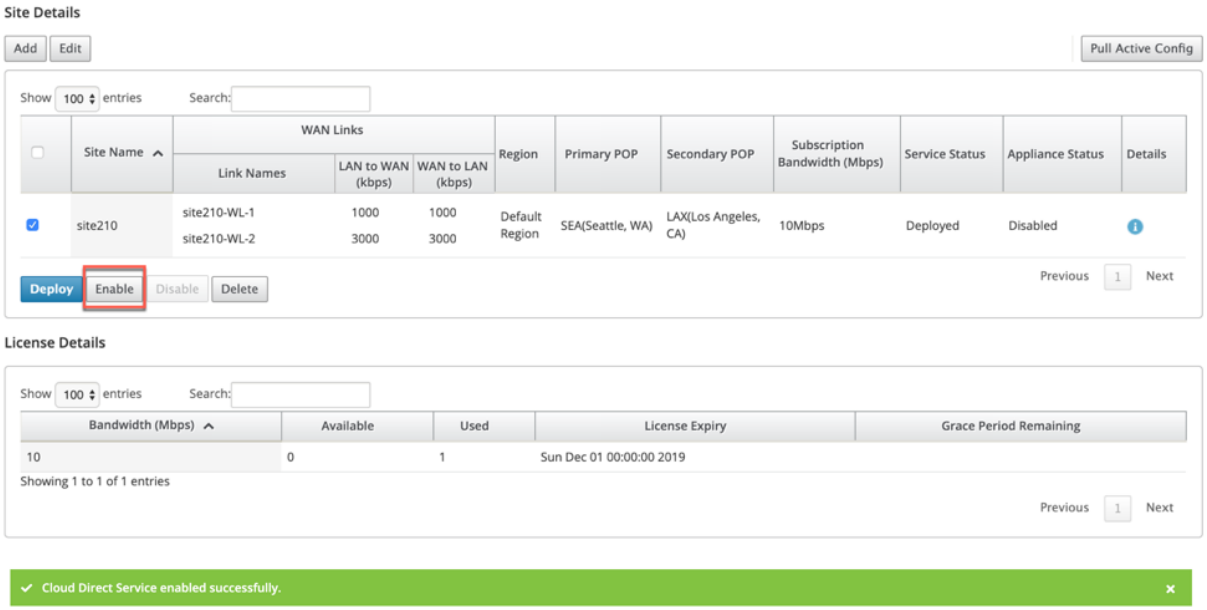
服务状态显示为待重新部署。部署网站。已编辑站点的部署过程已完成。

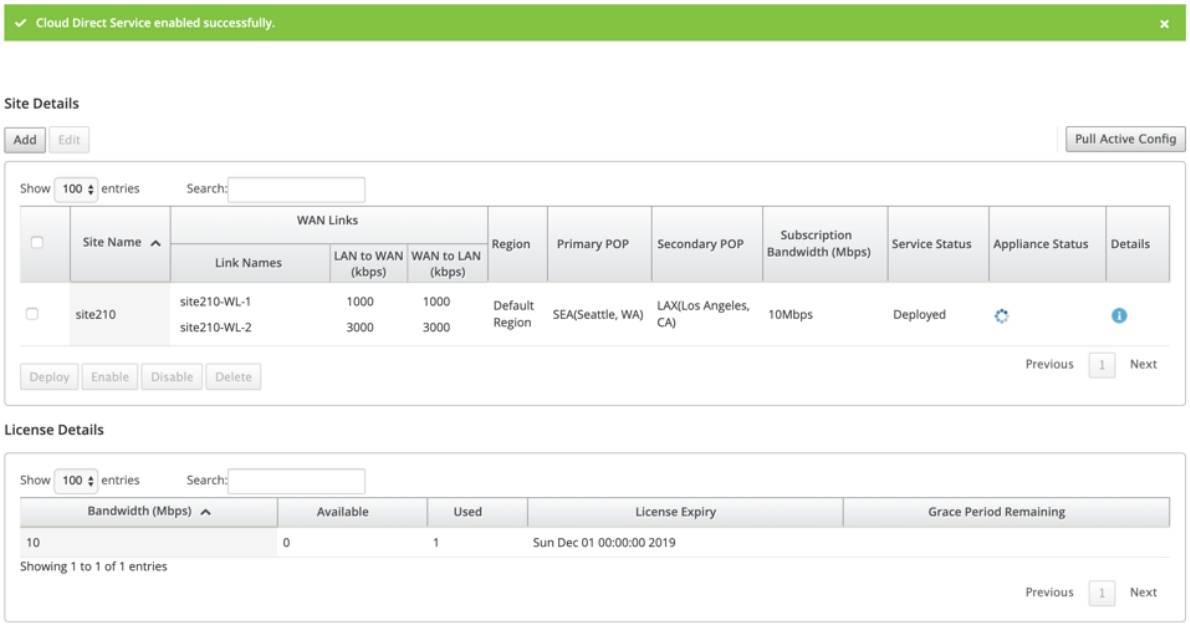




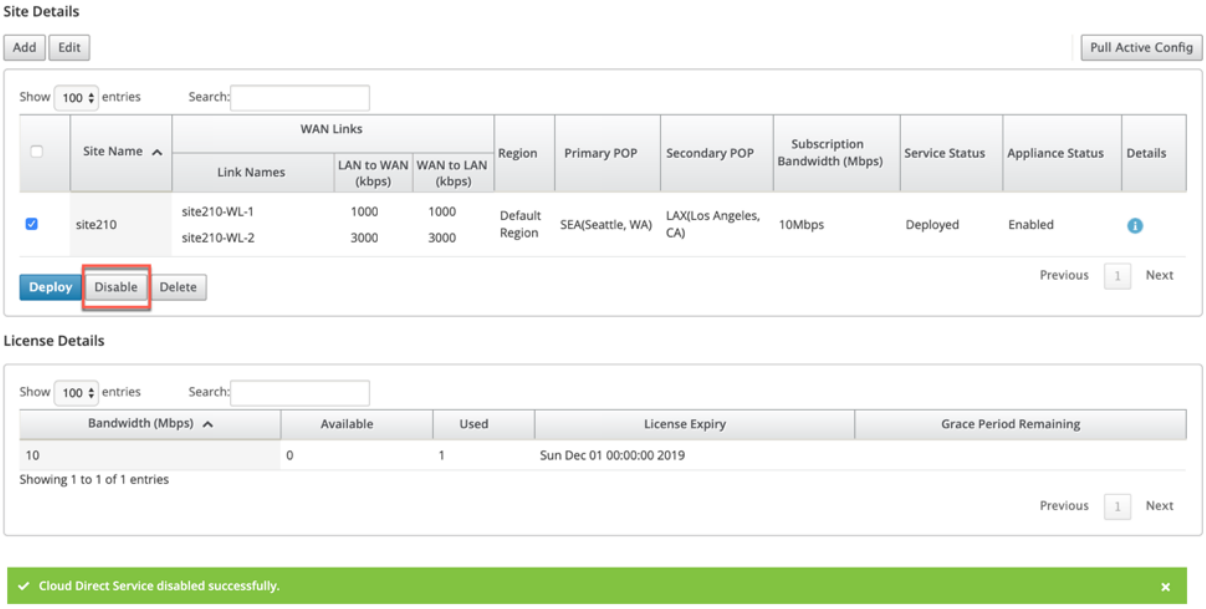
启用和禁用站点

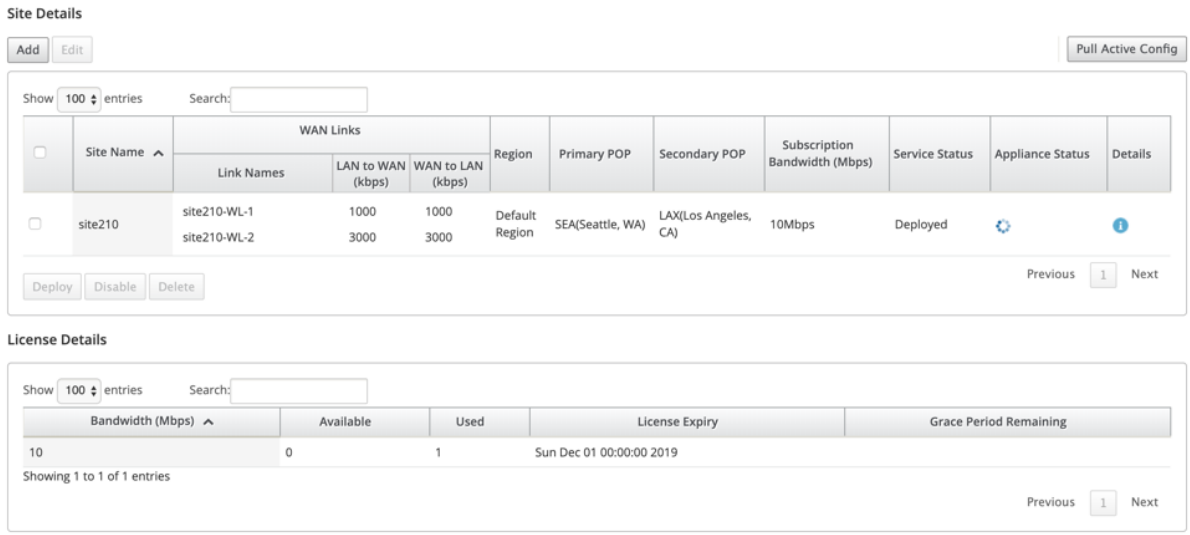
您可以启用装置状态显示为禁用的已部署站点。若要启用站点，请单击启用。





单击禁用以禁用已部署的站点。禁用网站将不再使用云直接服务来引导互联网流量。如果在设备上配置，则所有流量都将通过 Internet 服务重定向。

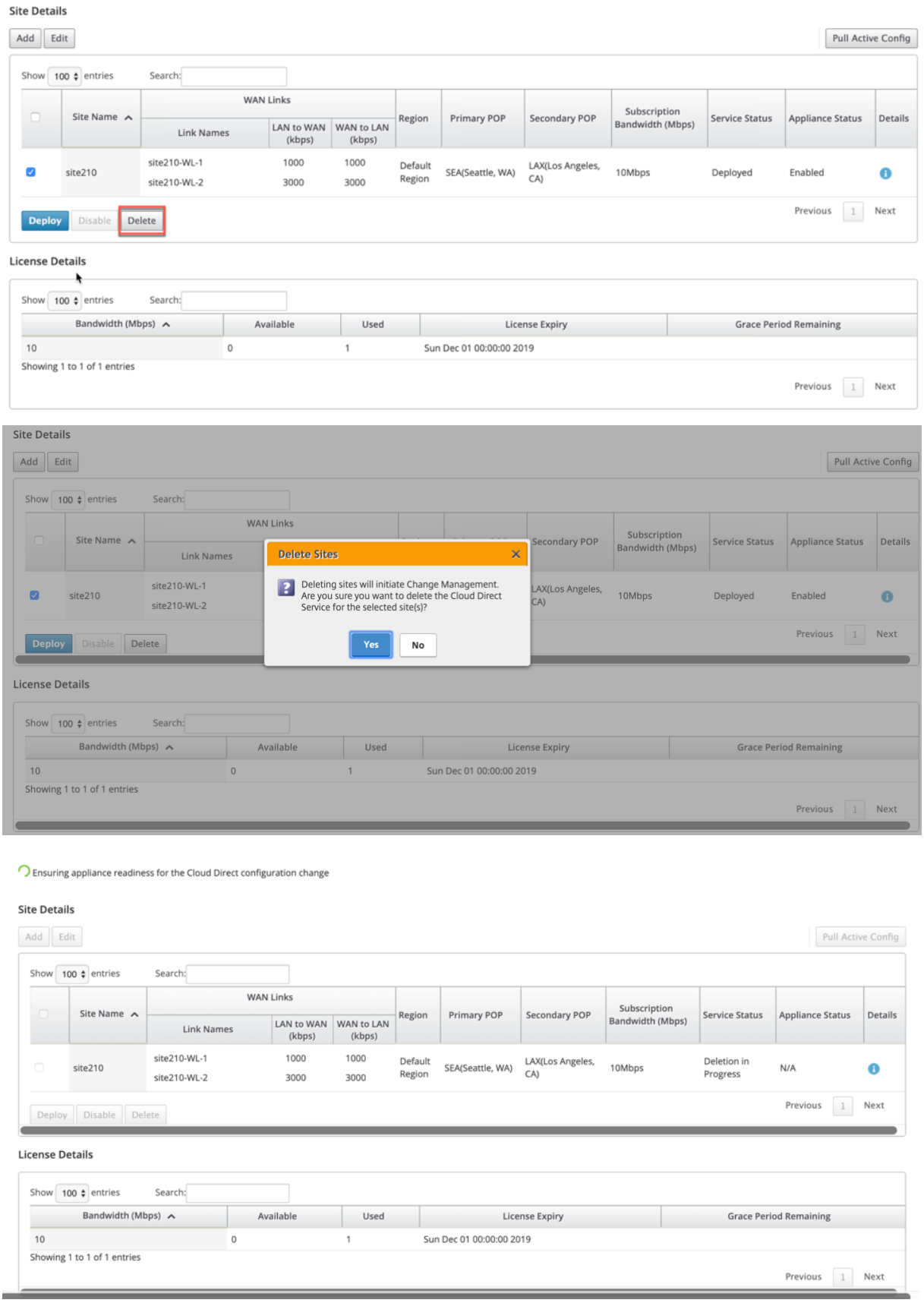


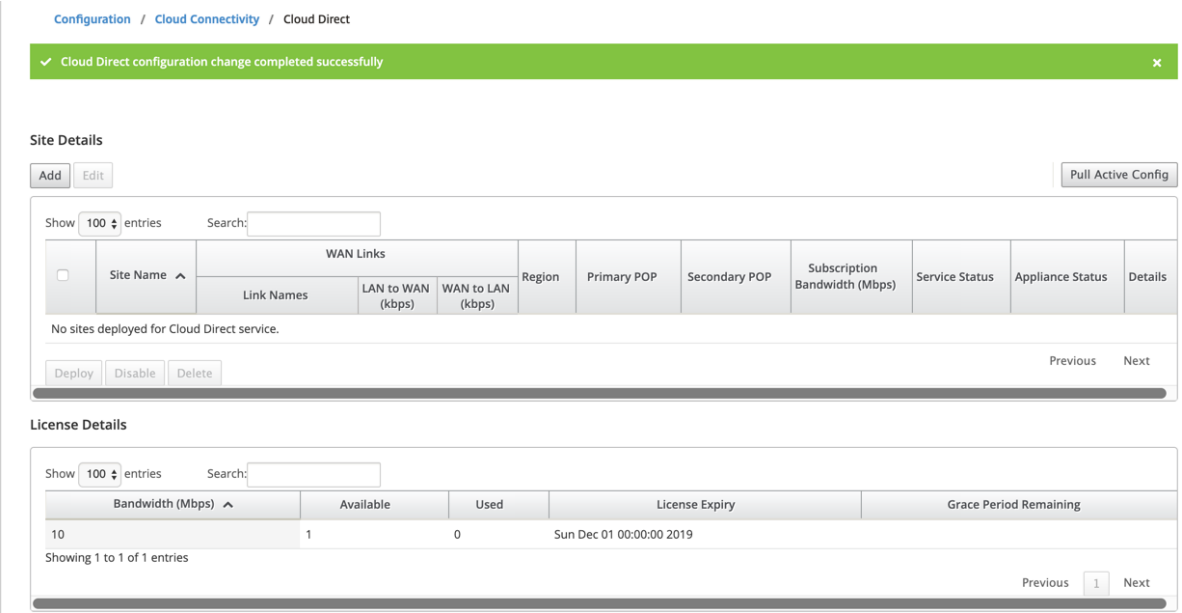


网站删除

您可以选择删除不再需要 Cloud Direct 连接的站点。要删除站点，请选择该站点，然后单击删除。系统将显示一条确认消息，用于删除站点。

通过更改管理过程删除所有云直接服务配置。

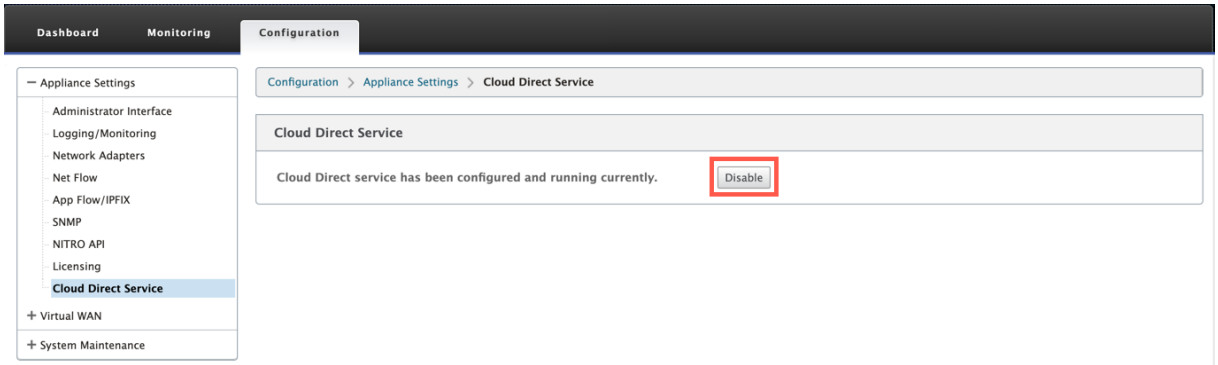




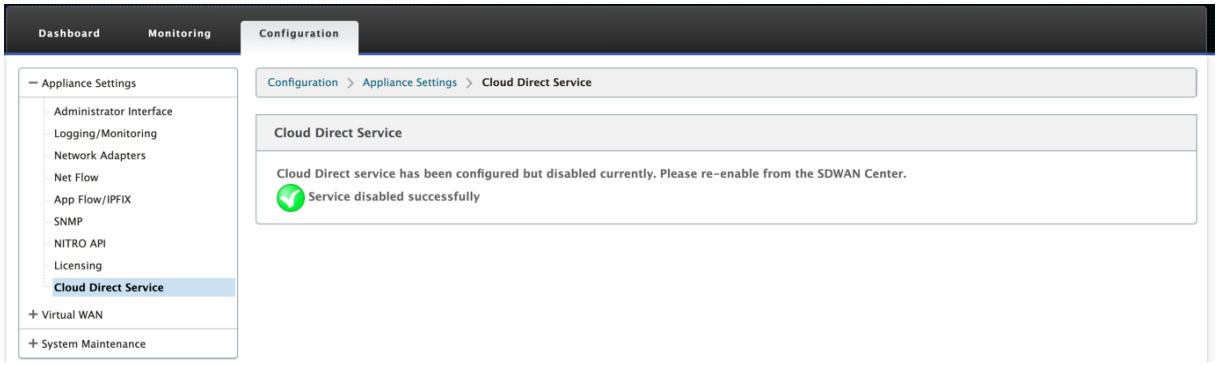
Citrix SD-WAN 上的云直接服务状态

您可以在本地 SD-WAN 设备上验证 Cloud Direct 服务状态。

转到 Citrix SD-WAN GUI，导航到配置 > 展开设备设置 > 选择 **Cloud Direct** 服务。



单击 禁用 选项以禁用 Cloud Direct 服务。



故障排除

部署 Cloud Direct 服务时，SD-WAN Center 上可能出现的最常见错误消息如下所示。

错误/状态消息将显示在 SDWAN Center 上的配置 > 云连接 > **Cloud Direct** 下。

“**Cloud Direct** 许可证错误**!** 请上载 **{bandwidth} Mbps** 带宽的额外许可证”

- 通过导航到配置 > 许可 > 文件管理选项，在 SDWAN Center 上载有效的 Cloud Direct 许可证，然后继续部署此功能

“由于 **Citrix Cloud Workspace** 登录问题导致的 **Cloud Direct** 配置高可用性”

- 通过导航到配置 > 云连接选项，在 SDWAN Center 重新输入 Citrix Cloud Workspace 登录凭据。

“**Cloud Direct** 配置处理错误**!** 站点 **{site_name}(IP: {mgmt_ip})** 不支持 **Cloud Direct**”

- 检查管理端口上是否可以访问 SD-WAN 设备或设备（在 HA 部署的情况下）。

“站点的 **Cloud Direct** 配置高可用性配置检查错误**: {site_name}**”

- 检查 HA 对中两个设备的连接性是否与正在部署的站点相对应。

“两个高可用性对设备必须可访问才能执行 **Cloud Direct** 配置”

- 在 HA 对的 SD-WAN 设备上部署 Cloud Direct 服务时，辅助设备和主设备都需要在管理端口上访问。

“**Cloud Direct** 配置处理错误**!** 站点 **{site_name}(IP: {mgmt_ip})** 遇到 **SSO** 登录问题”

- 请检查 SD-WAN 设备是否已启动/运行并在管理端口上可访问。SD-WAN Center 无法对 SDWAN 设备执行单点登录时，将显示此错误。

“**Cloud Direct** 配置处理过程中遇到内部错误”

- 这可能是由于在执行配置检查或其余处理过程中出现多种错误情况。用户可能需要查看日志并再次执行操作。

“**Cloud Direct** 配置处理已取消**! MCN** 还没有准备好进行更改管理”

- 检查 MCN 是否可访问并启动并运行，以及其更改管理状态是否为“network_staging”。

“**Cloud Direct** 配置处理错误**!** 站点 **{site_name}(IP: {mgmt_ip})** 支持 **Cloud Direct**。请执行单步升级以获得 **Cloud Direct** 支持”

- 通过 **MCN** > 更改管理在 SD-WAN 设备上执行单步软件升级。完成此过程后，请重新尝试为此站点部署 Cloud Direct 服务。

“**Cloud Direct** 配置处理错误**! SD WAN** 更改管理操作失败”

- 更改管理操作不知何故没有成功。请查看 SDWAN Center 日志了解详细信息。

“**Cloud Direct** 配置处理错误**!** 在站点 **{site_name}** 上启用服务失败”

- 无法在 SD-WAN 设备上启用 Cloud Direct 服务。在执行单点登录时检查特定设备的连接性或 HA 对中的设备是否连接或是否存在任何问题。有关详细信息，请查看 SD-WAN Center 和设备上的日志。

“**Cloud Direct** 配置处理错误**!** 在站点 **{site_name}** 上禁用服务失败”

- 无法在 SD-WAN 设备上禁用 Cloud Direct 服务。在执行单点登录时检查特定设备或 HA 对中的设备是否连接或是否存在任何问题。有关详细信息，请查看 SD-WAN Center 和设备上的日志。

“**Cloud Direct** 配置处理错误**!** 配置映像推送到站点 **{site_name}** 失败”

- 无法通过 REST api 在设备上上载特定于服务的映像，或者无法访问 HA 对中的两个设备。

“**Cloud Direct** 服务在配置处理过程中遇到错误。在 **SD WAN** 配置中发现了审核错误**!**”

- 尝试编译 SDWAN 配置时发现审计错误。详情请查看 SD-WAN Center 日志。

“**Cloud Direct** 配置处理错误**!** 为站点 **{site_name}** 创建站点失败”

- 尝试为相应的 SDWAN 设备创建站点时出现服务端错误。请查看 SDWAN Center 日志了解更多详细信息。

“**Cloud Direct** 配置处理错误**!** 为站点 **{site_name}** 更新站点失败”

- 尝试修改相应 SDWAN 设备的站点相关设置时出现服务端错误。请查看 SDWAN Center 日志了解更多详细信息。

日志中看到的错误消息 **(SDWAN_common.log)**

在以下几种情况下，Cloud Direct 服务部署在 SD-WAN 设备上，但可能无法按预期运行。您可以使用 SD-WAN_common.log 下载和查看本地 SDWAN 设备上的日志以了解更多详细信息。

场景 **1**

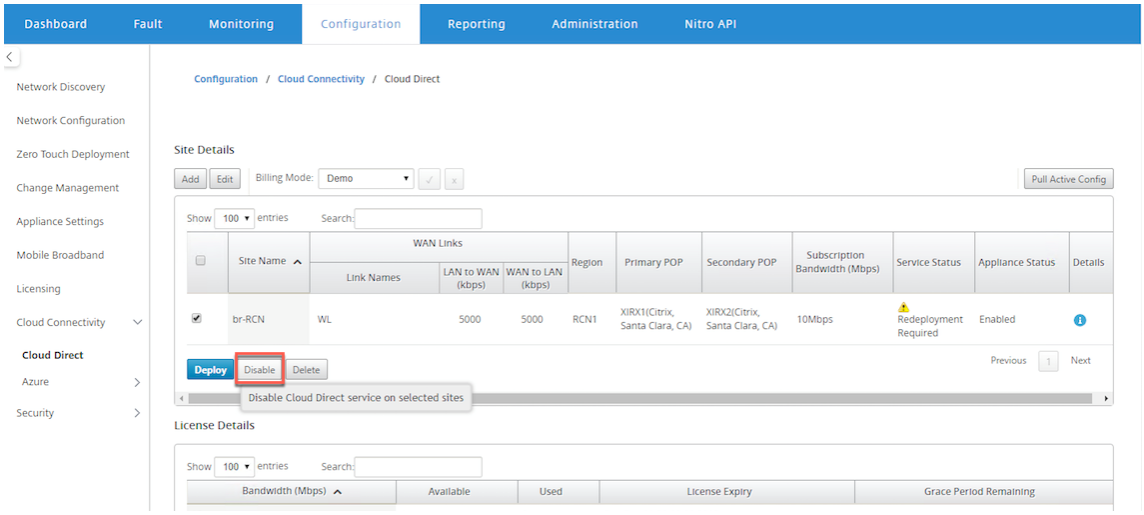
“检测到 **Cloud Direct** 虚拟机没有响应…立即禁用云直接服务！““云直接服务已被禁用。“ 在本地 SDWAN 设备上运行的底层 KVM 无法按预期方式运行。在这种情况下，设备上的 Cloud Direct 服务功能将被禁用。

方案 **2**

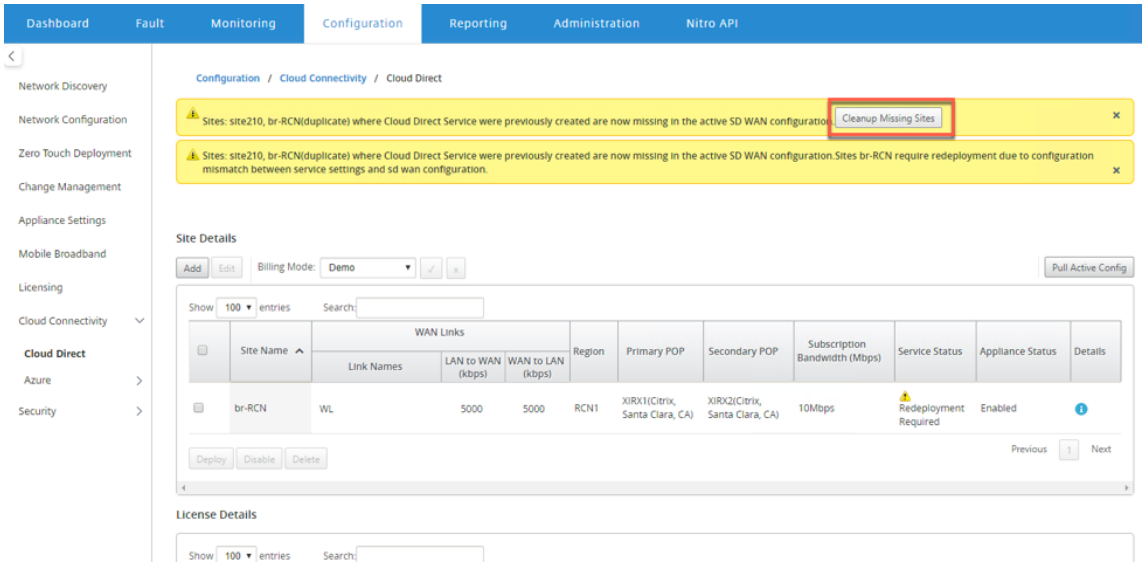
“过去 **5** 分钟内没有看到隧道数据包…立即禁用云直接服务！”“云直接服务已被禁用。“ SD-WAN 设备和用于 Cloud Direct 服务的隧道端点之间没有建立隧道。这可能是由于 wan-link 配置错误、通过已配置的 wan-link 缺乏互联网连接、推送到设备的不兼容或无效的数据 /config 映像，或任何防火墙规则在通过 wan-link 接收 UDP 隧道数据包时可能会丢弃 UDP 隧道数据包。在这种情况下，设备上的 Cloud Direct 服务功能将被禁用。

当您在使用不同 Cloud Direct 配置激活 MCN 上的配置时（例如：为 Cloud Direct 更改了 NAT 配置），这可能会导致流量永久中断。要克服此阻塞，您可以按照以下步骤之一选择设备上存在的不同路由：

1. 在 SD-WAN Center GUI 中，导航到配置 > 云连接 > **Cloud Direct**。选择云直接设备，然后单击禁用选项以禁用云直接服务。



2. 导航到配置 > 云连接 > **Cloud Direct** 并拉取活动配置以获取清理通知。您可以单击针对受影响的云直接设备显示的清理缺少站点通知按钮。此操作将禁用设备上运行的 Cloud Direct 服务。



3. 重新部署 SD-WAN Center 上的云直接服务，以便对受影响的设备使用云直接服务。

使用 **Citrix SD-WAN Center** 集成 **Citrix SD-WAN** 和 **Zscaler**

April 13, 2021

Citrix SD-WAN 和 Zscaler 帮助企业通过为 Internet 上托管的应用程序和资源提供安全的本地越狱来转换其 WAN 以便进行云迁移。在降低成本和复杂性的同时，新的 WAN 基础结构技术（例如 SD-WAN）提高了网络的灵活性和扩展能力，从而改进了分布式组织的用户体验。

SD-WAN 解决方案通过允许通信发送到本地以加入到 Internet，简化了路由。SD-WAN 提供使用应用程序控制功能将流量路由到 Internet（删除中央 DC 环境）的灵活性。但是，将网络连接到 Internet 会带来很大的安全风险。通过云服务保护本地突破的集中化方法消除了维护分支机构安全基础设施的开销。所有流量都通过分支网络中的 Citrix SD-WAN 可靠地路由到 Zscaler（基于云的安全平台）。您可以消除昂贵的基础设施，保护网络免受威胁和漏洞的侵害

Citrix SD-WAN

Citrix SD-WAN 通过安全地启用本地分支到 Internet 越狱来帮助企业移动到云，以创建可允许或拒绝直接从分支进行的 Internet 访问的策略。Citrix SD-WAN 通过 4000 个应用程序（包括各个 SaaS 应用程序）的集成数据库组合来标识应用程序，并使用深度包检测技术来实时发现应用程序并对其进行分类。它使用这些应用知识来引导流量从分支机构到 Internet、云或 SaaS。

Zscaler

Zscaler 是主要的基于云的安全平台，在不需要本地硬件、设备或软件的情况下提供卓越的安全性。Zscaler 会在 Internet 周围放置一个外围环境，以便企业无需在每个办公室周围放置安全外围。Zscaler 云安全平台在全球 100 多个数据中心作为一系列安全检查站。通过将 Internet 流量重定向到 Zscaler，企业可以即时保护存储、分支和远程位置。Zscaler 将连接用户和 Internet，检查每个字节的流量（即使已加密或压缩），以便用户安全并在所有隐藏的威胁被确认后才可以渗入企业网络。

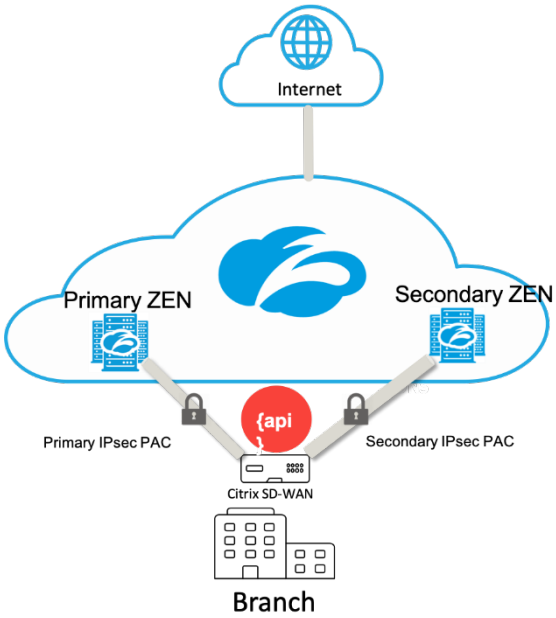
Citrix SD-WAN 允许创建允许来自分支机构和 Zscaler 的云安全平台的直接 Internet 分支的策略，方法是检查云服务中与用户连接的所有 Internet 绑定流量，以确保安全。

Zscaler 强制节点 (ZEN)

Citrix SD-WAN 支持 Zscaler API，用于在兹斯卡勒云网络中自动创建 Citrix SD-WAN 和兹斯卡勒强制节点 (ZEN) 之间的 IPsec 隧道。ZEN 是一种功能齐全的内联 Internet 安全网关，用于检查所有 Internet 流量双向攻击，并强制实施安全性和合规性策略。

Zscaler API 为每个分支提供了两个最接近的数据中心位置，使 SD-WAN 能够有效地实现通信。组织可以允许 Zscaler 自动选择距离分支最近的 ZEN，方法是让 ZEN 查看 Citrix SD-WAN 上配置的 WAN 链接的 IP 地址，也可以手动选择 **Zens**。

> 注意
>
> 如果隧道处于 UP 状态，则两条路径始终处于活动模式。如果任何隧道向下，则相应的路线变得无法到达，在这种情况下，另一条路线将保持运行。



优势

集成 Citrix SD-WAN 和 Zscaler 的优势包括：

- 在分布式企业中更快地采用 SaaS 和云。
  - 将安全集中在云服务中，无需在每个分支中具有该服务。
  - 不需要对通过 Internet 传输的流量进行回程处理，这允许分支机构的本地 Internet 越狱。
- 通过自动连接到 Secure Web Gateway 关，简化了 IT 管理。
  - API 支持自动配置到 Zscaler 的安全隧道
- 通过缩短回程 SaaS 流量的延迟改进了用户体验。
  - 出于安全目的，消除了中心辐射型模型依赖关系
- 消除分支机构昂贵的安全堆栈
  - 减少必须在分支机构部署和管理防火墙的开销。
- 确保 Internet 绑定的流量始终是安全的。
  - 安全策略不会将用户绑定到物理位置。
  - 提供沙盒、检查所有端口和协议（包括 SSL、URL 过滤、高级威胁防护等），以防止出现零天攻击。

支持的功能

使用 SD-WAN 设备的 Zscaler 部署支持以下功能：

- 将用户定义的互联网流量转发到 Zscaler，从而实现直接互联网突破。
- 基于每个客户站点使用 Zscaler 进行直接互联网访问（DIA)。
  - 在某些站点上，您可能希望向 DIA 提供本地安全设备，而不使用 Zscaler。
  - 在某些站点上，您可能会选择回程线路流量（另一个客户站点）以访问 Internet。
- 虚拟路由和转发部署。
- 一个 WAN 链接，作为 Internet 服务的一部分。

Zscaler 是一种云服务。必须将其设置为服务并定义底层 WAN 链接：

- 在数据中心和分支站点上配置可信公共 Internet WAN 链接。
- 为 Intranet 服务自动配置 IPsec 通道。

在 **Citrix SD-WAN Center** 工作流中部署 **Zscaler**

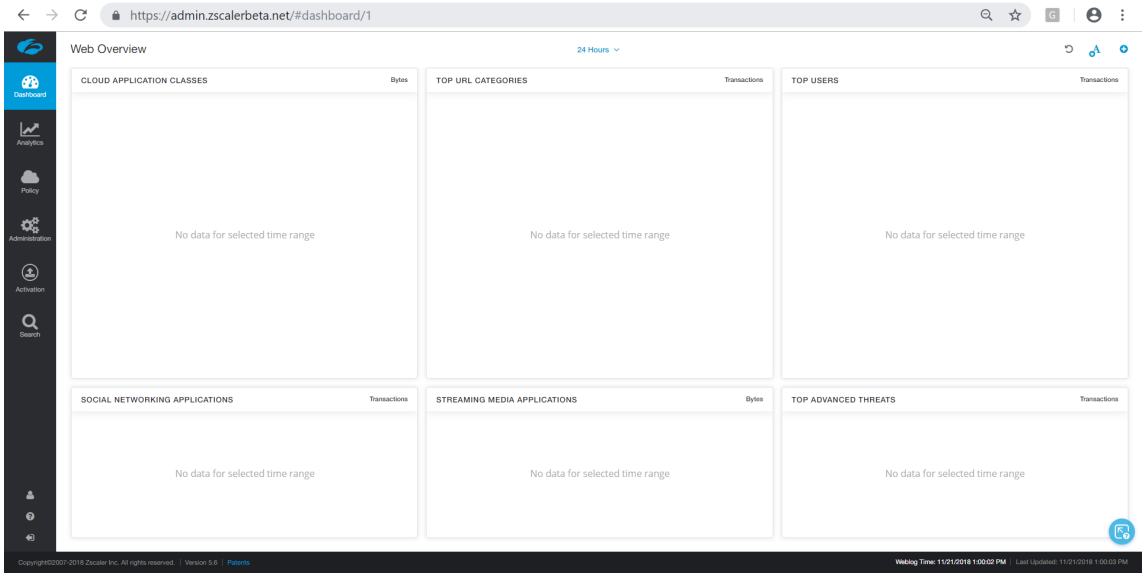
下面是在 SD-WAN Center 中定义用于部署 Zscaler 的工作流的高级别步骤。

1. 将 Zscaler 订阅配置为 SD-WAN Center（一次性）。登录 Zscaler 网站以获取订阅信息。
2. 在 Citrix SD-WAN Center GUI 中选择部署。
   - 使用 Internet WAN 链接和预先配置的应用程序对象部署站点的配置。
   - 建立连接。
   - 获取/更新 IPsec 状态。

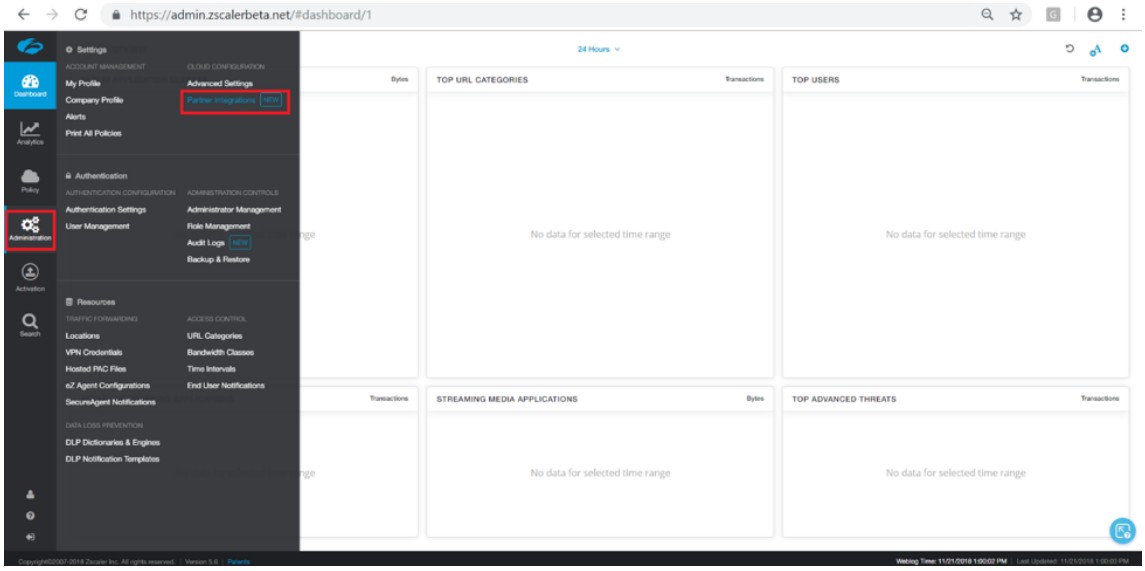
Zscaler 订阅

在 SD-WAN Center 中继续配置 Zscaler 之前，需要登录 Zscaler 门户。

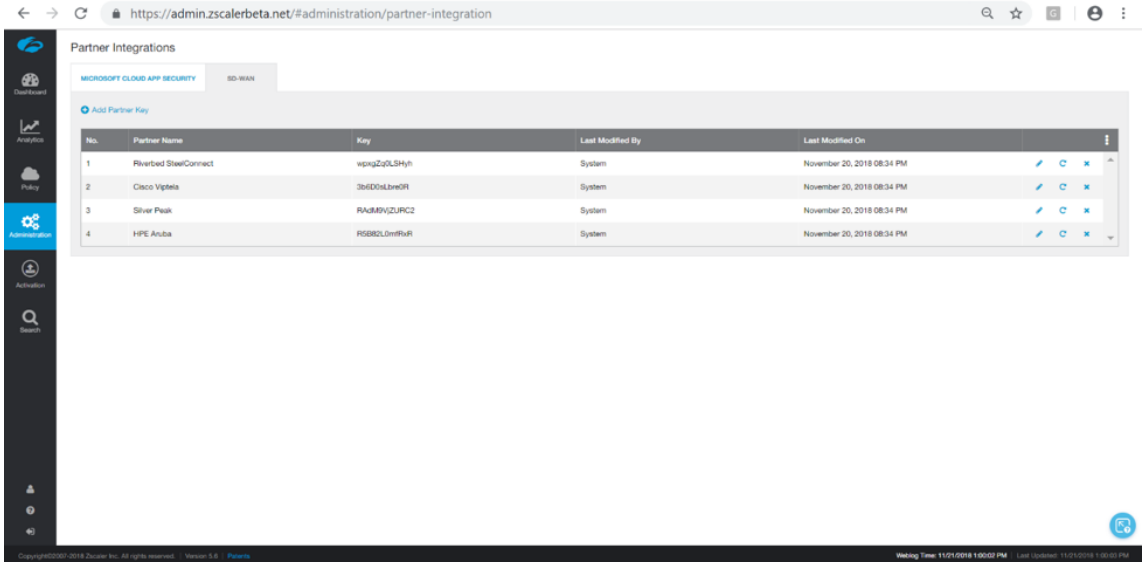
1. 登录 Zscaler 网站以获取订阅信息。此时将打开“控制板”页面。

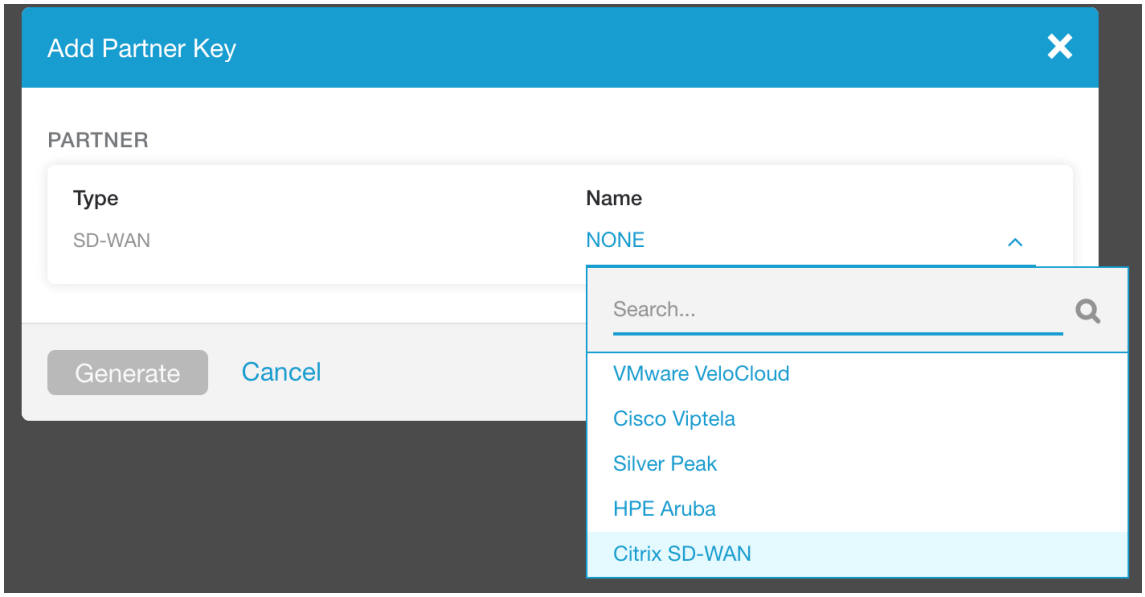


2. 单击管理 **>** 合作伙伴集成。



3. 在合作伙伴集成页面上，选择 **SD-WAN**。单击添加合作伙伴密钥。

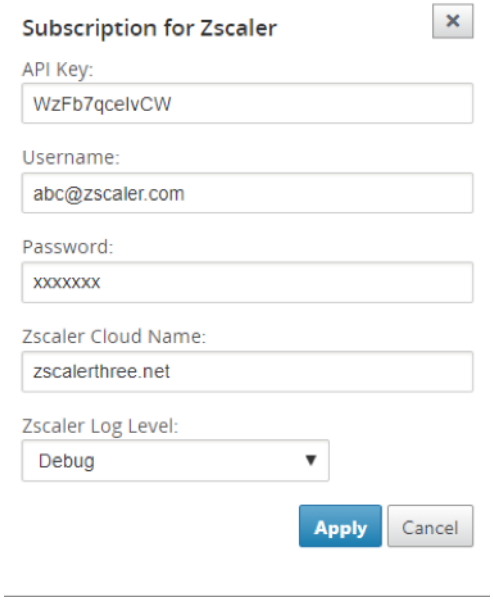




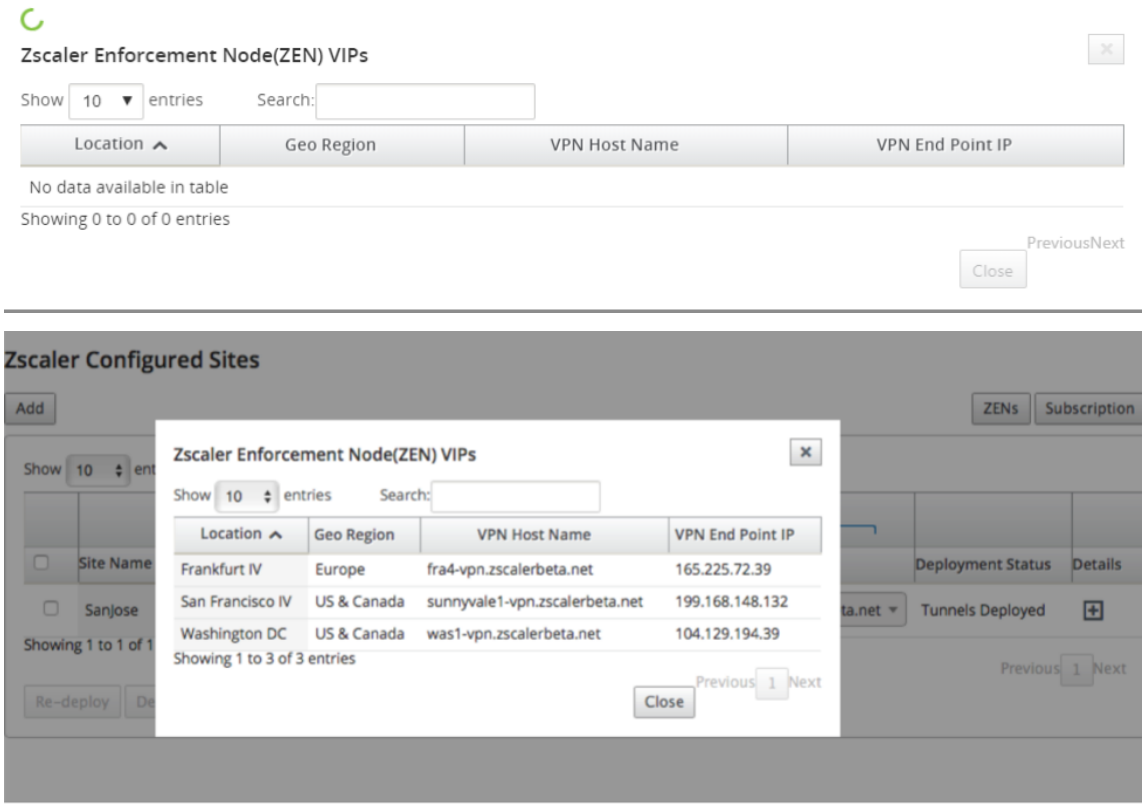
4. 为合作伙伴密钥选择 **Citrix SDWAN**，然后单击生成。存放钥匙。

在 **Citrix SD-WAN Center** 中配置 **Zscaler**

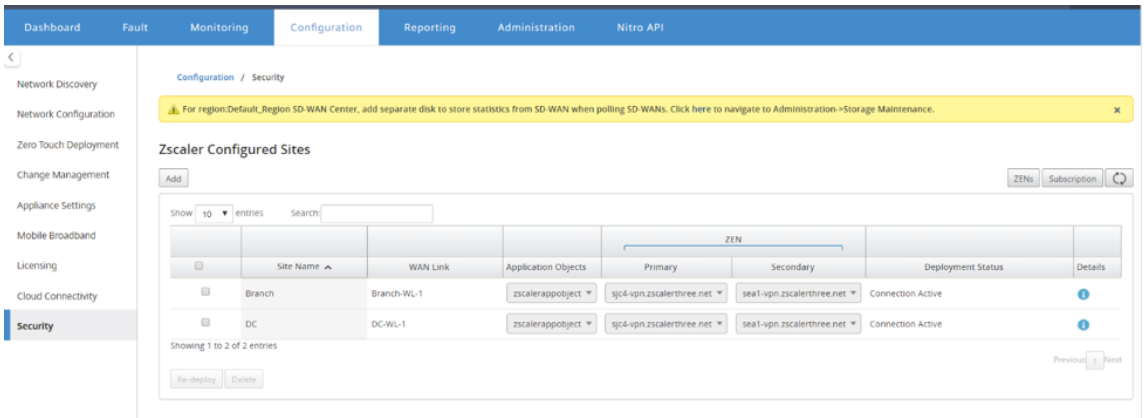
1. 在 Citrix SD-WAN Center GUI 中，导航到配置 **>** 安全页面。此时将打开 **Zscaler** 配置站点页面。
2. 单击订阅。输入在上述步骤中创建的 Zscaler API（合作伙伴密钥）。提供您的 Zscaler 用户名和密码。选择 **Zscaler Cloud** 名称、**Zscaler** 日志级别，然后单击应用。



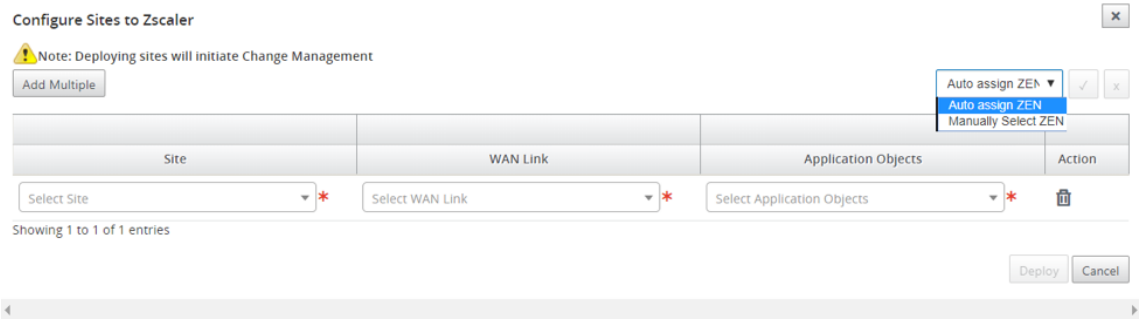
3. ZEN 提供此 Zscaler 云订阅的可用 VPN 端点的列表。



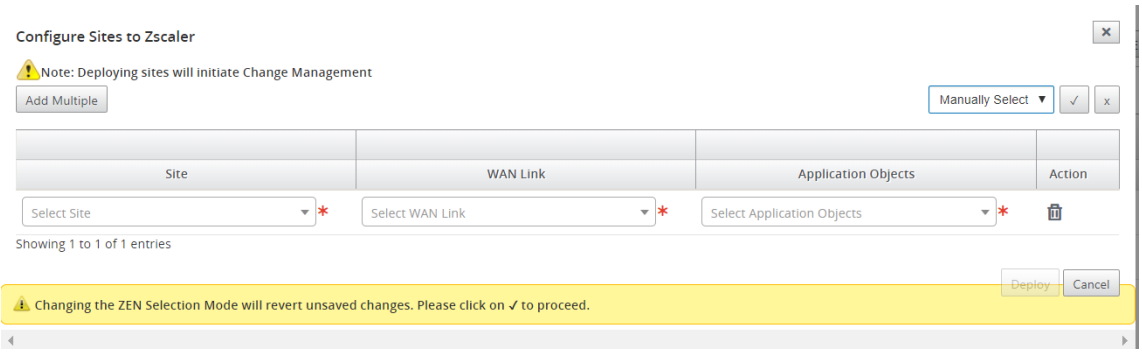
4. 输入 Zscaler 订阅和 ZEN 详细信息后，可以开始将站点添加到 Zscaler。单击添加。



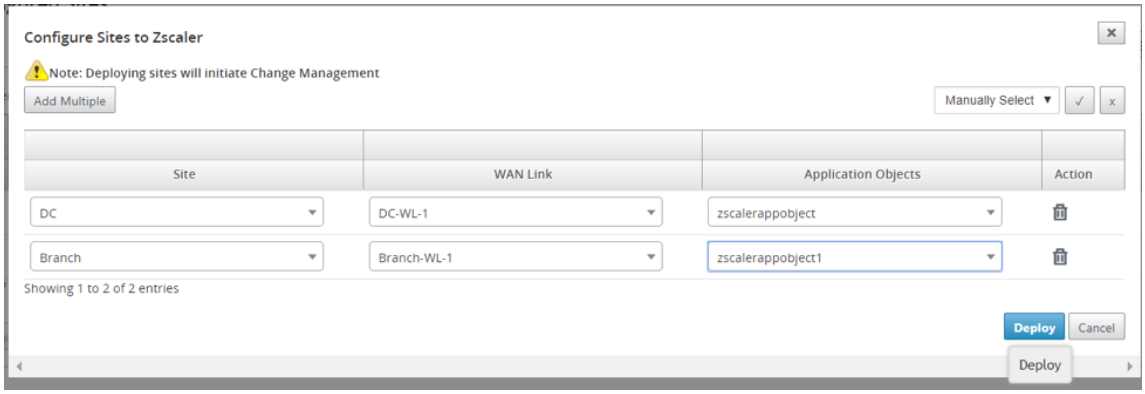
5. 在将站点配置为 **Zscaler** 对话框中，添加站点、**WAN** 链接和应用程序对象。默认情况下，自动分配 **ZEN** 选项处于选中状态。

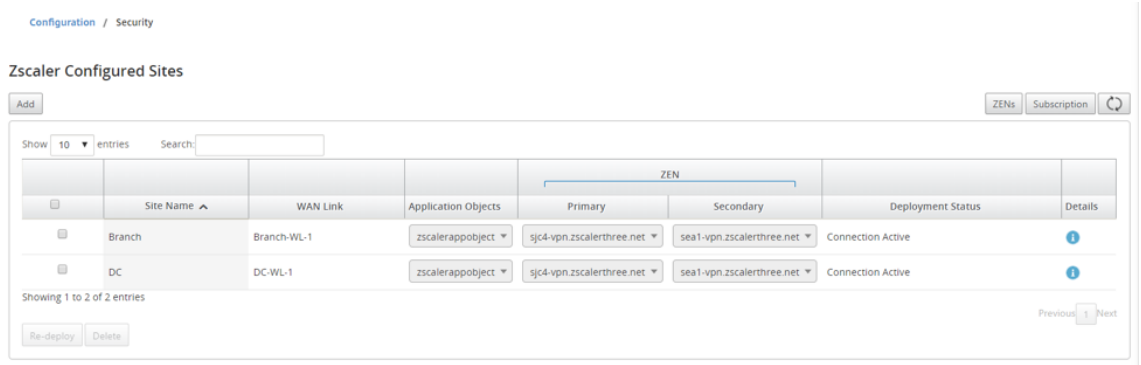


您可以手动选择 **ZEN**。但是，系统将显示以下消息，通知未保存的更改将丢失。



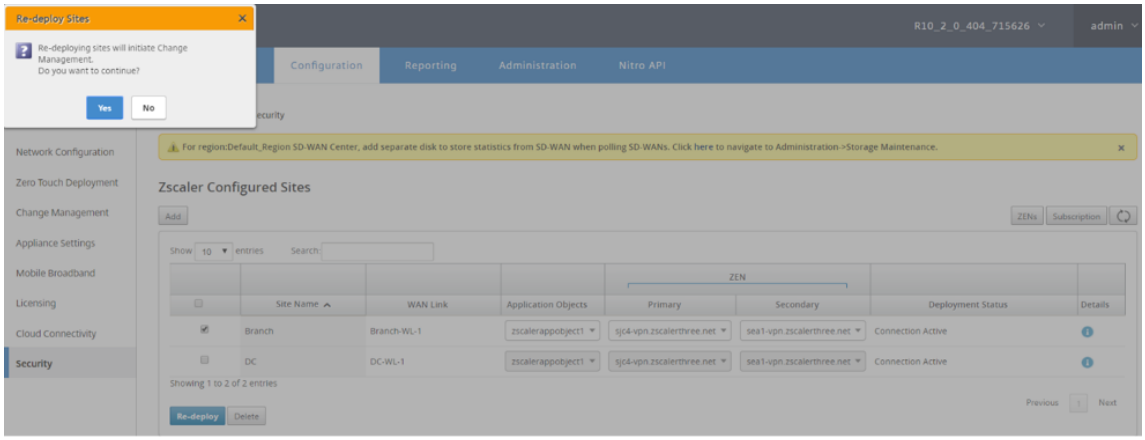
6. 选择所需的站点，然后单击部署。您可以通过选择添加多个站点来选择添加多个站点。将部署所选站点并显示配置页面。



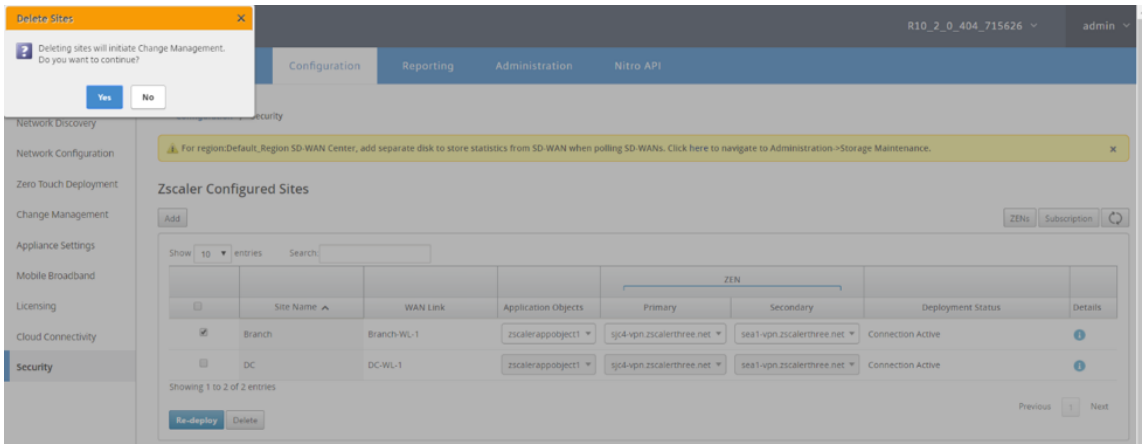


请注意，主和辅 ZEN IP 地址已填充，并且部署状态为连接处于活动状态。

7. 如果您更改了已配置站点的 VPN 端点或应用程序对象，请单击重新部署。对 SD-WAN Center 中已配置的站点所做的任何更改都将触发在分支站点和 DC 站点上配置的设备上的更改管理过程。

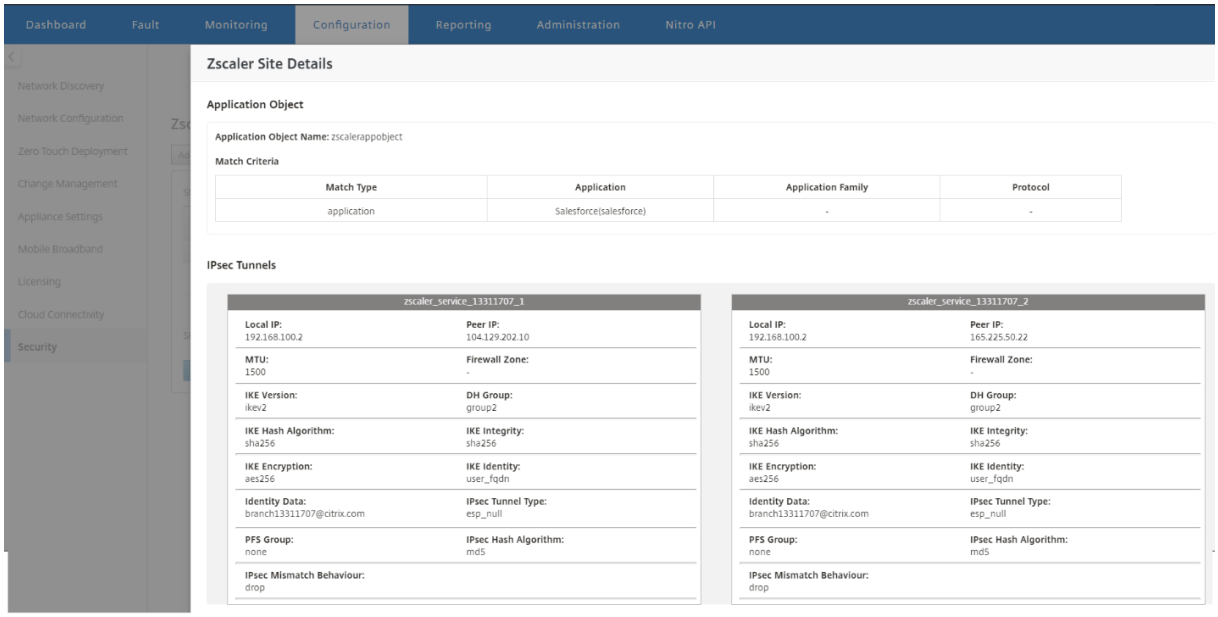


删除站点也会触发更改管理过程。



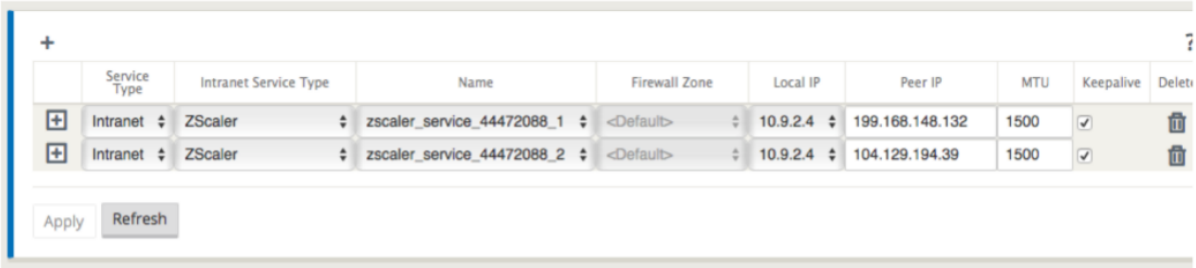
监视和故障排除

选择已配置的站点以查看有关应用程序对象和主/辅助 IP 地址的详细信息。您可以单击“详细 信息”图标以查看有关已配置站点的完整信息。



IPsec 隧道配置

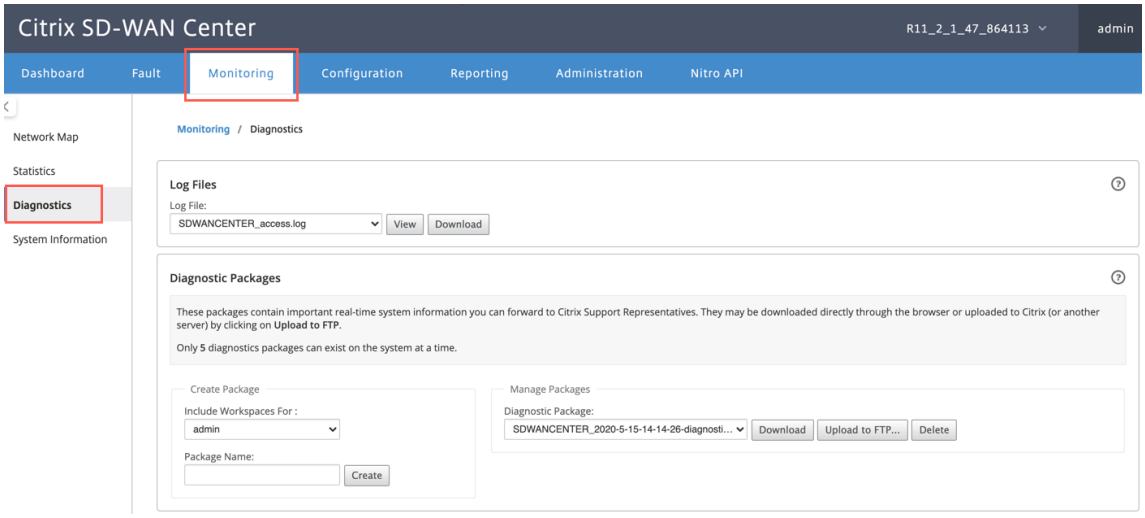
SD-WAN Center GUI 中的“详细信息”页面提供与主端点和辅助端点的 IPsec 通道配置有关的信息。对等 IP 是从 Zscaler 获得的。在 SD-WAN 设备 GUI 配置编辑器中验证 IPsec 通道配置。



您可以查看和下载 Zscaler 日志，这些日志可用于对 Citrix SD-WAN Center 中的问题进行故障排除。

要查看 Zscaler 日志文件：

1. 在 Citrix SD-WAN Center Web 界面中，单击 监视 选项卡 > 诊断。

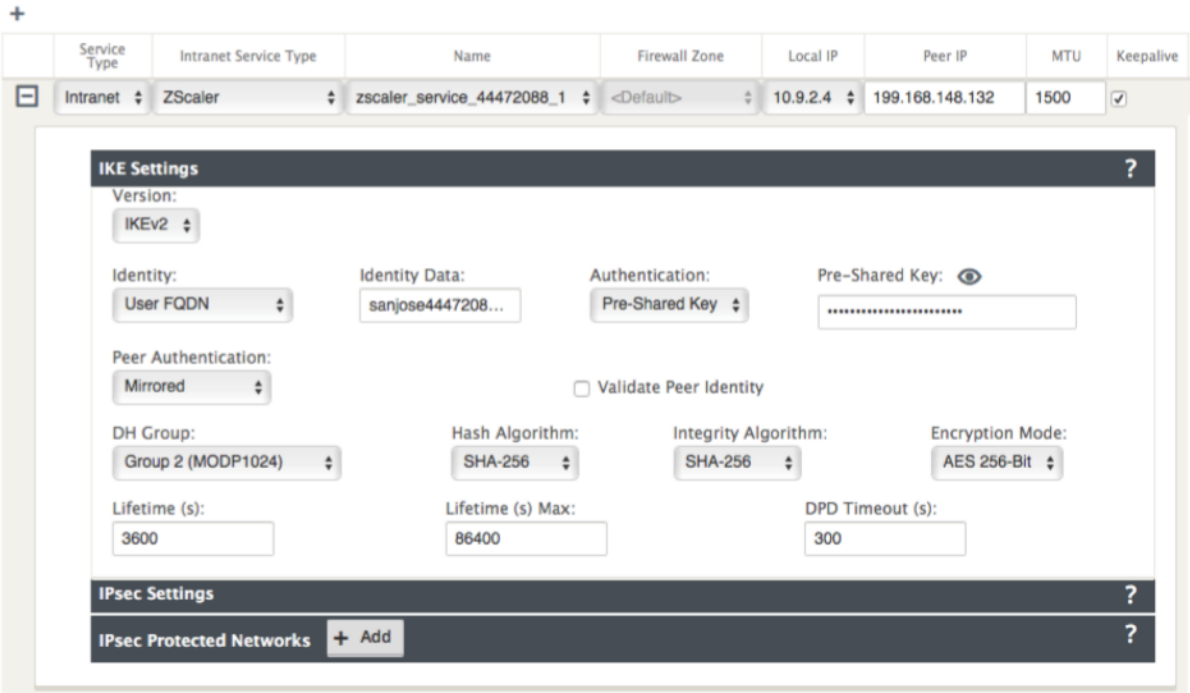


2. 从 日志文件 下拉列表中，选择要查看的 Zscaler 日志文件。单击查看。
3. 如果要将日志文件下载到您的计算机上，请单击下载。

IKE 设置

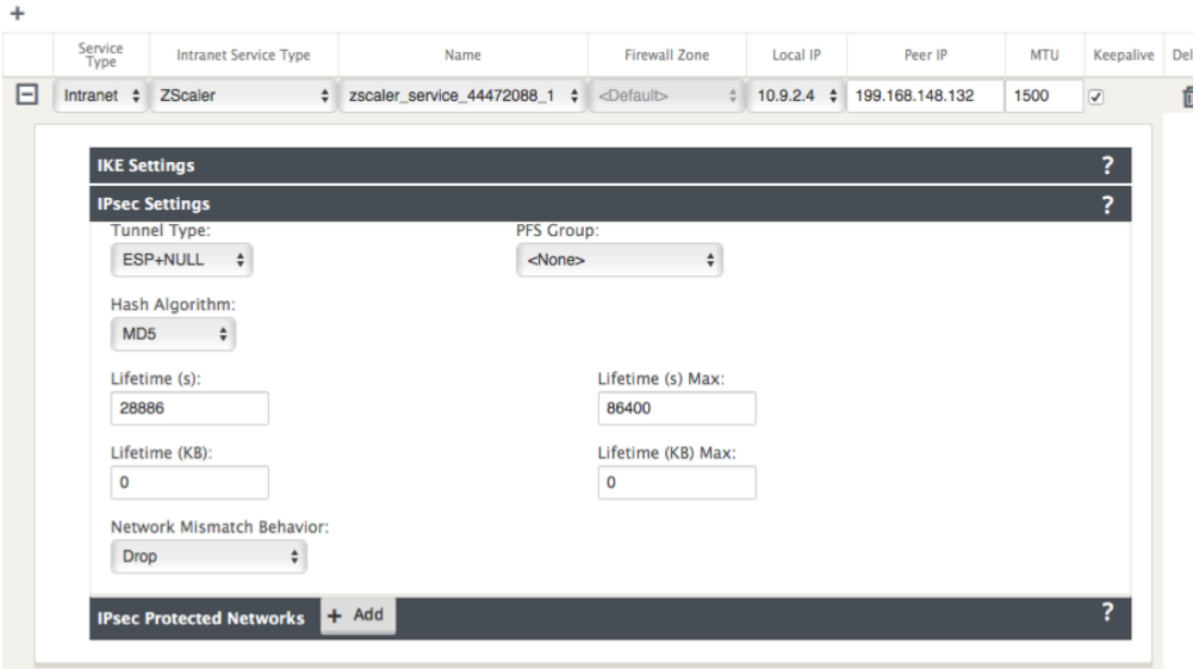
在 SD-WAN 设备中为 IPsec 通道配置选择以下 IKE/IPSec 设置。有关配置 IPsec 通道–IKE 设置的详细信息，请参阅如何在 SD-WAN 和第三方设备之间配置 IPsec 隧道主题。

- IKE 版本 - IKEv2
- IKE 身份—用户 FQDN
- 哈希算法 - SHA-256
- 完整性算法—SHA-256
- 加密模式—AES 256 位
- IPSec —隧道模式
- IPsec 加密—空



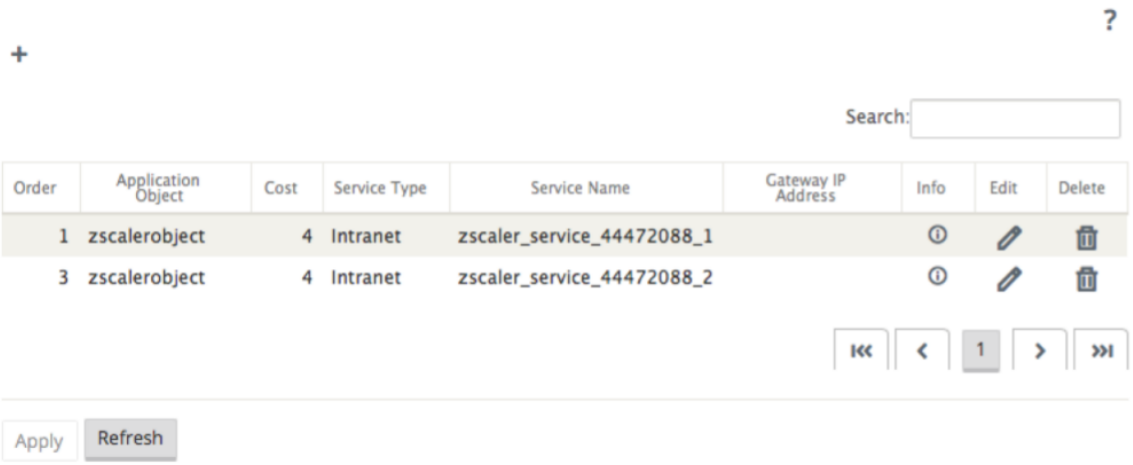
IPsec 设置

有关配置 IPsec 通道设置的详细信息，请参阅如何在 SD-WAN 和第三方设备之间配置 IPsec 隧道主题。



应用程序对象

确保已配置应用程序对象。有关配置应用程序路由的详细信息，请参阅应用程序分类主题。



> 注意：
>
> 作为自动化工作流的一部分，不支持 GRE 隧道配置。但是，仍允许手动配置。有关详细信息，请参阅使用 GRE 通道和 IPsec 通道的 Zscaler 集成。

监视

April 13, 2021

Citrix SD-WAN Center 控制板允许您在单个窗格中查看 SD-WAN 网络统计信息和图形。有关详细信息，请参阅控制板。

您还可以在 Citrix SD-WAN Center 中查看 SD-WAN 网络事件和报告。

监视相关文章：

诊断包

事件通知

日志文件

内存转储

轮询时间间隔

统计信息

系统信息

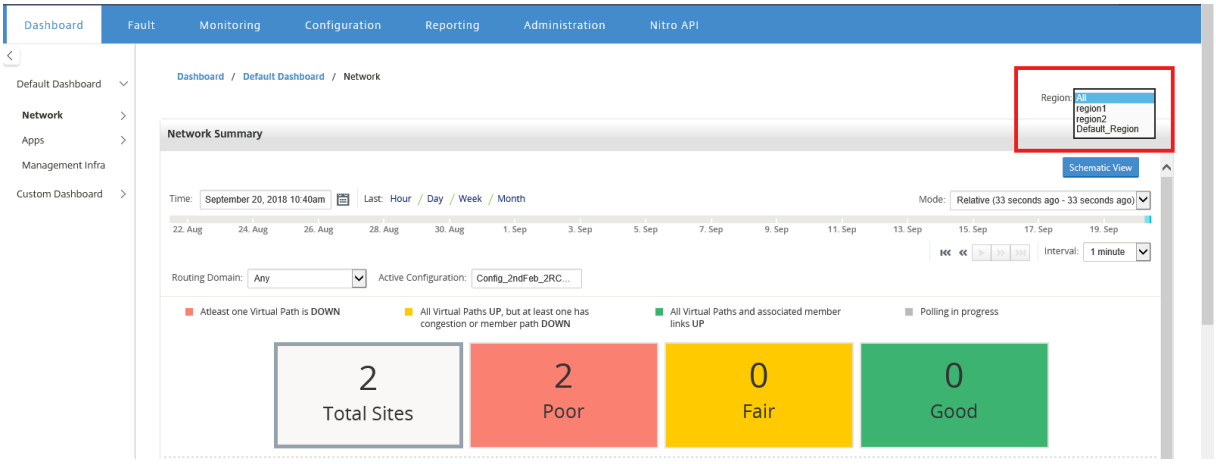
控制板

April 13, 2021

Citrix SD-WAN Center 控制板一目了然地显示常见统计信息的子集。对于单区域部署，将从 Citrix SD-WAN Center 中发现的 MCN 获取统计信息。对于多区域部署，将从所有区域性 Citrix SD-WAN Center 收集器获取所选时间间隔的统计信息。您可以查看以下统计信息：

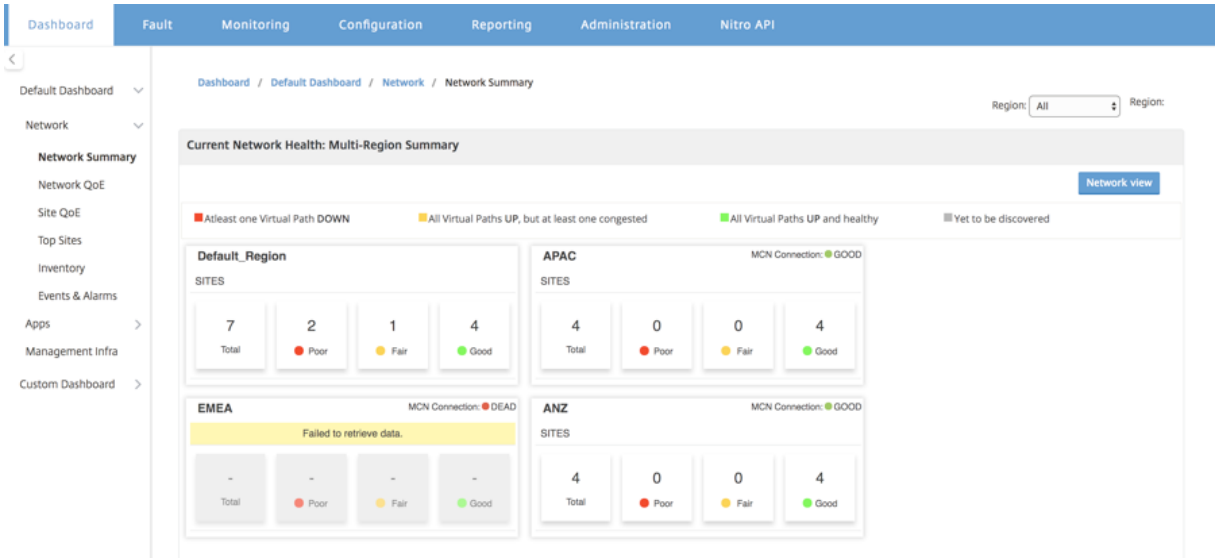
- 网络摘要
- 网络 QoE
- 热门站点
- 清单
- 事件和警报
- 热门应用
- HDX QoE
- 管理基础结构

对于单区域部署，系统会在控制板上显示默认的区域统计信息。对于多区域部署，可以选择查看多区域控制板或区域控制板。要查看多区域控制板，请在区域菜单中选择全部。



您可以在每个区域磁贴上查看 MCN 连接状态。MCN 连接状态是 RCN 和 MCN 之间虚拟路径的运行状况。

> 注意
>
> 对于多区域部署，默认的区域统计信息包含 MCN 管理的所有站点的统计信息。它还可能包括 RCN 的统计数据，因为 RCNs 具有 MCN 的虚拟路径。
>
> 地区下拉菜单在 Citrix SD-WAN Center 收集器中不可用。



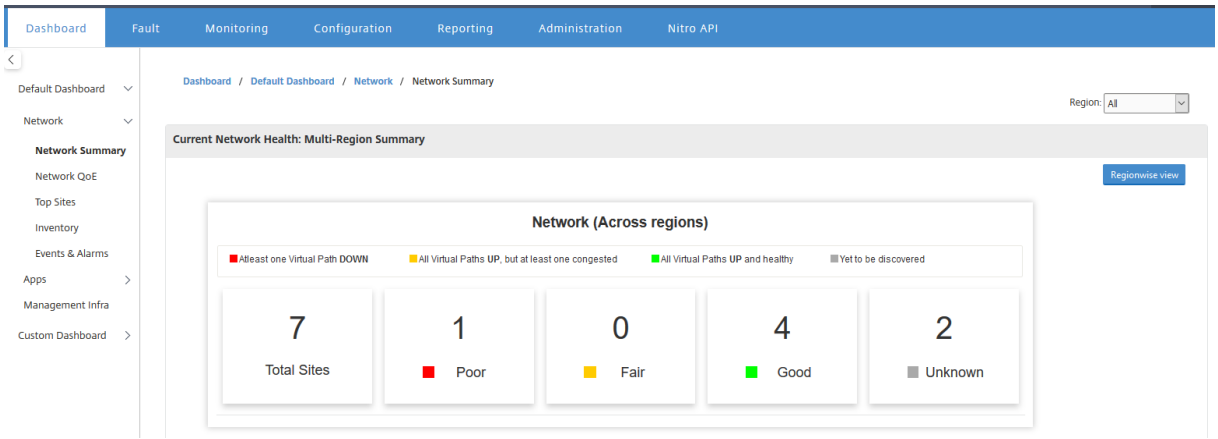
此时将根据所配置的轮询时间间隔刷新 Citrix SD-WAN Center 控制板。默认轮询时间间隔为 5 分钟。有关详细信息，请参阅轮询时间间隔。

网络摘要

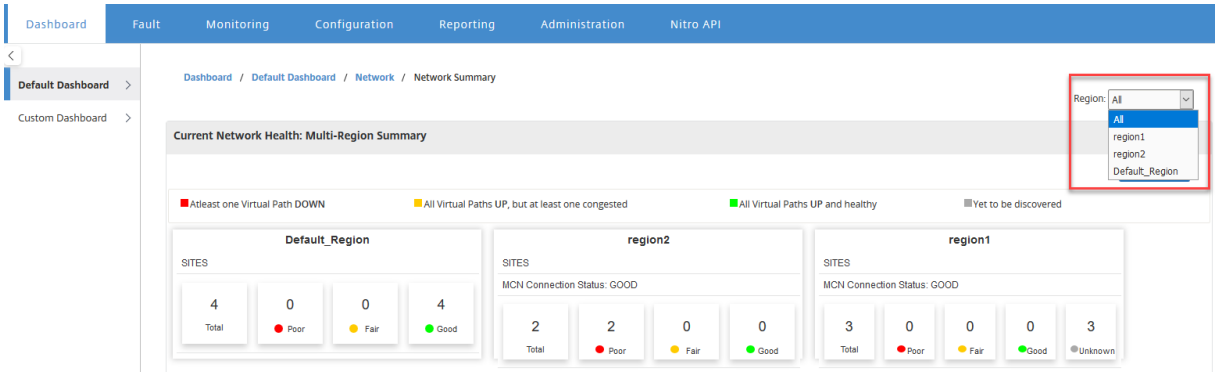
对于多区域部署，网络摘要小组件概述了所有不同区域的网络运行状况。将显示网络中每个区域的地区卡，其中包含以下信息：

- 该地区的站点总数。
- 处于“差”状态的站点数量。当至少有一个虚拟路径为“关闭”时，站点处于较低状态。
- 处于博览会状态的网站数量。如果站点中的所有虚拟路径都已启动，但至少有一个路径出现拥堵问题或者成员路径已关闭，站点将处于公平状态。
- 处于良好状态的站点数量。所有虚拟路径和关联的成员路径都设置为“正常”时，站点处于良好状态。
- 处于“未知”状态的站点数量。轮询正在进行时，站点处于“未知”状态。

要查看多区域网络摘要，请导航到控制板 > 默认控制板 > 网络 > 网络摘要，然后在区域下拉菜单中，选择全部。



默认情况下，屏幕在网络视图中显示。您可以通过单击区域明智视图查看多区域网络摘要的当前网络运行状况。您还可以在每个区域磁贴上查看 MCN 连接状态。



单击区域卡可向下钻取到区域控制板。

对于单个区域，网络摘要小组件提供了所选区域的网络运行状况概述。

要查看区域网络摘要，请导航到控制板 > 默认控制板 > 网络 > 网络摘要，然后在地区下拉菜单中选择一个区域。

您可以在切片视图或逻辑示意图视图中查看区域网络摘要。

可以使用“日程表”控件查看选定时间段内的网络状态摘要。您还可以在一段时间范围内播放或暂停网络状态。

模式有助于将时间视为相对或绝对概念。

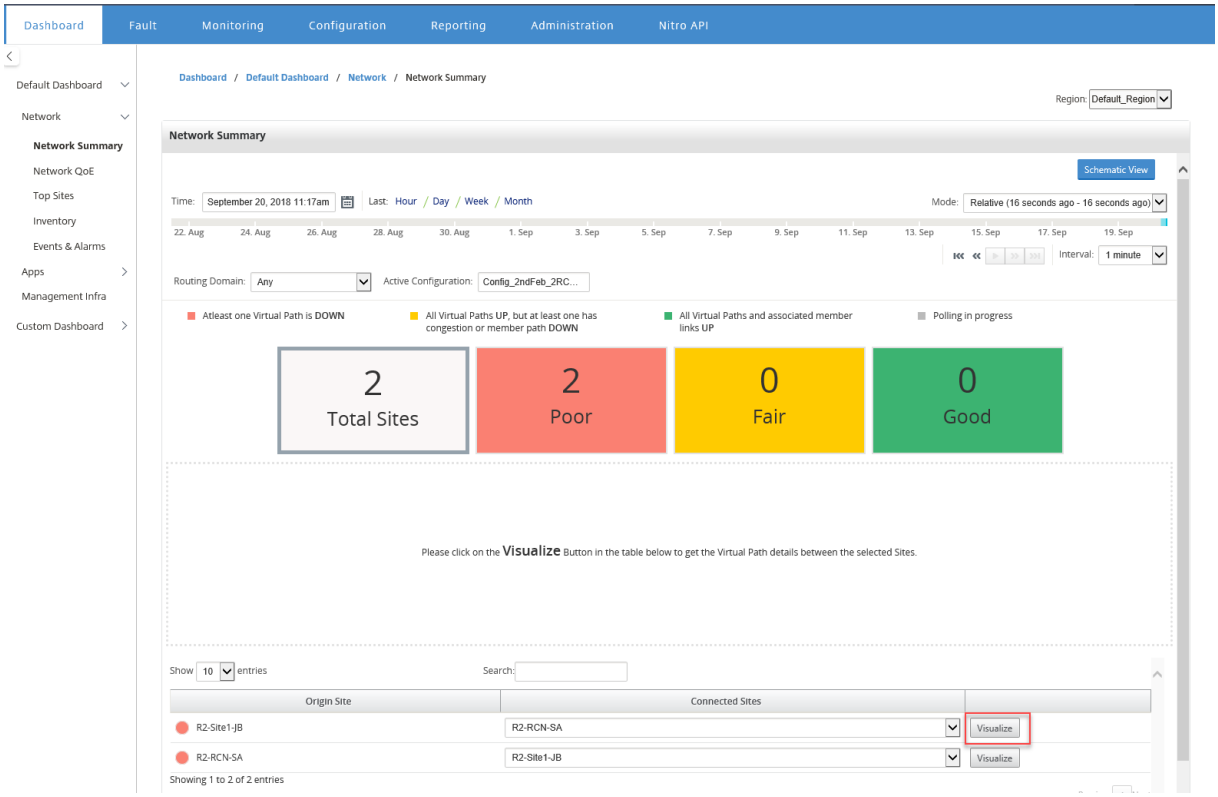
有关时间线和模式的详细信息，请参阅时间线控件。

瓷砖视图

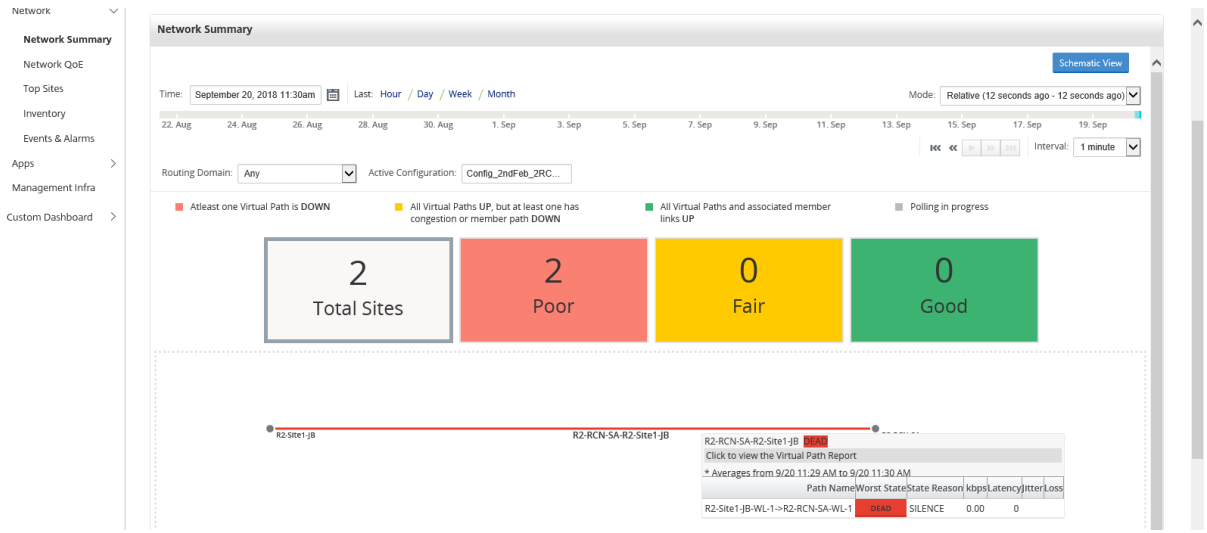
平铺视图提供以下信息：

- 该地区的站点总数。
- 处于“差”状态的站点数量。当至少有一个虚拟路径为“关闭”时，站点处于较低状态。
- 处于博览会状态的网站数量。如果站点中的所有虚拟路径都已启动，但至少有一个路径出现拥堵问题或者成员路径已关闭，站点将处于公平状态。
- 处于良好状态的站点数量。所有虚拟路径和关联的成员路径都设置为“正常”时，站点处于良好状态。
- 处于“未知”状态的站点数量。轮询正在进行时，站点处于“未知”状态。

要查看两个站点之间的路径的图形表示，请选择该路径，然后单击显示。



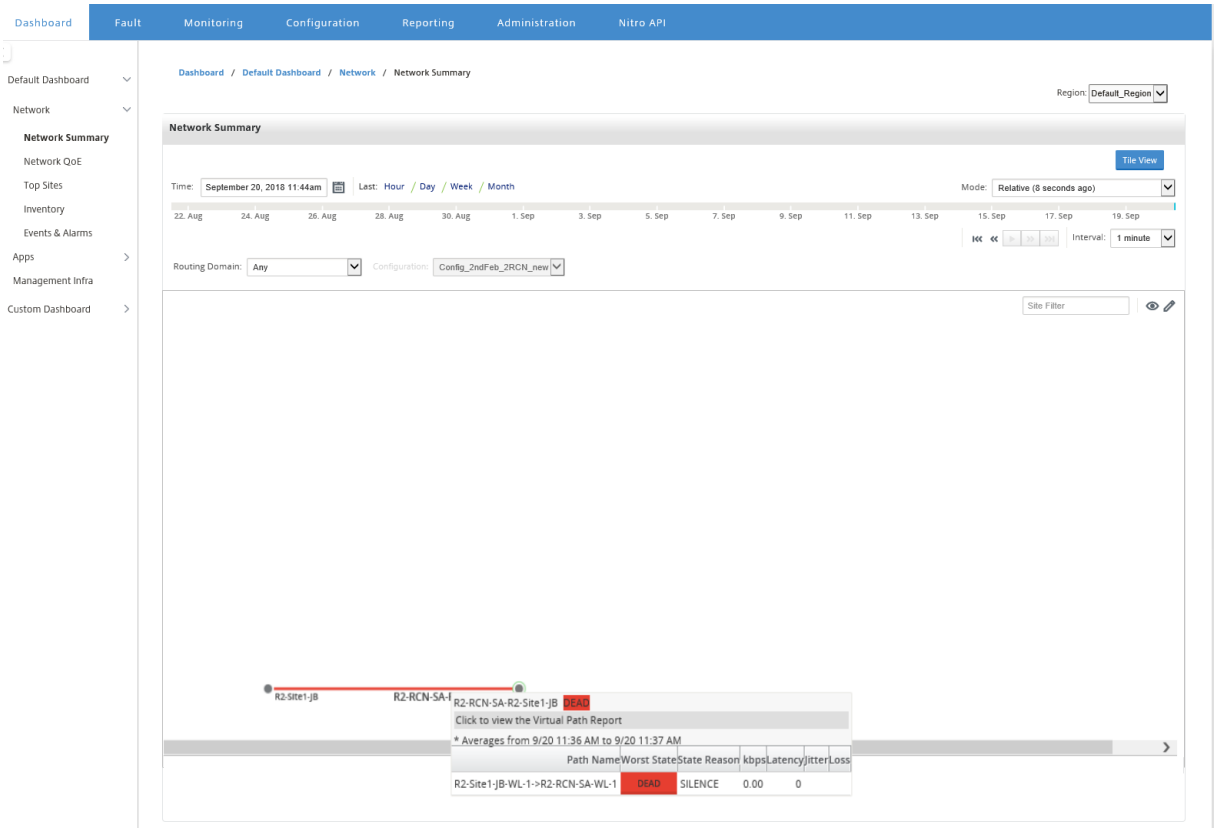
将鼠标光标悬停在站点或路径上以查看更多详细信息。单击要查看的站点，然后选择报告选项。



示意图视图

示意图视图提供 SD-WAN 网络的图形视图。此部分中显示的信息将根据所选配置和路由域进行更新。要在此处查看网络映射，必须从主控制器节点 (MCN) 导入网络配置和网络映射。有关详细信息，请参阅 导入 MCN 配置。

将鼠标光标悬停在站点或路径上以查看更多详细信息。单击站点以查看报告选项。

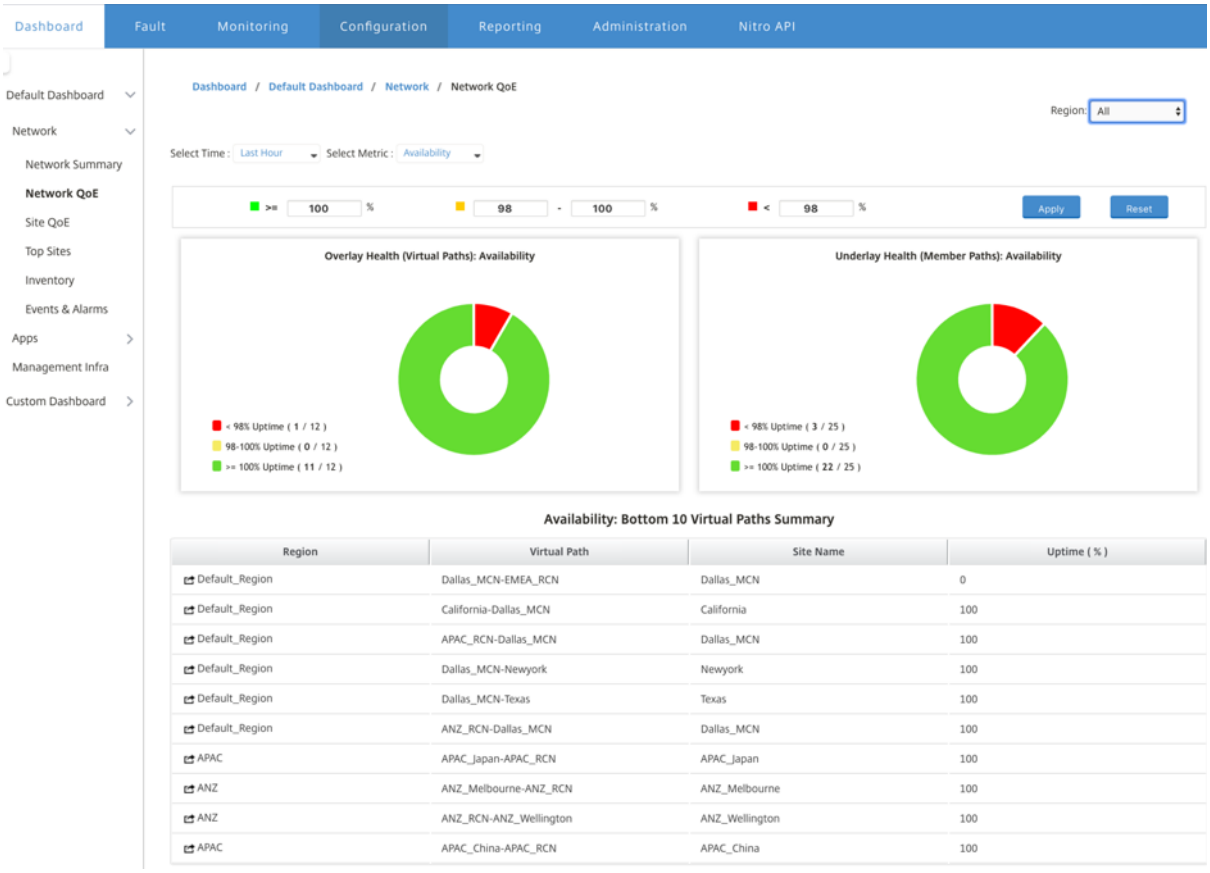


网络 **QoE**

网络 **QoE** 小组件提供了虚拟路径的可用性、丢失、延迟以及抖动参数的图形表示形式。它提供覆盖虚拟路径和底层成员路径的统计信息。

对于多区域部署，可以根据所选指标查看底部 10 个虚拟路径的列表。在所选时间间隔内，将从所有区域收集器收集虚拟路径数据。您可以查看最需要注意的虚拟路径的带宽、抖动、损耗和拥塞详细信息。

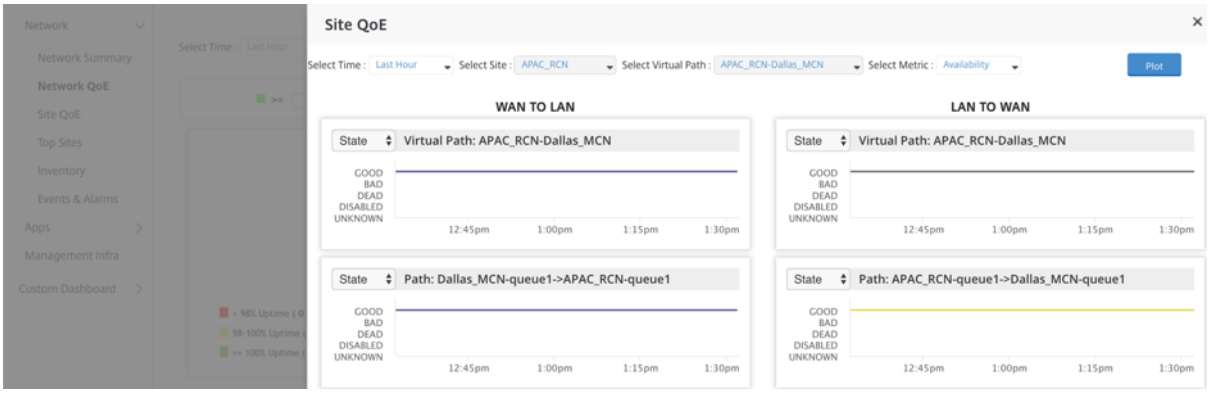
要查看多区域虚拟路径运行状况，请导航到控制板 > 默认控制板 > 网络 > 网络 **QoE** ，然后在地区下拉菜单中选择全部。



对于单个区域，可以根据所选指标查看底部 10 个虚拟路径的列表。在选定的时间间隔内收集统计信息。您可以查看最需要注意的虚拟路径的带宽、抖动、损耗和拥塞详细信息。

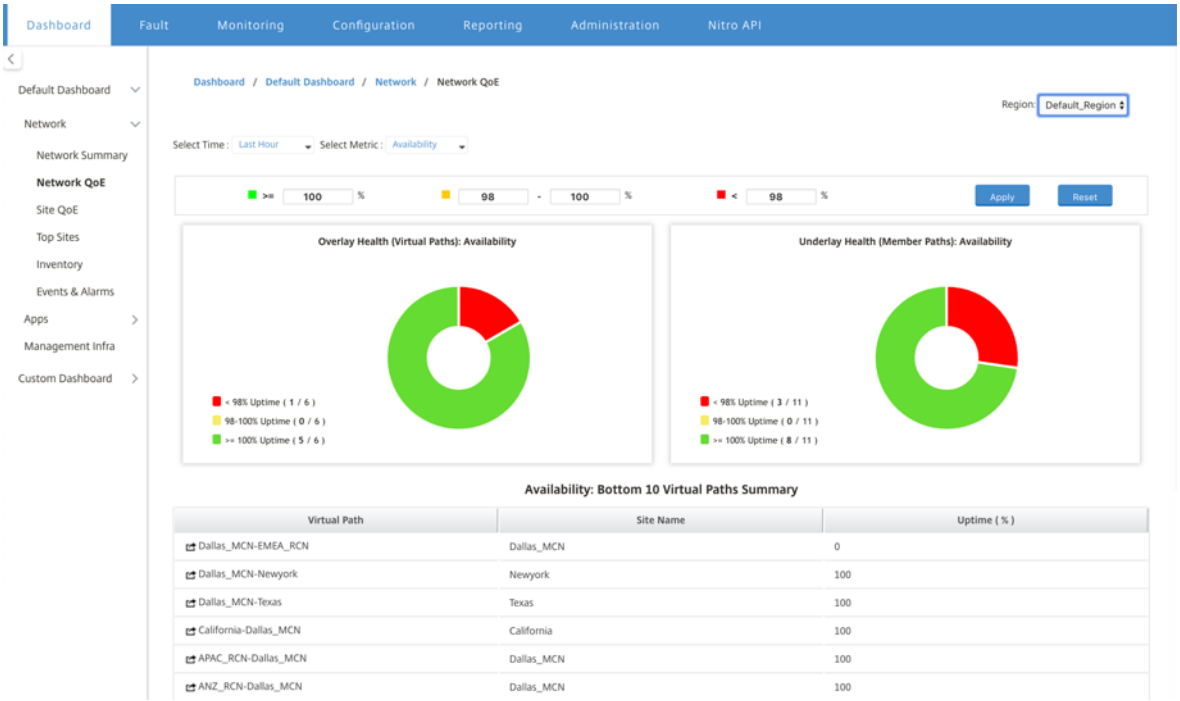
可以在选定的时间间隔内比较所选指标（可用性、丢失、抖动、延迟）的覆盖和底层路径。您还可以设置指标的自定义阈值，并在单击应用时保存它们。单击重置以存储默认阈值。

用户还可以通过使用每行左侧的向下钻取按钮 向下钻取 到表中的任何虚拟路径。此时将显示一个站点 **QoE** ，其中包含管道及其基础成员路径之间的详细比较。



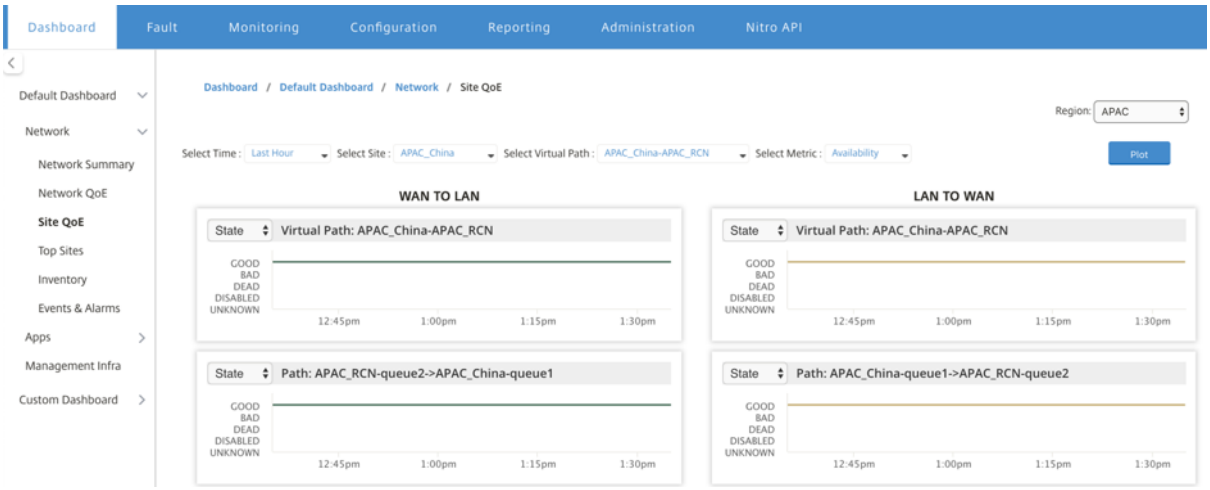
在该滑块中，根据您单击的行选择站点名称和虚拟路径，并将其禁用。但是，用户可以选择不同的时间范围和指标，然后单击“绘图”选项以绘制新图表。

要查看区域虚拟路径运行状况统计信息，请导航到控制板 > 默认控制板 > 网络 > 网络 **QoE**，然后在地区下拉菜单中选择一个区域。



网站 **QoE**

您可以使用 Site QoE 作为比较虚拟路径及其底层成员路径的工具。您需要从此站点和指标中选择一个站点和任何虚拟路径。单击绘图。

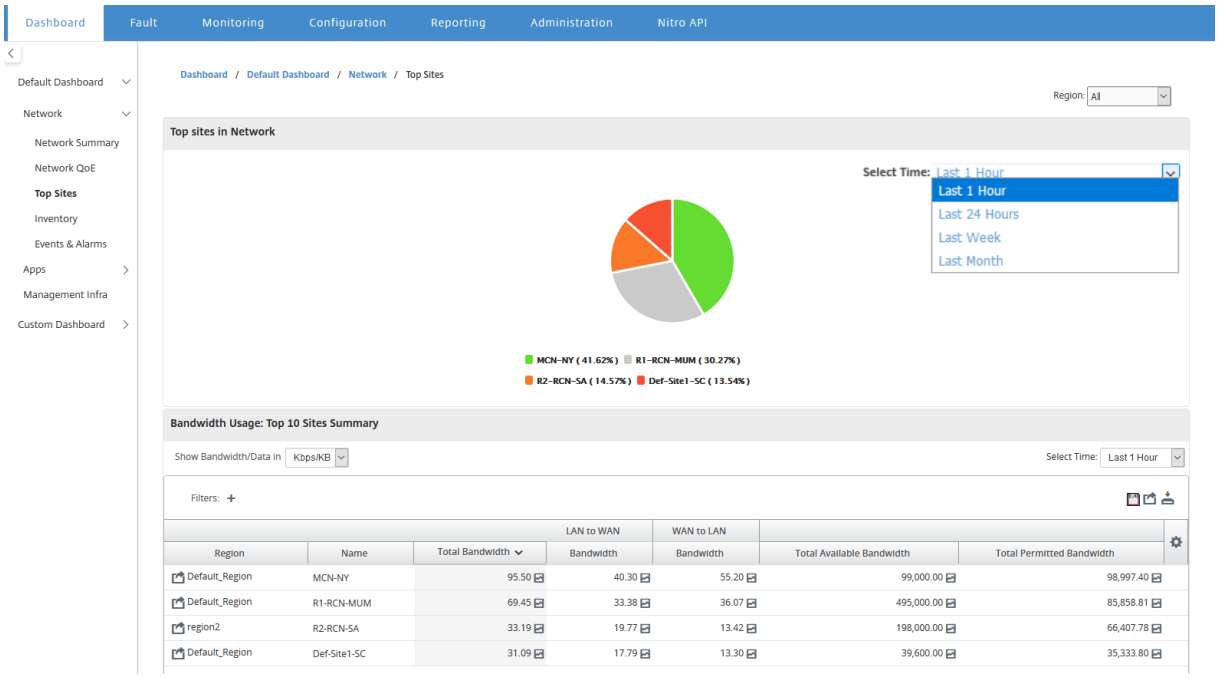


在第一节中，它会绘制 **WAN** 到 **LAN** 和 **LAN** 到 **WAN** 方向中的虚拟路径统计信息绘制到。下面的部分将绘制所有底层成员路径图表。这两种情况在区域和网络层面都存在。

热门站点

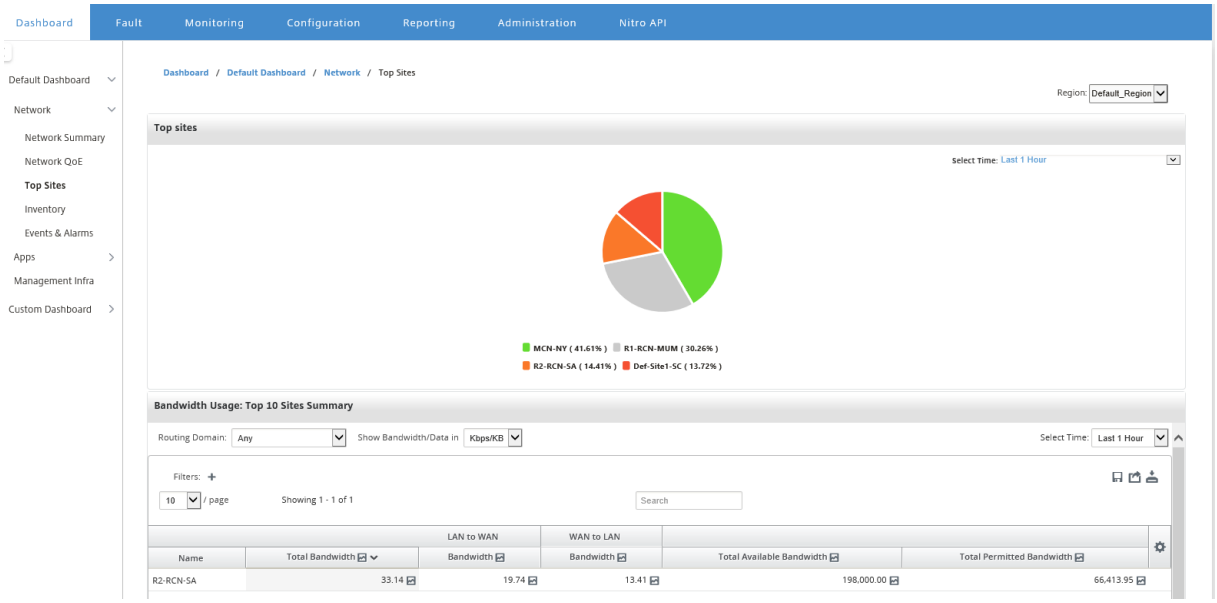
对于多区域部署，热门站点小组件将在选定的时间间隔内列出所有区域中的前 10 个站点（具有最高带宽使用情况）。

要查看所有区域中的最上面的站点，请导航到控制板 > 默认控制板 > 网络 > 热门站点，然后在地区下拉菜单中选择全部。



单击站点或指标可查看详细的报告和统计信息。

对于单个区域，”热门站点”小组件显示该区域中所有站点的带宽使用情况统计信息。在选定的时间间隔内收集统计信息。您可以根据路由域过滤站点。



清单

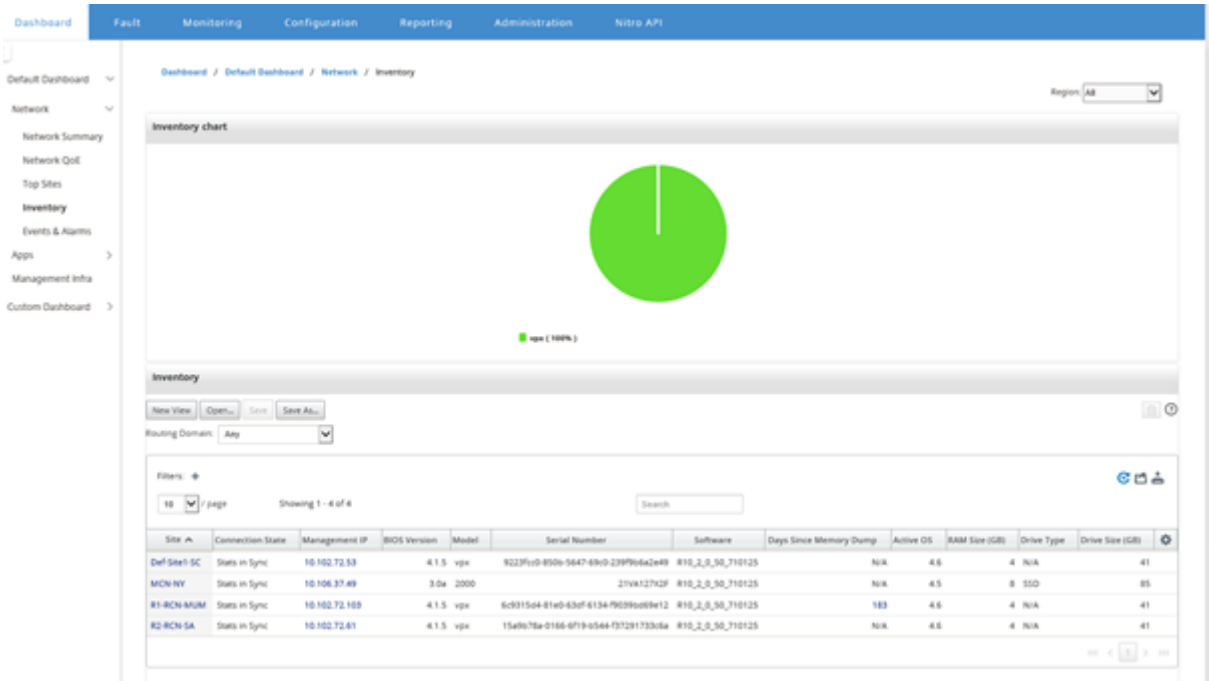
每 30 分钟，清单管理器都会从在 Citrix SD-WAN Center 上发现的所有 Citrix SD-WAN 设备收集硬件信息。

要查看多区域库存统计数据，请导航到控制板 > 默认控制板 > 网络 > 清单，然后在地区下拉菜单中选择。

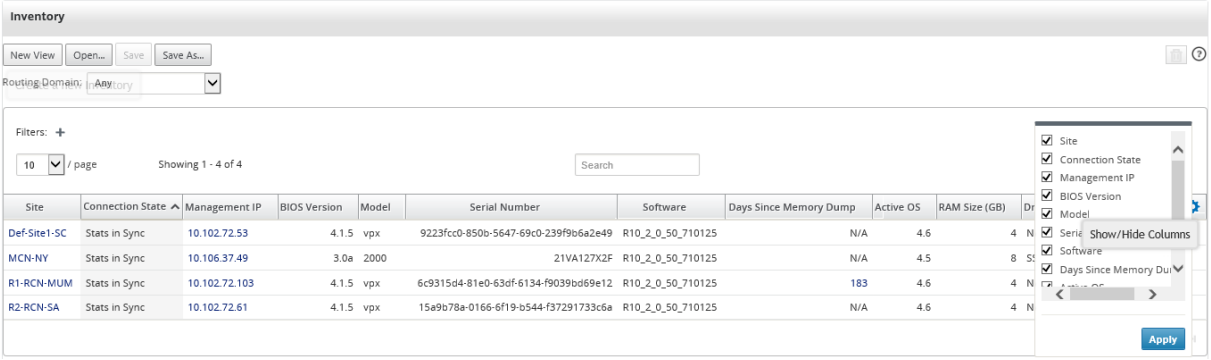
要查看特定区域的清单统计信息，请在区域下拉菜单中选择该区域。

您可以查看以下清单统计信息：

- 站点：在 MCN 中运行的配置中找到的站点的名称。如果设备是辅助 MCN，则名称旁边会显示“(辅助)”。您可以单击该名称以访问设备 Web 控制台。
- 连接状态：连接到设备的状态。连接无法访问或未通过身份验证时，将显示一个红色图标。
- 管理 **IP**：设备的管理 IP 地址。您可以单击该 IP 地址以访问设备 Web 控制台。
- **BIOS** 版本：设备的 BIOS 版本。
- 型号：设备的硬件型号。
- 序列号：设备的序列号。
- 软件；SD-WAN 软件版本号。
- 自内存转储后经过的天数：自上次系统错误内存转出起经过的时间。如果设备在过去的四天内转储了内存，则会在时间旁边显示错误图标。如果在 5 到 10 天前发生内存转储，则会显示警告图标。如果没有可用的转储，将显示 N/A。单击此时间将打开 SD-WAN 的“日志”页面。
- 活动操作系统：设备上当前运行的操作系统。
- **RAM** 大小 **(GB)**：设备上当前安装的容量 (GB)。
- 驱动器类型：设备上安装的数据存储驱动器类型。该值可以是 SSD（固态驱动器），也可以是 HDD（硬磁盘驱动器）。
- 驱动器大小 **(GB)**：设备上当前安装的数据存储驱动器的大小 (GB)。



> 注意
>
> 您可以使用显示/隐藏列选项来排列库存统计表的列。



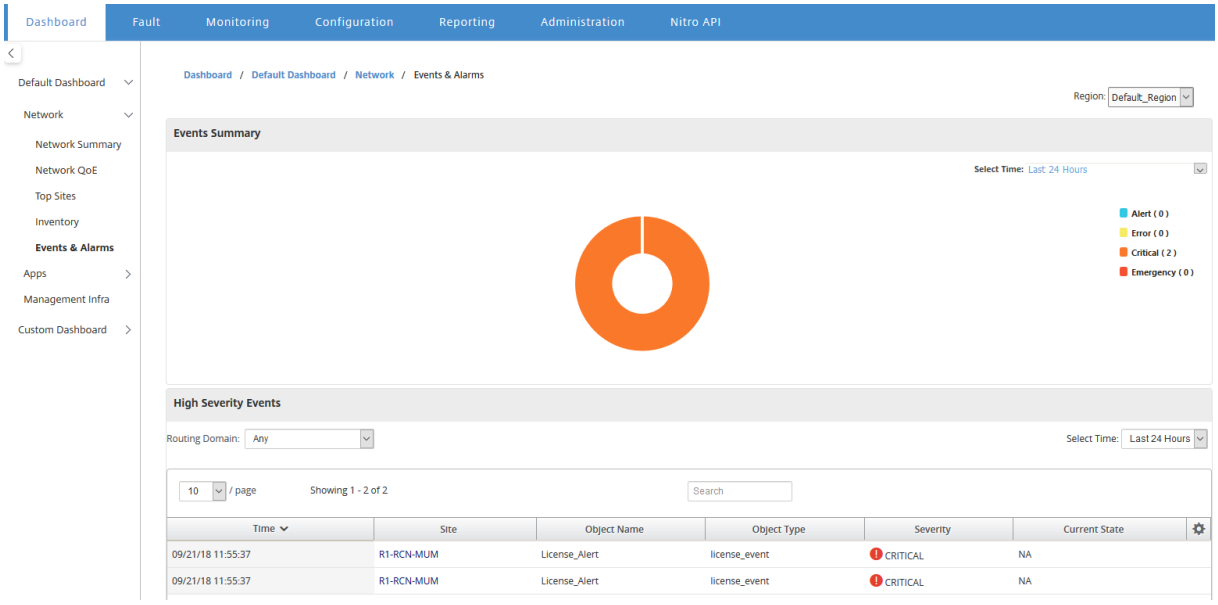
事件和警报

对于多区域部署，可以查看网络中所有区域的事件和警报。此信息将在选定的时间间隔内收集。要查看多区域事件和统计信息，请导航到控制板 > 默认控制板 > 网络 > 事件和警报，然后在地区下拉菜单中选择全部。

您还可以查看单个区域的所有事件和警报。此信息将在选定的时间间隔内收集。要查看事件和警报统计信息，请导航到控制板 > 默认控制板 > 网络 > 事件 **&** 警报，然后在地区下拉菜单中选择一个区域。

事件摘要部分提供了有关事件类型和事件数量的图形化概览。您可以单击图表以查看 故障 页面上的事件。该展示还概述了每个类别中有多少个事件。可以在单个 SD-WAN 设备上配置警报触发器。有关详细信息，请参阅事件通知。

高严重性事件部分显示严重事件的列表。您可以根据路由域过滤事件。本节中显示的信息是从故障选项卡收集的。有关详细信息，请参阅事件。

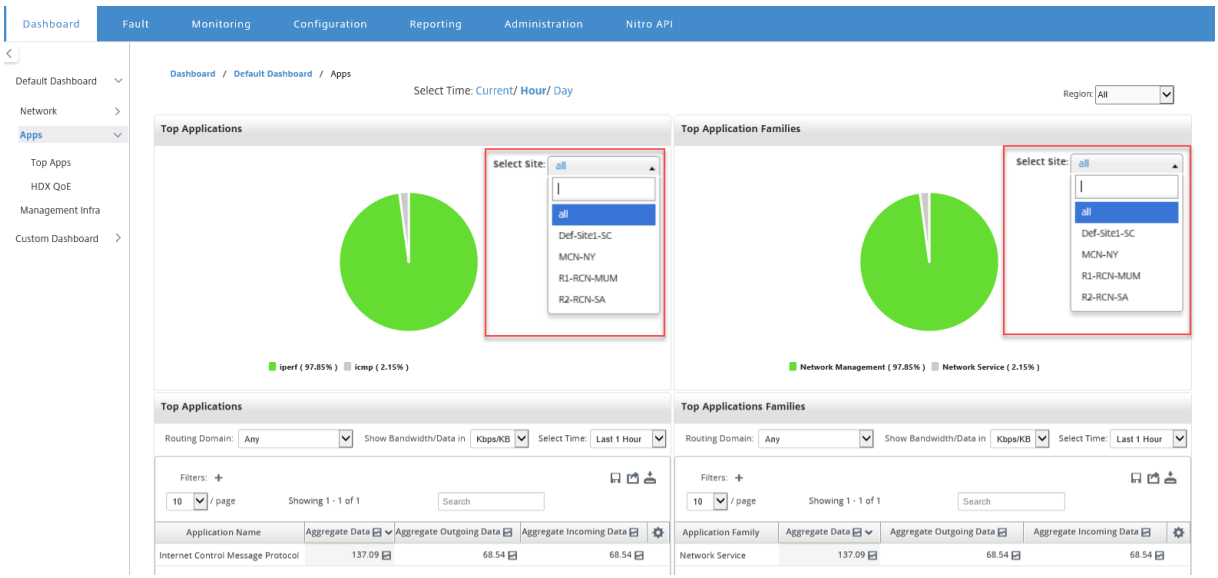


应用程序

排名前几位的应用程序

通过深数据包检查 (DPI)，SD 设备可以解析通过其传输的流量，并确定应用程序和应用程序系列类型。对于多区域部署，可以在网络中的所有地区查看最上面的应用程序和热门应用程序系列。此信息将在选定的时间间隔内收集。

要在网络中的所有区域中查看最高的应用程序统计信息，请导航到控制板 > 默认控制板 > 应用程序 **>** 热门应用程序**,** 然后在地区下拉菜单中选择全部。

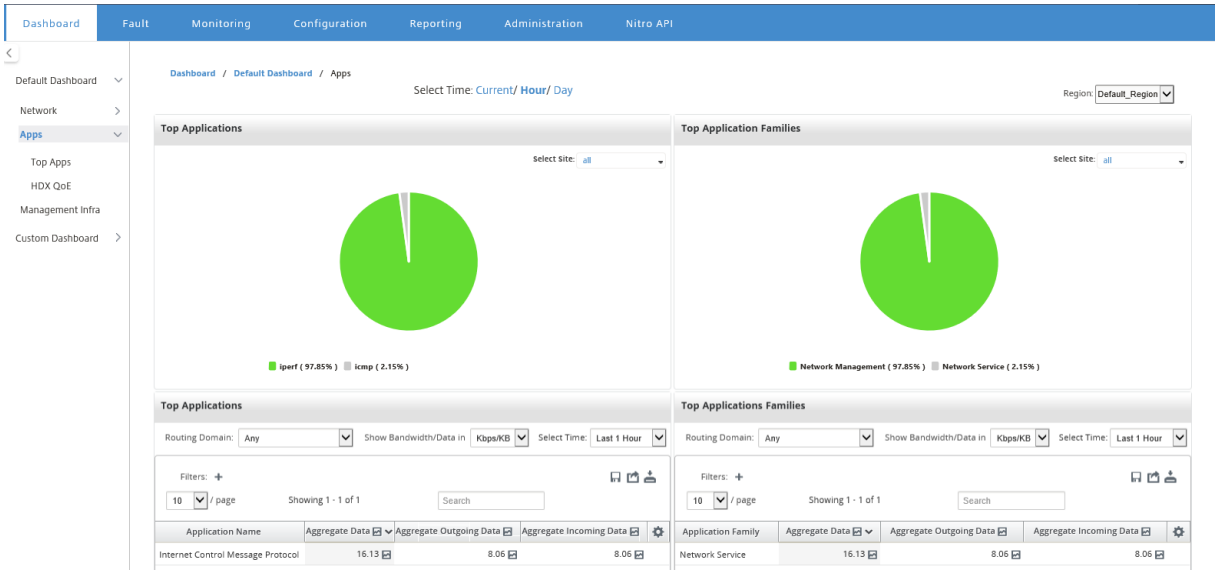


您可以查看最适用于站点的可搜索下拉列表，以供选择应用程序和应用程序系列。

您还可以查看特定区域的热门应用程序和热门应用程序系列。

要查看某个区域的应用程序统计信息，请导航到控制板 > 默认控制板 > 应用程序 **>** 热门应用程序，然后在地区下拉菜单中选择一个区域 **。**

您可以将站点和时间间隔选择为过去 24 小时、过去 1 小时或当前。

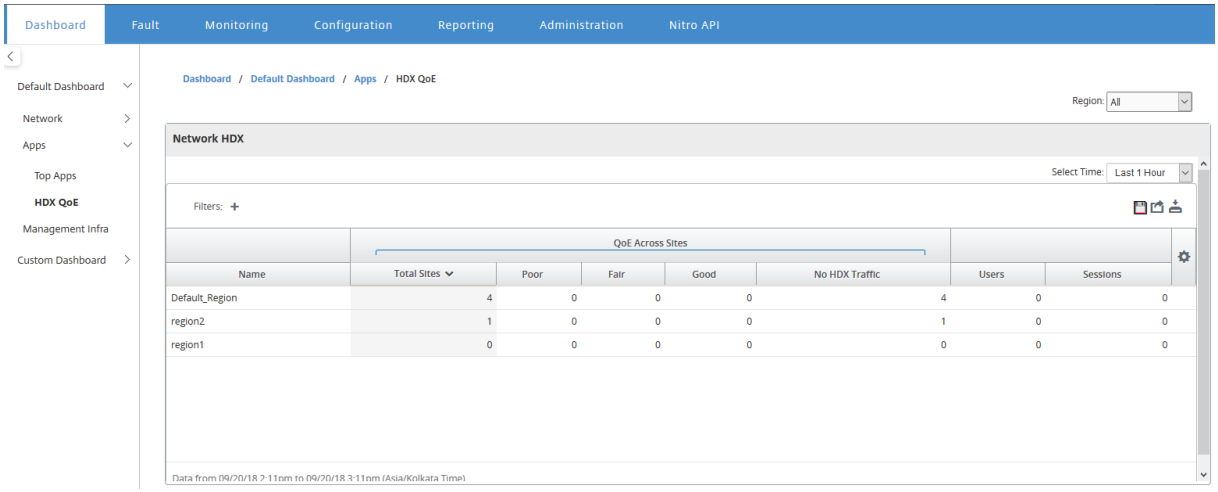


HDX QoE

体验质量 (QoE) 是一个计算索引，可以帮助您了解 ICA 质量的体验。此指数是针对从 WAN 到站点遍历的所有 ICA 应用程序流量计算的。QoE 计算中使用了数据包丢弃、抖动和延迟的统计信息。QoE 是一个介于 [0，100] 之间的整数，数值越高，用户体验越好。在数据包处理过程中，会在数据路径上跟踪抖动、延迟和数据包丢弃统计数据。

根据 HDX 流量的 QoE，整个网络中的站点被归类为良好、公平、差或没有 HDX 流量。有关详细信息，请参阅HDX QoE。

要在网络中的所有区域中查看站点的 HDX QoE，请导航到控制板 > 默认的“控制板 > **Apps > HDX QoE**”，然后在“地区”下拉菜单中选择全部。

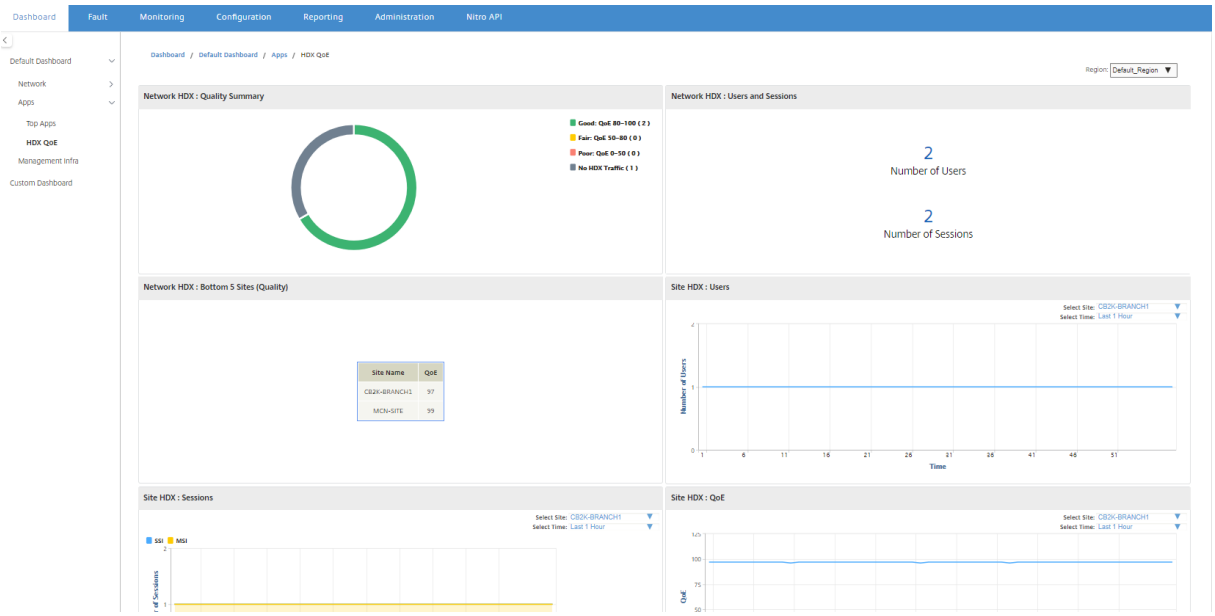


您可以查看各个区域的以下 HDX QoE 指标。

- 网络 HDX：质量摘要
- 网络 HDX：用户和会话

- 网络 HDX：底部五个站点（质量）
- 站点 HDX：用户
- 站点 HDX：会话
- Site HDX：体验质量

要查看 HDX QoE 统计信息，请导航到控制板 > 默认控制板 > 应用程序 **> HDX QoE**，然后在区域下拉菜单中选择一个区域。

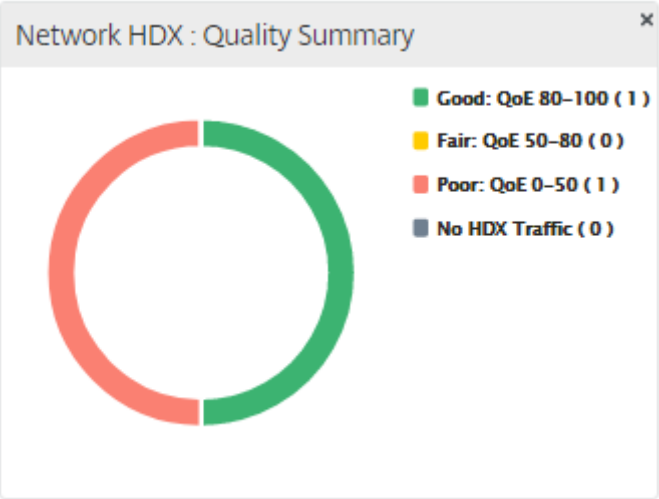


> 注意
>
> 有时，来自不同站点的 HDX 控制板数据和 HDX 报告可能看起来不同步，因为每个站点的统计信息分别进行轮询。
>
> 在 HDX 控制板小组件上，您可能会看到一个不具有 HDX 流量的站点，但可能存在非零数量的 HDX 会话和用户。当 HDX 会话在该轮询时间段空闲并仍保持在打开状态时，会发生此问题。

网络 **HDX**：质量摘要

HDX 流量分为以下质量类别：

质量	QoE 范围
良好	80–100
一般	50–80
不佳	0–50
没有 HDX 流量	不适用

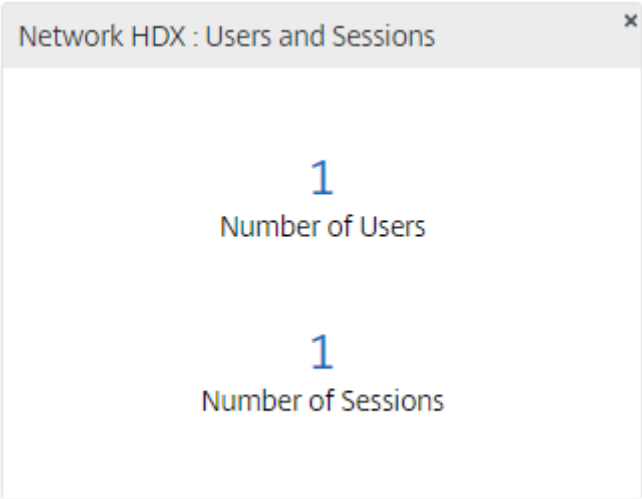


您可以单击图表以查看每个站点的 HDX 报告。有关详细信息，请参阅如何查看 HDX 报告。

网络 **HDX**：用户和会话

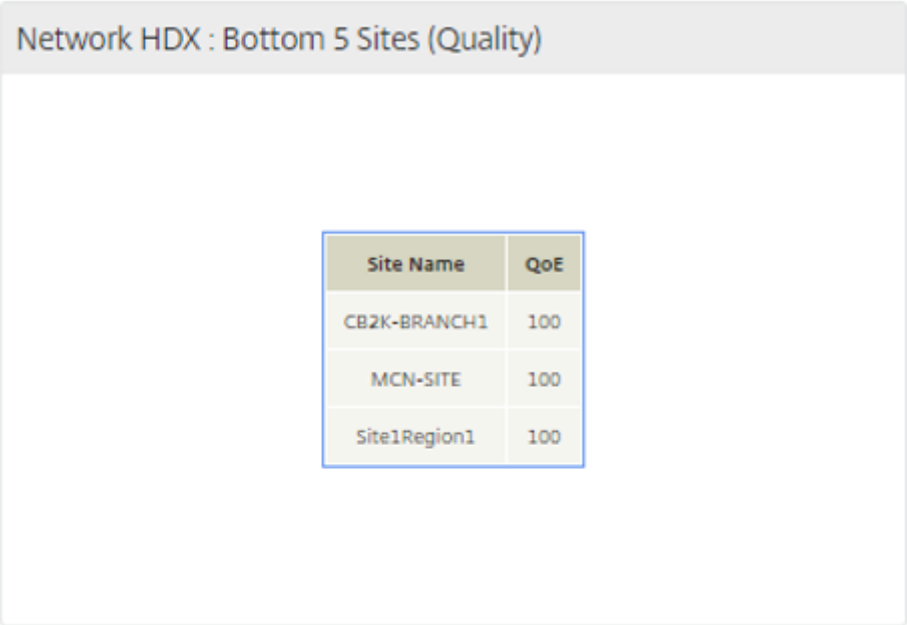
此小组件提供有关活动 HDX 用户和会话数量的信息。会话数是指活动的单会话 ICA (SSI) 和多会话 ICA (MSI) 会话的总数。

> 注意
>
> 在当前版本中，用户数量不基于不同的用户名。即，两个不同计算机上的单个用户启动的两个会话被视为两个用户。



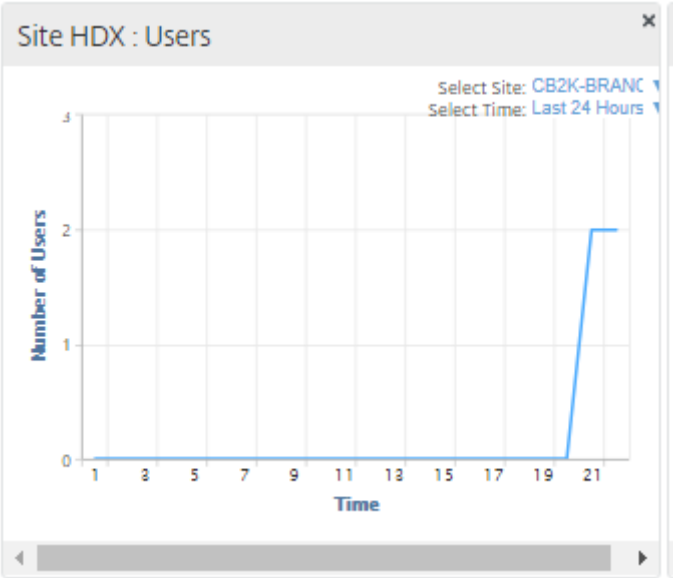
网络 **HDX**：底部的 **5** 个站点（质量）

此小部件提供了 QoE 分数最低的 5 个站点的列表。它可以帮助推动更好的最终用户体验



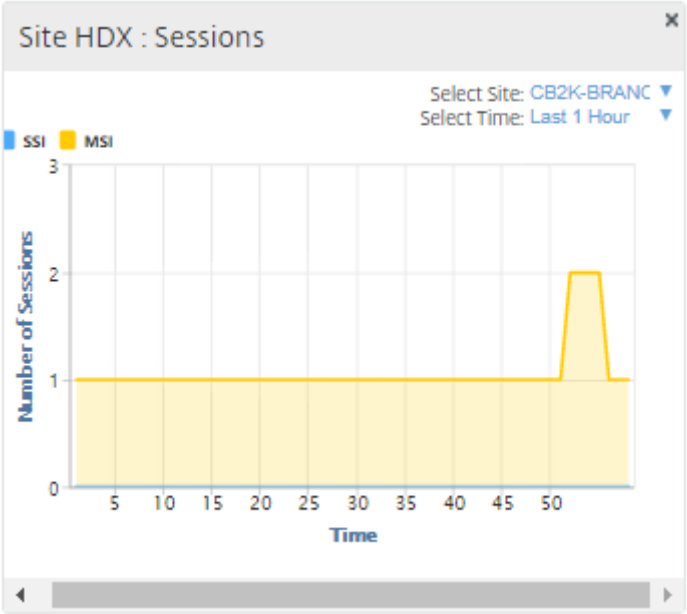
站点 **HDX**：用户

此小组件提供了在所选时间间隔内在特定站点处于活动状态的用户数的图形表示。您可以选择站点和时间间隔为过去 24 小时、过去 1 小时或最后 5 分钟。



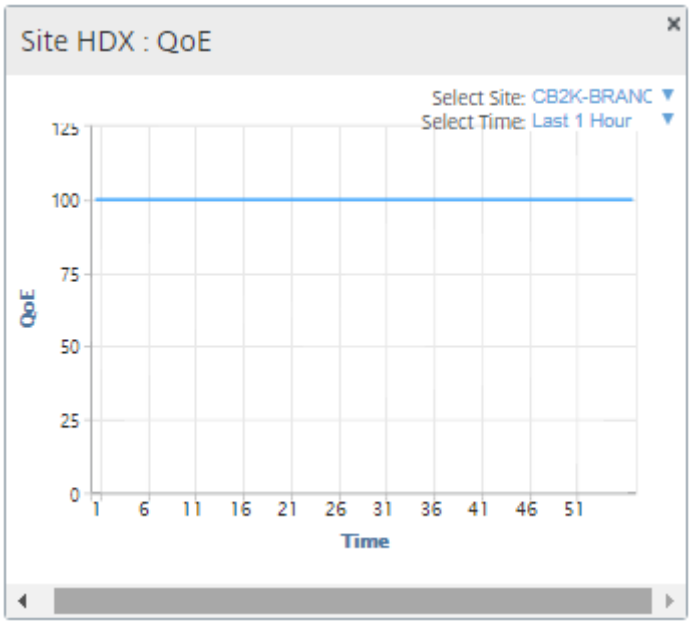
站点 **HDX**：会话

此小组件提供了在所选时间间隔内在特定站点处于活动状态的 MSI 和 SSI 会话数的图形表示。您可以选择站点和时间间隔为过去 24 小时、过去 1 小时或最后 5 分钟。



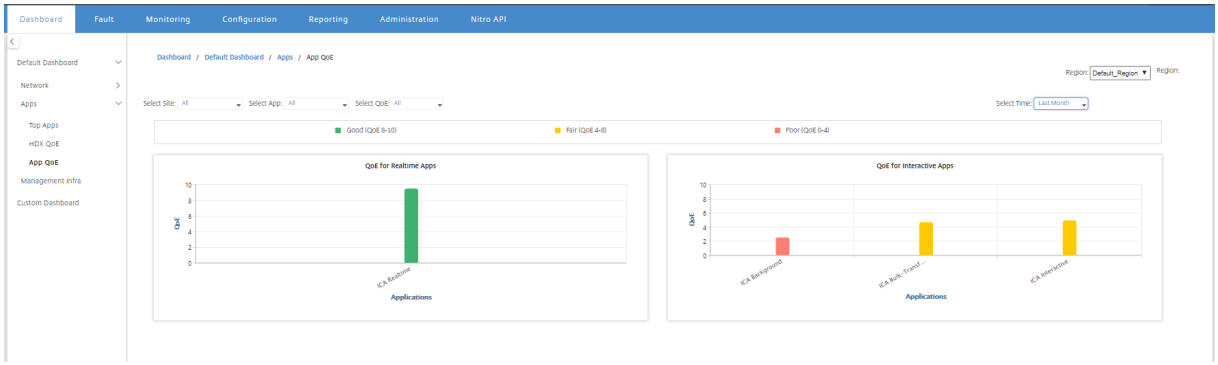
Site HDX：体验质量

此小组件提供了选定时间间隔内特定站点的整体 QoE 的图形表示。您可以选择站点和时间间隔为过去 24 小时、过去 1 小时或最后 5 分钟。



应用程序 **QoE**

应用程序 QoE 是衡量应用程序体验质量的衡量标准。应用程序 QoE 的分数范围为 0-10，其中 10 表示优异的质量，0 表示质量差。有关详细信息，请参阅应用程序 QoE。您可以查看实时和交互式流量的应用程序 QoE 分数。

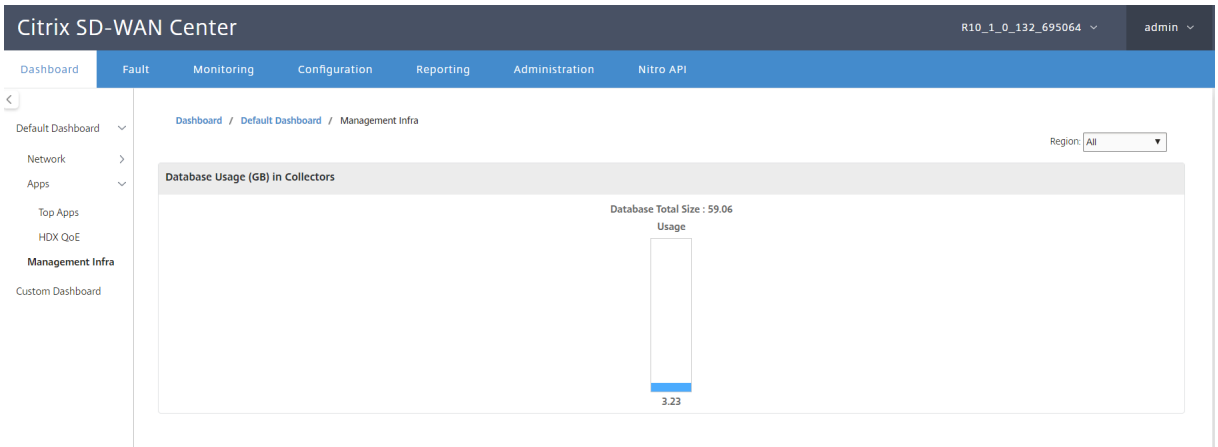


您可以按站点、应用程序或 QoE 类型筛选应用程序 QoE 统计信息。

管理基础结构

通过“管理基础结构”页面，您可以查看 Citrix SD-WAN Center 数据库使用情况和存储统计信息。

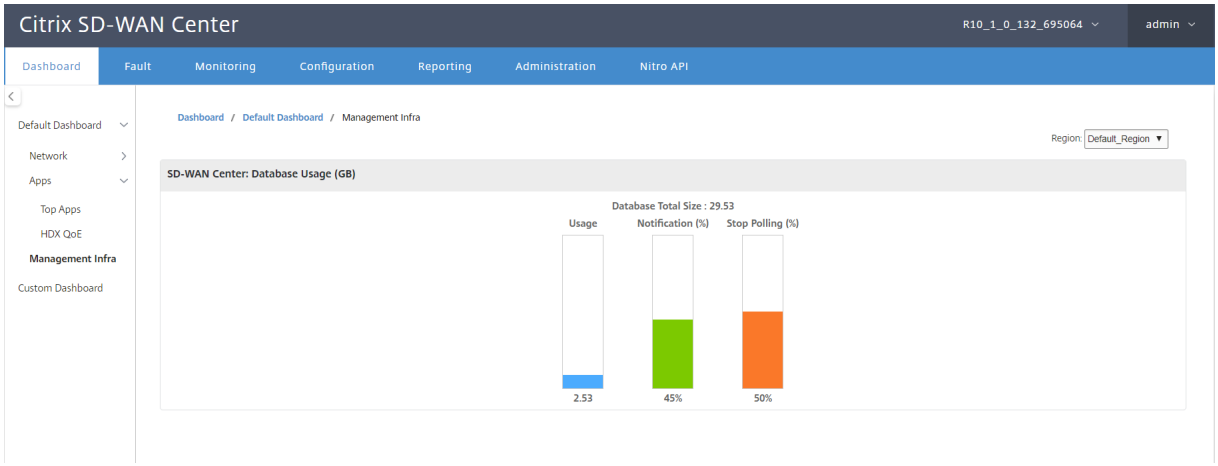
对于多区域部署，可以查看网络中所有收集器的数据库使用情况。要查看多区域数据库统计数据，请导航到控制板 > 默认控制板 > 管理基础结构，然后在区域下拉菜单中选择全部。



要查看特定区域的 Citrix SD-WAN Center 的数据库统计信息，请导航到控制板 > 默认控制板 > 管理基础结构，然后在区域下拉菜单中选择一个区域。

数据库使用情况部分显示数据库资源使用情况的图形概况以及发送通知的阈值，或停止数据收集。您可以单击图表以查看数据库维护页面上的详细信息。

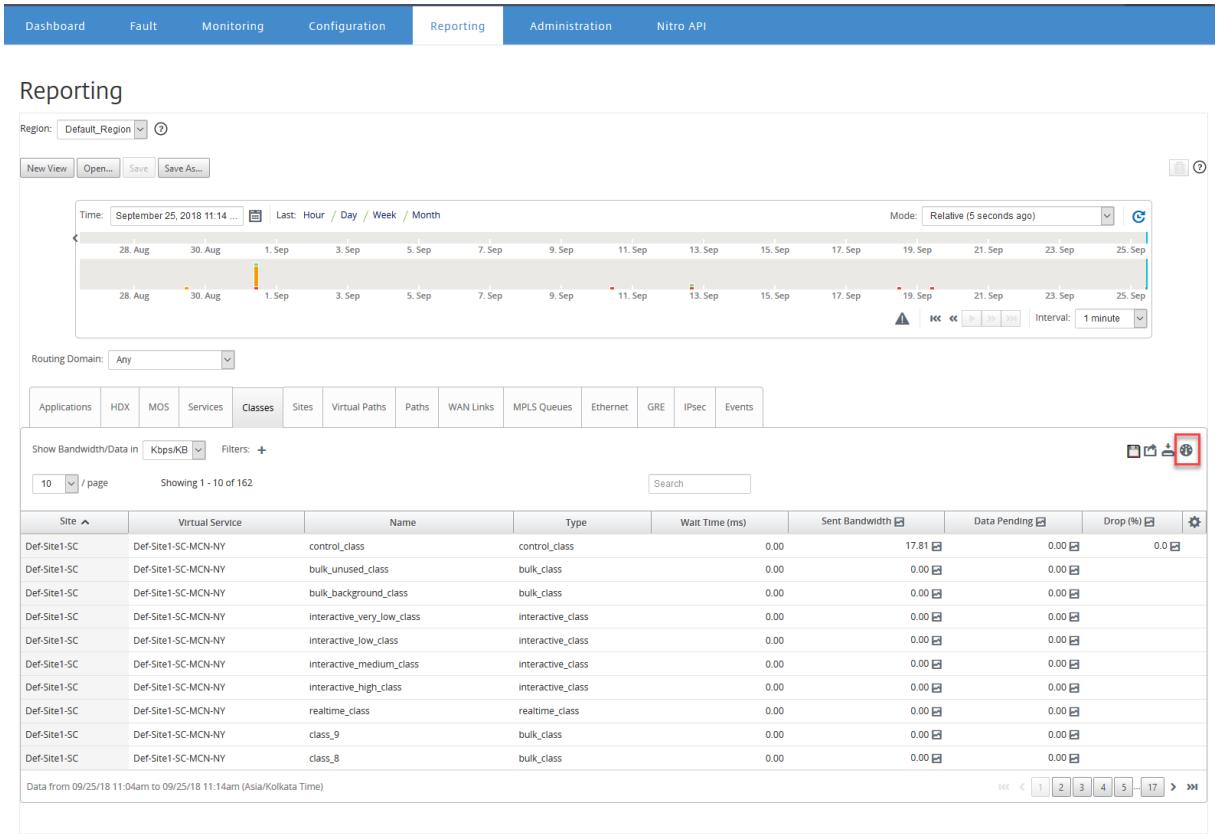
- 使用情况：当前正在使用的数据库容量 (GB)。
- 通知：生成数据库使用情况通知的阈值。阈值是数据库最大大小的百分比。如果配置了电子邮件警报，当数据库的大小超过此阈值时，会发送电子邮件通知。有关详细信息，请参阅事件通知。
- 停止轮询：用于停止统计轮询的阈值。阈值是数据库最大大小的百分比。数据库大小超过此阈值时，轮询将停止。有关详细信息，请参阅管理数据库。



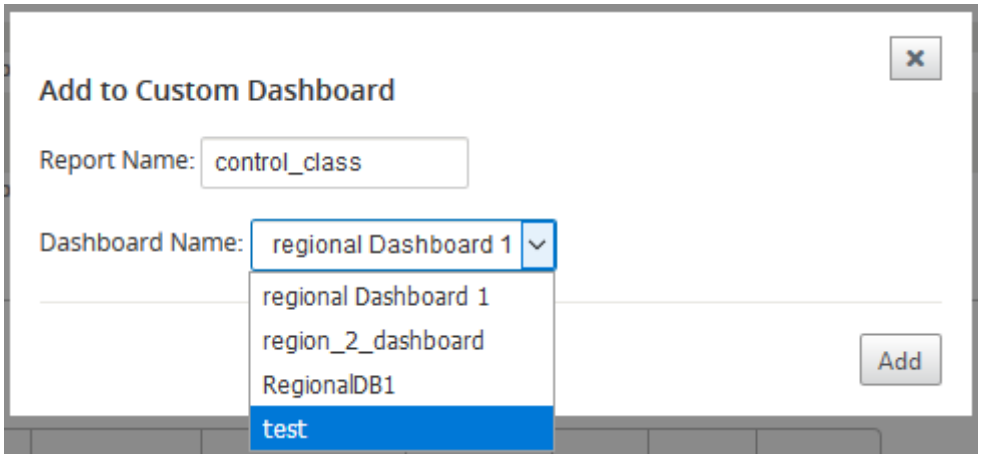
自定义控制板

您可以自定义 Citrix SD-WAN Center 控制板，并根据您的分析需求选择要在控制板上查看的统计信息。创建区域详细信息或全局摘要的自定义控制板。您还可以自定义现有报告。

> 注意
>
> 现在可以在报告页面上使用添加到控制板选项，将报告作为小组件固定到您的自定义控制板。



输入报告名称，然后选择“自定义”控制板。



对于区域详细信息自定义控制板，可以从以下地区级别小组件中进行选择：

- 网站摘要
- 虚拟路径
- 地区事件
- 区域警报摘要
- 清单管理器（每个地区）
- 每个地区的热门网站
- 路径
- MPLS 队列
- 以太网
- LAN GRE 隧道
- IPsec 隧道
- 服务摘要
- 班级
- 站点事件
- 每个地区的热门应用
- 每个区域的顶级应用程序
- 站点 HDX：用户
- 站点 HDX：会话
- 站点 HDX：QoE
- MOS 应用
- 数据库使用

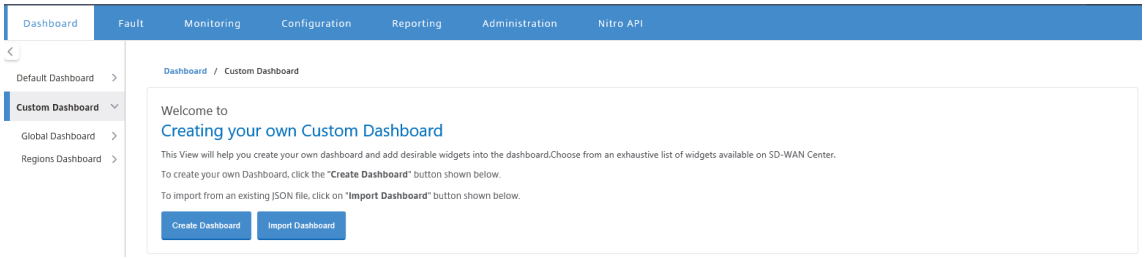
对于全局摘要自定义控制板，可以从以下网络级别小组件中进行选择：

- 多区域摘要
- 网络中的虚拟路径健康
- 事件

- 警报摘要
- 库存经理
- 网络中的热门网站
- 网络 HDX
- 收集器中的数据库使用
- 热门应用
- 热门应用系列

要创建自定义控制板，请执行以下操作：

1. 导航到控制板 > 自定义控制板，然后单击创建控制板。

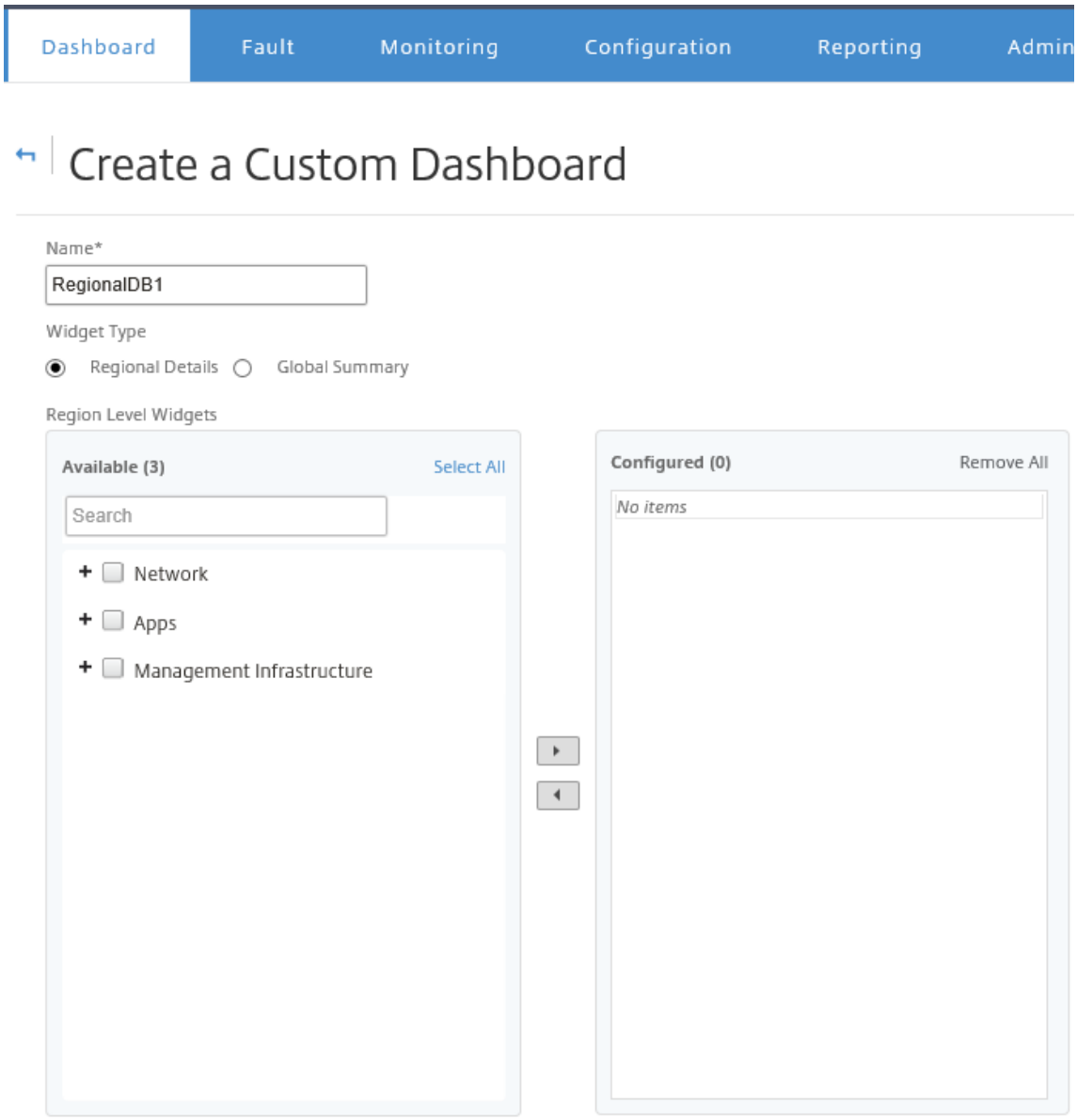


> 注意
>
> 您也可以通过单击导入控制板导入 JSON 格式的现有控制板。

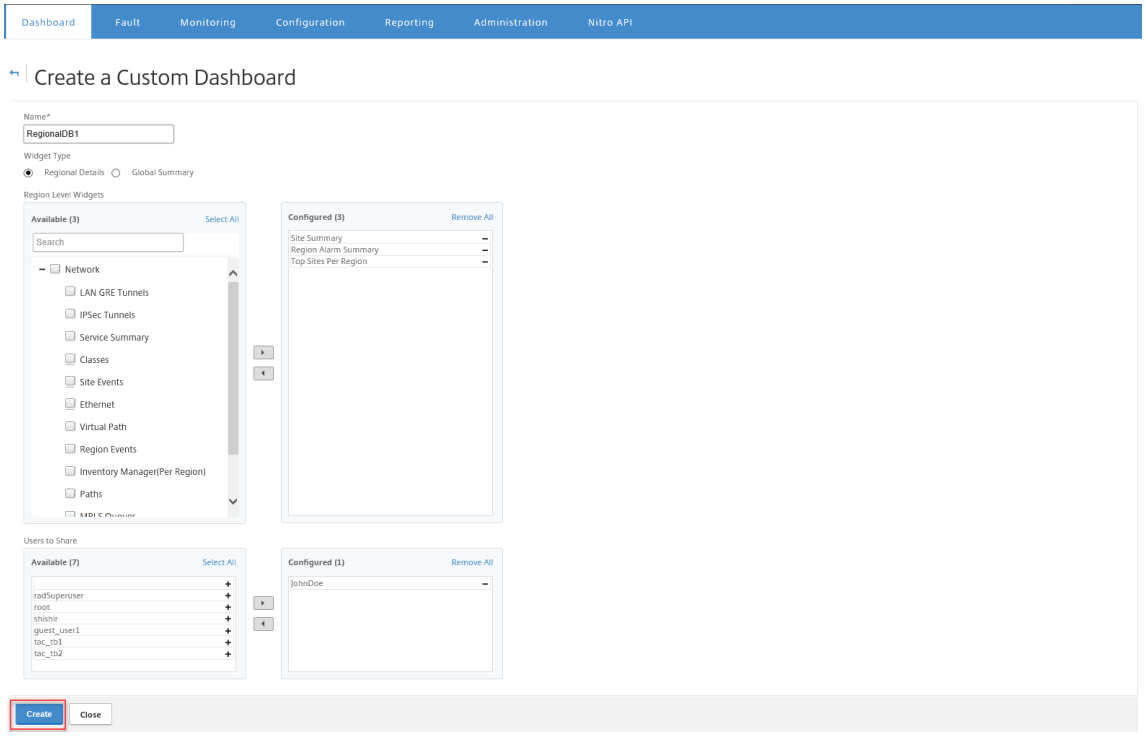
2. 在名称字段中，输入自定义控制板的名称。
3. 选择小组件类型。选择全局摘要要查看网络级小组件，请选择区域详细信息查看区域级小组件。

4. 单击添加，然后选择所需的小组件。

   小组件分为三个级别：网络、应用程序和管理基础结构。



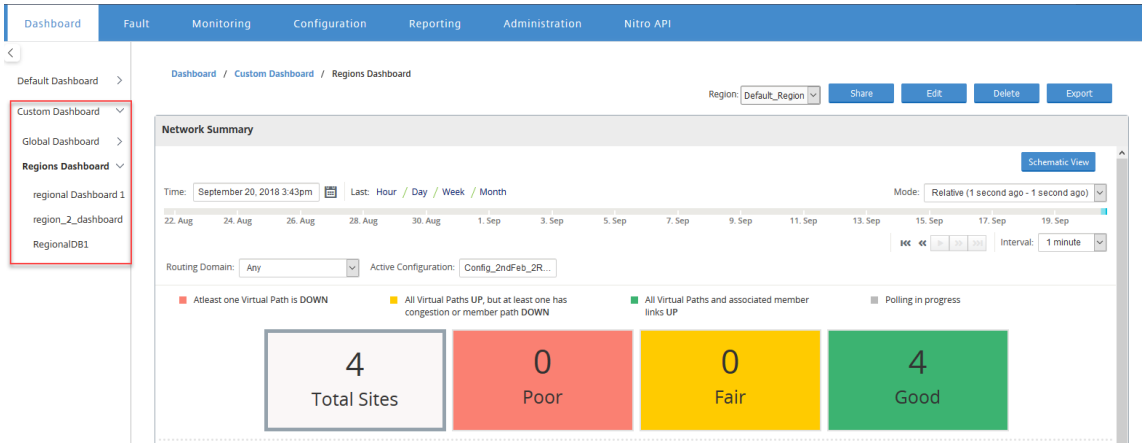
> 注意
>
> 在单区域部署中，仅可使用区域级别的小组件。



您还可以与多个用户共享自定义控制板。有关用户的详细信息，请参阅用户帐户。

5. 单击创建。新创建的自定义控制板列在自定义控制板下。

> 提示
>
> 您可以编辑或删除自定义控制板。



诊断包

April 13, 2021

诊断包由所有系统日志文件、系统信息以及其他必要的详细信息组成，这些信息可以帮助 Citrix SD-WAN 支持团队诊断和解决系统问题。

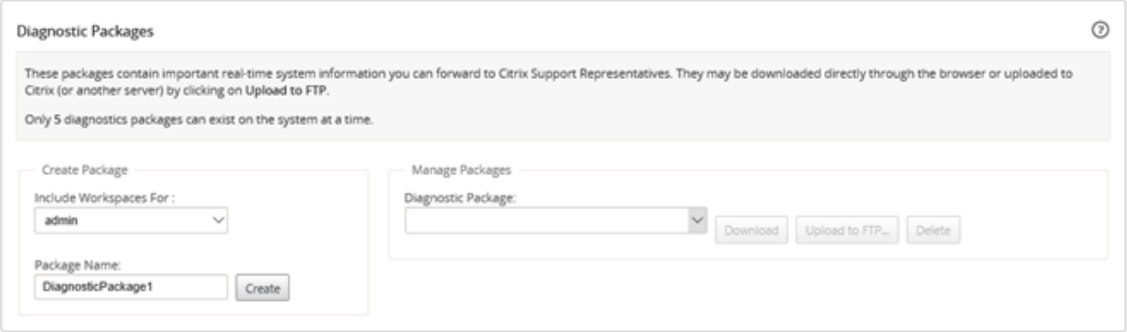
创建软件包后，可以将其下载到您的计算机上，然后将其发送给 Citrix 的客户支持，或者直接将其上载到 Citrix 客户支持服务器（或另一台服务器）。

> 注意
>
> Citrix SD-WAN Center 一次最多可存储五个诊断包。

要创建诊断包，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击监视选项卡，然后单击诊断。
2. 在诊断包部分中的创建软件包下，从包含工作区下拉列表中选择一个将工作区复制到诊断程序的用户。

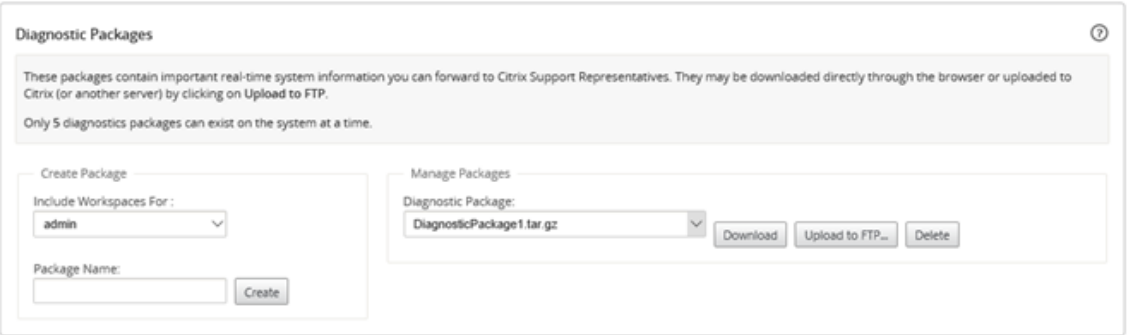
   > 注意
   >
   > 诊断程序包将包括所选用户最近修改的五种配置。



3. 在软件包名称字段中，输入诊断包的名称。
4. 单击创建。这将运行系统诊断程序并生成诊断程序包。

要下载诊断包，请执行以下操作：

1. 在诊断包部分中的管理包下，从诊断包下拉列表中，选择要下载的软件包。



2. 单击下载。诊断程序包将下载到您的本地计算机。

要将诊断包上载到 FTP 服务器，请执行以下操作：

1. 在诊断包部分中的管理包下，从诊断包下拉列表中，选择要上载的软件包。
2. 单击上载到 **FTP**。此时将打开上载到 **FTP** 服务器对话框，以指定 ftp 身份验证信息，并将该软件包上载到 Citrix 客户支持 FTP 服务器或另一个 FTP 主机上。

3. 在客户名称字段中，输入协助 Citrix SD-WAN 支持标识诊断包的名称。
   将在 Citrix FTP 服务器上创建一个具有此名称的目录，您的文件将上载到该位置。
4. 在 **FTP** 主机字段中，输入 FTP 服务器的 IP 地址或主机名（如果配置了 DNS）。
5. 在用户名字段中，输入要用来登录 FTP 服务器的用户名。
6. 在密码字段中，输入与用户名关联的密码。
7. 单击上载。

> 注意
>
> 建议定期删除旧诊断包，以防止超出允许的最大软件包数上限。要删除现有诊断包，请从诊断包下拉列表中选择一个诊断包，然后单击删除。

事件

April 13, 2021

Citrix SD-WAN Center 收集来自网络中所有发现的设备的事件信息。在事件查看器页面中，可以过滤和查看此事件信息。

事件详细信息包括以下信息。

- 时间：生成事件的时间。
- 站点：生成事件的站点的名称。
- 设备 **ID**：显示生成事件的设备是主设备 (**0**) 还是辅助 (**1**) 设备。

  > 注意
  >
  > 默认情况下，“设备 ID”列处于隐藏状态。要显示该列，请单击显示/隐藏 (齿轮图标)，然后从下拉菜单中选择设备 **ID** 复选框

- 对象名称：生成事件的对象的名称。
- 对象类型：生成事件的对象的类型。
- 严重性：事件的严重性级别。
- 以前的状态：在事件之前对象的状态。如果不适用，状态将被列为“未知“。
- 当前状态：事件发生时对象的状态。
- 说明：事件的文本描述。

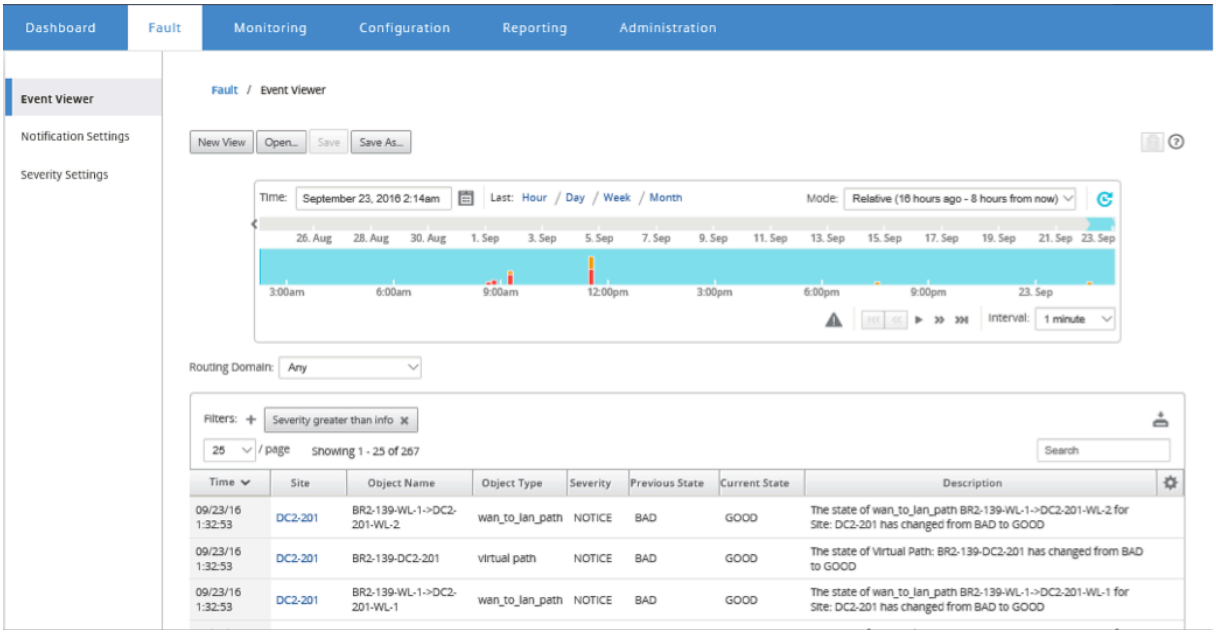
查看事件

您可以查看事件，对其进行过滤并从“事件查看器”页面下载。

访问事件查看器页面。

在 Citrix SD-WAN Center Web 界面中，单击 故障 选项卡。

默认情况下，将显示“事件查看器”页面。



您可以使用时间线控件选择和查看特定时间段的报告。有关详细信息，请参阅时间线控件。

> 注意
>
> 您可以查看过去 30 天的事件数据。超出此时间段的所有数据都将自动从 SD-WAN Center 收集器和各自的区域收集器中删除。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。

使用过滤器

您可以创建自定义过滤器来缩小事件表结果范围。

要创建并应用过滤器，请执行以下操作：

1. 单击“筛选器”部分标签右侧的 **+** 图标。
2. 从下拉菜单中选择一个类别。

   可用的选项包括：

   - 大小
   - 对象名称
   - 对象类型
   - 严重性
   - 以前的状态
   - 当前状态

3. 从中间下拉菜单中选择一个运算符。

   这些选项如下所示：

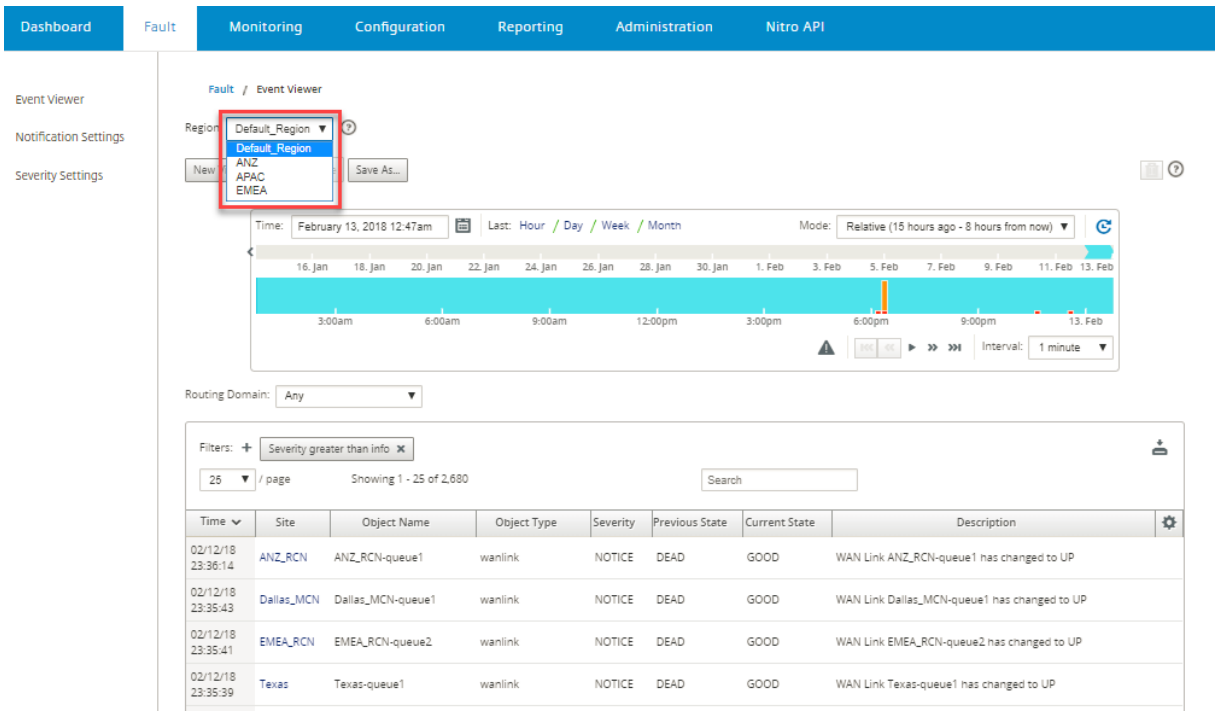
   - 是
   - 不是
   - 是其中之一
   - 包含
   - 不包含
   - 小于
   - 小于或等于
   - 大于
   - 大于或等于

4. 输入用于分隔筛选器的字符串或值。

> 注意
>
> 此字段区分大小写。

> 注意
>
> 您可以创建和应用多个过滤器。
> 对于多区域网络，可以选择特定的区域以查看事件。

事件数据是从相应区域的收集器中获取的。



> 注意
>
> 在单区域网络部署中，区域 下拉列表不可用。

要将事件表下载为 CSV 文件，请执行以下操作：

单击事件表右上角的下载图标。

有关事件统计信息的详细信息，请参阅事件报告。

可以将 Citrix SD-WAN Center 配置为以电子邮件、SNMP 陷阱或 syslog 消息的形式发送不同事件类型的外部事件通知。有关详细信息，请参阅事件通知。

事件通知

April 13, 2021

可以将 Citrix SD-WAN Center 配置为以电子邮件、SNMP 陷阱或 syslog 消息的形式发送不同事件类型的事件通知。配置完电子邮件、SNMP 和 syslog 通知设置后，可以选择不同事件类型的严重性，并选择模式（电子邮件、SNMP、syslog）以发送事件通知。对于等于或高于事件类型的指定严重级别的事件，将生成通知。

可用严重性级别如下所示，以降序显示顺序：

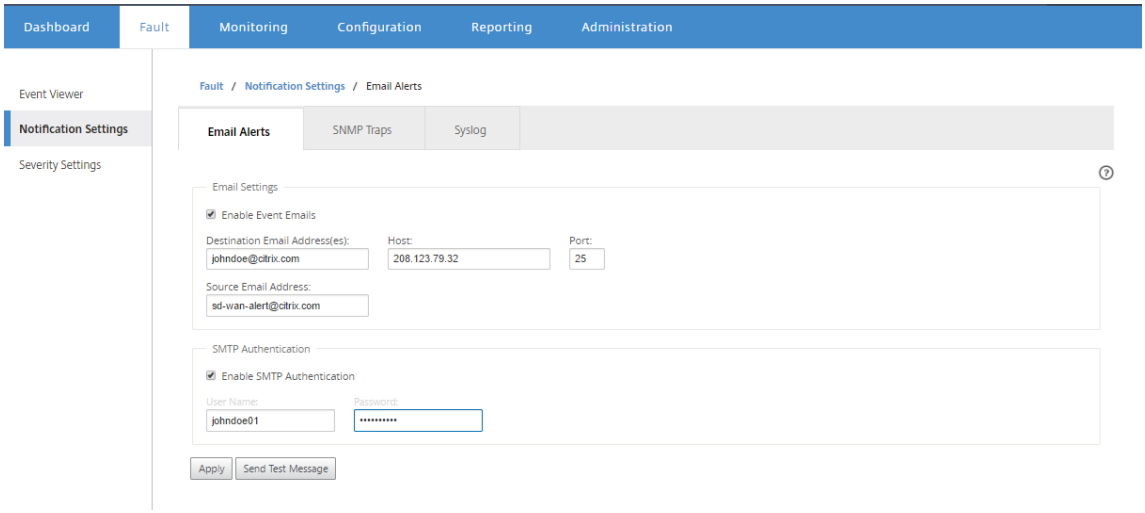
- 紧急情况
- 警报
- 严重
- 错误
- 警告
- 通知
- 信息
- DEBUG

> 提示
>
> 可以通过以下方法配置通知设置：通过电子邮件、SNMP 陷阱或 Syslog 消息在网络中的 Citrix SD-WAN Center 和各个 Citrix SD-WAN 设备上接收事件警报。
>
> 但是，在 Citrix SD-WAN Center 上启用通知将允许您接收整个 Citrix SD-WAN 网络（即 MCN 以及所有站点）的事件通知。虽然在 Citrix SD-WAN 设备上启用通知，但仅允许您从单个设备接收通知。
>
> 建议仅在 Citrix SD-WAN Center 上启用通知，以避免网络中其他 Citrix SD-WAN 设备发出冗余通知。

配置邮件通知设置

要配置电子邮件通知设置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 管理界面中，导航到故障 > 通知设置 > 电子邮件警报。



2. 选择启用事件电子邮件。
3. 在目标电子邮件地址字段中，输入要向其发送警报通知的电子邮件地址。

> 注意
>
> 您可以输入多个电子邮件地址，以分号分隔。

4. 在主机字段中，输入外部 SMTP 服务器的 IP 地址或主机名，以将电子邮件中继到 Internet。
5. 在端口字段中，输入要用于 SMTP 连接的端口号。The default port is 25.
6. 在源电子邮件地址字段中，输入发送电子邮件警报的电子邮件地址。
7. 选择启用 **SMTP** 身份验证。
8. 在用户名字段中，输入用于身份验证的 SMTP 服务器的用户名。
9. 在密码字段中，输入与用于身份验证的 SMTP 服务器的用户名关联的密码。

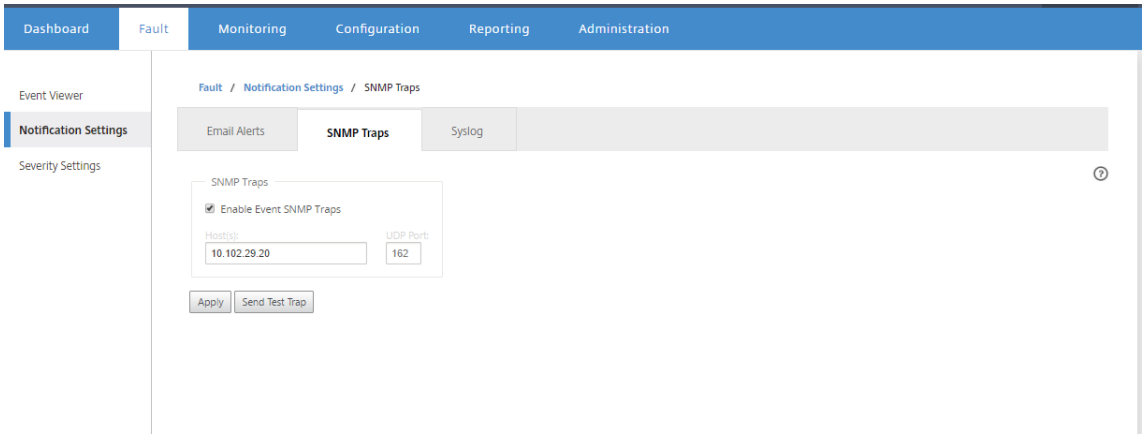
> 注意
>
> 单击发送测试消息，向已配置收件人发送示例电子邮件警报。

10. 单击应用。

配置 **SNMP** 陷阱通知设置

要配置 SNMP 陷阱通知设置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 管理界面中，导航到故障 > 通知设置 > **SNMP** 陷阱。
2. 选择启用事件 **SNMP** 陷阱。



3. 在主机字段中，输入外部 SNMP 系统的 IP 地址或主机名。该主持人将作为 SNMP 陷阱接收事件。

> 注意
>
> 可以输入多个 IP 地址或主机名，以分号分隔。

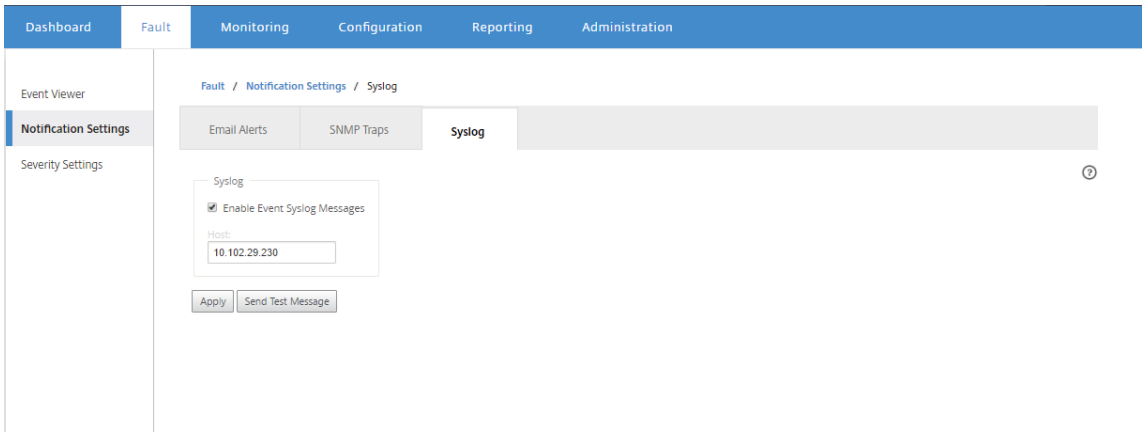
4. 在 **UDP** 端口字段中，输入要用来发送 SNMP 陷阱的 UDP 端口。默认情况下，UDP 端口设置为 162。
5. 单击应用以应用 SNMP 陷阱通知设置。

> 注意
>
> 或者，单击发送测试陷阱以确认系统是否能够向配置的目标发送 SNMP 陷阱。

配置 **syslog** 通知设置

要配置 Syslog 通知设置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 管理界面中，导航到故障 > 通知设置 > **Syslog**。
2. 选择启用事件系统日志消息。



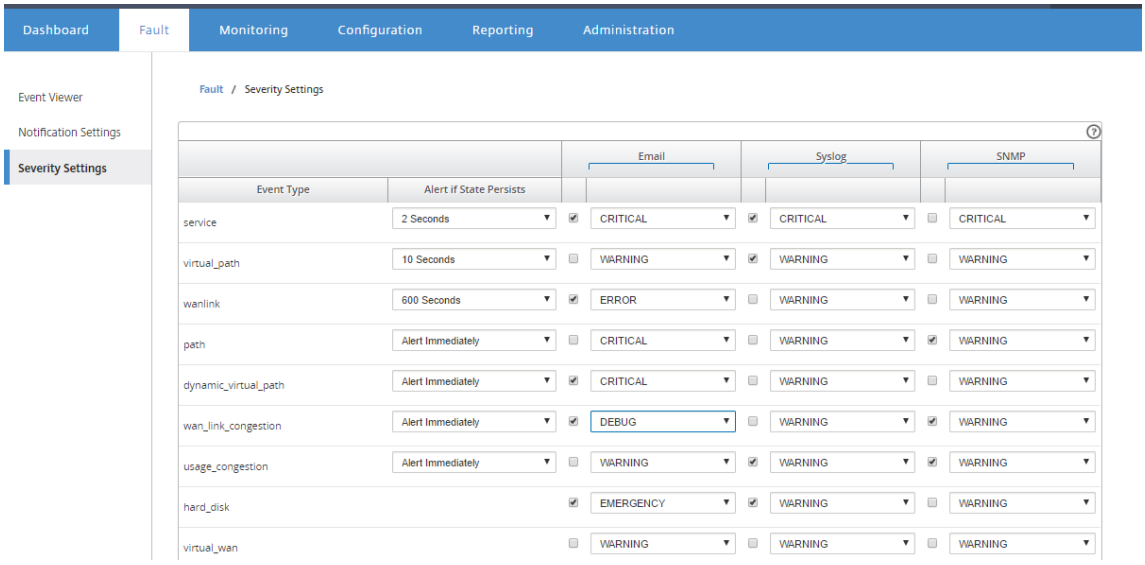
3. 在主机字段中，输入将用于接收事件作为 syslog 消息的外部 syslog 服务器的 IP 地址或主机名。
4. 单击应用以应用系统日志通知设置。

> 注意
>
> 或者，单击发送测试消息以确认系统是否可以将 syslog 消息发送到已配置的主机。

配置事件通知

要配置事件通知，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 管理界面中，导航到故障 > 严重性设置。
2. 在如果状态持续存在，则发出警报字段中，选择将发送事件仍保持在其后的持续时间。



3. 对于每种事件类型，请选择通知选项并选择严重性。

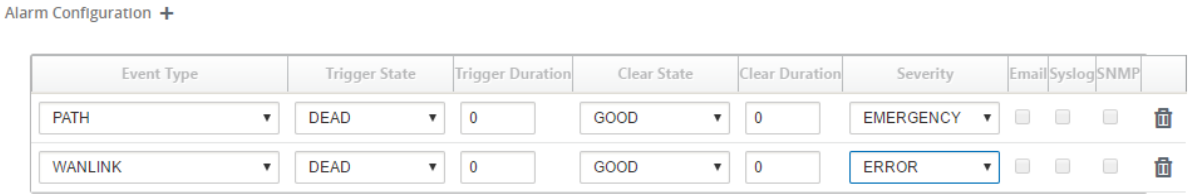
> 注意
>
> 只有在配置了相应的通知设置后，才能启用电子邮件、Syslog 和 SNMP 通知选项。

4. 单击应用。

配置警报

您还可以在 Citrix SD-WAN Center 中配置警报，并将其推送到各个设备。

要在 Citrix SD-WAN Center 中配置警报，请导航到配置 > 设备设置 > 通知设置 > 警报配置，然后单击 **+**。



为以下字段选择或输入值：

- 事件类型：Citrix SD-WAN 设备可以为网络中特定子系统或对象触发警报，这些事件称为事件类型。可用的事件类型包括 SERVICE、VIRTUAL_PATH、WANLINK、PATH、DYNAMIC_VIRTUAL_PATH、WAN_LINK_CONGESTION、USAGE_CONGESTION、FAN、POWER_SUPPLY、PROXY_ARP、ETHERNET、DISCOVERED_MTU、GRE_TUNNEL 和 IPSEC_TUNNEL。
- 触发器状态：为事件类型触发警报的事件状态。可用的 触发状态 选项取决于所选事件类型。
- 触发器持续时间：这是持续时间（秒），用于确定设备触发警报的速度。输入 0 以接收即时警报，或者输入介于 15-7200 秒之间的值。如果触发器持续时间内同一个对象上发生其他事件，则不会触发警报。仅当事件持续时间超过触发器持续时间时，才会触发其他警报。
- 清除状态：触发警报后清除事件类型警报的事件状态。可用的清除状态选项取决于所选的触发器状态。
- 清除持续时间：此持续时间（以秒为单位）决定在清除警报之前等待的时长。输入 0 可立即清除警报，或者输入介于 15-7200 秒之间的值。如果在指定时间内同一个对象上发生了另一个清除状态事件，则不会清除警报。
- 严重性：用户定义的字段，确定警报的紧急程度。严重性显示在触发或清除警报时发送的警报以及触发的警报摘要中。
- 电子邮件：通过电子邮件发送事件类型的警报触发器和清除警报。
- **Syslog**：事件类型的警报触发器和清除警报通过 Syslog 发送。
- **SNMP**：警报触发器和清除事件类型的警报通过 SNMP 陷阱发送。

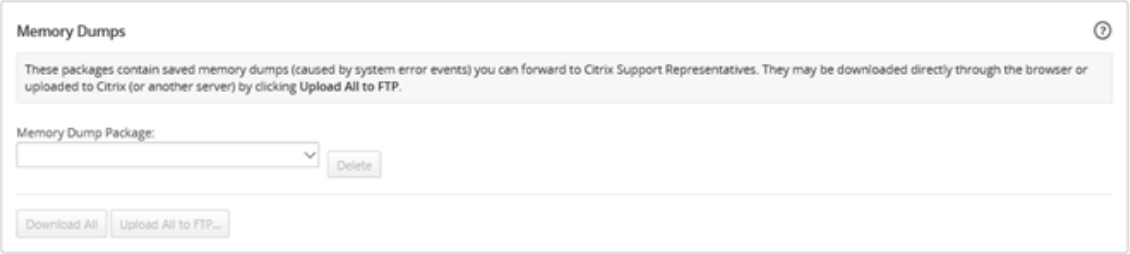
内存转储

April 13, 2021

进程崩溃时会生成内存转储。可以在一个组合的软件包中下载系统上当前的所有内存转储，并将其上载到 FTP 服务器以供 Citrix 支持团队进行检查。但是，您可以删除单个内存转储。

要下载内存转储，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击监视选项卡，然后单击诊断。
2. 在内存转储部分中，从内存转储包、下拉列表中选择内存转储包。



3. 单击 全部下载。将内存转储包保存在本地计算机上。

要将内存转储包上载到 FTP 服务器，请执行以下操作：

1. 在内存转储部分中，从内存转储包、下拉列表中选择内存转储包。
2. 单击上载到 **FTP** 服务器。此时将打开全部上载到 **FTP** 对话框，以指定 FTP 身份验证信息并将软件包上载到 Citrix 客户支持 FTP 服务器或另一个 FTP 主机上。

3. 在客户名称字段中，输入协助 Citrix SD-WAN 支持标识诊断包的名称。

   将在 Citrix FTP 服务器上创建一个具有此名称的目录，您的文件将上载到该位置。
4. 在 **FTP** 主机字段中，输入 FTP 服务器的 IP 地址或主机名（如果配置了 DNS）。
5. 在用户名字段中，输入要用来登录 FTP 服务器的用户名。
6. 在密码字段中，输入与用户名关联的密码。
7. 单击上载。

日志文件

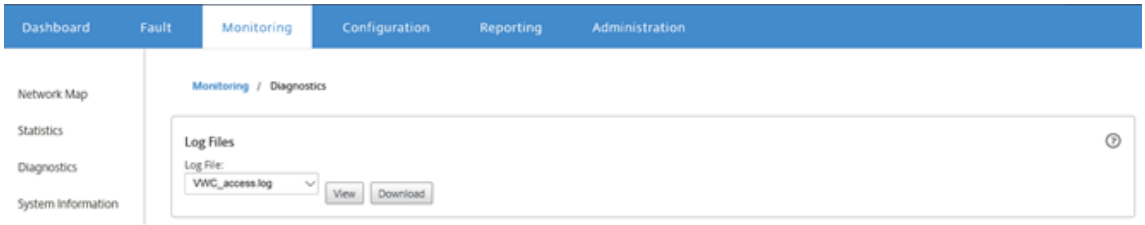
April 13, 2021

日志文件可收集与 Web 控制台、用户界面异常、内部崩溃等有关的信息。可以使用这些日志来对 Citrix SD-WAN Center 中出现的问题进行故障排除。

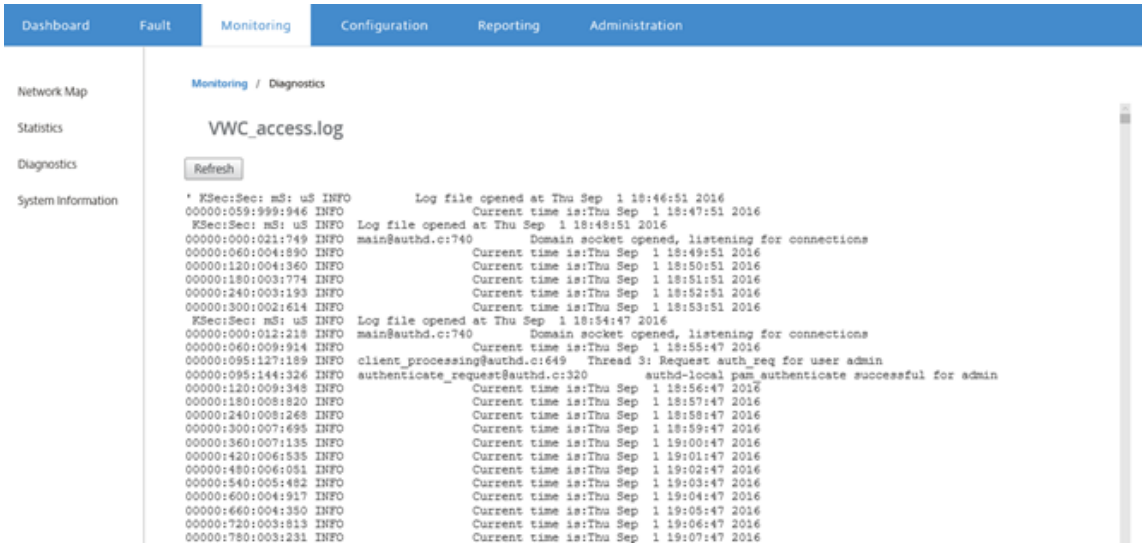
要查看日志文件，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击监视选项卡。
2. 单击诊断。

3. 在日志文件下拉列表中，选择要查看的日志文件。



4. 单击查看。将显示日志文件内容。



5. 如果要将日志文件下载到您的计算机上，请单击下载。

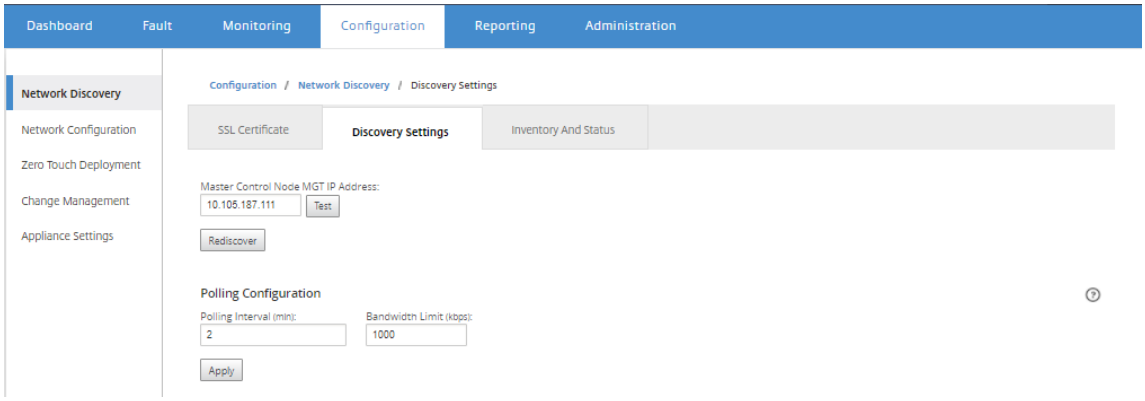
轮询时间间隔

April 13, 2021

轮询是指从发现的设备收集统计信息的过程。发现设备后，您可以为轮询操作配置间隔和带宽限制。有关发现设备的信息，请参阅单区域网络部署或多区域网络部署。

要执行轮询配置，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，导航到配置 > 网络发现 > 发现设置。



2. 在轮询时间间隔字段中，输入轮询频率（分钟）。范围为 2 至 60 分钟。默认值为 5 分钟。
3. 在带宽限制字段中，输入轮询带宽限制 (kbps)。将轮询统计信息从设备传输到 Citrix SD-WAN Center 时，MCN 将限制到指定值的带宽。范围为 100 Kbp-1 Gbps。默认值为 1 Mbps。
4. 单击应用。

统计信息

April 13, 2021

您可以查看 Citrix SD-WAN Center 收集的统计数据（以图表形式）。这些图形绘制为时间线，而不是使用情况，以便您了解各种网络对象属性的使用趋势。您可以查看网络范围内应用程序统计信息的图表。对于 SD-WAN 网络中的每个站点，可以查看以下网络参数的图形：

- Bandwidth（带宽）
- QoS
- 虚拟路径
- 互联网服务
- 内联网服务
- 直通服务
- WAN 链接
- 以太网接口
- GRE 通道
- IPsec 隧道
- 应用程序
- 应用系列

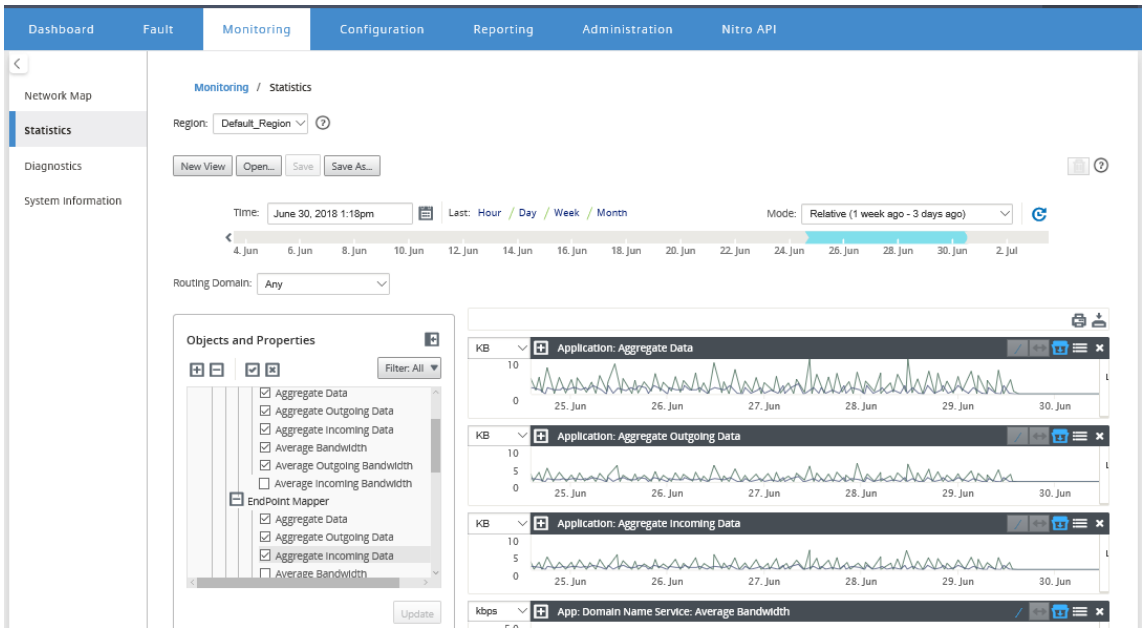
> 提示
>
> 可以根据您的要求创建视图，保存并打开现有视图。

要查看统计图形，请执行以下操作：

1. 在 Citrix SD-WAN Center Web UI 中，导航到监视 > 统计信息。
2. 选择区域和路由域。
3. 从对象和属性的分层树中，找到并选择感兴趣的属性。

> 提示
>
> 您还可以使用筛选器下拉菜单和预设菜单来简化查找和选择属性的过程。

4. 单击更新以显示选定属性的图形。

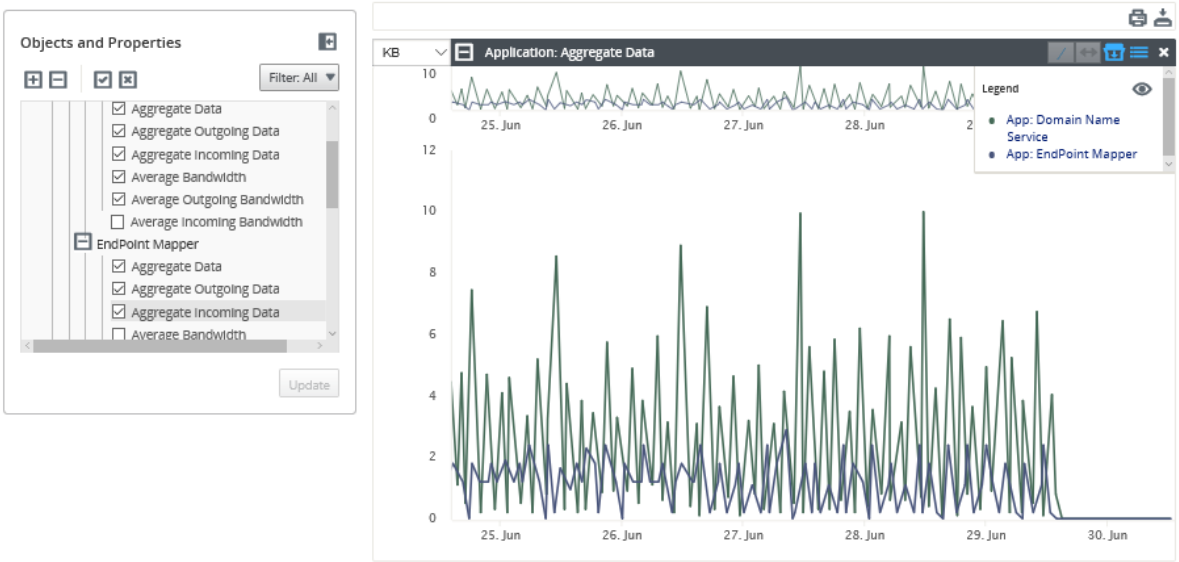


> 提示
>
> 取消选中某个属性，然后单击更新，以从图形显示区域中删除该属性的图形。

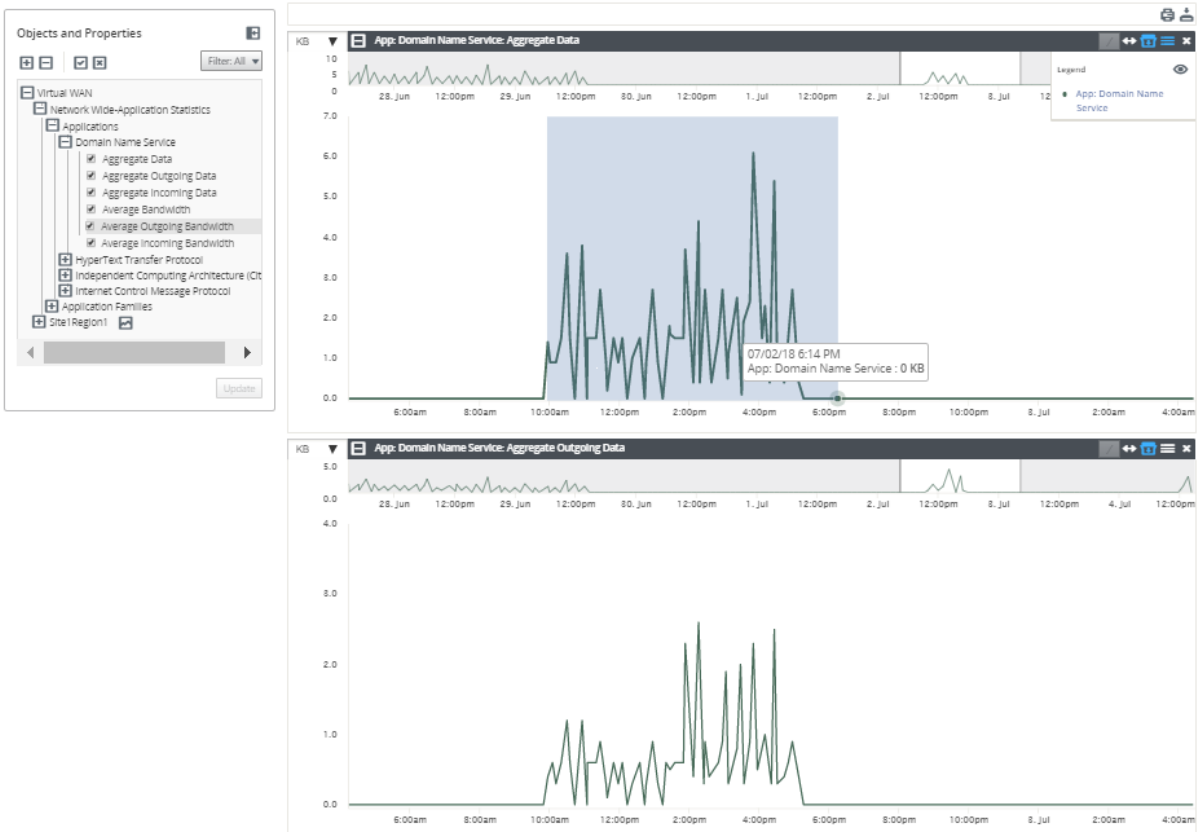
5. 为当前视图选择一个周期。有关详细信息，请参阅时间线控件。

   图表将根据所选属性显示。

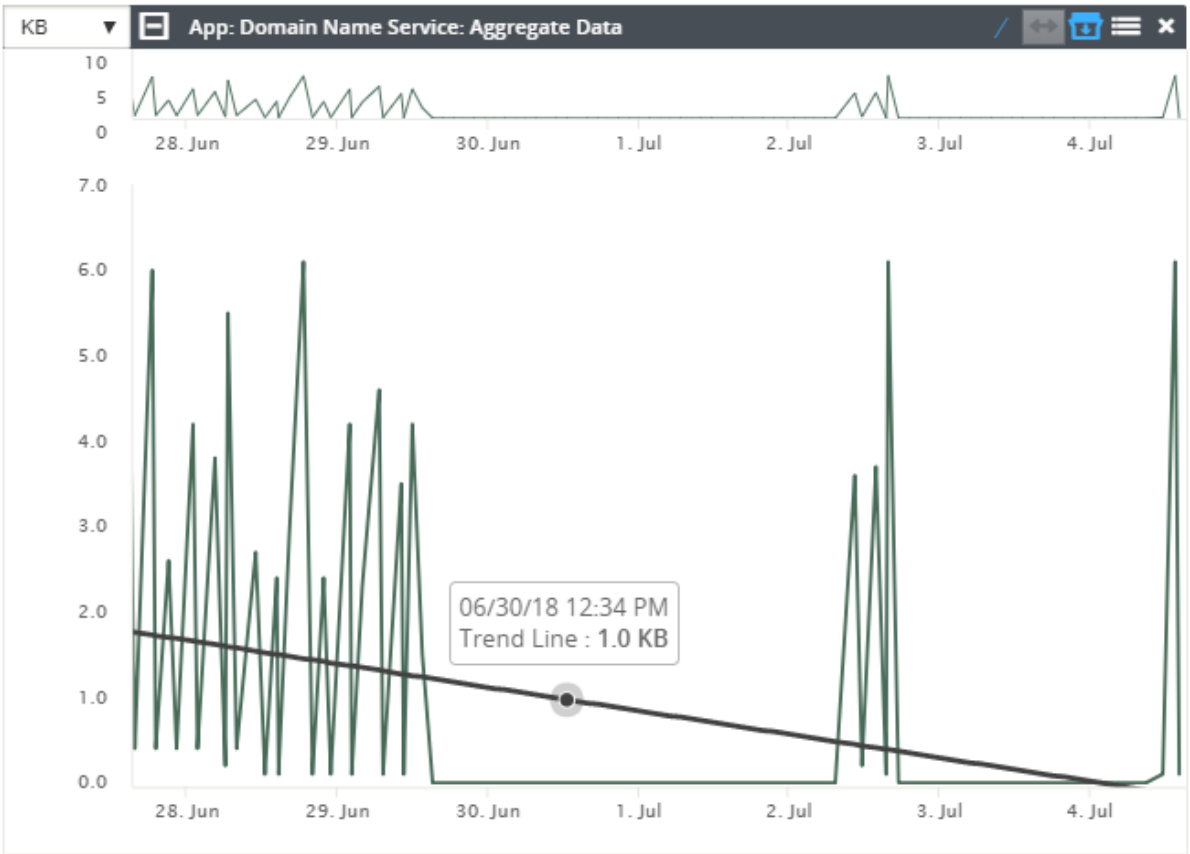
> 提示
>
> 如果您选择多个属性，趋势视图模式下将显示图形以节省垂直空间。单击图表标题可显示和隐藏完全展开的图表。您还可以在图表上显示和隐藏趋势视图和图例。



> 提示
>
> 要缩放图形，请单击并拖动图形绘图区域。放大一个图表可将所有图形缩放至选定的时间，以保持一致的视图。单击“重置”图标 (↔) 重置缩放。



> 提示
>
> 可以通过单击 (/) 图标来显示和隐藏趋势线。



> 注意
>
> 您可以打印图形，或将图形集下载为 CSV 文件。

系统信息

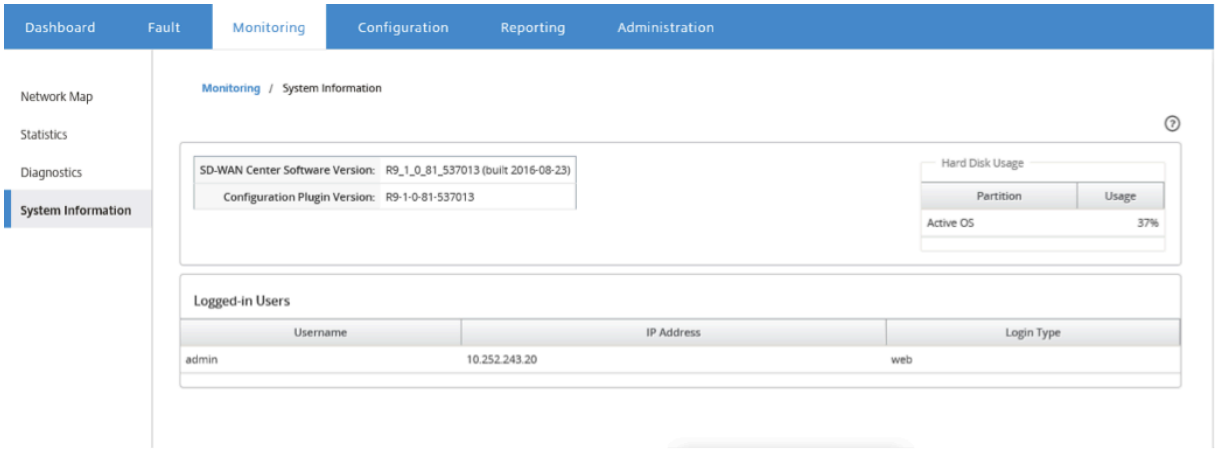
April 13, 2021

系统信息页面上将显示以下信息：

- **Citrix SD-WAN Center** 软件版本：当前安装并在此虚拟机上运行的 Citrix SD-WAN Center 软件版本。
- 配置插件版本：当前安装并在此 Citrix SD-WAN Center 虚拟机中运行的配置编辑器插件的版本。
- 硬盘使用情况：操作系统和数据分区使用的硬盘空间量。
- 已登录的用户：当前登录到此 Citrix SD-WAN Center 虚拟机的每个用户的用户名、IP 地址和登录类型。

要显示系统信息，请执行以下操作：

在 Citrix SD-WAN Center Web 界面中，单击监视选项卡，然后单击系统信息。



报告

April 13, 2021

Citrix SD-WAN Center 提供以下报告：

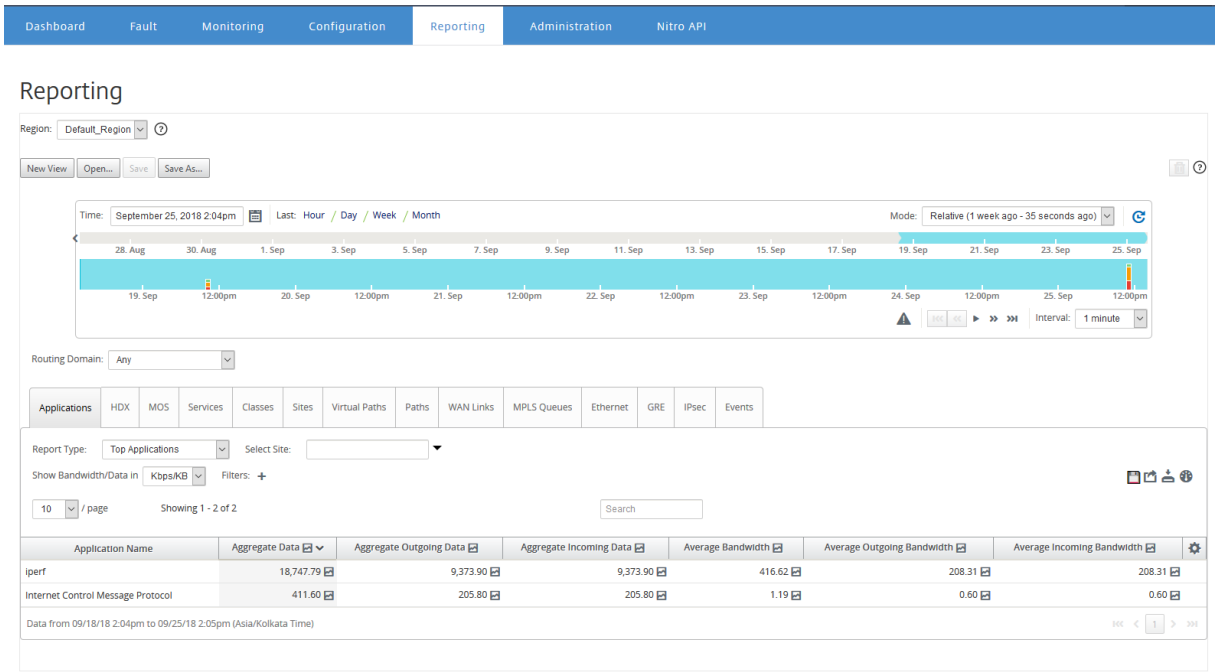
- 应用程序：显示有关传入流量、传出流量以及热门应用程序、站点和应用程序系列的总流量的详细信息。
- **HDX**：显示每个站点的详细 HDX 数据。
- 站点：显示虚拟 WAN 中每个站点的站点级别统计信息。站点行展开以显示为站点筛选的服务表。
- 服务：按服务类型（虚拟路径、Internet、Intranet 和直通）显示虚拟 WAN 中每个站点的摘要统计信息。服务行展开以显示服务类型的单个服务。
- 虚拟路径：显示 SD-WAN 中每个虚拟路径的虚拟路径级别的统计信息。虚拟路径行展开以显示虚拟路径中包含的路径。

> 注意
>
> 虚拟路径数据从这两个端点的角度进行录制，因此，每个虚拟路径可能有两行由记录统计信息的站点来标识。

- 路径：显示虚拟 WAN 中每个路径的路径级统计数据。
- **WAN** 链接：在虚拟 WAN 中的每个站点上显示 WAN 链路级别的每个 WAN 链路级别的统计信息。WAN 链接行展开以显示该 WAN 链接的每种服务类型的使用情况摘要。然后，每个服务类型行将展开以显示该类型的每项服务的使用情况。如果 WAN 链接是一个专用 MPLS 链接，则将显示一个包含 WAN 链接的 MPLS 队列的第二个表。
- **MPLS** 队列：MPLS Queue 行会展开以显示该队列的每个服务类型的使用情况摘要。然后，每个服务类型行将展开以显示该类型的每项服务的使用情况。
- 类：显示虚拟 WAN 中每个虚拟路径的每个类的类级别统计信息。

- **MOS** 分数：平均意见得分 (MOS) 提供了应用程序交付给最终用户的体验质量的数字度量。
- 以太网接口：显示虚拟 WAN 中每个站点的每个接口的以太网接口级别的统计信息。
- **GRE** 隧道：在 WAN 中的每个站点上显示每个 LAN GRE 通道的统计信息。
- **IPsec** 隧道：显示 WAN 中每个站点的每个 IP 安全通道的统计信息。
- 事件：显示在虚拟 WAN 中的每个站点发生的事件的摘要计数。事件行会展开以根据对象类型显示该站点的摘要计数。然后，每个对象类型将展开以显示该类型的每个对象的摘要计数。

在 Citrix SD-WAN Center Web 界面的报告选项卡上，可以查看所有报告或所选报告。您也可以下载报告。

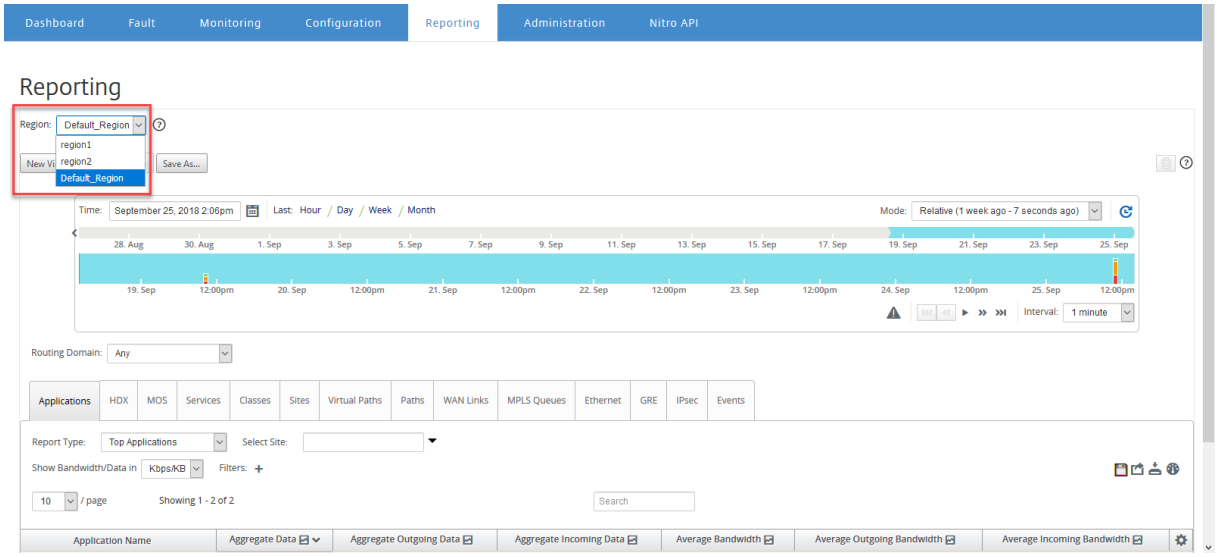


您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。

对于多区域网络，可以选择特定的区域以查看统计报告。

报告数据是从相应区域的收集器中获取的。



> 注意
>
> 在单区域网络部署中，区域 下拉列表不可用。

有关查看不同报告的更多详细信息，请参阅以下主题：

申请报告

带宽报告

课堂报告

以太网接口报告

事件报告

GRE 隧道报告

HDX 报告

IPsec 隧道报告

链接绩效报告

面向应用程序的 MOS

MPLS 队列报告

应用程序报告

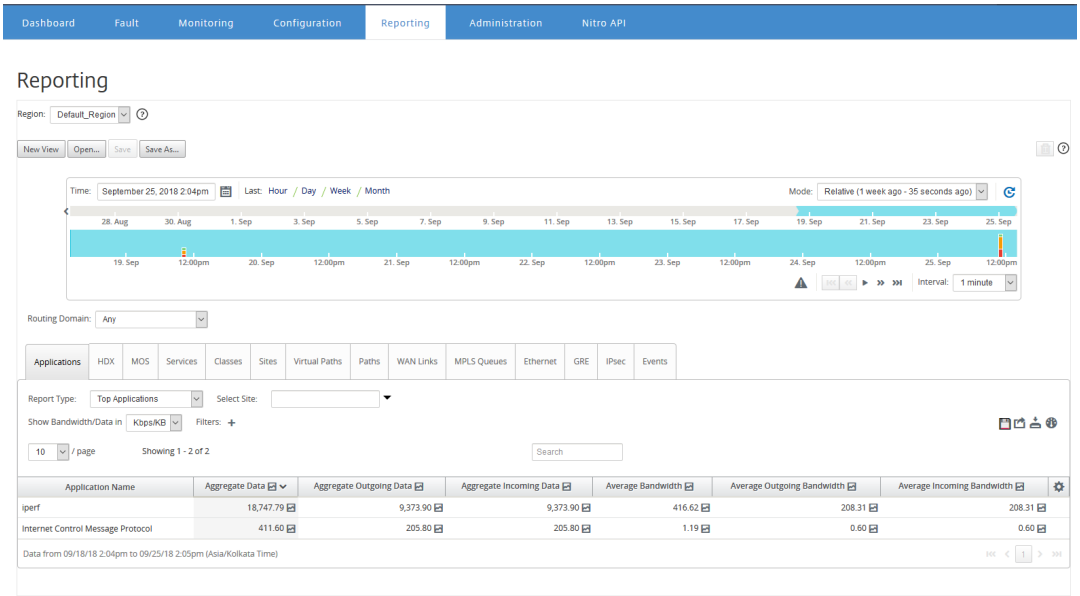
April 13, 2021

通过深数据包检查 (DPI)，SD 设备可以解析通过其传输的流量，并确定应用程序和应用程序系列类型。Citrix SD-WAN 设备记录每个应用程序的传入和传出流量的字节数和带宽。SD-WAN Center 按定义的轮询时间间隔轮询 SD-WAN 设备，获取此数据，并将其显示在控制板和报告中。

您可以查看热门应用程序、热门站点和热门应用程序系列报告。这些报告提供了有关总数、传入和传出数据和带宽的详细信息。

要在 **Citrix SD-WAN Center** 中查看应用程序报告，请执行以下操作：

1. 在 Citrix SD-WAN Center Web UI 中，导航到报告 > 应用程序。
2. 在时间线控件中，选择时间间隔。有关详细信息，请参阅时间线控件。
3. 选择要显示数据的单位。您可以选择以 Kbps、Mbps 或 Gbps 为单位查看报告数据。
4. 在报告类型下拉列表中，选择以下报告类型之一：
   - 最大应用程序：在网络中用于所选时间间隔的最上面的应用程序。您可以按站点名称过滤热门应用程序。默认情况下，将显示所有站点的最上面一个应用程序。
   - 最热门应用程序系列：在网络中使用的热门应用程序系列。您可以按站点名称筛选热门应用程序系列。默认情况下，将显示所有站点的热门应用程序系列。
   - 最多站点：所选时间间隔顶部站点的流量。您可以按应用程序或应用程序系列名称筛选热门站点



对于每种报告类型，可以查看以下数据：

- 聚合的传入数据：从 WAN 进入站点的应用程序数据。
- 聚集输出数据：从站点发送到 WAN 的应用程序数据。
- 聚合数据：传入和传出流量的总和。
- 平均传入带宽：传入应用程序流量的带宽。
- 平均传出带宽：传出应用程序流量的带宽。

- 平均带宽：传入和传出应用程序流量占用的带宽总量。

> 提示
>
> 对于每个值，您可以将鼠标光标悬停在图形图标上以查看小型图形，或者单击以在另一个窗口中打开图形视图。有关详细信息，请参阅统计信息。

应用程序 **QoE** 报告

April 13, 2021

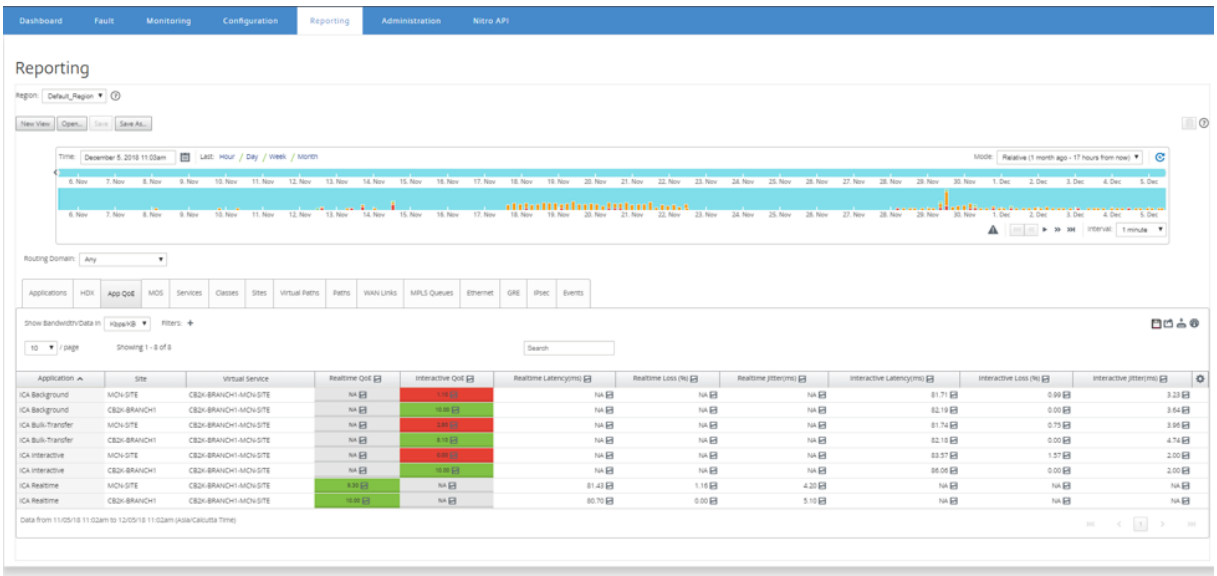
应用程序 **QoE** 是衡量应用程序体验质量的衡量标准。应用程序 QoE 得分范围为 0 至 10，其中 10 代表优异的质量，0 表示质量差。有关详细信息，请参阅应用程序 **QoE** 部分。

要查看应用程序 QoE 报告，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 **>** 应用程序 **QoE**，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间段的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 应用程序：应用程序或应用程序对象名称。
- 站点：站点的名称。
- 虚拟服务：使用的虚拟路径服务。
- 实时 **QoE**：适用于实时流量的 QoE 分数。
- 交互式 **QoE**：适用于交互流量的 QoE 分数。

- 实时延迟：实时流量的延迟（以毫秒为单位）。
- 实时丢失：实时流量的丢失百分比。
- 实时抖动：实时流量观察到的抖动以毫秒为单位。
- 交互式延迟：交互流量的延迟（以毫秒为单位）。
- 交互式丢失：交互流量的丢失百分比。
- 交互抖动：交互流量观察到的抖动（以毫秒为单位）。

> 提示：
>
> 对于每个值，您可以将鼠标光标悬停在图形图标上以查看小型图形，或者单击以在另一个窗口中打开图形视图。

有关详细信息，请参阅统计信息。

带宽报告

April 13, 2021

Citrix SD-WAN Center 提供从 SD-WAN 网络中的不同站点轮询的带宽统计数据的中央视图。

在 Citrix SD-WAN 配置中，流过虚拟路径的通信被分类为属于实时、交互或批量类类型。这些类是预定义的，但您可以自定义这些类并对其应用规则。有关详细信息，请参阅自定义类和规则（按 IP 地址和端口号）。

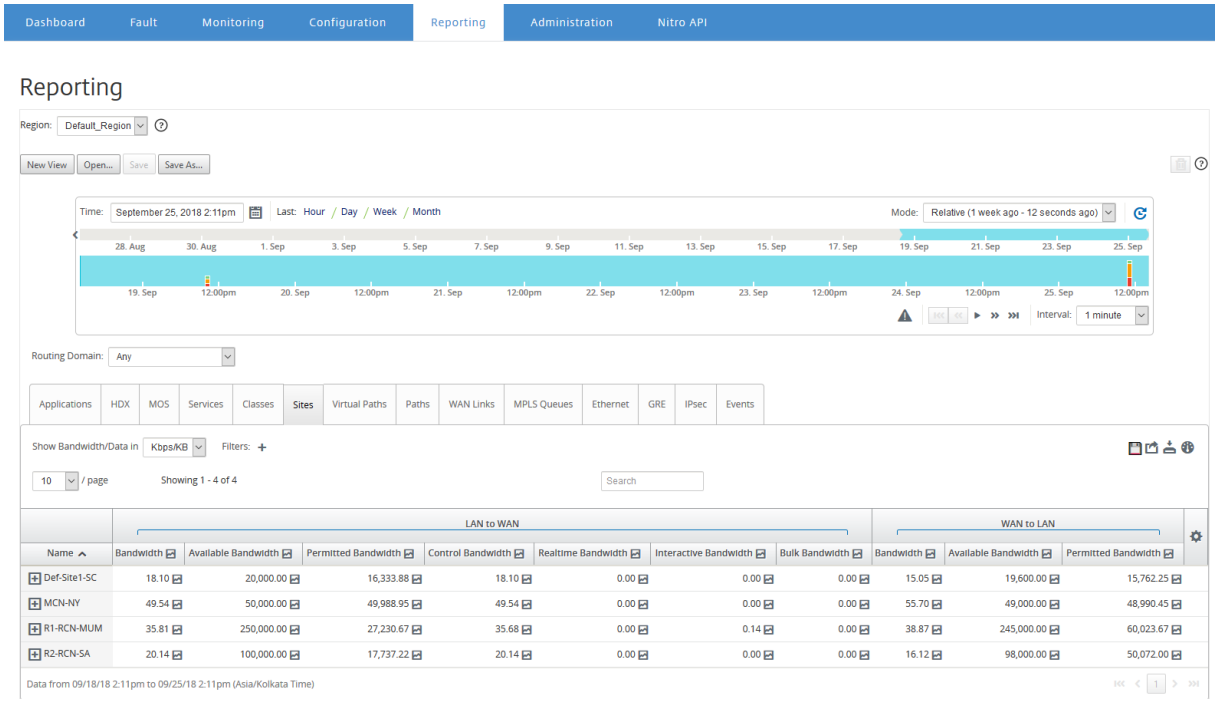
使用 Citrix SD-WAN Center 时，可以查看每个站点、路径或 WAN 链接级别上属于这些类类型的应用程序所占用的带宽统计数据以及基本带宽统计数据。

要查看带宽统计数据，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > 站点，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 带宽：所有数据包类型占用的带宽总量。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。例如，在上方屏幕截图中，SITE2、带宽 = 1120.99 + 166.61 + 117.21 + 810.78 + 26.40
- 可用带宽：分配给站点的所有 WAN 链接的总带宽。
- 控制带宽：用于传输包含路由、计划和链接统计信息的控制数据包的带宽。
- 允许的带宽：传输信息可用的带宽。
- 实时带宽：属于 Citrix SD-WAN 配置中的实时类类型的应用程序所占用的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 Citrix SD-WAN 配置中的交互类类型的应用程序所占用的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 Citrix SD-WAN 配置中的大容量类类型的应用程序所占用的带宽。这些应用程序涉及的人工干预非常少，通常由系统本身处理（例如，FTP、备份操作）。

课堂报告

April 13, 2021

可以将虚拟服务分配给特定的 QoS 类，并且可以将不同的带宽限制应用于不同的类。一个类可以是以下三种基本类型之一：

- 实时类：提供要求提示服务达到一定带宽限制的通信流。低延迟优先于总吞吐量。

- 交互类：提供对丢失和延迟非常敏感的通信流。交互类的优先级低于实时，但其优先级高于批量流量。
- 大容量类：提供需要较高带宽并且对丢失敏感的通信流。批量课程的优先级最低。

为不同的类指定不同的带宽要求时，虚拟路径计划程序可以对来自相同类型的多个类的竞争性带宽请求进行仲裁。计划程序使用“层次结构公平服务曲线”(HFSC) 算法来实现各类的公平。

有关自定义类的详细信息，请参阅自定义类。

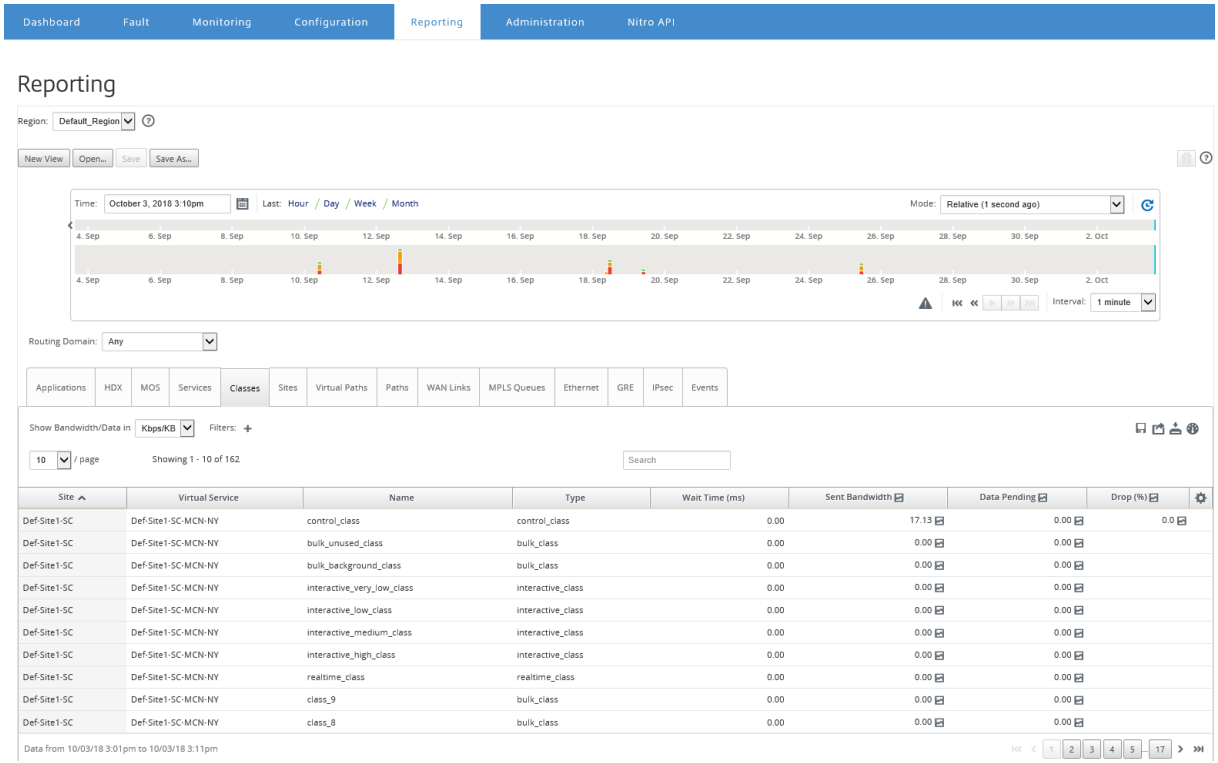
要查看类统计信息，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > 类，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间段的报告。有关详细信息，请参阅时间线控件。

> 注意
>
> 您可以查看过去 30 天的课堂数据。超出此时间段的所有数据都将自动从 SD-WAN Center 收集器和各自的区域收集器中删除。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 名称：类名称
- 类型：类类型。Reeleatime、交互式或批量。
- 等待时间：传输数据包的时间间隔（以毫秒为单位）。
- 发送带宽：传输的带宽

- 发送的数据：发送的数据（以 Kbps 为单位）。
- 发送的数据包数：发送的数据包数。
- 待决数据：要发送的数据，以 Kbps 为单位。
- 待决数据包：要发送的数据包数。
- 丢弃：丢弃的数据百分比。
- 丢弃的数据：丢弃的数据，以 Kbps 为单位。
- 丢弃的数据包：由于网络拥挤而丢弃的数据包数。
- 数据覆盖率：可用数据的所选时间段的百分比。

> 注意
>
> 单击设置图标以选择要查看的指标。

以太网接口报告

April 13, 2021

Citrix SD-WAN Center 提供了 SD-WAN 网络中不同 Citrix SD-WAN 设备上的所有以太网接口的中央视图。这可以帮助您在故障排除过程中快速查看是否有任何端口关闭。您还可以在每个端口查看传输和接收的带宽或数据包详细信息。您还可以查看在特定时间段内这些接口上发生的错误数。

在设置 SD-WAN 网络过程中，将在每个 Citrix SD-WAN 设备上配置以太网接口。

有关为 MCN 站点配置接口组的信息，请参阅配置 MCN。

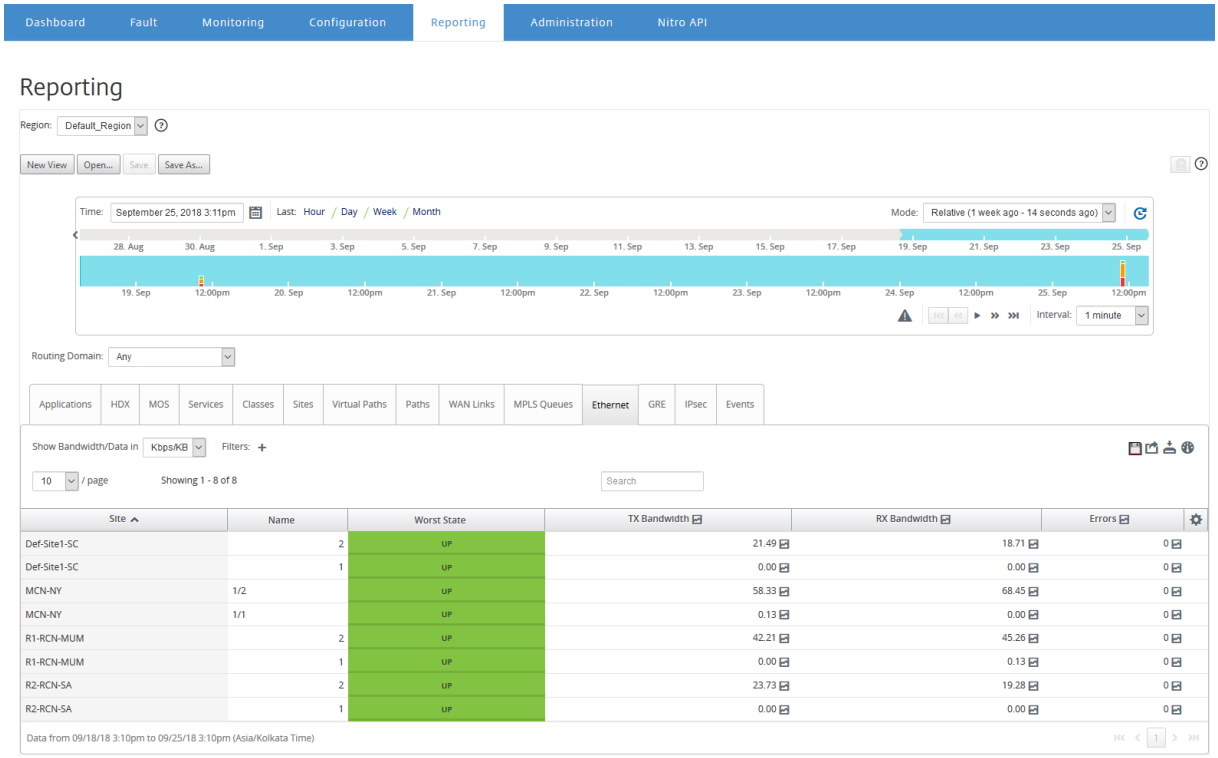
有关为分支站点配置接口组的信息，请参阅配置分支节点。

查看以太网接口统计信息：

在 Citrix SD-WAN Center 中，导航到报告 > **Ethernet**，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 名称：以太网接口的名称。
- 最差状态：在选定时间段内观察到的最差状态。
- **TX** 带宽：传输的带宽。
- **RX** 带宽：已接收带宽。
- **TX** 数据包：传输的数据包数。
- **RX** 数据包：接收的数据包数。
- 错误数：在选定的时间段内观察到的错误数。
- 数据覆盖率：数据可用的选定时间段的百分比。

> 注意
>
> 单击设置图标以选择要查看的指标。

事件报告

April 13, 2021

您可以查看在 SD-WAN 网络中的每个站点发生的不同事件的计数。

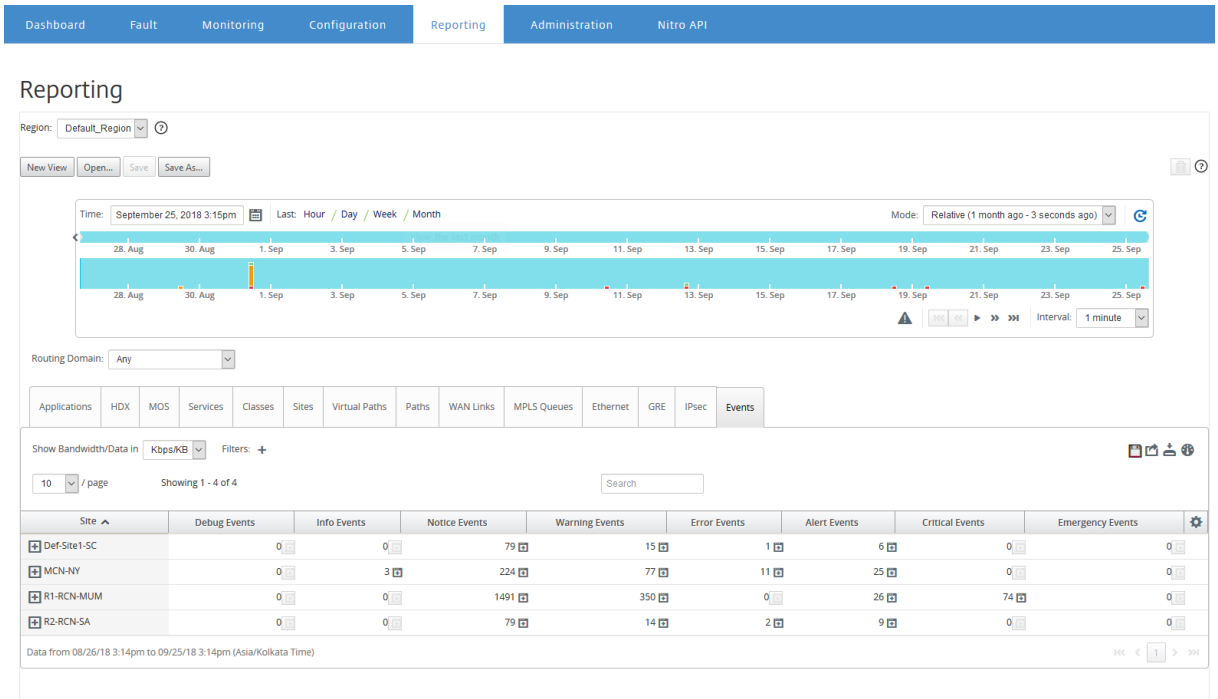
有关事件的详细信息，请参阅事件。

要查看事件统计信息，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > 事件，并在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 信息事件：在选定时间段内发生的信息事件数。这些都是低级别的事件。
- 通知事件：在选定时间段内发生的通知事件数。这些是管理员应该了解的事件。
- 警告事件：在选定时间段内发生的警告事件数。这些事件需要在不久的将来采取行动。
- 错误事件数：在选定的时间段内发生的错误事件数。这些事件表示某种类型的错误。
- 警报事件：在选定时间段内发生的警报事件数。这些事件可能需要采取行动。
- 严重事件：在选定时间段内发生的关键事件数。这些事件表明危机迫在眉睫。
- 紧急事件：在选定时间段内发生的紧急事件数。这些事件指示直接危机（例如，电源故障、风扇故障、超出硬盘阈值、禁用服务）。
- 调试事件：在选定时间段内发生的调试事件数。在 Citrix SD-WAN 设备上使用测试电子邮件或测试 Syslog 选项时，将生成调试事件。

> 注意
>
> 单击设置图标以选择要查看的指标。

下表列出了报告事件的对象状态更改的几个示例。

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

可以将 Citrix SD-WAN Center 配置为以电子邮件、SNMP 陷阱或 syslog 消息的形式发送不同事件类型的外部事件通知。有关详细信息，请参阅 事件通知。

GRE 隧道报告

April 13, 2021

您可以使用隧道机制在另一协议中传输一个协议的数据包。携带其他协议的协议称为传输协议，而携带的协议称为乘客协议。通用路由封装 (GRE) 是一种通道机制，它使用 IP 作为传输协议，并可以传输许多不同的乘客协议。

隧道源地址和目标地址用于标识隧道中虚拟点对点链路的两个端点。

有关在 Citrix SD-WAN 设备上配置 GRE 通道的详细信息，请参阅 GRE 隧道。

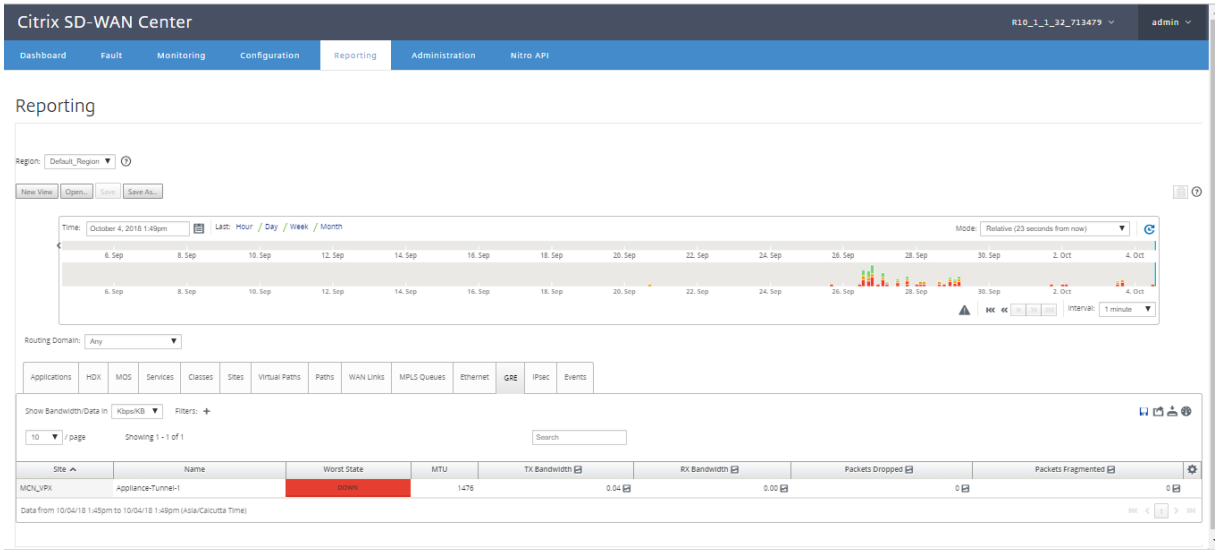
Citrix SD-WAN Center 可以显示您的 Citrix SD-WAN 网络中配置的所有 GRE 通道的状态。

要查看 **GRE** 通道统计数据，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > **GRE**，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 最差状态：在选定时间段内观察到的最差状态。
- **MTU**：最大传输单位—可以通过特定链路传输的最大 IP 数据报的大小。
- **TX** 带宽：传输的带宽。
- **RX** 带宽：已接收带宽。
- **TX** 数据包：传输的数据包数。
- **RX** 数据包：接收的数据包数。
- 丢弃的数据包：由于网络拥挤而丢弃的数据包数。
- 零碎的数据包：零碎的数据包数。数据包将分段以创建小型数据包，该数据包可以通过传输的 MTU 小于原始数据报。这些碎片由接收主机重新组装。
- 数据覆盖率：数据可用的选定时间段的百分比。

> 注意
>
> 单击设置图标以选择要查看的指标。

HDX 报告

April 13, 2021

从下拉列表中选择以下报告类型之一：

- HDX 站点统计数据
- HDX 摘要（适用于 HDX 信息通道可用和不可用的会话）
- HDX 用户会话（仅适用于仅 HDX 信息通道可用的会话）
- HDX Apps（仅适用于仅 HDX 信息通道可用的会话）

HDX 站点统计

HDX 报告提供了每个站点的详细 HDX 数据。每个站点的数据显示在两个视图中。

Summary View（摘要视图）

摘要视图显示站点的以下数据：

- **QoE** 指 数-体验质量 (QoE) 是介于 0—100 之间的数值。价值越高，用户体验越好。
- 用户—站点上的活跃用户数。
- **TCP** 流 -站点上使用 TCP 协议的活动 HDX 会话数。
- **UDP** 流—站点上使用 UDP 协议的活动 HDX 会话数。
- 会话—站点上包括小规模集成 (SSI) 和中规模集成 (MSI) 会话的活动 HDX 会话的总数。

详情视图

您可以单击单个站点以查看影响 QoE 的所有变量的详细信息。每对行都显示给定虚拟路径在本地和远程端计算的数据的 QoE 因子。

影响 QoE 的延迟、抖动和数据包丢弃变量是 Citrix SD-WAN 设备正在测量的有效数字。例如，网络中的数据包丢弃的百分比可能更高，因为 Citrix SD-WAN 通过自己的协议纠正数据包丢弃，应用程序看到的有效数据包丢失将会小得多，从而提高 HDX 应用程序的 QoE。

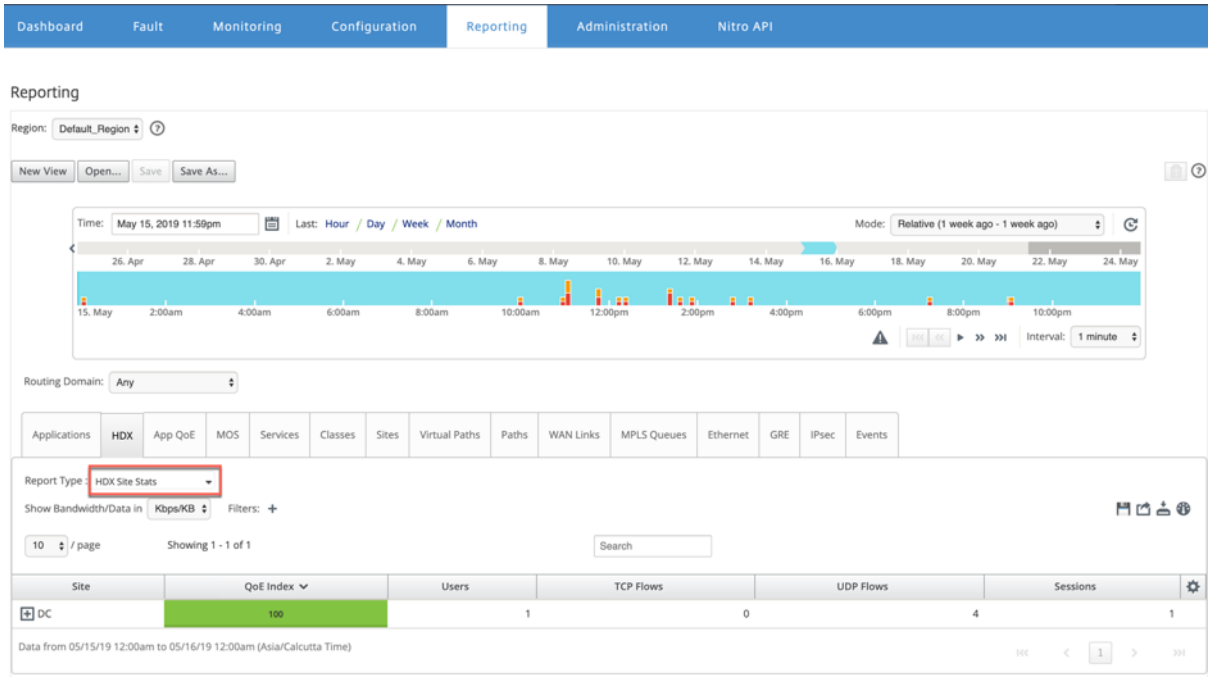
同样，通过数据包重复来改进延迟还会改进 HDX 应用程序的 QoE。换句话说，Citrix SD-WAN 通过改善影响 QoE 的因素来提高 HDX 流量的 QoE。有关详细信息，请参阅HDX QoE。

要查看 **HDX** 报告，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到 报告 > **HDX**，然后在时间轴控件中选择一个期间。

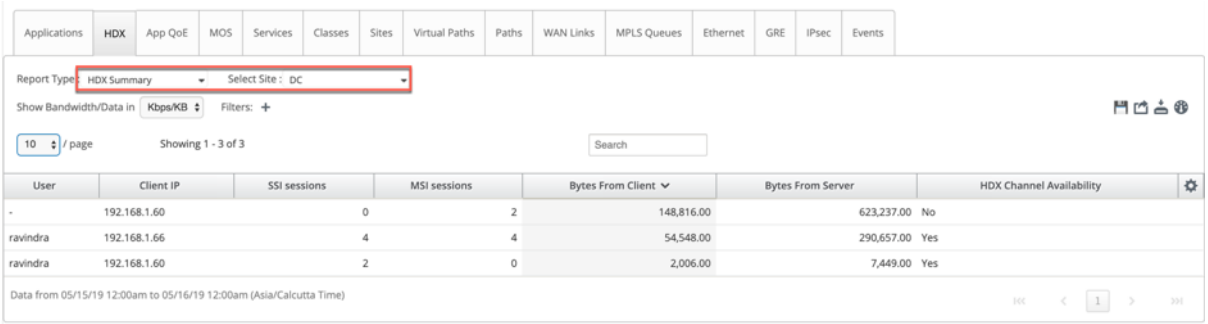
您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



HDX 摘要

从下拉列表中选择 **HDX** 摘要报告和站点。“HDX 摘要”报告显示在选定时间段内登录的每个用户的报告。

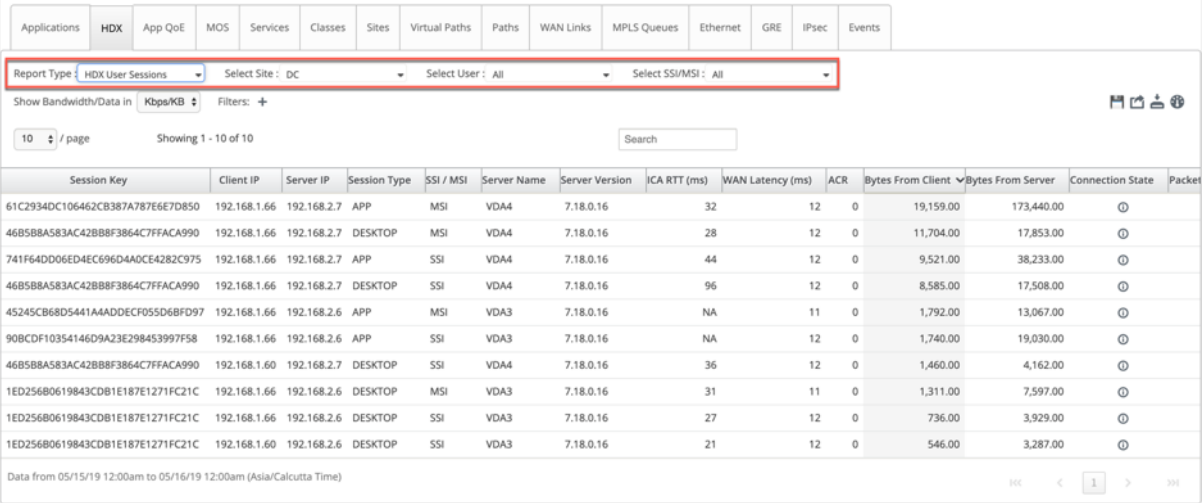


在 HDX 摘要报告中，您可以查看以下参数：

- 用户：用户的名称。
- 客户端 **IP**：客户端 IP 地址。
- **SSI** 会话：活动单流 ICA (SSI) 会话数。
- **MSI** 会话：活动多流 ICA (MSI) 会话数。
- 来自客户端的字节数：客户端大小（以字节为单位）。
- 来自服务器的字节数：服务器的大小（以字节为单位）。
- **HDX** 通道可用性：提供 HDX 信息通道可用性状态为是/否。如果频道不可用，则用户名显示为连字符 (-)。

HDX 用户会话

在 HDX 用户会话报告中，您可以查看每个用户使用的每个会话详细信息。从下拉列表中选择站点、用户、SSI 或 MSI。默认情况下，选择用户和选择 **SSI/MSI** 字段显示全部。



Session Key	Client IP	Server IP	Session Type	SSI / MSI	Server Name	Server Version	ICA RTT (ms)	WAN Latency (ms)	ACR	Bytes From Client	Bytes From Server	Connection State	Packet
61C2934DC106462CB387A787E6E7D850	192.168.1.66	192.168.2.7	APP	MSI	VDA4	7.18.0.16	32	12	0	19,159.00	173,440.00		
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.66	192.168.2.7	DESKTOP	MSI	VDA4	7.18.0.16	28	12	0	11,704.00	17,853.00		
741F64DD06ED4EC696D4A0CE4282C975	192.168.1.66	192.168.2.7	APP	SSI	VDA4	7.18.0.16	44	12	0	9,521.00	38,233.00		
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.66	192.168.2.7	DESKTOP	SSI	VDA4	7.18.0.16	96	12	0	8,585.00	17,508.00		
45245CB68D5441A4ADDECF055D6BFD97	192.168.1.66	192.168.2.6	APP	MSI	VDA3	7.18.0.16	NA	11	0	1,792.00	13,067.00		
90BCDF10354146D9A23E298453997F58	192.168.1.66	192.168.2.6	APP	SSI	VDA3	7.18.0.16	NA	12	0	1,740.00	19,030.00		
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.60	192.168.2.7	DESKTOP	SSI	VDA4	7.18.0.16	36	12	0	1,460.00	4,162.00		
1ED256B0619843CDB1E187E1271FC21C	192.168.1.66	192.168.2.6	DESKTOP	MSI	VDA3	7.18.0.16	31	11	0	1,311.00	7,597.00		
1ED256B0619843CDB1E187E1271FC21C	192.168.1.66	192.168.2.6	DESKTOP	SSI	VDA3	7.18.0.16	27	12	0	736.00	3,929.00		
1ED256B0619843CDB1E187E1271FC21C	192.168.1.60	192.168.2.6	DESKTOP	SSI	VDA3	7.18.0.16	21	12	0	546.00	3,287.00		

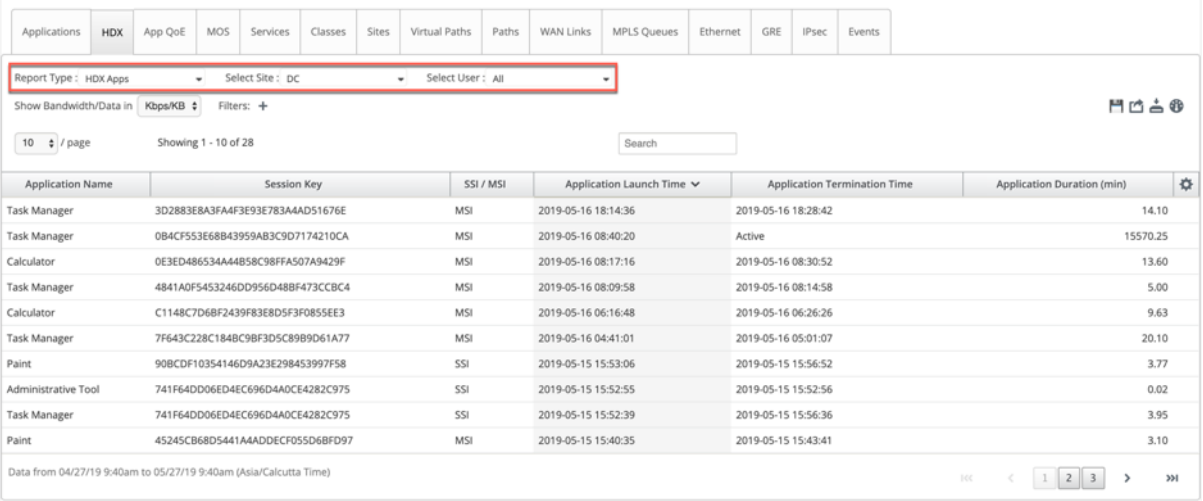
您可以使用“搜索”或“筛选器**:+** ”选项根据您的要求找出所需的会话信息。

- 会话键：会话键代表 ICA 会话的唯一标识。
- 客户端 **IP**：每个会话的客户端 IP 地址。
- 服务器 **IP**：每个会话的服务器 IP 地址。
- 会话类型：会话的类型（桌面、应用程序）。
- **SSI/MSI**：显示是 SSI 会话还是 MSI 会话。
- 服务器名称：显示服务器的名称。
- 服务器版本：显示服务器的版本。
- **ICA RTT (**毫秒**)**：显示 ICA 往返时间 (RTT)，以毫秒为单位。这是客户端和服务器之间的端到端往返时间。
- **WAN** 延迟：WAN 上的延迟，在虚拟路径上的两个 SD-WAN 之间。此延迟不包括客户端或服务器端网络延迟。
- **ACR**：显示客户端自动重新连接计数。
- 来自客户端的字节数：客户端大小（以字节为单位）。
- 来自服务器的字节数：服务器的大小（以字节为单位）。
- 连接状态：悬停鼠标可查看连接状态。
  - 对于 MSI，有四个连接。这些连接是 L4 级别（TCP/UDP 状态）。
  - 对于 SSI，只有一次连接。

- 来自客户端的数据包：客户端的数据包数。
- 来自服务器的数据包：来自服务器的数据包数。

HDX 应用程序

您可以查看特定用户或所有用户使用的所有应用程序。选择站点和用户以查看应用程序详细信息。



- 应用程序名称：提供 HDX 应用程序的名称。
- 会话密钥：提供用于该特定应用程序的唯一会话密钥。
- **SSI/MSI**：显示是 SSI 会话还是 MSI 会话。
- 应用程序启动时间：提供应用程序启动的时间和日期。
- 应用程序终止时间：提供应用程序终止时间和日期。如果某个应用程序处于活动状态，则该应用程序将显示为活动状态，而非终止时间。
- 应用程序持续时间 **(**分钟**)**：提供应用程序时间间隔（分钟）。

> 注意
>
> - 如果存在任何意外错误，例如，如果 HDX 会话信息在设备上不可用，则即使启用了 HDX 用户报告，也不会显示基于 **HDX** 用户的报 告。报表中的某些字段（如用户名、服务器名称、服务器版本、ICA RTT）可能显示为不适用。
> - 只有当 SD-WAN 从 Xen 应用程序/Xen 桌面服务器接收应用程序终止时间时，才会显示 **HDX** 应用程序报告中的应用程序终止时间。否则，即使已关闭，部分应用程序也报告处于活动状态。
> - 由于 Citrix Virtual Apps and Desktops（以前为 XenApp 和 XenDesktop）的限制，HDX 应用程 序报告中显示的应用程序名称 仅限于 19 个字符。

IPsec 隧道报告

April 13, 2021

IP 安全 (IPsec) 协议提供安全服务（如加密敏感数据、身份验证、防止重放以及 IP 数据包的数据机密性）。封装安全有效负载 (ESP) 和身份验证头 (AH) 是用于提供这些安全服务的两种 IPsec 安全协议。

在 IPsec 通道模式下，整个原始 IP 数据包受到 IPsec 保护。原始 IP 数据包将打包并加密，并在通过 VPN 通道传输数据包之前添加一个新 IP 报头。

有关在 Citrix SD-WAN 设备上配置 IPsec 隧道的更多信息，请参阅 IPsec 隧道终止。

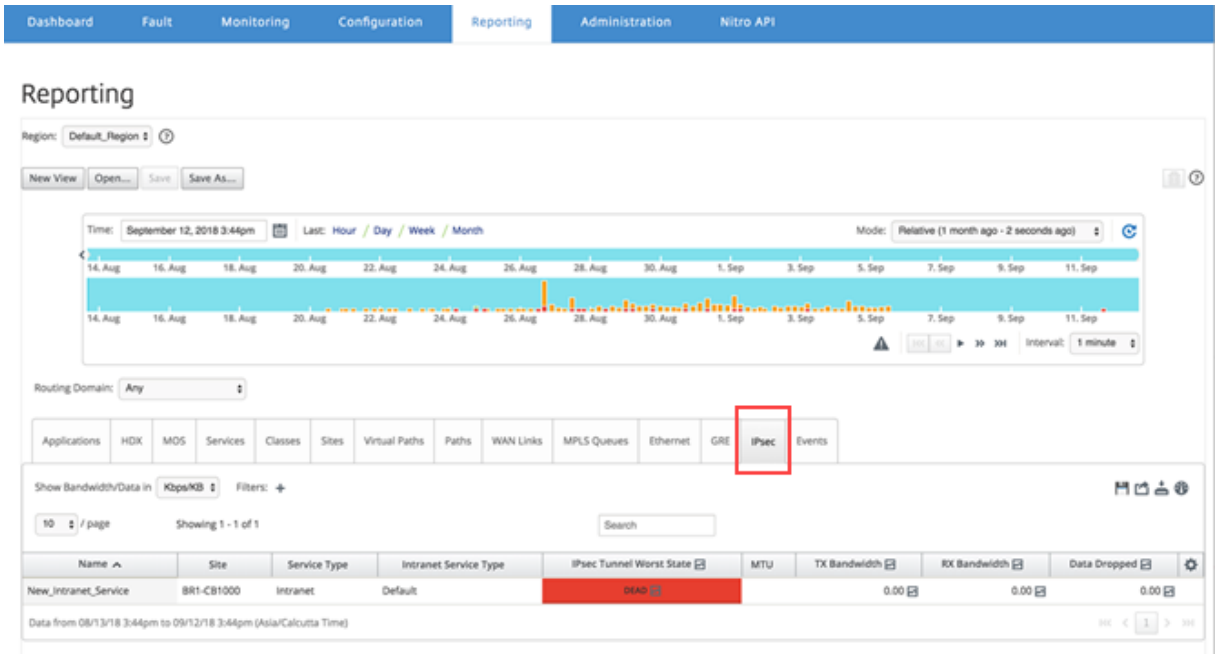
Citrix SD-WAN Center 可以显示您的 Citrix SD-WAN 网络中配置的所有 IPsec 通道的状态。

要查看 **IPsec** 通道统计数据**,** 请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 >**IPsec** 通道，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 名称：应用程序名称。
- 站点：站点的名称。
- 服务类型：服务类型。
- **Intranet** 服务类型：与 IPsec 通道关联的 Intranet 服务类型。下面是 Intranet 服务的类型：
  - 默认值

  - Microsoft Azure 虚拟广域网
  - Zscaler
  - Citrix SaaS Gateway

- **IPsec** 最差状态：在选定时间段内观察到的最差状态。
- **MTU**：最大传输单位—可以通过特定链路传输的最大 IP 数据报的大小。
- **TX** 带宽：传输的带宽。
- **RX** 带宽：已接收带宽。
- **TX** 数据包：传输的数据包数。
- **RX** 数据包：接收的数据包数。
- 丢弃的数据：丢弃的数据，以 Kbps 为单位。
- 丢弃的数据包：丢弃的数据包数。

> 注意
>
> 单击设置图标以选择要查看的指标。

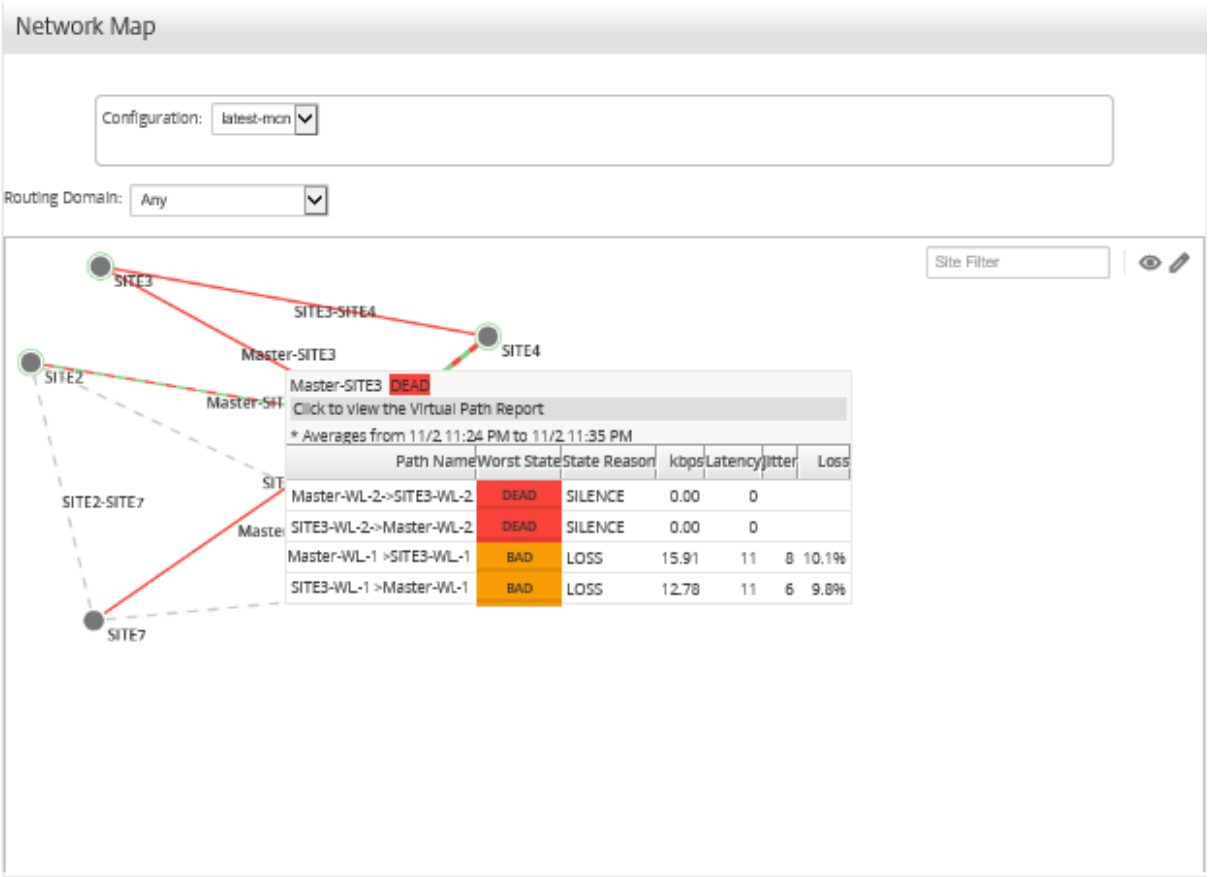
链路性能报告

April 13, 2021

Citrix SD-WAN Center 可以在站点、服务、虚拟路径或 WAN 链路级别显示性能统计信息。

考虑一个组织 ABC 有四个分支机构的网络。SITE3 已经报告了电压降低情况。也就是说，员工有时无法查看 Intranet 页面。您怀疑这是因为底层链接的性能。

您可以通过将鼠标光标悬停在控制板上的网络地图上的站点和数据中心之间的路径上，获得链接统计信息的高级视图。



在上面的屏幕截图中，站点 3 与主控制器节点 (MCN) 之间有两个 WAN 链接（WL-1 和 WL-2），并显示最近 10 分钟的统计信息。

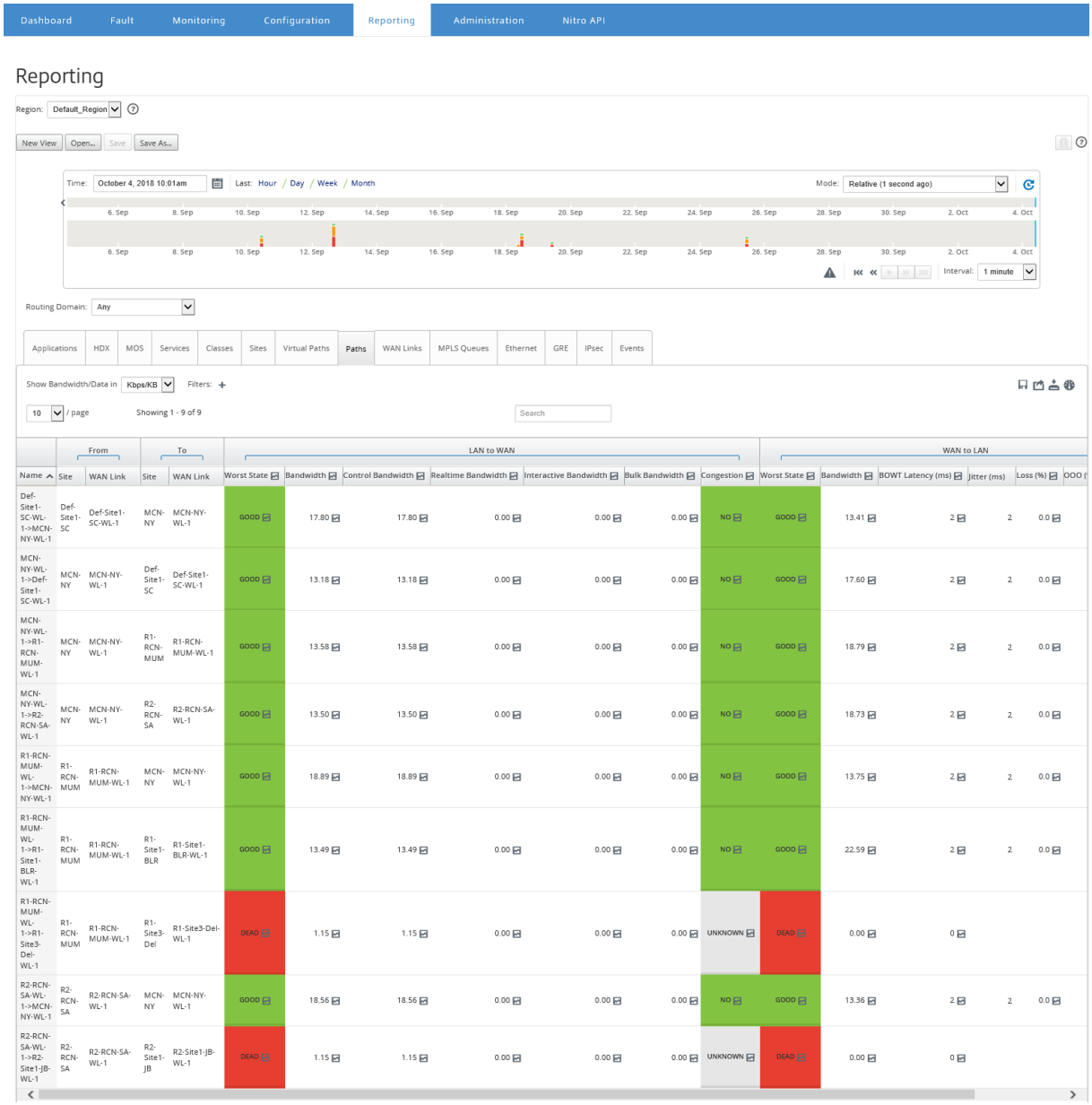
虚拟路径 Master-WL2->SITE3-WL2 and SITE3-WL2 ->Master-WL2 无法正常工作，备选路径 Master-WL1->SITE3-WL1 和 SITE3-WL1 ->Master-WL1 处于不良状况，因此会导致传输数据占大量百分比。这是 SITE3 上电压降低的可能原因。

或者，您可以导航到报告 > 路径，以查看链接统计信息。

在日程表控制中，选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



Name	From Site	From WAN Link	To Site	To WAN Link	LAN to WAN Worst State	LAN to WAN Bandwidth	LAN to WAN Control Bandwidth	LAN to WAN Realtime Bandwidth	LAN to WAN Interactive Bandwidth	LAN to WAN Bulk Bandwidth	LAN to WAN Congestion	WAN to LAN Worst State	WAN to LAN Bandwidth	WAN to LAN BOWT Latency (ms)	WAN to LAN Jitter (ms)	WAN to LAN Loss (%)	WAN to LAN OOO
Def-Site1-SC-WL-1->MCN-NY-WL-1	Def-Site1-SC	Def-Site1-SC-WL-1	MCN-NY	MCN-NY-WL-1	GOOD	17.80	17.80	0.00	0.00	0.00	NO	GOOD	13.41	2	2	0.0	
MCN-NY-WL-1->Def-Site1-SC-WL-1	MCN-NY	MCN-NY-WL-1	Def-Site1-SC	Def-Site1-SC-WL-1	GOOD	13.18	13.18	0.00	0.00	0.00	NO	GOOD	17.60	2	2	0.0	
MCN-NY-WL-1->R1-RCN-MUM-WL-1	MCN-NY	MCN-NY-WL-1	R1-RCN-MUM	R1-RCN-MUM-WL-1	GOOD	13.58	13.58	0.00	0.00	0.00	NO	GOOD	18.79	2	2	0.0	
MCN-NY-WL-1->R2-RCN-SA-WL-1	MCN-NY	MCN-NY-WL-1	R2-RCN-SA	R2-RCN-SA-WL-1	GOOD	13.50	13.50	0.00	0.00	0.00	NO	GOOD	18.73	2	2	0.0	
R1-RCN-MUM-WL-1->MCN-NY-WL-1	R1-RCN-MUM	R1-RCN-MUM-WL-1	MCN-NY	MCN-NY-WL-1	GOOD	18.89	18.89	0.00	0.00	0.00	NO	GOOD	13.75	2	2	0.0	
R1-RCN-MUM-WL-1->R1-Site1-BLR-WL-1	R1-RCN-MUM	R1-RCN-MUM-WL-1	R1-Site1-BLR	R1-Site1-BLR-WL-1	GOOD	13.49	13.49	0.00	0.00	0.00	NO	GOOD	22.59	2	2	0.0	
R1-RCN-MUM-WL-1->R1-Site3-Del-WL-1	R1-RCN-MUM	R1-RCN-MUM-WL-1	R1-Site3-Del	R1-Site3-Del-WL-1	DEAD	1.15	1.15	0.00	0.00	0.00	UNKNOWN	DEAD	0.00	0			
R2-RCN-SA-WL-1->MCN-NY-WL-1	R2-RCN-SA	R2-RCN-SA-WL-1	MCN-NY	MCN-NY-WL-1	GOOD	18.56	18.56	0.00	0.00	0.00	NO	GOOD	13.36	2	2	0.0	
R2-RCN-SA-WL-1->R2-Site1-JB-WL-1	R2-RCN-SA	R2-RCN-SA-WL-1	R2-Site1-JB	R2-Site1-JB-WL-1	DEAD	1.15	1.15	0.00	0.00	0.00	UNKNOWN	DEAD	0.00	0			

您可以查看以下指标：

- 名称：路径名称。
- 从 (站点和 **WAN** 链接)：来源站点和 WAN 链接。
- 到 (站点和 **WAN** 链接)：目标站点和 WAN 链接。
- **LAN** 到 **WAN**
  - 工作状态：
  - 带宽：所有数据包类型占用的带宽总量。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。
  - 控制带宽：用于传输包含路由、计划和链接统计信息的控制数据包的带宽。
  - 实时带宽：属于 SD-WAN 配置中的实时类类型的应用程序占用的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。

  - 交互带宽：在 SD-WAN 配置中属于交互类类型的应用程序占用的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
  - 批量带宽：在 SD-WAN 配置中属于散装类类型的应用程序占用的带宽。这些应用程序涉及的人工干预非常少，通常由系统本身处理（例如，FTP、备份操作）。
  - 拥堵：由于 WAN 中数据包传输量增加或出现意外延迟而导致出现拥塞。

- **WAN** 到 **LAN**：
  - 最差状态：在一段时间内观察到 LAN 状态的最差的 WAN。
  - 带宽：
  - **BOWT** 延迟 **(**毫秒**)**：将数据包从一个点移动到另一个点（以毫秒为单位）所用的最佳单向时间 (BOWT)。
  - 抖动 **(**毫秒**)**：已接收的数据包延迟的变化，以毫秒为单位。
  - 丢失 **(%)**：数据包丢失的百分比。
  - **OOO (%)**：未按照正确顺序或顺序 (OOO) 排列的数据包百分比。
  - 拥堵：由于 WAN 中数据包传输量增加或出现意外延迟而导致出现拥塞。

单击设置图标，然后选择要在报告中查看的参数。

面向应用程序的 **MOS**

April 13, 2021

平均意见得分 (MOS) 提供了应用程序交付给最终用户的体验质量的数字度量。它主要用于 VoIP 应用程序。在 Citrix SD-WAN 中，MOS 还可以通过将流量判断为 VoIP 呼叫来评估非 VoIP 应用程序的质量。

Citrix SD-WAN Center 计算并显示通过虚拟路径的流量的 MOS。为每个 Citrix SD-WAN 设备上的每个应用程序启用估算 **MOS** 选项，以在 Citrix SD-WAN Center 中显示这些应用程序的 MOS 成绩。

有关为 Citrix SD-WAN 中的应用程序启用 MOS 的详细信息，请参阅添加 规则组并启用 MOS。

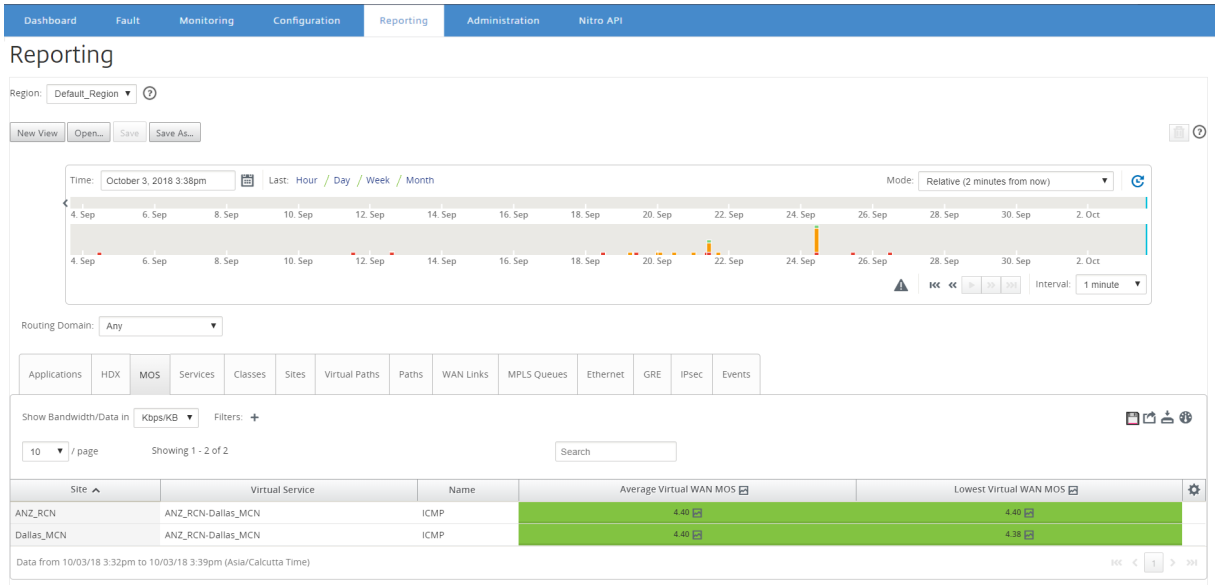
> 注意
>
> 在“规则”下，启用“跟踪性能”选项，以估算应用程序的 MOS 并在 Citrix SD-WAN Center 中显示。有关规则的详细信息，请参阅规则（按 IP 地址和端口号）。

要查看应用程序的 **MOS,** 请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > 应用程序，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- 名称：应用程序的名称。
- 平均虚拟 **WAN MOS**：在选定时间段内计算出的平均质量分数。
- 最低虚拟 **WAN MOS**：在选定时间段内计算的最低质量分数。

分数按如下所示进行评分：

- 5 —用户非常满意。
- 4 —用户感到满意。
- 3 —用户不满意。
- 2 —用户非常不满意。
- 1 —不推荐。

MPLS 队列报告

April 13, 2021

MPLS 队列提供由标准差分服务代码点 (DSCP) 标记控制的服务队列。这些标签控制虚拟 WAN 上两个站点之间的服务质量。

MPLS 队列允许 MPLS 提供程序根据 DSCP 标记来标识流量，以便提供程序能够应用服务类。

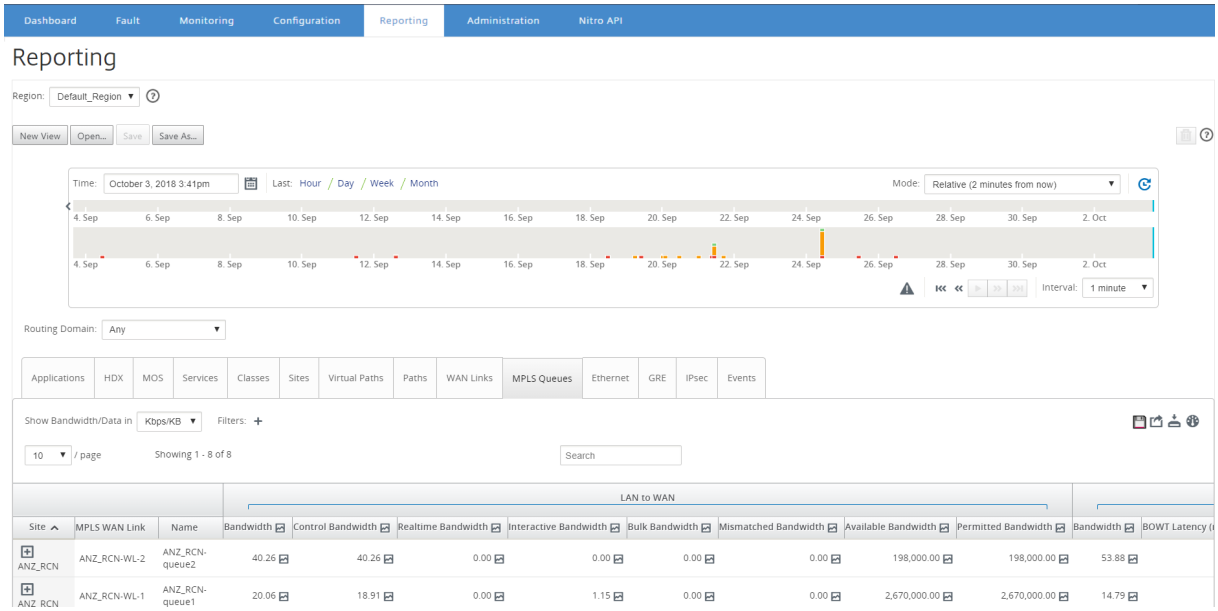
有关在 Citrix SD-WAN 设备上配置专用 MPLS WAN 链接的详细信息，请参阅 MPLS 队列。

要查看 MPLS 队列统计信息，请执行以下操作：

在 Citrix SD-WAN Center 中，导航到报告 > **MPLS** 队列，然后在日程表控制中选择一个时间段。

您可以使用时间线控件选择和查看特定时间范围的报告。有关详细信息，请参阅时间线控件。

您还可以创建、保存和打开报表视图。有关详细信息，请参阅管理视图。



您可以查看以下指标：

- **MPLS WAN** 链接：MPLS 队列所属的 MPLS WAN 链路的名称。
- 名称：DSCP 标记名称。
- 带宽：所有数据包类型占用的带宽总量。带宽 = 控制带宽 + 实时带宽 + 交互带宽 + 批量带宽。
- 控制带宽：用于传输包含路由、计划和链接统计信息的控制数据包的带宽。
- 实时带宽：属于 Citrix SD-WAN 配置中的实时类类型的应用程序所占用的带宽。此类应用程序的性能在很大程度上取决于网络延迟。延迟数据包比丢失的数据包（例如 VoIP、Skype for Business）差。
- 交互带宽：属于 Citrix SD-WAN 配置中的交互类类型的应用程序所占用的带宽。此类应用程序的性能取决于网络延迟以及数据包丢失（例如 XenDesktop、XenApp）的巨大程度。
- 批量带宽：属于 Citrix SD-WAN 配置中的大容量类类型的应用程序所占用的带宽。这些应用程序涉及的人工干预非常少，通常由系统本身处理（例如，FTP、备份操作）。
- 带宽不匹配：与定义的 DSCP 标记不匹配的帧将映射到指定了不匹配带宽的默认队列。
- 可用带宽：分配给站点的所有 WAN 链接的带宽总量。
- 允许的带宽：传输信息可用的带宽。
- **BOWT** 延迟：将数据包从一个点移动到另一个点（以毫秒为单位）所用的最佳单向时间。
- 抖动：已接收的数据包延迟的变化，以毫秒为单位。
- 数据包丢失：数据包丢失次数。
- 丢失：数据包丢失百分比。
- **OOO**：顺序不正确的数据包的百分比。
- 拥堵：由于 WAN 中数据包传输量增加或出现意外延迟而导致出现拥塞。

> 注意
>
> 单击设置图标以选择要查看的指标。

管理

April 13, 2021

可以使用以下管理选项管理和维护 Citrix SD-WAN Center VPX。

配置日期和时间

HTTPS 证书

导入 MCN 配置

管理数据库

芒盖视图

软件升级

时间线控件

用户帐户

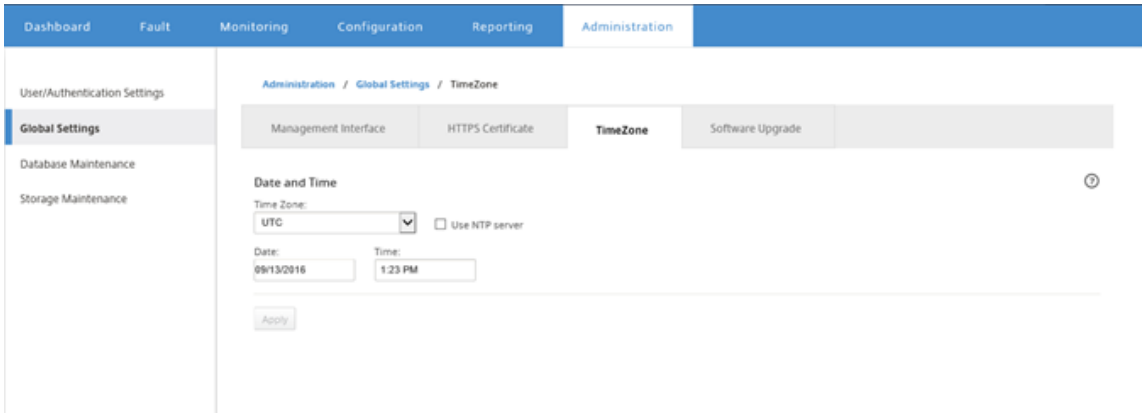
配置日期和时间

April 13, 2021

可以手动或通过使用 NTP 服务器来更改 Citrix SD-WAN Center 管理系统的日期和时间。如果选择使用 **NTP** 服务器选项，则无法手动输入当前日期和时间。

要手动设置日期和时间，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击时区。



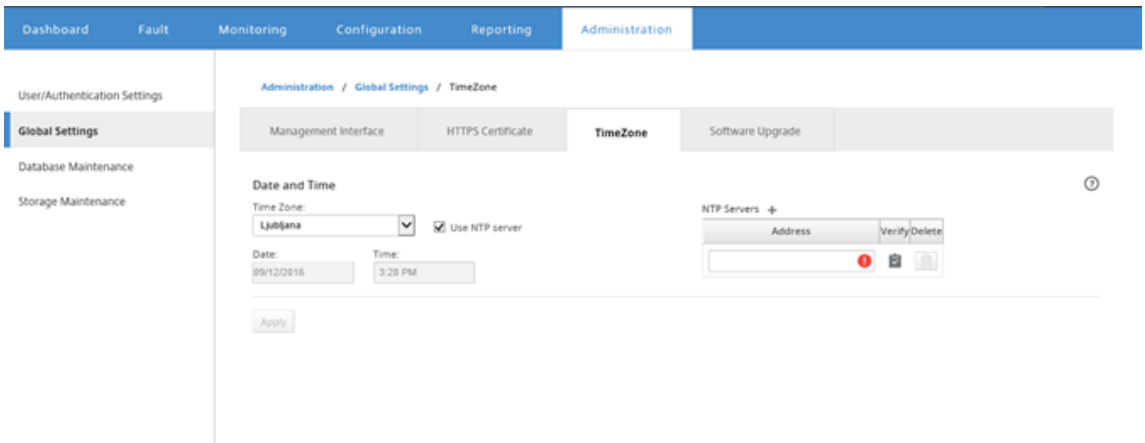
3. 在时区字段中，选择当前时区中的城市。或者，输入您所在时区的当前日期和时间。
4. 单击应用。

可以将 Citrix SD-WAN Center 时钟与外部 NTP 服务器同步。

要使用 NTP 服务器设置日期和时间，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击时区。
3. 选择使用 **NTP** 服务器。

   这将禁用日期和时间字段，并显示 NTP 服务器表格。



4. 要添加新的 NTP 服务器，请单击 NTP 服务器旁边的 **+** 图标。
5. 在地址字段中，输入 NTP 服务器的 **IP** 地址。

   最多可以指定三台 NTP 服务器，但必须至少指定一个。这些服务器用作备份 NTP 服务器，如果一个服务器处于关闭状态，Citrix SD-WAN Center 将自动与另一个 NTP 服务器同步。

   如果为 NTP 服务器指定了域名，则还必须配置 DNS 服务器，除非您已完成此操作。要从表格中删除服务器条目，请单击该条目的“删除”列中的删除图标。

6. 在应用您的设置之前，请单击验证确认服务器是否可访问。

7. 单击应用。

HTTPS 证书

April 13, 2021

建立到 Citrix SD-WAN Center 的安全管理 HTTPS 连接需要 HTTPS 证书。

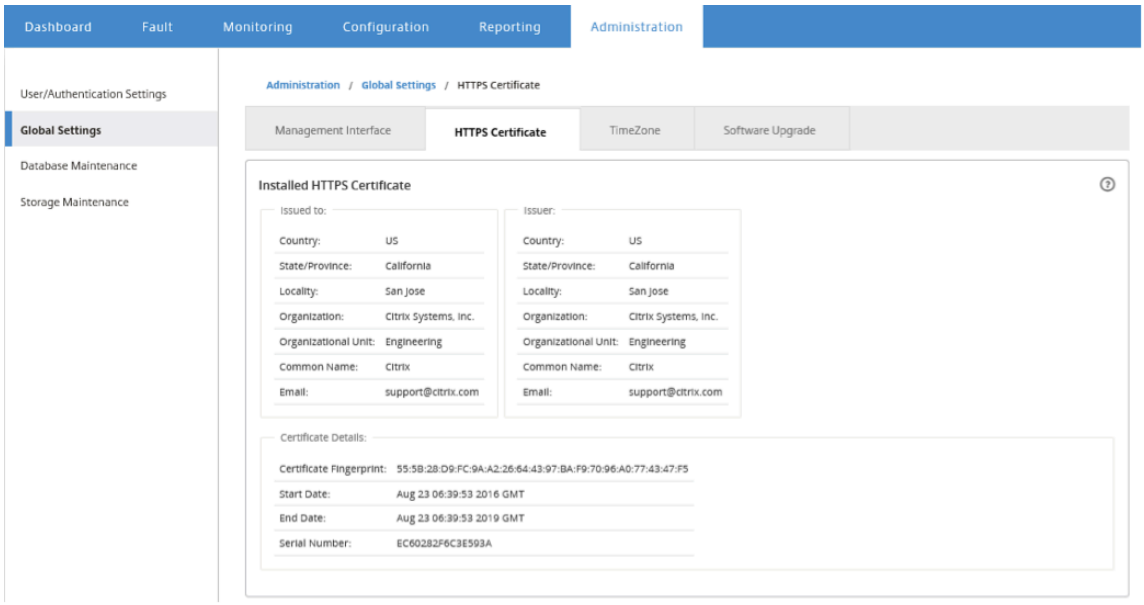
查看安装的 HTTPS 证书详情

CitrixTo 评估当前证书，则可以显示证书详细信息。

要显示 Citrix SD-WAN Center 上已安装的 HTTPS 证书的详细信息，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击 **HTTPS** 证书。

   HTTPS 证书详细信息显示在已安装的 **HTTPS** 证书部分。

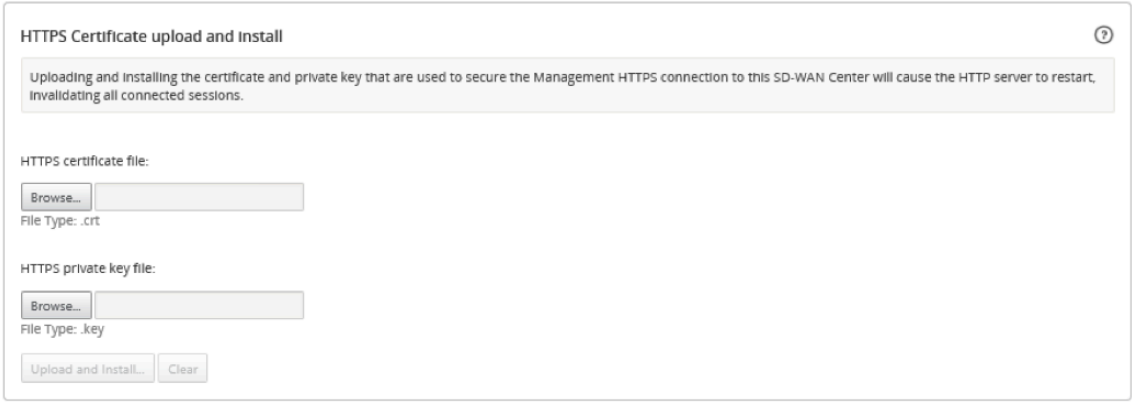


上载并安装 HTTPS 证书

在操作完成之前，安装 HTTPS 证书会将 Citrix SD-WAN Center 置于维护模式。操作完成后，Web 服务器将重新启动，使所有已连接的会话失效。如果重新启动 Web 服务器时与服务器的连接断开，维护模式屏幕将自动重新加载上一个页面并在浏览器中显示安全通知。如果屏幕未重新加载，请单击继续重新加载以前的页面。

要上载并安装 HTTPS 证书，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击 **HTTPS** 证书。
3. 在 **HTTPS** 证书上载和安装部分中的 **HTTPS** 证书文件字段中，单击浏览并选择一个 HTTPS 证书。
4. 对于 **HTTPS** 专用密钥文件，请单击浏览并选择一个 HTTPS 专用密钥文件。
5. 单击上载并安装。



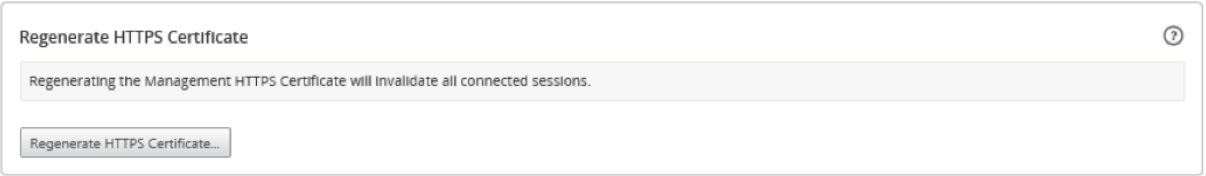
重新生成 **HTTPS** 证书

您可以重新生成用于将管理 HTTPS 连接固定到 Citrix SD-WAN Center 的自签名证书。在操作完成之前，重新生成 HTTPS 证书会将 Citrix SD-WAN Center 置于维护模式。操作完成后，Web 服务器将重新启动，使所有已连接的会话失效。

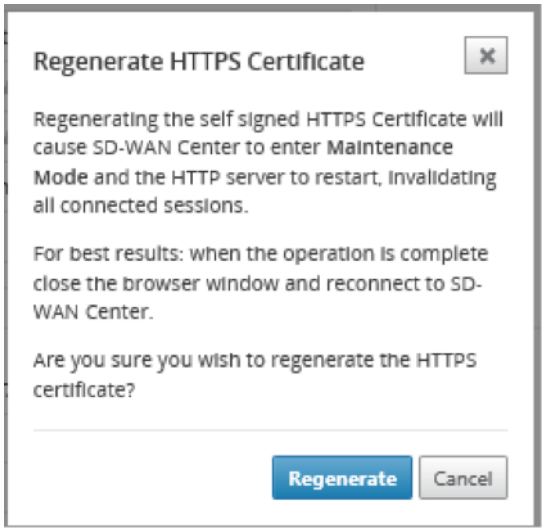
如果重新启动 Web 服务器时与服务器的连接断开，维护模式屏幕将自动重新加载上一个页面并在浏览器中显示安全通知。如果屏幕未显示，请单击继续重新加载以前的页面。

要重新生成 HTTPS 证书，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击 **HTTPS** 证书。
3. 在重新生成 **HTTPS** 证书部分中，单击重新生成 **HTTPS** 证书。



将显示“重新生成 HTTPS 证书”消息。单击重新生成。



导入 **MCN** 配置

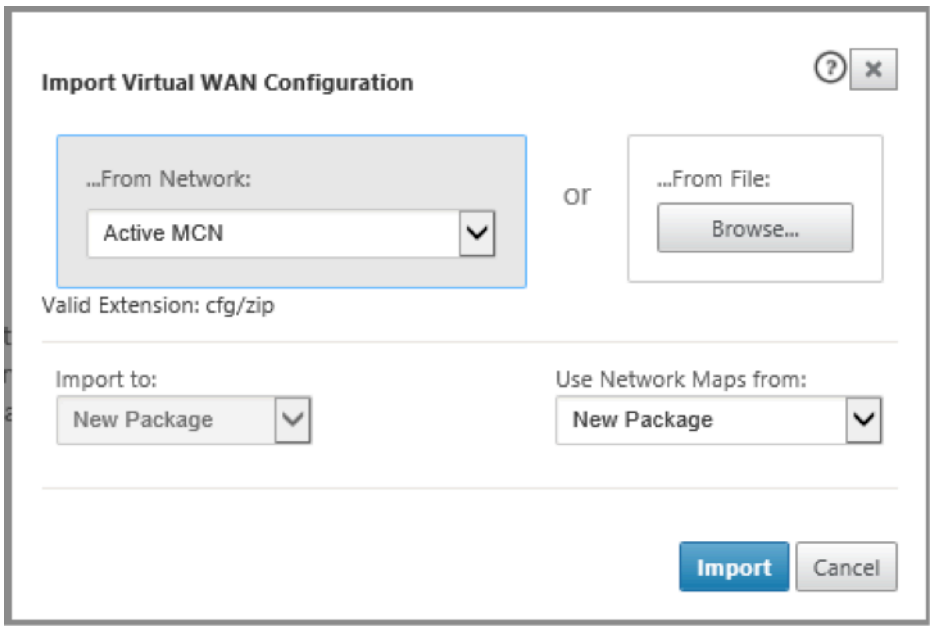
April 13, 2021

设置 Citrix SD-WAN Center 并在主控制节点 (MCN) 和 Citrix SD-WAN Center 之间建立连接时，可以将 MCN 配置导入 Citrix SD-WAN Center 并查看网络映射。

导入功能将配置导入到打开的或新的 Citrix SD-WAN 主配置中。如果在使用导入功能时，Citrix SD-WAN 主服务器配置处于打开状态，新的 Citrix SD-WAN 主服务器配置将覆盖该配置及其映射。如果未打开 Citrix SD-WAN 主服务器配置，则将创建一个无标题软件包。

要将 MCN 配置导入 Citrix SD-WAN Center，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击配置选项卡。
2. 单击网络配置，然后单击导入。



3. 在发件人网络字段中，选择以下选项之一：

   - 活动 **MCN**：连接到活动的 MCN 并下载当前配置。
   - 其他：连接到另一 MCN 的 IP 地址并下载当前配置。您可能必须在 MCN 中安装该 Citrix SD-WAN Center 中的安全证书，才能导入配置。

   有关详细信息，请参阅安装 Citrix SD-WAN Center 证书。

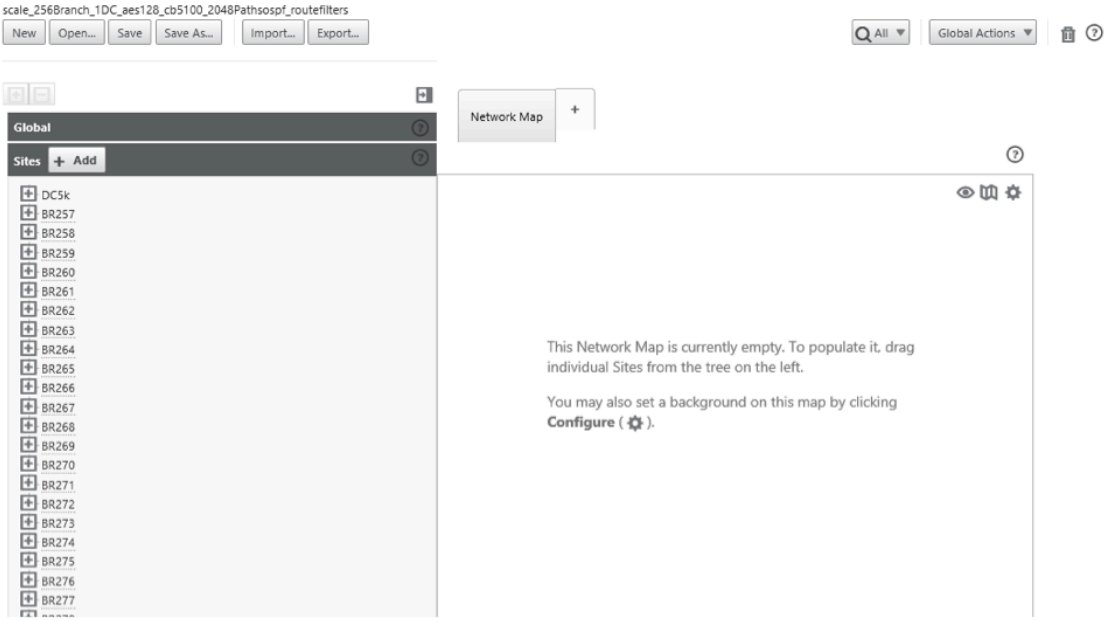
4. 或者，在从文件部分中，单击浏览，然后选择要从您的计算机上载的配置。

5. 在导入到字段中，选择当前包以将所选文件的内容导入到当前打开的软件包中。

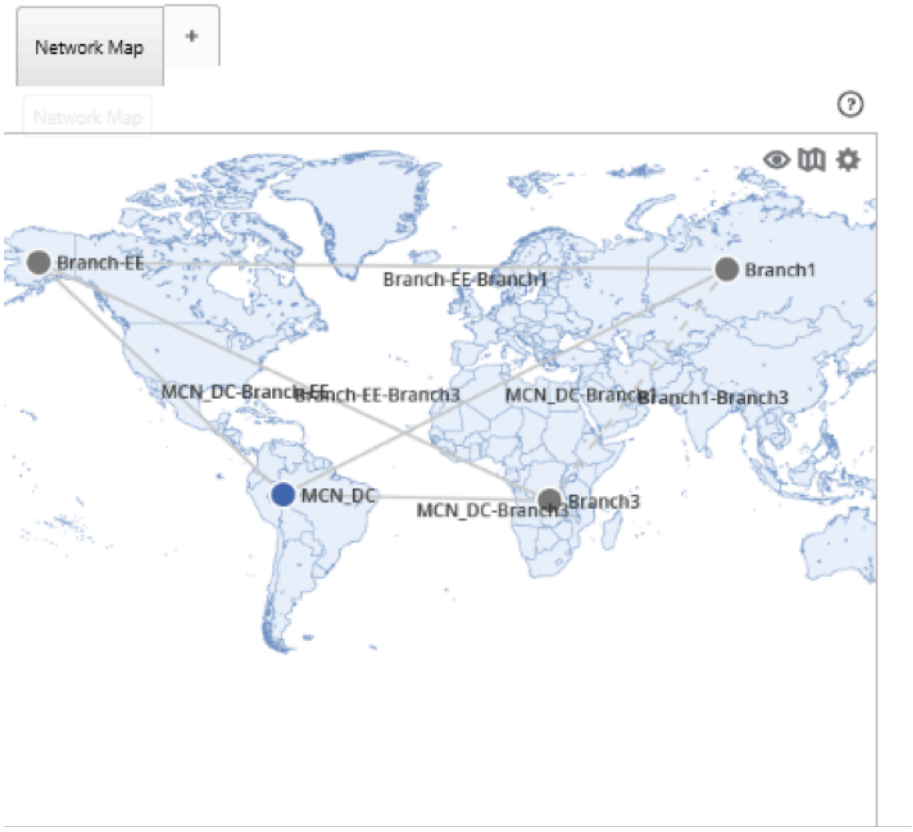
6. 在使用网络映射来自的字段中，选择以下选项之一。

   - 当前包：在导入后保留当前保存的网络映射集。
   - 新软件包：使用所导入软件包中的网络映射，并丢弃当前的一组地图。
   - 这两种软件包：除当前保存的地图外，还使用导入的映射。

7. 单击导入。配置已导入。



8. 在网络映射部分中。单击“设置”图标，然后选择自动填充以自动添加配置中的每个站点并将其安排到地图。



管理数据库

April 13, 2021

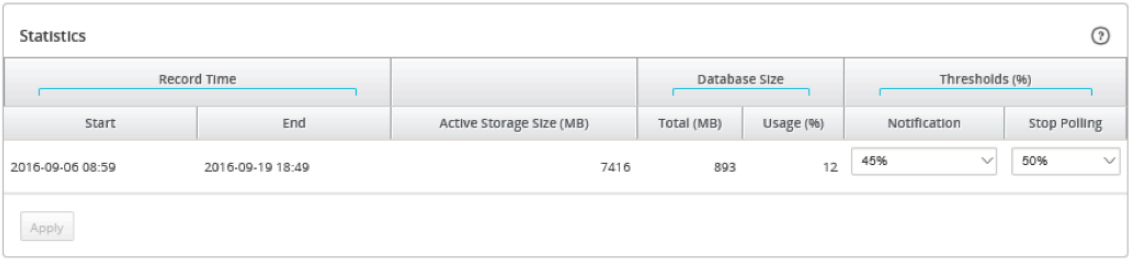
您可以监视和管理数据库，以确保有足够的可用磁盘空间来存储网络中所有发现的设备的轮询数据。

查看数据库统计

统计信息表将显示可用的数据库统计数据，并包含用于指定数据库磁盘使用阈值的通知和轮询的输入字段。

要查看数据库统计数据，请执行以下操作：

1. 在 Citrix SD-WAN Center Web UI 中，单击管理选项卡。
2. 单击数据库维护。在统计信息部分下，将显示以下信息。
   - 录制时间：显示数据库中最旧记录和最新记录的日期和时间戳。此列包含以下信息：
     - 开始：显示数据库中最旧记录的日期和时间戳。
     - 结束：显示数据库中最新记录的日期和时间戳。
   - 活动存储大小 **(MB)**：显示当前活动存储的磁盘空间。
   - 数据库大小 **(MB)**：显示当前数据库大小和使用信息。此列包含以下信息：
     - 总计 **(MB)**：显示数据库的总大小 (MB)。
     - 使用情况 **(%)**：显示当前活动存储器磁盘空间中数据库磁盘使用率的百分比。



要设置通知和轮询阈值，请执行以下操作：

1. 在通知字段中，输入要用作生成数据库使用通知的阈值的数据库大小或活动存储大小所占的百分比。当数据库使用率超过此阈值时，将发送电子邮件通知。
2. 在停止轮询字段中，输入停止统计信息轮询时使用的数据库磁盘使用阈值（百分比)。从下拉菜单中选择一个从 **10%** 到 **50%** 的值。默认值为 **50**%。
3. 单击应用。

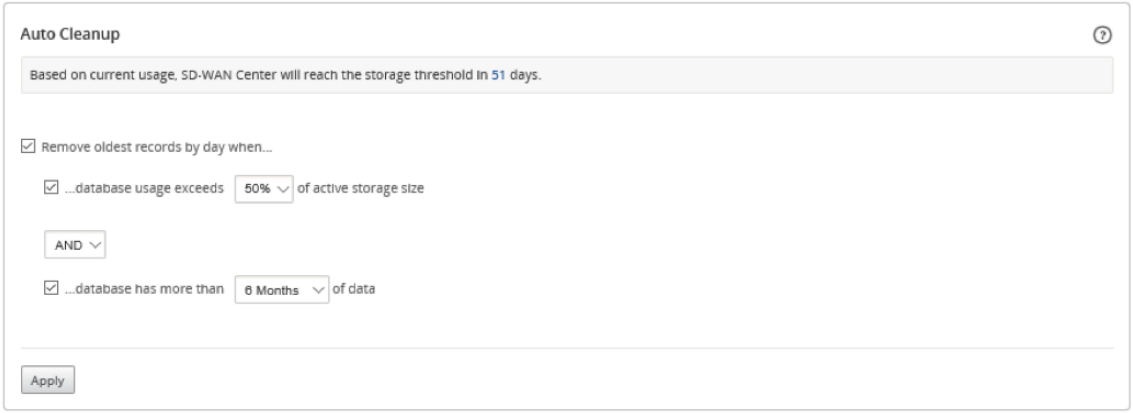
配置自动清理

要使数据库磁盘使用保持在控制之下，可以指定阈值，超过此值时，将从数据库中触发旧记录的删除操作。

要启用数据库清理并配置阈值，请执行以下操作：

1. 在 Citrix SD-WAN Center Web UI 中，单击管理选项卡。
2. 单击数据库维护。
3. 在自动清除部分下，选中删除按天排序的最旧记录复选框以启用数据库清理。

   如果启用了此功能，则每隔一天会在凌晨 2:00 自动检查数据库。如果达到或超过指定阈值，检查将启动数据库清理。默认情况下，不启用此设置。



4. 选择 …数据库使用量超过活动存储大小 **(%)**，然后从下拉菜单中选择一个百分比，以指定用于数据库清理的阈值。这些选项的增量为 **10%** 到 **50%** ，增量为 **5%**。
5. 从下拉菜单中选择 **AND** 或 **OR**，在“…数据库使用率超过…”和“…数据库具有超过…”阈值之间的下拉菜单中的运算符，以指定运算符来申请此规则这些阈值。默认值为 **AND**。
6. 选择…数据库中包含超过 [# months] 个月的数据，然后从下拉菜单中选择月数，以指定要在数据库中保留数据的数据库清理的时间跨度阈值。这些选项是从 **3** 个月到 **12** 个月以一个月为增量。
7. 单击应用。

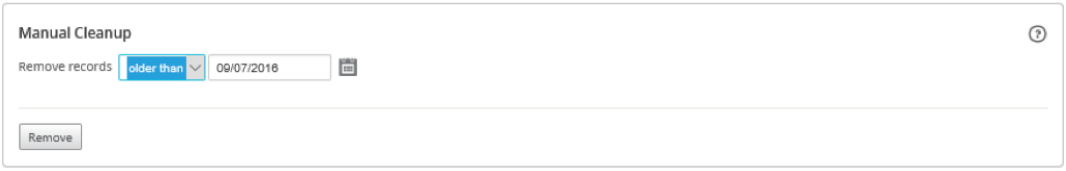
配置手动清理

您可以根据指定的条件从数据库中手动删除统计信息和事件记录。

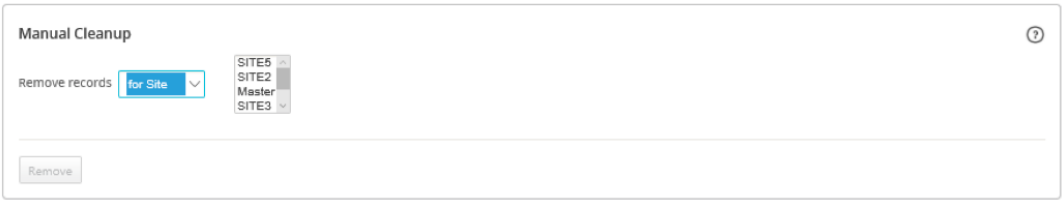
要执行手工数据库清理，请执行以下操作：

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击数据库维护。
3. 在手动清除部分下，从删除记录下拉菜单中选择一个过滤器。过滤选项包括：

- 早于：删除在指定日期之前收集的记录。选择此过滤器时，将显示“日期字段”和“日历选择”按钮。单击日历按钮以选择日期。所有早于指定日期的记录都将被删除。



- 对于站点：删除在指定日期之前收集的记录。选择此过滤器时，将显示“日期字段”和“日历选择”按钮。单击日历按钮以选择日期。所有早于指定日期的记录都将被删除。



4. 单击删除。

管理视图

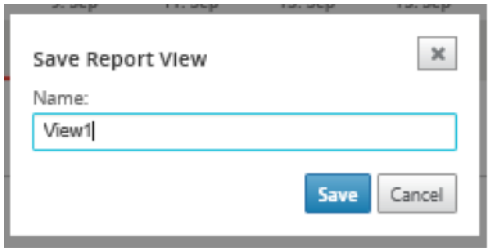
April 13, 2021

通过“故障报告”、“网络映射和统计”页面，可以创建、显示、修改和删除各个视图。

> 注意
>
> 过程中使用的屏幕截图可能因视图类型而异，具体取决于实际的用户界面。

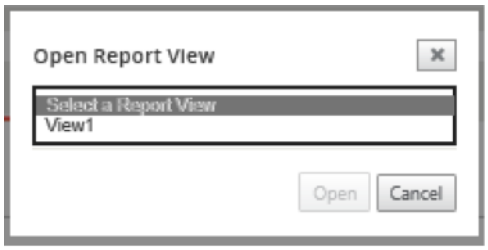
要创建新视图，请执行以下操作：

1. 单击新建视图时，将创建一个新的未命名视图，并将时间规格重置为当前时间。
2. 创建并应用过滤器，或者做必要的更改。
3. 单击 另存为。
4. 在保存视图对话框中，输入视图的名称。
5. 单击保存。



要打开并修改现有视图，请执行以下操作：

1. 单击打开。
2. 在打开视图对话框中，从下拉列表中选择一个报告视图。
3. 单击打开。此时将打开“事件”视图。
4. 根据需要进行必要的修改。
5. 单击保存。



要删除视图，请打开该视图，然后单击删除图标。

软件升级

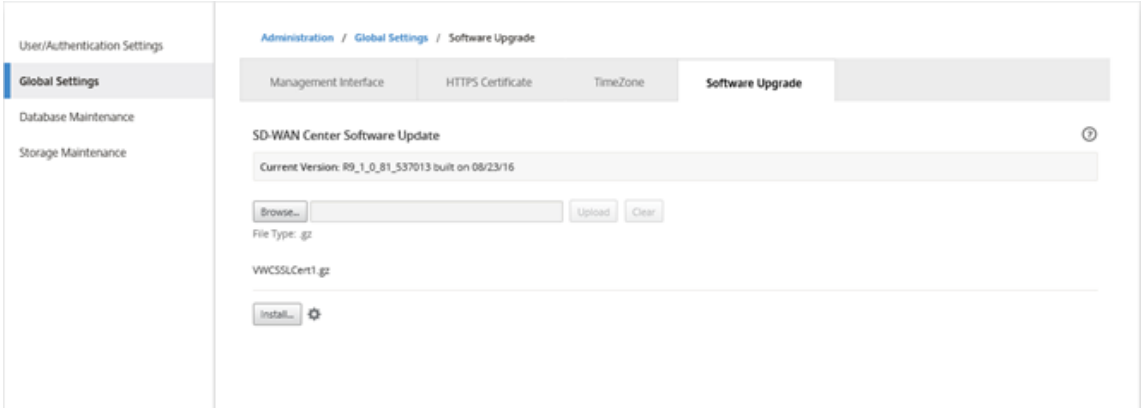
April 13, 2021

可以使用“软件升级”选项将 Citrix SD-WAN Center 软件升级到最新版本。软件升级过程将 Citrix SD-WAN Center 置于维护模式。如果需要迁移数据库，此过程可能需要几个小时。在这段时间内，不会从虚拟 WAN 收集统计数据，所有 Citrix SD-WAN Center 功能将不可用。

> 重要
>
> 建议在维护时间内运行升级。
>
> 注意
>
> 将相应的 Citrix SD-WAN Center 软件包下载到您的本地计算机。您可以从 下载 页面下载此软件包。

上载和安装 Citrix SD-WAN Center 软件的新版本

1. 在 Citrix SD-WAN Center Web 界面中，单击管理选项卡。
2. 单击全局设置，然后单击软件升级。



3. 单击浏览打开文件浏览器，然后选择要上载的软件包。
4. 单击上载，将选定的软件包上载到当前的 Citrix SD-WAN Center 虚拟机。
5. 上载完成后，单击安装。
6. 系统提示确认时，单击安装。
7. 在显示的对话框中，选择我接受最终用户许可协议复选框，然后单击安装。

用户帐户

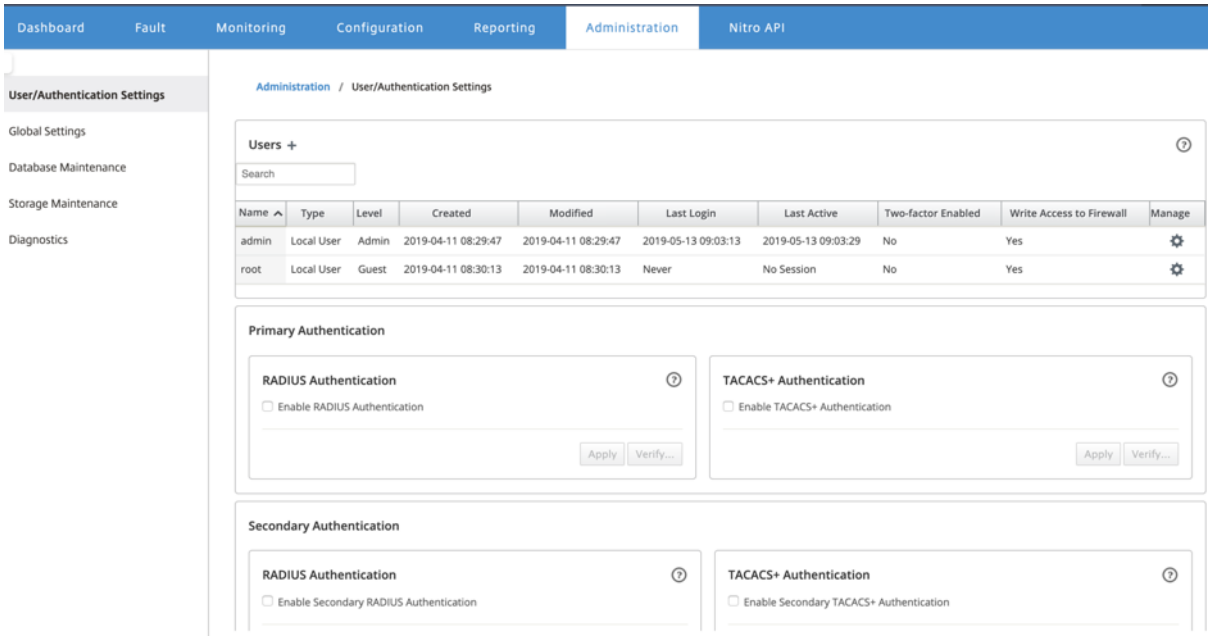
April 13, 2021

您可以至少查看已登录 Citrix SD-WAN Center 虚拟机的所有本地和远程用户帐户的列表一次。通过 RADIUS 或 TACACS+ 身份验证服务器对远程用户帐户进行身份验证。您还可以向 Citrix SD-WAN Center 中添加新的本地用户帐户。

> 注意
>
> 如果用户帐户在远程身份验证服务器上可用，但从不用于登录 Citrix SD-WAN Center，则不会显示在用户列表中。

要查看 SD-WAN Center Web 界面中的用户帐户，请导航到管理 **>** 用户**/**身份验证设置。

用户部分中将显示一个用户帐户列表。

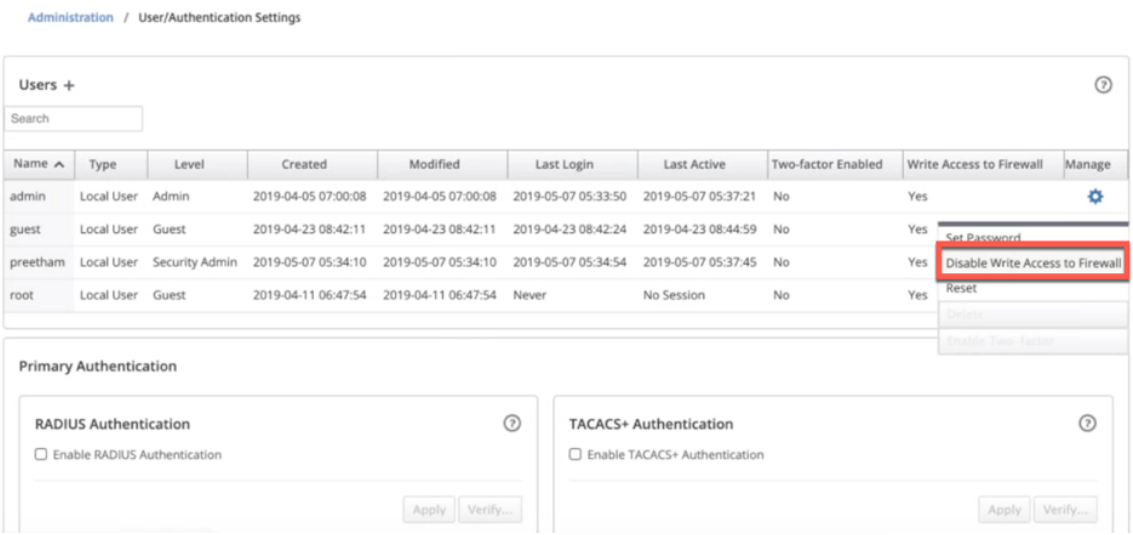


将显示以下信息：

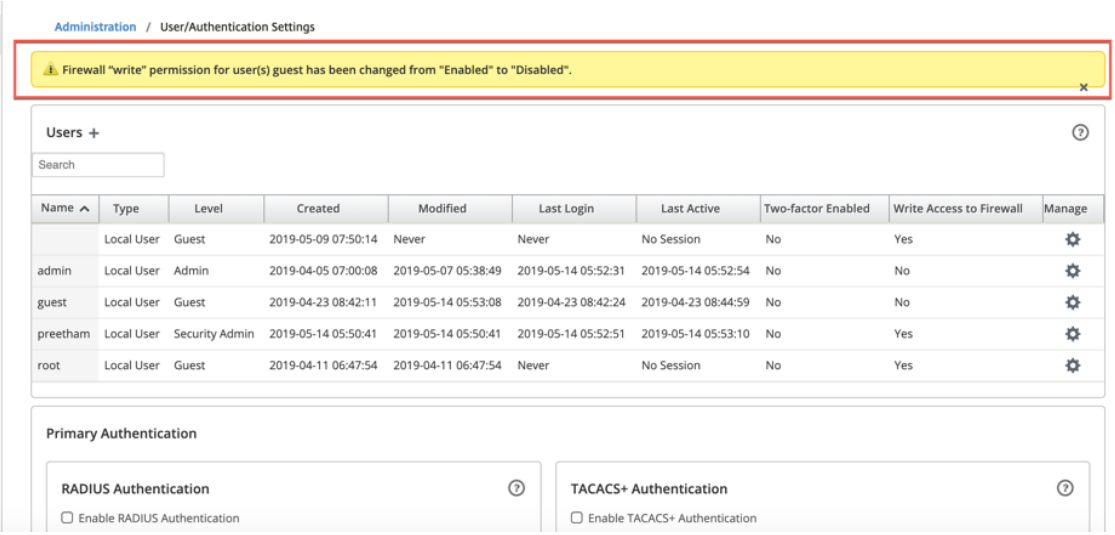
- 名称：用户名。
- 类型：用户帐户类型，可以是以下各项之一：
  - ** 本地 **：使用 SD-WAN Center 界面在本地创建和管理的用户帐户。
  - **RADIUS**：通过 RADIUS 服务器进行身份验证的远程用户帐户。
  - **TACACS+**：通过 TACACS+ 服务器进行身份验证的远程用户帐户。
- 级别：以下三个级别的帐户权限：
  - 管理员：管理员帐户具有管理权限。它对所有部分都具有读写访问权限。
  - 来宾：来宾帐户是可以访问控制板、报告和监视页面的只读帐户。
  - 安全管理员：只有在对其余部分具有只读访问权限的情况下，安全管理员才具有配置编辑器中与防火墙和安全相关的设置的读取-写入权限。

管理员可以创建并导出配置，安全管理员可以导入配置，并根据需要进行安全相关更改。只有安全管理员才能更改或修改安全功能配置。

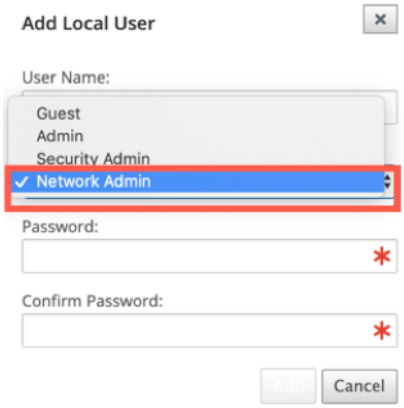
> 注意：
> 安全管理员有权禁用其他用户（管理员/来宾）对防火墙的写入权限。



如果安全管理员为任何特定用户更改了防火墙写入权限，则会向所有用户显示通知条。此通知按用户显示，因此每个登录用户必须确认警告才能删除该通知。



- 网络管理员：网 络管理员 没有防火墙的访问权限。网络管理员只能对“网络”设置具有读写访问权限，同时对其余部分具有只读访问权限。



网络管理员不能使用托管防火墙节点。在这种情况下，网络管理员必须导入新配置。网络和安全相关的设置都由超级管理员（管理员）维护。

网络和安全管理员只能对配置进行更改，但只能由超级管理员在网络上应用。

超级管理员具有以下权限：

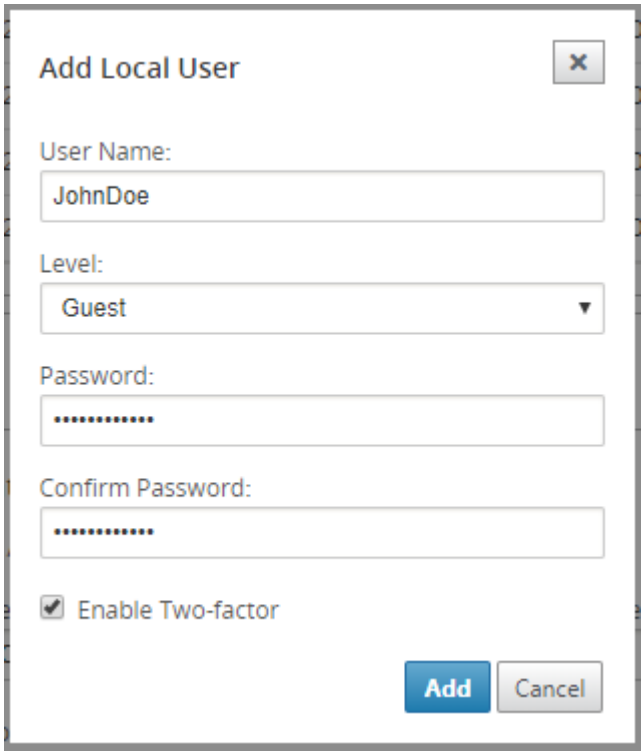
- 可以将配置导出到更改管理收件箱，以便对网络执行配置和软件更新。
- 还可以切换网络管理员和安全管理员的读取和写入权限。

- 创建时间：对于本地用户帐户，创建用户帐户的日期。对于远程用户帐户，为第一个登录会话的日期。
- 修改时间：对于本地用户帐户，为上次更改密码的日期。对于远程用户，为第一个登录会话的日期。
- 上次登录：用户最后一次成功登录的日期。工具提示显示用于登录的设备的 IP 地址。
- 上次活动：最后一次向服务器发出请求的日期。工具提示显示用于登录的设备的 IP 地址。
- 管理：单击齿轮图标可查看包含以下 选项的菜单：
  - 设置密码：更改本地用户帐户的密码。要更改 root 用户密码，需要使用当前的 root 用户密码。您不能更改远程用户帐户的 密码。
  - 重置：删除此用户帐户的工作区和首选项。
  - 删除：从 SD-WAN Center 中删除本地用户帐户、工作区和首选项。您无法删除远程帐户和管理员帐户。
  - 已启用双重身份验证：为本地和远程用户帐户启用双重身份验证。有关详细信息，请参阅双因素身份验证。
- 对防火墙的写入权限：显示已启用或禁用对防火墙的写入访问。

要向 Citrix SD-WAN Center 添加新的本地用户帐户，请执行以下操作：

> 注意
>
> 在 Citrix SD-WAN Center 本地创建的用户帐户没有权限，无法编辑网络配置软件包并将其导出到 MCN。

1. 在用户旁边，单击添加图标 +。此时将显示添加本地用户对话框。



2. 输入以下参数的值：

   - 用户名：本地用户帐户的用户名。
   - 级别：帐户权限。来宾用户帐户是只读 帐户，仅限于查看控制板、报告和统计信息。来宾 用户帐户没有编辑网络 配置包并将其导出到 MCN 的权限。
   - 密码：用户帐户的密码。
   - 确认密码：重新输入密码以确认。

3. 选择启用双重身份验证以为本地用户帐户启用双重身份验证。

   > 注意
   >
   > 仅当配置了辅助身份验证服务器时，才会显示启用双重选项。
   >
   > 配置辅助身份验证服务器（RADIUS 或 TACAS+ 身份验证）。确保在辅助身份验证服务器上配置了用户帐户。有关详细信息，请参阅二级身份验证。

4. 单击添加。系统将创建新用户帐户，并将帐户信息添加到用户表中。

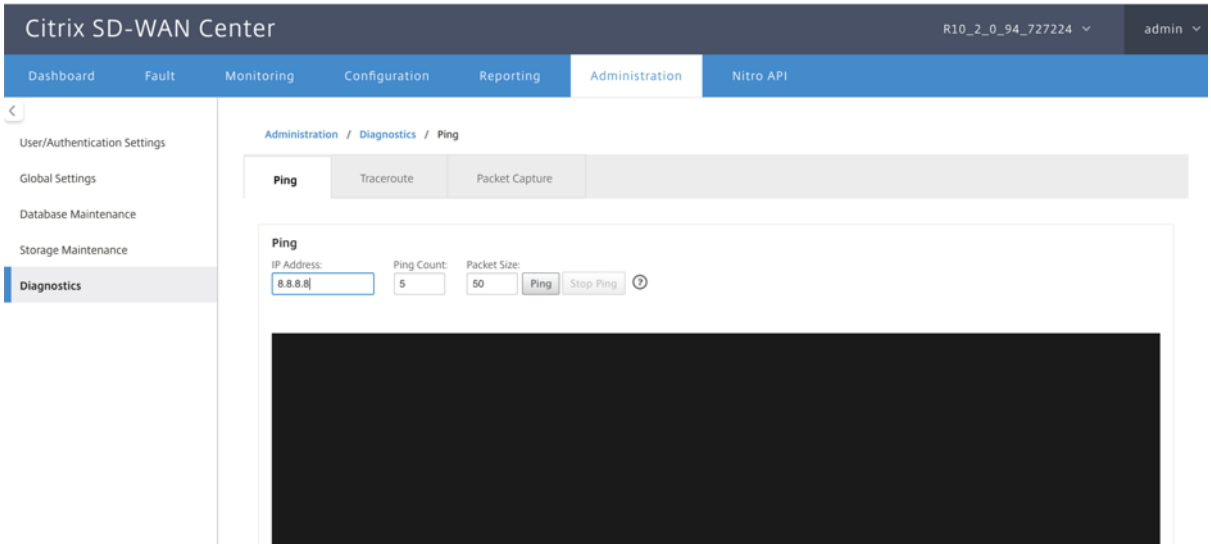
> 注意
>
> Citrix SD-WAN Center 最多可以有 600 个本地用户。

诊断

April 13, 2021

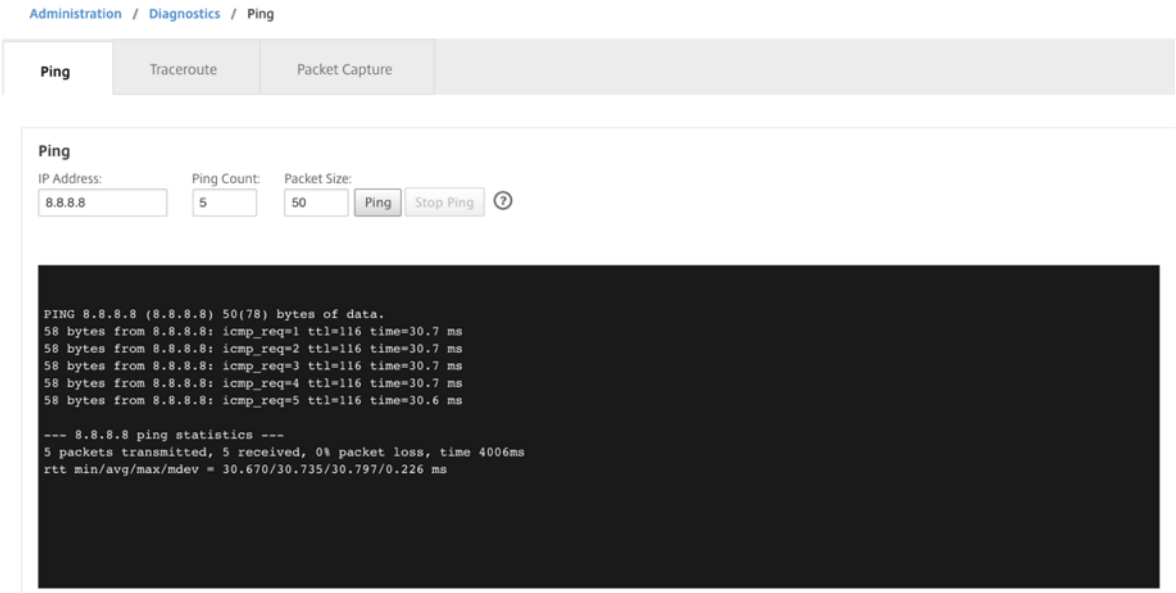
Citrix SD-WAN Center 诊断实用程序提供 Ping、Traceroute 和数据包捕获功能，用于测试和调查 Citrix SD-WAN Center 设备上的连接问题。**Citrix SD-WAN Center** 控制板控制数据集合中的诊断选项。

要使用诊断工具，请导航到管理 **>** 诊断。



Ping

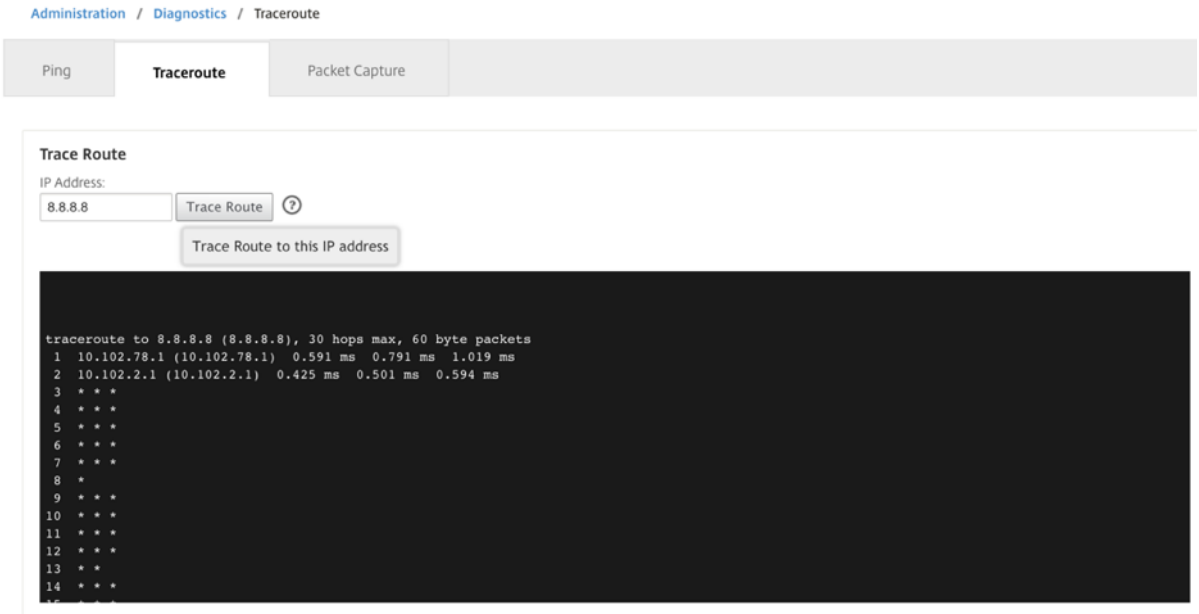
可以使用 **Ping** 选项 PING SD-WAN Center 网络中的任何管理 IP 地址。



提供一个有效的 IP 地址以及 ping 计数的数目（发送 ping 请求的次数）和数据包大小（数据字节数)。单击停止 **ping** 以停止正在进行的 Ping 搜索。

Traceroute

使用 **Traceroute** 选项确保 IP 地址可以访问。您可以通过显示路由和测量数据包的传输延迟来追踪网络中的任何管理 IP 地址。

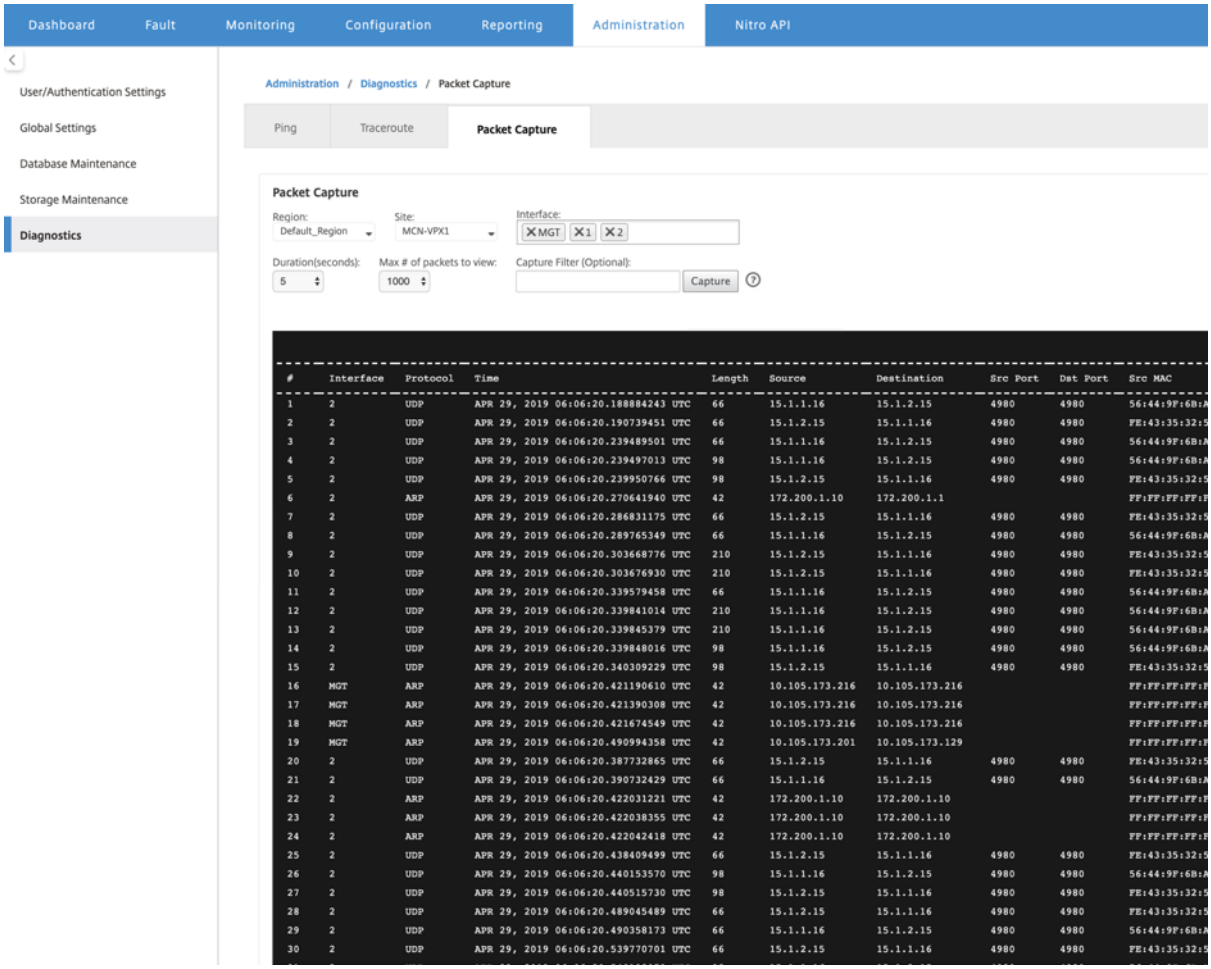


输入有效的管理 IP 地址以跟踪路由。单击跟踪路由。

> 注意：
>
> traceroute 结果显示最多 30 跳。

数据包捕获

使用数据包捕获选项可截获正在遍历所选站点中当前所选活动接口的数据包。



为数据包捕获操作提供以下输入：

- 区域-从下拉列表中选择由 SD-WAN Center 管理的区域。
- 站点 - 所选区域中的可用站点。从下拉列表中选择一个站点。
- 接口 -活动接口可用于在所选站点中捕获数据包。从下拉列表中选择接口或添加接口。至少选择一个接口来触发数据包捕获。

  > 注意：
  >
  > 能够一次在所有接口上运行数据包捕获，有助于加快故障排除任务。

- 持续时间（秒） -必须捕获数据的持续时间（以秒为单位）。
- 要查看的数据包的 最大数量-在数据包捕获结果中要查看的数据包的最大限制。
- 捕获筛选器（可选） -可选捕获筛选器字段接受用于确定捕获哪些数据包的筛选器字符串。数据包与过滤字符串相比较，如果比较结果为 true，则捕获数据包。如果过滤器为空，则将捕获所有数据包。有关详细信息，请参阅捕获过滤器。

  下面是此捕获过滤器的一些示例：

- **Ether proto\ARP** - 仅捕获 ARP 数据包
- **Ether proto\IP** - 仅捕获 IPv4 数据包
- **VLAN 100** - 仅捕获 VLAN 为 100 的数据包\
- **Host 10.40.10.20** - 仅捕获与地址 10.40.10.20 的主机之间的 IPv4 数据包
- **Net 10.40.10.0 Mask 255.255.255.0** - 仅捕获 10.40.10.0/24 子网中的 IPv4 数据包
- **IP proto \ TCP** - 仅捕获 IPv4/TCP 数据包
- **Port 80** - 仅捕获发至或来自端口 80 的 IP 数据包
- **Port range 20–30** - 仅捕获端口 20 到 30 之间的 IP 数据包
- **Host 10.40.10.20 and Port 80 and TCP** - 仅捕获主机 10.40.10.20 上 TCP 端口 80 中的 IP 数据包

> 注意：
>
> 捕获文件的最大大小限制为 575 MB。数据包捕获文件达到此大小时，将停止数据包捕获。

单击捕获以查看数据包捕获结果。