Citrix SD-WAN 万诺普 11.1

Machine translated content

Disclaimer

Contents

关于 **Citrix SD-WAN WANOP**

December 15, 2022

Citrix SD-WAN WANOP 设备优化您的 WAN 链接，为用户提供最大的响应能力和任何距离的吞吐量。Citrix SD-WAN WANOP 设备易于部署，因为它的工作透明。20 分钟的安装可以加速您的 WAN 流量，而无需其他配置。您不必更改应用程序、服务器、客户端或网络基础结构。但是，您可以在 Citrix SD-WAN WANOP 安装后更改它们，而不会影响流量加速。仅当 WAN 链接发生变化时，才需要重新配置 Citrix SD-WAN WANOP 设备。

Citrix SD-WAN WANOP 设备支持全方位优化，包括：

- 多会话压缩，压缩比高达 10000:1。
- 适用于 Windows 网络文件系统 (CIFS)、虚拟应用程序（ICA 和 CGP，包括新的多会话 *ICA* 标准）、Microsoft Outlook (MAPI) 和 SSL 的协议加速。
- 流量调整以确保高优先级和交互式流量优先于低优先级或批量流量。
- 高级 TCP 协议加速，可减少拥挤或高延迟链接的延迟。
- 视频缓存。

Citrix SD-WAN WANOP 的工作原理？

Citrix SD-WAN WANOP 产品成对工作，在链接的每一端一个，以加速通过链接的流量。由发件人完成的转换由接收人反转。

但是，一个设备（或虚拟设备）可以处理多个链接，因此您不必为每个连接指定一对。

企业通常每个站点有一个 Citrix SD-WAN WANOP 设备（较大站点的设备，较小站点的设备），尽管拥有众多分支机构的公司在其中央数据中心可能有多个设备。

从具有 Citrix SD-WAN WANOP 设备的站点到没有 Citrix SD-WANOP 设备正常运行但其流量未加速的站点的链接。

Citrix SD-WAN WANOP 功能包括在相对较慢的链路上实现快速性能的强大压缩，以及用于处理拥塞的无损流量控制。TCP 优化可以克服有问题的链接的主要限制，而应用程序优化可以消除专为高速本地网络设计的应用程序的局限性。自动检测功能使部署快速轻松。

Citrix SD-WAN WANOP 的功能和优势

工作人员等待计算机响应的任何时间都会浪费时间，从而导致生产力下降。当用户远程工作或使用场外资源时，其生产力取决于其网络连接的响应能力。要保护连接的响应能力，就需要先进的网络加速。

Citrix SD-WAN WANOP 产品系列通过一系列多重互锁优化提供可靠的 WAN 和 Internet 链路性能，从而保护您的工作效率。为了在整个企业中提供最大的生产力，Citrix SD-WAN WANOP 产品可满足各种需求，从最大的数据中心到最小的分支机构，甚至是个人笔记本电脑。

Citrix SD-WAN WANOP 提供强大的可用性，即使是对小型或降级的链接亦如此。

功能一览：

有关详细信息，请参阅 表。

特点和优点：

以下是 Citrix SD-WAN WANOP 产品线的一些主要优势。

压缩克服了低链路速度。与局域网相比，广域网链接和互联网链接最明显的问题是其带宽低。一个 1 Mbps 的广域网的吞吐量仅为 100 Mbps 的局域网吞吐量的 1%。如何克服低链路带宽？用压缩。100:1 的压缩比使 1 Mbps 链路能够以 100 Mbps 的速度快速传输数据。只要满足以下标准，即可实现这一加速系数：

- 压缩算法必须能够提供高压缩比。
- 压缩算法必须非常快（比链路带宽快得多，理想情况下与 LAN 一样快）。
- 链接的 LAN 段必须具有独立于 WAN 段的流量控制，因为不同的段以不同的速率处理数据。
- 必须使用多个压缩引擎来处理不同类型的流量的不同需求。交互式流量需要相对较少的带宽，但对延迟非常敏感，而批量传输对带宽非常敏感，但对延迟不敏感。

TCP 协议加速克服了拥塞。任何尝试发送流量超过链路速度的速度都会导致拥塞，从而导致许多由于数据包丢失和高排队延迟而导致的问题。

无损流量控制。TCP/IP 协议没有直接降低发件人速度的流量控制，并且缺乏这种必要的控制机制使数据包丢失和过度排队延迟正常，即使在关键任务链接上也是如此。（如果有的话，这个问题随着时间的推移越来越严重，正如关于 **bufferbloat** 现象的论文所证明的那样。）

Citrix SD-WAN WANOP 设备通过提供 TCP/IP 协议中省略的流量控制来解决此问题。与简单重新分配丢包的普通服务质量 (QoS) 解决方案不同，Citrix SD-WAN WANOP 提供了无损流量控制，控制端点发件人传输数据的速率，而不是允许发件人以他们喜欢的任何速度传输数据，并在发送时丢弃数据包太多了每个发送者只发送尽可能多的数据，因为 Citrix SD-WAN WANOP 允许它发送, 而不会丢弃一个数据包, 并且这些数据被放置在链接以完全正确的速率，以保持链接满而不溢出. 通过消除多余的数据，Citrix SD-WAN WANOP 不会强制丢弃它。如果没有 Citrix SD-WAN WANOP，丢弃的数据包必须再次发送，从而导致不必要的延迟。无损流量控制还消除了过度缓冲导致的延迟。无损流量控制是在繁忙链路上实现最大响应能力的关键，从而使一个曾经拥挤到 40% 利用率不可用的链路能够在 95% 的利用率下保持高效率和响应能力。

消除基于距离的不公平现象。具有高延迟或数据包丢失的链接很难在全带宽下使用，特别是对于普通 TCP 变体（如 TCP Reno）而言。其后果是过多的延迟和难以获取您付费的带宽。链接距离越长，问题就越糟。

Citrix SD-WAN WANOP TCP 协议加速最大限度地减少这些影响，允许洲际甚至卫星链路全速运行。

流量调整自动管理带宽。在输出端，类似公平排队的算法可确保每个连接独立排队，并给出其在链路带宽中的公平份额。流量调整策略允许不同的服务具有较高或较低的先例。应用程序优化可克服设计限制

设计用于局域网的应用程序和协议因广域网的性能差而臭名昭著，因为设计人员没有考虑到长时间的光速延迟对其协议的影响。例如，一个简单的 Windows 文件系统 (CIFS) 操作可能需要多达 50 次往返，因为消息通过网络来回传递。在 100 毫秒往返时间的广域网中，50 次往返导致延迟 5 秒。

尽管光速延迟是一个基本限制，但应用程序优化可以在较少的往返行程中执行相同的操作，通常是通过推测操作。如果原始应用程序一次发出一个命令，并在发出下一个命令之前等待它完成，那么发出一系列命令通常是完全安全的，而无需等待。此外，数据传输可以通过预取、预读和写入操作的组合加速。通过将尽可能多的操作包装到一次往返，性能可以提高 10 倍或更多。

Citrix SD-WAN WANOP 优化在 CIFS/SMB（Windows 文件系统）、MAPI（Outlook/Exchange 协议）和 HTTP 上特别有效。

多项优化可增强 **Virtual Apps/Virtual Desktops (Citrix HDX)** 的性能。由于 Citrix SD-WAN WANOP 设备是 Citrix 产品，因此它们在加速 Citrix 协议（如 Citrix Virtual Apps and Desktops）方面特别有效。Citrix SD-WAN WANOP 加速的各个方面都与这些协议发挥作用，从而使远程用户体验尽可能高效。

Citrix SD-WAN WANOP 设备与 Citrix Virtual Apps and Desktops 服务器协商会话选项。这允许 Citrix SD-WAN WANOP 设备应用以下增强功能：

- 它将服务器的本机压缩替换为性能更高的 Citrix SD-WAN WANOP 压缩。
- 它将连接的流量整形优先级基于嵌入在每个 Citrix Virtual Apps and Desktops 连接中的优先级位。这允许连接的优先级根据流量类型而变化。例如，交互式任务是高优先级任务，打印作业是低优先级任务。
- 它根据正在使用的 Virtual Apps 或 Virtual Desktops 收集和报告统计信息。
- 它维护原始连接的端到端加密。

自动检测，实现最小的配置。由于该解决方案是双端的，要求链接的两端都存在 Citrix SD-WAN WANOP 产品，因此部署似乎会给远程办公室带来负担，尤其是没有专门 IT 人员的远程办公室。然而，Citrix SD-WAN WANOP 被设计为非常容易安装和维护。一个典型的安装需要大约 20 分钟。唯一需要的参数是常规网络参数（如 IP 地址和子网掩码）、Citrix 许可证服务器的地址以及链接的发送和接收速度。

由于自动检测，Citrix SD-WAN WANOP 可以确定哪些连接可以加速（哪些连接不能），而无需任何手动配置。将自动检测到链接另一端的 Citrix SD-WAN WANOP，然后加速连接。您可以以临时方式将 Citrix SD-WAN WANOP 设备添加到您的网络中。您甚至不需要通知现有的电器一个新的到来。他们发现它自己。

Citrix SD-WAN WANOP 使用 TCP 头选项来报告其存在，并与远程 Citrix SD-WAN WANOP 协商加速参数，因为 TCP 头选项是 TCP 标准的一部分，此方法效果非常好，除非在防火墙被编程为拒绝所有，但最常见的选项。此类防火墙存在，但可将其配置为允许 Citrix SD-WAN WANOP 使用的选项传递。

Citrix SD-WAN WANOP 操作对发送者和接收者都是透明的。网络中的其他设备不知道 Citrix SD-WAN WANOP 存在。他们继续工作，就像在 Citrix SD-WAN WANOP 安装之前一样。此透明度还消除了在服务器或客户端上安装特殊软件的任何需要，以便从 Citrix SD-WAN WANOP 加速中受益。一切都是透明的。

产品线功能：

Citrix SD-WAN WANOP 产品线中的每个产品都提供基本的 Citrix SD-WAN WANOP 加速功能。大多数型号还有其他功能，例如：

- 视频缓存
- 具有以太网旁路功能的多个加速桥梁

- 通过 GUI、CLI、SNMP、AppFlow 和 Citrix ADM 进行监视和管理。

不同的 Citrix SD-WAN WANOP 产品具有不同的功能。支持更高 WAN 带宽的产品也支持更多的用户，并且通常拥有更多的资源：更多的 CPU 功率、更多的内存、更大的磁盘和更加加速的桥接。

在您自己的硬件上运行的产品（例如 Citrix SD-WAN WANOP 插件和 Citrix SD-WAN WANOP VPX）的功能取决于硬件的速度以及您专门用于加速的系统资源量。

有关最新规范，请参阅 CitrixSD-WAN 产品数据表。

Citrix SD-WAN WANOP 架构

Citrix SD-WAN WANOP 设备加速通过您 WAN 链接的流量。要加速 WAN，您至少需要两台 Citrix SD-WAN WANOP 设备，每个要加速的站点都有一台。

发件人端 Citrix SD-WAN WANOP 设备将一系列优化和转换应用于流量，例如压缩和加密。许多操作要求 Receiver 端 Citrix SD-WAN WANOP 执行反向操作（例如解压缩或解密）才能将流量还原到其原始状态。

因此，大多数优化要求流量通过两个 Citrix SD-WAN WANOP 设备。某些优化是单端的，并且由本地设备单独执行。这些优化包括流量调整和视频缓存。

Citrix SD-WAN WANOP 设备在很大程度上是透明的网络。设备本身似乎是一个桥，而不是路由器、Gateway 或代理。这种隐形性允许在不配置任何其他硬件的情况下安装设备。设备优化也是透明的，仅由链接另一端的合作伙伴设备检测到。

Citrix SD-WAN WANOP 设备可以随意添加到网络中，因为它们的自动检测和自动协商功能可确保其他设备立即检测到网络上的新设备，并且加速立即开始。

尽管上图显示了只有两台设备的网络，但是单个 Citrix SD-WAN WANOP 设备可以与任意数量的合作伙伴站点进行通信。全部支持点对点、中心和辐射网络和网状网络。

除了独立设备外，Citrix SD-WAN WANOP 加速产品还包括虚拟机（Citrix SD-WAN WANOP VPX 系列）和适用于 Windows 系统的可安装加速服务（Citrix SD-WAN WANOP 插件）。

加速度意味着什么

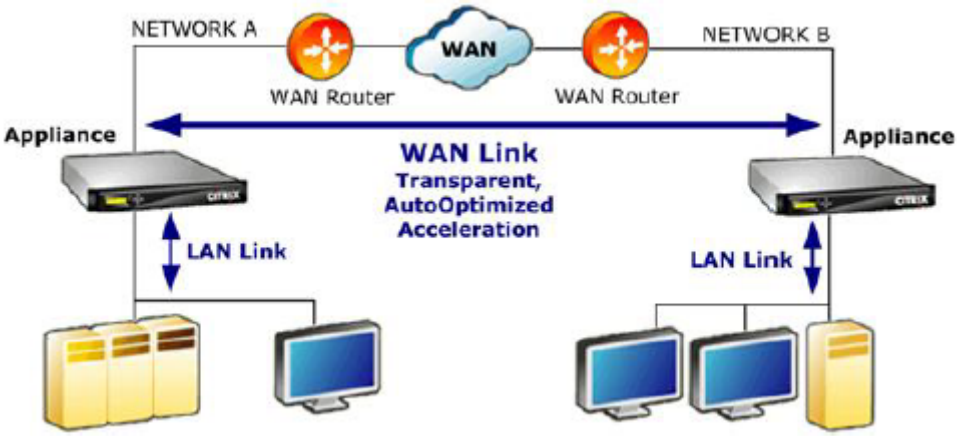
在 Citrix SD-WAN WANOP 术语中，“加速”是减少事务时间，从而减少用户花费等待的时间。由于用户花费等待的时间意味着直接的生产力损失，加速的主要好处是提高生产力。

在网络流量中，事务范围从非常小（telnet 或 SSH 端点会话中的单字节数据）到非常大（如 FTP 传输），后者大小通常超过千兆字节。一个实用的加速器必须加速从交互式流量到批量流量的整个范围的交易规模，从而提供全面的最佳性能和用户体验。Citrix SD-WAN WANOP 技术通过各种方式实现这一点。

加速工作原理：管道

要了解 Citrix SD-WAN WANOP 设备的工作原理，请仔细查看流量管道图。正如你所看到的，有两个管道：

1. 发送管道，用于加速从本地局域网进入 WAN 的数据。
2. 接收管道，用于加速数据退出 WAN 并进入本地局域网。



发送管道

要了解设备，请考虑一次发送管道一个单元。

1. 输入缓冲区。设备接收来自 LAN 的数据包。由于非 TCP/IP 流量仅由流量成形程序优化，因此非 TCP 数据包直接转移到流量成形程序。TCP/IP 流量（从现在开始称为 TCP 流量）遍历管道的其余部分。
2. 视频缓存。如果 TCP 流量与视频缓存的设置相匹配，请求将交给视频缓存单元。
3. 局部自动检测。除了流量成形外，发件人端优化还需要远程设备以及本地设备。任何未通过远程设备的连接都会转移到流量成形器。此操作由 LAN 端自动检测逻辑执行。远程设备的实际测试由 WAN-side 自动检测装置完成。
4. LAN 端流控制。Citrix SD-WAN WANOP 充当透明 TCP 代理，代表端点 Receiver 接收和确认来自端点发件人的数据包。这样，设备就能以全局域网速度快速接受来自本地发件人的大量数据，无论流量在 WAN 上移动的速度如何。（普通 TCP 使用端到端速度控制，这不够敏捷，无法实现最大性能。）此外，Citrix SD-WAN WANOP 流量控制是无损的，这意味着本地发件人永远不会看到丢弃的数据包，从而提高了可靠性和效率。
5. 应用程序引擎。Citrix SD-WAN WANOP 执行多种协议的特定优化，包括：
   - Citrix Virtual Apps and Desktops，使用 ICA 和 CGP 协议。
   - Windows 文件系统（CIFS，包括 SMB1 和 SMB2 版本）
   - Outlook/Exchange (MAPI)

   这些优化缩短了事务时间。这是通过重写、合并和重新排序命令、使用预读和写入、使用协议知识进行更高级的流量成形和压缩提示来完成的。

6. 压缩引擎压缩使事务变得更小，从而减少通过链接传输数据所需的时间。Citrix SD-WAN WANOP 压缩机使用多种压缩算法，其中一些对于小型事务非常有效，一些针对批量事务进行了优化，另一些针对中型事务。Citrix SD-WAN WANOP 压缩程序很容易实现 10000:1 的压缩比。压缩机速度非常快，可以在全 WAN 速度下保持高压缩比。借助 Citrix SD-WAN WANOP 处理，以 100:1 比率压缩的文件可以通过 1 Mbps 链接轻松发送，总吞吐量为 100 Mbps。
7. 安全引擎某些 Citrix SD-WAN WANOP 功能要求两个设备彼此之间以及与源服务器之间建立安全的对等关系。安全引擎验证此对等关系并加密它们之间的加速数据连接。安全的对等关系允许使用 SSL 压缩和加速加密虚拟应用程序/虚拟桌面 (ICA/CGP)、Windows 文件系统 (CIFS) 和 Outlook/Exchange (MAPI) 流量。
8. 横侧流量控制和自动检测。WAN 链接是发生流量减慢的地方，如果链接拥挤，数据包将丢失并且必须重新传输。重新传输数据包始终会导致显著延迟，有时会持续一秒钟。WAN 侧流量控制单元使用先进的重传元件和先进的 TCP/IP 协议，在“干净”和“困难”链接中实现最大性能。自动检测单元通过连接识别是否存在合作伙伴 Citrix SD-WAN WANOP 单元，从而防止在不需要优化的地方使用优化，并允许现有设备在添加到网络后立即检测到新设备。自动检测使用 TCP 标头字段中的选项。这通常是透明的，但可能会被某些防火墙阻止，这些防火墙需要重新配置。
9. 应用程序分类器。本单元检查通过 Citrix SD-WAN WANOP 流动的所有流量，并确定它所属的应用程序或协议。此信息用于报告和流量塑形程序。
10. 流量造型器。为了避免拥堵、过度排队和其他可避免的延迟源，流量成形器将流量注入到 WAN 的数据速率略低于 WAN 的数据速率，以确保 WAN 永远不会超出。采用加权公平排队算法确保所有流量获得其公平份额的链路带宽。流量调整策略允许不同的流量类型接收不同的权重，因此某些流量获得的带宽比其他流量更多。

接收管道

接收方向的管道类似于发送方向，除了它不是加密，而是解密，而是不是压缩，我们进行解压缩。另外，请注意，接收方向上还有一个流量成形器，将流量成形策略应用于传入 WAN 流量，以便对两个方向进行调节。

自动检测和数据包级转换

自动检测算法插入 TCP 标头选项，以宣布 Citrix SD-WAN WANOP 设备的存在并促进协商。这些选项在 24-31 范围内。使用以下数据包级别转换：

- 在连接的初始数据包（SYN 数据包）上，发送设备附加标识自身为 Citrix SD-WAN WANOP 设备的标头选项，并声明其他功能（如压缩）。这被称为“标记 SYN 数据包”。
- 收到标记 SYN 数据包后，接收设备会将标头选项附加到 SYN-ACK 数据包，然后依次识别自身并宣布其功能。
- 一旦发送设备收到标记的 SYN-ACK 数据包，就可以根据两个设备共享的任何功能加速连接。例如，如果两个设备都声明支持压缩，则会压缩连接。
- 两个方向的 TCP 初始序列号 (ISN) 通过向原始值添加 2,000,000,000 来更改。如果一台设备发生故障或路由更改阻止其查看连接中的所有流量，这是一项防止连接继续的预防措施。一旦连接加速，它必须在其整个生命周期内保持加速。

- MSS 值减少（通常为 1380 字节），以确保每个数据包都有空间用于插入的 Citrix SD-WAN WANOP TCP 头选项。
- 连接的 IP 地址和端口号保持不变。

预先确认

SYN 和 SYN-ACK 数据包从端到端流：

- SYN 数据包从端点客户端、通过客户端设备、通过 WAN、通过服务器端设备流，最后流向服务器。
- SYN-ACK 数据包从服务器端设备（通过服务器端设备）通过 WAN 流动，通过客户端设备流动，最后流向客户端。

连接的最终数据包、FIN、FIN-ACK 和 RST 数据包也是如此。

但是，其他数据包是预先确认的。例如，当服务器端设备从服务器接收数据包时，它会立即通过 LAN 确认该数据包，并对其进行缓冲，以便最终通过 WAN 传输。这使得服务器端设备的缓冲区能够非常快速地填充，因此它始终拥有大量数据可用于压缩和其他优化。（这与正常的 TCP 操作非常不同，其中所有确认都来自 WAN 的另一侧，使得确认速度非常慢，并且强制连接的每个段移动速度不会比最慢的段快，从而大大降低了加速的有效性。）

将流量移入和移出设备

Citrix SD-WAN WANOP 设备有许多“转发模式”。转发模式是使流量进出设备的一种方法。最常见的是内联模式，其中 Citrix SD-WAN WANOP 似乎是桥接设备。在一个桥接端口上进入的数据包似乎会退出另一个桥接端口。当然，Citrix SD-WAN WANOP 以各种方式转换数据，因此在许多情况下，退出第二个端口的数据包与进入第一个端口的数据包不相同，但这就是它在网络的其余部分看起来的方式。

在内联模式不实际的情况下，还有其他几种方法可用，最值得注意的是 WCCP 模式。这些是“单臂”模式，使用单个接口电缆。

> 提示
>
> 您可以使用 Citrix ADM 管理和监视 Citrix SD-WAN WANOP 设备，有关更多信息，请参阅 使用 Citrix ADM 管理 Citrix SD-WAN 实例。

开始使用 **Citrix SD-WAN WANOP**

April 23, 2021

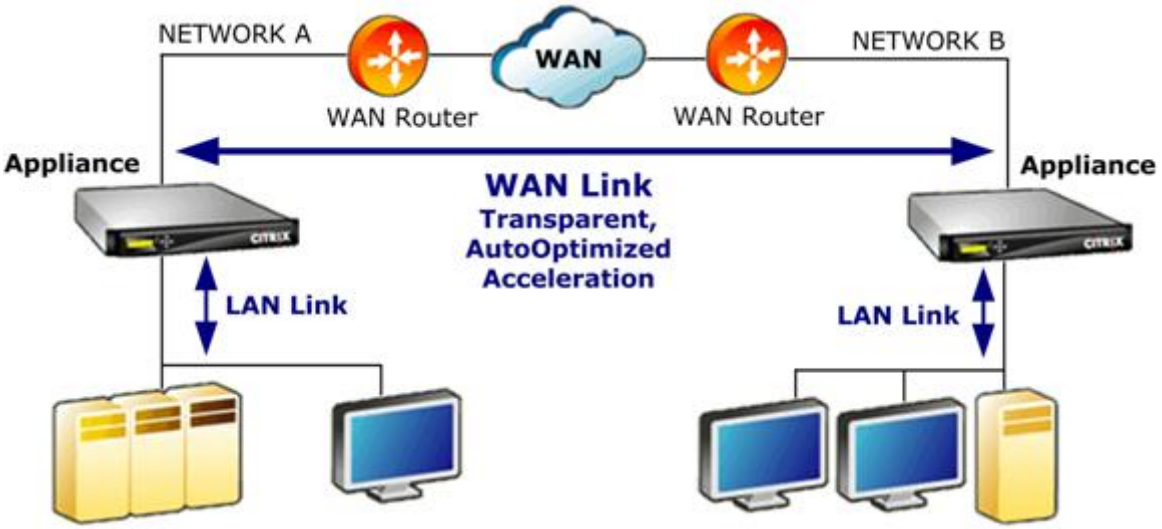
成功部署 Citrix SD-WAN WANOP 设备并不困难，但部署不当可能会导致问题并提供不足的加速。请务必选择具有足够容量的设备，以便您希望他们加速的链接。产品选择也是决定如何最好地将设备融入拓扑中时要考虑的因素之一。

最基本的部署条件是：

- TCP 连接中的所有数据包必须通过受支持的两个 加速单元（Citrix SD-WAN WANOP 设备或插件）的组合。
- 流量必须在两个方向上穿过两个加速单位。

当满足这些条件时，加速是自动的。

当流量通过两台电器时，加速提高性能



对于只有一个 WAN 网络的站点，可通过将 Citrix SD-WAN WANOP 设备与 WAN 内联来满足这些条件。在更复杂的站点中，还有其他选项可用。一些，例如 WCCP 的支持，在所有型号上都可以使用。其他产品仅适用于某些型号。因此，更复杂的站点的需求可能会限制您对设备的选择。

评估选项时，请考虑在设备发生故障或必须禁用时保持网络的各个部分正常运行的重要性。对于内联部署，Citrix 建议使用 以太网旁路卡。此卡在 Citrix SD-WAN WANOP 设备上是可选的，它具有一个在设备出现故障时关闭的中继，从而允许数据包通过即使断电或被删除。

冗余是所有类型的部署的考虑因素。Citrix SD-WAN WANOP 设备提供不同类型的冗余：

- SD-WAN WANOP 4000/5000 设备具有双电源。
- SD-WAN WANOP 4000/5000 设备具有冗余磁盘驱动器。
- 设备可以在高可用性模式下使用（两个具有自动故障转移功能的冗余设备）。所有型号都支持此模式。

> 注意
>
> 有关 Citrix SD-WAN WANOP 设备和部署模式的详细信息，请参阅SD-WAN WANOP 平台文档。

根据容量选择设备

April 23, 2021

为了正常操作，Citrix SD-WAN WANOP 设备必须具有足够的资源来支持要加速的 WAN 链接数量，并支持这些链接的所有用户。选择 Citrix SD-WAN WANOP
设备时，三种容量非常重要：链路容量（带宽）、用户容量和磁盘容量。

链路容量

选择 Citrix SD-WAN WANOP 设备时，最重要的因素是它支持您的 WAN 链接。如果您的站点具有单个 WAN 链接，则您的设备应支持链接速度。例如，Citrix SD-WAN WANOP 2000-010 可支持高达 10 Mbps 的链接，这适合 8 Mbps 的链接，但不适合 12 Mbps 的链接。如果您的站点有多个链接需要由单个设备加速，则该设备应支持将所有这些 WAN 链接添加到一起的总速度。

支持的最大速度由设备硬件和产品许可证的组合决定。许可带宽限制是许可证支持的最大链路速度。

产品	许可广域网 **BW** 范围
当前产品	
SD-WAN WANOP 插件	不适用
SD-WAN WANOP 400	每秒 2-6 兆位
SD-WAN WANOP 800	每秒 2-10 兆位
SD-WAN WANOP 2000、2000WS	每秒 10 至 50 兆位
SD-WAN WANOP 3000	5 0-155
SD-WAN WANOP 4000	310-1000 Mbps
SD-WAN WANOP 5000	1500-2000 Mbps
SD-WAN WANOP VPX	每秒 1-45 兆位

表 1. 按产品线分列的许可带宽限制

Virtual Apps/Virtual Desktops 用户容量

每台设备应是 XenApp 或 Virtual Desktops 用户的最大数量。当您的部署使用虚拟应用程序或虚拟桌面时，不应超过此值。如果您不使用虚拟应用程序或虚拟桌面，请将此数字视为其他应用程序用户数量的粗略指南。

产品	最大用户数量
SD-WAN WANOP 插件	1
SD-WAN WANOP 400	10-30

产品	最大用户数量
SD-WAN WANOP 800	20-100
SD-WAN WANOP 2000、2000WS	100-300
SD-WAN WANOP 3000	300-500
SD-WAN WANOP VPX	20-350
SD-WAN WANOP 4000	750-2,500
SD-WAN WANOP 5000	3500-5000

表 2. 虚拟应用/虚拟桌面用户容量

磁盘大小

磁盘空间主要用于压缩历史记录，并且磁盘空间越多会导致更高的压缩性能。

SD-WAN WANOP 4000/5000 系列提供从 1.8 TB 到 2.4 TB 的磁盘容量。相比之下，SD-WAN WANOP 3000 为 2.1 TB，SD-WAN WANOP 2000 为 470 GB，SD-WAN WANOP 800 为 80 GB，SD-WAN WANOP 400 为 40 GB。SD-WAN WANOP VPX 具有 100-500 GB 的磁盘容量。理想情况下，设备的磁盘容量应大于链路数据的周期时间。例如，包含大多数每天更新流量的链接应具有 24 小时或更长的磁盘容量。由于链接主要包含用户会话，此窗口可能会更小。（1 Mbps 的链接可以全速传输大约 10 GB 每天。）

表 3. 磁盘大小的数据生命周期示例

家电型号	链路速度 **1 Mbps**	链路速度**-10 Mbps**	链路速度**-100 Mbps**	链路速度**-1000 Mbps**
链路利用率为 **33%** 的数据生命周期				
SD-WAN WANOP 800	23 天	2.3 天	不适用	不适用
SD-WAN WANOP 2000、2000WS	141 天	14 天	不适用	不适用
SD-WAN WANOP 5000	717 天	72 天	7.2 天	17 小时
100% 链路利用率下的数据生命周期				
SD-WAN WANOP 800	8 天	19 小时	不适用	不适用

家电型号	链路速度 **1 Mbps**	链路速度**-10 Mbps**	链路速度**-100 Mbps**	链路速度**-1000 Mbps**
SD-WAN WANOP 2000、2000WS	47 天	4.7 天	不适用	不适用
SD-WAN WANOP 5000	239 天	24 天	2.4 天	6 小时

基于数据中心拓扑选择部署模式

April 23, 2021

设备可以按照您的 WAN 链接放置。该设备使用两个桥接以太网端口进行内联模式。数据包进入一个以太网端口并通过另一个端口退出。此模式将设备置于 WAN 路由器和 LAN 之间。对于网络的其余部分，它就好像设备根本不存在。它的操作是完全透明的。

内联模式与其他部署模式相比具有以下优势：

- 最佳性能。
- 非常简单的配置，只使用快速安装页面。
- 无需重新配置您的其他网络设备。

其他模式（WCCP，虚拟内联，重定向器）不太方便设置，通常需要重新配置路由器，并且性能稍低。

基本的部署考虑因素是站点是具有单个 WAN 路由器还是多个 WAN 路由器。您还必须考虑在哪些模式下可以使用哪些功能。支持 VPN 的要求会影响设备在网络中的位置。

访问网关设备支持 Citrix SD-WAN WANOP TCP 优化，从而在使用访问网关部署 Citrix SD-WAN WANOP 设备时启用加速 VPN 连接。

部署模式概述

设备可以在以下模式中部署：

转发模式

- 内联模式—最高性能、最透明的模式。数据在一个加速以太网端口上流入，另一个端口上流出。不需要任何类型的路由器重新配置。
- 内联双桥—与内联相同，但具有两个独立的加速桥。

- **WCCP** 模式—当内联模式不实际时推荐使用。大多数路由器支持。只需要三行路由器配置。若要在思科路由器上使用 WCCP 模式，路由器应至少运行 IOS 版本 12.0 (11) S 或 12.1 (3) T。（WCCP 代表 Web 缓存通信协议，但该协议通过 2.0 版大幅扩展，以支持各种网络设备。）
- 虚拟内联模式—类似于 WCCP 模式。使用基于策略的路由。通常需要路由器上的专用 LAN 端口。不建议在没有以太网旁路卡的设备上使用。若要在思科路由器上使用虚拟内联模式，路由器应运行 IOS 版 12.3 (4) T 或更高版本。
- 组模式—用于站点内的两个或多个内联设备（每个链接一个）。仅当多个桥接、WCCP 和虚拟内联模式都不切实际时才建议使用。
- 高可用性模式—透明地将两个内联或虚拟内联设备组合到一个主/辅助对中。主设备处理所有流量。如果失败，则辅助设备将接管。不需要配置路由器。需要带有以太网旁路卡的设备。
- 透明模式 - 与 Citrix SD-WAN WANOP 插件进行通信的推荐模式。在透明模式下，插件启动连接的方式与 Citrix SD-WAN WANOP 设备基本相同，保留连接的原始 IP 地址和端口号，并将 Citrix SD-WANOP 选项添加到所选数据包的 TCP/IP 标头。相比之下，在重定向器模式下（不推荐），插件会更改数据包的目标 IP 和端口号，以匹配设备的信令 IP（和端口）。
- 重定向器模式（不推荐）-由 Citrix SD-WAN WANOP 插件用于将流量转发到设备。可用作独立模式或与其他部署之一组合使用。不需要配置路由器。

加速模式

- **Softboost** 模式-推荐用于大多数链接的高性能 TCP 变体。尽管它提供的性能低于 hardboost 模式，但它适用于任何部署。像正常的 TCP 一样，但速度更快。
- **Hardboost** 模式-高度攻击性、带宽受限的 TCP 变体，适用于高速链路、洲际链路、卫星链路和其他固定速度链路，这些链路很难实现全速链路。建议用于不需要流量成形的固定速度点对点链路。

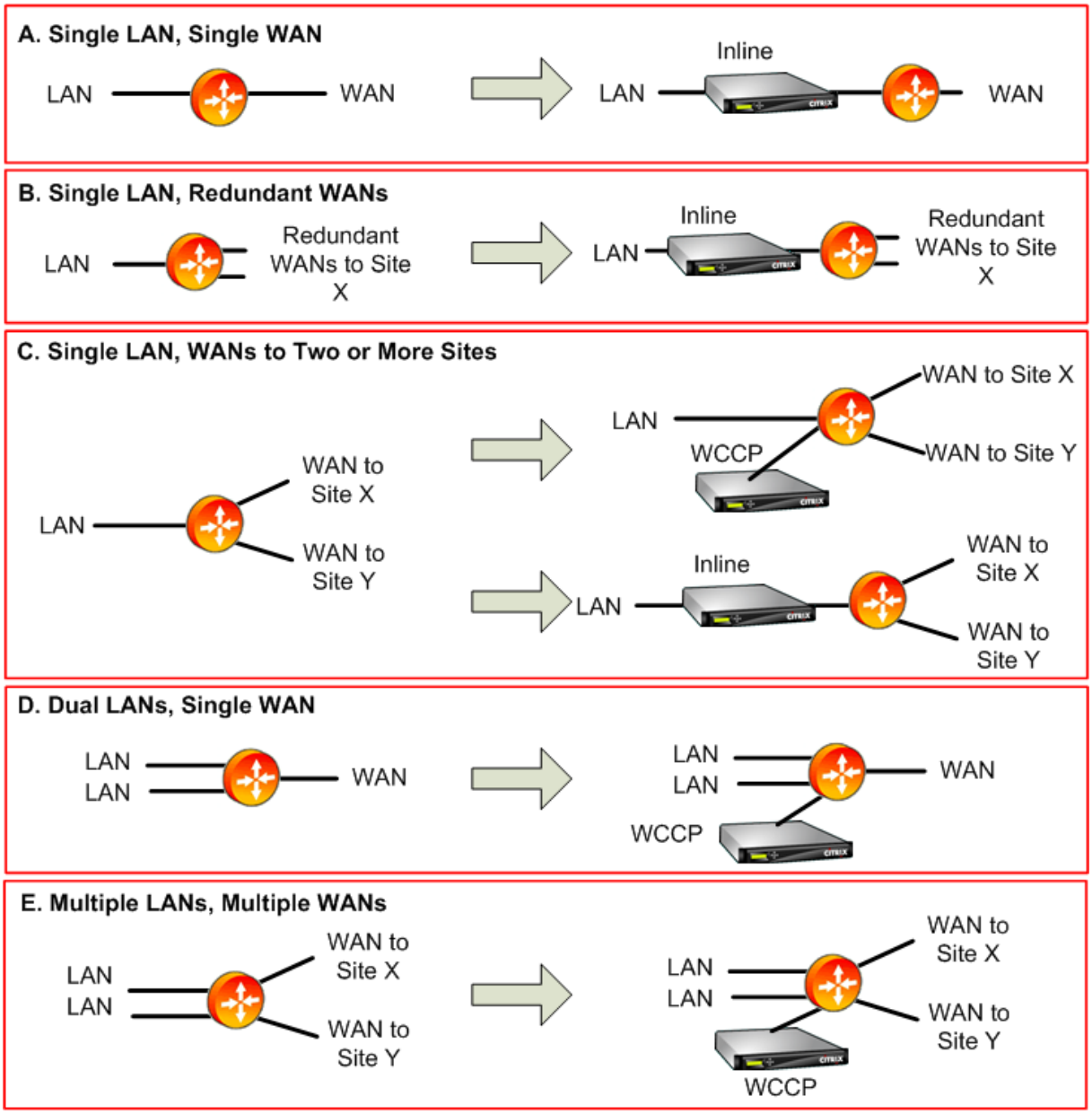
> 注意
>
> 有关 Citrix SD-WAN WANOP 设备和部署模式的详细信息，请参阅Citrix SD-WAN WANOP 平台文档。

具有一个 **WAN** 路由器的站点

April 23, 2021

对于只有一个 WAN 路由器的站点，部署中的主要问题是允许 Citrix SD-WAN WANOP 设备与路由器协调工作。下图显示了单个路由器的推荐部署模式。将其与路由器线路连接进行比较，以找到适合您环境的最佳模式。

基于 WAN 路由器拓扑的推荐部署模式



有关推荐部署模式的评论：

1. 单局域网，单个广域网：内联模式。路由器具有单个主动 LAN 接口和单个主动 WAN 接口。这种情况下推荐的模式是内联模式，它提供了最简单的安装、最多的功能和任何模式的最高性能。
2. 单局域网，冗余 **WAN**：内联模式。内联模式也是这种配置的最佳选择。
3. 单个局域网，多个 **WAN**：内联或 **WCCP**。这种拓扑分为两类：中心辐射或多跳。在中心和辐射部署中，连接主要在辐射站点和中心站点之间。在多跳部署中，许多连接位于两个辐射站点之间，数据通过中心站点传递。因此，单个多跳连接可能涉及多达三个设备，具体取决于集线器站点的设备在流量流中的位置的详细信息。

   为了在多跳部署中正确调整流量，集线器站点的 WAN 路由器上的所有 WAN 流量也必须通过设备，而不是由路由器直接在 WAN 接口之间传递。在这种情况下，WCCP 是首选模式。如果部署是中心辐射的，并且大多数流量

终止在中心站点上，则最好进行内联部署。

4. 双局域网，单个广域网：内联（带双桥）或 **WCCP**。双加速桥、WCCP 模式或虚拟内联模式支持此模式。
5. 多个局域网，多个 **WAN**：内联（双桥）或 **WCCP**。这与案例 C 类似，但由于存在多个 LAN 接口以及多个 WAN 而复杂。WCCP 总是可以在这里使用。在双局域网的情况下，具有双桥的设备也可以在内联模式下使用。

   有关更多信息，请参阅 表

具有多个 **WAN** 路由器的站点

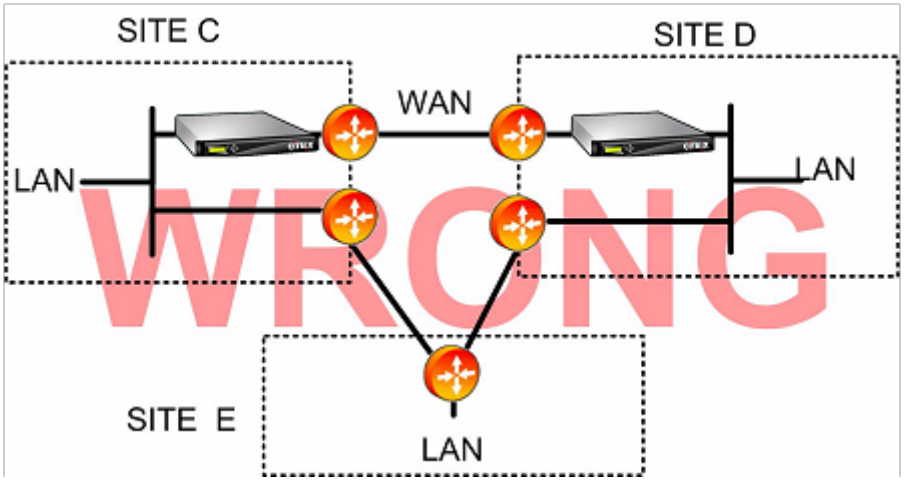
April 23, 2021

同一站点的多个 WAN 路由器提高了 不对称路由的可能性。通常情况下，IP 网络不受数据包走的路径的影响，只要它们到达目的地。但是，设备依赖于查看连接中的每个数据包。不接受“终端”数据包。

在只有一个 WAN 路由器的站点中，非对称路由不是问题，因为设备可以放置在路由器和站点其余部分之间的路径中，这样进出路由器的流量也会通过设备。但是，对于两个 WAN 路由器，非对称路由可能会成为一个问题。

由于故障转移到辅助链路或其他形式的动态路由和负载平衡，安装期间或更高版本可能会出现非对称路由问题。下图显示了可能遭受非对称路由影响的示例站点。如果站点 C 和 D 总是使用直接路径，C-D 或 D-C，在相互发送流量时，一切都很好。但是，采用较长路径 C-E-D 或 D-E-C 的数据包绕过设备，导致新连接未加速并挂起现有连接。

非对称路由

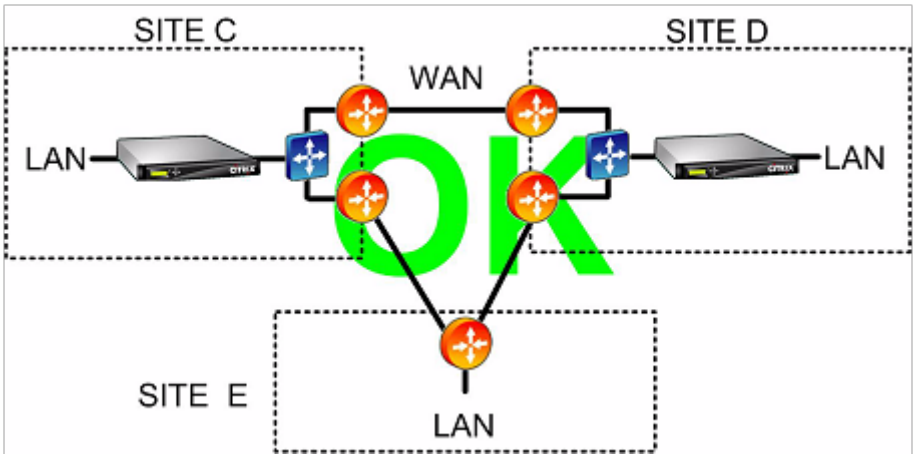


非对称路由可通过路由器配置、设备放置或设备配置来解决。

如果路由器配置为确保给定连接的所有数据包始终在两个方向通过设备，则不存在不对称性。

如果设备位于合并所有 WAN 流的点之后，则可避免不对称性，并加速所有流量，如下图所示。

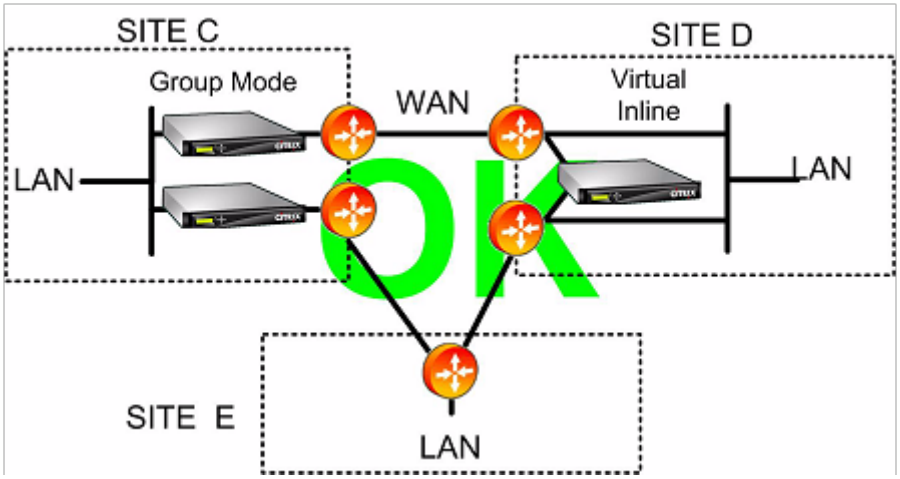
通过适当放置设备来避免非对称路由



将设备配置为使用以下不对称转发模式之一可以消除问题：

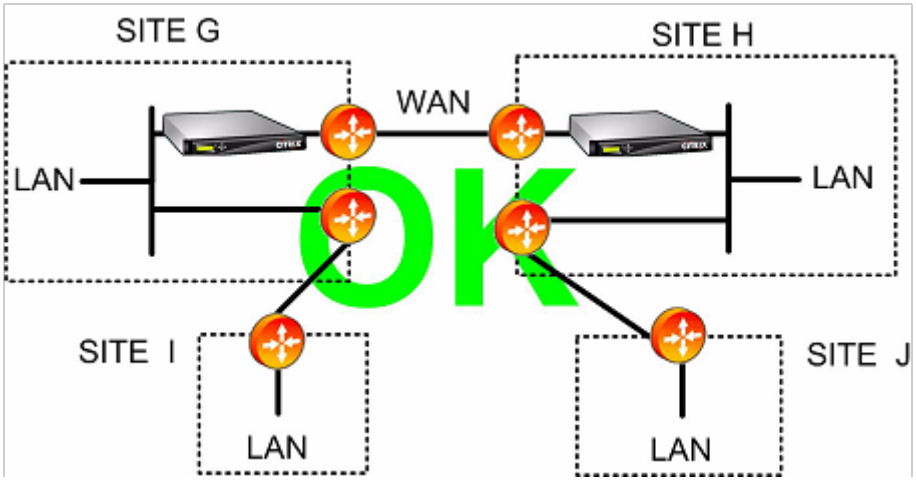
- 多个桥梁。具有两个加速桥接或 加速对（例如，apA 和 apB）的设备允许在内联模式下加速两个链路。这两个链接可以是完全独立的、负载平衡的或主/备份的链接。
- *WCCP* 模式 允许单个设备在多个 WAN 路由器之间共享，允许它处理所有 WAN 流量，无论它到达哪个链接。
- 虚拟内联模式 允许单个设备在多个 WAN 路由器之间共享，使其能够处理所有 WAN 流量，无论其到达哪个链接。
- 组模式 允许两个或多个内联设备相互共享流量，确保到达错误链接的流量被正确传递。由于组模式需要多台设备，因此这是一种昂贵的解决方案，最适合加速链路具有广泛物理分离的安装，从而使其他替代方案变得困难。例如，如果两个 WAN 链接位于同一城市的不同办公室（但校园通过 LAN 速度链接连接），则组模式可能是唯一的选择。

使用组模式或虚拟内联模式消除非对称路由



> 注意
>
> 链接的一端可以使用虚拟内联模式，而另一端则使用组模式。链接的两端不必使用相同的转发模式。

只有一个 WAN 链接的站点不能有不对称的路由问题



在各种部署模式下处理的设备故障

April 23, 2021

Citrix SD-WAN WANOP 设备具有防止在软件、硬件和电源故障的情况下丢失连接的保护措施。这些保障措施取决于模式。

在 内联模式下，设备在硬件、软件或电源故障时保持网络连续性。如果存在，则当断电或发生其他故障时，设备中的旁路继电器将关闭。没有旁路卡的内联设备通常会在发生严重故障的情况下阻止流量，但在某些情况下，即当网络堆栈正在运行但加速软件已被禁用或由于持续错误而自行关闭时，它们会继续转发流量。

现有加速连接通常在发生故障后变得无响应，并最终由应用程序或网络堆栈在其中一个终点终止。某些加速连接可能会在失败后继续作为未加速连接。新连接在未加速模式下运行。

当设备恢复联机时，现有连接将作为未加速连接继续运行。新的连接速度加快。

在 **WCCP** 模式下，路由器绕过停止响应的设备，并在设备再次开始响应时重新打开连接。WCCP 协议执行整体运行状况检查。

如果“验证-可用性”选项与 虚拟内联模式一起使用，路由器的行为就像 WCCP 模式一样，在设备不可用时绕过设备，并在设备不可用时重新连接。如果未使用“验证可用性”，则转发到设备的所有数据包将被丢弃，如果设备不可用。

在 组模式下，可以将设备配置为失败“打开”（桥接禁用）或“关闭”（桥接或旁路继电器启用）。

在 高可用性 模式下，如果一个 HA 设备出现故障，另一个设备将自动接管。在 HA 模式下，设备的旁路卡将被禁用，因此如果 HA 设备处于内联模式并且两个设备都出现故障，则连接将丢失。

在重定向器模式下，Citrix SD-WAN WANOP 插件在重定向器模式设备上执行运行状况检查，并绕过无响应的设备，直接将流量发送到端点服务器。

支持的模式和特征矩阵

April 23, 2021

一般来说，所有模式都同时处于活动状态。但是，某些组合不应一起使用，如下表所示。

支持的组合，带以太网旁路卡的单元							
配置	内联	虚拟内联	**WCCP-GRE**	**WCCP L2**	多桥接	效果很高。	组模式
Citrix SD-WAN WANOP 插件	**Y**	**Y**	**Y**	**Y**	**Y**	**Y**	N
内联	**Y**	N	N	N	**Y**	**Y**	**Y**
虚拟内联		**Y**	**Y**	**Y**	**Y**	**Y**	N
WCCP-GRE			**Y**	**Y**	**Y**	**Y**	N
WCCP L2				**Y**	**Y**	**Y**	N
多桥接					**Y**	**Y**	N
效果很高。						**Y**	**Y**

支持的组合，无以太网旁路卡的单元							
配置	内联	虚拟内联	**WCCP-GRE**	**WCCP L2**	多桥接	效果很高。	组模式
Citrix SD-WAN WANOP 插件	N	N	N	N	N	N	N
内联	**Y**	N	N	N	N	N	N
虚拟内联		**Y**	**Y**	**Y**	N	N	N
WCCP-GRE			**Y**	**Y**	N	N	N

支持的组合， 带以太网旁 路卡的单元				
WCCP L2	**Y**	N	N	N
多桥接		N	N	**Y**
效果很高。			N	N

Y = 是，支持。否 **=** 不受支持。

使用 **Access Gateway VPN** 配置 **Citrix SD-WAN WANOP** 插件

April 23, 2021

访问网关标准版 VPN 支持 Citrix SD-WAN WANOP 插件加速，前提是将 Citrix SD-WAN WANOP 设备与访问网关设备一起部署，并且访问网关设备配置为支持该设备。

有关 Citrix SD-WAN WANOP 插件支持其他 VPN，请参阅您的 VPN 文档或联系您的 Citrix 代表。

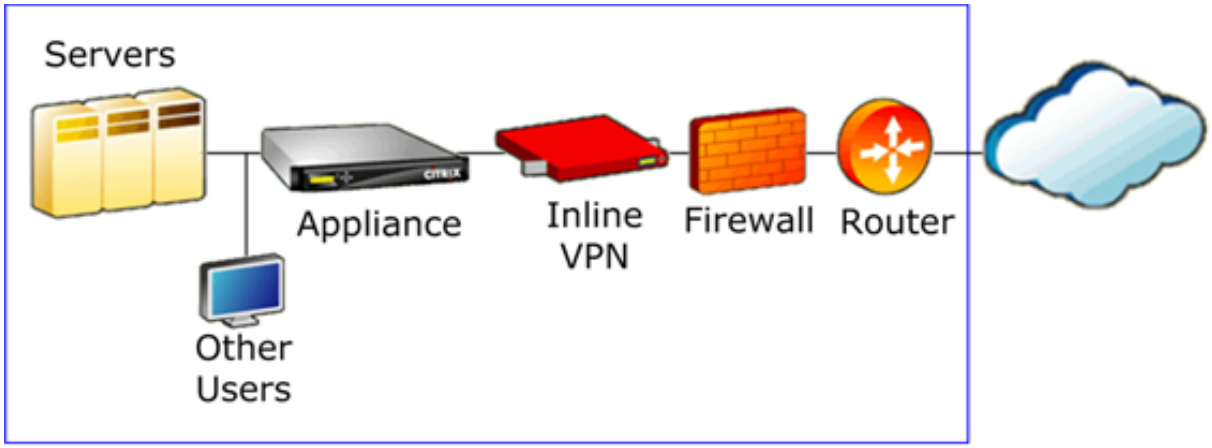
要配置 Citrix SD-WAN WANOP 支持，请使用访问网关管理工具，如下所示：

1. 在“全局群集策略”页上的“高级选项”下，选中使用 **Citrix SD-WAN WANOP** 插件启用 **TCP** 优化复选框。
2. 确保 Citrix SD-WAN WANOP（重定向器 IP 和管理 IP）使用的 IP 地址在访问策略管理器页面的“网络资源”部分中启用了访问权限。
3. 对于其中的每个地址，启用所有协议（TCP、UDP、ICMP）并启用保留 TCP 选项。
4. 请确保“访问策略管理器”页上的“用户组: 默认: 网络策略”下包含这些相同的地址。

VPN 支持选项

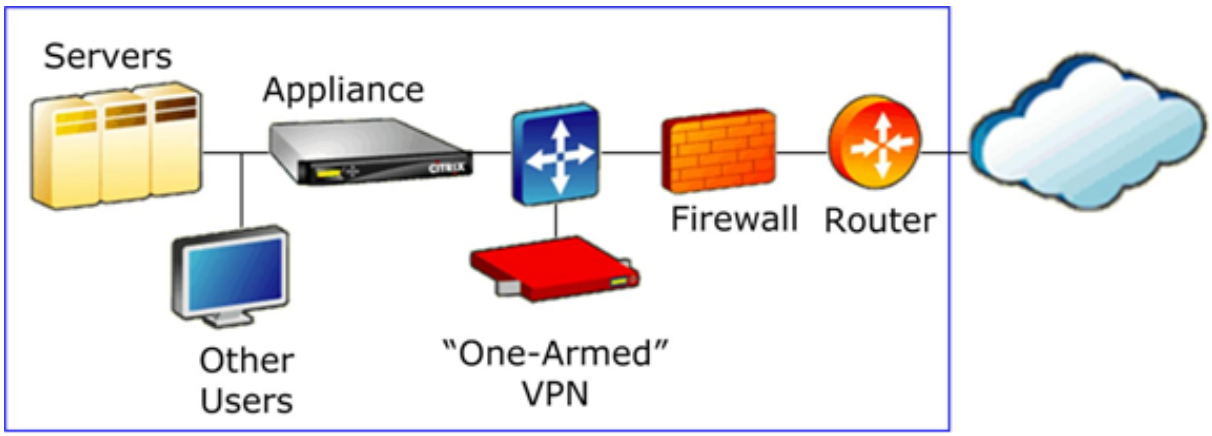
VPN 支持只是将设备放在 VPN 的局域网一侧的问题，如下图所示。这种放置可确保设备接收和传输解压缩、解密、纯文本版本的链路流量，从而使压缩和应用程序加速工作。（应用程序加速和压缩对加密流量没有影响。但是，TCP 协议加速适用于加密流量。）

用于内联 VPN 的 VPN 线路连接



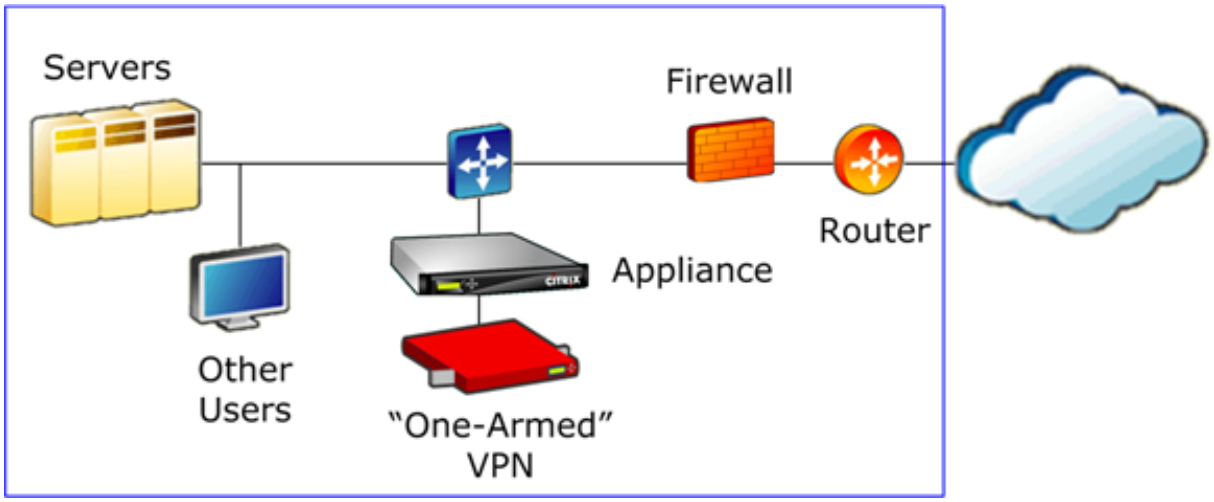
下图显示了加速单臂 VPN 的一个选项。设备位于 VPN 的服务器端。具有本地目标的所有 VPN 流量都会加速。具有远程目标的 VPN 流量不会加速。非 VPN 流量也可以加速。

单臂 VPN 加速，选项 A



下图显示了加速单臂 VPN 的另一种选择。设备位于 VPN 的服务器端。具有本地目标的所有 VPN 流量都会加速。具有远程目标的 VPN 流量不会加速。非 VPN 流量也可以加速。

单臂 VPN 加速，选项 B



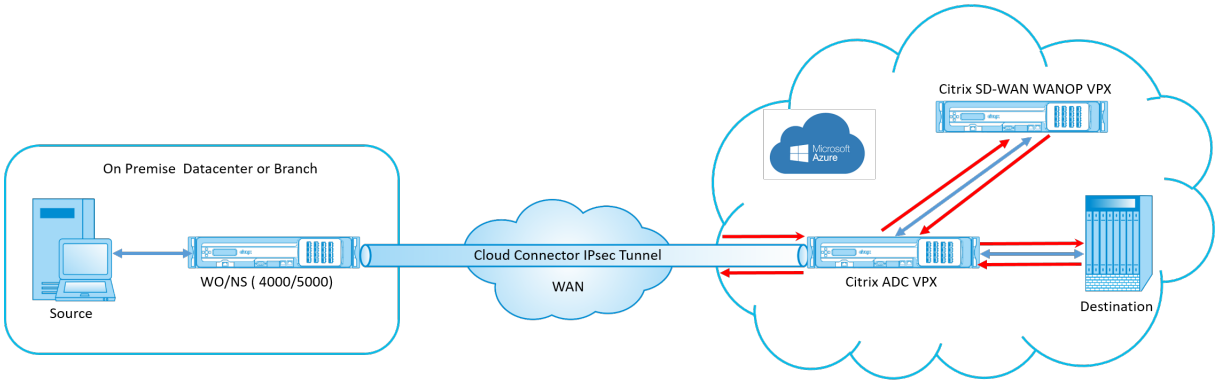
> 重要
>
> 为了有效加速，VPN 必须保留 TCP 标头选项。大多数 VPN 都这样做。

在 Microsoft Azure 上部署 SD-WAN WANOP VPX

April 23, 2021

Citrix SD-WAN WANOP 版现已在 Azure 市场上推出，可在企业数据中心/分支机构和 Azure 云之间实现 WAN 优化。由于 L2 模式支持在云基础结构上不可用，因此无法在 Azure 云中将 Citrix SD-WAN WANOP 部署为独立 VPX。但是，您可以在 Azure 云基础结构中部署思 Citrix SD-WAN WANOP VPX 和 Citrix ADC VPX。Citrix ADC 使用 Cloud Connector 创建 IPSec 隧道，而 Citrix SD-WAN WANOP VPX 可加速连接，从而为应用程序提供类似 LAN 的性能。

Azure 云拓扑中的 Citrix SD-WAN WANOP



拓扑图显示了部署在数据中心或分支机构内部的 Citrix SD-WAN 4000/5000。您还可以在双盒模式下部署 Citrix SD-WAN WANOP 和 Citrix ADC 设备，也可以是 VPX。在 Azure 云 VNET 上，使用 Citrix ADC VPX 以单臂 (PBR) 模式部署 Citrix SD-WAN WANOP VPX。

部署概述

若要在 Microsoft Azure 上部署 SD-WAN WANOP，请执行以下操作：

1. 在 Azure 云上部署 Citrix ADC VPX 实例。有关详细信息，请参阅在 Microsoft Azure 上部署 Citrix ADC VPX 实例。在四个不同的子网中配置四个网络接口，并在所有网络接口上启用 IP 转发。四个网络接口用作：
    - 管理接口
    - 广域网侧接口，适用于 IPSec 通道

- LAN 端接口，连接到服务器
- WANOP 通信接口，与 Citrix SD-WAN WANOP VPX 在 Azure 云上进行通信。

2. 在 Azure 云上部署 Citrix SD-WAN WANOP VPX。有关详细信息，请参阅下面的部署过程。

   > 注意：在 WANOP 接口上启用 IP 转发。

3. 使用 Citrix ADC WAN 接口的公有 IP 地址，在本地设备和 Azure 云上的 Citrix ADC VPX 之间配置 IPSec 隧道。有关配置 IP 通道的更多信息，请参阅IP 通道。
4. 将 Citrix ADC VPX 配置为将数据包重定向到 Citrix SD-WAN WANOP VPX。使用 WANOP 通信接口的私有 IP 地址，创建负载平衡虚拟服务器。有关详细信息，请参阅创建负载平衡虚拟服务器。
5. 在 Azure 上配置以下路由表：

   - Citrix ADC VPX 上面向 WANOP 的接口的路由表-路由表条目应分别具有源地址和目标地址作为客户端子网和服务器子网。Citrix ADC VPX 面向 WANOP 的接口 IP 地址是下一个跃点。
   - Citrix SD-WAN WANOP 接口的路由表-路由表条目应分别具有源地址和目标地址作为客户端子网和服务器子网。Citrix SD-WAN WANOP 接口 IP 地址是下一个跃点。

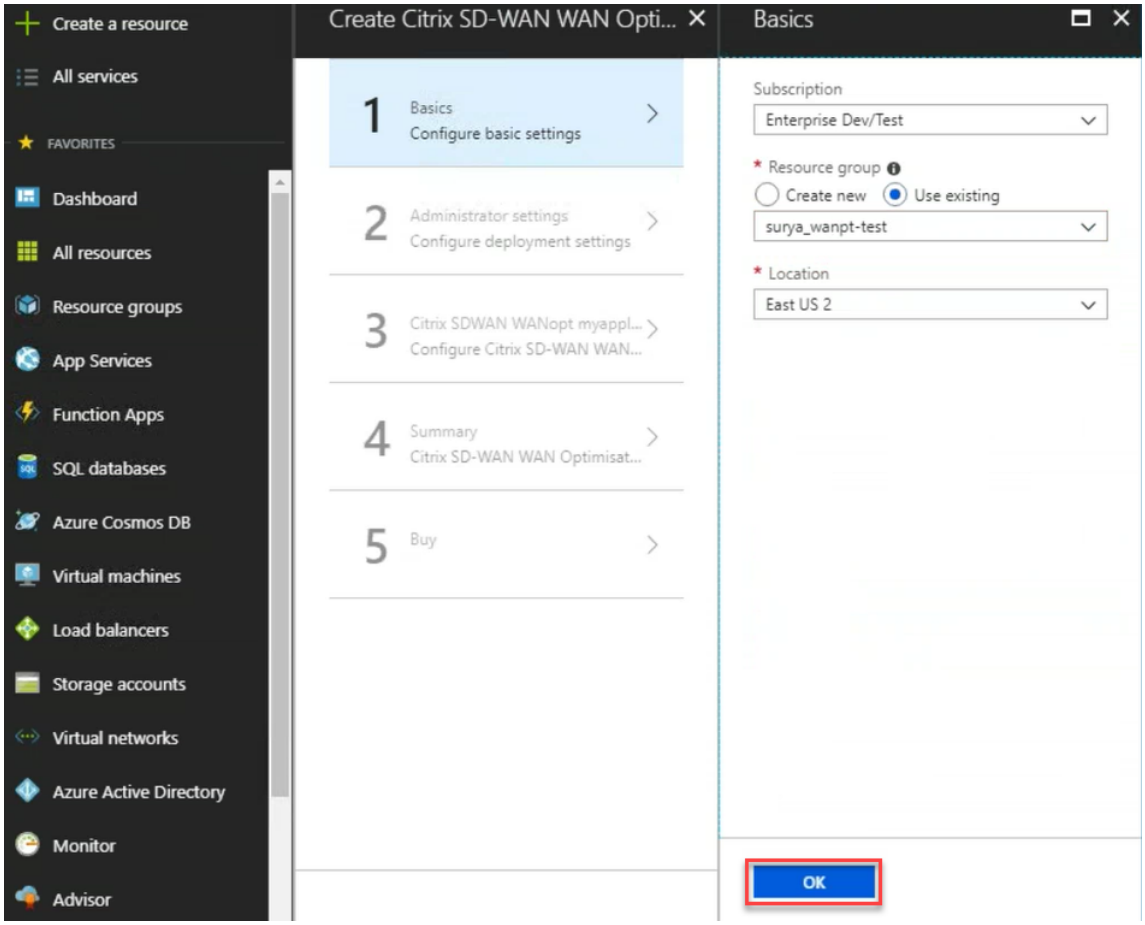
在上面的示例中，当源尝试访问云目标上的应用程序时，数据包会流经已建立的 IPSec 通道。在 Azure 云 VNET 端，Citrix ADC VPX 接收数据包、解密并将其转发到 Citrix SD-WAN WANOP VPX。Citrix SD-WAN WANOP VPX 处理数据包、优化数据包并将其发送回 Citrix ADC VPX。Citrix ADC VPX 将数据包发送到目标。在返回路径上，Citrix ADC VPX 将数据包转发到 Citrix SD-WAN WANOP VPX 以进行优化。优化的数据包通过已建立的 IPSec 通道传送回源。

在 **Microsoft Azure** 上部署 **Citrix SD-WAN WANOP VPX**

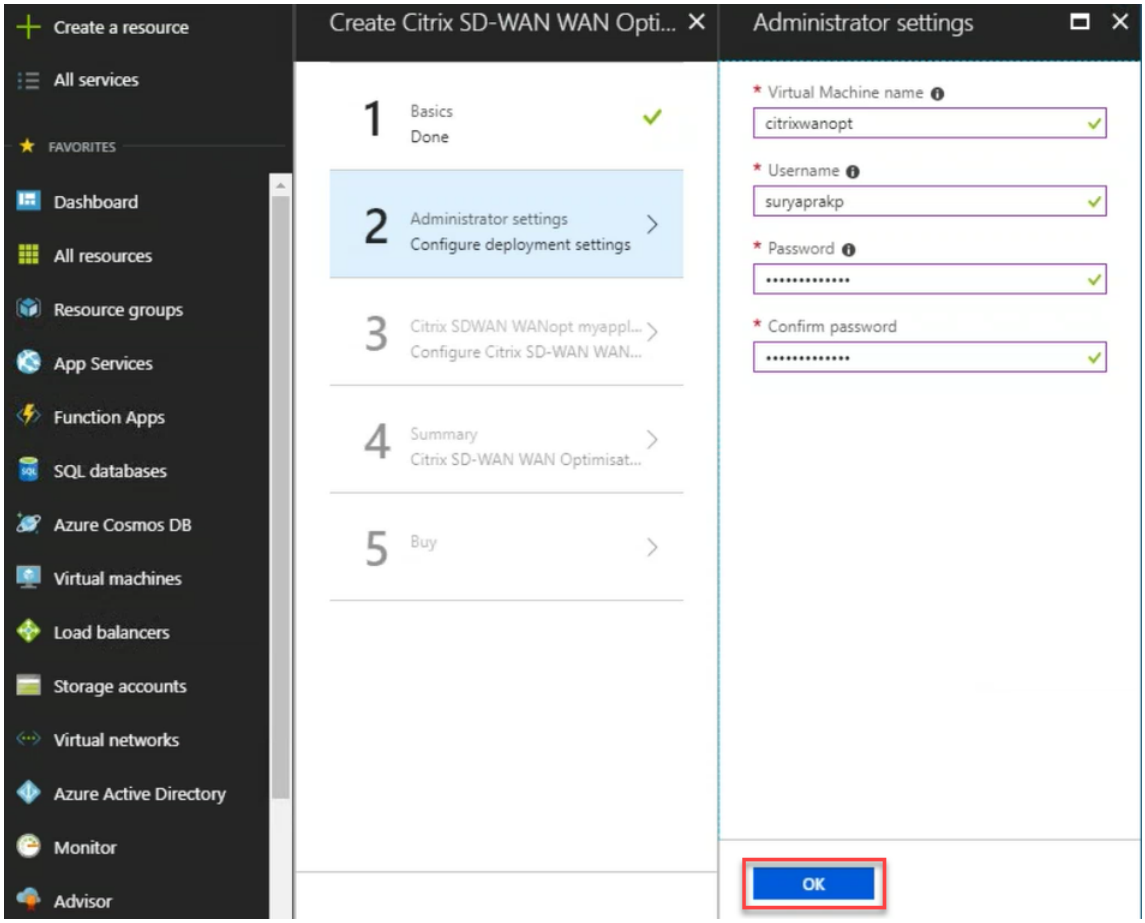
若要在 Microsoft Azure 上部署 Citrix SD-WAN WANOP VPX，请执行以下操作：

1. 在 Microsoft Azure 中，导航到主页 > 市场 > 网络连接，搜索 **Citrix SD-WAN WANOP** 并进行安装。
2. 在 Citrix SD-WAN OP 页面上，从下拉列表中选择 资源管理器，然后单击 创建。此时将显示创建 **Citrix SD-WAN WAN** 优化页面。
3. 在基础部分中，选择订阅类型、资源组和位置。单击确定。

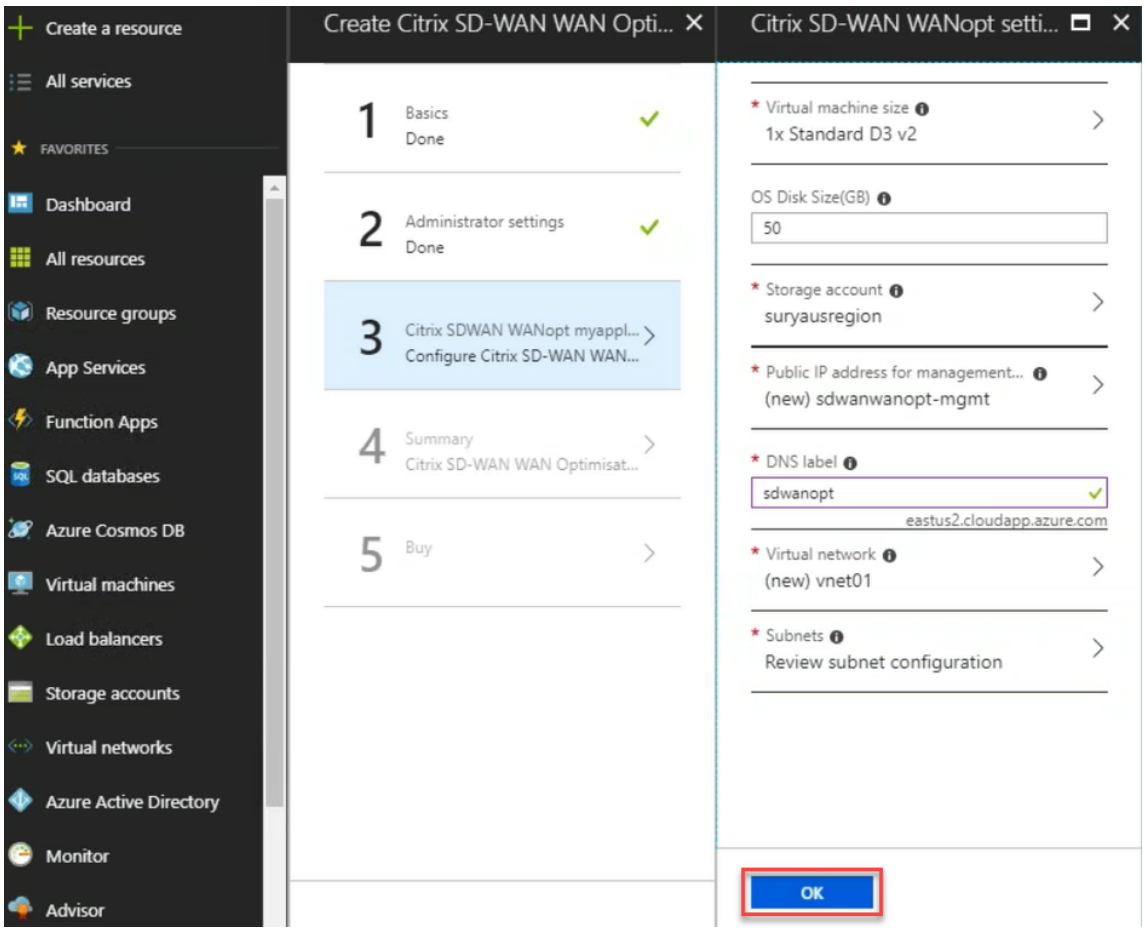
   > 注意：
   >
   > 您可以选择创建资源组。资源组是一个容器，用于保存 Azure 解决方案的相关资源。资源组可以包括解决方案的所有资源，或者仅包括要作为一个组管理的资源。



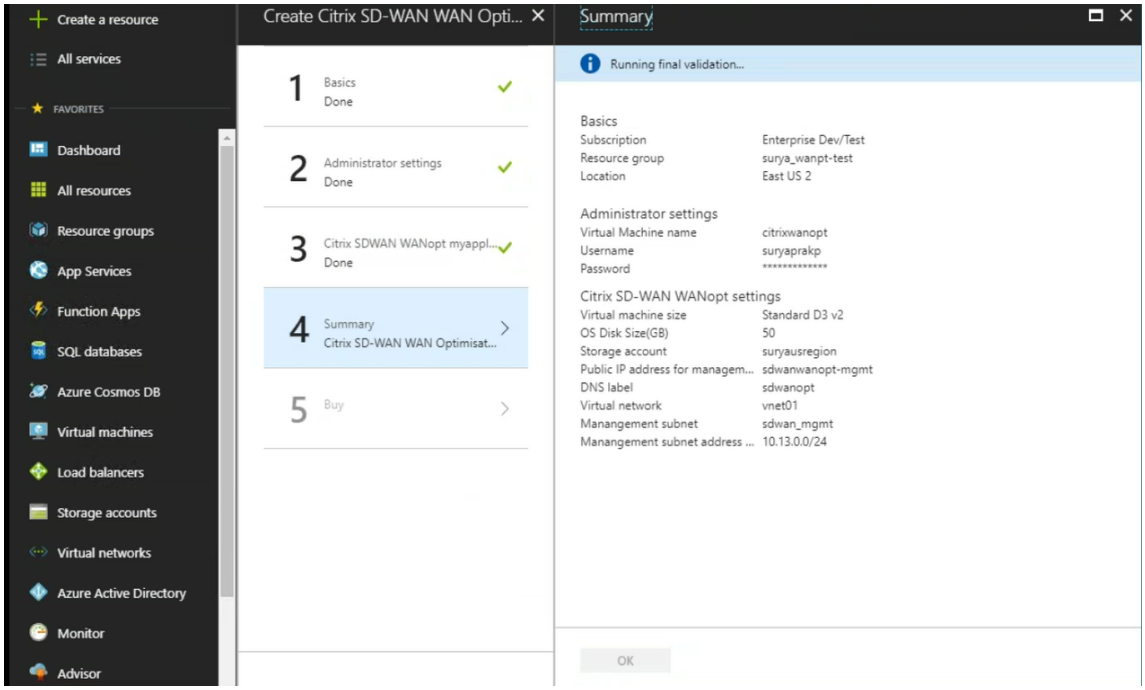
4. 在管理员部分中，输入 Citrix SD-WAN WANOP 虚拟机的名称和凭据。单击 **OK**（确定）。



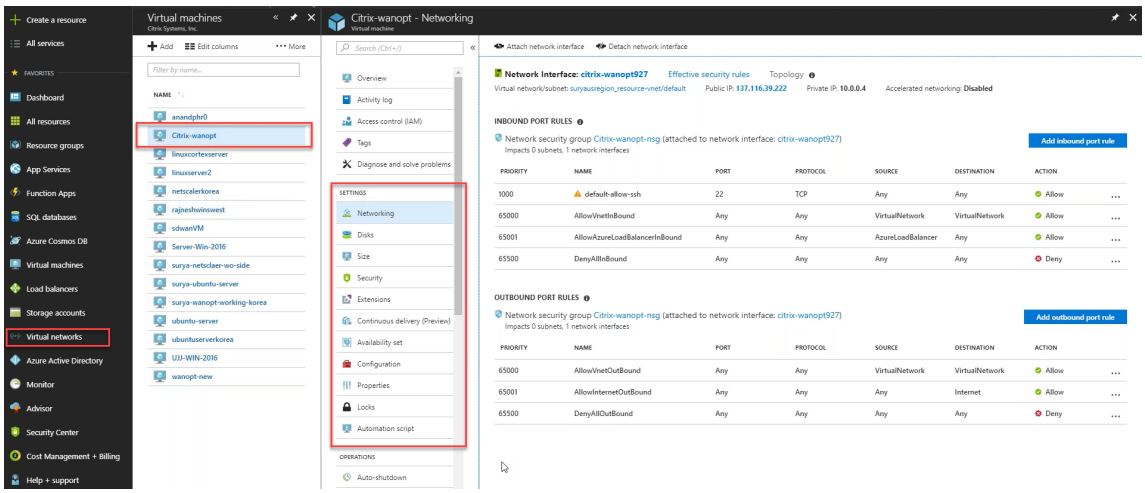
5. 在 **Citrix SD-WAN WANOP** 设置部分，根据您的要求配置 Citrix SD-WAN WANOP VPX 的设置。单击确定。



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，导航到 虚拟网络 以查看 Citrix SD-WAN WANOP VPX。您可以使用设置选项进一步配置虚拟机参数。



SD-WAN WANOP 升级过程

April 23, 2021

本节提供有关下载和升级 Citrix SD-WAN 广域网优化 (WANOP) 软件包的信息。

> 注意：
>
> 下载软件之前，必须获取并注册 Citrix SD-WAN 软件许可证。有关信息，请参阅许可。

下载软件包

要下载 Citrix SD-WAN WANOP 软件包，请转到 URL 产品下载。本网站提供了下载软件的说明。

要下载 Citrix SD-WAN WANOP 软件包，请执行以下操作：

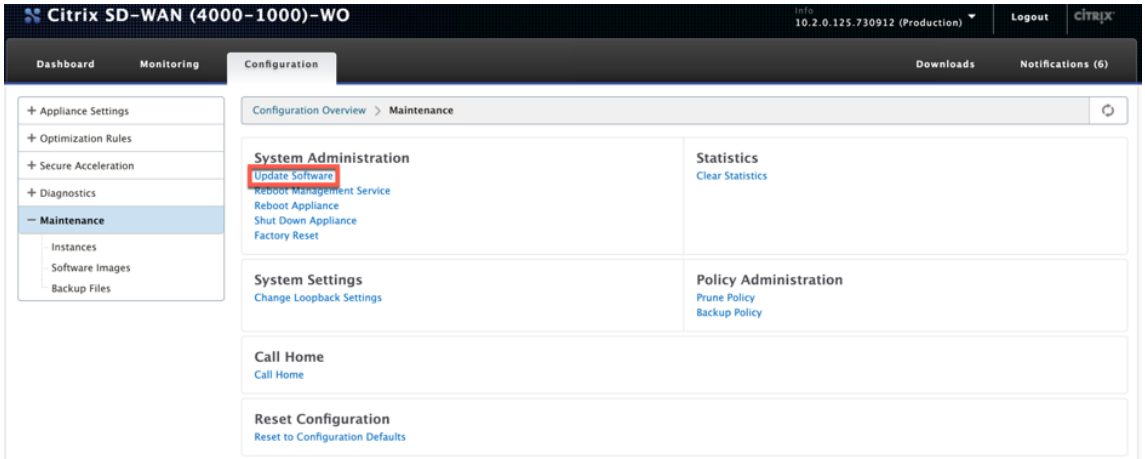
1. 使citrix.com用您的凭据登录。
2. 转到下载页面并从下拉列表中选择产品（Citrix SD-WAN）。
3. 展开 **Citrix SD-WAN WANOP** 版本 并选择所需的软件版本。
4. 以下下下载选项可用。下载所需软件。
   - 下载适用于 SD-WAN WANOP 400/800/1000/1000WS/2000/2000WS/3000/4000/4100/5000/5100 设备的.upg 升级文件。
   - 下载 SD-WAN WANOP VPX 设备的.bin 升级文件。

有关 SD-WAN WANOP 支持的平台的更多信息，请参阅SD-WAN 平台模型和软件包。

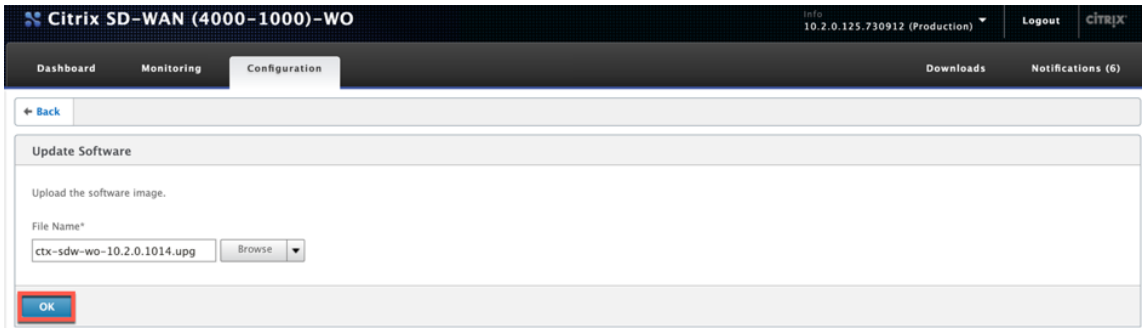
升级过程

执行以下过程以更新软件：

1. 导航到 配置 **>** 维护 **>** 系统管理 **>** 单击 更新软件。

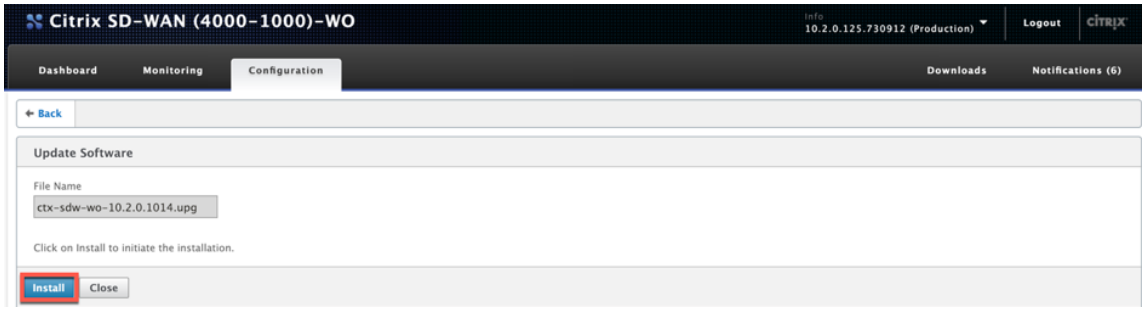


2. 单击浏览以提供 **ctx-sdw-wo-10.2.X.upg** 文件。单击 **OK**（确定）。



您可以看到上传状态栏。

3. 当一条消息宣布上载成功时，单击 安装”。



4. 设备执行升级，根据平台模型，升级需要 10-40 分钟。它显示一系列状态消息，从 准备升级” 开始，到 已成功升级 结束。
5. 单击 确定 以显示更新后的用户界面。

初始配置

April 23, 2021

检查连接后，您可以在网络上部署 SD-WAN 设备。

从 Citrix 发送的设备上配置了默认 IP 地址。要在网络上部署设备，必须在设备上配置适当的 IP 地址以加速网络流量。

初始配置包括以下任务：

- 确定初始配置的先决条件。
- 记录初始配置过程中所需的各种值。
- 通过将设备连接到以太网端口来配置设备。
- 通过串行控制台分配管理 IP 地址。

默认情况下，初始配置将以内联模式部署设备。

必备条件

April 23, 2021

要部署 Citrix SD-WAN 4100 或 5100 设备，必须在配置设备之前完成以下先决条件设置。

软件版本

本文档涵盖 SD-WAN 软件的发布。有关与 SD-WAN 软件所需版本相对应的 NetScaler 软件的推荐版本，请参阅发行说明。切勿使用 SD-WAN 4100 和 5100 设备推荐的版本以外的任何版本。

许可证文件

加速器设备的数量取决于硬件平台和应用于设备的许可证类型。下面的列表显示了由配置向导自动配置的加速器的数量：

- 型号 310：两个
- 型号 500：三个
- 型号 1000 和 1500：六个
- 型号 2000：八个

在开始预配设备之前，Citrix 建议您备好许可证文件，因为在配置过程的早期阶段需要许可证文件。要下载许可证文件，请完成“我的帐户所有许可工具 - 用户指南”中描述的过程。

安装硬件

从 Citrix 收到硬件设备后，需要将其安装在网络中。要安装 SD-WAN 4100/5100 设备硬件，请按照上的安装步骤操作安装硬件。

部署工作表

April 23, 2021

> 注意
>
> 仅当使用 9.3 版配置向导预配出厂重置设备时，才使用此工作表。如果您只是将之前配置的系统升级到版本 9.3，则设备将保留其以前的配置，这种配置将不同。

设备至少使用两个端口：管理端口（通常为 0/1）和流量端口（如 10/1）。内联模式使用成对的流量端口，例如端口 10/1 和 10/2。必须提前选择端口，因为配置取决于端口的身份。

设备直接使用三个子网：管理子网、外部流量子网和内部流量子网。在每个子网上使用多个 IP 地址。每个子网必须与正确的子网掩码一起指定。

下图是这些参数的工作表。它支持内联和 WCCP 模式，具有和不具有高可用性。下面的表格描述了每个条目的含义。

表 1. 部署工作表参数

参数	示例	您的价值	说明
管理子网			

	参数	示例	您的价值	说明
M2.	网关 IP 地址	10.199.79.254		为管理子网提供服务的默认网关。
M3.	子网掩码	255.255.255.128		管理子网的子网掩码。
M4.	Xen 虚拟机管理程序 IP 地址	10.199.79.225		Xen 虚拟机管理程序的 IP 地址。
M5.	服务虚拟机 IP 地址	10.199.79.226		管理服务虚拟机的 IP 地址，用于控制配置。
M6.	加速器 UI	10.199.79.227		加速器 GUI，也称为 Broker UI，它将实例作为一个单元进行管理。
M7.	NetScaler 管理 IP 地址	10.199.79.245		NetScaler 实例的 GUI 和 CLI 接口的 IP 地址。
外部流量子网				
T1.	路由器 IP 地址	172.17.17.1		外部流量子网上路由器的 IP 地址。
T2.	子网掩码	255.255.255.0		外部流量子网的子网掩码。
T3.	NetScaler IP 地址	172.17.17.2		外部流量子网上的 NetScaler IP 地址。
T4.	外部信令 IP 地址	172.17.17.10		到此 IP 地址的流量在加速器的信令 IP 地址之间进行负载平衡。
T5.	外部 WCCP IP 地址 #1	172.17.17.11		通过 NAT 映射到加速器 #1 上的 WCCP VIP。
T6.	外部 WCCP IP 地址 #2	172.17.17.12		通过 NAT 映射到加速器 #2 上的 WCCP VIP。
T7.	本地 LAN 子网	10.200.0.0/16		要加速的本地 LAN 子网。这是唯一接收加速的子网。
T8.	GRE 路由器主机 ID	不适用		仅限 WCCP-GRE。GRE 路由器的主机 ID.

	参数	示例	您的价值	说明
T9.	流量端口	10/1		用于加速流量的端口。
T10+.	（内联）更多流量端口			对其他流量端口。
T11, T12	(WCCP) 服务组：TCP、UDP	71, 72		WCCP 加速器 #1 使用的服务组。首先是 TCP 流量，第二个是 UDP。
T13, T14	（未使用）			
T15, T16	链接 #2 使用的（内联）端口	10/5, 10/6		如果在内联模式下使用多个链接，则这些端口用于链接 #2。
T17, T18	链接 #3 使用的（内联）端口	10/7, 10/8		如果在内联模式下使用多个链接，则这些端口用于链接 #3。
VLAN1.1、VLAN1.2、VLAN1.3、VLAN1.4	用于桥接 #1 的外部 VLAN	412		使用 VLAN 中继时，这些标记为穿越桥 #1 的 VLAN。
VLAN2.1、VLAN2.2、VLAN2.3、VLAN2.4				使用 VLAN 中继时，这些标记为穿越桥 #2 的 VLAN。
VLAN3.1、VLAN3.2、VLAN3.3、VLAN3.4	用于桥接 #1 的外部 VLAN			使用 VLAN 中继时，这些标记为穿越桥 #3 的 VLAN。

配置设备

April 23, 2021

在开始配置设备之前，必须将管理服务的 IP 地址更改为管理网络中的 IP 地址，以便可以通过网络访问设备。您可以通过以太网端口或串行控制台将计算机连接到设备来更改管理 IP 地址。

通过以太网端口分配管理 IP 地址

April 23, 2021

使用以下过程对配备 Windows Server 的每台 SD-WAN 1000 或 2000 设备进行初始配置。该过程完成以下任务：

- 配置要在站点上使用的设备。
- 安装 Citrix 许可证。
- 启用加速。
- 启用流量成形（仅限内联模式）。

对于内联部署，此配置可能是您所需的全部内容，因为大多数加速功能默认处于启用状态，且无需额外配置。

如果要通过串行控制台将设备连接到计算机来配置设备，请通过完成此过通过串行控制台分配管理 IP 地址程从工作表中分配管理服务 IP 地址，然后运行步骤 4 至 15 的下列程序.

> 注意：
>
> 您必须具有对设备的物理访问权限。

通过将计算机连接到 SD-WAN 设备的以太网端口 0/1 来配置设备

1. 将计算机（或具有以太网端口的其他配备浏览器的设备）的以太网端口地址设置为 192.168.100.50，网络掩码为 255.255.0.0。在 Windows 设备上，这是通过更改 LAN 连接的 Internet 协议版本 4 属性来完成的，如下所示。您可以将 Gateway 关和 DNS 服务器字段留空。

2. 使用以太网电缆，将此计算机连接到 SD-WAN 设备上标记为 PRI 的端口。
3. 打开设备。使用计算机上的 Web 浏览器，使用默认管理服务 IP 地址（即）访问设备http://192.168.100.1。
4. 在登录页面上，使用以下默认凭据登录设备：

- 用户名：nsroot
- 密码：nsroot

1. 通过单击 开始”启动配置向导。
2. 在 平台配置 页面上，从工作表中输入相应的值，如以下示例所示：

3. 单击完成。此时将显示“正在进行的安装…”消息的屏幕。此过程大约需要 2 到 5 分钟，具体取决于您的网络速度。
4. 将显示重定向到新的管理 IP 消息。
5. 单击确定。
6. 从以太网端口拔出计算机，然后将该端口连接到管理网络。
7. 将计算机的 IP 地址重置为之前的设置。

8. 从管理网络上的计算机，通过在 Web 浏览器中输入新的管理服务 IP 地址登录到设备`https://<Managemnt_IP_Address>`。
9. 要继续配置，请接受证书并继续。继续选项因您使用的 Web 浏览器而异。
10. 通过使用 **nsroot** 用户名和密码来登录到设备工作表。
11. 要完成配置过程，请参阅预配设备。

通过串行端口分配管理 IP 地址

April 23, 2021

如果不想更改计算机的设置，可以通过使用串行空调制解调器电缆将其连接到计算机来配置设备。您必须具有对设备的物理访问权限。

通过串行控制台配置设备

1. 将串行空调制解调器电缆连接到设备的控制台端口。
2. 使用设置 9600,N,8,1, p 将电缆的另一端连接到运行端点仿真器的计算机的串行 COM 端口，例如 Microsoft HyperTerminal。
3. 在 HyperTerminal 输出中，按 **Enter** 键。终端屏幕将显示登录提示。注意：您可能需要按 En **ter** 两次或三次，具体取决于您正在使用的端点程序。
4. 在登录提示符下，使用以下默认凭据登录到设备：

- 用户名：nsroot
- 密码：nsroot

1. 在 **$** 提示符处，运行以下命令以切换到设备的 shell 提示符：`$ ssh 169.254.0.10`
2. 输入 是 以继续连接到管理服务。
3. 使用以下默认凭据登录到设备的 shell 提示符：
   密码：nsroot。
4. 在登录提示符下，运行以下命令以打开管理服务初始网络地址配置菜单：`# networkconfig`
5. 键入 **1** 并按 **Enter** 键选择选项 1，并为管理服务指定新的管理 IP 地址。
6. 键入 **2** ，然后按 **Enter** 键选择选项 2，然后为 Citrix Hypervisor 指定新的管理 IP 地址。
7. 键入 **3** ，然后按 **Enter** 键选择选项 3，并指定 IP 地址的网络掩码。
8. 键入 **4** ，然后按 **Enter** 键选择选项 4，并为管理服务 IP 地址指定默认 Gateway。
9. 键入 **8** 并按 **Enter** 键保存设置并退出。
10. 通过在管理网络上计算机的 Web 浏览器中输入设备的新管理服务 IP 地址来访问 SD-WAN 设备`https://<Management_Service_IP_Address>`。
11. 要继续配置，请接受证书并继续。继续选项因您使用的 Web 浏览器而异。
12. 要完成配置过程，请参阅预配设备。

预配设备

April 23, 2021

将 IP 地址分配给管理服务后，您可以准备好预配 NetScaler 和加速器实例。登录到设备时，将显示配置向导。

使用配置向导时，请牢记以下几点：

- 以下过程假定您已填写配置工作表。
- 如果您更改管理网络的 IP 地址，或者将默认 Gateway 更改为不在管理网络上的地址，则除非您与管理端口处于同一个以太网段，否则您将失去与设备的连接。
- 使用配置向导时，请仔细检查条目。向导没有“后退”按钮。如果您需要修改上一个屏幕，请使用浏览器上的 后退 按钮。这将带您到登录页面，然后转到上一个屏幕。
- 仅当您首次登录设备以配置设备时，才会显示配置向导。完成设备配置后，此向导将无法访问，并且仅在恢复出厂设置后才会重新出现。仔细检查你的条目。

此向导将引导您完成设备的全新配置。

> 注意：
>
> 如果您在这些过程中随时收到 #SESS_CORRUPTED 错误，请单击“
> 注销”，清除浏览器缓存，关闭浏览器，然后再次打开。

要使用配置向导配置设备，请执行以下操作：

1. 在欢迎页面上，单击 开始。

   > 注意：
   >
   > “开始”页面之后的所有页面都有一个标题，标题显示“部署模式：联机/L2 模式”，但此向导用于所有部署模式。

2. 请按照以下步骤配置完全符合 7.3 标准的系统：

   - 从我的 Citrix 上的 7.3 版下载页面获取以下 7.3 版软件发行版：
     - 管理服务（作为.tgz 文件）
     - NetScaler 虚拟机（作为.xva 文件）
     - 加速器 VM（作为.xva 文件）
     - 升级捆绑包（作为.upg）文件
   - 导航到 “系统”**>** “配置”**>** “管理服务”**>** “软件映像 页面，然后从“操作”列表中选择 上传。
   - 上传 7.3 版管理服务映像（作为.tgz 文件分发）。
   - 导航到 系统”**>** “配置”**>** “**NetScaler\ >** “软件映像 页面，然后上传版本 7.3 NetScaler XVA 映像。
   - 导航到 “系统”**>** “配置”**>** “**SD-WAN**”**>** “软件映像 页面，然后上传加速器 XVA 映像。
   - 导航到 系统”**>** “配置”**>** “管理服务 页面，然后单击 升级管理服务 链接。

- 选择您最近上传的管理服务映像，然后单击 确定”。
- 当屏幕左下角显示“管理服务更新成功”时，注销并清除浏览器缓存。在管理服务重新启动（几分钟）后登录。
- 在 欢迎 屏幕上，单击 开始。

3. 对于“管理访问设置”，根据网络设置为各个字段指定值。以下屏幕截图显示了本文档中使用的示例值。输入值，如下所示：

   - **Citrix Hypervisor IP** 地址—（工作表上的项目 M4；如果这是高可用性对中的第二台设备，则 H4。）内置 Citrix Hypervisor 虚拟机管理程序的管理地址。该地址必须是管理网络上的有效地址。
   - 管理服务 **IP** 地址—（工作表上的项目 M5，如果这是高可用性对中的第二个设备，则 H5）。用于执行大多数系统管理任务的管理服务 VM 的地址。该地址必须是管理网络上的有效地址。
   - 网络掩码—（工作表中的项目 M3）。管理网络的子网掩码。
   - 网关—（工作表中的项目 M2）。管理网络的默认网关。
   - **DNS** 服务器-DNS 服务器的 IP 地址。这是一个必需的参数。
   - **NTP** 服务器—您的时间服务器的 IP 或 FQDN 地址。这将由设备中的所有虚拟机使用。> 注意，如果您使用高级 CIFS 或 MAPI 加速，设备的系统时间必须接近 Windows 域服务器的系统时间，因此请选择与 Windows 域服务器上的时间保持密切关系的 NTP 服务器。

     > 注意：
     >
     > 除非将 NTP 服务器指定为 IP 地址，否则加速器不会使用该地址。

   - 时区—从下拉菜单中选择您的时区。
   - 更改密码—选中此复选框并键入两次新的 nsroot 密码以更改密码。同样的密码用于管理服务和帐户 nsroot 的 NetScaler 实例，以及管理员帐户的加速器。如果没有更改密码，它仍然设置为 nsroot（默认值）。

     图 1. 配置的“管理访问设置
     ”页中的字段的示例值

4. 检查您的设置，然后单击 继续。
5. 在 管理许可证 部分，查看 名称 字段中是否已列出相应的许可证。如果是这样，请选择它并跳到步骤 8。
6. 单击 更新许可证 部分中的 上传。
7. 导航到包含许可证文件的文件夹并打开该文件。
8. 单击 添加许可证，然后上传 Citrix 提供的许可证文件。许可证将添加到设备中，如下图所示。

   图 2. 在配置向导的“管理许可证文件”页面上添加到设备的示例许可证

   您还可以通过单击链 接并使用我的 Citrix 凭据。

9. 在 名称字 段中选择许可证，然后单击 继续。此时将显示 SD-WAN 设置页面。填写以下字段：

a) 网络设置—此部分通知管理网络的加速器。

- **SD-WAN** 加速器 **IP** 地址—从工作表中输入 M6 的值。这是加速器的 IP 地址
- **NetScaler IP** 地址—从工作表中输入 M7 的值。这是 NetScaler GUI 的 IP 地址。
- 使用系统网络掩码和 **Gateway**—如果要使用在“平台配置”页面中指定的网络掩码和网关 IP 地址，请选择此选项。
- 网络掩码—从工作表中输入 M3 的值。这是管理网络的子网掩码（网掩码）（请注意，您已在上一页中输入此掩码）。
- 网关—再次从工作表中输入 M2 的值。
- 信号 **IP** 地址—从工作表中输入 T4 值。这是加速器的外部信号 IP 地址，SD-WAN 插件用于连接到设备。
- 信号网络掩码—从工作表中输入 T2 的值。这是外部流量网络的子网掩码（网络掩码）。

b) **XVA** 文件—此部分允许您为 NetScaler 和加速器实例指定之前上传的 XVA 文件（Xen 虚拟机）。选择您在步骤 2 中上传的 XVA 图像。

图 3. SD-WAN 设置页面

10. 单击继续。向导开始预配所需的实例，如下图所示。

    图 4. 预配进度指示器

11. 预配置实例后，将您的一个本地 LAN 子网添加到工作表中列表 T7 中的 链接配置 部分，如下图所示。此子网作为本地 LAN 子网添加到加速器中。如果您有多个 LAN 子网，则可以在配置向导完成后将它们添加到加速器 GUI 中的 **LAN** 链接 定义中。单击 添加 以添加子网。

    图 5. 链接配置位于本页

    底部

12. 注销，然后重新登录。如果您看到“检测到版本不兼容性”消息，请安装您在步骤 2 中下载的升级包。

基本配置已完成。接下来，执行特定于部署模式的配置（如 WCCP 模式）。

> 注意：
>
> 向导完成后，将为基本设置配置设备。要为特定部署方案配置设备，请参阅部署模式。

部署模式

April 23, 2021

SD-WAN 设备充当虚拟 Gateway。它既不是 TCP 端点，也不是路由器。像任何 Gateway 一样，它的工作是缓冲传入的数据包，并以正确的速度将它们放到传出链接上。此数据包转发可以通过不同的方式进行，例如内联模式、虚拟内

联模式和 WCCP 模式。尽管这些方法称为 模式，但您不必禁用一种转发模式即可启用另一种转发模式。如果您的部署支持多种模式，则设备使用的模式将由每个数据包的以太网和 IP 格式自动确定。

由于设备支持不同的转发模式和不同类型的非转发连接，因此需要一种区分一种流量和另一种流量的方法。它通过检查目标 IP 地址和目标以太网地址（MAC 地址）来执行此操作，如下表所示。例如，在内联模式下，设备充当桥接。与其他流量不同，桥接数据包会发送到设备以外的系统，而不是设备本身。地址字段既不包含设备的 IP 地址，也不包含设备的以太网 MAC 地址。

除了纯转发模式之外，设备还必须考虑其他类型的连接，包括与 GUI 的管理连接以及在高可用性对成员之间传递的检测信号。为了完整起见，这些额外的流量模式也列在下表中。

表 **1.** 以太网和 **IP** 地址如何决定模式

目标 IP 地址	目的地以太网地址	模式
非设备	非设备	内联或直通
非设备	设备	虚拟内联或 L2 WCCP
设备	设备	直接（用户界面访问）
電器 (VIP)	设备	高可用性。代理模式
设备（WCCP GRE 数据包）	设备	WCCP GRE 模式
设备（信号 IP）	设备	信令连接（SD-WAN 插件信令连接（SD-WAN 插件，安全对等）或重定向器模式连接（SD-WAN 插件）

所有模式都可以同时处于活动状态。给定数据包使用的模式由以太网和 IP 标头决定。

转发模式是：

- 内联模式，在此模式下，设备可透明地加速其两个以太网端口之间的流量。在此模式下，设备（在网络的其余部分）显示为以太网桥。建议使用内联模式，因为它需要的配置最少。
- **WCCP** 模式，它使用 WCCP v 2.0 协议与路由器通信。这种模式很容易在大多数路由器上进行配置。WCCP 具有两个变体：WCCP-GRE 和 WCCP-L2。WCCP-GRE 将 WCCP 流量封装在通用路由封装 (GRE) 通道内。WCCP-L2 使用未封装的网络第 2 层（以太网）传输。
- 虚拟内联模式，在此模式下，路由器将 WAN 流量发送到设备，设备将其返回路由器。在此模式下，设备似乎是路由器，但不使用路由表。它将返回流量发送到真正的路由器。当内联模式和高速 WCCP 操作不实际时，建议使用虚拟内联模式。
- 组模式，允许两台设备一起运行，以加速一对广泛分离的 WAN 链路。
- 高可用性模式，允许设备作为活动/备用高可用性对运行。如果主设备发生故障，则辅助设备将接管。

为了完整性，此处列出了其他流量类型：

- 直通流量 是指设备不尝试加速的任何流量。它是一个流量类别，而不是转发模式。
- 直接访问，设备充当普通服务器或客户端。GUI 和 CLI 是使用 HTTP、HTTPS、SSH 或 SFTP 协议直接访问的示例。直接访问流量还可以包括 NTP 和 SNMP 协议。
- 设备到设备的通信，其中可以包括信令连接（用于安全对等和 SD-WAN 插件）、VRRP 检测信号（用于高可用性模式）和加密 GRE 通道（用于组模式）。
- 弃用的模式。代理模式和重定向器模式是旧式转发模式，不应在新安装中使用。

SD-WAN 4100/5100 设备有两种推荐的部署模式：WCCP 和内联。这些模式通常在没有高可用性（高可用性）的情况下使用，而在高可用性的情况下则较少使用。

目前，Citrix 推荐用于大多数部署的 WCCP 模式，具有单个路由器并且没有高可用性。当 WCCP 不可用时，请使用内联模式。

虽然目前并非建议使用以下所有模式，但它们都受支持：

- 带有单个路由器的 WCCP 模式
- 具有单个路由器和高可用性的 WCCP 模式
- 在 WCCP 模式下的两个或多个设备与 NetScaler MPX 设备的级联
- WCCP 模式下的两个或多个设备与 NetScaler MPX 设备的级联高可用性
- 内联模式
- 高可用性的内联模式
- 虚拟内联模式
- 高可用性的虚拟内联模式

> 注意
>
> 虽然支持 WCCP 和内联模式以外的模式，但它们没有完整的记录，不推荐用于典型安装。在考虑其中一种模式时，请联系您的 Citrix 代表。

自定义以太网端口

April 23, 2021

典型设备有四个以太网端口：两个加速桥接端口，称为加速对 *A*（apA.1 和 apA.2），带有旁路（故障到线）继设备，以及两个未加速的主板端口，称为主板端口和 Aux1。桥接端口提供加速，而主板端口有时用于辅助目的。大多数安装只使用桥接端口。

一些 SD-WAN 单元只有主板端口。在这种情况下，两个主板端口被桥接。

设备的用户界面可以通过 VLAN 或非 VLAN 网络访问。您可以将 VLAN 分配给设备的任何桥接端口或主板端口，以便进行管理。

图 1. 以太网端口

端口列表

端口命名如下：

以太网端口	名称
主板端口 1	主要（如果没有旁路卡，则为 apA.1）
主板端口 2	Auxiliary1 或 Aux1（如果没有旁路卡，则 apA.2）
桥 #1	加速对 A（apA，附有端口 apA.1 和 apA.2）
桥 #2	加速对 B（apB，端口 apB.1 和 apB.2）

表 1. 以太网端口名

端口参数

April 23, 2021

每个桥接和主板端口可以是：

- 已启用或已禁用
- 已分配 IP 地址和子网掩码
- 已分配默认 Gateway
- 分配给 VLAN
- 设置为 1000 兆位/秒、100 兆位/秒或 10 兆位/秒
- 设置为全双工、半双工或自动（在 SD-WAN WANOP 4000/5000 设备上，某些端口可以设置为 10 Gbps）

除了速度/双工设置之外，所有这些参数都在配置：IP 地址页面上设置。速度/双工设置在“配置：界面”页面上设置。

> 关于参数的注意事项：

- 禁用的端口不响应任何流量。
- 基于浏览器的 UI 可以在所有端口上独立启用或禁用。
- 要在具有 IP 地址的端口上保护 UI，请在“配置：管理员界面：Web 访问”页面上选择 HTTPS 而不是 HTTP。
- 即使网桥没有 IP 地址，内联模式也可以工作。所有其他模式都要求将 IP 地址分配给端口。
- 流量不会在接口之间进行路由。例如，桥接 apA 上的连接不会跨越到主端口或 Aux1 端口，但仍保留在桥接 apA 上。所有路由问题都留给您的路由器。

加速桥梁（**apA** 和 **apB**）

April 23, 2021

每个设备至少有一对以太网端口，用作加速桥，称为 *apA* （用于 加速对 *A* ）。网桥可以在内联模式 *，* 充当透明网桥，就像它是以太网交换机一样。数据包流入一个端口，流出另一个端口。桥也可以在一个臂模式，中的数据包流入一个端口并返回同一端口。

如果桥接或设备发生故障，则具有旁路卡的设备可维持网络连续性。

某些单位具有多个加速对，这些额外的加速对被命名为 apB、apC 等。

旁路卡

如果设备失电或以其他方式出现故障，则内部继设备关闭，两个桥接端口通过电气连接。此连接可保持网络连续性，但使网桥端口无法访问。因此，您可能需要使用其中一个主板端口进行管理访问。

警告：如果主端口未连接到您的网络，请勿启用该端口。否则，您无法访问设备，以太网旁路和链接关闭传播如

旁路卡是标准的一些型号和可选的其他型号. Citrix 建议您为所有内联部署购买带有旁路卡的设备。

旁路功能与连接两个端口的交叉电缆一样连接，这是正确连接安装的正确行为。

重要提示：必须测试旁路安装-不正确的线路连接可能在正常运行中工作，但不能在旁路模式下工作。以太网端口能够容忍不当的线路连接，并且通常以静默方式进行调整。旁路模式是硬接线的，没有这样的适应性。在设备关闭的情况下测试内联安装，以验证线路连接是否适用于旁路模式。

使用多个网桥

如果设备配备了两个加速网桥，则可以使用它们来加速两个不同的链路。这些链路可以是完全独立的，也可以是连接到同一站点的冗余链路。冗余链路可以是负载平衡的，也可以用作主链路和故障转移链路。

图 1. 使用双桥

当设备为给定连接发送数据包时，数据包将通过设备接收该连接的最新输入数据包的同一桥发送。因此，设备遵守路由器做出的任何链路决策，并自动跟踪当前的负载平衡或主链路/故障转移算法。对于非负载平衡链路，后一种算法还确保数据包始终使用正确的桥接。

WCCP 和虚拟内联模式

WCCP 模式和虚拟内联模式均支持多个桥接。使用情况与单桥情况相同，但 WCCP 有额外的限制，即给定 WCCP 服务组的所有流量必须到达同一桥。

具有多个桥接的高可用性

两个具有多个桥接的单元可以在一个高可用性对中使用。只需匹配桥梁，以便所有链接通过两个设备。

主板端口

April 23, 2021

虽然旁路继设备关闭时无法访问旁路卡上的以太网端口，但主板端口保持活动状态。如果桥接端口无法访问，有时可以通过主板端口访问故障的设备。

主端口

如果启用了主端口并为其分配了 IP 地址，则设备将使用该 IP 地址将自身标识到其他加速单位。此地址在内部用于多种目的，并且在“监视：优化：连接”页面上的“合作伙伴单位”字段中对用户最可见。如果未启用主板端口，设备将使用加速对 A 的 IP 地址。

主端口用于：

- 通过基于 Web 的 UI 进行管理
- 用于组模式的后台通道
- 高可用性模式的后台通道

Aux1 端口

Aux1 端口与主端口相同。如果 Aux1 端口已启用且主端口未启用，则设备将从 Aux1 端口的 IP 地址获取其标识。如果两者都已启用，则主端口的 IP 地址是本机的标识

VLAN 支持

April 23, 2021

虚拟局域网 (VLAN) 使用以太网标头的一部分来指示给定以太网框架属于哪个虚拟网络。SD-WAN 设备支持所有转发模式下的 VLAN 中继（内联、WCCP、虚拟内联和组模式）。使用 VLAN 标记的任意组合进行正确处理和加速。

例如，如果一个通过加速桥接的流量流被地址为 10.0.0.1、VLAN 100，而另一个地址为 10.0.0.1、VLAN 111，则设备知道这些是两个不同的目的地，即使两个 VLAN 具有相同的 IP 地址。

您可以将 VLAN 分配给设备的所有以太网端口、部分以太网端口，或者不分配给任何以太网端口。如果将 VLAN 分配给端口，则管理界面（GUI 和 CLI）仅侦听该 VLAN 上的流量。如果没有分配 VLAN，则管理界面仅侦听没有 VLAN 的流量。在“配置：设备设置：网络适配器：IP 地址”选项卡上进行此选择。

自定义以太网端口

April 23, 2021

典型设备有四个以太网端口：两个加速桥接端口，称为加速对 *A*（apA.1 和 apA.2），带有旁路（故障到线）继设备，以及两个未加速的主板端口，称为主板端口和 Aux1。桥接端口提供加速，而主板端口有时用于辅助目的。大多数安装只使用桥接端口。

一些 SD-WAN 单元只有主板端口。在这种情况下，两个主板端口被桥接。

设备的用户界面可以通过 VLAN 或非 VLAN 网络访问。您可以将 VLAN 分配给设备的任何桥接端口或主板端口，以便进行管理。

图 1. 以太网端口

端口列表

端口命名如下：

以太网端口	名称
主板端口 1	主要（如果没有旁路卡，则为 apA.1）
主板端口 2	Auxiliary1 或 Aux1（如果没有旁路卡，则 apA.2）
桥 #1	加速对 A（apA，附有端口 apA.1 和 apA.2）
桥 #2	加速对 B（apB，端口 apB.1 和 apB.2）

表 1. 以太网端口名

以太网旁路和链接关闭传播

April 23, 2021

注意：链接向下传播已添加到带 7.2.1 版本的 SD-WAN（以前的 SD-WAN）1000、2000、3000、4000 和 5000 台设备中。

大多数设备型号都包含用于内联模式的“故障到线”（以太网旁路）功能。如果电源出现故障，继设备关闭，输入和输出端口与电气连接，从而允许以太网信号从一个端口传递到另一个端口，就好像设备不在那里一样。在故障到线模式下，设备看起来像连接两个端口的交叉电缆。

设备硬件或软件的任何故障都会关闭继设备。重新启动设备时，旁路中继将保持关闭状态，直到设备完全初始化，从而始终保持网络连续性。此功能是自动的，无需用户配置。

当旁路继设备关闭时，设备的桥接端口将无法访问。

如果载波在其中一个桥接端口上丢失，则载波将丢弃在另一个桥接端口上，以确保链接关闭条件传播到设备另一端的设备上。因此，监视链路状态的单元（如路由器）会被告知桥梁另一侧的条件。

链路向下传播有两种工作模式：

- 如果未启用主端口，则一个桥接端口上的链接关闭状态会在另一个桥接端口上短暂镜像，然后重新启用该端口。这允许通过仍连接的端口到达设备，以执行管理、高可用性检测信号和其他任务。
- 如果启用了主端口，设备将假定（不检查）主端口用于管理、高可用性检测信号和其他任务。一个桥接端口上的链接关闭条件在另一个端口上持续镜像，直到运营商恢复或重新启动设备为止。即使在 GUI 中启用了主端口但未连接到网络，也是如此，因此在不使用时应禁用主端口（默认）。

加速整个站点

April 23, 2021

内联模式，加速 WAN 上的所有流量显示了内联模式的典型配置。对于这两个站点，设备都放置在 LAN 和 WAN 之间，因此可以加速的所有 WAN 流量都会加速。这是实现加速度的最简单方法，应该在实际情况下使用。

由于所有链路流量都在设备中流动，因此公平排队和流量控制的好处可防止链路超出。

在 IP 网络中，瓶颈 Gateway 确定整个链路的队列行为。通过成为瓶颈 Gateway，设备可以控制链路，并可以智能地管理链路。这是通过将带宽限制设置为略低于链路速度来完成的。完成此操作后，链路性能是理想的，即使在完全使用链路的情况下，延迟和损失也会降至最低。

部分站点加速

April 23, 2021

要为特定系统组（如远程备份服务器）预留设备的加速带宽，可以在仅包含这些系统的分支网络上安装设备。下图显示了这一点。

图 1. 内联模式，仅加速选定系统

SD-WAN 流量调整依赖于控制整个链路，因此流量调整对于此拓扑无效，因为设备只能看到一部分链路流量。延迟控制取决于瓶颈 Gateway，交互式响应可能受到影响。

WCCP 模式

April 23, 2021

Web 缓存通信协议 (WCCP) 是思科推出的动态路由协议。WCCP 版本 2 最初仅用于 Web 缓存，成为一种更通用的协议，适用于 Citrix SD-WAN 设备等加速器使用。

当内联操作不切实际时，WCCP 模式是安装 SD-WAN 设备的最简单方法。当发生非对称路由时，也就是说，当来自同一连接的数据包通过不同的 WAN 链接到达时，它也很有用。在 WCCP 模式下，路由器使用 WCCP 2.0 协议来转移通过设备的流量。设备接收到后，加速引擎和流量成形器将流量视为在内联模式下接收流量。

> 注意
>
> - 为了本次讨论的目的, WCCP 版本 1 被认为已过时，只提供 WCCP 版本 2。
> - 标准的 WCCP 文档称 WCCP 客户端为“缓存”。为避免与实际缓存混淆，Citrix 通常避免将 WCCP 客户端称为“缓存”。相反，WCCP 客户端通常被称为“设备”。
> - 本讨论使用术语“路由器”来表示支持 WCCP 的路由器和支持 WCCP 的交换机。虽然这里使用了“路由器”一词，但一些高端交换机也支持 WCCP，并且可以与 SD-WAN 设备一起使用。
>
> SD-WAN 设备支持两种 WCCP 模式：
>
> - WCCP 是自 3.x 发布以来支持的原始 SD-WCCP 产品。它支持单个设备服务组（无群集）。
> - 在 7.2 版中引入的 WCCP 群集允许您的路由器在多台设备之间进行负载平衡。

WCCP 模式的工作原理

WCCP 部署 SD-WAN 设备的物理模式是单臂模式，在此模式下，设备直接连接到 WAN 路由器上的专用端口。WCCP 标准包括一个协议协商，其中设备将自身注册到路由器，两者协商使用它们支持的共同功能。协商成功后，将根据 WCCP 路由器和路由器上定义的重定向规则在路由器和设备之间路由流量。

WCCP 模式设备只需要一个以太网端口。设备必须部署在专用路由器端口（或支持 WCCP 的交换机端口）上，或者通过 VLAN 与其他流量隔离。不要混合内联模式和 WCCP 模式。

下图显示了如何将路由器配置为拦截选定接口上的流量并将其转发到启用 WCCP 的设备。每当启用 WCCP 的设备不可用时，流量不会被拦截，并且会正常转发。

图 1. WCCP 流量量

流量封装

WCCP 允许以下任一模式在路由器和设备之间转发流量：

- L2 模式-要求路由器和设备位于同一 L2 段（通常为以太网段）上。IP 数据包未修改，只有 L2 地址被更改以转发数据包。在许多设备中，L2 转发是在硬件层执行的，从而获得最大的性能。由于其性能优势，L2 转发是首选模式，但并非所有支持 WCCP 的设备都支持该模式。
- GRE 模式—通用路由封装 (GRE) 是一种路由协议，理论上设备可以放置在任何地方，但是为了性能起见，必须将设备放置在靠近路由器的位置，在快速、不拥塞的路径上，尽可能减少交换机和路由器。GRE 是原来的 WCCP 模式. 将创建 GRE 标头并将数据包附加到其中。接收设备删除 GRE 头。通过封装，设备可以位于未直接连接到路由器的子网上。但是，封装过程和随后的路由都会增加路由器的 CPU 开销，并且添加 28 字节 GRE 头可能会导致数据包碎片，从而增加额外的开销。

WCCP 模式支持多个路由器和 GRE VS L2 转发。每个路由器可以有多个 WAN 链接。每个链接都可以有自己的 WCCP 服务组。

除非设备管理 UDP 流量以及 TCP 流量，否则流量调整无法有效。如果需要流量调整，建议使用第二个服务组（每个 WAN 链接都有 UDP 服务组）。

注册和状态更新

WCCP 客户端（设备）使用 UDP 端口 2048 向路由器注册自己，并协商必须向路由器发送哪些流量，以及必须为此流量使用哪些 WCCP 功能。设备对此流量进行操作，并将生成的流量转发到原始端点节点。通过 WCCP 注册过程和检测信号协议跟踪设备的状态。设备首先通过 WCCP 控制通道（UDP 端口 2048）与路由器联系，设备和路由器分别使用名为“Hhere_I_Am”和“I_See_YU”的数据包交换信息。默认情况下，此过程每 10 秒重复一次。如果路由器在其中三个时间间隔内无法接收来自设备的消息，则会认为该设备发生故障，并停止向其转发流量，直到重新建立联系人为止。

服务和服务组

使用同一路由器的不同设备可以提供不同的服务。为了跟踪哪些服务分配给哪些设备，WCCP 协议使用服务组标识符(一个字节整数)。当设备向路由器注册自身时，它也包括服务组号。

- 单个设备可以支持多个服务组。
- 单个路由器可以支持多个服务组。
- 单个设备可以对多个路由器使用同一个服务组。
- 单个路由器可以对多个设备使用同一个服务组。对于 SD-WAN 设备，WCCP 群集模式下支持多台设备，而 WCCP 模式下支持单台设备。
- 每个设备为每个方向和每个服务组独立指定一个“返回类型”（L2 或 GRE）。SD-WAN 4000/5000 设备始终为两个方向指定相同的返回类型。其他 SD-WAN 设备允许退货类型不同。

图 2. 为不同的服务使用不同的 WCCP 服务组

多个服务组 可以在同一设备上与 WCCP 一起使用。例如，设备可以从一个 WAN 链接接接收服务组 51 流量，从另一个 WAN 链接接接收服务组 62 流量。该设备还支持多个路由器。所有路由器都使用相同的服务组还是不同的路由器使用不同的服务组是无动于衷的。

服务组跟踪。如果数据包到达一个服务组，则相同连接的输出数据包将在同一服务组上发送。如果数据包到达多个服务组上的同一连接，则输出数据包将跟踪该连接的最近查看的服务组。

高可用性行为

当 WCCP 在高可用性模式下使用时，主设备会在与路由器联系时发送自己的 apA 或 apB 管理 IP 地址，而不是高可用性对的虚拟地址。如果发生故障转移，新的主设备会自动与路由器联系，重新建立 WCCP 通道。在大多数情况下，WCCP 超时期限和高可用性故障转移时间重叠。因此，网络中断小于两个延迟的总和。

标准 WCCP 只允许 WCCP 服务组中的单个设备。如果新设备尝试与路由器联系，则会发现另一台设备正在处理服务组，并且新设备会设置警报。它会定期检查以确定该服务组是否与其他设备处于活动状态，并且新设备在其他设备变为非活动状态时处理该服务组。WCCP 群集允许每个服务组多台设备。

部署拓扑

下图显示了一个简单的 WCCP 部署, 适用于 L2 或 GRE. 流量端口 (1/1) 直接连接到专用路由器端口 (Gig 4/12)。

图 3. WCCP 简单部署

在此示例中，SD-WAN 4000/5000 以单臂模式部署，流量端口 (1/1) 和管理端口 (0/1) 各连接到自己的专用路由器端口。

在路由器上，WCCP 在 WAN 和 LAN 端口上的语句中配置了相同的 IP WCCP 重定向。使用了两个服务组，即 71 和 72。服务组 71 用于 TCP 流量，服务组 72 用于 UDP 流量。设备不会加速 UDP 流量，但可以对其应用流量调整策略。

> 注意：WCCP 规范不允许转发 TCP 和 UDP 以外的协议，因此 ICMP 和 GRE 等协议始终绕过设备。

WCCP 群集

SD-WAN 设备支持 WCCP 群集，这使您的路由器能够负载平衡多台设备之间的流量。有关将 SD-WAN 设备部署为群集的更多信息，请参阅WCCP 群集。

WCCP 规范

有关 WCCP 的详细信息，请参阅 Web 缓存通信协议 V2，修订版本 1http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00。

> 注意
>
> 在 WCCP 中部署 SD-WAN 以实现交换机冗余时，我们可以将交换机 2 连接到 apB。为 apB 创建一个不同的 SG，给它一个低于 apA SG 的优先级。如果 apA 更高的 SG 已启动，则将用于重定向。如果下降，将使用 apB SG。请注意，apA 和 apB 需要位于不同的子网中。

WCCP 模式（非聚集）

April 23, 2021

WCCP 模式只允许 WCCP 服务组中的单个设备。如果新设备尝试与路由器联系，则会发现另一台设备正在处理服务组，并且新设备会设置警报。它会定期检查以确定该服务组是否与其他设备处于活动状态，并且新设备在其他设备变为非活动状态时处理该服务组。

> 注意：
> WCCP 群集允许每个服务组多个设备。

局限性和最佳做法

以下是（非群集）WCCP 模式的限制和最佳实践：

- 在具有多个加速对的设备上，给定 WCCP 服务组的所有流量必须到达同一个加速对。
- 请勿在同一设备上混合内联流量和 WCCP 流量。设备不强制执行此指南，但违反该指南可能会导致加速方面的困难。（WCCP 和虚拟内联模式可以混合使用，但前提是 WCCP 和虚拟内联流量来自不同的路由器。）
- 对于具有单个 WAN 路由器的站点，在内联模式不实际时使用 WCCP。
- 每个服务组只支持一个设备。如果多个设备尝试连接到具有相同服务组的同一路由器，协商将仅针对第一个设备成功。
- 对于具有由同一设备提供服务的多个 WAN 路由器的站点，WCCP 可用于支持一个、部分或全部 WAN 路由器。其他路由器可以使用虚拟内联模式。

路由器支持 WCCP

为 WCCP 配置路由器非常简单。WCCP 版本 2 的支持包括在所有现代路由器, 已被添加到思科 IOS 版本 12.0 (11) S 和 12.1 (3) T. 最佳路由器配置策略取决于路由器和交换机的特性。流量成形需要两个服务组。

如果路由器支持反向路径转发，则必须在所有端口上禁用它，因为它可能会将 WCCP 流量与欺骗流量混淆。此功能可以在较新的思科路由器，如思科 7600 中找到。

路由器配置策略

有两种基本方法可以将流量从路由器重定向到设备：

仅在 **WAN** 端口上，添加“WCCP 重定向到”语句和“WCCP 重定向出”语句。
在路由器上的每个端口上，除了连接到设备的端口外，添加一个“WCCP 重定向”语句。

第一种方法仅将 WAN 流量重定向到设备，而第二种方法将所有路由器流量重定向到设备，无论是否与 WAN 相关。在具有多个 LAN 端口和大量 LAN 到 LAN 流量的路由器上，将所有流量发送到设备可能会使其 LAN 段过载，并使设备承受这种不必要的负载。如果使用 GRE, 不必要的流量也可以加载路由器.

在某些路由器上，“重定向进入”路径更快，并且在路由器 CPU 上的负载比“重定向出”路径更少。如有必要，这可以通过在路由器上的直接实验来确定：尝试两种重定向方法在满网络负载下查看哪种方法提供了最高的传输速率。

某些路由器和支持 WCCP 的交换机不支持“WCCP 重定向出”，因此必须使用第二种方法。为了避免路由器过载，最佳做法是避免通过设备重定向大量路由器端口，可能通过使用两个路由器，一个用于 WAN 路由，另一个用于 LAN 到 LAN 路由。

一般来说，方法 1 更简单，而方法 2 可能提供更高的性能。

流量成形和 **WCCP**

服务组可以是 TCP 或 UDP，但不能同时使用。要使流量成形程序有效，这两种 WAN 流量都必须通过设备。因此：

加速需要一个服务组，用于 TCP 流量。
流量调整需要两个服务组，一个用于 TCP 流量，另一个用于 UDP 流量。两者之间的区别是在设备上配置的，路由器接受此配置。

配置路由器

设备自动协商 WCCP-GRE 或 WCCP-L2。主要选择是 单播操作（其中设备配置了每个路由器的 IP 地址）或 多播操作（其中设备和路由器都配置了多播地址）。

正常（单播）操作—对于正常操作，过程是声明 WCCP 版本 2 和路由器的 WCCP 组 ID 作为一个整体，然后在每个 WAN 接口上启用重定向。以下是思科 IOS 示例：

```
config term
ip wccp version 2
! We will configure the appliance to use group 51 for TCP and 52 for
    UDP.
ip wccp 51
ip wccp 52

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
```



```
! source reachable”  statement), delete or comment out the statement:
! ip verify unicast source reachable-via any
! Repeat on all ports.

ip wccp 51 redirect out
ip wccp 51 redirect in
ip wccp 52 redirect out
ip wccp 52 redirect in

! If the appliance is inline with one of the router interfaces
! (NOT SUPPORTED), add the following line for that interface
! to prevent loops:
ip wccp redirect exclude in
^Z
<!--NeedCopy-->
```

如果多个路由器要使用同一个设备，则每个路由器的配置如上所示，使用相同的服务组或不同的服务组。

多播操作—为设备和每个路由器提供多播地址时，配置与正常操作略有不同。以下是思科 IOS 示例：

```
config term
ip wccp version 2
ip wccp 51 group-address 225.0.0.1

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable”  statement), delete or comment out the statement:
! ip verify unicast source reachable-via any

ip wccp 51 redirect out
ip wccp 51 redirect in
!
! The following line is needed only on the interface facing the other
    router,
! if there is another router participating in this service group.
ip wccp 51 group-listen

!If the appliance is inline with one of the router interfaces,
!(which is supported but not recommended), add
!the following line for that interface to prevent loops:
ip wccp redirect exclude in
^Z
<!--NeedCopy-->
```

SD-WAN 设备上 WCCP 模式的基本配置过程

对于大多数站点，您可以使用以下过程在设备上配置 WCCP 模式。该过程将多个参数设置为合理的默认值。高级部署可能需要将这些参数设置为其他值。例如，如果路由器已使用 WCCP 服务组 51，则需要为设备使用不同的值。

要在设备上配置 WCCP 模式，请执行以下操作：

1. 在配置：设备设置：WCCP 页面上。
2. 如果尚未定义服务组，则会显示“选择模式”页面。选项是单 SD-WAN 和群集（多 SD-WAN）。选择单个 SD-WAN。你被带到 WCCP 页面。
   注意：模式标签具有误导性。“单 SD-WAN”模式也用于 SD-WAN 高可用性对。
3. 如果未启用 WCCP 模式，请单击 启用。
4. 单击 添加服务组。
5. 默认接口 (apA)、协议 (TCP)、WCCP 优先级 (0)、路由器通信 (单播)、(密码空白) 和生存时间 (1) 值通常不必更改您创建的第一个服务组，但如果这样做，请在提供的字段中键入新值。
6. 在 路由器寻址 字段（如果您使用的是单播）或 多播地址 字段（如果您使用的是多播）中，键入路由器的 IP 地址。将 IP 用于 WCCP 与设备进行通信的路由器端口。
7. 如果多个路由器正在使用 WCCP 与此设备进行通信，请立即添加更多路由器。
8. 如果您的路由器有特殊要求，请相应地设置路由器转发（自动/GRE/Level-2）、路由器数据包返回（自动/GRE/Level-2）和路由器分配（掩码/哈希）字段。对于大多数路由器，默认值会产生最佳结果。
9. 单击添加。
10. 重复上述步骤为 UDP 流量创建另一个服务组（例如，服务组 ID 52 和协议 UDP）。
11. 转到监视：设备性能：WCCP 页面。状态 字段应在 60 秒内更改为“已连接”。
12. 通过链接发送流量，并在“连接”页面上验证连接是否已到达并正在加速。

WCCP 服务组配置详细信息

在服务组中，WCCP 路由器和 SD-WAN 设备（WCCP 术语中的“WCCP Cache”）协商通信属性（功能）。路由器在“我看到你”消息中宣传其功能。通信属性是：

- 转发方法：GRE 或 Level-2
- 数据包返回方法（仅限多播）：GRE 或 2 级
- 赋值方法：散列或掩码
- 密码（默认为无）

如果设备检测到其属性与路由器属性之间的不兼容，则会触发警报。由于服务组的特定属性（如 GRE 或级别 2），设备可能不兼容。在多播服务组中，当“自动”选择选择连接了特定路由器的特定属性时，可以触发警报，但该属性与后续路由器不兼容。

以下是 SD-WAN 设备中的通信属性的基本规则。

对于路由器转发：

- 选择“自动”时，首选项为级别 2，因为它对路由器和设备都更有效。如果路由器支持，并且路由器与设备位于同一子网上，则协商级别 2。
- 如果选择了“自动”，则单播服务组中的路由器可以协商不同的方法。
- 多播服务组中的路由器必须使用相同的方法，无论是强制使用“GRE”或“级别 2”，还是使用“Auto”（由服务组中的第一个路由器确定）进行连接。

- 对于不兼容，警报宣布路由器“具有不兼容的路由器转发。”

对于路由器分配：

- 默认值为哈希值。
- 当选择“自动”时，将与路由器协商模式。
- 服务组中的所有路由器必须支持相同的分配方法（哈希或掩码）。
- 对于任何服务组，如果此属性配置为“Auto”，设备会在连接第一个路由器时选择“哈希”或“掩码”。如果路由器支持，则选择“哈希”。否则，“蒙版”被选中。通过手动选择服务组中所有路由器通用的方法，可以最大限度地减少后续路由器与自动选择的方法不兼容的问题。
- 对于不兼容，警报宣布路由器“具有不兼容的路由器分配方法”。
- 使用任何一种方法，服务组中的单个设备都会指示服务组中的所有路由器将所有 TCP 或 UDP 数据包引导到设备。路由器可以通过访问列表或选择要重定向到服务组的接口来修改此行为。

  对于掩码方法，设备协商“源 IP 地址”掩码。设备不提供选择“目标 IP 地址”或源或目标端口的机制。“源 IP 地址”掩码不具体标识任何特定的 IP 地址或范围。该协议不提供指定特定 IP 地址的方法。默认情况下，由于服务组中只有一个设备，因此使用一位掩码来节省路由器资源。（版本 6.0 使用了更大的掩模。）

对于密码：

- 如果路由器需要密码，则设备上定义的密码必须匹配。如果路由器不需要密码，则设备上的密码字段必须为空。

WCCP 测试和故障排除

使用 WCCP 时，设备提供不同的监视 WCCP 接口状态的方法，您的路由器也应该提供信息。

监视：设备性能：**WCCP** 页面—WCCP 页面报告 WCCP 链接的当前状态，并报告大多数问题。

日志条目—监视：设备性能：日志记录页面在每次建立或丢失 WCCP 模式时显示一个新条目。

图 1. WCCP 日志条目（格式随发布而有所不同）

路由器状态—在路由器上，“show ip WCCP”命令显示 WCCP 链接的状态：

```
Router>enable
Password:
Router#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  172.16.2.4
        Protocol Version:                   2.0

    Service Identifier: 51
        Number of Cache Engines:            0
        Number of routers:                  0
        Total Packets Redirected:           19951
```



```
        Redirect access-list:                -none-
        Total Packets Denied Redirect:       0
        Total Packets Unassigned:            0
        Group access-list:                   -none-
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
<!--NeedCopy-->
```

验证 **WCCP** 模式

您可以从 SD-WAN GUI 监视 WCCP 配置。

监视 WCCP 配置

1. 导航到 “监视” **>** “设备性能” **>** “**WCCP** 页面。
2. 选择一个缓存，然后单击 获取信息。缓存状态页面显示 WCCP 配置，如下图所示。
3. 启动应通过 SD-WAN 设备转发的流量，并在“监视 **>** “优化” **>** “连接”页面上监视连接。
   - 如果连接显示在 加速连接 选项卡上，则表示一切正常工作的指示器。
   - 如果连接位于 未加速连接 选项卡上，请查看 详细信息 列。检测到的路由不对称消息意味着路由器上的 IP WCCP 重定向线之一丢失或出现错误，或者客户端-服务器和服务器-客户端流量采用不同的路径。
   - 如果没有显示连接，但设备报告已连接到路由器，并且 WCCP 监视页面没有显示任何错误，则问题可能与路由器配置有关。

WCCP 群集

December 15, 2022

通过 WCCP 群集功能，您可以将多个 SD-WAN 设备分配给相同的链接，从而使加速容量倍增。您最多可以集群 32 台相同的设备，容量可达 32 倍。因为它使用 WCCP 2.0 标准，WCCP 群集适用于大多数路由器和一些智能交换机，很可能包括您已经使用的交换机。

因为它使用分散式协议，WCCP 群集允许随意添加或删除 SD-WAN 设备。如果设备发生故障，则其流量将重新路由到存在的设备。

SD-WAN 高可用性（使用两台设备来提供单台设备的性能）与 SD-WAN 高可用性不同，作为 WCCP 群集部署的相同设备的性能是单台设备的两倍，既提供冗余又提高了性能。

除了随着站点需求的增加添加更多设备外，您还可以使用 Citrix 的“随增长付费”功能通过许可证升级提高设备的功能。

建议用于管理 WCCP 群集时使用 CitrixCommand Center。下图显示了 WCCP 模式下 SD-WAN 设备群集的基本网络，由 Citrix Command Center 管理。

图 1. 使用 Citrix Command Center 管理的 SD-WAN 群集

负载平衡 **WCCP** 集群

WCCP 协议在称为集群的容错负载平衡阵列中支持多达 32 台设备。在下面的示例中，除了 IP 地址之外，三个相同的设备（相同型号、相同的软件版本）以相同的方式连接并配置相同。使用具有相同路由器的相同服务组的设备可以成为负载平衡的 WCCP 群集。当新设备向路由器注册自身时，它可以加入现有设备池并接收其所占的流量份额。如果设备离开网络（如没有检测信号所示），则会重新平衡群集，以便仅使用剩余设备。

图 2. 一个具有三个设备的负载均衡的 WCCP 集群

群集中的一个设备被选为指定缓存，并控制群集中设备的负载平衡行为。指定的缓存是 IP 地址最低的设备。由于设备具有相同的配置，所以哪一个是指定的缓存并不重要。如果当前指定的缓存脱机，则不同的设备将成为指定的缓存。

指定的缓存确定负载平衡流量的分配方式，并通知路由器这些决策。路由器与集群的所有成员共享信息，因此即使指定的缓存脱机，群集也可以运行。

> 注意：按照正常配置，SD-WAN 4000/5000 设备显示为两个 WCCP 缓存到路由器中。

负载均衡算法

WCCP 中的负载平衡是静态的，除非设备进入或离开群集，这会导致群集在其当前成员之间重新平衡。

WCCP 标准支持基于掩码或散列的负载平衡。例如，SD-WAN WCCP 群集仅使用掩码方法，使用的掩码为 1-6 位的 32 位 IP 地址。这些地址位可以是非连续的。将蒙版时产生相同结果的所有地址发送到同一设备。负载平衡的有效性取决于选择合适的掩码值：如果选择较差的掩码可能会导致负载平衡不佳，甚至没有任何流量，所有流量都发送到单个设备。

部署拓扑

根据您的网络拓扑，您可以使用单个路由器或多个路由器部署 WCCP 群集。无论是连接到单个路由器还是多个路由器，群集中的每个设备都必须与正在使用的所有路由器相同连接。

单路由器部署

在下图中，三个 SD-WAN 设备可加速数据中心的 200 Mbps WAN。该网站支持 750 个虚拟应用程序用户。

如上所示SD-WAN 数据表，SD-WAN 3000-100 可以支持 100 Mbps 和 400 用户，因此一对这些设备支持 200 Mbps 和 800 用户，这满足了数据中心对 200 Mbps 链路和 750 的要求用户。

但是，为了容错，如果一台设备发生故障，WCCP 群集应继续运行，而不会出现过载。当计算需要两个时，可以通过使用三个设备来实现这一点。这就是所谓的 N+1 规则。

故障是一个不寻常的事件，所以通常所有三个设备都在运行。在这种情况下，每个设备只支持 67 Mbps 和 250 个用户，留下了大量的余量，并且充分利用集群的 CPU 功率是单个设备的三倍和压缩历史记录的三倍这一事实。

如果没有 WCCP 群集，那么多的容量和容错将需要一对 SD-WAN 4000-500 设备处于高可用性模式。一次只有其中一个设备处于活动状态。

多路由器部署

使用多个 WAN 路由器类似于使用单个 WAN 路由器。如果上一个示例被更改为包括两个 100 Mbps 的链接而不是一个 200 Mbps 的链接，则拓扑会更改，但计算不会更改。

限制

在 WCCP 群集中配置设备有以下限制：

- 群集中的所有设备必须是同一型号并使用相同的软件版本。
- 群集内设备之间的参数同步不是自动的。使用 Command Center 将设备作为一个组进行管理。
- SD-WAN 流量成形不是有效的，因为它依赖于将整个链路作为一个单元进行控制，并且没有一个设备能够做到这一点。可以改用路由器 QoS。
- 基于 WCCP 的负载平衡算法不会随负载动态变化，因此实现良好的负载平衡需要进行一些调整。
- 不支持缓存分配的哈希方法。掩码分配是支持的方法。
- 虽然 WCCP 标准允许蒙版长度为 1-7 位，但设备支持 1-6 位的蒙版。
- 不支持多播服务组。仅支持单播服务组。
- 使用相同服务组对的所有路由器必须支持相同的转发方法（GRE 或 L2）。
- 与路由器协商的转发和返回方法必须匹配: 两者必须是 GRE 或两者都必须是 L2. 一些路由器在两个方向上不支持 L2，导致“路由器的前进或返回或分配功能不匹配”的错误。“在这种情况下，服务组必须配置为 GRE。
- SD-WAN VPX 不支持 WCCP 群集。
- 设备仅支持（并协商）未加权（等于）缓存分配。不支持加权分配。
- 某些较旧的设备（如 SD-WAN 700）不支持 WCCP 群集。
- （仅限 SD-WAN 4000/5000）L2 模式下，每个接口需要两个加速器实例。每个设备支持三个接口（然后仅支持具有六个或更多加速器实例的设备）。
- （仅限 SD-WAN 4000/5000）来自路由器的 WCCP 控制数据包必须与服务组的设备上配置的路由器 IP 地址之一匹配。实际上，应使用路由器的 IP 地址连接到设备的接口。无法使用路由器的环回 IP。

部署工作表和群集限制

在下面的工作表中，您可以计算安装所需的设备数量和建议的掩码字段大小。建议的蒙版大小比安装的最小蒙版大小大 1-2 位。

参数	值	备注

使用的设备型号		—
支持的 Citrix Virtual Apps and Desktops 每台设备	Uspec =	来自数据手册
WAN 链接上的 Citrix Virtual Apps and Desktops 用户	Uwan =	—
用户过载系数	Uoverload = Uwan/Uspec =	—
每台设备支持的 BW	BWspec =	来自数据手册
广域网连接路	BWwan =	—
BW 过载系数	BWoverload = BWwan/BWspec =	—
所需设备数量	N = max(Uoverload, BWoverload) +1 =	包括一个备用品
		—
存储桶的最小数量	Bmin = N，向上四舍五入 2 =	—
如果使用 SD-WAN 4000 或 5000，	Bmin = 2N，四舍五入到 2 =	—
建议值	如果 Bmin <= 16，则 B = 4 Bmin，否则 2 Bmin =	—
地址掩码中的“一”位数	M = log2(B)	如果 B=16，M=4。

掩码值：掩码值是一个 32 位地址掩码，其中多个“一”位等于前面提供的工作表中的 M。通常，这些位可以是远程站点使用的 WAN 子网掩码中的最小有效位。如果远程站点的蒙版不同，请使用中位数蒙版。（例如：对于 /24 子网，子网的最小有效位为 0x00 00 nn 00。要设置为一的位数为 log2（掩码大小）：如果掩码大小为 16，请将 4 位设置为一。因此，对于掩码大小为 16 和 /24 子网，请将掩码值设置为 0x00 00 0f 00。）

仅当所选子网字段在流量中均匀分布时，上述准则才起作用，也就是说，掩码选择的每个地址位对于一半远程主机，对于另一半则是零。否则，负载平衡会受损。这种均匀分布可能只适用于网络字段中的几位（只有 2 位）。如果您的网络是这样，而不是掩盖子网字段的违规区域中的位，而是将这些位置置换到具有 50/50 属性的主机地址字段的一部分。例如，如果一个 /24 子网中只有三个子网位具有 50/50 属性，并且您正在使用四个掩码位，则 0x00 07 10 的掩码可避免 0x00 00 0800 的违规位，并将其置换为 0x00 00 00 00 10，地址字段的一部分可能具有 50/50 属性，如果远程子网通常每个至少使用 32 个 IP 地址。

参数	值	备注
最终遮罩值		—

加速桥	通常 apA
WAN 服务组	路由器上尚未使用的服务组 (51-255)
LAN 服务组	另一个未使用的服务组
路由器 IP 地址	面向设备的端口上路由器接口的 IP 地址
WCCP 协议（通常为“自动”）	—
DC 算法	如果您只有两台设备或正在使用 HSRP 或 GSLB 等动态负载平衡，请使用“确定性”。否则，请使用“破坏性最小”。

在 WCCP 群集中配置设备有以下限制：

- 群集中的所有设备必须是同一型号并使用相同的软件版本。
- 群集内设备之间的参数同步不是自动的。使用 Command Center 将设备作为一个组进行管理。
- SD-WAN 流量成形不是有效的，因为它依赖于将整个链路作为一个单元进行控制，并且没有一个设备能够做到这一点。可以改用路由器 QoS。
- 基于 WCCP 的负载平衡算法不会随负载动态变化，因此实现良好的负载平衡需要进行一些调整。
- 不支持缓存分配的哈希方法。掩码分配是支持的方法。
- 虽然 WCCP 标准允许蒙版长度为 1-7 位，但设备支持 1-6 位的蒙版。
- 不支持多播服务组；仅支持单播服务组。
- 使用相同服务组对的所有路由器必须支持相同的转发方法（GRE 或 L2）。
- 与路由器协商的转发和返回方法必须匹配: 两者必须是 GRE 或两者都必须是 L2. 一些路由器在两个方向上不支持 L2，导致“路由器的前进或返回或分配功能不匹配”的错误。“在这种情况下，服务组必须配置为 GRE。
- SD-WAN VPX 不支持 WCCP 群集。
- 设备仅支持（并协商）未加权（等于）缓存分配。不支持加权分配。
- 某些较旧的设备（如 SD-WAN 700）不支持 WCCP 群集。
- （仅限 SD-WAN WANOP 4000/5000）L2 模式下，每个接口需要两个加速器实例。每个设备最多支持三个接口（然后支持具有六个或更多加速器实例的设备）。
- （仅限 SD-WAN 4000/5000）来自路由器的 WCCP 控制数据包必须与服务组的设备上配置的路由器 IP 地址之一匹配。实际上，应使用路由器的 IP 地址连接到设备的接口。无法使用路由器的环回 IP。

测试和故障排除

监视 > 设备 > 应用程序性能 > **WCCP** 页面不仅显示本地设备的当前状态，而且显示已加入群集的所有其他设备的当前状态。选择一个 WCCP 缓存，然后单击 获取信息。

缓存状态”选项卡 显示本地设备的状态。当一切顺利时，状态是“25：有任务”。您必须手动刷新页面以监视状态的更改。如果设备在超时期限内未达到“25: 已分配”状态，则会显示其他信息性状态消息。

当您单击 服务组或路由器 选项卡时，将显示其他信息。

群集摘要”选项卡 显示有关整个 WCCP 群集的信息。作为 WCCP 协议的副作用，群集的每个成员都有关于所有其他成员的信息，因此可以从群集中的任何设备监视此信息。

您的路由器还可以提供状态信息。请参阅您的路由器文档。

配置 **WCCP** 群集

在完成部署拓扑、考虑所有限制并填写部署工作表后，即可在 WCCP 群集中部署设备。要配置 WCCP 群集，您需要执行以下任务：

- 配置 NetScaler 实例
- 配置路由器
- 配置设备

虚拟内联模式

April 23, 2021

> 注意：
>
> 仅当内联模式和 WCCP 模式都不切实际时才使用虚拟内联模式。请勿在同一设备内混合内联模式和虚拟内联模式。但是，您可以在同一设备中混合虚拟内联模式和 WCCP 模式。Citrix 不建议使用不支持运行状况监视的路由器进行虚拟内联模式。

在虚拟内联模式下，路由器使用基于策略的路由 (PBR) 规则将传入和传出 WAN 流量重定向到设备以进行加速，而设备将处理的数据包转发回路由器。几乎所有的配置任务都在路由器上执行。设备上唯一要配置的是转发方法，建议使用默认方法。

与 WCCP 一样，虚拟内联部署不需要重新线路连接，也不需要停机，并且它为具有两个或更多 WAN 链接的部署中遇到的非对称路由问题提供了解决方案。与 WCCP 不同，它不包含内置状态监视或运行状况检查，因此难以进行故障排除。因此，WCCP 是推荐的模式，只有当内联模式和 WCCP 模式都不切实际时，才建议使用虚拟内联模式。

示例

下图显示了一个简单的网络，在该网络中，目的地或从远程站点接收的所有流量都将重定向到设备。在此示例中，本地站点和远程站点都使用虚拟内联模式。

图 1. 虚拟内联示例

以下是本示例中网络的一些配置详细信息：

- 端点系统的网关设置为本地路由器（这不是虚拟内联模式唯一的）。
- 每个路由器都配置为将传入和传出 WAN 流量重定向到本地设备。
- 每个设备处理从其本地路由器接收的流量，并将其转发回路由器。
- 路由器上配置的 PBR 规则通过允许数据包只进行一次往返设备，从而阻止路由循环。设备转发回路由器的数据包将发送到其原始（本地或远程）目标。
- 每个设备都将其默认 Gateway 设置为本地路由器的地址，如往常一样（在 配置**:** 网络适配器 页面上）。将数据包转发回路由器的选项是“返回到以太网发件人”和“发送到网关”。

在设备上配置数据包转发

April 23, 2021

虚拟内联模式提供两种数据包转发选项：

返回到以太网发件人（默认）-此模式允许多个路由器共享一台设备。设备将虚拟内联输出数据包转发回其来源的位置，如传入数据包的以太网地址所示。如果两个路由器共享一台设备，则每个路由器都会返回自己的流量，但不会返回来自另一台路由器的流量。此模式也适用于单个路由器。

发送到 **Gateway**（不推荐）-在此模式下，虚拟内联输出数据包将转发到默认网关进行传递，即使这些数据包是针对本地子网上的主机也是如此。此选项通常比“返回以太网发件人”选项不太理想，因为它会为路由结构添加一个容易忘记的复杂元素。

要指定数据包转发选项—在“配置：优化规则：优化规则：优化”页面上，在“虚拟内联”旁边，选择“返回以太网发件人”或“发送到网关”。

路由器配置

April 23, 2021

路由器在支持虚拟内联模式时有三个任务：

1. 它必须将传入和传出 WAN 流量转发到 SD-WAN 设备。
2. 它必须将 SD-WAN 流量转发到其目的地（WAN 或 LAN）。
3. 它必须监视设备的运行状况，以便在设备出现故障时可以绕过设备。

基于策略的规则

在虚拟内联模式下，如果路由规则不区分设备已转发的数据包和未转发的数据包，则数据包转发方法可以创建路由循环。您可以使用任何区分的方法。

典型的方法是将路由器的以太网端口之一专用于设备，并创建基于数据包到达的以太网端口的路由规则。到达专用于设备的接口上的数据包永远不会转发回设备，但到达任何其他接口上的数据包都可以。

基本路由算法是：

- 请勿将数据包从设备转发回设备。
- 如果数据包从 WAN 到达，请将其转发到设备。
- 如果数据包发送到 WAN，请转发到设备。
- 请勿将 LAN 到 LAN 的流量转发到设备。
- 除非所有 WAN 流量通过设备，否则流量调整无法有效。

> 注意：在考虑路由选项时，请记住，返回数据（而不仅仅是传出数据）必须在设备中流动。例如，将设备放在本地子网上并将其指定为本地系统的默认路由器在虚拟内联部署中不起作用。传出数据将通过设备流动，但传入数据会绕过它。要在不重新配置路由器的情况下强制使用数据，请使用内联模式。

运行状况监视

如果设备发生故障，则不应将数据路由到设备。默认情况下，基于思科策略的路由不进行运行状况监视。要启用运行状况监视，请定义规则以监视设备的可用性，并为“设置 ip 下一跃点”命令指定“验证可用性”选项。使用此配置时，如果设备不可用，则不会应用路由，并且会绕过设备。

重要提示：Citrix 建议仅在与运行状况监视一起使用时使用虚拟内联模式。许多支持基于策略的路由器不支持运行状况检查。健康监测功能相对较新。它成为在思科 IOS 版本 12.3 (4) T.

以下是用于监视设备可用性的规则示例：

“‘ pre codeblock
!- Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachabilit y ! rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now

```
此规则定期以 192.168.1.200 的方式对设备进行调整。您可以针对 123 进行测试，以查看单位是否向上。

## 路由示例

以下示例说明了为中所示的本地和远程站点配置 Cisco 路由器[虚拟内联示例](/zh-cn/citrix-sd-wan-wanop/11-1/cb-deployment-modes-con/br-adv-virt-inline-mode-con.html)。为了说明运行状况监视，本地站点的配置包括运行状况监视，但远程站点的配置不包括运行状况监视。

注意：本地站点的配置假定已配置 ping 监视器。

```



```
这 些 示 例 符 合 思 科 IOS CLI。 它 们 可 能 不 适 用 于 来 自 其 他 供 应 商 的 路 由 器。

本 地 站 点， 启 用 运 行 状 况 检 查：

``` pre codeblock
!
! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
!- Now set the appliance as the next hop, if it' s up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
<!--NeedCopy-->
```

远程站点（无运行状况检查）：

“‘ pre codeblock

! This example does not use health-checking.

! Remember, health-checking is always recommended,

! so this is a configuration of last resort.

!

!


```

ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!_

```
上述每个示例都将访问列表应用于路径图，并将路径图附加到界面。访问列表标识来自一个加速站点并在另一个站点终止的所有流量（源 IP 为 10.10.10.0/24，目的地为 20.20.20.0/24，反之亦然）。有关访问列表和路由图的详细信息，请参阅路由器的文档。

此配置将所有匹配的 IP 流量重定向到设备。如果您只想重定向 TCP 流量，则可以按如下方式更改访问列表配置（此处仅显示远程端的配置）：

```pre codeblock
!
 ip access-list extended client_side
 permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
 ip access-list extended wan_side
```


```

```
 permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
<!--NeedCopy-->
```

请注意，对于访问列表，不使用普通掩码。改为使用通配符掩码。请注意，当以二进制读取通配符掩码时，“1”被认为是“不关心”位。

适用于多 **WAN** 环境的虚拟内联

April 23, 2021

具有多个 WAN 链接的企业通常具有非对称路由策略，这似乎要求内联设备同时存放在两个位置。虚拟内联模式通过使用路由器配置通过设备发送所有 WAN 流量（无论使用何种 WAN 链接）来解决非对称路由问题。下图显示了一个简单的多 WAN 链路部署示例。

两个本地端路由器将流量重定向到本地设备。两个路由器的 FE 0/0 端口与设备位于相同的广播域中。本地设备必须使用默认的虚拟内联配置（返回到以太网发件人）。

图 1. 带有两个 WAN 路由器的虚拟内联模式

虚拟内联模式和高可用性

April 23, 2021

虚拟内联模式可用于高可用性（高可用性）配置。下图显示了一个简单的高可用性部署。在虚拟内联模式下，一对设备充当一个虚拟设备。对于高可用性对，路由器配置与单个设备的路由器配置相同，只是在路由器配置表中使用了高可用性对的虚拟 IP 地址，而不是单个设备的 IP 地址。在此示例中，本地设备必须使用默认的虚拟内联配置（返回到以太网发件人）。

图 1. 高可用性示例

监视和故障排除

April 23, 2021

在虚拟内联模式下，与 WCCP 模式不同，设备不提供特定于虚拟内联的监视。要对虚拟内联部署进行故障排除，请登录设备并使用“控制面板”页面验证流量是否流入和流出设备。流量转发失败通常是由路由器配置中的错误引起的。

如果“监视：使用情况”或“监视：连接”页面显示正在转发流量，但没有发生加速（假设已在 WAN 链接的另一端安装了设备），请检查以确保传入 WAN 流量和传出 WAN 流量都被转发到设备。如果只转发一个方向，则无法进行加速。

要测试运行状况检查，请关闭设备的电源。运行状况检查算法超时后，路由器应停止转发流量。

组模式

April 23, 2021

在组模式下，两个或多个设备将成为单个虚拟设备。这种模式是解决非对称路由问题的一种解决方案，非对称路由被定义为给定连接中的某些数据包通过给定设备但其他数据包不通过的任何情况。设备体系结构的一个限制是，除非给定连接中的所有数据包通过相同的两个设备，否则无法进行加速。组模式克服了此限制。

组模式可以与多个或冗余链接一起使用，而无需重新配置路由器。

> 注意
>
> SD-WAN 4000 或 5000 设备上不支持组模式。

组模式仅适用于 WAN 链接一侧的设备；本地设备既不知道也不关心远程设备是否使用组模式。

组模式使用检测信号机制验证组的其他成员是否处于活动状态。数据包仅转发给活动的组成员。

避免非对称路由是使用组模式的主要原因，但组模式并不是唯一可用于此目的的方法。如果您决定它是环境的最佳方法，则可以通过设置几个参数来启用它。如果用于确定哪个设备负责特定连接的默认机制不能提供最佳加速，则可以更改转发规则。

图 1. 带冗余链接的组模式

图 2. 带有可能非对称路由的非冗余链路的组模式

图 3. 附近校园的群组模式

何时使用组模式

April 23, 2021

在以下一组情况下使用组模式：

- 您有多个 WAN 链接。
- 存在不对称路由的可能性（给定连接上的数据包可能通过任何一个链接传输）。
- 组模式似乎比使用单个设备的替代方案更简单，更实用。

替代办法是：

- WCCP 模式，通过 WCCP 协议将来自两个或多个链接的流量通过 WAN 路由器发送到同一设备。
- 虚拟内联模式，您的路由器通过同一设备（或高可用性对）从两个或多个链接发送流量。

- 多个桥梁，其中每个链路通过同一设备中的不同加速桥梁。
- LAN 级聚合，将设备（或高可用性对）置于更靠近 LAN 的位置，在 WAN 流量被拆分为两个或多个路径之前。

组模式的工作原理

April 23, 2021

在组模式下，属于组的设备各自拥有组的一部分连接的所有权。如果给定设备是连接的所有者，则该设备将做出有关该连接的所有加速决策，并负责压缩、流控制、数据包重新传输等。

如果某个设备收到其不是所有者的连接的数据包，则该设备将数据包转发给该所有者的设备。所有者检查数据包，做出适当的加速决策，并将任何输出数据包转发回非拥有的设备。此过程保留路由器所做的链路选择，同时允许所有的设备管理连接中的所有数据包。对于路由器，引进设备没有后果。路由器不需要以任何方式重新配置，设备也不需要了解路由机制。他们只是接受路由器的转发决定。

图 1. 组模式下的发送端流量

图 2. 组模式下的接收端流量

组模式有两种用户可选的失效模式，用于控制组成员在其中一个失败时彼此交互的方式。故障模式还决定发生故障的设备的旁路卡是打开（阻止通过设备的流量）还是保持关闭状态（允许流量通过）。失效模式如下：

继续加速**-** 如果组成员发生故障，其旁路卡将打开，且没有通信通过发生故障的设备。如果使用冗余链接，结果可能是故障转移。否则，链接无法访问。该组中的其他设备继续加速。通常的哈希算法处理更改的条件。（也就是说，使用旧的哈希算法，如果失败的单元被指示为所有者，则应用基于新的较小组的哈希算法。这样可以保留尽可能多的旧连接。）

请勿加速**-** 如果组成员发生故障，其旁路卡将关闭，允许流量在不加速的情况下通过。由于未加速路径引入了非对称路由，因此组中的其他成员在检测到故障时也会进入直通模式。

启用组模式

April 23, 2021

要启用组模式，请创建由两个或更多设备组成的组。一个设备只能是一个组的成员。组成员通过设备许可证中的 IP 地址和 SSL 公用名称进行标识。

所有组模式参数都位于“设置: 组模式”页面的“配置设置: 组模式”表中。

图 1. 组模式页面

启用组模式

1. 选择要用于组通信的地址。在“配置：高级部署：组模式”选项卡上的“组模式配置”表顶部，“成员 VIP”下的表单元格包含用于与其他组成员通信的端口的管理地址。使用（未标签）下拉菜单选择正确的地址（例如，要使用 Aux1 端口，请选择您分配给 Aux1 端口的 IP 地址）。然后，单击更改 VIP。
2. 至少添加一个组成员到列表。（支持三个或三个以上的组，但很少使用。）在“成员 VIP”列的下一个单元格中，键入其他设备用于组模式通信的端口的 IP 地址。
3. 在 SSL 公用名列中键入其他组成员的 SSL 公用名。SSL 公用名称列在其他设备的“配置：高级部署：高可用性”选项卡上。如果其他组成员是高可用性对，则列出的名称是主设备的 SSL 公用名称。

   > 注意：
   >
   > 如果本地设备不是高可用性对的一部分，则高可用性辅助 SSL 公用名称中的第一个单元为空。如果其他组成员是高可用性对，请指定高可用性中高可用性辅助设备的 SSL 公用名称可用性辅助 SSL 公用名称列。

4. 单击“添加”。
5. 对组中的任何其他设备或高可用性对重复步骤 2-4。
6. 组成员列表下的三个按钮被切换，因此每个按钮都被标记为与其当前设置相反：
   a) 顶部按钮读取“检测到 成员故障时不加速”或“在检测到成员故障时继续加速。“不加速…”设置始终有效且不会阻止流量，但是如果任何成员失败，其他组成员将进入旁路模式，这会导致完全丧失加速。使用“继续加速”选项，故障设备的桥接变成开路，并且链路失败。如果 WAN 路由器通过导致故障转移响应，则此选项适用。新连接以及属于幸存设备的开放连接将加速。
   b) 底部按钮现在应标记为禁用组模式。如果不是，请通过单击按钮启用组模式。
7. 刷新屏幕。页面顶部应列出组模式合作伙伴，但显示有关其状态的警告，因为它们尚未为组模式配置。例如，它可能表示找不到合作伙伴或正在运行不同的软件版本。
8. 与组的其他成员重复此过程。在启用组的最后一个成员后 20 秒内，“组模式状态”行应显示 NORMAL，其他列出的组模式成员应显示状态：“联机和配置: 正常”。

转发规则

April 23, 2021

默认情况下，组模式连接的 所有者 由源和目标 IP 地址的哈希设置。组中的每个设备使用相同的算法来确定哪个组成员拥有给定连接。此方法不需要配置。可以选择通过用户可设置的规则指定所有者。

由于组模式哈希与负载均衡器使用的哈希不完全相同，因此大约一半的流量倾向于转发到双设备组中的拥有设备。在最坏的情况下，转发会导致 LAN 端接口上的负载增加一倍，从而使实际 WAN 流量的设备峰值转发速率降低一半。

如果主要或 Aux1 以太网端口用于组成员之间的流量，则可以降低此速度损失。例如，如果您有一组两台设备，则可以使用以太网电缆连接两台设备的主端口，然后在每台设备的“组模式”页面上指定主端口。但是，如果组模式成员之间转发的流量最小化，则可实现最大性能。

所有者可以根据特定的 IP/端口规则进行设置。这些规则必须在组中的所有设备上相同。组中的每个成员都会验证其组模式配置是否与其他成员相同。如果不是所有的配置都相同，则没有任何成员设备进入组模式。

如果流量首先到达拥有连接的设备，则会加速并正常转发。如果它首先到达组中的另一个设备，它将通过 GRE 通道转发给其所有者，这将加速它并将其返回到原始设备以进行转发。因此，组模式保持路由器的链路选择不变。

使用基于 IP 的显式转发规则可以减少组模式转发的数量。这在主链接/备份链接方案中特别有用，其中每个链接处理特定范围的 IP 地址，但在另一个链接关闭时可充当备份。

图 1. 基于 IP 的所有者选择

转发规则可以确保组成员只处理其“自然”流量。在许多安装中，流量通常通过其正常链路路由，而且很少与另一个链路相交，这些规则可以大幅降低开销。

按顺序计算规则，从上到下，并使用第一个匹配规则。规则与可选 IP 地址/掩码对（与源地址和目标地址进行比较）以及可选端口范围进行匹配。

无论规则的顺序如何，如果伙伴设备不可用，无论规则是否匹配，都不会将流量转发到它。

例如，在下图中，成员 172.16.1.102 是进入或从其自身子网 (172.16.1.0/24) 的所有流量的所有者，而成员 172.16.0.184 是所有其他流量的所有者。

如果一个数据包到达单元 172.16.1.102，并且该数据包没有被发送到/从净值 172.16.1.0/24，则它被转发到 172.16.0.184。

但是，如果单元 172.16.0.184 失败，则单元 172.16.1.102 不再转发数据包。它尝试处理流量本身。通过单击“组模式”选项卡上的检测到成员故障时不加速，可以禁止此行为。

在具有主 WAN 链接和备份 WAN 链接的设置中，编写转发规则以将所有流量发送到主链接上的设备。如果主 WAN 链接失败，但主设备不失败，则 WAN 路由器故障转移并通过辅助链接发送流量。辅助链路上的设备将流量转发到主链路设备，加速将继续不受干扰。此配置在链路故障转移后维护加速连接。

图 2. 转发规则

监视和故障排除组模式

April 23, 2021

在组模式安装中应该检查两件事情：

- 两台设备已进入组模式，可在任何一台设备的“配置：高级部署：组模式”页面上确定。
- 分别通过禁用另一个设备并暂时断开其中一个链接的连接来确定组模式对的行为在其他成员发生故障时和其中一个链接失败时可以根据需要进行组模式对的行为。

自定义以太网端口

April 23, 2021

典型设备有四个以太网端口：两个加速桥接端口，称为加速对 *A*（apA.1 和 apA.2），带有旁路（故障到线）继设备，以及两个未加速的主板端口，称为主板端口和 Aux1。桥接端口提供加速，而主板端口有时用于辅助目的。大多数安装只使用桥接端口。

一些 SD-WAN 单元只有主板端口。在这种情况下，两个主板端口被桥接。

设备的用户界面可以通过 VLAN 或非 VLAN 网络访问。您可以将 VLAN 分配给设备的任何桥接端口或主板端口，以便进行管理。

图 1. 以太网端口

端口列表

端口命名如下：

以太网端口	名称
主板端口 1	主要（如果没有旁路卡，则为 apA.1）
主板端口 2	Auxiliary1 或 Aux1（如果没有旁路卡，则 apA.2）
桥 #1	加速对 A（apA，附有端口 apA.1 和 apA.2）
桥 #2	加速对 B（apB，端口 apB.1 和 apB.2）

表 1. 以太网端口名

高可用性模式的工作原理

April 23, 2021

在高可用性（高可用性）对中，一个设备是主设备，另一个设备是辅助设备。主服务器监视其自身和辅助服务器的状态。如果检测到问题，流量处理将失败转移到辅助设备。现有的 TCP 连接将被终止。为确保成功故障转移，这两个设备保持其配置同步。在 WCCP 模式的高可用性配置中，处理流量的设备保持与上游路由器的通信。

状态监视 启用高可用性后，主设备使用 VRRP 协议每秒向辅助设备发送一次检测信号。此外，主设备还监视其以太网端口的运营商状态。以前有效端口上的运营商丢失意味着连接丢失。

故障转移 如果主设备的检测信号发生故障，或者主设备在任何之前处于活动状态的以太网端口上出现载波丢失 5 秒钟的情况，则辅助设备将接管，成为主设备。当发生故障的设备重新启动时，它将成为辅助设备。新的主要宣布自己在网络上与 ARP 广播. 不使用 MAC 欺骗。在辅助设备上禁用以太网桥接，使主设备成为内联流量的唯一路径。两个设备上都禁止故障到线，以防止循环。

> 警告
>
> 以太网旁路功能在高可用性模式下被禁用。如果内联高可用性对中的两台设备断电，则连接将丢失。如果在停电期间需要 WAN 连接，则必须至少将一台设备连接到备用电源。
>
> 注意
>
> 高可用性对中的辅助设备有其中一个桥接端口，端口 apA.1，禁用以防止转发循环。如果设备具有双桥接，apB.1 也会被禁用。在单臂安装中，使用端口 apA.2。否则，启用高可用性时，辅助设备将无法访问。

主/辅助分配—如果两个设备都重新启动，则第一个完全初始化自身的设备将成为主设备。也就是说，这些设备没有分配角色，并且第一个可用的设备将作为主设备接管。用于 VRRP 检测信号的接口上具有最高 IP 地址的设备将用作断开器（如果两者同时可用）。

故障转移期间的连接终止—作为故障转移的副作用，加速和未加速的 TCP 连接都会终止。非 TCP 会话不受影响，除了由于主设备故障和故障转移到辅助设备之间的短时间（几秒钟）导致的延迟。用户体验打开连接的关闭，但他们可以打开新连接。

配置同步—两台设备同步其设置，以确保辅助设备已准备好接管主设备。如果通过基于浏览器的界面更改配置，主设备会立即更新辅助设备。

除非两个设备运行相同的软件版本，否则无法启用高可用性。

WCCP 模式下的高可用性—当 WCCP 与高可用性对一起使用时，主设备会与路由器建立通信。设备使用 apA 或 apB 上的管理 IP 地址，而不是虚拟 IP 地址与路由器进行通信。故障转移后，新的主设备将与路由器建立 WCCP 通信。

线路连接要求

April 23, 2021

高可用性对中的两个设备以并行排列或单臂排列方式安装在同一子网上，下图显示了这两个设备。在单臂配置中，使用 apA.2 端口（以及可选的 apB.2 端口），而不是 apA.1 端口。无论是在内联模式还是单臂模式下部署，某些型号都需要单独的管理 LAN。这仅在中间图中描述。

图 1. 用于高可用性对的电缆连接

不要使用额外的开关破坏上述拓扑。不支持随机开关配置。每个交换机必须是单个、单片式交换机、单个逻辑交换机或同一机箱的一部分。

如果在连接到设备的路由器或交换机端口上启用生成树协议 (STP)，则故障转移将起作用，但故障转移时间可能会增加到大约 30 秒。如果未启用 STP，故障转移时间大约为 5 秒。因此，要实现最短的故障转移间隔，请在连接到设备的端口上禁用 STP。

其他要求

April 23, 2021

高可用性对中的两台设备必须满足以下条件：

- 具有相同的硬件，如“控制板”页面上的“系统硬件”条目所示。
- 运行完全相同的软件版本。
- 配备以太网旁路卡。要确定设备中安装的内容，请参阅“控制面板”页面。

不支持高可用性的设备在“配置：高可用性”页面上显示警告。

对高可用性对的管理访问权限

April 23, 2021

配置高可用性（高可用性）对时，您可以为该对分配一个虚拟 IP (VIP) 地址，从而使您能够像单个设备一样管理这两个设备。启用高可用性模式后，通过其 IP 地址管理辅助设备大多处于禁用状态，大多数参数显示为灰色。每个页面上都会显示一条警告消息。将高可用性 VIP 用于所有管理任务。但是，您可以从辅助设备的管理 UI 中禁用其高可用性状态。

配置高可用性对

April 23, 2021

您可以将两个新安装的设备配置为高可用性对，也可以通过向现有安装添加第二个设备来创建高可用性对。

先决条件：物理安装和基本配置过程

配置高可用性

1. 确保不超过一个设备连接到流量网络（在加速桥梁上）。如果两者都已连接，则将一条桥梁电缆与第二台设备上的有源桥梁断开。这将防止转发循环。
2. 在第一台设备的“功能”页面上，禁用“流量处理”。这将禁用加速，直到配置高可用性对。
3. 对第二台设备重复此操作。
4. 在第一台设备上，转到“配置：高级部署：高可用性”选项卡，如下所示。
5. 选中启用复选框。
6. 单击配置高可用性虚拟 IP 地址链接，并将虚拟 IP 地址分配给 apA 接口。此地址稍后将用于控制两个设备作为一个单元。
7. 返回到“高可用性”页面，然后在“VRRP VRID”字段中，为该对分配 VRRP ID。尽管该值默认为零，但 VRRP ID 号的有效范围是 1 到 255。在此范围内，您可以指定不属于网络上其他 VRRP 设备的任何值。

8. 在合作伙伴 SSL 公用名字段中，键入其他设备的 SSL 公用名称，该公用名称显示在该设备的配置：高级部署：高可用性选项卡的合作伙伴 SSL 公用名称字段中。此处使用的 SSL 凭据是出厂安装的。
9. 单击更新。
10. 在第二台设备上重复步骤 3-8。如果要通过加速桥接（如 apA）管理设备，则可能需要重新连接在步骤 1 中删除的以太网电缆才能连接到第二台设备。如果是这样，请将此电缆插入并断开第一台设备上的相应电缆。
11. 使用您的浏览器，导航到高可用性对的虚拟 IP 地址。在“功能”页面上启用流量处理。任何进一步的配置都将从此虚拟地址执行。
12. 插入断开连接的电缆。
13. 在每个设备上，配置：高级部署：高可用性页面现在应显示高可用性处于活动状态，并且一个设备是主设备，另一个设备是辅助设备。如果不是这种情况，屏幕顶部会显示一个警告横幅，指示问题的性质。

图 1. 高可用性配置页面

在高可用性对上更新软件

April 23, 2021

更新高可用性对上的 SD-WAN 软件会导致更新过程中的一个点故障转移。

注意：单击“更新”按钮将终止所有打开的 TCP 连接。

更新高可用性对上的软件

1. 登录到两台设备。
2. 在辅助设备上，更新软件并重新启动。重新启动后，设备仍然是辅助设备。验证安装是否成功。主设备应显示辅助设备存在，但由于版本不匹配，自动参数同步不起作用。
3. 在主设备上，更新软件，然后重新启动。重新启动会导致故障转移，辅助设备将成为主设备。重新启动完成后，高可用性应该完全建立，因为两个设备都运行相同的软件。

保养/恢复高可用性对的参数

April 23, 2021

系统维护：备份/还原功能可用于保存和恢复高可用性对的参数，如下所示：

备份参数

像往常一样使用备份功能。也就是说，通过高可用性 VIP 地址登录 GUI（正常管理高可用性对时），然后在“系统管理：备份/还原”页面上单击“下载设置”。

恢复参数

1. 通过清除“配置：高级部署：高级可用性（高可用性）”选项卡上的“已启用”复选框，禁用两台设备上的高可用性。
2. 从一个设备的桥上拔下网络电缆。（称之为“设备 A.”）
3. 从电源 A 上拔下电源线。
4. 通过在“系统维护: 备份/还原”页面上上传先前保存的一组参数，然后单击“还原设置”，还原其他设备（设备 B）上的参数。（完成此操作需要重新启动，从而重新启用高可用性）。
5. 等待设备 B 重新启动。它成为主要的。
6. 重新启动设备 A.
7. 登录到设备 A 的 GUI 并在“配置：高级部署：高级可用性（高可用性）”选项卡上重新启用高可用性。设备从主设备获取其参数。
8. 插入在步骤 2 中删除的网络电缆。

这两台设备现在都恢复和同步。

高可用性对故障排除

April 23, 2021

如果设备报告任何无法进入高可用性模式，错误消息也将记录原因。可能干扰高可用性模式的一些问题包括：

- 另一台设备未运行。
- 两台设备上的高可用性参数不相同。
- 这两个设备不运行相同的软件版本。
- 这两台设备的型号不相同。
- 设备之间的线路连接不正确或不完整不允许高可用性检测信号在它们之间传递。
- 一台或两台设备上的高可用性/组模式 SSL 证书已损坏或丢失。

双盒模式

April 23, 2021

双盒模式是一种基于 WCCP 的单臂部署，SD-WAN SE 设备充当 WCCP 路由器，SDWAN-WANOP（4000/5000）设备充当 WCCP 客户端，帮助建立 WCCP 融合。这样，到达 SD-WAN SE 设备的所有面向虚拟路径/Intranet 服务的 TCP 数据包都会重定向到 SDWAN-WANOP 设备，通过为客户流量提供 SD-WAN SE 和 WANOP 优势，从而实现优化优势。

仅在以下设备型号上支持双盒模式：

- SD-WAN SE 设备–4000、4100 和 5100
- SD-WAN WANOP 设备–4000、4100、5000 和 5100

> 注意
>
> 启用双盒模式时，无法访问高可用性和 WCCP 部署模式。但是，这些部署模式可供用户管理。
>
> 重要
>
> - 虽然启用双盒模式时禁用旧版 WCCP 部署，但只能从 WCCP 监视页面验证服务组融合。双盒模式的监视部分下没有单独的 GUI 页面。
> - 如果在标准版设备上运行的 WCCP 进程在短时间间隔内重新启动多次，例如，一分钟内 3 次，则服务组将自动关闭。在这种情况下，要在 WANOP 设备上获得 WCCP 融合，请在 WANOP 设备 Web GUI 中重新启用 WCCP 功能。
> - 当 WCCP 配置或与标准版设备上的配置相关的 WAN 优化发生更改时，外部 WANOP 设备将重新启动。例如，在配置编辑器接口组中启用/禁用 WCCP 复选框，然后是更改管理过程，也会重新启动 WANOP 设备。
>
> 注意
>
> 另外，在实现双盒模式时需要注意以下几点：
>
> - 当选择路由域从配置编辑器重定向到 WANOP 设备时，应将其添加到已启用 WCCP 的接口组中。
> - 同样的路由域的流量也应该在合作伙伴站点上选择。例如，**MCN** > **Branch01** 观察 WAN 优化优势。
> - 如果在启用 WCCP 的接口组中选择了路由域，则包含桥接接口的另一个接口组应配置相同的路由域。只有在启用 WCCP 的接口组配置了路由域时，传输具有 WAN 优化优势的端到端流量是不够的。

Citrix SD-WAN 标准版

要在 DC 或分支站点的标准版设备中配置双盒模式解决方案，请执行以下操作：

1. 在 SD-WAN SE Web 管理界面中，转到 配置 > 虚拟 **WAN** > 配置编辑器。打开现有配置包或创建包。
2. 在所选配置包中，转到 高级 选项卡以查看配置详细信息。
3. 打开 全局 设置并展开 路由域 以查看 重定向到 **WANOP** 复选框已启用。
4. 展开 DC 以在界面 组设置下为虚拟接口 启用 **WCCP** ，该设备指示启用了哪个虚拟网络接口。
5. 展开 站点 **+** 添加 以查看分支路由域和接口组设置。在分支站点下，为路由域启用 重定向到 **WANOP** 复选框。

> 注意
>
> 只有那些只配置了一个以太网接口的虚拟网络接口才能启用 WCCP 侦听器。不要在桥接对上启用 WCCP 监听器。它旨在在 SD-WAN SE 和 SD-WAN WANOP 设备之间的一个 ARM 接口上启用。

Citrix SD-WAN ANOP 配置

要在 SD-WAN WANOP 设备 Web GUI 中配置双框部署模式，请执行以下操作：

1. 在 SD-WAN WANOP Web 管理界面中，转到配置 > 设备设置 > 高级部署 > 双盒解决方案。
2. 单击编辑图标以编辑双盒模式设置。将显示有关 缓存 **IP** 的信息对话框。单击确定。
3. 启用双盒已启用复选框。
4. 输入对等 **IP**。对等 IP 是 SD-WAN 标准版设备的 IP 地址。
5. 输入用户凭据，然后单击应用。

双盒模式配置和可管理性

以下是部署时需要考虑的双盒模式配置和可管理性点中的一些：

- 下面提到的 SD-WAN WANOP 配置可以从 SD-WAN SE 配置编辑器配置为统一窗格
  - 服务类别
  - 应用程序分类器
  - 功能
  - 系统调整

监视

您可以直接使用 SD-WAN SE 设备的 Web UI 的“监视”页面监视 SD-WAN WANOP 流量。这样可以在处理数据流量时对 SDWAN-SE 和 SDWAN-WO 设备进行单个窗格监视。您可以在 SDWAN-SE UI 的 WAN 优化节点下查看连接详细信息、安全合作伙伴详细信息等。

配置

您可以直接从 SDWAN-SE 配置 页面在 **APPFLOW** 节点下配置 **APPFLOW**。这使 SDWAN-SE 能够充当配置 APPFLOW 和其他数据处理配置属性（如服务类、应用程序分类器）的单个窗格。在 SDWAN-SE 上完成的配置反映了 SDWAN-WO 配置，保持了无缝的 APPFLOW 功能支持。

Citrix Application Delivery Management (ADM) 已发现 SD-WANOP，如果在双盒模式下使用，则应隔离并且在关闭此模式之前不使用 Citrix ADM 进行配置。这是因为用于流量处理的 WANOP 配置是由 SD-WAN SE 设备在双盒模式下管理的。

高级优化或安全加速应直接在 SDWAN-SE 设备上配置，就像我们在 SDWAN-WO 设备上配置的那样。这有助于维护配置的单个窗格，如域加入或安全加速/SSL 配置文件创建高级优化或 SSL 代理。

- 应单独管理 SD-WAN SE 和 SD-WAN WANOP 设备的许可。
- 每个 SD-WAN SE 和 SD-WAN WANOP 设备的软件升级应该使用各自的软件包进行单独管理。例如，对于 SD-WAN SE 和升级 UPG SD-WAN WANOP.
- 应通过 WCCP 部署模式在 SD-WAN SE 和外部 WANOP 设备之间配置数据路径集成。
  - 在数据路径级别，通过 WANOP 和 SE 之间的数据路径集成，在单臂模式下提供 WCCP 和虚拟广域网功能，从而获得优化优势。

统一配置和监视

启用 SD-WAN SE 和 SDWAN-WANOP 设备的双盒模式时，可以查看 SD-WAN SE 设备中的配置，类似于查看 SD-WAN-EE 设备中的双盒配置的方式。

1. 转到 配置 > 虚拟广域网 **>** 广域网优化
2. 配置 > 设备设置下的 AppFlow 节点
3. 配置下的 WAN 优化节点。

   此信息将从 SD-WAN WANOP 设备重定向，该设备与 SD-WAN SE 设备处于双盒模式。

   与 WANOP 相关的配置，如 SSL 加速和 AppFlow 现在可以从 SD-WAN SE 网页 GUI 执行。

   现在可以通过 SD-WAN SE Web GUI 在监控 > WAN 优 化下 监 控与流量相关的统计信息，例如连接、压缩、CIFS/SMB、ICA Advanced、MAPI 和合作伙伴，类似于 SD-WAN 高级版设备。

双盒模式下 **SD-WANOP** 设备的管理 **IP** 地址变更

要在双盒模式下更改 SDWAN-WANOP 设备的管理 IP 地址，请执行以下操作：

1. 在 SD-WAN SE 设备上执行命令 清除同步。它可以确保 SD-WAN WANOP IP 地址信息被清除以进行 GUI 重定向。
2. 禁用并启用 SD-WAN WANOP 设备上的双盒模式配置。SD-WANOP 设备的新 IP 地址（已更改的 IP）被发送到 SD-WAN SE。新更改的 IP 地址将显示在 URL 重定向页面中。

管理 IP 地址用于对等 IP 地址配置。

在 **SD-WAN WANOP** 设备上禁用双盒模式

若要从双盒模式中禁用 SD-WAN WANOP 和 SD-WAN SE 设备或解耦，请执行以下操作：

1. 从 SD-WAN WANOP 设备禁用双盒模式。
2. 预计将在 SD-WAN SE Web GUI 中看到 SD-WAN WANOP 设备双盒模式页面。要清除这些页面，请执行命令：清除同步。

常见问题解答

April 23, 2021

- 加速
- 压缩
- CIFS 和 MAPI
- RPC over HTTP
- SCPS
- 安全对等
- SSL 认证
- Citrix SD-WAN WANOP 插件
- 流量成形
- 升级
- 视频缓存
- Office 365

加速

April 23, 2021

加速度是否使用隧道？

不，加速是透明的，使用与原始连接相同的 IP 地址和端口号。这允许您当前的监视方法继续正常工作。

加速如何改变数据包流？

对于非压缩连接，加速将选项添加到数据包的 TCP 标头，但保持数据包有效负载不变。这些选项允许连接各端的 Citrix SD-WAN WANOP 设备相互通信。此外，还会调整 TCP 序列号，以防止路由问题或设备故障在同一连接中混合加速数据包和非加速数据包。

通过压缩连接，当然会压缩负载，压缩机的输出将累积成全尺寸的数据包。结果是，例如，3:1 的压缩导致传输的数据包是三分之一，而不是相同数量的数据包，每个数据包减少到三分之一的大小。压缩还使用 Citrix SD-WAN WANOP TCP 头选项和序列号调整。

加速度的基本要求是什么？

加速需要连接的两端都使用 Citrix SD-WANOP 设备，连接必须使用 TCP 协议，并且连接的所有数据包必须通过 Citrix SD-WAN WANOP 设备。

CIFS 和 MAPI

April 23, 2021

在 **Citrix SD-WAN WANOP** 设备上配置 **MAPI** 和签名 **SMB** 之前，需要哪些先决条件？

在 Citrix SD-WAN WANOP 设备上配置 MAPI 和签名 SMB 之前，必须满足以下条件：

- 在客户端以及服务器端设备上，安全对等选项应设置为 True。
- 必须将委托用户添加到数据中心端设备，其状态应标记为“成功”。
- 数据中心端设备必须成功加入域。
- 服务器端设备上配置的 DNS IP 地址必须可访问。

  有关详细信息，请参阅配置 Citrix SD-WAN WANOP 设备以优化安全的 Windows 流量。

我需要在域控制器上为委托用户配置什么？

在 Citrix SD-WAN WANOP 设备上为用户配置委派之前，必须在域控制器上创建用户。

我是否需要在 **DNS** 服务器上配置任何内容？

是。在 DNS 服务器上，必须为域控制器的所有 IP 地址配置正向和反向查找。

在使 **Citrix SD-WAN WANOP** 设备加入域之前，需要验证哪些内容？

在使设备加入域之前，请验证以下内容：

- 配置到主 DNS 或辅助 DNS 服务器的 IP 地址应该是可访问的。
- 域应该是可访问的。
- 已解析的域 IP 地址应该是可访问的。
- 或者，应该通过预域加入检查实用程序的状态。

如何验证 **Citrix SD-WAN WANOP** 设备是否已准备好将用户添加为委托用户？

您可以使用 Windows 域页面上的检查委托用户实用程序验证用户。如果所有参数的状态没有任何错误消息，则设备已准备好将用户添加为委托用户。

如果实用程序显示任何故障，则必须在将用户添加为委托用户之前解决这些问题。您可以参考日志以了解测试结果。

是否有服务器端 **Citrix SD-WAN WANOP** 设备的主机名和主机名长度的任何要求？

在服务器端 Citrix SD-WAN WANOP 设备上，请确保主机名在网络中是唯一的。此外，主机名的长度不得超过 15 个字符。

我可以在域中配置单向信任吗？

不，客户端和服务器必须是与 Citrix SD-WAN WANOP 设备的域具有双向信任的域的成员。设备不支持单向信任。

我可以使用 **Macintosh Outlook** 客户端并获得 **Citrix SD-WAN WANOP** 设备的加速优势吗？

否。麦金托什 Outlook 不使用 MAPI 作为通信协议。因此，您不能在此设置中使用 Macintosh Outlook。

我是否需要使分支端 **Citrix SD-WAN WANOP** 设备加入域以加速加密 **MAPI**？

否。您不需要使分支端 Citrix SD-WAN WANOP 设备加入域以加速加密 MAPI。

我可以在数据中心侧配置一个 **Citrix SD-WAN WANOP 2000** 设备与 **Windows Server** 加密 **MAPI**？

是。您可以在数据中心端配置配备 Windows Server 的 Citrix SD-WAN WANOP 2000 设备进行加密 MAPI。

当我使 **Citrix SD-WAN WANOP** 设备加入域并且网络上存在配置了不同时区的 **NTP** 服务器时，设备是否与域控制器或 **NTP** 服务器同步时间？

当您使 Citrix SD-WAN WANOP 设备加入域时，设备始终与域控制器而不是 NTP 服务器同步其时间。

在 **Citrix SD-WAN WANOP** 设备上，清除黑名连接的默认持续时间是多少？

默认情况下，黑色列出的连接将在 900 秒内清除。

Citrix SD-WAN WANOP 设备上支持哪些 **Outlook** 身份验证机制？

从版本 6.2.4 开始，设备支持协商（默认）和 NTLM v2 Outlook 身份验证，但不支持 Kerberos 身份验证。但是，版本 6.2.3 和更早版本只支持协商 Outlook 身份验证。

Citrix SD-WAN WANOP 是否支持 **Outlook Anywhere**、**RPC over HTTPS**？

是的，从版本 7.3 开始。

压缩

April 23, 2021

Citrix SD-WAN WANOP 压缩的优势是什么？

虽然压缩的基本机制是缩小数据流，但这样做的好处是使事情更快。较小的文件（或较小的事务）传输所需的时间较少。大小无关紧要：压缩点是速度。

如何衡量压缩效益？

有两种测量压缩效益的方法：时间和压缩比。当 WAN 链接是主要瓶颈时，这两者是相互关联的。由于 Citrix SD-WAN WANOP 压缩机速度非常快，实时压缩数据，压缩 5:1 的文件在五分之一的时间传输。在遇到次要瓶颈之前，这一点始终如一。例如，如果客户端速度太慢，无法处理全速传输，则 5:1 的压缩比可提供低于 5:1 的加速。

压缩是如何工作的？

压缩引擎会保留先前通过链接传输的数据，最新的数据保留在内存中，磁盘上的数据数量更大。当再次遇到之前传输的字符串时，它将替换为对上一个副本的引用。此引用通过 WAN 而不是实际字符串发送，另一端的设备会查找引用并将其复制到输出流中。

最大可实现的压缩比是多少？

Citrix SD-WAN WANOP 设备上可实现的最大压缩比约为 10000:1。

预期的压缩比是多少？

总体压缩率是所有尝试压缩链路上数据流的平均值。有些压缩比其他人更好，有些从来没有压缩。设备使用服务类来防止向压缩机发送明显不可压缩的流。压缩对不同类型数据的影响如下所示：

一次性压缩或加密的数据流不会再被看到，并且已经被压缩或加密，例如加密 SSH 隧道和实时摄像机监视—不会压缩，因为它们的数据流永远不会两次相同。

压缩二进制数据或被多次看到的加密数据在第二次和后续传输中压缩得非常好，在这些后续传输中，压缩比在数百到数千到一之间。在第一次转移时，他们不会压缩。此类数据的平均压缩比取决于多次查看数据的频率。虽然单个传输有时显示压缩率超过 1 000:1，但链路上压缩二进制数据的平均值在大多数链路上介于 1.5:1 和 5:1 之间，某些链路的平均值高于 10:1，具体取决于流量的性质。

文本流和未压缩/未加密的二进制数据即使在第一次传递也会压缩。文本流压缩得很好，因为即使不相关的文本也有许多子字符串共同点。文档、源代码、HTML 页面等都是如此。在 1.5:1 到 4:1 的顺序上进行首次压缩是常见的。在第二次和后续传递中，它们压缩几乎以及压缩二进制数据（100:1 或更多）。未压缩的二进制数据是可变的，但压缩通常比文本更好。未压缩的二进制数据示例包括 CD 映像、可执行文件以及未压缩的图像、音频和视频格式。在第二次和随后的过程中，它们压缩了关于以及压缩的二进制数据。

Citrix Virtual Apps and Desktops 数据在文件传输、打印机输出和视频方面的压缩特别出色，前提是以前相同的数据流遍历了链路。由于协议开销，峰值压缩约为 40:1，平均压缩可能在 3:1 左右。交互式数据流（如屏幕更新）给出的压缩结果大约为 2:1。

缓存和压缩有什么区别？

缓存将整个命名对象保存在客户端设备上。在文件系统缓存的情况下，名称可以是路径和文件名，在 Web 缓存的情况下是 URL。如果您传输具有不同名称的相同对象，则缓存不会带来任何好处。如果传输与缓存对象名称相同的对象，但内容略有差异，则缓存不会带来任何好处。如果可以从缓存中提供对象，则不会从服务器中提取对象。

另一方面，压缩没有对象名称的概念，并且只要传输中的字符串匹配已经在压缩历史中的字符串，就会带来好处。这意味着，如果您下载文件、更改 1% 的内容并上传新文件，则上传时可能会达到 99:1 的压缩。如果您下载文件，然后将其

上传到远程站点上的其他目录，则可能也会实现较高的压缩率。压缩不需要文件锁定，也不会受到“陈旧”的影响。该对象总是从服务器获取，因此始终是字节逐字节正确的。

RPC over HTTPS

April 23, 2021

是否必须创建一个服务类来通过 **HTTPS** 连接加速 **RPC**?

创建新服务类是一项可选任务。您可以使用现有的 HTTPS 服务类。但是，要专门为通过 HTTPS 连接创建 RPC 的报表，您必须创建新的服务类并将 SSL 配置文件绑定到该服务类。如果不希望通过 HTTPS 连接为 RPC 创建服务类，则可以将已创建的 SSL 配置文件绑定到 Web（私有安全）服务类。

我没有通过 **HTTPS** 应用程序为 **RPC** 创建任何服务类。这将如何影响通过 **HTTPS** 连接报告 **RPC**?

将设备升级到版本 7.3 时，创建的通过 HTTPS 创建的 RPC 应用程序不属于任何服务类。因此，所有通过 HTTPS 的 RPC 连接都列为报表中的 TCP 其他连接。如果要将这些连接分类为通过 HTTPS 连接的 RPC，则必须为这些应用程序创建服务类。

设备上是否有通过 **HTTPS** 进行 **RPC** 的默认服务类?

否。设备仅具有默认应用程序，而不具有默认服务类。您必须为应用程序创建服务类。

设备是否通过 **HTTPS** 连接向 **RPC** 提供任何 **SSL** 压缩优势?

否。设备不通过 HTTP 连接为 RPC 提供任何 SSL 压缩优势。压缩优势仅适用于 HTTPS 流量的加密和解密。

与 **MAPI** 类似，设备是否通过 **HTTPS** 优化 **RPC** 连接的延迟?

否。设备不会通过 HTTPS 优化 RPC 的延迟。

通过 **HTTP** 的 **MAPI** 与通过 **HTTPS** 的 **RPC** 不同吗?

是。通过 HTTP 的 MAPI 是在 Microsoft Exchange Server 2013 SP1 或更高版本上支持的新协议。

客户端和服务器端 **Citrix SD-WAN WANOP** 设备上的通过 **HTTPS** 设置的 **RPC** 设置有什么区别?

除了创建服务类并通过 HTTPS 向其添加 RPC 应用程序之外，您无需在客户端 Citrix SD-WAN WANOP 设备上进行任何其他配置。

如果我在透明代理模式下配置 **SSL** 配置文件，会发生什么情况?

某些 Exchange Server 需要 TLS 会话票证支持。要加速与这些服务器的连接，您需要使用拆分代理创建 SSL 配置文件，因为透明代理模式不支持 TLS 会话票证。

如果 **Microsoft Exchange Server** 使用负载平衡设置，那么在通过 **HTTPS** 服务类创建 **RPC** 时，应该向筛选器规则添加哪个目标 **IP** 地址?

如果您使用的是负载平衡设备，请在通过 HTTP 服务类创建 RPC 时将其虚拟 IP (VIP) 地址添加到筛选器规则。

如何在 **Outlook (MAPI)** 页面中区分 **MAP** 和 **RPC** 通过 **HTTPS** 流量?

您可以根据 Outlook (MAPI) 页上显示的应用程序区分流量。例如，通过 HTTPS 使用 MAPI 和 RPC 用于以下应用程序:

- **MAPI**：MAPI 和 eMAPI
- 通过 **HTTPS** 进行的 **RPC**：HTTP 地方应用程序协议、HTTP 地方应用程序协议、HTTPS 地方应用程序协议和 HTTPS 地方应用程序协议

SCPS

April 23, 2021

什么是 **SCPS** 协议?

空间通信协议标准协议 (SCPS) 协议是 TCP 协议的一个变体.

SCPS 协议有什么用途?

SCPS 协议用于卫星通信和类似应用。

Citrix SD-WAN WANOP 设备上是否支持 **SCPS** 协议?

是。Citrix SD-WAN WANOP 设备支持 SCPS 协议并加速使用此协议传输数据。

是否可以将启用 **SCPS** 的设备与未启用 **SCPS** 的设备一起使用?

是。如果必须将启用 SCPS 的设备与未启用 SCPS 的设备混合，请以不会发生不匹配的方式部署它们。您可以使用基于 IP 的服务类规则或安排部署，以便每个路径都具有匹配的设备。

如果我在链接的另一端一端使用启用了 **SCPS** 的设备，会发生什么情况?

如果连接一端的设备启用了 SCPS，而另一端没有启用，则重新传输性能会受到影响。此情况也会导致“SCPS 模式不匹配”警报。

启用了 **SCPS** 的设备和默认设备的行为有什么区别?

启用了 SCPS 和默认设备行为之间的主要区别在于使用 SCPS 风格的“选择性负面确认”（零食）而不是标准的选择性确认（Sack）。

安全对等

April 23, 2021

哪些 **Citrix SD-WAN WANOP** 功能需要安全对等?

当您打算使用以下任一功能时，需要在链接的两端建立 Citrix SD-WAN WANOP 设备之间的安全对等：

- SSL 压缩
- 签署的 CIFS 支助
- 加密 MAPI 支持

在配置安全隧道之前，我是否需要考虑任何事情？

是。您必须订购并接收加密许可证，然后才能在 Citrix SD-WAN WANOP 设备到链接末端之间配置安全隧道。

当您在链接的一端对设备启用安全对等时，会发生什么情况？

当您在链接一端的 Citrix SD-WAN WANOP 设备上启用安全对等时，另一个设备将检测到该设备并尝试打开 SSL 信令隧道。如果两个设备通过此隧道成功地相互身份验证，则这些设备具有安全的对等关系。两个设备之间的所有加速连接都将加密，并启用压缩功能。

如果我不在合作伙伴设备上启用安全对等，会发生什么情况？

如果设备启用了安全对等，则不会加密或压缩与其没有安全对等关系的伙伴的连接，尽管 TCP 流量控制加速仍可用。禁用压缩，以确保来自受保护伙伴的压缩历史记录中存储的数据不能与不安全的伙伴共享。

为什么我需要密钥库密码？

您需要密钥库密码才能访问安全参数。此密码不同于管理员的密码，并允许安全管理与其他任务分离。如果重置密钥库密码，则所有现有的加密数据和私钥都将丢失。

为了保护数据，即使设备被盗，每次重新启动设备时都必须重新输入密钥库密码。在完成此操作之前，禁用安全对等和压缩。

我从 **Citrix** 收到的 **Citrix SD-WAN WANOP** 设备是否包含用于设置安全隧道的密钥和证书？

否。Citrix SD-WAN WANOP 产品在没有 SSL 信令隧道所需的密钥和证书的情况下发货。你必须自己生成它们。

SSL 加速

April 23, 2021

加速度是否使用隧道？

不，加速是透明的，使用与原始连接相同的 IP 地址和端口号。这允许您当前的监视方法继续正常工作。

加速如何改变数据包流？

对于非压缩连接，加速将选项添加到数据包的 TCP 标头，但保持数据包有效负载不变。这些选项允许连接各端的 Citrix SD-WAN WANOP 设备相互通信。此外，还会调整 TCP 序列号，以防止路由问题或设备故障在同一连接中混合加速数据包和非加速数据包。

通过压缩连接，当然会压缩负载，压缩机的输出将累积成全尺寸的数据包。结果是，例如，3:1 的压缩导致传输的数据包是三分之一，而不是相同数量的数据包，每个数据包减少到三分之一的大小。压缩还使用 Citrix SD-WAN WANOP TCP 头选项和序列号调整。

加速度的基本要求是什么?

加速需要连接的两端都使用 Citrix SD-WAN WANOP 设备，连接必须使用 TCP 协议，并且连接的所有数据包必须通过 Citrix SD-WAN WANOP 设备。

Citrix SD-WAN WANOP 插件

April 23, 2021

我可以使用哪些方法在我的计算机上安装 **Citrix SD-WAN WANOP** 插件?

可以使用下列方法之一在计算机上安装 Citrix SD-WAN WANOP 插件:

- 独立安装：运行微软安装程序 (msi) 文件。
- 静默安装：运行以下命令:

  ```
  *\> msiexec.exe /i path\\CitrixSD-WANWANOPPluginReleasex64-\<
  Release\\_Nunmer\> /qn*
  ```

- 远程安装：从 Citrix Receiver 远程安装 Citrix SD-WAN WANOP 插件。此安装是使用销售服务器完成的。

我可以自定义 **Citrix SD-WAN WANOP** 插件安装程序吗?

是。您可以使用 Citrix SD-WAN WANOP 插件的 msi 文件自定义信令 IP 地址和基于光盘的压缩 (DBC) 大小。

安装 **Citrix SD-WAN WANOP** 插件的最低硬件要求是什么?

对于 Citrix SD-WAN WANOP 插件，您的计算机应满足以下要求:

- Pentium 4 级 CPU
- 至少 4 GB 的内存
- 最少 2 GB 可用硬盘空间

我可以在哪些操作系统上安装 **Citrix SD-WAN WANOP** 插件?

可以在以下操作系统上安装 Citrix SD-WAN WANOP 插件:

操作系统	版本	版本
Windows XP	家庭，专业	32-bits

操作系统	版本	版本
Windows Vista	Home Basic、Home Premium、Business、Enterprise、Ultimate	32-bits
Windows 7	Home Basic、Home Premium、Business、Enterprise、Ultimate	32 位、64 位
Windows 8	专业、企业	32 位、64 位
Windows 10	专业、企业	32 位、64 位

在安装 **Citrix SD-WAN WANOP** 插件之前，应采取哪些预防措施？

在计算机上安装 Citrix SD-WAN WANOP 插件之前，请采取以下预防措施：

- 根据您的操作系统版本，下载 32 位或 64 位 Citrix SD-WAN WANOP 安装程序版本。
- 无法在压缩的驱动器或文件夹上安装 Citrix SD-WAN WANOP 插件。
- 确保计算机具有足够的可用磁盘空间。
- 您不能降级 Citrix SD-WAN WANOP 插件版本。如果要使用早期的 Citrix SD-WAN WANOP 版本，则必须卸载当前版本，然后安装较早版本。

哪些 **Citrix SD-WAN WANOP** 设备支持 **Citrix SD-WAN WANOP** 插件？

以下 Citrix SD-WAN WANOP 设备支持 Citrix SD-WAN WANOP 插件：

- SD-WAN WANOP 2000
- 配备 Windows Server 的 SD-WAN WANOP 2000 设备
- SD-WAN WANOP 3000
- SD-WAN WANOP 4000
- SD-WAN WANOP 5000

哪些 **Citrix SD-WAN WANOP** 设备不支持 **Citrix SD-WAN WANOP** 插件？

以下 Citrix SD-WAN WANOP 设备不支持 Citrix SD-WAN WANOP 插件：

- SD-WAN WANOP 400
- SD-WAN WANOP 700
- SD-WAN WANOP 800
- 配备 Windows Server 的 SD-WAN WANOP 1000

是否需要在 **Citrix SD-WAN WANOP 2000**、**3000** 和 **VPX** 设备上安装并发 **(CCU)** 许可证才能使用 **Citrix SD-WAN WANOP** 插件？

是。必须在 Citrix SD-WAN WANOP 2000、3000 和 VPX 设备上安装 CCU 许可证才能使用 Citrix SD-WAN WANOP 插件。

我是否需要在 **Citrix SD-WAN WANOP 4000** 和 **5000** 设备上安装 **CCU** 许可证才能使用 **Citrix SD-WAN WANOP** 插件？

否。您不需要在 Citrix SD-WAN WANOP 4000 和 5000 设备上安装 CCU 许可证即可使用 Citrix SD-WAN WANOP 插件。设备基础许可证足以让 Citrix SD-WAN WANOP 插件连接到这些设备。

Citrix 对于加速子网的建议有哪些？

Citrix 建议执行以下操作以加速子网：

- 切勿使用 ALL/ALll 进行加速配置。根据要求指定子网。
- 不要为 Citrix Gateway VIP 地址配置加速。

Windows 瘦客户端上是否支持 **Citrix SD-WAN WANOP** 插件？

否。Windows 瘦客户端上不支持 Citrix SD-WAN WANOP 插件。

Citrix SD-WAN WANOP 插件支持哪些 **Citrix Receiver** 和 **Citrix Gateway** 版本？

Citrix SD-WAN WANOP 插件支持 Citrix Receiver 4.1 和 Citrix Gateway 10.5 版本。

Citrix SD-WAN WANOP 插件不支持哪些 **Citrix SD-WAN WANOP** 功能？

Citrix SD-WAN WANOP 插件不支持以下 Citrix SD-WAN WANOP 功能：

- 视频缓存
- 流量成形
- IPv6

是否需要在 **Citrix SD-WAN WANOP 4000** 或 **5000** 设备上配置加速规则，以便 **Citrix SD-WAN WANOP** 插件能够使用？

是。必须在 Citrix SD-WAN WANOP 4000 或 5000 设备上配置加速规则，以便 Citrix SD-WAN WANOP 插件能够使用。

信号通道源滤波的意义是什么？

通过使用信号通道源筛选，您可以允许或拒绝特定子网或 IP 地址连接到设备并获取加速规则的功能。被拒绝的源子网无法建立信令连接并加速流量。

局域网检测的意义是什么？

启用 LAN 检测时，当 Citrix SD-WAN WANOP 插件和设备位于同一 LAN 上时，它会阻止流量加速。本地加速是不可取的，因为将设备的带宽限制应用于本地连接可能会降低本地流量的速度。

要加速流量，**Citrix SD-WAN WANOP** 插件和设备之间的最小建议 **RTT** 值是多少？

Citrix 建议您配置的 RTT 值大于本地局域网上的任何 RTT（ping 时间），但小于任何远程用户的 RTT 值。20 毫秒的默认值对于大多数网络来说是足够的。

为 **Citrix SD-WAN WANOP** 插件定义加速规则时，应考虑哪些条件？

为 Citrix SD-WAN WANOP 插件定义加速规则时，请考虑以下条件：

- 为设备本地的所有子网定义加速规则。这些子网是安装设备的站点上的 LAN 子网。
- 如果存在不属于 LAN 的任何目标 IP 地址，请为这些 IP 地址添加排除规则。请确保排除 IP 地址的规则位于加速子网流量的规则之前。这包括 IP 地址显示为本地的远程站点上的子网。
- 如果您使用 VPN 以内联模式安装了设备，并且该设备在透明模式下运行，则可以将设备配置为加速所有企业流量，而不仅仅是源自或发往本地站点的流量。在这种情况下，唯一的加速连接是 Citrix SD-WAN WANOP 插件和 VPN 之间的连接。加速 Citrix SD-WAN WANOP 插件和 VPN 之间的流量是最佳的。

Citrix SD-WAN WANOP 插件崩溃和存储在计算机上的跟踪文件在哪里？

Citrix SD-WAN WANOP 插件的崩溃和跟踪文件存储在以下文件夹中：

- 崩溃文件：C:/ProgramFiles/Citrix/Citrix SD-WAN WANOP
- 跟踪文件：C:/Users/admin/AppData/Local/Temp

Citrix SD-WAN WANOP 插件如何连接到高可用性对？

Citrix SD-WAN WANOP 插件始终连接到相同的信令 IP 地址。信令 IP 地址仅绑定到高可用性对的主设备，而不绑定到辅助设备。因此，Citrix SD-WAN WANOP 插件始终连接到高可用性对的主设备。

Citrix SD-WAN WANOP 插件支持哪些部署模式？

Citrix SD-WAN WANOP 插件支持以下部署模式：

- 内联。
- WCCP。
- 高可用性。
- Citrix SD-WAN WANOP 插件与 NAT 部署。
- Citrix SD-WAN WANOP 插件与 Citrix SD-WAN WANOP 设备在 WCCP 模式下使用 ICA 代理.
- Citrix SD-WAN WANOP 插件与 Citrix SD-WAN WANOP 4000 或 5000 设备。在此部署中，管理端口 (0/1) 连接到管理网络，并且 信令 IP 地址位于不同的网络上。

数据包如何在透明和重定向器模式下流动？

在透明模式下，Citrix SD-WAN WANOP 设备不会更改数据包的源 IP 地址。在重定向器模式下，Citrix SD-WAN WANOP 设备代理服务器并更改数据包的 IP 地址。

> 注意
>
> Citrix 建议使用透明模式进行生产部署。

如何在 **Citrix SD-WAN WANOP** 插件和设备之间建立安全隧道?

要在 Citrix SD-WAN WANOP 插件和设备之间建立安全隧道，请完成以下过程:

1. 在 Citrix SD-WAN WANOP 插件用户界面上，打开证书选项卡。
2. 选择 **CA** 证书 选项。
3. 单击 导入 并上传相关 CA 证书。
4. 选择要存储证书的证书存储区。
5. 选择 客户端证书 选项。
6. 单击导入。
7. 选择适当的证书格式并上传相关证书。
8. 将证书存储在证书存储区中。
9. 如果私钥受密码保护，请输入密码以解密私钥。
10. 您必须将相同的 CA 证书和密钥对上传到设备才能建立安全隧道。

如何验证是否已建立安全隧道?

要验证是否已建立安全隧道，请完成以下过程:

1. 安装了 Citrix SD-WAN WANOP 插件的计算机，请运行以下命令:

   \> telnet localhost 1362

2. 在控制台上，运行以下命令:

   \> showtunnels

   以下是命令的示例输出。如果输出包含“已连接可用”部分中的文本安全，则已建立安全隧道。如果未建立安全隧道，则文本将读取 明文。

   ```
   ```
   Showtunnels
   Message Tunnels:
   Connected Available:
   172.16.9.100 auto,secure,client,initiator,configured
   CN: mike.199.130
   ```

   Connected Available : 1
   Clients: 1 peers: 0
   “‘

 
   ```

有关 Citrix SD-WAN WANOP 插件的更多信息，请参阅 [Citrix SD-WAN WANOP 插件] (/en-us/citrix-sd-wan-wanop/11-1/wanopt-plug-in.html)。

流量成形

April 23, 2021

什么是 **Citrix SD-WAN WANOP** 流量成形？

Citrix SD-WAN WANOP 流量调整使用一组策略来设置不同链路流量的优先级，并以接近但不超过链路速度的速率将流量发送到链路。与仅适用于 TCP/IP 流量的加速不同，流量成形器处理链接上的所有流量。

流量成形的好处是什么？

根据您设置的策略，流量调整使用稀缺的链接资源，因此已知重要的流量将比已知不重要的流量获得更多的带宽。

流量塑造者如何与 **Citrix Virtual Apps and Desktops** 流量进行交互？

Citrix SD-WAN WANOP 设备解析虚拟应用程序/虚拟桌面数据流，并了解不同类型的流量及其优先级，从而有利于高优先级流量。它是唯一能够确定加密 ICA 流优先级并为 MultiStream ICA 提供本机支持的产品，该产品将用户的会话分成多达四个具有不同优先级的连接。

什么是加权公平排队？

Citrix SD-WAN WANOP 设备使用加权公平队列，这为每个连接提供单独的队列。通过公平的排队，太快的连接只能溢出自己的队列。它对其他连接没有影响。

加权和非加权公平排队有什么区别？

加权公平排队包括给予某些流量比其他流量更高的优先级（权重）的选项。权重为 2 的流量接收的流量是流量带宽的两倍，权重为 1。在 Citrix SD-WAN WANOP 配置中，权重将在流量调整策略中分配。

什么是链接定义？

链接定义指定与已定义的链接关联的流量、允许在链接上接收的流量的最大带宽以及通过链接发送的流量的最大带宽。该定义还将流量标识为入站或出站流量以及 Wanside 或 LAN 端流量。

链接定义有什么好处？

链接定义使设备能够防止 WAN 链接上的拥塞和丢失，并执行流量调整。该定义还将流量标识为入站或出站流量以及 Wanside 或 LAN 端流量。将通过设备流动的所有流量与链接定义列表进行比较，第一个匹配定义标识流量所属的链接。

我没有使用默认策略配置任何服务类。但是，流量调整报告显示由默认策略表示的大量流量。我是否配置错误？

否。您的配置没有问题。流量调整仅适用于 WAN 链接。LAN 或任何其他链接上的流量由默认策略表示。

例如，考虑一种配置，您可以创建一个服务类（如 Managment_Service_Class），该服务类将管理子网作为目标 IP 地址，并将自定义流量调整策略绑定到此服务类。在这种情况下，当 WAN 上没有流量时，您可以注意到管理流量在服

务类报表中被归类为管理 _Service_Class。但是，在流量调整策略报告中，默认策略的条目仍然存在，您可能希望作为自定义流量调整策略存在。

在流量调整策略报告中，设备不使用管理 _Service_Class 策略的自定义流量调整策略，并应用默认策略。为了避免这种混淆，您可以清除“所有其他”选项或为管理界面定义 LAN 类型链接。

升级 (OS) 流程

April 23, 2021

新的 **WANOP** 操作系统内核升级支持哪个 **SD-WAN** 版本？

Citrix SD-WAN 版本 10.1 及更高版本。

所有 **SD-WAN** 平台都支持新操作系统吗？

是。所有 SD-WANOP（VPX、物理、云）和高级/企业版设备均支持操作系统升级。

版本 **10.1** 支持的 **WANOP VPX** 配置文件（**RAM/**磁盘**/vCPU**）是什么？

- 6 GB 内存、100 GB 磁盘和 2 个虚拟 CPU
- 6 GB 内存、250 GB 磁盘和 2 个虚拟 CPU
- 8 GB 内存、500 GB 磁盘和 4 个虚拟 CPU
- 16 GB 内存、500 GB 磁盘和 4 个虚拟 CPU

使用版本 **10.0** 或更低版本运行的 **WANOP** 与 **10.1** 版本之间的关键特性有什么区别？

功能	10.0 或更早版本	10.1 或更高版本	注意
WANOP 上的视频缓存支持	支持	不支持	无
WANOP VPX 的最低内存要求	4 GB 内存	6 GB 内存	无
WANOP VPX 部署向导	支持	不支持	无
适用于 WANOP VPX 的主要/apA 适配器管理 IP 地址	默认情况下，DHCP 处于禁用状态	DHCP 在默认情况下处于启用状态	无
在 Citrix Hypervisor 理程序上升级对现有独立 WANOP VPX 的支持	支持	受支持。应导入新的 SD-WAN 10.1 XVA 图像	无

功能	10.0 或更早版本	10.1 或更高版本	注意
升级对具有 Citrix Hypervisor 6.0 虚拟机管理程序版本的物理 WANOP 平台的支持（随 7.2.2 或更早的工厂基础映像版本提供的平台将具有 Citrix Hypervisor 6.0 版本）版本 10.1	支持	您必须将 Citrix Hypervisor 升级到 6.5 版本（使用 WANOP Citrix Hypervisor 6.5 升级包），然后执行 WANOP 10.1 升级	单击“配置”GUI，将显示 Citrix Hypervisor 虚拟机管理程序版本

支持将独立 **Citrix Hypervisor** 上运行的 **WANOP VPX** 升级到 **10.1** 版本，如果不支持，为什么？

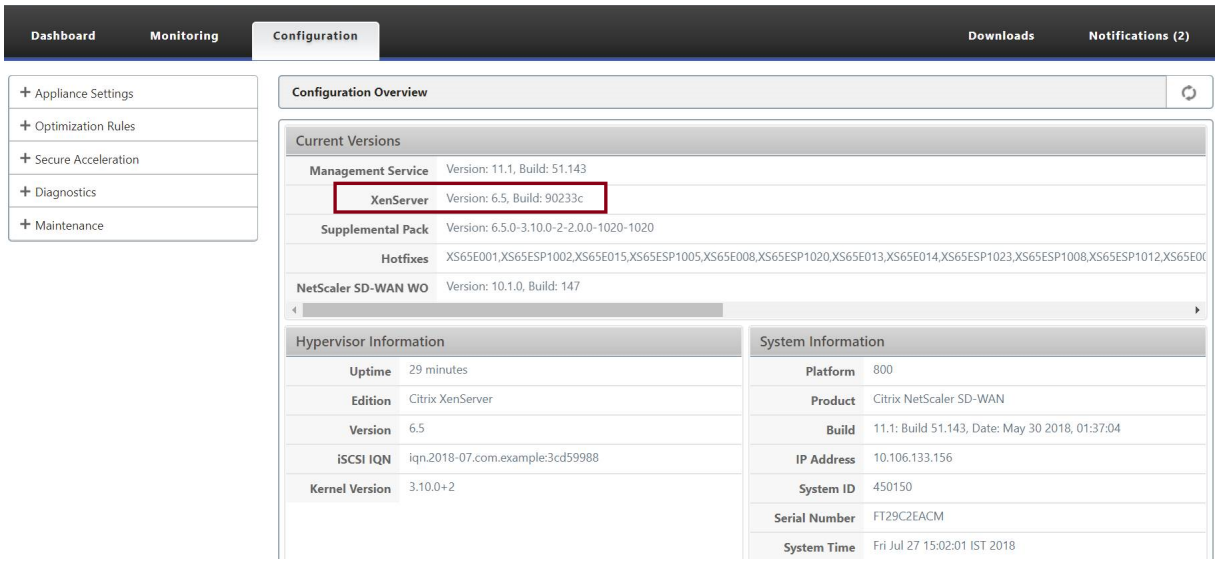
由于 PV 到 HVM 转换，因此不支持此升级。您必须使用 XVA 映像在 10.1 Citrix Hypervisor WANOP VPX 上预配新的 SD-WAN 版本。

在独立 **ESXi** 上运行的 **WANOP VPX** 升级**/Hyper-V (**与 **WO** 构建 **10.0** 或更早版本**)** 到 **10.1** 版本是支持**,** 如果没有**,** 为什么？

支持此升级。升级前，请注意新的 RAM 资源需求变化。

物理设备上的 **WANOP** 升级 **(**与 **WANOP** 版本 **10.0** 或更早版本**)** 到 **10.1** 版本是支持**,** 如果不是**,** 为什么？

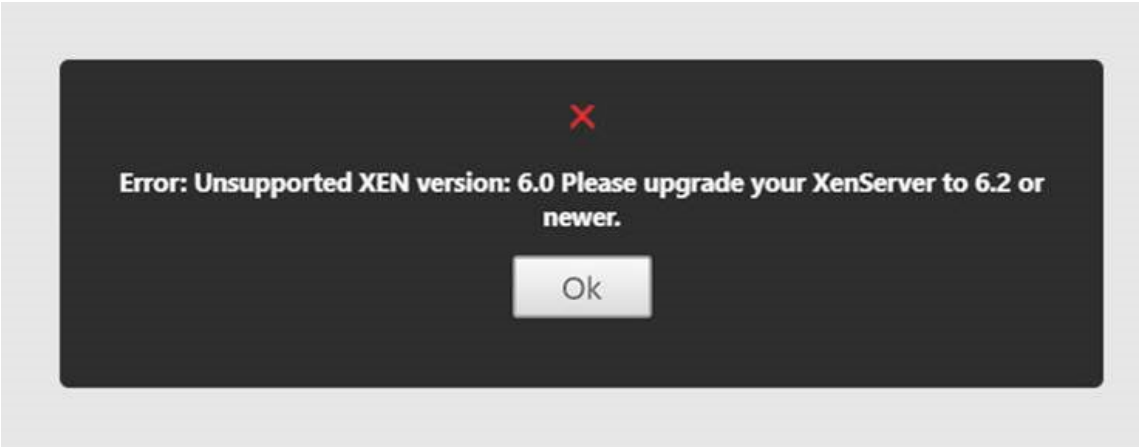
支持此升级。此升级的先决条件是让托管 Citrix Hypervisor 虚拟机管理程序（在物理 SD-WAN 设备上）具有 Citrix Hypervisor 版本 6.2/6.5 或更高版本。这可以通过使用 配置 选项卡来验证。



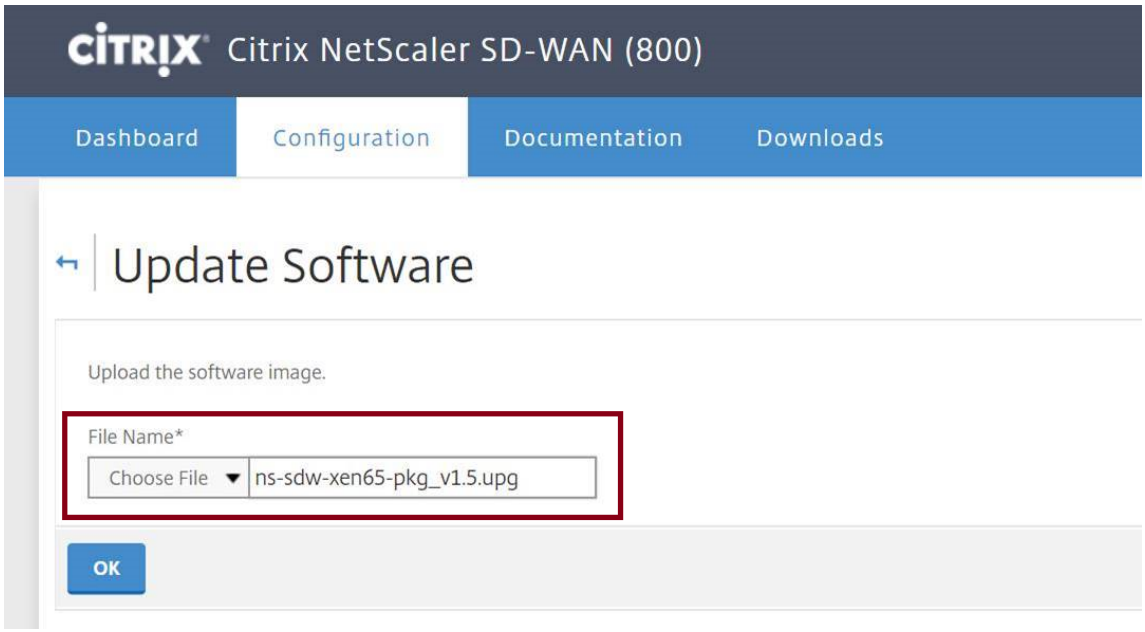
如果物理 **WANOP** 设备未使用 **Citrix Hypervisor 6.2/6.5** 或更高版本运行，用户必须执行什么操作？

升级 SD-WAN WO 版本之前，您必须升级 Citrix Hypervisor。例如，在下面的使用案例中，让我们考虑计划升级运行于 7.2.2（具有 Citrix Hypervisor 6.0 版本）的 SD-WAN 800 WANOP 平台。

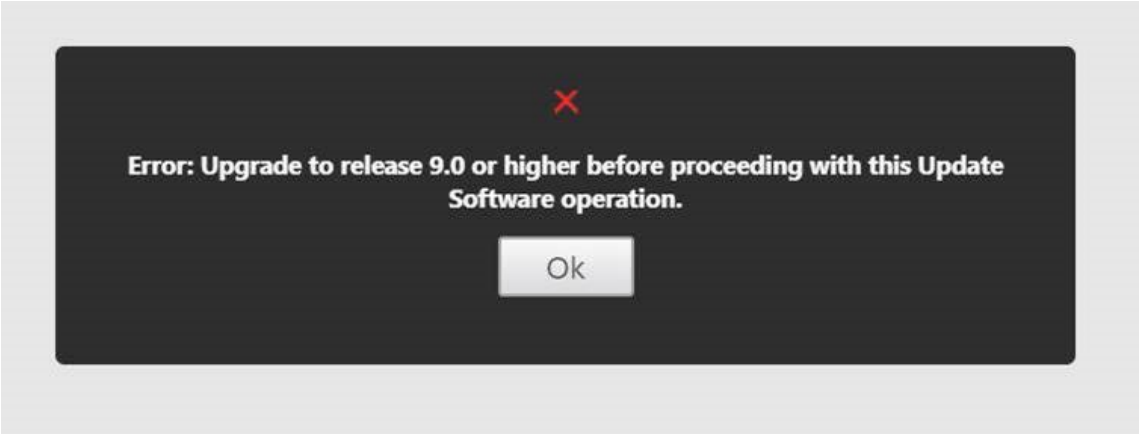
1. 将此设备升级到 SD-WAN 10.1 版本时，会出现以下错误消息。



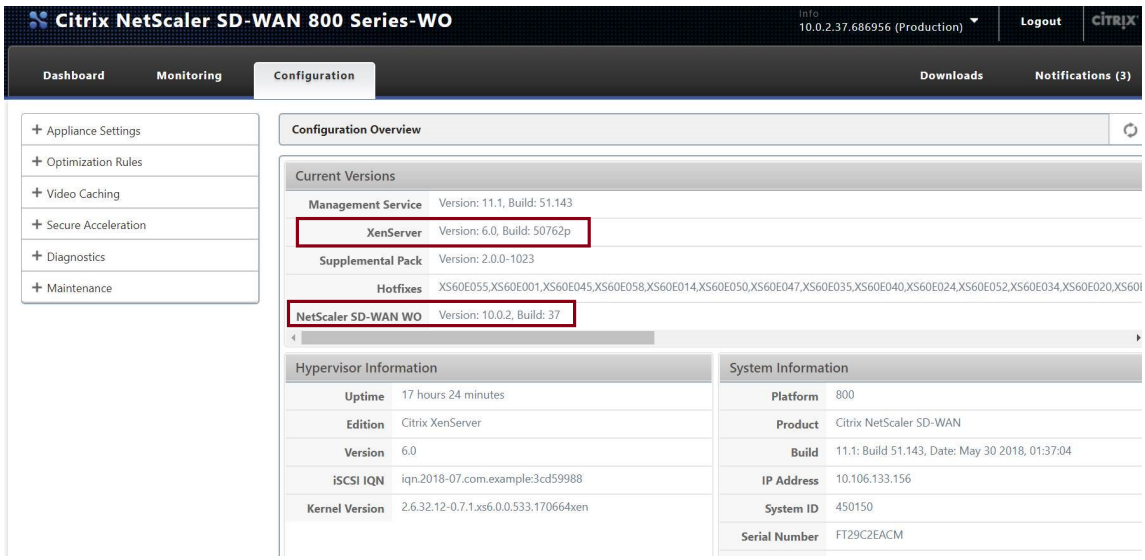
2. 使用“ns-sdw-xen65-pkg_v1.5.upg”将 Citrix Hypervisor 程序升级到 6.5（这可以从 Citrix 下载网站下载。



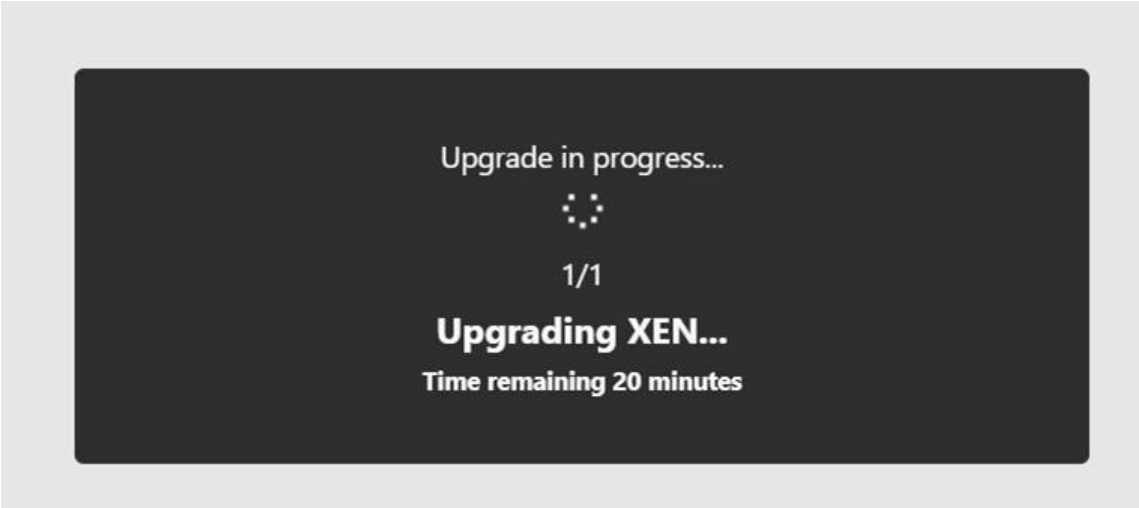
3. 如果 SD-WAN WO 没有 9.0 或更高版本，则不会升级到 Citrix Hypervisor 6.5。将显示以下错误消息。

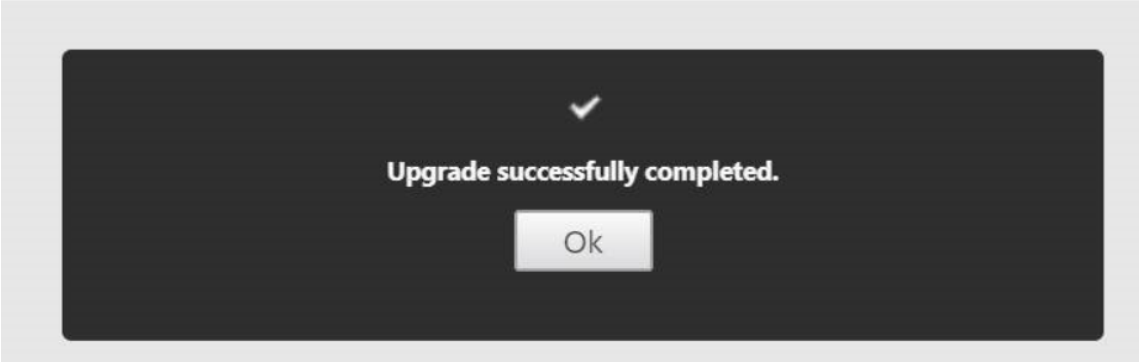


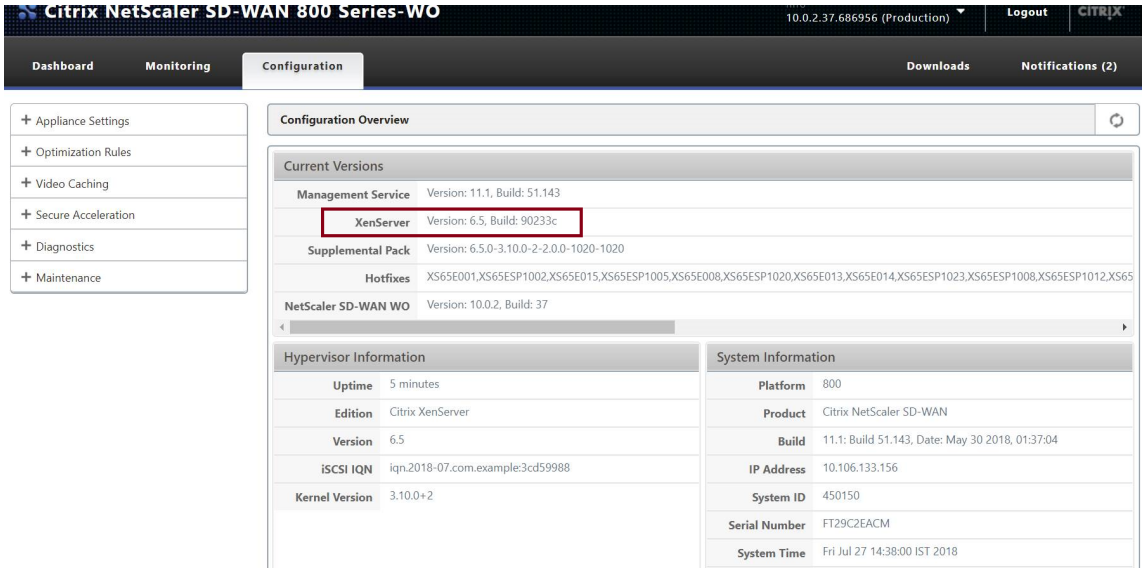
4. 让我们假设，用户现在已将 WO 版本升级到 10.0.2。



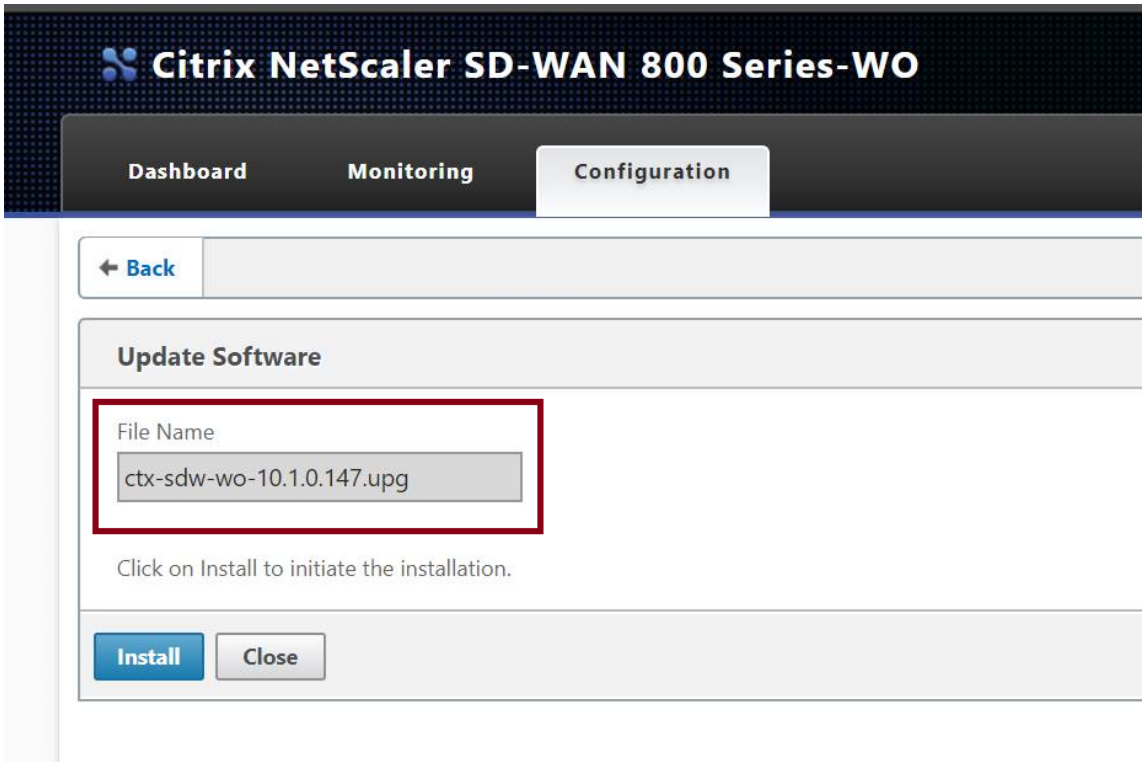
5. 现在，使用“ns-sdw-xen65-pkg_v1.5.upg”将 Citrix Hypervisor 程序升级到 6.5。

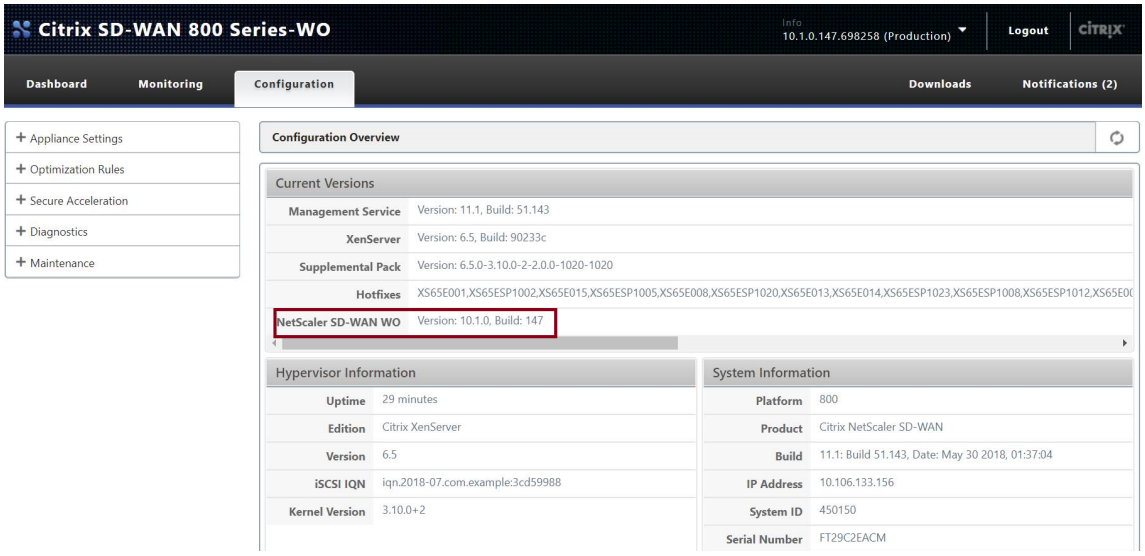






6. 现在，将 SD-WAN 升级到 10.1 版本。





客户端到服务器 **ICMP Ping** 工作正常，但 **TCP** 流量不会通过 **WANOP VPX** 设备（禁用 **WANOP** 流量处理工作正常）？

检查客户端、服务器和路由器上的防火墙设置。

当 WANOP VPX 或客户端/服务器作为 VM 托管时，请确保在端点主机 VM 上禁用校验和。

```
Linux 命令示例：
ethtool -K eth0 tx off
ethtool -K eth0 rx off
道德工具-卸载 eth0 tx 关闭
道德工具-卸载 eth0 rx 关闭
```


在两个 WO VPX 上启用“校验和。发送量”参数应为“开”。

```
示例：
Checksum.SendForceSW on
```

由于新的 **WO** 操作系统内核，**SDWAN SE/EE/WO** 设备升级流程是否有任何变化？

不能。

视频缓存

April 23, 2021

视频缓存与基于磁盘的压缩有何不同？

使用缓存时，本地设备提供缓存对象的本地副本，而无需从远程服务器再次下载该副本。缓存不需要链接的两端（只是在本地端）设备。通过压缩，远程服务器提供对象的远程副本。远程（服务器端）设备对其进行压缩，从而减小其大小，从而提高其传输速度，本地（客户端）设备将其解压缩。

压缩适用于已修改和未修改的对象。如果文件在服务器上更改 1%，则下一次传输实现高达 99:1 的压缩。

缓存仅适用于未修改的对象。如果服务器上的文件更改为 1%，则必须全部下载新版本。缓存和压缩是互补的技术，因为任何未缓存的技术都会被压缩，从而实现两者的好处。

是否可以在视频缓存和其他 **Citrix SD-WAN WANOP** 功能之间对设备的总内存进行分区？

否。所需的缓存分区和内存不可配置。

支持的视频容器格式是什么？

视频缓存独立于编解码器格式，支持所有主要容器格式。

是否可以在我自己的站点上激活内部和外部企业视频的缓存？

是。如果通过 HTTP 访问这些视频，您可以配置这些站点进行缓存。

我可以配置缓存对象的最大大小吗？

是。不会缓存大于您配置的限制的对象。要设置此限制，请导航到 配置 > 优化规则 > 视频缓存，然后从可用限制中选择值。

视频缓存如何改善用户体验？

缓存可改善多次查看视频的用户体验，特别是在速度较慢的链接上。给定视频流的第一个查看器不会受益于视频缓存功能，但后续视图将从 Citrix SD-WAN WANOP 设备以局域网速度传输，并且还会减少 WAN 使用量。

此外，如果第二个用户在仍在为第一个用户流式传输时请求相同的视频，则第二个用户将收到缓存副本。

与常规 Citrix SD-WAN WANOP TCP 操作不同，设备保留原始源和目标 IP 地址，设备将客户端的源地址替换为分配给加速桥的 IP 地址，因此通过设备的所有 HTTP 流量似乎都来自设备本身。

哪些 **Citrix SD-WAN WANOP** 设备支持视频缓存？

以下设备支持视频缓存功能：

- SD-WAN WANOP 800 设备与所有带宽许可证型号.
- 配备 Windows Server 的 SD-WAN WANOP 1000 设备，使用所有带宽许可证型号。
- SD-WAN WANOP 2000 设备与所有带宽许可证型号。
- 配备 Windows Server 的 SD-WAN WANOP 2000 设备，使用所有带宽许可证型号。
- SD-WAN WANOP 3000 设备与所有带宽许可证型号.

对于视频缓存，**Citrix SD-WAN WANOP** 设备上支持哪些部署模式？

- 支持的部署-内联虚拟内联、VLAN 和 WCCP
- 不支持的功能-Citrix SD-WAN WANOP 高可用性、组模式和菊花链

视频缓存支持哪些文件扩展名？

视频文件名必须具有以下扩展名之一：.3gp、.avi、.dat、.divx、.dvx、.dv-avi、.flv、.fmv、.h264、.hdmov、.m15、.m1v、.m21、.m2a、.m2v、.m4e、.m4v、.m75、.moov、.mov、.movie、.mp21、mp2v、.mp4、.mp4v、.mpe、.mpeg、mpeg4、mpg、mpg2、.mpv、.mts、.ogg、.ogv、.qt、.qtm、.ra、.rm、.ram、.rmd、.rms、rmvb、.rp、rv、.swf、.ts、.vfw、.vob、.webm、.wm、.wma、.wmv 和.wtv。

是否可以在不受支持的 **Citrix SD-WAN WANOP** 平台上启用视频缓存功能？

否。视频缓存功能不能在不受支持的平台上使用。

启用视频缓存功能的最低配置和其他先决条件是什么？

要启用视频缓存功能，您必须：

- 为 apA 接口分配有效的 IP 地址和 Gateway，如果存在，则分配给 apB 接口。
- 在设备上，配置可解析为 www.citrix.com 的有效 DNS 服务器。
- “所选视频缓存应用程序”列表中至少有一个应用程序。
- 检查 Citrix SD-WAN WANOP GUI 警报/现有配置警报的通知。

Citrix SD-WAN WANOP 插件是否可以使用视频缓存功能？

否。不能将视频缓存功能与 Citrix SD-WAN WANOP 插件一起使用。

支持哪些浏览器和设备？

视频缓存支持互联网浏览器、火狐浏览器和 Chrome 浏览器。视频可以在 Windows 7 或 8、Apple iPad 和 Android iOS 设备上观看。

Citrix SD-WAN WANOP 设备是否支持所有视频网站的视频缓存？

否。视频网站可用并从“视频缓存”配置页面上的“支持的应用程序”列表中添加。默认情况下，支持的应用程序包括 YouTube、Vimeo、优酷、日报和 Metaacafe。如果不使用缓存避免机制（例如向 URL 添加随机字符），则可以通过指定其 IP 地址来添加其他网站。

视频缓存是否支持 **SNMP** 监视？

是。您可以使用 SNMP MIB 监视视频缓存特定任务。

非 **HTTP** 流量是否支持视频缓存？

否。非 HTTP 流量（如 HTTPS、RTSP 和 RTMP）不支持视频缓存。

我可以将视频缓存与发送到端口 **80** 以外的端口的 **HTTP** 流量一起使用吗？

是。对于视频缓存，您可以向设备添加自定义端口。要为视频缓存添加自定义端口，请导航到 配置 > 优化规则 > 视频缓存 页面，然后单击 设置”选项卡上的“全局设 置”链接。

Citrix SD-WAN WANOP 压缩（使用 **HTTP** 服务类策略）是否可以与视频缓存一起使用？

是。当缓存对象同时存在于 Citrix SD-WAN WANOP 压缩历史记录和视频缓存中时，缓存点击时从缓存中提供内容，并在缓存未命中时从服务器中提取（并压缩）。

当有透明代理时，需要 **IP** 地址配置的现有 **HTTP** 应用程序是否需要任何更改？

是。Citrix SD-WAN WANOP 执行 HTTP 透明代理，其中它替换数据包的源 IP 地址。因此，如果现有 HTTP 应用程序具有某些策略（例如阻止某些 IP 地址或代理机制），则必须更改这些策略。

HTTP 代理连接的系统内存和连接限制是什么？

要确定限制，请检查“视频缓存调试”页面（支持.html）上的图形和统计信息。此外，请验证 VideoCach.cmd 统计信息命令是否显示以下信息。

	SD-WAN WANOP 800	配备 Windows Server 的 SD-WAN 1000	配备 Windows Server 的 SD-WAN 2000	SD-WAN 2000	SD-WAN 3000
磁盘	25 GB	25 GB	50 GB	50 GB	99 GB
RAM	375 MB	375 MB	700 MB	700 MB	1024 MB
HTTP 连接总数限制	1000	1000	1500	1500	3000
最大 HTTP 写入限制	200	200	300	300	600

达到上述 HTTP 连接限制后，会绕过新连接。

> 注意
>
> 请确保您不更改上述配置。

视频缓存的监视页面是否仅包含视频流量？

是。非视频 HTTP 流量（即使它被代理拦截）不包含在视频缓存 GUI 统计信息中。

是否需要在 **Citrix SD-WAN WANOP** 设备上使用有效 **IP** 地址配置 **apA** 以及 **apB** 接口？

否。您不需要为这两个接口分配有效的 IP 地址。从 apA 接口接收的 HTTP 数据包使用 apA IP 地址进行代理，从 apB 接口接收的 HTTP 数据包使用 apB IP 地址进行代理。

如果未为接口配置 IP 地址，则该接口上接收的 HTTP 数据包不会获得缓存优势。

可以缓存的视频文件的最小和最大大小限制是多少？

- 最小值：100 KB
- 最大数量：300 MB
- 默认值：100 MB

如何清除视频缓存磁盘？

按照最近使用最少算法的指定清除缓存对象。

当我将 **Citrix SD-WAN WANOP** 设备从版本 **6.x** 升级到 **7.y** 并启用了视频缓存时，会发生什么情况？

现有的 Citrix SD-WAN WANOP DBC 历史将丢失，并创建一个单独的视频缓存分区。

当我将 **Citrix SD-WAN WANOP** 设备从版本 **7.y** 降级到 **6.x** 并启用了视频缓存时，会发生什么情况？

Citrix SD-WAN WANOP DBC 和视频缓存历史记录被保留。但是，视频缓存功能不适用于 6.x 版本。

当我将 **Citrix SD-WAN WANOP** 设备从版本 **7.x** 升级到 **7.y** 并启用了视频缓存时，会发生什么情况？

Citrix SD-WAN WANOP DBC 和视频缓存历史记录将被保留。

我在分支机构中有一个共享管理和数据流量的网络。我应该如何在这个网络中配置视频缓存？

如果您有单个网络用于管理和数据流量，Citrix 建议您将主 IP 地址添加到加速桥接端口的 LAN 端。

我可以同时运行的预留任务的最大数量是多少？

一个如果您尝试同时启动多个预任务，则设备会以先到先出的方式构建一个任务队列。

我可以在设备上配置的最大视频源数量是多少？

100

我可以添加到设备中的预填充条目的最大数量是多少？

50

从目录列出的文件夹中下载和缓存的视频文件的最大数量是多少？

300

由预编入功能启动的视频下载和缓存是否会获得基于磁盘的压缩 **(DBC)** 优势？

是。由于视频文件已缓存，因此从缓存中尝试访问视频。

Office 365 加速

April 23, 2021

1. 为什么我们解析 SAN？

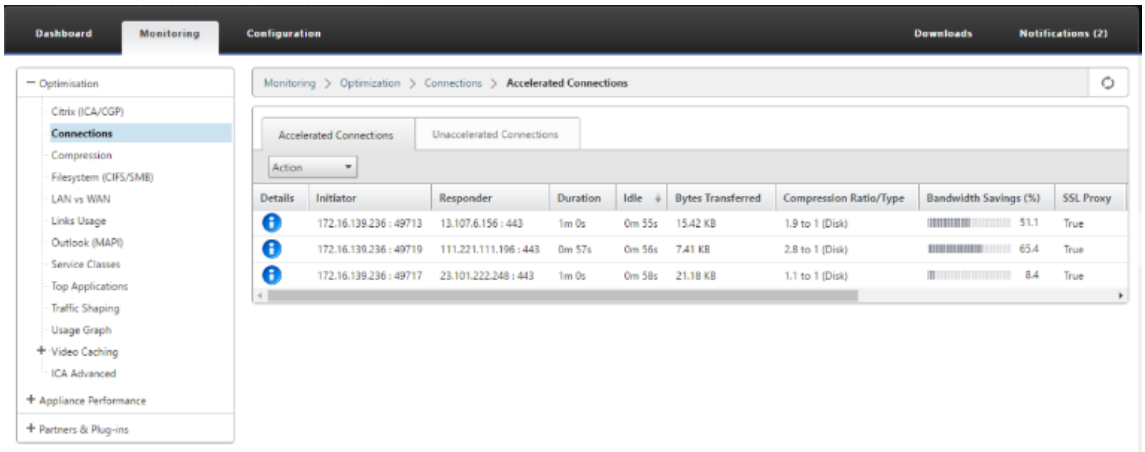
   为每个域创建多个 FQDNS 配置文件是乏味的，为了克服这一点，我们从证书中解析 SAN。

2. 什么是排除列表？

   显示错误或警告消息如果浏览器或应用程序不包含 CA 证书，则在这种情况下，在尝试从浏览器或应用程序连接几次（2-3 次）后，客户端的 IP 地址将被添加到排除列表中。在下一次尝试中，连接不是 SSL 代理，并且页面加载时没有任何错误或警告。客户端 IP 地址将保留在排除列表中 48 小时。排除列表仅为拆分代理维护。

3. 在哪里查看 Office 365 加速连接信息？

   导航到 监视 > 连接 > 加速连接，检查 SSL 代理状态。有关连接详细信息，请单击详细信息图标。



4. 如果默认情况下没有启用排除列表选项作为 SSL 配置文件配置的一部分，会发生什么情况？

   如果浏览器或应用程序不包含 CA 证书，则会显示错误或警告，并且来自该客户端或应用程序的连接将被阻止。要避免此类问题，请选择 排除列表 选项作为 SSL 配置文件配置的一部分。

5. 如果所需的 SAN 不是配置/创建的代理证书的一部分，会发生什么情况？

   连接不会被 SSL 代理，对于非代理 SSL 连接，也不会有加速优势。

6. 如果客户端不是域的一部分，或者如果客户端没有域的根证书，会发生什么？

   如果未启用排除列表，连接将被阻止。

7. 如果数据中心侧 Citrix SD-WAN WANOP 没有根或中间 CA 的，会发生什么？

   连接被阻止，或部分加载需要缺少根或中间 CA 的 Office 365 应用程序页。要取消阻止连接或使这些页面完全加载，请添加适当的 CA 证书或禁用 SSL 配置文件加速。

8. 如何知道哪些客户端被排除在加速之外？

   排除的客户端信息可以通过日志或使用 CLI 命令 显示 *ssl*-排除-*list* 来知道。

9. 当客户被排除时该怎么办？

   默认情况下，将在 48 小时后清除设备中的列表信息。用户可以使用 CLI 命令强制清除排除列表信息`*clear ssl-exclude-list -\<all\>/\<Client\\_IP\>*`。

10. 如何知道哪些 SSL 连接（SNI）不代理？

    从日志或使用 CLI 命令 显示 *ssl*-非代理 *SNI*，您可以知道非代理 SNI 的列表。

11. 如何清除非代理 SNI？

    使用 CLI 命令`*clear ssl-non-proxied-sni -\<all\>/\<server name identifier\>*`。

12. 客户端处于排除状态的默认时间是多少？

    客户端保持在排除状态 48 小时。

13. 我们可以为特定服务类应用多个配置文件吗？

    是的，我们可以应用具有多个 SSL 配置文件的服务类。

    为此，请在虚拟 WAN 设备上导航到 配置 > 服务类 > **Web**（**Internet** 安全） > 编辑 **>** 编辑 ** （应用程序）并添加可用的配置文件。

14. 如何检查非代理连接的原因？

    检查 TCP 连接页面，有关更多信息，请检查日志。要调试非代理连接问题，请执行以下操作。

    a) 如果日志没有显示有效配置-请设置有效的配置。有关配置 Office 365 功能的更多信息，请参阅Office 365 加速。

    b) 如果日志显示证书验证失败-向数据中心端 Citrix SD-WAN WANOP 设备添加有效的 CA 证书。

    c) 如果日志显示客户端已排除 - 有关被排除的客户端的信息可以使用 CLI 命令 `*clear ssl-exclude-list -\<all\>/\<Client\\_IP\>*` 从设备中清除。

附加说明

- 登录到 OneDrive 客户端有时会显示警告消息“虚假警告”，这是来自 Microsoft (https://support.microsoft.com/en-us/kb/3097938) 的一个已知问题，非 Citrix SD-WAN WANOP 设备特有。

- 对于要代理的 Office 365 重定向页面，建议创建一个单独的代理证书，其中包含与重定向页面的证书相对应的 SAN 列表。使用此代理证书创建另一个配置文件并应用于服务类。还可以在 Citrix SD-WAN WANOP 设备中添加相关 CA。
- 有时浏览器不显示正确的 CA 证书，在这种情况下，使用 Wireshark 或 OpenSSL 获取根和中间 CA 名称，并从“真实”源（例如 Windows SSL 存储）获取证书。
- 从不同的浏览器访问 Office 365 应用程序时，没有必需的证书，并且禁用了排除列表选项，可以观察到浏览器行为的差异。
- 当 Office 365 连接是 SSL 代理（也就是说 SSL 代理设置为 True）并且在浏览器办公室中显示 365 证书而不是代理证书时，建议以认知模式打开浏览器并检查行为或清除缓存，然后再次检查行为。
- Microsoft Office 365 包括许多组件和应用程序，如 OneDrive、Outlook、SharePoint、Word、PPT、Excel、OneNote。所有这些应用程序都经过测试，并已知工作没有任何问题。其他应用程序也可以在没有任何问题的情况下工作；但是，此状态可能会随着时间的推移而改变，并且您可能会遇到未知问题。

压缩

April 23, 2021

Citrix SD-WAN WANOP 压缩使用突破性技术提供透明的多级压缩。这是对任意字节流的真正压缩。它不是应用程序感知的，对连接边界无动于衷，并且可以在第二次出现在数据中时以最佳方式压缩字符串。Citrix SD-WAN WANOP 压缩工作在任何链路速度。

压缩引擎速度非常快，使压缩加速系数接近压缩比。例如，垄断 1.5 Mbps T1 链路并实现 100:1 压缩比的批量传输可以提供近 100x 或 150 Mbps 的加速比，前提是广域网带宽是传输中唯一的瓶颈。

与大多数压缩方法不同，Citrix SD-WAN WANOP 压缩历史记录在同一两个设备之间传递的所有连接之间共享。连接 A 提前几小时、几天甚至几周发送的数据可以在以后通过连接 B 引用，并获得压缩的全部加速优势。由此产生的性能远远高于通过传统方法可以实现的。

压缩可以使用设备的磁盘和内存，从而提供高达 TB 的压缩历史记录。

压缩工作原理

所有压缩算法都会扫描要压缩的数据，搜索与之前发送的字符串匹配的数据字符串。如果未找到此类匹配项，则会发送文字数据。如果找到匹配项，则匹配的数据将替换为指向前一个匹配项的指针。在一个非常大的匹配字符串中，兆字节甚至千兆字节的数据可以由只包含几个字节的指针表示，并且只需要通过链接发送这些几个字节。

压缩引擎受其压缩历史记录的大小的限制。传统压缩算法（如 LZS 和 ZLIB）使用 64 KB 或更少的压缩历史记录。Citrix SD-WAN WANOP 设备保持至少 100 GB 的压缩历史记录。Citrix SD-WAN WANOP 算法的压缩历史记录是传统算法的 100 多万倍，因此可以找到更多匹配项和更长的匹配项，从而产生更出色的压缩比。

Citrix SD-WAN WANOP 压缩算法非常快，因此即使入门级设备也可以使压缩机的输出饱和 100 Mbps 局域网。性能最高的型号可提供远远超过 1 Gbps 的吞吐量。

只压缩有效负载数据。但是，标题是间接压缩的。例如，如果连接达到 4:1 的压缩，则每四个全尺寸输入数据包只会发送一个全尺寸输出数据包。因此，标头数据量也减少了 4:1。

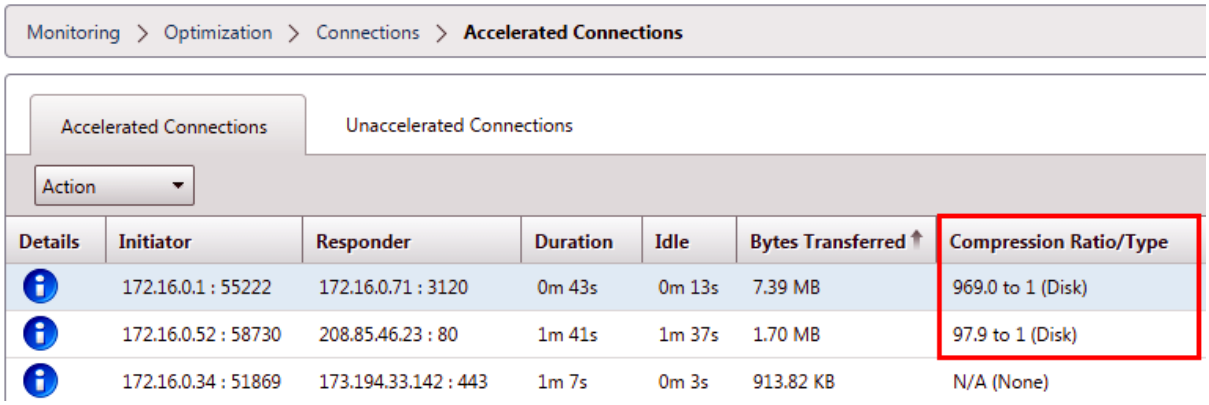
压缩作为通用优化：

Citrix SD-WAN WANOP 压缩与应用程序无关：它可以压缩来自任何非加密 TCP 连接的数据。

与缓存不同，压缩性能在不断变化的数据时非常稳健。使用缓存时，更改文件的单个字节会使缓存中的整个副本失效。通过压缩，更改文件中间的单个字节只会创建两个大匹配项，由一个不匹配数据字节分隔，并且由此产生的传输时间仅略大于以前。因此，压缩比会随着变化量而正常降低。如果您下载文件，请更改 1% 的文件，然后再次上传，预计上传时的压缩比为 99:1。

大压缩历史记录的另一个优点是使用 Citrix SD-WAN WANOP 技术轻松压缩预压缩数据。例如，JPEG 图像或 YouTube 视频是预压缩的，在第一次通过链接发送时，几乎没有可能进行额外的压缩。但是，无论何时再次发送，整个传输都会减少到几个字节，即使它是由不同的用户或使用不同的协议（例如第一次通过 FTP 和下一次通过 HTTP）发送。

实际上，压缩性能取决于遍历链接的数据量与之前遍历链接的数据相同。金额因应用程序而异，每天，甚至从时刻到时刻。当查看主动加速连接列表时，预计会看到 1:1 到 10000:1 之间的比率。

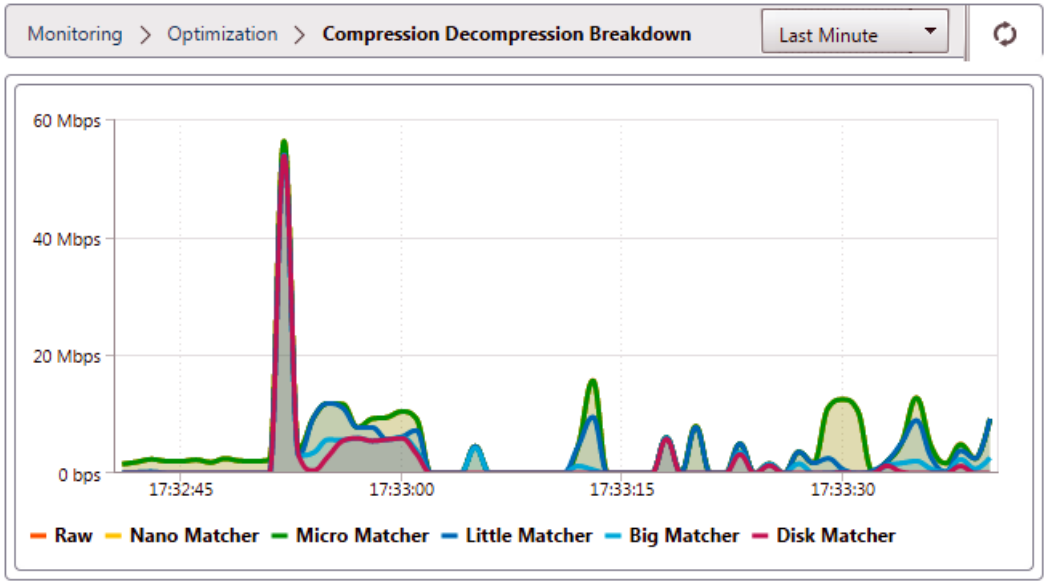


压缩加密协议：

许多显示压缩性能较差的连接都是因为它们是加密的。加密流量通常是不可压缩的，但 Citrix SD-WAN WANOP 设备可以在设备加入安全基础结构时压缩加密连接。Citrix SD-WAN WANOP 设备自动将安全基础架构与 Citrix Virtual Apps and Desktops 加入安全基础架构，并可以通过手动配置加入 SSL、Windows 文件系统 (CIFS/SMB) 和 Outlook/Exchange (MAPI) 服务器的安全基础架构。

自适应零配置操作：

为了满足不同类型的流量的不同需求，Citrix SD-WAN WANOP 设备使用的不是一个而是五个压缩引擎，因此可以轻松满足从最大规模的批量传输到最对延迟敏感的交互流量的一切需求。压缩引擎会根据不断变化的各个连接需求进行动态匹配，从而自动优化压缩。另一个好处是压缩引擎不需要配置。



基于内存的压缩

大多数压缩引擎都使用 RAM 来存储其压缩历史记录。这称为基于内存的压缩。有些设备将千兆字节的内存用于这些压缩引擎。基于内存的压缩具有较低的延迟，通常会为交互式任务（如虚拟应用程序/虚拟桌面流量）自动选择。

基于磁盘的压缩

基于磁盘的压缩引擎使用几十 GB 至 TB 的内存来存储压缩历史记录，从而实现更多更好的压缩匹配。基于磁盘的压缩引擎速度非常快，但有时比基于内存的引擎具有更高的延迟，并且通常会自动选择批量传输。

启用或禁用压缩

在配置：服务类页面上，按服务类别启用压缩。此页面具有针对每个服务类的下拉菜单，其中包含以下选项：

- 磁盘，这意味着启用了基于磁盘和基于内存的压缩。除非您有禁用该选项的特定原因，否则应选择此选项。
- 内存，这意味着启用了基于内存的压缩，但基于磁盘的压缩不启用。此设置很少使用，因为如果启用了两种类型的压缩，设备会自动选择内存或磁盘。
- 仅限流量控制，可禁用压缩，但启用流量控制加速。为始终加密的服务和 FTP 控制通道选择此选项。
- 无，这意味着压缩和流量控制都被禁用。

有关详细信息，请参阅服务类别。

测量基于磁盘的压缩性能

“

报表: 压缩”页面的“压缩状态”选项卡报告系统启动以来或使用“清除”按钮重置统计信息后的系统压缩性能。单个连接的压缩在系统日志中的连接关闭消息中报告。

压缩性能因多种因素而异，包括数据流中的冗余量，以及数据协议的结构（在较小程度上）。

某些应用程序（如 FTP）发送纯数据流；TCP 连接有效负载始终与原始数据文件相同。其他（例如 CIFS 或 NFS）不会发送纯数据流，而是在同一流中混合命令、元数据和数据。压缩引擎通过实时解析连接负载来区分文件数据。这样的数据流可以很容易地在第二次传递时产生 100:1 和 10000:1 之间的压缩比。

链接的平均压缩率取决于长匹配、短匹配和无匹配的相对流行率。这个比率取决于流量，在实践中难以预测。

测试结果显示了多级压缩作为一个整体的效果，基于内存和基于磁盘的压缩各自作出贡献。

在填充可用于基于磁盘的压缩的存储空间之前，才能实现最大压缩性能，从而提供与新数据匹配的先前数据量。在一个完美的世界中，测试不会结束，直到设备的磁盘不仅被填充，而且至少被填充和覆盖一次，以确保达到稳定状态运行。但是，很少有管理员拥有这么多代表性的数据可供他们使用。

性能测试中的另一个困难是，加速通常暴露网络中的弱环节，通常是客户端、服务器或 LAN 的性能，这些环节有时被误诊为令人失望的加速性能。

您可以使用 Iperf 或 FTP 进行初步测试和初步测试。Iperf 是有用的初步测试。它非常可压缩（即使在第一次传递），并且在两个端点系统上使用相对较少的 CPU 并且没有磁盘资源。如果双方的 LAN 使用千兆以太网，Iperf 的压缩性能应通过 T1 链路发送超过 200 Mbps；如果端点和设备之间的 LAN 路径中有任何快速以太网设备，则应略低于 100 Mbps。

Iperf 预安装在设备上（在诊断菜单下），并可从中获取http://iperf.sourceforge.net/。理想情况下，它应该从端点系统安装和运行，以便对网络进行端到端的测试，而不仅仅是从设备到设备进行测试。

FTP 对于比 Iperf 更真实的测试非常有用。FTP 简单而熟悉，其结果易于理解。二通性能应与 Iperf 大致相同。否则，限制因素可能是其中一个端点系统上的磁盘子系统。

要测试基于磁盘的压缩系统，请执行以下操作：

1. 在启用基于磁盘的压缩的两台设备之间传输多 GB 数据流。请注意此传输过程中实现的压缩。根据数据的性质，第一次传递可能会出现相当大的压缩。
2. 第二次传输相同的数据流并注意压缩的影响。

高级版中的压缩报告

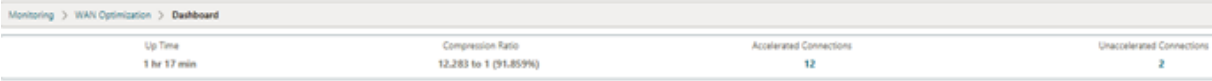
Citrix SD-WAN 高级版本没有通过具有协议或应用程序关联的 WANOP 服务类显示每个协议或应用程序基础上的压缩报告的视图。如果您使用的是高级 (企业) 版设备，则唯一可供压缩的报表是连接级别压缩报表，该报表不能显示协议已经优化或压缩的范围。压缩报告在 WAN 优化 GUI 中可用，它显示了所有唯一协议的分解以及报告在一段时间内的优化方式。

在 Citrix SD-WAN 高级（企业）版设备 GUI 中，针对 WAN 优化，在 WAN 优化仪表板下添加了以下小组件。

- 整合压缩比—通过 WANOP 设备的所有流量以及加速和非加速连接的总数。这允许您监视从 LAN 传输到 WAN 的总流量。
- 压缩比-前 10 个服务类别.
- 汇总链路吞吐量-局域网和广域网。

整合压缩率：

此报表显示传输到 WANOP 的所有流量的合并压缩比，以及加速和非加速连接的总数。它还显示设备中 WANOP 服务的正常运行时间。



汇总链路吞吐量：

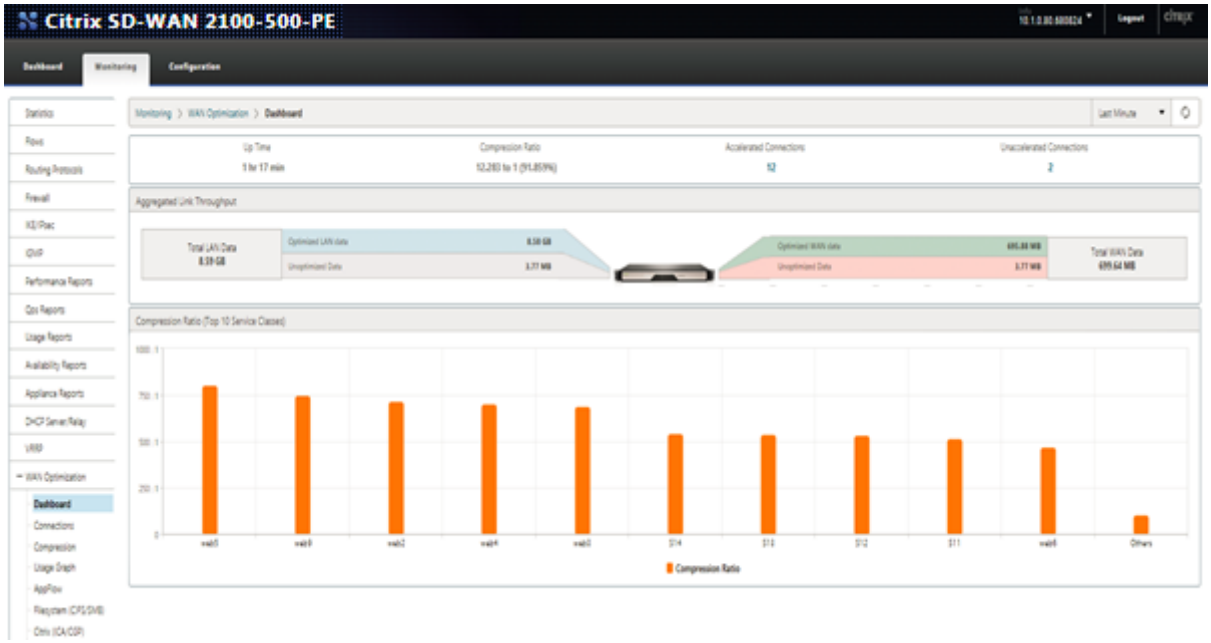
此报表显示传输到 WANOP 的总流量以及在两端优化和未优化数据类别中通过分解传输的总流量。

压缩率（前 **10** 个服务类别）：

在 Citrix SD-WAN 设备 GUI 中，您可以通过导航到 监 控” > “W **AN** 优化 来检查连接详细信息和压缩比（每个服务级仪表板）。此自动选择仪表板节点，并以仪表板的形式提供概述。

图形显示按服务类分类的流量压缩比前 10 个值。

此时将显示一个额外的“其他”栏，该栏显示除了前 10 个服务类压缩比报告之外，作为系统一部分的所有其他加速连接的压缩比率。



HTTP 加速

April 23, 2021

Citrix SD-WAN WANOP 加速器使用各种零配置优化来加快 HTTP 流量。这反过来会加速使用 HTTP 协议的网页和任何其他应用程序（文件下载、视频流、自动更新等）。

加速 HTTP 的优化包括压缩、流量成形、流量控制和缓存。

压缩

HTTP 是 Citrix SD-WAN WANOP 多级压缩的理想应用程序。

静态内容（包括标准 HTML 页面、图像、视频和二进制文件）会接收不同量的首次压缩，通常对于预压缩的二进制内容为 1:1，对于基于文本的内容，通常为 2:1 或更多。从第二次看到对象时开始，两个最大的压缩引擎（基于内存的压缩和磁盘基压缩）提供极高的压缩比，较大的对象的压缩比为 1000:1 或更多。如此高的压缩比，WAN 链路不再是限制因素，服务器、客户端或 LAN 成为瓶颈。

设备在压缩机之间动态切换，以提供最佳性能。例如，设备在 HTTP 标头上使用较小的压缩机，在 HTTP 主体上使用较大的压缩机。

动态内容（包括 HTTP 标头和动态生成的页面）是由处理较小匹配的三个压缩引擎压缩的。第一次看到页面时，压缩是好的。当看到前一页上的变体时，压缩会更好。

流量成形

HTTP 由交互式和批量流量组成。每个用户的流量都是两者的混合，有时相同的连接包含两者的混合。流量成形器无缝和动态地确保每个 HTTP 连接获得其公平的链路带宽份额，防止批量传输以牺牲交互式用户为代价垄断链接，同时确保批量传输获得交互式连接不使用的任何带宽。

流量控制

高级重传算法和其他 TCP 级优化可以在延迟和丢失的情况下保持响应能力并保持传输速率。

视频缓存

版本 7.0 缓存中引入了视频文件的 HTTP 缓存涉及将 HTTP 对象保存到本地存储，并将其提供给本地客户端，而无需从服务器重新加载它们。

缓存和压缩有什么区别？虽然缓存提供了类似于压缩的加速，但这两种方法是不同的，使它们相互补充。

- 压缩加快了从远程服务器传输的速度，如果不存在压缩，这种较高的数据速率会给服务器带来更高的负载。缓存可防止从服务器传输，并减少服务器上的负载。
- 压缩适用于任何数据流，这与之前的传输类似—如果您在远程服务器上更改文件的名称并再次传输，压缩将完美地工作。只有当客户端请求的对象和磁盘上的对象已知相同时，缓存才起作用-如果您更改远程服务器上的文件的名称并再次传输该文件，则不使用缓存副本。
- 压缩数据的传递速度不能超过服务器发送速度。缓存数据仅取决于客户端设备的速度。
- 压缩是 CPU 密集型的；缓存不是。

HTML5 的工作原理

April 23, 2021

HTML5 使用 HTTP，这是用于客户端和服务器之间通信的请求/响应协议。客户端启动 TCP 连接并使用它向服务器发送 HTTP 请求。服务器通过授予可用资源的访问权限来响应这些请求。客户端和服务器建立连接后，它们之间交换的消息仅包含 WebSocket 标头，而不包含 HTTP 标头。

HTML5 的基础结构由 WebSocket 组成，它进一步利用现有的 HTTP 基础结构，为客户端和 Web 服务器之间的通信提供轻量级机制。您通常在浏览器和 Web 服务器中实现 WebSocket 协议。但是，您可以将此协议用于任何客户端或服务器应用程序。

当客户端尝试使用 WebSocket 建立连接时，Web 服务器将 WebSocket 握手视为升级请求，并且服务器切换到 WebSocket 协议。WebSocket 协议允许浏览器和 Web 服务器之间频繁交互。因此，您可以使用此协议进行实时更新，例如股票指数和分数卡，甚至现场游戏。这是可能的，因为服务器采用标准化方式向客户端发送未经请求的响应，同时保持开放连接，以便客户端浏览器和服务器之间进行双向持续通信。

> 注意
>
> 您还可以通过使用其他各种技术，如彗星，以非标准化的方式实现这种效果。有关彗星的更多信息，请参阅http://en.wikipedia.org/wiki/Comet_(programming)。

WebSocket 协议通过 TCP 端口 80 和 443 进行通信。这有助于在使用防火墙阻止非 Web Internet 连接的环境中进行通信。此外，WebSocket 有自己的碎片机制。一个 WebSocket 消息可以作为多个 WebSocket 帧发送。

> 注意
>
> 如果服务器上的 Web 应用程序不支持，则无法使用 WebSocket。

HTML5 如何建立一个 webSocket 会话

支持 HTML5 的浏览器使用 JavaScript API 执行以下任务：

- 打开一个 WebSocket 连接。
- 通过 WebSocket 连接进行通信。
- 关闭 WebSocket 连接。

要打开 WebSocket 连接，浏览器会向服务器发送 HTTP 升级消息以切换到 WebSocket 协议。服务器接受或拒绝此请求。以下是示例客户端请求和服务器响应的片段：

- 客户端请求

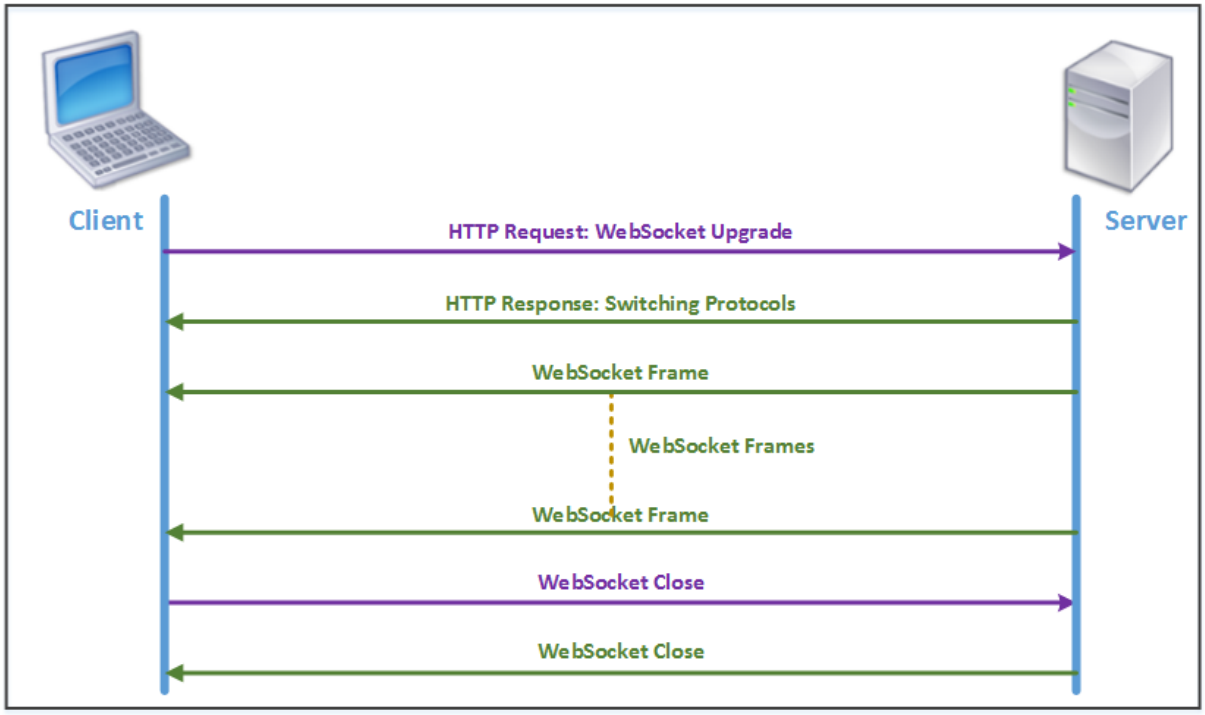
  示例

  ```
  pre codeblock GET /HTTP/1.1 Upgrade: websocket Sec-websocket-
  protocol: <List of protocols that the client supports over this
   websocket session, such as an application level protocol, for
   example ICA.> Sec-websocket-extensions: <List of extensions
  client wants applied to this session, such as compression.> Sec-
  Websocket-version: <Version of websocket protocol that the client
   intends to use.> <!--NeedCopy-->
  ```

- 示例服务器响应

  ```
  pre codeblock HTTP/1.1 101 Switching Protocols Upgrade: websocket
   Connection: Upgrade Sec-Websocket-Protocol: <One from the list
  of protocols in the client request.> Sec-Websocket-extensions:
  <List of extensions server accepts for session.> Sec-Websocket-
  version: <Version of websocket protocol that the server supports
  .> <!--NeedCopy-->
  ```

下图显示了客户端和服务器之间交换的消息顺序：



在 HTML5 连接期间，客户端和服务器之间交换以下消息：

- 客户端发送 HTTP 请求以升级 WebSocket。
- 服务器响应客户端请求并切换到 WebSocket 协议。
- 服务器将 WebSocket 帧发送到客户端。
- 客户端发送关闭 WebSocket 的请求。
- 服务器关闭 WebSocket。

互联网协议版本 **6 (IPv6)** 加速

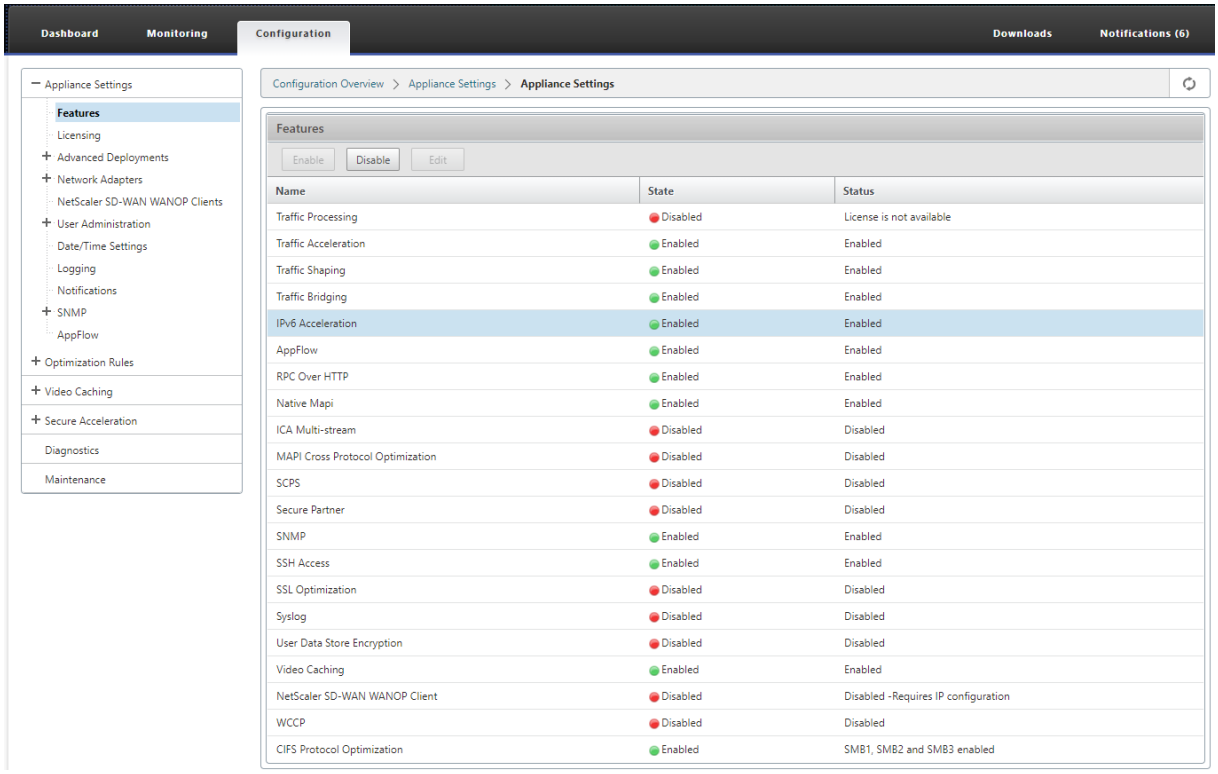
April 23, 2021

当您通过设备连接到 Internet 时，设备将被分配一个 IP 地址。IP 地址标识设备并指示其位置。连接到互联网的设备数量正在迅速增加。因此，很难使用现有版本的 Internet 协议 (IP) IPv4（使用 32 位地址）来管理 IP 地址的请求。通过使用 IPv4，可以为连接到互联网的设备分配约 43 亿个地址。

IPv6 通过使用 128 位地址和十六进制标签来标识 IPv6 网络上设备的网络接口来解决此问题。由于 IPv6 支持的 IP 地址远远多于 IPv4，组织和应用程序正在逐步引入对 IPv6 协议的支持。

IPv4 和 IPv6 协议不可互操作，这使得转换变得困难。要加速来自 Citrix SD-WAN WANOP 设备支持的各种应用程序的不断增加的 IPv6 流量，可以启用 IPv6 加速功能。

默认情况下，设备上禁用 IPv6。要在 Citrix SD-WAN WANOP 设备上启用 IPv6 加速，请导航到配置 > 设备设置 > 功能页面并启用 **IPv6** 加速功能。

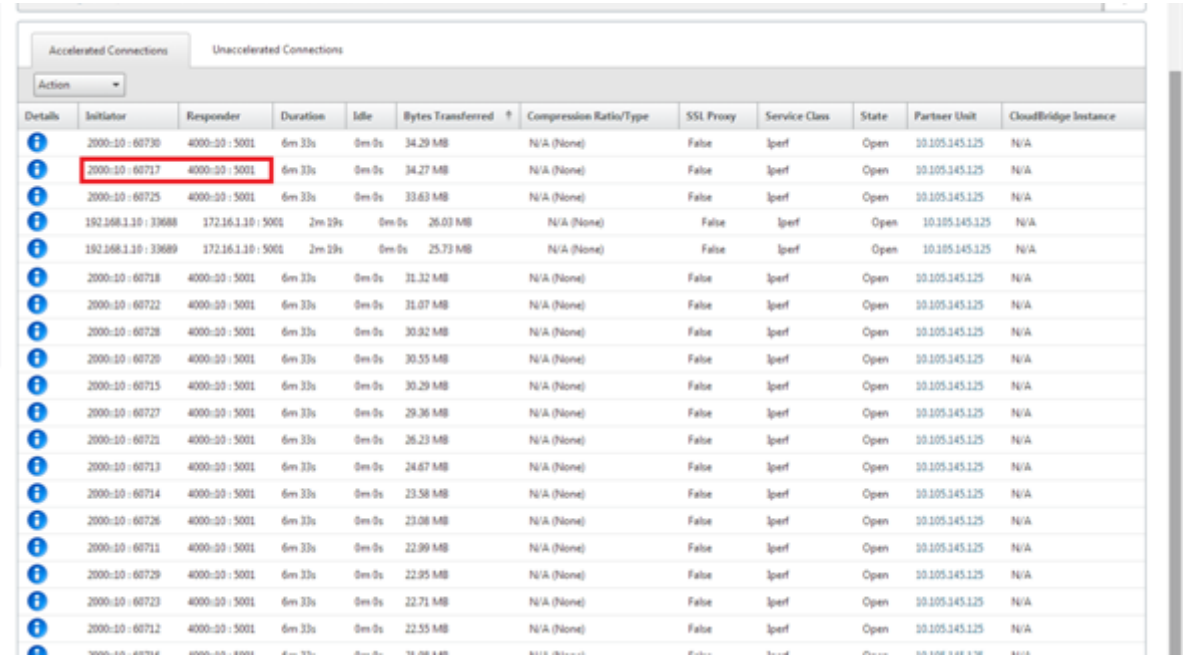


验证 **IPv6** 连接

在设备上启用 IPv6 加速后，设备会开始使用 IPv6 协议加速应用程序的流量。要确保设备正在加速 IPv6 流量，您可以监视设备上的此类连接。

要监视 IPv6 连接，请导航到 监视”选项卡。监视 选项卡的 连接 页面显示 IPv6 协议流量相关统计信息：

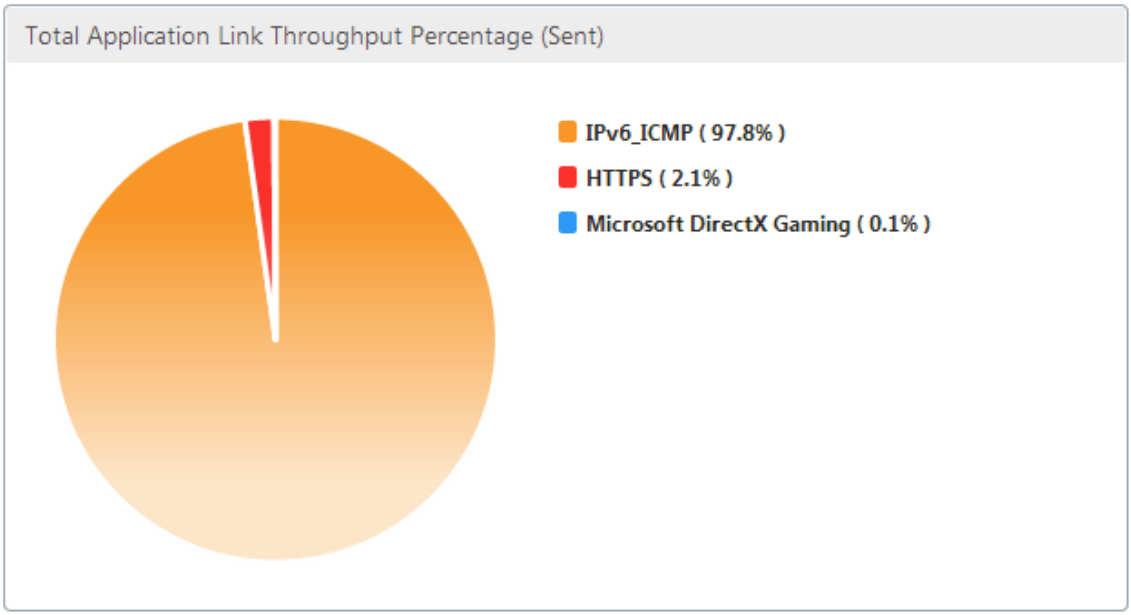
连接：“连接”页面列出了与设备建立的所有连接的详细信息。此页面由两个选项卡组成，即加速连接和未加速连接。“加速连接” 选项卡列出了设备正在加速的所有连接。您可以通过参考每个条目的 “启动程序” 和 “响应程序” 列来识别此选项卡中的 IPv6 流量。如果这些列包含十六进制 IP 地址值，则该条目表示 IPv6 连接，如以下屏幕截图所示。



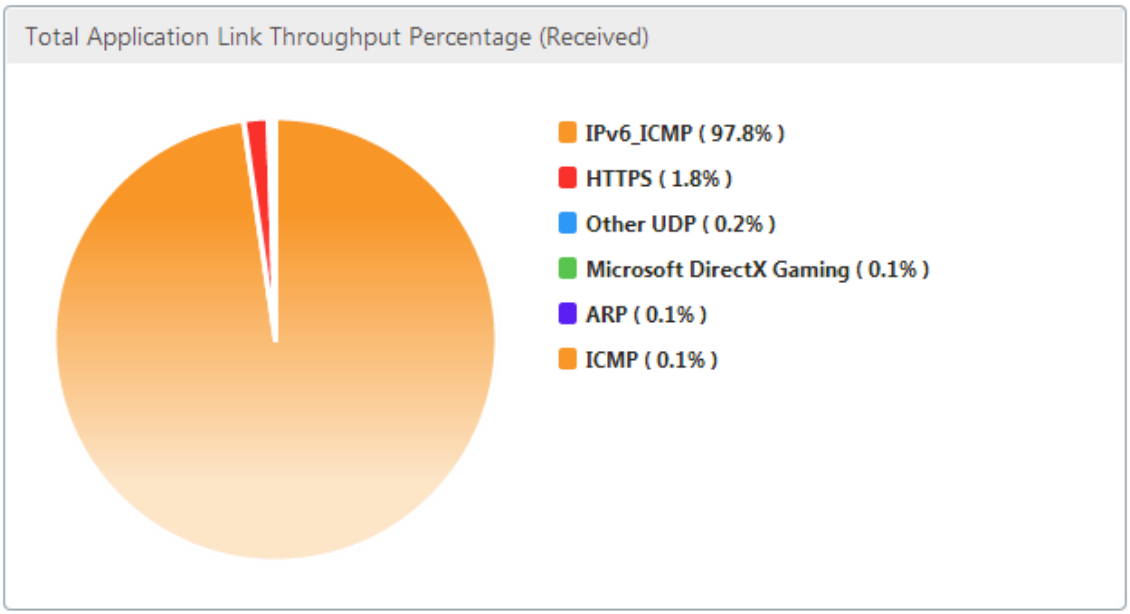
未加速的 IPv6 连接列在“未加速的连接”选项卡上。如果要加速这些连接，可能需要对设备上的应用程序参数进行故障排除和微调。与 加速连接 选项卡上一样，您可以通过引用每个条目的 启动 程序”和 响应程序 列来识别此选项卡上的 IPv6 连接。

热门应用程序：“热门应用程序”页面提供时间范围内的粒度，可用于以图形方式表示 Citrix SD-WAN 设备提供的各种应用程序的流量吞吐量。默认情况下，流量吞吐量按最后一分钟显示。但是，您可以通过从页面标题栏的可用列表中选择“最后一分钟”、“最后一小时”、“最后一天”、“最后一周”或“最后一个月”来更改时间范围。此页面有三个选项卡：顶部应用程序图表、上次重新启动以及 活动应用程序（自上次重新启动）。“顶级应用程序图表”选项卡包含以下统计信息：

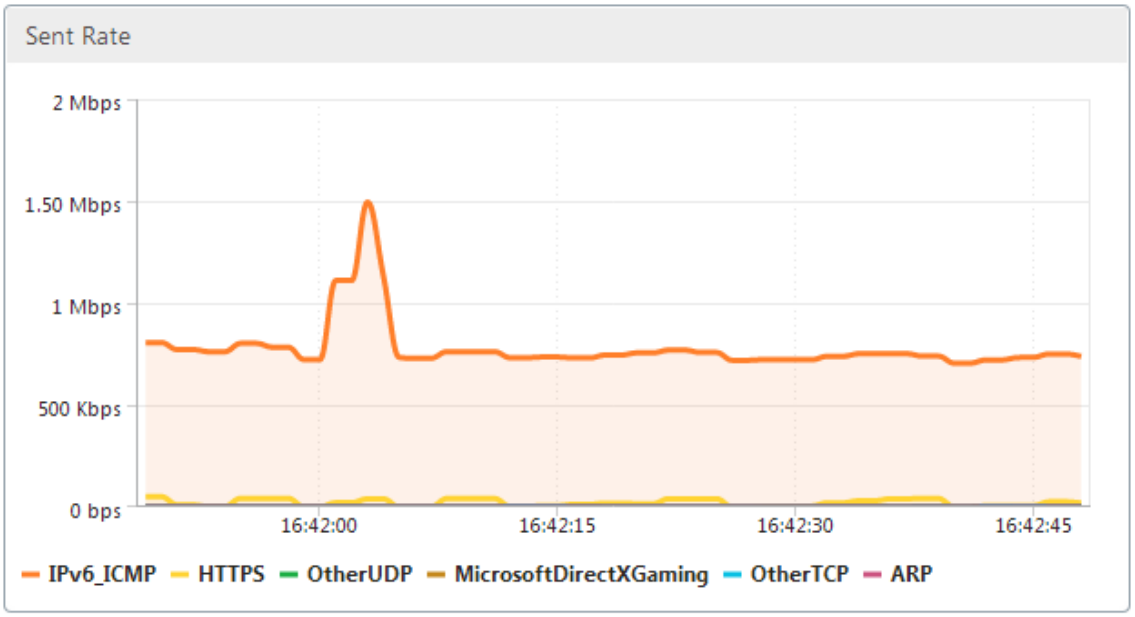
- 应用程序链接总吞吐量百分比（已发送）：这是一个饼图，描述了设备已发送到每个应用程序的流量百分比。如果设备为使用 IPv6 协议的应用程序发送了相当大比例的流量，则该应用程序的流量百分比在此图中显示。



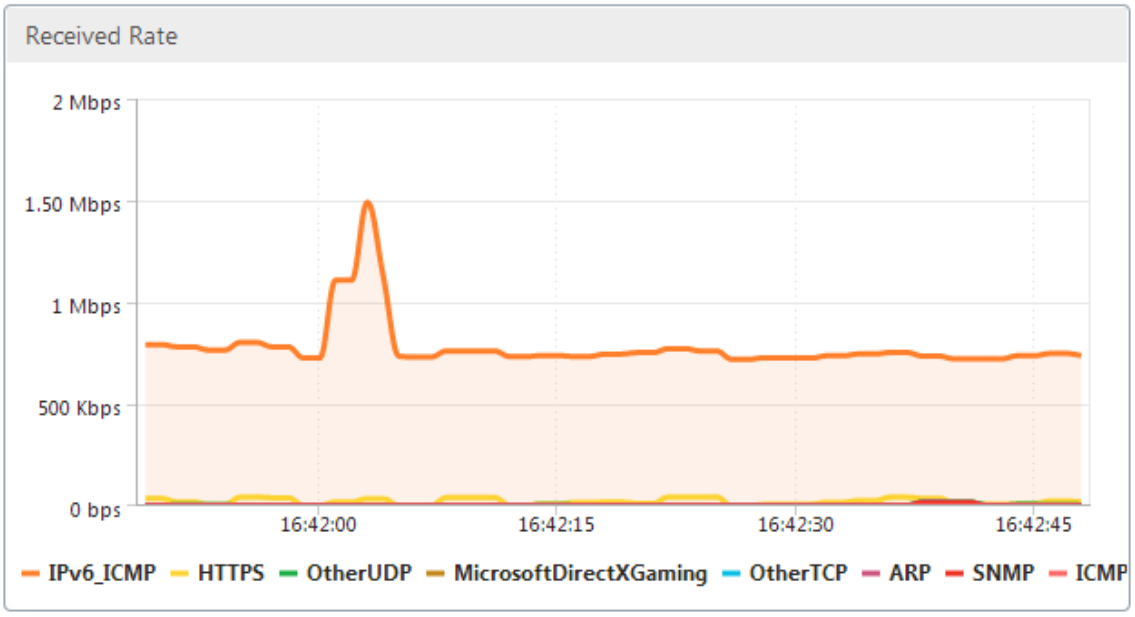
- 应用程序链接总吞吐量百分比（已接收）：这是一个饼图，描述了设备从每个应用程序接收的流量百分比。如果设备从使用 IPv6 协议的应用程序接收了很大百分比的流量，则图形显示应用程序生成的流量百分比。



- 发送速率：这是一系列数据的堆叠图，描述了设备向每个应用程序发送流量的速率（以每秒位数为单位）。如果设备已使用 IPv6 协议向应用程序发送数据，则此图中还会绘制一系列描绘使用 IPv6 协议的每个应用程序。



- 接收速率：这是一系列数据的堆叠图，描绘了设备从每个应用程序接收流量的速率（以位每秒为单位）。如果设备从使用 IPv6 协议的应用程序接收了数据，则此图中还会绘制一系列描绘使用 IPv6 协议的每个应用程序。



- 顶部应用程序表：这是每个应用程序的统计数据表。该表列出了设备为其提供流量服务的所有应用程序，以及以位每秒为单位的发送和接收速率、发送和接收的总字节数、应用程序的流量百分比以及设备为应用程序服务流量的速率。如果设备已为使用 IPv6 协议的应用程序提供流量，则此表中将列出该应用程序及其统计信息。

Top Applications

Application	Sent Rate (bps)	Received Rate (bps)	Total Bytes Sent	Total Bytes Received	Total %	Order
IPv6_ICMP	719.56 K	719.56 K	5.4 M	5.4 M	98.3	1
HTTPS	10.57 K	9.64 K	79.3 K	72.35 K	1.38	2
Microsoft DirectX Gaming	416	416	3.14 K	3.14 K	0.06	4
Other TCP	312	312	2.35 K	2.35 K	0.04	5
Other UDP	128	1.7 K	984	12.73 K	0.12	3
ARP	24	488	232	3.66 K	0.04	6
SNMP	0	496	0	3.76 K	0.03	7
ICMP	0	376	0	2.84 K	0.03	8

- 应用程序组：这是每个应用程序及其应用程序组和父应用程序（如果有）的统计信息表。该表列出了为应用程序发送和接收的字节。每个应用程序及其应用程序组和父应用程序都显示为超链接。如果单击超链接，则会显示您单击的链接的统计信息的细节。如果设备已为使用 IPv6 协议的应用程序提供流量，则此表中将列出该应用程序及其统计信息。

Application Groups

Application	Application Group	Parent Application	Bytes Sent	Bytes Received
IPv6_ICMP	IP Protocols	IPv4	5.4 M	5.4 M
HTTPS	Web, Security Protocols	TCP	79.3 K	72.35 K
Microsoft DirectX Gaming	Games	TCP	3.14 K	3.14 K
Other TCP	N/A	N/A	2.35 K	2.35 K
Other UDP	N/A	N/A	984	12.73 K
ARP	Legacy Or Non-IP	N/A	232	3.66 K
SNMP	Network Management, Infrastructure	UDP	0	3.76 K
ICMP	Infrastructure, IP Protocols	IPv4	0	2.84 K

自上次重新启动 以来”选项卡包含自重新启动设备以来应用程序流量的统计信息。该选项卡包含应用程序链接总吞吐量百分比（已发送）和应用程序链接总吞吐量百分比（已接收）图形以及热门应用程序和应用程序组表，其中描述的统计数据与“顶部应用程序图表”选项卡类似，但包含设备重新启动后的数据。活动应用程序（自上次重新启动以来）选项卡包含一个列出设备重新启动以来所有活动应用程序的表。此表包含有关发送和接收速率、发送和接收的总字节数以及为应用程序发送和接收的总数据包的详细信息。

链接定义

April 23, 2021

链接定义使设备能够防止 WAN 链接上的拥塞和丢失，并执行流量调整。链接定义指定与已定义的链接关联的流量、允许在链接上接收的流量的最大带宽以及通过链接发送的流量的最大带宽。该定义还将流量标识为入站或出站流量以及 Wanside 或 LAN 端流量。将通过设备流动的所有流量与链接定义列表进行比较，第一个匹配定义标识流量所属的链接。

通过执行快速安装过程，您可以自定义设备的默认链接定义。然后，您定义了设备到 WAN 的链接及其到 LAN 的链接。对于简单的内联部署，无需进一步配置链接定义。其他类型的部署需要额外配置链接定义。

每个链路都有两个带宽限制，代表发送速度和接收速度。只有当已知链路速度时，设备才能以完全正确的速度将流量注

入链路，从而消除因尝试发送过多而导致的拥塞和数据包丢失，或因发送过少而导致的性能损失。当放置在快速 LAN 和较慢的 WAN 之间并充当虚拟网关时，设备能够接收流量的速度超过 WAN 的接收速度，从而造成流量积压。此积压的存在使设备能够选择接下来要发送的数据包，而这种选择反过来使流量变形成为可能。除非有来自多个流的数据包可供选择，否则无法将一个流优于另一个流。因此，流量调整取决于虚拟 Gateway 的存在并正确设置带宽限制。

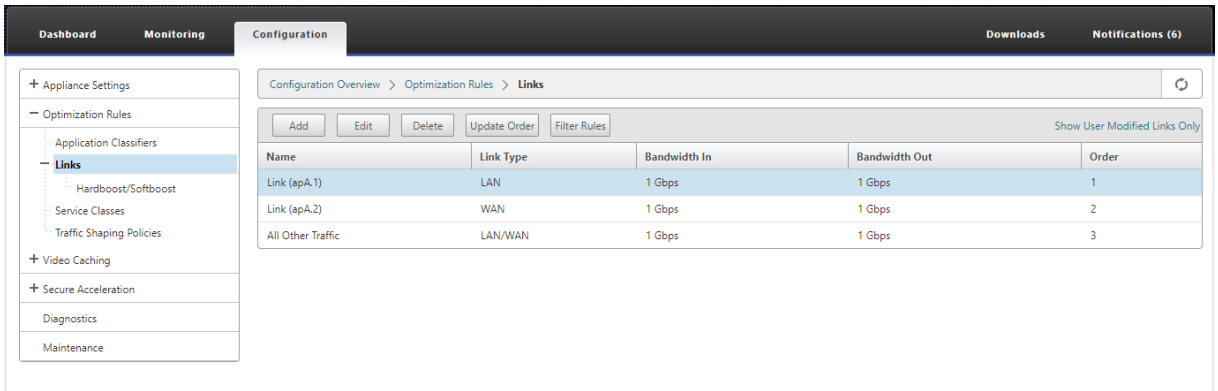
> 注意
>
> 链路定义通常适用于与加速的桥接端口对的连接。主板端口和 Aux1 两个端口也可以被定义为链接，但这样做很少用于任何目的，因为它们用于管理和作为高可用性和组模式的后台通道，而不是 WAN 流量。
>
> 重要
>
> 重要提示：出于链接定义的目的，链接 是物理链接，具有自己的带宽容量。它通常是离开建筑物的电缆。请记住以下几点：
>
> - VLAN 不是一个链接。
> - 虚拟链接不是链接。
> - 隧道不是一个连接。

默认链接定义

导航到 配置 > 优化规则 > 链接 以查看当前定义的链接。默认情况下定义以下链接。

1. **apA.1**, 加速桥上的两个端口之一.
2. **apA.2**，加速桥上的另一个端口。
3. 如果该系统具有双加速桥梁，则也存在 apB.1 和 apB.2。
4. “所有其他流量”，它不是真正的链接，但是对于与任何实际链接定义不匹配的流量而言是一个全面的。

链接在此页面上显示的顺序非常重要。确定数据包属于哪个链接时，设备会按顺序测试链接，然后选择第一个匹配链接。这意味着允许重叠定义，并且链接中的最后一个定义可以匹配所有流量，用作默认链接。要更改订单，请单击 更新订单。



管理流量成形中的链接定义

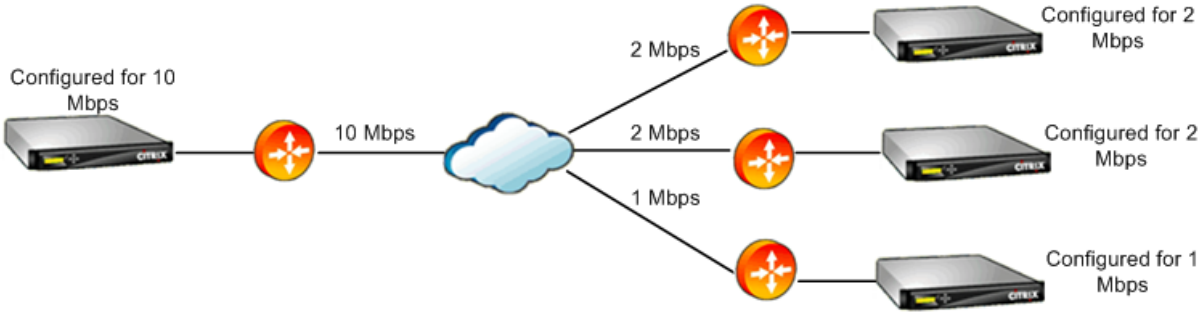
April 23, 2021

要管理链接，流量成形程序需要以下信息：

- 发送和接收方向的链接速度。
- 链接是 WAN 链接还是 LAN 网络。
- 一种区分链路流量与其他流量的方法。
- 流量在链接上流动的方向。

链路速度—链路速度总是指物理链路的速度。在 WAN 链接的情况下，WAN 段的速度是使用 Citrix SD-WAN WANOP 设备在构建中终止的。不考虑链接的另一端的速度。例如，下图显示了一个由四个设备组成的网络。每个设备的传入和传出带宽设置为其本地 WAN 段速度的 95%，而不考虑远程端点的速度。

图 1. 本地带宽限制跟踪本地链路速度



将带宽限制设置为链路速度的 95% 而不是 100% 的原因是为了允许链路开销（很少有链路可以以 100% 的发布速度传输数据），并确保设备稍慢于链路，以便成为一个轻微的瓶颈。除非流量成形器是连接中的瓶颈，否则流量成形不会有效。

区分不同类型的流量—在每个链接定义中，您必须声明该定义是应用于 WAN 链接还是 LAN 网络。

流量成形程序需要知道数据包是否在 WAN 上行驶，如果是，则需知道在哪个方向上行驶。要提供此信息，请执行以下操作：

- 对于简单的内联部署，您声明加速桥的一个端口属于 WAN 链接，而另一个端口属于 LAN。
- 在其他部署模式下，设备检查 IP 地址、MAC 地址、VLAN 或 WCCP 服务组。（请注意，尚不支持 WCCP 服务组的测试。）
- 如果站点有多个 WAN，则本地链接定义必须包含允许设备区分流量和不同 WAN 的规则。

配置链接定义

April 23, 2021

链接定义排列在一个有序列表中，每个链接有一个条目，从上到下对每个进入或离开设备的数据包进行测试。第一个匹配定义确定数据包所属的链接。在每个链接定义中都有一个有序的规则列表，这些规则也会从上到下进行测试。将每个数据包与这些规则进行比较，如果它与其中一个数据包匹配，则该数据包将被视为通过该链接传递。

在单个规则中，所有字段都是 ANded 一起的，因此所有指定值都必须匹配。所有字段默认为“任意”，即始终匹配的通配符条目。当字段由列表（例如 IP 子网列表）组成时，列表条目将在一起。也就是说，如果任何元素匹配，整个列表被视为匹配。

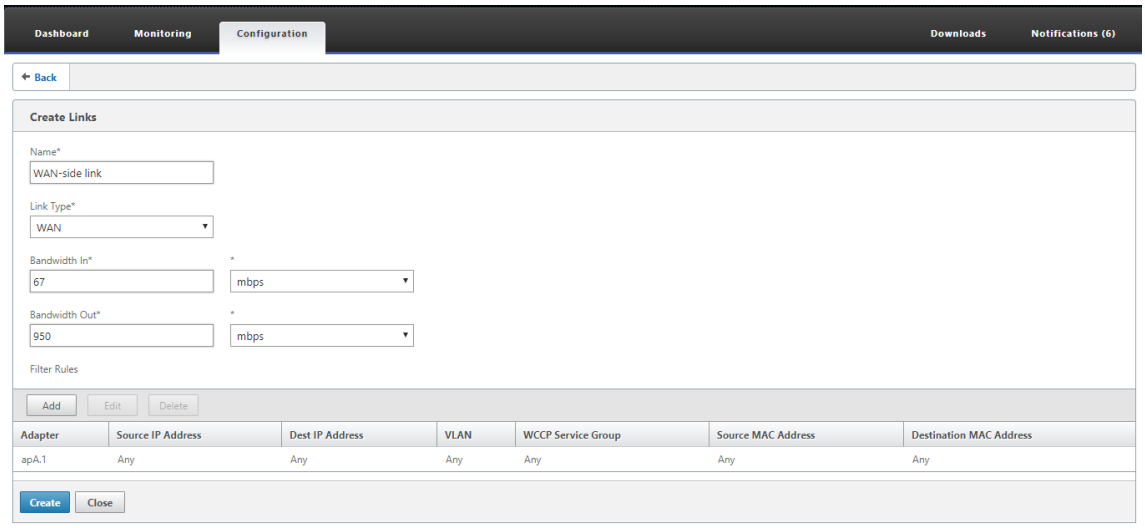
链接可以基于与流量关联的以太网适配器、源和目标 IP 地址、VLAN 标签、WCCP 服务组（仅适用于 WCCP-GRE）以及源和目标以太网 MAC 地址。简单的内联部署可能只识别 LAN 端和 Wan 端加速桥接端口 (aP.1 和 apA.2)，而复杂的数据中心部署可能需要使用提供的大部分选项来消除流量歧义。

根据其 IP 地址定义链接是可能的，除非使用冗余链接。由于给定的数据包可能遍历主动-备用或主动-主动双链路部署中的链路，因此必须使用其他一些方法来确定数据包正在使用的链路。如果使用双桥，则一条链路的流量可以通过 apA，另一条通过 apB，并且可以通过适配器来定义链路。如果两个链接由不同的路由器提供，则可以使用路由器的 MAC 地址分开流量。当所有其他故障时，可以使用 WCCP-GRE，路由器可以为每个 WAN 链接使用不同的服务组，从而使 Citrix SD-WAN WANOP 单元能够按服务组分辨链路流量。

Citrix 建议对简单的内联部署进行基于端口的链接定义，对所有其他部署进行基于 IP 的链接定义。

要配置链接定义：

1. 导航到“配置”> “优化规则”> “链接”，然后单击“添加”。



2. 输入以下参数的值：

   - 名称：链接的描述性名称，也可以描述它是 LAN 侧链接还是 WAN 侧链接。

- 链接类型：链接类型，LAN 或 WAN。
- 带宽入：传入带宽限制。
- 带宽输出：传出带宽限制。

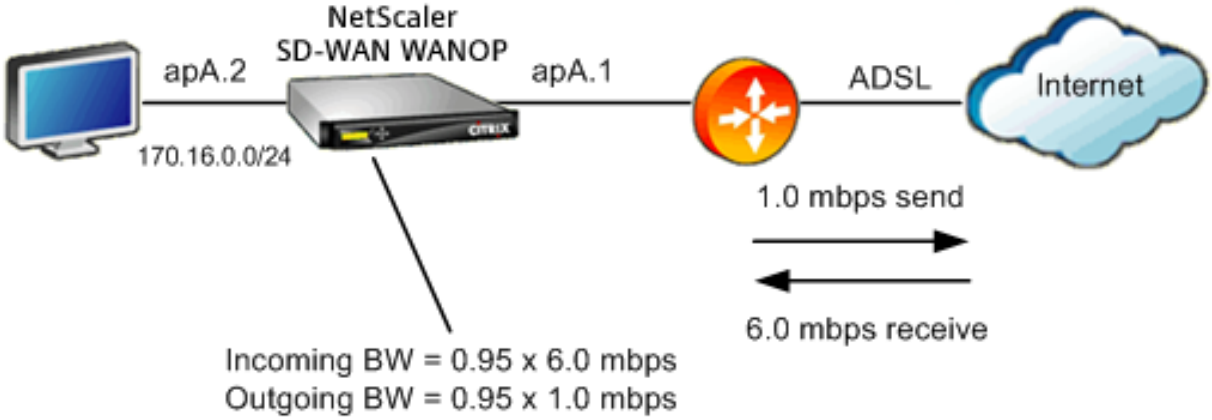
3. 在 筛选规则 部分中，单击 添加 并输入以下参数的值：
   - 适配器：指定适配器列表（以太网端口）。当链接可以通过以太网适配器识别时，这简化了配置。
   - 源 **IP** 地址：对于输入本机的数据包，将考虑源 IP 规则（忽略退出本机的数据包）。在这些数据包上，Src IP 字段中的规则与 IP 标头中的源地址字段进行比较。该规则指定 IP 地址或子网的列表。还支持负面匹配，例如“排除 10.0.0.1”。
   - 目标 **IP** 地址：将针对退出单元的数据包考虑目标 IP 规则（忽略进入单元的数据包）。在这些数据包上，Dst IP 字段中的规则与 IP 标头中的目标地址字段进行比较。该规则指定 IP 地址或子网的列表。还支持负面匹配，例如“排除 10.0.0.1”。
   - **VLAN**： VLAN 规则应用于进入或退出本机的数据包的 VLAN 标头。
   - **WCCP** 服务组： WCCP 服务组规则适用于进入或离开设备的 GREP 封装的 WCCP 数据包。（此规则不适用于 L2 WCCP。）
   - 源 **MAC** 地址：源 MAC 地址用作筛选条件。
   - 目标 **MAC** 地址：用作分析条件的目标 MAC 地址。
4. 单击创建。

   流量分类器以专门的方式使用 Src IP 和 Dest IP 字段（这同样适用于 Src MAC 和 DST MAC）：
   - 仅在进入设备的数据包上检查 Src 字段。
   - 仅在离开设备的数据包上检查 DST。

内联链接

大多数 Citrix SD-WAN WANOP 设备使用简单的内联部署，其中每个加速桥只提供一个 WAN 链接。这是最简单的配置模式。

简单的内联链接



在上图中，通过加速桥梁的所有流量都假定为 WAN 流量。该链接是一个 ADSL 链接，具有不同的发送和接收速度（向下 6.0 mbps，向上 1.0 mbps）。广域网连接到加速桥接端口 apA.1，LAN 连接加速桥接端口 apA.2。

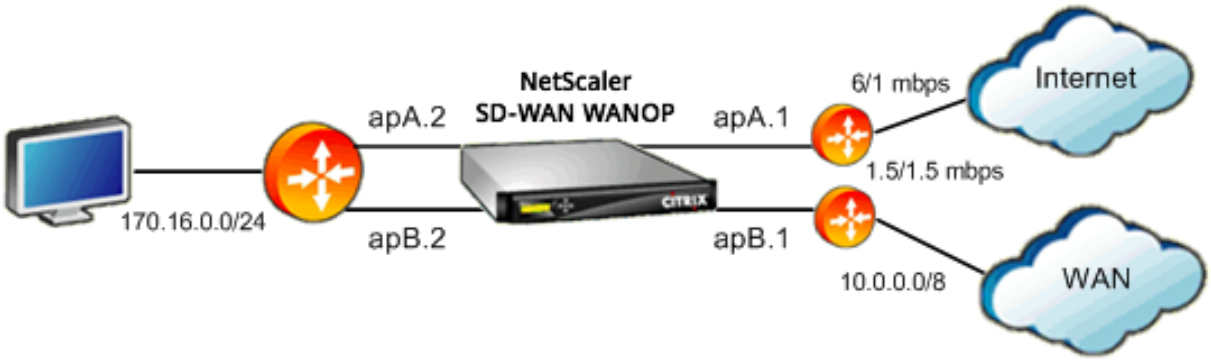
定义 Wan-side 链接 (aP.1) 的任务是：

1. 为广域网指定一个描述性名称，例如“广域网至总部 (aP.1)”。
2. 将类型设置为“WAN”。
3. 将传入和传出带宽限制设置为标称链路速度的 95%。
4. 验证是否已定义指定 WAN 以太网适配器的规则，在此示例中，该适配器为 apA。
5. 单击创建。

局部网络端链接 (apA.2) 的任务类似：

1. 为其指定一个描述性名称，例如“本地局域网 (apA.2)”。
2. 将类型设置为“LAN”。
3. 将传入和传出带宽限制设置为标称以太网速度的 95%（95 mbps 或 950 mbps）。
4. 验证是否存在指定 LAN 以太网适配器的规则，在此示例中，该适配器为 apA.2。
5. 单击创建。

具有双桥的内联部署



配置类似于简单的内联链接配置，但该站点除了 ADSL 互联网链接外还有第二个链接，即 T1 链接到企业广域网。Citrix SD-WAN WANOP 设备具有两个加速桥，每个 WAN 链接一个。

配置几乎与单桥箱一样简单，还有以下附加步骤：

1. 编辑 apB 上的第二个 WAN 链接，在本例中为 apB.1。将类型设置为“WAN”。将链路带宽设置为 1.5 mbps T1 速度的 95%，并为链接指定一个新名称，例如“WAN 到总部”。
2. 在“局域网”定义中添加指定 apB.2 的规则，并删除 apB.2 的默认链接定义。（或者，您可以编辑 apB.2 的默认链接定义，将其指定为 LAN 链接，就像对 apA.2 所做的那样。）

非内联链接

对于简单的内联部署（每个加速桥只提供一个 WAN）以外，请使用 IP 子网而不是桥接端口来区分 LAN 流量和 WAN 流量。此方法对于仅使用单桥端口的单臂部署至关重要。IP 子网有时也适用于内联部署，尤其是当设备提供多个 WAN 时。但是，对于简单的内联部署，基于端口的链接更容易定义。

流量分类器在检查 Src IP 和 DST IP 时应用专门的约定：

- 仅在进入设备的数据包中检查 Src IP 字段。
- 仅在离开设备的数据包中检查 DST IP 字段。

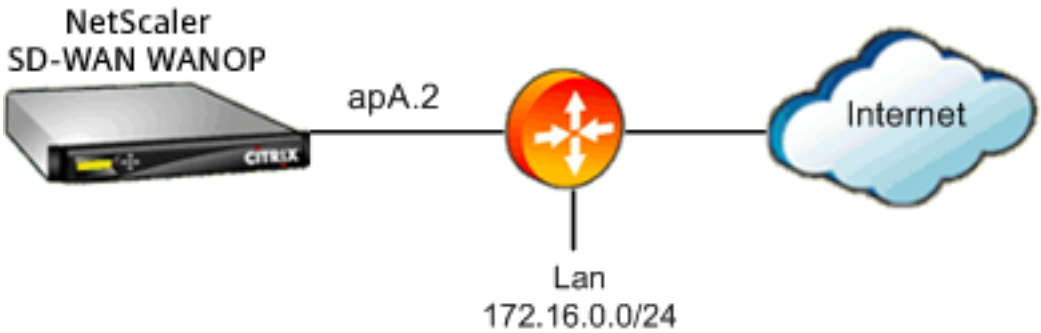
这种约定有时会令人困惑，但它允许隐式地将数据包传输方向视为定义的一部分。

在链接定义中使用 **IP** 地址

要使用基于 IP 的规则配置简单的内联 LAN 定义，您可以使用 LAN 子网来定义 LAN 和 WAN 链接，而不必指定以太网端口：

- 为 LAN 链接定义创建规则，并在 Src IP 字段中指定 LAN 子网。
- 为 WAN 链接定义创建规则，并在 Dst IP 字段中指定 LAN 子网（而不是 WAN 子网）。

WCCP 和虚拟内联模式



使用基于 IP 的规则配置 WCCP 或虚拟内联部署与在链接定义中使用 IP 地址相同，因为 LAN 和 WAN IP 子网是相同的。

使用 WCCP-GRE 时，GRE 标头将被忽略，并使用封装的数据包中的 IP 标头。因此，此相同的链接定义适用于 WCCP-L2、WCCP-GRE、内联和虚拟内联模式。

(WCCP 和虚拟内联模式需要配置路由器。WCCP 还要求在配置：高级部署页面上进行配置。)

使用 **Citrix Application Delivery Management** 管理和监视

December 15, 2022

Citrix SD-WAN WANOP AppFlow 支持使 Citrix SD-WAN WANOP 设备实现灵活的自定义监视。

AppFlow 界面与 Citrix Application Delivery Management (ADM) 配合使用。Citrix ADM 使用 AppFlow 开放标准从设备接收详细信息。Citrix ADM 允许您监控、管理和查看网络中 Citrix SD-WAN 设备的分析。

Citrix ADM 支持各种设备，并且可以提供更完整的网络视图。Citrix SD-WAN WANOP 设备具有广泛的 WAN 流量视图，包括有关虚拟应用程序/虚拟桌面流量的详细统计信息，它提供了有关 WAN 用户体验的关键见解。

有关详细信息，请参阅使用 Citrix Application Delivery Management 管理 Citrix SD-WAN 实例。

虚拟应用/虚拟桌面的例子

在 Citrix Virtual Apps and Desktops 环境中，如果分支机构用户的性能较低，管理员可能需要监控虚拟应用程序或虚拟桌面上托管的网络、用户和应用程序。管理员可能需要询问以下问题：

- 网络的哪一部分导致了不良的用户体验？
- 识别已发布应用程序缓慢的简单方法是什么？
- 在给定时间段内，哪些虚拟通道消耗的带宽最多？
- 在给定时间段内，哪些虚拟桌面或虚拟应用程序用户消耗的带宽最多？
- 对于给定的虚拟桌面用户，平均客户端和服务器端延迟以及平均抖动是多少？
- 按指定时间段内的正常运行时间和启动总次数，所有虚拟应用程序用户中最热门的应用程序是多少？
- 什么是数据中心延迟？

Citrix SD-WAN WANOP AppFlow 支持为上述所有问题提供了答案，例如，允许将拥挤的 WAN 链接与慢速服务器或慢速客户端区分开来。

Citrix Cloud Connector

April 23, 2021

Citrix SD-WAN WANOP 设备的 Citrix Cloud Connector 功能将企业数据中心连接到外部云和托管环境，使云成为企业网络的安全扩展。云托管应用程序似乎在一个连续的企业网络上运行。借助 Citrix Cloud Connector，您可以利用云提供商提供的容量和效率来增强数据中心。

Citrix Cloud Connector 使您能够将应用程序迁移到云中，以降低成本并提高可靠性。

Citrix SD-WAN WANOP 设备的 WAN 优化功能可加速流量，为跨企业数据中心和云运行的应用程序提供类似 LAN 的性能。

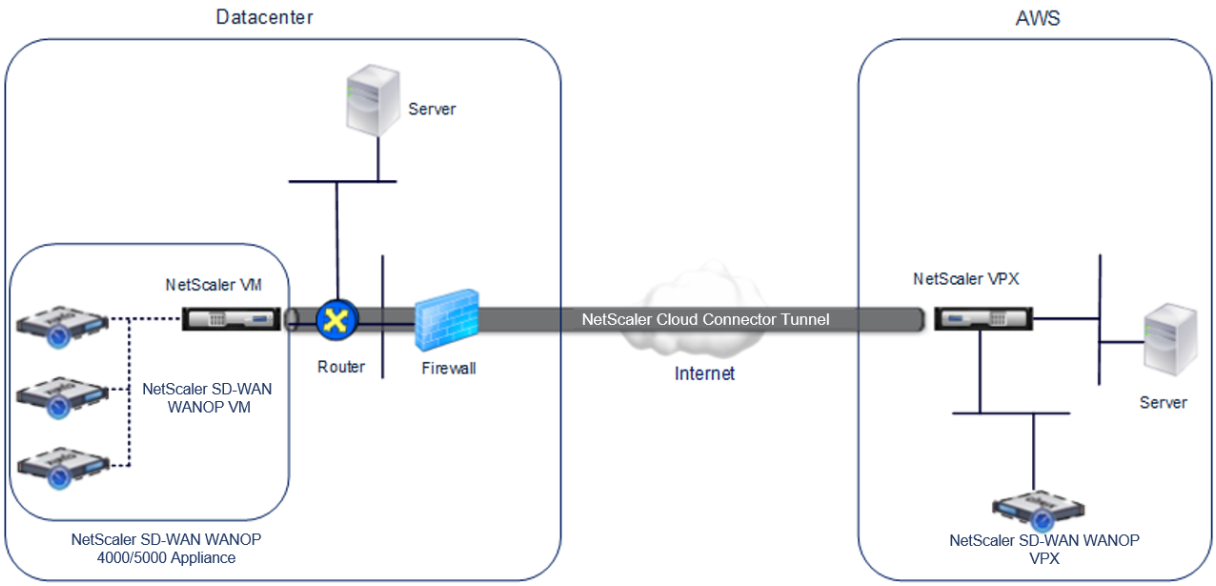
除了在数据中心和云之间使用 Citrix Cloud Connector 外，还可以使用它连接两个数据中心，以实现高容量安全和加速链接。

要实施 Citrix Cloud Connector 解决方案，可以通过设置名为 Citrix Cloud Connector 隧道的隧道将数据中心连接到另一个数据中心或外部云。

要将数据中心连接到另一个数据中心，您需要在两台设备之间设置 Citrix Cloud Connector
隧道，每个数据中心设置一台设备。

要将数据中心连接到外部云（例如，Amazon AWS 云），您需要在数据中心中的 Citrix SD-WAN WANOP 设备与驻留在云中的虚拟设备 (VPX) 之间设置 Citrix Cloud Connector 隧道。远程终点可以是 Citrix Cloud Connector 或具有白金许可证的 Citrix VPX。

下图显示了在数据中心和外部云之间设置的 Citrix Cloud Connector 隧道。



在其间设置 Citrix Cloud Connector 隧道的设备称为 Citrix Cloud Connector 隧道的端点或对等点。

Citrix Cloud Connector 隧道使用以下协议：

- 通用路由封装 (GRE) 协议
- 开放标准 IPsec 协议套件，处于传输模式

GRE 协议提供了一种机制，用于封装来自各种网络协议的数据包，以便通过另一种协议转发。GRE 用于：

- 连接运行非 IP 和非路由协议的网络。
- 跨广域网 (WAN) 桥梁。
- 为需要通过不同网络发送不变的任何类型的流量创建传输通道。

GRE 协议通过向数据包添加 GRE 标头和 GRE IP 标头来封装数据包。

Internet 协议安全性 (IPSec) 协议套件可确保 Citrix Cloud Connector 隧道中的对等方之间的通信。

在 Citrix Cloud Connector 隧道中，IPSec 可确保：

- 数据完整性
- 数据源身份验证
- 数据保密（加密）
- 防止重播攻击

IPsec 使用 GRE 封装的数据包加密的传输模式。加密由封装安全有效负载 (ESP) 协议完成。ESP 协议通过使用 HMAC 哈希函数确保数据包的完整性，并通过使用加密算法确保机密性。在对数据包进行加密并计算 HMAC 后，将生成 ESP 标头。ESP 标头插入 GRE IP 标头后，和, ESP 拖车插入在加密的有效负载的末尾.

Citrix Cloud Connector 隧道中的对等机使用 Internet 密钥交换版本 (IKE) 协议（IPSec 协议套件的一部分）协商安全通信，如下所示：

- 两个对等方使用以下身份验证方法之一相互进行身份验证：
  - 预共享密钥身份验证。在每个对等方上手动配置称为预共享密钥的文本字符串。对等方的预共享密钥相互匹配以进行身份验证。因此，要使身份验证成功，您必须在每个对等方上配置相同的预共享密钥。
  - 数字证书认证。启动程序（发件人）对等程序使用其私钥对邮件交换数据进行签名，而另一个 Receiver 对等程序则使用发件人的公钥验证签名。通常，在包含 X.509v3 证书的消息中交换公钥。此证书提供了一定级别的保证，即证书中表示的对等方的身份与特定公钥相关联。
- 然后，同行谈判达成协议：
  - 一种加密算法。
  - 加密密钥，用于在一个对等方中加密数据并在另一个对等方中解密数据。

安全协议、加密算法和加密密钥的协议称为安全关联 (SA)。SAS 是单向的（单纯）。例如，当两个对等方（CB1 和 CB2）通过连接器通道进行通信时，CB1 具有两个安全关联。一个 SA 用于处理外包，另一个 SA 用于处理入站数据包。

SAS 在指定的时间长度（称为生命周期）后过期。这两个对等方使用 Internet 密钥交换 (IKE) 协议（IPsec 协议套件的一部分）协商新的加密密钥并建立新的 SAS。有限生命周期的目的是防止攻击者破解钥匙。

此外，Citrix Cloud Connector
隧道端点上的 Citrix SD-WAN WANOP 实例可在隧道上提供广域网优化。

配置 **Citrix Cloud Connector** 隧道的先决条件

在 AWS 云与数据中心配置为单臂模式的 Citrix SD-WAN WANOP 设备之间设置 Citrix Cloud Connector 隧道之前，请验证以下任务是否已完成：

1. 确保数据中心中的 Citrix SD-WAN WANOP 设备已正确设置。有关在使用 WCCP/Virtual Inline 协议的单臂模式下部署 Citrix SD-WAN 设备的更多信息，请参阅具有一个 WAN 路由器的站点。
2. 在 AWS 云上安装、配置和启动 Citrix 虚拟设备（VPX 实例）。有关详细信息，请参阅在 AWS 上安装 NetScaler VPX。
3. 在 AWS 云上安装、配置和启动 Citrix SD-WAN WANOP 虚拟设备 (VPX) 实例。有关详细信息，请参阅在亚马逊 AWS 上安装 SD-WAN VPX S AMI。
4. 在 AWS 上，将 AWS 上的 Citrix SD-WAN WANOP VPX 实例绑定到 AWS 上的 Citrix VPX 实例中的负载平衡虚拟服务器。通过 Citrix SD-WAN WANOP VPX 实例发送流量时，需要此绑定才能通过 Citrix Cloud Connector 隧道实现 WAN 优化。

使用命令行界面创建负载平衡虚拟服务器：

在命令提示符下，键入：

- **enable ns mode** l2
- **add lb vserver** <cbvpxonaws_vs_name> ANY * * -**l2Conn** ON -**m** MAC

要在 **AWS** 上添加 **Citrix SD-WAN WANOP VPX** 实例作为服务并使用命令行界面将其绑定到负载平衡虚拟服务器，请执行以下操作：

在命令提示符下，键入：

- **add service** < cbvpxonaws_service_name> <cbvpxonaws_IP> ANY * -**cltTimeou**t 14400 -**svrTimeout** 14400
- **bind lb vserver** <cbvpxonaws_vs_name> <cbvpxonaws_service_name>

配置 **Cloud Connector** 隧道

April 23, 2021

要配置 Citrix Cloud Connector 隧道，请使用 Citrix VPX 设备的配置实用程序执行以下任务：

- 创建 **IPSec** 配置文件—IPSec 配置文件实体指定要由 Citrix Cloud Connector 隧道中的 IPSec 协议使用的 IPSec 协议参数，如 IKE 版本、加密算法、哈希算法和 PSK。
- 创建 **IP** 隧道并将 **IPSec** 配置文件与其关联—IP 隧道指定本地 IP 地址、远程 IP 地址、用于设置 Citrix Cloud Connector 隧道的协议以及 IPSec 配置文件实体。创建的 IP 隧道实体也称为 Citrix Cloud Connector 隧道实体。
- 创建 **PBR** 规则并将 **IP** 隧道与其关联-PBR 实体指定一组条件和一个 IP 隧道（Citrix Cloud Connector 隧道）实体。源 IP 地址范围和目标 IP 范围是 PBR 实体的条件。必须设置源 IP 地址范围和目标 IP 地址范围，以指定其流量要穿过 Citrix Cloud Connector 隧道的子网。例如，假设请求数据包来自数据中心子网上的客户端，并且发往 AWS 云中子网上的服务器。如果此数据包与数据中心中 Citrix SD-WAN WANOP 设备上 Citrix 虚拟设备上 PBR 实体的源和目标 IP 范围相匹配，则将考虑用于 Citrix SD-WAN WANOP 处理，该数据包通过与 PBR 实体关联的 Citrix Cloud Connector 隧道发送数据包。

要使用命令行界面创建 **IPSec** 配置文件，请执行以下操作：

在命令提示符下，键入：

- `**add ipsec profile** \<ipsec\\_profile\\_name\> -**encAlgo** AES -**hashAlgo** HMAC\\_SHA1 -**lifetime** 500 -**psk** \<password \>`

要使用命令行界面创建 **IP** 隧道并将 **IPSec** 配置文件绑定到它：

在命令提示符下，键入：

- `**add iptunnel** \<tunnel\\_name\> \<Remote CBC Public IP\> \<remote\\_cbs\\_Netmask\> \<lan\\_subnet\\_IP\> -**protocol** GRE -**ipsecProfileName** \<ipsec\\_profile\>`

使用命令行界面创建 **PBR** 规则并将 **IPSec** 隧道绑定到该规则：

在命令提示符下，键入：

- `**add ns pbr** \<pbr\\_name\> ALLOW -**srcIP** = \<local\\_lan\\_subnet\> -**destIP** = \<remote\\_lan\\_subnet\> -**ipTunnel** \<tunnel\\_name\>`
- **apply ns pbrs**

要使用配置实用程序创建 **IPSec** 配置文件，请执行以下操作：

1. 导航到 系统 > **Citrix Cloud Connector** > **IPSec** 配置文件。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在“添加 IPsec 配置文件”对话框中，设置以下参数：
   - 名称
   - 加密算法
   - 哈希算法
   - IKE 协议版本（选择 V2）
4. 使用以下 IPSec 身份验证方法之一，供两个对等方使用。
   - 对于预共享密钥身份验证方法，请设置预共享密钥存在参数。
   - 对于数字证书身份验证方法，请设置以下参数：
     - 公钥
     - 私有密钥
     - 对等公钥
5. 单击 **Create**（创建），然后单击 **Close**（关闭）。

要使用配置实用程序创建 **IP** 隧道并将 **IPSec** 配置文件绑定到它：

1. 导航到 系统 > **Citrix Cloud Connector** > **IP** 隧道。
2. 在 IPv4 隧道选项卡上，单击添加。
3. 在“添加 IP 通道”对话框中，设置以下参数：
   - 名称

- 远程 IP
- 远程屏蔽
- 本地 IP 类型（在本地 IP 类型下拉列表中，选择子网 IP）。
- 本地 IP（所选 IP 类型的所有配置 IP 都将填充到“本地 IP”下拉列表中。从列表中选择所需的 IP。）
- 协议
- IPsec 配置文件

4. 单击 **Create**（创建），然后单击 **Close**（关闭）。

使用配置实用程序创建 **PBR** 规则并将 **IPSec** 隧道绑定到该规则：

1. 导航到系统 > 网络 > **PBR**。
2. 在 PBR 选项卡上，单击添加。
3. 在创建 PBR 对话框中，设置以下参数：
   - 名称
   - 操作
   - 下一个跳类型（选择 IP 通道）
   - IP 通道名称
   - 源 IP 低
   - 源 IP 高
   - 目标 IP 低
   - 目标 IP 高
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。

   数据中心中 Citrix SD-WAN WANOP 设备上的新 Citrix Cloud Connector 隧道配置将显示在管理服务用户界面的“主页”选项卡上。

   AWS 云中 Citrix VPX 设备上相应的新 Citrix Cloud Connector 隧道配置将显示在配置实用程序中。

   Citrix Cloud Connector 隧道的当前状态将在“已配置的 Citrix SD-WAN WANOP”窗格中指示。绿色圆点表示通道已向上。红点表示通道已关闭。

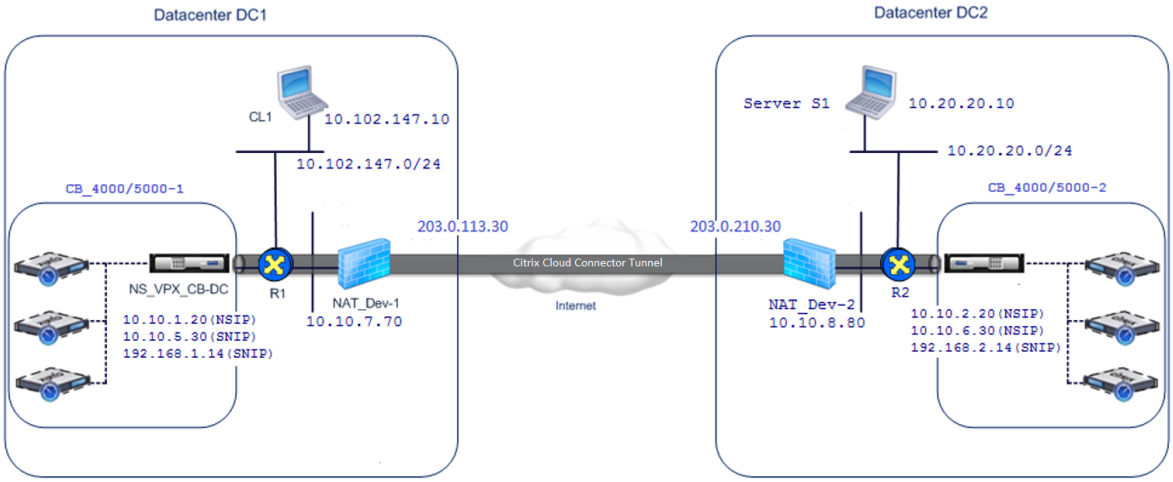
配置两个数据中心之间的 **Cloud Connector** 隧道

April 23, 2021

您可以在两个不同数据中心之间配置 Citrix Cloud Connector 隧道以扩展网络，而无需重新配置网络，并利用两个数据中心的功能。在两个地理位置上分隔的数据中心之间的 Citrix Cloud Connector 隧道使您能够实现冗余并防止设置出现故障。Citrix Cloud Connector 隧道有助于实现两个数据中心的基础架构和资源的最佳利用率。两个数据中心的可用应用程序对用户显示为本地应用程序。

要将数据中心连接到另一个数据中心，您可以在驻留在一个数据中心的 SD-WAN WANOP 4000/5000 设备与驻留在另一个数据中心的另一个 SD-WANOP 4000/5000 设备之间设置 Citrix Cloud Connector 隧道。

要了解如何在两个不同数据中心之间配置 Citrix Cloud Connector 接器隧道，请考虑在数据中心 DC1 中的 Citrix 设备 CB_4000/5000-1 与数据中心 DC2 中的 Citrix 设备 CB_4000/5000-2 之间设置 Cloud Connector 隧道的示例。



单臂模式下 (WCCP/PBR) 下的 CB_4000/5000-1 和 CB_4000/5000-2 功能。它们可实现数据中心 DC1 和 DC2 中的专用网络之间的通信。例如，CB_4000/5000-1 和 CB_4000/5000-2 可通过 Citrix Cloud Connector 隧道在数据中心 DC1 中的客户端 CL1 与数据中心 DC2 中的服务器 S1 之间进行通信。客户端 CL1 和服务器 S1 位于不同的专用网络上。

为了在 CL1 和 S1 之间进行正确的通信，L3 模式在 NS_VPX_CB_4000/5000-1 和 NS_CB_4000/5000-2 上启用，路由配置如下：

- 路由器 R1 具有通过 NS_VPX_CB_4000/5000-1 到达 S1 的路由。
- NS_VPX_CB_4000/5000_1 具有通过 R1 达到 NS_VPX-CB_4000/5000-2 的路由。
- S1 应该有一个通过 NS_VPX-CB_4000/5000-2 达到 CL1 的路由。
- NS_VPX-CB_ 4000/5000-2 具有通过 R2 达到 NS_VPX_CB_4000/5000-1 的路由。

下表列出了数据中心 DC1 中 CB_4000/5000-1 上的设置。

实体	名称	详细信息
客户端 CL1 的 IP 地址		10.102.147.10
NAT 设备 **NAT-Dev-1** 上的设置		
公共端的 NAT IP 地址		203.0.113.30*
私有端的 NAT IP 地址		10.10.7.70
CB_4000/5000-1 上的设置		
CB_4000/5000-1 的管理服务 IP 地址		10.10.1.10
CB_4000/5000-1 上运行的 **NS_VPX_CB_4000/5000-1** 上的设置		
NSIP 地址		10.10.1.20
SNIP 地址		10.10.5.30
Cloud Connector 隧道	Cloud_Connector_DC1-DC2	Citrix Cloud Connector 隧道的本地端点 IP 地址 = 10.10.5.30，Citrix Cloud Connector 隧道的远程端点 IP 地址 = 203.0.210.30* **GRE** 隧道详情 名称 = 云端连接器 _DC1-DC2 **IPSec** 配置文件详细信息 名称 = 云端连接器 _DC1-DC2，加密算法 = AES，哈希算法 = HMAC SHA1
基于策略的路由	CBC_DC1_DC2_PBR	源 IP 范围 = datacenter1 中的子网 = 10.102.147.0-10.102.147.255，目标 IP 范围 = datacenter2 中的子网 = 10.20.20.0-10.20.20.255，下一个跃点类型 = IP 隧道，IP 隧道名称 = CBC_DC1_DC2

* 这些应该是公有 IP 地址。

下表列出了数据中心 DC2 中 CB-4000/5000-2 上的设置。

实体	名称	详细信息
服务器 S1 的 IP 地址		10.20.20.10
NAT 设备 **NAT-Dev-2** 上的设置		
公共端的 NAT IP 地址		203.0.210.30*
私有端的 NAT IP 地址		10.10.8.80
CB_4000/5000-2 上的设置		
CB_SDX-1 的管理服务 IP 地址		10.10.2.10
CB_4000/5000-2 上运行的 **NS_VPX_CB_4000/5000-2** 上的设置		
NSIP 地址		10.10.2.20
SNIP 地址		10.10.6.30
Citrix Cloud Connector 隧道	Cloud_Connector_DC1-DC2	Citrix Cloud Connector 隧道的本地端点 IP 地址 = 10.10.6.30，Citrix Cloud Connector 隧道的远程端点 IP 地址 = 203.0.113.30* **GRE** 隧道详情 名称 = 云端连接器 _DC1-DC2 **IPSec** 配置文件详细信息 名称 = 云端连接器 _DC1-DC2，加密算法 = AES，哈希算法 = HMAC SHA1
基于策略的路由	CBC_DC1_DC2_PBR	源 IP 范围 = datacenter2 中的子网 = 10.20.20.0-10.20.20.255，目标 IP 范围 = datacenter1 中的子网 = 10.102.147.0-10.102.147.255，下一个跃点类型 = IP 隧道，IP 隧道名称 = CBC_DC1_DC2

* 这些应该是公有 IP 地址。

以下是 Citrix Cloud Connector 隧道中的流量：

1. 客户端 CL1 向服务器 S1 发送请求。
2. 该请求到达运行在 Citrix SD-WAN WANOP 设备 CB_4000/5000-1 上的 Citrix 虚拟设备 NS_VPX_CB_4000/5000-1。

3. NS_VPX_CB_4000/5000-1 将数据包转发到在 Citrix SD-WAN WANOP 设备 CB_4000/5000-1 上运行的 SD-WAN WANOP 实例之一以进行 WAN 优化。在处理数据包之后，SD-WAN WANOP 实例将数据包返回到 NS_VPX_CB_4000/5000-1。
4. 请求数据包匹配 PBR 实体 CBC_DC1_DC2_PBR（在 NS_VPX_CB_4000/5000-1 中配置）中指定的条件，因为请求数据包的源 IP 地址和目标 IP 地址分别属于在 CBC_DC1_DC2_PBR 中设置的源 IP 范围和目标 IP 范围。
5. 由于隧道 CBC_DC1_DC2_PBR 绑定到 CBC_DC1_DC2_PBR，设备准备要通过云连接器 _DC1-DC2 隧道发送的数据包。
6. NS_VPX_CB_4000/5000-1 使用 GRE 协议通过向数据包添加 GRE 标头和 GRE IP 标头来封装每个请求数据包。在 GRE IP 标头中，目标 IP 地址是数据中心 DC2 中的 Cloud Connector 隧道（Cloud_Connector _DC1-DC2）端点的地址。
7. 对于 Cloud Connector 通道 Cloud_Connector_DC1-DC2，NS_VPX_CB_4000/5000-1 将按照 NS_VPX_CB_4000/5000-1 与 NS_VPX_CB_4000/5000-2 之间的约定检查用于处理出站数据报的 storedIPSec 安全性关联 (SA) 参数。在 NS_VPX_CB_4000/5000-1 中的 IPSec 封装安全有效负载 (ESP) 协议使用这些 SA 参数的出站数据包，以加密 GRE 封装数据包的有效负载。
8. ESP 协议通过使用 HMAC 哈希函数和为 Citrix Cloud Connector 隧道 Cloud_Connector_DC1-DC2 指定的加密算法来确保数据包的完整性和机密性。ESP 协议, 在加密 GRE 有效载荷和计算 HMAC 后, 生成 ESP 头和 ESP 拖车，并插入它们之前和加密 GRE 有效载荷的末尾, 分别.
9. NS_VPX_CB_4000/5000-1 sends the resulting packet NS_VPX_CB_4000/5000-2.
10. NS_VPX_CB_4000/5000-2 checks the stored IPSec security association (SA) parameters for processing inbound packets, as agreed between CB_DC-1 and NS_VPX-AWS for the Cloud Connector tunnel Cloud_Connector_DC1-DC2. NS_VPX_CB_4000/5000-2 上的 IPSec ESP 协议将这些 SA 参数用于入站数据包，并使用请求数据包的 ESP 标头来解密数据包。
11. NS_VPX_CB_4000/5000-2 然后通过删除 GRE 标头来解压包。
12. NS_VPX_CB_4000/5000-2 会将生成的数据包转发到 CB_4000/5000-2，从而对数据包应用与万优化相关的处理。CB_VPX_CB_4000/5000-2 然后将生成的数据包返回到 NS_VPX_CB_4000/5000-2.
13. 生成的数据包与在步骤 2 中 CB_VPX_CB_4000/5000-2 接收到的数据包相同。此数据包的目标 IP 地址设置为服务器 S1 的 IP 地址。NS_VPX_CB_4000/5000-2 将此数据包转发到服务器 S1。
14. S1 处理请求数据包并发送响应数据包。响应数据包中的目标 IP 地址是客户端 CL1 的 IP 地址，源 IP 地址是服务器 S1 的 IP 地址。

配置数据中心和 **AWS/Azure** 之间的 **Cloud Connector** 隧道

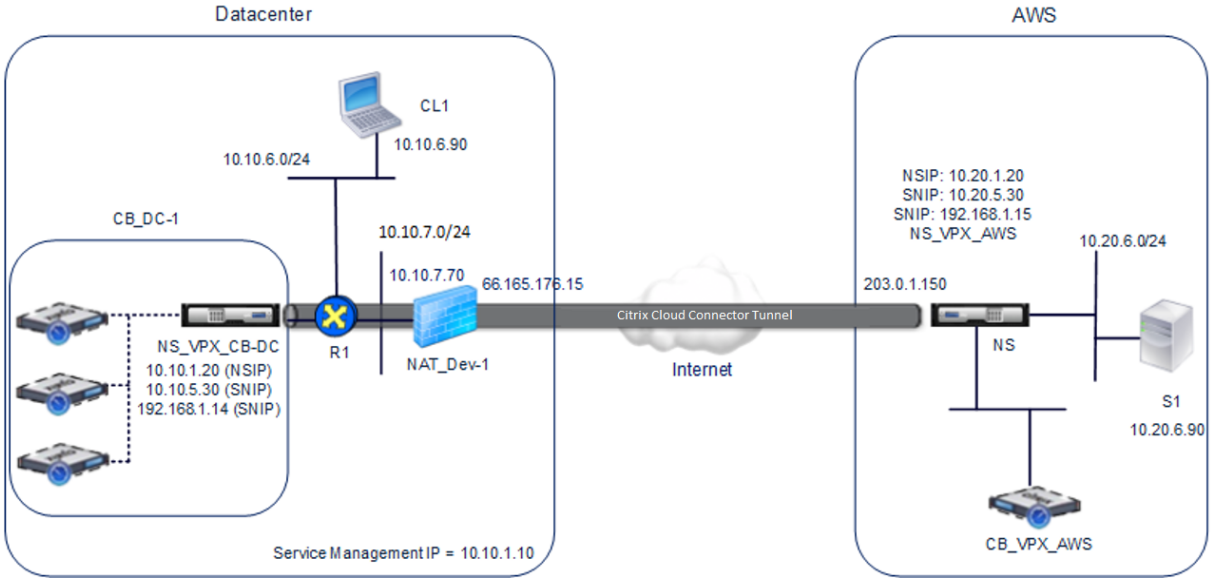
April 23, 2021

您可以在数据中心和 AWS 或 Azure 云之间配置 Cloud Connector 隧道。

请考虑一个示例，其中在数据中心的 WCCP/PBR 单臂模式下部署的 Citrix SD-WAN WANOP 设备 CB_DC-1 和 AWS 云之间配置了 Citrix Cloud Connector 隧道。CB_DC-1 连接到路由器 R1。NAT 设备还连接到 R1，用于数据中心和 Internet 之间的连接。

注意：示例中的设置也适用于任何类型的 Citrix SD-WAN WANOP 部署。此示例中的此设置包括基于策略的路由，而不是 Netbridge，用于允许所需子网的流量通过 Citrix Cloud Connector 隧道。

如下图所示，Citrix Cloud Connector 隧道是在 Citrix SD-WAN WANOP 设备 CB_DC-1 上运行的 Citrix 虚拟设备 NS_VPX_CB-DC 和在 AWS 云上运行的 Citrix 虚拟设备 NS_VPX-AWS 之间建立的。为了优化 Citrix Cloud Connector 隧道上的流量流，NS_VPX_CB-DC 与在 CB_DC-1 上运行的 Citrix SD-WAN WANOP 实例配对，而在 AWS 端，运行在 AWS 上的 Citrix SD-WAN WANOP 虚拟设备 CB_VPX-AWS 配对。



下表列出了本示例中数据中心中的设置。

实体	名称	详细信息
客户端 CL1 的 IP 地址		10.10.6.90
NAT 设备 **NAT-Dev-1** 上的设置		
公共端的 NAT IP 地址		66.165.176.15 *
私有端的 NAT IP 地址		10.10.7.70
在 **CB_DC-1** 上的设置		
CB_DC-1 的管理服务 IP 地址		10.10.1.10
在 **CB_DC-1** 上运行的 **NS_VPX_CB-DC** 上的设置		

实体	名称	详细信息
NSIP 地址		10.10.1.20
SNIP 地址		10.10.5.30
IPSec 配置文件	CBC_DC_AWS_IPSec_Profile	IKE 版本 = v2，加密算法 = AES，哈希算法 = HMAC SHA1
Cloud Connector 隧道	CBC_DC_AWS	Cloud Connector 隧道的本地端点节点 IP 地址 = 10.10.5.30，Cloud Connector 的远程端点节点 IP 地址 = 映射到 AWS 上的 NS_VPX-AWS 上的 Cloud Connector 端点节点地址 (SNIP) = 203.0.1.150*，隧道协议 = GRE 和 IPSEC，IPSec 配置文件名称 = CBC_DC_AWS_IPSec_Profile
基于策略的路由	CBC_DC_AWS_PBR	源 IP 范围 = 数据中心中的子网 = 10.10.6.0-10.10.6.255，目标 IP 范围 = AWS 中的子网 = 10.20.6.0-10.20.6.255，下一个跃点类型 = IP 隧道，IP 隧道名称 = CBC_DC_AWS

* 这些应该是公有 IP 地址。

下表列出了此示例中 AWS 云上的设置。

实体	名称	详细信息
—	—-	—-
服务器 S1 的 IP 地址		10.20.6.90
** 在 NS_VPX-AWS 上的设置 **
NSIP 地址		10.20.1.20
映射到 NSIP 地址的公共 EIP 地址		203.0.1.120*
SNIP 地址		10.20.5.30
映射到 SNIP 地址的公共 EIP 地址		203.0.1.150*
IPSec profile	CBC_DC_AWS_IPSec_Profile
IKE version = v2, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
Cloud Connector tunnel	CBC_DC_AWS	Local endpoint IP address of the Cloud Connector tunnel =10.20.5.30, Remote endpoint IP address of the Cloud Connector tunnel = Public NAT IP address of NAT device NAT-Dev-1 in the datacenter = 66.165.176.15*, Tunnel protocol = GRE and IPSEC, IPSec profile name = CBC_DC_AWS_IPSec_Profile

| Policy based route | CBC_DC_AWS_PBR | Source IP range = Subnet in the AWS = 10.20.6.0-10.20.6.255, Destination IP range = Subnet in datacenter = 10.10.6.0-10.10.6.255, Next hop type = IP Tunnel, IP tunnel name = CBC_DC_AWS |

* 这些应该是公有 IP 地址。

在 CB_DC-1 上的 NS_VPX_CB-DC 和 NS_VPX-AWS 两者都可以在 L3 模式下运行。它们可以实现数据中心和 AWS 云中的私有网络之间的通信。NS_VPX_CB-DC 和 NS_VPX-AWS 可通过 Cloud Connector 隧道在数据中心的客户端 CL1 与 AWS 云中的服务器 S1 之间进行通信。客户端 CL1 和服务器 S1 位于不同的专用网络上。

注意：AWS 不支持 L2 模式。因此，必须在两个端点上只启用 L3 模式。

为了在 CL1 和 S1 之间进行正确通信，在 NS_VPX_CB-DC 和 NS_VPX-AWS 上启用 L3 模式，路由配置如下：

- R1 具有通过 NS_VPX_CB-DC 到达 S1 的路径。
- NS_VPX_CB-DC 具有通过 R1 到达 NS_VPX-AWS 的路由。
- S1 应该有一条通过 NS_VPX-AWS 到达 CL1 的路径。
- NS_VPX-AWS 具有通过上游路由器到达 NS_VPX_CB-DC 的路由。

以下是在数据中心的各种网络设备上配置的路由，以便 Cloud Connector 隧道正常工作：

路由	网络	网关
路由器 **R1** 上的路由		
到达服务器 S1 的路由	10.20.6.X/24	NS_VPX_CB-DC 的通道端点 SNIP 地址 = 10.10.5.30
到达 Cloud Connector 隧道远端端点的路径	映射到 NS_VPX-AWS 的 Cloud Connector SNIP 地址的 EIP 地址 = 203.0.1.50	NAT 设备的专用 IP 地址 = 10.10.7.70
NS_VPX_CB-DC 上的路线		
到达 NS_VPX-AWS 的路径	映射到 NS_VPX-AWS 的 Cloud Connector SNIP 地址的 EIP 地址 = 203.0.1.50	R1 的 IP 地址 = 10.10.5.1

以下是在 AWS 云上的各种网络设备上配置的路由，以便 Cloud Connector 隧道正常工作：

路由	网络	网关
服务器 **S1** 上的路由		
到达客户端 CL1 的路由	10.10.6.X/24	NS_VPX-AWS 的隧道端点 SNIP 地址 = 10.10.6.1

路由	网络	网关
Citrix 虚拟设备 **NS_VPX-AWS** 上的路由		
到达 NS_VPX_CB-DC 的路线	数据中心中的 NAT_Dev-1 的公有 IP 地址 = 66.165.176.15 *	AWS 上上游路由器的 IP 地址

以下是 Cloud Connector 隧道中客户端 CL1 请求数据包的流量：

1. 客户端 CL1 向服务器 S1 发送请求。
2. 请求到达在 Citrix SD-WAN WANOP 设备 CB_DC-1 上运行的 Citrix 虚拟设备 NS_VPX_CB-DC。
3. NS_VPX_CB-DC 会将数据包转发到在 Citrix SD-WAN WANOP 设备 CB_DC-1 上运行的一个 Citrix SD-WANOP 实例以进行广域网优化。处理数据包后，Citrix SD-WAN WANOP 实例将数据包返回到 NS_VPX_CB-DC。
4. 请求数据包与 PBR 实体 CBC_DC_AWS_PBR（在 NS_VPX_CB-DC 中配置）中指定的条件匹配，因为请求数据包的源 IP 地址和目标 IP 地址分别属于 CBC_DC_AWS_PBR 中设置的源 IP 范围和目标 IP 范围。
5. 由于 Cloud Connector 隧道 CBC_DC_AWS 绑定到 CBC_DC_AWS_PBR，设备会准备要通过 CBC_DC_AWS 隧道发送的数据包。
6. NS_VPX_CB-DC 使用 GRE 协议通过向数据包添加 GRE 标头和 GRE IP 标头来封装每个请求数据包。GRE IP 标头的目标 IP 地址设置为 AWS 端的 Cloud Connector 隧道 (CBC_DC-AWS) 端点的 IP 地址。
7. 对于 Cloud Connector 隧道 CBC_DC-AWS，NS_VPX_CB-DC 会根据 NS_VPX_CB-AWS 和 NS_VPX-AWS 之间的协议，检查存储的 IPSec 安全关联 (SA) 参数以处理出站数据包。NS_VPX_CB-DC 中的 IPSec 封装安全有效负载 (ESP) 协议将这些 SA 参数用于出站数据包，以加密 GRE 封装数据包的有效负载。
8. ESP 协议通过使用 HMAC 哈希函数和为 Cloud Connector 隧道 CBC_DC-AWS 指定的加密算法来确保数据包的完整性和机密性。ESP 协议, 在加密 GRE 有效载荷和计算 HMAC 后, 生成 ESP 头和 ESP 拖车，并插入它们之前和加密 GRE 有效载荷的末尾, 分别.
9. NS_VPX_CB-DC 将生成的数据包发送到 NS_VPX-AWS。
10. NS_VPX-AWS 会根据 CB_DC-1 与适用于 Cloud Connector 通道 CBC_DC-AWS 的 NS_VPX-AWS 之间的协议，检查存储的 IPSec 安全关联 (SA) 参数以处理入站数据包。NS_VPX-AWS 上的 IPSec ESP 协议将这些 SA 参数用于入站数据包，并使用请求数据包的 ESP 标头来解密数据包。
11. NS_VPX-AWS 然后通过删除 GRE 标头来解压数据包。
12. NS_VPX-AWS 将生成的数据包转发到 CB_VPX-AWS，后者将 WAN 优化相关的处理应用于数据包。然后，CB_VPX-AWS 将生成的数据包返回到 NS_VPX-AWS。
13. 生成的数据包与 CB_DC-1 在步骤 2 中接收的数据包相同。此数据包的目标 IP 地址设置为服务器 S1 的 IP 地址。NS_VPX-AWS 将此数据包转发到服务器 S1。

14. S1 处理请求数据包并发送响应数据包。响应数据包中的目标 IP 地址是客户端 CL1 的 IP 地址，源 IP 地址是服务器 S1 的 IP 地址。

Office 365 加速

April 23, 2021

Citrix SD-WAN WANOP 优化了 WAN，为跨分支机构和远程站点的业务应用程序提供一致的用户体验。

微软 Office 365 是一个软件即服务 (SaaS) 应用程序，它提供了企业级生产力应用程序的微软 Office 套件。此应用程序托管在云端，并按需交付给用户。

Office 365 加速功能允许分支机构获得 Citrix SD-WAN WANOP 为 Microsoft Office 365 应用程序提供的优化优势。

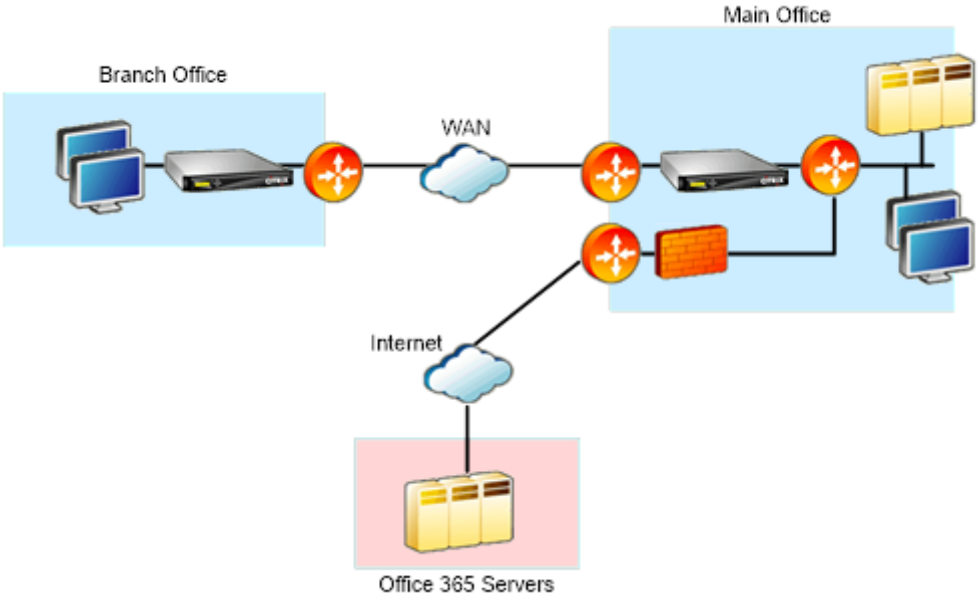
用例

当广域网段比互联网段慢得多，并且 Microsoft 的 Office 365 服务器更接近较大的办公室比分支机构。

拓扑

分支机构 Office 365 通信通过 WAN 发送到主办公室，然后通过 Internet 转发到 Office 365 服务器。分支机构和主要办公室之间的区段加速。

> 注意
>
> 主办公室和 Microsoft Office 365 服务器之间的区段不加速。建议主办公室连接到最近的 Office 365 服务器。



它是如何工作的?

Citrix SD-WAN WANOP SSL 加速可以解密和加速 Office 365 流量，从而提供压缩。简而言之，Office 365 分支机构加速可以被认为是通过 HTTPS 加速的 RPC 的特殊情况。

过程

1. 在分支机构和主办公室 Citrix SD-WAN WANOP 设备之间创建安全对等。
2. 在域证书颁发机构 (CA) 中生成代理证书/私钥。
3. 在 Citrix SD-WAN WANOP 中添加所有必需的 CA。
   a) CA、中级 CA、微软证书的根 CA。
   b) 为 Office 365 URL 生成的代理证书/私钥。

   > 注意
   >
   > 为避免在浏览器上发生安全警报，代理证书必须由 Windows 域的 CA 服务器签名，这使得任何域用户都可以接受。

4. 创建 SSL 拆分代理配置文件并将拆分代理绑定到服务类（Web（互联网安全））。
5. 启动 Office 365 连接并检查加速连接。

> 警告
>
> 除非手动安装证书，否则不属于域的分支机构设备将显示安全警告。Firefox 用户也必须手动安装证书，因为 Firefox 不支持设备的证书存储。

配置 **Office 365** 加速

要配置 Office 365 加速：

1. 如安全对等互连 *(/en-us/citrix-sd-wan-wanop/11-1/secure-traffic-acceleration/secure-peering.html)* 中所述，在两个 *Citrix SD-WAN WANOP* 设备之间建立 *[安全对等]* 关系
2. 创建新证书。

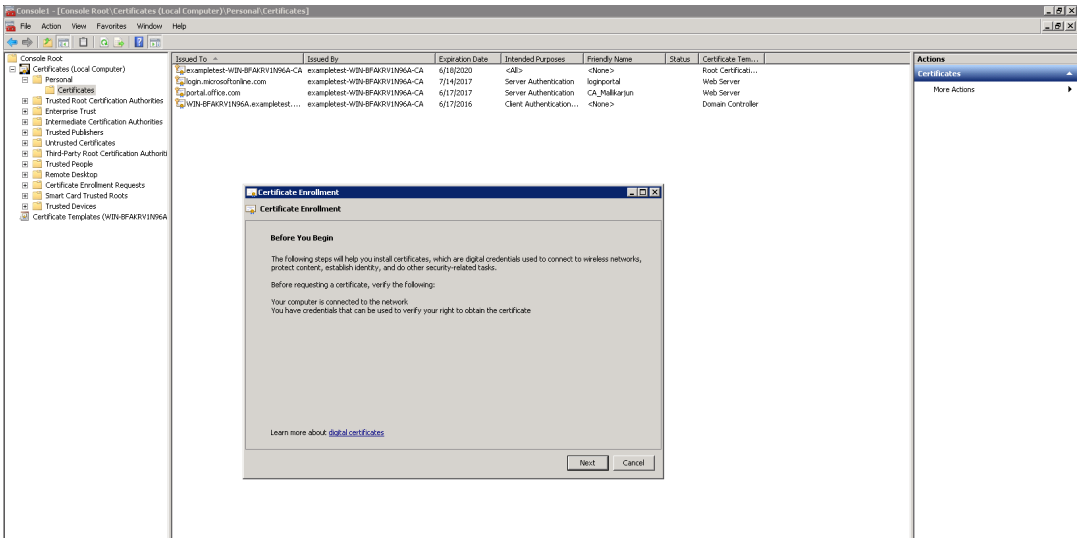
> 注意
>
> 服务器端 Citrix SD-WAN WANOP 设备充当 Office 365 和客户端之间的中介，因此这些证书将由服务器端域控制器签名，但它引用 Office 356 域。

   a) 登录到 Windows 域的证书颁发机构服务器。

   b) 如有必要，添加证书颁发 机构、证书模板和证书的管理单元。

   c) 导航到 证书模板 > **Web** 服务器属性 > 安全，然后选择所有选项。

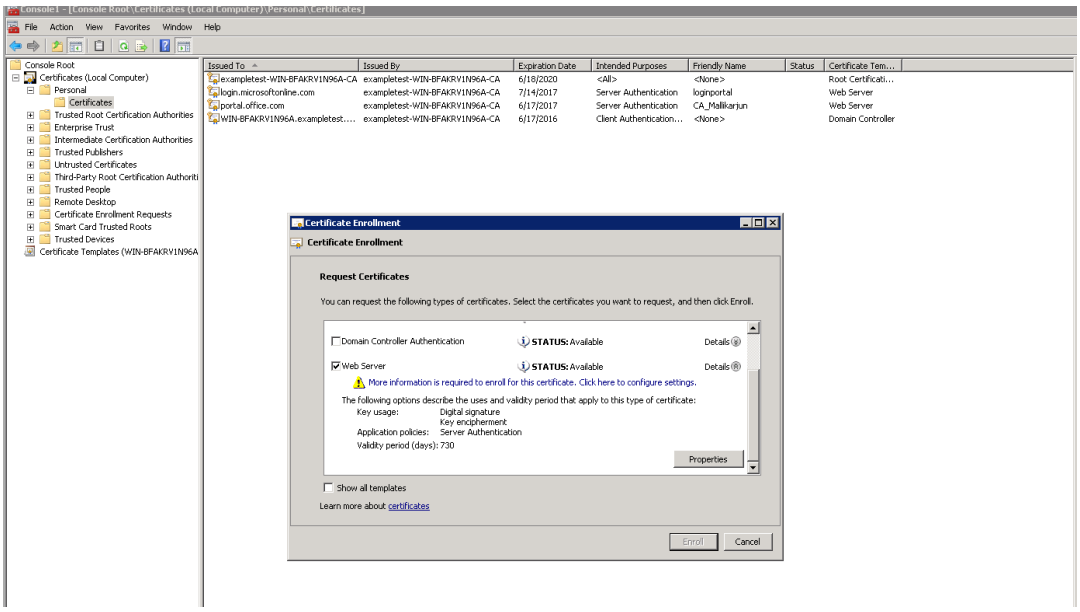
   d) 导航到 证书 > 个人 > 证书（计算机） > 所有任务 > 申请新证书。



   e) 在 证书注册窗口中，单击 下一步。

   f) 在 “选择证书注册策略 窗口中，选择 活动目录注册策略。

   g) 在 **Active Directory** 注册策略 窗口中，选择 **Web** 服务器 > 详细信息 > 属性。



3. 将 Office365 证书中的信息复制到您的新证书中。您最终将获得来自三个 Office365 证书的单个证书。按如下方式进行操作：

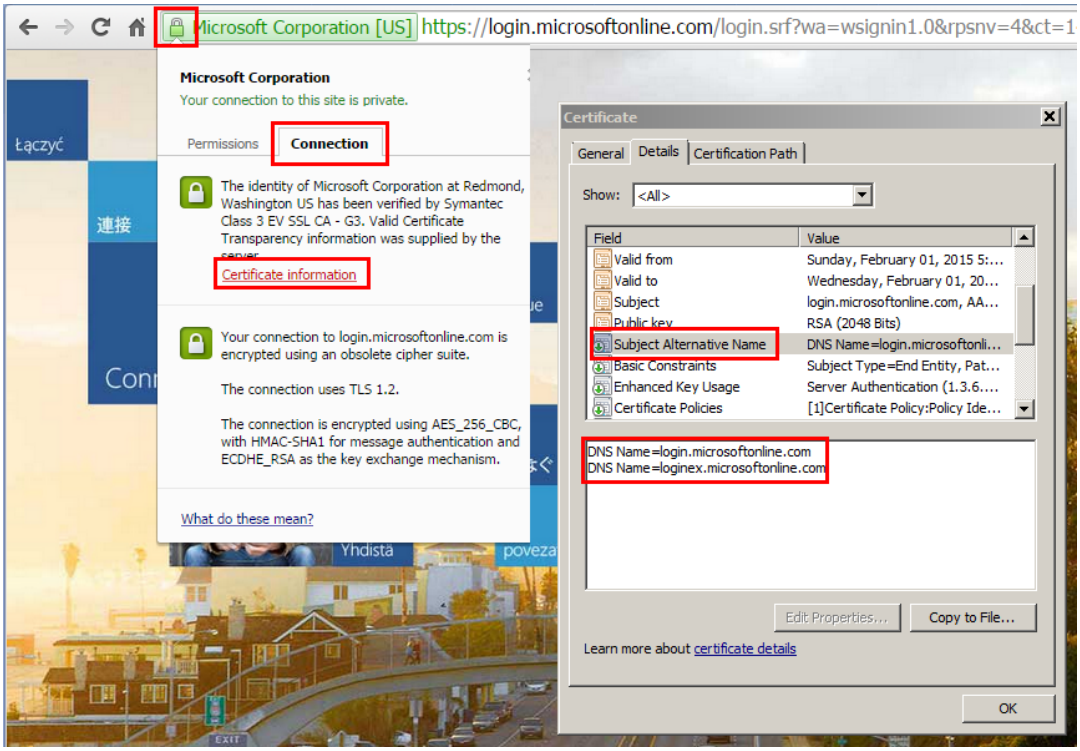
   a) 在浏览器中，如 Chrome，输入 url-https://login.microsoftonline.com。

   > 注意
   >
   > 请勿登录。

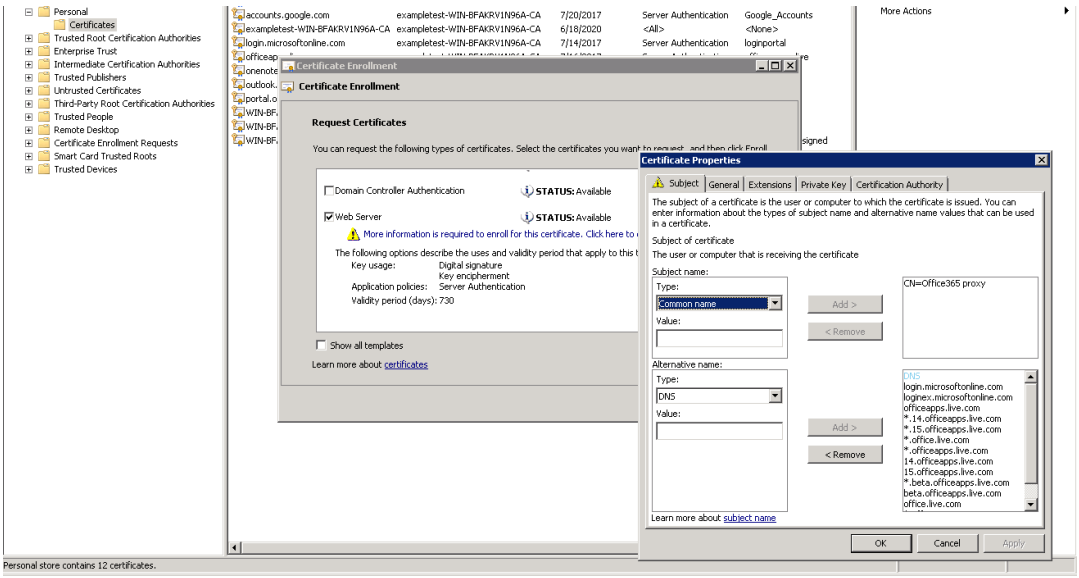
   b) 单击 URL 栏上的挂锁图标，然后选择 连接 > 证书信息 > 详细 信息。

   > 注意
   >
   > 这些说明是针对 Chrome 浏览器的；其他浏览器的过程也是相同的。

   c) 点击 主题备用名称，这将显示 DNS 名称列表，例如“登录.microsoftonline.com”。复制它下面的文本框中的信息。

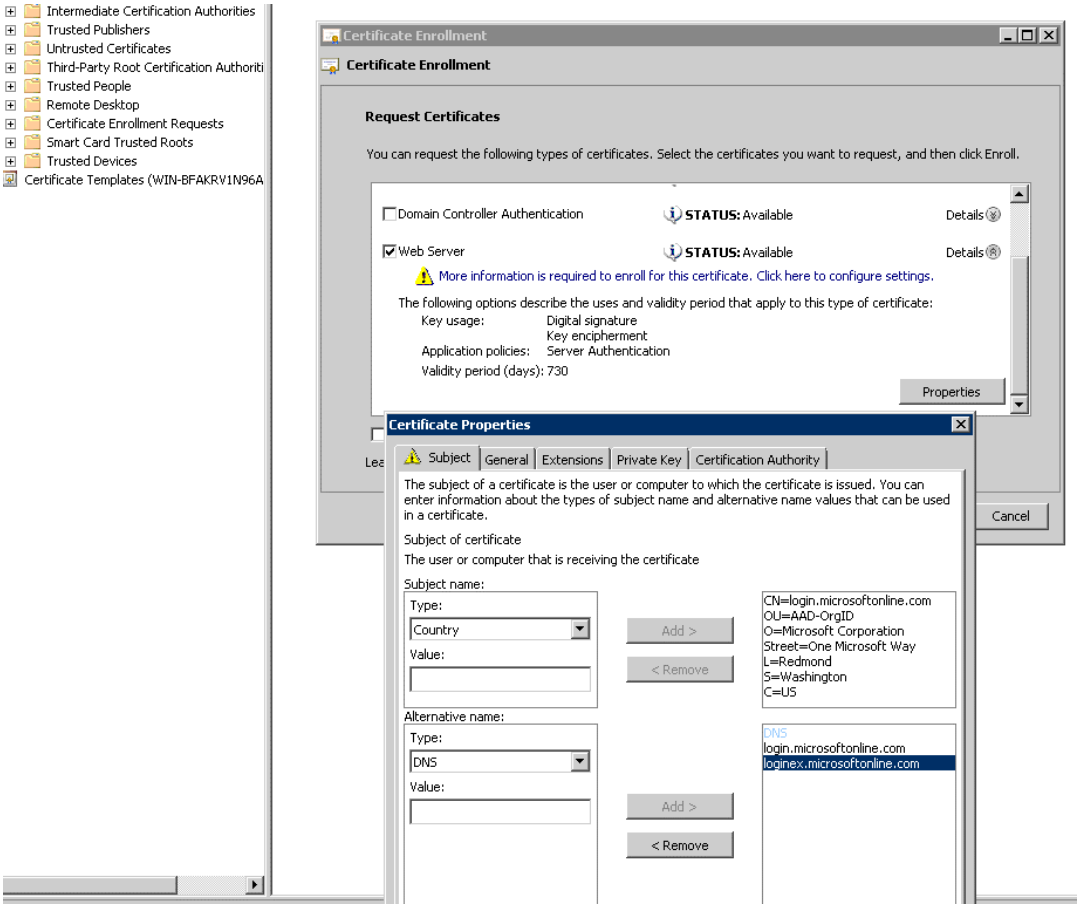


d) 返回到新证书的 证书属性 窗口。添加 值 字段中的备用名称与 类型 为 **DNS**，以匹配 Microsoft 证书中的每个备用名称。



e) 重复发现使用者备用名称的过程，并将其添加到证书中的https://outlook.office365.com、https://portal.office.com、https://office.live.com和https://sharepoint.com（SharePoint URL 是客户特定的）。

f) 为新证书创建公用名称。上面的示例显示了一个通用名称为“Office365 代理”。

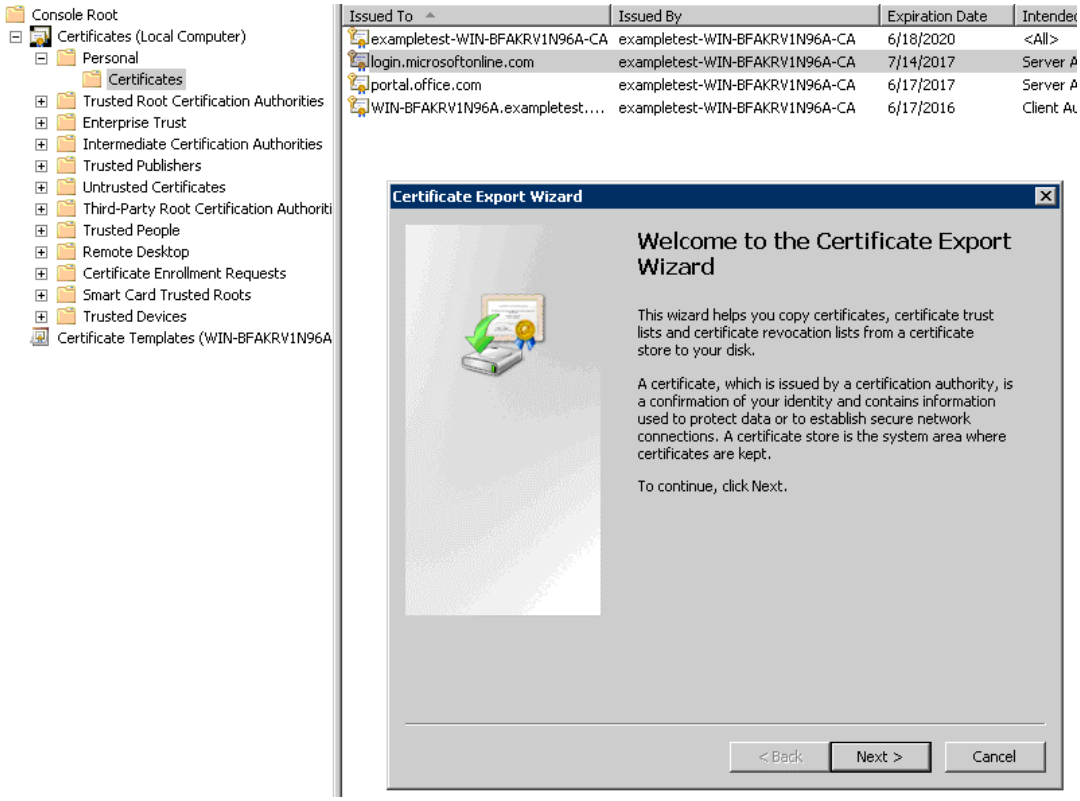


g) 在 私钥 选项卡中，选择 使私钥可导 出”。

h) 单击确定、注册和完成。

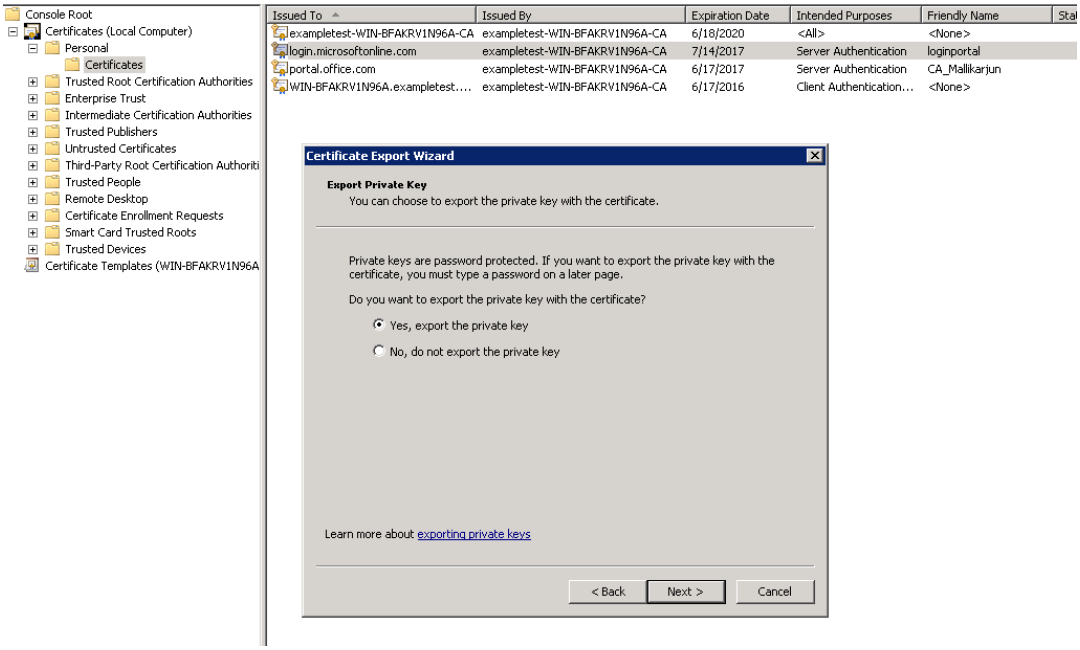
4. 导出证书。

a) 在 证 书” > 个人 > 证 书” 下，选择上述创建的代理证书，然后选择 所有任务 > 导出。



b) 此时将显示 证书导出向导。单击下一步。

c) 在 导出私钥中，选择选项 是，导出私钥，然后单击 下一步。

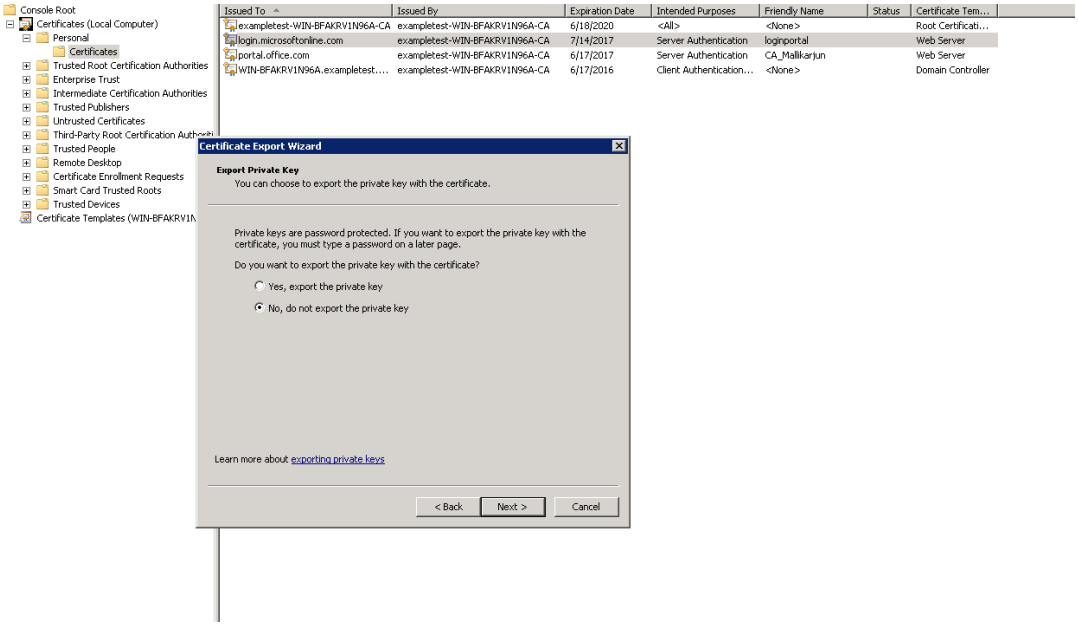


d) 保留导出文件格式的默认值。

e) 键入并确认密码，导出私钥，然后将证书保存为 *loginportal.pfx*。

5. 导出您的证书。

   a) 在 证书导出向导中，单击 下一步。在 导出私钥中，选择选项 否，不要导出私钥。单击下一步。



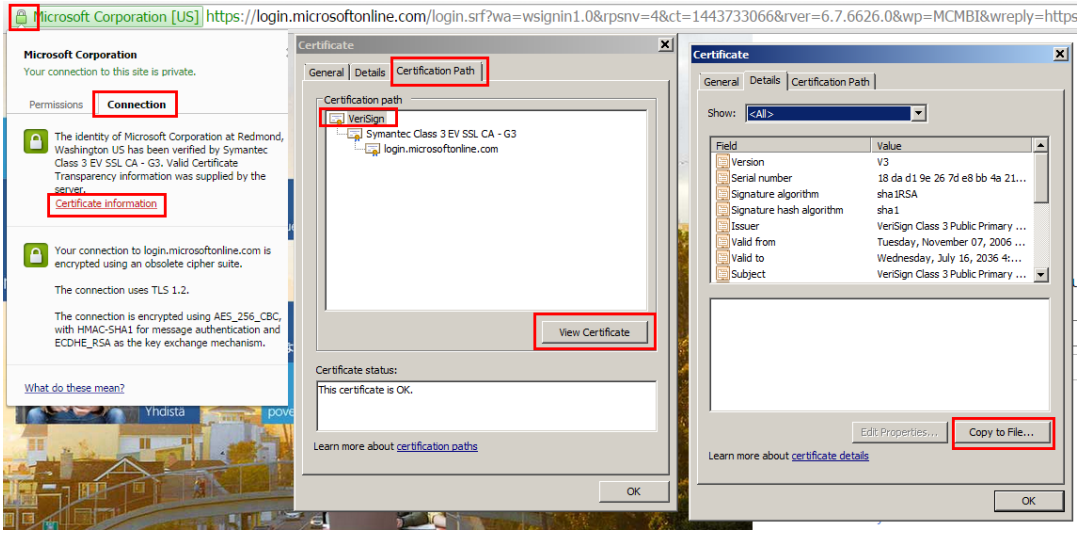
   b) 保留导出文件格式的默认值。

   c) 键入并确认密码，然后导出私钥和证书，然后将文件保存到文件名，如 office365_keys.pfx。

6. 下载 Microsoft 证书的根 CA 和中间 CA 的公钥。

   a) 从浏览器中，导航到https://login.microsoftonline.com。单击浏览器中的挂锁图标。导航到 连接 > 证书信息 > 证书路径。

   b) 选择根证书（列表顶部的证书），然后单击 查看证书 > 详细信息 > 复制到文件。此时将显示 证书导出向导。单击下一步。



c) 输入文件名并保存文件。

> 注意
>
> 或者，您可以使用 Wireshark 或 OpenSSL 获取根和中间 CA 名称，并从“真实”源（例如，Windows SSL 存储）获取证书。

d) 重复步骤 6 以保存以下域的根 CA 和中间 CA:

i. login.microsoftonline.com

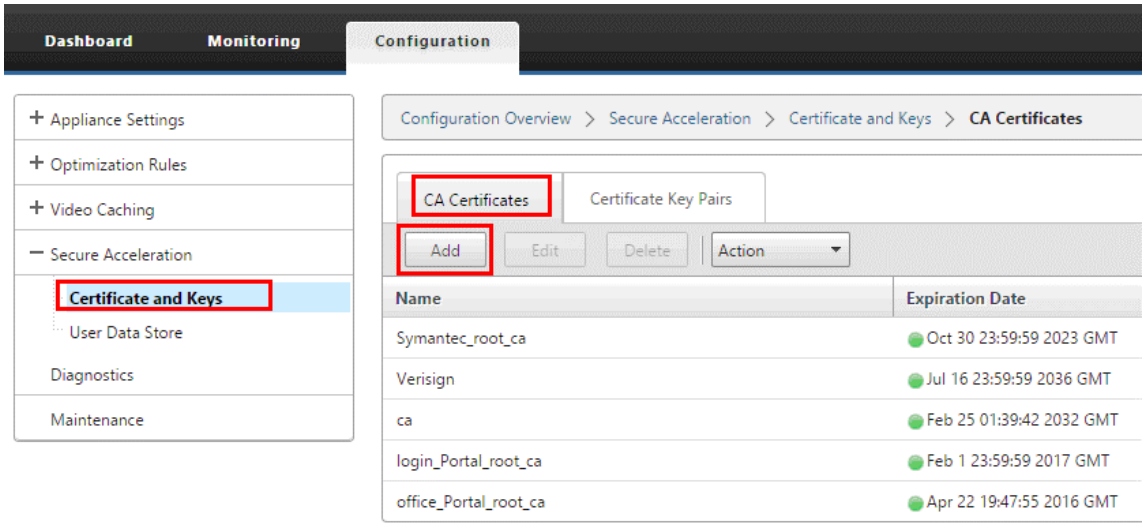
ii. portal.office.com

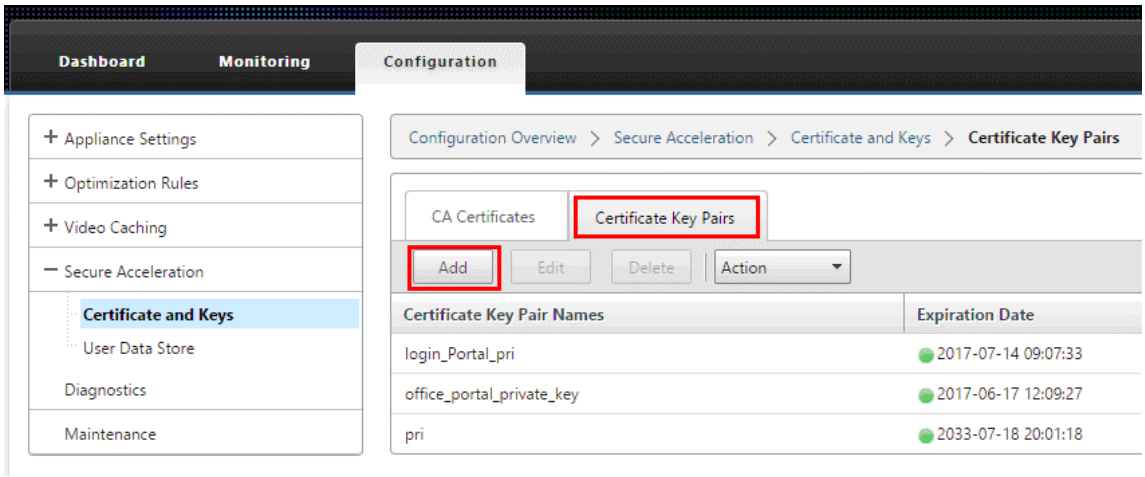
iii. outlook.office356.com

iv. *.sharepoint.com

v. office.live.com

7. 将所有 Office 365 服务器 CA、代理证书/密钥对和私钥添加到服务器端 Citrix SD-WAN WANOP 设备。使用“证书 和密钥”页面上的 **CA** 证 书 选项卡添加 CA。证书和证书/密钥对添加到 证书/密钥对 选项卡上。





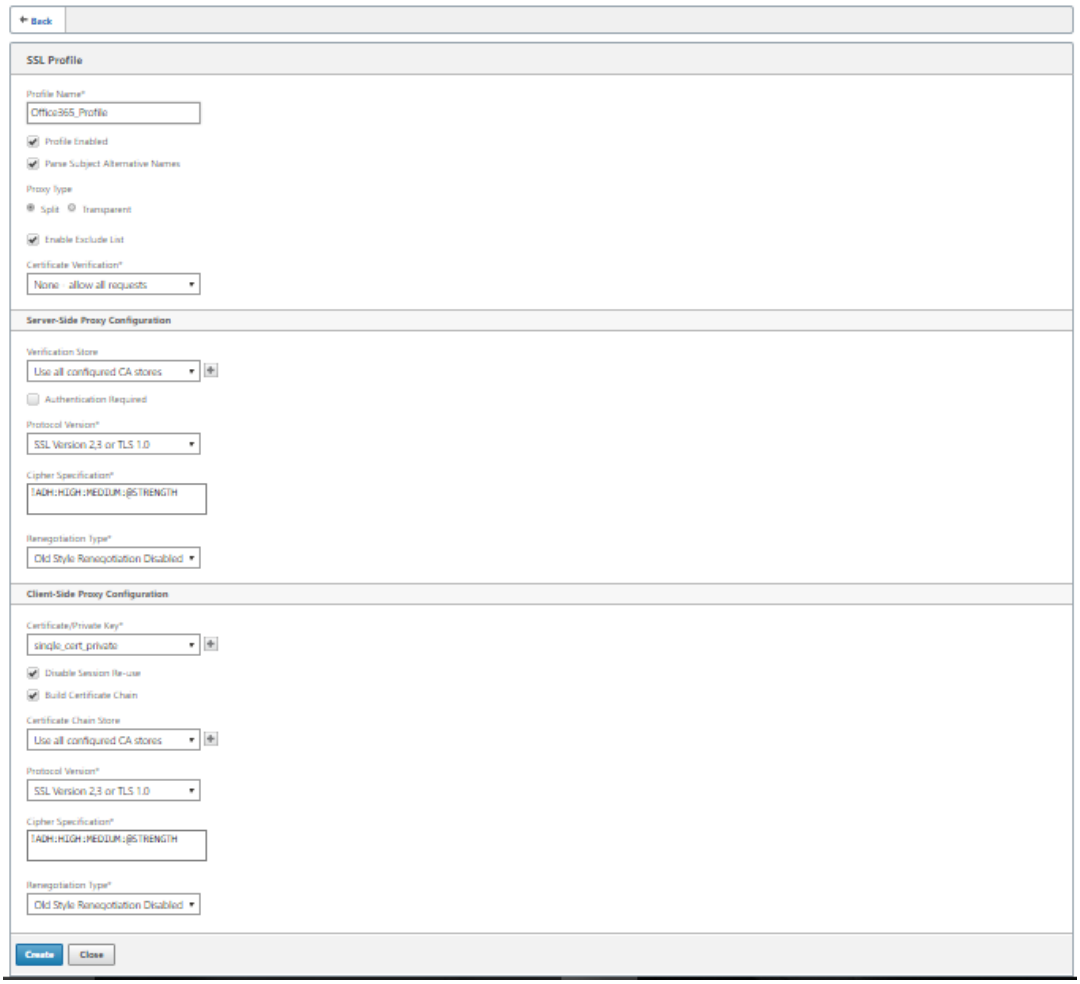
8. 创建 SSL 拆分代理配置文件并将拆分代理绑定到 Web（Internet 安全）服务类。

   a) 导航到 配置 > 安全加速 > **SSL** 配置文件 > 添加配置文件。

   b) 输入您选择的配置文件名称。选择 启用配置文件”、解析主题 备用名称” 和 拆分代理”。

   c) 在 服务器端代理配置 > 验证存储 下，选择 使用所有已配置的 **CA** 存储。

   d) 在 客户端代理配置 > 证书/私钥 下，选择您之前创建和导出的证书/私钥对（示例中显示为 loginportal.pfx）。选择 构建证书链。在证 书链商店下选择与证书/密钥对关联的 CA。

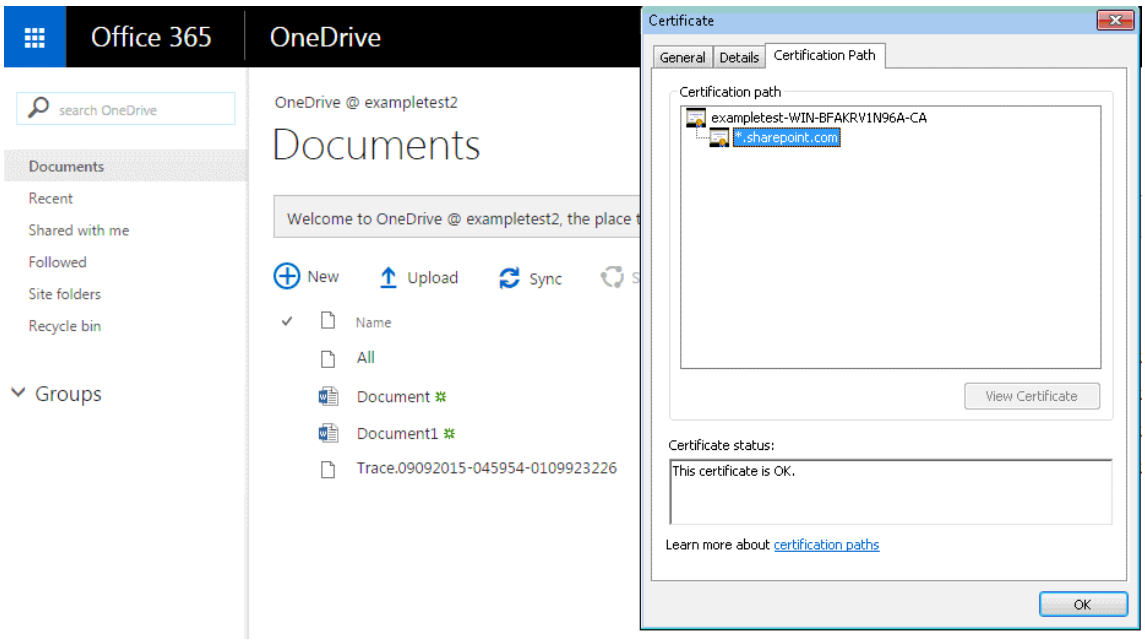


9. 将创建的 SSL 配置文件绑定到 Internet（Web 安全）服务类。导航到 配置 > 优化规则 > 服务类，然后将 SSL 配置文件添加到 SSL 配置文件列表中。

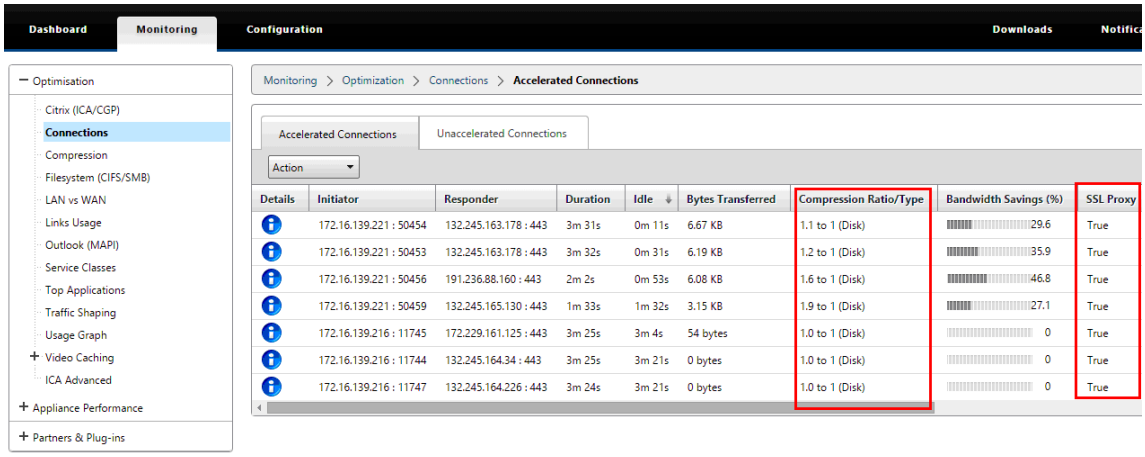
10. 为 **Internet**（**Web** 安全）服务类启用加速和基于磁盘的压缩。

11. 从浏览器启动 Office 365 会话。

    连接加速。在浏览器中，证书应将根 CA（而不是实际的 Office 365 证书）显示为服务器端设备的 CA 证书。



12. 在“设备 监视 > 连接 页面上，验证 Office 365 连接是否已压缩并正在接收 SSL 加速。

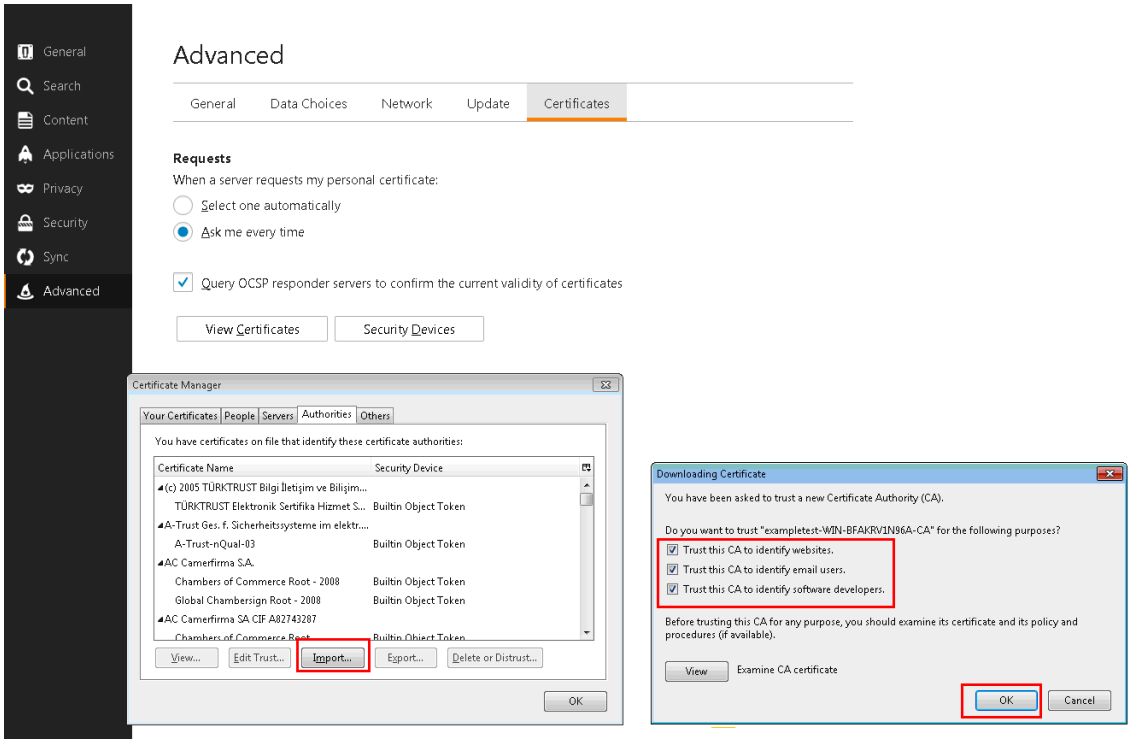


> 注意
>
> Firefox 默认不接受设备的证书，但拥有自己的证书存储区。因此，其他浏览器以及整个设备在正常 Windows 域行为中接受的凭据必须手动安装到 Firefox 中。要将证书安装到 Firefox 中，请按照“将证书安装到 Firefox”部分中的步骤操作。

将证书安装到火狐浏览器

将服务器端设备的代理证书安装到 Firefox 证书存储区：

1. 在 Firefox 浏览器中，导航到 选项 > 高级 > 证书 > 查看证书” > “颁 发 机构 > 导入。
2. 上传本地 CA 代理证书，选择 下载证 书”向导中的所有选项，然后单 击“确定。



SCPS 支持

April 23, 2021

Citrix SD-WAN WANOP 支持 SCPS（空间通信协议标准）TCP 变体。SCPS 被广泛用于卫星通信。

有关 SCPShttp://www.scps.org 的一般信息，请参阅。

SCPS 是用于卫星通信和类似应用的 TCP 变体。如果在“配置：调整”页面上选择了 **SCPS** 选项，设备可以加速 SCPS 连接。

SCPS 和默认设备行为之间的主要实际区别在于，使用 SCPS 风格的“选择性负面确认”（零食）代替标准选择性确认（SAK）。这两种增强数据重传输的方法是相互排斥的，因此如果连接一端的设备启用了 SCPS，而另一端没有启用，则重新传输性能会受到影响。此情况也会导致“SCPS 模式不匹配”警报。

如果必须将启用 SCPS 的设备与未启用 SCPS 的设备混合，请以不会发生不匹配的方式部署它们。您可以使用基于 IP 的服务类规则或安排部署，以便每个路径都具有匹配的设备。

安全的流量加速

April 23, 2021

通过安全对等来实现安全的流量接入。若干高级功能要求链接两端的 Citrix SD-WAN WANOP 设备建立彼此之间的 安全对等关系，从而设置 SSL 信令隧道（也称为 信令连 接）。这些 功能包括 SSL 压缩、签名 CIFS 支持和加密 MAPI 支持。

启用安全对等后，对于尚未与本地设备建立安全对等关系的所有伙伴设备（以及运行 Citrix SD-WAN WANOP 插件的计算机），将自动禁用压缩。

要建立安全对等关系，您必须生成安全密钥和证书，并在设备之间配置安全信号隧道。在配置隧道之前，请从 Citrix 订购加密许可证。

安全对等

April 23, 2021

如果设备启用了安全对等，则不会加密或压缩与其没有安全对等关系的伙伴的连接，尽管 TCP 流量控制加速仍可用。禁用压缩，以确保来自受保护伙伴的压缩历史记录中存储的数据不能与不安全的伙伴共享。

当连接一端的设备检测到另一个设备已启用安全对等时，它会尝试打开 SSL 信令隧道。如果两个设备通过此隧道成功地相互身份验证，则它们具有安全的对等关系。两个设备之间的所有加速连接都将加密，并启用压缩功能。

> 注意
>
> 启用了安全对等的设备不会压缩到不安全伙伴的连接，因此很难将同一设备与有担保伙伴和不安全伙伴混合使用。设计加速网络时请记住这一点。

访问安全参数需要密钥库密码。此密钥库密码不同于管理员的密码，以允许安全管理与其他任务分开。如果重置密钥库密码，则所有现有的加密数据和私钥都将丢失。

为了保护数据，即使设备被盗，每次重新启动设备时都必须重新输入密钥库密码。在完成此操作之前，禁用安全对等和压缩。

生成安全密钥和证书

Citrix SD-WAN WANOP 产品在没有 SSL 信令隧道所需的密钥和证书的情况下发货。你必须自己生成它们。您可以通过生成凭据的常规过程生成密钥和证书，也可以使用来自的“openssl”软件包来生成密钥和证书http://www.openssl.org。

出于测试目的，您可以生成和使用基于私钥（您也可以生成）的自签名 X509 证书。在生产中，使用引用受信任的证书颁发机构的证书。以下示例从 PC 上的命令行调用 openssl 以生成私钥 (
my.key) 和自签名证书 (
my.crt)：


```
pre codeblock
# Generate a 2048-bit private key
openssl genrsa -out my.key 2048
# Now create a Certificate Signing Request
openssl req -new -key my.key -out my.csr
# Finally, create a self-signed certificate with a 365-day expiration
openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
<!--NeedCopy-->
```

对于生产使用，请参阅组织的安全策略。

配置安全对等

有两种方法可以建立安全对等：

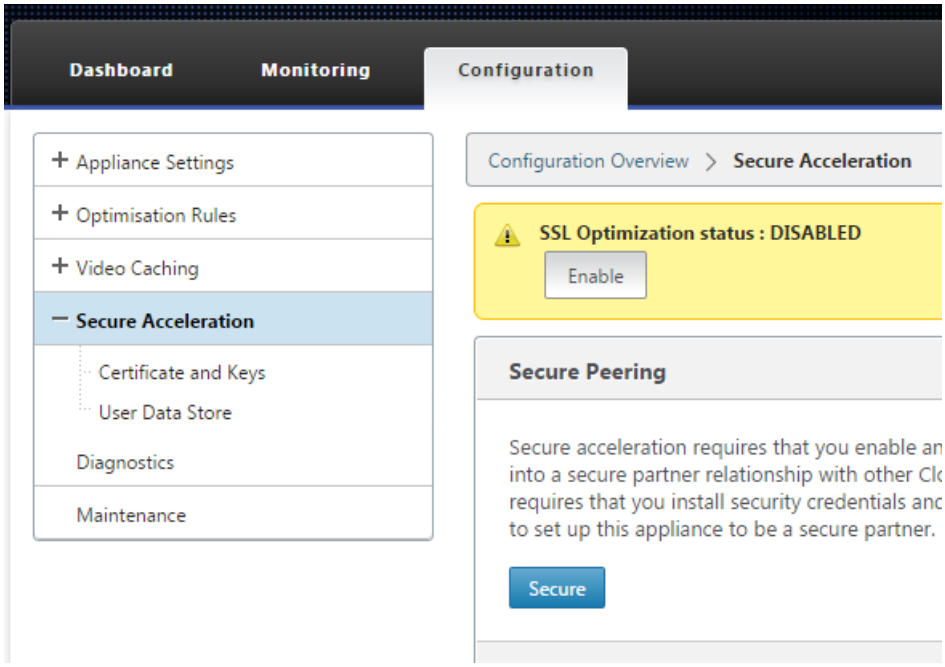
1. 使用设备生成的凭据。
2. 使用您自己提供的凭据。

   由于启用了安全对等的设备只会压缩与与其具有安全对等关系的合作伙伴设备的连接，因此此过程应同时应用于您的所有设备。

要准备安全对等的设备：

在网络中的每个设备上执行以下步骤。

1. 在设备上安装加密许可证。没有加密许可证，安全加速不可用。
   a) 如果尚未这样做，请从 Citrix 获取加密许可证。
   b) 如果您使用的是网络许可证服务器，请转到“配置”> “设备设置”> “许可”。在 添加许可证 部分，单击编辑，然后选择远程许可证服务器并设置加密许可证开启。
   c) 如果您使用的是本地许可，请转到“配置”> “设备设置”> “许可”。在 添加许可证 页面中，单击“本地许可证服务器”选项，然后单击 添加 以上传本地加密许可证。
   d) 在“配置”> 设备设置 > “许可”页面上验证成功安装许可证。在许可信息下，加密许可证应显示为有效且未来有效期。
2. 转到 配置 > 安全加速 页面。如果页面有一个标记为“安全”的按钮，请单击该按钮。



3. 如果您被自动转到密钥库设置屏幕，请执行以下操作：

   a) 输入密钥库密码两次，然后单击保存。

   b) 屏幕更新以显示“安全对等证书和密钥”部分时，单击“启用安全对等和 CA 证书”，然后单击“保存”。

   c) 跳到步骤 6。

4. 如果您未自动进入密钥库设置屏幕，请单击 安全对等下的铅笔图标，然后单击 密钥库设置下的铅笔图标。在密钥库状态下拉菜单上打开，然后输入密钥库密码两次。单击保存。

5. 通过转到 配置 > 安全加速 页面并单击“启用”按钮来 启用 安全对等。在此阶段忽略任何警告。当所需的额外配置完成时，此设置启用安全对等。

6. 通过转到 配置 > 安全加速 用户数据存储 并单击铅笔图标来启用压缩历史的加密。单击 启用磁盘加密，然后单击保存。用户数据存储加密可防止未经授权读取基于磁盘的压缩历史记录，以防设备被盗或返回工厂。磁盘数据加密的安全性取决于密钥库密码。此功能使用 AES-256 加密。（磁盘数据加密不会加密整个磁盘，只是加密压缩历史记录。）

7. 如果您使用的是设备生成的凭据，请跳到下一步。如果您使用自己的凭据，请执行以下操作：

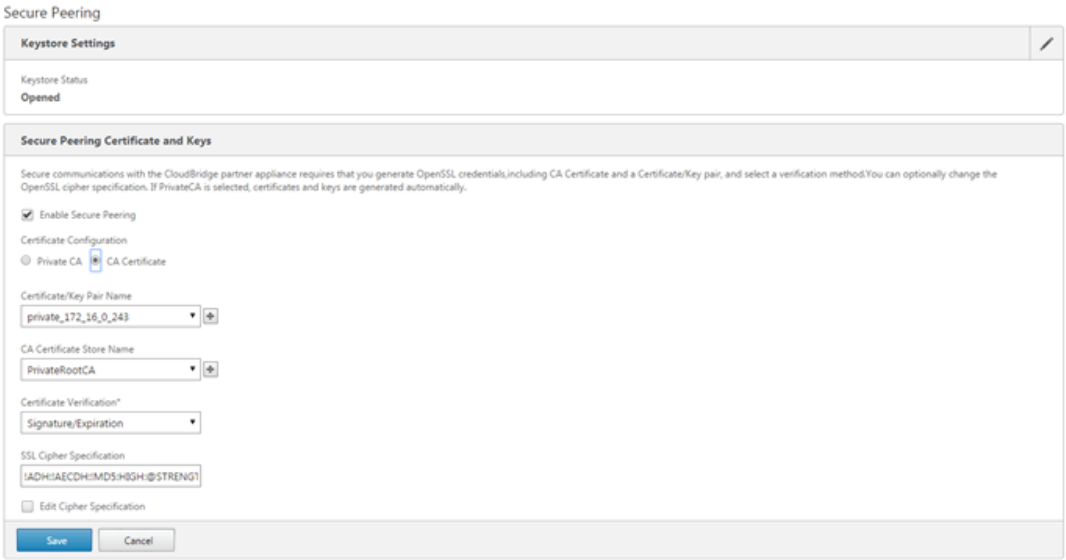
   a) 转到 配置 > 安全加速，然后单击安全对等下的铅笔图标，然后单击 安全对等证书和密钥 下的铅笔图标。单击 启用安全对等和证书配置 > **CA** 证书。将显示凭据规范字段。

   b) 在 证书/密钥对名称下，单击 **+** 图标，然后上传或粘贴此设备的证书/密钥对。如果凭据需要，还输入密钥密码或文件密码。单击创建。

   c) 在 **CA** 证书存储名称下，单击 **+** 图标，然后上传或粘贴此设备的 CA 证书。

   d) 保留“证书验证”和“SSL 密码规范”字段的默认值，除非您的组织另有要求。

e) 单击保存。



8. 对您的其余设备重复此操作。
9. 如果您使用的是您自己提供的凭据，则安全对等配置已完成。
10. 如果您使用的是设备生成的凭据，请执行以下过程。

要对设备生成的凭据使用安全对等：

1. 使用上面的“准备设备以保护对等”过程为此过程准备您的设备。
2. 在一个数据中心设备上，转到 配置 > 安全加速，然后单击 启用 按钮（如果存在）以启用安全对等。
3. 单击安全对等下的铅笔图标。密钥库应该是打开的。如果不是，立即打开它。
4. 单击安 全对等证书和密钥下的铅笔图标。单击 启用安全对等和私有 **CA** 选项，然后单击 保存。这将生成本地自签名 CA 证书和本地证书密钥对。
5. 点击 已连接对等 方下的 **+** 。输入远程设备之一的 IP 地址、管理员用户名和管理员密码，然后单击 连接”。这会为远程设备颁发 CA 证书和证书密钥对，并将其复制到远程设备。

   > 注意
   >
   > 对于 SD-WANOP 设备，IP 地址可以是任何启用 Web 访问的接口的 IP 地址。对于 SD-WAN PE 设备，IP 地址是管理 IP 地址。

6. 对其他远程设备重复此过程。
7. 在数据中心设备上，通过转到 监视 > 合作伙伴和插件 > 安全合作伙伴 来验证连接性。对于每个远程设备，“安全”字段的内容应为“True”，并且“连接状态”应为“连接可用”。

CIFS、SMB2 和 MAPI

April 23, 2021

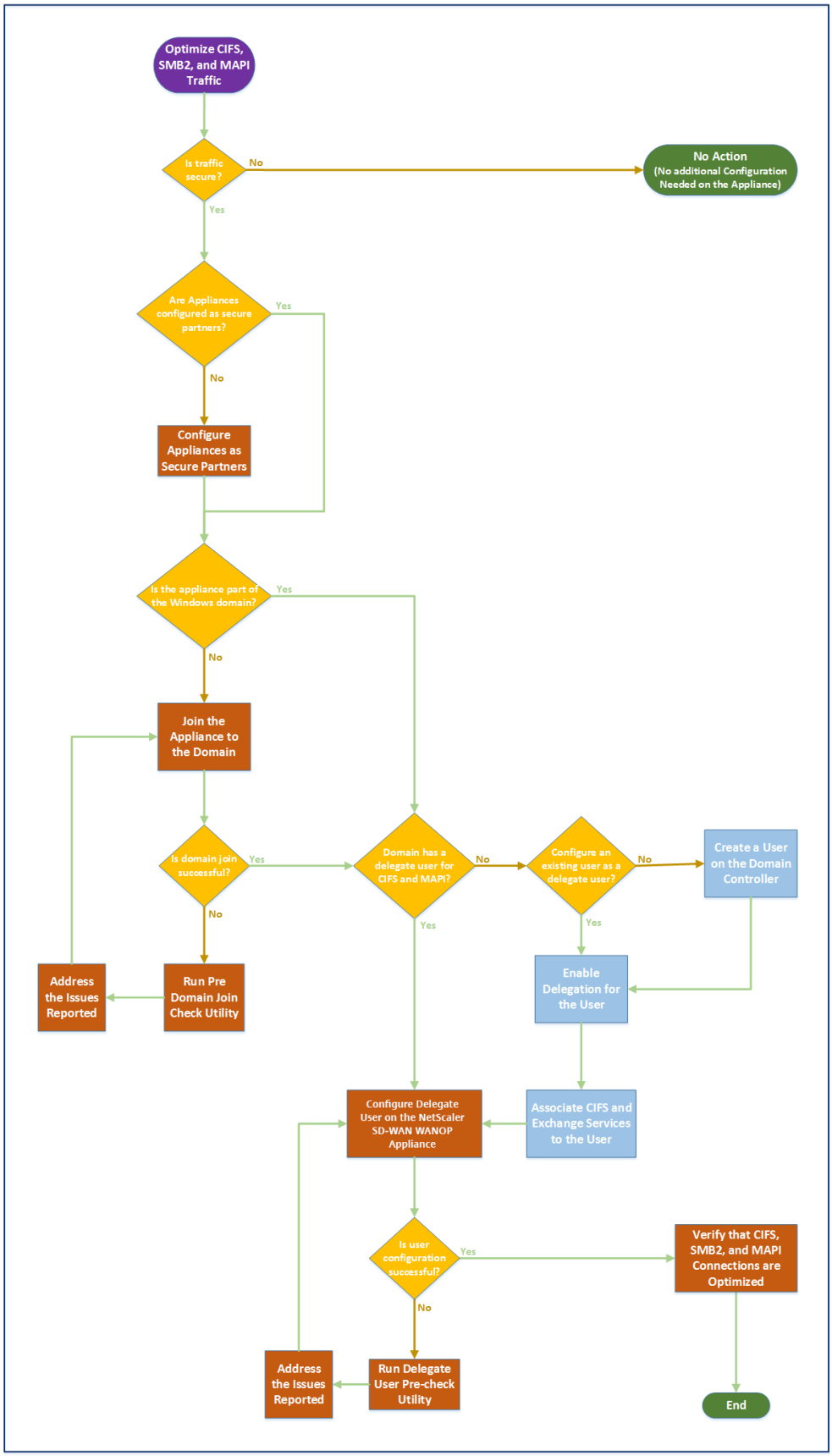
Windows 是部署在网络上的常见操作系统之一。Windows 操作系统支持跨位置共享的分布式资源。例如，您可以从各个分支机构访问数据中心中的资源。对于通过网络访问，Windows 使用通用 Internet 文件系统 (CIFS) 协议访问共享文件，并使用邮件应用程序编程接口 (MAPI) 协议通过 Microsoft Outlook 访问电子邮件。也就是说，Windows 使用 CIFS 协议的基于 CIF（Windows 和 Samba）的文件传输和目录浏览，和 Microsoft Outlook 使用 MAPI 协议来访问 Outlook 数据。

您可以使用 Citrix SD-WAN WANOP 设备来优化网络上的 CIFS、服务器消息块版本 2 (SMB2) 和 MAPI 连接。

除了支持 Windows 操作系统外，Citrix SD-WAN WANOP 设备还支持 NetApp 和 Hitachi 存储系统上的 CIFS 和 SMB2。

下面的流程图显示了配置 Citrix SD-WAN WANOP 设备以优化 CIFS、SMB2 和 MAPI 流量的完整过程。

配置用于优化 CIFS、SMB2 和 MAPI 流量的 Citrix SD-WAN WANOP 设备



配置 Citrix SD-WAN WANOP 设备以优化安全的 Windows 流量

April 23, 2021

必须先将 Citrix SD-WAN WANOP 设备添加到 Windows 安全基础结构中，然后才能优化已签名的 Windows 文件系统和加密的 MAPI Outlook/Exchange 流量。

由于在最近的 Windows 版本中增强了 Windows 安全系统，客户端和服务器通过对数据进行身份验证和加密来保护流量。这要求 Citrix SD-WAN WANOP 设备是 Windows 安全基础结构的受信任成员，然后才能优化已签名的 Windows 文件系统和加密的 MAPI Outlook/Exchange 流量。

将设备添加到 Windows 安全基础结构后，该设备具有以下功能：

- 通过使用签名的 SMB 和签名的 SMB2 协议，加速 Microsoft Windows Server、NetApp 服务器和 Hitachi HNAS 的文件服务器流量。
- 加速 Microsoft Exchange Server 通信时，Outlook 客户端使用加密的 MAPI 或 RPC 通过 HTTPS 对其进行访问。

Citrix SD-WAN WANOP 设备在 Windows 安全系统中的工作原理

将设备加入 Windows 域需要管理员凭据。当它加入 Windows 域时，设备将成为域的受信任成员。这允许将设备声明为域安全基础结构的成员。

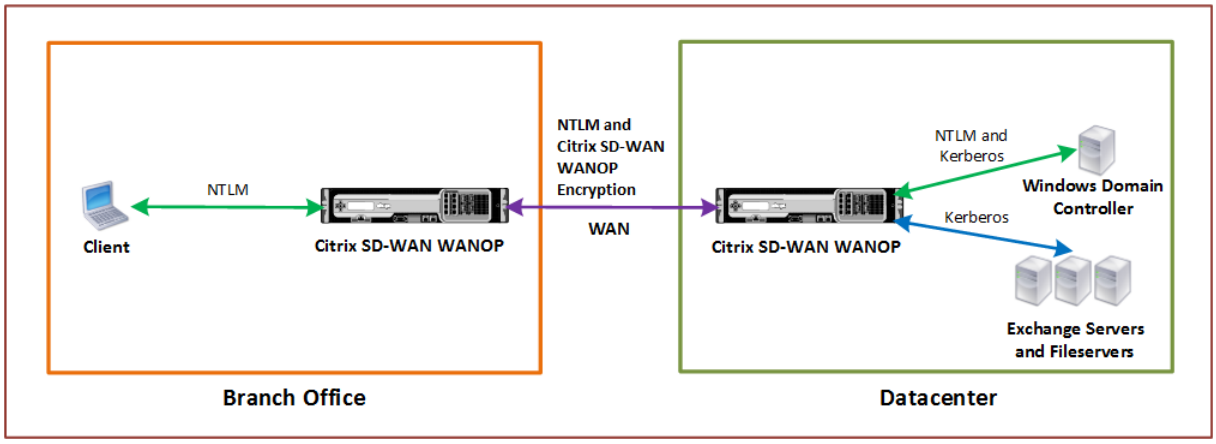
设备成为 Windows 安全基础结构的一部分后，用户必须先进行身份验证，然后才能访问资源。为了避免在域中配置大量用户的困难，您可以将身份验证责任委派给委派用户。

在活动目录中创建委托用户。此用户与普通用户类似，但具有特殊权限。创建委托用户后，必须在 Citrix SD-WAN WANOP 设备上配置此用户。当用户使用 Windows 协议（例如 CIFS 和 MAPI）访问经过身份验证和加密的数据流时，设备使用委托用户代表用户进行身份验证。

为了加速 CIFS 和 MAPI 流量，标准 Windows 委派机制允许您将安全委派限制到相关服务。自 Windows Server 2003 发布以来，此限制委派一直可用。

成为域的一部分后，设备会加速安全的 Windows 流量。加入 Windows 域的数据中心设备必须与远程设备或 Citrix SD-WAN WANOP 插件具有安全的对等关系，但只有数据中心设备才能加入 Windows 域。出于 CIFS 或 MAPI 加速的目的，远程设备充当数据中心设备的从属，通过两者之间的安全 SSL 隧道进行控制。因此，委派用户凭据不会离开数据中心。

下图显示了此设置的示例拓扑图。



在上图中，分支机构客户端访问数据中心的资源。分支机构客户端位于另一个域中，使用 NTLM 身份验证作为 Windows 安全系统的一部分。与安全对等关系中的两个 Citrix SD-WAN WANOP 设备之间的所有加速连接一样，通过 WAN 加密 CIFS 或 MAPI 连接和 NTLM 身份验证。根据 Windows 域控制器版本，来自数据中心 Citrix SD-WAN WANOP 设备的用户请求将使用 NTLM 或 Kerberos 身份验证协议进行身份验证。域对用户进行身份验证后，对 Exchange Server 和文件服务器的后续访问请求将使用 Kerberos 身份验证协议。然后，Citrix SD-WAN WANOP 设备优化客户端和服务器之间建立的连接。

如果设备没有安全的对等关系，或者如果数据中心设备未成功加入域，则这些连接将使用 TCP 流控制加速，该加速不执行任何安全操作、压缩或数据转换。建立客户端和服务器之间的连接，就好像 Citrix SD-WAN WANOP 设备不在那里一样。

您可以在 Windows 操作系统上配置不同的客户端身份验证模式。Citrix SD-WAN WANOP 设备优化的连接类型取决于您配置的客户端身份验证模式。

下表列出了 Windows 上的 Windows 客户端身份验证模式以及相应的 Citrix SD-WAN WANOP 优化。

Windows 操作系统支持身份验证和优化

客户端操作系统	客户端身份验证模式	优化	注意
Windows XP/Windows Vista/Windows7/Windows 8	协商身份验证 (SPNEGO)	TCP 流量控制加速，压缩，CIFS 协议加速	用于所有 Windows 版本的默认设置。
Windows XP/Windows Vista/Windows 7/Windows 8	仅限 NTLM 或仅限 Kerberos	仅 TCP 流量控制加速	非默认身份验证模式

注意：如果您使用仅 NTLM 或仅 Kerberos 客户端身份验证模式，则不会加速流量，如果它已加密。

将 **Citrix SD-WAN WANOP** 设备添加到 **Windows** 安全系统的要求

要优化安全的 Windows 签名 SMB 和加密的 MAPI 流量的流量，Citrix SD-WAN WANOP 部署必须满足以下要求，然后再将设备添加到 Windows 安全基础结构：

- 客户端和服务器端加速设备都必须建立安全的对等关系。
- 设备必须使用与 Windows 域服务器上的时间密切同步的 NTP 服务器。理想情况下，设备和 Windows 域服务器都是同一 NTP 服务器的所有客户端。
- 不能 为（非默认）仅 **Kerberos** 或仅 **NTLM** 选项配置 Outlook。加速需要使用默认（协商）选项。
- 客户端和服务器可以是与服务器端设备的域具有双向信任的任何域的成员。不支持单向信任。
- 必须在域控制器上设置 Kerberos 委托用户，以供参与域安全基础结构的设备使用。
- 域的 DNS 服务器 IP 地址必须配置并在服务器端设备上访问。
- 域服务器必须完全可访问，同时对 DNS 服务器上配置的域控制器的所有 IP 地址进行正向和反向查找。
- 服务器端 Citrix SD-WAN WANOP 设备的主机名必须唯一。使用默认主机名“主机名”可能会导致问题。

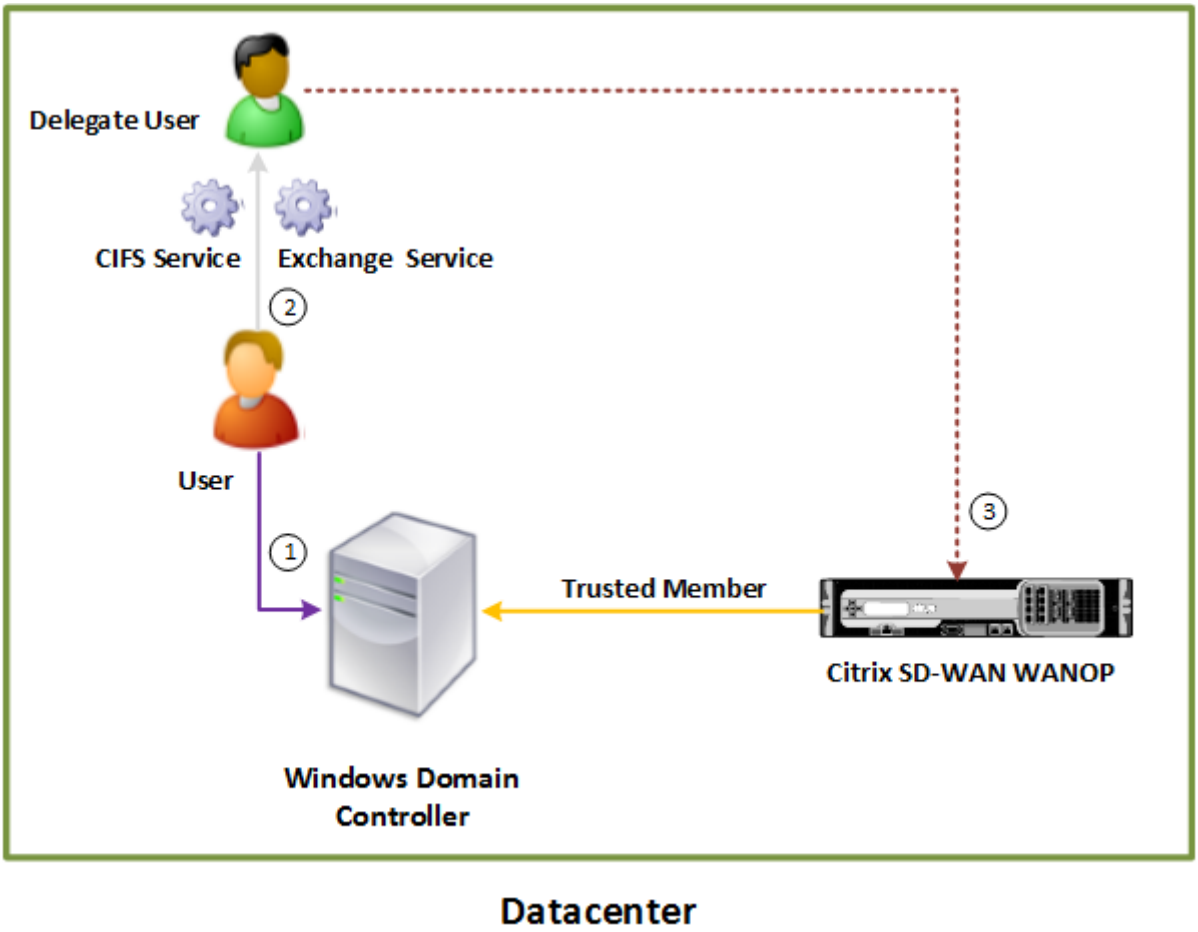
> 注意
>
> Macintosh Outlook 客户端不使用 MAPI (Outlook/Exchange) 标准，并且不加速此功能。

将 **Citrix SD-WAN WANOP** 设备添加到 **Windows** 安全基础结构

要优化安全 Windows 流量，Citrix SD-WAN WANOP 设备必须是 Windows 安全系统的一部分，并且必须使用安全系统或域对自身进行身份验证。如下图所示，要使设备成为 Windows 安全系统的一部分，必须使设备加入域（使用管理凭据）。此外，您需要通过将 CIFS 和 Exchange 服务与该用户关联，将新用户或现有用户配置为委托用户。然后，您必须在 Citrix SD-WAN WANOP 设备上配置此委托用户。

您可以使用 预域检查 实用程序来了解将设备加入域时是否存在任何问题。

> 注意
>
> Windows 安全系统使用 Exchange 服务来管理 MAPI 连接。配置设置以优化安全 Windows 流量



将 **Citrix SD-WAN WANOP** 设备加入到 **Windows** 域中：

当设备加入域时，它会与域控制器交换共享机密，从而允许设备无限期地保留域的一部分。将设备加入域时，请确保您拥有域控制器的管理员凭据。

若要确保 Citrix SD-WAN WANOP 设备优化了 CIFS 和 MAPI 流量（包括通过 HTTPS 封装为 RPC 的流量），必须将设备设置为 Windows 文件服务器和 Exchange Server 所属域的一部分。您需要将服务器端设备加入域。

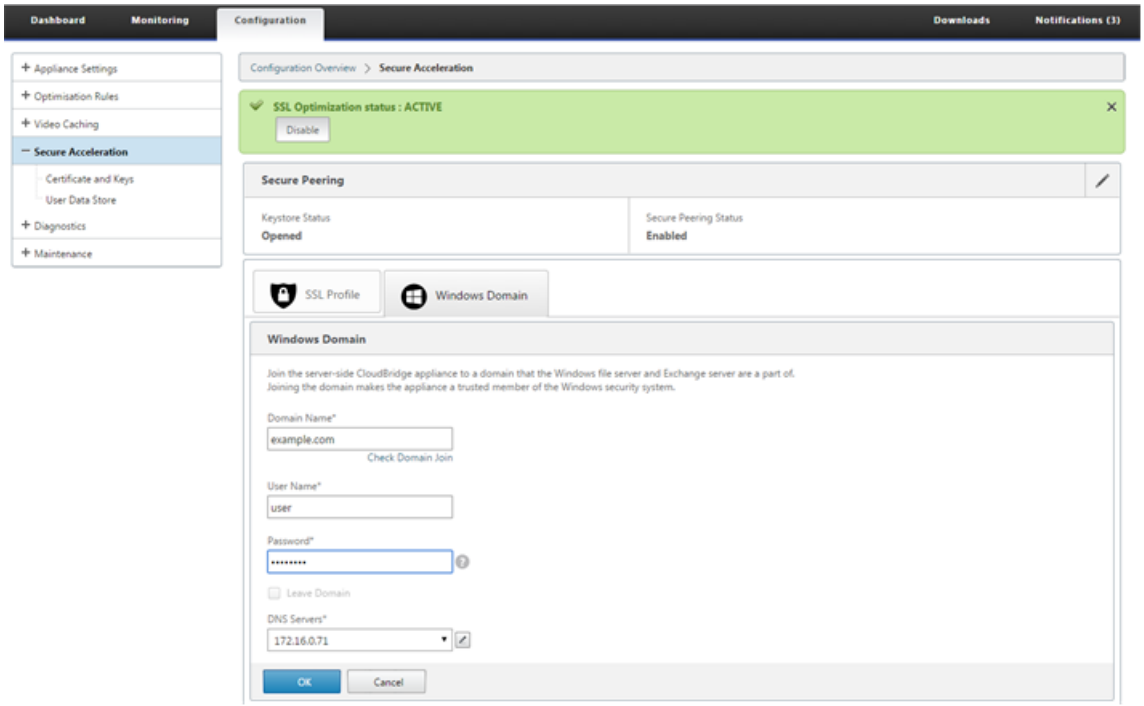
注意：域管理凭据不会保存在设备上。

要将 **Citrix SD-WAN WANOP** 设备加入到 **Windows** 域，请执行以下操作：

1. 导航到 配置 > 安全加速 > **Windows** 域 选项卡。
2. 单击 加入 **Windows** 域。
3. 在域名字段中输入 Windows 域名。
4. 在“用户名”字段中，输入域控制器管理员的用户名。
5. 在密码字段中，指定域控制器管理员密码。
6. 如有必要，请编辑 DNS 服务器，以便与 Windows 域保持一致。

7. 单击确定。

8. 在“委派用户”部分中，添加委派用户，如下面的过程所述。



配置委托用户：

将设备加入 Windows 域后，必须创建一个用户，该设备可用于对域的用户进行身份验证。此用户称为委 托用户。

注意：要创建委托用户帐户，您需要对 Windows 域控制器和设备的管理员访问权限。如果您没有 Windows 域控制器的管理员访问权限，请确保授权的管理员在域控制器上执行所需的任务。

通过使用 Kerberos 委派设置用户身份验证涉及两个任务：在域控制器上配置委托用户，然后将此用户添加到 Citrix SD-WAN WANOP 设备。

在域控制器上配置委托用户：

在 Citrix SD-WAN WANOP 设备上配置委派用户之前，必须在域控制器上配置具有所需属性的委派用户。您可以创建委托用户帐户或使用现有用户帐户作为委托用户帐户。

创建帐户或选择现有帐户后，为此用户启用委派。然后，您将委派用户与 CIFS 和 Exchange 服务关联，以便可以加速这些服务的流量。将此用户添加到 Citrix SD-WAN WANOP 设备后，设备将显示与此帐户关联的服务的委派凭据。

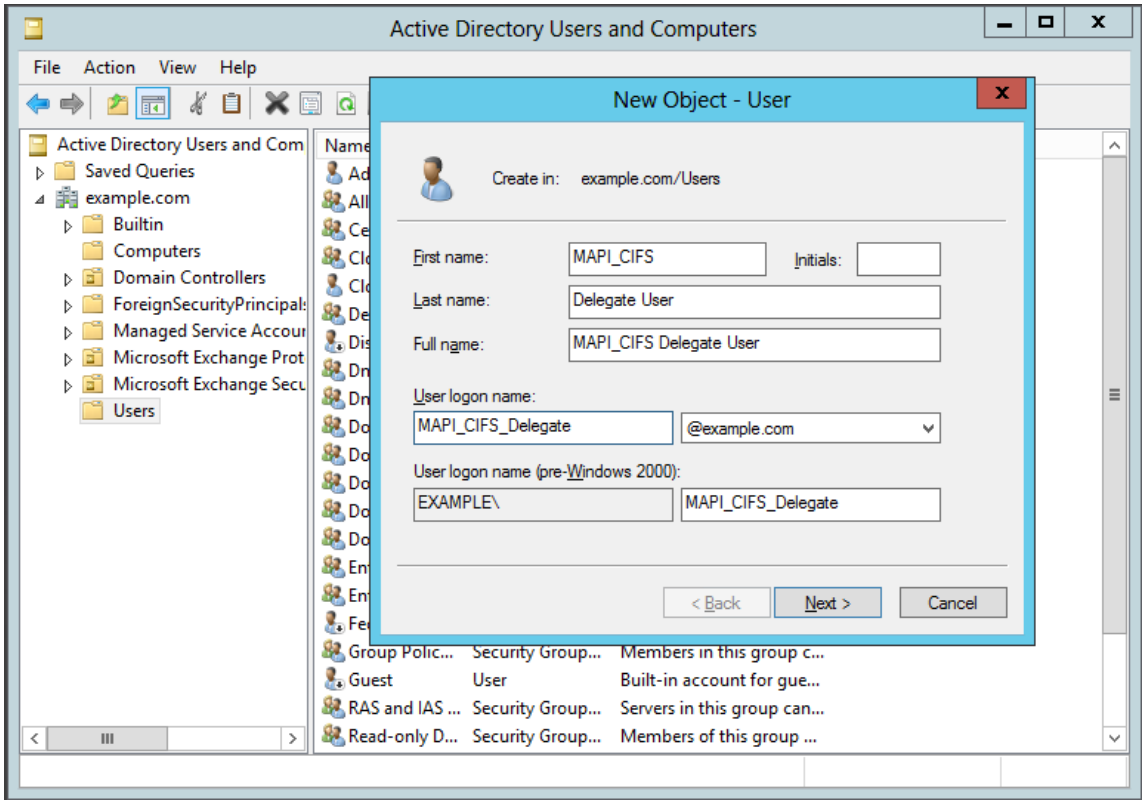
创建委托用户帐户：

在 Windows 域控制器上创建委派用户帐户，以便 Citrix SD-WAN WANOP 设备可以代表用户使用此帐户通过域控制器对其进行身份验证。

注意：如果要将现有用户配置为委托用户，请跳过此过程。

要创建委托用户帐户，请执行以下操作：

1. 以管理员身份登录到 Windows 域控制器。请确保文件服务器或 Exchange Server 是此域的成员。
2. 从“开 始 菜单中，打开 **Active Directory** 用户和计算机 窗口。
3. 创建委托用户，如以下屏幕截图所示：

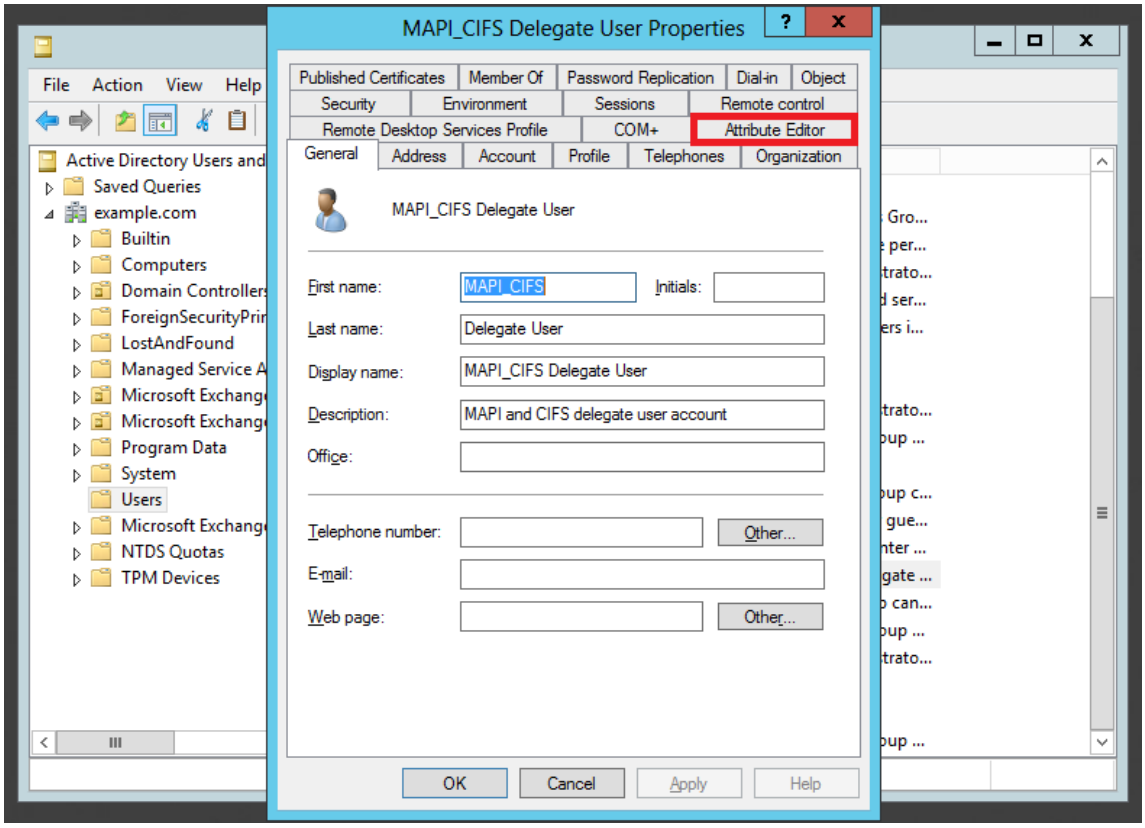


为用户启用委派：

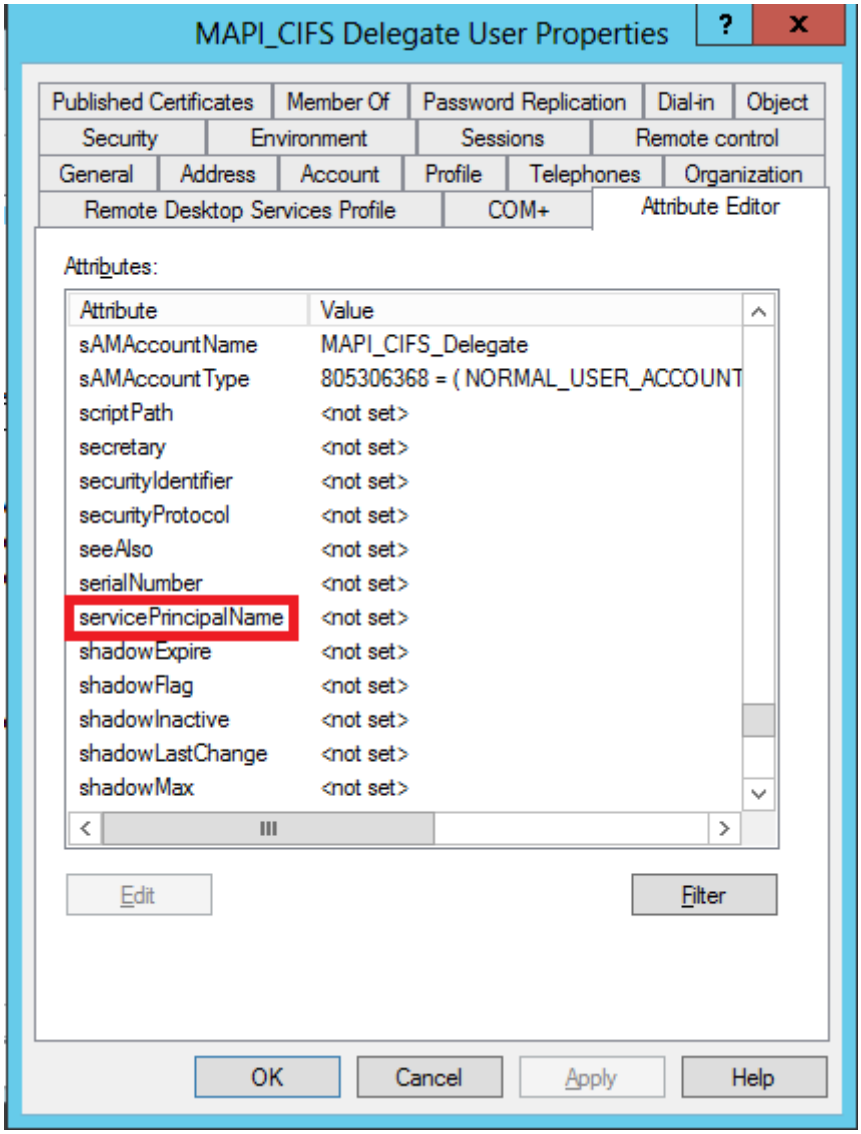
到目前为止，您创建的用户与您在 Active Directory 服务器上创建的任何用户类似。若要为用户启用委派，必须将委派用户的服务主体名称属性设置为 委派 并将委派用户与所需服务关联。这使得用户具有附加到它的特殊权限并使其成为委托用户。

要为用户启用委派，请执行以下操作：

1. 从“开 始 菜单中，打开 **Active Directory** 用户和计算机 窗口。
2. 从“视图”菜单中，选择 高级功能”。
3. 选择用 户 节点。
4. 右键单击要成为委托用户的用户。
5. 从快捷菜单中，选择“属 性 并导航到 属性编辑器 选项卡，如以下屏幕截图所示：

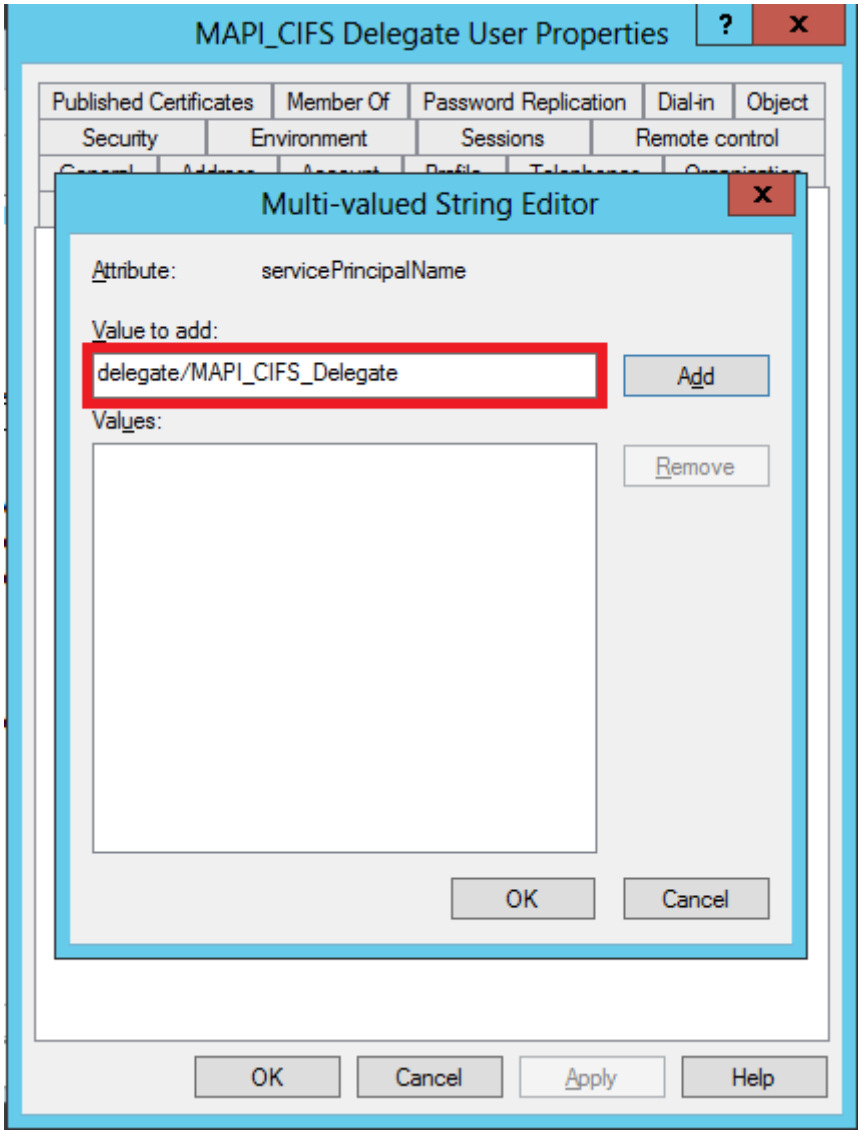


6. 从 属性 列表中，选择 **servicePrincipalName**，如以下屏幕截图所示：

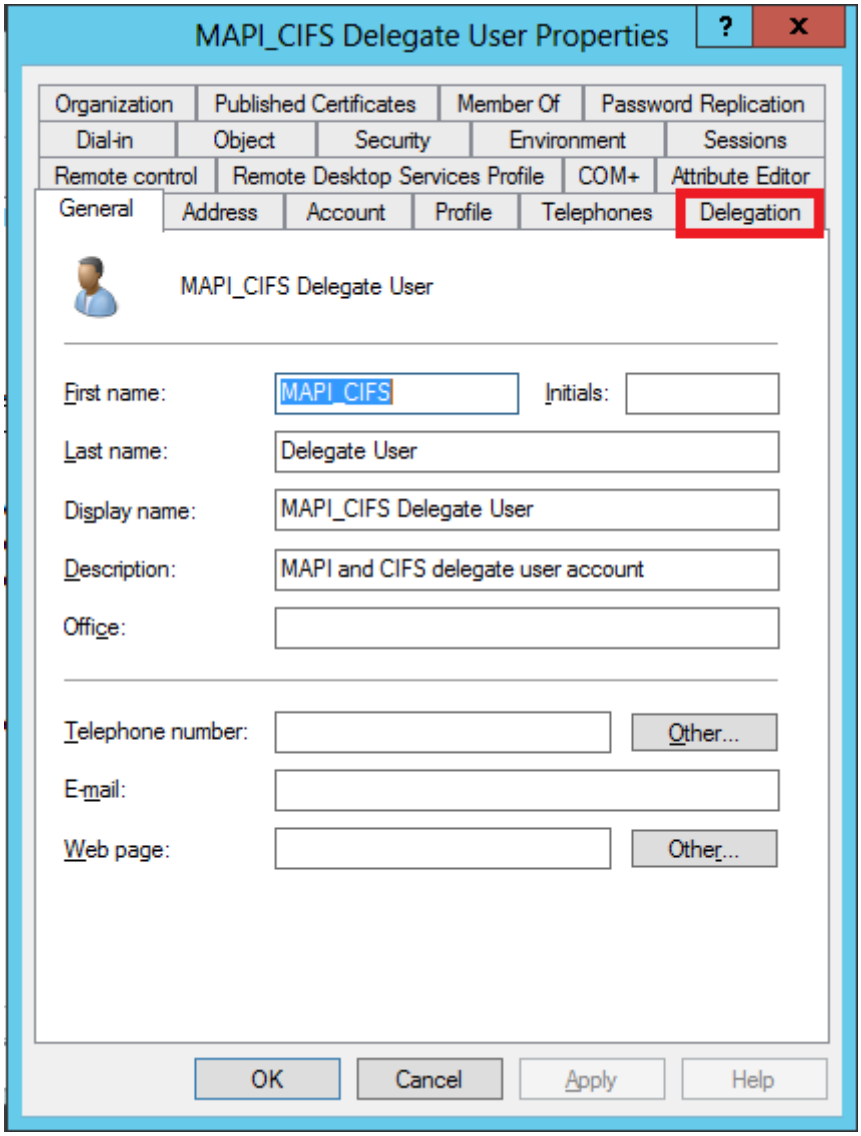


7. 单击编辑。

8. 在 多值字符串编辑器 对话框的 要添加的值 字段中，指定 委托 **/< User_Name >** ，如以下屏 幕 截图所示：



9. 单击添加。
10. 单击确定。
11. 单击应用。
12. 单击确定。
13. 打开用户的 **MAPI-CIFS** 委派用户属性 对话框，并验证是否已将“委 派 选项卡添加到对话框中，如以下屏幕截图所示：



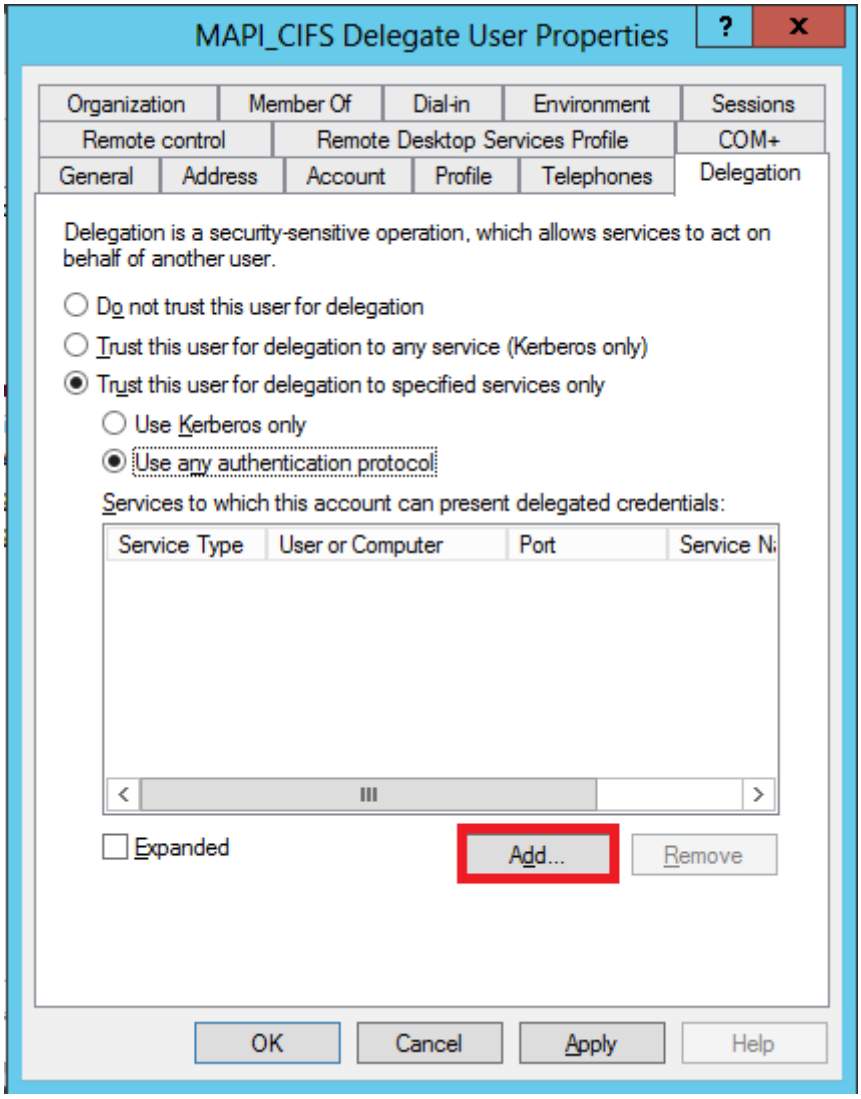
将委托用户与 **CIFS** 和 **Exchange** 服务关联：

为用户启用“委派”选项卡后，您可以将用户与用户可以为其提供委派凭据的服务关联。将此用户添加到 Citrix SD-WAN WANOP 设备时，设备会为与此帐户关联的服务提供委派凭据。

注意：Windows 安全基础结构使用 Exchange 服务来管理 MAPI 流量。

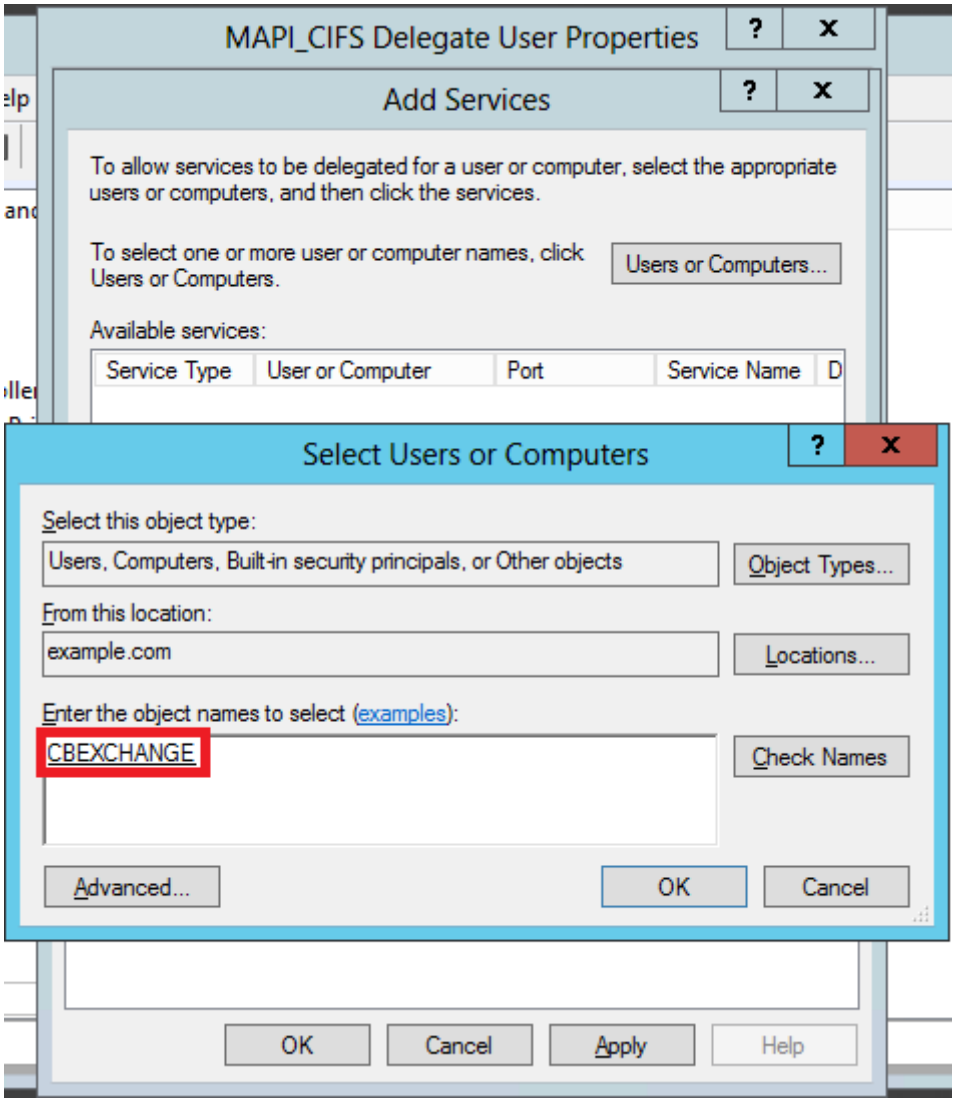
要将委派用户与 **CIFS** 和 **Exchange** 服务关联，请执行以下操作：

1. 在“委派”选项卡中，选择 信任此用户以便仅委派到特定服务 选项。
2. 选择“使 用任何身份验证协议 选项。
3. 单击 添加”，如以下屏幕截图所示：



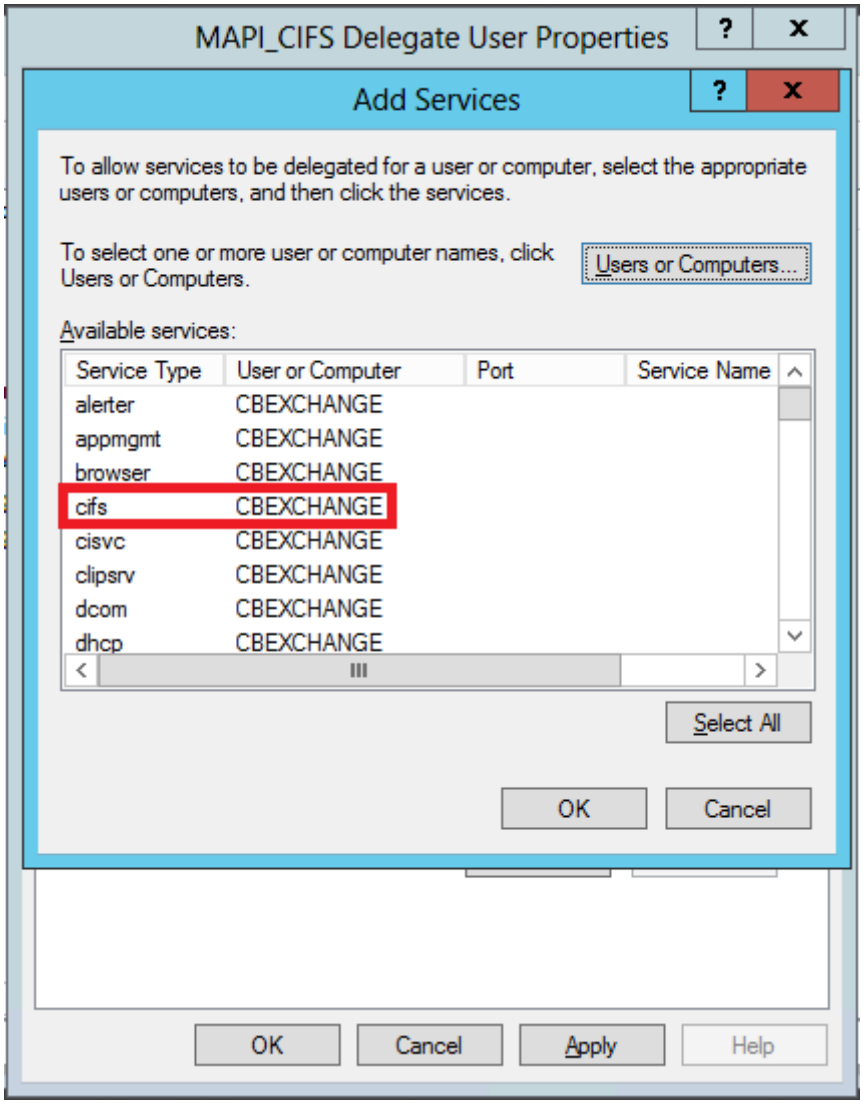
4. 在 添加服务 对话框中，单击 用户和计算机。

5. 在“选 择用户或计算机 对话框中，添加要选择的本地计算机，如以下屏幕截图所示：



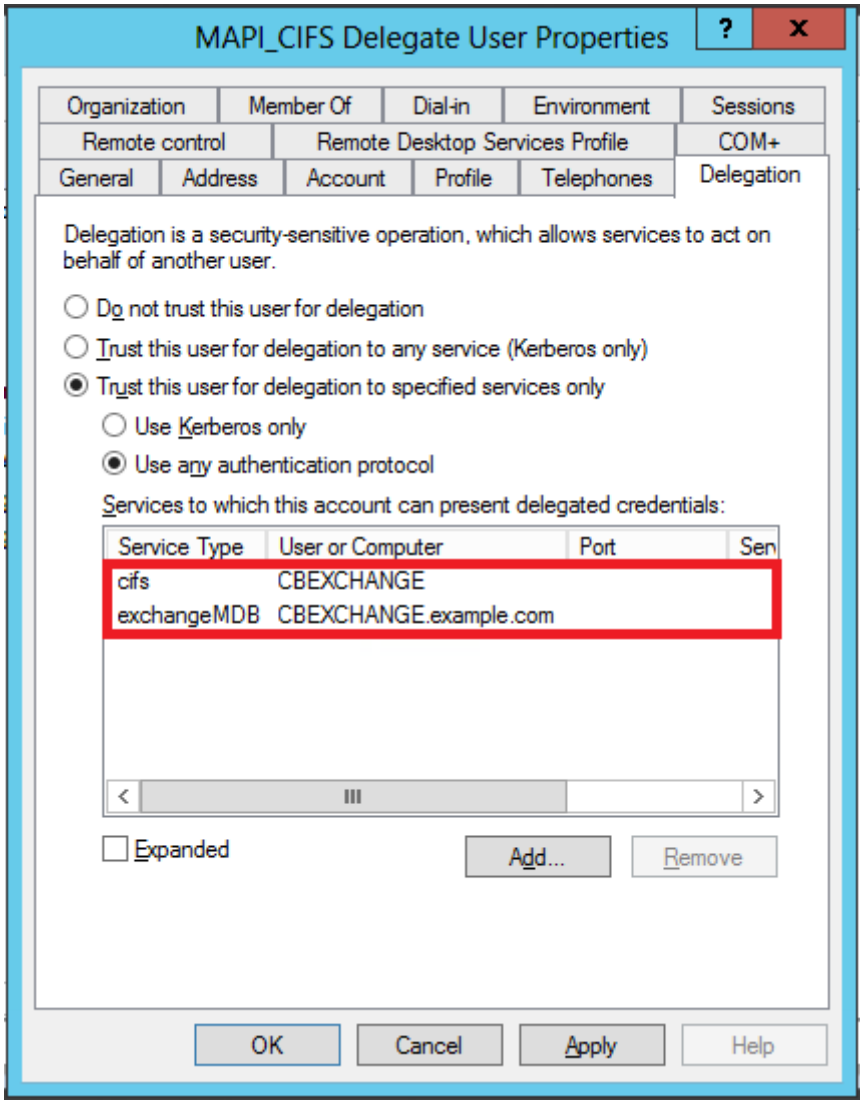
6. 单击 **OK**（确定）。

7. 在“添加服务”对话框中的 可用服务 列表中，选择 **cifs** ，如以下屏幕截图所示：



8. 如果您必须在 Citrix SD-WAN WANOP 设备上设置 MAPI 加速，请按住 **Ctrl** 键，然后选择 **exchangeMDB** 服务。

9. 单击 **OK**（确定）。您选择的服务将添加到 此帐户可向其呈现委派凭据的服 务列表中，如以下屏幕截图所示：



10. 单击 **OK**（确定）。
11. 关闭 **Active Directory** 用户和计算机 窗口。

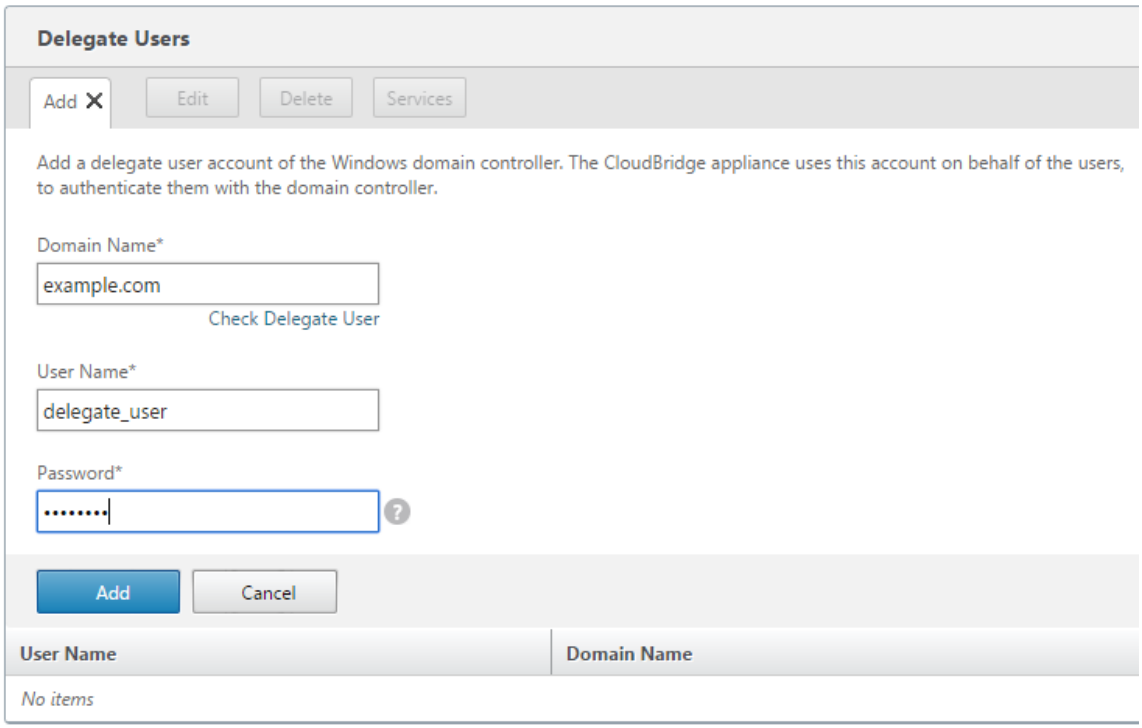
在 **Citrix SD-WAN WANOP** 设备上配置委托用户：

在 Active Directory 服务器上配置委派用户后，必须在 Citrix SD-WAN WANOP 设备上配置此用户，以便设备能够向域显示此用户的委派凭据。这样，设备就可以主动优化高级 CIFS 和 MAPI 加速功能的网络流量。

要将委托用户添加到服务器端设备，请执行以下操作：

1. 导航到 配置 > 安全加速 > **Windows** 域 选项卡。
2. 单击加入 **Windows** 域按钮（如果存在）。
3. 在 委派用户下，单击 添加。
4. 在 域名 字段中，指定域名。这通常是您在 **Windows** 域部分下指定的域。

5. 在“用 户名 字段中，输入委派用户的用户名。
6. 在 密码 字段中，指定委派用户的密码。
7. 单击添加。

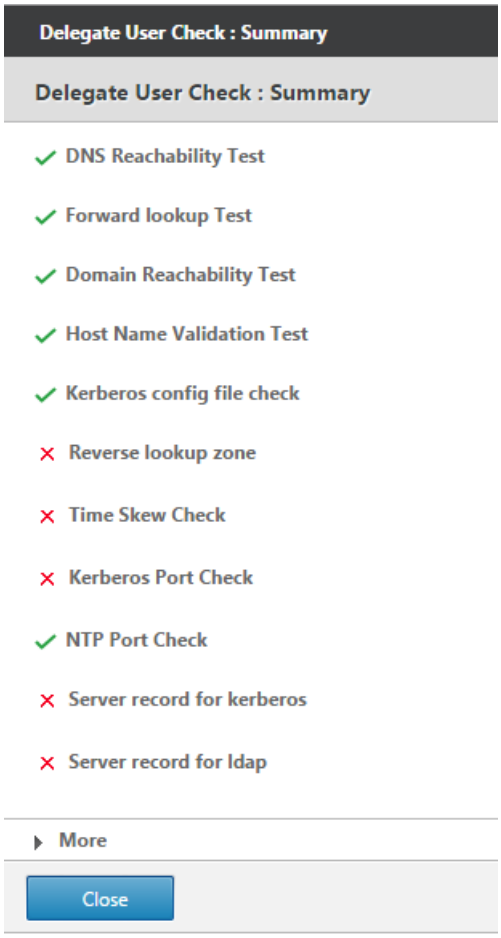


验证设备是否已加入域

如果在将设备添加到域后，您注意到设备未优化安全 Windows 流量，则某些错误可能导致设备无法加入域。您可以使用 预域检查 实用程序来查看加入域的设备是否存在任何问题。在尝试将设备加入域之前，您甚至可以运行此实用程序来确定可能出现的问题。

要检查委托用户，请执行以下操作：

1. 登录到服务器端 Citrix SD-WAN WANOP 设备。
2. 导航到配置 > 安全加速 > **Windows** 选项卡。
3. 单击加入 **Windows** 域按钮（如果存在）。
4. 选择一个委托用户，然后单击 编辑。
5. 点击 检查委托用户。
6. 等待委派用户域检查完成并检查结果。



配置 CIFS 和 SMB2/SMB3 加速

April 23, 2021

CIFS 加速功能为基于 CIFS（Windows 和 Samba）的文件传输和目录浏览提供了一套协议特定的性能增强功能，包括 CIFS 传输和相关协议（如 DCERPC）的增强功能。

CIFS 加速有三个部分：

- TCP 流量控制加速—无论协议版本（SMB1、SMB2 或 SMB3）或身份验证和加密程度如何，都会对所有加速 CIFS 连接执行此操作。
- CIFS 协议加速—这些优化通过减少运行 CIFS 命令所需的往返次数来提高 CIFS 性能。在 SMB1 和 SMB2 CIFS 连接上自动执行这些优化，这些连接要么不使用 CIFS 数据包身份验证（“签名”），要么使用签名并且设备已加入 Windows 域中的“安全委托”角色。
- CIFS 压缩—只要 CIFS 连接满足 CIFS 协议加速要求，就会自动压缩它们。此外，SMB3 连接在未签名和解密时进行压缩。

在启用了 CIFS 签名的网络上，CIFS 协议加速和压缩要求您禁用 CIFS 数据包身份验证（签名），或者让数据中心设备加入 Windows 域，并在数据中心设备和远程设备之间创建安全的对等关系和 Citrix SD-WAN WANOP 插件。

表 **1. CIFS** 加速功能，按 **SMB** 协议版本以及设备是否已加入 **Windows** 域。

SMB 版本	**TCP** 流控制	压缩	协议加速
		禁用签名	
SMB 1.0	Y	Y	Y
SMB 2.0	Y	Y	Y
SMB 2.1	Y	Y	N
SMB 3.0	Y	Y	N
		启用签名，*Citrix SD-WAN WANOP* 已加入域 **	
SMB 1.0	Y	Y	Y
SMB 2.0	Y	Y	Y
SMB 2.1	Y	Y	Y
SMB 3.0	Y	Y	Y *
		启用签名，*Citrix SD-WAN WANOP* 尚未加入域	
SMB 1.0	Y	N	N
SMB 2.0	Y	N	N
SMB 2.1	Y	N	N
SMB 3.0	Y	N	N

* SMB 3.0 支持已在 7.4.2 版中添加。

** Citrix SD-WAN WANOP 不支持 NTLMv2 身份验证 (默认适用于 Windows 7) 与 SMB 1/SMB 2/SMB 3 和 NetApp 服务器。启用 Kerberos 身份验证允许加速。

表 **2.** 客户端和服务器操作系统使用哪个 **SMB** 协议版本。

客户端/服务器 **OS**	**Windows 8**、**Windows 10** 或 **Windows Server 2012**	**Windows 7** 或 **Windows Server 2008 R2**	**Windows Vista** 或 **Windows Server 2008**	早期版本的 **Windows**
Windows 8、**Windows 10** 或 **Windows Server 2012**	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 或 **Windows Server 2008 R2**	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista 或 **Windows Server 2008**	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
早期版本的 **Windows**	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

支持的 **CIFS** 版本：

并非每个 CIFS 实现都使用设备识别的请求模式。这些不受支持的版本在所有情况下都无法实现加速，如下表所示。

表 **3. Citrix SD-WAN WANOP** 支持 **CIFS** 服务器和客户端。

产品	服务器	客户端
Windows Server 2003-2012	是 *	是 *
Windows XP、Vista 7、8、2000	是 *	是 *
NetApp	是 **	不适用
日立	是 **	不适用
Windows NT	是	否
Windows ME 及更早版本	否	否
其他	请参阅“注释”	请参阅“注释”

* 在 7.4.2 版中引入了 SMB 3.0 支持。

在 7.4.2 版本之前，尚未对 SMB 3.0 的 ** 操作进行测试。

> 注意：大多数第三方 CIFS 实现模拟上面列出的服务器或客户端之一。在仿真成功的范围内，流量会加速或不加速，如上表所示。如果仿真的行为与 CIFS 加速器期望的行为不同，则该连接将终止 CIFS 加速。

在对给定 CIFS 实现的 CIFS 加速行为进行测试之前，无法确定知道。

CIFS 加速模式如下：

- 大文件读取和写入
- 小文件读取和写入
- 目录浏览。

大型文件读取和写入—这些 SMB1 优化适用于至少 640 KB 的文件传输。安全预读和后写技术用于流式传输数据，而不会暂停每次传输（传输不超过 64 KB）。

只有当传输具有 BATE 或独占锁并且“简单”时，才会启用这些优化。“文件副本总是简单的。通过应用程序打开的文件可能是也可能不是，具体取决于它们在应用程序中的处理方式。

CIFS 加速可以很容易地获得 10 倍的加速比，前提是您的链路和磁盘速度足以容纳当前传输速度的十倍。如有必要，可以获得 50 倍的加速，但由于内存消耗，通常不能启用。如果 10 倍不够，请联系您的 Citrix 代表。

小文件读取和写入—小文件增强更多地围绕元数据（目录）优化，而不是围绕数据流。本机 CIFS 不会以高效的方式组合元数据请求。CIFS 加速是如此。与大文件加速一样，除非它们是安全的，否则不会执行这些优化（例如，如果 CIFS 客户端未被授予目录上的排他锁，则不会执行这些优化）。使用 SMB2 协议时，文件元数据将在本地缓存，以便进行更大的改进。

目录浏览—标准 CIFS 客户端以极低效率的方式执行目录浏览，需要大量往返打开远程文件夹。CIFS 加速度将往返次数减少到 2 或 3 次。使用 SMB2 协议时，目录数据会在本地缓存，以进行更大的改进。

CIFS 协议加速

所有型号都支持 CIFS 加速。CIFS 是一种基于 TCP 的协议，并从流量控制中受益。然而，CIFS 的实施方式在长途网络上效率很低，需要过多的往返旅行才能完成一项业务。由于协议对链路延迟非常敏感，因此完全加速必须具有协议感知。

CIFS 加速度通过各种技术减少往返行程次数。分析来自客户端的请求模式，并预测其下一个操作。在许多情况下，即使预测错误，也可以安全地采取行动，这些安全操作是许多优化的基础。

例如，SMB1 客户端以非重叠的方式发出顺序文件读取，等待每个 64KB 读取完成，然后再发出下一个读取。通过实现预读，设备可以通过提前获取预期数据来安全地提供高达 10 倍的加速度。

其他技术可加速目录浏览和小文件操作。加速不仅应用于 CIFS 操作，还应用于相关的 RPC 操作。

必备条件

所有型号都支持 CIFS 加速。CIFS 是一种基于 TCP 的协议，并从流量控制中受益。然而，CIFS 的实施方式在长途网络上效率很低，需要过多的往返旅行才能完成一项业务。由于协议对链路延迟非常敏感，因此完全加速必须具有协议感知。

CIFS 加速度通过各种技术减少往返行程次数。分析来自客户端的请求模式，并预测其下一个操作。在许多情况下，即使预测错误，也可以安全地采取行动，这些安全操作是许多优化的基础。

例如，SMB1 客户端以非重叠的方式发出顺序文件读取，等待每个 64KB 读取完成，然后再发出下一个读取。通过实现预读，设备可以通过提前获取预期数据来安全地提供高达 10 倍的加速度。

其他技术可加速目录浏览和小文件操作。加速不仅应用于 CIFS 操作，还应用于相关的 RPC 操作。

如果您的网络使用 CIFS 签名，则设备必须是域的受信任成员。要使设备成为域的受信任成员，请参阅将 Citrix SD-WAN WANOP 设备添加到 Windows 安全基础结构。

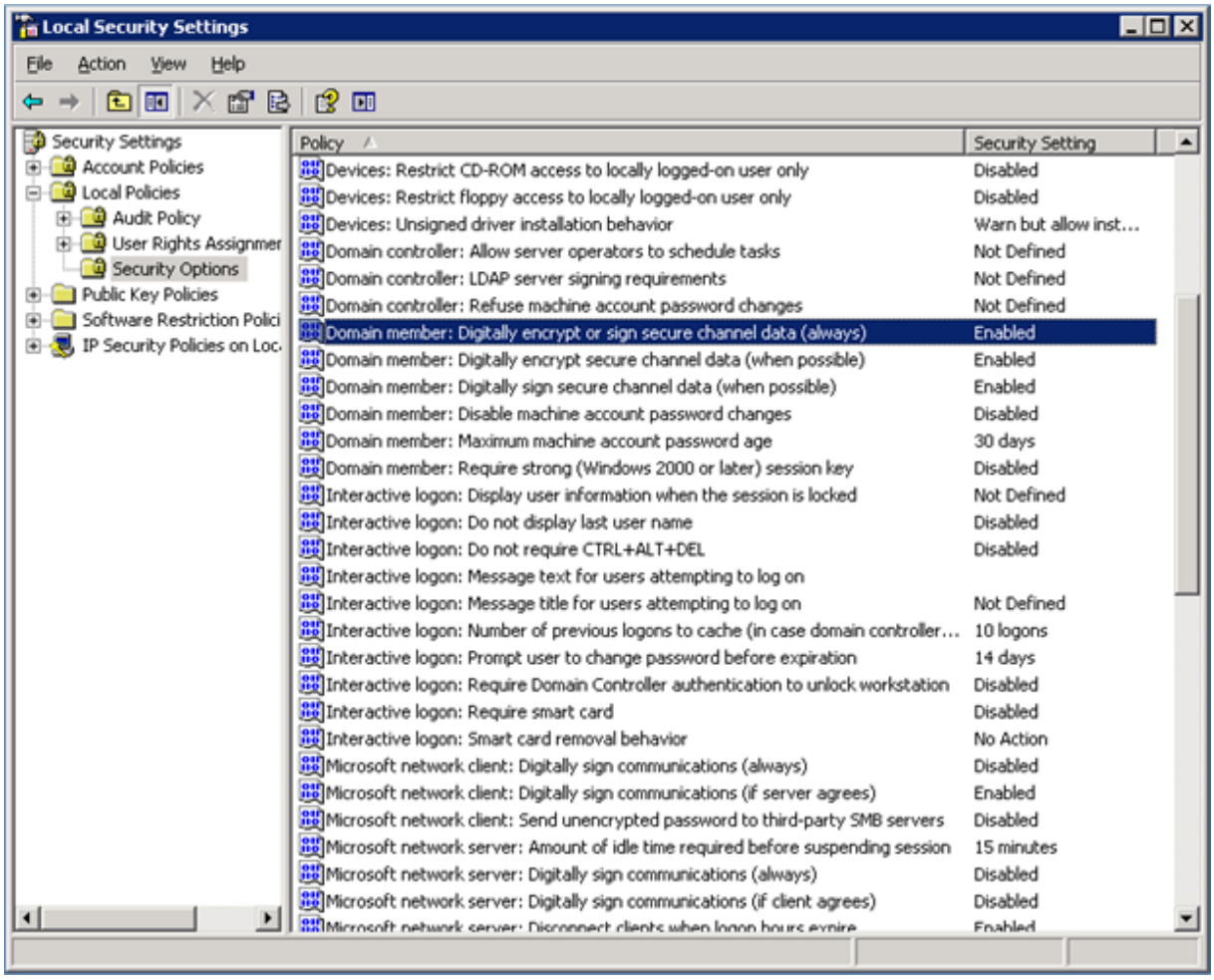
配置 **CIFS** 协议加速

默认情况下，对于不使用 CIFS 签名的连接，将启用 CIFS 加速。如果您的网络使用签名，则可以禁用该签名，也可以禁用服务器端设备加入 Windows 域。

禁用 **CIFS** 签名

根据其安全设置，Windows Server 或域服务器可能需要调整其安全设置。

图 1. Windows Server 安全选项、Windows Server 2003 和 Windows Server 2008。



Windows 文件服务器有两种安全模式：“密封”和“签名”。

密封加密数据流并完全防止 CIFS 协议加速。

签名将身份验证数据添加到每个数据包，而无需加密数据流。这可以防止加速，除非您已经实施了中描述的过程将 Citrix SD-WAN WANOP 设备添加到 Windows 安全基础结构。满足此要求时，签名将自动加速。否则，必须禁用签名（如果尚未禁用签名）才能进行协议加速。

默认情况下，Windows 文件服务器提供签名，但不需要签名，域服务器除外，默认情况下需要签名。

要使用当前需要签名的系统实现 CIFS 加速，您必须更改系统安全设置以禁用此要求。您可以在文件服务器上的本地安全设置或组策略中执行此操作。以下示例（对于 Windows Server 2003 和 Windows Server 2008）显示了本地设置。当然，集团政策的变化几乎完全相同。

Citrix SD-WAN WANOP

更改服务器设置以允许 **CIFS** 加速

1. 导航到系统的“本地安全设置”页面。

2. 设置域成员：数字加密或签署安全通道数据（始终）为禁用。
3. 将 Microsoft 网络客户端：将通信数字签名（始终）设置为禁用。
4. 将 Microsoft 网络服务器：将通信数字签名（始终）设置为已禁用。

解释 **CIFS** 统计数据

监视：文件系统 (CIFS/SMB) 页面显示了加速 CIFS 连接的列表。这些连接分为“优化”和“非优化”连接。因为所有这些连接都加速（使用流量控制和压缩），所以“优化”连接除了流量控制和压缩外还具有 CIFS 优化，而“非优化”连接仅具有流量控制和压缩。

CIFS 管理摘要

- 即使在相对较短的链路距离下，CIFS 加速也能显著提高。
- CIFS 加速在客户端首次访问文件系统时开始。如果在文件服务器和客户端已启用并正在运行的情况下启用了加速，则在多分钟内不会发生加速，直到预先存在的 CIFS 连接完全关闭。CIFS 连接是非常持久的，并且在关闭自身之前持续很长时间，即使在空闲时也是如此。这种行为在测试期间很烦人，但在正常部署中没有什么重要性。
- 卸载和重新装载 Windows 中的文件系统不会关闭 CIFS 连接，因为 Windows 不会真正卸载文件系统。重新启动客户端或服务器的工作。对于侵入性较小的措施，请使用 Windows 命令行中的 NET USE 设备名称 /DELETE 命令完全卸载卷。在 Linux 中，smbmount 和卸载完全卸载卷。
- 在设备上禁用然后重新启用 CIFS 读取和写入优化会引起类似的问题。启用 CIFS 时，现有连接不会加速，并且“监视：文件系统 (CIFS/SMB) 页面上检测到的协议错误”数量会短暂增加。
- CIFS 统计信息可能会令人困惑，因为只有离文件服务器最远的设备才会报告 CIFS 加速时使用完整统计信息。另一个设备将其视为普通加速度。
- 在代理模式下不支持 CIFS 加速。
- 如果 Windows Server 没有进行 CIFS 加速，请检查服务器的安全设置。

配置 **MAPI** 加速

April 23, 2021

Microsoft Outlook 加速为 Microsoft Outlook 客户端和 Microsoft Exchange Server 之间的流量提供了改进的性能，通过各种优化（包括数据预取和压缩）增加吞吐量。

此功能也称为“MAPI 加速”，在 Outlook 与 Exchange Server 之间使用的 MAPI 协议之后。

在 Outlook 数据流未加密的网络中（Outlook 2007 之前的默认值），此功能不需要任何配置。

(在对 Outlook 数据进行加密的网络（默认为 Outlook 2007 及更高版本）中，可以通过以下两种方式之一获得加速：通过禁用 Outlook 客户端中的加密或通过让设备加入 Windows 域 []/en-us/citrix-sd-wan-wanop/11-1/secure-traffic-acceleration/cifs-smb2-mapi.html。)

支持的 **Outlook** 交换版本和模式

Citrix SD-WAN WANOP 设备在以下情况下提供 MAPI 加速的 Microsoft Outlook 2003-2016 和 Exchange Server 2003-2010：

- 支持支持的客户端和服务器的任何组合（使用 MAPI 协议）。
- 如果服务器端设备已加入 Windows 域，则使用 MAPI 加密的连接将加速。否则，它们不是，并且应在 Outlook 客户端中禁用加密。

> 注意
>
> 在 Exchange Server 2013 MAPI 协议更改为 RPC 通过 HTTP 协议，支持 此协议。使用 Exchange Server SP1 时，通过 HTTP 协议的 RPC 更改为 MAPI 通过 HTTP 协议，目前不支持此协议。

必备条件

如果您的网络使用加密的 Outlook 数据（这是 Outlook 2007 及更高版本中的默认设置），则必须实现以下先决条件之一，以确保 MAPI 连接加速：

- 禁用 Outlook 客户端中的加密。
- 执行中描述的任务将 Citrix SD-WAN WANOP 设备添加到 Windows 安全基础结构。

配置

Outlook 加速是默认情况下启用的零配置功能。（如果不需要，可以通过在 “
配置：服务类策略” 页面上禁用 **MAPI** 服务类 的加速来禁用它。）Outlook 加速自动发生，如果满足以下条件：

- WAN 的 Exchange Server 端有一个设备。
- WAN 的 Outlook 末端有一个设备，或者运行 Outlook 的系统也在运行 Citrix SD-WAN WANOP 插件。
- 所有 Outlook/Exchange 流量通过设备（或设备和插件）。
- 重新启动 Exchange Server 或 Outlook（加速不会开始，直到现有的 MAPI 连接关闭）。
- 在 Outlook 上禁用加密，或者服务器端设备属于 Windows 域并与客户端设备（或 Citrix SD-WAN WANOP 插件）具有安全的对等关系。在设备已加入 Windows 域的情况下，域上的身份验证必须保留在默认设置（协商），以便加速工作。

禁用对 **Outlook 2007** 或 **2010** 年展望上的加密

除非服务器端设备已加入 Windows 域并与客户端设备（或 Citrix SD-WAN WANOP 插件）具有安全的对等关系，否则必须禁用 Outlook 和 Exchange Server 之间的加密才能进行加速。

默认情况下，在 Outlook 2007 之前禁用了加密。从 Outlook 2007 开始，默认情况下启用加密。

执行情况说明

MAPI 使用与其他协议不同的数据格式。这种差异阻碍了有效的跨协议压缩。也就是说，首先通过 FTP 传输，然后作为电子邮件附件传输的文件在第二次传输时不会获得压缩优势。如果以 MAPI 格式发送两次相同的数据，则第二次传输将收到完全压缩。

SSL 压缩

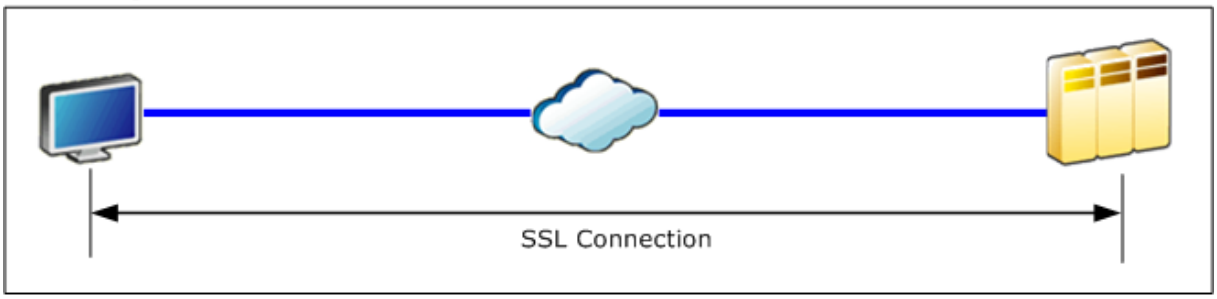
April 23, 2021

Citrix SD-WAN WANOP SSL 压缩将多会话压缩应用于 SSL 连接（例如，HTTPS 流量），提供高达 10000:1 的压缩比。

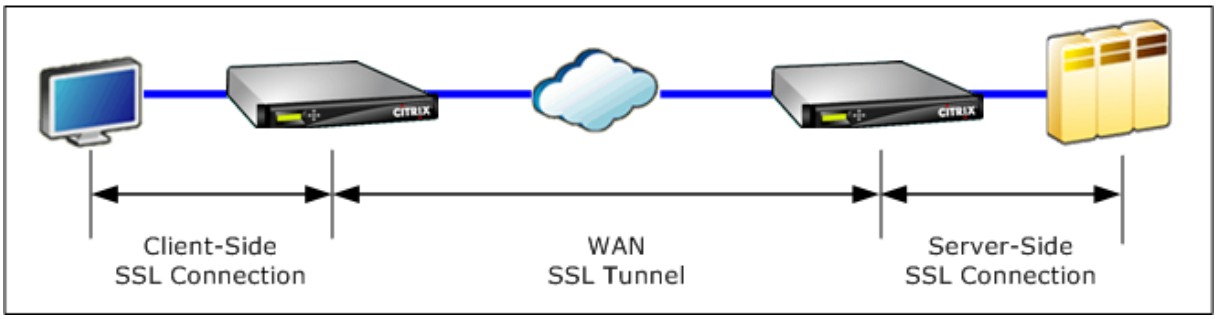
> 注意
>
> SSL 压缩需要加速链路末端的两个设备之间的安全对等（信令）连接。

通过将连接拆分为三个加密区段，从端到端维护加密：客户端设备、客户端设备到服务器端设备以及服务器端设备到服务器端设备。

Ordinary SSL Connection



Accelerated SSL Connection



警告：SSL 压缩会解密加密的数据流，除非使用“用户数据加密”选项，否则两个加速单元的压缩历史记录都会保留已解密数据的明文记录。验证您的部署和设置是否与组织的安全策略一致。Citrix 建议您在配置 SSL 加速所需的安全对等信号连接时启用对每个单元的压缩历史记录的加密。

> 注意
>
> - 启用 SSL 压缩后，设备将停止尝试与其没有安全对等关系的其他设备（无论是 Citrix SD-WAN WANOP 还是 SD-WAN WANOP 插件）进行压缩。因此，此功能最适合将所有设备配置为 SSL 压缩的网络。
> - 启用 SSL 压缩后，您必须在每次重新启动设备时手动键入密钥存储密码。

SSL 压缩的工作原理

April 23, 2021

SSL 压缩可以访问连接的明文数据，因为服务器端设备充当端点服务器的 安全委托。这种行为是可能的，因为服务器端设备配置了服务器安全凭证（私钥和证书）的副本，使其能够代表服务器执行操作。对于客户端，此行为等同于直接与端点服务器进行通信。

由于设备作为服务器的安全委托工作，因此大多数配置位于服务器端设备上。客户端设备（或插件）充当服务器端设备的卫星，不需要每个服务器配置。

服务器端和客户端设备通过 *SSL* 信令连接共享会话状态。无论原始连接是否加密，两台设备之间的所有加速连接都通过 *SSL* 数据连接发送。

注意：SSL 压缩不一定会加密所有链接流量。最初加密的流量保持加密，但未加密的流量并不总是加密。设备不会尝试加密未加速的流量。由于不能绝对保证任何给定的连接都会被加速（各种事件阻止加速），因此不能保证设备会加密给定的未加密连接。

SSL 压缩工作在以下两种模式之一：透明代理或拆分代理。这两种模式支持略有不同的 SSL 功能。您可以选择提供给定应用程序所需功能的模式。

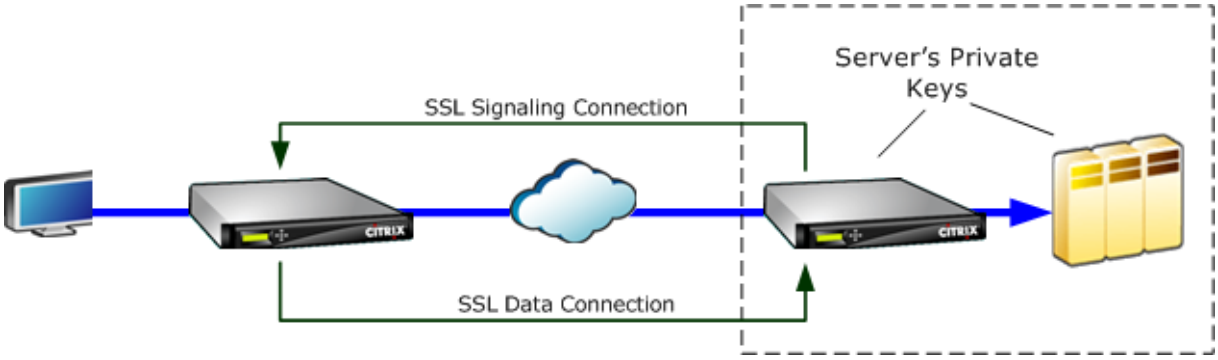
使用哪种 **SSL** 代理模式- 仅当您需要真正的客户端身份验证（即正确标识单个端点节点客户端的身份验证）并且您不需要 Diffie-Hellman、Temp RSA、TLS 会话票证时，才使用 SSL 透明代理模式，SSL 版本 2，或会话重新协商。对所有其他部署使用 SSL 拆分代理。

SSL 透明代理

在 *SSL* 透明代理模式下（不要与 Citrix SD-WAN WANOP 插件上的透明模式混淆），服务器端设备伪装为服务器。服务器的凭据（证书密钥对）安装在服务器端设备上，以便它可以代表服务器执行操作。然后，服务器端设备将客户端设备配置为处理连接的客户端。服务器的凭据未安装在客户端设备上。

在此模式下支持真正的客户端身份验证，但临时 RSA 和 Diffie-Hellman 不支持。SSL 透明代理模式适用于需要客户端身份验证的应用程序，但前提是不需要以下功能：Diffie-Hellman、Temp RSA、TLS 会话票证、SSL 版本 2。此外，不得尝试重新协商会话，否则连接终止。

客户端设备无需进行任何配置（与服务器端设备配置安全对等关系除外），并且客户端不需要配置，客户端将连接与服务器直接通信一样处理。



SSL 拆分代理

SSL 拆分代理模式 在大多数情况下是首选的，因为它支持许多应用程序需要的临时 RSA 和 Diffie-Hellman。在 SSL 拆分代理模式下，服务器端设备伪装为客户端的服务器，伪装为服务器的客户端。您可以在服务器端设备上安装服务器凭据（证书密钥对），以允许其代表服务器执行操作。

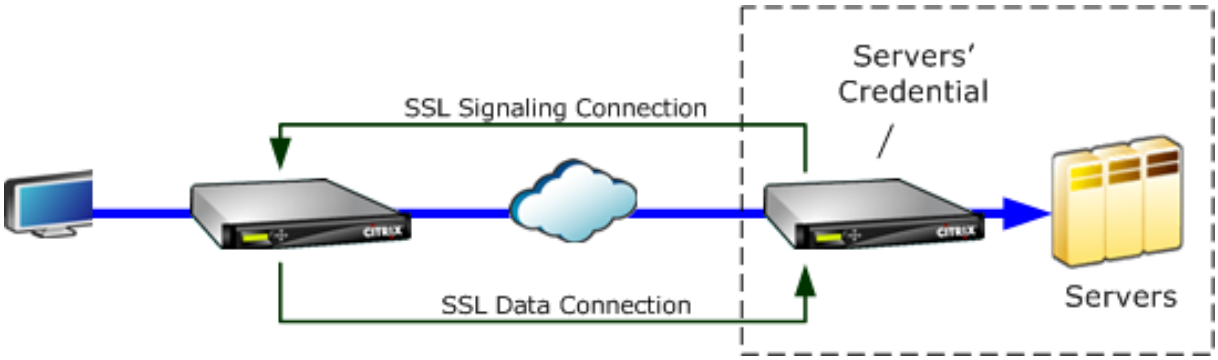
如果您安装可选的客户端凭据，则拆分代理模式还支持代理客户端身份验证，如果端点服务器应用程序请求客户端身份验证，则会显示这些凭据。将显示这些客户端凭据，而不是实际的端点节点客户端的凭据。（如果应用程序需要端点客户端凭据，请使用透明代理。）

由于在此模式下不支持真正的客户端身份验证，因此服务器无法对实际的端点客户端进行身份验证。如果服务器端设备未配置客户端凭据，则服务器端应用程序在客户端身份验证时所做的所有尝试都将失败。如果服务器端设备配置了客户端凭据，则无论实际客户端的身份如何，都将使用这些凭据回复所有客户端身份验证请求。

客户端设备不需要配置（与服务器端设备配置安全对等关系除外），并且客户端不需要配置，客户端上将连接视为直接与服务器通信。服务器端设备上的服务器凭据未安装在客户端设备上。

要支持多个服务器，可以在设备上安装多个私有证书密钥对，每个 SSL 配置文件一个。服务类定义中的特殊 SSL 规则将服务器与 SSL 配置文件匹配，因此 SSL 配置文件与凭据匹配。

在 SSL 拆分代理模式下，CA 证书和证书密钥对以及 CA 证书实际上不必匹配服务器的证书，尽管它们可以。由于拆分代理的性质，服务器端设备可以使用客户端应用程序可以接受的凭据（由受信任的机构颁发的有效凭据）。请注意，在 HTTPS 连接的情况下，如果公用名与 URL 中的域名不匹配，Web 浏览器会发出警告。一般来说，使用服务器凭据的副本是更无故障的选项。



配置 **SSL** 压缩

April 23, 2021

Citrix SD-WAN O SSL 压缩功能可实现 SSL 连接的多会话压缩（例如，HTTPS 流量），提供高达 10000:1 的压缩比。有关详细信息，请参阅SSL 压缩。

要使 SSL 压缩工作，Citrix SD-WAN WANOP 设备需要来自服务器或客户端的证书。要支持多个服务器，可以在设备上安装多个私钥，每个 SSL 配置文件一个。服务类定义中的特殊 SSL 规则将服务器与 SSL 配置文件匹配，因此 SSL 配置文件与私钥匹配。

SSL 压缩工作在拆分代理或透明代理模式下，您可以根据您的要求选择模式。有关详细信息，请参阅SSL 压缩的工作原理。

> 注意
>
> 目前不支持透明代理模式。

为了使用 SSL 隧道启用安全访问，SSL 代理中使用了最新的 SSL 协议 TLS 1.2。您可以选择仅使用 TLS1.2 协议或使用 TLS1.0、TLS1.1 和 TLS1.2 协议。

> 注意
>
> SSL 协议 SSL v3 和 SSL v2 不再受支持。

要配置 **SSL** 压缩，请执行以下操作：

1. 获取服务器的 CA 证书和私有证书密钥对的副本，并将其安装在服务器端设备上。这些凭据可能是特定于应用程序的。也就是说，服务器的 Apache Web 服务器的凭据可能与通过 HTTPS 运行 RPC 的 Exchange Server 的凭据不同。
2. 您可以选择创建拆分代理 SSL 配置文件或透明代理 SSL 配置文件。

   有关配置拆分代理 SSL 配置文件的信息，请参阅下面的 配置拆分代理 **SSL** 配置文件 部分。

   有关配置透明代理 SSL 配置文件的信息，请参阅下面的 配置透明代理 **SSL** 配置文件 部分。

   > 注意
   >
   > 目前不支持透明代理 SSL 配置文件。

3. 将 SSL 配置文件附加到服务器端设备上的服务类。这可以通过基于服务器 IP 创建新服务类或修改现有服务类来完成。

   有关更多信息，请参阅下面的 创建或修改服务类 部分。
4. 在客户端设备上设置服务类。SSL 流量不会被压缩，除非它属于客户端设备上的服务类，从而启用加速和压缩。这可以是普通的服务类规则，而不是 SSL 规则（只有服务器端设备需要 SSL 规则），但必须启用加速和压缩。流量属于现有服务类，如“HTTPS”或“其他 TCP 流量”。如果此类的策略启用加速和压缩，则不需要其他配置。
5. 验证规则的操作。通过设备发送应接收 SSL 加速的流量。在服务器端设备上，在“监视：优化：连接：加速连接”选项卡上，服务类列应与您为安全加速设置的服务类匹配，SSL 代理列应为适当的连接列出 True。

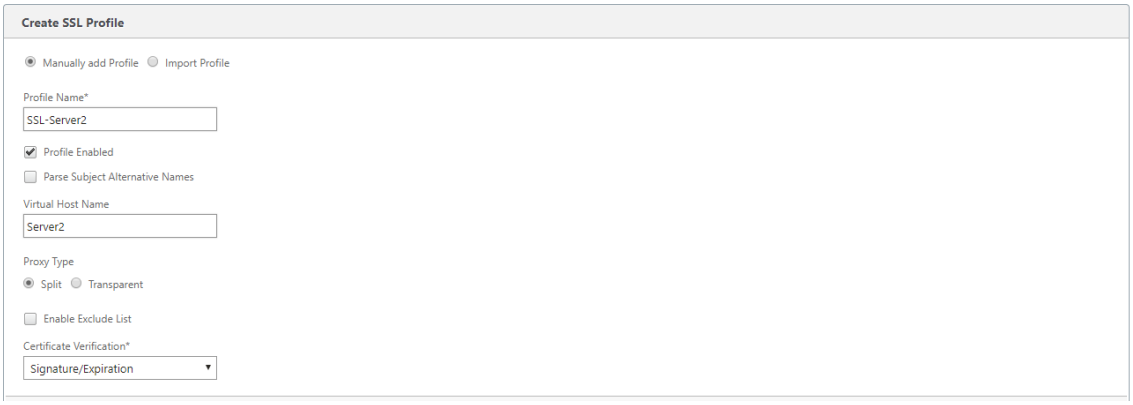
配置拆分代理 **SSL** 配置文件

要配置拆分代理 **SSL** 配置文件，请执行以下操作：

1. 在服务器端 Citrix SD-WAN O 设备中，导航到 配置 > 安全加速 > **SSL** 配置文 件，然后单击 添加配置文件。

   > 注意
   >
   > 您可以手动添加 SSL 配置文件或导入存储在本地计算机上的配置文件。

2. 在 配置文件名称 字段中，输入 SSL 配置文件的名称，然后选择 已启用配置文件。
3. 如果 SSL 服务器使用多个虚拟主机名，请在 虚拟主机名 字段中输入目标虚拟主机名。这是服务器凭据中列出的主机名。



> 注意
>
> 要支持多个虚拟主机，请为每个主机名创建单独的 SSL 配置文件。

4. 选择 拆分 代理类型。
5. 在 证书验证 字段中，保留默认值（签名/过期），除非您的策略另有规定。
6. 执行服务器端代理配置：

   在 验证存储 字段中，选择现有服务器证书颁发机构 (CA)，或单击 **+** 上载服务器 CA。

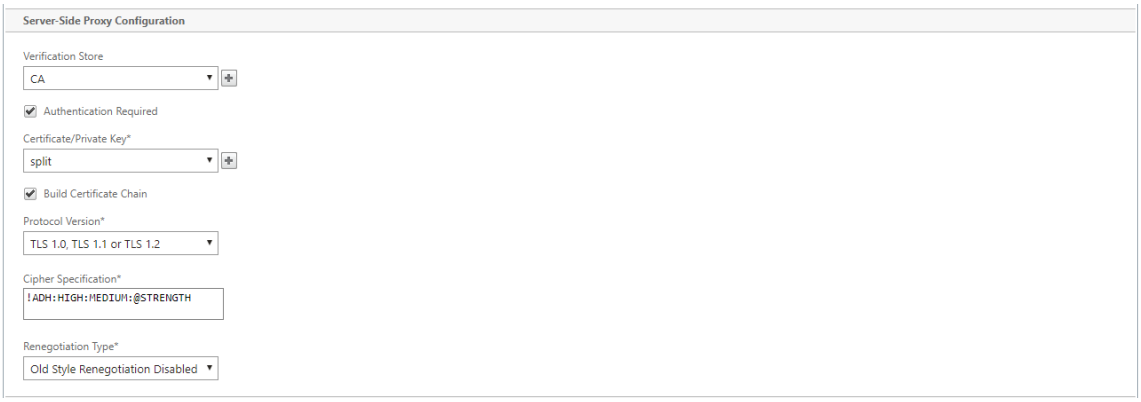
   选择 需要身份验证”，然后在“证书**/**私钥字段中选择一个证书密钥对，或单击 **+** 上载证书密钥对。

   在“协 议版本 字段中，选择服务器接受的协议。

   > 注意
   >
   > Citrix SD-WAN WO 仅支持 **TLS1.0**、**TLS1.1** 或 **TLS1.2** 或 **TLS1.2** 的组合 **。** 不支持 SSL 协议 SSLv3 和 SSLv2。

   如有必要，请使用 OpenSSL 语法编辑密 码规范 字符串。

   如果需要，请从“重新协商类型”下拉列表中选择 重新协商类型，以允许客户端 SSL 会话重新协商。



7. 执行客户端代理配置：

   在 证书**/**私钥 字段中，保留默认值。

选择 构建证书链 以允许服务器端设备构建 SSL 证书链。

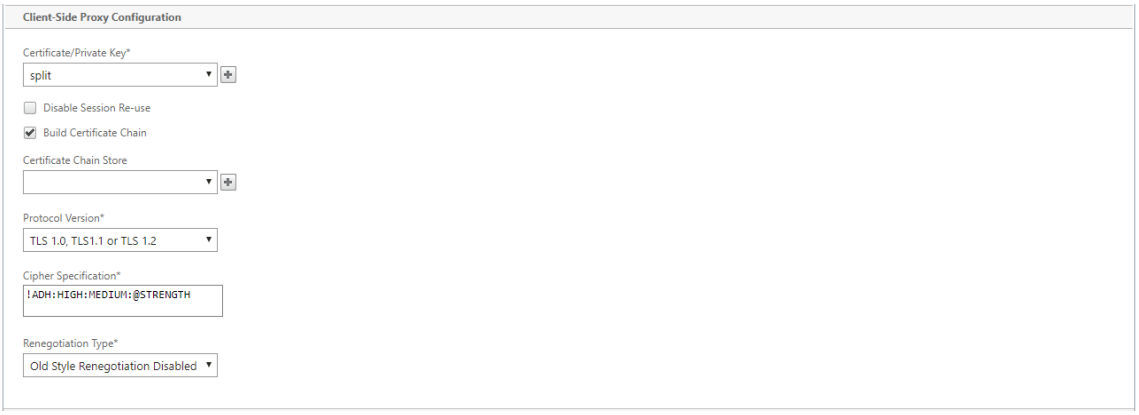
如果需要，请选择或上载 CA 存储以用作证书链存储。

在 协议版 本”字段中，选择要在客户端支持的协议版本。

> 注意
>
> Citrix SD-WAN WO 仅支持 **TLS1.0**、**TLS1.1** 或 **TLS1.2** 或 **TLS1.2** 的组合 **。** 不支持 SSL 协议 SSLv3 和 SSLv2。

如有必要，请编辑客户端密码规范。

如果需要，请从“重新协商类型”下拉列表中选择 重新协商类型，以允许客户端 SSL 会话重新协商。



8. 单击创建。

配置透明代理 **SSL** 配置文件

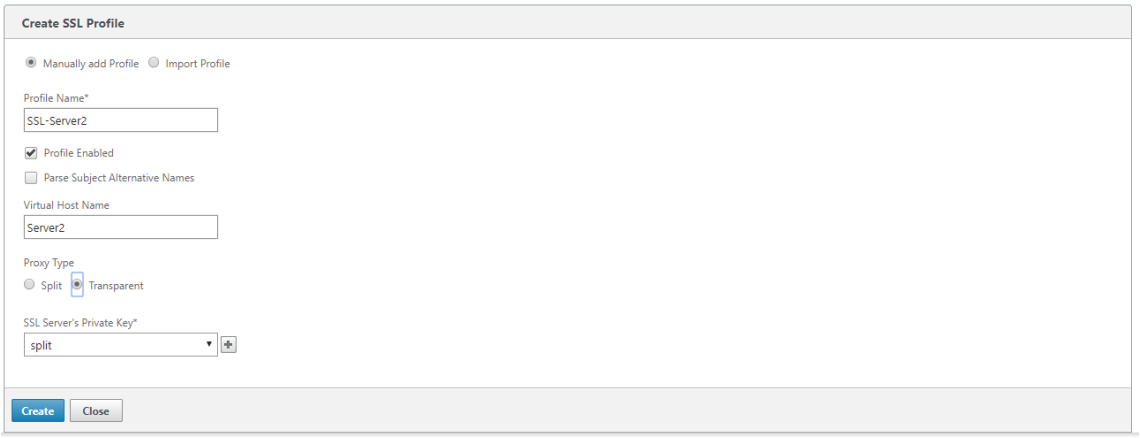
要配置透明代理 **SSL** 配置文件，请执行以下操作：

1. 在服务器端 Citrix SD-WAN O 设备中，导航到 配置 > 安全加速 > **SSL** 配置文 件，然后单击 添加配置文件。

   > 注意
   >
   > 您可以手动添加 SSL 配置文件或导入存储在本地计算机上的配置文件。

2. 在 配置文件名称 字段中，输入 SSL 配置文件的名称，然后选择 已启用配置文件。
3. 如果 SSL 服务器使用多个虚拟主机名，请在 虚拟主机名 字段中输入目标虚拟主机名。这是服务器凭据中列出的主机名。

   > 注意
   >
   > 要支持多个虚拟主机，请为每个主机名创建单独的 SSL 配置文件。



4. 选择 透明 代理类型。
5. 在 **SSL** 服务器的私有密钥 字段中，从下拉菜单中选择服务器的私有密钥，或单击 **+** 上载新的私有密钥。
6. 单击创建。

创建或修改服务类

要创建或修改服务类并附加 **SSL** 配置文件，请执行以下操作：

1. 在 Citrix SD-WAN WO 设备 Web 界面中，导航到 配置 **>** 优化规则 **>** 服务类，然后单击 添加。要编辑现有服务类，请选择相应的服务类，然后单击 编辑”。
2. 在“名称”字段中，输入新服务类的名称（例如，“加速 HTTPS”）。
3. 通过将加速策略设置为 磁盘、内存或 流量控制来启用压缩。
4. 在 筛选规则 部分中，单击 添加。
5. 在 目标 **IP** 地址”字段中，键入服务器的 IP 地址（例如，172.16.0.1 或相当于 172.16.0.1/32）。
6. 在 方向 字段中，将规则设置为单向。如果指定了双向，则 SSL 配置文件将被禁用。
7. 在 **SSL** 配置文 件”部分中，选择您创建的 SSL 配置文件并将其移动到 已配置 部分。
8. 单击 创建 以创建规则。
9. 单击 创建 以创建服务类。

更新的 **CLI** 命令

Citrix SD-WAN O 9.3 支持最新的 TLS1.2 SSL 协议。您可以选择仅使用 TLS1.2 协议或任何版本的 TLS 协议。不支持 SSL 协议 SSL v3 和 SSL v2 以及透明代理 SSL 配置文件。添加 **ssl-**配置文件 和 设置 **ssl-Profile** CLI 命令将更新以反映这些更改。

add ssl-profile:


```
*-name  “profile-name” *

*\[-state {
 enable, disable }
 \]*

*-proxy-type split*

*\[-virtual-hostname  “hostname” \]*

*-cert-key  “cert-key-pair-name” *

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores,  “store-name”  }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*

*\[-verification-store {
 use-all-configured-CA-stores,  “store-name”  }
 \]*

*\[-server-side-protocol {
  TLS-1.2, TLS-version-any }
 \]*

*\[-server-side-ciphers  “ciphers” \]*

*\[-server-side-authentication {
 enable, disable }
 \]*

*\[-server-side-cert-key  “cert-key-pair-name” \]*

*\[-server-side-build-cert-chain {
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
```



```
54   TLS-1.2, TLS-version-any }
55  \]*
56
57 *\[-client-side-ciphers  “ciphers” \]*
58
59 *\[-client-side-renegotiation {
60  disable-old-style, enable-old-style, new-style,*
61
62 *compatible }
63  \]*
```

set ssl-profile:

```
1  *-name  “profile-name”  \[-state {
2   enable, disable }
3   \]*
4
5  *\[-proxy-type split\]*
6
7  *\[-virtual-hostname  “hostname” \]*
8
9  *\[-cert-key  “cert-key-pair-name” \]*
10
11 *\[-build-cert-chain {
12  enable, disable }
13  \]*
14
15 *\[-cert-chain-store {
16  use-all-configured-CA-stores,  “store-name”  }
17  \]*
18
19 *\[-cert-verification {
20  none, Signature/Expiration, Signature/Expiration/*
21
22 *Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
23  \]*
24
25 *\[-verification-store {
26  use-all-configured-CA-stores,  “store-name”  }
27  \]*
28
29 *\[-server-side-protocol {
30  TLS-1.2, TLS-version-any }
31  \]*
32
33 *\[-server-side-ciphers  “ciphers” \]*
34
35 *\[-server-side-authentication {
36  enable, disable }
37  \]*
38
39 *\[-server-side-cert-key  “cert-key-pair-name” \]*
40
```



```
*\[-server-side-build-cert-chain {
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
 TLS-1.2, TLS-version-any }
 \]*

*\[-client-side-ciphers  “ciphers” \]*

*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*
```

使用 **Citrix SD-WAN WANOP** 插件进行 **SSL** 压缩

April 23, 2021

Citrix SD-WAN WANOP 插件始终用作客户端单元，因此除了为 SSL 信号（安全对等）连接安装凭据以外，不需要其他 SSL 配置。插件和设备上的 SSL 压缩的主要区别在于插件无法对基于磁盘的压缩历史记录中的用户数据进行加密。

警告：由于插件上基于磁盘的压缩历史记录未加密，因此它会保留潜在敏感和临时加密通信的明文记录。在物理访问不受控制的计算机上，这种缺乏加密的潜在危险。因此，Citrix 建议采用以下最佳做法：

- 请勿在您的设备上使用 证书验证：无。（请注意，在这种情况下，设备拒绝允许使用没有适当证书的插件进行压缩。）
- 仅在可验证以满足组织对物理或数据安全要求的系统上安装证书（例如，使用全磁盘加密的笔记本电脑）。

Citrix SD-WAN WANOP 插件支持 SSL 拆分代理和 SSL 透明代理。该插件在没有证书密钥对的情况下发送 SSL 信令连接。如果需要，所有插件都可以使用相同的凭据，或者每个插件都可以拥有自己的凭据。

除非已安装凭据，否则插件不会尝试 SSL 压缩。

插件从设备继承其加密许可证。

RPC over HTTP

April 23, 2021

Microsoft Exchange Server 是跨组织使用的常见电子邮件服务器之一。由于 Microsoft Exchange Server 中最近的增强功能，您可以通过 Internet 安全地连接到它。根据可用带宽，您可能会遇到发送到 Outlook 客户端的电子邮件中的延迟。除了 MAPI 协议之外，Citrix SD-WAN WANOP 设备还支持通过 HTTPS 进行远程过程调用（通过 HTTPS 进行 RPC）来优化 Microsoft Exchange 流量。此功能也称为 Outlook 任何地方。

通过 HTTPS 的 RPC 不是一个新的协议，但从微软 Exchange 2013 开始，它将 MAPI 替换为默认协议。RPC 通过 HTTPS 的主要优点是，它使客户端能够通过 Internet 安全地连接到邮件服务器。

当您通过 HTTPS 使用 RPC 时，Microsoft Exchange Server 必须使用数字证书和私钥对 Outlook 客户端进行身份验证。客户端和服务器之间的通信使用 HTTPS 作为传输协议。

在 Citrix SD-WAN WANOP 设备上，以下 Microsoft Outlook 和 Exchange Server 版本支持通过 HTTPS 进行 RPC：

- Microsoft Outlook
  - Microsoft Outlook 版本 2007
  - Microsoft Outlook 版本 2010
  - Microsoft Outlook 版本 2013
- Microsoft Exchange Server
  - Microsoft Exchange Server 版本 2007
  - Microsoft Exchange Server 版本 2010
  - Microsoft Exchange Server 版本 2013

其中，除了 Microsoft Exchanges Server 2013 以外的所有版本都支持 MAPI（通过 TCP）以及通过 HTTPS 的 RPC。但是，Microsoft Exchange Server 2013 强制连接通过 HTTPS 使用 RPC，无论您使用的 Microsoft Outlook 版本，连接到 Exchange 服务器。

通过 **HTTPS** 配置 **RPC**

默认情况下，设备上启用了通过 HTTPS 的 RPC 功能。但是，要将设备配置为通过 HTTPS 加速 RPC，您必须执行以下其他任务：

- 配置加密的 MAPI。
- 使用服务器证书配置 SSL 配置文件。
- 通过 HTTPS 服务类创建 RPC 并将 SSL 配置文件绑定到它。

配置加密 **MAPI**

> 注意
>
> 如果您已在设备上配置了加密的 MAPI 加速，请跳过此部分。

Microsoft Outlook 使用 Outlook 客户端和 Microsoft Exchange Server 之间的邮件应用程序编程接口 (MAPI) 连接。MAPI 连接使用由 HTTP 连接封装的 RPC。因此，在 Citrix SD-WAN WANOP 设备上配置通过 HTTPS 的 RPC 之前，必须在设备上配置加密的 MAPI。

先决条件：

配置加密 MAPI 之前，请确保满足以下先决条件：

- 在客户端以及服务器端设备上，安全对等选项应设置为 True。要配置安全伙伴，请参阅安全对等。
- 在服务器端设备上配置的 DNS IP 地址必须可访问。
- 数据中心端设备必须成功加入域。
- 必须将委托用户添加到数据中心端设备，其状态应标记为“成功”。

有关详细信息，请参阅配置 Citrix SD-WAN WANOP 设备以优化安全的 Windows 流量。

使用服务器证书配置 **SSL** 配置文件

封装 MAPI 连接的 HTTPS 连接受 SSL 保护。因此，通过 HTTPS 进行 RPC 需要通过 TCP 端口 443 进行连接。此端口分配给 HTTPS，Web 服务器管理员通常在防火墙应用程序中保持打开状态。使用 SSL 保护的通信有助于 RPC 通过 HTTPS 维护所有通信的安全性。

若要通过 HTTPS 启用 RPC 加速，必须在设备上安装服务器证书。使用此服务器证书，您可以配置 SSL 配置文件，通过 HTTPS RPC 用于安全通信。要使用 Exchange Server 证书配置 SSL 配置文件，请参阅安装服务器和客户端证书。

> 注意
>
> 您必须仅在数据中心端设备上配置 SSL 配置文件。

通过 **HTTPS** 服务类创建 **RPC** 并将 **SSL** 配置文件绑定到它

若要通过 HTTP 连接优化 RPC，必须创建列出 HTTPS 和所有 MAPI 应用程序的服务类。您必须提供 Microsoft Exchange Server 的 IP 地址作为此服务类的目标 IP 地址，然后将您创建的 SSL 配置文件绑定到此服务类。将配置文件绑定到服务类可确保 Outlook 客户端和 Microsoft Exchange Server 之间的通信通过使用此配置文件得到保护。

> 注意
>
> 您必须仅在数据中心端设备上配置 SSL 配置文件并将其绑定到服务类。

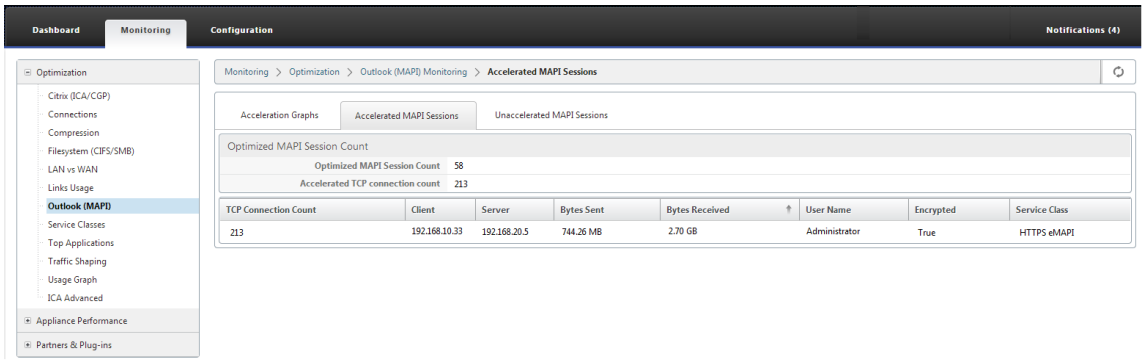
通过 **HTTPS** 连接验证加速的 **RPC**

在设备上配置了通过 HTTPS 的 RPC 后，可以在 MAPI 的监视页面上验证设备是否正在通过 HTTPS 加速 RPC 连接。加速 MAPI 会话选项卡上列出了通过 HTTPS 连接的加速 RPC。

> 注意
>
> 您必须在客户端设备上以及服务器端 Citrix SD-WAN WANOP 设备上配置通过 HTTPS 的 RPC，以便通过 HTTPS 连接加速 RPC。

验证正在加速通过 HTTPS 连接的 RPC

1. 导航到监视 > 优化 > **Outlook (MAPI)**。
2. 在加速 **MAPI** 会话选项卡上，验证通过 HTTPS 连接的 RPC 已加速。



> 注意
>
> 应用程序具有以下可能的值：HTTPS eMAPI、HTTP eMAPI、HTTPS MAPI 和 HTTP MAPI。

TCP 流量控制加速

April 23, 2021

在高链路利用率和远距离的情况下，普通 WAN 的响应速度非常差。对于普通的非加速 WAN 链路，一个广泛使用的经验法则是：“一旦链路利用率达到 40%，就应该增加更多带宽，因为性能和可靠性已经降低到链路基本上无法使用的地步。“互动性能受到影响，使人们难以完成工作，并且连接经常超时。加速链接没有这个问题。95% 利用率的链接仍然是完全可用的。

Citrix SD-WAN WANOP 设备将成为控制 WAN 链接上的 TCP 流量的虚拟网关。普通 TCP 由端点设备在每个连接的基础上进行控制。对链路流量进行最佳控制是困难的，因为端点设备和单个连接都不知道链路速度或竞争流量的数量。另一方面，Gateway 处于监视和控制链路流量的理想位置。普通网关浪费这个机会，因为它们无法提供 TCP 缺乏的流量控制。Citrix SD-WAN WANOP 技术增加了网络设备和 TCP 连接中缺少的智能。即使在高损耗或极端距离等恶劣条件下，也能大幅提高 WAN 性能。

Citrix SD-WAN WANOP 流量控制是无损和透明的，它实现了广泛的速度优化。由于自动发现和自动配置，不需要配置。但是，如果防火墙阻止加速算法使用的 TCP 选项，则可能需要调整防火墙。

无损透明流量控制

April 23, 2021

在通过两个设备（一个位于发送站点，一个位于接收站点）或 Citrix SD-WANOP 设备和 Citrix SD-WAN WANOP 插件的任何 TCP 连接上执行加速操作。尽管上图显示了由两台设备组成的网络，但任何设备都可以同时加速任意数量的其他配备设备的站点之间的连接。这允许每个站点使用一个设备，而不是每个链接使用两个设备。

与任何 Gateway 一样，Citrix SD-WAN WANOP 设备将数据包指向链接。然而，与普通网关不同的是，它对每个链路段实施透明、无损流量控制，包括：

- 发件人和发送设备之间的 LAN 段
- 发送和接收设备之间的 WAN 段
- 接收设备和接收机之间的 LAN 段

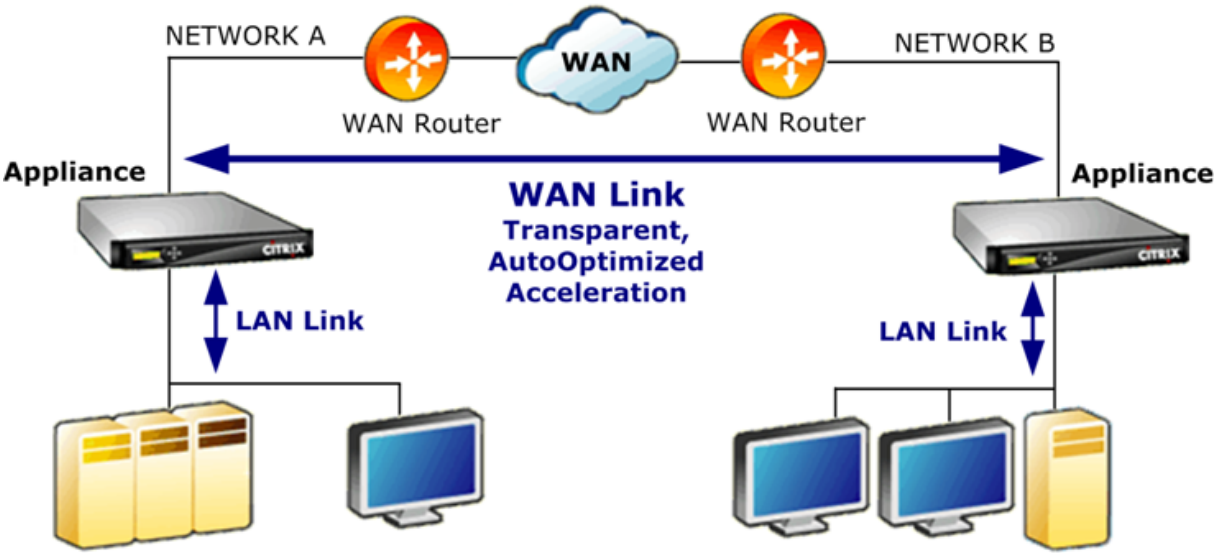
流量控制可以独立管理这三个区段中的每一个区段。这些段是部分解耦的，因此每个段都可以独立控制其速度。当连接速度需要快速上升或下降到公平的带宽份额时，这一点很重要，并且作为支持增强 WAN 算法和压缩的手段也很重要。

TCP 协议旨在使每个 TCP 连接尝试持续增加其带宽使用。但是，链路带宽是有限的。结果是链接变得超出。Citrix SD-WAN WANOP 流量控制保持 TCP 连接以正确的速度流动。链接已填充，但永远不会超出，因此排队延迟和数据包丢失最小化，同时最大化吞吐量。

对于普通的 TCP，长时间运行的连接（有时间抓住所有带宽）往往会挤出短时运行的连接。此问题，它会破坏交互式响应，不会发生与流控制。

流量控制是 Citrix SD-WAN WANOP 系列中所有设备的标准功能。

图 1. 加速度透明地提高性能



速度优化

April 23, 2021

大多数 TCP 实施在 WAN 链路上表现不佳。仅举两个问题，标准的 TCP 重传算法（选择性确认和 TCP 快速恢复）对于损失率高的链接不足，并且不考虑短期事务连接的需求。

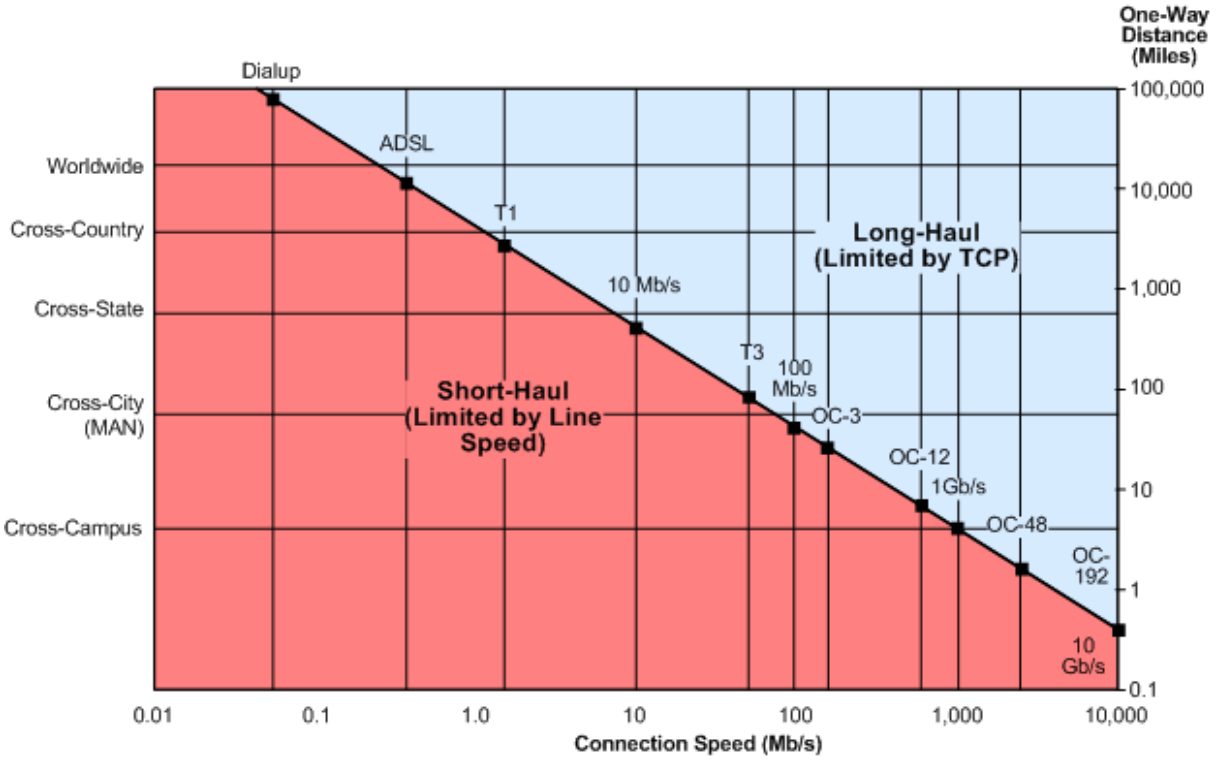
Citrix SD-WAN WANOP 实现广泛的广域网优化，以保持数据在各种不利条件下流动。这些优化以透明方式工作，以确保数据尽快到达目的地。

WAN 优化以透明方式运行，不需要任何配置。

WAN 优化是所有 Citrix SD-WAN WANOP 设备的标准功能。

下图显示了当端点使用标准 TCP (TCP Reno) 时，不加速的不同距离传输速度。例如，无论链路的实际速度如何，千兆位吞吐量在半径几英里内就可以实现，100 Mbps 可达到 100 英里以下，全球连接的吞吐量限制在 1 Mbps 以下。然而，随着加速度，对角线上方的速度将变得可用于应用程序。距离不再是限制因素。

图 1. 非加速 TCP 性能随着距离而下降



> 注意
>
> 如果没有 Citrix 加速，TCP 吞吐量与距离成反比，因此无法提取长途高速链路的全部带宽。使用加速度时，距离因子消失，并且可以在任何距离使用链接的全速。（图表基于匹兹堡超级计算机中心 Mathas 等人的模型。）

加速传输性能大致等于链路带宽。传输速度不仅高于未加速 TCP，而且在不断变化的网络条件下也更加稳定。其作用是使远程连接具有与本地连接相同的效果。无论链路利用率如何，用户感知的响应能力都保持不变。与普通 TCP 不同，在 90% 的使用率下运行 WAN 对于交互式任务是无用的，加速链接的响应速度与 10% 的链接利用率相同。

对于短途连接（上图中低于对角线的连接），在良好的网络条件下很少或根本没有加速，但是如果网络退化，性能下降要比普通 TCP 慢得多。

非 TCP 流量（如 UDP）不会加速。但是，它仍然由流量塑形器管理。

示例

高级 TCP 优化的一个示例是称为 事务模式的重传优化。TCP 的一个特点是，如果事务中的最后一个数据包被丢弃，则在 Receiver 超时 (RTO) 周期结束之前，发件人不会注意到其丢失。这种延迟总是至少一秒长，而且往往更长，是造成在有损链接上出现的多秒延迟的原因，这种延迟使交互式会话不愉快或不可能。

事务模式通过在短暂的延迟后自动重新传输事务的最终数据包来解决此问题。因此，除非删除两个副本，否则 RTO 不会发生，这是不可能的。

批量传输基本上是一个巨大的事务，所以事务模式用于批量传输的额外带宽可以只有每个文件一个数据包。但是，交互式流量（例如按键或鼠标移动）具有较小的事务。事务可能由一个小型的数据包组成。发送这样的数据包两次具有适度

的带宽要求。实际上，事务模式在交互式流量上提供正向错误纠正 (FEC)，并为其他流量提供事务结束 RTO 保护。

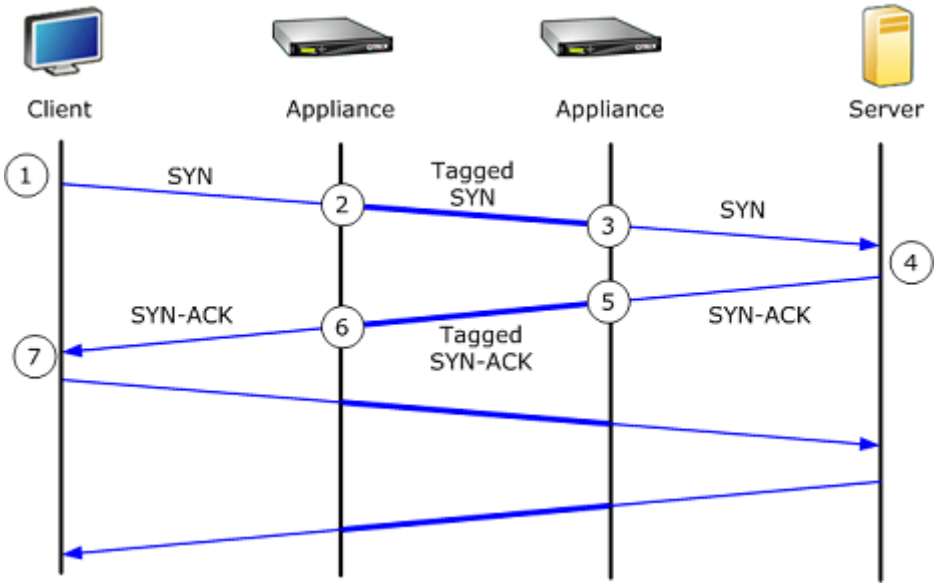
自动发现和自动配置

April 23, 2021

在称为自动发现的过程中，Citrix SD-WAN WANOP 单元会自动检测对方的存在。设备将 TCP 标头选项附加到每个连接中的第一个数据包：SYN 数据包（由客户端发送到服务器以打开连接）和 SYN-ACK 数据包（由服务器发送到客户端以指示连接已被接受）。通过标记 SYN 数据包并侦听标记 SYN 和 SYN-ACK 数据包，这些设备可以通过连接实时检测彼此的存在。

自动发现的主要优点是，每次向网络添加新设备时，您都不必重新配置所有设备。他们自动找到对方。此外，同样的过程允许自动配置。这两个设备使用 TCP 标头选项来交换操作参数，包括带宽限制（发送和接收方向）、基本加速模式（hardboost 或 softboost）以及可接受的压缩模式（磁盘、内存或无）。每个设备需要的有关其合作伙伴的所有信息都与每个连接交换，从而允许每个连接变化（例如，允许的压缩类型中的每个服务类别变化）。

图 1. 自动发现的工作原理



自动发现过程的工作原理如下：

1. 客户端与往常一样，通过向其发送 TCP SYN 数据包来打开到服务器的 TCP 连接。
2. 在将一组特定于设备的 TCP 头选项附加到 SYN 数据包并调整其窗口大小之后，第一个设备会传递 SYN 数据包。
3. 第二个设备读取 TCP 选项，从数据包中删除它们，然后将它们转发到服务器。
4. 服务器通过像往常一样使用 TCP SYN-ACK 数据包来接受连接。
5. 第二个设备记住此连接是加速的候选项，并将其自己的加速选项附加到 SYN-ACK 标头。

6. 第一个设备读取第二个设备添加的选项，从数据包标头剥离这些选项，然后将数据包转发到客户端。连接现在已加速。这两个设备已经通过选项值交换了必要的参数，并在连接持续时间内将它们存储在内存中。

连接加速，并且加速对客户端、服务器、路由器和防火墙是透明的。

TCP 流量控制模式

April 23, 2021

TCP 流量控制有两种模式：软提升和硬提升。

Softboost 使用基于速率的发送器，以最高速度发送链路带宽限制的速度加快的流量。如果带宽限制设置略低于链路速度，则数据包丢失和延迟将最小化，同时最大化链路利用率。交互式应用程序可以看到快速响应时间，而批量传输应用程序则可以看到高带宽。Softboost 与任何拓扑中的其他应用共享网络，并与第三方 QoS 系统互操作。

硬加速比软加速更为主动。通过忽略数据包丢失和其他所谓的“拥塞信号”，它在存在严重、与拥塞无关的损失的链路上表现非常好，例如卫星链路。它也是优秀的低质量，长途链路，具有高背景数据包丢失，例如许多海外链路。仅建议使用 Softboost 无法实现足够性能的点对点链接使用 Hardboost。

Softboost 是默认模式，在大多数情况下推荐使用。

> 注意
>
> - Hardboost 应仅用于固定速度点对点链路或集线辐射部署，其中集线器带宽至少等于加速辐射带宽的总和。
> - Softboost 和 hardboost 是相互排斥的，这意味着必须相互通信的所有设备都必须设置相同。如果一个单元设置为硬加速，另一个单元设置为软加速，则不会发生加速。

要选择软提升模式，请执行以下操作：

Softboost 是默认模式，在大多数情况下推荐使用。

1. 导航到 配置 > 链接 > 硬提升/软提升，然 后单击编辑。
2. 选择 软提升 作为 广域网提升模式。

3. 单击保存

要选择硬提升模式，请执行以下操作：

仅在固定速度点对点链路或集线辐射链路上选择 hardboost 模式，其中集线器带宽大于或等于加速辐射链路的带宽。

1. 导航到 配置 > 链接 > 硬提升/软提升，然 后单击编辑。
2. 选择 硬提升 作为 广域网提升模式。
3. 将 **WAN** 带宽接收限制 设置为链路速度的 95%。
4. 单击保存。

防火墙注意事项

April 23, 2021

Citrix SD-WAN WANOP 设备使用 TCP 选项会使来自防火墙的加速流量面临风险，这些防火墙对使用不太常见的 TCP 选项拒绝连接服务的严格规则。

某些防火墙会剥离“未知”选项，然后转发数据包。此操作可防止加速，但不会影响连接性。

其他防火墙拒绝向具有未知选项的连接提供服务。也就是说，防火墙会删除带有 Citrix SD-WAN WANOP 选项的 SYN 数据包。当设备检测到重复的连接尝试失败时，它会在没有选项的情况下重试。这在延迟可变长度后恢复连接，通常在 20-60 秒的范围内，但没有加速。

任何未通过未修改的 Citrix SD-WAN WANOP 选项的防火墙都必须重新配置，以接受 24—31（十进制）范围内的 TCP 选项。

大多数防火墙不会阻止这些选项。但是，思科 ASA 和 PIX 防火墙（可能还有其他版本 7.x 固件）默认情况下可能会这样做。

应检查链接两端的防火墙，因为任何一个都可能允许对传出连接进行选项，但在传入连接上阻止它们。

以下示例应使用 7.x 固件与思科 ASA 55x0 防火墙配合使用。由于它全局允许 24-31 范围内的选项，因此没有自定义的每个接口或每个单位配置：

```
 ====================================================================
 CONFIGURATION FOR CISCO ASA 55X0 WITH 7.X CODE TO ALLOW TCP OPTIONS
 ====================================================================
 hostname(config)# tcp-map WSOptions
 hostname(config-tcp-map)# tcp-options range 24 31 allow
 hostname(config-tcp-map)# class-map WSOptions-class
 hostname(config-cmap)# match any
 hostname(config-cmap)# policy-map WSOptions
 hostname(config-pmap)# class WSOptions-Class
 hostname(config-pmap-c)# set connection advanced-options WSOptions
 hostname(config-pmap-c)# service-policy WSOptions global
<!--NeedCopy-->
```

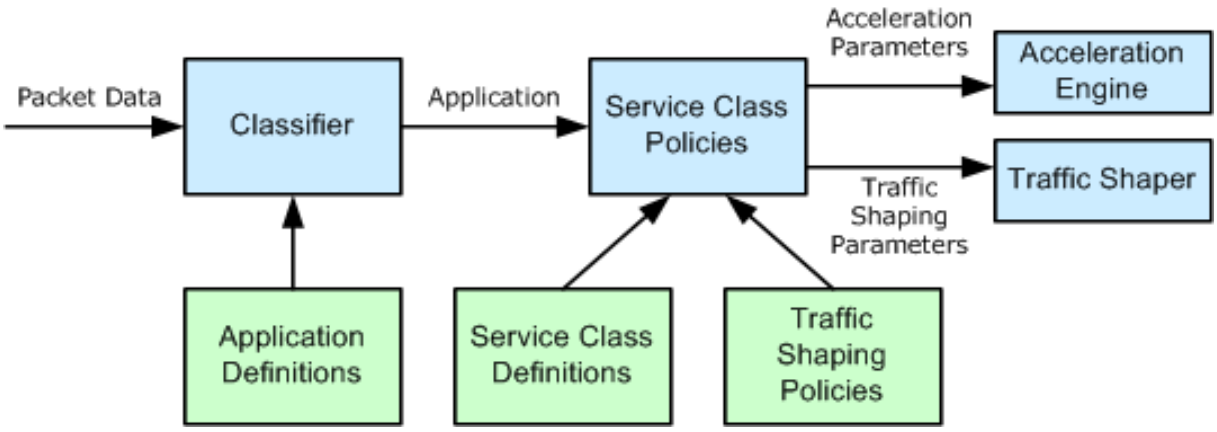

PIX 防火墙的配置类似：

```
 ======================================================
 POLICY MAP TO ALLOW APPLIANCE TCP OPTIONS TO PASS (PIX 7.x)
 ======================================================
 pixfirewall(config)#access-list tcpmap extended permit tcp any any
 pixfirewall(config)# tcp-map tcpmap
 pixfirewall(config-tcp-map)# tcp-opt range 24 31 allow
 pixfirewall(config-tcp-map)# exit
 pixfirewall(config)# class-map tcpmap
 pixfirewall(config-cmap)# match access-list tcpmap
 pixfirewall(config-cmap)# exit
 pixfirewall(config)# policy-map global_policy
 pixfirewall(config-pmap)# class tcpmap
 pixfirewall(config-pmap-c)# set connection advanced-options tcpmap
<!--NeedCopy-->
```

流量分类

April 23, 2021

Citrix SD-WAN WANOP 设备的两个主要功能是流量成形（可最大限度地提高所有类型流量的链路使用率）和加速（可应用压缩和各种优化来加速 TCP 流量）。流量成形和加速的两个基本组成部分是应用分类机制和服务级机制。前者标识流量的类型，以便后者可以将流量分配给服务类。每个服务类都有流量调整策略和加速策略。



应用程序分类器

April 23, 2021

应用程序分类器使用应用程序定义按协议和应用程序对流量进行分类。此信息用于创建报表，并按服务类机制使用。许多应用程序已经定义，您可以根据需要定义更多应用程序。

应用定义中的协议和端口规格

应用程序分类器使用来自互联网号码分配机构 (IANA) 的官方协议和端口规范http://www.iana.org。有时候，除官方应用程序之外的应用程序使用端口。分类器通常无法检测到这种使用。如果您的网络使用此类应用程序，通常可以通过在应用程序分类器中重命名应用程序来解决此问题，以指示在网络上使用此端口的实际应用程序。例如，如果您使用端口 3128 不用于 Squid Web 缓存的标准用途，而是用于 SOCKS 代理，则可以将鱿鱼 (TCP) 应用程序重命名为 SOKS（端口 3128），以便清楚起见。

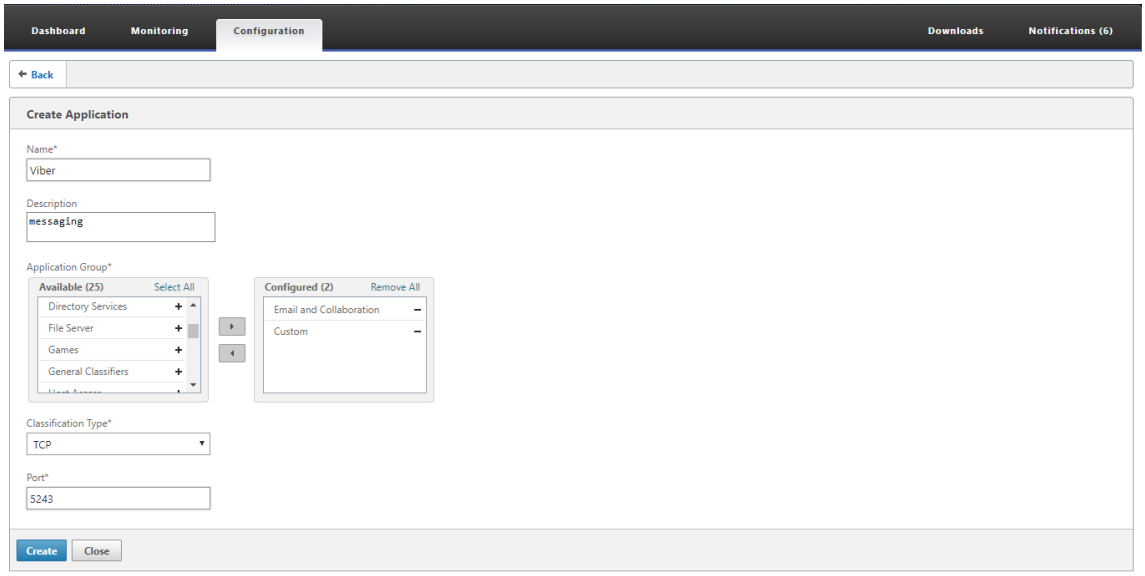
应用程序不得具有重叠的定义。例如，如果网络上的一个应用程序使用 TCP 端口 3120 和 3128，而另一个应用程序使用端口 3120，则只有一个 Citrix SD-WAN WANOP 应用程序定义可以包含端口 3120。

配置应用程序定义

- 动态 TCP，适用于使用动态端口分配的应用程序
- 乙醚类型，用于以太网包类型
- ICA 已发布应用，适用于虚拟应用程序/虚拟桌面
- 知识产权，用于 IP 协议，如 ICMP 或 GRE
- TCP，用于 TCP 应用程序
- UDP，用于 UDP 应用程序
- Web 地址，针对特定网站或域。

要配置应用程序防御，请执行以下操作：

1. 导航到配置 > 优化规则 > 应用程序分类器，然后单击添加。



2. 在 创建应用程序 页面上，设置以下参数：

- 名称 -应用程序分类器的名称。必须以 ASCII 字母数字或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、散列 (#)、句点 (.)、冒号 (:)、at (@)、等于 (=) 和连字符 (-)。最大长度：31 个字符。
- 描述 -应用程序分类器的描述。
- 应用程序组 -应用程序分类器属于此应用程序组。应用程序组是一组根据其功能进行分类的预定义应用程序组。
- 分类类型 -要用于此应用程序分类器的高级分类。高级别分类主要是基于应用程序使用的端口进行的。
- 端口—要使用的端口号。您可以输入范围、列表或介于 0 到 65535 之间的数字。

3. 单击创建。

   应用程序分类器页面列出了 SD-WAN WANOP 分类器识别的所有应用程序。

应用程序分类器页面列出了 SD-WAN WANOP 分类器识别的所有应用程序。

> 提示
>
> 单击 自动发现 以允许数据流中看到的任何 Citrix 已发布应用程序自动添加到应用程序列表中。一旦发现，它们将显示在报告中，并可用于流量调整策略。

服务类别

April 23, 2021

为服务类分配了流量调整策略和加速策略，用于匹配服务类定义的所有连接。服务类可以基于以下参数：

- 应用程序
- IP 或 VLAN 地址
- DSCP 位
- SSL 配置文件

建议将默认服务类定义作为起点。修改它们，如果它们证明不适合你的链接。

服务类在有序列表中定义。与正在处理的流量匹配的第一个定义成为流量的服务类。

加速决策与流量调整策略之间的差异

要做出加速决策，Citrix SD-WAN WANOP 设备会检查每个 TCP 连接的初始 SYN 数据包，以确定连接是否是加速的候选项。SYN 数据包不包含有效负载，只包含标头，因此加速决策必须基于 SYN 数据包标头的内容，例如连接的目标端口或目标 IP 地址。加速，一旦应用，将持续连接的持续时间。

与加速决策不同，流量调整策略可以基于连接数据流的内容。根据应用程序分类器接收足够数据进行最终分类所需的时间，可能会在其生命周期内重新分类连接。

例如，HTTP 连接中的第一个数据包`http://www.example.com`是包含标头但没有负载的 SYN 数据包。标头的 IP 目标端口为 80，与 HTTP: Internet 服务类定义相匹配，因此加速引擎将其加速决策作为基础，在这种情况下，该服务类无（无加速）。

流量成形程序使用 HTTP: Internet 服务类中的流量成形策略，但此决策是临时性的。第一个有效负载数据包包含字符串 GET`http://www.example.com`，该字符串与应用程序分类器中的示例应用程序定义相匹配。包含示例应用程序的服务类由流量成形程序选择，而不是包含 HTTP: Internet 的服务类，流量成形程序使用该服务类定义中命名的服务类策略。

> 注意
>
> 无论服务类策略如何，报告功能都会跟踪示例应用程序的使用情况。
>
> 重要
>
> 所有流量都与应用程序和服务类相关联，并且所有服务类都具有流量调整策略，但只有 TCP 连接具有加速策略，而不是没有。

配置服务类定义

由于服务类定义是一个有序列表，因此作为一般情况例外的定义必须在服务类页面上较为一般的定义之前。规则与流量匹配的第一个定义是应用的定义。例如：

- 基于 URL 的服务类必须位于服务类列表中的 HTTP 服务类之前，因为任何基于 URL 的规则也与 HTTP 服务类匹配。因此，将 HTTP 服务类放在第一位将防止使用基于 URL 的规则或已发布的基于应用程序的规则。
- 同样，基于 ICA（虚拟应用程序/虚拟桌面）发布的应用程序的服务类必须先于 Citrix 服务类。

由于所有基于 URL 的规则都与 HTTP 服务类匹配，因此将 HTTP 服务类放在它们之上将导致基于 URL 的规则或已发布的基于应用程序的规则永远不会被使用。

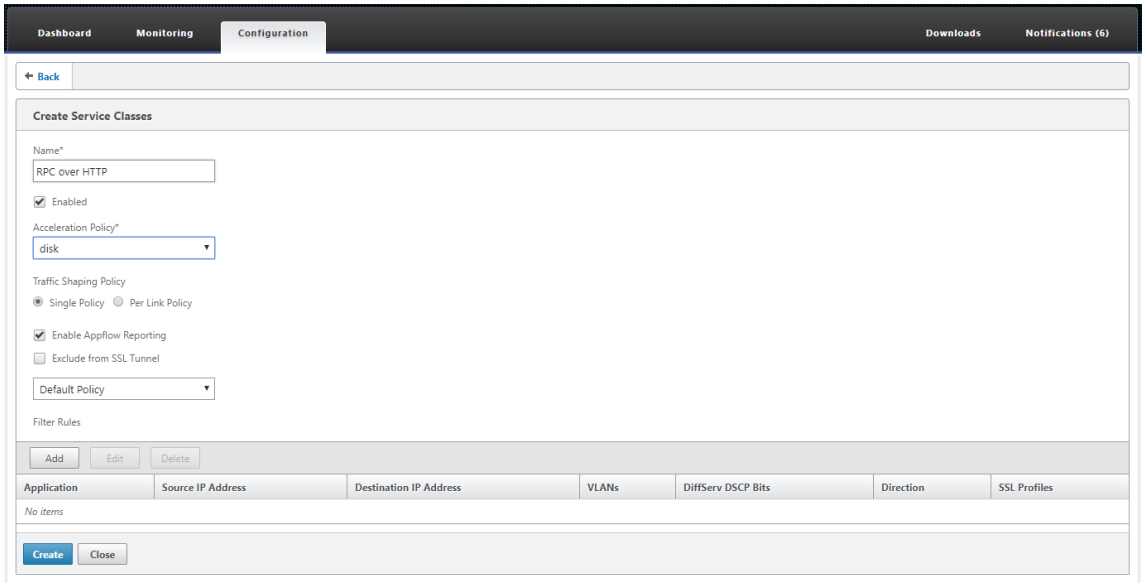
Configuration Overview > Optimization Rules > **Service Classes**

Add | Edit | Delete | Update Order | Filter Rules | Show User Modified Service Classes Only

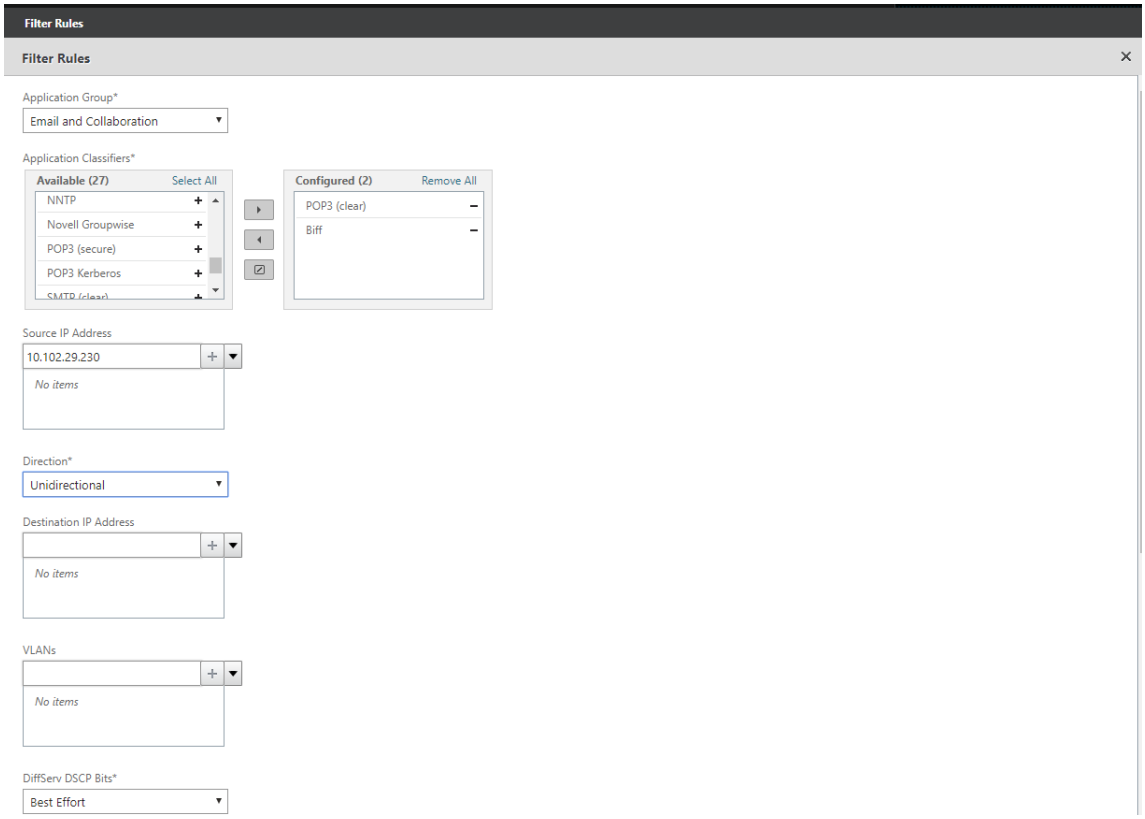
Order	Name	Status	Acceleration Policy	Traffic Shaping Policy	Appflow Reporting Status
1	ICA	Enabled	disk	ICA Priorities	Enabled
2	Web (Private)	Enabled	disk	Default Policy	Enabled
3	Web (Private-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
4	Web (Internet)	Enabled	disk	Default Policy	Enabled
5	Web (Internet-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
6	CIFS	Enabled	disk	Default Policy	Enabled
7	NFS	Enabled	disk	Default Policy	Enabled
8	Microsoft Exchange (MAPI)	Enabled	disk	Default Policy	Enabled
9	Mail (Other)	Enabled	disk	Default Policy	Enabled
10	VOIP and Multimedia	Enabled	None	VOIP Traffic	Enabled
11	VOIP Webcam	Enabled	None	High Priority Traffic	Enabled
12	FTP Data	Enabled	disk	Low Priority Traffic	Enabled
13	FTP Control	Enabled	Flow Control Only	Default Policy	Enabled
14	Instant Messaging	Enabled	disk	Default Policy	Enabled
15	Session Applications	Enabled	Flow Control Only	Default Policy	Enabled
16	Directory and Security	Enabled	Flow Control Only	Default Policy	Enabled
17	Database Applications	Enabled	Flow Control Only	Default Policy	Enabled
18	Secure Applications	Enabled	Flow Control Only	Default Policy	Enabled
19	Iperf	Enabled	Flow Control Only	Low Priority Traffic	Enabled
20	NetApp SnapMirror	Enabled	memory	Default Policy	Enabled
21	Other TCP Traffic	Enabled	None	Default Policy	Enabled
22	Unclassified Traffic	Enabled	None	Default Policy	Enabled

要通过 HTTP 服务类创建 RPC 并将 SSL 配置文件绑定到它：

1. 导航到 配置 > 优化规则 > 服务类，然后单击 添加。



2. 在“名 称 字段中，输入服务类的名称。
3. 请确保已选中 已启用 选项。
4. 从加 速策略 列表中，选择加速策略。内存 和 磁盘 指定用于压缩的流量历史记录的存储位置。磁盘 通常是最佳选择，因为设备会自动选择磁盘或内存，具体取决于哪些磁盘或内存更适合流量。内存 仅指定内存。选择“仅 流量控制 可禁用压缩，但启用流量控制加速。为始终加密的服务和 FTP 控制通道选择此选项。“无 仅用于不可压缩的加密流量和实时视频。
5. 选择 启用 **AppFlow** 报告 以启用此服务类的 AppFlow 报告。来自此服务类的信息包含在任何 AppFlow 报告中。AppFlow 是解锁由网络基础设施处理的应用事务数据的行业标准。WAN 优化 AppFlow 界面与任何 AppFlow 收集器一起工作，以生成报告。收集器使用 AppFlow 开放标准从设备接收详细信息。
6. 选择 从 **SSL** 隧道中排除”以从 SSL 隧道中排除与服务类关联的流量。
7. 在流量调整策略列表中，确保选择了 默认策略 选项。流量调整策略具有加权优先级和其他属性，用于决定如何处理匹配流量（相对于其他流量）。大多数服务类都设置为“默认策略”，但可以为较高优先级的流量分配一个更高优先级的流量调整策略，而且可以为较低优先级的流量分配一个较低优先级的策略。
8. 在“筛选规则”部分中，单击 添加 以创建将“任意”作为所有参数的默认值的筛选规则。如果某个给定连接的规则被评估为 TRUE，则该连接将分配给该服务类。大多数服务类的筛选规则仅由应用程序列表组成，但规则也可以包括 IP 地址、VLAN 标签、DSCP 值和 SSL 配置文件名称。规则中的所有字段默认为“任意”（通配符）。规则中的字段是一起的。
9. 单击 添加 以添加筛选器规则。



10. 从 应用程序组 列表中，选择 电子邮件和协作。
11. 从 可 用”列表中，选择所需的应用程序。
12. 将选定的应用程序移动到 已配置 列表。
13. 在 源 **IP** 地址 字段中，添加客户端 IP 地址。
14. 从“方 向 列表中，选择流量的方向。
15. 从 **SSL** 配置文件 列表中，选择您创建的 SSL 配置文件。
16. 单击创建。

> 注意
>
> - 您必须仅在数据中心端设备上配置 SSL 配置文件并将其绑定到服务类。
> - 只有将过滤规则方向设置为单向的服务类才能与 SSL 配置文件关联。

流量成形

April 23, 2021

Apr 18, 2018

流量成形允许您调节网络流量，以确保一定水平的服务质量 (QoS)。您可以调节数据包流入网络（带宽限制）或流出网络（速率限制）。

使用流量调整策略，您可以设置不同链路流量的优先级，并以接近但不超过链路速度的速率将流量发送到链路。与仅适用于 TCP/IP 流量的加速不同，流量成形器处理链接上的所有流量。

您可以为被认为比其余流量流量更重要的流量流量设置高带宽，从而使您能够以最佳方式使用稀缺的链接资源。

流量调整基于加权公平排队，这给每个服务类的链路带宽公平份额。如果链接处于空闲状态，则任何连接（在任何服务类中）都可以使用整个链接。当多个连接争夺链路带宽时，流量成形器会应用流量成形策略来确定正确的流量组合。

有关加权公平排队的信息，请参阅加权公平排队。

要配置流量调整：

1. 配置链接定义。

   流量成形器使用链路定义来确定发送和接收链路速度以及其他链路相关信息。有关流量塑形器如何使用链接定义以及如何配置链接定义的更多信息，请参阅 链接定义。

2. 配置应用程序定义。

   流经链接的流量由应用程序分类器检查，以确定它所属的应用程序，然后在服务类列表中查找应用程序以确定它所属的服务类。有关应用程序分类以及如何配置应用程序定义的更多信息，请参阅流量分类。

3. 创建流量调整策略。

   您可以使用默认流量调整策略或创建新策略来根据您的网络要求设置加权优先级和其他参数。有关创建流量调整策略的信息，请参阅流量成形策略。

4. 配置服务类定义并将流量调整策略与服务类关联。

   有关配置服务类定义的信息，请参阅服务类别。

流量塑形器的一些亮点：

- 所有 WAN 流量都受流量影响：加速连接、未加速连接和非 TCP 流量（如 UDP 流量和 GRE 流量）。
- 算法是加权公平排队，其中管理员为每个服务类分配优先级。每个服务类都表示一个带宽池，有权获得链接速度的最小部分，等于（my_ 优先/sum_of_all_ 优先级）。加权优先级为 100 的服务类获得的带宽是加权优先级为 50 的服务类的两倍。您可以指定从 1 到 256 的权重。
- 服务类中的每个连接将获得分配给该服务类的带宽的相等份额。
- 每个连接获得其公平的链路带宽份额，因为在压缩之后，优先级将应用于实际传输的 WAN 数据。例如，如果您有两个具有相同优先级的数据流，一个实现 10:1 压缩，另一个实现 2:1 压缩，则用户会看到吞吐量差 5:1，即使两个连接的 WAN 链接使用情况相同。实际上，这种差异是可取的，因为 WAN 带宽而不是应用程序带宽，是需要管理的稀缺资源。

- 流量调整政策同样适用于加速流量和非加速流量。例如，加速的虚拟应用程序连接和未加速的虚拟应用程序连接都可以接收流量调整，因此与批量流量相比，两者的优先级都可以提高。另一个例子是，时间敏感的非 TCP 流量，如 VoIP（使用 UDP 协议）可以加快。
- 流量调整适用于发送和接收方向的 WAN 链接，既适用于加速的流量，也适用于非加速的流量。即使链接的另一端未配备 Citrix SD-WAN WANOP 设备，此功能也可防止拥塞和延迟增加。例如，可以对互联网下载进行优先排序和管理。
- 如果需要，可以根据每个链接指定服务类的流量调整策略。
- 除了直接调整流量外，流量成形程序还可以通过设置差异服务代码点 (DSCP) 字段来通知下游路由器每个数据包所需的流量类型来间接影响流量。

加权公平排队

April 23, 2021

在任何链接中，瓶颈 Gateway 都会确定队列纪律，因为非瓶颈网关中的数据不会备份。如果没有队列中的挂起数据，则排队协议无关紧要。

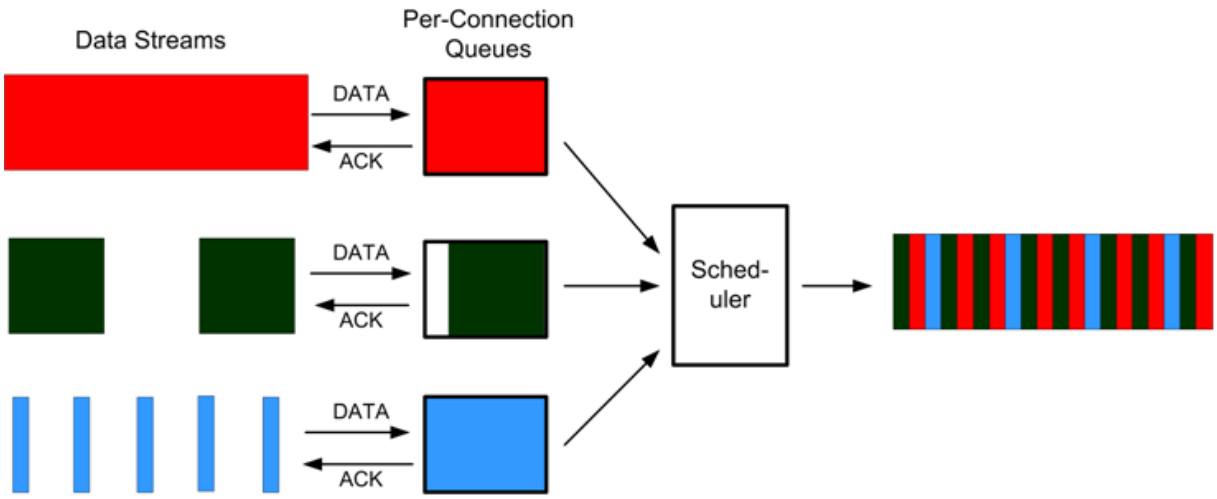
大多数 IP 网络使用深度 FIFO 队列。如果流量到达速度比瓶颈速度快，队列会填满，所有数据包都会增加排队时间。有时，流量被分成几个不同的类与单独的 FIFO，但问题仍然存在。发送过多数据的单个连接可能会导致同类中所有其他连接的大量延迟、数据包丢失或两者。

Citrix SD-WAN WANOP 设备使用加权公平队列，这为每个连接提供单独的队列。通过公平的排队，太快的连接只能溢出自己的队列。它对其他连接没有影响。但是由于无损流量控制，没有太快的连接，队列不会溢出。

结果是，每个连接都以公平的方式计量其流量到链路中，并且整个链路具有最佳的带宽和延迟配置文件。

下图显示了公平排队的效果。需要小于其公平份额的带宽（底部连接）的连接获得的带宽与尝试使用的带宽相同。此外，它的排队延迟非常少。尝试使用超过公平份额的连接将获得公平份额，加上使用少于公平份额的连接所留下的任何带宽。

图 1. 公平排队在行动



最佳延迟配置文件为交互式和事务性应用程序的用户提供理想的性能，即使用多个批量传输共享链接也是如此。无损透明流量控制和公平排队的组合使您能够安全透明地将各种流量组合在同一条路上。

加权公平排队和非加权公平排队之间的区别在于，加权公平排队包括给予某些流量比其他流量更高的优先级（权重）的选项。权重为 2 的流量接收的流量是流量带宽的两倍，权重为 1。在 Citrix SD-WAN WANOP 配置中，权重将在流量调整策略中分配。

流量成形策略

April 23, 2021

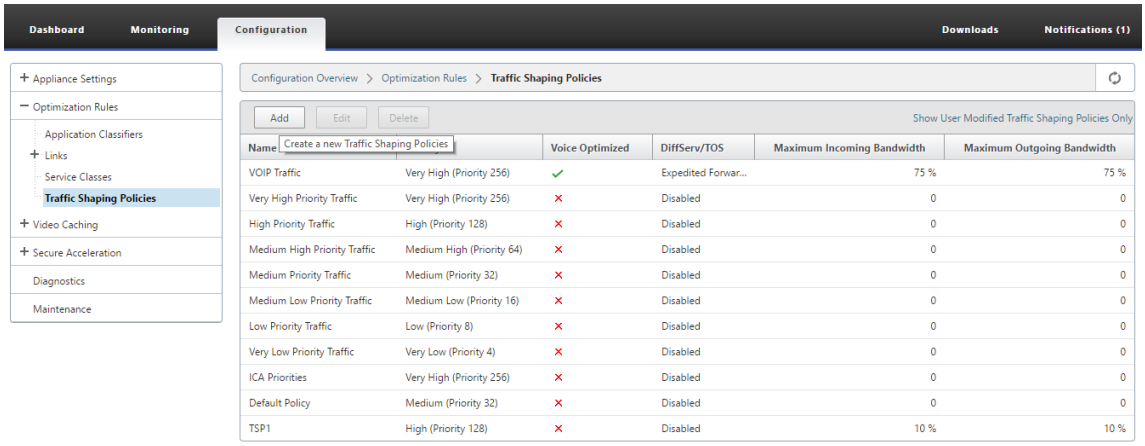
每个服务类定义都与流量调整策略相关联，该策略为相关服务类的流量设置参数。您可以为有特殊需求的站点创建和配置流量调整策略，但默认策略设置适用于大多数安装，具有以下优势：

- 提高了对 Citrix Virtual Apps and Desktops 等交互式流量的响应能力。
- 保护延迟和抖动敏感的 VoIP 流量。
- 在高峰期没有“撞墙”。即使在极端负载下，您也可以获得可用的性能。
- 通过允许批量传输以填充交互式任务遗留的任何带宽，从而提高带宽利用率。
- 将公平排队的好处扩展至所有流量

Citrix SD-WAN WANOP 设备随附了出厂默认流量调整策略，该策略涵盖广泛的优先级。这些策略在 流量调整策略 页面中列出。除 默认策略外，不能编辑或删除其他出厂默认策略。原因是为了确保它们在所有电器上具有相同的含义。要进行更改，请使用新参数创建新的流量调整策略，并更改相应的服务类定义以引用新的流量调整策略。

要创建流量调整策略，请执行以下操作：

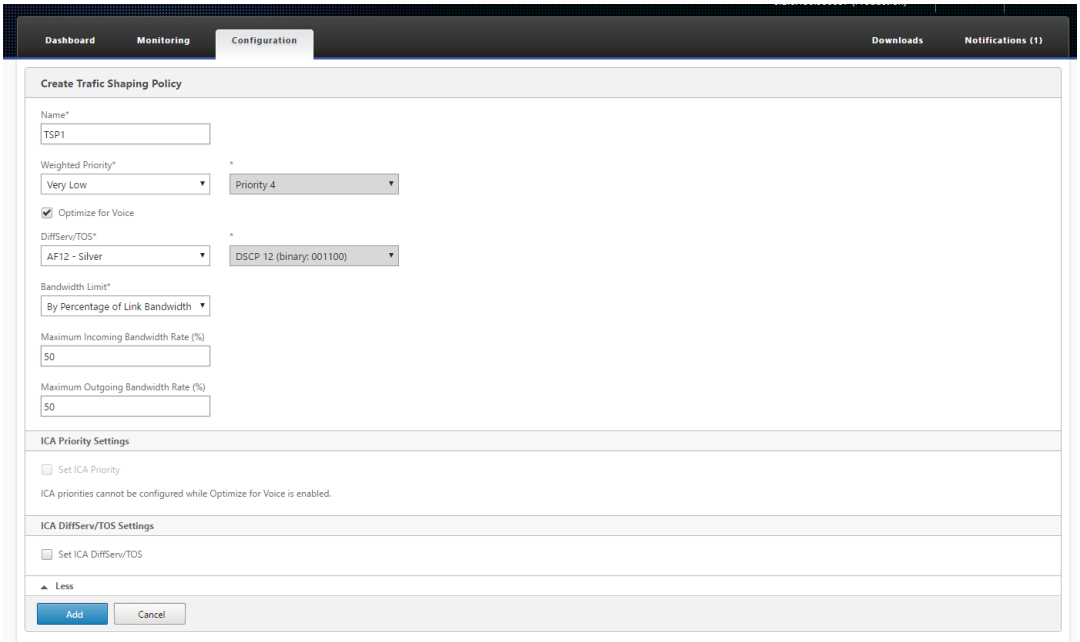
1. 在 SD-WAN WANOP 管理 UI 中，导航到 配置 > 优化规则 > 流量调整策略，然后单击 添加。



2. 在 创建流量调整策略 页面中，输入以下参数的值：

   - 名称—新策略的名称。必须是唯一的。
   - 加权优先级—您可以选择现有优先级值，也可以选择介于 1 到 256 之间的自定义值。优先级为 256 的连接将获得带宽共享的 256 倍，优先级为 1 的连接。
   - 优化语音—如果选中，此策略将有效地具有无限优先级。这对于大多数流量来说是非常不可取的，因为如果有足够的“针对语音”流量来填充链接，它会阻止有意义的流量成形，并会导致其他流量的数据匮乏。仅用于 VoIP，并且始终与策略的带宽限制一起使用（例如，链路速度的 50%）

     > 注意
     >
     > 设置 ICA 优先级时无法配置语音优化。

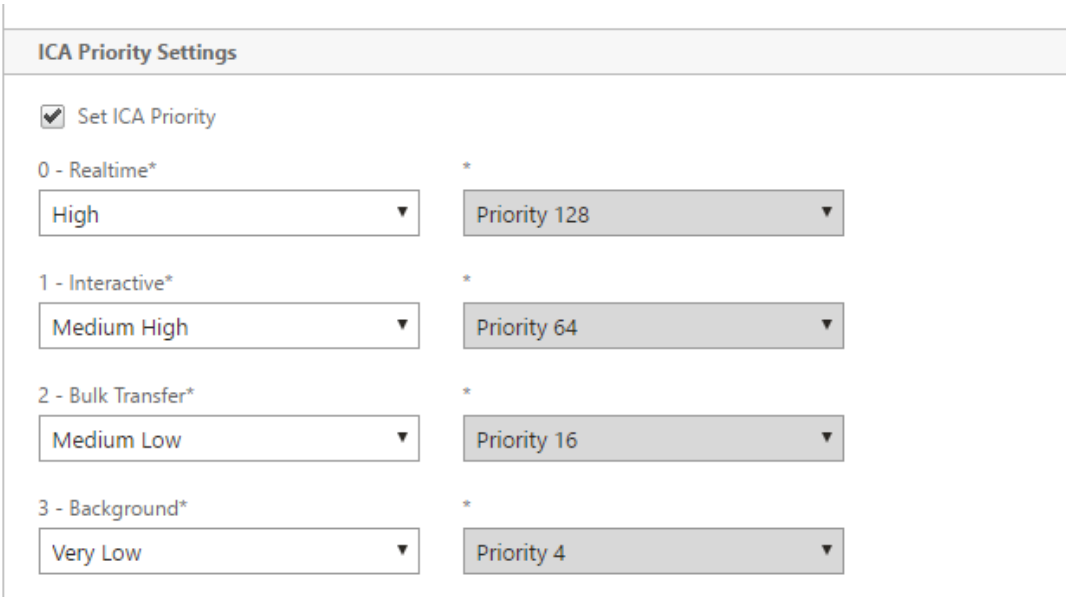


   - **Diffserv/TOS** —将输出数据包上的 DSCP 位设置为所选值。用于控制下游路由器。

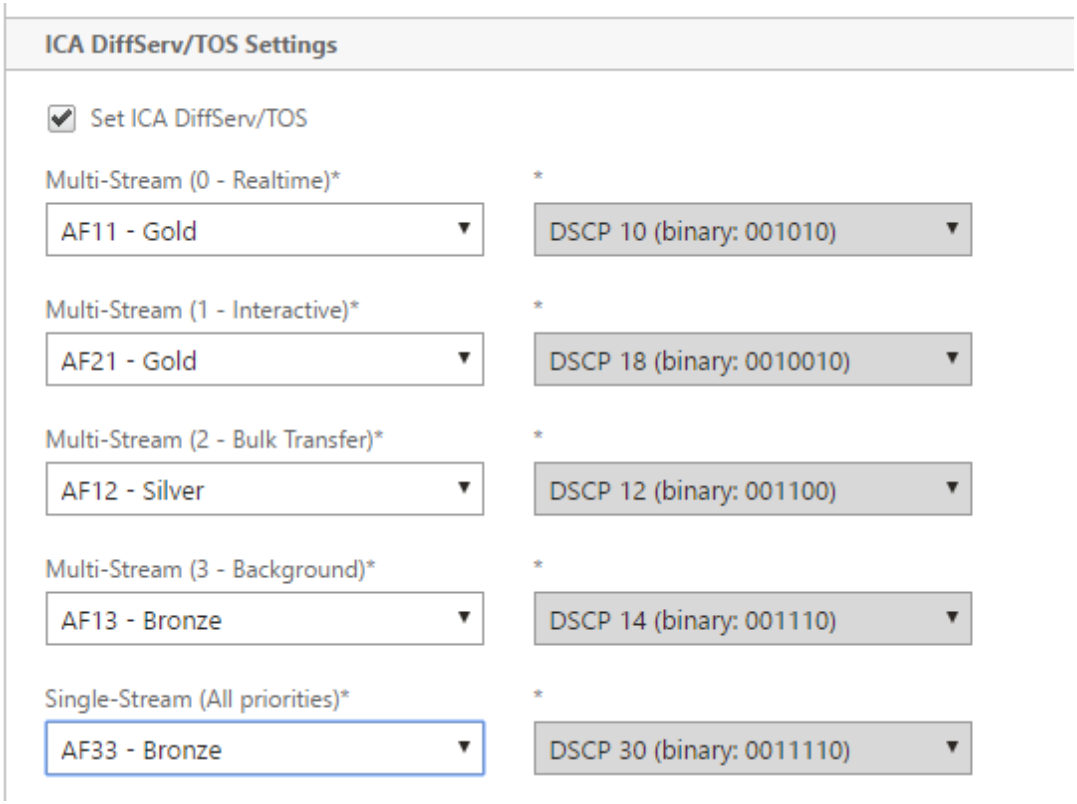
- 带宽限制—使用此策略防止流量超过指定带宽（以链路速度的百分比或绝对值表示）。Citrix 建议指定百分比，以便相同的定义可应用于不同速度的链接。此功能可能会使带宽未使用。例如，设置为链路速度 50% 的策略不允许受影响的流量使用超过 50% 的链路，即使链路在其他方面处于空闲状态。以这种方式限制流量与最大性能不一致，因此除了使用“语音优化”设置的 VoIP 流量之外，此功能很少使用。

  > 注意
  >
  > 配置 带宽限制 仅适用于 Citrix SD-WAN WANOP 版本。对于 Citrix SD-WAN PE 版本，默认情况下禁用 带宽限制 参数。

- 设置 **ICA** 优先级—如果此策略用于 Citrix Virtual Apps/Virtual Desktop 流量，则实时、交互式、批量传输和后台流量的流量的内部优先级将被此处设置的优先级覆盖。



- 设置 **ICA Diffserv/TOS**：对于 ICA（虚拟应用程序/虚拟桌面）流量，四个 ICA 优先级值中的每个值都可以使用不同的 DSCP 值进行标记。此功能对于新的多流 ICA 功能特别有用，在该功能中，虚拟应用程序或虚拟桌面客户端针对不同的优先级使用不同的连接。



3. 单击添加。新创建的流量调整策略列表中列出了流量调整策略。

   现在，您可以将流量调整策略与服务类关联，有关更多信息，请参阅服务类别。

视频缓存

April 23, 2021

许多组织使用视频进行时间不敏感的通信（例如，培训课程和预先录制给员工的消息）。通过视频传递消息不仅具有成本效益，而且当观众分布在时区时也很方便。但是，通过互联网播放视频时会消耗大量的带宽。带宽不足会导致延迟，从而影响用户体验并降低视频通信的影响。

视频缓存可改善 HTTP 视频流的查看体验，特别是在速度较慢的链接上。视频缓存保留在本地 Citrix SD-WAN WANOP 设备上。当本地用户查看已缓存的视频时，设备可以以全局域网速提供缓存副本。

将设备配置为缓存视频后，它会缓存用户查看的视频。您还可以使用预先编入选项从本地视频服务器获取选定的视频，以备将来使用。

视频缓存功能使用拦截代理缓存来检查所有 HTTP 请求。满足下列要求的请求将被缓存。视频不会从缓存中提供，除非缓存引擎将视频评估为新鲜视频。否则，将再次为查看器读取它们，并覆盖以前缓存的版本。

保证最新内容。每次查看视频时，缓存都会检查源服务器，如果视频已更改，则会丢弃缓存内容并下载新内容。

> 注意
>
> 缓存现在是透明的。也就是说，客户端和服务器的 IP 地址都是端到端的。在早期版本中，Citrix SD-WAN WANOP 设备的 IP 地址显示为源地址。

满足以下所有条件时，会缓存视频：

- 用于流式传输视频的协议是 HTTP。默认情况下，端口 80 配置为视频缓存。但是，如果您配置了另一个端口（例如 Web 服务器的 8080），则必须指定此端口用于缓存视频。
- 您已添加要缓存视频的视频源。默认情况下，YouTube、Vimeo、优酷、日常运动和 Metaacafe 视频源都会添加到设备中，但仅启用 YouTube 和 Vimeo。如果要缓存来自任何其他默认源的视频，则必须启用它们。添加新视频源时，您可以在添加视频源时启用它们。
- 除了 YouTube、Vimeo、Metacafe、Dailymotion 和优酷之外，您还可以指定其他网站、IP 地址或子网作为视频源。请注意，这些网站不应有任何避免机制，例如向 URL 添加随机字符。
- 视频必须采用可识别的视频格式之一，并具有以下文件扩展名之一：.3gp、.avi、.dat、.divx、.dvx、.dv-avi、.flv、.fmv、.h264、.hdmov、.m15、.m1v、.m21、.m2a、.m2v、.m4e、.m4v、.m75、.moov、.mov、.movie、.mp21、mp2v、.mp4、.mp4v、.mpe、.mpeg、mpeg4、mpg、mpg2、.mpv、.mts、.ogg、.ogv、.qt、.qtm、.ra、.rm、.ram、.rmd、.rms、rmvb、.rp、rv、.swf、.ts、.vfw、.vob、.webm、.wm、.wma、.wmv 和.wtv。

支持的平台

以下设备支持视频缓存功能：

- SD-WAN WANOP 600 设备，具有 1 Mbps 和 2 Mbps 带宽许可证型号。
- SD-WAN WANOP 800 设备与所有带宽许可证型号.
- 配备 Windows Server 的 SD-WAN WANOP 1000 设备，使用所有带宽许可证型号。
- SD-WAN WANOP 2000 设备与所有带宽许可证型号。
- 配备 Windows Server 的 SD-WAN WANOP 2000 设备，使用所有带宽许可证型号。
- SD-WAN WANOP 3000 设备与所有带宽许可证型号.
- 适用于 Amazon 的 SD-WAN WANOP VPX 和 SD-WAN WANOP VPX

支持视频服务器

Adobe Flash 媒体服务器 4.5 或更高版本支持视频缓存功能。此外，视频缓存支持通过 HTTP 提供视频作为静态链接的任何视频服务器。

支持的部署模式

视频缓存支持内联、VLAN 中继端口内联、虚拟内联和 WCCP 部署模式。

使用视频缓存功能的注意事项

以下是使用视频缓存功能时需要注意的几点。

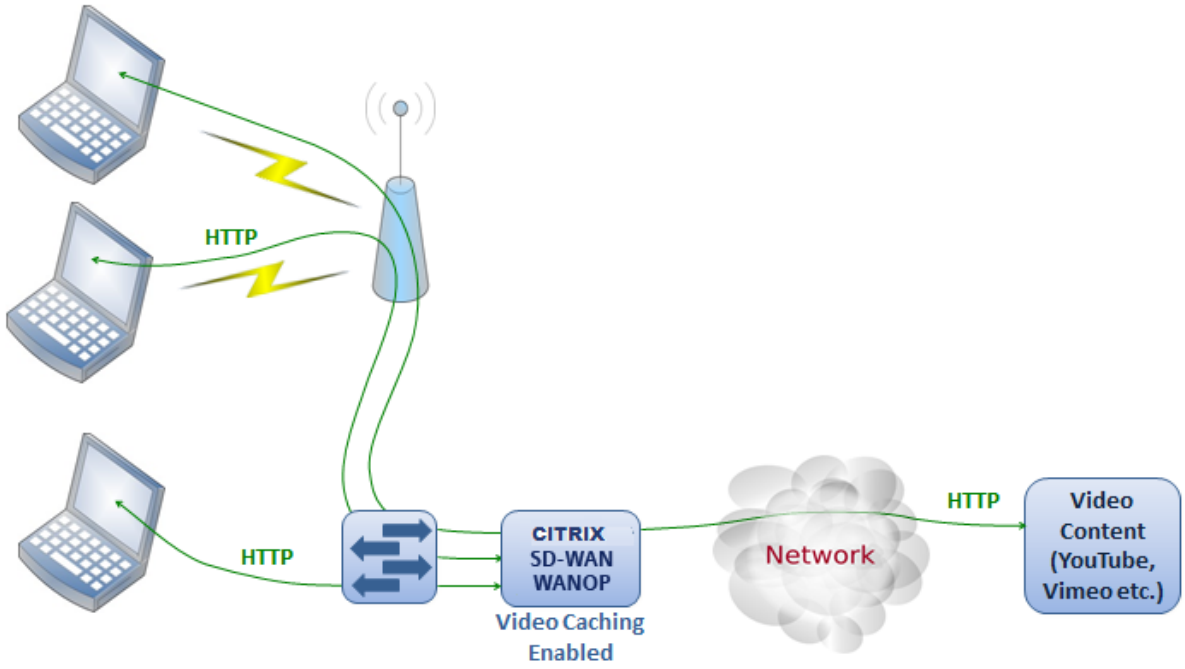
- 如果任何受支持的网站改变了其显示内容的方式，则在更新视频缓存策略文件之前，这些网站的视频缓存优势可能无法实现。对于此类偶尔更改，Citrix 提供了一个更新的视频缓存策略文件。要使用它，请参阅升级视频缓存策略文件。
- 某些视频网站可能对同一视频使用不同的文件格式，具体取决于用于访问视频的操作系统或浏览器。这可能会导致缓存未命中。
- 一些视频网站，如 YouTube，适应网络条件。因此，视频的质量可能取决于缓存时的网络条件。

视频缓存场景

April 23, 2021

在以下情况下，您可以在 Citrix SD-WAN WANOP 设备上部署视频缓存：

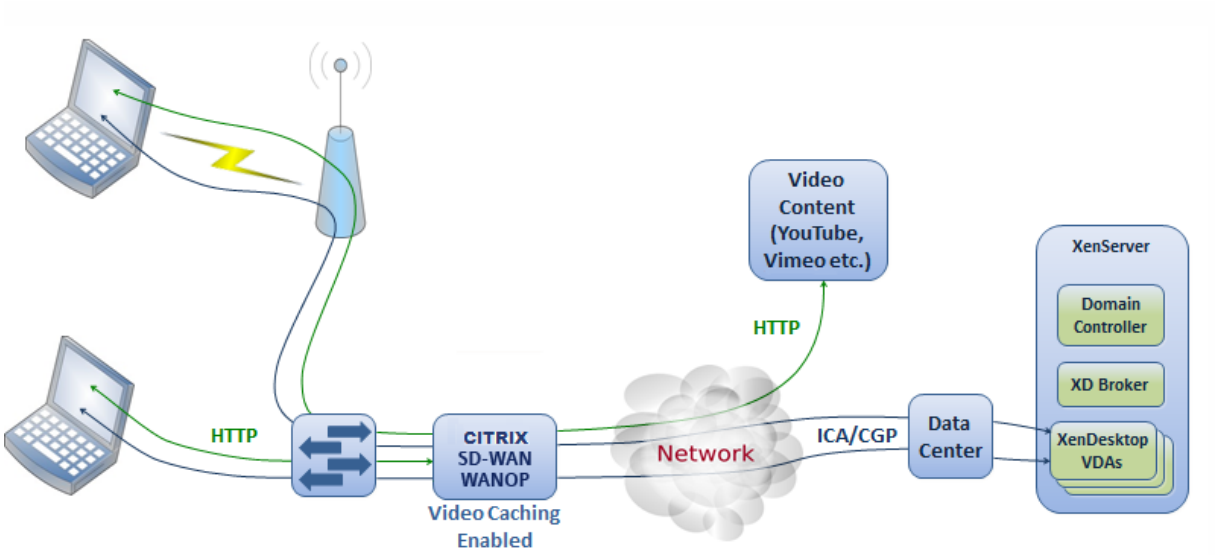
分支机构访问权限



在此用例中，用户通过其计算机上的 Web 浏览器访问互联网。涉及来自已启用站点（如 Vimeo）的视频内容的请求缓存在本地 Citrix SD-WAN WANOP 设备上。随后对同一视频的任何访问都会导致本地设备上的缓存命中，从而允许以 LAN 速度传输视频，而无需等待远程服务器。

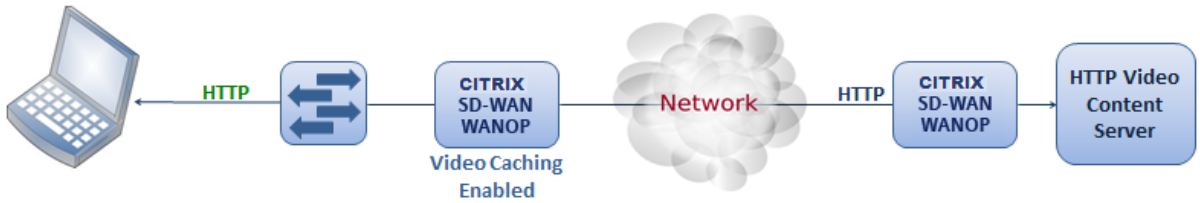
与其他 Citrix SD-WAN WANOP 功能不同，它们可以加速配对设备之间的流量，此功能是一种单端操作，只需要本地设备，并且可以访问视频网站。

使用 **HDX MediaStream** 闪存重定向的 **Citrix Virtual Apps and Desktops** 用户的分支办公室



HDX Flash 重定向是 Citrix Virtual Apps and Desktops 的一项功能。Flash 视频通过此功能将闪存视频隧道传送到本地系统，而不是使用服务器端或数据中心 Internet 在远程虚拟桌面上显示视频。视频将流式传输到实际客户端计算机，并使用分支机构 Internet 在实际客户端上呈现。在分支端 Citrix SD-WAN WANOP 设备上启用视频缓存功能可以显著改善用户的查看体验。此外，启用该功能可降低流式视频的带宽要求。

企业 **HTTP** 视频网络服务器



在此使用案例中，用户可以从数据中心访问视频 Web 服务器。在分支端 Citrix SD-WAN WANOP 设备上启用视频缓存功能时，从分支端 Citrix SD-WANOP 设备的缓存中提供用户请求。这有助于减少到数据中心 Citrix SD-WAN WANOP 设备的网络流量。因此，数据中心 Citrix SD-WAN WANOP 设备的带宽可用于为其他分支机构提供流量。

配置视频缓存

April 23, 2021

您可以通过 Citrix SD-WAN WANOP 图形用户界面或命令行界面配置视频缓存功能。默认情况下，设备配置为缓存来自 YouTube 和 Vimeo 的视频。默认情况下，还会在设备上配置优酷、元器件保护和日常运动。所有你需要做的就是启用它们。您可以添加视频网站，例如提供视频教程或其他信息的内部网站。

> 注意
>
> 视频缓存默认情况下未启用的可选功能。除非您有大量 HTTP 视频流量，否则无需启用它。

必备条件

要在设备上配置视频缓存，请确保满足以下先决条件：

- 您已为计划用于视频缓存的加速桥接端口配置了适当的 IP 地址。
- 您可以从设备 ping apA/apB Gateway。
- DNS 服务器详细信息是准确的。
- 设备可以解析 DNS 名称为 www.Citrix.com。
- Citrix SD-WAN WANOP APX IP 地址在您的企业网络中具有 HTTP 访问权限。

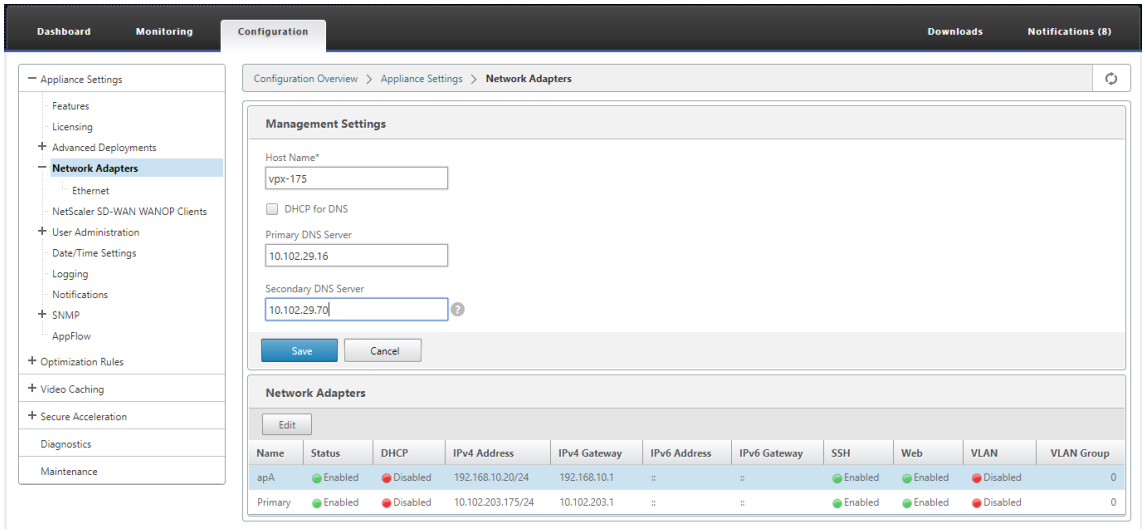
- 如果设备部署在两个网络设备的中继端口之间，则必须在“网络配置”页面上指定具有该设备用于发送 HTTP 请求的 IP 地址的 VLAN ID。
- 对于 **Web**（**Internet**）和 **Web**（专用）服务类，加 速策略设置不应设置为 无。

启用视频缓存功能

您必须先启用视频缓存功能，然后才能开始使用该功能。

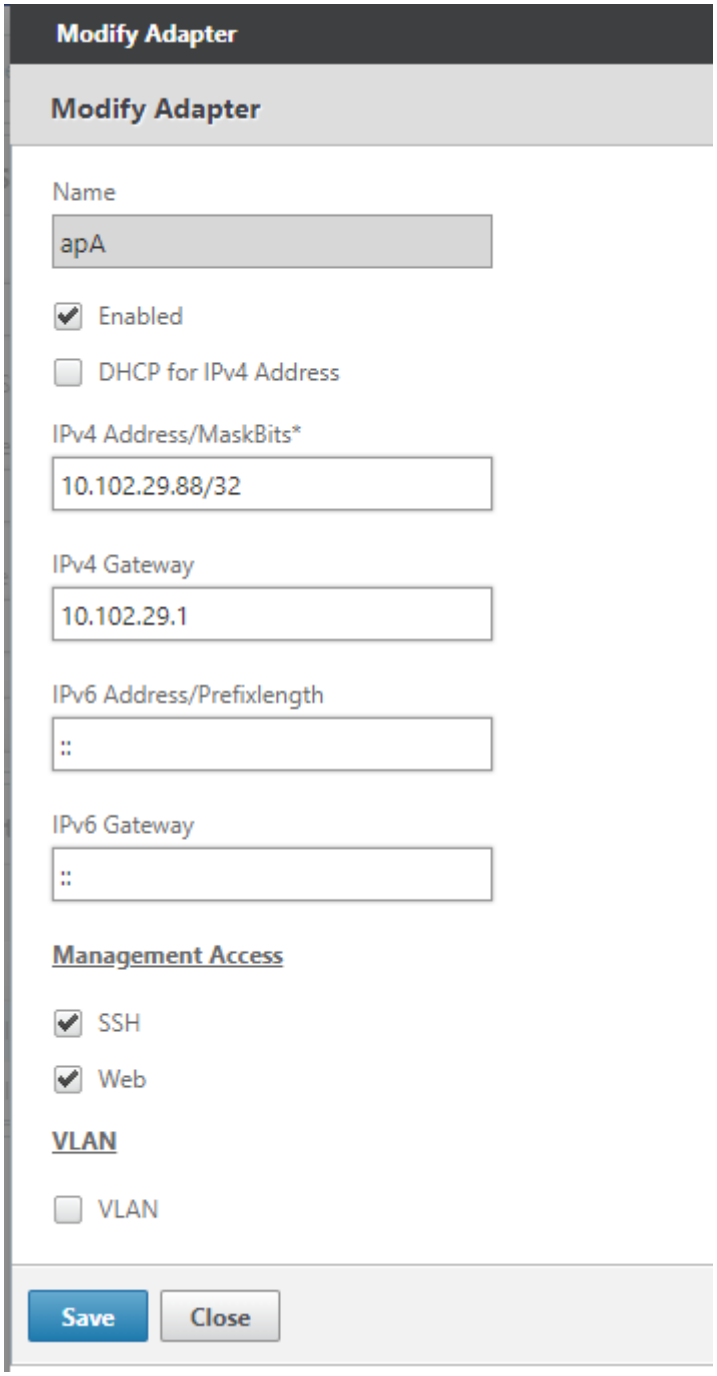
要启用视频缓存，请执行以下操作：

1. 导航到配置 > 设备设置 > 网络适配器，在管理设置部分下，验证并确保主 DNS 服务器详细信息是否准确，并且设备是否能够解析 DNS 名称 www.Citrix.com。单击编辑图标可更改设置。



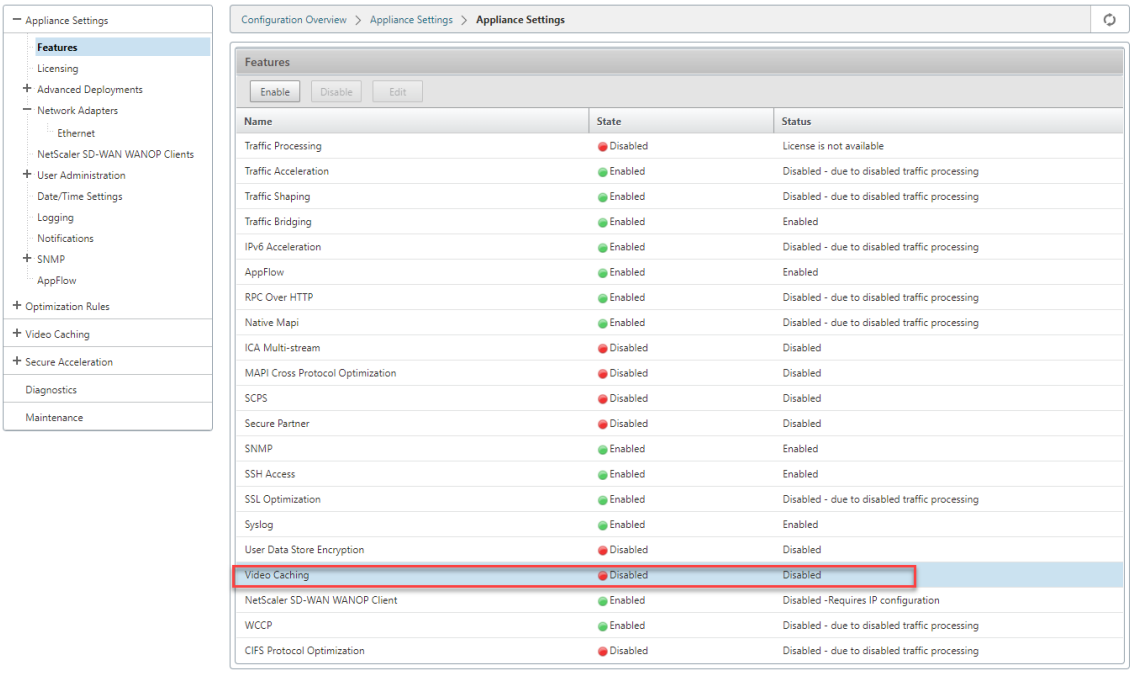
2. 导航到 配置 > 设备设置 > 网络适配器。在网络适配器部分，选择加速对（例如 apA）并单击编辑。

   确保为加速对指定的 IP 地址、网络掩码和默认网 Gateway IP 地址准确无误。



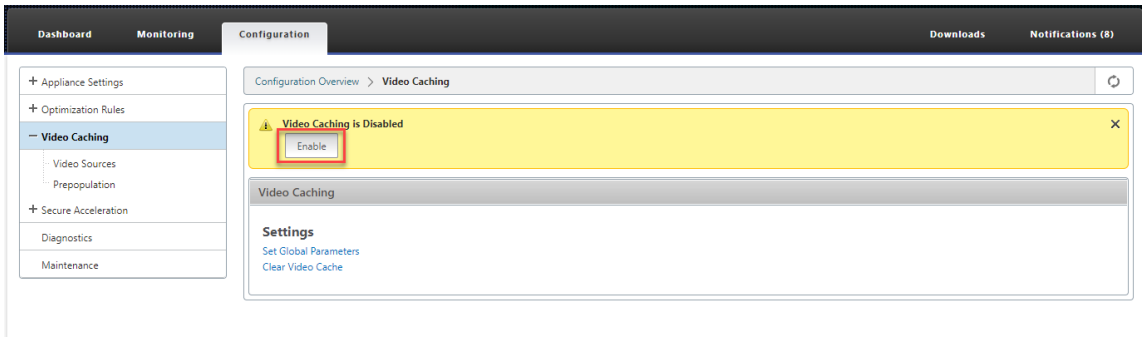
3. 导航到 配置 > 设备设置 > 功 能”页面并启用 视频缓存 功能。

   将显示一个确认对话框，单击 是。



> 注意
>
> 服务重新启动并创建新的缓存分区。如果您首次在设备上启用该功能，则会通过减少分配给其他基于磁盘的压缩的磁盘空间来创建新分区。重置基于磁盘的压缩历史记录，并终止现有连接。

4. 或者，您也可以导航到 配置 > 优化规则 > 视频缓存，然后单击 启用。



添加视频网站

该设备配置为缓存来自 YouTube 和 Vimeo 的视频，部分配置为缓存来自优酷、Metacafe 和 Dailymotion 的视频。要从后三个站点中的任何一个缓存视频，您必须启用该站点。一旦用户访问已启用网站的视频，就会被缓存。您可以通过将其主机名或 IP 地址添加到设备上的“视频源”列表来配置不需要 URL 重写的其他视频网站。您还可以包括没有任何缓存避免机制的自定义站点。

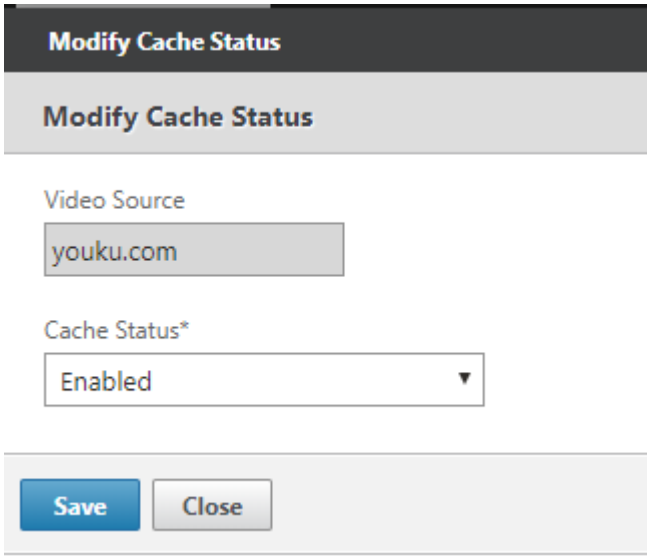
您必须启用这些视频源，然后设备才能缓存其中的视频。

视频缓存功能将视频源用于配置工作流。如果您使用主机名或网站/主机名配置任何视频源，则设备代理流过设备的所有 HTTP 流量。但是，如果仅使用 IP 地址配置所有视频源，则设备仅代理和缓存这些 IP 地址。无论您是使用主机名还是

IP 地址，如果您的组织不允许访问 YouTube、Vimeo、Dailymotion、Metacafe 和优酷网站，请确保禁用这些视频源。

要启用视频源，请执行以下操作：

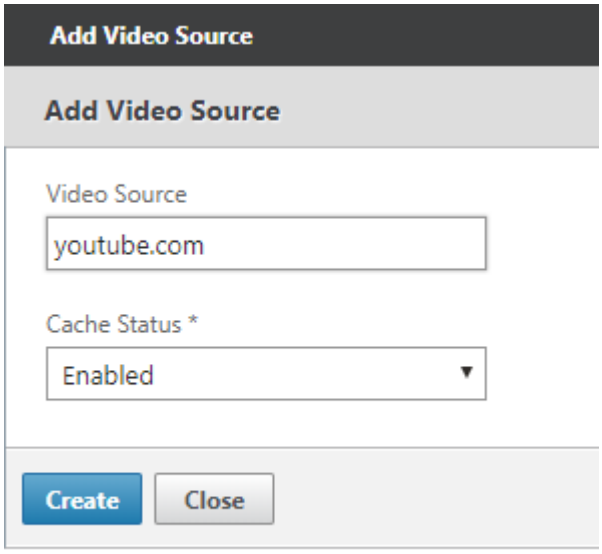
1. 导航到 配置 > 优化规则 > 视频缓存 > 视频源。
2. 从列表中选择一个视频源单击 修改。



3. 在 缓存状态 下拉框中，选择 启用，然后单击 保存。

要添加视频源，请执行以下操作：

1. 导航到 配置 > 优化规则 > 视频缓存 > 视频源，单击 添加。
2. 在 视频源 字段中，键入要添加到视频源列表中的 Web 服务器的网站名称或 IP 地址。
3. 在 缓存状态 列表中，确保 已选择“已启用。如果您希望稍后为此站点启用视频缓存，则可以从此列表中选择 禁用”。



4. 单击创建。

   要删除视频源，请从“视频源”列表中选择该 视频源，然后单击 删除。

视频预填充

April 23, 2021

Citrix SD-WAN WANOP 设备可以在任何人查看视频之前从内部视频服务器下载和缓存视频。如果您希望确保所有用户都获得相同的好处（例如，在特定时间播放自我训练视频时），此功能非常有用。您可以安排要从中获取视频的静态 URL。

获取的视频存储在视频缓存中。只要用户发送 URL 请求，视频就会从缓存中提供，即使是第一次访问视频也是如此。

要提前获取视频，您可以执行以下任务：

- 指定要提前缓存视频的 URL。
- 安排缓存视频的日期和时间。
- 安排要缓存视频的间隔。
- 管理您已添加到列表中的条目。

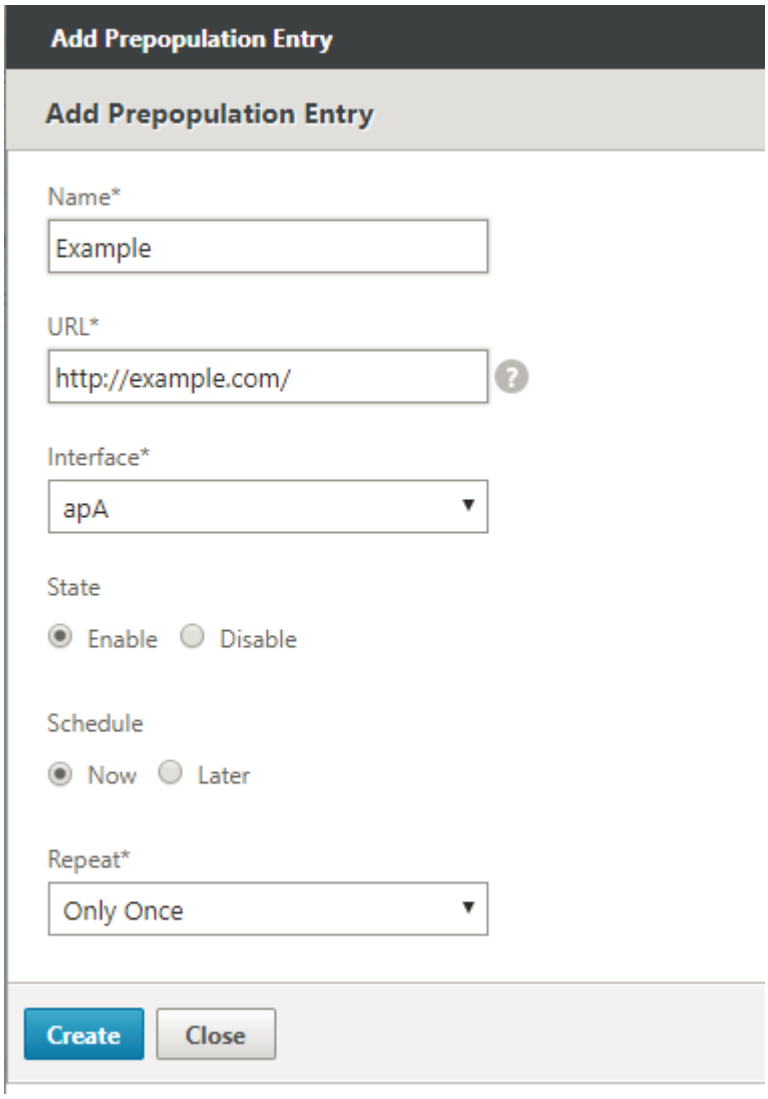
要提前下载和缓存视频，您必须指定特定视频的 URL 或启用目录索引的视频文件夹的绝对路径。

> 注意
>
> 如果您只是将条目添加到视频预填充任务，则会下载并缓存相关视频。但是，当客户端访问视频时，它从视频服务

> 器提供，并且不会获得缓存优势。若要确保客户端获得缓存优势，必须将预填充任务中使用的视频服务器或 IP 地址添加到视频源列表中。

要提前添加 **URL** 以缓存视频，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 预 编入”，然后单击 添加。



2. 在 名称 字段中，指定可用于标识预填入条目的名称。
3. 在 **URL** 字段中，指定要缓存一个或多个视频的 URL。URL 可以是特定视频或视频服务器。请确保指定完整的 URL 或视频文件夹。
4. 在 接口 字段中，选择加速桥接端口以从 URL 下载视频。
5. 将 状态 设置为 启用 以接收状态信息。各州及其描述如下表所示。
6. 您可以立即开始将视频从 URL 下载并缓存到设备，也可以在预定时间下载视频。
7. 单击创建。

下表描述了状态消息：

状态	说明
已配置	在为 URL 配置第一个视图并添加新任务之前，获取用于缓存的视频。
连接超时错误	与服务器的连接已超时，服务器没有响应。
错误 301-永久移动	要下载和缓存的视频已永久移动到另一个位置。
错误 403-禁止	访问要下载和缓存的视频将被拒绝。
错误 404-未找到	要下载和缓存的视频在提供的链接中不可用。
错误 504：服务器无法访问	您指定的 URL 无法访问。
已成功下载“x”文件	为 URL 下载成功，并且“x”数量的媒体文件下载到缓存中。
无法从“y”文件中下载“x”	从 URL 下载某些媒体文件失败。
无法下载 x 个文件	无法从 URL 下载任何媒体文件。
下载已完成	此条目的所有 URL 的处理已完成。
正在下载	下载正在进行中。
正在启动	设备已开始从 URL 下载媒体文件。
删除此条目	该条目正在从 URL 列表中删除。
无法获取目录列表	无法从您指定的远程目录获取列表。
通过清除缓存操作删除条目	该条目已被清除缓存操作清除。
正在更新状态	设备正在更新条目的状态。
计划已经过时间	下载远程对象的计划时间已过去。
缓存中的“x”/”y”文件	刷新条目的状态时，设备发现缓存中存在“y”文件数中的“x”文件数。
为视频缓存禁用接口 AP”x “	没有为视频缓存启用桥接接口 AP”x “。
刷新状态	正在刷新条目的状态。
错误 0	下载视频时出现未知错误。联系 Citrix 技术支持团队以解决此问题。

管理视频缓存预先生成

您可以管理视频缓存预填入，以控制从 URL 下载和缓存视频的方式。您可以执行以下任务来管理视频缓存预先生成：

- 在预定的日期和时间之前或之后开始下载视频。

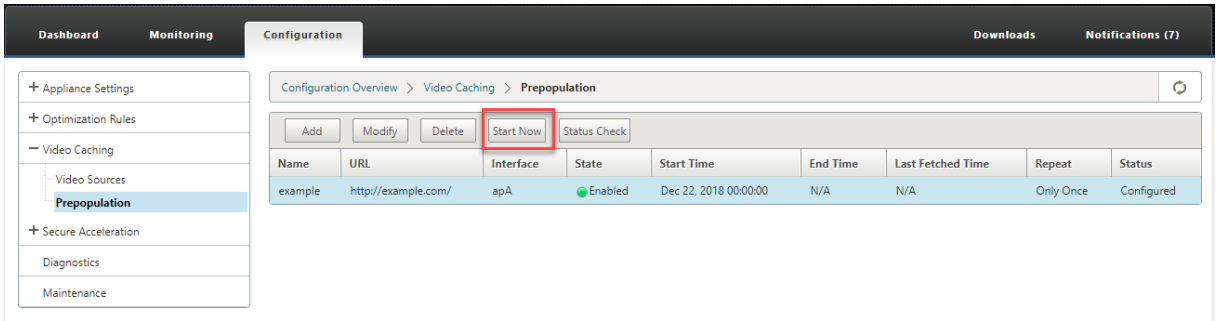
- 更新条目的 URL。
- 禁用 URL 条目中的视频缓存。
- 安排从 URL 条目的视频缓存。
- 更新 URL 条目的接口。
- 刷新 URL 条目的状态。
- 删除 URL 条目。

下面的流程图显示了在管理视频预人体功能的各种活动时所遵循的流程控制。

下载视频

如果网站或您添加的 URL 的技术问题妨碍了计划下载和缓存，您可以随时开始下载和缓存视频。

要立即下载和缓存视频，请导航到 配置 > 视频缓存 > 预 填入”，选择要缓存的视频的条目，然后单击“立 即开始。更新视频的状态大约需要一分钟。



单击“立即开始”后，“状态”列将显示从 URL 下载视频的状态。

更新预填充条目的 URL

添加了提前下载和缓存视频的 URL 后，您可以微调 URL 以获得最佳结果，例如在视频位置发生变化或媒体文件名称在源中发生更改时重新配置 URL。

要更新 **URL**，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 预填入 页面。
2. 选择要更新的条目，然后单击 修改。
3. 在 URL 字段中，指定新 URL。
4. 单击 **OK**（确定）。

禁用预填入条目中的 URL 中的视频缓存

如果要定期使用给定 URL 中的视频预填充缓存，则无需删除该条目。您可以禁用它，然后在需要时启用它。

要禁用条目，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 预填入 页面。
2. 选择要更新的条目，然后单击 修改。
3. 从“状态”中，选择 禁用 选项。
4. 单击 **OK**（确定）。

预先填入条目中的 URL 中的视频缓存

您可以安排要开始从 URL 下载视频并将其缓存到设备的日期和时间。例如，您可能需要在预期用户开始访问视频之前获取视频。这不仅节省了磁盘空间，而且还将最新版本的视频放入缓存中。

要从 **URL** 计划缓存：

1. 导航到 配置 > 视频缓存 > 预填入 页面。
2. 选择要更新的条目，然后单击 修改。
3. 从 计划”中，选择“以 后”选项。
4. 在 开始 字段中，指定要从 URL 下载视频的日期和时间。日期和时间的格式是 YYYY-MM-DD HH: MM: SS。
5. 从“重 复 列表中，选择下载和缓存视频的频率。可用选项如下：
   - 仅限一次：在预定的日期和时间从 URL 下载视频一次。
   - 每日：每天从 URL 下载视频，从预定的日期和时间开始。下载从您指定的开始时间每天开始。
   - 每周：每周从 URL 下载一次视频，从预定的日期和时间开始。下载从您指定的日期和时间开始每周。
   - 每月：从网址下载视频一次，从预定的日期和时间开始。下载从您指定的日期和时间每月开始。
6. 单击 **OK**（确定）。

更新 **URL** 条目中的界面

如果您在网络上配置了多个链接，则可能需要使用特定链接来下载视频，因为网络连接更好。要配置多个链接，请使用可用的桥接端口，例如 apA 和 apB 桥接端口。您可以使用这些端口下载 URL 条目的视频。

要更新 **URL** 条目的接口，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 预置人体。
2. 选择要更新的条目。然后单击 修改。
3. 从 接口 列表中，选择要用于 URL 条目的接口。该列表显示设备上可用和配置的接口。
4. 单击 **OK**（确定）。

刷新 **URL** 条目的状态

随着时间的推移，缓存视频的状态可能会发生变化。定期检查条目的状态可确保用户在访问视频时不会得到意外的结果。

要检查从 **URL** 缓存的视频的最新状态，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 预置人体。
2. 选择要刷新缓存视频状态的条目。
3. 点击 状态检查。

删除 **URL** 条目

如果您不需要 URL 条目，则可以从列表中删除。要删除 URL 条目，请选择该条目，然后单击 删除”。

> 注意
>
> 从列表中删除视频预置任务时，它还会从缓存中删除相关视频对象。

验证视频缓存

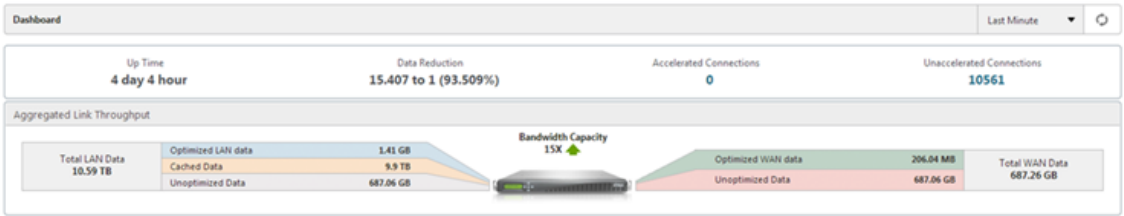
April 23, 2021

“监视”页面、“仪表板”页面和“使用情况”页面上的图形和数据可帮助您评估视频缓存配置所带来的好处。视频缓存产生的数据减少率（类似于整体压缩率）显示在仪表板、视频缓存监视页面和使用率图表页面上。此外，将鼠标悬停在“控制面板”页面上的“数据减少率”上将显示缓存效益百分比以及受支持平台上的压缩效益百分比。

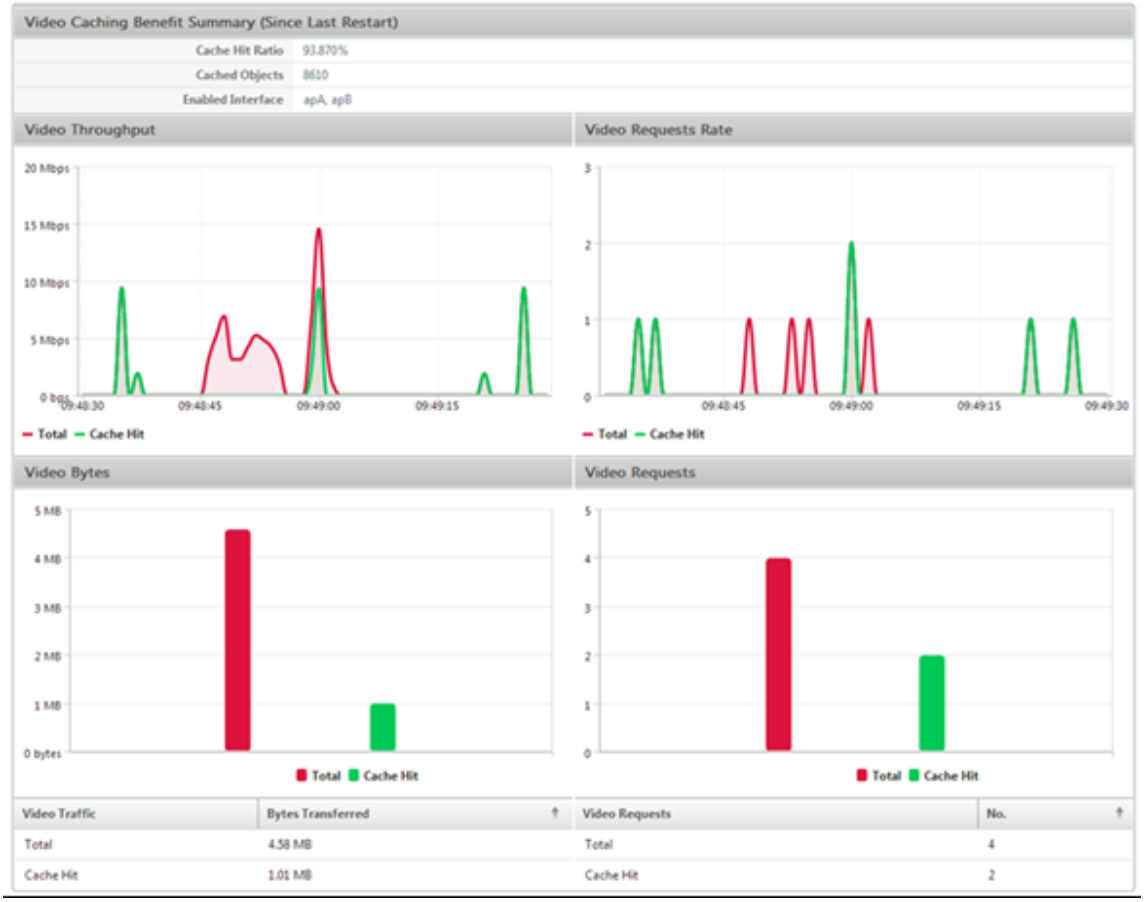
缓存的目的不仅是为了节省带宽，还是为了提高性能，降低视频服务器的负载，并减少网络拥堵的影响。

因视频缓存而节省的预计 WAN 带宽显示如下：

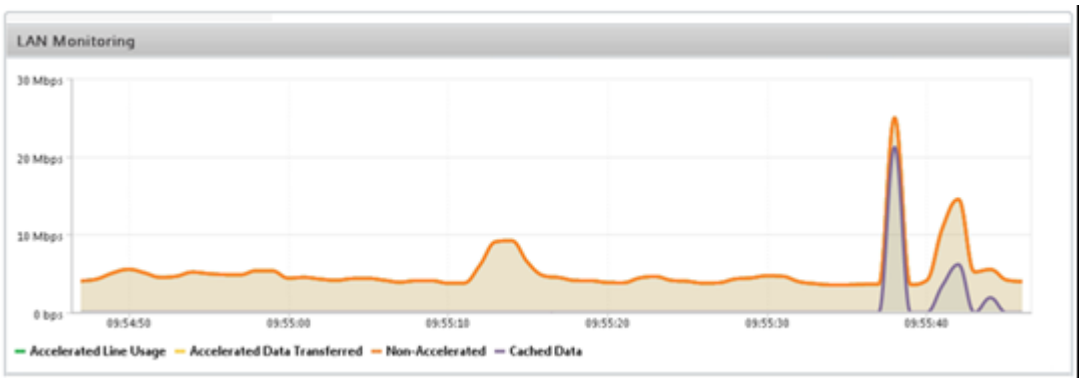
- 在“控制板”页面上，您可以将光标悬停在控制板上的“数据减少”字段上，以百分比形式查看缓存优势。您还可以在“聚合链路吞吐量”下查看缓存（缓存数据）提供的字节。



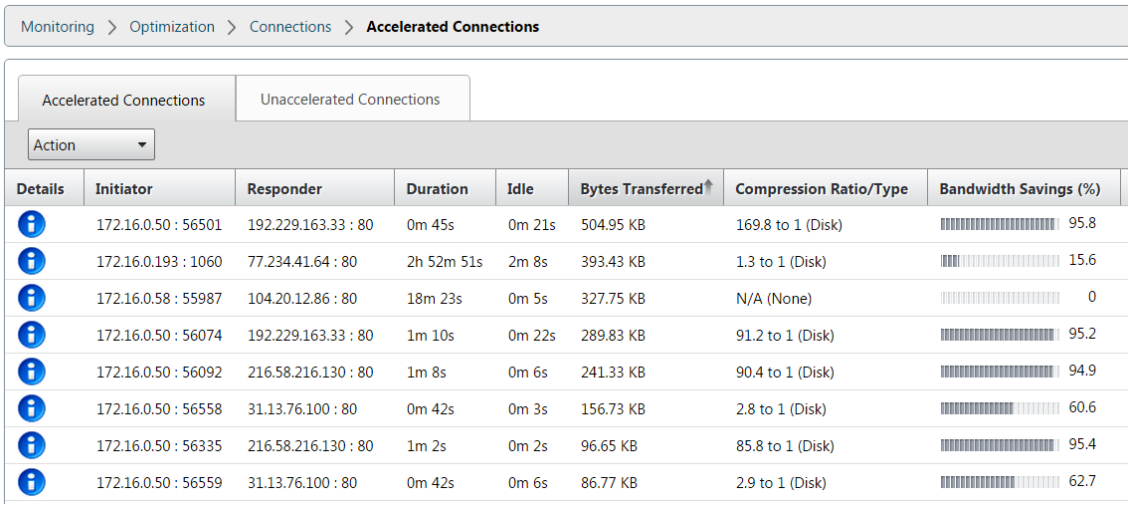
- 在 监视 > 视频缓存 页面上，您可以查看缓存对象的数量和缓存命中率（百分比）。条形图和时间图显示 1 分钟、1 小时、1 天、1 周和 1 个月内从缓存中提供的请求和字节数。此数据也以图表下方的表格格式显示。



- 在 监视 > 优化 > 使用图 页面上，您可以在 LAN 监视图中查看缓存的数据。



- 在 监 控” > 视频缓存 > **HTTP** 状态 列表 页上，您可以监视改进的缓存行为。此页面报告与视频缓存相关的 HTTP 连接状态。
- 在 监视 > 优化 > 连接 页面上，您可以在“加速连接”选项卡上查看缓存的连接。缓存命中和缓存未命中均显示在此处。即使没有加速缓存连接，也会在此处显示。也就是说，即使连接中未涉及合作伙伴 Citrix SD-WAN WANOP 设备，缓存的连接也会在此处显示。节省带宽 (%) 列显示了事务节省多少 WAN 带宽的条形图，无论是通过缓存还是压缩。虽然缓存和压缩的目的是提高速度和可用性，而不是降低带宽使用率，但速度和可用性的增加往往与带宽的减少有关。也就是说，90% 的带宽节省意味着速度提高 10 倍。



Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)
	172.16.0.50 : 56501	192.229.163.33 : 80	0m 45s	0m 21s	504.95 KB	169.8 to 1 (Disk)	95.8
	172.16.0.193 : 1060	77.234.41.64 : 80	2h 52m 51s	2m 8s	393.43 KB	1.3 to 1 (Disk)	15.6
	172.16.0.58 : 55987	104.20.12.86 : 80	18m 23s	0m 5s	327.75 KB	N/A (None)	0
	172.16.0.50 : 56074	192.229.163.33 : 80	1m 10s	0m 22s	289.83 KB	91.2 to 1 (Disk)	95.2
	172.16.0.50 : 56092	216.58.216.130 : 80	1m 8s	0m 6s	241.33 KB	90.4 to 1 (Disk)	94.9
	172.16.0.50 : 56558	31.13.76.100 : 80	0m 42s	0m 3s	156.73 KB	2.8 to 1 (Disk)	60.6
	172.16.0.50 : 56335	216.58.216.130 : 80	1m 2s	0m 2s	96.65 KB	85.8 to 1 (Disk)	95.4
	172.16.0.50 : 56559	31.13.76.100 : 80	0m 42s	0m 6s	86.77 KB	2.9 to 1 (Disk)	62.7

管理视频缓存源

April 23, 2021

您可以通过配置全局设置来全局管理视频源，也可以通过更改视频源的状态单独管理视频源。

配置全局设置

通过全局设置，您可以在设备级别配置功能。无论您添加了哪种视频源，这些设置都适用于设备上的整个视频缓存功能。可以执行以下操作：

- 配置缓存对象的最大大小
- 配置 DNS 后缀
- 配置缓存端口
- 更新视频缓存策略文件

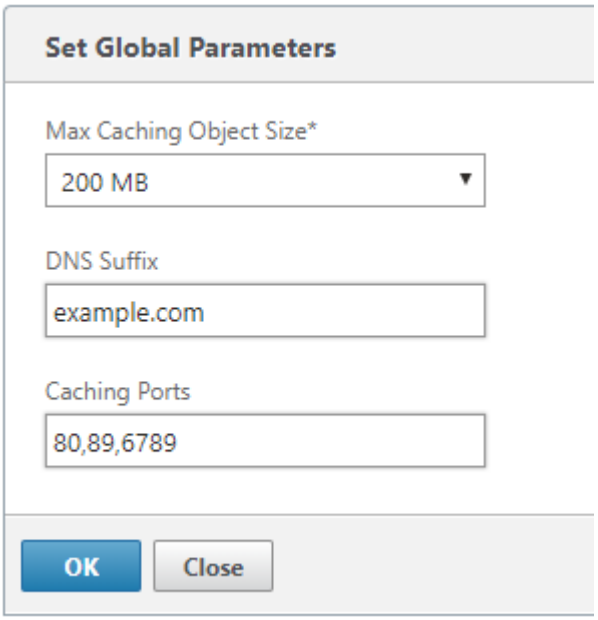
您可以为缓存对象配置最大大小。超过此限制的对象不会缓存。默认情况下，最大缓存对象大小为 100 MB。

对于不包含完整域名并且要求将域名后缀添加到视频服务器的主机名的 URL，需要附加默认域名才能从服务器获取响应。例如，当您访问`http://training/CitrixSD-WANWANOP\\_VideoCaching.mp4`视频时，设备可能需要将 URL 转换为`http://training.example.com/CitrixSD-WANWANOP\\_VideoCaching.mp4`。在这种情况下，您必须将 example.com 指定为域名后缀。

视频缓存功能需要 HTTP 视频服务器的端口号。默认值为端口 80。如果 HTTP 视频服务器使用的端口不是此已知的 HTTP 端口，则必须将端口号添加到缓存端口列表中。

要配置视频缓存的全局设置，请执行以下操作：

1. 导航到 配置 > 视频缓存 > 设置全局参数。



2. 在 最大缓存对象大小 字段中，设置缓存对象的最大大小。

   从可用限制中选择一个值。超过此限制的对象不会缓存。

3. 在 **DNS** 后缀 字段中，输入要追加到不包含完整域名并且要求将域名后缀添加到视频服务器的主机名的 URL 的域名。

4. 在 缓存端口 字段中，键入 HTTP 视频服务器的端口以将其添加到缓存端口列表中。或者，添加以逗号分隔的多个端口号。

5. 单击 **OK**（确定）。

设备将 10% 的分配磁盘空间用于管理目的。当磁盘使用率达到分配磁盘空间的 90% 时，表示磁盘已满。要缓存更多视频对象，设备会从视频缓存中删除使用最少的对象。除非缓存提供过时的视频对象，否则无需清除缓存。

要清除视频缓存，请导航到 配置 > 视频缓存，然后单击 清除视频缓 存”。

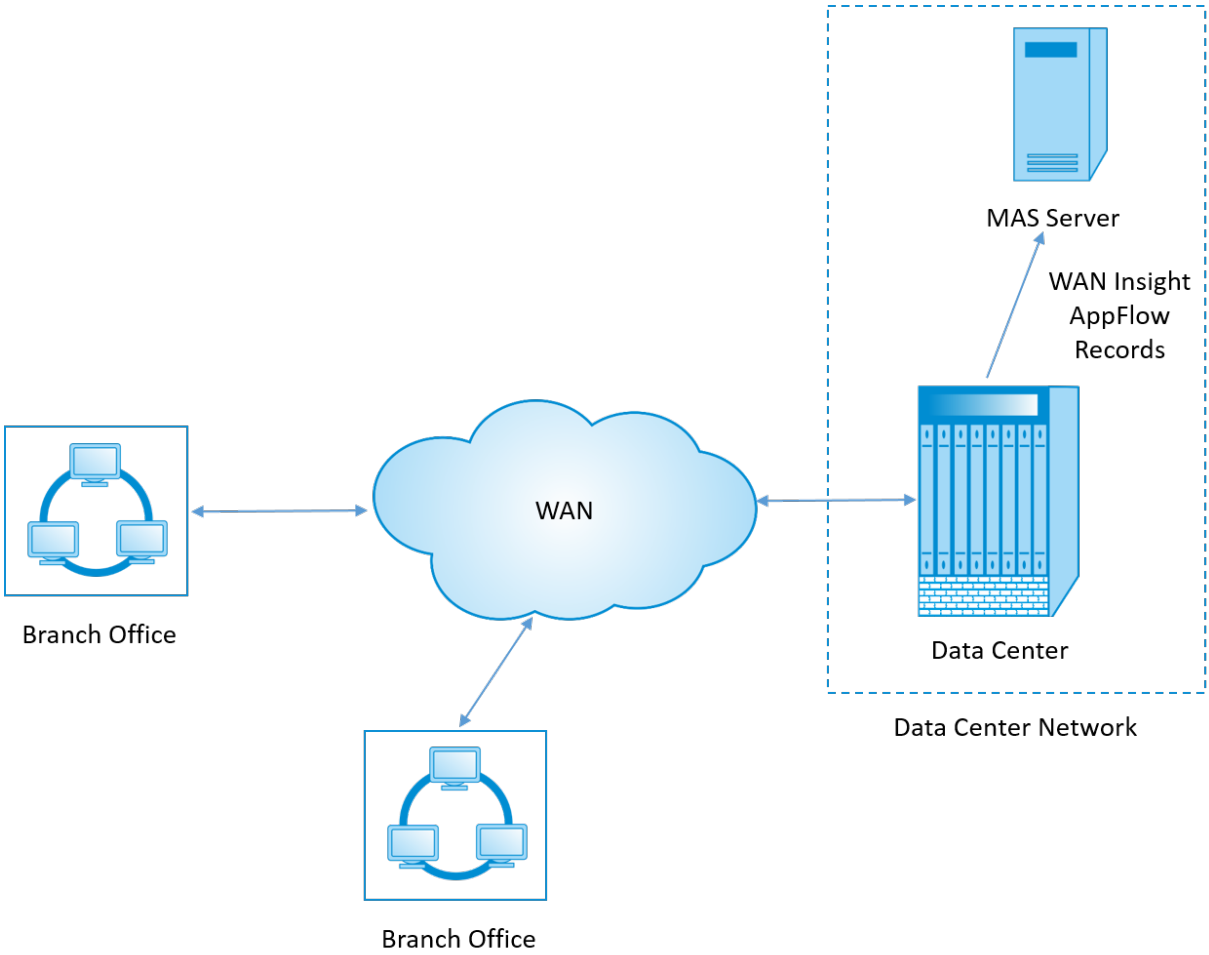
WAN 见解

December 15, 2022

Citrix SD-WAN WANOP 设备通过提高数据中心和分支站点之间的网络数据流的效率，优化了通过 WAN 交付大量应用程序。通过 WAN Insight 分析，管理员可以轻松监视数据中心与分支 WAN 优化设备之间传输的加速和未加速 WAN 流量。通过 WAN Insight 可以查看网络上的客户端、应用程序和分支，从而有助于有效地对网络问题进行故障排除。实时报告和历史报告使您能够主动解决问题（如果有）。

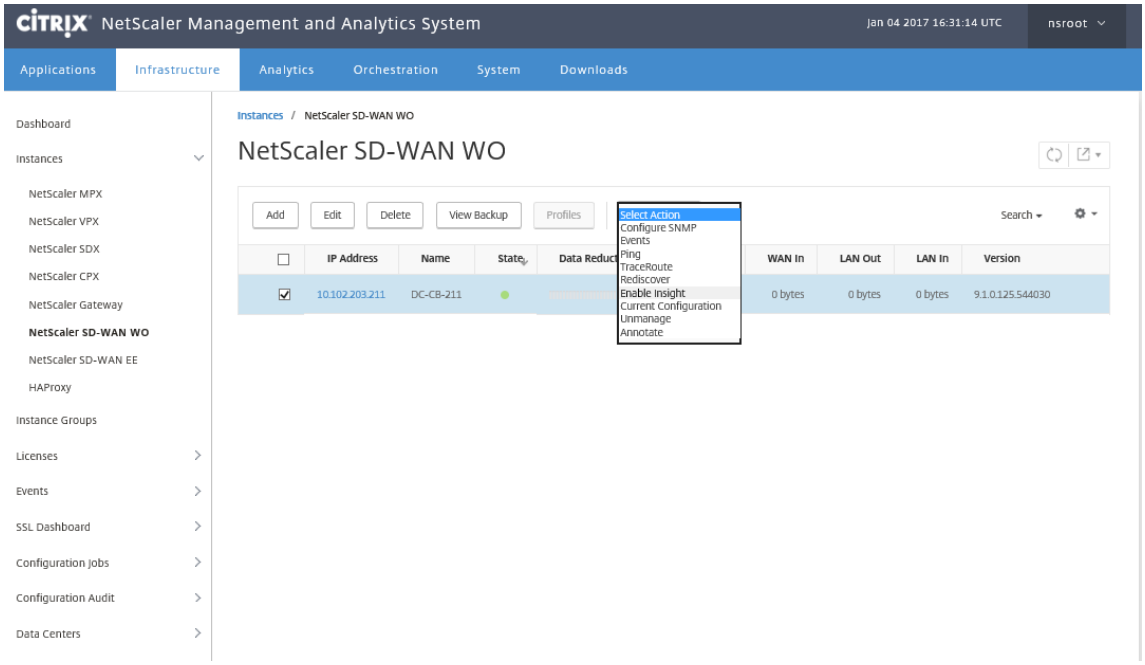
通过对数据中心 WAN 优化设备启用分析，Citrix Application Delivery Management (ADM) 可以收集数据并提供数据中心和分支 WAN 优化设备的报告和统计信息。

> 注意
>
> 有关添加实例的信息，请参阅将实例添加到 Citrix ADM。

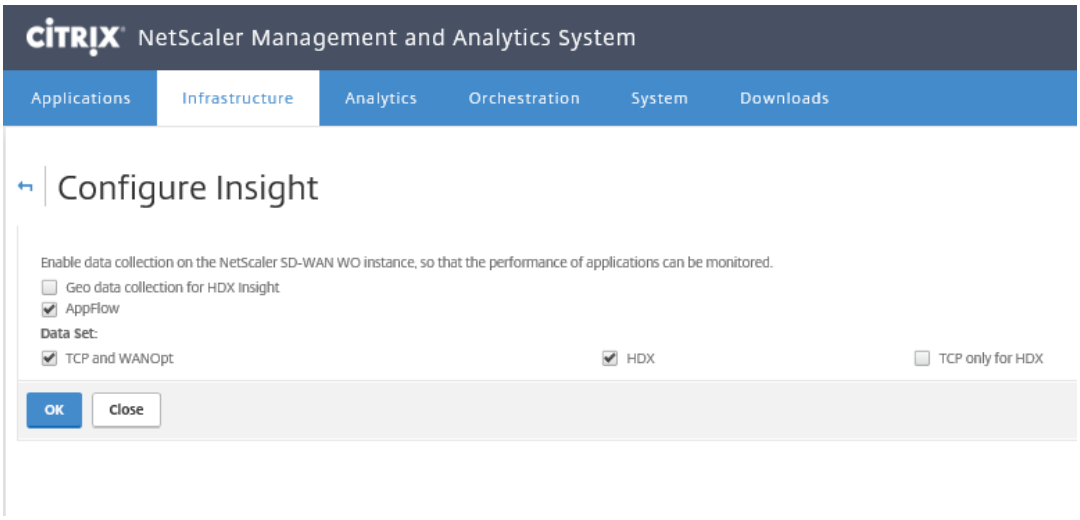


要在 **WAN** 优化设备上启用分析：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 导航到基础架构 > 实例 > **Citrix SD-WAN WO**，然后选择数据中心 WAN 优化设备。



4. 从操作下拉列表中，选择启用 **Insight**。
5. 根据需要选择以下参数：
   - **HDX Insight** 的地理数据收集：与谷歌 Geo API 共享客户端 IP 地址。
   - **AppFlow**：开始从 WAN 优化实例中收集数据。
   - **TCP** 和 **Wanopt**：提供 TCP 和 Wanopt Insight 报告。
   - **HDX**：提供 HDX Insight 报告。
   - **TCP** 仅适用于 **HDX**：仅为 HDX Insight 报告提供 TCP。



6. 单击 **OK**（确定）。

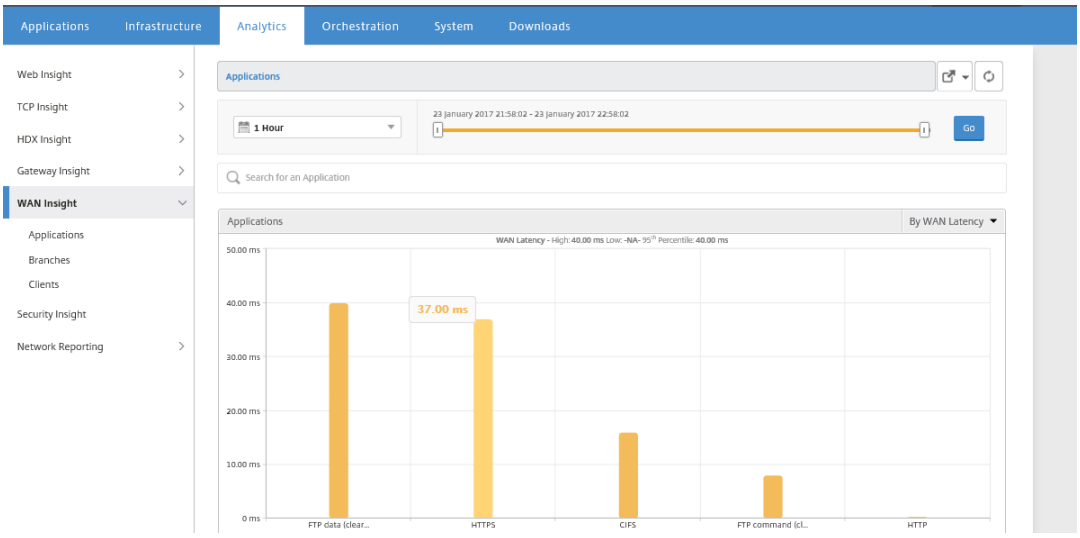
要查看 **WAN** 见解报告，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 导航到分析 > **WAN** 见解。

> 注意
>
> 只有在将 SD-WO 实例添加到 Citrix ADM 后，才可见 WAN 智能分析选项。

您可以查看以下报告：

- 应用程序 -显示所选持续时间内所有应用程序的使用情况和性能统计信息。
- 分支机构**-** 显示所有 WAN 优化分支设备的使用情况和性能统计信息。
- 客户端**-** 显示每个分支中访问 WAN 优化设备的所有客户端的使用情况和性能统计信息。



显示以下指标：
** 指标 **	** 说明 **
——-	————
Active Accelerated Connections（活动加速连接）	加速的活动 WAN 连接数。
Active Unaccelerated Connections（活动未加速连接）	未加速的活动 WAN 连接数。
WAN 延迟	用户与应用程序交互时遇到的延迟（以毫秒为单位）。
Compression Ratio（压缩比）	在选定的持续时间内分支机构与数据中心设备之间的数据压缩比率。
Packets Sent（发送的数据包数）	在选定的持续时间内 WAN 优化设备通过网络发送的数据包数。
Packets Received（接收的数据包数）	在选定的持续时间内 WAN 优化设备从网络接收的数据包数。
Bytes Sent over WAN（通过 WAN 发送的字节数）	Citrix WAN 优化设备在选定持续时间内通过 WAN 发送的字节数。
Bytes Received over WAN（通过 WAN 接收的字节数）	在选定的持续时间内 WAN 优化设备从 WAN 接收的字节数。

LAN RTO	在选定的持续时间内 WAN 优化设备向 LAN 重新传输超时的次数。
WAN RTO	在选定的持续时间内 WAN 优化设备向 WAN 重新传输超时的次数。
Retransmit Packets (LAN)（重新传输数据包 (LAN)）	在选定的持续时间内 WAN 优化设备向 LAN 网络重新传输的数据包数。
Retransmit Packets (WAN)（重新传输数据包 (WAN)）	在选定的持续时间内 WAN 优化设备向 WAN 网络重新传输的数据包数。

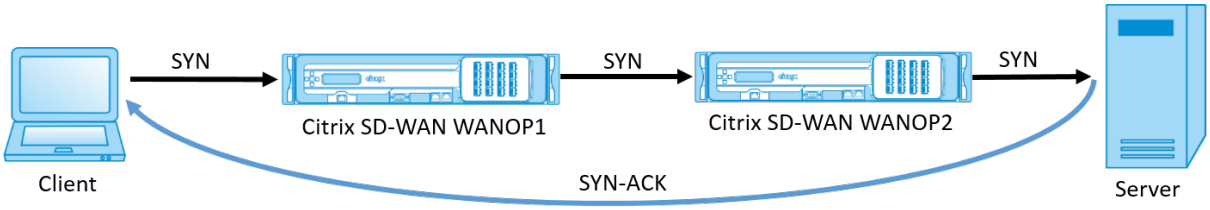
非对称路由

April 23, 2021

在 Citrix SD-WAN WANOP 网络中，当相同 TCP 连接从客户端到服务器或服务器端到客户端的数据包没有通过一个或两个客户端和服务器端 WANOP 设备时，会发生非对称路由。观察到以下不对称的情况。

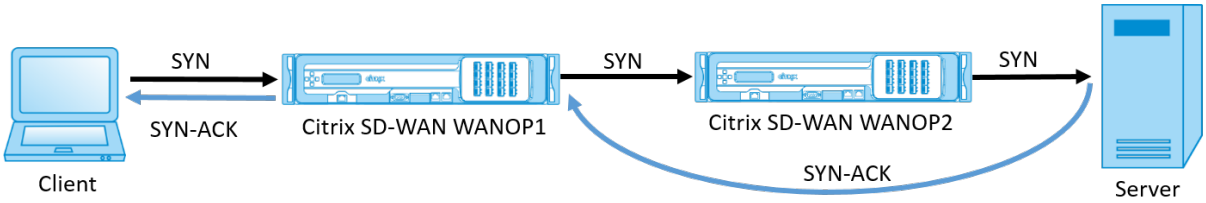
完全不对称：

当数据包通过客户端和服务器端 Citrix SD-WAN WANOP 设备从客户端流向服务器时，会发生完全不对称。但是，在从服务器到客户端的返回路径上，数据包采取不同的路由，绕过 Citrix SD-WAN WANOP 设备。



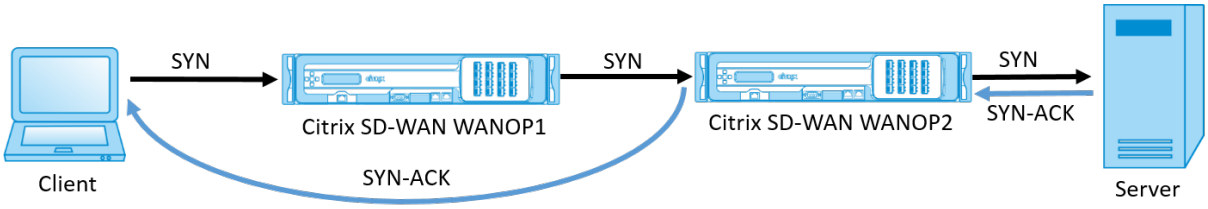
服务器端不对称：

当数据包通过客户端和服务器端 Citrix SD-WAN WANOP 设备从客户端流向服务器时，会发生服务器端不对称性。但是，在返回路径上，数据包绕过服务器端 Citrix SD-WAN WANOP 设备，但遍历客户端 Citrix SD-WAN WANOP 设备。



客户端不对称：

当数据包通过客户端和服务器端 Citrix SD-WAN WANOP 设备从客户端流向服务器时，会发生客户端不对称性。但是，在返回路径上，数据包遍历服务器端 Citrix SD-WAN WANOP 设备，但绕过客户端 Citrix SD-WAN WANOP 设备。



处理 **Citrix SD-WAN WANOP** 网络中的不对称

在 Citrix SD-WAN WANOP 网络中，当发生完全不对称时，TCP 连接被重置。为了避免 TCP 连接中断并继续发送未加速的流量，SD-WAN WANOP 10.1 中引入了非对称连接列表。默认情况下，此功能处于禁用状态；您可以在客户端和服务器端 SD-WANOP 设备上启用此功能。

首次检测到非对称连接时，客户端和服务器之间的 TCP 连接会被重置，并且元组的条目会在非对称连接列表中进行。元组由客户端 IP 地址和服务器 IP 地址组成。来自元组的后续连接通过未加速。连接元组保留在非对称连接列表中，默认超时时间为 4 小时，或直到检测到对称性为止。在超时发生或设备动态检测到不对称不再存在之前，未加速直通是有效的。

当检测到客户端不对称或服务器端不对称时，将保留 TCP 连接，并且数据包未加速通过 Citrix SD-WAN WANOP 设备。

要在 Citrix SD-WAN WANOP 设备上启用非对称连接列表，请执行以下操作：

1. 访问 WANOP CLI 命令提示符（WANOP 加速器/经纪商 IP）。
2. 使用以下凭据登录：

```
**登录为: ** * cli*****

**登录**:  **** * 管理员*****

**密码**: **** *nsroot*****
```

> 注意
>
> 管理员的默认密码是 *nsroot*。如果您更改了密码，请使用正确的密码。

3. 键入以下命令并按回车键。

```
*将参数 AssymetricConnectionList.Enable 设置为 on*
```

> 注意
>
> 您可以根据您的网络要求配置超时时间段，使用 *AssymetricConnectionList.AutoFlushDuration* 命令。

有多个参数可用于不对称列表，这些参数可根据您的网络环境按需进行微调。有关详细信息，请联系 Citrix 客户支持。

Citrix SD-WAN WANOP 客户端插件

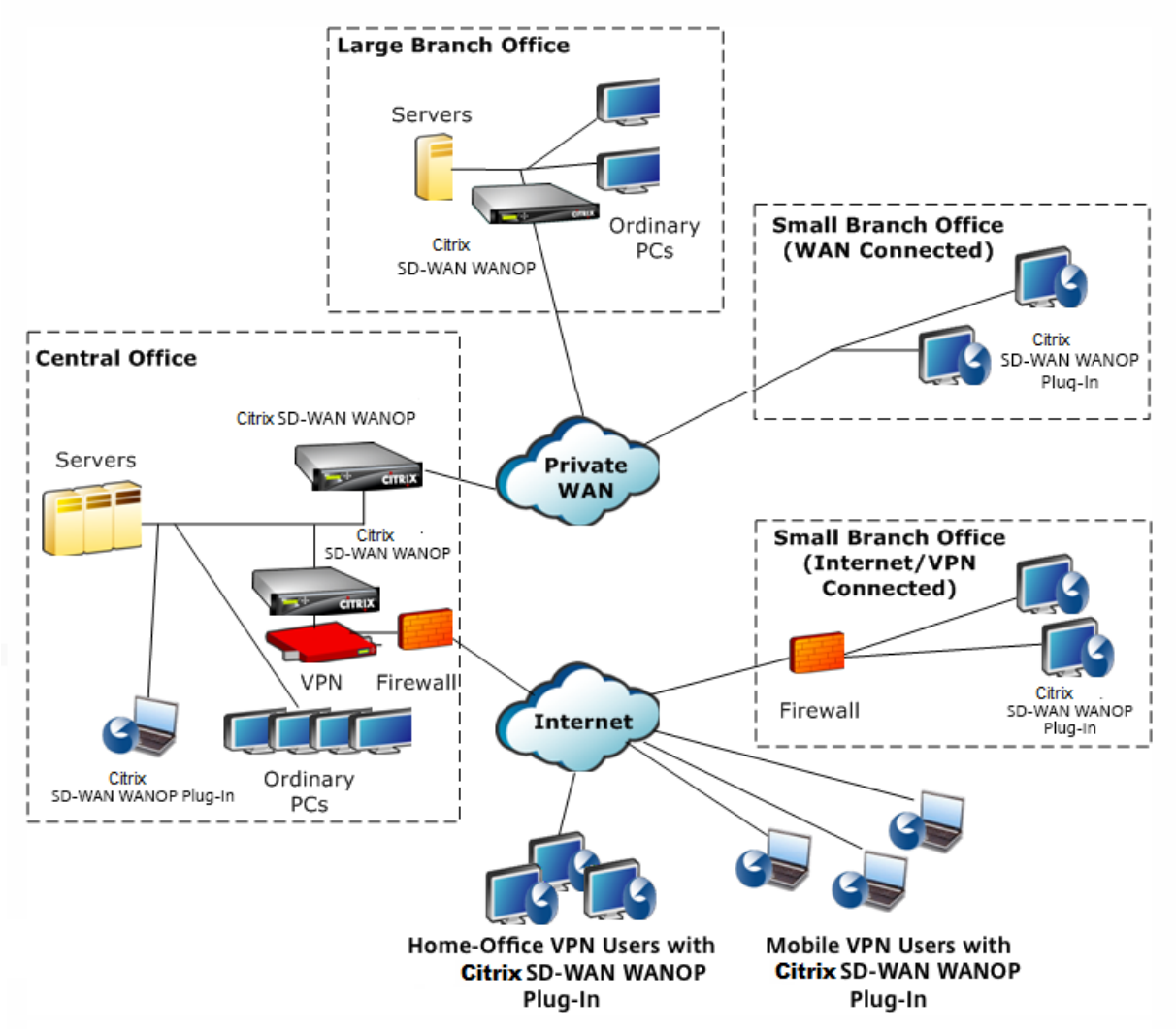
April 23, 2021

Citrix WANOP 客户端插件是一种基于软件的网络加速器，可在 Windows 笔记本电脑和工作站上运行，在任何地方提供加速，而不仅仅是在具有 WANOP 客户端插件设备的办公室。它连接到链接另一端的 Citrix WANOP 设备。

WANOP 客户端插件操作的原理通常与 WANOP 客户端插件设备的原理相同。有关插件文档中未包含的主题，请参阅较大的文档集。

该插件作为标准的微软安装文件 (MSI) 分发。插件部署需要在链接的另一端对 WANOP 设备进行某些特定于插件的配置。如果使用 WANOP 设备的 DNS 或 IP 地址以及其他一些参数自定义 MSI 文件，则用户在其 Windows 计算机上安装插件时不必输入任何配置信息。

图 1. 显示 WANOP 客户端插件的典型 WANOP 客户端插件网络



> 注意
>
> 该插件受 Citrix Receiver 1.2 或更高版本的支持，并且可由 Citrix Receiver 分发和管理。

硬件和软件要求

April 23, 2021

在加速链接的客户端，Windows 台式机和笔记本电脑系统支持
WANOP 客户端插件，但不支持上网本或瘦客户端。Citrix 建议运行
WANOP 客户端插件的计算机遵循以下最低硬件规范：

- Pentium 4 级 CPU
- 2 GB RAM
- 2 GB 可用磁盘空间

Windows 10 平台支持 WANOP 客户端插件，需要以下系统要求：

- 4 GB 内存
- 10GB 可用磁盘空间

以下操作系统支持 WANOP 客户端插件：

- Windows XP Home
- Windows XP Professional
- Windows Vista（Home Basic、Home Premium、Business、Enterprise 和 Ultimate 的所有 32 位版本）
- Windows 7（Home Basic、Home Premium、Professional、Enterprise 和 Ultimate 的所有 32 位和 64 位版本）
- Windows 8（Enterprise Edition 的 32 位和 64 位版本）
- Windows 10（Enterprise Edition 的 32 位和 64 位版本）

在服务器端，以下设备当前支持
WANOP 客户端插件部署：

- WANOP 客户端插件 VPX
- WANOP 客户端插件 2000
- WANOP 客户端插件 3000

- WANOP 客户端插件 4000
- WANOP 客户端插件 5000

WANOP 插件的工作原理

April 23, 2021

WANOP 客户端插件产品使用您现有的 WAN/VPN 基础设施。安装插件的计算机将继续访问 LAN、WAN 和 Internet，就像安装插件之前一样。无需更改路由表、网络设置、客户端应用程序或服务器应用程序。

Citrix 接入网关 VPN 需要少量的 WANOP 客户端插件特定配置。

插件和设备处理连接的方式有两种变化：透明模式 和 重定向模式。重定向器是新部署不推荐使用的旧模式。

- 插件到设备加速的透明模式 与设备到设备加速非常相似。WANOP 客户端插件设备在插件和服务器之间传输时必须位于数据包所采用的路径中。与设备到设备的加速一样，透明模式可作为透明代理工作，从连接的一端保留源和目标 IP 地址以及端口号。
- 重定向器模式（不推荐）使用显式代理。插件将传出的数据包重新定向器 IP 地址。设备将数据包重新地址到服务器，同时将返回地址更改为指向自身而不是插件。在此模式下，设备不必物理上与 WAN 接口和服务器之间的路径内联（尽管这是理想的部署）。

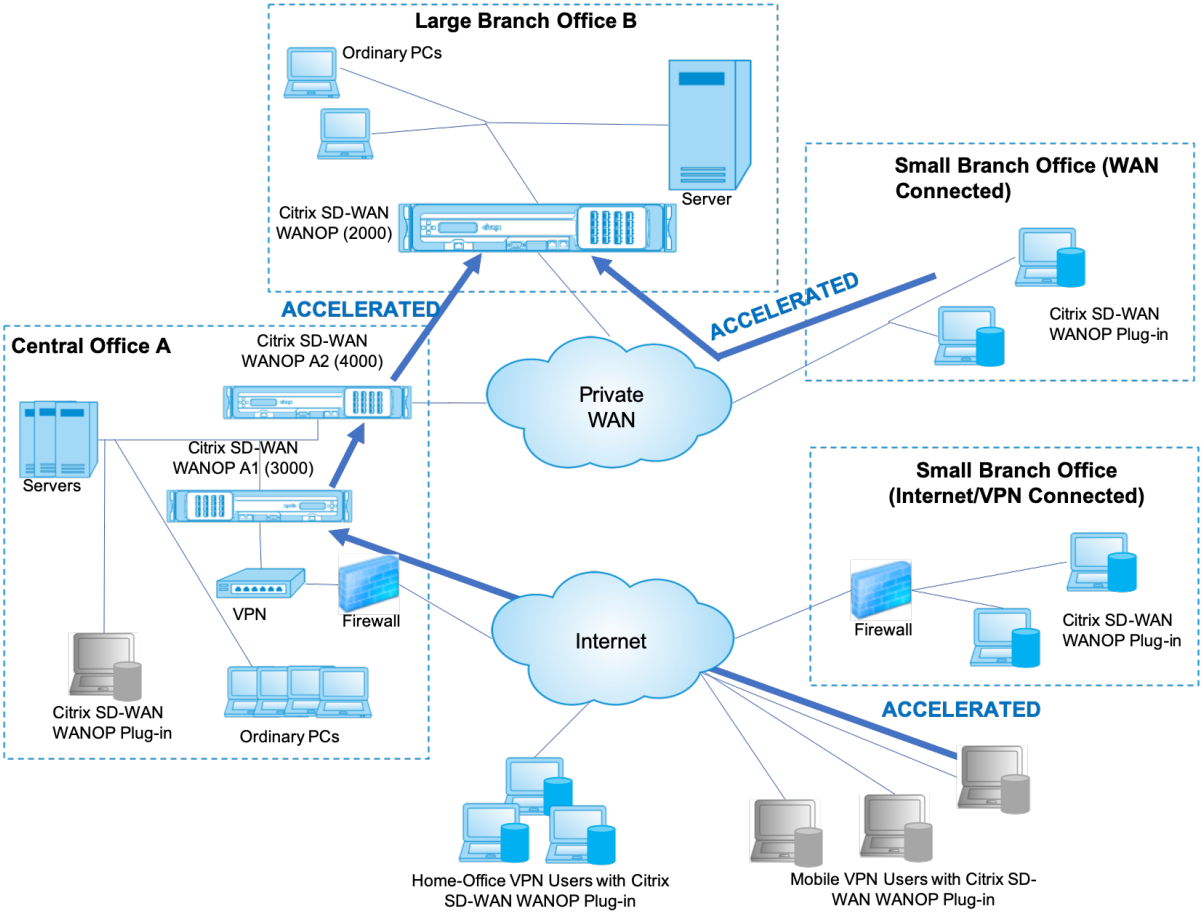
  最佳实践：当你可以使用透明模式，当你必须使用重定向模式。

透明模式

在透明模式下，用于加速连接的数据包必须通过目标设备，就像在设备到设备的加速中一样。

插件配置为可用于加速的设备列表。它尝试联系每个设备，打开信号连接。如果信令连接成功，插件会从设备下载加速规则，从而发送设备可加速的连接的目标地址。

图 1. 透明模式，突出显示三个加速路径



> 注意
>
> - 流量流-透明模式可加速 Citrix WANOP 客户端插件与启用了插件的设备之间的连接。
> - 许可-设备需要许可证才能支持所需数量的插件。在图中，Citrix SD-WAN WANOP A2 不需要为插件加速许可，因为 Citrix SD-WAN WANOP
> A1 为站点 A 提供插件加速。
> - 菊花链-如果连接在通往目标设备的路上通过多个设备，则中间的设备必须启用“菊花链”，否则加速被阻止。在图中，来自大型分支机构 B 的家庭办公室和移动 VPN 用户的流量由 Citrix SD-WAN WANOP B 加速。为此，Citrix SD-WAN WANOP A1 和 A2 必须启用菊花链。

每当插件打开新连接时，它都会查看加速规则。如果目标地址与任何规则匹配，插件会尝试通过将加速选项附加到连接中的初始数据包（SYN 数据包）来加速连接。如果插件已知的任何设备将加速选项附加到 SYN-ACK 响应数据包，则会与该设备建立加速连接。

应用程序和服务器不知道已建立加速连接。只有插件软件和设备知道正在发生加速。

透明模式类似于设备到设备的加速，但与其不完全相同。不同之处是：

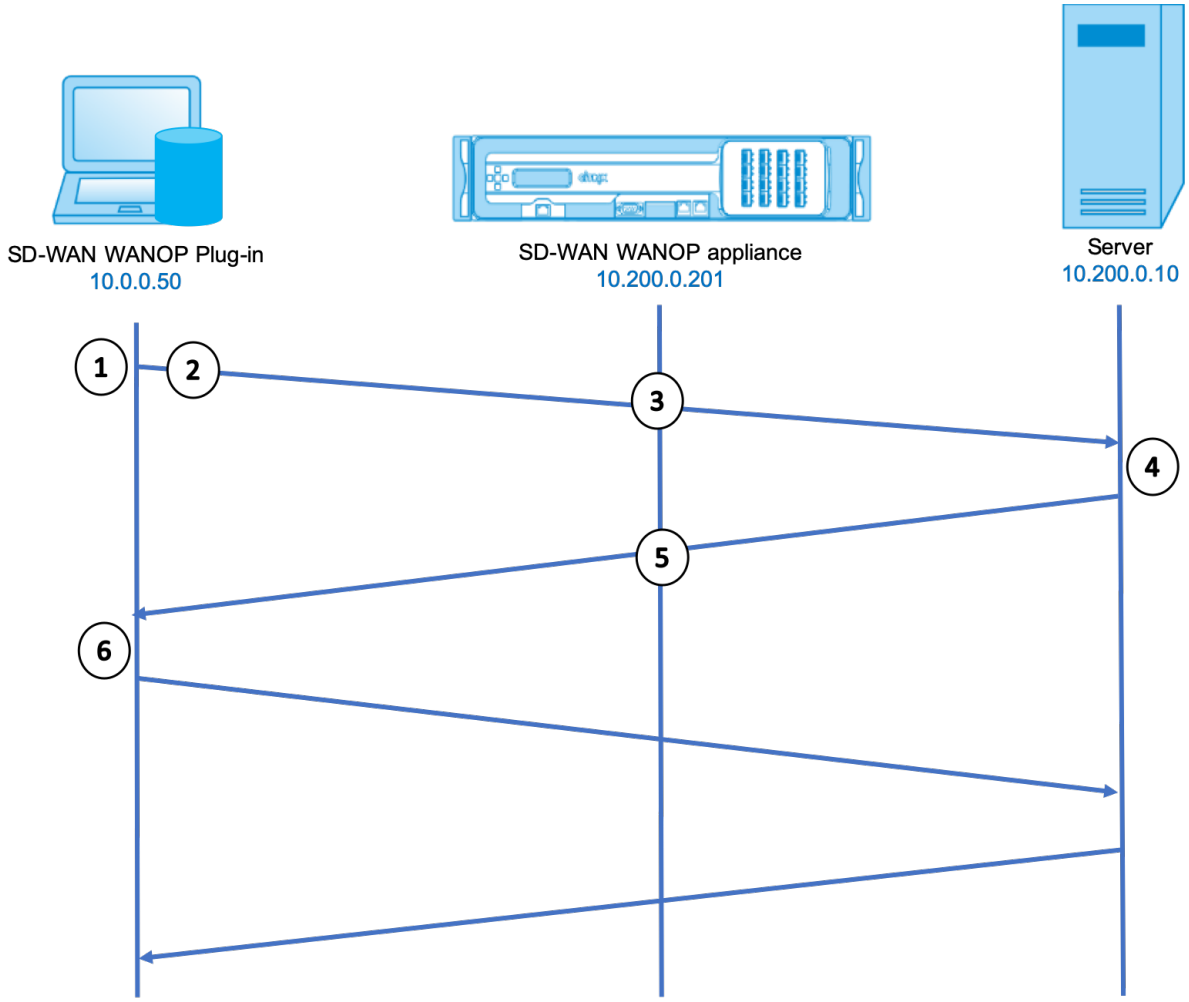
- 仅客户端启动的连接—透明模式仅接受由配备插件的系统启动的连接。如果将配备插件的系统用作服务器，则不会加速服务器连接。另一方面，无论哪一端是客户端，哪一端是服务器，设备到设备的加速都会起作用。（主动模式 FTP 被视为特殊情况，因为启动插件请求的数据传输的连接是由服务器打开的。）

- 信令连接-透明模式使用插件和设备之间的信令连接传输状态信息。设备到设备加速不需要信令连接，但安全对等关系除外，默认情况下处于禁用状态。如果插件无法打开信令连接，则不会尝试通过设备加速连接。
- 菊花链-对于位于插件与其所选目标设备之间路径中的设备，必须在 配置：调整 菜单上启用菊花链。

透明模式通常与 VPN 一起使用。WANOP 客户端插件与大多数 IPsec 和 PPTP VPN 以及 Citrix Access Gateway VPN 兼容。

下图显示了透明模式下的数据包流。此数据包流几乎与设备到设备的加速相同，只是决定是否尝试加速连接是基于通过信令连接下载的加速规则。

图 2. 透明模式下的数据包流



1. 用户的应用程序打开到服务器的 TCP 连接，发送 TCP SYN 数据包。

   Src: 10.0.0.50, Dst: 10.200.0.10

2. WANOP 插件会查找目标地址，并发现它与设备加速的子网匹配。它将 WANOP 选项附加到 SYN 数据包的 TCP 标头。没有更改地址。

   Src: 10.0.0.50, Dst: 10.200.0.10

3. 设备记录 SYN 选项并识别这是可加速连接。它从数据包中剥离选项，并允许它传递给服务器。没有更改地址。

   Src: 10.0.0.50, Dst: 10.200.0.10

4. 服务器接受连接并使用 TCP SYN-ACK 数据包进行响应。

   Src: 10.200.0.10, Dst: 10.0.0.50

5. 设备使用 TCP 标头选项标记 SYN-ACK 数据包，该选项显示将发生加速。

   Src: 10.200.0.10, Dst: 10.0.0.50

6. WANOP 插件接收 SYN-ACK 数据包。数据包标头中的选项指示连接已加速。插件会剥离这些选项并将 SYN-ACK 数据包传递给应用程序。连接现已完全打开并加速。

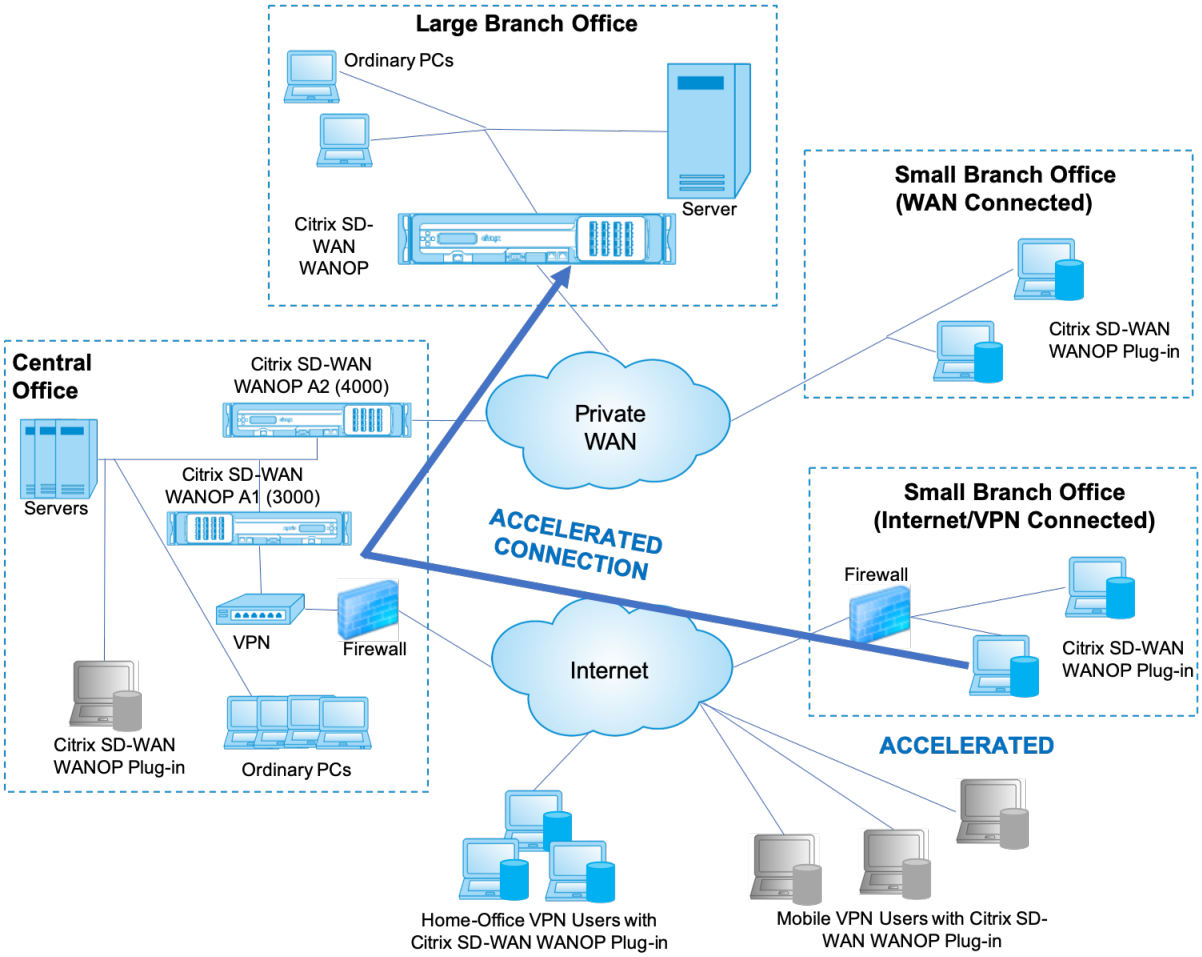
重定向器模式

重定向器模式的工作方式与透明模式有所不同：

- WANOP 客户端插件软件通过将数据包明确地寻址到设备来重定向数据包。
- 因此，重定向器模式设备不必拦截所有 WAN-Link 流量。由于加速连接是直接给它的，因此只要插件和服务器都能到达，它就可以放置在任何地方。
- 设备执行其优化，然后将输出数据包重定向到服务器，将数据包中的源 IP 地址替换为自己的地址。从服务器的角度来看，连接始于设备。
- 来自服务器的返回流量会发送到设备，该设备在返回方向上执行优化，并将输出数据包转发到插件。
- 目标端口号不会更改，因此网络监视应用程序仍然可以对流量进行分类。

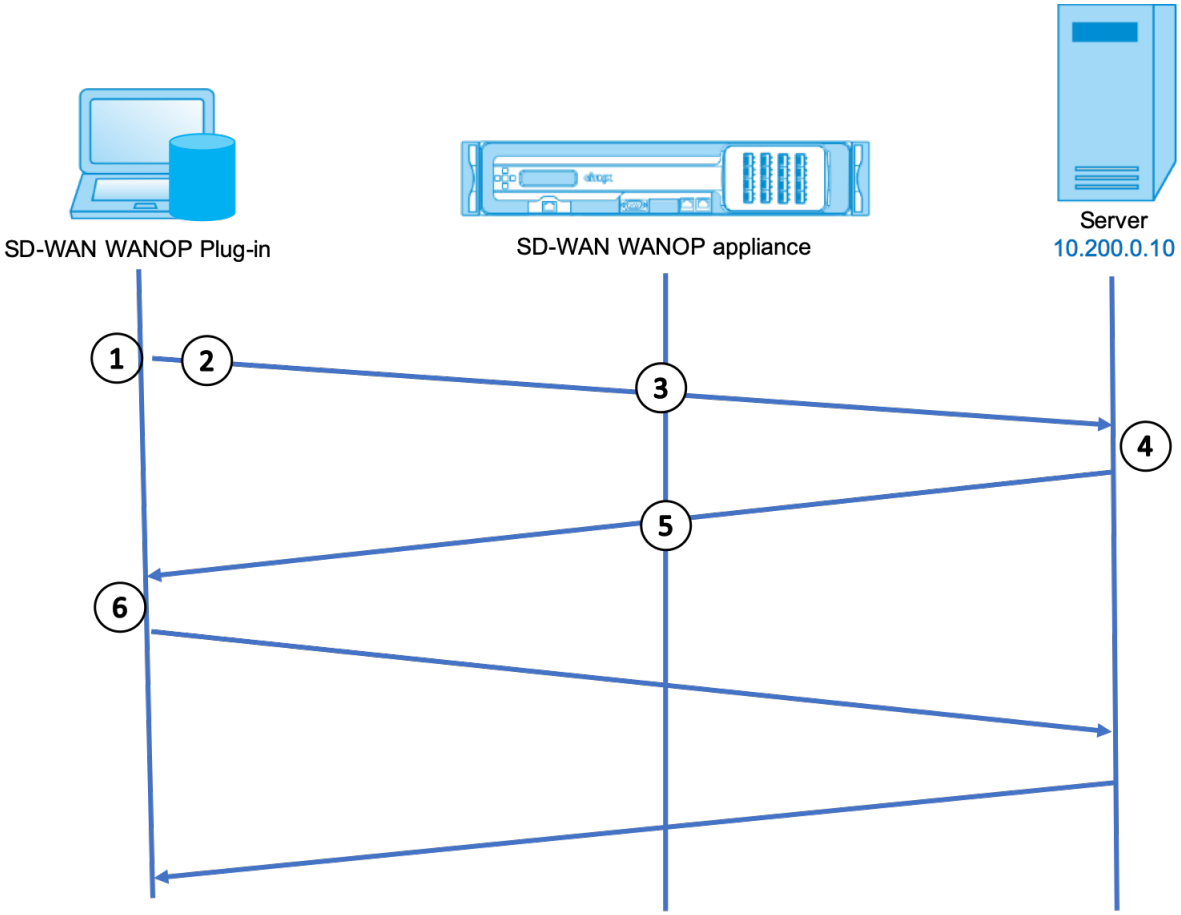
下图显示了重定向器模式的工作原理。

图 1. 重定向器模式



下图显示了 重定向器模式下的数据包流和地址映射。

图 2. 重定向器模式下的数据包流



1. 用户的应用程序打开到服务器的 TCP 连接，发送 TCP SYN 数据包。

   Src: 10.0.0.50, Dst: 10.200.0.10

2. Citrix SD-WAN WANOP 插件会查找目标地址，并决定将连接重定向到 10.200.0.201 的设备。

   Src: 10.0.0.50, Dst: 10.200.0.201

   (10.200.0.10 保留在 TCP 选项字段中。选项 24-31 用于各种参数。)

3. 设备接受连接并将数据包转发到服务器（使用 TCP 选项字段中的目标地址），然后将自己作为源。

   Src: 10.200.0.201, Dst: 10.200.0.10

4. 服务器接受连接并使用 TCP SYN-ACK 数据包进行响应。

   Src: 10.200.0.10, Dst: 10.200.0.201

5. 设备重写地址并将数据包转发到插件（将服务器地址置于选项字段中）。

   Src: 10.200.0.201, Dst: 10.0.0.50

6. 连接现已完全打开。客户端和服务器通过设备来回发送数据包。

   虽然地址在重定向器模式下分配，但去除端口号是 nit（尽管临时端口号可能是）。数据未封装。重定向器模式是一个代理，而不是一个隧道。

数据包之间没有 1:1 关系（尽管最终，接收的数据始终与发送的数据相同）。压缩可能会将多个输入数据包减少到单个数据包中。CIFS 荣誉将执行推测性的预读和白人后备操作。还, 如果应用程序和 Replter 插件之间丢弃数据包, 重新传输由设备处理, noyt 服务器, 使用先进的恢复算法.

插件如何选择设备

每个插件都配置了它可以联系以请求加速连接的设备列表。

每个设备都有 加速规则列表，该列表是设备可以建立加速连接的目标地址或端口的列表。插件从设备下载这些规则，并将每个连接的目标地址和端口与每个设备的规则集匹配。如果只有一台设备提供加速给定连接，则选择非常简单。如果多个设备提供加速连接，则插件必须选择其中一个设备。

设备选择的规则如下所示：

- 如果提供加速连接的所有设备都是重定向模式设备，则会选择插件的设备列表中最左侧的设备。（如果将设备指定为 DNS 地址，并且 DNS 记录具有多个 IP 地址，则这些地址也会从左到右扫描。）
- 如果提供加速连接的某些设备使用重定向器模式，而有些设备使用透明模式，则忽略透明模式设备，并从重定向器模式设备中进行选择。
- 如果提供加速连接的所有设备都使用透明模式，则插件不会选择特定的设备。* 它会启动 WANOP Client 插件 SYN 选项的连接，并且无论哪个候选设备将适当的选项附加到返回的 SYN-ACK 数据包中。这允许实际上与流量一致的设备标识到插件中的自身。但是，插件必须与响应设备具有开放的信号连接，否则不会发生加速。
- 某些配置信息被视为全局信息。此配置信息取自可以打开信令连接的列表中最左侧的设备。

部署用于插件的设备

April 23, 2021

客户端加速需要在 WANOP 客户端插件设备上进行特殊配置。其他注意事项包括设备放置。插件通常部署用于 VPN 连接。

尽可能使用专用设备

尝试将同一设备用于插件加速和链路加速通常很困难，因为这两种用途有时要求设备位于数据中心的不同点，而这两种用途可以调用不同的服务类规则。

此外，单个设备可以用作插件加速的端点节点或用作站点到站点加速的端点节点，但不能同时用于同一连接。因此，当您将设备用于 VPN 的插件加速和站点到站点加速到远程数据中心时，插件用户不会接收站点到站点加速。此问题的严重程度取决于插件用户使用的数据有多少来自远程站点。

最后，由于专用设备的资源不会在插件和站点到站点需求之间划分，因此它们可为每个插件用户提供更多的资源，从而提高性能。

尽可能使用内联模式

应将设备部署在与其支持的 VPN 单元相同的站点上。通常情况下，这两个单位是相互一致的。内联部署提供最简单的配置、最多的功能和最高的性能。为了获得最佳效果，设备应直接与 VPN 单元保持一致。

但是，设备可以使用除组模式或高可用性模式之外的任何部署模式。这些模式适用于设备到设备和客户端到设备加速。它们可以单独使用（透明模式）或与重定向器模式组合使用。

将设备置于网络的安全部分

设备依赖于您的现有安全基础结构，与服务器相同。它应该与服务器放置在防火墙（和 VPN 单元，如果使用）的同一侧。

避免 **NAT** 问题

插件端的网络地址转换 (NAT) 是透明处理的，不是一个问题。在设备方面，NAT 可能会很麻烦。应用以下准则以确保顺利部署：

- 将设备放在与服务器相同的地址空间中，以便用于访问服务器的任何地址修改也应用于设备。
- 切勿使用设备未与其自身关联的地址访问设备。
- 设备必须能够通过使用插件用户访问相同服务器的相同 IP 地址来访问服务器。
- 简而言之，请勿将 NAT 应用于服务器或设备的地址。

选择软提升模式

在配置设置：带宽管理页面上，选择 Softboost 模式。Softboost 是唯一支持 WANOP 客户端插件插件的加速类型。

定义插件加速规则

设备维护一个加速规则列表，用于告知客户端要加速哪些流量。每个规则都指定一个地址或子网以及设备可以加速的端口范围。

加速什么-加速什么流量的选择取决于设备的使用情况：

- VPN 加速器-如果设备被用作 VPN 加速器，所有 VPN 流量都通过设备，则无论目的地如何，所有 TCP 流量都应加速。

- 重定向器模式-与透明模式不同，处于重定向器模式的设备是显式代理，导致插件将其流量转发到重定向器模式设备，即使这样做是不可取的。如果客户端将流量转发到远离服务器的设备，特别是如果此“三角形路由”引入了缓慢或不可靠的链接，则加速可能会起反作用。因此，Citrix 建议将加速规则配置为允许给定设备仅加速其自己的站点。
- 其他用途-当插件既不用作 VPN 加速器，也不用于重定向器模式时，加速规则应包括远程用户和数据中心本地的地址。

在 配置：**WANOP** 客户端插件：加速规则选项卡上定义规则- 在设备上定义加速规则。

按顺序计算规则，并从第一个匹配规则执行操作（加速或排除）。要加速连接，它必须与加速规则匹配。

默认操作是不加速。

1. 在配置：WANOP 插件：加速规则选项卡上：
    - 为设备可以访问的每个本地 LAN 子网添加加速规则。也就是说，单击 添加”，选择“加 速”，然后键入子网 IP 地址和掩码。
    - 对设备本地的每个子网重复此操作。
2. 如果您需要排除包含范围的某些部分，请添加“排除”规则并将其移动到更常规的规则之上。例如，10.217.1.99 看起来像一个本地地址。如果它实际上是 VPN 单元的本地端点节点，请在 10.217.1.0/24 的加速规则上方的行上创建一个排除规则。
3. 如果要仅对单个端口（不推荐）使用加速，例如 HTTP 端口 80，请将“端口”字段中的通配符替换为特定端口号。您可以通过添加额外的规则（每个端口一个）来支持其他端口。
4. 一般来说，在一般规则之前列出狭窄的规则（通常是例外）。
5. 单击应用。如果您在应用更改之前离开此页面，则不会保存更改。

IP 端口使用情况

对于 IP 端口使用，请使用以下指南：

- 用于与 **WANOP** 客户端插件进行通信的端口—插件通过信令连接维护与设备的对话框，默认情况下，信令连接位于端口 443 (HTTPS) 上，这是通过大多数防火墙允许的。
- 用于与服务器通信的端口—WANOP 客户端插件插件与设备之间的通信使用的端口与客户端用于与服务器通信的端口相同（如果插件和设备不存在）。也就是说，当客户端在端口 80 上打开 HTTP 连接时，它会连接到端口 80 上的设备。设备依次与端口 80 上的服务器联系。

  在重定向器模式下，只保留已知端口（即 TCP SYN 数据包上的目标端口）。临时端口不会被保留。在透明模式下，保留两个端口。

  设备假定它可以在客户端请求的任何端口上与服务器通信，而客户端假定它可以在任何所需端口上与设备通信。如果设备遵守与服务器相同的防火墙规则，则此功能很好。在这种情况下，在直接连接中成功的任何连接都会在加速连接中成功。

TCP 选项使用和防火墙

WANOP 客户端插件参数在 TCP 选项中发送。TCP 选项可以出现在任何数据包中，并保证存在于建立连接的 SYN 和 SYN-ACK 数据包中。

防火墙不得阻止 24-31（十进制）范围内的 TCP 选项，否则无法进行加速。大多数防火墙不会阻止这些选项。但是，默认情况下，具有版本 7.x 固件的思科 PIX 或 ASA 防火墙可能会这样做，因此您可能需要调整其配置。

自定义插件的 **MSI** 文件

April 23, 2021

您可以更改
WANOP 客户端插件分发文件中的参数，该文件采用标准的 Microsoft 安装程序 (MSI) 格式。自定义需要使用 MSI 编辑器。

> 注意
>
> 已编辑过的参数中已更改。MSI 文件仅适用于新安装。当现有插件用户更新到新版本时，其现有设置将保留。因此，更改参数后，您应该建议用户在安装新版本之前卸载旧版本。

最佳做法：

创建解析到最近已启用插件的设备的 DNS 条目。例如，定义“Repeater.mycompany.com”，并将其解析为您的设备（如果您只有一个设备）。或者，假如您有五台设备，将 Repeater.mycompany.com 解析为您的五台设备中的一台，选择设备是根据靠近客户端或 VPN 单元的程度进行的。例如，使用与特定 VPN 关联的地址的客户端应看到 Repeater.mycompany.com 解析为连接到该 VPN 的 WANOP 客户端插件设备的 IP 地址。使用 MSI 编辑器（如 Oorca）将此地址构建到插件二进制文件中。添加、移动或删除设备时，更改 DNS 服务器上的此单个 DNS 定义会自动更新插件上的设备列表。

您也可以将 DNS 条目解析为多个设备，但除非所有设备的配置相同，否则这是不可取的，因为插件从列表中最左侧的设备获取其中一些特征，并在全局范围内应用它们（包括 SSL 压缩特征）。这可能会导致不希望的和令人困惑的结果，尤其是当 DNS 服务器为每个请求旋转 IP 地址的顺序时。

安装略卡 **MSI** 编辑器：

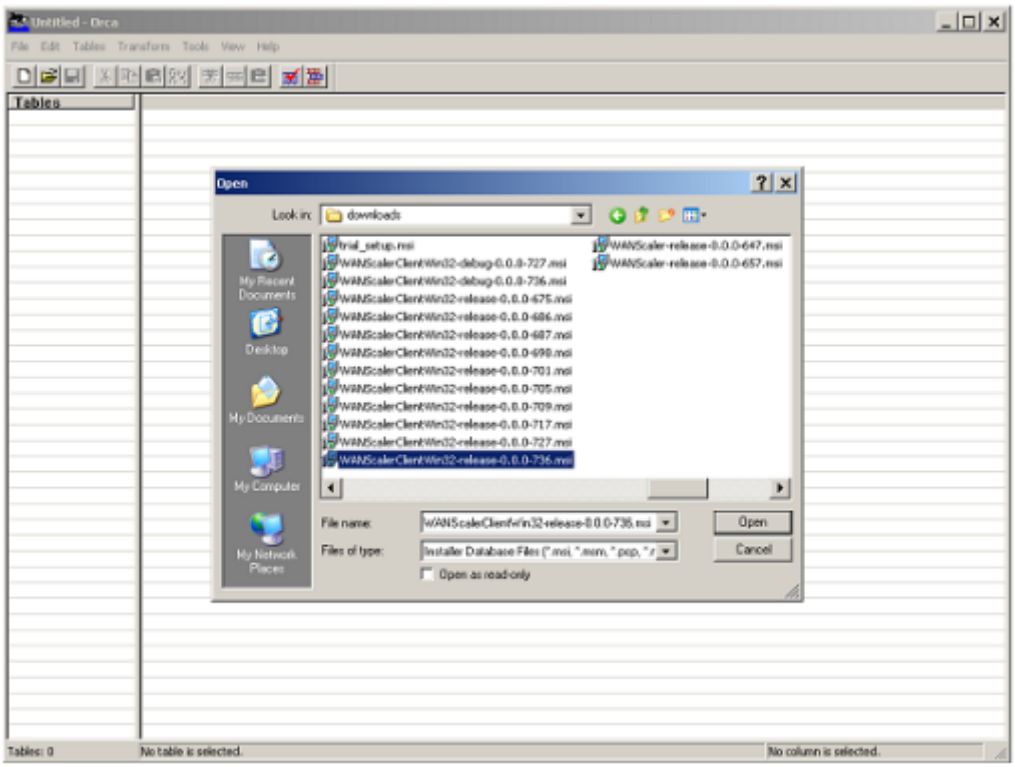
有许多 MSI 编辑器，包括 Oorca，它是微软免费平台 SDK 的一部分，可以从微软下载。

要安装 **Orca MSI** 编辑器，请执行以下操作：

1. 下载软件开发工具包的 PSDK-x86.exe 版本并执行它。按照安装说明进行操作。
2. 安装 SDK 后，必须安装 Orca 编辑器。它将在 Microsoft 平台 SDK\Bin\Orca.Msi 下进行。启动 Orca.msi 以安装实际的逆载鲸编辑器 (orca.exe)。
3. 运行逆载—微软提供其在线的逆载鲸文档。以下信息介绍了如何编辑最重要的 WANOP 客户端插件参数。

4. 启动逆载鲸与 开始 **>** 所有程序 **>** 逆载鲸。当出现空白的 Orca 窗口时，打开 WANOP 客户端插件 MSI 文件，其中包含“文 件” **>** “打开”。

   图 **1.** 使用奥卡岛



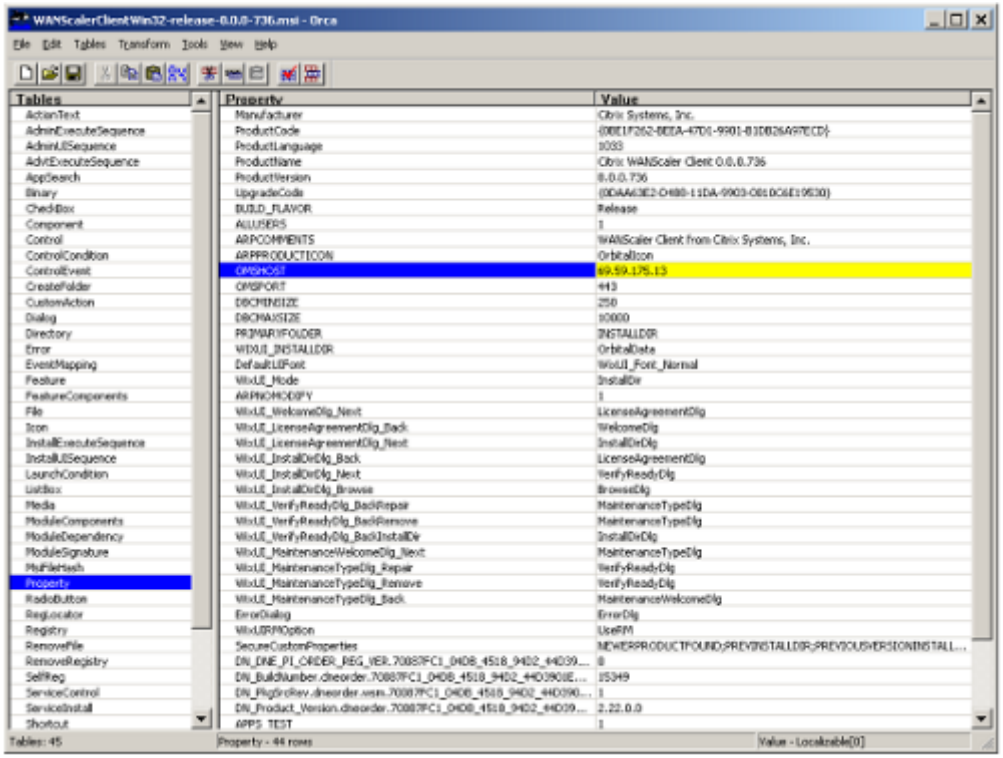
5. 在表菜单上，单击属性。此时将显示.MSI 文件的所有可编辑属性的列表。编辑下表中显示的参数。要编辑参数，请双击其值，键入新值，然后按 En **ter** 键。

   有关详细信息，请参阅 表。

   a) 在表菜单上，单击属性。此时将显示.MSI 文件的所有可编辑属性的列表。编辑下表中显示的参数。要编辑参数，请双击其值，键入新值，然后按 En **ter** 键。

      有关详细信息，请参阅 表。

      图 **2**：在 **Orca** 中编辑参数：



6. 完成后，使用 文件：另存为”命令以 新文件名保存已编辑的文件；例如 test.msi。

您的插件软件现已定制。

> 注意
>
> 一些用户在 orca 中看到一个错误，导致它将文件截断为 1 MB。检查保存的文件的大小。如果已截断，请创建原始文件的副本，然后使用“保存”命令覆盖原始文件。

使用 Orca 自定义设备列表并将自定义 MSI 文件分发给用户后，用户在安装软件时无需键入任何配置信息。

在 **Windows** 上部署插件

April 23, 2021

WANOP 客户端插件是一个可执行的 Microsoft 安装程序 (MSI) 文件，您可以下载和安装与任何其他 Web 分布式程序一样。从 Citrix.com Web 站点的 MyCitrix 部分获取此文件。

> 注意
>
> WANOP 客户端插件用户界面将自己称为“Citrix 加速插件管理器”。

插件所需的唯一用户配置是设备地址列表。此列表可以由逗号分隔的 IP 或 DNS 地址列表组成。这两种形式可以混合。

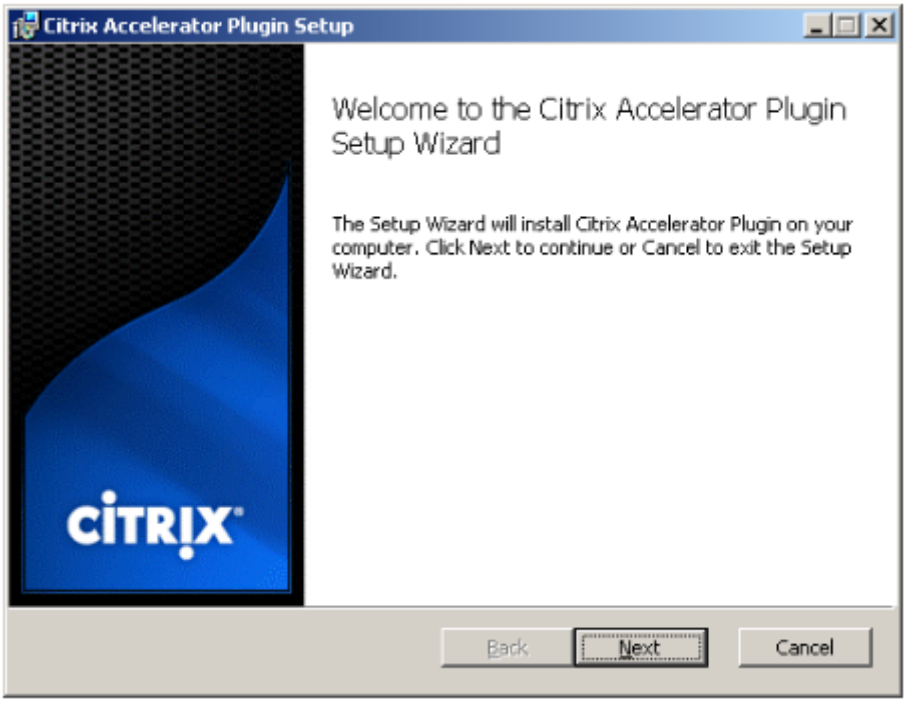
您可以自定义分发文件，以便默认情况下列表指向您的设备。安装后，操作是透明的。通过适当的设备发送到加速子网的流量，并将所有其他流量直接发送到服务器。用户应用程序不知道任何这种情况正在发生。

安装

要在 Windows 系统上安装 WANOP 客户端插件插件加速器，请执行以下操作：

1. Repeater*.msi 文件是一个安装文件。关闭所有应用程序和可能打开的任何窗口，然后按常规方式启动安装程序（在文件窗口中双击，或使用 run 命令）。

   图 **1.** 初始安装屏幕：

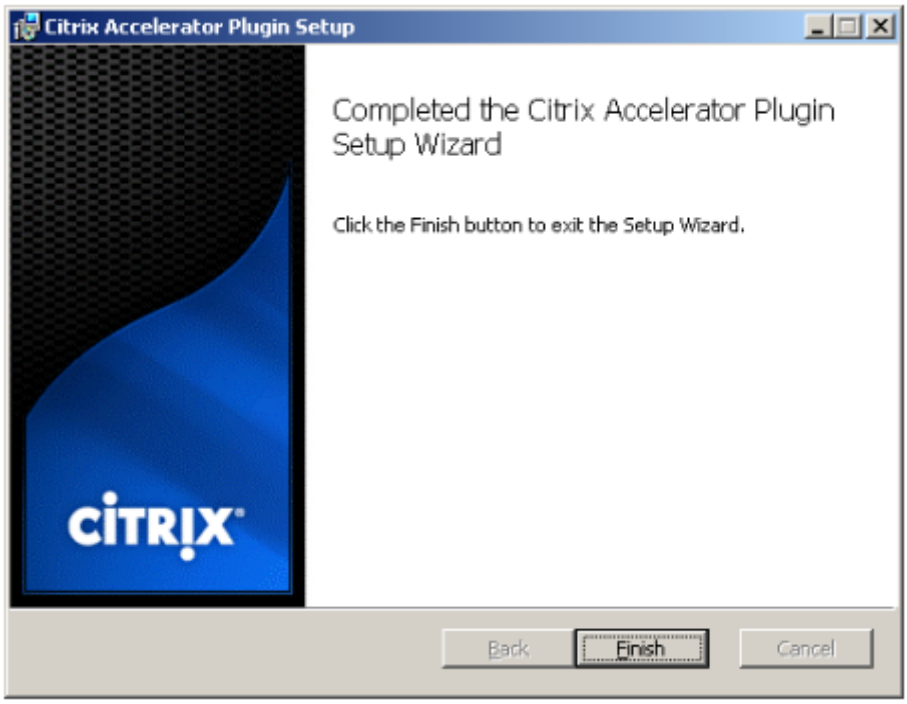
   以下步骤适用于交互式安装。可以使用以下命令执行静默安装：

   客户端 *_msi_* 文件*/qn*

2. 安装程序会提示输入安装软件的位置。您指定的目录用于客户端软件和基于磁盘的压缩历史记录。它们总共需要最低 500 MB 的磁盘空间。

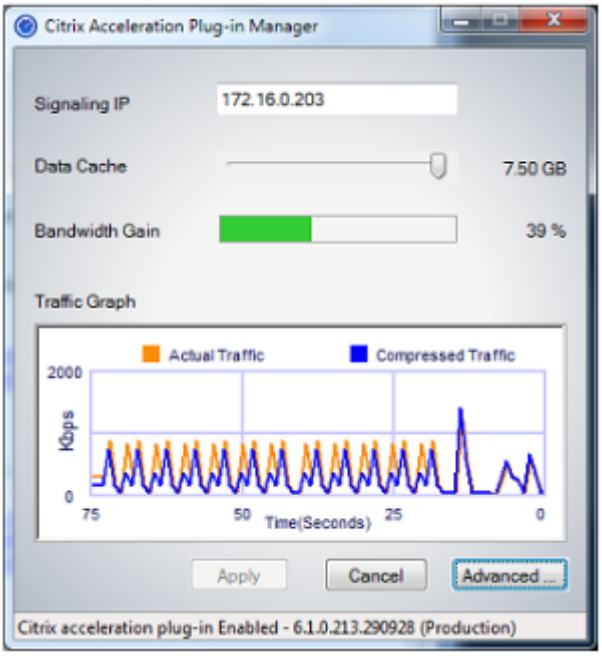
3. 安装程序完成后，它可能会要求您重新启动系统。重新启动后，WANOP 客户端插件插件将自动启动。

   图 **2.** 最终安装屏幕：



4. 右键单击任务栏中的加速器图标，然后选择 管理加速 以启动 Citrix 插件加速器管理器。

图 **3. Citrix** 加速器插件管理器，初始（基本）显示：



5. 如果尚未为用户自定义.MSI 文件，请指定信令地址和用于压缩的磁盘空间量：

   - 在设备：信令地址字段中，键入设备的信令 IP 地址。如果您有多个启用了插件的设备，请将它们全部列出，并以逗号分隔。IP 地址或 DNS 地址均可接受。

- 使用“数据缓存”滑块，选择用于压缩的磁盘空间量。更多更好。7.5 GB 是不是太多，如果你有那么多的磁盘空间可用。
- 按“应用”。

WANOP 客户端插件加速器现在正在运行。未来与加速子网的所有连接都将加速

在插件的“高级规则”选项卡上，“加速规则”列表应将每个设备显示为“已连接”，并将每个设备的加速子网显示为“已加速”。如果没有，请检查信令地址 IP 字段和一般网络连接。

插件故障排除

插件安装通常顺利。如果没有，请检查以下问题：

常见问题：

- 如果您不重新启动系统，WANOP 客户端插件将无法正常运行。
- 如果磁盘碎片过多，会导致压缩性能低下。
- 加速失败（诊断 选项卡上未列出加速连接）通常表示某些事情阻止了与设备的通信。检查插件上的 配置：加速规则 列表，以确保已成功联系设备，并且目标地址包含在其中一个加速规则中。连接故障的典型原因包括：
  - 设备未运行，或者加速已禁用。
  - 防火墙正在剥离插件和设备之间的某个时候剥离 WANOP 客户端插件 TCP 选项。
  - 该插件正在使用不受支持的 VPN。

确定性网络增强器锁定错误

在极少数情况下，安装插件并重新启动计算机后，将出现两次以下错误消息：

确定性的网络增强器安装需要首先重新启动，以释放锁定的资源。请在重新启动计算机后再次运行此安装。

如果发生上述情况，请执行以下操作：

1. 转到 添加/删除程序 并删除 WANOP 客户端插件（如果存在）。
2. 转到 控制面板 > 网络适配器 > 局域连接 > 属性，找到确定性网络增强器的条目，清除其复选框，然后单 击 确定。（您的网络适配器可能由“本地连接”以外的名称调用。）
3. 打开命令窗口并转到 c:windowsinf（或者如果您在非标准位置安装了 Windows，则该等效目录）。
4. 键入以下命令：

   find “dne2000.cat” oem*.inf

5. 找到返回匹配行的 highest-numbered oem*.inf 文件（匹配行是为 CatalogFile= dne2000.cat）并对其进行编辑。例如：

   notepad oem13.inf

6. 删除除顶部以分号开头的三行之外的所有内容，然后保存文件。这将清除任何不适当或过时的设置，下次安装将使用默认值。
7. 重试安装。

其他安装问题

安装 WANOP 客户端插件时出现的任何问题通常都是由于现有网络、防火墙或防病毒软件干扰安装。通常，一旦安装完成，就没有进一步的问题。

如果安装失败，请尝试以下步骤：

1. 确保插件安装文件已复制到本地系统。
2. 断开任何活动的 VPN/远程网络客户端。
3. 暂时禁用任何防火墙和防病毒软件。
4. 如果其中一些是困难的，做你可以。
5. 重新安装 WANOP 客户端插件。
6. 如果这不起作用，请重新启动系统并重试。

Citrix SD-WAN WANOP 插件 GUI

April 23, 2021

右键单击 **Citrix** 加速器插件图标并选择 管理 加速时，将显示 WANOP 客户端插件 GUI。首先显示 GUI 的基本显示。还有一个高级显示器，可以根据需要使用。

基本显示器

在“基本”页面上，您可以设置两个参数：

- “信令地址”字段指定插件可连接到的每个设备的 IP 地址。Citrix 建议仅列出一个设备，但您可以创建逗号分隔的列表。这是一个有序列表，最左侧的设备优先于其他设备。尝试使用可以建立信号连接的最左侧设备加速。您可以同时使用 DNS 地址和 IP 地址。

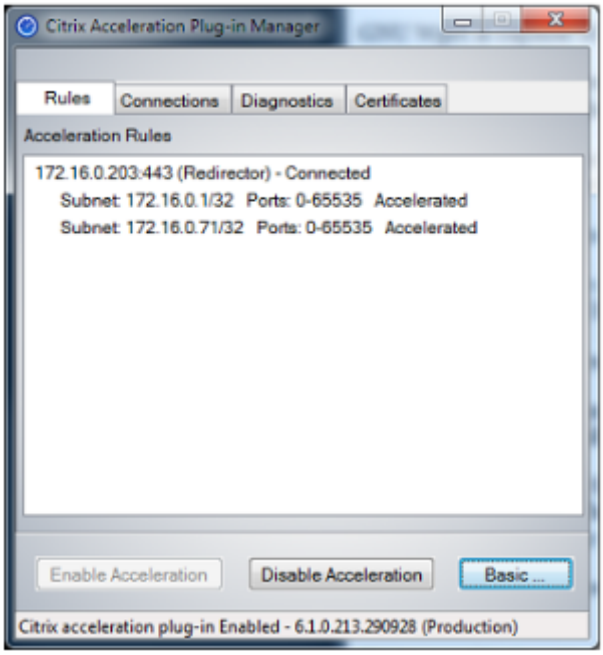
  示例：10.200.33.200、ws.mycompany.com、ws2.mycompany.com

- “数据缓存”滑块可调整分配给插件基于磁盘的压缩历史记录的磁盘空间量。更多更好。

此外，还有一个按钮移动到高级显示屏。

高级显示器

“高级”页面包含四个选项卡：规则、连接、诊断和证书。



显示屏底部有按钮，用于启用加速、禁用加速和返回到基本页面。

规则选项卡

“规则”选项卡显示从设备下载的加速规则的缩写列表。每个列表项显示设备的信令地址和端口、加速模式（重定向器或透明）和连接状态，后面是设备规则摘要。

连接选项卡

连接 选项卡列出了不同类型的打开连接的数量：

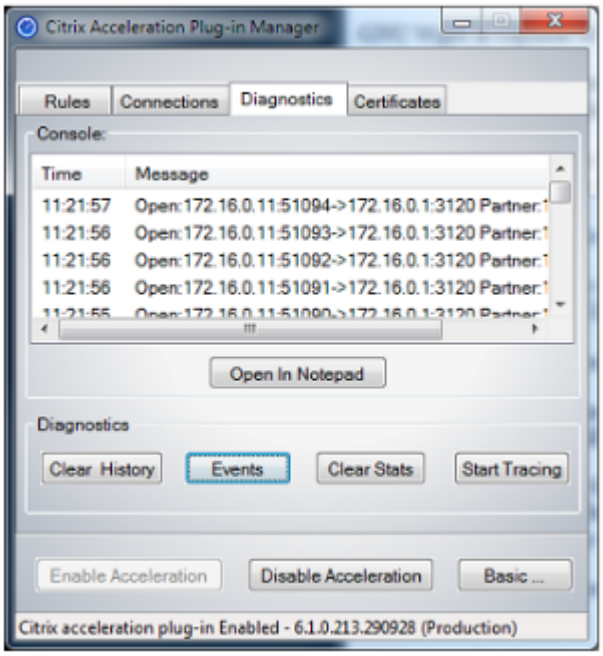
- 加速连接—WANOP 客户端插件插件与设备之间的打开连接数。此数字包括每个设备的一个信令连接，但不包括加速 CIFS 连接。单击“更多”将打开一个窗口，其中包含每个连接的简要摘要。（所有“更多”按钮允许您将窗口中的信息复制到剪贴板，如果您想与支持部门共享。）
- 加速 **CIFS** 连接—与 CIFS（Windows 文件系统）服务器的打开、加速连接的数量。这通常与挂载的网络文件系统的数量相同。单击“更多”将显示与加速连接相同的信息，以及在使用 WANOP 客户端插件的特殊 CIFS 优化运行 CIFS 连接时报告活动状态字段。

- 加速的 **MAPI** 连接 - 打开的加速 Outlook/Exchange 连接的数量。
- 加速 **ICA** 连接—使用 ICA 或 CGP 协议的打开、加速 Citrix Virtual Apps and Desktops 连接的数量。
- 未加速连接—打开未加速的连接。您可以单击“更多”以显示连接未加速的简要说明。通常情况下，原因是没有任何设备会加速目标地址，该地址作为服务策略规则报告。
- 打开/关闭连接—未完全打开但正在打开或关闭的连接（TCP “半打开”或“半关闭”连接）。“更多”按钮显示有关这些连接的一些附加信息。

诊断选项卡

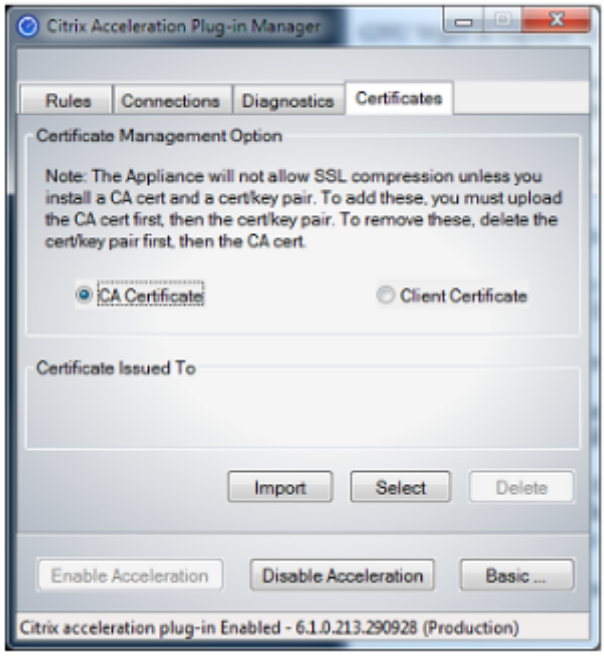
“诊断”页面报告不同类别中的连接数以及其他有用信息。

- 开始跟踪/停止跟踪—如果您报告问题，Citrix 代表可能会要求您执行连接跟踪以帮助确定问题。此按钮启动和停止追踪。停止跟踪时，弹出窗口会显示跟踪文件。按照您的 Citrix 代表推荐的方式将其发送给他或她。
- 清除历史记录-不应使用此功能。
- 清除统计信息—按此按钮可清除“性能”选项卡上的统计信息。
- 控制台-带有最近状态消息的可滚动窗口，主要是连接打开和连接关闭消息，但也有错误消息和其他状态消息。



证书选项卡

在“证书”选项卡上，您可以为可选的安全对等功能安装安全凭据。这些安全证书的目的是使设备能够验证插件是否是受信任的客户端。



要上载 CA 证书和证书密钥对，请执行以下操作：

1. 选择 CA 证书管理。
2. 单击导入。
3. 上载 CA 证书。证书文件必须使用支持的文件类型之一（.pem、.crt、.cer 或.spc）。可能会出现一个对话框，要求您选择要使用的证书存储区并向您显示关键字列表。选择列表中的第一个关键字。
4. 选择 客户端证书管理。
5. 单击导入。
6. 选择证书密钥对的格式（PKCS12 或 PEM/DER）。
7. 单击 **Submit**（提交）。

> 注意
>
> 对于 PEM/DER，证书和密钥有单独的上载框。如果您的证书密钥对合并在一个文件中，请为每个框指定两次文件。

更新 **Citrix SD-WAN WANOP** 插件

April 23, 2021

要安装更新版本的 WANOP 客户端插件，请按照首次安装插件时使用的相同步骤操作。

卸载 **WANOP** 客户端插件

要卸载 WANOP 客户端插件，请使用 Windows 添加/删除程序实用程序。WANOP 客户端插件在当前安装的程序列表中列为 **Citrix** 加速插件。选择它并单击 删除。

重新启动系统以完成客户端的卸载。

Citrix Virtual Apps and Desktops 加速

April 23, 2021

> 注意
>
> 在本次讨论中，*Virtual Apps* 是指 ICA 和 CGP 协议流。因此，关于 Virtual Apps 的说法也适用于 Virtual Desktops。

Virtual Apps/Virtual Desktops (ICA/CGP) 加速包括三个组成部分：

- 压缩—设备与虚拟应用程序客户端和服务器合作，压缩虚拟应用程序数据流以获取交互式数据（键盘/鼠标/显示器/音频）和批处理数据（打印和文件传输）。此交互以透明方式进行，无需配置设备。较旧的虚拟应用程序服务器（4.x 版）需要进行少量配置，如下所述。
- 多流 **ICA**—除了压缩外，Citrix SD-WAN WANOP 设备还支持新的多流 ICA 协议，其中多达四个连接用于不同 ICA 优先级，而不是将同一连接上的所有优先级复用。这种方法为交互式任务提供了更大的响应能力，尤其是当与设备的流量成形结合使用时。
- 流量调整—Citrix SD-WAN WANOP 流量塑形器使用虚拟应用程序数据协议中的优先级位实时调整连接的优先级，将每个连接的带宽份额与连接当前传输的内容相匹配。

  > 注意
  >
  > 默认情况下，多流 ICA 处于禁用状态。它可以在功能页面上启用。多流 ICA 和 AutoQoS 需要启用会话可靠性。

为了优化 Citrix Virtual Apps and Desktops 7.0 及更高版本的 ICA 连接，Citrix SD-WAN WANOP 设备支持 Citrix Receiver for Chrome 1.4 及更高版本，以及适用于 HTML5 版本 1.4 及更高版本的 Citrix Receiver。

HDX 从 **UDP/EDT** 到 **TCP** 的传输协议—在某些网络条件下，UDP/EDT 不能用作交付 HDX 流量的优化协议。您可以将协议更改为 TCP，以便 WANOP 可以 提供：

- 压缩/DDup 优势
- 可见性（本地报告和 HDX Insight）

WANOP 可以阻止 EDT 流量并强制将会话强制到 TCP。在会话启动期间，Citrix Receiver 在 TCP 和 EDT 上启动会话。如果未建立 EDT 会话，则使用 TCP 会话。WANOP GUI 提供了一个选项来强制在 TCP 协议上的会话在功能页面上。

配置虚拟应用程序加速

April 23, 2021

虚拟应用程序加速适用于虚拟应用程序中的 ICA 和 CGP 协议。Citrix SD-WAN WANOP 设备、虚拟应用程序服务器和虚拟应用程序客户端可协作加速虚拟应用程序连接，与虚拟应用程序相比，提供了显著的加速。这种合作需要所有三个组成部分的最新版本。

虚拟应用程序压缩可在交互式通道（例如鼠标、键盘和屏幕数据）的基于内存的压缩与批量任务（例如文件传输和打印作业）的基于磁盘的压缩之间动态切换。压缩比随着压缩历史记录的填充而增加，从而增加可与新数据匹配的数据量。虚拟应用程序压缩提供的数据缩减量是无辅助虚拟应用的几倍，在重复性批量传输（例如打印或保存同一文档的连续版本）时，通常超过 50:1。

Virtual Apps 压缩可防止用户互相干扰，从而实现高链路利用率而不会出现拥塞。

启用虚拟应用程序加速

1. 检查 ICA 服务类策略。在“配置：服务类”页面上，ICA 服务类应在“加速”列中显示磁盘，并在“流量调整”列中显示 ICA 优先级。如果不是，请编辑服务类定义。
2. 更新虚拟应用程序 4.x 服务器和客户端。（虚拟应用程序 5.0 或更高版本不需要）。使用 Presentation Server 4.5 与修补程序汇总包 PSE450W2K3R03（测试版）或更高版本。此版本包括以下服务器和客户端软件，必须安装这两个软件才能进行虚拟应用程序压缩：
   a) 服务器软件包 PSE450R03W2K3WS.msp 或更高版本。
   b) 客户端版本 11.0.0.5357 或更高版本。
3. 将虚拟桌面服务器和客户端更新为 4.0 或更高版本。
4. 验证虚拟应用服务器注册表设置（虚拟应用程序 5.0 或更高版本不需要。）在 Virtual Apps 服务器上，验证以下设置并根据需要更正或创建它们：

   ```
   pre codeblock HKLM\System\CurrentControlSet\Control\Citrix\
   WanScaler\EnableForSecureIca = 1 HKLM\System\CurrentControlSet
   \Control\Citrix\WanScaler\EnableWanScalerOptimization = 1 HKLM\
   System\CurrentControlSet\Control\Citrix\WanScaler\UchBehavior = 2
    <!--NeedCopy-->
   ```

   它们均为 DWORD 值。
5. 打开和使用通过更新的 Citrix SD-WAN WANOP 的已更新的虚拟应用程序客户端和服务器之间的虚拟应用程序连接。默认情况下，这些会话使用 CGP。对于 ICA，在客户端上的 Citrix 程序邻域下，清除“自定义 ICA 连接”复选框。然后，右键单击连接图标，导航到 属性 > 选项，然后单击 启用会话可靠 性”复选框。多流 ICA 和 AutoQoS 需要启用会话可靠性。

6. 验证加速。

   通过加速链接启动虚拟应用程序会话后，加速 ICA 连接应显示在设备的“监控：连接”页面上。压缩比大于 1:1 表示正在进行压缩。

优化 Citrix Receiver for HTML5

December 15, 2022

必须在 HTML5 WebSocket 上提供动态内容工作的应用程序。Citrix Receiver for Chrome 和 Citrix Receiver for HTML5 是支持 HTML5 WebSocket 的应用程序。这些应用程序简化了对虚拟桌面的访问，因为它们可以与支持 HTML5 WebSockets 的最新 Web 浏览器集成在一起。

> 注意
>
> 您无需对设备配置进行任何更改即可使用此功能。

Citrix SD-WAN WANOP 设备如何优化 Citrix Receiver for HTML5

在典型的分支办公室和数据中心设置中，虚拟桌面代理 (VDA) 之类的共享资源安装在数据中心的 Citrix Hypervisor 服务器上。来自分支机构的客户端通过使用 Citrix Receiver 通过网络访问这些共享资源。

在典型的分支办公室和数据中心设置中，虚拟桌面代理 (VDA) 之类的共享资源安装在数据中心的 Citrix Hypervisor 服务器上。来自分支机构的客户端通过使用 Citrix Receiver 通过网络访问这些共享资源。

由于符合 HTML 要求，VDA 使用在端口 8008 上运行的 WebSocket 侦听器。访问应用程序时，客户端在端口 8008 上启动 TCP 连接，并使用它向服务器发送 HTTP 请求以升级连接并使用 WebSocket 协议。客户端与 VDA 协商 WebSocket 连接后，开始独立计算架构 (ICA) 协商，客户端和服务器通过 HTML5 使用 ICA 来交换数据。有关客户端和服务器之间交换的邮件顺序的详细信息，请参阅客户端和服务器之间交换的邮件。

在客户端和服务器之间建立连接后，Citrix SD-WAN WANOP 设备通过加快网络流量，并使用 Citrix Receiver for HTML5 加速网页和其他应用程序，从而开始优化连接。优化 Citrix Receiver for HTML5 的功能类似于 HTTP 加速。

> 注意
>
> - 有关 HTML5 的更多信息，请参阅HTML5 的工作原理。
> - 有关 Citrix Receiver for HTML5 的详细信息，请参阅Receiver for HTML5。
> - 有关 Receiver for HTML5 的系统要求的详细信息，请参阅 系统要求。

配置 **Citrix SD-WAN WANOP** 设备以优化 **Citrix Receiver for HTML5**

Citrix Receiver for HTML5 连接的优化为零配置功能。您不必对设备进行任何配置更改。将 Citrix SD-WAN WANOP 软件升级到 CB 7.3.1 或更高版本时，会在设备上创建 alt-http 应用程序分类器，并将此应用程序分类器映射到端口 8008，该端口是虚拟桌面的默认设置。只要升级软件设备，它就可以优化使用 Citrix Receiver for HTML5 的本机 Chrome 连接。

如果通过 Citrix Receiver for HTML5 的连接使用 SSL 加密，则连接通过 SSL 使用 ICA。要使用 Citrix Receiver for HTML5 启用通过 SSL 加速的 ICA，您需要配置标准 SSL 加速，其中包括服务类和 SSL 配置文件映射中的适当目标 IP 地址。如果您计划以 ICA 代理模式部署设备，则必须将 StoreFront VIP 地址映射到 StoreFront 证书。同样，如果计划以任何端到端 SSL 加密部署模式部署设备，则必须将 VDA IP 地址映射到 VDA 证书。

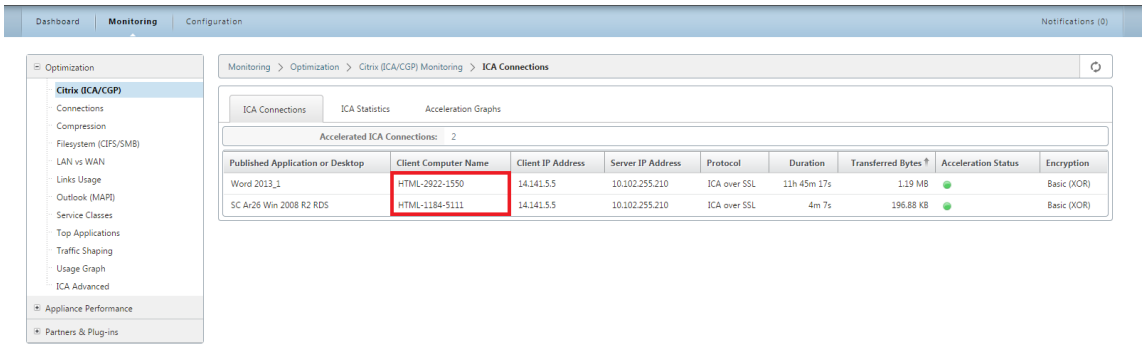
> 警告
>
> 请确保不要将 alt-http 应用程序的端口号更改为任何其他端口号。如果删除此应用程序分类器或需要对其进行任何更改，则必须将端口 8008 添加到 HTTP 应用程序分类器中。

验证 **Citrix Receiver for HTML5** 连接

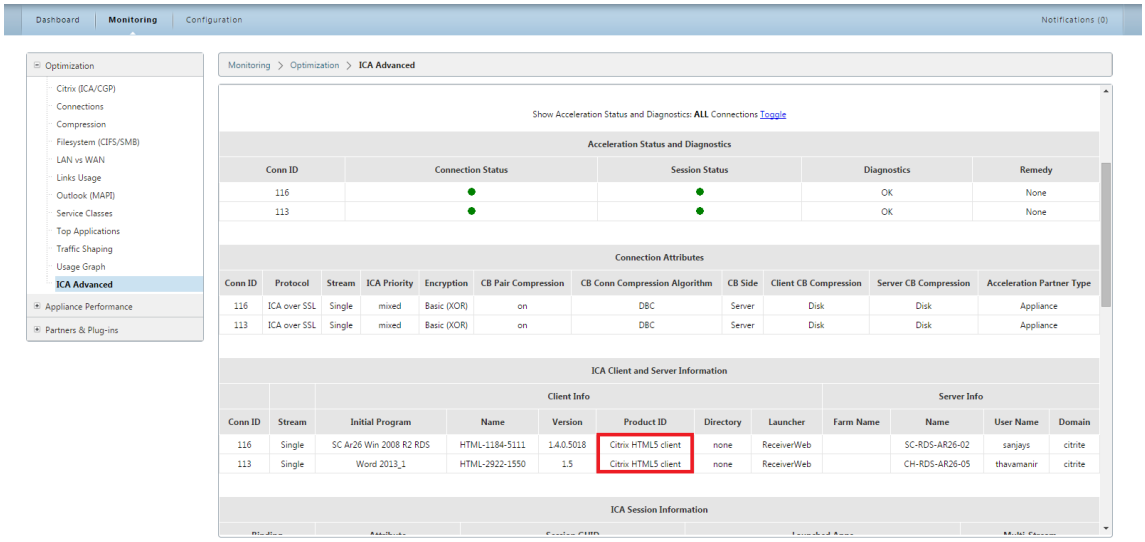
要验证设备是否优化 Citrix Receiver for HTML5 连接，您可以检查连接是否列在 Citrix (ICA/CGP) 和 ICA 高级监视页面中。监视页面中是否存在 HTML5 连接表明设备正在优化 Citrix Receiver for HTML5。

要验证 **Citrix SD-WAN WANOP** 设备上的 **Citrix Receiver for HTML5** 连接，请执行以下操作：

1. 导航到 监视 > 优化 > **Citrix (ICA/CGP)** 页面。
2. 在 **ICA** 连接 选项卡上，验证是否列出了 HTML5 连接。在“客户端计算机名称”列中以 HTML 作为前缀显示 HTML5 连接，如以下屏幕截图所示：



3. 导航到 “监视” **>** “优化” **>** “**ICA** 高级 页面。
4. 在 **Conn** 信息 选项卡中，向下滚动到 ICA 客户端和服务器信息部分。HTML5 连接的条目在“产品 ID”列中具有 Citrix HTML5 客户端，如以下屏幕截图所示：

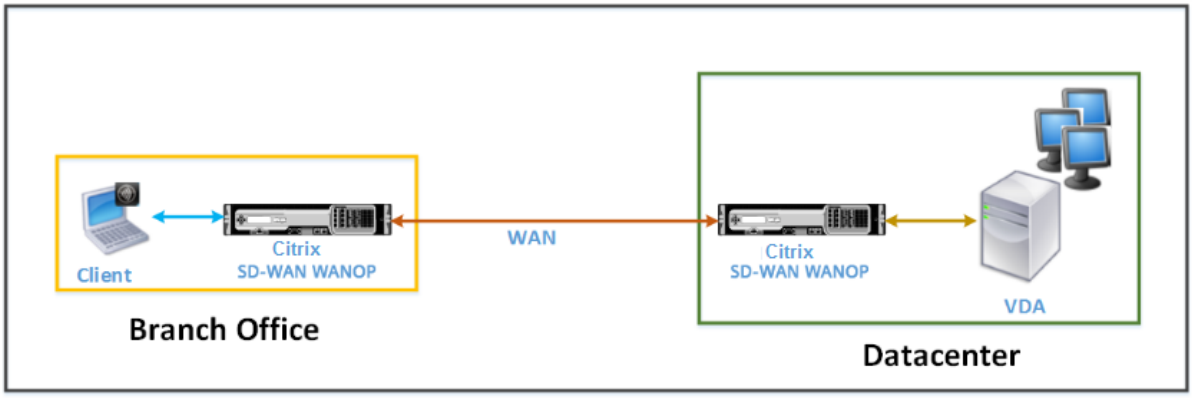


部署模式

April 23, 2021

在典型的 Citrix SD-WAN WANOP 部署中，Citrix SD-WANOP 设备在分支机构和数据中心之间进行配对。您可以在数据中心中安装共享资源（如 VDA）。来自各分支机构的客户端使用 Citrix Receiver 访问数据中心资源，如下图所示。

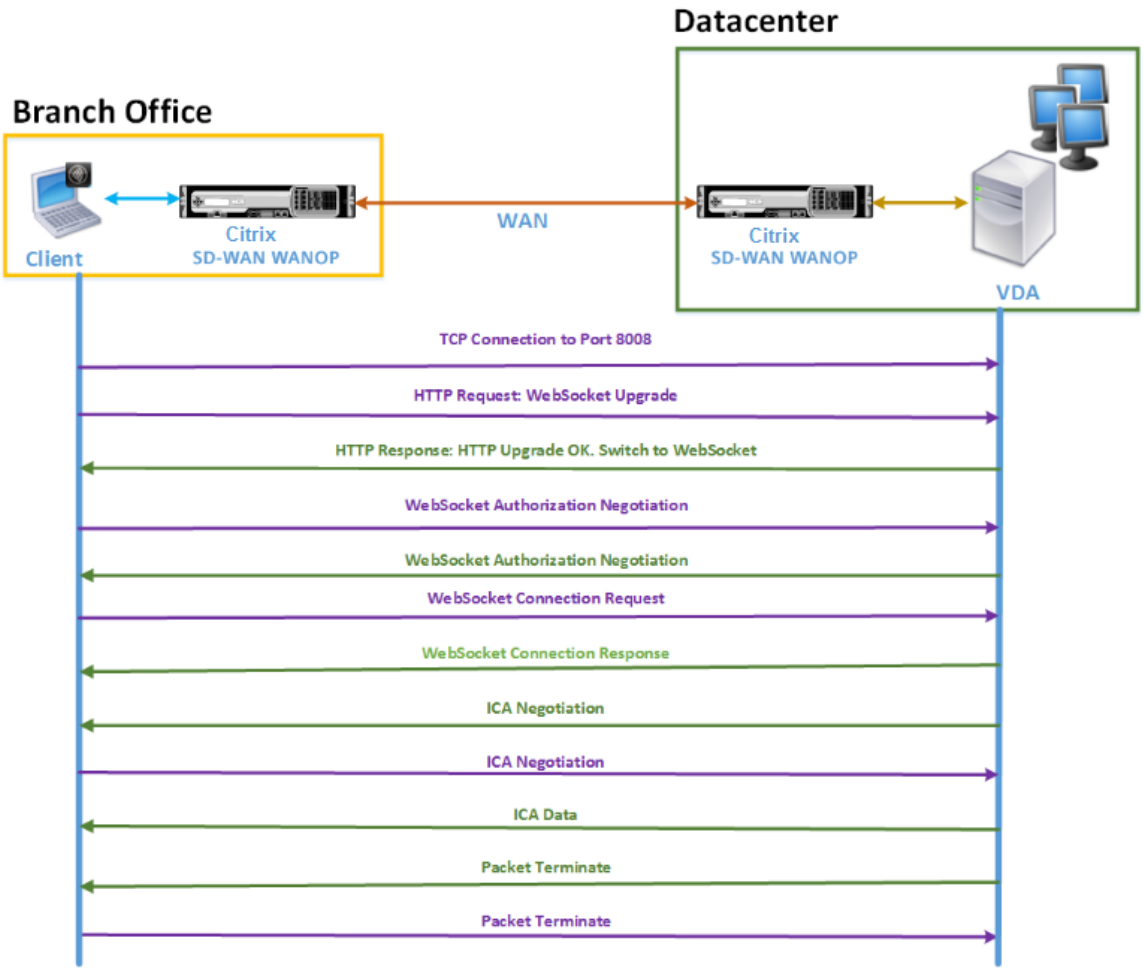
典型的 Citrix SD-WAN WANOP 部署拓扑



客户端在其本地计算机上安装 Citrix Receiver 软件产品，如 Citrix Receiver for HTML5，并使用该产品访问数据中心中的资源。通过 Citrix SD-WAN WANOP 设备对连接进行了优化。

了解客户端和服务器之间交换的消息

与任何类型的网络连接一样，使用 Citrix Receiver for HTML5 的客户端与服务器交换各种消息。下图显示了在客户端和服务器之间建立连接时，客户端和服务器之间的典型消息流。



如上图所示，当分支机构的客户端想要访问数据中心服务器资源时，客户端和服务器之间交换以下消息序列：

1. 客户端使用 Citrix Receiver for HTML5 向端口 8008 上的 VDA 发送 TCP 连接请求。
2. 建立 TCP 连接后，客户端会向 VDA 发送 WebSocket 升级请求。
3. VDA 响应升级请求并切换到 WebSocket 协议。
4. 客户端和 VDA 协商 WebSocket 授权。
5. 客户端向 VDA 发送 WebSocket 连接请求。
6. VDA 响应 WebSocket 连接请求。
7. VDA 启动与客户端的 ICA 协商。
8. ICA 协商后，VDA 开始传输 ICA 数据。

9. VDA 发送数据包终止消息。
10. 客户端使用数据包终止消息进行响应。

> 注意
>
> 上面的示例列出了通过 WebSocket 为 ICA 交换的示例消息。如果您通过公共网关协议 (CGP) 使用 ICA，则客户端和服务器协商 CGP 而不是 WebSocket。但是，对于 ICA 通过 TCP，客户端和服务器协商 ICA。

根据您在网络上部署的组件，连接将在不同的点终止。上图表示的是在网络上没有部署任何其他组件的拓扑。因此，客户端在端口 8008 上直接与 VDA 通信。但是，如果您已在数据中心安装 Gateway 关（如 Citrix Gateway），则与网关建立连接，并代理 VDA。在 Gateway 关协商 WebSocket 授权之前，不会与 VDA 进行通信。Gateway 关协商 WebSocket 授权后，它将打开与 VDA 的连接。此后，Gateway 关充当中间人，并将消息从客户端传递到 VDA，反之亦然。

同样，如果在客户端上安装的 Citrix Gateway 插件与数据中心安装的 Citrix 网关之间创建 VPN 隧道，则网关在建立 TCP 连接后立即透明地将所有客户端消息转发到 VDA，反之亦然。

> 注意
>
> 要优化需要端到端 SSL 加密的连接，需要在 VDA 上的端口 443 上建立 TCP 连接。

支持的部署模式

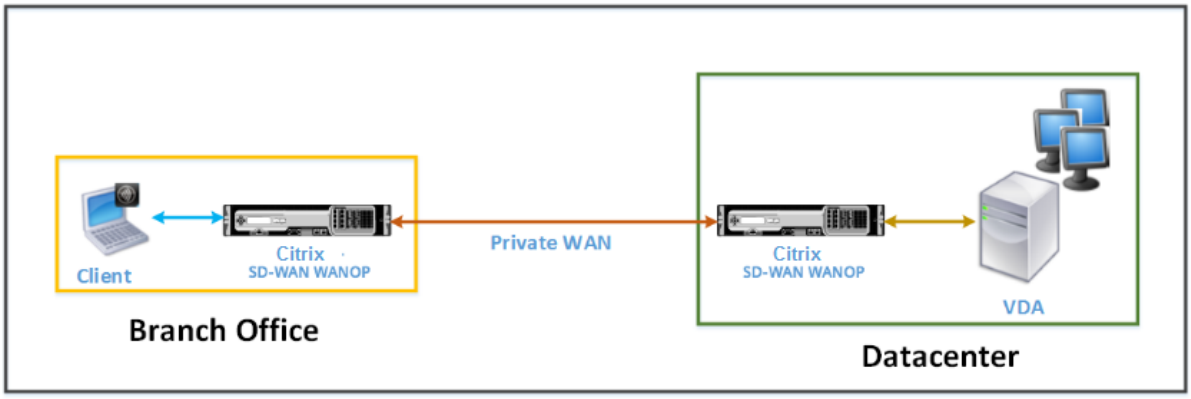
配置 Citrix SD-WAN WANOP 设备以优化 Citrix Receiver for HTML5 时，您可以根据您的网络要求考虑以下任何部署模式。要优化 Citrix Receiver for HTML5，Citrix SD-WAN WANOP 设备支持以下部署模式：

- 直接访问
- 通过端到端 SSL 加密直接访问
- ICA 代理模式
- 采用端到端 SSL 加密的 ICA 代理模式
- 完整的虚拟专用网络 (VPN) 模式
- 具有端到端 SSL 加密功能的完整虚拟专用网络 (VPN) 模式

直接访问：

下图显示了在直接访问模式下安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

在直接访问模式下部署的 Citrix SD-WAN WANOP 设备



在直接访问模式下，在分支机构和数据中心以内联模式安装了一对 Citrix SD-WAN WANOP 设备。客户端通过专用 WAN 通过 Citrix Receiver for HTML5 访问 VDA 资源。通过在 ICA 级别使用加密来保护从客户端到 VDA 资源的连接。在“了解客户端与服务器之间交换的消息”中解释了客户端与 VDA 之间交换的消息。

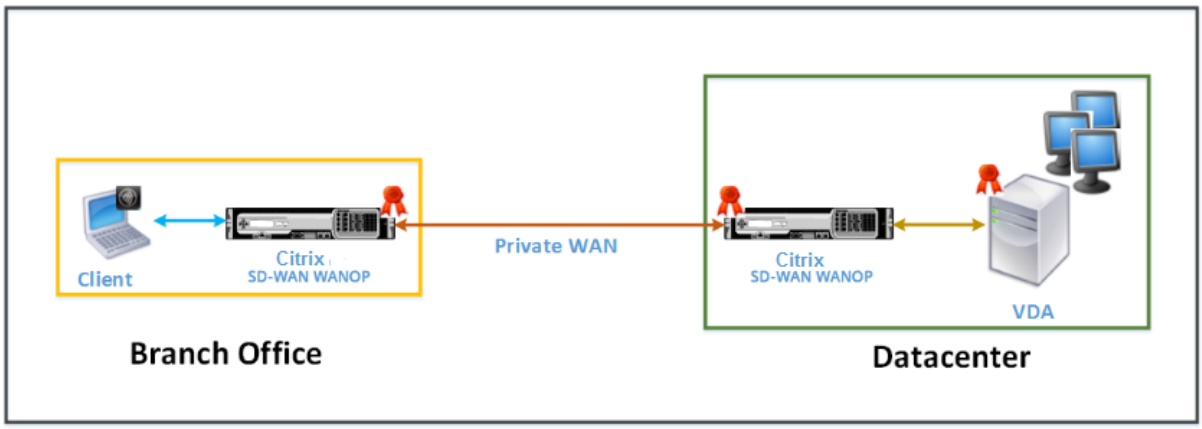
安装在客户端与 VDA 数据中心之间的 Citrix SD-WAN WANOP 设备可优化在它们之间建立的 Citrix Receiver for HTML5 连接。

直接访问部署适用于客户端在无需使用 Citrix Gateway 或任何其他防火墙的情况下连接的企业 Intranet。在内联模式下部署 Citrix SD-WAN WANOP 设备并且专用 WAN 中的客户端连接到 VDA 资源时，您可以通过直接访问部署设置。

通过端到端 **SSL** 加密直接访问：

下图显示了以端到端 SSL 加密保护的直接访问模式安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

以直接访问模式部署的 Citrix SD-WAN WANOP 设备，采用端到端 SSL 加密保护



使用端到端 SSL 加密模式的直接访问与直接访问模式类似，不同之处在于客户端与 VDA 资源之间的连接受 SSL 加密保护，并使用端口 443 而不是端口 8008 进行连接。

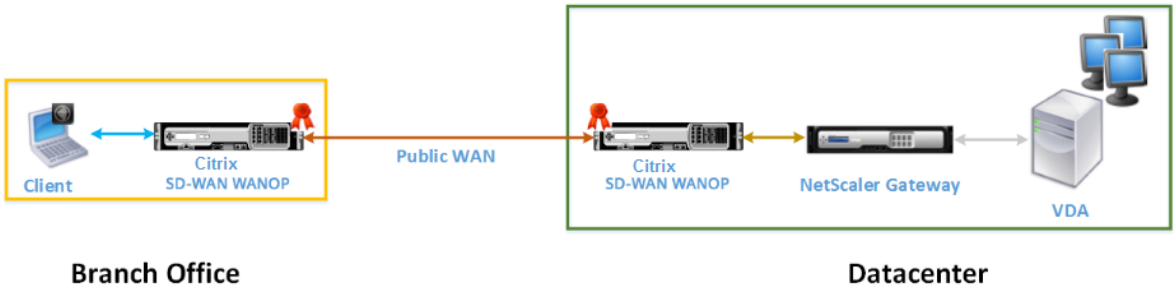
在此部署中，一对 Citrix SD-WAN WANOP 设备之间的通信是通过使两个设备受保护的伙伴来保护的。此部署适用于通过 SSL 加密保护客户端和 VDA 资源之间的连接的企业网络。

> 注意
>
> 您必须在设备上配置适当的证书才能创建安全合作伙伴。有关安全合作伙伴关系的更多信息，请参阅安全对等。

ICA 代理模式：

下图显示了在 ICA 代理模式下安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

在 ICA 代理模式下部署的 Citrix SD-WAN WANOP 设备



在 ICA 代理模式下，在分支机构和数据中心以内联模式安装了一对 Citrix SD-WAN WANOP 设备。此外，您还可以在数据中心安装代理 VDA 的 Citrix Gateway。客户端通过公用 WAN 通过 Citrix Receiver for HTML5 访问 VDA 资源。由于 Gateway 代理 VDA，因此建立了两个连接：客户端与 Citrix 网关之间的 SSL 连接以及 Citrix Gateway 和 VDA 之间的 ICA 安全连接。Citrix Gateway 代表客户端建立与 VDA 资源的连接。通过 ICA 级别的加密来保护从 Gateway 到 VDA 资源的连接。

在“了解客户端与服务器之间交换的消息”中解释了客户端与 VDA 之间交换的消息。但是，在这种情况下，连接将在 Citrix Gateway 终止。只有在 Gateway 协商 WebSocket 授权后，网关才会代理 VDA 并打开与 VDA 的连接。然后，Gateway 透明地将消息从客户端传递到 VDA，反之亦然。

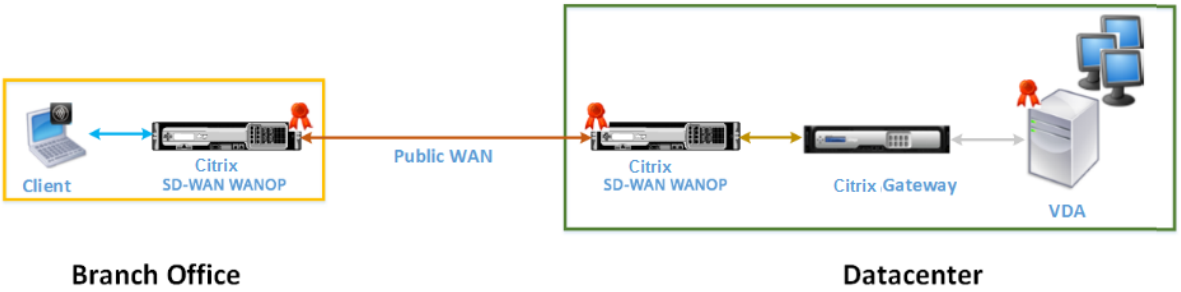
如果希望用户从公用 WAN 访问 VDA 资源，可以考虑部署 ICA 代理模式设置。

> 注意
>
> 您必须在设备上配置适当的证书才能创建安全合作伙伴。有关安全合作伙伴关系的更多信息，请参阅安全对等。

使用端到端 **SSL** 加密的 **ICA** 代理模式：

下图显示了在使用端到端 SSL 加密保护的 ICA 代理模式下安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

以 ICA 代理模式部署的 Citrix SD-WAN WANOP 设备，采用端到端 SSL 加密保护



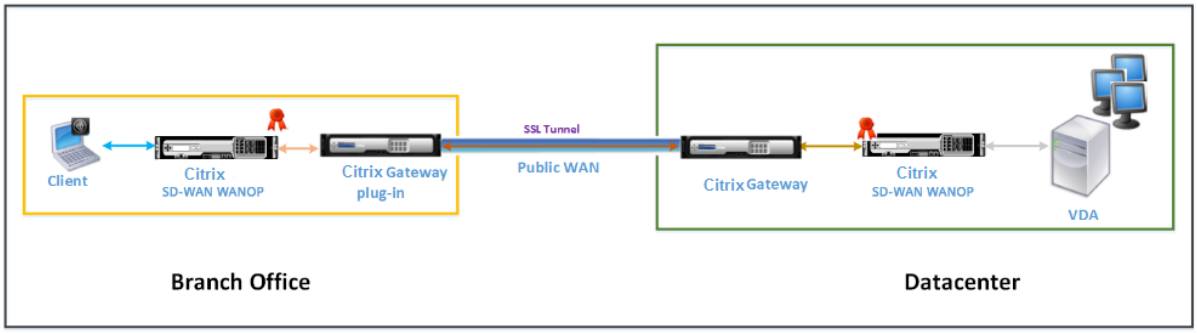
具有端到端 SSL 加密模式的 ICA 代理模式与普通 ICA 代理模式类似，区别在于 Citrix Gateway 和 VDA 之间的连接通过 SSL 加密而不是使用 ICA 安全连接来保护。在这种情况下，必须在 Citrix SD-WAN WANOP 设备和 VDA 上安装适当的证书。Citrix Gateway 和 VDA 之间的连接使用端口 443 而不是端口 8008，就像普通 ICA 代理模式一样。

此部署适用于必须保护客户端与 VDA 之间的端到端通信的网络，包括 Citrix Gateway 和 VDA 之间的连接。

完整的虚拟专用网络 **(VPN)** 模式：

下图显示了在完整虚拟专用网络 (VPN) 模式下安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

在 VPN 模式下部署的 Citrix SD-WAN WANOP 设备



在完整 VPN 模式下，一对 Citrix SD-WAN WANOP 设备以内联模式跨分支机构和数据中心安装。除了 Citrix receiver for HTML5 之外，还可以在客户端上安装 Citrix Gateway 插件，并在数据中心安装与外部网络接口的 Citrix Gateway。客户端上的 Citrix Gateway 关插件和数据中心上的 Citrix 网关在建立连接时通过网络创建 SSL 隧道或 VPN。因此，客户端可以直接安全访问 VDA 资源，并通过 Citrix SD-WAN WANOP 设备进行透明连接。当客户端连接在 Citrix Gateway 终止时，网关将打开与 VDA 上端口 8008 的透明连接。

客户端与 VDA 之间交换的邮件将在“了解客户端与服务器之间交换的邮件”部分中进行说明。但是，在这种情况下，连接将在 Citrix Gateway 终止。Gateway 关代理 VDA 并在端口 8008 打开与 VDA 的透明连接，并以透明方式将所有消息从客户端传递到 VDA，反之亦然。

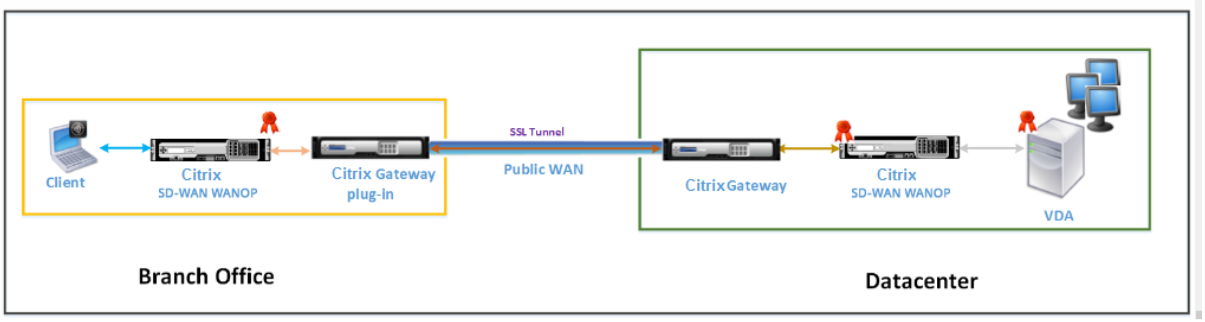
Citrix SD-WAN WANOP 插件使客户端能够访问资源，而不考虑客户端的位置。如果希望客户端需要从其桌面以外的位置访问 VDA 资源，则可以在完全虚拟专用网络 (VPN) 模式下部署安装程序。

此部署适用于期望员工在旅行时访问资源的组织。

具有端到端 **SSL** 加密功能的完整虚拟专用网络 **(VPN)** 模式：

下图显示了以端到端 SSL 加密保护的完整 VPN 模式安装在客户端上的 Citrix Receiver for HTML5 的部署拓扑。

以 VPN 模式部署的 Citrix SD-WAN WANOP 设备，采用端到端 SSL 加密保护



具有端到端 SSL 加密部署的完整虚拟专用网络 (VPN) 模式类似于普通的完整 VPN 模式，不同之处在于 Citrix Gateway 和 VDA 之间的通信通过 SSL 加密保护，并使用端口 443 而不是端口 8008。

此部署适用于需要对正在旅行的员工访问的资源进行端到端 SSL 加密的组织。

自适应传输互操作性

April 23, 2021

自适应传输是 Citrix Virtual Apps and Desktops 的数据传输机制。此传输速度更快，能够扩展，改进了应用程序的交互性，并且在具有挑战性的远距离 WAN 和 Internet 连接中互动性更强。自适应传输维持高服务器可扩展性，并有效利用带宽。借助自适应传输，ICA 虚拟通道可以自动响应不断变化的网络条件。它们可以在 Citrix 协议（名为 Enlightened Data Transport (EDT)）与 TCP 之间智能地切换基本协议，以实现最佳性能。默认情况下，启用自适应传输，并在可能的情况下使用 EDT，并回退到 TCP。

Citrix SD-WAN WANOP 提供跨会话标记化压缩（数据重复数据消除），包括基于 URL 的视频缓存。如果办公地点的两个或更多人观看同一客户端获取的视频，或者传输或打印同一文件或文档的重要部分，则可显著降低带宽。此外，通过在分支机构的设备上运行面向 ICA 数据缩减和打印作业压缩的进程，WANOP 将提供 VDA 服务器 CPU 卸载并启用更高的 Citrix Virtual Apps and Desktops 服务器可扩展性。

当 TCP 用作数据传输协议时，Citrix SD-WAN WANOP 支持上述优化。在网络连接上使用 Citrix SD-WAN WANOP 时，请选择 TCP 并禁用 EDT。通过使用 TCP 流量控制和拥塞控制，Citrix SD-WAN WANOP 可确保在高延迟和中度数据包丢失的情况下与 EDT 相当的交互性。

有关在 Citrix Virtual Apps and Desktops 上配置适应传输的信息，请参阅 自适应传输。

Citrix Hypervisor 6.5 升级

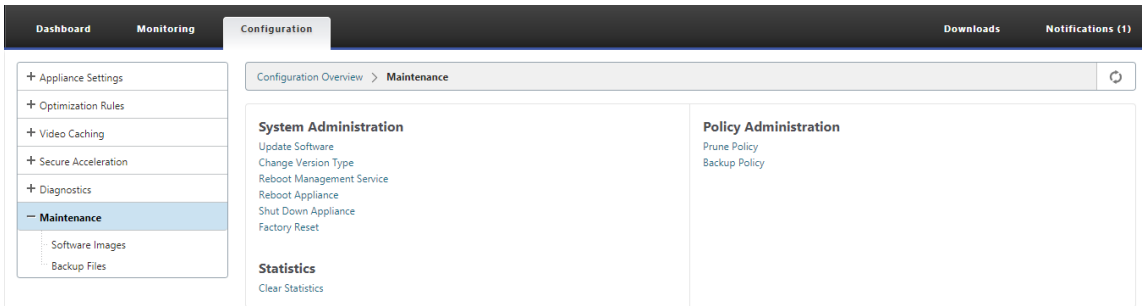
April 23, 2021

> 重要
>
> 要升级到 **Citrix Hypervisor** 版本 **6.5**，设备必须运行 **Citrix SD-WAN WANOP** 软件版本 **9.0.x** 或更高版本。
>
> 注意
>
> 当设备在低于 9.0.x 版本的软件版本上运行时，请勿尝试升级以防止升级问题。

如何升级到 **Citrix Hypervisor 6.5**

要在 SD-WAN WANOP 设备上升级到 Citrix Hypervisor 6.5，请确保设备正在运行软件版本 9.0.x 或更高版本。如果设备运行较旧的软件发布版本，请先升级到最新的软件发布版本。

1. 在 Citrix SD-WAN WANOP GUI 中，转到 配置 > 维护 > 更新软件。下载 **ns-sdw-wo-<Build_No> .upg 文件以升级设备。

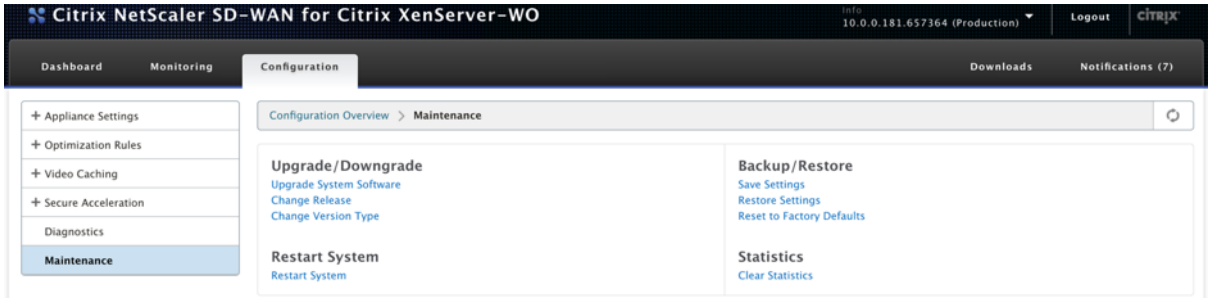


2. 升级到最新软件版本的 WANOP 软件后，在 GUI 中导航到 配置 **>** 维护 **>** 更新软件。上载 *ns-sdw-xen65-pkg_v1.5.upg* 文件。
3. 等待大约 20 分钟完成升级。升级成功完成后，设备会重新启动。

维护

April 23, 2021

使用 维护 页面执行维护活动，例如升级降级系统软件、备份和恢复配置以及清除统计信息。



升级/降级

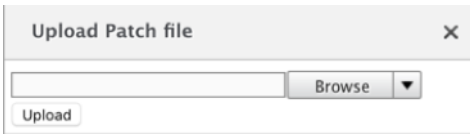
升级系统软件

对于每个设备型号，都有不同的 Citrix SD-WAN 软件包。您需要为要包含在网络中的设备下载相应的 SD-WAN WANOP 软件包，并将其保存在本地驱动器中。

通过从 Citrix 获取的修补程序文件升级设备软件。

> 注意：
>
> 如果设备运行较旧的软件发布版本，则需要先升级到最新的软件发布版本。

要升级系统软件，请转到 配置 **>** 维护。选择 升级/降级下的升级系统软 件，选择修补程序文件，然后将其上传到设备。



修补程序文件将由设备检查。只有有效的补丁文件才能将系统升级到与当前使用的版本不同的版本。

升级保留许可证文件和系统设置。升级后的单元不需要重新配置，除了随新版本添加的任何新功能。

更改发布

更改发布页面显示当前安装的发布。如果要更改发布版本，请单击 更改发布 选项，然后从下拉列表中选择发布，然后单击 更改。

更改版本类型

更改版本类型 选项允许您选择版本的调试版本。您可以从“类型”下拉列表中选择版本 类型，然后单击 更改。以下是可能的调试版本：

- 默认值
- 级别 1

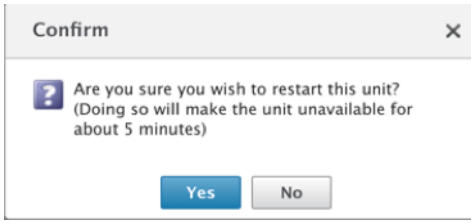
- 级别 2
- 默认 MC
- 一级 MC
- 二级 MC

您需要按照支持团队的指示执行此操作。

重新启动系统

安装修补程序后，弹出消息将询问设备是否可以重新启动。在设备重新启动之前，不会应用修补程序。如果您选择不立即重新启动系统，则会在每个页面的顶部放置一个提醒。

单击 重新启动系统 以重新启动 SD-WANOP 设备。此过程需要几分钟时间。



备份设置

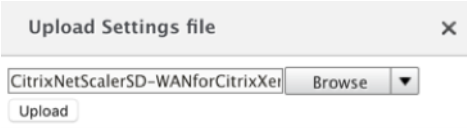
您可以通过将设备配置另存为文本文件来备份设备配置。

单击 保存设置”，文本文件将下载到您的本地驱动器。无法保存“管理 IP”页面上的许可证文件、SSH 参数和 IP 地址。该文件是普通文本文件，但不应手动编辑。

恢复设置

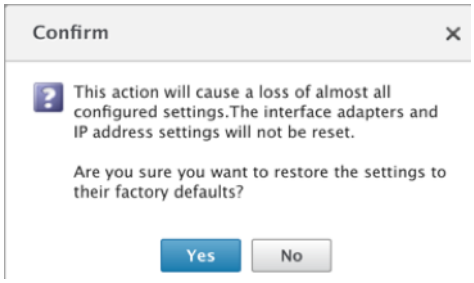
保存文件后，可将其还原到同一 SD-WAN WANOP 设备。

设备维护旧版本的副本。还原设置 选项有助于还原配置的设置。“管理 IP”页面上的许可证文件、SSH 参数和 IP 地址不会从较新版本复制回旧版本。相反，设备将恢复为升级旧版本时有效的设置。



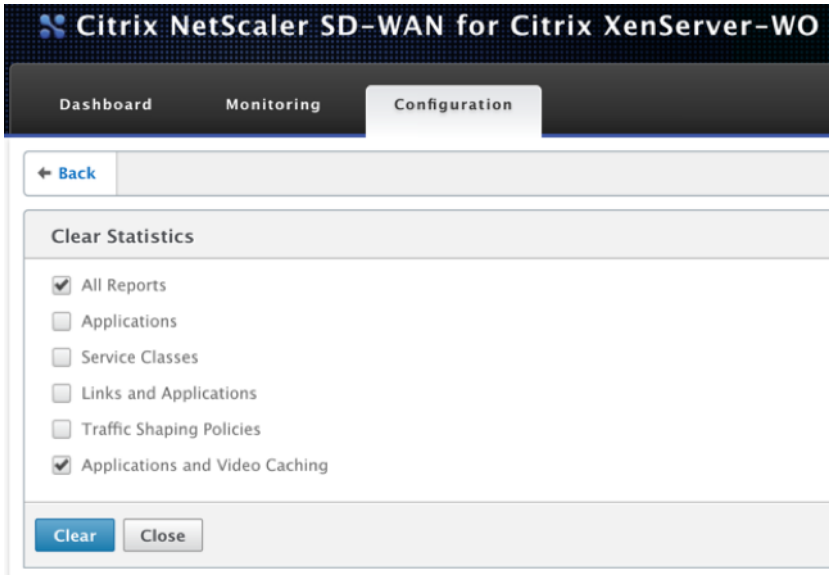
重置为出厂默认值

重置为出厂默认值 选项允许重置设置。它将 IP 地址、带宽设置和许可证以外的所有参数设置为出厂默认值。单击 重置为出厂默认值”，将显示一条确认消息。如 果 要将设置还原为出厂默认值，请单击“是”。



清晰的统计数据

清除统计信息 页允许重置 SD-WAN WANOP 设备的统计信息。它还允许创建从所需采样窗口开始的报表。选择要从设备中清除的统计数据选项，然后单击 清除”。



诊断

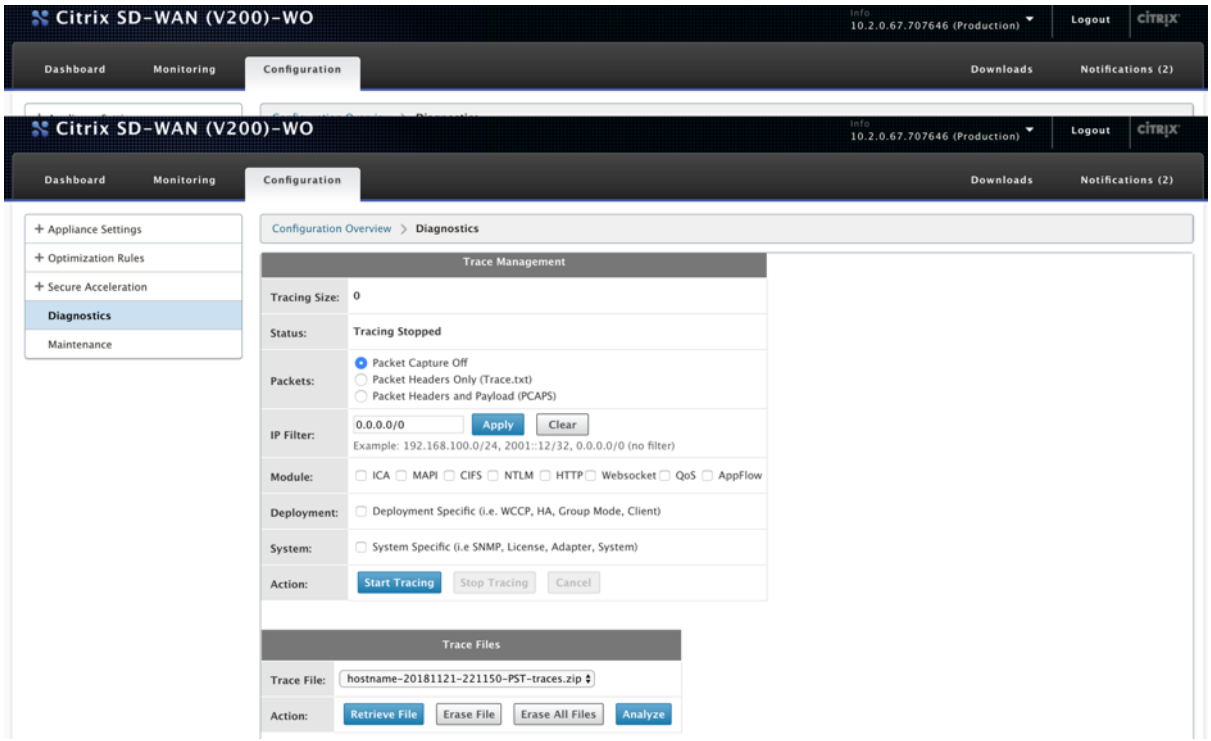
April 23, 2021

本节提供诊断工具，用于识别 SD-WAN WANOP 网络中的网络问题并进行故障排除。您还可以获取系统日志文件、系统信息和其他必要的详细信息，以帮助 Citrix SD-WAN 支持团队诊断和解决网络问题。

以下是 SD-WAN WANOP 中可用的诊断工具：

- 跟踪
- 数据包分析器
- 旁路卡测试
- 检索课程

- 线路测试仪
- Ping
- Traceroute
- 系统信息
- 诊断数据



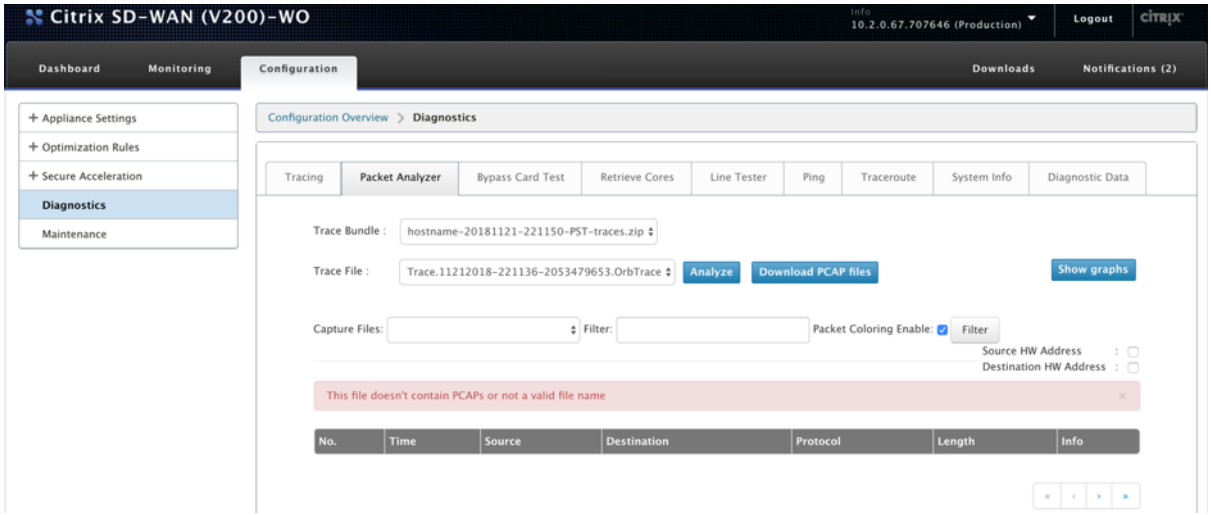
跟踪

跟踪 工具用于监视流过 SD-WAN WANOP 网络的数据包。它可以打开每个数据包并识别所使用的协议、源和目标的 IP 地址以及其他有效负载信息。Citrix 支持团队使用此信息查找网络问题的根本原因。

您可以选择 仅跟踪数据包标头 或 数据包标头和有效负载。您可以选择要跟踪的模块，并指定跟踪应该是部署特定的还是系统特定的。

单击开 始跟踪，设备开始跟踪数据包。当您单击 停止跟踪时，结果打包
到 ZIP 存档中。此档案可以使用 检索文件 选项下载到您的
计算机上。然后，您可以将这些文件转发给支持团队。跟踪文件还提供崩溃分析数据。

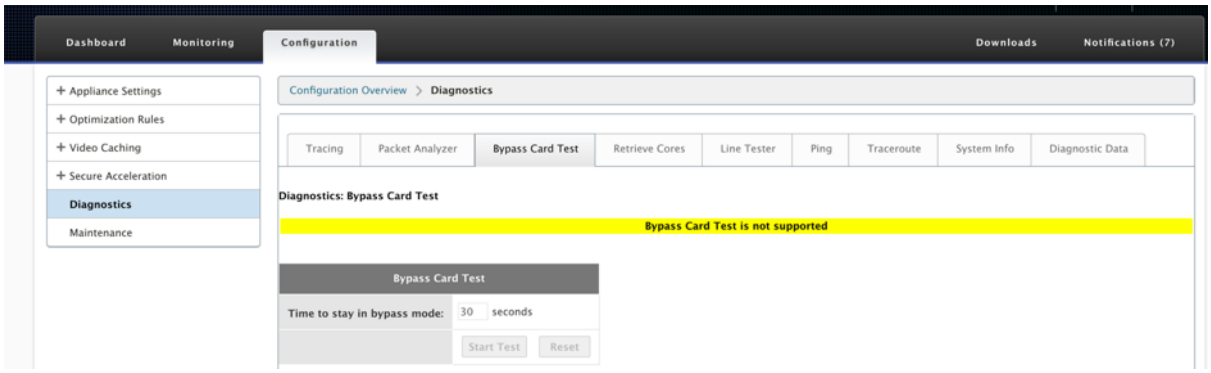
单击 分析 以查看有关数据包分 析器选项卡中的数据包 的详细信息。



您可以查看时间、源地址、目标地址、协议、长度和有效负载信息。

旁路卡测试

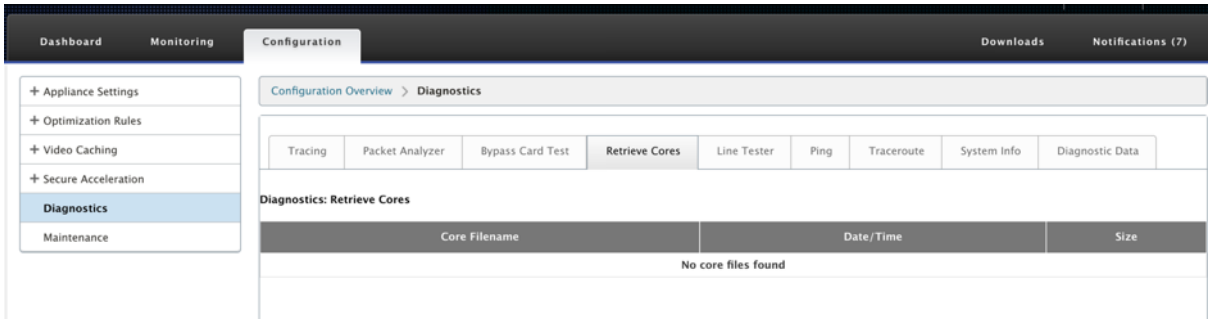
您可以在内联（故障到线）模式下测试设备部署的以太网接口的故障到线功能。输入设备保持旁路模式的秒数，然后单击 开始测试”。在此期间，会绕过设备。之后将恢复正常操作。



检索内核

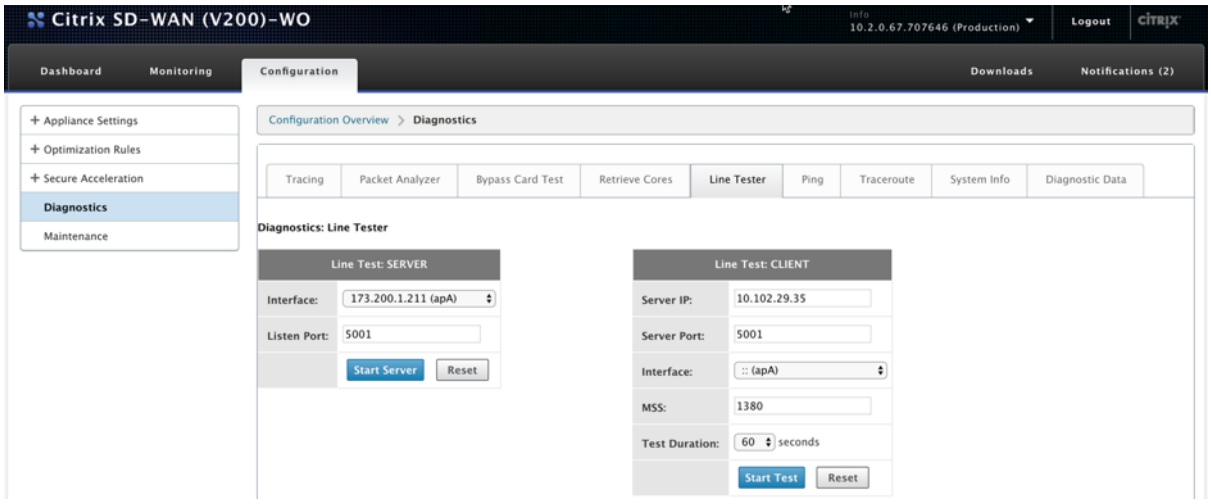
当 SD-WAN WANOP 设备异常退出或崩溃时创建核 心文件。设备崩溃后自动重新启动。在持续崩溃的情况下，加速处于禁用状态，但管理界面仍处于活动状态。

您可以选择并检索在设备崩溃期间或设备行为异常时创建的所需核心文件。检索到的文件保存在 ZIP 存档中。您可以与支持团队共享，以便进一步分析。



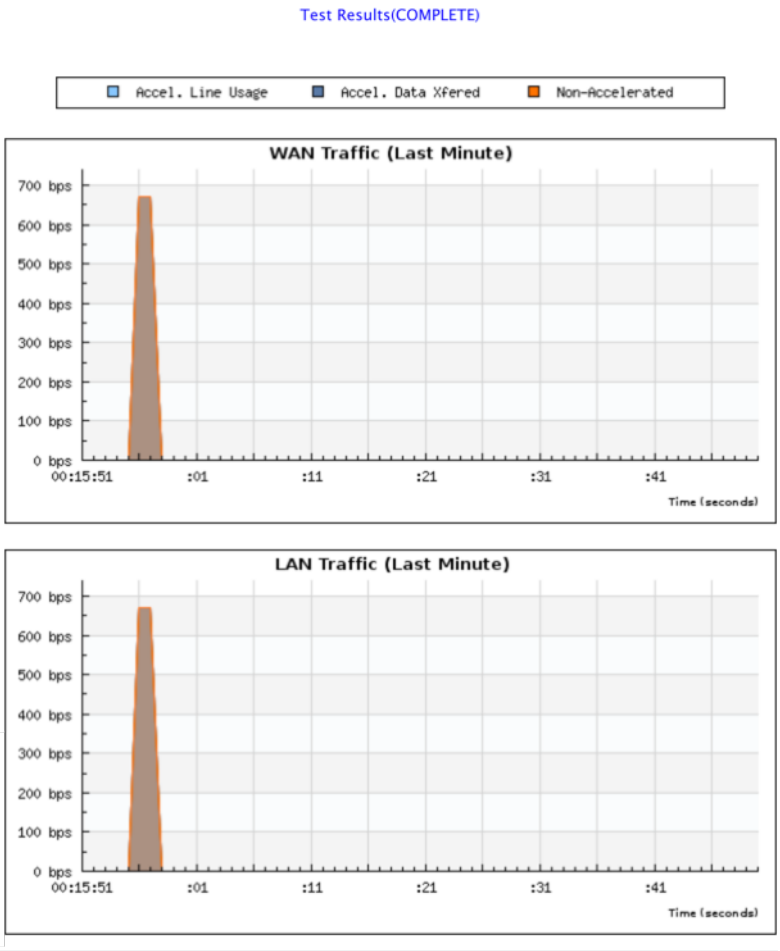
线路测试仪

线测试：服务器 功能在设备上启动一个 iperf 服务器，在 TCP 模式下运行。此选项可用于验证 WANOP 设备之间的连接性以及对网络流量进行故障排除。要运行 iperf 测试，一个系统（设备或另一个主机）必须将 iperf 作为服务器运行，另一个系统必须以客户端身份连接到该系统。



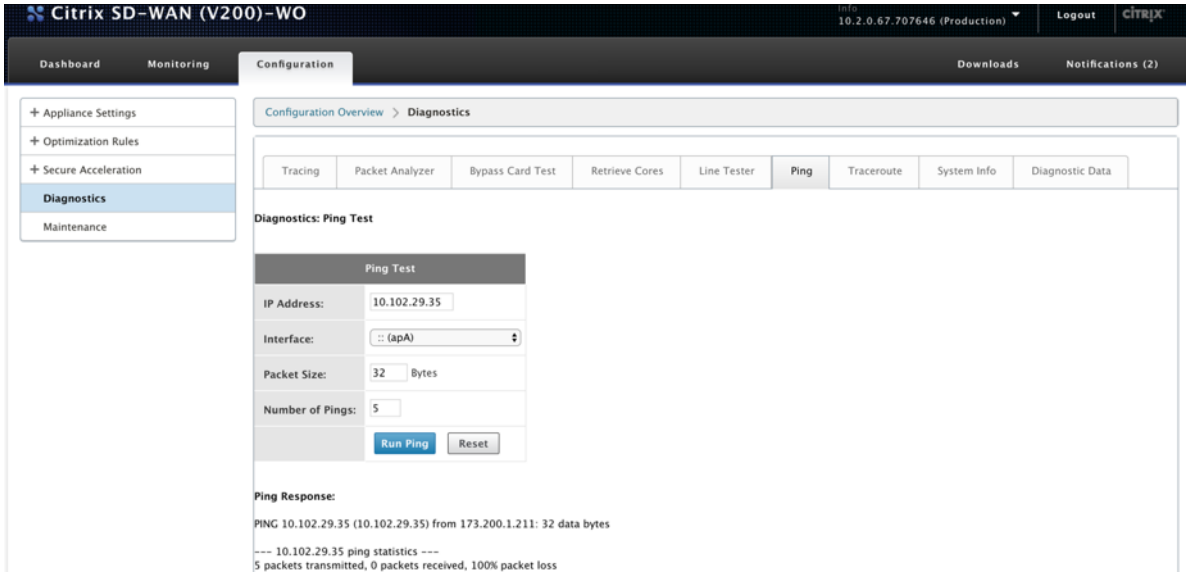
您可以使用默认的 线路测试服务器 界面和端口号。单击 启动服务器 以启动设备上的 iperf 服务器。

线测试：客户端 函数在本机上启动一个 iperf 客户端，在 TCP 模式下运行。您还可以指定 iperf 服务器端口号和测试长度。测试完成后，将报告连接速度。单击 开始测试 以查看 WAN 和 LAN 流量结果。



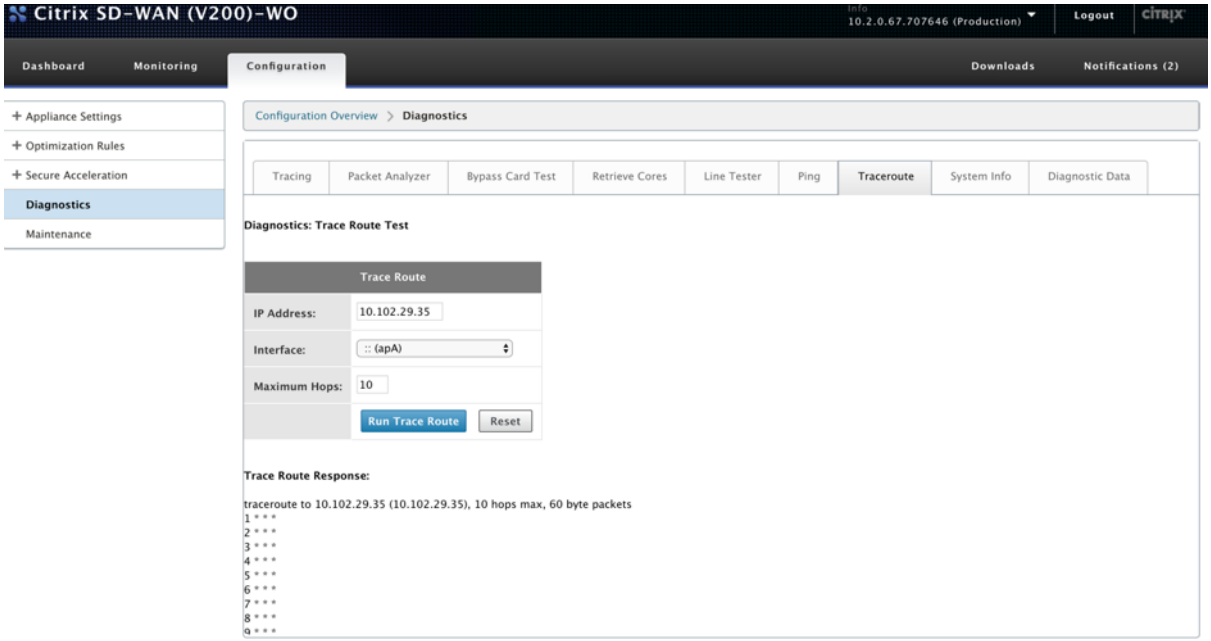
Ping

Ping 允许您检查 SD-WAN 网络中网络元素的连接性。输入网络元素的 IP 地址，然后单击 运行 **Ping** 以查看结果。



Traceroute

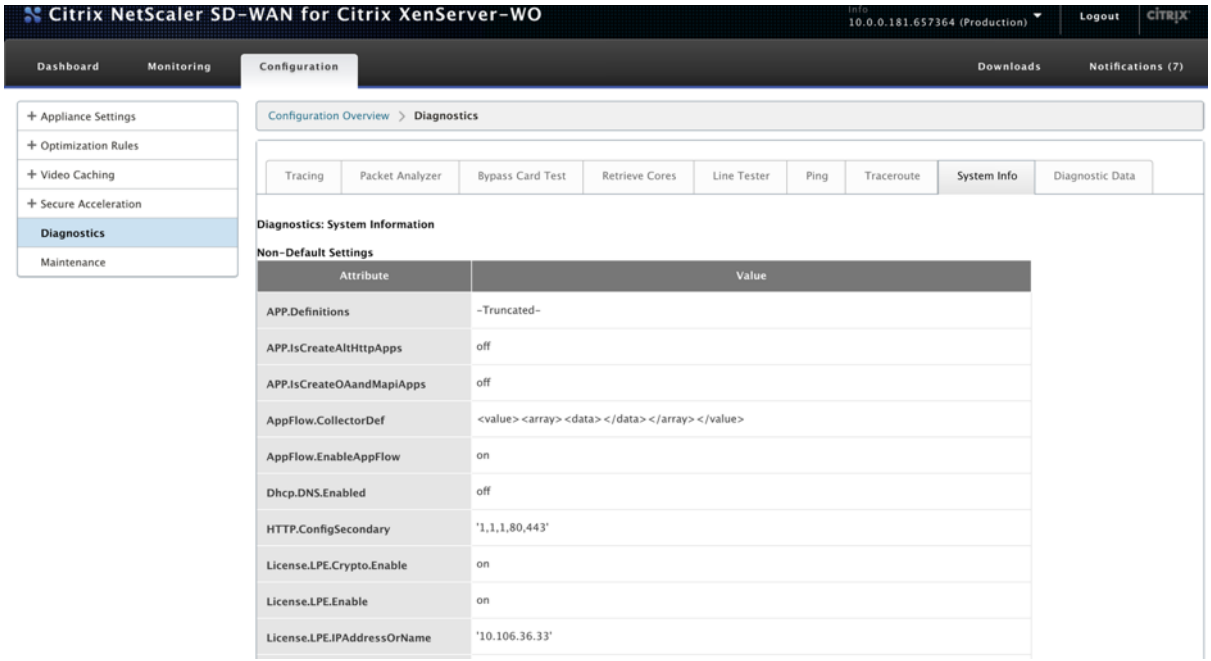
Traceroute 允许您记录 SD-WAN 设备与 SD-WAN 网络或互联网上任何其他网络元素之间的路由。它计算并显示每个跃点花费的时间量。



系统信息

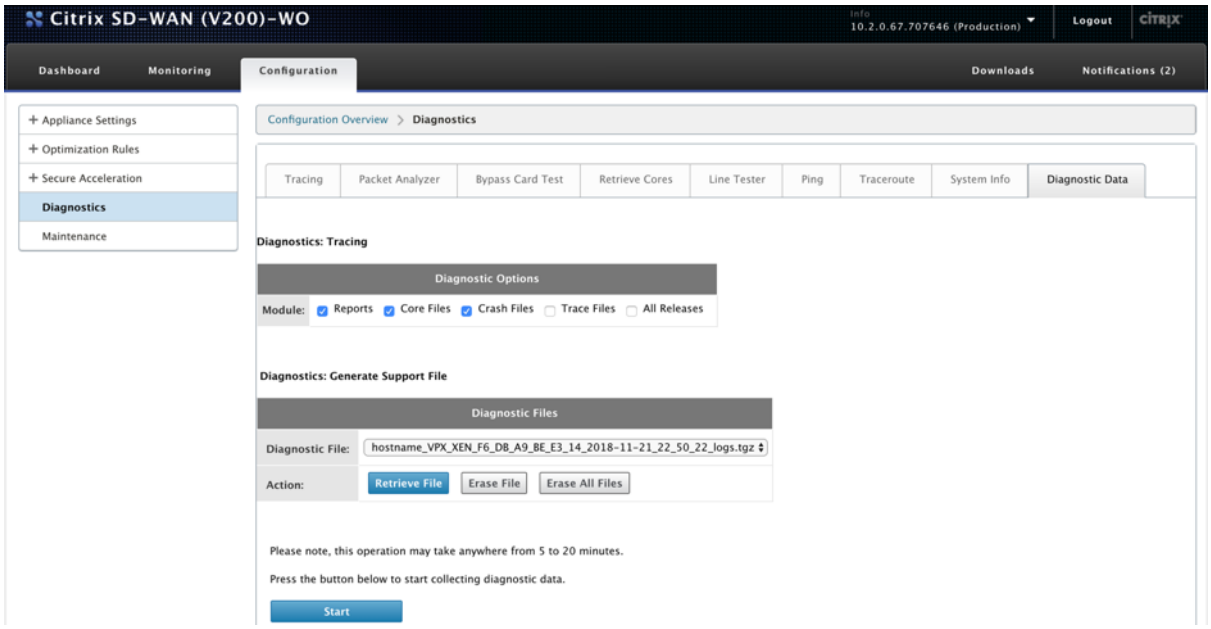
系 统信息 列出未设置为默认值的所有参数。此信息为只读信息。如果怀疑存在某种错误配置，则由支持部门使用。当您报告问题时，系统可能会要求您检查此页面上的一个或多个值。

它提供了 非默认设置、适配器主适配器的详细信息、适配器 **apA.2** 的 详细信息和适配器 **apA.1** 的详细信息。



诊断数据

诊断数据 允许您打包诊断数据，以便 Citrix 支持团队进行分析。选择所需的诊断文件，然后单击 开始”。然后，您可以单击 检索文件 以下载 zip 档案，并与 Citrix 支持部门共享。



故障排除

April 23, 2021

以下主题提供问题列表、问题原因以及某些 Citrix SD-WAN WANOP 功能的解决步骤。

CIFS 和 MAPI

Citrix SD-WAN WANOP 插件

RPC over HTTPS

视频缓存

Citrix Virtual Apps and Desktops 加速

CIFS 和 MAPI

April 23, 2021

- 问题：域控制器已从网络中删除。但是，Citrix SD-WAN WANOP 设备无法离开域。

  原因：这是设备的已知问题。

  解决办法：在 Windows 域页面中，将 DNS 更改为可以解析预期域的 DNS。接下来，使用“重新加入域 选项使 Citrix SD-WAN WANOP 设备加入该域。现在尝试离开域。

- 问题：MAPI 连接未优化，并显示以下错误消息：

  不支持 Outlook 中的非默认设置

  原因：这是版本 6.2.3 和更早版本的已知问题。

  解决方案：将设备升级到最新版本。

- 问题：设备优化了 MAPI 连接。但是，监视页将发送和接收的字节数显示为零。

  原因：这是设备的已知问题。

  解决方法：这是一个良性问题，不会影响设备的功能。你可以忽略它。

- 问题：无法在 Citrix SD-WAN WANOP 设备之间建立安全对等。

  原因：未正确配置与合作伙伴设备的安全对等。

  解决方案：执行以下操作：

  1. 验证您是否已将 CA 和服务器证书的适当组合上传到设备。
  2. 导航到 **Citrix SD-WAN WANOP** > 配置 > **SSL** 设置 > 安全合作伙伴页面。

3. 在 合作伙伴安全 部分的 证书验证 下，选择 无-允许所有请求 选项，以确保证书永远不会过期。
4. 验证设备是否可以与合作伙伴设备建立安全对等。
5. 验证侦听部分是否有预期 Citrix SD-WAN WANOP 设备的 IP 地址条目。

- 问题：连接到 Exchange 群集时，有时会绕过或提示具有优化连接的 Outlook 用户输入登录凭据。

  原因：MAPI 优化要求 Exchange 群集中的每个节点与 exchangeMDB 服务主体名称 (SPN) 相关联。随着时间的推移，由于需要更多容量，您可以向群集添加其他节点。但是，有时配置任务可能无法完成，使群集中的某些节点没有 SPN 设置。此问题最常见于 Exchange Server 2003 或 Exchange Server 2007 的 Exchange 群集中。

  解决方法：在设置中的每个 Exchange Server 上执行以下操作：

  1. 访问域 Controller。
  2. 打开命令提示符。
  3. 运行以下命令：

     ```
     pre codeblock setspn -A exchangeMDB/Exchange1 Exchange1
     setspn -A exchangeMDB/Exchange1.example.com Exchange1 <!--
     NeedCopy-->
     ```

- 问题：尝试连接到 Outlook 时，将显示“尝试连接”消息，然后终止连接。

  原因：客户端 Citrix SD-WAN WANOP 设备具有在服务器端设备上不存在的黑名单条目。

  解决方法：从两台设备中删除黑名单条目，或（推荐）将设备的软件升级到版本 6.2.5 或更高版本。

- 问题：即使通过域前检查，设备也无法加入域。

  原因：这是一个已知的问题。

  解决方案：执行以下操作：

  1. 使用 SSH 实用程序访问设备。
  2. 使用根凭据登录到设备。
  3. 运行以下命令：

     ```
     /opt/likewise/bin/domainjoin-cli join \<Domain\\_Name\>
     administrator
     ```

- 问题：向 Citrix SD-WAN WANOP 设备添加委派用户时，将显示 LdapError 错误消息。

  解决方法：执行以下操作之一：

  – 在 Citrix SD-WAN WANOP 设备的 DNS 服务器上，验证是否为每个域控制器 IP 地址配置了反向查找区域。

  - 验证客户端计算机的系统时钟与 Active Directory 服务器的系统时钟同步。使用 Kerberos 时，必须同步这些时钟。
  - 通过再次为委派用户提供密码，在 Windows 域页面上更新委派用户。

- 问题：向 Citrix SD-WAN WANOP 设备添加委派用户时，将显示时间偏斜错误消息。

  解决方法：验证设备是否已加入域。如果不是，请将设备加入域。这将设备时间与域服务器时间同步，并解决问题。

- 问题：为了加速，客户端暂时排除在外。将委派用户添加到 Citrix SD-WAN WANOP 设备时，会出现最后一个错误（Kerberos 错误。）错误消息。

  原因：委托用户配置为 仅使用 **Kerberos** 身份验证。

  解决方案：验证在域控制器上，委托用户的身份验证设置是否为 使用任何身份验证协议”。

- 问题：将委派用户添加到 Citrix SD-WAN WANOP 设备时，将显示委派用户未准备就绪错误消息。

  解决方法：如果消息仅显示在客户端设备上，请忽略该消息。但是，如果消息显示在服务器端设备上，请运行 **Windows Domain** 页面上可用的委派用户预检查工具，然后在服务器端设备上配置委派用户。

- 问题：最后一个错误（服务器未被委派进行 Kerberos 身份验证。请添加委托用户，检查服务列表和服务器允许委托。）当您将委派用户添加到 Citrix SD-WAN WANOP 设备时，将显示 URL：4 错误消息。

  解决方案：验证在域控制器上正确配置了委托用户，并且您已向域控制器添加了适当的服务。

- 问题：设备无法加入域。

  解决方法：运行 Windows 域页面上可用的域预检查工具，并解决问题（如果有）。如果域预检查工具未报告任何问题，请与 Citrix 技术支持联系，以获取解决问题的进一步帮助。

Citrix SD-WAN WANOP 插件

April 23, 2021

- 问题：我面临信号通道连接问题。如何解决这些问题？

  解决方法：要解决信令通道连接问题，请执行以下故障排除步骤：

  - 验证您是否已正确配置信令 IP 地址。您可以通过 ping 信令 IP 地址并验证响应来执行此操作。
  - 验证 WANOP 设备上是否启用了信号状态。
  - 验证网络上安装的防火墙不会删除 WANOP TCP 选项。
  - 验证 WANOP 设备上是否安装了有效的 WANOP 插件许可证。
  - 验证信令通道源筛选配置不阻止客户端源 IP 地址。

  - 如果您已启用 LAN 检测，请验证 WANOP 插件和 WANOP 设备之间的往返时间是否为可接受的值。

- 问题：在 WANOP 4000 设备上，我无法禁用 WANOP 插件。

  原因：这是一个已知的问题。

  决议：无。您不能禁用 WANOP 4000 设备上的 WANOP 插件。

- 问题：使用 WANOP 插件连接到 WANOP 设备时，“警报”选项卡上会记录以下错误消息条目：

  <Number> 尝试连接到此设备的 WANOP 插件超过当前限制。

  原因：与 WANOP 设备的连接数已超过许可用户限制。

  解决方法：等待用户断开连接或终止连接。

- 问题：在 WANOP 4000 或 5000 设备上配置了错误的信令 IP 地址。

  解决方法：要更新 WANOP 4000 或 5000 设备上的信令 IP 地址，请完成以下步骤：

  1. 登录到 WANOP 设备的 Citrix 实例。
  2. 导航到流量管理 > 负载平衡 > 虚拟服务器 > BR_LB_VIP_SIG 页面。
  3. 更新信令 IP 地址。
  4. 保存配置。

- 问题：CIFS 和 ICA 流量没有加速。

  解决方法：要解决此问题，请执行以下故障排除步骤：

  - 验证是否为 WANOP 插件正确定义了 IP 地址和端口号的加速规则。
  - 验证是否在信令连接成功后建立了 CIFS 或 ICA 连接。
  - 验证正在使用的服务类的加速策略。

RPC over HTTPS

April 23, 2021

- 问题：将设备的软件升级到 7.3 版后，监视报告没有通过 HTTPS 连接进行 RPC 的特殊类别。

  原因：将设备升级到版本 7.3 时，通过 HTTPS 的 RPC 应用程序不属于其自己的服务类。因此，所有通过 HTTPS 的 RPC 连接都列为报表中的 TCP 其他连接。

  解决方法：要将这些连接分类为通过 HTTPS 连接的 RPC，请为其应用程序创建服务类。

- 问题：通过 HTTPS 为 RPC 创建服务类后，所有 HTTP 和 HTTPS 流量都被归类为通过 HTTP 的 RPC。

  原因：您尚未将目标 IP 地址添加到通过 HTTPS 应用程序为 RPC 创建的服务类中。

  解决方法：通过添加服务器的目标 IP 地址，修改通过 HTTPS 应用程序为 RPC 创建的服务类。

视频缓存

April 23, 2021

- 问题：将条目添加到预填充任务列表后，该条目仍处于已配置状态。

  原因：预先生成任务需要大约一分钟的时间移动到“下载”状态。

  解决方法：一分钟后检查条目的状态，或刷新页面以验证状态是否更改为“下载”。

- 问题：将条目添加到预填充任务列表后，条目的状态显示“错误 403”。但是，该网站在 Web 浏览器中正常工作。

  原因：Citrix SD-WAN WANOP apA 的 IP 地址无法访问视频服务器。

  解决方法：要解决此问题，请验证并更新以下内容：

  - 跨防火墙访问规则
  - 视频服务器的 httpd.conf 文件中基于源 IP 地址的限制

  原因：视频服务器不支持 HEAD 方法。

  解决方法：视频服务器必须允许此方法使用 Citrix SD-WAN WANOP IP 地址。

  原因：视频服务器上未启用文件夹的目录列表。

  解决方案：视频服务器必须为文件夹启用目录列表。

- 问题：为预填体任务创建条目后，无法修改或删除条目。

  原因：您可能已单击该条 目的立即开始。

  解决方案：这是通过设计。单击该条目的“立 即开始 并且该条目处于排队、开始或下载状态后，您无法修改或删除该条目。您只能在下载完成后删除条目。

- 问题：为预填充任务创建条目后，视频不会被下载和缓存。条目的状态显示“下载失败”。

  原因：预填入条目没有视频的绝对 URL。

  解决方案：要解决此问题，请完成以下过程：

  1. 验证预填入条目是否具有视频的实际 URL，例如`http://10.102.29.16/Citrix SD-WAN WANOP\\_demo.mp4`，而不是 HTML 文件。Citrix SD-WAN WANOP 设备无法搜索 HTML 文件的内容以查找视频链接。

2. 验证 HTTP 协议是否用于提供视频。您可以使用 Web 浏览器的“查看源”选项来验证这一点。
3. 您可以使用 Web 浏览器的“开发人员工具”选项获取视频的绝对 URL。

Citrix Virtual Apps and Desktops 加速

April 23, 2021

- 问题：将设备升级到版本 7.3.1 后，ICA 连接不会在 ICA 监视页面中归类为 Citrix Receiver for HTML5 连接。

  原因：在设备上定义的服务类是 **HTTP**（私有），而不是 Web（私有）。将设备升级到版本 7.3.1 时，**ALTHTP** 应用程序不会添加到此服务类。因此，即使优化通过 Citrix Receiver for HTML5 建立的 ICA 连接，但在 ICA 监视页面中，这些连接不会被归类为 Citrix Receiver for HTML5 连接。

  解决方法：要对 Citrix Receiver for HTML5 的 ICA 连接进行分类，请完成以下过程：

  1. 导航到 配置 > 优化规则 > 服务类 页面。
  2. 编辑 **HTTP**（专用）服务类。
  3. 点击 添加规则。
  4. 在“筛选规则”的“应用程序”下，单击 任意”。
  5. 从应用程序列表中，选择 **ALTHP**。
  6. 单击添加。
  7. 单击保存。
  8. 根据需要对筛选器规则进行其他更改。
  9. 单击保存。