Citrix ADC 12.1

Machine translated content

Disclaimer

Contents

Citrix ADC 入门

December 20, 2021

本主题介绍 Citrix ADC 设备的基本功能和配置详细信息。安装和配置网络设备的系统和网络管理员可以参考此内容。

Citrix ADC 简介

Citrix ADC 设备是一种应用交换机，用于执行特定于应用的流量分析，从而智能地分配和优化 Web 应用 4 - 7 层 (L4–L7) 的网络流量，并确保其安全。例如，Citrix ADC 设备对单个 HTTP 请求（而非长期存在的 TCP 连接）的决策进行负载均衡。负载平衡功能有助于减慢服务器故障的速度，同时减少客户端的中断。ADC 功能可大致分为：

1. 数据交换
2. 防火墙安全性
3. 优化
4. 策略基础结构
5. 数据包流
6. 系统限制

数据交换

如果部署在应用程序服务器之前，Citrix ADC 将通过定向客户端请求的方式确保实现最佳流量分配。管理员可以根据 HTTP 或 TCP 请求正文中的信息以及 L4-L7 标头信息（例如 URL、应用程序数据类型或 Cookie）对应用程序流量进行分段。大量的负载平衡算法以及广泛的服务器运行状况检查可确保将客户端请求定向到适当的服务器，从而提高了应用程序的可用性。

防火墙安全性

Citrix ADC 安全性和保护可保护 Web 应用程序免受应用程序层攻击。ADC 设备允许合法的客户端请求，而且可以阻止恶意的请求。它提供针对拒绝服务 (DoS) 攻击的内置防御措施，并支持应用程序保护功能，防止应用程序流出现会损坏服务器的合法激增。可用的内置防火墙可保护 Web 应用程序免受应用程序层攻击，包括缓冲区溢出攻击、SQL 注入企图、跨站点脚本攻击等。此外，该防火墙通过对机密的公司信息和敏感的客户数据进行加密，提供身份窃取防护。

优化

优化可卸载资源密集型操作，例如安全套接字层 (SSL) 处理、数据压缩、客户端保持活动状态、TCP 缓冲以及服务器静态和动态内容的缓存。这样可以提升服务器场中服务器的性能，从而提高应用程序的速度。ADC 设备支持多种透明的 TCP 优化，可缓解由于高延迟和网络链接拥塞而引起的问题。因而加快了应用程序的交付速度，同时不需要更改客户端或服务器的配置。

策略基础结构

策略定义关于 Citrix ADC 上的流量过滤和管理的具体详细信息。策略由两部分组成：表达式和操作。表达式定义策略匹配的请求类型。操作告诉 ADC 设备当请求匹配表达式时应执行的操作。例如，表达式可能要使特定的 URL 模式与某种类型的安全性攻击相匹配，配置为断开或重置连接。每个策略都有优先级，优先级决定策略的评估顺序。

当 ADC 设备收到流量时，相应的策略列表会决定如何处理流量。列表中的每个策略均包含一个或多个表达式，它们一起定义连接要匹配策略必须满足的条件。

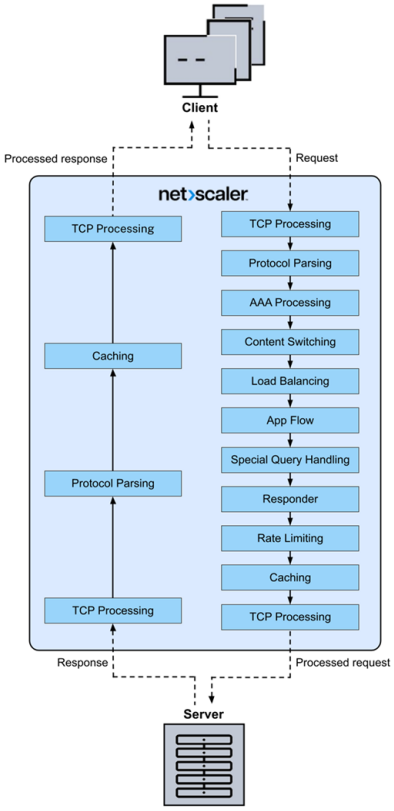
对于除重写以外的所有策略类型，设备仅实施具有请求匹配项的第一个策略。对于重写策略，ADC 设备将按顺序评估策略，并按相同的顺序执行相关操作。策略优先级对于获得您所需的结果非常重要。

数据包流

根据要求，您可以选择配置多项功能。例如，您可以同时选择配置压缩和 SSL 卸载功能。此时，系统在将传出的数据包发送到客户端之前，可能首先对数据包进行压缩，然后进行加密。

下图显示了 Citrix ADC 设备中的 DataStream 数据包流。MySQL 和 MS SQL 数据库支持 DataStream。

下图显示了 Citrix ADC 设备中的 DataStream 数据包流。MySQL 和 MS SQL 数据库支持 DataStream。有关 DataStream 功能的信息，请参阅 DataStream。



> 注意：如果流量针对内容交换虚拟服务器，则设备将按以下顺序评估策略：
>
> 1. 绑定到全局覆盖。
> 2. 绑定到负载平衡虚拟服务器。
> 3. 绑定到内容交换虚拟服务器。
> 4. 绑定到全局默认值。
>
> 这样，如果一个策略规则设置为 true，而 gotopriorityexpression 设置为 END，我们将停止进一步进行策略评估。
> 在内容交换过程中，如果没有选择负载平衡虚拟服务器或绑定到内容交换虚拟服务器，我们将评估仅绑定到内容交换虚拟服务器的响应者策略。

系统限制

安装 Citrix ADC 软件 9.2 或更高版本时，每个 Citrix ADC 功能都有系统限制。有关详细信息，请参阅 Citrix 文章 CTX118716。

Citrix ADC 设备适用于网络中的哪个位置?

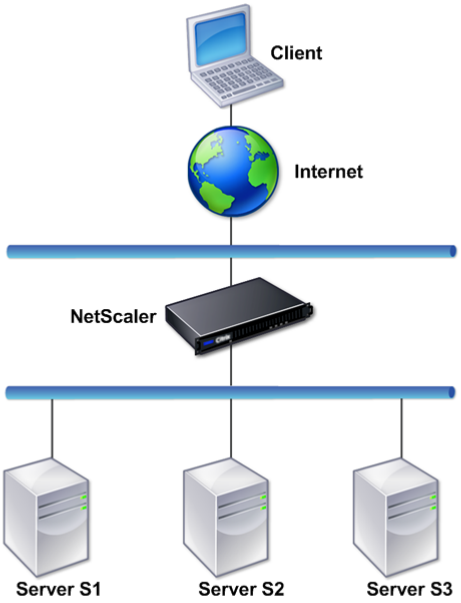
December 20, 2021

Citrix ADC 设备的位置介于客户端与服务器之间，以便客户端请求和服务器响应都能经过该设备。在典型安装中，在设备上配置的虚拟服务器提供连接点，客户端使用这些连接点来访问位于设备后面的应用程序。在这种情况下，设备拥有与其虚拟服务器相关联的公用 IP 地址，而实际服务器隔离在专用网络中。还可以在透明模式下将设备用作 2 层桥接器或 3 层路由器，甚至可以将其中某些功能与其他模式结合使用。

物理部署模式

逻辑上位于客户端与服务器之间的 Citrix ADC 设备可以在两种物理模式下部署：内联模式和单臂模式。在内联模式下，多个网络接口连接到不同的以太网段，且设备置于客户端与服务器之间。设备有单独的网络接口连接到每个客户端网络，有单独的网络接口连接到每个服务器网络。在此配置中，设备和服务器可以存在于不同的子网中。这些服务器可以位于公用网络中，客户端可以通过设备直接访问服务器，同时设备透明地应用 L4-L7 功能。通常情况下，虚拟服务器（稍后介绍）配置为提供实际服务器的抽象。下图显示了一个典型的内联部署。

图 1. 内联部署



在单臂模式下，设备只有一个网络接口连接到以太网段。在这种情况下，设备不会隔离网络的客户端和服务器端，而是通过配置的虚拟服务器提供对应用程序的访问。单臂模式可以简化在某些环境中安装 Citrix ADC 所需的网络更改。

有关内嵌（双臂）和单臂部署的示例，请参阅常见网络拓扑简介。

Citrix ADC 作为 L2 设备

作为 L2 设备的 Citrix ADC 装置据说在 L2 模式下工作。在 L2 模式下，ADC 设备在满足以下所有条件时在网络接口之间转发数据包：

- 数据包发送往另一台设备的介质访问控制 (MAC) 地址。
- 目标 MAC 地址位于不同的网络接口上。
- 该网络接口属于同一虚拟 LAN (VLAN) 的成员。

默认情况下，所有网络接口都是预定义的 VLAN (VLAN 1) 的成员。地址解析协议 (ARP) 请求和响应被转发到属于同一个 VLAN 的所有网络接口。为避免桥接环路，如果另一个 L2 设备与 Citrix ADC 设备并行工作，则必须禁用 L2 模式。

有关 L2 和 L3 模式的交互方式的信息，请参阅数据包转发模式。

有关配置 L2 模式的信息，请参阅数据包转发模式中的“启用和禁用第 2 层模式”部分。

Citrix ADC 作为数据包转发设备

Citrix ADC 设备可以用作数据包转发设备，此工作模式称为 L3 模式。启用 L3 模式后，如果存在到达目标的路由，设备将转发发往不属于设备的 IP 地址的所有已接收单播数据包。设备还可以在 VLAN 之间路由数据包。

在 2 层和 3 层两种工作模式下，设备通常会丢弃符合以下条件的数据包：

- 多播帧
- 发送给设备的 MAC 地址（非 IP 和非 ARP）的未知协议帧
- 跨树协议（除非 BridgeBPDU 为“ON”[已启用]）

有关 L2 和 L3 模式的交互方式的信息，请参阅数据包转发模式。

有关配置 L3 模式的信息，请参阅数据包转发模式。

Citrix ADC 设备如何与客户端和服务器通信

December 15, 2021

Citrix ADC 设备通常部署在服务器场的前面，用作客户端与服务器之间的透明 TCP 代理，无需进行任何客户端配置。这种基本工作模式称为“请求切换”技术，是 Citrix ADC 功能的核心。通过请求切换技术，设备能够对 TCP 连接进行多路复用和卸载，维护持续型连接并在请求（应用程序层）级别管理流量。这是可以实现的，因为设备可以将 HTTP 请求与传送请求的 TCP 连接分离。

根据配置，设备可以在将请求转发到服务器之前对流量进行处理。例如，如果客户端尝试访问服务器上的安全应用程序，设备可以在将流量发送到该服务器之前执行必要的 SSL 处理。

为便于安全高效地访问服务器资源，设备使用一组统称为 Citrix ADC 拥有的 IP 地址的 IP 地址。要管理网络流量，可以将 Citrix ADC 拥有的 IP 地址分配给作为配置构建基块的虚拟实体。例如，要配置负载平衡，可以创建虚拟服务器用于接收客户端请求，并将这些请求分配给服务（即，表示服务器上的应用程序的实体）。

Citrix ADC 拥有的 IP 地址简介

为了用作代理，Citrix ADC 设备使用多种 IP 地址。Citrix ADC 拥有的关键 IP 地址包括：

- Citrix ADC IP (NSIP) 地址

  NSIP 地址是用于进行管理、对设备本身进行常规系统访问以及在高可用性配置中实现设备间通信的 IP 地址。

- 虚拟服务器 IP (VIP) 地址

  VIP 地址是与虚拟服务器相关联的 IP 地址。它是客户端连接到的公用 IP 地址。管理多种流量的一个设备可配置有多个 VIP。

- 子网 IP (SNIP) 地址

  SNIP 地址用于连接管理和服务器监视。您可以为每个子网指定多个 SNIP 地址。SNIP 地址可以绑定到 VLAN。

- IP 集

  IP 集是一组 IP 地址，这些 IP 地址在设备上配置为 SNIP IP 集通过有意义的名称进行标识，这些名称有助于确定其中所含 IP 地址的用途。

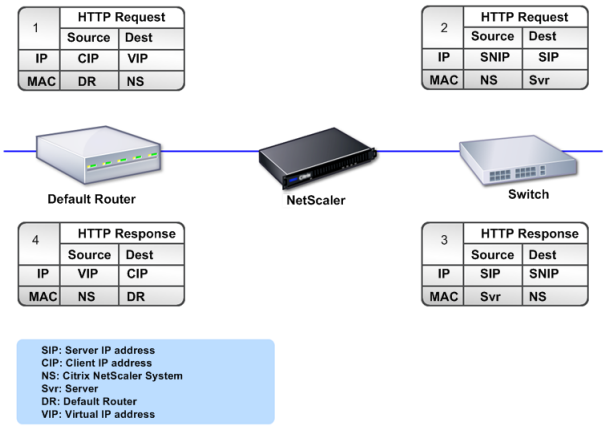
- 网络配置文件

  网络配置文件中包含一个 IP 地址或 IP 集。网络配置文件可绑定到负载平衡或内容交换虚拟服务器、服务、服务组或监视器。在与物理服务器或对等机通信期间，设备使用在配置文件中指定的地址作为源 IP 地址。

如何管理流量

由于 Citrix ADC 设备用作 TCP 代理，因此它会在将数据包发送到服务器之前转换 IP 地址。配置虚拟服务器时，客户端连接到 Citrix ADC 设备上的 VIP 地址，而不直接连接服务器。设备根据虚拟服务器上的设置，选择适当的服务器，并将客户端请求发送到该服务器。默认情况下，设备使用 SNIP 地址与服务器建立连接，如下图所示。

图 1. 基于虚拟服务器的连接



如果没有虚拟服务器，当设备收到请求时，会以透明方式将请求转发给服务器。这称为透明工作模式。在透明模式下工作时，设备可将传入客户端请求的源 IP 地址转换为 SNIP 地址，但不会更改目标 IP 地址。要使此模式生效，必须正确配置 L2 或 L3 模式。

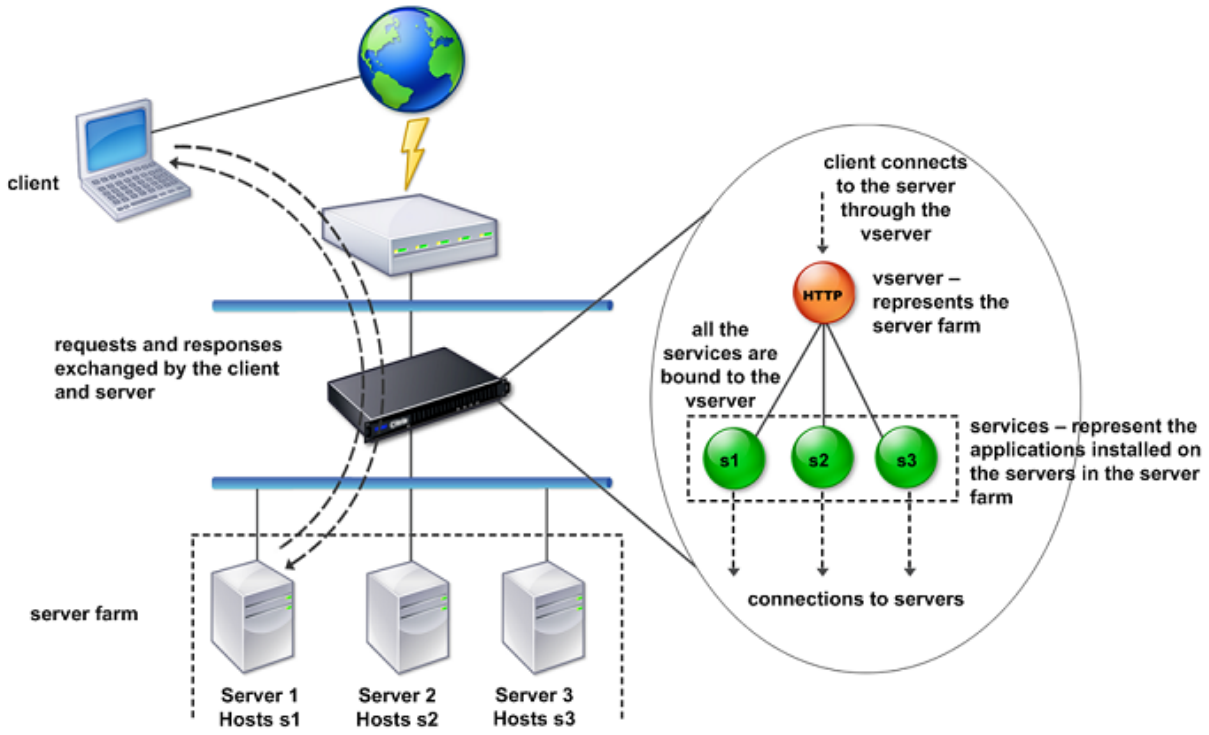
如果服务器需要使用实际客户端 IP 地址，可以将设备配置为通过插入客户端 IP 地址作为附加字段来修改 HTTP 标头，或配置为使用客户端 IP 地址而不是 SNIP 地址来连接服务器。

流量管理构建基块

Citrix ADC 设备的配置通常由作为流量管理构建基块的一系列虚拟实体组成。构建基块方法可帮助分离通信流量。虚拟实体是抽象概念，通常表示 IP 地址、端口以及用于处理流量的协议处理程序。客户端通过这些虚拟实体访问应用程序和资源。最常用的实体是虚拟服务器和服务。虚拟服务器表示服务器场或远程网络中的服务器组；服务表示每个服务器上的特定应用程序。

大多数功能和流量设置是通过虚拟实体启用的。例如，您可以通过特定的虚拟服务器配置设备，使其压缩连接到服务器场的客户端的所有服务器响应。要为特定的环境配置设备，您需要确定相应的功能，然后选择正确的虚拟实体组合以实现这些功能。大多数功能是通过互相绑定的级联结构的虚拟实体实现的。在这种情况下，虚拟实体就像组合到所交付应用程序的最终结构中的基块。您可以添加、删除、修改、绑定、启用和禁用虚拟实体以配置功能。下图说明了本节中涉及的概念。

图 2. 流量管理构建基块的工作原理



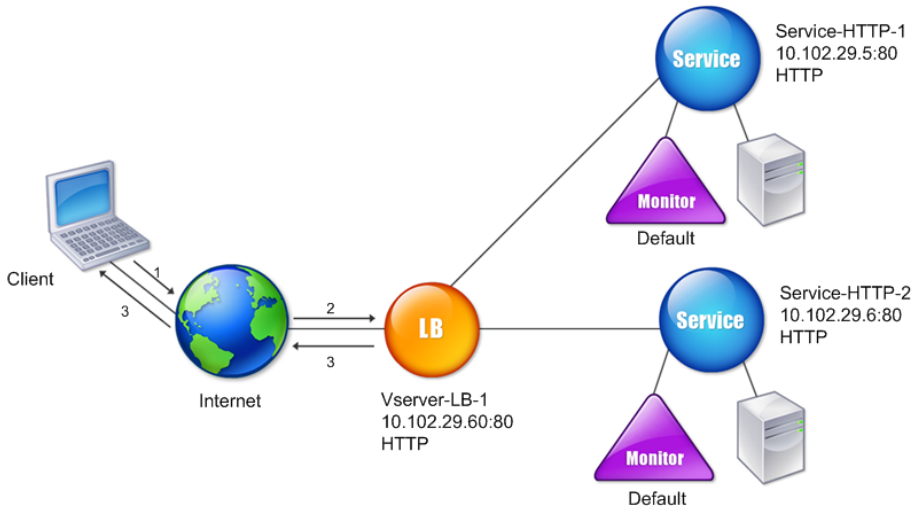
简单的负载平衡配置

在下图显示的示例中，Citrix ADC 设备配置为用作负载平衡器。对于此配置，您需要配置特定于负载平衡的虚拟实体，并按特定顺序对其进行绑定。作为负载平衡器，设备可在多个服务器之间分配客户端请求，从而优化资源的利用。

典型负载平衡配置的基本构建基块是服务和负载平衡虚拟服务器。服务表示服务器上的应用程序。虚拟服务器通过提供客户端要连接到的单个 IP 地址来实现服务器抽象化。要确保将客户端请求发送至服务器，您必须将每项服务绑定到虚拟服务器，即，您必须为每个服务器创建服务，并将这些服务绑定到虚拟服务器。客户端使用 VIP 地址连接到 Citrix ADC

设备。通过 VIP 地址收到客户端请求时，设备会将其发送到由负载平衡算法决定的服务器。负载平衡使用一个称为监视程序的虚拟实体，来跟踪某特定的已配置服务（服务器与应用程序）是否可用于接收请求。

图 3. 负载平衡虚拟服务器、服务和监视程序



除配置负载平衡算法外，您还可以配置多个可影响负载平衡配置行为和性能的参数。例如，可以将虚拟服务器配置为根据源 IP 地址维护持久性。然后，设备将来自任何特定 IP 地址的所有请求定向到同一台服务器。

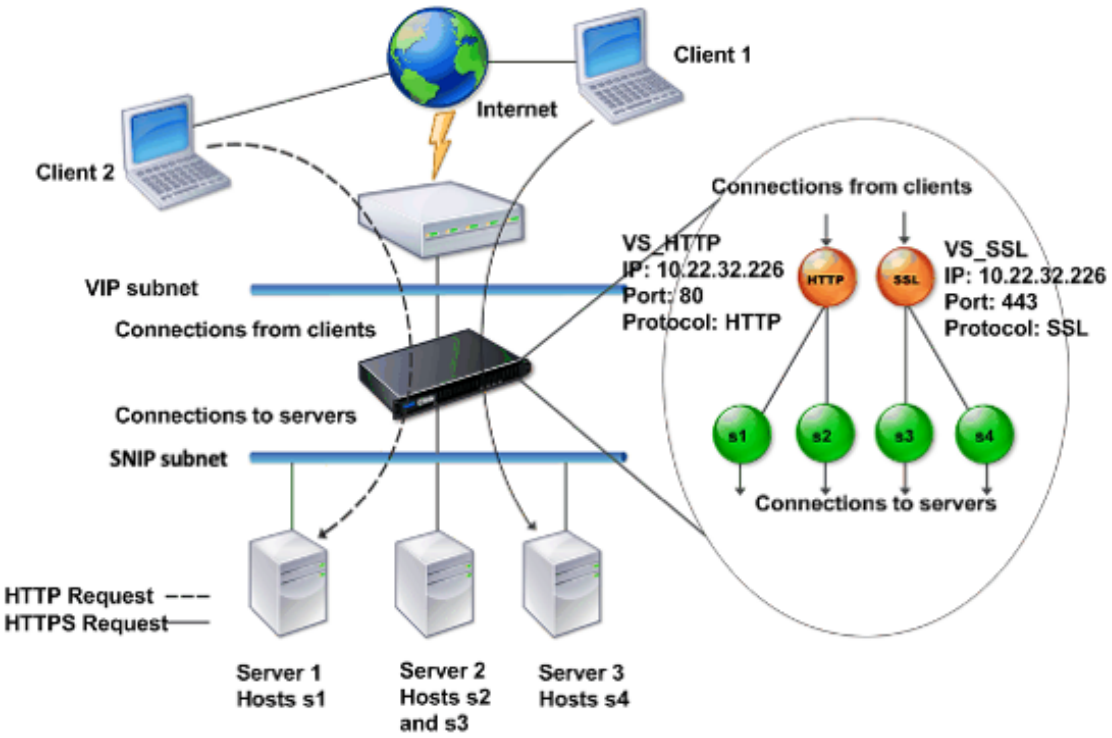
虚拟服务器简介

虚拟服务器是一个指定的 Citrix ADC 实体，外部客户端可以用它来访问服务器上托管的应用程序。虚拟服务器由字母数字名称、虚拟 IP (VIP) 地址、端口和协议表示。虚拟服务器的名称仅在本地有意义，旨在使虚拟服务器更易于识别。当客户端尝试访问服务器上的应用程序时，会将请求发送至 VIP 而不是物理服务器的 IP 地址。通过 VIP 地址收到请求时，设备将终止虚拟服务器上的连接，并代表客户端使用其与服务器之间的连接。虚拟服务器的端口和协议设置决定虚拟服务器所表示的应用程序。例如，Web 服务器可以由端口和协议分别设置为 80 和 HTTP 的虚拟服务器和服务表示。多个虚拟服务器可以使用相同的 VIP 地址，但必须使用不同的协议和端口。

虚拟服务器是提供各项功能的关键所在。大多数功能（例如压缩、缓存和 SSL 卸载）通常是在虚拟服务器上启用的。通过 VIP 地址收到请求时，设备将按照接收请求的端口及其协议选择适当的虚拟服务器。然后，设备根据在虚拟服务器上配置的功能对请求进行处理。

在大多数情况下，虚拟服务器与服务协同工作。您可以将多个服务绑定到一个虚拟服务器。这些服务表示在服务器场中的物理服务器上运行的各个应用程序。处理通过 VIP 地址收到的请求之后，设备会将其转发给由虚拟服务器上配置的负载平衡算法决定的服务器。下图说明了这些概念。

图 4. 多个虚拟服务器具有相同 VIP 地址



上图所示的配置由两个具有通用 VIP 地址但端口和协议不同的虚拟服务器组成。其中每个虚拟服务器都绑定了两种服务。服务 s1 和 s2 都绑定到 VS_HTTP，并且表示服务器 1 和服务器 2 上的 HTTP 应用程序。服务 s3 和 s4 都绑定到 VS_SSL，并且表示服务器 2 和服务器 3 上的 SSL 应用程序（服务器 2 同时提供 HTTP 和 SSL 应用程序）。通过 VIP 地址收到 HTTP 请求时，设备将根据 VS_HTTP 的设置处理请求，并将其发送给服务器 1 或服务器 2。同样，通过 VIP 地址收到 HTTPS 请求时，设备将根据 VS_SSL 的设置处理请求，并将其发送给服务器 2 或服务器 3。

虚拟服务器并非始终由特定 IP 地址、端口号或协议表示。还可由通配符表示，在这种情况下称为通配符虚拟服务器。例如，使用通配符而不是 VIP 配置虚拟服务器（但具有特定的端口号）时，设备将解释并处理所有符合该协议且发送给预定义端口的流量。对于使用通配符而不是 VIP 和端口号表示的虚拟服务器，设备将解释并处理所有符合该协议的流量。

虚拟服务器可以分组为以下类别：

- 负载平衡虚拟服务器

  接收请求并将请求重定向到适当的服务器。适当服务器的选择基于用户配置的负载平衡方法进行。

- 缓存重定向虚拟服务器

  将对动态内容和静态内容的客户端请求分别重定向到源服务器和缓存服务器。缓存重定向虚拟服务器通常与负载平衡虚拟服务器协同工作。

- 内容交换虚拟服务器

  根据客户端请求的内容将通信流定向到某个服务器。例如，您可以创建一个内容交换虚拟服务器，将对映像的所有客户端请求定向到仅提供映像的服务器。内容交换虚拟服务器通常与负载平衡虚拟服务器协同工作。

- 虚拟专用网络 (VPN) 虚拟服务器

  解密通道通信并将其发送给 Intranet 应用程序。

- SSL 虚拟服务器

  接收并解密 SSL 通信流，然后将其重定向到适当的服务器。适当服务器的选择与负载平衡虚拟服务器的选择相类似。

服务简介

服务表示服务器上的应用程序。虽然服务通常与虚拟服务器结合使用，但是在没有虚拟服务器的情况下，服务仍可以管理特定于应用程序的流量。例如，您可以在 Citrix ADC 设备上创建 HTTP 服务来表示 Web 服务器应用程序。当客户端尝试访问 Web 服务器上托管的 Web 站点时，设备会拦截 HTTP 请求，并创建与 Web 服务器之间的透明连接。

在仅服务模式下，设备用作代理。它可终止客户端连接，使用 SNIP 地址与服务器建立连接，并将传入客户端请求的源 IP 地址转换为 SNIP 地址。虽然客户端将请求直接发送至服务器的 IP 地址，但是服务器会将其视为来自 SNIP 地址。设备可转换 IP 地址、端口号和序列号。

服务也是应用功能的关键所在。以 SSL 加速为例。要使用此功能，必须创建一个 SSL 服务，并将 SSL 证书绑定到该服务。当收到 HTTPS 请求时，设备会将流量解密并以明文形式发送到服务器。在仅服务模式下只能配置有限的一组功能。

服务使用称为监视程序的实体来跟踪应用程序的运行状况。每项服务都绑定有一个默认监视程序（根据服务类型确定）。根据监视程序中配置的设置，设备每隔一定的时间向应用程序发送探测以确定其状态。如果探测失败，设备会将服务标记为 down（关闭）。在这种情况下，设备以相应的错误消息响应客户端请求，或根据配置的负载平衡策略重新路由这些请求。

Citrix ADC 产品线简介

January 9, 2023

Citrix ADC 产品线优化了通过 Internet 和专用网络实现的应用程序交付，从而将应用程序级别的安全性、优化和通信管理组合到单台集成设备中。可以将 Citrix ADC 设备安装在服务器机房中，并通过该设备路由托管服务器的所有连接。然后，您启用的 Citrix ADC 功能以及设置的策略将应用于传入通信和传出通信。

Citrix ADC 设备可以作为现有负载均衡器、服务器、缓存和防火墙的组件集成到任何网络中。它不需要额外的客户端或服务器端软件，可以使用其基于 Citrix ADC Web 的 GUI 和 CLI 配置实用程序进行配置。

本主题包括以下几个部分：

- Citrix ADC 硬件平台
- Citrix ADC 版本
- ADC 硬件支持的版本
- 支持的浏览器

Citrix ADC 硬件平台

Citrix ADC 硬件适用于具有一系列硬件规格的各种平台：

Citrix ADC MPX 硬件平台

Citrix ADC SDX 硬件平台

Citrix ADC 版本

Citrix ADC 操作系统有三个版本：

- Standard
- Advanced
- Premium

标准版和高级版的功能有限。所有版本均需要功能许可证。

有关 Citrix ADC 软件版本的详细信息，请参阅 Citrix ADC 版本数据手册。

有关如何获取和安装许可证的信息，请参阅许可。

Citrix ADC 硬件支持的版本

有关所有 Citrix ADC 硬件平台以及这些平台支持的软件版本，请参阅下面的兼容性列表：

Citrix ADC MPX 硬件-软件兼容性列表

Citrix ADC SDX 硬件-软件兼容性列表

支持的浏览器

要访问 Citrix ADC GUI，您的工作站必须具有受支持的 Web 浏览器。

下表列出了适用于 NetScaler GUI 版本 12.0、12.1 和 13.0 的兼容浏览器：

操作系统	浏览器	版本
Windows 7 及更高版本	Internet Explorer	11、Edge 及更高版本
Windows 7 及更高版本	Mozilla Firefox	45 及更高版本
Windows 7 及更高版本	Chrome	60 及更高版本
MAC	Mozilla Firefox	45 及更高版本
MAC	Safari	10.1.1 及更高版本

Citrix ADC 11.1 的兼容浏览器版本如下：

操作系统	浏览器	版本
Windows 7 及更高版本	Internet Explorer	8、9、10、11、Edge
Windows 7 及更高版本	Mozilla Firefox	45 及更高版本
Windows 7 及更高版本	Chrome	60 及更高版本
MAC	Mozilla Firefox	45 及更高版本
MAC	Safari	10.1.1 及更高版本

安装硬件

January 9, 2023

安装 Citrix ADC 设备之前，请先查看安装前核对表。

要使用 SDX 设备，您必须按照表中提供的资源中的说明完成以下任务。按照给定的顺序完成任务。

任务

说明

1. 阅读安全、小心、警告及其他信息

   在安装产品之前，请阅读您需要了解的注意事项和危险信息。

2. 准备安装

   打开设备的包装，确保所有部件都已交付，准备场地和机架，并在安装新设备之前遵循基本的电气安全预防措施。

3. 安装硬件

   在机架中安装设备，安装收发器（如果可用），然后将设备连接到网络和电源。

4. 配置设备。

使用 GUI 或串行控制台配置 Citrix ADC 设备的初始设置。

请按照以下文档中提供的步骤完成这些任务：

- Citrix ADC MPX 硬件文档
- Citrix ADC SDX 硬件文档

访问 **Citrix ADC** 设备

April 15, 2024

Citrix ADC 设备具有命令行界面 (CLI) 和 GUI。GUI 包含用于配置设备的配置实用程序，以及名为“控制板”的统计实用程序。对于初始访问，所有设备出厂时均配置了默认 Citrix ADC IP 地址 (NSIP) 192.168.100.1 和默认子网掩码 255.255.0.0。您可以在初始配置期间分配新的 NSIP 和关联的子网掩码。

如果在部署多台 Citrix ADC 设备时遇到 IP 地址冲突，请检查以下可能的原因：

- 所选的 NSIP 是否为已分配给网络中其他设备的 IP 地址？
- 是否将同一个 NSIP 分配给了多台 Citrix ADC 设备？
- 可通过所有物理端口访问 NSIP。Citrix ADC 上的端口是主机端口而不是交换机端口。

下表汇总了可用的访问方法。

访问方法	端口	是否需要默认 IP 地址？（是/否）
CLI	控制台	N
CLI 和 GUI	以太网	Y

命令行接口

可以通过以下两种方式访问 CLI：将工作站连接到控制台端口进行本地访问，或者通过安全外壳 (SSH) 从同一网络中的任何工作站连接以进行远程访问。

通过控制台端口登录命令行接口

设备有一个控制台端口，用于连接到计算机工作站。要登录到设备，需要使用串行交叉电缆以及安装有终端仿真程序的工作站。

要通过控制台端口登录 CLI，请执行以下步骤：

1. 将控制台端口连接到工作站上的串行端口。有关详细信息，请参阅连接控制台电缆。
2. 在工作站上，启动超级终端或任何其他终端仿真程序。如果未显示登录提示，您可能需要按 Enter 键一次或多次以显示该提示。
3. 在“User Name”（用户名）中，键入 `nsroot`。在“Password”（密码）中，键入 `nsroot`，如果该密码不起作用，请尝试键入设备的序列号。序列号条形码位于设备背面。

使用 **SSH** 登录命令行接口

SSH 协议是从同一网络中的任何工作站远程访问设备的首选远程访问方法。可以使用 SSH 版本 1 (SSH1) 或 SSH 版本 2 (SSH2)。

如果您没有可用的 SSH 客户端，可以下载并安装以下任意 SSH 客户端程序：

- PuTTY

  在多个平台上支持的开源软件。下载地址：

  http://www.chiark.greenend.org.uk/~sgtatham/putty/

- `Vandyke` Software SecureCRT

  在 Windows 平台上支持的商业软件。下载地址：

  http://www.vandyke.com/products/securecrt/

上述程序均已通过 Citrix ADC 团队的测试，证实其可以与 Citrix ADC 设备一起正常运行。其他程序可能也正常运行，但尚未经过测试。

要验证 SSH 客户端是否安装正确，请使用该客户端连接到您的网络中接受 SSH 连接的任何设备。

要使用 SSH 客户端登录 Citrix ADC 设备，请按照以下步骤进行操作：

1. 在您的工作站上启动 SSH 客户端。
2. 对于初始配置，请使用默认 IP 地址 (NSIP)，即 192.168.100.1。对于后续的访问，请使用初始配置期间指定的 NSIP。选择 SSH1 或 SSH2 作为协议。
3. 在“User Name”（用户名）中，键入 `nsroot`。在“Password”（密码）中，键入 `nsroot`，如果该密码不起作用，请尝试键入设备的序列号。序列号条形码位于设备背面。例如：

```
login as: nsroot


```



```
Using keyboard-interactive authentication.


Password:


Last login: Tue Jun 16 10:37:28 2009 from 10.102.29.9




Done


>

<!--NeedCopy-->
```

Citrix ADC GUI

> 重要：
>
> 通过 HTTPS 访问 Citric ADC GUI 需要证书-密钥对。在 ADC 上，证书-密钥对会自动绑定到内部服务。在 MPX 或 SDX 设备上，默认密钥大小为 1024 字节，在 VPX 实例上，默认密钥大小为 512 字节。但是，现今的大多数浏览器都不接受小于 1024 字节的密钥。因此，通过 HTTPS 访问 VPX 配置实用程序将被阻止。

此外，如果启动时 MPX 设备上不存在许可证，而您稍后添加许可证并重新启动设备，则可能会丢失证书绑定。

Citrix 建议您在 Citrix ADC 上安装至少 1024 字节的证书密钥对，以便 HTTPS 访问 GUI。此外，在启动 ADC 之前，请安装恰当的许可证。

GUI 包括一个配置实用程序和一个名为“控制板”的统计实用程序，您可以通过连接到设备上的以太网端口的工作站访问这两个实用程序。

运行 GUI 的工作站的系统要求如下：

- 对于基于 Windows 的工作站，需要 Pentium 166 MHz 或更快的处理器。
- 对于基于 Linux 的工作站，建议使用运行 Linux 内核 v2.2.12 或更高版本的 Pentium 平台以及 `glibc` 2.12-11 或更高版本。至少需要 32 MB 的 RAM，建议使用 48 MB 的 RAM。工作站必须支持 16 位色模式、结合使用 KDE 和 KWM 窗口管理器，并且将显示设置为本地主机。
- 对于基于 Solaris 的工作站，需要运行 Solaris 2.6、Solaris 7 或 Solaris 8 的 Sun。

工作站必须安装受支持的 Web 浏览器才能访问配置实用程序和控制板。

支持以下浏览器。

操作系统：
Windows 7

浏览器：Internet Explorer（版本 9、10 和 11）、Mozilla Firefox（版本 3.6.25 及更高版本）、Google Chrome（最新版本）。

操作系统：
Windows 64 位

浏览器：Internet Explorer（版本 8、9、10 和 11）、Google Chrome（最新版本）

操作系统：
MAC
浏览器：Mozilla Firefox（版本 3.6.25 及更高版本），Safari（版本 5.1.3 及更高版本）、Google Chrome（最新版本）

使用 **Citrix ADC GUI**

登录到配置实用程序后，即可通过包含上下文相关帮助的图形界面配置设备。

要登录 GUI，请按照以下步骤进行操作：

1. 打开 Web 浏览器，并输入 Citrix ADC IP (NSIP) 作为 HTTP 地址。如果您尚未设置初始配置，请输入默认 NSIP (`http://192.168.100.1`)。系统将显示 Citrix Logon（Citrix 登录）页面。

   注意：如果有两台 Citrix ADC 设备具有高可用性设置，请勿通过输入辅助 Citrix ADC 设备的 IP 地址来访问 GUI。如果您执行此操作并使用 GUI 配置辅助设备，您的配置更改将不会应用到主 Citrix ADC 设备。

2. 在“User Name”（用户名）文本框中，键入 `nsroot`。
3. 在“Password”（密码）文本框中，键入在初始配置期间分配给 `nsroot` 帐户的管理密码，然后单击 **Login**（登录）。如果该密码不起作用，请尝试键入设备的序列号。序列号条形码位于设备背面。

   要访问联机帮助，请从右上角的“Help”（帮助）菜单中选择“Help”（帮助）。

使用统计实用程序

控制板（即统计实用程序）是一款基于浏览器的应用程序，显示可用于监视 Citrix ADC 设备性能的图和表。

要登录控制板，请按照以下步骤进行操作：

1. 打开 Web 浏览器，并输入 NSIP 作为 HTTP 地址。系统将显示 Citrix Logon（Citrix 登录）页面。
2. 在 **User Name**（用户名）文本框中，键入 `nsroot`。
3. 在 **Password**（密码）文本框中，键入在初始配置期间分配给 `nsroot` 帐户的管理密码。如果该密码不起作用，请尝试键入设备的序列号。序列号条形码位于设备背面。

首次配置 ADC

January 9, 2023

有关 Citrix ADC MPX 设备的初始配置，请参阅 Citrix MPX 设备的初始配置。

有关 Citrix SDX 设备的初始配置，请参阅 Citrix SDX 设备的初始配置。

NITRO API

可以使用 NITRO API 配置 Citrix ADC 设备。NITRO 通过表述性状态转移 (REST) 接口提供功能。因此，可以用任何编程语言来开发 NITRO 应用程序。此外，对于必须以 Java 或.NET 或 Python 开发的应用程序，NITRO API 将通过打包为独立软件开发工具包 (SDK) 的相关库提供。有关详细信息，请参阅 NITRO API。

保护您的 Citrix ADC 部署

February 16, 2024

为了在 Citrix ADC 设备的部署生命周期内维护安全性，Citrix 建议您考虑以下安全设置：

- 物理安全性
- 设备安全性
- 网络安全性
- 管理

不同的部署可能需要考虑不同的安全注意事项。Citrix ADC 安全部署指南提供了一般性安全指导，帮助您根据特定的安全要求决定适当的安全部署。

有关安全部署 Citrix ADC 设备的指导的详细信息，请参阅 Citrix ADC 安全部署指南。

配置高可用性

December 15, 2021

可以在高可用性配置中部署两台 Citrix ADC 设备，其中一台设备主动接受连接并管理服务器，而辅助设备负责监视第一台设备。在高可用性配置中，主动接受连接并管理服务器的 Citrix ADC 设备称为主设备，另一台称为辅助设备。如果主设备出现故障，则辅助设备将成为主设备，并开始主动接受连接。

高可用性对中的每台 Citrix ADC 设备通过发送定期消息（称为检测信号消息或运行状况检查）来监视另一台设备，从而确定对等节点的运行状况或状态。如果主设备的运行状况检查失败，则辅助设备将在特定时间段内重试连接。有关高可用性的详细信息，请参阅高可用性。如果在指定时间段结束时重试仍失败，辅助设备将在故障转移过程中接替主设备。下图显示了两种高可用性配置，一种是单臂模式，另一种是双臂模式。

图 1. 单臂模式下的高可用性

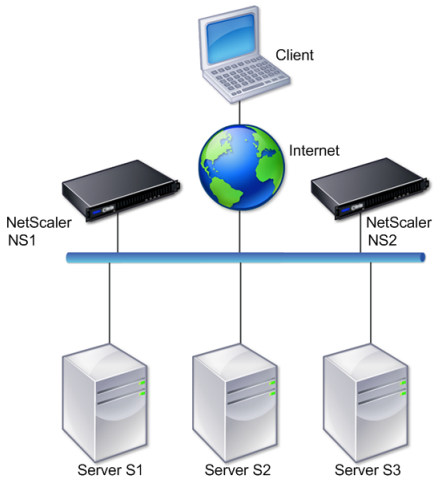
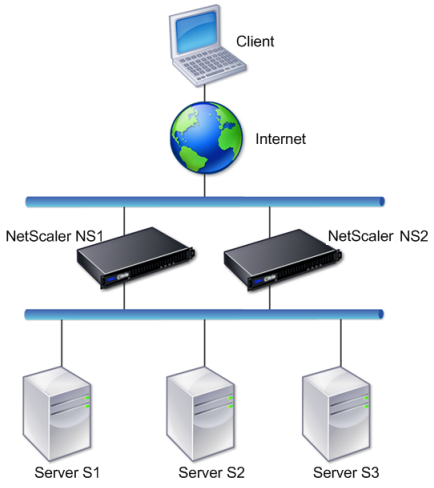


图 2. 双臂模式下的高可用性



在单臂配置中，NS1 和 NS2 以及服务器 S1、S2 和 S3 均连接到交换机。

在双臂配置中，NS1 和 NS2 均连接到两个交换机。服务器 S1、S2 和 S3 均连接到第二个交换机。客户端与服务器之间的流量经过 NS1 或 NS2。

要设置高可用性环境，请将一个 ADC 设备配置为主设备，将另一个配置为辅助设备。请在每个 ADC 设备上执行以下任务：

- 添加节点。
- 对未使用的接口禁用高可用性监视功能。

添加节点

节点是对等 Citrix ADC 设备的逻辑表示形式。它通过 ID 和 NSIP 标识对等单元。设备使用这些参数与对等单元进行通信并跟踪其状态。添加节点时，主设备和辅助设备将异步交换检测信号消息。节点 ID 是一个不能大于 64 的整数。

通过 **CLI**

要使用命令行界面添加节点，请按照以下步骤进行操作：

在命令提示窗口中，键入以下命令以添加节点并验证节点是否成功添加：

- add HA node <id> <IPAddress>
- show HA node <id>

  示例

```
 add HA node 0 10.102.29.170
  Done
> show HA node 0
 1)      Node ID:      0
         IP:   10.102.29.200 (NS200)
         Node State: UP
         Master State: Primary
         SSL Card Status: UP
         Hello Interval: 200 msecs
         Dead Interval: 3 secs
         Node in this Master State for: 1:0:41:50 (days:hrs:min:
            sec)
 <!--NeedCopy-->
```

通过 **GUI**

要使用 GUI 添加节点，请按照以下步骤进行操作：

1. 导航到 **System**（系统）> **High Availability**（高可用性）。
2. 在 **Nodes**（节点）选项卡上单击 **Add**（添加）。
3. 在 **Create HA Node**（创建高可用性节点）页面上的 **Remote Node IP Address**（远程节点 IP 地址）文本框中，键入远程节点的 NSIP 地址（例如 10.102.29.170）。

4. 确保选中 **Configure remote system to participate in High Availability setup**（将远程系统配置为加入高可用性设置）复选框。在 **Remote System Login Credentials**（远程系统登录凭据）下的文本框中提供远程节点的登录凭据。
5. 选中 **Turn off HA monitor on interfaces/channels that are down**（在已关闭的接口/通道上关闭高可用性监视程序）复选框，对关闭的接口禁用高可用性监视程序。

确认您添加的节点显示在“Nodes”（节点）选项卡下的节点列表中。

对未使用的接口禁用高可用性监视功能

高可用性监视程序是用于监视接口的虚拟实体。必须对未连接或未用于通信的接口禁用该监视程序。对状态为“DOWN”（关闭）的接口启用该监视程序后，节点的状态将变为“NOT UP”（不可用）。在高可用性配置中，进入“NOT UP”（不可用）状态的主节点可能会导致高可用性故障转移。接口在以下情况下会被标记为“DOWN”（关闭）：

- 接口未连接
- 接口运行不正常
- 连接接口的电缆工作不正常

通过 **CLI**

要使用命令行接口对未使用的接口禁用高可用性监视程序，请执行以下步骤：

在命令提示窗口中，键入以下命令以对未使用的接口禁用高可用性监视程序，并验证是否成功禁用：

- set interface <id> -haMonitor OFF
- show interface <id>

  示例

```
> set interface 1/8 -haMonitor OFF
  Done
> show interface 1/8
        Interface 1/8 (Gig Ethernet 10/100/1000 MBits) #2
        flags=0x4000 <ENABLED, DOWN, down, autoneg, 802.1q>
        MTU=1514, native vlan=1, MAC=00:d0:68:15:fd:3d, downtime
            238h55m44s
        Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
                 throughput 0

        RX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        TX: Pkts(0) Bytes(0) Errs(0) Drops(0) Stalls(0)
        NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0)
            Muted(0)
        Bandwidth thresholds are not set.
 <!--NeedCopy-->
```

  如果已对某个未使用的接口禁用高可用性监视程序，该接口的 show interface 命令输出中将不包含“HAMON”。

通过 **GUI**

要使用 GUI 禁用未使用的接口的高可用性监视器，请按照以下步骤进行操作：

1. 导航到 System（系统）> Network（网络）> Interfaces（接口）。
2. 选择必须对其禁用监视程序的接口。
3. 单击打开。此时将显示 Modify Interface（修改接口）对话框。
4. 在 HA Monitoring（高可用性监视功能）中，选择 OFF（关闭）选项。
5. 单击确定。
6. 确认当选择该接口时，在页面底部的“Details”（详细信息）部分中显示“HA Monitoring: OFF”（高可用性监视功能: 已关闭）。

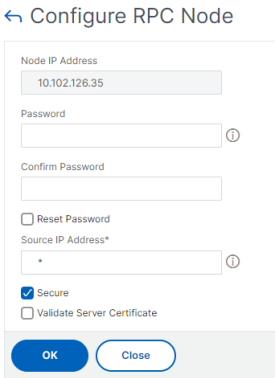
更改 **RPC** 节点密码

December 15, 2021

要与其他 Citrix ADC 设备通信，每个设备都需要了解其他设备，包括如何在 Citrix ADC 设备上进行身份验证。RPC 节点是内部系统实体，用于系统与系统之间的配置和会话信息通信。每个 Citrix ADC 设备上都有一个 RPC 节点，用于存储信息，例如另一个 Citrix ADC 设备的 IP 地址和用于身份验证的密码。与其他 Citrix ADC 设备联系的 Citrix ADC 设备将在 RPC 节点中检查密码。

使用 **GUI** 更改 **RPC** 节点密码

1. 导航到 **System**（系统）> **Network**（网络）> **RPC**。
2. 在 **RPC** 窗格中，选择节点，然后单击 **Edit**（编辑）。
3. 在配置 **RPC** 节点中，键入新密码。
4. 在 **Source IP Address**（源 IP 地址）中，键入用于与对等系统节点通信的现有节点的 IP 地址。



5. 选择 **Secure**（安全），然后单击 **OK**（确定）。

> 注意
>
> 启用 **Secure**（安全）选项后，设备会对从节点发送到其他 RPC 节点的所有通信进行加密，从而保护 RPC 通信。

使用 **CLI** 更改 **RPC** 节点密码

在命令行中，键入以下命令：

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]
show ns rpcNode
<!--NeedCopy-->
```

示例：

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>

<!--NeedCopy-->
```

首次配置 **FIPS** 设备

December 20, 2021

> 备注
>
> - 可以在此处找到 FIPS 常见问题解答：FIPS 常见问题解答。
> - 可以在此处找到 VPX FIPS 配置：Citrix ADC VPX FIPS 认证的设备。

要对配置实用程序进行 HTTPS 访问并保护远程过程调用，需要证书-密钥对。RPC 节点是内部系统实体，用于系统与系统之间的配置和会话信息通信。每个设备上都有一个 RPC 节点。此节点可存储密码，针对通过联系设备提供的密码进行核对。要与其他 Citrix ADC 设备通信，每个设备都需要了解其他设备，包括如何在其他设备上进行身份验证。RPC 节点维护该信息，包括其他 Citrix ADC 设备的 IP 地址以及用于在每台设备上进行身份验证的密码。

在 Citrix ADC MPX 设备虚拟设备上，证书-密钥对会自动绑定到内部服务。在 FIPS 设备上，必须将证书-密钥对导入到 FIPS 卡的硬件安全模块 (HSM) 中。要执行此操作，必须配置 FIPS 卡，创建证书-密钥对，并将其绑定到内部服务。

使用 **CLI** 配置安全 **HTTPS**

要使用 CLI 配置安全 HTTPS，请按照以下步骤进行操作

1. 在设备的 FIPS 卡上初始化硬件安全模块 (HSM)。有关初始化 HSM 的信息，请参阅配置 HSM。
2. 如果设备是高可用性设置的一部分，请启用 SIM。有关在主设备和辅助设备上启用 SIM 的信息，请参阅在高可用性设置中配置 FIPS 设备。
3. 将 FIPS 密钥导入到设备的 FIPS 卡的 HSM 中。在命令提示符下，键入：

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. 添加证书-密钥对。在命令提示符下，键入：

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. 将上一步中创建的证书-密钥绑定到以下内部服务。在命令提示符下，键入：

   ```
   bind ssl service nshttps-127.0.0.1-443 -certkeyname server
   bind ssl service nshttps-::11-443 -certkeyname server
   ```

使用 **GUI** 配置安全 **HTTPS**

要使用 GUI 配置安全 HTTPS，请按照以下步骤进行操作：

1. 在设备的 FIPS 卡上初始化硬件安全模块 (HSM)。有关初始化 HSM 的信息，请参阅配置 HSM。
2. 如果设备是高可用性设置的一部分，请启用安全信息系统 (SIM)。有关在主设备和辅助设备上启用 SIM 的信息，请参阅在高可用性设置中配置 FIPS 设备。
3. 将 FIPS 密钥导入到设备的 FIPS 卡的 HSM 中。有关导入 FIPS 密钥的详细信息，请参阅导入现有 FIPS 密钥部分。
4. 导航到 **Traffic Management**（流量管理）**> SSL > Certificates**（证书）。
5. 在详细信息窗格中，单击 **Install**（安装）。
6. 在 Install Certificate（安装证书）对话框中，键入证书详细信息。
7. 单击 **Create**（创建），然后单击 **Close**（关闭）。
8. 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）。
9. 在详细信息窗格中的 **Action**（操作）选项卡上，单击 **Internal Services**（内部服务）。
10. 从列表中选择 `nshttps-127.0.0.1-443`，然后单击 **Open**（打开）。
11. 在 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）窗格中，选择在步骤 7 中创建的证书，单击 **Add**（添加），然后单击 **OK**（确定）。
12. 从列表中选择 `nshttps-::11-443`，然后单击 **Open**（打开）。

13. 在 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）窗格中，选择在步骤 7 中创建的证书，单击 **Add**（添加），然后单击 **OK**（确定）。
14. 单击确定。

使用 **CLI** 配置安全 **RPC**

要使用 CLI 配置安全 RPC，请按照以下步骤进行操作：

1. 在设备的 FIPS 卡上初始化硬件安全模块 (HSM)。有关初始化 HSM 的信息，请参阅配置 HSM。
2. 启用安全信息系统 (SIM)。有关在主设备和辅助设备上启用 SIM 的信息，请参阅在高可用性设置中配置 FIPS 设备。
3. 将 FIPS 密钥导入到设备的 FIPS 卡的 HSM 中。在命令提示符下，键入：

   ```
   import ssl fipskey serverkey -key ns-server.key -inform PEM
   ```

4. 添加证书-密钥对。在命令提示符下，键入：

   ```
   add certkey server -cert ns-server.cert -fipskey serverkey
   ```

5. 将证书-密钥对绑定到以下内部服务。在命令提示符下，键入：

   ```
   bind ssl service nsrpcs-127.0.0.1-3008 -certkeyname server
   bind ssl service nskrpcs-127.0.0.1-3009 -certkeyname server
   bind ssl service nsrpcs-::1l-3008 -certkeyname server
   ```

6. 启用安全 RPC 模式。在命令提示符下，键入：

   ```
   set ns rpcnode <IP address> -secure YES
   ```

   有关更改 RPC 节点密码的详细信息，请参阅更改 RPC 节点密码。

使用 **GUI** 配置安全 **RPC**

要使用 GUI 配置安全 RPC，请按照以下步骤进行操作：

1. 在设备的 FIPS 卡上初始化硬件安全模块 (HSM)。有关初始化 HSM 的信息，请参阅配置 HSM。
2. 启用安全信息系统 (SIM)。有关在主设备和辅助设备上启用 SIM 的信息，请参阅在高可用性设置中配置 FIPS 设备。
3. 将 FIPS 密钥导入到设备的 FIPS 卡的 HSM 中。有关导入 FIPS 密钥的详细信息，请参阅导入现有 FIPS 密钥部分。
4. 导航到 **Traffic Management**（流量管理）**> SSL > Certificates**（证书）。
5. 在详细信息窗格中，单击 **Install**（安装）。
6. 在 **Install Certificate**（安装证书）对话框中，键入证书详细信息。

7. 单击 **Create**（创建），然后单击 **Close**（关闭）。
8. 导航到 **Traffic Management**（流量管理）**> Load Balancing**（负载平衡）**> Services**（服务）。
9. 在详细信息窗格中的 **Action**（操作）选项卡上，单击 **Internal Services**（内部服务）。
10. 从列表中选择 `nsrpcs-127.0.0.1-3008`，然后单击 **Open**（打开）。
11. 在 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）窗格中，选择在步骤 7 中创建的证书，单击 **Add**（添加），然后单击 **OK**（确定）。
12. 从列表中选择 `nskrpcs-127.0.0.1-3009`，然后单击 **Open**（打开）。
13. 在 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）窗格中，选择在步骤 7 中创建的证书，单击 **Add**（添加），然后单击 **OK**（确定）。
14. 从列表中选择 `nsrpcs-::11-3008`，然后单击 **Open**（打开）。
15. 在 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）窗格中，选择在步骤 7 中创建的证书，单击 **Add**（添加），然后单击 **OK**（确定）。
16. 单击确定。
17. 导航到 **System**（系统）**> Network**（网络）**> RPC**。
18. 在详细信息窗格中，选择“IP address”（IP 地址）并单击 **Open**（打开）。
19. 在 **Configure RPC Node**（配置 RPC 节点）对话框中，选择 **Secure**（安全）。
20. 单击确定。

通用网络拓扑

December 20, 2021

如 Citrix ADC 设备适用于网络中的哪个位置? 中的“物理部署模式”部分中所述，您既可以在客户端与服务器之间以内嵌方式部署 Citrix ADC 设备，也可以在单臂模式下进行部署。内嵌模式使用双臂拓扑，这是最常见的一种部署类型。

设置通用双臂拓扑

在双臂拓扑中，一个网络接口连接到客户端网络，另一个网络接口连接到服务器网络，从而确保所有流量均流经此设备。此拓扑可能要求您重新连接硬件，并且还可能会导致暂时停机。双臂拓扑的基本变体包括多个子网和透明模式。前者通常是设备位于公用子网中，服务器位于专用子网中，后者是设备和服务器均位于公用网络中。

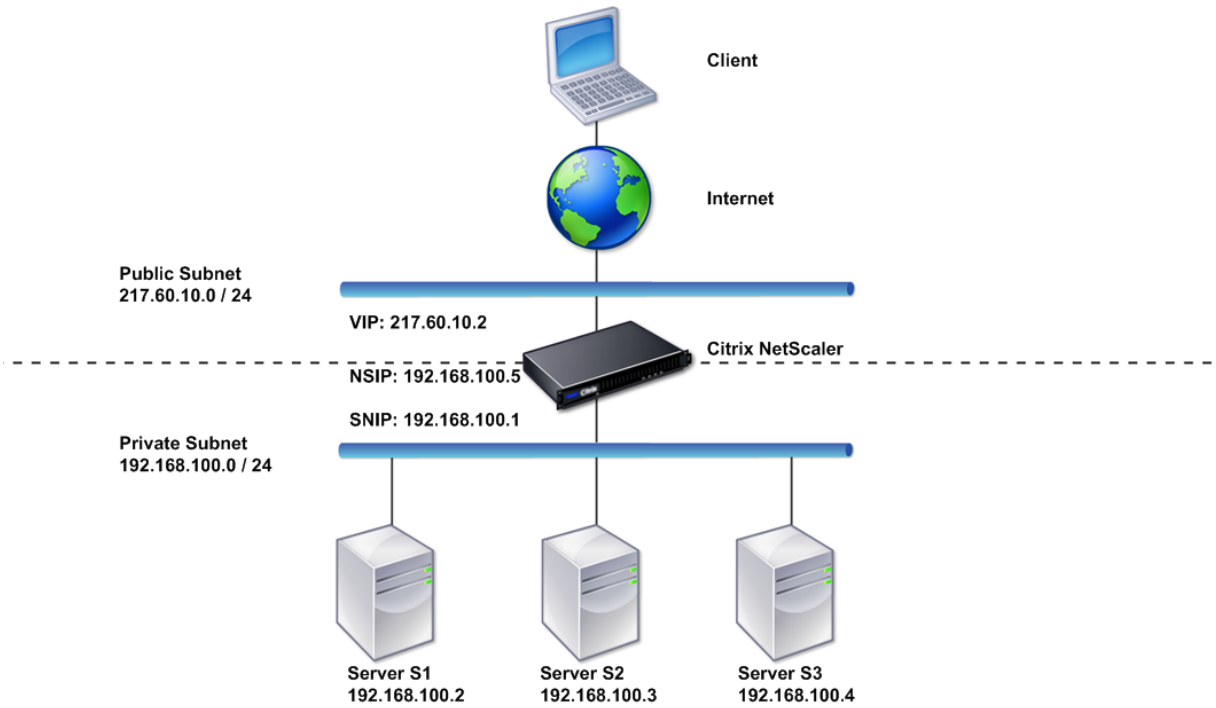
设置简单的双臂多子网拓扑

最常用的一种拓扑是将 Citrix ADC 设备置于客户端与服务器之间，并配置一个虚拟服务器来处理客户端请求。此配置在客户端与服务器位于不同的子网中时使用。在大多数情况下，客户端和服务器分别位于公用子网和专用子网中。

例如，假设在双臂模式下部署的设备用于管理服务器 S1、S2 和 S3，在设备上配置了一个 HTTP 类型的虚拟服务器，并且这些服务器上运行有 HTTP 服务。这些服务器位于专用子网中，并且在设备上配置了一个 SNIP 与这些服务器进行通信。必须在设备上启用“Use SNIP”（使用 SNIP）选项，以便它使用 SNIP 而不是 MIP。

如下图所示，VIP 位于公用子网 217.60.10.0 中，而 NSIP、服务器和其他 SNIP 位于专用子网 192.168.100.0/24 中。

图 1. 多子网、双臂模式拓扑图



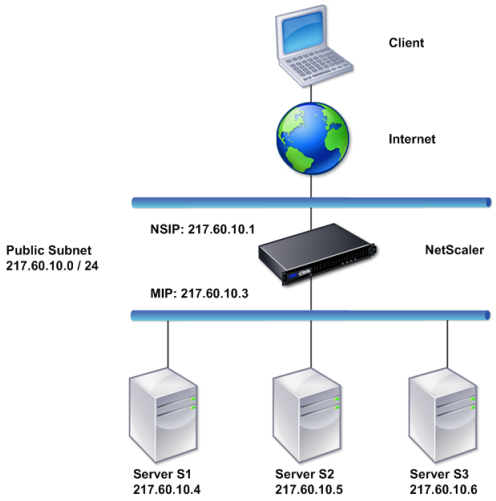
要在具有多个子网的双臂模式下部署 Citrix ADC 设备，请执行以下步骤：

1. 按照配置 NetScaler IP 地址 (NSIP) 中所述配置 NSIP 和默认网关。
2. 按照配置子网 IP 地址中所述配置 SNIP。
3. 按照启用或禁用 USNIP 模式中所述启用 USNIP 选项。
4. 按照创建虚拟服务器部分和配置服务部分中所述配置虚拟服务器和服务。
5. 将其中一个网络接口连接到专用子网，将另一个接口连接到公用子网。

设置简单的双臂透明拓扑

如果客户端需要直接访问服务器而不干扰虚拟服务器，可使用透明模式。服务器 IP 地址必须是公共的，因为客户端需要能够访问这些服务器。在下图显示的示例中，Citrix ADC 设备位于客户端与服务器之间，因此流量必须经由此设备。您必须启用第 2 层模式才能桥接数据包。NSIP 和 MIP 位于同一个公用子网 217.60.10.0/24 中。

图 2. 双臂、透明模式拓扑图



要在双臂透明模式下部署 Citrix ADC 设备，请执行以下步骤

1. 按照配置 NetScaler IP 地址 (NSIP) 中所述配置 NSIP 和默认网关。
2. 启用 L2 模式，如启用和禁用第 2 层模式中所述。
3. 将托管服务器的默认网关配置为 MIP。
4. 将网络接口连接到交换机上的相应端口。

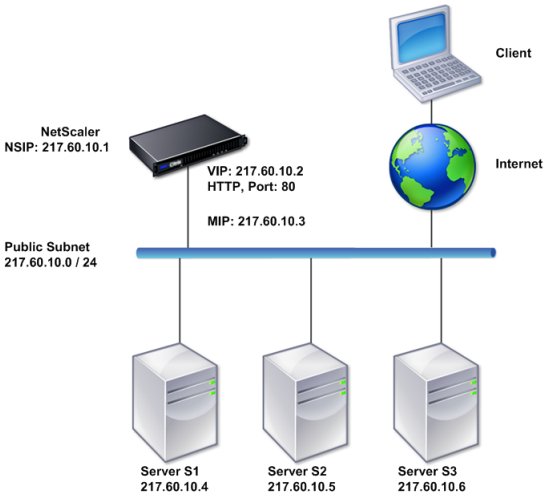
设置常见的单臂拓扑

具有单个子网的单臂拓扑和具有多个子网的单臂拓扑是单臂拓扑的两个基本变体。

设置简单的单臂单子网拓扑

如果客户端与服务器位于同一个子网中，则可以使用具有单个子网的单臂拓扑。例如，假设在单臂模式下部署的 Citrix ADC 设备用于管理服务器 S1、S2 和 S3。在 ADC 设备上配置了一个 HTTP 类型的虚拟服务器，并且在这些服务器上运行有 HTTP 服务。如下图所示，Citrix ADC IP 地址 (NSIP)、映射 IP 地址 (MIP) 和服务器 IP 地址位于同一个公用子网 217.60.10.0/24 中。

图 3. 单子网、单臂模式拓扑图



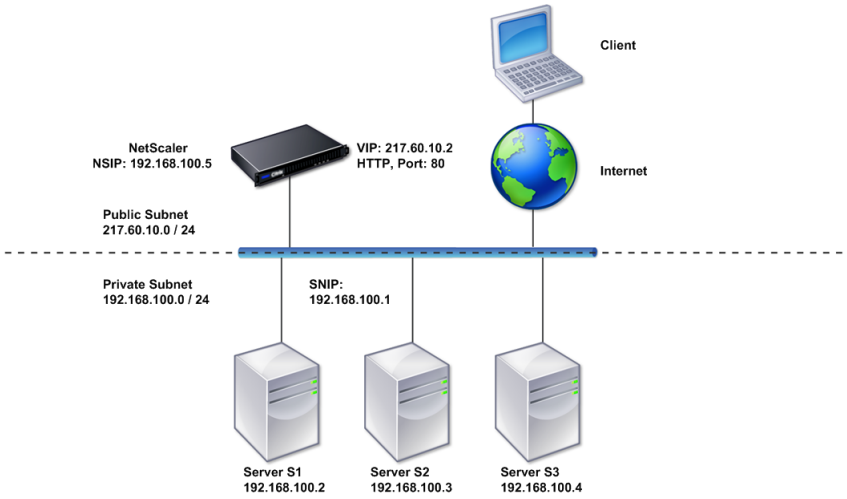
要在单臂模式下部署 Citrix ADC 设备，请按照下列步骤操作：

1. 按照配置 Citrix ADC IP 地址 (NSIP) 中所述配置 NSIP 和默认网关。
2. 按照创建虚拟服务器部分和配置服务部分中所述配置虚拟服务器和服务。
3. 将其中一个网络接口连接到交换机。

设置简单的单臂多子网拓扑

如果客户端与服务器位于在不同的子网中，则可以使用具有多个子网的单臂拓扑。例如，假设在单臂模式下部署的 Citrix ADC 设备用于管理服务器 S1、S2 和 S3，这些服务器连接到网络中的交换机 SW1。在该设备上配置了一个 HTTP 类型的虚拟服务器，并且在这些服务器上运行有 HTTP 服务。这三个服务器位于专用子网中，因此配置了一个子网 IP 地址 (SNIP) 用于与其通信。必须启用“Use Subnet IP address (USNIP)”（使用子网 IP 地址 (USNIP)）选项，以便该设备使用 SNIP 而不是 MIP。如下图所示，虚拟 IP 地址 (VIP) 位于公用子网 217.60.10.0/24 中；NSIP、SNIP 和服务器 IP 地址位于专用子网 192.168.100.0/24 中。

图 4. 多子网、单臂模式拓扑图



要在具有多个子网的单臂模式下部署 Citrix ADC 设备，请执行以下步骤：

1. 按照配置 NetScaler IP 地址 (NSIP) 中所述配置 NSIP 和默认网关。
2. 按照配置子网 IP 地址中所述配置 NSIP 并启用 USNIP 选项。
3. 按照创建虚拟服务器部分和配置服务部分中所述配置虚拟服务器和服务。
4. 将其中一个网络接口连接到交换机。

系统管理设置

December 15, 2021

完成初始配置后，您可以配置设置以定义 Citrix ADC 设备的行为以及简化连接管理。有多个选项可用于处理 HTTP 请求和响应。路由、桥接以及基于 MAC 的转发模式可用于处理并非发送到 Citrix ADC 设备的数据包。您可以定义网络接口的特性，并可以聚合这些接口。为防止出现计时问题，可以将 Citrix 时钟与网络时间协议 (NTP) 服务器同步。Citrix ADC 设备可以在各种 DNS 模式下运行，包括作为授权域名服务器 (ADNS) 运行。您可以设置 SNMP 使其用于系统管理，并且可以自定义系统事件的 Syslog 日志记录。部署之前，请确认您的配置完整且正确无误。

系统设置

December 15, 2021

系统设置的配置包括基本任务，例如配置 HTTP 端口以实现连接保持活动状态和服务器卸载，设置每个服务器的最大连接数目，以及设置每个连接的最大请求数目。如果代理 IP 地址不适用，您可以启用客户端 IP 地址插入功能，并且可以更改 HTTP Cookie 版本。

还可以对 Citrix ADC 设备进行配置，使其在限定范围内的端口上打开 FTP 连接，而不是在用于数据连接的临时端口上打开。这样可以提高安全性，因为在防火墙上打开所有端口是不安全的。您可以将端口范围设置为 1,024 到 64,000 之间的任意范围。

部署之前，请检查验证核对表以验证您的配置。要配置 HTTP 参数和 FTP 端口范围，请使用 Citrix ADC GUI。

可以修改下表中所述的 HTTP 参数类型。

参数类型：HTTP 端口信息

指定：托管服务器使用的 Web 服务器 HTTP 端口。如果指定这些端口，则设备可以针对目标端口与指定端口相匹配的任何客户端请求执行请求切换。

> 注意：
>
> 如果传入的客户端请求并非发往在设备上明确配置的服务或虚拟服务器，则该请求中的目标端口必须与一个全局配置的 HTTP 端口相匹配。这样设备即可将连接保持活动状态并执行服务器卸载。

参数类型：限制

指定：每个托管服务器的最大连接数，以及通过每个连接发送的最大请求数。例如，如果将 Max Connections（最大连接数）设置为 500，且设备托管三个服务器，则对于与其中每一个服务器之间的连接，设备可打开的最大连接数为 500。默认情况下，设备可以与它托管的任一服务器建立数目不限的连接。要将每个连接的请求数目指定为无限制，请将 Max Requests（最大请求数）设置为 0。

> 注意：
>
> 如果您使用的是 Apache HTTP 服务器，则必须将 Max Connections（最大连接数）设置为等于 Apache httpd.conf 文件中的 MaxClients 参数值。对于其他 Web 服务器，此参数为可选设置。

参数类型：客户端 IP 插入

指定：允许/禁止将客户端 IP 地址插入到 HTTP 请求标头中。可以在相邻的文本框中指定标头字段的名称。当设备托管的 Web 服务器接收到子网 IP 地址时，该服务器会将其标识为客户端的 IP 地址。某些应用程序需要将客户端的 IP 地址用于日志记录目的，或者用于动态决定将由 Web 服务器提供的内容。

可以允许将实际客户端 IP 地址插入到从该客户端发送到设备托管的一个、多个或所有服务器的 HTTP 标头请求中。然后，您可以通过镜像修改服务器访问插入的地址（使用 Apache 模块、ISAPI 接口或 NSAPI 接口）。

参数类型：cookie 版本

指定：在虚拟服务器上配置 COOKIEINSERT 持久性时要使用的 HTTP Cookie 版本。默认版本 0 是 Internet 上最常见的类型。或者，您可以指定版本 1。

参数类型：请求/响应

指定：用于处理特定请求类型以及启用/禁用 HTTP 错误响应日志记录的选项。

参数类型：服务器标头插入

指定：在 Citrix ADC 生成的 HTTP 响应中插入服务器标头。

要使用 GUI 配置 HTTP 参数，请按照以下步骤进行操作：

1. 在导航窗格中，展开 **System**（系统），然后单击 **Settings**（设置）。
2. 在详细信息窗格中，单击 **Settings**（设置）下的 **Change HTTP parameters**（更改 HTTP 参数）。
3. 在 **Configure HTTP parameters**（配置 HTTP 参数）对话框中，指定上表中所列标题下显示的某些或所有参数的值。
4. 单击确定。

要使用 GUI 设置 FTP 端口范围，请按照以下步骤进行操作：

1. 在导航窗格中，展开 **System**（系统），然后单击 **Settings**（设置）。
2. 在详细信息窗格中，单击 **Settings**（设置）下的 **Change global system settings**（更改全局系统设置）。
3. 在 **FTP Port Range**（FTP 端口范围）下，根据要指定的范围，将最低和最高端口号（例如 5000 和 6000）分别键入到 **Start Port**（起始端口）和 **End Port**（结束端口）文本框中。
4. 单击确定。

数据包转发模式

December 15, 2021

Citrix ADC 设备可以路由或桥接并非发送给设备拥有的 IP 地址（即，IP 地址不是 NSIP、MIP、SNIP、配置的服务或配置的虚拟服务器）的数据包。默认情况下，会启用 L3 模式（路由）并禁用 L2 模式（桥接），但您可以更改配置。下面的流程图显示了设备如何评估数据包以及如何处理、路由、桥接或丢弃这些数据包。

图 1. 第 2 层和第 3 层模式之间的交互

设备可以使用以下模式转发其收到的数据包：

- 第 2 层 (L2) 模式
- 3 层 (L3) 模式
- 基于 MAC 的转发模式

启用和禁用第 **2** 层模式

第 2 层模式可控制第 2 层转发（桥接）功能。使用此模式可以将 Citrix ADC 设备配置为用作第 2 层设备，桥接不是发送给它的数据包。如果启用此模式，数据包不会转发给任何 MAC 地址，因为数据包可以到达设备的任何接口，而每个接口都有其自己的 MAC 地址。

如果禁用第 2 层模式（默认设置），设备将丢弃不是发送至其 MAC 地址的数据包。如果另一个第 2 层设备与设备并行安装，则必须禁用第 2 层模式以避免桥接（第 2 层）环路。可以使用配置实用程序或命令行启用第 2 层模式。

注意：设备不支持跨树协议。如果启用了第 2 层模式，为避免环路，请勿将设备上的两个接口连接到同一个广播域。

使用 **CLI** 启用或禁用第 **2** 层模式

在命令提示窗口中，键入以下命令以启用/禁用第 2 层模式，并验证其是否成功启用/禁用：

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

  示例

```
    > enable ns mode l2
    >  Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 ON
    .
    .
    .
    Done
    >

    > disable ns mode l2
    >  Done
    > show ns mode

    Mode Acronym Status
    ------- ------- ------
    1) Fast Ramp FR ON
    2) Layer 2 mode L2 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

使用 GUI 启用或禁用第 2 层模式

1. 在导航窗格中，展开 **System**（系统），然后单击 **Settings**（设置）。
2. 在详细信息窗格中，单击 **Modes** and **Features**（模式与功能）下的 **Configure modes**（配置模式）。

3. 要启用第 2 层模式，请在 **Configure Modes**（配置模式）对话框中选中 **Layer 2 Mode**（第 2 层模式）复选框。要禁用第 2 层模式，请清除该复选框。
4. 单击确定。详细信息窗格中将显示 Enable/Disable Mode(s)?（是否启用/禁用模式?）消息框。
5. 单击是。

启用和禁用第 3 层模式

第 3 层模式控制第 3 层转发功能。可以使用此模式将 Citrix ADC 设备配置为查找路由表，并转发不是发送给它的数据包。如果启用了第 3 层模式（默认设置），设备将执行路由表查找，并转发不是发送到任何设备自有 IP 地址的所有数据包。如果禁用第 3 层模式，设备将丢弃这些数据包。

使用 CLI 启用或禁用第 3 层模式

在命令提示窗口中，键入以下命令以启用/禁用第 3 层模式，并验证其是否成功启用/禁用：

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

  示例

```
> enable ns mode l3
>  Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
2) Layer 2 mode L2 OFF
.
.
.
9) Layer 3 mode (ip forwarding) L3 ON
.
.
.
Done
>

> disable ns mode l3
>  Done
> show ns mode

Mode Acronym Status
------- ------- ------
1) Fast Ramp FR ON
```



```
    2) Layer 2 mode L2 OFF
    .
    .
    .
    9) Layer 3 mode (ip forwarding) L3 OFF
    .
    .
    .
    Done
    >
<!--NeedCopy-->
```

使用 **GUI** 启用或禁用第 **3** 层模式

1. 在导航窗格中，展开 System（系统），然后单击 Settings（设置）。
2. 在详细信息窗格中，单击 Modes and Features（模式与功能）下的 Configure modes（配置模式）。
3. 要启用第 3 层模式，请在 Configure Modes（配置模式）对话框中选中 “Layer 3 Mode (IP Forwarding)”（第 3 层模式 (IP 转发)）复选框。要禁用第 3 层模式，请清除该复选框。
4. 单击确定。详细信息窗格中将显示 Enable/Disable Mode(s)?（是否启用/禁用模式?）消息框。
5. 单击是。

启用和禁用基于 **MAC** 的转发模式

可以使用基于 MAC 的转发模式更高效地处理流量，并在转发数据包时避免多路由或 ARP 查找，因为 Citrix ADC 设备可以记住源的 MAC 地址。为避免多次查找，设备对于为其执行 ARP 查找的每个连接，都会缓存其源 MAC 地址，并将数据返回至该 MAC 地址。

使用 VPN 设备时，基于 MAC 的转发模式非常有用，因为设备可确保所有流经特定 VPN 的流量都经过同一个 VPN 设备传输。

下图显示了基于 MAC 的转发流程。

图 2. 基于 MAC 的转发流程

如果启用了基于 MAC 的转发，设备将缓存以下对象的 MAC 地址：

- 入站连接的来源（例如路由器、防火墙或 VPN 设备等传输设备）。
- 响应请求的服务器。

服务器通过设备响应时，设备会将响应数据包的目标 MAC 地址设置为缓存的地址，从而确保流量以对称方式传输，然后将响应转发给客户端。该流程不涉及路由表查找和 ARP 查找功能。但是，当设备启动连接时，它将使用路由表和 ARP 表进行查找。要启用基于 MAC 的转发，请使用配置实用程序或命令行。

某些部署要求传入和传出路径经过不同的路由器。在这些情况下，基于 MAC 的转发会破坏拓扑设计。对于要求传入和传出路径经过不同路由器的全局服务器负载平衡 (GSLB) 站点，您必须禁用基于 MAC 的转发，并使用设备的默认路由器作为传出路由器。

如果禁用基于 MAC 的转发并启用第 2 层或第 3 层连接，则路由表可以为传出和传入连接指定不同的路由器。要禁用基于 MAC 的转发，请使用配置实用程序或命令行。

使用 **CLI** 启用或禁用基于 **Mac** 的转发

在命令提示窗口中，键入以下命令以启用/禁用基于 MAC 的转发模式，并验证该模式是否成功启用/禁用：

- enable ns mode <Mode>
- disable ns mode <Mode>
- show ns mode

  示例

  “‘ pre codeblock

  > enable ns mode mbf
  > Done
  > show ns mode

```
1   Mode                        Acronym           Status
2   -------                     -------           ------   1)  Fast
       Ramp                   FR                ON   2)  Layer 2
       mode                L2                OFF   .   .   .   6)
       MAC-based forwarding        MBF               ON   .   .   .
         Done   >
```

  > disable ns mode mbf
  > Done
  > show ns mode

```
1   Mode                        Acronym           Status
2   -------                     -------           ------   1)  Fast
       Ramp                   FR                ON   2)  Layer 2
       mode                L2                OFF   .   .   .   6)
       MAC-based forwarding        MBF               OFF   .   .   .
          Done   >  <!--NeedCopy--> ```
```

使用 GUI 启用或禁用基于 Mac 的转发

1. 在导航窗格中，展开 **System**（系统），然后单击 **Settings**（设置）。
2. 在详细信息窗格中，单击 **Modes and Features**（模式与功能）组下的 **Configure modes**（配置模式）。
3. 要启用基于 MAC 的转发模式，请在 **Configure Modes**（配置模式）对话框中选中 **MAC Based Forwarding**（基于 MAC 的转发）复选框。要禁用基于 MAC 的转发模式，请清除该复选框。
4. 单击确定。详细信息窗格中将显示 Enable/Disable Mode(s)?（是否启用/禁用模式?）消息框。
5. 单击是。

网络接口

December 15, 2021

Citrix ADC 接口以插槽/端口表示法编号。除修改单个接口的特性外，您还可以将虚拟 LAN 配置为将流量限制到特定的主机组。还可以将链路聚合形成高速通道。

虚拟 **LANs**

Citrix ADC 设备支持（第 2 层）端口和 IEEE802.1Q 标记的虚拟局域网 (VLAN)。如果您需要将流量限制到特定的工作站组，则 VLAN 配置非常有用。可以使用 IEEE 802.1q 标记功能，将一个网络接口配置为属于多个 VLAN。

可以将配置的 VLAN 绑定到 IP 子网。ADC 设备（如果配置为子网中主机的默认路由器）然后将在这些 VLAN 之间执行 IP 转发。

Citrix ADC 设备支持以下类型的 VLAN。

- 默认 VLAN

  默认情况下，Citrix ADC 设备上的网络接口作为未标记的网络接口包含在一个基于端口的 VLAN 中。此默认 VLAN 的 VID 为 1 并且永久存在。不能将其删除，也不能更改其 VID。

- 基于端口的 VLAN

  基于端口的 VLAN 的成员身份由共享一个公用独占式第 2 层广播域的一组网络接口定义。您可以配置多个基于端口的 VLAN。将接口作为未标记成员添加到新 VLAN 时，该接口将从默认 VLAN 中自动删除。

- 已标记的 VLAN

  网络接口可以是 VLAN 的已标记或未标记成员。每个网络接口都仅是一个 VLAN（其本机 VLAN）的未标记成员。未标记的网络接口将来自本机 VLAN 的帧作为未标记的帧进行转发。已标记的网络接口可以是多个 VLAN 的成员。配置标记时，请确保链路的两端具有匹配的 VLAN 设置。可以使用配置实用程序定义已标记的 VLAN (nsvlan)，该 VLAN 可以绑定任何端口作为 VLAN 的已标记成员。配置此 VLAN 需要重新启动 ADC 设备，因此必须在初始网络配置期间执行。

链路聚合通道

链路聚合将来自多个端口的传入数据组合到单个高速链路中传输。配置链路聚合通道可以提高 Citrix ADC 设备与其他所连接设备之间的通信通道的容量和可用性。聚合的链路也称为通道。

如果将网络接口绑定到通道，则通道参数优先于网络接口参数。一个网络接口只能绑定到一个通道。将网络接口绑定到链路聚合通道会更改 VLAN 配置。换句话说，将网络接口绑定到某个通道，会将这些接口从其原来所属的 VLAN 中删除，并将其添加到默认 VLAN。但是，您可以将该通道绑定回原来的 VLAN，或绑定到新的 VLAN。例如，如果您已将

网络接口 1/2 和 1/3 绑定到 ID 为 2 的 VLAN，然后将它们绑定到链路聚合通道 LA/1，则这些网络接口将移动到默认 VLAN，但是您可以将它们绑定到 VLAN 2。

注意：还可以使用链路聚合控制协议 (LACP) 配置链路聚合。有关详细信息，请参阅使用链路聚合控制协议配置链路聚合。

时钟同步

December 15, 2021

您可以对 Citrix ADC 设备进行配置，使其本机时钟与网络时间协议 (NTP) 服务器同步。这样可以确保其时钟与网络中的其他服务器具有相同的日期和时间设置。NTP 使用用户数据报协议 (UDP) 端口 123 作为其传输层。必须在 NTP 配置文件中添加 NTP 服务器，以便设备定期从这些服务器获取更新。

如果您没有本地 NTP 服务器，可以在官方 NTP 站点 http://www.ntp.org 上查找公共开放访问的 NTP 服务器列表。

要在设备上配置时钟同步，请执行以下步骤：

1. 登录到命令行并输入 shell 命令。
2. 在 shell 提示符下，将 ntp.conf 文件从 /etc 目录复制到 /nsconfig 目录。如果该文件已存在于 /nsconfig 目录中，请确保从 ntp.conf 文件中删除以下条目：

   ```
   restrict localhost

   restrict 127.0.0.2
   ```

   只有在将设备用作时间服务器时，才需要使用上述条目。但是，Citrix ADC 设备不支持此功能。
3. 编辑 /nsconfig/ntp.conf，在文件的服务器下键入所需 NTP 服务器的 IP 地址以及 restrict 条目。
4. 在 /nsconfig 目录中创建名为 rc.netscaler 的文件（如果该目录中不存在此文件）。
5. 通过添加以下条目编辑 /nsconfig/rc.netscaler：/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ntpd.log &

   此条目可启动 ntpd 服务、检查 ntp.conf 文件，并在 /var/log 目录中记录消息。

   注意：如果 Citrix ADC 设备与时间服务器之间的时间差超过 1000 秒，ntpd 服务将终止，并在 ADC 日志中记录一条消息。要避免此种情况，您需要使用 -g 选项启动 ntpd，以强制进行时间同步。在 /nsconfig/rc.netscaler 中添加以下条目：

   ```
   /usr/sbin/ntpd -g -c /nsconfig/ntp.conf -l /var/log/ntpd.log &
   ```

   如果不希望在有较大时间差时强制同步时间，可以手动设置日期，然后再次启动 ntpd。可以通过在 shell 中运行以下命令来检查设备与时间服务器之间的时间差：


```
ntpdate -q <IP address or domain name of the NTP server>
<!--NeedCopy-->
```

6. 重新启动设备以启用时钟同步。

   注意：如果要先启动时间同步，然后再重新启动设备，请在 shell 提示符下输入以下命令（已在步骤 5 中将该命令添加到 rc.netscaler 文件中）：

```
/usr/sbin/ntpd -c /nsconfig/ntp.conf -l /var/log/ ntpd.log &
<!--NeedCopy-->
```

DNS 配置

December 15, 2021

可以将 Citrix ADC 设备配置为用作授权域名服务器 (ADNS)、DNS 代理服务器、端点解析器或转发器。可以添加 DNS 资源记录，例如 SRV 记录、AAAA 记录、A 记录、MX 记录、NS 记录、CNAME 记录、PTR 记录和 SOA 记录。此外，设备还可以平衡外部 DNS 服务器上的负载。

通常的做法是将设备配置为转发器。要实现此配置，您需要添加外部名称服务器。添加外部服务器之后，应验证配置是否正确。

您可以添加、删除、启用和禁用外部名称服务器。可以通过指定名称服务器的 IP 地址来创建名称服务器，也可以将现有虚拟服务器配置为名称服务器。

添加名称服务器时，可以指定 IP 地址或虚拟 IP 地址 (VIP)。如果使用 IP 地址，设备将使用轮询负载平衡方法，将请求分配到配置的各个名称服务器。如果使用 VIP，则可以指定任何负载平衡方法。

使用 CLI 添加名称服务器

在命令提示窗口中，键入以下命令以添加名称服务器并验证配置：

- add dns nameServer <IP>
- show dns nameServer <IP>

  示例

  “‘ pre codeblock

  > add dns nameServer 10.102.29.10
  > Done
  > show dns nameServer 10.102.29.10
  > 1) 10.102.29.10 - State: DOWN


```
Done
```

使用 **GUI** 添加名称服务器

1. 导航到 **Traffic Management**（流量管理）> **DNS** > **Name Servers**（名称服务器）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Create Name Server**（创建名称服务器）对话框中，选择 **IP Address**（IP 地址）。
4. 在 **IP Address**（IP 地址）文本框中，键入名称服务器的 IP 地址（例如 10.102.29.10）。如果要添加外部名称服务器，请清除 **Local**（本地）复选框。
5. 单击 **Create**（创建），然后单击 **Close**（关闭）。
6. 确认添加的名称服务器显示在 **Name Servers**（名称服务器）窗格中。

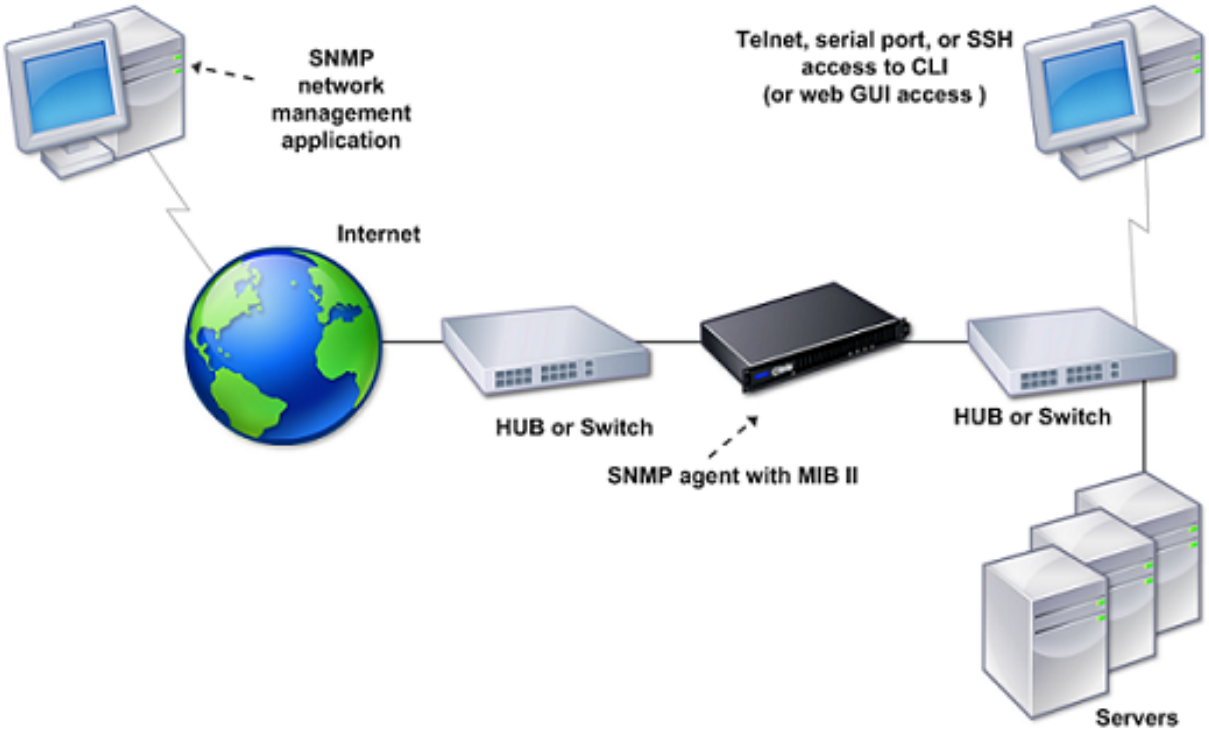
SNMP 配置

December 15, 2021

简单网络管理协议 (SNMP) 网络管理应用在外部计算机上运行，可查询 Citrix ADC 设备上的 SNMP 代理。该代理在管理信息库 (MIB) 中搜索网络管理应用请求的数据，并将数据发送给该应用。

SNMP 监视功能使用陷阱消息和警报。SNMP 陷阱消息是代理为发送异常情况信号而生成的异步事件，这些情况由警报指示。例如，如果要在 CPU 使用率高于 90% 时获得通知，您可以为该条件设置警报。下图显示了具有启用并配置了 SNMP 的 Citrix ADC 设备的网络。

图 1. Citrix ADC 设备上的 SNMP



Citrix ADC 设备上的 SNMP 代理支持 SNMP 版本 1 (SNMPv1)、SNMP 版本 2 (SNMPv2) 和 SNMP 版本 3 (SNMPv3)。由于在双语模式下运行，因此该代理可以处理 SNMPv2 查询（例如 Get-Bulk）和 SNMPv1 查询。SNMP 代理还发送符合 SNMPv2 的陷阱，并支持 SNMPv2 数据类型（例如 counter64）。在处理 SNMP 查询时，SNMPv1 管理器（其他服务器上向 ADC 设备请求 SNMP 信息的程序）使用 NS-MIB-smiv1.mib 文件。SNMPv2 管理器使用 NS-MIB-smiv2.mib 文件。

Citrix ADC 设备支持以下企业特定的 MIB：

- 标准 MIB-2 组的子集。提供 MIB-2 组 SYSTEM、IF、ICMP、UDP 和 SNMP。
- 系统企业 MIB。提供特定于系统的配置和统计数据。

要配置 SNMP，您需要指定哪些管理器可以查询 SNMP 代理、添加将接收 SNMP 陷阱消息的 SNMP 陷阱侦听器并配置 SNMP 警报。

添加 **SNMP** 管理器

您可以配置一个运行符合 SNMP 版本 1、2 或 3 的管理应用程序的工作站来访问设备。此类工作站称为 SNMP 管理器。如果未在设备上指定 SNMP 管理器，设备将接受并响应来自网络中所有 IP 地址的 SNMP 查询。如果配置了一个或多个 SNMP 管理器，设备将仅接受并响应来自这些特定 IP 地址的 SNMP 查询。指定 SNMP 管理器的 IP 地址时，可以使用 netmask 参数授予从整个子网访问的权限。最多可以添加 100 个 SNMP 管理器或网络。使用 CLI 添加 SNMP 管理器

在命令提示窗口中，键入以下命令以添加 SNMP 管理器并验证配置：

```
add snmp manager <IPAddress> ... [-netmask <netmask>]
```



```
show snmp manager <IPAddress>
```

示例：

```
add snmp manager 10.102.29.5 -netmask 255.255.255.255
show snmp manager 10.102.29.5
10.102.29.5 255.255.255.255
```

要使用 **GUI** 添加 **SNMP** 管理器，请执行以下操作：

1. 在导航窗格中，依次展开 **System**（系统）和 **SNMP**，然后单击 **Managers**（管理器）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Add SNMP Manager** （添加 SNMP 管理器）对话框中，将运行管理应用程序的工作站的 IP 地址（例如 10.102.29.5）键入到 **IP Address**（IP 地址）文本框中。
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。
5. 确认所添加的 SNMP 管理器显示在窗格底部的 **Details**（详细信息）部分中。

添加 **SNMP** 陷阱侦听器

在配置警报后，需要指定设备将陷阱消息发送到的陷阱侦听器。除了指定陷阱侦听器的 IP 地址和目标端口等参数外，还可指定陷阱类型（一般或特定）以及 SNMP 版本。

最多可配置 20 个陷阱侦听器，用于接收一般或特定陷阱。

使用 **CLI** 添加 **SNMP** 陷阱侦听器

在命令提示窗口中，键入以下命令以添加 SNMP 陷阱，并验证该陷阱是否成功添加：

- `add snmp trap specific <IP>`
- `show snmp trap`

示例：

```
Trap type: SPECIFIC
Destination IP: 10.102.29.3
TD: 0
Destination Port: 162
Source IP: NetScaler IP
Version: V2
Min-Severity: -
AllPartition: DISABLED
Community: public
<!--NeedCopy-->
```


使用 **GUI** 添加 **SNMP** 陷阱侦听器

1. 在导航窗格中，依次展开“System”（系统）和 SNMP，然后单击 Traps（陷阱）。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 Create SNMP Trap Destination（创建 SNMP 陷阱目标）对话框中，将 IP 地址（例如 10.102.29.3）键入到 Destination IP Address（目标 IP 地址）文本框中。
4. 单击 Create（创建），然后单击 Close（关闭）。
5. 确认添加的 SNMP 陷阱显示在窗格底部的 Details（详细信息）部分中。

配置 **SNMP** 警报

您可以配置警报，以便在发生与其中一个警报对应的事件时，设备能够生成陷阱消息。配置警报包括启用警报和设置生成陷阱的严重级别。有五种严重级别：“Critical”（严重）、“Major”（主要）、“Minor”（次要）、“Warning”（警告）和“Informational”（信息）。只有在警报的严重性与为陷阱指定的严重性相匹配时，才会发送陷阱。

默认情况下某些警报处于启用状态。如果您禁用 SNMP 警报，则在发生相应的事件时设备不会生成陷阱消息。例如，如果您禁用登录失败 SNMP 警报，则在登录失败时设备不会生成陷阱消息。

使用 **CLI** 启用或禁用警报

在命令提示窗口中，键入以下命令以启用或禁用警报，并验证是否成功启用或禁用该警报：

- set snmp alarm <trapName> \[-state ENABLED \| DISABLED \]
- show snmp alarm <trapName>

  示例

```
    > set snmp alarm LOGIN-FAILURE -state ENABLED
    >  Done
    > show snmp alarm LOGIN-FAILURE
    >  Alarm Alarm Threshold Normal Threshold Time State Severity
       Logging
    >  ----- --------------- ---------------- ---- -------- ---------
       --------
    >  1) LOGIN-FAILURE N/A N/A N/A ENABLED - ENABLED
    >  Done
    >  >
<!--NeedCopy-->
```

使用 **CLI** 设置警报的严重性

在命令提示窗口中，键入以下命令以设置警报的严重性，并验证严重性是否正确设置：

- set snmp alarm <trapName> \[-severity <severity>\]

- show snmp alarm <trapName>

  示例

```
    > set snmp alarm LOGIN-FAILURE -severity Major
    >  Done
    > show snmp alarm LOGIN-FAILURE
    >  Alarm Alarm Threshold Normal Threshold Time State Severity
       Logging
    >  ----- --------------- ---------------- ---- -------- ---------
       --------
    >  1) LOGIN-FAILURE N/A N/A N/A ENABLED Major ENABLED
    >  Done
    >  >
<!--NeedCopy-->
```

使用 **GUI** 配置警报

1. 在导航窗格中，依次展开 System（系统）、SNMP，然后单击 Alarms（警报）。
2. 在详细信息窗格中，选择一个警报（例如 LOGIN-FAILURE），然后单击 Open（打开）。
3. 在 Configure SNMP Alarm（配置 SNMP 警报）对话框中，从 State（状态）下拉列表中选择 “Enabled”（已启用）以启用该警报。要禁用警报，请选择 Disabled（禁用）。
4. 在 Severity（严重性）下拉列表中，选择严重性选项，例如 “Major”（主要）。
5. 单击 OK（确定），然后单击 Close（关闭）。
6. 查看窗格底部的 Details（详细信息）部分，确认 SNMP 警报的参数配置正确。

验证配置

December 15, 2021

完成系统配置之后，请填写以下核对表以验证您的配置。

配置核对表

- 运行的版本是：
- 无不兼容性问题。（在内部版本的发行说明中记录了不兼容性问题。）
- 端口设置（速度、双工模式、流量控制、监视）与交换机的端口设置相同。
- 已配置足够的 SNIP IP 地址，可在峰值时段支持所有服务器端连接。
  - 已配置的 SNIP IP 地址数量为：__
  - 预计的同时服务器连接数量是：

    [ ] 62,000 [ ] 124,000 [ ] 其他 ____

拓扑配置核对表

已使用路由解析其他子网中的服务器。

输入的路由是：

_____

- 如果 Citrix ADC 设备位于公私拓扑中，则已配置反向 NAT。
- 在 ADC 设备上配置的故障转移（高可用性）设置在单臂或双臂配置中解析。所有未使用的网络接口都已禁用：

  _____

- 如果 ADC 设备放置在外部负载均衡器的后面，则外部负载均衡器上的负载均衡策略不是“最少连接”。

  在外部负载平衡器上配置的负载平衡策略是：_____

  _____

- 如果将 ADC 设备放置在防火墙前面，则防火墙的会话超时值设置为大于等于 300 秒。

  注意：Citrix ADC 设备上的 TCP 空闲连接超时为 360 秒。如果防火墙上的超时值设置为 300 秒或更长，则设备可以有效地执行 TCP 连接多路复用，因为连接不会提前关闭。

  为会话超时配置的值是：_____

服务器配置核对表

- 已在所有服务器上启用“保持活动”。

  为保持活动超时配置的值是：_____

- 已将默认网关设置为正确的值。（默认网关应该是 Citrix ADC 设备或上游路由器。）默认网关为：

  _____

- 服务器端口设置（速度、双工模式、流量控制、监视）与交换机的端口设置相同。

  _____

- 如果使用 Microsoft® Internet Information Server，则已在该服务器上启用缓冲。
- 如果使用 Apache Server，则已在服务器和 Citrix ADC 设备上配置 MaxConn（最大连接数）参数。

  设置的 MaxConn（最大连接数）值是：_____

  _____

- 如果使用 Netscape Enterprise Server，则会在 Citrix ADC 设备上设置每个连接的最大请求数参数。设置的每个连接的最大请求数值是：_____

  _____

软件功能配置核对表

- 是否需要禁用第 2 层模式功能?（如果另一个第 2 层设备与 Citrix ADC 设备并行运行，则禁用此功能。）

  启用或禁用的原因：

  _____

- 是否需要禁用基于 MAC 的转发功能?（如果由返回流量使用的 MAC 地址不同，则应将其禁用。）

  启用或禁用的原因：

  _____

- 是否需要禁用基于主机的重复使用?（服务器上是否存在虚拟主机?）

  启用或禁用的原因：

  _____

- 是否需要更改浪涌保护功能的默认设置?

  更改或不更改的原因：

  _____

访问核对表

- 可以从客户端网络 ping 系统 IP。
- 可以从服务器端网络 ping 系统 IP。
- 可以通过 Citrix ADC ping 托管服务器。
- 可以从托管服务器 ping Internet 主机。
- 可以通过浏览器访问托管服务器。
- 可以使用浏览器从托管服务器访问 Internet。
- 可以使用 SSH 访问系统。
- 对所有托管服务器的管理访问权限均有效。

> 注意：
>
> 在使用 ping 实用程序时，请确保被 ping 的服务器启用了 ICMP 回显，否则 ping 将不会成功。

防火墙核对表

满足以下防火墙要求：

- UDP 161 (SNMP)

- UDP 162（SNMP 陷阱）
- TCP/UDP 3010 (GUI)
- HTTP 80 (GUI)
- TCP 22 (SSH)

Citrix ADC 设备上的负载平衡流量

December 15, 2021

负载平衡功能在多个服务器之间分配客户端请求，从而优化资源的利用。在通过数量有限的服务器向大量客户端提供服务的真实场景中，服务器可能发生过载，降低服务器场的性能。Citrix ADC 设备使用负载平衡标准来防止出现瓶颈，方法是：当收到客户端请求时，将各个请求转发到最适合处理该请求的服务器。

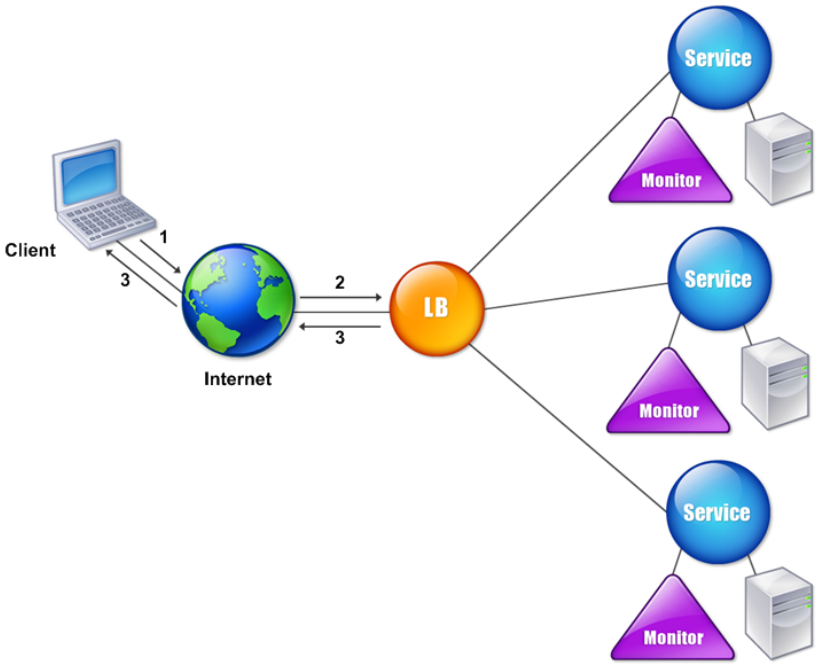
要配置负载平衡，需要定义一个虚拟服务器，使其作为服务器场中多个服务器的代理，并平衡这些服务器之间的负载。

当客户端启动与服务器的连接时，虚拟服务器将终止客户端连接并启动与选定服务器的新连接，或重复使用与服务器的现有连接，以执行负载平衡。负载平衡功能提供从 4 层（TCP 和 UDP）到 7 层（FTP、HTTP 和 HTTPS）的流量管理。

Citrix ADC 设备使用多种算法（称为负载平衡方法）来确定如何在服务器之间分配负载。默认负载平衡方法是“最少连接”方法。

典型的负载平衡部署由下图中所述的实体组成。

图 1. 负载平衡体系结构



各实体的功能如下：

- 虚拟服务器。实体由 IP 地址、端口和协议表示。虚拟服务器 IP 地址 (VIP) 通常为公用 IP 地址。客户端向此 IP 地址发送连接请求。虚拟服务器表示一组服务器。
- 服务。服务是服务器或服务器上运行的应用程序的逻辑表示。标识服务器的 IP 地址、端口和协议。这些服务已绑定到虚拟服务器。
- 服务器对象。以 IP 地址表示的实体。在创建服务时会创建服务器对象。服务的 IP 地址用作服务器对象的名称。您也可以创建服务器对象，然后使用该服务器对象创建服务。
- 监视程序。跟踪服务运行状况的实体。设备使用绑定到每项服务的监视程序定期探测服务器。如果服务器未在指定的响应超时时间内做出响应，并且指定次数的探测均失败，则服务将标记为“DOWN”（关闭）。然后，设备将在其余服务之间执行负载平衡。

负载平衡

December 15, 2021

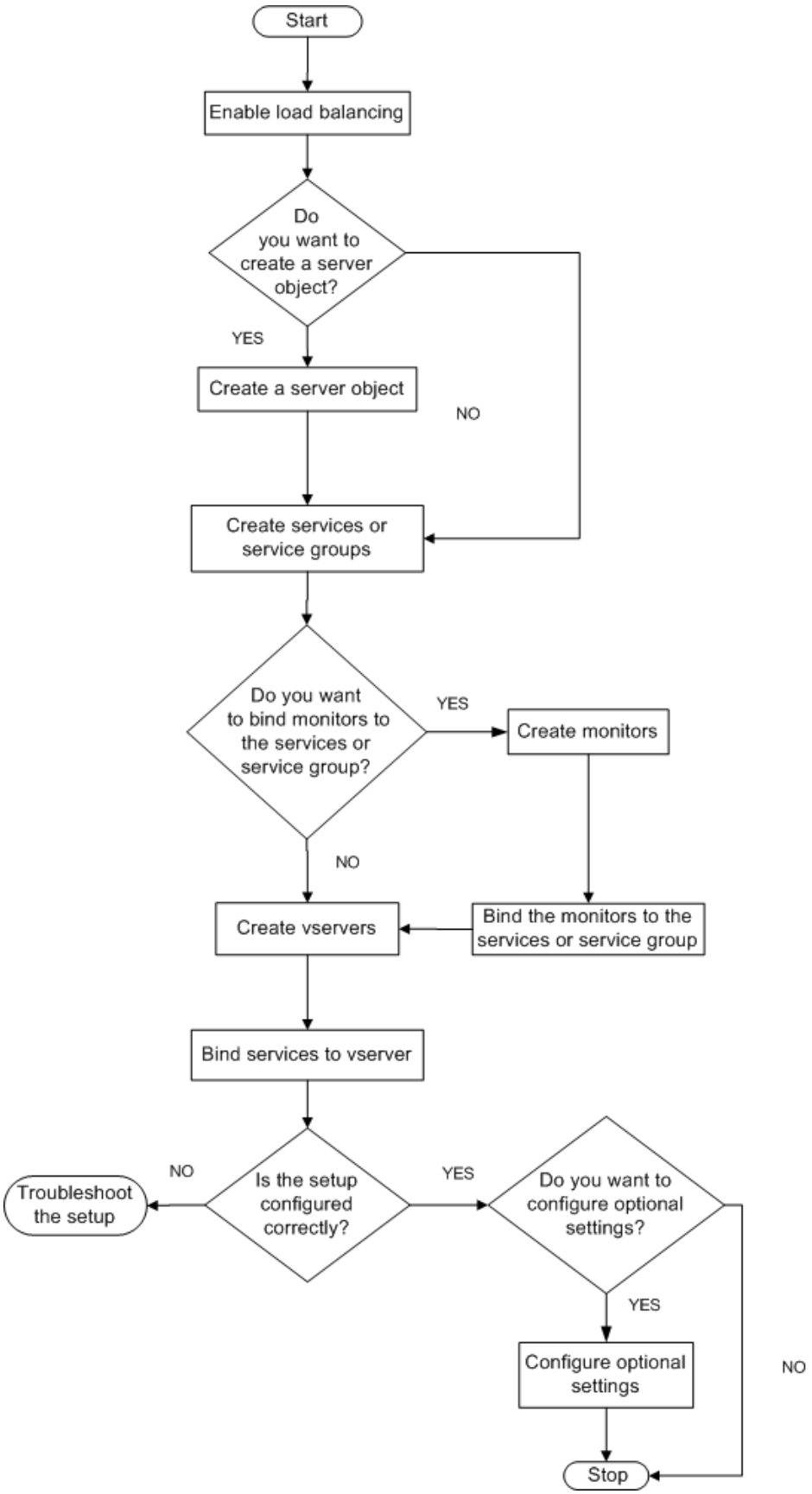
要配置负载平衡，您必须首先创建服务。然后创建虚拟服务器，并将服务绑定到虚拟服务器。默认情况下，Citrix ADC 设备将显示器绑定到每个服务。绑定服务之后，请通过确保所有设置均正确无误来验证您的配置。

> 注意：
>
> 部署配置之后，可以显示统计数据，了解该配置中实体的性能情况。可以使用统计实用程序或 stat lb vserver <vserverName> 命令。

也可以向服务分配权重。然后，负载平衡方法会使用分配的权重来选择服务。但是，开始时您可以将可选任务限制为：针对必须保持与特定服务器之间连接的会话配置某些基本的永久性设置，以及某些基本的配置保护设置。

下面的流程图说明了配置任务的顺序。

图 1. 负载平衡配置任务的顺序



启用负载平衡

配置负载平衡之前，请确保已启用负载平衡功能。

使用 **CLI** 启用负载平衡

在命令提示窗口中，键入以下命令以启用负载平衡并验证是否成功启用：

- enable feature lb
- show feature

  示例

  “‘ pre codeblock

  > enable feature lb
  > Done
  > show feature

```
Feature                    Acronym          Status
-------                    -------          ------   1)  Web
    Logging                WL               OFF   2)  Surge
    Protection           SP               OFF   3)  Load Balancing
                LB               ON   .   .   .   9)  SSL
    Offloading             SSL              ON   .   .   .  Done
    <!--NeedCopy--> ```
```

使用 **GUI** 启用负载平衡

1. 在导航窗格中，展开 System（系统），然后单击 Settings（设置）。
2. 在详细信息窗格中，单击 Modes and Features（模式与功能）下的 Change basic features（更改基本功能）。
3. 在 Configure Basic Features（配置基本功能）对话框中，选中 Load Balancing（负载平衡）复选框，然后单击 OK（确定）。
4. 在 Enable/Disable Feature(s)?（是否启用/禁用功能?）消息框中，单击 Yes（是）。

配置服务和虚拟服务器

确定要进行负载平衡的服务后，可通过以下方法来实施初始负载平衡配置：创建服务对象，创建负载平衡虚拟服务器，并将这些服务对象绑定到该虚拟服务器。

使用 **CLI** 实现初始负载平衡配置

在命令提示窗口中，键入以下命令以实施并验证初始配置：

- add service <name> <IPaddress> <serviceType> <port>
- add lb vserver <vServerName> <serviceType> \[<IPaddress> <port>\]
- bind lb vserver <name> <serviceName>
- show service bindings <serviceName>

  示例

```
> add service service-HTTP-1 10.102.29.5 HTTP 80
  Done
> add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
  Done
> bind lb vserver vserver-LB-1 service-HTTP-1
  Done
> show service bindings service-HTTP-1
    service-HTTP-1 (10.102.29.5:80) - State : DOWN

      1)      vserver-LB-1 (10.102.29.60:80) - State : DOWN
  Done
 <!--NeedCopy-->
```

使用 **GUI** 实现初始负载平衡配置

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）。
2. 在详细信息窗格中，单击 Getting Started（开始使用）下的 Load Balancing wizard（负载平衡向导），并按照说明创建基本负载平衡设置。
3. 返回导航窗格，展开 Load Balancing（负载平衡），然后单击 Virtual Servers（虚拟服务器）。
4. 选择您配置的虚拟服务器，并确认页面底部显示的参数配置正确。
5. 单击打开。
6. 通过确认已在 Services（服务）选项卡上为每项服务选中 Active（活动）复选框，确定已将每项服务绑定到虚拟服务器。

持久性设置

December 15, 2021

如果您要在由虚拟服务器表示的服务器上保持连接状态（例如，电子商务中使用的连接），必须对该虚拟服务器配置持久性。然后，设备将使用配置的负载平衡方法进行初始服务器选择，而将来自同一个客户端的所有后续请求都转发到该服务器。

如果配置了持久性，它会在选定服务器之后取代负载平衡方法。如果配置的持久性适用于关闭的服务，设备将使用负载平衡方法来选择新服务，对于来自客户端的后续请求，新服务将具有持久性。如果选定的服务处于“Out Of Service”（中断服务）状态，它仍将继续处理未决请求，但不再接受新的请求或连接。关闭期结束后，现有连接将关闭。下表列出了可以配置的持久性类型。

持久性类型	持续型连接
源 IP、SSL 会话 ID、规则、DESTIP、SRCIPDESTIP	250K
CookieInsert、URL 被动、自定义服务器 ID	内存限制。如果是 CookieInsert 并且超时不为 0，则在达到内存限制之前，连接数目不受限制。

表 1. 并发持续型连接数目限制

如果由于设备缺乏资源而无法保持配置的持久性，将使用负载平衡方法进行服务器选择。持久性将在配置的时间内保持，具体取决于持久性类型。某些持久性类型专用于某些虚拟服务器。下表显示了对应关系。

持久性类型标头 **1**	**HTTP**	**HTTPS**	**TCP**	**UDP/IP**	**SSL_Bridge**
源 IP	是	是	是	是	是
CookieInsert	是	是	否	否	否
SSL Session ID（SSL 会话 ID）	否	是	否	否	是
URL Passive（URL 被动）	是	是	否	否	否
Custom Server ID（自定义服务器 ID）	是	是	否	否	否
规则	是	是	否	否	否
SRCIPDESTIP	不适用	不适用	是	是	不适用
DESTIP	不适用	不适用	是	是	不适用

表 2. 适用于各种虚拟服务器类型的持久性类型

还可以为一组虚拟服务器指定持久性。对一组虚拟服务器启用持久性之后，无论该组中的哪一个虚拟服务器接收到客户端请求，客户端请求都将定向到选定的同一个服务器。在经过配置的持久性时间之后，就可以选择该组中的任何虚拟服务器来处理传入的客户端请求。

两种常用的持久性类型是基于 Cookie 的持久性和基于 URL 中服务器 ID 的持久性。

配置基于 **cookie** 的持久性

在启用基于 Cookie 的持久性之后，Citrix ADC 设备会将一个 HTTP Cookie 添加到 HTTP 响应的 Set-Cookie 标头字段中。Cookie 包含关于必须将 HTTP 请求发送到的服务的信息。客户端存储 Cookie 并在所有后续请求中包括该 Cookie，并且 ADC 使用它为这些请求选择服务。您可以在 HTTP 类型或 HTTPS 类型的虚拟服务器上使用此类型的持久性。

Citrix ADC 设备将插入 cookie <NSC_XXXX>= <ServiceIP> <ServicePort>

其中：

- «NSC_XXXX> 是从虚拟服务器名称派生的虚拟服务器 ID。
- «ServiceIP> 是服务的 IP 地址的十六进制值。
- «ServicePort> 是服务的端口的十六进制值。

ADC 在插入 Cookie 时对 ServiceIP 和 ServicePort 进行加密，在收到 Cookie 时对它们进行解密。

注意：如果不允许客户端存储 HTTP Cookie，则后续请求不会含有 HTTP Cookie，并且不使用持久性。

默认情况下，ADC 设备发送符合 Netscape 规范的 HTTP Cookie 版本 0。它还可发送符合 RFC 2109 的 Cookie 版本 1。

您可以为基于 HTTP Cookie 的持久性配置超时值。请注意以下问题：

- 如果使用 HTTP Cookie 版本 0，Citrix ADC 设备将插入 cookie 到期时间（HTTP cookie 的 expires 属性）的绝对协调世界时 (GMT)，按 ADC 设备中当前 GMT 时间和超时值之和计算。
- 如果使用 HTTP Cookie 版本 1，ADC 设备将插入相对到期时间（HTTP Cookie 的 Max-Age 属性）。在这种情况下，客户端软件将计算实际的到期时间。

注意：当前安装的大多数客户端软件（Microsoft Internet Explorer 和 Netscape 浏览器）识别 HTTP Cookie 版本 0；但是，某些 HTTP 代理识别 HTTP Cookie 版本 1。

如果将超时值设置为 0，则不论使用哪一个 HTTP Cookie 版本，ADC 设备均不指定到期时间。此时到期时间取决于客户端软件，如果关闭该软件，此类 Cookie 就会无效。这种持久性类型不占用任何系统资源。因此，它可以容纳无数个持久性客户端。

管理员可以更改 HTTP cookie 版本。

使用 **CLI** 更改 **HTTP cookie** 版本

在命令提示窗口中，键入：

```
set ns param [-cookieversion ( 0 | 1 )]
<!--NeedCopy-->
```

示例：


```
set ns param -cookieversion 1
<!--NeedCopy-->
```

使用 **GUI** 更改 **HTTP cookie** 版本

1. 导航到 System（系统）> Settings（设置）。
2. 在详细信息窗格中，单击 Change HTTP Parameters（更改 HTTP 参数）。
3. 在 Configure HTTP Parameters（配置 HTTP 参数）对话框中的 Cookie 下，选择 Version 0（版本 0）或 Version 1（版本 1）。

注意：有关参数的信息，请参阅配置基于 cookie 的持久性。

使用 **CLI** 配置基于 **cookie** 的持久性

在命令提示窗口中，键入以下命令以配置基于 Cookie 的持久性并验证配置：

```
set lb vserver <name> -persistenceType COOKIEINSERT

show lb vserver <name>
<!--NeedCopy-->
```

示例：

```
set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: COOKIEINSERT (version 0)
    Persistence Timeout: 2 min
    .
    .
    .
 Done
<!--NeedCopy-->
```

使用 **GUI** 配置基于 **cookie** 的持久性

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。
2. 在详细信息窗格中，选择要为其配置持久性的虚拟服务器（例如 vserver-LB-1），然后单击 Open（打开）。
3. 在 Configure Virtual Server (Load Balancing)（配置虚拟服务器 (负载平衡)）对话框中，从 Method and Persistence（方法和持久性）选项卡上的 Persistence（持久性）列表中选择 COOKIEINSERT。

4. 在 Time-out (min)（超时 (分钟)）文本框中，键入超时值（例如 2）。
5. 单击确定。
6. 选择虚拟服务器并查看窗格底部的 Details（详细信息）部分，确认其持久性配置正确。

配置基于 **URL** 中服务器 **ID** 的持久性

Citrix ADC 设备可以根据 URL 中的服务器 ID 维护持久性。在称为 URL 被动持久性的技术中，ADC 从服务器响应中提取服务器 ID，并将其嵌入客户端请求的 URL 查询中。服务器 ID 是指定为十六进制数的 IP 地址和端口组合。ADC 从后续的客户端请求中提取服务器 ID，然后用它来选择服务器。

URL 被动持久性要求配置负载表达式或策略基础结构表达式，指定服务器 ID 在客户端请求中的位置。有关表达式的详细信息，请参阅策略配置和参考。

注意：如果无法从客户端请求中提取服务器 ID，系统将根据负载平衡方法来选择服务器。

示例：负载表达式

表达式 URLQUERY 中包含 sid=，将系统配置为从客户端请求的 URL 查询中提取服务器 ID（匹配标记 sid= 之后的部分）。因此，URL 为 `http://www.citrix.com/index.asp?\\&sid;=c0a864100050` 的请求将定向到 IP 地址为 10.102.29.10、端口为 80 的服务器。

超时值不影响此类型的持久性，只要能够从客户端请求中提取服务器 ID，就可以保持这种持久性。此持久性类型不占用任何系统资源，因此可以容纳无数个持久性客户端。

> 注意：
>
> 有关参数的信息，请参阅负载平衡。

使用 **CLI** 基于 **URL** 中的服务器 **ID** 配置持久性

在命令提示窗口中，键入以下命令以配置基于 URL 中服务器 ID 的持久性并验证配置：

```
set lb vserver <name> -persistenceType URLPASSIVE

<show lb vserver <name>
<!--NeedCopy-->
```

示例：

```
set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
Done
show lb vserver vserver-LB-1
    vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
    .
    .
    .
    Persistence: URLPASSIVE
    Persistence Timeout: 2 min
```



```
      .
      .
      .
Done
<!--NeedCopy-->
```

使用 **GUI** 基于 **URL** 中的服务器 **ID** 配置持久性

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。
2. 在详细信息窗格中，选择要为其配置持久性的虚拟服务器（例如 vserver-LB-1），然后单击 Open（打开）。
3. 在 Configure Virtual Server (Load Balancing)（配置虚拟服务器 (负载平衡)）对话框中，从 Method and Persistence（方法和持久性）选项卡上的 Persistence（持久性）列表中选择 URLPASSIVE。
4. 在 Time-out (min)（超时 (分钟)）文本框中，键入超时值（例如 2）。
5. 在 Rule（规则）文本框中，输入有效的表达式。或者，也可以单击 Rule（规则）文本框旁边的 Configure（配置），使用 Create Expression（创建表达式）对话框来创建表达式。
6. 单击确定。
7. 选择虚拟服务器并查看窗格底部的 Details（详细信息）部分，确认其持久性配置正确。

配置功能以保护负载平衡配置

December 15, 2021

可以配置 URL 重定向以提供虚拟服务器故障通知，还可以配置备份虚拟服务器，使其在主虚拟服务器不可用时接管其工作。

配置 **URL** 重定向

您可以配置一个重定向 URL，使其在 HTTP 或 HTTPS 类型的虚拟服务器处于关闭或禁用状态时传达设备的状态。此 URL 可以是本地或远程链接。设备使用 HTTP 302 重定向。

重定向 URL 可以是绝对 URL 或相对 URL。如果配置的重定向 URL 包含绝对 URL，HTTP 重定向将发送到配置的位置，而不考虑在传入的 HTTP 请求中指定的 URL。如果配置的重定向 URL 仅包含域名（相对 URL），则在将传入的 URL 附加到重定向 URL 中配置的域之后，HTTP 重定向将发送到某个位置。

注意：如果负载平衡虚拟服务器配置有备份虚拟服务器和重定向 URL，则备份虚拟服务器将优先于重定向 URL。在这种情况下，当主虚拟服务器和备份虚拟服务器均处于关闭状态时，将使用重定向。

使用 **CLI** 配置虚拟服务器以将客户端请求重定向到 **URL**

在命令提示窗口中，键入以下命令以配置虚拟服务器，从而将客户端请求重定向到 URL 并验证配置：

- set lb vserver <name> -redirectURL <URL>
- show lb vserver <name>

示例

```
> set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.
  com/mysite/maintenance
  Done
> show lb vserver vserver-LB-1
     vserver-LB-1 (10.102.29.60:80) - HTTP   Type: ADDRESS
     State: DOWN
     Last state change was at Wed Jun 17 08:56:34 2009 (+666 ms)
     .
     .
     .
     Redirect URL: http://www.newdomain.com/mysite/maintenance
     .
     .
     .
  Done
 >
 <!--NeedCopy-->
```

使用 **GUI** 配置虚拟服务器以将客户端请求重定向到 **URL**

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。
2. 在详细信息窗格中，选择要为其配置 URL 重定向的虚拟服务器（例如 vserver-LB-1），然后单击 Open（打开）。
3. 在“Configure Virtual Server (Load Balancing)”(配置虚拟服务器 (负载平衡))对话框中，向“Advanced”(高级）选项卡上的“Redirect URL”（重定向 URL）文本框中键入 URL（例如 `http://www.newdomain.com/mysite/maintenance`），然后单击“OK”（确定）。
4. 确认您为服务器配置的重定向 URL 显示在窗格底部的 Details（详细信息）部分中。

配置备份虚拟服务器

如果主虚拟服务器处于关闭或禁用状态，设备可以将连接或客户端请求定向到备份虚拟服务器，备份虚拟服务器会将客户端流量转发给服务。设备还可以向客户端发送关于站点停用或维护的通知消息。备份虚拟服务器是对客户端透明的代理。

可以在创建虚拟服务器或更改现有虚拟服务器的可选参数时配置备份虚拟服务器。也可以为现有备份虚拟服务器配置备份虚拟服务器，从而创建级联的备份虚拟服务器。级联备份虚拟服务器的最大深度为 10。设备可以搜索运行中的备份虚拟服务器，然后访问该虚拟服务器以交付内容。

可以在主虚拟服务器上配置 URL 重定向，以便在主虚拟服务器和备份虚拟服务器处于关闭状态或达到其处理请求的阈值时使用。

注意：如果不存在备份虚拟服务器，则除非在虚拟服务器上配置了重定向 URL，否则系统会显示一条错误消息。如果同时配置了备份虚拟服务器和重定向 URL，将优先使用备份虚拟服务器。

使用 **CLI** 配置备份虚拟服务器

在命令提示窗口中，键入以下命令以配置备份虚拟服务器并验证配置：

- set lb vserver <name> \[-backupVserver <string>\]
- show lb vserver <name>

  示例

  “‘ pre codeblock

```
set lb vserver vserver-LB-1 -backupVserver vserver-LB-2
Done
show lb vserver vserver-LB-1
vserver-LB-1 (10.102.29.60:80) - HTTP Type: ADDRESS
State: DOWN
Last state change was at Wed Jun 17 08:56:34 2009 (+661 ms)
.
.
.
Backup: vserver-LB-2
.
.
.
Done
“‘
```

使用 **GUI** 设置备份虚拟服务器

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。
2. 在详细信息窗格中，选择要为其配置备份虚拟服务器的虚拟服务器（例如 vserver-LB-1），然后单击 Open（打开）。
3. 在“Configure Virtual Server (Load Balancing)”（配置虚拟服务器 (负载平衡)）对话框中，从“Advanced”（高级）选项卡上的 “Backup Virtual Server”（备份虚拟服务器）列表中选择备份虚拟服务器（例如 vserver-LB-2），然后单击“OK”（确定）。
4. 确认配置的备份虚拟服务器显示在窗格底部的 Details（详细信息）部分中。

注意：如果主服务器关闭并在重新开启后用作备份服务器，并且您希望备份虚拟服务器用作主服务器，直至您明确地重新建立主虚拟服务器，请选中“Disable Primary When Down”（禁用处于关闭状态的主服务器）复选框。

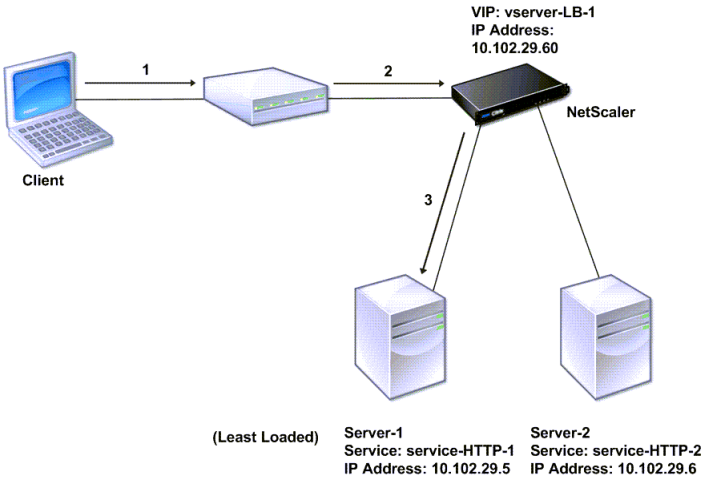
典型的负载平衡方案

December 20, 2021

在负载平衡设置中，Citrix ADC 设备在逻辑上位于客户端与服务器场之间，负责管理发送到服务器的通信流量。

下图显示了基本负载平衡配置的拓扑。

图 1. 基本负载平衡拓扑

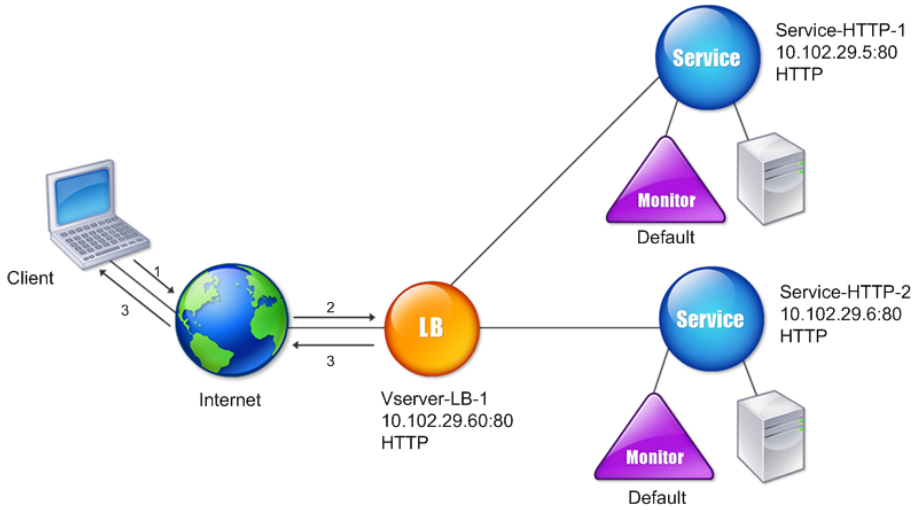


虚拟服务器选择服务，然后指定该服务处理客户端请求。假设在上图的方案中，创建了服务 service-HTTP-1 和 service-HTTP-2，并将这两个服务绑定到虚拟服务器 virtual server-LB-1。virtual server-LB-1 将客户端请求转发给 service-HTTP-1 或 service-HTTP-2。系统使用“最少连接”负载平衡方法为每个请求选择服务。下表列出了必须在系统中配置的基本实体的名称和值。

表 1. LB 配置参数值

下图显示了上表中所述的负载平衡示例值和必需参数。

图 2. 负载平衡实体模型



下表列出了使用命令行接口配置此负载平衡设置时使用的命令。

任务	命令
启用负载平衡	enable feature lb
创建服务 service-HTTP-1	add service service-HTTP-1 10.102.29.5 HTTP 80
创建服务 service-HTTP-2	add service service-HTTP-2 10.102.29.6 HTTP 80
创建名为 vserver-LB-1 的虚拟服务器	add lb vserver vserver-LB-1 HTTP 10.102.29.60 80
将服务 service-HTTP-1 绑定到虚拟服务器 vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-1
将服务 service-HTTP-2 绑定到虚拟服务器 vserver-LB-1	bind lb vserver vserver-LB-1 service-HTTP-2

表 2. 初始配置任务

有关初始配置任务的详细信息，请参阅设置基本负载平衡。

任务	命令
查看虚拟服务器 vserver-LB-1 的属性	show lb vserver vserver-LB-1
查看虚拟服务器 vserver-LB-1 的统计数据	stat lb vserver vserver-LB-1
查看服务 service-HTTP-1 的属性	show service service-HTTP-1
查看服务 service-HTTP-1 的统计数据	stat service service-HTTP-1
查看服务 service-HTTP-1 的绑定	show service bindings service-HTTP-1

表 3. 验证任务

任务	命令
在虚拟服务器 vserver-LB-1 上配置持久性	set lb vserver vserver-LB-1 -persistenceType SOURCEIP -persistenceMask 255.255.255.255 -timeout 2
在虚拟服务器 vserver-LB-1 上配置 COOKIEINSERT 持久性	set lb vserver vserver-LB-1 -persistenceType COOKIEINSERT
在虚拟服务器 vserver-LB-1 上配置 URLPassive 持久性	set lb vserver vserver-LB-1 -persistenceType URLPASSIVE
配置虚拟服务器，以将客户端请求重定向到虚拟服务器 vserver-LB-1 上的 URL	set lb vserver vserver-LB-1 -redirectURL http://www.newdomain.com/mysite/maintenance
在虚拟服务器 vserver-LB-1 上设置备份虚拟服务器	set lb vserver vserver-LB-1 -backupVserver vserver-LB-2

表 4. 自定义任务

有关配置持久性的详细信息，请参阅选择和配置持久性设置。 有关配置虚拟服务器以将客户端请求重定向到 URL ，以及设置备份虚拟服务器的信息，请参阅配置功能以保护负载平衡配置。

使用压缩加速负载平衡通信

December 15, 2021

压缩是优化带宽使用率的常用方法，大多数 Web 浏览器均支持压缩数据。如果启用了压缩功能，Citrix ADC 设备将拦截客户端发出的请求，并确定该客户端是否可接受压缩的内容。收到服务器发出的 HTTP 响应之后，设备将检查响应内容，以确定是否可对其进行压缩。如果内容是可压缩的，设备将对其进行压缩，修改响应标头以指明执行的压缩类型，并将压缩的内容转发到客户端。

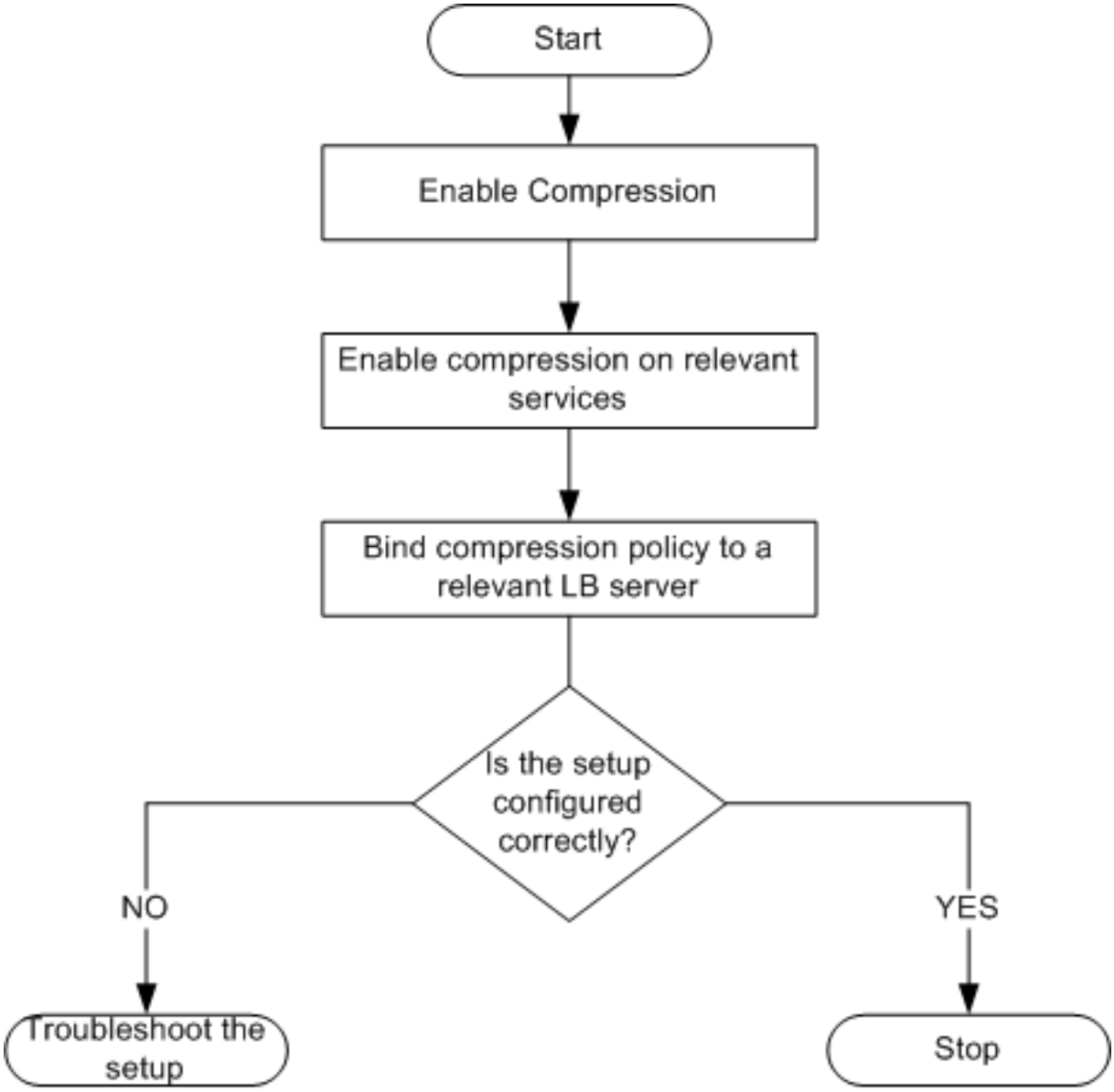
Citrix ADC 压缩是一项基于策略的功能。策略可过滤请求和响应以确定要压缩的响应，并指定要应用于每个响应的压缩类型。设备提供了多种内置策略来压缩常见的 MIME 类型，例如 text/html、text/plain、text/xml、text/css、text/rtf、application/msword、application/vnd.ms-excel 和 application/vnd.ms-powerpoint。您也可以创建自定义策略。设备不会压缩已压缩的 MIME 类型，例如 application/octet-stream、二进制数据、字节数据以及压缩图像格式（例如 GIF 和 JPEG）。

要配置压缩，您必须全局启用压缩，并对将提供要压缩的响应的每项服务启用压缩。如果您已配置用于负载平衡或内容交换的虚拟服务器，则应将策略绑定到这些虚拟服务器。否则，这些策略将应用于经由设备传输的所有通信。

压缩配置任务的顺序

下面的流程图显示了在一个负载平衡设置中，基本压缩配置任务的顺序。

图 1. 压缩配置任务的顺序



> 注意：上图中的步骤假定已配置负载平衡。

启用压缩

默认情况下不启用压缩。您必须启用压缩功能才能允许对发送给客户端的 HTTP 响应进行压缩。

使用 **CLI** 启用压缩

在命令提示窗口中，键入以下命令以启用压缩并验证配置：

- enable ns feature CMP
- show ns feature


```
    > enable ns feature CMP



     Done

    > show ns feature



            Feature                        Acronym              Status

            -------                        -------              ------

     1)     Web Logging                    WL                   ON

     2)     Surge Protection               SP                   OFF

     .

     7) Compression Control CMP ON

     8)     Priority Queuing               PQ                   OFF

     .

     Done
<!--NeedCopy-->
```

使用 **GUI** 启用压缩

1. 在导航窗格中，展开 System（系统），然后单击 Settings（设置）。
2. 在详细信息窗格中，单击 Modes and Features（模式与功能）下的 Change basic features（更改基本功能）。
3. 在“Configure Basic Features”（配置基本功能）对话框中，选择“Compression”（压缩）复选框，然后单击“OK”（确定）。
4. 在 Enable/Disable Feature(s)?（是否启用/禁用功能?）对话框中，单击 Yes（是）。

配置服务以压缩数据

除全局启用压缩外，您还必须对将交付要压缩的文件的每项服务启用压缩。

使用 **CLI** 对服务启用压缩

在命令提示窗口中，键入以下命令对服务启用压缩并验证配置：

- set service <name> -CMP YES
- show service <name>

```
> show service SVC_HTTP1


SVC_HTTP1 (10.102.29.18:80) - HTTP


State: UP


Last state change was at Tue Jun 16 06:19:14 2009 (+737 ms)


Time since last state change: 0 days, 03:03:37.200


Server Name: 10.102.29.18


Server ID : 0   Monitor Threshold : 0


Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits


Use Source IP: NO


Client Keepalive(CKA): NO


Access Down Service: NO


TCP Buffering(TCPB): NO


HTTP Compression(CMP): YES


Idle timeout: Client: 180 sec   Server: 360 sec
```



```


Client IP: DISABLED


Cacheable: NO


SC: OFF


SP: OFF


Down state flush: ENABLED




1)      Monitor Name: tcp-default


State: DOWN     Weight: 1


Probes: 1095    Failed [Total: 1095 Current: 1095]


Last response: Failure - TCP syn sent, reset received.


Response Time: N/A


Done
<!--NeedCopy-->
```

使用 **GUI** 对服务启用压缩

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Services（服务）。
2. 在详细信息窗格中，选择要为其配置压缩的服务（例如 service-HTTP-1），然后单击 Open（打开）。
3. 在“Advanced”（高级）选项卡上，选中“Settings”（设置）下的“Compression”（压缩）复选框，然后单击“OK”（确定）。
4. 确认当选中该服务时，“HTTP Compression(CMP): ON”（HTTP 压缩 (CMP): 开）是否在窗格底部的 **Details**（详细信息）部分中显示。

将压缩策略绑定到虚拟服务器

如果将策略绑定到虚拟服务器，该策略仅可由与该虚拟服务器相关联的服务进行评估。可使用 Configure Virtual Server (Load Balancing)（配置虚拟服务器 (负载平衡)）对话框或从 Compression Policy Manager（压缩策略管理器）对话框，将压缩策略绑定到虚拟服务器。本主题包含使用 Configure Virtual Server (Load Balancing)（配置虚拟服务器 (负载平衡)）对话框将压缩策略绑定到负载平衡虚拟服务器的说明。有关如何使用“Compression Policy Manager”（压缩策略管理器）对话框将压缩策略绑定到负载平衡虚拟服务器的信息，请参阅 Configuring and Binding Policies with the PolicyManager（使用策略管理器配置和绑定策略）。

使用命令行将压缩策略绑定到虚拟服务器，或取消压缩策略与虚拟服务器的绑定

在命令提示窗口中，键入以下命令，将压缩策略绑定到负载平衡虚拟服务器，或取消压缩策略与负载平衡虚拟服务器的绑定，并验证配置：

- (bind\|unbind) lb vserver <name> -policyName <string>
- show lb vserver <name>

示例：

```
      bind lb vserver lbvip -policyName ns_cmp_msapp
 Done
> show lb vserver lbvip
lbvip (8.7.6.6:80) - HTTP Type: ADDRESS
State: UP
Last state change was at Thu May 28 05:37:21 2009 (+685 ms)
Time since last state change: 19 days, 04:26:50.470
Effective State: UP
Client Idle Timeout: 180 sec
Down state flush: ENABLED
Disable Primary Vserver On Down : DISABLED
Port Rewrite : DISABLED
No. of Bound Services : 1 (Total) 1 (Active)
Configured Method: LEASTCONNECTION
Current Method: Round Robin, Reason: Bound service's state changed to
    UP
Mode: IP
Persistence: NONE
Vserver IP and Port insertion: OFF
Push: DISABLED Push VServer:
Push Multi Clients: NO
Push Label Rule:

Bound Service Groups:
1) Group Name: Service-Group-1

1) Service-Group-1 (10.102.29.252: 80) - HTTP State: UP Weight: 1

1) Policy : ns_cmp_msapp Priority:0
Done
```



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

使用 **GUI** 将压缩策略绑定到负载平衡虚拟服务器，或取消压缩策略与负载平衡虚拟服务器的绑定

1. 导航到 Traffic Management（流量管理）> Load Balancing（负载平衡）> Virtual Servers（虚拟服务器）。
2. 在详细信息窗格中，选择要将压缩策略绑定到或从其取消绑定的虚拟服务器，（例如 Vserver-LB-1），然后单击 Open（打开）。
3. 在 Configure Virtual Server (Load Balancing)（配置虚拟服务器 (负载平衡)）对话框中，单击 Policies（策略）选项卡上的 Compression（压缩）。
4. 执行以下操作之一：
   - 要绑定压缩策略，请单击 Insert Policy（插入策略），然后选择要绑定到虚拟服务器的策略。
   - 要取消绑定压缩策略，请单击要从虚拟服务器取消绑定的策略的名称，然后单击 Unbind Policy（取消绑定策略）。
5. 单击确定。

使用 **SSL** 保护负载平衡通信

December 15, 2021

Citrix ADC SSL 卸载功能可明显改进执行 SSL 事务的 Web 站点的性能。通过将 CPU 密集型 SSL 加密和解密任务从本地 Web 服务器卸载到设备，SSL 卸载功能可确保 Web 应用程序能够安全交付，且不会在服务器处理 SSL 数据时导致性能下降。解密 SSL 通信之后，所有标准服务都可以对其进行处理。SSL 协议可以无缝运用于各种类型的 HTTP 和 TCP 数据，为使用此类数据的事务提供安全通道。

要配置 SSL，您必须首先启用 SSL。然后，在设备上配置 HTTP 或 TCP 服务以及 SSL 虚拟服务器，并将这些服务绑定到该虚拟服务器。还必须添加一个证书密钥对，并将其绑定到 SSL 虚拟服务器。如果使用 Outlook Web Access 服务器，则必须创建一个操作以启用 SSL 支持，并创建策略以应用该操作。SSL 虚拟服务器可拦截传入的加密的通信，并使用协商确定的算法对其进行解密。然后，SSL 虚拟服务器将解密的数据转发到设备上的其他实体，以进行相应的处理。

有关 SSL 卸载的详细信息，请参阅 SSL 卸载和加速。

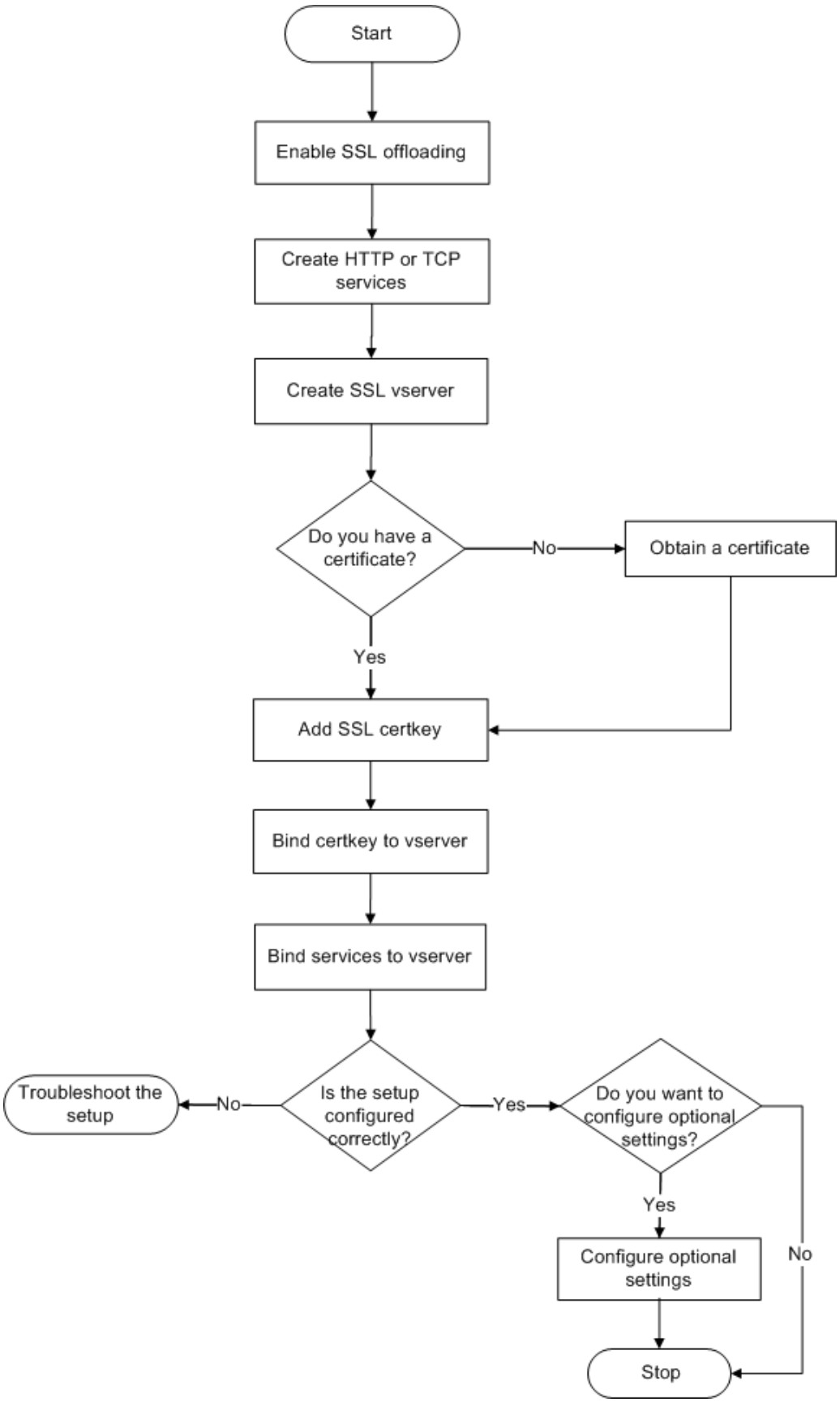
SSL 配置任务的顺序

要配置 SSL，您必须首先启用 SSL。然后，必须在 Citrix ADC 设备上创建 SSL 虚拟服务器和 HTTP 或 TCP 服务。最后，必须将一个有效的 SSL 证书和已配置的服务绑定到该 SSL 虚拟服务器。

SSL 虚拟服务器可拦截传入的加密通信，并使用协商确定的算法对其进行解密。然后，SSL 虚拟服务器将解密的数据转发到 Citrix ADC 设备上的其他实体，以进行相应的处理。

下面的流程图显示了基本 SSL 卸载设置配置任务的顺序。

图 1. SSL 卸载配置任务的顺序



启用 SSL 卸载

必须先启用 SSL 功能，然后才能配置 SSL 卸载。虽然无需启用 SSL 功能即可在设备上配置基于 SSL 的实体，但必须启用 SSL，这些实体才能运行。

使用 CLI 启用 SSL

在命令提示窗口中，键入以下命令以启用 SSL 卸载并验证配置：

- enable ns feature SSL
- show ns feature

```
> enable ns feature ssl



Done


> show ns feature


Feature Acronym Status


------- ------- ------


1) Web Logging WL ON


2) SurgeProtection SP OFF


3) Load Balancing LB ON . . .


 9) SSL Offloading SSL ON


10) Global Server Load Balancing GSLB ON . .


Done >
<!--NeedCopy-->
```


使用 **GUI** 启用 **SSL**

1. 在导航窗格中，展开 **System**（系统），然后单击 **Settings**（设置）。
2. 在详细信息窗格中，单击 **Modes and Features**（模式与功能）下的 **Change basic features**（更改基本功能）。
3. 选中 **SSL Offloading**（SSL 卸载）复选框，然后单击 **OK**（确定）。
4. 在 **Enable/Disable Feature(s)?**（是否启用/禁用功能?）消息框中，单击 **Yes**（是）。

创建 **HTTP** 服务

设备上的服务表示服务器上的应用程序。配置后，服务处于禁用状态，直到设备可访问网络中的服务器并监视其状态。本主题包含创建 HTTP 服务的步骤。

注意：对于 TCP 流量，请执行此主题和接下来的主题中介绍的步骤，但需创建 TCP 服务而非 HTTP 服务。

使用 **CLI** 添加 **HTTP** 服务

在命令提示窗口中，键入以下命令以添加 HTTP 服务并验证配置：

```
-  add service <name> (<IP> | <serverName>) <serviceType> <port>
-  show service <name>
<!--NeedCopy-->
```

示例：

```
> add service SVC_HTTP1 10.102.29.18 HTTP 80


 Done


> show service SVC_HTTP1


        SVC_HTTP1 (10.102.29.18:80) - HTTP


        State: UP


        Last state change was at Wed Jul 15 06:13:05 2009


        Time since last state change: 0 days, 00:00:15.350


        Server Name: 10.102.29.18

```



```

        Server ID : 0   Monitor Threshold : 0


        Max Conn: 0     Max Req: 0      Max Bandwidth: 0 kbits


        Use Source IP: NO


        Client Keepalive(CKA): NO


        Access Down Service: NO


        TCP Buffering(TCPB): NO


        HTTP Compression(CMP): YES


        Idle timeout: Client: 180 sec   Server: 360 sec


        Client IP: DISABLED


        Cacheable: NO


        SC: OFF


        SP: OFF


        Down state flush: ENABLED




1)      Monitor Name: tcp-default


                State: UP       Weight: 1


                Probes: 4       Failed [Total: 0 Current: 0]


                Last response: Success - TCP syn+ack received.
```



```


                    Response Time: N/A


 Done



<!--NeedCopy-->
```

使用 **GUI** 添加 **HTTP** 服务

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL Offload**（**SSL** 卸载）**> Services**（服务）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Create Service**（创建服务）对话框中，将服务名称、IP 地址和端口（例如 SVC_HTTP1、10.102.29.18 和 80）分别键入到“Service Name”（服务名称）、“Server”（服务器）和“Port”（端口）文本框中。
4. 在 **Protocol**（协议）列表中选择服务类型，例如 HTTP。
5. 单击 **Create**（创建），然后单击 **Close**（关闭）。此时 Services（服务）页面中将显示您配置的 HTTP 服务。
6. 选择该服务并查看窗格底部的 Details（详细信息）部分，确认您配置的参数已正确配置。

添加基于 **SSL** 的虚拟服务器

在基本 SSL 卸载设置中，SSL 虚拟服务器可拦截加密的通信，将其解密，并将明文消息发送到绑定到该虚拟服务器的服务。将 CPU 密集型 SSL 处理卸载到设备可使后端服务器能够处理更多请求。

使用 **CLI** 添加基于 **SSL** 的虚拟服务器

在命令提示窗口中，键入以下命令以创建基于 SSL 的虚拟服务器并验证配置：

```
-  add lb vserver <name> <serviceType> [<IPAddress> <port>]
-  show lb vserver <name>
<!--NeedCopy-->
```

> 小心：为确保安全连接，在启用基于 SSL 的虚拟服务器之前，必须将一个有效的 SSL 证书绑定到该虚拟服务器。

示例：

```
> add lb vserver vserver-SSL-1 SSL 10.102.29.50 443



```



```
  Done


 > show lb vserver vserver-SSL-1


  vserver-SSL-1 (10.102.29.50:443) - SSL Type: ADDRESS


  State: DOWN[Certkey not bound] Last state change was at Tue Jun 16
     06:33:08 2009 (+176 ms)


  Time since last state change: 0 days, 00:03:44.120


  Effective State: DOWN Client Idle Timeout: 180 sec


  Down state flush: ENABLED


  Disable Primary Vserver On Down : DISABLED


  No. of Bound Services : 0 (Total) 0 (Active)


  Configured Method: LEASTCONNECTION Mode: IP


  Persistence: NONE


  Vserver IP and Port insertion: OFF


  Push: DISABLED Push VServer: Push Multi Clients: NO Push Label Rule:
     Done
<!--NeedCopy-->
```

使用 **GUI** 添加基于 **SSL** 的虚拟服务器

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL Offload**（**SSL** 卸载）**> Virtual Servers**（虚拟服务器）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Create Virtual Server (SSL Offload)**（创建虚拟服务器 (SSL 卸载)）对话框中，在“Name”（名称）、“IP Address”（IP 地址）和“Port”（端口）文本框中分别键入虚拟服务器的名称、IP 地址和端口（例如 Vserver-SSL-1、10.102.29.50 和 443)）。

4. 在 **Protocol**（协议）列表中选择虚拟服务器的类型，例如 SSL。
5. 单击 **Create**（创建），然后单击 **Close**（关闭）。
6. 选择虚拟服务器并查看窗格底部的 Details（详细信息）部分，确认您配置的参数已正确配置。该虚拟服务器标记为“DOWN”（关闭），因为尚未对其绑定证书密钥对和服务。

> 小心：为确保安全连接，在启用基于 SSL 的虚拟服务器之前，必须将一个有效的 SSL 证书绑定到该虚拟服务器。

将服务绑定到 **SSL** 虚拟服务器

解密传入数据之后，SSL 虚拟服务器会将数据转发到与该虚拟服务器绑定的服务。

可以加密设备与服务器之间的数据传输，也可通过明文方式传输。如果设备与服务器之间的数据传输已加密，则端到端的整个事务将是安全的。有关如何为系统配置端到端安全性的详细信息，请参阅 SSL 卸载和加速。

使用 **CLI** 将服务绑定到虚拟服务器

在命令提示窗口中，键入以下命令以将服务绑定到 SSL 虚拟服务器并验证配置：

```
-  bind lb vserver <name> <serviceName>
-  show lb vserver <name>
<!--NeedCopy-->
```

示例：

```
> bind lb vserver vserver-SSL-1 SVC_HTTP1




  Done


 > show lb vserver vserver-SSL-1 vserver-SSL-1 (10.102.29.50:443) - SSL
     Type:


  ADDRESS State: DOWN[Certkey not bound]


  Last state change was at Tue Jun 16 06:33:08 2009 (+174 ms)


  Time since last state change: 0 days, 00:31:53.70


  Effective State: DOWN Client Idle


  Timeout: 180 sec
```



```


  Down state flush: ENABLED Disable Primary Vserver On Down :


  DISABLED No. of Bound Services : 1 (Total) 0 (Active)


  Configured Method: LEASTCONNECTION Mode: IP Persistence: NONE Vserver
      IP and


  Port insertion: OFF Push: DISABLED Push VServer: Push Multi Clients:
     NO Push Label Rule:




  1) SVC_HTTP1 (10.102.29.18: 80) - HTTP


  State: DOWN Weight: 1


  Done
<!--NeedCopy-->
```

使用 **GUI** 将服务绑定到虚拟服务器

1. 导航到 **Traffic Management**（流量管理）**> SSL Offload**（**SSL** 卸载）**> Virtual Servers**（虚拟服务器）。
2. 在详细信息窗格中，选择虚拟服务器，然后单击 **Open**（打开）。
3. 在 **Services**（服务）选项卡上的 **Active**（活动）列中，选中要绑定到所选虚拟服务器的服务旁边的复选框。
4. 单击确定。
5. 确认窗格底部 Details（详细信息）部分中的 Number of Bound Services（绑定服务数）计数器按绑定到虚拟服务器的服务数量递增。

添加证书密钥对

SSL 证书是 SSL 密钥交换和加密-解密过程不可或缺的元素。该证书在 SSL 握手过程中用于创建 SSL 服务器的标识。可以使用 Citrix ADC 设备上现有的有效 SSL 证书，也可以创建您自己的 SSL 证书。此设备支持高达 4096 位的 RSA/DSA 证书。

> 注意：
>
> Citrix 建议您使用由受信任的证书颁发机构所颁发的有效 SSL 证书。所有 SSL 客户端均不兼容无效证书和自创

> 建的证书。

必须首先将证书与其相应的密钥进行配对，然后才能将其用于 SSL 处理。然后，证书密钥对将绑定到虚拟服务器，用于 SSL 处理。

使用 **CLI** 添加证书密钥对

在命令提示窗口中，键入以下命令以创建证书密钥对并验证配置：

```
-  add ssl certKey <certkeyName> -cert <string> [-key <string>]
-  show sslcertkey <name>
<!--NeedCopy-->
```

示例：

```
> add ssl certKey CertKey-SSL-1 -cert ns-root.cert -key ns-root.key
 Done


> show sslcertkey CertKey-SSL-1


   Name: CertKey-SSL-1 Status: Valid,


   Days to expiration:4811 Version: 3


   Serial Number: 00 Signature Algorithm: md5WithRSAEncryption Issuer:
      C=US,ST=California,L=San


   Jose,O=Citrix ANG,OU=NS Internal,CN=de fault


   Validity Not Before: Oct 6 06:52:07 2006 GMT Not After : Aug 17
      21:26:47 2022 GMT


   Subject: C=US,ST=California,L=San Jose,O=Citrix ANG,OU=NS Internal,
      CN=d efault Public Key


   Algorithm: rsaEncryption Public Key


   size: 1024


 Done
<!--NeedCopy-->
```


使用 **GUI** 添加证书密钥对

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL > Certificates**（证书）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Install Certificate**（安装证书）对话框中，将要添加的证书密钥对的名称（例如 Certkey-SSL-1）键入到 Certificate-Key Pair Name（证书密钥对名称）文本框中。
4. 在 **Details**（详细信息）下，单击 **Certificate File Name**（证书文件名称）中的 **Browse (Appliance)**（浏览 (设备)）查找证书。证书和密钥均存储在设备的 /nsconfig/ssl/ 文件夹中。要使用本地系统上的证书，请选择 **Local**（本地）。
5. 选择要使用的证书，然后单击 **Select**（选择）。
6. 在 **Private Key File Name**（私钥文件名称）中，单击 **Browse (Appliance)**（浏览 (设备)）查找私钥文件。要使用本地系统上的私钥，请选择 **Local**（本地）。
7. 选择要使用的私钥，然后单击 **Select**（选择）。要对证书密钥对中使用的密钥进行加密，请在 Password（密码）文本框中键入用于加密的密码。
8. 单击安装。
9. 双击证书密钥对，并在 Certificate Details（证书详细信息）窗口中确认参数配置正确并已保存。

将 **SSL** 证书密钥对绑定到虚拟服务器

将 SSL 证书与其对应的密钥配对后，必须将证书密钥对绑定到 SSL 虚拟服务器，使其可用于 SSL 处理。要进行安全会话，需要在客户端计算机与设备上基于 SSL 的虚拟服务器之间建立连接。然后，该虚拟服务器才会对传入流量执行 SSL 处理。因此，在设备上启用 SSL 虚拟服务器之前，必须将一个有效的 SSL 证书绑定到该 SSL 虚拟服务器。

使用 **CLI** 将 **SSL** 证书密钥对绑定到虚拟服务器

在命令提示窗口中，键入以下命令以将 SSL 证书密钥对绑定到虚拟服务器并验证配置：

```
-  bind ssl vserver <vServerName> -certkeyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

示例：

```
> bind ssl vserver Vserver-SSL-1 -certkeyName CertKey-SSL-1




Done


> show ssl vserver Vserver-SSL-1
```



```
10
11
12
13
14
15      Advanced SSL configuration for VServer Vserver-SSL-1:
16
17
18      DH: DISABLED
19
20
21      Ephemeral RSA: ENABLED Refresh Count: 0
22
23
24      Session Reuse: ENABLED Timeout: 120 seconds
25
26
27      Cipher Redirect: ENABLED
28
29
30      SSLv2 Redirect: ENABLED
31
32
33      ClearText Port: 0
34
35
36      Client Auth: DISABLED
37
38
39      SSL Redirect: DISABLED
40
41
42      Non FIPS Ciphers: DISABLED
43
44
45      SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED
46
47
48
49
50
51  1) CertKey Name: CertKey-SSL-1 Server Certificate
52
53
54  1) Cipher Name: DEFAULT
55
56
57     Description: Predefined Cipher Alias
58
59
60  Done
61  <!--NeedCopy-->
```


使用 **GUI** 将 **SSL** 证书密钥对绑定到虚拟服务器

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL Offload**（**SSL** 卸载）**> Virtual Servers**（虚拟服务器）。
2. 选择要绑定证书密钥对的虚拟服务器（例如 Vserver-SSL-1），然后单击 **Open**（打开）。
3. 在 **Configure Virtual Server (SSL Offload)**（配置虚拟服务器 (SSL 卸载)）对话框中，从 **SSL Settings**（SSL 设置）选项卡上的 **Available**（可用）下，选择要绑定到虚拟服务器的证书密钥对（例如 Certkey-SSL-1），然后单击 **Add**（添加）。
4. 单击确定。
5. 确认您选择的证书密钥对显示在 Configured（已配置）区域中。

配置对 **Outlook Web Access** 的支持

如果您在 Citrix ADC 设备上使用 Outlook Web Access (OWA) 服务器，则必须配置此设备，以便将一个特殊标头字段 FRONT-END-HTTPS: ON 插入到定向至 OWA 服务器的 HTTP 请求中，从而使这些服务器生成 `https://` 而非 `http://` 类型的 URL 链接。

注意：只能为基于 HTTP 的 SSL 虚拟服务器和服务启用 OWA 支持。不能将其应用于基于 TCP 的 SSL 虚拟服务器和服务。

要配置 OWA 支持，请执行以下操作：

- 创建一个 SSL 操作以启用 OWA 支持。
- 创建一个 SSL 策略。
- 将策略绑定到 SSL 虚拟服务器。

创建一个 **SSL** 操作以启用 **OWA** 支持

要启用 Outlook Web Access (OWA) 支持，必须创建 SSL 操作。SSL 操作绑定到 SSL 策略，并在传入数据与该策略指定的规则相匹配时触发。

使用 **CLI** 创建 **SSL** 操作以启用 **OWA** 支持

在命令提示窗口中，键入以下命令来创建 SSL 操作以启用 OWA 支持并验证配置：

```
-  add ssl action <name> -OWASupport ENABLED
-  show SSL action <name>
<!--NeedCopy-->
```

示例：


```
    > add ssl action Action-SSL-OWA -OWASupport enabled



     Done


    > show SSL action Action-SSL-OWA


     Name: Action-SSL-OWA


     Data Insertion Action: OWA


     Support: ENABLED


     Done
<!--NeedCopy-->
```

使用 **GUI** 创建 **SSL** 操作以启用 **OWA** 支持

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL > Policies**（策略）。
2. 在详细信息窗格中，单击 **Actions**（操作）选项卡上的 **Add**（添加）。
3. 在 **Create SSL Action**（创建 SSL 操作）对话框的 **Name**（名称）文本框中，键入 `Action-SSL-OWA`。
4. 在“Outlook Web Access”下，选择 **Enabled**（已启用）。
5. 单击 **Create**（创建），然后单击 **Close**（关闭）。
6. 确认 Action-SSL-OWA 显示在 **SSL Actions**（SSL 操作）页面中。

创建 **SSL** 策略

SSL 策略是使用策略基础结构创建的。每个 SSL 策略都具有一个绑定的 SSL 操作，在传入通信与该策略中配置的规则相匹配时执行该操作。

使用 **CLI** 创建 **SSL** 策略

在命令提示窗口中，键入以下命令以配置 SSL 策略并验证配置：

```
-  add ssl policy <name> -rule <expression> -reqAction <string>
-  show ssl policy <name>
```



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

示例：

```
> add ssl policy Policy-SSL-1 -rule ns_true -reqaction Action-SSL-OWA

Done

> show ssl policy Policy-SSL-1

Name: Policy-SSL-1 Rule: ns_true

Action: Action-SSL-OWA Hits: 0

Policy is bound to following entities

1) PRIORITY : 0

Done
<!--NeedCopy-->
```

使用 **GUI** 创建 **SSL** 策略

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL > Policies**（策略）。
2. 在详细信息窗格中，单击 **Add**（添加）。
3. 在 **Create SSL Policy**（创建 SSL 策略）对话框的 **Name**（名称）文本框中，键入 SSL 策略的名称（例如，Policy-SSL-1）。
4. 在 **Request Action**（请求操作）中，选择要与此策略关联的已配置 SSL 操作，例如 Action-SSL-OWA。`ns_true` 正则表达式可将策略应用于所有成功的 SSL 握手通信。但是，如果必须过滤特定的响应，可以使用更为详细的信息来创建策略。有关配置精细策略表达式的详细信息，请参阅 SSL 操作和策略。
5. 在 **Named Expressions**（命名表达式）下，选择内置的正则表达式 ns_true，然后单击 **Add Expression**（添加表达式）。此时“Expression”（表达式）文本框中将出现表达式 ns_true。
6. 单击 **Create**（创建），然后单击 **Close**（关闭）。
7. 选择策略并查看窗格底部的 Details（详细信息）部分，确认该策略配置正确。

将 **SSL** 策略绑定到 **SSL** 虚拟服务器

为 Outlook Web Access 配置 SSL 策略后，将此策略绑定到将解析传入 Outlook 流量的虚拟服务器。如果传入数据与在 SSL 策略中配置的任何规则匹配，则将触发该策略并执行与其关联的操作。

使用 **CLI** 将 **SSL** 策略绑定到 **SSL** 虚拟服务器

在命令提示窗口中，键入以下命令以将 SSL 策略绑定到 SSL 虚拟服务器并验证配置：

```
-  bind ssl vserver <vServerName> -policyName <string>
-  show ssl vserver <name>
<!--NeedCopy-->
```

示例：

```
> bind ssl vserver Vserver-SSL-1 -policyName Policy-SSL-1

 Done

> show ssl vserver Vserver-SSL-1

Advanced SSL configuration for VServer Vserver-SSL-1:

DH: DISABLED

Ephemeral RSA: ENABLED

Refresh Count: 0

Session Reuse: ENABLED

Timeout: 120 seconds

Cipher Redirect: ENABLED

SSLv2 Redirect: ENABLED

ClearText Port: 0

Client Auth: DISABLED

SSL Redirect: DISABLED

Non FIPS Ciphers: DISABLED

SSLv2: DISABLED SSLv3: ENABLED TLSv1: ENABLED

1) CertKey Name: CertKey-SSL-1 Server Certificate

1) Policy Name: Policy-SSL-1 Priority: 0

1) Cipher Name: DEFAULT Description: Predefined Cipher Alias

Done
<!--NeedCopy-->
```


使用 **GUI** 将 **SSL** 策略绑定到 **SSL** 虚拟服务器

请按照以下步骤进行操作：

1. 导航到 **Traffic Management**（流量管理）**> SSL Offload**（**SSL** 卸载）**> Virtual Servers**（虚拟服务器）。
2. 在详细信息窗格中，选择虚拟服务器（例如 Vserver-SSL-1），然后单击 **Open**（打开）。
3. 在 “Configure Virtual Server (SSL Offload)”（配置虚拟服务器 (SSL 卸载)）对话框中，单击 **Insert Policy**（插入策略），然后选择要绑定到 SSL 虚拟服务器的策略。也可以双击 Priority（优先级）字段并键入新的优先级。
4. 单击确定。

功能概览

January 27, 2022

各种 Citrix ADC 功能既可以单独配置，也可以结合使用来满足特定需要。虽然某些功能可归为多种类别，但多数 Citrix ADC 功能通常可以分为以下几类：应用程序交换和流量管理功能、应用程序加速功能、应用程序安全性和防火墙功能以及应用程序可视性功能。

要了解各功能执行其处理的顺序，请参阅功能的处理顺序部分。

应用程序交换和流量管理功能

April 8, 2022

下面是应用程序切换和流量管理功能。

SSL 卸载

从 Web 服务器透明地卸载 SSL 加密和解密，从而释放服务器资源，以便处理内容请求。SSL 对应用程序的性能造成沉重负担，会导致许多优化措施不起作用。使用 SSL 卸载与加速可以将 Citrix 请求切换技术的所有优势应用于 SSL 流量，确保安全交付 Web 应用程序而不会降低最终用户性能。

有关详细信息，请参阅 SSL 卸载与加速。

访问控制列表

将传入的数据包与访问控制列表 (ACL) 进行比较。如果某个数据包与 ACL 规则相匹配，则此规则中指定的操作将应用于该数据包。否则将应用默认操作 (ALLOW)，此时该数据包将正常进行处理。要使设备将传入的数据包与 ACL 进行比

较，您需要应用 ACL。所有 ACL 在默认情况下都处于启用状态，但是要使 Citrix ADC 设备将传入的数据包与 ACL 进行比较，您必须应用这些 ACL。如果某个 ACL 不必是查找表的一部分，但仍需保留在配置中，则应该在应用之前将其禁用。ADC 设备不会将传入的数据包与禁用的 ACL 进行比较。

有关详细信息，请参阅访问控制列表。

负载平衡

负载平衡决策基于多种算法制定，包括轮询、最少连接、加权最小带宽、加权最少数据包、最短响应时间以及基于 URL、域源 IP 或目标 IP 的哈希。支持 TCP 和 UDP 协议，因此 Citrix ADC 设备可以对使用这些协议作为基础载波的所有流量（例如，HTTP、HTTPS、UDP、DNS、NNTP 和一般防火墙流量）进行负载平衡。此外，ADC 设备可以基于源 IP、Cookie、服务器、组或 SSL 会话维护会话持久性。NetScaler 允许用户将自定义扩展内容验证 (ECV) 应用于服务器、缓存、防火墙及其他基础结构设备，以确保这些系统正常工作并为用户提供正确的内容。它还可以使用 Ping、TCP 或 HTTP URL 执行运行状况检查，而用户可以基于 Perl 脚本创建监视程序。
为了提供高规格的 WAN 优化，可通过 Citrix ADC 设备对数据中心部署的 CloudBridge 设备进行负载平衡。这样可以显著提高带宽和并发会话数。

有关详细信息，请参阅负载平衡。

流量域

流量域提供了在单个 Citrix ADC 设备中创建逻辑 ADC 分区的方法。通过流量域可以为不同的应用程序进行网络流量分段。可以使用流量域创建多个隔离环境，其中的资源相互不进行交互。属于特定流量域的应用程序只与该域中的实体进行通信并在该域中处理流量。属于某个流量域的流量不能跨越另一个流量域的边界。因此，只要地址在同一个域中不重复，即可在设备上使用重复的 IP 地址。

有关详细信息，请参阅流量域。

网络地址转换

网络地址转换 (NAT) 涉及修改经过 Citrix ADC 设备的 IP 数据包的源和/或目标 IP 地址和/或 TCP/UDP 端口号。在该设备上启用 NAT 可以增强您的专用网络的安全性，在数据通过 Citrix ADC 设备时修改网络的源 IP 地址，保护专用网络不受公用网络（例如 Internet）的干扰。

Citrix ADC 设备支持以下类型的网络地址转换：

INAT：在入站 NAT (INAT) 中，在 Citrix ADC 设备上配置的 IP 地址（通常为公用 IP 地址）将代表服务器侦听连接请求。对于设备在公用 IP 地址上收到的请求数据包，ADC 将使用服务器的专用 IP 地址替换目标 IP 地址。换言之，设备在客户端和服务器之间起到了代理的作用。INAT 配置涉及 INAT 规则，该规则定义了 Citrix ADC 设备上 IP 地址与服务器的 IP 地址之间的 1:1 关系。

RNAT — 在反向 NAT (RNAT) 中，对于服务器发起的会话，Citrix ADC 设备将使用设备上配置的 IP 地址（SNIP 类型）替换服务器生成的数据包中的源 IP 地址。因此，设备可防止泄露服务器生成的任何数据包中的服务器 IP 地址。RNAT 配置涉及 RNAT 规则，该规则指定了条件。设备将在与条件相匹配的数据包中执行 RNAT 处理。

无状态 **NAT46** 转换：无状态 NAT46 可通过 IPv4 到 IPv6 的数据包转换启用 IPv4 网络和 IPv6 网络之间的通信，反之亦然，它不会在 Citrix ADC 设备上保留任何会话信息。无状态 NAT46 配置涉及 IPv4-IPv6 INAT 规则和 NAT46 IPv6 前缀。

有状态 **NAT64** 转换 — 有状态 NAT64 功能可通过 IPv6 到 IPv4 的数据包转换启用 IPv4 客户端和 IPv6 服务器之间的通信，反之亦然，同时在 Citrix ADC 设备上保留会话信息。有状态 NAT64 配置涉及 NAT64 规则和 NAT64 IPv6 前缀。

有关详细信息，请参阅配置网络地址转换。

多路径 **TCP** 支持

Citrix ADC 设备支持多路径 TCP (MPTCP)。MPTCP 是 TCP/IP 协议的扩展，用于标识和使用可在主机之间使用以维护 TCP 会话的多个路径。必须在 TCP 配置文件上启用 MPTCP，并将其绑定到虚拟服务器。启用 MPTCP 时，虚拟服务器充当 MPTCP 网关，并将与客户端的 MPTCP 连接转换为与服务器的 TCP 连接。

有关详细信息，请参阅 MPTCP（多路 TCP）。

内容交换

根据配置的内容交换策略确定要将请求发送到的服务器。可以基于 IP 地址、URL 和 HTTP 标头配置策略规则。这允许交换决策基于用户和设备特性进行，例如用户的身份、所用代理的类型以及用户所请求的内容。

有关详细信息，请参阅内容交换。

全局服务器负载平衡 **(GSLB)**

扩展 NetScaler 的流量管理功能，使其包括分布式 Internet 站点和全球企业。无论安装是分布在多个网络位置还是单个位置中的多个群集，NetScaler 都可以在它们之间维护可用性并分配流量。NetScaler 可做出智能 DNS 决策，从而防止将用户发送至关闭或过载的站点。启用了基于邻近度的 GSLB 方法时，NetScaler 可以根据客户端的本地 DNS 服务器 (LDNS) 相对于不同站点的邻近程度，做出负载平衡决策。基于邻近度的 GSLB 方法的主要优点是，通过选择最接近的可用站点加快响应速度。

有关详细信息，请参阅全局服务器负载平衡。

动态路由

使路由器可以自动从邻近的路由器获取拓扑信息、路由和 IP 地址。启用了动态路由时，相应的路由进程将侦听路由更新并公告路由。还可以将路由进程置于被动模式。路由协议使上游路由器可以使用等价多路径技术，通过负载平衡将流量

分配到托管在两台独立 NetScaler 设备上的相同虚拟服务器。

有关详细信息，请参阅配置动态路由。

链路负载平衡

对多个 WAN 链路进行负载平衡并提供链路故障转移，从而进一步优化网络性能并确保业务持续性。通过应用智能流量控制和运行状况检查以在上游路由器之间有效地分配流量，确保网络连接保持高可用性。根据策略和网络条件，确定对传入流量和传出流量进行路由的最佳 WAN 链路，并通过提供快速的故障检测和故障转移功能，使应用程序免受 WAN 或 Internet 链路失败影响。

有关详细信息，请参阅链路负载平衡。

TCP 优化

可以使用 TCP 配置文件优化 TCP 流量。TCP 配置文件定义了 NetScaler 虚拟服务器处理 TCP 流量的方式。管理员可以使用内置 TCP 配置文件，也可以配置自定义配置文件。定义 TCP 配置文件后，可以将其绑定到单个虚拟服务器或绑定到多个虚拟服务器。

可以通过 TCP 配置文件启用的一些主要优化功能如下所示：

- TCP 保持活动状态 — 按指定的时间间隔检查对等机的运行状态，以防止链路中断。
- 选择性确认 (SACK) — 提高数据传输的性能，尤其是在长肥网络中 (Long Fat Network, LFN)。
- TCP 窗口缩放 — 允许通过长肥网络 (LFN) 有效地传输数据。

有关 TCP 配置文件的详细信息，请参阅配置 TCP 配置文件。

CloudBridge 连接器

Citrix NetScaler CloudBridge
连接器功能是 Citrix OpenCloud 框架的基本组成部分，是一款用于构建云扩展数据中心的工具。通过 OpenCloud Bridge，您无需重新配置网络便可将云中的一个或多个 Citrix ADC 设备或 NetScaler 虚拟设备连接到网络。云托管应用程序看似在一个连续的企业网络中运行。OpenCloud Bridge 的主要用途是允许公司将其应用程序移至云中，从而降低成本和应用程序故障的风险。此外，OpenCloud Bridge 还可增强云环境中的网络安全性。OpenCloud Bridge 是一个 2 层网络桥，可将云实例中的 Citrix ADC 设备或 NetScaler 虚拟设备连接到局域网中的 Citrix ADC 设备或 NetScaler 虚拟设备。此连接通过使用基本路由封装 (GRE) 协议的通道实现。GRE 协议提供一种机制，可以封装来自各种网络协议的数据包，以便通过其他协议来转发。然后，Internet 协议安全 (IPsec) 协议套件用于确保 OpenCloud Bridge 中对等端之间的通信安全。

有关详细信息，请参阅 CloudBridge。

DataStream

NetScaler DataStream 功能提供了一种智能机制，可根据发送的 SQL 查询分配请求，从而在数据库层实现请求交换。

在数据库服务器之前部署时，NetScaler 可确保以最优方式分配来自应用程序服务器和 Web 服务器的流量。管理员可以根据 SQL 查询中的信息并基于数据库名称、用户名、字符集和数据包大小对流量进行分段。

可以配置负载平衡以基于负载平衡算法来交换请求，或者通过配置内容交换来详细制定交换标准，从而根据 SQL 查询参数（如用户名和数据库名称）及命令参数来制定决策。可以进一步配置监视器，以跟踪数据库服务器的状态。

Citrix ADC 设备上的高级策略基础结构包括可用于评估和处理请求的表达式。高级表达式可计算与 MySQL 数据库服务器关联的流量。可以在高级策略中使用基于请求的表达式（以 MYSQL.CLIENT 和 MYSQL.REQ 开头的表达式），在内容交换虚拟服务器绑定点制定请求切换决策，并可使用基于响应的表达式（以 MYSQL.RES 开头的表达式）评估对服务器用户配置的运行状况监视器的响应。

注意： MySQL 和 MS SQL 数据库支持 DataStream。

有关详细信息，请参阅 DataStream。

应用程序加速功能

December 15, 2021

- AppCompress

  使用 gzip 压缩协议为 HTML 和文本文件提供透明压缩。典型的 4:1 压缩比最多可减少数据中心外 50% 的带宽需求。此功能还可以减少必须传送至用户的浏览器的数据量，从而极大地缩短最终用户响应时间。

- 缓存重定向

  管理流向反向代理、透明代理或正向代理缓存场的流量。检查所有请求，并识别不可缓存的请求，然后通过持续型连接将其直接发送到源服务器。通过智能地将不可缓存的请求重定向回原始 Web 服务器，Citrix ADC 设备可在减少这些请求的总带宽消耗和响应延迟的同时，释放缓存资源并提高缓存命中率。

  有关详细信息，请参阅缓存重定向。

- AppCache

  通过为静态和动态内容提供符合 HTTP/1.1 和 HTTP/1.0 的快速内存中 Web 缓存，帮助优化 Web 内容和应用程序数据交付。此板载缓存可存储传入的应用程序请求结果，即使当传入的请求受保护或数据被压缩时也是如此，然后重复利用这些数据来满足对相同信息的后续请求。通过直接从板载缓存提供数据，设备消除了将静态和动态内容请求传送到服务器的需要，从而减少页面重新生成次数。

  有关详细信息，请参阅集成缓存。

- TCP 缓存

  缓冲服务器的响应并以客户端的速度将其传送给客户端，因此更快地卸载服务器，进而改善 Web 站点的性能。

应用程序安全性和防火墙功能

December 15, 2021

下面是安全性和防火墙功能。

拒绝服务 **(DoS)** 攻击防御

检测恶意的分布式拒绝服务 (DDoS) 攻击及其他类型的恶意攻击，并在这些攻击到达服务器之前阻止它们，防止其影响网络和应用程序性能。Citrix ADC 设备识别合法的客户端并提升其优先级，使可疑的客户端无法消耗过高比例的资源而使您的站点陷于瘫痪。设备提供可防止以下类型的恶意攻击的应用程序级别保护：

- SYN Flood 攻击
- Pipeline 攻击
- Teardrop 攻击
- Land 攻击
- Fraggle 攻击
- Zombie 连接攻击

通过防止为相应连接分配服务器资源，设备积极地防御这些类型的攻击。这样可以使服务器免遭与这些事件关联的数据包洪流的攻击。

通过使用 ICMP 速率限制和积极的 ICMP 数据包检测，设备还可以保护网络资源免受基于 ICMP 的攻击。它可执行强大的 IP 重组，删除各种可疑和畸形的数据包，并将访问控制列表 (ACL) 应用于站点流量以进一步提供保护。

有关详细信息，请参阅 HTTP 拒绝服务保护。

内容过滤

在 7 层级别保护 Web 站点免受恶意攻击。设备根据基于 HTTP 标头的用户配置规则检查每个传入的请求，并执行用户配置的操作。这些操作可以包括重置连接、删除请求或向用户的浏览器发送错误消息。这使设备可以屏蔽有害的请求，降低服务器遭受攻击的风险。

此功能还可以分析 HTTP GET 和 POST 请求并过滤出已知的错误签名，使其可以保护服务器免遭基于 HTTP 的攻击。

有关详细信息，请参阅内容过滤。

响应方

可以使用高级过滤器等功能生成从设备到客户端的响应。此功能的一些常见用途包括生成重定向响应、用户定义的响应和重置。

有关详细信息，请参阅响应程序。

重写

修改 HTTP 标头和正文文本。可以使用重写功能将 HTTP 标头添加到 HTTP 请求或响应，对单个 HTTP 标头进行修改，或删除 HTTP 标头。此功能还允许您修改请求和响应中的 HTTP 正文。

收到请求或发送响应时，设备将检查重写规则，如果存在适用规则，它会先将这些规则应用于请求或响应，然后再将其继续传递至 Web 服务器或客户端计算机。

有关详细信息，请参阅重写。

优先队列

设置用户请求的优先级，以确保在请求量猛增时首先为最重要的流量服务。可以根据请求 URL、Cookie 或各种其他因素确定优先级。设备根据为请求配置的优先级将请求置于一个三层队列中，使业务关键型事务即使在浪涌或站点攻击期间也可以平稳地进行。

有关详细信息，请参阅优先级队列。

浪涌保护

调节向服务器传输的用户请求流，并控制可以同时访问服务器资源的用户数，从而在服务器达到其最大容量时，使任何后续请求排队等候。通过控制建立连接的速率，设备可以阻止大量请求突然涌入您的服务器，从而防止站点过载。

有关详细信息，请参阅浪涌保护。

Citrix Gateway

```
Citrix Gateway is a secure application access solution that provides
    administrators granular application-level policy and action controls
     to secure access to applications and data while allowing users to
    work from anywhere. It gives IT administrators a single point of
    control and tools to help ensure compliance with regulations and the
     highest levels of information security across and outside the
    enterprise. At the same time, it empowers users with a single point
    of access — optimized for roles, devices, and networks — to the
    enterprise applications and data they need. This unique combination
    of capabilities helps maximize the productivity of today's mobile
    workforce.
```


有关详细信息，请参阅 Citrix Gateway。

应用程序防火墙

通过过滤每个受保护的 Web 服务器与连接至该 Web 服务器上任何 Web 站点的用户之间的流量，保护应用程序免遭黑客和恶意软件滥用，例如跨站点脚本攻击、缓冲区溢出攻击、SQL 注入攻击及强制浏览等。应用程序防火墙可检查所有流量，寻找攻击 Web 服务器安全性或滥用 Web 服务器资源的证据，并采取适当的措施来防止这些攻击得逞。

有关详细信息，请参阅应用程序防火墙。

应用程序可见性功能

December 15, 2021

- NetScaler Insight Center

  NetScaler Insight Center 是一款高性能收集器，提供了跨 Web 和 HDX (ICA) 流量的端到端用户体验。它可以收集 NetScaler ADC 设备生成的 HTTP 和 ICA AppFlow 记录，并填充涵盖 3 层到 7 层统计信息的分析报告。NetScaler Insight Center 对过去五分钟内的实时数据，以及过去一小时、一天、一周乃至一个月内收集的历史数据进行深入分析。
  HDX (ICA) 分析控制板使您能够从 HDX 用户、应用程序、桌面，甚至网关级别信息进行逐级浏览。同样，HTTP 分析使您能够一览 Web 应用程序、访问的 URL、客户端 IP 地址和服务器 IP 地址，以及其他控制板。管理员可从任何控制板逐级浏览并标识难点，具体取决于用例。

- 使用 AppFlow 增强了应用程序可见性

  Citrix ADC 设备是对数据中心中所有应用程序流量进行控制的中心点。它可收集对应用程序性能监视、分析和业务智能应用程序有价值的流和用户会话级别信息。AppFlow 使用 Internet 协议流信息导出 (IPFIX) 格式（这是在 RFC 5101 中定义的开放 Internet 工程任务组 (IETF) 标准）传输此信息。IPFIX（Cisco 的 NetFlow 的标准化版本）广泛用于监视网络流信息。AppFlow 定义新的信息元素来表示应用程序级别的信息。

  通过使用 UDP 作为传输协议，AppFlow 可将收集的数据（称为流记录）传输到一个或多个 IPv4 收集器。收集器可聚合流记录，并生成实时或历史报告。

  AppFlow 在事务级别为 HTTP、SSL、TCP 和 SSL_TCP 通信流提供可见性。可对要监视的通信流类型进行采样和过滤。

  要限制监视的通信流类型，可通过对应用程序流量进行采样和过滤来为虚拟服务器启用 AppFlow。AppFlow 还可为虚拟服务器提供统计信息。

  还可为表示应用程序服务器的特定服务启用 AppFlow，并监视传输到该应用程序服务器的流量。

  有关详细信息，请参阅 AppFlow。

- Stream Analytics

  Web 站点或应用程序的性能取决于常用的内容交付的优化程度。缓存和压缩等技术有助于加快将服务交付到客户端的速度，但您需要确定常用资源，然后缓存或压缩这些资源。可以通过聚合有关 Web 站点或应用程序流量的实时统计数据，来确定常用资源。资源相对于其他资源的访问频率以及这些资源占用的带宽等统计数据可帮助您确定是否需要缓存或压缩这些资源，以提升服务器性能和网络利用率。响应时间及应用程序并行连接数量等统计数据可帮助您确定是否必须增强服务器端的资源。

  如果 Web 站点或应用程序变化不频繁，可使用用于收集统计数据的产品，然后手动分析统计数据并优化内容的交付。但是，如果您不希望进行手动优化，或者 Web 站点或应用程序具有动态性，则需要使用不仅能收集统计数据而且还能够自动根据统计数据优化资源交付的基础结构。在 Citrix ADC 设备上，此功能由 Stream Analytics 功能提供。该功能在单个 Citrix ADC 设备上运行并根据定义的标准收集运行时统计数据。与 Citrix ADC 策略配合使用时，该功能还提供进行自动实时通信优化所需的基础结构。

  有关详细信息，请参阅操作分析。