NetScaler Gateway 13.1

Machine translated content

Disclaimer

Contents

NetScaler Gateway 发行说明

February 1, 2024

发行说明描述了软件在特定版本中的变化情况，以及该版本中存在的已知问题。

发行说明文档包括以下全部或部分内容：

- 新增功能：内部版本中发布的增强功能和其他更改。
- 已修复的问题：内部版本中已修复的问题。
- 已知问题：内部版本中存在的问题。
- 注意事项：使用构建时要记住的重要方面。
- 限制：内部版本中存在的限制。

> 重要： NetScaler Gateway 发行说明作为 ADC 发行说明的一部分。
> 有关 NetScaler Gateway 13.1 增强功能、已知问题和错误修复的详细信息，请参阅 发行说明 页面。

注意：

- 问题描述下的 [# XXXXXX] 标签是 NetScaler 团队使用的内部跟踪 ID。
- 这些发行说明未记录安全相关的修复。有关安全相关修复和建议的列表，请参阅安全公告。

关于 NetScaler Gateway

February 1, 2024

NetScaler Gateway 易于部署且易于管理。最典型的部署配置是在 DMZ 中找到 NetScaler Gateway 设备。可以在网络中安装多个 NetScaler Gateway 设备以进行更复杂的部署。

首次启动 NetScaler Gateway 时，可以使用串行控制台、配置实用程序中的设置向导或动态主机配置协议 (DHCP) 来执行初始配置。在 MPX 设备上，您可以使用设备前面板上的 LCD 键盘执行初始配置。您可以配置特定于内部网络的基本设置，例如 IP 地址、子网掩码、默认网关 IP 地址和域名系统 (DNS) 地址。配置基本网络设置后，可以配置特定于 NetScaler Gateway 操作的设置，例如身份验证、授权、网络资源、虚拟服务器、会话策略和终端节点策略的选项。

在安装和配置 NetScaler Gateway 之前，请查看本节中的主题以获取有关规划部署的信息。部署规划可以包括确定设备的安装位置、了解如何在 DMZ 中安装多台设备以及许可要求。您可以在任何网络基础架构中安装 NetScaler Gateway，而无需更改安全网络中运行的现有硬件或软件。NetScaler Gateway 支持其他网络产品，例如服务器负载平衡器、缓存引擎、防火墙、路由器和 IEEE 802.11 无线设备。

在配置 NetScaler Gateway 之前，您可以在安装前清单中编写设置以备使用。

NetScaler Gateway 设备	提供有关 NetScaler Gateway 设备和设备安装说明的信息。
预安装核对表	提供在网络中安装 NetScaler Gateway 之前要查看的规划信息和要完成的任务列表。
常见部署	提供有关在网络 DMZ 中、在没有 DMZ 的安全网络中以及与其他设备一起部署 NetScaler Gateway 以支持负载平衡和故障切换的信息。还提供有关使用 Citrix Virtual Apps and Desktops 部署 NetScaler Gateway 的信息。
许可	提供有关在设备上安装许可证的信息。还提供有关在多台 NetScaler Gateway 设备上安装许可证的信息。

NetScaler Gateway 体系结构

NetScaler Gateway 的核心组件包括：

- 虚拟服务器。NetScaler Gateway 虚拟服务器是一个内部实体，代表用户可用的所有已配置服务。虚拟服务器也是用户访问这些服务的接入点。可以在单个设备上配置多个虚拟服务器，从而允许一个 NetScaler Gateway 设备为具有不同身份验证和资源访问要求的多个用户社区提供服务。
- 身份验证、授权和审核。可以配置身份验证、授权和记帐，以允许用户使用 NetScaler Gateway 或位于安全网络中的身份验证服务器（例如 LDAP 或 RADIUS）识别的凭据登录 NetScaler Gateway。授权策略定义用户权限，确定给定用户有权访问哪些资源。有关身份验证和授权的详细信息，请参阅配置身份验证和授权。审核服务器维护有关 NetScaler Gateway 活动的数据，包括用户登录事件、资源访问实例和操作错误。此信息存储在 NetScaler Gateway 或外部服务器上。有关审核的更多信息，请参阅在 NetScaler Gateway 上配置审核
- 用户连接。用户可以使用以下访问方法登录 NetScaler Gateway：
  - 适用于 Windows 的 Citrix Secure Access 客户端是安装在基于 Windows 的计算机上的软件。用户可以通过右键单击基于 Windows 的计算机上的通知区域中的图标来登录。如果用户使用的计算机上未安装 Citrix Secure Access 客户端，则可以使用 Web 浏览器登录下载和安装插件。如果用户安装了 Citrix Workspace 应用程序，则用户可以通过 Citrix Workspace 应用程序使用 Citrix Secure Access 客户端登录。在用户设备上安装 Citrix Workspace 应用程序和 Citrix Secure Access 代理时，Citrix Workspace 应用程序会自动添加 Citrix Secure Access 客户端。
  - 适用于 macOS X 的 Citrix Secure Access 客户端，允许运行 macOS X 的用户登录。它具有与适用于 Windows 的 Citrix Secure Access 客户端相同的特性和功能。您可以通过安装 NetScaler Gateway 10.1 版本，内部版本 120.1316.e 来为此插件版本提供端点分析支持。
  - Citrix Workspace 应用程序，允许用户使用 Web Interface 或 Citrix StoreFront 连接到服务器场中已发布的应用程序和虚拟桌面。

  - Citrix Workspace 应用程序、Secure Hub、WorxMail 和 WorxWeb，允许用户访问 Citrix Endpoint Management 中托管的 Web 和 SaaS 应用程序、iOS 和 Android 移动应用程序以及 ShareFile 数据。
  - 用户可以从使用 NetScaler Gateway Web 地址的 Android 设备进行连接。当用户启动应用程序时，连接使用 Micro VPN 将网络流量路由到内部网络。如果用户从 Android 设备进行连接，则必须在 NetScaler Gateway 上配置 DNS 设置。有关更多信息，请参阅使用适 用于 Android 设备的 DNS 后缀支持 DNS 查询。
  - 用户可以从使用 NetScaler Gateway Web 地址的 iOS 设备进行连接。您可以在全局或会话配置文件中配置 Secure Browse。当用户在其 iOS 设备上启动应用程序时，VPN 连接将启动，连接将通过 NetScaler Gateway 进行路由。
  - 无客户端访问，为用户提供所需的访问权限，而无需在用户设备上安装软件。

    配置 NetScaler Gateway 时，您可以创建策略来配置用户的登录方式。您还可以通过创建会话和端点分析策略来限制用户登录。

- 网络资源。这些服务包括用户通过 NetScaler Gateway 访问的所有网络服务，例如文件服务器、应用程序和网站。
- 虚拟适配器。NetScaler Gateway 虚拟适配器支持需要 IP 欺骗的应用程序。安装 Citrix Secure Access 客户端后，虚拟适配器将安装在用户设备上。当用户连接到内部网络时，NetScaler Gateway 和内部服务器之间的出站连接将使用内部网 IP 地址作为源 IP 地址。作为配置的一部分，Citrix Secure Access 客户端从服务器接收此 IP 地址。

  如果在 NetScaler Gateway 上启用拆分通道，则所有 Intranet 流量都将通过虚拟适配器路由。拦截绑定到 Intranet 的流量时，虚拟适配器将拦截 A 和 AAAA 记录类型的 DNS 查询，同时保持所有其他 DNS 查询不变。未绑定到内部网络的网络流量通过安装在用户设备上的网络适配器进行路由。互联网和专用局域网 (LAN) 连接保持打开和连接状态。如果禁用拆分通道，则所有连接都将通过虚拟适配器进行路由。任何现有连接都会断开连接，用户必须重新建立会话。

  如果配置 Intranet IP 地址，则通过虚拟适配器使用 Intranet IP 地址欺骗到内部网络的流量。

用户连接的工作方式

用户可以从远程位置连接到他们的电子邮件、文件共享和其他网络资源。用户可以使用以下软件连接到内部网络资源：

- Citrix Secure Access 客户端
- Citrix Workspace 应用程序
- WorxMail 和 WorxWeb
- Android 和 iOS 移动设备

连接 **Citrix Secure Access** 客户端

Citrix Secure Access 客户端允许用户通过以下步骤访问内部网络中的资源：

1. 用户通过在 Web 浏览器中键入 Web 地址来首次连接到 NetScaler Gateway。此时将显示登录页面，并提示用户输入用户名和密码。如果配置了外部身份验证服务器，NetScaler Gateway 将与服务器联系，身份验证服务器将验证用户的凭据。如果配置了本地身份验证，NetScaler Gateway 将执行用户身份验证。
2. 如果配置预身份验证策略，则当用户在基于 Windows 的计算机或 macOS X 计算机上的 Web 浏览器中键入 NetScaler Gateway Web 地址时，NetScaler Gateway 会在登录页面出现之前检查是否存在任何基于客户端的安全策略。安全检查会验证用户设备是否满足与安全相关的条件，例如操作系统更新、防病毒防护和正确配置的防火墙。如果用户设备未通过安全检查，NetScaler Gateway 将阻止用户登录。无法登录的用户必须下载必要的更新或软件包，然后将其安装在用户设备上。当用户设备通过预身份验证策略时，将显示登录页面，用户可以输入登录凭据。如果安装 NetScaler Gateway 10.1 版本 120.1316.e，则可以在 macOS X 计算机上使用高级端点分析。
3. NetScaler Gateway 成功对用户进行身份验证后，NetScaler Gateway 将启动 VPN 通道。NetScaler Gateway 提示用户下载并安装适用于 Windows 的 Citrix Secure Access 客户端或适用于 macOS X 的 Citrix Secure Access 客户端。
4. 如果配置身份验证后扫描，则在用户成功登录后，NetScaler Gateway 将扫描用户设备以查找所需的客户端安全策略。您可以要求与预身份验证策略相同的安全相关条件。如果用户设备扫描失败，则表示未应用策略或将用户置于隔离组中，并且用户对网络资源的访问受到限制。
5. 建立会话后，用户将被定向到 NetScaler Gateway 主页，用户可以在其中选择要访问的资源。NetScaler Gateway 随附的主页称为访问界面。如果用户使用适用于 Windows 的 Citrix Secure Access 客户端登录，则 Windows 桌面通知区域中的图标显示用户设备已连接，并且用户会收到一条消息，说明连接已建立。用户还可以在不使用访问界面的情况下访问网络中的资源，例如打开 Microsoft Outlook 和检索电子邮件。
6. 如果用户请求同时通过了身份验证前和身份验证后安全检查，NetScaler Gateway 将联系请求的资源，并在用户设备与该资源之间启动安全连接。
7. 用户可以通过右键单击基于 Windows 的计算机上通知区域中的 NetScaler Gateway 图标，然后单击注销来关闭活动会话。会话也可能由于不活动而超时。会话关闭后，通道将关闭，用户将无法再访问内部资源。用户还可以在浏览器中键入 NetScaler Gateway Web 地址。当用户按 Enter 键时，将显示用户可以从中注销的访问界面。

注意：如果在内部网络中部署 Citrix Endpoint Management，则从内部网络外部连接的用户必须首先连接到 NetScaler Gateway。当用户建立连接时，用户可以访问 Citrix Endpoint Management 上托管的 Web 和 SaaS 应用程序、Android 和 iOS 移动应用程序以及 ShareFile 数据。用户可以通过无客户端访问来连接 Citrix Secure Access 客户端，也可以使用 Citrix Workspace 应用程序或 Secure Hub 进行连接。

与 **Citrix Workspace** 应用程序连接

用户可以连接 Citrix Workspace 应用程序以访问其基于 Windows 的应用程序和虚拟桌面。用户还可以从 Endpoint Management 访问应用程序。要从远程位置进行连接，用户还可以在其设备上安装 Citrix Secure Access 客户端。Citrix Workspace 应用程序自动将 Citrix Secure Access 客户端添加到其插件列表中。当用户登录 Citrix Workspace 应用程序时，他们还可以登录 Citrix Secure Access 客户端。您还可以将 NetScaler Gateway 配置为在用户登录 Citrix Workspace 应用程序时执行单点登录 Citrix Secure Access 客户端。

连接 **iOS** 和 **Android** 设备

用户可以使用 Secure Hub 从 iOS 或 Android 设备进行连接。用户可以使用 Secure Mail 访问他们的电子邮件，并使用 WorxWeb 连接到网站。

当用户从移动设备进行连接时，连接会通过 NetScaler Gateway 进行路由以访问内部资源。如果用户连接到 iOS，则可以启用 Secure Browse 作为会话配置文件的一部分。如果用户使用 Android 系统连接，则连接会自动使用 Micro VPN。此外，
Secure Mail 和 WorxWeb 使用 Micro VPN 通过 NetScaler Gateway 建立连接。您不必在 NetScaler Gateway 上配置 Micro VPN。

常见 **NetScaler Gateway** 部署

February 1, 2024

您可以在组织内部网络（或 Intranet）的外围部署 NetScaler Gateway，以提供对驻留在内部网络中的服务器、应用程序和其他网络资源的安全单点访问。所有远程用户必须先连接到 NetScaler Gateway，然后才能访问内部网络中的任何资源。

NetScaler Gateway 最常安装在网络中的以下位置：

- 在网络中 DMZ
- 在没有 DMZ 的安全网络中

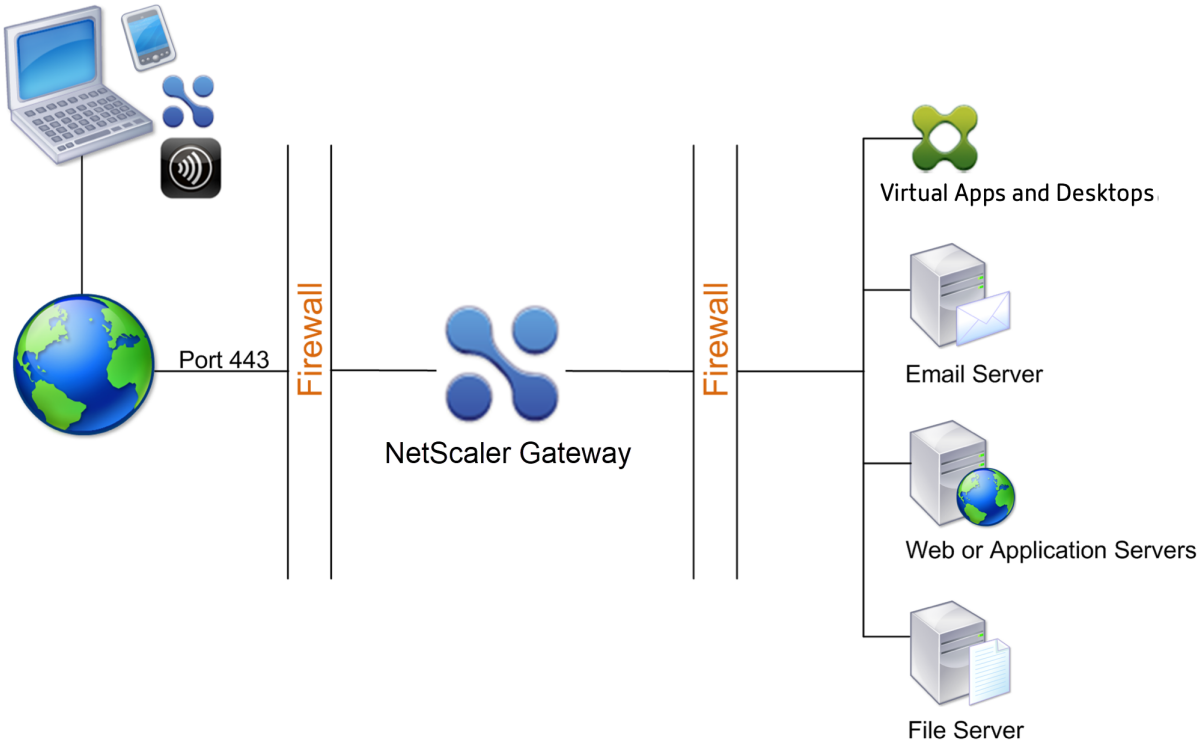
您还可以使用 Citrix Virtual Apps、Citrix Virtual Desktops、StoreFront 和 Citrix Endpoint Management 部署 NetScaler Gateway，以允许用户访问其 Windows、Web、移动和 SaaS 应用程序。如果您的部署包括 Citrix Virtual Apps、StoreFront 和桌面 7，则可以在单跃点或双跃点 DMZ 配置中部署 NetScaler Gateway。早期版本的 Citrix Virtual Desktops 或 Citrix Endpoint Management 不支持双跃点部署。

有关使用这些和其他支持的 NetScaler 解决方案扩展您的 NetScaler Gateway 安装的更多信息，请参阅 与 NetScaler 产品集成主题 。

在 **DMZ** 中部署 **NetScaler Gateway**

许多组织都使用 DMZ 来保护其内部网络。DMZ 是位于组织的安全内部网络和 Internet（或任何外部网络）之间的子网。在 DMZ 中部署 NetScaler Gateway 时，用户可以通过适用于 Windows 的 Citrix Secure Access 或 Citrix Workspace 应用程序进行连接。

图 1. 在 DMZ 中部署的 NetScaler Gateway



在上图所示的配置中，您可以在 DMZ 中安装 NetScaler Gateway，然后将其配置为连接到 Internet 和内部网络。

DMZ 中的 NetScaler Gateway 连接

在 DMZ 中部署 NetScaler Gateway 时，用户连接必须遍历第一个防火墙才能连接到 NetScaler Gateway。默认情况下，用户连接使用端口 443 上的 SSL 来建立此连接。要允许用户连接到达内部网络，必须允许通过第一个防火墙在端口 443 上使用 SSL。

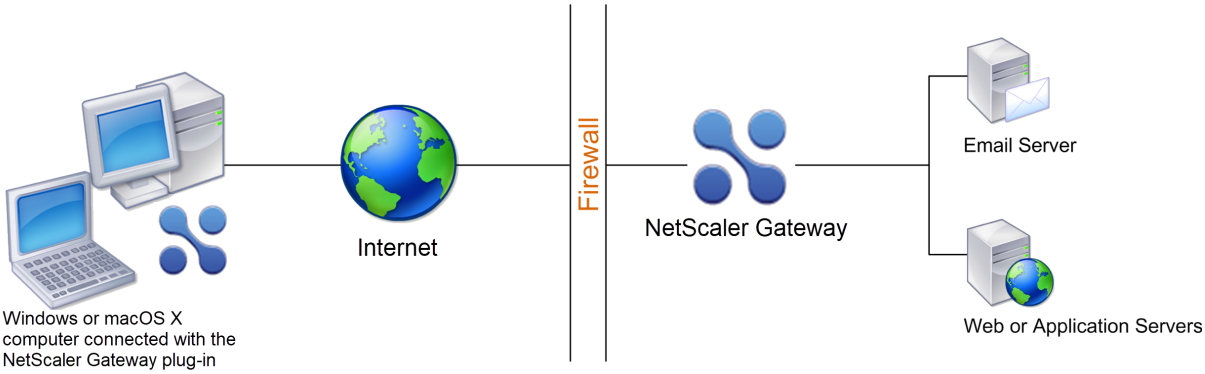
NetScaler Gateway 会解密来自用户设备的 SSL 连接，并代表用户建立与第二个防火墙后面的网络资源的连接。必须通过第二个防火墙打开的端口取决于您授权外部用户访问的网络资源。

例如，如果您授权外部用户访问内部网络中的 Web 服务器，并且此服务器侦听端口 80 上的 HTTP 连接，则必须允许通过第二个防火墙在端口 80 上使用 HTTP。NetScaler Gateway 代表外部用户设备建立通过第二个防火墙到内部网络上的 HTTP 服务器的连接。

在安全的网络中部署 NetScaler Gateway

您可以在安全网络中安装 NetScaler Gateway。在这种情况下，一个防火墙站在 Internet 和安全网络之间。NetScaler Gateway 驻留在防火墙内以控制对网络资源的访问。

图 1. NetScaler Gateway 部署在安全网络中



在安全网络中部署 NetScaler Gateway 时，请将 NetScaler Gateway 上的一个接口连接到 Internet，将另一个接口连接到安全网络中运行的服务器。将 NetScaler Gateway 置于安全网络中可为本地和远程用户提供访问权限。由于此配置只有一个防火墙，因此对于从远程位置进行连接的用户而言，部署的安全性降低了。尽管 NetScaler Gateway 会拦截来自 Internet 的流量，但在对用户进行身份验证之前，流量会进入安全网络。在 DMZ 中部署 NetScaler Gateway 时，用户会在网络流量到达安全网络之前进行身份验证。

在安全网络中部署 NetScaler Gateway 时，适用于 Windows 的 Citrix Secure Access 连接必须穿过防火墙才能连接到 NetScaler Gateway。默认情况下，用户连接使用端口 443 上的 SSL 协议来建立此连接。要支持此连接，必须在防火墙上打开端口 443。

客户端软件要求

February 1, 2024

NetScaler Gateway 支持使用 Citrix Secure Access 客户端进行用户连接。当用户使用插件登录时，它会建立一个完整的 VPN 通道。使用 Citrix Secure Access 客户端，用户可以连接到您允许访问的网络资源。

如果在 NetScaler Gateway 上配置了端点策略，则当用户登录时，NetScaler Gateway 会自动在用户设备上下载并安装 Citrix EPA 客户端。

Citrix Secure Access 客户端系统要求

Citrix Secure Access 客户端建立了从客户端计算机到 NetScaler Gateway 设备的安全连接。

该插件作为桌面应用程序分发，适用于 Microsoft Windows、macOS X 和 Linux 操作系统。使用 Web 浏览器对 NetScaler Gateway 设备的安全 URL 进行身份验证后，插件将自动下载并安装在计算机上。

该插件作为适用于 Android 和 iOS 设备的移动应用程序进行配置。

> 注意：
>
> - 要安装插件，操作系统需要管理员/root 权限。

> - 支持 Citrix Secure Access 客户端的浏览器也支持无客户端 VPN。

以下操作系统和 Web 浏览器支持 Citrix Secure Access 客户端作为桌面应用程序。

操作系统	支持的浏览器
macOS X（10.9 及更高版本）	Safari 7.1 或更高版本；Google Chrome 版本 30 或更高版本；Mozilla Firefox 版本 30 或更高版本
Windows 11	Google Chrome 30 或更高版本；Mozilla Firefox 发行版 24 或更高版本；Edge Chromium
Windows 10（x86 和 x64）	Google Chrome 30 或更高版本；Mozilla Firefox 发行版 24 或更高版本；Edge Chromium
Linux；Ubuntu 18.04 LTS，20.04 LTS，22.04 LTS。	Mozilla Firefox 版本 44 及更高版本；Google Chrome 50 及更高版本

> 注意：
>
> 目前，适用于 Ubuntu 的 Citrix Secure Access 客户端和 Citrix EPA 客户端仅支持默认 GNOME 显示管理器。

如果缺少所需的依赖项包，则命令会列出它们，插件安装将失败。这些依赖项包必须手动安装。管理员可以通过使用命令行界面键入以下命令来安装丢失的软件包。

```
apt-get install <dependency package>
<!--NeedCopy-->
```

以下操作系统支持 Citrix Secure Access 客户端作为移动应用程序。

VPN 应用	支持的操作系统
Android	Android 7.0 及更高版本
iOS	iOS 12.0 及更高版本

> 注意：
>
> 如果您使用的是最新的 Apple 操作系统版本，例如 macOS 14/iOS 17 及更高版本，那么我们建议您升级到 Citrix Secure Access 客户端/Citrix SSO 版本 23.09.1 或更高版本。

端点分析要求

NetScaler Gateway 在用户设备上安装 Citrix EPA 客户端。Citrix EPA 客户端会扫描用户设备以了解您在 NetScaler Gateway 上配置的端点安全要求。这些要求包括操作系统、防病毒软件或 Web 浏览器版本等信息。

当用户首次使用浏览器连接到 NetScaler Gateway 时，门户网站会请求安装 Citrix EPA 客户端。在随后尝试登录时，Citrix EPA 客户端会验证升级控制配置，以确认是否需要升级 Citrix EPA 客户端。如有必要，用户会收到下载和安装最新的 Citrix EPA 客户端的提示。适用于 Windows 的 Citrix EPA 客户端作为 Windows 32 位应用程序安装。适用于 macOS 的 Citrix EPA 客户端作为 64 位应用程序安装。安装或使用 Citrix EPA 客户端不需要特殊权限，除非使用 EPA 访问设备证书。有关如何使用 EPA 进行设备证书身份验证的详细信息，请参阅使用设备证书进行身份验证。

管理员 UI 控制台上的工具提示详细说明了扫描。有关 EPA 库的详细信息，请参阅 https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/。

> 重要提示：
>
> - 支持 EPA 的浏览器也支持无客户端 VPN。
> - 在预身份验证端点分析中，如果用户未安装端点分析插件或跳过扫描，则用户无法使用 Citrix Secure Access 客户端登录。
> - 在身份验证后端点分析中，用户可以使用无客户端访问或使用 Citrix Workspace 应用程序来访问不需要扫描的资源。
> - 对于与 OPSWAT 相关的扫描，必须在客户端计算机上安装二进制软件包 `epaPackage.exe`。

要使用端点分析插件，用户设备上需要以下软件：

操作系统	支持的浏览器
macOS（10.9 及更高版本）	Safari 7.1 或更高版本；Google Chrome 版本 30 或更高版本；Mozilla Firefox 版本 30 或更高版本
Windows 11	Google Chrome 30 或更高版本；Mozilla Firefox 发行版 24 或更高版本；Edge Chromium
Windows 10	Google Chrome 30 或更高版本；Mozilla Firefox 发行版 24 或更高版本；Edge Chromium
Linux；Ubuntu 18.04 LTS，20.04 LTS，22.04 LTS。	Mozilla Firefox 版本 44 及更高版本；Google Chrome 50 及更高版本

注意：

- 支持前面提到的所有版本的操作系统变体。
- 不支持 S 模式下的 Windows 10 和 Windows 11。
- 对于 Windows 版本，必须安装所有服务包和关键更新。
- 对于 Mozilla Firefox 版本，Endpoint Analysis 必须启用插件。所需的最低版本为 3.0。

NetScaler Gateway 与 NetScaler 产品的兼容性

February 1, 2024

下表提供了 NetScaler Gateway 13.1 兼容的 NetScaler 产品和版本。

> 注意：
>
> NetScaler Gateway 功能可在 NetScaler VPX 上使用。

NetScaler 产品和支持的版本

NetScaler 产品	发布版本
Citrix SD-WAN	10.2, 11.0
NetScaler 平台	当前所有 MPX 和 VPX 型号，包括符合 FIPS 标准的设备。
StoreFront	当前支持的所有 StoreFront 版本。
Citrix Virtual Apps and Desktops	7.15、1808、1811、1903、1906、1909、2003、2009、2112、1912 LTSR、2203 LTSR
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

Citrix Workspace 应用程序、Citrix 移动生产力应用程序和插件

* 下表列出了每个软件版本的第一个支持的版本。除非另有说明，否则支持所有后续版本。有关发布生命周期的更多信息，请参阅产品列表。

Citrix Workspace 应用程序或插件	支持的最低版本 *
适用于 macOS X 的 Citrix Secure Access 客户端	3.1.8
适用于 Windows 的 Citrix Secure Access 客户端	12.0
适用于 iOS 的 Citrix Secure Access 客户端	3.1.4
适用于 Android 的 Citrix Secure Access 客户端	2.0.14
适用于 Android 的 Citrix Workspace 应用程序	3.11
适用于 iOS 的 Citrix Workspace 应用程序	7.1.3
适用于 Mac 的 Citrix Workspace 应用程序	12.4
适用于 Windows 的 Citrix Workspace 应用程序	4.4

Citrix Workspace 应用程序或插件	支持的最低版本 *
适用于 Linux 的 Citrix Workspace 应用程序	13.4
适用于 HTML5 的 Citrix Workspace 应用程序	2.3
适用于 Chrome 的 Citrix Workspace 应用程序	2.3
Secure Hub for iOS	10.5
Secure Hub for Android	10.5
Secure Mail for iOS	10.5
适用于 iOS 的 SecureWeb	10.5
Secure Mail for Android	10.5
Android 版 SecureWeb	10.5

> 注意：
>
> - 有关每个 VPN 客户端支持的一些常用功能的详细信息，请参阅 NetScaler Gateway VPN 客户端和支持的功能。

NetScaler Gateway 许可

February 1, 2024

安装 NetScaler Gateway 后，您可以从 Citrix 获取平台或通用许可证文件。登录 Citrix 网站以访问可用许可证并生成许可证文件。生成许可证文件后，您可以将其下载到计算机上。当许可证文件在计算机上时，您可以将其上载到 NetScaler Gateway。有关 Citrix 许可的详细信息，请参阅 Citrix 许可系统。

在获取许可证文件之前，请确保使用设置向导配置设备的主机名，然后重新启动设备。

要获取许可证，请转到激活、升级和管理 NetScaler 许可证网页。在此页面上，您可以获取新许可证并激活、升级和管理 NetScaler 许可证。

重要提示：

> - 您必须在 NetScaler Gateway 上安装许可证。该设备未从 NetScaler 许可证服务器获得许可证。
> - Citrix 建议您保留收到的所有许可证文件的本地副本。保存配置文件的备份副本时，上载的所有许可证文件都包含在备份中。如果必须重新安装 NetScaler Gateway 设备软件并且没有配置备份，则需要原始许可证文件。

在 NetScaler Gateway 上安装许可证之前，请设置设备的主机名，然后重新启动 NetScaler Gateway。您可以使用安装向导来配置主机名。为 NetScaler Gateway 生成通用许可证时，许可证中将使用主机名。

NetScaler Gateway 许可证类型

NetScaler Gateway 需要平台许可证。平台许可证允许使用 ICA 代理无限数量地连接 Citrix Virtual Apps、Citrix Virtual Desktops 或 StoreFront。要允许从 Citrix Secure Access 客户端、SmartAccess 登录点或 Secure Hub、WorxWeb 或 Secure Mail 通过 VPN 连接到网络，还必须添加通用许可证。NetScaler Gateway VPX 随附平台许可证。

以下 NetScaler Gateway 版本支持平台许可证：

- NetScaler Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler VPX

> 重要：Citrix 建议您保留收到的所有许可证文件的本地副本。保存配置文件的备份副本时，所有上载的许可证文件都包含在备份中。如果需要重新安装 NetScaler Gateway 设备软件并且没有配置备份，则需要原始许可证文件。

平台许可证

平台许可证允许用户无限制地连接 Citrix Virtual Apps 上的已发布应用程序或 Citrix Virtual Desktops 中的虚拟桌面使用 Citrix Receiver 进行的连接不使用 NetScaler Gateway 通用许可证。这些连接只需要平台许可证。平台许可证随所有新 NetScaler Gateway 订单（无论是物理订单还是虚拟订单）以电子方式交付如果您已拥有保修或维护协议涵盖的设备，则可以从 Citrix 网站获取平台许可证。

通用许可证

NetScaler Gateway 通用许可证将并发用户会话的数量限制为购买的许可证数量。如果您购买了 100 个许可证，则可以随时拥有 100 个并发会话。如果您购买标准版许可证，则可以随时拥有 500 个并发会话。当用户结束会话时，将为下一个用户释放该许可证。从多台计算机登录 NetScaler Gateway 的用户占用每个会话的许可证。

如果所有许可证都被占用，则在用户结束会话或管理员使用配置实用程序终止会话之前，不能打开其他连接。连接关闭时，许可证将被释放，并且可用于新用户。

收到 NetScaler Gateway 设备后，许可按以下顺序进行：

- 您会在电子邮件中收到许可证访问代码（许可证密钥）。
- 您可以使用设置向导使用主机名配置 NetScaler Gateway。
- 您可以从 Citrix 网站分配 NetScaler Gateway 许可证。在分配过程中，使用主机名将许可证绑定到设备。
- 您可以在 NetScaler Gateway 上安装许可证文件。

通用许可证支持以下功能：

- 完整 VPN 通道
- Micro VPN
- 端点分析
- 基于策略的 SmartAccess
- 无客户端访问网站和文件共享

获取通用许可证　在访问 Citrix Web 站点以获取通用许可证之前，您需要提供以下信息。

- 您的 Citrix 帐户用户 ID 和密码。

  在 Citrix 网站上注册 (https://www.citrix.com/welcome/create-account/) 以接收您的用户 ID 和密码。
  注意：如果找不到许可证代码或用户 ID 和密码，请与 Citrix 客户服务部门联系。

- NetScaler Gateway
  的主机名

  Citrix 网站上此名称的输入字段区分大小写，因此请确保复制主机名与 NetScaler 设备上的配置完全相同。

- 要包含在许可证文件中的许可证数量

  无需一次下载您有权享有的所有许可证。例如，如果贵公司购买了 100 个许可证，则可以选择下载 50 个许可证。
  您可以稍后在另一个许可证文件中分配其余部分。可以在
  NetScaler Gateway 上安装多个许可证文件。

  注意：在获取许可证之前，请确保使用安装向导配置 NetScaler 设备的主机名，然后重新启动设备。

获取通用许可证

1. 使用 Citrix 凭据登录到 Citrix Web 站点 (https://www.citrix.com/en-in/account/)。
2. 在 **Citrix Manage Licenses is here**（此处为 Citrix 管理许可证）下，按照说明获取许可证文件。

安装通用许可证　要安装许可证，请参阅“安装许可证”。安装后，验证是否正确安装了许可证。

验证通用许可证的安装　在继续操作之前，请验证您的通用许可证是否已正确安装。

使用 **CLI** 验证通用许可证的安装

1. 使用 SSH 客户端（例如 PuTTY）打开与 NetScaler 设备的 SSH 连接。
2. 使用管理员凭据登录 NetScaler 设备。
3. 使用 show license 命令验证“SSL VPN = YES”以及最大用户数是否已从 5 个增加到预期的并发用户数。

使用 **GUI** 验证通用许可证的安装

1. 在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 `http://192.168.100.1`。
2. 在 User Name（用户名）和 Password（密码）中，键入管理员凭据。
3. 在导航窗格中，展开 System（系统），然后单击 Licenses（许可证）。
4. 在许可证窗格中，您会在 **Citrix Gateway** 旁边看到一个绿色的复选标记。允许的最大 NetScaler Gateway 用户数字段显示在 NetScaler 设备上许可的并发用户会话数。

相关资源

- Citrix 许可系统
- NetScaler 数据手册
- NetScaler 和 NetScaler Gateway 许可证的类型

在 **NetScaler Gateway** 上安装许可证

February 1, 2024

成功将许可证文件下载到计算机后，可以在 NetScaler Gateway 上安装许可证。该许可证安装在 /nsconfig/license 目录中。

如果使用安装向导在 NetScaler Gateway 上配置初始设置，则在运行向导时会安装许可证文件。如果您分配了部分许可证，然后再分配一个额外的号码，则可以在不使用安装向导的情况下安装许可证。

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“许可证”。
2. 在详细信息窗格中，单击 **Manage Licenses**（管理许可证）。
3. 单击 添加新许可证，然后单击 浏览，导航到许可证文件，然后单击 确定。

   配置实用程序中将显示一条消息，指出您必须重新启动 NetScaler Gateway 单击“重启”。

设置最大用户数

在设备上安装许可证后，您需要设置允许连接到设备的最大用户数。可以在全局身份验证策略中设置最大用户计数。

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改身份验证 **AAA** 设置”。
3. 在“最大用户数”中，键入用户总数，然后单击“确定”。

   此字段中的数量与许可证文件中包含的许可证数量相对应。此数字必须小于或等于设备上安装的许可证总数。例如，您安装了一个包含 100 个用户许可证的许可证和另一个包含 400 个用户许可证的许可证。许可证总数等于

500。可以登录的最大用户数等于或小于 500。如果有 500 个用户登录，则在用户注销或您终止会话之前，任何尝试登录超出该数量的用户都将被拒绝访问。

验证通用许可证安装

在继续之前，请确认您的通用许可证已正确安装。

使用 **GUI** 验证通用许可证的安装

1. 在导航窗格中，在配置实用程序中的“Configuration”（配置）选项卡上，展开 System（系统），然后单击 Licenses（许可证）。

   在 许可证 窗格中，您会在 NetScaler Gateway 旁边 看到一个绿色的复选标记。允许的最大 NetScaler Gateway 用户 数字段显示设备上许可的并发用户会话数。

使用 **CLI** 验证通用许可证的安装

1. 使用 SSH 客户端（如 PuTTY）打开与设备的安全外壳 (SSH) 连接。
2. 使用管理员凭据登录设备。
3. 在命令提示符处键入；

```
1 show license
2 <!--NeedCopy-->
```

如果参数 SSL VPN 等于是，最大用户数参数等于许可证数量，则许可证安装正确。

NetScaler Gateway 许可常见问题解答

February 1, 2024

如何获得试用或演示许可证方面的帮助

现在，许多 NetScaler 产品都以全面、私密的 1:1 专家主导的演示体验形式提供。我们的 Citrix 专家根据您的需求、用例和活动项目自定义演示。无需下载、许可证或安装。您只需进行最少的设置即可观看即时演示。演示结束后，要继续进行适用于您的服务的 Citrix 解决方案的概念验证或试用版，请联系 Citrix 专家。对于演示，请单击 https://demo.citrix.com/。

如何安装许可证

有关安装许可证的详细信息，请参阅在 NetScaler Gateway 上安装许可证。

Gateway 许可证有哪些不同类型

平台许可证允许使用 ICA 代理无限数量地连接 Citrix Virtual Apps、Citrix Virtual Desktops 或 StoreFront。通用许可证是 NetScaler 平台许可证之上的附加许可证。这允许从 Citrix Secure Access 客户端、SmartAccess 登录点或 Secure Hub、Secure Web 或 Secure Mail 通过 VPN 连接到网络。有关详细信息，请参阅 NetScaler Gateway 许可证类型。

支持多少个并发用户会话

支持的会话取决于网关许可证类型。有关详细信息，请参阅 NetScaler Gateway 许可证类型

另一个要考虑的因素是底层硬件本身的容量。有关性能注意事项，请参阅 NetScaler MPX/SDX 数据表或 NetScaler VPX 数据表。

如何查看当前许可的并发用户会话

在配置选项卡上的配置实用程序中，展开 系统，然后单击 许可证。
在 许可证 窗格中，您会在 NetScaler Gateway 旁边 看到一个绿色的复选标记。允许的最大 **NetScaler Gateway** 用户 数字段显示设备上许可的并发用户会话数。

如何检查是否已达到许可的吞吐量限制

您可以使用提取实时吞吐量 `newnslog`。例如，如果许可证吞吐量为 500 Mbps，则可以使用以下命令提取超过 500 的实时吞吐量。

```
1 nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
     more
2 <!--NeedCopy-->
```



```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index    rtime totalcount-val       delta rate/sec symbol-name&device-no&time
    12     7000      801130681        3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13        0      460776045        3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14     7000      801134437        3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15        0      460779784        3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16     7000      801138166        3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17        0      460783497        3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18     7000      801141896        3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19        0      460787213        3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20     7000      801145623        3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21        0      460790929        3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22     7000      801149353        3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23        0      460794646        3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24     7000      801153067        3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25        0      460798342        3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

如何检查数据包是否在达到许可吞吐量时丢弃

您可以使用以下命令检查数据包是否被丢弃。

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index    rtime     totalcount-val       delta rate/sec symbol-name&device-no&time
    0 1966993        23723602         478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
    1       0        48048402         465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
    2       0      8307679782      145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
    3    7000        23723933         331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
    4       0        48048712         310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
    5       0      8307787105      107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
    6    7000        23723941           8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
    7       0        48048735          23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
    8       0      8307811163       24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

如何找出 **NetScaler** 设备的许可吞吐量是多少

从 CLI 运行 `show license` 命令，然后使用型号从 ADC 或网关 MPX、SDX 和 VPX 数据手册获取吞吐量。


```
> sh license
        License status:
                              Web Logging: YES
                        Surge Protection: YES
                          Load Balancing: YES
                       Content Switching: YES
                       Cache Redirection: YES
                             Sure Connect: YES
                     Compression Control: YES
                       Delta Compression: NO
                        Priority Queuing: YES
                          SSL Offloading: YES
           Global Server Load Balancing: YES
                          GSLB Proximity: YES
                    Http DoS Protection: YES
                        Dynamic Routing: YES
                      Content Filtering: YES
                     Integrated Caching: YES
                                SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                    AAA: YES
                             OSPF Routing: YES
                              RIP Routing: YES
                              BGP Routing: YES
                                  Rewrite: YES
                IPv6 protocol translation: YES
                     Application Firewall: YES
                                Responder: YES
                           HTML Injection: YES
                           NetScaler Push: YES
                    Web Interface on NS: YES
                                AppFlow: YES
                              CloudBridge: YES
                        Model Number ID: 5500
 Done
> 
```

CITRIX

Citrix NetScaler | Datasheet

NetScaler platform	MPX 9500	MPX 7500	MPX 5500	VPX 10/200/1000/3000
Platform attributes				
Processor	Intel Xeon L5410 (4 cores total)	Intel Xeon L5410 (4 cores total)	Intel Xeon E5205 (2 cores total)	Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™
Memory	8 GB	8 GB	4 GB	
Ethernet ports	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	4x 10/100/1000 BASE-T	• Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC
Transceivers support	SX, LX	SX, LX		
Software upgradable performance		Upgrade option to MPX 9500		Upgrade options to VPX 200, VPX 1000 and VPX 3000
Platform performance				
System throughput, Gbps	3	1	0.5	Up to 3.0[2]
HTTP requests/sec	200,000	100,000	50,000	Up to 100,000
SSL transactions/sec	20,000	10,000	5,000	Up to 500
SSL throughput, Gbps	3	1	0.5	Up to 1.0
Compression throughput, Gbps	2	1	0.5	Up to 0.75
SSL VPN: concurrent users	10,000	10,000	5,000	Up to 300[3]

如何向现有 **Gateway** 许可证添加更多用户

您可以安装额外的通用许可证。例如，假设您安装了一个包含 100 个用户许可证的通用许可证。如果安装包含 400 个用户许可证的第二个通用许可证，则用户许可证总数等于 500 个。

开始之前的准备工作

February 1, 2024

在安装 NetScaler Gateway 之前，必须评估基础架构并收集信息，以规划满足组织特定需求的访问策略。在定义访问策略时，需要考虑安全影响并完成风险分析。您还需要确定允许用户连接的网络，并决定启用用户连接的策略。

除了规划可供用户使用的资源外，您还需要规划部署方案。NetScaler Gateway 与以下 NetScaler 产品兼容：

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Web Interface
- Citrix SD-WAN

有关部署 NetScaler Gateway 的更多信息，请参阅 常见部署和 与 NetScaler 产品集成

在准备访问策略时，请采取以下初步步骤：

- 识别资源。列出要为其提供访问权限的网络资源，例如 Web、SaaS、移动或已发布的应用程序、虚拟桌面、服务以及您在风险分析中定义的数据。
- 开发访问方案。创建描述用户如何访问网络资源的访问方案。访问方案由用于访问网络的虚拟服务器、端点分析扫描结果、身份验证类型或两者的组合定义。您还可以定义用户登录网络的方式。
- 识别客户端软件。您可以通过 Citrix Secure Access 客户端提供完整的 VPN 访问权限，要求用户使用 Citrix Workspace 应用程序、Secure Hub 或使用无客户端访问登录。您还可以限制对 Outlook Web App 或 WorxMail 的电子邮件访问权限。这些访问方案还决定了用户在获得访问权限时可以执行的操作。例如，您可以指定用户是可以使用已发布的应用程序还是通过连接到文件共享来修改文档。
- 将策略与用户、组或虚拟服务器相关联。当个人或一组用户满足指定条件时，您在 NetScaler Gateway 上创建的策略将强制执行。您可以根据创建的访问方案来确定条件。然后，您可以通过控制用户可以访问的资源以及用户可以对这些资源执行的操作来创建扩展网络安全性的策略。您可以将策略与适当的用户、组、虚拟服务器或全局关联。

本部分包括以下主题，可帮助您规划访问策略：

- 安全规划包括有关身份验证和证书的信息。
- 定义您可能需要的网络硬件和软件的先决条件。
- 在配置 NetScaler Gateway 之前，可用于记下设置的安装前清单。

安装 **NetScaler Gateway** 的先决条件

在 NetScaler Gateway 上配置设置之前，请查看以下先决条件：

- NetScaler Gateway 实际安装在您的网络中，并且可以访问网络。NetScaler Gateway 部署在防火墙后面的 DMZ 或内部网络中。您还可以在双跃点 DMZ 中配置 NetScaler Gateway，并配置与服务器场的连接。Citrix 建议在 DMZ 中部署设备。
- 您可以使用默认网关或指向内部网络的静态路由来配置 NetScaler Gateway，以便用户可以访问网络中的资源。默认情况下，NetScaler Gateway 配置为使用静态路由。
- 用于身份验证和授权的外部服务器已配置并正在运行。有关详细信息，请参阅 身份验证和授权。
- 该网络具有用于名称解析的域名服务器 (DNS) 或 Windows 互联网命名服务 (WINS) 服务器，以提供正确的 NetScaler Gateway 用户功能。
- 您从 Citrix 网站下载了用于用户与 Citrix Secure Access 客户端连接的通用许可证，许可证已准备好安装在 NetScaler Gateway 上。
- NetScaler Gateway 具有由受信任的证书颁发机构 (CA) 签名的证书。有关详细信息，请参阅安装和管理证书。

在安装 NetScaler Gateway 之前，请使用安装前清单记下您的设置。

规划安全

规划 NetScaler Gateway 部署时，必须了解与证书以及身份验证和授权相关的基本安全问题。

配置安全证书管理

默认情况下，NetScaler Gateway 包含一个自签名的安全套接字层 (SSL) 服务器证书，该证书使设备能够完成 SSL 握手。自签名证书足以用于测试或示例部署，但是 NetScaler 不建议将其用于生产环境。在生产环境中部署 NetScaler Gateway 之前，Citrix 建议您请求并接收来自已知证书颁发机构 (CA) 的签名 SSL 服务器证书，然后将其上载到 NetScaler Gateway。

如果在 NetScaler Gateway 必须作为 SSL 握手中的客户端运行的任何环境中部署 NetScaler Gateway（启动与另一台服务器的加密连接），则还必须在 NetScaler Gateway 上安装受信任的根证书。例如，如果您使用 Citrix Virtual Apps 和 Web Interface 部署 NetScaler Gateway，则可以使用 SSL 加密从 NetScaler Gateway 到 Web Interface 的连接。在此配置中，必须在 NetScaler Gateway 上安装受信任的根证书。

验证支持

您可以将 NetScaler Gateway 配置为对用户进行身份验证并控制用户对内部网络上的网络资源的访问权限（或授权）级别。

在部署 NetScaler Gateway 之前，您的网络环境必须具有支持以下身份验证类型之一的目录和身份验证服务器：

- LDAP

- RADIUS
- TACACS+
- 支持审核和智能卡的客户端证书
- 具有 RADIUS 配置的 RSA
- SAML 身份验证

如果您的环境不支持这些身份验证类型中的任何一种，或者您的远程用户人数较少，则可以在 NetScaler Gateway 上创建本地用户列表。然后，您可以配置 NetScaler Gateway 以根据此本地列表对用户进行身份验证。使用此配置，您无需在单独的外部目录中维护用户帐户。

保护 **NetScaler Gateway** 部署的安全

不同的部署可能需要考虑不同的安全注意事项。NetScaler 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。

有关详细信息，请参阅 NetScaler 安全部署准则。

网关预安装清单

February 1, 2024

该清单包含安装 NetScaler Gateway 之前必须完成的任务和规划信息的列表。

提供了空间，以便您可以在完成每项任务并做笔记时检查每个任务。Citrix 建议您记下在安装过程中和配置 NetScaler Gateway 时需要输入的配置值。

有关安装和配置 NetScaler Gateway 的步骤，请参阅安 装 NetScaler Gateway。

用户设备

- 确保用户设备满足 Citrix Secure Access 系统要求中所述的安装必备条件
- 识别用户连接的移动设备。注意：如果用户连接到 iOS 设备，则必须在会话配置文件中启用 Secure Browse。

NetScaler Gateway 基本网络连接

Citrix 建议您在开始配置设备之前获取许可证和签名的服务器证书。

- 识别并记下 NetScaler Gateway 主机名。注意：这不是完全限定的域名 (FQDN)。FQDN 包含在绑定到虚拟服务器的签名服务器证书中。
- 从 Citrix 网站获取通用许可证

- 生成证书签名请求 (CSR) 并发送给证书颁发机构 (CA)。输入将 CSR 发送到证书颁发机构的日期。
- 记下系统 IP 地址和子网掩码。
- 记下子网 IP 地址和子网掩码。
- 写下管理员密码。NetScaler Gateway 随附的默认密码为 `nsroot`。
- 记下 NetScaler Gateway 侦听安全用户连接的端口号。默认端口为 TCP 端口 443。此端口必须在不安全的网络（Internet）和 DMZ 之间的防火墙上打开。
- 记下默认网关 IP 地址。
- 记下 DNS 服务器的 IP 地址和端口号。默认端口号为 53。此外，如果要直接添加 DNS 服务器，则还必须在设备上配置 ICMP (ping)。
- 记下第一个虚拟服务器 IP 地址和主机名。
- 记下第二个虚拟服务器 IP 地址和主机名（如果适用）。
- 记下 WINS 服务器 IP 地址（如果适用）。

可通过 **NetScaler Gateway** 访问的内部网络

- 记下用户可以通过 NetScaler Gateway 访问的内部网络。例如：10.10.0.0/24
- 输入用户使用 Citrix Secure Access 客户端通过 NetScaler Gateway 进行连接时需要访问的所有内部网络和网段。

高可用性

如果您有两台 NetScaler Gateway 设备，则可以在高可用性配置中部署它们，其中一个 NetScaler Gateway 接受并管理连接，而另一台 NetScaler Gateway 则监视第一台设备。如果第一个 NetScaler Gateway 出于任何原因停止接受连接，则第二个 NetScaler Gateway 将接管并开始主动接受连接。

- 记下 NetScaler Gateway 软件版本号。
- 两台 NetScaler Gateway 设备上的版本号必须相同。
- 记下管理员密码 (`nsroot`)。两台设备上的密码必须相同。
- 记下主要的 NetScaler Gateway IP 地址和 ID。最大身份证号码为 64。
- 记下辅助 NetScaler Gateway IP 地址和 ID。
- 获取并在两台设备上安装通用许可证。
- 在两台设备上安装相同的通用许可证。
- 记下 RPC 节点密码。

身份验证和授权

NetScaler Gateway 支持多种不同的身份验证和授权类型，可以用不同的组合。有关身份验证和授权的详细信息，请参阅 身份验证和授权。

LDAP 身份验证

如果您的环境包含 LDAP 服务器，则可以使用 LDAP 进行身份验证。

- 记下 LDAP 服务器的 IP 地址和端口。

  如果允许与 LDAP 服务器进行不安全的连接，则默认端口为 389。如果使用 SSL 加密与 LDAP 服务器的连接，则默认端口为 636。

- 记下安全类型。

  您可以使用或不使用加密来配置安全性。

- 记下管理员绑定 DN。

  如果 LDAP 服务器需要身份验证，请输入 NetScaler Gateway 在查询 LDAP 目录时必须使用的管理员 DN 进行身份验证。一个例子是 cn=administrator,cn=Users,dc=ace, dc=com。

- 写下管理员密码。

  密码与管理员绑定 DN 关联。

- 记下基本 DN。

  用户所在的 DN（或目录级别）；例如，ou=users,dc=ace,dc=com。

- 记下服务器登录名属性。

  输入指定用户登录名的 LDAP 目录人员对象属性。默认值为 sAMAccountName。如果您没有使用 Active Directory，则此设置的常用值为 cn 或 uid。
  有关 LDAP 目录设置的详细信息，请参阅 配置 LDAP 身份验证

- 写下组属性。
  输入 LDAP 目录人员对象属性，该属性指定用户所属的组。默认值为 memberOf。此属性使 NetScaler Gateway 能够识别用户所属的目录组。

- 写下子属性名称。

RADIUS 验证和授权

如果您的环境包含 RADIUS 服务器，则可以使用 RADIUS 进行身份验证。
RADIUS 身份验证包括 RSA SecurID、SafeWord 和金雅拓 Protiva 产品。

- 记下主 RADIUS 服务器 IP 地址和端口。默认端口是 1812。
- 记下主 RADIUS 服务器密钥（共享机密）。
- 记下辅助 RADIUS 服务器 IP 地址和端口。默认端口是 1812。
- 记下辅助 RADIUS 服务器密钥（共享机密）。
- 记下密码编码的类型（PAP、CHAP、MS-CHAP v1、MSCHAP v2）。

SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供商 (IdP) 和服务提供商之间交换身份验证和授权。

- 获取并在 NetScaler Gateway 上安装安全的 IdP 证书。
- 写下重定向 URL。
- 写下用户字段。
- 写下签名证书名称。
- 写下 SAML 发行者的名称。
- 记下默认的身份验证组。

通过防火墙打开端口（单跳 **DMZ**）

如果您的组织使用单个 DMZ 保护内部网络，并且在 DMZ 中部署 NetScaler Gateway，请通过防火墙打开以下端口。如果要在双跃点 DMZ 部署中安装两台 NetScaler Gateway 设备，请参阅在 防火墙上打开适当的端口。

在不安全的网络和 **DMZ** 之间的防火墙上

- 在互联网和 NetScaler Gateway 之间的防火墙上打开一个 TCP/SSL 端口（默认为 443）。用户设备通过此端口连接到 NetScaler Gateway。

在安全网络之间的防火墙上

- 在 DMZ 和安全网络之间的防火墙上打开一个或多个适当的端口。NetScaler Gateway 通过这些端口连接到一个或多个身份验证服务器或在安全网络中运行 Citrix Virtual Apps and Desktops 的计算机。
- 记下身份验证端口。

  仅打开适合 NetScaler Gateway 配置的端口。

  - 对于 LDAP 连接，默认值为 TCP 端口 389。
  - 对于 RADIUS 连接，默认值为 UDP 端口 1812。记下 Citrix Virtual Apps and Desktops 端口。
- 如果要将 NetScaler Gateway 与 Citrix Virtual Apps and Desktops 结合使用，请打开 TCP 端口 1494。如果启用会话可靠性，请打开 TCP 端口 2598 而不是 1494。Citrix 建议将这两个端口都保持打开状态。

Citrix Virtual Desktops、**Citrix Virtual Apps**、**Web Interface** 或 **StoreFront**

如果要部署 NetScaler Gateway 以通过 Web Interface 或 StoreFront 提供对 Citrix Virtual Apps and Desktops 的访问权限，请完成以下任务。此部署不需要 Citrix Secure Access 客户端。用户仅使用 Web 浏览器和 Citrix Receiver 通过 NetScaler Gateway 访问已发布的应用程序和桌面。

- 记下运行 Web Interface 或 StoreFront 的服务器的 FQDN 或 IP 地址。
- 记下运行 Secure Ticket Authority (STA) 的服务器的 FQDN 或 IP 地址（仅适用于 Web Interface）。

Citrix Endpoint Management

如果在内部网络中部署 Citrix Endpoint Management，请完成以下任务。如果用户从外部网络（例如 Internet）连接到 Endpoint Management，则用户必须先连接到 NetScaler Gateway，然后才能访问移动、Web 和 SaaS 应用程序。

- 记下 Endpoint Management 的 FQDN 或 IP 地址。
- 识别用户可以访问的 Web、SaaS 和移动 iOS 或 Android 应用程序。

使用 Citrix Virtual Apps 进行双跃点 DMZ 部署

如果要在双跃点 DMZ 配置中部署两台 NetScaler Gateway 设备以支持访问运行 Citrix Virtual Apps 的服务器，请完成以下任务。

第一个 DMZ 中的 NetScaler Gateway

第一个 DMZ 是位于内部网络最外边缘（最靠近 Internet 或不安全的网络）的 DMZ。客户端通过隔离互联网和 DMZ 的防火墙在第一个 DMZ 中连接到 NetScaler Gateway。在第一个 DMZ 中安装 NetScaler Gateway 之前，请先收集此信息。

- 为此 NetScaler Gateway 完成此清单的 NetScaler Gateway 基本网络连接部分中的项目。

  完成这些项目后，接口 0 将此 NetScaler Gateway 连接到互联网，接口 1 将此 NetScaler Gateway 连接到第二个 DMZ 中的 NetScaler Gateway。

- 在主设备上配置第二个 DMZ 装置信息。

  要将 NetScaler Gateway 配置为双跃点 DMZ 中的第一个跃点，必须在第一个 DMZ 的设备上的第二个 DMZ 中指定 NetScaler Gateway 的主机名或 IP 地址。在第一个跃点中指定何时在设备上配置 NetScaler Gateway 代理后，请将其全局绑定到 NetScaler Gateway 或虚拟服务器。

- 记下设备之间的连接协议和端口。

  要将 NetScaler Gateway 配置为双 DMZ 中的第一个跃点，必须指定连接协议和第二个 DMZ 中 NetScaler Gateway 侦听连接的端口。连接协议和端口是带 SSL 的 SOCKS（默认端口 443）。协议和端口必须通过分隔第一个 DMZ 和第二个 DMZ 的防火墙打开。

第二个 **DMZ** 中的 **NetScaler Gateway**

第二个 DMZ 是离内部安全网络最近的 DMZ。部署在第二个 DMZ 中的 NetScaler Gateway 充当 ICA 流量的代理，在外部用户设备和内部网络上的服务器之间穿越第二个 DMZ。

- 为此 NetScaler Gateway 完成此清单的 NetScaler Gateway 基本网络连接部分中的任务。

  完成这些项目后，接口 0 会在第一个 DMZ 中将此 NetScaler Gateway 连接到 NetScaler Gateway。接口 1 将此 NetScaler Gateway 连接到安全网络。

安装和配置 **NetScaler Gateway** 设备

February 1, 2024

收到 NetScaler Gateway 设备后，您可以打开设备的包装并准备站点和机架。根据说明确定设备的安装位置符合环境标准并且服务器机架已安装到位后，即可安装硬件。装载设备后，将其连接到网络、电源以及用于初始配置的控制台终端。打开设备后，您可以执行初始配置，然后分配管理和网络 IP 地址。请务必遵守安装说明中列出的注意事项和警告。

安装 NetScaler VPX 虚拟设备时，必须首先获取虚拟设备映像并将其安装在虚拟机管理程序或其他虚拟机监视器上。

Citrix 建议使用 NetScaler Gateway 预安装清单 主题，以便在尝试配置 NetScaler Gateway 设备之前记下您的设置。该清单包括有关安装 NetScaler Gateway 和设备的信息。

使用向导配置 **NetScaler Gateway** 设备

February 1, 2024

NetScaler Gateway 具有以下六个向导，可用于在设备上配置设置：

- 首次登录 NetScaler Gateway 设备时，将显示首次设置向导。
- 快速配置向导可帮助您为与 Citrix Endpoint Management、StoreFront 和 Web Interface 的连接配置正确的策略、表达式和设置。
- NetScaler Gateway 向导可帮助您配置 NetScaler Gateway 特定的设置。
- 设置向导可帮助您首次配置基本 NetScaler Gateway 设置。
- Citrix Endpoint Management 集成配置可帮助您配置 NetScaler Gateway 和 Citrix Endpoint Management 环境。
- 已发布的应用程序向导可帮助您使用 Citrix Workspace 应用程序配置用户连接的设置

首次安装向导

在 NetScaler Gateway 设备上完成安装和配置初始设置后，首次登录配置实用程序时，如果不满足以下条件，将显示首次设置向导：

- 您没有在设备上安装许可证。
- 您没有配置子网或映射的 IP 地址。
- 如果设备的默认 IP 地址是 192.168.100.1。

使用首次设置向导配置 **NetScaler Gateway**

要首次配置 NetScaler Gateway（物理设备或 VPX 虚拟设备），您需要在与设备相同的网络上配置管理计算机。

分配 NetScaler Gateway IP (NSIP) 地址作为设备的管理 IP 地址和服务器可以连接的子网 IP (SNIP) 地址。您可以分配一个同时适用于 NetScaler Gateway 和 SNIP 地址的子网掩码。还要配置时区。如果分配主机名，则可以通过指定设备名称而不是 NSIP 地址来访问设备。

首次安装向导中有两个部分。在第一部分中，您将配置 NetScaler Gateway 设备的基本系统设置，包括：

NSIP 地址、SNIP 地址和子网掩码
设备主机名
DNS 服务器
时区
管理员密码
在第二部分中，安装许可证。如果指定 DNS 服务器的地址，则可以使用硬件序列号 (HSN) 或许可证密钥来分配许可证，而不是将许可证从本地计算机上载到设备。

注意：Citrix 建议将许可证保存到本地计算机。

配置完这些设置后，NetScaler Gateway 会提示您重新启动设备。当您再次登录设备时，可以使用其他向导和配置实用程序来配置其他设置。

快速配置向导

快速配置向导允许您在 NetScaler Gateway 上配置多个虚拟服务器。您可以添加、编辑和删除虚拟服务器。

快速配置向导允许对以下部署进行无缝配置：

- Web Interface 连接到 Citrix Virtual Apps and Desktops，能够配置安全票证颁发机构 (STA) 的多个实例
- 仅限 Citrix Endpoint Management
- 仅限 StoreFront
- Citrix Endpoint Management 和 StoreFront 在一起

快速配置向导允许您在设备上配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全的端口重定向到安全端口
- LDAP 服务器
- RADIUS 服务器
- Certificates（证书）
- DNS 服务器
- Citrix Endpoint Management 和 Citrix Virtual Apps and Desktops

  注意：要启用 **SSO**，必须在创建 NetScaler Gateway 会话配置文件 > 客户端体验选项卡中为会话操作手动启用单点登录 **Web** 应用程序 选项。

NetScaler Gateway 支持用户直接连接到 Citrix Endpoint Management，这使用户可以访问其 Web、SaaS 和移动应用程序以及对 ShareFile 的访问权限。您还可以为 StoreFront 配置设置，使用户可以访问其基于 Windows 的应用程序和虚拟桌面。

运行快速配置向导时，将基于 Citrix Endpoint Management、StoreFront 和 Web Interface 设置创建以下策略：

- 会话策略，包括 Receiver、Receiver for Web、Citrix Secure Access 客户端和 Program Neighborhood Agent 的策略和配置文件
- 无客户端访问
- LDAP 和 RADIUS 身份验证

使用快速配置向导配置设置

您可以使用快速配置向导在 NetScaler Gateway 中配置设置以启用与 Citrix Endpoint Management、StoreFront 或 Web Interface 的通信。完成配置后，向导会为 NetScaler Gateway、Endpoint Management、StoreFront 或 Web Interface 之间的通信创建正确的策略。这些策略包括身份验证、会话和无客户端访问策略。向导完成后，策略将绑定到虚拟服务器。

完成快速配置向导后，NetScaler Gateway 可以与 Endpoint Management 或 StoreFront 进行通信，用户可以访问其基于 Windows 的应用程序和虚拟桌面以及 Web、SaaS 和移动应用程序。然后，用户可以直接连接到 Endpoint Management。

在向导期间，您可以配置以下设置：

- 虚拟服务器名称、IP 地址和端口
- 从不安全的端口重定向到安全端口
- Certificates（证书）
- LDAP 服务器
- RADIUS 服务器

- 身份验证的客户端证书（仅适用于双重身份验证）
- Endpoint Management、StoreFront 或 Web Interface

快速配置向导支持 LDAP、RADIUS 和客户端证书身份验证。您可以按照以下准则在向导中配置双重身份验证：

- 如果选择 LDAP 作为主要身份验证类型，则可以将 RADIUS 配置为辅助身份验证类型。
- 如果选择 RADIUS 作为主要身份验证类型，则可以将 LDAP 配置为辅助身份验证类型。
- 如果选择客户端证书作为主要身份验证类型，则可以将 LDAP 或 RADIUS 配置为辅助身份验证类型。

不能使用快速配置向导创建多个 LDAP 身份验证策略。例如，您要配置一个在“服务器登录名属性”字段中使用 **sAMAccountName** 的策略，在“服务器登录名属性”字段中配置另一个使用用户主体 名称 (UPN) 的 LDAP 策略。要配置这些单独的策略，请使用 NetScaler Gateway 配置实用程序创建身份验证策略。有关详细信息，请参阅 配置 LDAP 身份验证。

您可以使用以下方法在快速配置向导中为 NetScaler Gateway 配置证书：

- 选择设备上安装的证书。
- 安装证书和私钥。
- 选择一个测试证书。
  注意：如果您使用测试证书，则必须添加证书中的完全限定域名 (FQDN)。

您可以通过以下两种方式之一打开 快速配置向导：

- 当您在 NetScaler Gateway 登录页面上并在部署类型中选择 **NetScaler Gateway** 时，将显示主页选项卡。如果在“部署类型”中选择任何其他选项，则不会显示“主页”选项卡。
- 通过 **NetScaler Gateway** 详细信息窗格中的“创建/监视 **Citrix** Gateway”链接。如果您安装了启用 NetScaler 功能的许可证，则会显示该链接。如果仅为 NetScaler Gateway 许可设备，则不会显示链接。

最初运行向导后，可以再次运行向导以创建更多虚拟服务器和设置。

重要：如果使用快速配置向导配置额外的 NetScaler Gateway 虚拟服务器，则必须使用唯一的 IP 地址。不能使用与现有虚拟服务器相同的 IP 地址。例如，您有一个 IP 地址为 192.168.10.5 且端口号为 80 的虚拟服务器。运行快速配置向导以创建第二个虚拟服务器，其 IP 地址为 192.168.10.5，端口号为 443。当您尝试保存配置时，会发生错误。

使用快速配置向导配置设置

1. 在配置实用程序中，执行以下操作之一：
   a) 如果设备仅获得 NetScaler Gateway 的许可，请单击主 页 选项卡。
   b) 如果设备获得包含 NetScaler 功能的许可，请在配置选项卡的导航窗格中，单击 **NetScaler Gateway** ，然后在详细信息窗格的 入门下，单击 为企业应用商店配置 **NetScaler Gateway**。
2. 在控制板中，单击 创建新 **NetScaler Gateway**。
3. 在 **NetScaler Gateway** 设置中，配置以下内容：
   a) 在 名称中，键入虚拟服务器的名称。

b) 在 **IP** 地址中，键入虚拟服务器的 IP 地址。
c) 在 **Port**（端口）中，键入端口号。默认端口号为 443。
d) 选择将请求从端口 80 重定向到安全端口，以允许用户从端口 80 连接到端口 443。

4. 单击继续。
5. 在证书页面上，执行以下操作之一：

a) 单击 选择证书，然后在证书中选择证书。
b) 单击 安装证书，然后在 选择证书 和 选择密钥中，单击 浏览 导航到证书和私钥。
c) 单击 使用测试证书，然后在证书 FQDN 中输入测试证书中包含的完全限定域名 (FQDN)。

6. 单击继续。
7. 在身份验证设置中，执行以下操作：

a) 在 主身份验证中，选择 LDAP、RADIUS 或证书。
b) 选择身份验证服务器或配置您在上一步中选择的身份验证类型的设置。如果选择 Cert，请选择客户端证书或安装新的客户端证书。
c) 在 辅助身份验证中，选择身份验证类型，然后配置身份验证服务器设置。

8. 单击继续。

完成网络和身份验证设置配置后，可以配置 Citrix Endpoint Management 或 Citrix Virtual Apps and Desktops（StoreFront 或 Web Interface）设置。

配置企业存储设置　NetScaler Gateway 仅支持用户通过 Endpoint Management 访问 Web、SaaS 和移动应用程序以及 ShareFile。如果您还部署了 StoreFront 或 Web Interface，则用户可以访问基于 Windows 的应用程序和虚拟桌面。您可以为以下选项配置设置：

- 仅限 Endpoint Management
- 仅限 StoreFront
- Endpoint Management 和 StoreFront 在一起
- 仅限 Web Interface

在上述过程中单击“继续”时，可以为部署方案配置设置。以下过程从 Citrix 集成设置页面开始。

创建虚拟服务器后，在快速配置向导中编辑虚拟服务器将不允许更改 Citrix Endpoint Management 或 Citrix Virtual Apps and Desktops 设置。

例如，如果在配置 **Citrix Enterprise Store** 设置之前在任何阶段取消虚拟服务器的配置，则向导会自动选择 Web Interface，而无需配置任何设置。发生这种情况时，您可以编辑虚拟服务器详细信息以配置 Web Interface，但无法切换到 Citrix Endpoint Management。要进行切换，必须创建新的虚拟服务器，并且在配置过程中不得随时取消向导。如果不需要 Web Interface 虚拟服务器，可以使用快速配置向导将其删除。

仅为 **StoreFront** 配置设置

1. 单击 **Citrix Virtual Apps and Desktops**。
2. 在 部署类型中，选择 **StoreFront**。
3. 在 **StoreFront FQDN** 中，输入 StoreFront 服务器的完全限定域名 (FQDN)。
4. 在 **Receiver for Web Path**（Receiver for Web 路径）中，保留默认路径或者输入您自己的路径。
5. 选择 **HTTPS** 以实现安全的用户连接
6. 在 单点登录域中，输入 StoreFront 的域。
7. 如果部署 StoreFront 并提供对 Citrix Virtual Apps 中已发布应用程序或 Citrix Virtual Desktops 中的虚拟桌面的虚拟桌面的访问权限，请在 STA **URL** 中输入运行安全票证颁发机构 (STA) 的服务器的完整 IP 地址或 FQDN。
8. 单击 **Done**（完成）。

当用户通过 NetScaler Gateway 连接到 StoreFront 时，用户可以从 Receiver for Web 或 Receiver 启动其应用程序和桌面。

仅为 **Endpoint Management** 配置设置

1. 单击 **Citrix Endpoint Management**。
2. 在 应用程序控制器 **FQDN** 中，输入 Endpoint Management 的 FQDN。
3. 单击 **Done**（完成）。

配置 **Web Interface** 设置

1. 在快速配置向导中，单击 **Citrix Virtual Apps and Desktops**。
2. 在部署类型中，选择 **Web Interface**，然后配置以下内容：
    a) 在 **Citrix Virtual Apps** 站点 **URL** 中，键入 Web Interface 的完整 IP 地址或 FQDN。
    b) 在 **Citrix Virtual Apps Services Site URL**（Citrix Virtual Apps Services 站点 URL）中，键入带有 Citrix Workspace 应用程序路径的 Web Interface 的完整 IP 地址或 FQDN。您可以输入默认路径或输入自己的路径。
    c) 在 单点登录域中，输入要使用的域。
    d) 在 **STA URL** 中，键入运行 STA 的服务器的完整 IP 地址或 FQDN。
3. 单击 **Done**（完成）。

NetScaler Gateway 向导

您可以使用 NetScaler Gateway 向导在设备上配置以下设置：

- Virtual servers（虚拟服务器）
- Certificates（证书）
- 命名服务提供商
- 身份验证

- Authorization（授权）
- Port redirection（端口重定向）
- 无客户端访问
- SharePoint 的无客户端访问

使用 **NetScaler Gateway** 向导配置设置

运行安装向导后，可以运行 NetScaler Gateway 向导来配置 NetScaler Gateway 上的其他设置。您可以从配置实用程序运行 NetScaler Gateway 向导。

NetScaler Gateway 随附测试证书。如果没有来自证书颁发机构 (CA) 的签名证书，则可以在使用 NetScaler Gateway 向导时使用测试证书。收到签名证书后，您可以删除测试证书并安装签名证书。Citrix 建议在向用户公开使用 NetScaler Gateway 之前获取签名证书。

注意：您可以在 NetScaler Gateway 向导中创建证书签名请求 (CSR)。如果使用 NetScaler Gateway 向导创建 CSR，则必须退出向导，然后在收到来自证书颁发机构的签名证书时再次启动向导。有关证书的详细信息，请参阅 安装和管理证书。

配置虚拟服务器时，可以在 NetScaler Gateway 向导中为 Internet 协议版本 6 (IPv6) 配置用户连接。有关使用 IPv6 进行用户连接的详细信息，请参阅 为用户连接配置 IPv6。

启动 **NetScaler Gateway** 向导

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 NetScaler Gateway。
2. 在详细信息窗格的入门下，单击 NetScaler Gateway 向导。
3. 单击 Next（下一步），然后按照向导中的说明执行操作。

设置向导

您可以使用安装向导在设备上配置以下初始设置：

- 系统 IP 地址和子网掩码
- 映射的 IP 地址和子网掩码
- 主机名
- Default gateway（默认网关）
- 许可证

注意：在运行安装向导之前，请从 Citrix 网站下载许可证。有关详细信息，请参阅 许可 NetScaler Gateway

已发布应用程序

您可以使用已发布的应用程序向导将 NetScaler Gateway 配置为连接到内部网络中运行 Citrix Virtual Apps and Desktops 的服务器。使用“发布的应用程序”向导，您可以：

- 选择虚拟服务器以连接到服务器场。
- 为 Web Interface 或 StoreFront、单点登录和 Secure Ticket Authority 的用户连接配置设置。
- 为 SmartAccess 创建或选择会话策略。

在向导中，您还可以为用户连接创建会话策略表达式。有关配置 NetScaler Gateway 以连接到服务器场的详细信息，请参阅通过 Web Interface 提供对已发布应用程序和虚拟桌面的访问权限。

集成 **Citrix Endpoint Management** 配置

您可以使用 Citrix Endpoint Management MDM 部署 NetScaler Gateway，该 MDM 提供扩展、确保应用程序的高可用性和维护安全性的能力。要使用 Citrix Endpoint Management 配置，您需要安装版本 10.1，内部版本 120.1316.e。

集成 Citrix Endpoint Management 配置将创建以下内容：

- 设备管理器的负载平衡服务器。
- 使用电子邮件筛选功能对 Microsoft Exchange 服务器进行负载平衡。
- ShareFile 的负载平衡服务器。

有关使用集成 Citrix Endpoint Management 配置创建设置的详细信息，请参阅 为 Citrix Endpoint Management 环境配置设置

配置 **NetScaler Gateway**

February 1, 2024

在 NetScaler Gateway 上配置基本网络设置后，可以配置详细设置，以便用户可以连接到安全网络中的网络资源。这些设置包括：

- Virtual servers（虚拟服务器）。您可以在 NetScaler Gateway 上配置多个虚拟服务器，这样您就可以根据必须实施的用户场景创建不同的策略。每个虚拟服务器都有自己的 IP 地址、证书和策略集。例如，您可以配置虚拟服务器，并根据用户在组中的成员身份以及绑定到虚拟服务器的策略限制用户访问内部网络中的网络资源。您可以使用以下方法创建虚拟服务器：
  - 快速配置向导
  - NetScaler Gateway 向导
  - 配置实用程序

- High availability（高可用性）。在网络中部署两台 NetScaler Gateway 设备时，可以配置高可用性。如果主设备发生故障，辅助设备可以在不影响用户会话的情况下接管。
- 证书。您可以使用证书来保护用户与 NetScaler Gateway 的连接。创建证书签名请求 (CSR) 时，将完全限定的域名添加到证书中。您可以将证书绑定到虚拟服务器。
- Authentication（身份验证）。NetScaler Gateway 支持多种身份验证类型，包括本地 LDAP、RADIUS、SAML、客户端证书和 TACACS+。此外，您还可以配置级联身份验证和双因素身份验证。
  注意：如果您使用 RSA、Safeword 或金雅拓 Protiva 进行身份验证，则可以使用 RADIUS 配置这些类型。
- User connections（用户连接）。您可以使用会话配置文件配置用户连接。在配置文件中，您可以确定用户可以登录的插件，以及用户可能需要的任何限制。然后，您可以使用一个配置文件创建策略。您可以将会话策略绑定到用户、组和虚拟服务器。
- 主页。您可以使用默认的访问界面作为主页，也可以创建自定义主页。用户成功登录 NetScaler Gateway 后，将显示主页。
- 端点分析。您可以在 NetScaler Gateway 上配置策略，以便在用户登录时检查用户设备中的软件、文件、注册表项、进程和操作系统。端点分析允许您通过要求用户设备安装所需的软件来提高网络的安全性。

使用配置实用程序

配置实用程序允许您配置大多数 NetScaler Gateway 设置。您可以使用 Web 浏览器访问配置实用程序。

登录配置实用程序

1. 在 Web 浏览器中，键入 NetScaler Gateway 的系统 IP 地址，例如 `http://192.168.100.1`。
   注意：NetScaler Gateway 已预先配置了默认 IP 地址
   192.168.100.1 和子网掩码
   255.255.0.0。
2. 在用户名和密码中，键入 `nsroot`.
3. 在部署类型中，选择 NetScaler Gateway，然后单击登录。

首次登录配置实用程序时，默认情况下会在 主页 选项卡上打开控制板。在主 页 选项卡上，您可以使用快速配置向导配置虚拟服务器、身份验证、证书和 Citrix Endpoint Management 的设置。您还可以在快速配置向导中配置 StoreFront 或 Web Interface 设置。

有关配置 NetScaler Gateway 的更多信息，请参阅：

- 使用安装向导配置初始设置。
- 使用快速配置向导配置设置
- 使用 NetScaler Gateway 向导配置设置。

创建虚拟服务器

February 1, 2024

虚拟服务器是用户登录的接入点。每个虚拟服务器都有自己的 IP 地址、证书和策略集。虚拟服务器由 IP 地址、端口和接受传入流量的协议组成。虚拟服务器包含用户登录设备时的连接设置。您可以在虚拟服务器上配置以下设置：

- Certificates（证书）
- 身份验证
- 策略
- 书签
- 地址池（也称为 IP 池或内部网 IP）
- 使用 NetScaler Gateway 进行双跃点 DMZ 部署
- Secure Ticket Authority
- SmartAccess ICA 代理会话传输

如果运行 NetScaler Gateway 向导，则可以在向导期间创建虚拟服务器。您可以通过以下方式配置更多虚拟服务器：

- 来自虚拟服务器节点。此节点位于配置实用程序的导航窗格中。您可以使用配置实用程序添加、编辑和删除虚拟服务器。
- 使用快速配置向导。如果在环境中部署 Citrix Endpoint Management、StoreFront 或 Web Interface，则可以使用快速配置向导创建虚拟服务器以及部署所需的所有策略。

如果希望用户登录并使用特定的身份验证类型（例如 RADIUS），则可以配置虚拟服务器并为服务器分配唯一的 IP 地址。用户登录时，系统会将他们定向到虚拟服务器，然后提示他们输入 RADIUS 凭据。

您还可以配置用户登录 NetScaler Gateway 的方式。您可以使用会话策略配置用户软件的类型、访问方法以及用户登录后看到的主页。

创建虚拟服务器

您可以使用 NetScaler Gateway GUI 或快速配置向导添加、修改、启用或禁用和删除虚拟服务器。有关使用快速配置向导配置虚拟服务器的详细信息，请参阅
使用快速配置向导配置设置。

使用 **GUI** 创建虚拟服务器

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 在详细信息窗格中，单击“添加”。
3. 根据需要配置设置。
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。

使用 **CLI** 创建虚拟服务器

在命令提示窗口中，键入：

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

示例：

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

将网络配置文件绑定到 **VPN** 虚拟服务器时的注意事项

您可以创建网络配置文件（网络配置文件）以将设备配置为使用指定的源 IP 地址并将网络配置文件绑定到 VPN 虚拟服务器。但是，在将网络配置文件绑定到 VPN 虚拟服务器时，请注意以下事项。

- 将网络配置文件绑定到 NetScaler Gateway 虚拟服务器时，网络配置文件不会选择虚拟服务器或服务用于传输到后端服务器的流量的特定 SNIP。相反，网关设备会忽略网络配置文件绑定，并使用轮询方法选择剪断。
- Net 配置文件不适用于动态生成的服务（STA、SF 监视器）。对于 STA 和其他动态生成的服务，您可以直接将网络配置文件绑定到这些监视器，然后在此时使用这些监视器。但是，如果同一设备上有多个网关，则所有网关对配置的监视器使用相同的网络配置文件。

有关网络配置文件的更多详细信息，请参阅 使用指定的源 IP 进行后端通信。

虚拟服务器上的当前用户和已连接用户总数

当前用户：登录到特定虚拟服务器的用户数。建议您监视当前用户是否跟踪 CCU。

已连接用户总数：通过特定虚拟服务器拥有一个或多个活动连接的用户数。连接的用户总数主要在 ICA Proxy 中使用。

在以下情况下，您可以使用已连接用户总数计数器：

- 请考虑已建立 ICA 连接，但没有建立相应的身份验证、授权和审核会话。在这种情况下，用户启动应用程序或桌面并关闭浏览器，继续在启动的应用程序或桌面上工作。身份验证、授权和审核会话超时，但连接仍处于活动状态。连接的用户总数可用于识别仍处于连接状态的用户。
- 在 HDX 最佳路由中，身份验证网关和 ICA 网关可以位于不同的设备上。在这种情况下，连接的用户总数可用于标识 ICA 网关上已连接的用户数。

注意事项：

- 当存在活动会话（尚未超时）但这些会话上没有活动连接时，当前用户超过连接的总用户数。例如，用户启动了应用程序或桌面并立即将其关闭，但没有从身份验证、授权和审核会话中注销。

- 如果身份验证、授权和审核会话超时但 ICA 连接仍处于活动状态，则连接的用户总数将超过当前用户
- 在纯 VPN 设置中（不涉及 ICA），当前用户数和已连接用户总数相等。

在虚拟服务器上配置连接类型

创建和配置虚拟服务器时，可以配置以下连接选项：

- 使用 Citrix Workspace 应用程序仅连接到没有 SmartAccess、端点分析或网络层通道功能的 Citrix Virtual Apps and Desktops。
- 与 Citrix Secure Access 客户端和 SmartAccess 的连接，允许使用 SmartAccess、端点分析和网络层通道功能。
- 与 Secure Hub 的连接，可建立从移动设备到 NetScaler Gateway 的 Micro VPN 连接。
- 来自多个设备的用户通过 ICA 会话协议建立的并行连接。这些连接将迁移到单个会话，以防止使用多个通用许可证。

如果希望用户在没有用户软件的情况下登录，则可以配置无客户端访问策略并将其绑定到虚拟服务器。

在虚拟服务器上配置基本连接或 **SmartAccess** 连接

1. 导航到 **NetScaler Gateway** ，然后单击 虚拟服务器。
2. 在详细信息窗格中，单击“添加”。
3. 在 名称中，键入虚拟服务器的名称。
4. 在 **IP** 地址 和 端口中，键入虚拟服务器的 IP 地址和端口号。
5. 执行以下操作之一：
   - 要仅允许 ICA 连接，请单击“基本模式”。
   - 要允许用户使用 Secure Hub、Citrix Secure Access 客户端和 SmartAccess 登录，请单击 **SmartAccess** 模式。
   - 要允许 SmartAccess 管理多个用户连接的 ICA 代理会话，请单击 **ICA** 代理会话迁移。
6. 配置虚拟服务器的其他设置，单击 创建，然后单击 关闭。

为通配符虚拟服务器配置侦听策略

您可以将 NetScaler Gateway 虚拟服务器配置为限制虚拟服务器在特定 VLAN 上侦听的能力。您可以使用监听策略创建通配符虚拟服务器，该策略将其限制为处理指定 VLAN 上的流量。

配置参数包括：

参数	说明
名称	虚拟服务器的名称。该名称是必需的，创建虚拟服务器后无法更改它。名称不能超过 127 个字符，第一个字符必须是数字或字母。您还可以使用以下字符：at 符号 (@)、下划线 (_)、短划线 (-)、句点 (.)、冒号 (:)、井号 (#) 和空格。
IP	虚拟服务器的 IP 地址。对于绑定到 VLAN 的通配符虚拟服务器，值始终为 *。
类型	服务的行为。您可以选择 HTTP、SSL、FTP、TCP、SSL_TCP、UDP、SSL_TCP、UDP、SSL_BRIDGE、NNTP、DNS、ANY、SIP-UDP、DNS-TCP 和 RTSP。
端口	虚拟服务器监听用户连接的端口。端口号必须介于 0 和 65535 之间。对于绑定到 VLAN 的通配符虚拟服务器，值通常为 *。
听优先级	分配给监听策略的优先级。优先级的评估顺序相反；数字越小，分配给监听策略的优先级越高。
监听策略规则	用于标识虚拟服务器必须侦听的 VLAN 的策略规则。规则是：CLIENT.VLAN.ID.EQ (<ipaddressat>) 对于 <ipaddressat>，用分配给 VLAN 的 ID 号替换。

使用侦听策略创建通配符虚拟服务器

1. 在导航窗格中，展开 **NetScaler Gateway** ，然后单击 虚拟服务器。
2. 在详细信息窗格中，单击“添加”。
3. 在 名称中，键入虚拟服务器的名称。
4. 在 协议中，选择协议。
5. 在 **IP** 地址中，键入虚拟服务器的 IP 地址。
6. 在 **Port** 中，键入虚拟服务器的端口。
7. 在“高级”选项卡上的“侦听策略”下的“侦听优先级”中，键入监听策略的优先级。
8. 在侦听策略规则旁边，单击 配置。
9. 在“创建表达式”对话框中，单击“添加”，配置表达式，然后单击“确定”。
10. 单击 **Create**（创建），然后单击 **Close**（关闭）。

在 **NetScaler Gateway** 上配置 **IP** 地址

February 1, 2024

您可以配置 IP 地址以登录配置实用程序和用户连接。NetScaler Gateway 配置了用于管理访问的默认 IP 地址 192.168.100.1 和子网掩码 255.255.0.0。每当缺少用户为系统 IP (NSIP) 地址配置的值时，将使用默认 IP 地址。

- NSIP 地址。NetScaler Gateway 的管理 IP 地址，用于对设备的所有与管理相关的访问。NetScaler Gateway 还使用 NSIP 地址进行身份验证。
- 默认网关。将流量从安全网络外部转发到 NetScaler Gateway 的路由器。
- 子网 **IP (SNIP)** 地址。通过与辅助网络上的服务器通信来表示用户设备的 IP 地址。

SNIP 地址使用端口 1024 到 64000。

NetScaler Gateway 如何使用 IP 地址

NetScaler Gateway 根据正在发生的函数从 IP 地址获取流量。作为一般准则，以下列表介绍了几个函数以及 NetScaler Gateway 为每个函数使用 IP 地址的方式：

- 身份验证。NetScaler Gateway 使用的 IP 地址取决于身份验证服务器类型。
  - LDAP /RADIUS/TACACS 服务器。如果 AAAD 直接与身份验证虚拟服务器通信，则使用 NSIP 地址。
  - 如果使用负载平衡器作为代理，则负载平衡器将使用 SNIP 地址进行身份验证。AAAD 使用 NSIP 地址与负载平衡器进行通信。NetScaler 使用的 IP 地址取决于与身份验证虚拟服务器通信的实体。
  - SAML/OAUTH/WEBAUTH 服务器：这些服务器使用 SNIP 地址进行通信。
- 从主页传输文件。NetScaler Gateway 使用 SNIP 地址。
- **DNS** 和 **WINS** 查询。NetScaler Gateway 使用 SNIP 地址。
- 安全网络中资源的网络流量。NetScaler Gateway 使用 SNIP 地址或 IP 池，具体取决于 NetScaler Gateway 上的配置。
- **ICA** 代理设置。NetScaler Gateway 使用 SNIP 地址。

子网 IP 地址

子网 IP 地址允许用户从驻留在另一个子网上的外部主机连接到 NetScaler Gateway。添加子网 IP 地址时，将在路由表中创建相应的路由条目。每个子网只能输入一个条目。路由条目对应于子网中添加的第一个 IP 地址。

与系统 IP 地址和映射的 IP 地址不同，在 NetScaler Gateway 的初始配置期间不必指定子网 IP 地址。

映射的 IP 地址和子网 IP 地址使用端口 1024 到 64000。

添加子网 IP 地址

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统\ > 网络”，然后单击“**IP**”。
2. 在详细信息窗格中，单击“添加”。
3. 在“创建 IP”对话框的“IP 地址”中，键入 IP 地址。
4. 在 Netmask 中，键入子网掩码。
5. 在 IP 类型下，选择子网 IP，单击 关闭，然后单击 创建。

为用户连接配置 **IPv6**

您可以使用互联网协议版本 6 (IPv6) 将 NetScaler Gateway 配置为侦听用户连接。配置以下设置之一时，可以选中 IPv6 复选框，然后在对话框中输入 IPv6 地址：

- 全局设置—发布的应用程序—ICA 代理
- 全局验证-RADIUS
- 全局身份验证-LDAP
- 全局身份验证-TACACS
- 会话配置文件-发布的应用程序-ICA
- NetScaler Gateway 虚拟服务器
- 创建身份验证服务器 - RADIUS
- 创建身份验证服务器-LDAP
- 创建身份验证服务器 - TACACS
- 创建审核服务器
- 高可用性设置
- 绑定/解绑路由监视器以实现高可用性
- 虚拟服务器（负载平衡）

当您将 NetScaler Gateway 虚拟服务器配置为监听 IPv6 地址时，用户只能连接 Citrix Workspace 应用程序。IPv6 不支持用户与 Citrix Secure Access 客户端的连接。

您可以使用以下准则在 NetScaler Gateway 上配置 IPv6：

- Citrix Virtual Apps 和 Web Interface。为用户连接配置 IPv6 时，如果存在使用 IPv6 的映射 IP 地址，Citrix Virtual Apps 和 Web Interface 服务器也可以使用 IPv6。Web Interface 必须安装在 NetScaler Gateway 后面。当用户通过 NetScaler Gateway 进行连接时，IPv6 地址将转换为 IPv4。连接返回后，IPv4 地址将转换为 IPv6。
- Virtual servers（虚拟服务器）。运行 NetScaler Gateway 向导时，可以为虚拟服务器配置 IPv6。在虚拟服务器页面的 NetScaler Gateway 向导中，单击 IPv6 并输入 IP 地址。只能使用 NetScaler Gateway 向导为虚拟服务器配置 IPv6 地址。
- 其他。要为 ICA 代理、身份验证、审核和高可用性配置 IPv6，请在对话框中选中 IPv6 复选框，然后键入 IP 地址。

解析位于安全网络中的 **DNS** 服务器

February 1, 2024

如果您的 DNS 服务器位于防火墙后面的安全网络中，并且防火墙阻止了 ICMP 通信，则无法测试与服务器的连接，因为防火墙阻止了请求。您可以通过执行以下步骤来解决此问题：

- 使用解析为已知的完全限定域名 (FQDN) 的自定义 DNS 监视器创建 DNS 服务。

- 在 NetScaler Gateway 上创建不可直接寻址的 DNS 虚拟服务器。
- 将服务绑定到虚拟服务器。

注意：

- 仅当 DNS 服务器位于防火墙后面时，才配置 DNS 虚拟服务器和 DNS 服务。
- 如果在设备上安装 NetScaler 负载平衡许可证，则导航窗格中不会显示“虚拟服务器和服务”节点。您可以通过展开负载平衡然后单击虚拟服务器来执行此过程。

配置 **DNS** 服务和 **DNS** 监视器

1. 在配置实用程序的配置选项卡的导航窗格中，展开虚拟服务器和服务，然后单击虚拟服务器。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在名称中，键入服务的名称。
4. 在协议中，选择 DNS。
5. 在 IP 地址中，键入 DNS 服务器的 IP 地址。
6. 在 Port（端口）中，键入端口号。
7. 在服务选项卡上，单击添加。
8. 在“监视器”选项卡上的“可用”下，选择“DNS”、“添加”、“创建”，然后单击“关闭”。
9. 在创建虚拟服务器 (负载平衡) 对话框中，单击创建，然后单击关闭。

接下 来，使用以下过程创建 DNS 虚拟服务器：配置 DNS 虚拟服务器 ，然后将 DNS 服务绑定到虚拟服务器。

将 **DNS** 服务绑定到 **DNS** 虚拟服务器

1. 在“配置虚拟服务（负载平衡）”对话框中的“服务”选项卡上，单击“添加”，选择 DNS 服务，单击“创建”，然后单击“关闭”。

配置 **DNS** 虚拟服务器

February 1, 2024

要配置 DNS 虚拟服务器，请指定名称和 IP 地址。与 NetScaler Gateway 虚拟服务器一样，您必须为 DNS 虚拟服务器分配 IP 地址。但是，此 IP 地址必须位于目标网络的内部，以便用户设备能够解析所有内部地址。另外，请指定 DNS 端口。

注意：如果在设备上安装 NetScaler 负载平衡许可证，则导航窗格中不会显示“
虚拟服务器和服务”节点。您可以使用负载平衡虚拟服务器配置此功能。有关更多信息，请参阅 NetScaler 产品文档中的 NetScaler 文档。

配置 **DNS** 虚拟服务器

1. 在配置实用程序的配置选项卡的导航窗格中，展开虚拟服务器和服务，然后单击虚拟服务器。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在 名称中，键入虚拟服务器的名称。
4. 在 IP 地址中，键入 DNS 服务器的 IP 地址。
5. 在端口中，键入 DNS 服务器监听的端口。
6. 在协议中，选择 DNS，然后单击创建。

最后，根据部署的需要，通过以下两种方法之一将 DNS 虚拟服务器与 NetScaler Gateway 关联：

- 将服务器全局绑定到 NetScaler Gateway。
- 基于每个虚拟服务器绑定 DNS 虚拟服务器。

如果在全球范围内部署 DNS 虚拟服务器，则所有用户都可以访问它。然后，您可以通过将 DNS 虚拟服务器绑定到虚拟服务器来限制用户。

配置名称服务提供商

February 1, 2024

NetScaler Gateway 使用名称服务提供商将 Web 地址转换为 IP 地址。

运行 NetScaler Gateway 向导时，可以配置 DNS 服务器或 WINS 服务器。您还可以使用配置实用程序配置其他 DNS 或 WINS 服务器。

向 **NetScaler Gateway** 添加 **DNS** 服务器

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在网络配置选项卡上，单击添加。
4. 在“插入名称服务器”对话框的“IP 地址”中，键入 DNS 服务器的 IP 地址，单击“创建”，然后单击“关闭”。
5. 在配置实用程序中单击确定。

将 **WINS** 服务器添加到 **NetScaler Gateway**

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“网络配置”选项卡的 WINS 服务器 IP 中，键入 WINS 服务器的 IP 地址，然后单击“确定”。

接下来，指定 DNS 虚拟服务器名称和 IP 地址。与 NetScaler Gateway 虚拟服务器一样，必须为虚拟服务器分配 IP 地址。但是，此 IP 地址必须位于目标网络的内部，以便用户设备能够正确解析所有内部地址。您还必须指定 DNS 端口。

如果为名称解析配置 DNS 服务器和 WINS 服务器，则可以使用 NetScaler Gateway 向导选择首先执行名称查找的服务器。

指定名称查找优先级

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 NetScaler Gateway。
2. 在详细信息窗格的入门下，单击 NetScaler Gateway 向导。
3. 单击“下一步”以接受当前设置，直到进入“名称服务提供者”页。
4. 在名称查找优先级中，选择 WINS 或 DNS，然后继续到向导结束。

配置服务器启动的连接

February 1, 2024

对于在启用 IP 地址的情况下登录 NetScaler Gateway 的每个用户，DNS 后缀都会附加到用户名后面，并将 DNS 地址记录添加到设备的 DNS 缓存中。此技术有助于为用户提供 DNS 名称，而不是用户的 IP 地址。

将 IP 地址分配给用户的会话时，可以从内部网络连接到用户的设备。例如，连接到远程桌面或虚拟网络计算 (VNC) 客户端的用户可以访问用户设备来诊断问题应用程序。两个具有内部网络 IP 地址且远程登录的 NetScaler Gateway 用户也可以通过 NetScaler Gateway 相互通信。允许在设备上发现已登录用户的内部网络 IP 地址有助于进行此通信。

远程用户可以使用以下 ping 命令发现可以登录 NetScaler Gateway 的用户的内部网络 IP 地址，然后：

```
ping \<username.domainname\>
```

服务器可以通过以下不同方式启动与用户设备的连接：

- TCP 或 UDP 连接。连接可以来自内部网络中的外部系统，也可以来自登录到 NetScaler Gateway 的另一台计算机。分配给登录到 NetScaler Gateway 的每个用户设备的内部网络 IP 地址将用于这些连接。介绍了 NetScaler Gateway 支持的不同类型的服务器启动的连接。
  对于 TCP 或 UDP 服务器启动的连接，服务器事先了解用户设备的 IP 地址和端口并与之建立连接。NetScaler Gateway 会拦截此连接。

  然后，用户设备与服务器建立初始连接，并且服务器通过已知或派生自第一个已配置端口的端口连接到用户设备。

  在这种情况下，用户设备与服务器建立初始连接，然后使用嵌入此信息的应用程序特定协议与服务器交换端口和 IP 地址。这使 NetScaler Gateway 能够支持应用程序，例如活动 FTP 连接。
- 端口命令。这在活动的 FTP 和某些 IP 语音协议中使用。

- 插件之间的连接。NetScaler Gateway 通过使用内部网络 IP 地址支持插件之间的连接。

  通过这种类型的连接，使用同一 NetScaler Gateway 的两个 NetScaler Gateway 用户设备可以相互启动连接。这种类型的一个例子是使用即时消息传递应用程序，例如 Office Communicator 或 Yahoo! 信使。

如果用户注销 NetScaler Gateway 但注销请求未到达设备，则用户可以使用任何设备再次登录，然后用新会话替换以前的会话。在为每个用户分配一个 IP 地址的部署中，此功能可能会有所帮助。

当用户首次登录 NetScaler Gateway 时，将创建一个会话并为该用户分配一个 IP 地址。如果用户注销但注销请求丢失，或者用户设备无法执行干净注销，则会话将在系统中保留。如果用户尝试从同一台设备或另一台设备再次登录，则在成功进行身份验证后，将显示转移登录对话框。如果用户选择转移登录信息，则 NetScaler Gateway 上的上一个会话将关闭并创建新会话。登录转移在注销后仅有两分钟处于活动状态，如果同时尝试从多台设备登录，则最后一次登录尝试将替换原始会话。

为服务器启动的连接配置专用端口范围

从 Citrix Secure Access 客户端版本 23.10.1.7 开始，您可以为服务器启动的连接 (SIC) 配置范围从 49152 到 64535 的专用端口。配置专用端口可以避免在使用端口在 Citrix Secure Access 客户端与客户端上的第三方应用程序之间创建套接字时可能出现的冲突。这仅在使用 WFP 驱动程序时适用。

您可以使用 `SicBeginPort` Windows VPN 注册表来配置专用端口。或者，您可以使用 NetScaler 上的 VPN 插件自定义 JSON 文件配置专用端口范围。

如果服务器启动连接，Citrix Secure Access 客户端将使用从 `SicBeginPort` Windows VPN 注册表开始的前 1000 个端口来创建套接字。如果注册表是在客户端上配置的，则注册表设置优先于 NetScaler JSON 设置。

以下是 NetScaler 上的 VPN 插件 JSON 配置示例：

```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json

{
 "SicBeginPort" : 51000 }

<!--NeedCopy-->
```

有关注册表设置的详细信息，请参阅 NetScaler Gateway Windows VPN 客户端注册表项。

> 注意：
>
> 用于创建套接字的默认端口范围为 62500—63500。

在 **NetScaler Gateway** 上配置路由

February 1, 2024

为了提供对内部网络资源的访问，NetScaler Gateway 会将数据路由到内部安全网络。默认情况下，NetScaler Gateway 使用静态路由。

NetScaler Gateway 可以将数据路由到的网络由配置 NetScaler Gateway 路由表和为 NetScaler Gateway 指定的默认网关的方式决定。

NetScaler Gateway 路由表必须包含将数据路由到用户可能需要访问的任何内部网络资源所需的路由。

NetScaler Gateway 支持以下路由协议：

- 路由信息协议（RIP v1 和 v2）
- 开放最短路径优先 (OSPF)
- 边界网关协议 (BGF)

配置静态路由

设置与其他主机或网络的通信时，如果不使用动态路由，则需要配置从 NetScaler Gateway 到新目的地的静态路由。

配置静态路由

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”**>**“网络”**>**“高级”，然后单击“路由”。
2. 在详细信息窗格的基本选项卡上，单击 添加。
3. 配置路由的设置，然后单击 创建。

测试静态路由

1. 在配置实用程序的导航窗格中，展开 系统，然后单击 诊断。
2. 在详细信息窗格中的实用程序下，单击 **Ping**。
3. 在参数下的主机名中，键入设备的名称。
4. 在“高级”下的“源 IP 地址”中，键入设备的 IP 地址，然后单击“运行”。

   如果您与另一台设备成功通信，则消息表明传输和接收的数据包数量相同，没有丢失任何数据包。

   如果您没有与其他设备通信，则状态消息表明收到的数据包为零，所有数据包都丢失了。要纠正这种缺乏通信的情况，请重复该过程以添加静态路由。

要停止测试，请在 **Ping** 对话框中单击 停止，然后单击 关闭。

配置自动协商

February 1, 2024

默认情况下，设备配置为使用自动协商，其中 NetScaler Gateway 同时向双向传输网络流量并确定适当的适配器速度。如果将默认设置保留为
自动协商，NetScaler Gateway 将使用全双工操作，其中网络适配器能够同时向双向发送数据。

如果禁用自动协商，NetScaler Gateway 将使用半双工操作，在这种操作中，适配器可以在两个节点之间双向发送数据，但适配器一次只能使用一个方向或另一个方向。

对于首次安装，Citrix 建议您将 NetScaler Gateway 配置为对连接到设备的端口使用自动协商。最初登录并配置 NetScaler Gateway 后，可以禁用自动协商。您不能全局配置自动协商。必须启用或禁用每个接口的设置。

启用或禁用自动协商

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统**\ >** 网络”，然后单击“接口”。
2. 在详细信息窗格中，选择接口，然后单击 打开。
3. 在“配置接口”对话框中执行以下操作之一：
    - 要启用自动协商，请单击“自动协商”旁边的“是”，然后单击“确定”。
    - 要禁用自动协商，请单击“自动协商”旁边的“否”，然后单击“确定”。

在 **NetScaler Gateway** 上配置主机名和 **FQDN**

February 1, 2024

主机名是与许可证文件关联的 NetScaler Gateway 设备的名称。主机名对于设备是唯一的，在下载通用许可证时使用。在运行设置向导首次配置 NetScaler Gateway 时，可以定义主机名。

完全限定域名 (FQDN) 包含在绑定到虚拟服务器的签名证书中。您不需要在 NetScaler Gateway 上配置 FQDN。一台设备可以使用证书将唯一的 FQDN 分配给 NetScaler Gateway 上配置的每个虚拟服务器。

您可以通过查看证书的详细信息来查找证书的 FQDN。FQDN 位于证书的主题字段中。

查看证书的 **FQDN**

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **SSL**，然后单击 证书。
2. 在详细信息窗格中，选择一个证书，单击 操作，然后单击 详细信息。
3. 在证书详细信息对话框中，单击 主题。证书的 FQDN 将显示在列表中。

NetScaler Gateway 上的策略和配置文件

February 1, 2024

NetScaler Gateway 上的策略和配置文件允许您在指定的方案或条件下管理和实施配置设置。单个策略说明或定义了在满足一组指定条件时生效的配置设置。每个策略都有一个唯一的名称，并且可以将配置文件绑定到该策略。

策略如何运作

策略由布尔条件和称为配置文件的设置集合组成。在运行时评估条件以确定是否必须应用策略。

配置文件是使用特定参数的设置集合。配置文件可以有任何名称，您可以在多个策略中重复使用它。您可以在配置文件中配置多个设置，但每个策略只能包含一个配置文件。

您可以使用配置的条件和配置文件将策略绑定到虚拟服务器、组、用户或全局。策略由它们控制的配置设置类型来引用。例如，在会话策略中，您可以控制用户的登录方式以及用户可以保持登录状态的时间。

如果您将 NetScaler Gateway 与 Citrix Virtual Apps 结合使用，NetScaler Gateway 策略名称将作为筛选器发送到 Citrix Virtual Apps。将 NetScaler Gateway 配置为与 Citrix Virtual Apps 和 SmartAccess 兼容时，您可以在 Citrix Virtual Apps 中配置以下设置：

- 在设备上配置的虚拟服务器的名称。该名称将作为 NetScaler Gateway 场名称发送到 Citrix Virtual Apps。
- 预身份验证或会话策略的名称将作为过滤器名称发送。

有关将 NetScaler Gateway 配置为与 Citrix Endpoint Management 兼容的更多信息，请参阅为 Citrix Endpoint Management 环境配置设置。

有关将 NetScaler Gateway 配置为与 Citrix Virtual Apps and Desktops 兼容的更多信息，请参阅使用Web Interface 访问 Citrix Virtual Apps 和 Citrix Virtual Desktops 资源和与 Citrix Endpoint Management 或 StoreFront 集成。

有关预身份验证策略的更多信息，请参阅 配置端点策略。

条件策略

配置策略时，可以使用任何布尔表达式来表示应用策略的条件。配置条件策略时，可以使用任何可用的系统表达式，例如：

- 客户端安全字串
- 网络信息
- HTTP 标头和饼干
- 一天中的时间
- 客户端证书值

您还可以创建仅在用户设备满足特定条件时应用的策略，例如 SmartAccess 的会话策略。

配置条件策略的另一个示例是更改用户的身份验证策略。例如，您可以要求从内部网络外部（例如从家用计算机或使用移动设备上的 Micro VPN）连接到 Citrix Secure Access 客户端的用户使用 LDAP 进行身份验证，并要求通过 WAN 连接的用户使用 RADIUS 进行身份验证。

注意：如果在会话配置文件中将策略规则配置为安全设置的一部分，则无法使用基于端点分析结果的策略条件。

策略的优先事项

按照策略绑定的顺序对策略进行优先级排序和评估。

以下两种方法确定策略优先级：

- 策略绑定到的级别：全局、虚拟服务器、组或用户。策略级别按从最高到最低的顺序排列如下：
  - 用户（最高优先级）
  - 组
  - 虚拟服务器
  - 全局（最低优先级）
- 无论策略绑定到哪个级别，数字优先级都优先。如果全局绑定的策略的优先级号为 1，而绑定到用户的另一个策略的优先级号为 2，则全局策略优先级。较低优先级的数字会使策略具有更高的优先级。

在 **NetScaler Gateway** 上创建策略

您可以使用配置实用程序创建策略。创建策略后，将策略绑定到适当的级别：用户、组、虚拟服务器或全局。将策略绑定到这些级别之一时，如果满足策略条件，用户将收到配置文件中的设置。每个策略和配置文件都有唯一的名称。

如果将 Citrix Endpoint Management 或 StoreFront 作为部署的一部分，则可以使用快速配置向导配置此部署的设置。有关向导的详细信息，请参阅使用快速配置向导配置设置。

配置系统表达式

February 1, 2024

系统表达式指定强制执行策略的条件。例如，预身份验证策略中的表达式是在用户登录时强制执行的。会话策略中的表达式在用户通过身份验证并登录 NetScaler Gateway 后进行评估和实施。

NetScaler Gateway 上的表达式包括：

- 限制用户在建立与 NetScaler Gateway 的连接时可以使用的对象的通用表达式。例如，请参阅：
  - 会话策略

- 客户端安全表达式，用于定义必须在用户设备上安装和运行的软件、文件、进程或注册表值。例如，请参阅：
  - 端点策略
- 基于网络的表达式，根据网络设置限制访问。例如，请参阅：
  - 流量策略
  - 授权策略

NetScaler Gateway 也可以用作 NetScaler 设备。设备上的某些表达式更适用于 NetScaler。通用表达式和基于网络的表达式通常用于 NetScaler，通常不与 NetScaler Gateway 一起使用。NetScaler Gateway 上使用客户端安全表达式来确定用户设备上是否安装了正确的项目。

配置客户端安全表达

表达式是策略的组成部分。表达式表示根据请求或响应进行评估的单个条件。您可以创建一个简单的表达式安全字符串来检查条件，例如：

- 包括服务包的用户设备操作系统
- 防病毒软件版本和病毒定义
- 文件
- 进程
- 注册表值
- 用户证书

NetScaler Gateway 上的证书管理

February 1, 2024

在 NetScaler Gateway 上，您可以使用证书创建安全连接和对用户进行身份验证。

要建立安全连接，在连接的一端需要有服务器证书，在连接的另一端需要颁发服务器证书的证书颁发机构 (CA) 的根证书。

- 服务器证书。服务器证书证明服务器的身份。NetScaler Gateway 需要这种类型的数字证书。
- 根证书。根证书用来识别为服务器证书签名的 CA。根证书属于证书颁发机构。用户设备需要这种类型的数字证书来验证服务器证书。

与用户设备上的 Web 浏览器建立安全连接时，服务器会将其证书发送到设备。

当用户设备收到服务器证书时，Web 浏览器（例如 Internet Explorer）会检查哪个 CA 颁发了证书，以及该 CA 是否受到用户设备的信任。如果 CA 不受信任，或者它是测试证书，Web 浏览器会提示用户接受或拒绝该证书（实际上是接受或拒绝访问站点的能力）。

NetScaler Gateway 支持以下三种类型的证书：

- 绑定到虚拟服务器的测试证书，也可用于连接到服务器场。NetScaler Gateway 随附预安装的测试证书。
- 由 CA 签名并与私钥配对的 PEM 或 DER 格式的证书。
- PKCS #12 格式的证书，用于存储或传输证书和私钥。PKCS #12 证书通常从现有的 Windows 证书作为 PFX 文件导出，然后安装在 NetScaler Gateway 上。

Citrix 建议使用由受信任的 CA（例如 Thawte 或 Verisign）签名的证书。

创建证书签名请求

February 1, 2024

要使用 SSL 或 TLS 提供安全通信，NetScaler Gateway 上需要服务器证书。在将证书上载到 NetScaler Gateway 之前，您需要生成证书签名请求 (CSR) 和私钥。您可以使用 NetScaler Gateway 向导中包含的创建证书请求或配置实用程序来创建 CSR。创建证书请求会创建一个.csr 文件，该文件通过电子邮件发送给证书颁发机构 (CA) 进行签名，并创建一个保留在设备上的私钥。CA 对证书进行签名，然后通过您提供的电子邮件地址将其退还给您。收到签名证书后，可以将其安装在 NetScaler Gateway 上。当您收到来自 CA 的证书时，您需要将证书与私钥配对。

重要：使用 NetScaler Gateway 向导创建 CSR 时，必须退出向导并等待 CA 向您发送签名证书。收到证书后，可以再次运行 NetScaler Gateway 向导以创建设置并安装证书。有关 NetScaler Gateway 向导的详细信息，请参阅使用 NetScaler Gateway 向导配置设置。

使用 **NetScaler Gateway** 向导创建 **CSR**

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的入门下，单击 **NetScaler Gateway** 向导。
3. 按照向导中的说明进行操作，直到进入“指定服务器证书”页面。
4. 单击 创建证书签名请求 并填写字段。
   注意：完全限定域名 (FQDN) 不必与 NetScaler Gateway 主机名相同。FQDN 用于用户登录。
5. 单击“创建”将证书保存在计算机上，然后单击“关闭”。
6. 在不保存设置的情况下退出 NetScaler Gateway 向导。

使用 **NetScaler GUI** 创建 **CSR**

您还可以使用 NetScaler GUI 创建 CSR，而无需运行 NetScaler Gateway 向导。

1. 导航到 流量 管理 > **SSL > SSL** 文件，然后选择创建证书签名请求 **(CSR)**。
2. 完成证书的设置，然后单击 创建。

创建证书和私钥后，通过电子邮件将证书发送给 CA，例如 Thawte 或 Verisign。

有关详细过程，请参阅 创建证书签名请求。

在 **NetScaler Gateway** 上安装签名证书

当您收到来自证书颁发机构 (CA) 的签名证书时，请将其与设备上的私钥配对，然后在 NetScaler Gateway 上安装该证书。

使用 **GUI** 将签名证书与私钥配对

1. 使用安全外壳 (SSH) 程序（例如 WinSCP）将证书复制到 NetScaler Gateway 到文件夹 nsconfig/ssl。
2. 在配置实用程序中的配置选项卡的导航窗格中，展开 **SSL >** 证书。
3. 在 **SSL** 证书 页面中，单击 开始使用。
4. 在详细信息窗格中，单击“安装”。
5. 在 **Certificate-Key Pair Name**（证书密钥对名称）中，键入证书的名称。
6. 在 证书文件名中，单击 装置。
7. 导航到证书，单击 选择，然后单击 打开。
8. 在 密钥文件名中，单击 装置。私钥的名称与证书签名请求 (CSR) 的名称相同。私钥位于 NetScaler Gateway 上\ nsconfig\ ssl 目录中。
9. 选择私钥，然后单击“打开”。
10. 如果证书是 PEM-format，请在“密码”中键入私钥的密码。
11. 如果要为证书到期时配置通知，请选择过 期时通知。
12. 在“通知期限”中，键入天数，单击“创建”，然后单击“关闭”。

使用 **GUI** 将证书和私钥绑定到虚拟服务器

创建并链接证书和私钥对后，将其绑定到虚拟服务器。

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在“证书”选项卡上的“可用”下，选择一个证书，单击“添加”，然后单击“确定”。

使用 **CLI** 将证书和私钥绑定到虚拟服务器

在命令提示窗口中，键入：

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```


示例：

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
<!--NeedCopy-->
```

注意：如果设备证书不需要 OCSP 检查，则 oscpCheck 是可选的。

使用 **GUI** 从虚拟服务器取消绑定测试证书

安装签名证书后，取消绑定到虚拟服务器的所有测试证书。您可以使用配置实用程序解绑测试证书。

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在“证书”选项卡上的“已配置”下，选择测试证书，然后单击“删除”。

配置中间证书

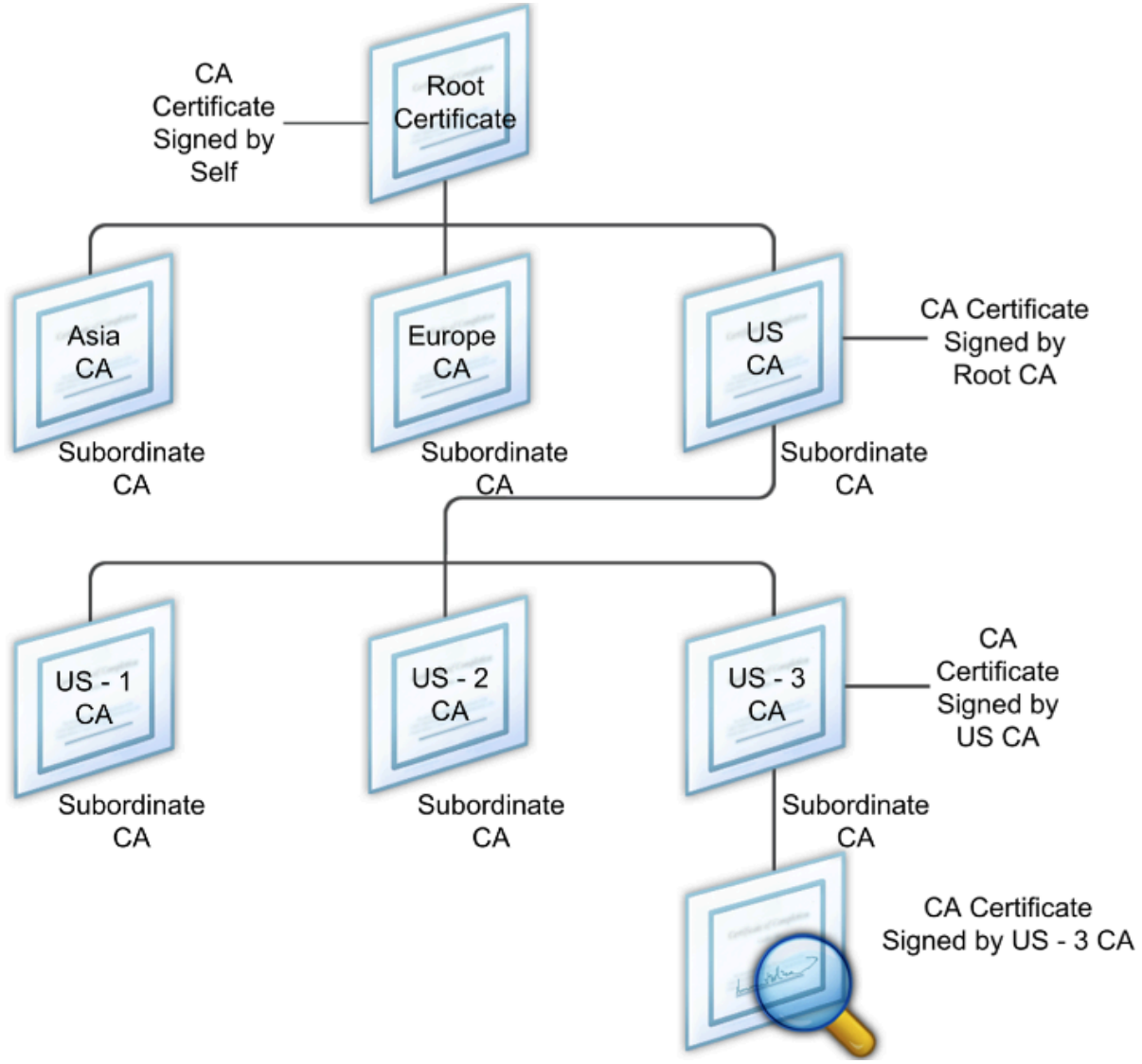
February 1, 2024

中间证书是介于 NetScaler Gateway（服务器证书）和根证书（安装在用户设备上）之间的证书。中间证书是链的一部分。

有些组织委派专人负责颁发证书，以解决各组织单位在地域上彼此独立的问题，或者对组织的不同部门应用不同的颁发策略。

可以通过设置从属证书颁发机构 (CA) 来委派颁发证书的责任。CA 可以签署自己的证书（即，它们是自签名的），也可以由其他证书颁发机构签名。X.509 标准包括一个用于设置 CA 层次结构的模型。在此模型中，如下图所示，根 CA 位于层次结构的顶部，是证书颁发机构的自签名证书。直属于根 CA 的 CA 具有由根证书颁发机构签名的 CA 证书。在层次结构中处于从属 CA 之下的 CA 拥有由从属 CA 签名的 CA 证书。

图 1. 展示典型数字证书链层次结构的 X.509 模型



如果服务器证书由具有自签名证书的 CA 签署，则证书链正好由两个证书组成：最终实体证书和根证书颁发机构。如果用户或服务器证书由中间证书颁发机构签名，则证书链会更长。

下图显示了前两个元素是最终实体证书（在本例中为 gwy01.company.com）和中间证书颁发机构的证书，按顺序排列。中间证书颁发机构的证书后跟其证书颁发机构的证书。此列表将一直持续到列表中的最后一个证书是针对根证书颁发机构的证书。证书链中的每个证书用来证实前一个证书的身份。

图 2. 典型的数字证书链

安装中间证书

1. 在配置实用程序的配置选项卡的导航窗格中，展开 SSL，然后单击证书。
2. 在详细信息窗格中，单击“安装”。
3. 在证书密钥对名称中，键入证书的名称。
4. 在详细信息下的证书文件名中，单击浏览（装置），然后在列表中选择本地或装置。
5. 导航到计算机（本地）或 NetScaler Gateway（设备）上的证书。
6. 在证书格式中，选择 PEM。
7. 单击“Install”（安装），然后单击“Close”（关闭）。

在 NetScaler Gateway 上安装中间证书时，无需指定私钥或密码。

在设备上安装证书后，证书需要链接到服务器证书。

将中间证书链接到服务器证书

1. 在配置实用程序的配置选项卡的导航窗格中，展开 SSL，然后单击证书。
2. 在详细信息窗格中，选择服务器证书，然后在操作中单击链接。
3. 在 CA 证书名称旁边，从列表中选择中间证书，然后单击确定。

使用设备证书进行身份验证

February 1, 2024

NetScaler Gateway 支持设备证书检查，可让您将设备身份绑定到证书的私钥。设备证书检查可以配置为经典或高级端点分析 (EPA) 策略的一部分。在传统的 EPA 策略中，只能为 EPA 预身份验证配置设备证书。

NetScaler Gateway 会在端点分析扫描运行之前或在登录页面出现之前验证设备证书。如果配置端点分析，端点扫描将运行以验证用户设备。当设备通过扫描且 NetScaler Gateway 验证设备证书后，用户可以登录 NetScaler Gateway。

> 重要提示：
>
> - 默认情况下，Windows 要求管理员权限才能访问设备证书。
> - 要为非管理员用户添加设备证书检查，必须安装 VPN 插件。VPN 插件版本必须与设备上的 EPA 插件版本相同。
> - 您可以向网关添加多个 CA 证书并验证设备证书。
> - 如果在 NetScaler Gateway 上安装两个或更多设备证书，则用户必须在开始登录 NetScaler Gateway 时或在端点分析扫描运行之前选择正确的证书。
> - 创建设备证书时，它必须是 X.509 证书。
> - 如果您有中间 CA 颁发的设备证书，则必须同时绑定中间 CA 证书和根 CA 证书。

> - EPA 客户端需要用户具有本地管理员权限才能访问计算机证书存储区。这种情况很少发生，因此解决方法是安装可以访问本地存储的完整 NetScaler Gateway 插件。

有关创建设备证书的详细信息，请参阅以下内容：

- Microsoft Web 站点上 Active Directory 证书服务 (AD CS) 中的网络设备注册服务 (NDES)。
- 如何使用 Apple 技术支持网站上的 DC/RPC 和 Active Directory 证书配置文件负载向 Microsoft 证书颁发机构申 请证书。
- 请访问目录服务团队 Microsoft 支持博客上的iPad/ iPhone 证书颁发。
- 在 Windows IT 专业版网站上设置网络设备注册服务 。
- Microsoft System Center Web 站点上的为 Configuration Manager 部署 PKI 证书的分步示例：Windows Server 2008 证书颁发机构。

配置设备证书的步骤

要配置设备证书，必须完成以下步骤：

- 在 NetScaler Gateway 上安装设备证书颁发者的证书颁发机构证书。有关详细信息，请参阅 在 NetScaler Gateway 上安装签名证书。
- 将设备证书颁发者的证书颁发机构证书绑定到 NetScaler Gateway 虚拟服务器并启用 OCSP 检查。有关详细信息，请参阅 在 NetScaler Gateway 上安装签名证书。
- 在设备证书颁发者的证书颁发机构证书上创建并绑定 OCSP（响应者）。有关详细信息，请参阅使用 OCSP 监视证书状态。

在虚拟服务器上启用设备证书检查，并将设备证书颁发者的证书颁发机构证书添加到设备证书清单中。有关详细信息，请参阅在虚拟服务器上启用设备证书检查以了解经典的 EPA

在 Windows 计算机上完成客户端配置和设备证书验证。有关详细信息，请参阅在 Windows 计算机上验证设备证书。

> 注意：
>
> 所有打算使用设备证书 EPA 检查的客户端都必须在计算机的系统证书存储区中安装设备证书。

在虚拟服务器上启用设备证书检查以获取经典 **EPA** 策略

创建设备证书后，可以使用 将现有证书导入和安装到 NetScaler Gateway 的过程在 NetScaler Gateway 上安装证书。

1. 在“配置”选项卡上，导航到 **NetScaler Gateway >** 虚拟服务器。
2. 在 **NetScaler Gateway** 虚拟服务器页面上，选择现有虚拟服务器，然后单击“编辑”。
3. 在 **VPN Virtual Servers**（VPN 虚拟服务器）页面的 **Basic Settings**（基本设置）部分下，单击 **Edit**（编辑）。

4. 清除 启用身份验证 框以禁用身份验证。
5. 选中 启用设备证书 框以启用设备证书
6. 单击 添加 将可用的设备证书颁发者的 CA 证书名称添加到列表中。
7. 要将 CA 证书绑定到虚拟服务器，请单击 设备证书的 **CA** 部分下的 **CA** 证书，单击 添加，选择证书，然后单击 **+**。

> 注意：
>
> 有关在虚拟服务器上启用和绑定设备证书以实现高级 EPA 策略的信息，请参阅 作为 EPA 组件的 nFactor 中的设备证书。

在 **Windows** 计算机上验证设备证书

1. 打开浏览器并访问 NetScaler Gateway FQDN。
2. 允许 Citrix 端点分析 (EPA) 客户端运行。如果尚未安装，请安装 EPA。

   Citrix EPA 会运行并验证设备证书，如果设备证书 EPA 检查通过，则重定向到身份验证页面，否则会将您重定向到 EPA 错误页面。如果您有其他 EPA 检查，则 EPA 扫描结果取决于配置的 EPA 检查。

要在客户端上进行进一步调试，请检查客户端上的以下 EPA 日志：
C:\Users<User name>\ AppData\ 本地\ Citrix\ AGEE\ nsepa.txt

注意：

> 不支持使用 CRL 进行设备证书验证。

导入并安装现有证书

February 1, 2024

您可以从运行 Internet 信息服务 (IIS) 的基于 Windows 的计算机或运行 Secure Gateway 的计算机导入现有证书。

导出证书时，请确保还导出了私钥。有时，您无法导出私钥，这意味着无法在 NetScaler Gateway 上安装证书。如果发生这种情况，请使用证书签名请求 (CSR) 创建证书。有关详细信息，请参阅 创建证书签名请求。

从 Windows 导出证书和私钥时，计算机会创建个人信息交换 (.pfx) 文件。然后，此文件将作为 PKCS #12 证书安装在 NetScaler Gateway 上。

如果要用 NetScaler Gateway 替换 Secure Gateway，则可以从 Secure Gateway 导出证书和私钥。如果要进行从 Secure Gateway 到 NetScaler Gateway 的就地迁移，则应用程序和设备上的完全限定域名 (FQDN) 必须相同。从 Secure Gateway 导出证书时，您会立即停用 Secure Gateway，在 NetScaler Gateway 上安装证书，然后测试配置。如果 Secure Gateway 和 NetScaler Gateway 具有相同的 FQDN，则它们不能同时在您的网络上运行。

如果您使用的是 Windows Server 2003 或 Windows Server 2008，则可以使用 Microsoft 管理控制台导出证书。有关详细信息，请参阅 Windows 联机帮助。

保留所有其他选项的默认值，定义密码，然后将.pfx 文件保存到计算机。导出证书后，然后将其安装在 NetScaler Gateway 上。

在 **NetScaler Gateway** 上安装证书和私钥

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“入门”下，单击 NetScaler Gateway 向导。
3. 单击“下一步”，选择现有虚拟服务器，然后单击“下一步”。
4. 在 证书选项中，选择 安装 **PKCS #12 (.pfx)** 文件 e。
5. 在 **PKCS #12** 文件名中，单击 浏览，导航到证书，然后单击 选择。
6. 在 ((密码)) 中，键入私钥的密码。

   这是将证书转换为 PEM 格式时使用的密码。
7. 单击 下一步 以完成 NetScaler Gateway 向导，而不更改任何其他设置。

在 NetScaler Gateway 上安装证书后，证书将显示在 **SSL\ >** 证书 节点的配置实用程序中。

创建私钥

1. 在配置实用程序的配置选项卡的导航窗格中，单击 **SSL**。
2. 在详细信息窗格中的 **SSL** 密钥下，单击创建 **RSA** 密钥。
3. 在密钥文件名中，键入私钥的名称或单击“浏览”导航到现有文件。
4. 在密钥大小 **(**位**)** 中，键入私钥的大小。
5. 在公共指数值中，选择 F4 或 3。

   RSA 密钥的公共指数值。这是密码算法的一部分，是创建 RSA 密钥所必需的。这些值为 F4（十六进制：0x10001）或 3（十六进制：0x3）。默认值为 F4。
6. 在密钥格式中，选择 PEM 或 DER。Citrix 建议将 PEM 格式用于证书。
7. 在 **PEM** 编码算法中，选择 DES 或 DES3。
8. 在 **PEM** 密码短语和验证密码短语中，键入密码，单击创建，然后单击关闭。

   注意：要分配密码短语，密钥格式必须为 PEM，并且必须选择编码算法。

要在配置实用程序中创建 DSA 私钥，请单击创建 **DSA** 密钥，然后按照创建 RSA 私钥所执行的步骤操作。

证书吊销列表

February 1, 2024

证书颁发机构 (CA) 有时会发出证书吊销列表 (CRL)。CRL 包含有关不再可信的证书的信息。例如，假设 Ann 离开了 XYZ 公司。公司可以将 Ann 的证书放在 CRL 上，以防止她使用该密钥签署消息。

同样，如果私钥已泄露或证书已过期且正在使用新证书，则可以撤销证书。在信任公钥之前，请确保证书没有出现在 CRL 上。

NetScaler Gateway 支持以下两种 CRL 类型：

- 列出已吊销或不再有效的证书的 CRL
- 在线证书状态协议 (OSCP)，一种用于获取 X.509 证书吊销状态的互联网协议

要添加 **CRL**：

在 NetScaler Gateway 设备上配置 CRL 之前，请确保 CRL 文件存储在本地设备上。在高可用性设置的情况下，CRL 文件必须存在于两台 NetScaler Gateway 设备上，并且两台设备上该文件的目录路径必须相同。

如果需要刷新 CRL，可以使用以下参数：

- CRL 名称：要添加到 NetScaler 上的 CRL 的名称。最多 31 个字符。
- CRL 文件：要添加到 NetScaler 上的 CRL 文件的名称。默认情况下，NetScaler 会在 /var/netscaler/ssl 目录中查找 CRL 文件。最多 63 个字符。
- URL：最多 127 个字符
- 基本 DN：最多 127 个字符
- 绑定 DN：最多 127 个字符
- 密码：最多 31 个字符
- 天数：最多 31

1. 在配置实用程序中的配置选项卡上，展开 SSL，然后单击 CRL。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“添加 CRL”对话框中，为以下各项指定值：
    - CRL 名称
    - CRL 文件
    - 格式（可选）
    - CA 证书（可选）
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。在 CRL 详细信息窗格中，选择您配置的 CRL，然后验证屏幕底部显示的设置是否正确。

要在 **GUI** 中使用 **LDAP** 或 **HTTP** 配置 **CRL** 自动刷新，请执行以下操作：

CRL 由 CA 定期生成和发布，有时甚至在撤销特定证书后立即生成和发布。Citrix 建议您定期更新 NetScaler Gateway 设备上的 CRL，以防止客户端尝试使用无效证书进行连接。

NetScaler Gateway 设备可以从网站或 LDAP 目录刷新 CRL。当您指定刷新参数和 Web 位置或 LDAP 服务器时，在运行命令时，CRL 不必出现在本地硬盘驱动器上。第一次刷新将副本存储在本地硬盘驱动器上，位于 CRL File 参数指定的路径中。存储 CRL 的默认路径为 /var/netscaler/ssl。

CRL 刷新参数

- **CRL** 名称

  NetScaler Gateway 上正在刷新的 CRL 的名称。

- 启用 **CRL** 自动刷新

  启用或禁用 CRL 自动刷新。

- **CA Certificate**（CA 证书）

  签发 CRL 的 CA 的证书。必须在设备上安装此 CA 证书。NetScaler 只能从安装了证书的 CA 更新 CRL。

- **Method**（方法）

  用于从 Web 服务器 (HTTP) 或 LDAP 服务器获取 CRL 刷新的协议。可能的值：HTTP、LDAP。默认值：HTTP。

- **Scope**（范围）

  LDAP 服务器上的搜索操作范围。如果指定的范围为“
  基本”，则搜索将与基本 DN 处于同一级别。如果指定的范围为“
  一”，则搜索将扩展到基本 DN 以下的一个级别。

- 服务器 **IP**

  从中检索 CRL 的 LDAP 服务器的 IP 地址。选择 IPv6 以使用 IPv6 IP 地址。

- 端口

  LDAP 或 HTTP 服务器通信的端口号。

- **URL**

  从中检索 CRL 的网站的 URL。

- **Base DN**（基础 DN）

  LDAP 服务器用来搜索 CRL 属性的基本 DN。
  注意：Citrix 建议使用基本 DN 属性而不是 CA 证书中的颁发者名称在 LDAP 服务器中搜索 CRL。发行人名称字段可能与 LDAP 目录结构的 DN 不完全匹配。

- **Bind DN**（绑定 **DN**）

  bind DN 属性用于访问 LDAP 存储库中的 CRL 对象。绑定 DN 属性是 LDAP 服务器的管理员凭据。配置此参数以限制对 LDAP 服务器的未经授权的访问。

- 密码

  用于访问 LDAP 存储库中的 CRL 对象的管理员密码。如果限制对 LDAP 存储库的访问，即不允许匿名访问，则需要密码。

- **Interval**（时间间隔）

  必须执行 CRL 刷新的时间间隔。对于即时 CRL 刷新，请将间隔指定为 NOW。可能的值：每月、每日、每周、现在、无。

- 天数

  必须执行 CRL 刷新的那一天。如果间隔设置为 DAILY，则该选项不可用。

- **Time**（时间）

  必须执行 CRL 刷新的确切时间（24 小时格式）。

- 二进制

  将基于 LDAP 的 CRL 检索模式设置为二进制。可能的值：YES, NO。默认值：否。

1. 在导航窗格中，展开 SSL，然后单击 CRL。
2. 选择要为其更新刷新参数的已配置 CRL，然后单击“打开”。
3. 选择启用 CRL 自动刷新选项。
4. 在 CRL 自动刷新参数组中，为以下参数指定值：
   注意：星号 (*) 表示必填参数。
   - Method（方法）
   - 二进制
   - Scope（范围）
   - 服务器 IP
   - Port*（端口 *）
   - URL
   - 基本 DN*
   - Bind DN（绑定 DN）
   - 密码
   - Interval（时间间隔）
   - Days（日期）
   - Time（时间）
5. 单击创建。在 CRL 窗格中，选择您配置的 CRL，然后验证屏幕底部显示的设置是否正确。

使用 **OCSP** 监视证书状态

联机证书状态协议 (OCSP) 是一种 Internet 协议，用于确定客户端 SSL 证书的状态。NetScaler Gateway 支持 RFC 2560 中定义的 OCSP。与证书吊销列表 (CRL) 相比，OCSP 在及时信息方面具有显著优势。客户证书的最新吊销状态

在涉及大量资金和高值股票交易的交易中特别有用。它还使用更少的系统和网络资源。OCSP 的 NetScaler Gateway 实施包括请求批处理和响应缓存。

OCSP 的 **NetScaler Gateway** 实施

NetScaler Gateway 在 SSL 握手期间收到客户端证书时，NetScaler Gateway 设备上的 OCSP 验证开始。为了验证证书，NetScaler Gateway 会创建一个 OCSP 请求并将其转发给 OCSP 响应者。为此，NetScaler Gateway 要么从客户端证书中提取 OCSP 响应程序的 URL，要么使用本地配置的 URL。在 NetScaler Gateway 评估来自服务器的响应并确定是允许还是拒绝事务之前，事务处于挂起状态。如果来自服务器的响应延迟到配置的时间之后，并且没有配置其他响应程序，NetScaler Gateway 将允许该事务或显示错误，具体取决于您将 OCSP 检查设置为可选还是强制。NetScaler Gateway 支持批处理 OCSP 请求和缓存 OCSP 响应，以减少 OCSP 响应程序的负载并提供更快的响应。

OCSP 请求批处理

每次 NetScaler Gateway 收到客户端证书时，都会向 OCSP 响应程序发送请求。为了避免 OCSP 响应程序过载，NetScaler Gateway 可以在同一请求中查询多个客户端证书的状态。为了使请求批处理有效地工作，您需要定义一个超时时间，以便在等待形成批处理时不会延迟处理单个证书。

OCSP 响应缓存

缓存从 OCSP 响应程序收到的响应可以更快地响应用户，并减少 OCSP 响应程序的负载。从 OCSP 响应程序收到客户端证书的吊销状态后，NetScaler Gateway 会在本地缓存预定义的时间长度内的响应。在 SSL 握手期间收到客户端证书时，NetScaler Gateway 首先检查其本地缓存中是否有此证书的条目。如果找到仍然有效的条目（在缓存超时限内），则会对该条目进行评估，然后接受或拒绝客户端证书。如果找不到证书，NetScaler Gateway 会向 OCSP 响应程序发送请求，并在配置的时间长度内将响应存储在其本地缓存中。

配置 **OCSP** 证书状态

配置在线证书状态协议 (OCSP) 涉及添加 OCSP 响应程序、将 OCSP 响应程序绑定到证书颁发机构 (CA) 的签名证书，以及将证书和私钥绑定到安全套接字层 (SSL) 虚拟服务器。如果您需要将不同的证书和私钥绑定到已配置的 OCSP 响应程序，则需要先解除响应程序的绑定，然后将响应程序绑定到其他证书。

配置 **OCSP**

1. 在配置选项卡的导航窗格中，展开 SSL，然后单击 OCSP 响应程序。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“Name”（名称）中，键入配置文件的名称。

4. 在 URL 中，键入 OCSP 响应程序的 Web 地址。

   此字段是必填字段。Web 地址不能超过 32 个字符。

5. 要缓存 OCSP 响应，请单击缓存，然后在超时中键入 NetScaler Gateway 保存响应的分钟数。
6. 在请求批处理下，单击启用。
7. 在批处理延迟中，指定允许对一组 OCSP 请求进行批处理的时间（以毫秒为单位）。

   这些值可以介于 0 到 10000 之间。默认值为 1。

8. 在按时产生的偏差中，键入 NetScaler Gateway 在设备必须检查或接受响应时可以使用的时间量。
9. 如果要禁用 OCSP 响应程序的签名检查，请在“响应验证”下选择“信任响应”。

   如果启用信任响应，请跳过步骤 8 和步骤 9。

10. 在证书中，选择用于对 OCSP 响应进行签名的证书。

    如果未选择证书，则将使用 OCSP 响应程序绑定到的 CA 来验证响应。

11. 在请求超时中，键入等待 OCSP 响应的毫秒数。

    此时间包括批处理延迟时间。这些值可以介于 0 到 120000 之间。默认值为 2000。

12. 在签名证书中，选择用于签署 OCSP 请求的证书和私钥。如果不指定证书和私钥，则不会对请求进行签名。
13. 要启用一次使用的号码 (nonce)extension，请选择 Nonce。
14. 要使用客户端证书，请单击客户端证书插入。
15. 单击 Create（创建），然后单击 Close（关闭）。

管理 **NetScaler Gateway** 配置设置

February 1, 2024

对 NetScaler Gateway 进行配置更改时，这些更改将保存在日志文件中。您可以查看几种类型的配置设置：

- 已保存配置。您可以查看保存在 NetScaler Gateway 上的设置。
- 运行配置。您可以查看已配置但尚未保存为 NetScaler Gateway 的已保存配置的活动设置，例如虚拟服务器或身份验证策略。
- 正在运行与保存的配置。您可以在 NetScaler Gateway 上并排比较正在运行的配置和保存的配置。

您还可以清除 NetScaler Gateway 上的配置设置。

重要：如果选择清除 NetScaler Gateway 上的设置，则会删除证书、虚拟服务器和策略。Citrix 建议您不要清除配置。

保存 **NetScaler Gateway** 配置

您可以将 NetScaler Gateway 上的当前配置保存到网络中的计算机，查看当前运行配置，并比较保存的配置和正在运行的配置。

在 **NetScaler Gateway** 上保存配置

1. 在配置实用程序的详细信息窗格上方，单击保存图标，然后单击是。

在 **NetScaler Gateway** 上查看和保存配置文件

保存的配置是保存在 NetScaler Gateway 上日志文件中的设置，例如虚拟服务器、策略、IP 地址、用户、组和证书的设置。

在 NetScaler Gateway 上配置设置时，可以将设置保存到计算机上的文件中。如果需要重新安装 NetScaler Gateway 软件或意外删除了某些设置，则可以使用此文件还原配置。如果需要还原设置，可以将文件复制到 NetScaler Gateway，然后使用命令行界面或程序（如 WinSCP）重新启动设备，以将文件复制到 NetScaler Gateway。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格的查看配置下，单击已保存的配置。
3. 在“保存的配置”对话框中，单击“将输出文本保存到文件”，命名该文件，然后单击“保存”。
   注意：Citrix 建议使用文件名 ns.conf 保存文件。

查看当前运行配置

在未努力保存的情况下对 NetScaler Gateway 进行的任何更改都称为运行配置。这些设置在 NetScaler Gateway 上处于活动状态，但不会保存在设备上。如果配置了其他设置，例如策略、虚拟服务器、用户或组，则可以在运行配置中查看这些设置。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格的查看配置下，单击运行配置。

比较保存的配置和正在运行的配置

您可以查看设备上保存了哪些设置，并将这些设置与运行配置进行比较。您可以选择保存运行配置或更改配置。

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格的查看配置下，单击已保存的 v/s 正在运行。

清除 **NetScaler Gateway** 配置

您可以清除 NetScaler Gateway 上的配置设置。您可以从以下三个级别的设置中进行选择以清除：

重要：Citrix 建议在清除 NetScaler Gateway 配置设置之前保存配置。

- 基本。清除设备上的所有设置，但系统 IP 地址、默认网关、映射的 IP 地址、子网 IP 地址、DNS 设置、网络设置、高可用性设置、管理密码以及功能和模式设置除外。
- 已扩展。清除除系统 IP 地址、映射的 IP 地址、子网 IP 地址、DNS 设置和高可用性定义之外的所有设置。
- 已满。将配置恢复为原始出厂设置，但不包括维护与设备的网络连接所需的系统 IP (NSIP) 地址和默认路由。

清除全部或部分配置时，功能设置将设置为出厂默认设置。

清除配置时，不会删除存储在 NetScaler Gateway 上的文件，例如证书和许可证。文件 ns.conf 没有改变。如果要在清除配置之前保存配置，请先将配置保存到计算机中。如果保存配置，则可以在 NetScaler Gateway 上还原 ns.conf 文件。将文件还原到设备并重新启动 NetScaler Gateway 后，将还原 ns.conf 中的所有配置设置。

对配置文件（如 rc.conf）的修改不会恢复。

如果您有高可用性对，则两台 NetScaler Gateway 设备的修改方式相同。例如，如果清除一台设备上的基本配置，则更改将传播到第二台设备。

清除 **NetScaler Gateway** 配置设置

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”，然后单击“诊断”。
2. 在详细信息窗格的维护下，单击清除配置。
3. 在“配置级别”中，选择要清除的级别，然后单击“运行”。

NetScaler Gateway 上的证书管理

February 1, 2024

在 NetScaler Gateway 上，您可以使用证书创建安全连接和对用户进行身份验证。

要建立安全连接，在连接的一端需要有服务器证书，在连接的另一端需要颁发服务器证书的证书颁发机构 (CA) 的根证书。

- 服务器证书。服务器证书证明服务器的身份。NetScaler Gateway 需要这种类型的数字证书。
- 根证书。根证书用来识别为服务器证书签名的 CA。根证书属于证书颁发机构。用户设备需要这种类型的数字证书来验证服务器证书。

与用户设备上的 Web 浏览器建立安全连接时，服务器会将其证书发送到设备。

当用户设备收到服务器证书时，Web 浏览器（例如 Internet Explorer）会检查哪个 CA 颁发了证书，以及该 CA 是否受到用户设备的信任。如果 CA 不受信任，或者它是测试证书，Web 浏览器会提示用户接受或拒绝该证书（实际上是接受或拒绝访问站点的能力）。

NetScaler Gateway 支持以下三种类型的证书：

- 绑定到虚拟服务器的测试证书，也可用于连接到服务器场。NetScaler Gateway 随附预安装的测试证书。
- 由 CA 签名并与私钥配对的 PEM 或 DER 格式的证书。
- PKCS #12 格式的证书，用于存储或传输证书和私钥。PKCS #12 证书通常从现有的 Windows 证书作为 PFX 文件导出，然后安装在 NetScaler Gateway 上。

Citrix 建议使用由受信任的 CA（例如 Thawte 或 Verisign）签名的证书。

创建证书签名请求

February 1, 2024

要使用 SSL 或 TLS 提供安全通信，NetScaler Gateway 上需要服务器证书。在将证书上载到 NetScaler Gateway 之前，您需要生成证书签名请求 (CSR) 和私钥。您可以使用 NetScaler Gateway 向导中包含的创建证书请求或配置实用程序来创建 CSR。创建证书请求会创建一个.csr 文件，该文件通过电子邮件发送给证书颁发机构 (CA) 进行签名，并创建一个保留在设备上的私钥。CA 对证书进行签名，然后通过您提供的电子邮件地址将其退还给您。收到签名证书后，可以将其安装在 NetScaler Gateway 上。当您收到来自 CA 的证书时，您需要将证书与私钥配对。

重要：使用 NetScaler Gateway 向导创建 CSR 时，必须退出向导并等待 CA 向您发送签名证书。收到证书后，可以再次运行 NetScaler Gateway 向导以创建设置并安装证书。有关 NetScaler Gateway 向导的详细信息，请参阅使用 NetScaler Gateway 向导配置设置。

使用 **NetScaler Gateway** 向导创建 **CSR**

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的入门下，单击 **NetScaler Gateway** 向导。
3. 按照向导中的说明进行操作，直到进入“指定服务器证书”页面。
4. 单击 创建证书签名请求 并填写字段。
   注意：完全限定域名 (FQDN) 不必与 NetScaler Gateway 主机名相同。FQDN 用于用户登录。
5. 单击“创建”将证书保存在计算机上，然后单击“关闭”。
6. 在不保存设置的情况下退出 NetScaler Gateway 向导。

使用 **NetScaler GUI** 创建 **CSR**

您还可以使用 NetScaler GUI 创建 CSR，而无需运行 NetScaler Gateway 向导。

1. 导航到 流量 管理 > **SSL > SSL** 文件，然后选择创建证书签名请求 **(CSR)**。
2. 完成证书的设置，然后单击 创建。

创建证书和私钥后，通过电子邮件将证书发送给 CA，例如 Thawte 或 Verisign。

有关详细过程，请参阅 创建证书签名请求。

在 **NetScaler Gateway** 上安装签名证书

当您收到来自证书颁发机构 (CA) 的签名证书时，请将其与设备上的私钥配对，然后在 NetScaler Gateway 上安装该证书。

使用 **GUI** 将签名证书与私钥配对

1. 使用安全外壳 (SSH) 程序（例如 WinSCP）将证书复制到 NetScaler Gateway 到文件夹 nsconfig/ssl。
2. 在配置实用程序中的配置选项卡的导航窗格中，展开 **SSL >** 证书。
3. 在 **SSL** 证书 页面中，单击 开始使用。
4. 在详细信息窗格中，单击“安装”。
5. 在 **Certificate-Key Pair Name**（证书密钥对名称）中，键入证书的名称。
6. 在 证书文件名中，单击 装置。
7. 导航到证书，单击 选择，然后单击 打开。
8. 在 密钥文件名中，单击 装置。私钥的名称与证书签名请求 (CSR) 的名称相同。私钥位于 NetScaler Gateway 上\ nsconfig\ ssl 目录中。
9. 选择私钥，然后单击“打开”。
10. 如果证书是 PEM-format，请在“密码”中键入私钥的密码。
11. 如果要为证书到期时配置通知，请选择过 期时通知。
12. 在“通知期限”中，键入天数，单击“创建”，然后单击“关闭”。

使用 **GUI** 将证书和私钥绑定到虚拟服务器

创建并链接证书和私钥对后，将其绑定到虚拟服务器。

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在“证书”选项卡上的“可用”下，选择一个证书，单击“添加”，然后单击“确定”。

使用 **CLI** 将证书和私钥绑定到虚拟服务器

在命令提示窗口中，键入：


```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

示例：

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
<!--NeedCopy-->
```

注意：如果设备证书不需要 OCSP 检查，则 oscpCheck 是可选的。

使用 **GUI** 从虚拟服务器取消绑定测试证书

安装签名证书后，取消绑定到虚拟服务器的所有测试证书。您可以使用配置实用程序解绑测试证书。

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在“证书”选项卡上的“已配置”下，选择测试证书，然后单击“删除”。

配置中间证书

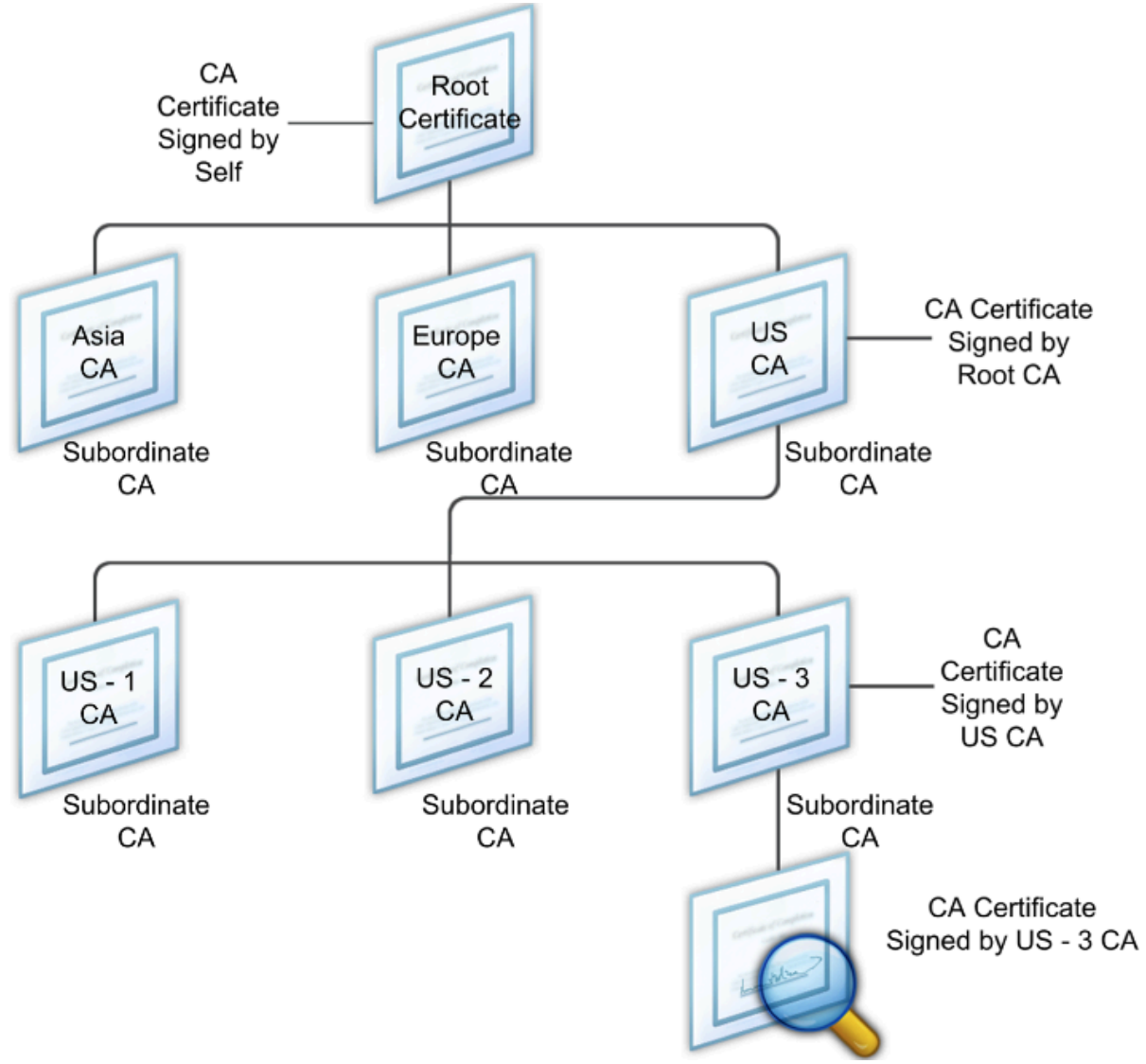
February 1, 2024

中间证书是介于 NetScaler Gateway（服务器证书）和根证书（安装在用户设备上）之间的证书。中间证书是链的一部分。

有些组织委派专人负责颁发证书，以解决各组织单位在地域上彼此独立的问题，或者对组织的不同部门应用不同的颁发策略。

可以通过设置从属证书颁发机构 (CA) 来委派颁发证书的责任。CA 可以签署自己的证书（即，它们是自签名的），也可以由其他证书颁发机构签名。X.509 标准包括一个用于设置 CA 层次结构的模型。在此模型中，如下图所示，根 CA 位于层次结构的顶部，是证书颁发机构的自签名证书。直属于根 CA 的 CA 具有由根证书颁发机构签名的 CA 证书。在层次结构中处于从属 CA 之下的 CA 拥有由从属 CA 签名的 CA 证书。

图 1. 展示典型数字证书链层次结构的 X.509 模型



如果服务器证书由具有自签名证书的 CA 签署，则证书链正好由两个证书组成：最终实体证书和根证书颁发机构。如果用户或服务器证书由中间证书颁发机构签名，则证书链会更长。

下图显示了前两个元素是最终实体证书（在本例中为 gwy01.company.com）和中间证书颁发机构的证书，按顺序排列。中间证书颁发机构的证书后跟其证书颁发机构的证书。此列表将一直持续到列表中的最后一个证书是针对根证书颁发机构的证书。证书链中的每个证书用来证实前一个证书的身份。

图 2. 典型的数字证书链

安装中间证书

1. 在配置实用程序的配置选项卡的导航窗格中，展开 SSL，然后单击证书。
2. 在详细信息窗格中，单击“安装”。
3. 在证书密钥对名称中，键入证书的名称。
4. 在详细信息下的证书文件名中，单击浏览（装置），然后在列表中选择本地或装置。
5. 导航到计算机（本地）或 NetScaler Gateway（设备）上的证书。
6. 在证书格式中，选择 PEM。
7. 单击“Install”（安装），然后单击“Close”（关闭）。

在 NetScaler Gateway 上安装中间证书时，无需指定私钥或密码。

在设备上安装证书后，证书需要链接到服务器证书。

将中间证书链接到服务器证书

1. 在配置实用程序的配置选项卡的导航窗格中，展开 SSL，然后单击证书。
2. 在详细信息窗格中，选择服务器证书，然后在操作中单击链接。
3. 在 CA 证书名称旁边，从列表中选择中间证书，然后单击确定。

使用设备证书进行身份验证

February 1, 2024

NetScaler Gateway 支持设备证书检查，可让您将设备身份绑定到证书的私钥。设备证书检查可以配置为经典或高级端点分析 (EPA) 策略的一部分。在传统的 EPA 策略中，只能为 EPA 预身份验证配置设备证书。

NetScaler Gateway 会在端点分析扫描运行之前或在登录页面出现之前验证设备证书。如果配置端点分析，端点扫描将运行以验证用户设备。当设备通过扫描且 NetScaler Gateway 验证设备证书后，用户可以登录 NetScaler Gateway。

> 重要提示：
>
> - 默认情况下，Windows 要求管理员权限才能访问设备证书。
> - 要为非管理员用户添加设备证书检查，必须安装 VPN 插件。VPN 插件版本必须与设备上的 EPA 插件版本相同。
> - 您可以向网关添加多个 CA 证书并验证设备证书。
> - 如果在 NetScaler Gateway 上安装两个或更多设备证书，则用户必须在开始登录 NetScaler Gateway 时或在端点分析扫描运行之前选择正确的证书。
> - 创建设备证书时，它必须是 X.509 证书。
> - 如果您有中间 CA 颁发的设备证书，则必须同时绑定中间 CA 证书和根 CA 证书。

> - EPA 客户端需要用户具有本地管理员权限才能访问计算机证书存储区。这种情况很少发生，因此解决方法是安装可以访问本地存储的完整 NetScaler Gateway 插件。

有关创建设备证书的详细信息，请参阅以下内容：

- Microsoft Web 站点上 Active Directory 证书服务 (AD CS) 中的网络设备注册服务 (NDES)。
- 如何使用 Apple 技术支持网站上的 DC/RPC 和 Active Directory 证书配置文件负载向 Microsoft 证书颁发机构申 请证书。
- 请访问目录服务团队 Microsoft 支持博客上的iPad/ iPhone 证书颁发。
- 在 Windows IT 专业版网站上设置网络设备注册服务 。
- Microsoft System Center Web 站点上的为 Configuration Manager 部署 PKI 证书的分步示例：Windows Server 2008 证书颁发机构。

配置设备证书的步骤

要配置设备证书，必须完成以下步骤：

- 在 NetScaler Gateway 上安装设备证书颁发者的证书颁发机构证书。有关详细信息，请参阅 在 NetScaler Gateway 上安装签名证书。
- 将设备证书颁发者的证书颁发机构证书绑定到 NetScaler Gateway 虚拟服务器并启用 OCSP 检查。有关详细信息，请参阅 在 NetScaler Gateway 上安装签名证书。
- 在设备证书颁发者的证书颁发机构证书上创建并绑定 OCSP（响应者）。有关详细信息，请参阅使用 OCSP 监视证书状态。

在虚拟服务器上启用设备证书检查，并将设备证书颁发者的证书颁发机构证书添加到设备证书清单中。有关详细信息，请参阅在虚拟服务器上启用设备证书检查以了解经典的 EPA

在 Windows 计算机上完成客户端配置和设备证书验证。有关详细信息，请参阅在 Windows 计算机上验证设备证书。

> 注意：
>
> 所有打算使用设备证书 EPA 检查的客户端都必须在计算机的系统证书存储区中安装设备证书。

在虚拟服务器上启用设备证书检查以获取经典 **EPA** 策略

创建设备证书后，可以使用 将现有证书导入和安装到 NetScaler Gateway 的过程在 NetScaler Gateway 上安装证书。

1. 在“配置”选项卡上，导航到 **NetScaler Gateway >** 虚拟服务器。
2. 在 **NetScaler Gateway** 虚拟服务器页面上，选择现有虚拟服务器，然后单击“编辑”。
3. 在 **VPN Virtual Servers**（VPN 虚拟服务器）页面的 **Basic Settings**（基本设置）部分下，单击 **Edit**（编辑）。

4. 清除 启用身份验证 框以禁用身份验证。
5. 选中 启用设备证书 框以启用设备证书
6. 单击 添加 将可用的设备证书颁发者的 CA 证书名称添加到列表中。
7. 要将 CA 证书绑定到虚拟服务器，请单击 设备证书的 **CA** 部分下的 **CA** 证书，单击 添加，选择证书，然后单击 **+**。

> 注意：
>
> 有关在虚拟服务器上启用和绑定设备证书以实现高级 EPA 策略的信息，请参阅 作为 EPA 组件的 nFactor 中的设备证书。

在 **Windows** 计算机上验证设备证书

1. 打开浏览器并访问 NetScaler Gateway FQDN。
2. 允许 Citrix 端点分析 (EPA) 客户端运行。如果尚未安装，请安装 EPA。

   Citrix EPA 会运行并验证设备证书，如果设备证书 EPA 检查通过，则重定向到身份验证页面，否则会将您重定向到 EPA 错误页面。如果您有其他 EPA 检查，则 EPA 扫描结果取决于配置的 EPA 检查。

要在客户端上进行进一步调试，请检查客户端上的以下 EPA 日志：
C:\Users<User name>\ AppData\ 本地\ Citrix\ AGEE\ nsepa.txt

注意：

> 不支持使用 CRL 进行设备证书验证。

导入并安装现有证书

February 1, 2024

您可以从运行 Internet 信息服务 (IIS) 的基于 Windows 的计算机或运行 Secure Gateway 的计算机导入现有证书。

导出证书时，请确保还导出了私钥。有时，您无法导出私钥，这意味着无法在 NetScaler Gateway 上安装证书。如果发生这种情况，请使用证书签名请求 (CSR) 创建证书。有关详细信息，请参阅 创建证书签名请求。

从 Windows 导出证书和私钥时，计算机会创建个人信息交换 (.pfx) 文件。然后，此文件将作为 PKCS #12 证书安装在 NetScaler Gateway 上。

如果要用 NetScaler Gateway 替换 Secure Gateway，则可以从 Secure Gateway 导出证书和私钥。如果要进行从 Secure Gateway 到 NetScaler Gateway 的就地迁移，则应用程序和设备上的完全限定域名 (FQDN) 必须相同。从 Secure Gateway 导出证书时，您会立即停用 Secure Gateway，在 NetScaler Gateway 上安装证书，然后测试配置。如果 Secure Gateway 和 NetScaler Gateway 具有相同的 FQDN，则它们不能同时在您的网络上运行。

如果您使用的是 Windows Server 2003 或 Windows Server 2008，则可以使用 Microsoft 管理控制台导出证书。有关详细信息，请参阅 Windows 联机帮助。

保留所有其他选项的默认值，定义密码，然后将.pfx 文件保存到计算机。导出证书后，然后将其安装在 NetScaler Gateway 上。

在 **NetScaler Gateway** 上安装证书和私钥

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格的“入门”下，单击 NetScaler Gateway 向导。
3. 单击“下一步”，选择现有虚拟服务器，然后单击“下一步”。
4. 在 证书选项中，选择 安装 **PKCS #12 (.pfx)** 文件 e。
5. 在 **PKCS #12** 文件名中，单击 浏览，导航到证书，然后单击 选择。
6. 在 ((密码)) 中，键入私钥的密码。

   这是将证书转换为 PEM 格式时使用的密码。
7. 单击 下一步 以完成 NetScaler Gateway 向导，而不更改任何其他设置。

在 NetScaler Gateway 上安装证书后，证书将显示在 **SSL\ >** 证书 节点的配置实用程序中。

创建私钥

1. 在配置实用程序的配置选项卡的导航窗格中，单击 **SSL**。
2. 在详细信息窗格中的 **SSL** 密钥下，单击创建 **RSA** 密钥。
3. 在密钥文件名中，键入私钥的名称或单击“浏览”导航到现有文件。
4. 在密钥大小 **(**位**)** 中，键入私钥的大小。
5. 在公共指数值中，选择 F4 或 3。

   RSA 密钥的公共指数值。这是密码算法的一部分，是创建 RSA 密钥所必需的。这些值为 F4（十六进制：0x10001）或 3（十六进制：0x3）。默认值为 F4。
6. 在密钥格式中，选择 PEM 或 DER。Citrix 建议将 PEM 格式用于证书。
7. 在 **PEM** 编码算法中，选择 DES 或 DES3。
8. 在 **PEM** 密码短语和验证密码短语中，键入密码，单击创建，然后单击关闭。

   注意：要分配密码短语，密钥格式必须为 PEM，并且必须选择编码算法。

要在配置实用程序中创建 DSA 私钥，请单击创建 **DSA** 密钥，然后按照创建 RSA 私钥所执行的步骤操作。

证书吊销列表

February 1, 2024

证书颁发机构 (CA) 有时会发出证书吊销列表 (CRL)。CRL 包含有关不再可信的证书的信息。例如，假设 Ann 离开了 XYZ 公司。公司可以将 Ann 的证书放在 CRL 上，以防止她使用该密钥签署消息。

同样，如果私钥已泄露或证书已过期且正在使用新证书，则可以撤销证书。在信任公钥之前，请确保证书没有出现在 CRL 上。

NetScaler Gateway 支持以下两种 CRL 类型：

- 列出已吊销或不再有效的证书的 CRL
- 在线证书状态协议 (OSCP)，一种用于获取 X.509 证书吊销状态的互联网协议

要添加 **CRL**：

在 NetScaler Gateway 设备上配置 CRL 之前，请确保 CRL 文件存储在本地设备上。在高可用性设置的情况下，CRL 文件必须存在于两台 NetScaler Gateway 设备上，并且两台设备上该文件的目录路径必须相同。

如果需要刷新 CRL，可以使用以下参数：

- CRL 名称：要添加到 NetScaler 上的 CRL 的名称。最多 31 个字符。
- CRL 文件：要添加到 NetScaler 上的 CRL 文件的名称。默认情况下，NetScaler 会在 /var/netscaler/ssl 目录中查找 CRL 文件。最多 63 个字符。
- URL：最多 127 个字符
- 基本 DN：最多 127 个字符
- 绑定 DN：最多 127 个字符
- 密码：最多 31 个字符
- 天数：最多 31

1. 在配置实用程序中的配置选项卡上，展开 SSL，然后单击 CRL。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“添加 CRL”对话框中，为以下各项指定值：
    - CRL 名称
    - CRL 文件
    - 格式（可选）
    - CA 证书（可选）
4. 单击 **Create**（创建），然后单击 **Close**（关闭）。在 CRL 详细信息窗格中，选择您配置的 CRL，然后验证屏幕底部显示的设置是否正确。

要在 **GUI** 中使用 **LDAP** 或 **HTTP** 配置 **CRL** 自动刷新，请执行以下操作：

CRL 由 CA 定期生成和发布，有时甚至在撤销特定证书后立即生成和发布。Citrix 建议您定期更新 NetScaler Gateway 设备上的 CRL，以防止客户端尝试使用无效证书进行连接。

NetScaler Gateway 设备可以从网站或 LDAP 目录刷新 CRL。当您指定刷新参数和 Web 位置或 LDAP 服务器时，在运行命令时，CRL 不必出现在本地硬盘驱动器上。第一次刷新将副本存储在本地硬盘驱动器上，位于 CRL File 参数指定的路径中。存储 CRL 的默认路径为 /var/netscaler/ssl。

CRL 刷新参数

- **CRL** 名称

  NetScaler Gateway 上正在刷新的 CRL 的名称。

- 启用 **CRL** 自动刷新

  启用或禁用 CRL 自动刷新。

- **CA Certificate**（CA 证书）

  签发 CRL 的 CA 的证书。必须在设备上安装此 CA 证书。NetScaler 只能从安装了证书的 CA 更新 CRL。

- **Method**（方法）

  用于从 Web 服务器 (HTTP) 或 LDAP 服务器获取 CRL 刷新的协议。可能的值：HTTP、LDAP。默认值：HTTP。

- **Scope**（范围）

  LDAP 服务器上的搜索操作范围。如果指定的范围为“
  基本”，则搜索将与基本 DN 处于同一级别。如果指定的范围为“
  一”，则搜索将扩展到基本 DN 以下的一个级别。

- 服务器 **IP**

  从中检索 CRL 的 LDAP 服务器的 IP 地址。选择 IPv6 以使用 IPv6 IP 地址。

- 端口

  LDAP 或 HTTP 服务器通信的端口号。

- **URL**

  从中检索 CRL 的网站的 URL。

- **Base DN**（基础 DN）

  LDAP 服务器用来搜索 CRL 属性的基本 DN。
  注意：Citrix 建议使用基本 DN 属性而不是 CA 证书中的颁发者名称在 LDAP 服务器中搜索 CRL。发行人名称字段可能与 LDAP 目录结构的 DN 不完全匹配。

- **Bind DN**（绑定 **DN**）

  bind DN 属性用于访问 LDAP 存储库中的 CRL 对象。绑定 DN 属性是 LDAP 服务器的管理员凭据。配置此参数以限制对 LDAP 服务器的未经授权的访问。

- 密码

  用于访问 LDAP 存储库中的 CRL 对象的管理员密码。如果限制对 LDAP 存储库的访问，即不允许匿名访问，则需要密码。

- **Interval**（时间间隔）

  必须执行 CRL 刷新的时间间隔。对于即时 CRL 刷新，请将间隔指定为 NOW。可能的值：每月、每日、每周、现在、无。

- 天数

  必须执行 CRL 刷新的那一天。如果间隔设置为 DAILY，则该选项不可用。

- **Time**（时间）

  必须执行 CRL 刷新的确切时间（24 小时格式）。

- 二进制

  将基于 LDAP 的 CRL 检索模式设置为二进制。可能的值：YES, NO。默认值：否。

1. 在导航窗格中，展开 SSL，然后单击 CRL。
2. 选择要为其更新刷新参数的已配置 CRL，然后单击“打开”。
3. 选择启用 CRL 自动刷新选项。
4. 在 CRL 自动刷新参数组中，为以下参数指定值：
   注意：星号 (*) 表示必填参数。
   - Method（方法）
   - 二进制
   - Scope（范围）
   - 服务器 IP
   - Port*（端口 *）
   - URL
   - 基本 DN*
   - Bind DN（绑定 DN）
   - 密码
   - Interval（时间间隔）
   - Days（日期）
   - Time（时间）
5. 单击创建。在 CRL 窗格中，选择您配置的 CRL，然后验证屏幕底部显示的设置是否正确。

使用 **OCSP** 监视证书状态

联机证书状态协议 (OCSP) 是一种 Internet 协议，用于确定客户端 SSL 证书的状态。NetScaler Gateway 支持 RFC 2560 中定义的 OCSP。与证书吊销列表 (CRL) 相比，OCSP 在及时信息方面具有显著优势。客户证书的最新吊销状态

在涉及大量资金和高值股票交易的交易中特别有用。它还使用更少的系统和网络资源。OCSP 的 NetScaler Gateway 实施包括请求批处理和响应缓存。

OCSP 的 **NetScaler Gateway** 实施

NetScaler Gateway 在 SSL 握手期间收到客户端证书时，NetScaler Gateway 设备上的 OCSP 验证开始。为了验证证书，NetScaler Gateway 会创建一个 OCSP 请求并将其转发给 OCSP 响应者。为此，NetScaler Gateway 要么从客户端证书中提取 OCSP 响应程序的 URL，要么使用本地配置的 URL。在 NetScaler Gateway 评估来自服务器的响应并确定是允许还是拒绝事务之前，事务处于挂起状态。如果来自服务器的响应延迟到配置的时间之后，并且没有配置其他响应程序，NetScaler Gateway 将允许该事务或显示错误，具体取决于您将 OCSP 检查设置为可选还是强制。NetScaler Gateway 支持批处理 OCSP 请求和缓存 OCSP 响应，以减少 OCSP 响应程序的负载并提供更快的响应。

OCSP 请求批处理

每次 NetScaler Gateway 收到客户端证书时，都会向 OCSP 响应程序发送请求。为了避免 OCSP 响应程序过载，NetScaler Gateway 可以在同一请求中查询多个客户端证书的状态。为了使请求批处理有效地工作，您需要定义一个超时时间，以便在等待形成批处理时不会延迟处理单个证书。

OCSP 响应缓存

缓存从 OCSP 响应程序收到的响应可以更快地响应用户，并减少 OCSP 响应程序的负载。从 OCSP 响应程序收到客户端证书的吊销状态后，NetScaler Gateway 会在本地缓存预定义的时间长度内的响应。在 SSL 握手期间收到客户端证书时，NetScaler Gateway 首先检查其本地缓存中是否有此证书的条目。如果找到仍然有效的条目（在缓存超时限内），则会对该条目进行评估，然后接受或拒绝客户端证书。如果找不到证书，NetScaler Gateway 会向 OCSP 响应程序发送请求，并在配置的时间长度内将响应存储在其本地缓存中。

配置 **OCSP** 证书状态

配置在线证书状态协议 (OCSP) 涉及添加 OCSP 响应程序、将 OCSP 响应程序绑定到证书颁发机构 (CA) 的签名证书，以及将证书和私钥绑定到安全套接字层 (SSL) 虚拟服务器。如果您需要将不同的证书和私钥绑定到已配置的 OCSP 响应程序，则需要先解除响应程序的绑定，然后将响应程序绑定到其他证书。

配置 **OCSP**

1. 在配置选项卡的导航窗格中，展开 SSL，然后单击 OCSP 响应程序。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“Name”（名称）中，键入配置文件的名称。

4. 在 URL 中，键入 OCSP 响应程序的 Web 地址。

   此字段是必填字段。Web 地址不能超过 32 个字符。

5. 要缓存 OCSP 响应，请单击缓存，然后在超时中键入 NetScaler Gateway 保存响应的分钟数。
6. 在请求批处理下，单击启用。
7. 在批处理延迟中，指定允许对一组 OCSP 请求进行批处理的时间（以毫秒为单位）。

   这些值可以介于 0 到 10000 之间。默认值为 1。

8. 在按时产生的偏差中，键入 NetScaler Gateway 在设备必须检查或接受响应时可以使用的时间量。
9. 如果要禁用 OCSP 响应程序的签名检查，请在“响应验证”下选择“信任响应”。

   如果启用信任响应，请跳过步骤 8 和步骤 9。

10. 在证书中，选择用于对 OCSP 响应进行签名的证书。

    如果未选择证书，则将使用 OCSP 响应程序绑定到的 CA 来验证响应。

11. 在请求超时中，键入等待 OCSP 响应的毫秒数。

    此时间包括批处理延迟时间。这些值可以介于 0 到 120000 之间。默认值为 2000。

12. 在签名证书中，选择用于签署 OCSP 请求的证书和私钥。如果不指定证书和私钥，则不会对请求进行签名。
13. 要启用一次使用的号码 (nonce)extension，请选择 Nonce。
14. 要使用客户端证书，请单击客户端证书插入。
15. 单击 Create（创建），然后单击 Close（关闭）。

测试您的 **NetScaler Gateway** 配置

February 1, 2024

在 NetScaler Gateway 上配置初始设置后，可以通过连接到设备来测试设置。

要测试 NetScaler Gateway 设置，请创建本地用户帐户。然后，使用虚拟服务器 IP 地址或设备的完全限定域名 (FQDN)，打开 Web 浏览器并键入 Web 地址。例如，在地址栏中，键入 `https://my.company.com` 或 `https://192.168.96.183`。

在登录屏幕上，输入您之前创建的用户帐户的用户名和密码。登录后，系统会提示您下载并安装 Citrix Secure Access 客户端。

安装并成功连接 Citrix Secure Access 客户端后，将出现访问接口。访问界面是 NetScaler Gateway 的默认主页。

使用 **GUI** 创建用户帐户

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway\ >** 用户管理，然后单击 **AAA** 用户。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在“User Name”（用户名）中，键入用户名。
4. 如果使用本地身份验证，请清除外部身份验证复选框。默认情况下，使用外部身份验证类型（例如 LDAP 或 RADIUS）对用户进行身份验证。如果清除此复选框，NetScaler Gateway 将对用户进行身份验证。
5. 在“Password”（密码）和“Confirm Password”（确认密码）中，键入用户的密码，单击“Create”（创建），然后单击“Close”（关闭）。

使用配置实用程序添加用户时，可以将以下策略绑定到用户：

- Authorization（授权）
- 流量、会话和审核
- 书签
- 内联网应用程序
- 内联网 IP 地址

如果使用测试用户帐户登录时遇到问题，请检查以下内容：

- 如果收到证书警告，则说明 NetScaler Gateway 上将安装测试证书或无效证书。如果设备上安装了由证书颁发机构 (CA) 签名的证书，请确保用户设备上有相应的根证书。
- 如果使用 CA 签名的证书，请验证是否使用签名证书签名请求 (CSR) 正确生成了站点证书，以及在 CSR 中输入的唯一判别名 (DN) 数据是否准确。问题也可能是主机名与签名证书上的 IP 地址不匹配。检查配置的证书的公用名是否与配置的虚拟服务器 IP 地址信息相对应。
- 如果没有出现登录屏幕或出现任何其他错误消息，请查看设置过程并确认您已正确执行所有步骤并准确输入了所有参数。

升级 **NetScaler Gateway** 软件

February 1, 2024

当有新版本可用时，您可以升级驻留在 NetScaler Gateway 上的软件。您可以在 Citrix Web 站点上检查更新。只有在发布更新时 NetScaler Gateway 许可证处于 Subscription Advantage 计划下时，才能升级到新版本。您可以随时续 Subscription Advantage。有关更多信息，请参阅 NetScaler 支持网站。

Citrix 升级指南中还提供了升级路径和兼容产品信息。

有关最新 NetScaler Gateway 维护版本的信息，请参阅 Citrix 知识中心。

检查软件更新

1. 访问 Citrix Web 站点。
2. 单击我的帐户并登录。
3. 单击下载。
4. 在“查找下载”下，选择 **NetScaler Gateway**。
5. 在 **Select Download Type**（选择下载类型）中，选择 **Product Software**（产品软件），然后单击 **Find**（查找）。
   您还可以选择 虚拟设备 以下载 NetScaler VPX。选择此选项时，将显示适用于每个虚拟机管理程序所对应的虚拟机的软件列表。
6. 在 NetScaler Gateway 页面上，展开 **NetScaler** 网关或访问网关。
7. 单击要下载的设备软件版本。
8. 在要下载的版本的设备软件页面上，选择虚拟设备，然后单击 下载。
9. 按照屏幕上的说明下载软件。

将软件下载到计算机后，可以使用升级向导或命令提示符安装软件。

使用升级向导升级 NetScaler Gateway

1. 在配置实用程序的 配置选项卡的导航窗格中，单击系统。
2. 在详细信息窗格中，单击 升级向导。
3. 单击 **Next**（下一步），然后按照向导中的说明执行操作。

使用命令提示符升级 NetScaler Gateway

1. 要将软件上载到 NetScaler Gateway，请使用安全的 FTP 客户端（如 WinSCP）连接到设备。
2. 将软件从计算机复制到设备上的 /var/`nsinstall` 目录。
3. 使用安全外壳 (SSH) 客户端（如 PuTTY）打开与设备的 SSH 连接。
4. 登录 NetScaler Gateway。
5. 在命令提示符处，键入：`shell`
6. 要切换到目 `nsinstall` 录，请在命令提示符处键入：`cd /var/nsinstall`
7. 要查看目录的内容，请键入：`ls`
8. 要解压软件，请键入：tar -xvzf build_X_XX.tgz,，其中 build_X_XX.tgz 是要升级到的版本的名称。
9. 要开始安装，请在命令提示符处键入：`./installns`
10. 安装完成后，重新启动 NetScaler Gateway。

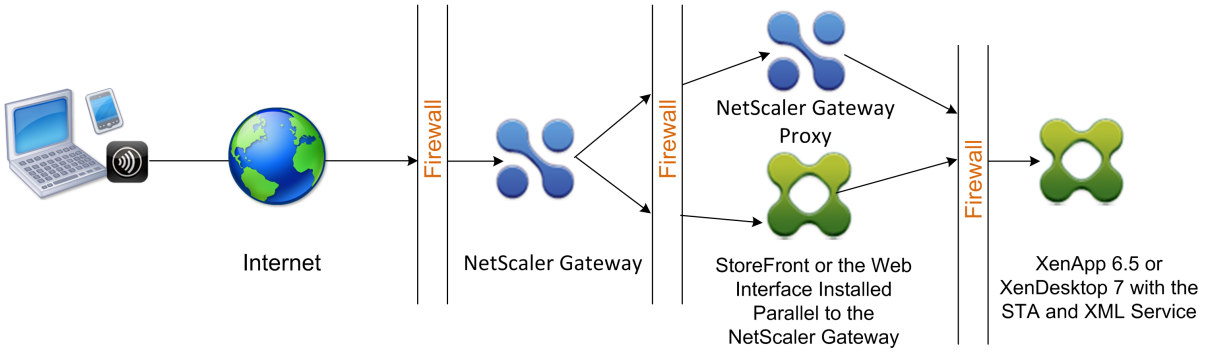
NetScaler Gateway 重新启动后，要验证安装是否成功，请启动配置实用程序。设备上的 NetScaler Gateway 版本显示在右上角。

在双跃点 DMZ 中部署 NetScaler Gateway

February 1, 2024

部分组织使用三个防火墙来保护其内部网络。这三个防火墙将 DMZ 划分为两个阶段以提供额外的安全层供内部网络使用。此网络配置称为双跃点 DMZ。

图 1. 在双跃点 DMZ 中部署的 NetScaler Gateway 设备



> 注意：
>
> 为了说明起见，上面的示例描述了将三个防火墙与 StoreFront、Web Interface 和 Citrix Virtual Apps 结合使用的双跃点配置。但是，您也可以使用双跃点 DMZ，其中一台设备位于 DMZ 中，另一台设备位于安全网络中。如果在 DMZ 中配置一台设备，在安全网络中配置一台设备的双跃点配置，则可以忽略在第三个防火墙上打开端口的说明。

您可以配置双跃点 DMZ 以支持 Citrix StoreFront 或与 NetScaler Gateway 代理并行安装的 Web Interface。用户使用 Citrix Workspace 应用程序连接。

> 注意：
>
> 如果使用 StoreFront 在双跃点 DMZ 中部署 NetScaler Gateway，适用于 Citrix Workspace 应用程序的基于电子邮件的自动发现将无法正常工作

Double-Hop 部署的工作原理

您可以在双跃点 DMZ 中部署 NetScaler Gateway 设备，以控制对运行 Citrix Virtual Apps 的服务器的访问。双跃点部署中的连接如下所示：

- 用户通过使用 Web 浏览器和 Citrix Workspace 应用程序选择已发布的应用程序，在第一个 DMZ 中连接到 NetScaler Gateway。
- Citrix Workspace 应用程序将在用户设备上启动。用户连接到 NetScaler Gateway 以访问安全网络中服务器场中运行的已发布应用程序。

注意：双跃点 DMZ 部署不支持 Secure Hub 和适用于 Windows 的 Citrix Secure Access 客户端。只有 Citrix Workspace 应用程序用于用户连接。

- 第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。
- 第二个 DMZ 中的 NetScaler Gateway 用作 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。第一个 DMZ 中的 NetScaler Gateway 与内部网络中的安全票证颁发机构 (STA) 之间的通信也可通过第二个 DMZ 中的 NetScaler Gateway 进行代理。

NetScaler Gateway 支持 IPv4 和 IPv6 连接。您可以使用配置实用程序配置 IPv6 地址。

下表建议了对各种 ICA 功能的双跃点部署支持：

ICA 功能	双跃点支持
SmartAccess	是
SmartControl	是
Enlightened Data Transport (EDT)	是
HDX Insight	是
ICA 会话可靠性（端口 2598）	是
ICA 会话迁移	是
ICA 会话超时	是
多流 ICA	是（仅限 TCP）
Framehawk	否
UDP 音频	否

为双跃点 **DMZ** 部署做好准备

配置双跃点 DMZ 部署时，必须回答以下问题：

- 我想支持负载平衡吗?
- 我应该在防火墙上打开哪些端口?
- 我需要多少个 SSL 证书?
- 在开始部署之前，我需要哪些组件?

本节中的主题包含的信息可帮助您根据自己的环境回答这些问题。

开始部署所需的组件

在开始双跃点 DMZ 部署之前，请确保您具有以下组件：

- 必须至少有两个 NetScaler Gateway 设备可用（每个 DMZ 一个）。
- 运行 Citrix Virtual Apps 的服务器必须安装并在内部网络中运行。
- Web Interface 或 StoreFront 必须安装在第二个 DMZ 中，并配置为与内部网络中的服务器场一起运行。
- 在第一个 DMZ 中，NetScaler Gateway 上必须至少安装一个 SSL 服务器证书。此证书可确保 Web 浏览器和用户与 NetScaler Gateway 的连接已加密。

  如果要加密双跃点 DMZ 部署中其他组件之间发生的连接，则需要额外的证书。

双跃点 **DMZ** 部署中的通信流

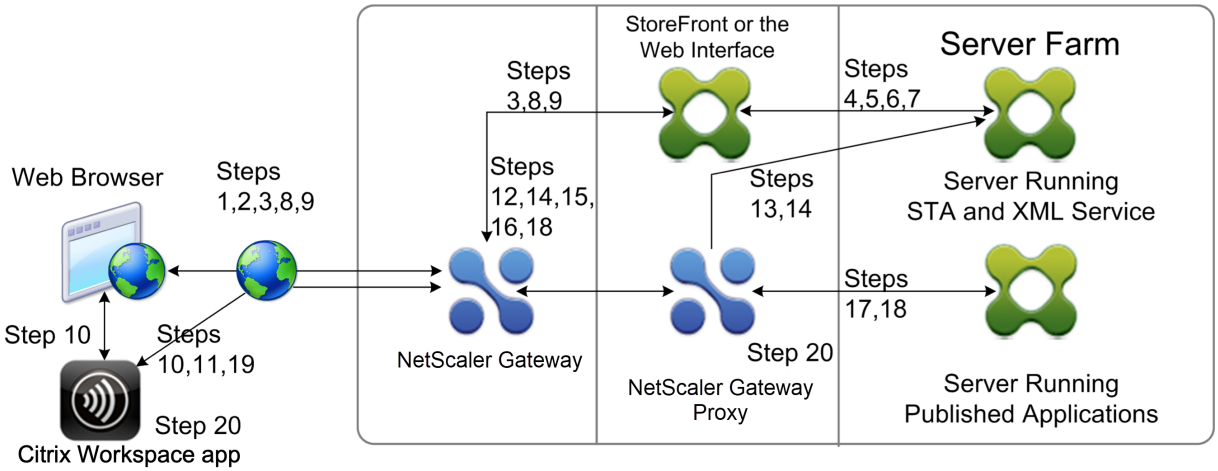
February 1, 2024

要了解双跃点 DMZ 部署中涉及的配置问题，您必须对双跃点 DMZ 部署中的各种 NetScaler Gateway 和 Citrix Virtual Apps 组件如何通信以支持用户连接有基本的了解。StoreFront 和 Web Interface 的连接过程是相同的。

尽管用户连接过程在一个连续的流程中进行，但该过程涉及以下高级步骤。

- 验证用户身份
- 创建会话票证
- 启动 Citrix Workspace 应用程序
- 完成连接

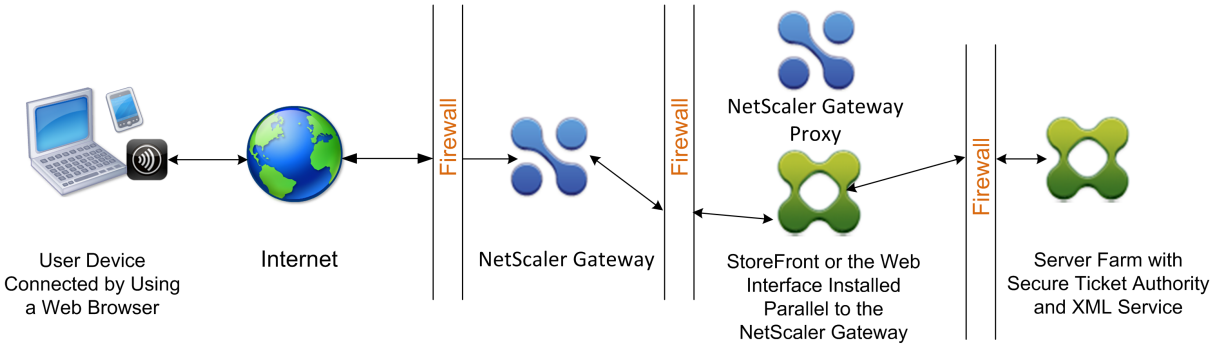
下图显示了在用户连接到 StoreFront 或 Web Interface 的过程中发生的步骤。在安全网络中，运行 Citrix Virtual Apps 的计算机也在运行 Secure Ticket Authority (STA)、XML 服务和已发布的应用程序。



连接过程

在双跃点 **DMZ** 部署中，对用户进行身份验证是用户连接过程的第一步。

下图显示了此部署中的用户连接过程。



在用户身份验证阶段，将发生以下基本过程：

1. 用户在第一个 DMZ 中输入 NetScaler Gateway 的地址，例如 https://www.ng.wxyco.com 在 Web 浏览器中连接到 NetScaler Gateway。如果在 NetScaler Gateway 上启用了登录页面身份验证，NetScaler Gateway 将对用户进行身份验
2. 第一个 DMZ 中的 NetScaler Gateway 会收到请求。
3. NetScaler Gateway 会将 Web 浏览器连接重定向到 Web Interface。
4. Web Interface 会将用户凭据发送到在内部网络的服务器场中运行的 Citrix XML 服务。
5. Citrix XML 服务会对用户进行身份验证。
6. XML 服务创建用户有权访问的已发布应用程序的列表，并将此列表发送到 Web Interface。

   注意：

   - 如果在 NetScaler Gateway 上启用身份验证，则设备会向用户发送 NetScaler Gateway 登录页面。用户在登录页面上输入身份验证凭据，设备将对用户进行身份验证。然后，NetScaler Gateway 将用户凭据返回到 Web Interface。
   - 如果未启用身份验证，NetScaler Gateway 将不会执行身份验证。设备连接到 Web Interface，检索 Web Interface 登录页面，然后将 Web Interface 登录页发送给用户。用户在 Web Interface 登录页面上输入身份验证凭据，NetScaler Gateway 将用户凭据传回 Web Interface。

   创建会话票证是双跃点 **DMZ** 部署中用户连接过程的第二阶段。

   在会话票证创建阶段，将执行以下基本过程：

7. Web Interface 与内部网络中的 XML 服务和 Secure Ticket Authority (STA) 进行通信，为用户有权访问的每个已发布应用程序生成会话票证。会话票证包含运行托管已发布应用程序的 Citrix Virtual Apps 的计算机的别名地址。

8. STA 保存托管已发布应用程序的服务器的 IP 地址。然后 STA 将请求的会话票证发送到 Web Interface。每个会话票证都包含一个别名，该别名表示托管已发布应用程序的服务器的 IP 地址，但不是实际的 IP 地址。
9. Web Interface 会为每个已发布的应用程序生成一个 ICA 文件。ICA 文件包含 STA 签发的票证。然后，Web Interface 会创建一个网页，并使用指向已发布应用程序的链接列表填充网页，然后将此网页发送到用户设备上的 Web 浏览器。

   启动 Citrix Workspace 应用程序是双跃点 DMZ 部署中用户连接过程的第三阶段。基本过程如下：
10. 用户在 Web Interface 中单击指向已发布应用程序的链接。Web Interface 会将该已发布应用程序的 ICA 文件发送到用户设备的浏览器。

    ICA 文件包含指示 Web 浏览器启动 Receiver 的数据。

    ICA 文件还包含第一个 DMZ 中 NetScaler Gateway 的完全限定域名 (FQDN) 或域名系统 (DNS) 名称。
11. Web 浏览器启动 Receiver，用户通过使用 ICA 文件中的 NetScaler Gateway 名称在第一个 DMZ 中连接到 NetScaler Gateway。进行初始 SSL/TLS 握手是为了建立运行 NetScaler Gateway 的服务器的身份。

    在双跃点 **DMZ** 部署中，完成连接是用户连接过程的第四个也是最后一个阶段。

    在连接完成阶段，将发生以下基本过程：

    - 用户在 Web Interface 中单击指向已发布应用程序的链接。
    - Web 浏览器接收由 Web Interface 生成的 ICA 文件并启动 Citrix Workspace 应用程序。
      注意：ICA 文件包含指示 Web 浏览器启动 Citrix Workspace 应用程序的代码。
    - Citrix Workspace 应用程序在第一个 DMZ 中启动与 NetScaler Gateway 的 ICA 连接。
    - 第一个 DMZ 中的 NetScaler Gateway 与内部网络中的 Secure Ticket Authority (STA) 进行通信，以将会话票证中的别名地址解析为运行 Citrix Virtual Apps 或 StoreFront 的计算机的真实 IP 地址。此通信由 NetScaler Gateway 代理通过第二个 DMZ 进行代理。
    - 第一个 DMZ 中的 NetScaler Gateway 完成了与 Citrix Workspace 应用程序的 ICA 连接。
    - Citrix Workspace 应用程序现在可以通过两个 NetScaler Gateway 设备与内部网络上运行 Citrix Virtual Apps 的计算机进行通信

    完成用户连接过程的详细步骤如下：
12. Citrix Workspace 应用程序将已发布应用程序的 STA 票证发送到第一个 DMZ 中的 NetScaler Gateway。
13. 第一个 DMZ 中的 NetScaler Gateway 与内部网络中的 STA 联系以进行票证验证。要联系 STA，NetScaler Gateway 会在第二个 DMZ 中建立与 NetScaler Gateway 代理的 SSL 连接的 SOCKS 或 SOCKS。
14. 第二个 DMZ 中的 NetScaler Gateway 代理将票证验证请求传递给内部网络中的 STA。STA 会验证票证并将其映射到运行 Citrix Virtual Apps 的托管已发布应用程序的计算机。
15. STA 向第二个 DMZ 中的 NetScaler Gateway 代理发送响应，该响应将在第一个 DMZ 中传递给 NetScaler Gateway。此响应将完成票证验证，并包含托管已发布应用程序的计算机的 IP 地址。
16. 第一个 DMZ 中的 NetScaler Gateway 将 Citrix Virtual Apps 用服务器的地址合并到用户连接数据包中，然后将此数据包发送到第二个 DMZ 中的 NetScaler Gateway 代理。

17. 第二个 DMZ 中的 NetScaler Gateway 代理向连接数据包中指定的服务器发出连接请求。
18. 服务器在第二个 DMZ 中响应 NetScaler Gateway 代理。第二个 DMZ 中的 NetScaler Gateway 代理将此响应传递给第一个 DMZ 中的 NetScaler Gateway，以在第一个 DMZ 中完成服务器与 NetScaler Gateway 之间的连接。
19. 第一个 DMZ 中的 NetScaler Gateway 通过将最终连接数据包传递到用户设备来完成与用户设备的 SSL/TLS 握手。从用户设备到服务器的连接已建立。
20. ICA 流量在用户设备和服务器之间通过第一个 DMZ 中的 NetScaler Gateway 和第二个 DMZ 中的 NetScaler Gateway 代理在用户设备和服务器之间流动。

在双跃点 **DMZ** 中安装和配置 **NetScaler Gateway**

February 1, 2024

您需要完成几个步骤才能在双跃点 DMZ 中部署 NetScaler Gateway。这些步骤包括在两个 DMZ 中安装装置，以及为用户设备连接配置装置。

在第一个 **DMZ** 中安装 **NetScaler Gateway**

要在第一个 DMZ 中安装 NetScaler Gateway，请按照 安装硬件中的说明进行操作。

如果要在第一个 DMZ 中安装多个 NetScaler Gateway 设备，则可以在负载平衡器后面部署这些设备。

在第一个 **DMZ** 中配置 **NetScaler Gateway**

在双跃点 DMZ 部署中，必须将第一个 DMZ 中的每个 NetScaler Gateway 配置为将连接重定向到第二个 DMZ 中的 StoreFront 或 Web Interface。

重定向到 StoreFront 或 Web Interface 是在 NetScaler Gateway 全局或虚拟服务器级别执行的。要通过 NetScaler Gateway 连接到 Web Interface，用户必须与启用了重定向到 Web Interface 的 NetScaler Gateway 用户组关联。

在第二个 **DMZ** 中安装 **NetScaler Gateway**

第二个 DMZ 中的 NetScaler Gateway 设备称为 NetScaler Gateway 代理，因为它在第二个 DMZ 中代理 ICA 和 Secure Ticket Authority (STA) 流量。
安装硬件 以在第二个 DMZ 中安装每台 NetScaler Gateway 设备。

您可以使用此安装过程在第二个 DMZ 中安装其他设备。

在第二个 DMZ 中安装 NetScaler Gateway 设备后，可以配置以下设置：

- 在 NetScaler Gateway 代理上配置虚拟服务器。
- 在第一个和第二个 DMZ 中配置 NetScaler Gateway 设备以相互通信。
- 将第二个 DMZ 中的 NetScaler Gateway 全局绑定或绑定到虚拟服务器。
- 在第一个 DMZ 中的设备上配置 STA。
- 打开用于分隔 DMZ 的防火墙中的端口。
- 在设备上安装证书。

在 **NetScaler Gateway** 代理上的虚拟服务器上配置设置

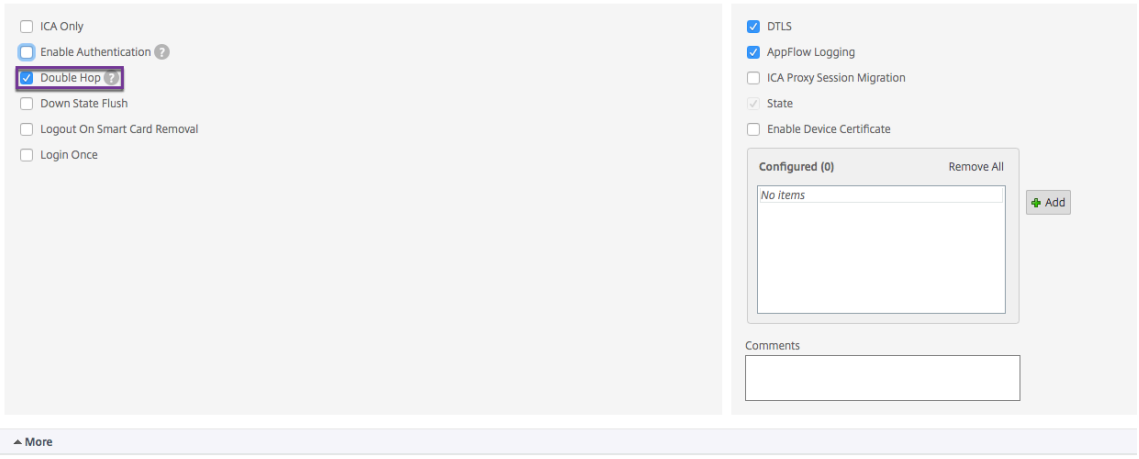
February 1, 2024

要允许在 NetScaler Gateway 设备之间传递连接，请在 NetScaler Gateway 代理上的虚拟服务器中启用双跃点。

用户连接时，NetScaler Gateway 设备会对用户进行身份验证，然后代理与代理设备的连接。在第一个 DMZ 的 NetScaler Gateway 上，将虚拟服务器配置为在第二个 DMZ 中与 NetScaler Gateway 进行通信。请勿在 NetScaler Gateway 代理上配置身份验证或策略。Citrix 建议在虚拟服务器上禁用身份验证。

使用 **GUI** 在 **NetScaler Gateway** 代理上的虚拟服务器上启用双跃点

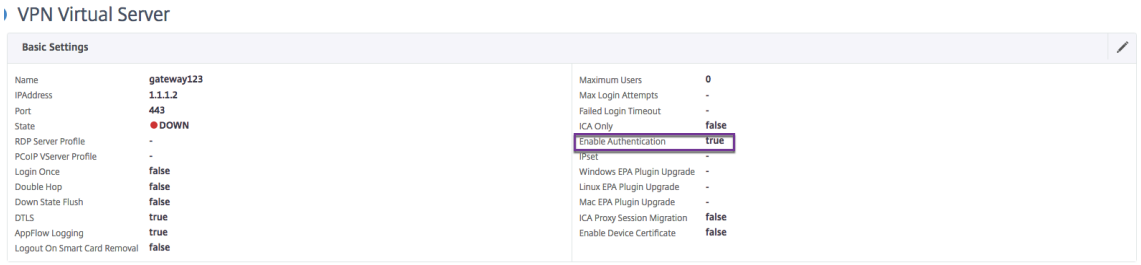
1. 导航到 **Configuration**（配置）**> NetScaler Gateway > Virtual Servers**（虚拟服务器）。
2. 选择虚拟服务器，然后单击 **Edit**（编辑）。
3. 在“基本设置”部分中，单击“编辑”图标，然后单击“更多”。
4. 选择“双跃点”。



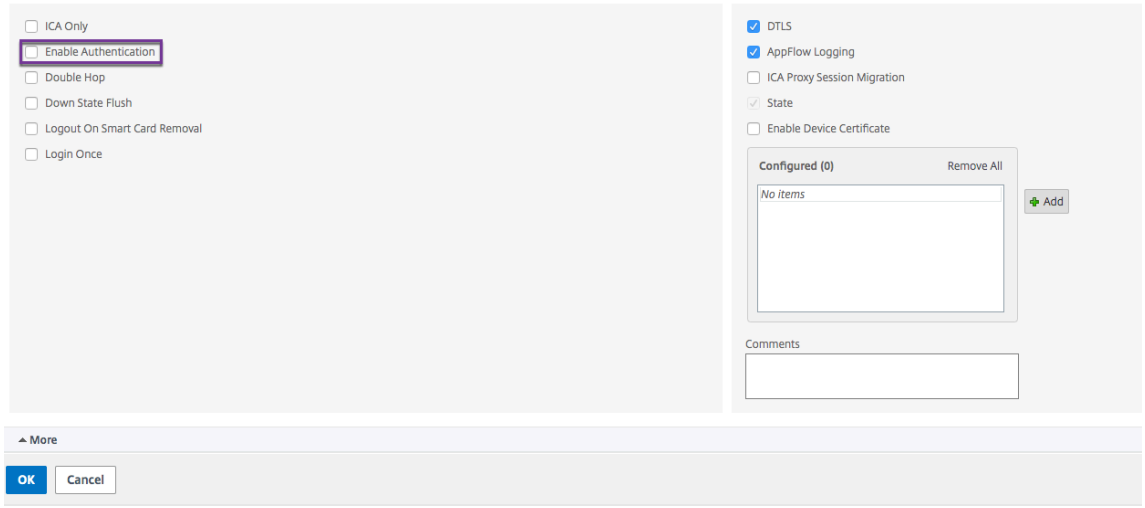
5. 单击确定。

使用 **GUI** 在 **NetScaler Gateway** 代理上的虚拟服务器上禁用身份验证

1. 导航到 **Configuration**（配置）**> NetScaler Gateway > Virtual Servers**（虚拟服务器）。
2. 选择虚拟服务器，然后单击 **Edit**（编辑）。
3. 在“基本设置”部分中，单击“编辑”图标，然后单击“更多”。



4. 清除 启用身份验证 复选框。



5. 单击确定。

将设备配置为与设备代理通信

February 1, 2024

在双跃点 DMZ 中部署 NetScaler Gateway 时，必须在第一个 DMZ 中配置 NetScaler Gateway，以便与第二个 DMZ 中的 NetScaler Gateway 代理进行通信。

如果在第二个 DMZ 中部署多个设备，则需要将第一个 DMZ 中的每个设备配置为与第二个 DMZ 中的每个代理设备进行通信。

注意：如果要使用 IPv6，可以使用配置实用程序配置下一跳服务器。为此，请展开
NetScaler Gateway > 资源，然后单击

下一跳服务器。按照以下过程中的步骤操作，然后选中
IPv6 复选框。

将 **NetScaler Gateway** 配置为与 **NetScaler Gateway** 代理进行通信

1. 在配置实用程序中的“配置”选项卡上，展开 NetScaler Gateway > 资源，然后单击“下一跳服务器”。
2. 在详细信息窗格中，单击 Add（添加）。
3. 在名称中，键入第一个 NetScaler Gateway 的名称。
4. 在 IP 地址中，键入第二个 DMZ 中 NetScaler Gateway 代理的虚拟服务器 IP 地址。
5. 在端口中，键入端口号，单击创建，然后单击关闭。如果您使用的是安全端口，例如 443，请选择 Secure。

必须将第一个 DMZ 中安装的每个 NetScaler Gateway 配置为与第二个 DMZ 中安装的所有 NetScaler Gateway 代理设备进行通信。

为 NetScaler Gateway 代理配置设置后，将策略绑定到 NetScaler Gateway Global 中的下一跳服务器或虚拟服务器。

在全局范围内绑定 **NetScaler Gateway** 下一跳服务器

1. 在配置实用程序中的“配置”选项卡上，展开 NetScaler Gateway > 资源，然后单击“下一跳服务器”。
2. 在详细信息窗格中，选择下一跳服务器，然后在操作中选择全局绑定。
3. 在“配置下一跳服务器全局绑定”对话框的“下一跳服务器名称”中，选择代理设备，然后单击“确定”。

将 **NetScaler Gateway** 下一跳服务器绑定到虚拟服务器

1. 在配置实用程序中的配置选项卡上，展开 NetScaler Gateway，然后单击虚拟服务器。
2. 在详细信息窗格中，选择虚拟服务器，然后单击“打开”。
3. 在“已发布的应用程序”选项卡上的“下一跳服务器”下，单击某个项目，然后单击

您还可以从“已发布的应用程序”选项卡添加下一跳服务器。

配置 **NetScaler Gateway** 以处理 **STA** 和 **ICA** 流量

February 1, 2024

在双跃点 DMZ 中部署 NetScaler Gateway 时，必须在第一个 DMZ 中配置 NetScaler Gateway，以适当地处理与 Secure Ticket Authority (STA) 和 ICA 流量的通信。运行 STA 的服务器可以全局绑定，也可以绑定到虚拟服务器。

配置 STA 后，您可以将 STA 全局绑定，也可以绑定到虚拟服务器。

要全局配置和绑定 STA：

1. 在 GUI 中的“配置”选项卡上，展开 **NetScaler Gateway** ，然后单击“全局设置”。
2. 在详细信息窗格的“服务器”下，单击绑定/取消绑定将由 **Secure Ticket Authority** 使用的 **STA** 服务器。
3. 在“绑定 /取消绑定 **STA** 服务器”对话框中，单击“添加”。
4. 在“配置 **STA** 服务器”对话框 的 **URL** 中，键入运行 STA 的服务器的路径，例如 http://mycompany.com 或 http://ipAddress，然后单击“创建”。

要配置 STA 并将其绑定到虚拟服务器：

1. 在 GUI 中的“配置”选项卡上，展开 **NetScaler Gateway** ，然后单击“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“打开”。
3. 在“已发布的应用程序”选项卡上的 **Secure Ticket Authority** 下，单击“添加”。
4. 在“配置 **STA** 服务器”对话框的 URL 中，键入运行 STA 的服务器的路径，例如 http://mycompany.com 或 http://ipAddress，然后单击“创建”。

注意：

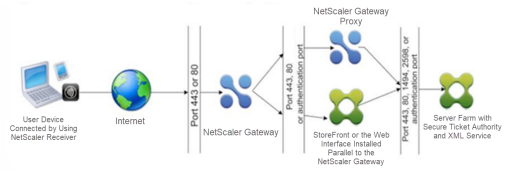
如果 VPN 虚拟服务器共享相同的下一跃点虚拟服务器和 STA 服务器，则当公用 STA 服务器与共享同一下一跃点虚拟服务器的虚拟服务器解除绑定时，连接将被重置。

打开防火墙上的相应端口

February 1, 2024

必须确保在防火墙上打开适当的端口，以支持双跃点 DMZ 部署中涉及的各种组件之间发生的不同连接。有关连接过程的详细信息，请参阅 双跃点 DMZ 部署中的通信流。

下图显示了可在双跃点 DMZ 部署中使用的常见端口。



下表显示了通过第一个防火墙发生的连接以及为支持这些连接而必须打开的端口。

通过第一个防火墙的连接	使用的端口
来自互联网的 Web 浏览器在第一个 DMZ 中连接到 NetScaler Gateway。注意： NetScaler Gateway 包含一个选项，可将在端口 80 上建立的连接重定向到安全端口。如果在 NetScaler Gateway 上启用此选项，则可以通过第一个防火墙打开端口 80。当用户在端口 80 上与 NetScaler Gateway 建立未加密的连接时，NetScaler Gateway 会自动将连接重定向到安全端口。	通过第一个防火墙打开 TCP 端口 443。
来自互联网的 Citrix Workspace 应用程序在第一个 DMZ 中连接到 NetScaler Gateway。	通过第一个防火墙打开 TCP 端口 443。

下表显示了通过第二个防火墙发生的连接以及为支持这些连接而必须打开的端口。

通过第二个防火墙的连接	使用的端口
第一个 DMZ 中的 NetScaler Gateway 连接到第二个 DMZ 中的 Web Interface。	打开 TCP 端口 80 以建立不安全的连接，或打开 TCP 端口 443 以通过第二个防火墙进行安全连接。
第一个 DMZ 中的 NetScaler Gateway 在第二个 DMZ 中连接到 NetScaler Gateway。	打开 TCP 端口 443，通过第二个防火墙建立安全的 SOCKS 连接。
如果您在第一个 DMZ 中的 NetScaler Gateway 上启用了身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。示例包括用于 RADIUS 的端口 1812 和用于 LDAP 的端口 389。

下表显示了通过第三个防火墙发生的连接以及为支持这些连接而必须打开的端口。

通过第三个防火墙的连接	使用的端口
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的 XML 服务。	打开端口 80 进行不安全的连接，或打开端口 443 以通过第三个防火墙进行安全连接。
StoreFront 或第二个 DMZ 中的 Web Interface 连接到内部网络中服务器上托管的 Secure Ticket Authority (STA)。	打开端口 80 进行不安全的连接，或打开端口 443 以通过第三个防火墙进行安全连接。
第二个 DMZ 中的 NetScaler Gateway 连接到驻留在安全网络中的 STA。	打开端口 80 进行不安全的连接，或打开端口 443 以通过第三个防火墙进行安全连接。
第二个 DMZ 中的 NetScaler Gateway 与内部网络中服务器上的已发布应用程序或虚拟桌面建立 ICA 连接。	打开 TCP 端口 1494 以支持通过第三个防火墙的 ICA 连接。如果在 Citrix Virtual Apps 上启用了会话可靠性，请打开 TCP 端口 2598 而不是 1494。

通过第三个防火墙的连接	使用的端口
如果您在第一个 DMZ 中的 NetScaler Gateway 上启用了身份验证，则此设备可能需要连接到内部网络中的身份验证服务器。	打开身份验证服务器侦听连接的 TCP 端口。示例包括用于 RADIUS 的端口 1812 和用于 LDAP 的端口 389。

维护和监视系统

February 1, 2024

完成 NetScaler Gateway 的配置后，您需要维护和监视设备。您可以通过以下方式执行此操作：

- 您可以将 NetScaler Gateway 升级到最新版本的软件。登录 Citrix 网站时，可以导航到 NetScaler Gateway 下载站点并下载软件。您可以在 Citrix 知识中心找到维护版本的自述文件。
- 您可以将 NetScaler Gateway 配置和管理任务分配给组中的不同成员。通过委派管理，您可以为个人分配访问级别，从而限制他们在 NetScaler Gateway 上执行特定任务。
- 您可以将 NetScaler Gateway 配置保存到设备或计算机上的文件中。您可以比较当前运行的配置和已保存的配置。您还可以从 NetScaler Gateway 中清除配置。
- 您可以在 NetScaler Gateway 配置实用程序中查看、刷新和最终用户会话。
- 您可以在 NetScaler Gateway 上配置日志记录。这些日志提供了有关设备的重要信息，在遇到问题时非常有用。

配置委派管理员

February 1, 2024

NetScaler Gateway 具有默认的管理员用户名和密码。默认用户名和密码为 `nsroot`。首次运行安装向导时，可以更改管理员密码。

您可以创建更多管理员帐户，并为每个帐户分配不同级别的 NetScaler Gateway 访问权限。这些额外的帐户称为委派管理员。例如，您分配了一个人来监视 NetScaler Gateway 连接和日志，另一个人负责在 NetScaler Gateway 上配置特定设置。第一个管理员具有只读访问权限，第二个管理员对设备的访问权限有限。

要配置委派管理员，请使用命令策略以及系统用户和组。

配置委派管理员时，配置过程为：

- 添加系统用户。系统用户是具有指定权限的管理员。所有管理员都会继承他们所属组的策略。
- 添加系统组。系统组包含具有特定权限的系统用户。系统组的成员继承他们所属的一个或多个组的策略。

- 创建命令策略。命令策略允许您定义允许用户或组访问和修改 NetScaler Gateway 配置的哪些部分。您还可以规范允许管理员和组配置哪些命令，例如命令组、虚拟服务器和其他元素。
- 通过设置优先级将命令策略绑定到用户或组。配置委派管理时，为管理员或组分配优先级，以便 NetScaler Gateway 可以确定哪个策略优先。

NetScaler Gateway 具有默认的拒绝系统命令策略。命令策略不能全局绑定。将策略直接绑定到系统管理员（用户）或组。如果用户和组没有关联的命令策略，则会应用默认拒绝策略，并且用户无法运行任何命令或配置 NetScaler Gateway。

您可以配置自定义命令策略，为用户权限分配定义更详细的级别。例如，您可以授予一个人向 NetScaler Gateway 添加会话策略的能力，但不允许用户执行任何其他配置。

为委派管理员配置命令策略

February 1, 2024

NetScaler Gateway 有四个内置命令策略，可用于委派管理：

- 只读 允许只读访问以显示除系统命令组和命令之外的所有 `ns.conf show` 命令。
- **Operator** 允许只读访问，还允许访问以启用和禁用服务上的命令。此策略还允许访问将服务和服务器设置为“访问关闭”。
- 网络 允许几乎完整的系统访问，不包括系统命令和 shell 命令。
- 超级用户 授予完整的系统权限，例如授予默认管理员的权限 `nsroot`。

命令策略包含内置表达式。使用配置实用程序创建系统用户、系统组、命令策略和定义权限。

在 **NetScaler Gateway** 上创建管理用户

1. 在配置实用程序的导航窗格中的“配置”选项卡上，展开“系统”>“用户管理”，然后单击“系统用户”。
2. 在详细信息窗格中，单击“添加”。
3. 在 用户名中，键入用户名。
4. 在“密码”和“确认密码”字段中，键入密码。
5. 要将用户添加到组，请在 成员中单击 添加。
6. 在“可用”中，选择一个组，然后单击向右箭头。
7. 单击 命令策略 **>** 操作 **>** 插入。
8. 在“插入命令策略”对话框中，选择命令，单击“确定”**>**“创建”**>**“关闭”。

创建管理组

管理组包含对 NetScaler Gateway 具有管理权限的用户。您可以在配置实用程序中创建管理组。

使用配置实用程序配置管理组

1. 在配置实用程序的导航窗格中的“配置”选项卡上，展开“系统”>“用户管理”，然后单击“系统组”。
2. 在详细信息窗格中，单击“添加”。
3. 在 组名称中，键入组的名称。
4. 要将现有用户添加到组，请在 成员中单击 添加。
5. 在“可用”下，选择一个用户，然后单击向右箭头。
6. 在 命令策略下的 操作中，单击 插入，选择一个或多个策略，单击 确定，单击 创建，然后单击 关闭。

为委派管理员配置自定义命令策略

February 1, 2024

配置自定义命令策略时，需要提供策略名称，然后配置策略组件以创建命令规范。使用命令规范，您可以限制允许管理员使用的命令。例如，您希望拒绝管理员使用 remove 命令的权限。配置策略时，将操作设置为 deny，然后配置参数。

您可以配置简单或高级命令策略。配置简单策略时，可以在设备上配置组件，例如 NetScaler Gateway 和身份验证。配置高级策略时，选择称为实体组的组件，然后选择允许管理员在组中执行的命令。

创建简单的自定义命令策略

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”>“用户管理”，然后单击“命令策略”。
2. 在详细信息窗格中，单击“添加”。
3. 在 策略名称中，键入策略的名称。
4. 在“操作”中，选择“允许”或“拒绝”。
5. 在 命令规范下，单击 添加。
6. 在“添加命令”对话框的“简单”选项卡的“操作”中，选择委派管理员可以执行的操作。
7. 在“实体组”下，选择一个或多个组。

   您可以按 CTRL 键选择多个组。
8. 单击 **Create**（创建），然后单击 **Close**（关闭）。

创建高级自定义命令策略

1. 在配置实用程序的导航窗格中的“配置”选项卡上，展开“系统”>“用户管理”，然后单击“命令策略”。
2. 在详细信息窗格中，单击“添加”。

3. 在 策略名称中，键入策略的名称。
4. 在“操作”中，选择“允许”或“拒绝”。
5. 在 命令规范下，单击 添加。
6. 在“添加命令”对话框中，单击“高级”选项卡。
7. 在 实体组 中，选择命令所属的组，例如身份验证或高可用性。
8. 在 实体下，选择策略。

   您可以按 CTRL 键选择列表中的多个项目。
9. 在“操作”中，选择命令，单击“创建”，然后单击“关闭”。

   您可以按 CTRL 键选择列表中的多个项目。
10. 单击“创建”，然后单击“关闭”。
11. 在“创建命令策略”对话框中，单击“创建”，然后单击“关闭”。

单击“创建”时，表达式将显示在“创 建命令策略”对话框中的“命令 规范”下。

创建自定义命令策略后，您可以将其绑定到用户或组。

> 注意：您只能将自定义命令策略绑定到您创建的用户或组。您无法将自定义命令策略绑定到用户 `nsroot`。

将自定义命令策略绑定到用户或组

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开“系统”>“用户管理”，然后单击“系统用户”或单击“系统组”。
2. 在详细信息窗格中，从列表中选择一个用户或组，然后单击 打开。
3. 在 命令策略下，选择策略，然后单击 确定。

在 **NetScaler Gateway** 上配置审核

February 1, 2024

NetScaler Gateway 允许您记录设备收集的状态和状态信息。您可以使用审核日志按时间顺序查看事件历史记录。日志中的消息包含有关生成消息的事件的信息、时间戳、消息类型、预定义的日志级别和消息信息。您可以配置确定记录的信息和存储消息的位置的设置。

NetScaler Gateway 当前支持两种日志格式：本地日志的专有日志格式和用于 syslog 服务器的 syslog 格式。您可以将审核日志配置为提供以下信息：

级别	说明
紧急情况	仅记录主要错误。日志中的条目表明 NetScaler Gateway 遇到严重问题，导致其无法使用。
警报	记录可能导致 NetScaler Gateway 无法正常运行但对其运行不重要的问题。可以尽快采取纠正措施，以防止 NetScaler Gateway 遇到严重问题。
关键的	记录不限制 NetScaler Gateway 运行但可能升级为更大问题的严重条件。
错误	记录因 NetScaler Gateway 上的操作失败而产生的条目。
警告	记录可能导致错误或严重错误的潜在问题。
通知	记录的问题比信息级别日志更深入，但其用途与通知相同。
信息	记录 NetScaler Gateway 执行的操作。此日志级别对于故障排除非常有用。

如果配置 TCP 压缩，NetScaler Gateway 审核日志还会存储 NetScaler Gateway 的压缩统计信息。针对不同数据实现的压缩率存储在每个用户会话的日志文件中。

NetScaler Gateway 使用日志签名 SessionID。这使您可以按会话而不是每个用户跟踪日志。作为会话一部分生成的日志具有相同的 SessionID。如果用户使用相同的 IP 地址从同一用户设备建立两个会话，则每个会话都有一个唯一的 SessionID。

> 重要：如果您编写了自定义日志解析脚本，则需要在自定义解析脚本中进行此签名更改。

在 **NetScaler Gateway** 上配置日志

February 1, 2024

在 NetScaler Gateway 上配置日志记录时，可以选择将审核日志存储在 NetScaler Gateway 上或将其发送到系统日志服务器。您可以使用配置实用程序创建审核策略并配置用于存储审核日志的设置。

创建审核策略

1. 在配置实用程序中的配置选项卡上，展开 **NetScaler Gateway** > 策略 > 审核。
2. 在名称中，键入策略的名称。
3. 选择以下选项之一：
    - 如果要将日志发送到 Syslog 服务器，请使用 Syslog。

- Nslog 以将日志存储在 NetScaler Gateway 上。

  > 注意：如果选择此选项，日志将存储在设备上的 /var/log 文件夹中。

4. 在详细信息窗格中，单击“添加”。
5. 为存储日志的服务器信息键入以下信息：
   - 在 名称中，键入服务器的名称。
   - 在“服务器”下，键入日志服务器的名称或 IP 地址。
6. 单击 Create（创建），然后单击 Close（关闭）。

创建审核策略后，您可以将策略绑定到以下任意组合：

- 全球
- Virtual servers（虚拟服务器）
- 组
- 用户

在全局范围内绑定审核策略

1. 在配置实用程序中的配置选项卡上，展开 **NetScaler Gateway** > 策略 > 审核。
2. 选择 **Syslog** 或 **Nslog**。
3. 在详细信息窗格中，单击 操作，然后单击 全局绑定。
4. 在“将审核策略绑定/取消绑定 到 全局”对话框的“详细信息”下，单击“插入策略”。
5. 在 策略名称下，选择一个策略，然后单击 确定。

修改审核策略

您可以修改现有的审核策略来更改将日志发送到的服务器。

1. 在配置实用程序中的 配置 选项卡上，展开 **NetScaler Gateway** > 策略 > 审核
2. 选择 **Syslog** 或 **Nslog**。
3. 在详细信息窗格中，单击策略，然后单击 打开。
4. 在“服务器”中，选择新服务器，然后单击“确定”。

删除审核策略

您可以从 NetScaler Gateway 中删除审核策略。删除审核策略时，该策略将自动取消绑定。

1. 在配置实用程序中的配置选项卡上，展开 **NetScaler Gateway** > 策略 > 审核。
2. 选择 系统日志 或 **Nslog**。
3. 在详细信息窗格中，单击策略，然后单击 删除。

配置 **ACL** 日志记录

February 1, 2024

您可以将 NetScaler Gateway 配置为记录与扩展访问控制列表 (ACL) 匹配的数据包的详细信息。除 ACL 名称外，记录的详细信息还包括特定于数据包的信息，例如源和目标 IP 地址。信息存储在系统日志或 nslog 文件中，具体取决于您启用的日志记录类型（syslog 或 nslog）。

您可以在全局级别和 ACL 级别启用日志记录。但是，要在 ACL 级别启用日志记录，还必须在全局级别启用它。全局设置优先。

为了优化日志记录，当来自同一流的多个数据包与 ACL 匹配时，只记录第一个数据包的详细信息。对于属于同一流的其他每个数据包，计数器都会增加。流程被定义为一组对以下参数具有相同值的数据包：

- 源 IP
- 目标 IP
- 源端口
- 目的端口
- 协议（TCP 或 UDP）

如果数据包不是来自同一个流，或者持续时间超过平均时间，则会创建一个新的流。平均时间是指同一流的数据包不生成其他消息的时间（尽管计数器会增加）。

> 注意：在任何给定时间可以记录的不同流的总数限制为 10,000。

下表介绍了可用于在规则级别为扩展 ACL 配置 ACL 日志记录的参数。

参数名称	说明
Logstate	ACL 的日志记录功能的状态。可能的值：ENABLED 和 DISABLED。默认值：已禁用。
Ratelimit	特定 ACL 可以生成的日志消息数。默认值：100。

使用配置实用程序配置 **ACL** 日志记录

您可以为 ACL 配置日志记录，并指定规则可以生成的日志消息数量。

1. 在配置实用程序的导航窗格中，展开 系统 > 网络，然后单击 ACL。
2. 在详细信息窗格中，单击 扩展 **ACL** 选项卡，然后单击添加。
3. 在“创建扩展 **ACL**”对话框的“名称”中，键入策略的名称。
4. 选中“日志状态”复选框。
5. 在 日志速率限制 文本框中，键入要为规则指定的速率限制，然后单击 创建。

配置 ACL 日志记录后，可以在 NetScaler Gateway 上启用它。创建审核策略，然后将其绑定到用户、组、虚拟服务器或全局。

在 **NetScaler Gateway** 上启用 **ACL** 或 **TCP** 日志记录

1. 在配置实用程序的导航窗格中，展开 **NetScaler Gateway** > 策略 > 审核。
2. 选择 syslog 或 `nslog`。
3. 在“服务器”选项卡上，单击“添加”。
4. 在“创建审核服务器”对话框的“名称”中，键入服务器的名称，然后配置服务器设置。
5. 单击 **ACL** 日志记录 或 **TCP** 日志记录，然后单击 创建。

启用 **Citrix Secure Access** 日志记录

February 1, 2024

您可以配置 Citrix Secure Access 客户端，将所有错误记录到存储在用户设备上的文本文件中。用户可以配置 Citrix Secure Access 客户端，设置用户设备上的登录级别，以记录特定的用户活动。当用户配置日志记录时，插件会在用户设备上创建以下两个文件：

- hooklog<num>.txt，它记录 Citrix Secure Access 客户端生成的拦截消息。
- nssslvpn.txt，其中列出了插件的错误。

> 注意： hooklog.txt 文件不会自动删除。Citrix 建议定期删除这些文件。

用户日志位于用户设备上 Windows 中的以下目录中：

- Windows XP（所有用户）：%SystemDrive%:\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP（特定于用户）：%SystemDrive%:\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows Vista（特定于用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 7（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 7（特定于用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8（所有用户）：%SystemDrive%:\ProgramData\Citrix\AGEE
- Windows 8（特定于用户）：%SystemDrive%:\Users\%username%\AppData\Local\Citrix\AGEE

您可以使用这些日志文件对 Citrix Secure Access 客户端进行故障排除。用户可以通过电子邮件将日志文件发送给技术

在配置对话框中，用户可以设置 Citrix Secure Access 客户端的日志级别。日志记录级别为：

- 记录错误消息
- 记录事件消息
- 记录 Citrix Secure Access 客户端统计数据
- 记录所有错误、事件消息和统计信息

有关适用于 Windows 的 Citrix Secure Access 客户端日志记录功能的更多详细信息，请参阅改进的 Windows 客户端日志收集。

监视 **ICA** 连接

February 1, 2024

您可以使用
ICA 连接对话框监视服务器场上的活动用户会话。此对话框提供以下信息：

- 连接到服务器场的人员的用户名
- 服务器群的域名
- 用户设备的 IP 地址
- 用户设备的端口号
- 运行 Citrix Virtual Apps and Desktops 的服务器的 IP 地址
- 运行 Citrix Virtual Apps and Desktops 的服务器的端口号

1. 导航到配置 **> NetScaler Gateway**。
2. 在“监视连接”部分中，单击 **ICA** 连接。

ICA 会话日志

`ns.log` 文件以以下格式打印 ICA 会话日志：

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT
    0-PPE-1 : default ICA Message 141327 0 :  "[Remote ip =
    10.10.99.86:514] [EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-
    c6333447a76] Received response from STA server {
 sta-server=10.11.40.222:80,type=ResponseData }
 "
<!--NeedCopy-->
```

自发行版 13.1 内部版本 50.x 起，对 ICA 日志进行了以下增强：

- 显示 TCP、EDT、CGP 和 SOCKS 等连接类型。
- 显示 ICA 通用唯一标识符 (UUID)。
- 所有 STA 日志都显示为信息级日志。

身份验证和授权

February 1, 2024

NetScaler Gateway 采用灵活的身份验证设计，允许对 NetScaler Gateway 的用户身份验证进行广泛的您可以使用行业标准身份验证服务器并配置 NetScaler Gateway 以使用服务器对用户进行身份验 NetScaler Gateway 还支持基于客户端证书中存在的属性进行身份验证。NetScaler Gateway 身份验证旨在适应使用单一来源进行用户身份验证的简单身份验证过程以及依赖多种身份验证类型的更复杂的级联身份验证过程。

NetScaler Gateway 身份验证包含用于创建本地用户和组的本地身份验证。此设计围绕使用策略来控制您配置的身份验证过程。您创建的策略可以在 NetScaler Gateway 全局或虚拟服务器级别应用，并且可用于根据用户的源网络有条件地设置身份验证服务器参数。

由于策略是全局绑定或绑定到虚拟服务器的，因此您还可以为策略分配优先级，以便在身份验证过程中创建多个身份验证服务器的级联。

NetScaler Gateway 包括对以下身份验证类型的支持。

- 本地
- 轻型目录访问协议 (LDAP)
- RADIUS
- SAML
- TACACS+
- 客户端证书身份验证（包括智能卡身份验证）

NetScaler Gateway 还支持 RSA SecurID、Gemalto Protiva 和 SafeWord。可以使用 RADIUS 服务器配置这些类型的身份验证。

虽然身份验证允许用户登录 NetScaler Gateway 并连接到内部网络，但授权定义用户可以访问的安全网络中的资源。您可以使用 LDAP 和 RADIUS 策略配置授权。

配置默认全局身份验证类型

February 1, 2024

安装 NetScaler Gateway 并运行 NetScaler Gateway 向导时，您在向导中配置了身份验证。此身份验证策略会自动绑定到 NetScaler Gateway 全局级别。在 NetScaler Gateway 向导中配置的身份验证类型是默认身份验证类型。您可以通过再次运行 NetScaler Gateway 向导来更改默认授权类型，也可以在配置实用程序中修改全局身份验证设置。

如果需要添加其他身份验证类型，可以使用配置实用程序在 NetScaler Gateway 上配置身份验证策略并将策略绑定到 NetScaler Gateway。在全局配置身份验证时，可以定义身份验证类型、配置设置以及设置可以进行身份验证的最大用户数。

配置并绑定策略后，您可以设置优先级来定义优先级的身份验证类型。例如，您可以配置 LDAP 和 RADIUS 身份验证策略。如果 LDAP 策略的优先级为 10，而 RADIUS 策略的优先级号为 15，则无论将每个策略绑定到何处，LDAP 策略都将优先。这称为级联身份验证。

您可以选择从 NetScaler Gateway 内存中缓存或 NetScaler Gateway 上运行的 HTTP 服务器提供登录页面。如果选择从内存中缓存提供登录页面，则从 NetScaler Gateway 传递登录页面的速度明显快于从 HTTP 服务器传送登录页面的速度。选择从内存缓存中传送登录页可缩短大量用户同时登录时的等待时间。作为全局身份验证策略的一部分，您只能配置缓存中登录页的传递。

您还可以配置作为身份验证的特定 IP 地址的网络地址转换 (NAT) IP 地址。此 IP 地址对于身份验证是唯一的，不是 NetScaler Gateway 子网、映射或虚拟 IP 地址。这是一个可选设置。

注意：不能使用 NetScaler Gateway 向导配置 SAML 身份验证。

您可以使用快速配置向导配置 LDAP、RADIUS 和客户端证书身份验证。运行向导时，可以从 NetScaler Gateway 上配置的现有 LDAP 或 RADIUS 服务器中进行选择。您还可以配置 LDAP 或 RADIUS 的设置。如果使用双重身份验证，Citrix 建议使用 LDAP 作为主要身份验证类型。

全局配置身份验证

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改身份验证设置”。
3. 在“最大用户数”中，键入可以使用此身份验证类型进行身份验证的用户数。
4. 在 NAT IP 地址中，键入用于身份验证的唯一 IP 地址。
5. 选择 E 启用静态缓存可更快地传送登录页面。
6. 选择 启用增强的身份验证反馈，以便在身份验证失败时向用户提供消息。用户收到的消息包括密码错误、帐户已禁用或锁定或未找到用户，仅举几例。
7. 在 默认身份验证类型中，选择身份验证类型。
8. 配置身份验证类型的设置，然后单击确定。

配置未经授权的身份验证

February 1, 2024

授权定义允许用户通过 NetScaler Gateway 连接到的资源。您可以使用表达式配置授权策略，然后将策略设置为允许或拒绝。您可以将 NetScaler Gateway 配置为仅使用身份验证，而无需授权。

在未经授权的情况下配置身份验证时，NetScaler Gateway 不会执行组授权检查。您为用户或组配置的策略将分配给用户。

有关配置授权的详细信息，请参阅 配置授权。

配置授权

February 1, 2024

授权指定了用户在登录 NetScaler Gateway 时有权访问的网络资源。授权的默认设置为拒绝对所有网络资源的访问。Citrix 建议使用默认的全局设置，然后创建授权策略来定义用户可以访问的网络资源。

您可以使用授权策略和表达式在 NetScaler Gateway 上配置授权。创建授权策略后，可以将其绑定到您在设备上配置的用户或组。

配置授权策略

February 1, 2024

配置授权策略时，可以将其设置为允许或拒绝访问内部网络中的网络资源。例如，要允许用户访问 10.3.3.0 网络，请使用以下表达式：

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

授权策略适用于用户和组。用户通过身份验证后，NetScaler Gateway 通过从 RADIUS、LDAP 或 TACACS+ 服务器获取用户的组信息来执行组授权检查。如果用户的组信息可用，NetScaler Gateway 会检查该组允许的网络资源。

要控制用户可以访问哪些资源，必须创建授权策略。如果不需要创建授权策略，则可以配置默认的全局授权。

如果在授权策略中创建拒绝访问文件路径的表达式，则只能使用子目录路径，而不能使用根目录。例如，使用 fs.path 包含“\\dir1\\dir2”而不是 fs.path 包含“\\rootdir\\dir1\\dir2”。如果在本示例中使用第二个版本，则策略将失败。

配置授权策略后，然后将其绑定到用户或组，如下面的任务所示。

默认情况下，首先根据绑定到虚拟服务器的策略验证授权策略，然后针对全局绑定的策略进行验证。如果您全局绑定策略并希望全局策略优先于绑定到用户、组或虚拟服务器的策略，则可以更改策略的优先级编号。优先级编号从零开始。较低优先级的数字使策略的优先级越高。

例如，如果全局策略的优先级编号为 1，而用户的优先级为 2，则首先应用全局身份验证策略。

> 重要提示：
>
> - 传统授权策略仅适用于 TCP 流量。
> - 高级授权策略可应用于所有类型的流量（TCP/UDP/ICMP/DNS）。
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if “type” is not explicitly mentioned or “type” is set to REQUEST, the

> behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>
> – The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

有关高级授权策略的更多详细信息，请参阅文章https://support.citrix.com/article/CTX232237。

授权策略表达式示例

以下是授权策略的表达式示例：

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1"DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

使用 **GUI** 配置授权策略

1. 导航到 **NetScaler Gateway >** 策略 **>** 授权。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“操作”中，选择“允许”或“拒绝”。
5. 在“表达式”中，单击“表达式编辑器”。
6. 要开始配置表达式，请单击选 择 并选择必要的元素。
7. 表达式完 成 后，单击“完成”。
8. 单击创建。

使用 **GUI** 将授权策略绑定到用户

1. 导航到 **NetScaler Gateway** > 用户管理。
2. 单击 **AAA** 用户。
3. 在详细信息窗格中，选择一个用户，然后单击 编辑。
4. 在 高级设置中，单击 授权策略。
5. 在 策略绑定 页面中，选择策略或创建策略。
6. 在 优先级中，设置优先级编号。
7. 在 类型中，选择请求类型，然后单击 确定。

使用 **GUI** 将授权策略绑定到组

1. 导航到 **NetScaler Gateway>** 用户管理。
2. 单击 **AAA** 组。
3. 在详细信息窗格中，选择一个组，然后单击 编辑。
4. 在 高级设置中，单击 授权策略。
5. 在 策略绑定 页面中，选择策略或创建策略。
6. 在 优先级中，设置优先级编号。
7. 在 类型中，选择请求类型，然后单击 确定。

设置默认全局授权

February 1, 2024

要定义用户在内部网络上有权访问的资源，可以配置默认的全局授权。您可以通过允许或拒绝全局访问内部网络上的网络资源来配置全局授权。

您创建的任何全局授权操作都将直接或通过组应用于尚未与其关联的授权策略的所有用户。用户或组授权策略始终会覆盖全局授权操作。如果默认授权操作设置为拒绝，则必须对所有用户或组应用授权策略，才能使这些用户或组可以访问网络资源。此要求有助于提高安全性。

要设置默认全局授权：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“安全”选项卡上的“默认授权操作”旁边，选择允许或拒绝，然后单击“确定”。

禁用身份验证

February 1, 2024

如果您的部署不需要身份验证，则可以将其禁用。可以为每个不需要身份验证的虚拟服务器禁用身份验证。

重要：Citrix 建议谨慎禁用身份验证。如果未使用外部身份验证服务器，请创建本地用户和组以允许 NetScaler Gateway 对用户进行身份验证。禁用身份验证将停止使用身份验证、授权和记帐功能来控制和监视与 NetScaler Gateway 的连接。当用户键入要连接到 NetScaler Gateway 的 Web 地址时，不会显示登录页面。

禁用身份验证

1. 在配置实用程序的导航窗格中，展开 NetScaler Gateway，然后单击虚拟服务器。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在身份验证选项卡的用户身份验证下，单击以清除启用身份验证。

为特定时间配置身份验证

February 1, 2024

您可以配置身份验证策略，以便允许用户在特定时间（例如在正常工作时间）访问内部网络。当用户尝试在其他时间登录时，登录将被拒绝。

要限制用户登录 NetScaler Gateway 的时间，请在身份验证策略中创建表达式，然后将其绑定到虚拟服务器或全局绑定。

为时间、日期或星期几配置身份验证

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在身份验证下，选择身份验证类型。
3. 在详细信息窗格中，单击策略选项卡，选择身份验证策略，然后单击打开。
4. 在“配置身份验证策略”对话框的“表达式”下的“匹配任意表达式”旁边，单击“添加”。
5. 在添加表达式对话框的表达式类型中，选择日期/时间。
6. 在限定符中，选择以下选项之一：

   - 是时候配置用户无法登录的时间了。
   - DATE 用于配置用户无法登录的日期。
   - DAYOFWEEK 来配置用户无法登录的日期。

   示例：TIME: 2020-10-12-02:30:00GMT DATE: 2020-10-12 DAYOFWEEK: Monday
7. 在运算符中，选择值。
8. 在值中，单击文本框旁边的日历，然后选择日期、日期或时间。
9. 单击确定两次，单击关闭，然后单击确定。

身份验证策略的工作原理

February 1, 2024

用户登录 NetScaler Gateway 时，将根据您创建的策略对其进行身份验证。该策略定义了身份验证类型。单个身份验证策略可用于简单的身份验证需求，并且通常在全局级别绑定。您还可以使用默认的身份验证类型，即本地身份验证类型。如果配置本地身份验证，则还必须在 NetScaler Gateway 上配置用户和组。

您可以配置多个身份验证策略并将其绑定以创建详细的身份验证过程和虚拟服务器。例如，您可以通过配置多个策略来配置级联身份验证和双因素身份验证。您还可以设置身份验证策略的优先级，以确定哪些服务器以及 NetScaler Gateway 检查用户凭据的顺序。身份验证策略包括表达式和操作。例如，如果将表达式设置为 True 值，则当用户登录时，操作会将用户登录评估为 true，然后用户可以访问网络资源。

创建身份验证策略后，可以在全局级别或将策略绑定到虚拟服务器。将至少一个身份验证策略绑定到虚拟服务器时，当用户登录到虚拟服务器时，不会使用绑定到全局级别的任何身份验证策略，除非全局身份验证类型的优先级高于绑定到虚拟服务器的策略。

用户登录 NetScaler Gateway 时，将按以下顺序评估身份验证：

- 检查虚拟服务器是否存在任何绑定的身份验证策略
- 如果身份验证策略未绑定到虚拟服务器，NetScaler Gateway 将检查全局身份验证策略。
- 如果身份验证策略未绑定到虚拟服务器或全局绑定，则会通过默认身份验证类型对用户进行身份验证。

如果配置 LDAP 和 RADIUS 身份验证策略并希望全局绑定策略以进行双重身份验证，则可以在配置实用程序中选择策略，然后选择策略是主要身份验证类型还是辅助身份验证类型。您还可以配置组提取策略。

配置身份验证配置文件

February 1, 2024

您可以使用 NetScaler Gateway 向导或配置实用程序创建身份验证配置文件。配置文件包含身份验证策略的所有设置。您可以在创建身份验证策略时配置配置文件。

使用 NetScaler Gateway 向导，您可以使用所选的身份验证类型来配置身份验证。如果要在运行向导后配置其他身份验证策略，则可以使用配置实用程序。有关 NetScaler Gateway 向导的详细信息，请参阅 使用 NetScaler Gateway 向导配置设置。

使用配置实用程序创建身份验证策略

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在导航窗格中的“身份验证”下，选择身份验证类型。

3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 如果使用的是外部身份验证类型，请单击“服务器”旁边的“新建”。
5. 在“创建身份验证服务器”对话框中，配置身份验证类型的设置，单击“创建”，然后单击“关闭”。
6. 在创建身份验证策略对话框的命名表达式旁边，选择 True 值，单击添加表达式，单击创建，然后单击关闭。
   注意：选择身份验证类型并保存身份验证配置文件时，无法更改身份验证类型。要使用其他身份验证类型，必须创建新策略。

使用配置实用程序修改身份验证策略

您可以修改已配置的身份验证策略和配置文件，例如身份验证服务器的 IP 地址或表达式。

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在导航窗格中的“身份验证”下，选择身份验证类型。
3. 在详细信息窗格的“服务器”选项卡上，选择一个服务器，然后单击“打开”。

删除身份验证策略

如果从网络中更改或删除了身份验证服务器，请从 NetScaler Gateway 中删除相应的身份验证策略。

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在导航窗格中的“身份验证”下，选择身份验证类型。
3. 在详细信息窗格的“策略”选项卡上，选择一个策略，然后单击“删除”。

绑定身份验证策略

February 1, 2024

配置身份验证策略后，可以全局绑定策略或将策略绑定到虚拟服务器。您可以使用配置实用程序绑定身份验证策略。

使用 **GUI** 全局绑定身份验证策略

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 单击身份验证类型。
3. 在详细信息窗格的 策略 选项卡上，单击服务器，然后在 操作中单击 全局绑定。
4. 在“主策略”或“辅助”选项卡的“详细信息”下，单击“插入策略”。
5. 在“策略名称”下，选择策略，然后单击“确定”。

   注意：选择策略时，NetScaler Gateway 会自动将表达式设置为 True 值。

使用 **GUI** 取消绑定全局身份验证策略

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 在“策略”选项卡的“操作”中，单击“全局绑定”。
3. 在“将身份验证策略绑定/取消绑定到全局”对话框的“主策略”或“辅助策略”选项卡上，在“策略名称”中，选择策略，单击“取消绑定策略”，然后单击“确定”。

设置身份验证策略的优先级

February 1, 2024

默认情况下，首先根据绑定到虚拟服务器的策略验证身份验证策略，然后根据全局绑定的策略进行验证。如果您在全局范围内绑定身份验证策略，并希望全局策略优先于绑定到虚拟服务器的策略，则可以更改策略的优先级编号。优先级编号从零开始。较低优先级的数字使身份验证策略的优先级越高。

例如，如果全局策略的优先级编号为 1，而虚拟服务器的优先级为 2，则首先应用全局身份验证策略。

设置或更改全局身份验证策略的优先级

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在“策略”选项卡上的“操作”中，单击“全局绑定”。
3. 在“绑定/取消绑定身份验证全局策略”对话框中的“主”或“辅助”选项卡的“优先级”下，键入数字，然后单击“确定”。

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 选择虚拟服务器，然后单击打开。
3. 单击身份验证选项卡，然后选择主要或辅助。
4. 选择策略，然后在“优先级”中键入优先级的编号，然后单击“确定”。

配置本地用户

February 1, 2024

您可以在 NetScaler Gateway 上本地创建用户帐户，以补充身份验证服务器上的用户。例如，您可能要为临时用户（例如顾问或来宾）创建本地用户帐户，但不在身份验证服务器上为这些用户创建条目。

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

创建本地用户

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中展开 **NetScaler Gateway >** “用户管理”，然后单击 **AAA** 用户。
2. 在详细信息窗格中，单击“添加”。
3. 在 用户名中，键入用户名。
4. 如果使用本地身份验证，请清除 外部身份验证。
   注意：选择 外部身份验证 可让用户根据外部身份验证服务器（例如 LDAP 或 RADIUS）进行身份验证。清除该复选框可让 NetScaler Gateway 根据本地用户数据库进行身份验证。
5. 在“密码”和“确认密码”中，键入用户的密码，单击“创建”，然后单击“关闭”。

更改用户密码

创建本地用户后，您可以更改用户的密码或将用户帐户配置为针对外部身份验证服务器进行身份验证。

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中展开 **NetScaler Gateway >** “用户管理”，然后单击 **AAA** 用户。
2. 在详细信息窗格中，选择一个用户，然后单击 打开。
3. 在“密码”和“确认密码”中，键入用户的新密码，然后单击“确定”。

更改用户的身份验证方法

如果您有为本地身份验证配置的用户，则可以将身份验证更改为外部身份验证服务器。为此，请启用外部身份验证。

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中展开 **NetScaler Gateway >** “用户管理”，然后单击 **AAA** 用户。
2. 在详细信息窗格中，选择一个用户，然后单击 打开。
3. 选择 外部身份验证，然后单击 确定。

要删除用户

您还可以从 NetScaler Gateway 中删除用户。

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中展开 **NetScaler Gateway >** “用户管理”，然后单击 **AAA** 用户。

2. 在详细信息窗格中，选择一个用户，然后单击 删除。

从 NetScaler Gateway 中删除用户时，所有关联的策略也将从用户配置文件中删除。

配置组

February 1, 2024

您可以在 NetScaler Gateway 上拥有属于本地组的组，可以使用本地身份验证对用户进行身份验证。如果使用外部服务器进行身份验证，NetScaler Gateway 上的组将配置为与内部网络中身份验证服务器上配置的组匹配。当用户登录并通过身份验证时，如果组名与身份验证服务器上的组匹配，则用户将继承 NetScaler Gateway 上该组的设置。

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

如果使用本地身份验证，请创建用户并将其添加到 NetScaler Gateway 上配置的组中。然后，用户将继承该组的设置。

重要：如果用户是 Active Directory 组的成员，则 NetScaler Gateway 上该组的名称必须与 Active Directory 组的名称相同。

要创建组

1. 在配置实用程序中，单击 配置 选项卡，然后在导航窗格中展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，单击“添加”。
3. 在“组名”中，键入组的名称，单击“创建”，然后单击“关闭”。

删除组

您也可以从 NetScaler Gateway 中删除用户组。

1. 在配置实用程序中，单击 配置 选项卡，然后在导航窗格中展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，选择该组，然后单击“删除”。

向组中添加用户

February 1, 2024

您可以在创建组期间或之后将用户添加到组中。您可以将用户添加到多个组，以便用户可以继承绑定到这些组的策略和设置。

要将用户添加到组：

1. 在配置实用程序中，单击“配置”选项卡，在导航窗格中展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 用户。
2. 在详细信息窗格中，选择一个组，然后单击 打开。
3. 在 用户 选项卡上的 可用用户下，选择用户，单击 添加，然后单击 确定。

为组配置策略

February 1, 2024

配置组后，可以使用“组”对话框应用指定用户访问权限的策略和设置。如果您使用本地身份验证，则可以创建用户并将其添加到在 NetScaler Gateway 上配置的组中。然后，用户将继承该组的设置。

您可以在“组”对话框中为一组用户配置以下策略或设置：

- 用户
- 授权策略
- 审核策略
- 会话策略
- 流量策略
- 书签
- 内联网应用程序
- 内联网 IP 地址

在您的配置中，您可能有属于多个组的用户。此外，每个组可能有一个或多个绑定会话策略，并配置了不同的参数。属于多个组的用户将继承分配给该用户所属的所有组的会话策略。要确保哪个会话策略评估优先于另一个会话策略评估，必须设置会话策略的优先级。

例如，您的 group1 绑定了使用主页 www.homepage1.com 配置的会话策略。Group2 绑定了使用主页 www.homepage2.com 配置的会话策略。当这些策略绑定到没有优先级编号或具有相同优先级编号的各个组时，同时属于这两个组的用户显示的主页取决于首先处理哪个策略。通过为主页 www.homepage1.com 的会话策略设置一个较低优先级的编号（优先级较高），您可以确保属于这两个组的用户都能收到主页 www.homepage1.com。

如果会话策略没有分配优先级编号或具有相同的优先级编号，则按以下顺序评估优先级：

- 用户
- 组
- 虚拟服务器
- 全局

如果策略绑定到同一级别、没有优先级编号或策略具有相同的优先级编号，则评估顺序按策略绑定顺序进行。先绑定到某个级别的策略优先于之后绑定的策略。

如果我们有一个用户绑定到多个组，每个组都绑定了 IIP，则该用户可以从任何绑定的组中获得免费 IP。

配置 **LDAP** 身份验证

February 1, 2024

您可以将 NetScaler Gateway 配置为对一个或多个 LDAP 服务器的用户访问进行身份验证。

LDAP 授权要求在 Active Directory、LDAP 服务器和 NetScaler Gateway 上使用相同的组名称。字符和大小写也必须匹配。

默认情况下，使用安全套接字层 (SSL) 或传输层安全性 (TLS) 进行 LDAP 身份验证是安全的。有两种类型的安全 LDAP 连接。对于一种类型，LDAP 服务器在与 LDAP 服务器用于接受清除 LDAP 连接的端口分开的端口上接受 SSL 或 TLS 连接。用户建立 SSL 或 TLS 连接后，可以通过该连接发送 LDAP 流量。

LDAP 连接的端口号为：

- 389 用于不安全的 LDAP 连接
- 636 用于安全的 LDAP 连接
- 3268 用于 Microsoft 不安全的 LDAP 连接
- 3269 用于 Microsoft 安全 LDAP 连接

第二种类型的安全 LDAP 连接使用 StartTLS 命令并使用端口号 389。如果在 NetScaler Gateway 上配置端口号 389 或 3268，则服务器将尝试使用 StartTLS 进行连接。如果使用任何其他端口号，服务器将尝试使用 SSL 或 TLS 进行连接。如果服务器无法使用 StartTLS、SSL 或 TLS，则连接将失败。

如果指定 LDAP 服务器的根目录，NetScaler Gateway 将搜索所有子目录以查找用户属性。在大型目录中，这种方法可能会影响性能。因此，Citrix 建议您使用特定组织单位 (OU)。

下表包含 LDAP 服务器的用户属性字段示例：

LDAP 服务器	用户属性	区分大小写
Microsoft Active Directory 服务器	sAMAccountName	否
Novell eDirectory	ou	是
IBM 目录服务器	uid	是
Lotus Domino	CN	是
Sun ONE 目录（以前称为 iPlanet）	uid 或 cn	是

下表包含基本 DN 的示例：

LDAP 服务器	基本 DN
Microsoft Active Directory 服务器	DC=citrix,DC=local
Novell eDirectory	ou=users,ou=dev
IBM 目录服务器	cn=users
Lotus Domino	OU=City,O=Citrix, C=US
Sun ONE 目录（以前称为 iPlanet）	ou=People,dc=citrix,dc=com

下表包含绑定 DN 的示例：

LDAP 服务器	Bind DN（绑定 DN）
Microsoft Active Directory 服务器	CN=Administrator, CN=Users, DC=citrix, DC=local
Novell eDirectory	cn=admin, o=citrix
IBM 目录服务器	LDAP_dn
Lotus Domino	CN=Notes Administrator, O=Citrix, C=US
Sun ONE 目录（以前称为 iPlanet）	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

注意：有关 LDAP 服务器设置的详细信息，请参阅
确定 LDAP 目录中的属性。

使用配置实用程序配置 **LDAP** 身份验证

February 1, 2024

1. 导航到 **NetScaler Gateway** > 策略 > 身份验证。
2. 单击 **LDAP**。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 在名称中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。

6. 在 名称中，键入服务器的名称。
7. 在 服务器下的 **IP** 地址和端口中，键入 LDAP 服务器的 IP 地址和端口号。
8. 在 类型中，为 Active Directory 选择 **AD** 或 **Novell** 目录服务选择 **NDS** 。
9. 在“连接设置”下，完成以下操作：

   a) 在 基本 **DN**（用户位置）中，键入用户所在的基本 DN。基本 DN 搜索位于所选目录（AD 或 NDS）下的用户。

   通过删除用户名并指定用户所在的组，从绑定 DN 派生基本 DN。基本 DN 的语法示例包括：

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   b) 在 管理员绑定 **DN** 中，键入用于查询 LDAP 目录的管理员绑定 DN。绑定 DN 的语法示例包括：

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

   对于 Active Directory，指定为 cn=groupname 的组名是必需的。您在 NetScaler Gateway 中定义的组名称与 LDAP 服务器上的组名称必须相同。

   对于其他 LDAP 目录，组名不是必需的，或者在必要时指定为 ou=groupname。

   NetScaler Gateway 使用管理员凭据绑定到 LDAP 服务器，然后搜索用户。找到用户后，NetScaler Gateway 将取消绑定管理员凭据并与用户凭据重新绑定。

   c) 在 管理员密码和确认管理员密码中，键入 LDAP 服务器的管理员密码。

10. 要自动检索更多 LDAP 设置，请单击 检索属性。

    单击“检索属性”时，“其他设置”下的字段将自动填充。如果要忽略此步骤，请继续执行步骤 12 和 13。否则，请跳到步骤 14。

11. 在“其他设置”下的“服务器登录名属性”中，键入 NetScaler Gateway 必须在该属性下查找正在配置的 LDAP 服务器的用户登录名。默认值为 `samAccountName`。
12. 在 搜索筛选器中，键入值以搜索与单个或多个活动目录组关联的用户。

    例如，memberOf=CN=GatewayAccess,OU=Groups,DC=Users,DC=lab。

    > 注意：
    >
    > 您可以使用上述示例将 NetScaler Gateway 仅限于特定 AD 组的成员访问。

13. 在 组属性中，保留 Active Directory 的默认 memberOf 或将属性更改为正在使用的 LDAP 服务器类型的属性。此属性使 NetScaler Gateway 能够在授权期间获取与用户关联的组。

14. 在 安全 类型中，选择安全类型，然后单击 创建。
15. 要允许用户更改其 LDAP 密码，请选择 允许更改密码。

    注意：

    - 如果选择“纯文本”作为安全类型，则不支持允许用户更改密码。
    - 如果为了安全起见选择 纯文本 或 **TLS** ，请使用端口号 389。如果选择 **SSL**，请使用端口号 636。

确定 **LDAP** 目录中的属性

February 1, 2024

如果您在确定 LDAP 目录属性方面需要帮助，以便能够在 NetScaler Gateway 上配置身份验证设置，则可以使用 Softerra 提供的免费 LDAP 浏览器轻松查找它们。

您可以从 Softerra LDAP 管理员网站下载 LDAP浏览器。安装浏览器后，设置以下属性：

- LDAP 服务器的主机名或 IP 地址。
- LDAP 服务器的端口。默认值为 389。
- 基本 DN 字段，您可以将其留空。LDAP 浏览器提供的信息可帮助您确定必须在 NetScaler Gateway 上配置此设置的基本 DN。
- 匿名绑定检查确定 LDAP 服务器是否需要用户凭据才能连接到 LDAP 服务器。如果 LDAP 服务器需要凭据，请清除该复选框。

完成设置后，LDAP 浏览器将在左侧窗格中显示配置文件名称并连接到 LDAP 服务器。

配置 **LDAP** 组提取

February 1, 2024

如果使用双重身份验证，则会串联从主身份验证源和辅助身份验证源中提取的组。授权策略可以应用于从主身份验证服务器或辅助身份验证服务器中提取的组。

将从 LDAP 服务器获取的组名称与在 NetScaler Gateway 上本地创建的组名进行比较。如果两个组名匹配，则本地组的属性将应用于从 LDAP 服务器获取的组。

如果用户属于多个 LDAP 组，NetScaler Gateway 将从用户所属的所有组中提取用户信息。如果用户是 NetScaler Gateway 上两个组的成员，并且每个组都有绑定的会话策略，则该用户将从这两个组继承会话策略。要确保用户收到正确的会话策略，请设置会话策略的优先级。

有关 LDAP 组成员资格属性的详细信息，请参阅以下内容：

如何直接从用户对象进行 **LDAP** 组提取

February 1, 2024

评估来自组对象的组成员资格的 LDAP 服务器支持 NetScaler Gateway 授权。

某些 LDAP 服务器允许用户对象包含有关对象所属组的信息，例如 Active Directory（通过使用 memberOf 属性）或 IBM eDirectory（通过使用组成员资格属性）。用户的组成员资格可以是来自用户对象的属性，例如 IBM 目录服务器（通过使用 ibm-allGroups）或 Sun ONE 目录服务器（通过使用 nsRole）。这两种类型的 LDAP 服务器都支持 NetScaler Gateway 组提取。

例如，在 IBM Directory Server 中，可以使用 ibm-allGroups 属性返回所有组成员资格，包括静态组、动态组和嵌套组。在 Sun ONE 中，所有角色（包括托管角色、筛选角色和嵌套角色）都是通过使用 nsRole 属性计算的。

LDAP 组提取是如何从组对象间接进行的

February 1, 2024

间接评估来自组对象的组成员资格的 LDAP 服务器与 NetScaler Gateway 授权不兼容。

某些 LDAP 服务器（例如 Lotus Domino）仅允许组对象包含有关用户的信息。这些 LDAP 服务器不允许用户对象包含有关组的信息，因此与 NetScaler Gateway 组提取不兼容。对于此 LDAP 服务器类型，通过在组的成员列表中查找用户来执行组成员资格搜索。

LDAP 授权组属性字段

February 1, 2024

下表包含 LDAP 组属性字段的示例：

LDAP 服务器	LDAP 属性
Microsoft Active Directory 服务器	memberOf
Novell eDirectory	groupMembership

LDAP 服务器	LDAP 属性
IBM 目录服务器	ibm-allGroups
Sun ONE 目录（以前称为 iPlanet）	nsRole

配置 **LDAP** 授权

February 1, 2024

您可以通过设置组属性名称和子属性在身份验证策略中配置 LDAP 授权。

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在身份验证下，单击身份验证类型。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在名称中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在 名称中，键入服务器的名称。
7. 在服务器下，键入 LDAP 服务器的 IP 地址和端口。
8. 在 组属性中，键入 memberOf。
9. 在“子属性名称”中，键入 CN，然后单击“创建”。
10. 在“创建身份验证策略”对话框中，选择“命名表达式”旁边的表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **LDAP** 嵌套组提取

February 1, 2024

NetScaler Gateway 可以查询 LDAP 组，并从您在身份验证服务器上配置的祖先组中提取组和用户信息。例如，您创建了 group1，然后在该组中创建了 group2 和 group3。如果用户属于 group3，NetScaler Gateway 将从所有嵌套的祖先组（group2、group1）中提取到指定级别的信息。

您可以使用身份验证策略配置 LDAP 嵌套组提取。运行查询时，NetScaler Gateway 会搜索这些组，直到达到最大嵌套级别或搜索所有可用组为止。

配置 **LDAP** 嵌套组抽取

1. 在配置实用程序的导航窗格中，展开 **NetScaler Gateway >** 策略 **>** 身份验证/授权 **>** 身份验证 **>** 身份验证，然后单击 **LDAP**。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“服务器”旁边，单击“新建”。
5. 在 名称中，键入服务器的名称。
6. 配置 LDAP 服务器的设置。
7. 展开“嵌套组提取”，然后单击“启用”。
8. 在 最大嵌套级别中，键入 NetScaler Gateway 检查的级别数。
9. 在 组名标识符中，键入用于唯一标识 LDAP 服务器上组名的 LDAP 属性名称，例如 `sAMAccountName`。
10. 在 组搜索属性中，键入要在搜索响应中获取的 LDAP 属性名称，以确定任何组的父组。例如，`memberOf`。
11. 在 组搜索子属性中，键入要作为组搜索属性的一部分进行搜索的 LDAP 子属性名称，以确定任何组的父组。例如，键入 CN。
12. 在“组搜索筛选器”中，键入查询字符串。例如，筛选器可以是 `&(samaccountname=test)(objectClass=\*)`。
13. 单击“创建”，然后单击“关闭”。
14. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

为多个域配置 **LDAP** 组提取

February 1, 2024

如果您有多个用于身份验证的域并且正在使用 StoreFront 或 Web Interface，则可以将 NetScaler Gateway 配置为使用组提取将正确的域名发送到 Web Interface。

在 Active Directory 中，您需要为网络中的每个域创建一个组。创建组后，添加属于该组和指定域的用户。在 Active Directory 中配置组后，您可以在 NetScaler Gateway 上为多个域配置 LDAP 组提取。

要为多个域配置 NetScaler Gateway 进行组提取，您需要创建与网络中的域数相同的会话和身份验证策略数量。例如，您有两个名为 Sampa 和 Child 的域。每个域都收到一个会话策略和一个身份验证策略。

创建策略后，您可以在 NetScaler Gateway 上创建组，然后将会话策略绑定到组。然后，将身份验证策略绑定到虚拟服务器。

如果在多个域中部署 StoreFront，则域之间必须存在信任关系。

如果在多个域中部署 Citrix Endpoint Management 或 Web Interface，则这些域无需相互信任。

为组提取创建会话策略

February 1, 2024

为组提取创建会话策略时，第一步是创建两个会话配置文件并设置以下参数：

- 启用 ICA 代理。
- 添加 Web Interface Web 地址。
- 添加 Windows 域。
- 将配置文件添加到会话策略并将表达式设置为 true。

创建用于组提取的会话配置文件

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中，单击“配置文件”选项卡，然后单击“添加”。
3. 在名称中，键入配置文件的名称。例如，键入 Sampa。
4. 在 已发布的应用程序 选项卡上，执行以下操作

   a) 在 **ICA** 代理旁边，单击 覆盖全局，然后选择 开。
   b) 在 **Web Interface** 地址旁边，单击“覆盖全局”，然后键入 Web Interface 的 Web 地址。
   c) 在 单点登录域旁边，单击 覆盖全局，键入 Windows 域的名称，然后单击 创建。

5. 在 名称中，清除第一个域的名称，然后键入第二个域的名称，例如 Child。
6. 在“单点登录域”旁边，清除第一个 Windows 域的名称，然后键入第二个域的名称，单击“创建”，然后单击“关闭”。

创建会话配置文件后，您将创建两个会话策略。每个会话策略都使用其中一个配置文件。

创建会话策略

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在 请求配置文件中，选择第一个域的配置文件。
5. 在 命名表达式旁边，单击 常规，选择 **True** 值，单击 添加表达式，然后单击 创建。
6. 在 名称中，将名称更改为第二个域。
7. 在“请求配置文件”中，选择第二个域的配置文件，单击“创建”，然后单击“关闭”。

为多个域创建 **LDAP** 身份验证策略

February 1, 2024

在 NetScaler Gateway 上创建会话策略后，您可以创建几乎相同的 LDAP 身份验证策略。配置身份验证策略时，重要字段是
搜索筛选器。在此字段中，必须键入在 Active Directory 中创建的组的名称。

首先创建身份验证配置文件，然后创建身份验证策略。

为多个域组提取创建身份验证配置文件

1. 在配置实用程序的配置选项卡上，展开 **Citrix Gateway >** 策略 **>** 身份验证。
2. 在导航窗格中，单击 **LDAP**。
3. 在详细信息窗格中，单击 服务器 选项卡，然后单击 添加。
4. 在 名称中，键入第一个域的名称，例如 Sampa。
5. 配置 LDAP 服务器的设置，然后单击 创建。
6. 重复步骤 3、4 和 5 以配置第二个域的身份验证配置文件，然后单击“关闭”。

创建并保存配置文件后，创建身份验证策略。

为多个域组提取创建身份验证策略

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 在详细信息窗格中，单击 策略 选项卡，然后单击 添加。
3. 在 名称中，键入第一个域的名称。
4. 在“身份验证类型”中，选择 **LDAP**。
5. 在 服务器中，选择第一个域的身份验证配置文件。
6. 在 命名表达式旁边，单击 常规，选择 **True** 值，单击 添加表达式，然后单击 创建。
7. 在名称中，键入第二个域的名称。
8. 在 服务器中，选择第二个域的身份验证配置文件，单击 创建，然后单击 关闭。

为多个域的 **LDAP** 组提取创建组和绑定策略

February 1, 2024

创建身份验证策略后，您可以在 NetScaler Gateway 上创建组。创建组后，将身份验证策略绑定到虚拟服务器。

在 **NetScaler Gateway** 上创建组

1. 在配置实用程序中的 配置 选项卡的导航窗格中，展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，单击“添加”。
3. 在 组名称中，键入第一个 Active Directory 组的名称。
   重要：在 NetScaler Gateway 上创建用于从多个域中提取组的组时，组名称必须与您在 Active Directory 中定义的组相同。组名也区分大小写，大小写必须与您在 Active Directory 中输入的大小写匹配。
4. 在“策 略”选项卡上，单击“会话”，然后单击“插入策略”。
5. 在“策略名称”下，双击该策略，然后单击“创建”。

将身份验证策略绑定到虚拟服务器

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在身份验证选项卡上，单击 主要的，在 策略名称下，双击 插入策略，然后选择第一个身份验证策略。
4. 在 策略名称下，单击 插入策略，双击第二个身份验证策略，然后单击 确定。

LDAP 身份验证的 **14** 天密码到期通知

February 1, 2024

NetScaler Gateway 设备支持基于 LDAP 的身份验证的 14 天密码到期通知。通过使用此功能，管理员可以通知最终用户密码过期阈值时间（以天为单位）。有关更多详细信息，请参阅 LDAP 身份验证的 14 天密码到期通知。

配置客户端证书身份验证

February 1, 2024

登录 NetScaler Gateway 虚拟服务器的用户也可以根据提供给虚拟服务器的客户端证书属性进行身份验证。客户端证书身份验证也可以与其他身份验证类型（例如 LDAP 或 RADIUS）一起使用，以提供双重身份验证。

要根据客户端证书属性对用户进行身份验证，必须在虚拟服务器上启用客户端身份验证，并且必须请求客户端证书。必须在 NetScaler Gateway 上将根证书与虚拟服务器绑定在一起。

当用户登录 NetScaler Gateway 虚拟服务器时，身份验证后，将从证书的指定字段中提取用户名信息。此字段通常为 Subject:CN。如果成功提取用户名，则用户将通过身份验证。在以下情况下，身份验证失败。

- 如果用户在安全套接字层 (SSL) 握手期间未提供有效的证书。

- 用户名提取失败，身份验证失败。

可以通过将默认身份验证类型设置为使用客户端证书，基于客户端证书对用户进行身份验证。还可以基于客户端 SSL 证书创建一个证书操作，用于定义身份验证过程中要执行的操作。

使用 **GUI** 将客户端证书配置为默认身份验证类型

1. 转到“配置”**>** “**NetScaler Gateway**”，然后单击“全局设置”。
2. 在详细信息窗格中的 身份验证设置下，单击 更改身份验证证书设置。
3. 选择 开 以根据需要使用证书启用双重身份验证。
4. 在 用户名字段中，选择包含用户名的证书字段的类型。
5. 在 组名字段中，选择包含组名的证书字段的类型。
6. 在 默认授权组中，键入默认组的名称，然后单击 确定。

从客户端证书中提取用户名

如果在 NetScaler Gateway 上启用了客户端证书身份验证，则将基于客户端证书的某些属性对用户进行身份验证。身份验证成功后，将从证书中提取用户的用户名或用户名和组名。此外，还会应用为该用户指定的策略。

配置和绑定客户端证书身份验证策略

February 1, 2024

您可以创建客户端证书身份验证策略并将其绑定到虚拟服务器。您可以使用策略限制对特定组或用户的访问。此策略优先于全局策略。

要配置客户端证书身份验证策略：

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 在导航窗格中的“身份验证”下，单击 **CERT**。
3. 在详细信息窗格中，单击“添加”。
4. 在 名称 字段中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在名称中，键入配置文件的名称。
7. 在“双因素”旁边，选择“关”。
8. 在“用户名”字段和“组名”字段中，选择值，然后单击并创建。
   注意：如果之前已将客户端证书配置为默认身份验证类型，请使用与策略相同的名称。如果您填写了默认身份验证类型的“用
   户名”字段和“
   组名”字段，请为配置文件使用相同的值。

9. 在“创建身份验证策略”对话框中，选择“命名表达式”旁边的表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

要将客户端证书策略绑定到虚拟服务器：

配置客户端证书身份验证策略后，可以将其绑定到虚拟服务器。

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击“打开”。
3. 在“配置 **NetScaler Gateway** 虚拟服务器”对话框中，单击“身份验证”选项卡。
4. 单击“主”或“辅助”。
5. 在 详细信息下，单击 插入策略。
6. 在“策略名称”中，选择策略，然后单击“确定”。

要配置虚拟服务器以请求客户端证书，请执行以下

如果要使用客户端证书进行身份验证，则必须配置虚拟服务器，以便在 SSL 握手期间请求客户端证书。

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击 虚拟服务器，然后单击 打开。
3. 在 证 书选项卡上，单击 **SSL** 参数。
4. 在 其他下，单击 客户端身份验证。
5. 在 客户端证书中，选择 可选 或 强制，然后单击确定两次。如果要在同一虚拟服务器上允许其他身份验证类型且不需要使用客户端证书，请选择 可 选。

> 注意
>
> - 有关回调 URL 的详细信息，请参阅 导入 NetScaler Gateway。
> - 有关证书的详细信息，请参阅 安装、链接和更新证书。

配置双重客户端证书身份验证

February 1, 2024

您可以将客户端证书配置为首先对用户进行身份验证，然后要求用户使用辅助身份验证类型（例如 LDAP 或 RADIUS）登录。在这种情况下，客户端证书首先对用户进行身份验证。然后，将显示一个登录页面，他们可以在其中输入用户名和密码。安全套接字层 (SSL) 握手完成后，登录序列可以采用以下两种路径之一：

- 不会从证书中提取用户名和组。用户会看到登录页面，提示您输入有效的登录凭据。NetScaler Gateway 会像普通密码身份验证一样对用户凭据进行身份验证。
- 用户名和组名是从客户端证书中提取的。如果仅提取用户名，则会向存在登录名的用户显示登录页面，用户无法修改该名称。只有密码字段为空。

NetScaler Gateway 在第二轮身份验证期间提取的组信息将附加到 NetScaler Gateway 从证书中提取的组信息（如果有）。

配置智能卡身份验证

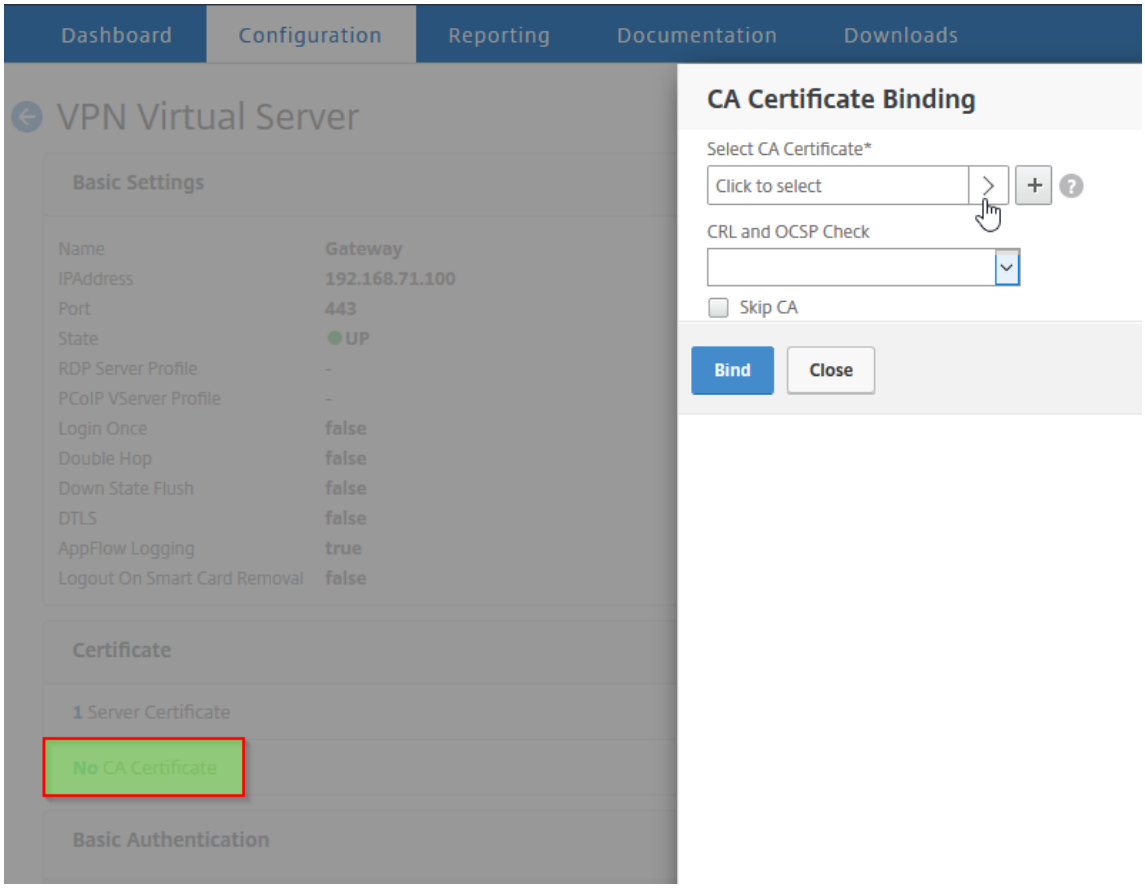
February 1, 2024

您可以将 NetScaler Gateway 配置为使用加密智能卡对用户进行身份验证。

要使用 NetScaler Gateway 配置智能卡，您需要执行以下操作：

- 创建证书身份验证策略。有关详细信息，请参阅 配置客户端证书验证。
- 将身份验证策略绑定到虚拟服务器。
- 将颁发客户端证书的证书颁发机构 (CA) 的根证书添加到 NetScaler Gateway。有关详细信息，请参阅在 NetScaler Gateway 上安装根证书。

  重要：将根证书添加到虚拟服务器以进行智能卡身份验证时，必须从选择 **CA** 证书列表中选择证书。



创建客户端证书后，您可以将称为闪存的证书写入智能卡。完成该步骤后，您可以测试智能卡。

如果为智能卡直通身份验证配置 Web Interface，如果存在以下任一情况，单点登录 Web Interface 将失败：

- 如果改为将“已发布的应用程序”选项卡上的域设置为 `mydomain`.com 而非 `mydomain`。
- 如果未在“已发布的应用程序”选项卡上设置域名，并且如果运行将值设置为 1 的命令 `wi-sso-split-upn`。在这种情况下，用户主名称包含域名“`mydomain`.com”。

您可以使用智能卡身份验证来简化用户的登录过程，同时还可以增强用户访问基础架构的安全性。对内部企业网络的访问受基于证书的使用公钥基础结构的双重身份验证所保护。私钥受硬件控制保护，离不开智能卡。使用智能卡和 PIN，用户可以方便地从一系列的企业设备访问其桌面和应用程序。

可以使用智能卡实现 StoreFront 对用户的身份验证，以访问 Citrix Virtual Apps and Desktops 提供的桌面和应用程序。登录 StoreFront 的智能卡用户还可以访问 NetScaler Endpoint Management 提供的应用程序。但是，用户必须再次进行身份验证，才能访问使用客户端证书身份验证的 Endpoint Management

有关更多信息，请参阅 StoreFront 文档中的 配置智能卡身份验证 。

使用安全 **ICA** 连接配置智能卡身份验证

使用 NetScaler Gateway 上配置了单点登录的智能卡登录并建立安全 ICA 连接的用户可能会收到两次提示输入其个人标识号 (PIN) 的提示。

- 登录时和尝试启动已发布资源时。如果 Web 浏览器和 Citrix Workspace 应用程序使用的虚拟服务器配置为使用客户端证书，则会出现这种情况。
- Citrix Workspace 应用程序不会与 Web 浏览器共享进程或安全套接字层 (SSL) 连接。因此，当 ICA 连接完成与 NetScaler Gateway 的 SSL 握手时，第二次需要客户端证书。

要防止用户收到第二个 PIN 提示，您必须更改两个设置：

- 必须禁用 VPN 虚拟服务器上的客户端身份验证。
- 必须启用 SSL 重新协商。

配置虚拟服务器后，将一个或多个 STA 服务器绑定到虚拟服务器，如在 Web Interface 5.3 中配置 NetScaler Gateway 设置中所述。

您可能还想测试智能卡身份验证。

要禁用客户端身份验证：

1. 在配置实用程序的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在主详细信息窗格中选择相关的虚拟服务器，然后单击编辑。
3. 在“高级选项”窗格中，单击“SSL 参数”。
4. 清除“客户端身份验证”复选框。
5. 单击 Done（完成）。

要启用 SSL 重新协商：

1. 使用配置实用程序，从“配置”选项卡中导航到“流量管理”，然后单击“SSL”。
2. 在主面板中，单击更改高级 SSL 设置。
3. 从“拒绝 SSL 重新协商”菜单中，选择“否”。

要测试智能卡身份验证：

1. 将智能卡连接到用户设备。
2. 打开 Web 浏览器并登录 NetScaler Gateway。

配置 **RADIUS** 身份验证

February 1, 2024

您可以将 NetScaler Gateway 配置为通过一个或多个 RADIUS 服务器验证用户访问权限。如果您使用的是 RSA SecurID、SafeWord 或金雅拓 Protiva 产品，则这些产品中的每一个都是使用 RADIUS 服务器进行配置的。

您的配置可能需要使用网络访问服务器 IP 地址 (NAS IP) 或网络访问服务器标识符 (NAS ID)。将 NetScaler Gateway 配置为使用 RADIUS 身份验证服务器时，请遵循以下准则：

- 如果启用 NAS IP 的使用，则设备会将其配置的 IP 地址发送到 RADIUS 服务器，而不是建立 RADIUS 连接时使用的源 IP 地址。
- 如果配置 NAS ID，设备会将标识符发送到 RADIUS 服务器。如果不配置 NAS ID，则设备将其主机名发送到 RADIUS 服务器。
- 启用 NAS IP 时，设备将忽略使用 NAS IP 配置为与 RADIUS 服务器通信的任何 NAS ID。

配置金雅拓 **Protiva**

Protiva 是金雅拓为利用金雅拓智能卡身份验证的优势而开发的强大身份验证平台。使用 Protiva，用户可以使用 Protiva 设备生成的用户名、密码和一次性密码登录。与 RSA SecurID 类似，身份验证请求被发送到 Protiva 身份验证服务器，服务器验证或拒绝密码。要将金雅拓 Protiva 配置为与 NetScaler Gateway 兼容，请使用以下准则：

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装可扩展 Internet Authentication Server (IAS) 的 Protiva SAS 代理软件。确保记下 IAS 服务器的 IP 地址和端口号。
- 在 NetScaler Gateway 上配置 RADIUS 身份验证配置文件，然后输入 Protiva 服务器的设置。

配置 **SafeWord**

SafeWord 产品线使用基于令牌的密码提供安全身份验证。用户输入密码后，SafeWord 会立即使密码失效，并且无法再次使用。配置 SafeWord 服务器时，您需要以下信息：

- NetScaler Gateway 的 IP 地址。IP 地址必须与您在 RADIUS 服务器客户端配置中配置的 IP 地址相同。NetScaler Gateway 使用内部 IP 地址与 RADIUS 服务器进行通信。配置共享密钥时，应使用内部 IP 地址。如果配置两台设备以实现高可用性，请使用虚拟内部 IP 地址。
- 一个共享的秘密。
- SafeWord 服务器的 IP 地址和端口。默认端口号为 1812。

配置 **RADIUS** 身份验证

February 1, 2024

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 单击 RADIUS，然后在详细信息窗格的策略选项卡上，单击添加。
3. 在“创建身份验证策略”对话框的“名称”中，键入策略的名称。
4. 在名称中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在“创建身份验证策略”对话框的“名称”中，键入服务器的名称。
7. 在服务器下的 IP 地址中，键入 RADIUS 服务器的 IP 地址。
8. 在端口中，键入端口。默认值为 1812。
9. 在详细信息下的私有密钥和确认私有密钥中，键入 RADIUS 服务器密钥。
10. 在 NAS ID 中，键入标识符号，然后单击创建。
11. 在“创建身份验证策略”对话框中，选择“命名表达式”旁边的表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

选择 **RADIUS** 身份验证协议

February 1, 2024

NetScaler Gateway 支持配置为使用多种协议进行用户身份验证的 RADIUS 实现，包括：

- 密码身份验证协议 (PAP)
- 挑战握手身份验证协议 (CHAP)
- Microsoft 质询握手身份验证协议（MS-CHAP 版本 1 和版本 2）

如果您的 NetScaler Gateway 部署配置为使用 RADIUS 身份验证，并且 RADIUS 服务器配置为使用 PAP，则可以通过向 RADIUS 服务器分配强共享密钥来加强用户身份验证。强 RADIUS 共享密钥由大写和小写字母、数字和标点的随机序列组成，长度至少为 22 个字符。如果可能的话，使用随机字符生成程序来确定 RADIUS 共享机密。

要进一步保护 RADIUS 流量，请为每个 NetScaler Gateway 设备或虚拟服务器分配不同的共享密钥。在 RADIUS 服务器上定义客户端时，还可以为每个客户端分配单独的共享密钥。如果执行此操作，则必须单独配置使用 RADIUS 身份验证的每个 NetScaler Gateway 策略。

创建 RADIUS 策略时，可以在 NetScaler Gateway 上配置共享密钥作为策略的一部分。

配置 **IP** 地址提取

February 1, 2024

您可以将 NetScaler Gateway 配置为从 RADIUS 服务器中提取 IP 地址。当用户向 RADIUS 服务器进行身份验证时，服务器将返回分配给该用户的带框的 IP 地址。在访问请求中，框架 IP 地址也称为 RADIUS 属性 8 帧 IP 地址。

以下是 IP 地址提取的组件：

- 允许远程 RADIUS 服务器从内部网络为登录 NetScaler Gateway 的用户提供 IP 地址。
- 允许使用 **ipaddress** 类型配置任何 RADIUS 属性，包括供应商编码的属性。

配置 RADIUS 服务器进行 IP 地址提取时，您可以配置供应商标识符和属性类型。供应商 ID 和属性用于在 RADIUS 客户端和 RADIUS 服务器之间建立关联。

- 供应商标识符 (ID) 使 RADIUS 服务器能够从 RADIUS 服务器上配置的 IP 地址池中为客户端分配 IP 地址。供应商 ID 是 RADIUS 响应中提供内部网络 IP 地址的属性。值为零表示该属性未经供应商编码
- 属性类型是 RADIUS 响应中的远程 IP 地址属性。最小值为 1，最大值为 255。

常见的配置是提取 RADIUS 属性成 帧的 **IP** 地址。供应商 ID 设置为 0 或未指定。属性类型设置为 8。

要使用 **GUI** 从 **RADIUS** 服务器配置 **IP** 地址提取，请执行以下操作：

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证，然后单击 **RADIUS**。
2. 在 详细信息 窗格的 策 略选项卡上，选择 RADIUS 策略，然后单击 打开。
3. 在“配置身份验证策略”对话框中，单击“服务器”旁边的“修改”。
4. 在 详细信息下的 组供应商标识符中，键入值。
5. 在“组属性类型”中，键入值，然后单击“确定”两次。

配置 **RADIUS** 组提取

February 1, 2024

您可以使用称为组提取的方法配置 RADIUS 授权。配置组提取允许您管理 RADIUS 服务器上的用户，而不是将其添加到 NetScaler Gateway。

您可以使用身份验证策略并配置组供应商标识符 (ID)、组属性类型、组前缀和组分隔符来配置 RADIUS 授权。配置策略时，需要添加表达式，然后将策略全局绑定或绑定到虚拟服务器。

在 **Windows Server 2003** 上配置 **RADIUS**

如果在 Windows Server 2003 上使用 Microsoft Internet Authentication Service (IAS) 进行 RADIUS 授权，则在配置 NetScaler Gateway 期间，您需要提供以下信息：

- 供应商 ID 是您在 IAS 中输入的特定于供应商的代码。
- Type 是供应商分配的属性编号。
- 属性名称是您在 IAS 中定义的属性名称的类型。默认名称是 CTXSUserGroups=

如果 RADIUS 服务器上未安装 IAS，则可以通过控制面板中的添加或删除程序进行安装。有关详细信息，请参阅 Windows 联机帮助。

要配置 IAS，请使用 Microsoft 管理控制台 (MMC) 并安装 IAS 的管理单元。按照向导操作，确保选择以下设置：

- 选择本地计算机。
- 选择远程访问策略并创建自定义策略。
- 为策略选择 Windows 组。
- 选择以下协议之一：
  - Microsoft 质询握手身份验证协议版本 2 (MS-CHAP v2)
  - Microsoft 质询握手身份验证协议 (MS-CHAP)
  - 挑战握手身份验证协议 (CHAP)
  - 未加密的身份验证（PAP、SPAP）
- 选择供应商特定的属性。

  供应商特定属性需要将您在服务器上的组中定义的用户与 NetScaler Gateway 上的用户进行匹配。为满足此要求，请将供应商特定的属性发送到 NetScaler Gateway。确保选择 RADIUS = 标准。
- RADIUS 的默认值为 0。使用此编号作为供应商代码。
- 供应商分配的属性编号为 0。

  这是为“用户组”属性分配的编号。该属性为字符串格式。
- 为属性格式选择字符串。

  属性值需要属性名称和组。

  对于接入网关，属性值为 CTXSUserGroups=groupname。如果定义了两个组，例如销售和财务，则属性值为 CTXSUserGroups=sales;finance。用分号分隔每个组。
- 删除“编辑拨入配置文件”对话框中的所有其他条目，保留显示供应商特定的条目。

在 IAS 中配置远程访问策略后，可以在 NetScaler Gateway 上配置 RADIUS 身份验证和授权。

配置 RADIUS 身份验证时，请使用您在 IAS 服务器上配置的设置。

在 **Windows Server 2008** 上配置 **RADIUS** 进行身份

在 Windows Server 2008 上，您可以使用网络策略服务器 (NPS) 来配置 RADIUS 身份验证和授权，该服务器取代了互联网身份验证服务 (IAS)。要安装 NPS，可以使用“服务器管理器”并将 NPS 添加为角色。

安装 NPS 时，选择网络策略服务。安装完成后，您可以通过从“开始”菜单上的“管理服务”启动 NPS 来为网络配置 RADIUS 设置。打开 NPS 时，可以将 NetScaler Gateway 添加为 RADIUS 客户端，然后配置服务器组。

配置 RADIUS 客户端时，请确保选择以下设置：

- 对于供应商名称，请选择 RADIUS 标准。
- 记下共享密钥，因为您需要在 NetScaler Gateway 上配置相同的共享密钥。

对于 RADIUS 组，您需要 RADIUS 服务器的 IP 地址或主机名。不要更改默认设置。

配置 RADIUS 客户端和组后，可以在以下两个策略中配置设置：

- 连接请求策略，您可以在其中配置 NetScaler Gateway 连接的设置，包括网络服务器的类型、网络策略的条件以及策略的设置。
- 用于配置可扩展身份验证协议 (EAP) 身份验证和供应商特定属性的网络策略。

配置连接请求策略时，为网络服务器的类型选择未指定。然后，您可以通过选择 NAS 端口类型作为条件，选择虚拟 (VPN) 作为值来配置条件。

配置网络策略时，需要配置以下设置：

- 选择远程访问服务器（VPN 拨号）作为网络访问服务器的类型。
- 为 EAP 选择加密身份验证 (CHAP) 和未加密身份验证（PAP 和 SPAP）。
- 为供应商特定属性选择 RADIUS 标准。

  默认属性编号为 26。此属性用于 RADIUS 授权。

  NetScaler Gateway 需要供应商特定的属性才能将服务器上组中定义的用户与 NetScaler Gateway 上的用户进行匹配。这是通过将供应商特定的属性发送到 NetScaler Gateway 来完成的。

- 选择字符串作为属性格式。

  属性值需要属性名称和组。

  对于 NetScaler Gateway，属性值为 CTXSUserGroups= groupname。如果定义了两个组，例如销售和财务，则属性值为 CTXSUserGroups=sales;finance。用分号分隔每个组。

- 分隔符是您在 NPS 上用来分隔组的分隔符，例如分号、冒号、空格或句点。

在 IAS 中配置完远程访问策略后，可以在 NetScaler Gateway 上配置 RADIUS 身份验证和授权。

配置 **RADIUS** 授权

February 1, 2024

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 单击 RADIUS。
3. 在策略选项卡中，单击添加。
4. 在名称中，键入策略的名称。
5. 在服务器下方 * 单击 +
6. 在名称中，键入 RADIUS 服务器的名称。
7. 在服务器下，键入 RADIUS 服务器的 IP 地址和端口。
8. 在详细信息下，输入组供应商标识符和组属性类型的值。
9. 在密码编码中，选择身份验证协议，然后单击创建。
10. 在“创建身份验证策略”对话框中，选择“命名表达式”旁边的表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **RADIUS** 用户记帐

February 1, 2024

NetScaler Gateway 可以向 RADIUS 会计服务器发送用户会话开始和停止消息。为每个用户会话发送的消息包含 RFC2866 中定义的属性的子集。表 1 列出了支持的属性以及发送它们的 RADIUS 记帐消息的类型（RAD_START 和 RAD_STOP）。表 2 列出了可分配给 `Acct-Terminate-Cause` 属性的预定义值以及相应的 NetScaler Gateway 事件。

表 1. 支持的 RADIUS 属

属性	含义	RAD_START	RAD_STOP
用户名称	与会话关联的用户的名称。	X	X
Session-Id	NetScaler 会话 ID。	X	X
Acct-Session-Time	会话持续时间秒。		X
Acct-Terminate-Cause	帐户终止的原因。		X

表 2. RADIUS 终止原因

NetScaler 注销方法	RADIUS 终止原因
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
其他	RAD_TERM_NAS_ERROR

配置 RADIUS 用户记帐需要创建一对策略。第一个策略是 RADIUS 身份验证策略，它指定要向其发送记帐消息的 RADIUS 服务器。第二个是使用 RADIUS 记帐策略作为其操作的会话策略。

要配置 RADIUS 用户记帐，您必须：

1. 创建 RADIUS 策略以定义 RADIUS 记帐服务器。记帐服务器可以是用于 RADIUS 身份验证的同一台服务器。
2. 创建会话策略，使用 RADIUS 策略作为指定 RADIUS 用户记帐服务器的操作。
3. 全局绑定会话策略，使其应用于所有流量或 NetScaler Gateway 虚拟服务器，以便仅应用于流经该虚拟服务器的流量。

创建 **RADIUS** 策略

1. 在配置实用程序的导航窗格中，展开 NetScaler Gateway 节点，然后展开策略。
2. 展开身份验证并选择 RADIUS。
3. 在详细信息窗格的“策略”选项卡上，单击“添加”。
4. 输入策略的名称。
5. 从“服务器”菜单中选择服务器，或单击 + 图标并按照提示添加新的 RADIUS 服务器。
6. 在“表达式”窗格中，从“已保存的策略表达式”菜单中选择 ns_true。
7. 单击创建。

创建会话策略

配置指定 RADIUS 记帐服务器的 RADIUS 策略后，创建在操作中应用此记帐服务器的会话策略，如下所示：

1. 在配置实用程序的导航窗格中，展开 NetScaler Gateway 节点，然后展开策略。
2. 选择 会话。
3. 在主详细信息窗格中，选择添加。
4. 输入策略的名称。
5. 在“操作”菜单中，单击 + 图标以添加新的会话操作。
6. 输入会话操作的名称。
7. 单击“客户端体验”选项卡。
8. 在“会计策略”菜单中，选择您之前创建的 RADIUS 策略。
9. 单击创建。
10. 在“表达式”窗格中，从“已保存的策略表达式”菜单中选择 ns_true。
11. 单击创建。

全局绑定会话策略

1. 在配置实用程序的导航窗格中，展开 NetScaler Gateway 节点，然后展开策略。
2. 选择 会话。
3. 从主详细信息窗格的“操作”菜单中，选择“全局绑定”。
4. 单击绑定。
5. 在“策略”窗格中，选择您之前创建的会话策略，然后单击“插入”。
6. 在策略列表中，单击会话策略的优先级条目，然后输入一个介于 0 到 64000 之间的值。
7. 单击确定。

将会话策略绑定到 **NetScaler Gateway** 虚拟服务器

1. 在配置实用程序的导航窗格中，展开 NetScaler Gateway 节点，然后选择虚拟服务器。
2. 在主详细信息窗格中，选择虚拟服务器，然后单击编辑。
3. 在“策略”窗格中，单击 + 图标以选择策略。
4. 从“选择策略”菜单中选择“会话”，然后确保在“选择类型”菜单中选择了“请求”。
5. 单击继续。
6. 单击绑定。
7. 在“策略”窗格中，选择您之前创建的会话策略，然后单击“插入”。
8. 单击确定。

配置 **SAML** 身份验证

February 1, 2024

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在身份提供商 (IdP) 和服务提供商之间交换身份验证和授权。NetScaler Gateway 支持 SAML 身份验证。

配置 SAML 身份验证时，需要创建以下设置：

- IdP 证书名称。这是与 IdP 上的私钥对应的公钥。
- 重定向 URL。这是身份验证 IdP 的 URL。未经身份验证的用户将被重定向到此 URL。
- 用户字段。如果 IdP 使用与主题标记的 NameIdentifier 标签不同的格式发送用户名，则可以使用此字段提取用户名。这是一个可选设置。
- 签名证书名称。这是 NetScaler Gateway 服务器的私钥，用于对 IdP 的身份验证请求进行签名。如果未配置证书名称，则断言将以未签名方式发送，或者身份验证请求将被拒绝。
- SAML 发行人名称。发送身份验证请求时使用此值。发行者字段中必须有一个唯一的名称来表示发送断言的权限。此字段为可选字段。
- 默认身份验证组。这是身份验证服务器上用于对用户进行身份验证的组。
- 两个因素。此设置启用或禁用双因素身份验证。
- 拒绝无符号断言。如果启用，如果未配置签名证书名称，NetScaler Gateway 将拒绝用户身份验证。

NetScaler Gateway 支持 HTTP 后绑定。在此绑定中，发送方用 200 OK 回复用户，其中包含带有所需信息的表单自动发布。具体而言，默认表单必须包含两个名为 `SAMLRequest` 和 `SAMLResponse` 的隐藏字段，具体取决于表单是请求还是响应。该表单还包括 RelayState，这是发送方用来发送未经依赖方处理的任意信息的状态或信息。依赖方将信息发送回去，这样当发送方与 RelayState 一起收到断言时，发送方知道下一步该怎么做。建议您对 RelayState 进行加密或模糊处理。

> 注意
>
> - 当使用 NetScaler Gateway 作为 Citrix Cloud 的 IdP 时，您无需在 NetScaler Gateway 上配置 **RelayState** 规则。
> - 如果是 IdP 链接，则仅在第一个 SAML 策略上配置 **RelayState** 规则就足够了。在这种情况下，IdP 链接是指配置的 SAML 操作指的是包含另一个 SAML 操作的身份验证虚拟服务器 IdP 的场景。

配置 **Active Directory** 联合服务 **2.0**

您可以在以联合服务器角色使用的任何 Windows Server 2008 或 Windows Server 2012 计算机上配置 Active Directory 联合身份验证服务 (AD FS) 2.0。将 ADFS 服务器配置为与 NetScaler Gateway 兼容时，需要使用 Windows Server 2008 或 Windows Server 2012 中的“信赖方信任向导”配置以下参数。

Windows Server 2008 年参数：

- 信赖方信托。您可以提供 NetScaler Gateway 元数据文件位置，例如 https://vserver.fqdn.com/ns.metadata.xml，其中 vserver.fqdn.com 是 NetScaler Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- 授权规则。您可以允许或拒绝用户访问信赖方。

Windows Server 2012 年参数：

- 信赖方信托。您可以提供 NetScaler Gateway 元数据文件位置，例如 https://vserver.fqdn.com/ns.metadata.xml，其中 vserver.fqdn.com 是 NetScaler Gateway 虚拟服务器的完全限定域名 (FQDN)。您可以在绑定到虚拟服务器的服务器证书上找到 FQDN。
- AD FS 配置文件。选择 AD FS 配置文件。
- 证书。NetScaler Gateway 不支持加密。您不需要选择证书。
- 启用对 SAML 2.0 WebSSO 协议的支持。这将启用对 SAML 2.0 SSO 的支持。您可以提供 NetScaler Gateway 虚拟服务器 URL，例如 https:netScaler.virtualServerName.com/cgi/samlauth。

  此 URL 是 NetScaler Gateway 设备上的断言使用者服务 URL。这是一个常量参数，NetScaler Gateway 期望在此 URL 上收到 SAML 响应。
- 信赖方信任标识符。输入名称 NetScaler Gateway。这是一个用于标识信赖方的 URL，例如 https://netscalerGateway.virtualServerName.com/adfs/services/trust。
- 授权规则。您可以允许或拒绝用户访问信赖方。
- 配置声明规则。您可以使用发行转换规则配置 LDAP 属性的值，也可以使用模板将 LDAP 属性作为声明发送。然后，您可以配置 LDAP 设置，其中包括：
  - 电子邮件地址
  - sAMAccountName
  - User Principal Name (UPN)（用户主体名称 (UPN)）
  - MemberOf
- 证书签名。您可以通过选择中继方的属性然后添加证书来指定签名验证证书。

  如果签名证书小于 2048 位，则会显示一条警告消息。您可以忽略警告以继续操作。如果要配置测试部署，请在中继方上禁用证书吊销列表 (CRL)。如果不禁用检查，AD FS 会尝试 CRL 验证证书。

  您可以通过运行以下命令来禁用 CRL：Set-ADFWRelayingPartyTrust - SigningCertficateRevocatonCheck None-TargetName NetScaler

配置设置后，请在完成中继方信任向导之前验证信赖方数据。您可以使用终端节点 URL 检查 NetScaler Gateway 虚拟服务器证书，例如 https://vserver.fqdn.com/cgi/samlauth。

在中继方信任向导中完成配置设置后，选择已配置的信任，然后编辑属性。执行以下操作：

- 将安全哈希算法设置为 SHA-1。

  注意：NetScaler 仅支持 SHA-1。

- 删除加密证书。不支持加密断言。
- 编辑索赔规则，包括以下内容：
  - 选择转换规则
  - 添加声明规则
  - 选择声明规则模板：将 LDAP 属性作为声明发送
  - 给个名字
  - 选择属性存储：Active Directory
  - 选择 LDAP 属性：<Active Directory parameters>
  - 选择外出索赔规则作为“名称 ID”

  注意：不支持属性名称 XML 标记。
- 配置单点注销的注销 URL。声明规则是发送注销 URL。自定义规则必须是以下内容：

```
pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
.fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
/2005/05/identity/claimproperties/attributename"] = "urn:oasis:
names:tc:SAML:2.0:attrname-format:unspecified"); <!--NeedCopy-->
```

配置 AD FS 设置后，下载 AD FS 签名证书，然后在 NetScaler Gateway 上创建证书密钥。然后，您可以使用证书和密钥在 NetScaler Gateway 上配置 SAML 身份验证。

配置 **SAML** 双因素身份验证

您可以配置 SAML 双因素身份验证。使用 LDAP 身份验证配置 SAML 身份验证时，请遵循以下准则：

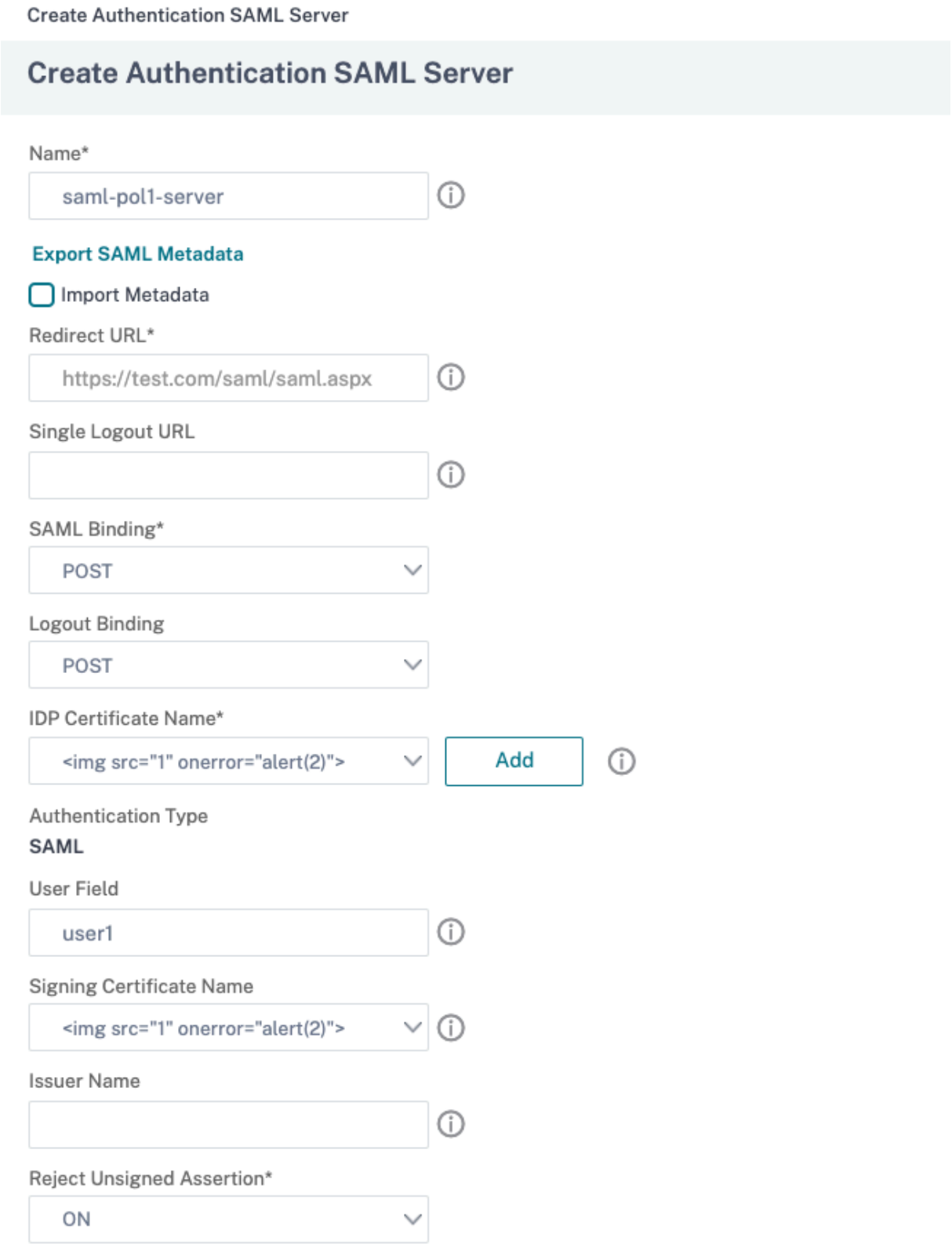
- 如果 SAML 是主要身份验证类型，请在 LDAP 策略中禁用身份验证并配置组提取。然后，将 LDAP 策略绑定为辅助身份验证类型。
- SAML 身份验证不使用密码，只使用用户名。此外，SAML 身份验证仅在身份验证成功时通知用户。如果 SAML 身份验证失败，则不会通知用户。由于未发送失败响应，SAML 必须是级联中的最后一个策略或唯一的策略。
- 建议您配置实际的用户名而不是不透明的字符串。
- SAML 不能绑定为辅助身份验证类型。

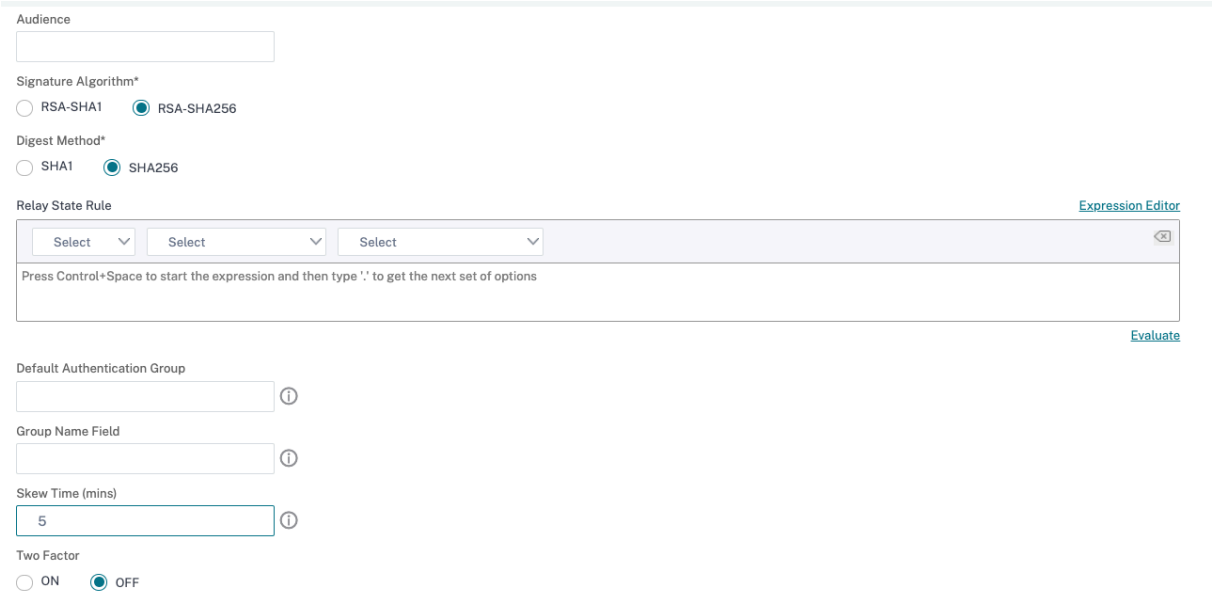
配置 **SAML** 身份验证

February 1, 2024

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 在导航窗格中，单击 **SAML**。

3. 在详细信息窗格中，单击“添加”。
4. 在“创建身份验证策略”对话框的“名称”中，键入策略的名称。





1. 在“服务器”旁边，单击“新建”。
2. 在 名称中，键入服务器配置文件的名称。
3. 在 IdP 证书名称中，选择一个证书或单击 安装。这是安装在 SAML 或 IdP 服务器上的证书。

   如果单击“安装”，请添加证书和私钥。有关详细信息，请参阅安装和管理证书。
4. 在 重定向 **URL** 中，输入身份验证身份提供程序 (IdP) 的 URL。

   这是用户登录 SAML 服务器的 URL。这是 NetScaler Gateway 将初始请求重定向到的服务器。
5. 在 单一注销 **URL** 中，指定 URL，以便设备能够识别何时将客户端发送回 IdP 以完成注销过程。
6. 在 **SAML** 绑定中，选择用于将客户端从 SP 移动到 IdP 的方法。这在 IdP 上必须是相同的，这样它才能理解客户端如何连接到它。当设备充当 SP 时，它支持开机自检、重定向和工件绑定。
7. 在 注销绑定中，选择 重定向。
8. 在 **IDP** 证书名称中，选择 SAML 签名证书下的 IdPCert 证书 (Base64)。

   > 注意：
   >
   > 您也可以单击 导入元数据，然后选择存储元数据配置的 URL。

9. 在 用户字段中，输入要提取的用户名。
10. 在 签名证书名称中，选择设备用于签署对 IdP 的身份验证请求的 SAML SP 证书（带有私钥）。必须将相同的证书（不带私钥）导入到 IdP，以便 IdP 可以验证身份验证请求签名。大多数 IdP 不需要此字段

    这是绑定到 NetScaler Gateway 虚拟 IP 地址的证书。SAML 颁发者名称是用户登录的完全限定域名 (FQDN)，例如 lb.example.com 或 ng.example.com。
11. 在 颁发者名称中，输入负载平衡的 FQDN 或设备向其发送初始身份验证 (GET) 请求的 NetScaler Gateway 虚拟 IP 地址。

12. 在 拒绝无符号断言中，指定是否需要对来自 IdP 的断言进行签名。您可以确保只有断言必须签名 (开) 或者断言和 IdP 的响应都必须签名 (STICT)。
13. 在 受众中，输入 IdP 发送的断言适用的受众。这通常是表示服务提供商的实体名称或 URL。
14. 在 签名算法中，选择 RSA-SHA256
15. 在 摘要方法中，选择 SHA256
16. 在 默认身份验证组中，输入身份验证成功时选择的默认组以及提取的组。
17. 在 组名称中，输入包含用户组的断言中标记的名称。
18. 在 **Skew Time (mins)** 中，指定服务提供商在传入断言上允许的时钟偏差（以分钟为单位）。
19. 单击“创建”，然后单击“关闭”。
20. 在创建身份验证策略对话框的命名表达式旁边，选择常规，选择 True 值，单击 添加表达式，单击 创建，然后单击 关闭。

引用

- 作为 SAML SP 的 NetScaler
- NetScaler 作为 SAML IdP
- SAML 支持的其他功能

使用 **SAML** 身份验证登录 **NetScaler Gateway**

February 1, 2024

您可以使用 SAML 身份验证使用 VPN 客户端和 Workspace 应用程序登录 NetScaler Gateway。该插件仅支持通过绑定到身份验证虚拟服务器的高级 SAML 策略（即 nFactor 身份验证）进行 SAML 身份验证。

重要：当 SAML 策略直接绑定到 VPN 虚拟服务器（即非 nFactor 身份验证）时，插件不支持 SAML 身份验证。

支持的平台和应用

下表列出了支持用于登录 NetScaler Gateway 的 SAML 身份验证的平台和应用程序。

产品	版本
NetScaler Gateway	版本 12.0 构建 41.16 及更高版本

产品	版本
VPN 客户端	版本 12.1 构建 49.37 及更高版本。支持的平台：Windows 7、Windows 8、Windows 8.1、Windows 10
Workspace 应用版本	Windows：1808；Mac：1808

使用高级 **SAML** 策略配置 **SAML** 身份验证

有关使用高级 SAML 策略配置 SAML 身份验证的详细信息，请参阅 NetScaler 作为 SAML IdP。

SAML 身份验证中的改进功能

February 1, 2024

此功能需要 SAML 知识、基本的身份验证熟练程度和 FIPS 了解才能使用此信息。

您可以将以下 NetScaler 功能用于与 SAML 2.0 规范兼容的第三方应用程序和服务器：

- SAML 服务提供商 (SP)
- SAML 身份提供商 (IdP)

SP 和 IdP 允许在云服务之间使用单点登录 (SSO)。SAML SP 功能提供了一种解决来自 IdP 的用户声明的方法。IdP 可以是第三方服务或其他 NetScaler 设备。SAML IdP 功能用于断言用户登录并提供 SP 使用的声明。

作为 SAML 支持的一部分，IdP 和 SP 模块都对发送给对等方的数据进行数字签名。数字签名包括来自 SP 的身份验证请求、来自 IdP 的断言以及这两个实体之间的注销消息。数字签名验证消息的真实性。

SAML SP 和 IdP 的当前实现在数据包引擎中执行签名计算。这些模块使用 SSL 证书对数据进行签名。在符合 FIPS 标准的 NetScaler 中，SSL 证书的私钥在数据包引擎或用户空间中不可用，因此当前的 SAML 模块尚未准备好用于 FIPS 硬件。

本文档介绍将签名计算卸载到 FIPS 卡的机制。签名验证是在软件中完成的，因为公钥可用。

解决方案

增强了 SAML 功能集，可以使用 SSL API 进行签名卸载。有关这些受影响的 SAML 子功能的详细信息，请参阅 NetScaler 产品文档：

1. SAML SP 发布绑定—对 AuthnRequest 进行签名
2. SAML IdP Post 绑定-签署断言/响应/两者

3. SAML SP 单一注销方案—在 SP 启动的模型中对 LogoutRequest 进行签名并在 IdP 启动的模型中对 LogoutResponse 进行签名
4. SAML SP 工件绑定—对 ArtifactResolve 请求进行签名
5. SAML SP 重定向绑定—对 AuthnRequest 进行签名
6. SAML IdP 重定向绑定—响应/断言/全部签名
7. SAML SP 加密支持—断言解密

平台

该 API 只能卸载到 FIPS 平台。

配置

卸载配置在 FIPS 平台上自动执行。

但是，由于 FIPS 硬件中的用户空间无法使用 SSL 私钥，因此在 FIPS 硬件上创建 SSL 证书时会发生轻微的配置更改。

以下是配置信息：

- `add ssl fipsKey fips-key`

  创建 CSR 并在 CA 服务器上使用它来生成证书。然后，您可以在中复制该证书 `/nsconfig/ssl`。让我们假设该文件是 fips3cert.cer。

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  然后在 SAML SP 模块的 SAML 操作中指定此证书。

- `set samlAction <name> -samlSigningCertName fips-cert`

  同样，您可以在 SAML IdP 模块的 `samlIdpProfile` 中使用。

- `set samlidpprofile fipstest -samlIdpCertName fips-cert`

FIPS 密钥第一次不可用。如果没有 FIPS 密钥，请按照所述创建 FIPS 密钥。

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent
    (3 | F4)]

create certreq <reqFileName> -fipskeyName <string>
<!--NeedCopy-->
```


配置 **TACACS+** 身份验证

February 1, 2024

您可以配置 TACACS+ 服务器进行身份验证。与 RADIUS 身份验证类似，TACACS+ 使用私钥、IP 地址和端口号。默认端口号为 49。

要将 NetScaler Gateway 配置为使用 TACACS+ 服务器，请提供服务器 IP 地址和 TACACS+ 密钥。只有当正在使用的服务器端口号不是默认端口号 49 时，才需要指定端口。

要使用用户界面配置 TACACS+ 身份验证，请执行以下步骤。

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 单击 **TACACS**。
3. 在详细信息窗格中，单击“添加”。
4. 在 名称 字段中，键入策略的名称。
5. 在“服务器”字段旁边，单击“添加”以创建新的 TACACS 服务器，或单击“编辑”对现有 TACACS 服务器进行更改。
6. 在 名称 字段中，键入服务器的名称。
7. 在“**IP** 地址”下，键入 IP 地址。
8. 在 端口下，使用默认端口号 49。
9. 在 **TACACS** 密钥 字段中，键入密钥。在 确认 **TACACS** 密钥 字段中，键入相同的密钥进行确认。
10. 单击 **More**（更多）。
11. 在 授权中，选择 开，然后单击 创建。
12. 在 创建身份验证 **TACACS** 策略 对话框中，选择表达式，单击创建，然后单击关闭。

要使用命令行界面配置 TACACS+ 身份验证，请键入以下命令。

```
1 add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
     |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
2  -tacacsSecret  }
3
4 [-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
     auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
     defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
     Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
5 [-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
     Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
6 [-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
      [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
     string>]
7 <!--NeedCopy-->
```

在 NetScaler Gateway 中配置 TACACS+ 服务器设置后，绑定策略以使其处于活动状态。您可以在全局或虚拟服务器级别绑定策略。有关绑定身份验证策略的详细信息，请参阅 绑定验证策略。

清除配置基本设置不得清除 **TACACS** 配置

February 1, 2024

本主题重点介绍在运行 clear config 命令时不清除所有与 RBA（基于角色的访问）相关的配置。

当前的 clear config 命令在以下三个级别之一中执行：

- 基本
- 已扩展
- 完全集成

根据级别，NetScaler 配置将被清除并重置为出厂默认设置。

使用的命令是；

```
clear ns config [-force] <level>
<!--NeedCopy-->
```

新命令添加了一个旋钮，允许/拒绝删除所有与 RBA 相关的配置。

新命令

描述的是 Clear RBA 配置功能：

1. 是/否旋钮，默认值：是。

   管理员决定是否保留 RBA 配置。

2. 仅支持清除配置的基本级别。
3. 以下配置未清除：

   - 添加/绑定系统用户/组。
   - 添加 cmd 策略。
   - TACACS 命令（添加 TACACS 操作/策略）。
   - 绑定系统全局

   注意：如果策略绑定到全局系统或清除，则保留与 TACACS 相关的配置（操作/策略）

CLI 配置

使用的命令是；


```
clear config [ - force] <level> [-RBAconfig]
<!--NeedCopy-->
```

默认情况下，它设置为 YES，并根据级别清除配置。

如果—RBAconfig 设置为 NO，则保留与 RBA 相关的配置。包括以下内容：

- 添加/绑定系统用户/组
- 绑定系统全局
- TACACS 相关命令（添加 TACACS 操作/策略）
- 添加 cmd 策略

配置多重身份验证

February 1, 2024

您可以在 NetScaler Gateway 中配置两种类型的多重身份验证：

- 设置身份验证优先级级别的级联身份验证
- 双重身份验证，要求用户通过使用两种类型的身份验证登录

如果您有多个身份验证服务器，则可以设置身份验证策略的优先级。您设置的优先级决定了身份验证服务器验证用户凭据的顺序。具有较低优先级编号的策略优先于具有较高优先级编号的策略。

您可以让用户对两个不同的身份验证服务器进行身份验例如，您可以配置 LDAP 身份验证策略和 RSA 身份验证策略。当用户登录时，他们首先使用自己的用户名和密码进行身份验证。然后，他们使用个人识别码 (PIN) 和 RSA 令牌中的代码进行身份验证。

配置级联身份验证

February 1, 2024

身份验证允许您使用策略优先级来创建多个身份验证服务器的级联。配置级联时，系统会遍历级联策略定义的每个身份验证服务器，以验证用户的凭据。优先级身份验证策略按升序级联，优先级值的范围可以在 1-9999 之间。在全局或虚拟服务器级别绑定策略时，可以定义这些优先级。

在身份验证期间，当用户登录时，首先检查虚拟服务器，然后检查全局身份验证策略。如果用户同时属于虚拟服务器和全局身份验证策略，则首先应用来自虚拟服务器的策略，然后再应用全局身份验证策略。如果希望用户接收全局绑定的身份验证策略，请更改策略的优先级。当全局身份验证策略的优先级编号为 1 且绑定到虚拟服务器的身份验证策略的优先级为 2 时，则全局身份验证策略优先。例如，您可以将三个身份验证策略绑定到虚拟服务器，并且可以设置每个策略的优先级。

如果用户未能根据主级联中的策略进行身份验证，或者该用户成功根据主级联中的策略进行身份验证，但未能根据辅助级联中的策略进行身份验证，身份验证过程将停止，用户将重定向到错误页面。

注意：Citrix 建议在将多个策略绑定到虚拟服务器或全局绑定时，为所有身份验证策略定义唯一的优先级。

设置全局身份验证策略的优先级

1. 在配置实用程序的“配置”选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 选择全局绑定的策略，然后在 操作中单击 全局绑定。
3. 在“绑定/取消绑定身份验证全局策略”对话框的“优先级”下，键入数字，然后单击“确定”。

更改绑定到虚拟服务器的身份验证策略的优先级

您还可以修改绑定到虚拟服务器的身份验证策略。

1. 在配置实用程序的配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“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. 单击“身份验证”选项卡，然后单击“主”或“辅助”。
4. 在身份验证策略旁边的“优先级”下，键入数字，然后单击“确定”。

配置双重身份验证

February 1, 2024

NetScaler Gateway 支持双因素身份验证。通常，在对用户进行身份验证时，NetScaler Gateway 会在通过任何一种配置的身份验证方法成功对用户进行身份验证后立即停止身份验证过程。在某些情况下，您可能需要在一台服务器上对用户进行身份验证，但需要从另一台服务器中提取组。例如，如果您的网络针对 RADIUS 服务器对用户进行身份验证，但您也使用 RSA SecurID 令牌身份验证，并且用户组存储在该服务器上，则可能需要向该服务器对用户进行身份验证，以便提取组。

如果使用两种身份验证类型对用户进行身份验证，并且其中一种类型是客户端证书身份验证，则可以将证书身份验证策略配置为第二种身份验证方法。例如，您使用 LDAP 作为主要身份验证类型，将客户端证书用作辅助身份验证。当用户使用自己的用户名和密码登录时，他们便可以访问网络资源。

配置双重身份验证时，请选择身份验证类型是主要还是辅助类型。

配置双因素身份验证

1. 在配置实用程序的“配置”选项卡上，展开 NetScaler Gateway > 策略 > 身份验证。
2. 在策略选项卡上，单击全局绑定。

3. 在“将身份验证策略绑定/取消绑定到全局”对话框中，单击“主”。
4. 单击“插入策略”。
5. 在策略名称下，选择身份验证策略。
6. 单击“辅助”，重复步骤 4 和 5，然后单击“确定”。

选择单点登录的身份验证类型

February 1, 2024

如果在 NetScaler Gateway 上配置了单点登录和双重身份验证，则可以选择用于单点登录的密码。例如，您已将 LDAP 配置为主要身份验证类型，将 RADIUS 配置为辅助身份验证类型。当用户访问需要单点登录的资源时，默认情况下会发送用户名和主密码。您可以在会话配置文件中设置单点登录 Web 应用程序时必须使用哪个密码。

为单点登录配置身份验证

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略 **>** 会话。
2. 在详细信息窗格中，单击 配置文件 选项卡，然后执行以下操作之一：
   - 要创建新的配置文件，请单击 添加。
   - 要修改现有配置文件，请单击“打开”。
3. 在“客户端体验”选项卡上的“凭据索引”旁边，单击“覆盖全局”，选择“主”或“辅助”。
4. 如果这是新的配置文件，请单击“创建”，然后单击“关闭”。
5. 如果要修改现有配置文件，请单击“确定”。

配置客户端证书和 **LDAP** 双重身份验证

February 1, 2024

您可以使用带有 LDAP 身份验证和授权的安全客户端证书，例如将智能卡身份验证与 LDAP 结合使用。用户登录，然后从客户端证书中提取用户名。客户端证书是身份验证的主要形式，LDAP 是辅助形式。客户端证书身份验证必须优先于 LDAP 身份验证策略。设置策略的优先级时，为客户端证书身份验证策略分配的数字小于分配给 LDAP 身份验证策略的编号。

要使用客户端证书，必须在运行 Active Directory 的同一台计算机上运行企业证书颁发机构 (CA)，例如 Windows Server 2008 中的证书服务。您可以使用 CA 创建客户端证书。

要使用具有 LDAP 身份验证和授权的客户端证书，它必须是使用安全套接字层 (SSL) 的安全证书。要将安全客户端证书用于 LDAP，请在用户设备上安装客户端证书，然后在 NetScaler Gateway 上安装相应的根证书。

在配置客户端证书之前，请执行以下操作：

- 创建虚拟服务器。
- 为 LDAP 服务器创建 LDAP 身份验证策略。
- 将 LDAP 策略的表达式设置为 True 值。

使用 **LDAP** 配置客户端证书身份验证

1. 在配置实用程序中的配置选项卡上，展开 **NetScaler Gateway >** 策略**\ >** 身份验证。
2. 在导航窗格中的“身份验证”下，单击“证书”。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在名称中，键入策略的名称。
5. 在“身份验证类型”中，选择 Cert。
6. 在“服务器”旁边，单击“新建”。
7. 在名称中，键入服务器的名称，然后单击创建。
8. 在“创建身份验证服务器”对话框的“名称”中，键入服务器的名称。
9. 在双因素旁边，选择开。
10. 在“用户名”字段中，选择“主题:CN”，然后单击“创建”。
11. 在创建身份验证策略对话框的命名表达式旁边，选择 True 值，单击添加表达式，单击创建，然后单击关闭。

创建证书身份验证策略后，将策略绑定到虚拟服务器。绑定证书身份验证策略后，将 LDAP 身份验证策略绑定到虚拟服务器。

重要：在将 LDAP 身份验证策略绑定到虚拟服务器之前，必须将证书身份验证策略绑定到虚拟服务器。

在 **NetScaler Gateway** 上安装根证书

创建证书身份验证策略后，从 CA 下载并安装 Base64 格式的根证书，然后将其保存在计算机上。然后，您可以将根证书上载到 NetScaler Gateway。

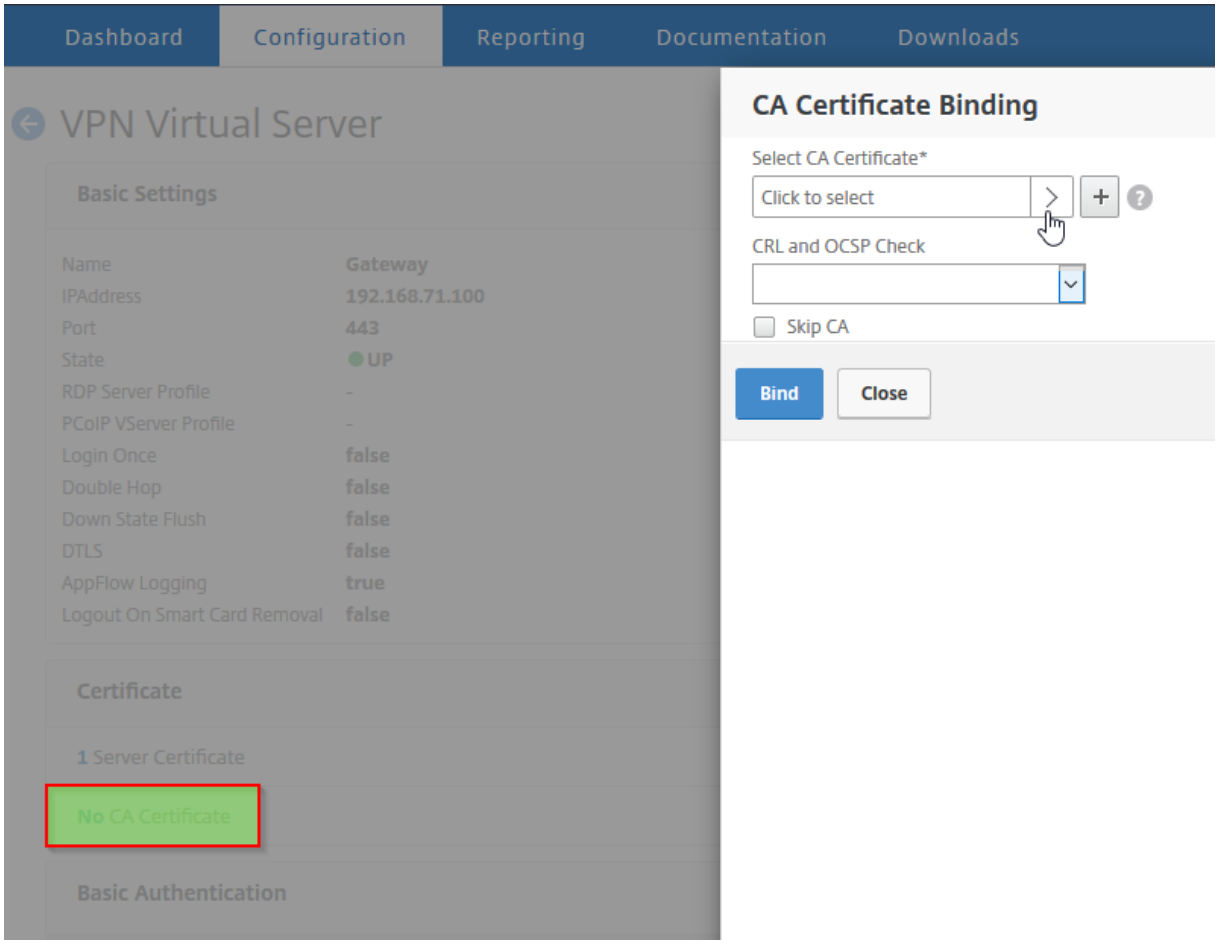
1. 在配置实用程序的配置选项卡的导航窗格中，展开 SSL，然后单击证书。
2. 在详细信息窗格中，单击“安装”。
3. 在证书-密钥对名称中，键入证书的名称。
4. 在“证书文件名”中，单击“浏览”，然后在列表中选择“装置”或“本地”。
5. 导航到根证书，单击打开，然后单击安装。

将根证书添加到虚拟服务器

在 NetScaler Gateway 上安装根证书后，将证书添加到虚拟服务器的证书存储中。

重要：将根证书添加到虚拟服务器以进行智能卡身份验证时，必须从
“选择 **CA** 证书”列表框中选择证书，如下图所示。

图 1. 添加根证书作为 CA



1. 在配置实用程序的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“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“打开”。
3. 在“证书”选项卡上的“可用”下，选择证书，在列表中的“添加”旁边，单击“CA”，然后单击“确定”。
4. 重复步骤 2。
5. 在证书选项卡上，单击 SSL 参数。
6. 在其他下，选择客户端身份验证。
7. 在其他下的客户端证书旁边，选择可选，然后单击确定两次。
8. 配置客户端证书后，使用 Citrix Secure Access 客户端登录 NetScaler Gateway 来测试身份验证。如果安装了多个证书，则会收到提示，要求您选择正确的证书。选择证书后，将出现登录屏幕，其中包含从证书中获取的信息填充的用户名。键入密码，然后单击“登录”。

如果在登录屏幕的“用户名”字段中看不到正确的用户名，请检查 LDAP 目录中的用户帐户和组。在 NetScaler Gateway 上定义的组必须与 LDAP 目录中定义的组相同。在 Active Directory 中，在域根级别配置组。如果创建的 Active Directory 组不在域根级别，则可能会导致客户端证书读取错误。

如果用户和组不在域根级别，NetScaler Gateway 登录页面将显示在 Active Directory 中配置的用户名。例如，在 Active Directory 中，您有一个名为用户的文件夹，证书上写着 CN=Users。在登录页面的“用户名”中，将显示“用户”一词。

如果不想将组和用户帐户移动到根域级别，则在 NetScaler Gateway 上配置证书身份验证服务器时，请将“用户名字段”和“组名称”字段留空。

配置单点登录

February 1, 2024

您可以将 NetScaler Gateway 配置为支持使用 Windows 进行单点登录、Web 应用程序（如 SharePoint）、文件共享和 Web Interface。单点登录还适用于用户可以通过访问界面中的文件传输实用程序或通知区域中的 NetScaler Gateway 图标菜单访问的文件共享。

如果在用户登录时配置单点登录，他们将自动重新登录，而无需再次输入凭据。

使用 **Windows** 配置单点登录

February 1, 2024

用户通过从桌面启动 Citrix Secure Access 客户端来打开连接。您可以通过启用单点登录来指定 Citrix Secure Access 客户端在用户登录 Windows 时自动启动。配置单点登录时，用户的 Windows 登录凭据将传递到 NetScaler Gateway 进行身份验证。为 Citrix Secure Access 客户端启用单点登录可简化用户设备上的操作，例如安装脚本和自动驱动器映射。

仅当用户设备登录到组织的域时才启用单点登录。如果启用了单点登录，并且用户从不在您的域中的设备进行连接，则系统会提示用户登录。

您可以通过全局或使用附加到会话策略的会话配置文件在 Windows 上配置单点登录。

使用 **Windows** 全局配置单点登录

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，单击“使用 **Windows** 单点登录”，然后单击“确定”。

使用会话策略在 **Windows** 上配置单点登录

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“客户端体验”选项卡上的“使用 **Windows** 单点登录”旁边，单击“覆盖全局”，单击“使用 **Windows** 单点登录”，然后单击“确定”。
7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置单点登录到 **Web** 应用程序

February 1, 2024

您可以将 NetScaler Gateway 配置为向内部网络中使用基于 Web 的身份验证的服务器提供单点登录。通过单点登录，您可以将用户重定向到自定义主页，例如 SharePoint 站点或 Web Interface。您还可以通过 Citrix Secure Access 客户端从主页上配置的书签或用户在 Web 浏览器中键入的 Web 地址配置资源的单点登录。

如果要将主页重定向到 SharePoint 站点或 Web Interface，请提供该站点的 Web 地址。通过 NetScaler Gateway 或外部身份验证服务器对用户进行身份验证后，用户将被重定向到指定的主页。用户凭据以透明方式传递给 Web 服务器。如果 Web 服务器接受凭据，则用户将自动登录。如果 Web 服务器拒绝这些凭据，则用户会收到一条身份验证提示，询问其用户名和密码。

您可以在全局范围内或使用会话策略配置 Web 应用程序的单点登录。

在全局范围内配置 **Web** 应用程序的单点登录

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在客户端体验选项卡上，单击单点登录到 Web 应用程序，然后单击确定。

使用会话策略配置 **Web** 应用程序的单点登录

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策 略”选项卡上，选择一个会话策略，然后单击“打开”。
3. 在“配置会话策略”对话框中，单击“请求配置文件”旁边的“修改”。
4. 在“客户端体验”选项卡上的“单点登录 Web 应用程序”旁边，单击“全局覆盖”，单击“单点登录到 Web 应用程序”，然后单击“确定”。

为单点登录 **Web** 应用程序定义 **HTTP** 端口

只有目标端口被视为 HTTP 端口的网络流量才会尝试单点登录。要允许对使用端口 80 以外的端口进行 HTTP 流量的应用程序进行单点登录，请在 NetScaler Gateway 上添加一个或多个端口号。您可以启用多个端口。这些端口是全局配置的。

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在 网络配置 选项卡上，单击 高级设置。
4. 在“HTTP 端口”下，键入端口号，单击“添加”，然后单击“确定”两次。

   您可以为要添加的每个端口重复步骤 4。

注意：如果内部网络中的 Web 应用程序使用公有 IP 地址，则单点登录不起作用。要启用单点登录，无论使用无客户端访问还是 Citrix Secure Access 客户端进行用户设备连接，都必须在全局策略设置中启用分离通道。如果无法在全局级别启用拆分通道，请创建使用专用地址范围的虚拟服务器。

使用 **LDAP** 配置对 **Web** 应用程序的单点登录

February 1, 2024

当您配置单点登录并且用户使用格式为 username@domain.com 的用户主体名称 (UPN) 登录时，默认情况下，单点登录将失败，用户必须进行两次身份验证。如果需要使用此格式进行用户登录，请修改 LDAP 身份验证策略以接受此形式的用户名。

配置 **Web** 应用程序的单点登录

1. 在配置实用程序的配置选项卡上，展开 **NetScaler Gateway >** 策略 **>** 身份验证。
2. 在详细信息窗格的“策 略”选项卡上，选择 LDAP 策略，然后单击“打开”。
3. 在“配置身份验证策略”对话框中，在“服务器”旁边，单击“修改”。
4. 在“连接设置”下的“基本 DN（用户位置）”中，键入 DC=DOMAINNAME、DC=Com。
5. 在 管理员绑定 **DN** 中，键入 LDAPaccount@domainname.com，其中 domainname.com 是域名的名称。
6. 在 管理员密码 和 确认管理员密码中，键入密码。
7. 在“其他设置”下的“服务器登录名属性”中，键入 userPrincipalName。
8. 在 组属性中，键入 memberOf。
9. 在 子属性名称中，键入 CN。
10. 在 **SSO** 名称属性中，键入用户登录的格式，然后单击 确定 两次。此值为 `SamAccountName` 或 `UserPrincipalName`。

配置域的单点登录

February 1, 2024

如果用户连接到运行 Citrix Virtual Apps 的服务器并使用 SmartAccess，则可以为连接到服务器场的用户配置单点登录。使用会话策略和配置文件配置对已发布应用程序的访问权限时，请使用服务器场的域名。

您还可以将单点登录配置为网络中的文件共享。

配置域的单点登录

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策 略”选项卡上，选择一个会话策略，然后单击“打开”。
3. 在“配置会话策略”对话框中，单击“请求配置文件”旁边的“修改”。
4. 在“配置会话配置文件”对话框的“已发布的应用程序”选项卡的“单点登录域”中，单击“覆盖全局”，键入域名，然后单击“确定”两次。

有关使用 Citrix Virtual Apps 配置 NetScaler Gateway 的更多信息，请参阅 将 NetScaler Gateway 与 Citrix Virtual Apps and Desktops集成。

为 **Microsoft Exchange 2010** 配置单点登录

February 1, 2024

以下部分介绍了 NetScaler Gateway 上适用于 Microsoft Exchange 2010 的单点登录 (SSO) 的配置。适用于 Outlook Web 访问 (OWA) 2010 的 SSO 在以下情况下不起作用：

- 在 Microsoft Exchange 2010 上使用基于表单的身份验证。
- 使用身份验证、授权和审核流量管理策略对虚拟服务器进行负载平衡

> 注意：此配置仅适用于使用身份验证、授权和审核流量管理策略对虚拟服务器进行负载平衡。它不适用于 OWA 2010 中使用无客户端 VPN 的 SSO。

以下步骤是在 NetScaler Gateway 上为 Microsoft Exchange 2010 配置 SSO 之前必须考虑的先决条件。

- 在 OWA 2010 中，SSO 的操作 URL 表单有所不同。相应地修改流量管理策略。
- 您需要重写策略才能在 logon.aspx 请求中设置 PBack cookie。在正常情况下，您可以在客户端设置 PBack cookie，然后单击提交。
- 使用 SSO 时，对 logon.aspx 的响应将被消耗，NetScaler Gateway 会生成表单请求。表单提交请求中未附加 cookie。

- OWA 服务器需要表单提交请求中的 PBack cookie。需要重写策略才能在表单提交请求中附加 PBack cookie。

使用 **CLI** 执行以下操作

1. 配置身份验证、授权和审核流量管理

```
add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.
owa"-userField username -passwdField password -ssoSuccessRule "
http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.
GT(70"-responsesize 15000 -submitMethod POST
```

2. 配置流量管理策略并绑定策略

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

使用 **CLI** 重写配置

在命令提示符下，键入：

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

备用重写配置

在极少数情况下，Microsoft Outlook 可能不会发出 OWA 会话 cookie，并且可能也不会插入 Pback cookie。在运行上述命令来实现重写配置之后，可能会出现此问题。

要克服这些情况并作为解决方法，您可以配置以下命令而不是重写配置。

在命令提示符下，键入：

- `add rewrite action set_pback_cookie insert_http_header "Cookie""PBack=0"'`

- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\" logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

配置一次性密码使用

February 1, 2024

您可以将 NetScaler Gateway 配置为使用一次性密码，例如令牌个人标识号 (PIN) 或通行码。用户输入通行码或 PIN 后，身份验证服务器会立即使该一次性密码失效，并且用户无法再次输入相同的 PIN 或密码。

包括使用一次性密码的产品包括：

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

要使用其中每种产品，请将内部网络中的身份验证服务器配置为使用 RADIUS。有关详细信息，请参阅 配置 RADIUS 验证。

例如，如果在 NetScaler Gateway 上将身份验证配置为在 RADIUS 上使用一次性密码（例如 RSA SecurID 令牌提供），NetScaler Gateway 将尝试使用缓存的密码重新对用户进行身份验证。当您更改 NetScaler Gateway 或 Citrix Secure Access 客户端与 NetScaler Gateway 之间的连接中断然后恢复时，就会发生这种重新身份验证。

当连接配置为使用 Citrix Workspace 应用程序并且用户使用 RADIUS 或 LDAP 连接到 Web Interface 时，也可能会尝试重新进行身份验证。当用户启动应用程序并使用该应用程序，然后返回 Receiver 启动另一个应用程序时，NetScaler Gateway 将使用缓存的信息对用户进行身份验证。

配置 **RSA SecurID** 身份验证

February 1, 2024

在为 RSA SecureID 身份验证配置 RSA/ACE 服务器时，您需要完成以下步骤：

使用以下信息配置 RADIUS 客户端：

- 提供 NetScaler Gateway 设备的名称。

- 提供描述（不是强制性的）。
- 提供系统 IP 地址。
- 在 NetScaler Gateway 和 RADIUS 服务器之间提供共享密钥。
- 将品牌/型号配置为标准 RADIUS。

在代理主机配置中，您需要以下信息：

- 提供 NetScaler Gateway 的完全限定域名 (FQDN)（与绑定到虚拟服务器的证书上显示的相同）。提供 FQDN 后，单击 Tab 键，网络地址窗口将自行填充。

  输入 FQDN 后，将自动显示网络地址。如果没有，请输入系统 IP 地址。

- 使用通信服务器提供代理类型。
- 配置为导入允许通过 NetScaler Gateway 进行身份验证的所有用户或一组用户。

如果尚未配置，请为 RADIUS 服务器创建代理主机条目，包括以下信息：

- 提供 RSA 服务器的 FQDN。

  输入 FQDN 后，将自动显示网络地址。如果没有，请提供 RSA 服务器的 IP 地址。

- 提供代理类型，即 RADIUS 服务器。

有关配置 RSA RADIUS 服务器的详细信息，请参阅制造商的文档。

要配置 RSA SecurID，请创建身份验证配置文件和策略，然后将策略全局绑定或绑定到虚拟服务器。要创建 RADIUS 策略以使用 RSA SecurID，请参阅 配置 RADIUS 身份验证。

创建身份验证策略后，将其绑定到虚拟服务器或全局绑定。有关详细信息，请参阅 绑定验证策略。

使用 **RADIUS** 配置密码返回

February 1, 2024

您可以将域密码替换为令牌从 RADIUS 服务器生成的一次性密码。当用户登录 NetScaler Gateway 时，他们会输入令牌中的个人识别码 (PIN) 和通行码。NetScaler Gateway 验证其凭据后，RADIUS 服务器会将用户的 Windows 密码返回到 NetScaler Gateway。NetScaler Gateway 接受来自服务器的响应，然后使用返回的密码进行单点登录，而不是使用用户在登录过程中键入的密码。此带有 RADIUS 功能的密码返回允许您配置单点登录，而无需用户撤回其 Windows 密码。

当用户使用密码返回登录时，他们可以访问内部网络中所有允许的网络资源，包括 Citrix Endpoint Management、StoreFront 和 Web Interface。

要使用返回的密码启用单点登录，请使用密码供应商标识符和密码属性类型参数在 NetScaler Gateway 上配置 RADIUS 身份验证策略。这两个参数会将用户的 Windows 密码返回到 NetScaler Gateway。

NetScaler Gateway 支持 Imprivata OneSign。Imprivata OneSign 的最低要求版本为 4.0，其中包含服务包 3。Imprivata OneSign 的默认密码供应商标识符为 398。Imprivata OneSign 的默认密码属性类型代码为 5。

您可以使用其他 RADIUS 服务器返回密码，例如 RSA、Cisco 或 Microsoft。将 RADIUS 服务器配置为在供应商特定的属性值对中返回用户单点登录密码。在 NetScaler Gateway 身份验证策略中，必须为这些服务器添加 密码供应商标识符和密码 属性类型参数。

您可以在 互联网号码分配机构 (IANA) 网站上找到供应商标识符的完整列表。例如，RSA 安全性的供应商标识符为 2197，Microsoft 为 311，Cisco Systems 的供应商标识符为 9。供应商支持的特定于供应商的属性必须与供应商确认。例如，Microsoft 已在 Microsoft 供应商特定的 RADIUS 属性上发布了供应商特定属性的列表。

您可以选择任何供应商特定的属性，在供应商的 RADIUS 服务器上存储用户的单点登录密码。如果使用供应商标识符和用户密码存储在 RADIUS 服务器上的属性配置 NetScaler Gateway，NetScaler Gateway 将请求发送到 RADIUS 服务器的访问请求数据包中的属性值。如果 RADIUS 服务器使用访问接受数据包中的相应属性值对进行响应，则无论您使用哪个 RADIUS 服务器，密码返回都会起作用。

要使用返回的密码配置单点登录：

1. 在配置实用程序中的配置选项卡上，展开 **NetScaler Gateway >** 策略\ **>** 身份验证。
2. 在导航窗格中，单击 **RADIUS**。
3. 在详细信息窗格中，单击“添加”。
4. 在“创建身份验证策略”对话框的“名称”中，键入策略的名称。
5. 在“服务器”旁边，单击“新建”。
6. 在 名称中，键入服务器的名称。
7. 配置 RADIUS 服务器的设置。
8. 在 密码供应商标识符中，键入 RADIUS 服务器返回的供应商标识符。此标识符的最小值必须为 1。
9. 在 密码属性类型中，键入 RADIUS 服务器在供应商特定 AVP 代码中返回的属性类型。该值的范围可以在 1 到 255 之间。
10. 在“创建身份验证策略”对话框中，在“命名表达式”旁边，选择表达式，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置 **SafeWord** 身份验证

February 1, 2024

SafeWord 产品线通过使用基于令牌的密码来帮助提供安全的身份验证。用户输入密码后，该密码将被 SafeWord 失效，无法再次使用。

如果访问网关正在替换 Secure Gateway 和 Web Interface 部署中的 Secure Gateway，则可以选择不在访问网关上配置身份验证，并继续允许 Web Interface 为传入的 HTTP 流量提供 SafeWord 身份验证。

访问网关支持以下产品的 SafeWord 身份验证：

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord for Citrix
- SafeWord RemoteAccess

您可以通过以下方式将访问网关配置为使用 SafeWord 产品进行身份验证：

- 将身份验证配置为使用作为 SafeWord PremierAccess 一部分安装的 PremierAccess RADIUS 服务器，并允许它处理身份验证。
- 配置身份验证以使用 SafeWord IAS 代理，该代理是 SafeWord RemoteAccess、适用于 Citrix 的 SafeWord 和 SafeWord PremierAccess 4.0 的组成部分。
- 安装 SafeWord Web Interface 代理以支持 Citrix Web Interface。您不必在访问网关上配置身份验证，Citrix Web Interface 可以处理此问题。此配置不使用 PremierAccess RADIUS 服务器或 SafeWord IAS 代理。

配置 SafeWord RADIUS 服务器时，您需要以下信息：

- 接入网关的 IP 地址。在 RADIUS 服务器上配置客户端设置时，请使用接入网关 IP 地址。
- 一个共享的秘密。
- SafeWord 服务器的 IP 地址和端口。

配置 **Gemalto Protiva** 身份验证

February 1, 2024

Protiva 是一个强大的身份验证平台，旨在利用金雅拓智能卡身份验证的优势。使用 Protiva，用户可以使用 Protiva 设备生成的用户名、密码和一次性密码登录。与 RSA SecurID 类似，身份验证请求将发送到 Protiva 身份验证服务器，密码将被验证或拒绝。

要将金雅拓 Protiva 配置为支持 NetScaler Gateway，请使用以下准则：

- 安装 Protiva 服务器。
- 在 Microsoft IAS RADIUS 服务器上安装 Protiva Internet Authentication Server (IAS) 代理插件。确保记下 IAS 服务器的 IP 地址和端口号。

nFactor 用于网关身份验证

February 1, 2024

nFactor 身份验证为身份验证提供了一系列全新的可能性。使用 nFactor 的管理员在为虚拟服务器配置身份验证因素时可以享受身份验证、授权和审核

两个保单银行或两个因素不再限制管理员。可以扩大保单银行的数量以适应不同的需求。根据以前的因素，nFactor 确定了一种身份验证方法。使用 nFactor 可以实现动态登录表单和失败时的操作。

> 重要
>
> - 从版本 13.0 build 67.x 开始，标准许可证仅支持 nFactor 身份验证，仅适用于网关/VPN 虚拟服务器，不支持身份验证虚拟服务器。在标准许可证中，nFactor 可视化工具 GUI 不能用于在 nFactor 流程中创建 EPA。此外，您不能编辑登录架构，但必须按原样使用出厂设置的登录架构。
> - 要使 NetScaler 支持 nFactor 身份验证，需要高级许可证或高级许可证。有关使用 NetScaler 进行 nFactor 身份验证的更多信息，请参阅 nFactor 身份验证

身份验证、授权和审核功能许可要求

下表列出了可用身份验证、授权和审核功能的许可要求。

	标准许可证	高级许可证	高级许可证
本地验证	是	是	是
LDAP 身份验证	是	是	是
RADIUS 身份验证	是	是	是
TACACS 身份验证	是	是	是
Web 身份验证	是	是	是
客户端证书身份验证	是	是	是
协商身份验证	是	是	是
SAML 身份验证	是	是	是
OAuth 身份验证	否	是	是
本机 **OTP**	否	是	是
电子邮件 **OTP**	否	是	是
OTP 的推送通知	否	否	是
基于知识的问答（**KBA** 身份验证）	否	是	是
自助服务密码重置 **(SSPR)**	否	是	是
nFactor 可视化工具	是	是	是

> 注意
>
> - 有关为 NetScaler 标准许可证配置 nFactor 的步骤，请参阅 NetScaler Standard 许可证中的为 nFactor 身份验证创建网关虚拟服务器部分。
> - 在 NetScaler Standard 许可证中，只有不可寻址的身份验证、授权和审核虚拟服务器才能绑定到网关/VPN 虚拟服务器。
> - NetScaler 标准许可证中不允许自定义 LoginSchema。nFactor 支持是基本的，只有默认且已经添加了设备随附的登录架构。管理员可以在其配置中使用它们，但不能添加登录架构。因此，GUI 选项被禁用。

用例

nFactor 身份验证可根据用户配置文件启用动态身份验证流程。有时，流程对用户来说可能很简单直观。在其他情况下，它们可以与保护活动目录或其他身份验证服务器结合使用。以下是 Gateway 的一些特定要求：

1. 动态选择用户名和密码。传统上，客户端（包括浏览器和 Receiver）使用 Active Directory (AD) 密码作为第一个密码字段。第二个密码保留给一次性密码 (OTP)。但是，为了保护 AD 服务器，必须首先验证 OTP。nFactor 可以在不需要客户端修改的情况下完成此操作。
2. 多租户身份验证端点。一些组织为证书用户和非证书用户使用不同的网关服务器。当用户使用自己的设备登录时，NetScaler 设备的用户访问级别因所使用的设备而异。网关可以满足不同的身份验证需求。
3. 基于组成员身份的身份验证。一些组织从 AD 服务器获取用户属性以确定身份验证要求。个人用户的身份验证要求可能有所不同。
4. 身份验证协同因素。有时，不同的身份验证策略对用于对不同的用户组进行身份验证。提供配对策略可提高身份验证的效从属策略可以从一个流程中创建。通过这种方式，独立的策略集成为自己的流程，从而提高效率并降低复杂性。

身份验证响应处理

NetScaler Gateway 回调寄存器处理身份验证响应。AAAD（身份验证守护程序）响应和成功/失败/错误/对话代码将提供给回调句柄。成功/失败/错误/对话代码指示 Gateway 采取适当的措施。

客户支持

下表详细介绍了配置详细信息。

客户端	nFactor 支持	身份验证策略绑定点	EPA
浏览器	是	身份验证	是

客户端	nFactor 支持	身份验证策略绑定点	EPA
Citrix Workspace 应用程序	是	VPN	是
网关插件	是	VPN	是

注意：

- Citrix Workspace 应用程序支持以下列出的版本中受支持的操作系统的 nFactor 身份验证。
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5：通过应用商店网络支持
  - Chrome 浏览器：通过商店网络支持

命令行配置

Gateway 虚拟服务器需要一个名为属性的身份验证虚拟服务器。作为属性的虚拟服务器名称是此模型所需的唯一配置。

```
1 add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
2 <!--NeedCopy-->
```

authnVsName 是身份验证虚拟服务器的名称。authnVsName 虚拟服务器必须配置高级身份验证策略并用于 nFactor 身份验证。

```
1 add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
     -profile>
2 set vpn vserver <name> -authnProfile <name-of-profile>
3 <!--NeedCopy-->
```

其中 authnProfile 是以前创建的身份验证配置文件。

互操作挑战

除 rfWeb 客户端外，大多数旧版网关客户端都是基于 Gateway 发送的响应建模的。例如，预计许多客户端对 /vpn/index.html 的响应为 302。这些客户端还依赖于各种网关 cookie，例如“pwcount”、“NSC_CERT”。

端点分析 **(EPA)**

NetScaler 身份验证、授权和审核模块不支持 nFactor 中的 EPA。因此，NetScaler Gateway 虚拟服务器执行 EPA。在 EPA 之后，登录凭据将使用前面提到的 API 发送到身份验证虚拟服务器。身份验证完成后，网关将继续进行身份验证后流程，并建立用户会话。

错误配置注意事项

Gateway 客户端只发送一次用户凭据。Gateway 通过登录请求从客户端获取一个或两个凭据。在旧模式下，最多有两个因素。获得的密码用于这些因素。但是，使用 nFactor，可以配置的因素数量实际上是无限的。从 Gateway 客户端获取的密码将根据配置的因素重复使用（根据配置）。必须注意不要多次重复使用一次性密码（OTP）。同样，管理员必须确保在某个因素下重复使用的密码确实适用于该因素。

定义客户端

提供配置选项是为了帮助 NetScaler 确定浏览器客户端与 Receiver 等胖客户端。

为管理员提供了一个名为 ns_vpn_client_useragents 的模式集，用于为所有客户端配置模式。

同样，将“Citrix Receiver”字符串绑定到上面的 `patset` 以忽略用户代理中包含“Citrix Receiver”的所有客户端。

限制网关的 **nFactor**

如果存在以下条件，则不会发生用于网关身份验证的 nFactor。

1. authnProfile 未设置为 NetScaler Gateway。
2. 高级身份验证策略未绑定到身份验证虚拟服务器，并且在中提到了同一身份验证虚拟服务器 `authnProfile`。
3. HTTP 请求中的用户代理字符串与 `patset` ns_vpn_client_useragent 中配置的用户代理匹配。

如果不满足这些条件，则使用绑定到 Gateway 的经典身份验证策略。

如果用户代理或其中的一部分绑定到前面提到的 `patset`，则来自这些用户代理的请求不会参与 nFactor 流程。例如，以下命令限制所有浏览器的配置（假设所有浏览器的用户代理字符串中都包含“Mozilla”）：

```
bind patset ns_vpn_client_useragents Mozilla
<!--NeedCopy-->
```

LoginSchema

LoginSchema 是登录表单的逻辑表示形式。XML 语言对其进行了定义。LoginSchema 的语法符合 Citrix 的通用表单协议规范。

LoginSchema 定义了产品的“视图”。管理员可以提供表单的自定义说明、辅助文本等。登录架构包括表单本身的标签。客户可以提供成功或失败消息来描述在给定时刻显示的表单。

使用以下命令配置登录架构。

```
add authentication loginSchema <name> -authenticationSchema <string> [-
    userExpression <string>] [-passwdExpression <string>] [-
    userCredentialIndex <positive_integer>]
[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
    <positive_integer>] [-SSOCredentials ( YES | NO )]
<!--NeedCopy-->
```

参数说明

- name-新登录架构的名称。这是一个强制性的参数。最大长度：127
- authenticationSchema - 用于读取要为登录页面 UI 发送的身份验证架构的文件的名称。此文件包含按照 Citrix Forms 身份验证协议的元素的 xml 定义，以便能够呈现登录表单。如果管理员不想提示用户输入其他凭据，但继续使用先前获取的凭据，则 noschema 可以作为参数提供。这仅适用于与用户定义因素一起使用的 loginSchema，而不适用于虚拟服务器因素。

这是一个强制性的参数。最大长度：255

- userExpression - 用于在登录期间提取用户名的表达式。这可以是任何相关的高级策略表达式。最大长度：127
- passwdExpression - 用于在登录期间提取密码的表达式。这可以是任何相关的高级策略表达式。最大长度：127
- userCredentialIndex-用户输入的用户名必须存储在会话中的索引。最小值：1，最大值：16
- passwordCredentialIndex-用户输入密码的索引必须存储在会话中。最小值：1，最大值：16
- authenticationStrength - 当前身份验证的权重最小值：0，最大值：65535
- SSOCredentials -此选项指示当前因素凭据是否为默认 SSO (SingleSignOn) 凭据。可能的值：YES, NO。默认值：NO

需要 **LoginSchema** 和 **nFactor** 知识

预构建的 loginSchema 文件位于以下 NetScaler 位置 **/nsconfig/loginschema/LoginSchema/**。这些预先构建的 loginSchema 文件适合常见的使用案例，必要时可以进行修改以进行细微的变化。

此外，大多数具有很少自定义设置的单因素用例不需要登录架构配置。

建议管理员查看文档以获取使 NetScaler 能够发现因素的其他配置选项。用户提交凭据后，管理员可以配置多个因素来灵活选择和处理身份验证因素。

在不使用 **LoginSchema** 的情况下配置双重身份验证

NetScaler 会根据配置自动确定双因素要求。用户提供这些凭据后，管理员就可以在虚拟服务器上配置第一组策略。对于每个策略，都可以有一个“nextFactor”配置为“passthrough”。“直通”意味着 NetScaler 必须使用现有凭据集处理登录，而无需访问用户。通过使用“直通”因素，管理员可以编程方式推动身份验证流程。建议管理员阅读 nFactor 规范或部署指南以了解更多详细信息。请参阅
多重 (nFactor) 身份验证。

用户名和密码表达式

要处理登录凭据，管理员必须配置 loginSchema。具有很少 loginSchema 自定义项的单因素或双因素用例不需要指定的 XML 定义。LoginSchema 具有其他属性，例如 userExpression 和 passwdExpression，这些属性可用于更改用户显示的用户名或密码。

登录架构是高级策略表达式，也可用于覆盖用户输入。这可以通过在 **-authenticationSchema** 中为参数附加一个字符串来实现，如以下示例所示。

以下是分别修改用户输入的用户名和密码的示例。

- 将用户名的用户输入从更改 `username@citrix.com` 为 `username@xyz.com`

```
1  add authentication loginSchema user_schema -authenticationSchema
       LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
       BEFORE_STR("@").APPEND("@xyz.com")"
2  <!--NeedCopy-->
```

- 考虑一个场景，即用户在配置的登录架构中首先提供密码和通行码。要使用用户在第一个因素中提供的通行 码，在第二个因素中使用 密 码，可以使用以下命令修改现有的登录架构。

```
1  add authentication loginSchema user_schema -authenticationSchema
       LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
       PASSWORD2"
2  <!--NeedCopy-->
```

```
1  add authentication loginSchema user_schema_second -
       authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
       PASSWORD"
2  <!--NeedCopy-->
```

nFactor 配置中的高级步骤

下图说明了 nFactor 配置中涉及的高级步骤。

GUI 配置

本节介绍以下主题：

- 创建虚拟服务器
- 创建身份验证虚拟服务器
- 创建验证 CERT 配置文件
- 创建身份验证策略
- 添加 LDAP 身份验证服务器
- 添加 LDAP 身份验证策略
- 添加 RADIUS 身份验证服务器
- 添加 RADIUS 身份验证策略
- 创建身份验证登录架构
- 创建策略标签

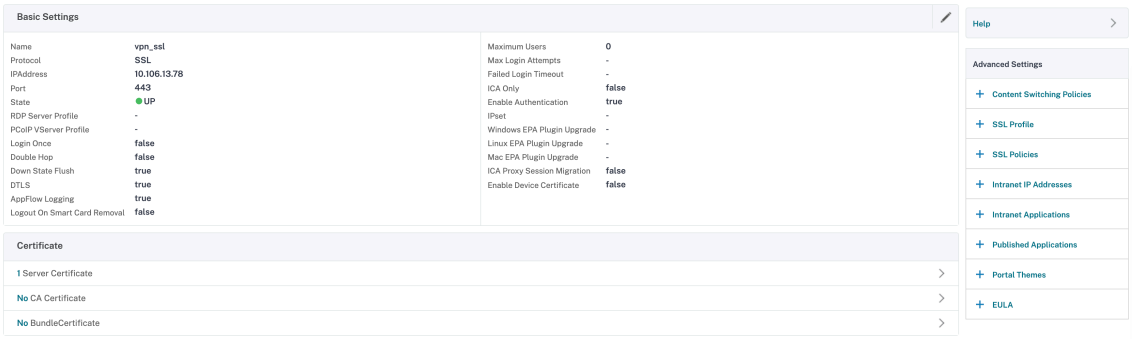
创建虚拟服务器

1. 导航到 **NetScaler Gateway>** 虚拟服务器。

2. 单击 添 加按钮以创建网关虚拟服务器。
3. 输入以下信息，然后单击 **OK**（确定）。

参数名称	参数说明
输入虚拟服务器的名称。	NetScaler Gateway 虚拟服务器的名称。必须以 ASCII 字母或下划线 (_) 字符开头，并且必须仅包含 ASCII 字母数字、下划线、哈希 (#)、句点 (.)、空格、冒号 (:)、at (@)、等于 (=) 和连字符 (-)。可以在创建虚拟服务器后进行更改。以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的服务器”或“我的服务器”）。
输入虚拟服务器的 IP 地址类型	从下拉菜单中选择 IP 地址或不可寻址选项。
输入虚拟服务器的 IP 地址。	互联网协议地址（IP 地址）是分配给加入使用 Internet 协议进行通信的计算机网络的每台设备的数字标签。
输入虚拟服务器的端口号。	输入端口号。
输入身份验证配置文件。	虚拟服务器上的验证配置文件实体此实体可用于将身份验证卸载到身份验证、授权和审核虚拟服务器以进行多重 (nFactor) 身份验证
输入 RDP 服务器配置文件。	与虚拟服务器关联的 RDP 服务器配置文件的名称。
输入最大用户数。	此虚拟服务器上允许的最大并发用户会话数。允许登录此虚拟服务器的实际用户数取决于用户许可证的总数。
输入最大登录尝试次数。	最大登录尝试次数。
输入失败的登录超时。	如果用户超过允许的最大尝试次数，则帐户被锁定的分钟数。
输入 Windows EPA 插件升级。	用于为 Win 设置插件升级行为的选项。
输入 Linux EPA 插件升级。	用于设置 Linux 的插件升级行为的选项。
进入 MAC EPA 插件升级	用于为 Mac 设置插件升级行为的选项。
一次登录	此选项启用/禁用此虚拟服务器的无缝 SSO。

参数名称	参数说明
仅限 ICA	如果设置为开，则表示基本模式，用户可以使用 Citrix Workspace 应用程序或浏览器登录，并访问在 `Wihome` 参数指出的 Citrix Virtual Apps and Desktops 环境中配置的已发布应用程序。不允许用户使用 Citrix Secure Access 客户端进行连接，也无法配置端点扫描。在此模式下，可以登录和访问应用程序的用户数量不受许可证的限制。-设置为 OFF 时，它意味着 SmartAccess 模式，在该模式下，用户可以使用 Citrix Workspace 应用程序、浏览器或 Citrix Secure Access 客户端登录。管理员可以将端点扫描配置为在客户端系统上运行，然后使用结果控制对已发布应用程序的访问。在此模式下，客户端可以在其他客户端模式下连接到网关，即 VPN 和无客户端 VPN。在此模式下，可以登录和访问资源的用户数量受 CCU 许可证的限制。
启用验证	要求连接到 NetScaler Gateway 的用户进行身份验证
双跃点	在双跃点配置中使用 NetScaler Gateway 设备。双跃点部署通过使用三个防火墙将 DMZ 分为两个阶段，为内部网络提供了额外的安全层。这样的部署可以在 DMZ 中有一台设备，在安全网络中可以有一台设备。
向下状态刷新	将虚拟服务器标记为 DOWN 时关闭现有连接，这意味着服务器可能已超时。断开现有连接可以释放资源，在某些情况下可以加快过载负载平衡设置的恢复速度。在服务器上启用此设置，当连接被标记为 DOWN 时，可以安全地关闭这些连接。不要在必须完成事务的服务器上启用 DOWN 状态刷新。
DTLS	此选项启动/停止虚拟服务器上的转弯服务
AppFlow 记录	记录包含标准 NetFlow 或 IPFIX 信息的 AppFlow 记录，例如流的开始和结束的时间戳、数据包计数和字节计数。还记录包含应用程序级信息的记录，例如 HTTP Web 地址、HTTP 请求方法和响应状态代码、服务器响应时间和延迟。
ICA 代理会话迁移	此选项确定当用户从另一台设备登录时是否传输现有 ICA 代理会话。
状态	虚拟服务器的当前状态，如 UP、DOWN、BUSY 等。
启用设备证书	指示作为 EPA 一部分的设备证书检查是打开还是关闭。



4. 选择页面的“无服务器证书”部分。
5. 单击“选择服务器证书”下的 **>** 以选择服务器证书。
6. 选择 SSL 证书，然后单击“选择”按钮。
7. 单击绑定。
8. 如果看到关于 没有可用密码的警告，请单击 确定
9. 单击“继续”按钮。
10. 在“身份验证”部分中，单击右上角的 **+** 图标。

创建身份验证虚拟服务器

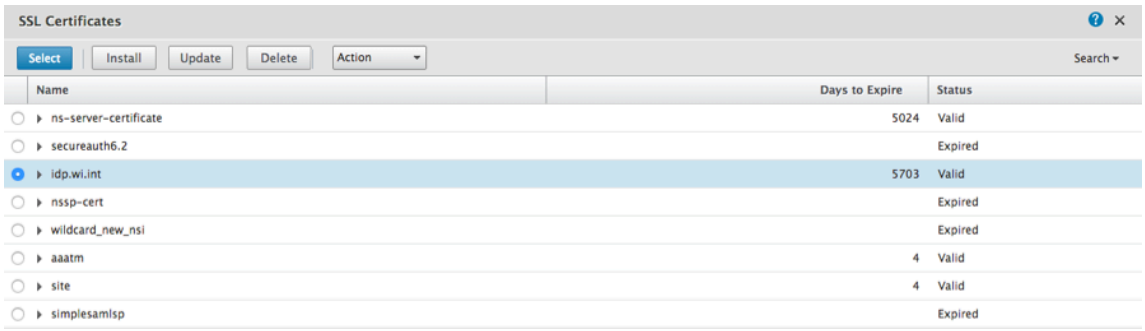
1. 导航到安全 **> NetScaler AAA** —应用程序流量 **>** 虚拟服务器。
2. 单击添加按钮。
3. 完成以下基本设置以创建身份验证虚拟服务器。

   注意：设置名称右侧的 * 符号表示必填字段。

   - 输入新身份验证虚拟服务器的 名称。
   - 输入 **IP** 地址类型。IP 地址类型可以配置为不可寻址。
   - 输入 **IP** 地址。IP 地址可以为零。
   - 输入身份验证虚拟服务器的 协议 类型。
   - 输入虚拟服务器接受连接的 **TCP** 端口。
   - 输入身份验证虚拟服务器设置的身份验证 Cookie 的 域。
4. 单击确定。
5. 单击 无服务器证书。
6. 从列表中选择所需的服务器证书。

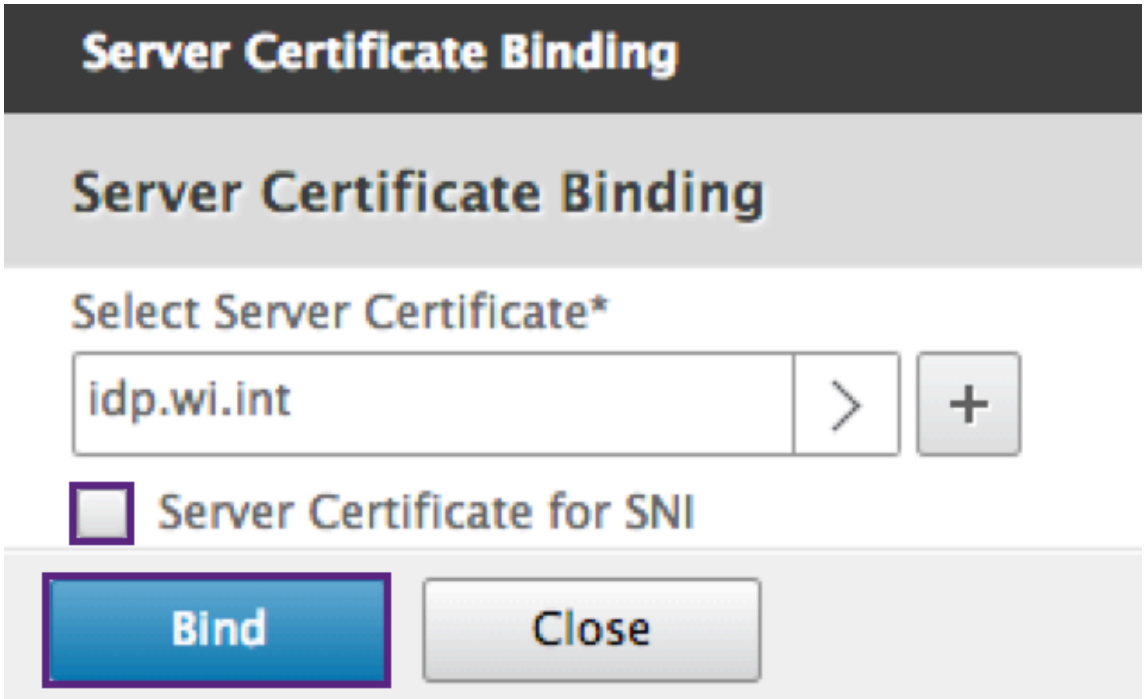
7. 选择所需的 SSL 证书，然后单击“选择”按钮。

   注意：身份验证虚拟服务器不需要绑定到它的证书。



8. 配置 服务器证书绑定。

   - 选中 **SNI** 的服务器证书 框以绑定用于 SNI 处理的一个或多个证书密钥。
   - 单击“绑定”按钮。



创建身份验证 **CERT** 配置文件

1. 导航到 安全**-> NetScaler AAA** —应用程序流量**->** 策略**->** 身份验证**->** 基本策略**-> CERT**。
2. 选择配置文件选项卡，然后选择 添加。
3. 完成以下字段以创建身份验证证书配置文件。设置名称右侧的 * 符号表示必填字段。

   - 名称 -客户端证书身份验证服务器配置文件（操作）的名称。

- 两个因素—在这种情况下，双因素身份验证选项是 NOOP。
- 用户名字段—输入从中提取用户名的客户端证书字段。必须设置为“使用者”或“颁发者”（包括两组双引号）。
- 组名称字段 -输入从中提取组的客户端证书字段。必须设置为“使用者”或“颁发者”（包括两组双引号）。
- 默认身份验证组 -这是除提取的组之外，在身份验证成功时选择的默认组。

4. 单击创建。

创建身份验证策略

> 注意
>
> 如果使用 AAA.Login 配置具有策略规则的第一因素策略，则必须使用 OR 条件配置以下表达式，Citrix Workspace 应用程序才能支持 nFactor 部署。
>
> ```
> || HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
> ```

1. 导航到 安全**-> NetScaler AAA** —应用程序流量**->** 策略**->** 身份验证**->** 高级策略**->** 策略。
2. 选择“添 加”按钮
3. 完成以下信息以创建身份验证策略。设置名称右侧的 * 符号表示必填字段。

   a) 名称—输入高级身份验证策略的名称。必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) 磅 (#)、空格 ()、at (@)、等于 (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   b) 操作类型 -输入身份验证操作的类型。

   c) 操作 -输入策略匹配时要执行的身份验证操作的名称。

   d) 日志操作 -输入请求与此策略匹配时要使用的消息日志操作的名称。

   e) 表达式 -输入策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 NetScaler 命名规则的名称或默认语法表达式。

   f) 备 注—输入任何注释以保留有关此策略的信息。

4. 单击创建

添加 **LDAP** 身份验证服务器

1. 导航到 安全**-> NetScaler AAA** —应用程序流量**->** 策略**->** 身份验证**->** 基本策略**-> LDAP**。
2. 通过选择“服务器”选项卡并选择“添加”按钮来 添 加 LDAP 服 务器。

添加 **LDAP** 身份验证策略

1. 转到 安全 **> NetScaler AAA** —应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 策略。
2. 单击 添加 以添加身份验证策略。
3. 完成以下信息以创建身份验证策略。设置名称右侧的 * 符号表示必填字段。

   a) 名称 -高级身份验证策略的名称。
   必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) 磅 (#)、空格 ()、at (@)、等于 (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   b) 操作类型 -身份验证操作的类型。

   c) 操作 -策略匹配时要执行的身份验证操作的名称。

   d) 日志操作 -请求与此策略匹配时要使用的消息日志操作的名称。

   e) 表达式 -策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 NetScaler 命名规则或默认语法表达式的名称。

   f) 评论 -保留有关此策略的信息的任何评论。
4. 单击“创建”。

添加 **RADIUS** 身份验证服务器

1. 导航到 安全 **> NetScaler AAA** —应用程序流量 **>** 策略 身份验证 **>** 基本策略 **> RADIUS**。
2. 要添加服务器，请选择服务 器 选项卡，然后选择 添加 按钮。
3. 输入以下命令以创建身份验证 RADIUS 服务器。设置名称右侧的 * 符号表示必填字段。
   a) 输入 RADIUS 操作的 名称。
   b) 输入分配给 RADIUS 服务器的 服务器名称 或 服务器 **IP** 地址。
   c) 输 入 RADIUS 服务器侦听连接的端口号。
   d) 在几秒钟内输入 超 时值。NetScaler 设备将等待 RADIUS 服务器的响应，直到配置的超时值到期。
   e) 输入 RADIUS 服务器和 NetScaler 设备之间共享的 密钥。需要密钥才能允许 NetScaler 设备与 RADIUS 服务器进行通信。
   f) 确认密钥。
4. 单击“创建”。

添加 **RADIUS** 身份验证策略

1. 导航到 安全 **> NetScaler AAA** —应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 策略。
2. 单击 添加 创建身份验证策略。
3. 完成以下信息以创建身份验证策略。设置名称右侧的 * 符号表示必填字段。

   a) 名称 -高级身份验证策略的名称。
   必须以字母、数字或下划线字符 (_) 开头，并且必须仅包含字母、数字和连字符 (-)、句点 (.) 磅 (#)、空格 ()、at (@)、等于 (=)、冒号 (:) 和下划线字符。创建身份验证策略后无法更改。

   以下要求仅适用于 NetScaler CLI：如果名称包含一个或多个空格，请将名称用双引号或单引号括起来（例如，“我的身份验证策略”或“我的身份验证策略”）。

   a) 操作类型 -身份验证操作的类型。

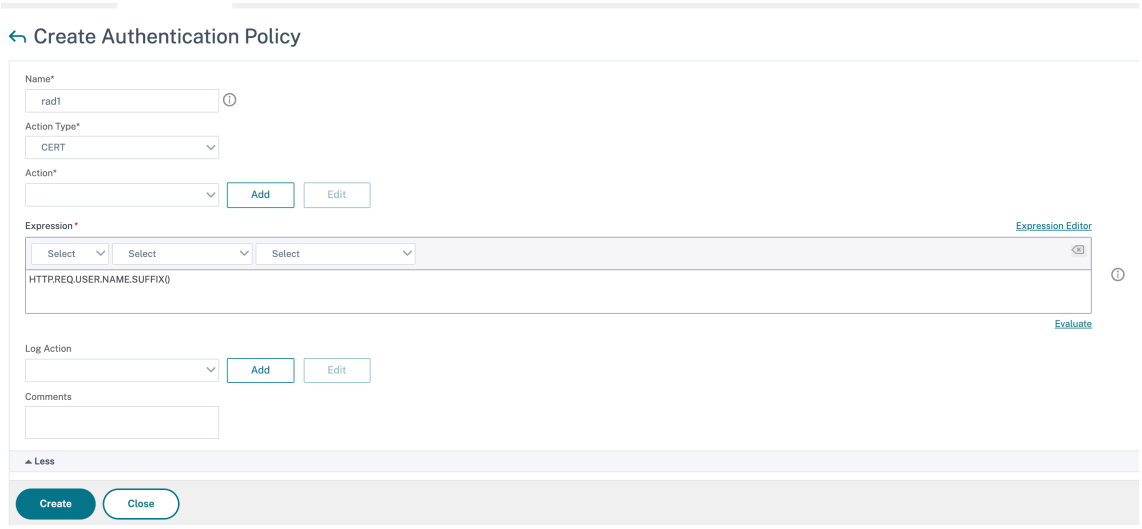
   b) 操作 -策略匹配时要执行的身份验证操作的名称。

   c) 日志操作 -请求与此策略匹配时使用的消息日志操作的名称。

   d) 表达式 -策略用于确定是否尝试使用身份验证服务器对用户进行身份验证的 NetScaler 命名规则或默认语法表达式的名称。

   e) 评论 - 用于保留有关本策略的信息的任何评论。

4. 单击“确定”。您创建的身份验证策略将列在策略列表中。



创建身份验证登录架构

1. 导航到 安全 **> NetScaler AAA** —应用程序流量 **>** 登录架构。
2. 选择配置文件选项卡，然后单击 添加 按钮。

3. 填写以下字段以创建身份验证登录架构：

   a) 输入 名称—新登录架构的名称。

   b) 输入 身份验证架构 -用于读取要为登录页面 UI 发送的身份验证架构的文件的名称。根据 Citrix Forms 身份验证协议，此文件必须包含元素的 xml 定义，才能呈现登录表单。如果管理员不想提示用户输入更多凭据，但继续使用先前获取的凭据，则可以将noschema “” 作为参数提供。这仅适用于与用户定义因素一起使用的 loginSchema，而不适用于虚拟服务器因素

   c) 输入 用户表达式 -登录期间用户名提取的表达式

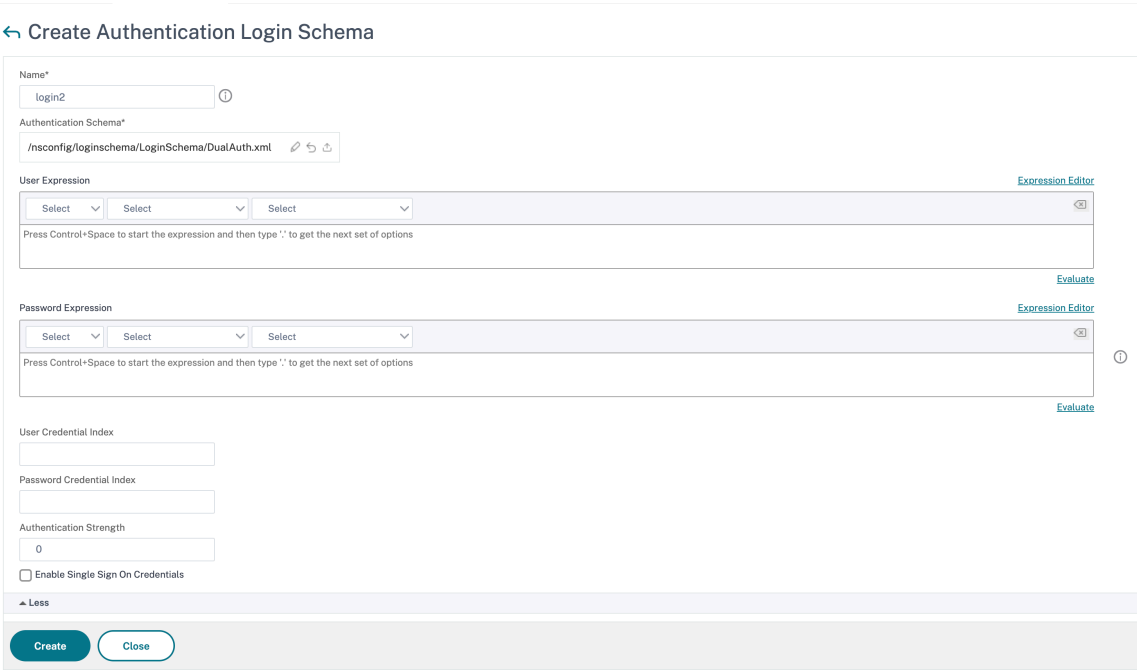
   d) 输入 密码表达式 -登录时提取密码的表达式

   e) 输入 用户凭据索引 -用户输入的用户名存储在会话中的索引。

   f) 输入 密码凭据索引 -用户输入的密码必须存储在会话中的索引。

   g) 输入 身份验证强度 -当前身份验证的权重。

4. 单击 “创建”。您创建的登录架构配置文件必须出现在登录架构配置文件列表中。



创建策略标签

策略标签指定特定因素的身份验证策略。每个策略标签对应于一个因素。策略标签指定必须向用户显示的登录表单。必须将策略标签绑定为身份验证策略或另一个身份验证策略标签的下一个因素。通常情况下，策略标签包括特定身份验证机制的身份验证策略。但是，您也可以拥有针对不同身份验证机制的身份验证策略的策略标签。

1. 导航到 安全 **> NetScaler AAA** —应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 策略标签。
2. 单击添加按钮。

3. 填写以下字段以创建身份验证策略标签：

   a) 输入新身份验证策略标签的 名称。

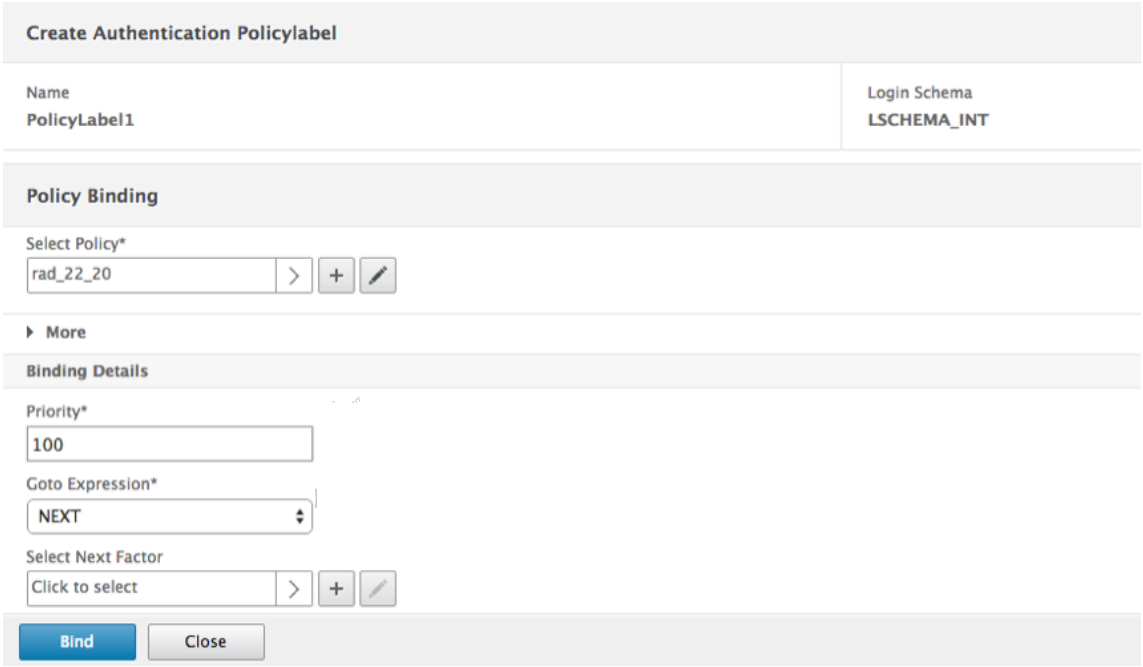
   b) 输入与身份验证策略标签关联的 登录架构。

   c) 单击继续。

4. 从下拉菜单中选择策略。
5. 选择所需的 身份验证策略，然后单击选 择 按钮。
6. 填写以下字段：

   a) 输入策略绑定的 优先级。

   b) 输入 **Gto** 表达式—表 达式指定当前策略规则的计算结果为 TRUE 时将评估的下一个策略的优先级。



7. 选择所需的身份验证策略，然后单击 选择 按钮。
8. 单击“绑定”按钮。
9. 单击 **Done**（完成）。
10. 查看身份验证策略标签。

nFactor 身份验证的 **re-Captcha** 配置

从 NetScaler 版本 12.1 build 50.x 开始，NetScaler Gateway 支持新的头等舱操作“captchaAction”，该操作可简化 Captcha 配置。由于 Captcha 是一流的诉讼，因此它可能是其自身的一个因素。您可以在 nFactor 流程中的任何地方注入 Captcha。

以前，您还必须编写自定义的 WebAuth 策略，并对 RfWebUI 进行更改。随着 captchaACtion 的引入，您不必修改 JavaScript。

> 重要
>
> 如果在架构中将 Captcha 与用户名或密码字段一起使用，则在满足 Captcha 之前，“提交”按钮将被禁用。

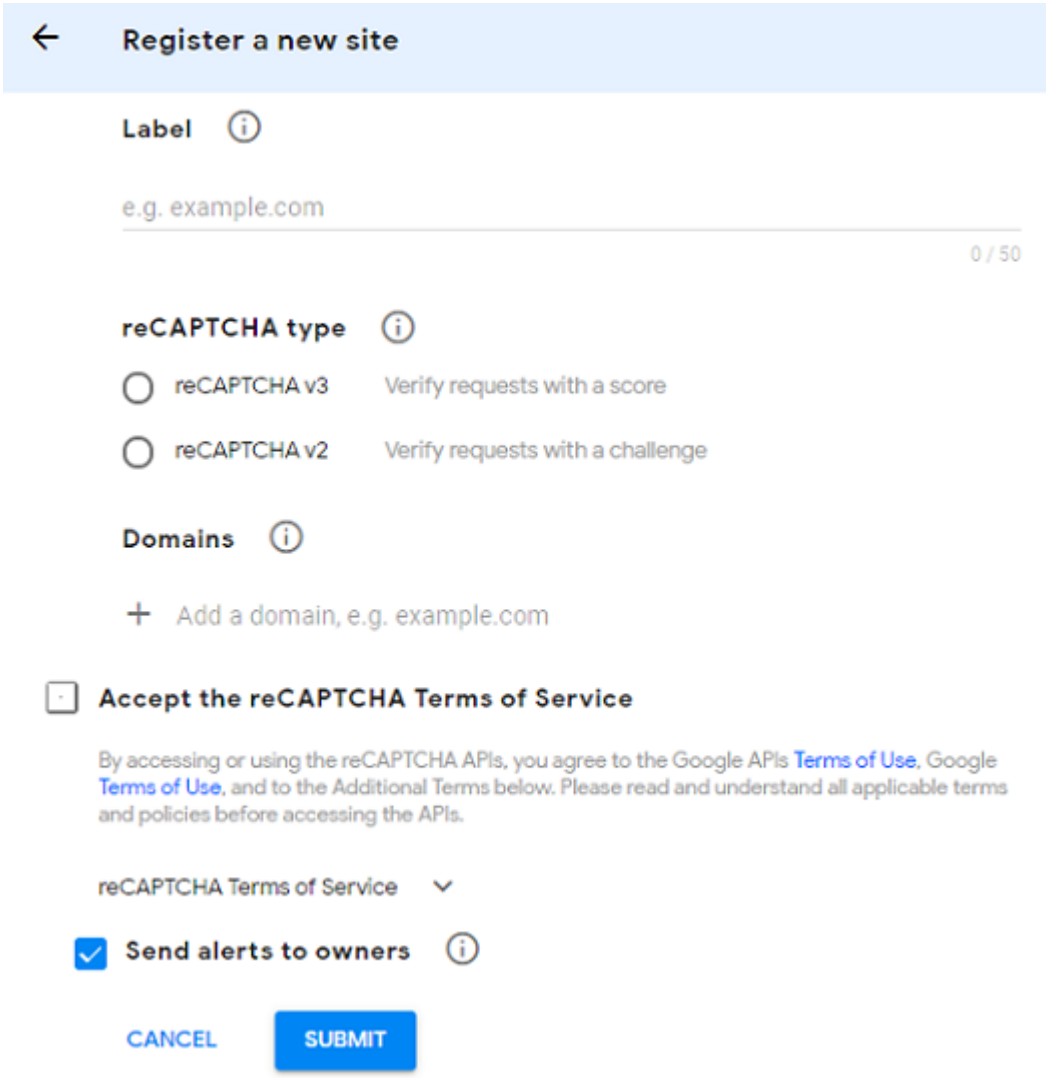
Captcha 配置

Captcha 配置涉及两个部分。

1. Google 上用于注册 Captcha 的配置。
2. NetScaler 设备上的配置以将 Captcha 用作登录流程的一部分。

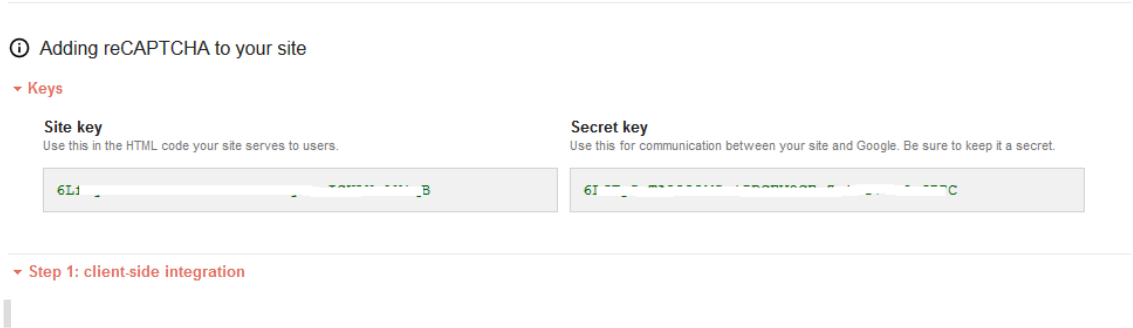
Google 上的 Captcha 配置 在以下位置注册 Captcha 的域：https://www.google.com/recaptcha/admin#list。

1. 导航到此页面时，将显示以下屏幕。



> 注意
>
> 只能使用 reCAPTCHA v2。“不可见的 reCAPTCHA”仍在预览中。

2. 注册域名后，将显示“SiteKey”和“SecretKey”。



> 注意
>
> 出于安全原因，“SiteKey”和“SecretKey”显示为灰色。“SecretKey”必须保持安全。

NetScaler 设备上的 **Captcha** 配置　NetScaler 设备上的 Captcha 配置可分为三个部分：

- 显示 Captcha 屏幕
- 将 Captcha 响应发布到 Google 服务器
- LDAP 配置是用户登录的第二个因素（可选）

显示 **Captcha** 屏幕　登录表单自定义是通过 SingleAuthCaptcha.xml 登录架构完成的。此自定义在身份验证虚拟服务器上指定，并发送到 UI 以呈现登录表单。内置登录架构 SingleAuthCaptcha.xml 位于 NetScaler 设备上的 /nsconfig/loginSchema/LoginSchema 目录中。

> 重要
>
> - 可以修改现有架构，具体取决于您的用例和不同的架构。例如，如果您只需要 Captcha 因素（没有用户名或密码）或使用 Captcha 进行双重身份验证。
> - 如果执行了任何自定义修改或重命名了文件，Citrix 建议将所有登录架构从 /nsconfig/loginschema/LoginSchema 目录复制到父目录 /nsconfig/loginschema。

使用 **CLI** 配置 **Captcha** 的显示

```
1  -  add authentication loginSchema singleauthcaptcha -
       authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3  -  add authentication loginSchemaPolicy singleauthcaptcha -rule true -
       action singleauthcaptcha
4
5  -  add authentication vserver auth SSL <IP> <Port>
6
7  -  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to
       -key-file>
8  -  bind ssl vserver auth -certkey vserver-cert
9  -  bind authentication vserver auth -policy singleauthcaptcha -priority
        5 -gotoPriorityExpression END
10 <!--NeedCopy-->
```

将 **Captcha** 响应发布到 **Google** 服务器　配置必须向用户显示的 Captcha 后，管理员会将配置发布到 Google 服务器，以验证来自浏览器的 Captcha 响应。

验证来自浏览器的 **Captcha** 响应

```
1  -  add authentication captchaAction myrecaptcha -sitekey <sitekey-
       copied-from-google> -secretkey <secretkey-from-google>
2
3  -  add authentication policy myrecaptcha -rule true -action myrecaptcha
```



```
4  -  bind authentication vserver auth -policy myrecaptcha -priority 1
5  <!--NeedCopy-->
```

需要使用以下命令来配置是否需要 AD 身份验证。否则，您可以忽略此步骤。

```
1  -  add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
       636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn
      adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -
      encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
       memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -
      defaultAuthenticationGroup ldapGroup
2
3  -  add authenticationpolicy ldap-new -rule true -action ldap-new
4  <!--NeedCopy-->
```

LDAP 配置是用户登录的第二个因素（可选） LDAP 身份验证发生在 Captcha 之后，您将其添加到第二个因素中。

```
1  -  add authentication policylabel second-factor
2  -  bind authentication policylabel second-factor -policy ldap-new -
      priority 10
3  -  bind authentication vserver auth -policy myrecaptcha -priority 1 -
      nextFactor second-factor
4  <!--NeedCopy-->
```

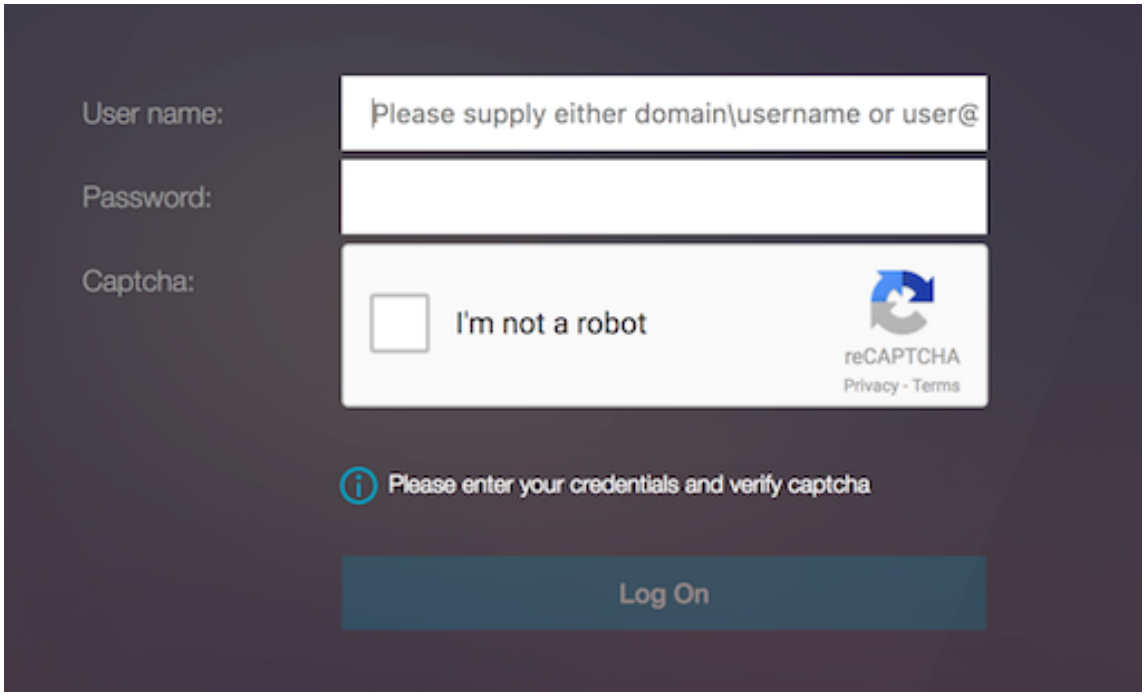
管理员需要添加相应的虚拟服务器，具体取决于是使用负载平衡虚拟服务器还是 NetScaler Gateway 设备进行访问。如果需要负载平衡虚拟服务器，管理员必须配置以下命令：

```
1  add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
      authenticationHost nssp.aaatm.com`
2  <!--NeedCopy-->
```

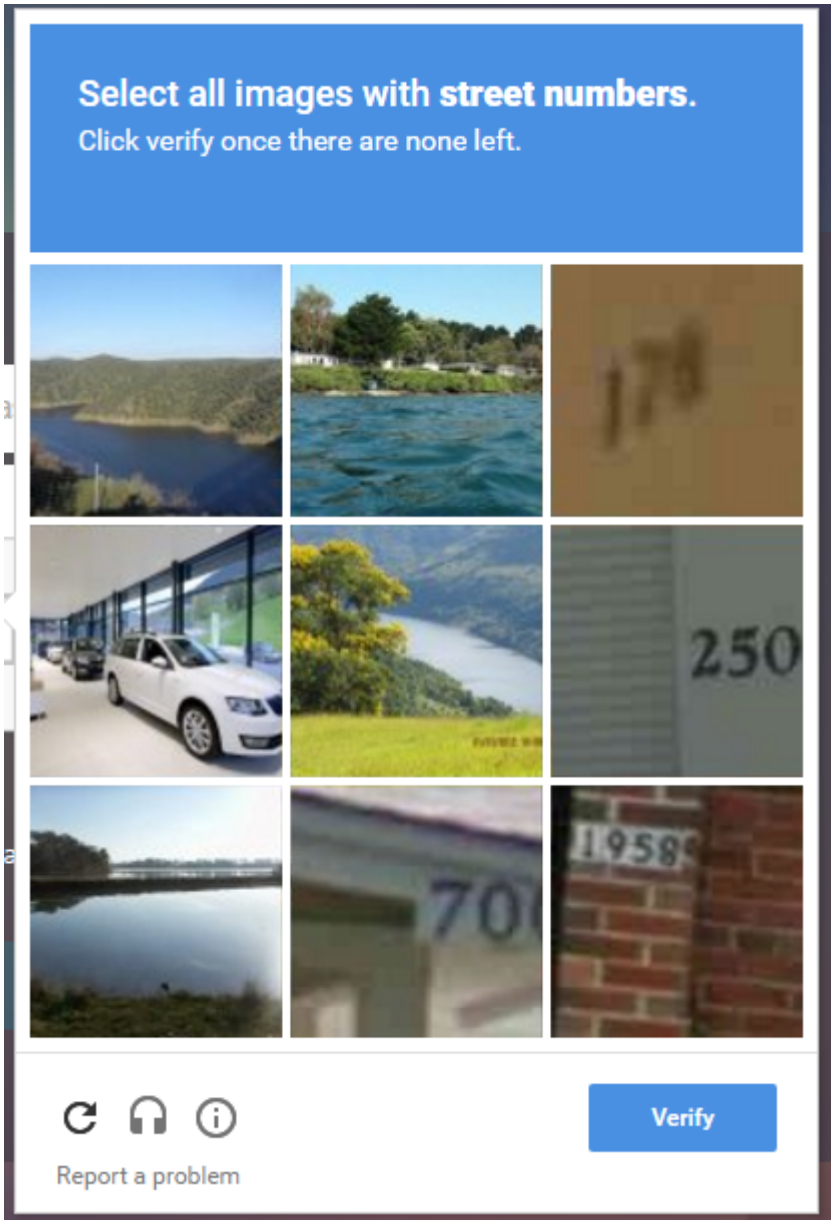
nssp.aaatm.com - 解析为身份验证虚拟服务器。

Captcha 的用户验证 配置完上述部分中提到的所有步骤后，请参阅前面的用户界面屏幕截图。

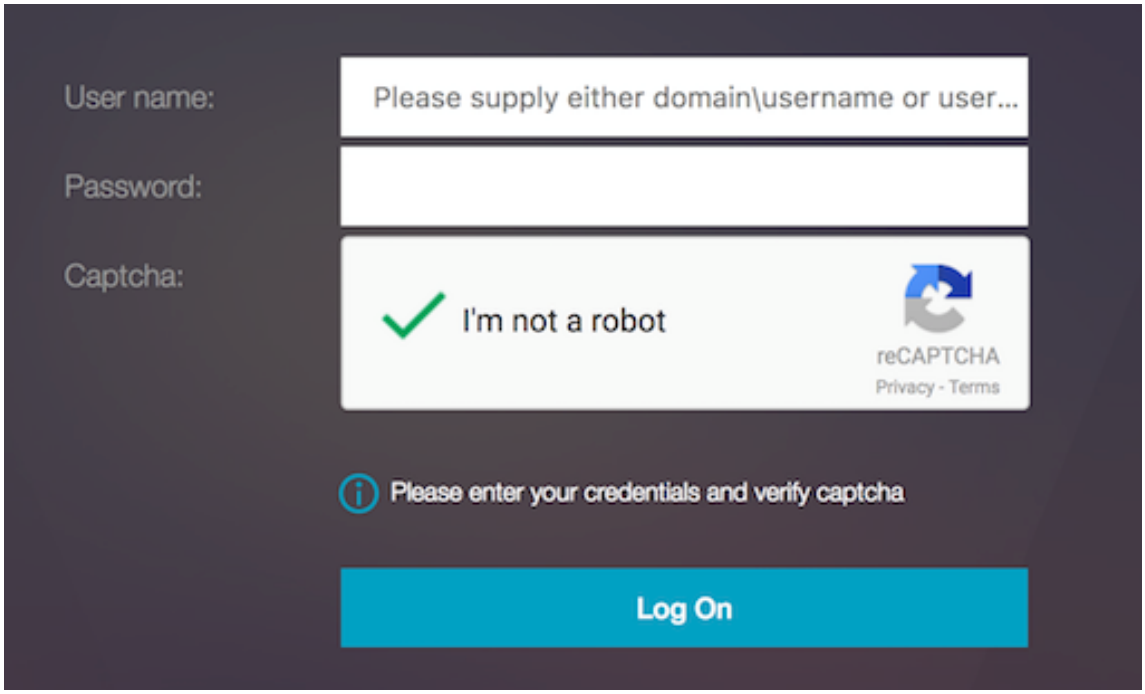
1. 身份验证虚拟服务器加载登录页面后，将显示登录屏幕。在 Captcha 完成之前，登录将被禁用。



2. 选择“我不是机器人”选项。此时将显示 Captcha 小部件。



3. 在显示完成页面之前，您将浏览一系列 Captcha 图像。
4. 输入 AD 凭据，选中 **I'm not a robot**（我不是机器人）复选框，然后单击 **Log On**（登录）。如果身份验证成功，您将被重定向到所需的资源。

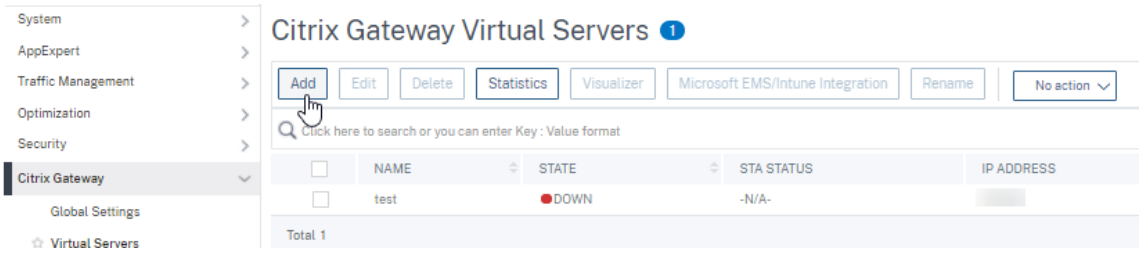


注意：

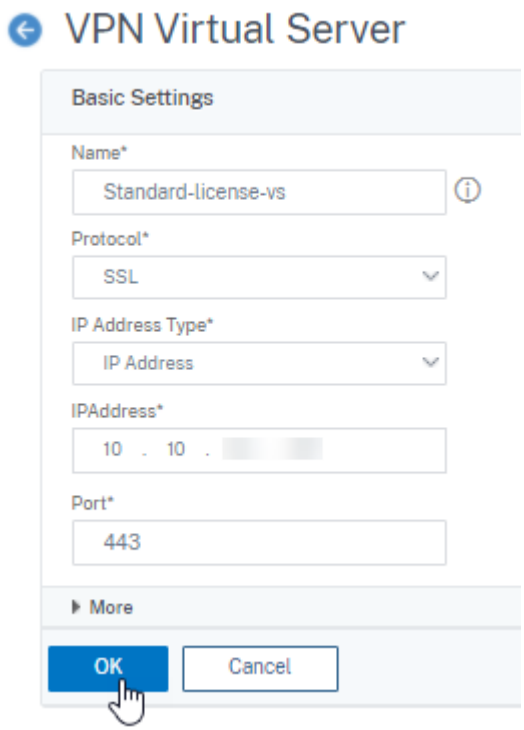
- 如果 Captcha 与 AD 身份验证一起使用，则在 Captcha 完成之前，凭据的“提交”按钮将被禁用。
- Captcha 发生在其自身的一个因素中。因此，任何后续验证（如 AD）都必须在 Captcha 的 `nextfactor` 中进行。

在 **NetScaler** 标准许可证中创建用于 **nFactor** 身份验证的网关虚拟服务器

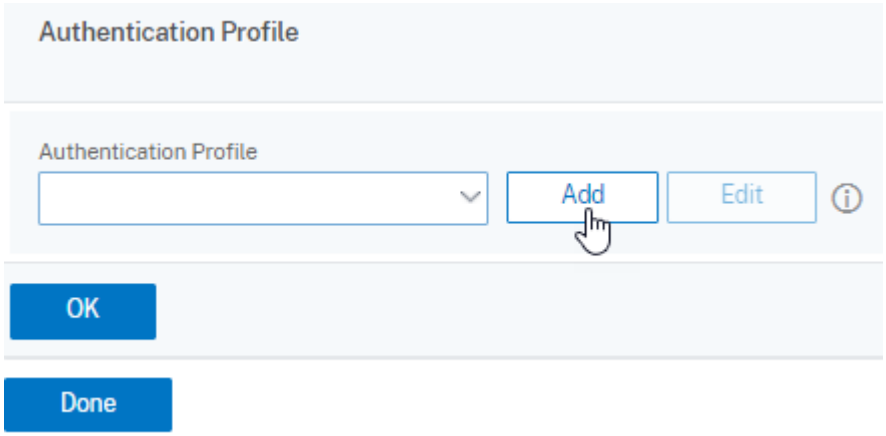
1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 在 **NetScaler Gateway** 虚拟服务器 页面上，单击 添加。



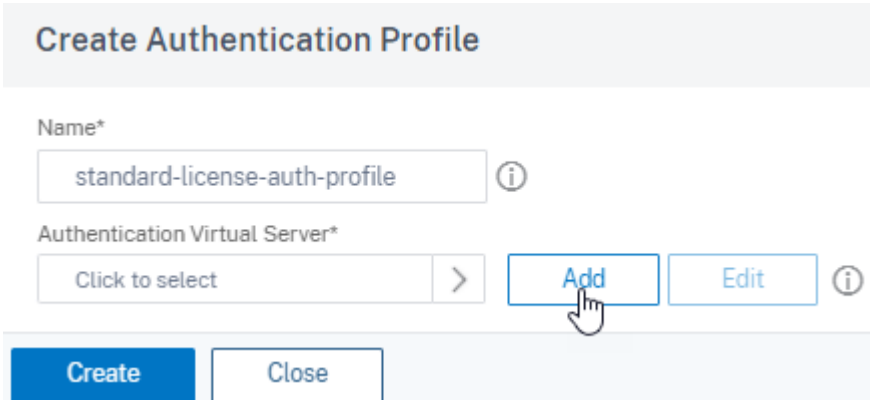
3. 在 **VPN** 虚拟服务器页面上输入以下详细信息，单击“确定”，然后单击“继续”。
   - 名称-NetScaler Gateway 虚拟服务器的名称
   - 协议-选择 **SSL**
   - IP 地址-NetScaler Gateway 虚拟服务器的 IP 地址
   - 端口-输入 443



4. 在 **VPN** 虚拟服务器 页面上，单击 身份验证配置文件旁边的加号图标。
5. 单击 添加 以配置身份验证配置文件。

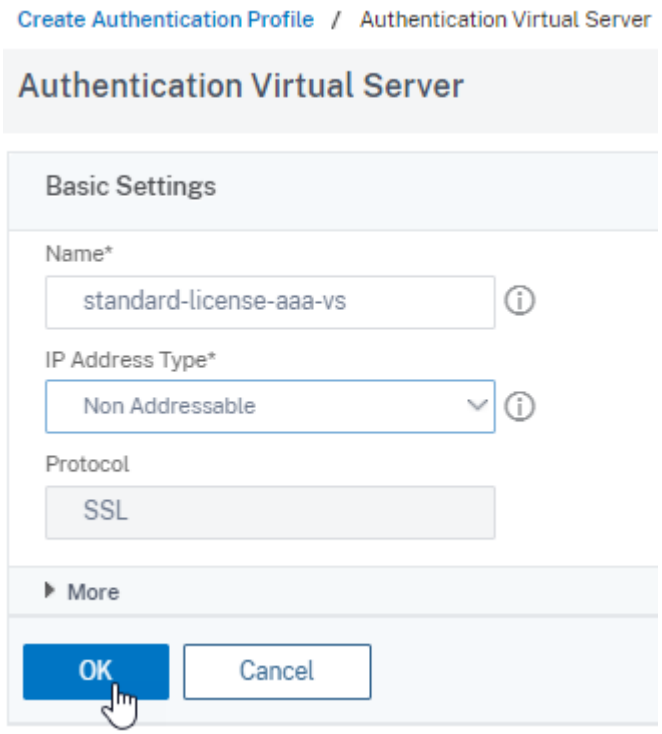


6. 输入身份验证配置文件的名称，然后单击 添加。



7. 在 **VPN** 虚拟服务器页面上输入以下详细信息，单击“确定”，然后单击“继续”。

   - 名称—身份验证、授权和审核虚拟服务器的名称
   - 协议-选择 不可寻址。在 NetScaler Standard 许可证中，只有不可寻址的身份验证、授权和审核虚拟服务器才能绑定到网关/VPN 虚拟服务器。



> 注意：
>
> - 在 NetScaler 标准许可证中，创建策略的步骤与支持的策略类型的高级许可证相同。
> - NetScaler 标准许可证不支持在 nFactor 配置中添加新的登录架构。

引用

有关端到端 nFactor 配置示例，请参阅 配置 nFactor 身份验证。

Unified Gateway 可视化工具

February 1, 2024

Unified Gateway 可视化工具使用 Unified Gateway 向导提供配置的可视表示。Unified Gateway 可视化工具用于添加和编辑配置以及诊断后端问题。

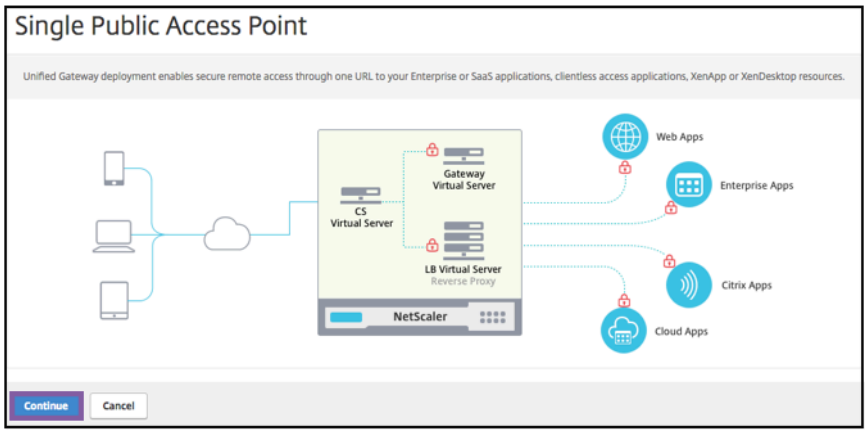
Unified Gateway 可视化工具显示以下内容：

配置	配置
身份验证前策略	身份验证策略
CS 虚拟服务器	VPN 虚拟服务器
LB 虚拟服务器	XA/XD 应用程序
网络应用程序	SaaS 应用程序

Unified Gateway 部署可通过一个 URL 安全地远程访问企业或 SaaS 应用程序、无客户端访问应用程序、Citrix Virtual Apps 和桌面资源。

配置 Unified Gateway

1. 从菜单中选择 Unified Gateway。
2. 在下一个屏幕上，确认您有以下信息，然后单击“开始使用”：
    - Unified Gateway 的公有 IP 地址。
    - 带有可选 Root-CA 证书的服务器证书链（.PFX 或.PEM）。
    - 基于 LDAP /RADIUS/客户端证书的身份验证详细信息
    - 应用程序详细信息（SaaS 应用程序的 URL 或 Citrix Virtual Apps and Desktops 服务器详细信息）
3. 单击“继续”按钮。

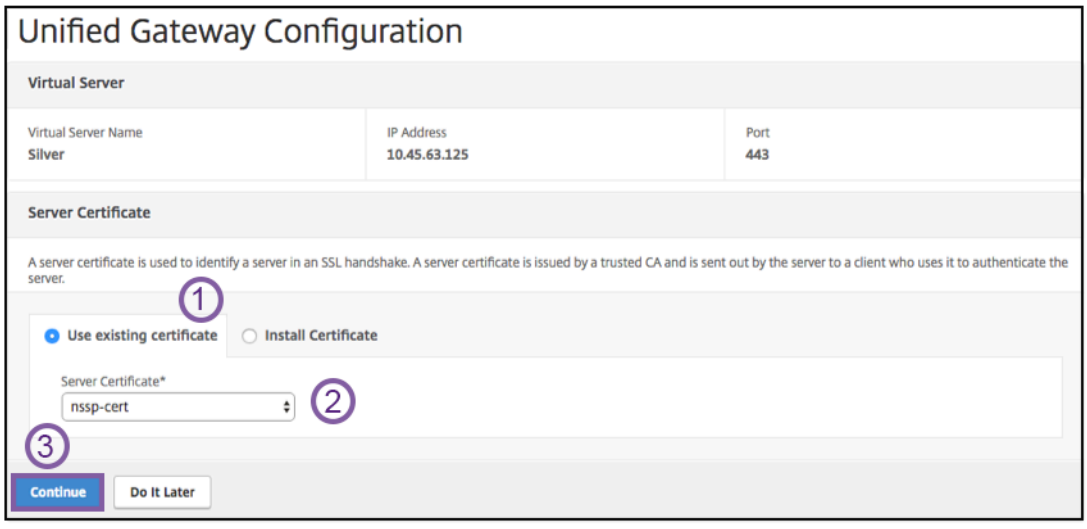


创建 **Unified Gateway** 配置虚拟服务器。

1. 输入虚拟服务器的配置 名称。
2. 输入 **Unified Gateway** 部署的面向公众的 **Unified Gateway IP** 地址。
3. 输入 端口 号。端口号范围为 1—65535。
4. 单击继续。

填写以下信息以指定服务器证书。

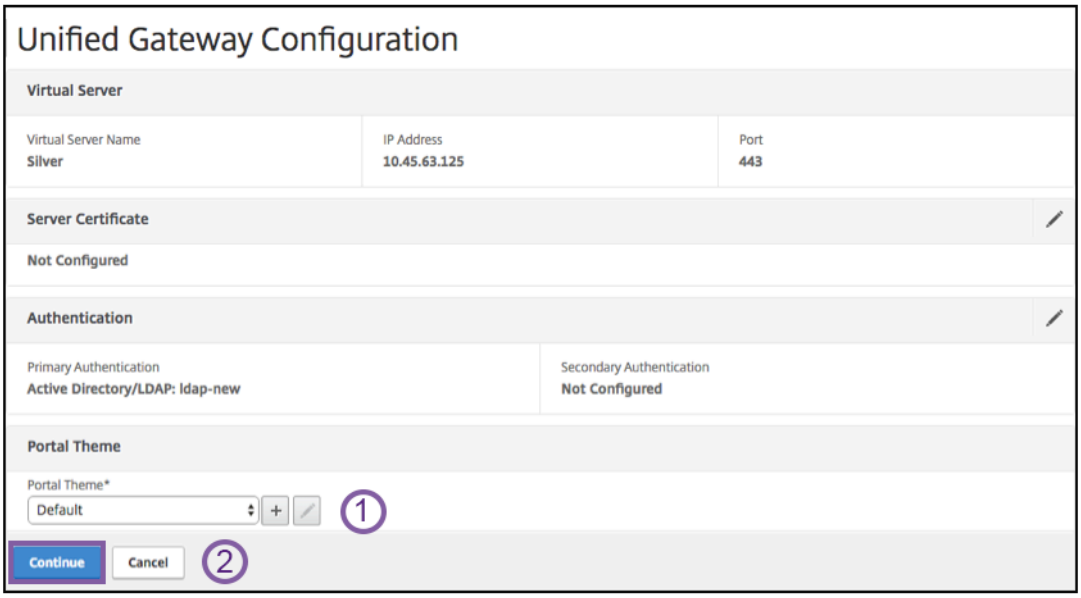
1. 选择 使用现有证书 或 安装证书 单选按钮。
2. 从菜单中选择 服务器证书。
3. 单击“继续”按钮。



完成以下信息以指定身份验证。

1. 从菜单中选择 主要身份验证方法。
2. 选择 使用现有服务器 或 添加新服务器 单选按钮。
3. 单击“继续”按钮。
4. 从菜单中选择 门户主题。

5. 单击继续。
6. 选择 **Web** 应用程序 或 **Citrix Virtual Apps** 桌面 单选按钮。
7. 单击继续。



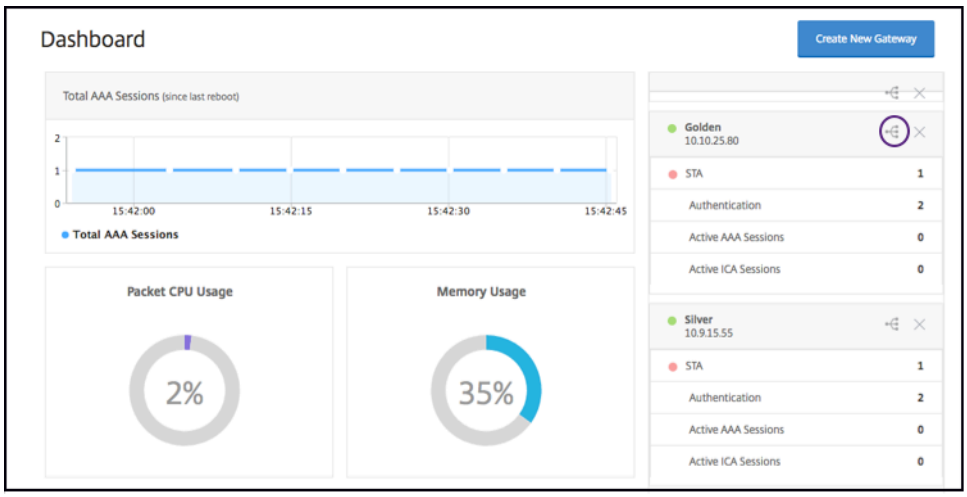
选择应用

完成以下信息以指定 **Web** 应用程序。

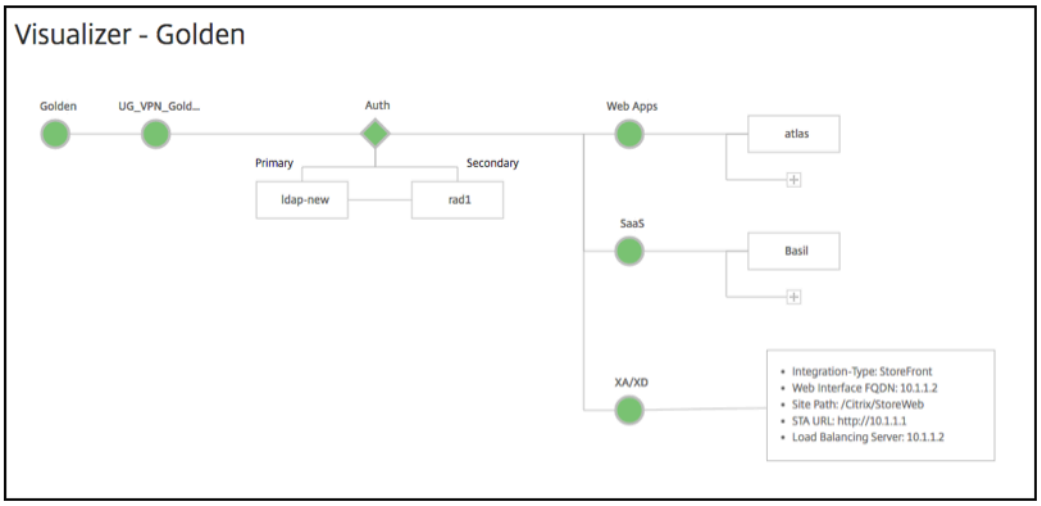
1. 输入书签链接的名称。
2. 选择 VPN URL 代表的应用程序类型。可能的值如下：
   - 内联网应用程序
   - 无客户端访问
   - SaaS
   - 此 NetScaler 上预配置的应用程序
3. 选中此框可使此应用程序可通过 Unified Gateway URL 访问。
4. 输入书签链接的 URL。
5. 从图标 URL 中选择一个文件来获取图标文件。MaxLength = 255
6. 单击“继续”按钮。
7. 单击 **Done**（完成）。
8. 单击继续。
9. 单击 **Done**（完成）。

GUI 配置

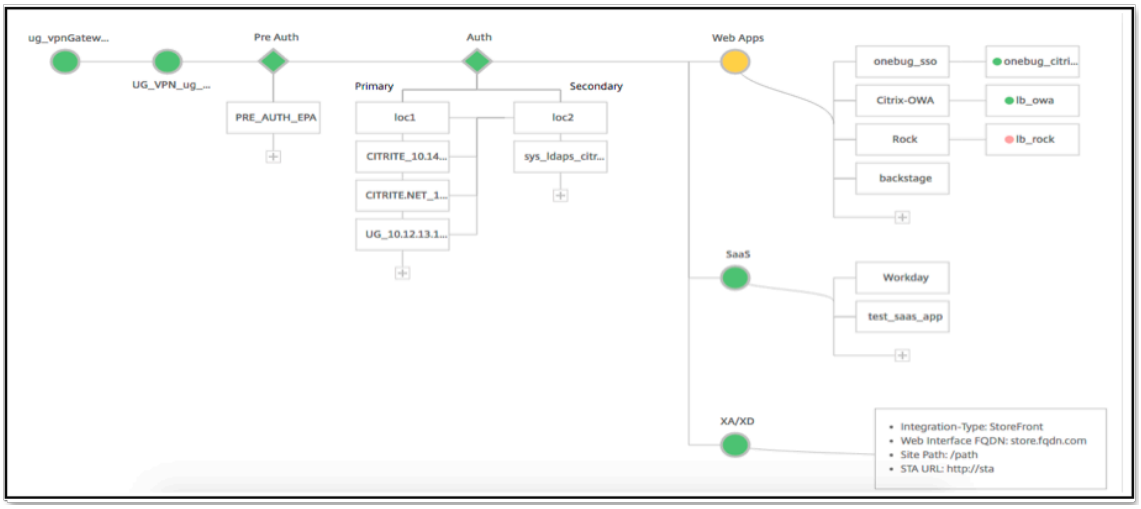
1. 从菜单中选择 Unified Gateway。
2. 单击 **Unified Gateway** 可视化工具 图标以访问已配置的网关实例。



Unified Gateway 可视化工具看起来像一个流程图，如下图所示：



Unified Gateway 可视化工具有 PreAuth `Auth`、和应用程序部分。如果 VPN 虚拟服务器具有预身份验证策略，则只有在 Unified Gateway 可视化工具中才会显示 `pre-auth`。



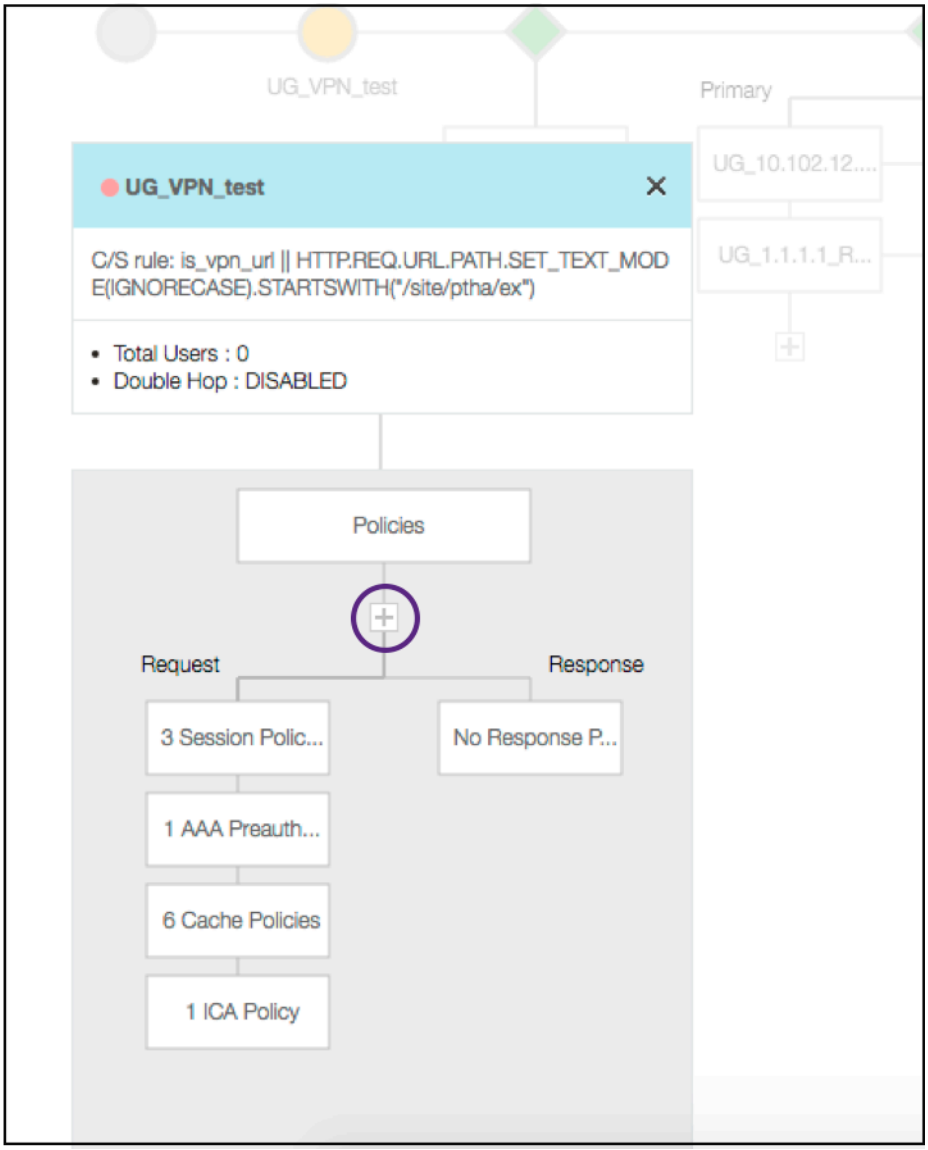
Unified Gateway 可视化工具对负载平衡和 VPN 虚拟服务器使用颜色编码方案来指示其状态。

颜色	说明
红色	表示服务器已关闭。
灰色	表示尚未配置 WebApp/Citrix Virtual Apps。
绿色	意味着虚拟服务器一切都很好。
橙色	表示负载平衡虚拟服务器服务之一。已关闭，但仍能正常运行。

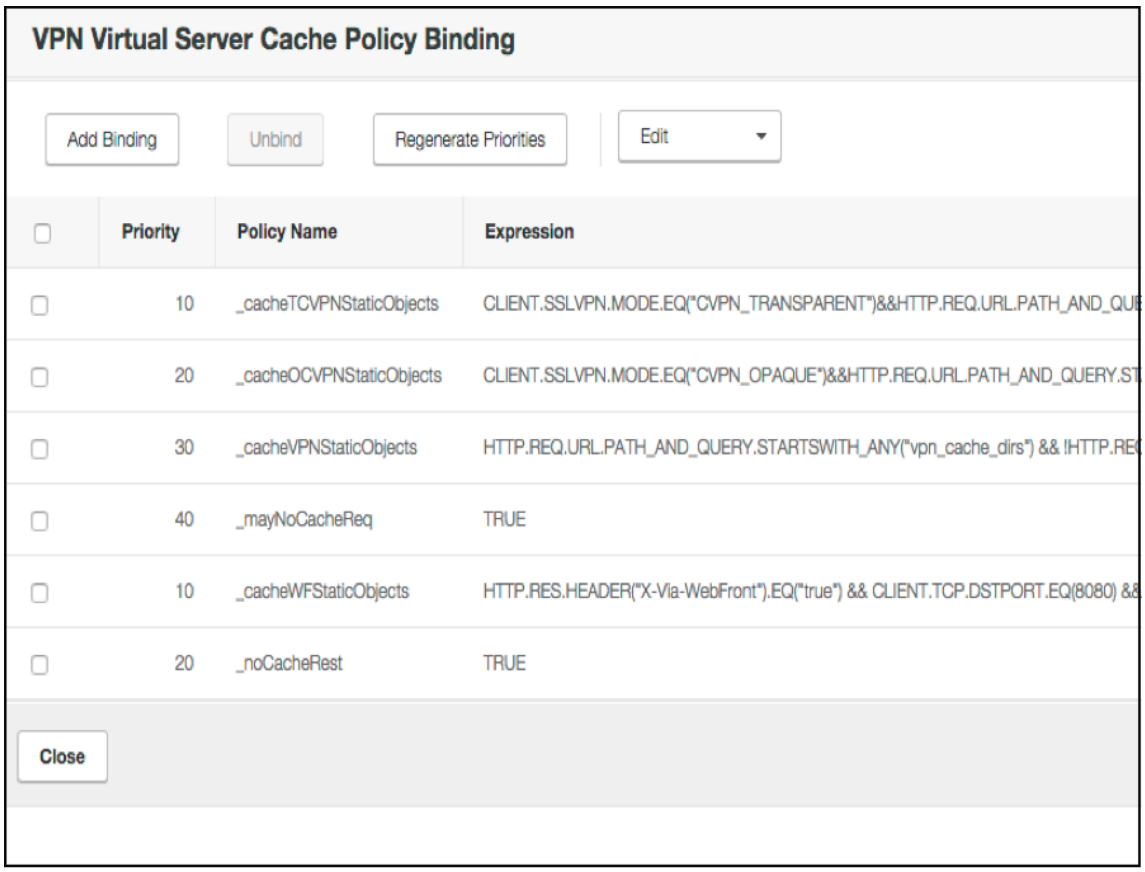
VPN 虚拟服务器的详细信息

要获取 VPN 虚拟服务器的详细信息，请单击 **VPN** 虚拟服务器节点。弹出窗口显示详细信息，例如 C/S 规则和所有策略。

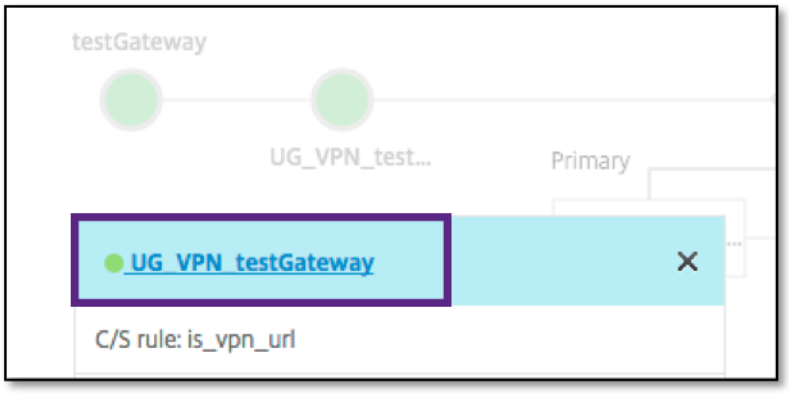
1. 通过单击 (+) 图标将策略添加到 VPN 实体。



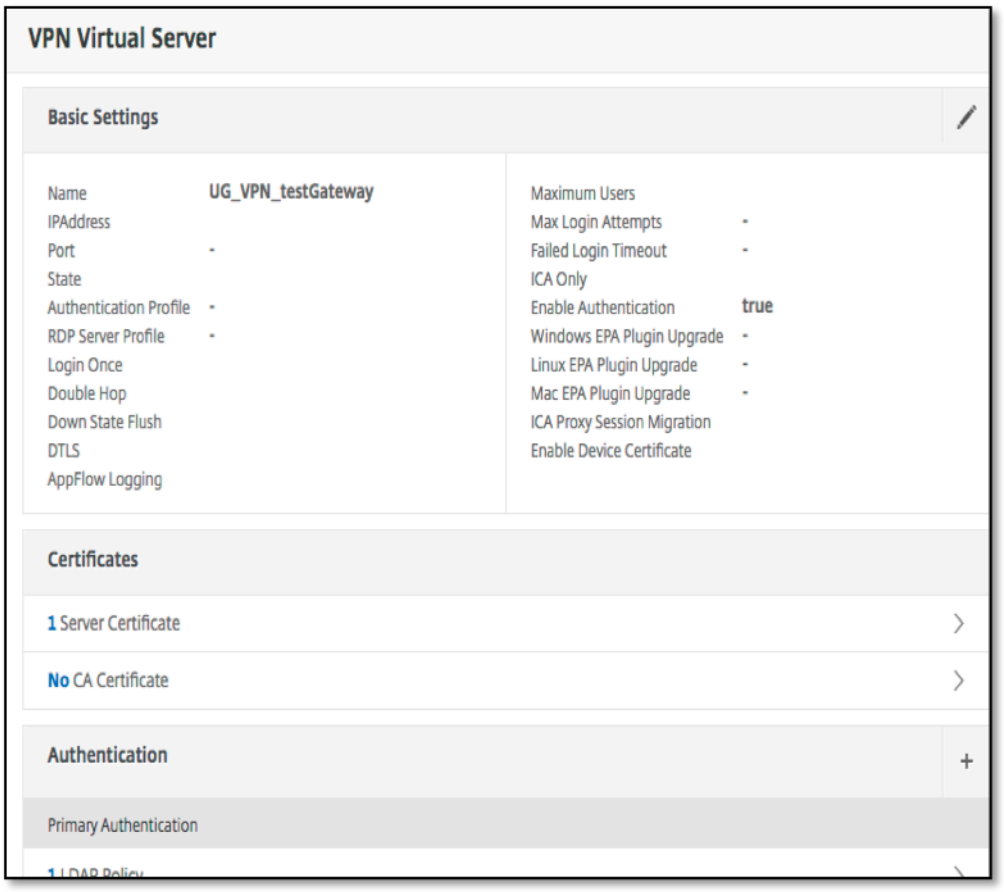
2. 单击所需的节点以获取已配置的策略的详细信息。



对于 VPN 虚拟服务器信息，弹出窗口中的 VPN 标题是一个可单击的实体，可转到详细说明 VPN 虚拟服务器的滑块。



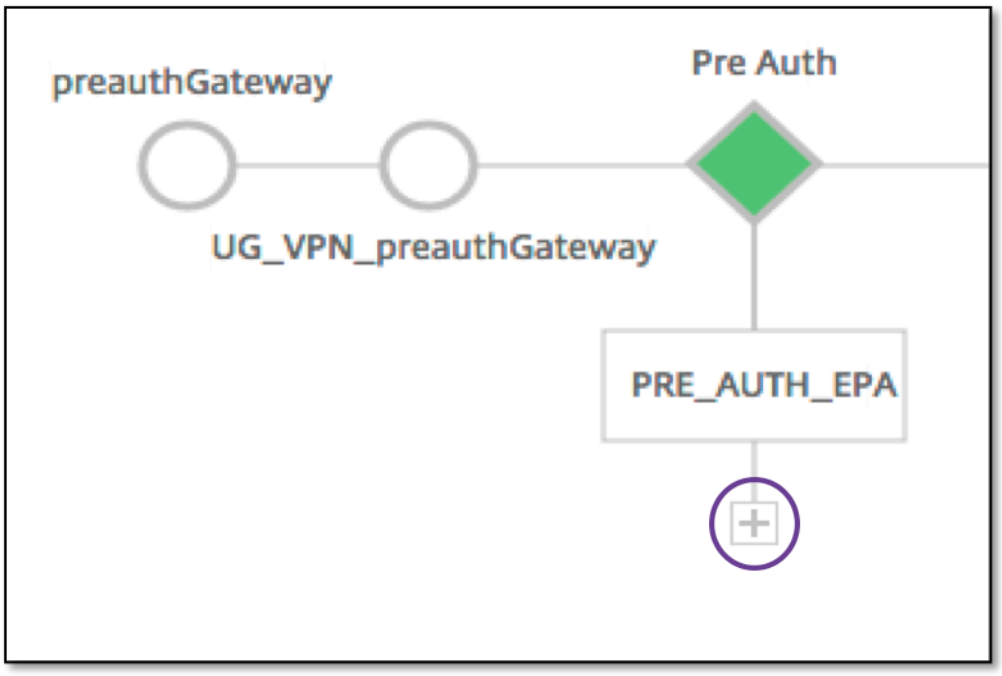
此处显示了 VPN 服务器的详细信息。



The Pre Auth Block

如果 VPN 虚拟服务器具有与之关联的预身份验证策略，Unified Gateway 可视化工具将显示一个 `Pre Auth` 块。`Pre Auth` 块显示策略，并提供向 VPN 添加预身份验证策略的选项。

1. 单击 **+** 添加 `preauth` 策略。

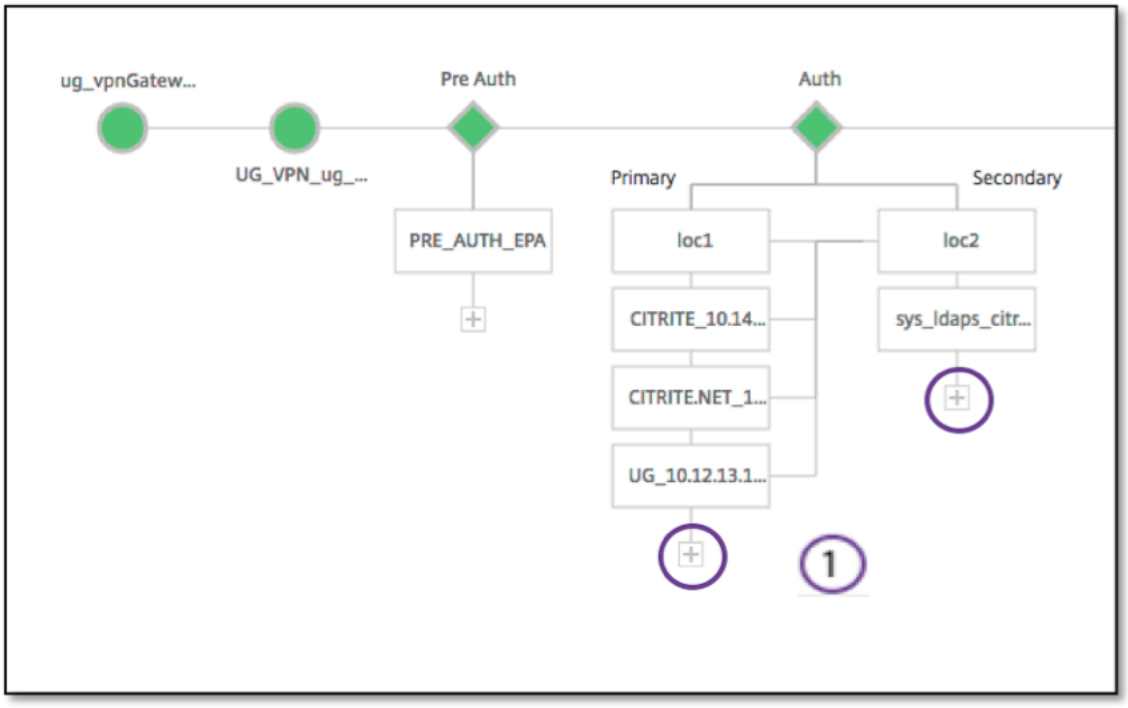


在没有关联预身份验证策略的情况下，此块将在视图中隐藏。

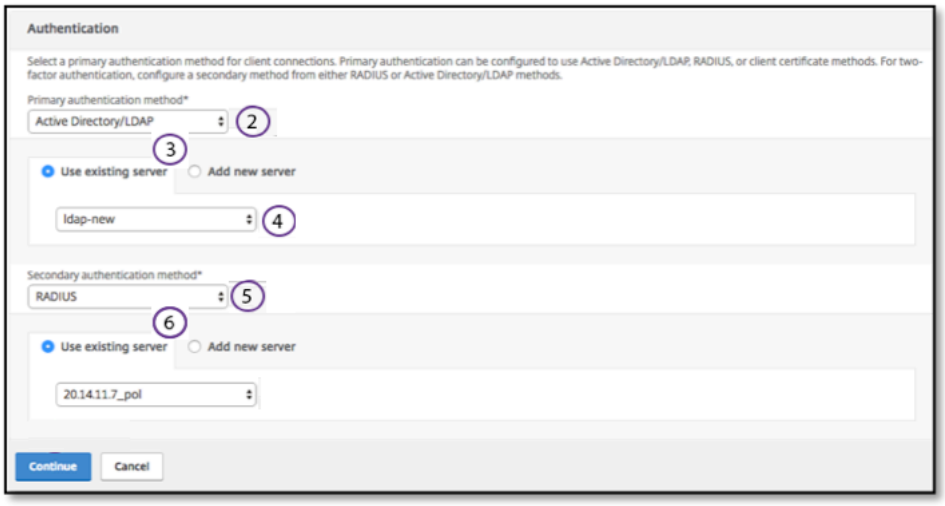
The Auth Block

Auth 块列出了主要和次要策略。Auth 块提供了添加策略的选项。

1. 单击主列表中的 **+** 添加主身份验证绑定，或单击辅助列表中的 + 添加辅助身份验证绑定。

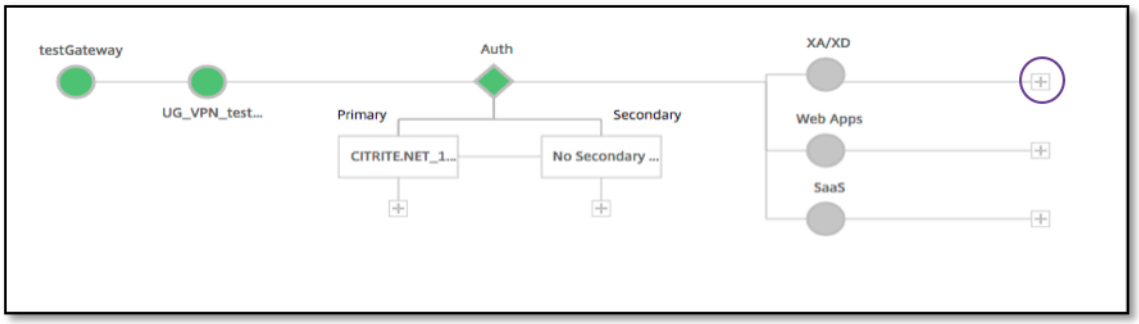


2. 从 主身份验证方法 菜单中选择一个选项。
3. 通过选择单选按钮来指定它是 现有服务器还是添加新服务器。
4. 从 **LDAP** 策略名称 菜单中选择一个选项。
5. 从 辅助身份验证方法 菜单中选择 **RADIUS** 。
6. 通过选择单选按钮来指定是要使用现有服务器还是添加新服务器。
7. 单击继续。



添加 **StoreFront**

1. 单击 XA/XD 附近的 **+** ，即可添加“XA/XD”应用程序。



您可以选择您的积分点。这些选项包括 StoreFront、WI 或 WionNS。单击继续。

1. 填写以下字段以配置 StoreFront。需要强制性信息的字段用 * 标注。

   |** 字段 **|** 说明 **|
   |–|–|
   |StoreFront FQDN*| 输入 StoreFront 服务器的 FQDN。最大长度：255 个字符。示例：//store-front.xendt.net|

| 站点路径 *| 输入已在 StoreFront 上配置的网站的 Receiver 路径。|
|Single Sign-on Domain*| 输入用户身份验证的默认域 |
| 店铺名称 *| 输入 StoreFront 显示器的名称。
STORENAME 是一个参数，用于定义 StoreFront 服务商店名称以探测 StoreFront 服务器的运行状况。适用于 StoreFront 显示器。最大长度：31|
| 安全票证颁发机构服务器 *| 输入 Secure Ticket Authority URL，通常显示在交付控制器上。
示例：http://sta|
|StoreFront 服务器 *| 输入 StoreFront 服务器的 IP 地址
	协议 *	输入服务器使用的协议。
端口 *	输入服务器使用的端口。
负载平衡	输入 StoreFront 服务器的负载平衡配置。
虚拟服务器 *	输入 Unified Gateway 部署的面向公众的 IP 地址。

2. 单击“继续”。

添加 **SaaS**

1. 单击 **+** 添加 SaaS 应用程序，它将转到添加 SaaS 页面。填写以下字段以配置 SaaS。需要强制性信息的字段用 * 标注。

字段	说明
名称 *	输入书签链接的名称。
应用程序类型	输入此 VPN URL 代表的应用程序类型。可能的值包括：此 NetScaler 上的 Intranet 应用程序/无客户端访问/SaaS /预配置应用程序
输入 URL *	输入内联网应用程序的 URL。
选择 文件	输入 URL 以获取用于显示此资源的图标文件。MaxLength = 255

添加 **WebApp**

1. 单击 **+** 添加 Web 应用程序，它将转到添加 Web 应用程序页面。要配置 Web 应用程序，请填写以下字段。需要强制性信息的字段用 * 标注。

字段	说明
名称 *	输入书签链接的名称。

字段	说明
应用程序类型	输入此 VPN URL 代表的应用程序类型。可能的值包括：此 NetScaler 上的 Intranet 应用程序/无客户端访问/SaaS /预配置应用程序
输入 URL *	输入内联网应用程序的 URL。
选择 文件	输入 URL 以获取用于显示此 resource.MaxLength = 255 的图标文件。

如果可以通过 Unified Gateway URL 访问应用程序，则可以通过单击该应用程序来访问负载平衡服务器的详细信息：

单击 (+) 可以添加新策略，单击显示策略信息的节点可以查看所有绑定的策略。

还会显示绑定到负载平衡器的服务数量以及整体状态信息。进一步单击列出所有服务。可以向负载平衡器添加新服务。

有关负载平衡器的更多详细信息，可单击弹出窗口的标题，进入负载平衡虚拟服务器详细信息页面。

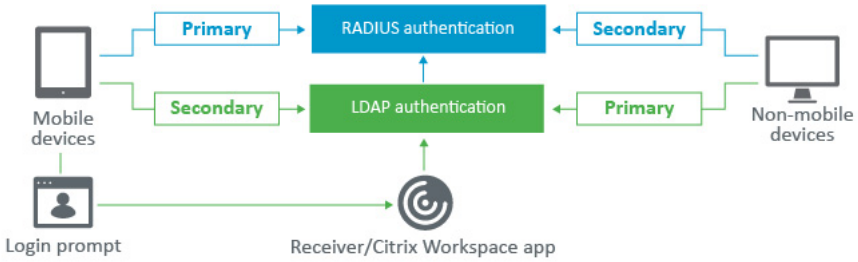
将 **NetScaler Gateway** 配置为在移动/平板电脑设备上使用 **RADIUS** 和 **LDAP** 身份验证

February 1, 2024

本节介绍如何将 NetScaler Gateway 设备配置为在移动/平板电脑设备上使用 RADIUS 身份验证作为主要身份验证，将 LDAP 身份验证用作辅

本节中演示的配置仍然允许所有其他连接首先使用 LDAP，然后使用 RADIUS。

在 Citrix Workspace 应用程序上配置双重身份验证以用于移动/平板电脑设备时，必须添加 RSA SecureID (RADIUS 身份验证) 作为主身份验证。但是，当用户收到提示输入用户名和密码、Receiver 上的密码时，他们将把 LDAP 放在第一位，RADIUS 作为第二个凭据。从管理员的角度来看，它与非移动配置相比是不同的配置。



完成以下过程，将 NetScaler Gateway 设备配置为在移动/平板电脑设备上使用 RADIUS 身份验证作为主身份验证，将 LDAP 身份验证用作辅

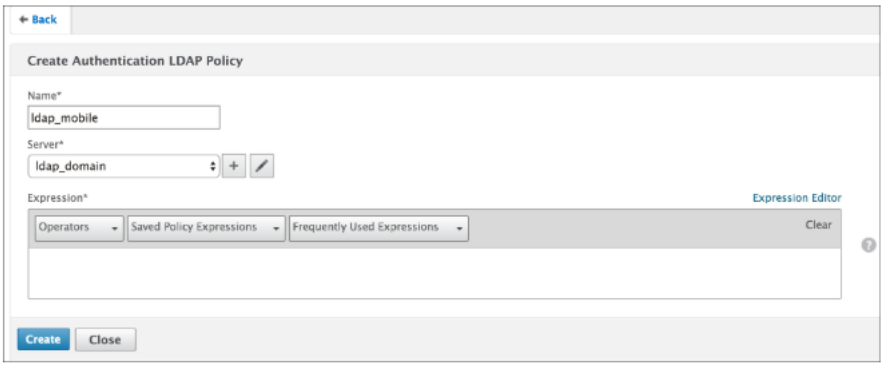
1. 从配置实用程序中，选择 **NetScaler Gateway >** 策略 **>** 身份验证，然后为移动设备和非移动设备的 LDAP 和 RSA 创建身份验证策略。为了避免出现允许用户绕过 RADIUS 身份验证的逻辑条件，这是必要的。
2. 单击 LDAP 的“服务器”选项卡下的“添加”选项后，输入 LDAP 服务 器 详细信息。
3. 通过选择所需的 LDAP 服务器为移动设备创建 LDAP 策略。

   要仅将此策略绑定到移动设备，请使用以下表达式：

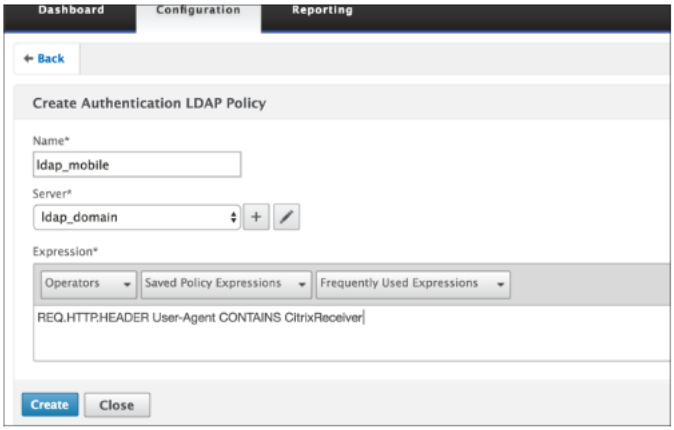
   ```
   1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```

   相应的高级表达式如下：

   ```
   1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
   ```

4. 单击 表达式编辑器 创建策略：

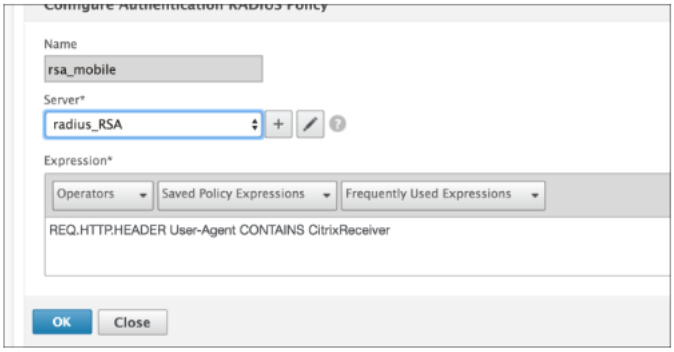


5. 为移动设备创建 RADIUS 策略和 RADIUS 服务器。

   - 从 **NetScaler Gateway >** 策略 **>** 身份验证 **> RADIUS** 导航到 **RADIUS** 选项。单击服务器选项卡下的添加。

- 添加所需的详细信息。RADIUS 身份验证的默认端口是 1812。

- 要仅将此策略绑定到移动设备，请使用以下表达式：

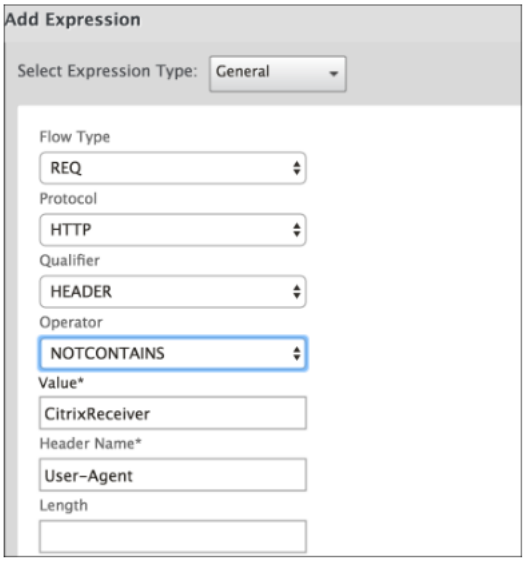


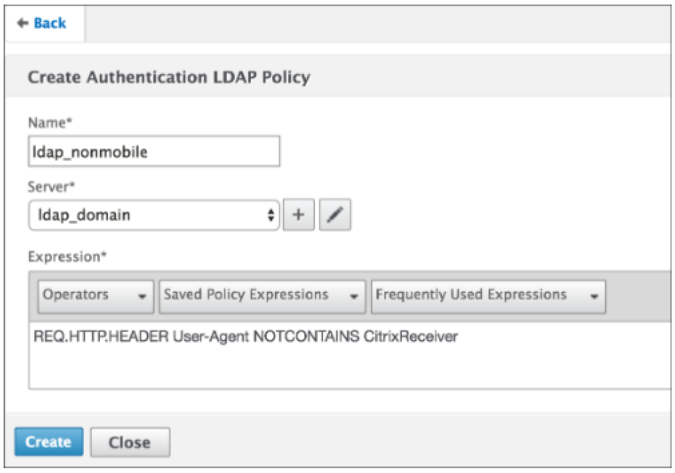
6. 按照相同的步骤为非移动设备创建 LDAP 策略。要仅将此策略绑定到非移动设备，请使用以下表达式：

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

相应的高级表达式如下：

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

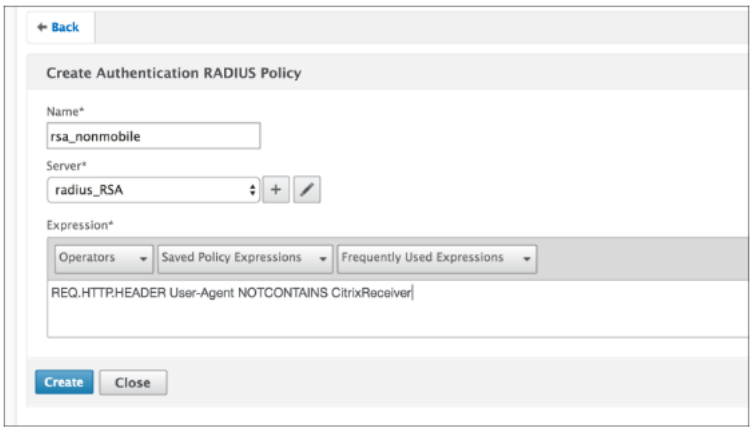


7. 为非移动设备创建 RADIUS 策略。要仅将此策略绑定到非移动设备，请使用以下表达式：

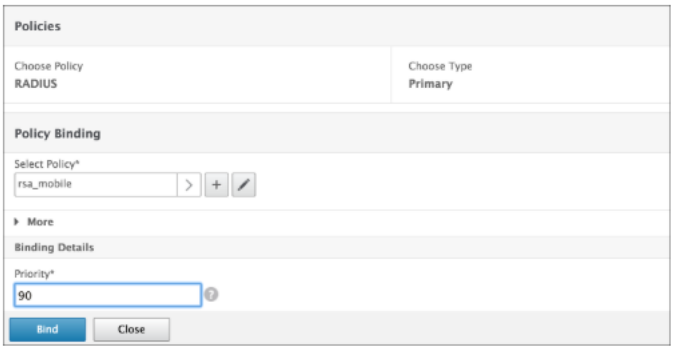
```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

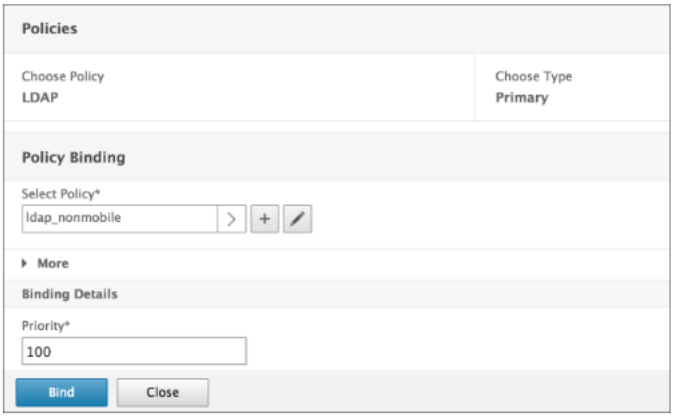
相应的高级表达式如下：

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

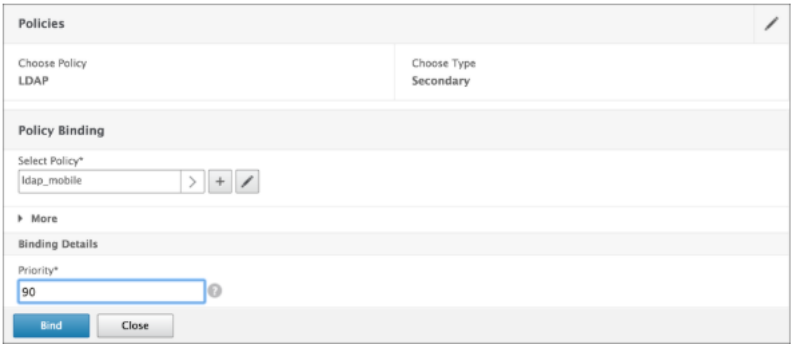



8. 转到 NetScaler Gateway 虚拟服务器的属性，然后单击 身份验证 选项卡。在主身份验证策略上，将 RSA_Mobile 策略添加为最高优先级，将 LDAP_NonMobile 策略添加为次要优先级：





9. 在辅助身份验证策略中，将 LDAP_Mobile 策略添加为最高优先级，然后将 RSA_NonMobile 策略添加为次要优先级：

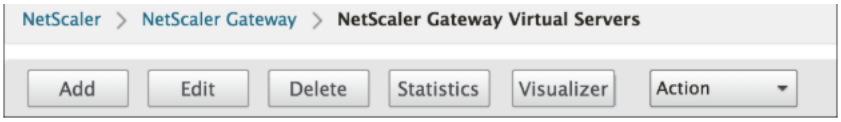


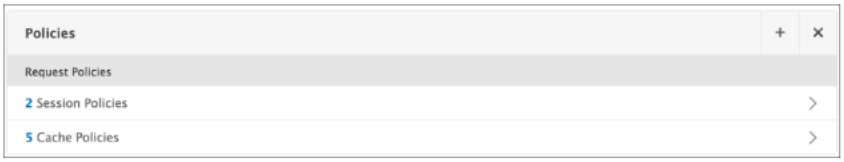
> 会话策略必须具有正确的单点登录凭据索引，也就是说，它必须是 LDAP 凭据。对于移动设备，会 话配置文件 **>** 客户端体验 下的 凭据索引 必须设置为 辅助，即 LDAP。

因此，您需要两个会话策略，一个用于移动设备，另一个用于非移动设备。

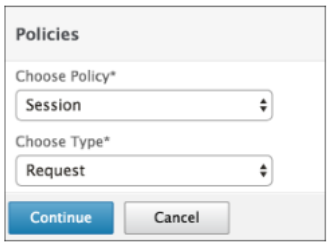
- 对于移动设备，会话策略和会话配置文件将显示在以下屏幕截图中。

  要创建会话策略，请导航到所需的虚拟服务器，然后单击 编辑，转到策略部分，然后单击 + 号：





- 从菜单中选择“会话”选项。



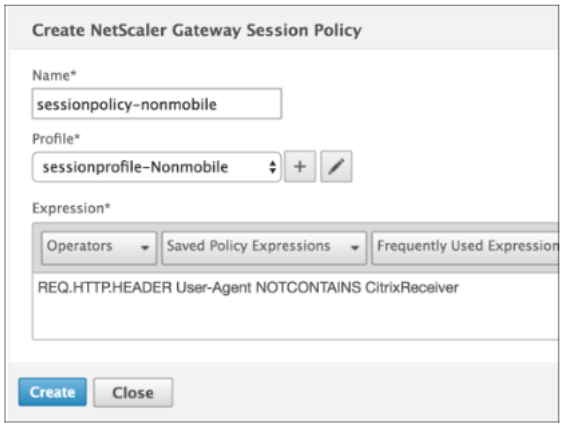
- 输入所需的会话策略名称，然后单击 + 以创建配置文件。对于移动设备，会 话配置文件 **>** 客户端体验 下的凭据索引 必须设置为 辅助，即 LDAP。
- 对于非移动设备，请执行相同的步骤。“会话配置文件” **>** “客户端体验” 下的凭据索引 必须设置为“主”，即 LDAP。

必须将表达式更改为：

```
1 REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

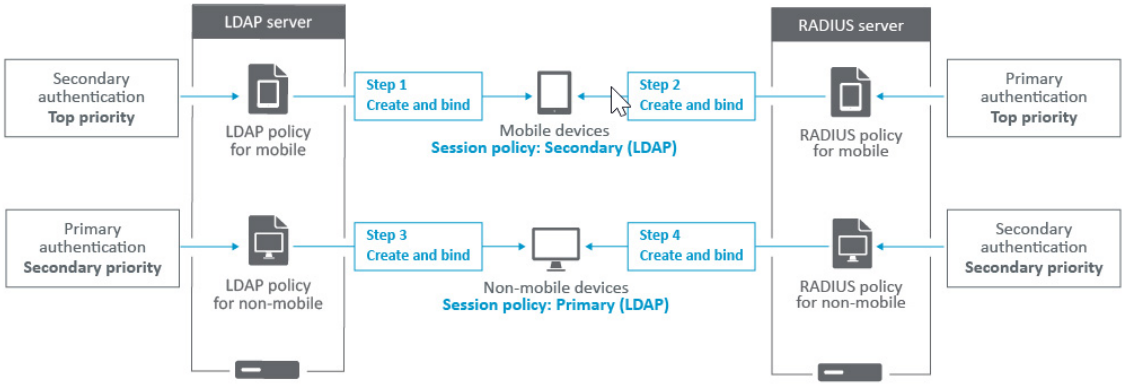

相应的高级表达式如下：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```



- 要为非移动用户创建配置文件，请单击 + 号。

10. 下图显示了所需虚拟服务器下的策略和配置文件。
11. 同样在 StoreFront 上，在 NetScaler Gateway 配置下设置为使用“登录类型”=“域和安全令牌”



限制一个 **Active Directory** 组的成员访问 **NetScaler Gateway**

February 1, 2024

NetScaler Gateway 支持两种限制登录访问权限的方法。

- LDAP 搜索筛选器—只有与 LDAP 搜索筛选器匹配的用户名（例如，Active Directory 组成员身份）才能登录 NetScaler Gateway。
- 允许在 NetScaler Gateway 会话策略或配置文件中登录的组—此方法支持多个 Active Directory 组。有关详细信息，请参阅https://support.citrix.com/article/CTX125797。

本文介绍 LDAP 搜索筛选器方法。

概述

当用户在 NetScaler Gateway 虚拟服务器的登录页面上输入凭据并按 ENTER 键时，设备首先在 Active Directory (LDAP) 中搜索用户名。如果 LDAP 策略或服务器中未定义 LDAP 搜索筛选器，则设备将搜索所有 Active Directory 用户名以查找匹配项。找到匹配项后，设备随后会提取用户的完整唯一判别名 (DN)，并使用用户的 DN 和密码对 Active Directory 进行身份验证。

如果定义了 LDAP 搜索筛选器，则只搜索与 LDAP 搜索筛选器匹配的用户名以查找匹配的用户名。例如，如果 LDAP 搜索筛选器构建为仅搜索 Active Directory 组的成员，则用户输入的用户名必须与该组的成员匹配。

必备条件

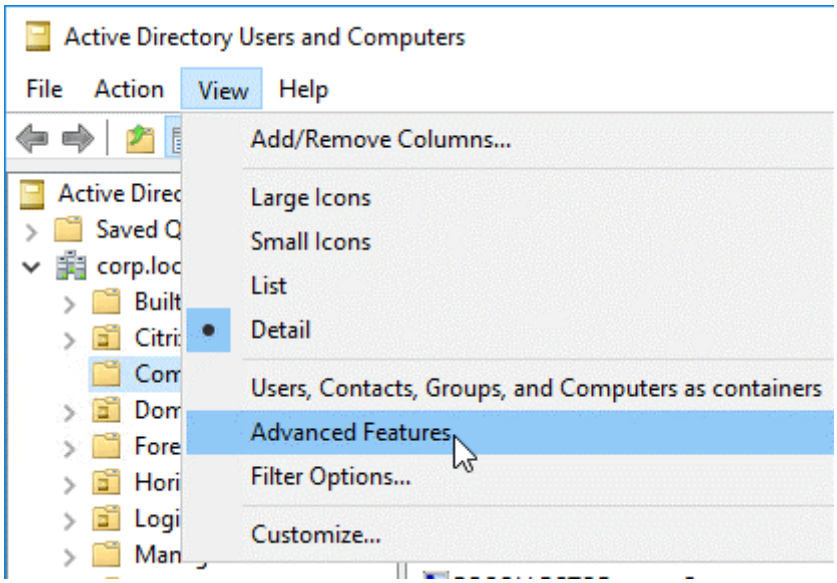
必须配置 NetScaler Gateway 虚拟服务器以进行 LDAP 身份验证。

为一个 **Active Directory** 组的成员配置 **LDAP** 搜索筛选器的步骤

1. 确定具有访问权限的 Active Directory 组，并获取其完整的唯一判别名。

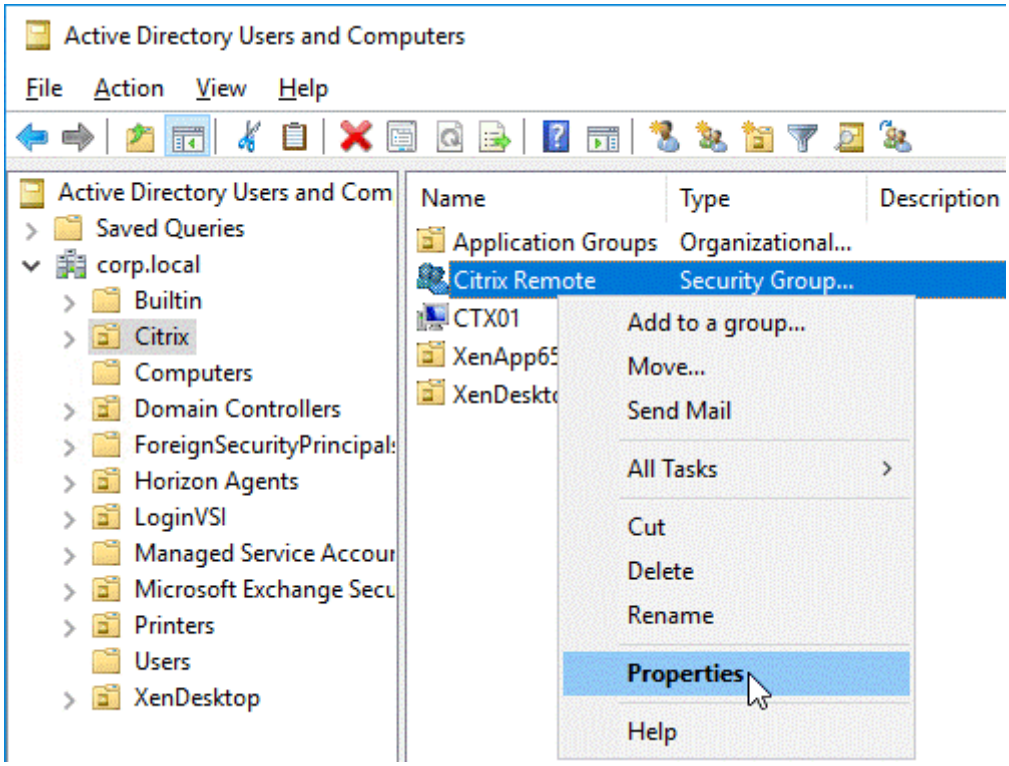
   获取组的完整唯一判别名称的一种简单方法是通过 Active Directory 用户和计算机。

2. 在 Active Directory 用户和计算机中，从 查看 菜单中启用 高级功能。

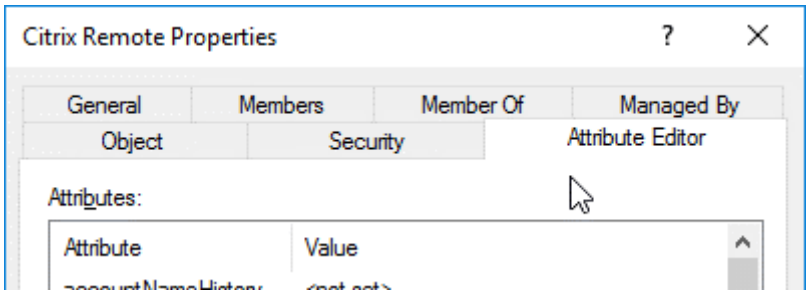


3. 浏览树到组对象，右键单击，然后单击 属性。

   注意：您不能使用“查找”。相反，您必须在树中导航才能找到对象。

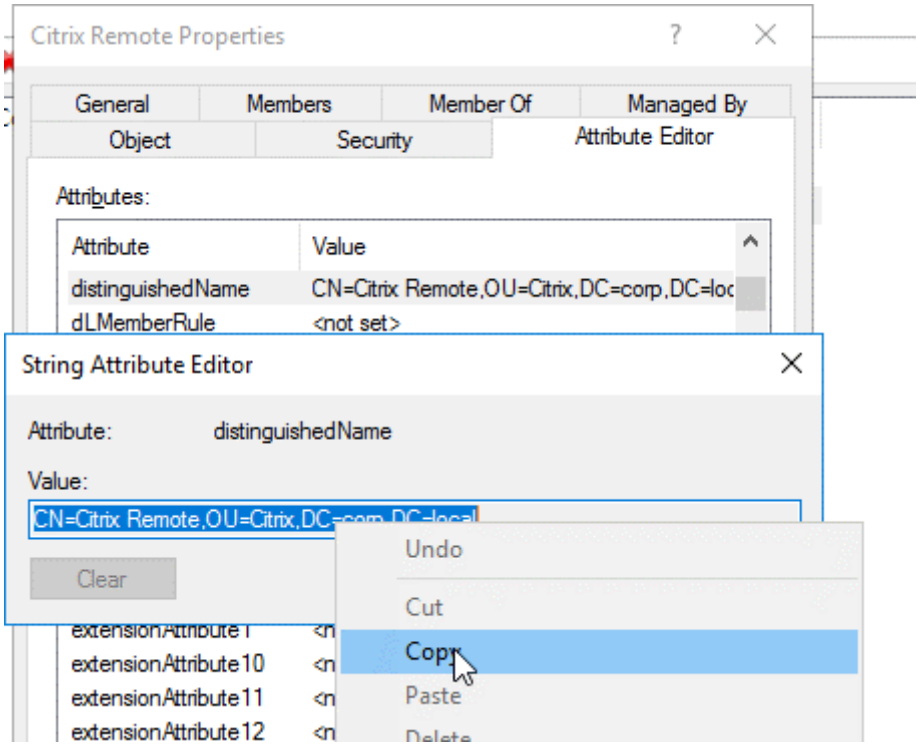


4. 在右侧，切换到 属性编辑器 选项卡。

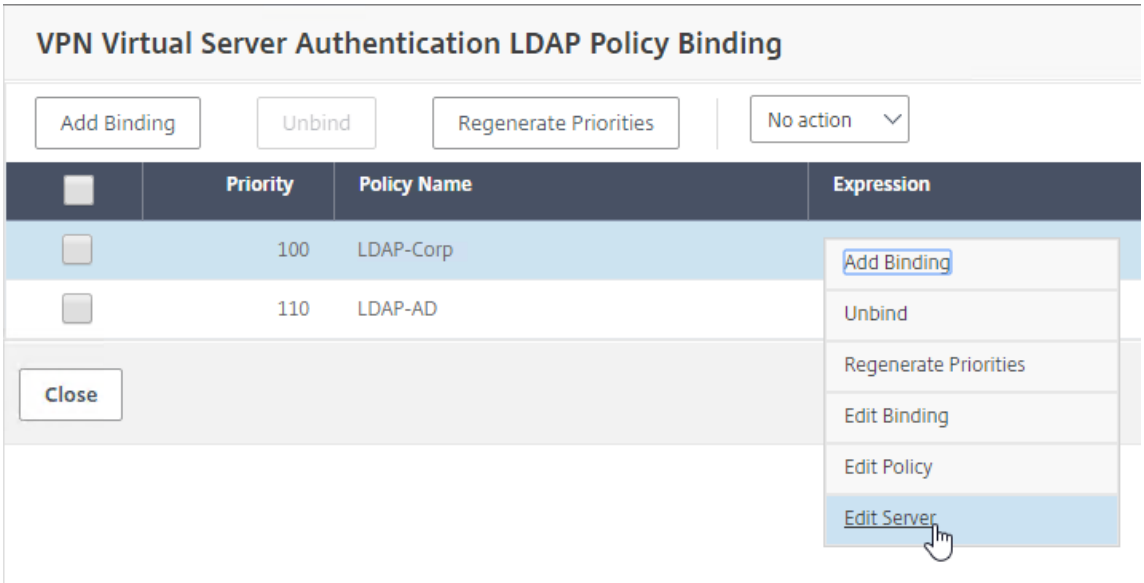


仅当启用了 高级功 能并且尚未使用 查找 功能时，此选项卡才可见。

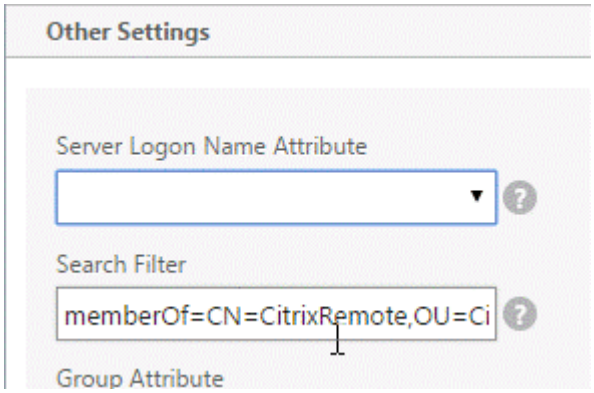
5. 向下滚动到 **distinguishedName**，双击，然后将其复制到剪贴板。



6. 在 NetScaler Gateway GUI 中，导航到 **NetScaler Gateway >** 虚拟服务器。
7. 选择现有 NetScaler Gateway 虚拟服务器，然后单击 编辑。
8. 在“基本身份验证”部分中，单击 **LDAP** 策略。
9. 右键单击现有 LDAP 策略，然后单击 编辑服务器。



10. 在“其他设置”部分的“搜索筛选器”字段中，键入 **memberOf=** ，然后将 Active Directory 组的唯一判别名粘贴在等号 (=) 之后。



以下是一个示例搜索筛选器：

memberOf=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local

注意：默认情况下，NetScaler 仅搜索直接属于 Active Directory 组的用户名。如果要搜索嵌套组，请将 Microsoft OID 添加到 LDAP 搜索筛选器中。OID 插入在 memberOf 和 = 之间。

示例： memberOf:1.2.840.113556.1.4.1941:=CN=Citrix Remote,OU=Citrix,DC=corp,DC=local

11. 单击确定。

使用高可用性

February 1, 2024

两台 NetScaler Gateway 设备的高可用性部署可以在任何事务中提供不间断的操作。将一台设备配置为主节点，将另一台设备配置为辅助节点时，主节点接受连接并管理服务器，而辅助节点则监视主节点。如果因任何原因主节点无法接受连接，将由辅助节点接替其职责。

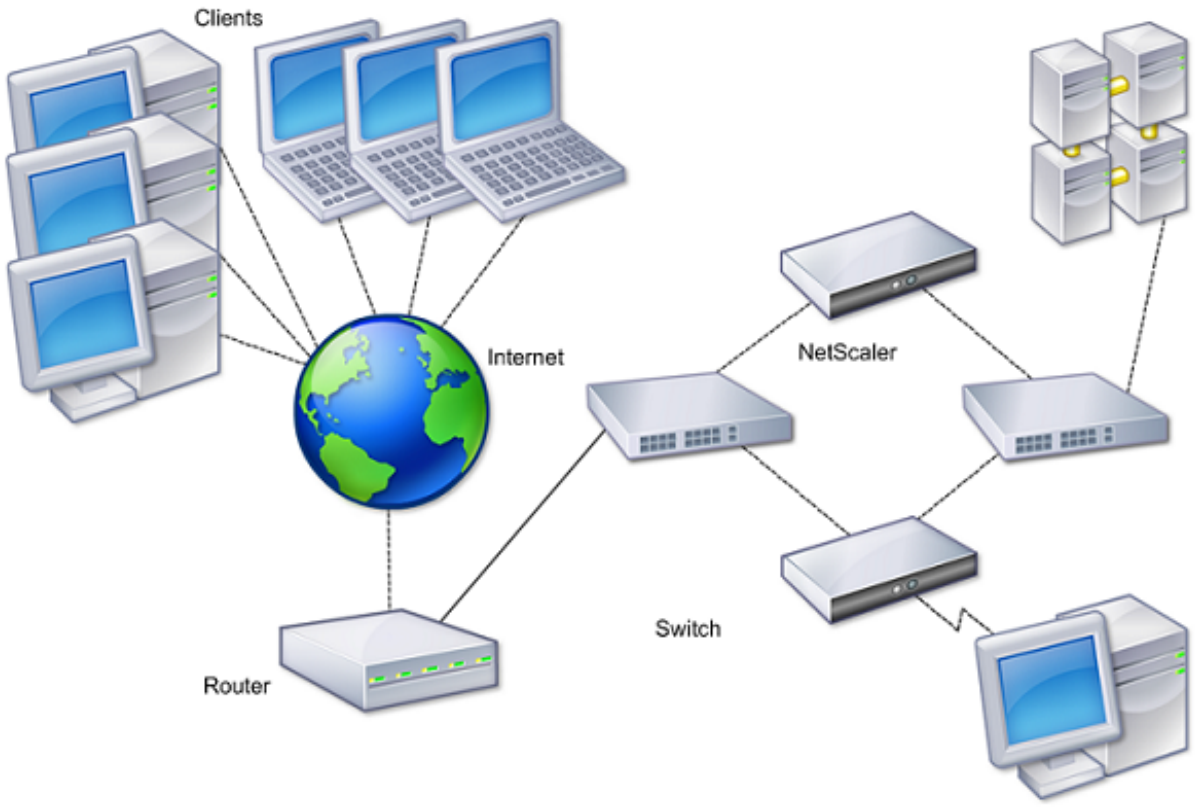
辅助节点通过定期发送消息（通常称为心跳消息或运行状况检查）来监视主节点，以确定主节点是否正在接受连接。如果运行状况检查失败，辅助节点将在指定的时间段内重试连接，之后它将确定主节点无法正常运行。然后，辅助节点接管主节点（称为故障转移的过程）。

故障切换后，所有客户端都必须重新建立与托管服务器的连接，但会话持久性规则将保持故障切换之前的状态。

启用 Web 服务器日志记录持久性后，不会因故障切换而丢失任何日志数据。要启用日志记录持久性，日志服务器配置必须在 log.conf 文件中包含两个系统的条目。

下图显示了具有高可用性对的网络配置。

图 1. 高可用性配置中的 NetScaler Gateway 设备



配置高可用性的基本步骤如下：

1. 创建基本设置，两个节点都位于同一子网中。
2. 自定义节点传达运行状况检查信息的时间间隔。
3. 自定义节点保持同步的过程。
4. 自定义命令从主命令到辅助命令的传播。
5. 或者，配置故障安全模式以防止出现两个节点都不是主节点的情况。
6. 如果您的环境包含不接受 NetScaler Gateway 免费 ARP 消息的设备，请配置虚拟 MAC 地址。

当您准备好进行更复杂的配置时，可以在不同的子网中配置高可用性节点。

为了提高高可用性设置的可靠性，您可以配置路由监视器并创建冗余链路。在某些情况下，例如在进行故障排除或执行维护任务时，您可能希望强制某个节点进行故障切换（将主节点分配给另一个节点），或者强制辅助节点保持辅助节点或强制主节点保持主节点。

高可用性的工作原理

February 1, 2024

在高可用性对中配置 NetScaler Gateway 时，辅助 NetScaler Gateway 会通过定期发送消息（也称为心跳消息或运行状况检查）来监视第一台设备，以确定第一台设备是否正在接受连接。如果运行状况检查失败，辅助 NetScaler

Gateway 将在指定的时间段内再次尝试连接，直到确定主设备无法正常工作。如果辅助设备确认运行状况检查失败，则辅助 NetScaler Gateway 将接管主 NetScaler Gateway。这称为故障转移。

以下端口用于在 NetScaler Gateway 设备之间交换与高可用性相关的信息：

- UDP 端口 3003 用于交换 hello 数据包以传达时间间隔的状态。
- TCP 端口 3010 用于高可用性配置同步。
- TCP 端口 3011 用于同步配置设置。

配置高可用性的指导原则

在配置高可用性对之前，必须查看以下准则：

- 每个 NetScaler Gateway 设备必须运行相同版本的 NetScaler Gateway 软件。您可以在配置实用程序的页面顶部找到版本号。
- NetScaler Gateway 不会在两台设备之间自动同步密码。您可以选择使用配对中其他设备的用户名和密码配置每个 NetScaler Gateway。
- 主 NetScaler Gateway 和辅助 NetScaler Gateway 上的配置文件 ns.conf 中的条目必须匹配，但以下情况除外：
  - 主要和辅助 NetScaler Gateway 设备必须分别使用自己的唯一系统 IP 地址进行配置。使用设置向导在任一 NetScaler Gateway 上配置或修改系统 IP 地址。
  - 在高可用性对中，NetScaler Gateway ID 和关联的 IP 地址必须指向另一个 NetScaler Gateway。

    例如，如果您有两个名为 AG1 和 AG2 的设备，则必须使用唯一的 NetScaler Gateway ID 和 AG2 的 IP 地址配置 AG1。您必须使用唯一的 NetScaler Gateway ID 和 AG1 的 IP 地址配置 AG2。

    注意：每个 NetScaler Gateway 设备始终被标识为节点 0。为每台设备配置唯一的节点 ID。
- 高可用性对中的每个设备必须具有相同的许可证。有关许可的详细信息，请参阅许可。
- 如果您使用的方法不是直接通过配置实用程序或命令行界面（例如，导入 SSL 证书或更改为启动脚本）在任一节点上创建配置文件，则必须将配置文件复制到另一个节点或创建相同的该节点上的文件。
- 配置高可用性对时，请确保主设备和辅助设备的映射 IP 地址和默认网关地址相同。如有必要，可以通过运行安装向导随时更改映射的 IP 地址。

您可以使用安装前核对表查看需要在高可用性部署中配置的特定设置的列表。有关详细信息，请参阅 安装前清单。

为高可用性配置设置

February 1, 2024

要设置高可用性配置，需要创建两个节点，每个节点将另一个节点的 NetScaler Gateway IP 地址定义为远程节点。首先，您可以登录要为高可用性配置的两个 NetScaler 设备之一，然后添加节点。将另一台设备的 NetScaler Gateway

IP 地址指定为新节点的地址。然后，登录到另一台设备并添加具有第一台设备的 NetScaler Gateway IP 地址的节点。算法确定哪个节点成为主节点，哪个节点成为辅助节点

在配置设备之前，请添加一个高可用性节点。此节点表示高可用性对中的第一个或第二个 NetScaler Gateway。要配置高可用性，首先需要创建节点，然后配置高可用性设置。

添加高可用性节点

1. 在配置实用程序的配置选项卡的导航窗格中，展开 系统 **>** 高可用性。
2. 在详细信息窗格的节点选项卡上，单击 添加。
3. 在 创建 **HA** 节点 页面的 远程节点 **IP** 地址 文本框中，键入要添加为远程节点的 NetScaler 的 NSIP 地址。如果 NetScaler Gateway IP 地址是 IPv6 地址，请在输入地址之前选中 **IPv6** 复选框。
4. 如果要自动将本地节点添加到远程节点，请选择配置远程系统以参与高可用性设置。如果不选择此选项，则必须登录到远程节点所代表的设备，然后添加当前正在配置的节点。
5. 单击以启用 关闭 **HA Monitor** 接口**/**通道关闭。
6. 如果远程设备的用户名和密码不同，则在远程系统登录凭据中，单击远程系统的登录凭据与自身节点不同。
7. 在 用户名中，键入远程设备的用户名。
8. 在 密码中，键入远程设备的密码。
9. 单击确定。

启用或禁用辅助节点

您只能禁用或启用辅助节点。禁用辅助节点后，它会停止向主节点发送心跳消息，因此主节点无法再检查辅助节点的状态。启用节点后，该节点将参与高可用性配置。

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的节点选项卡上，选择本地节点，然后单击打开。
3. 在高可用性配置节点对话框的高可用性状态中，选择已启用（不参与 HA）。
4. 单击确定。状态栏中将显示一条消息，指出已成功配置节点。

配置高可用性的设置

1. 在配置实用程序的配置选项卡的导航窗格中，展开 系统 **>** 高可用性。
2. 在详细信息窗格的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在 **HA** 配置节点 对话框的 ID 中，键入节点标识符的编号。ID 为另一台设备指定唯一的节点编号。
4. 在“**IP** 地址”中，键入系统 IP 地址，然后单击“确定”。IP 地址指定另一台设备的 IP 地址。

注意：高可用性对中节点的最大 ID 为 64。

更改 **RPC** 节点密码

February 1, 2024

要与其他 NetScaler Gateway 设备通信，每个设备都需要了解其他设备，包括如何在 NetScaler Gateway 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 NetScaler Gateway 上存在一个 RPC 节点，并存储信息，例如其他 NetScaler Gateway 设备的 IP 地址和用于身份验证的密码。与另一个 NetScaler Gateway 联系的 NetScaler Gateway 会检查 RPC 节点内的密码。

NetScaler Gateway 要求在高可用性对中的两台设备上使用 RPC 节点密码。两台设备上的密码必须相同。主设备必须知道辅助 RPC 节点密码，辅助设备必须知道主 RPC 节点密码。最初，每个 NetScaler Gateway 都使用相同的 RPC 节点密码进行配置。要增强安全性，必须更改默认的 RPC 节点密码。您可以使用配置实用程序来配置和更改 RPC 节点。

在添加节点或添加全局服务器负载平衡 (GSLB) 站点时，会隐式创建 RPC 节点。您无法手动创建或删除 RPC 节点。

> 重要信息：
>
> 您还必须保护设备之间的网络连接。在配置 RPC 节点密码时，可以通过选中 **Secure** 复选框来配置安全性。

更改 **RPC** 节点密码并启用安全连接

1. 导航到“系统” **>** “网络” **>** “**RPC**”。
2. 在详细信息窗格中，选择节点，然后单击 编辑。
3. 在“密码”和“确认密码”中，键入新密码。
4. 在 源 **IP** 地址中，键入其他 NetScaler Gateway 设备的系统 IP 地址。
5. 单击 安全，然后单击 确定。

> 注意：
>
> 启用 安全 选项后，设备会加密从该节点发送到其他 RPC 节点的所有通信，从而保护 RPC 通信。

使用 **CLI** 更改 **RPC** 节点密码

在命令提示符下，键入：

```
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-->
```

配置主设备和辅助设备以实现高可用性

February 1, 2024

更改 RPC 节点密码并启用安全通信后，使用配置实用程序配置主要和辅助 NetScaler Gateway 高可用性节点。

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的节点选项卡上，选择一个节点，然后单击编辑。
3. 在高可用性状态下，单击已启用（主动参与 HA），然后单击确定。

配置通信间隔

February 1, 2024

将 NetScaler Gateway 配置为高可用性对时，可以将辅助 NetScaler Gateway 配置为以特定的时间间隔进行侦听，以毫秒 (毫秒) 为单位。这些间隔称为 hello 间隔和死区间。

hello 间隔是心跳消息发送到对等节点的时间间隔。死区间是指在未收到心跳数据包的情况下将对等节点标记为 DOWN 的时间间隔。检测信号消息是发送到高可用性对中另一个节点的端口 3003 的 UDP 数据包。

配置 hello 间隔时，可以使用 200 到 1000 的值。默认值为 200。死区间值为 3 到 60。默认值为 3。

> 注意
>
> 死间隔必须设置为 hello 间隔的倍数。

为辅助 **NetScaler Gateway** 配置通信间隔

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。

2. 在详细信息窗格的节点选项卡上，选择一个节点，然后单击编辑。
3. 在“间隔”下，执行以下一项或两项操作：
    - 在 Hello Interval (毫秒) 中，键入值，然后单击确定。默认值为 200 毫秒。
    - 在死区间 (秒) 中，键入值，然后单击确定。默认设置为三秒钟。

同步 **NetScaler Gateway** 设备

February 1, 2024

默认情况下，高可用性对中的 NetScaler Gateway 设备的自动同步处于启用状态。通过自动同步，您可以对一台设备进行更改，并使更改能够自动传播到第二台设备。同步使用端口 3010。

发生以下情况时，同步开始：

- 辅助节点将重新启动。
- 故障转移后，主节点变为辅助节点。

您可以禁用同步，这会阻止辅助 NetScaler Gateway 在主设备上发生更改时将其配置与主 NetScaler Gateway 同步。您也可以强制同步。

您可以在配对中的辅助节点上启用或禁用高可用性同步。

启用或禁用高可用性同步

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的节点选项卡上，选择一个节点，然后单击编辑。
3. 在“配置节点”对话框的“HA 同步”下，执行以下操作之一：
    - 要禁用同步，请清除辅助节点将从主节点获取配置复选框。
    - 要启用同步，请选中辅助节点将从主节点获取配置复选框。
4. 单击确定。状态栏中将显示一条消息，指出节点配置成功。

强制设备之间的同步

除了自动同步之外，NetScaler Gateway 还支持高可用性对中的两个节点之间的强制同步。

您可以在主 NetScaler Gateway 设备和辅助 NetScaler Gateway 设备上强制同步。但是，如果同步已在进行中，则命令将失败，NetScaler Gateway 将显示警告。在以下情况下，强制同步也会失败：

- 在独立系统上强制同步。
- 辅助节点已禁用。

- 在辅助节点上禁用高可用性同步。

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在节点选项卡上，单击强制同步。

在高可用性设置中同步配置文件

February 1, 2024

在高可用性设置中，您可以将各种配置文件从主节点同步到辅助节点。

在高可用性设置中同步文件的参数

- 模式

  要执行的同步类型。以下说明在括号中包括用于指定选项的命令行参数。

  - 除了许可证和 **rc.conf** （全部）之外的所有内容。同步与系统配置、NetScaler Gateway 书签、SSL 证书、SSL CRL 列表、HTML 注入脚本和应用程序防火墙 XML 对象相关的文件。
  - 书签（书签）。同步所有 NetScaler Gateway 书签。
  - **SSL** 证书和密钥 (`ssl`)。同步 SSL 功能的所有证书、密钥和 CRL。
  - 许可证和 **rc.conf** (杂项)。同步所有许可证文件和 rc.conf 文件。
  - 包括许可证和 **rc.conf** (all_plus_misc) 在内的所有内容。同步与系统配置、NetScaler Gateway 书签、SSL 证书、SSL CRL 列表、HTML 注入脚本、应用程序防火墙 XML 对象、许可证和 rc.conf 文件相关的文件。

注意：如果在设备上安装 NetScaler 许可证，则有更多可用选项。

使用配置实用程序在高可用性设置中同步文件

1. 在导航窗格中，展开 系统，然后单击 诊断。
2. 在详细信息窗格的“实用程序”下，单击“启动 **HA** 文件同步”。
3. 在“开始文件同步”对话框的“模式”菜单中，选择适当的同步类型（例如，除许可证和 rc.conf 之外的所有内容），然后单击“确定”。

配置命令传播

February 1, 2024

在高可用性设置中，在主节点上发出的任何命令在主节点上运行命令之前都会自动传播到辅助节点并在辅助节点上运行。如果命令传播失败，或者如果在辅助节点上执行命令失败，则主节点将运行命令并记录错误。命令传播使用端口3011。

在高可用性对配置中，默认情况下在主节点和辅助节点上都启用命令传播。您可以在高可用性对中的任一节点上启用或禁用命令传播。如果在主节点上禁用命令传播，则命令不会传播到辅助节点。如果在辅助节点上禁用命令传播，则从主节点传播的命令不会在辅助节点上运行。

注意：重新启用传播后，请记住强制同步。

注意：如果在禁用传播时发生同步，则在禁用传播生效之前所做的任何与配置相关的更改都将与辅助节点同步。同步过程中禁用传播的情况也是如此。

在主节点上启用或禁用传播

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在 **HA** 传播下，执行以下操作之一：
    - 要禁用高可用性传播，请清除 主节点将配置传播到辅助 节点复选框。
    - 要启用高可用性传播，请选中 主节点将配置传播到辅助 节点复选框。
4. 单击确定。

命令传播故障排除

February 1, 2024

以下列表描述了命令传播可能失败的原因以及恢复设置的解决方案：

- 网络连接未激活。如果命令传播失败，请检查主 NetScaler Gateway 设备和辅助 NetScaler Gateway 设备之间的网络连接。
- 辅助 NetScaler Gateway 上缺少资源。如果命令在主 NetScaler Gateway 上成功执行，但无法传播到辅助 NetScaler Gateway，请直接在辅助 NetScaler Gateway 上运行命令以查看错误消息。发生此错误的原因可能是命令所需的资源存在于主 NetScaler Gateway 上，而在辅助 NetScaler Gateway 上不可用。另外，请验证每台设备上的许可证文件是否匹配。

  例如，验证每个 NetScaler Gateway 上是否存在所有安全套接字层 (SSL) 证书。验证两台 NetScaler Gateway 设备上是否存在任何初始化脚本自定义。
- 身份验证失败。如果收到身份验证失败错误消息，请验证每台设备上的 RPC 节点设置。

配置故障安全模式

February 1, 2024

在高可用性配置中，故障安全模式可确保当两个节点未通过运行状况检查时，一个节点始终是主节点。故障安全模式可确保当节点仅部分可用时，备份方法可以激活并处理流量。

您可以在每个节点上独立配置高可用性故障安全模式。

下表显示了一些故障安全案例。NOT_UP 状态表示节点未通过运行状况检查，但该节点仍处于部分可用状态。UP 状态表示节点通过了运行状况检查。

表 1. 故障安全模式案例

节点 A（主）运行状况	节点 B（次要）运行状况	默认的高可用性行为	启用故障安全的高可用性行为	说明
NOT_UP (failed last)	NOT_UP (failed first)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	如果两个节点一个接一个地发生故障，那么作为最后一个主节点的节点仍然是主节点。
NOT_UP (failed first)	NOT_UP (failed last)	A (Secondary), B (Secondary)	A (Secondary), B (Primary)	如果两个节点一个接一个地发生故障，那么作为最后一个主节点的节点仍然是主节点。
UP	UP	A (Primary), B (Secondary)	A (Primary), B (Secondary)	如果两个节点都通过了运行状况检查，则启用了故障安全功能的行为不会改变。
UP	NOT_UP	A (Primary), B(Secondary)	A (Primary), B (Secondary)	如果只有辅助节点发生故障，则启用了故障安全的情况下行为不会改变。
NOT_UP	UP	A (Secondary), B(Primary)	A (Secondary), B(Primary)	如果只有主服务器发生故障，则启用故障安全功能后的行为不会改变。

节点 A（主）运行状况	节点 B（次要）运行状况	默认的高可用性行为	启用故障安全的高可用性行为	说明
NOT_UP	UP (STAYSECONDARY)	A (Secondary), B (Secondary)	A (Primary), B (Secondary)	如果辅助设备配置为 STAYSecondary，则即使出现故障，主服务器仍然是主要的。

配置故障安全模式

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的节点选项卡上，选择一个节点，然后单击编辑。
3. 在“配置节点”对话框的“故障安全模式”下，选择“即使两个节点都运行状况不佳时也维护一个主节点”，然后单击“确定”

配置虚拟 **MAC** 地址

February 1, 2024

虚拟 MAC 地址在高可用性设置中由主要和辅助 NetScaler Gateway 设备共享。

在高可用性设置中，主 NetScaler Gateway 拥有所有浮动 IP 地址，例如映射的 IP 地址或虚拟 IP 地址。它使用自己的 MAC 地址响应针对这些 IP 地址的地址解析协议 (ARP) 请求。因此，外部设备（例如路由器）的 ARP 表将使用浮动 IP 地址和主 NetScaler Gateway MAC 地址进行更新。发生故障转移时，辅助 NetScaler Gateway 将作为新的主 NetScaler Gateway 接管。然后，它使用免费地址解析协议 (GARP) 来通告从主设备获取的浮动 IP 地址。新的主设备通告的 MAC 地址是其自己的接口的地址。

某些设备不接受 NetScaler Gateway 生成的 GARP 消息。因此，某些外部设备会保留旧的主 NetScaler Gateway 公布的旧 IP 到 Mac 映射。这种情况可能会导致站点变得不可用。要解决此问题，请在高可用性对的两个 NetScaler Gateway 设备上配置虚拟 MAC 地址。此配置意味着两台 NetScaler Gateway 设备具有相同的 MAC 地址。因此，当发生故障转移时，辅助 NetScaler Gateway 的 MAC 地址将保持不变，并且无需更新外部设备上的 ARP 表。

要创建虚拟 MAC 地址，请创建虚拟路由器标识符 (ID) 并将其绑定到接口。在高可用性设置中，用户需要将 ID 绑定到两台设备上的接口。

当虚拟路由器 ID 绑定到接口时，系统会生成一个虚拟 MAC 地址，其中虚拟路由器 ID 作为最后一个八位字节。通用虚拟 MAC 地址的一个示例是 00:00:5e:00:01:<VRID>。例如，如果您创建了一个值为 60 的虚拟路由器 ID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是虚拟路由器 ID 的十六进制表示形式。您可以创建 255 个虚拟路由器 ID，范围从 1 到 254。

您可以为 IPv4 和 IPv6 配置虚拟 MAC 地址。

配置 **IPv4** 虚拟 **MAC** 地址

February 1, 2024

创建 IPv4 虚拟 MAC 地址并将其绑定到接口时，从该接口发送的任何 IPv4 数据包都使用绑定到该接口的虚拟 MAC 地址。如果没有绑定到接口的 IPv4 虚拟 MAC 地址，则使用该接口的物理 MAC 地址。

通用虚拟 MAC 地址的格式为 00:00:5e:00:01:<VRID>。例如，如果创建值为 60 的 VRID 并将其绑定到接口，则生成的虚拟 MAC 地址为 00:00:5e:00:01:3c，其中 3c 是 VRID 的十六进制表示形式。您可以创建 255 个 VRID，其值介于 1 到 255 之间。

创建或修改 **IPv4** 虚拟 **MAC** 地址

February 1, 2024

您可以通过为其分配虚拟路由器 ID 来创建 IPv4 虚拟 MAC 地址。然后，您可以将虚拟 MAC 地址绑定到接口。不能将多个虚拟路由器 ID 绑定到同一个接口。要验证虚拟 MAC 地址配置，必须显示并检查虚拟 MAC 地址以及绑定到虚拟 MAC 地址的接口。

配置虚拟 **MAC** 地址的参数

- VrID

  标识虚拟 MAC 地址的虚拟路由器 ID。可能的值：1—255。

- `ifnum`

  要绑定到虚拟 MAC 地址的接口号（插槽/端口表示法）。

配置虚拟 **MAC** 地址

1. 导航到“系统”**>**“网络”，然后单击“**VMAC**”。
2. 在详细信息窗格的 **VMAC** 选项卡上，单击 添加。
3. 在 创建 **VMAC** 对话框的 虚拟路由器 **ID** 中，键入值。
4. 在 关联的接口下的 可用接口中，选择一个网络接口，单击 添加，单击 创建，然后单击关 闭。

创建虚拟 MAC 地址后，它将显示在配置实用程序中。如果选择了网络接口，则虚拟路由器 ID 将绑定到该接口。

删除虚拟 **MAC** 地址

要删除虚拟 MAC 地址，您需要删除相应的虚拟路由器 ID。

1. 导航到“系统”**>**“网络”，然后单击“**VMAC**”。
2. 在详细信息窗格中，选择一个项目，然后单击 删除。

绑定和取消绑定虚拟 **MAC** 地址

创建虚拟路由器 ID 时，您在 NetScaler Gateway 上选择了一个网络接口，然后将虚拟路由器 ID 绑定到网络接口。您还可以从网络接口解除虚拟 MAC 地址的绑定，但保留在 NetScaler Gateway 上配置的 MAC 地址。

1. 导航到“系统”**>**“网络”，然后单击“**VMAC**”。
2. 在详细信息窗格中，选择一个项目，然后单击 打开。
3. 在 已配置的接口下，选择一个网络接口，单击 删除，单 击确定，然后单击 关闭。

配置 **IPv6** 虚拟 **MAC** 地址

February 1, 2024

NetScaler Gateway 支持 IPv6 数据包的虚拟 MAC 地址。您可以将任何接口绑定到 IPv6 的虚拟 MAC 地址，即使将 IPv4 虚拟 MAC 地址绑定到该接口也是如此。从接口发送的任何 IPv6 数据包都使用绑定到该接口的虚拟 MAC 地址。如果没有绑定到接口的虚拟 MAC 地址，则 IPv6 数据包将使用物理 MAC。

为 **IPv6** 创建或修改虚拟 **MAC** 地址

February 1, 2024

通过为 IPv6 虚拟 MAC 地址分配 IPv6 虚拟路由器 ID 来创建它。然后将虚拟 MAC 地址绑定到接口。不能将多个 IPv6 虚拟路由器 ID 绑定到一个接口。要验证虚拟 MAC 地址配置，请显示并检查虚拟 MAC 地址和绑定到虚拟 MAC 地址的接口。

为 **IPv6** 配置虚拟 **MAC** 地址的参数

- `Virtual Router ID`

  标识虚拟 MAC 地址的虚拟路由器 ID。可能的值：1—255。

- `ifnum`

  要绑定到虚拟 MAC 地址的接口号（插槽/端口表示法）。

为 **IPv6** 配置虚拟 **MAC** 地址

1. 在配置实用程序中的“配置”选项卡上，展开“系统” **>** “网络”，然后单击“VMAC”。
2. 在详细信息窗格的 VMAC6 选项卡上，执行以下操作之一：
   - 要创建新的虚拟 MAC 地址，请单击“添加”。
   - 要修改现有的虚拟 MAC 地址，请单击“打开”。
3. 在创建 VMAC6 或配置 VMAC6 对话框的虚拟路由器 ID 中，输入值，例如 vrID6。
4. 在关联接口中，单击 添加 **>** 创建 **>** 关闭。状态栏中将显示一条消息，指出虚拟 MAC 地址已配置。

删除 **IPv6** 的虚拟 **MAC** 地址

1. 在配置实用程序中的“配置”选项卡上，展开“系统” **>** “网络”，然后单击“VMAC”。
2. 在详细信息窗格的 VMAC6 选项卡上，选择要删除的虚拟路由器 ID，然后单击删除。状态栏中会显示一条消息，指出虚拟 MAC 地址已删除。

在不同的子网中配置高可用性对

February 1, 2024

典型的高可用性部署是指高可用性对中的两个设备都位于同一子网中。高可用性部署还可以包含两个 NetScaler Gateway 设备，其中每个设备位于不同的网络中。本主题介绍后一种配置，包括示例配置以及一个网络内和跨网络的高可用性配置之间的差异列表。

您还可以配置链路冗余和路由监视器。这些 NetScaler Gateway 功能在跨网络高可用性配置中非常有用。这些功能还涵盖每个 NetScaler Gateway 为确保合作伙伴设备处于活动状态而使用的运行状况检查过程。

独立网络配置的工作原理

NetScaler Gateway 设备连接到两个不同网络上的不同路由器，称为 R3 和 R4。设备通过这些路由器交换检测信号数据包。心跳数据包是定期发生的信号，可确保连接仍处于活动状态。您可以扩展此配置以适应涉及任意数量接口的部署。

注意：如果在网络上使用静态路由，则必须在所有系统之间添加静态路由，以确保成功发送和接收检测信号数据包。（如果在系统上使用动态路由，则不需要静态路由。）

当高可用性对中的设备驻留在两个不同的网络上时，辅助 NetScaler Gateway 必须具有独立的网络配置。这意味着不同网络上的 NetScaler Gateway 设备无法共享映射的 IP 地址、虚拟 LAN 或网络路由。这种类型的配置称为独立网络配置或对称网络配置，其中高可用性对中的 NetScaler Gateway 设备具有不同的可配置参数。

下表总结了独立网络配置的可配置参数，并显示了必须如何在每个 NetScaler Gateway 上设置这些参数：

可配置参数	行为
IP 地址	特定于 NetScaler Gateway。仅在该设备上处于活动状态。
虚拟 IP 地址	浮动。
虚拟局域网	特定于 NetScaler Gateway。仅在该设备上处于活动状态。
路由	特定于 NetScaler Gateway。仅在该设备上处于活动状态。链路负载平衡 (LLB) 路由处于浮动状态。
访问控制列表 (ACL)	浮动（普通）。两台设备均处于活动状态
动态路由	特定于 NetScaler Gateway。仅在该设备上处于活动状态。辅助 NetScaler Gateway 还必须运行路由协议并与上游路由器对等。
L2 模式	浮动（普通）。两台设备均处于活动状态
L3 模式	浮动（普通）。两台设备均处于活动状态
反向网络地址转换 (NAT)	特定于 NetScaler Gateway。使用虚拟 IP 地址反向 NAT，因为 NAT IP 地址是浮动的。

> 注意：
>
> 公有 IP 地址支持 INC 模式下的 IPSET。有关详细信息，请参阅 具有 Azure 负载平衡器前端 IP 验证的参考设计的 NetScaler 高可用性。

添加远程节点

February 1, 2024

当高可用性对中的两个节点位于不同的子网中时，每个节点必须具有不同的网络配置。因此，要将两个独立的系统配置为高可用性对，必须在配置过程中指定独立的网络计算模式。

添加高可用性节点时，必须为每个未连接或未用于流量的接口禁用高可用性监视器。

为独立网络计算模式添加远程节点

1. 在配置实用程序的配置选项卡的导航窗格中，展开 系统 **>** 高可用性。
2. 在详细信息窗格中，单击 节点 选项卡，然后单击 添加。
3. 在“高可用性设置”对话框的“远程节点 **IP** 地址”文本框中，键入作为远程节点的设备的 NetScaler Gateway IP 地址。

   要使用 IPv6 地址，请在输入 IP 地址之前单击 **IPv6** 复选框。
4. 如果要自动将本地节点添加到远程节点，请选择配置远程系统以参与高可用性设置。如果不选择此选项，则必须登录到远程节点所代表的设备，然后添加当前正在配置的节点。
5. 单击可在关闭的接口/通道上启用清除 HA 监视器。
6. 单击以在自模式下启用打开 INC（独立网络配置）模式。
7. 单击确定。节 点页面显示高可用性配置中的本地和远程节点。

删除远程节点

1. 在配置实用程序的配置选项卡的导航窗格中，展开 系统 **>** 高可用性。
2. 在详细信息窗格中，单击 节点 选项卡。
3. 选择要删除的节点，单击“删 除”，然后单击“是”。

配置路由监视器

February 1, 2024

无论内部路由表包含任何动态获知的路由还是静态路由，您都可以使用路由监视器使高可用性状态依赖于内部路由表。在高可用性配置中，每个节点上的路由监视器会检查内部路由表，以确保始终存在用于到达特定网络的路由条目。如果路由条目不存在，则路由监视器的状态将更改为 DOWN。

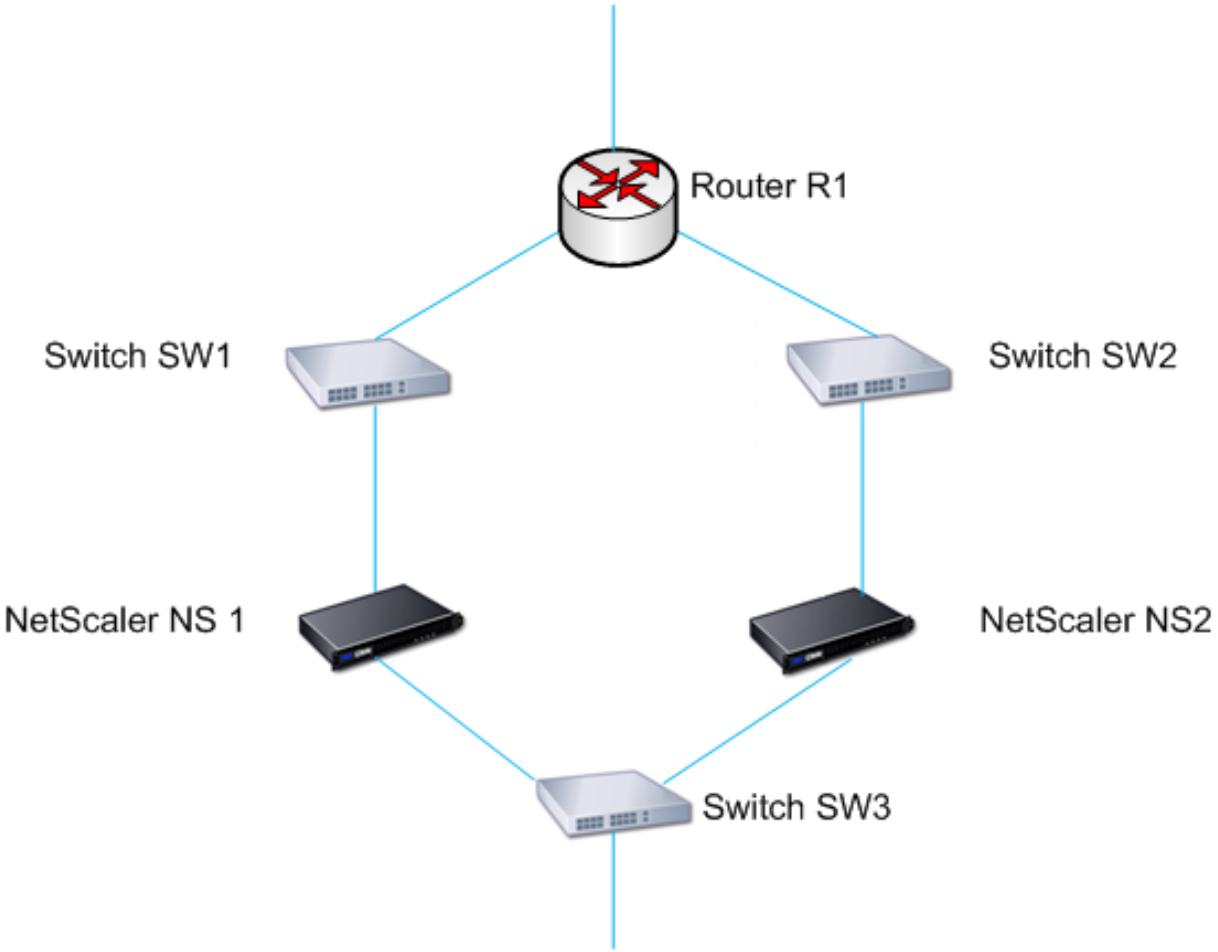
如果 NetScaler Gateway 设备只有用于到达网络的静态路由，并且您想要为网络创建路由监视器，则必须为静态路由启用受监视的静态路由。受监视的静态路由会从内部路由表中删除无法访问的静态路由。如果在静态路由上禁用受监视的静态路由，则无法到达的静态路由可能会保留在内部路由表中，这违背了路由监视器的目的。

启用或禁用的独立网络配置设置都支持路由监视器。下表显示了在高可用性设置中启用或禁用独立网络配置的路由监视器时发生的情况。

在禁用的独立网络配置模式下处于高可用性的路由	在已启用的独立网络配置模式下处于高可用性状态
路由监视器由节点传播并在同步期间进行交换。	路由监视器既不会由节点传播，也不会在同步过程中交换。
路由监视器仅在当前主节点中处于活动状态。	路由监视器在主节点和辅助节点上都处于活动状态。
无论内部路由表中是否存在路由条目，NetScaler Gateway 设备始终将路由监视器的状态显示为 UP。	如果内部路由表中不存在相应的路由条目，NetScaler Gateway 设备会将路由监视器的状态显示为 DOWN。
在以下情况下，路由监视器开始监视其路由，以允许 NetScaler Gateway 了解动态路由，这可能需要长达 180 秒的时间：重启、故障转移、为 v6 路由设置 route6 命令、为 v4 路由设置路由 `msr` 启用/禁用命令、添加新的路由监视器	不适用。

当您禁用独立网络配置模式并且希望主节点的网关无法访问时，路由监视器非常有用，这是高可用性故障转移的条件之一。

例如，您可以在双臂拓扑中的高可用性设置中禁用独立网络配置，该拓扑在同一子网中具有 NetScaler Gateway 设备 NS1 和 NS2，路由器 R1 和交换机 SW1、SW2 和 SW3，如下图所示。由于 R1 是此设置中的唯一路由器，因此您希望每当无法从当前主节点访问 R1 时，高可用性设置都能进行故障切换。您可以在每个节点上配置路由监视器（分别是 RM1 和 RM2），以监视从该节点到达 R1 的可达性。



当 NS1 作为当前主节点时，网络流如下所示：

1. NS1 上的路由监视器 RM1 监视 NS1 的内部路由表，以确定是否存在路由器 R1 的路由条目。NS1 和 NS2 定期通过交换机 SW1 或 SW3 交换机交换心跳消息。
2. 如果交换机 SW1 出现故障，NS1 上的路由协议会检测到 R1 无法到达，因此从内部路由表中删除 R1 的路由条目。NS1 和 NS2 定期通过交换机 SW3 交换机交换心跳消息。
3. 检测到内部路由表中没有 R1 的路由条目，RM1 将启动故障切换。如果从 NS1 和 NS2 到 R1 的路由都关闭，则每 180 秒进行一次故障切换，直到其中一台设备能够到达 R1 并恢复连接为止。

添加或删除路由监视器

February 1, 2024

当高可用性对的设备驻留在不同的网络上时，NetScaler Gateway 的高可用性状态取决于是否可以访问该设备。在跨网络高可用性配置中，每个 NetScaler Gateway 上的路由监视器都会扫描内部路由表，以确保其他 NetScaler Gateway 的条目始终存在。

添加路由监视器

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在“绑定/取消绑定路由监视器”对话框中的“路由监视器”选项卡上，单击“操作”，然后单击“配置”。
3. 在“指定路由监视器”下的“网络”中，键入其他 NetScaler Gateway 设备的网络 IP 地址。

   要配置 IPv6 地址，请单击 IPv6，然后键入 IP 地址。
4. 在 Netmask 中，键入另一个网络的子网掩码，单击添加，然后单击确定。

完成此过程后，路由监视器将绑定到 NetScaler Gateway。

注意：当路由监视器未绑定到 NetScaler Gateway 时，任一设备的高可用性状态由接口的状态决定。

删除路由监视器

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在路由监视器选项卡上，单击操作，然后单击配置。
3. 在已配置的路由监视器下，选择监视器，单击删除，然后单击确定。

配置链路冗余

February 1, 2024

链接冗余将网络接口组合在一起，以防止由于具有其他正常运行的接口的 NetScaler Gateway 的一个网络接口出现故障而导致故障尽管第一个接口仍然可以使用其第二个链接来处理用户请求，但主 NetScaler Gateway 上的第一个接口出现故障将触发故障转移。配置链路冗余时，可以将两个接口组合到一个故障转移接口集中，从而防止单个链路故障导致故障转移到辅助 NetScaler Gateway，除非主 NetScaler Gateway 上的所有接口都无法正常工作。

故障切换接口集中的每个接口都维护独立的网桥条目。未绑定到故障接口集的 NetScaler Gateway 上已启用的监视器接口和高可用性称为关键接口，因为如果这些接口中的任何一个出现故障，将触发故障转移。

配置链路冗余

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在故障切换接口集选项卡上，单击添加。
3. 在名称中，键入集的名称。
4. 在接口中，单击添加。
5. 在“可用接口”下，选择一个接口，然后单击箭头将该接口移动到“已配置”。
6. 对第二个界面重复步骤 4 和 5，然后单击“创建”。

您可以根据需要添加任意数量的接口，以实现接口之间的故障切换。

从故障切换接口集中删除接口

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在故障切换接口集选项卡上，选择一个集，然后单击删除。

删除故障切换接口集

如果不再需要故障转移接口集，则可以将其从 NetScaler Gateway 中删除。

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在故障切换接口集选项卡上，选择一个集，然后单击删除。

了解故障转移的原因

February 1, 2024

以下事件可能导致高可用性配置中的故障切换：

1. 如果辅助节点在超过辅助节点上设置的死区间间隔的一段时间内未收到来自主节点的心跳数据包。有关设置无效间隔的更多信息，请参阅 配置通信间隔。节点未从对等节点接收检测信号数据包的可能原因包括：
   - 网络配置问题阻止检测信号在高可用性节点之间穿过网络。
   - 对等节点遇到硬件或软件故障，导致它冻结（挂起）、重启或以其他方式停止处理和转发心跳数据包。
2. 主节点遇到 SSL 卡的硬件故障。
3. 主节点三秒钟内不会在其网络接口上接收任何心跳数据包。
4. 在主节点上，不属于故障切换接口集 (FIS) 或链路聚合 (LA) 通道且启用了高可用性监视器 (HAMON) 的网络接口发生故障。接口已启用，但进入 DOWN 状态。
5. 在主节点上，FIS 中的所有接口都失败。接口已启用，但进入 DOWN 状态。
6. 在主节点上，启用了哈蒙的 LA 频道失败。接口已启用，但进入 DOWN 状态。
7. 在主节点上，所有接口都失败。在这种情况下，无论哈蒙配置如何，都会发生故障切换。
8. 在主节点上，手动禁用所有接口。在这种情况下，无论哈蒙配置如何，都会发生故障切换。
9. 您可以在任一节点上发出强制故障切换命令来强制故障转移。
10. 绑定到主节点的路由监视器将关闭。

强制从节点进行故障切换

February 1, 2024

例如，如果需要替换或升级主节点，则可能需要强制进行故障切换。您可以强制从主节点或辅助节点进行故障切换。强制故障转移不会传播，也不会同步。要在强制故障切换后查看同步状态，可以查看节点的状态。

在下列任何一种情况下，强制故障转移会失败：

- 在独立的系统上强制执行故障转移。
- 辅助节点已禁用。
- 辅助节点配置为保持辅助状态。

如果 NetScaler Gateway 设备在运行强制故障转移命令时检测到潜在问题，则会显示警告消息。该消息包含触发警告并在继续之前请求确认的信息。

在主节点或辅助节点上强制故障切换

February 1, 2024

如果在主节点上强制进行故障切换，则主节点将成为辅助节点，辅助节点将成为主节点。只有当主节点可以确定辅助节点处于启动状态时，才能进行强制故障切换。

如果辅助节点处于关闭状态，则强制故障转移命令将返回以下错误消息：“由于对等体状态无效，无法进行操作。纠正并重试。”

如果辅助系统处于声明状态或处于非活动状态，则该命令将返回以下错误消息：`"Operation not possible now. Please wait for system to stabilize before retrying."`

如果从辅助节点运行强制故障转移命令，则辅助节点变为主节点，主节点变为辅助节点。只有当辅助节点的运行状况良好且该节点未配置为保持辅助节点时，才能发生强制故障切换。

如果辅助节点无法成为主节点，或者如果辅助节点配置为保持辅助节点（使用 STAYEDECURNY 选项），则该节点将显示以下错误消息：“无法进行操作，因为我的状态无效。有关详细信息，请查看节点。”

在主节点或辅助节点上强制进行故障切换

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择主节点，然后在“操作”中单击“强制故障转移”。
3. 在警告对话框中，单击是。

强制主节点保持主节点

February 1, 2024

在高可用性配置中，即使在设备故障转移之后，也可以强制主 NetScaler Gateway 保持主要状态。您只能在独立 NetScaler Gateway 设备和作为高可用性对中主设备的 NetScaler Gateway 上配置此设置。

强制主节点保持主节点

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的节点选项卡上，选择一个节点，然后单击编辑。
3. 在高可用性状态下，单击保持主要状态，然后单击确定。

只能使用以下命令清除此配置：

```
clear configuration full
```

以下命令不会更改 NetScaler Gateway 高可用性配置：

```
clear configuration basic
```

```
clear configuration extended
```

强制辅助节点保持辅助节点

February 1, 2024

在高可用性设置中，您可以强制辅助 NetScaler Gateway 保持辅助状态，而与主 NetScaler Gateway 的状态无关。将 NetScaler Gateway 配置为保持辅助状态时，即使主 NetScaler Gateway 出现故障，它仍将保持辅助状态。

例如，在现有的高可用性设置中，假设您需要升级主 NetScaler Gateway，并且此过程需要指定的时间。在升级期间，主 NetScaler Gateway 可能会变得不可用，但您不希望辅助 NetScaler Gateway 接管。您希望它保持辅助 NetScaler Gateway，即使它检测到主 NetScaler Gateway 中的故障也是如此。

如果高可用性对中 NetScaler Gateway 的状态配置为保持辅助状态，则它不会参与高可用性状态机转换。您可以在节点 选项卡上的配置实用程序中检查 NetScaler Gateway 的状态。

此设置适用于独立版和辅助 NetScaler Gateway。

设置高可用性节点时，它不会传播或同步，只会影响配置设置的 NetScaler Gateway。

强制辅助节点保持辅助节点

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择一个节点，然后单击“编辑”。
3. 在“高可用性状态”下，单击“保持辅助”（保持在侦听模式），然后单击“确定”。

使 **NetScaler Gateway** 作为活动的高可用性设备恢复运行

1. 在配置实用程序中，在“配置”选项卡的导航窗格中，展开“系统”，然后单击“高可用性”。
2. 在详细信息窗格的“节点”选项卡上，选择将保留主节点的设备，然后单击“打开”。
3. 在高可用性状态下，单击已启用（主动参与 HA），然后单击确定。

使用聚类

February 1, 2024

NetScaler Gateway 可以在群集配置中部署，以便为 VPN 客户端流量提供高吞吐量、高可用性和可扩展性。在群集中，一组 NetScaler Gateway 设备或虚拟机作为单个系统映像运行，以协调用户会话和管理到网络资源的流量。NetScaler Gateway 群集可以使用至少两个、最多 32 个 NetScaler Gateway 设备或虚拟机配置为群集节点来构建。

在开始配置
NetScaler Gateway 群集之前，请先阅读 NetScaler 群集文档。请特别注意该文档中的以下主题。

- 请参阅 硬件和软件要求 以验证计划使用的系统是否满足要求。
- 有关 聚类概念的说明，请参阅聚类的工 作原理。
- 请参阅 设置节点间通信 以规划部署并确定可能与您的环境相关的任何注意事项。

NetScaler Gateway 群集作为斑点 VIP 配置类型 NetScaler 群集运行。

> 重要：
>
> 群集不支持 **XenApp** 和 **XenDesktop** 向导，因此在 **GUI >** 导航窗格 **>** 与 **NetScaler** 产品集成 部分中找不到 **XenApp** 和 **XenDesktop** 向导。

配置群集化

February 1, 2024

设置 NetScaler Gateway 群集的主要任务是：

1. 确定哪个 NetScaler Gateway 设备或虚拟机是配置协调器，然后在该系统上创建群集实例（如果尚未存在）。
2. 将 NetScaler Gateway 系统作为节点加入群集。
3. 在群集实例上创建一个节点组，并设置了 STICKY 选项。
4. 将单个群集节点绑定到群集节点组。
5. 在配置协调器上配置 NetScaler Gateway 虚拟服务器，然后将其绑定到群集节点组。

有多种方法可用于配置 NetScaler 群集。以下一组任务使用配置实用程序中可用的最直接的方法。

使用配置实用程序创建 **NetScaler Gateway** 群集实例

准备好部署详细信息后，在作为配置协调器的 NetScaler Gateway 上开始配置。

警告：创建群集实例会清除配置。如果您需要保存现有系统配置以供参考，请在继续进行群集配置之前存档副本。群集建立后，可以在配置协调器上重新应用要在群集中使用的任何现有设置。

1. 在 NSIP 地址登录 NetScaler 配置实用程序。
2. 展开系统节点，然后展开群集子节点。
3. 在详细信息窗格中，单击 管理群集。
4. 在群集配置对话框中，设置创建群集所需的参数。
    a) 输入群集实例 ID。群集实例 ID 是群集实例的数字标识符。默认值为 1，但您可以将其设置为 1 到 16 之间的任意数字。
    b) 输入群集 IP 地址。群集 IP 地址是群集的配置协调器 IP 地址，即群集的管理 IP 地址。
    c) 选择首选的背板接口。这是用于群集节点之间通信的 NetScaler Gateway 接口。
5. 单击创建。
6. 出现确认系统重新启动的提示时，单击“是”。
7. 节点启动并且同步成功后，从群集 IP 地址更改节点和群集 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更 改 RPC 节点密码。
8. 等待系统重新启动。一旦可用，请使用步骤 4 (2) 中配置的群集 IP 地址登录配置实用程序。

注意：在 系统信息详细信息 窗格中，NSIP 地址的本地节点将报告为配置协调器。这确认基本群集实例现在正在运行。

配置协调器的本地节点将自动添加到群集中。在以下任务中可以添加更多节点。

向 **NetScaler Gateway** 群集添加节点

建立群集实例后，您可以开始向群集添加其他 NetScaler Gateway 节点。

要向群集添加更多 NetScaler Gateway 系统，可以使用配置实用程序远程发出群集节点创建和加入群集设置。

注意：在配置 NetScaler Gateway 设置之前，必须完成向群集添加节点的操作。这样，如果群集配置出现问题，并且想要删除群集然后重新开始，则不必重复 NetScaler Gateway 配置。

1. 在群集 IP 地址登录 NetScaler 配置实用程序。
2. 展开“系统”节点，然后展开“群集”子节点。
3. 在详细信息窗格中，单击 管理群集。
4. 在群集节点详细信息窗格中，单击 添加。
5. 在 创建群集节点 窗格中，输入此节点的唯一节点 ID。
6. 输入要添加为群集节点的系统的 NetScaler IP 地址。
7. 在 群集节点凭据 窗格中，输入远程 NetScaler Gateway 系统的 NetScaler Gateway 用户名和密码。
8. 在配置协调器凭据窗格中，输入本地授权用户的密码。
9. 单击创建。
10. 出现提示时，单击“是”以允许保存系统配置并对远程 NetScaler Gateway 执行热重启。
11. 节点启动并且同步成功后，从群集 IP 地址更改节点和群集 IP 地址的 RPC 凭据。有关更改 RPC 节点密码的更多信息，请参阅更 改 RPC 节点密码。

对于要配置为群集节点的每个其他远程 NetScaler Gateway 系统，重复步骤 4 到 11。

验证群集节点是否包含在群集节点详细信息窗格的主动节点列表中。如果缺少任何节点，请重复步骤 4 到 10，直到列出所有必需的节点。

创建群集节点组

添加群集节点后，即可创建群集节点组。

1. 在群集 IP 地址登录 NetScaler 配置实用程序。
2. 展开“系统”节点，然后展开“群集”子节点。
3. 单击 节点组。
4. 在详细信息窗格中，单击“添加”。
5. 输入群集节点组的名称。
6. 选择 粘性 选项以支持 NetScaler Gateway 虚拟服务器类型。
7. 单击继续。

现在已建立群集节点组。在离开配置实用程序的此区域之前，您可以将本地 NetScaler Gateway 节点绑定到新的群集节点组。这是绑定到群集组的唯一节点。

将本地群集节点绑定到群集节点组

由于 NetScaler Gateway 群集配置是斑点类型，因此只能将一个节点绑定到该节点组。以下过程将配置协调器上的本地节点绑定到节点组，但群集中的任何节点都可用于此绑定。

1. 在高级窗格中，展开群集节点。
2. 在中间的群集节点窗格中，选择无群集节点。
3. 在群集节点配置屏幕上，单击绑定。
4. 为此 NetScaler Gateway 系统选择由 NSIP 地址表示的本地节点。

5. 单击“插入”。
6. 单击确定。
7. 单击 Done（完成）。

群集现已填充完毕，可以按照以下任务的配置共享 NetScaler Gateway 虚拟服务器。

将 **NetScaler Gateway** 虚拟服务器绑定到群集节点组

建立群集后，您可以继续构建群集部署要提供的 NetScaler Gateway 配置。要将配置绑定到群集，您需要创建 NetScaler Gateway 虚拟服务器并将其绑定到设置为类型为 Sticky 的群集节点组。将虚拟服务器绑定到群集节点组后，您可以继续配置 NetScaler Gateway。

如果配置了多个 NetScaler Gateway 虚拟服务器，则这些虚拟服务器也必须绑定到群集节点组。

注意：如果尚未配置 NetScaler Gateway 虚拟服务器，则可能必须首先在
系统 **>** 设置 **>** 配置基本功能下启用 **NetScaler Gateway** 以及身份验证、授权和审核功能。

1. 在群集 IP 地址登录 NetScaler 配置实用程序。
2. 展开“系统”节点，然后展开“群集”子节点。
3. 单击 节点组。
4. 在“节点组”窗格中，选择所需的节点组名称，然后单击“编辑”。
5. 在右侧的“高级”窗格中，展开“虚拟服务器”选项，然后单击 + 图标以添加虚拟服务器。
6. 选择 VPN 虚拟服务器类型，然后单击 继续。
7. 单击绑定。
8. 如果列出了所需的虚拟服务器，请选择它，然后单击 插入，然后单击 确定。
9. 如果必须创建新的虚拟服务器，请单击 添加。继续完成 NetScaler 虚拟服务器配置。最起码，所需要做的只是创建虚拟服务器，以便它可以绑定到群集节点组。
10. 虚拟服务器在 NetScaler Gateway 虚拟服务器列表中可用后，选择它，然后单击 插入。
11. 单击确定。
12. 单击 **Done**（完成）。

注意：如果配置了多个 NetScaler Gateway 虚拟服务器，则必须使用相同的方法将这些虚拟服务器绑定到群集节点组。

Unified Gateway

February 1, 2024

带 **Unified Gateway** 的 **NetScaler**：一个 **URL**

具有 Unified Gateway 的 NetScaler 可让桌面和移动用户通过单个 URL 简化对任何应用程序的安全访问。在这个单一 URL 后面，管理员可以通过单点来配置、安全和控制对应用程序的远程访问。通过无缝单点登录所需的所有应用程序以及易于使用的登录/注销，远程用户的体验得到了改善。

为此，带网关的 NetScaler 以及 NetScaler 的内容交换功能和广泛的身份验证基础架构可通过此单个 URL 提供对组织站点和应用程序的访问。此外，无论身在何处，远程用户都可以使用 iOS 或 Android 移动设备以及 Linux、PC 或 Mac 系统和 Citrix Secure Access 客户端，统一访问 Unified Gateway URL。

Unified Gateway 部署允许对以下类别的应用程序进行单个 URL 访问：

- 内联网应用程序。
- 无客户端应用
- 软件即服务应用程序
- NetScaler 提供的预配置应用程序
- Citrix Virtual Apps and Desktops 发布的应用程序

Intranet 应用 程序可能是驻留在安全企业网络内的任何基于 Web 的应用程序。这些是内部资源，例如组织内部网站点、错误跟踪应用程序或 Wiki。

无客户端应用程序 Unified Gateway 通常也驻留在安全的企业网络内，它提供对 Outlook Web Access 和 SharePoint 的单个 URL 访问。这些应用程序提供对 Exchange 电子邮件和团队资源的访问权限，而无需专用的客户端软件，远程用户可以使用

SaaS 应用程序（通常也称为云应用程序）是组织所依赖的基于云的外部应用程序，例如 ShareFile、Salesforce 或 NetSuite。提供基于 SAML 的单点登录的 SaaS 应用程序支持。

一些组织可能已经预先配置了在 **NetScaler** 负载平衡配置中部署的 **NetScaler** 服务的应用程序。通常，这也被称为“reverse-proxy 理”应用程序。当用于部署的虚拟服务器位于同一 NetScaler Unified Gateway 实例或设备上时，Unified Gateway 支持这些应用程序。这些应用程序可能有自己的身份验证配置，该配置独立于 Unified Gateway 配置。

任何已发布的 **Citrix Virtual Apps and Desktops** 已发布的应用程序都可以通过 Unified Gateway URL 提供。可以选择将 SmartAccess 和 SmartControl 策略应用于对这些资源的精细策略和访问控制。

Unified Gateway 配置向导

使用 Unified Gateway 部署配置 NetScaler 的推荐方法是使用 Unified Gateway 配置向导。该向导将引导您完成配置，创建所有必需的虚拟服务器、策略和表达式，并根据提供的详细信息应用设置。初始设置后，该向导可用于管理您的部署并监视其操作。

> 注意：
>
> Unified Gateway 配置向导不执行初始系统配置。在配置 Unified Gateway 之前，您的 NetScaler Gateway

> 设备或 VPX 实例必须完成基本安装。请参阅使用首次设置向导配置 NetScaler Gateway 的安装说明以完成基本配置。

向导配置的 Unified Gateway 元素包括：

- Unified Gateway 主虚拟服务器
- Unified Gateway 虚拟服务器的 SSL 服务器证书
- 主要身份验证配置和任何可选的辅助
- 门户主题选择和可选的自定义
- 要通过 Unified Gateway 门户访问的用户应用程序

对于这些元素中的每一个，您都需要提供配置信息。对于基本的 Unified Gateway 部署，需要以下信息。

- 对于主 Unified Gateway 虚拟服务器，部署的公有 IP 地址和 IP 端口号。这是在 DNS 中解析为 Unified Gateway URL 的主机名的 IP 地址。例如，如果您的 Unified Gateway 部署的 URL 是 `https://mycompany.com/`，则 IP 地址必须解析为 mycompany.com。
- 用于部署的已签名 SSL 服务器证书。NetScaler Gateway 支持 PEM 或 PFX 格式的证书。
- 主身份验证服务器信息。此身份验证配置支持的身份验证系统基于 LDAP /Active Directory、RADIUS 和证书。还可能会创建辅助 LDAP 或 RADIUS 身份验证配置。必须提供身份验证服务器 IP 地址以及任何相关的管理员凭据或目录属性。对于证书身份验证，必须提供设备证书属性和 CA 证书。
- 可能会选择门户主题。如果需要自定义或品牌化的门户设计，则可以使用向导将自定义图形上载到系统。
- 对于基于 Web 的用户应用程序，必须指定各个应用程序的 URL。对于要使用 SAML 单点登录身份验证的 Web 应用程序，该实用程序会收集断言使用者服务 URL 以及其他可选的 SAML 参数。提前收集使用 SAML 身份验证系统的应用程序的配置详细信息。
- 对于要通过 Unified Gateway 部署提供的 Citrix Virtual Apps and Desktops 发布的资源，必须指定集成点（StoreFront、Web Interface 或 Web Interface on NetScaler）。该实用程序需要集成点的完全限定域名、站点路径、单点登录域、Secure Ticket Authority (STA) 服务器 URL 以及其他具体取决于集成点的类型。

其他配置管理

对于 Unified Gateway 配置实用程序中不可用的站点特定设置，例如备用 SSL 设置或会话策略，您可以在 NetScaler Gateway 配置实用程序中管理所需的设置。Unified Gateway 配置实用程序创建这些设置后，您可以在内容交换或 VPN 虚拟服务器上修改这些设置。

内容交换虚拟服务器

这是部署的主 IP 地址和 URL 背后的 NetScaler 配置实体。SSL 服务器证书和参数在此虚拟服务器上进行管理。由于此虚拟服务器是部署的响应网络主机，因此如有必要，可以在此虚拟服务器上修改 ICMP 服务器响应和 RHI 状态。可以在 流量管理 **>** 内容交换 **>** 虚拟服务器的配置选项卡下找到内容交换虚拟服务器。

> 重要：
>
> 将 Unified Gateway 环境升级到 13.0 版本 58.x 或更高版本时，在网关或 VPN 虚拟服务器之前配置的内容交换虚拟服务器中禁用 DTLS 旋钮。升级后在内容交换虚拟服务器中手动启用 DTLS 旋钮。如果使用向导进行配置，请不要启用 DTLS 旋钮。

VPN 虚拟服务器

Unified Gateway 配置的所有其他 VPN 参数、配置文件和策略绑定都在此虚拟服务器上进行管理，包括主身份验证配置。此实体在 **NetScaler Gateway** > 虚拟服务器 的“配置”选项卡下进行管理。相关 VPN 虚拟服务器的名称包括在初始 Unified Gateway 配置期间为内容交换虚拟服务器指定的名称。

> 注意：
>
> 为 Unified Gateway 部署创建的 VPN 虚拟服务器不可寻址，并分配了 0.0.0.0 IP 地址。

Unified Gateway FAQ

February 1, 2024

什么是 **Unified Gateway**

Unified Gateway 是 NetScaler 11.0 版本中的一项新功能，可在单个虚拟服务器（称为 Unified Gateway 虚拟服务器）上接收流量，然后根据需要在内部将流量定向到 Unified Gateway 虚拟服务器的虚拟服务器。

Unified Gateway 功能允许最终用户使用单个 IP 地址或 URL（与 Unified Gateway 虚拟服务器关联）访问多个服务。管理员可以释放 IP 地址并简化 NetScaler Gateway 部署的配置。

作为编队的一部分，每个 Unified Gateway 虚拟服务器都可以前端一个 NetScaler Gateway 虚拟服务器以及零个或多个负载平衡虚拟服务器。Unified Gateway 通过使用 NetScaler 设备的内容交换功能来工作。

Unified Gateway 部署的一些示例：

- Unified Gateway 虚拟服务器-> [一台 NetScaler Gateway 虚拟服务器]
- Unified Gateway 虚拟服务器-> [一台 NetScaler Gateway 虚拟服务器，一台负载平衡虚拟服务器]
- Unified Gateway 虚拟服务器-> [一台 NetScaler Gateway 虚拟服务器，两台负载平衡虚拟服务器]
- Unified Gateway 虚拟服务器-> [一台 NetScaler Gateway 虚拟服务器，三台负载平衡虚拟服务器]

每个负载平衡虚拟服务器都可以是托管后端服务的任何标准负载平衡服务器，例如 Microsoft Exchange 或 Citrix ShareFile。

为什么要使用 **Unified Gateway**

Unified Gateway 功能使最终用户能够使用单个 IP 地址或 URL（与 Unified Gateway 虚拟服务器关联）访问多个服务。对于管理员而言，优势在于他们可以释放 IP 地址并简化 NetScaler Gateway 部署的配置。

是否可以有多台 **Unified Gateway** 虚拟服务器

是。可以根据需要有尽可能多的 Unified Gateway 虚拟服务器。

为什么 **Unified Gateway** 需要内容交换

内容交换功能是必需的，因为内容交换虚拟服务器是接收流量并在内部将其定向到相应虚拟服务器的服务器。内容交换虚拟服务器是 Unified Gateway 功能的主要组件。

在 **11.0** 之前的版本中，内容交换可用于接收多个虚拟服务器的流量。这种用法也称为 **Unified Gateway** 吗

11.0 之前的版本支持使用内容交换虚拟服务器来接收多个虚拟服务器的流量。但是，内容交换无法将流量定向到 NetScaler Gateway 虚拟服务器。

11.0 中的增强功能使内容交换虚拟服务器能够将流量定向到任何虚拟服务器，包括 NetScaler Gateway 虚拟服务器。

Unified Gateway 中的内容交换策略发生了什么变化

1. 为内容切换操作添加了新的命令行参数“-targetVserver”。新参数用于指定目标 NetScaler Gateway 虚拟服务器。示例：

   ```
   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
   ```

   在 NetScaler Gateway 配置实用程序中，内容切换操作有一个新选项“目标虚拟服务器”，该选项可引用 NetScaler Gateway 虚拟服务器。

2. 新的高级策略表达式 is_vpn_url 可用于匹配 NetScaler Gateway 和特定于身份验证的请求。

Unified Gateway 目前不支持哪些 **NetScaler Gateway** 功能

Unified Gateway 支持所有功能。但是，通过 VPN 插件进行本机登录时报告了一个小问题（问题 ID 544325）。在这种情况下，无缝单点登录 (SSO) 不起作用。

使用 **Unified Gateway**，**EPA** 扫描的行为是什么

使用 Unified Gateway 时，仅针对 NetScaler Gateway 访问方法触发端点分析，而不会针对 NetScaler AAA TM 访问触发端点分析。如果用户尝试访问 NetScaler AAA TM 虚拟服务器，即使身份验证是在 NetScaler Gateway 虚拟服务器上完成的，也不会触发 EPA 扫描。但是，如果用户试图获得无客户端 VPN /完全 VPN 访问权限，则会触发配置的 EPA 扫描。在这种情况下，将完成身份验证或无缝 SSO。

Unified Gateway 的许可证要求是什么

Unified Gateway 仅支持高级和高级许可证。它不适用于仅 NetScaler Gateway 或标准许可证版本。

与 **Unified Gateway** 一起使用的 **NetScaler Gateway** 虚拟服务器是否需要 **IP/Port/SSL** 配置

对于与 Unified Gateway 虚拟服务器一起使用的 NetScaler Gateway 虚拟服务器，NetScaler Gateway 虚拟服务器上不需要 IP/Port/SSL 配置。但是，对于 RDP 代理功能，您可以将相同的 SSL/TLS 服务器证书绑定到 NetScaler Gateway 虚拟服务器。

我是否需要重新配置 **NetScaler Gateway** 虚拟服务器上的 **SSL/TLS** 证书以用于 **Unified Gateway** 虚拟服务器

您无需重新置备当前绑定到 NetScaler Gateway 虚拟服务器的证书。您可以自由重复使用任何现有的 SSL 证书，并将这些证书绑定到 Unified Gateway 虚拟服务器。

单个 **URL** 和多主机部署有什么区别？我需要哪一个

单个 URL 是指 Unified Gateway 虚拟服务器处理一个完全限定域名 (FQDN) 的流量的能力。如果 Unified Gateway 使用的 SSL/TLS 服务器证书已使用 FQDN 填充了证书主题，则存在此限制。例如：ug.citrix.com

如果 Unified Gateway 使用通配符服务器证书，它可以处理多个子域的流量。例如：*.citrix.com

另一个选项是具有服务器名称指示器 (SNI) 功能的 SSL/TLS 配置，以允许绑定多个 SSL/TLS 服务器证书。示例：auth.citrix.com、auth.citrix.de、auth.citrix.co.uk、auth.citrix.co.jp

单主机与多台主机类似于网站通常托管在 Web 服务器上的方式（例如 Apache HTTP 服务器或 Microsoft Internet Information Services (IIS)）。如果只有一台主机，则可以使用站点路径切换流量，就像在 Apache 中使用别名或“虚拟目录”一样。如果有多台主机，则可以使用主机标头切换流量，就像在 Apache 中使用虚拟主机的方式一样。

Unified Gateway 可以使用哪些身份验证机制

与 NetScaler Gateway 兼容的所有现有身份验证机制也与 Unified Gateway 兼容。

其中包括 LDAP、RADIUS、SAML、Kerberos、基于证书的身份验证等。

当 NetScaler Gateway 虚拟服务器放置在 Unified Gateway 虚拟服务器后面时，升级之前在 NetScaler Gateway 虚拟服务器上配置的任何身份验证机制都会自动使用。除了为 NetScaler Gateway 虚拟服务器分配不可寻址的 IP 地址 (0.0.0.0) 外，不涉及其他配置步骤。

什么是“**SelfAuth**”’ 身份验证

SelfAuth 本身不是身份验证类型。SelfAuth 描述了如何创建 URL。新的命令行参数可用于 VPN URL 配置。`ssotype` 示例：

```
> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelfAuth 是 `ssotype` 参数的值之一。这种类型的 URL 可用于访问与 Unified Gateway 虚拟服务器不在同一域中的资源。配置书签时，可以在配置实用程序中看到该设置。

什么是“**StepUp**”身份验证”

如果需要额外的身份验证，访问 NetScaler AAA TM 资源需要更安全级别的身份验证，则可以使用 StepUp 身份验证。在命令行上，使用 authnProfile 命令设置 authenticationLevel 参数。示例：

```
1 add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
     AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
     **-**AuthenticationLevel 100
2 <!--NeedCopy-->
```

此身份验证配置文件绑定到负载平衡虚拟服务器。

NetScaler AAA TM 虚拟服务器是否支持 **StepUp** 身份验证

是的，它受支持。

什么是 **`login once/logout once`**

`Login Once`: VPN 用户只需登录一次 NetScaler AAA TM 或 NetScaler Gateway 虚拟服务器。从那时起，VPN 用户可以无缝访问所有企业/云 /Web 应用程序。用户无需重新进行身份验证。但是，重新身份验证是针对特殊情况进行的，例如 NetScaler AAA TM StepUp。

`Logout Once`：创建第一个 NetScaler AAA TM 或 NetScaler Gateway 会话后，它将用于为该用户创建后续的 NetScaler AAA TM 或 NetScaler Gateway 会话。如果这些会话中的任何一个已注销，NetScaler 设备还会注销用户的其他应用程序或会话。

是否可以在 **Unified Gateway** 级别指定通用身份验证策略，并在负载平衡虚拟服务器级别使用 **NetScaler AAA TM** 负载平衡特定于虚拟服务器的身份验证绑定支持此用例的配置步骤是什么

如果您需要为 Unified Gateway 后面的 NetScaler AAA TM 虚拟服务器指定单独的身份验证策略，则需要有一个单独的、可独立寻址的身份验证虚拟服务器（类似于普通 NetScaler AAA TM 配置）。负载平衡虚拟服务器上的身份验证主机设置必须指向此身份验证虚拟服务器。

如何配置 **Unified Gateway**，以便绑定的 **NetScaler AAA TM** 虚拟服务器具有自己的身份验证策略

在这种情况下，负载平衡服务器必须将身份验证 FQDN 选项设置为指向 NetScaler AAA TM 虚拟服务器。NetScaler AAA TM 虚拟服务器必须具有独立的 IP 地址，并且可以从 NetScaler 和客户端访问。

对通过 **Unified Gateway** 虚拟服务器的用户进行身份验证是否需要 **NetScaler AAA TM** 身份验证虚拟服务器

不是。NetScaler Gateway 虚拟服务器甚至可以对 NetScaler AAA TM 用户进行身份验证。

在 **Unified Gateway** 虚拟服务器或 **NetScaler Gateway** 虚拟服务器上，在哪里指定 **NetScaler Gateway** 身份验证策略

身份验证策略将绑定到 NetScaler Gateway 虚拟服务器。

如何在 **Unified Gateway** 内容交换虚拟服务器后面的 **NetScaler AAA TM** 虚拟服务器上启用身份验证

在 NetScaler AAA TM 上启用身份验证，然后将身份验证主机指向 Unified Gateway 内容交换 FQDN。

如何在内容切换背后添加 **TM** 虚拟服务器（单一 **URL** 还是多主机）

为单个 URL 添加 NetScaler AAA TM 虚拟服务器与为多个主机添加虚拟服务器没有区别。无论哪种情况，虚拟服务器都会作为内容切换操作中的目标添加。单个 URL 与多主机之间的区别是通过内容切换策略规则来实现的。

如果将 **NetScaler AAA TM** 负载平衡虚拟服务器移动到 **Unified Gateway** 虚拟服务器后面，绑定到该虚拟服务器的身份验证策略会发生什么变化

身份验证策略绑定到身份验证虚拟服务器，身份验证虚拟服务器绑定到负载平衡虚拟服务器。对于 Unified Gateway 虚拟服务器，Citrix 建议将 NetScaler Gateway 虚拟服务器作为单一身份验证点，这样就无需在身份验证虚拟服务器上执行身份验证（甚至不需要特定身份验证虚拟服务器）。将身份验证主机指向 Unified Gateway 虚拟服务器 FQDN 可确保由 NetScaler Gateway 虚拟服务器完成身份验证。如果将身份验证主机指向 Unified Gateway 的内容交换，

但仍绑定了身份验证虚拟服务器，则绑定到身份验证虚拟服务器的身份验证策略将被忽略。但是，如果将身份验证主机指向独立的可寻址身份验证虚拟服务器，则绑定的绑定身份验证策略将生效。

如何为 **NetScaler AAA TM** 会话配置会话策略

如果在 Unified Gateway 中，未为 NetScaler AAA TM 虚拟服务器指定身份验证虚拟服务器，则 NetScaler AAA TM 会话将继承 NetScaler Gateway 会话策略。如果指定了身份验证虚拟服务器，则会应用绑定到该虚拟服务器的 NetScaler AAA TM 会话策略。

NetScaler 11.0 中的 **NetScaler Gateway** 门户有哪些更改

在 11.0 之前的 NetScaler 版本中，可以在全局级别设置单个门户自定义设置。给定 NetScaler 设备中的每个网关虚拟服务器都使用全局门户自定义设置。

在 NetScaler 11.0 中，使用门户主题功能，您可以设置多个门户主题。主题可以全局绑定或绑定到特定的虚拟服务器。

NetScaler 11.0 是否支持 **NetScaler Gateway** 门户自定义

使用配置实用程序，您可以使用新的门户主题功能完全自定义和创建门户主题。您可以上载不同的图像，设置配色方案，更改文本标签等。

可以自定义的门户页面包括：

- 登录页面
- 端点分析页
- 端点分析错误页面
- 端点后分析页
- VPN 连接页
- 门户主页

在此版本中，您可以使用独特的门户设计自定义 NetScaler Gateway 虚拟服务器。

NetScaler 高可用性或群集部署是否支持门户主题

是。NetScaler 高可用性和群集部署支持门户主题。

我的自定义设置是否会作为 **NetScaler 11.0** 升级过程的一部分进行迁移

不是。升级到 NetScaler 11.0 时，不会自动迁移通过 rc.conf/rc.netscaler 文件修改或使用 10.1/10.5 中的自定义主题功能调用的 NetScaler Gateway 门户页面的现有自定义项。

是否需要遵循任何升级前步骤才能为 **NetScaler 11.0** 中的门户主题做好准备

必须从 rc.conf 或 rc.netscaler 文件中删除任何现有的自定义项。

另一种选择是，如果使用自定义主题，则必须为它们分配默认设置：

1. 导航到 配置 **> NetScaler Gateway >** 全局设置
2. 单击“更改全局设置”。
3. 单击 客户端体验，然后从 **UI** 主题 列表中选择 默认。

我有存储在 **NetScaler** 实例上的自定义项，由 **rc.conf** 或 **rc.netscaler** 调用。如何移动到门户主题

Citrix 知识中心文章 CTX126206 详细介绍了 NetScaler 9.3 和 10.0 版本最高 10.0 版本 73.5001.e 的此类配置。自 NetScaler 10.0 版本 10.0 73.5002.e（包括 10.1 和 10.5）以来，UITHEME 自定义参数已可用于帮助客户在重新启动期间保留自定义项。如果自定义项存储在 NetScaler 硬盘驱动器上，并且您想继续使用这些自定义项，请备份 11.0 GUI 文件并将其插入现有的自定义主题文件中。如果要移动到门户主题，必须首先在“客户端体验”下的“全局设置”或“会话”配置文件中取消设置 UITHEME 参数。或者，您可以将其设置为 DEFAULT 或 GREENBUBBLE。然后您就可以开始创建和绑定门户主题了。

在升级到 **NetScaler 11.0** 之前，如何导出当前的自定义设置并保存它们？我可以将导出的文件移动到其他 **NetScaler** 设备吗

上载到 **ns_gui_custom** 文件夹的自定义文件位于磁盘上，并在升级过程中保留。但是，这些文件可能与新的 NetScaler 11.0 内核和作为内核一部分的其他 GUI 文件并不完全兼容。因此，Citrix 建议备份 11.0 GUI 文件并自定义备份。

此外，配置实用程序中没有实用程序可以将 **ns_custom_gui** 文件夹导出到另一个 NetScaler 设备。使用 SSH 或 WinSCP 之类的文件传输实用程序将文件从 NetScaler 实例中删除。

NetScaler AAA TM 虚拟服务器是否支持门户主题

是。NetScaler AAA TM 虚拟服务器支持门户主题。

NetScaler Gateway 11.0 的 **RDP** 代理功能发生了什么变化

自 NetScaler 10.5.e 增强版发布以来，已对 RDP 代理进行了许多增强。在 NetScaler 11.0 中，此功能可从第一个发布的版本中使用。

许可变更

NetScaler 11.0 中的 RDP 代理功能只能用于高级版和高级版。必须为每个用户获取 Citrix 并发用户 (CCU) 许可证。

启用命令

在 NetScaler 10.5.e 中，没有启用 RDP 代理的命令。在 NetScaler 11.0 中，已添加启用命令：

```
enable feature rdpproxy
<!--NeedCopy-->
```

该功能必须获得许可才能运行此命令。

其他 **RDP** 代理更改

服务器配置文件中的预共享密钥 (PSK) 属性已成为必填项。

要将 RDP 代理的现有 NetScaler 10.5.e 配置迁移到 NetScaler 11.0，必须了解并解决以下详细信息。

如果管理员想要将现有的 RDP 代理配置添加到选定的 Unified Gateway 部署中：

- 必须编辑 NetScaler Gateway 虚拟服务器的 IP 地址并将其设置为不可寻址的 IP 地址 (0.0.0.0)。
- 任何 SSL/TLS 服务器证书、身份验证策略都必须绑定到作为所选 Unified Gateway 编队一部分的 NetScaler Gateway 虚拟服务器。

如何将基于 **NetScaler 10.5.e** 的远程桌面协议 **(RDP)** 代理配置迁移到 **NetScaler 11.0**

选项 1：使用高级或高级许可证，使用 RDP 代理配置保持现有 NetScaler Gateway 虚拟服务器的原样。

选项 2：使用 RDP 代理配置移动现有 NetScaler Gateway 虚拟服务器，将其置于 Unified Gateway 虚拟服务器后面。

选项 3：将具有 RDP 代理配置的独立 NetScaler Gateway 虚拟服务器添加到现有标准版设备。

如何使用 **NetScaler 11.0** 版本为 **RDP** 代理配置设置 **NetScaler Gateway**

使用 NS 11.0 版本部署 RDP 代理有两种选项：

1. 使用面向外部的 NetScaler Gateway 虚拟服务器。这需要 NetScaler Gateway 虚拟服务器使用一个外部可见的 IP 地址 /FQDN。此选项是 NetScaler 10.5.e 中提供的选项。
2. 在 NetScaler Gateway 虚拟服务器前端使用 Unified Gateway 虚拟服务器。

使用选项 2 时，NetScaler Gateway 虚拟服务器不需要自己的 IP 地址 /FQDN，因为它使用不可寻址的 IP 地址 (0.0.0.0)。

HDX Insight 是否与 Unified Gateway 兼容

使用 Unified Gateway 部署 NetScaler Gateway 时，必须满足以下条件：

- NetScaler Gateway 虚拟服务器必须绑定有效的 SSL 证书。
- NetScaler Gateway 虚拟服务器必须处于 UP 状态才能在 NetScaler ADM 上生成 AppFlow 记录，以进行 HDX Insight 报告。

如何迁移我现有的 HDX Insight 配置

不需要迁移。如果将 NetScaler Gateway 虚拟服务器放在 Unified Gateway 虚拟服务器后面，绑定到 NetScaler Gateway 虚拟服务器的 AppFlow 策略将继续执行。

对于 NetScaler Gateway 虚拟服务器的 NetScaler ADM 上的现有数据，有两种可能性：

- 如果在迁移到 Unified Gateway 的过程中将 NetScaler Gateway 虚拟服务器的 IP 地址分配给 Unified Gateway 虚拟服务器，则数据将保持链接到 NetScaler Gateway 虚拟服务器
- 如果为 Unified Gateway 虚拟服务器分配了单独的 IP 地址，则 NetScaler Gateway 虚拟服务器中的 AppFlow 数据将链接到该新 IP 地址。因此，现有数据不是新数据的一部分。

NetScaler Gateway 设备上的 VPN 配置

February 1, 2024

> 重要：
>
> 出于以下原因，本部分中的屏幕截图以灰度方案进行维护：
>
> - 帮助视障读者，尤其是色盲或色差的读者。
> - 使用灰度图像以通用形式表示图像，该形式不显示可能已在用户浏览器或操作系统中完成的颜色编码自定义的影响。

用户可以使用以下方法通过 NetScaler Gateway 连接到组织的网络资源：

- 包含用户设备上安装的所有 Citrix 插件的 Citrix Workspace 应用程序。
- 适用于 Web 的 Citrix Workspace 应用程序，允许用户使用 Web 浏览器连接到应用程序、桌面和 ShareFile。
- Secure Hub，允许用户从其 iOS 和 Android 设备访问 Secure Mail、WorxWeb 和移动应用程序。
- 适用于 Windows、macOS X 或 Linux 的 Citrix Secure Access 客户端。
- 适用于 iOS 和 Android 的 NetScaler Gateway 应用程序。
- 无客户端访问，为用户提供所需的访问权限，而无需安装用户软件。
- 与 Citrix SD-WAN 插件的互操作性。

如果用户安装了 Citrix Secure Access 客户端，然后从适用于 Windows Server 2008 的 Citrix Virtual Apps 6.5（包括 Feature Pack 和 Feature Pack 2）、Citrix Virtual Desktops 7.0 或更高版本中安装 Citrix Workspace 应用程序，则 Citrix Workspace 应用程序会自动添加 Citrix Secure Access 客户端。用户可以通过网络浏览器或 Citrix Workspace 应用程序连接 Citrix Secure Access 客户端。

SmartAccess 会根据端点分析扫描的结果自动确定允许用户设备使用的访问方法。有关 SmartAccess 的详细信息，请参阅 配置 SmartAccess。

NetScaler Gateway 支持适用于 iOS 和 Android 移动设备的 Citrix Endpoint Management 移动生产力应用程序。NetScaler Gateway 包含 Secure Browse，允许从建立 Micro VPN 通道的 iOS 移动设备连接到 NetScaler Gateway。与 Secure Hub 连接的 Android 设备还会自动建立 Micro VPN 通道，提供对内部网络中资源的 Secure Web 和移动应用程序级别的访问。如果用户从具有 移动生产力应用程序的 Android 设备连接，则必须在 NetScaler Gateway 上配置 DNS 设置。有关详细信息，请参阅使用适 用于 Android 设备的 DNS 后缀支持 DNS 查询。

用户如何连接 **Citrix Secure Access** 客户端

February 1, 2024

NetScaler Gateway 的运行方式如下：

- 当用户尝试通过 VPN 通道访问网络资源时，Citrix Secure Access 客户端会加密所有发往组织内部网络的网络流量，并将数据包转发到 NetScaler Gateway。
- NetScaler Gateway 终止 SSL 通道，接受任何目的地为专用网络的传入流量，然后将流量转发到专用网络。NetScaler Gateway 通过安全通道将流量发送回远程计算机。

当用户键入 Web 地址时，他们会收到一个登录页面，他们可以在其中输入凭据并登录。如果凭据正确，NetScaler Gateway 将完成与用户设备的握手。

如果用户在代理服务器后面，用户可以指定代理服务器和身份验证凭据。有关详细信息，请参阅 为用户连接启用代理支持。

Citrix Secure Access 客户端安装在用户设备上。第一次连接后，如果用户使用基于 Windows 的计算机登录，则可以使用通知区域中的图标建立连接。

建立安全通道

当用户连接到 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序时，客户端软件会在端口 443（或 NetScaler Gateway 上任何已配置的端口）上建立安全通道并发送身份验证信息。建立通道后，NetScaler Gateway 会向 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序发送配置信息，描述需要保护的网络，并在启用地址池时包含 IP 地址。

通过安全连接建立通道专用网络流

当 Citrix Secure Access 客户端启动并对用户进行身份验证时，将捕获所有发往指定专用网络的网络流量，并通过安全通道重定向到 NetScaler Gateway。Citrix Workspace 应用程序必须支持 Citrix Secure Access 客户端，才能在用户登录时通过安全通道建立连接。

Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 为 iOS 和 Android 移动设备建立安全通道。

NetScaler Gateway 会拦截用户设备建立的所有网络连接，并通过安全套接字层 (SSL) 将这些连接复用到 NetScaler Gateway，在这里，流量将被解复用，并将连接转发到正确的主机和端口组合。

连接受适用于单个应用程序、应用程序子集或整个 Intranet 的管理安全策略的约束。您可以指定远程用户可以通过 VPN 连接访问的资源（IP 地址/子网对的范围）。

Citrix Secure Access 客户端为定义的内联网应用程序拦截以下协议并通过通道传输这些协议：

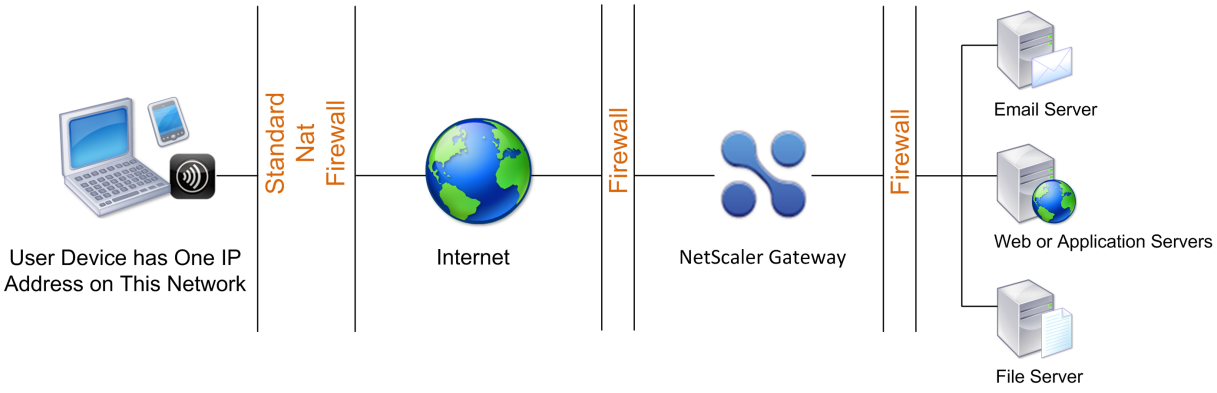
- TCP（所有端口）
- UDP（所有端口）
- ICMP（类型 8 和 0-回应请求/回复）

来自用户设备上本地应用程序的连接会安全地通过通道传输到 NetScaler Gateway，从而重新建立与目标服务器的连接。目标服务器将连接视为源自专用网络上的本地 NetScaler Gateway，因此隐藏了用户设备。这也称为反向网络地址转换 (NAT)。隐藏 IP 地址可以增加源位置的安全性。

在本地，在用户设备上，所有与连接相关的流量，例如 SYN-ACK、PUSH、ACK 和 FIN 数据包，都由 Citrix Secure Access 客户端重新创建，从私人服务器出现。

通过防火墙和代理进行连接

Citrix Secure Access 客户端的用户有时位于另一个组织的防火墙内，如下图所示：



NAT 防火墙维护一个表，允许它们将安全数据包从 NetScaler Gateway 路由回用户设备。对于面向电路的连接，NetScaler Gateway 维护一个端口映射的反向 NAT 转换表。反向 NAT 转换表使 NetScaler Gateway 能够匹配连接并通过通道将数据包发回具有正确端口号的用户设备，以便数据包返回到正确的应用程序。

Citrix Secure Access 客户端的控制升级

当 NetScaler 插件的版本与 NetScaler Gateway 修订版本不匹配时，系统管理员控制其执行方式。新选项控制 Mac、Windows 或操作系统的插件升级行为。

对于 VPN 插件，可以在 NetScaler 设备用户界面的两个位置设置升级选项：

- 在全局设置
- 在会话配置文件级别

要求

- Windows EPA 和 VPN 插件版本必须大于 11.0.0.0
- Mac EPA 插件版本必须大于 3.0.0.31
- Mac VPN 插件版本必须大于 3.1.4 (357)

> 注意：
>
> 如果 NetScaler 设备升级到 11.0 版本，则无论升级控制配置如何，所有以前的 VPN（和 EPA）插件都会升级到最新版本。对于后续升级，它们遵循以前的升级控制配置。

插件行为

对于每种客户端类型，NetScaler Gateway 允许使用以下三个选项来控制插件升级行为：

- 总是

只要最终用户的插件版本与 NetScaler 设备随附的插件不匹配，插件就会始终升级。这是默认行为。如果您不想在企业中运行多个插件版本，请选择此选项。

- 基本（和安全性）

插件仅在认为必要时才进行升级。在以下两种情况下，必须进行升级

- 已安装的插件与当前的 NetScaler 设备版本不兼容。
- 必须更新已安装的插件才能进行必要的安全修复。

如果要尽量减少插件升级次数，但又不想错过任何插件安全更新，请选择此选项

- 从不

插件没有升级。

用于控制 **VPN** 插件升级的 **CLI** 参数

NetScaler Gateway 支持适用于 Windows 和 Mac 操作系统的两种类型的插件（EPA 和 VPN）。为了在会话级别支持 VPN 插件升级控制，NetScaler Gateway 支持两个名为 WindowsInPluginUpgrade 和 MacPluginUpgrade 的会话配置文件参数。

这些参数可在全局、虚拟服务器、组和用户级别使用。每个参数的值可以为“始终”、“基本”或“从不”。有关这些参数的说明，请参阅 插件行为。

用于控制 **EPA** 插件升级的 **CLI** 参数

NetScaler Gateway 支持适用于 Windows 和 Mac 操作系统的 EPA 插件。为了在虚拟服务器级别支持 EPA 插件升级控制，NetScaler Gateway 支持两个名为 WindowSEpaPluginUpgrade 和 macepaPluginUpgrade 的虚拟服务器参数。

这些参数在虚拟服务器级别可用。每个参数的值可以为“始终”、“基本”或“从不”。有关这些参数的说明，请参阅 插件行为。

VPN 配置

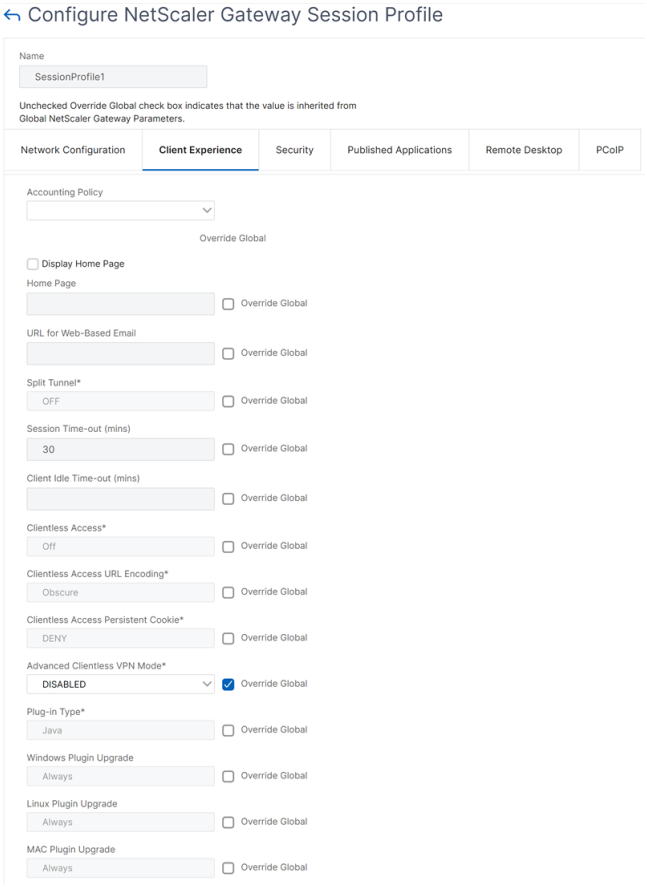
请按照以下步骤进 行 **Windows**、**Linux** 和 **Mac** 插件的 **VPN** 配置。

1. 转到 **NetScaler >** 策略 **>** 会话。
2. 选择所需的会话策略，然后单击 编辑。
3. 选择“客户体验”选项卡。
4. 这些对话框选项会影响升级行为。

    - 总是
    - 基本
    - 从不默

      认值为“始终”。

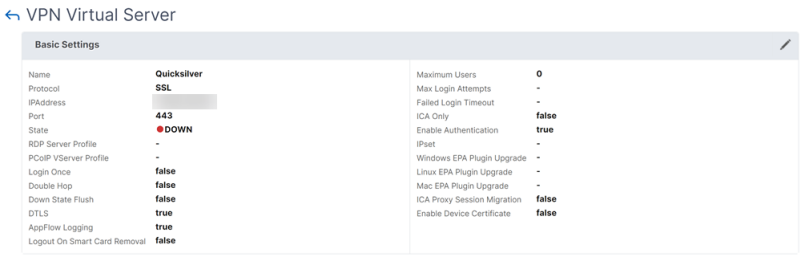
5. 选中每个选项右侧的复选框。选择应用升级行为的频率。



EPA 配置

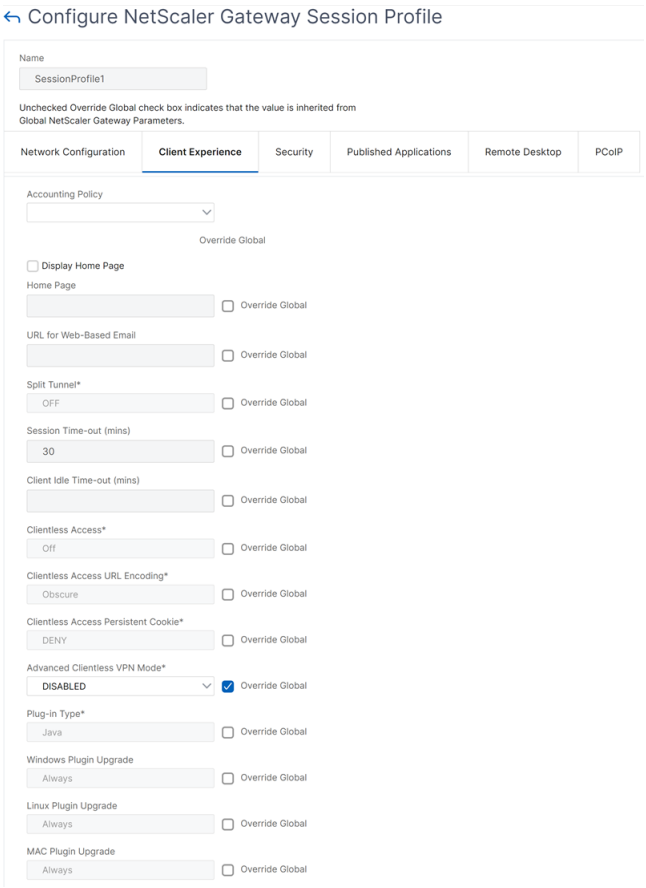
对于 Windows、Linux 和 Apple 插件的 EPA 配置，请按照以下步骤操作。

1. 转到 **NetScaler Gateway >** 虚拟服务器。
2. 选择一个服务器，然后单击 编辑 按钮。
3. 单击 铅笔 图标。



4. 单击 更多
5. 出现的对话框会影响升级行为。可用选项如下：
    - 总是

- 基本
- 从不



NetScaler Gateway 上的完整 VPN 设置

February 1, 2024

本节介绍如何在 NetScaler Gateway 设备上配置完整的 VPN 设置。它包含网络考虑因素以及从网络角度解决问题的理想方法。

必备条件

- 安装 SSL 证书并将其绑定到 VPN 虚拟服务器。
  - CTX109260- 如何在 NetScaler 设备上生成和安装公共 SSL 证书
  - CTX122521- 如何使用与设备主机名匹配的受信任 CA 证书替换 NetScaler 设备的默身份验证书
  - NetScaler 文档- 将证书密钥对绑定到基于 SSL 的虚拟服务器

- 为 NetScaler Gateway 创建身份验证配置文件。
  - 有关其他信息，请参阅 NetScaler 文档- 配置外部用户身份验证
  - 有关其他信息，请参阅清单：使用 AD FS 实施和管理单点登录
- 下载 VPN 客户端。
- 创建允许完整 VPN 连接的会话策略。

当用户连接到 Citrix Secure Access 客户端、Secure Hub 或 Citrix Workspace 应用程序时，客户端软件会在端口 443（或 NetScaler Gateway 上任何已配置的端口）上建立安全通道并发送身份验证信息。通道建立后，NetScaler Gateway 将配置信息发送到 Citrix Secure Access 客户端、Citrix Secure Hub 或 Citrix Workspace 应用程序，描述要保护的网络。如果启用 Intranet IP，则该信息还包含 IP 地址。

您可以通过定义用户可以在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括以下内容：

- 拆分通道
- 用户的 IP 地址，包括地址池（内部网 IP）
- 通过代理服务器的连接
- 定义允许用户访问的域
- 超时设置
- 单点登录
- 通过 NetScaler Gateway 连接的用户软件
- 移动设备的访问权限

您可以使用作为会话策略一部分的配置文件来配置大多数用户设备连接。您还可以使用按身份验证、流量和授权策略定义用户设备连接设置。它们也可以使用 Intranet 应用程序进行配置。

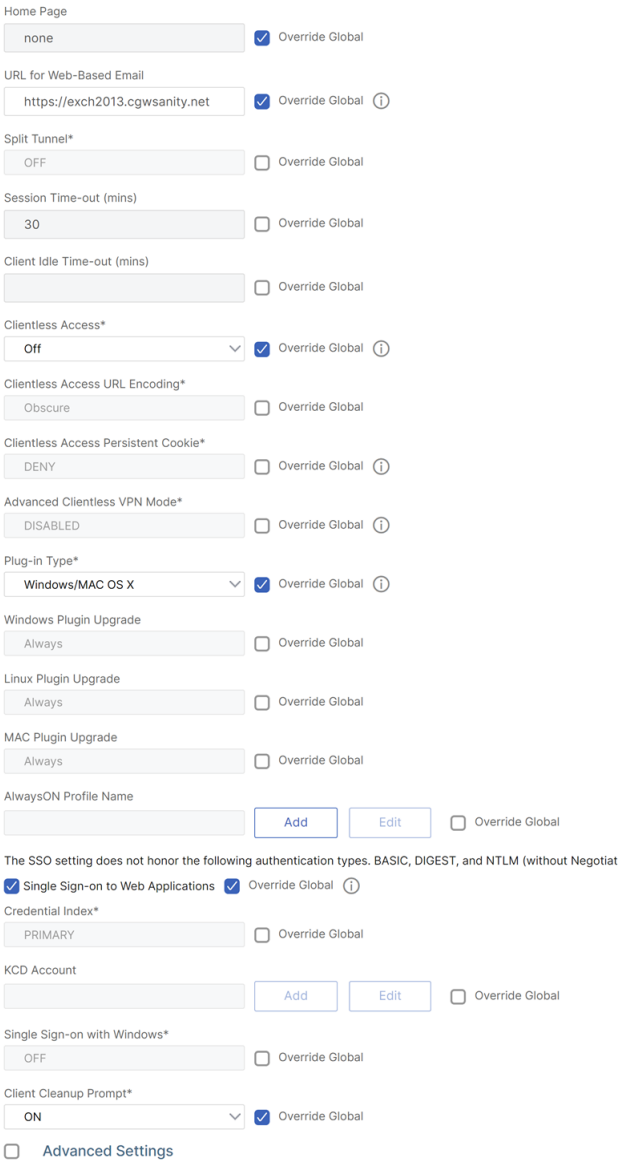
在 **NetScaler Gateway** 设备上配置完整的 **VPN** 设置

要在 NetScaler Gateway 设备上配置 VPN 设置，请完成以下过程：

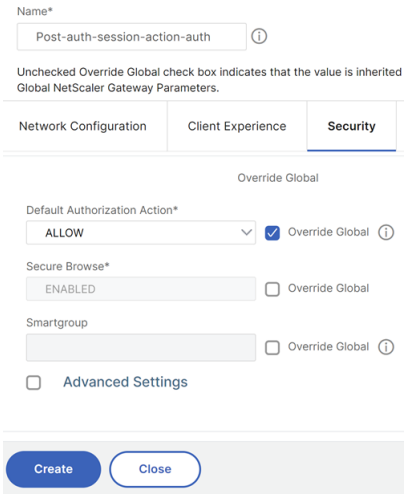
1. 导航到“流量管理”**>**“**DNS**”。
2. 选择“名称服务器”节点，如以下屏幕截图所示。确保已列出 DNS 名称服务器。如果不可用，请添加 DNS 名称服务器。

3. 展开 **NetScaler Gateway >** 策略。
4. 选择“会 话”节点。
5. 在 NetScaler Gateway 会话策略和配置文件页面中，单击 配置文件 选项卡，单击 添加。
   对于在“配置 NetScaler Gateway 会话配置文件”对话框中配置的每个组件，请确保为相应组件选择“覆盖全局”选项。

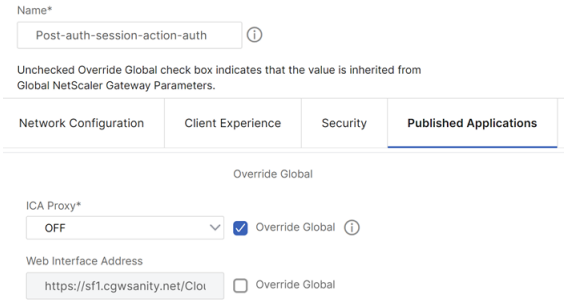
6. 单击“客户端体验”选项卡。
7. 如果您想在用户登录 VPN 时显示任何 URL，请在主页字段中键入 Intranet 门户 URL。如果主页参数设置为“nohomepage.html”，则不会显示主页。插件启动时，浏览器实例启动并自动终止。
8. 确保从拆分通道列表中选择所需的设置。
9. 如果您想要 FullVPN，请从 无客户端访问 列表中选择 关 闭。
10. 确保从 插件类型 列表中选择了 **Windows/Mac OS X** 。
11. 如果需要，请选择 单点登录到 **Web** 应用程序 选项。
12. 如有必要，请确保选择“客户端清理提示符”选项，如以下屏幕截图所示：



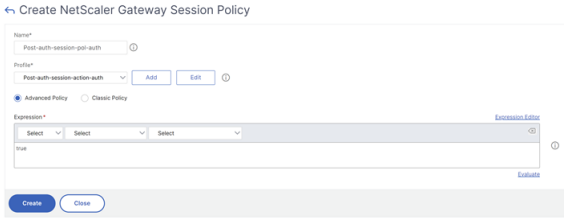
13. 单击安全选项卡。
14. 确保从“默认授权操 作”列表中选择了“允许”，如以下屏幕截图所示：



15. 单击 **Published Applications**（已发布的应用程序）选项卡。
16. 确保从“已发布的应用程序”选项下的 **ICA** 代理 列表中选择 了 OFF。

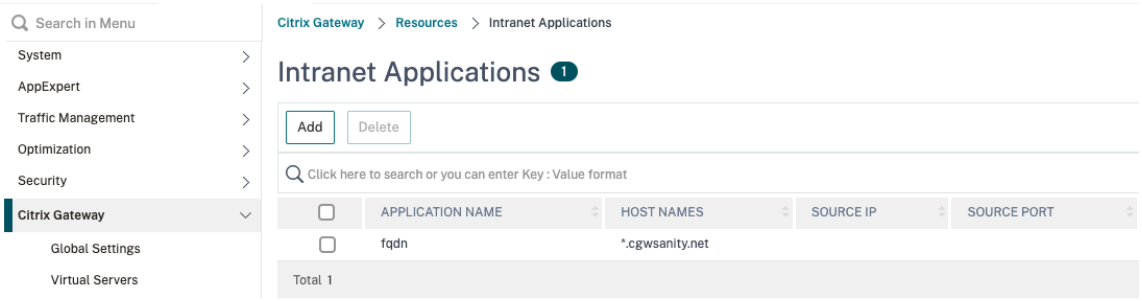


17. 单击创建。
18. 单击关闭。
19. 单击虚拟服务器中 **NetScaler Gateway** 会话策略和配置文件页面的策略选项卡，或根据需要在组/用户级别激活会话策略。
20. 使用必填表达式或 true 创建会话策略，如以下屏幕截图所示：



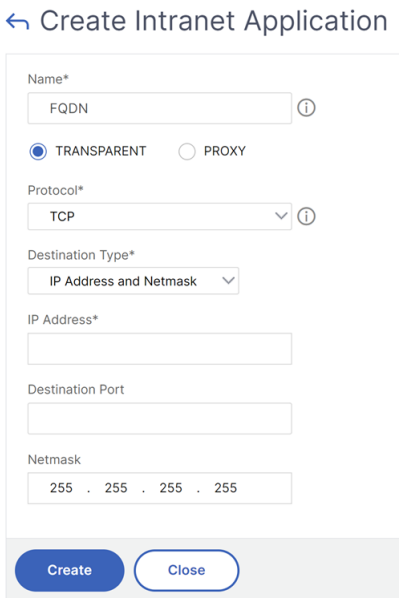
21. 将会话策略绑定到 VPN 虚拟服务器。有关详情，请参阅 绑定会话策略。

    如果将拆分通道配置为开，则必须配置希望用户在连接到 VPN 时访问的 Intranet 应用程序。有关内联网应用程序的详细信息，请参阅为 Citrix Secure Access 客户端配置内联网应用程序。



a) 转到 **NetScaler Gateway >** 资源 **>** 内联网应用程序。

b) 创建一个 Intranet 应用程序。为带 Windows 客户端的 FullVPN 选择“透明”。选择要允许的协议（TCP、UDP 或 ANY）、目标类型（IP 地址和掩码、IP 地址范围或主机名）。



c) 如有必要，使用以下表达式为 iOS 和 Android 上的 VPN 设置新策略：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.
REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.
HEADER("User-Agent").CONTAINS("Android")
```

d) 根据需要绑定在 USER/GROUP/VSERVER 级别创建的 Intranet 应用程序。

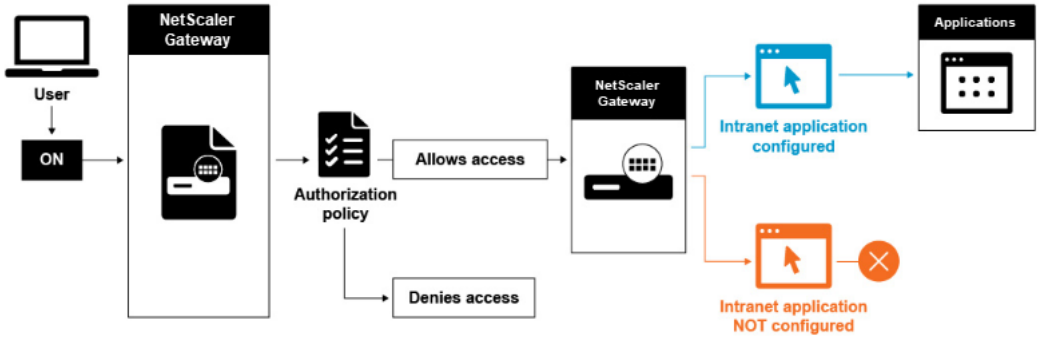
配置拆分通道

1. 导航到配置 > **NetScaler Gateway >** 策略 **>** 会话。
2. 在详细信息窗格的配置文件选项卡上，选择一个配置文件，然后单击 编辑。
3. 在“客户端体验”选项卡上的“拆分通道”旁边，选择“全局覆盖”，选择一个选项，然后单击“确定”。

配置拆分通道和授权

规划 NetScaler Gateway 部署时，请务必考虑拆分通道以及默认授权操作和授权策略。

例如，您有一个允许访问网络资源的授权策略。您已将拆分通道设置为开，并且未将 Intranet 应用程序配置为通过 NetScaler Gateway 发送网络流量。当 NetScaler Gateway 具有此类配置时，允许访问资源，但用户无法访问该资源。



如果授权策略拒绝访问网络资源，Citrix Secure Access 客户端会向 NetScaler Gateway 发送流量，但在以下情况下访问该资源会被拒绝。

- 您已将拆分通道设置为开。
- Intranet 应用程序配置为通过 NetScaler Gateway 路由网络流量

有关授权策略的详细信息，请查看以下内容：

- 配置授权
- 配置授权策略
- 设置默认全局授权

配置对内部网络资源的网络访问

1. 导航到 配置 > **NetScaler Gateway >** 资源 **> Intranet** 应用程序。
2. 在详细信息窗格中，单击“添加”。
3. 填写允许网络访问的参数，单击 创建，然后单击 关闭。

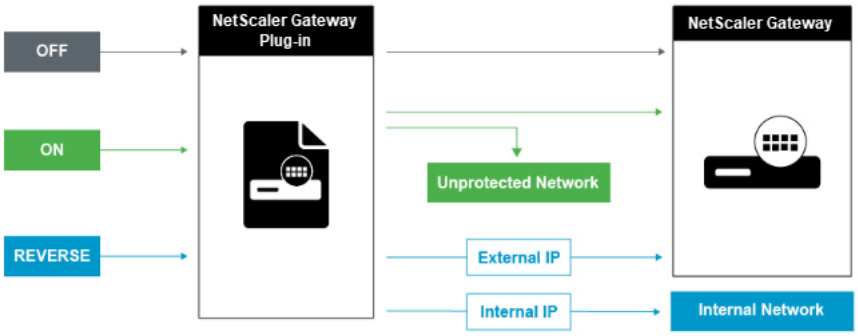
当我们没有为 VPN 用户设置内部网 IP 时，用户会将流量发送到 NetScaler Gateway VIP，然后 NetScaler 设备从那里构建一个新的数据包到内部局域网上的 Intranet 应用程序资源。这个新的数据包将从 SNIP 发送到 Intranet 应用程序。从这里，Intranet 应用程序获取数据包，对其进行处理，然后尝试回复该数据包的来源（本例中为 SNIP）。SNIP 获取数据包并将回复发送给发出请求的客户端。

使用 Intranet IP 地址时，用户会将流量发送到 NetScaler Gateway VIP，然后 NetScaler 设备将从那里将客户端 IP 映射到池中配置的内部网 IP 之一。请注意，NetScaler 设备将拥有 Intranet IP 池，因此不得在内部网络中使用这些范围。NetScaler 设备会像 DHCP 服务器一样为传入的 VPN 连接分配内部网 IP。NetScaler 设备为用户将要访问的局域网上的内联网应用程序构建一个新数据包。这个新的数据包将从 Intranet IP 之一发往 Intranet 应用程序。从这

里，Intranet 应用程序获取数据包，对其进行处理，然后尝试回复该数据包的来源（INTRANET IP）。在这种情况下，需要将回复数据包路由回内部网 IP 所在的 NetScaler 设备（请记住，NetScaler 设备拥有 Intranet IP 子网）。要完成此任务，网络管理员必须有指向 INTRANET IP 的路由，指向其中一个剪辑。建议将流量指向 SNIP，该 SNIP 保存数据包首次离开 NetScaler 设备的路由，以避免任何非对称流量。

分割通道选项

以下是各种分割通道选项。



拆分通道关闭

当分割通道设置为关闭时，Citrix Secure Access 客户端会捕获来自用户设备的所有网络流量，并将流量通过 VPN 通道发送到 NetScaler Gateway。换句话说，VPN 客户端会建立从客户端 PC 到 NetScaler Gateway VIP 的默认路由，这意味着所有流量都需要通过通道发送才能到达目的地。由于所有流量都将通过通道发送，因此授权策略必须确定是允许流量传递到内部网络资源还是被拒绝。

设置为“关闭”时，所有流量都将通过通道，包括到达网站的标准 Web 流量。如果目标是监视和控制此 Web 流量，则必须使用 NetScaler 设备将这些请求转发到外部代理。用户设备也可以通过代理服务器进行连接以访问内部网络。NetScaler Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要为用户连接启用代理支持，必须在 NetScaler Gateway 上指定这些设置。您可以指定 NetScaler Gateway 上的代理服务器使用的 IP 地址和端口。代理服务器用作所有与内部网络的进一步连接的转发代理。

有关更多信息，请查看以下链接：

- 为用户连接启用代理支持

拆分通道打开

您可以启用分割通道以防止 Citrix Secure Access 客户端向 NetScaler Gateway 发送不必要的网络流量。如果启用分割通道，Citrix Secure Access 客户端仅通过 VPN 通道发送发往受 NetScaler Gateway 保护的网络（内联网应用程序）的流量。Citrix Secure Access 客户端不会将发往未受保护网络的网络流量发送到 NetScaler Gateway。当 Citrix Secure Access 客户端启动时，它会从 NetScaler Gateway 获取内联网应用程序列表，并为客户端 PC 的内

联网应用程序选项卡上定义的每个子网建立路由。Citrix Secure Access 客户端检查从用户设备传输的所有数据包，并将数据包中的地址与 Intranet 应用程序列表（启动 VPN 连接时创建的路由表）进行比较。如果数据包中的目标地址在其中一个内联网应用程序内，Citrix Secure Access 客户端将数据包通过 VPN 通道发送到 NetScaler Gateway。如果目标地址不在定义的 Intranet 应用程序中，则不会对数据包进行加密，然后用户设备会使用最初在客户端 PC 上定义的默认路由来适当地路由数据包。“启用拆分通道时，Intranet 应用程序将定义被拦截并通过通道发送的网络流量”。

反向拆分通道

NetScaler Gateway 还支持反向拆分通道，该通道定义 NetScaler Gateway 不会拦截的网络流量。如果将拆分通道设置为反向，则 Intranet 应用程序将定义 NetScaler Gateway 不会拦截的网络流量。启用反向剥离通道时，定向到内部 IP 地址的所有网络流量都会绕过 VPN 通道，而其他流量则通过 NetScaler Gateway。反向拆分通道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无线网络并使用 Citrix Secure Access 客户端登录，则 NetScaler Gateway 不会拦截发往打印机或无线网络中其他设备的网络流量。

> 注意：
>
> 适用于 Windows 的 Citrix Secure Access 客户端还支持来自 Citrix Secure Access 版本 22.6.1.5 及更高版本的基于 FQDN 的反向分割通道。

注意事项　基于 **IP** 的反向分割通道：

- 基于 IP 地址的规则数量限制为 1024。
- DNE 和 WFP 司机均提供支持。

基于主机名的反向分割通道：

- 在 VPN 会话期间可以访问的主机名数量受到 FQDN 欺骗范围内指定的可用 IP 地址数量的限制。这是因为每个主机名都占用 FQDN 欺骗范围中的一个 IP 地址。IP 范围用尽后，将最近分配的最少的 IP 地址重新用于下一个新主机名。
- 必须配置 DNS 后缀。

  > 注意：
  >
  > 对于 Windows 客户端，只有 WFP 驱动程序支持基于主机名的反向分割通道。将“EnableWFP”注册表值设置为 1，启用 WFP 驱动程序模式。有关更多信息，请参阅使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端。

基于 **IP** 和基于主机名的反向分割通道：

- 仅支持 WFP 驱动程序。基于 IP 的反向拆分通道和基于主机名的反向拆分通道中提到的所有其他准则均适用。

配置名称服务解析

在安装 NetScaler Gateway 期间，您可以使用 NetScaler Gateway 向导配置其他设置，包括名称服务提供商。域名服务提供商会将完全限定的域名 (FQDN) 转换为 IP 地址。在 NetScaler Gateway 向导中，您还可以执行以下操作：

- 配置 DNS 或 WINS 服务器
- 设置 DNS 查找的优先级
- 设置重试连接到服务器的次数。

运行 NetScaler Gateway 向导时，可以添加 DNS 服务器。您可以使用会话配置文件将其他 DNS 服务器和 WINS 服务器添加到 NetScaler Gateway。然后，您可以指示用户和组连接到与最初使用向导配置的名称解析服务器不同的名称解析服务器。

在 NetScaler Gateway 上配置另一台 DNS 服务器之前，请创建一个虚拟服务器，用作 DNS 服务器以进行名称解析。

在会话配置文件中添加 DNS 或 WINS 服务器

1. 在配置实用程序中，配置选项卡 > **NetScaler Gateway >** 策略 **>** 会话。
2. 在详细信息窗格的 配置文件 选项卡上，选择一个配置文件，然后单击 打开。
3. 在“网络配置”选项卡上，执行以下操作之一：
    - 要配置 DNS 服务器，请在 **DNS** 虚拟服务器旁边，单击“覆盖全局”，选择服务器，然后单击“确定”。
    - 要配置 WINS 服务器，请在 **WINS** 服务器 **IP** 旁边，单击“覆盖全局”，键入 IP 地址，然后单击“确定”。

引用

- 拆分通道
- 用户如何连接 Citrix Secure Access 客户端
- 关于 NetScaler Gateway
- 选择用户访问方法

选择用户访问方法

February 1, 2024

您可以将 NetScaler Gateway 配置为通过以下方案提供用户连接：

- 使用 Citrix Workspace 应用程序的用户连接。Citrix Workspace 应用程序与 StoreFront 或 Web Interface 兼容，为用户提供对服务器场中已发布的应用程序或虚拟桌面的访问权限。Citrix Workspace 应用程序是使用 ICA 网络协议建立用户连接的软件。用户在用户设备上安装 Citrix Workspace 应用程序。当用户在基于

Windows 或基于 Mac 的计算机上安装 Citrix Workspace 应用程序时，Citrix Workspace 应用程序会包含所有插件，包括用于用户连接的 Citrix Secure Access 客户端。NetScaler Gateway 还支持来自适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 的 Citrix Workspace 用户可以通过 Citrix Endpoint Management、StoreFront 或 Web Interface 连接到其虚拟桌面以及基于 Windows 的 Web、移动和 SaaS 应用程序。

- 用户与 Secure Hub 的连接。用户可以连接到 Endpoint Management 中配置的移动、Web 和 SaaS 应用程序。用户在他们的移动设备（Android 或 iOS）上安装 Secure Hub。当用户登录 Secure Hub 时，他们可以安装 WorxMail 和 WorxWeb 以及您在 Endpoint Management 中安装的任何其他移动应用程序。Secure Hub、Secure Mail 和 WorxWeb 使用 Micro VPN 技术通过 NetScaler Gateway 建立连接。
- 使用 Citrix Secure Access 客户端作为独立应用程序进行用户连接。Citrix Secure Access 客户端是用户可以下载并安装在用户设备上的软件。当用户使用插件登录时，用户可以像在办公室一样访问安全网络中的资源。资源包括电子邮件服务器、文件共享和 Intranet 网站。
- 使用无客户端访问进行用户连接。无客户端访问为用户提供所需的访问权限，无需在用户设备上安装软件，例如 Citrix Secure Access 客户端或 Citrix Workspace 应用程序。无客户端访问允许通过访问界面连接到一组有限的 Web 资源，例如 Outlook Web Access 或 SharePoint、Citrix Virtual Apps 上发布的应用程序、Citrix Virtual Apps and Desktops 中的虚拟桌面以及安全网络中的文件共享。用户可以通过在 Web 浏览器中输入 NetScaler Gateway Web 地址进行连接，然后从选择页面中选择无客户端访问。
- 预身份验证或身份验证后扫描失败时的用户连接。这种情况称为访问方案回退。如果用户设备未通过初始端点分析扫描，则访问场景回退允许用户设备使用 Citrix Workspace 应用程序从 Citrix Secure Access 客户端回退到 StoreFront 或 Web Interface。

  如果用户通过 Citrix Workspace 应用程序登录 NetScaler Gateway，则预身份验证扫描将不起作用。NetScaler Gateway 建立 VPN 通道时，身份验证后扫描确实有效。

用户可以使用以下方法下载和安装 Citrix Secure Access 客户端：

- 使用网络浏览器连接到 NetScaler Gateway。
- 连接到配置为接受 NetScaler Gateway 连接的 StoreFront。
- 使用组策略对象 (GPO) 安装插件。
- 将 NetScaler 插件上载到推销服务器。

部署 **Citrix Secure Access** 客户端以供用户访问

February 1, 2024

NetScaler Gateway 附带以下用于用户访问的插件：

- 适用于 Windows 的 Citrix Secure Access 客户端
- 适用于 Mac 的 Citrix Secure Access 客户端

当用户首次登录 NetScaler Gateway 时，他们会从网页下载并安装 Citrix Secure Access 客户端。用户可以通过在基于 Windows 的计算机上单击通知区域中的 NetScaler Gateway 图标来登录。在 macOS X 计算机上，用户可以从 **Dock** 或应用程序 菜单登录。如果您将 NetScaler Gateway 升级到新的软件版本，Citrix Secure Access 客户端会在用户设备上自动更新。

使用 **MSI** 安装程序包部署 **Citrix Secure Access** 客户端

您可以使用 Microsoft Active Directory 基础架构或标准的第三方 MSI 部署工具（例如 Windows Server 更新服务）来部署 Citrix Secure Access 客户端。如果使用支持 Windows 安装程序包的工具，则可以使用任何支持 MSI 文件的工具部署软件包。然后，您可以使用部署工具在适当的用户设备上部署和安装软件。

使用集中式部署工具的优势

- 能够遵循安全要求。例如，您可以在不为非管理员用户启用软件安装权限的情况下安装用户软件。
- 控制软件版本。您可以同时向所有用户部署软件的更新版本。
- 可扩展性。集中式部署策略可轻松扩展以支持更多用户。
- 积极的用户体验。您可以部署、测试和解决与安装相关的问题，而无需用户参与此过程。

当首选对用户软件安装进行管理控制并且可以随时访问用户设备时，Citrix 建议使用此选项。

有关更多信息，请参阅从 Active Directory 部署 Citrix Secure Access 客户端。

确定要部署哪个软件插件

如果 NetScaler Gateway 部署不需要在用户设备上使用任何软件插件，则将您的部署视为提供无客户端访问。在这种情况下，用户只需要 Web 浏览器即可访问网络资源。但是，某些功能需要用户设备上的插件软件。

为用户选择 **Citrix Secure Access** 客户端

February 1, 2024

配置 NetScaler Gateway 时，可以选择用户的登录方式。用户可以使用以下插件之一登录：

- 适用于 Windows 的 Citrix Secure Access 客户端
- 适用于 macOS 的 Citrix Secure Access 客户端

通过创建会话策略，然后将策略绑定到用户、组或虚拟服务器来完成配置。您还可以通过配置全局设置来启用插件。在全局配置文件或会话配置文件中，您可以选择 Windows 或 macOS X 作为插件类型。当用户登录时，他们会收到全局或会话配置文件和策略中定义的插件。为插件类型创建单独的配置文件。

全局配置插件

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“客户端体验”选项卡上的“插件类型”旁边，选择 Windows/macOS X，然后单击“确定”。

在会话配置文件中为 **Windows** 或 **macOS** 配置插件类型

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 执行以下操作之一：
   - 如果要创建会话策略，请在详细信息窗格中单击 添加。
   - 如果要更改现有策略，请选择一个策略，然后单击“打开”。
3. 创建配置文件或修改现有配置文件。为此，请执行以下操作之一：
   - 在“请求配置文件”旁边，单击“新建”。
   - 在“请求配置文件”旁边，单击“修改”。
4. 在“客户端体验”选项卡上的“插件类型”旁边，单击“覆盖全局”，然后选择 **Windows/macOS X**。
5. 执行以下操作之一：
   - 如果要创建配置文件，请单击“创建”，在策略对话框中设置表达式，单击“创建”，然后单击“关闭”。
   - 如果您正在修改现有配置文件，则在进行选择后，请两次单击“确定”。

适用于 **Windows** 的 **Citrix Secure Access** 客户端

当用户登录 NetScaler Gateway 时，他们会在用户设备上下载并安装 Citrix Secure Access 客户端。

要安装插件，用户必须是本地管理员或管理员组的成员。此限制仅适用于首次安装。插件升级不需要管理员级别的访问权限。

要使用户能够连接和使用 NetScaler Gateway，您需要向他们提供以下信息：

- NetScaler Gateway Web 地址，例如 https://NetScalerGatewayFQDN/
- 如果您配置了端点资源和策略，则运行 Citrix Secure Access 客户端的任何系统要求

根据用户设备的配置，您可能还需要提供以下信息：

- 如果用户在其计算机上运行防火墙，他们必须更改防火墙设置，这样防火墙就不会阻止流入或来自与您授予访问权限的资源对应的 IP 地址的流量。Citrix Secure Access 客户端自动处理 Windows XP 中的 Internet 连接防火墙和 Windows XP Service Pack 2、Windows Vista、Windows 7、Windows 8 或 Windows 8.1 中的 Windows XP 和 Windows 防火墙。
- 想要通过 NetScaler Gateway 连接向 FTP 发送流量的用户必须将其 FTP 应用程序设置为执行被动传输。被动传输意味着远程计算机建立与 FTP 服务器的数据连接，而不是 FTP 服务器与远程计算机建立数据连接。

- 想要通过连接运行 X 客户端应用程序的用户必须在其计算机上运行 X 服务器 XManager，例如。
- 安装适用于 Windows 的 Receiver 或 Mac 版 Receiver 的用户可以从 Receiver 或使用网络浏览器启动 Citrix Secure Access 客户端。向用户提供有关如何通过 Receiver 或 Web 浏览器登录 Citrix Secure Access 客户端的说明。

由于用户在处理文件和应用程序时就好像他们是组织网络的本地用户一样，因此您无需重新培训用户或配置应用程序。

要首次建立安全连接，请使用 Web 登录页面登录 NetScaler Gateway。Web 地址的典型格式是 https://companyname.com。当用户登录时，他们可以在自己的计算机上下载并安装 Citrix Secure Access 客户端。

安装适用于 **Windows** 的 **Citrix Secure Access** 客户端

1. 在 Web 浏览器中，键入 NetScaler Gateway 的 Web 地址。
2. 键入用户名和密码，然后单击“登录”。
3. 选择网络访问，然后单击下载。
4. 按照说明安装插件。

下载完成后，Citrix Secure Access 客户端将连接并在基于 Windows 的计算机的通知区域中显示一条消息。

如果您希望用户在不使用 Web 浏览器的情况下连接 Citrix Secure Access 客户端，则可以将插件配置为在用户右键单击 Windows 计算机通知区域中的 **NetScaler Gateway** 图标时显示登录对话框，或者从“开始”菜单启动插件。

为适用于 **Windows** 的 **Citrix Secure Access** 客户端配置登录对话框

要将 Citrix Secure Access 客户端配置为使用登录对话框，用户必须登录才能完成此过程。

1. 在基于 Windows 的计算机上，在通知区域中，右键单击 NetScaler Gateway 图标，然后单击配置 NetScaler Gateway。
2. 单击配置文件选项卡，然后单击更改配置文件
3. 在“选项”选项卡上，单击“使用 Citrix Secure Access 客户端登录”。
   注意：如果用户从 Receiver 中打开“
   配置 NetScaler Gateway”对话框，则“
   选项”选项卡不可用。

为适用于 **Windows** 的 **Citrix Secure Access** 客户端设置拦截模式

如果您正在为 Windows 配置 Citrix Secure Access 客户端，则还需要配置拦截模式并将其设置为透明。

1. 在配置实用程序中，单击配置选项卡，展开 **NetScaler Gateway >** 资源，然后单击 **Intranet** 应用程序。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。

4. 单击“透明”。
5. 在 协议中，选择 任何。
6. 在目标类型中，选择 **IP** 地址和网络掩码。
7. 在 **IP** 地址 中键入 IP 地址。
8. 在 **Netmask** 中，键入子网掩码，单击 创建，然后单击 关闭。

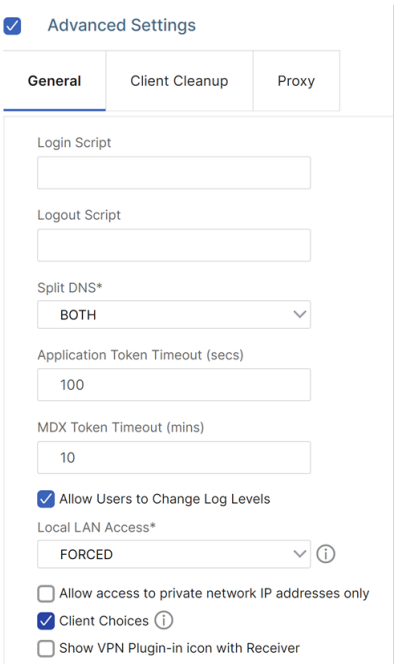
根据 **ADC** 配置对最终用户实施本地 **LAN** 访问

管理员可以限制最终用户在其客户端计算机上禁用本地局域网访问选项。一个新选项“强制”将添加到现有的“本地局域网访问”参数值中。当本地局域网访问值设置为 FORCED 时，客户端计算机上始终为最终用户启用本地局域网访问。最终用户无法使用 Citrix Secure Access 客户端用户界面禁用本地局域网设置。

通过将本地 LAN 访问参数设置为 ON，管理员可以让最终用户访问其客户端计算机上的本地 LAN 资源。要阻止最终用户访问其客户端计算机上的本地 LAN 资源，管理员可以将本地 LAN 访问参数设置为 OFF。有关最终用户配置的详细信息，请参阅 macOS 的本地局域网访问和 iOS 的本地局域网访问。

要使用 **GUI** 启用 **Forced** 选项，请执行以下操作：

1. 导航到 **NetScaler Gateway >** 全局设置 **>** 更改全局设置。
2. 单击“客户端体验”选项卡，然后单击“高级设置”。
3. 在 本地局域网访问中，选择 强制。



要使用 **CLI** 启用 **Forced** 选项，请运行以下命令：

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```


> 备注：
>
> - 适用于 macOS/iOS 的 Citrix Secure Access 客户端及更高版本支持 NetScaler Gateway 的本地局域网访问功能。
> - 从适用于 Windows 的 Citrix Secure Access 客户端 23.10.1.7 开始，如果在 NetScaler Gateway 上将“本地局域网访问”参数设置为“强制”，则计算机级通道支持本地局域网接入。

Microsoft Edge WebView 对 Windows Citrix Secure Access 的支持 - 预览版

Microsoft Edge WebView 对 Windows Citrix Secure Access 的支持引入了增强的最终用户体验。有关详细信息，请参阅 Microsoft Edge WebView 对 Windows Citrix Secure Access 的支持

使用 Windows 筛选平台的 Windows Citrix Secure Access 客户端

Windows 筛选平台 (WFP) 是一组 API 和系统服务，提供用于创建网络过滤应用程序的平台。WFP 旨在取代以前的包过滤技术，即与 DNE 驱动程序一起使用的网络驱动程序接口规范 (NDIS) 过滤器。Windows Citrix Secure Access 客户端的 22.6.1.5 版本支持 WFP 模式。

安装 WFP 版本

您可以使用以下方法之一安装 WFP 版本。

- 使用 DNE 和 WFP 驱动程序安装 VPN 插件（默认方法）

  当插件安装了 DNE 和 WFP 驱动程序时，管理员可以通过注册表旋钮使用 WFP 或 DNE 驱动程序进行通道传输。默认情况下，DNE 驱动程序用于通道。

- 仅使用 WFP 驱动程序安装 VPN 插件（跳过 DNE 驱动程序安装）

  某些第三方应用程序不支持 DNE 驱动程序，即使未使用。对于这些部署，管理员可以使用此安装类型。由于未安装 DNE 驱动程序，因此只使用 WFP 驱动程序进行通道开发。

选择 WFP 驱动程序而不是 DNE 驱动程序

执行以下步骤以选择 WFP 驱动程序而不是 DNE 驱动程序。

> 注意：
>
> 这仅适用于默认安装方法。

1. 下载 WFP 支持的 VPN 插件版本并安装新的 VPN 插件。
2. 默认情况下，DNE 驱动程序用于通过通道传输流量。要使用 WFP 驱动程序进行通道传输，管理员必须创建以下注册表项：

- REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
  - REG_TYPE - REG_DWORD
  - REG_NAME - EnableWFP
  - REG_VALUE —将值设置为 1 以使用 WFP，将 0 设置为 DNE（如果此注册表值不存在或设置为 0，则默认启用 DNE）

> 注意：
>
> 将通道模式从 DNE 切换到 WFP 后，或者相反，必须重新启动系统才能使更改正确生效。

完全跳过 **DNE** 安装

执行以下步骤可跳过 DNE 安装。

1. 执行 VPN 插件的全新卸载。

   a) 卸载计算机上的当前 VPN 插件并重新启动计算机。

   b) 使用以下任一选项检查 DNE 驱动程序是否已卸载。

   - 打开提升的命令提示符（或 PowerShell)。运行以下命令（示例输出显示系统上安装了基于 DNE 的驱动程序）

```
PS C:\Users\Administrator> sc qc cag
[SC] QueryServiceConfig SUCCESS
SERVICE_NAME: cag
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 2   AUTO_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : ??\C:\Program Files\Common Files\
    Deterministic Networks\Common Files\cag.sys
LOAD_ORDER_GROUP   :
TAG                : 0
DISPLAY_NAME       : Citrix cag plugin for Access Gateway
DEPENDENCIES       :
SERVICE_START_NAME :
PS C:\Users\Administrator> sc qc dne
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dne
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 1   SYSTEM_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys
LOAD_ORDER_GROUP   : NDIS
TAG                : 38
DISPLAY_NAME       : DNE LightWeight Filter
DEPENDENCIES       :
SERVICE_START_NAME :
<!--NeedCopy-->
```


如果未安装驱动程序，则会显示以下输出：

```
The specified service does not exist as an installed service.
```

由于其他供应商也使用 DNE 驱动程序 (dnelwf64.sys)，因此即使系统上未安装 Citrix Secure Access 客户端，它也可能存在。另一方面，CAG 插件仅由 Citrix Secure Access 客户端使用。

- 也可以通过尝试启动 CAG 和 DNE 驱动程序来检查 DNE 的存在。使用管理员权限打开命令提示符并运行以下命令：

```
net start cag
net start dne
<!--NeedCopy-->
```

  - 如果输出消息指示无法找到服务（服务名称无效。），则插件和驱动程序组件已成功卸载。在这种情况下，请移至步骤 2。
  - 如果未成功卸载插件和驱动程序组件，请按照 https://citrix.sharefile.com/d-s829800c3821a4a8f869ad324de6f0332 中提供的说明在客户端计算机上运行清理实用程序。
    * 解压清理实用程序并将其复制到文件夹。
    * 在命令提示符下运行 nsRmSAC.exe。
    * 重新启动客户端计算机。

2. 创建以下注册表项。

   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - SkipDNE
     - REG_VALUE-设置为 1 可确保计算机上未安装 DNE
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE-设置为 1 以启用 WFP（如果跳过 DNE 安装，则必须创建此条目）

   > 注意：
   >
   > - 如果在安装之前未创建注册表项，则默认情况下会安装 DNE。此外，您可以检查 VPN 日志文件以验证是否使用了 WFP 或 DNE。
   > - 如果跳过 DNE 安装，则必须将 EnableWFP 设置为 1。在这种情况下，如果不重新安装 Citrix Secure Access 客户端，就无法切换到基于 DNE 的插件。

3. 安装新的 VPN 插件。

4. 确认系统上是否安装了 WFP 驱动程序。打开提升的命令提示符并运行以下命令。示例输出显示系统上安装了 WFP 驱动程序。


```
PS C:\Users\Administrator> sc qc ctxsgwcallout
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ctxsgwcallout
    TYPE               : 1  KERNEL_DRIVER
    START_TYPE         : 1   SYSTEM_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : ??\C:\Program Files\Citrix\Secure Access
       Client\ctxsgwcallout.sys
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Citrix Secure Access Callout Driver
    DEPENDENCIES       :
    SERVICE_START_NAME :
<!--NeedCopy-->
```

如果未安装驱动程序，则会显示以下输出：

```
The specified service does not exist as an installed service.
```

1. 重新启动客户端计算机。

WFP 的优势

以下是如果在客户端上安装独立的 WFP 驱动程序，WFP 的一些优势在于。

- 基于 **FQDN** 的反向拆分通道支持： WFP 驱动程序支持基于 FQDN 的反向拆分通道。DNE 驱动程序不支持此功能。有关更多详细信息，请参阅 拆分通道选项。
- **Wireshark** 支持： DNE 不允许在客户端计算机上捕获双向流量，因为它与以太网/Wi-Fi 适配器链接。对于新的 WFP 驱动程序来说，这不是问题。任何流量捕获（单向或双向）都经过加密，并且需要 SSL 密钥才能对其进行解密。
- **NMAP** 支持：新的 WFP 驱动程序支持 NMAP 扫描，而 VPN 插件用于通道传送流量，而 DNE 不允许 NMAP 扫描，而 VPN 插件则用于对流量进行通道传输。
- 网络速度：在某些情况下，如果在客户端计算机上安装了 DNE，则下载和上载速度会受到影响，而 WFP 的情况并非如此。
- 提高了 **nslookup** 性能：有时使用 DNE 时，尝试次数较少时 `nslookup` 无法响应，而 WFP 则没有观察到同样的情况。
- 与 **UDP** 相比提高了 **iperf** 性能：使用 DNE，在使用 iperf over UDP 进行可扩展性测试时观察到一些数据包丢失。WFP 没有发现数据包丢失。

从 **Active Directory** 部署 **Citrix Secure Access** 客户端

February 1, 2024

如果用户没有在用户设备上安装 Citrix Secure Access 客户端的管理权限，则可以从 Active Directory 为用户部署插件。使用此方法部署 Citrix Secure Access 客户端时，可以提取安装程序，然后使用组策略部署该程序。这种类型的部署的一般步骤是：

- 正在提取 MSI 软件包。
- 使用组策略分发插件。
- 创建分发点。
- 使用组策略对象分配 Citrix Secure Access 客户端包。

  注意：只有 Windows 7、Windows 8 和 Windows 10 支持从 Active Directory 分发 Citrix Secure Access 客户端。

您可以从配置实用程序或 Citrix 网站下载 MSI 软件包。

从配置实用程序下载 **Citrix Secure Access** 客户端 **MSI** 软件包

1. 在配置实用程序中，单击 下载。
2. 在 Citrix Secure Access 客户端下，单击下载适用于 **Windows** 的 **NetScaler Gateway** 插件，然后将 **nsvpnc_setup.exe** 文件保存到您的 Windows 服务器。

   注意：

   - 对于 64 位计算机，必须将文件 Agee_setup.exe 保存到 Windows 服务器中。
   - 如果未出现“文件下载”对话框，请在单击“下载适用于 **Windows** 的 **Citrix Secure Access** 客户端”链接时按 Ctrl 键。
3. 在命令提示符处，导航到保存 **nsvpnc_setup.exe** 的目标文件夹，然后键入：

   ```
   nsvpnc_setup /c
   <!--NeedCopy-->
   ```

   这将提取文件 agee.msi。

   注意：对于 64 位计算机，导航到保存 **Agee_setup.exe** 的目标文件夹，然后键入：

   ```
   Agee_setup.exe /c
   <!--NeedCopy-->
   ```

   这将提取文件 agee64.msi。

4. 将提取的文件保存到 Windows 服务器上的文件夹中。

解压缩文件后，使用 Windows Server 上的组策略分发文件。

在开始分发之前，请在 Windows Server 2003、Windows Server 2008 或 Windows Server 2012 上安装组策略管理控制台。有关详细信息，请参阅 Windows 联机帮助。

注意：当您使用组策略发布 Citrix Secure Access 客户端时，Citrix 建议将软件包分配给用户设备。MSI 软件包是基于每台设备安装的。

在分发软件之前，请在发布服务器上的网络共享上创建分发点，例如 Microsoft Internet 安全和加速 (ISA) 服务器。

创建分发点

1. 以管理员身份登录到发布服务器。
2. 创建一个文件夹并在网络上共享该文件夹，对需要访问分发包的所有帐户具有读取权限。
3. 在命令提示符下，导航到保存提取文件的文件夹，然后键入：msiexec-a agee.msi
4. 在“网络位置”屏幕上，单击“更改”，然后导航到要在其中创建 Citrix Secure Access 客户端管理安装的共享文件夹。
5. 单击 确定，然后单击 安装。

将解压缩的软件包放到网络共享上后，将该软件包分配给 Windows 中的组策略对象。

成功将 Citrix Secure Access 客户端配置为托管软件包后，该插件将在用户设备下次启动时自动安装。

> 注意：将安装包分配给计算机后，用户必须重新启动计算机。

安装开始时，用户会收到一条消息，表明 Citrix Secure Access 客户端正在安装。

使用 **Active Directory** 管理 **Citrix Secure Access** 客户端

February 1, 2024

Citrix Secure Access 客户端的每个版本都打包为完整的产品安装，而不是补丁。当用户登录且 Citrix Secure Access 客户端检测到插件的新版本时，插件会自动升级。您也可以部署 Citrix Secure Access 客户端，使用 Active Directory 进行升级。

为此，请为 Citrix Secure Access 客户端创建分发点。创建组策略对象并为其分配新版本的插件。然后，在新软件包和现有软件包之间创建一个链接。创建链接后，Citrix Secure Access 客户端将更新。

从用户设备上删除 **Citrix Secure Access** 客户端

要从用户设备上删除 Citrix Secure Access 客户端，请从组策略对象编辑器中删除分配的软件包。

从用户设备中删除插件后，用户会收到一条消息，提示该插件正在卸载。

使用 **Active Directory** 对 **Citrix Secure Access** 客户端安装进行故障排除

如果在用户设备启动时无法安装分配的软件包，则可能会在应用程序事件日志中看到以下警告：

无法将更改应用到软件安装设置。由于管理员已启用组策略的登录优化，软件安装策略应用程序已延迟到下次登录。错误是：组策略框架必须在同步前台策略刷新中调用扩展程序。

此错误是由 Windows XP 中的快速登录优化引起的，其中允许用户在操作系统初始化所有网络组件（包括组策略对象处理）之前登录。某些策略可能需要多次重启才能生效。要解决此问题，请在 Active Directory 中禁用快速登录优化。

要解决托管软件的其他安装问题，Citrix 建议使用组策略启用 Windows 安装程序日志记录。

将 **Citrix Secure Access** 客户端与 **Citrix Workspace** 应用程序集成

February 1, 2024

NetScaler Gateway 支持 Citrix Workspace 应用程序。协调系统由以下组件组成：

- 适用于 Windows 3.4 或更高版本的 Citrix Workspace
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- StoreFront 2.1 或更高版本
- Endpoint Management 2.8 及更高版本或 Citrix Endpoint Management 10
- Citrix 网站上托管的 Citrix更新服务

有关 NetScaler Gateway 与 NetScaler 产品的兼容性的更多信息，请参阅与 NetScaler 产品的兼容性。

您可以配置 NetScaler Gateway，这样当用户登录设备时，Citrix Secure Access 客户端会打开一个允许单点登录 Citrix Workspace 应用程序主页的 Web 浏览器。用户可以从主页下载 Citrix Workspace 应用程序。

当用户使用 Citrix Workspace 应用程序登录时，用户连接可以通过以下方式通过 NetScaler Gateway 进行路由：

- 直接进入 Endpoint Management
- 直接进入 StoreFront
- 如果未在 Endpoint Management 中配置 MDX 移动应用程序，则先转到 StoreFront 和 Endpoint Management
- 如果在 Endpoint Management 中配置了 MDX 移动应用程序，则转到 Endpoint Management 和 StoreFront

> 注意：
>
> 仅 Endpoint Management 2.0、Endpoint Management 2.5、Endpoint Management 2.6、Endpoint

> Management 2.8 和 Endpoint Management 2.9 支持直接路由到 Endpoint Management 的连接。如果您的网络中部署了 Endpoint Management 1.1，则用户连接必须通过 StoreFront 进行路由。

用户如何与 **Citrix Workspace** 应用程序建立连接

February 1, 2024

用户可以从 Citrix Workspace 应用程序连接到以下应用程序、桌面和数据：

- 在 StoreFront 和 Web Interface 中发布的基于 Windows 的应用程序和虚拟桌面
- 通过 Citrix Endpoint Management 访问的 ShareFile 数据

用户可以使用以下任一 Citrix Workspace 应用程序登录：

- 适用于 Web 的 Citrix Workspace 应用
- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Android 的 Citrix Workspace 应用程序

用户可以使用 Web 浏览器或用户设备上的 Citrix Workspace 应用程序图标使用适用于 Web 的 Citrix Workspace 应用程序登录。

当用户使用任何版本的 Citrix Workspace 应用程序登录时，应用程序、ShareFile 数据和桌面都会显示在浏览器或 Citrix Workspace 应用程序窗口中。

解耦 **Citrix Workspace** 应用程序图标

February 1, 2024

如果将 Citrix Virtual Apps and Desktops 部署配置为与 Citrix Workspace 应用程序集成的 Citrix Secure Access 客户端，则连接到 VPN 的用户看不到该插件的图标。**Citrix Secure Access** 图标通常位于 Windows 系统托盘或 macOS X Finder 的菜单栏中。此图标是插件设置和控件的界面。对于 Windows 用户，当集成 Citrix Workspace 应用程序和 Citrix Secure Access 客户端时，Citrix Workspace 应用程序中的“关于”对话框会显示 Citrix Secure Access 客户端的控件。对于 macOS X 用户，集成后 Citrix Secure Access 客户端没有任何控件可用。

某些集成部署可能需要公开插件控件，同时保留底层功能的集成。为此，请使用以下 CLI 命令或 NetScaler 配置实用程序任务切换 VPN 客户端的图标集成。

使用 **CLI** 设置图标集成

在命令提示窗口中，键入：

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

使用 **GUI** 设置图标集成

1. 在配置选项卡上，导航到 **NetScaler Gateway >** 全局设置。
2. 单击“更改全局设置”，然后选择“客户端体验”选项卡。
3. 单击“高级设置”。
4. 选择在 Citrix Workspace 应用程序中 显示 **VPN** 插件 图标。

为 **ICA** 连接配置 **IPv6**

February 1, 2024

NetScaler Gateway 支持用于 ICA 连接的 IPv6 地址。使用 IPv6 连接到 Web Interface 或 StoreFront 的连接与 IPv4 连接的工作方式相同。当用户使用 NetScaler Gateway Web 地址进行连接时，NetScaler Gateway 将代理与 Web Interface 或 StoreFront 的连接。

您可以为部署在一个 DMZ 中或部署在双跃点 DMZ 中的 NetScaler Gateway 配置 IPv6。

您可以使用命令行在 NetScaler Gateway 上启用 IPv6。您可以使用以下准则：

- 在设备上启用 IPv6。
- 配置子网 IP 地址。
- 设置 DNS 解析顺序。
- 设置 Web Interface 或 StoreFront Web 地址。
- 将 Secure Ticket Authority (STA) 绑定到 NetScaler Gateway。

默认情况下，映射的 IP 地址不支持 IPv6 地址。要将用户通信路由到内部网络，您需要创建子网 IP 地址，然后将 NetScaler Gateway 配置为使用子网 IP 地址。

如果在网络中部署多个 IPv6 子网，请在 NetScaler Gateway 上为网络中的每个子网创建多个 IPv6 子网 IP 地址。网络路由使用子网 IP 地址将 IPv6 数据包发送到相应的子网。

使用 **CLI** 为 **ICA** 代理配置 **IPv6**

1. 使用安全外壳 (SSH) 连接（例如从 PuTTY）登录 NetScaler Gateway。在命令提示窗口中，键入：

```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter  -resolutionOrder AAAAThenAQuery AThenAAAAQuery
    OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`

<!--NeedCopy-->
```

其中 是 StoreFront 的域名或 IP 地址。

示例：

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb
    `.
<!--NeedCopy-->
```

或

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
<!--NeedCopy-->
```

> 注意：
>
> 如果使用 IPv6 地址配置此参数，则 IP 地址必须包含在括号中。

在 **NetScaler Gateway** 上配置 **Citrix Workspace** 应用程序主页

February 1, 2024

您可以全局配置 Citrix Workspace 应用程序主页，也可以作为会话配置文件的一部分配置。如果要为无法通过 NetScaler Gateway 识别 StoreFront 的 Web 和更早的 Citrix Workspace 应用程序版本配置 Citrix Workspace 应用程序，则需要创建两个单独的会话配置文件。字段 Citrix Workspace 应用程序主页需要为每个配置文件提供正确的 Web 地址，以便用户能够成功登录。

对于通过 NetScaler Gateway 识别 StoreFront 的 Citrix Workspace 应用程序，您可以让适用于 Web 的 Citrix Workspace 应用程序和 Citrix Workspace 应用程序共享配置但是，Citrix 建议您为适用于 Web 的 Citrix Workspace 应用程序配置会话配置文件，为所有其他 Citrix Workspace 应用程序配置单独的会话配置文件

全局配置 **Citrix Workspace** 应用程序主页

要全局配置 Citrix Workspace 应用程序主页：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在全局 NetScaler Gateway 设置对话框中，单击已发布的应用程序选项卡。
4. 在 Citrix Workspace 应用程序主页中，键入 Citrix Workspace 应用程序或适用于 Web 的 Citrix Workspace 应用程序主页的 Web 地址，然后单击“确定”。

在会话配置文件中配置 **Citrix Workspace** 应用程序主页

要在会话配置文件中配置 Citrix Workspace 应用程序主页：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格的“配置文件”选项卡上，单击“添加”。
3. 在 创建 **NetScaler Gateway** 会话配置文件 对话框中，在 **Citrix Receiver** 主 页旁边的 已发布应用程序 选项卡上，单击 覆盖全局。
4. 在 Citrix Workspace 应用程序主页中，键入 Citrix Workspace 应用程序或适用于 Web 的 Citrix Workspace 应用程序主页的 Web 地址，然后单击创建。

将 **Citrix Workspace** 应用程序主题应用到 **NetScaler Gateway** 登录页面

February 1, 2024

您可以使用 NetScaler Gateway 用户界面将 Citrix Workspace 应用程序主题应用到 NetScaler Gateway 的登录页面。您可以在 Citrix Workspace 应用程序主题和您创建的自定义主题之间切换。创建自定义主题后，清除浏览器缓存以防止出现缓存的页面。

默认情况下，NetScaler Gateway 登录页面使用 RfWebUI 视觉主题，该主题与 StoreFront 使用的统一用户界面的样式相匹配。如果您使用的是 Citrix Workspace 平台或带有全新 Workspace 用户界面的本地 StoreFront，请按照此支持文章中提供的说明进行操作。或者，您可以创建自己的自定义主题。有关详细信息，请参阅 NetScaler Gateway 登录页面创建自定义主题。

确保 NetScaler Gateway 门户主题绑定到 VPN 虚拟服务器。有关详细信息，请参阅将门户主题绑定到 VPN 虚拟服务器。

为 **NetScaler Gateway** 登录页面创建自定义主题

February 1, 2024

您可以使用 GUI 为 NetScaler Gateway 的登录页面创建自定义主题。您还可以保留默认主题或使用 Citrix Workspace 应用程序主题。当您选择将自定义主题应用于登录页面时，可以使用 NetScaler Gateway 命令行创建和部署主题。然后，您可以使用 GUI 设置自定义主题页面。

您可以使用 NetScaler Gateway 全局设置配置自定义主题页面。

您可以将此功能用于以下版本的 NetScaler Gateway：

- NetScaler Gateway 10.1
- 访问网关 10，内部版本 73.5002.e（必须在版本 71.6104.e 之后安装此版本才能将此功能与 Endpoint Management 版本 2.5、2.6 或 2.8 一起使用）
- 访问网关 10，构建 71.6104.e

使用 **CLI** 创建和部署自定义主题

要使用命令行创建和部署自定义主题，请执行以下操作：

1. 登录 NetScaler Gateway 命令行。
2. 在命令提示符处，键入 shell。
3. 在命令提示符处键入 `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`。
4. 使用配置实用程序切换到自定义主题，然后在 /var/ns_ns_gui_custom/ns_gui/VPN 下进行自定义更改。您可以：
    - 对 css/ctx. 验证.css 文件进行编辑。
    - 将自定义徽标复制到 /var/ns_ns_gui_custom/ns_gui/vpn/媒体文件夹。注意：您可以使用 WinSCP 传输文件。
5. 如果您有多台 NetScaler Gateway 设备，请对所有设备重复步骤 3 和 4。

NetScaler Gateway Windows VPN 客户端注册表项

February 1, 2024

VPN 客户端注册表项在 **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client** 下可用。下表列出了 NetScaler Gateway VPN 客户端注册表项、值以及每个值的简要说明。

注册表项	注册表类型	值和描述
AlwaysOnService	REG_DWORD	1 => 建立计算机级通道但不建立用户级通道。2 => 建立计算机级通道和用户级通道。
AlwaysOnURL	REG_SZ	用户要连接到的 NetScaler Gateway 虚拟服务器的 URL。示例：*https://xyz.companyDomain.com*
AlwaysOn	REG_DWORD	1 => 在 VPN 失败时允许网络访问。2=> VPN 失败时阻止网络访问。
locationDetection	REG_DWORD	1 => 启用位置检测。0 => 禁用位置检测。
suffixList	REG_SZ	内联网域的分号分隔的列表。在启用位置检测时使用。
AlwaysOnAllowlist	REG_SZ	在 Always On 严格模式下，驱动程序允许使用分号分隔的 IP 地址或 FQDN 列表。
ProductVersion	REG_SZ	当前 Citrix Secure Access 客户端安装的版本。
InstallDir	REG_SZ	Citrix Secure Access 客户端的安装位置。
userCertCAList	REG_SZ	在 Always Oon 服务的上下文中使用，客户可以在此服务中指定要从中选择客户证书的 CA 列表。
addedRoutes/modifiedRoutes	REG_SZ	为内部插件通信而创建。用户不得修改此密钥。
ProductCode	REG_SZ	此密钥在内部使用。用户不得修改此密钥
EnableAutoUpdate	REG_DWORD	用于从客户端控制插件更新功能。设置为 0 可禁用自动更新功能。设置为 1 以尊重 ADC 配置。
已连接	REG_DWORD	成功连接后，此键设置为 1，否则设置为 0。此密钥在内部使用。用户不得修改此密钥。

注册表项	注册表类型	值和描述
EnableVA	REG_DWORD	IIP 存在时是否必须启用 Citrix 虚拟适配器。此密钥在内部使用。用户不得修改此密钥。
DisableGA	REG_DWORD	设置为 1 以禁用 Google Analytics。
DisableCredProv	REG_DWORD	启用用户登录前始终打开时，Windows VPN 插件会添加凭据提供程序以在登录屏幕上显示通道状态。如果不需要此附加功能，请创建此注册表并将其设置为 1。
ClientControl	REG_DWORD	1 => 允许用户注销或连接到其他网关。0 => 阻止用户注销或连接到其他网关。
ForcedLogging	REG_DWORD	将此键设置为 1 可启用调试日志记录。
NoDHCPRoute	REG_DWORD	如果设置为 1，则不会添加 DHCP 服务器路由。
DisableIntuneDeviceEnrollment	REG_DWORD	如果设置为 1，则不会执行 Intune 设备注册。
HttpTimeout	REG_DWORD	HTTP 超时以秒为单位进行配置。如果未配置超时，则使用默认超时。根据 Windows 标准，默认超时值为 100 秒。
secureDNSUpdate	REG_DWORD	0 => VPN 插件仅尝试不安全的 DNS 更新。1 => VPN 插件首先尝试不安全的 DNS 更新。如果不安全的 DNS 更新失败，VPN 插件将尝试进行安全 DNS 更新。这是从 21.3.1.2 Windows 插件版本开始的默认行为。2 => VPN 插件仅尝试安全 DNS 更新。
DisableIconHide	REG_DWORD	1 => Citrix Workspace 应用程序和网关插件显示在任务栏上。0 => 网关插件图标已与适用于 Windows 的 Citrix Workspace 应用程序集成。运行完整 VPN 会话时，任务栏上看不到网关插件。

注册表项	注册表类型	值和描述
SecureChannelResetTimeoutSeconds	REG_DWORD	默认情况下，不设置或添加此注册表值。当“SecureChannelReset-TimeoutSeconds”的值为 0xFFFFFFFF 或不在注册表中时，VPN 插件会等待 SecureChannelReset() API 调用完成后再开始通道传输数据流量。这是默认行为。管理员必须在客户端上设置此注册表，以便 VPN 插件在等待 API 调用完成的指定时间后开始传输数据流量。
DisableDNSRoutes	REG_DWORD	默认值 0 => 如果 DNS 服务器不同于物理接口的默认网关，则 VPN 插件会为 DNS 服务器添加路由。但是，根据 Windows 客户端计算机拓扑，可能并不总是需要 DNS 服务器路由。如果设置为 1，则 VPN 插件不会为 DNS 服务器添加显式路由。
overrideIPV6DnsDrop	REG_DWORD	1 => 允许 IPv6 DNS 流量通过 VPN 流动。0 => 限制 IPv6 DNS 流量。
DisallowCaptivePortals	REG_DWORD	1 => VPN 插件在启动 VPN 会话之前尝试连接到 Microsoft Connect 测试 页来检查是否有专属门户。0 => VPN 插件会跳过强制门户检查。
EnableWFP	REG_DWORD	默认值 0 => 默认情况下，DNE 处于启用状态。1 => VPN 插件使用 WFP。0 => VPN 插件使用 DNE。

注册表项	注册表类型	值和描述
ConfigSize	REG_DWORD	默认情况下，Windows 客户端支持 64 KB 的配置文件大小。使用此注册表可增加配置文件的大小。如果配置文件大小大于默认值 (64 KB)，则每增加 64 KB，就必须将 ConfigSize 注册表值设置为 5 x 64 KB（转换为字节后）。例如，如果您要额外增加 64 KB，则必须将注册表值设置为 64 x 1024 x 5 = 327680。同样，如果您要增加 128 KB，则必须将注册表值设置为 64 x 1024 x (5+5) = 655360。
SecureAccessLogInScript	REG_SZ	Citrix Secure Access 服务在连接到 Citrix Secure Private Access 服务时使用此注册表项访问登录脚本配置。有关详细信息，请参阅登录和注销脚本配置注册表。
SecureAccessLogOutScript	REG_SZ	Citrix Secure Access 服务在连接到 Citrix Secure Private Access 服务时使用此注册表项访问注销脚本配置。有关详细信息，请参阅登录和注销脚本配置注册表。
EnableKerberosAuth	REG_DWORD	0 => 默认值。1 => VPN 客户端使用 Kerberos 身份验证方法进行自动登录。
SicBeginPort	REG_DWORD	避免使用端口在 Citrix Secure Access 客户端与客户端上的第三方应用程序之间创建套接字时可能出现的冲突。允许的范围是 49152 到 64535（十六进制格式的 C000 到 FC17)。仅当 `EnableWFP` 也设置为 1 时，VPN 客户端最多使用自 `SicBeginPort` 起的 1000 个端口。

> 重要提示：

> - 您可以根据自己的部署应用注册表项。例如，AlwaysOnService 注册表项仅适用于 Always on 服务，而 ClientControl 注册表项不适用于 Always on 服务。有关更多详细信息，请参阅单个部署文档。
> - `secureDNSUpdate` 仅适用于已加入域的客户端设备。
> - 对于适用于 Windows 23.1.1.8 及更高版本的 Citrix Secure Access 客户端，注册表项名称为 `overrideIPV6DnsDrop`。对于适用于 Windows 22.10.1.9 及更早版本的 Citrix Secure Access 客户端，注册表项名称为 `overrideIP6DnsDrop`。

强制对身份验证 **cookie** 使用 **HttpOnly** 标志

February 1, 2024

从 NetScaler Gateway 版本 13.1-37.x 及更高版本开始，HttpOnly 标志在 VPN 场景的身份验证 cookie 上可用，即 NSC_AAAC 和 NSC_TMAS cookie。NSC_TMAS 身份验证 cookie 在 nFactor 身份验证期间使用，NSC_AAAC cookie 用于经过身份验证的会话。Cookie 上的 HttpOnly 标志使用 JavaScript 文档 cookie 选项限制 cookie 的访问。这有助于防止 Cookie 因跨站脚本而被盗用。

支持的场景

nFactor 身份验证支持 HTTPOnly 标志。

将 **NetScaler AAA** 参数的 **HttpOnlyCookie** 旋钮与 **tmsession** 的 **HttpOnlyCookie** 旋钮一起使用时的行为：

- 当启用身份验证、授权和审核参数的 httpOnlyCookie 旋钮并使用 nFactor 身份验证时，身份验证、授权和审核参数的 HttpOnlyCookie 旋钮会覆盖 TM 会话的 HttpOnlyCookie 旋钮。此外，无论会话类型如何；无论是 VPN 会话、TM 会话还是 nFactor 身份验证期间，NSC_TMAS 和 NSC_AAAC 都被标记为 HttpOnly。
- 如果禁用 HttpOnlyCookie 旋钮，则不会为 VPN 会话设置 HttpOnly 标志。对于身份验证、授权和审核方案，HttpOnly 标志是根据 TM 会话旋钮值设置的。

使用 **CLI** 配置 **HttpOnly** 功能

- 启用 HTTPOnly 标志

```
set aaa parameter -httpOnlyCookie ENABLED
<!--NeedCopy-->
```

- 检查 HttpOnly 功能的状态

```
show aaa parameter
<!--NeedCopy-->
```


限制

- 启用 HttpOnly 功能后，Citrix Secure Access 客户端上的“主页”按钮不起作用。
- 在任何经典身份验证中均未设置 HttpOnly 标志。

自定义 **VPN** 用户的用户门户

February 1, 2024

为 VPN 用户提供门户服务的 NetScaler Gateway 安装包括一个选项，用于选择门户主题以创建门户页面的自定义外观。您可以从提供的一组主题中进行选择，也可以使用模板作为模板来构建自定义或品牌门户。使用配置实用程序，您可以通过添加新徽标、背景图像、自定义输入框标签以及基于 CSS 的门户设计的各种其他属性来修改主题。内置门户主题包括五种语言的内容：英语、法语、西班牙语、德语和日语。不同的用户以不同的语言提供服务，具体取决于他们的 Web 浏览器报告的区域设置。

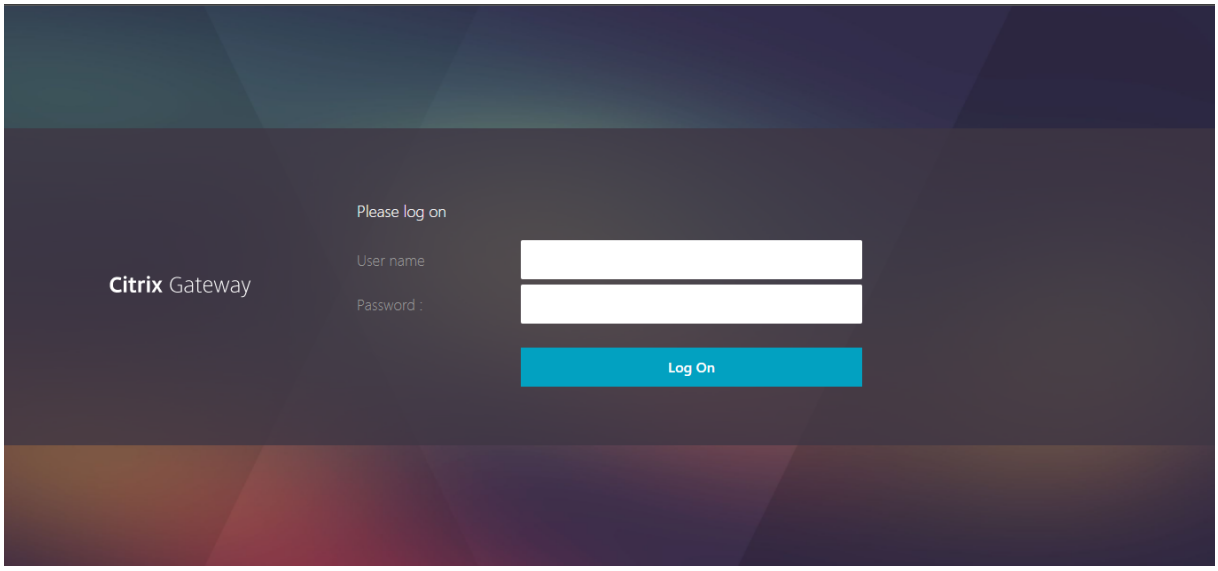
您可以创建在允许 VPN 用户登录之前向其提供的自定义 EULA。最终用户许可协议功能支持特定于区域设置的 EULA 版本，这些版本根据用户的 Web 浏览器报告的区域设置向用户显示。

门户主题和 EULA 配置都可以在 VPN 虚拟服务器和 VPN 全局级别独立绑定。

> 重要：
>
> NetScaler 不支持需要修改代码的自定义，也不支持解决除恢复到默认主题以外的问题。

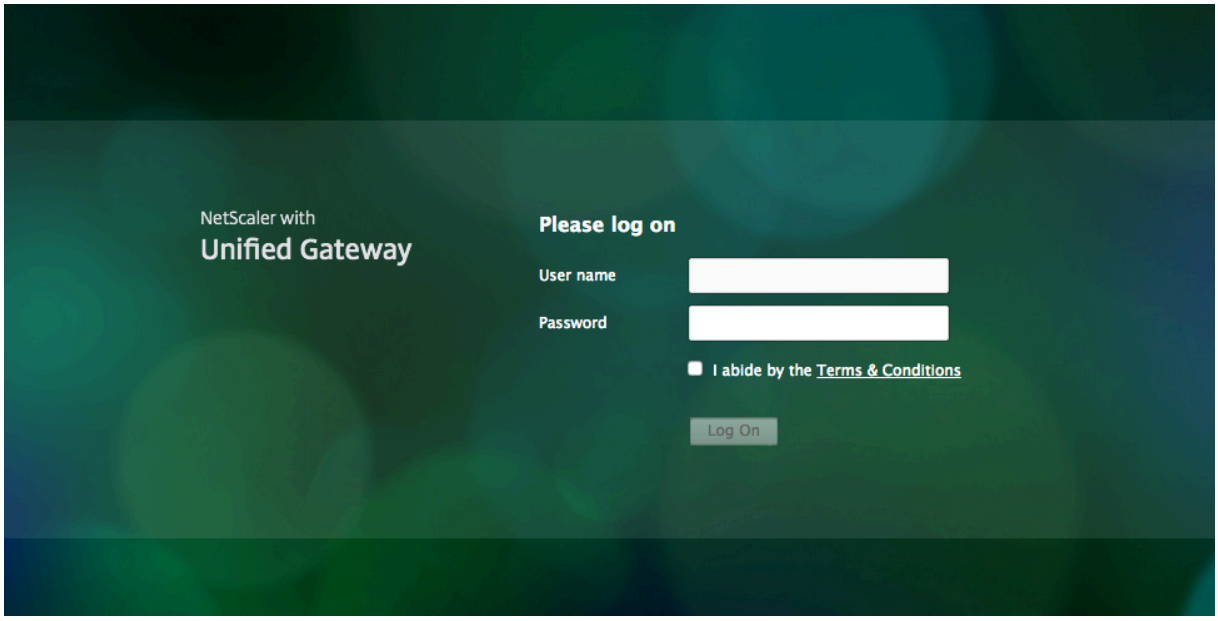
应用门户主题

默认情况下，从版本 13.0 版本 67.43 开始，VPN 门户配置为使用 RFWeBUI 主题。以前，这 `Caxton theme` 是默认主题。您也可以应用绿色气泡和 X1 主题。

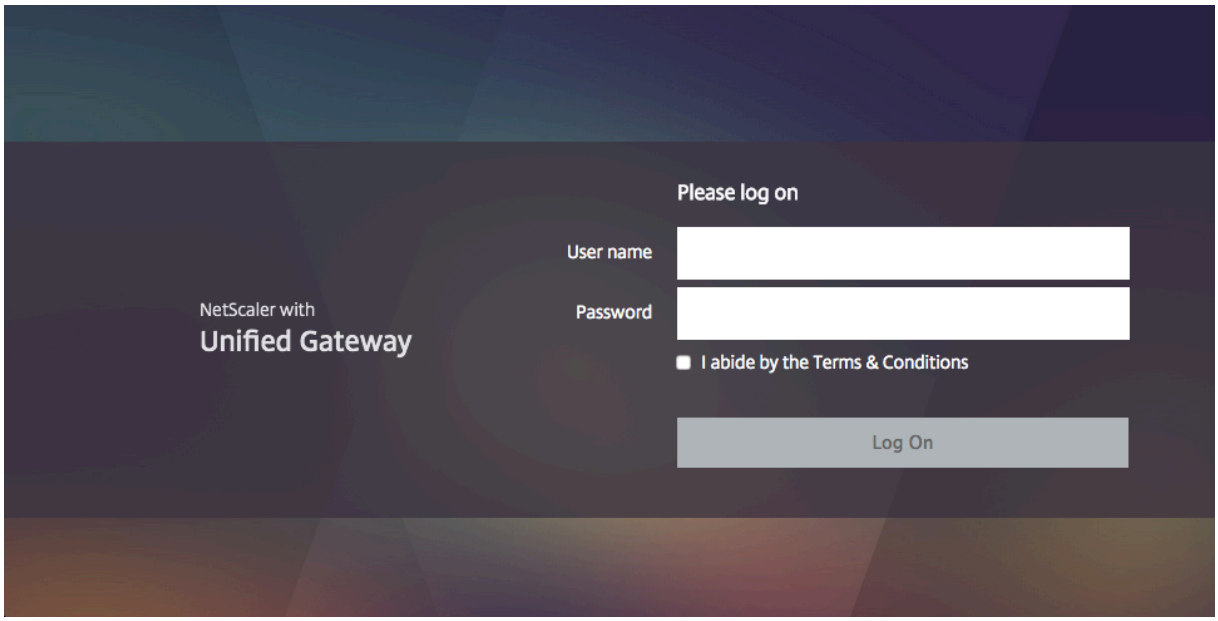


卡克斯顿主题

绿色泡泡主题



X1 主题



您可以将提供的任何主题直接应用于 VPN 虚拟服务器或作为全局 VPN 绑定。

将门户主题绑定到 **VPN** 虚拟服务器

您可以在现有虚拟服务器上或在创建新的虚拟服务器时绑定门户主题。

使用 **CLI** 将门户主题绑定到 **VPN** 虚拟服务器

在命令提示窗口中，键入：

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

使用 **GUI** 将门户主题绑定到 **VPN** 虚拟服务器

1. 在 配置 选项卡上，导航到 **NetScaler Gateway** ，然后单击 虚拟服务器。
2. 选择虚拟服务器，然后单击 编辑。
3. 如果门户主题尚未绑定到虚拟服务器，请单击详细信息窗格中 高级设置 下的 门户主题。否则，门户主题选项已在详细信息窗格中展开。
4. 在详细信息窗格中的 门户主题下，单击 无门户主题以展开门户主题绑定窗口。
5. Click 单击以选择。
6. 在“门户主题”窗口中，单击主题名称，然后单击“选择”。
7. 单击绑定。

8. 单击 **Done**（完成）。

如果要创建 VPN 虚拟服务器，则可以在 **VPN** 虚拟服务器编辑 窗格中执行从步骤 3 开始的上一过程中的步骤绑定门户主题。

将门户主题绑定到 **VPN** 全局

使用 **CLI** 将门户主题绑定到 **VPN** 全局

在命令提示符下，键入;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```

使用 **GUI** 将门户主题绑定到 **VPN** 全局

1. 在“配置”选项卡上，导航到 **NetScaler Gateway**。
2. 在主详细信息窗格中，单击 **NetScaler Gateway** 策略管理器。
3. 单击“**+**”图标。
4. 在 绑定点 列表中，选择 资源。
5. 在“连接类型”列表中，选择“门户主题”。
6. 单击继续。
7. 在 绑定点屏幕中，单击 添加绑定。
8. 单击 单击以选择。
9. 在“门户主题”窗口中，单击主题名称，然后单击“选择”。
10. 单击绑定。
11. 单击关闭。
12. 单击“完成”。

> 提示：
>
> 进行更改后，请在命令行上使用“save ns config”命令或单击配置实用程序中的保存图标，以确保将更改保存到 NetScaler 配置文件中。

创建门户主题

要创建自定义门户设计，请使用提供的门户主题之一作为模板。系统使用您指定的名称创建所选模板主题的副本。

使用股票门户主题作为自定义门户主题的模板

要创建门户主题，可以使用配置实用程序或命令行创建主题实体。但是，详细的自定义控件仅在配置实用程序中可用。

使用 **CLI** 创建门户主题

在命令提示符下，键入;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```

使用 **GUI** 创建门户主题

1. 在 配置 选项卡上，导航到 **NetScaler Gateway** ，然后单击 门户主题。
2. 在主详细信息窗格中，单击 添加。
3. 输入主题的名称，然后从模板列表中选择一个模板，然后单击“确定”。
4. 此时，您将看到门户主题编辑窗口的首次视图。单击确定以退出。

您可以继续使用首次视图自定义新门户主题。

创建新主题后，您可以将其绑定到 VPN 虚拟服务器或 VPN 全局。您可以在创建后或完成自定义后立即绑定新模版。

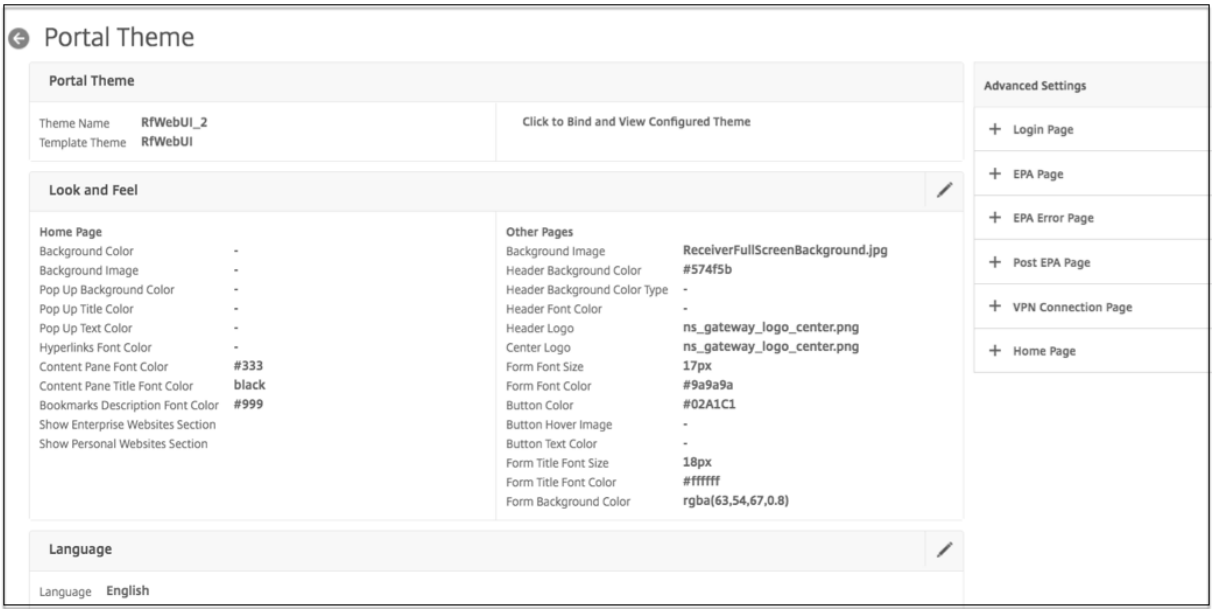
门户主题自定义

要自定义门户主题，请使用配置实用程序中的门户主题界面。为了获得最佳结果，您必须在使用此界面之前了解它的各种元素。

关于门户主题界面

要在 NetScaler Gateway 配置实用程序中打开 门户主题界面，请在 配置 选项卡上导航到 **NetScaler Gateway** ，然后单击 门户主题。您可以按照创建 门户主题中的说明创建主题，也可以在主详细信息窗格中选择现有主题，然后单击 编辑。

门户主题自定义页面有四个用于修改门户设计的主要组件窗格：门户主题窗格、外观窗格、高级设置 窗格和 语言 窗格。



页面顶部的“门户主题”窗格会报告加载哪个主题进行编辑以及它所基于的模板主题。此处的查看选项允许您查看自定义设置，而无需通过用户连接访问 VPN。使用查看选项需要将主题绑定到 VPN 虚拟服务器，并且绑定在查看窗口关闭后仍然有效。

在页面中央的“外观和感觉”窗格中，您可以配置主题的常规属性，例如标题、背景颜色和图像、字体属性和徽标。当此窗格处于编辑模式时，属性图例可用于指导门户页面上使用“外观和感觉”属性的位置。

“高级设置”窗格包含各个门户页面的屏幕内容控件。要加载页面内容进行编辑，请单击列出的其中一个页面。然后，页面控件会在其他中心窗格的下方打开。只要尚未修改页面，在对 Portal Theme 进行编辑的 高级设置 窗格中，页面就会保持折叠状态。

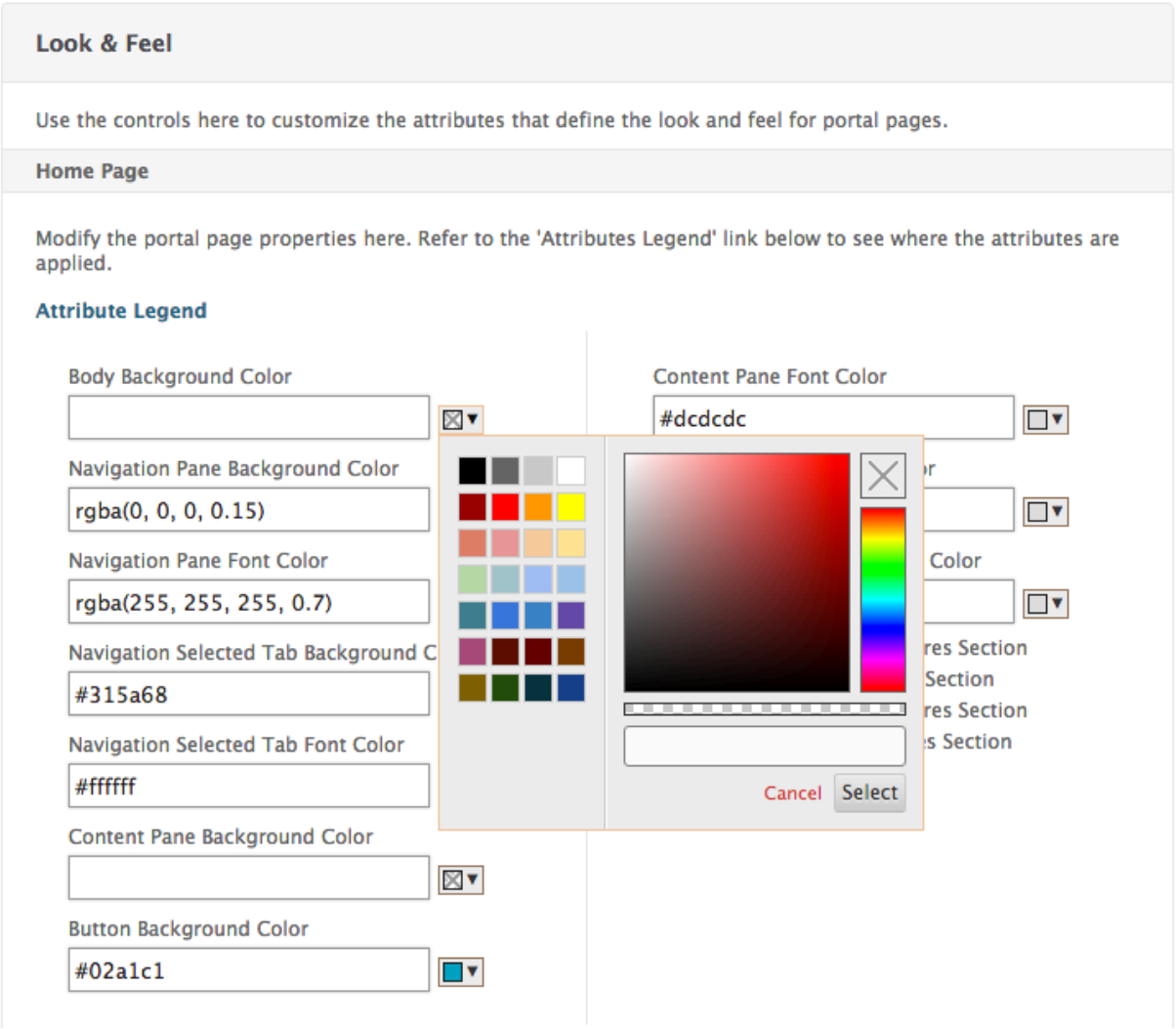
在 语 言窗格中，您可以选择从“高级设置”窗格中选择要编辑的页面时加载哪种语言。默认情况下会加载英语页面。

可自定义页面属性的类型

自定义门户主题时，可以在门户主题界面中修改一系列属性。除了可以编辑的文本和支持的语言外，还可以定制门户布局的图形元素以满足您的需求。每个页面元素类型都有参数或建议，在修改它们之前需要考虑。

颜色

门户设计指定属性的颜色，例如页面背景、突出显示、标题和正文内容的文本、按钮控件和悬停响应。要自定义颜色属性，可以直接为选定项目输入颜色值，也可以使用提供的拾色器生成颜色值。该界面支持以 RGBA 格式、HTML 十六进制三重格式和 X11 颜色名称输入有效的 HTML 颜色值。通过单击属性输入字段旁边的颜色框，可以访问任何适用的颜色属性的拾色器。



字体

除了字体颜色之外，您还可以修改某些页面属性的字体大小。对于这些属性中的每一个，菜单提供了每个属性的可用大小，具体取决于门户的设计。

图像

对于图像，每个控件的弹出式描述提供了尺寸建议和其他要求。描述根据属性在页面上的位置及其功能而有所不同。您可以使用 PNG 或 JPEG 图像文件格式。您可以选择要上载的图像，方法是选中项目文件名下方的复选框，然后浏览到图像在本地计算机驱动器上的驻留位置。

標籤

在“高级设置”部分中，您可以选择要修改的特定门户页面的文本。如果修改页面的默认英文文本，则不会重新翻译其他语言的文本。提供替代语言页面内容是为了方便起见，但需要手动更新任何自定义项。要编辑页面的其他语言版本，请首先通过单击打开的门户页面的 **X** 图标来折叠窗口（如果窗口处于打开状态）。然后在“语言”窗格中选择 语言，然后单击“确定”。在选择其他语言之前，从“高级设置”窗格中打开的所有门户页面均使用该语言。

> 重要
>
> 在高可用性或群集部署中，仅当分别在主协调器或配置协调器 NetScaler 实体上进行门户主题设置时，门户主题才会在共享配置中分布。

较旧的门户自定义项

对于在 11.0 之前的 NetScaler Gateway 或 Access Gateway 版本中创建的带有手动修改的自定义门户设计的安装，NetScaler 强烈建议在自定义界面中从新的门户主题开始。如果无法执行此操作，则可以手动应用自定义项，但不提供直接支持。

使用手动自定义门户时，必须将自定义门户设置为全局门户配置。但是，这样做意味着应用的全局门户配置 不能 被 VPN 虚拟服务器级门户主题绑定覆盖。在这种情况下，尝试使用配置实用程序或命令行创建 VPN 虚拟服务器绑定会返回错误。

此外，在高可用性和群集配置的情况下，必须在部署中的每个节点上执行任何手动自定义，因为 NetScaler 文件系统上的基础文件不会在自动共享配置中分发。

手动创建自定义门户配置

要在升级到 NetScaler Gateway 11.0 后手动应用较旧的自定义门户配置，您需要修改现有门户页面的副本，将自定义门户文件放入 NetScaler 文件系统中，然后选择 自定义 作为 **UITHEME** 参数。

您可以使用 WinSCP 或任何其他安全复制程序将文件传输到 NetScaler 文件系统。

1. 登录 NetScaler Gateway 命令行。
2. 在命令提示符处，键入 **shell**
3. 在命令提示符处，键入 **mkdir /var/ns_gui_custom; cd /netscaler; tar-cvzf /var/ns_gui_custom/customtheme ns_gui/***。
4. 在命令提示符处，键入 **cd /var/netscaler/**登录**/**主题**/**
   - 如果要自定义绿色气泡主题，请输入 **cp -r** `Greenbubble` **Custom** 以复制绿色气泡主题。
   - 如果要自定义默认主题 (`Caxton`)，请键入 **cp-r** 默认自定义。
   - 要自定义 X1 主题，请键入 **cp-r X1** 自定义。
5. 在 **/var/netscaler/logon/themes/Custom** 下对复制的文件进行必要的更改，以手动自定义主题。
   - 对 **css/base.css** 进行必要的编辑。
   - 将任何自定义镜像复制到 **/var/ns_ns_ns_gui/vpn/**媒体 目录。
   - 对 **resources/** 目录中存在的文件中的标签进行更改。这些文件对应于门户支持的区域设置。
   - 如果还需要对 HTML 页面或 JavaScript 文件进行更改，则可以使其与 **/var/ns_gui_custom/ns_gui/**中的文件相关。
6. 完成所有自定义更改后，在提示符下输入：**tar –cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

> 重要
>
> 在上述步骤中复制主题目录时，必须完全按照“自定义”输入复制的文件夹名称，因为目录名称在 NetScaler shell 界面中区分大小写。如果未精确输入目录名称，则当 **UITHEME** 设置配置为 CUS **TO**M 时，将无法识别该文件夹。

选择自定义主题作为 **VPN** 全局参数

手动自定义的门户配置完成并复制到 NetScaler 文件系统后，需要将其应用于 NetScaler Gateway 配置。这可以通过将 UITHEME 参数设置为 CUSTOM 来完成，可以使用命令行或配置实用程序来完成。

要使用命令行，请输入以下命令来设置 **UITHEME** 参数。

```
set vpn parameter UITHEME CUSTOM
<!--NeedCopy-->
```

要使用配置实用程序设置 UITHEME 参数，请使用以下步骤。

1. 在 配置 选项卡上，导航到 **NetScaler Gateway >** 全局设置。
2. 单击“更改全局设置”。
3. 单击“客户端体验”选项卡。
4. 滚动到屏幕底部，然后从 **UI** 主题 列表菜单中选择 自定义。
5. 单击确定。

您的手动自定义门户现在是提供给 VPN 用户的门户设计。

创建 **EULA**

VPN 门户系统提供了将 EULA 应用于入口配置的选项。将 EULA 绑定到 NetScaler Gateway 配置后，无论是在 VPN 全局范围内还是在相关的 VPN 虚拟服务器上，VPN 用户必须同意 EULA 作为条款和条件，然后才能在 VPN 中进行身份验证。

与门户主题一样，根据用户的 Web 浏览器报告的区域设置，为用户提供特定语言的最终用户许可协议。如果语言环境与任何受支持的语言都不匹配，则默认提供的语言为英语。对于每个 EULA，您可以使用每种支持的语言输入自定义消息。EULA 配置不提供预翻译的内容，因为它是针对门户主题的内容。如果用户报告的区域设置与未输入 EULA 内容的语言匹配，则当用户单击 VPN 登录页面上的“条款和条件”链接时，将返回空白页。

要创建最终用户许可协议，您可以使用配置实用程序中的任一控件，位于 **NetScaler Gateway >** 全局设置 **> EULA** 或 **NetScaler Gateway **** 资源 **>** 最终用户 许可协议的配置选项卡上。“全局设置”窗格中的控件用于管理 **VPN** 全局 **EULA** 绑定，而“资源”>“EULA”节点上的控件用于对 **EULA** 配置进行常规操作。您可以通过在 NetScaler Gateway > 虚拟服务器上编辑 VPN 虚拟服务器来管理 VPN 虚拟服务器 **EULA 绑定。一些命令也可用于管理 EULA 实体的命令行。但是，完整的 EULA 管理控件仅在配置实用程序中可用。

使用 **CLI** 创建 **EULA** 实体

在命令提示窗口中，键入：

```
add vpn eula <name>
<!--NeedCopy-->
```

使用 **GUI** 创建 **EULA** 实体

1. 导航到 **NetScaler Gateway >** 资源 **>** 最终用户许可协议。
2. 单击 添加 以创建实体。
3. 输入实体的名称。
4. 对于每种语言，粘贴相关选项卡下的内容。您可以使用纯文本或 HTML 标记来设置内容的格式，包括添加换行符的
 标记。
5. 单击创建。

创建 EULA 实体后，它可以全局绑定到 VPN 配置，也可以绑定到 VPN 虚拟服务器。

使用 **CLI** 将 **EULA** 绑定到 **VPN** 全局

在命令提示符下，键入;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

使用 **GUI** 将最终用户许可协议绑定到 **VPN** 全局

1. 在 配置 选项卡上，导航到 **NetScaler Gateway >** 全局设置。
2. 在主详细信息窗格中，单击 配置最终用户许可协议。
3. 单击 **Add Binding**（添加绑定）。
4. 单击 单击以选择。
5. 选择一个 EULA 实体，然后单击 选择。
6. 单击绑定。
7. 单击关闭。

使用 **CLI** 将 **EULA** 绑定到 **VPN** 虚拟服务器

在命令提示符下，键入;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```


使用 **GUI** 将 **EULA** 绑定到 **VPN** 虚拟服务器

1. 在“配置”选项卡上，浏览至 **NetScaler Gateway >** 虚拟服务器。
2. 在主详细信息窗格中，选择一个 VPN 虚拟服务器，然后单击 编辑。
3. 在页面右侧的“高级设置”窗格中，单击 **EULA**。
4. 在新添加的最终用户许可协议窗格中，单击 **No EULA**。
5. `Click` 单击以选择。
6. 选择一个 EULA 实体，然后单击 选择。
7. 单击绑定。
8. 单击 **Done**（完成）。

通过创建自定义页面提示用户升级较旧的浏览器或不受支持的浏览器

February 1, 2024

如果客户端使用不安全的密码（例如 SSLv3）连接到 NetScaler VIP 地址，则可以将其重定向到自定义页面，提示他们升级到最新版本的 Internet Explorer、Firefox、Chrome 或 Safari 浏览器。

注意：根据互联网工程任务组 (ITEF) 的 RFC6176，TLS 服务器不得支持 SSLv2。因此，NetScaler 设备不支持 12.1 及更高版本中的 SSLv2。

如何创建自定义页面以提示用户升级基于 **SSL** 的旧版不受支持的浏览器

- 使用规则创建 NetScaler 响应程序策略 `client.ssl.version.eq()`。该版本返回 SSL 协议版本。
  - 如果事务不是基于 SSL 的，则返回 0。
  - 如果交易是 SSLv2，则返回 0x002。
  - 如果交易是 SSLv3，则返回 0x300。
  - 如果交易是 TLSv1，则返回 0x301。
- 您必须启用 SSLv3（或其他早期版本）才能触发响应程序策略。

  例如，如果 NetScaler 设备上禁用了 SSLv3，并且具有使用 SSLv3 的旧版浏览器的客户端尝试连接，则访问将被拒绝。
- 如果您的部署在指定的时间段（一两个月）内需要 SSLv3 或更早版本，请配置以下内容：
  - 启用 SSLv3 协议。
  - 更新自定义页面以包含在指定时间段之后浏览器无法连接到设备的信息。

使用 **NetScaler Gateway** 配置无客户端 **VPN** 访问

February 1, 2024

无客户端访问允许用户获得所需的访问权限，无需他们安装用户软件，例如 Citrix Secure Access 客户端或 Receiver。用户可以使用其 Web 浏览器连接到 Web 应用程序，例如 Outlook Web Access。

您可以使用以下步骤配置无客户端访问：

- 全局或使用绑定到用户、组或虚拟服务器的会话策略启用无客户端访问。
- 选择 Web 地址编码方法。

要仅对特定虚拟服务器启用无客户端访问，请在全局范围内禁用无客户端访问，然后创建会话策略以启用它。

如果使用 NetScaler Gateway 向导配置设备，则可以选择在向导中配置无客户端访问。向导中的设置将全局应用。在 NetScaler Gateway 向导中，您可以配置以下客户端连接方法：

- Citrix Secure Access 客户端。用户只能使用 Citrix Secure Access 客户端登录。
- 使用 Citrix Secure Access 客户端，允许访问场景回退。用户使用 Citrix Secure Access 客户端登录 NetScaler Gateway。如果用户设备未能通过端点分析扫描，则允许用户使用无客户端访问登录。发生这种情况时，用户对网络资源的访问权限有限。
- 允许用户使用 Web 浏览器和无客户端访问登录。用户只能使用无客户端访问登录，并获得对网络资源的有限访问权限。

无客户端 **VPN** 访问策略的工作原理

可以通过创建策略配置对 Web 应用程序的无客户端访问。您可以在配置实用程序中配置无客户端访问策略的设置。无客户端访问策略由规则和配置文件组成。您可以使用 NetScaler Gateway 随附的预配置的无客户端访问策略。您还可以创建自己的自定义无客户端访问策略。

NetScaler Gateway 为以下内容提供了预配置的策略：

- Outlook Web 访问和 Outlook Web 应用程序
- SharePoint 2007
- 所有其他 Web 应用程序

> 注意：
>
> 只有使用高级无客户端访问才能支持 OWA 2016 和 SharePoint 2016。

请记住预配置的无客户端访问策略的以下特征：

- 它们是自动配置的，无法更改。
- 每个策略都在全球范围内受到约束。

- 除非您在全局或通过创建会话策略启用无客户端访问，否则不会强制执行每个策略。
- 即使未启用无客户端访问，也无法删除或修改全局绑定。

对其他 Web 应用程序的支持取决于您在 NetScaler Gateway 上配置的重写策略。Citrix 建议测试您创建的所有自定义策略，以确保成功重写应用程序的所有组件。

如果您允许来自 Receiver for Android、适用于 iOS 的 Receiver 或 Citrix Secure Hub 的连接，则必须启用无客户端访问。对于在 iOS 设备上运行的 Citrix Secure Hub，还必须在会话配置文件中启用 Secure Browse。Secure Browse 和无客户端访问协同工作，允许来自 iOS 设备的连接。如果用户未连接 iOS 设备，则不必启用 Secure Browse。

快速配置向导可为移动设备配置正确的无客户端访问策略和设置。Citrix 建议运行快速配置向导，为与 StoreFront 和 Citrix Endpoint Management 的连接配置正确的策略。

您可以将自定义无客户端访问策略全局绑定或绑定到虚拟服务器。如果要将无客户端访问策略绑定到虚拟服务器，则需要创建自定义策略，然后将其绑定。要对全局或虚拟服务器实施不同的无客户端访问策略，请更改自定义策略的优先级编号，使其编号低于预配置的策略，从而使自定义策略的优先级更高。如果没有其他无客户端访问策略绑定到虚拟服务器，则优先使用预配置的全局策略。

> 注意：
>
> 您不能更改预配置的无客户端访问策略的优先级编号。

启用无客户端 **VPN** 访问

在全局级别启用无客户端访问时，所有用户都会收到无客户端访问的设置。您可以使用 NetScaler Gateway 向导、全局策略或会话策略来启用无客户端访问。

在全局设置或会话配置文件中，无客户端访问具有以下设置：

- 开。启用无客户端访问。如果禁用客户端选择但未配置或禁用 StoreFront，则用户将使用无客户端访问进行登录。
- 关。默认情况下不启用无客户端访问。用户使用 Citrix Secure Access 客户端登录后，将启用无客户端访问。如果您禁用客户端选项，但未配置或禁用 StoreFront，则用户将使用 Citrix Secure Access 客户端登录。如果用户登录时端点分析失败，则用户会收到具有无客户端访问权限的选择页面。
- 已禁用。无客户端访问已禁用。当您选择 禁用时，用户将无法使用无客户端访问进行登录，并且无客户端访问的图标不会出现在选择页面上。

如果未使用 NetScaler Gateway 向导启用无客户端访问，则可以使用配置实用程序全局或在会话策略中启用无客户端访问。

在全局启用无客户端访问

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。

2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上的“无客户端访问”旁边，选择“开”，然后单击“确定”。

使用会话策略启用无客户端访问

如果只希望选定的一组用户、组或虚拟服务器使用无客户端访问，请在全局范围内禁用或清除无客户端访问。然后，使用会话策略启用无客户端访问并将其绑定到用户、组或虚拟服务器。

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略 **>** 会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“客户体验”选项卡上，在“无客户端 访问权限”旁边，单击“覆盖全局”，选择“打开”，然后单击“创建”。
7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。
8. 单击“创建”，然后单击“关闭”。

创建启用无客户端访问的会话策略后，将其绑定到用户、组或虚拟服务器。

对 **Web** 地址进行编码

启用无客户端访问时，您可以选择对内部 Web 应用程序的地址进行编码或将地址保留为明文。这些设置是：

- 晦涩难懂。这使用标准的编码机制来掩盖资源的域和协议部分。
- 清楚。该 Web 地址未经编码，用户可以看到。
- 加密。使用会话密钥对域和协议进行加密。加密 Web 地址后，同一 Web 资源的每个用户会话的 URL 都不同。如果用户将编码后的 Web 地址添加为书签，请将其保存在 Web 浏览器中然后注销，当用户登录并尝试使用书签再次连接到该 Web 地址时，他们将无法连接到该 Web 地址。
  注意：如果用户在会话期间将加密的书签保存在访问界面中，则每次用户登录时书签都会起作用。

您可以全局配置此设置，也可以作为会话策略的一部分进行配置。如果将编码配置为会话策略的一部分，则可以将其绑定到用户、组或虚拟服务器。

全局配置 **Web** 地址编码

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“客户端体验”选项卡上的“无客户端访问 URL 编码”旁边，选择编码级别，然后单击“确定”。

通过创建会话策略来配置 **Web** 地址编码

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在“客户端体验”选项卡上，在“无客户端访问 URL 编码”旁边，单击“覆盖全局”，选择编码级别，然后单击“确定”。
7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建无客户端访问策略

如果要使用与默认无客户端访问策略相同的设置，但要将策略绑定到虚拟服务器，则可以复制默认策略，为策略提供新名称。您可以使用配置实用程序复制默认策略。

将新策略绑定到虚拟服务器后，可以设置策略的优先级，以便在用户登录时首先运行该策略。

使用默认设置创建无客户端访问策略

1. 在配置实用程序的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击无客户端访问。
2. 在详细信息窗格的策略选项卡上，单击默认策略，然后单击添加。
3. 在名称中，键入策略的新名称，单击创建，然后单击关闭。

将无客户端访问策略绑定到虚拟服务器

创建策略后，将其绑定到虚拟服务器。

1. 在配置实用程序的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“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“打开”。
3. 在配置 NetScaler Gateway 虚拟服务器对话框中，单击策略选项卡，然后单击无客户端。
4. 单击“插入策略”，从列表中选择一个策略，然后单击“确定”。

创建和评估无客户端访问策略表达式

当您为无客户端访问创建策略时，可以为该策略创建自己的表达式。创建完表达式后，可以计算表达式的准确性。

1. 在配置实用程序的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击无客户端访问。
2. 在详细信息窗格的策略选项卡上，单击默认策略，然后单击添加。

3. 在名称中，键入策略的名称。
4. 在“配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 配置重写设置，然后单击创建。
7. 在“创建无客户端访问策略”对话框的“表达式”下，单击“添加”。
8. 在“添加表达式”对话框中，创建表达式，然后单击“确定”。
9. 在“创建无客户端访问策略”对话框中，单击“评估”，如果表达式测试正确，请单击“创建”。

使用 **NetScaler Gateway** 进行高级无客户端 **VPN** 访问

February 1, 2024

无客户端 VPN 提供了一种通过 NetScaler Gateway 提供对公司内部网资源的远程访问的方法，而无需在客户端计算机上安装 VPN 客户端应用程序。无客户端 VPN 使用客户端的 Web 浏览器提供对企业 Web 应用程序、门户和其他资源的远程访问。
高级无客户端 VPN 解决方案消除了以下与无客户端 VPN 有关的限制：

- 有时无法识别相对 URL。
- 无法识别动态生成的相对 URL。

先进的无客户端 VPN 可以识别绝对 URL 和主机名，并以全新且独特的方式重写它们，而不是尝试重写 HTTP 响应/网页中存在的相对 URL。SharePoint 不再需要使用默认文件夹来重写 URL，并且支持自定义 SharePoint 访问权限。

必备条件

以下是配置高级无客户端 VPN 的先决条件。

- 通配符服务器证书 -高级无客户端 VPN 以独特的方式重写 URL。每个用户的每个 URL 都会保持这种唯一性。例如，如果 Web 应用程序托管在上 `https://webapp.customer.com`，VPN 虚拟服务器托管在上 `https://vpn.customer.com`，则高级无客户端 VPN 会将其重写为 `https://cvpneqwerty.vpn.customer.com`。这意味着，每个 URL 都被重写为 VPN 虚拟服务器的子域。在这个新的 URL 中，`cvpneqwerty` 可以解密回 `https://webapp.customer.com`。字符串 `cvpneqwerty` 是动态的，因此对于 SSL，必须使用通配符证书绑定 VPN 虚拟服务器。

  如果服务器使用托管 `https://vpn.customer.com`，那么服务器证书现在必须包含（vpn.customer.com 和.vpn.customer.com）的条目作为 CN 或 SAN 证书的一部分（其中 CN = 普通名称，SAN= 使用者备用名称）。在 NetScaler Gateway 上，绑定此证书的过程保持不变。
  注意：通配符证书只支持一级证书（即 ..customer.com 是不允许的）。如果您已经在使用通配符证书（用于 *.customer.com）并进行托管 `https://vpn.customer.com`，则这不适用于高级无客户端 VPN。您必须使用获得新证书 `*.vpn.customer.com`。

- 通配符 **DNS** 条目 -客户端（Web 浏览器）必须解析高级无客户端 VPN 应用程序的 FQDN。在设置 NetScaler Gateway 服务器时，您必须已配置 DNS 条目才能解析 vpn.customer.com。这允许浏览器将 vpn.customer.com 解析为您的 VPN 虚拟服务器的 IP 地址。要将诸如 `https://cvpnqwerty.vpn.customer.com` 等的 URL 解析为相同 IP（VPN 虚拟服务器的 IP 地址），必须为 `vpn.customer.com` 的域添加新记录。在 DNS 服务器中找到域设置，然后使用与之前相同的 IP 地址为“*”添加新的主机记录。添加主机记录后，您必须看到成功的 ping 响应 `https://cpvnanything.vpn.customer.com`。

配置高级无客户端 **VPN** 访问

要使用命令行界面配置高级无客户端 **VPN** 访问，请在命令提示符下键入：

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

如果会话操作绑定到虚拟服务器，则还必须为该会话操作启用高级无客户端 VPN 模式选项。

示例：

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```

要使用 **NetScaler GUI** 配置高级无客户端 **VPN** 访问，请执行以下操作：

1. 在 NetScaler GUI 中，导航到“配置”**>**“**NetScaler**”**>**“全局设置”。
2. 在“全局设置”页面上，单击“更改全局设置”，然后选择“客户端体验”选项卡。
3. 在“客户端体验”选项卡上的“无客户端访问”列表中，单 击“开”。
4. 在“客户端体验”选项卡上的“高级无客户端 **VPN** 模式”列表中，单击“启用”。
   如果从“高级无客户端 **VPN** 模式”列表中选择“严格”，NetScaler 设备将仅响应经典无客户端 VPN 形式的 StoreFront URL，并阻止所有其他经典的无客户端 VPN 请求。此选项在设备上提供了更安全的配置，用于交付内部 Web 资源。

> 注意：
>
> - 如果会话操作绑定到虚拟服务器，则必须为该会话操作以及从 配置 **NetScaler Gateway** 会话配置文件页面的“客 户端体验”选项卡启用“高级无客户端 VPN 模式”选项 卡。
> - 您可以选择 覆盖全局 选项来覆盖全局设置。
> - 您也可以在会话级别配置高级无客户端 VPN 功能。

注意事项

高级无客户端 VPN 旨在提供对企业 Web 应用程序的访问权限。此类应用对于所需的每种资源（JavaScript、css、图像等）只有一个 FQDN。由于我们将内部应用程序的完整 FQDN 编码为单八位字节（无客户端 VPN），因此我们失去了

子域关系。因此，每当使用 CORS 配置企业 WebApp 时，有时您在通过高级无客户端 VPN 访问它时可能会注意到问题。

为用户配置域访问权限

February 1, 2024

如果用户使用无客户端访问进行连接，则可以限制允许用户访问的网络资源、域和网站。您可以使用 NetScaler Gateway 向导或全局设置创建用于包括或排除对域的访问权限的列表。

您可以允许访问所有网络资源、域和网站，然后创建排除列表。排除列表引用了不允许用户访问的一组特定资源。用户无法访问排除列表中的任何域。

您还可以拒绝访问所有网络资源、域和网站，然后创建特定的包含列表。包含列表引用了用户可以访问的资源。用户无法访问未出现在列表中的任何域。

注意：如果为 Citrix Endpoint Management 或 StoreFront 配置无客户端访问策略，并且用户连接到 Receiver for Web，则需要允许 Receiver for Web 可以访问的域。这是必需的，因此 NetScaler Gateway 可以为 StoreFront 和 Endpoint Management 重写网络流量。

使用 **NetScaler Gateway** 向导配置域访问权限

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 NetScaler Gateway。
2. 在详细信息窗格的入门下，单击 NetScaler Gateway 向导。
3. 单击“下一步”，然后按照向导中的说明进行操作，直到到达“配置无客户端访问”页。
4. 单击配置域以进行无客户端访问，然后执行以下操作之一：
    - 要创建排除的域列表，请单击排除域。
    - 要创建包含的域的列表，请单击允许域。
5. 在域名下，键入域名，然后单击添加。
6. 对要添加到列表中的每个域重复步骤 5，完成后单击“确定”。
7. 使用 NetScaler Gateway 向导继续配置设备。

使用配置实用程序配置域设置

您还可以使用配置实用程序中的全局设置来创建或修改域列表。

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的无客户端访问下，单击为无客户端访问配置域。
3. 执行以下操作之一：

- 要创建排除的域列表，请单击排除域。
- 要创建包含的域的列表，请单击允许域。

4. 在域名下，键入域名，然后单击添加。
5. 对要添加到列表中的每个域重复步骤 4，完成后单击“确定”。

使用 **SharePoint 2003**、**SharePoint 2007** 和 **SharePoint 2013** 的无客户端 **VPN** 访问

February 1, 2024

NetScaler Gateway 可以重写来自一个或多个 SharePoint 2003、SharePoint 2007 或 SharePoint 2013 网站的内容，这样用户就可以在不需要 Citrix Secure Access 客户端的情况下访问这些内容。要成功完成重写过程，必须为 NetScaler Gateway 配置网络中每个 SharePoint 服务器的主机名。

您可以使用 NetScaler Gateway 向导或配置实用程序来配置 SharePoint 站点的主机名。

在 NetScaler Gateway 向导中，浏览向导以配置设置。进入“配置无客户端访问”页时，键入 SharePoint 站点的 Web 地址，然后单击“添加”。

要在运行 NetScaler Gateway 向导后首次添加更多网站或配置 SharePoint，请使用配置实用程序。

> 重要提示：
>
> 经典无客户端访问支持 SharePoint 2013 和 OWA 2013 之前的版本。高级无客户端访问支持 SharePoint 2016 和 OWA 2016 及更高版本。

使用 **NetScaler** 图形用户界面为 **SharePoint** 配置无客户端访问

1. 导航到 **NetScaler Gateway** > 全局设置。
2. 在详细信息窗格中的无客户端访问下，单击 为 **SharePoint** 配置无客户端访问。
3. 在 SharePoint 的无客户端访问下，在 SharePoint 服务器的主机名中，键入 SharePoint 站点的主机名，然后单击 添加。
4. 对要添加到列表中的每个 SharePoint 站点重复步骤 3，然后在完成后单 击“确定”。

将 **SharePoint** 站点设置为主页

如果要将 SharePoint 站点设置为用户的主页，请配置会话配置文件并输入 SharePoint 站点的主机名。

将 **SharePoint** 站点配置为主页

1. 导航到 **NetScaler Gateway >** 策略，然后单击 会话。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在“客户端体验”选项卡上的“主页”旁边，单击“覆盖全局”，然后键入 SharePoint 站点的名称。
7. 在无客户端访问旁边，单击 覆盖全局，选择 开，然后单击 创建。
8. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

完成会话策略后，将其绑定到用户、组、虚拟服务器或全局。当用户登录时，他们会将 SharePoint 网站视为他们的主页。

为 **SharePoint 2007** 服务器启用名称解析

SharePoint 2007 服务器将配置的服务器名称作为响应的一部分在各个 URL 中的主机名发送。如果配置的 SharePoint 服务器名称不是完全限定域名 (FQDN)，NetScaler Gateway 将无法使用 SharePoint 服务器名称解析 IP 地址，并且某些用户函数超时并显示错误消息“HTTP: 1.1 网关超时”。这些功能可以包括签入和签出文件、查看工作区以及在用户使用无客户端访问登录时上载多个文件。

要解决此问题，您可以尝试以下方法之一：

- 在 NetScaler Gateway 上配置 DNS 后缀，以便在名称解析之前将 SharePoint 主机名转换为 FQDN。
- 在 NetScaler Gateway 上为每个 SharePoint 服务器名称配置一个本地 DNS 条目。
- 更改所有 SharePoint 服务器名称以使用 FQDN，例如 Sharepoint.Intranet 域名而不是 SharePoint，

配置 **DNS** 后缀

1. 在配置实用程序的配置选项卡的导航窗格中，展开 **DNS** ，然后单击 **DNS** 后缀。
2. 在详细信息窗格中，单击“添加”。
3. 在 **DNS** 后缀中，键入 Intranet 域名作为后缀，单击 创建，然后单击 关闭。

您可以为要添加的每个域重复步骤 3。

为 **NetScaler Gateway** 上的每个 **SharePoint** 服务器名称配置本地 **DNS** 记录

1. 在配置实用程序的导航窗格中，展开 **DNS >** 记录，然后单击 地址记录。
2. 在详细信息窗格中，单击“添加”。
3. 在 主机名中，键入 DNS 地址记录的 SharePoint 主机名。

4. 在“**IP** 地址”中，键入 SharePoint 服务器的 IP 地址，单击“添加”，单击“创建”，然后单击“关闭”。

为其添加 A 记录的主机名不得有 CNAME 记录。此外，设备上不能有重复的 A 记录。

启用无客户端 **VPN** 访问持久 **Cookie**

February 1, 2024

访问 SharePoint 的某些功能(例如打开和编辑 SharePoint 服务器上托管的 Microsoft Word、Excel 和 PowerPoint 文档）需要持久性 Cookie。

永久性 Cookie 会保留在用户设备上，并随每个 HTTP 请求一起发送。NetScaler Gateway 会在将永久性 Cookie 发送到用户设备上的插件之前对其进行加密，并且只要会话存在，就会定期刷新 Cookie。如果会话结束，cookie 将变为陈旧。

在 NetScaler Gateway 向导中，管理员可以在全局范围内启用持久性 Cookie。您还可以创建会话策略，以便为每个用户、组或虚拟服务器启用永久性 Cookie。

以下选项可用于永久性 Cookie：

- 允许启用永久性 Cookie，用户可以打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 拒绝会禁用永久性 Cookie，并且用户无法打开和编辑存储在 SharePoint 中的 Microsoft 文档。
- 提示提示用户在会话期间允许或拒绝持久性 Cookie。

如果用户未连接到 SharePoint，则无客户端访问不需要持久 Cookie。

为 **SharePoint** 的无客户端 **VPN** 访问配置永久性 **Cookie**

您可以在全局范围内或作为会话策略的一部分为 SharePoint 的无客户端访问配置永久性 Cookie。

要全局配置持久性 **Cookie**

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格中的“Settings”（设置）下，单击“Change global settings”（更改全局设置）。
3. 在“客户端体验”选项卡上的“无客户端访问持久 Cookie”旁边，选择一个选项，然后单击“确定”。

将持久性 **Cookie** 配置为会话策略的一部分

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。

4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在“客户端体验”选项卡上的“无客户端访问持久 Cookie”旁边，单击“覆盖全局”，选择一个选项，然后单击“创建”。
7. 在创建身份验证策略对话框的命名表达式旁边，选择常规，选择 True 值，单击添加表达式，单击创建，然后单击关闭。

适用于移动设备的 **Citrix SSO VPN** 客户端

February 1, 2024

Citrix SSO 是适用于移动设备（macOS、iOS 和 iOS）的 VPN 客户端。Citrix SSO 在 macOS、iOS 和 Android 系统上提供完整的移动设备管理 (MDM) 支持。使用 MDM 服务器，管理员可以远程配置和管理设备级别的 VPN 配置文件和 PerApp VPN 配置文件。
Citrix SSO 还支持大多数常用功能。

引用

- Citrix Secure Access 客户端
- NetScaler Gateway VPN 客户端和支持的功能

配置“客户端选择”页面

February 1, 2024

您可以将 NetScaler Gateway 配置为向用户提供多个登录选项。通过配置客户端选择页面，用户可以选择使用以下选项从一个位置登录：

- 适用于 Windows 的 Citrix Secure Access 客户端
- 适用于 macOS X 的 Citrix Secure Access 客户端
- StoreFront
- Web Interface
- 无客户端访问

用户使用绑定到 NetScaler Gateway 或虚拟服务器的证书中的 Web 地址登录 NetScaler Gateway。通过创建会话策略和配置文件，您可以确定用户收到的登录选项。根据 NetScaler Gateway 的配置方式，客户端选择页面最多显示三个图标，表示以下登录选项：

- 网络访问。当用户首次使用 Web 浏览器登录 NetScaler Gateway，然后选择网络访问时，将显示下载页面。当用户单击“下载”时，插件将下载并安装在用户设备上。下载和安装完成后，将显示访问界面。如果您安装了更新版本或恢复到较旧版本的 NetScaler Gateway，适用于 Windows 的 Citrix Secure Access 客户端会以静默方式升级或降级到设备上的版本。如果用户使用适用于 Mac 的 Citrix Secure Access 客户端进行连接，则在用户登录时检测到新的设备版本时，插件会静默升级。此版本的插件不会以静默方式降级。
- Web Interface 或 StoreFront。如果用户选择要登录的 Web Interface ，将显示 Web Interface 页面。然后，用户可以访问其发布的应用程序或虚拟桌面如果用户选择 StoreFront 登录，Receiver 将打开，用户可以访问应用程序和桌面。
  注意：如果将 StoreFront 配置为客户端选项，则应用程序和桌面不会显示在访问界面的左窗格中。
- 无客户端访问。如果用户选择无客户端访问进行登录，则会显示访问界面或您的自定义主页。在访问界面中，用户可以导航到文件共享、网站和使用 Outlook Web Access。

Secure Browse 允许用户从 iOS 设备通过 NetScaler Gateway 进行连接。如果启用 Secure Browse，则当用户使用 Secure Hub 登录时，Secure Browse 将禁用客户端选择页面。

登录时显示“客户端选择”页

启用客户端选择选项后，用户可以在成功对 NetScaler Gateway 进行身份验证后使用 Citrix Secure Access 客户端、Web Interface、Receiver 或无客户端访问登录。登录成功后，网页上会显示图标，用户可以从中选择建立连接的方法。

您可以启用客户端选择，而无需使用端点分析或实施访问方案回退。如果未定义客户端安全表达式，则用户会收到 NetScaler Gateway 上配置的设置的连接选项。如果用户会话存在客户端安全表达式，并且用户设备未能通过端点分析扫描，则选择页面将仅提供使用 Web Interface 的选项（如果已配置）。否则，用户可以使用无客户端访问权限登录。

您可以全局配置客户端选择，也可以使用会话配置文件和策略来配置

> 重要：
>
> 配置客户端选项时，请勿配置隔离组。未通过端点分析扫描且被隔离和对待的用户设备与通过端点扫描的用户设备相同的用户设备。

全局启用客户选择选项

1. 在 GUI 中的配置选项卡的导航窗格中，展开 **NetScaler Gateway** ，然后单击 全局设置。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上，单击“高级设置”。
4. 在常规选项卡上，单击 客户端选择，然后单击 确定。

启用客户端选择作为会话策略的一部分

您还可以将客户端选择配置为会话策略的一部分，然后将其绑定到用户、组和虚拟服务器。

1. 在 GUI 中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击 会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在客户端体验选项卡上，单击 高级。
7. 在“常规”选项卡上的“客户端选择”旁边，单击“覆盖全局”、“客户端选择”、“确定”，然后单击“创建”。
8. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置客户端选择选项

除了使用会话配置文件和策略启用客户端选择之外，还需要配置用户软件的设置。例如，您希望用户使用 Citrix Secure Access 客户端、StoreFront 或 Web Interface 或无客户端访问登录。创建一个启用所有三个选项和客户端选项的会话配置文件。然后，创建一个会话策略，其表达式设置为 True 值并附加了配置文件。接下来，将会话策略绑定到虚拟服务器。

在创建会话策略和配置文件之前，您需要为用户创建一个授权组。

创建授权组

1. 在配置实用程序中的配置选项卡的导航窗格中，**NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，单击“添加”。
3. 在 组名称中，键入组的名称。
4. 在“用户”选项卡上，选择用户，为每个用户单击“添加”，单击“创建”，然后单击“关闭”。

以下过程是使用 Citrix Secure Access 客户端、StoreFront 和无客户端访问进行客户端选择的会话配置文件示例。

为客户选择创建会话配置文件

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略 **>** 会话。
2. 在详细信息窗格中，单击“配置文件”选项卡，然后单击“添加”。
3. 在名称中，键入配置文件的名称。
4. 在“客户端体验”选项卡上，执行以下操作：

    a) 在“主页”旁边，单击“覆盖全局”，然后清除“显示主页”。这将禁用访问接口。
    b) 在“无客户端访问”旁边，单击“覆盖全局”，然后选择“关”。

c) 在“插件类型”旁边，单击“覆盖全局”，然后选择 Windows/Mac OS X。
d) 单击 高级设置，然后在 客户端选择旁边单击 覆盖全局，然后单击 客户端选择

5. 在 安 全选项卡上的 默认授权操作旁边，单击 覆盖全局，然后选择 允许。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在 授权组下，单击 覆盖全局，单击 添加，然后选择组。
8. 在 已发布的应用程序 选项卡上，执行以下操作

a) 在 **ICA** 代理旁边，单击“覆盖全局”，然后选择“关”。
b) 在“**Web Interface** 地址”旁边，单击“覆盖全局”，然后键入 StoreFront 的 Web 地址，例如 http://ipAddress/Citrix/。
c) 在 **Web Interface** 门户模式旁边，单击 覆盖全局，然后选择 **COMPAC**T。
d) 在 单点登录域旁边，单击 覆盖全局，然后键入域的名称。

9. 单击“创建”，然后单击“关闭”。

如果您想使用适用于 Java 的 Citrix Secure Access 客户端作为客户端选择，请在客户端体验选项卡的插件类型中选择 **Java**。如果选择此选项，则必须配置 Intranet 应用程序并将拦截模式设置为代理。

创建会话配置文件后，创建会话策略。在策略中，选择配置文件，然后将表达式设置为 True 值。

要使用 StoreFront 作为客户端选择，还必须在 NetScaler Gateway 上配置 Secure Ticket Authority (STA)。STA 绑定到虚拟服务器。

> 注意：
>
> 如果运行 StoreFront 的服务器不可用，则 Citrix Virtual Apps 选项不会显示在选择页面上。

全局配置 **STA** 服务器

1. 在配置实用程序中的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“服务器”下，单击“绑定/取消绑定 **STA** 服务器”以供安全票证颁发机构使用。
3. 在“绑定 /取消绑定 **STA** 服务器”对话框中，单击“添加”。
4. 在“配置 **STA** 服务器”对话框的“URL”中，键入 STA 服务器的 Web 地址，然后单击“创建”。
5. 重复步骤 3 和 4 以添加更多 STA 服务器，然后单击“确定”。

将 **STA** 绑定到虚拟服务器

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击 **Open**（打开）。
3. 在 已发布的应用程序 选项卡上的 **Secure Ticket Authority** 发机构下的 活动下，选择 STA 服务器，然后单击 确定。

您还可以在 已发布的应用程序 选项卡上添加 STA 服务器

配置访问方案回退

February 1, 2024

SmartAccess 允许 NetScaler Gateway 根据端点分析扫描的结果自动确定允许用户设备使用的访问方法。如果用户设备未通过初始端点分析扫描，Accessecure Access fallback 允许用户设备使用 Citrix Workspace 应用程序从 Citrix Secure Access 客户端回退到 Web Interface 或 StoreFront，从而进一步扩展了此功能。

要启用访问方案回退，请配置身份验证后策略，以确定用户在登录 NetScaler Gateway 时是否收到替代访问方法。此身份验证后策略定义为客户端安全表达式，您可以全局配置或作为会话配置文件的一部分进行配置。如果配置会话配置文件，则该配置文件将与会话策略相关联，然后将其绑定到用户、组或虚拟服务器。启用访问方案回退时，NetScaler Gateway 将在用户身份验证后启动端点分析扫描。不符合身份验证后回退扫描要求的用户设备的结果如下：

- 如果启用了客户端选项，则用户只能使用 Citrix Workspace 应用程序登录 Web Interface 或 StoreFront。
- 如果禁用了无客户端访问和客户端选择，则可以将用户隔离到仅提供 Web Interface 或 StoreFront 访问权限的组中。
- 如果 NetScaler Gateway 上启用了无客户端访问和 Web Interface 或 StoreFront，并且禁用了 ICA 代理，则用户将回退到无客户端访问。
- 如果未配置 Web Interface 或 StoreFront 且无客户端访问设置为允许，则用户将回退到无客户端访问。

禁用无客户端访问时，必须为访问方案回退配置以下设置组合：

- 为身份验证后备扫描定义客户端安全参数。
- 定义 Web Interface 主页。
- 禁用客户端选择。
- 如果用户设备未通过客户端安全检查，则会将用户置于隔离组中，该组仅允许访问 Web Interface 或 StoreFront 以及已发布的应用程序。

为访问方案回退创建策略

要配置 NetScaler Gateway 以进行访问方案回退，您需要通过以下方式创建策略和组：

- 创建一个隔离组，如果端点分析扫描失败，用户将被放置在该组中。
- 创建在端点分析扫描失败时使用的全局 Web Interface 或 StoreFront 设置。
- 创建覆盖全局设置的会话策略，然后将会话策略绑定到组。
- 创建在端点分析失败时应用的全局客户端安全策略。

配置访问方案回退时，请遵循以下准则：

- 要使用客户端选择或访问方案回退，所有用户都需要使用 Endpoint Analysis 插件。如果端点分析无法运行，或者用户在扫描期间选择了跳过扫描，则拒绝用户访问。
  注意：NetScaler Gateway 10.1 版本 120.1316.e 中删除了跳过扫描的选项。

- 启用客户端选项后，如果用户设备未能通过端点分析扫描，用户将被置于隔离组中。用户可以继续使用 Citrix Secure Access 客户端或 Citrix Workspace 应用程序登录 Web Interform 或 StoreFront。
  注意：如果启用客户端选项，Citrix 建议您不要创建隔离组。未能通过端点分析扫描的用户设备将被隔离，其处理方式与通过端点扫描的用户设备的处理方式相同。
- 如果端点分析扫描失败并将用户置于隔离组中，则绑定到隔离组的策略只有在没有直接绑定到该用户且优先级编号与绑定到隔离组的策略相同或低的策略时，绑定到隔离组的策略才有效。
- 您可以为访问界面和 Web Interface 或 StoreFront 使用不同的 Web 地址。配置主页时，Citrix Secure Access 客户端的访问接口主页优先，Web Interface 用户优先使用 Web Interface 主页。Citrix Workspace 应用程序主页优先于 StoreFront。

创建隔离组

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，单击“添加”。
3. 在“组名”中，键入组的名称，单击“创建”，然后单击“关闭”。
   重要：隔离组的名称不得与用户可能属于的任何域组的名称匹配。如果隔离组与 Active Directory 组名称匹配，则即使用户设备通过了端点分析安全扫描，也会隔离用户。

创建组后，将 NetScaler Gateway 配置为在用户设备无法通过端点分析扫描时回退到 Web Interface 。

配置设置以隔离用户连接

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 **NetScaler Gateway** 设置”对话框中，在“已发布的应用程序”选项卡上的 **ICA** 代理旁边，选择“关”。
4. 在 **Web Interface** 地址旁边，键入 StoreFront 或 Web Interface 的 Web 地址。
5. 在 单点登录域旁边，键入 Active Directory 域的名称，然后单击 确定。

配置全局设置后，创建覆盖全局 ICA 代理设置的会话策略，然后将会话策略绑定到隔离组。

为访问方案回退创建会话策略

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“已发布的应用程序”选项卡上，单击 **ICA Proxy** 旁边的“覆盖全局”，选择“开”，然后单击“创建”
6. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建会话策略后，将策略绑定到隔离组。

将会话策略绑定到隔离组

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
2. 在详细信息窗格中，选择一个组，然后单击 打开。
3. 单击会话。
4. 在“策 略”选项卡上，选择“会话”，然后单击“插入策略”。
5. 在“策略名称”下，选择策略，然后单击“确定”。

在 NetScaler Gateway 上创建启用 Web Interface 或 StoreFront 的会话策略和配置文件后，创建全局客户端安全策略。

创建全局客户端安全策略

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。
4. 在 客户端安全中，输入表达式。有关配置系统表达式的详细信息，请参阅 配置系统表达式 和 配置复合客户端安全
5. 在 隔离组中，选择在组过程中配置的组，然后单击 确定。

为 **Citrix Secure Access** 客户端配置连接

February 1, 2024

您可以通过定义用户可以在内部网络中访问的资源来配置用户设备连接。配置用户设备连接包括：

- 定义允许用户访问的域。
- 为用户配置 IP 地址，包括地址池（Intranet IP）。
- 配置超时设置。
- 配置单点登录。
- 配置客户端拦截。
- 配置拆分通道。
- 通过代理服务器配置连接。
- 配置用户软件以通过 NetScaler Gateway 进行连接。
- 配置移动设备的访问权限。

您可以使用作为会话策略一部分的配置文件来配置大多数用户设备连接。您还可以使用 Intranet 应用程序、预身份验证和流量策略来定义用户设备连接设置。

> 注意：
>
> Windows VPN 插件和 EPA 插件收集各种操作的遥测数据。要禁用该功能，请在客户端计算机上执行以下操作。
>
> 将 REG_DWORD 类型的注册表“HKLM\Software\Citrix\Secure Access Client\DisableGA”设置为 1。

配置用户会话的数量

February 1, 2024

您可以在特定时间点（全局级别或每个虚拟服务器级别）配置允许连接到 NetScaler Gateway 的最大用户数。当连接到设备的用户数超过您配置的值时，不会在 NetScaler Gateway 上创建会话。如果用户数超过允许的数量，用户会收到一条错误消息。

设置全局用户限制

在全局配置用户限制时，该限制适用于与系统中不同虚拟服务器建立会话的所有用户。当用户会话数达到您设置的值时，无法在 NetScaler Gateway 上的任何虚拟服务器上建立新会话。

在为 NetScaler Gateway 设置默认身份验证类型时，可以在全局级别设置最大用户数。

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改身份验证设置”。
3. 在“全局身份验证设置”对话框的“最大用户数”中，键入用户数，然后单击“确定”。

设置每个虚拟服务器的用户限制

您还可以将用户限制应用于系统上的每个虚拟服务器。在为每个虚拟服务器配置用户限制时，该限制仅适用于与特定虚拟服务器建立会话的用户。与其他虚拟服务器建立会话的用户不受此限制的影响。

1. 在配置实用程序的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击虚拟服务器，然后单击打开。
3. 在“最大用户数”中，键入用户数，然后单击“确定”。

配置超时设置

February 1, 2024

如果在指定的分钟数内连接上没有活动，则可以将 NetScaler Gateway 配置为强制断开连接。在会话超时（断开连接）前一分钟，用户会收到一条警报，指示会话已关闭。如果会话关闭，用户必须重新登录。

以下超时选项可用。

- 强制超时。如果启用此设置，则无论用户正在执行什么操作，NetScaler Gateway 都会在超时间隔过后断开会话连接。超时间隔过后，用户无法采取任何措施来防止断开连接。此设置适用于与 Citrix Secure Access 客户端、Citrix Workspace 应用程序、Secure Hub 或通过网络浏览器连接的用户。最小值为 1，最大值为 65535。
- 会话超时。如果启用此设置，如果在指定的时间间隔内未检测到任何网络活动，NetScaler Gateway 将断开会话连接。此设置适用于与 Citrix Secure Access 客户端、Citrix Workspace 应用程序、Citrix Secure Hub 或通过网络浏览器连接的用户。默认超时设置为 30 分钟。最小值为 1，最大值为 65535。
- 空闲会话超时。在指定时间间隔内没有用户活动（例如通过鼠标、键盘或触摸）时，Citrix Secure Access 客户端终止空闲会话的持续时间。此设置仅适用于连接到 Citrix Secure Access 客户端的用户。最小值为 1，最大值为 9999。

您可以通过输入 1 到 65536 之间的值来指定超时间隔的分钟数来启用任何超时设置。如果启用其中多个设置，则经过的第一个超时间隔将关闭用户设备连接。

您可以通过配置全局设置或使用会话配置文件来配置超时设置。将配置文件添加到会话策略时，该策略随后会绑定到用户、组或虚拟服务器。在全局配置超时设置时，这些设置将应用于所有用户会话。

> 注意：
>
> - 在始终开启（服务模式或用户模式）下，VPN 客户端会忽略所有超时。强制超时和会话超时决策在 NetScaler 设备上发生，因此这些超时按预期工作。如果发生此类超时，VPN 插件将尝试执行自动身份验证。
>
>   在 Always Oon 中，由于用户设备必须始终通过 VPN 通道连接，因此请勿配置强制超时或客户端空闲超时。但是，可以将会话超时配置为摆脱陈旧的会话。
> - 某些应用程序（如 Microsoft Outlook）会自动将网络流量探测器发送到电子邮件服务器，无需任何用户干预 Citrix 建议您将空闲会话超时配置为会话超时，以确保用户设备上无人值守的会话在合理的时间内超时。

配置强制超时

强制超时会在指定时间后自动断开 Citrix Secure Access 客户端的连接。您可以全局配置强制超时，也可以作为会话策略的一部分配置。

配置全局强制超时

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 NetScaler Gateway，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在 网络配置 选项卡上，单击 高级设置。
4. 在强制超时 (分钟) 中，键入用户可以保持连接的分钟数。

5. 在强制超时警告 (分钟) 中，键入在用户收到连接即将断开连接的警告之前的分钟数，然后单击 确定。

在会话策略中配置强制超时

如果要进一步控制谁会收到强制超时，请创建会话策略，然后将该策略应用于用户或组。

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway** > 策略，然后单击会话。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在 网络配置 选项卡上，单击 高级。
7. 在“超时”下，单击“覆盖全 局”，然后在“强制超时（分钟）”中键入用户可以保持连接的分钟数。
8. 在“强制超时警告（分钟）”旁边，单击“覆盖全局”，然后键入警告用户连接将断开的分钟数。单击确定两次。
9. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置会话或空闲超时

您可以使用 NetScaler GUI 在全局范围内配置会话和客户端超时设置或创建会话策略。创建会话策略和配置文件时，将表达式设置为 True。

> 注意：
>
> 如果您没有明确覆盖全局设置并在 客户端体验 **>** 会话超时（分钟）中设置会话超时，这可能会导致需要重新登录的身份验证循环。即使默认会话超时为 30 分钟，也会出现这种情况。

使用 **GUI** 全局配置会话或客户端空闲超时

1. 在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡上，执行以下一项或两项操作：
   - 在 会话超时 **(**分钟**)** 中，键入分钟数。
   - 在“客户端空闲超时 **(**分钟**)**”中，键入分钟数，然后单击“确定”。

使用 **GUI** 使用会话策略配置会话或客户端空闲超时设置

1. 在 配置 选项卡的导航窗格中，展开 **NetScaler Gateway** > 策略，然后单击 会话
2. 在 **NetScaler Gateway** 会话策略和配置文件 页面中，单击 会话配置文件，然后单击 添加。
3. 在“Name”（名称）中，键入配置文件的名称。

4. 在“客户端体验”选项卡上，执行以下一项或两项操作：
    - 在“会 话超时 **(**分钟**)**”旁边，单击“覆盖全局”，然后键入分钟数，然后单击“创建”。
    - 在“客户端空闲超时 **(**分钟**)**”旁边，单击“覆盖全局”，键入分钟数，然后单击“创建”。
5. a) 在 **NetScaler Gateway** 会话策略和配置文件 页面中，单击 会话策略，然后单击 添加。
6. 在 创建 **NetScaler Gateway** 会话策略中，
    - 在 名称中，输入策略的名称。
    - 在 配置文件中，选择用于指定满足规则条件时新会话策略要应用的操作的配置文件。
    - 选择 高级策略。
    - 在“表 达式”字段中，添加表达式或命名表达式的名称，指定与策略匹配的流量。
    - 单击“创建”，然后单击“关闭”。

连接到内部网络资源

February 1, 2024

您可以配置 NetScaler Gateway 以使用户能够访问内部网络中的资源。如果禁用拆分通道，则来自用户设备的所有网络流量都将发送到 NetScaler Gateway，并且授权策略将确定是否允许流量传递到内部网络资源。启用拆分通道时，只有目的地为内部网络的流量会被用户设备拦截并发送到 NetScaler Gateway。您可以使用 Intranet 应用程序配置 NetScaler Gateway 拦截的 IP 地址。

如果您使用适用于 Windows 的 Citrix Secure Access 客户端，请将拦截模式设置为透明。如果您使用的是适用于 Java 的 Citrix Secure Access 客户端，请将拦截模式设置为代理。将拦截模式设置为透明时，可以使用以下命令允许访问网络资源：

- 单个 IP 地址和子网掩码
- 一系列 IP 地址

如果将拦截模式设置为代理，则可以配置目标和源 IP 地址以及端口号。

配置对内部网络资源的网络访问

1. 在配置实用程序中的 配置 选项卡的导航窗格中，展开 NetScaler Gateway，展开资源，然后单击 **Intranet** 应用程序。
2. 在详细信息窗格中，单击“添加”。
3. 完成允许网络访问的参数，单击 创建，然后单击 关闭。

配置拆分通道

February 1, 2024

您可以启用分割通道以防止 Citrix Secure Access 客户端向 NetScaler Gateway 发送不必要的网络流量。

当您不启用分割通道时，Citrix Secure Access 客户端会捕获来自用户设备的所有网络流量，然后通过 VPN 通道将流量发送到 NetScaler Gateway。

如果您启用分割通道，Citrix Secure Access 客户端仅通过 VPN 通道发送发往受 NetScaler Gateway 保护的网络的流量。Citrix Secure Access 客户端不会将发往未受保护网络的网络流量发送到 NetScaler Gateway。

当 Citrix Secure Access 客户端启动时，它会从 NetScaler Gateway 获取内联网应用程序列表。Citrix Secure Access 客户端检查用户设备在网络上载输的所有数据包，并将数据包中的地址与内联网应用程序列表进行比较。如果数据包中的目标地址在其中一个内联网应用程序内，Citrix Secure Access 客户端将数据包通过 VPN 通道发送到 NetScaler Gateway。如果目标地址不在定义的 Intranet 应用程序中，则数据包不会加密，用户设备会适当地路由数据包。启用拆分通道时，Intranet 应用程序将定义被拦截的网络流量。

> 注意：
>
> 如果用户使用 Citrix Workspace 应用程序连接到服务器场中的已发布应用程序，则无需配置拆分通道。

NetScaler Gateway 还支持反向拆分通道，该通道定义 NetScaler Gateway 不会拦截的网络流量。如果将拆分通道设置为反向，则 Intranet 应用程序将定义 NetScaler Gateway 不会拦截的网络流量。启用反向剥离通道时，定向到内部 IP 地址的所有网络流量都会绕过 VPN 通道，而其他流量则通过 NetScaler Gateway。反向拆分通道可用于记录所有非本地 LAN 流量。例如，如果用户拥有家庭无线网络并使用 Citrix Secure Access 客户端登录，则 NetScaler Gateway 不会拦截发往打印机或无线网络中其他设备的网络流量。

有关 Intranet 应用程序的更多信息，请参阅 配置客户端拦截。

您可以将拆分通道配置为会话策略的一部分。

配置拆分通道

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 策略，然后单击“会话”。
2. 在详细信息窗格的 配置文件 选项卡上，选择一个配置文件，然后单击 打开。
3. 在 客户端体验 选项卡上的 拆分通道旁边，选择 全局覆盖，选择一个选项，然后单击 确定 两次。

配置拆分通道和授权

规划 NetScaler Gateway 部署时，请务必考虑拆分通道以及默认授权操作和授权策略。

例如，您有一个允许访问网络资源的授权策略。您已将拆分通道设置为开，并且未将 Intranet 应用程序配置为通过 NetScaler Gateway 发送网络流量。当 NetScaler Gateway 具有此类配置时，允许访问资源，但用户无法访问该资源。

如果授权策略拒绝访问网络资源，将分割通道设置为 ON，并且内部网应用程序配置为通过 NetScaler Gateway 路由网络流量，则 Citrix Secure Access 客户端将流量发送到 NetScaler Gateway，但对该资源的访问被拒绝。

有关分割通道选项的更多信息，请参阅 拆分通道选项。

配置客户端拦截

February 1, 2024

您可以使用 Intranet 应用程序为 NetScaler Gateway 上的用户连接配置拦截规则。默认情况下，当您在设备上配置系统 IP 地址、映射的 IP 地址或子网 IP 地址时，将基于这些 IP 地址创建子网路由。Intranet 应用程序是根据这些路由自动创建的，并且可以绑定到虚拟服务器。如果启用拆分通道，则必须定义 Intranet 应用程序才能进行客户端拦截。

您可以使用 GUI 配置内部网应用程序。您可以将 Intranet 应用程序绑定到用户、组或虚拟服务器。

如果启用拆分通道并且用户使用 WorxWeb 或 WorxMail 进行连接，则在配置客户端拦截时，必须为 Citrix Endpoint Management 和 Exchange 服务器添加 IP 地址。如果不启用拆分通道，则无需在 Intranet 应用程序中配置 Endpoint Management 和 Exchange IP 地址。

有关分割通道配置的信息，请参阅 配置分割通道。

为 **Citrix Secure Access** 客户端配置内联网应用程序

您可以通过定义以下内容来创建用于用户访问资源的 Intranet 应用程序：

- 一个 IP 地址
- 一系列 IP 地址
- 一个主机名

当您在 NetScaler Gateway 上定义内联网应用程序时，适用于 Windows 的 Citrix Secure Access 客户端会拦截发往该资源的用户流量，并通过 NetScaler Gateway 发送流量。

配置 Intranet 应用程序时，请考虑以下事项：

- 当拆分通道开启时，
  - 配置内部网应用程序。
  - 为每个身份验证、授权和审核组分配 Intranet 应用程序。
- 当拆分通道处于关闭状态时，
  - 所有流量均通过 VPN 通道拦截。
  - 无需配置内联网应用程序。
- 当拆分通道为反向时，

- 配置内部网应用程序。未由 Intranet 应用程序指定的流量通过 VPN 通道。
- 将要从 VPN 中排除的 Intranet 应用程序分配给每个身份验证、授权和审核组。

> 重要：
>
> 无论分割通道配置如何，拦截都必须设置为透明。

注意：

- 配置 Intranet 应用程序时，必须选择与用于建立连接的插件软件类型相对应的拦截模式。
- 您不能将 Intranet 应用程序配置为同时进行代理拦截和透明拦截。

为一个 **IP** 地址创建 **Intranet** 应用程序

1. 在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 资源，然后单击 **Intranet** 应用程序。
2. 在详细信息窗格中，单击“添加”。
3. 在“Name”（名称）中，键入配置文件的名称。
4. 在“创建 **Intranet** 应用程序”对话框中，选择“透明”。
5. 在目标类型中，选择 **IP** 地址和网络掩码。
6. 在“协议”中，选择应用于网络资源的协议。
7. 在 **IP** 地址中，键入 IP 地址。
8. 在 **Netmask** 中，键入子网掩码，单击 创建，然后单击 关闭。

配置 **IP** 地址范围

如果您的网络中有多台服务器，例如 Web、电子邮件和文件共享，则可以配置包含网络资源 IP 范围的网络资源。此设置允许用户访问 IP 地址范围中包含的网络资源。

1. 在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 资源，然后单击“内联网应用程序”。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入配置文件的名称。
4. 在“协议”中，选择应用于网络资源的协议。
5. 在“创建内联网应用程序”对话框中，选择“透明”。
6. 在 目标类型中，选择 **IP** 地址范围。
7. 在“**IP** 开始”中，键入起始 IP 地址，然后在“IP 结束”中键入结束 IP 地址，单击“创建”，然后单击“关闭”。

为主机名创建 **Intranet** 应用程序

1. 在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 资源，然后单击 **Intranet** 应用程序。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入配置文件的名称。

4. 在“创建 **Intranet** 应用程序”对话框中，选择“透明”。
5. 在 目标类型中，选择 主机名。
6. 在协议中，选择 任意，单击 创建，然后单击 关闭。

> 重要提示：
>
> - 从 13.0 版本 36.27 及更高版本开始，Windows VPN 插件支持基于主机名 (FQDN) 的拆分通道规则。您必须同时升级 NetScaler 设备和 Windows VPN 插件才能发布 13.0 版本 36.27 或更高版本。
> - 还支持通配符主机名。例如，如果配置了主机名为“*.example.com”的 Intranet 应用程序，则 `a1.example.com`、`b2.example.com` 等将通过通道传输。
> - 只有将拆分通道设置为“开”或“反向”时，基于主机名的内联网应用程序才能运行。

配置名称服务解析

February 1, 2024

在安装 NetScaler Gateway 期间，您可以使用 NetScaler Gateway 向导配置其他设置，包括名称服务提供商。域名服务提供商会将完全限定的域名 (FQDN) 转换为 IP 地址。在 NetScaler Gateway 向导中，您可以配置 DNS 或 WINS 服务器、设置 DNS 查找的优先级以及重试连接到服务器的次数。

运行 NetScaler Gateway 向导时，可以添加 DNS 服务器。您可以使用会话配置文件向 NetScaler Gateway 添加更多 DNS 服务器和 WINS 服务器。然后，您可以指示用户和组连接到与最初使用向导配置的名称解析服务器不同的名称解析服务器。

在 NetScaler Gateway 上配置额外的 DNS 服务器之前，请创建一个虚拟服务器，该服务器充当 DNS 服务器以进行名称解析。

在会话配置文件中添加 **DNS** 或 **WINS** 服务器

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 策略，然后单击“会话”。
2. 在详细信息窗格的 配置文件 选项卡上，选择一个配置文件，然后单击 打开。
3. 在“网络配置”选项卡上，执行以下操作之一：
   - 要配置 DNS 服务器，请在 DNS 虚拟服务器旁边，单击“覆盖全局”，选择服务器，然后单击“确定”。
   - 要配置 WINS 服务器，请在 WINS 服务器 IP 旁边，单击“覆盖全局”，键入 IP 地址，然后单击“确定”。

> 重要：
>
> 对于附加到 VPN 会话配置文件的不可寻址 DNS 虚拟服务器，不会评估响应程序策略。

为用户连接启用代理支持

February 1, 2024

用户设备可以通过代理服务器进行连接以访问内部网络。NetScaler Gateway 支持 HTTP、SSL、FTP 和 SOCKS 协议。要为用户连接启用代理支持，请在 NetScaler Gateway 上指定设置。您可以指定 NetScaler Gateway 上的代理服务器使用的 IP 地址和端口。代理服务器用作所有与内部网络的进一步连接的转发代理。

代理设置

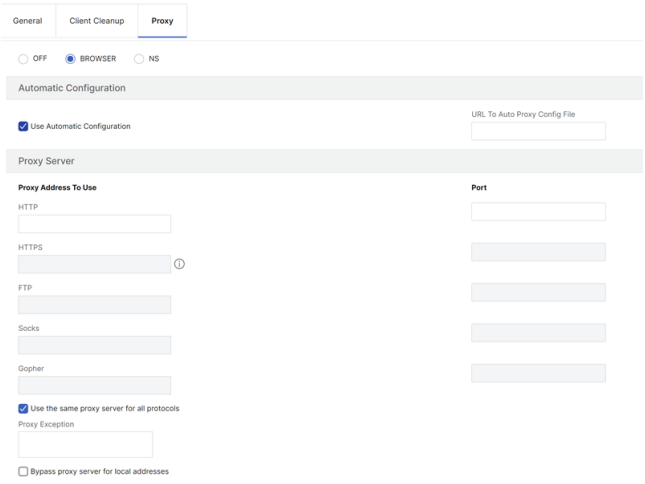
您可以在浏览器或 NetScaler 设备上配置代理设置。要在浏览器或设备上配置代理服务器设置，请导航到 全局 **NetScaler Gateway** 设置 **>** “客户端体验”选项卡 **>** “高级设置” **>** “代理”，然后选择“浏览器”或“**NS**”（

- 浏览器：当您选择在浏览器上配置代理设置时，可以通过提供指向自动代理配置文件的链接来使用自动配置选项。自动配置可能会覆盖手动设置。

  另外，当您选择 浏览器时，您可以通过选择代理例外选项来绕过以前配置的代理。

  注意：不同类型的客户端对于 浏览器 代理配置具有不同的功能。有关详细信息，请参阅 NetScaler Gateway VPN 客户端和支持的功能。

- **NS**：如果在 NetScaler 设备上配置代理设置，则无法使用自动配置选项。在设备上配置代理设置时，无法绕过以前配置的代理。



为用户连接配置代理支持

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上，单击“高级设置”。

4. 在“代理”选项卡的“代理设置”下，选择“浏览器”。
5. 对于协议，键入 IP 地址和端口号，然后单击 确定。

> 注意：
>
> - 如果选择 **NS**，则可以配置仅支持安全和不安全 HTTP 连接的代理服务器。
> - 在 NetScaler Gateway 上启用代理支持后，可以在与协议对应的代理服务器的用户设备上指定配置详细信息。
>
>   启用代理支持后，NetScaler Gateway 会将代理服务器详细信息发送到客户端 Web 浏览器，并更改浏览器上的代理配置。
>
>   - When the user device connects to NetScaler Gateway, the user device can communicate with the proxy server directly for connection to the user’ s network.
>   - When the user device disconnects from NetScaler Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

将一台代理服务器配置为使用 **NetScaler Gateway** 的所有协议

您可以配置一个代理服务器以支持 NetScaler Gateway 使用的所有协议。此设置为所有协议提供一个 IP 地址和端口组合。

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上，单击“高级设置”。
4. 在“代理”选项卡的“代理设置”下，选择“浏览器”。
5. 对于协议，请键入 IP 地址和端口号。
6. 单击对所有协议使用相同的代理服务器，然后单击 确定。

禁用拆分通道并将所有代理设置设置为开时，代理服务器设置将传播到用户设备。如果将代理设置设置为“装置”，则这些设置不会传播到用户设备。

NetScaler Gateway 代表用户设备连接到代理服务器。代理设置不会传播到用户的浏览器，因此无法在用户设备和代理服务器之间进行直接通信。

将 **NetScaler Gateway** 配置为代理服务器

将 NetScaler Gateway 配置为代理服务器时，不安全和安全的 HTTP 是唯一受支持的协议。

1. 在导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上，单击“高级设置”。

4. 在“代 理”选项卡上的“代理设置”下，选择 **NS**。
5. 对于协议，键入 IP 地址和端口号，然后单击 确定。

配置地址池

February 1, 2024

在某些情况下，连接到 Citrix Secure Access 客户端的用户需要 NetScaler Gateway 的唯一 IP 地址。例如，在 Samba 环境中，连接到映射网络驱动器的每个用户都需要看起来来自不同的 IP 地址。为组启用地址池（也称为 IP 池）时，NetScaler Gateway 可以为每个用户分配唯一的 IP 地址别名。

您可以使用 Intranet IP 地址配置地址池。以下类型的应用程序可能需要使用从 IP 池中提取的唯一 IP 地址：

- IP 语音
- 活动 FTP
- 即时通讯
- 安全外壳 (SSH)
- 用于连接到计算机桌面的虚拟网络计算 (VNC)
- 用于连接到客户端桌面的远程桌面 (RDP)

您可以将 NetScaler Gateway 配置为为连接到 NetScaler Gateway 的用户分配内部 IP 地址。可以将静态 IP 地址分配给用户，也可以将一系列 IP 地址分配给组、虚拟服务器或全局系统。

NetScaler Gateway 允许您将内部网络中的 IP 地址分配给远程用户。内部网络上的 IP 地址可以为远程用户提供地址。如果选择使用一定范围的 IP 地址，系统会根据需要将该范围内的 IP 地址动态分配给远程用户。

配置地址池时，请注意以下事项：

- 必须正确路由分配的 IP 地址。为确保路由正确，请考虑以下事项：
  - 如果未启用拆分通道，请确保 IP 地址可以通过网络地址转换 (NAT) 设备路由。
  - 使用 Intranet IP 地址的用户连接访问的任何服务器都必须配置适当的网关才能到达这些网络。
  - 在 NetScaler Gateway 上配置网关或静态路由，以便将来自用户软件的网络流量路由到内部网络。
- 分配 IP 地址范围时，只能使用连续的子网掩码。范围的子集可以分配给较低级别的实体。例如，如果 IP 地址范围绑定到虚拟服务器，则将该范围的子集绑定到组。
- IP 地址范围不能绑定到绑定级别内的多个实体。例如，绑定到组的地址范围的子集不能绑定到另一个组。
- NetScaler Gateway 不允许您在用户会话主动使用 IP 地址时删除或取消绑定 IP 地址。
- 使用以下层次结构将内部网络 IP 地址分配给用户：
  - 用户的直接绑定
  - 分组分配的地址池
  - 虚拟服务器分配的地址池

  - 全球范围的地址

- 分配地址范围时只能使用连续的子网掩码。但是，已分配范围的子集可能会进一步分配给较低级别的实体。
  绑定的全局地址范围可以具有绑定到以下内容的范围：

  - 虚拟服务器
  - 组
  - 用户

- 绑定的虚拟服务器地址范围可以有绑定到以下内容的子集：

  - 组
  - 用户

绑定的组地址范围可以有绑定到用户的子集。

为用户分配 IP 地址后，该地址将保留用于用户下次登录，直到地址池范围用尽为止。当地址用尽时，NetScaler Gateway 会从 NetScaler Gateway 注销时间最长的用户那里回收 IP 地址。

如果无法回收某个地址并且所有地址都在使用中，NetScaler Gateway 将不允许用户登录。您可以通过允许 NetScaler Gateway 在所有其他 IP 地址都不可用时将映射的 IP 地址用作 Intranet IP 地址来防止出现这种情况。

内联网 **IP DNS** 注册

如果将 Intranet IP 分配给客户端计算机，并且在 VIP 通道建立之后，VPN 插件会检查该客户端计算机是否已加入域。如果客户端计算机是加入域的计算机，VPN 插件将启动 DNS 注册过程，以将计算机的主机名 Intranet 与分配的 Intranet IP 地址关联起来。在通道重建之前，此注册将被还原。

要成功注册 DNS，请确保设置了以下 `nsapimgr` 旋钮。还要确保权威 DNS 服务器设置为允许“不安全”的 DNS 更新。

- **`nsapimgr` -ys enable_vpn_dns_override=1**：此标志与其他配置参数一起发送到 NetScaler Gateway VPN 客户端。如果未设置此标志并且当 VPN 客户端拦截 DNS/WINS 请求时，它会通过通道向 NetScaler Gateway 虚拟服务器发送相应的“GET /DNS”HTTP 请求以获取解析的 IP 地址。但是，如果设置了“enable_vpn_dnstruncate_fix”标志，VPN 客户端将 DNS/WINS 请求透明地转发给 NetScaler Gateway 虚拟服务器。在这种情况下，DNS 数据包将通过 VPN 通道按原样发送到 NetScaler Gateway 虚拟服务器。如果从 NetScaler Gateway 中配置的域名服务器返回的 DNS 记录很大，不适合 UPD 响应数据包，这会有所帮助。在这种情况下，当客户端恢复使用 TCP-DNS 时，此 TCP-DNS 数据包按原样到达 NetScaler Gateway 服务器，因此 NetScaler Gateway 服务器向 DNS 服务器发出 TCP-DNS 查询。
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1**：NetScaler Gateway 服务器本身使用此标志。如果设置了此标志，NetScaler Gateway 会覆盖 NetScaler Gateway 上配置的 DNS 服务器的“DNS 端口上的 TCP 连接”的目标（而不是尝试将它们发送到传入的 TCP-DNS 数据包中最初存在的 DNS-server-IP）。对于 UDP DNS 请求，默认情况下使用配置的 DNS 服务器进行 DNS 解析。适用于 Windows 的 NetScaler Gateway 插件支持安全和非安全的 DNS 更新。默认情况下，21.7.1.1 或更高版本中存在安全 DNS 更新支持。

默认情况下，Windows 插件上的安全 DNS 更新处于禁用状态。要启用它，请在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access 中创建一个类型为 REG_DWORD 的值并将其设置为 1。

- 将该值设置为 1 时，VPN 插件会先尝试不安全的 DNS 更新。如果不安全的 DNS 更新失败，VPN 插件会尝试安全 DNS 更新。
- 要仅尝试安全 DNS 更新，可以将该值设置为 2。

有关设置这些旋钮的更多信息，请参阅 https://support.citrix.com/article/CTX200243。

为用户、组或虚拟服务器配置地址池

1. 在配置实用程序的导航窗格中，展开 **NetScaler Gateway**，执行以下操作之一：
   - 展开 NetScaler Gateway 用户管理，然后单击 **AAA** 用户。
   - 展开 NetScaler Gateway**>**“用户管理”，然后单击 **AAA** 组。
   - 展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，单击用户、组或虚拟服务器，然后单击 打开。
3. 在 **Intranet** IP 选项卡的 IP 地址和子网掩码中，键入 IP 地址和子网掩码，然后单击 添加。
4. 对要添加到池中的每个 IP 地址重复步骤 3，然后单击“确定”。

全局配置地址池

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格中的 **Intranet IP** 下，单击要分配唯一的静态 IP 地址或 IP 地址池供所有客户端 NetScaler Gateway 会话使用，请配置 Intranet IP。
3. 在“绑定 **Intranet IP**”对话框中，单击“操作”，然后单击“插入”。
4. 在“IP 地址和子网掩码”中，键入 IP 地址和子网掩码，然后单击“添加”。
5. 对要添加到池中的每个 IP 地址重复步骤 3 和 4，然后单击“确定”。

定义地址池选项

您可以使用会话策略或全局 NetScaler Gateway 设置来控制是否在用户会话期间分配 Intranet IP 地址。通过定义地址池选项，您可以将 Intranet IP 地址分配给 NetScaler Gateway，同时禁止对特定用户组使用 Intranet IP 地址。

您可以通过以下三种方式之一使用会话策略来配置地址池：

- **Nospillover** -为 Intranet IP 地址配置地址池时，您将获得一个包含池中可用 IP 的会话。对于已使用所有可用 Intranet IP 地址的用户，将显示“转移登录”页面。
- 溢出 - 当您配置地址池并将映射的 IP 用作 Intranet IP 地址时，映射的 IP 地址将用于已使用所有可用 Intranet IP 地址的用户。
- **Off** -未配置地址池。

> 注意：
>
> 如果未配置映射的 IP 地址，则使用 SNIP。

定义地址池

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 在 网络配置 选项卡上，单击 高级。
7. 在 Intranet IP 旁边，单击 覆盖全局，然后选择一个选项。
8. 如果在步骤 9 中选择溢出，请在映射的 IP 旁边单击覆盖全局，选择设备的主机名，单击确定，然后单击创建。
9. 在“创建会话策略”对话框中，创建表达式。单击“创建”，然后单击“关闭”。

配置“转移登录”页面

如果用户没有可用的 Intranet IP 地址，然后尝试与 NetScaler Gateway 建立另一个会话，则会出现“转移登录”页面。“转移登录”页面允许用户使用新会话替换其现有 NetScaler Gateway 会话。

如果注销请求丢失或用户未执行彻底注销，也可以使用“转移登录”页面。例如：

- 为用户分配了一个静态内部网 IP 地址，并拥有现有的 NetScaler Gateway 会话。如果用户尝试从另一台设备建立第二个会话，则会出现“转移登录”页面，用户可以将会话转移到新设备。
- 为用户分配了五个内部网 IP 地址，并通过 NetScaler Gateway 拥有五个会话。如果用户尝试建立第六个会话，则会出现“转移登录”页面，用户可以选择用新会话替换现有会话。

> 备注：
>
> - 如果没有为用户分配可用 IP 地址，因此无法建立新的会话，则会显示一条错误消息。
> - 适用于 Android 的 Citrix Secure Access 23.12.1 及更高版本在始终可用的 VPN 模式下支持 NetScaler Gateway 的转移登录功能。

仅当您配置地址池并禁用溢出功能时，才会显示“转移登录”页面。

配置 **DNS** 后缀

当用户登录 NetScaler Gateway 并获得 IP 地址时，用户名和 IP 地址组合的 DNS 记录将添加到 NetScaler Gateway DNS 缓存中。您可以将 DNS 后缀配置为在将 DNS 记录添加到缓存时附加到用户名。这允许用户通过 DNS 名称进行引用，这比 IP 地址更容易记住。当用户从 NetScaler Gateway 注销时，记录将从 DNS 缓存中删除。

配置 **DNS** 后缀

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击“会话”。
2. 在详细信息窗格的“策 略”选项卡上，选择一个会话策略，然后单击“打开”。
3. 在“请求配置文件”旁边，单击“修改”。
4. 在 网络配置 选项卡上，单击 高级。
5. 在“Intranet IP DNS 后缀”旁边，单击“覆盖全局”，键入 DNS 后缀，然后单击“确定”三次。

支持 **VoIP** 电话

February 1, 2024

当您将 NetScaler Gateway 安装为独立设备并且用户连接到 Citrix Secure Access 客户端时，NetScaler Gateway 支持与 IP 语音 (VoIP) 软电话进行双向通信。

NetScaler Gateway 支持以下 VoIP 软电话。

- 思科软电话
- Avaya IP 软件电话

IP PBX 和用户设备上运行的软件电话软件之间支持安全通道。要允许 VoIP 流量通过安全通道，您必须在同一用户设备上安装 Citrix Secure Access 客户端和一部支持的软电话。当 VoIP 流量通过安全通道发送时，支持以下软件电话功能：

- 从 IP 软电话发出的拨出呼叫
- 拨打到 IP 软件电话的来电
- 双向语音流量

对 VoIP 软电话的支持是通过使用内部网 IP 地址配置的。您必须为每个用户配置一个 Intranet IP 地址。如果您使用的是 Cisco Softphone 通信，则在配置 Intranet IP 地址并将其绑定到用户之后，无需进行其他配置。有关配置 Intranet IP 地址的详细信息，请参阅 配置地址池。

如果启用拆分通道，请创建 Intranet 应用程序并指定 Avaya Softphone 应用程序。此外，您必须启用透明拦截。

配置 **Access Interface**

February 1, 2024

NetScaler Gateway 包含一个默认主页，该主页将在用户登录后显示。默认主页称为访问接口。您可以使用访问界面作为主页，或将 Web Interface 配置为主页或自定义主页。

访问界面包含三个面板。如果您的部署中有 Web Interface ，则用户可以在访问界面的左侧面板中登录 Receiver。如果您的部署中有 StoreFront，则用户无法从左侧面板登录 Receiver。

访问接口用于提供内部和外部网站的链接，以及指向内部网络中文件共享的链接。您可以通过以下方式自定义访问界面：

- 更改访问接口。
- 创建访问接口链接。

用户还可以通过添加自己的网站和文件共享链接来自定义访问界面。用户还可以使用主页将文件从内部网络传输到他们的设备。

> 注意：
>
> 当用户登录并尝试从访问接口打开文件共享时，文件共享不会打开，用户会收到错误消息“无法与服务器建立 TCP 连接”。要解决此问题，请将防火墙配置为允许从 NetScaler Gateway 系统 IP 地址到 TCP 端口 445 和 139 上的文件服务器 IP 地址的流量。

更改访问接口

您可能希望将用户定向到自定义主页，而不是依赖访问界面。为此，请在 NetScaler Gateway 上安装主页，然后将会话策略配置为使用新主页。

安装自定义主页

1. 在配置实用程序中，单击“配置”选项卡，然后在导航窗格中单击 **NetScaler Gateway**。
2. 在详细信息窗格中的 自定义访问接口下，单击 上载访问接口。
3. 要从网络中计算机上的文件安装主页，请在“本地文件”中单击“浏览”，导航到该文件，然后单击“选择”。
4. 要使用安装在 NetScaler Gateway 上的主页，请在“远程路径”中单击“浏览”，选择文件，然后单击“选择”。
5. 单击 上载，然后单击 关闭。

将访问界面替换为自定义主页

您可以使用全局设置或会话策略和配置文件来配置自定义主页以替换默认主页 Access Interface。配置策略后，您可以将策略绑定到用户、组、虚拟服务器或全局绑定。配置自定义主页时，用户登录时不会显示访问界面。

全局配置自定义主页

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户端体验”选项卡的“主页”中，单击“显示主页”，然后输入自定义主页的 Web 地址。
4. 单击 确定，然后单击 关闭。

在会话配置文件中配置自定义主页

1. 在配置实用程序的“配置”选项卡的导航窗格中，展开 **NetScaler Gateway** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“客户端体验”选项卡上的“主页”旁边，单击“覆盖全局”，单击“显示主页”，然后键入主页的 Web 地址。
7. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“True 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建和应用 **Web** 链接

February 1, 2024

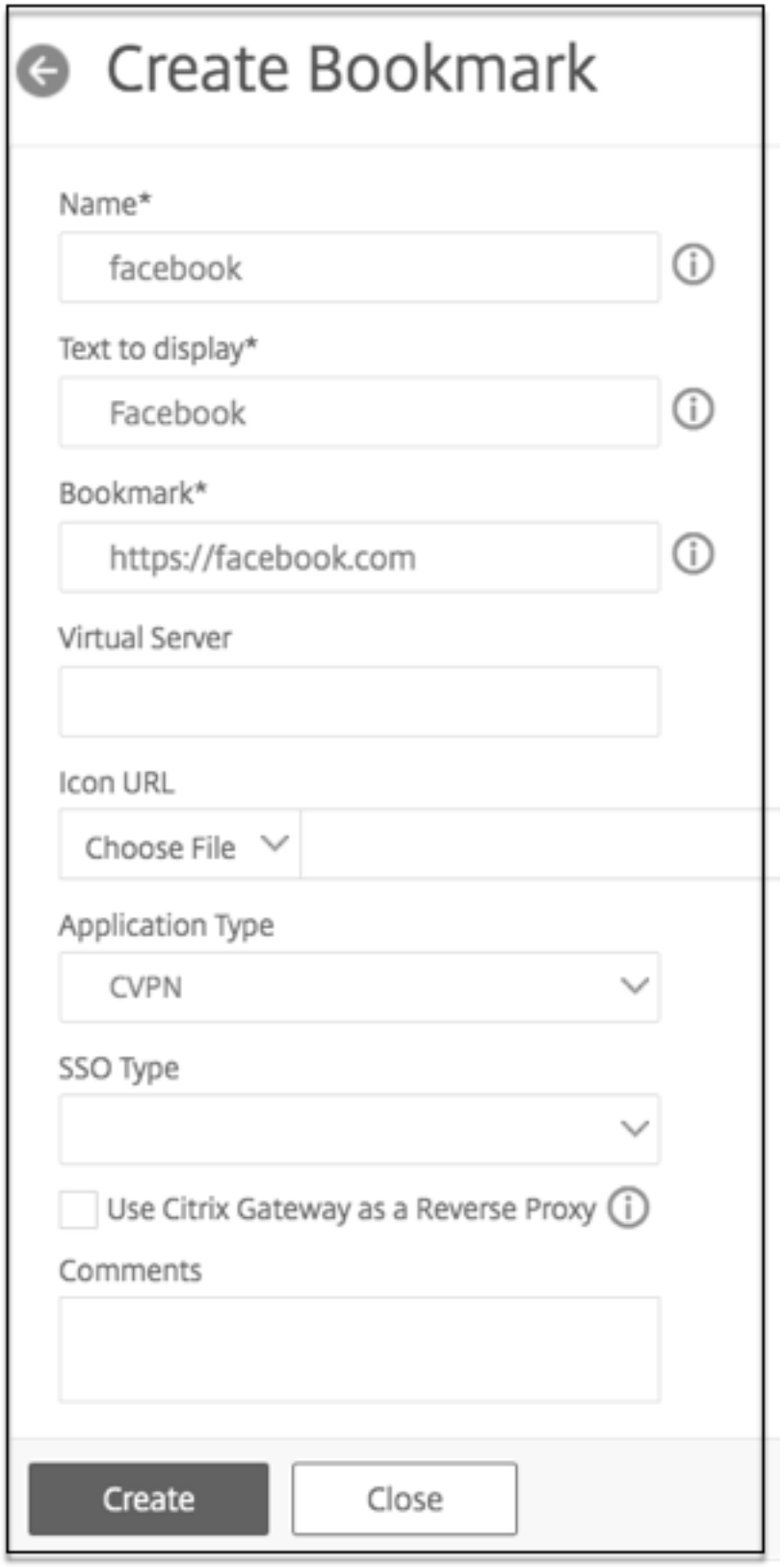
您可以将访问接口配置为显示一组指向用户可用的内部资源的链接。创建这些链接要求您首先将这些链接定义为资源。然后，将它们绑定到用户、组、虚拟服务器或全局，以使其在访问界面中处于活动状态。您创建的链接将显示在“企业网站”下的“网站”窗格中。

> 重要：
>
> 从 NetScaler 版本 13.0 版本 64.xx 起，不支持通过 NetScaler Gateway 进行的文件共享。

创建企业书签

在会话策略中创建访问接口链接

1. 在配置实用程序中的 配置 选项卡的导航窗格中，展开 **NetScaler Gateway >** 资源，然后单击 门户书签。
2. 在详细信息窗格中，单击“添加”。



3. 在 名称中，键入书签的名称。

4. 在 要显示的文本中，键入链接的描述。描述将显示在 访问界面中。
5. 在书签中，键入应用程序的 Web 地址。
6. 在虚拟服务器中，键入关联的负载平衡/内容交换虚拟服务器的名称。此字段为可选字段。
7. 在图标 **URL** 中，除默认主题外，所有主题均支持上载的图标。建议的最大大小为 70x70 像素。我们建议您使用透明图像。此字段为可选字段。
8. 在 应用程序类型中，选择 URL 所代表的应用程序类型（VPN、无客户端 VPN 或 SaaS）。此字段为可选字段。
9. 在 **SSO** 类型中，选择要为书签配置的 SSO 类型。配置 SSO 后，用户无需在后续登录中输入凭据即可访问应用程序。支持以下 SSO 类型：
   - Unified Gateway：此 SSO 配置允许通过单个 URL 安全地远程访问应用程序的多个资源。
   - 自助身份验证：在此 SSO 配置中，提示 NetScaler Gateway 用户提供登录凭据以访问应用程序。
   - 基于 SAML 的身份验证：在这个 SSO 配置中，NetScaler Gateway 使用 IdP 来验证用户详细信息，生成 SAML 断言并将其发送到 SP。如果验证通过，则 SSO 成功。

   > 注意：
   >
   > 如果启用无客户端访问，则可以确保对网站的请求通过 NetScaler Gateway。例如，您为 Google添加了书签。选中使用 **NetScaler Gateway** 作为反向代理复选框。选中此复选框时，网站请求将从用户设备发送到 NetScaler Gateway，然后发送到网站。清除该复选框后，请求将从用户设备发送到网站。仅当启用无客户端访问时，此复选框才可用。

10. 单击“创建”，然后单击“关闭”。

绑定访问接口链接

您可以将访问接口链接绑定到以下位置：

- 用户
- 组
- Virtual servers（虚拟服务器）

保存配置后，用户可以在 主页 选项卡的访问界面中使用这些链接，这是用户成功登录后看到的第一个页面。

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   - 展开 **NetScaler Gateway** 用户管理，然后单击 **AAA** 用户。
   - 展开 **NetScaler Gateway** 用户管理，然后单击 **AAA** 组。
   - 展开 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在详细信息窗格中，执行以下操作之一：
   - 选择一个用户，然后单击“打开”。

- 选择一个组，然后单击“打开”。
- 选择虚拟服务器，然后单击打开。

3. 在对话框中，单击书 签 选项卡。
4. 在“可用书签”下，选择一个或多个书签，单击向右箭头以移动已配置书签下的书签，然后单击“确定”。

使用 **GUI** 全局绑定书签

1. 在 配置 选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击全局设置。
2. 在详细信息窗格中的 书签下，单击 创建指向要在 **NetScaler Gateway** 门户页面上访问的 **HTTP** 和 **Windows** 文件共享应用程序的链接。

3. 在 配置 **VPN** 全局绑定 * 对话框中，单击 添加。
4. 在“可用”下，选择一个或多个书签，单击向右箭头将书签移动到“已配置”下，然后单击“确定”。

使用 **CLI** 添加企业书签

在命令提示符下，键入：

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

示例：

Web 书签

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```


使用 **CLI** 绑定企业书签

您可以将企业书签绑定到用户、组、虚拟服务器和全局级别。

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  - urlName <string>
<!--NeedCopy-->
```

示例：

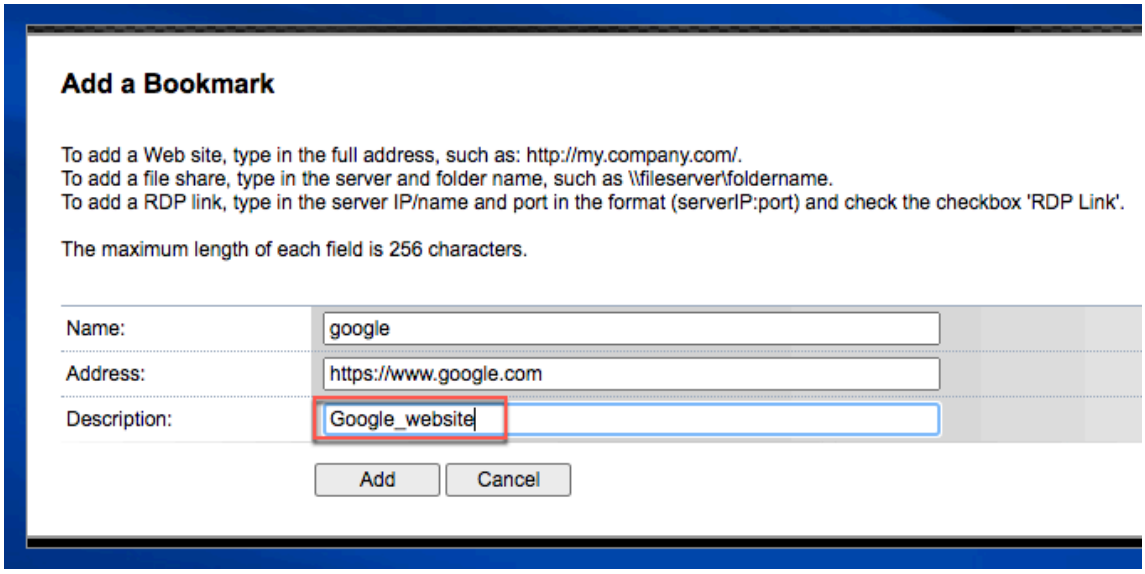
```
bind vpn global -urlName google
<!--NeedCopy-->
```

创建个人书签

您只能从 VPN 虚拟服务器创建个人网站。没有用于添加个人书签的 NetScaler Gateway 管理员 GUI。

1. 登录 VPN 虚拟服务器。
2. 单击 网络访问 或 无客户端访问 以添加书签。
3. 单击添加。

4. 输入书签详细信息，例如网站名称、地址和描述。



5. 单击添加。

您添加的网站将显示在相应的选项卡下。

在书签中配置用户名令牌

您可以使用特殊标记username% 配置书签和文件共享 URL。用户登录时，令牌将替换为每个用户的登录名。例如，您为名为 Jack 的员工创建一个书签，作为 \\EmployeeServer\%username%\ 的文件夹。当 Jack 登录时，文件共享 URL 将映射到 \\EmployeeServer\Jack\。在书签中配置用户名令牌时，请记住以下情况：

- 如果您使用的是一种身份验证类型，则用户名将替换令牌username%%。
- 如果使用双重身份验证，则使用主身份验证类型中的用户名替换%username% 令牌。
- 如果您使用的是客户端证书身份验证，则客户端证书身份验证配置文件中的用户名字段将用于替换username%% 令牌。

流量策略

February 1, 2024

流量策略允许您为用户连接配置以下设置：

- 强制缩短从不受信任的网络访问的敏感应用程序的超时时间。
- 将网络流量切换为对某些应用程序使用 TCP。如果选择 TCP，则必须为某些应用程序启用或禁用单点登录。
- 确定要使用其他 HTTP 功能处理 Citrix Secure Access 客户端流量的情况。
- 定义与文件类型关联一起使用的文件扩展名。

创建流量策略

要配置流量策略，请创建配置文件并配置以下参数：

- 协议（HTTP 或 TCP）
- 应用程序超时
- 单点登录 Web 应用程序
- 形成单点登录
- 文件类型关联
- 中继器插件
- Kerberos 受限委派 (KCD) 帐户

创建流量策略后，您可以将策略绑定到虚拟服务器、用户、组或全局。

例如，您在内部网络的服务器上安装了 Web 应用程序 PeopleSoft 人力资源。您可以为此应用程序创建流量策略，以定义目标 IP 地址、目标端口，还可以设置用户可以保持登录应用程序的时间长度，例如 15 分钟。

如果要配置其他功能，例如对应用程序的 HTTP 压缩，则可以使用流量策略来配置设置。创建策略时，请使用 HTTP 参数执行操作。在表达式中，为运行应用程序的服务器创建目标地址。

流量策略表达式示例

以下是流量策略的表达式示例：

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

使用 **GUI** 配置流量策略

1. 展开 **NetScaler Gateway >** 策略，然后单击 流量。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在 创建流量策略 对话框的 名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在 协议中，选择 **HTTP** 或 **TCP**。

   注意：如果选择 TCP 作为协议，则无法配置单点登录，并且在配置文件对话框中禁用该设置。
7. 在 **AppTimeout (**分钟**)** 中，键入分钟数。此设置限制用户可以保持登录 Web 应用程序的时间。
8. 要启用 Web 应用程序的单点登录，请在 单点登录中选择 开。

   注意：如果要使用基于表单的单点登录，则可以在流量配置文件中配置设置。有关详细信息，请参阅 配置基于表单的单点登录。
9. 要指定文件类型关联，请在“文件类型关联”中选择“开”。
10. 要使用中继器插件优化网络流量，请在 **Citrix SD-WAN** 中选择开，单击创建，然后单击关闭。
11. 如果在设备上配置 KCD，请在 KCD 帐户中选择该帐户。

    有关在设备上配置 KCD 的详细信息，请参阅在 NetScaler 设备上配置 Kerberos 受限委派。
12. 在“创建流量策略”对话框中，创建或添加表达式，单击“创建”，然后单击“关闭”。

配置基于表单的单点登录

基于表单的单点登录允许用户一次性登录到网络中的所有受保护应用程序。在 NetScaler Gateway 中配置基于表单的单点登录时，用户可以访问需要基于 HTML 表单的登录的 Web 应用程序，而无需再次键入密码。如果没有单点登录，用户需要单独登录才能访问每个应用程序。

创建表单单一登录配置文件后，您可以创建包含表单一登录配置文件的流量配置文件和策略。有关更多信息，请参阅 创建流量策略。

配置基于表单的单点登录

1. 展开 **NetScaler Gateway >** 策略，然后单击“流量”。
2. 在详细信息窗格中，单击 表单 **SSO** 配置文件 选项卡，然后单击 添加。
3. 在名称中，键入配置文件的名称。

4. 在 操作 **URL** 中，键入完成的表单要提交到的 URL。

   注意：该 URL 是根相对 URL。

5. 在 用户名中，为用户名字段键入属性的名称。
6. 在“密码”中，键入密码字段的属性名称。
7. 在 **SSO** 成功规则中，创建一个表达式来描述策略调用此配置文件时所采取的操作。也可以使用此字段下的“前缀”、“添加”和“运算符”按钮来创建表达式。

   该规则检查单点登录是否成功。

8. 在 名称值对中，键入用户名字段值，然后键入 & 符号 (&)，然后键入密码字段值。

   值名称用 & 符号分隔，例如 name1=value1&name2=value2。

9. 在 响应大小中，键入允许完整响应大小的字节数。键入响应中要解析以提取表单的字节数。
10. 在 提取中，选择名称/值对是静态还是动态。默认设置为动态。
11. 在 提交方法中，选择单点登录表单用于将登录凭据发送到登录服务器的 HTTP 方法。默认值为 Get。
12. 单击“创建”，然后单击“关闭”。

配置 **SAML** 单点登录

您可以为单点登录 (SSO) 创建 SAML 1.1 或 SAML 2.0 配置文件。用户可以连接到支持 SAML 协议的 Web 应用程序以进行单点登录。NetScaler Gateway 支持 SAML Web 应用程序的身份提供商 (IdP) 单点登录。

配置 **SAML** 单点登录

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway\ >** 策略，然后单击流量。
2. 在详细信息窗格中，单击 SAML SSO 配置文件选项卡。
3. 在详细信息窗格中，单击 Add（添加）。
4. 在“Name”（名称）中，键入配置文件的名称。
5. 在签名证书名称中，输入 X.509 证书的名称。
6. 在 ACS URL 中，输入身份提供商或服务提供商的声明使用者服务。断言消费者服务 URL (ACS URL) 为用户提供 SSO 功能。
7. 在中继状态规则中，从保存的策略表达式和常用表达式为策略构建表达式。从“运算符”列表中选择以定义如何计算表达式。要测试表达式，请单击评估。
8. 在发送密码中，选择开或关。
9. 在颁发者名称中输入 SAML 应用程序的身份。
10. 单击 Create（创建），然后单击 Close（关闭）。

绑定流量策略

您可以将流量策略绑定到虚拟服务器、组、用户以及 NetScaler Gateway Global。您可以使用配置实用程序绑定流量策略。

使用 **GUI** 全局绑定流量策略

1. 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击流量。
2. 在详细信息窗格中，选择一个策略，然后在操作中单击全局绑定。
3. 在“绑定/取消绑定流量策略”对话框的“详细信息”下，单击“插入策略”。
4. 在策略名称下，选择策略，然后单击确定。

删除流量策略

您可以使用配置实用程序从 NetScaler Gateway 中删除流量策略。如果使用配置实用程序删除流量策略，并且该策略绑定到用户、组或虚拟服务器级别，则必须首先取消绑定该策略。然后，您可以删除该策略。

使用 **GUI** 取消绑定流量策略

1. 展开 **NetScaler Gateway**，然后单击 虚拟服务器。
   - 展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 组。
   - 展开 **NetScaler Gateway >** 用户管理，然后单击 **AAA** 用户。
2. 在详细信息窗格中，选择虚拟服务器、组或用户，然后单击 打开。
3. 在 配置 **NetScaler Gateway** 虚拟服务器、配置 **AAA** 组或 配置 **AAA** 用户 对话框中，单击 策略 选项卡。
4. 单击 流量，选择策略，然后单击 取消绑定策略。
5. 单击“确定”，然后单击“关闭”。

解除流量策略绑定后，您可以删除该策略。

使用 **GUI** 删除流量策略

1. 展开 NetScaler Gateway > 策略，然后单击“流量”。
2. 在详细信息窗格的“策略”选项卡上，选择流量策略，然后单击“删除”。

会话策略

February 1, 2024

会话策略是应用于用户、组、虚拟服务器和全局的表达式和设置的集合。

您可以使用会话策略配置用户连接的设置。您可以定义设置来配置用户登录时使用的软件，例如适用于 Windows 的 Citrix Secure Access 客户端或适用于 Mac 的 Citrix Secure Access 客户端。您还可以配置要求用户使用 Citrix Workspace 应用程序或 Secure Hub 登录的设置。会话策略在用户通过身份验证后进行评估和应用。

会话策略将根据以下规则应用：

- 会话策略始终覆盖配置中的全局设置。
- 未使用会话策略设置的任何属性或参数都是在为虚拟服务器建立的策略上设置的。
- 未由会话策略或虚拟服务器设置的任何其他属性均由全局配置设置。

> 重要：
>
> 以下说明是创建会话策略的一般准则。有关为不同配置（例如无客户端访问或访问已发布应用程序）配置会话策略的具体说明。这些说明可能包含配置特定设置的说明。但是，该设置可以是会话配置文件和策略中包含的许多设置之一。这些说明指导您在会话配置文件中创建设置，然后将该配置文件应用于会话策略。您可以在配置文件和策略中更改设置，而无需创建会话策略。此外，您可以在全局级别创建所有设置，然后创建会话策略来覆盖全局设置。

如果在网络中部署 Citrix Endpoint Management 或 StoreFront，Citrix 建议使用快速配置向导来配置会话策略和配置文件。运行向导时，您可以定义部署的设置。然后，NetScaler Gateway 会创建所需的身份验证、会话和无客户端访问策略。

创建会话策略

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 NetScaler Gateway > 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在“Name”（名称）中，键入配置文件的名称。
6. 完成会话配置文件的设置，然后单击创建。
7. 在“创建会话配置文件”对话框中，为策略添加表达式，单击“创建”，然后单击“关闭”。
   注意：在表达式中，选择
   True value，以便策略始终应用于其绑定到的级别。

会话策略表达式示例

以下是会话策略的表达式示例：

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`

- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

绑定会话策略

创建会话策略后，将其绑定到用户、组、虚拟服务器或全局。会话策略按以下顺序作为层次结构应用：

- 用户
- 组
- Virtual servers（虚拟服务器）
- 全球

使用 **GUI** 将会话策略绑定到虚拟服务器

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 选择虚拟服务器，然后单击 **Edit**（编辑）。您还可以创建新的虚拟服务器。
3. 向下滚动到“策略”部分，然后单击 **+** 图标。
4. 在 选择策略中，选择 会话。
5. 在 选择类型中，选择 请求，然后单击 继续。
6. 在 选择策略中，选择要绑定到此虚拟服务器的策略。
7. 在 优先级中，输入策略的优先级编号。
8. 单击绑定。

使用 **GUI** 将会话策略绑定到身份验证、授权和审核组

1. 导航到 **NetScaler Gateway >** 用户管理 **> AAA** 组。
2. 选择现有的身份验证、授权和审核组，然后单击 编辑。您还可以创建身份验证、授权和审核组。
3. 在“高级设置”中，单击“策略”，然后单击“**+**”图标。
4. 在 选择策略中，选择 会话，然后单击 继续。
5. 在 选择策略中，选择要绑定到此身份验证、授权和审核组的策略。
6. 在 优先级中，输入策略的优先级编号。
7. 单击绑定。

使用 **GUI** 将会话策略绑定到身份验证、授权和审核用户

1. 导航到 **NetScaler Gateway >** 用户管理 **> AAA** 用户。
2. 选择现有 NetScaler 用户，然后单击 编辑。您还可以创建身份验证、授权和审核用户。
3. 在“高级设置”中，单击“策略”，然后单击“**+**”图标。

4. 在 选择策略中，选择 会话，然后单击 继续。
5. 在选择策略中，选择要绑定到此身份验证、授权和审核用户的策略。
6. 在 优先级中，输入策略的优先级编号。
7. 单击绑定。

注意：有关优先级的详细信息，请参阅 https://support.citrix.com/article/CTX214588。

创建会话配置文件

会话配置文件包含用户连接的设置。

会话配置文件指定在用户设备满足策略表达式条件时应用于用户会话的操作。配置文件与会话策略一起使用。您可以使用配置实用程序独立于会话策略创建会话配置文件，然后将该配置文件用于多个策略。一个策略只能使用一个配置文件。

在会话配置文件中为用户连接配置网络设置

您可以使用会话 配置文件中的“网络配置”选项卡为用户连接配置以下网络设置：

- DNS 服务器
- WINS 服务器 IP 地址
- 可用作内部网 IP 地址的映射 IP 地址
- 地址池的溢出设置（Intranet IP 地址）
- 内联网 IP DNS 后缀
- HTTP 端口
- 强制超时设置

在会话配置文件中配置连接设置

您可以使用会话配置文件中的“客户端体验”选项卡配置以下连接设置：

- 访问界面或自定义主页
- 基于 Web 的电子邮件的 Web 地址，例如 Outlook Web Access
- 插件类型（适用于 Windows 的 Citrix Secure Access 客户端或适用于 macOS X 的 Citrix Secure Access 客户端）
- 拆分通道
- 会话和空闲超时设置
- 无客户端访问
- 无客户端访问 URL 编码
- 插件类型（Windows 或 Mac）
- 单点登录 Web 应用程序

- 身份验证的凭据索引
- 使用 Windows 进行单点登录
- 客户端清理行为
- 登录脚本
- 客户端调试设置
- 拆分 DNS
- 访问专用网络 IP 地址和本地局域网访问
- 客户选择
- 代理设置

有关配置用户连接设置的更多信息，请参阅为 Citrix Secure Access 客户端配置连接。

在会话配置文件中配置安全设置

您可以使用会话配置文件中的“安全”选项卡配置以下安全设置：

- 默认授权操作（允许或拒绝）
- Secure Browse 来自 iOS 设备的连接
- 隔离组
- 授权组

有关在 NetScaler Gateway 上配置授权的详细信息，请参阅 配置授权。

在会话配置文件中配置 **Citrix Virtual Apps and Desktops** 设置

您可以使用会话配置文件中的 已发布应 用程序选项卡为与运行 Citrix Virtual Apps and Desktops ktop 的服务器的连接配置以下设置：

- ICA 代理，这是使用 Citrix Workspace 应用程序的客户端连接
- Web Interface 地址
- Web Interface 门户模式
- 单点登录到服务器场域
- Citrix Workspace 应用程序主页
- 帐户服务地址

有关配置用于连接到服务器场中已发布应用程序的设置的详细信息，请参阅 通过 Web Interface 提供对已发布应用程序和虚拟桌面的访问权限。

您可以独立于会话策略创建会话配置文件。创建策略时，您可以选择要附加到策略的配置文件。

使用 **GUI** 创建会话配置文件

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中，单击 配置文件 选项卡，然后单击 添加。
3. 配置配置文件的设置，单击“创建”，然后单击“关闭”。

创建配置文件后，您可以将其包含在会话策略中。

使用 **GUI** 将配置文件添加到会话策略

1. 在配置实用程序的导航窗格中，展开 访问网关 **>** 策略，然后单击 会话。
2. 在“策略”选项卡上，执行以下任一操作：
   - 单击添加以创建会话策略。
   - 选择一个策略，然后单击 打开。
3. 在 请求配置文件中，从列表中选择一个配置文件。
4. 完成会话策略的配置，然后执行以下操作之一：
   a) 单击 创建，然后单击 关闭 以创建策略。
   b) 单击“确定”，然后单击“关闭”以修改策略。

对企业书签的高级策略支持

February 1, 2024

可以将企业书签（VPN URL）配置为高级策略。

> 备注：
>
> - NetScaler Gateway 支持面向企业书签的 HTTP、HTTPS 和 RDP 协议。
> - NetScaler Gateway 仅支持企业书签的绝对 URL。

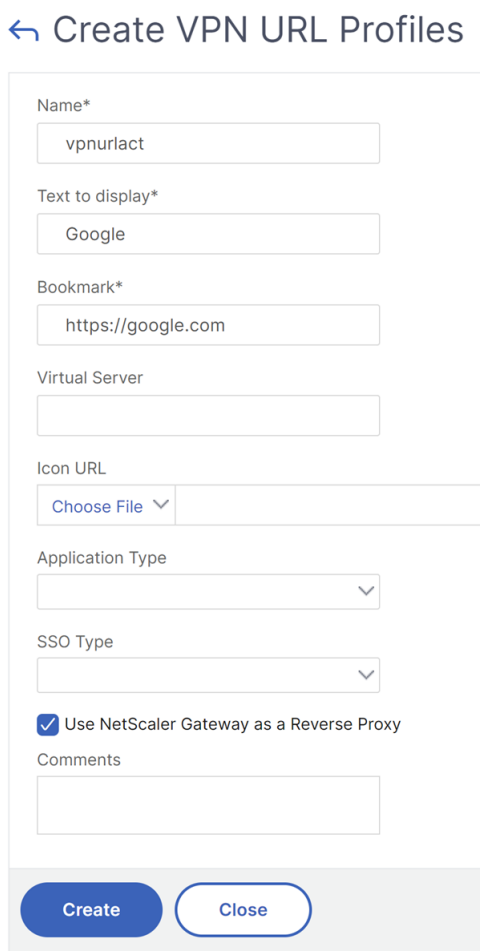
将 **VPN URL** 配置为高级策略

在 **GUI** 上

1. 创建 VPN URL 配置文件。
   - 导航到“配置”**>**“**NetScaler Gateway**”**>**“策略”**>**“**VPN URL**”。
   - 在 **VPN URL** 策略和配置文件 页面上，选择 **VPN URL** 配置文件 选项卡，然后单击 添加。
   - 更新必填字段，然后单击“创建”。
     - 名称：VPN URL 配置文件的名称。

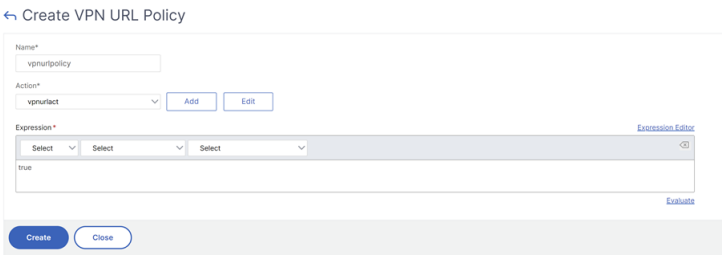
- 要显示的文本：链接的简要描述。描述显示在访问接口上。
- 书签：应用程序的 Web 地址。
- 虚拟服务器：已配置的关联负载平衡或内容交换虚拟服务器的名称。此字段为可选字段。
- 图标 URL：除默认主题外，所有主题都支持在此字段中上载的图标。建议的最大大小为 70x70 像素。我们建议您使用透明图像。此字段为可选字段。
- 应用程序类型：选择 URL 所代表的应用程序类型（VPN、无客户端 VPN 或 SaaS）。此字段为可选字段。
- SSO 类型：您要为书签配置的 SSO 类型。配置 SSO 后，用户无需在后续登录中输入凭据即可访问应用程序。支持以下 SSO 类型：
  - Unified Gateway：此 SSO 配置允许通过单个 URL 安全地远程访问应用程序的多个资源。
  - 自助身份验证：在此 SSO 配置中，提示 NetScaler Gateway 用户提供登录凭据以访问应用程序。
  - 基于 SAML 的身份验证：在这个 SSO 配置中，NetScaler Gateway 使用 IdP 来验证用户详细信息，生成 SAML 断言并将其发送到 SP。如果验证通过，则 SSO 成功。

> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



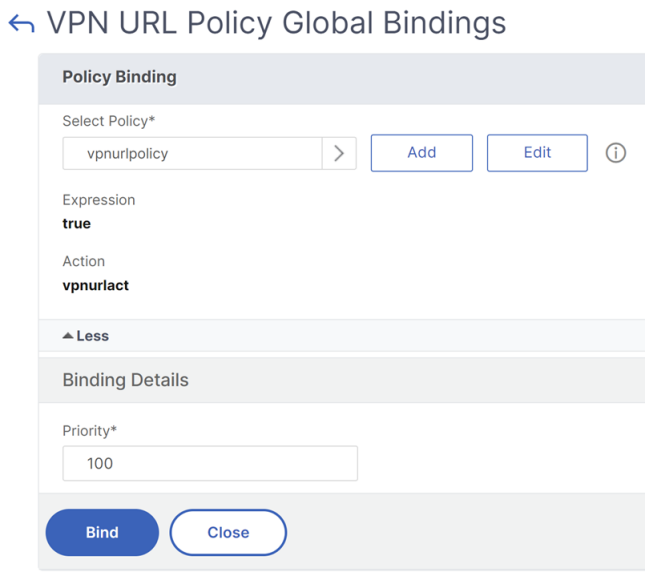
2. 创建 VPN URL 策略。

   - 导航到“配置”**>**“**NetScaler Gateway**”**>**“策略”**>**“**VPN URL**”。
   - 在 **VPN URL** 策略和配置文件 页面上，选择 **VPN URL** 策略 选项卡，然后单击 添加。
   - 更新必填字段，然后单击“创建”。
     - 名称：VPN URL 策略的名称。
     - 操作：选择已配置的 VPN URL 配置文件。如果下拉列表中没有配置文件，请单击“添加”并重复步骤 1。
     - 表达式：有关高级策略表达式的信息，请参阅策略和表达式。



3. 将 VPN URL 策略绑定到绑定点。

- 导航到“配置”**>**“**NetScaler Gateway**”**>**“策略”**>**“**VPN URL**”。
- 在 **VPN URL** 策略和配置文件 页面上，选择 **VPN URL** 策略 选项卡。
- 从“选择操作”下拉列表中选择“全局绑定”。
- 选择 VPN URL 策略。如果未列出任何策略，请单击“添加”并重复步骤 2。
- 在 绑定详细信息 部分中，为 VPN URL 策略分配优先级。



在 **CLI** 上

创建 **VPN URL** 操作：

在命令提示符处，键入以下内容：

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-
    vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment
    <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype
     <applicationtype>] \[-samlSSOProfile <string>]
```

NetScaler Gateway 支持对 VPN URL 操作进行以下操作：

- 添加

```
add vpn urlAction <name> -linkName <string> -actualURL <string>
    \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )]
    \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>]
    \[-applicationtype <applicationtype>] \[-samlSSOProfile <
    string>]
```

- 设置


```
set vpn urlAction <name> \[-vServerName <string>] \[-
    clientlessAccess \( ON | OFF )] \[-comment <string>] \[-
    iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <
    applicationtype>] \[-samlSSOProfile <string>]
```

- 未设置

```
unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
    comment] [-iconURL] [-ssotype] [-applicationtype] [-
    samlSSOProfile]
```

> 注意：
>
> 如果将无客户端访问设置为“开”，则可以确保对 Web 站点的请求从用户设备发送到 NetScaler Gateway，然后发送到 Web 站点。

- **show**

```
show vpn urlAction [<name>]
```

- 删除

```
remove vpn urlAction <name>
```

- 重命名

```
rename vpn urlAction <name>@ <newName>@
```

创建 **VPN URL** 策略：

NetScaler Gateway 支持 VPN URL 策略的以下操作：

- 添加

```
add vpn urlPolicy <name> -rule <expression> -action <string> [-
    comment <string>] [-logAction <string>]
```

- 设置

```
set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
    [-comment <string>] [-logAction <string>]
```

- 未设置

```
unset vpn urlPolicy <name> [-comment] [-logAction]
```

- **show**

```
show vpn urlPolicy [<name>]
```

- 删除


```
remove vpn urlPolicy <name>
```

- 重命名

```
rename vpn urlpolicy <name>@ <newName>@
```

- 统计数据

```
stat vpn urlpolicy \[<name>] \[-detail] \[-fullValues] \[-ntimes
   <positive\_integer>] \[-logFile <input\_filename>] \[-
   clearstats \( basic | full )]
```

将策略绑定到绑定点：

NetScaler Gateway 支持以下操作 VPN URL 策略绑定：

- 捆绑

```
bind vpn vserver <vserver name> -policy <string> -priority <
   positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
bind aaa group <groupName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
```

- 取消绑定

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```

> 注意：
>
> 绑定点是 aaauser、aaagroup、vpnvserver 和 vpnglobal。

端点策略

February 1, 2024

端点分析 (EPA) 是一个扫描用户设备并检测信息的过程，例如操作系统更新、防病毒、防火墙和 Web 浏览器软件的存在和版本级别。端点分析允许您在用户的设备连接到您的网络之前确定其是否满足您的要求。也可以将其配置为在用户

保持连接状态时定期检查是否有任何更改。您可以在用户会话期间检查用户设备上的文件、进程和注册表项，以确保该设备继续满足要求。

> 重要提示：
>
> - Endpoint Analysis 旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。
> - EPA 客户端可作为独立客户端使用，还与 Citrix Secure Access 客户端捆绑在一起。Citrix EPA 客户端和 Citrix Secure Access 客户端相互独立。

端点策略的工作方式

您可以将 NetScaler Gateway 配置为在用户登录之前检查用户设备是否满足特定要求。这称为预身份验证策略。您可以将 NetScaler Gateway 配置为检查用户设备中是否存在您在策略中指定的防病毒、防火墙、反垃圾邮件、进程、文件、注册表项、Internet 安全或操作系统。如果用户设备未通过预身份验证扫描，则不允许用户登录。

要验证预身份验证策略中未使用的其他要求，您可以配置会话策略并将其绑定到用户或组。这种类型的策略称为身份验证后策略，它在用户会话期间运行，以确保所需的标准（例如防病毒软件或进程）保持合规。

配置预身份验证或身份验证后策略时，NetScaler Gateway 会下载端点分析插件，然后在用户的设备上运行扫描。每次用户登录时，Endpoint Analysis 插件都会自动运行。

您可以使用以下三种类型的策略来配置端点策略：

- 使用“是”或“否”参数的预身份验证策略。扫描将确定用户设备是否满足指定的要求。如果扫描失败，用户将无法在登录页面上输入凭据。
- 会话策略是有条件的，可用于 SmartAccess。
- 会话策略中的客户端设备检查表达式。如果用户设备未能满足客户端设备检查表达式的要求，则可以将用户配置为置于隔离组中。如果用户设备通过扫描，则可以将用户置于可能需要其他检查的其他组中。

您可以将检测到的信息合并到策略中，从而可以根据用户设备授予不同的访问级别。例如，您可以向从具有当前防病毒和防火墙软件要求的用户设备远程连接的用户提供具有下载权限的完全访问权限。对于从不兼容设备连接的用户，您可以提供更严格的访问级别，允许用户在远程服务器上编辑文档，而无需下载文档。所有运行 EPA 的设备都被视为不合规设备。

端点分析执行以下基本步骤：

- 检查有关用户设备的初始信息集，以确定要应用哪些扫描。
- 运行所有适用的扫描。当用户尝试连接时，Endpoint Analysis 插件会检查用户设备是否满足预身份验证或会话策略中指定的要求。如果用户设备通过扫描，则允许用户登录。如果用户设备扫描失败，则不允许用户登录。

  注意：端点分析扫描在用户会话使用许可证之前完成。
- 将用户设备上检测到的属性值与配置的扫描中列出的所需属性值进行比较。
- 生成输出，验证是否找到所需的属性值。

> 注意：
>
> 创建端点分析策略的说明只是一般准则。一个会话策略中可以有许多设置。配置会话策略的具体说明可能包含配置特定设置的说明。但是，该设置可以是会话配置文件和策略中包含的许多设置之一。

EPA 表达式示例

以下是某些 EPA 组件的表达式示例，例如终止进程、删除文件和设备证书：

- Windows：
  - 终止进程：`sys.client_expr(\ “proc_0_perl\ “)-killProcess processToKill.exe`
  - 设备证书：`sys.client_expr( “device-cert_0_0” )`
  - 删除文件：`sys.client_expr(\ “proc_0_perl\ “)-deletefiles “C:/removefile.txt”`
- MAC
  - 终止进程：`sys.client_expr(\ “proc_0_perl\ “)-killProcess processToKill.exe`
  - 设备证书：`sys.client_expr( “device-cert_0_0” )`
  - 删除文件：`sys.client_expr(\ “proc_0_perl\ “)-deletefiles “C:/removefile.txt”`

评估用户登录选项

用户登录时，他们可以选择跳过端点分析扫描。如果用户跳过扫描，NetScaler Gateway 将此操作作为失败的端点分析处理。当用户扫描失败时，他们只能访问 Web Interface 或者通过无客户端访问获得。

例如，您想使用 Citrix Secure Access 客户端为用户提供访问权限。要使用插件登录 NetScaler Gateway，用户必须运行防病毒应用程序，例如诺顿防病毒软件。如果用户设备未运行应用程序，则用户只能使用 Receiver 登录并使用已发布的应用程序。您还可以配置无客户端访问，这将限制对指定应用程序（如 Outlook Web Access）的访问。

要配置 NetScaler Gateway 以实现此登录方案，请将限制性会话策略分配为默认策略。然后，您可以配置设置，以便在用户设备通过 Endpoint Analysis 扫描时将用户升级到特权会话策略。此时，用户可以访问网络层，可以使用 Citrix Secure Access 客户端登录。

要将 **NetScaler Gateway** 配置为首先强制执行限制性会话策略，请执行以下步骤：

- 如果指定的应用程序未在用户设备上运行，请在启用 ICA 代理的情况下配置全局设置和所有其他必要设置。
- 创建启用 Citrix Secure Access 客户端的会话策略和配置文件。

- 在会话策略的规则部分中创建一个表达式来指定应用程序，例如（`client.application.process(symantec.exe)exists`）

  用户登录时，首先应用会话策略。如果端点分析失败或用户跳过扫描，NetScaler Gateway 将忽略会话策略中的设置（会话策略中的表达式被视为 false）。因此，用户可以使用 Web Interface 或无客户端访问限制访问。如果端点分析通过，NetScaler Gateway 将应用会话策略，用户拥有对 Citrix Secure Access 客户端的完全访问权限。

跳过 **EPA** 扫描

您只能跳过身份验证后和高级身份验证的 EPA 扫描。所有支持的操作系统的浏览器都可以使用 Skip EPA。用户必须单击访问网关时出现的“跳过 **EPA**”按钮。如果用户跳过扫描，NetScaler Gateway 将此操作作为失败的端点分析处理。当用户扫描失败时，他们只能访问 Web Interface 或者通过无客户端访问获得。

另请参阅https://support.citrix.com/article/CTX200748。

Ubuntu 支持的端点分析扫描

为 Ubuntu 操作系统安装的 EPA 插件支持以下端点分析 (EPA) 扫描。列出了配置每项扫描的示例表达式以及 EPA 扫描。您可以在身份验证策略中配置这些表达式。

- 文件
  - 存在：：sys.client_expr（“file_0_/home/user/test.txt”）
  - **MD5** 校验和：sys.client_expr(“file_0*/home/user/test.txt_md5* ce780e271debcc29f551546e8db3368f”)
  - 文件中的文本（支持正则表达式）：sys.client_expr（“file_0_/home/user/test.txt_search_cloud”）
- 进程
  - 存在：sys.client_expr（“proc_0_perl”）
  - **MD5** 校验和：sys.client_expr（“proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a”）
  - 路径：sys.client_expr（“proc_0*perl_path*/usr/bin/perl”）
- 文件系统设备或装载点名称：sys.client_expr（“mountpoint_0_/sys”）

如果您使用的是高级策略，则可以从 GUI 生成每次扫描的表达式（安全 **> AAA >** 策略 **>** 身份验证 **>** 高级策略 **> EPA**）。

注意：在“表达式编辑器”页中，对于 Linux 客户端，可以选择“公 用”，然后选择“进程”、“文件”或“挂载点”。

预身份验证策略和配置文件

February 1, 2024

> 重要：
>
> 端点分析旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

您可以将 NetScaler Gateway 配置为在用户通过 NetScaler Gateway 身份验证之前检查用户的设备。如果用户的设备不符合贵组织的要求，这可以用来限制访问权限。设备检查可以使用特定于虚拟服务器的单个策略或全局策略来实现，如以下两个过程所述。

预身份验证策略由配置文件和表达式组成。您可以将配置文件配置为使用表达式来允许或拒绝某个进程在用户设备上运行。例如，文本文件 clienttext.txt 正在用户的设备上运行。当用户登录 NetScaler Gateway 时，您可以根据文本文件是否正在运行来允许或拒绝访问。如果您不想允许用户在进程运行时登录，则可以配置预身份验证配置文件，以便在用户登录之前停止该进程。

您可以为预身份验证策略配置以下设置：

- 表达式。包括以下设置以帮助您创建表达式：
  - 表达式。显示所有表达式。
  - 匹配任何表达式。配置策略以匹配所选表达式列表中存在的任何表达式。
  - 匹配所有表达式。配置策略以匹配所选表达式列表中存在的所有表达式。
  - 表格表达式。使用 `OR` (||)`or` `AND` (&&) 运算符创建包含现有表达式的复合表达式。
  - 高级自由格式。使用表达式名称和 `OR` (||)`and` `AND` (&&) 运算符创建自定义复合表达式。只选择所需的那些表达式，然后从所选表达式列表中省略其他表达式。
  - 添加。创建表达式。
  - 修改。修改现有表达式。
  - 删除。从复合表达式列表中删除选定的表达式。
  - 命名表达式。选择已配置的命名表达式。您可以从 NetScaler Gateway 上已存在的表达式菜单中选择命名表达式。
  - 添加表达式。将选定的命名表达式添加到策略中。
  - 替换表达式。将选定的命名表达式替换为策略。
  - 预览表达式。显示选择命名表达式时在 NetScaler Gateway 上配置的详细字符串。

配置预验证配置文件

使用 **GUI** 全局配置预身份验证配置文件

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击“全局设置”。

2. 在详细信息窗格的“设置”下，单击“更改预身份验证设置”。
3. 在“全局预身份验证设置”对话框中，配置以下设置：

   a) 在“操作”中，选择“允许”或“拒绝”。

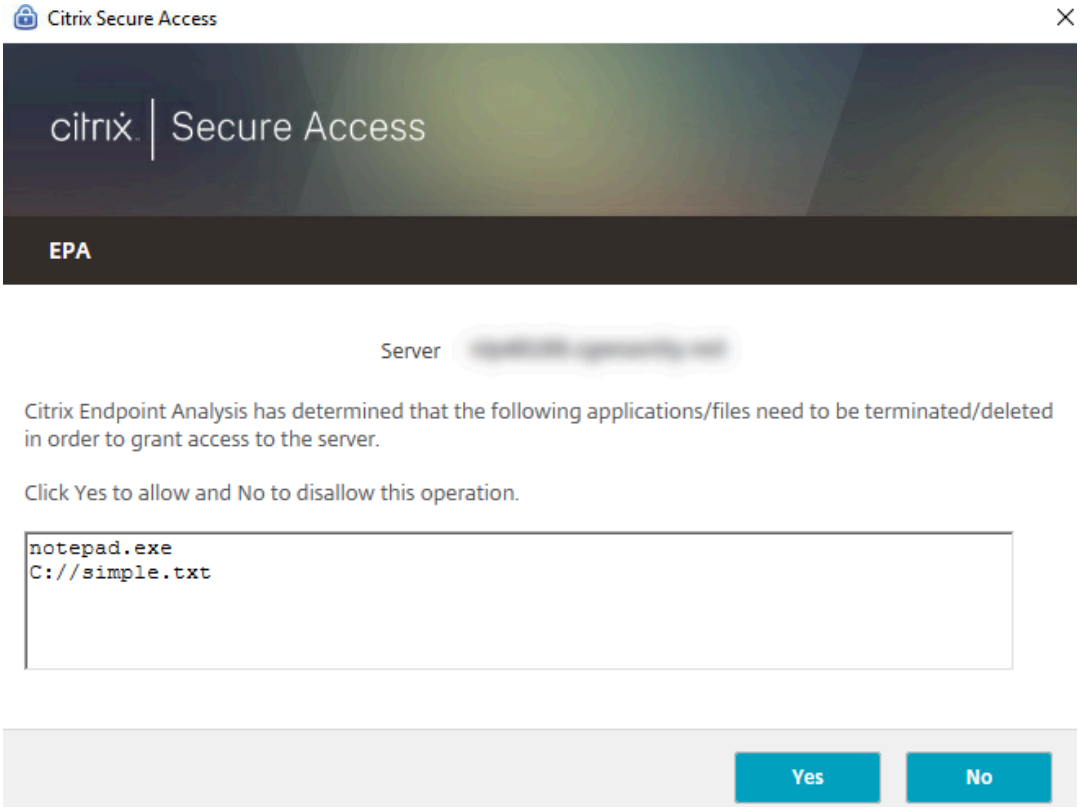
   端点分析发生后拒绝或允许用户登录。

   b) 在 要取消的进程中，输入流程。

   这指定了端点分析插件必须停止的进程。

   c) 在 要删除的文件中，输入文件名。

   这指定了端点分析插件必须删除的文件。删除或取消流程时，会向最终用户显示通知。



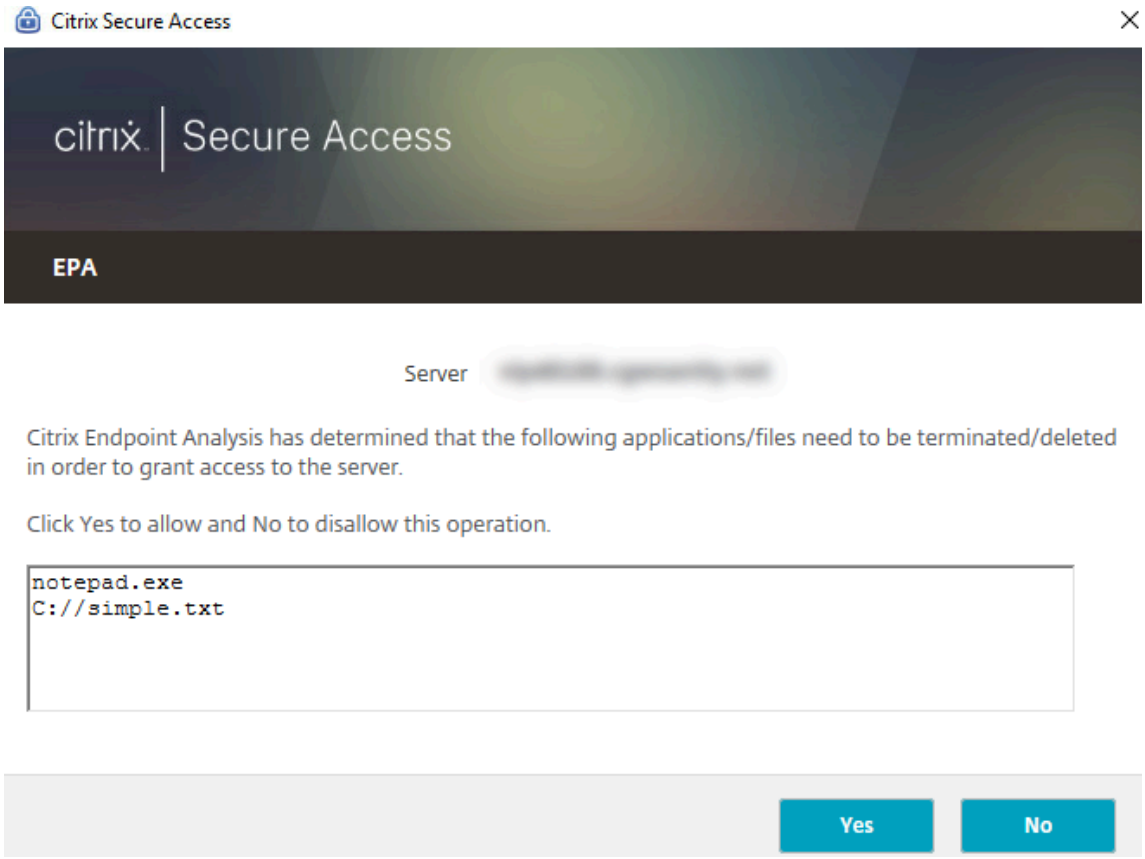
4. 在“表达式”中，您可以保留表达式 ns_true 或为特定应用程序（例如防病毒软件或安全软件）构建表达式，然后单击“确定”。

使用 **GUI** 配置预身份验证配置文件

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证**/**授权，然后单击“预身份验证 **EPA**”。
2. 在详细信息窗格的“配置文件”选项卡上，单击“添加”。
3. 在 名称中，键入要检查的应用程序的名称。
4. 在 操作中，选择 允许 或 拒绝。
5. 在 要取消的进程中，键入要停止的进程的名称。

6. 在“要删除的文件”中，键入要删除的文件的名称，例如 c:\clientext.txt，单击“创建”，然后单击“关闭”。

   这指定了端点分析插件必须删除的文件。删除或取消流程时，会向最终用户显示通知。



如果您使用 GUI 配置预身份验证配置文件，则可以通过单击“策略”选项卡上的“添加”来创建预身份验证 策略。在 创建预身份验证策略 对话框中，从 请求配置文件菜单中选择配置文件。

将预配置的表达式添加到预身份验证策略

NetScaler Gateway 附带预配置的表达式，称为命名表达式。配置策略时，可以为策略使用命名表达式。例如，您希望预身份验证策略检查具有更新病毒定义的赛门铁克防病毒 10。创建预身份验证策略并按照以下过程中所述添加表达式。

创建预身份验证或会话策略时，可以在创建策略时创建表达式。然后，您可以使用表达式将策略应用于虚拟服务器或全局应用。

以下过程介绍如何使用配置实用程序将预配置的防病毒表达式添加到策略中。

将命名表达式添加到预身份验证策略

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证/授权，然后单击“预身份验证 **EPA**”。

2. 在详细信息窗格中，选择一个策略，然后单击“打开”。
3. 在 命名表达式旁边，选择 反病毒，然后从列表中选择防病毒产品。
4. 单击 添加表达式，单击 创建，然后单击 关闭。

配置定制表达式

自定义表达式是您在策略中创建的表达式。创建表达式时，需要配置表达式的参数。

您也可以创建自定义表达式来引用常用字符串。这简化了配置预身份验证策略以及维护已配置表达式的过程。

例如，您要为 Symantec antivirus 10 创建自定义表达式，并确保病毒定义的有效期不超过三天。创建策略，然后配置表达式以指定病毒定义。

以下过程显示如何在预身份验证策略中创建表达式。您可以在会话策略中使用相同的步骤。

创建预身份验证策略和自定义表达式

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证**/**授权，然后单击“预身份验证 **EPA**”。
2. 在详细信息窗格中，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在创建身份验证配置文件对话框的 名称中，键入配置文件的名称，然后在 操作中选择 允许，然后单击 创建。
6. 在“创建预身份验证策略”对话框中，单击“我匹配任何表达式”旁边的“添加”。
7. 在 表达式类型中，选择 客户端安全。
8. 配置以下设置：
    a) 在 组件中，选择 反病毒。
    b) 在 名称中，键入应用程序的名称。
    c) 在限定符中，选择版本。
    d) 在 运算符中，选择 **==**。
    e) 在 值中，键入值。
    f) 在“新鲜度”中，键入 3，然后单击“确定”。
9. 在“创建预身份验证策略”对话框中，单击“创建”，然后单击“关闭”。

配置自定义表达式时，它会添加到策略对话框中的“表达式”框中。

配置复合表达式

预身份验证策略可以有一个配置文件和多个表达式。如果配置复合表达式，则可以使用运算符来指定表达式的条件。例如，您可以将复合表达式配置为要求用户设备运行以下防病毒应用程序之一：

- 赛门铁克防病毒软件 10

- McAfee Antivirus 11
- Sophos 杀毒软件 4

您可以使用 OR 运算符配置表达式以检查上述三个应用程序。如果 NetScaler Gateway 在用户设备上检测到任何应用程序的正确版本，则允许用户登录。策略对话框中的表达式如下所示：

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

有关复合表达式的详细信息，请参阅 配置复合表达式。

绑定预身份验证策略

创建预身份验证策略后，将该策略绑定到其适用的级别。您可以将预身份验证策略绑定到虚拟服务器或全局绑定。

全局创建和绑定预身份验证策略

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格中，单击 更改预身份验证设置。
3. 在“全局预身份验证设置”对话框的“操作”中，选择 允许 或 拒绝。
4. 在名称中，键入策略的名称。
5. 在“全局预身份验证设置”对话框中，选择 命名表达式旁边的“常规”，选择“**True**”值，单击“添加表达式”，单击“创建”，然后单击关闭。

将预身份验证策略绑定到虚拟服务器

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击“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. 在配置 NetScaler Gateway 虚拟服务器对话框中，单击 策略 选项卡，然后单击 预身份验证。
4. 在详细信息下，单击 插入策略，然后在策略名称下，选择预身份验证策略。
5. 单击确定。

取消绑定和删除预身份验证策略

如有必要，您可以从 NetScaler Gateway 中删除预身份验证策略。在删除预身份验证策略之前，请将其从虚拟服务器或全局解除绑定。

取消绑定全局预身份验证策略

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证/授权，然后单击“预身份验证 **EPA**”。
2. 在详细信息窗格中，选择一个策略，然后在“操作”中，单击“全局绑定”。

3. 在“将 身份验证预策略绑定/取消绑定到全局”对话框中，选择一个策略，单击“取消绑定策略”，然后单击“确定”。

从虚拟服务器取消绑定预身份验证策略

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击“虚拟服务器”。
2. 在 配置 **NetScaler Gateway** 虚拟服务器 对话框中，单击 策略 选项卡，然后单击 预身份验证。
3. 选择策略，然后单击 取消绑定策略。

取消绑定预身份验证策略时，您可以从 NetScaler Gateway 中删除该策略。

删除预身份验证策略

1. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证/授权，然后单击“预身份验证 **EPA**”。
2. 在详细信息窗格中，选择一个策略，然后单击 删除。

设置预身份验证策略的优先级

您可以有多个绑定到不同级别的预身份验证策略。例如，您有一个检查全局绑定的特定防病毒应用程序的策略和绑定到虚拟服务器的防火墙策略。用户登录时，首先应用绑定到虚拟服务器的策略。然后应用全局绑定的策略。

您可以更改预身份验证扫描的发生顺序。要使 NetScaler Gateway 首先应用全局策略，请更改绑定到虚拟服务器的策略的优先级编号，使其具有比全局绑定的策略更高的优先级编号。例如，将全局策略的优先级编号设置为 1，将虚拟服务器策略设置为 2。用户登录时，NetScaler Gateway 首先运行全局策略扫描，然后运行虚拟服务器策略扫描。

更改预身份验证策略的优先级

1. 在“配置”选项卡上，单击 **NetScaler Gateway**，然后单击“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. 在策略选项卡上，单击 预身份验证。
4. 在“优先级”下，键入策略的优先级编号，然后单击“确定”。

身份验证后策略

February 1, 2024

> 重要：
>
> 端点分析旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

身份验证后策略是用户设备为保持会话活动状态而必须满足的一组通用规则。如果策略失败，与 NetScaler Gateway 的连接将终止。配置身份验证后策略时，可以为可以设置条件的用户连接配置任何设置。

您可以使用会话策略配置身份验证后策略。首先，创建应用该策略的用户。然后，将用户添加到组中。接下来，将会话、流量策略和 Intranet 应用程序绑定到组。

您还可以将组指定为授权组。此类组允许您根据会话策略中的客户端设备检查表达式将用户分配到组。

如果用户设备不符合该策略的要求，您还可以配置身份验证后策略以将用户置于隔离组中。一个简单的策略包括客户端设备检查表达式和一条消息。当用户位于隔离组中时，用户可以登录 NetScaler Gateway；但是，他们对网络资源的访问权限有限。

不能使用相同的会话配置文件和策略创建授权组和隔离组。创建身份验证后策略的步骤相同。创建会话策略时，可以选择授权组或隔离组。您可以创建两个会话策略，并将每个策略绑定到组。

身份验证后策略也可用于 SmartAccess。有关 SmartAccess 的更多信息，请参阅 在 NetScaler Gateway 上配置 SmartAccess。

> 注意：
>
> 此功能仅适用于 Citrix Secure Access 客户端。如果用户使用 Citrix Workspace 应用程序登录，则端点分析扫描仅在登录时运行。

配置身份验证后策略

您可以使用会话策略配置身份验证后策略。一个简单的策略包括客户端设备检查表达式和一条消息。

使用 **GUI** 配置身份验证后策略

1. 展开 **NetScaler Gateway >** 策略，然后单击“会话”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在 客户端安全下，单击 覆盖全局，然后单击 新建。
8. 配置客户端设备检查表达式，然后单击“创建”。
9. 在“客户端安全”下的“隔离组”中，选择一个组。
10. 在 错误消息中，键入身份验证后扫描失败时希望用户收到的消息。

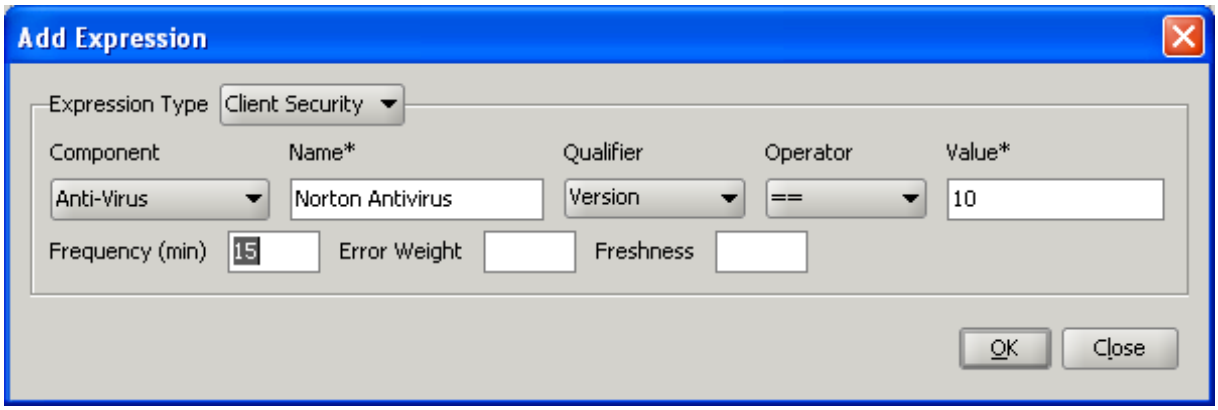
11. 在授权组下，单击 覆盖全局，选择一个组，单击 添加，单击 确定，然后单击 创建。
12. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

配置身份验证后扫描的频率

您可以将 NetScaler Gateway 配置为按指定的时间间隔运行身份验证后策略。例如，您配置了客户端设备检查策略，并希望该策略每 10 分钟在用户设备上运行一次。您可以通过在策略中创建自定义表达式来配置此频率。

> 注意：
>
> 身份验证后策略的频率检查功能仅适用于 Citrix Secure Access 客户端。如果用户使用 Citrix Workspace 应用程序登录，则端点分析扫描仅在登录时运行。

您可以按照“配置 身份验证后策略”过程设置配置客户端设备检查策略时的频率（以分钟为单位）。下图显示了可以在“添加表达式”对话框中输入频率值的位置。



隔离和授权组

当用户登录 NetScaler Gateway 时，您可以将他们分配给在 NetScaler Gateway 或安全网络中的身份验证服务器上配置的组。如果用户未能通过身份验证后扫描，则可以将该用户分配到称为隔离组的受限组，该组会限制对网络资源的访问。

您还可以使用授权组来限制用户对网络资源的访问。例如，您可能有一组合同人员只能访问您的电子邮件服务器和文件共享。当用户设备通过您在 NetScaler Gateway 上定义的设备检查要求时，用户可以动态成为组的成员。

您可以使用全局设置或会话策略来配置绑定到用户、组或虚拟服务器的隔离和授权组。您可以根据会话策略中的客户端设备检查表达式将用户分配到组。当用户是组成员时，NetScaler Gateway 会根据组成员资格应用会话策略。

配置授权组

配置 Endpoint Analysis 扫描时，可以在用户设备通过扫描时将用户动态添加到授权组。例如，您可以创建端点分析扫描来检查用户设备域成员身份。在 NetScaler Gateway 上，创建一个名为“加入域的计算机”的本地组，然后将其

添加为通过扫描的任何人的授权组。当用户加入组时，用户将继承与该组关联的策略。

您无法将授权策略全局绑定或绑定到虚拟服务器。当用户未配置为 NetScaler Gateway 上另一个组的成员时，可以使用授权组提供一组默认的授权策略。

使用会话策略配置授权组

1. 导航到 **NetScaler Gateway >** 策略，然后单击 会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“安全”选项卡上，单击“高级设置”。
7. 在“授权组”下，单击“覆盖全局”，然后从下拉列表中选择一个组。
8. 单击“添加”，单击“确定”，然后单击“创建”。
9. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”，单击“创建”，然后单击“关闭”。

创建会话策略后，可以将其绑定到用户、组或虚拟服务器。

配置全局授权组

1. 展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。
4. 在“授权组”下，从下拉列表中选择一个组。
5. 单击“添加”，然后单击“确定”。

如果要全局删除授权组或从会话策略中删除授权组，请在“安全设置-高级”对话框中，从列表中选择授权组，然后单击“删除”。

配置隔离组

配置隔离组时，您可以使用会话配置文件中的“安全设置-高级设置”对话框配置客户端设备检查表达式。

为隔离组配置客户端设备检查表达式

1. 导航到 **NetScaler Gateway >** 策略，然后单击 会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。

6. 在“安全”选项卡上，单击“高级设置”。
7. 在 客户端安全下，单击 覆盖全局，然后单击 新建。
8. 在“客户端表达式”对话框中，配置客户端设备检查表达式，然后单击“创建”。
9. 在隔离组中，选择该组。
10. 在“错误消息”中，键入描述用户问题的消息，然后单击“创建”。
11. 在“创建会话策略”对话框中，在“命名表达式”旁边，选择“常规”，选择“**True** 值”，单击“添加表达式”。
12. 单击“创建”，然后单击“关闭”。

创建会话策略后，将其绑定到用户、组或虚拟服务器。

> 注意：
>
> 如果 Endpoint Analysis 扫描失败并将用户置于隔离组中，则绑定到隔离组的策略只有在没有直接绑定到该用户且优先级编号与绑定到隔离组的策略相同或低的策略时，绑定到隔离组的策略才有效。

配置全局隔离组

1. 展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“安全”选项卡上，单击“高级设置”。
4. 在“客户端安全”中，配置客户端设备检查表达式。
5. 在隔离组中，选择该组。
6. 在“错误消息”中，键入向用户描述问题的消息，然后单击“确定”。

用户设备的预身份验证设备检查表达式

February 1, 2024

> 重要：
>
> 端点分析旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

NetScaler Gateway 在用户登录期间或会话期间的其他配置时间提供各种端点合规性检查，以帮助验证用户设备。只有通过这些检查的用户设备才允许建立 NetScaler Gateway 会话。

以下是您可以在 NetScaler Gateway 上配置的对用户设备的检查类型：

- 反垃圾邮件
- 防病毒
- 文件策略
- 互联网安全

- 操作系统
- 个人防火墙
- 流程策略
- 注册表策略
- 服务策略

如果用户设备上的设备检查失败，则在后续检查通过之前不会建立新的连接（如果是定期检查）；但是，流经现有连接的流量会继续通过 NetScaler Gateway。

您可以使用配置实用程序在旨在对用户设备进行检查的会话策略中配置预身份验证策略或设备检查表达式。

配置防病毒、防火墙、互联网安全或反垃圾邮件表达式

您可以在“添加表达式”对话框中配置防病毒、防火墙、Internet 安全和反垃圾邮件策略的设置。每个策略的设置都是相同的：不同之处在于您选择的值。例如，如果要检查用户设备的 Norton 防病毒版本 10 和 ZoneAlarm Pro，则可以在会话或预身份验证策略中创建两个表达式，用于指定每个应用程序的名称和版本号。

选择“客户端安全”作为表达式类型时，可以配置以下内容：

- 组件：客户端安全性的类型，例如防病毒、防火墙或注册表项。
- 名称：应 用程序、进程、文件、注册表项或操作系统的名称。
- 限定符：表达式检查的组件的版本或值。
- 运算符：检查值是否存在或等于该值。
- 值：用户设备上的防病毒、防火墙、Internet 安全或反垃圾邮件软件的应用程序版本。
- 频率：运行身份验证后扫描的频率，以分钟为单位。
- 错误权重：当多个表达式具有不同的错误字符串时，为嵌套表达式中包含的每条错误消息分配的权重。权重决定显示哪条错误消息。
- 新鲜度：定义病毒定义的年龄。例如，您可以配置表达式，使病毒定义的时间不超过三天。

将客户端设备检查策略添加到预身份验证或会话策略中

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
   b) 在配置实用程序的配置选项卡的导航窗格中，展开 NetScaler Gateway > 策略 > 身份验证/授权，然后单击预身份验证 **EPA**。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在匹配任何表达式旁边，单击添加。
5. 在“添加表达式”对话框的“表达式类型”中，选择“客户端安全”。
6. 配置以下内容的设置：

a) 在组件中，选择要扫描的项目。
b) 在名称中，键入应用程序的名称。
c) 在限定赛中，选择 版本。
d) 在运算符中，选择值。
e) 在“值”中，键入客户端设备检查字符串，单击“确定”，单击“创建”，然后单击“关闭”。

配置服务策略

服务是在用户设备上静默运行的程序。创建会话或预身份验证策略时，可以创建一个表达式，以确保在建立会话时用户设备正在运行特定服务。

配置服务策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中，在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击“会话”。
   b) 在配置实用程序中，在“配置”选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略 **>** 身份验证/授权，然后单击“预身份验证 EPA”。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在匹配任何表达式旁边，单击添加。
5. 在“添加表达式”对话框的“表达式类型”中，选择“客户端安全”。
6. 配置以下内容的设置：
   a) 在组件中，选择服务。
   b) 在名称中，键入服务的名称。
   c) 在限定符中，留空或选择版本。
   d) 根据您在限定符中的选择，执行以下操作之一：
      - 如果留空，请在运算符中选择 == 或!=
      - 如果选择了“版本”，请在“运算符”的“值”中键入值，单击“确定”，然后单击“关闭”。

您可以在以下位置查看基于 Windows 的计算机上所有可用服务的列表以及每项服务的状态：

控制面板 **>** 管理 工具 **>** 服务

> 注意：
>
> 每项服务的服务名称与列出的名称不同。通过查看
> 属性对话框来检查服务的名称。

配置流程策略

创建会话或预身份验证策略时，您可以定义一个规则，要求所有用户设备在用户登录时运行特定进程。该过程可以是任何应用程序，也可以包括自定义的应用

注意：在基于 Windows 的计算机上运行的所有进程的列表显示在 Windows 任务管理器的“进程”选项卡上。

配置进程策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway\ >** 策略，然后单击会话。
   b) 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略**\ >** 身份验证**/**授权，然后单击预身份验证 EPA。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在匹配任何表达式旁边，单击添加。
5. 在“添加表达式”对话框的“表达式类型”中，选择“客户端安全”。
6. 配置以下内容的设置：
   a) 在组件中，选择进程。
   b) 在名称中，键入应用程序的名称。
   c) 在运算符中，选择 EXISTS 或 NOTEXISTS，单击确定，然后单击关闭。

配置 Endpoint Analysis 策略（身份验证前或身份验证后）以检查进程时，可以配置 MD5 校验和。

为策略创建表达式时，可以将 MD5 校验和添加到正在检查的进程中。例如，如果您正在检查 notepad.exe 是否在用户设备上运行，则表达式为：
CLIENT.APPLICATION.PROCESS(notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

配置操作系统策略

创建会话或预身份验证策略时，可以配置客户端设备检查字符串，以确定用户登录时用户设备是否正在运行特定的操作系统。您还可以配置表达式以检查特定的 Service Pack 或修补程序。

Windows 和 Macintosh 的值为：

操作系统	值
macOS X	macOS
Windows 8.1	win8.1

操作系统	值
Windows 8	win8
Windows 7	win7
Windows Vista	vista
Windows XP	winxp
Windows Server 2008	win2008
Windows Server 2003	win2003
Windows 2000 Server	win2000
Windows 64 位平台	win64

使用 **GUI** 配置操作系统策略

1. 在导航窗格中，执行以下操作之一：
   a) 导航到 **NetScaler Gateway >** 策略，然后单击 会话。
   b) 导航到 **NetScaler Gateway >** 策略 **>** 预身份验证。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在 请求操作 中，选择现有操作或创建一个操作。
5. 单击 **Expression Editor**（表达式编辑器）。
6. 在 选择表达式类型中，选择 客户端安全。
7. 配置以下内容的设置：
   a) 在 组件中，选择 操作系统。
   b) 在 名称中，键入操作系统的名称。
   c) 在限定符中，执行以下操作之一：
      - 将字段留空
      - 选择 服务包
      - 选择 修补程序
      - 选择 版本（仅适用于 macOS）
   d) 根据您在步骤 7 中的选择，在 Operator 中，执行以下操作之一：
      - 如果限定符为空，请在运算符中选择 EQUAL (= =)、NOTEQUAL (!=)、EXISTS 或 NOTEXISTS。
      - 如果选择了 Service Pack 或 Hotfix，请选择运算符，然后在值中键入值。
8. 单击 完成，然后单击 关闭。

如果要配置 Service Pack（例如 client.os）（winxp）.sp，如果 值 字段中没有数字，NetScaler Gateway 将返回错误消息，因为表达式无效。

如果操作系统存在补丁包 3 和补丁包 4 等服务包，则可以仅为 Service Pack 4 配置检查，因为 Service Pack 4 的存在会自动表明存在以前的服务包。

配置注册表策略

创建会话或预身份验证策略时，可以检查用户设备上是否存在注册表项以及注册表项的值。只有当特定条目存在或具有配置的值或更高的值时，才会建立会话。

配置注册表达式时，请遵循以下准则：

- 四个反斜杠用于分隔键和子键，例如

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- 下划线用于分隔子项和关联的值名称，例如

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- 反斜杠 (\) 用于表示空格，如以下两个示例所示：

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

以下是注册表表达式，用于在用户登录时查找 Citrix Secure Access 客户端注册表项：

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> 注意：
>
> 如果您正在扫描注册表项和值，并在“表达式”对话框中选择“高级自由格式”，则表达式必须以 CLIENT.REG 开头。

以下最常见的五种类型支持注册表检查：

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

要检查的注册表值使用以下类型：

- 字符串

  对于字符串值类型，检查区分大小写。

- DWORD

  对于 DWORD 类型，将比较该值，且必须相等。

- 扩展字符串

  不支持其他类型，例如二进制和多字符串。

- 只支持‘==’比较运算符。
- 不支持其他比较运算符，例如 <、> 和区分大小写的比较。
- 注册表字符串的总长度必须小于 256 字节。

您可以向表达式添加值。该值可以是软件版本、Service Pack 版本或注册表中显示的任何其他值。如果注册表中的数据值与您正在测试的值不匹配，则拒绝用户登录。

> 注意：
>
> 您无法扫描子项中的值。扫描必须与命名值和关联的数据值相匹配。

配置注册表策略

1. 在配置实用程序的导航窗格中，执行以下操作之一：
   a) 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway\ >** 策略，然后单击会话。
   b) 在配置实用程序中的配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略**\ >** 身份验证**/**授权，然后单击预身份验证 EPA。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在匹配任何表达式旁边，单击添加。
5. 在“添加表达式”对话框的“表达式类型”中，选择“客户端安全”。
6. 配置以下内容的设置：
   a) 在组件中，选择注册表。
   b) 在名称中，键入注册表项的名称。
   c) 在限定符中，留空或选择值。
   d) 在 Operator 中，执行以下操作之一：
      - 如果限定符留空，请选择“EXISTS”或“NOTEXISTS”
      - 如果您在限定词中选择了值，请选择 == 或!==
   e) 在“值”中，键入注册表编辑器中显示的值，单击“确定”，然后单击“关闭”。

配置复合客户端设备检查表达式

您可以组合客户端设备检查字符串以形成复合客户端设备检查表达式。

NetScaler Gateway 中支持的布尔运算符包括：

- 和 (&&)

或者 (

-
- Not (!)

为了提高精度，您可以使用括号将字符串组合在一起。

> 注意：
>
> 如果使用命令行配置表达式，请在形成复合表达式时使用圆括号将设备检查表达式分组在一起。使用括号可以改善对客户端表达式的理解和调试。

使用 **AND (&&)** 运算符配置策略

AND (&&) 运算符的工作原理是合并两个客户端设备检查字符串，这样复合校验只有在两个校验都为 True 时才能通过。从左到右计算表达式，如果第一次检查失败，则不会执行第二次检查。

您可以使用关键字“AND”或符号“&&”配置 AND (&&) 运算符。

示例：

以下是客户端设备检查，用于确定用户设备是否已安装并正在运行版本 7.0 的 Sophos 防病毒软件。它还会检查 Net Logon 服务是否在同一台计算机上运行。

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
EXISTS
```

此字符串也可以配置为：

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
EXISTS
```

使用 **OR (||)** 运算符配置策略

OR（||）运算符的工作原理是组合两个设备校验字符串。当任何一项检查为 true 时，复合检查通过。从左到右计算表达式，如果第一次检查通过，则不会执行第二次检查。如果第一次检查没有通过，则执行第二次检查。

可以使用关键字 OR 或符号 || 配置 OR（||）运算符。

示例：

下面是客户端设备检查，用于确定用户设备上是否有文件 `c:\\file.txt` 或者正在运行 `putty.exe` 进程。

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```


此字符串也可以配置为

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```

使用 **NOT (!)** 配置策略操作者

NOT (!) 或者否定运算符否定客户端设备检查字符串。

示例：

如果文件 c:\sophos_virus_defs.dat 文件的存在时间不超过两天，则会通过以下客户端设备检查：

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

EPA 扫描是 **nFactor** 身份验证的一个因素

February 1, 2024

> 重要：
>
> 端点分析旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

以下是 nFactor EPA 的一些基本实体。

EPA 操作： EPA 操作是 nFactor EPA 引入的一种操作类型。它包含以下内容：

- 客户端设备检查表达式：此表达式被发送到网关 EPA 插件进行评估。
- 成功组：如果配置了该组，如果 EPA 结果为 True，则该组将继承给网关会话。
- 隔离组：如果配置了此组，如果 EPA 结果为假，则该组将继承给网关会话。
- killProcess：这表示 EPA 进程必须终止的进程的名称。
- deleteFiles：指定 EPA 进程必须删除的文件以逗号分隔的路径。

在会话期间，可以使用组来确定客户是否满足某些 EPA 条件。
如果在给定因素下，EPA 失败且最后一项操作不包含“隔离组”，则终止对该用户的身份验证。
如果存在“隔离组”，则继续进行身份验证，管理员可以检查该组是否授予有限访问权限。有关详细信息，请参阅 EPA 执行。

EPA 策略：在 nFactor 中，添加所有策略的语法都相同“添加身份验证策略”。但是，操作的类型使该策略有资格成为 EPA 策略。

EPA 系数： EPA 系数是一种常规的策略标签。没有一个名为 EPA 因素的实体。一旦 EPA 策略与某个因素绑定，它就会继承使其成为 EPA 因素的某些属性。

> 注意：
>
> 本文档中通常使用“EPA 因素”一词来指代 EPA 策略中的一个因素。

EPA —隔离：如果在给定因素下，所有操作的所有客户端设备检查表达式均失败，并且如果最后一个操作包含“隔离组”，则将该组添加到会话中并调查 nextFactor。也就是说，尽管失败了，但“隔离小组”的存在使会议有资格进入下一阶段。但是，由于继承了特殊组，管理员可以将会话授予受限访问权限或额外的身份验证策略（如 OTP 或 SAML）。

如果上次操作时没有隔离组，则身份验证将在失败时终止。

nFactor 中的 **EPA** 还使用以下实体：

- **LoginSchema**：登录表单的 XML 表示形式。它定义了登录表单的“视图”，还具有“因素”的属性。
- 策略标签或策略因素：它是一组在给定身份验证阶段尝试的策略。
- 虚拟服务器标签：虚拟服务器也是策略标签，即可以将策略绑定到虚拟服务器。但是，虚拟服务器是各种策略标签的集合，因为它是用户访问的入口点。
- 下一个因素：它用于指定给定身份验证策略成功后要采用的策略标签/因素。
- **NO_AUTHN** 策略：其操作总是成功的特殊策略。
- 直通因素：是一个策略标签/因素，其登录架构不包含视图。这表示 NetScaler 设备在没有用户干预的情况下以给定因素继续进行身份验证。

有关更多信息，请参阅 nFactor 概念、实体和术语。

EPA Factor 互斥

EPA 因素包含一项或多项 EPA 策略。一旦 EPA 策略绑定到某个因素，则不允许针对该因素使用常规身份验证策略。此限制是为了提供最佳的用户体验和端点分析的干净分离。此规则的唯一例外是 No_AUTHN 策略。由于 NO_AUTHN 策略是用于模拟“故障时跳转”的特殊策略，因此 EPA 系数允许使用该策略。

EPA 执行

在任何给定因素（包括虚拟服务器因素）下，在提供登录表单之前，NetScaler 设备会检查是否为 EPA 配置了该因素。如果是这样，它会向客户端 (UI) 发送特定的响应，以便触发 EPA 序列。此序列包括客户端请求客户端设备检查表达式并发送结果。

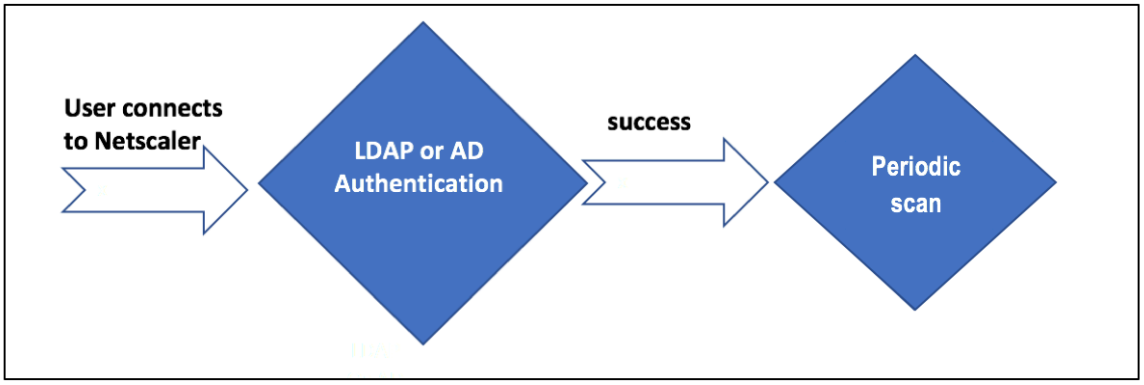
一个因素中所有策略的客户端设备检查表达式会立即发送给客户端。在 NetScaler 设备上获得结果后，将按顺序评估所有操作中的每个表达式。导致 EPA 成功的第一个操作将终止该因素，如果配置了 DefaultGroup，则会继承到会话中。如果遇到 No_AUTHN 策略，它将被视为自动成功。如果指定了 nextFactor，则设备将继续使用该因素。否则，身份验证将终止。

此条件也适用于第一个因素。如果在虚拟服务器上的 EPA 之后没有身份验证策略因素，则身份验证将终止。这与传统的策略行为不同，后者始终在 EPA 之后显示用户的登录页面。

但是，如果没有成功的 EPA 策略，NetScaler Gateway 将查看为该因素或级联中最后一个 EPA 策略配置的隔离组。如果使用隔离组配置了最后一个策略，则会将该组添加到会话中，并检查 nextFactor。如果存在 nextFactor，则身份验证将继续进行该因素。否则，身份验证将完成。

将 **EPA** 扫描配置为在身份验证后运行

您可以将 EPA 扫描配置为在身份验证后运行。在以下示例中，EPA 扫描用作 nFactor 或多重身份验证的最终检查。在此设置中，如果 EPA 扫描在任何此类检查期间失败，会话将终止。



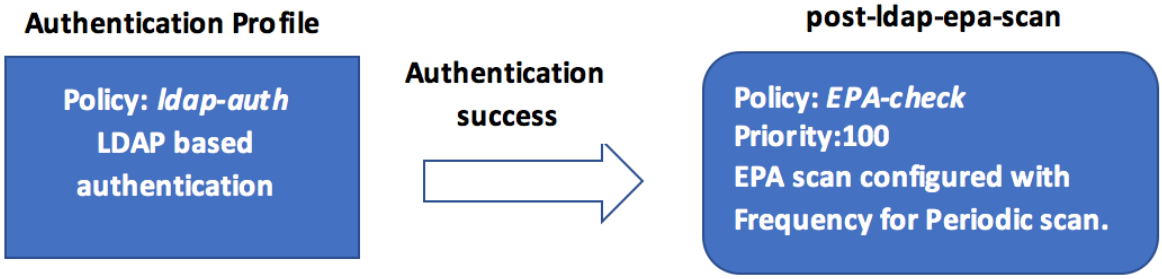
- 用户尝试连接到 NetScaler Gateway 虚拟 IP。
- 将向用户呈现一个包含用户名和密码字段的登录页面，以提供登录凭据。使用这些凭据，LDAP 或基于 AD 的身份验证将在后端执行。如果成功，将向用户显示一个弹出窗口以授权 EPA 扫描。
- 用户授权后，将执行 EPA 扫描，并根据用户客户端设置的成功或失败提供访问权限。
- 如果扫描成功，则会定期执行 EPA 扫描，以了解配置的设备检查要求是否仍然得到满足。
- 如果 EPA 扫描在任何此类检查期间失败，则会话将终止。

必备条件

假定以下配置已到位：

- VPN 虚拟服务器、网关和身份验证虚拟服务器配置
- LDAP 服务器配置和相关策略。

以下部分捕获所需的策略和策略标签配置，以及策略和策略标签到身份验证配置文件的映射。



在 **CLI** 上

1. 创建在 LDAP 身份验证之前执行 EPA 扫描的操作，并将其与 EPA 扫描策略相关联。

```
add authentication epaAction pre-ldap-epa-action -csecexpr "sys.client_expr ("proc_2_firefox")"

add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-epa-action
<!--NeedCopy-->
```

前面的表达式会扫描进程“Firefox”是否正在运行。EPA 客户端每 2 分钟检查一次进程是否存在，由扫描表达式中的数字“2”表示。

2. 配置托管 EPA 扫描策略的策略标签 `pre-ldap-epa-label`。

```
add authentication policylabel pre-ldap-epa-label -loginSchema LSCHEMA_INT
<!--NeedCopy-->
```

> 注意：
>
> LSCHEMA_INT 是一个没有架构（无架构）的内置架构，这意味着在此步骤中不会向用户显示其他网页。

3. 将步骤 1 中配置的策略与步骤 2 中配置的策略标签相关联。这样就完成了身份验证机制。

```
bind authentication policylabel pre-ldap-epa-label -policyName pre-ldap-epa-pol -priority 100 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. 配置 LDAP 操作和策略。

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN -passwdChange ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
<!--NeedCopy-->
```

5. 创建启用 SSO 的登录架构。

```
add authentication loginSchema ldap-schema -authenticationSchema "/nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
<!--NeedCopy-->
```

6. 配置策略标签 `ldap-pol-label`，用于托管 LDAP 身份验证策略。

```
add authentication policylabel ldap-pol-label -loginSchema ldap-schema
```



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

7. 将步骤 5 中配置的登录架构绑定到步骤 6 中配置的策略标签。

```
bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT
<!--NeedCopy-->
```

8. 创建在 LDAP 身份验证后执行 EPA 扫描的操作，并将其与 EPA 扫描策略相关联。

```
add authentication epaAction post-ldap-epa-action -csecexpr "sys.
    client_expr ("proc_2_chrome")"

add authentication Policy post-ldap-epa-pol -rule true -action
    post-ldap-epa-action

add authentication policylabel post-ldap-epa-label -loginSchema
    LSCHEMA_INT

bind authentication policylabel post-ldap-epa-label -policyName
    post-ldap-epa-pol -priority 100 -gotoPriorityExpression
<!--NeedCopy-->
```

9. 综上所述，将策略 `pre-ldap-epa-pol` 关联到身份验证虚拟服务器，下一步指向策略标签 `ldap-pol-label` 进行 EPA 扫描。

```
bind authentication vserver user.auth.test -policy pre-ldap-epa-
    pol -priority 100 -nextFactor ldap-pol-label -
    gotoPriorityExpression NEXT

bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post
    -ldap-epa-label
<!--NeedCopy-->
```

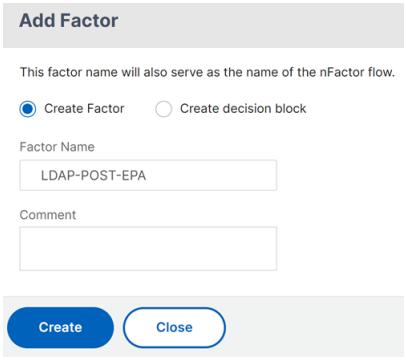
> 注意：
>
> - 在配置为多个银色的定期 EPA 中，考虑了具有定期 EPA 配置的最新银色。
> - 定期扫描只能使用 EPA 插件运行，不能在浏览器上运行。
> - 在第一个示例中，EPA 是扫描寻找进程“Firefox”的第一个因素。
> - 如果 EPA 扫描成功，则会导致 LDAP 身份验证，然后进行下一次 EPA 扫描，该扫描将查找“Chrome”进程。
> - 如果将多个定期扫描配置为不同的因素，则最新扫描优先。在这种情况下，EPA 插件在成功登录后每 2 分钟扫描一次“Chrome”进程。

在 **GUI** 上（使用 **nFactor** 可视化工具）

您可以使用 GUI 上的 nFactor 可视化工具将高级 EPA 扫描配置为一个因素。在以下示例中，我们使用 LDAP 作为第一个因素，将 EPA 用作下一个因素。

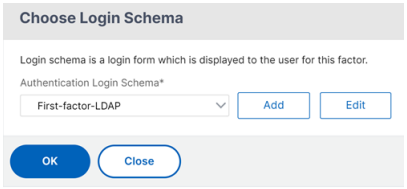
1. 为 nFactor 流创建第一个因素。

   - 导航到 **Security**（安全）**> AAA-Application Traffic**（**AAA -** 应用程序流量）**> nFactor Visualizer**（**nFactor** 可视化工具）**> nFactor Flows**（**nFactor** 流程），然后单击 **Add**（添加）。
   - 单击 **+** 以添加 nFactor 流。
   - 添加因素并单击“创建”。



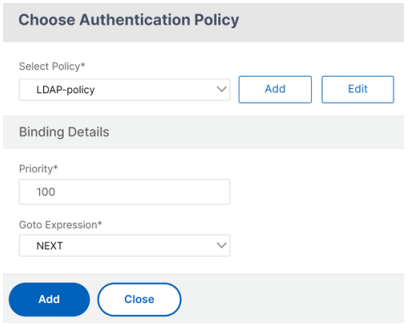
2. 为第一个因素创建登录架构和策略。

   - 在第一个因素图块上，单击“添加架构”以添加登录架构。您可以从下拉列表中选择现有的身份验证登录架构，也可以创建登录架构。
   - 要创建身份验证登录架构，请单击“添加”。有关身份验证登录架构的详细信息，请参阅配置 nFactor 身份验证。

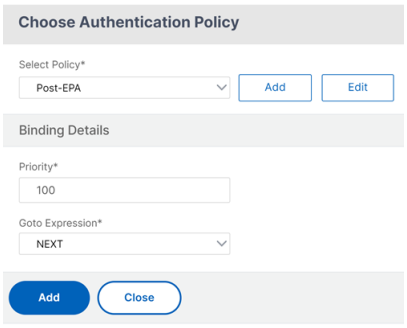


   - 单击 添加策略 以添加 LDAP 策略。如果已经创建 LDAP 策略，则可以选择相同的策略。单击添加。

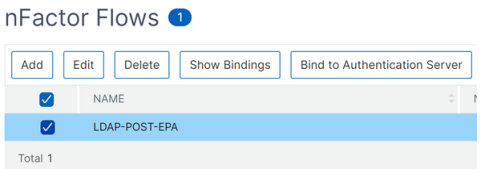
> 注意：
>
> 如果未创建 LDAP 策略，则可以创建一个。单击“选择策略”下拉列表旁边的“添加”按钮。在“操作”字段中，选择 LDAP。有关添加身份验证 LDAP 服务器的详细信息，请参阅 https://support.citrix.com/article/CTX123782。



3. 创建下一个因素并将其连接到第一个因素。
   - 单击绿色或红色的 **+** 图标，将 EPA 添加为下一个因素。
   - 在“下一个要连接的因素”页面上创建下一个因素。
   - 将“添加架构”部分留空，以使默认的架构不应用于此因素。
4. 为下一个因素添加策略。
   - 单击“添加策略”以添加身份验证后 EPA 策略和操作。
   - 您可以从现有策略列表中进行选择，也可以创建策略。要从现有策略中进行选择，请从“选择策略”下拉列表中选择一个策略，提供绑定详细信息，然后单击“添加”。
   - 要创建策略，请单击“选择策略”下拉列表旁边的“添加”按钮。



5. nFactor 流程完成后，单击“完成”。
6. 将 nFactor 流绑定到身份验证服务器。
   - 导航到安全 **AAA -** 应用程序流量 **> nFactor** 可视化工具 **> nFactor** 流。
   - 选择 nFactor，然后单击“绑定到身份验证服务器”。



引用

- nFactor 概念、实体和术语

- 如何在 NetScaler Gateway 上配置 LDAP 身份验证
- LDAP 身份验证
- 高级端点分析扫描

Windows 客户端上的 EPA 扫描分类类型

February 1, 2024

> 重要：
>
> 端点分析旨在根据预先确定的合规性标准分析用户设备，并不强制或验证最终用户设备的安全性。建议使用端点安全系统来保护设备免受本地管理员攻击。

以下新的分类类型将添加到 EPA 扫描中以查找缺失的补丁。如果客户端缺少以下任何修补程序，则 EPA 扫描将失败。

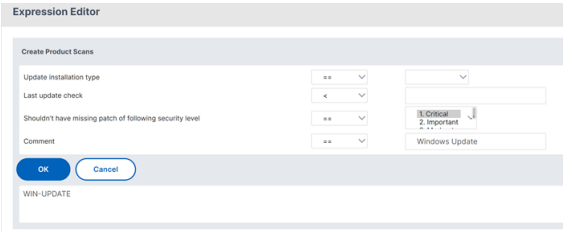
- 应用程序
- 连接器
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- 指导
- SecurityUpdates
- ServicePacks
- 工具
- UpdateRollups
- 更新

> 备注：
>
> - 早些时候，EPA 对缺失修补程序的扫描是在 Windows 客户端上按严重性级别进行的：“严重”、“重要”、“中”和“低”。
> - 如果您使用的是适用于 Windows 的 Citrix Secure Access 23.8.1.1 及更高版本，扫描 `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` 仅限于启用了自动更新的客户端。如果禁用自动更新，则此扫描将返回不同的结果。

使用 GUI 配置 EPA 扫描分类类型

1. 导航到 **NetScaler Gateway >** 策略 **>** 预身份验证。
2. 创建新的预身份验证策略或编辑现有策略。

3. 单击 **OPSWAT EPA** 编辑器 链接。
4. 在表达式编辑器中，选择“窗口”**>** “**Windows** 更新”。
5. 在 不应该缺少以下 **Windows** 更新分类类型的修补程序中，选择缺失补丁的分类类型。
6. 单击确定。



客户可以升级到 OPSWAT 版本 4.3.2744.0s 以使用这些选项。

引用

- 有关 Windows 服务器更新服务分类 GUID 的详细信息，请参阅 https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85)。
- 有关 Microsoft 软件更新术语的说明，请参阅 https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates。

高级端点分析扫描

February 1, 2024

dvanced Endpoint Analysis (EPA) 用于扫描用户设备以满足在 NetScaler Gateway 上配置的端点安全要求。如果用户设备尝试访问 NetScaler Gateway，则在管理员授予对 NetScaler Gateway 的访问权限之前，将对该设备进行扫描以获取安全信息，例如操作系统、防病毒、网络浏览器版本等。有关 Citrix EPA 客户端系统要求的更多信息，请参阅 Endpoint Analysis 要求。

高级 EPA 扫描是一种基于策略的扫描，您可以在 NetScaler Gateway 上对其进行配置以进行身份验证会话。该策略在用户设备上执行注册表检查，根据评估，该策略允许或拒绝访问 NetScaler 网络。

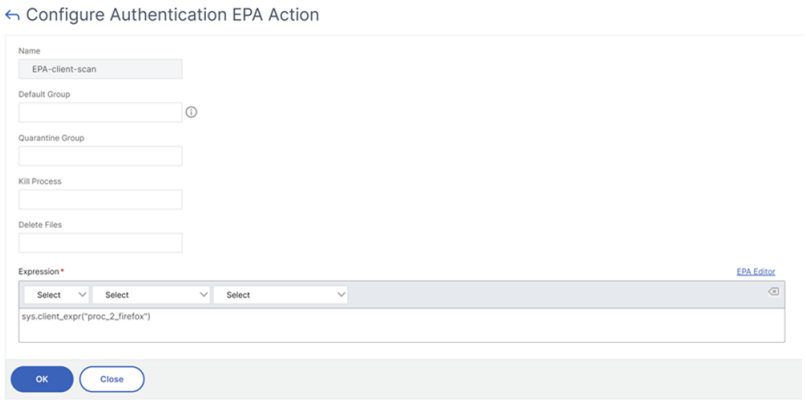
您可以使用 GUI 或 CLI 配置高级 EPA 扫描。

在 **GUI** 上

1. 创建 EPA 操作。

   导航到安全 **> AAA -** 应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 操作 **> EPA**，然后单击添加。在“创建身份验证 **EPA** 操作”页面上，更新以下信息，然后单击“创建”。

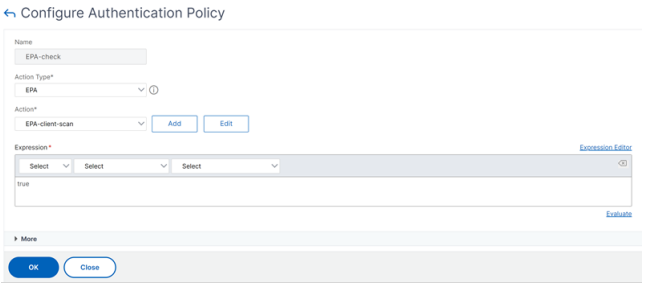
- 名称：EPA 操作的名称。
- 默认组：EPA 检查成功时选择的默认组。
- 隔离组：EPA 检查失败时选择的隔离组。
- 终止进程：指定要由 EPA 插件终止的进程名称的字符串。多个进程必须用逗号分隔。
- 删除文件：指定要由 EPA 插件删除的文件的路径和名称的字符串。多个文件必须用逗号分隔。
- 表达式：有关 EPA 表达式格式，请参阅高级端点分析策略表达式参考。



2. 创建相应的 EPA 政策。

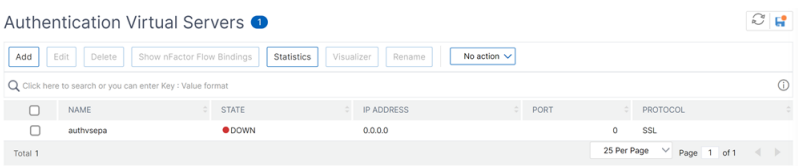
   导航到“安全”**>**“**AAA -** 应用程序流量”**>**“策略”**>**“身份验证”**>**“高级策略”**>**“策略”，然后单击“添加”。在“创建身份验证策略”页面上，更新以下信息，然后单击“创建”。

   - 名称：高级 EPA 策略的名称。
   - 操作类型：身份验证操作的类型。
   - 操作：策略匹配时要执行的身份验证操作的名称。
   - 表达式：有关 EPA 表达式格式，请参阅高级端点分析策略表达式参考。
   - 日志操作：请求与此策略匹配时要使用的消息日志操作的名称。允许的最大长度为 127 个字符。

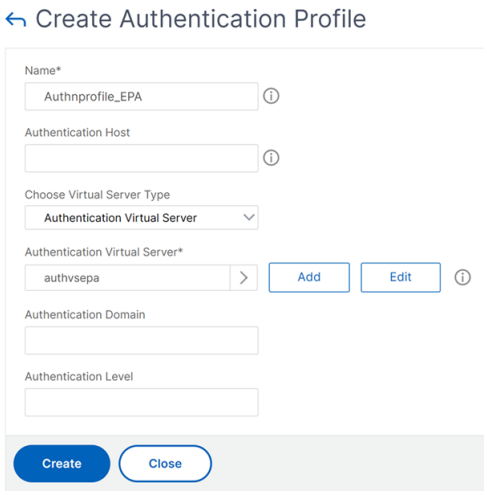


3. 配置身份验证虚拟服务器和身份验证配置文件。

   - 导航到“安全”**>**“**AAA -** 应用程序流量”**>**“身份验证虚拟服务器”，然后单击“添加”。

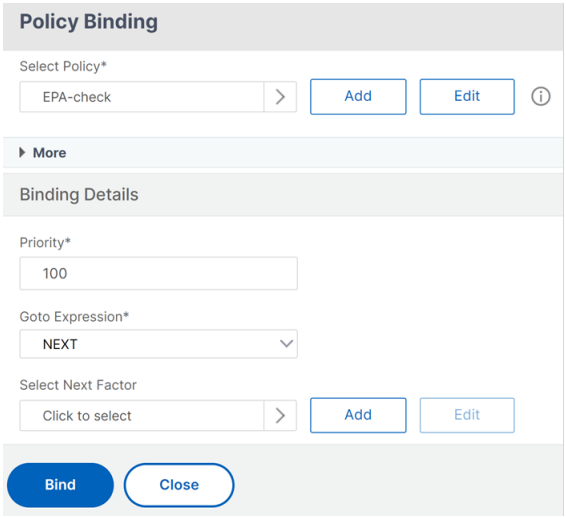


- 导航到“安全”**>**“**AAA -** 应用程序流量”**>**“身份验证配置文件”，然后单击“创建”。



4. 将高级 EPA 策略绑定到身份验证虚拟服务器。

   - 导航到“安全”**>**“**AAA -** 应用程序流量”**>**“身份验证虚拟服务器”，然后选择身份验证虚拟服务器。
   - 在“高级身份验证策略”部分中选择策略。
   - 在“策略绑定”部分中单击“绑定”。



5. 将 EPA 策略绑定到 nFactor 流。

   有关如何将高级 EPA 策略作为一个因素添加到 nFactor 流程的详细信息，请参阅 EPA 扫描作为 nFactor 身份验证中的一个因素。

在 **CLI** 上

1. 创建执行 EPA 扫描的操作。


```
add authentication epaAction EPA-client-scan -csecexpr "sys.
   client_expr ("proc_2_firefox")"
<!--NeedCopy-->
```

上述表达式会扫描进程“Firefox”是否正在运行。EPA 插件每 2 分钟检查一次进程是否存在，由扫描表达式中的数字“2”表示。

2. 将 EPA 操作与高级的 EPA 策略关联起来。

```
add authentication Policy EPA-check -rule true -action EPA-client-
   scan
<!--NeedCopy-->
```

3. 配置身份验证虚拟服务器和身份验证配置文件。

```
add authentication vserver authnvsepa ssl -ip address
   10.104.130.129 -port 443
<!--NeedCopy-->
```

```
add Authnprofile_EPA -authnVsName authnvsepa
<!--NeedCopy-->
```

4. 将高级 EPA 策略绑定到身份验证虚拟服务器。

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
<!--NeedCopy-->
```

升级 **EPA** 库

要使用 NetScaler GUI 升级 EPA 库，请执行以下操作：

1. 导航到配置 **> NetScaler Gateway >** 更新客户端组件。
2. 在 更新客户端组件下，单击升级 **EPA** 库 链接。
3. 选择所需的文件，然后单击 升级。

> 重要提示：
>
> - 在 NetScaler Gateway 高可用性中，必须同时在主节点和辅助节点上升级 EPA 库。
> - 在 NetScaler Gateway 群集设置中，必须在所有群集节点上升级 EPA 库。

有关 OPSWAT 为 NetScaler 扫描提供的 Windows 和 MAC 支持的应用程序的列表，请参阅 https://support.citrix.com/article/CTX234466。

排查高级端点分析扫描的

为了帮助排除高级端点分析扫描的故障，客户端插件会将日志记录信息写入客户端端点系统上的文件中。这些日志文件可以在以下目录中找到，具体取决于用户的操作系统。

Windows Vista、**Windows 7**、**Windows 8**、**Windows 8.1** 和 **Windows 10**：

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP：

C:\Documents 和设置\ 所有用户\ 应用程序数据\ Citrix\ AGEE\ nsepa.txt

Mac OS X 系统：

~/ 库/应用程序 Support/Citrix/EPAPlugin/epaplugin.log

（其中 ~ 符号表示相关 macOS 用户的主目录路径。）
（其中 ~ 符号表示相关 macOS 用户的主目录路径。）

Ubuntu：

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

高级端点分析策略表达式参考

February 1, 2024

本主题介绍高级端点分析表达式的格式和构造。NetScaler Gateway 配置实用程序会自动构建此处包含的表达式元素，不需要手动配置。

表达式格式

高级端点分析表达式具有以下格式：

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _…)
```

其中：

SCAN-type 是正在分析的应用程序的类型。

商品编码是被分析应用程序的产品标识。

方法名称是要分析的产品或系统属性。

方法比较器是为分析选择的比较器。

方法参数是正在分析的一个或多个属性值。

示例：

client.application(ANTIVIR_2600*RTP*==_TRUE)

> 注意：
>
> 对于非应用程序扫描类型，表达式前缀为 CLIENT.SYSTEM 而不是 CLIENT.APPLICATION。

表情字符串

高级端点分析中支持的每种扫描类型在表达式中使用唯一标识符。下表列举了每种扫描类型的字符串。

扫描类型	扫描型表达式字符串
反钓鱼	ANTIPHI
反间谍软件	ANTISPY
防病毒	ANTIVIR
备份客户端	BACKUP
设备访问控制	DEV-CONT
数据丢失防护	DATA-PREV
桌面共享	DESK-SHARE
防火墙	FIREWALL
运行状况代理	HEALTH
硬盘加密	HD-ENC
即时通讯	IM
Web 浏览器	BROWSER
P2P	P2P
补丁管理	PATCH
URL 过滤	URL-FILT
MAC 地址	MAC
域名检查	DOMAIN

扫描类型	扫描型表达式字符串
数字注册表扫描	REG-NUM

> 注意：
>
> 对于 macOS X 特定扫描，表达式在方法类型之前包含前缀 MAC-。因此，对于防病毒和反网络钓鱼扫描，方法分别是 MAC-ANTIVIR 和 MAC-ANTIPHI。
>
> 例如：
>
> 客户端。应用程序（MAC-防病毒 _2600_RTP_==_TRUE）

应用扫描方法

在配置高级端点分析表达式时，方法用于定义端点扫描的参数。这些方法包括方法名称、比较器和值。下表列举了可在表达式中使用的方法。

常见的扫描方法：

以下方法用于多种类型的应用程序扫描。

Method（方法）	说明	比较器	可能的值
版本 *	指定应用程序的版本。	<, <=, >, >=, !=, ==	版本字符串
AUTHENTIC**	检查应用程序是否真实。	==	TRUE
已启用	检查应用程序是否已启用。	==	TRUE
正在运行	检查应用程序是否正在运行。	==	TRUE
评论	注释字段（被扫描忽略）。在表达式中由 [] 描绘。	==	任何文字

* VERSION 字符串可以指定最多四个值的十进制字符串，例如 1.2.3.4。

** 一个真实的检查验证应用程序的二进制文件的真实性。

> 注意：
>
> 您可以为应用程序扫描类型选择通用版本。选择通用扫描时，产品编码为 0。

Gateway 提供了一个选项，用于为每种类型的软件配置通用扫描。使用通用扫描，管理员可以扫描客户端计算机，而无需将扫描检查限制在任何特定产品上。

对于通用扫描，只有在用户系统上安装的产品支持该扫描方法时，扫描方法才有效。要了解哪些产品支持特定的扫描方法，请联系 NetScaler 支持人员。

独特的扫描方法：

以下方法对于指定类型的扫描是唯一的。

Method（方法）	说明	比较器	可能的值
ENABLED-FOR	检查所选应用程序是否启用了反钓鱼软件。	`allof`, `anyof`, `noneof`	对于 **Windows**: Internet Explorer、Mozilla Firefox、Google Chrome、Opera、Safari。对于 **Mac**: Safari、Mozilla Firefox、Google, Chrome、Opera

表 2. 反间谍软件和防病毒

Method（方法）	说明	比较器	可能的值
RTP	检查实时保护是否开启。	==	TRUE
SCAN-TIME	自执行完整系统扫描以来有多少 分钟。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-TIME	病毒特征码文件更新后的分钟 数（即病毒特征码文件标记与当前时间戳之间的分钟数）。	<, <=, >, >=, !=, ==	任何正数
VIRDEF-FILE-VERSION	定义文件的版本。	<, <=, >, >=, !=, ==	版本字符串
ENGINE-VERSION	引擎版本。	<, <=, >, >=, !=, ==	版本字符串

表 3. 备份客户端

Method（方法）	说明	比较器	可能的值
LAST-BK-ACTIVITY	自上次备份活动完成以来已有多少 分钟。	<, <=, >, >=, !=, ==	任何正数

表 4. 数据丢失预防

Method（方法）	说明	比较器	可能的值
已启用	检查应用程序是否已启用以及时间保护是否打开。	==	TRUE

表 5. 运行状况检查代理

Method（方法）	说明	比较器	可能的值
SYSTEM-COMPL	检查系统是否合规。	==	TRUE

表 6. 硬盘加密

Method（方法）	说明	比较器	可能的值
ENC-PATH	用于检查加密状态的 PATH。	没有运算符	任何文字
ENC-TYPE	检查指定路径的加密类型是否。	allof, anyof, noneof	包含以下选项的列表：未加密、部分、加密、虚拟、暂停、等待

表 7. Web 浏览器

Method（方法）	说明	比较器	可能的值
DEFAULT	检查是否设置为默认浏览器。	==	TRUE

表 8. 补丁管理 </caption>

Method（方法）	说明	比较器	可能的值
–	–	–	–
SCAN-TIME	自上次扫描修补程序以来执行了多少分钟。	<, <=, >, >=, !=, ==	任何正数
MISSED-PATCH	客户端系统不会缺少这些类型的修补程序。	anyof, noneof	任何预先选定的（Patch Manager 服务器上预先选择的修补程序
NON|

表 9. MAC 地址

Method（方法）	说明	比较器	可能的值
ADDR	检查客户端计算机的 MAC 地址是否在给定列表中。	anyof, noneof	可编辑列表

表 10. 域成员资格

Method（方法）	说明	比较器	可能的值
SUFFIX	检查给定列表中是否存在客户端计算机。	anyof, noneof	可编辑列表

表 11. 数字注册表项

Method（方法）	说明	比较器	可能的值
PATH	注册表检查的路径。格式为：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate。不需要对特殊字符进行转义。所有注册表根项：HKEY_LOCAL_MACHINE、HKEY_CURRENT_USER、HKEY_USERS、HKEY_CLASSES_ROOT、HKEY_CURRENT_CONFIG	没有运算符	任何文字

Method（方法）	说明	比较器	可能的值
REDIR-64	遵循 64 位重定向。如果设置为 TRUE，则遵循 WOW 重定向（即，在 32 位系统上选中注册表路径，但对于 64 位系统，将检查 WOW 重定向路径。）如果未设置，则不会遵循 WOW 重定向（也就是说，对于 32 位和 64 位系统，将检查相同的注册表路径。）对于未重定向的注册表项，此设置无效。有关在 64 位系统上重定向的注册表项列表，请参阅以下文章：http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE
值	上述路径的预期值。此扫描仅适用于 REG_DWORD 和 REG_QWORD 的注册表类型。	<, <=, >, >=, !=, ==	任何数字

EPA 扫描 MAC 地址

February 1, 2024

从 NetScaler 版本 13.0-88.x 开始，您可以为允许或特定 MAC 地址配置 EPA 扫描配置。NetScaler 使用策略表达式和模式集来指定 MAC 地址列表。

在 NetScaler 版本 13.0-88.x 之前，必须将所有允许的 MAC 地址列表指定为 EPA 表达式的一部分。如果客户有大量允许使用的 MAC 地址，那么在一个表达式中添加所有 MAC 地址就很麻烦了。此外，在单个表达式中添加 MAC 地址的数量也有限制。

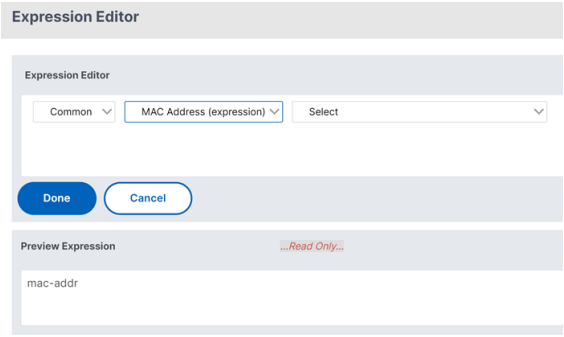
例如，


```
add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
<!--NeedCopy-->
```

使用 **GUI** 配置 **EPA** 扫描 **MAC** 地址

以前在 **Windows** 扫描类别中提供的 **MAC** 地址（表达式）选项现在在 NetScaler GUI 的“常用”扫描类别中可用。此选项允许用户配置 EPA 扫描，以获取允许或特定 MAC 地址的列表。

> 注意：
>
> Citrix Secure Access 客户端 22.10.1 及更高版本支持 NetScaler 在 GUI 上处理 EPA 扫描配置的这种方法。



1. 配置模式集。有关详细信息，请参阅 配置模式集。
2. 为每个模式集创建相应的策略表达式。

   配置表达式时，在表达式编辑器中，选择 **AAA >** 登录 **> CLIENT_MAC_ADDR > EQUAL_ANY(string) >** 模式集。

   有关配置高级表达式的详细信息，请参阅在 策略中配置高级策略表达式。
3. 为前面步骤中配置的表达式创建 EPA 扫描。有关详细信息，请参阅 高级端点分析扫描。

使用 **CLI** 配置 **EPA** 扫描 **MAC** 地址

1. 将 MAC 地址存储在模式集中。

   在命令提示窗口中，键入：

   ```
   add policy patset <name> [-comment <string>]
   <!--NeedCopy-->
   ```


Example:

‘‘‘

add policy patset patset1
bind policy patset patset1 1A-C8-9C-83-BO-F7
bind policy patset patset1 02-50-F2-0A-77-7C …and so on up to 3K entries.vvvvvvvvvvvvvvvvvvvvv
add policy patset patset2
bind policy patset patset2 1A-2B-3C-4D-5E-6A
bind policy patset patset2 1A-2B-3C-4D-5E-6B …and so on up to 3K entries.

‘‘‘

2. 使用 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any() 为每个模式集创建相应的策略表达式

   在命令提示窗口中，键入：

   ```
   Add policy expression <name> <value> [-comment <string>] [-
       clientSecurityMessage <string>]
   ```

   示例：

   ```
   add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset1")
   add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
       patset2")
   ```

3. 使用配置的策略表达式创建 EPA 扫描

   在命令提示窗口中，键入：

   ```
   add authentication epaAction <name>  -csecexpr <expression>
   ```

   示例：

   ```
   add authentication epaAction epa -csecexpr q/sys.client_expr("
       proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  ||
       sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-
       addr_0_exp2") || sys.client_expr("proc_0_firefox")/
   ```

   配置预身份验证策略，

   ```
   add authentication Policy epapol -rule true -action epa
   ```

   绑定预身份验证策略，

   ```
   bind authentication vserver <name> -policy epapol -priority 10 -
       gotoPriorityExpression NEXT
   ```

注意事项

- 为允许的 MAC 地址列表配置 EPA 扫描仅适用于 nFactor 身份验证流程。

- 建议在一个模式集中存储不超过 3000 个条目。
- MAC 地址必须配置为 1A-2B-3C-4D-5E-6F 格式。
- EPA 扫描的格式为 `mac-addr_0_<policy-expression-name>`。在此格式中，`mac-addr_0_` 是静态值，您必须在后面输入策略表达式名称 `mac-addr_0_`。
- 可以使用符号适当分隔 EPA 扫描（ ||， &&）。
- 要向模式集中添加许多 MAC 地址，可以使用基于文件的模式集导入。建议最多存储 3000 个条目/模式集，以获得最佳性能。
- 如果文件中存在 MAC 地址，则可以使用基于文件的模式集导入并在导入过程中指定适当的分隔符来创建模式集。

引用

- 配置模式集。
- 使用基于文件的导入创建模式集。
  “‘

管理用户会话

February 1, 2024

您可以通过活动用户会话对话框在 NetScaler GUI 中管理用户会 话。此对话框显示 NetScaler Gateway 上的活动用户会话列表。您可以使用用户名、组名或 IP 地址查看最终用户或组会话。您还可以在此对话框中查看活动会话。会话信息包括：

- 用户名
- 用户设备的 IP 地址
- 用户设备的端口号
- 虚拟服务器的 IP 地址
- 虚拟服务器的端口号
- 分配给用户的内联网 IP 地址

使用 **GUI** 管理用户会话

查看用户会话

1. 在 NetScaler GUI 导航窗格中，单击 **NetScaler Gateway**。
2. 在详细信息窗格中的监视器连接下，单击 活动用户会话。
3. 在 活动用户会话中，从以下类型中进行选择。

- 活跃用户
- 活跃的组
- **Intranet IP**-选择 Intranet IP 时，必须输入内网 IP 地址和子网掩码。

4. 单击继续。

刷新会话列表

您可以将有关会话的更新信息检索到 NetScaler Gateway。

1. 在 NetScaler GUI 导航窗格中，单击 **NetScaler Gateway**。
2. 在详细信息窗格中的监视器连接下，单击 活动用户会话。
3. 单击 刷新。

最终用户或组会话或具有特定 **Intranet IP** 地址的会话

您可以终止用户和组会话。您还可以结束具有特定 Intranet IP 地址和子网掩码的会话。

1. 在 NetScaler GUI 导航窗格中，单击 **NetScaler Gateway**。
2. 在详细信息窗格中的监视器连接下，单击 活动用户会话。
3. 在“会话”下，选择具有特定 Intranet IP 地址的用户、组或会话，然后单击“结束”。

使用 **CLI** 管理用户会话

您可以使用以下 CLI 命令查看用户会话、最终用户或组会话。

- `show aaa session`-显示绑定到指定用户、组、IP 地址或 IP 范围的所有 NetScaler 身份验证、授权和审核或 VPN 连接。
- `show vpn icaConnection` -显示使用 ICA 代理的所有活动连接。
- `show system session` -显示有关所有当前系统会话或指定会话的信息。

始终启用

February 1, 2024

NetScaler Gateway 的“始终开启”功能可确保用户始终连接到企业网络。这种持久的 VPN 连接是通过自动建立 VPN 通道来实现的。

> 注意
>
> 始终开启功能支持 NetScaler 12.0 Build 51.24 及更高版本的强制门户。

何时使用“始终开启”

当您需要根据用户位置提供无缝 VPN 连接并且必须阻止未连接到 VPN 的用户访问网络时，请使用“始终开启”。

以下场景说明了始终开机的用法。

- 员工在企业网络之外启动笔记本电脑，需要帮助才能建立 VPN 连接。
  解决方案：当笔记本电脑在企业网络外部启动时，Always Oon 无缝建立通道并提供 VPN 连接。
- 使用 VPN 连接的员工进入企业网络。员工已切换到企业网络，但仍保持连接到 VPN 通道，这不是理想的状态。
  解决方案：当员工进入企业网络时，Always Oon 会拆除 VPN 通道并将员工无缝切换到企业网络。
- 员工移出企业网络并关闭笔记本电脑（而不是关闭）。员工在笔记本电脑上恢复工作时需要帮助来建立 VPN 连接。
  解决方案：当员工移出企业网络时，Always On 会无缝建立通道并提供 VPN 连接。
- 企业希望在用户未连接到 VPN 通道时规范向其提供的网络访问权限。
  解决方案：根据配置，始终开启会限制访问，允许用户仅访问网关网络。

了解永远在用的框架

Always Oon 会自动将用户连接到客户端之前建立的 VPN 通道。当用户首次需要 VPN 通道时，用户必须连接到 NetScaler Gateway URL 并建立通道。将 Always Oon 配置下载到客户端后，此配置将推动随后建立通道。

Citrix Secure Access 客户端可执行文件始终在客户端计算机上运行。当用户登录或网络发生变化时，Citrix Secure Access 客户端会确定用户笔记本电脑是否在企业网络上。根据位置和配置，Citrix Secure Access 客户端要么建立通道，要么拆除现有通道。

只有在用户登录到计算机后，才会启动通道建立。Citrix Secure Access 客户端使用客户端计算机的凭据向网关服务器进行身份验证，并尝试建立通道。

自动重建通道

当 NetScaler Gateway 关闭 VPN 通道时，会触发通道的自动重建。

> 注意
>
> 当端点分析失败时，NetScaler Gateway 客户端不会重新尝试建立通道，但会显示错误消息。如果身份验证失败，NetScaler Gateway 客户端会提示用户输入凭据。

支持无缝建立通道的用户验证方法

支持的用户身份验证方法如下：

- 用户名 + AD 密码：如果使用 Windows 用户名和密码进行身份验证，Citrix Secure Access 客户端将使用这些凭据无缝建立通道。
- 用户证书：如果使用用户证书进行身份验证并且客户端上只有一个证书，则 Citrix Secure Access 客户端将使用此证书无缝建立通道。如果安装了多个客户端证书，则在用户选择首选证书后建立通道。Citrix Secure Access 客户端将此首选证书用于以后的通道。

  如果智能卡共享用户证书，则与存储中存在的证书相比，如果证书是动态安装在存储区中的，则无法实现自动登录。
- 用户证书和用户名 + AD 密码：此身份验证方法是前面描述的身份验证方法的组合。

> 注意
>
> 支持所有其他身份验证机制，但通道建立对于任何其他身份验证方法都不是无缝的。

始终开启的配置要求

企业管理员必须对受管设备强制执行以下操作：

- 用户不能结束特定配置的进程/服务
- 用户必须无法卸载软件包以进行特定配置
- 用户必须无法更改特定的注册表项

> 注意
>
> 如果用户具有管理权限，则该功能可能无法按预期运行，例如非托管设备。

启用始终开启功能时的注意事项

在启用始终开启功能之前，请查看以下部分。

主要网络访问：建立通道后，将根据拆分通道配置确定到企业网络的流量。没有提供其他配置来覆盖此行为。

客户端计算机的代理设置：连接到网关服务器时会忽略客户端计算机的代理设置。

> 注意
>
> 不会忽略 NetScaler 设备的代理配置。只有客户端计算机的代理设置会被忽略。系统上配置了代理的用户会收到通知，说明 VPN 插件已忽略其代理设置。

配置始终开启

要配置始终开启，请在 NetScaler Gateway 设备上创建始终在线配置文件并应用该配置文件。

要创建“始终在线”配置文件：

1. 在 NetScaler GUI 中，导航到 配置 **> NetScaler Gateway >** 策略 **> AlwaysOn**。
2. 在 **AlwaysOn** 配置文件 页面上，单击 添加。
3. 在“创建 **AlwaysOn** 配置文件”页上，输入以下详细信息：

    - 名称—配置文件的名称。
    - ** 基于位置的 VPN（客户端注册表名称：LocationDetection）—选择以下设置之一：
        - 远程，使客户端能够检测其是否在企业网络中，如果不在企业网络中，则建立通道。远程是默认设置。
        - 无论客户身在何处，都可以让客户跳过位置检测并建立通道
    - 客户端控制—选择以下设置之一：
        - 拒绝以防止用户注销并连接到另一个网关。“拒绝”是默认设置。
        - 允许允许 用户注销并连接到另一个网关。
    - **VPN** 时的网络访问失败（客户端注册表名称：**AlwaysOn**）—选择以下设置之一：
        - 完全访问权限：在通道未建立时允许网络流量进出客户端。完全访问权限是默认设置。
        - 仅限于 **Tor Gateway** ，用于在通道未建立时防止网络流量流入或流出客户端。但是，允许进出网关 IP 地址的流量。
          注意：在“仅到网关”模式下，只有虚拟服务器、DNS 和 DHCP 流量会被解除阻止。要取消阻止其他网站、IP 地址范围或 IP 地址，必须使用分号分隔的 FQDN、IP 地址范围或 IP 地址列表来设置 **AlwaysOnAllowlist** 注册表。
          例如，mycompany.com,mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. 单击创建完成配置文件的创建。

要应用“始终在线”配置文件：

1. 在 NetScaler 界面中，选择 配置 **> NetScaler Gateway >** 全局设置。
2. 在“全局设置”页面上，单击“更改全局设置”链接，然后选择“客户端体验”选项卡。
3. 从 **AlwaysOn** 配置文件名称 下拉菜单中，选择新创建的配置文件，然后单击 确定。

注意：可以在会话配置文件中进行类似的配置，以便在组级别、服务器杠杆或用户级别应用策略。

关于 **IIP** 的说明

机器级通道使用基于证书的身份验证，创建的会话将证书的公用名作为用户名。因此，如果设备证书具有唯一的公用名，则不同计算机的会话具有不同的用户名，因此具有不同的 IIP。确保生成具有唯一名称的设备证书。理想情况下，必须使用计算机名称作为设备证书的公用名。

管理员用户和非管理员用户不同配置的行为摘要

下表总结了不同配置的行为。它还详细说明了某些用户操作的可能性，这些操作可能会影响 Always ON 功能。

networkAccessONVPNFailure	客户端控制	非管理员用户	管理员用户
fullaccess	允许	通道会自动建立。用户可以注销并远离网络。用户还可以指向另一个 NetScaler Gateway。	通道会自动建立。用户可以注销并远离企业网络。用户还可以指向另一个 NetScaler Gateway。
fullaccess	拒绝	通道会自动建立。用户无法注销或指向另一个 NetScaler Gateway。	通道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移至另一个 NetScaler Gateway。
onlyToGateway	允许	通道会自动建立。用户可以注销（没有网络访问权限）。用户还可以指向另一个 NetScaler Gateway，在这种情况下，该访问权限仅授予新指向的 NetScaler Gateway。	通道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移至另一个 NetScaler Gateway。
onlyToGateway	拒绝	通道会自动建立。用户无法注销或指向另一个 NetScaler Gateway。	通道会自动建立。用户可以卸载 Citrix Secure Access 客户端或移至另一个 NetScaler Gateway。

“始终打开”关闭时允许选定的 **URL**

即使 Always ON 关闭且网络已锁定，用户也可以访问一些网站。管理员可以使用 **AlwaysOnAllowlist** 注册表添加您希望在 AlwaysOnAllowlist 关闭时启用访问权限的网站。

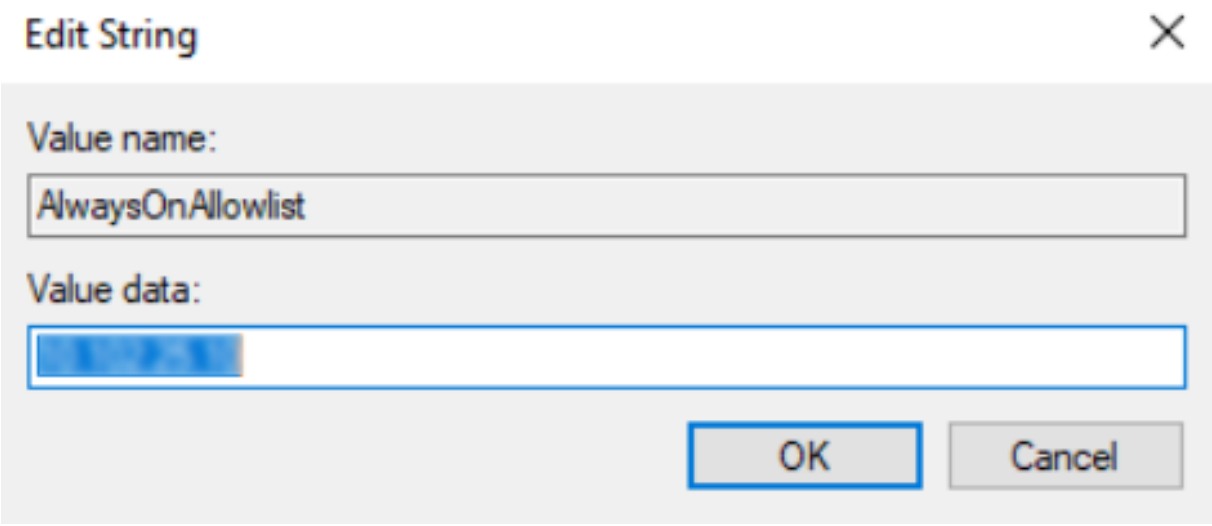
> 注意：
>
> - 13.0 版本 47.x 及更高版本支持 **AlwaysOnAllowlist** 注册表。
> - **AlwaysOnAllowlist** 注册表位置是 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client。
> - **AlwaysOnAllowlist** 注册表中不支持通配符 URL/FQDN。

设置 **AlwaysOnAllowlist** 注册表

使用分号分隔的要允许访问的 FQDN、IP 地址范围或 IP 地址列表设置 **AlwaysOnAllowlist** 注册表。

示例：例如.citrix.com; 10.103.184.156; 10.102.0.0-10.102.255.100

下图显示了一个示例 **AlwaysOnAllowlist** 注册表。



在 **Windows** 登录之前始终可用的 **VPN**（正式的 **Always On** 服务）

February 1, 2024

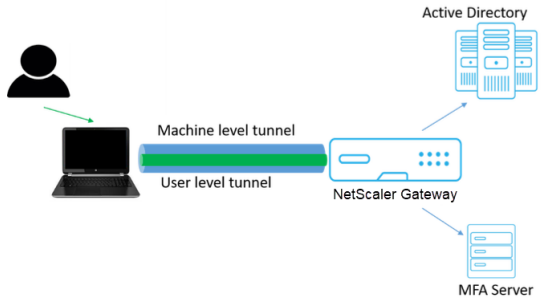
Windows 登录前的 **AlwaysOn VPN** （正式为始终开启服务）功能使用户甚至可以在用户登录 Windows 系统之前就建立计算机级 VPN 通道。在计算机关闭之前，通道将保持活动状态。用户登录后，计算机级 VPN 通道将由用户级 VPN 通道接管。用户注销后，用户级通道将被撕裂并建立计算机级通道。只能使用高级身份验证策略来配置 **Windows** 登录前始终开启 **VPN** 。有关详细信息，请参阅在 Windows 登录之前配置始终可用的 VPN。

Windows 登录前始终开启 **VPN** 功能

- 管理员可以为首次远程工作的用户提供一次性密码，用户可以使用该密码连接到域控制器来更改其密码。
- 管理员甚至可以在用户登录之前远程管理/强制执行设备的 AD 策略。
- 管理员可以在用户登录后根据用户组为用户提供精细级别的控制。例如，使用用户级通道，您可以限制或提供对特定用户组的资源访问权限。
- 可以根据用户要求为 MFA 配置用户通道。
- 多个用户可以使用同一台计算机。根据用户配置文件提供对选择性资源的访问权限。例如，多个用户可以轻松地在自助终端中使用一台计算机。
- 远程工作的用户连接到域控制器以更改密码。
- Windows 计算机可以使用企业活动目录 (AD) 验证用户的登录凭据，并且不会缓存计算机上的 Windows 凭据。此外，新的公司 AD 用户还可以无缝登录计算机。
- 甚至在用户登录之前，Windows 计算机就成为企业内部网的一部分，从而允许 IT 管理员从公司网络访问客户端计算机以进行调试。
- 即使不同的用户登录或注销计算机，Windows 计算机的 VPN 通道仍保持连接状态。

在 **Windows** 登录之前了解始终可用的 **VPN**

以下是“**Windows** 登录前始终开启 **VPN**”功能的事件流。



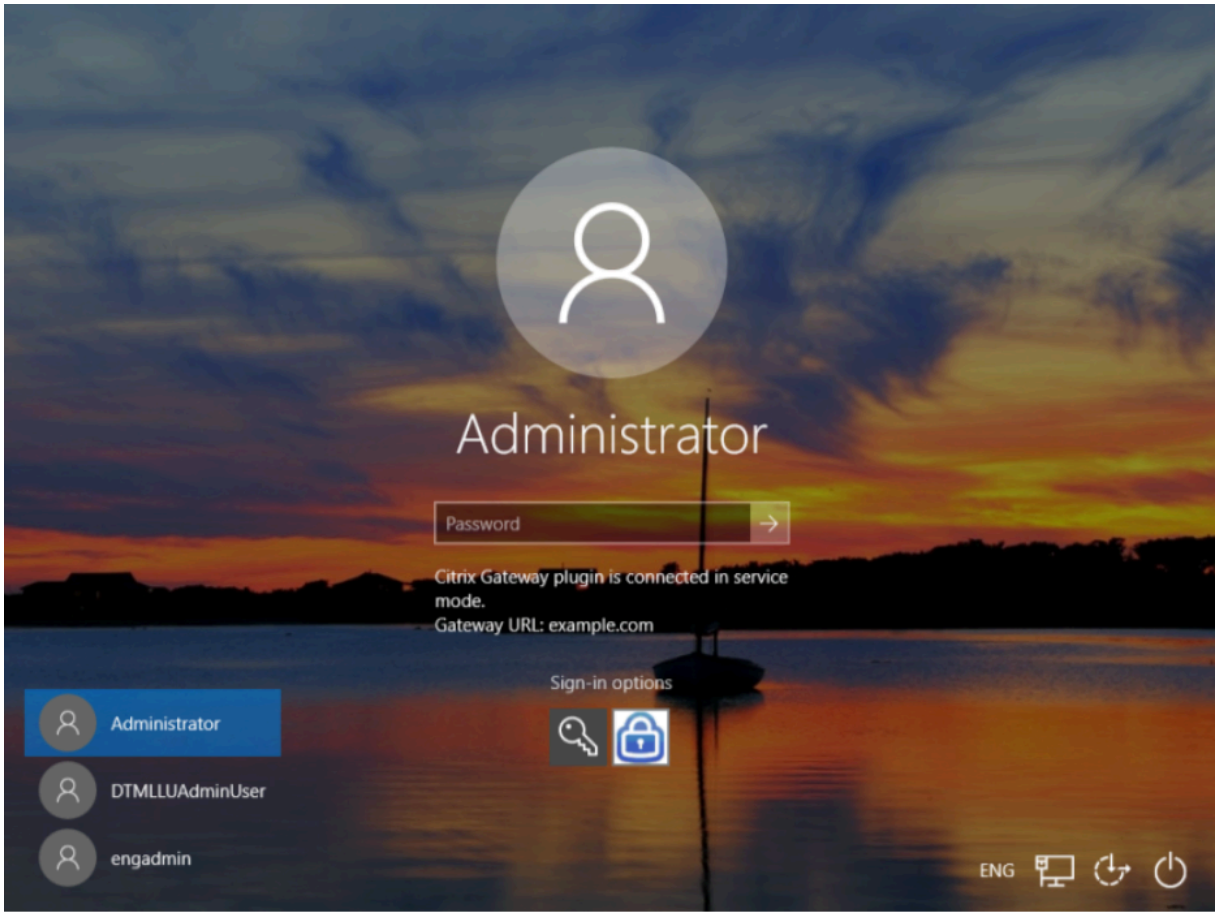
- 用户打开笔记本电脑。使用设备证书作为身份建立通往 NetScaler Gateway 的计算机级通道。
- 用户使用 AD 凭据登录到笔记本电脑。
- 登录后，用户面临 MFA 的挑战。
- 成功进行身份验证后，计算机级通道将替换为用户级通道。
- 用户注销后，用户级通道将替换为计算机级通道。

注意事项：

- NetScaler Gateway 和 VPN 插件的版本必须为 13.0.41.20 及更高版本。
- 如果客户端计算机没有互联网连接，请 在建立 **VPN** 通道之前 **Windows** 登录等待互联网连接可用之前始终 打开 VPN。
- 如果客户端计算机连接到俘虏门户网络，请 在 **Windows** 登录等待用户向俘虏门户进行身份验证之前始终打开 **VPN** 。在用户登录并启用互联网访问后，在 **Windows** 登录之前始终打开 **VPN** 建立了 VPN 通道。
- Windows 登录前始终可用的 VPN 功能支持 NetScaler 的强制门户。
- 如果 Windows 未启用缓存的登录凭据选项，则在以下情况下用户将无法登录：
  - 计算机没有 Internet 连接
  - 计算机已连接到强制门户网络
- 在向最终用户显示登录页面之前，管理员必须检查设备证书吊销状态。

Windows 登录配置之前的始终可用的 **VPN** 之后的 **Windows** 凭据管理器屏幕

配置“**Windows** 登录前始终打开 **VPN**”功能后，**Windows** 凭据管理器 屏幕将按如下所示进行修改。



单击 登录屏幕上的登录选项 时，将显示以下信息：

- NetScaler Gateway 图标表示计算机是否已连接到 NetScaler Gateway。
- 根据用户配置模式，登录屏幕上会显示以下语句之一。
  - NetScaler Gateway 已在服务模式下连接
  - NetScaler Gateway 已在用户模式下连接

在 **Windows** 登录之前配置始终可用的 **VPN**

February 1, 2024

本节介绍了使用高级策略在 **Windows** 登录前配置始终可用的 **VPN** 的详细信息。

必备条件

- NetScaler Gateway 和 VPN 插件的版本必须为 13.0.41.20 及更高版本。

- 要使解决方案正常运行，需要 NetScaler Advanced Edition 及更高版本。
- 您只能使用高级策略来配置功能。
- VPN 虚拟服务器必须已启动并正在运行。

高级配置步骤

在 **Windows** 登录前始终可用的 **VPN** 配置涉及以下高级步骤：

1. 设置计算机级通道
2. 设置用户级通道（可选）
3. 启用用户身份验证

    a) 配置 VPN 虚拟服务器，安装 CA 证书，并将证书密钥绑定到虚拟服务器。
    b) 创建身份验证配置文件
    c) 创建身份验证虚拟服务器
    d) 创建验证策略
    e) 将策略绑定到身份验证配置文件

计算机级通道

使用设备证书作为身份建立通往 NetScaler Gateway 的计算机级通道。设备证书必须安装在计算机存储下的客户端计算机中。这仅适用于 Windows 登录前始终开启服务。

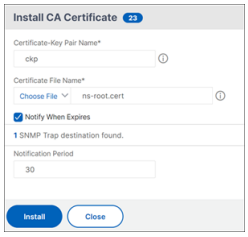
有关设备证书的更多详细信息，请参阅 使用设备证书进行身份验证。

> 重要：
>
> 如果 NetScaler Gateway 设备上的 VPN 虚拟服务器配置在非标准端口（443 以外）上，则计算机级通道将无法按预期工作。

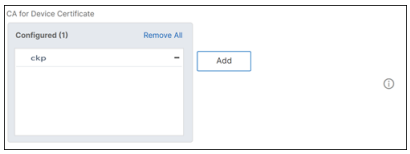
使用设备证书设置计算机级通道

使用 **GUI** 进行基于设备证书的身份验证配置

1. 在配置选项卡上，导航到 **NetScaler Gateway>** 虚拟服务器。
2. 在“NetScaler Gateway 虚拟服务器”页面上，选择现有虚拟服务器，然后单击“编辑”。
3. 在“证书”下，单击 **CA** 证书。
4. 在 **CA** 证书绑定页面上，单击“选择 **CA** 证书”字段旁边的“添加”，更新所需信息，然后单击“安装”。



5. 在 **VPN** 虚拟服务器页面上，单击编辑图标。
6. 在“基本设置”部分中，单击“更多”。
7. 单击“设备证书 **CA**”部分旁边的“添加”，然后单击“确定”。



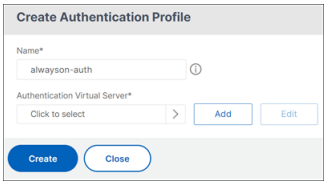
注意：请勿选中“启用设备证书”复选框。

8. 要将 CA 证书绑定到虚拟服务器，请单击 证书部分下的 **CA** 证书。单击 **SSL** 虚拟服务器 **CA** 证书绑定页面下的 ** 添加 绑定 ** 。

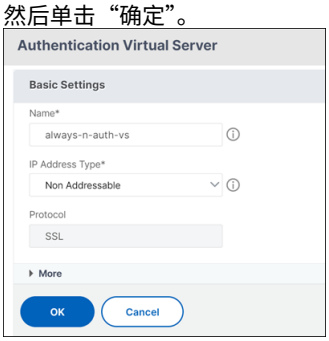
> 注意：
>
> - 设备证书的使用者公用名 (CN) 字段不能为空。如果设备尝试使用空的 CN 设备证书登录，则会使用用户名为“匿名”创建其 VPN 会话。在 IIP 中，如果多个会话具有相同的用户名，则以前的会话将断开连接。因此，启用 IIP 后，您会注意到由于公用名为空而对功能造成的影响。
> - 所有可能 对颁发给客户端的设备证书进行签名的 **CA** 证书（根证书和中间证书）都必须绑定在步骤 **4** 和 **5** 中的虚拟服务器 的 **CA** 证书绑 定部分以及虚拟服务器的 CA 证书绑定部分下。有关将 CA 证书与中级/从属证书关联的详细信息，请参阅 安装、链接和更新证书。
> - 如果配置了多个设备证书，将为 VPN 连接尝试使用有效期最长的证书。如果此证书允许 EPA 成功扫描，则会建立 VPN 连接。如果此证书在扫描过程中失败，则使用下一个证书。此过程将一直持续到尝试所有证书为止。

9. 在 **CA** 证书绑定页面上，选择证书。
10. 单击绑定。
11. 创建身份验证虚拟服务器。

    a) 在 **VPN** 虚拟服务器页面上，导航到高级设置 **>** 身份验证配置文件，然后单击添加。
    b) 在“创建身份验证配置文件”页面上，为身份验证配置文件指定名称，然后单击“创建”。



c) 在“身份验证虚拟服务器”页面上，为身份验证虚拟服务器分配一个名称。将 IP 地址类型选择为不可寻址，然后单击“确定”。



> 注意：
>
> 身份验证虚拟服务器始终保持关闭状态。

12. 创建身份验证策略。

a) 在“安全”**>**“**AAA** 应用程序流量”**>**“身份验证虚拟服务器”页面的“高级身份验证策略”部分，选择身份验证策略并单击“添加绑定”。

b) 在“策略绑定”页面上，单击“选择策略”字段旁边的“添加”。

c) 在“创建身份验证策略”页面上；

i. 为高级身份验证策略分配一个名称。

ii. 从“操作类型”列表中选择 **EPA** 。

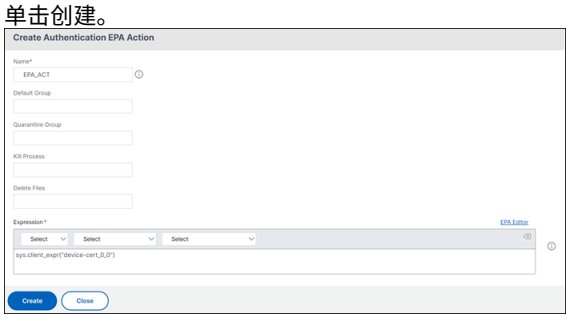
iii. 单击 操作 旁边的 添加。

d) 在创建身份验证 EPA 操作页面上；

i. 为 EPA 操作指定名称。

ii. 在“表达式”字段 `sys.client_expr("device-cert_0_0")` 中输入。

iii. 单击创建。



13. 在“创建身份验证策略”页面上；

a) 为身份验证策略指定名称。

b) 在 表达式 字段中输入 **is_aosservice** 。

c) 单击创建。

14. 在策略绑定页面上，在 优先级 中输入 **100** ，然后单击 绑定。

使用 **CLI** 配置基于设备证书的身份验证

1. 在 VPN 虚拟服务器上安装 CA 证书。

```
add ssl certkey ckp -cert t_CA.cer
<!--NeedCopy-->
```

2. 将 CA 证书绑定到 VPN 虚拟服务器。

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

示例

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
<!--NeedCopy-->
```

3. 添加身份验证虚拟服务器。

```
add authentication authnProfile <name>  {
 -authnVsName <string> }

<!--NeedCopy-->
```

示例

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
<!--NeedCopy-->
```

4. 创建身份验证 EPA 操作。

```
add authentication epaAction <name> -csecexpr <expression>
<!--NeedCopy-->
```


Example

‘‘‘

add authentication epaAction epa-act -csecexpr sys.client_expr("device-cert_0_0") -defaultgroup epa_pass

‘‘‘

5. 创建身份验证策略

```
add authentication Policy <name> -rule <expression> -action <string>
```

示例：

```
add authentication Policy always_on_epa_auth -rule is_aoservice -action epa_auth
```

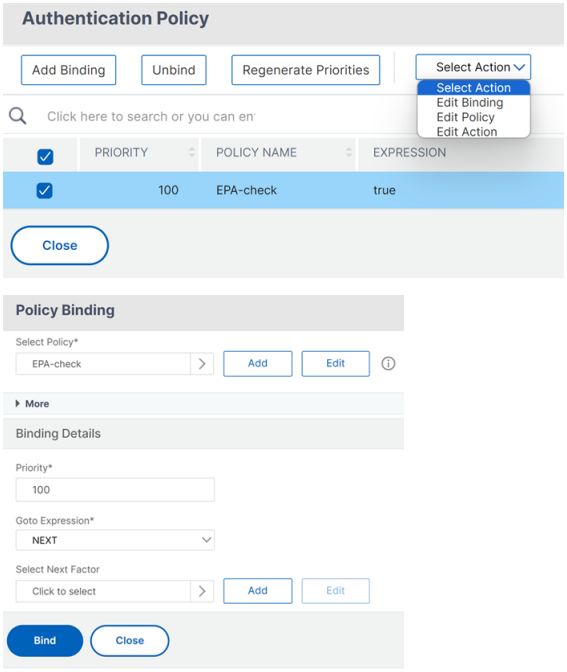
> 重要提示：
>
> - 计算机级通道配置现已完成。要在 Windows 登录后设置用户级通道，请参阅 用户级通道部分。
> - 在客户端计算机上，设备证书采用.pfx 格式。.pfx 证书安装在 Windows 计算机上，因为 Windows 可以理解.pfx 格式。此文件包含证书和密钥文件。此证书必须与绑定到虚拟服务器的域相同。可以使用客户端证书向导生成.pfx 和服务器证书和密钥。这些证书可与证书颁发机构一起使用以生成带有服务器证书和域的相应.pfx。证书.pfx 安装在个人文件夹的计算机帐户中。该 `show aaa session` 命令显示 NetScaler 设备上的设备通道。

用户级通道

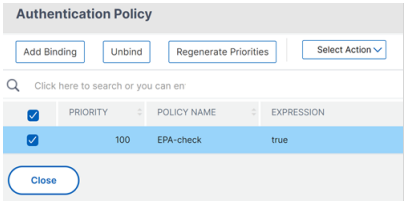
使用 **GUI** 将计算机级通道替换为用户级通道

注意：该表达式适用 `is_aoservice.not` 于 NetScaler Gateway 版本 13.0.41.20 及更高版本。

1. 为用户身份验证配置策略。
   a) 导航到 **NetScaler Gateway >** 虚拟服务器，然后选择虚拟服务器。
   b) 在 **Advanced Settings**（高级设置）中，单击 **Authentication Profile**（身份验证配置文件）。
   c) 配置身份验证配置文件。
   d) 在配置 **>** 安全 **> AAA** 应用程序流量 **>** 身份验证虚拟服务器页面上，选择身份验证策略。
   e) 在选择操作中，单击编辑绑定，然后将策略绑定的 **GoTo** 表达式更改为 **NEXT** 而非 **END**。



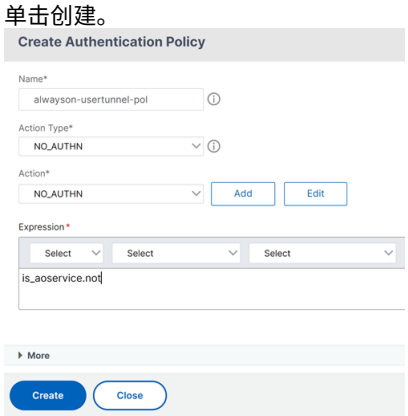
f) 单击“绑定”，然后在“身份验证策略”页面中，单击“添加绑定”。



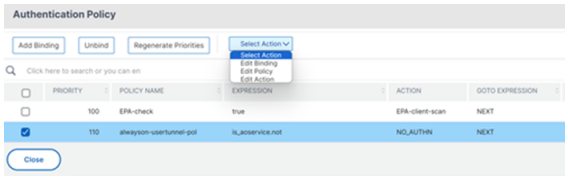
g) 在策略绑定页面上，单击 选择策略 旁边的 添加。

在“创建身份验证策略”页面上；

i. 输入要创建的“无身份验证”策略的名称。
ii. 选择操作类型作为 **No_AUTHN**。
iii. 在“表达式”字段中输入 **is_aoservice.not** 。
iv. 单击创建。



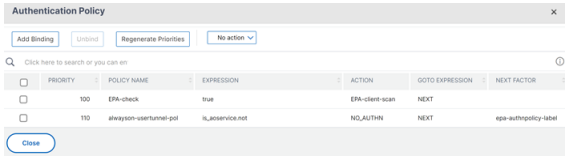
2. 在 **Select Action**（选择操作）中，单击 **Edit Binding**（编辑绑定）。



3. 在策略绑定页面上，在 优先级 中输入 **110**。单击 选择下一个因素旁边 的 添加。

   a) 在“身份验证策略标签”页上，输入策略标签的描述性名称，选择登录架构，然后单击 继续。
   b) 在 选择策略中，单击 添加 并创建 LDAP 身份验证策略。
   c) 单击“创建”，然后单击“绑定”。
   d) 单击“完成”，然后单击“绑定”。

   在“身份验证策略”页面中，下一个因素 列显示已配置的下一个因素策略。



4. 您可以将 LDAP 策略配置为身份验证策略的下一个因素。

   a) 在“创建身份验证策略”页面上，输入 LDAP 策略的名称。
   b) 选择“操作类型”作为 **LDAP**。
   c) 输入 操作 作为配置的 LDAP 操作。

> 注意：
>
> - 有关创建登录架构 XML 文件的信息，请参阅 登录架构 XML 文件。
> - 有关创建策略标签的信息，请参阅 对策略标签进行身份验证。
> - 有关创建 LDAP 身份验证策略的信息，请参阅 使用配置实用程序配置 LDAP 身份验证。

使用 **CLI** 将计算机级通道替换为用户级通道

1. 将策略绑定到身份验证虚拟服务器

```
bind authentication vserver <name> -policy <name> -priority  <
    positive_integer> -gotoPriorityExpression <expression>
```

   示例

```
bind authentication vserver alwayson-auth-vserver -policy alwayson
    -auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. 添加带有操作 `NO_AUTH` 和表达式 `is_aoservice.not`，的身份验证策略，并将其绑定到策略。


```
add authentication Policy <name> -rule <expression> -action <
    string>

bind authentication vserver <name> -policy <name> -priority <
    positive_integer> -gotoPriorityExpression <expression>
```

示例

```
add authentication Policy alwayson-usertunnel-pol -rule
    is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson
    -usertunnel-pol -priority 110
```

3. 添加下一个因素并将策略标签绑定到下一个因素。

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -
    priority <positive_integer> -gotoPriorityExpression <expression
    > -nextFactor <string>
```

示例

```
add authentication policylabel user-tunnel-auth-label -loginSchema
     singleauth_alwayson

bind authentication policylabel user -policyName alwayson-
    usertunnel-pol -priority 100
```

4. 配置 LDAP 策略并将其绑定到用户通道策略标签。

```
add authentication policy <name>  -rule <expression>  -action <
    string>

bind authentication vserver <vserver_name> -policy <string>  -
    priorit < positive integer>  gotoPriorityExpression <string>
```

示例

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName
     LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

客户端配置

`AlwaysOn`, `locationDetection`, and `suffixList registries` 是可选的，只有在需要位置检测功能时才需要。

要访问注册表项项，请导航到以下路径：计算机 **>HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client**

注册表项	注册表类型	值和描述
AlwaysOnService	REG_DWORD	1 => 建立计算机级通道但不建立用户级通道；2 => 建立计算机级通道和用户级通道
AlwaysOnURL	REG SZ	用户要连接到的 NetScaler Gateway 虚拟服务器的 URL。示例：`https://xyz.companyDomain.com` 重要：只有一个 URL 负责计算机级通道和用户级通道。AlwaysOnURL 注册表可帮助服务和用户级组件工作，并根据设计连接单独的通道，即计算机级通道和用户级通道
AlwaysOn	REG_DWORD	1 => 在 VPN 失败时允许网络访问；2=> VPN 失败时阻止网络访问
AlwaysOnAllowlist	REG_SZ	计算机在严格模式下运行时必须列入白名单的 IP 地址或 FQDN 的分号分隔列表。示例：`8.8.8.8;linkedin.com`
UserCertCAList	REG_SZ	以逗号或分号分隔的根 CA 名称列表，即证书的颁发者名称。在 AlwaysOn 服务的上下文中使用，客户可以在此服务中指定要从中选择客户证书的 CA 列表。示例：`cgwsanity.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => 启用位置检测；0 => 禁用位置检测
suffixList	REG SZ	分号分隔的域列表，负责在启用位置检测时检查计算机是否在内联网中。示例：`citrite.net`, `cgwsanity.net`

有关这些注册表项的详细信息，请参阅 始终开启。

> 注意：
>
> 配置“始终可用”服务时，客户端会忽略在 NetScaler Gateway 虚拟服务器或 NetScaler 上配置的“始终开启”配置文件。因此，在配置始终可用的服务时，请确保还启用了 `locationDetection` 和 `AlwaysOn` VPN 注册表。
> “‘

使用高级策略创建 **VPN** 策略

February 1, 2024

经典策略引擎 (PE) 和高级策略基础架构 (PI) 是 NetScaler 当前支持的两种不同的策略配置和评估框架。

高级策略基础架构包含强大的表达式语言表达式语言可用于定义策略中的规则、定义操作的各个部分以及支持的其他实体。表达式语言可以解析请求或响应的任何部分，还可以让您深入浏览标头和有效负载。相同的表达式语言可在 NetScaler 支持的每个逻辑模块中进行扩展和工作。

> 注意：
> 建议您使用高级策略来创建策略。

为什么要从经典策略迁移到高级策略

高级策略具有丰富的表达式集，比传统策略提供更大的灵活性。随着 NetScaler 扩展并满足各种客户端的需求，必须支持远远超出高级策略的表达式。有关详细信息，请参阅 策略和表达式。

以下是高级策略的新增功能。

- 能够访问邮件正文。
- 支持许多其他协议。
- 访问系统的许多其他功能。
- 具有更多的基本函数、运算符和数据类型。
- 满足 HTML、JSON 和 XML 文件的解析需求。
- 有助于快速并行多字符串匹配（`patsets`等等）。

现在可以使用高级策略配置以下 VPN 策略。

- 会话策略
- 授权策略
- 流量策略
- 通道策略
- 审核策略

此外，端点分析（EPA）可以配置为用于身份验证功能的 nFactor。EPA 用作尝试连接到 Gateway 设备的端点设备的网守。在终端设备上显示网关登录页面之前，根据网关管理员配置的资格标准，检查设备的最低硬件和软件要求。根据执行的检查结果授予对网关的访问权限。以前，EPA 被配置为会话策略的一部分。现在，它可以链接到 nFactor，从而在何时可以执行方面提供更大的灵活性。有关 EPA 的更多信息，请参阅 端点策略如何运作 主题。有关 nFactor 的更多信息，请参阅 nFactor 身份验证 主题。

使用案例：

使用高级 **EPA** 预身份验证 **EPA**

身份验证前 EPA 扫描在用户提供登录凭据之前进行。有关将 NetScaler Gateway 配置为 nFactor 身份验证并将预身份验证 EPA 扫描作为身份验证因素之一的信息，请参阅 CTX224268 主题。

使用高级 **EPA** 进行身份验证后 **EPA**

验证后 EPA 扫描会在验证用户凭据之后进行。在传统的策略基础架构下，身份验证后 EPA 被配置为会话策略或会话操作的一部分。在高级策略基础架构下，EPA 扫描将配置为 nFactor 身份验证中的 EPA 因素。有关将 NetScaler Gateway 配置为 nFactor 身份验证并将身份验证后 EPA 扫描作为身份验证因素之一的信息，请参阅 CTX224303 主题。

使用高级策略的身份验证前和身份验证后

EPA 可以在身份验证之前和身份验证后执行。有关使用预身份验证和身份验证后 EPA 扫描配置 NetScaler Gateway 进行 nFactor 身份验证的信息，请参阅 CTX231362 主题。

定期 **EPA** 扫描是 **nFactor** 身份验证的一个因素

在传统的策略基础架构下，定期 EPA 扫描被配置为会话策略操作的一部分。在高级策略基础架构下，可以将其配置为 nFactor 身份验证中的 EPA 因素的一部分。

有关将定期 EPA 扫描配置为 nFactor 身份验证中的一个因素的更多信息，请单击CTX231361 主题。

故障排除：

故障排除时应牢记以下几点。

- 同一类型的经典和高级策略（例如，会话策略）不能绑定到同一实体/绑定点。
- 所有 PI 策略都必须具有优先级。
- VPN 的高级策略可以绑定到所有绑定点。
- 具有相同优先级的高级策略可以绑定到单个绑定点。
- 如果未选择任何已配置的授权策略，则会应用在 VPN 参数中配置的全局授权操作。

- 在授权策略中，如果授权规则失败，则不会撤消授权操作。

经典策略常用的高级策略等效表达式：

经典策略表达式	高级策略表达式
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS(“bar”) [注意使用“…”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

使用 **SSL VPN** 虚拟服务器配置 **DTLS VPN** 虚拟服务器

February 1, 2024

您可以使用与已配置的 SSL VPN 虚拟服务器相同的 IP 地址和端口号为 NetScaler Gateway 配置 DTLS VPN 虚拟服务器。配置 DTLS VPN 虚拟服务器使您能够将高级 DTLS 密码和证书绑定到 DTLS 流量以增强安全性。

> 重要提示：
>
> - 默认情况下，对于现有 SSL VPN 虚拟服务器，DTLS 功能设置为“ON”（开）。在创建 DTLS VPN 虚拟服务器之前，请禁用服务器的功能。

> - NetScaler Gateway 版本 13.0 版本 64.x 及更高版本支持适用于 DTLS 网关虚拟服务器的 SNI。
> - 从 NetScaler 版本 13.0 版本 79.x 开始，默认情况下启用 `helloverifyrequest` 参数。在 DTLS 配置文件上启用 `helloverifyrequest` 参数有助于降低攻击者或机器人压倒网络吞吐量的风险，从而可能导致出站带宽耗尽的风险。也就是说，它有助于缓解 DTLS DDoS 扩增攻击。有关 `helloverifyrequest` 参数的详细信息，请参阅 DTLS 配置文件。
> - 处理 UDP 流量时，如果后端服务器推送大量流量，NetScaler 设备的内存消耗会增加。因此，由于客户端上有 TCP MUX 连接，NetScaler 设备无法将此流量推送到客户端。在这种情况下，Citrix 建议您使用 DTLS 协议。

注意事项

- 可以从 13.0 Build 58.x 开始配置 NetScaler Gateway 设备上的 DTLS VPN 虚拟服务器。
- 在 NetScaler Gateway 设备上配置 DTLS VPN 虚拟服务器之前，必须已在设备上配置 SSL VPN 虚拟服务器。
- DTLS VPN 虚拟服务器使用配置的 SSL VPN 虚拟服务器的 IP 地址和端口号。
- 如果 DTLS 握手失败，则连接将回退到 TLS。
- 要仅使用 DTLS，您可以通过仅将 DTLS 密码绑定到 DTLS 流量来禁用 TLS。
- 当 TCP 流量通过 VPN 进行通道传输时，不支持 DTLS 多路复用。

使用 **GUI** 配置 **DTLS VPN** 虚拟服务器

1. 在“配置”选项卡上，导航到 **NetScaler Gateway >** 虚拟服务器。
2. 在 **NetScaler Gateway Virtual Servers**（NetScaler Gateway 虚拟服务器）页面上，选择现有的 SSL VPN 虚拟服务器，然后单击 **Edit**（编辑）。
3. 在 **VPN** 虚拟服务器页面上，单击编辑图标并清除 **DTLS** 复选框，然后单击确定。
4. 导航回 **NetScaler Gateway >** 虚拟服务器，然后单击添加。
5. 在“基本设置”下，输入以下字段的值，然后单击“确定”。
   - 名称 - DTLS VPN 虚拟服务器的名称
   - 协议- 选择“DTLS”
   - IP 地址 - 输入 SSL VPN 虚拟服务器 IP 地址
   - 端口 - 输入 SSL VPN 虚拟服务器端口号
6. 在 **NetScaler Gateway** 虚拟服务器页面上，选择您之前添加的虚拟服务器，然后单击编辑。
7. 在证书下，单击箭头图标以选择所需的证书密钥。
8. 在服务器证书绑定 **>** 选择服务器证书中，选择现有的 SSL 证书密钥或创建一个证书。
9. 单击 **Server Certificate Binding**（服务器证书绑定）页面上的 **Bind**（绑定）。

> 注意：
>
> - 要使用 DTLS 1.2，请单击 SSL 参数下的编辑图标，然后选中 **DTLS 1.2** 复选框。
> - DTLS 类型的 VPN 虚拟服务器支持服务器名称指示 (SNI)。

使用 **CLI** 配置 **DTLS VPN** 虚拟服务器

在命令提示符下，键入下面的一组命令：

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
<!--NeedCopy-->
```

DTLS 1.0 照常运行，要使用 DTLS 1.2，请键入以下命令：

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
<!--NeedCopy-->
```

示例

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
<!--NeedCopy-->
```

要为 **DTLS** 类型 **VPN** 虚拟服务器启用 **SNI**，请键入以下命令：

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key> <-SNICert>
<!--NeedCopy-->
```

示例

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver \_XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.insight.net.cer_CERT\_" -snICert

<!--NeedCopy-->
```

支持的 **DTLS VPN** 虚拟服务器参数

DTLS 类型的 VPN 虚拟服务器仅支持以下参数。

- Ipaddress

- 端口
- 状态
- 双跃点
- downstateflush
- 备注
- Appflowlog
- Icmpvsrresponse

不支持的 **DTLS VPN** 虚拟服务器参数

DTLS 类型的 VPN 虚拟服务器不支持以下参数。

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

使用 **XenApp** 和 **XenDesktop** 向导配置 **DTLS** 虚拟服务器

1. 单击与 **Citrix** 产品集成下的 **XenApp** 和 **XenDesktop**。

2. 在 XenApp 和 XenDesktop 安装向导中，选择 **StoreFront** 并单击继续。
3. 在 **NetScaler Gateway** 设置页面上，启用为此 **VPN** 虚拟服务器配置 **DTLS** 侦听器复选框，然后单击继续。

   现已配置 DTLS 侦听器。
4. 在“服务器证书”中，单击选择文件以选择服务器证书，然后单击继续。
5. 指定证书文件和密钥文件名，然后单击继续。
6. 在 **StoreFront** 部分下，按如下所示提供所需参数的值，然后单击继续。
7. 在身份验证部分下，按如下所示提供所需参数的值，然后单击测试连接。

   确保服务器可访问，提供超时值和服务器登录名称属性，然后单击 **Continue**（继续）。
8. 单击 **Done**（完成）完成配置。

限制

- DTLS 1.2 仅在 Windows 客户端上受支持。
- 带有 DTLS 的 VPN 虚拟服务器不支持 IPv6 地址。
- DTLS VPN 虚拟服务器不支持 SSL 策略和 SSL 配置文件。此外，不支持绑定 VPN 虚拟服务器策略。
- NetScaler Gateway DTLS VPN 虚拟服务器不支持以下功能。但是，NetScaler Gateway SSL VPN 虚拟服务器支持以下功能：
  - 带内容交换虚拟服务器的 Unified Gateway
  - UDP MUX
  - UDP 视频
  - UDP 音频
  - PCOIP
- 不支持与 DTLS VPN 虚拟服务器统计数据相关的 `stat vpn vserver` 命令。
- DTLS 虚拟服务器不支持 HSM 密钥。
- 不支持群集配置。

与 **NetScaler** 产品集成

February 1, 2024

如果您是负责安装和配置 NetScaler Gateway 的系统管理员，则可以将设备配置为支持 Citrix Endpoint Management、StoreFront 和 Web Interface 。

用户可以从内部网络或远程位置直接连接到 Endpoint Management。当用户连接时，他们可以访问他们的 Web、SaaS 和移动应用程序。它们还可以从任何设备支持位于 ShareFile 中的文档。

要允许用户通过 NetScaler Gateway 连接到服务器场，请在 StoreFront 或 Web Interface 以及 NetScaler Gateway 上配置设置。当用户连接时，他们可以访问已发布的应用程序和虚拟桌面。

将 NetScaler Gateway 与 Endpoint Management、StoreFront 和 Web Interface 集成的配置步骤假定如下：

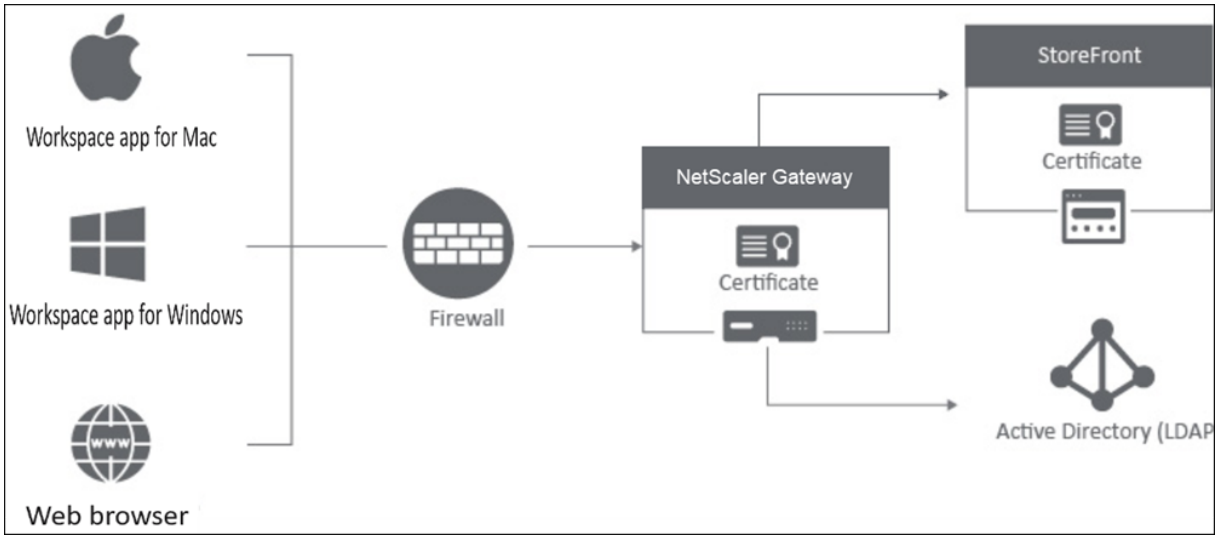
- NetScaler Gateway 位于 DMZ 中，并连接到现有网络。
- NetScaler Gateway 作为独立设备部署，远程用户可以直接连接到 NetScaler Gateway。
- StoreFront、Endpoint Management、Citrix Virtual Apps、Citrix Virtual Desktops 和 Web Interface 驻留在安全网络中。
- ShareFile 是在 Endpoint Management 中配置的。有关 ShareFile 的详细信息，请参阅 ShareFile 主题和为用户访问配置 ShareFile 主题。

部署 StoreFront 和 Endpoint Management 的方式取决于您向移动设备提供的应用程序。如果用户有权访问使用 MDX Toolkit 打包的 MDX 应用程序，则 Endpoint Management 将驻留在安全网络中的 StoreFront 前面。如果您不提供对 MDX 应用程序的访问权限，则 StoreFront 将驻留在安全网络中的 Endpoint Management 之前。

将 **NetScaler Gateway** 与 **StoreFront** 集成

February 1, 2024

本文介绍如何为使用 Citrix Workspace 应用程序或 Web 浏览器的用户创建用于远程访问 StoreFront 的 NetScaler Gateway 虚拟服务器。



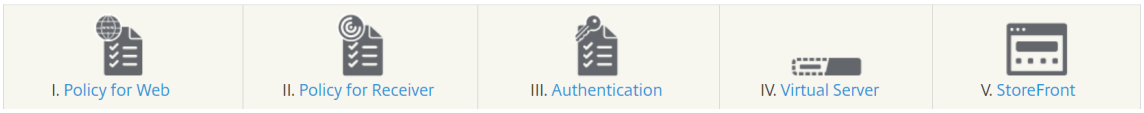
用户通过 Web 浏览器或 Citrix Workspace 应用程序连接到 NetScaler Gateway。NetScaler Gateway 根据配置的策略对用户进行身份验证。如果身份验证成功，则 NetScaler Gateway 允许用户单点登录应用商店并将 StoreFront 应用商店代理给用户。

> 重要提示：
>
> 我们建议您不要使用 Citrix Virtual Apps and Desktops 向导将 NetScaler Gateway 与 StoreFront 集成，因为它使用经典身份验证策略（已过时）创建无效配置。

配置 **NetScaler Gateway** 以与 **StoreFront** 配合使用

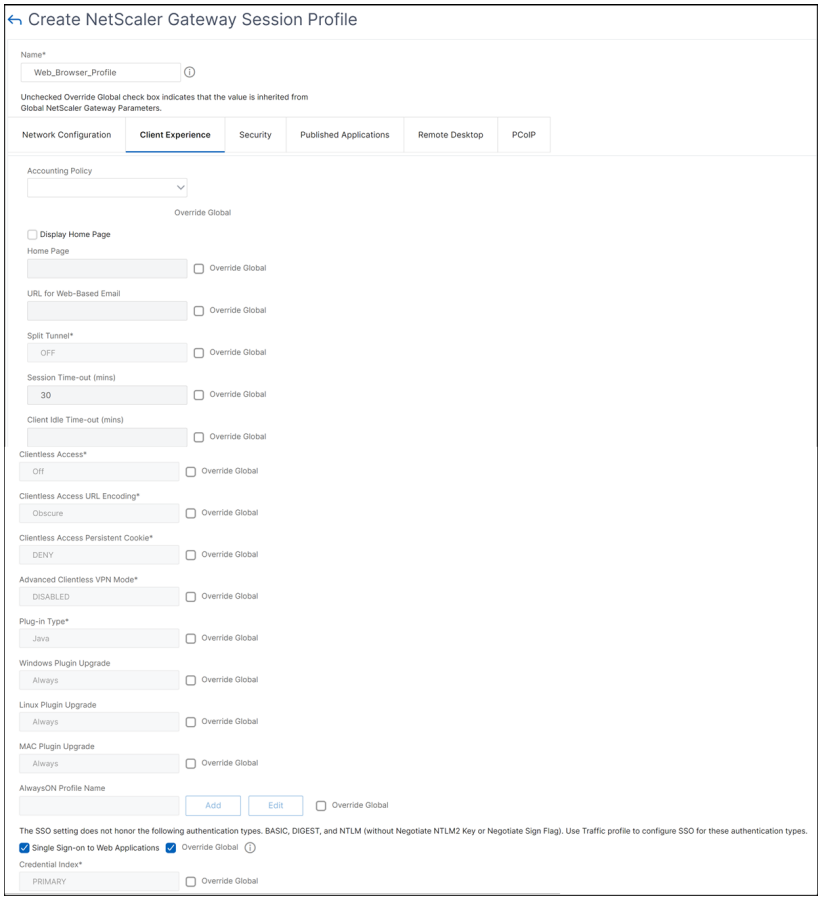
要将 NetScaler Gateway 与 StoreFront 集成，请完成以下步骤：

1. 为基于 Web 浏览器的访问创建会话策略
2. 为基于 Citrix Workspace 应用程序的访问创建会话策略
3. 创建身份验证配置文件
4. 创建 NetScaler Gateway 虚拟服务器
5. 在 StoreFront 上添加 NetScaler Gateway 实例

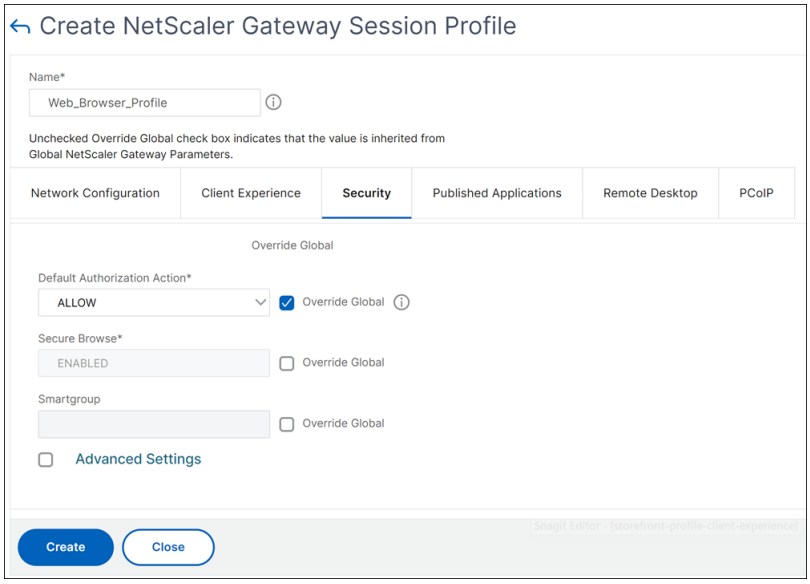


1. 为基于 **Web** 浏览器的访问创建会话策略

1. 导航到配置 **> NetScaler Gateway >** 策略 **>** 会话。
2. 在会话配置文件选项卡中，单击“添加”。
3. 为会话配置文件指定名称。
4. 在“客户端体验”选项卡中，启用以下设置：
   - 插件类型：默认情况下，插件类型设置为 **Java**。尽管此设置是可选的，但如果用户想要禁用完整 VPN，则建议使用。
   - 单点登录 **Web** 应用程序：通过选择此选项，当用户登录 NetScaler Gateway 时，它会将凭据转发到 StoreFront 网站。此设置使用户不必两次输入证书。但是，您还必须在 StoreFront 上启用从 NetScaler Gateway 直通身份验证方法。如果您要求用户使用不同的凭据登录 NetScaler Gateway 和 StoreFront 应用商店，请禁用此选项。



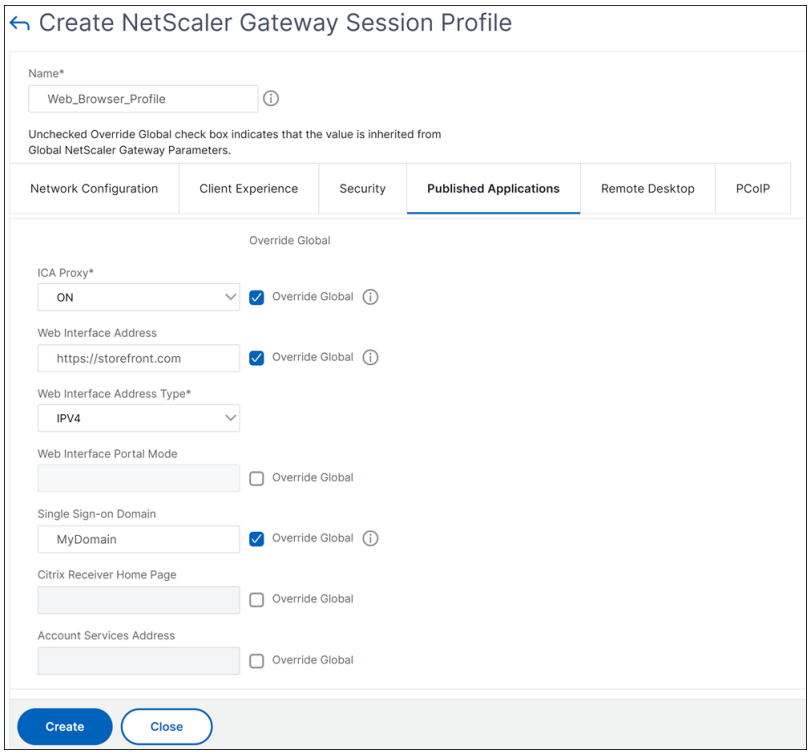
5. 在“安全”选项卡中，启用“默认授权操作”并将其设置为“允许”。



6. 在“已发布的应用程序”选项卡中，启用以下设置：

   - **ICA** 代理：设置为开。
   - **Web Interface** 地址：StoreFront 服务器的 FQDN，后面是应用商店 Web 站点的路径。

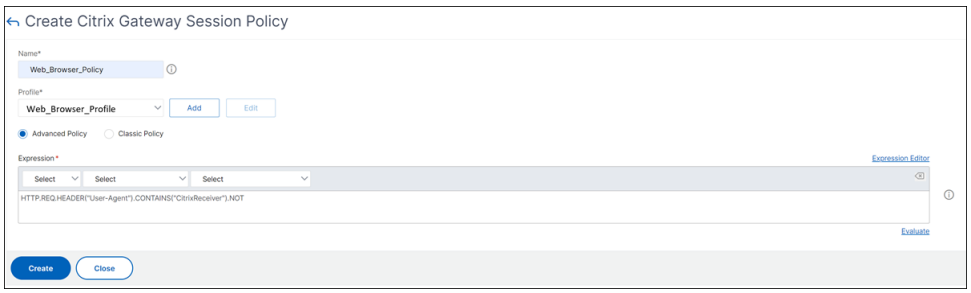
- 单点登录域：如果只使用一个域，则可以选择输入该域的 NetBIOS 名称。



7. 单击创建。
8. 在会话策略选项卡中，单击添加。NetScaler 需要使用会话策略来区分基于 Web 浏览器的连接和基于 Citrix Workspace 应用程序的连接。此策略适用于基于 Web 浏览器的连接。
9. 在名称中，为会话策略指定一个名称。
10. 在配置文件中，选择您创建的会话配置文件。
11. 单击“高级策略”选项，然后在“表达式”下输入以下语法：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

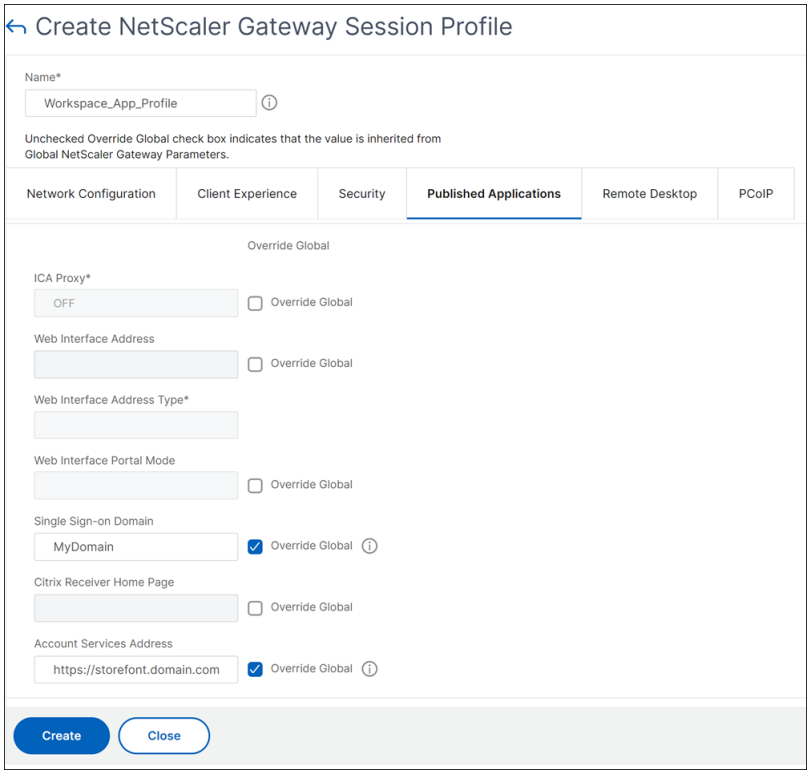
12. 单击创建。



有关 NetScaler Gateway 会话策略的更多详细信息，请参阅会话策略。

2. 为基于 **Citrix Workspace** 应用程序的访问创建会话策略

重复上述步骤，为基于 Citrix Workspace 应用程序的访问创建会话策略和会话配置文件。但是，在“已发布的应用程序”选项卡中，您必须配置“帐户服务地址”设置，而不是配置 Web Interface 地址。此步骤要求您提供 StoreFront 服务器的 FQDN。Citrix Workspace 应用程序使用此地址来发现服务器上可用的应用商店。



3. 创建身份验证配置文件

根据需要配置的身份验证方法类型，在 NetScaler 上创建身份验证配置文件。

尽管此步骤是可选的，但我们建议在授予 StoreFront 访问权限之前，使用 NetScaler Gateway 对用户的身份进行身份验证。

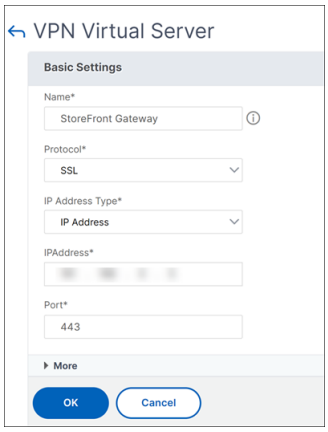
有关更多详细信息，请参阅身份验证和授权。

4. 创建 **NetScaler Gateway** 虚拟服务器

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 单击“添加”以添加 NetScaler Gateway 虚拟服务器。
3. 为虚拟服务器分配名称和地址。

> 注意：
>
> 如果您选择不使用 NetScaler Gateway 对用户进行身份验证，请单击“更多”并清除“启用身份验证”复选框。

4. 在“证书”下，单击“服务器证书”。
5. 上载服务器证书，然后单击“绑定”。
6. 添加会话策略：
   a) 在“策略”下，单击 **+**。
   b) 从“选择策略”下拉列表中，选择会话。从“类型”下拉列表中，选择“请求”，然后单击“继续”。
   c) 在“策略绑定”下，单击“选择策略”，然后选择之前创建的基于 Web 浏览器的会话策略和基于 Citrix Workspace 应用程序的会话策略，然后单击“绑定”将会话策略绑定到虚拟服务器。
7. 在“已发布的应用程序”下，单击 **STA** 服务器。指定至少一个 Security Ticket Authority (STA) URL。如果您使用的是 Citrix Virtual Apps and Desktops，请输入 Desktop Delivery Controller 的 URL。如果您使用的是 Citrix DaaS，请输入 Citrix Cloud Connector 的 URL。
8. 在“身份验证配置文件”下，选择您创建的身份验证配置文件。此步骤是必需的，因为不再支持经典策略。
9. 单击 **Done**（完成）。



5. 在 **StoreFront** 上添加 **NetScaler Gateway** 实例

有关如何在 StoreFront 上添加 NetScaler Gateway 实例的说明，请参阅配置 NetScaler Gateway。

引用

有关 StoreFront 和 NetScaler Gateway 集成的更多详细信息，请参阅以下主题：

- 添加 NetScaler Gateway
- 设计 StoreFront 和 NetScaler Gateway 集成

将 **Citrix Virtual Apps and Desktops** 与 **NetScaler Gateway** 集成

February 1, 2024

要管理对已发布资源和数据的访问，可以部署和配置 StoreFront 服务器。为了进行远程访问，建议在 StoreFront 前面添加 NetScaler Gateway。

> 注意
>
> 有关如何将 Citrix Virtual Apps and Desktops 与 NetScaler Gateway 集成的详细配置步骤，请参阅 StoreFront 文档。

下图说明了包含 Citrix NetScaler Gateway 的 Citrix 简化部署的示例。NetScaler Gateway 与 StoreFront 通信来保护 Citrix Virtual Apps and Desktops 提供的应用程序和数据。用户设备运行 Citrix Workspace 应用程序来创建安全连接以及访问其应用程序、桌面和文件。

用户使用 NetScaler Gateway 登录并进行身份验证。NetScaler Gateway 部署在 DMZ 中并受到保护。配置了双重身份验证。用户会根据用户凭据获得相关的资源和应用程序。应用程序和数据位于相应的服务器上（图中未显示）。安全性敏感应用程序和数据使用单独的服务器。

使用 **Citrix Endpoint Management**、**Citrix Virtual Apps** 和桌面进行部署

February 1, 2024

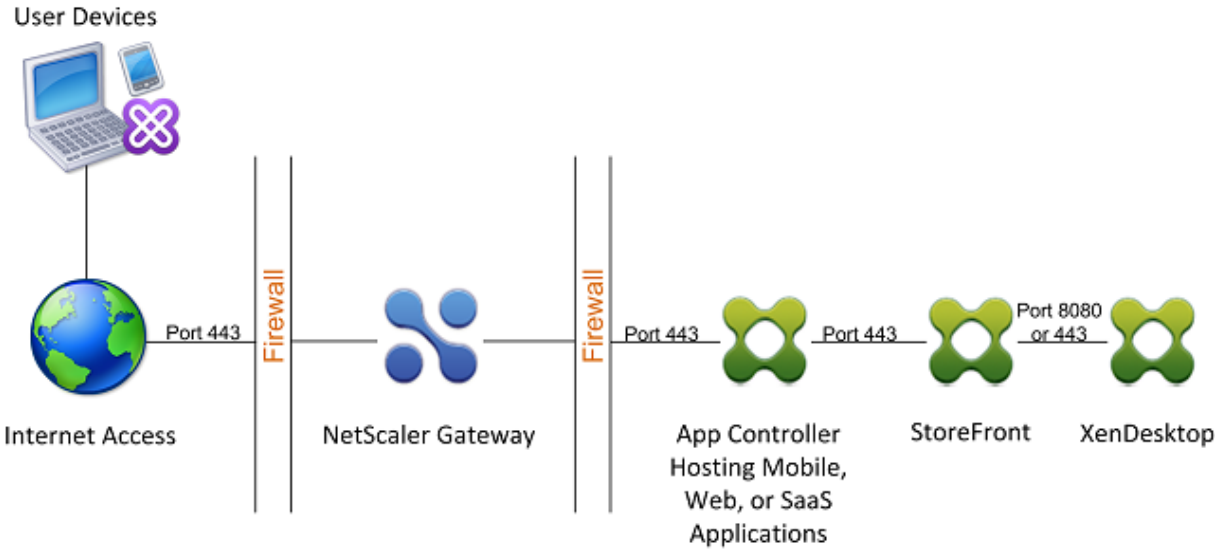
您可以让用户连接到网络中托管的 Windows、Web、SaaS 和移动应用程序和虚拟桌面。您可以使用 NetScaler Gateway、Citrix Endpoint Management 和 Citrix Virtual Apps and Desktops 为远程和内部用户提供对应用程序和桌面的访问权限。NetScaler Gateway 对用户进行身份验证，然后允许他们使用 Citrix Workspace 应用程序或 Secure Hub 访问其应用程序。

用户使用 Citrix Workspace 应用程序和 StoreFront 连接到在 Citrix Virtual Apps 中发布的基于 Windows 的应用程序以及 Citrix Virtual Desktops 中发布的虚拟桌面。

Citrix Endpoint Management 包含 Citrix Endpoint Management，允许用户连接到 Web、SaaS 和 MDX 应用程序。Endpoint Management 允许您管理单点登录 (SSO) 的 Web、SaaS 和 MDX 应用程序以及 ShareFile 文档。您可以在内部网络中安装 Endpoint Management。远程用户通过 NetScaler Gateway 连接到 Endpoint Management，以访问其应用程序和 ShareFile 数据。远程用户可以连接 Citrix Secure Access 客户端、Citrix Workspace 应用程序或 Secure Hub 来访问应用程序和 ShareFile。内部网络中的用户可以使用 Citrix Workspace 应用程序直接连接到 Endpoint Management。下图显示了使用 Endpoint Management 和 StoreFront 部署的 NetScaler Gateway。

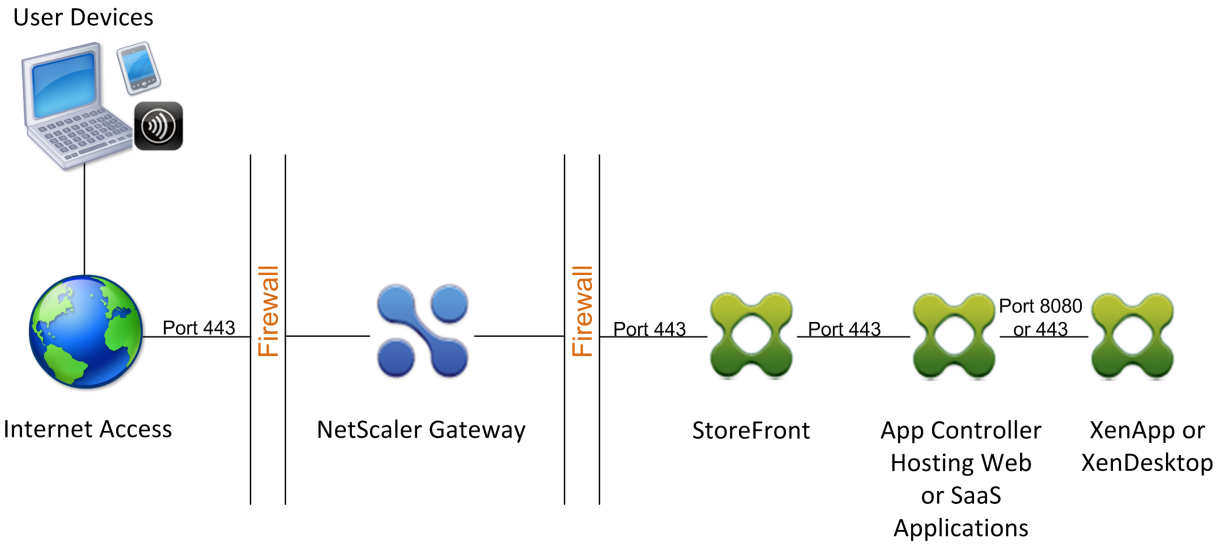
如果您的部署提供了从 Endpoint Management 对 MDX 应用程序的访问权限以及从 StoreFront 访问基于 Windows 的应用程序的权限，则可以在 StoreFront 前部署 Endpoint Management，如下图所示：

图 1. 在 StoreFront 前部署带有 Endpoint Management 功能的 NetScaler Gateway



如果您的部署不提供对 MDX 应用程序的访问权限，则 StoreFront 将驻留在 Endpoint Management 之前，如下图所示：

图 2. 在 Endpoint Management 之前使用 StoreFront 部署 NetScaler Gateway



对于每次部署，StoreFront 和 Endpoint Management 必须驻留在内部网络中，NetScaler Gateway 必须位于 DMZ 中。有关部署 Endpoint Management 的更多信息，请参阅 安装 Endpoint Management 主题。
有关部署 StoreFront 的更多信息，请参阅 StoreFront 主题。

为您的 **Citrix Endpoint Management Environment** 配置设置

February 1, 2024

适用于 Citrix Endpoint Management 的 NetScaler 向导将指导您完成 Citrix Endpoint Management 部署的 NetScaler 功能的配置。您可以使用向导执行以下操作：

- 设置微型 **VPN**。在这种情况下，远程用户可以访问内部网络中的应用程序和桌面。
  - 对于 Citrix Endpoint Management 仅 MAM 模式，必须使用 NetScaler Gateway 进行身份验证。
  - 对于 MDM 部署，Citrix 建议对移动设备 VPN 使用 NetScaler Gateway。
  - 对于耳鼻喉科部署，如果用户选择退出 MDM 注册，则设备将在旧版 MAM 模式下运行，并使用 NetScaler Gateway FQDN 进行注册。
- 配置基于证书的身份验证。Citrix Endpoint Management 的默认配置是用户名和密码身份验证。要为 Citrix Endpoint Management 环境的注册和访问添加另一层安全性，请考虑使用基于证书的身份验证。
- 负载平衡 **Citrix Endpoint Management** 服务器。如果您有多个 Citrix 端点管理服务器，或者 Citrix Endpoint Management 位于 DMZ 或内部网络内部（因此流量从设备流向 NetScaler 再到 Citrix 端点管理），则所有 Citrix 端点管理设备模式都需要 NetScaler 负载平衡。在这种情况下，NetScaler 设备位于用户设备和 Citrix Endpoint Management 服务器之间的隔离区中，用于对从移动设备发送到 Citrix Endpoint Management 服务器的加密数据进行负载平衡。

- 使用电子邮件筛选功能对 **Microsoft Exchange** 服务器进行负载平衡。在这种情况下，NetScaler 设备位于用户设备和 Citrix Endpoint Management NetScaler Connector (XNC) 之间，以及在用户设备和 Microsoft Exchange CAS 服务器之间。来自用户设备的所有请求都将发送到 NetScaler Gateway 设备，然后该设备与 XNC 通信以检索有关设备的信息。根据 XNC 的响应，NetScaler 设备会将请求从列入白名单的设备转发到内部网络中的服务器，或者从列入黑名单的设备中断连接。
- 根据请求的内容类型对 **ShareFile StorageZones** 连接器进行负载平衡。此方案会提示您输入有关存储区域控制器环境的基本信息，然后生成执行以下操作的配置：
  - 跨存储区域控制器负载平衡流量。
  - 为 StorageZones 连接器提供用户身份验证。
  - 验证 ShareFile 上载和下载的 URI 签名。
  - 在 NetScaler 设备上终止 SSL 连接。

有关配置 ShareFile 的更多信息，请参阅 为存储区域控制器配置 NetScaler。

> 重要提示：
>
> 在使用 Citrix Endpoint Management 向导之前，请务必参阅以下 Citrix Endpoint Management 部署文章以获取设计和部署信息以及建议：
>
> Citrix Endpoint Management 集成
>
> 与 NetScaler Gateway 和 NetScaler 集成
>
> MDX 应用程序的 SSO 和代理注意事项
>
> 身份验证
>
> 您只能使用适用于 Citrix Endpoint Management 的 NetScaler 向导一次。如果您想要多个 Citrix Endpoint Management 实例，例如用于测试、开发和生产环境，则必须为其他环境手动配置 NetScaler。以下支持文章列出了向导运行的命令，并提供了运行这些命令以创建 NetScaler 实例的说明：
>
> NetScaler 上的 Citrix Endpoint Management 向导生成的命令-SSL 桥
>
> NetScaler 上的 Citrix Endpoint Management 向导生成的命令-SSL 卸载

NetScaler 功能的许可要求

您必须安装许可证才能启用以下 NetScaler 功能：

- Citrix Endpoint Management MDM 负载平衡需要 NetScaler 标准许可证。
- 使用 StorageZones 进行 ShareFile 负载平衡需要 NetScaler 标准许可证。
- Exchange 负载平衡需要 NetScaler 许可证或高级许可证以及集成缓存许可证。

适用于 **Citrix Endpoint Management** 的 **NetScaler** 向导

本节提供了使用适用于 Citrix Endpoint Management 的 NetScaler 向导执行以下操作的示例：

- 设置微型 VPN 访问权限，以便远程用户连接到内部网络中 Citrix Endpoint Management 托管的资源
- 配置基于证书的身份验证。有关获取和安装公共 SSL 证书的信息，请参阅 安装和管理证书。
- 为 Citrix Endpoint Management 服务器配置负载平衡。

要使用向导：

1. 在 NetScaler GUI 中，单击“配置”选项卡，然后在“与 **Citrix** 产品集成”部分中单击 **XenMobile**。
2. 选择 Citrix Endpoint Management 版本，然后单击 开始使用。
3. 选择要配置的功能。此向导只能使用一次，因此必须手动执行后续配置。这些说明假设您选择了以下设置：通过 **NetScaler Gateway** 进行访问（适用于在 ENT 或 MAM 模式下运行的 Citrix Endpoint Management）和平衡 **Citrix Endpoint Management** 服务器的负载。
4. 在 **NetScaler Gateway** 配置页面上，输入面向外部的 NetScaler Gateway IP 地址、端口和虚拟服务器名称的值。
5. 在 **NetScaler Gateway** 的服务器证书页面的证书文件中，从本地或设备中选择证书文件。
   - 本地：在您的计算机上选择证书
   - 设备：在 NetScaler Gateway（设备）上选择证书。
6. 在“身份验证”页面的“主身份验证方法”中，选择“客户端证书”，然后输入证书配置文件的名称。

   以下各步骤假定您已配置证书策略。

   如果必须创建证书策略，请单击“创建证书策略”。在 Citrix Endpoint Management 证书屏幕上，选择现有服务器证书或安装新证书。如果您运行多台 Citrix Endpoint Management 服务器，则需要为每台服务器添加一个证书。在“服务器登录名属性”中，根据您的要求指定 userPrincipalName 或 sAMAccountName。
7. 单击“双重身份验证”以启用双重身份验证，客户端证书身份验证，然后使用 LDAP 或 RADIUS 作为辅助身份验证类型。
8. 在辅助身份验证方法中，选择辅助身份验证方法。
   - 使用客户端证书作为主要身份验证类型，您可以选择将 LDPA（或 RADIUS）配置为辅助身份验证类型。

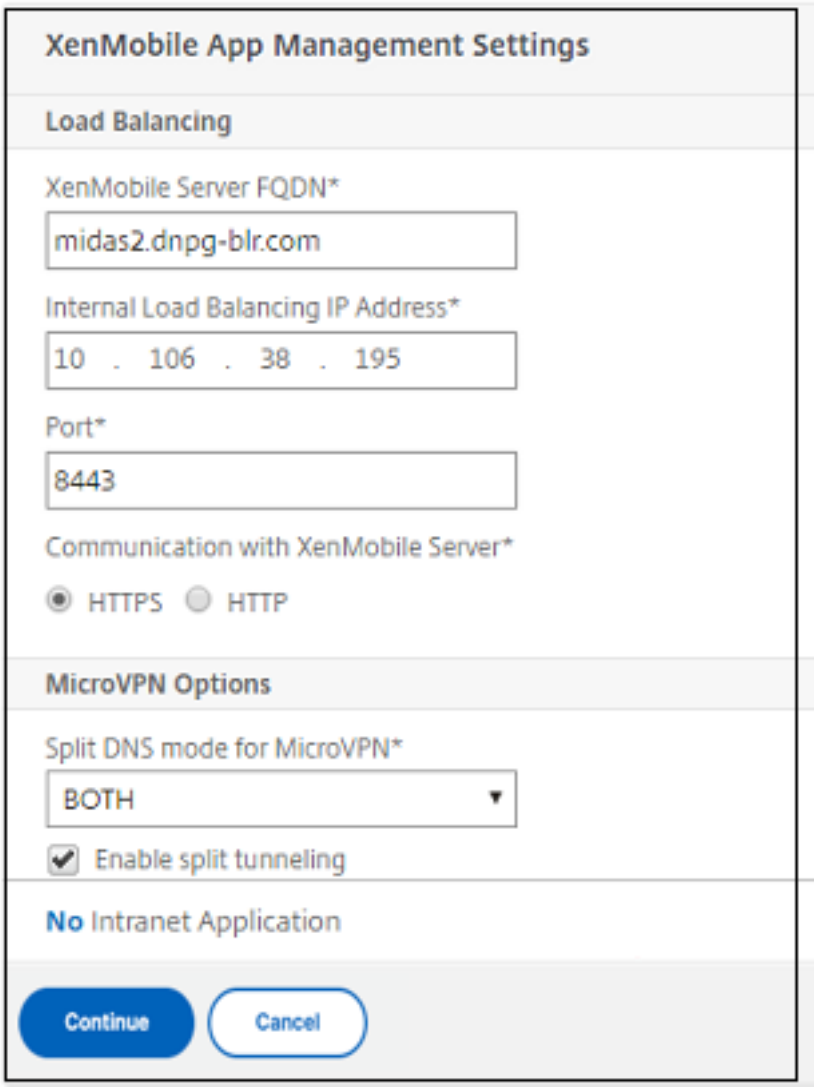
     要仅使用客户端证书身份验证，请将 第二种身份验证方法 保留为 无，然后单击 继

     要使用客户端证书 + 域 (LDAP) 身份验证，请将辅助身份验证方法更改为 **LDAP** 并配置身份验证服务器设置。
9. 配置 **Citrix Endpoint Management** 应用程序管理设置。
   - 输入 **Citrix Endpoint Management FQDN**。这是 MAM 的负载平衡 FQDN。

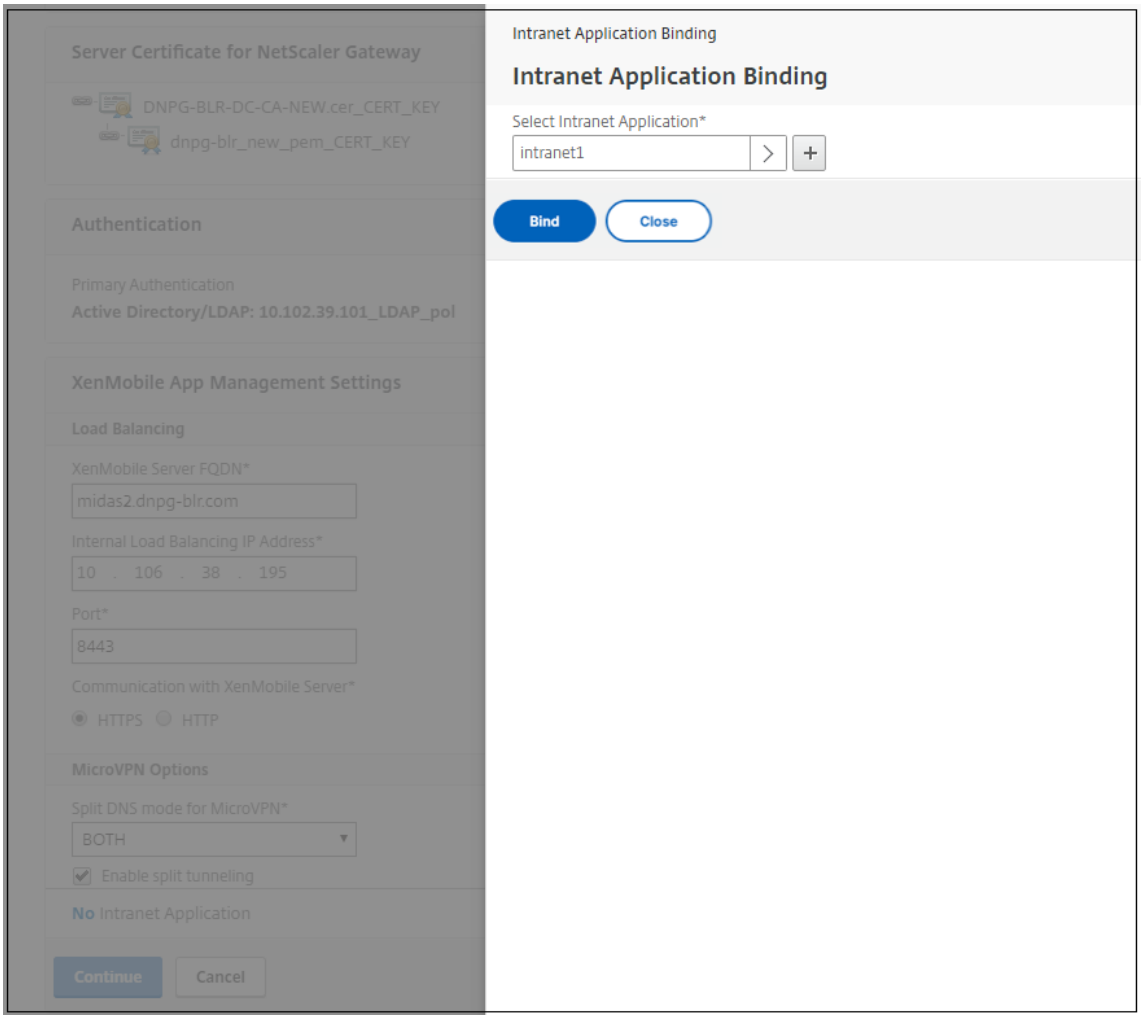
- 为 负载平衡 **Citrix Endpoint Management** 服务器的虚拟服务器输入仅限 **MAM** 的内部负载平衡 **IP** 地址。NetScaler Gateway 通过此 MAM 负载平衡虚拟 IP 与 Citrix Endpoint Management 进行通信。
- 这是 SSL 卸载部署，因此请在与 Citrix Endpoint Management 服务器通信中选择 **HTTP**。
- **MicroVPN** 的拆分 **DNS** 模式字段会自动设置为两者。

如果您的部署需要拆分通道，请选择 启用拆分通道。接下来，如果启用拆分通道，请配置 Intranet 应用程序绑定。

默认情况下，安全 Web 访问通过通道传输到内部网络，这意味着 Secure Web 使用每个应用程序的 VPN 通道返回到内部网络进行所有网络访问，NetScaler 设备使用拆分通道设置。

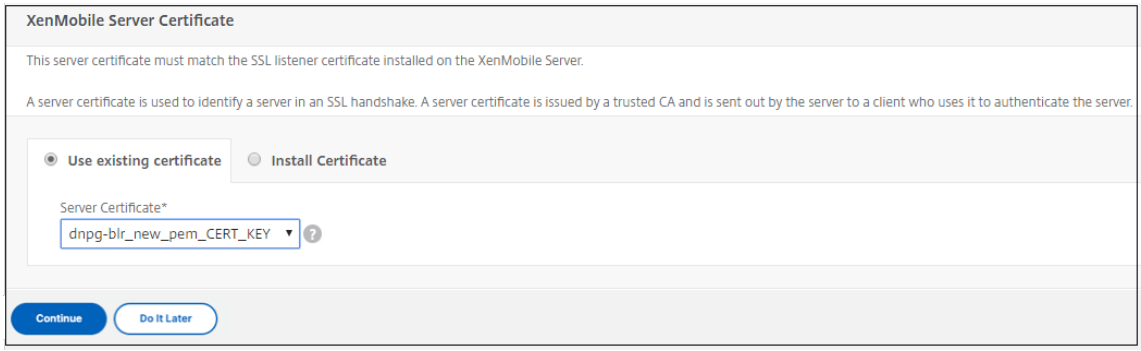


10. 要在 NetScaler Gateway 上为用户连接配置拦截规则，必须配置 **Intranet** 应用程序绑定。单击 **+** 添加绑定。

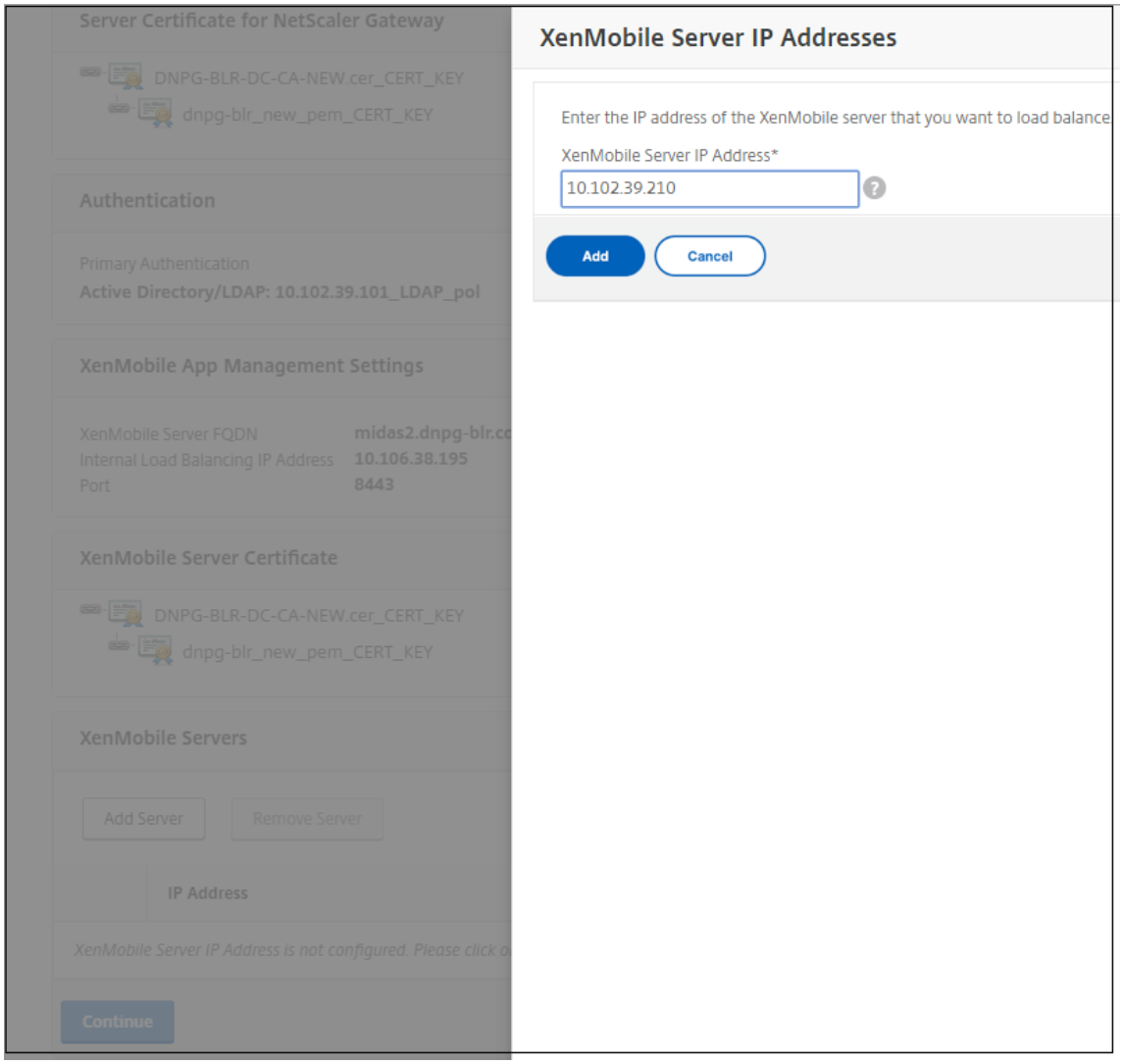


11. 填写允许网络访问的参数，然后单击 创建。

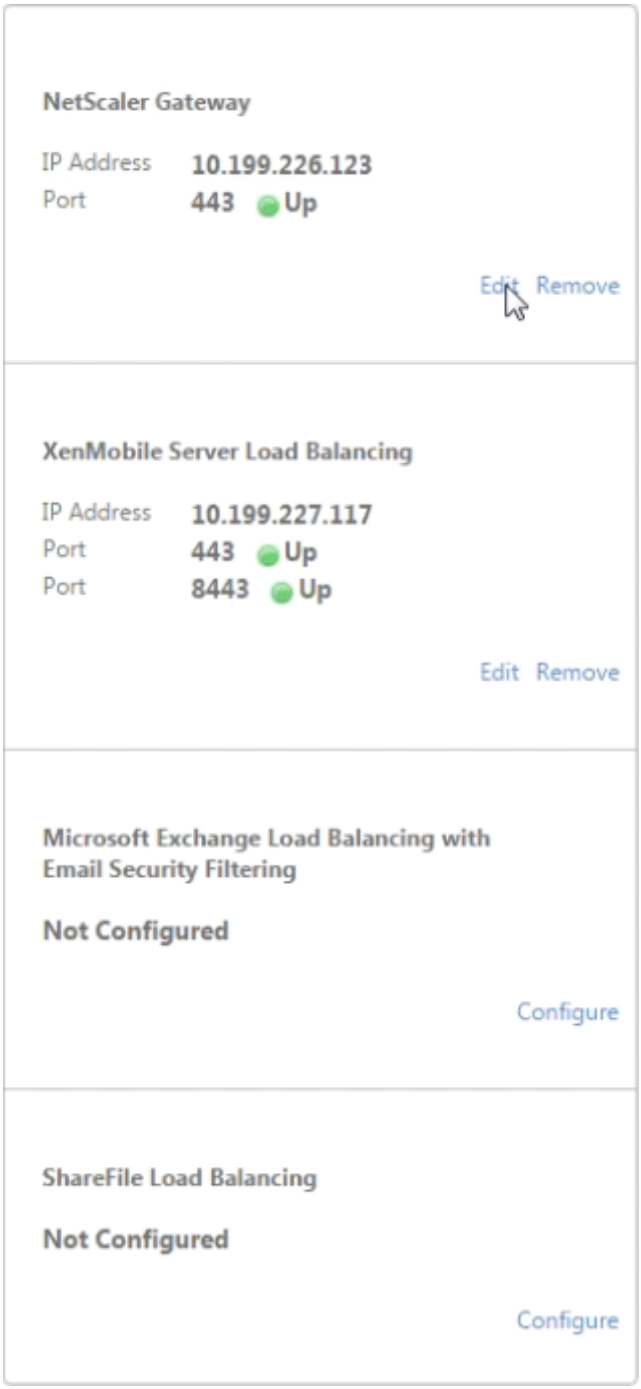
12. 添加 Citrix Endpoint Management 证书。这用于 MAM 负载平衡虚拟服务器。



13. 在 **Citrix Endpoint Management** 服务器下，单击 添加服务器 以添加要绑定到负载平衡虚拟 **IP** 的 **Citrix Endpoint Management IP** 地址。



在 NetScaler 控制面板上，确认已配置 NetScaler Gateway 和 Citrix Endpoint Management 负载平衡。



如果您使用用户证书中的 sAMAccount 属性来替代用户主体名称 (UPN)，请按照手动配置 NetScaler Gateway 进行客户端证书身份验证中所述配置证书配置文件。

为 Citrix Endpoint Management 或 Citrix XenMobile Server 配置负载平衡服务器

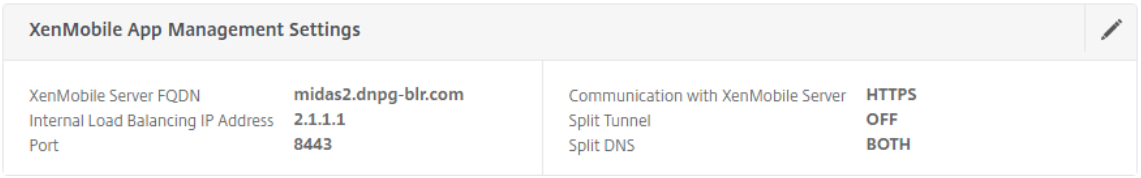
February 1, 2024

使用适用于 **Citrix Endpoint Management** 的 **NetScaler** 向导进行初始设置后，如本节所述，使用 NetScaler Gateway 配置实用程序配置负载平衡。对于 Citrix Endpoint Management，请使用 SSL 卸载。对于 Citrix Endpoint Management 服务器，请务必参阅 与 NetScaler Gateway 和 NetScaler 集成中“部署摘要”下的负载平衡模式建议。

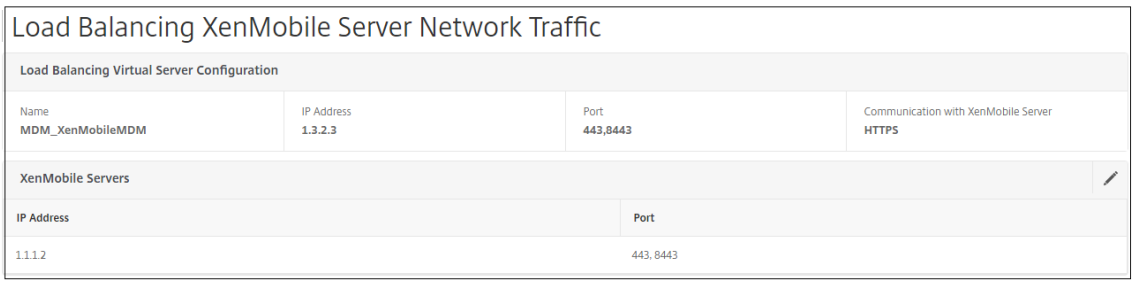
要对 NetScaler VIP 使用 SSL 桥接模式

如果 Citrix Endpoint Management 位于 DMZ 中，请使用 SSL 桥接模式。在 SSL Bridge 模式下使用 NetScaler VIP 对 Citrix 端点管理进行负载平衡时，Internet 流量将直接流向 Citrix Endpoint Management 服务器，连接在那里终止。SSL 桥接模式是易于设置和故障排除的最简单模式。

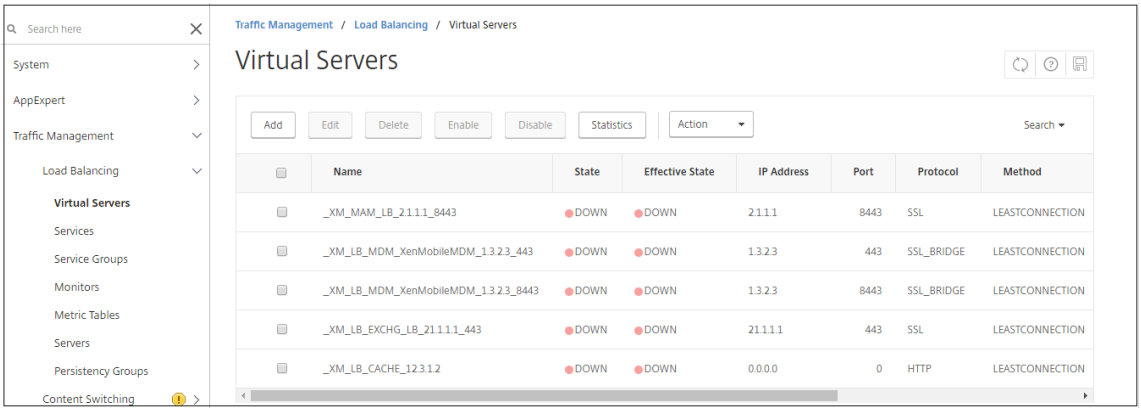
1. 在配置 SSL Bridge 模式之前，请转到 **Citrix Endpoint Management** 应用程序管理设置 并验证 与 **Citrix Endpoint Management** 服务器的通信 是否为 **HTTPS**。



2. 登录配置实用程序后，在 主页 选项卡的 **MDM Server LB** 中，单击 配置。
3. 在 用于设备管理的 **LB** 虚拟服务器下的 名称中，键入服务器的名称。
4. 在 **IP** 地址中，键入虚拟服务器的 IP 地址，然后单击 继续。
5. 在 负载平衡 **Citrix Endpoint Management MDM** 服务器 页面上，重复步骤 3 和 4，然后单击 创建。
6. 验证设置是否正确，然后单击“完成”。



7. 要验证负载平衡配置，请转到 流量管理 **>** 虚拟服务器。

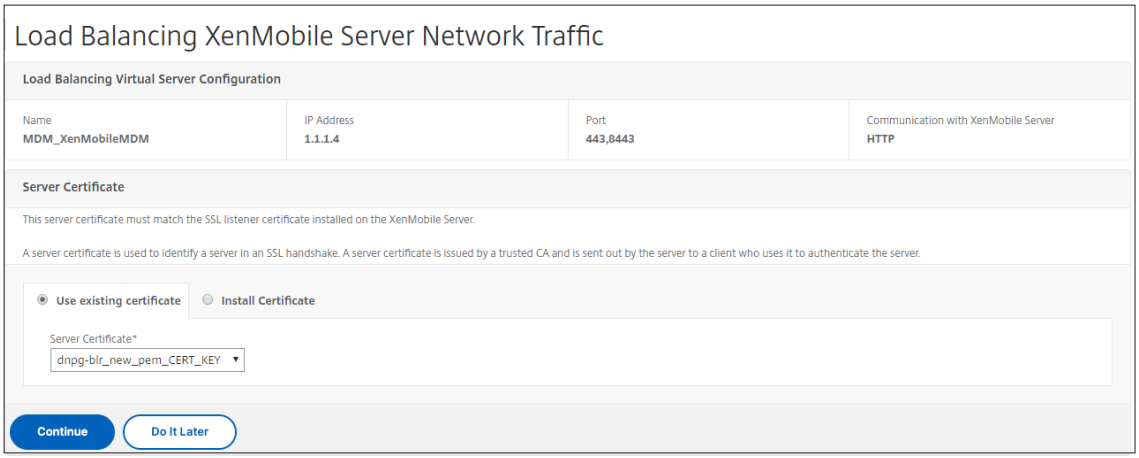


对 **NetScaler VIP** 使用 **SSL** 卸载模式

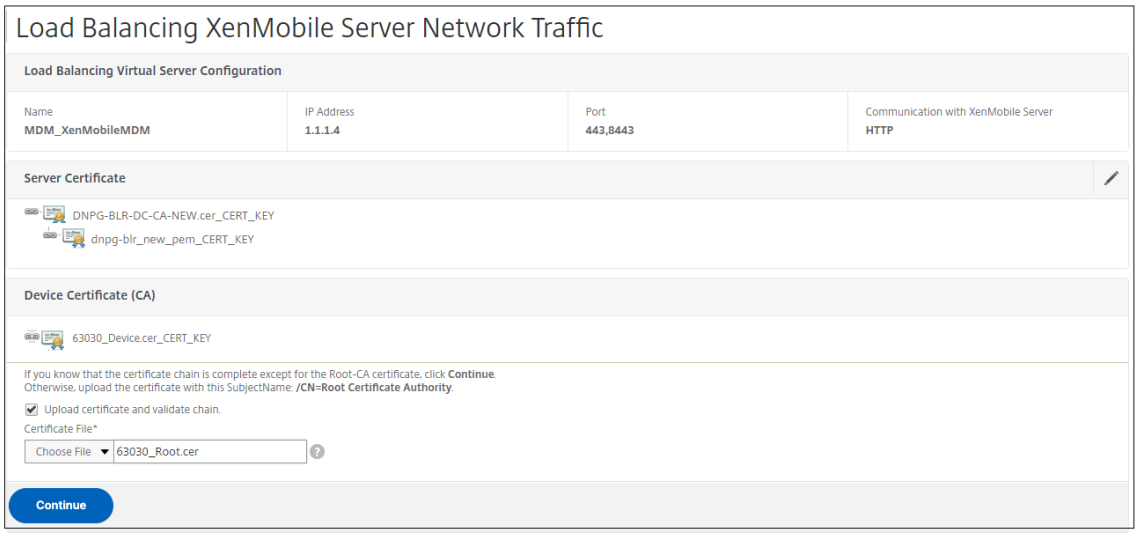
对 Citrix Endpoint Management 使用 SSL 卸载。当内部部署 Citrix Endpoint Management 位于内部网络中时，如果需要满足安全标准，还可以使用 SSL 卸载。在 SSL 卸载模式下使用 NetScaler VIP 对 Citrix Endpoint Management 进行负载平衡时，Internet 流量将直接流向 NetScaler 设备，连接在该设备上终止。然后，NetScaler Gateway 会建立从设备到 Citrix Endpoint Management 的新会话。SSL 卸载模式在设置和故障排除过程中涉及更多复杂性。

1. 在配置 SSL 卸载模式之前，请转到 **Citrix Endpoint Management** 应用程序管理设置 并验证 与 **Citrix Endpoint Management** 服务器的通信 是否为 **HTTP**。

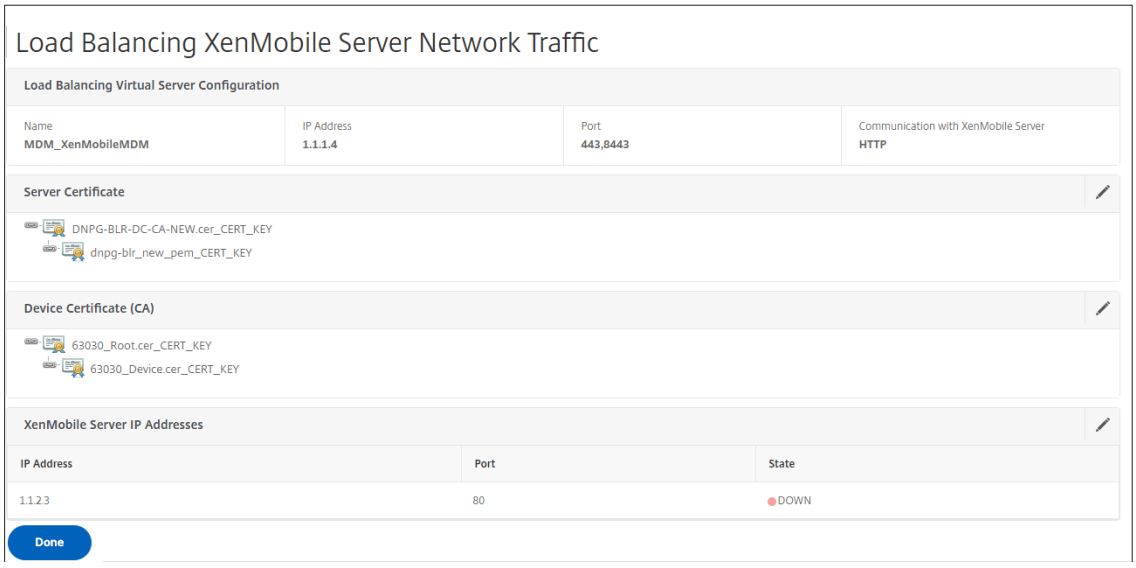
2. 登录配置实用程序。在“主 页”选项卡上的“**MDM Server LB**”中，单击“配置”。
3. 在 用于设备管理的 **LB** 虚拟服务器下的 名称中，键入服务器的名称。
4. 在 **IP** 地址中，键入虚拟服务器的 IP 地址，然后单击 继续。
5. 在 负载平衡 **Citrix Endpoint Management MDM** 服务器 页面上，重复步骤 3 和 4，然后单击 创建。
6. 验证设置，然后单击“完成”。
7. 当系统提示您添加服务器证书时，选择服务器证书，然后单击 继续。



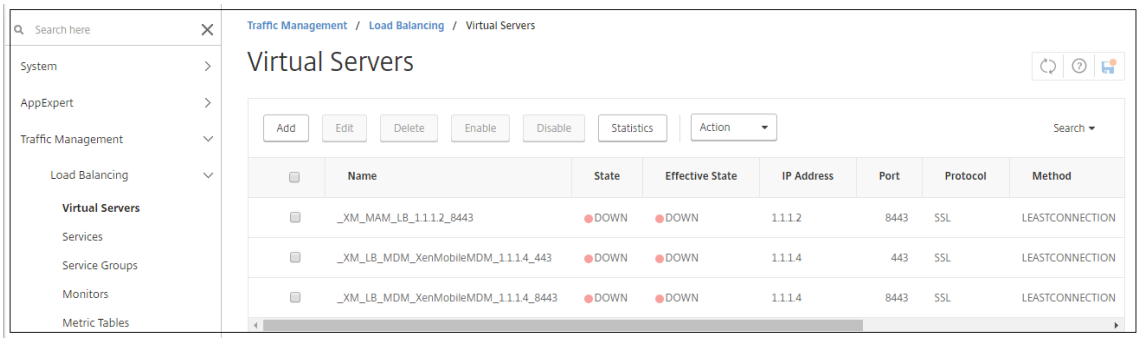
8. 指定 CA 证书，然后单击 继续。



9. 保持相同的 Citrix Endpoint Management IP 地址。单击 **Done**（完成）。



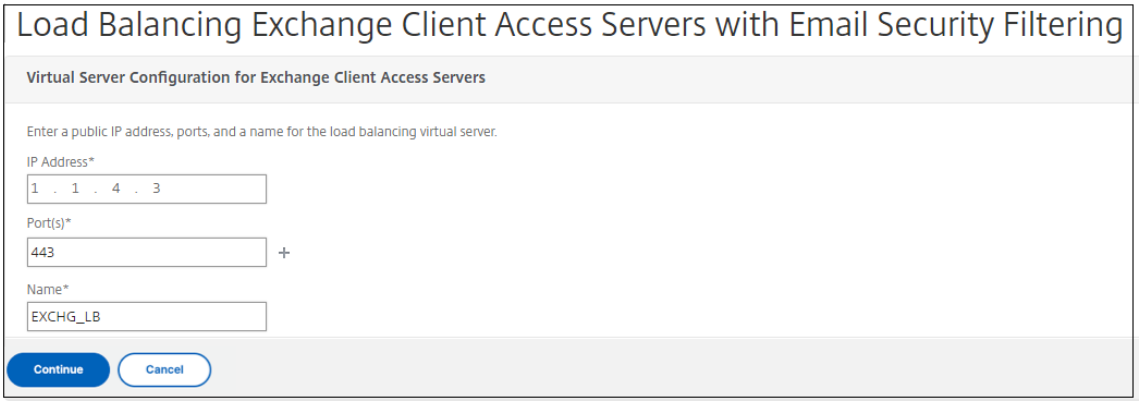
10. 要验证负载平衡配置，请转到 流量管理 > 虚拟服务器。



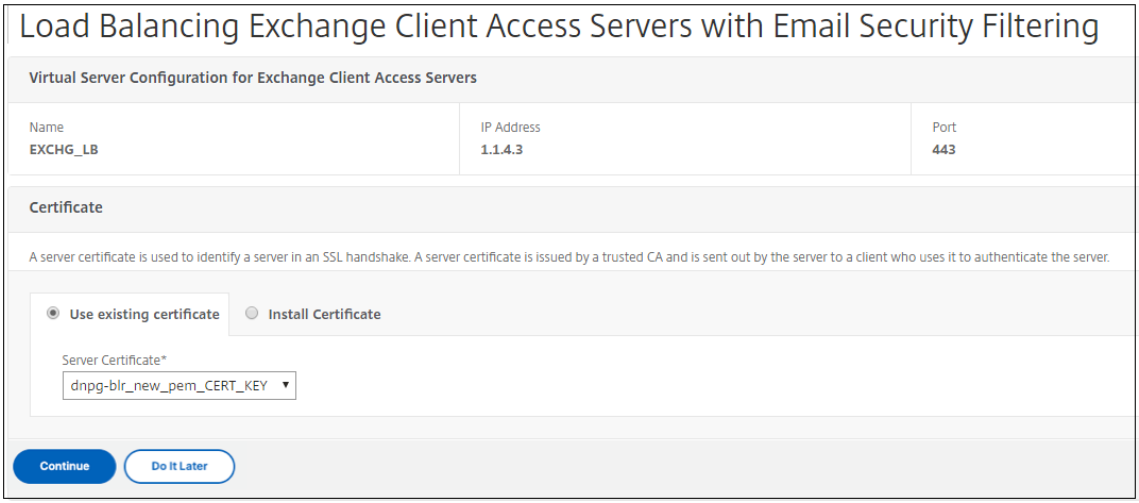
使用电子邮件安全筛选功能为 **Microsoft Exchange** 配置负载平衡服务器

February 1, 2024

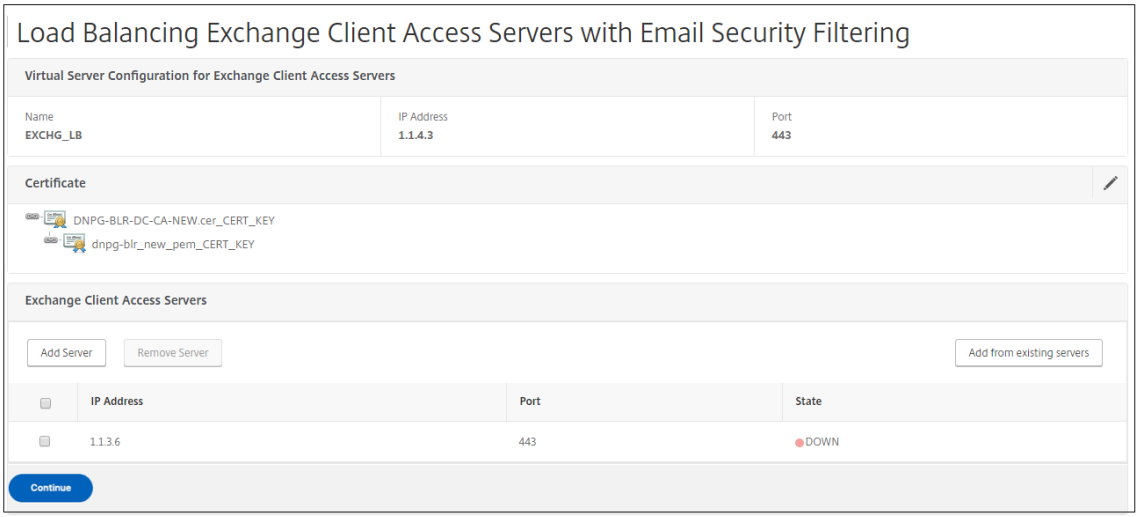
1. 在“主 页”选项卡上的“**MDM Server LB**”中，单击“配置”。
2. 在 **Exchange CAS** 的 **LB** 虚拟服务器下的 名称中，键入服务器的名称。
3. 在 **IP** 地址中，键入虚拟服务器的 IP 地址。
4. 在 **Port**（端口）中，键入端口号。要添加更多端口，请单击加号 (**+**)，然后键入端口号。
5. 单击继续。



6. 在 证书下，选择现有证书或安装计算机（本地）或 NetScaler 设备（设备）上的证书。
7. 单击继续。



8. 在 **Exchange Citrix Analytics** 服务实例下，键入虚拟服务器的名称、IP 地址和端口号。然后，单击 添加 并继续。



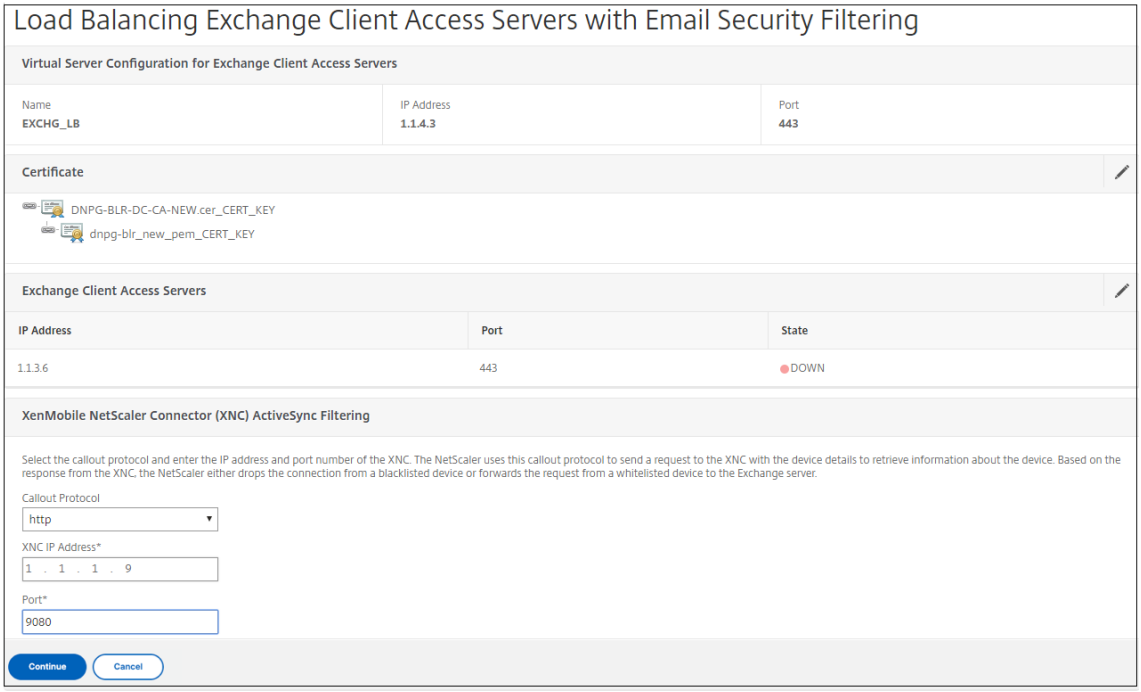
单击完成时，将显示用于配置 Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync 筛选的字段。

配置 **Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync** 筛选

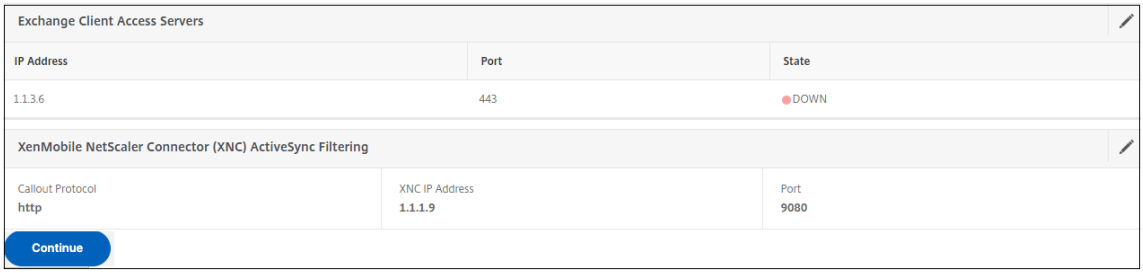
February 1, 2024

Citrix Endpoint Management NetScaler Connector (XNC) 向 NetScaler 提供 ActiveSync 客户端的设备级授权服务，该服务充当 Exchange ActiveSync 协议的反向代理。Citrix Endpoint Management 中定义的策略与 XNC 在本地定义的规则的组合控制授权。

1. 在 **Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync** 筛选下，对于标注协议，选择 **http** 或 **https**。
2. 在 **XNC IP** 地址中，键入 Citrix Endpoint Management NetScaler Connector 的 IP 地址。
3. 在 端口中，键入 **9080** 作为 HTTP 网络流量，键入 **9443** 作为 HTTPS 网络流量，然后单击 继续。



将显示您的配置。



允许使用 **Citrix** 移动生产力应用程序从移动设备访

February 1, 2024

适用于 XenMobile 的 NetScaler 向导配置所需的设置，以允许用户通过 NetScaler Gateway 从受支持的设备连接到内部网络中的移动应用程序和资源。用户通过使用安全中心（以前称为 Citrix Secure Hub）进行连接，它可以建立 Micro VPN 通道。用户连接时，VPN 通道将打开到 NetScaler Gateway，然后传递到内部网络中的 XenMobile。然后，用户可以从 XenMobile 访问其 Web、移动和 SaaS 应用程序。

要确保用户在使用多个设备同时连接到 NetScaler Gateway 时使用单个通用许可证，可以在虚拟服务器上启用会话传输。有关详细信息，请参 阅在虚拟服务器上配置连接类型。

如果在使用 NetScaler for XenMobile 向导后需要更改配置，请使用本文中的部分获取指导。在更改设置之前，请确保了解更改的含义。有关详细信息，请参阅 XenMobile 部署 文章。

在 **NetScaler Gateway** 中配置 **Secure Browse**

您可以更改 Secure Browse 作为全局设置的一部分或作为会话配置文件的一部分。您可以将会话策略绑定到用户、组或虚拟服务器。配置 Secure Browse 时，还必须启用无客户端访问。但是，无客户端访问不需要启用 Secure Browse。配置无客户端访问时，将 无客户端访问 **URL** 编码 设置为 清除。

要全局配置 Secure Browse：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 **NetScaler Gateway** 设置”对话框的“安 全”选项卡上，单击“**Secure Browse**”，然后单击“确定”。

要在会话策略和配置文件中配置 Secure Browse：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格中，执行以下操作之一：
   - 如果要创建新的会话策略，请单击 添加。
   - 如果要更改现有策略，请选择一个策略，然后单击 打开。
3. 在策略中，创建配置文件或修改现有配置文件。为此，请执行以下操作之一：
   - 在“请求配置文件”旁边，单击“新建”。
   - 在“请求配置文件”旁边，单击“修改”。
4. 在 安 全选项卡上的 **Secure Browse** 旁边，单击 覆盖全局，然后选择 **Secure Browse**。
5. 执行以下操作之一：
   - 如果要创建新的配置文件，请单击 创建，在策略对话框中设置表达式，单击 创建，然后单击 关闭。
   - 如果您正在修改现有配置文件，则在进行选择后，请两次单击“确定”。

要在 Secure Browse 模式下为 Secure Web 配置流量策略：

使用以下步骤配置流量策略，以便在 Secure Browse 模式下通过代理服务器路由 Secure Web 流量。

1. 在配置实用程序中的 配置 选项卡上，展开 **NetScaler Gateway >** 策略，然后单击 流量。
2. 在右窗格中，单击“流量配置文件”选项卡，然后单击“添加”。
3. 在 名称中，输入配置文件的名称，选择 **TCP** 作为协议，然后保持其余设置不变。

4. 单击创建。
5. 单击 流量配置文件 选项卡，然后单击 添加。
6. 在 名称中，输入配置文件的名称，然后选择 **HTTP** 作为 协议。
   此流量配置文件适用于 HTTP 和 SSL。无客户端 VPN 流量设计上是 HTTP 流量，无论目标端口或服务类型如何。因此，您可以在流量配置文件中将 SSL 和 **HTTP** 流量指定为 **HTTP** 。
7. 在 代理中，输入代理服务器的 IP 地址。在 端口中，输入代理服务器的端口号。
8. 单击创建。
9. 单击 流量策略 选项卡，然后单击 添加。
10. 输入流量策略的 名称，对于 请求配置文件，选择您在步骤 3 中创建的流量配置文件。输入以下 表达式，然后单击 创建：

```
1 REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
     User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
     CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
     Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
     HTTP.URL CONTAINS StoreWeb
2 <!--NeedCopy-->
```

    该规则根据主机标头执行检查。要绕过来自代理的活动同步流量，请替换 **`ActiveSyncServer`** 为相应的活动同步服务器名称。
11. 单击 流量策略 选项卡，然后单击 添加。输入流量策略的 名称，对于 请求配置文件，选择在步骤 6 中创建的流量配置文件。输入以下 表达式，然后单击 创建：

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

12. 单击 流量策略 选项卡，然后单击 添加。输入流量策略的 名称，对于 请求配置文件，选择在步骤 6 中创建的流量配置文件。输入以下 表达式，然后单击 创建：

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

13. 导航到 **NetScaler Gateway >** 虚拟服务器，在右窗格中选择虚拟服务器，然后单击 编辑。
14. 在 策略 行上，单击 **+**。
15. 从“选择策略”菜单中，选择“流量”。
16. 单击继续。
17. 在 策略绑定下的“选择策略”对面，单击 **。

18. 选择您在步骤 10 中创建的策略，然后单击 确定。
19. 单击绑定。
20. 在 策略下，单击 流量策略。
21. 在 **VPN** 虚拟服务器流量策略绑定下，单击 添加绑定。
22. 在策略绑定下的“选择策略”菜单旁边，单击 **>** 以查看策略列表。
23. 选择您在步骤 11 中创建的策略，然后单击 确定。
24. 单击绑定。
25. 在 策略下，单击 流量策略。
26. 在 **VPN** 虚拟服务器流量策略绑定下，单击 添加绑定。
27. 在策略绑定下的“选择策略”菜单旁边，单击 **>** 以查看策略列表。
28. 选择您在步骤 12 中创建的策略，然后单击 确定。
29. 单击绑定。
30. 单击关闭。
31. 单击 **Done**（完成）。

请务必在 XenMobile 控制台中配置 Secure Web 网络 (WorxWeb) 应用程序。转到 配置 **>** 应用程序，选择 Secure Web 应用程序，单击 编辑，然后进行以下更改：

- 在 应用程序信息 页面上，将 初始 **VPN** 模式 更改为 **Secure Browse**。
- 在 **iOS** 页面上，将 初始 **VPN** 模式 更改为 **Secure Browse**。
- 在 **Android** 页面上，将 首选 **VPN** 模式 更改为 **Secure Browse**。

配置应用程序和 **MDX** 令牌超时

当用户从 iOS 或 Android 设备登录时，将颁发应用程序令牌或 MDX 令牌。该令牌类似于 Secure Ticket Authority (STA)。

您可以设置令牌处于活动状态的秒数或分钟数。如果令牌过期，用户将无法访问请求的资源，例如应用程序或网页。

令牌超时是全局设置。配置该设置时，它适用于登录 NetScaler Gateway 的所有用户。

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“全局 **NetScaler Gateway** 设置”对话框中的“客户端体验”选项卡上，单击“高级设置”。
4. 在 常规 选项卡上的 应用程序令牌超时 **(**秒**)** 中，输入令牌到期前的秒数。默认值为 **100** 秒。
5. 在 **MDX** 令牌超时 **(**分钟**)** 中，输入令牌到期前的分钟数，然后单击 确定。默认值为 **10** 分钟。

为移动设备禁用端点分析

如果配置端点分析，则需要配置策略表达式，以便端点分析扫描不会在 Android 或 iOS 移动设备上运行。移动设备不支持端点分析扫描。

如果将端点分析策略绑定到虚拟服务器，则必须为移动设备创建辅助虚拟服务器。请勿将身份验证前或身份验证后策略绑定到移动设备虚拟服务器。

在预身份验证策略中配置策略表达式时，可以添加 User-Agent 字符串以排除 Android 或 iOS。当用户从这些设备之一登录并排除设备类型时，端点分析不会运行。

例如，您可以创建以下策略表达式来检查 User-Agent 是否包含 Android、应用程序 virus.exe 是否不存在，如果进程 keylogger.exe 正在运行，则使用预身份验证配置文件结束该进程。策略表达式可能如下所示：

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

创建预身份验证策略和配置文件后，将策略绑定到虚拟服务器。当用户从 Android 或 iOS 设备登录时，扫描不会运行。如果用户从基于 Windows 的设备登录，则扫描确实会运行。

有关配置预身份验证策略的更多信息，请参阅 配置端点策略。

通过使用适用于 **Android** 设备的 **DNS** 后缀来支持 **DNS** 查询

当用户从 Android 设备建立 Micro VPN 连接时，NetScaler Gateway 会向用户设备发送拆分 DNS 设置。NetScaler Gateway 支持基于您配置的拆分 DNS 设置拆分 DNS 查询。NetScaler Gateway 还可以支持基于您在设备上配置的 DNS 后缀的拆分 DNS 查询。如果用户从 Android 设备进行连接，则必须在 NetScaler Gateway 上配置 DNS 设置。

拆分 DNS 的工作方式如下：

- 如果将拆分 DNS 设置为“本地”，则 Android 设备会将所有 DNS 请求发送到本地 DNS 服务器。
- 如果将拆分 DNS 设置为 远程，则所有 DNS 请求都将发送到 NetScaler Gateway（远程 DNS 服务器）上配置的 DNS 服务器进行解析。
- 如果您将拆分 DNS 设置为“两者”，则 Android 设备会检查 DNS 请求类型。
  - 如果 DNS 请求类型不是“A”，它会将 DNS 请求数据包发送到本地和远程 DNS 服务器。
  - 如果 DNS 请求类型为“A”，Android 插件将提取查询 FQDN，并将该 FQDN 与 NetScaler 设备上配置的 DNS 后缀列表进行匹配。如果 DNS 请求的 FQDN 匹配，则 DNS 请求将发送到远程 DNS 服务器。如果 FQDN 不匹配，则 DNS 请求将发送到本地 DNS 服务器。

下表总结了基于 A 类记录和后缀列表的拆分 DNS 的工作原理。

拆分 DNS 设置	这是 A 型记录吗?	它在后缀列表中吗?	DNS 请求的发送地点
本地	两者都是或否	两者都是或否	本地
远程	两者都是或否	两者都是或否	远程
两者都	否	不适用	两者都
两者都	是	是	远程
两者都	是	否	本地

要配置 DNS 后缀，请执行以下操作：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格的“策 略”选项卡上，选择一个会话策略，然后单击“打开”。
3. 在“请求配置文件”旁边，单击“修改”。
4. 在 网络配置 选项卡上，单击 高级。
5. 在 **Intranet IP DNS** 后缀旁边，单击“覆盖全局”，键入 DNS 后缀，然后单击三次“确定”。

要在 NetScaler Gateway 上全局配置拆分 DNS：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway**，然后单击“全局设置”。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在“客户体验”选项卡上，单击“高级设置”。
4. 在 常规 选项卡的 拆分 **DNS** 中，选择 两者、远程或 本地，然后单击 确定。

要在 NetScaler Gateway 上的会话策略中配置拆分 DNS：

1. 在配置实用程序中，在配置选项卡的导航窗格中，展开 **NetScaler Gateway >** 策略，然后单击会话。
2. 在详细信息窗格的“策略”选项卡上，单击“添加”。
3. 在名称中，键入策略的名称。
4. 在“请求配置文件”旁边，单击“新建”。
5. 在名称中，键入配置文件的名称。
6. 在“客户体验”选项卡上，单击“高级设置”。
7. 在 常规 选项卡上的 拆分 **DNS** 旁边，单击 覆盖全局，选择 两者、远程或 本地，然后单击 确定。
8. 在 创建会话策略 对话框的 命名表达式旁边，选择 常规，选择 **True**，单击 添加表达式，单击 创建，然后单击 关闭。

为 **Citrix Endpoint Management** 配置域和安全令牌身份验证

February 1, 2024

您可以将 Citrix Endpoint Management 配置为要求用户使用其 LDAP 凭据和一次性密码使用 RADIUS 协议进行身份验证。本节介绍该双因素身份验证类型所需的 NetScaler Gateway 配置。

必备条件

如果尚未运行适用于 Citrix Endpoint Management 的 NetScaler 向导，请参阅为 Citrix Endpoint Management 环境配置设置中的适用于 *Citrix Endpoint Management* 的 *NetScaler* 向导部分。确保您的 NetScaler 配置包括以下内容：

- **LDAP** 端口号 = **636** （这是安全 LDAP 连接的默认端口）
- 根据您的要求，服务器登录名属性 = **samAccountName** 或 **userPrincipalName**

配置域和安全令牌身份验证

1. 转到 **NetScaler Gateway >** 虚拟服务器。选择虚拟服务器，然后单击 编辑。
2. 单击 没有 **CA** 证书。
3. 在选择 **CA** 证书中，选择一个证书，单击确定，单击绑定，然后单击完成。
4. 转到策略 **>** 会话 **>** 会话配置文件，选择配置文件，然后单击编辑。
5. 单击“客户端体验”选项卡。
6. 在凭据索引中，选择次要。
7. 单击确定。
8. 转到 策略 **>** 身份验证 **> LDAP**，单击 **LDAP** 策略 选项卡，然后单击 编辑。
9. 使用以下表达式为 Citrix Endpoint Management 和 Citrix Virtual Apps and Desktops 使用单独的 NetScaler Gateway VIP。

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. 转到 策略 **>** 身份验证 **> RADIUS** ，然后单击 服务器 选项卡。
11. 单击 添加，输入 RADIUS 服务器详细信息，然后单击 创建。
12. 转到 策略，然后单击 添加。
13. 输入策略的 名称。从服务器下拉菜单中，选择您创建的 RADIUS 服务器名称。
14. 在表达式中，输入 **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver**，然后单击创建。
15. 选择虚拟服务器，然后单击 编辑。
16. 在 主身份验证下，单击 **LDAP** 策略。
17. 选择策略，单击 取消绑定，然后单击 关闭。

18. 在 身份验证 行上，单击 **+** 添加 RADIUS 身份验证。
19. 在 选择类型下，从 选择策略中选择 **RADIUS**。
20. 单击绑定。
21. 选择您之前创建的 RADIUS 身份验证策略，然后单击“插入”。
22. 单击确定。
23. 要将 LDAP 添加为辅助身份验证策略：在 身份验证 行上，单击 **+**。
24. 从 选择策略中，选择 **LDAP**。
25. 从 选择类型中，选择 辅助。
26. 从选 择策略中，选择 LDAP 策略。
27. 选择策略，然后单击 确定。
28. 单击绑定。
29. 单击 **Done**（完成）。
30. 验证您创建的策略是否具有最高优先级。这样可以确保即使为非移动用户添加了更多策略，它们也具有最高的优先级。有关详细信息，请参阅 设置身份验证策略的优

配置客户端证书或客户端证书和域身份验证

February 1, 2024

在使用 NetScaler 仅证书身份验证或证书加域身份验证时，可以使用适用于 Citrix Endpoint Management 的 NetScaler 执行 Citrix 端点管理所需的配置。您只能运行适用于 Citrix Endpoint Management 的 NetScaler 向导一次。有关使用向导的信息，请参阅 为 Citrix Endpoint Management 环境配置设置。

如果您已经使用过向导，请使用本文中的说明了解客户端证书身份验证或客户端证书加域身份验证所需的其他配置。

要确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证，请参阅本文后面的“NetScaler 证书吊销列表 (CRL)”。

使用 **GUI** 配置 **NetScaler Gateway** 以进行客户端证书身份验证

1. 导航到流量管理 **>** 负载平衡 **>** 虚拟服务器。
2. 选择 **SSL** 类型的虚拟服务器，然后在“**SSL** 参数”部分中将“启用会话重用”设置为已禁用。
3. 导航到 **NetScaler Gateway >** 虚拟服务器。
4. 选择 **SSL** 类型的虚拟服务器，然后单击 编辑。

5. 在 **SSL** 参数 部分中，单击编辑图标。
6. 选择 客户端身份验 证，在 客户端证书中，选择 强制
7. 创建身份验证证书策略，以便 Citrix Endpoint Management 可以从 Secure Hub 提供给 NetScaler Gateway 的客户端证书中提取用户主体名称 或 **sAMAccount**。
8. 导航到 **NetScaler Gateway >** 策略 **>** 身份验证 **> CERT**。
9. 单击 配置 式选项卡，然后单击 添加。
10. 为证书配置文件设置以下参数：

    身份验证类型：**CERT**

    双因素：**OFF** （仅用于证书身份验证）

    用户名字段：主题：**CN**

    组名称字段：**SubjectAltName:PrincipalName**
11. 在 NetScaler Gateway 虚拟服务器中，仅将证书身份验证策略绑定为 主身份验 证。
12. 绑定根 CA 证书以验证提供给 NetScaler Gateway 的客户端证书的信任度。

使用 **GUI** 为 **NetScaler Gateway** 配置客户端证书和域身份验证

1. 导航到流量管理 **>** 负载平衡 **>** 虚拟服务器。
2. 选择 **SSL** 类型的虚拟服务器，然后在“**SSL** 参数”部分中将“启用会话重用”设置为已禁用。
3. 转到 **NetScaler Gateway >** 策略 **>** 身份验证 **>** 证书。
4. 单击“配置文件”选项卡，单击“添加”。
5. 输入配置文件的 名称，将 双因素 设置为 开，然后从 用户名字段中选择 **SubjectAltNamePrincipalName**。
6. 单击 策略 选项卡，然后单击 添加。
7. 输入策略的 名称，从 服务器 中选择证书配置文件，设置表 达式，然后单击 创建。
8. 转到 虚拟服务器，选择 **SSL** 类型的虚拟服务器，然后单击 编辑。
9. 在 身份验证旁边，单击 **+** 添加证书身份验证。
10. 要选择身份验证方法，请在选择策略中选择证书，然后在选择类型中选择主要。这会将证书身份验证绑定为主身份验证，其优先级与 LDAP 身份验证类型相同。
11. 在 策略绑定下，单击 单击以选择 以选择之前创建的证书策略。
12. 选择之前创建的证书策略，然后单击 确定。
13. 将 优先级 设置为 **100** ，然后单击 绑定。在后续步骤中配置 LDAP 身份验证策略时，请使用相同的优先级编号。
14. 在 **LDAP** 策略所在行中，单击 **。

15. 选择策略，然后从 编辑 下拉菜单中单击 编辑绑定。
16. 输入与为证书策略指定的相同 优先级 值。单击绑定。
17. 单击关闭。
18. 单击 **SSL** 参数部分中的编辑图标。
19. 选中“客户端身份验证”复选框，在“客户端证书”中选择“强制”，然后单击“确定”。
20. 单击 **Done**（完成）。

NetScaler 证书吊销列表 **(CRL)**

Citrix Endpoint Management 仅支持第三方证书颁发机构的证书吊销列表 (CRL)。如果您配置了 Microsoft CA，Citrix Endpoint Management 将使用 NetScaler 来管理吊销。配置基于客户端证书的身份验证时，请考虑是否需要配置 NetScaler 证书吊销列表 (CRL) 设置 **Enable CRL Auto Refresh**（启用 CRL 自动刷新）。此步骤可确保处于仅 MAM 模式的设备的用户无法使用设备上的现有证书进行身份验证。Citrix Endpoint Management 会重新颁发新证书，因为它不会限制用户在吊销用户证书时生成用户证书。此设置提高了 CRL 检查过期的 PKI 实体时 PKI 实体的安全性。

Microsoft Intune 集成

February 1, 2024

Microsoft Intune 与 NetScaler Gateway 的集成提供了 NetScaler Gateway 和 Intune 提供的一流的应用程序访问和数据保护解决方案。

您将获得最完整的安全生产力应用程序套件，包括电子邮件、日历、联系人、笔记、文档编辑和远程访问，所有这些都可以跨不同平台进行集中管理。Intune 和 NetScaler Gateway 集成提供世界一流的移动设备管理 (MDM) 功能，而 Citrix Secure Access 客户端技术使这些 Intune 开明的应用程序能够通过 NetScaler Gateway 安全地访问企业数据和应用程序。

该集成允许 NetScaler Gateway 从 Intune 中提取合规性数据，从而启用条件访问策略。条件访问策略使 NetScaler Gateway 能够更好地控制基于设备功能等的访问规范。例如，管理员可以创建一个策略，其中仅向禁用了“摄像头”的设备授予访问权限。

配置 NetScaler Gateway 虚拟服务器后，NetScaler Gateway 支持 Azure Active Directory 库 (ADAL) 令牌身份验证。配置后，使用 Citrix 仅限网络的包装程序或 SDK 打包的移动应用程序通过使用 ADAL 令牌访问 NetScaler Gateway，该应用程序可以直接从 AAD 获取该令牌。

Citrix Micro VPN 与 Microsoft Endpoint Manager 集成

NetScaler Gateway 客户可以将 Micro VPN 与 Microsoft Endpoint Manager (Intune) 结合使用。Citrix Micro VPN 与 Microsoft Endpoint Management 集成使您的应用程序能够访问本地资源。

Citrix Micro VPN 技术提供了按需 VPN，可降低数据传输成本并简化安全性，因为 VPN 通道并不总是处于活动状态。相反，它仅在需要时处于活动状态，从而降低了风险并优化了设备的性能，从而获得更好的用户体验。这也有助于延长移动电池寿命。NetScaler 的 micro VPN 技术为移动用户提供了对内部业务资源的安全访问，同时为他们提供最佳的用户体验。

Micro VPN 仅在以下用例中受支持：

- 仅限 Intune 移动应用程序管理 (MAM)
- Intune 移动设备管理 (MDM) 和移动应用程序管理 (MAM)

> 重要提示：
>
> 对于 SSL VPN 功能，micro VPN 需要 NetScaler Gateway Advanced 或 Premium Edition （VPX 3000 或更高版本）以及 Citrix Endpoint Management 权限。Citrix Endpoint Management 授权可确保在 Microsoft Edge 移动浏览器（iOS 和 Android）上持续支持 micro VPN SDK。有关详细信息，请联系您的销售、客户或合作伙伴代表。

有关设置 Citrix Micro VPN 与 Microsoft Endpoint Manager 的集成的详细信息，请参阅设置 NetScaler Gateway 以便在 Microsoft Endpoint Manager 中使用 Micro VPN。

何时使用集成的 Intune MDM 解决方案

February 1, 2024

以下场景说明了集成的 Intune MDM 解决方案的使用：

- 一位新客户决定使用本地 NetScaler Gateway 部署来加入 Intune
- 现有 NetScaler Gateway 用户想要使用 Intune 添加移动设备管理功能
- 现有 Intune 用户希望允许移动设备或应用程序使用公司 DMZ 中的 NetScaler Gateway 物理或虚拟设备访问位于公司网络内部的数据

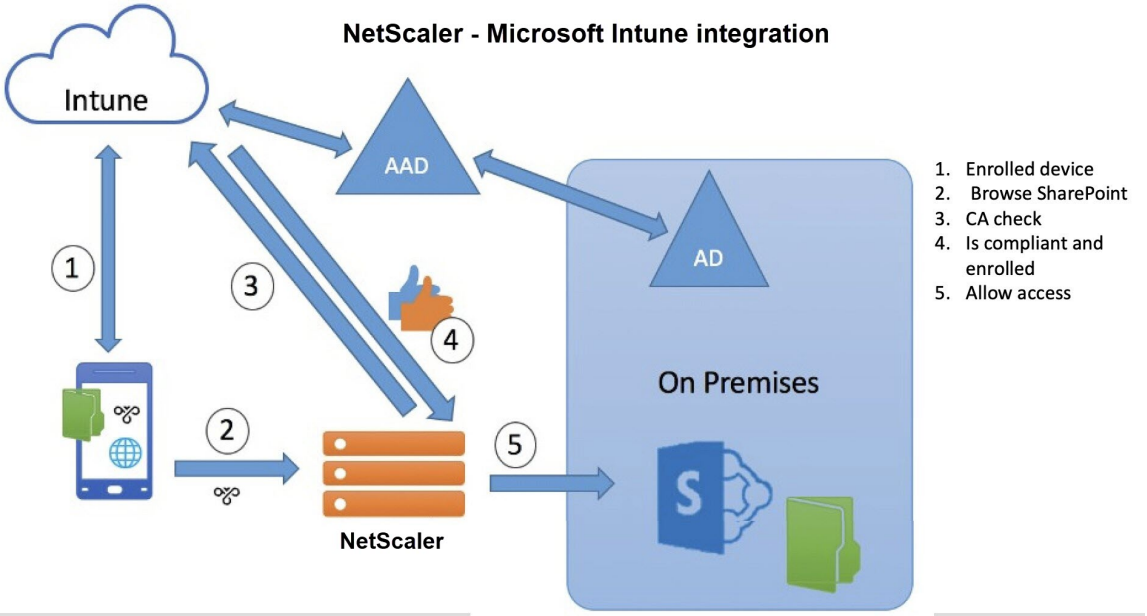
> 注意
>
> 仅支持 iOS 和 Android 客户端。

了解 NetScaler Gateway MDM 与 Intune 的集成

February 1, 2024

以下是典型的 NetScaler Gateway MDM 与 Intune 集成中的事件流示例：

1. 使用 Intune 注册移动设备。
2. 企业批准的应用程序和设备策略将推送到设备。
3. 从设备浏览 SharePoint（本地应用程序）。
4. 浏览器请求将发送到 NetScaler Gateway。
5. NetScaler Gateway 设备会向 Intune 检查设备的注册状态。
6. 如果成功注册了合规设备，则会授予 SharePoint 访问权限。



当设备不符合条件访问策略时，NetScaler Gateway VPN 客户端会显示一条错误消息。该消息提供了从设备到 Intune 托管的页面的链接，使用户可以选择注册或修复设备的合规性状态。

> 注意：
>
> 管理员在将证书推送到 Intune 时必须确保以下几点，以便用户可以区分其设备上的各种证书。

- 证书必须有主题摘要。
- 不同证书的主题摘要必须是不同的。

Intune NAC v2 API 支持

作为 Intune NAC v2 API 支持的一部分，您必须绑定证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为 CA 证书的一部分进行发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果有中间证书，这些证书也必须绑定到这里。

有关更多详细信息，请参阅 Intune NAC v2 API 支持

为 **NetScaler Gateway** 虚拟服务器配置网络访问控制设备检查以进行单因素登录

February 1, 2024

本主题提供有关将 NetScaler Gateway 配置为使用 Microsoft Intune 提供的网络访问合规性 (NAC) 安全性从移动设备（iOS 和 Android）连接到内部网络的信息。当用户尝试从 iOS 或 Android VPN 客户端连接到 NetScaler Gateway 时，网关首先向 Intune 服务检查设备是否为受管设备和合规设备。

- 托管：使用 Intune 公司门户客户端注册设备。
- 合规：应用从 Intune MDM 服务器推送的必需策略。

只有当设备既受管又符合要求时，才会建立 VPN 会话，并向用户提供对内部资源的访问权限。

> 注意：
>
> - 在此设置中，后端的 NetScaler Gateway 会与 Intune 服务进行对话。SSL 配置文件处理到 NetScaler Gateway 的传入连接。NetScaler Gateway 后端通信可处理后端云服务 (Intune) 的任何 SNI 要求。
> - NetScaler Gateway 版本 13.0 版本 64.x 及更高版本支持适用于 DTLS 网关虚拟服务器的 SNI。
> - 仅当 Intune 管理门户（现在称为 Microsoft Endpoint Manager）配置 VPN 配置文件时，才支持针对 PerApp VPN 甚至是设备范围的 VPN 的 Intune NAC 检查。最终用户添加的 VPN 配置文件不支持这些功能。最终用户设备必须由其 Intune 管理员从 Microsoft Endpoint Manager 将 VPN 配置文件部署到其设备，才能使用 NAC 检查。

许可

此功能需要 Citrix 企业版许可证。

系统要求

- NetScaler Gateway 版本 11.1 版本 51.21 或更高版本
- iOS VPN —10.6 或更高版本
- Android VPN —2.0.13 或更高版本
- Microsoft
  - Azure AD 访问权限（具有租户和管理员权限）
  - 启用 Intune 的租户

- 防火墙
  为从子网 IP 地址到 `https://login.microsoftonline.com` 和 `https://graph.windows.net`（端口 53 和端口 443）的所有 DNS 和 SSL 流量启用防火墙规则

必备条件

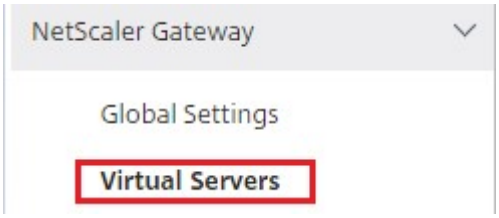
- 所有现有的身份验证策略必须从经典策略转换为高级策略。有关如何从传统策略转换为高级策略的信息，请参阅 https://support.citrix.com/article/CTX131024。
- 在 Azure 门户上创建 NetScaler Gateway 应用程序。有关详细信息，请参阅在 Azure 门户上配置 NetScaler Gateway 应用程序。
- 在使用以下应用程序特定信息创建的 NetScaler Gateway 应用程序上配置 OAuth 策略。
  - 客户端 ID/应用程序 ID
  - 客户端密/应用程序密钥
  - Azure 租户 ID

引用

- 本文档捕获 NetScaler Gateway 的设置配置。大多数 Citrix SSO 客户端 (iOS/Android) 配置都是在 Intune 端完成的。有关适用于 NAC 的 Intune VPN 配置的详细信息，请参阅 https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate。
- 要为 iOS 应用程序配置 VPN 配置文件，请参阅 https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios。
- 要在 Azure 门户上设置 NetScaler Gateway 应用程序，请参阅在 Azure 门户 上配置 NetScaler Gateway 应用程序。

使用 **nFactor** 添加 **NetScaler Gateway** 虚拟服务器以进行网关部署

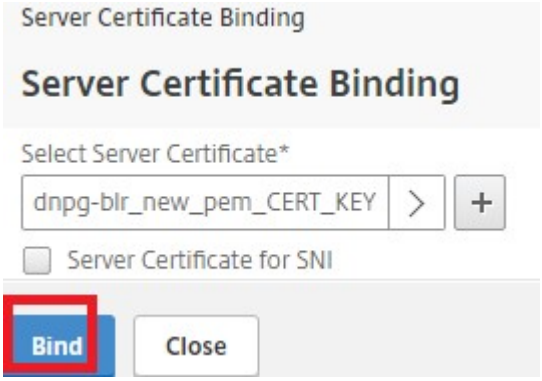
1. 导航到 **NetScaler Gateway >** 虚拟服务器。



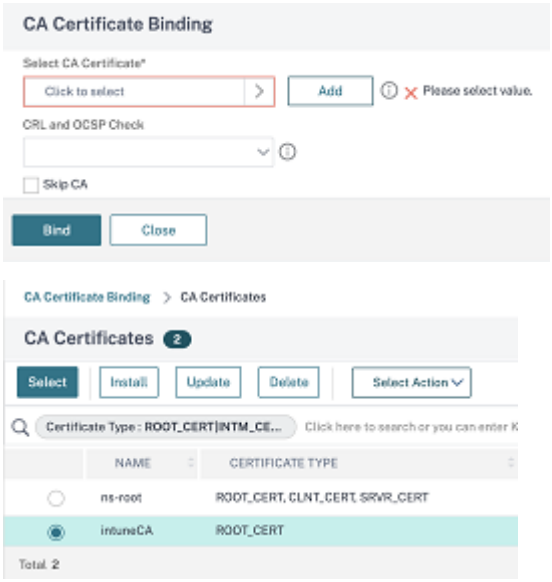
2. 单击添加。
3. 在“基本设置”区域中提供所需信息，然后单击“确定”。

4. 选择 服务器证书。

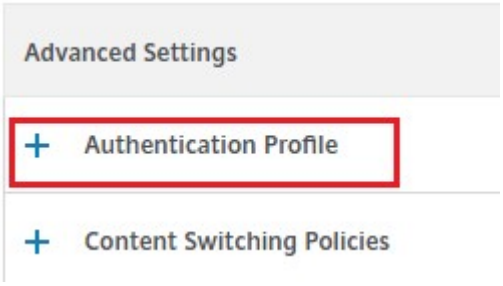
5. 选择所需的服务器证书并单击 绑定。



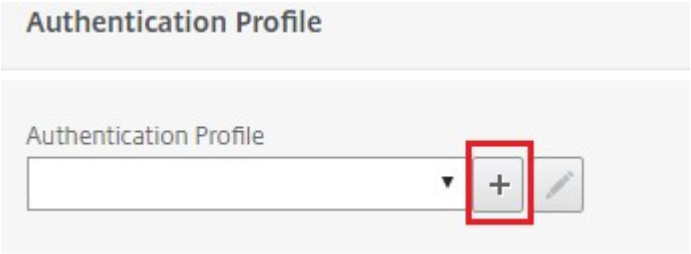
6. 作为 Intune NAC v2 API 支持的一部分，您必须绑定证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为客户端证书的一部分发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果有中间证书，这些证书也必须绑定到这里。有关 Intune 配置的更多信息，请参阅在 Azure 门户上配置 NetScaler Gateway 应用程序。要获得 Intune NAC v2 API 支持，请选择所需的 CA 证书，然后单击 绑定。



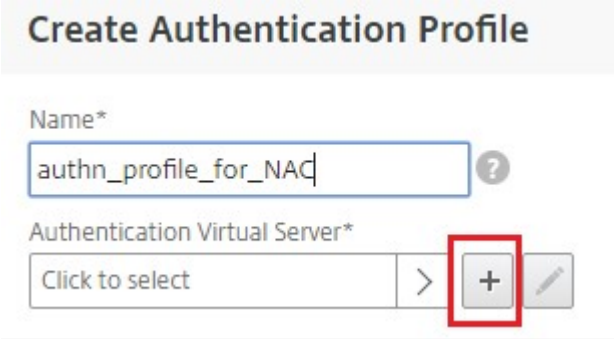
7. 单击继续。
8. 单击继续。
9. 单击继续。
10. 单击“策略”旁边的加号图标 **[+]**，然后从“选择 策略”列表中 选择“会话”，然后从“选择 类型”列表中选择“请求”，然后单击“继续”。
11. 单击“选择策略”旁边的加号图标 **[+]**。
12. 在 创建 **NetScaler Gateway** 会话策略 页面上，提供会话策略的名称。
13. 单击 配置文件 旁边的加号图标 [+]，然后在 创建 **NetScaler Gateway** 会话配置文件 页面上，提供会话配置文件的名称。
14. 在“客户端体验”选项卡上，单击“无客户端访问”旁边的复选框，然后从列表中选择“关闭”。
15. 单击 插件类型 旁边的复选框，然后从列表中选择 Windows/Mac OS X。
16. 单击 高级设置，然后选中 客户端选择旁边的复选 框，然后将其值设置为 开。
17. 在“安 全”选项卡上，单击“默认授权操作”旁边的复选框，然后从列表中选择“允许”。
18. 在“已发布的应用程序”选项卡上，单击 **ICA Proxy** 旁边的复选框，然后从列表中选择 关闭。
19. 单击“创建”。
20. 在 创建 **NetScaler Gateway** 会话策略 页面的“表达式”区域中，配置符合条件的表达式。
21. 单击创建。
22. 单击绑定。
23. 在 高级设置中选择验证配置文件。



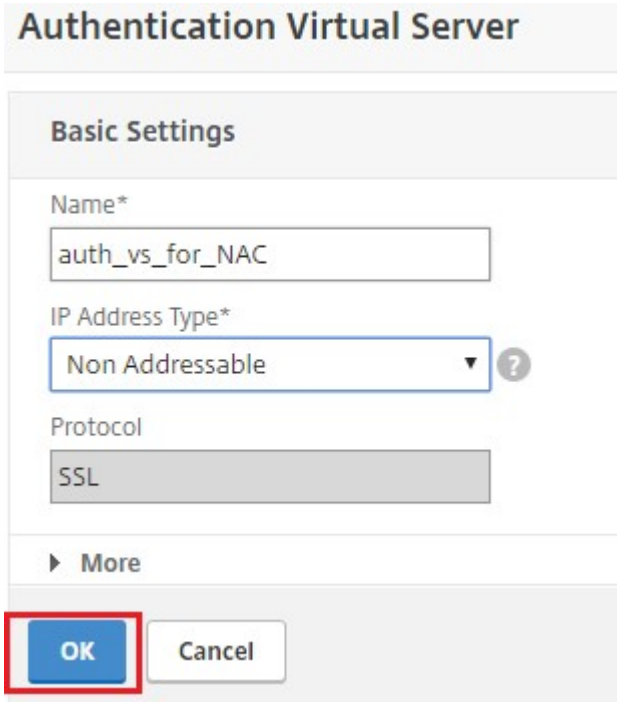
24. 单击加号图标 **[+]** 并提供身份验证配置文件的名称。



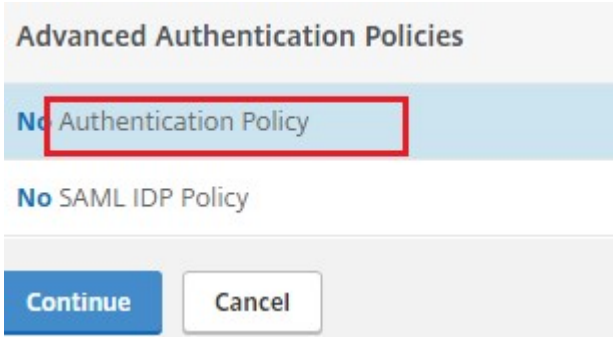
25. 单击加号图标 **[+]** 可创建身份验证虚拟服务器。



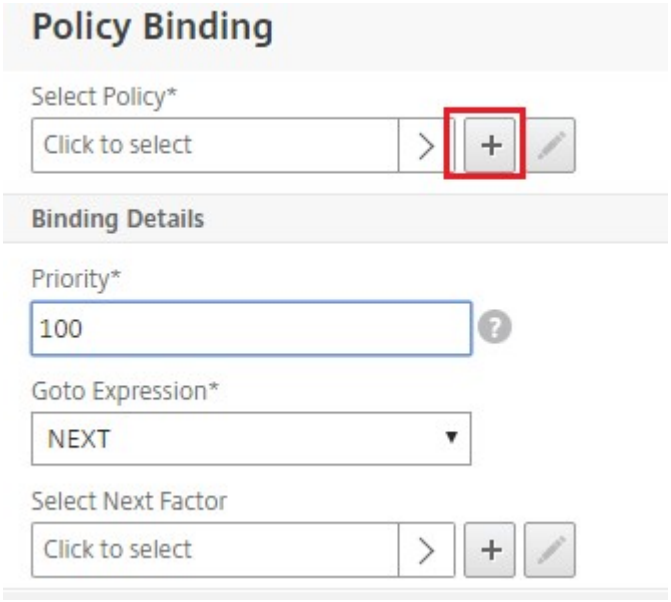
26. 在 基本设置 区域下指定身份验证虚拟服务器的名称和 IP 地址类型，然后单 击确定 IP 地址类型也可以是“不可寻址”。



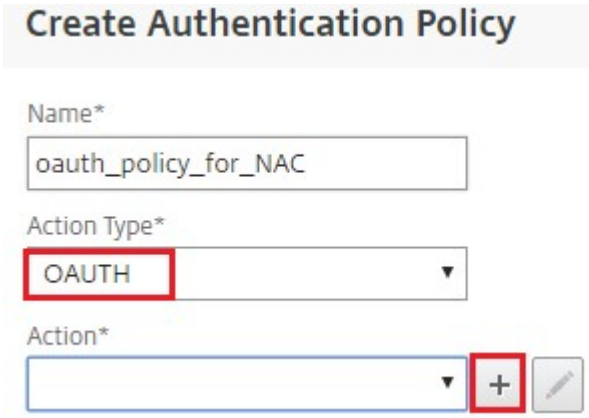
27. 单击 身份验证策略。



28. 在“策略绑定”视图下，单击加号图标 **[+]** 以创建身份验证策略。



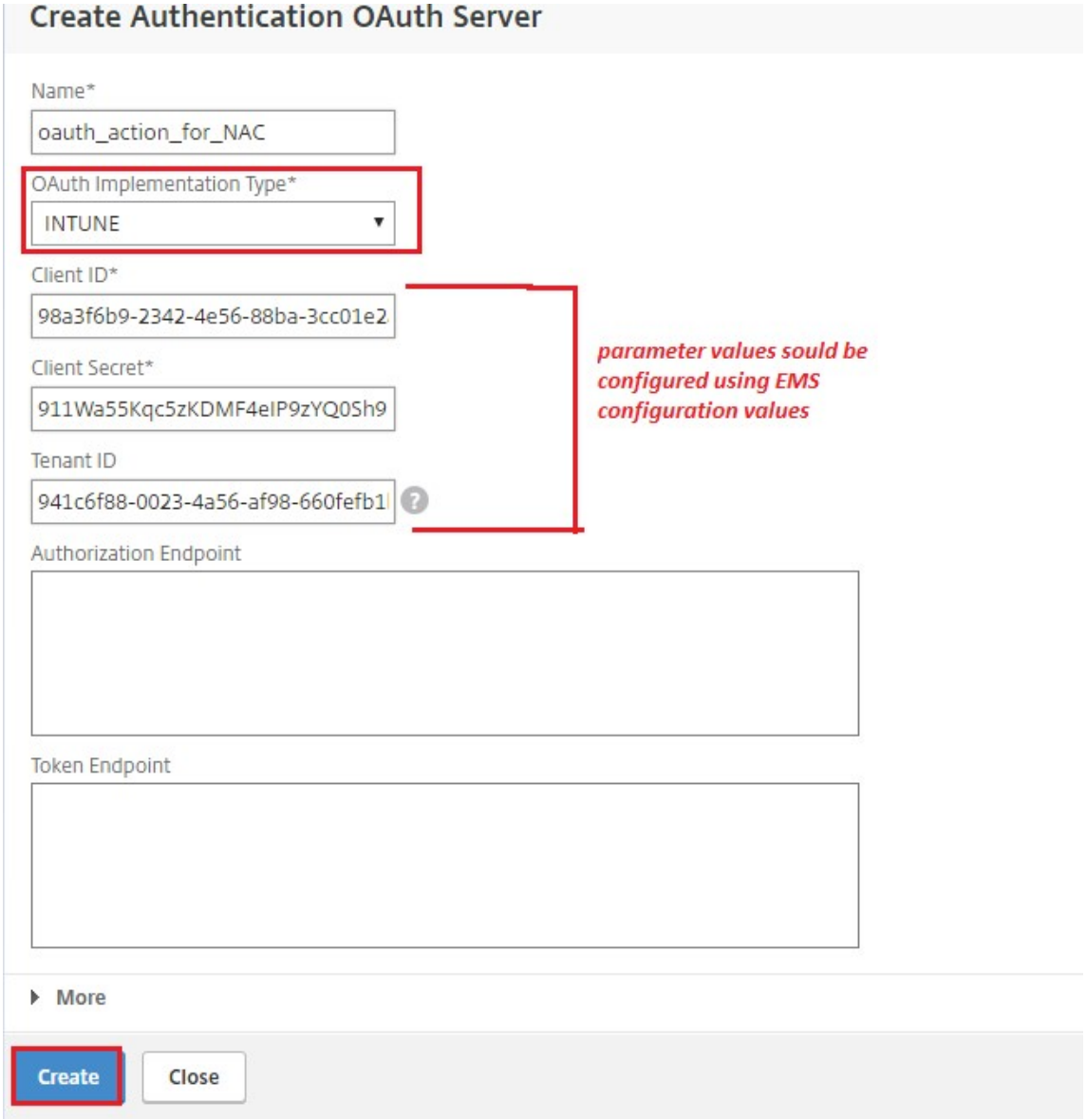
29. 选择 **OAUTH** 作为 操作类型，然后单击加号图标 **[+]** 为 NAC 创建 OAuth 操作。



30. 使用客户端 **ID**、客户端密钥 和 租户 **ID** 创建 OAuth 操作。

> 注意：
>
> - 客户端 **ID**、客户端密钥 和 租户 **ID** 是在 Azure 门户上配置 NetScaler Gateway 应用程序后生成的。
> - 记下客户端 ID/ 应用程序 ID、客户端密钥/应用程序密钥和 Azure 租户 ID 信息，以便稍后在 NetScaler Gateway 上创建 OAuth 操作时需要这些信息。

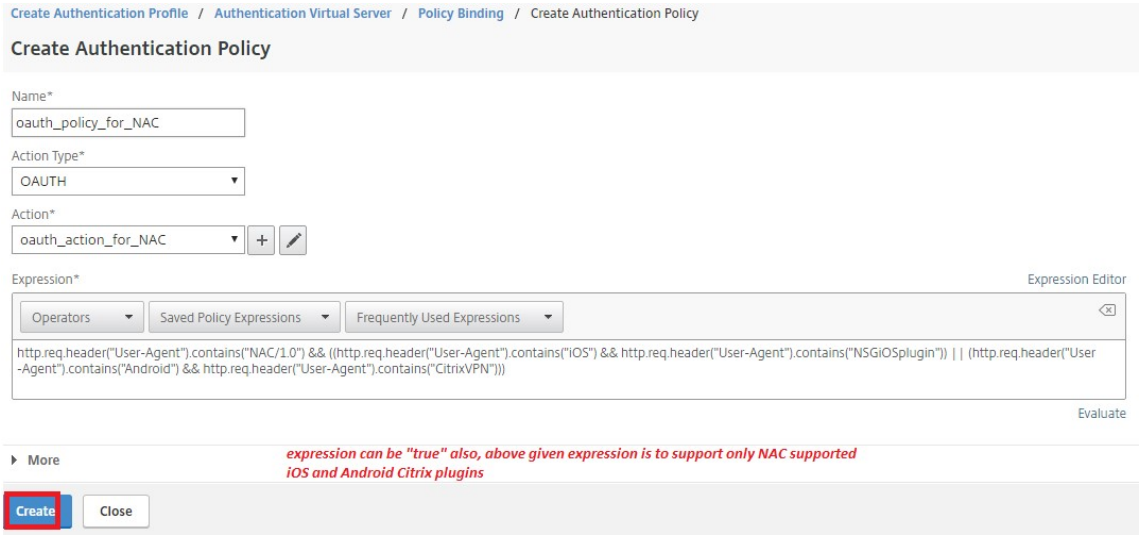
确保在设备上配置了适当的 DNS 名称服务器以进行解析并访问;
`https://login.microsoftonline.com/`,
-
- `https://graph.windows.net/`,- *.manage.microsoft.com。



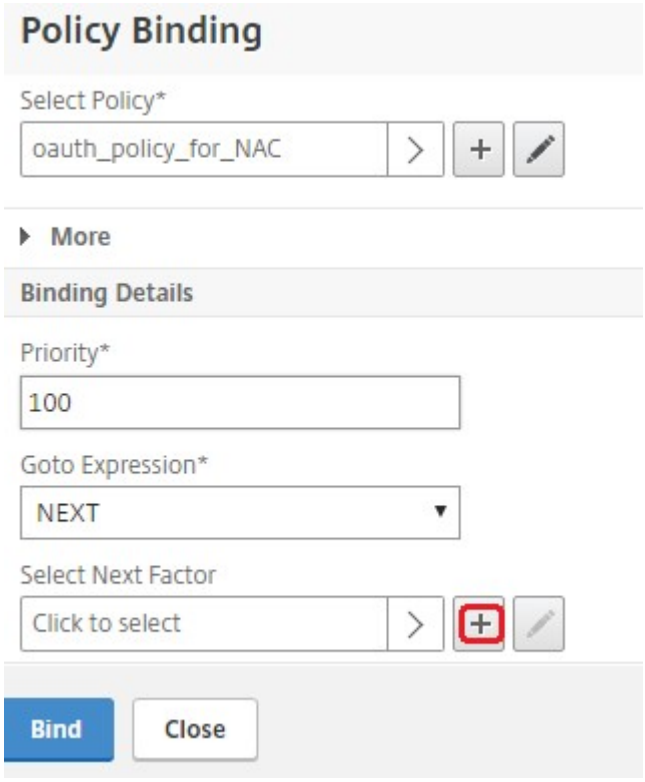
31. 为 **OAuth** 操作创建身份验证策略。

    规则：

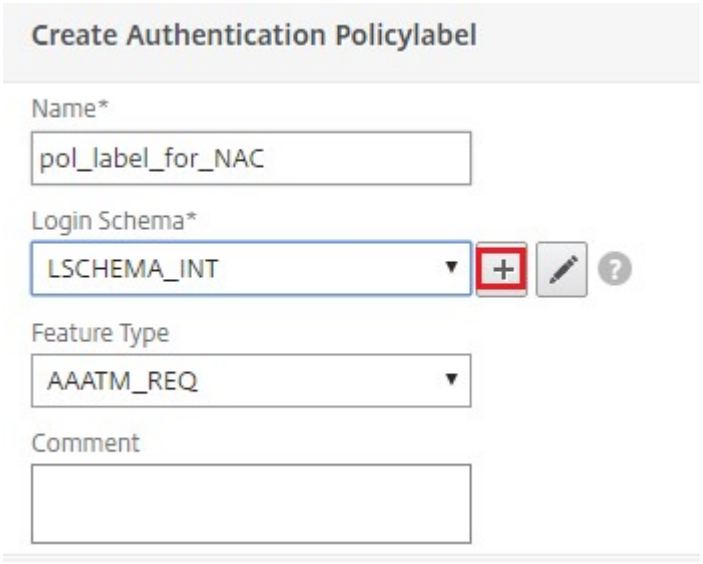
```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") && http.req.header("User-
    Agent").contains("NSGiOSplugin")) || (http.req.header("User-
    Agent").contains("Android") && http.req.header("User-Agent").
    contains("CitrixVPN")))
<!--NeedCopy-->
```

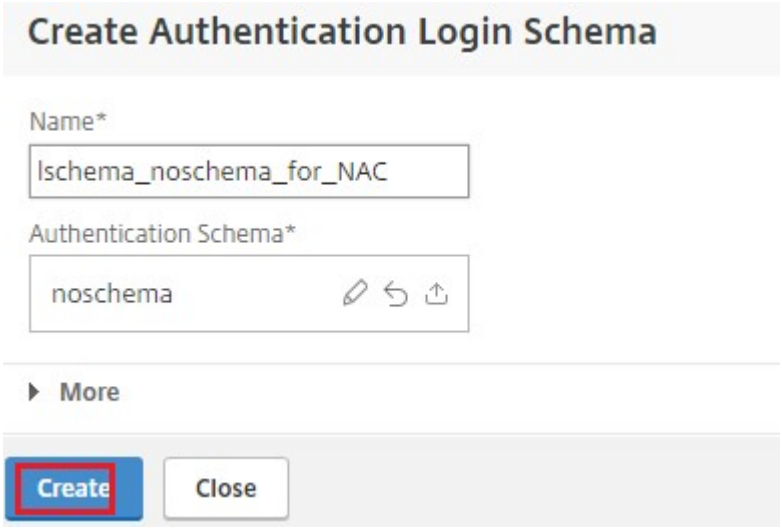
32. 单击加号图标 **[+]** 可创建 nextFactor 策略标签。



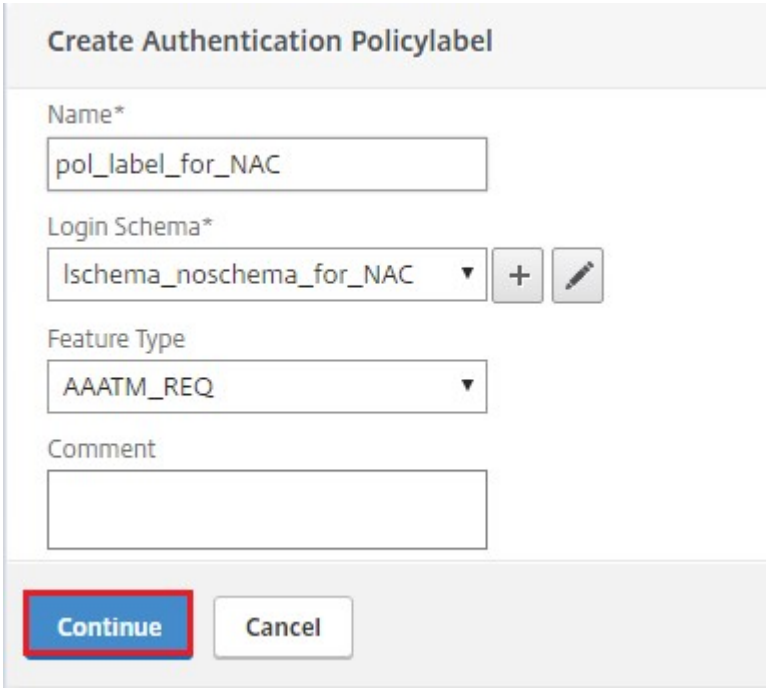
33. 单击加号图标 **[+]** 可创建登录架构。



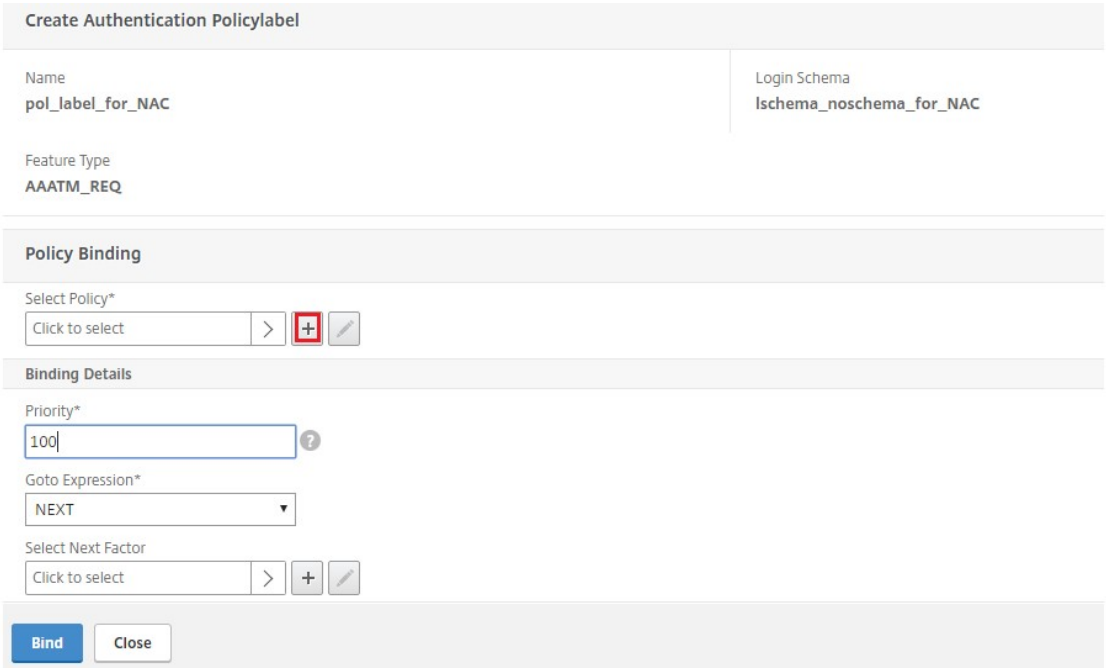
34. 选择 **noschema** 作为身份验证架构，然后单击 创建。



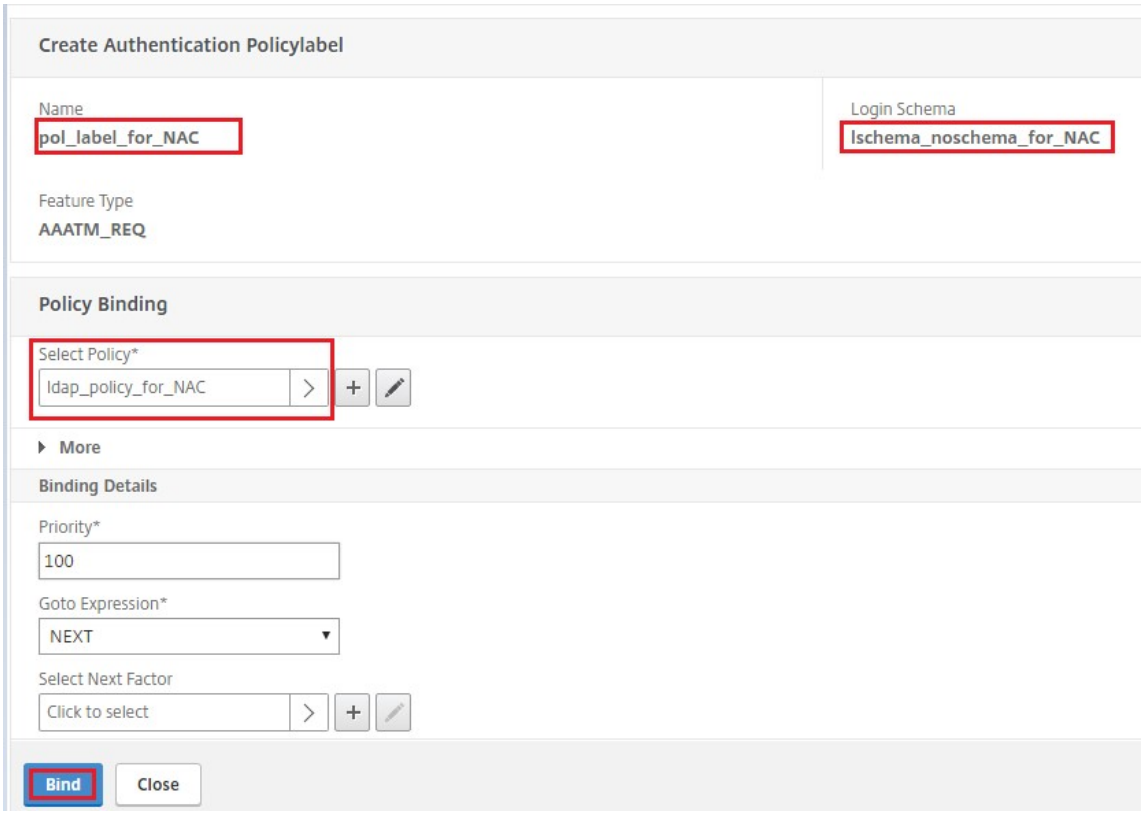
35. 选择创建的登录架构后，单击 继续。



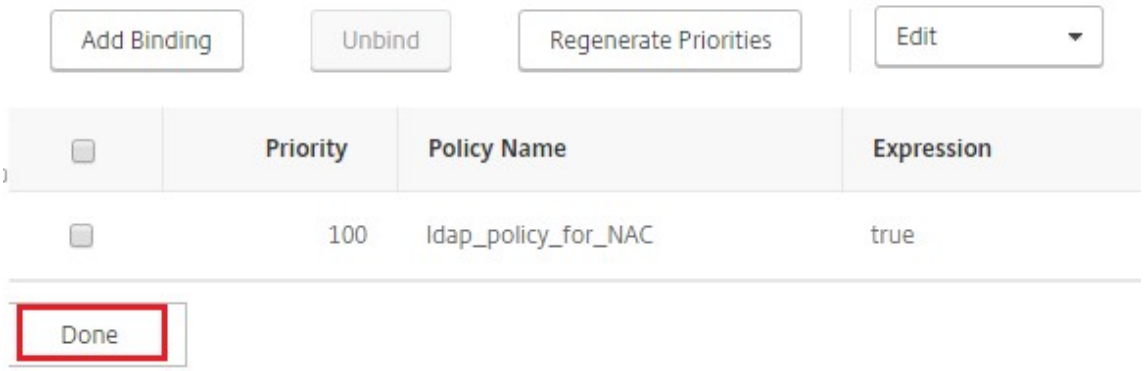
36. 在 选择策略中，选择用于用户登录的现有身份验证策略，或单击加号图标 + 创建身份验证策略。
有关创建验证策略的详细信息，请参阅 配置高级身份验证策 略和 配置 LDAP 身份验证。



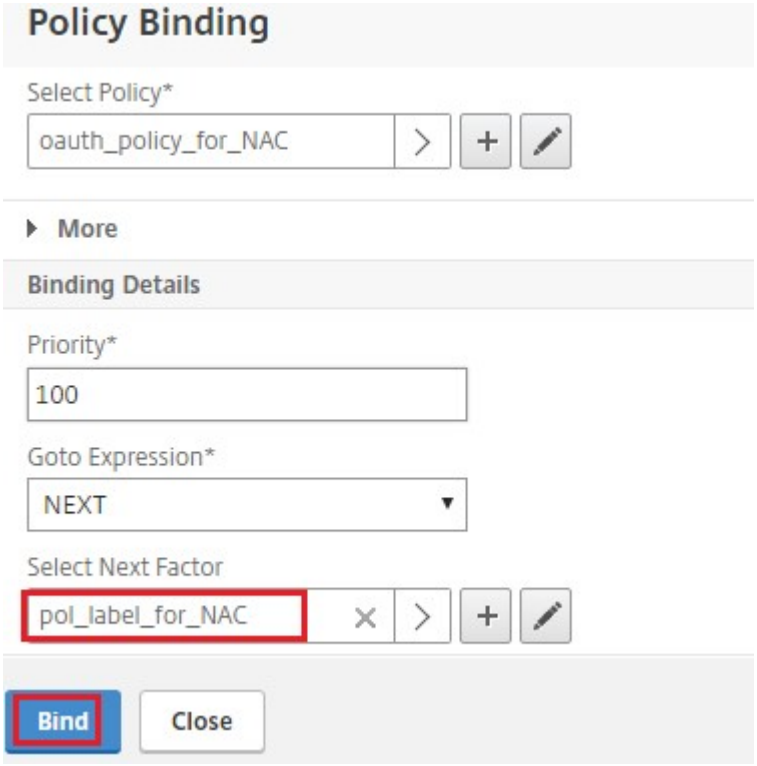
37. 单击绑定。



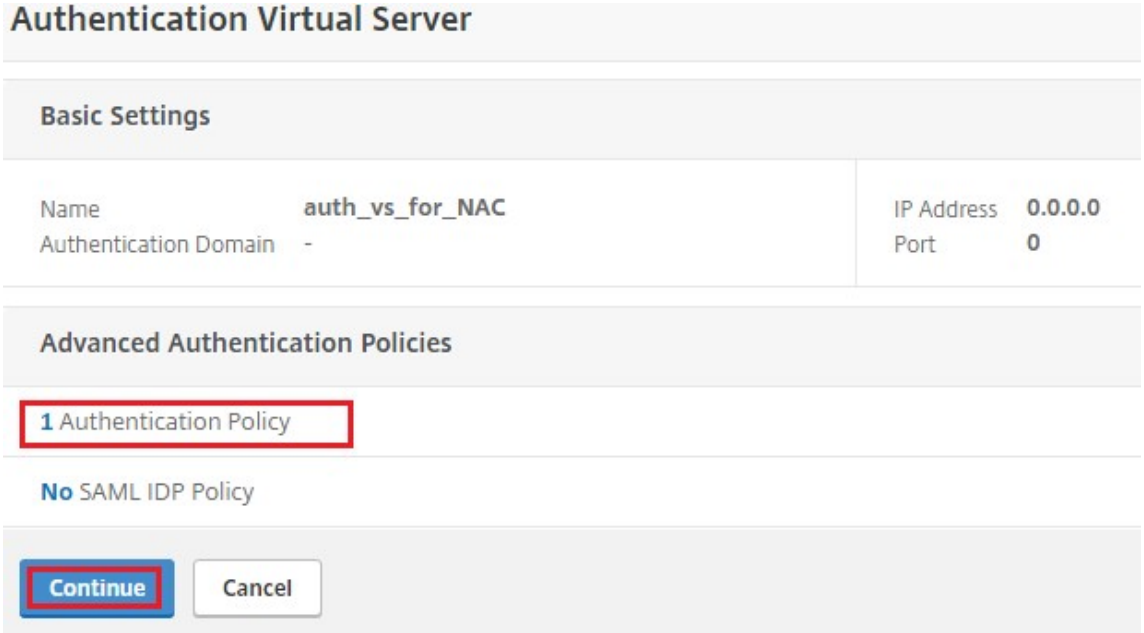
38. 单击 **Done**（完成）。



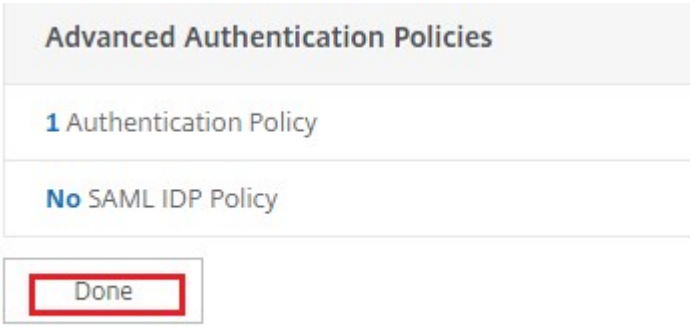
39. 单击绑定。



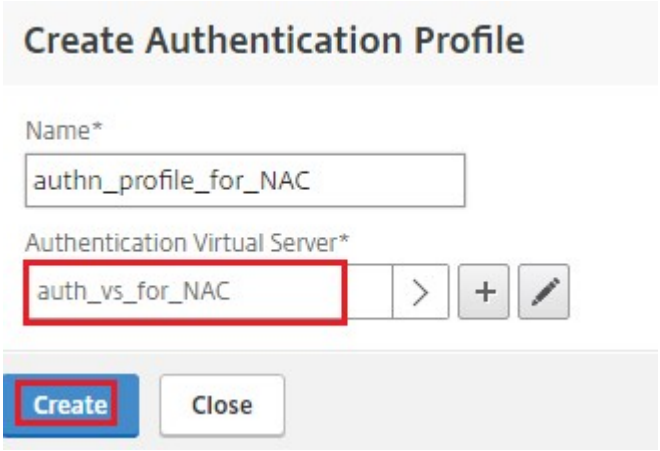
40. 单击继续。



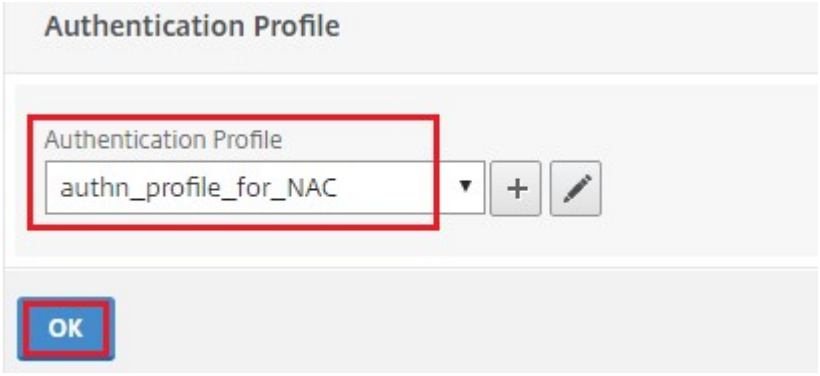
41. 单击 **Done**（完成）。



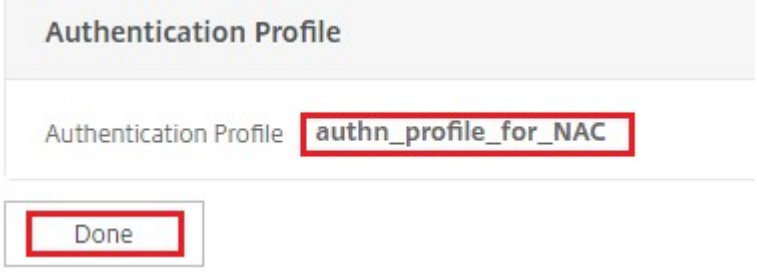
42. 单击创建。



43. 单击确定。



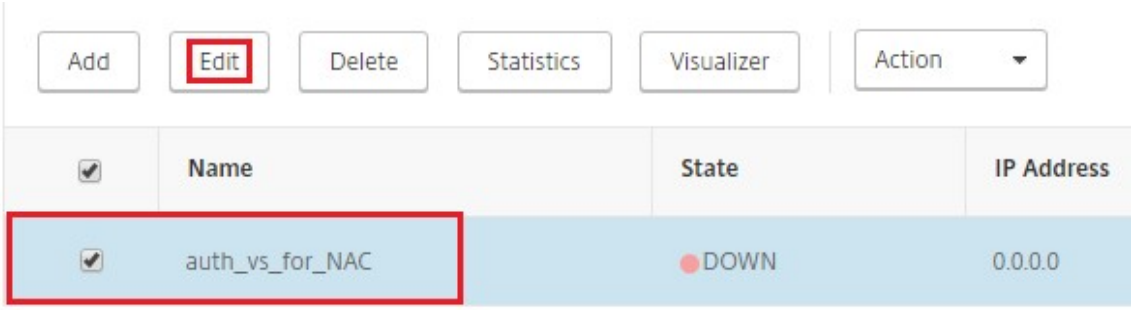
44. 单击 **Done**（完成）。



将身份验证登录架构绑定到身份验证虚拟服务器以指示 **VPN** 插件作为 **/cgi/login** 请求的一部分发送设备 **ID**

1. 导航到安全 > **AAA -** 应用程序流量 > 虚拟服务器。

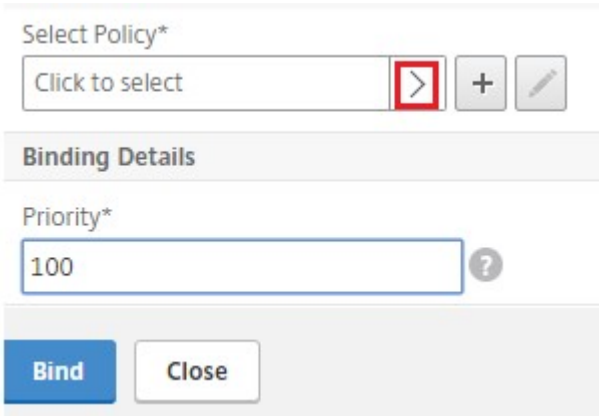
2. 选择之前选择的虚拟服务器，然后单击 编辑。



3. 单击 高级设置下的登录架构。

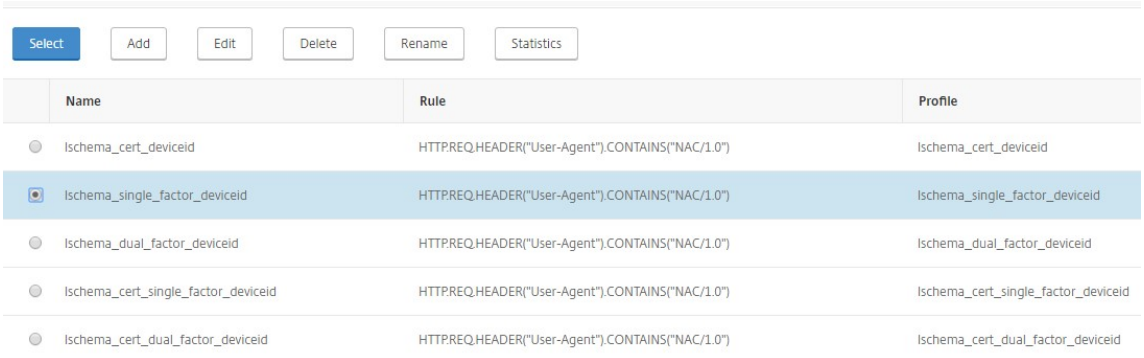
4. 单击 登录架构进 行绑定。

5. 单击 **[>]** 在登录架构策略中选择并绑定现有内部版本以进行 NAC 设备检查。

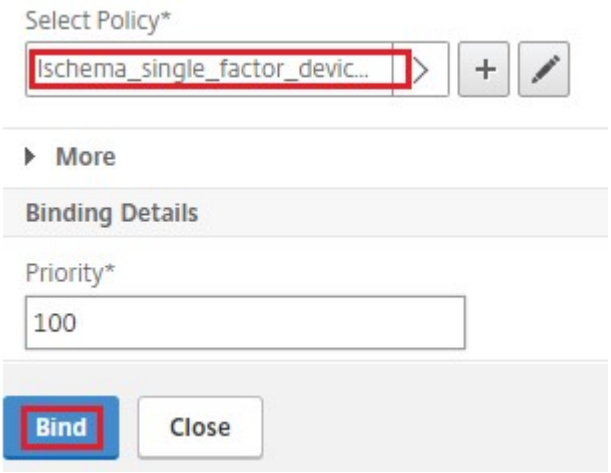


6. 选择适合您的身份验证部署的所需登录架构策略，然后单击 选择。

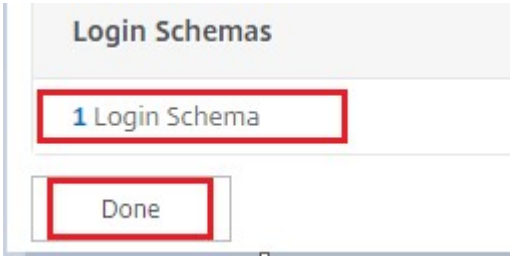
   在前面介绍的部署中，将使用单因素身份验证 (LDAP) 和 NAC OAuth 操作策略。因此选择了 **lschema_single_factor_deviceid** 。



7. 单击绑定。



8. 单击 **Done**（完成）。



Intune NAC v2 API 支持

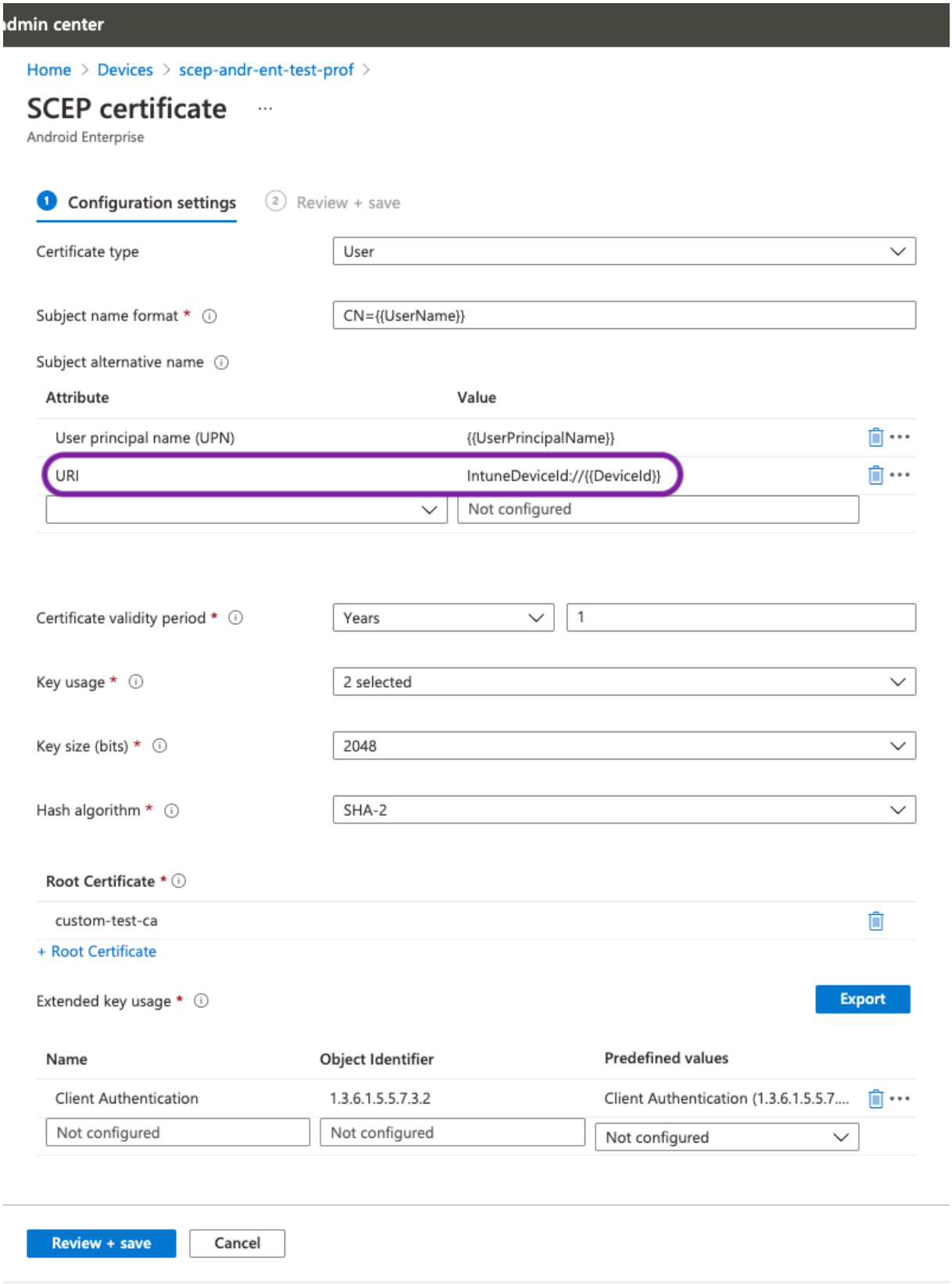
作为 Intune NAC v2 API 支持的一部分，您必须绑定证书颁发机构文件（CA 证书），以确保 NetScaler 设备从移动设备获取有效证书。在 Intune NAC v2 中，移动设备将设备 ID 作为 CA 证书的一部分进行发送。此处绑定的 CA 证书必须是用于向最终用户 iOS 和 Android 设备颁发客户端证书的证书。如果有中间证书，这些证书也必须绑定到这里。

您可以使用以下示例命令绑定您的 CA 证书。

```
1 bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -
     ocspCheck Optional
2 <!--NeedCopy-->
```

重要提示：

- Intune NAC v2 API 支持在 NetScaler Gateway 13.1 版本 12.50 或更高版本和 13.0 版本 84.11 或更高版本中提供。
- 必须通过在 VPN 和身份验证虚拟服务器上将 `clientAuth` 设置为 ENABLED，将 `clientCert` 设置为 OPTIONAL 以启用基于客户端证书的身份验证。`clientCert` 参数设置为 OPTIONAL，以便不需要 Intune NAC 检查的其他端点可以在不提供客户端证书的情况下通过同一虚拟服务器进行身份验证。Android 和 iOS 设备必须提供客户端证书。否则 Intune NAC 检查将失败。
- 您必须确保在移动设备上通过 Intune 置备的客户端证书必须在 URI 类型的 SAN 字段中具有 Intune 设备 ID，如用于网络访问控制的新 Microsoft Intune 服务文档中所述。有关详细信息，请参阅 https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696。
  URI 值字段的格式必须与下图所示的格式相同。此外，Citrix SSO 应用程序必须使用相同的证书对网关进行身份验证。



故障排除

常规问题

问题	解决方案
打开应用程序时，将显示“需要添加策略”消息	在 Microsoft Graph API 中添加策略
存在策略冲突	每个应用程序只允许使用一个策略
您的应用无法连接到内部资源	确保打开了正确的防火墙端口、使用了正确的租户 ID 等等

NetScaler Gateway 问题

问题	解决方案
为 Azure 上的网关应用程序配置所需的权限不可用。	检查是否有适当的 Intune 许可证可用。尝试使用 manage.windowsazure.com 门户来查看是否可以添加权限。如果问题仍然存在，请与 Microsoft 支持部门联系。
NetScaler Gateway 无法访问 `login.microsoftonline.comandgraph.windows.net`。	从 NS Shell，检查您是否能够访问以下 Microsoft 网站：cURL -v -k https://login.microsoftonline.com。然后，检查是否在 NetScaler Gateway 上配置了 DNS。还要检查防火墙设置是否正确（如果 DNS 请求被防火墙处理）。
配置 OAuthAction 后，ns.log 中会出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否设置了适当的权限。
`Sh OAuthAction` 命令不会将 OAuth 状态显示为已完成。	检查 Azure Gateway 应用程序的 DNS 设置和配置权限。
Android 或 iOS 设备不显示双重身份验证提示。	检查双重设备 ID 登录架构是否绑定到身份验证虚拟服务器。

NetScaler Gateway OAuth 状态和错误情况

状态	错误情况
AADFORGRAPH	密钥无效、URL 未解析、连接超时
MDMINFO	`*manage.microsoft.com`已关闭或无法访问

状态	错误情况
GRAPH	图形端点已关闭，无法访问
CERTFETCH	由于 DNS 错误，无法与“令牌端点：https://login.microsoftonline.com”对话。要验证此配置，请转到 Shell 提示符并键入 cURL https://login.microsoftonline.com。此命令必须验证。

注意：当 OAuth 状态成功时，状态将显示为“完成”。

Intune 配置检查

确保在 **Citrix SSO >** 启用网络访问控制 **(NAC)** 的基础 **iOS VPN** 配置 中选中 我同意复选框。否则，NAC 检查不起作用。

在 **Azure** 门户上配置 **NetScaler Gateway** 应用程序

February 1, 2024

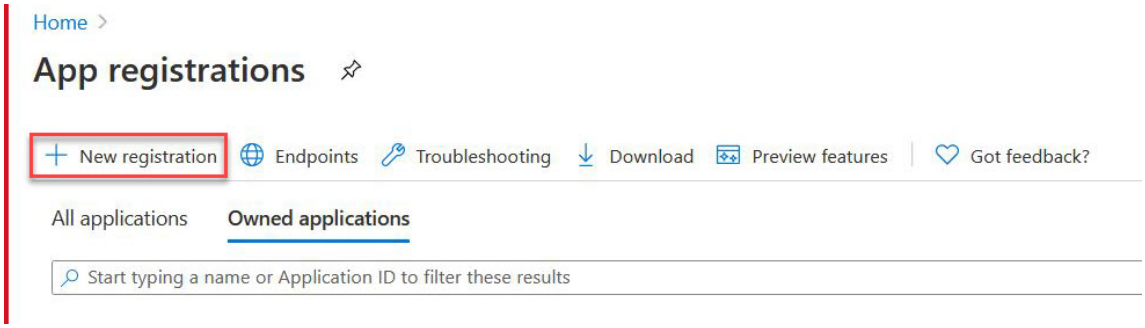
以下部分列出了在 Azure 门户上配置 NetScaler Gateway 应用程序的步骤。

必备条件

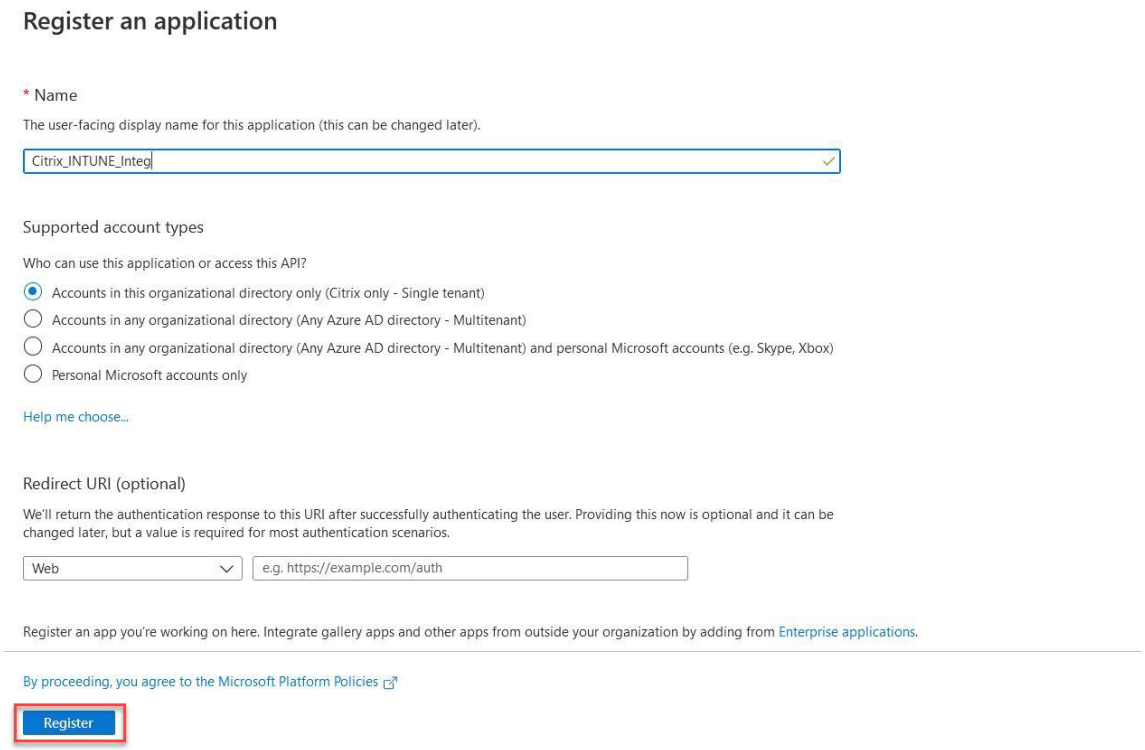
- Azure 全局管理员凭据
- Intune 许可已启用
- 对于 Intune 集成，您必须在 Azure 门户上创建 NetScaler Gateway 应用程序。
- 创建 NetScaler Gateway 应用程序后，使用以下应用程序特定信息在 NetScaler Gateway 上配置 OAuth 策略：
  - 客户端 ID/应用程序 ID
  - 客户端密/应用程序密钥
  - Azure 租户 ID
- NetScaler Gateway 使用应用程序客户端 ID 和客户端密钥与 Azure 进行通信并检查 NAC 合规性。

在 **Azure** 上创建 **NetScaler Gateway** 应用程序

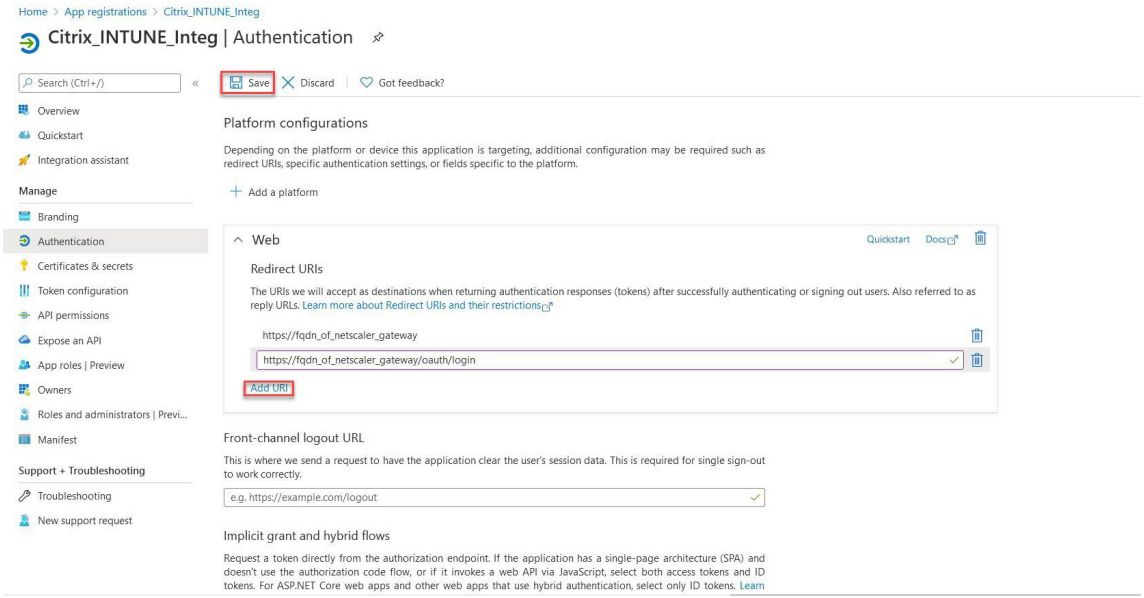
1. 登录到 portal.azure.com
2. 单击 **Azure Active Directory**。
3. 单击 应用注册，然后单击 新注册。



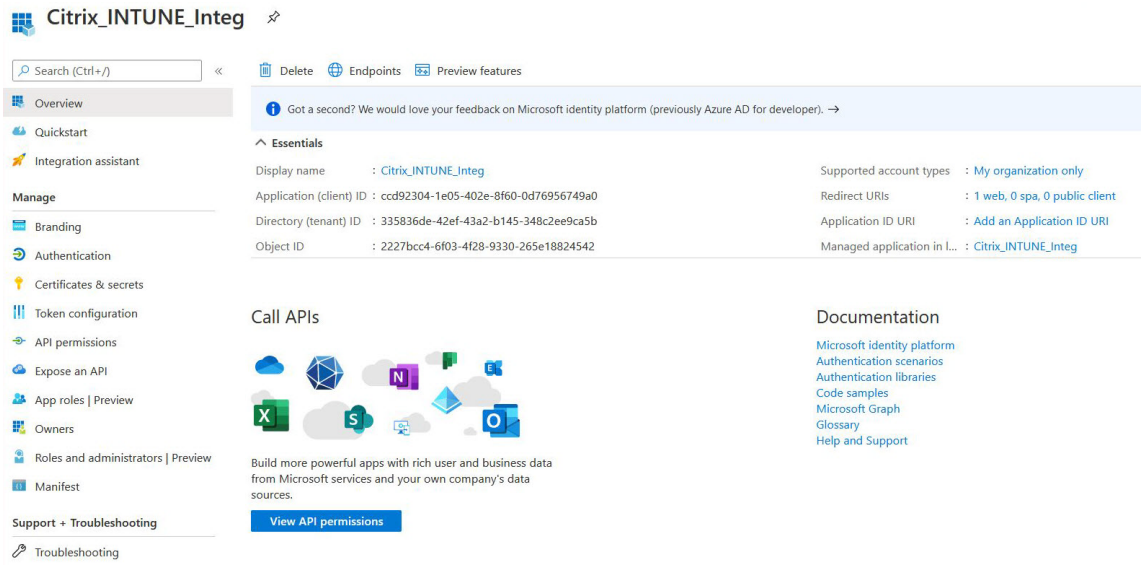
4. 在 注册应用程序 页面上，输入应用程序名称，然后单击 注册。



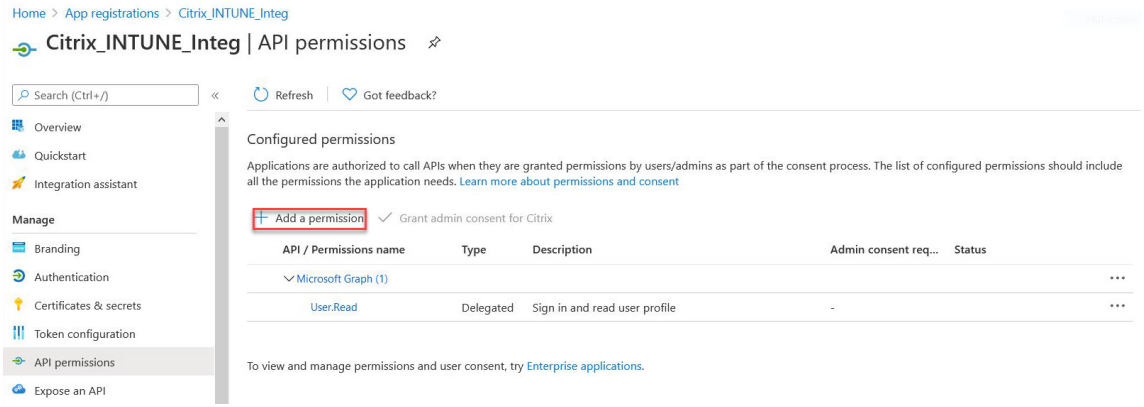
5. 导航到 身份验证，单击 添加 **URI**，输入适用于 NetScaler Gateway 的 FDQN，然后单击 保存。



6. 导航到 概 述页面以获取客户端 ID、租户 ID 和对象 ID。

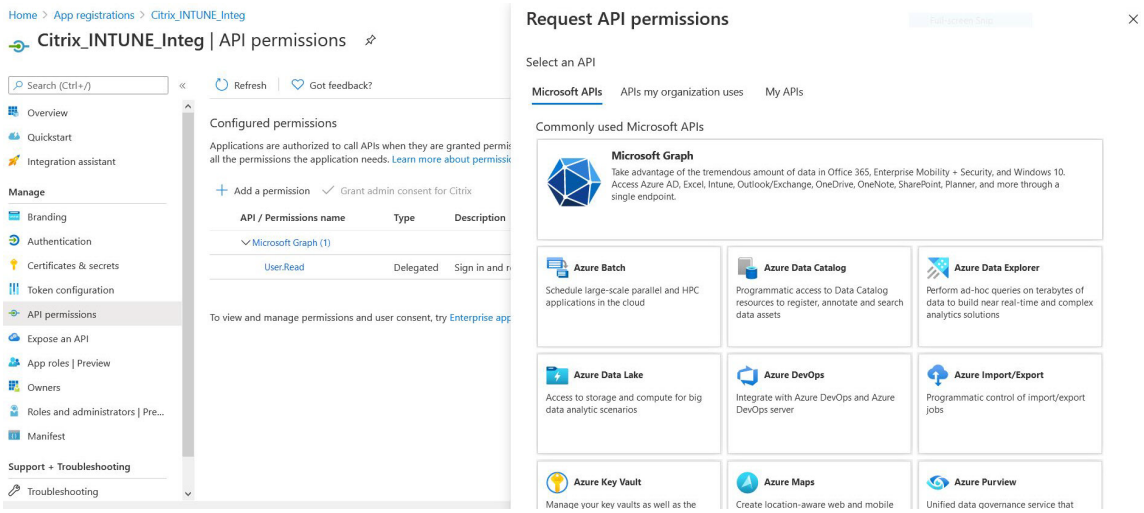


7. 导航到 **API** 权限，然后单击 添加权限。

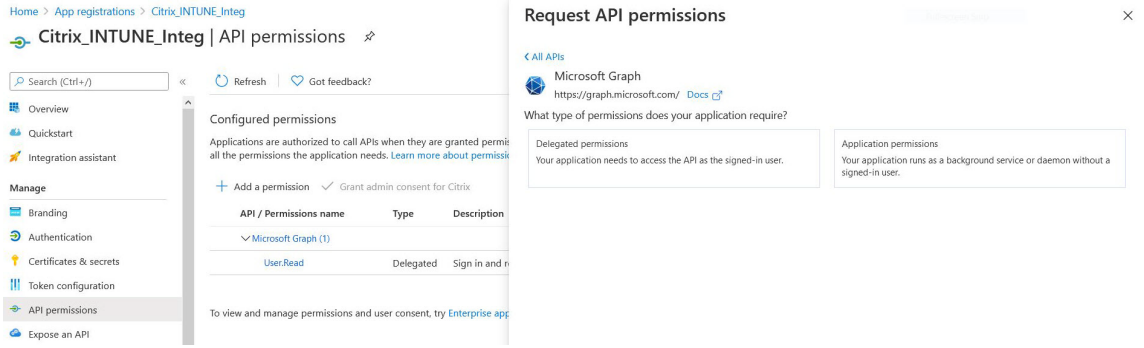


> 注意：
>
> 所有调用 `https://login.microsoftonline.com`、`https://graph.microsoft.com` 或 `https://graph.windows.net` 服务端点的 Azure AD 应用程序都需要为网关分配 API 权限才能调用 NAC API。可用的 API 权限包括：
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> 首选权限为 **Application.Read.All**。
>
> 有关详细信息，请参阅https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. 单击 **Microsoft Graph** 磁贴以配置 Microsoft Graph 的 API 权限。



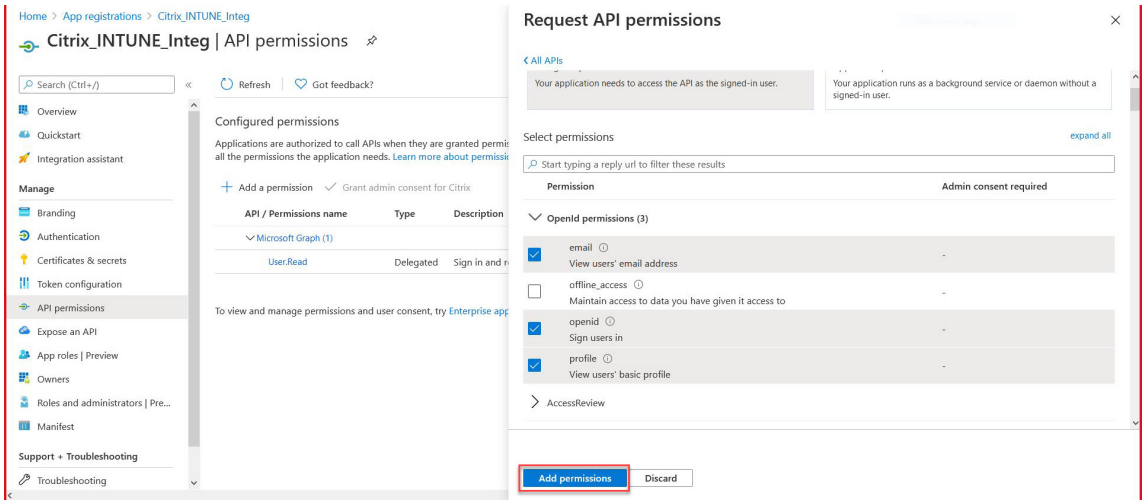
9. 单击委 派权限 磁贴。

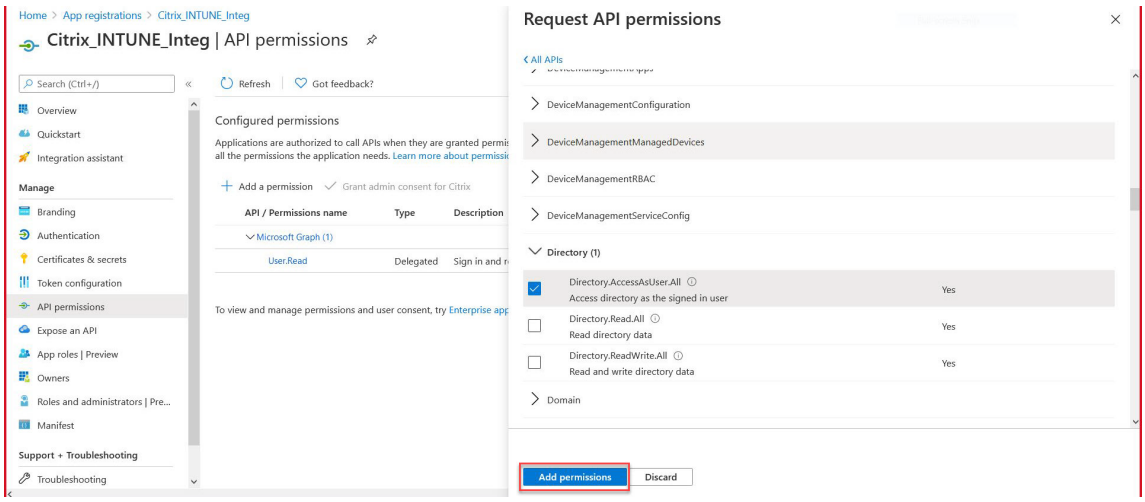


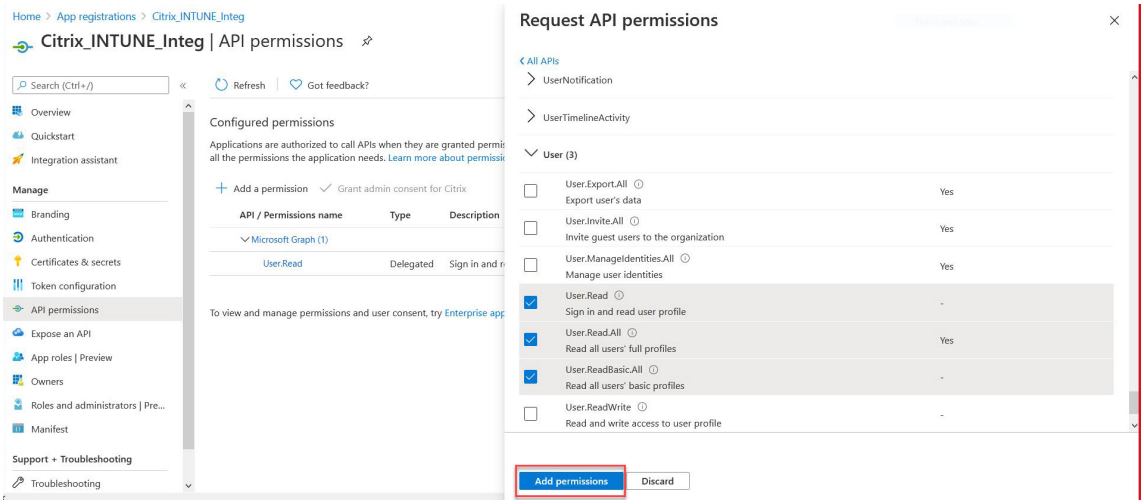
10. 选择以下权限，然后单击 添加权限。

    - 电子邮件

- openid
- 配置文件
- Directory.AccessAsUser.All
- User.Read
- User.Read.All
- User.ReadBasic.All







Intune NAC 检查的权限：

调用 `https://login.microsoftonline.com`、`https://graph.microsoft.com` 或 `https://graph.windows.net` 服务终结点的所有 Azure AD 应用程序都需要为网关分配 API 权限才能调用 NAC API。可用的 API 权限包括：

- Application.Read.All
- Application.ReadWrite.All
- Application.OwnedBy
- Directory.Read.All

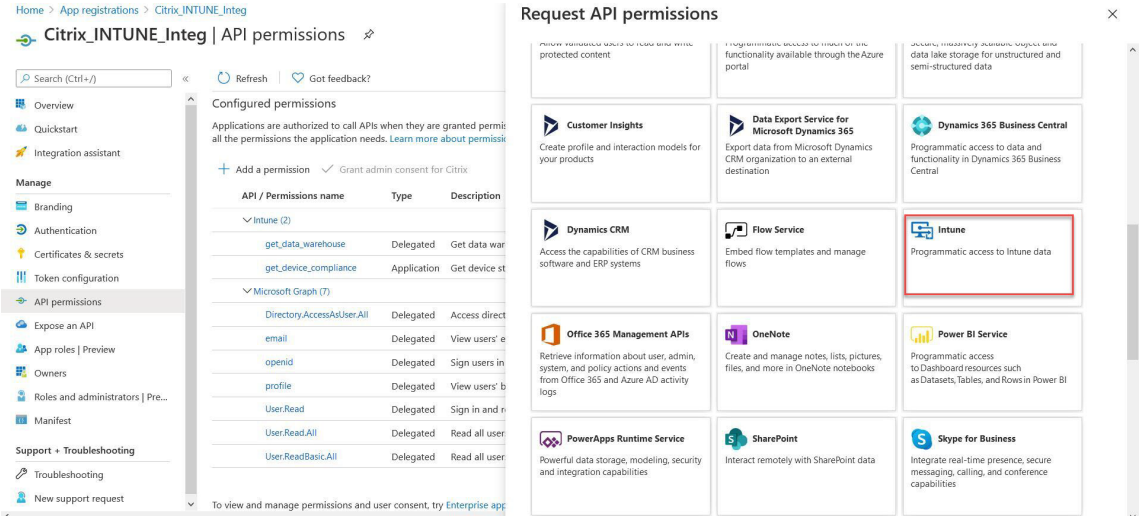
首选权限为 **Application.Read.All**。

有关更多详细信息，请参阅 https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

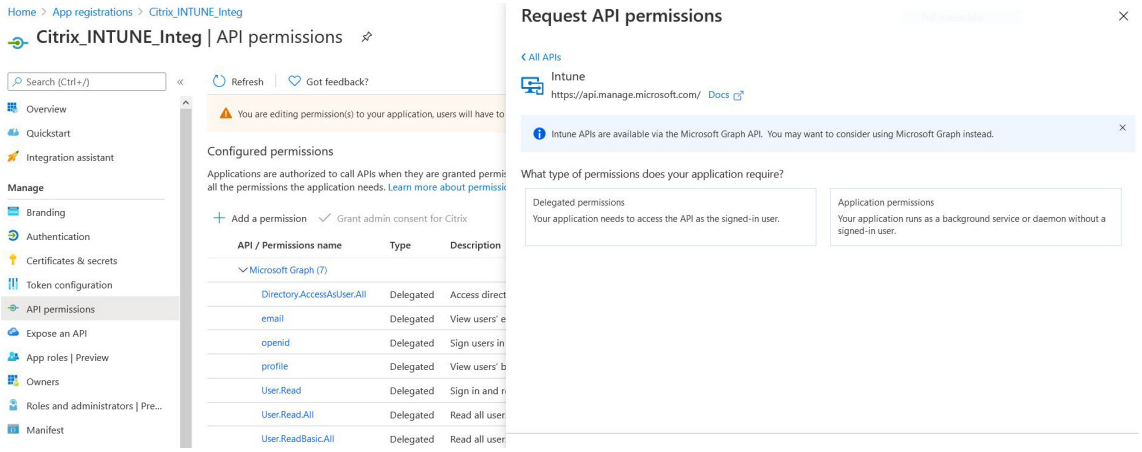
注意：

如果客户仅使用 Intune Action for NAC 检查，则唯一需要的权限是 Microsoft Graph 中的 **Application.Read.All**。

11. 单击 **Intune** 磁贴以配置 Intune 的 API 权限。



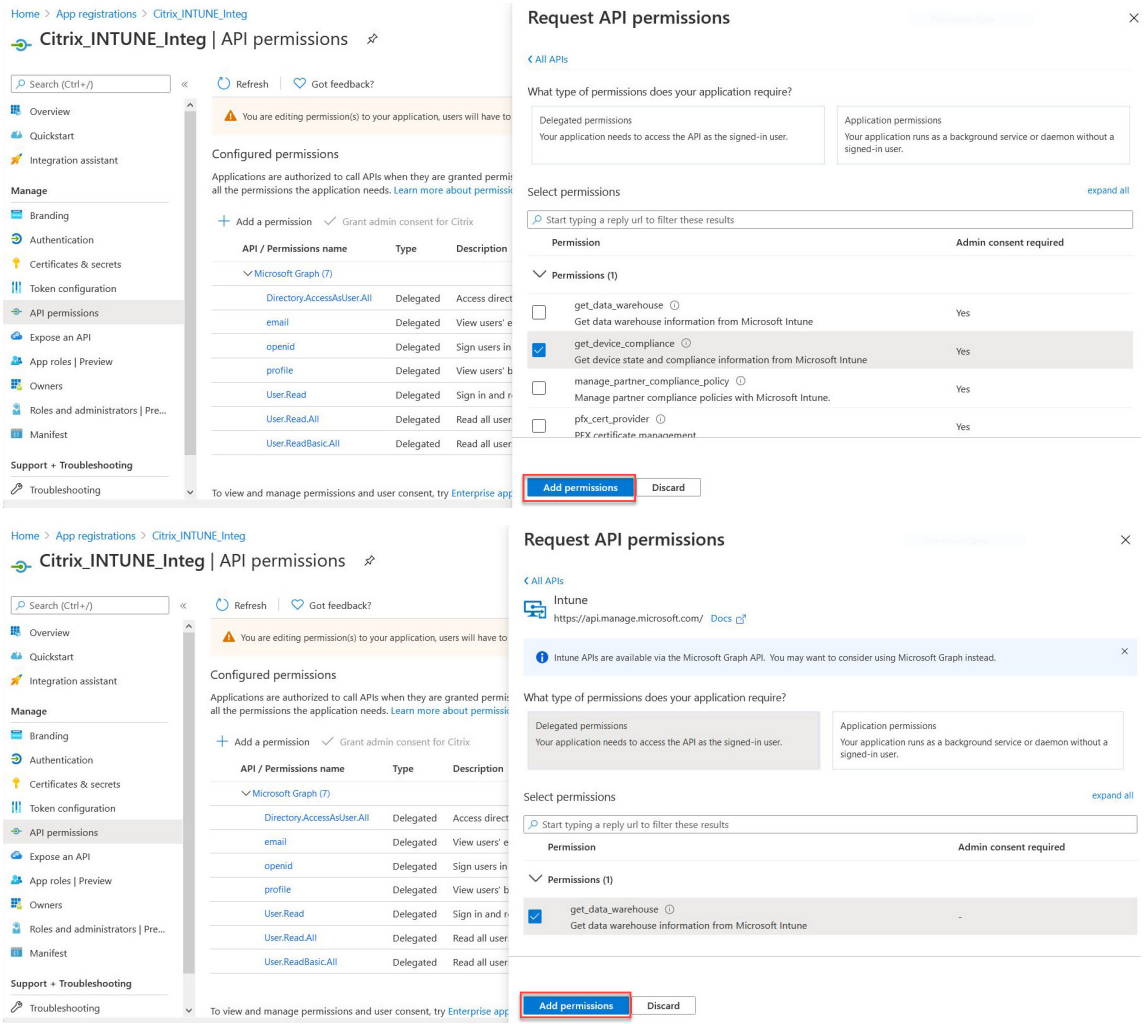
12. 单击 应用程序权限 磁贴和委 派权限 磁贴，分别为 Get_device_Compliance 和 Get_data_Warehouse 添加权限。



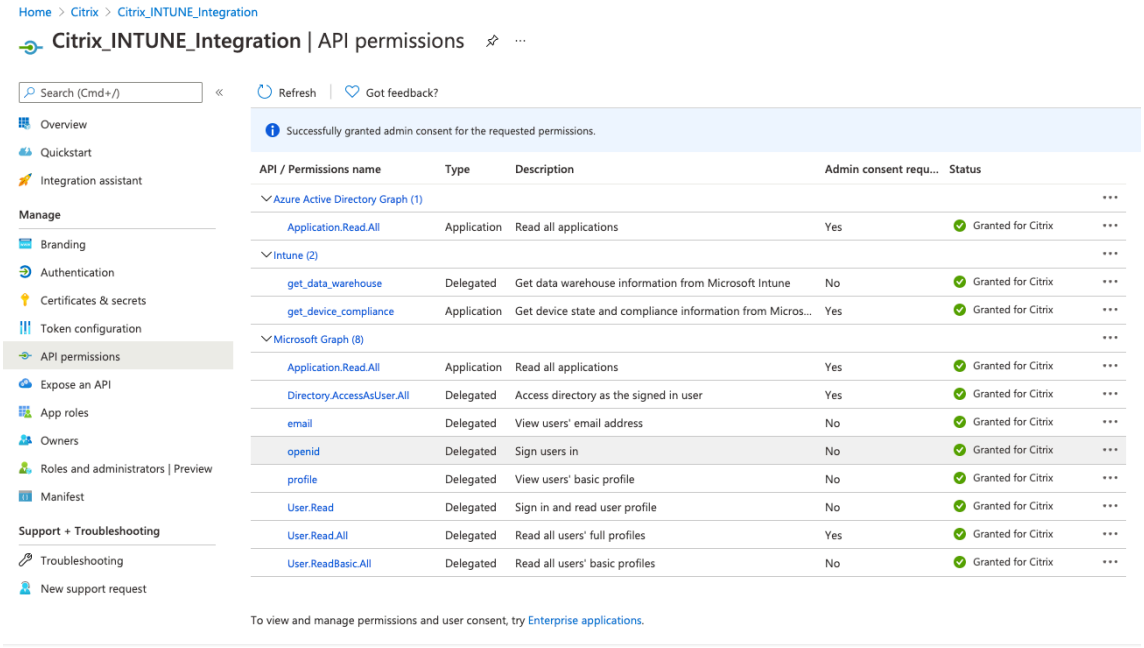
13. 选择以下权限，然后单击 添加权限。

    - get_device_Compliance-应用程序权限
    - Get_data_Warehouse-委派权限

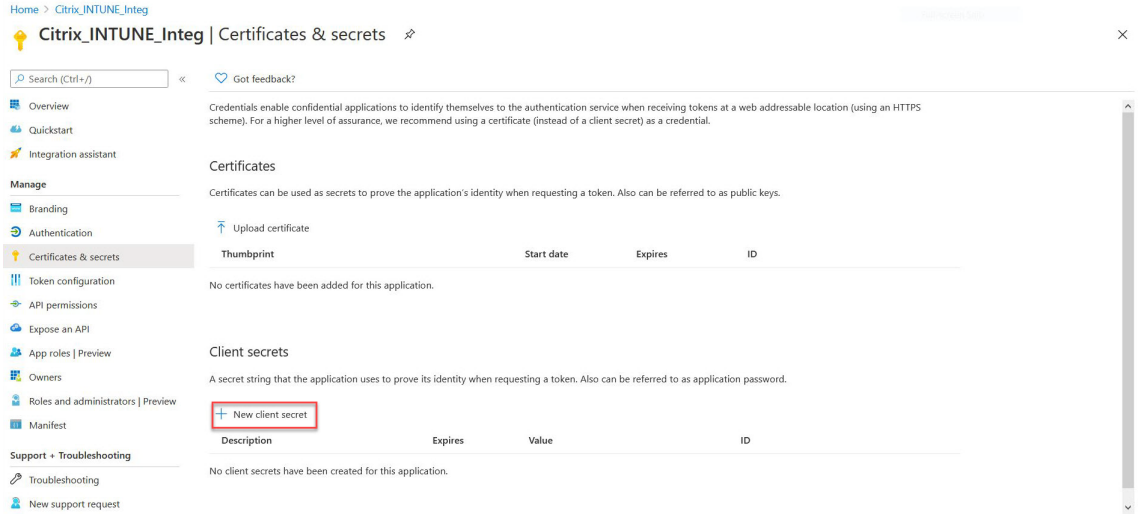
> 注意：
>
> 对于 Intune NAC 检查，唯一需要的权限是 **Get_device_compliance**。



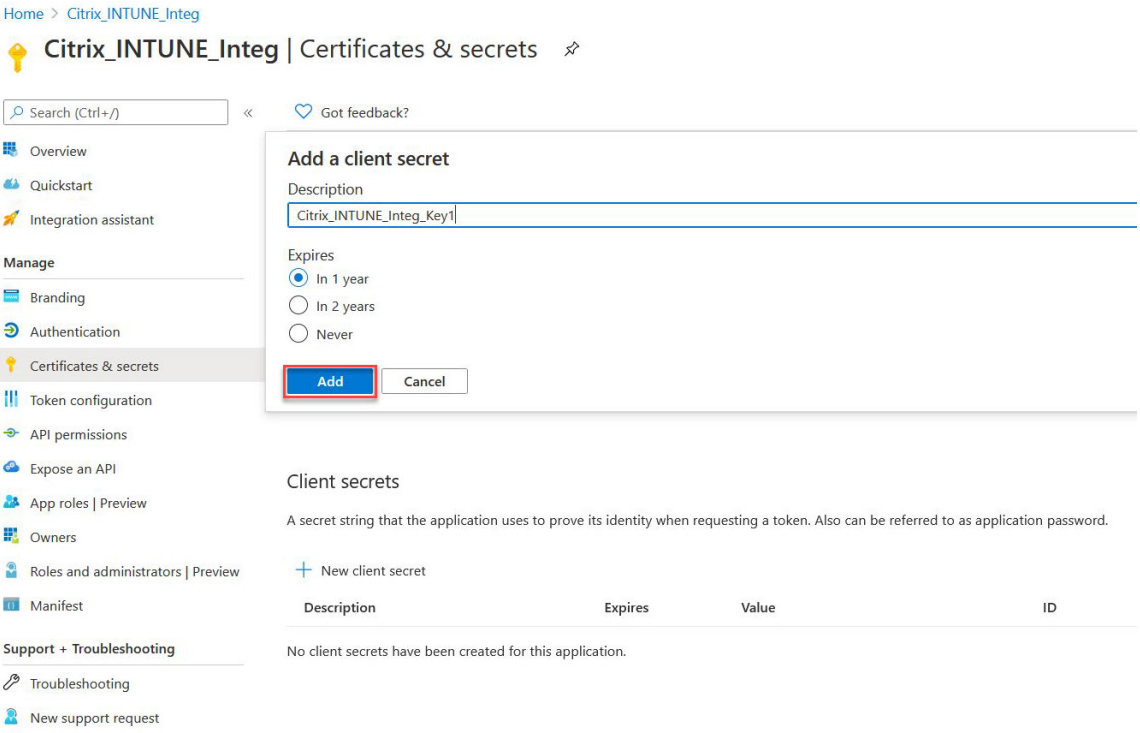
14. 以下页面列出了已配置的 API 权限。



15. 导航到 证书和密 钥，然后单击 新建客户端密钥。

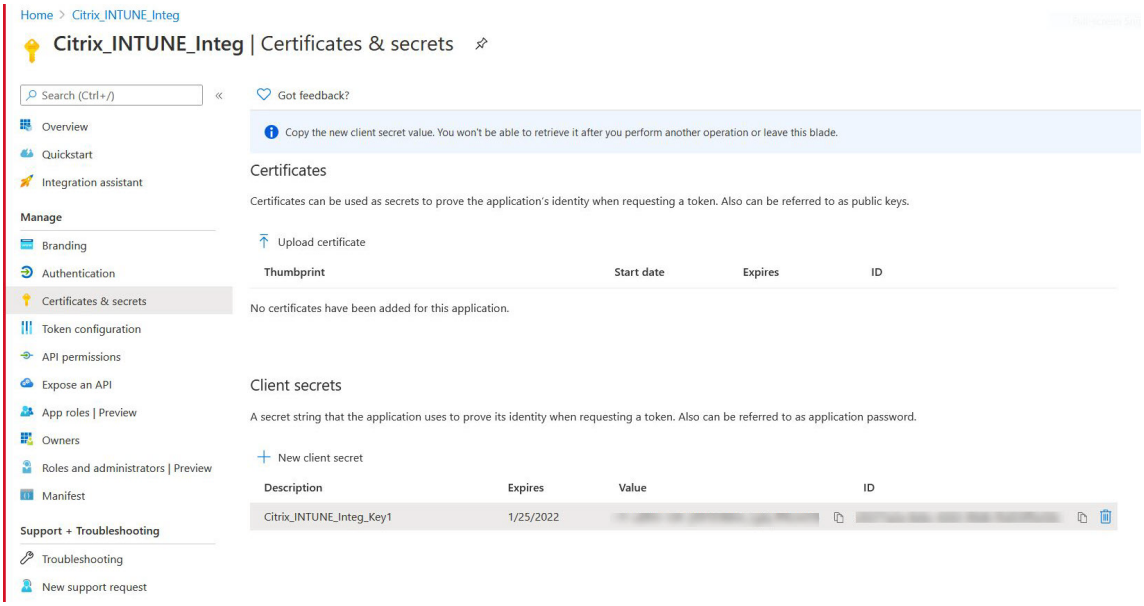


16. 在 添加客户端密钥 页面下，输入说明，选择过期，然后单击 添加。



17. 以下屏幕显示了已配置的客户端密钥。

> 注意
>
> 客户端密钥在生成时只显示一次。在本地复制显示的客户端密钥。在 NetScaler Gateway 设备上为 Intune 配置 OAuth 操作时，使用相同的客户端密钥以及与新注册的应用程序关联的客户端 ID。



Azure 门户上的应用程序配置现已完成。

了解 **Azure ADAL** 令牌身份验证

February 1, 2024

以下是典型的 NetScaler Gateway-Microsoft ADAL 令牌身份验证中的事件流：

1. 在 iOS 或 Android 系统中启动应用程序时，该应用程序会联系 Azure。系统会提示用户使用用户凭据登录。成功登录后，应用程序将获得 ADAL 令牌。

2. 此 ADAL 令牌将呈现给 NetScaler Gateway，该网关已配置为验证 ADAL 令牌。

3. NetScaler Gateway 使用 Microsoft 提供的相应证书来验证 ADAL 令牌的签名。

4. 成功验证后，NetScaler Gateway 将提取用户的主体名称 (UPN)，并向应用程序授予对内部资源的 VPN 访问权限。

配置 **NetScaler Gateway** 虚拟服务器以进行 **Microsoft ADAL** 令牌身份验证

February 1, 2024

要配置 NetScaler Gateway 虚拟服务器以监视 Microsoft ADAL 令牌身份验证，您需要以下信息：

- **CertendPoint**：包含用于 ADAL 令牌验证的 JSON 网络密钥 (JWK) 的终端节点的 URL。
- 受众：应用程序向其发送 ADAL 令牌的 NetScaler 虚拟服务器的 FQDN。
- 发行人：AAD 发行人的名称。默认情况下会填充。
- **tenAntiD**：Azure ADAL 注册的租户 ID。
- **ClientId**：作为 ADAL 注册的一部分提供给 Gateway 应用程序的唯一 ID。
- **ClientSecret**：作为 ADAL 注册的一部分提供给 Gateway 应用程序的密钥。
- **ResourceURI**：用于捕获资源 URI 的可选参数。如果未配置，NetScaler 将使用 Azure 商业资源 URI。

使用命令行界面执行以下步骤：

1. 创建 OAuth 操作。

```
1 add authentication OAuthAction <oauth-action-name> -OAuthType <
    INTUNE>  - clientid <clientID> -clientsecret <client-secret> -
    audience <audience name> -tenantid <tenantID> -issuer <issuer-
    name> -userNameField <upn> -certEndpoint <certEndpoint-name> -
    resourceURI <name of resource URI>
2 <!--NeedCopy-->
```

2. 创建要与新创建的 OAuth 操作关联的身份验证策略。

```
1 add authentication Policy <policy-name> -rule <true> -action <
    oauth intune action>
2 <!--NeedCopy-->
```


3. 将新创建的 OAuth 绑定到 AuthV。

```
bind authentication vserver <auth-vserver> -policy <oauth-intune-policy> -priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. 创建一个 LoginSchema。

```
add authentication loginSchema <loginSchemaName> -authenticationSchema <authenticationSchema" location" >
add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule true -action <loginSchemaName>
<!--NeedCopy-->
```

5. 使用 LoginSchema 绑定身份验证器。

```
bind authentication vserver <auth-vs> -policy <oauth-pol> -priority 2 -gotoPriorityExpression END
<!--NeedCopy-->
```

6. 添加身份验证配置文件并将其分配给 VPN 虚拟服务器。

```
add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name>
<!--NeedCopy-->
```

示例配置

```
add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -tenantid xxxx -issuer "[https://hello](https://hello/)" -userNameField upn -certEndpoint https://login.microsoftonline.com/common/discovery/v2.0/keys --resourceURI htpps://api.manage.microsoft.com

add authentication Policy oauth-intune-pol -rule true -action tmp-action
bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -priority 2 -gotoPriorityExpression END

add authentication loginSchema oauth-loginschema -authenticationSchema "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"

add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -action oauth-loginschema `

bind authentication vserver auth-vs-for-gw1-intune -policy oauth-loginschema-pol -priority 2 -gotoPriorityExpression END

add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-intune

```



```
14 set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
15 <!--NeedCopy-->
```

设置 NetScaler Gateway 以便在 Microsoft Endpoint Manager 中使用 Micro VPN

February 1, 2024

Citrix Micro VPN 与 Microsoft Endpoint Management 集成使您的应用程序能够访问本地资源。有关详细信息，请参阅 Citrix micro VPN 与 Microsoft Endpoint Manager 的集成。

系统要求

- NetScaler Gateway 版本
  - 13.1
  - 13.0
  - 12.1.50.x 或更高版本
  - 12.0.59.x 或更高版本

  您可以从 NetScaler Gateway 下载页面下载最新版本的 NetScaler Gateway。
- 运行 Windows 7 或更高版本的 Windows 桌面（仅适用于 Android 应用程序打包）
- Microsoft
  - Azure AD 访问权限（具有租户管理权限）
  - 启用了 Intune 的租户
- 防火墙规则
  - 为从 NetScaler Gateway 子网 IP 到 `*.manage.microsoft.com`、`https://login.microsoftonline.com`和 `https://graph.windows.net`（端口 443）的 SSL 流量启用防火墙规则
  - NetScaler Gateway 必须能够从外部解析上述 URL。

必备条件

- **Intune** 环境：如果您没有 Intune 环境，请设置一个。有关说明，请参阅 Microsoft 文档。

- **Edge** 浏览器应用程序： Micro VPN SDK 集成在适用于 iOS 和 Android 的 Microsoft Edge 应用程序和 Intune Managed Browser 应用程序中。有关 Managed Browser 的详细信息，请参阅 Microsoft Managed Browser 页面。
- **Citrix Endpoint Management** 权限：确保拥有有效的 Citrix Endpoint Management 权限，以便在 Microsoft Edge 移动浏览器（iOS 和 Android）上继续支持 micro VPN SDK。有关详细信息，请联系您的销售、客户或合作伙伴代表。

授予 **Azure Active Directory (AAD)** 应用程序权限

1. 同意 Citrix 多租户 AAD 应用程序以允许 NetScaler Gateway 使用 AAD 域进行身份验证。Azure 全局管理员必须访问以下 URL 并征得同意：

   https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent。

2. 同意 Citrix 多租户 AAD 应用程序以允许移动应用程序使用 NetScaler Gateway 微型 VPN 进行身份验证。仅当 Azure 全局管理员将默认值更改为“用户可以注册应用程序”从“是”更改为“否”时，才需要此链接。
   此设置可以在 Azure 门户中的 Azure **Active Directory >** 用户 **>** 用户设置下找到。
   Azure 全局管理员必须访问以下 URL 并征得同意（添加
   租户 ID）https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7。

为微型 **VPN** 配置 **NetScaler Gateway**

要将 Micro VPN 与 Intune 结合使用，必须将 NetScaler Gateway 配置为对 Azure AD 进行身份验证。现有的 NetScaler Gateway 虚拟服务器不适用于此用例。
首先，将 Azure AD 配置为与本地 Active Directory 同步。此步骤对于确保 Intune 与 NetScaler Gateway 之间正确进行身份验证是必要的。

下载脚本：.zip 文件包含自述文件，其中包含实现脚本的说明。您需要手动输入脚本所需的信息，然后在 NetScaler Gateway 上运行脚本来配置服务。您可以从 NetScaler 下载页面下载脚本文件。

> 重要：完成 NetScaler Gateway 配置后，如果看到 OAuth 状态而不是完成，请参阅故障排除部分。

配置 **Microsoft Edge** 浏览器

1. 登录到 https://endpoint.microsoft.com/，然后导航到 **Intune >** 移动应用程序。
2. 像往常一样发布 Edge 应用程序，然后添加应用程序配置策略。
3. 在管理下，单击应用程序配置策略。
4. 单击添加，然后为要创建的策略输入名称。在 设备注册类型中，选择 托管应用程序。
5. 单击 关联应用程序。

6. 选择要应用策略的应用程序（Microsoft Edge 或 Intune Managed Browser），然后单击“确定”。
7. 单击配置设置。
8. 在 名称 字段中，输入下表中列出的策略之一的名称。
9. 在值字段中，输入要为该策略应用的值。单击该字段以将策略添加到列表中。可以添加多个策略。
10. 单击确定，然后单击添加。

该策略将添加到您的策略列表中。

名称 (iOS/Android)	值	说明
–	–	–
MvpnGatewayAddress	https://external.companyname.com	NetScaler Gateway 的外部 URL
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSO 或 Unrestricted	MvpnNetworkAccessTunneledWebSS 是通道的默认设置
MvpnExcludeDomains	要排除的域名的逗号分隔列表	可选。默认值 = 空白
TunnelExcludeDomains	使用此客户端属性可覆盖默认的排除域列表。Default=app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com

> 注意： Web SSO 是设置中 Secure Browse 的名称。该行为是相同的。

- **MvpnNetworkAccess** - MvpnNetworkAccessTunneledWebSSO 通过 NetScaler Gateway（也称为通道 Web SSO）启用 HTTP/HTTPS 重定向。网关内联响应 HTTP 身份验证质询，提供单点登录 (SSO) 体验。要使用 Web SSO，请将此策略设置为 **MvpnNetworkAccessTunneledWebSSO**。目前不支持全通道重定向。使用“不受限制”可关闭微型 VPN 通道。
- **MvpnExcludeDomains** -要排除通过 NetScaler Gateway 反向 Web 代理路由的主机或域名的逗号分隔列表。即使 NetScaler Gateway 配置的拆分 DNS 设置可能会选择域或主机，也会排除主机或域名。

  > 注意：
  >
  > – 此策略仅适用于 **MvpnNetworkAccessTunneledWebSSO** 连接。如果设置 MvpnNetworkAccess 为“不受限制”，则忽略此策略。
  >
  > – 此策略仅适用于配置为反向拆分通道的 NetScaler Gateway 的通道-Web SSO 模式。

- **TunnelExcludeDomains** - 默认情况下，MDX 会将某些服务端点排除在 Micro VPN 通道之外。移动应用程序 SDK 和应用程序使用这些服务端点来实现各种功能。例如，服务端点包括不需要通过企业网络进行路由的服务，例如 Google Analytics、Citrix Cloud 服务和 Active Directory 服务。使用此客户端属性可覆盖默认的排除域列表。

  要配置此全局客户端策略，请在 Citrix Endpoint Management 控制台上，导航到设置 **>** 客户端属性，添加自定义注册表项 **TUNNEL_EXCLUDE_DOMAINS**，然后设置值。

值：要使用要从通道中排除的域替换默认列表，请键入以逗号分隔的域后缀列表。要在通道中包括所有域，请键入 none。默认值：

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis
-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com
,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,
hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf
.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.
google-analytics.com,stream.launchdarkly.com
```

故障排除

常规问题

问题	解决方案
打开应用程序时，将显示“需要添加策略”消息	在 Microsoft Graph API 中添加策略
存在策略冲突	每个应用程序只允许使用一个策略
打包应用程序时会出现“无法打包应用程序”消息。有关完整消息，请参阅下表	该应用程序已与 Intune SDK 集成在一起。您不需要用 Intune 包装应用程序
您的应用无法连接到内部资源	确保打开了正确的防火墙端口、更正了租户 ID 等

无法打包应用程序错误消息：

无法打包应用程序。*com.microsoft.intune.mam.apppackager.utils.AppPackagerException:* 此应用程序已集成 *MAM*
SDK。
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
不能打包此应用程序。

NetScaler Gateway 问题

问题	解决方案
为 Azure 上的网关应用程序配置所需的权限不可用。	检查是否有适当的 Intune 许可证可用。尝试使用 manage.windowsazure.com 门户来查看是否可以添加权限。如果问题仍然存在，请与 Microsoft 支持部门联系。
NetScaler Gateway 无法访问 `login.microsoftonline.com and graph.windows.net`。	从 NS Shell，检查您是否能够访问以下 Microsoft 网站：cURL -v -k https://login.microsoftonline.com。然后，检查是否在 NetScaler Gateway 上配置了 DNS。还要检查防火墙设置是否正确（如果 DNS 请求被防火墙处理）。
配置 OAuthAction 后，ns.log 中会出现错误。	检查 Intune 许可是否已启用，以及 Azure 网关应用程序是否设置了适当的权限。
Sh OAuthAction 命令不会显示 OAuth 状态为完成。	检查 Azure Gateway 应用程序的 DNS 设置和配置权限。
Android 或 iOS 设备不显示双重身份验证提示。	检查双重设备 ID 登录架构是否绑定到身份验证虚拟服务器。

NetScaler Gateway OAuth 状态和错误情况

状态	错误情况
AADFORGRAPH	密钥无效、URL 未解析、连接超时
MDMINFO	`*manage.microsoft.com`已关闭或无法访问
GRAPH	图形端点已关闭，无法访问
CERTFETCH	由于 DNS 错误，无法与“令牌端点：https://login.microsoftonline.com”对话。要验证此配置，请转到 shell 并键入 cURL https://login.microsoftonline.com。此命令必须验证。

注意：当 OAuth 状态成功时，状态将显示为“完成”。

扩展了对 **Azure AD** 图表的支持

February 1, 2024

由于 Azure AD 图表已弃用，因此触发新应用程序的客户无法使用 Azure AD 图形中提供的早期权限。但是，拥有现有应用程序的客户如果希望在更长时间内使用 Azure AD Graph 的旧权限，则可以通过在网关设备上进行一些配置更改来继续这样做。NetScaler Gateway 版本 13.1-27.xx 及更高版本支持此配置。

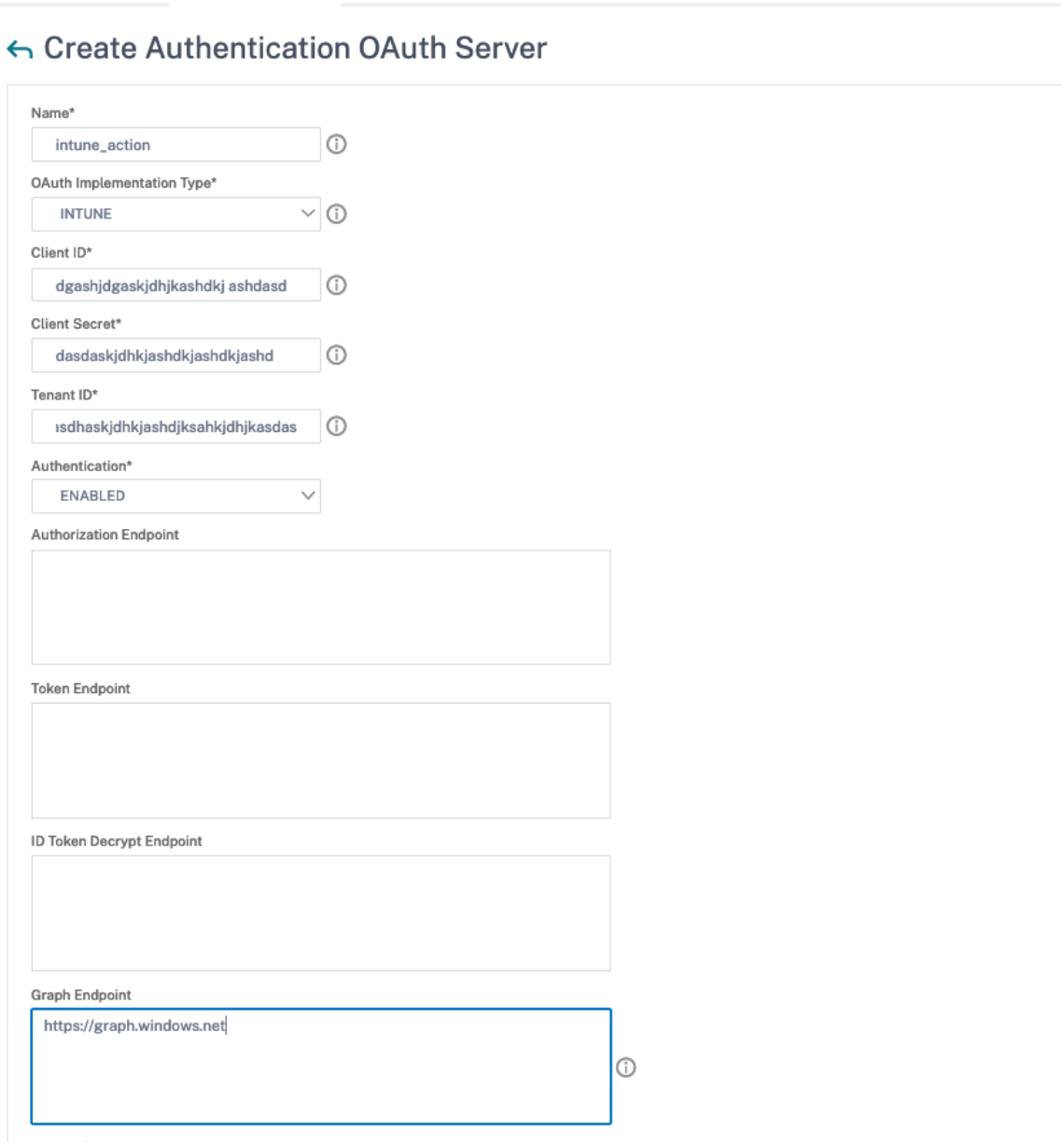
在 NetScaler Gateway 设备上执行以下配置更改：

1. 在命令提示符下，运行以下命令。

```
shell nsapimgr_wr.sh -ys call=” ns_intune_enable_old_endpoints”
<!--NeedCopy-->
```

2. 导航到“安全”**>**“**AAA-**应用程序流量”**>**“策略”**>**“身份验证”**>**“高级策略”**>**“操作”**>**“**OAUTH** 操作”。

   a) 选择一个现有 OAuth 服务器。
   b) 单击 **More**（更多）。
   c) 在图形端点中，确保 URL 与图中所示的相似。



HDX 开明的数据传输支持

February 1, 2024

NetScaler Gateway 对 HDX Enlightened Data Transport (EDT) 支持可确保为运行 Citrix Workspace 应用程序的用户提供虚拟桌面的高清会话中用户体验。

此外，在 Citrix Workspace 应用程序和 VDA 之间使用 DTLS 1.0 进行端到端加密，可以实现 EDT 终止。有关详细信息，请参阅 支持 DTLS 协议。

启用了 EDT 的 NetScaler Gateway 可在局域网和广域网条件下提供良好的用户体验。使用 EDT，从一个漫游到另一个时，您不需要任何管理或用户配置。这种好处在数据包丢失中等程度的高延迟网络中最为明显，在这种网络中，用户体验通常会落后于其他

何时使用 **Enlightened Data Transport** 支持

February 1, 2024

以下方案说明了如何使用启用 EDT 的 NetScaler Gateway。

- 用户希望在远程访问业务资源的同时获得与 LAN 环境一样出色的体验。
- 用户希望在 Wi-Fi 和蜂窝网络上获得丰富的虚拟应用程序和桌面用户体验，这些网络由于拥塞、高丢包和高延迟，网络质量较差。

使用 EDT 时要记住以下几点。

- 默认情况下，虚拟服务器级别的 DTLS 旋钮处于启用状态。
- 不支持带有 DTLS 的 IPv6。
- 现在可以将设备配置为 Receiver 和 VDA 之间的 EDT 流量的双跃点功能。有关详细信息，请单击 在双跃点 DMZ 中部署。

注意：在 12.1 版本 49.xx 及更高版本中，MPX FIPS 平台支持 EDT。在基于 Intel Coleto SSL 芯片的 MPX 设备上，12.1 版本 51.16 及更高版本支持 EDT。

配置 **NetScaler Gateway** 以支持 **Enlightened Data Transport** 和 **HDX Insight**

February 1, 2024

通过网关的 EDT 流量现在具有端到端可见性。实时和历史可见性数据的可用性使 NetScaler ADM 能够支持各种用例。

支持以下情况：

场景	EDT 支持
NetScaler Gateway	是
具有高可用性 (HA) 的 NetScaler Gateway	是
具有高可用性 (HA) 优化功能的 NetScaler Gateway	是
带 Unified Gateway 的 NetScaler	是

场景	EDT 支持
搭载 GSLB 的 NetScaler Gateway	是
带群集的 NetScaler Gateway	是
Citrix Workspace 应用程序到 NetScaler Gateway DTLS 加密	是
NetScaler Gateway 上的双 Secure Ticket Authority (STA)	是
NetScaler Gateway ICA 会话超时	是
NetScaler Gateway 多流 ICA	否
NetScaler Gateway 会话可靠性（端口 2598）	是
NetScaler Gateway 双跃点	是
NetScaler 到 VDA 的 DTLS 加密	是
HDX Insight	是
采用 IPv6 模式的 NetScaler Gateway	否
NetScaler Gateway SOCKS（端口 1494）	否
NetScaler 纯局域网代理（参见备注）	否

> 注意：
>
> 如果 NetScaler 局域网代理配置为局域网用户模式或透明模式，则不支持 EDT。但是，支持 TCP。有关详细信息，请参阅：
>
> - 配置出站 ICA 代理
> - 使用 SOCKS 使用 NetScaler 为局域网用户收集 HDX Insight 分析数据

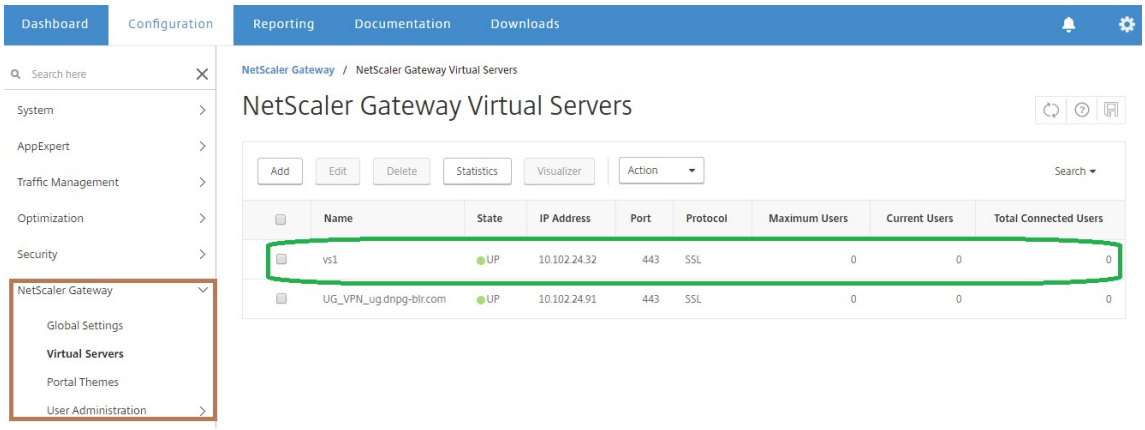
配置 **NetScaler Gateway** 以支持 **Enlightened Data Transport**

如果使用 Enlightened Data Transport (EDT)，则必须启用数据报传输层安全性 (DTLS) 才能加密 EDT 使用的 UDP 连接。必须在网关 VPN 虚拟服务器级别启用 DTLS 参数。此外，必须正确升级和配置 Citrix Virtual Apps and Desktops 组件，以实现 Gateway VPN 虚拟服务器和用户设备之间的加密流量。

> 注意：必须在 DMZ 中打开为 NetScaler Gateway 前端虚拟服务器配置的 UDP 端口（例如端口 443），虚拟服务器才能接收 DTLS 连接。DTLS 和 CGP 是 EDT 与 NetScaler Gateway 兼容的先决条件。

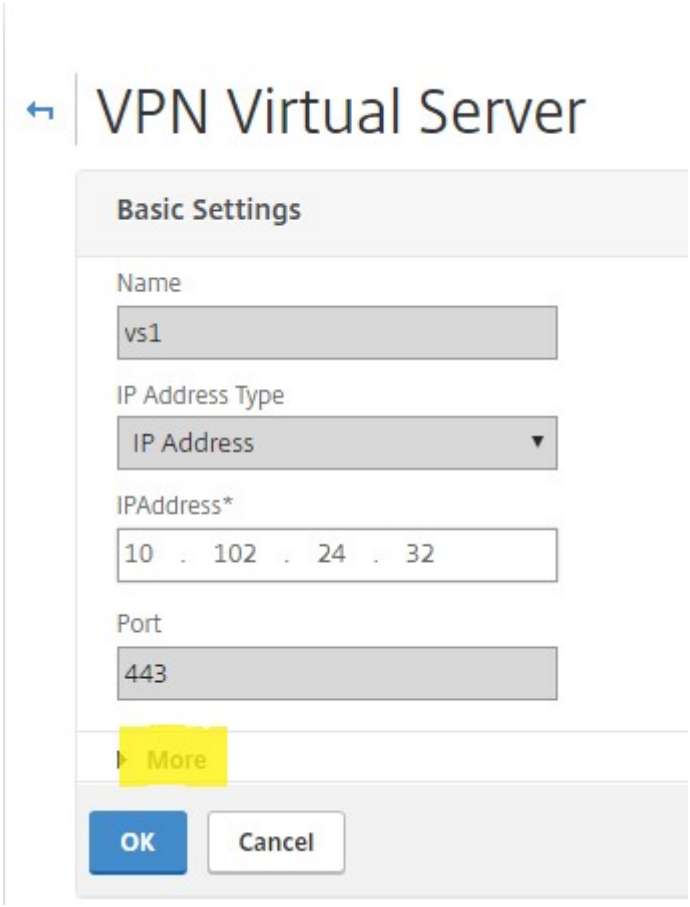
使用 **GUI** 将 **NetScaler Gateway** 配置为支持 **EDT**

1. 部署并配置 NetScaler Gateway 以与 StoreFront 通信并为 Citrix Virtual Apps and Desktops 进行用户身份验证。
2. 在 NetScaler GUI 的“配置”选项卡上，展开 **NetScaler Gateway** ，然后选择 虚拟服务器。



3. 单击 编辑 以显示 VPN 虚拟服务器的基本设置，然后验证 DTLS 设置的状态。

4. 单击“更多”以显示其他配置选项。



5. 选择 **DTLS** 可为数据报协议提供通信安全性。单击确定。VPN 虚拟服务器的“基本设置”区域显示 DTLS 标志设置为 **True**。

使用 **CLI** 配置 **NetScaler Gateway** 以获得 **EDT** 支持

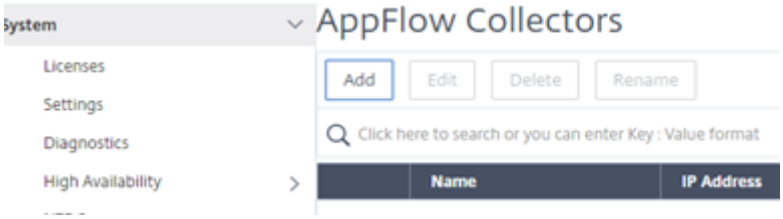
```
1 set vpn vserver vs1 -DTLS ON
```


配置 **NetScaler Gateway** 以支持 **HDX Insight**

HDX Insight 为通过 NetScaler 的虚拟应用程序和桌面的 HDX 流量提供端到端可见性。它还使管理员能够查看实时客户端和网络延迟指标、历史报告、端到端性能数据以及解决性能问题。

使用 **GUI** 将 **NetScaler Gateway** 配置为支持 **HDX Insight** 能分析

1. 在 配置 选项卡上，导航到 系统 **> AppFlow>** 收集器，然后单击 添加。



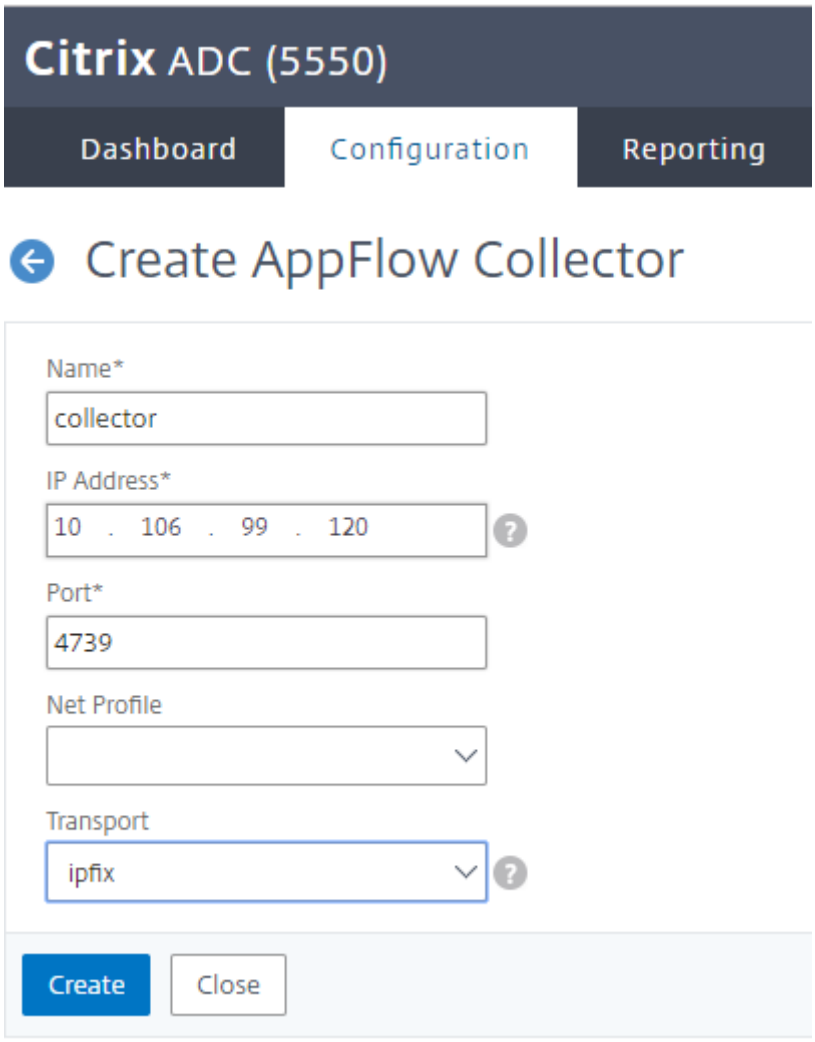
2. 在“创建 **AppFlow** 收集器”页上，填充以下字段，然后单击“创建”。
   名称—收集器的名称

   IP 地址—收集器的 IPv4 地址

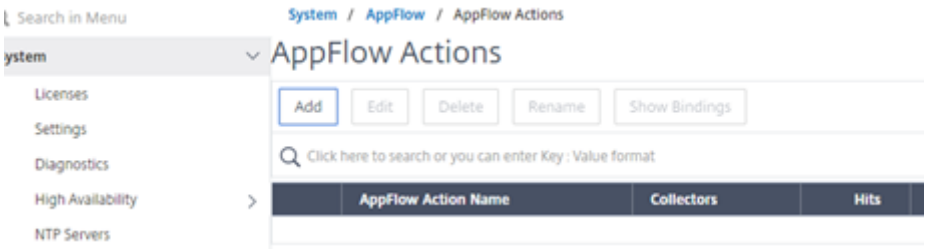
   端口—收集器监听的端口

   网络配置文件-要与收集器关联的网络配置文件。配置文件中定义的 IP 地址用作此收集器的 AppFlow 流量的源 IP 地址。如果未设置此参数，则将使用 NetScaler IP (NSIP) 地址作为源 IP 地址。

   运输—收集器的运输类型。



3. 导航到 系统 **> AppFlow >** 操作，单击 添加。

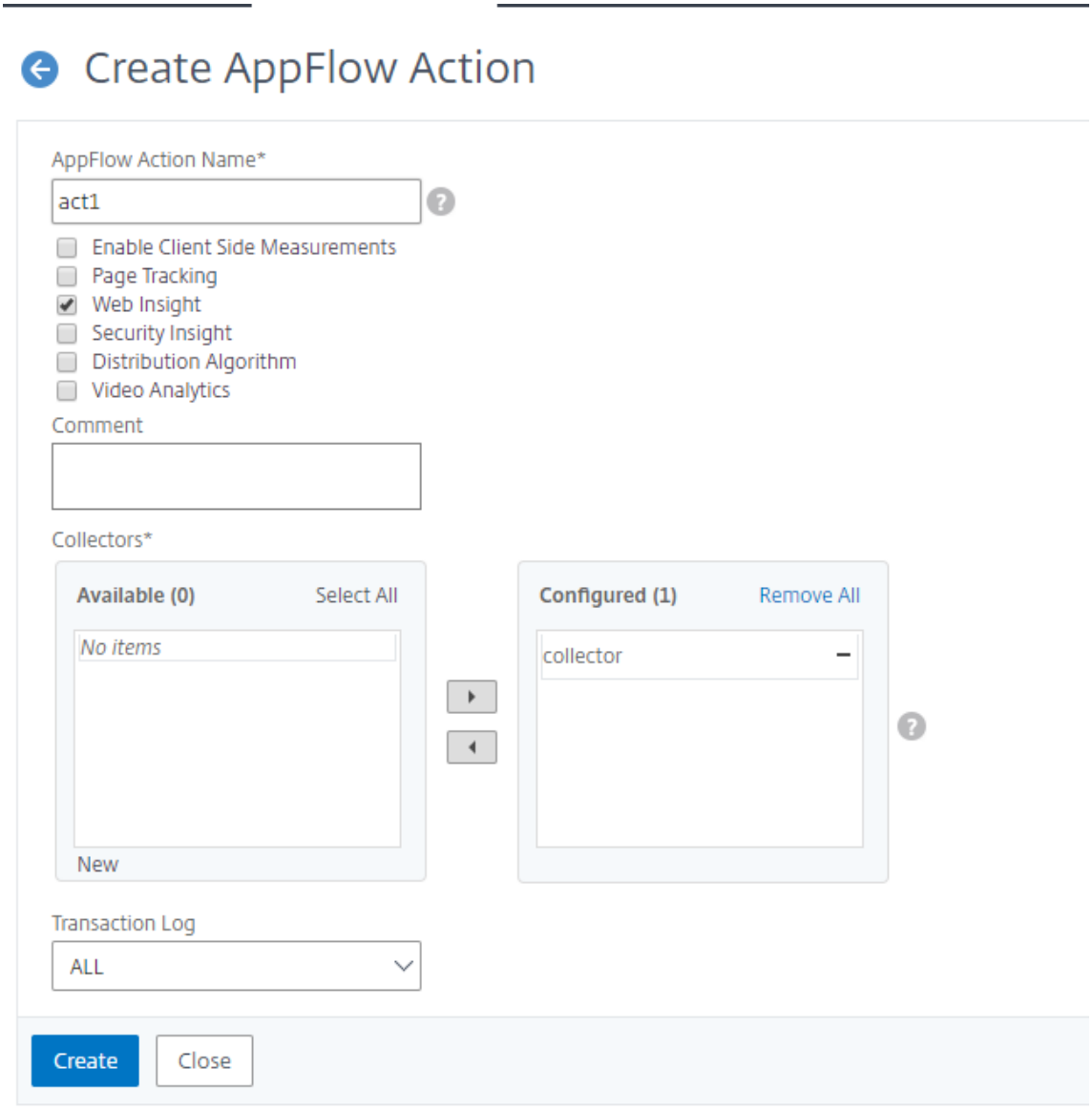


4. 在 创建 **AppFlow** 操作 页面上，填充以下字段，然后单击 创建。
   AppFlow 操作名称—操作的名称

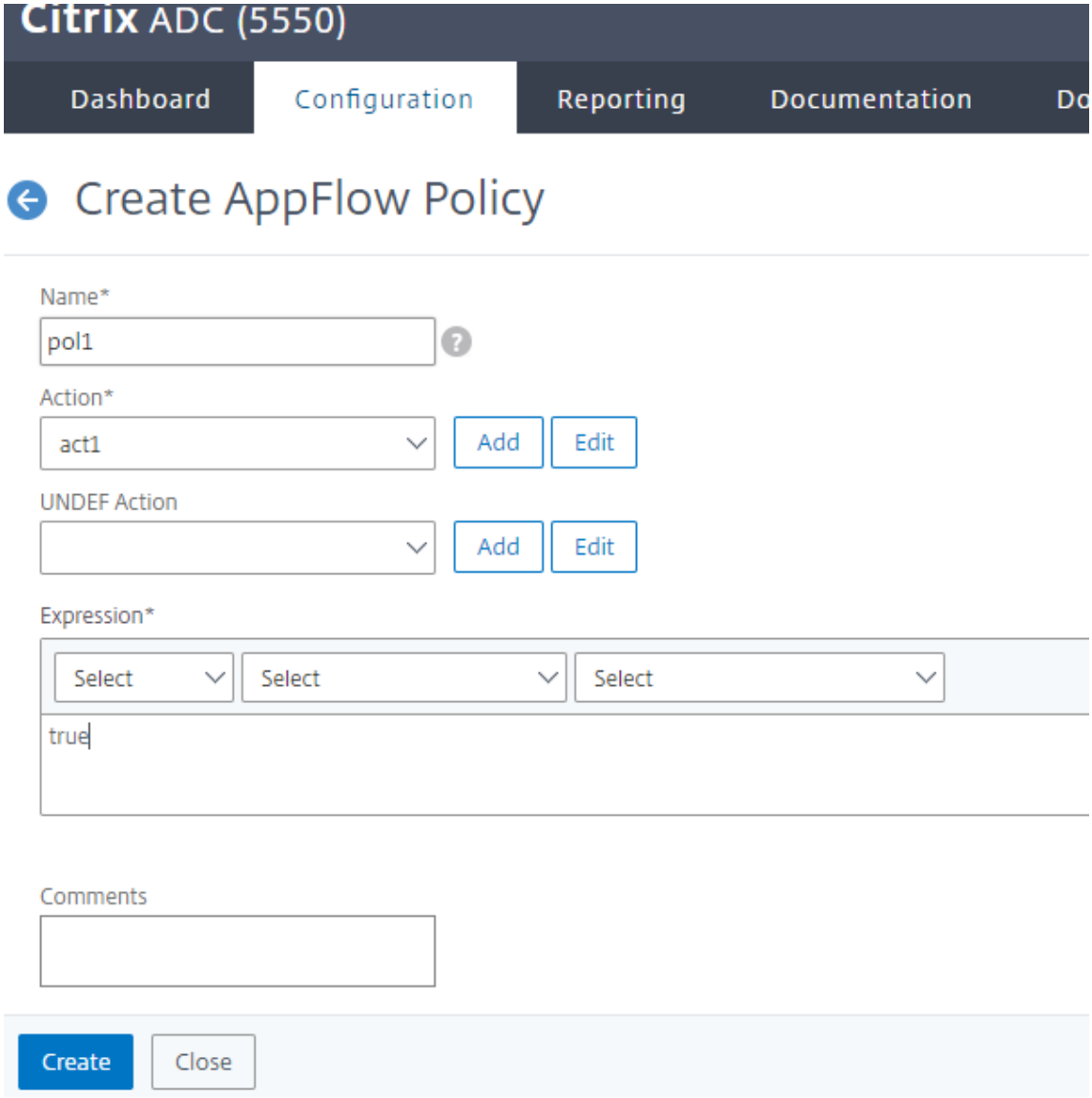
   评论—关于操作的任何评论

   收集器—选择要与 AppFlow 操作关联的收集器的名称。

   事务日志—要记录的事务类型。



5. 导航到 系统 **> AppFlow>** 策略，单击 添加。



6. 在 创建 **AppFlow** 策略 页面上，填充以下字段，然后单击 创建。

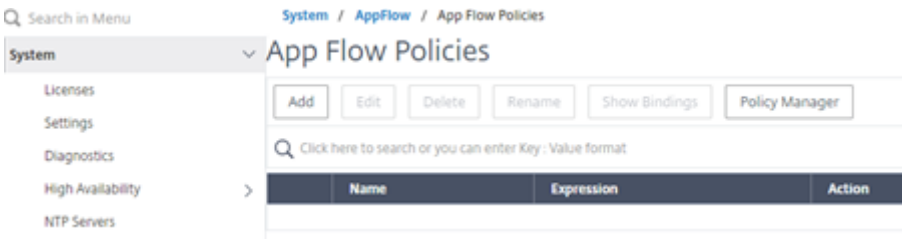
   名称—策略的名称。

   操作—要与策略关联的操作的名称。

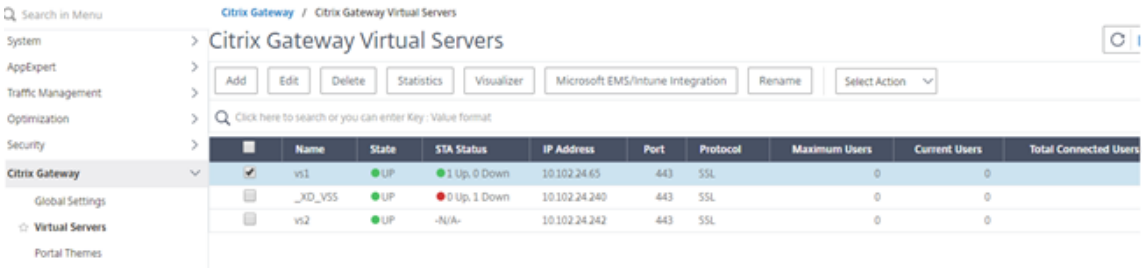
   UNDEF-发生未定义事件时要与此策略关联的 AppFlow 操作的名称。

   表达式-用于评估流量的表达式或其他值。必须是布尔表达式。

   评论—关于此策略的任何评论。

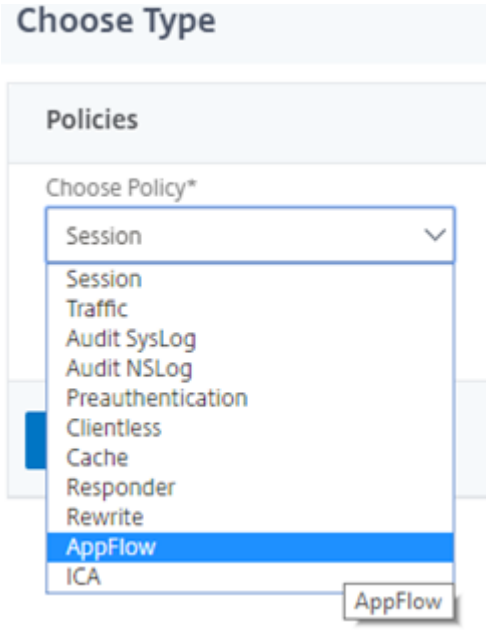


7. 导航到 **NetScaler Gateway>** 虚拟服务器，选择虚拟服务器，然后单击 编辑。

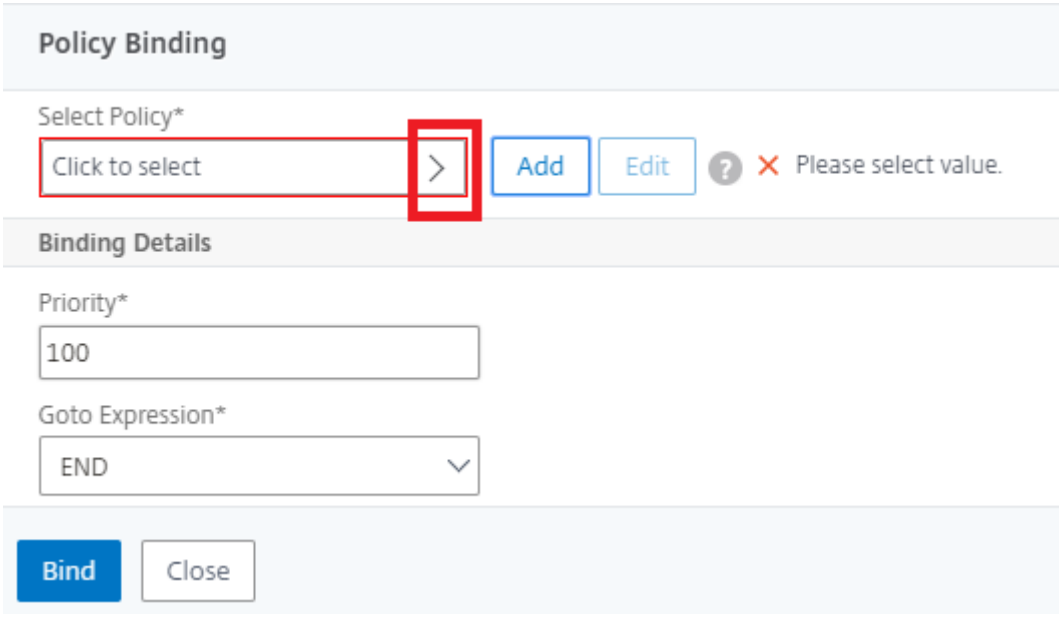


8. 向下滚动 **VPN** 虚拟服务器 页面，然后在 策略 部分下单击 **+**。

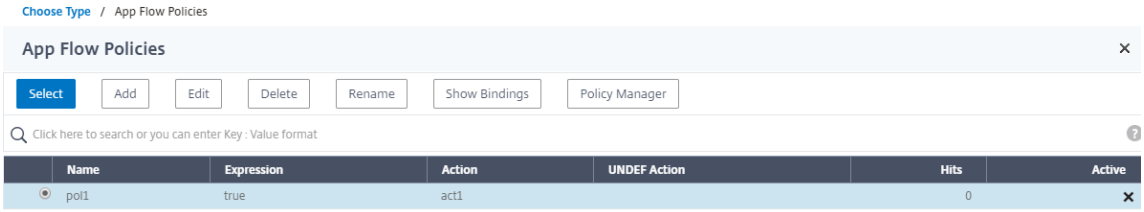
9. 在“选 择类型”屏幕的“选择策略”下拉菜单中，选择 **AppFlow**。在 选择类型 下拉菜单中，选择 请求 或 **ICA** 请求，然后单击 继续。



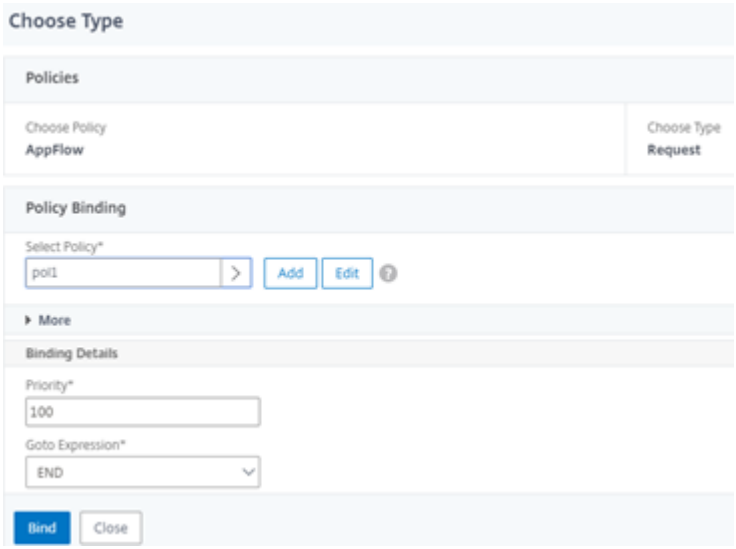
10. 单击选 择策略下突出显示的箭头。



11. 选择 **AppFlow** 策略，然后单击选择。



12. 最后单击 绑定。



要使用 **CLI** 配置适用于 **HDX Insight** 的 **NetScaler Gateway** 支持，请键入以下命令

```
1 add appflow collector col3 -IPAddress<ip_mas>
```



```
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
    type <ICA_Request>
```

为非 **NSAP HDX** 会话禁用 **HDX Insight**

在 NetScaler 设备中，您现在可以为非 NSAP HDX 会话禁用 HDX Insight。

在命令提示符下，键入：

```
set ica parameter HDXInsightNonNSAP (YES | NO )
<!--NeedCopy-->
```

默认情况下，非 NSAP 会话的 HDX Insight 处于启用状态。

通过 **NetScaler Gateway** 进行 **EDT** 的 **PMTUD** 发现和 **DF** 位传播

February 1, 2024

从版本 13.1 build 17.x 开始，NetScaler Gateway 设备支持对 EDT 路径最大传输单元发现 (PMTUD) 执行 DF 位。路径 MTU 发现有助于在建立会话时动态确定最大传输单元 (MTU)。DF 位强制可防止可能导致性能下降或无法建立会话的 EDT 碎片。

在早期版本中，NetScaler Gateway 支持 EDT 路径 MTUD，但不支持 DF 位强制。

有关更多详细信息，请参阅 EDT MTU 发现。

使用 **CLI** 启用 **PMTUD** 支持

在命令提示窗口中，键入：

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-
    HDXInsightNonNSAP ( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )]
     [-EDTPmtudDFTimeout <positive_integer>] [-L7LatencyFrequency <
    positive_integer>]
<!--NeedCopy-->
```

示例：

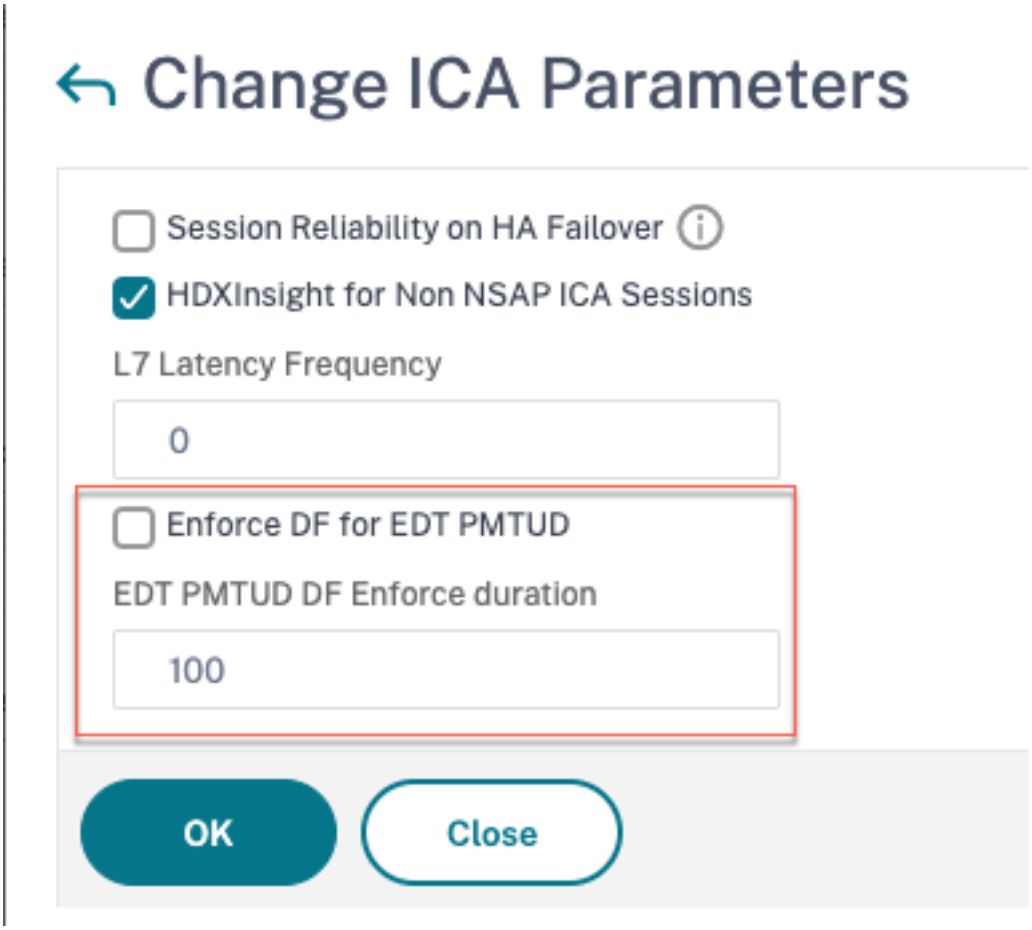
```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED -
    EDTPmtudDFTimeout 100
<!--NeedCopy-->
```


> 注意：
>
> 自版本 13.1 Build 42.x 及更高版本中，EDTPmtudDF 参数默认处于启用状态。以前，默认情况下，此选项处于禁用状态。

使用 **GUI** 启用 **PMTUD** 支持

1. 导航到“系统”**>**“设置”**>**“更改 **ICA** 参数”。
2. 在 **EDT PMTUD DF** 强制持续时间中，输入 PMTUD DF 强制执行的超时时间（以秒为单位）。

> 注意：
>
> 自版本 13.1 Build 42.x 及更高版本中，默认情况下，**EDT PMTUD** 的强制执行 **DF** 选项处于启用状态。以前，默认情况下，此选项处于禁用状态。



L7 延迟阈值

February 1, 2024

HDX Insight 中的 L7 延迟阈值功能主动检测应用程序级别的端到端网络延迟问题，并采取主动措施。L7 延迟阈值设定功能执行实时延迟监视以检测峰值，并在延迟超过观察到的最小延迟时向 HDX Insight 发送通知。

以前，每 60 秒向 HDX Insight 发送一次平均客户端和服务器端 L7 延迟值。在此间隔内看到的任何峰值均被平均化，因此仍未检测到。此外，没有实时延迟监视来检测这些峰值。

L7 延迟与 L4 延迟有何不同

网络延迟也会捕获并显示在 L4 级别。这些延迟是从 TCP 层计算出来的，不需要解析 ICA 流量。因此，它们相对容易获得，CPU 密集度较低。但是，L4 延迟的主要缺点是了解端到端延迟。如果路径中有 TCP 代理，则 L4 延迟仅捕获从 NetScaler 到 TCP 代理的延迟。这可能会导致信息不完整，从而导致调试问题的困难。

L7 延迟是通过解析 ICA 流量来计算的。L7 延迟计算是在 ICA 层完成的，因此中间代理不会导致延迟值不完整。因此，提供端到端延迟检测。

下图显示了带有和不带 TCP 代理的部署类型。

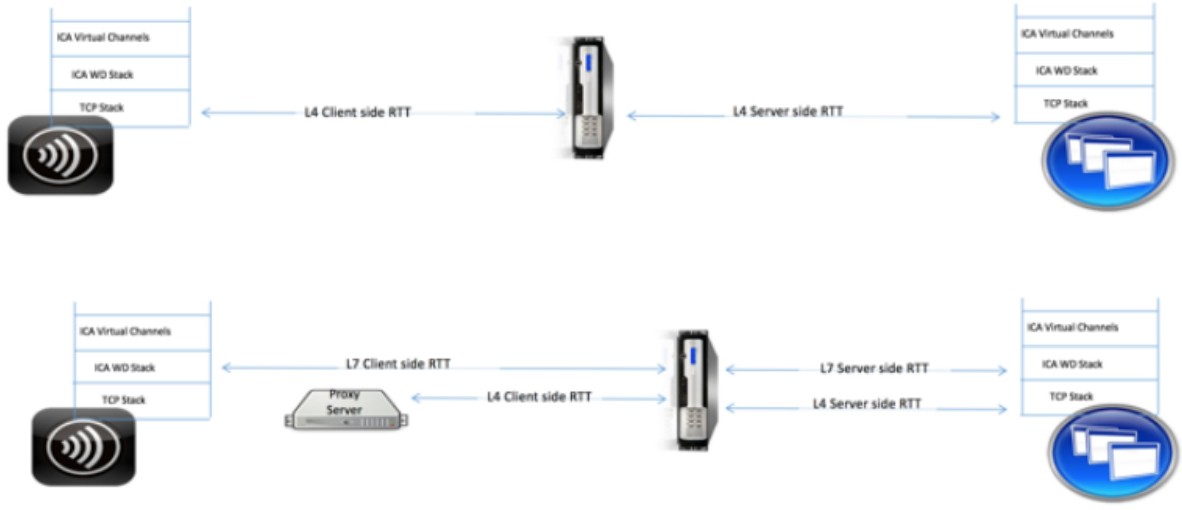


Fig 2. Deployment with TCP Proxies

ICA RTT 和 L7 延迟计算之间的区别

ICA RTT 表示从 Citrix Workspace 应用程序到 Virtual Delivery Agent (VDA) 的总往返时间。L7 延迟提供了有关客户端和服务器端延迟的详细信息。L7 客户端延迟是 Citrix Workspace 应用程序与 NetScaler Gateway 之间的延迟。L7 服务器延迟是 NetScaler Gateway 到 VDA 之间的延迟。

> 注意：仅 Citrix Virtual Apps and Desktops 7.13 及更高版本支持服务器的服务器端 L7 延迟计算。

使用 **CLI** 配置 **L7** 延迟阈值

1. 添加 ICA 延迟配置文件。

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
<!--NeedCopy-->
```

2. 添加 ICA 操作。

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. 添加 ICA 策略。

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
<!--NeedCopy-->
```

4. 将 ICA 策略绑定到 VPN 服务器或 ICA 全局绑定点。

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

或

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
<!--NeedCopy-->
```

或

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
<!--NeedCopy-->
```

参数

- 延迟监视：启用或禁用 L7 阈值监视的参数。启用此参数后，当设置的条件得到满足时，系统会向 HDX Insight 发送通知。

  默认值：已禁用

- **LatencyThresholdFactor**：活动延迟必须大于观察到的最小延迟才能得出超过阈值的结论，因此必须向 HDX Insight 发送通知的系数。

  默认值：4

  最小值：2

  最大值：65535

- **LatencyWaitTime**：设备在超过延迟阈值后等待向 HDX Insight 发送通知的时间（以秒为单位）。

  默认值：20

  最小值：1

  最大值：65535

- **LatencyNotifyInterval**：等待时间过后，设备向 HDX Insight 发送后续通知的时间间隔（以秒为单位）。

  默认值：20

  最小值：1

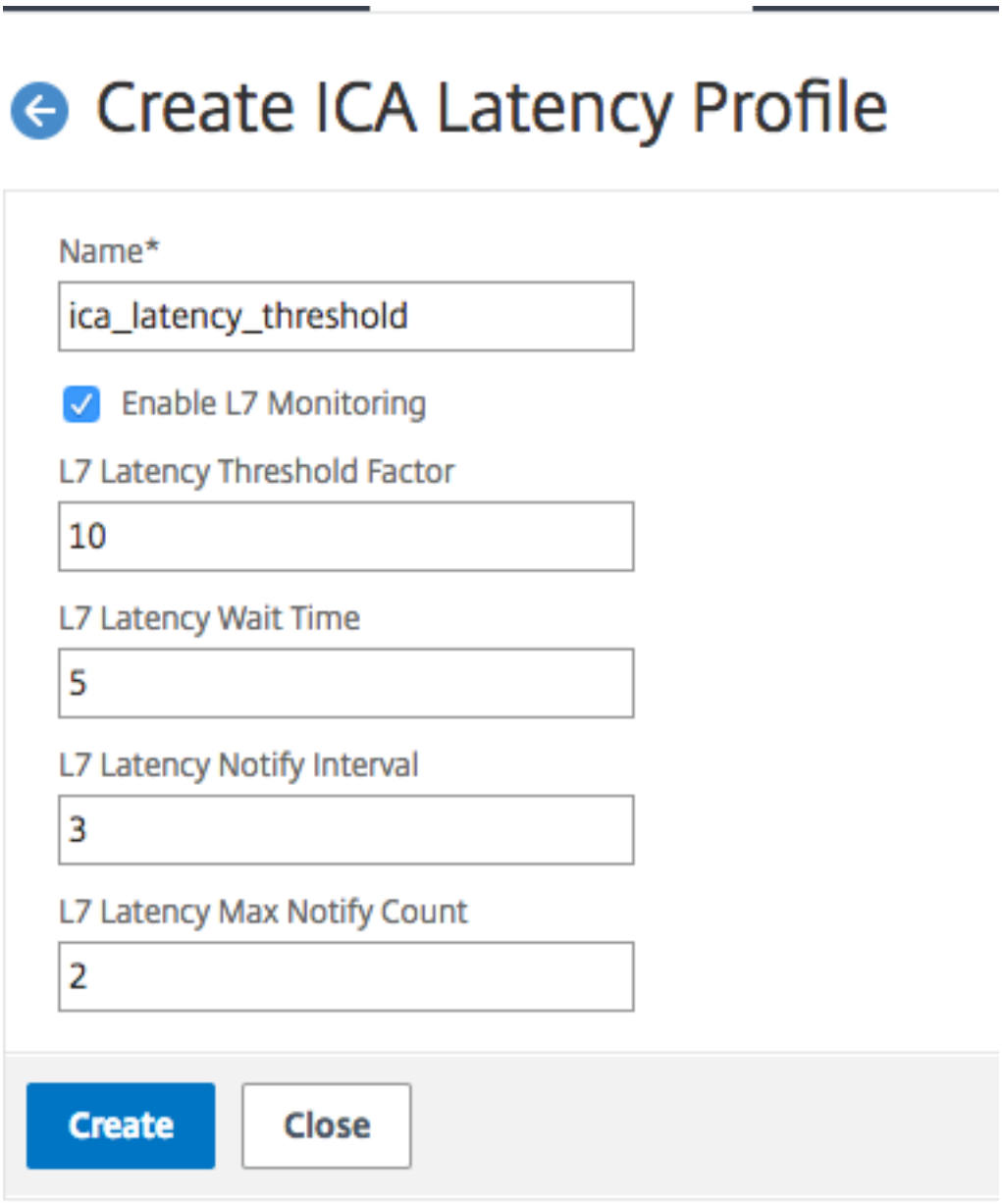
  最大值：65535

- **LatencyMaxNotifyCount**：在延迟超过阈值的时间间隔内可以发送到 HDX Insight 的最大通知数。

  默认值：5

使用 **GUI** 配置 **L7** 延迟阈值

1. 导航到 配置 > **NetScaler Gateway** > 策略 > **ICA**。
2. 选择 **ICA** 延迟配置文件 选项卡并单击 添加。
3. 在“创建 **ICA** 延迟概要文件”页中，执行以下操作。



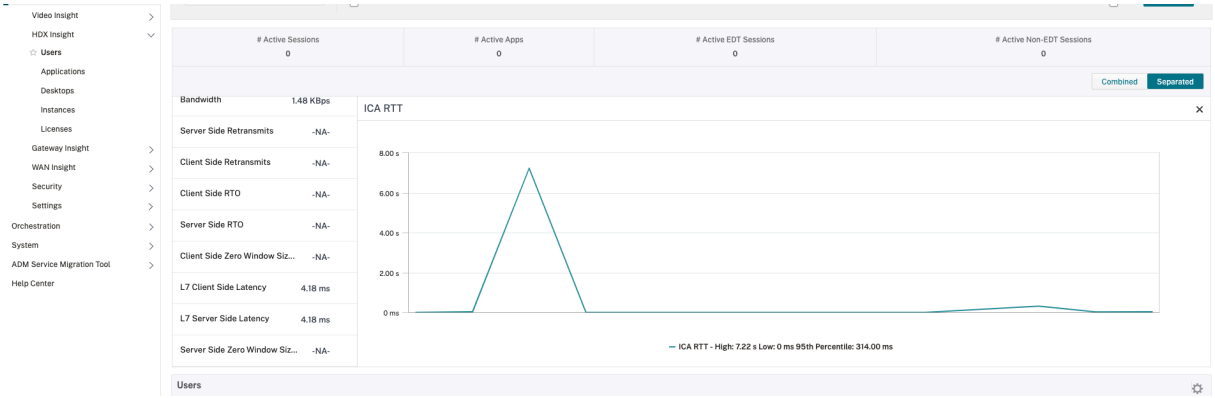
- 选择 **L7** 延迟监视 以启用 L7 阈值监视。
- 在 **L7** 阈值因素中，输入活动延迟必须超过观察到的最小延迟才能向 HDX Insight 发送通知的值。
- 在 **L7** 延迟等待时间中，输入设备在超过阈值后等待向 HDX Insight 发送通知的时间（以秒为单位）。
- 在 **L7** 延迟通知间隔中，输入设备在等待时间过后向 HDX Insight 发送后续通知的时间（以秒为单位）。
- 在 **L7** 延迟最大通知计数中，输入在延迟超过阈值的时间间隔内可以发送到 HDX Insight 的最大通知数。
  注意：超过阈值后，L7 延迟最大通知计数适用，当活动延迟低于阈值时，将重置 L7 延迟最大通知计数。这些通知的周期性受通知间隔的限制。

4. 单击创建。

> 重要：
>
> 配置 L7 延迟阈值参数后，必须配置 HDX Insight。有关详细信息，请参阅 配置 NetScaler Gateway 以支持 HDX Insight。

在 **NetScaler ADM** 中查看 **L7** 延迟参数

要在 NetScaler ADM 中查看 L7 延迟参数，请导航到 分析 **> HDX Insight >** 应用程序 或 分析 **> HDX Insight >** 用户。

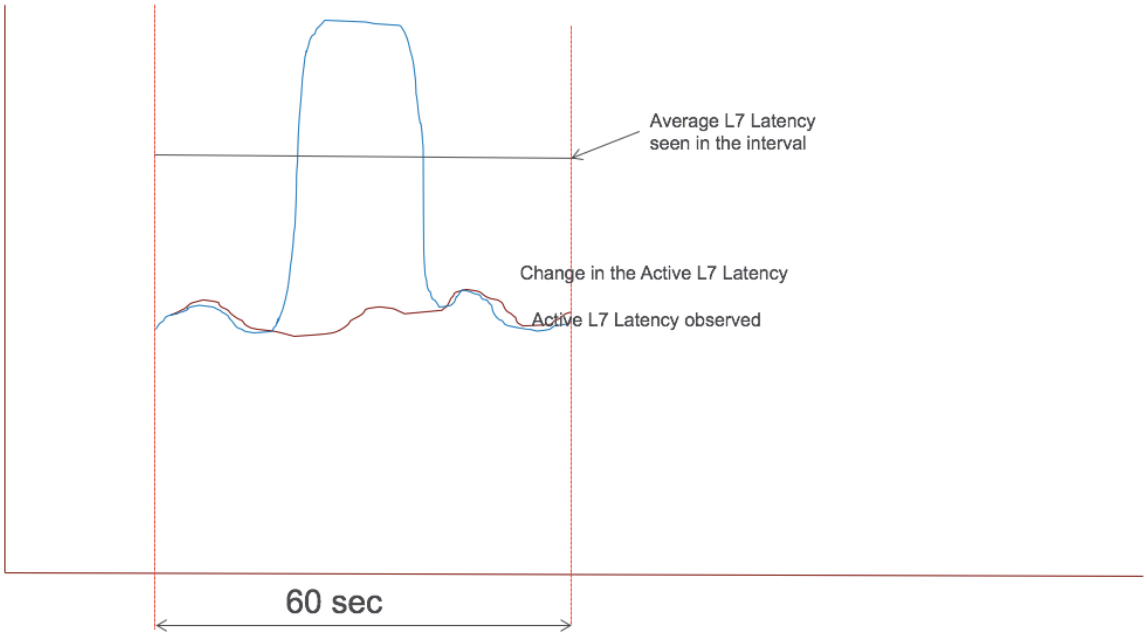


L7 延迟测量模型与 **L7** 延迟阈值报告模型的对比

L7 延迟测量模型

在 L7 延迟测量模块中，每隔 60 秒将客户端和服务器端 L7 平均延迟值发送到 HDX Insight。因此，在此间隔内看到的峰值将被平均化，因此仍未检测到。此外，L7 延迟测量模块没有实时延迟监视功能。

下图说明了一个示例 L7 延迟测量模型。

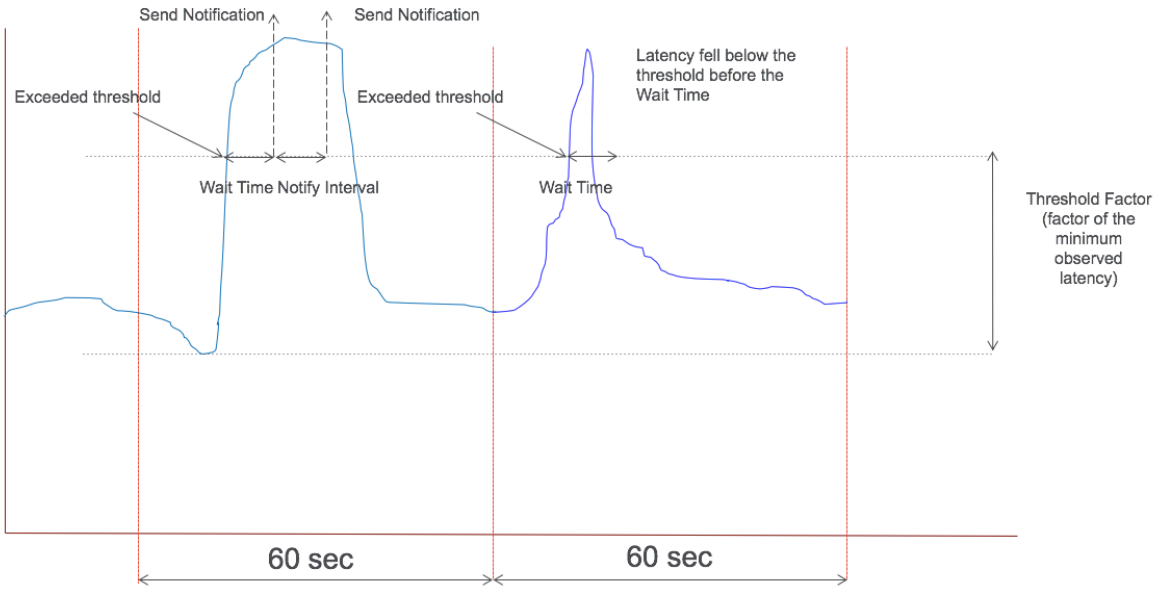


L7 延迟阈值报告模型

L7 延迟阈值报告模型具有实时延迟监视功能，可检测峰值。如果延迟超过观察到的最小延迟，则会向 HDX Insight 发送通知。

每当超过阈值系数时，都会检测到延迟增加。配置的阈值等待时间到期后，系统会向 HDX Insight 发送通知。等待时间过期且仍超出阈值系数后，会向 HDX Insight 发送后续通知。
如果在等待时间到期之前延迟值低于阈值系数，则不会向 HDX Insight 发送任何通知。

下图说明了示例 L7 延迟阈值报告模型。



可以在运行时配置以下参数：

- 阈值监视（ON/OFF）
- 阈值因素
- 阈值等待时间
- 通知间隔
- 最大通知计数

RDP 代理

February 1, 2024

RDP 代理功能作为 NetScaler Gateway 的一部分提供。在典型的部署中，RDP 客户端在远程用户的计算机上运行。NetScaler Gateway 设备部署在 DMZ 中，而 RDP 服务器场位于企业内部网络中。

远程用户；

1. 连接到 NetScaler Gateway 公有 IP 地址
2. 建立 SSL VPN 连接
3. 验证
4. 通过 NetScaler Gateway 设备访问远程桌面

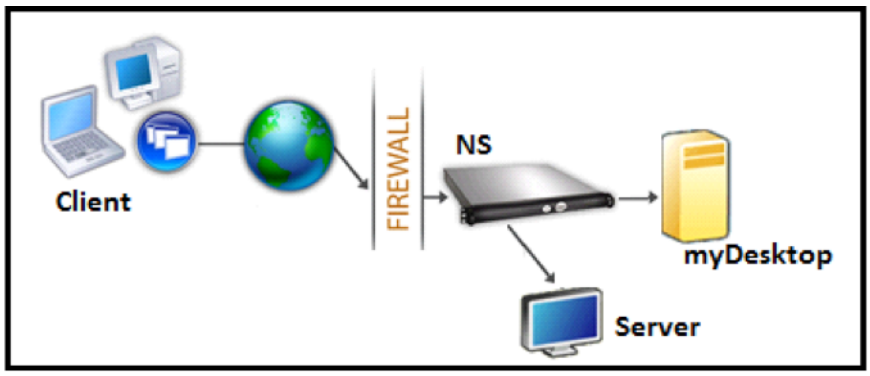
无客户端 VPN 和 ICA 代理模式支持 RDP 代理功能。

> 注意：
>
> NetScaler Gateway 不支持远程桌面会话主机 (RDSH)、远程应用程序、RDS 多用户、RDP 会话或 RDP 应用程序。

以下 RDP 代理功能提供通过 NetScaler Gateway 对远程桌面场的访问权限。

- 通过无客户端 VPN 或 ICA 代理模式（无全通道）保护 RDP 流量。
- 通过 NetScaler Gateway 访问 RDP 服务器的 SSO（单点登录）。如果需要，还提供了禁用 SSO 的选项。
- 强制（SmartAccess）功能，NetScaler 管理员可以通过 NetScaler Gateway 配置禁用某些 RDP 功能。
- 满足所有需求的单/无状态（双）网关解决方案 (VPN/ICA/RDP/Citrix Endpoint Management)。
- 与 RDP 的本机 Windows MSTSC 客户端兼容，无需任何自定义客户端。
- 在 MACOSX、iOS 和 Android 系统上使用 Microsoft 提供的现有 RDP 客户端。

下图描述了部署的概述：



通过无客户端 **VPN** 进行部署

在此模式下，RDP 链接通过 `add vpn url` 配置或通过外部门户以书签形式发布在 Gateway 主页或门户上。用户可以单击这些链接以访问远程桌面。

通过 **ICA** 代理进行部署

在此模式下，使用 `wihome` 参数在 Gateway VIP 上配置自定义主页。可以使用允许用户访问的远程桌面资源列表自定义此主页。此自定义页面可以托管在 NetScaler 上，或者如果是外部的，则可以是现有网关门户页面中的 iFrame。

在任一模式下，用户单击预配置的 RDP 链接或图标后，对应资源的 HTTPS 请求将到达 NetScaler Gateway。网关为请求的连接生成 RDP 文件内容并将其推送到客户端。调用本机 RDP 客户端，并连接到 Gateway 上的 RDP 侦听器。网关通过支持强制执行 (SmartAccess) 对 RDP 服务器执行单点登录。网关会根据 NetScaler 配置阻止客户端访问某些 RDP 功能，然后在 RDP 客户端和服务器之间代理 RDP 流量。

执法细节

NetScaler 管理员可以通过 NetScaler Gateway 配置配置某些 RDP 功能。NetScaler Gateway 为重要的 RDP 参数提供了“RDP 强制”功能。NetScaler 可确保客户端无法启用阻止的参数。如果启用了阻止的参数，则 RDP 强制功能将取代启用客户端的参数，并且不支持这些参数。

> 重要：强制功能仅在启用 SSO 的情况下适用。

用于实施的支持的 **RDP** 参数

支持强制执行以下重定向参数。这些参数可作为 RDP 客户端配置文件的一部分进行配置。

- 剪贴板的重定向
- 重定向打印机
- 磁盘驱动器的重定向
- COM 端口的重定向
- PNP 设备的重定向

连接流程

连接流程可分为两个步骤：

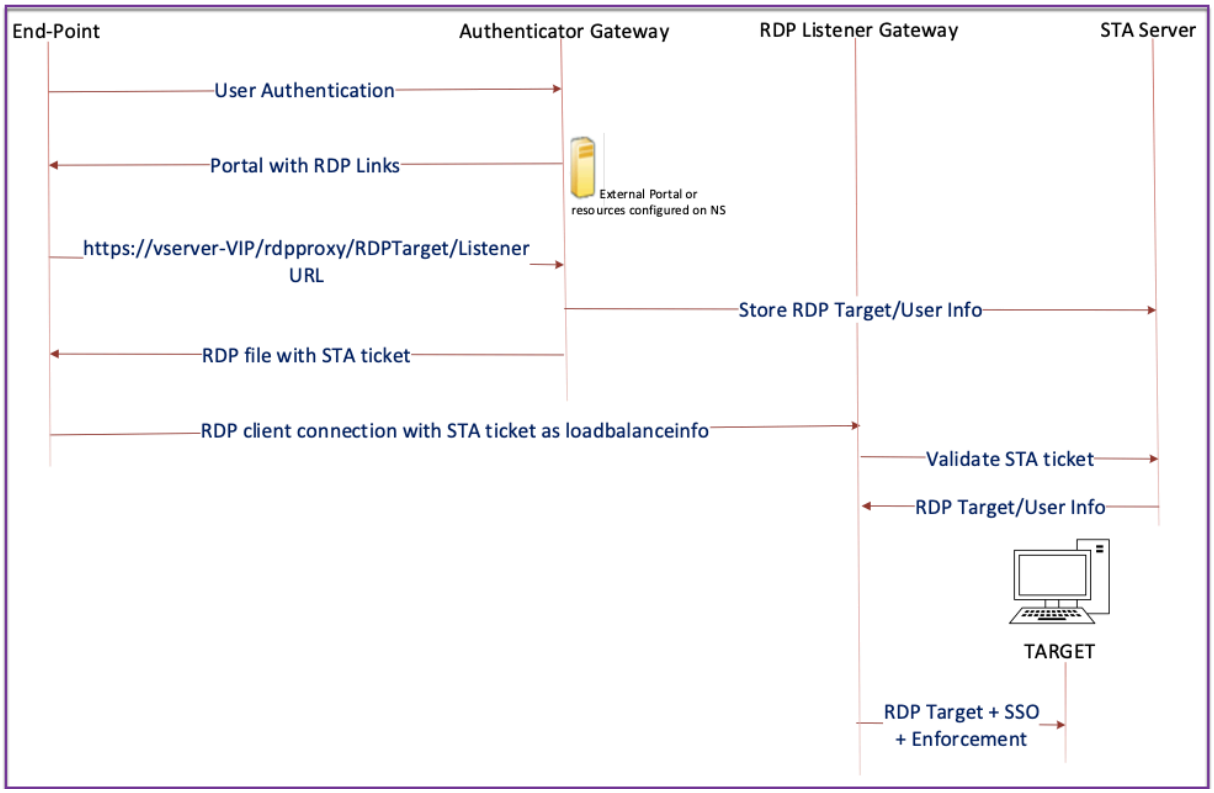
- RDP 资源枚举和 RDP 文件下载。
- RDP 连接启动。

基于上述连接流程，有两种部署解决方案：

- 无状态（双）网关解决方案-RDP 资源枚举和 RDP 文件下载通过身份验证器网关进行，但 RDP 连接启动通过 RDP 侦听器网关进行。
- 单一网关解决方案-RDP 资源枚举、RDP 文件下载和 RDP 连接启动通过同一网关进行。

无状态（双）网关兼容性

下图描述了部署情况：



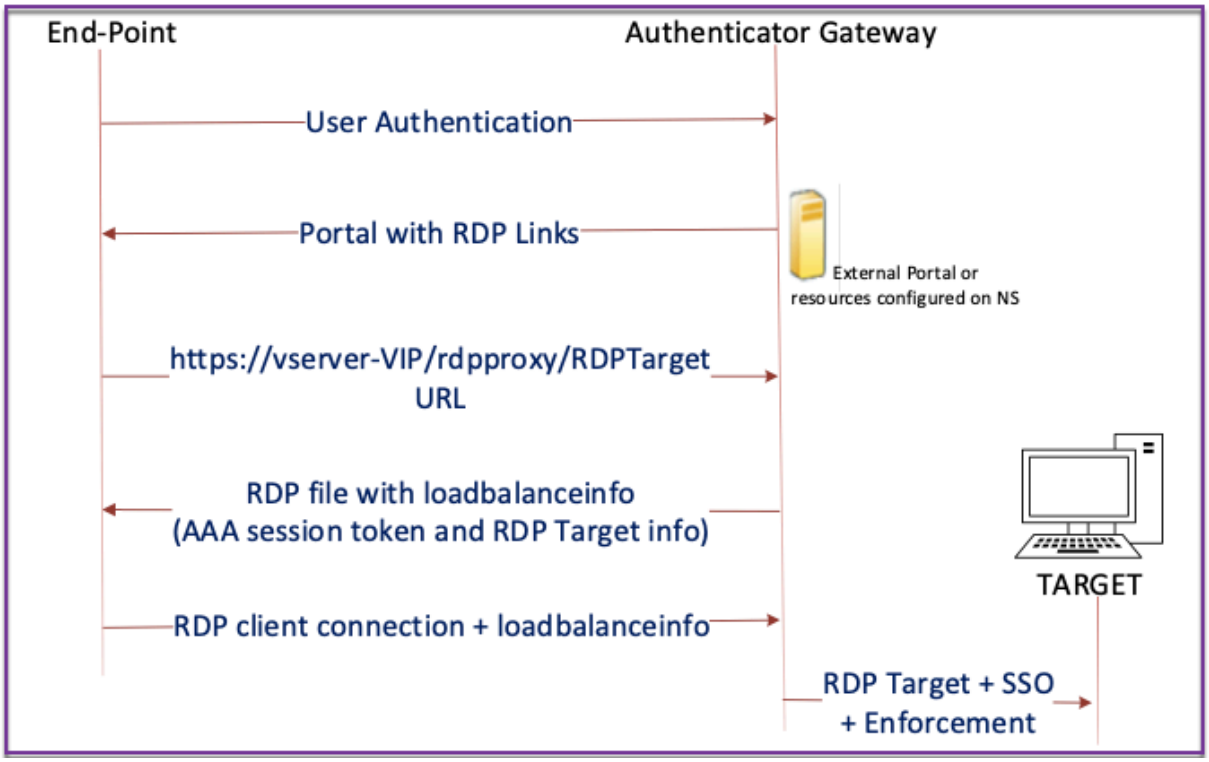
- 用户连接到身份验证器网关 VIP 并提供凭据。
- 成功登录网关后，用户将被重定向到主页或外部门户，其中枚举了用户可以访问的远程桌面资源。
- 用户选择 RDP 资源后，Authenticator Gateway VIP 将以指示用户单击的已发布资源的格式 `https://vserver-vip/rdpproxy/rdptarget/listener` 接收请求。此请求包含有关用户选择的 RDP 服务器的 IP 地址和端口的信息。
- 身份验证器网关处理 /rdpproxy/ 请求。由于用户已经通过身份验证，因此此请求附带有有效的 Gateway cookie。
- `RDPTarget` 和 `RDPUser` 信息存储在 STA 服务器上，然后生成 STA 票证。使用配置的预共享密钥对存储在 STA 服务器上的信息进行加密。身份验证器网关使用在网关虚拟服务器上配置的 STA 服务器之一。
- 在 /rdpproxy/ 请求中获取的“侦听器”信息将作为“`fulladdress`”放置到 `.rdp file` 中，STA 票证（预先附有 STA AuthID）将作为 `loadbalanceinfo` 放置到 `.rdp file` 中。
- 将 `.rdp file` 发送回客户端端点。
- 本机 RDP 客户端启动并连接到 `RDPListener Gateway`。它在初始数据包中发送 STA 票证。

  `RDPListener` 网关验证 STA 票证并获取 `RDPTarget` 和 `RDPUser` 信息。要使用的 STA 服务器是通过使用中存在的“AuthID”来检索的 `loadbalanceinfo`。
- 创建网关会话用于存储授权/审核策略。如果用户存在会话，则会重复使用该会话。
- `RDPListener` 网关使用 CREDSSP 连接到 `RDPTarget` 和单点登录。

> 重要提示：
>
> - 对于无状态 RDP 代理，STA 服务器会验证 RDP 客户端发送的 STA 票证以获取 RDPTarget/RDPUser 信息。除了 VPN 虚拟服务器之外，还必须绑定 STA 服务器。

单 **Gateway** 兼容性

下图描述了部署情况：



> 重要：
>
> 在单个网关部署的情况下，不需要 STA 服务器。身份验证器网关对 RDPTarget 和 NetScaler 身份验证、授权和审核会话 Cookie 进行安全编码，并将其作为 .rdp file 中的 loadbalanceinfo 发送。当 RDP 客户端在初始数据包中发送此令牌时，身份验证器网关将解码 RDPTarget 信息、查找会话并连接到 RDPTarget。

支持单个监听器

- RDP 和 SSL 流量的单个侦听器。
- 可以通过 NetScaler 设备上的相同 2 个元组（即 IP 和端口）处理 RDP 文件下载和 RDP 流量。

RDP 代理的许可证要求

高级版、高级版

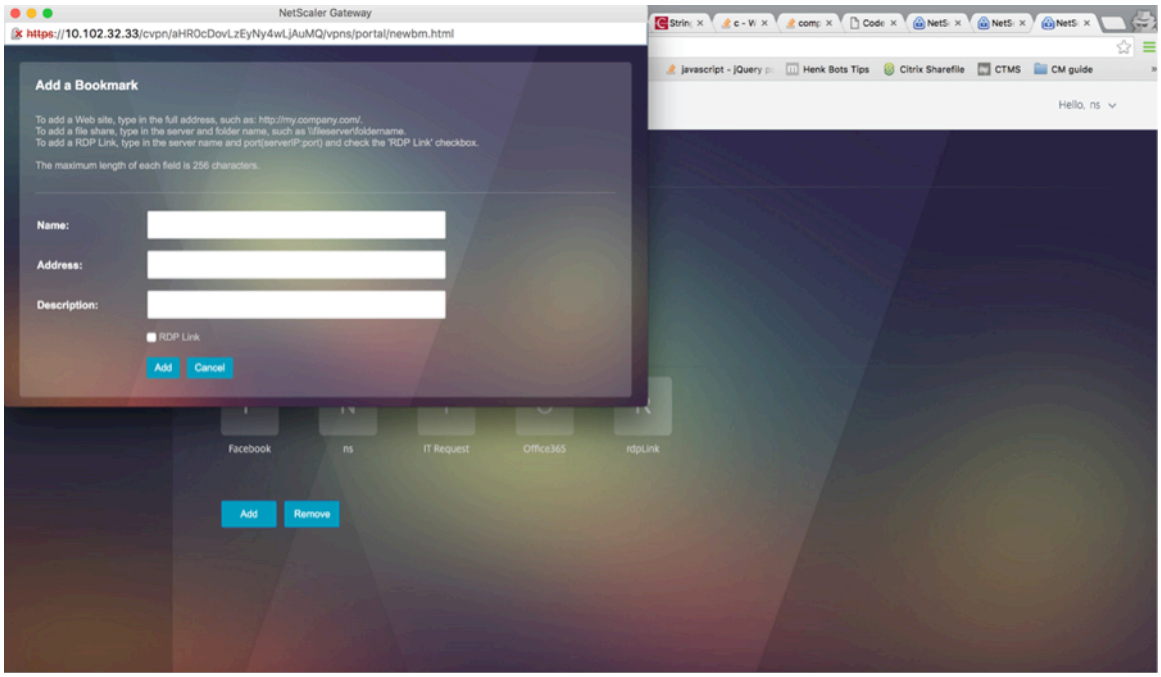
> 注意：
>
> 只有 Gateway 平台许可证或只有标准版的客户不能使用 RDP 代理功能。

您可以使用以下命令启用 RDP 代理。

```
enable feature rdpProxy
<!--NeedCopy-->
```

书签

通过门户生成 **RDP** 链接。您可以通过提供为用户提供生成自己的 URL 的选项，而不是为用户配置 RDP 链接或通过外部门户发布 RDP 链接 `targerIP:Port`。对于无状态的 RDP 代理部署，管理员可以将 RDP 侦听器信息包含在 FQDN: Port 格式中，作为 RDP 客户端配置文件的一部分。这是在 `rdpListener` 选项下完成的。此配置用于在双网关模式下通过门户生成 RDP 链接。



创建书签

1. 在门户页面上创建书签以访问 RDP 资源：（ActualURL 以 `rdp://`开头）。
2. Add VPN url <urlName> <linkName> <actualURL>
    - URL 必须采用以下格式：`rdp://<TargetIP:Port>`。

- 对于无状态 RDP 代理模式，URL 必须采用以下格式：`rdp://<TargetIP:Port>/<ListenerIP:Port>`
- URL 在门户上发布的格式如下：
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. 将书签绑定到用户、组、VPN 虚拟服务器或 VPN 全局。

要为 **RDP Proxy** 启用的功能和模式

```
- enable ns feature ssl

- enable ns feature sslvpn

- enable ns feature rdpproxy

- enable mode usnip
<!--NeedCopy-->
```

RDP Proxy 高级配置步骤

无状态 RDP 代理配置中涉及的以下高级步骤。

- 创建 RDP 服务器配置文件
- 创建 RDP 客户端配置文件
- 创建并绑定虚拟服务器
- 创建书签
- 创建或编辑会话配置文件或策略
- 绑定书签

配置客户端配置文件

在身份验证器网关上配置客户端配置文件。以下是示例配置：

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as 'fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
```



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

将 RDP 客户端配置文件与 VPN 虚拟服务器关联。

这可以通过配置会话操作 + 会话策略或通过设置全局 VPN 参数来完成。

示例：

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

或者

```
set vpn parameter  - rdpClientprofile <name>
<!--NeedCopy-->
```

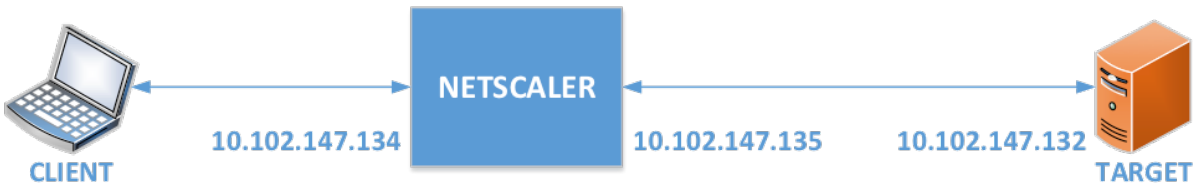
配置服务器配置文件

在监听器网关上配置服务器配置文件。

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
    listener> -rdpPort <port for terminating RDP client connections> -
    psk <key to decrypt RDPTarget/RDPUser information, needed while
    using STA>`
<!--NeedCopy-->
```

`rdp ServerProfile` 必须在 VPN 虚拟服务器上配置。

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
    rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```



使用 **CLI** 配置 **RDP** 代理

以下是使用 CLI 进行的 RDP 代理配置示例。

- 为用户添加包含目标信息的 VPN URL。


```
add aaa user Administrator  -password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   -urlName rdp
<!--NeedCopy-->
```

- 为 VPN 连接配置 RDP 客户端和服务器配置文件。

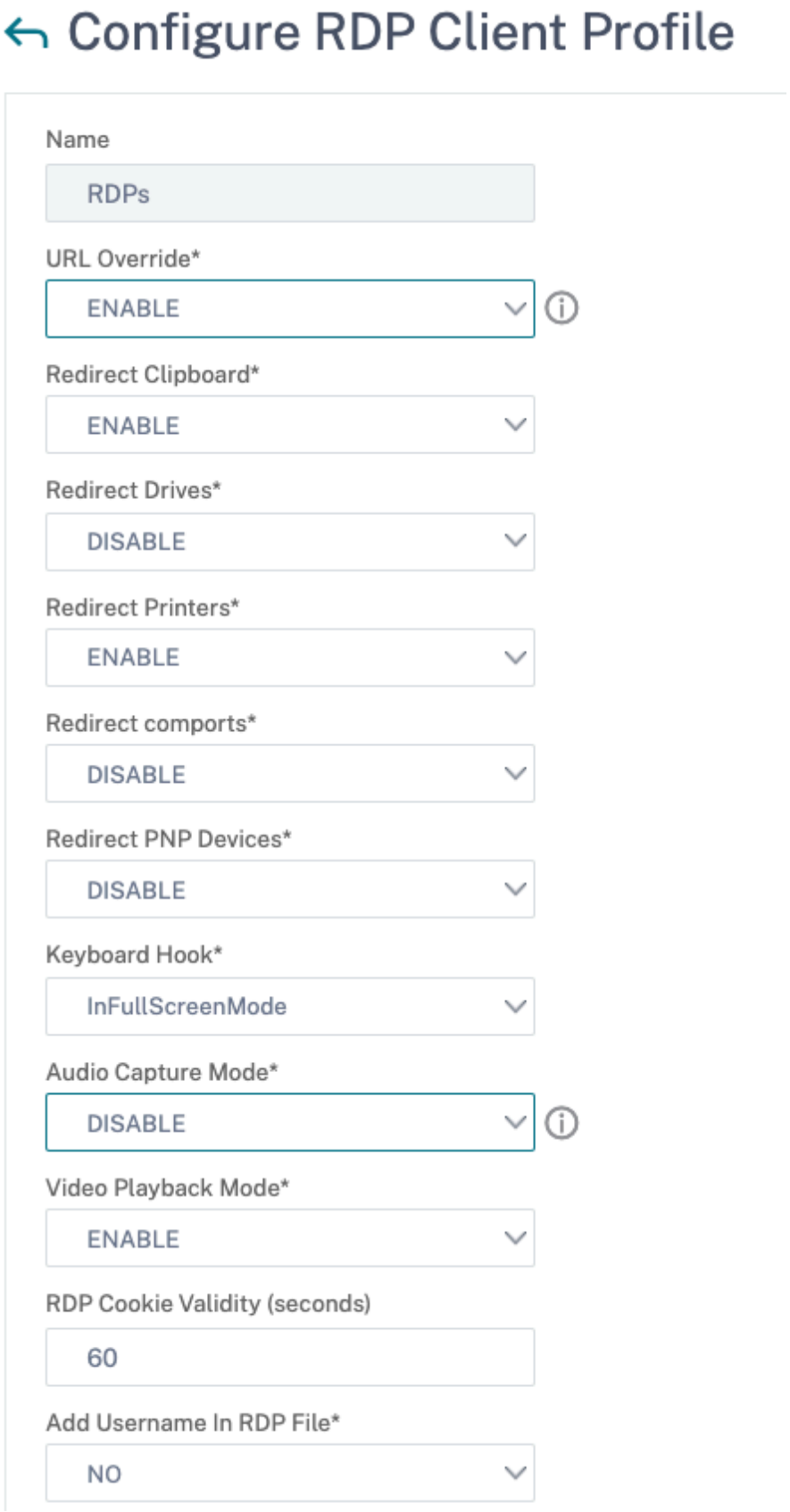
```
add rdp clientprofile p1  -psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  -
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

- 添加用于从 NetScaler 到目标的连接的 SNIP。

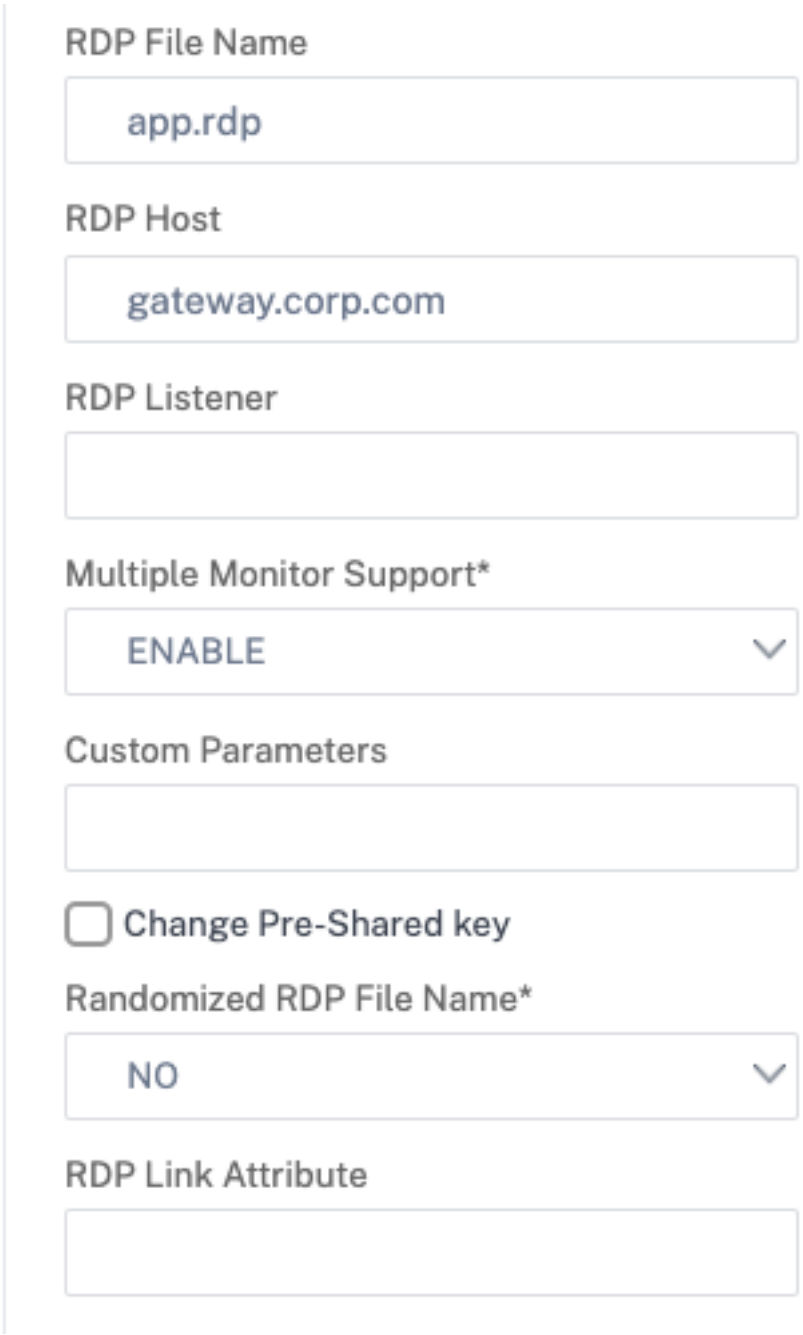
```
add ns ip 10.102.147.135  255.255.255.0  -type SNIP
<!--NeedCopy-->
```

使用 **GUI** 进行 **RDP** 代理配置

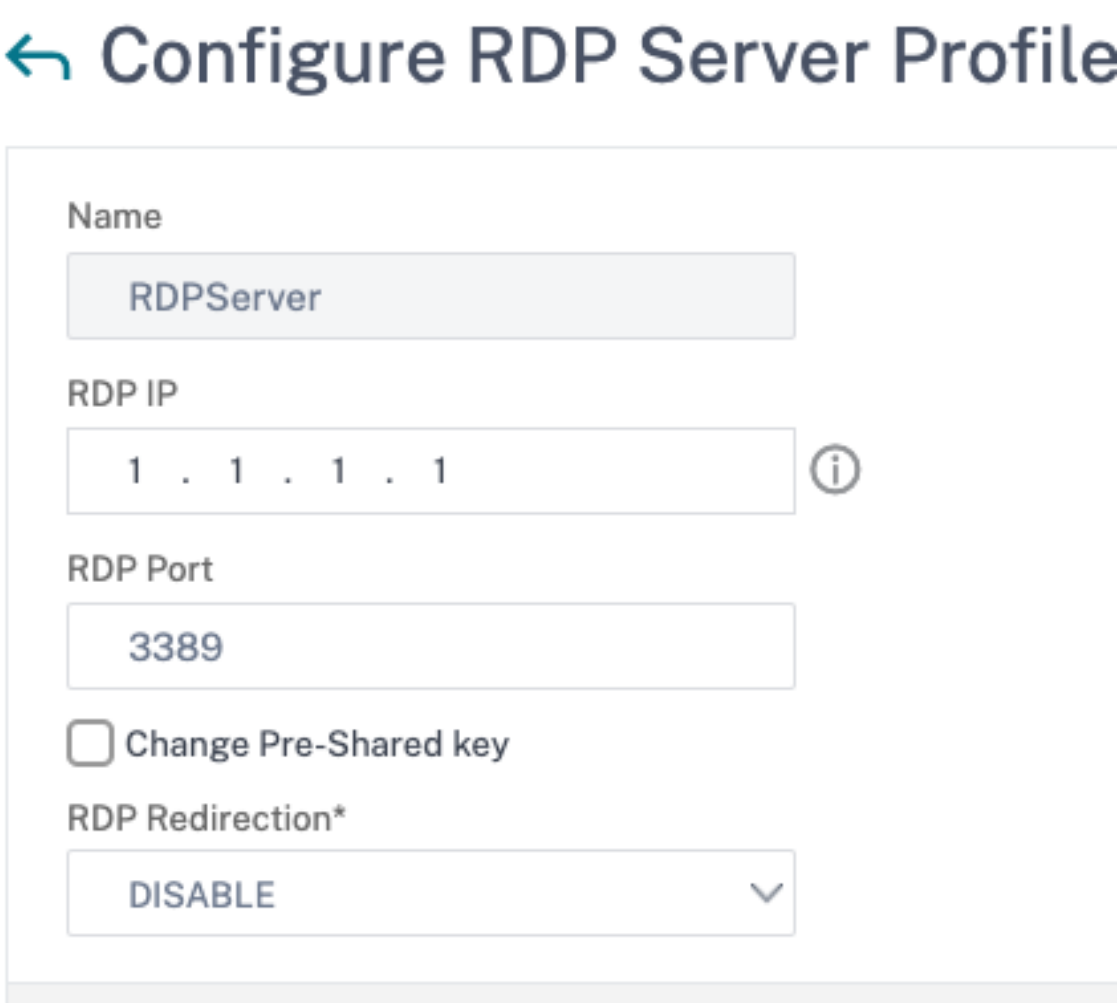
1. 导航到 **NetScaler Gateway >** 策略，右键单击 **RDP**，然后单击 启用功能。
2. 单击导航窗格上的 RDP。在右侧，选择 客户端配置文件 选项卡，然后单击 添加。
3. 输入客户端配置文件的名称和名称，然后对其进行配置。



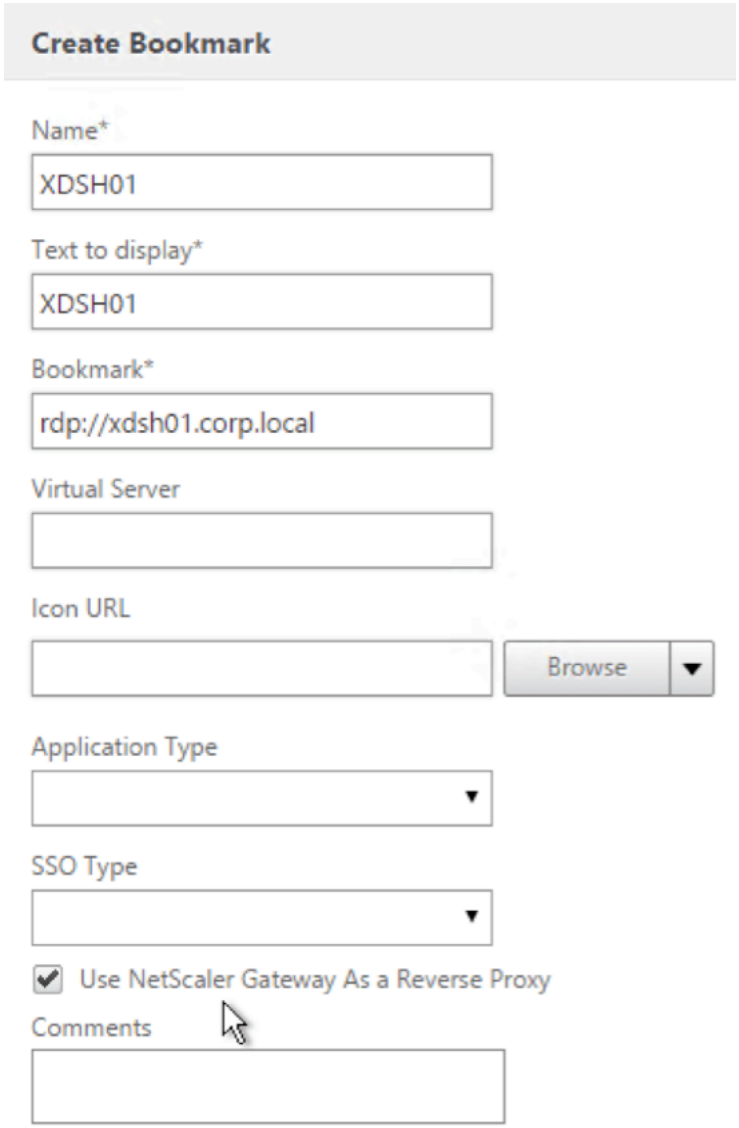
4. 在 “RDP 主机” 字段中，输入解析为 RDP 代理侦听器的 FQDN，该侦听器的 FQDN 通常与 NetScaler Gateway 设备的 FDQN 相同。
5. 在 预共享密钥中，输入密码，然后单击 确定。



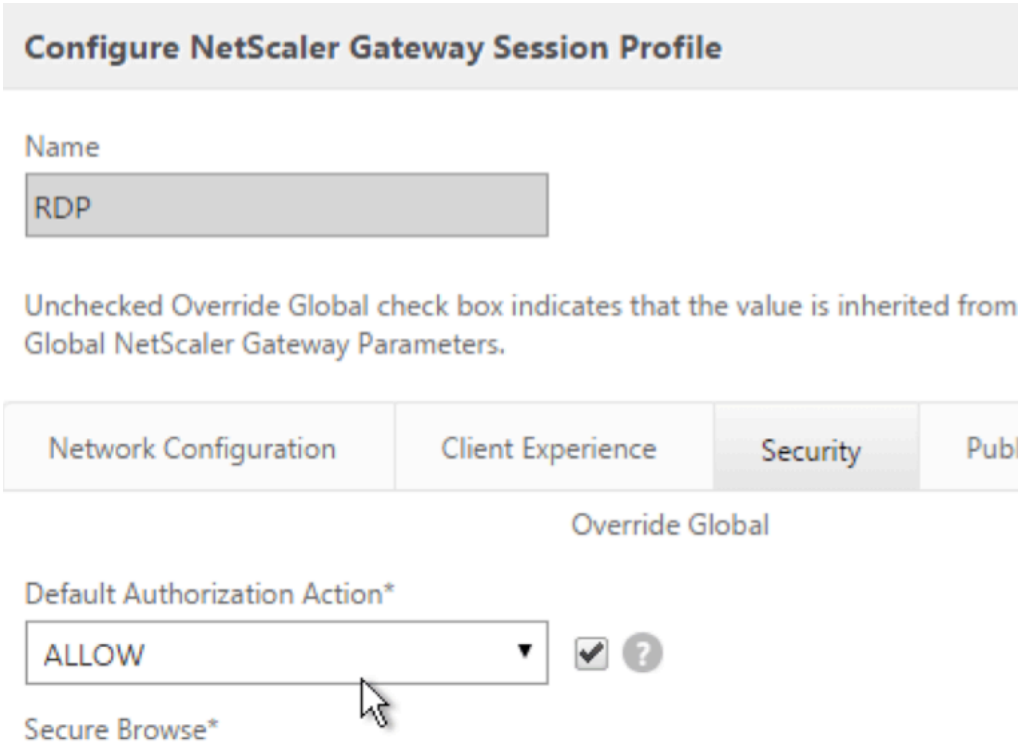
6. 输入服务器配置文件的名称。
7. 输入要绑定此配置文件的网关虚拟服务器的 IP 地址。
8. 输入为 RDP 客户端配置文件配置的相同预共享密钥。单击创建。



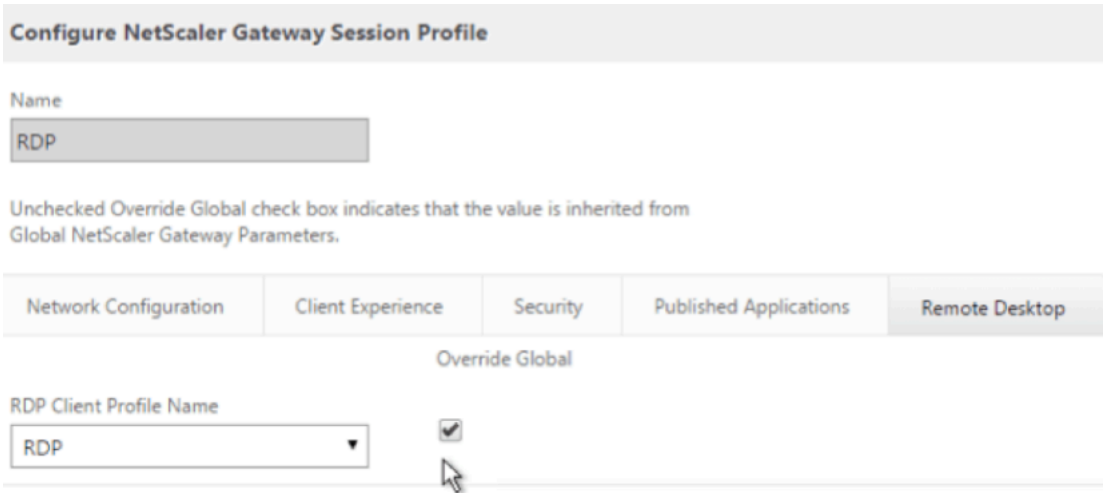
9. 如果要在无客户端访问门户页面上添加 RDP 书签，请在左侧展开 **NetScaler Gateway**，展开 资源，然后单击 书签。
10. 在右侧，单击 添加。
11. 给书签起个名字。
12. 对于 URL，请使用 **IP** 或 **DNS** 输入 **rdp://MyRDPServer**。
13. 选择 将 **NetScaler Gateway** 用作反向代理，然后单击 创建。
14. 根据您的要求创建书签。



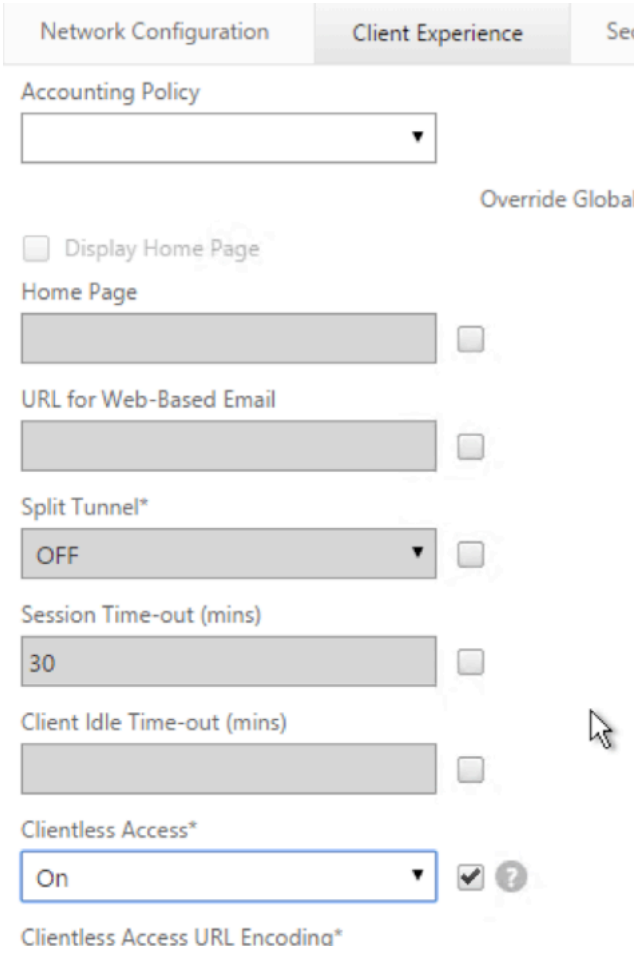
15. 创建或编辑会话配置文件。导航到 **NetScaler Gateway >** 策略 **>** 会话。
16. 在安全选项卡上，将 默认授权操作 设置为 允许。或者，您可以使用授权策略来控制访问权限。



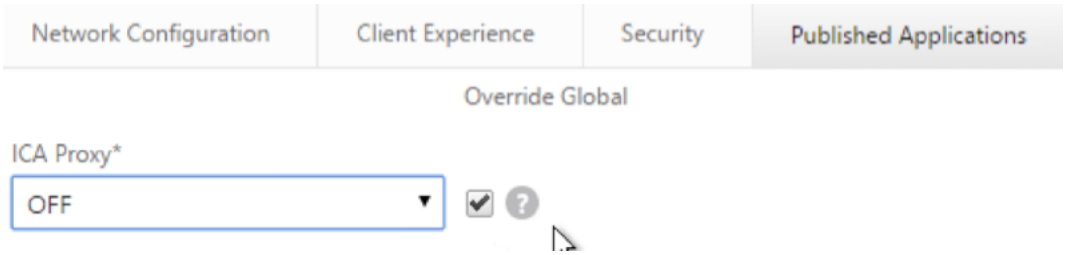
17. 在远程桌面选项卡上，选择您之前创建的 RDP 客户端配置文件。



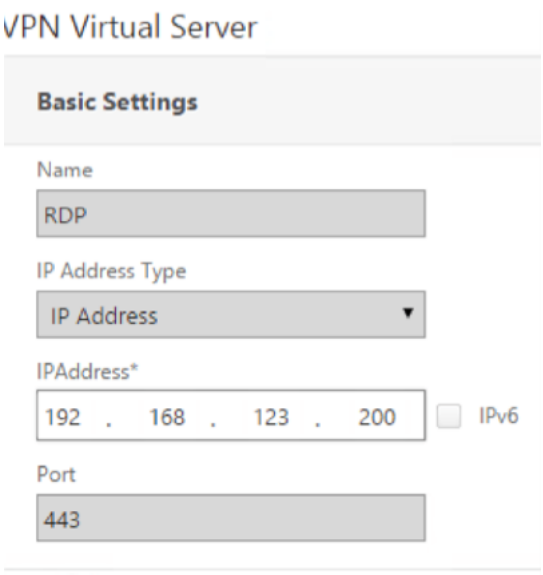
18. 如果要使用书签，请在“客户端体验”选项卡上，将“无客户端访问”设置为“开”。



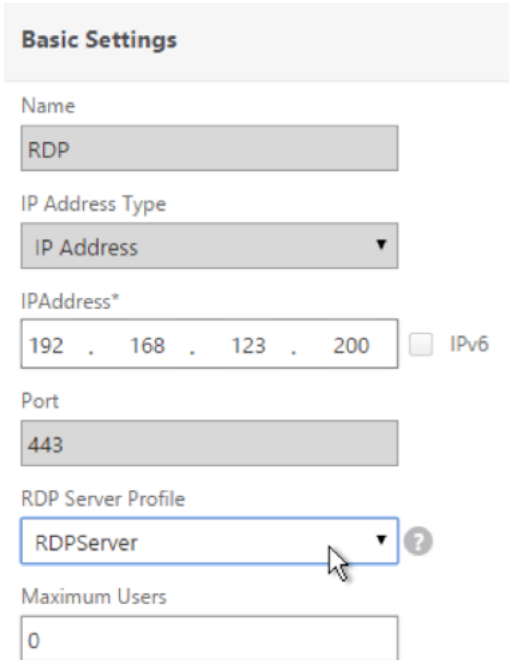
19. 在“已发布的应用程序”选项卡上，确保 ICA 代理处于 关闭状态。



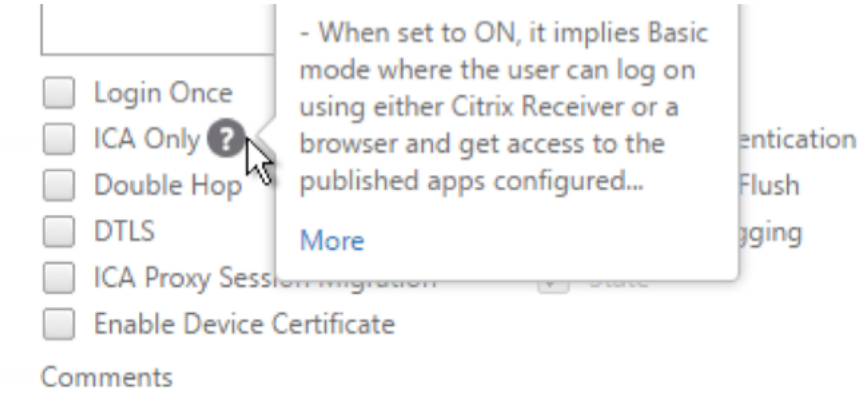
20. 修改或创建网关虚拟服务器。
21. 在“基本设置”部分中，单击“更多”。



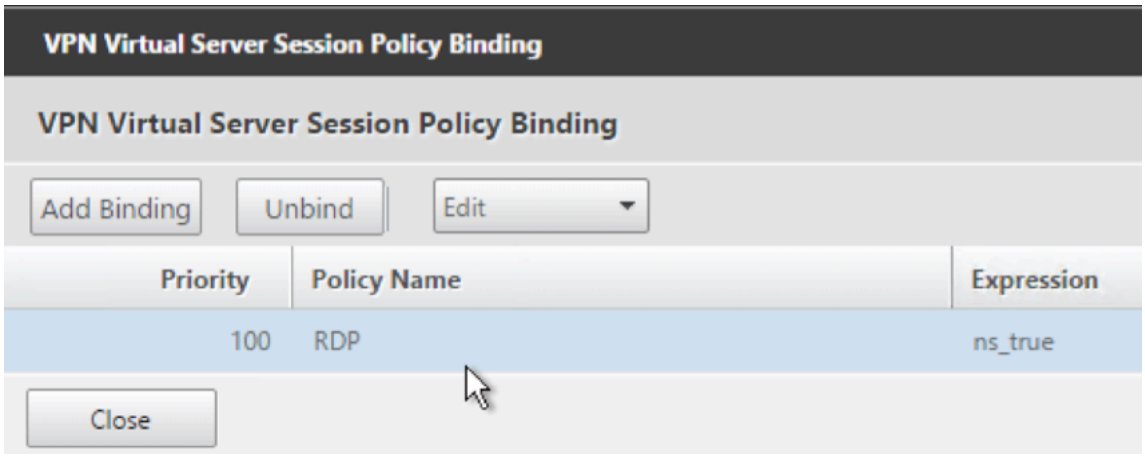
22. 使用 RDP 服务器配置文件列表选择您之前创建的 RDP 服务器配置文件。



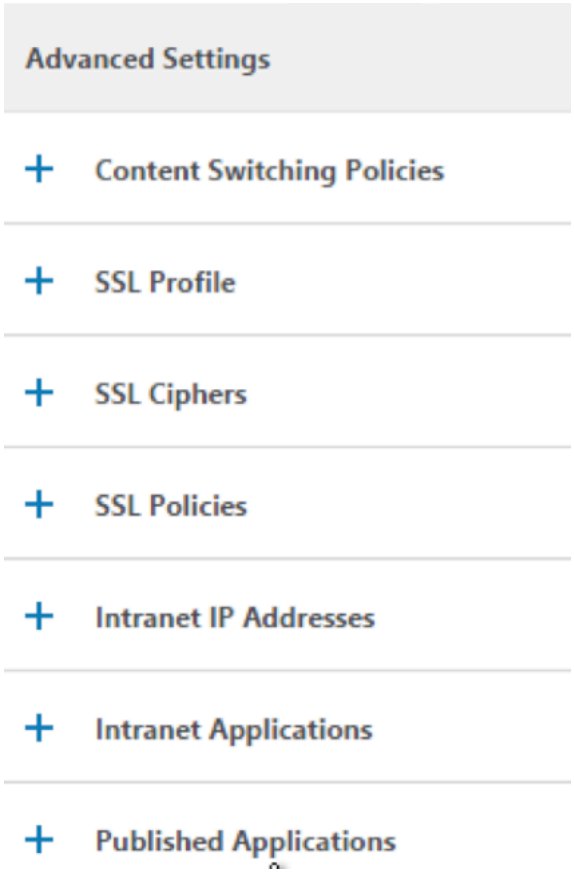
23. 向下滚动。确保未选中“仅 **ICA**”。



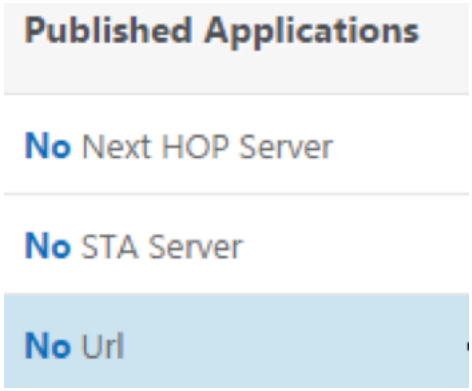
24. 绑定证书。
25. 绑定身份验证策略。
26. 绑定配置了 RDP 客户端配置文件的会话策略/配置文件。



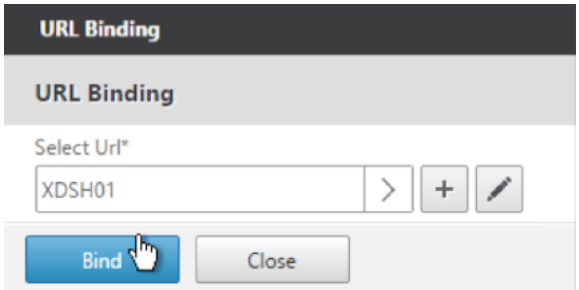
27. 您可以将书签绑定到 NetScaler Gateway 虚拟服务器或身份验证、授权和审核组。要绑定到 NetScaler Gateway 虚拟服务器，请在右侧的“高级设置”部分中单击 已发布的应用程序。



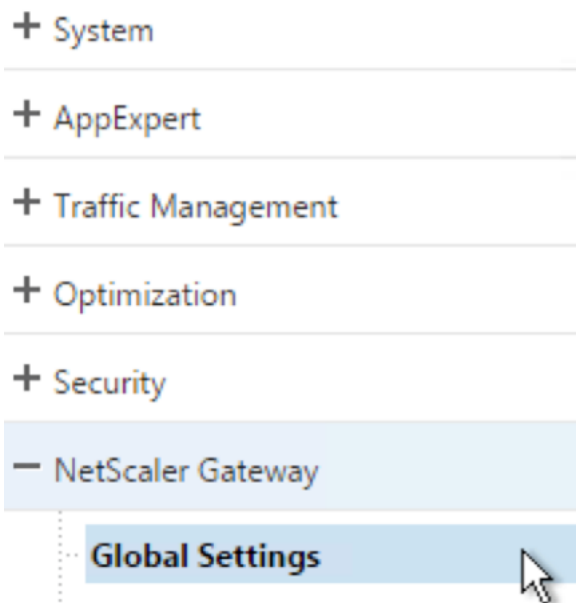
28. 在左侧的“已发布的应用程序”部分中，单击“无 **URL**”。



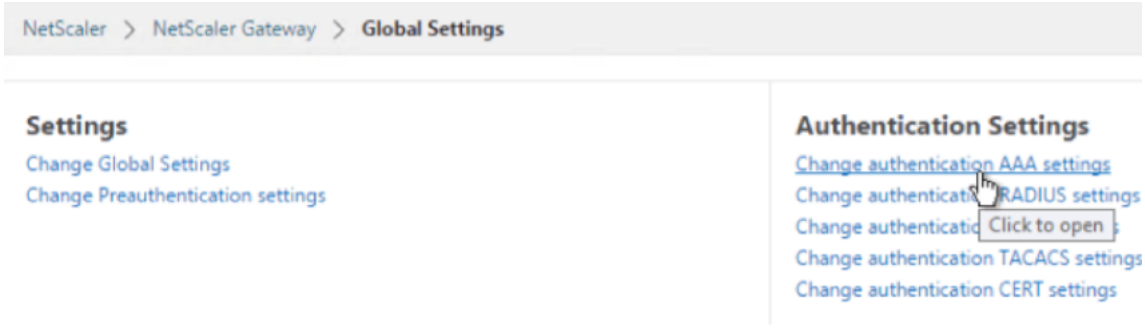
29. 绑定您的书签。



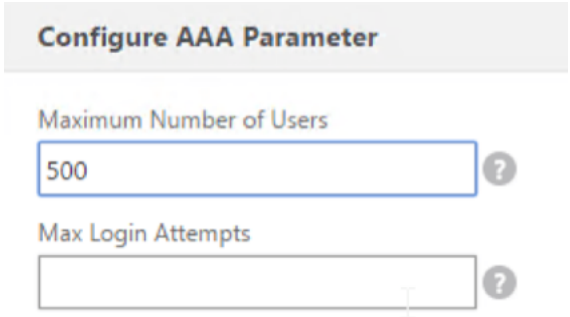
30. 由于未为此 NetScaler Gateway 虚拟服务器指定仅 ICA，因此请确保正确配置了 NetScaler Gateway 通用许可证。在左侧，展开 **NetScaler Gateway** ，然后单击 全局设置。



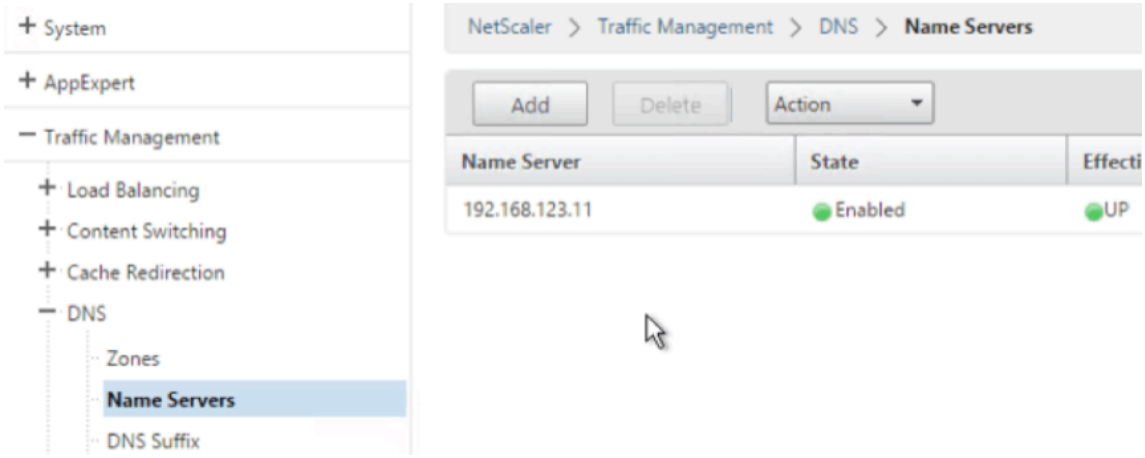
31. 在右侧，单击 更改身份验证 **AAA** 设置。



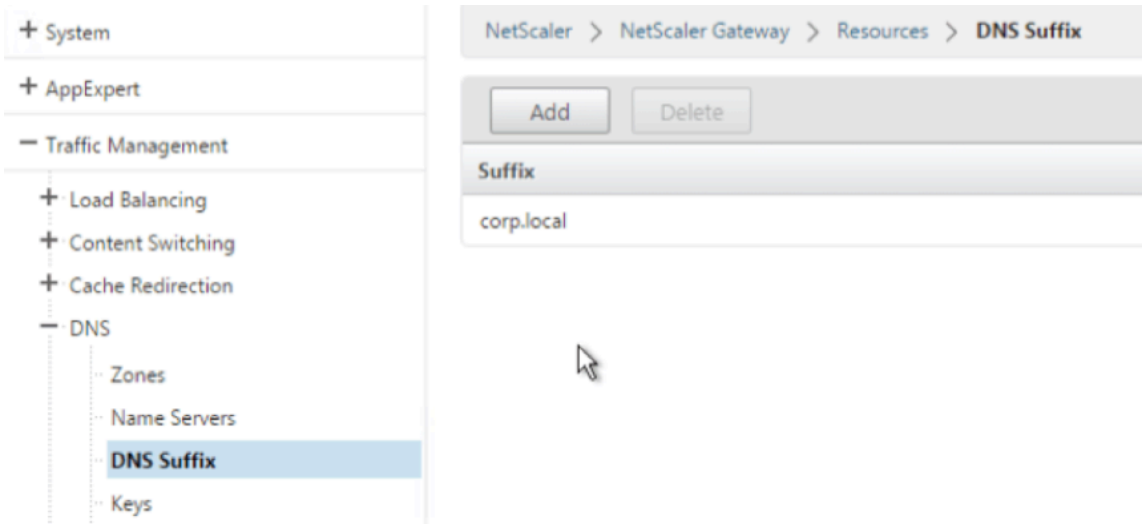
32. 将 最大用户数 更改为许可限制。



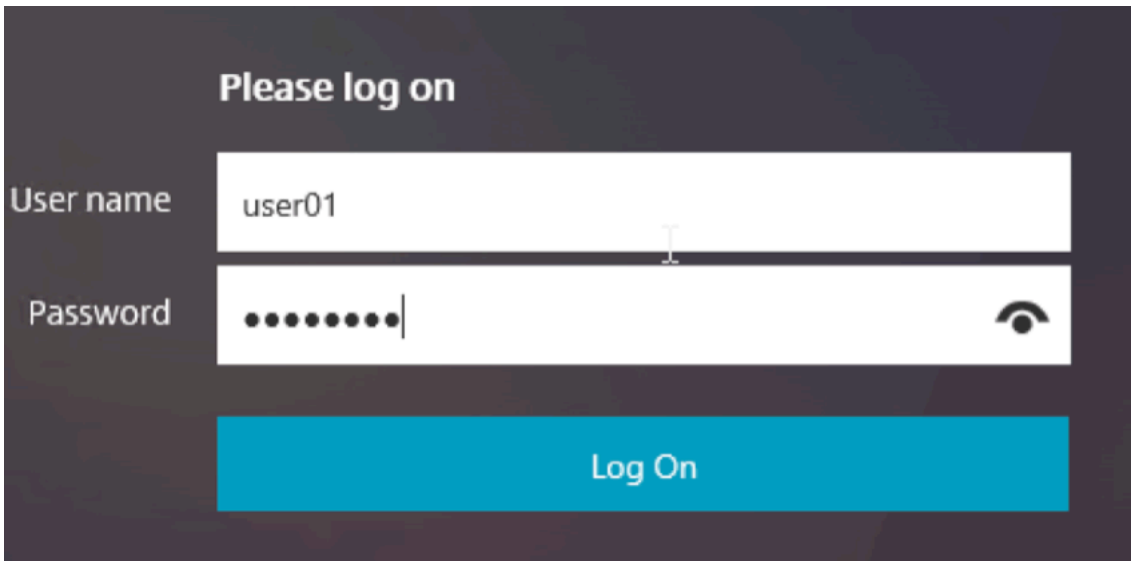
33. 如果要使用 DNS 连接到 RDP 服务器，请确保在设备上配置了 DNS 服务器（流量管理 **> DNS >** 名称服务器）。



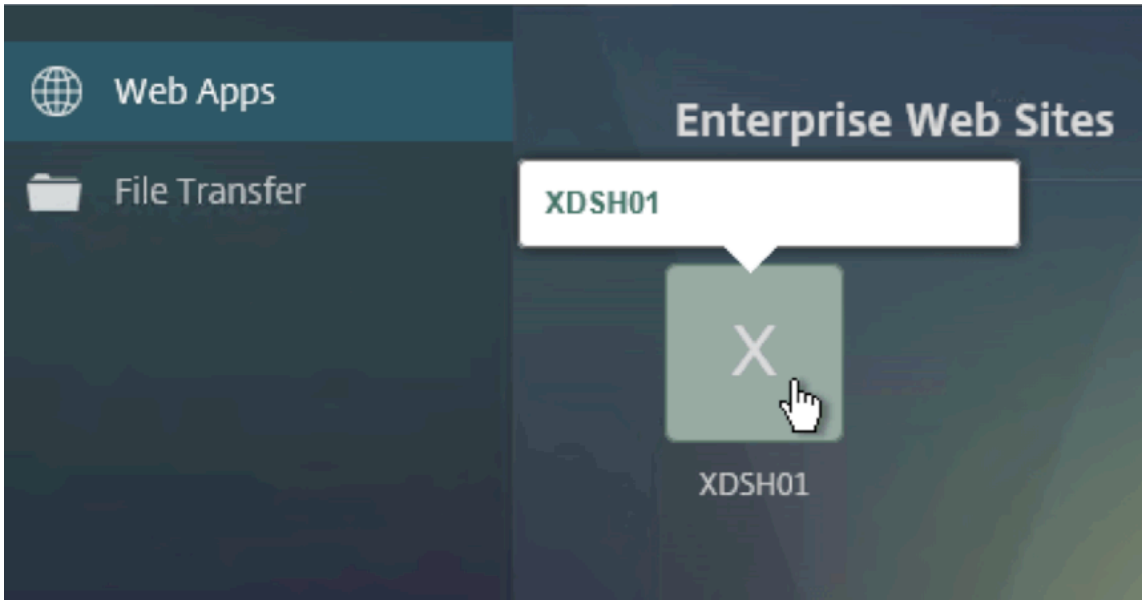
34. 如果要使用短名称而不是 FQDN，请添加 **DNS** 后缀（流量管理 **> DNS > DNS** 后缀）。



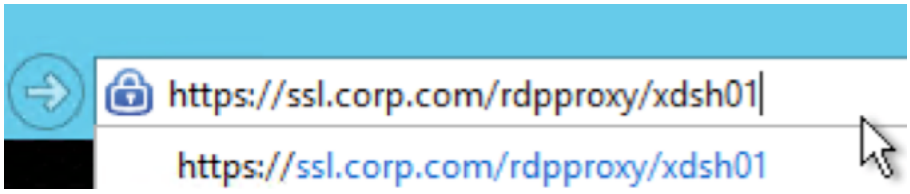
35. 连接到网关并登录。



36. 如果已配置 书签，请单击书 签。

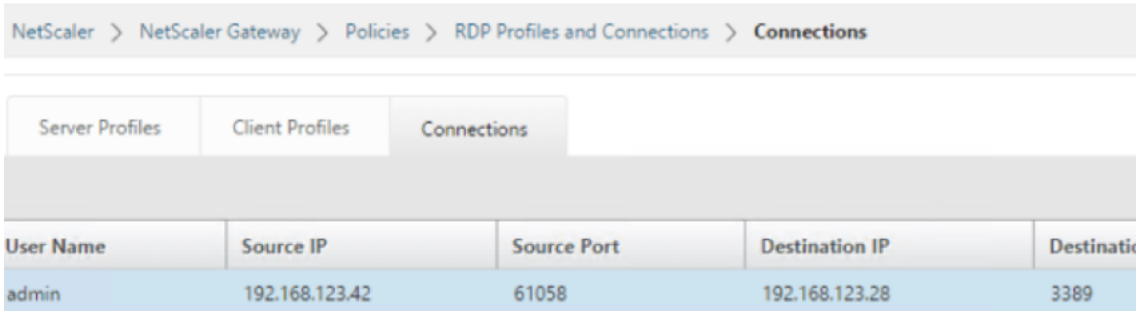


37. 您可以将地址栏更改为 **/rdpproxy/MyRDPServer**。您可以输入 IP 地址（例如 rdpproxy /192.168.1.50）或 DNS 名称（/rdpproxy /myserver）。



38. 打开下载的 `.rdp file`。

39. 您可以通过转到 **NetScaler Gateway** 策略 **> RDP** 来查看当前连接的用户。右侧是“连 接”选项卡。



禁用 **SSO** 的选项

可以通过配置 NetScaler 流量策略来禁用带有 RDP 代理的 SSO（单点登录）功能，以便始终提示用户输入凭据。禁用 SSO 后，RDP 强制 (SmartAccess) 将不起作用。

示例：

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

可以根据要求配置流量策略，以下是两个示例：

- 要为所有流量禁用 SSO：

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
   " <TrafficActionName>
<!--NeedCopy-->
```

- 基于源/目标 IP/FQDN 禁用 SSO

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
   ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

无状态 **RDP** 代理

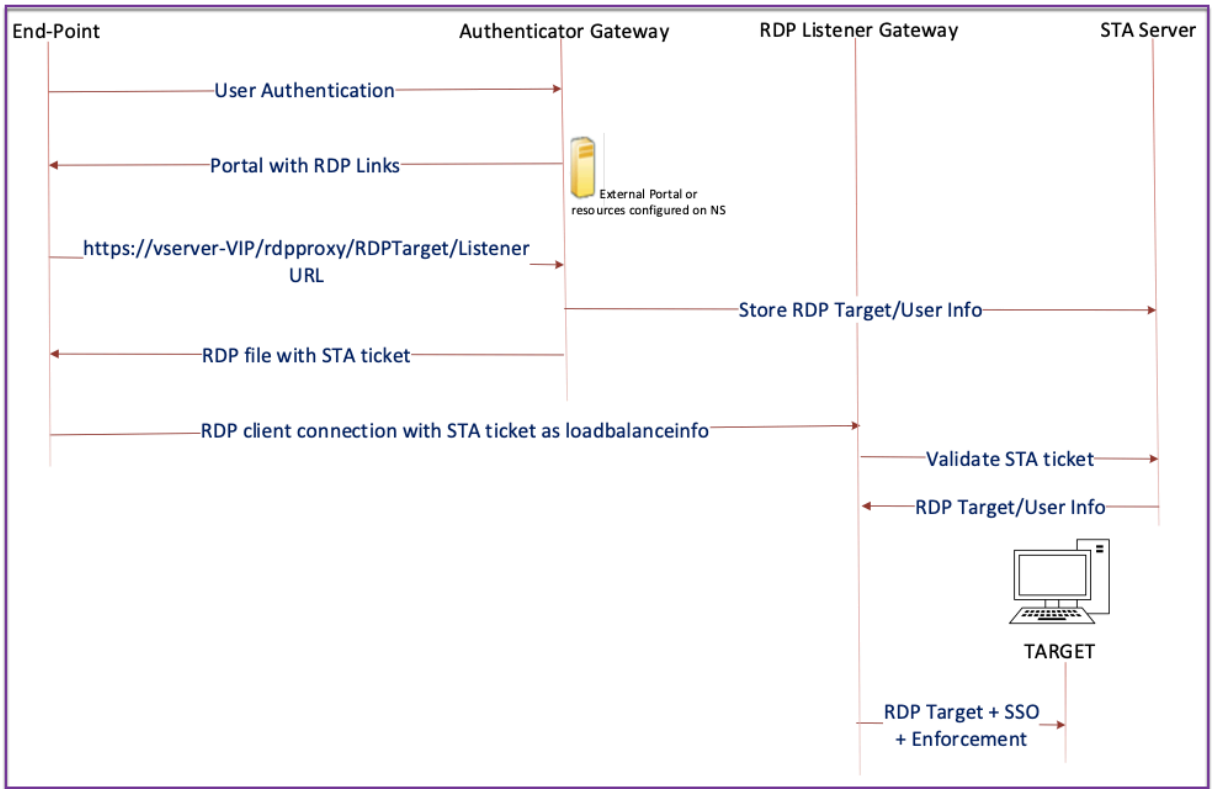
February 1, 2024

无状态 RDP 代理访问 RDP 主机。当用户在单独的 NetScaler Gateway 身份验证器 `RDPListener` 上进行身份验证时，将通过 NetScaler Gateway 上的授予访问权限。NetScaler Gateway 所需的 `RDPListener` 信息安全地存储在 STA 服务器上。只要 NetScaler Gateway 和应用程序枚举服务器可以访问 STA 服务器，就可以将 STA 服务器放置在任何地方。有关详细信息，请参阅 https://support.citrix.com/article/CTX101997。

连接流程

RDP 代理流程中涉及两个连接。第一个连接是用户与 NetScaler Gateway VIP 的 SSL VPN 连接，以及 RDP 资源的枚举。

第二个连接是与 NetScaler Gateway 上的 RDP 侦听器（使用 RDPip 和 RDPort 配置）的本机 RDP 客户端连接，以及随后将 RDP 客户端安全地代理到服务器数据包。



1. 用户连接到身份验证器网关 VIP 并提供凭据。
2. 成功登录网关后，用户将被重定向到主页/外部门户，该门户列举了用户可以访问的远程桌面资源。
3. 用户选择 RDP 资源后，身份验证器网关 VIP 将收到一个请求，格式 `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` 表示用户单击的已发布资源。此请求包含有关用户选择的 RDP 服务器的 IP 和端口的信息。
4. 身份验证器网关处理 /rdpproxy/ 请求。由于用户已经通过身份验证，因此此请求附带有有效的网关 cookie。
5. `RDPTarget` 和 `RDPUser` 信息存储在 STA 服务器上，然后生成 STA 票证。信息存储为 XML blob，可以选择使用配置的预共享密钥对其进行加密。如果加密，则 blob 将进行 base64 编码和存储。身份验证器网关使用在网关虚拟服务器上配置的 STA 服务器之一。
6. XML blob 采用以下格式

```
<Value name=" IPAddress" >ipaddr</Value>\n<Value name=" Port" >
    port</Value>n

<Value name=" `Username`" >username</Value>\n<Value name="
    Password" >pwd</Value>
<!--NeedCopy-->
```

7. 在 /rdpproxy/ 请求中获得的 `rdptargetproxy` 将作为“`fulladdress`”放置，STA 票证（预先附有 STA AuthID）作为 `loadbalanceinfo` 放置在.rdp 文件中。
8. `.rdp` 文件将被发送回客户端端点。

9. 本机 RDP 客户端启动并连接到 RDPListener Gateway。它以最初的 x.224 数据包发送 STA 票证。
10. RDPListener Gateway 验证 STA 票证并获取 RDPTarget 和 RDPUser 信息。要使用的 STA 服务器是使用中存在的“AuthID”检索的 loadbalanceinfo。
11. 创建 Gateway 会话用于存储授权/审核策略。如果用户存在会话，则会重复使用该会话。
12. RDPListener Gateway 使用 CREDSSP 连接到 RDPTarget 和单点登录。

必备条件

- 用户已在 NetScaler Gateway 身份验证器上进行身份验证。
- 初始 /rdpproxy URL 和 RDP 客户端连接到另一个 RDPListener NetScaler Gateway。
- 使用 STA 服务器的身份验证器网关可以安全地传递 RDPListener Gateway 信息。

使用 **CLI** 配置无状态 **RDP** 代理

- 添加 rdpServer 配置文件。服务器配置文件在上配置 RDPListener Gateway。

  注意：

  - 一旦在 VPN 虚拟服务器上配置了 RDP 服务器配置文件，就无法对其进行修改。此外，同一 ServerProfile 不能在另一台 VPN 虚拟服务器上重复使用。

```
add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
   RDP listener] -rdpPort [port for terminating RDP client
   connections] -psk [key to decrypt RDPTarget/RDPUser
   information, needed while using STA].
<!--NeedCopy-->
```

  使用以下命令在 VPN 虚拟服务器上配置 RDP 服务器配置文件：

```
add vpn vserver v1 SSL [publicIP] [
   portforterminatingvpnconnections] -rdpServerProfile [rdpServer
    Profile]
<!--NeedCopy-->
```

  示例

```
add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile
   rdp_server_prof
<!--NeedCopy-->
```

  > 重要提示：
  >
  > - 同一 STA 服务器必须同时绑定到 RDP 身份验证器网关和侦听器网关。
  > - 对于无状态 RDP 代理，STA 服务器会验证 RDP 客户端发送的 STA 票证以获取 RDP 目标服务器和

> RDP 用户的信息。除了 VPN 虚拟服务器之外，还必须绑定 STA 服务器。在以下示例中，RDP 目标服务器为 1.1.1.0，RDP 侦听器网关虚拟服务器为 1.1.1.2。
>
> ```
> 1       add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
> 2   <!--NeedCopy-->
> ```

使用以下命令在身份验证器网关上配置客户端配置文件：

```
1 add rdpClient profile <name> -rdpHost <optional FQDN that will be put
     in the RDP file as  'fulladdress' > [-rdpUrlOverride ( ENABLE |
     DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
     redirectDrives ( ENABLE | DISABLE )]
2
3          [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
              keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
              videoPlaybackMode ( ENABLE | DISABLE )]
4
5          [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
              ENABLE | DISABLE )] [-rdpCustomParams <string>]
6 <!--NeedCopy-->
```

—rdphost 配置用于单个网关部署中。只有 psk 是必填参数，它必须与 RDP 侦听器网关 RDP 服务器配置文件中添加的 PSK 相同。

- 将 RDP 配置文件与 VPN 虚拟服务器关联。

您可以通过配置会话操作 + 会话策略或设置全局 VPN 参数来关联 RDP 配置文件。

示例：

```
1 add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>
2
3 add vpn sessionpolicy <polname> NS_TRUE <actname>
4
5 bind vpn vserver <vservername> -policy <polname> -priority <
     prioritynumber>
6 <!--NeedCopy-->
```

或者

```
1 set vpn parameter  - rdpClientprofile <name>
2 <!--NeedCopy-->
```

使用 **GUI** 配置无状态 **RDP** 代理

无状态 RDP 代理配置涉及以下高级步骤。有关详细步骤，请参阅 RDP 代理配置。

- 创建 RDP 服务器配置文件
- 创建 RDP 客户端配置文件

- 创建虚拟服务器
- 创建书签
- 创建或编辑会话配置文件或策略
- 绑定书签

> 重要：
>
> 对于无状态 RDP 代理，除了 VPN 虚拟服务器之外，还必须绑定 STA 服务器。

连接计数器

添加了一个新的连接计数器 ns_rdp_tot_curr_active_conn，它保留了正在使用的活动连接数的记录。它可以被视为 NetScaler shell 上 `nsconmsg` 命令的一部分。计划稍后添加查看这些计数器的 CLI 命令。

升级说明

之前在 VPN 虚拟服务器上配置的 RdpIP 和 rdPort 是 RdpServerProfile 的一部分。将 `rdp Profile` 重命名为 `rdp ClientProfile`，并删除参数 clientSSL。因此，早期的配置不起作用。

RDP 连接重定向

February 1, 2024

NetScaler Gateway 设备现在支持在存在连接代理或会话目录的情况下进行 RDP 连接重定向。对于从客户端到服务器的每个连接，RDP 代理通信不再需要专用 URL。相反，代理使用单个 URL 连接到 RDP 服务器场，从而减少了管理员的维护和配置开销。

需要注意的是：

- 只有在启用 SSO 时才支持 RDP 连接重定向，并且在单网关和无状态或双网关模式以及强制 (SmartAccess) 模式下都支持 RDP 连接重定向。
- 只有支持 IP Cookie 的基于令牌的重定向才支持 RDP 代理功能。当禁用“使用 IP 地址 重定向”功能时，**Windows** 会话代理或连接代理将返还基于 **IP** 的 路由令牌“msts=”。
- 您可以在以下位置禁 用使用 **IP** 地址重定向 设置以启用基于令牌的重定向。
  `Computer Configuration` > `Policies` > `Administrative Templates` > `Windows Components` > `Remote Desktop Services` > `Remote Desktop Session Host` > `RD Connection Broker`。
- 在 RDSH 计算机上禁用使用 IP 地址重定向设置，而不是在连接代理计算机上禁用。
- 可以配置用于 RDP Proxy 连接的专用重定向器。

必备条件

- 创建 RDP 服务器配置文件以在 NetScaler Gateway 虚拟服务器上启用 3389 侦听器。
  如果要进行 RDP 的计算机不是任何 RDS 连接代理基础架构的成员，则不需要 3389 侦听器。
- 在 NetScaler Gateway 设备上启用 RDP 连接重定向，以在存在连接代理的情况下支持 RDP 代理。

在有连接代理的情况下部署 **RDP Proxy**

在存在连接代理的情况下，可以通过以下两种方式部署 RDP Proxy。

- 使用 RD 会话主机服务器参与 RD 连接代理负载平衡。
- 在存在 RDP 负载平衡功能的情况下。

当 **RD** 会话主机服务器参与 **RD** 连接代理负载平衡时：

在这种情况下，可以将 RDP URL 链接配置为指向其中一个 RDP 服务器作为目标服务器，该服务器充当重定向器。此外，可以将场中的一台 RDP 服务器作为目标服务器（在这种情况下，服务器不接受任何 RDP 会话）。

在存在 **RDP** 负载平衡功能的情况下：

如果未启用连接代理负载平衡，我们可以在 NetScaler 上提供 RDP 负载平衡功能，以便在存在连接代理的情况下对 RDP 会话执行所需的负载平衡。在这种情况下，必须将 RDP URL 链接配置为将 RDP 负载平衡器用作目标服务器。RDP 负载平衡器可以与 RDP 代理位于同一 NetScaler Gateway 设备上。有关更多信息，请参阅 负载平衡 RDP 服务器。

使用 **CLI** 在有连接代理的情况下配置 **RDP** 代理

在命令提示窗口中，键入：

```
1 add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
     DISABLE )
2
3 add rdpserverprofile serverProfileName -psk  “secretString”  -
     rdpRedirection ENABLE
4 <!--NeedCopy-->
```

使用 **NetScaler GUI** 配置 **RDP** 连接重定向

1. 导航到 **NetScaler Gateway >** 策略 **RDP**。
2. 右键单击 **RDP** 以 启用或禁用 RDP 重定向功能。

根据 LDAP 属性填充 RDP URL

February 1, 2024

您可以将 NetScaler Gateway 设备配置为从 LDAP 服务器属性中检索 RDP 服务器列表 (IP/FQDN)。根据检索到的列表，设备显示用户可以访问的服务器的 RDP URL。

使用 CLI 根据 LDAP 属性填充 RDP URL

在命令提示符下，键入：

```
add rdpclientprofile <Name>  -rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  -rdpUrlLinkAttribute
    rdpServerAttribute

<!--NeedCopy-->
```

在前面的示例中，rdpServerAttribute 对应于 LDAP 服务器上给定用户的 RDP 服务器详细信息。

注意：要从 LDAP 服务器获取 LDAP 属性详细信息，必须使用 pUrlLinkAttribute 配置的相同字符串配置 LDAP 操作。

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
     <"domain name"> -ldapBindDn <username> -ldapLoginName
    sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
    ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
    ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

LDAP 服务器配置

在 LDAP 服务器上，执行以下步骤：

1. 导航到特定 用户。
2. 在 **AD** 用户和计算机中，单击 查看，然后单击 详细信息。

3. 右键单击 用户名 并单击 属性编辑器。
4. 更改必需的属性 (DisplayName) 值，然后单击 确定。

使用 **GUI** 根据 **LDAP** 属性填充 **RDP URL**

1. 导航到 **NetScaler Gateway >** 策略 **RDP**。
2. 在“**RDP** 配置文件和连 接”页面上，单击“客户端配 置文件”选项卡，然后选择要在其中配置 RDP 链接属性的客户端配置文件。
3. 在“配置 **RDP** 客户端配置文 件”页的“**RDP** 链接属性”中，输入 LDAP 属性名称。

   注意： LDAP 属性值可以是逗号分隔的列表。

使用 **RDP** 代理随机化 **RDP** 文件名

February 1, 2024

单击 RDP URL 时，将下载一个 RDP 文件。再次单击 **RDP URL** 后，将下载同名的新 RDP 文件，从而弹出一个用现有文件替换新文件的弹出窗口。为避免这种情况，管理员可以选择随机设置 RDP 文件名。现在，通过以 <rdpFileName>_<outputof time()>.rdp 格式附加 time () 函数的输出，对文件名进行随机化。通过这样做，设备每次下载文件时都会生成唯一的 RDP 文件名。

配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持

要通过在命令提示符下使用命令行界面配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持，请键入：

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
          randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
          randomizeRDPFilename YES
4 <!--NeedCopy-->
```

要使用 **NetScaler GUI** 配置对使用 **RDP** 代理随机化 **RDP** 文件名的支持，请执行以下操作：

1. 导航到 **NetScaler Gateway** > 策略 > **RDP**。
2. 在“**RDP** 配置文件和连接”页面上，单击“客户端配 置文件”选项卡，然后选择要在其中配置随机化 RDP 文件名功能的客户端配置文件。
3. 在“配置 **RDP** 客户端配置 文件”页上，在“****** 随机化 **RDP** 文件名”字段旁边的菜单中选择“是 ******”。

配置 **RDP** 文件的名称

February 1, 2024

下载 RDP 文件后，可以使用配置的文件名将其存储在本地。

配置 **RDP** 文件的名称

要使用 CLI 配置 RDP 文件的名称，请在命令提示符处键入 **：

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

要使用 **GUI** 配置 **RDP** 文件的名称，请执行以下操作：

1. 导航到 **NetScaler Gateway** > 策略 > **RDP**。
2. 在 **RDP** 配置文件和连接 页面上，单击 客户端配置文件 选项卡。选择要在其中配置随机化 RDP 文件名功能的客户端配置文件。
3. 在“配置 **RDP** 客户端配置 文件”页上，在“RDP 文件名”字段中输入 **RDP** 配置文件的名称。文件的名称必须采用以下格式:。名称最多允许使用 31 个字符。

出站 **ICA** 代理支持

February 1, 2024

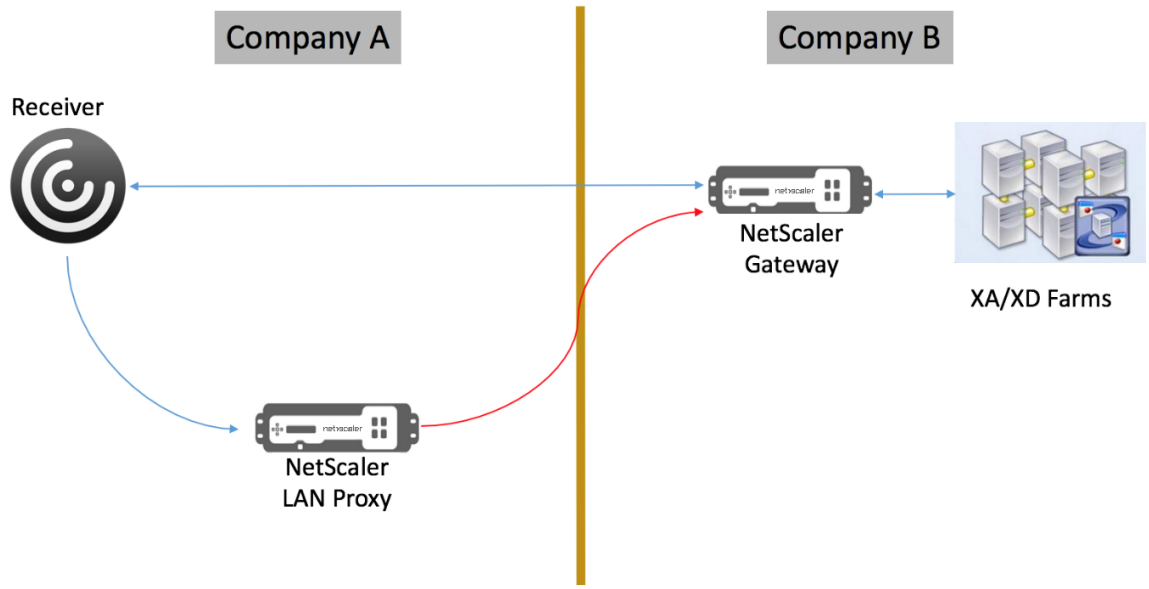
对 NetScaler Gateway 的出站 ICA 代理支持使网络管理员能够使用 SmartControl 功能，即使 Receiver 和 NetScaler Gateway 部署在不同的组织中也是如此。

以下场景说明了出站 ICA 代理解决方案的用法：

在不同的组织中部署 Receiver 和 NetScaler Gateway 时，网络管理员需要控制与 ICA 会话相关的功能。

了解出站 **ICA** 代理支持

为了将 SmartControl 功能带给拥有 Receiver 的企业组织 A 公司，我们需要添加一个充当局域网代理的 NetScaler 设备。NetScaler 局域网代理强制实施 SmartControl 并将流量代理到 B 公司的 NetScaler Gateway。在此部署方案中，接收方会将流量转发到 NetScaler 局域网代理，该代理允许 A 公司的网络管理员强制执行 SmartControl。下图描述了部署情况。



在这种情况下，局域网代理和 NetScaler Gateway 之间的流量通过 SSL 进行。

> 注意：请 勿在 NetScaler Gateway 上启用基于客户端证书的身份验证。

NetScaler 局域网代理上的 **SSL** 支持

从 13.0 版本 xx.xx 开始，Citrix Workspace 应用程序和 NetScaler 局域网代理之间的流量也受 SSL 支持。Citrix Workspace 应用程序对通过 SSL 发送到局域网代理的流量进行加密。局域网代理上的 SSL 支持可以与现有部署共存。

要在 Citrix Workspace 应用程序和 NetScaler 局域网代理之间通过 SSL 启用流量加密，必须在 NetScaler 局域网代理上执行以下操作：

- 在 VPN 虚拟服务器上禁用身份验证并启用双跃点。
- 将 Windows 客户端上的主机设置为 VPN 虚拟服务器的 IP 地址。
- 启用 SNI 和证书验证。
- 添加适当的 CA 证书并在全局启用它们。

配置出站 **ICA** 代理

February 1, 2024

出站 ICA 代理配置涉及配置 NetScaler 局域网代理和 NetScaler Gateway。

为 **ICA** 出站代理配置 **NetScaler** 局域网代理

您可以使用 CLI 执行以下步骤来配置出站 ICA 代理。

- 添加 VPN 虚拟服务器。

```
1 add vpn vserver <name> <serviceType> [<IPAddress> [-range <
     positive_integer>] [-ipset <string>]] [<port>] [-state (
     ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
     doubleHop ( ENABLED |DISABLED )]
2 <!--NeedCopy-->
```

- 设置 VPN 参数。

```
1 set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
     backendCertValidation ( ENABLED | DISABLED )]
2 <!--NeedCopy-->
```

- 添加 SSL 证书密钥对。

```
1 add ssl certKey ca_cert_verify -cert <certificate name>
2 <!--NeedCopy-->
```

- 全局绑定 SSL 证书密钥对。

```
1 bind vpn global -cacert ca_cert_verify
2 <!--NeedCopy-->
```

示例：

```
1 - add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
     OFF - doubleHop ENABLED
2
3 - set vpn parameter backendserverSni ENABLED backendcertValidation
     ENABLED
4
5 - add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer
6
7 - bind vpn global -cacert dnpg_ca
8
9 <!--NeedCopy-->
```

为 **ICA** 代理配置 **NetScaler Gateway**

有关为 ICA 代理配置 NetScaler Gateway 的详细信息，请参阅 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/deploying-netscaler-gateway-in-ica-proxy-mode.pdf

注意：对于 NetScaler 局域网代理上的 SSL 支持，无需在 NetScaler Gateway 配置中进行任何更改。

NetScaler Gateway 为 VMware Horizon View 启用了 PCoIP 代理支持

February 1, 2024

NetScaler Gateway 12.0 支持基于 IP 的个人计算机 (PCoIP) 协议，该协议是包括 VMware Horizon View 在内的多种非 Citrix VDI 解决方案的远程显示协议。PCoIP 类似于 Citrix HDX/ICA 协议和 Microsoft RDP 协议。PCoIP 使用 UDP 端口 4172。

通过 NetScaler Gateway 代理 PCoIP 时，NetScaler Gateway 可以取代传统的 PCoIP 远程访问解决方案，例如 View 安全服务器或 VMware 接入点。

以下情况说明了如何使用启用 **NetScaler Gateway** 的 **VMware Horizon View** 解决方案。

- 需要通过 NetScaler Gateway 远程访问 VMware Horizon View 桌面池和应用程序池而无需部署 Horizon View 安全服务器或 VMware 接入点的 VMware Horizon PCoIP 用户。
- PCoIP 用户通过 NetScaler Gateway 远程访问其他基于 PCoIP 的虚拟桌面解决方案。

> 注意
>
> NetScaler Gateway 作为远程访问解决方案进行部署。

为 VMware Horizon View 配置启用了 NetScaler Gateway 的 PCoI 代理

February 1, 2024

必备条件

版本 -NetScaler 12.0 或更高版本

通用许可证 -PCoIP 代理使用 NetScaler Gateway 的无客户端访问功能，这意味着每个 NetScaler Gateway 连接都必须获得 NetScaler Gateway 通用的许可。在 NetScaler Gateway 虚拟服务器上，确保清除 仅限 **ICA** 。

Horizon View 基础架构 -功能齐全的内部 Horizon View 确保您能够在没有 NetScaler Gateway 的情况下内部连接到 Horizon View 代理。确保 NetScaler 将代理连接到的 View 连接服务器上未启用 Horizon View **HTTP (S)** 安全通道 和 **PCoIP Secure Gateway** 。
支持以下版本的 VMware Horizon 视图。

- 连接服务器：7.0.1 及更高版本
- Horizon Client：4.2.0 及更高版本（Windows 和 Mac）

防火墙端口：

请务必满足以下各项条件：

- 必须从 Horizon View 客户端向 NetScaler Gateway VIP 开放 UDP 4172 和 TCP 443。
- 必须从 NetScaler SNIP 向所有内部 Horizon View 代理开放 UDP 4172。
- 在 NAT 之后部署的 NetScaler 支持 PCoIP 代理。以下是需要考虑的要点：
  - 支持基于 VPN 虚拟服务器 FQDN 参数设置
  - 仅支持可公开访问的 FQDN，不支持 IP
  - 仅支持 443 和 4172 个端口
  - 必须是静态 NAT

证书—NetScaler Gateway 虚拟服务器的有效证书。

身份验证—使用高级语法的 LDAP 身份验证策略/服务器。

Unified Gateway（可选）—如果是 Unified Gateway，则在添加 PCoIP 功能之前创建 Unified Gateway。

rfWebUI 门户主题—要通过 Web 浏览器访问 Horizon View，必须使用 rfWebUI 主题配置 NetScaler Gateway 虚拟服务器。

Horizon View 客户端—即使使用 NetScaler RFWebui 门户访问 Horizon 发布的图标，也必须在客户端设备上安装 Horizon View 客户端。

要配置 **NetScaler Gateway** 以支持 **VMware Horizon View** 的 **PCoIP** 代理，请执行以下操作：

1. 导航到 配置 **> NetScaler Gateway** 策略 **> PCoIP**。
2. 在 PCoIP 配置文件和 连接页面上创建虚拟服务器配置文件和 **PCoIP** 配置文件。
   a) 要创建虚拟服务器配置文件，请在 虚拟服务器配置文件 选项卡上单击 添加。
   b) 输入虚拟服务器配置文件的名称。
   c) 输入用于单点登录 View 连接服务器的 Active Directory 域名，然后单击 创建。
   注意：每个 NetScaler Gateway 虚拟服务器仅支持一个 Active Directory 域。此外，此处指定的域名也会显示在 Horizon View 客户端中。
   d) 单击“登录”。
   e) 要创建 PCoIP 配置文件，请在 配置文件 选项卡上，单击 添加。
      i. 输入 PCoIP 配置文件的名称。
      ii. 输入内部 VMware Horizon View 连接服务器的连接 URL，然后单击 创建。
   f) 导航到配置 **> NetScaler Gateway >** 策略 **>** 会话。
   g) 在右侧，选择“会话配置文件”选项卡。
   h) 在 **NetScaler Gateway** 会话策略和配置文件 页面上，创建或编辑 NetScaler Gateway 会话配置文件。
      i. 要创建 NetScaler Gateway 会话配置文件，请单击 添加，然后提供名称。

ii. 要编辑 NetScaler Gateway 会话配置文件，请选择该配置文件，然后单击 编辑。

i) 在“客户端体验”选项卡上，确保“无客户端访问”值设置为“开”。

j) 在“安 全”选项卡上，确保“默认授权操作”值设置为“允许”。

k) 在 **PCoIP** 选项卡上，选择所需的 PCoIP 配置文件，然后单击 创建。您还可以通过此选项卡创建或编辑 PCoIP 配置文件。

l) 单击 创建 或 确定 完成创建或编辑会话配置文件。

m) 如果已创建会话配置文件，则还必须创建相应的会话策略。

i. 导航到配置 **> NetScaler Gateway >** 策略 **>** 会话。

ii. 选择会 话策略 选项卡，然后单击 添加。

iii. 在创建 NetScaler Gateway 会话策略页面中，输入策略的名称。

iv. 在 配置文件中，选择现有配置文件或单击 添加 并创建配置文件。

v. 添加表达式。

A. 单击高级策略，然后单击表达式编辑器。
B. 在 表达式中，根据需要选择表达式。

vi. 单击“确定”。

n) 将创建的 PCoIP 虚拟服务器配置文件和会话策略绑定到 NetScaler Gateway 虚拟服务器。

i. 转到 **NetScaler Gateway >** 虚拟服务器。

ii. 在右侧，添加 新的 NetScaler Gateway 虚拟服务器或 编辑 现有的 NetScaler Gateway 虚拟服务器。

iii. 如果要编辑现有 NetScaler Gateway 虚拟服务器，请在“基本设置”部分中单击铅笔图标。

iv. 对于添加和编辑，在“基本设置”部分中，单击“更多”。

v. 使用 **PCoIP** 虚拟服务器配置文件 菜单选择所需的 PCoIP 虚拟服务器配置文件。

vi. 向下滚动并确保已清除“仅 ICA”。然后单击“确定”关闭“基本设置”部分。

vii. 如果要创建 NetScaler Gateway 虚拟服务器，请绑定 证书并绑定 LDAP 身份验证策略。

viii. 向下滚动到“策略”部分，然后单击加号图标。

ix. “选择类型”页默认为“会话 和 请求”。单击继续。

x. 在 策略绑定 部分中，单击 单击以选择。

xi. 选择配置了 PCoIP 配置文件的所需会话策略，然后单击 选择。

xii. 在 策略绑 定页面中，单击 绑定。

xiii. 如果要使用 Web 浏览器连接到 VMware Horizon View，请在 高级设置下添加 门户主题 部分。如果您仅使用 Horizon View 客户端连接到 NetScaler Gateway，则不必执行此步骤。

xiv. 使用 门户主题 菜单选择 **RfWebUI**，然后单击 确定。

xv. 已发布的 Horizon View 图标将添加到 RfWebUI 门户中。

> 注意： VMware 在使用除 RDP 之外的任何协议时使用两个或更多协议。这可能会导致请求在两个不同的后端服务器之间进行负载平衡。您可以通过跨所有协议设置单个持久性组来解决此问题，以确保所有连接都保留在同一 Citrix 虚拟服务器上。

启用 **USB** 重定向的步骤

可以从虚拟桌面和应用程序访问连接到客户端计算机的 USB 设备。以下是启用 USB 重定向的步骤：

1. 登录到 VMware Horizon 管理员控制台。
2. 导航到 清单 **>** 查看配置服务器。
3. 选择 连接服务器 选项卡。
4. 选择列出的连接服务器，然后单击 编辑。
5. 在“常 规”选项卡下，选择“**HTTP (S)** 安全通道”下的“使用安全通道连接到计算机”选项。在外部 URL 字段中提供 NetScaler Gateway 外部 **URL** 。

更新 **Unified Gateway** 的内容切换表达式

如果您的 NetScaler Gateway 虚拟服务器位于 Unified Gateway（内容交换虚拟服务器）之后，则必须更新内容交换表达式以包含 PCoIP URL 路径。

1. 在 NetScaler GUI 中，导航到 配置 **>** 流量管理 **>** 内容交换 **>** 策略。
2. 在“表达式”区域下附加以下 表达式，然后单击“确定”。

	http.req.url.path.eq (“/broker/xml”)	http.req.url.path.contains(“/broker/resources”)	http.req.url.path.eq (“/pcoip-client”)

使用 **PCoIP** 网关

1. 要进行连接，您必须在客户端设备上安装 Horizon View 客户端。安装完成后，您可以使用 Horizon View 客户端的用户界面连接到 NetScaler Gateway，也可以使用 NetScaler Gateway rfWebUI 门户页面查看从 Horizon 发布的图标。
2. 要查看活动的 PCoIP 连接，请转到 **NetScaler Gateway > PCoIP**。

3. 在右侧，切换到“连 接”选项卡。将显示活动会话，其中包含以下数据：用户名、Horizon View 客户端 IP 和 Horizon View 代理目标 IP。
4. 要终止连接，请右键单击“连接”选项卡，然后单击“终 止连接”。或者单击“终止所有连接”以终止所有 PCoIP 连接。

配置 **VMware Horizon View Connection Server**

February 1, 2024

要通过 NetScaler Gateway 支持 PCoIP 代理：

1. 登录到 **VMware Horizon** 管理员控制台。
2. 导航到 I 清 单—> 查看配置—> 服务器。
3. 选择 连接服务器 选项卡。
4. 选择列出的连接服务器，然后单击 编辑。
5. 在 常 规选项卡下，取消选择 HTTP (S) 安全通道下的使用安全通道连接 到计算机选项。
6. 单击 确定 关闭 编辑连接服务器设置 窗口。
7. 在所有列出的连接服务器上执行从 4 到 6 的步骤。

NetScaler Gateway 的出站代理支持的代理自动配置

February 1, 2024

将 NetScaler Gateway 设备配置为支持代理自动配置 (PAC) 时，PAC 文件的 URL 将推送到客户端浏览器。然后，根据 PAC 文件中定义的条件，将来自客户端的流量重定向到相应的代理。

以下是 PAC 用于出站代理的一些常见用例：

- 配置处理客户端流量的多个代理服务器。
- 对跨子网的代理流量进行负载平衡。

使用 **CLI** 配置 **NetScaler Gateway** 全局参数以支持 **PAC** 用于出站代理

在命令提示符下，键入：

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```


使用 **CLI** 将 **NetScaler Gateway** 配置为在会话配置文件中支持 **PAC**

在命令提示符下，键入：

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

哪里；

- **URL** —代理服务器的 URL
- 名称—VPN 会话的名称操作

使用 **GUI** 配置 **NetScaler Gateway** 全局参数以支持 **PAC** 用于出站代理

1. 导航到 配置 **> NetScaler Gateway >** 全局设置。
2. 在“全局设置”页面上，单击“更改全局设置”，然后选择“客户端体验”选项卡。
3. 在客户端体验选项卡上，选择高级设置，然后选择代理选项卡。
4. 在代理选项卡上，选择浏览器，然后选择使用自动配置。
5. 在“自动代理配置文件的 URL”字段中，键入所需 PAC 文件的 URL。
6. 单击创建。

使用 **GUI** 将 **NetScaler Gateway** 配置为在会话配置文件上支持 **PAC**

1. 导航到 配置 **> NetScaler Gateway >** 策略 **>** 会话。
2. 在 NetScaler Gateway 会话策略和配置文件页面上，创建 NetScaler Gateway 会话配置文件。
3. 选择会 话配置文件 选项卡，单击 添加，然后输入名称。
4. 在客户端体验选项卡上，选择 高级设置，然后选择 代理 选项卡。
5. 在代理选项卡上，选择 浏览器，然后选择 使用自动配置。
6. 在“自动代理配置文件的 URL”字段中，键入所需 PAC 文件的 URL。
7. 单击创建。
8. 单击创建。

SameSite cookie 属性的配置支持

February 1, 2024

`SameSite` 属性指示浏览器 cookie 是可用于跨站点上下文还是仅用于同一站点上下文。如果应用程序打算在跨站点上下文中访问，那么它只能通过 HTTPS 连接进行访问。有关详细信息，请参阅 RFC6265。

直到 2020 年 2 月，尚未在 NetScaler 设备中显式设置该 SameSite 属性。浏览器采用了默认值 (None)。未设置 SameSite 属性不会影响 NetScaler Gateway 和 NetScaler AAA 部署。

随着某些浏览器的升级，例如 Google Chrome 80，cookie 的默认跨域行为会发生变化。SameSite 属性可以设置为以下值之一。Google Chrome 的默认值设置为 Lax。对于某些版本的其他浏览器，SameSite 属性的默认值可能仍设置为“无”。

- 无：表示浏览器仅在安全连接时在跨站点环境中使用 cookie。
- 松懈：表示浏览器在同一站点上下文中使用 cookie 处理请求。在跨网站上下文中，只有像 GET 请求这样的安全 HTTP 方法才能使用 cookie。
- **Strict**（严格）：仅在同一站点环境中使用 cookie。

如果 cookie 中没有 SameSite 属性，Google Chrome 会假设功能为 SameSite = Lax。
因此，对于需要浏览器插入 cookie 的跨站点环境的 iframe 中的部署，Google Chrome 不会共享跨站点 cookie。因此，Web 站点中的 iframe 可能无法加载。

配置 SameSite cookie 属性

名为 SameSite 的新 Cookie 属性将添加到 VPN 和 NetScaler AAA 虚拟服务器中。可以在全局级别和虚拟服务器级别设置此属性。

要配置 SameSite 属性，必须执行以下操作：

1. 设置虚拟服务器的 SameSite 属性
2. 将 Cookie 绑定到 patset （如果浏览器丢弃了跨站点 Cookie，则浏览器会丢弃）

使用 CLI 设置 SameSite 属性

要在虚拟服务器级别设置 SameSite 属性，请使用以下命令。

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

要在全局级别设置 SameSite 属性，请使用以下命令。

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

注意：虚拟服务器级别设置的优先级高于全局级别设置。Citrix 建议在虚拟服务器级别设置 SameSite cookie 属性。

使用 **CLI** 将 **patset Cookie** 绑定到

如果浏览器丢弃跨站点 Cookie，则可以将该 cookie 字符串绑定到现有的 `ns_cookies_SameSite patset`，以便将 `SameSite` 属性添加到 cookie 中。

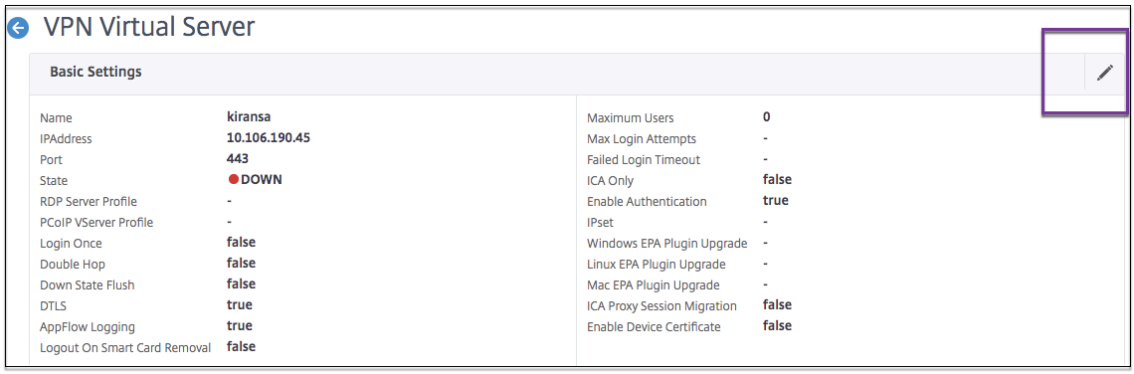
示例：

```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

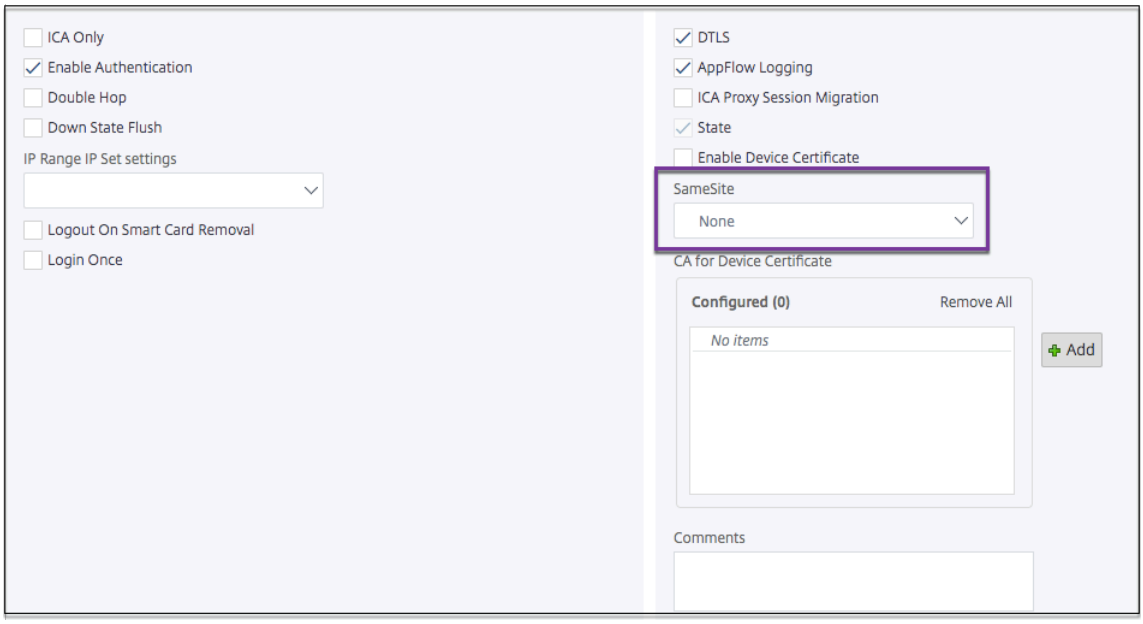
使用 **GUI** 设置 **SameSite** 属性

要在虚拟服务器级别设置 **SameSite** 属性：

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 选择虚拟服务器，然后单击 **Edit**（编辑）。
3. 在“基本设置”部分中选择编辑图标，然后单击“更多”。

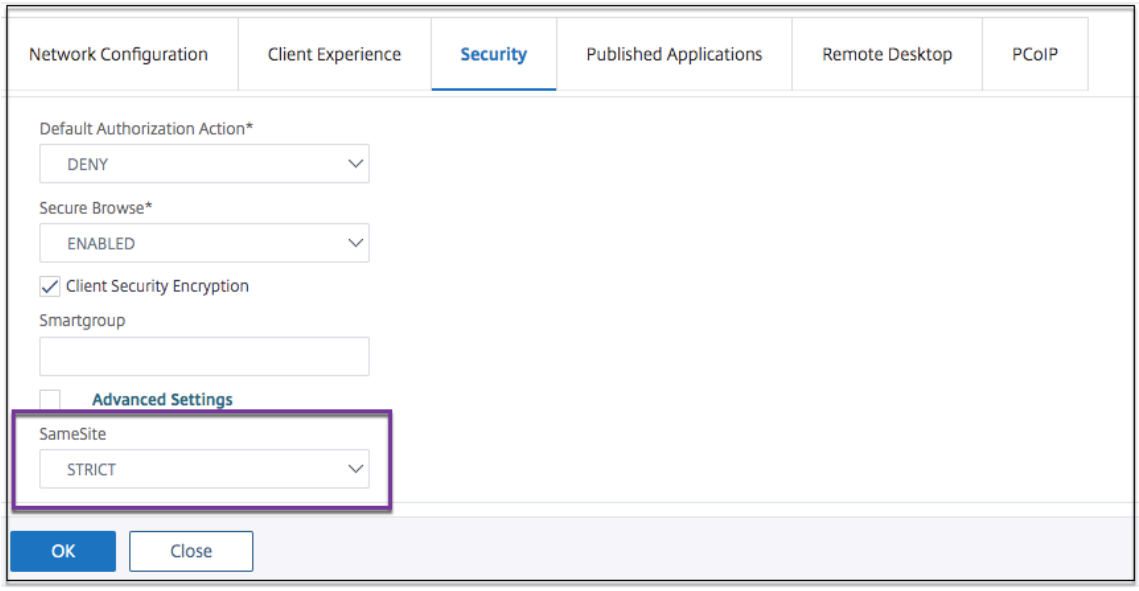


4. 在 **SameSite** 中，根据需要选择该选项。



要在全局级别设置 **SameSite** 属性：

1. 导航到 **NetScaler Gateway >** 全局设置 **>** 更改全局设置。
2. 单击安全选项卡。
3. 在中 **SameSite**，根据需要选择该选项。



网关 **UX** 配置上的 **RFWebui** 角色

February 1, 2024

RFWebui Persona 是一个为通过 NetScaler Gateway 登录的 NetScaler Gateway 用户提供新的登录和门户页面的主题。该门户向 Receiver、StoreFront 和 Citrix Endpoint Management 用户提供与直接访问这些产品之一时相同的 GUI。

何时使用 **RFWebui** 角色

当您需要不同的 NetScaler 产品提供的所有应用程序（例如 Web 和软件即服务 (SaaS) 应用程序、虚拟 Windows 应用程序和桌面）的单窗格视图时，请使用 NetScaler Gateway 中的 RfWebUI 角色。

以下场景说明了 RFWebui Persona 的用法。

- 用户使用网关访问 StoreFront，发现的 GUI 与在没有网关的情况下访问产品时看到的 GUI 不同。
  解决方案：当用户使用网关访问 StoreFront 时，RFWeBUI 主题提供的用户界面与他们在不使用网关的情况下访问产品时看到的类似。
- 用户使用网关访问 Citrix Workspace 应用程序、StoreFront 和 Citrix Endpoint Management 应用程序，并且由于应用程序未按逻辑方式分组，因此难以找到所需的应用程序。
  解决方案：RfWebUI 角色通过创建由不同产品（如 Receiver、StoreFront、Citrix Endpoint Management 等）提供的应用程序的逻辑捆绑，提供单一窗格视图的用户体验。

RfWebUI Persona 提供的功能

新的 RFWeBUI 提供以下功能：

- 转至
- 应用程序的聚合
- 用户配置的远程桌面协议 (RDP) 代理链接
- 收藏的应用

转至

转至：“转至”功能提供通过无客户端 VPN 访问网页的权限。用户只需在 书签 选项卡的 **URL** 部分中键入 URL，然后单击开始。

目前，转到功能仅支持 Outlook Web 应用程序 (OWA) 和 SharePoint URL。

> 注意：
> 只有会话策略中的 `clientlessAccessVPNMode` 参数为“启用”时，“转到”选项卡才可见。

应用程序的聚合

应用程序聚合： RFWeBUI 主题通过在描述性横幅下捆绑不同产品提供的应用程序来提供单一窗格视图。例如，NetScaler 管理员配置的所有 VPN URL 都位于名为 **Web** 和 **SaaS** 应用程序的捆绑包中，用户特定的 Web 书签位

于“个人书签”下。如果在 StoreFront 中配置了 Citrix Virtual Apps and Desktops 应用程序捆绑包，NetScaler Gateway 中的单窗格视图也会列出这些捆绑包。

用户配置的 **RDP** 代理链接

用户可以将 RDP 代理链接添加为个人书签。个人书签将显示在 桌 面选项卡下。

支持以下 RDP 模式：

- 单个网关
- 无状态（双）网关

> 注意：只有配置了 `RDPclientprofile` 时，用户才能添加 RDP 代理链接。有关 RDP 配置的更多信息，请参阅 RDP 代理文档。

收藏的应用

用户可以通过单击应用程序名称旁边的添加到 收藏夹 链接，将所需的应用 程序添加在 **Web** 和 **SaaS** 应用程序下以及 **** 个人书签 到收藏夹选项卡下。添加后的应用程序可以在收藏夹选项卡下看到。也可以通过单击“收藏夹”选项卡中应用程序旁边的“删除”链接从“收藏夹 **”选项卡中删除相同的内容。

启用 **RFWebui** 角色时的注意事项

RFWebui 角色不完全支持以下内容：

文件共享功能：不支持用于访问 SMB 文件共享的文件共享功能。向
主页发送电子邮件：向主页发送电子邮件 VPN 参数不能作为 NetScaler Gateway 门户的嵌入式视图使用。它可以作为应用程序在 RFWebui 的 **APPS** 选项卡下的 **Web** 和 **SaaS** 应用程序 捆绑包中进行访问。
Java 客户端：此主题中不提供用于建立 SSL 通道的基于浏览器的 Java 客户端。

配置 **RFWebui** 角色

要应用 **RFWebui** 角色，请执行以下操作：

1. 在 NetScaler 界面中，导航到 配置 **> NetScaler Gateway** 门户主题。
2. 在 门户主题 页面上，选中 **RFWebui** 复选框。
3. 单 击门户主题 页面右上角的保存图标。
4. 在“保 存确认”对话框中，单击“是”。

RfWebUI 配置参数

February 1, 2024

NetScaler Gateway 门户的整体行为受两个配置文件的影响：本地 NetScaler Gateway 配置文件和 StoreFront 文件。

根据您的部署，您可以通过更改 “plugins.xml” 文件中的属性来修改 NetScaler Gateway 门户行为。此文件在浏览器上显示为配置文件，这是请求的 `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`。

登录期间，将使用 NetScaler Gateway 配置文件。但是，当连接到 StoreFront 时，StoreFront 会发送一个新配置，并且之前的配置将被覆盖。对于无客户端 VPN 和 ICA，此行为有所不同。

对于 ICA，StoreFront 配置始终优先，但是即使在从 StoreFront 更新新配置之后，受 NetScaler Gateway 配置影响的无客户端 VPN 中的某些行为仍会保留。

下表列出了描述优先于无客户端 VPN 和 ICA 的配置的参数。

配置类型	sub 配置类型	参数	无客户端 VPN	ICA	说明
适用于 ICA 的无客户端 VPN /authManager 的会话	-	loginFormTimeout	NetScaler Gateway	-	定义登录页面超时的时间（以分钟为单位）
插件助手	-	enabled	StoreFront	StoreFront	启用或禁用插件助手
插件助手	-	upgradeAtLogin	StoreFront	StoreFront	登录时提示升级插件
插件助手	-	showAfterLogin	NetScaler Gateway	StoreFront	登录后显示插件提示
插件助手	-	showOnlyIfRequiredByApps	NetScaler Gateway	StoreFront	如果应用程序需要，则在登录后显示插件提示
插件助手	macOS/win32	path	NetScaler Gateway	StoreFront	定义插件的下载路径
插件助手	protocolHandler	enabled	NetScaler Gateway	StoreFront	在启动插件之前切换协议处理程序页面
插件助手	protocolHandler	platforms	NetScaler Gateway	StoreFront	标识插件支持的平台

配置类型	sub 配置类型	参数	无客户端 VPN	ICA	说明
插件助手	-	skipDoubleHopCheck	WhenDisabled NetScaler Gateway	StoreFront	切换 ICA 直通的双跃点 NetScaler Gateway 配置检查
用户界面	-	frameOptions	不适用	不适用	-
用户界面		autoLaunchDesktop	StoreFront	StoreFront	启用或禁用桌面启动
用户界面	workspaceControl	enabled	StoreFront	StoreFront	启用或禁用工作区控件
用户界面	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	切换为自动重新连接上一个会话（如果可用）
用户界面	workspaceControl	logoffAction	StoreFront	StoreFront	定义 Citrix Workspace 的注销行为
用户界面	workspaceControl	showReconnectButton	StoreFront	StoreFront	显示或隐藏重新连接按钮
用户界面	workspaceControl	showDisconnectButton	StoreFront	StoreFront	显示或隐藏断开连接按钮
用户界面	workspaceControl	showDesktopsView	StoreFront	StoreFront	显示或隐藏“桌面”视图
用户界面	workspaceControl	showAppsView	StoreFront	StoreFront	显示或隐藏“应用程序”视图
用户界面	workspaceControl	defaultView	StoreFront	StoreFront	选择“桌面”视图或“应用程序”视图
用户界面	receiverConfiguration	enabled	StoreFront	StoreFront	切换 Receiver 配置
用户界面	receiverConfiguration	showOnlyIfRequired	NetScaler Gateway	NetScaler Gateway	如果应用程序需要，则显示 Receiver 提示
用户界面	receiverConfiguration	downloadURL	StoreFront	StoreFront	下载 Receiver 的 URL
用户界面	appShortcuts	enabled	StoreFront	StoreFront	启用或禁用应用程序快捷方式选项卡

配置类型	sub 配置类型	参数	无客户端 VPN	ICA	说明
用户界面	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	允许重新连接会话

使用自定义插件自定义网关门户

February 1, 2024

NetScaler Gateway RFWeBUI 框架提供了添加自定义插件以自定义其网关门户的功能。这些自定义插件可用于向网关添加大型功能，例如，如果您想在网关流中添加一个全新的页面。对于其他用例，可以将代码添加到位置/var/netscaler/logon/themes/<custom_theme>/script.js 为网关主题提供的自定义脚本文件中。

1. 要添加自定义插件，请在该位置创建 JavaScript 文件 /var/netscaler/logon/LogonPoint/plugins/ns-gateway/。例如，您可以在中找到以下插件 /var/netscaler/logon/LogonPoint/plugins/ns-gateway/。

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   建议以 <plugin_name>.js 格式输入插件名称。

   所有这些插件文件都是由功能所需的 RfWebUI 框架提取的。

2. 创建插件文件后，使用以下代码作为示例向 RfWebUI 框架注册插件。

```
        (function ($) {

                    CTXS.ExtensionAPI.addPlugin( {

                                Name :  “plugin name” ,
                                initialize: function() {
  }

                     }
 );
             }
 )(jQuery);
<!--NeedCopy-->
```

   其中，

name 是给插件的名称。它用作插件的标识符。

initialize 接受函数作为用于初始化插件的参数。

3. 在函数中输入插件名称和初始化 CTXS.ExtensionAPI.addPlugin() 函数以注册插件。
添加的插件名称和位置必须注册到该位置的 plugins.xml 文件中 /var/netscaler/logon/themes/<custom_theme>/plugins.xml。

4. 编写插件代码后，必须在 /var/netscaler/logon/themes/<custom_theme>/plugins.xml 位置的 plugins.xml 文件中注册新添加的插件名称和位置。插件必须使用 plug-in 标记注册。

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient.js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js" />
</plugins>
<!--NeedCopy-->
```

5. 输入插件的名称和 src，以便 RfWebUI 可以识别和获取插件。

示例配置

以下示例配置可用于添加自定义插件，以向 NetScaler Gateway 登录页面添加页脚。

1. 在该位置创建 JavaScript 插件文件，/var/netscaler/logon/LogonPoint/plugins/ns-gateway/.

2. 将插件命名为 ns-footer.js
/var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js

3. 将以下代码添加到 RfWebUI 的注册插件中，然后在初始化函数中将页脚添加到网关。

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='text-align:center;color:white;font-size:15px;'><br>Disclaimer<BR><BR>"+
             " Access to this website is restricted to employees of Login Consultants<BR></div>");
```



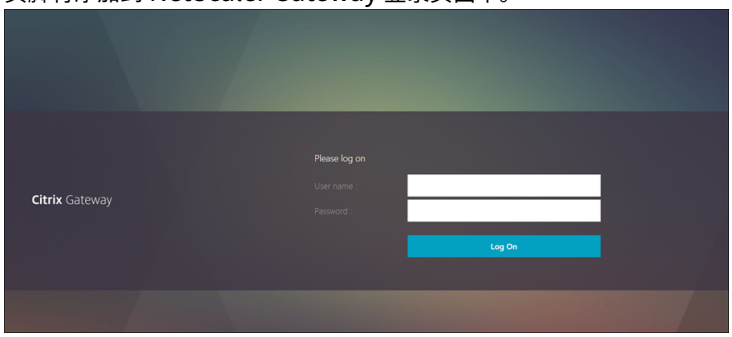
```
12                callback();
13            }
14    ;
15        }
16
17    }
18    );
19    }
20    )(jQuery);
21  <!--NeedCopy-->
```

4. 保存该文件。
5. 在 `var/netscaler/logon/themes/<custom_theme>/plugins.xml` 位置的 plugins.xml 中添加名称和 src。

```
1  <plugins>
2  <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
3  <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
       .js" />
4  <plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
       />
5  <plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
6  </plugins>
7  <!--NeedCopy-->
```

6. 配置要为其添加插件的自定义主题。
7. 使用命令 `flush cache contentgroup loginstaticobjects` 刷新缓存。
8. 重新加载入口屏幕。

   页脚将添加到 NetScaler Gateway 登录页面中。



创建和自定义登录架构

February 1, 2024

登录架构是为基于表单的身份验证提供结构的 XML 文件。

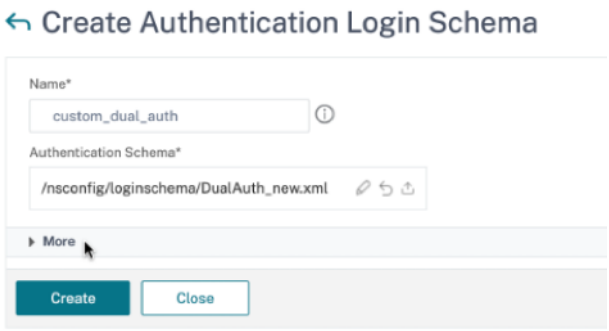
用户可以使用一组类似于基本 HTML 表单的用户界面结构来使用各种身份验证表单。

在 nFactor 身份验证中，身份验证因素链接在一起。每个因素可以有不同的登录架构页面或文件。在某些身份验证方案中，可以向用户显示多个登录屏幕。您还可以让一个登录架构收集可以传递给多个因素的信息，以便后者不必显示另一个登录模式。

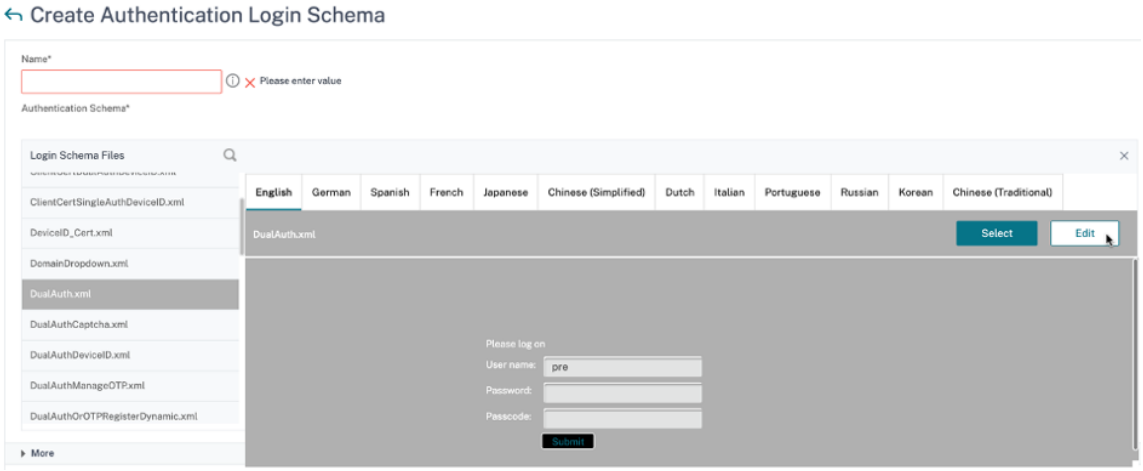
中的 NetScaler 设备包含登录架构 XML 文件 /nsconfig/loginschema/LoginSchema。

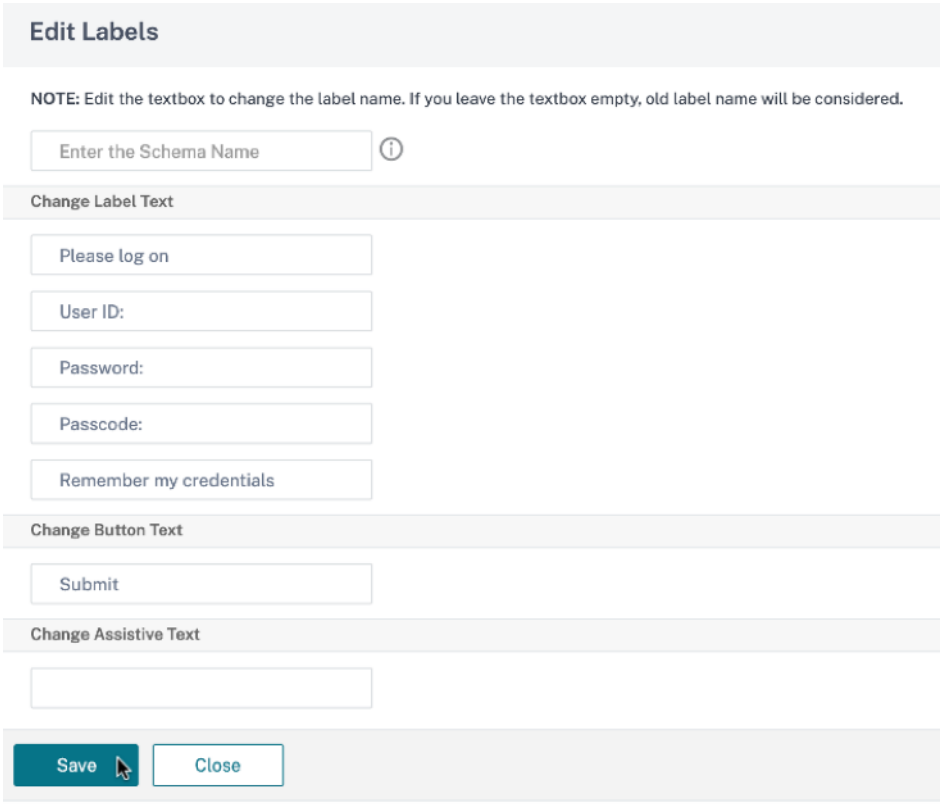
创建登录架构配置文件

1. 导航到 安全 **> AAA >** 登录架构。
2. 单击 配置文件 选项卡，然后单击 添加。
3. 在 身份验证架构中，单击铅笔图标。



4. 单击 **LoginSchema** 文件夹以查看其中的文件。
5. 选择其中一个文件并根据需要执行更改。
   - 单击右上角的“编辑”按钮更改标签。
   - 通过选择语言来编辑方案。

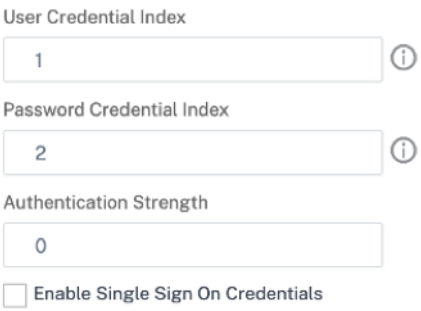


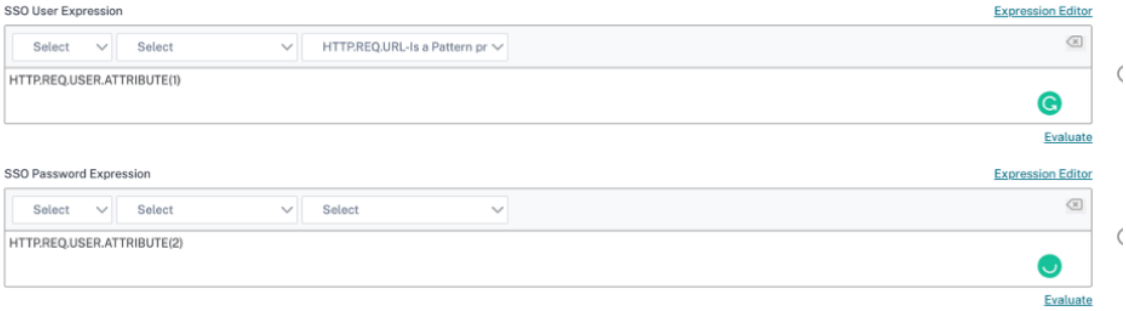


注意：修改后保存更改时，将创建一个包含这些更改的新架构 XML 文件。

6. 在右上角，单击 选择以选 择修改后的架构 XML。
7. 输入登录架构名称，然后单击 更多。

   注意：您可以在其他地方使用已经输入的凭据。例如，您可以使用用户名和密码之一进行 StoreFront 单点登录。您可以单击 更多，然后输入索引的唯一值。这些值可以介于 1 到 16 之间。您可以使用表达式 REQ.USER.ATTRIBUTE(#) 在流量策略或配置文件中引用这些索引值。





8. 单击 创建 以创建登录架构配置文件。

将登录架构配置文件绑定到身份验证、授权和审核虚拟服务器

要将登录架构配置文件绑定到身份验证、授权和审核虚拟服务器，必须首先创建登录架构策略。将登录架构配置文件绑定到身份验证策略标签时，不需要登录架构策略。

要创建和绑定登录架构策略，请执行以下操作：

1. 导航到 安全 **> AAA >** 登录架构。
2. 单击“策略”选项卡，然后单击“添加”。
3. 在 **Profile** 中，选择之前创建的登录架构配置文件。
4. 在 规则中，输入默认语法表达式，然后单击 创建。

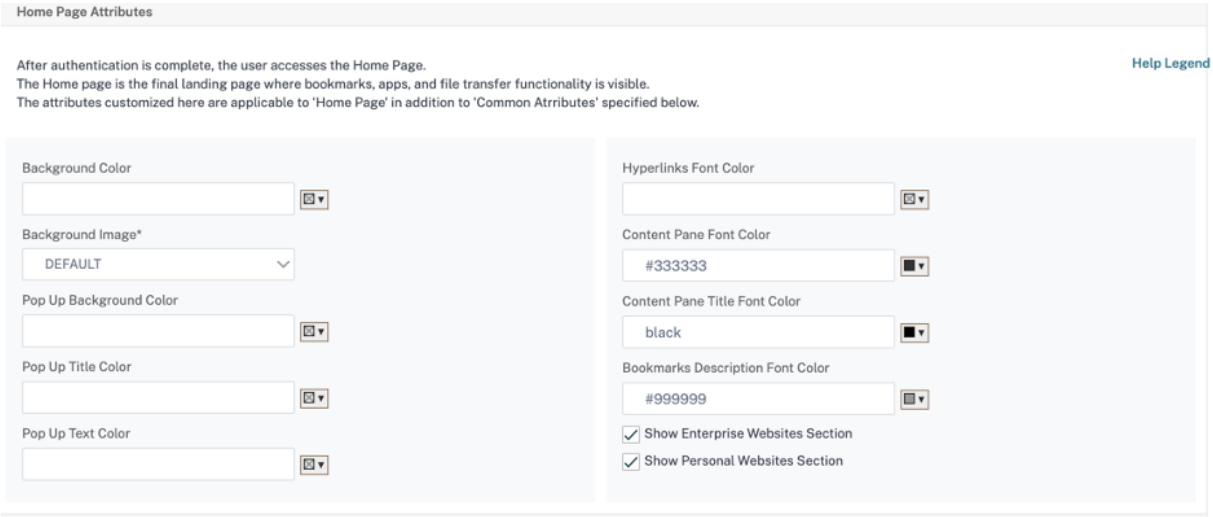
通过管理员 **UI** 进行门户自定义

February 1, 2024

管理员可以通过创建自定义主题来自定义门户主题，以实现用户门户的个性化外观。可以基于 RfWebUI、Default、X1 和 GreenBubble 主题创建自定义主题。

要创建自定义主题，请执行以下操作：

1. 在配置选项卡中，导航到 **NetScaler Gateway >** 门户主题，然后单击添加。
2. 输入自定义主题名称的名称。
3. 在 模板主题中，根据需要选择基本主题。默认情况下，**RfWebUI** 处于选中状态。
4. 单击确定。
5. 在“外观”部分中，根据主页的要求修改属性，然后单击“确定”。

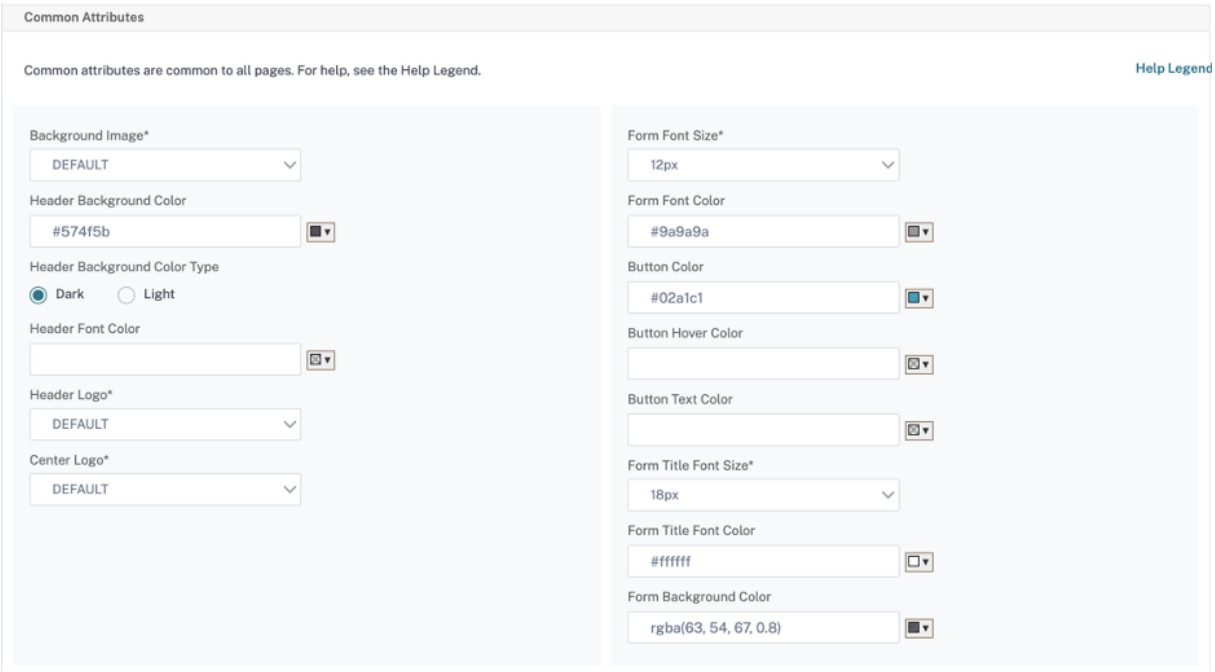


下图显示了基于 RfWebUi 的自定义主题。

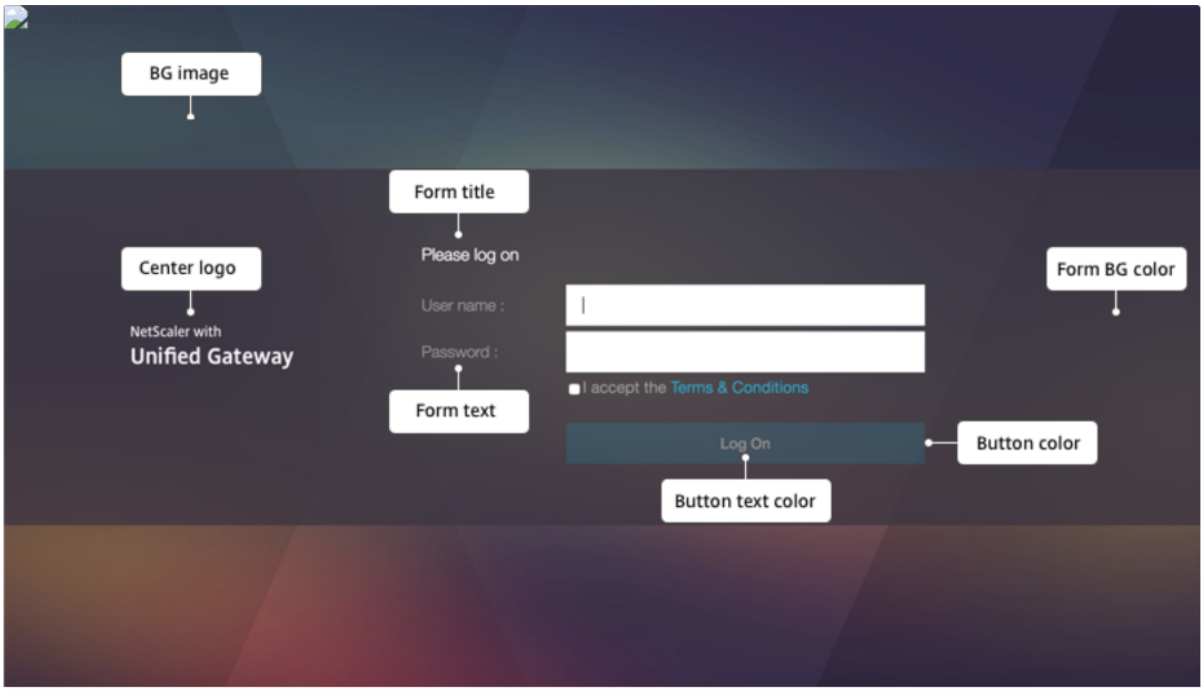
“帮助图例”链接会显示带有章节名称的图形页面显示，以帮助您选择要编辑的内容。

常用属性

“通用属性”部分提供了所有 NetScaler Gateway 登录页面通用的可配置设置。

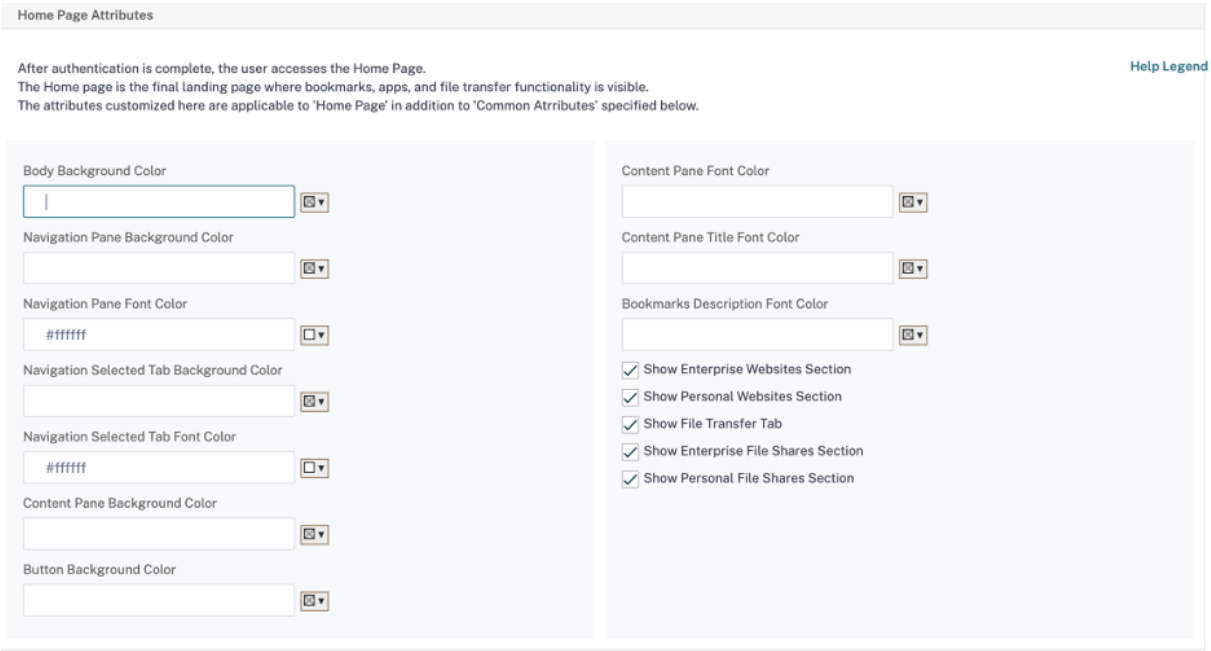


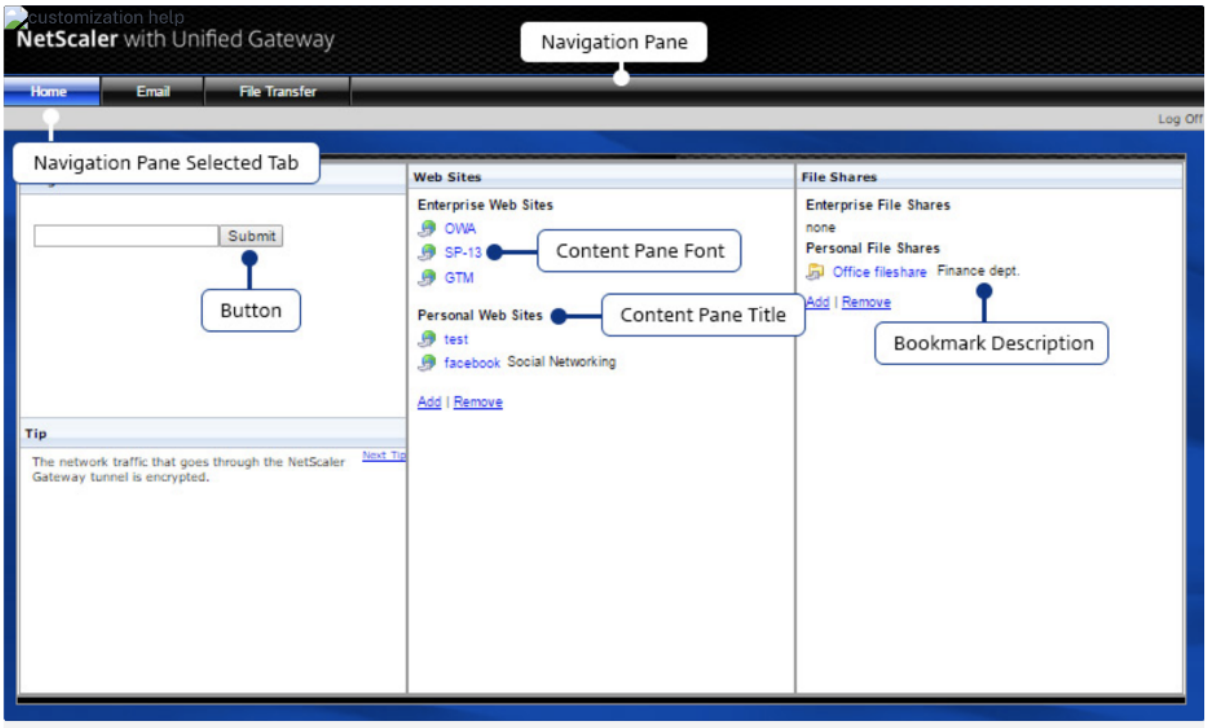
单击“帮助图例”链接可查看每个常用的可配置参数。

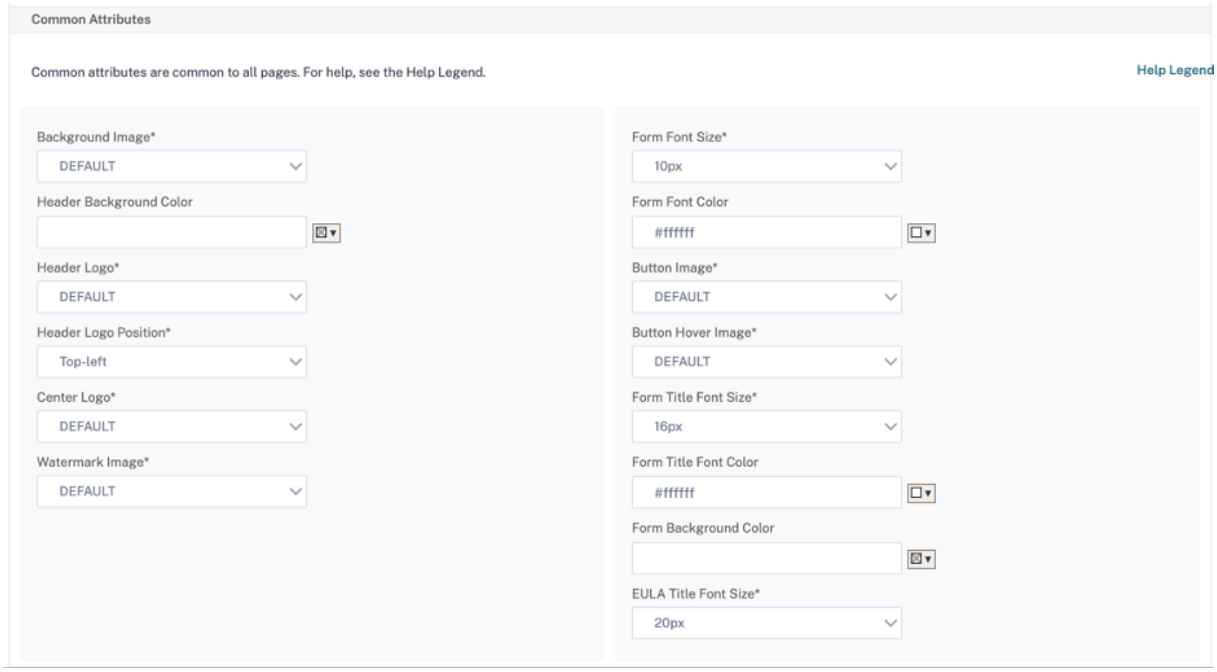


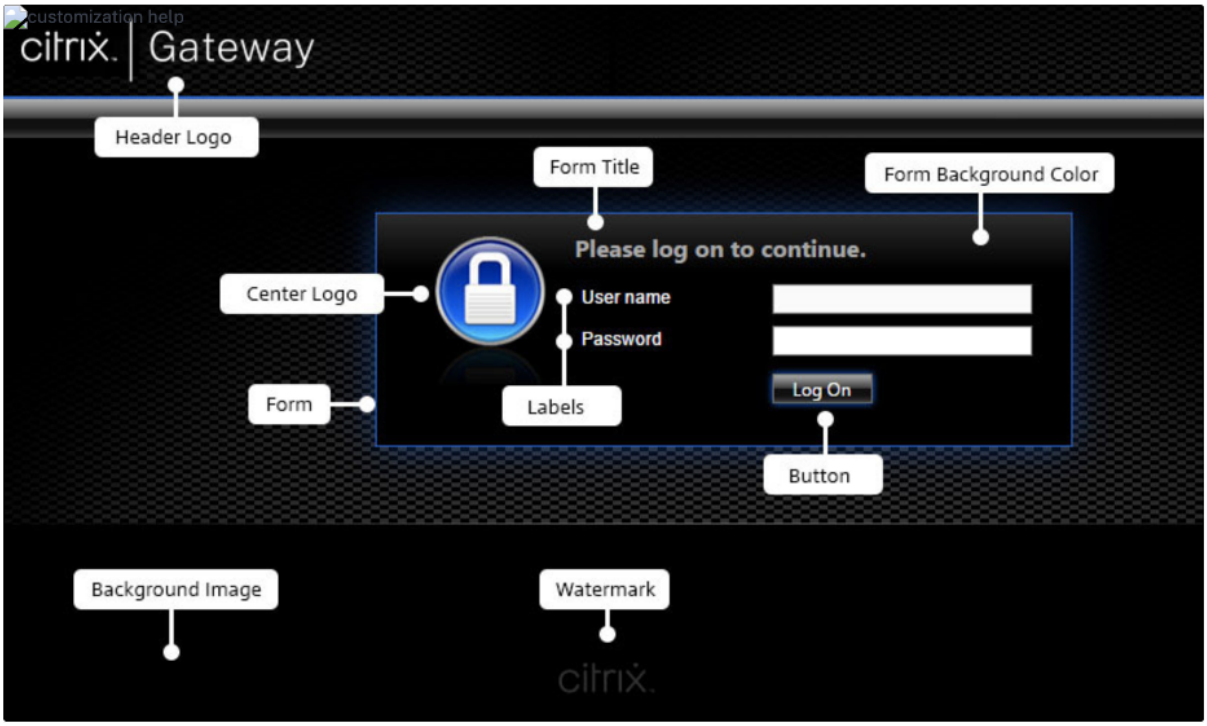
同样，对于基于 **Default** 的自定义主题，下图显示了主页的可用配置。

注意：这个配置对于 x1 和 GreenBubble 来说是不同的。







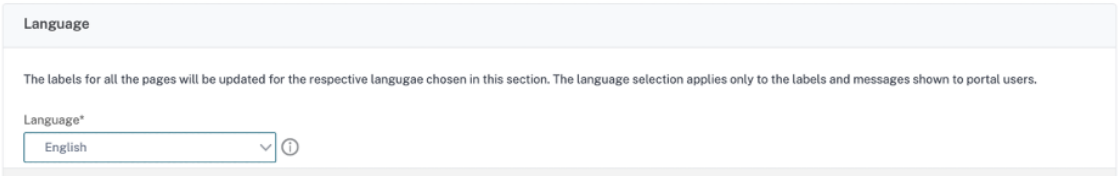


字符串自定义

除了网关门户主页的外观和外观外，admin UI 还在所有页面上启用字符串自定义。

要自定义字符串，请执行以下步骤：

1. 选择要编辑字符串的语言。字符串将以所选语言显示。默认情况下会选择英语。



注意：您选择的语言不会定义门户主题语言。它是为其自定义字符串的语言。

2. 在右侧的“高级设置”中，列出了可用于字符串自定义的页面。

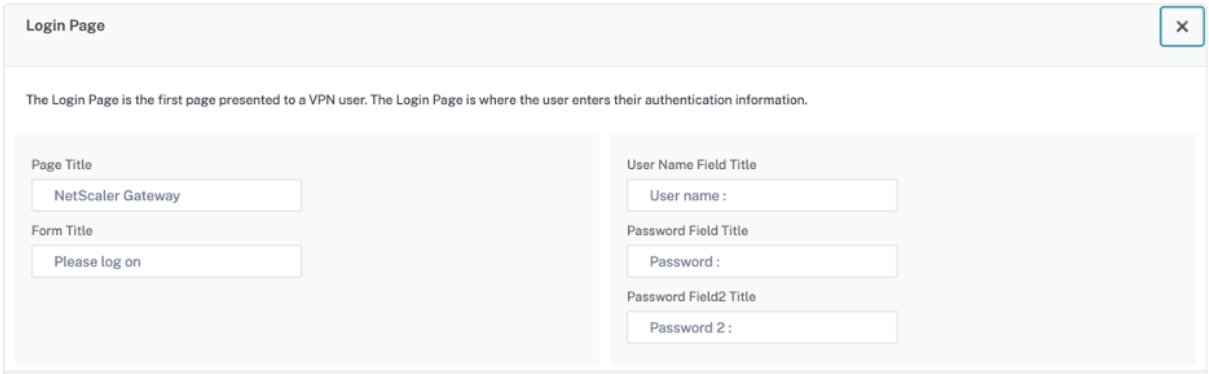
   - “登录”页面
   - EPA 页面
   - EPA 错误页面
   - EPA 后页面
   - “VPN 连接”页面
   - 主页

3. 选择要为其自定义字符串的页面，然后单击“编辑”图标。将显示带有预填字符串自定义项的表单。
4. 选择字段，然后根据需要添加或编辑字符串。
5. 单击 完成 以完成自定义门户主题的创建。稍后可以通过 **NetScaler Gateway >** 门户主题编辑主题。

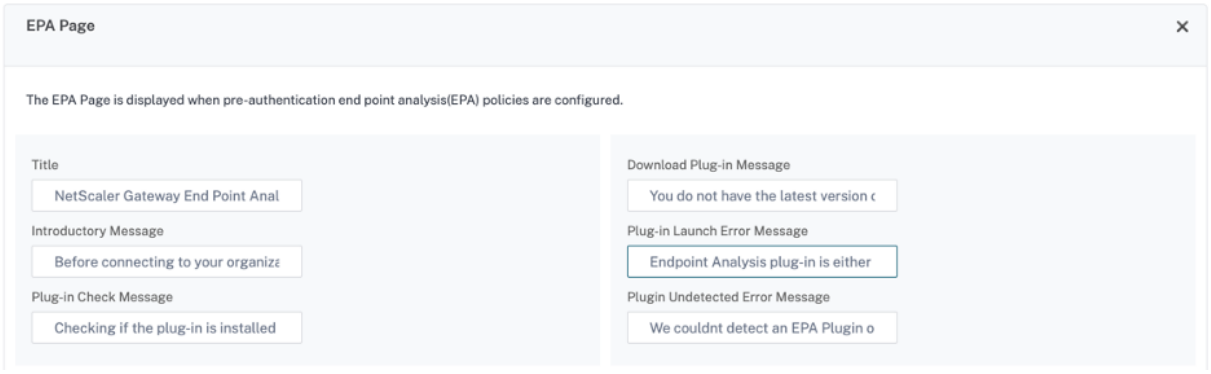
注意：如果该分区仍以先前选择的语言显示字符串，则可能是该部分在更改语言时已经打开。在这种情况下，请关闭该部分，选择语言，然后再次从“高级设置”中打开页面。

以下屏幕截图显示了每个页面可用的可自定义字符串集。

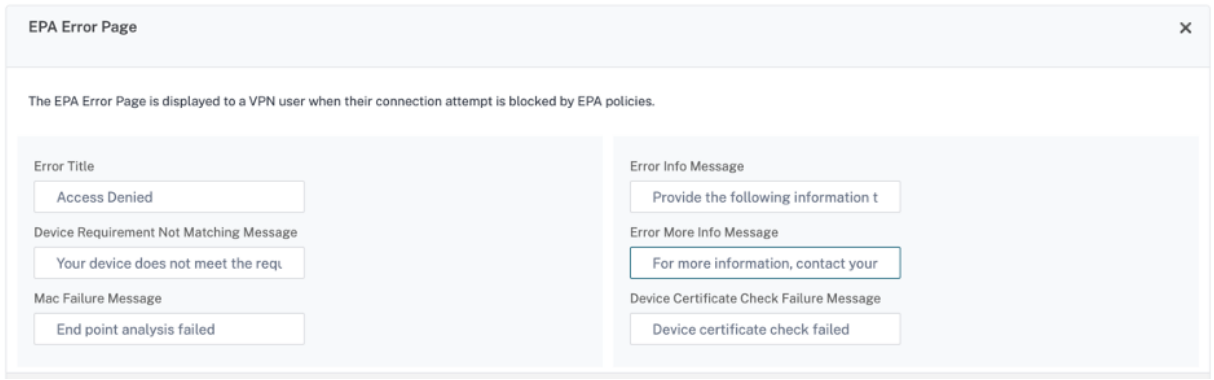
登录页面：



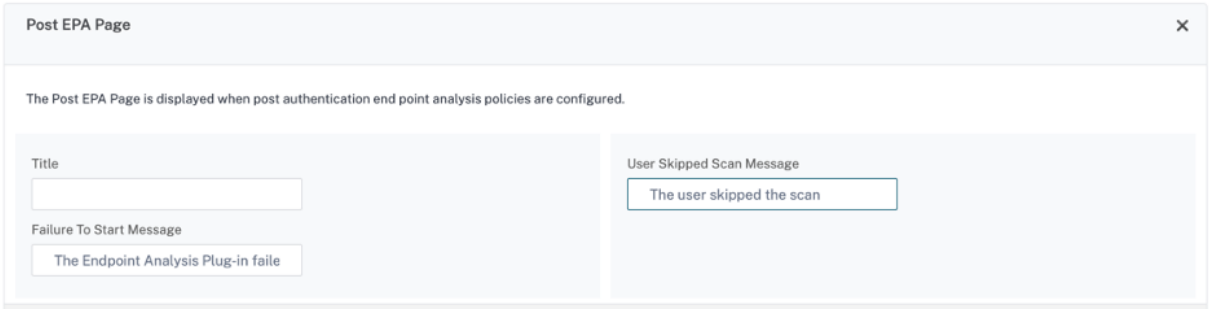
EPA 页面：



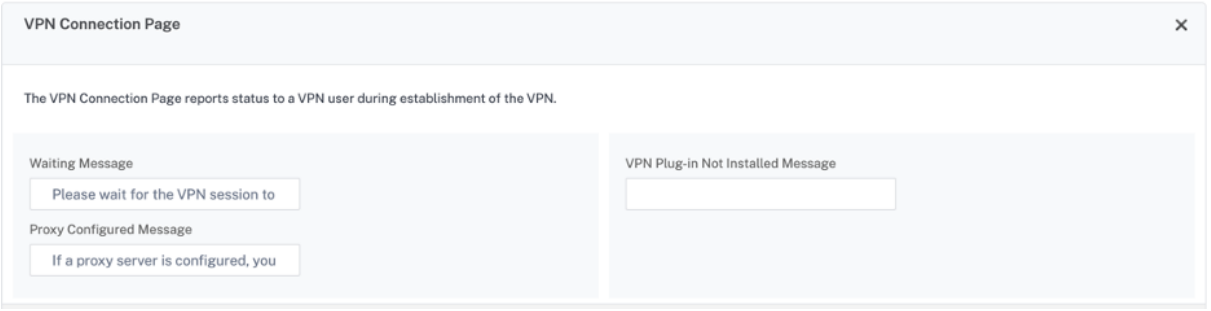
EPA 错误页面：



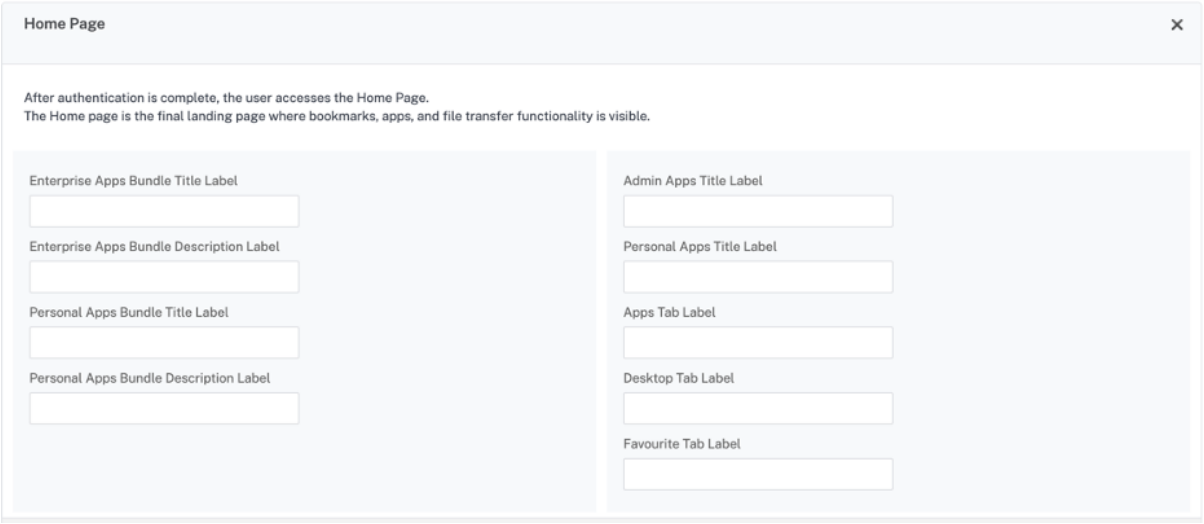
EPA 后页面：



VPN 连接页面：



主页：



为 **Office365** 优化 **NetScaler Gateway VPN** 拆分通道

February 1, 2024

随着组织比以往更快地适应远程办公选项，因此必须优化远程访问基础架构，以便在流量负载增加的情况下实现无缝连接。

> 重要提示：
>
> Microsoft 建议使用已发布的 IPv4 和 IPv6 地址范围配置分割通道，将发往关键 Office 365 服务的流量排除在 VPN 连接范围之外。为了获得最佳性能和最有效地利用 VPN 容量，必须在 VPN 通道之外直接路由到与以下应用程序关联的专用 IP 地址范围的流量：
>
> - Office 365 Exchange Online
> - SharePoint Online
> - Microsoft Teams（在 Microsoft 文档中称为“优化”类别）
>
> 有关此建议的更多详细信息，请参阅 Microsoft 指南 。

Microsoft 在 NetScaler Gateway 中的建议是通过使用拆分通道反向配置将 Microsoft 提供的 IP 地址列表直接路由到互联网以获取 O365 流量来实现的。

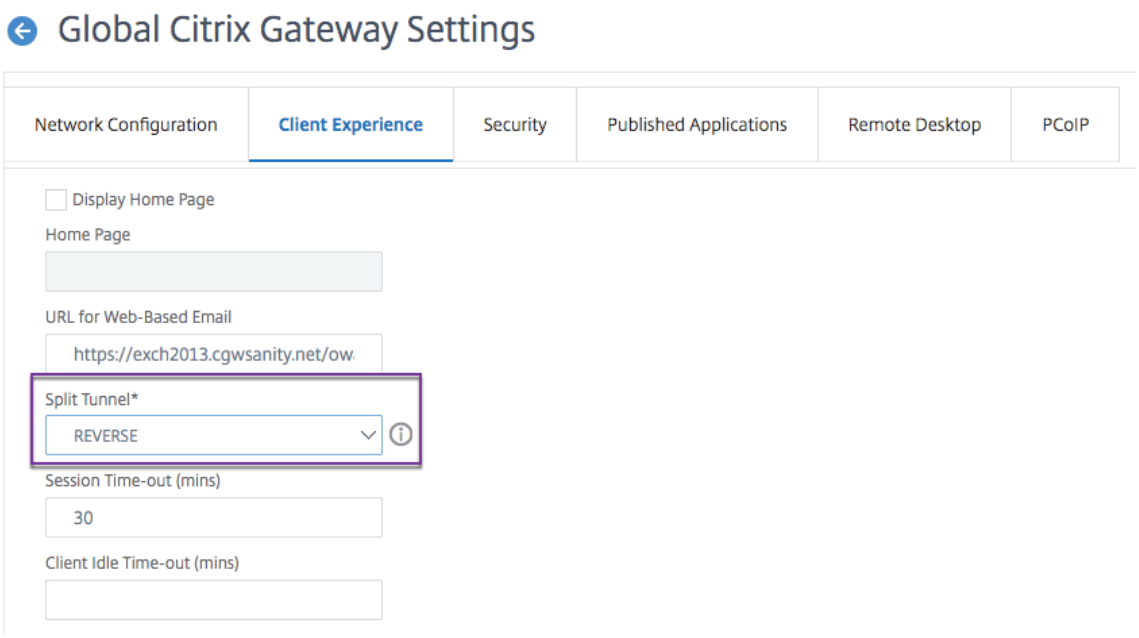
配置涉及以下内容，可使用 GUI 或 CLI 手动执行：

- 为反向配置配置配置分割通道。有关详细信息，请参阅 拆分通道选项。
- 配置内联网应用程序以使用户访问资源。

使用 **GUI** 进行配置

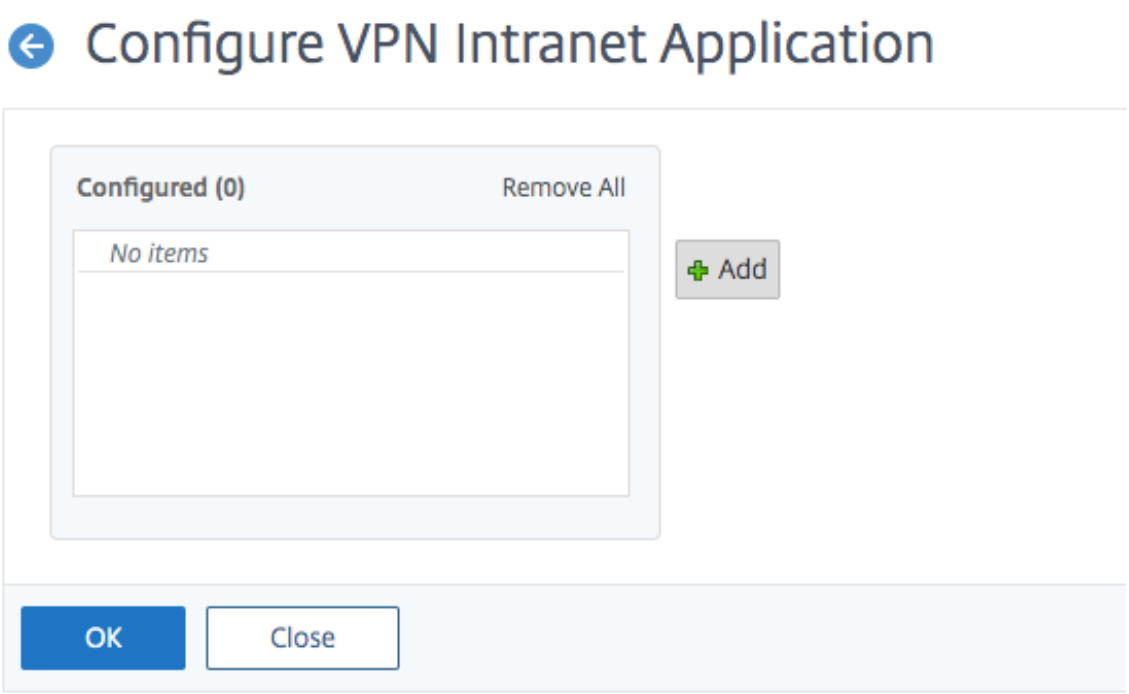
使用 **GUI** 配置拆分通道

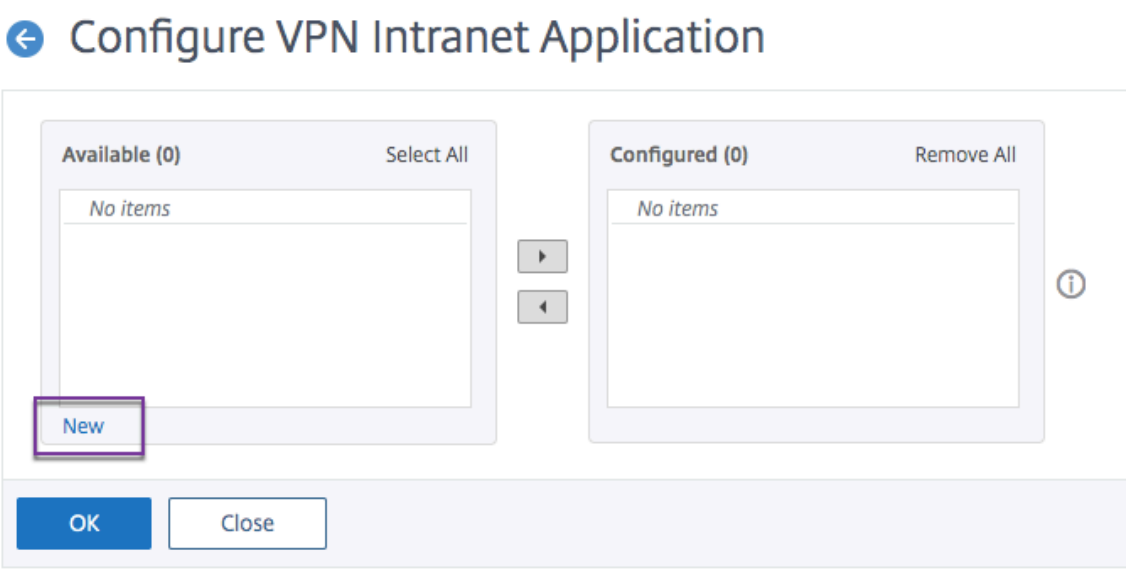
1. 在“配置”选项卡上，导航到 **NetScaler Gateway>** 全局设置。
2. 在详细信息窗格的“设置”下，单击“更改全局设置”。
3. 在 客户端体验 选项卡的 拆分通道中，选择 反向。
4. 单击确定。



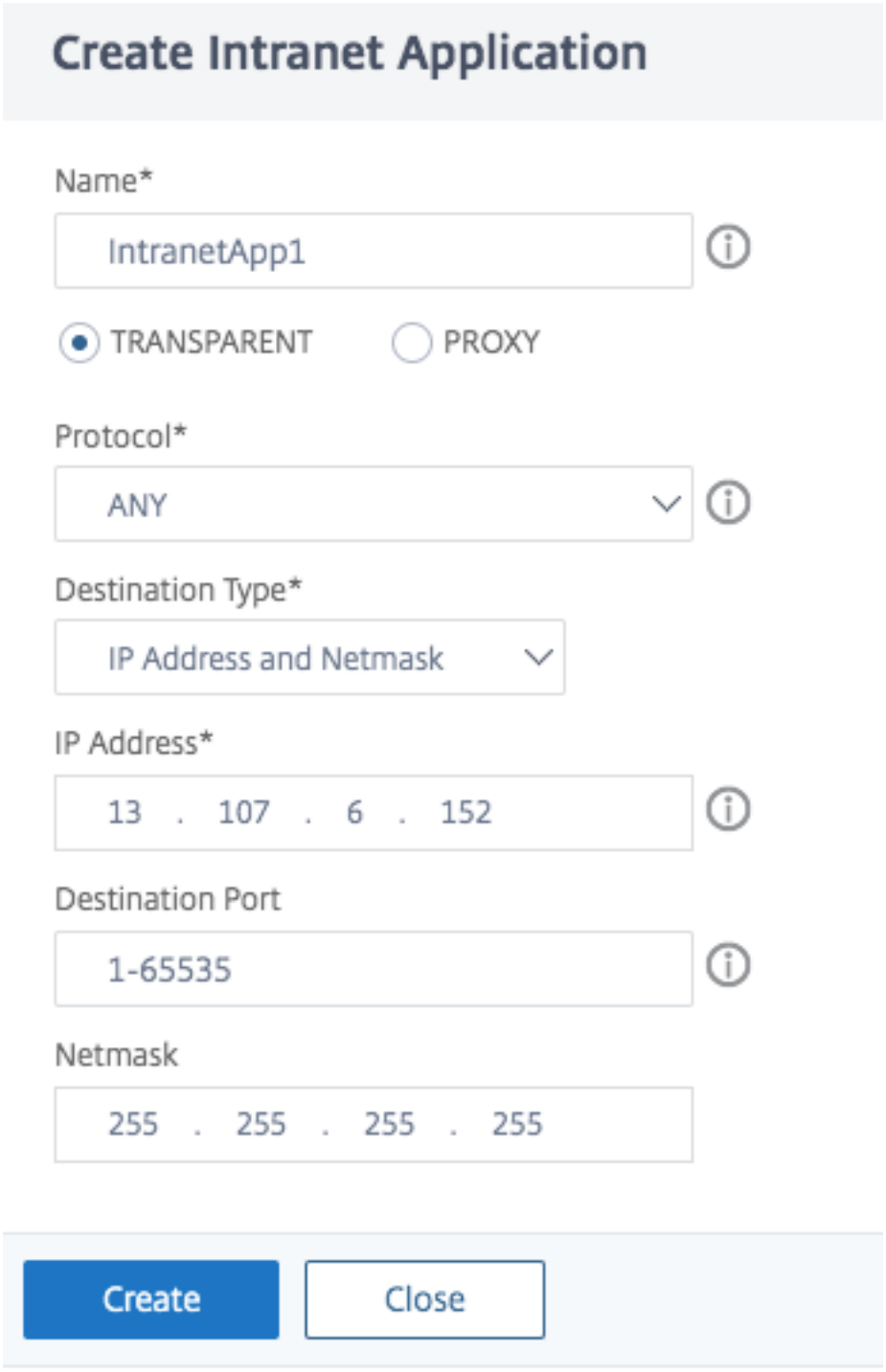
使用 **GUI** 创建 **VPN** 内部网应用程序

1. 在配置选项卡上，导航到 **Citrix Gateway >** 全局设置。
2. 在详细信息窗格中的 **Intranet** 应用程序下，单击链接。
3. 在“配置 **VPN Intranet** 应用程序”页中，单击“添加”，然后单击“新建”。





4. 在名称中，键入配置文件的名称。
5. 在协议中，选择适用于网络资源的协议。
6. 在目标类型中，选择 **IP** 地址和网络掩码。
7. 在 **IP** 地址中，输入 O365 流量必须直接路由到互联网的 IP 地址。有关 IP 地址的列表，请参阅 IP 地址列表。
8. 在 网络掩码中，输入网络掩码 IP 地址。



9. 单击 **Create**（创建），然后单击 **Close**（关闭）。

注意：对所有 IP 地址重复此过程。

使用 **CLI** 进行配置

- 要将拆分通道设置为反向，请在命令提示符下键入；

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- 要添加 VPN Intranet 应用程序，请在命令提示符下键入；

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
    255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

注意：对所有 IP 地址重复此过程。

- 要绑定 Intranet 应用程序，请在命令提示符下键入；

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

Office 365 服务（**EXO**、**SPO** 和 **Microsoft Teams**）的 **IP** 地址列表

参考资料：https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

> 来自 **Microsoft** 的说明：
>
> 作为 Microsoft 对 COVID-19 局势的回应的一部分，Microsoft 宣布暂时暂停一些计划中的 URL 和 IP 地址变更。此暂停旨在使客户 IT 团队能够自信、简单地实施针对在家办公 Office 365 场景的推荐网络优化。从 2020 年 3 月 24 日至 2020 年 6 月 30 日，这项暂停措施将停止更改关键 Office 365 服务（在线 Exchange、SharePoint Online 和 Microsoft Teams）对“优化”类别中包含的 IP 范围和 URL 的更改。

IPv4 地址范围

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22
150.171.40.0/22

191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

IPv6 地址范围

2603:1006::/40
2603:1016::/36
2603:1026::/36
2603:1036::/36
2603:1046::/36
2603:1056::/36
2603:1096::/38
2603:1096:400::/40
2603:1096:600::/40
2603:1096:a00::/39
2603:1096:c00::/40
2603:10a6:200::/40
2603:10a6:400::/40
2603:10a6:600::/40
2603:10a6:800::/40
2603:10d6:200::/40
2620:1ec:4::152/128
2620:1ec:4::153/128
2620:1ec:c::10/128
2620:1ec:c::11/128
2620:1ec:d::10/128
2620:1ec:d::11/128
2620:1ec:8f0::/46
2620:1ec:900::/46
2620:1ec:a92::152/128
2620:1ec:a92::153/128

2a01:111:f400::/48
2620:1ec:8f8::/46
2620:1ec:908::/46
2a01:111:f402::/48

UDP 流量的服务支持类型

February 1, 2024

对 UDP 的服务类型 (ToS) 支持可确保一旦发件人为 UDP 数据包配置了 ToS 值，NetScaler Gateway 将保留该值，直到数据包到达目的地为止。根据配置的值和目标网络的配置，目的网络将 UDP 数据包放入优先级出站队列中。

> 注意
> 使用 ToS 信息，您可以为每个 IP 数据包分配优先级，并请求特定处理，例如高吞吐量、高可靠性、低延迟等。

配置服务器名称指示扩展

February 1, 2024

现在可以将 NetScaler Gateway 设备配置为在发送到后端服务器的 SSL“客户端您好”数据包中包含服务器名称指示 (SNI) 扩展。SNI 扩展可帮助后端服务器识别 SSL 握手期间请求的 FQDN，并使用相应的证书进行响应。

> 注意
>
> 当多个 SSL 域托管在同一台服务器上时启用 SNI 支持。

要使用 **GUI** 将 **NetScaler Gateway** 配置为支持 **SNI**：

1. 在 NetScaler GUI 中，导航到“配置”**>**“**NetScaler**”**>**“全局设置”。
2. 单击“更改全局设置”链接，然后从“后端服务器 **SNI**”菜单中选择“启用”。

要使用命令行界面将 **NetScaler Gateway** 配置为支持 **SNI**，请在命令提示符下键入：

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

在 SSL 握手期间验证服务器证书

February 1, 2024

现在可以将 NetScaler Gateway 设备配置为在 SSL 握手期间验证后端服务器提供的服务器证书。

使用配置实用程序配置 NetScaler Gateway 全局参数以支持出站代理的 PAC

绑定 CA 证书

1. 导航到 配置 >**NetScaler Gateway** > **NetScaler Gateway** 策略管理器 > 证书绑定。**
2. 在 证书绑定 屏幕上，单击 **+** 图标。
3. 在 **CA** 证书绑定屏幕上，单击 添加绑定，然后单击 安装。
4. 在“证书文件名”字段中选择 证书文件名，然后单击“安装”。
5. 在 **CA** 证书绑定 屏幕上，选择证书，然后单击 绑定。
6. 单击 **Done**（完成）。

启用证书验证：

1. 导航到 **NetScaler Gateway >** 全局设置。
2. 单击“更改全局设置”。**
3. 从 后端服务器证书验证 下拉菜单中选择 已启用，然后单击 确定。

使用命令行配置 NetScaler Gateway 全局参数以支持服务器证书

在命令提示符下，键入以下命令：

```
1      bind vpn global cacert DNPGCA1
2
3      set vpn parameter backendcertValidation ENABLED
4  <!--NeedCopy-->
```

使用模板简化了 **SaaS** 应用程序配置

February 1, 2024

通过为流行的 SaaS 应用程序配置模板下拉菜单，可以简化 NetScaler Gateway 上使用单点登录的 SaaS 应用程序配置。可以从菜单中选择要配置的 SaaS 应用程序。该模板预先填充了配置应用程序所需的大部分信息。但是，仍然必须提供特定于客户的信息。

> 注意：
>
> 要配置和发布 SaaS 应用程序，请在 NetScaler Gateway 上配置和发布，然后在应用服务器上进行配置和发布。
>
> 下一节中的步骤将帮助您使用模板在 NetScaler Gateway 上配置和发布应用程序。然后转到介绍如何在应用服务器上配置和发布的部分。

使用模板配置和发布应用程序-**NetScaler Gateway** 特定配置

以下配置使用 AWS 控制台应用程序作为示例，说明如何使用模板配置和发布应用程序。

在开始之前，您需要以下内容：

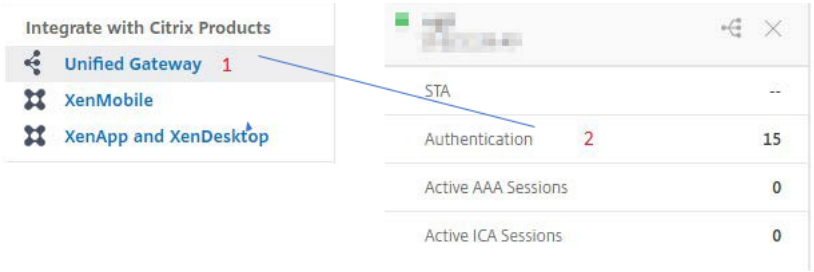
- AWS 控制台的管理员帐户
- NetScaler Gateway 的管理员帐户

AWS 控制台配置步骤如下：

1. 使用应用程序目录配置 AWS 控制台。
2. 从 NetScaler 导出 AWS 控制台 IdP 元数据。
3. 在 AWS 控制台中配置 IdP。

步骤 **1**：使用应用程序目录配置 AWS 控制台

1. 单击 **Unified Gateway >** 身份验证。

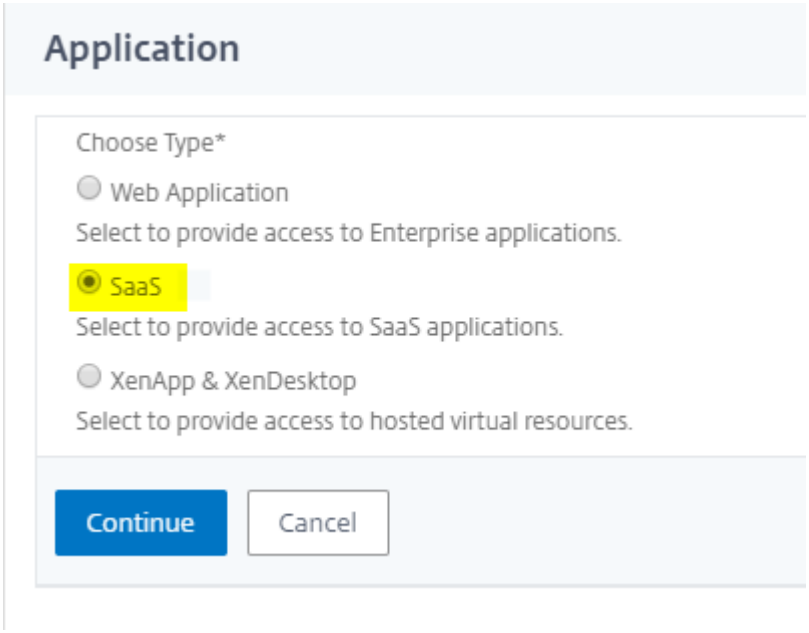


   此时将显示 Unified Gateway 配置屏幕。

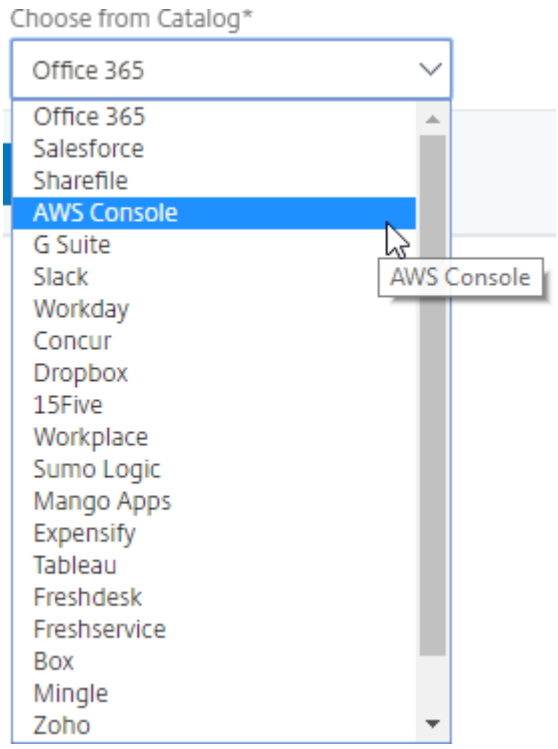
2. 在 应用程序 部分，单击编辑图标。现在，单击加号图标。此时将出现应用程序窗口

   应用程序

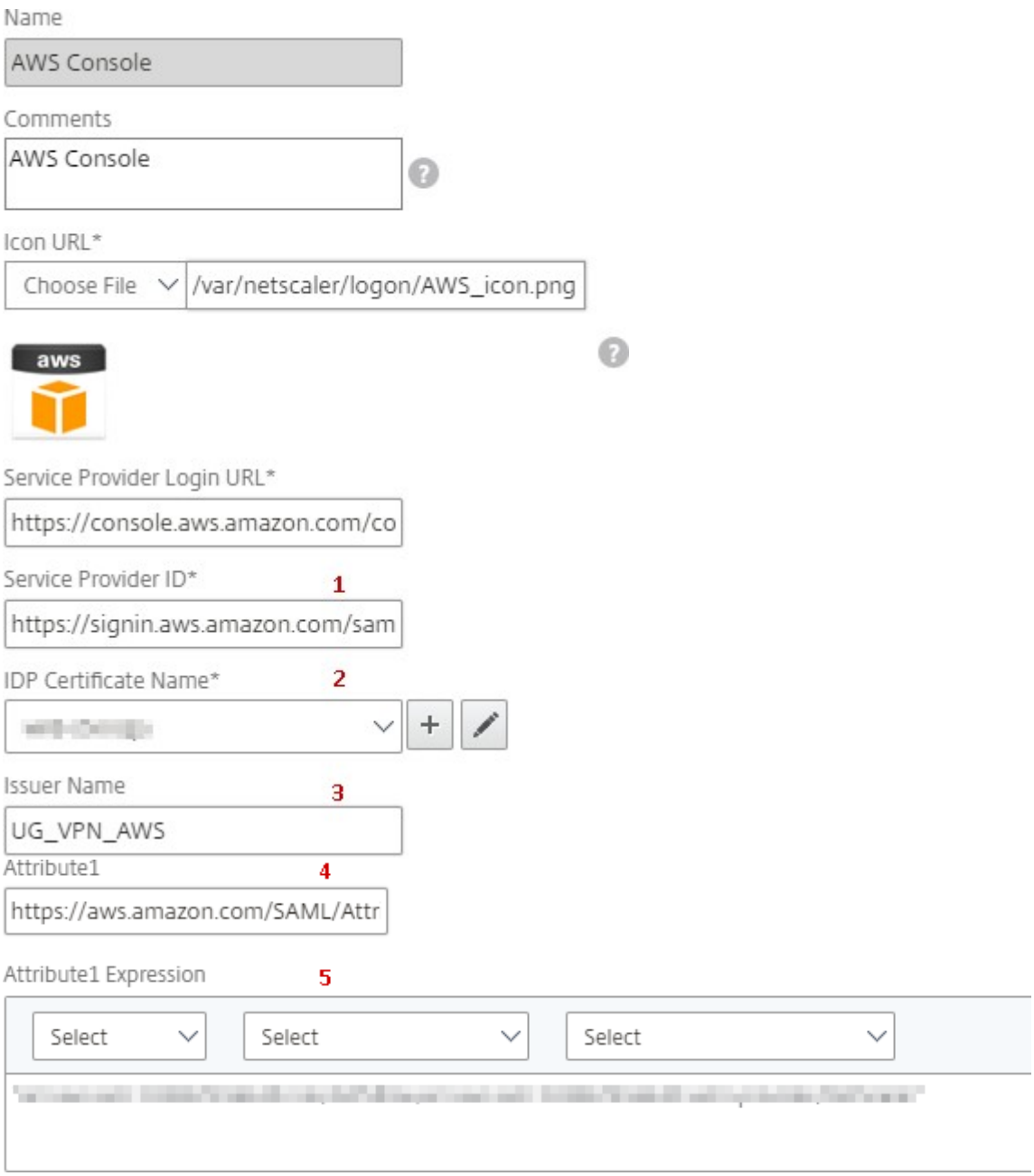
3. 从应用程序类型中选择 **SaaS** 。



4. 从下拉列表中选择 **AWS** 控制台。



5. 使用适当的值填充应用程序模板。



6. 输入以下 SAML 配置详细信息，然后单击 继续。

   服务提供商 **ID** —https://signin.aws.amazon.com/saml

   签名证书名称—必须选择 IdP 证书

   发行人名称—发行人名称可以根据您的选择填写

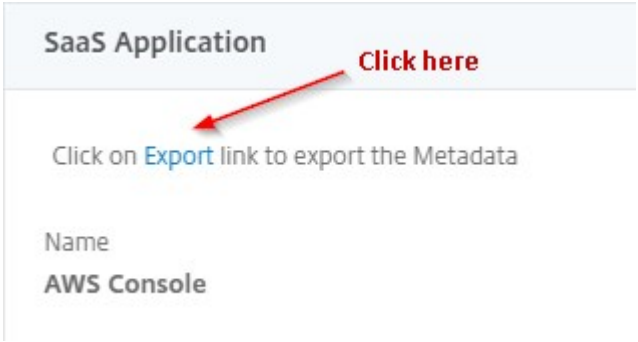
   属性 **1** —`https://aws.amazon.com/SAML/Attributes/Role`

   Attribute1 表达式 - `Role ARN, IdP ARN`，如步骤 3 所示

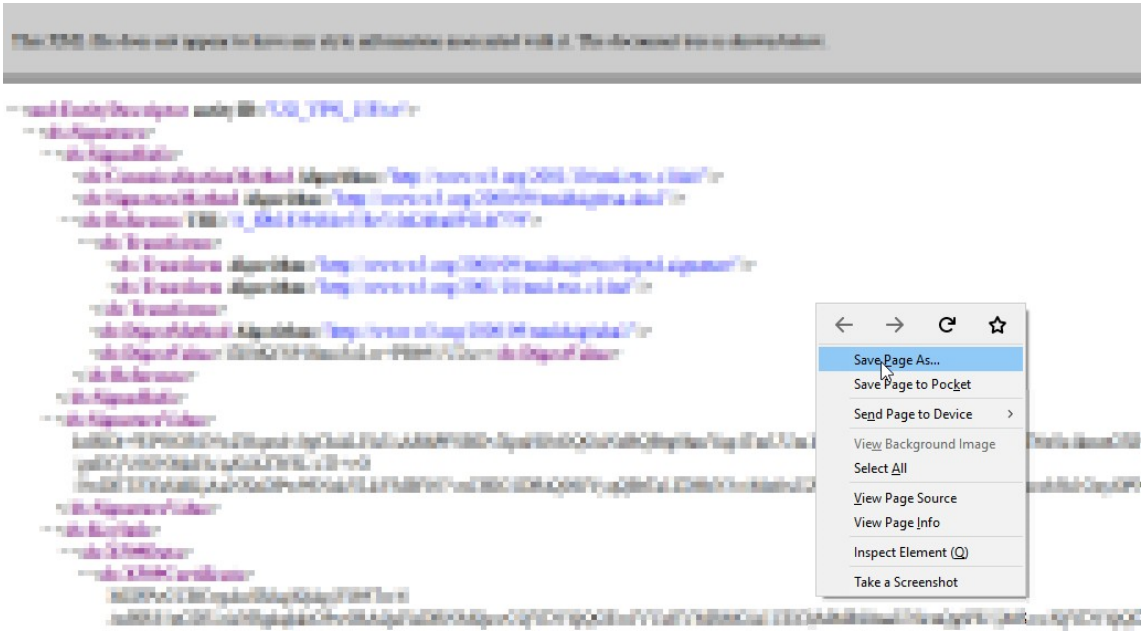
7. 单击 **Done**（完成）。

步骤 **2**：从 NetScaler Gateway 导出 AWS 控制台 IdP 元数据。

1. 单击 **Unified Gateway >** 身份验证。
2. 向下滚动并单击 **AWS** 控制台 模板。此时将显示 SaaS 应用程序窗口。单击 导出 链接。



3. 元数据 将在不同的窗口中打开。保存 **IdP** 元数据文件



步骤 **3**：在 AWS 控制台中配置 IdP。

使用模板配置和发布应用程序-特定于应用服务器

以下链接打开 PDF 文档，这些文档为使用模板配置和发布流行的 SaaS 应用程序提供了具体指导

- 15Five
- Absorb
- Accompa
- Adobe Captivate Prime

- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence
- Contactzilla
- Convo
- Circonus

- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub
- GlassFrog
- GotoMeeting
- HappyFox

- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript
- Marketo
- Mingle
- Mixpanel

- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard
- Remedyforce
- Robin
- Rollbar

- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria
- Testable
- TestFairy
- TextExpander

- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck
- Zendesk
- ZIVVER
- Zoho One

- ZIVVER
- Zoom