Citrix Application Delivery Management 13.0

Machine translated content

Disclaimer

Contents

发行说明

April 23, 2021

Citrix Application Delivery Management (ADM) 13.0 发行说明描述了构建中的新功能、对现有功能的增强以及已知问题。13.0 版本的发行说明文档包括以下部分：

- 新增功能：构建中发布的现有功能的新功能和增强功能。
- 已知问题：构建中存在的问题及其解决方法（如果适用）。
- 已修复的问题：构建中解决的问题。

要查看完整的发行说明文档，请单击以下链接。

发行说明	发布日期	版本
Citrix ADM 13.0 版本的版本 79.64 的发布说明	发布时间：2021 年 4 月 6 日	发行说明版本：1.0
Citrix ADM 13.0 版本的版本 76.29 的发布说明	发布时间：2021 年 2 月 19 日	发行说明版本：1.0
Citrix ADM 13.0 版本的版本 71.40 的发布说明	发布时间：2021 年 1 月 20 日	发行说明版本：2.0
Citrix ADM 13.0 版本的版本 67.42 的发布说明	发布时间：2020 年 10 月 28 日	发行说明版本：1.0。注意：构建 67.42 取代了构建 67.39
Citrix ADM 13.0 版本的版本 67.39 的发布说明	发布时间：2020 年 10 月 16 日	发行说明版本：2.0
Citrix ADM 13.0 版本的版本 64.35 的发布说明	发布时间：2020 年 10 月 16 日	发行说明版本：2.0
Citrix ADM 13.0 版本的版本 61.48 的发布说明	发布时间：2020 年 9 月 18 日	发行说明版本：2.0
Citrix ADM 13.0 版本版本 58.30 版本的发行说明	发表时间：二零一七年六月十日	发行说明版本：1.0
Citrix ADM 13.0 版本的版本 52.24 版本的发行说明	发表时间：二零一八年三月二十六日	发行说明版本：1.0
Citrix ADM 13.0 版本的版本 47.22 版本的发行说明	发布日期：二零一九年十二月十日	发行说明版本：1.0
Citrix ADM 13.0 版本的版本 41.28 版本的发行说明	发布日期：2019 年 9 月 27 日（建立 41.28 取代了建立 41.22）	发行说明版本：1.0

> 注意
>
> 这些发行说明不记录与安全相关的修补程序。有关与安全相关的修补程序和通知的列表，请参阅 Citrix 安全公告。

将本地 **Citrix ADM** 迁移到 **Citrix Cloud**

April 23, 2021

您可以将本地 **Citrix ADM 13.0 64.35** 或更高版本迁移到 Citrix Cloud。如果您的 ADM 有 12.1 或更早版本，则必须首先升级到 **13.0 64.35** 或更高版本，然后迁移到 Citrix Cloud。有关详细信息，请参阅升级部分。

通过 Citrix Cloud 提供的 ADM 服务使您能够获得：

- 更快的发布，大约每两周发布一次，最新功能更新。
- 基于机器学习的分析，用于应用程序安全性和机器人、性能和使用。
- 目前仅在 ADM 服务中支持的其他各种功能，例如高峰期和精益期分析、针对应用程序安全和机器人的基于机器学习的分析、应用程序 CPU 分析等。

要成功迁移，您必须：

- 确保在本地 ADM 中连接互联网，以实现 Citrix Cloud 可访问性
- 配置 ADM 服务代理
- 从 Citrix Cloud 获取客户端和秘密 CSV 文件
- 验证 ADM 服务许可
- 使用脚本迁移

配置 **ADM** 服务代理

要启用 Citrix ADC 实例和 Citrix ADM 之间的通信，必须配置代理。默认情况下，Citrix ADM 代理会自动升级到最新版本。您还可以选择代理升级的特定时间。有关详细信息，请参阅配置代理升级设置。

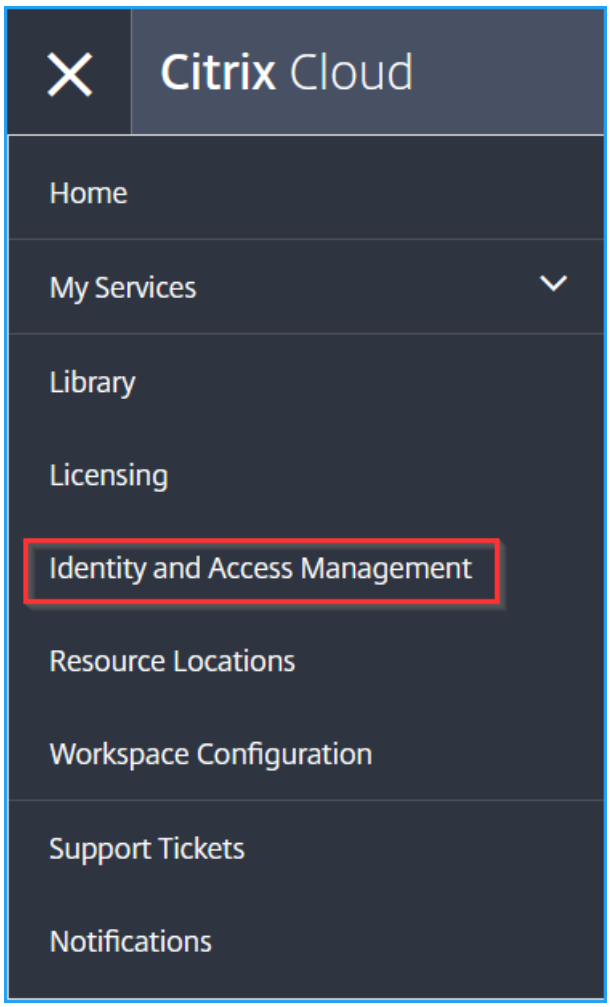
- 如果您现有的本地 ADM（独立或 HA 对）未配置本地代理，则必须为 ADM 服务至少配置一个代理。
- 如果您现有的本地 ADM（独立或高可用性对）已为多站点部署配置了本地代理，则必须为 ADM 服务配置相同数量的代理。

有关配置代理的详细信息，请参阅入门部分。

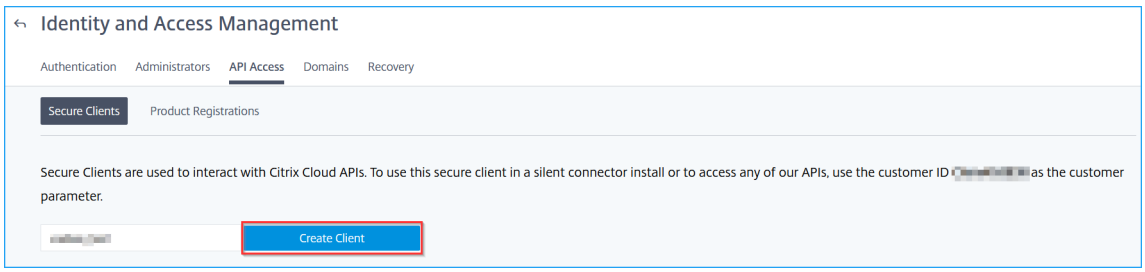
从 **Citrix Cloud** 获取客户端和秘密 **CSV** 文件

配置代理后，从 Citrix Cloud 页面获取客户端和密钥 CSV 文件：

1. 登录 citrix.cloud.com
2. 单击主页图标，然后选择身份和访问管理

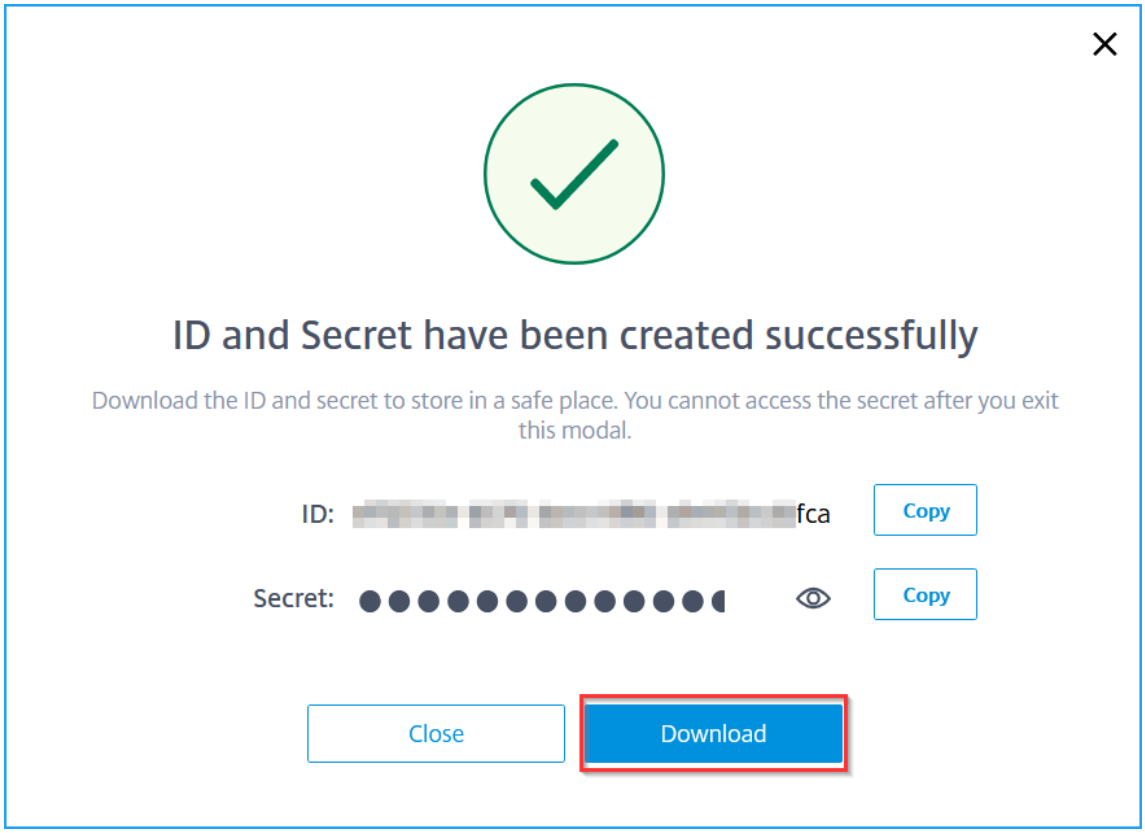


3. 在 **API** 访问选项卡中，输入安全客户端名称，然后单击 创建客户端。



4. 生成 ID 和密码。单击 下载并将 CSV 文件保存在本地 ADM 中。

   例如，将 CSV 文件保存到 /var 目录。



验证 **ADM** 服务许可证

您必须获得 ADM 服务的许可证。

- ADM 服务中的 VIP 许可证必须大于或等于本地 VIP 许可证。

  > 注意：
  >
  > 如果 VIP 许可证较少，则会随机选择虚拟服务器，ADM 服务的 VIP 级配置将失败。

- 如果将 ADM 本地部署用作许可证服务器，请在迁移之前将许可证重新分配给 ADM Service。有关详细信息，请参阅仅将 ADM 服务器配置为池许可证服务器和如何重新分配许可证文件。
- 如果您在本地 ADM 中使用池许可证，则必须获取 ADM 服务的池许可证，然后将许可证分配给 ADC 实例。有关详细信息，请参阅配置池许可。以下受支持的 ADC 版本使您能够修改 ADM 的许可证分配：
  - Citrix ADC SDX：13.0 74.11 或更高版本。
  - Citrix ADC VPX 和 MPX：13.0 47.24 或更高版本、12.1 58.14 或更高版本以及 11.1 65.10 或更高版本。

使用脚本迁移

- 对于 ADM 76.x 或更高版本的构建，迁移脚本(`servicemigrationtool.py` 和 `config_collect_onprem.py`）可作为构建的一部分提供，请参阅 `cd /mps/scripts`。
- 对于早于 76.x 版本的 ADM，您必须下载迁移脚本并在本地 ADM 中复制脚本。

> 注意
>
> 确保本地 ADM 在迁移期间具有互联网连接。

1. 使用 SSH 客户端登录本地 ADM。

> 注意
>
> 对于 ADM HA 对，请登录主节点。

2. 键入 **shell** ，然后按 **Enter** 键切换到 bash 模式。
3. 复制客户端 ID 和秘密 CSV 文件。例如，将文件复制到 /var 目录。

   复制 CSV 文件后，您可以验证 CSV 文件是否存在。

```
bash-3.2# cd /var
bash-3.2# pwd
/var
bash-3.2# ls -ltr secureclient.csv
-rw-r--r--  1 root  nobody  102 Dec 11 19:09 secureclient.csv
bash-3.2#
```

> 注意
>
> 对于 ADM HA 对，请在主节点中复制 CSV 文件。

4. 对于 ADM **13.0 76.xx** 版本，请运行以下命令以完成迁移：

   a) `cd /mps/scripts`

   b) `python servicemigrationtool.py <path of ClientID/Secret File in on-premises Citrix ADM VM>`

   例如，`python servicemigrationtool.py /var/secureclient.csv`

5. 对于 13.0 76.xx 之前的 ADM：

   a) 从以下位置下载迁移脚本：
   `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigrationtool_27.tgz`

   下载的文件包括两个捆绑脚本，“service 迁 ationtool_27.py和config_collect_onprem_27.py‘。

   b) 将两个脚本保存在本地 ADM 中。例如，保存在 /var 目录中

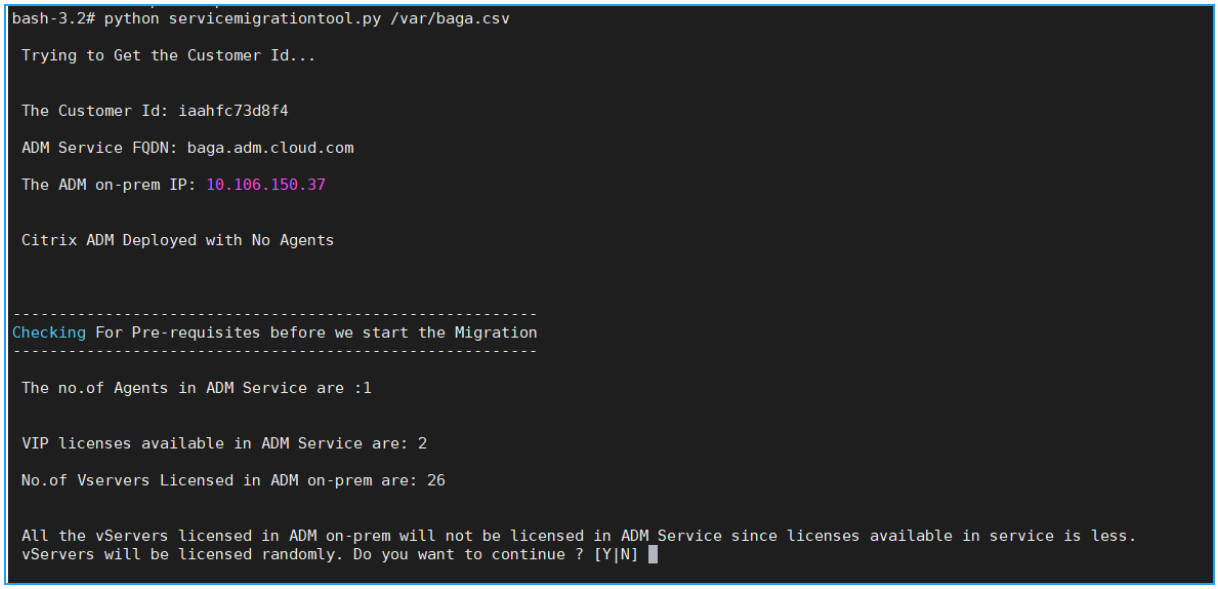
   c) 运行以下命令进行迁移：

i. `cd /var`

ii. `servicemigrationtool_27.py <path of ClientID/Secret File in on-premises ADM VM>`

例如，`python servicemigrationtool_27.py /var/secureclient.csv`

运行脚本后，它会检查先决条件，然后继续迁移。脚本首先检查许可证的可用性。仅当您的 ADM 服务许可证少于本地许可证时，才会显示以下消息。



如果选择 **Y**，则通过随机授予 VIP 许可来继续迁移。如果选择 **N**，脚本将停止迁移。

如果池许可证服务器的 ADC 实例版本不受支持，则会显示以下消息：


```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Changing of PooledLicense Server will be effective for below SDX/ADC versions
--------------------------------------------------------------------------------
  For SDX Versions: 13.0 74.11 Onwards
  For ADC Versions: 13.0 47.24 and Onwards
                    12.1 58.14 and Onwards
                    11.1 65.10 and Onwards
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------

 The List of ADCs supported for Pooled License Server change are:
['10.106.150.73', '10.102.60.25']

 The List of SDXs supported for Pooled License Server change are:
[]

 The List of ADCs not supported for Pooled License Server change are:
[]

 The List of SDXs not supported for Pooled License Server chagne are:
['10.102.103.238']

 Migration will change the License Server to ADM Service Agent.
 Do you want to change License Server in all the supported Pooled ADCs/SDXs ? [Y|N] n

 Do you want to continue with rest of the migration ? [Y|N]
```

如果选择 **Y**，则迁移过程会通过更改许可证服务器继续进行。如果选择 **N**，脚本将提示您是否要继续其余迁移。如果选择 **N**，脚本将停止迁移。

根据本地配置的不同，迁移完成的大约时间为几分钟到几小时。迁移完成后，您会看到以下消息：

```
--------------------------------------------------------------------------------
ADM OnPrem to ADM Service Configuration Migration is Complete.
Note: Please Look out for Failures and re-trigger the Tool after taking appropriate action.
--------------------------------------------------------------------------------
```

一旦所有 ADC 和 SD-WAN WANOP 实例及其各自的配置成功移动到 ADM 服务，迁移便会成功。成功迁移后，本地 Citrix ADM 将停止处理以下实例事件：

- SSL 证书
- 系统日志消息
- 备份
- 代理群集
- 绩效报告
- 配置审核
- Emon 调度程序

常见问题解答

April 23, 2021

ADM 服务

ADM 服务代理是否可选与本地 **Citrix ADM** 代理类似

不。ADM 服务代理是 ADM 服务的强制性，实例与 ADM 服务之间的所有通信都通过 ADM 服务代理进行。本地 ADM 代理是可选的；但是，您只能为节省带宽消耗配置本地代理。

为什么选择 **ADM** 服务

通过 Citrix Cloud 提供的 ADM 服务可提供以下优势，而无需新的定期构建：

- 基于云的 SaaS 产品与本地 Citrix ADM 相比，更容易入职，拥有成本更低。
- 更快的发布，大约每两周发布一次，最新功能更新。
- 基于机器学习的分析可实现应用程序安全性、性能和使用。
- 目前仅在 ADM 服务中支持的其他各种功能，例如高峰期和精益期分析、针对 WAF 和机器人的基于机器学习的应用安全分析、应用程序 CPU 分析等。

您还可以加入 Citrix ADM 服务月度网络研讨会，了解最新的产品功能和解决方案。使用以下链接注册参加网络研讨会：

https://attendee.gotowebinar.com/register/3423094569685671948

或

https://attendee.gotowebinar.com/register/6349500842104715533

如果本地 **Citrix ADM** 是 **HA** 对，迁移后会发生什么

所有配置都移动到 Citrix Cloud。不需要配置灾难恢复节点。

如果代理人出于任何原因停机会怎么办

在代理启动并运行之前，您可以预计潜在的数据丢失。但是，您还可以为多站点部署配置 ADM 代理，以确保在发生代理故障切换时的连续性。有关详细信息，请参阅为多站点部署配置 ADM 代理。

实例备份是否也迁移了

迁移中不包括备份。

历史数据也会迁移吗

历史数据不会迁移。您可以从本地 ADM 导出数据。

本地许可证是否也已迁移

不。本地许可证文件不能用于 ADM 服务。您必须获得 ADM 服务的许可证。有关详细信息，请参阅许可。如果您在本地 ADM 中使用池许可证，则必须获取 ADM 服务的池许可证，然后将许可证分配给实例。

什么不是从本地 **Citrix ADM** 迁移的

以下功能无法迁移到 ADM 服务：

- **RBAC** — 在 ADM 服务中，用户访问权限基于管理员的邀请。ADM 服务用户必须在 Citrix Cloud 中拥有帐户。因此，本地 ADM 用户不会迁移。
- 导出计划 — 导出计划包括各个页面的向下钻取和计划等详细信息。所有这些详细的导出计划都不会迁移。
- **SSL** 证书/密钥/**CSR** — ADM 服务只能显示 ADC SSL 证书/密钥/CSR。因此，上传到本地 Citrix ADM 的 SSL 证书/密钥不会迁移到 ADM 服务。

本地 **Citrix ADM** 与 **Citrix Director** 集成。集成会发生什么

Director 与 ADM 的集成目前仅在本地 ADM 中受支持。

迁移后，是否需要再次获得实例许可证或启用分析

您必须确保 ADM 服务中的许可证大于或等于本地 VIP 许可证。如果许可证已超过本地 Citrix ADM VIP，则虚拟服务器将自动获得许可。否则，许可证将随机分配。

迁移工具

运行迁移脚本后，将显示错误消息。问题可能是什么

将显示带有失败原因的日志文件。您可以采取适当的纠正措施，然后再次运行迁移脚本。一般来说，在运行迁移脚本之前，请确保：

- 配置 ADM 服务代理
- 获取 ADM 服务许可证
- 复制存储客户端和安全 CSV 文件的正确路径

ADC 实例的版本低于上述的池许可限制。如果选择 **“Y”** 选项来更改许可证服务器，会发生什么情况

只有受支持的 Citrix ADC MPX、VPX 和 SDX 版本才会更改许可证服务器。

如果迁移脚本有关 **ADC/SD-WAN WANOP** 实例的配置失败，会发生什么情况

ADC 和 SD-WAN WANOP 实例继续在本地 ADM 设置上工作。您可以根据建议的失败原因采取必要措施，然后再次运行迁移脚本。

如果一些 **ADC** 或 **SD-WAN WANOP** 实例无法转移到 **ADM** 服务，会发生什么情况。重新运行迁移脚本会帮助吗

是。重新运行脚本后，只迁移失败的实例。假设五个实例中有两个未能移动。在您采取纠正措施并重新运行迁移脚本后，之前成功移动的三个实例会显示“设备已存在”消息。之前失败的其他两个实例将成功迁移。

是否有日志文件来检查迁移状态

是的，在 `/var/mps/log/` 目录中生成一个日志文件。使用 python3.7 的 ADM 将日志文件作为 `servicemigrationtool.py.log`,而使用 python 2.7 的 ADM 将日志文件作为 `servicemigrationtool_27.py.log`。

如果会话在运行迁移脚本时终止会话会怎么样

您可以重新运行迁移脚本。在新会话中，上次会话中已添加的实例将显示为“设备已存在”，迁移将继续进一步。

如果 **ADM** 服务的许可证少于本地 **Citrix ADM** 并且迁移脚本已启动，会发生什么情况

运行迁移脚本后，将显示一条建议，提及许可证的次数较少，并提示继续或停止。如果要继续使用较小的许可证，虚拟服务器将从可用许可证中随机获得许可。

将本地 **Citrix ADM** 迁移到 **ADM** 服务快速帐户时会发生什么情况

ADM 服务 Express 帐户只有两个虚拟服务器许可证、两个样书配置包和两个配置作业。如果您的内部部署 ADM 具有超过这些配置，并且您使用 Express Account 启动迁移，则脚本只能迁移适用于 Express Account 的上述配置（两个虚拟服务器许可证、两个样书配置包和两个配置作业）

如果 **Citrix Cloud** 受邀用户（创建 **Citrix Cloud** 帐户的管理员用户除外）尝试迁移本地 **ADM** 设置，会发生什么情况

建议管理员运行迁移脚本。受邀用户没有管理员权限（AdminAUTSystem_Group）。因此，组、角色和策略迁移失败，并显示消息“用户没有权限”。

作为解决方案，管理员（创建 Citrix Cloud 帐户的人）可以将与受邀用户关联的组更改为“admin_group”。

故障排除

April 23, 2021

首次运行迁移脚本时，它会检查先决条件并继续进行迁移。如果满足所有先决条件，则迁移完成时没有任何错误。如果任何先决条件失败，脚本会显示带有原因的错误消息修复错误后，必须重新运行脚本。

> 注意
>
> 如果您看到显示“已存在”的错误消息，则表示：
>
> - 您可能已经运行迁移脚本一次以上，并且某些配置已迁移到 ADM 服务。
> - 在运行迁移脚本之前，您可能已经在 ADM 服务中手动创建了相同的配置。

请参阅以下一些错误消息：

将手动配置文件添加到 **ADM** 服务

```
==================Profiles Addition to ADM Service====================


60.26 : FAILURE : Profile 60.26 already exists


 The list of ADC profiles added to ADM Service are :

{'60.26': "['FAILURE']"}
```

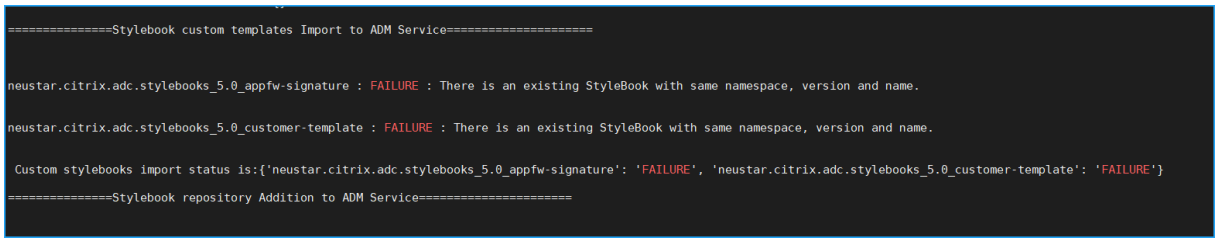
解决办法：如果在运行迁移脚本之前已在 Citrix ADM 服务中创建了管理员配置文件，请确保删除这些配置文件并重新运行迁移脚本。

将 **Citrix ADC** 设备添加到 **ADM** 服务

```
==============ADC Device Addition================

10.106.150.53 : FAILURE : Error in contacting Citrix ADC, invalid credentials.
10.102.60.26 : FAILURE :Device with this IP address already exists.


The list of ADCs added to ADM Service are:


['10.102.60.26']
```

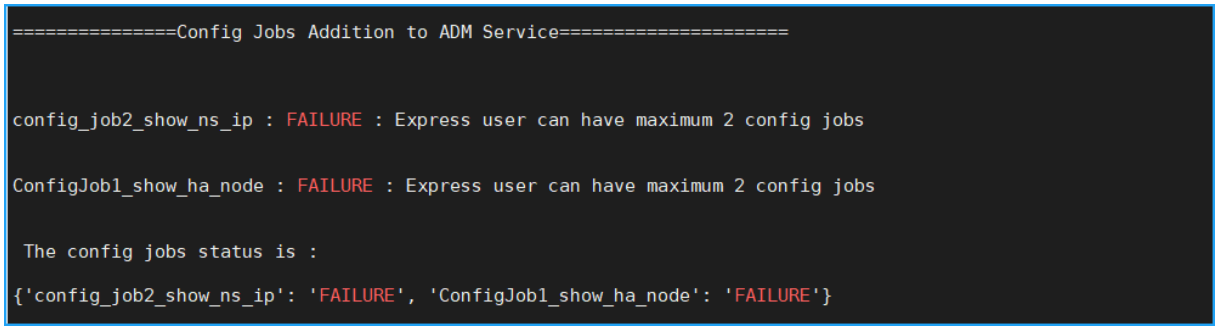
解决办法：在本地 ADM 中，确保实例状态，看看您是否可以在没有任何问题的情况下访问实例。如果任何问题仍然存在，请修复该问题，然后重新运行迁移脚本。

样书自定义模板导入到 **ADM** 服务



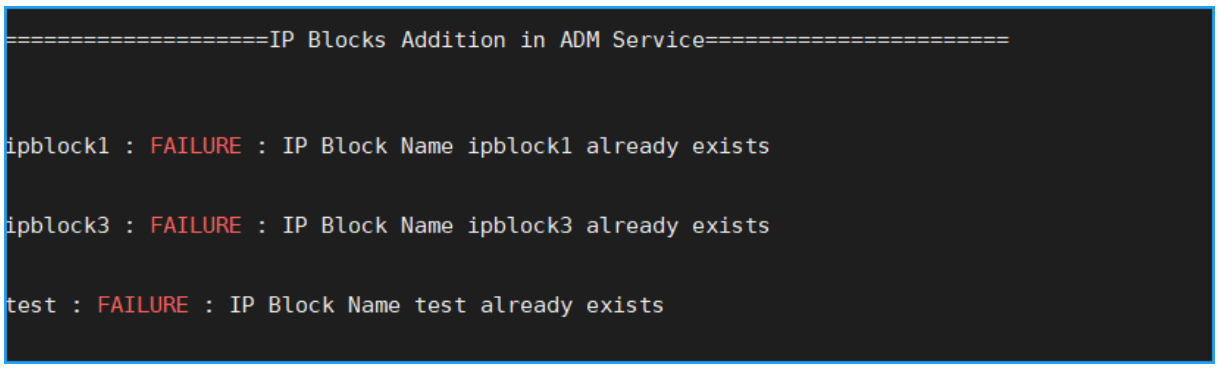
解决办法：此错误消息是已迁移的样书的示例。如果在运行迁移脚本之前，在 Citrix ADM 服务中手动创建了具有相同名称、版本和命名空间的样书，也可能会看到此错误。

添加到 **ADM** 服务的配置作业



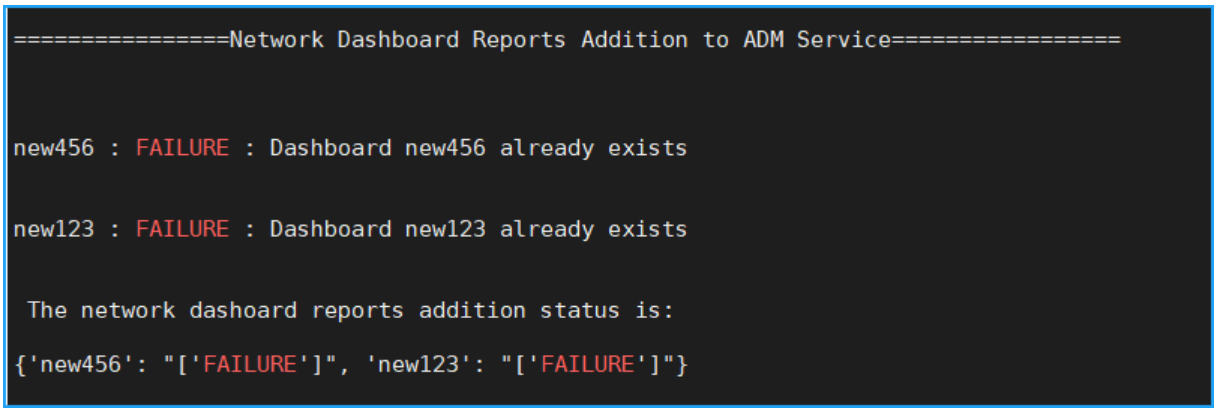
解决办法：如果您已订阅 Express Account 且有两个以上的配置作业，则会出现此错误。您必须获得有效订阅才能迁移所有配置作业。

添加到 **ADM** 服务的 **IP** 块



解决办法：删除在 ADM 服务中手动创建的 IP 块，然后重新运行迁移脚本。

网络仪表板报告添加状态



解决办法：删除在 ADM 服务中手动创建的仪表板，然后重新运行迁移脚本。

所有如何文章

April 23, 2021

Citrix Application Delivery Management (Citrix ADM) “操作方法文章” 简单、相关且易于实施有关 Citrix ADM 功能的文章。这些文章包含有关一些常见的 Citrix ADM 功能的信息，如实例管理、应用程序管理、样书、证书管理和分析。

单击下表中的功能名称可以查看对应功能的方法文章列表。

主题				
实例管理	事件管理	样本	证书管理	Citrix ADM 系统
应用程序管理	配置管理	身份验证	分析	网络功能

实例管理

如何监控全球分布的站点

如何管理 Citrix ADC 实例的管理分区

如何将实例添加到 Citrix ADM

如何在 Citrix ADM 上创建实例组

如何在 Citrix ADM 中为地理地图配置站点

如何使用 Citrix ADM 强制故障切换到辅助 Citrix ADC 实例

如何使用 Citrix ADM 强制辅助 Citrix ADC 实例保持辅助实例保持辅助

如何使用 Citrix ADM 备份和还原实例

如何使用 Citrix ADM 仪表板监视 HAProxy 实例

如何显示 HAProxy 实例上配置的前端的详细信息

如何显示 HAProxy 实例上配置的后端的详细信息

如何显示 HAProxy 实例上配置的服务器的详细信息

如何从 Citrix ADM 重新启动 HAProxy 实例

如何使用 Citrix ADM 备份和还原 HAProxy 实例

如何使用 Citrix ADM 编辑 HAProxy 配置文件

如何重新发现多个 Citrix ADC VPX 实例

如何轮询 Citrix ADM 中的 Citrix ADC 实例和实体

如何取消管理 Citrix ADM 上的实例

如何跟踪从 Citrix ADM 到实例的路由

配置管理

如何在 Citrix ADM 上创建配置作业

如何在配置作业中使用 SCP（put）命令

如何使用 Citrix ADM 升级 Citrix ADC SDX 实例

如何安排使用 Citrix ADM 中的内置模板创建的作业

如何重新安排使用 Citrix ADM 中的内置模板配置的作业

如何重复使用已执行的配置作业

如何使用 Citrix ADM 升级 Citrix ADC 实例

如何在 Citrix ADM 上的配置作业中使用变量

如何使用配置模板在 Citrix ADM 上创建审核模板

如何从 Citrix ADM 上的更正命令创建配置作业

如何在 Citrix ADM 上将运行和保存的配置命令从一个 Citrix ADC 实例复制到另一个实例

如何在 Citrix ADM 中为 Citrix SD-WAN WO 实例创建配置作业

如何使用录音和播放创建配置作业

如何使用配置作业将配置从一个实例复制到多个实例

如何在 Citrix ADM 上使用主配置模板

如何轮询 Citrix ADC 实例的配置审核

如何在配置作业中重复使用配置审计模板

如何导入和导出配置模板

如何为配置更改 SNMP 陷阱生成配置审核差异

证书管理

如何在 Citrix ADM 上配置企业策略

如何从 Citrix ADM 在 Citrix ADC 实例上安装 SSL 证书

如何从 Citrix ADM 更新已安装的证书

如何使用 Citrix ADM 链接和取消链接 SSL 证书

如何使用 Citrix ADM 创建证书签名请求 (CSR)

如何设置来自 Citrix ADM 的 SSL 证书到期通知

如何在 Citrix ADM 上使用 SSL 控制板

如何从 Citrix ADC 实例轮询 SSL 证书

应用程序管理

如何在 Citrix ADM 中创建应用程序定义

样本

如何查看不同的样书组

如何创建自己的样本

如何在 Citrix ADM 中使用用户定义的样本

如何使用 API 从样本创建配置

如何在样本中定义的虚拟服务器上启用分析和配置警报

如何创建样书以将文件上载到 Citrix ADM

如何使用 API 创建配置以上传任何文件类型

如何创建样本以将 SSL 证书和证书密钥文件上传到 Citrix ADM

如何使用 API 创建配置以上传证书和密钥文件

如何在商业企业中使用 Microsoft Skype for Business 样本

如何在商业企业中使用 Microsoft Exchange 样本

如何在商业企业中使用 Microsoft SharePoint 样本

分析

如何在实例上启用分析

如何配置自适应阈值

如何配置 SLA 管理

如何配置数据库总结以进行分析

如何使用 Citrix ADM 创建阈值和警报

如何禁用从 Citrix ADM 进行分析的 URL 数据收集

如何查看流式传输的视频类型和网络消耗的数据量

如何查看特定时间范围内的峰值数据速率

如何比较 ABR 视频的优化和未优化播放次数

如何比较 ABR 视频的优化和未优化播放时间

如何比较优化和未优化 ABR 视频的带宽消耗

如何比较优化和未优化 ABR 视频使用的数据量

如何查看网络效率

事件管理

如何为 Citrix ADM 上的事件设置事件年龄

如何使用 Citrix ADM 调度事件筛选器

如何为 Citrix ADM 中的事件设置重复电子邮件通知

如何通过使用 Citrix ADM 来禁止事件

如何使用事件控制板监视事件

如何在 Citrix ADM 上创建事件规则

如何修改 Citrix ADC 实例上发生的事件的报告严重性

如何在 Citrix ADM 中查看事件摘要

如何在 Citrix ADM 上显示 SNMP 陷阱的事件严重性和倾斜

如何使用 Citrix ADM 导出系统日志消息

如何禁止 Citrix ADM 中的系统日志消息

如何配置实例事件的修剪设置

身份验证

如何启用回退和级联外部身份验证服务器

如何添加 RADIUS 身份验证服务器

如何添加 LDAP 身份验证服务器

如何添加 TACAS 身份验证服务器

如何在 Citrix ADM 中提取身份验证服务器组

如何启用备用本地身份验证

Citrix ADM 系统

如何升级 Citrix ADM

如何重置 Citrix ADM 的密码

如何为 Citrix ADM 生成技术支持文件

如何在单个服务器部署中备份和还原您的 Citrix ADM 服务器

如何在 HA 对中备份和恢复 Citrix ADM 配置

如何在 Citrix ADM 中为非默认用户启用外壳访问

如何在 Citrix ADM 上配置 NTP 服务器

如何为 Citrix ADM 配置 SSL 设置

如何为 Citrix ADM 配置系统日志清除间隔

如何查看 Citrix ADM 的审核信息

如何配置 Citrix ADM 的系统通知设置

如何监视 Citrix ADM 的 CPU、内存和磁盘使用情况

如何为 Citrix ADM 配置密码组

如何在 Citrix ADM 上创建 SNMP 陷阱、管理器和用户

如何将主机名分配给 Citrix ADM 服务器

如何为 Citrix ADM 配置系统修剪设置

如何使用 Citrix ADM 配置系统备份设置

如何在 Citrix ADM 上配置和查看系统警报

网络功能

如何为负载平衡实体生成报告

如何导出或计划导出网络函数报告

概述

April 23, 2021

Citrix Application Delivery Management (ADM) 是一种集中式管理解决方案，它通过向管理员提供企业范围的可见性并自动化需要跨多个实例运行的管理作业来简化操作。您可以管理和监视 Citrix 应用程序网络产品，其中包括 Citrix ADC MPX、Citrix ADC VPX、Citrix ADC SDX、Citrix ADC CPX、Citrix Gateway 和 Citrix SD-WAN。您可以使用 ADM 从单个统一的控制台管理、监控整个全球应用程序交付基础架构并进行故障排除。

ADM 是一种在思杰虚拟机管理程序、VMware ESXi 和 Linux KVM 上运行的虚拟设备。ADM 通过收集有关 Web 应用程序和虚拟桌面流量的以下详细信息来解决应用程序可见性难题：

- 用户会话级别信息
- 网页性能数据
- 数据库信息流经站点的 ADC 实例，并提供可操作的报告。

ADM 使 IT 管理员能够在几分钟内进行故障排除并主动监控客户问题。

功能和解决方案

April 23, 2021

Citrix Application Delivery Management (ADM) 提供以下功能：

应用程序分析和管理

应用程序性能分析

“App Score”（应用程序分数）是定义应用程序执行良好情况的评分系统产品。它显示应用程序在响应能力方面表现良好、不易受到威胁以及所有系统都已启动并运行。

应用程序安全分析

“App Security Dashboard”（应用程序安全性控制板）提供应用程序的安全状态的历史视图。例如，它显示安全违规、签名违规和威胁指数等主要安全指标。App Security 仪表板还显示与攻击相关的信息，例如 SYN 攻击、小窗口攻击和针对已发现的 ADC 实例的 DNS 洪水攻击。

网络

实例

使您能够管理 Citrix ADC、Citrix Gateway、Citrix SD-WAN 和 HAProxy 实例。

实例组

让您能够对您的实例分组，如下所示：

- 静态组：允许您定义可以在不同任务（例如配置作业等）中使用的设备组。
- 专用 IP 块：让您可以根据地理位置对您的实例分组。

事件管理

当 ADC 实例的 IP 地址添加到 ADM 时，ADM 会发送 NITRO 调用，并隐式地将自身添加为实例接收陷阱或事件的陷阱目标。

事件表示托管 ADC 实例上发生的事件或错误。

证书管理

Citrix ADM 现在可以为您简化证书管理的各个方面。通过一个控制台可以建立自动化策略以确保合适的颁发者、密钥强度和正确的算法，同时密切跟踪未使用或即将过期的证书。要开始使用 ADM 的 SSL 仪表板及其功能，您必须了解什么是 SSL 证书以及如何使用 ADM 跟踪 SSL 证书。

配置管理

Citrix ADM 允许您创建配置作业，以帮助您在多个实例上轻松执行配置任务，例如创建实体、配置功能、复制配置更改、系统升级和其他维护活动。配置作业和模板将最重复的管理任务简化为 ADM 上的单个任务。

配置审核

让您能够监视和识别您的实例中的配置的异常情况。

- 配置建议：让您可以识别配置异常情况。
- 审核模板：让您可以监视某个特定配置的变化。

网络报告

您可以通过监控 ADM 上的网络报告来优化资源使用情况。

分析

Web Insight

提供企业 Web 应用程序的可见性，并允许 IT 管理员通过提供应用程序的集成实时监控来监控 Citrix ADC 所提供的所有 Web 应用程序。Web Insight 提供用户和服务器响应时间之类的关键信息，从而让 IT 组织能够监视并改进应用程序性能。

HDX Insight

提供通过 Citrix ADC 的 ICA 流量的端到端可见性。HDX Insight 让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。

Gateway Insight

通过它可以查看用户在登录时遇到的失败，无论访问模式为何。可以查看某个给定时间登录的用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。

Security Insight

提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。

SSL Insight

SSL Insight 提供对安全 Web 事务 (HTTPS) 的可见性，并允许 IT 管理员通过对安全 Web 事务提供集成的实时和历史性监视来监视 Citrix ADC 提供服务的所有安全 Web 应用程序。

TCP Insight

TCP Insight 提供了一个简单且可扩展的解决方案，用于监控 ADC 实例中使用的优化技术和拥塞控制策略（或算法）的指标，以避免数据传输中的网络拥塞。

Video Insight

Video Insight 功能提供了一个简单且可扩展的解决方案，用于监控 Citrix ADC 实例所使用的视频优化技术的指标，从而改善客户体验和运营效率。

WAN Insight

WAN Insight 分析使管理员能够轻松监控数据中心和分支广域网优化设备之间的加速和未加速的 WAN 流量。WAN Insight 还提供了网络上的客户端、应用程序和分支机构的可见性，以帮助有效地排除网络问题。

调配

Cloud Orchestration（云调配）

支持将 Citrix ADC 产品与 OpenStack 云编排集成。Citrix ADM 和 OpenStack 相互实现了彼此的 API，从而实现了 Citrix ADC 实例的负载平衡功能 (LBaaS) 与 OpenStack 云编排的集成。

调配

Citrix ADM 通过与不同供应商的 SDN 控制器集成来支持企业网络中的 SDN。ADM 同时支持 VMware NSX 管理器和思科应用策略基础架构控制器 (APIC)。

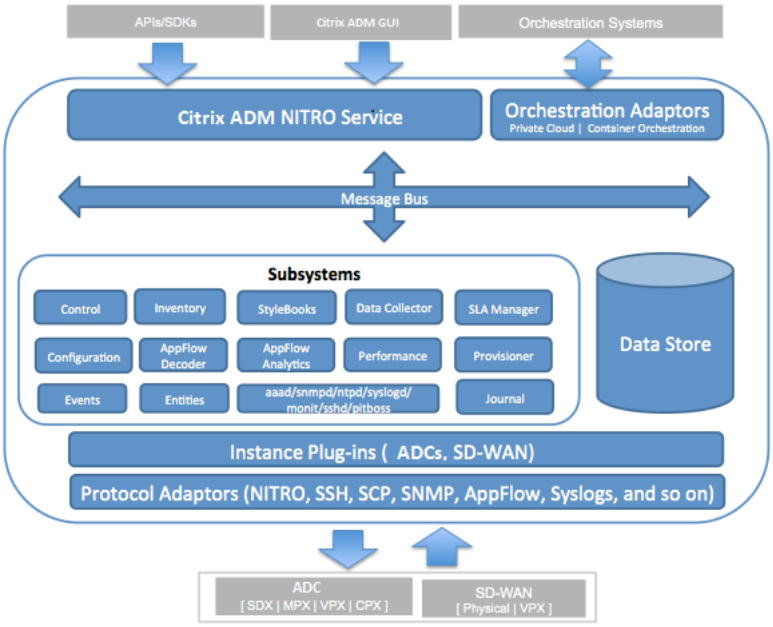
体系结构

April 23, 2021

Citrix Application Delivery Management (ADM) 数据库与服务器集成，服务器管理所有关键进程，如数据收集、NITRO 调用。服务器在其数据存储中存储实例详细信息的清单，例如主机名、软件版本、运行和保存的配置、证书详细信息以及在实例上配置的实体。单服务器部署适用于处理较小通信量或将数据存储较短时间的情况。

目前，ADM 支持两种类型的软件部署：单服务器和高可用性。

下图显示了 ADM 中的不同子系统，以及 ADM 服务器和受管实例之间的通信方式。



ADM 中的服务子系统充当 Web 服务器，处理使用端口 80 和 443 从 GUI 或 API 发送到 ADM 中子系统的 HTTP 请求和响应。这些请求通过使用 IPC（进程间通信）机制通过消息总线（消息处理系统）发送到子系统。请求会发送到控制子系统，该子系统处理信息或将其发送到合适的子系统。其他每个子系统（库存、样书、数据收集器、配置、AppFlow 解码器、AppFlow Analytics、性能、事件、实体、SLA 管理器、置备程序和日志）都具有特定的角色。

实例插件是共享库，它们对 ADM 支持的每种实例类型都是唯一的。通过使用 NITRO 调用或通过 SNMP、安全外壳 (SSH) 或安全拷贝 (SCP) 协议在 ADM 和托管实例之间传输信息。然后处理此信息并存储在内部数据库（数据存储）中。

Citrix ADM 如何发现实例

April 23, 2021

实例是您希望通过 Citrix 应用程序交付管理 (ADM) 发现、管理和监视的 Citrix 设备或虚拟设备。要管理和监视这些实例，必须将它们添加到 Citrix ADM 服务器中。您可以将以下 Citrix 设备和虚拟设备添加到 ADM：

- Citrix ADC 实例
  - Citrix MPX
  - Citrix VPX

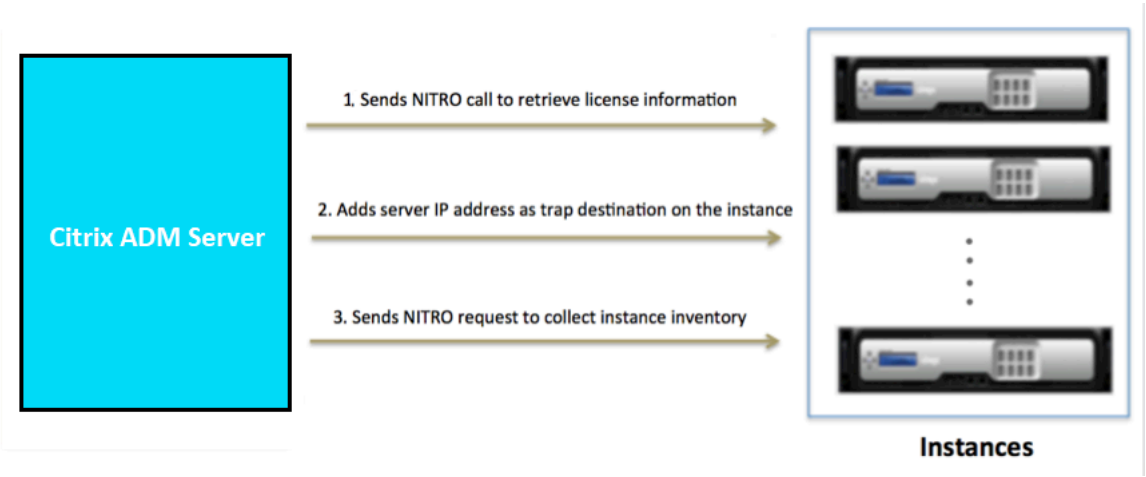
  - Citrix SDX
  - Citrix CPX
  - Citrix BLX
- Citrix Gateway 实例
- Citrix SD-WAN 实例

您可以在首次设置 Citrix ADM 服务器时或以后添加实例。

> 注意
>
> Citrix ADM 使用 ADC 实例的 Citrix ADC IP (NSIP) 地址进行通信。ADM 还可以发现具有已启用管理访问权限的子网 IP (SNIP) 地址的 ADC 实例。有关 ADC 实例和 ADM 之间必须打开的端口的信息，请参阅 端口。
>
> 如果要使用 SNIP 添加 ADC HA 对，请确保在 ADC HA 对上启用独立网络配置 (INC) 模式。有关添加实例的更多信息，请参阅 添加实例。
>
> 对于 Citrix SD-WAN WO，ADM 使用实例的管理 IP 地址进行通信。
>
> 您无法在 ADM 中添加 Citrix SD-WAN SE /PE 实例。您可以在 Citrix SD-WAN SE/PE 设备上将 ADM 配置为 AppFlow 收集器。

将实例添加到 ADM 服务器时，服务器会隐式地将自身添加为实例的陷阱目标，并收集实例的清单。

下图描述了 ADM 如何隐式发现和添加实例。



如图所示，Citrix ADM 隐式执行以下步骤。

1. Citrix ADM 使用实例配置文件详细信息登录到实例。使用 ADC NITRO 调用，ADM 检索实例的许可证信息。根据许可信息，它确定实例是 ADC 实例和 ADC 平台的类型（例如，Citrix ADC MPX、ADC VPX、ADC SDX、ADC BLX 或 Citrix Gateway）。成功检测实例后，该实例将添加到 ADM 的数据库中。

   对于 Citrix SD-WAN WO 实例，ADM 不会使用许可信息检测实例。它向实例发送一个 NITRO 请求以检查实例类型和版本。

如果实例配置文件没有包含正确的凭据，此步骤可能会失败。对于 ADC MPX、ADC VPX、ADC SDX、ADC BLX 和 Citrix Gateway 实例，如果许可证未应用于实例，则此步骤也可能失败。

> 注意
>
> 使用 HTTP，即使未在实例上配置许可证，您也可以将所有实例添加到 ADM 中。

2. ADM 会将其 IP 地址添加到实例上的陷阱目标列表中。这允许 ADM 接收在 ADC 实例上生成的陷阱。

   如果实例上的陷阱目标数超过陷阱目标最大限制，此步骤可能会失败。实例的最大限制为 20。

   对于 Citrix SD-WAN WO 实例，ADM 将其 IP 地址作为实例上的 SNMP 管理器添加。

3. ADM 通过发送 NITRO 请求从实例收集库存。它收集实例详细信息，例如主机名、软件版本、正在运行和保存的配置、证书详细信息、实例上配置的实体。

   如果存在网络或防火墙问题，此步骤可能会失败。

   要了解如何向 ADM 添加实例，请参阅 添加实例。

轮询概述

April 23, 2021

轮询是一个过程，Citrix Application Delivery Management (ADM) 从 Citrix ADC 实例收集某些信息。您可能已在全球范围内为您的组织配置了多个 Citrix ADC 实例。要通过 Citrix ADM 监视您的实例，Citrix ADM 必须从所有托管 ADC 实例收集某些信息，如 CPU 使用率、内存使用率、SSL 证书、许可功能、许可证类型等。以下是 ADM 和托管实例之间发生的不同类型的轮询：

- 实例轮询
- 清单轮询
- 性能数据收集
- 实例备份轮询
- 配置审核轮询
- SSL 证书轮询
- 实体轮询

Citrix ADM 使用 NITRO 调用、安全外壳 (SSH) 和安全拷贝 (SCP) 等协议从 Citrix ADC 实例轮询信息。

Citrix ADM 如何轮询托管实例和实体

默认情况下，Citrix ADM 会定期自动轮询。Citrix ADM 还允许您为少数轮询类型配置轮询间隔，并允许您在需要时手动轮询。

下表介绍了轮询类型、轮询间隔、使用的协议等的详细信息：

轮询类型	轮询时间间隔	轮询信息	使用的协议	轮询间隔配置
实例轮询	每 5 分钟（默认情况下）	统计信息，如状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量。	NITRO 调用。	否
清单轮询	每 60 分钟（默认情况下）	清单详细信息，如构建版本、系统信息、许可功能和模式。	NITRO 调用和 SSH	否
性能数据收集	每 5 分钟（默认情况下）	网络报告信息	NITRO 调用	否
实例备份轮询	每 12 小时（默认情况下）	受管 ADC 实例当前状态的备份文件	NITRO 调用、SSH 和 SCP。	是。导航到网络 > 实例 > **Citrix ADC**。选择实例，然后从选择操作” 列表中单击 “备 份/还原。
配置审核轮询	每 10 小时（默认情况下）	ADC 实例上发生的配置更改（例如，运行与保存的配置）	SSH、SCP 和 NITRO 调用	是。导航至 “ 网络” > “ 配置审核”。在 “配置审核” 页上，单击 设置并配置配置审核轮询的轮询间隔。
				您可以手动轮询配置审核，并立即将实例的所有配置审核添加到 Citrix ADM 中。为此，请导航到 “ 网络” > “ 配置审核”，然后单击 “ 立即轮询”。“ 立即轮询页面允许您轮询网络中的所有实例或选定实例。
SSL 证书轮询	每 24 小时一次（默认情况下）	安装在 Citrix ADC 实例上的 SSL 证书。	NITRO 调用和 SCP	是。导航到 “ 网络” > “ **SSL** 仪表板”。在 “SSL 控制面板” 页上，单击 设置以配置轮询间隔

轮询类型	轮询时间间隔	轮询信息	使用的协议	轮询间隔配置
				您可以手动轮询 SSL 证书，并立即将实例的所有证书添加到 Citrix ADM 中。为此，请导航到网络 > **SSL** 控制板，然后单击立 即轮询。“ 立即轮询页面允许您轮询网络中的所有实例或选定实例。
实体轮询	每 60 分钟（默认情况下）	在实例上配置的所有实体。实体是附加到 ADC 实例的策略、虚拟服务器、服务或操作。要启用实体轮询，请参阅 启用或禁用 ADM 功能。	NITRO 调用。	是，但不能设置为少于 10 分钟。要配置，请导航到 “网络” > “ 网络功能”。在 “网络功能” 页上，单击 设置以配置轮询间隔。
				您可以手动轮询实体，并立即将实例的所有实体添加到 Citrix ADM 中。为此，请导航到 “网络” > 网络功能”，然后单击 “立 即轮询。“ 立即轮询页面允许您轮询网络中的所有实例或选定实例

> 注意：除
>
> 了轮询之外，Citrix ADM 还通过发送到实例的 SNMP 陷阱接收由托管 ADC 实例生成的事件。例如，系统发生故障或配置发生更改时生成事件。
>
> 在实例备份期间，SSL 文件、CA 证书文件、ADC 模板、数据库信息等都会下载到 Citrix ADM。在配置审核过程中，ns.conf 文件会下载并存储在文件系统中。从托管 Citrix ADC 实例收集的所有信息都存储在数据库内部。

轮询实例的不同方式

以下是 Citrix ADM 对托管实例执行的不同轮询方法：

- 实例的全局轮询
- 手动轮询实例
- 对实体进行人工投票

实例的全局轮询

Citrix ADM 会根据您配置的时间间隔自动轮询网络中的所有托管实例。虽然默认轮询间隔为 30 分钟，但您可以通过导航到 “网 络” > “网络功能 > “设置” 来设置间隔。

手动轮询实例

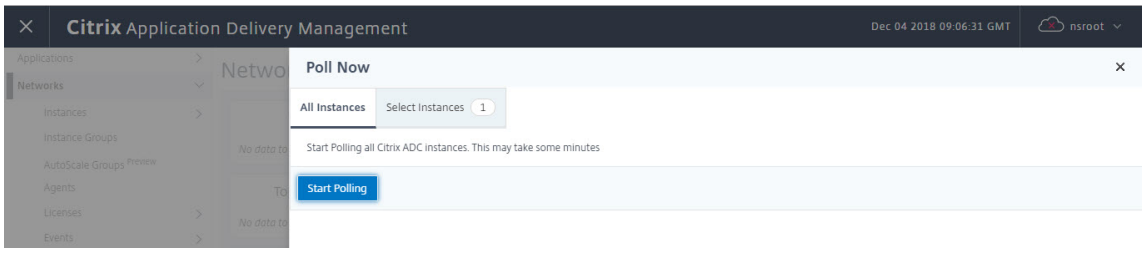
当 Citrix ADM 管理多个实体时，轮询周期需要较长的时间来生成报告，这可能导致出现空白屏幕，或者系统可能仍然显示较早的数据。

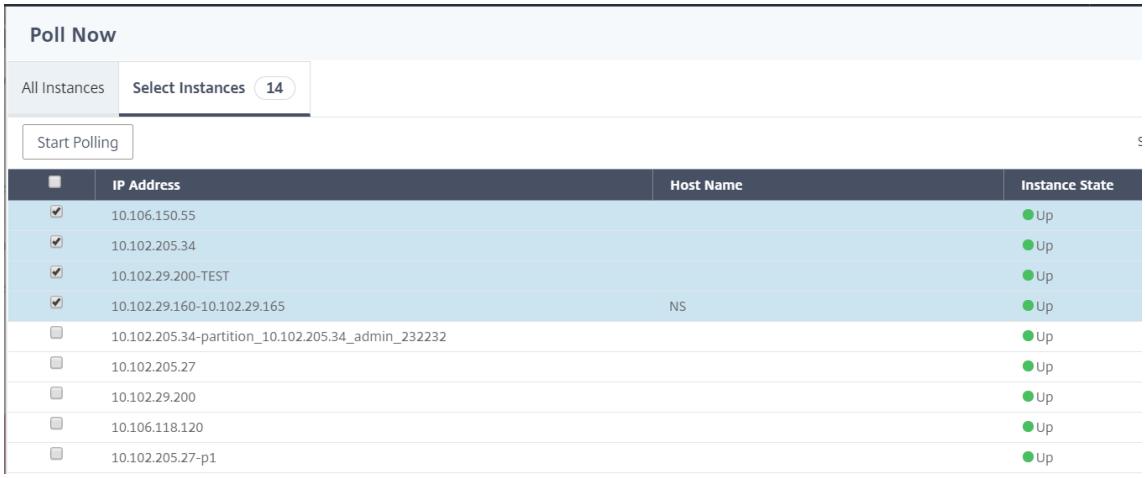
在 Citrix ADM 中，当不进行自动轮询时，有一个最小轮询间隔期。如果添加了新的 Citrix ADC 实例，或者更新了实体，Citrix ADM 将不会识别新实例或对实体所做的更新，直到下次轮询进行。并且，没有办法立即获取虚拟 IP 地址列表来执行进一步操作。您必须等待最小轮询时间间隔过去。尽管您可以执行手动轮询以发现新添加的实例，但这会导致整个 Citrix ADC 网络进行轮询，从而对网络造成沉重负载。Citrix ADM 现在允许您在任何给定时间仅轮询选定的实例和实体，而不是轮询整个网络。

Citrix ADM 会自动轮询托管实例，以便在一天中的设定时间收集信息。选定轮询可缩短 Citrix ADM 显示绑定到这些选定实例的实体的最新状态所需的刷新时间。

要轮询 **Citrix ADM** 中的特定实例，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “网 络” > “ 网络功能”。
2. 在 网络功能页上的右上角，单击 立即轮询。
3. 弹出页面 “立 即轮询为您提供了轮询网络中的所有 Citrix ADC 实例或轮询所选实例的选项。
   a) 所有实例选项卡-单击 开始轮询以轮询所有实例。
   b) 选择实例选项卡-从列表中选择实例
4. 单击 开始轮询。





Citrix ADM 启动手动轮询并添加所有实体。

对实体进行人工投票

Citrix ADM 还允许您轮询绑定到特定实例的几个选定实体。例如，您可以使用此选项来了解实例中特定实体的最新状态。在这种情况下，您无需轮询整个实例即可了解一个更新实体的状态。选择并轮询实体时，Citrix ADM 仅轮询该实体并更新 Citrix ADM GUI 中的状态。

考虑一个虚拟服务器处于“关闭”状态的示例。在下一次自动轮询发生之前，该虚拟服务器的状态可能已更改为 UP。要查看虚拟服务器的更改状态，您可能只需轮询该虚拟服务器，以便在 GUI 上立即显示正确的状态。

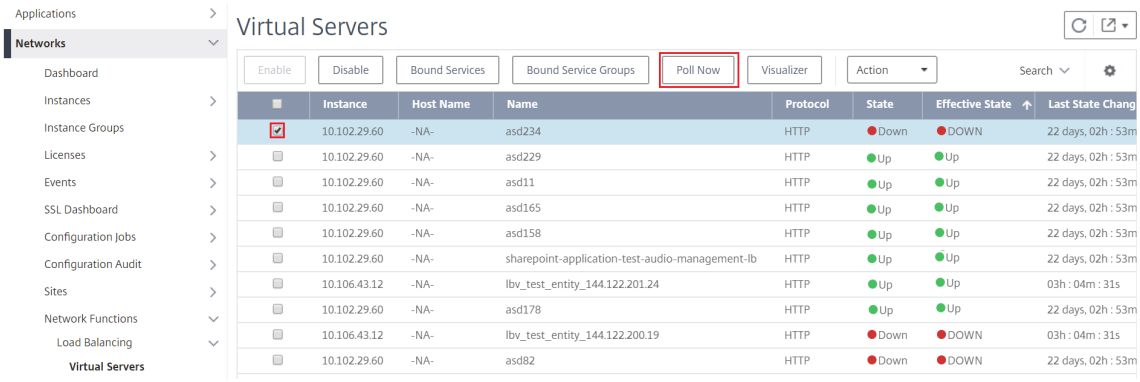
您现在可以轮询以下实体的状态下的任何更新：服务、服务组、负载平衡虚拟服务器、缓存减少虚拟服务器、内容交换虚拟服务器、身份验证虚拟服务器、VPN 虚拟服务器、GSLB 虚拟服务器和应用程序服务器。

> 注意
>
> 如果轮询虚拟服务器，则只轮询该虚拟服务器。服务、服务组和服务器等相关实体不进行轮询。如果需要轮询所有关联的实体，则必须手动轮询实体，或者必须轮询实例。

要轮询 **Citrix ADM** 中的特定实体，请执行以下操作：

例如，此任务将帮助您轮询负载平衡虚拟服务器。同样，您也可以轮询其他网络函数实体。

1. 在 Citrix ADM 中，导航到“网络**”>“**网络功能”>“负载平衡”>“虚拟服务器”。
2. 选择将状态显示为“关闭”的虚拟服务器，然后单击“立 即轮询”。虚拟服务器的状态现在更改为 UP。



数据管理

April 23, 2021

Citrix 收集有关 Citrix Application Delivery Management (ADM) 部署的统计信息，以了解部署使用情况和规模。统计信息包括您本地的 ADM 部署运行状况、状态和使用模式。统计数据可帮助 Citrix 主动解决 ADM 部署中的问题。

- 在 **Citrix Cloud** 上创建客户身份 -将 ADM 本地部署中有关 ADM 运行状况、状态和其他指标的重要统计信息发送到 Citrix Cloud 帐户。

  创建客户身份后，“云连接”通过创建 Citrix Cloud 帐户在本地 ADM 和 ADM 服务之间建立连接。请参阅配置客户身份。

- 配置维护脚本 -优化数据库。数据库优化可能会创建表、更改列等。同样的“云连接”功能用于配置维护脚本。请参阅使用维护脚本优化数据库。

- 客户用户体验改善计划 **(CUXIP)** -默认情况下启用此程序。它从 Citrix ADM 收集使用情况数据。此数据允许通过引导式工作流、搜索文章、产品通知、反馈、调查等优化 ADM 体验。请参阅客户用户体验改善计划。

配置客户身份

Citrix Application Delivery Management (ADM) 要求您在开始访问信息之前，先在 ADM GUI 上对自己进行身份验证。在 ADM 上进行身份验证之前，您必须在 Citrix Cloud 服务上自行注册。在 ADM GUI 上提供 Citrix 云用户凭据。有关详细信息，请参阅注册 Citrix Cloud。

有不同的方法可以在 Citrix ADM 上对自己进行身份验证。如果您是 ADM 上的新用户或现有用户，则以下各节将介绍工作流。

工作流 **1**-如果您是新用户

1. 在选定的 Hypervisor 上完成 Citrix ADM 的安装。
2. 配置各种必需的 IP 地址。

3. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址。
4. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。

   此时将打开 “ 配置客户身份” 页，您必须在其中使用 Citrix Cloud 凭据标识自己。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 以注册。
5. 单击 身份验证并提供您用于在 Citrix Cloud 上注册的电子邮件地址。
6. 选中 “ 我同意共享遥测数据” 旁边的复选框，然后单击 “ 提交”。

工作流 **2-**如果您是现有用户升级到最新 **ADM** 版本

1. 将 Citrix ADM 升级到最新版本后，请在 Web 浏览器中键入 Citrix ADM 的 IP 地址。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 此时将打开 “ 配置客户身份” 页，您必须在其中使用 Citrix Cloud 凭据标识自己。

   如果您尚未在 Citrix Cloud 上创建帐户，请单击 Citrix Cloud 以注册。
4. 单击 身份验证并提供您用于在 Citrix Cloud 上注册的电子邮件地址。
5. 选中 “我同意共享遥测数据” 旁边的复选框，然后单击 “提交”。

作为现有用户，您还可以稍后通过以下两种方式之一在 ADM 上配置您的身份：

- 导航到 **“系统” > “**系统管理”，然后单击 “ 身份验证”。
- 单击 ADM GUI 右上角的云符号。
  身份验证成功后，将 X 变成绿色复选标记。

> 注意：
>
> 确保以下域被列入白名单：
>
> - `*.citrixnetworkapi.net`
> - `*.blob.core.windows.net`

通过将数据上传到 Citrix ADM 并使用 Citrix ADM 功能，即表示您同意并同意 Citrix 可以收集、存储、传输、维护、处理和使用有关您的 Citrix 产品和服务的技术、用户或相关信息。

Citrix 收到的信息始终按照处理 Citrix.com 隐私政策。

诊断和数据收集

Citrix ADM 使用客户身份收集以下遥测：

- 在 **ADM** 中执行的操作：
  - 使用 Citrix ADM UI/API 接口执行的操作。
  - 使用 Citrix ADM SDK 接口执行的操作。

  - 一天内的操作计数。此计数包括来自 API 或 UI 的任何非 Get 请求。
  - ADM 完成的 ADC 升级计数。

- **Citrix ADM** 许可证信息：授权虚拟服务器的计数。
- 主要统计数据：
  - 事件规则的总计数。
  - 样书的总计数和用户定义样书。
  - 托管和自定义应用程序的计数。
  - 已注册代理的计数。
  - 整个 Citrix ADC（Rx+Tx）的总吞吐量。
  - 托管实例的计数。此计数还包括管理分区。
  - 使用 Citrix ADM SaaS 的管理员计数。
- **Citrix ADM** 的地理位置
- 部署信息：此信息包括部署类型，如高可用性、灾难恢复和 ADM 代理。

为什么要收集数据**?**

收集的遥测数据有助于：

- 建议正确的 Citrix ADM 大小调整和部署。
- 主动排除 ADM 内部部署的问题。

谁可以使用这些数据**?**

Citrix 是所收集信息的唯一所有者。Citrix 可以访问/收集您自愿提供给我们的信息。我们不会向任何人出售或出租这些信息。我们不会与我们组织以外的任何第三方共享您的信息，但为了满足您的请求而必要的情况除外。示例：配送订单或主动解决问题。

我们将您的数据保存多久**?**

通常，我们会存储个人/使用数据，直到用户使用我们的服务为止。或者，我们还有另一个目的。之后，数据的存储不再超过法律要求或允许的要求，或者用于内部报告和核对目的的必要。

所有遥测数据的存储时间不超过 13 个月或 396 天。

使用维护脚本优化数据库

维护脚本用于解决 ADM 内部部署数据库相关问题。ADM 软件自动从 ADM 服务下载数据库维护脚本，从而更快地解决数据库相关问题。之前，这些问题已通过手动运行脚本得到解决。

借助此功能，ADM 本地部署定期从 ADM 服务下载数据库维护脚本。为此，请确保配置客户身份。

维护脚本每天和每周运行。此外，脚本可能会创建表或添加或删除列以提高数据库性能。

客户用户体验改善计划

在 Citrix Systems，我们的目标是为用户提供引人入胜的产品体验。我们使用 CUXIP 通过提供搜索文章、应用内指南等来引导用户完成一些常见但详细的任务。我们还帮助我们的用户及时了解最近的所有公告。

通过 **CUXIP** 收集了哪些使用数据**?**

使用数据与用户操作有关。使用数据也称为事件级数据，包括从我们用户在网站上访问的页面到特定功能的点击次数等所有内容。使用数据是有关用户如何在我们的应用程序中移动的重要信息。这些数据可以优化我们的用户体验。

以下是我们收集的一些使用数据：

- 页面浏览量的详细信息，在每个页面上花费的时间。
- 访客 ID 是一种唯一的匿名标识符，可帮助识别页面上的唯一访客数量。
- 调查统计数据 — 得分、视图、提交数量等。

CUXIP 如何帮助您**?**

我们使用使用数据来改善您使用 ADM 的体验。以下是我们打算提升客户用户体验的一些方法：

- 应用程序内指导工作流程和搜索相关文章的能力。
- 从应用程序中参与调查，以帮助改进产品。
- 随时了解最近的公告和其他通知。
- 向产品团队发布问题或反馈。

CUXIP 是如何工作的**?**

Citrix ADM 装置可以位于内部网络中。浏览器必须具有互联网连接才能获得 CUXIP 上的引导式帮助的好处。

如何在 **ADM** 上禁用 **CUXIP?**

要禁用 CUXIP，请在 ADM GUI 中执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。
2. 在 **CUXIP** 设置中，并禁用 CUXIP。

我们的隐私政策变更

我们可能会不时更新我们的隐私政策。我们将通过在此页面上发布新的隐私政策来通知您有关变更。在变更生效之前，我们会通过电子邮件和/或我们服务的突出通知告知您，并更新本隐私政策顶部的“生效日期”。

建议您定期查看本隐私政策以了解任何更改。对本隐私政策的更改在发布在 Citrix 隐私政策 页面上时生效。

引用

Citrix 隐私政策：https://www.citrix.com/about/legal/privacy/

许可

April 23, 2021

当通过 `https` 协议发现实例时，Citrix Application Delivery Management (ADM) 需要经过验证的 Citrix ADC 许可证才能管理和监视 Citrix ADC 实例。

可以在没有许可证的情况下管理和监视任何数量的实例和实体。但是，您只能在应用程序仪表板上管理 30 个发现的应用程序，并在无需应用许可证的情况下查看 30 个虚拟服务器的分析数据。除了 30 个发现的应用程序或 30 个虚拟服务器之外，您必须购买并应用许可证。

	Citrix ADM 功能	[免费] 无论虚拟服务器计数如何，都不需要 Citrix ADM 许可证	超过 30 台虚拟服务器需要 Citrix ADM 许可证	Citrix ADC 许可证要求
分析	Web Insight	否	是	不适用
	HDX Insight*	否	是	高级（报告小于 1 小时）高级（报告 = 无限制）
	Security Insight	否	是	高级（或）高级应用防火墙许可证
	SSL Insight	否	是	不适用
	Gateway Insight	否	是	高级（报告小于 1 小时）高级（报告 = 无限制）
	TCP Insight	否	是	不适用
	Video Insight	否	是	高级（柠檬酸 T 1000 系列，VPX-T）
	WAN Insight	否	不适用	使用 Citrix SD-WAN 实例优化版 (WANOP)

	Citrix ADM 功能	[免费] 无论虚拟服务器计数如何，都不需要 Citrix ADM 许可证	超过 30 台虚拟服务器需要 Citrix ADM 许可证	Citrix ADC 许可证要求
应用程序				
	应用程序统计信息（应用程序控制板、应用程序安全性控制板）	否	是	应用程序仪表板和应用程序安全仪表板上的 Citrix ADC Web 应用程序防火墙相关信息需要高级（或）高级应用程序防火墙许可证。
	样本	是	否	不适用
网络				
	许可证服务器	是	否	不适用
	库存管理 一、基础架构仪表板、实例组、实例仪表板和站点	是	否	不适用
	事件管理和 Syslog	是	否	不适用
	配置作业、配置审核和配置建议	是	否	不适用
	网络报告（实例级别）	是	否	不适用
	网络报告（虚拟服务器级别）	是	否	不适用
	网络功能（虚拟服务器、服务、服务组、服务器的可见性和管理）	是	否	不适用
	SSL 证书管理、监视和控制板（实例级别）	是	否	不适用
	SSL 证书控制板（虚拟服务器级别）	是	否	不适用

	Citrix ADM 功能	[免费] 无论虚拟服务器计数如何，都不需要 Citrix ADM 许可证	超过 30 台虚拟服务器需要 Citrix ADM 许可证	Citrix ADC 许可证要求
系统				
	RBAC 和外部身份验证（实例级别）	是	否	不适用
	RBAC 和外部身份验证	是	否	不适用
调配				
	开放式堆栈集成	是	否	不适用
	VMware NSX 集成	是	否	不适用
	Cisco APIC 集成	是	否	不适用
	容器集成	是	否	不适用
第三方负载平衡器				
	HAProxy：跨主机/实例/后端/服务器/前端、下载或上传配置以及重新启动设备的可见性。	是	否	不适用
	应用程序控制板	否	是（需要单独的许可证）	不适用

* 对于与 Citrix ADM 支持的 Citrix 控制器集成 — Citrix 控制器必须具有高级许可证。

更多虚拟服务器的许可证在 10 个虚拟服务器包中提供。您可以通过 Citrix ADM GUI 获取有效的许可证并在 Citrix ADM 服务器上添加许可证。

高可用性

Citrix ADM 服务器可以包含 VIP、CICO 和池容量许可证。向 ADM 服务器颁发许可证时，许可证将绑定到服务器的主机 ID。而且，将许可证分配给其他 ADM 服务器受到限制。

如果将 ADM 高可用性对配置为许可证服务器，则主服务器和辅助服务器必须具有相同的许可证文件。因此，在 ADM 高可用性部署中，Citrix ADM 支持将相同的许可证文件分配给两台服务器。

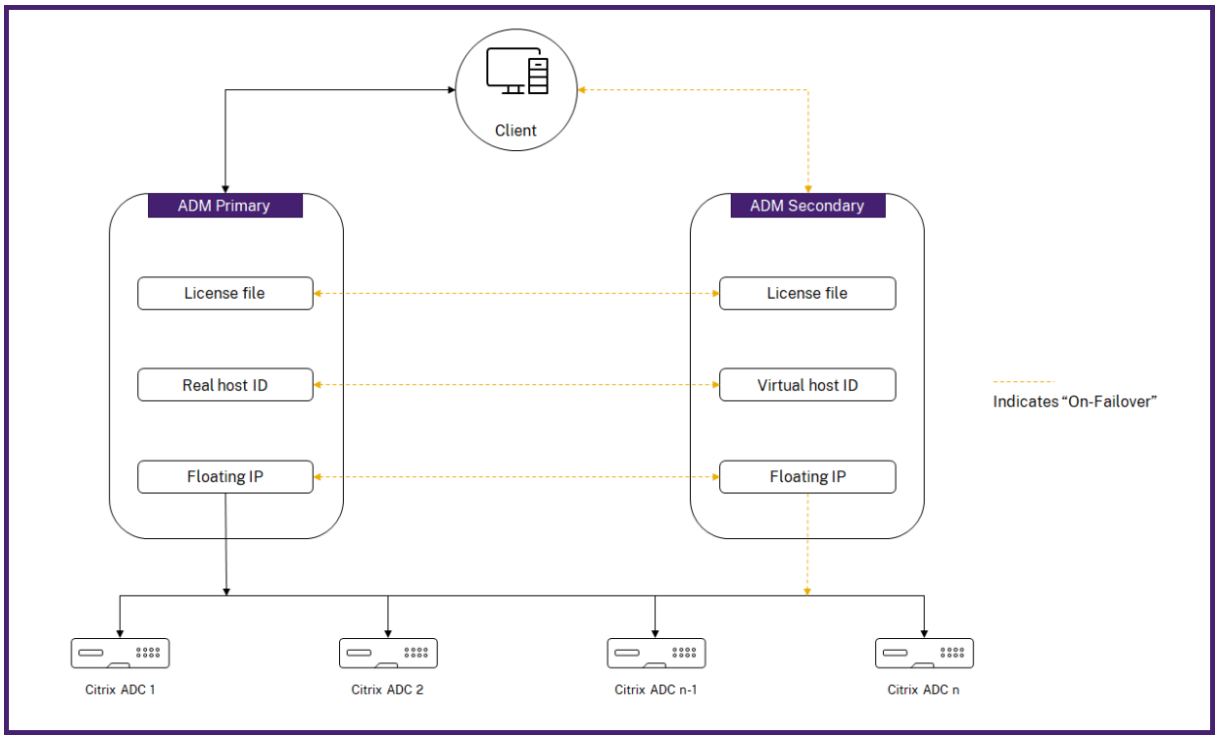
发生故障转移时，新的主动节点将在 30 天的宽限期内维护许可。

> 注意
>
> - 如果您已安装 Citrix ADM 12.1.49.x 或更早版本，则可以在 30 天的宽限期内维护辅助节点上的许可。宽限期过后，您必须与 Citrix 联系以重新托管原始许可证。
> - 对于 12.1.50.x 或更高版本，Citrix ADM 许可证会自动同步到辅助节点。
> - 池许可证从 12.1.50.x 或更高版本自动同步到辅助节点。

ADM 高可用性节点之间的许可证如何同步

无论何时发生故障切换，从属服务器都会承担主服务器的角色。主服务器的真实主机 ID 配置为新主服务器的虚拟主机 ID。许可证文件使用虚拟主机 ID 识别新的主服务器。

- 真实主机 **ID** -此 ID 是从 ADM 服务器的 MAC 地址生成的。每个 ADM 独立部署都有一个唯一的主机 ID。
- 虚拟主机 **ID** -此 ID 是在 HA 部署期间自动生成的。ADM 主服务器的真实主机 ID 用作从属服务器的虚拟主机 ID。此 ID 以加密格式存储在 ADM 数据库中，对此 ID 的修改受到限制。虚拟主机 ID 优先于真实的主机 ID。



假设 Node-1 是主服务器，Node-2 是辅助服务器。Node-1 的虚拟主机 ID 与 Node-2 同步。

1. Node-1 中可用的许可证文件将同步到 Node-2。
2. Node-1 上的任何新许可证文件都会定期同步到 Node-2。
3. ADM 确保许可证服务器仅在 Node-1 上运行，以避免许可证容量增加一倍。
4. Citrix ADC 实例使用浮动 IP 地址从 Node-1 中签出许可证。

许可证被锁定到 ADC 实例。要从 Citrix ADM HA 中签出许可证，实例需要特定设备的 IP 地址。当您在主服务器上应用许可证时，该服务器将负责许可，并将所有未来的许可证应用于该实例。只能从安装了许可证的服务器中删除许可证。

调配

调配模块独立于许可，且始终可用。

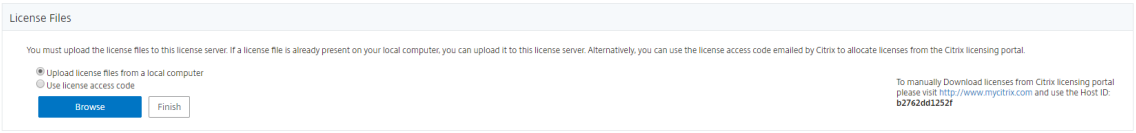
升级虚拟服务器许可证

您可以升级 Citrix ADM 上的许可，以监视和管理 Citrix ADC 设备上托管的更多虚拟服务器。

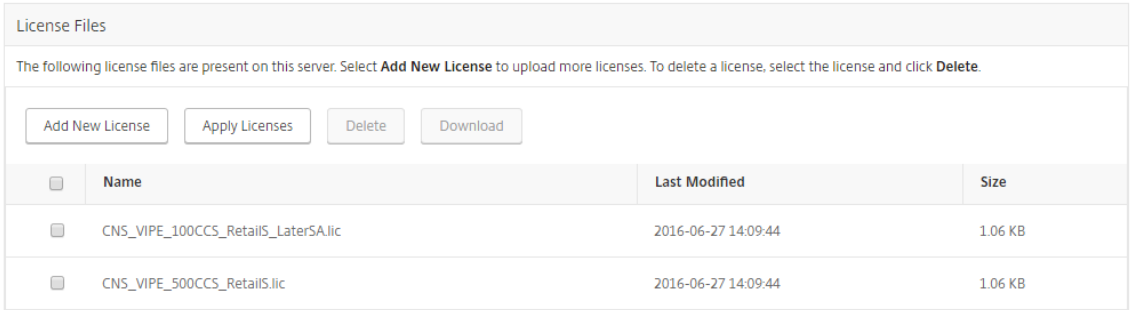
要升级设备许可证，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到 “ 网络” > “ 许可证” > “ 设置”。
3. 在详细信息窗格中，转到许可证文件，然后选择以下选项之一：
   - 从本地计算机上传许可证文件。如果本地计算机上已存在许可证，请单击 “浏览” 并选择要用于分配许可证的许可证文件 (.lic)。单击 **Finish**（完成）。
   - 使用许可证激活码。Citrix 通过电子邮件向您购买的许可证的许可证访问代码发送电子邮件。在文本框中输入许可证访问代码，然后单击 获取许可证。

   > 注意
   >
   > 如果选择此选项，则 Citrix ADM 必须连接到 Internet，否则必须有代理服务器可用。

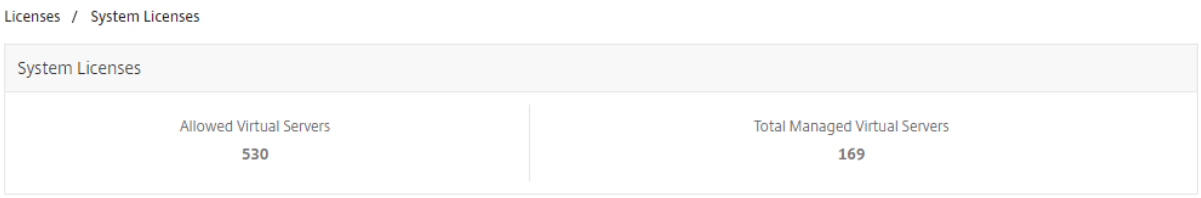


4. 您可以随时从 “许可证设置” 页面添加更多许可证。



验证

您可以通过导航到 **“系统” > “许可和分析”** 来验证 **Citrix ADM** 上安装的许可证。



管理虚拟服务器

您可以选择要通过 Citrix ADM 管理和监视的虚拟服务器或第三方虚拟服务器。

> 注意事项
>
> - 默认情况下，Citrix ADM 会在每个虚拟服务器轮询周期后自动对虚拟服务器进行随机许可。
> - 如果在 Citrix ADM 中发现的虚拟服务器总数低于已安装的虚拟服务器许可证数，则默认情况下，Citrix ADM 会为所有虚拟服务器授予许可证。

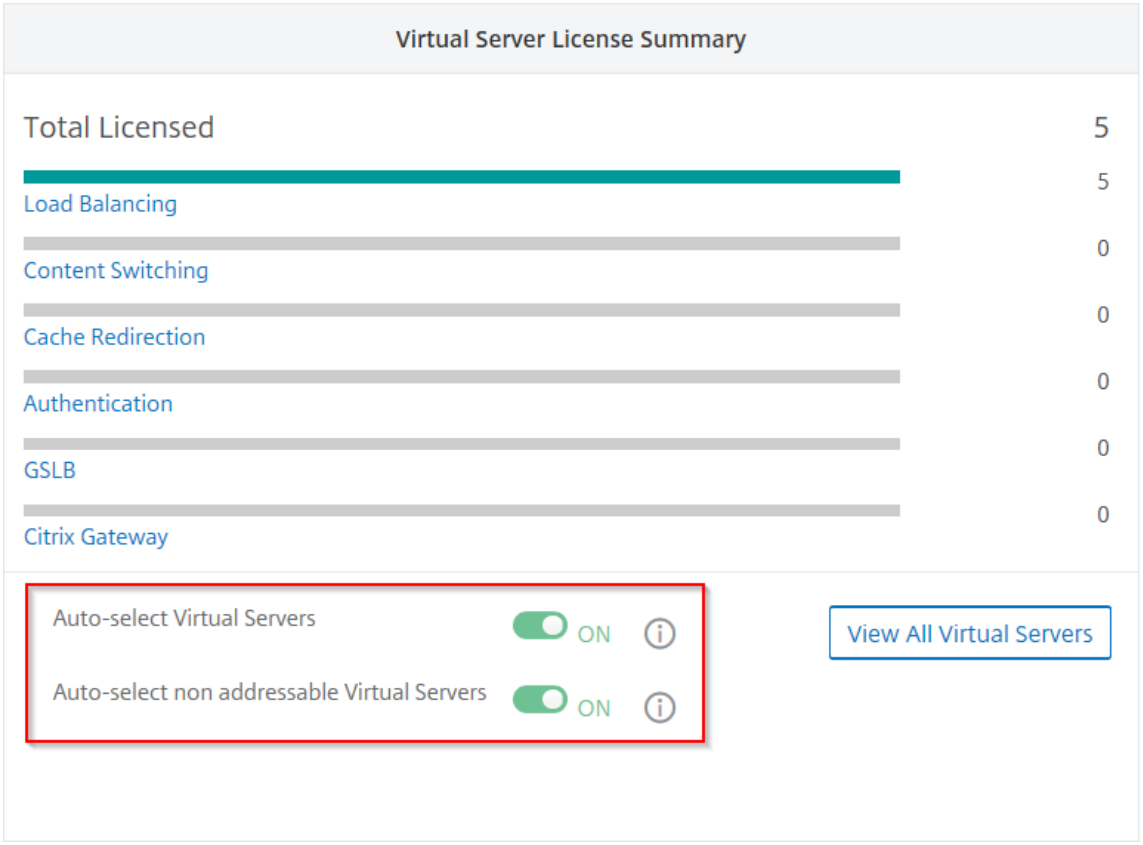
要手动选择虚拟服务器，或要仅对有限的虚拟服务器进行许可，您必须先禁用自动许可虚拟服务器，然后选择您要管理的虚拟服务器。

禁用自动许可虚拟服务器

1. 导航到 **“系统” > “许可和分析”**。

   控制板显示可用的虚拟服务器许可证、托管虚拟服务器以及虚拟服务器类型以及许可证到期信息。

2. 在 虚拟服务器许可证分配中，禁用 自动许可的虚拟服务器并 自动选择不可寻址的虚拟服务器。

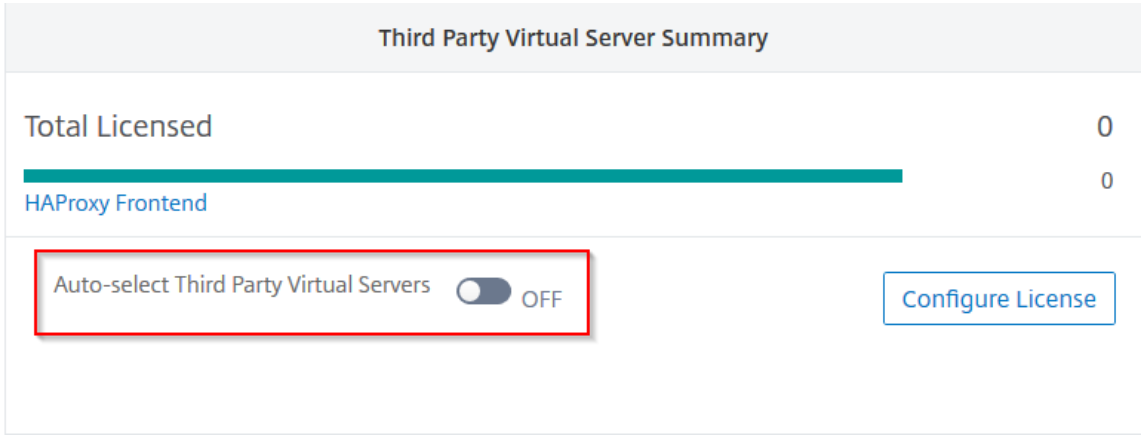


选择第三方虚拟服务器进行许可

1. 导航到 **“系统” > “许可和分析”**。

   控制板显示可用的虚拟服务器许可证、托管虚拟服务器以及虚拟服务器类型以及许可证到期信息。

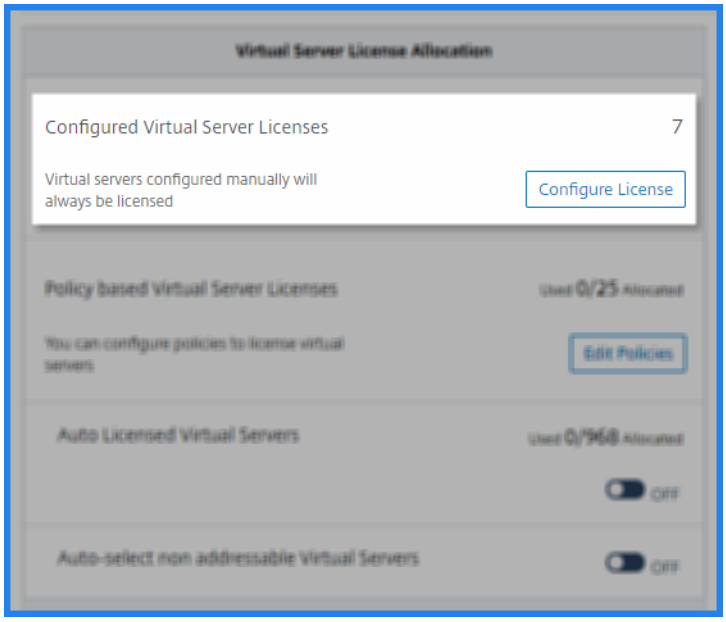
2. 在 第三方虚拟服务器摘要中，禁用 自动选择第三方虚拟服务器。



手动应用虚拟服务器许可证

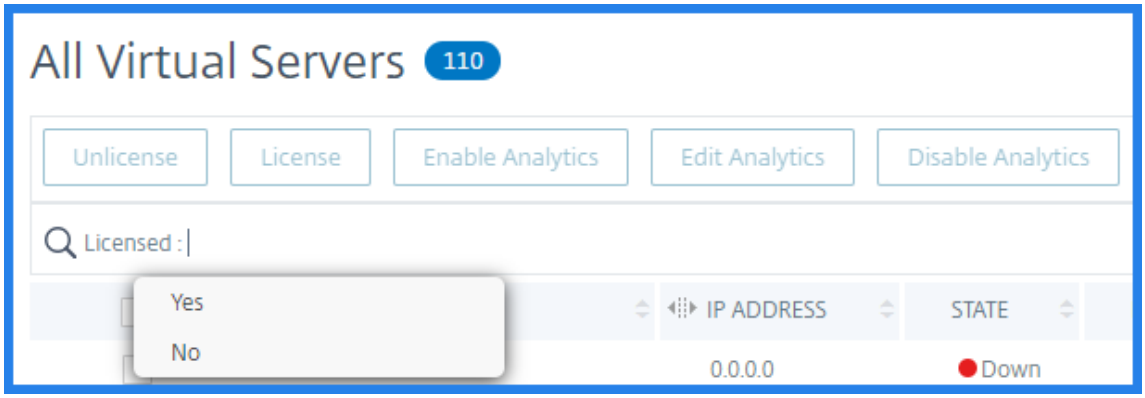
您可以手动将许可证应用于单个虚拟服务器。

1. 在“ 虚拟服务器许可证分配”中，选择“ 配置许可证”。



   此时将显示“ 所有玻璃体服务器”页面。

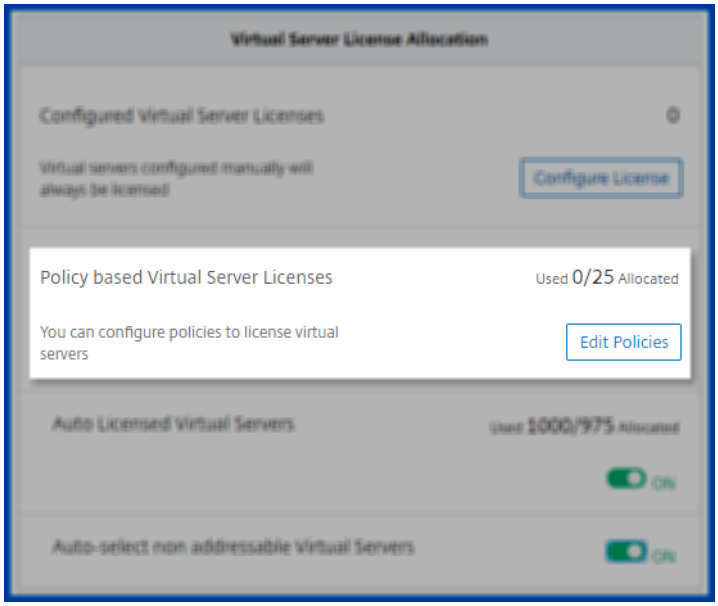
2. 使用属性：筛选未许可的虚拟服务器 `Licensed： No`。



3. 选择要许可的虚拟服务器。
4. 单击“ 许可证”。

配置基于策略的虚拟服务器许可

您可以配置策略以将许可证应用于虚拟服务器。此策略控制要自动许可的虚拟服务器的数量。它还将许可证仅应用于选定实例的虚拟服务器。

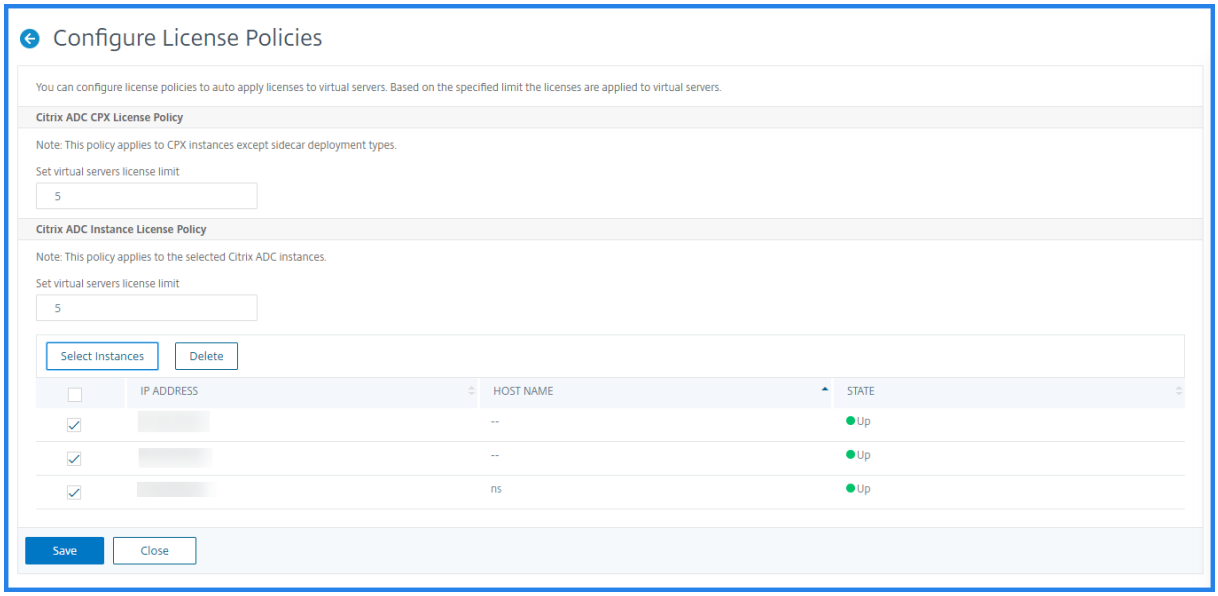


单击 编辑策略，您可以指定以下内容：

- 对 CPX 实例单独设置虚拟服务器限制以应用许可证。ADM 将许可证应用于 CPX 实例上的虚拟服务器，但不超过指定限制。

  > 重要信息：
  >
  > 此限制适用于 CPX 实例，但附带部署类型除外。
  >
  > 要查看侧车部署类型的 CPX 实例，请使用属性筛选虚拟服务器：`License Type: Freely Managed`。

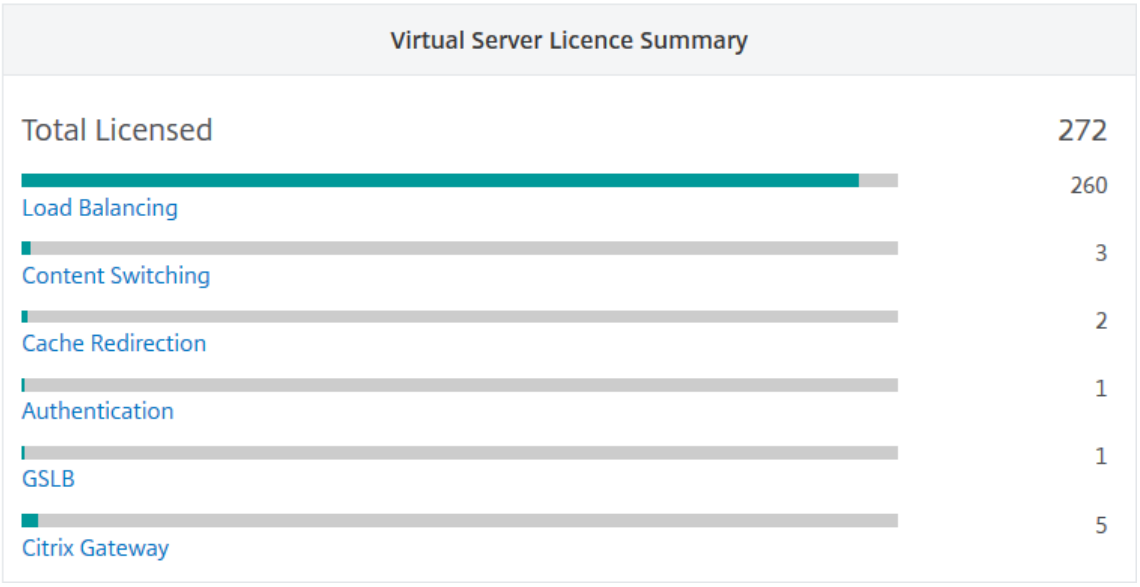
- 对选定 ADC 实例 (MPX/VPX/BLX) 设置虚拟服务器限制以应用许可证。ADM 将许可证应用于 ADC 实例上的虚拟服务器，但不超过指定限制。
- 选择要应用虚拟服务器许可证的优先级 ADC 实例。因此，ADM 只能将许可证应用于选定实例的虚拟服务器。



查看许可的虚拟服务器

将许可证应用到虚拟服务器后，您可以从 “许可 和分析” 页面查看已许可的虚拟服务器或第三方虚拟服务器。要查看许可的虚拟服务器，请执行以下步骤：

1. 导航到 **“系统” > “许可和分析”**。
2. 单击虚拟服务器 许可证摘要中的 **“许可总数”** 部分中的虚拟服务器类型。

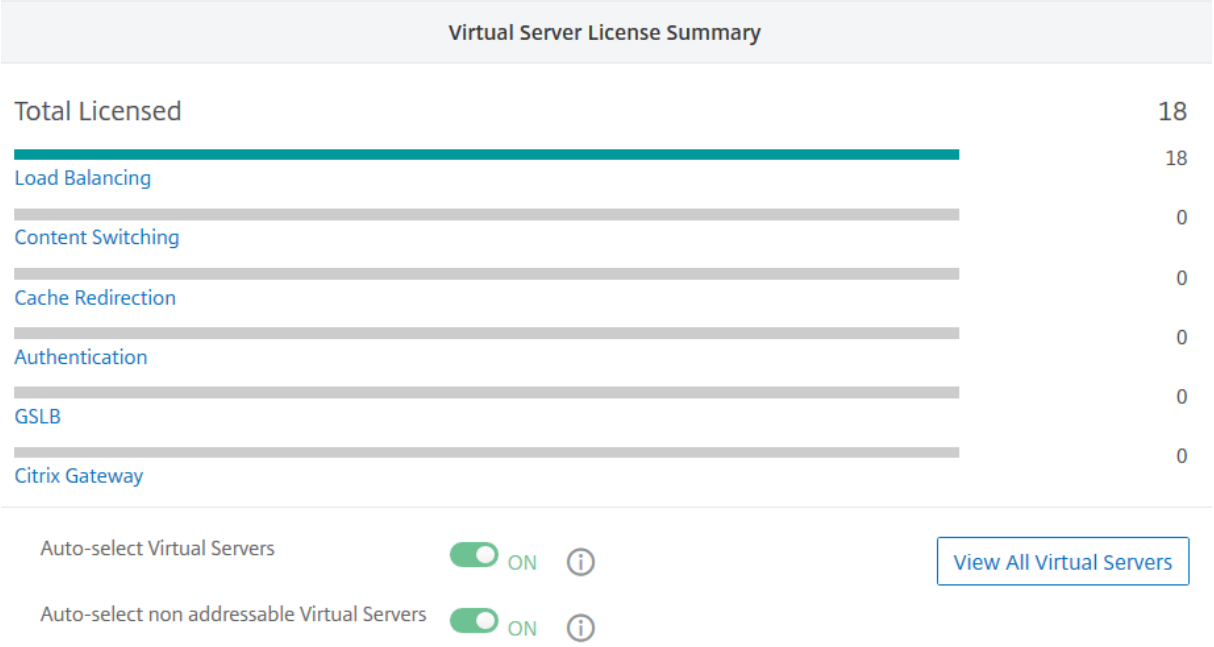


为不可寻址虚拟服务器配置自动许可证支持

默认情况下，Citrix ADM 不会自动将许可证应用于不可寻址的虚拟服务器。对于授权不可寻址虚拟服务器，必须禁用自动许可选项并手动选择不可寻址的虚拟服务器。这会增加您在应用许可证时最初手动选择不可寻址服务器的工作量。您

还需要在将新的不可寻址虚拟服务器添加到网络时手动选择这些服务器。

Citrix ADM 在 虚拟服务器许可证分配下的 Citrix ADM 中提供了一个选项。如果启用 “自动选择不可寻址的虚拟服务器” 选项，则自动应用许可证不可寻址的虚拟服务器。



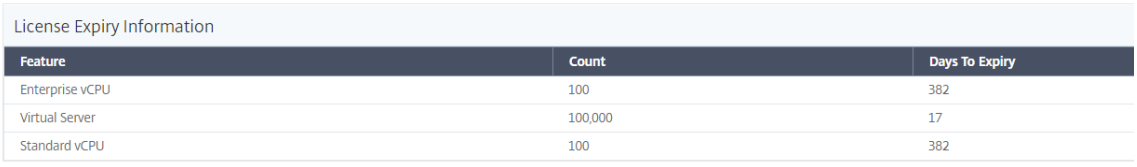
> 注意
>
> - 默认情况下，Citrix ADM 仍不会自动选择不可寻址的虚拟服务器进行许可。
> - 应用程序分析（应用程序仪表板）是当前在许可的非寻址虚拟服务器上支持的唯一分析。

虚拟服务器许可证的到期检查

现在，您可以在 Citrix ADM 中查看虚拟服务器许可证到期的状态并设置警报。

要查看许可证的状态，请执行以下操作：

1. 导航到 网络 > 许可证 > 系统许可证。
2. 在 许可证到期信息部分，您可以找到即将过期的许可证的详细信息：

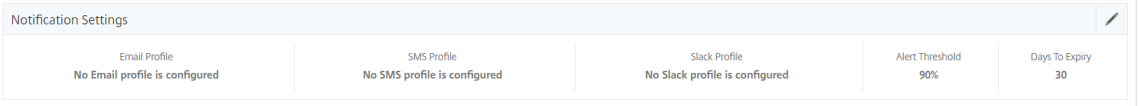


   - 功能：即将过期的许可证类型。

- 计数：受影响的虚拟服务器或实例的数量。
- **Days to expiry**（过期天数）：距离过期的天数。

要配置许可证的通知设置，请执行以下操作：

1. 导航到 “ 网络” > “ 许可证” > “ 设置”。
2. 在 “通 知设置” 部分，单击铅笔图标并编辑参数。



- 电子邮件配置文件：当许可证达到阈值或将要过期时发送通知的电子邮件配置文件或通讯组列表。
- **SMS**（短信）：**SMS** 配置文件或通讯组列表，用于在许可证达到阈值或将要过期时发送通知。
- **Slack** -指定 Slack 配置文件详细信息。
- 寻呼服务警报 -指定寻呼服务配置文件。根据您的 PagerDuty 门户中配置的通知设置，当您的证书即将过期时会发送通知。
- 通知我：设置通过电子邮件或 SMS 通知管理员的池许可证百分比。
- **License Expiry Threshold**（许可证过期阈值）：距离由 “Alert Threshold”（警报阈值）确定的许可证数过期的天数。
- 许可证到期：到期前剩余的天数。

系统要求

April 23, 2021

在安装 Citrix Application Delivery Management (ADM) 之前，必须了解软件要求、浏览器要求、端口信息、许可证信息和限制。

Citrix ADM 的要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
	注意： Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。

组件	要求
存储空间	默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。使用《Citrix ADM HA 部署指南》的最大限制部分（第 7 页）中提到的大小计算器。本指南可在我们的 下载站点 上的 **NetScaler MAS 12.1** 版 **>** 早期版本下找到。注意：您需要 Citrix 帐户才能访问部署指南和大小计算器。
	如果您的 Citrix ADM 存储需求超过 120 GB，则必须附加一个额外的磁盘。您只能添加一个附加磁盘。
	Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。
	有关详细信息，请参阅 如何将附加磁盘连接到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

Citrix ADM 内部部署代理的要求

组件	要求
—	—
RAM	32 GB
虚拟 CPU || 8 个 CPU
存储空间	30 GB
虚拟网络接口	1
吞吐量	1 Gbps

Citrix ADM 功能所需的最低 **Citrix ADC** 版本

Citrix ADM 功能	Citrix ADC 软件版本
样本	10.5 及更高版本
OpenStack/CloudStack 支持	11.0 及更高版本，如果需要分区
	11.1 及更高版本，如果需要在共享虚拟 LAN 上进行分区
NSX 支持	11.1 Build 47.14 及更高版本 (VPX)
Mesos/Marathon 支持	10.5 及更高版本

Citrix ADM 功能	Citrix ADC 软件版本
备份/还原	对于 Citrix ADC，10.1 及更高版本
	对于 Citrix SDX，11.0 及更高版本
使用作业监视/报告和配置	10.1 及更高版本
分析功能	
Web Insight	10.5 及更高版本
HDX Insight	10.1 及更高版本
Security Insight	11.0.65.31 及更高版本
Gateway Insight	11.0.65.31 及更高版本
Cache Insight	10.5 及更高版本 *
SSL Insight	12.0 及更高版本

* Citrix ADM 中不支持集成缓存度量，Citrix ADC 实例运行版本 11.0 版版本 66.x。

Citrix SD-WAN 实例管理的要求

Citrix SD-WAN 平台版本/版本和 **CitCitrix ADM** 功能的互操作性矩阵

平台版本	**Citrix SD-WAN WANOP**	**Citrix SD-WAN** 东南	**Citrix SD-WAN PE**
发现	是	是	是
配置	是	否	否
监视	是	否	否
报告（网络报告）	是	否	否
事件管理	是	否	否
HDX Insight	是	否	否
WAN Insight	是	否	否
HDX Insight（多跳部署）	是	是	否

Citrix SD-WAN 实例支持的瘦客户端

Citrix ADM 支持以下瘦客户端用于监视 Citrix SD-WAN 部署：

- Dell Wyse WTOS 型号 R10L Rx0L 瘦客户端
- NComputing N400
- Dell Wyse WTOS 型号 CX0 C00X Xenith
- Dell Wyse WTOS 型号 TXO T00X Xenith2
- Dell Wyse WTOS 型号 CX0 C10LE
- Dell Wyse WTOS 型号 R00LX Rx0L HDX 瘦客户端
- Dell Wyse Enhanced SUSE Linux Enterprise，型号 Dx0D、D50D
- Dell Wyse ZX0 Z90D7 (WES7) 瘦客户端

Citrix ADM 分析的要求

Citrix ADM 功能所需的最低 **Citrix Virtual Apps and Desktops** 版本

Citrix ADM 功能	Citrix Virtual Apps and Desktops 版本
HDX Insight	Citrix Virtual Apps and Desktops 7.0 及更高版本

> 注意
>
> Citrix Gateway 功能（版本 9.3 和 10.x 的标记为 Access Gateway Enterprise）必须在 Citrix ADC 实例上可用。Citrix ADM 不支持独立接入网关标准装置。

Citrix ADM 可以为在 Citrix 虚拟应用程序或 Citrix 虚拟桌面上发布并通过 Citrix Receiver 访问的应用程序生成报告。但是，此功能取决于安装了 Receiver 的操作系统。目前，Citrix ADC 不会解析通过在 iOS 或 Android 操作系统上运行的 Citrix Receiver 访问的应用程序或桌面的 ICA 流量。

支持 **HDX** 洞察的瘦客户端

- 基于 Dell Wyse Windows 的瘦客户端
- 基于 Wyse Linux 的戴尔瘦客户机
- 基于 Dell Wyse ThinOS 的瘦客户端
- 基于 10ZiG Ubuntu 的瘦客户端
- IGEL UD3 W7+ (M340)
- IGEL UD3 W7 (M340C)

HDX Insight 所需的 **Citrix ADC** 实例许可证

Citrix ADM 针对 HDX Insight 收集的数据取决于所监视的 Citrix ADC 实例的版本和许可证。仅针对运行 10.5 版及更高版本的 Citrix ADC 高级版和高级设备显示 HDX Insight 能分析报告。

Citrix ADC 许可证/期限	5 分钟	1 小时	1 天	1 周	> 1 个月
标准	否	否	否	否	否
Advanced	是	是	否	否	否
Premium	是	是	是	是	是

受支持的虚拟机管理程序

下表列出了 Citrix ADM 支持的虚拟机管理程序。

虚拟机管理程序	版本
Citrix Hypervisor	7.1 和 7.4
VMware ESX	6.0、6.5 和 6.7
Microsoft Hyper-V	第二届会议及第二届会议
通用 KVM	第 7.4 号和第 16 号文件

支持的操作系统和接收器版本

下表列出了 Citrix ADM 支持的操作系统以及每个系统当前支持的 Citrix Receiver 版本：

操作系统	Receiver 版本
Windows	4.0 标准版
Linux	13.0.265571 及更高版本
Mac	11.8 (Build 238301) 及更高版本
HTML5	1.5*
Chrome 应用程序	1.5*

* 适用于 Citrix 云桥（Citrix SD-WAN ANOP）7.4 版及更高版本。

支持的浏览器

下表列出了 Citrix ADM 支持的 Web 浏览器：

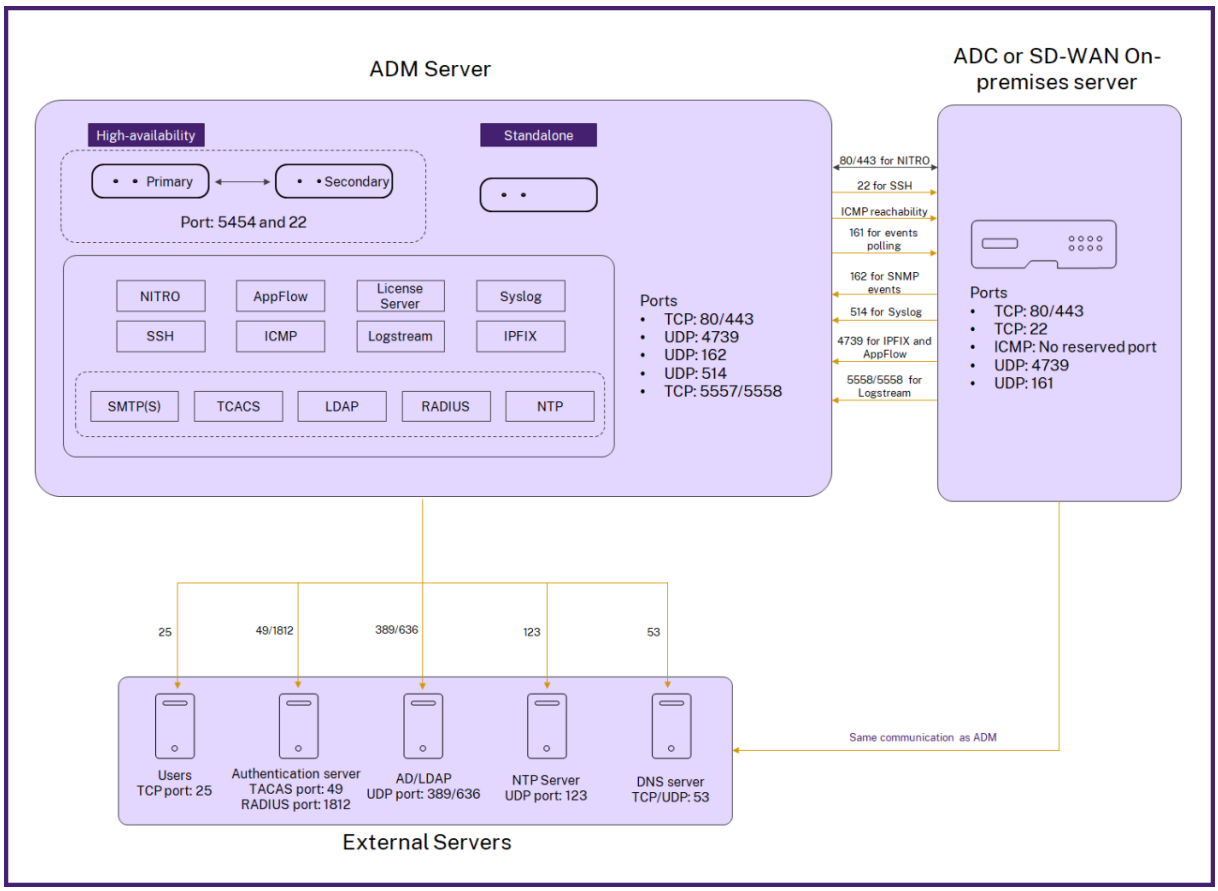
Web 浏览器	版本
Internet Explorer	11.0 及更高版本
Google Chrome	Chrome 19 及更高版本
Safari	Safari 5.1.1 及更高版本
Mozilla Firefox	Firefox 3.6.25 及更高版本

支持的端口

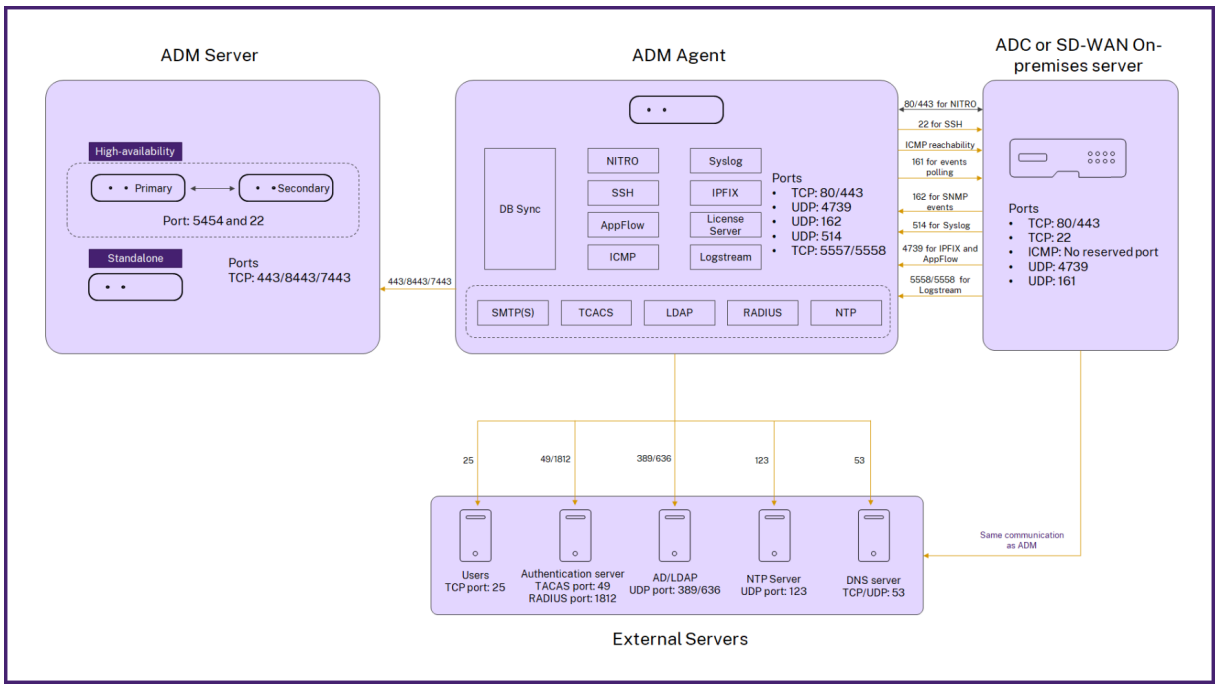
Citrix ADM 使用 Citrix ADC IP（称为 NSIP）地址与 Citrix ADC 进行通信。您可以使用 ADM 代理作为 ADC 实例与 ADM 或 SD-WAN 实例和 ADM 之间的中介。要与这些服务器建立通信，请打开所需的端口。

> 注意
>
> 如果已将 Citrix ADC 配置为高可用性模式，则 Citrix ADM 将使用 Citrix ADC 子网 IP（管理 SNIP）地址与 Citrix ADC 进行通信。对于使用 SNIP 与 Citrix ADM 进行通信，所需的端口保持不变。

无代理部署的网络端口图：



包括 **ADM** 代理的部署的网络端口图：



以下各节说明了所需的端口及其用途：

- ADM 服务器
- ADM 代理
- ADC 或 SD-WAN 实例
- 外部服务器

ADM 服务器的端口

下表说明了 ADM 服务器上必须打开的所需端口。

端口	类型	详细信息	通信方向
5454 和 22	TCP	在高可用性模式下，Citrix ADM 节点之间用于通信和数据库同步的默认端口。	Citrix ADM 主节点到 Citrix ADM 辅助节点
443/8443/7443	TCP	Citrix ADM 代理和 Citrix ADM 之间的通信端口。	Citrix ADM 代理启动与 Citrix ADM 的通信。然后，Citrix ADM 和代理程序互动。

如果 ADM 和 ADC 实例没有使用代理进行通信，请确保在 ADM 服务器上打开以下端口：

端口	类型	详细信息	通信方向
80/443	TCP	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 NITRO 通信。	Citrix ADM 代理将 Citrix ADC 和 Citrix ADC 转至 Citrix ADM 代理
4739	UDP	用于从 Citrix ADC 或 Citrix SD-WAN 实例到 Citrix ADM 的应用流通信。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM 代理
162	UDP	接收从 Citrix ADC 实例到 Citrix ADM 的 SNMP 事件。	Citrix ADC 到 Citrix ADM 代理
514	UDP	将系统日志消息从 Citrix ADC 或 Citrix SD-WAN 实例接收到 Citrix ADM。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM 代理

端口	类型	详细信息	通信方向
5557/5558	TCP	用于从 Citrix ADC 到 Citrix ADM 的日志流通信（用于安全洞察、Web 洞察和 HDX 洞察）。	Citrix ADC 到 Citrix ADM

ADM 代理的端口

下表说明了必须在 ADM 代理上打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 NITRO 通信。	Citrix ADM 代理将 Citrix ADC 和 Citrix ADC 转至 Citrix ADM 代理
4739	UDP	用于从 Citrix ADC 或 Citrix SD-WAN 实例到 Citrix ADM 的应用流通信。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM 代理
162	UDP	接收从 Citrix ADC 实例到 Citrix ADM 的 SNMP 事件。	Citrix ADC 到 Citrix ADM 代理
514	UDP	将系统日志消息从 Citrix ADC 或 Citrix SD-WAN 实例接收到 Citrix ADM。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM 代理
5557/5558	TCP	用于从 Citrix ADC 到 Citrix ADM 的日志流通信（用于安全洞察、Web 洞察和 HDX 洞察）。	Citrix ADC 到 Citrix ADM

ADC 和 **SD-WAN** 实例的端口

此表说明了 Citrix ADC 和 SD-WAN 实例上必须打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 NITRO 通信。443. 用于在高可用性模式下在 Citrix ADM 服务器之间进行 NITRO 通信。	Citrix ADM 到 Citrix ADC 和 Citrix ADC 到 Citrix ADM
22	TCP	用于从 Citrix ADM 到 Citrix ADC 或 Citrix SD-WAN 实例的 SSH 通信。用于在高可用性模式下部署的 Citrix ADM 服务器之间进行同步。此外，ADM 代理和 Citrix ADC 之间的 SSH 通信需要此端口。	Citrix ADM 到 Citrix ADC。或者，将 Citrix ADM 代理转到 Citrix ADC。
无保留的端口	ICMP	检测在高可用性模式下部署的 Citrix ADM 和 Citrix ADC 实例、SD WAN 实例或辅助 Citrix ADM 服务器之间的网络可访问性。	Citrix ADM 到 Citrix ADC
161	UDP	轮询来自 ADC 实例的事件。	Citrix ADM 到 Citrix ADC

> 注意：
>
> 在 ADM 高可用性部署的情况下，来自 ADM 的所有通信都使用主节点 IP 地址。

外部服务器的端口

下表说明了必须在外部服务器上打开的所需端口：

端口	类型	详细信息	通信方向
25	TCP	将 SMTP 通知从 Citrix ADM 发送给用户。	面向用户的 Citrix ADM。

端口	类型	详细信息	通信方向
389/636	TCP	用于身份验证协议的默认端口。用于 Citrix ADM 和 LDAP 外部身份验证服务器之间的通信。	Citrix ADM 到 LDAP 外部身份验证服务器
123	UDP	的默认 NTP 服务器端口，正在与多个时间源同步。	Citrix ADM 到 NTP 服务器
1812	RADIUS	用于身份验证协议的默认端口。用于 Citrix ADM 和 RADIUS 外部身份验证服务器之间的通信。	Citrix ADM 到 RADIUS 外部认证服务器
49	TACACS	用于身份验证协议的默认端口。用于 Citrix ADM 和 TACAS 外部身份验证服务器之间的通信。	Citrix ADM 到 TACACS 外部身份验证服务器

限制

在 Citrix ADM 12.1 或更高版本中，以下功能支持 IPv6 格式的 IP 地址：

1. 针对 Citrix ADM GUI 的管理访问权限
2. Citrix ADC 的管理访问权限
3. 登记和盘存
4. 网络控制板
5. SSL 仪表板
6. 配置作业
7. 配置审核
8. 网络功能
9. 网络报告
10. ADC 实例的备份和恢复
11. 来自 Citrix ADC 的 SNMP 事件

以下功能不支持 IPv6：

1. 高可用性浮动 IP

2. 从支持 IPv6 的 ADC 收到的系统日志
3. 支持 IPv6 的 ADC 上的样书
4. 分析
5. 池许可

入门

April 23, 2021

本文档指导您如何首次开始部署和设置 Citrix Application Delivery Management (ADM)。本文档面向管理 Citrix 网络设备（思杰 SD-WO、Citrix Gateway 等）和第三方设备（如 HAProxy）的网络和应用程序管理员。无论您计划使用 Citrix ADM 管理的设备类型如何，都必须按照本文档中的步骤操作。

如果您是 Citrix ADM 的现有用户，则建议您查看 [发行说明 ([])]、和 [许可证 ()] 详细 [升级 ()] 信息到最新版本的 Citrix ADM。

步骤 **1-**检查系统要求

在开始在数据中心部署 Citrix ADM 之前，请查看软件要求、浏览器要求、端口信息、许可证信息和限制。

- 许可证信息。可以在没有许可证的情况下管理和监视任何数量的实例和实体。但是，您只能管理 30 个发现的应用程序，并且只能查看两个虚拟服务器的分析信息，而无需应用许可证。要管理 30 多个应用程序或查看两个以上虚拟服务器的分析，您必须购买相应的许可证。了解更多。
- 操作系统和接收器要求。查看此信息以确保您有适用于支持的操作系统的正确 Receiver 版本。了解更多。
- 浏览器要求。要访问 Citrix ADM GUI，必须确保您拥有所需的浏览器和版本正确。了解更多。
- 端口。确保 Citrix ADM 与 Citrix ADC 和/或 SD-WAN 实例通信所需的端口处于打开状态。了解更多。
- **Citrix ADC** 实例要求。不同的 Citrix ADC 软件版本支持不同的 Citrix ADM 功能。查看此信息，以确保您已将 Citrix ADC 实例升级到正确版本。了解更多。
- **Citrix SD-WAN** 实例要求。查看此信息，以确保您已将 Citrix SD-WAN 实例升级到正确的版本，并且具有正确的平台版本。了解更多。

步骤 **2-**部署 **Citrix ADM**

要管理和监视应用程序和网络基础架构，必须首先在其中一个虚拟机管理程序上安装 Citrix ADM。您可以将 Citrix ADM 部署为单个服务器或高可用性模式。如果您使用的是 Citrix ADC Insight Center，则可以迁移到 Citrix ADM，除了分析功能外，还可以使用管理、监视、编排和应用程序管理功能。

- 单服务器部署。在 Citrix ADM 单服务器部署中，数据库与服务器集成，并且单个服务器处理所有流量。您可以使用思杰虚拟机管理程序、VMware ESXi、微软 Hyper-V 和 Linux KVM 部署 Citrix ADM。请参阅：
  - 使用思杰虚拟机管理程序的 Citrix ADM
  - Citrix ADM 与微软超 V
  - 采用 VMware ESXi 的 Citrix ADM
  - 采用 Linux KVM 服务器的 Citrix ADM
- 高可用性部署。两台 Citrix ADM 服务器的高可用性部署 (HA) 可提供不间断的操作。在高可用性设置中，两个 Citrix ADM 节点必须以主动-被动模式部署在同一子网上使用相同的软件版本和版本，并且必须具有相同的配置。通过部署 HA 后，可以在 Citrix ADM 主节点上配置浮动 IP 地址，无需单独使用 Citrix ADC 负载均衡器。要了解更多信息，请参阅在高可用性部署中进行配置。

步骤 **3-**将实例添加到 **Citrix ADM**

实例是您希望从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备或第三方设备。如果要管理和监视这些实例，则必须将实例添加到 Citrix ADM 服务器。您可以将以下实例添加到 Citrix ADM 中：

- Citrix ADC
  - Citrix ADC MPX
  - Citrix ADC VPX
  - Citrix ADC SDX
  - Citrix ADC CPX
  - Citrix Gateway
  - Citrix SD-WAN
- HAProxy

将实例添加到 Citrix ADM 服务器时，服务器会隐式与实例通信并收集这些实例的清单。

了解更多

步骤 **4-**在虚拟服务器上启用分析

要查看应用程序通信流的分析数据，必须在接收特定应用程序的流量的虚拟服务器上启用分析功能。

了解更多

步骤 **5-**在 **Citrix ADM** 上配置 **NTP** 服务器

您必须在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

了解更多

步骤 **6-**配置系统设置以获得最佳 **Citrix ADM** 性能

在开始使用 Citrix ADM 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

- 配置系统警报。您应该配置系统警报，以确保您可以了解任何严重或重大系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。
- 配置系统通知。可以发送通知来为一些系统相关的功能选择用户组。您可以在 Citrix ADM 中设置通知服务器，还可以配置电子邮件和短消息服务 (SMS) Gateway 服务器以向用户发送电子邮件和文本通知。这可确保您将收到任何系统级活动（例如，用户登录或系统重新启动）通知。
- 配置系统修剪设置。要限制存储在 Citrix ADM 服务器数据库中的报告数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。
- 配置系统备份设置。Citrix ADM 每天在 00:30 时间自动备份系统。默认情况下，它保存三个备份文件。您可能希望保留更多数量的系统备份。
- 配置实例备份设置。如果备份 Citrix ADC 实例的当前状态，则可以在实例变得不稳定时使用备份文件恢复稳定性。在执行升级之前这样做尤其重要。默认情况下，每 12 小时进行一次备份，且有三个备份文件保留在系统中。
- 配置实例事件修剪设置。要限制存储在 Citrix ADM 服务器数据库中的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。
- 配置实例系统日志清除设置。要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定将从 Citrix ADM 中删除以下系统日志数据的天数：
  - 通用系统日志数据
  - AppFirewall 数据
  - Citrix Gateway 数据。

    了解更多

下一步是什么

部署并设置 Citrix ADM 后，可以开始管理和监视实例和应用程序。

管理 **Citrix ADC** 实例和应用程序。Citrix ADC 实例支持所有 Citrix ADM 功能。您可以开始使用任何功能。

管理 **Citrix ADC SD-WAN** 实例。SD-WAN WO 实例并非所有 Citrix ADM 功能都受支持，例如，不支持证书管理或配置审核。要了解支持哪些功能以及如何使用它们，请参阅 使用 Citrix ADM 管理思杰 SD-WO。

管理 **HAProxy** 实例和应用程序。您可以监视 HAProxy 部署中配置的前端、后端和服务器。您还可以使用应用程序管理功能监视 Citrix ADM 监视的前端的实时统计信息。要了解 HAProxy 支持哪些功能以及如何使用它们，请参阅 使用 Citrix ADM 管理和监视 HAProxy 实例。

部署

April 23, 2021

在使用 Citrix ADM 管理和监视应用程序和网络基础架构之前，必须先将其安装到其中一个虚拟机管理程序或 Kubernetes 群集上。如果在 Hypervisor 上部署 Citrix ADM，则可以将其部署为单个服务器或高可用性模式。高可用性模式不适用于 Kubernetes 群集。如果您使用的是 NetScaler Insight Center，则可以将 Citrix ADM 迁移到该中心，除了分析功能外，还可以利用管理、监视、编排和应用程序管理功能。

- 单服务器部署：对于部署在 Hypervisor 上的独立 ADM，数据库与服务器集成，单个服务器处理所有流量。您可以使用思杰虚拟机管理程序、VMware ESXi、微软 Hyper-V 和 Linux KVM 部署 Citrix ADM。请参阅：
  - 思杰虚拟机管理程序上的 Citrix ADM
  - 微软 Hyper-V 上的 Citrix ADM
  - Citrix ADM 在 VMware ESXi 上
  - Linux KVM 服务器上的 Citrix ADM
  - 库贝内特斯群集上的 Citrix ADM
- 高可用性 **(HA)** 部署：两台 Citrix ADM 服务器的 HA 部署可提供不间断的操作。在 HA 设置中，两个 Citrix ADM 节点必须以主动-被动模式部署在同一子网上使用相同的软件版本和版本，并且必须具有相同的配置。通过部署 HA 后，可以在 Citrix ADM 主节点上配置浮动 IP 地址，无需使用单独的 Citrix ADC 负载均衡器。请参阅：在高可用性部署中进行配置。

> 注意：
>
> 高可用性不适用于部署在 Kubernetes 群集上的 ADM。

- 从 **NetScaler Insight Center** 迁移到 **Citrix ADM**：您可以将 NetScaler Insight Center 部署迁移到 Citrix ADM，而不会丢失现有配置、设置或数据。使用 Citrix ADM，您不仅可以查看由 Citrix ADC 和 Citrix SD-WAN 实例生成的各种分析，还可以通过单个统一的控制台管理、监控和故障排除整个全局应用程序交付基础架构。请参阅：从 NetScaler Insight Center 迁移到 Citrix ADM
- 将 **Citrix ADM** 与控制器集成：控制器与 Citrix ADM 集成，用于网络分析和性能管理。请参阅：将 Citrix ADM 与控制器集成

安装 **Citrix ADM** 的先决条件

April 23, 2021

您可以下载并安装适用于微软 HyperV、
VMware ESXi、Linux KVM 和 Citrix Hypervisor 平台的 Citrix Application Delivery Management (ADM) 作为虚拟设备。在安装 C
itrix ADM 之前，必须了解所有这些平台上的软件要求、浏览器要求、端口
信息、许可证信息和限制。

有关安装 Citrix ADM 的特定平台要求和详细步骤，请参阅以下主题：

- 使用思杰虚拟机管理程序的 Citrix ADM
- 采用微软 HyperV 的 Citrix ADM
- 采用 VMware ESXi 的 Citrix ADM
- 采用 Linux KVM 服务器的 Citrix ADM

Citrix ADM 的一般要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议对 Citrix ADM 部署使用固态硬盘 (SSD) 技术。
	所需的默认存储空间为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。使用《Citrix ADM HA 部署指南》的最大限制部分（第 7 页）中提到的大小计算器。本指南可在我们的 下载站点 上的 **NetScaler MAS 12.1** 版 **>** 早期版本下找到。注意：您需要 Citrix 帐户才能访问部署指南和大小计算器
	如果 Citrix ADM 存储需求超过 120 GB，则必须附加额外的磁盘。
	Citrix 建议您在初始部署时估算存储空间并附加额外的磁盘。您只能添加一个额外的磁盘。
	有关详细信息，请参阅如何将附加磁盘连接到 Citrix ADM。
虚拟网络接口	1

组件	要求
吞吐量	1 Gbps

> 注意：
>
> 思杰建议您在本地存储上托管 Citrix ADM VHD。当托管在 SAN 中的存储设备上时，Citrix ADM 可能无法按预期工作。

思杰虚拟机管理程序上的 **Citrix ADM**

April 23, 2021

要在 Citrix Hypervisor（以前称为 XenServer）上安装 Citrix ADM，您需要首先将 Citrix ADM .xva 映像文件下载到本地计算机。您需要使用 Citrix XenCenter 来执行 Citrix ADM 安装。

必备条件

在安装 Citrix ADM 之前，请验证是否满足以下要求：

- Citrix Hypervisor 7.1 或更高版本安装在符合最低要求的硬件上。
- 在满足最低要求的管理工作站上安装 XenCenter。您必须使用 XenCenter 才能在思杰虚拟机管理程序上安装 Citrix ADM。
- 您已下载了 Citrix ADM .XVA 映像文件。

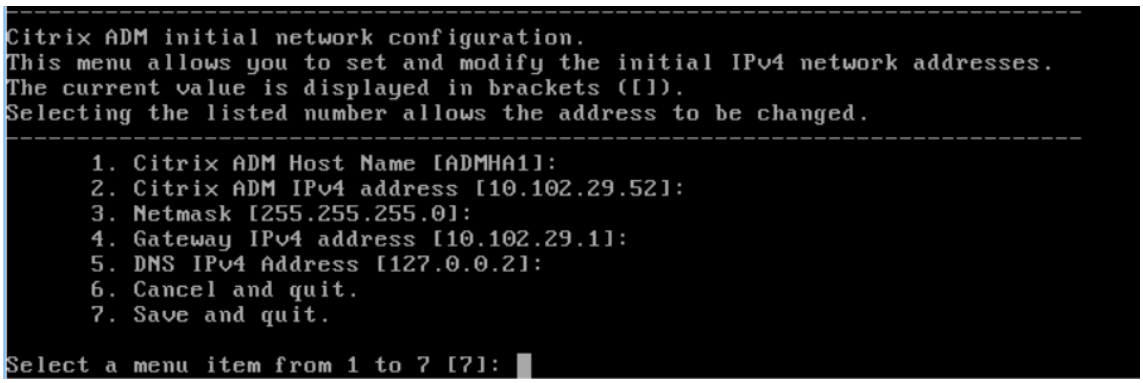
XenCenter 系统要求

XenCenter 是一款 Windows 客户端应用程序。它不能在与 Citrix Hypervisor 主机相同的计算机上运行。下表说明了最低系统要求。

组件	要求
操作系统	视窗 7、视窗服务器 2003 或视窗 10
.NET Framework	2.0 版或更高版本
CPU	750 MHz (MHz)，推荐：1 千兆赫兹（GHz）或更快
RAM	1 GB，建议：2 GB
NIC	100 Mbps 或速度更高的 NIC

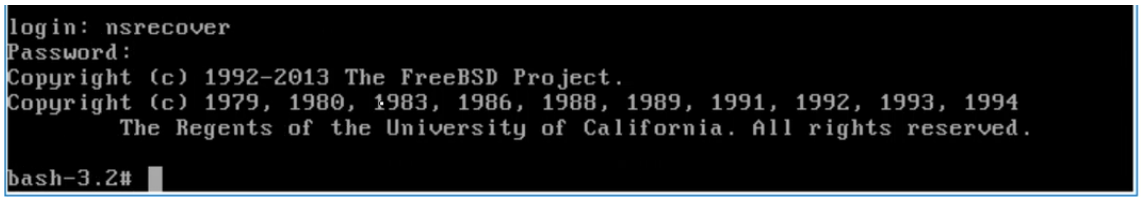
安装 **Citrix Application Delivery Management**

1. 将 XVA 映像文件导入 Citrix Hypervisor，然后从 “ 控制台” 选项卡配置初始网络配置选项。



2. 指定所需的 IP 地址后，保存配置设置。

3. 出现提示时，使用 ns 恢复/nsroot 凭据登录。



> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`、更新配置并保存配置。

4. 通过在 shell 提示符下键入命令来运行部署脚本：`/mps/deployment_type.py`

5. 选择作为 **Citrix ADM** 服务器的部署类型。如果不选择任何选项，默认情况下，它部署为服务器。

6. 键入是将 Citrix ADM 部署为独立部署。

7. 键入 “是” 以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，可以稍后更新初始配置设置。

验证

安装服务器后，您可以通过在 Web 浏览器中键入 Citrix ADM 服务器的 IP 地址来访问 GUI。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

微软 **Hyper-V** 上的 **Citrix ADM**

April 23, 2021

若要在 Microsoft Hyper-V 上安装 Citrix ADM，您必须首先将 Citrix ADM 映像文件下载到本地计算机。此外，请确保您的系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。

必备条件

在安装 Citrix ADM 虚拟设备之前，请验证是否满足以下要求：

- 在满足最低要求的硬件上安装 Microsoft Hyper-V 6.2 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 Microsoft Hyper-V 管理器。
- 您已下载 Citrix ADM 映像文件。

微软 **Hyper-V** 系统要求

Microsoft Hyper-V 是 Windows 客户端应用程序。下表说明了最低系统要求。

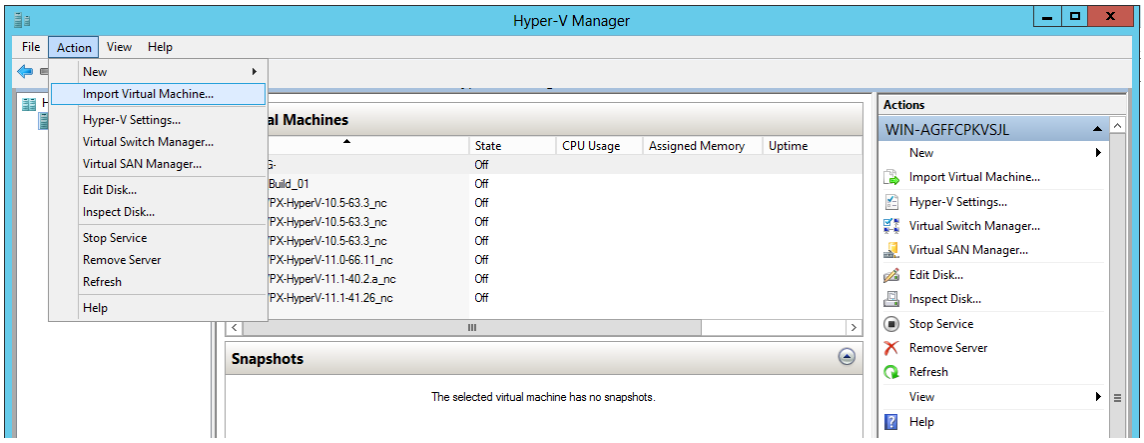
组件	要求
操作系统	Windows Server 2012 R2
.NET Framework	2.0 版或更高版本
CPU	750 MHz (MHz)，推荐：1 千兆赫兹（GHz）或更快
RAM	1 GB，建议：2 GB
NIC	100 Mbps 或速度更高的 NIC

安装 **Citrix Application Delivery Management**

可以安装的 Citrix ADM 服务器的数量取决于 Hyper-V 服务器上的可用内存。

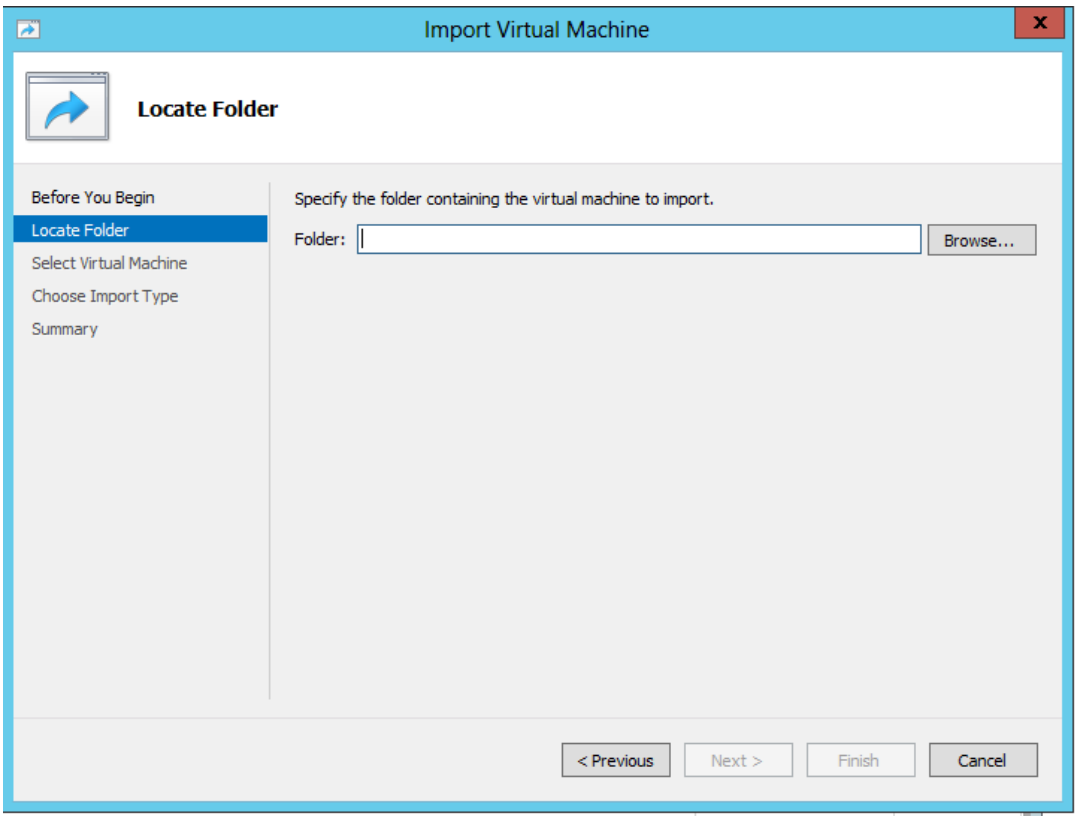
要安装 **Citrix ADM**，请执行以下操作：

1. 在工作站上启动 Hyper-V Manager 客户端。
2. 在 **Action**（操作）菜单上，单击 **Import Virtual Machine**（导入虚拟机）。



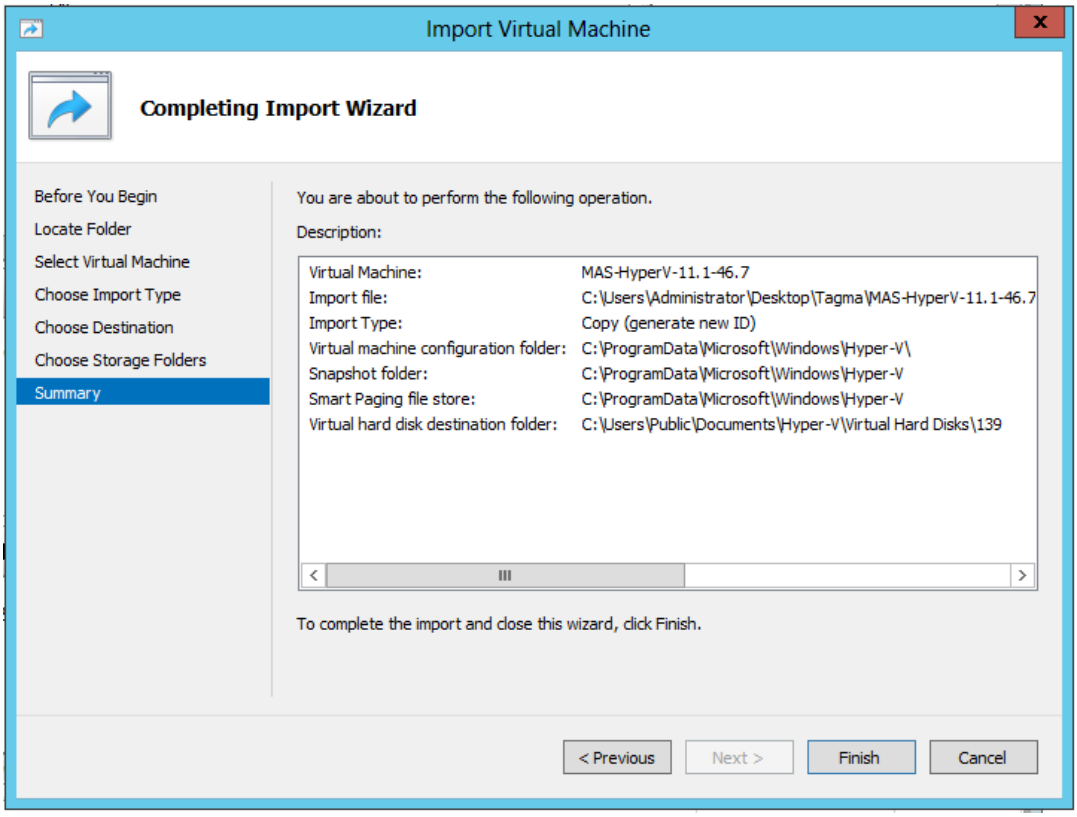
3. 导入 Hyper-V 图像，然后执行以下操作：
   a) 在“导入虚拟机”对话框的“ 查找文件夹”部分，浏览到保存 Citrix ADM Hyper-V 映像的文件夹，选择该文件夹，然后单击“ 下一步”。
   b) 在“Select Virtual Machine”（选择虚拟机）部分，选择适当的虚拟机名称。
   c) 在 **Choose Import Type**（选择导入类型）部分，选择“Copy the virtual machine (create a new unique ID)”（复制虚拟机 (创建新的唯一 ID)）选项，并单击“Next”（下一步）。
   d) 在 **Choose Destination**（选择目标）部分，可以指定要存储虚拟机文件的文件夹。

> 注意
>
> 默认情况下，向导将虚拟机文件导入您本地主机上的默认 Hyper-V 文件夹。



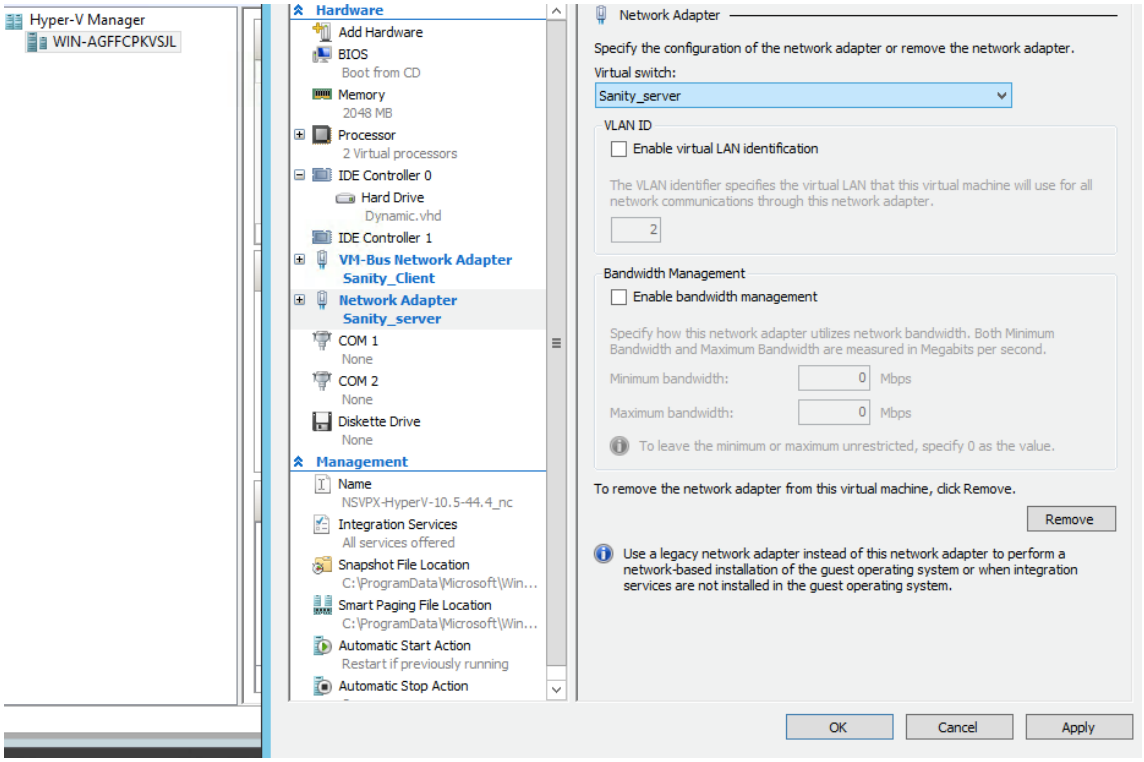
e) 在 **Choose Storage Folders**（选择存储文件夹）部分，可以选择要存储虚拟硬盘的位置，然后单击 **Next**（下一步）。

f) 可以在摘要窗格中确认虚拟机详细信息，单击 **Finish**（完成）。



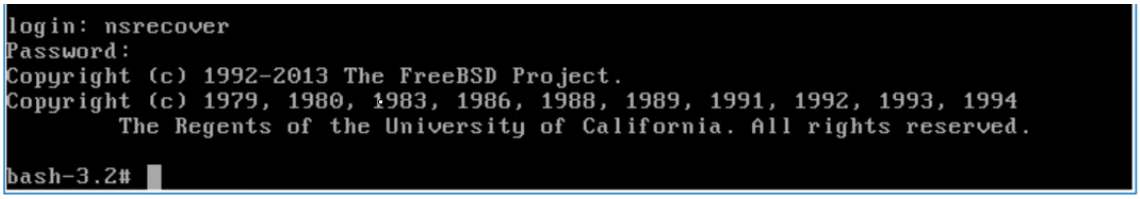
Citrix ADM Hyper-V 图像显示在右窗格中。

4. 右键单击 Citrix ADM Hyper-V 映像，然后单击 设置。
5. 在出现的对话框的左窗格中，导航到 “ 硬件” > “ **VM_Bus** 网络适配器”，然后在右窗格中，从 “网络” 列表中选择相应的网络。



6. 单击 应用，然后单击 确定。
7. 右键单击 Citrix ADM Hyper-V 映像，然后单击 连接。
8. 在“控制台”窗口中，单击“ 开始”按钮。
9. 配置初始网络配置选项。

10. 指定所需的 IP 地址后，保存配置设置。
11. 出现提示时，使用 ns 恢复/nsroot 凭据登录。



> 注意
>
> 登录后，如果要更新初始网络配置，请键入 networkconfig、更新配置并保存配置。

12. 通过在 shell 提示符下键入命令来运行部署脚本：

```
deployment_type.py
<!--NeedCopy-->
```

```
bash-3.2# deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
```

13. 选择作为 **Citrix ADM** 服务器的部署类型。如果不选择任何选项，默认情况下，它部署为服务器。

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

14. 键入是将 Citrix ADM 部署为独立部署。
15. 键入 **“是”** 以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，可以稍后更新初始配置设置。

验证

安装服务器后，您可以通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问 GUI。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

Citrix ADM 在 VMware ESXi 上

April 23, 2021

要在 VMware ESXi 上安装 Citrix ADM 虚拟设备，请使用 VMware vSphere 客户端。

必备条件

在开始安装虚拟设备之前，请确认以下要求：

- 安装受支持的 VMware ESXi 版本（6.0、6.5 和 6.7）。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 下载 Citrix ADM 安装文件。

> 注意
>
> 只有 **Citrix ADM 13.0** 版本 **47.22** 或更高版本支持虚拟动作。您可以计划和自动迁移 ESXi 虚拟机管理程序上部署的 ADM 服务器，包括 vSphere HA 和 vSphere DRS 设置。

安装 **Citrix ADM**

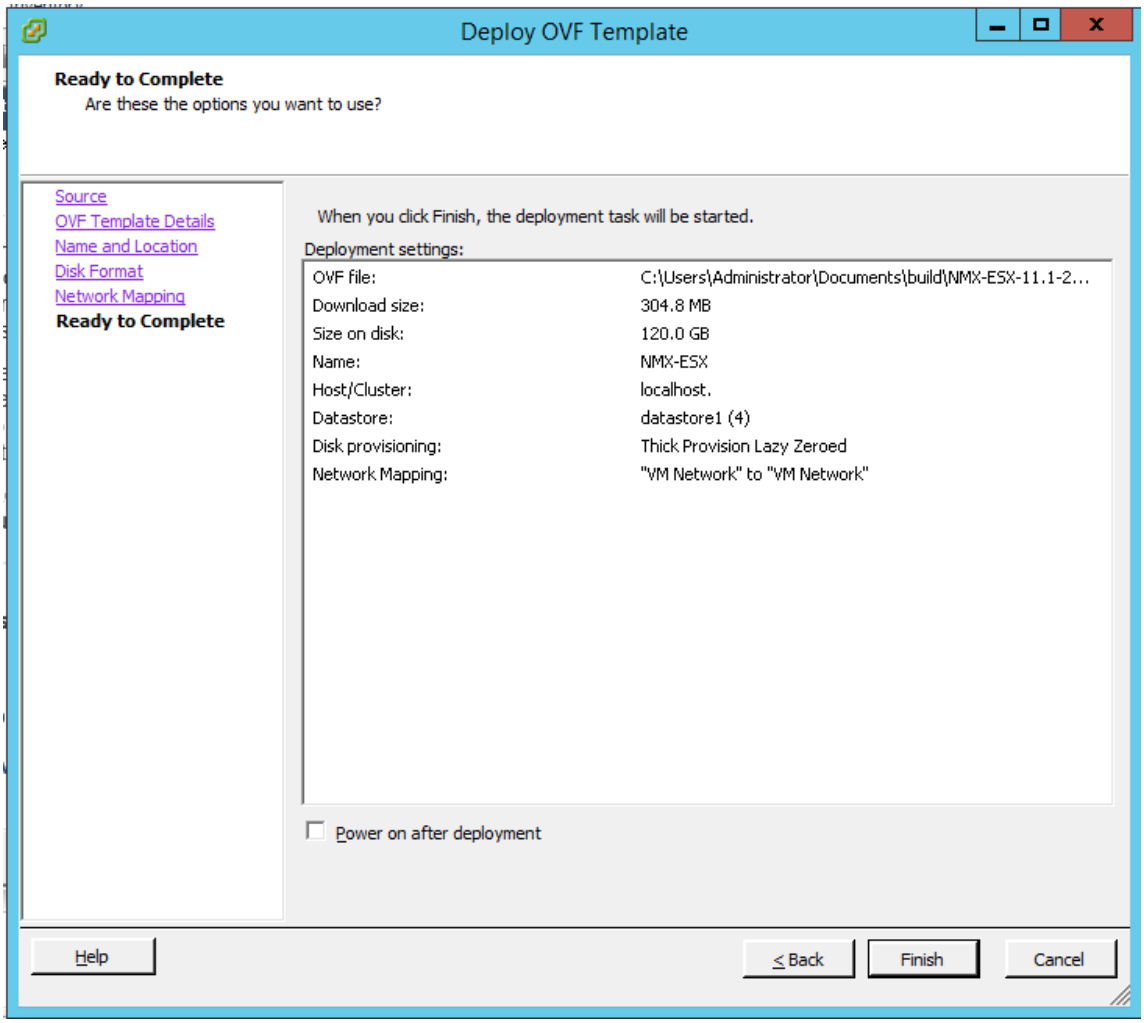
1. 在工作站上启动 VMware vSphere Client。
2. 在 “ **IP** 地址**/**名称” 文本框中，键入要连接到的 VMware ESXi 服务器的 IP 地址。
3. 在 **User Name**（用户名）和 **Password**（密码）文本框中，键入管理员凭据，然后单击 **Login**（登录）。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在 “部 署 **OVF** 模板” 对话框的 “ 从文件或 **URL** 部署” 中，选择.ovf 文件，然后单击 “ 下一步”。

   > 注意
   >
   > 如果出现带有以下文本的警告消息：所选主机上不支持操作系统标识符，请检查 VMware 服务器是否支持 FreeBSD 操作系统。单击是。

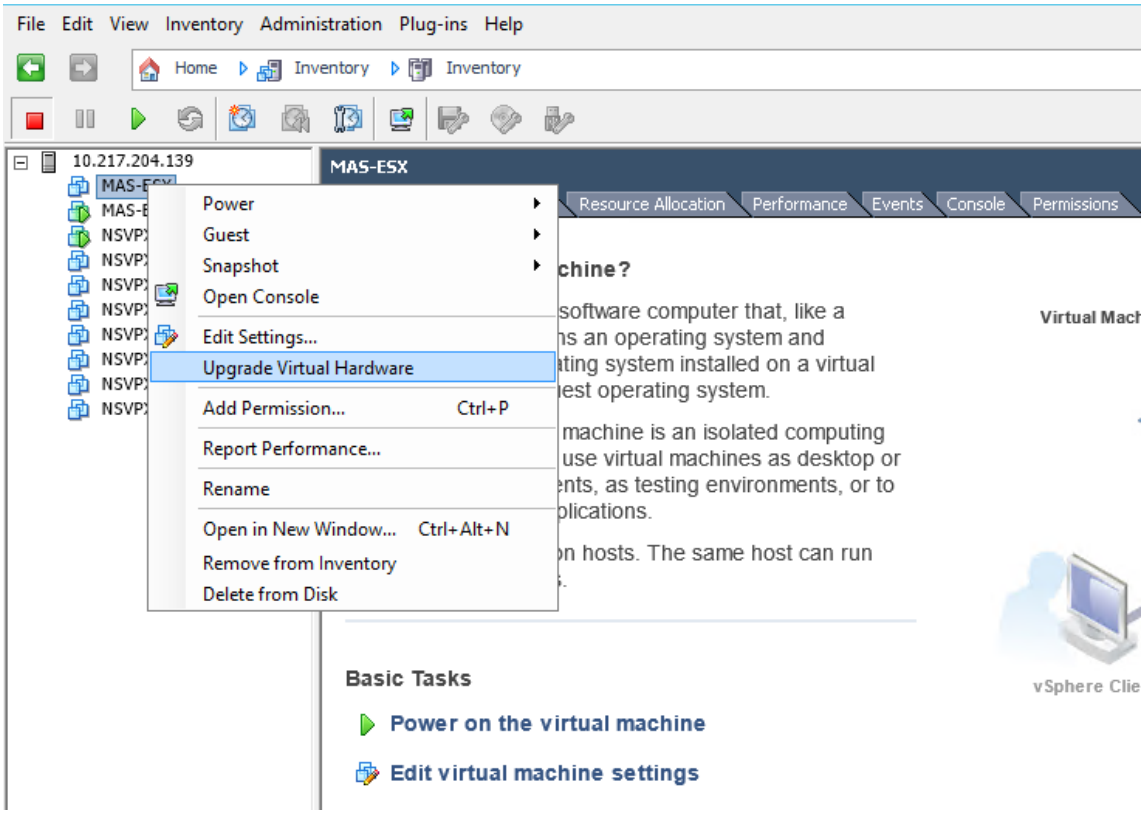
6. 在 “ **OVF** 模板详细信息” 页上，单击 “ 下一步”。
7. 键入 Citrix ADM 虚拟设备的名称，然后单击 下一步。
8. 指定 “Disk Format”（磁盘格式）：选择”Thin provisioned format”（瘦置备格式）或 “Thick provisioned format”（密集置备格式）。

   > 注意
   >
   > Citrix 建议您选择 “ 粗置备格式”。

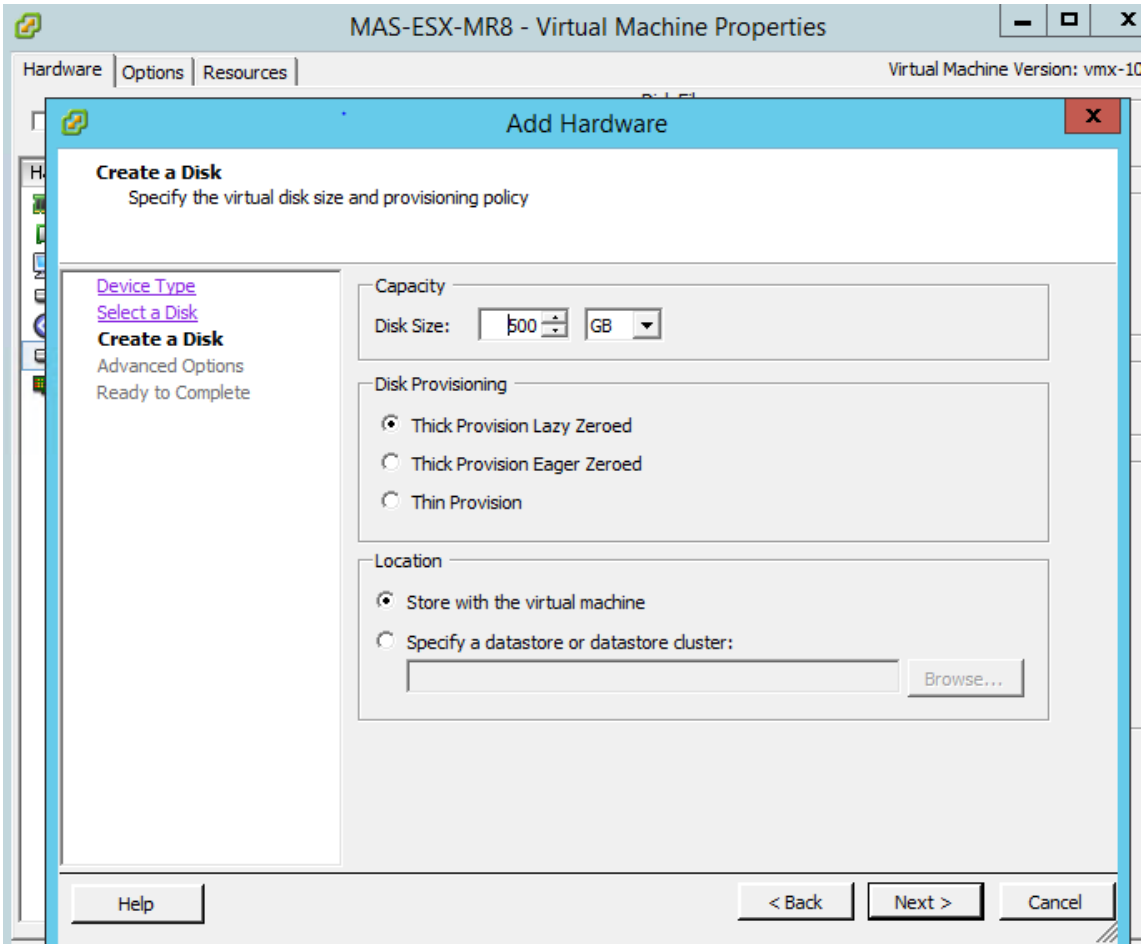
9. 单击 “ 完成” 开始安装过程。



10. 现在，您可以启动 Citrix ADM 虚拟设备。
11. 在导航窗格中，选择您安装的虚拟设备。在 清单菜单中，右键单击 虚拟机，然后单击 升级虚拟硬件。在 “ 确认虚拟机” 对话框中，单击 “ 是”。

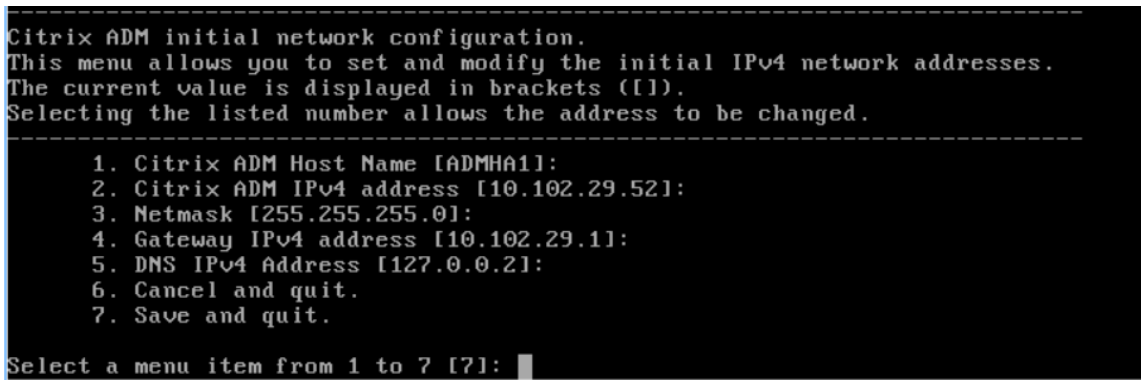


12. 在 清单菜单中，单击 虚拟机，然后单击 编辑设置。
13. 在 “ 虚拟机属性” 对话框中的 “ 硬件” 选项卡上，单击 “ 内存”，然后在右窗格中将内 存大小指定为 32 GB。
14. 单击 **CPU**，然后在右窗格中，将 CPU 指定为 8。单击确定。
15. 根据您的要求添加额外的磁盘。



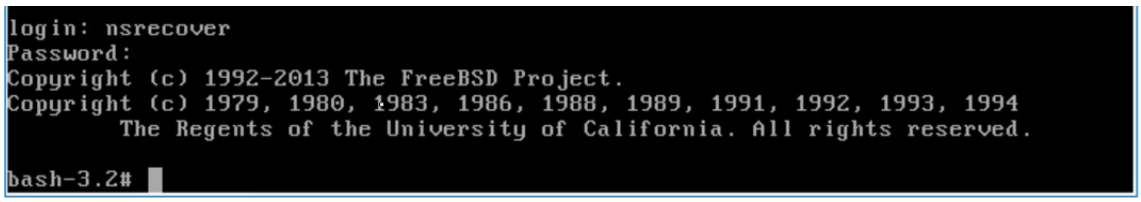
16. 在导航窗格中，选择您安装的虚拟设备。在 清单菜单中，单击 虚拟机，单击 电源，然后单击 打开电源。

17. 单击 控制台选项卡以显示 Citrix ADM 初始网络配置选项。



18. 指定所需的 IP 地址后，保存配置设置。

19. 出现提示时，使用 ns 恢复/nsroot 凭据登录。

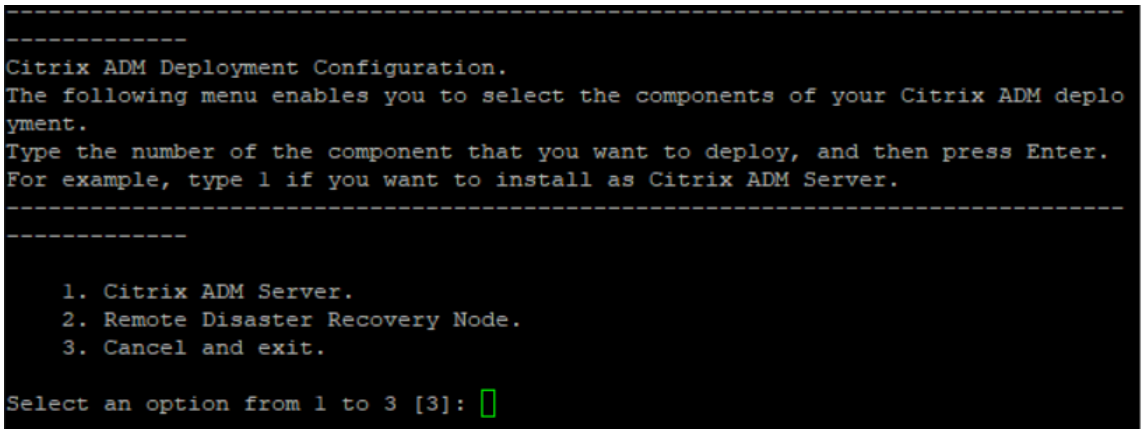


> 注意
>
> 登录后，如果要更新初始网络配置，请键入 networkconfig、更新配置并保存配置。

20. 通过在 shell 提示符下键入命令来运行部署脚本：

```
deployment_type.py
<!--NeedCopy-->
```

21. 选择作为 **Citrix ADM** 服务器的部署类型。如果不选择任何选项，默认情况下，它部署为服务器。



22. 键入是将 Citrix ADM 部署为独立部署。
23. 键入 “是” 以重新启动 Citrix ADM 服务器。

> 注意
>
> 安装 Citrix ADM 后，可以稍后更新初始配置设置。

验证

安装服务器后，您可以通过在浏览器中键入 Citrix ADM 服务器的 IP 地址来访问 GUI。用于登录服务器的默认管理员凭据是 nsroot/nsroot。

浏览器将显示 Citrix ADM 配置实用程序。

> 注意：在 VMware ESXi 上部署
>
> 时，Citrix ADM 可能需要 30 分钟或更长时间才能启动。

库贝内特斯群集上的 **Citrix ADM**

April 23, 2021

在 Kubernetes 群集上安装 Citrix ADM 虚拟设备之前，请阅读先决条件部分。

必备条件

在安装 ADM 之前，请确保满足以下先决条件。

库贝内特斯群集

- Kubernetes 群集必须是以下版本或更高版本：
  - 服务器版本 1.13
  - 客户端版本 1.13

  键入命令 `kubectl version` 以检查版本。
- 群集上安装的 Helm 应用程序必须是以下版本或更高版本。
  - 服务器版本 2.12.1
  - 客户端版本 2.12.0

  使用命 `helm version` 令检查版本。
- Kubernetes 集群 CNI（容器网络接口）必须是印花语版本 v3.1.3 或更高版本。
- 群集中的所有从属节点都必须在其上安装 NFS 客户端。这是因为 ADM 应用程序保留在网络文件服务器上装载的卷上的数据和配置。要在基于 UbuntuU 的下属机构上安装 NFS 客户端，请键入以下命令：

```
apt-get update
apt install nfs-common
```

- ADM 应用程序需要整个群集中的 32 GB 内存和 8 个 vCPU 以及 NFS 上的 120 GB 空间。

NFS 份额

ADM 应用程序需要持久卷来存储配置、证书、映像等数据。为此，ADM 需要 NFS 安装。应用程序需要共享网络装载中的两个文件夹：

- 一个用于存储证书、图像等文件

- 另一个用于数据库

> 注意
>
> 建议使用带 SSD 的 NFS。

这两个文件夹可以不同或相同。这两个文件夹都必须具有 777 权限。第一个文件夹必须至少具有 10 GB 的速度。第二个文件夹的大小取决于数据库中需要持久的数据量。最小大小为 100 GB。
对于生产环境，我们建议您使用生产级 NFS 解决方案。

Citrix ADC 设备

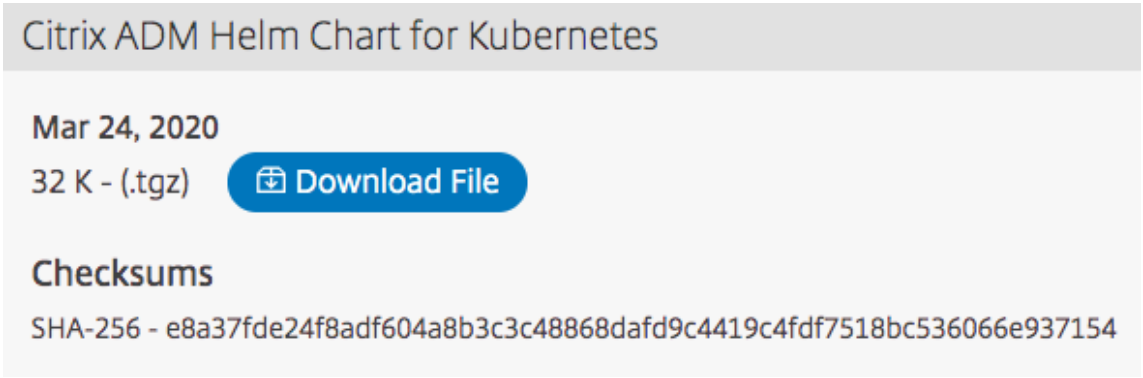
需要将 Citrix ADC 装置作为入口设备。ADC 在 Kubernetes
群集之外提供所需的应用程序服务。Citrix ADC 装置必须位于 Kubernetes 群集之外，并且工作节点必须可以从 ADC 访问。执行以下步骤:

- 在 ADC 上配置 SNIP。ADC 使用此 SNIP 访问 Kubernetes 群集的辅助节点。
- 确定要用作虚拟服务器 IP 地址的空闲 IP 地址，以使所需的应用程序服务在 Kubernetes 群集之外可用。

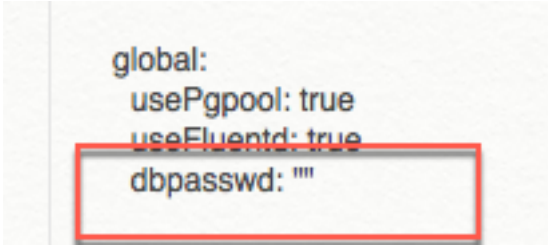
在库贝内特斯群集上安装 **ADM**

请按照以下步骤在 Kubernetes 集群上安装 ADM 设备:

1. 转到 Citrix 下载站点 并下载适用于 Kubernetes 的 Citrix ADM Helm 图表的文件。



2. 将下载的 Helm Chart Tarball 提取到 Kubernetes 集群主节点的 /var 目录中。
3. 打开目 `values.yaml` 录下的 `/var/citrixadm` 文件。
4. 在文件的 `dbpasswd` 字段中输入数据库的密码。



5. 更改以下值。ADM 应用程序使用这些值来配置 Citrix ADC 装置，以便将服务暴露于外部世界：

   - `ingressIP`：在 Citrix ADC 中配置的用于访问应用程序的虚拟 IP。
   - `applicationID`：用于将入口配置与 Citrix ADC 设备上的其余配置区分开来的唯一 ID。
   - `ingressADCIP`：Citrix ADC IP 地址 (NSIP)，用作 ADM 应用程序的入口。
   - `ingressADCUsername`：用于访问 Citrix ADC 装置的用户名。此用户必须具有写入权限。
   - `ingressADCPassword`：用户名的密码。

```
# ingressIP is the Virtual IP configured in the Citrix ADC for accessing the application
ingressIP: "xx.xx.xx.xx"

# coreDumpFilePath is the directory on slave nodes of the cluster which will be used to store core dumps files in case
application runs into faulty state
# this setting is optional
# Admin needs to create this directory on each of the slave nodes and then run the command: "echo <coreDumpFilePath_value>/
core.%h.%e.%p > /proc/sys/kernel/core_pattern"
coreDumpFilePath: "/var/mps/cores"

# applicationID is the identifier for ingress configuration
applicationID: "citrixadm"

# ingressADCIP is the NSIP of the northbound ADC used to expose the ADM application to the outside world
ingressADCIP: "xx.xx.xx.xx"

# ingressADCUsername is the username of the northbound ADC
ingressADCUsername: "nsroot"

# ingressADCUsername is the password for above username
ingressADCPassword: "nsroot"
```

6. 在 存储部分中更改以下值。这些值指定存储 ADM 应用程序所需的文件所需的持久性。

   - `nfsServer`：NFS 服务器的主机名或 IP 地址
   - `path`：挂载用于存储应用程序文件的文件夹的路径。
   - `size`：至少 10 GB。

   > 注意
   >
   > 此值的单位是 Gi。例如，10Gi 值，20Gi 值。

7. 转到下的 存储部分 `pg-datastore` 并更改以下值。这些值指定用于创建数据库的持久性。

   - `nsfServer`：NFS 服务器的主机名或 IP 地址。
   - `size`：装载用于数据存储的文件夹的路径。
   - `path`：至少 100 GB。

   > 注意
   >
   > 此值的单位是 Gi。例如，对于 100 千兆位数和 200 千兆位数。

8. 转到主节点中的 /var/Citrix 目录，然后运行以下命令来安装 ADM 应用程序：
   `helm install -n citrixadm --namespace <name> ./citrixadm`

   > 注意
   >
   > helm 3.x 版不支持此 helm 命令。

   此命令还会在集群中安装所需的 pod。命名空间参数是可选的。如果未提供命名空间，Helm 将在默认命名空间中安装 ADM。为了便于管理，请在单独的命名空间下安装 ADM。

9. 打开浏览器，然后键入 `http://< virtual server IP address >` 并使用 `nsroot/nsroot` 作为凭据登录 ADM。用于安全访问类型 `https://< virtual server IP address >`。

> 注意
>
> 在部署期间，ADM 应用程序会在数据存储中创建表，这可能需要一段时间。根据 Kubernetes 分配给 ADM 应用程序的各种容器的资源，服务可能需要 5-15 分钟才能启动。

Linux KVM 服务器上的 Citrix ADM

April 23, 2021

可在其上配置 Citrix Application Delivery Management (ADM) 的虚拟化平台包括 Linux-KVM。

在 Linux-KVM 上安装 Citrix ADM 之前，请确保系统具有硬件虚拟化扩展，并验证 CPU 虚拟化扩展是否可用。验证虚拟机管理程序上 `virsh`（用于管理虚拟机的命令行工具）是否可用。

使用您的管理员凭据登录到 Citrix.com 网站，访问最新的 Citrix ADM 安装文件，然后将其下载到您的计算机上。然后，在您的 Linux-KVM 平台上安装 Citrix ADM，并针对您的网络进行配置。

必备条件

在安装 Citrix ADM 虚拟设备之前，请验证 Linux-KVM 版本 3.6.11-4 及更高版本安装在符合最低要求的硬件上。

硬件要求

组件	要求
CPU	具有英特尔 VT-X 处理器中包含的硬件虚拟化功能的 64 位 x86 处理器。至少提供 2 个 CPU 内核以托管 Linux-KVM。注意：要测试 CPU 是否支持 Linux 主机，请在主机 Linux shell 提示符下输入以下命令：*. `egrep'^flags.\* ( vmx | svm )'/proc/cpuinfo`* 如果该扩展的 BIOS 设置被禁用，则必须在 BIOS 中启用它们。没有关于处理器速度的具体建议，但速度越高，Citrix ADM 的性能就越好。
内存 (RAM)	最低 4 GB，用于主机 Linux 内核。添加 VM 所需的其他内存。
硬盘	计算主机 Linux 内核和 VM 的空间要求。单个 Citrix ADM 虚拟机需要 120 GB 的磁盘空间。

> 注意
>
> 考虑到主机上没有其他虚拟机运行，指定的内存和硬盘要求用于在 OpenStack 平台上部署 Citrix ADM。OpenStack 的硬件要求取决于其上运行的虚拟机数量。

软件要求

Citrix 建议较新的内核，例如 64 位版本的 3.6.11-4 内核或更高版本。

网络要求

Citrix ADM 仅支持一个 Virtio 准虚拟化网络接口。确保将此接口连接到 Linux-KVM 主机的管理网络，以便 Citrix ADM 和 Linux-KVM 可以通信。

下载 **Citrix ADM** 安装文件

要从 www.citrix.com 下载 Citrix ADM 安装程序文件，请执行以下操作：

1. 打开 Web 浏览器并 www.citrix.com.cn 在地址栏中键入。
2. 将鼠标悬停 在 **“**登录” 选项上，然后单击 “M **y Account**”，输入您的 Citrix 凭据，然后再次单击 “ 登录”。
3. 导航至 “ 下载” 部分。
4. 从 “下 载” 列表中，选择 **Citrix Application Delivery Management**。
5. 在 **Citrix Application Delivery Management** 页面上，选择发行版。例如，选择 **13.0** 版。
6. 单击 “ 产品软件” 将其展开，然后单击最新版本。例如，选择 **NetScaler MAS** 版本（功能阶段）**13.0** 版本 **36.27**。

   将显示选定的构建页面。
7. 在 “ 跳转到下载” 列表中，选择 适用于 **KVM** 的 **NetScaler MAS** 映像，**13.0** 生成 **xx.xx**
8. 单击 下载文件，接受最终用户许可协议，然后将压缩映像文件下载到本地计算机上的任何文件夹。

在 **Linux-KVM** 上安装 **Citrix Application Delivery Management**

1. 使用 SSH，登录 KVM 主机。
2. 在 CLI 提示窗口中，通过使用任何一个文件传输程序，将映像复制到服务器上的一个文件夹中。
3. 导航到保存下载的映像的目录。
4. 在命令行上执行以下操作：

   a) 列出目录中的文件以确认映像文件是否存在。

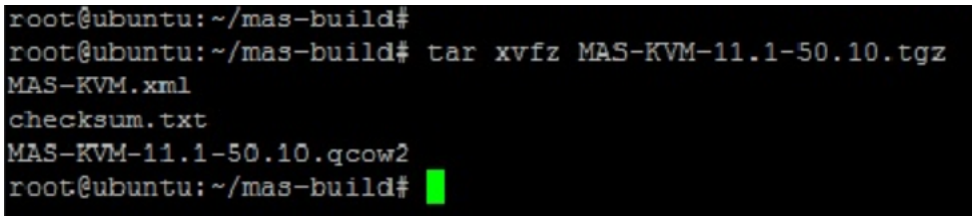
b) 使用 tar 命令可取消 Citrix Application Delivery Management 映像文件。解压缩的包中包含以下组件：

i. 指定 Citrix ADM 属性的域 XML 文件

ii. 指定域磁盘映像的校验和的文本文件

iii. 域磁盘映像

```
tar -xvfz MAS-KVM.tgz
MAS-KVM.xml
MAS-KVM.qcow2
checksum.txt
<!--NeedCopy-->
```



iv. 创建 MAS-KVM.xml 副本，保存为 MAS1-KVM.xml，作为备份选项。使用 vi 编辑器打开 MAS1-KVM.xml 文件。

v. 在 MAS1-KVM.xml 中编辑以下网络连接属性：

A. `name` -指定名称。

B. `mac` -指定 MAC 地址。

C. `source file` -指定绝对磁盘映像源路径。文件路径必须为绝对路径。

> 注意
>
> 域名和 MAC 地址必须具有唯一性。

D. `mode` -指定模式。

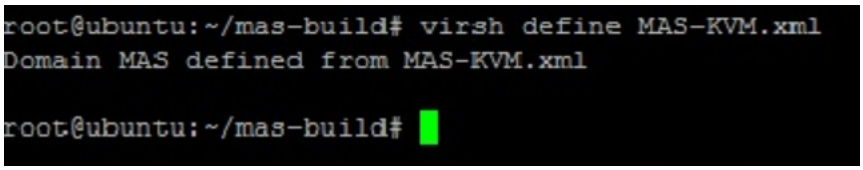
E. `model type` -设置为 VirTIO。

F. `source dev` -指定接口。

```
<name> MAS1-KVM</name>
<mac address='52:54:00:29:74:b3'/>
<source file='/var/ MAS-KVM.qcow2'/>
<source dev='eth0' mode='bridge'/>
<model type='virtio'/>
<!--NeedCopy-->
```

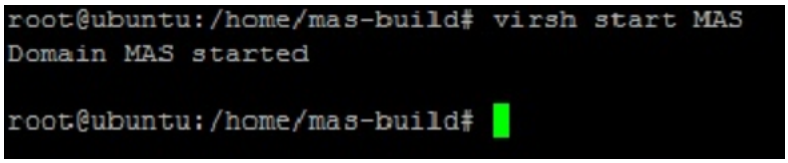
vi. 使用以下命令在 MAS1-KVM.xml 文件中定义 VM 属性：`virsh define \<FileName\>.xml`


```
virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml
<!--NeedCopy-->
```



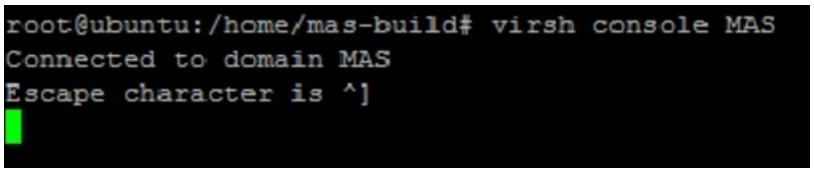
vii. 通过输入以下命令启动 Citrix ADM: `virsh start \[\<DomainName\> | \<DomainUUID\>\]`

```
virsh start MAS
Domain MAS started
<!--NeedCopy-->
```



viii. 您可以使用以下命令连接到 Citrix ADM 虚拟机: `virsh console \<DomainName\>`

```
virsh console MAS
Connected to domain MAS
Escape character is ^]
<!--NeedCopy-->
```



配置 Citrix Application Delivery Management

> 注意
>
> 在有些 Linux KVM 主机上，如果 FreeBSD 来宾有多个 CPU，他们将无法正确重新启动。重新启动 Citrix ADM 虚拟设备时，Citrix ADM CLI 和 GUI 将变得无响应。有关详细信息，请参阅https://bugs.launchpad.net/qemu/+bug/1329956
>
> 要避免 Citrix ADM 虚拟设备重新启动时 Citrix ADM CLI 和 GUI 无响应，请关闭 KVM 主机上的所有虚拟机，然后在 KVM 主机上执行以下操作:
>
> 1. 使用以下命令删除 kvm_intel 模块:


```
rmmod kvm\\_intel
```

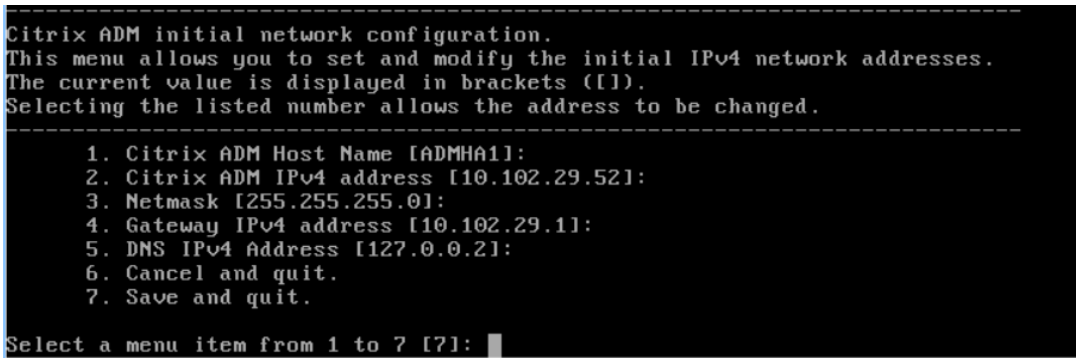
2. 使用以下命令禁用 **apicV** 并重新加载 kvm_intel 模块：
   `modprobe kvm\\_intel enable\\_apicv=N`
3. 在 KVM 主机上启动虚拟机。

安装 Citrix ADM 后，等待大约 10 分钟以使服务可用，然后登录 Citrix ADM。

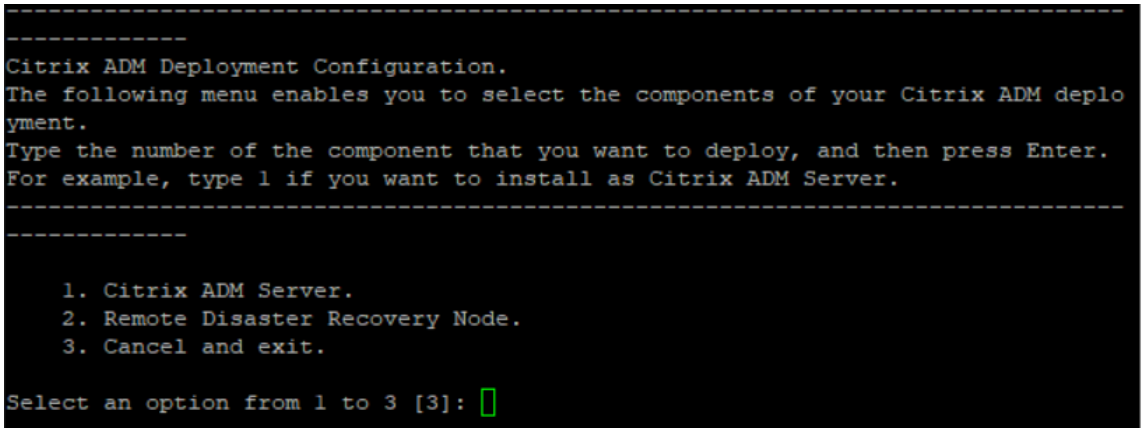
1. 在命令行上，使用默认的系统管理员凭据登录系统：
   - 用户名：`nsroot`
   - 密码: `nsroot`

   > 注意
   >
   > 首次登录后，更改管理密码。然后，配置 MAS 以在您的网络中运行。您可以从 Citrix ADM 用户界面更改密码。在 Citrix ADM 主页中，导航到 “ 系统” > “ 用户管理” > “用 户”。选择用户并单击 **Edit**（编辑），然后在 “Password”（密码）字段中更新密码。

2. 在提示符下键入：*shell*
3. 键入 网络配置以进入 Citrix ADM 初始网络配置菜单。配置管理 IP 地址。
4. 要完成 Citrix ADM 的初始网络配置，请按照提示操作。控制台显示 Citrix ADM 初始网络配置选项，用于设置 Citrix ADM 的以下参数。默认情况下，已填充主机名。
   a) 输入 **2** 以更新 Citrix ADM IPv4 地址-用于访问 Citrix ADM 的管理 IP 地址
   b) 输入 **3** 以更新与管理 IP 地址关联的子网掩码-子网掩码
   c) 输入 **4** 以更新 Gateway IPv4 地址 — Citrix ADM 管理 IP 地址子网的默认网关 IP 地址
   d) 输入 **7** 保存并退出-保存配置更改并退出系统。

5. 通过在 shell 提示符下键入命令来运行部署脚本：`deployment_type.py`
6. 在显示的部署屏幕中，选择作为 **Citrix ADM** 服务器的部署类型。



7. 键入 是将 Citrix ADM 部署为独立部署。
8. 键入 **“是”** 以重新启动 Citrix ADM 服务器。
9. Citrix ADM 服务器重新启动后，通过命令行或 GUI 使用默认管理员凭据作为 nsroot/nsroot 登录到 Citrix ADM。

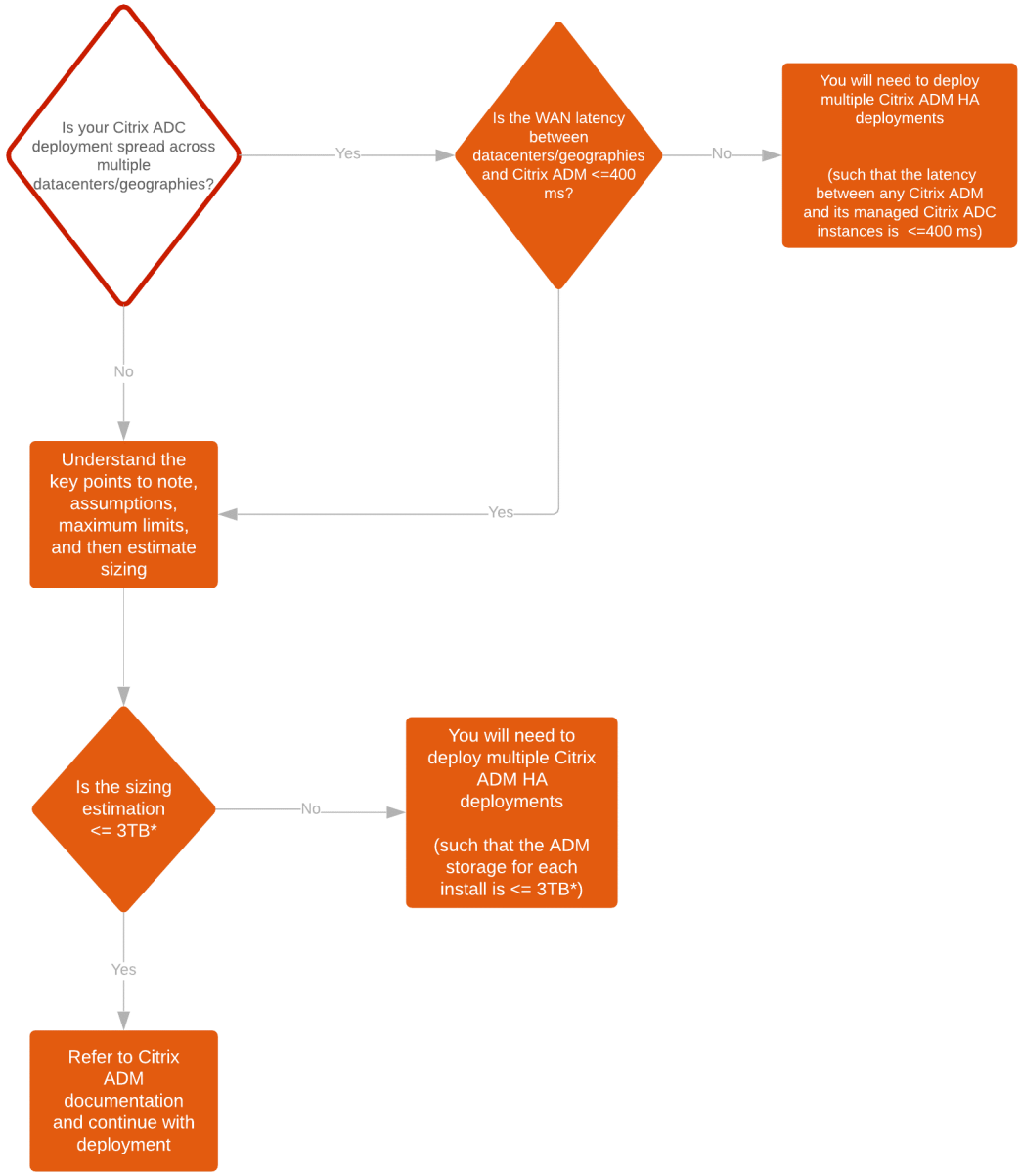
   您可以稍后通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问 Citrix ADM。登录到服务器的默认管理员凭据是 *nsroot/nsroot*。

配置高可用性部署

April 23, 2021

高可用性 (HA) 是指始终可供用户使用的系统，而不会中断服务。高可用性设置在系统停机、网络或应用程序故障期间至关重要，而且是任何企业的关键要求。以相同配置的主动-被动模式对两个 Citrix ADM 节点进行高可用性部署，可实现不间断的操作。

部署方案



> 注意
>
> 单个 Citrix ADM HA 部署的验证最大存储限制为 3 TB。有关详细信息，请参阅 部署指南。
>
> 重要
>
> 要使用 **HTTPS** 访问 **Citrix ADM 12.1** 版本 **48.18** 或更高版本，请执行以下操作：
>
> 如果您已将 Citrix ADC 实例配置为在高可用性模式下平衡 Citrix ADM 的负载，请首先删除 Citrix ADC 实例。然后，配置浮动 IP 地址以在高可用性模式下访问 Citrix ADM。

以下是 Citrix ADM 中高可用性部署的好处：

- 一种改进的机制，用于监视主节点和辅助节点之间的检测信号。
- 提供数据库的物理流复制，而不是逻辑双向复制。
- 能够在主节点上配置浮动 IP 地址，以免需要单独的 Citrix ADC 负载均衡器。
- 可使用浮动 IP 地址轻松访问 Citrix ADM 用户界面。
- 仅在主节点上提供 Citrix ADM 用户界面。通过使用主节点，您可以消除访问辅助节点和更改辅助节点的风险。
- 配置浮动 IP 地址可处理故障转移情况，不需要重新配置实例。
- 提供内置检测和处理大脑分裂情况的能力。

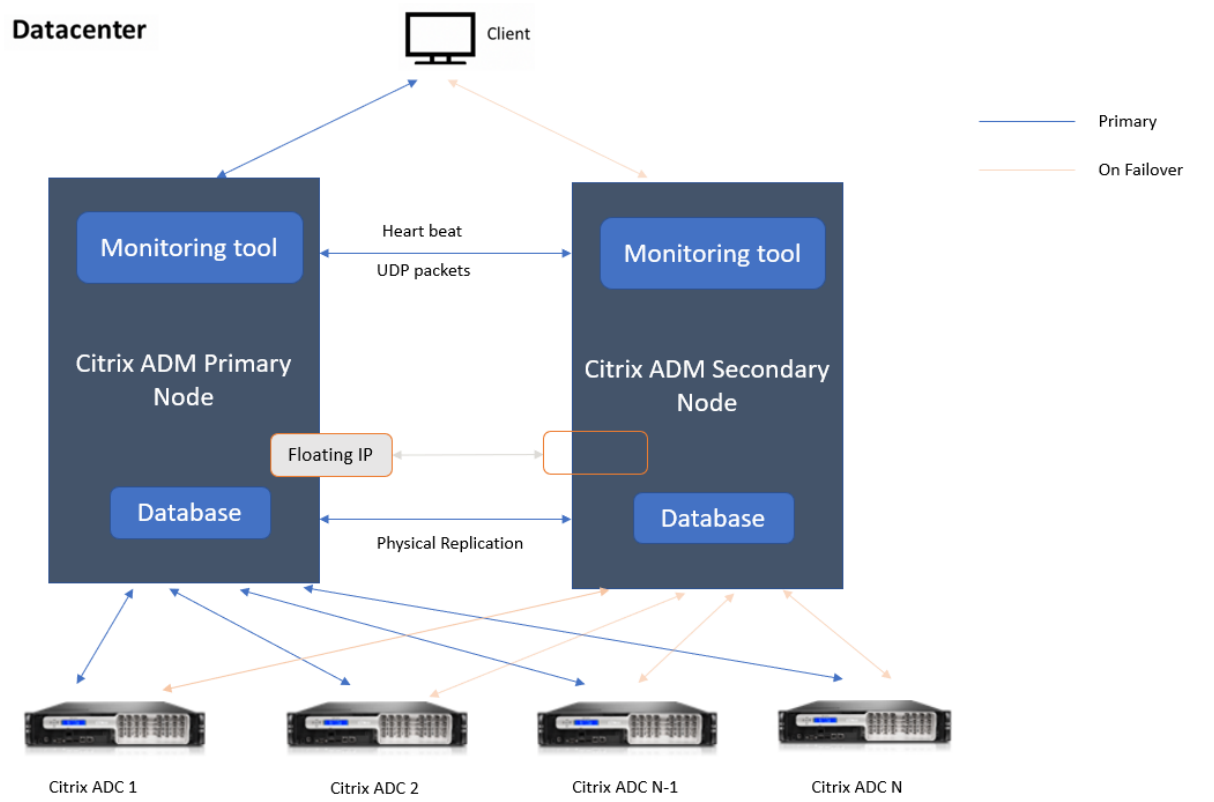
下表介绍了高可用性部署中使用的术语。

条款	说明
主节点	在高可用性部署中注册的第一个节点。
辅助节点	在高可用性部署中注册的第二个节点。
检测信号	在高可用性设置中，用于在主节点和辅助节点之间交换消息的机制。这些消息决定每个节点上应用程序的状态和运行状况。
浮动 IP 地址	浮动 IP 是一种 IP 地址，可以立即从一个节点移动到同一子网中的另一个节点。在内部，它被设置为主节点的网络接口上的别名。如果存在故障转移，则浮动 IP 地址将从旧的主地址无缝移动到新的主地址。它在高可用性设置中非常有用，因为它允许客户端使用单个 IP 地址与高可用性节点进行通信。

> 注意：有关端口和协议详细信息
>
> 的详细信息，请参阅 [端口 ()]。

高可用性体系结构的组件

下图显示了在高可用性模式下部署的两个 Citrix ADM 节点的体系结构。



在高可用性部署中，一个 Citrix ADM 节点配置为主节点 (MAS 1)，另一个配置为辅助节点 (MAS 2)。如果主节点由于任何原因导致故障，辅助节点将接管作为新的主节点。

监控工具

监视工具是一个内部过程，用于监视、警报和处理故障切换情况。该工具处于活动状态，并在每个节点上以高可用性运行。它负责启动子系统、在两个节点上启动数据库、确定主节点或辅助节点是否存在故障转移等。

主节点

主节点接受连接并管理实例。所有进程（如 AppFlow、SNMP、日志流、系统日志等）都由主节点管理。主节点上提供了 Citrix ADM 用户界面访问权限。浮动 IP 地址在主节点上配置。

辅助节点

辅助节点侦听从主节点发送的检测信号消息。辅助节点上的数据库仅处于只读副本模式。辅助节点中没有任何进程处于活动状态，并且无法在辅助节点上访问 Citrix ADM 用户界面。

物理流复制

主节点和辅助节点通过检测信号机制进行同步。使用数据库的物理流复制，辅助节点以只读副本模式启动。辅助节点侦听从主节点收到的检测信号消息。如果辅助节点在 180 秒的时间段内未收到任何检测信号，则该主节点将被视为关闭。然后，辅助节点接管作为主节点。

心跳消息

检测信号消息是在主节点和辅助节点之间发送和接收的用户数据报数据包 (UDP)。它监视 Citrix ADM 和数据库的所有子系统，以交换有关节点状态、运行状况、进程等的信息。信息每秒在高可用性节点之间共享一次。如果发生故障转移或高可用性状态中断，通知将作为警报发送给管理员。

浮动 **IP** 地址

浮动 IP 地址与高可用性设置中的主节点相关联。它是指定给主节点 IP 地址的别名，客户端可以使用该别名连接到主节点中的 Citrix ADM。由于浮动 IP 地址是在主节点上配置的，因此在发生故障转移时不需要重新配置实例。实例重新连接到相同的 IP 地址以达到新的主 IP 地址。

需要注意的要点

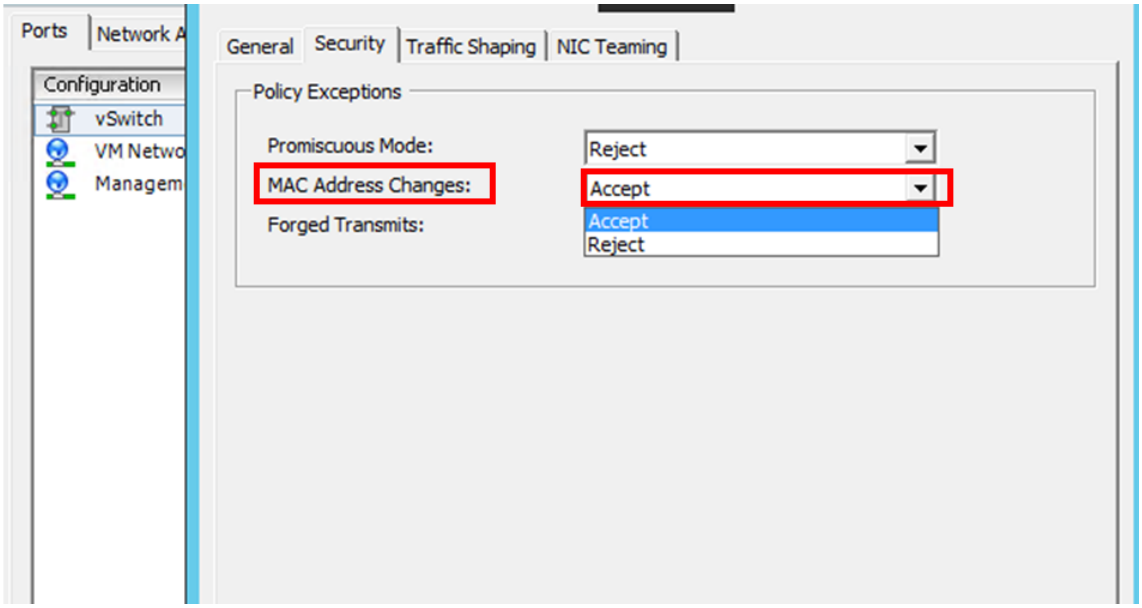
- 在高可用性设置中，两个 Citrix ADM 节点都以主动-被动模式部署。它们必须位于使用相同的软件版本和版本的同一子网上，并且具有相同的配置。
- 浮动 IP 地址：
  - 在主节点上配置浮动 IP 地址。
  - 如果存在故障转移，则无需重新配置实例。
  - 您可以通过使用主节点 IP 或浮动 IP 地址从用户界面访问高可用性节点。

    > 注意
    >
    > Citrix 建议您使用浮动 IP 地址访问用户界面。
- 数据库：
  - 在高可用性设置中，所有配置文件都会在一分钟的间隔内自动从主节点同步到辅助节点。
  - 通过数据库的物理复制即时执行数据库同步。
  - 辅助节点上的数据库处于只读副本模式。
- Citrix ADM 升级：
  - 内部进程隐式地从早期版本升级 Citrix ADM。

> 注意
>
> 升级成功后，您必须配置浮动 IP 地址。

- UDP 默认端口 5005 在节点上都可用于发送检测信号和接收消息。
- MAC 地址
  Hypervisor 中的“MAC 地址更改”选项的设置会影响虚拟机接收的流量。允许在虚拟交换机上启用 MAC 地址更改，以便浮动 IP 地址在故障转移后无缝移动到新的主节点。
  例如，在 VMware ESXi 上的高可用性部署 Citrix ADM 时，请确保接受对 MAC 地址的更改。ESXi 现在允许请求将活动 MAC 地址更改为初始 MAC 地址以外的其他地址。

  > 注意：
  >
  > 对于部署在 ESXI 版本 6.7 上的 Citrix ADM，您可以将 **MAC** 地址更改选项设置为也 拒绝。故障转移后，无论 **MAC** 地址更改设置如何，流量都会无缝流动到新的主节点。因此，接受对 MAC 地址的更改不是强制性的。
  >
  > 如果在低于 6.7 的 ESXI 版本上部署了 Citrix ADM，请确保将 **MAC** 地址更改选项设置为仅 接受。



必备条件

在为 Citrix ADM 节点设置高可用性之前，请注意以下先决条件：

- Citrix ADM 高可用性部署由 Citrix ADM 版本 12.0 版本 51.24 支持。
- 从 Citrix 下载站点下载 Citrix Application Delivery Management 映像文件 (.xva)：https://www.citrix.com/downloads/

Citrix 建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了虚拟计算资源的最低要求：

组件	要求
RAM	**32 GB**
虚拟 CPU	**8** 个 **CPU**
存储空间	Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。如果您的 Citrix ADM 存储需求超过 120 GB，则必须附加一个额外的磁盘。注意您只能添加一个附加磁盘。Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。有关详细信息，请参阅 如何将附加磁盘连接到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序	版本
Citrix Hypervisor	6.2 和 6.5
VMware ESXi	5.5 和 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	乌班图和费多拉

在高可用性模式下设置 **Citrix ADM**

1. 注册并部署第一台服务器（主节点）。
2. 注册并部署第二个服务器（辅助节点）。
3. 部署主节点和辅助节点以实现高可用性设置。

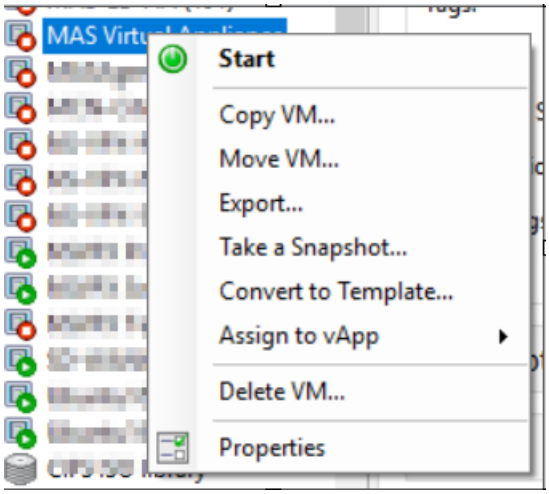
注册和部署第一台服务器（主节点）

注册第一个节点：

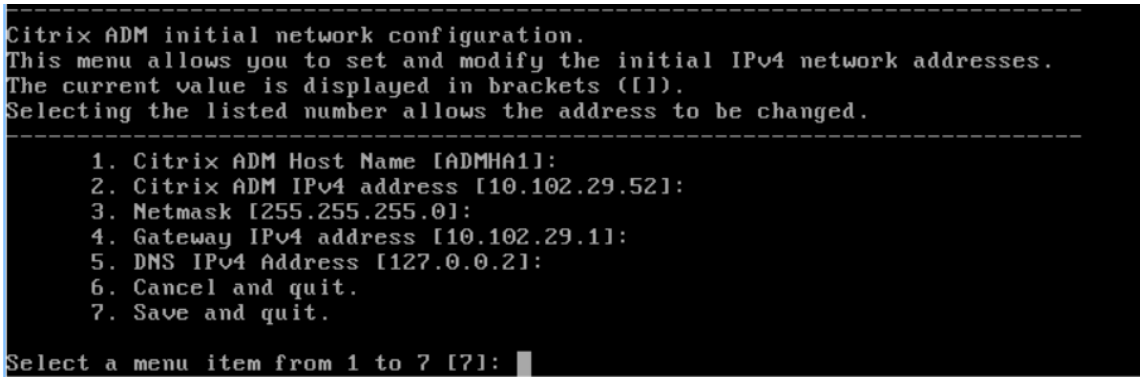
1. 使用从 Citrix 下载站点下载的.xva 映像文件，并将其导入到 Hypervisor 中。

   > ** 注
   >
   > 意 **.xva 图像文件可能需要几分钟才能导入并开始。您可以在屏幕底部看到状态。
   >
   >
   >

2. 导入成功后，右键单击并单击 “ 开始”。



3. 在 控制台选项卡中，使用初始网络配置配置 Citrix ADM。



4. 初始网络配置完成后，系统将提示登录。使用以下凭据登录 — *ns* 恢复/*nsroot*。

> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`、更新配置并保存配置。

5. 要部署主节点，请输入 **/mps/**部署类型**.py**。此时将显示 Citrix ADM 部署配置菜单。

6. 选择 **1** 将 Citrix ADM 服务器注册为主节点。


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

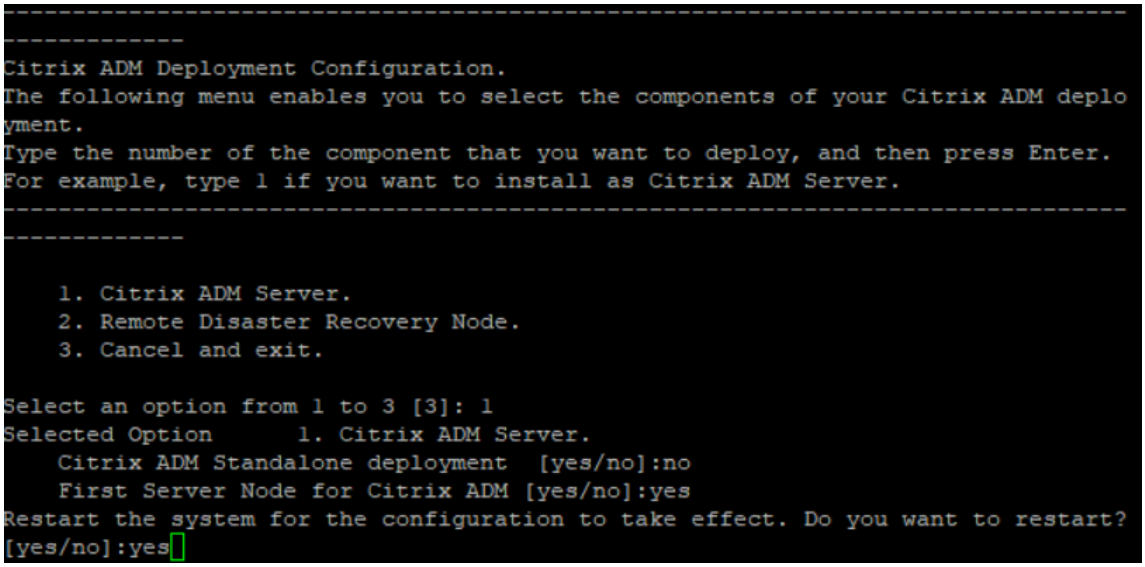
7. 控制台会提示您选择 Citrix ADM 独立部署。输入否以确认部署为高可用性。

```
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

8. 控制台提示您选择第一个服务器节点。输入 **Yes** 以确认节点为第一个节点。

```
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
```

9. 控制台提示您重新启动系统。输入 **“是”** 以重新启动。



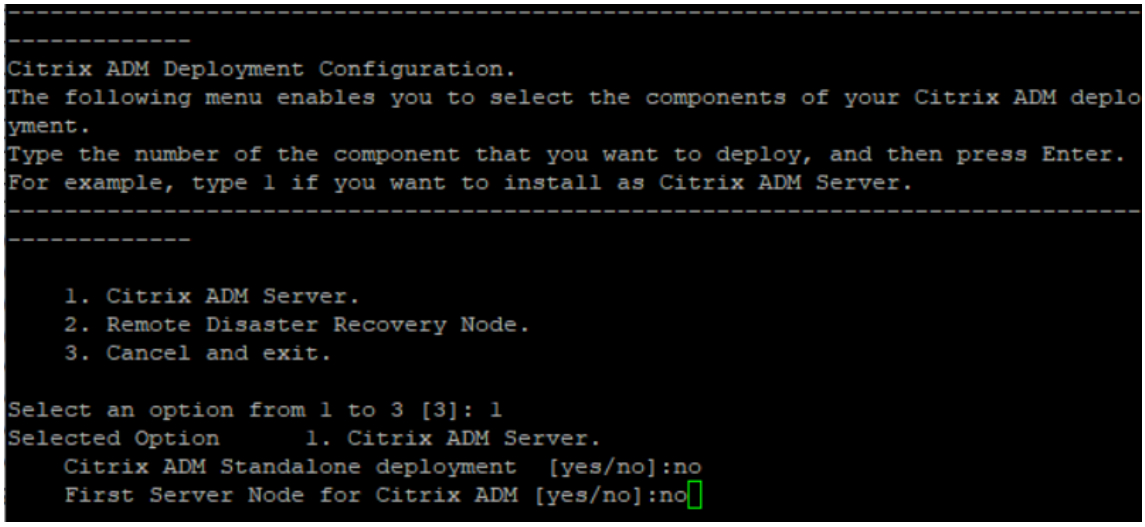
系统将重新启动，并在 Citrix ADM 用户界面中显示为主节点。

注册和部署第二个服务器（辅助节点）

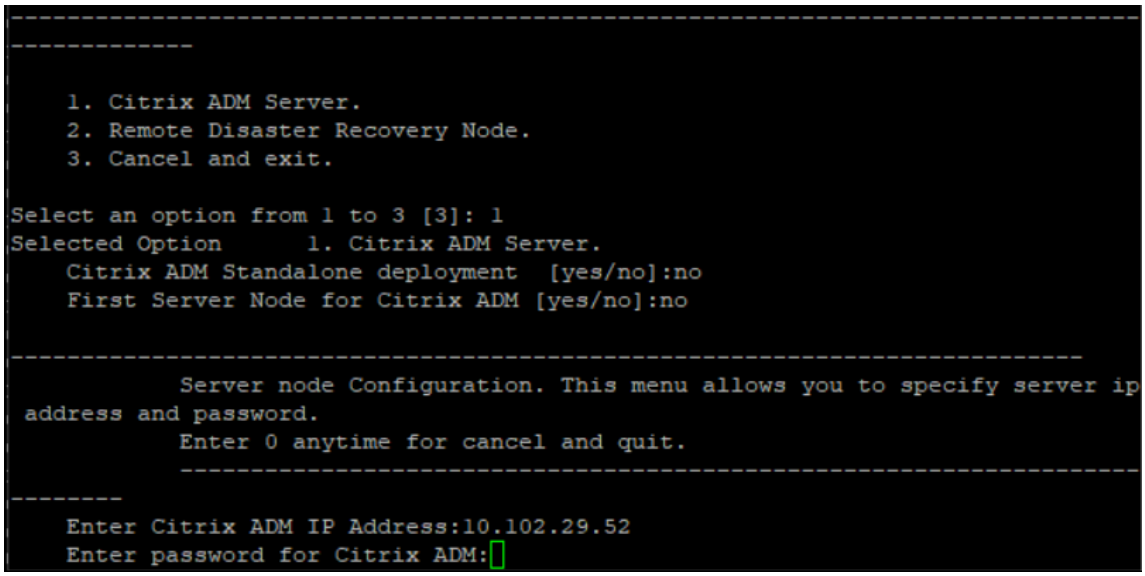
1. 使用从 Citrix 下载站点下载的 **.xva** 映像文件，并将其导入到 Hypervisor 中。
2. 在“ 控制台”选项卡中，使用下图所示的初始网络配置配置 Citrix ADM。
3. 初始网络配置完成后，系统将提示登录。使用以下凭据登录 — *ns* 恢复/*nsroot*。

   > 注意
   >
   > 登录后，如果要更新初始网络配置，请键入 `networkconfig`、更新配置并保存配置。

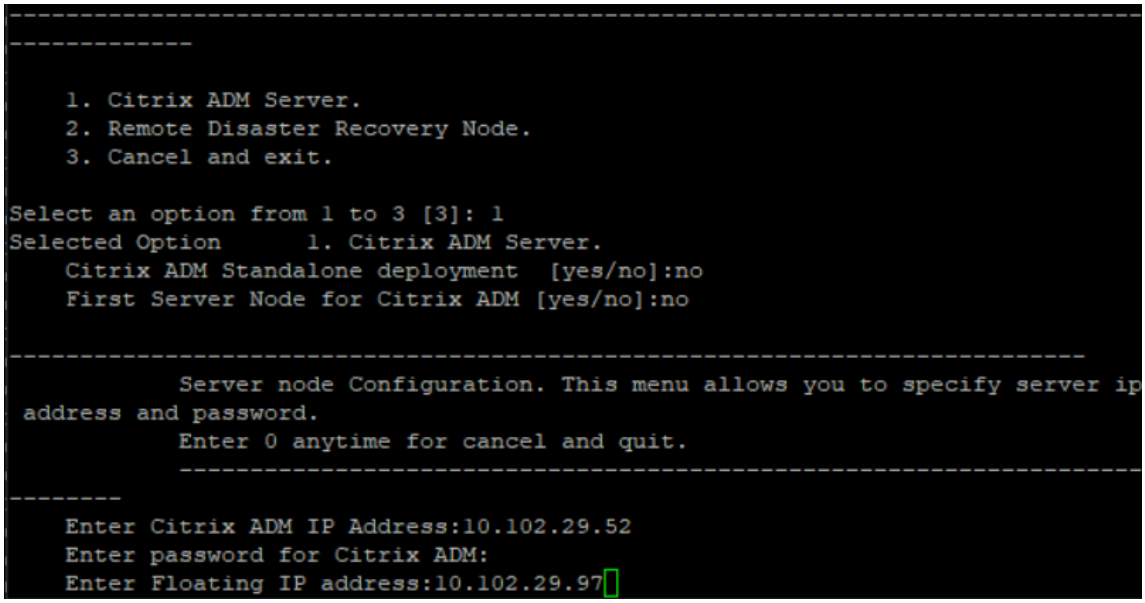
4. 要部署辅助节点，请输入 **/mps/**部署类型**.py**。此时将显示 Citrix ADM 部署配置菜单。
5. 选择 **1** 将 Citrix ADM 服务器注册为辅助节点。
6. 控制台会提示您选择 Citrix ADM 作为独立部署。输入否以确认部署为高可用性。
7. 控制台提示您选择第一个服务器节点。输入否以确认节点为第二台服务器。



8. 控制台会提示您输入主节点的 IP 地址和密码。



9. 控制台提示您输入浮动 IP 地址。



10. 控制台提示您重新启动系统。输入 **“是”** 以重新启动。

> 注意
>
> - 浮动 IP 地址对于节点的高可用性部署是必需的。
> - 如果配置中存在任何问题，系统将显示错误消息。
> - 系统重新启动，配置需要几分钟时间才能生效。

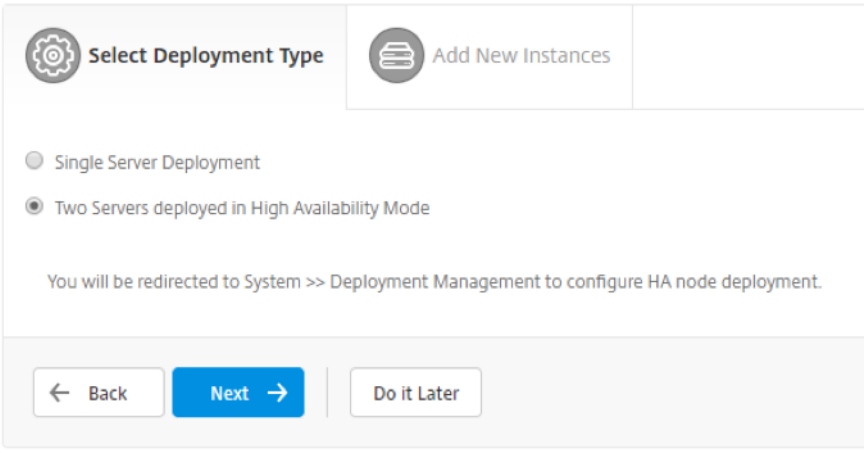
将主节点和辅助节点部署为高可用性对

注册完成后，Citrix ADM 用户界面上将显示主节点和辅助节点。将这些节点部署到高可用性对中。

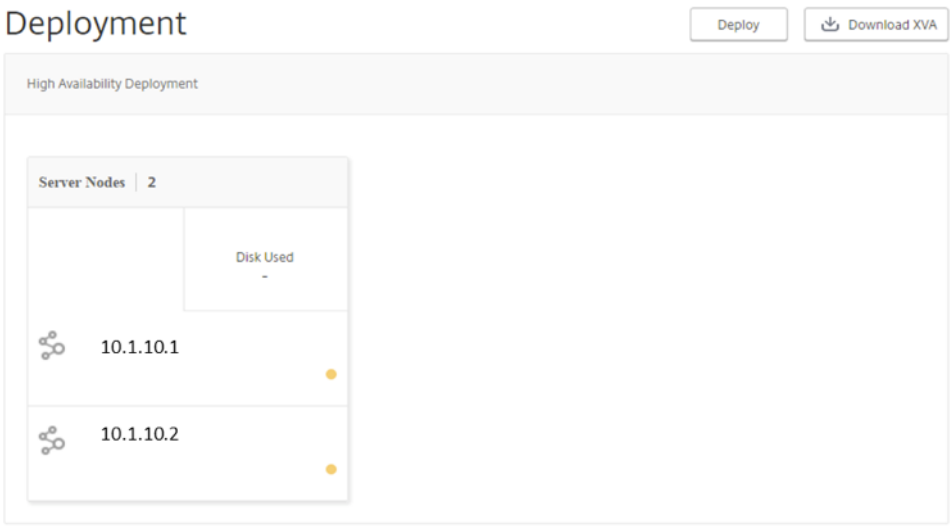
> 注意
>
> - 在将节点部署到高可用性对中之前，请确保在初始网络配置后重新启动后完成辅助节点。
> - 完成高可用性部署后，使用浮动 IP 地址访问 Citrix ADM 用户界面。

要将节点部署为高可用性对，请执行以下操作：

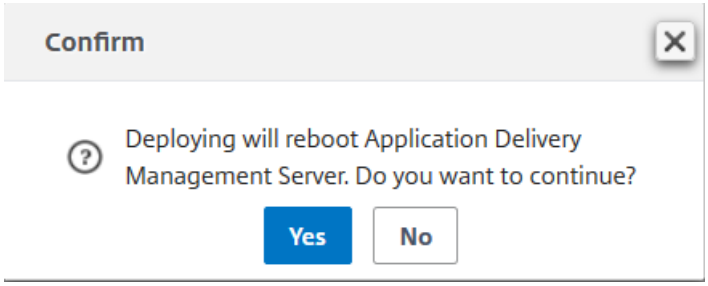
1. 打开 Web 浏览器并输入第一个 Citrix ADM 服务器节点的 IP 地址。
2. 在用户名和密码字段中，输入管理员凭据。
3. 单击主页中的 “ 开始”。
4. 选择部署类型作为在高可用性模式下部署的两台服务器，然后单击下一步。



5. 在“部署”页上，单击“部署”。



6. 将显示一条确认消息。单击是。



Citrix ADM 将重新启动，配置需要大约 10 分钟才能生效。

> 注意
>
> 您现在可以开始使用浮动 IP 地址。

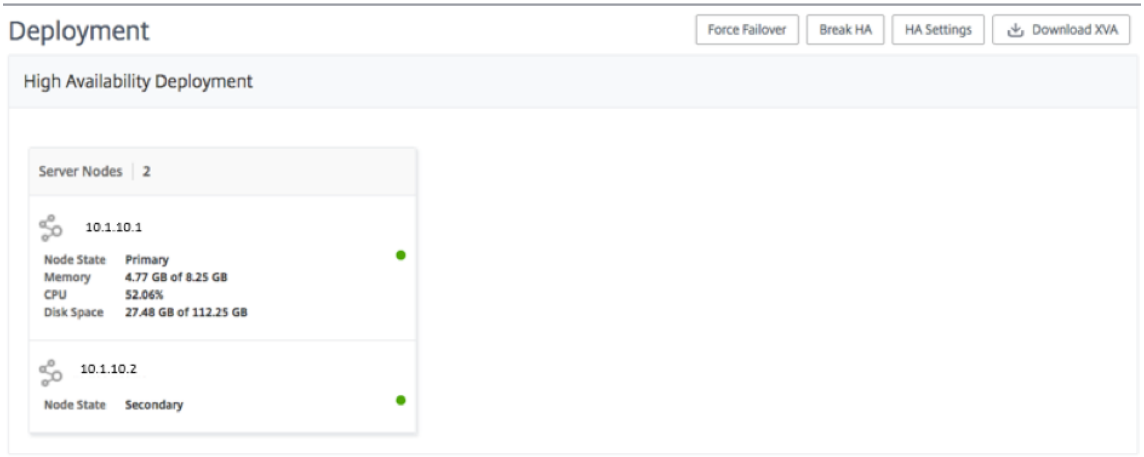
7. 使用管理员凭据登录到 Citrix ADM，单击主页中的“ 开始”，然后（可选）完成以下操作：

   a）添加 Citrix ADC 实例

b) 配置客户身份

> 注意
>
> 您也可以单击“ 跳过”以稍后完成，然后单击“ 完成”。

8. 导航到“ 系统”>“ 部署”以验证部署。



有关详细信息，请参阅 常见问题解答。

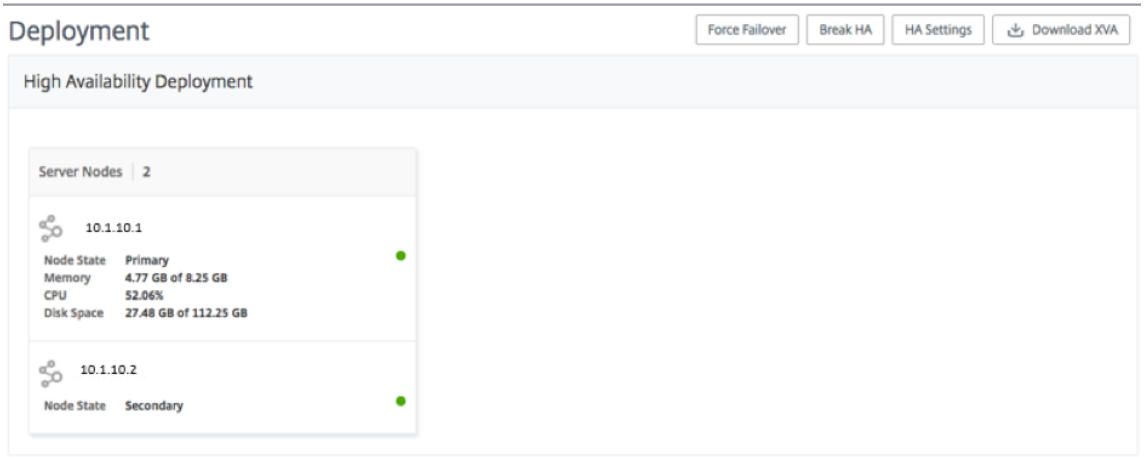
禁用高可用性功能

您可以在 Citrix ADM 高可用性对上禁用高可用性，并将节点转换为独立的 Citrix ADM 服务器。

> 注意
>
> 禁用主节点的高可用性。

要禁用高可用性，请执行以下操作：

1. 在 Web 浏览器中，输入 Citrix ADM 服务器主节点的 IP 地址。
2. 在“用 户名”和“密码”字段中，输入管理员凭据。
3. 在“系统”选项卡上，导航到“部署”，然后单击“中断高可用性”。



此时将显示一个对话框。单击 是以中断高可用性部署。

重新部署高可用性

禁用独立部署的高可用性后，可以再次将其重新部署到高可用性模式。重新部署高可用性类似于首次部署高可用性。欲了解更多详情，请参阅将主节点和辅助节点部署为高可用性对。

高可用性故障切换方案

遇到下列情况之一时，会发生故障转移：

- 节点故障：主节点故障，180 秒内未检测到主节点的检测信号。
- 应用程序运行状况故障：主节点已启动并正在运行，但其中一个 Citrix ADM 进程已关闭。

大脑分裂场景

如果由于网络链路中断，两个节点之间没有通信，则：

- 主节点继续作为主节点运行
- 由于无法接收检测信号，辅助节点将其作为主节点接管
- 两个节点都会运行各自的数据库实例

例如，在企业中，已将两个 Citrix ADM 节点部署为主节点和辅助节点。由于网络链路可能会停机，因此两个 Citrix ADM 节点之间的通信会完全中断。由于 180 秒以上没有检测信号交换，因此两个节点都认为自己是主节点。两个节点都充当活动节点并运行自己的数据库实例。

在 Citrix ADM 12.1 或更高版本中，网络链路和检测信号恢复后，这种大脑分裂情况将得到正常处理。高可用性同步会自动恢复。恢复时间取决于节点之间链路的数据和速度。

> 注意
>
> 在大脑拆分情况下，当旧主节点以高可用性重新连接时，旧主节点上发生的更改将重置为新主节点。在大脑拆分期间，新主节点上发生的更改保持不变。

配置灾难恢复以实现高可用性

April 23, 2021

灾害是由自然灾害或人为事件引起的业务功能突然中断。灾难影响数据中心的运营，之后必须完全重建和恢复在灾难现场丢失的资源和数据。数据中心中的数据丢失或停机至关重要，并使业务连续性崩溃。

Citrix ADM 灾难恢复 (DR) 功能为在高可用性模式下部署的 Citrix ADM 提供了完整的系统备份和恢复功能。恢复时，恢复站点中提供证书、配置文件和数据库的完整备份。

下表介绍了在 Citrix ADM 中配置灾难恢复时使用的术语。

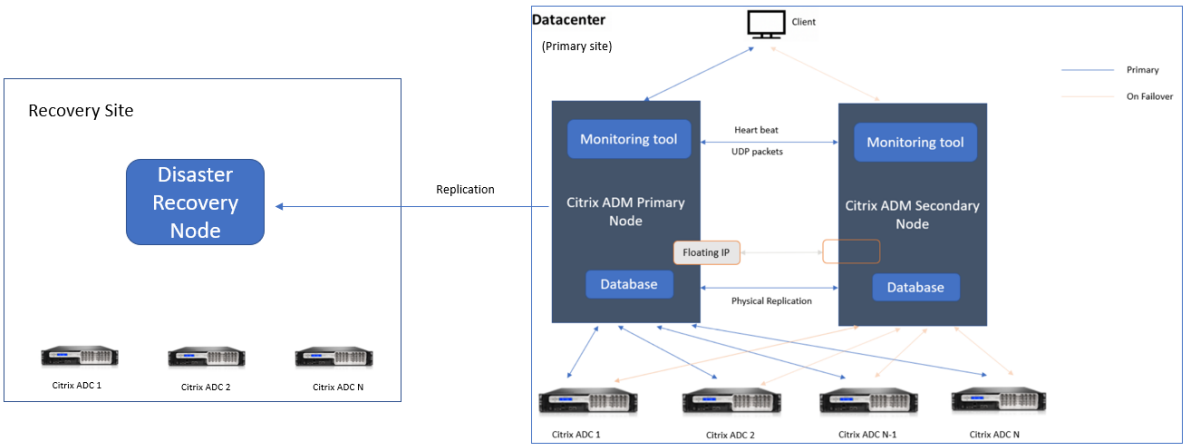
条款	说明
主站点（数据中心 A）	主站点以高可用性模式部署了 Citrix ADM 节点。
恢复站点（数据中心 B）	恢复站点具有以独立模式部署的灾难恢复节点。此节点处于只读模式，在主站点关闭之前不能运行。
灾难恢复节点	恢复节点是部署在恢复站点中的独立节点。如果主站点发生灾难且该节点无法正常工作，则此节点将使该节点可以运行（对新的主节点）。

> 注意：主站点和 DR 站点通过端口 5454 和 22 相互通信，默认情况下这些端口处于启用状态。
> 有关端口和协议详细信息的详细信息，请参阅 端口。

灾难恢复工作流程

下图显示灾难恢复工作流、灾难前的初始设置以及灾难后的工作流。

灾难前的初始设置



该图显示灾难发生之前的灾难恢复设置。

主站点以高可用性模式部署了 Citrix ADM 节点。要了解更多信息，请参阅高可用性部署

恢复站点具有远程部署的独立 Citrix ADM 灾难恢复节点。灾难恢复节点处于只读模式，从主节点接收数据以创建数据备份。还会发现恢复站点中的 Citrix ADC 实例，但它们没有任何流量通过这些实例。在备份过程中，所有数据、文件和配置都会从主节点复制到灾难恢复节点上。

必备条件

在设置灾难恢复节点之前，请注意以下先决条件：

- 要启用灾难恢复设置，主站点必须将 Citrix ADM 节点配置为高可用性模式。
- 主站点中 Citrix ADM 的独立部署不支持灾难恢复功能。
- Citrix ADM HA 对（在主站点中）和独立节点（在 DR 站点中）必须具有相同的软件版本、内部版本和配置。

Citrix 建议您将 CPU 优先级（在虚拟机属性中）设置为最高级别，以改善调度行为和网络延迟。

下表列出了配置灾难恢复节点的最低要求：

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。默认值为 120 GB。实际存储需求取决于 Citrix ADM 大小估计。如果您的 Citrix ADM 存储需求超过 120 GB，则必须连接额外的磁盘。注意您只能再添加一个磁盘。Citrix 建议您在初始部署时估算存储并连接更多磁盘。有关详细信息，请参阅如何将附加磁盘连接到 Citrix ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序	版本
Citrix Hypervisor	6.2 和 6.5
VMware ESXi	5.5 和 6.0
Microsoft Hyper-V	2012 R2
Linux KVM	乌班图和费多拉

首次灾难恢复设置

- 在高可用性模式下部署 Citrix ADM
- 部署并注册 Citrix ADM 灾难恢复节点
- 从用户界面启用和禁用灾难恢复设置

在高可用性模式下部署 **Citrix ADM**

要设置灾难恢复设置，请确保 Citrix ADM 以高可用性模式部署。有关在高可用性中部署 Citrix ADM 的信息，请参阅高可用性部署

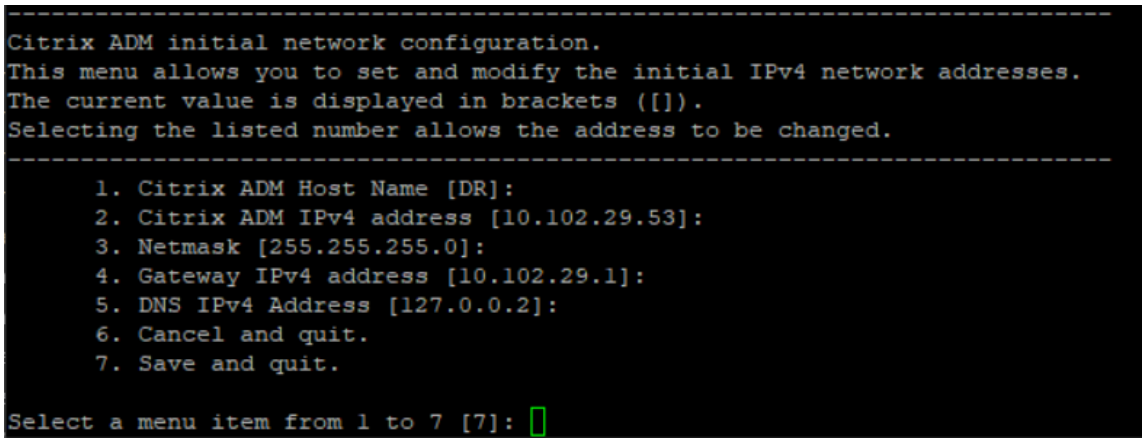
> 注意
>
> - 在高可用性模式下部署的 Citrix ADM 必须升级到 Citrix ADM 版本 13.0。
> - 向主节点注册灾难恢复节点时，必须使用浮动 **IP** 地址。

使用灾难恢复控制台部署和注册 **Citrix ADM** 灾难恢复节点

要注册 Citrix ADM 灾难恢复节点，请执行以下操作：

1. 从 Citrix 下载站点下载 `.xva` 映像文件并将其导入到 Hypervisor 中。
2. 在 控制台选项卡中，使用初始网络配置配置 Citrix ADM。

   > 注意
   >
   > 灾难恢复节点可以位于不同的子网上。

3. 初始网络配置完成后，系统将提示登录。使用以下凭据登录 — `nsrecover`/`nsroot`。

   > 重要信息：
   >
   > 请勿在注册过程中更改 DR 节点凭据 (`nsrecover`/`nsroot`)。成功注册 DR 节点后，您可以更改 DR 节点凭据。

4. 要部署灾难恢复节点，请键入 **/mps/**部署 **_type.py** ，然后按 Enter 键。此时将显示 Citrix ADM 部署配置菜单。


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. 选择 **2** 注册灾难恢复节点。

```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 2
Selected Option      2. Remote Disaster Recovery Node.
```

6. 控制台提示输入高可用性节点和密码的浮动 IP 地址。

7. 输入浮动 IP 地址和密码，将灾难恢复节点注册到主节点。

```
------------------------------------------------------------------------------
    Backup node Configuration.

    Specify the IP address and the password of the Citrix ADM server.
    Type 0 anytime to cancel and quit.
    ------------------------------------------------------------------------
    Enter Citrix ADM Floating IP Address:10.102.29.97
    Enter password for Citrix ADM:
```

灾难恢复节点现在已成功注册。

```
Stopping appd
Stopping nsulfd
Stopped nsulfd
Stopped appd
waiting for server to shut down.... done
server stopped
------------------------------------------------------------------------
    Backup node Registration successful.
    ------------------------------------------------------------------------
```


> ** 注
>
> 意 ** 灾难恢复节点没有 GUI。

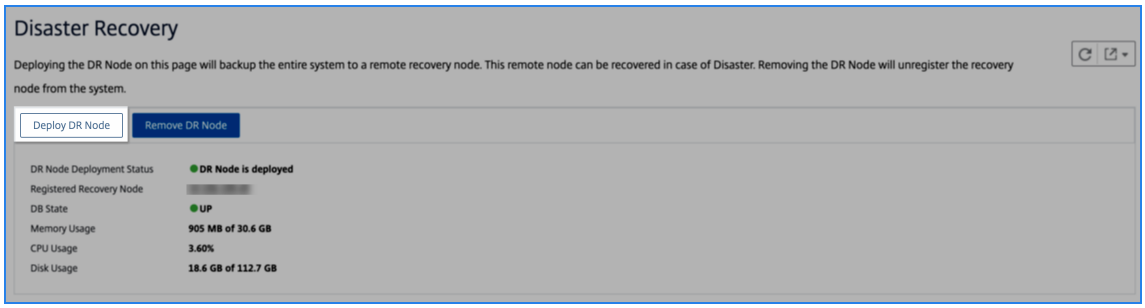
8. 如果要更改 DR 节点密码，请运行以下脚本：

```
/mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

使用 **Citrix ADM GUI** 部署灾难恢复节点

使用 DR 控制台成功注册灾难恢复节点后，从 Citrix ADM GUI 部署灾难恢复节点。此步骤启用 Citrix ADM 主站点的灾难恢复设置。

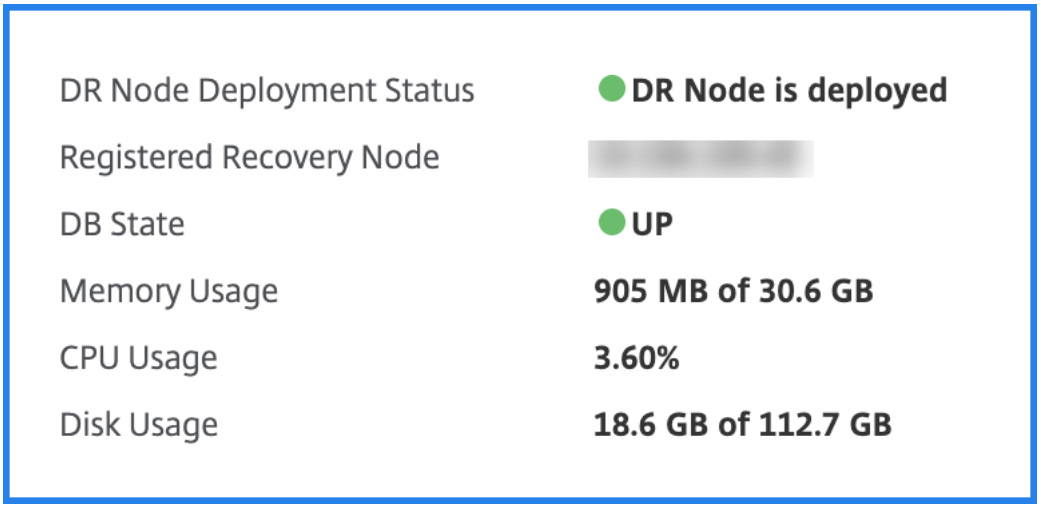
1. 导航到 **“系统” > “系统管理” > “灾难恢复设置”**。
2. 在 “ 灾难恢复” 页上，选择 “ 部署灾难恢复节点”。



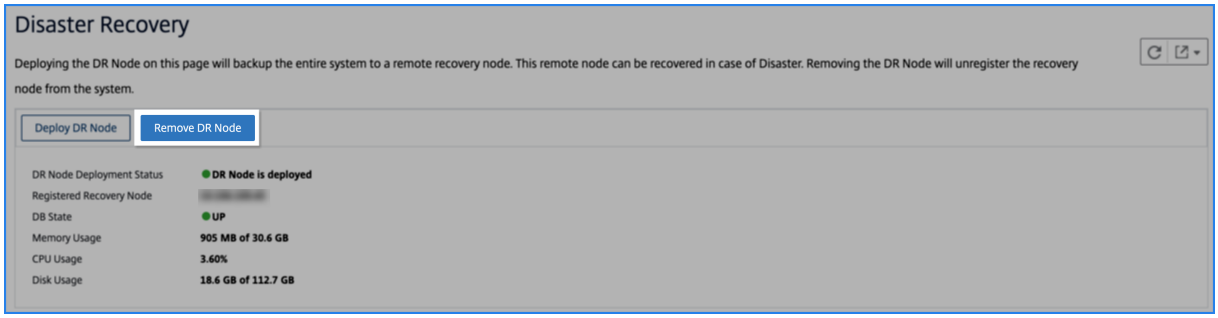
3. 将显示一个确认对话框。单击 “ 是” 继续。

> 注意
>
> 系统备份所需的时间取决于数据大小和 WAN 链路速度。

在 Citrix ADM GUI 中成功部署 DR 节点后，您可以监视 DR 节点的数据库状态、内存、CPU 和磁盘使用情况。



要禁用灾难恢复设置，请选择删除灾难恢复节点。将显示一个确认对话框。单击“是”继续。



要再次启用 DR 节点，请为高可用性对重新配置 DR 节点：

1. 使用 Hypervisor 或 SSH 控制台登录 DR 节点。
2. 按照中的可用过程配置 DR 节点使用灾难恢复控制台部署和注册 Citrix ADM 灾难恢复节点。
3. 使用 Citrix ADM GUI 部署灾难恢复节点。

有关详细信息，请参阅 常见问题解答。

> 重要
>
> - 管理员有责任检测主站点上是否发生了灾难。
> - 灾难恢复工作流由管理员在主站点关闭后手动启动。
> - 管理员必须通过在恢复站点的灾难恢复节点上运行恢复脚本来手动启动该过程。
> - 如果升级主站点中的 HA 对，则还必须手动升级 DR 站点中的独立节点。

灾难发生后的工作流程

灾难发生后主站点关闭时，必须按以下方式启动灾难恢复工作流：

1. 管理员发现灾难袭击了主站点，并且该站点无法正常运行。
2. 管理员启动恢复过程。
3. 管理员必须根据您的要求（在恢复站点）在灾难恢复节点上手动运行以下恢复脚本之一：
   - DR 节点上的 SNMP、系统日志和分析：

     ```
     1  /mps/scripts/pgsql/pgsql_restore_remote_backup.sh
     2
     3  <!--NeedCopy-->
     ```

   - 还将 DR 节点配置为许可证服务器：

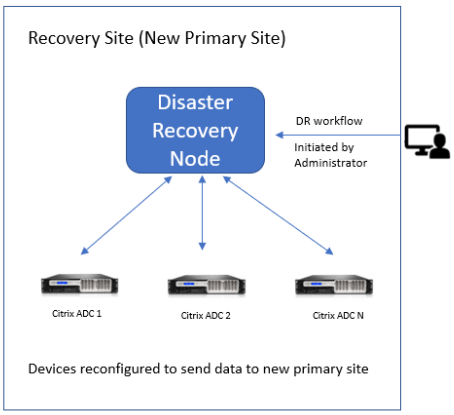
     ```
     1  /mps/scripts/pgsql/pgsql_restore_remote_backup.sh -reconfig-
           ls <IP-address-of-the-primary-site>
     2
     ```

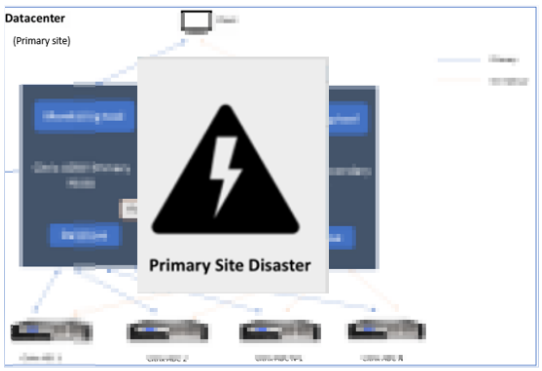


```
<!--NeedCopy-->
```

4. 在内部，Citrix ADC 实例会自动重新配置，以将数据发送到灾难恢复节点，该节点现在已成为新的主站点。

   下图显示灾难袭击主站点后的灾难恢复工作流。





> 注意：
>
> 在 DR 站点启动脚本后，DR 站点现在成为新的主站点。您还可以访问 DR 用户界面。

灾后恢复

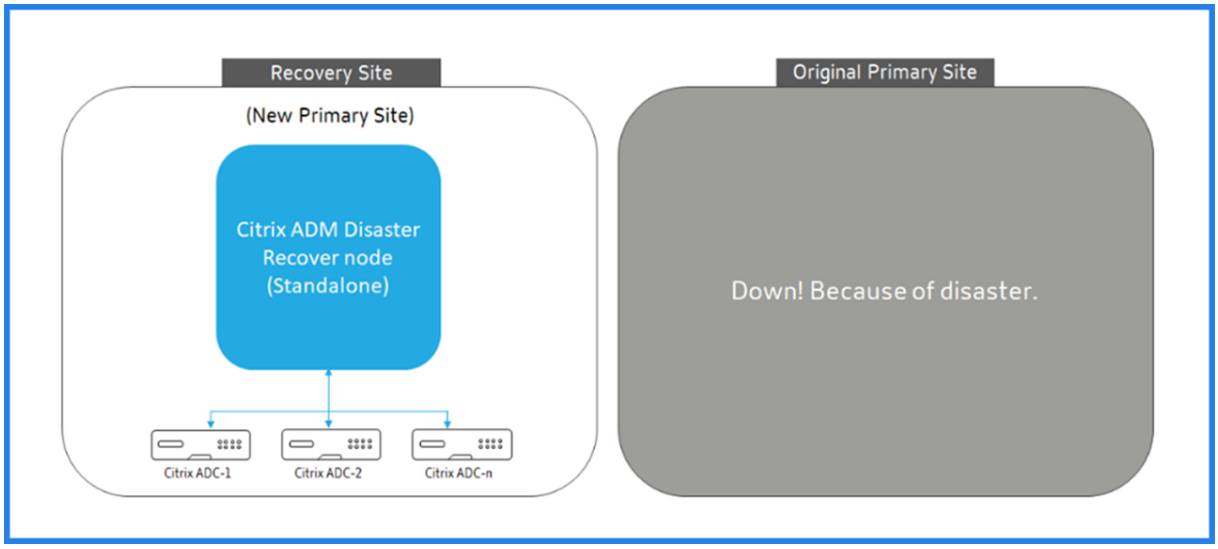
灾难发生并且管理员启动恢复脚本后，DR 站点现在成为新的主站点。

如果要稍后将配置还原到原始站点，请参阅将配置还原到原始主站点。

> 重要
>
> - 如果您已安装了 Citrix ADM 12.1.49.x 或更早版本，则可以在 30 天的宽限期内与 Citrix 联系，以便在 Citrix ADM（在 DR 站点）上重新托管原始许可证。
> - 对于 12.1.50.x 或更高版本，Citrix ADM 许可证会自动同步到 DR 站点（不需要联系 Citrix 获取许可证）。
> - 12.1.50.x 或更高版本支持 DR 站点的池许可证。如果您已为实例应用了池许可证，请手动将实例重新配置到 DR 站点。

将配置还原到原始主站点

灾难发生后，配置的灾难恢复 (DR) 节点将成为新的主站点，客户端通信流经此节点。



有关详细信息，请参阅灾难发生后的工作流程。

如果原始主站点没有灾难，并且您决定将所有操作移动到主站点，请重新配置原始主站点以匹配 DR 节点中的配置。

在开始之前，请确保主站点和灾难恢复站点都处于活动状态。

要从 DR 站点还原到原始主站点的更改，请执行以下步骤：

1. 登录到原始主站点并运行以下命令：

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password> &
<!--NeedCopy-->
```

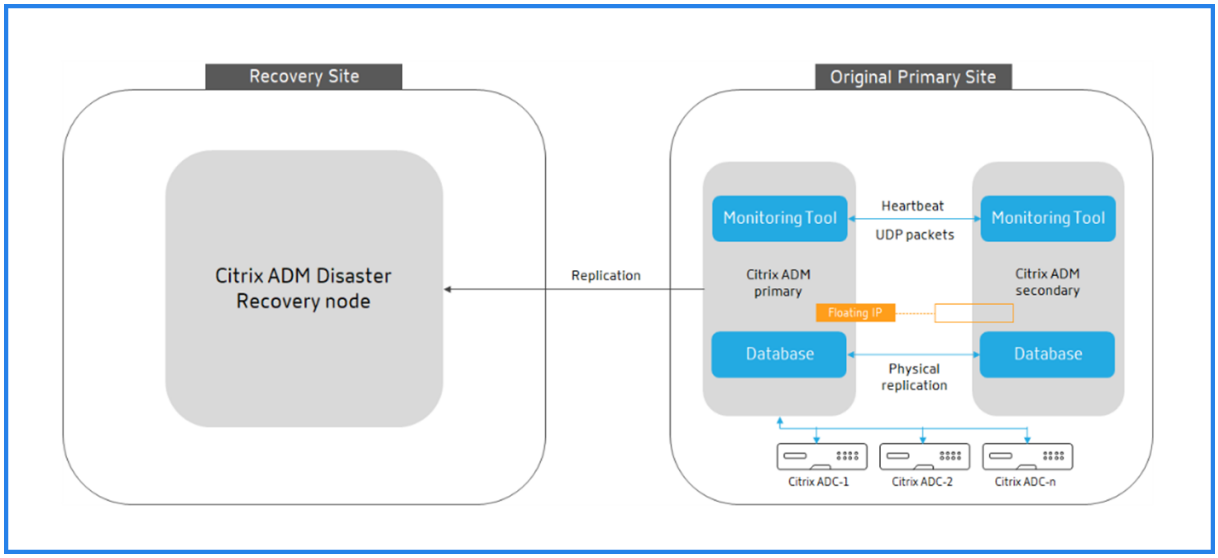
此命令仅将系统日志、SNMP 和分析配置到主站点。

如果要将主站点配置为 ADC 实例的池许可证服务器，请运行以下命令：

```
nohup /mps/sync_adm_node.py -I <DR-site-IP-address> -R <DR-node-password> -L <primary-node-password>  -O yes &
<!--NeedCopy-->
```

-O 命令获取 DR 站点 IP 地址并将主站点重新配置为池许可证服务器。

2. 重新配置 DR 站点。请参阅部署灾难恢复设置。



成功将配置从 DR 站点还原到原始主站点后，客户端流量会通过 Citrix ADM 主节点进行流动。

为多站点部署配置内部部署代理

April 23, 2021

在早期版本的 Citrix ADM 中，可以通过在主数据中心中运行的 Citrix ADM 管理和监视部署在远程数据中心中的 Citrix ADC 实例。Citrix ADC 实例将数据直接发送到主 Citrix ADM，导致广域网带宽消耗。此外，处理分析数据会利用主 Citrix ADM 的 CPU 和内存资源。

您可以将数据中心设在全球各地。代理在以下情况下发挥着至关重要的作用：

- 在远程数据中心中安装代理，以降低 WAN 带宽消耗。
- 限制直接向主 Citrix ADM 发送流量以进行数据处理的实例数。

> 注意
>
> - 建议在远程数据中心中为实例安装代理，但不是强制安装代理。如有必要，用户可以直接将 Citrix ADC 实例添加到主 Citrix ADM 中。
> - 如果为一个或多个远程数据中心安装了代理，则代理与主站点之间的通信是通过浮动 IP 地址进行的。有关详细信息，请参阅端口。
> - 您可以安装代理并将池许可证应用于一个或多个远程数据中心的实例。在这种情况下，主站点和一个或多个远程数据中心之间的通信是通过浮动 IP 地址。

在 Citrix ADM 12.1 或更高版本中，可以使用代理配置实例，以便与位于不同数据中心的主 Citrix ADM 进行通信。

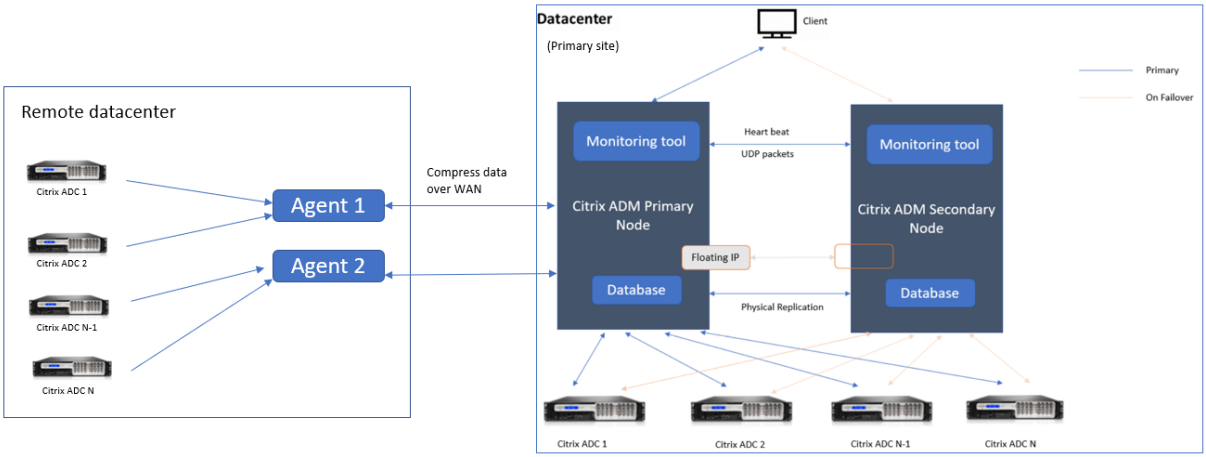
代理在不同数据中心的主 Citrix ADM 和发现的实例之间起到中介作用。以下是安装代理的好处：

- 这些实例配置为代理，以便将未处理的数据直接发送到代理，而不是主 Citrix ADM。代理执行第一级数据处理，并以压缩格式将处理的数据发送到主 Citrix ADM 进行存储。
- 代理和实例位于同一个数据中心，以便更快地处理数据。
- 对代理进行群集可在代理故障转移时重新分配 Citrix ADC 实例。当站点中的一个代理出现故障时，Citrix ADC 实例的流量将切换到同一站点中的另一个可用代理。

> 注意
>
> 每个站点要安装的代理数取决于正在处理的流量。

体系结构

下图显示了两个数据中心中的 Citrix ADC 实例以及使用基于多站点代理的体系结构的 Citrix ADM 高可用性部署。



主站点在高可用性配置中部署了 Citrix ADM 节点。主站点中的 Citrix ADC 实例直接向 Citrix ADM 注册。

在辅助站点中，代理部署并向主站点中的 Citrix ADM 服务器注册。这些代理在群集中工作，以便在发生代理故障转移时处理流量的连续流量。辅助站点中的 Citrix ADC 实例通过位于该站点内的代理向主 Citrix ADM 服务器注册。实例将数据直接发送到代理，而不是主 Citrix ADM。代理处理从实例接收到的数据，并以压缩格式将其发送到主 Citrix ADM。代理通过安全通道与 Citrix ADM 服务器进行通信，并压缩通过该通道发送的数据以提高带宽效率。

入门

- 在数据中心中安装代理
  - 注册代理
  - 将代理连接到站点
- 添加 Citrix ADC 实例
  - 添加新实例
  - 更新现有实例

在数据中心中安装代理

您可以安装和配置代理，以启用主 Citrix ADM 与另一个数据中心中的托管 Citrix ADC 实例之间的通信。

您可以在企业数据中心的以下虚拟机管理程序上安装代理：

- Citrix Hypervisor
- VMware ESXi
- Microsoft Hyper-V
- Linux KVM 服务器

> 注意
>
> 仅使用 Citrix ADM 高可用性部署支持多站点部署的本地部署代理。

在开始安装代理之前，请确保拥有 Hypervisor 必须为每个代理提供的所需虚拟计算资源。

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	30 千克
虚拟网络接口	1
吞吐量	1 Gbps

端口

出于通信目的，代理和 Citrix ADM 内部部署服务器之间必须打开以下端口。

类型	端口	详细信息	通信方向
TCP	8443, 7443, 443	用于代理与 Citrix ADM 内部部署服务器之间的出站和入站通信。	Citrix ADM 代理到 Citrix ADM

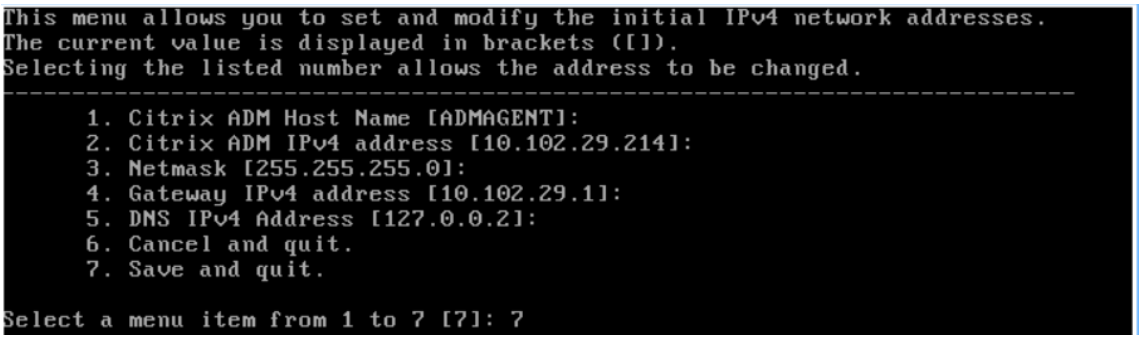
代理和 Citrix ADC 实例之间必须打开以下端口。

类型	端口	详细信息	通信方向
TCP	80	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的 NITRO 通信。	Citrix ADM 到 Citrix ADC 和 Citrix ADC 到 Citrix ADM

TCP	22	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的 SSH 通信。用于在高可用性模式下部署的 Citrix ADM 服务器之间进行同步。	Citrix ADM 至 Citrix ADC，将 Citrix ADM 代理转至 Citrix ADC
UDP	4739	用于代理与 Citrix ADC 或 Citrix SD-WAN 实例之间的应用流通信。	Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM
ICMP	无预留端口	检测 Citrix ADM 和 Citrix ADC 实例、SD WAN 实例或在高可用性模式下部署的辅助 Citrix ADM 服务器之间的网络可访问性。
UDP	161, 162	从 Citrix ADC 实例接收 SNMP 事件到代理。	端口 161-Citrix ADM 到 Citrix ADC
		端口 162-Citrix ADC 到 Citrix ADM
UDP	514	从 Citrix ADC 或 Citrix SD-WAN 实例接收系统日志消息到代理。|Citrix ADC 或 Citrix SD-WAN 到 Citrix ADM|	TCP
5557	用于代理程序和 Citrix ADC 实例之间的日志流通信。	思杰 ADC 到思杰 ADM

注册代理

1. 使用从 Citrix 下载站点下载的代理映像文件，并将其导入到 Hypervisor 中。代理映像文件的命名模式如下：**MASAGENT-<HYPERVISOR>-。** 例如：** 马斯代理-Xen-130-XY.xva**
2. 在 控制台选项卡中，使用初始网络配置配置 Citrix ADM。
3. 输入 Citrix ADM 主机名、IPv4 地址和 Gateway IPv4 地址。选择选项 7 以保存并退出配置。

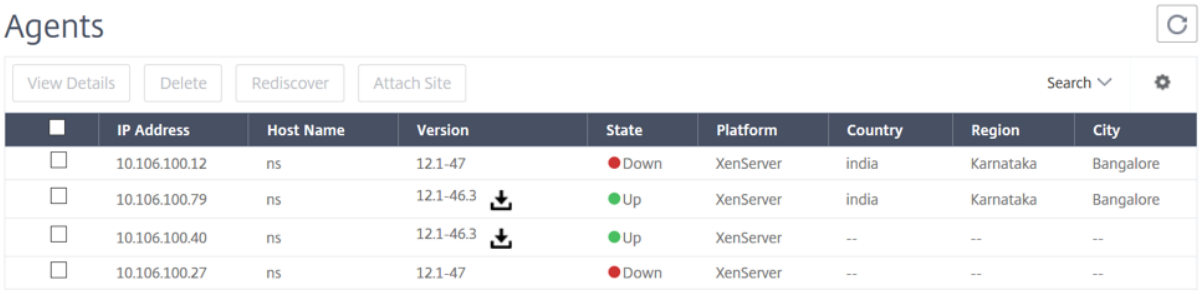


4. 注册成功后，控制台将提示登录。使用 *NSRecover/nsroot* 作为凭据。
5. 要注册代理，请输入 **/mps/register_agent_onprem.py**。如下图所示，将显示 Citrix ADM 代理注册凭据。
6. 输入 Citrix ADM 浮动 IP 地址和用户凭据。


```
bash-3.2# /mps/register_agent_onprem.py

------------------------------------------------------------------------------
-----------------------------------------
Citrix ADM Agent Registration with Citrix ADM On-Prem Server. This menu allows y
ou to specify Citrix ADM Server IP Address and admin credentials.
If Citrix ADM is deployed in HA mode, it is advisable to register with Citrix AD
M floating IP Address.
------------------------------------------------------------------------------
---------------------------------------
    Enter IP Address or URL:10.102.29.211
    Enter User Name:nsroot
    Enter Password:

Trying to register this agent with Citrix ADM  10.102.29.211
Dec  3 18:07:52 <auth.notice> ns date: date set by nsrecover
------------------------------------------------------------------------------
    Citrix ADM Agent Registration successful.
------------------------------------------------------------------------------
```

注册成功后，代理将重新启动以完成安装过程。

代理重新启动后，访问 Citrix ADM GUI，从主菜单转到 网络 **>** 代理页面以验证代理的状态。新添加的座席将显示为 “启动” 状态。

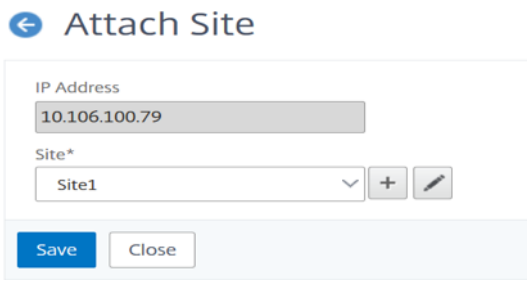


> 注意
>
> Citrix ADM 将显示代理的版本，并检查代理是否为最新版本。下载图标表示代理不在最新版本上，需要升级。Citrix 建议您将代理版本升级到 Citrix ADM 版本。

将代理连接到站点

1. 选择代理，然后单击 附加站点。
2. 在附加站点页面中，从列表中选择一个站点，或使用加号 (+) 按钮创建站点。
3. 单击 “ 保存”。

> 注意
>
> - 默认情况下，所有新注册的代理都会添加到默认数据中心。
> - 请务必将代理与正确的站点相关联。如果出现代理故障，分配给它的 Citrix ADC 实例将自动切换到同一站点中的其他正常运行的代理。



代理行动

您可以在 网络 **>** 客户端 **>** 选择操作下对座席应用各种操作。

在 **“选择操作”** 下，您可以使用以下功能：

安装新证书：如果您需要不同的代理证书来满足安全要求，则可以添加证书。

更改默认密码：为确保基础架构的安全性，请更改代理的默认密码。

生成技术支持文件：为选定的 Citrix ADM 代理生成技术支持文件。您可以下载此文件并将其发送给 Citrix 技术支持以进行调查和故障排除。

添加 **Citrix ADC** 实例

实例是您希望通过代理从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 或代理中：

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix Gateway
- Citrix SSL 转发代理
- Citrix SD-WAN O

有关详细信息，请参阅将实例添加到 Citrix ADM。

将现有实例附加到代理

如果实例已添加到主 Citrix ADM 中，则可以通过编辑代理将其附加到代理。

1. 导航到 **“网络” > “实例”**，然后选择实例类型。例如，Citrix ADC。
2. 单击 编辑以编辑现有实例。

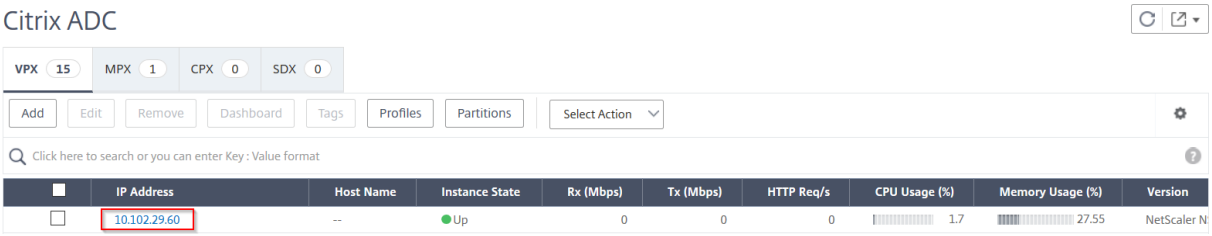
3. 单击以选择代理。
4. 在 代理页面中，选择要与实例关联的代理，然后单击确定。

> 注意：
>
> 确保选择要与实例关联的 站点。

访问实例的 **GUI** 以验证事件

添加实例并配置代理后，访问实例的 GUI 以检查是否配置了陷阱目标。

在 Citrix ADM 中，导航到 **“网络” > “实例”**。在 “实例” 下，选择要访问的实例类型（例如 Citrix ADC VPX），然后单击特定实例的 IP 地址。



所选实例的 GUI 将显示在弹出窗口中。

默认情况下，代理配置为实例上的陷阱目标。要确认，请登录到实例的 GUI 并检查陷阱目标。

> 重要
>
> 建议在远程数据中心中为 Citrix ADC 实例添加代理，但不是强制性的。
>
> 如果要将实例直接添加到主 MAS，请勿在添加实例时选择代理。

Citrix ADM 代理故障切换

代理故障切换可能发生在具有两个或多个注册代理的站点中。当代理在站点中处于非活动状态（关闭状态）时，Citrix ADM 将与其他活动代理重新分配非活动代理的 ADC 实例。

> 重要
>
> - 确保在您的帐户上启用了 代理故障切换功能。要启用此功能，请参阅 启用或禁用 ADM 功能。
> - 如果代理正在运行脚本，请确保该脚本存在于站点中的所有代理上。因此，更改的代理可以在代理故障转移后运行脚本。

要将站点附加到 ADM GUI 中的代理，请参阅将代理连接到站点。

要实现代理故障切换，请逐个选择 Citrix ADM 代理并连接到同一站点。

例如，两个代理 10.106.1xx.2x 和 10.106.1xx.3x 连接并在班加罗尔场址投入使用。如果一个代理处于非活动状态，Citrix ADM 将检测到该代理并将状态显示为关闭。

当 Citrix ADM 代理在站点中变为非活动状态（关闭状态）时，Citrix ADM 将等待五分钟，以便代理处于活动状态（启动状态）。如果代理处于非活动状态，Citrix ADM 会在同一站点中的可用代理之间自动重新分配这些实例。

Citrix ADM 每 30 分钟触发一次实例重新分配，以平衡站点中活动代理之间的负载。

在 **Kubernetes** 集群上将 **ADM** 代理作为微服务安装

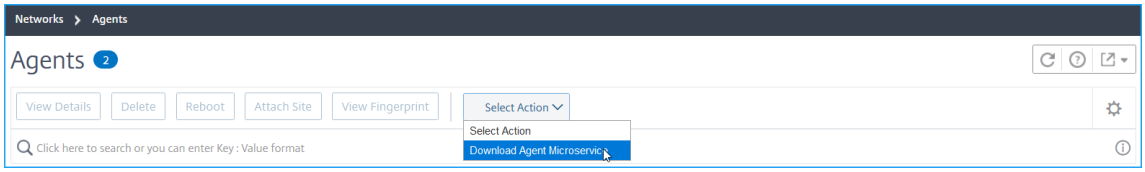
April 23, 2021

将 Citrix ADM 代理部署为微服务对于管理 Citrix ADC CPX 非常有用。仅当 Citrix ADM 和 Kubernetes 群集在其他网络上配置时，本文档中提供的过程才适用。在这种情况下，您可以将 ADM 代理配置为托管 Kubernetes 集群的微服务。

> 注意
>
> 您还可以在托管 Kubernetes 集群的网络上配置代理 本地代理 并注册代理。

快速入门

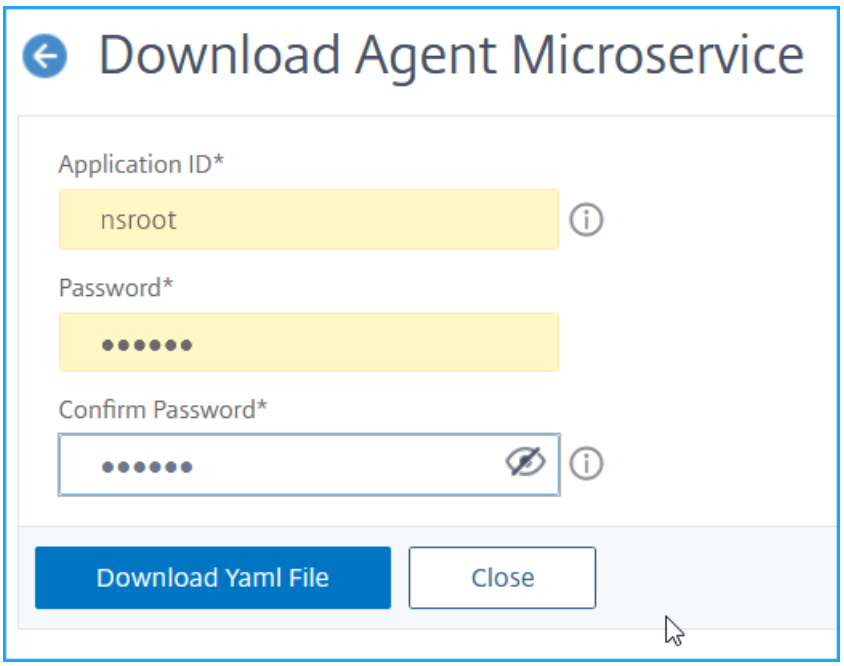
1. 在 Citrix ADM 中，导航到 网络 **>** 代理。
2. 从 **“选择操作”** 列表中，选择 “下 载代理微服务” 选项。



3. 在 “下 载代理微服务” 页中，指定以下参数：
   a) 应用程序 **ID** — 一个字符串 ID，用于为 Kubernetes 集群中的代理定义服务并将此代理与同一集群中的其他代理区分开来。
   b) 密码 — 指定 CPX 的密码，以便 CPX 使用此密码通过代理将 CPX 载入 ADM。
   c) 确认密码 — 指定相同的密码进行确认。

> 注意
>
> 不得使用默认密码 (nsroot)。

d) 点击 下载 **Yaml** 文件。



在 **Kubernetes** 群集中安装 **Citrix ADM** 代理

在 Kubernetes 主节点中：

1. 保存下载的 YAML 文件
2. 运行以下命令：

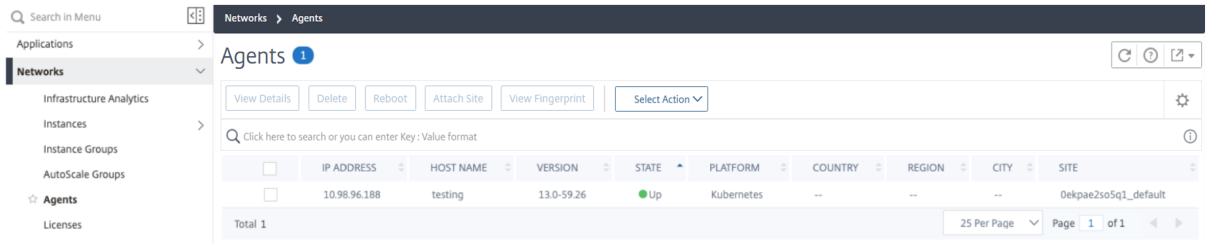
   ```
   kubectl create -f <yaml file>
   ```

   例如，`kubectl create -f testing.yaml`

   代理已成功创建。

   ```
   root@[redacted]:/# kubectl create -f testing.yaml
   deployment.apps/testing created
   service/testing created
   secret/testing created
   configmap/testing created
   root@[redacted]:/#
   ```

在 Citrix ADM 中，导航到 网络 > 代理以查看代理状态。



有关开始使用服务图的更多信息，请参阅 设置服务图表。

将 **Citrix ADM** 单服务器部署迁移到高可用性部署

April 23, 2021

您可以将 Citrix ADM 单个服务器升级到两台 Citrix ADM 服务器的高可用性部署。一对高可用性 Citrix ADM 服务器处于主动-被动模式，两个服务器的配置相同。在此类型的主动-被动部署中，一台 Citrix ADM 服务器被配置为主节点，另一台配置为辅助节点。如果由于任何原因，主节点出现故障，辅助节点将接管。

要将 Citrix ADM 单服务器迁移到高可用性对，您需要预配置新的 Citrix ADM 服务器节点，将其配置为第二台 Citrix ADM 单服务器，并将两台 Citrix ADM 服务器部署为高可用性对。

将 Citrix ADM 单服务器迁移到高可用性模式需要执行以下步骤：

1. 修改现有服务器节点
2. 置备第二个服务器节点
3. 以 HA 模式部署两个节点
4. 配置高可用性对

修改现有的 **Citrix ADM** 服务器节点

要将 Citrix ADM 从单个服务器迁移到高可用性模式，必须将服务器节点的初始部署类型更改为高可用性模式。

1. 在工作站或笔记本电脑上，打开现有 Citrix ADM 服务器节点的控制台。例如，假设您已将 IP 地址为 10.106.171.17 的 Citrix ADM 部署为独立服务器。
2. 登录到 Citrix ADM。默认凭据是 `nsroot` 和 `nsroot`。
3. 在 shell 提示符中，键入 **/mps/**部署类型**.py**，然后按 **Enter** 键。
4. 选择作为 Citrix ADM 服务器的部署类型。如果不选择任何选项，默认情况下，它部署为服务器。


```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]:
```

5. 部署控制台提示您选择服务器部署（作为独立部署）。键入 **No** 以确认部署为高可用性对。
6. 控制台提示选择（第一个服务器节点）。输入 **Yes**（是）确认节点为第一个服务器节点。
7. 控制台提示重新启动服务器。
8. 键入 **Yes** 以重新启动。

```
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:yes
Restart the system for the configuration to take effect. Do you want to restart?
 [yes/no]:yes
```

预配第二个服务器节点

必须在虚拟机管理程序上置备第二个服务器。使用在安装第一个服务器时使用的同一映像文件，或从 Citrix 下载站点获取相同版本的映像文件。

1. 将映像文件导入到 Hypervisor，然后从控制台选项卡配置初始网络配置选项，如以下屏幕中所述：

```
------------------------------------------------------------------------------
Citrix ADM initial network configuration.
This menu allows you to set and modify the initial IPv4 network addresses.
The current value is displayed in brackets ([]).
Selecting the listed number allows the address to be changed.
------------------------------------------------------------------------------
      1. Citrix ADM Host Name [CitrixADM]:
      2. Citrix ADM IPv4 address [10.102.29.211]:
      3. Netmask [255.255.255.0]:
      4. Gateway IPv4 address [10.102.29.1]:
      5. DNS IPv4 Address [127.0.0.2]:
      6. Cancel and quit.
      7. Save and quit.

Select a menu item from 1 to 7 [7]:
```

2. 指定所需的 IP 地址后，在 shell 提示符中键入 /mps/部署 _type.py，然后按 Enter 键。
3. 选择作为 **Citrix ADM** 服务器的部署类型。

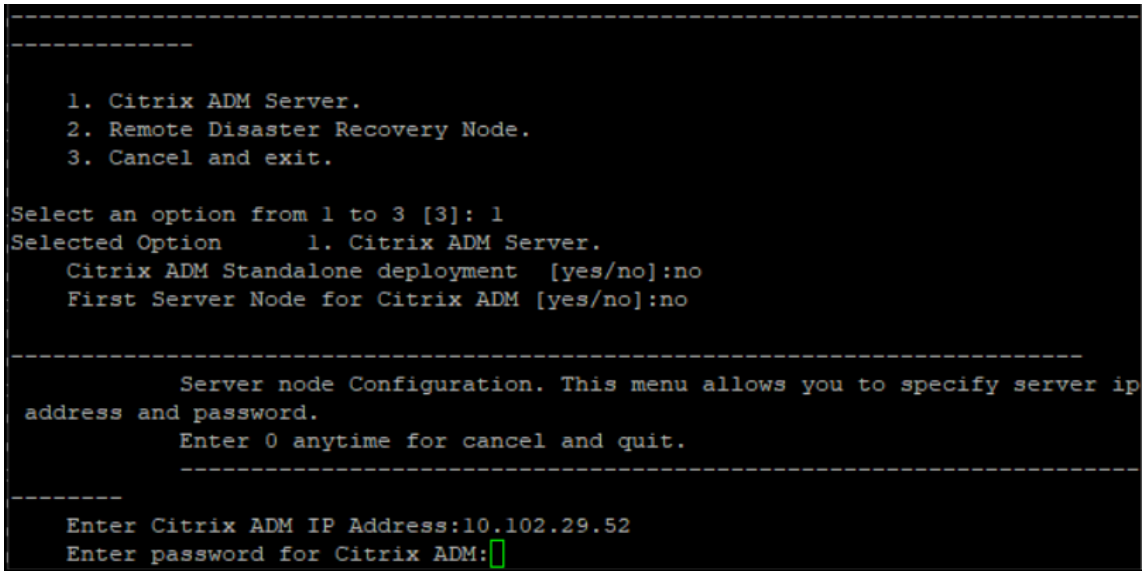
4. 部署控制台提示您选择服务器部署（作为独立部署）。键入 **No** 以确认部署为高可用性对。

```
bash-3.2# /mps/deployment_type.py
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
```

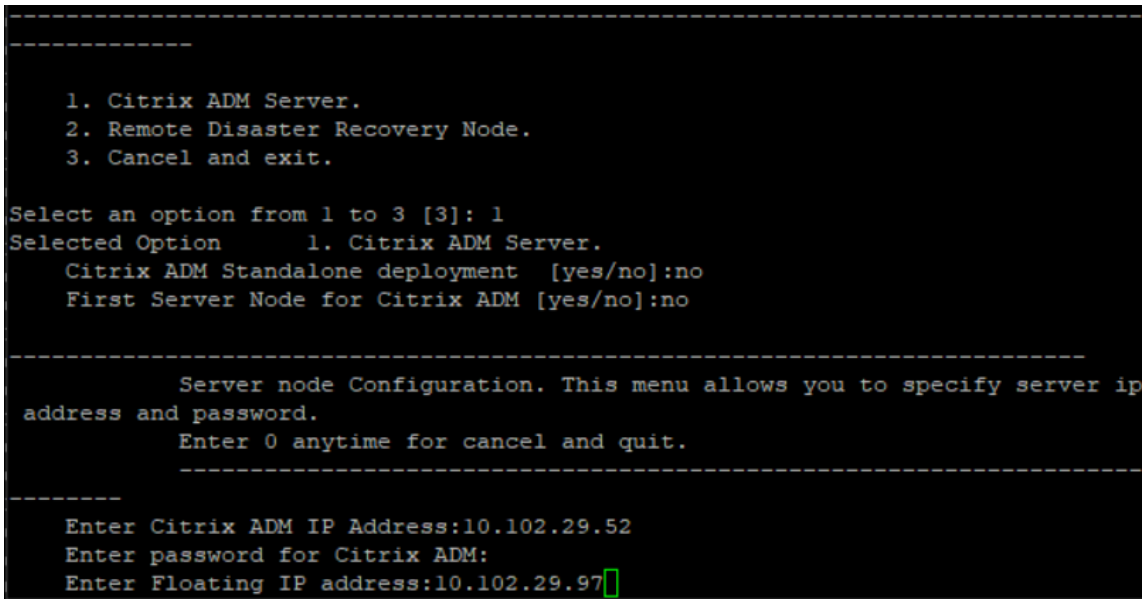
5. 控制台随后提示选择（第一个服务器节点）。键入 **No** 以确认该节点为第二个服务器节点。

```
------------------------------------------------------------------------------
-------------
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------
-------------

    1. Citrix ADM Server.
    2. Remote Disaster Recovery Node.
    3. Cancel and exit.

Select an option from 1 to 3 [3]: 1
Selected Option      1. Citrix ADM Server.
    Citrix ADM Standalone deployment  [yes/no]:no
    First Server Node for Citrix ADM [yes/no]:no
```

6. 输入第一台服务器的 IP 地址和密码。



7. 输入第一个节点的浮动 IP 地址。

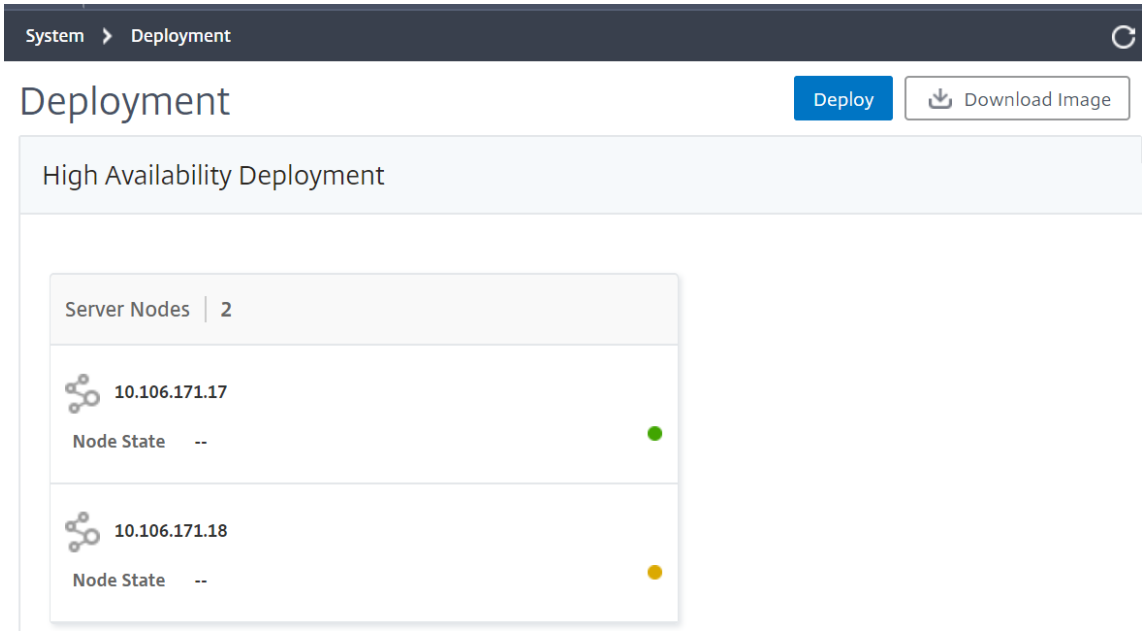


8. 控制台提示您重新启动系统。输入 **“是”** 以重新启动。

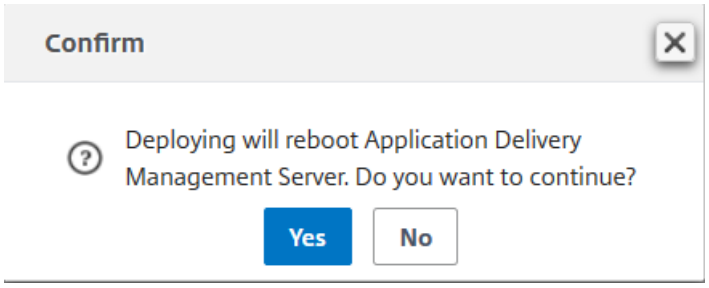
在高可用性模式下部署两台服务器

要以高可用性对的形式完成两个服务器节点的安装过程，必须从先前存在的 Citrix ADM 服务器节点的 GUI 中部署这些节点。部署两个服务器节点时，两个服务器之间即开始内部通信。

1. 在 Web 浏览器中，键入先前存在的 Citrix ADM 服务器节点的 IP 地址。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在 “ 系统” 选项卡上，导航到 “ 部署”，然后单击 “部 署”。

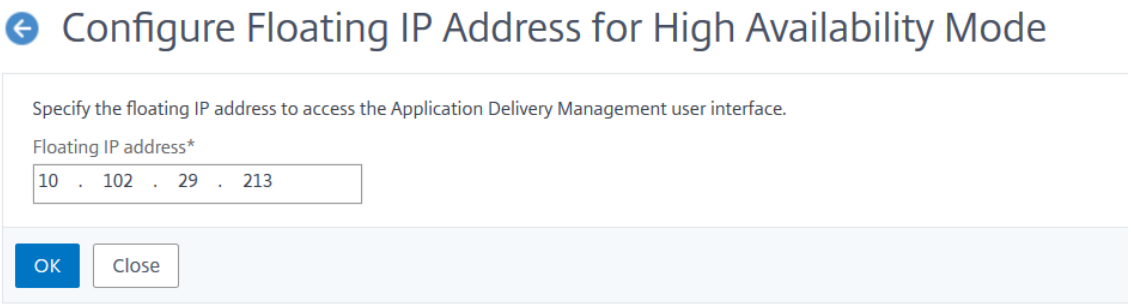


4. 此时将显示一条确认消息。单击是。



> 注意
>
> 在以高可用性部署 Citrix ADM 后，您可以访问主节点或浮动 IP 地址。从 12.1 版本开始，您无法访问辅助节点。

5. 虽然您在配置第二个服务器节点时输入了浮动 IP，但您可以选择在 “ 系统” 页上更新 FIP。单击 **HA** 设置 **>** 为高可用性模式配置浮动 **IP** 地址。您可以查看之前配置的浮动 IP 地址。您可以输入新的 IP 地址，然后单击 “确定”。



从 NetScaler Insight Center 迁移至 Citrix ADM

April 23, 2021

现在，您可以将 NetScaler Insight Center 部署迁移到 Citrix ADM，而不会丢失现有配置、设置或数据。使用 Citrix ADM，您不仅可以查看与应用程序关联的 Citrix ADC 实例生成的各种分析，还可以从单个统一的控制台管理、监视整个全局应用程序交付基础结构并进行故障排除。

> 注意
>
> 当前仅 NetScaler Insight Center 独立实例支持迁移。

必备条件

在将 NetScaler 智能分析中心虚拟设备迁移到 Citrix ADM 之前，请验证是否满足以下要求：

- 安装了 NetScaler Insight Center 11.1 Build 47.14 或更高版本。
- 您已下载了 Citrix ADM 12.0 版本 57.24 .tgz 映像文件。

  > 注意：
  >
  > 您需要安装 Citrix ADM 12.0 版本 57.24，然后升级到最新的 Citrix ADM 13.0 版本。有关详细信息，请参阅升级。

- 您已下载了 Citrix ADM 13.0 最新版本的.tgz 映像文件。

硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	120 GB
	注意： Citrix 建议您使用 **500 GB** 以获得更好的性能。此外，Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序要求	
Citrix Hypervisor	6.2、6.5
VMware ESX	5.5、6.0

组件	要求
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu、Fedora

安装过程

要将 **NetScaler Insight Center** 迁移到 **Citrix ADM**，请执行以下操作：

1. 登录 NetScaler 智能分析中心的 shell 提示符。
2. 将 Citrix ADM 12.0 版本 57.24 下载到 */var/mps/mps_* 映像文件夹中。
3. 通过使用焦油 **-zxvf** 构建**-mas-12.0-57.24.tgz** 命令解除 **TGZ** 文件。

```
bash-3.2# tar -zxvf build-mas-12.0.57.24.tgz
```

4. 使用安装 Citrix ADM 。**/**安装 **mas** 命令。

```
bash-3.2# ./installmas
```

5. 安装 Citrix ADM 12.0 版本 57.24 后，您需要通过执行上述步骤升级到最新的 Citrix ADM 13.0 版本。

迁移后，在 NetScaler 智能分析中心清单中发现的所有 Citrix ADC 实例都将显示在 Citrix ADM 的 网络 **>** 实例部分中。但是，第一次时，需要手动轮询发现的设备上托管的虚拟服务器。

> 注意
>
> 在 Citrix ADM 中，默认情况下，管理和监视在发现的 Citrix ADC 实例中创建的两个虚拟服务器没有许可成本。要监视和管理两个以上的虚拟服务器，请安装所需的 Citrix ADM 许可证。有关更多详细信息，请参阅Citrix ADM 许可。

将 **Command Center** 配置迁移到 **Citrix ADM**

April 23, 2021

现在，您可以将 Command Center 配置迁移到 Citrix Application Delivery Management (ADM)，而不会丢失 Command Center 部署和 Citrix ADM 部署的现有配置、设置或数据。迁移过程完成后，您可以在 Citrix ADM 中查看迁移的命令中心配置。

注意事项

- 以下部署支持将 Command Center 配置迁移到 Citrix ADM：
  - Command Center 独立到 Citrix ADM 独立部署或 Citrix ADM 高可用性部署。
  - Command Center 高可用性到 Citrix ADM 独立部署或 Citrix ADM 高可用性部署。

  > 注意：在将 Command Center 独立或高可用性部署迁移到 Citrix ADM 独立或高可用性部署时，
  >
  > 您必须仅使用命令中心和 Citrix ADM 高可用性部署的主节点 IP 地址。
- 您可以在相同或不同的 Citrix ADM 部署上多次运行 Command Center 工具：
  - 每当您在同一 Citrix ADM 首次运行 Command Center 工具时，对于已迁移并存在于 Citrix ADM 中的配置，日志将显示为失败。
  - 如果从早些时候运行该工具到现在为同一 Citrix ADM 添加了任何新配置，则除新的自定义任务之外的所有此类配置都将迁移到 Citrix ADM。
- Citrix ADC、Citrix ADC SDX 和思杰 SDX 设备支持将 Command Center 配置迁移到 Citrix ADM。
- Command Center 和 Citrix ADM 之间的所有通信均采用 HTTPS 连接。
- 强烈建议在迁移 Command Center 配置之前备份 Citrix ADM 的现有数据。
- 命令中心迁移完成后，Citrix ADM 中会自动发现 Citrix ADC 的管理分区。

限制

以下 Command Center 配置不会从命令中心装置迁移到 Citrix ADM：

- 设备备份配置文件
- SD-WAN WO 设备配置文件中的超时详细信息
- 不会迁移事件和警报触发器下的以下详细信息：
  - 运行命令操作的中止详细信息
  - 运行任务详细信息
  - 不会迁移所有参数（严重性/类别/实例/失败对象）为空的触发器
  - 如果选择了实例的 HA 群集、主要和辅助状态，则不会迁移具有处于这三种状态的实例的触发器
- 不会迁移无说明的自定义任务
- 事件严重性设置
- 事件规则计划详细信息
- Syslog 阻止过滤器
- 配置任务详细信息

- 审核模板
- 无设备的审核策略
- 审核策略计划详细信息
- 组 RBAC 授权的范围设置
- 数据库监视和管理设置
- 性能自定义报告
- 性能阈值
- 故障/syslog/报告/实体监视的自定义视图
- AppFirewall 和 NS 网关报告及其计划详细信息
- SD-WAN WO 自动配置详细信息
- 高可用性设置
- 计划的系统备份设置
- 数据库重试设置
- Syslog 清除计划时间
- 所有统计数据，例如，所有模块的 syslog、事件和审核日志。

必备条件

在将命令中心配置迁移到 Citrix ADM 之前，请确保满足以下先决条件：

- 您运行的是 Command Center 5.2 Build 48.2 或更高版本。
- 您已安装并配置了 Citrix ADM 版本 12.0 版本 51.24 或更高版本。
- 仅由管理用户运行 Command Center 配置迁移。
- 要成功迁移自定义任务，必须在 Command Center 中填写说明字段。
- Command Center 与 Citrix ADM 之间的通信基于 NITRO。必须在 Command Center 和 Citrix ADM 上配置并打开必要的 SSL（安全套接字层）和 TLS（传输层安全）协议设置，以进行 NITRO 通信。

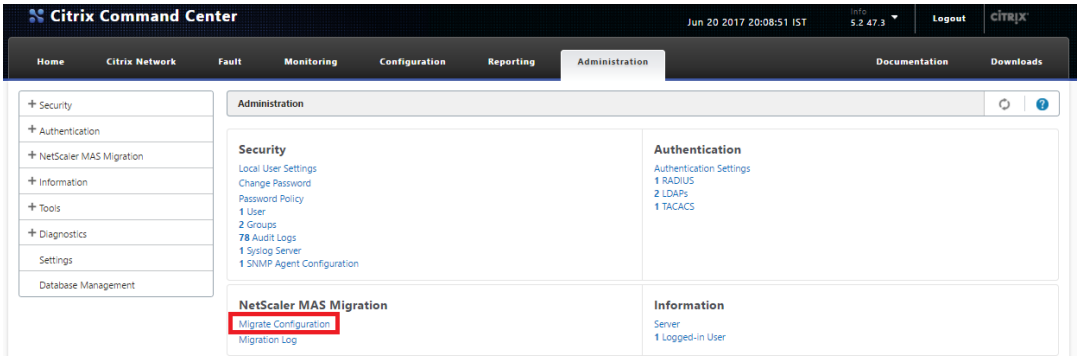
> 注意
>
> 如果您使用的是 Command Center 版本早于 5.2 版本 48.2，则必须将命令中心版本升级到 5.2 版本 48.2，然后将命令中心配置迁移到 Citrix ADM。有关升级 Command Center 装置的详细信息，请参阅 升级 Command Center。

迁移配置

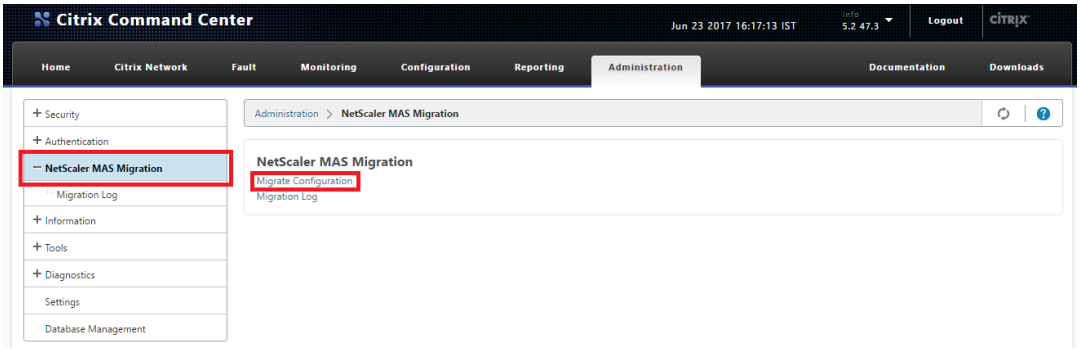
要将 Command Center 配置迁移到 Citrix ADM，您需要命令中心装置的 IP 地址和管理员凭据。

要将 **Command Center** 配置迁移到 **Citrix ADM**，请执行以下操作：

1. 在 Web 浏览器中，键入 Command Center 设备的 IP 地址。
2. 在“用户名”和“密码”字段中，键入管理员凭据并登录。
3. 成功登录后，在显示的屏幕上，选择“ 管理”选项卡，然后执行以下操作之一：
   - 在右窗格中的 **NetScaler MAS** 迁移下，选择 迁移配置，如下图所示。

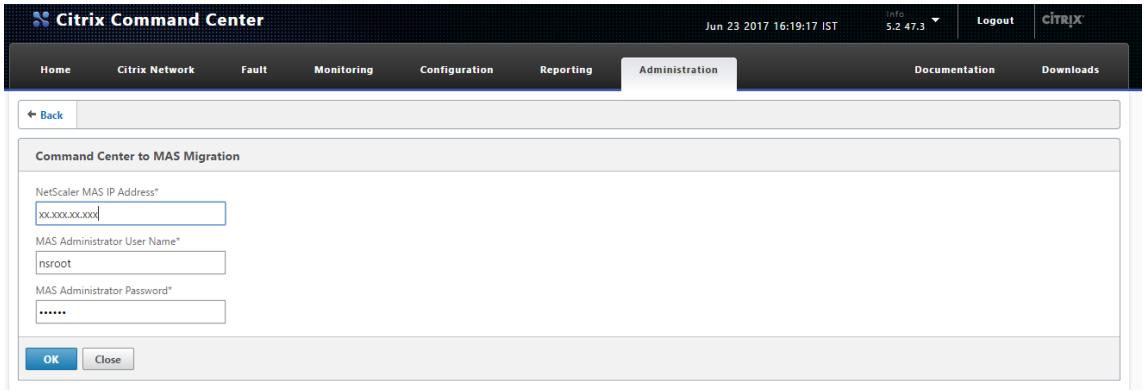


   - 在左窗格中，选择 **NetScaler MAS** 迁移，然后单击 迁移配置，如下图所示。

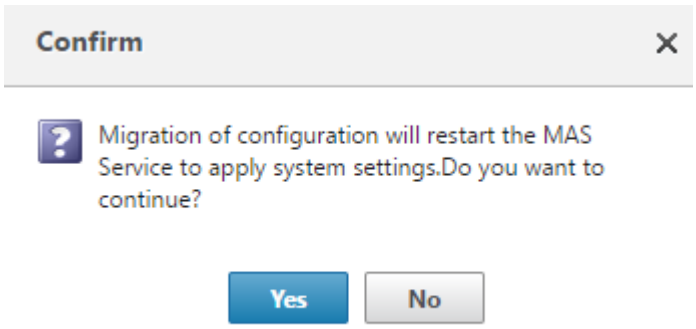


4. 在 命令中心到 **MAS** 迁移对话框中，输入 NetScaler MAS 服务器的 IP 地址和管理员凭据，然后单 击确定。

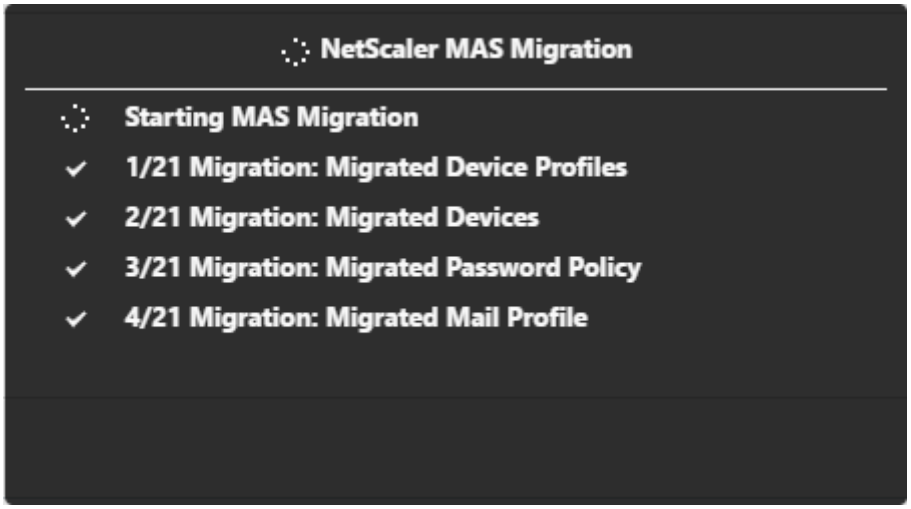
> 注意：
>
> 如果是 Citrix ADM 高可用性部署，请输入主节点 IP 地址。



5. 在确认提示时，单击 是。



屏幕上将报告迁移任务的进度。



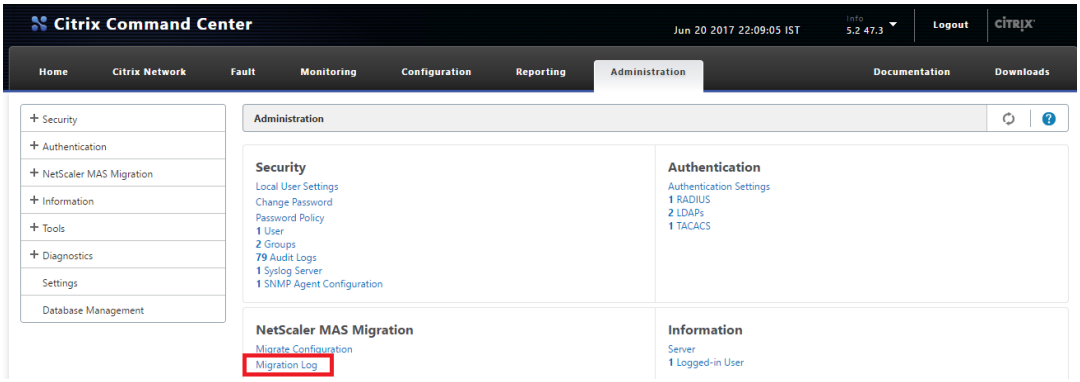
迁移配置操作将 Citrix ADM 部署的详细信息及其管理员凭据作为输入。然后，迁移配置操作将 Command Center 部署的配置迁移到 Citrix ADM 部署。

任务完成后，您可以从 Command Center 迁移日志和 Citrix ADM 数据验证迁移的命令中心配置。

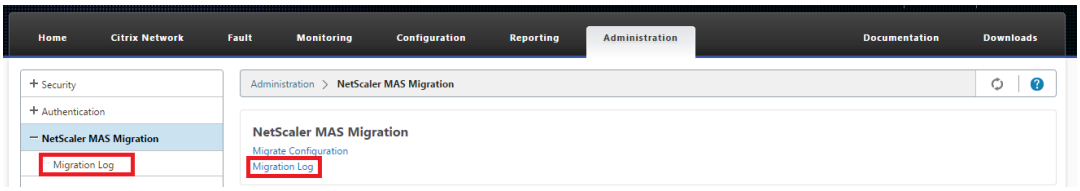
使用 **Command Center** 迁移日志确认迁移

1. 在命令中心 GUI 中的 “ 管理” 选项卡上，执行以下操作之一：

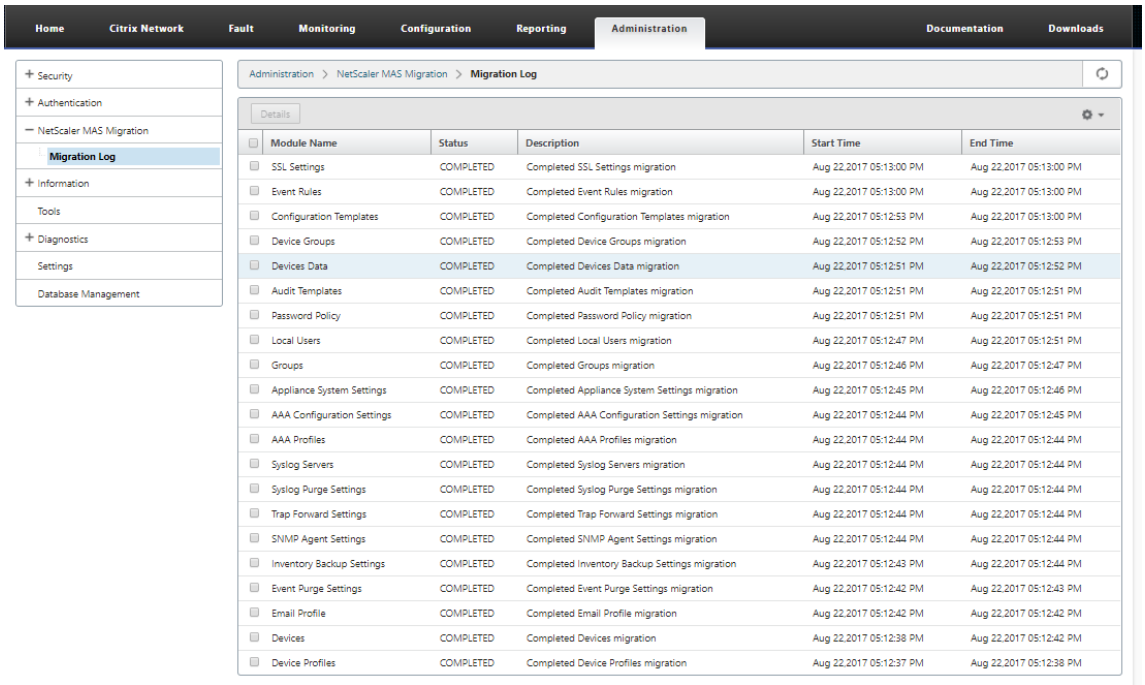
   - 在右窗格中的 **NetScaler MAS** 迁移下，单击 迁移日志。



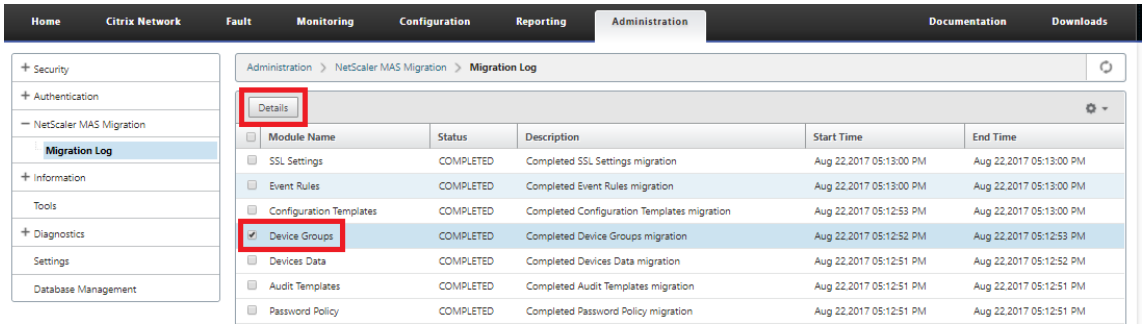
   - 在左窗格中，选择 **NetScaler MAS** 迁移，然后单击迁移日志。



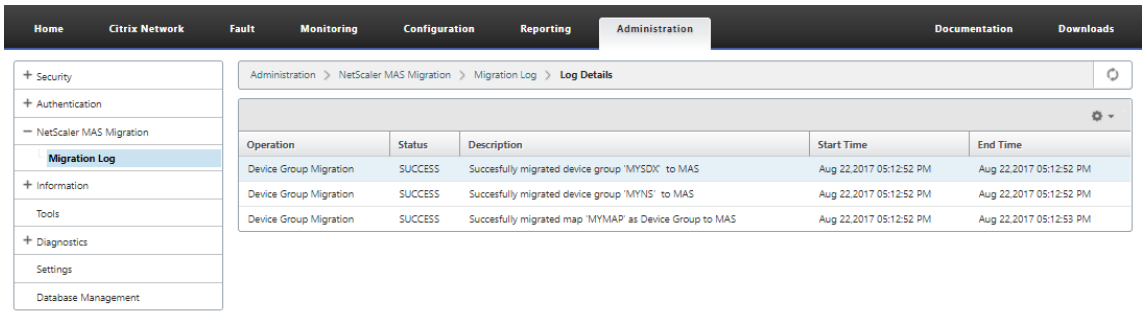
2. 查看迁移日志列表。



3. 要显示更多详细信息，请选择 模块名称，或者要显示特定模块的详细信息，请选择该模块，然后单击详 细信息。



4. 以下示例显示了某个选定模块的日志详细信息。



使用 **Citrix ADM** 验证迁移

在迁移过程中，Command Center 配置将迁移到 Citrix ADM，并在 Citrix ADM GUI 中显示为 Citrix ADM 配置。

迁移过程完成后，Citrix ADM 服务器将重新启动，并且可能会暂时停机。当 Citrix ADM 服务器启动并运行时，通过在浏览器的地址栏中键入 Citrix ADM 服务器的 IP 地址来访问 Citrix ADM GUI。

下表显示了迁移配置的 Citrix ADM 术语与 Command Center 使用的术语的对应方式。

Command Center 术语	Citrix ADM 术语
设备配置文件	实例配置文件
设备及其状态（例如托管/未托管）	实例及其状态（例如托管/未托管）
设备批注	实例批注
设备组	实例组
地图	实例组
事件和警报触发器	事件规则
内置和自定义任务命令	创建作业编辑器下的配置模板
计划审计策略	审核模板
密码策略	密码策略
用户（仅限本地用户）	系统用户

Command Center 术语	Citrix ADM 术语
组 *	系统组
身份验证配置文件和身份验证设置	身份验证配置文件和身份验证配置
电子邮件设置	电子邮件服务器/电子邮件通讯组列表
Syslog 服务器	Syslog 服务器
SSL 设置	SSL 设置
SNMP 代理配置	SNMP 管理器
陷阱转发设置	陷阱设置
事件清除设置	事件删除设置
清单设置	实例备份设置
Syslog 清除设置	Syslog 删除设置
设备网络设置，例如 DNS、NTP 和时区	Citrix ADM 网络设置，如 DNS、NTP 和时区

* 在 Command Center 具有所有权限的组将作为 Citrix ADM 中具有“管理员”角色的组进行迁移。所有其他 Command Center 组将迁移为 Citrix ADM 中具有“只读”角色的组。

将 **Citrix ADM** 与 **Citrix Director** 集成

April 23, 2021

Director 与 Citrix ADM 集成，用于网络分析和性能管理。

- 网络分析可从 Citrix ADM 获取 HDX Insight 分析报告，并提供网络的应用程序和桌面视图。通过此功能，Director 对部署中的 ICA 通信提供高级分析视图。
- 性能管理提供历史保留和趋势报告。通过历史数据保留与实时评估，可以创建趋势报告，其中包括容量趋势和运行状况趋势。

将 Citrix ADM 与控制器集成后，HDX Insight 报告在控制器中为您提供以下信息：

- “Trends”（趋势）页面中的“Network”（网络）选项卡显示对部署中的应用程序、桌面和用户产生的延迟和带宽影响。
- 用户详细信息页可以显示特定于某个特殊用户会话的延迟和带宽信息。

必备条件

HDX Insight 到 **Citrix ADM** 迁移的硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8
存储空间	500 GB。Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

软件要求

在迁移到 Citrix ADM 虚拟设备之前，请验证是否满足以下要求：

- 已安装 Director 1811 版
- 已安装 NetScaler HDX Insight 10.1 版或更高版本
- HDX Insight 和 Citrix ADM 支持 Citrix VDA 版本 7.0 及更高版本
- Citrix Workspace 虚拟应用程序和桌面 7.0 版及更高版本支持 Citrix 工作区
- 请确保有 MAC Citrix Receiver for Mac 11.8 版及更高版本以及 Windows Citrix Receiver for Windows 14.0 版和更高版本，以显示准确的 ICA RTT 指标
- 安装了 Citrix ADM 11.0 版及更高版本。有关如何安装 Citrix ADM 的详细信息，请参阅 部署 Citrix ADM。

限制

- 此功能的可用性取决于组织的许可证和管理员权限。
- ICA 会话的往返程时间 (RTT) 可正确显示 Citrix Receiver for Windows 3.4 或更高版本以及 Citrix Receiver for Mac 11.8 或更高版本的数据。对于早期版本的 Receiver，数据无法正确显示。
- 在 “Trends”（趋势）视图中，不会针对 VDA 7 之前的版本收集 HDX 连接登录数据。对于更早版本的 VDA，图表数据将显示为 0。
- 对于已经有存储空间低于 500 GB 的外部硬盘的部署，不能添加其他硬盘。

> 注意
>
> - 有关控制器的详细信息以及有关将 Citrix ADM 与控制器集成的步骤，请参阅https://docs.citrix.com/en-us/xenapp-and-xendesktop/7-15-ltsr/director/hdx-insight.html。

> - 有关 HDX Insight 的详细信息，请参阅http://docs.citrix.com/en-us/xenapp-and-xendesktop/7-11/director/hdx-insight.html。

将额外的磁盘附加到 **Citrix ADM**

April 23, 2021

Citrix Application Delivery Management (ADM) 存储需求根据您的 Citrix ADM 大小估计确定。默认情况下，Citrix ADM 为您提供 120 GB 的存储容量。如果存储数据需要超过 120 GB 的 GB，则可以附加额外的磁盘。

> 注意
>
> - 在初始部署 Citrix ADM 时，估计存储需求并将额外的磁盘附加到服务器。
> - 对于 Citrix ADM 单服务器部署，除了默认磁盘之外，您只能将一个磁盘连接到服务器。
> - 对于 Citrix ADM 高可用性部署，必须向每个节点附加一个额外的磁盘。两个磁盘的大小必须相同。
> - 如果之前连接了容量较低的外部磁盘，则必须先删除该磁盘，然后再连接新磁盘。
> - 您可以附加容量超过 2 TB 的额外磁盘。如有必要，磁盘的大小也可以小于 2 TB。
> - Citrix 建议对 Citrix ADM 部署使用固态驱动器 (SSD) 技术。

本文档介绍了关于附加额外的新磁盘、创建分区和调整其他磁盘大小的以下场景：

1. 附加一个新的额外磁盘
2. 启动磁盘分区工具
3. 在新的额外磁盘中创建分区
4. 调整现有额外磁盘的大小
5. 删除附加磁盘上的分区

在独立的 **Citrix ADM** 中附加额外的磁盘

执行以下步骤将磁盘连接到虚拟机：

1. 关闭 Citrix ADM 虚拟机。
2. 在 Hypervisor 中，将所需磁盘大小的额外磁盘连接到 Citrix ADM 虚拟机。

   新连接的较大磁盘存储数据库数据和 Citrix ADM 日志文件。现在，现有的 120 GB 默认磁盘用于存储核心文件、操作系统日志文件等。
3. 启动 Citrix ADM 虚拟机。

Citrix ADM 磁盘分区工具

Citrix ADM 现在提供了 **Citrix ADM** 磁盘分区工具，这是一种新的命令行工具。此工具的功能详细说明如下：

1. 使用该工具，您可以在新添加的额外磁盘中创建分区。
2. 您还可以使用此工具调整现有额外磁盘的大小。但是，现有的外部磁盘不得超过 2 TB。

   > 注意
   >
   > - 在不丢失数据的情况下，无法调整现有磁盘的大小超过 2 TB。这是由于平台上已知的限制。
   > - 要创建大于 2 TB 的存储容量，必须删除现有分区并使用此新工具创建分区。

3. 使用此新工具，您可以明确地在磁盘上执行任何分区操作。该工具为您提供了对磁盘和相关数据的清晰可见性和控制。

   > 注意：
   >
   > 您只能在连接到 Citrix ADM 服务器的其他磁盘上使用此工具。不能使用此工具在主（默认）120 GB 磁盘中创建分区。

启动磁盘分区工具

1. 使用 SSH 客户端（如 PuTTY）打开到 Citrix ADM 的 SSH 连接。
2. 使用管理员凭据登录到 Citrix ADM。
3. 切换到 shell 提示符并键入：

```
/mps/DiskPartitionTool.py
<!--NeedCopy-->
```

> 注意
>
> 对于高可用性部署中的 Citrix ADM，您必须在两个节点中启动该工具，并在将磁盘连接到相应的虚拟机后创建分区或调整分区大小。

在新的附加磁盘中创建分区

创建命令用于在添加新的辅助磁盘时创建分区。使用 “remove” 命令删除现有分区后，也可以使用此命令在现有辅助磁盘上创建分区。

```
(dpt): ?create
Creates a new partition on the attached disk. A swap partition of size 32GB is also created automatically.

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

> ** 注
>
> 意：** 使用磁盘分区工具创建分区时，没有 2 TB 的大小限制。该工具可以创建大于 2 TB 的分区。对磁盘进行分区时，将自动添加大小为 32 GB 的交换分区。然后，主分区将使用磁盘上的所有剩余空间。

命令运行后，将创建 GUID 分区表 (GPT) 分区方案。此外，还会创建一个 32 GB 的交换分区和数据分区来使用其余空间。然后在主分区上创建一个新的文件系统。

> 注意
>
> 此过程可能需要几秒钟，并且不能中断该过程。

```
(dpt): create

The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

```
Creating GPT partition scheme...
da1 created

Creating partition 1 using (456287933) blocks. Leaving aside 32G for swap...
da1p1 added

Creating partition 2 for swap using remaining 32G...
da1p2 added

Formatting the new partition. This may take some time (~20 seconds). Please be patient and don't interrup the process...
```

创建命令完成后，虚拟机将自动重新启动，以便装载新分区。

```
Create Done.
VM has to be rebooted for the new partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

重新启动后，新分区以 /var/mps 挂载。


```
bash-3.2# df -k
Filesystem  1024-blocks     Used     Avail Capacity  Mounted on
/dev/md0         456046   374346     72580    84%    /
devfs                 1        1         0   100%    /dev
procfs                4        4         0   100%    /proc
fdescfs               1        1         0   100%    /dev/fd
/dev/da0s1a     1623950   284466   1209568    19%    /flash
/dev/da0s1e   116073918 2812298 103975708     3%    /var
/dev/da1p1    495168802   43854 455511444     0%    /var/mps
```

添加的交换分区在 “create” 命令的输出中显示为交换空间。

```
CPU:  0.0% user,  0.0% nice,  0.0% system,  0.7% interrupt, 99.3% idle
Mem: 89M Active, 21M Inact, 123M Wired, 16M Cache, 74M Buf, 6965M Free
Swap: 37G Total, 37G Free
```

> 注意
>
> 创建分区后，该工具将重新启动虚拟机。

调整现有附加磁盘中的分区大小

您可以使用 **resize** 命令调整连接的（辅助）磁盘的大小。您可以调整具有 master boot record （MBR) 或 GPT 方案的磁盘大小。磁盘的大小必须小于 2 TB，最大为 2 TB。

> 注意
>
> - “resize” 命令旨在在不丢失任何现有数据的情况下运行。但是，Citrix 建议您先将此磁盘中的关键数据备份到外部存储，然后再尝试调整大小。在调整大小操作过程中磁盘数据可能会损坏的情况下，数据备份非常有用。
> - 在调整分区大小时，确保以 100 GB 的空间增量增加磁盘空间。这种增量增加可确保您不必更频繁地调整大小。

```
(dpt): ?resize
Resizes existing partition on attached disk to utilize all space available. Pre-conditions are:
1. Secondary disk exists and capcity of disk < 2TB
2. A single partition exists on secondary disk and there is atleast 100GB to gain by resizing

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

“resize” 命令会检查所有前提条件，如果满足所有前提条件并在您同意调整大小后继续执行。它会停止访问磁盘的进程，其中包括 Citrix ADM 子系统、PostgreSQL 数据库进程和 Citrix ADM 监视进程。进程停止后，磁盘将被卸载，以便为调整大小做好准备。调整大小是通过扩展分区以占用完整的可用空间，然后增加文件系统来完成的。如果磁盘上存在交换分区，则会在调整大小后将其删除并在磁盘末尾重新创建。交换分区将在文档的 “ 创建” 命令部分中讨论。

> 注意
>
> “不断增长的文件系统”过程可能需要一些时间才能完成，并注意在进行过程中不要中断该过程。调整分区大小后，该工具将重新启动虚拟机。

```
(dpt): resize

********************
***  WARNING !!  ***
********************
Resizing the partition/disk works without affecting the existing data.
However we strongly recommend you to manually backup your data before proceeding with the operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to resize (Y/N): y
```

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to resize existing partition.
Disabling swap on partition: /dev/da1p2
Deleting swap partition: da1p2
Resizing partition da1p1...
da1p1 resized

Adding a swap partition da1p2...
da1p2 added

Formatting the newly added portions of the partition. This may take some time (~10 seconds). Please be patient and don't
 interrup the process...
```

调整大小过程中的所有中间步骤（停止应用程序、调整磁盘大小、增加文件系统）都显示在控制台上。进程完成后，将看到以下消息。

```
Resize Done.
VM has to be rebooted for the resized partition to be used.
Rebooting VM now...

*** FINAL System shutdown message from nsroot@ns-mgmt-system ***

System going down IMMEDIATELY
```

重新启动后，可以使用 “df” 命令观察到大小的增加。以下是增加大小后的前后的详细信息：

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374864     72062    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1662048 105125958     2%    /var
/dev/da1s1a   152329216 3082226 137060654     2%    /var/mps
```

```
bash-3.2# df -k
Filesystem  1024-blocks    Used     Avail Capacity  Mounted on
/dev/md0         456046  374838     72088    84%    /
devfs                 1       1         0   100%    /dev
procfs                4       4         0   100%    /proc
fdescfs               1       1         0   100%    /dev/fd
/dev/da0s1a     1623950  284468   1209566    19%    /flash
/dev/da0s1e   116073918 1666800 105121206     2%    /var
/dev/da1s1a   304651668 3137954 277141582     1%    /var/mps
```

删除其他磁盘中的分区

辅助磁盘上的现有分区的大小可调整到 2 TB。这是由于对分区的已知限制造成的。如果您想要大于 2 TB 的磁盘，请连接新磁盘并使用磁盘分区工具对其进行分区。您还可以使用 remove 命令 删除现有分区，然后创建分区。

> 注意
>
> 删除现有分区会删除所有现有数据。因此，在使用此命令之前，任何关键数据都必须备份到外部存储。


```
(dpt): ?remove
Removes existing partition from attached disk.

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

运行 “remove” 命令要求您进行确认，一旦确认，它将停止使用辅助磁盘的所有进程（例如 ADM 子系统、PostgreSQL 进程和 ADM 监视器）。如果交换分区存在并且在分区上启用了交换，则交换将被禁用。

```
(dpt): remove

********************
***  WARNING !!  ***
********************
All data on the partition/disk will be PERMANENTLY ERASED as a result of this operation.
Backup the data before proceeding with this operation.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.

Are you sure you want to continue (Y/N): y
```

键入 “y” 时，该命令将卸载磁盘并删除磁盘上的所有分区。

```
Unmounting partition: /dev/da1p1 from: /var/mps
OK to remove existing partitions.
Disabling swap on partition: /dev/da1p2
Removing all partitions from: da1
Remove Done.
Rebooting VM now...
```

> 注意
>
> 删除分区后，该工具将重新启动虚拟机。

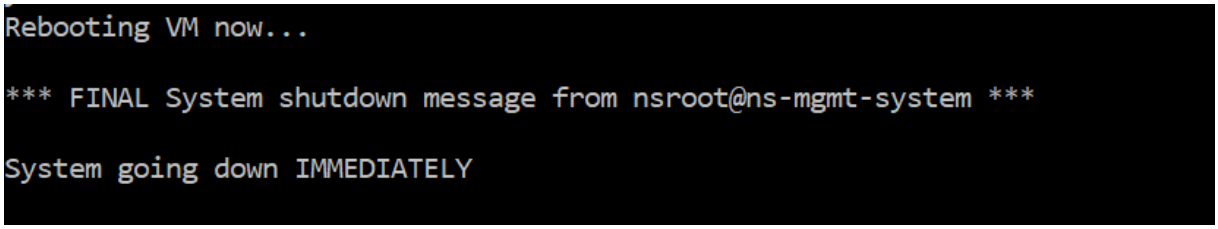
重新启动虚拟机

创建分区或调整分区大小时，或者创建交换文件时，重新启动虚拟机。更改仅在重新启动后生效。为此，工具中提供了重新启动命令。

```
(dpt): ?reboot
Reboot the VM. Note: VM has to be rebooted after new partition is created, existing one is resized or swap file is creat
ed.
The VM is rebooted automatically after these operations. If the automatic reboot does not happen, then this command can
be used to reboot the VM.
```

系统会提示您进行确认，一旦确认，它将停止所有进程（例如 ADM 子系统、PostgreSQL 进程和 ADM 监视器）。然后重新启动虚拟机。

```
(dpt): reboot
Are you sure you want to reboot the VM (Y/N): y
```

创建磁盘数据的备份文件

以下是在调整分区大小或删除分区之前备份 Citrix ADM 数据的步骤。

> 注意：
>
> 创建备份文件需要磁盘空间。Citrix 建议您确保在运行备份命令之前有足够的可用磁盘空间（50%或更多）。

1. 停止 ADM。

```
/mps/masd stop
<!--NeedCopy-->
```

2. 停止 PostgreSQL。

```
su -l mpspostgres /mps/scripts/pgsql/stoppgsql_smart.sh
<!--NeedCopy-->
```

3. 停止 ADM 监视器。

```
/mps/scripts/stop_mas_monit.sh
<!--NeedCopy-->
```

4. 创建一个塔球。

```
cd /var
tar cvfz /var/mps/mps_backup.tgz mps
<!--NeedCopy-->
```

> ** 注
>
> 意 ** 此操作需要时间，具体取决于要备份的数据的大小。

5. 生成校验和。

```
md5 mps_backup.tgz > mps_backup_checksum
<!--NeedCopy-->
```

6. 远程复制程序包和校验和。


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

7. 验证复制的程序包是否正确。生成传输文件的校验和并与源校验和进行比较。

8. 从 ADM 虚拟机中删除压缩包。

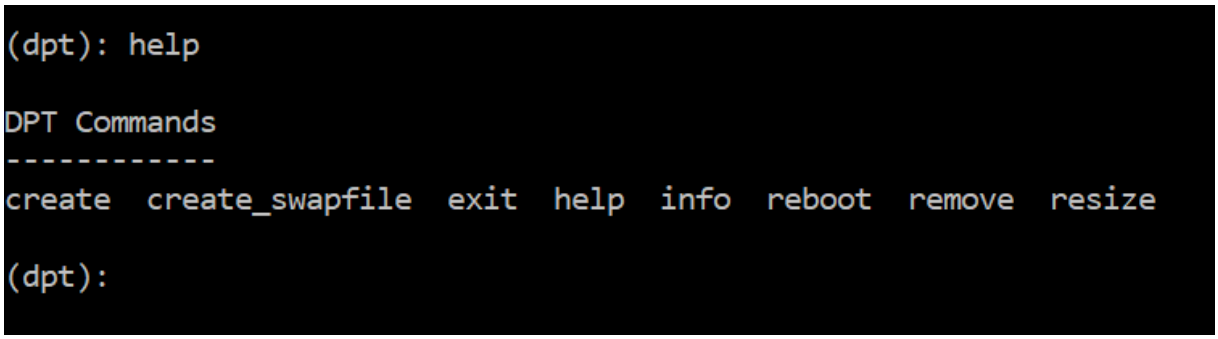
```
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

其他命令

除了前面列出的命令之外，还可以在工具中使用以下命令：

帮助命令：

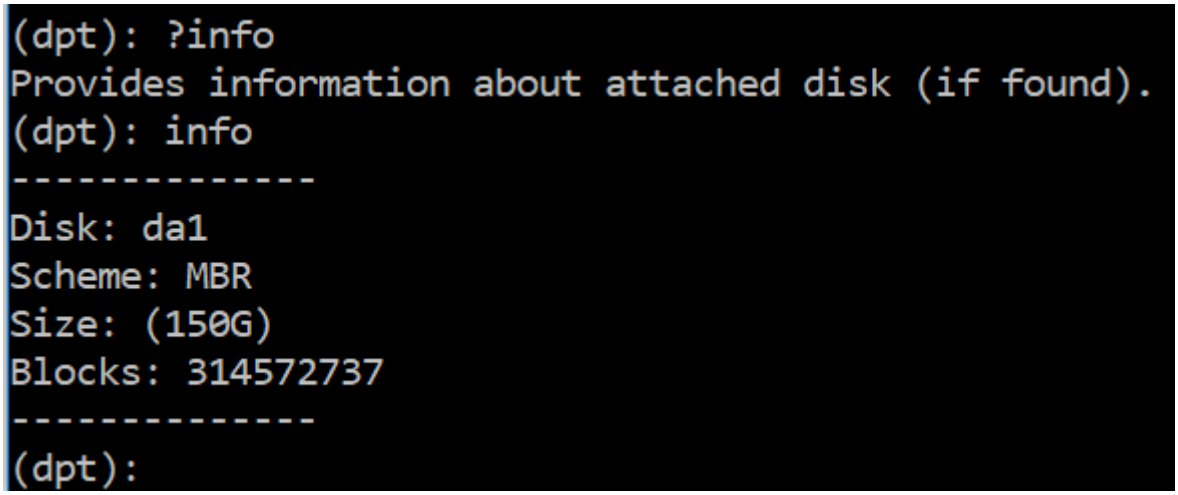
要列出支持的命令，请键入 **help** 或 **?** ，然后按回车键。要获得每个命令的进一步帮助，请按下 帮助或 **?** 后跟命令名称，然后按 Enter 键。



信息命令：

info 命令提供有关连接的辅助磁盘（如果磁盘存在）的信息。该命令提供设备名称、分区方案、人类可读形式的大小以及磁盘块数量。该方案可以是 MBR 或 GPT。MBR 方案意味着使用较早版本的 Citrix ADM 对磁盘进行分区。基于 MBR/GPT 的分区可以调整大小，但不能超过 2 TB。GPT 分区方案意味着使用 Citrix ADM 12.1 或更高版本对磁盘进行了分区。

> 注意 GPT 分区可以大于 2 TB
>
> ，但在创建时。但是，在创建具有较小大小的磁盘后，您不能将磁盘大小调整为大于 2 TB 的大小。这是平台的已知限制。



创建交换文件命令：

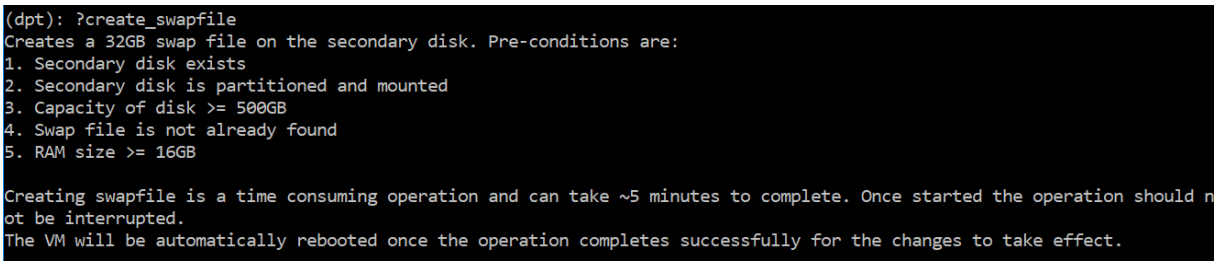
Citrix ADM 主磁盘上的默认交换分区为 4 GB，因此默认交换空间为 4 GB。对于 Citrix ADM 的默认内存配置（2 GB），此交换空间就足够了。但是，在使用较高内存配置运行 Citrix ADM 时，需要在磁盘上分配更多的交换空间。

> 注意
>
> 交换分区通常是在安装操作系统期间在硬盘驱动器 (HDD) 上创建的专用分区。此类分区也称为交换空间。交换分区用于模拟附加主内存的虚拟内存。

默认情况下，在早期版本的 Citrix ADM 中添加的辅助磁盘没有创建交换分区。“create_swapfile” 命令适用于使用没有交换分区的旧版 Citrix ADM 创建的辅助磁盘。命令会检查以下内容：

- 辅助磁盘的存在
- 正在装载的磁盘
- 磁盘的大小（至少 500 GB）
- 交换文件的存在

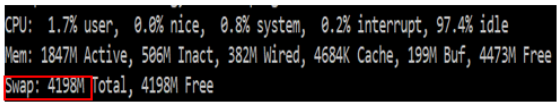
只有当内存大于或等于 16 GB 时，而不是在内存不足时，才有用 “create_swapfile” 命令。因此，此命令还会在继续创建交换文件之前检查内存。

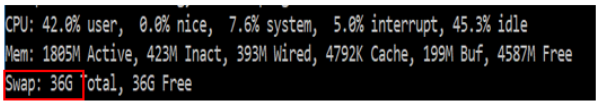


如果满足所有条件，并且用户同意继续操作，则会在辅助磁盘上创建一个 32 GB 的交换文件。交换文件创建过程需要几分钟才能完成，并注意在进行过程中不要中断该过程。成功完成后，将重新启动以使交换文件生效。


```
Creating swapfile. This may take some time (~5 mins). Please be patient and don't interrupt the process...
32768+0 records in
32768+0 records out
34359738368 bytes transferred in 724.061475 secs (47454173 bytes/sec)

Changing permissions for created swapfile...

Create (swapfile) Done.
VM has to be rebooted for the newly created swapfile to take effect.
```

重新启动后，可以使用 top 命令观察到交换量的增加。





退出命令：

要退出工具，请键入 exit 并按 **Enter** 键。

```
(dpt): exit
bash-3.2#
```

将其他磁盘连接到部署在高可用性中的 Citrix ADM

让我们考虑一种情况，即您已在没有任何辅助磁盘的高可用性设置中配置了一对 Citrix ADM 服务器。此外，让我们考虑您添加了 2 个或更多 Citrix ADC 实例，检查并确保所有进程都在运行。您可能希望在此设置中向虚拟机添加辅助磁盘。在高可用性设置中，必须向两个节点添加附加磁盘，如以下任务中所述：

1. 假定 Citrix ADM 节点名称为 “ADM_ 主节点” 和 “ADM_ 辅助节点名称。“
2. 首先，在 ADM_Senter 上运行分区工具，然后添加辅助磁盘。添加磁盘后，虚拟机将重新启动。
3. 重新启动后关闭 ADM_ 辅助设备。
4. 现在，在 ADM_Primary 上运行分区工具并添加辅助磁盘。添加磁盘后，虚拟机将重新启动。

   确保向两个节点添加容量相似的磁盘。例如，如果将容量为 500 GB 的磁盘添加到主节点，请向辅助节点添加容量为 500 GB 的磁盘。
5. ADM_ 主节点重新启动后，检查它是否是主节点。
6. 现在启动 ADM_ 辅助节点。确保它已作为辅助节点出现，并且数据库已同步。
7. 确认所有数据仍然存在。

要增加两个节点上的 **RAM** 容量，请执行以下操作：

1. 关闭 ADM_ 次级并根据需要增加 RAM 大小。不要重新启动节点。
2. 关闭 ADM_ 主要内存并根据需要增加内存大小。

确保在两个节点上均匀增加 RAM 大小。例如，如果将主节点上的 RAM 大小增加到 16 GB，则在辅助节点上也执行相同的操作。

3. 重新启动主数据器。
4. 重新引导 ADM_ 主节点后，检查它是否是主节点。
5. 现在启动 ADM_ 辅助节点。重新启动后，请确保它已经作为辅助，并且数据库同步正常工作。
6. 现在确认所有数据仍然存在。

> 注意：添加辅助磁盘
>
> 后，主节点需要一些时间才能启动。此外，向两个节点添加辅助磁盘和增加 RAM 容量的整个过程都需要两个节点停机一段时间。计划此维护活动时，请考虑此停机时间。

配置

April 23, 2021

只能使用 GUI 访问 Citrix ADM 服务器。您必须访问 GUI 才能添加实例、管理和监视实例和应用程序、查看分析以及配置 Citrix ADM 服务器。

工作站必须安装受支持的 Web 浏览器才能访问配置实用程序和控制板。

支持以下浏览器。

Web 浏览器	版本
Internet Explorer	11.0 及更高版本
Google Chrome	Chrome 19 及更高版本
Safari	Safari 5.1.1 及更高版本
Mozilla Firefox	Firefox 3.6.25 及更高版本

要访问 **Citrix ADM GUI**，请执行以下操作：

使用管理员凭据登录到 Citrix ADM。

登录到 Citrix ADM 后，您必须执行以下操作才能开始：

- 将实例添加到 Citrix ADM。如果要管理和监视这些实例，则必须将实例添加到 Citrix ADM 服务器。
- 在虚拟服务器上启用分析。要查看应用程序通信流的分析数据，必须在接收特定应用程序的流量的虚拟服务器上启用分析功能。
- 在 Citrix ADM 上配置 NTP 服务器。您必须在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将其时钟

与 NTP 服务器同步。

- 配置系统设置以获得最佳 Citrix ADM 性能。在开始使用 Citrix ADM 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

将实例添加到 **Citrix ADM**

April 23, 2021

实例是要从 Citrix ADM 发现、管理和监视的 Citrix 设备或虚拟设备。如果要管理和监视这些实例，则必须将实例添加到 Citrix ADM 服务器。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 中：

- Citrix ADC MPX
- Citrix ADC VPX
- Citrix ADC SDX
- Citrix ADC CPX
- Citrix ADC BLX
- Citrix Gateway
- Citrix SD-WAN

您可以在首次设置 Citrix ADM 服务器时或以后添加实例。然后，必须指定 Citrix ADM 可用于访问实例的实例配置文件。

> 注意
>
> - Citrix ADM 使用 Citrix ADC 实例的 NetScaler IP (NSIP) 地址进行通信。有关在 Citrix ADC 实例和 Citrix ADM 之间必须打开的端口的信息，请参阅 端口。
> - 对于思杰 SD-WO 和 Citrix SD-WAN EE 实例，Citrix ADM 使用实例的管理 IP 地址进行通信。
> - 要了解 Citrix ADM 如何发现实例，请参阅 发现实例。

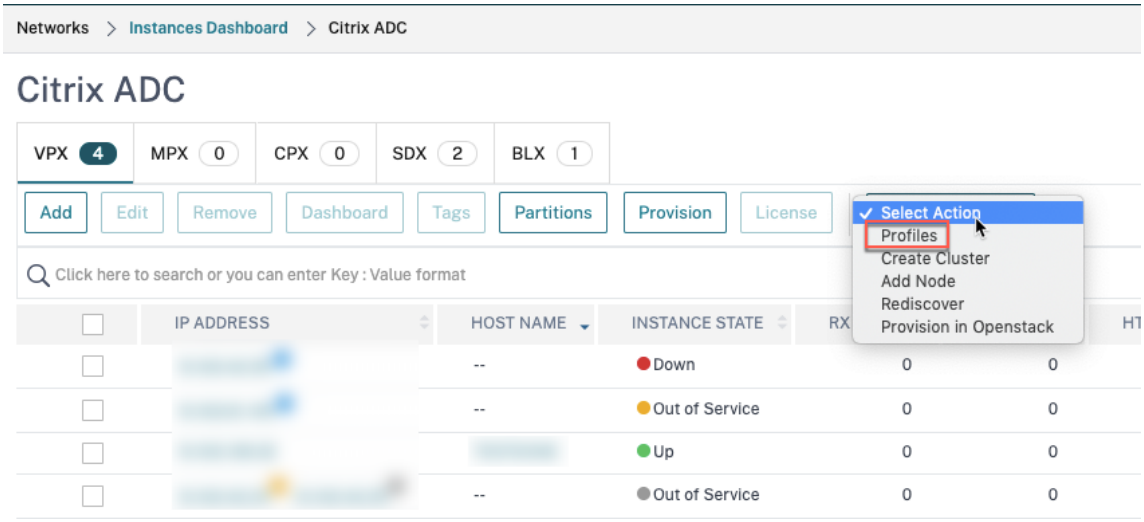
如何创建 **Citrix ADC** 配置文件

Citrix ADC 配置文件包含要添加到 Citrix ADM 的实例的用户名、密码、通信端口和身份验证类型。对于每个实例类型，都有一个默认的配置文件。例如，`nsroot` 是 Citrix ADC 实例的默认配置文件。默认配置文件通过使用默认 Citrix ADC 管理员凭据来定义。如果更改了实例的默认管理员凭据，可以为那些实例定义自定义实例配置文件。如果在发现实例后更改实例的凭据，则必须编辑实例配置文件或创建配置文件，然后重新发现实例。

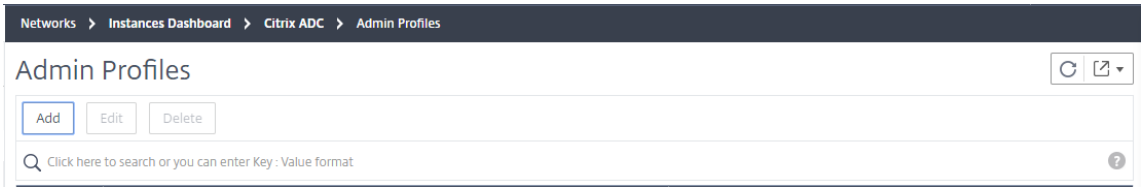
您可以从 “ 实例” 页面或在添加或更改实例时创建 Citrix ADC 配置文件。

要从 “实例” 页创建 **Citrix ADC** 配置文件，请执行以下操作：

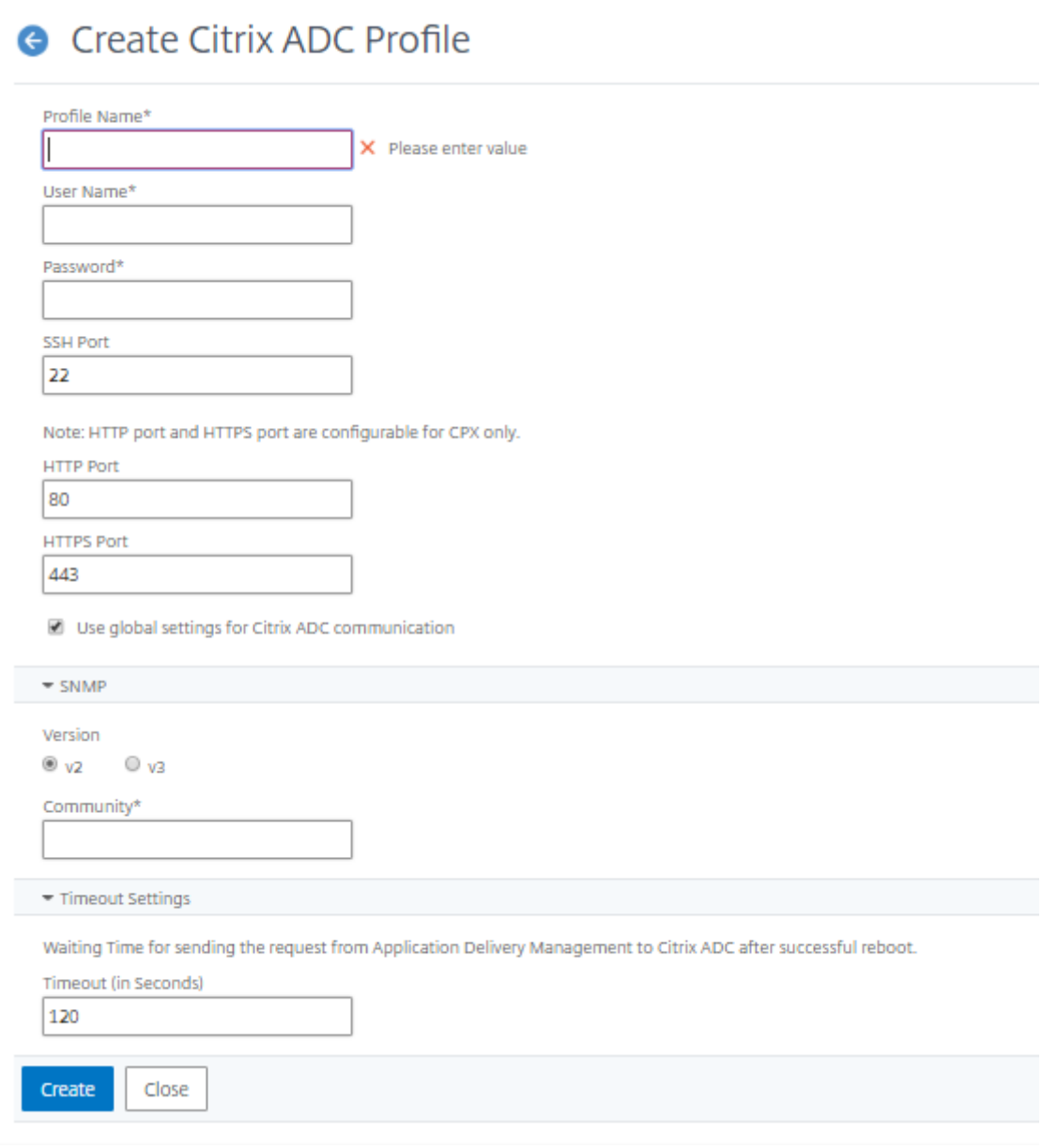
1. 导航到 网络 **>** 实例。
2. 选择一个实例。例如，Citrix ADC。
3. 在 Citrix ADC 页面上的 选择操作下，选择 配置文件。



4. 在 “ 管理员配置文件” 页面上，选择 “ 添加”。



5. 在 “ 创建 **Citrix ADC** 概要文件” 页上，执行以下操作：



a) 配置文件名称：指定 Citrix ADC 实例的配置文件名称。

b) 用户名：指定要登录到 Citrix ADC 实例的用户名。

c) 密码：指定登录到 Citrix ADC 实例的密码。

d) **SSH** 端口：为 Citrix ADM 和 Citrix ADC 实例之间的 SSH 通信指定端口。

e) **HTTP** 端口：指定 Citrix ADM 和 Citrix ADC 实例之间的 HTTP 通信端口。

> ** 注
>
> 意 ** 默认 HTTP 端口为 80。您还可以指定可能已在 Citrix ADC CPX 实例中配置的非默认或自定义 HTTP 端口。自定义 HTTP 端口只能用于 Citrix ADM 和 Citrix ADC CPX 之间的通信。

f) **HTTPS** 端口：为 Citrix ADM 和 Citrix ADC 实例之间的 HTTPS 通信指定端口。

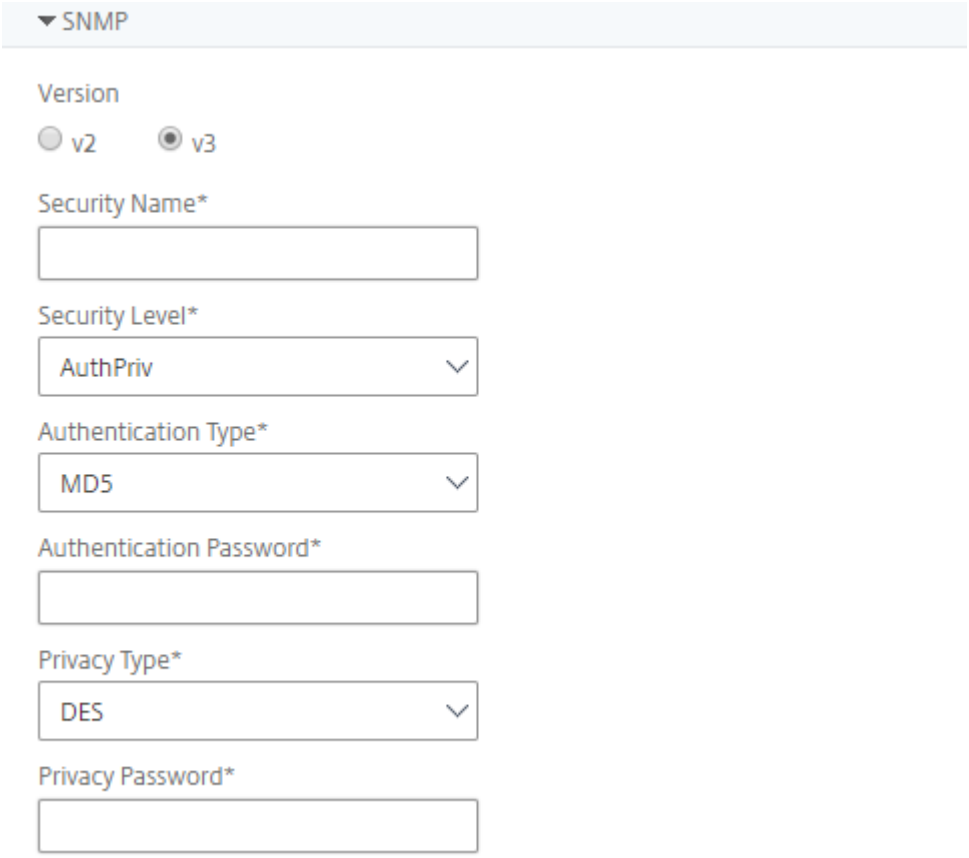
> ** 注
>
> 意 ** 默认的 HTTPS 端口为 443。您还可以指定可能已在 Citrix ADC CPX 实例中配置的非默认或自定义 HTTPS 端口。自定义 HTTPS 端口只能用于 Citrix ADM 和 Citrix ADC CPX 之间的通信。

g) 使用 **Citrix ADC** 通信的全局设置：如果要使用系统设置进行 Citrix ADM 和 Citrix ADC 实例之间的通信，请选择此选项，否则选择 HTTP 或 https。

h) **SNMP** 版本：选择 **SNMPv2** 或 **SNMPv3** ，然后执行以下操作：

i. 如果选择 SNMPv2，请指定用于身份验证的 社区名称。

ii. 如果选择 SNMPv3，请指定 安全名称和 安全级别。根据安全级别，选择 身份验证类型和 隐私类型。



> 注意
>
> 对于 Citrix ADC SDX，只支持 **SNMPv2** 。

i) 超时设置：指定 Citrix ADM 在重新启动后向 Citrix ADC 实例发送连接请求之前必须等待的时间。

j) 选择 创建。

将 **ADC** 实例添加到 **Citrix ADM**

您可以在首次设置 Citrix ADM 服务器时或以后添加实例。

要添加实例，您必须指定每个 Citrix ADC 实例的主机名或 IP 地址，或指定 IP 地址范围。

对于 SD-WAN 实例，则指定每个实例的 IP 地址，或指定 IP 地址范围。请注意，Citrix ADM 仅支持 Citrix SD-WAN WO 和 Citrix SD-WAN PE 版本。

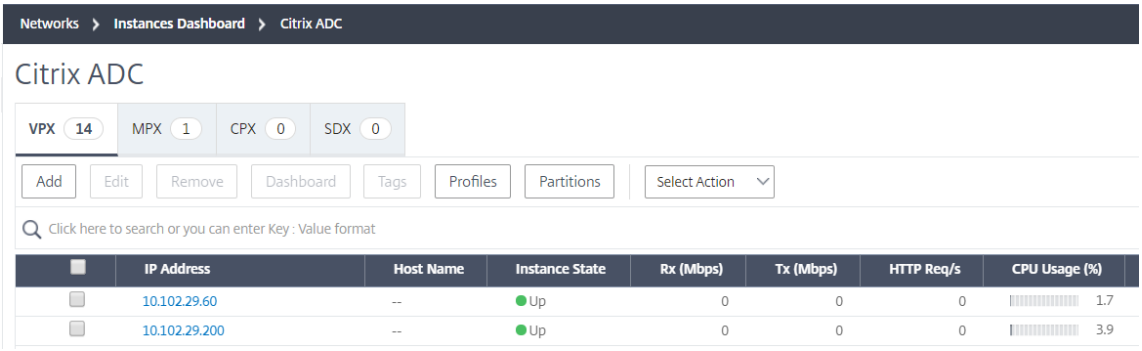
> 注意
>
> - 要添加在群集中配置的 Citrix ADC 实例，必须指定群集 IP 地址或群集设置中的任何一个单独节点。但是，在 Citrix ADM 上，群集仅由群集 IP 地址表示。
> - 对于设置为 HA 对的 Citrix ADC 实例，添加一个实例时，将自动添加该对中的另一个实例。

如果在高可用性模式中设置了两个 Citrix ADM 服务器，则在添加实例时，流量源通过 ADM 浮动 IP 地址。

当您从使用本地代理配置的远程数据中添加实例时，流量源是通过 ADM Agent 进行的。

要将实例添加到 **Citrix ADM**，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到 “网络” > “实例” > “ **Citrix ADC**”。选择要添加的实例类型（例如，Citrix ADC VPX），然后单击添加。



3. 选择以下选项之一：
   - 输入设备 **IP** 地址-对于 Citrix ADC 实例，请指定每个实例的主机名或 IP 地址，或指定 IP 地址范围。

     如果要使用 SNIP 发现 ADC HA 对，请确保启用独立网络配置 (INC) 模式。并使用以下格式指定 SNIP 地址：

     ```
     <SNIP of primary instance>#<SNIP of secondary instance>
     <!--NeedCopy-->
     ```

     例如，`10.10.10.11##10.10.10.12`

     对于 SD-WAN 实例，则指定每个实例的 IP 地址，或指定 IP 地址范围。
   - **Import from file**（从文件导入）- 上载包含要添加的所有实例的 IP 地址的文本文件。
4. 在 配置文件名称中，选择相应的实例配置文件，或通过单击 + 图标创建新配置文件。

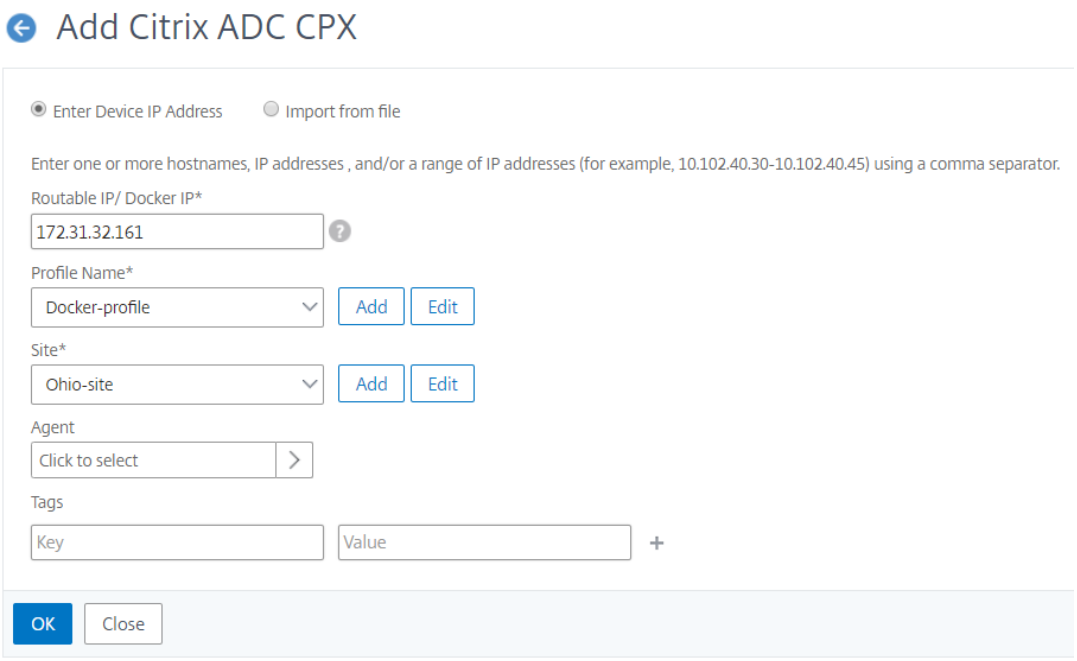
5. 在 站点中，选择要添加实例的位置，或通过单击 **+** 图标创建新位置。
6. 单击 **“确定”** 以启动向 Citrix ADM 添加实例的过程。

> 注意
>
> 如果要重新发现实例，请导航到 “ 网络” > “实 例” > “ **Citrix ADC**”。选择实例类型（例如 VPX）并选择要重新发现的实例，然后从 “ 选择操作” 列表中单击 “ 重新发现”。

将 **ADC CPX** 实例添加到 **Citrix ADM**

对 Citrix ADM 进行了增强，以支持在 CPX 功能方面已经完成的改进。现在，Citrix ADC CPX 实例通过为 CPX 提供 IP 地址和设备配置文件，将其添加到 Citrix ADM 中。CPX 实例的添加过程现在类似于在 ADM 中添加其他 ADC 类型（如 VPX 或 MPX）。此外，CPX 在 ADM 中的注册也得到了加强。当 CPX 启动时，Citrix ADM 会自动发现并注册 CPX 实例。不再通过 Docker 主机发现 CPX 实例。

1. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ”，然后单击 “ **CPX** ” 选项卡。
2. 单击 添加可在 Citrix ADM 中添加新的 CPX 实例。
3. 此时将打开 “ 添加 **Citrix ADC CPX** ” 页。输入以下参数的值：
   a) 您可以通过提供 CPX 实例的可访问 IP 地址或托管 CPX 实例的 Docker 容器的 IP 地址来添加 CPX 实例。
   b) 选择 CPX 实例的配置文件。
   c) 选择要部署实例的站点。
   d) 选择座席。
   e) 作为一个选项，您可以输入实例的键值对。通过添加键值对，您可以轻松地在以后搜索实例。



> 注意
>
> 对于 Citrix ADC CPX 实例，您必须在创建 CPX 实例配置文件时指定主机的 **HTTP**、**HTTPS**、**SSH** 和 **SNMP** 端口详细信息。您还可以在 “ 起始端口” 和 “端口 数” 字段中指定主机发布的端口范围。

4. 单击确定。

在 **Citrix ADM** 中添加独立的 **Citrix ADC BLX** 实例

独立的 Citrix ADC BLX 实例是在专用主机 Linux 服务器上运行的单个实例。

1. 导航到网络 > 实例 > **Citrix ADC**。
2. 在 **BLX** 选项卡中，单击 添加。
3. 从 “ 实例类型” 列表中选择 “ 独立” 选项。
4. 在 **IP** 地址字段中，指定 BLX 实例的 IP 地址。
5. 在 主机 **IP** 地址字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
6. 在 配置文件名称列表中，为 BLX 实例选择适当的配置文件，或创建配置文件。

   要创建配置文件，请单击 添加。

   > 重要信息：
   >
   > 确保您在配置文件中指定了正确的 Linux 服务器主机用户名和密码。

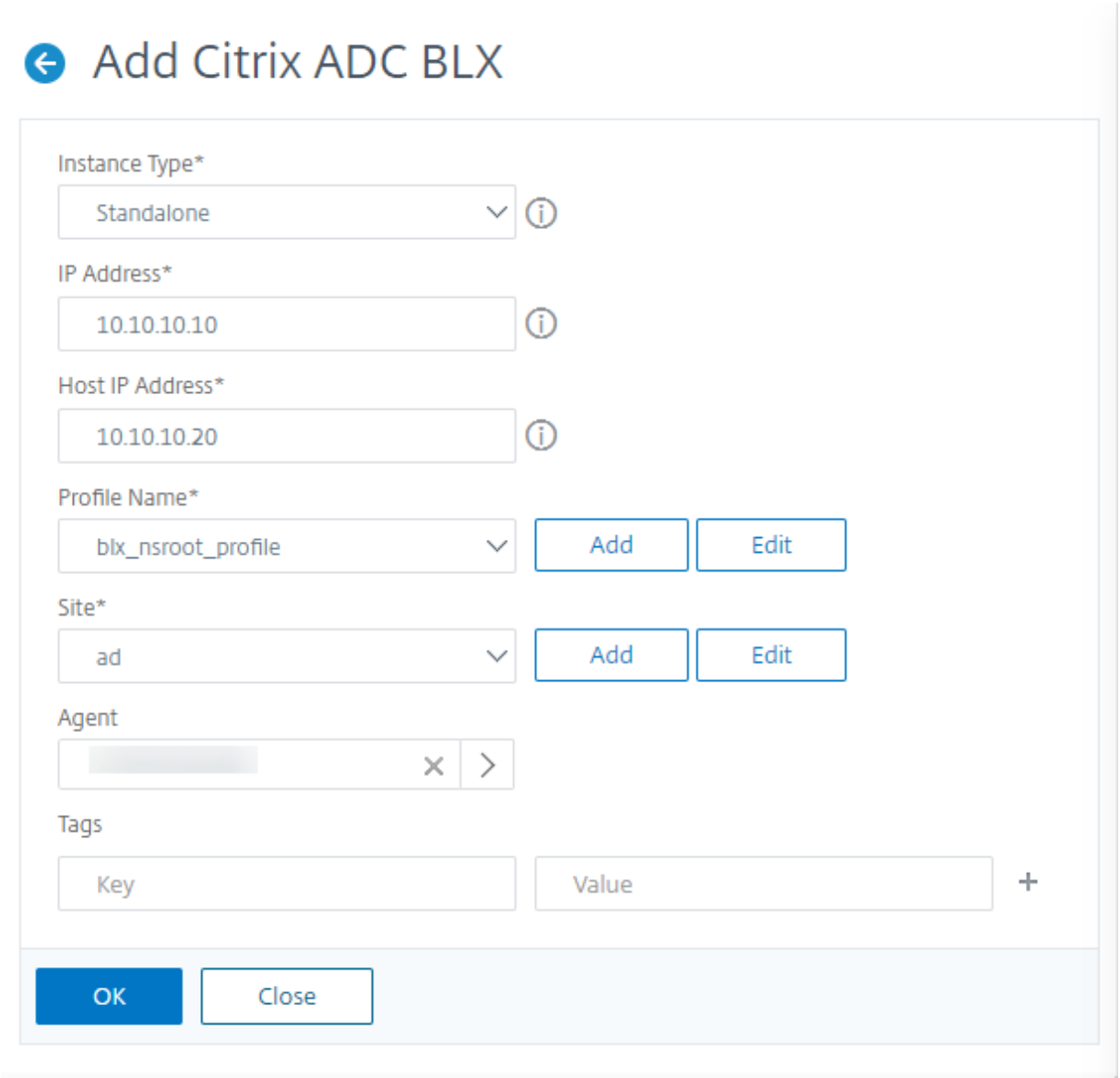
7. 在 “ 站点” 列表中，选择要添加实例的站点。

   如果要添加站点，请单击 添加”。

8. 在 代理列表中，选择要与实例关联的 Citrix ADM 代理。

   如果在 Citrix ADM 上只配置了一个代理，则默认情况下选择该代理。

9. 单击确定。



在 **Citrix ADM** 中添加高可用性 **Citrix ADC BLX** 实例

在不同主机 Linux 服务器上运行的高可用性 Citrix ADC BLX 实例。Linux 服务器不能托管多个 BLX 实例。

1. 在 **BLX** 选项卡中，单击 添加。
2. 从 “ 实例类型” 列表中选择 “ 高可用性” 选项。
3. 在 **IP** 地址字段中，指定 BLX 实例的 IP 地址。
4. 在 主机 **IP** 地址字段中，指定托管 BLX 实例的 Linux 服务器的 IP 地址。
5. 在对 等 **IP** 地址字段中，指定对等 BLX 实例的 IP 地址。
6. 在 对等主机 **IP** 地址字段中，指定托管对等 BLX 实例的 Linux 服务器的 IP 地址。

7. 在 配置文件名称列表中，为 BLX 实例选择适当的配置文件，或创建配置文件。

   要创建配置文件，请单击 添加。

   > 重要信息：
   >
   > 确保您在配置文件中指定了正确的 Linux 服务器主机用户名和密码。

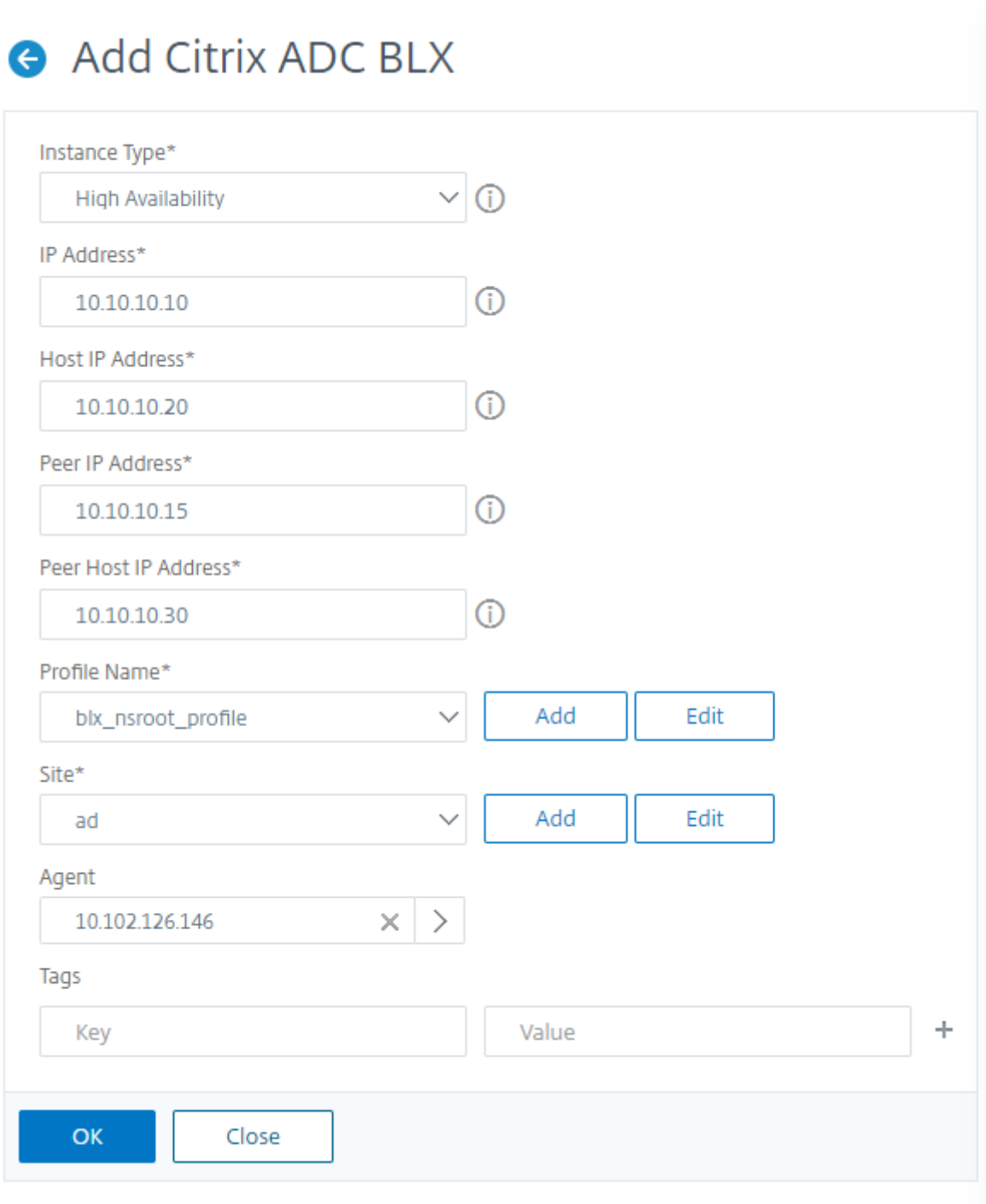
8. 在 “ 站点” 列表中，选择要添加实例的站点。

   如果要添加站点，请单击 添加”。

9. 在 代理列表中，选择要与实例关联的 Citrix ADM 代理。

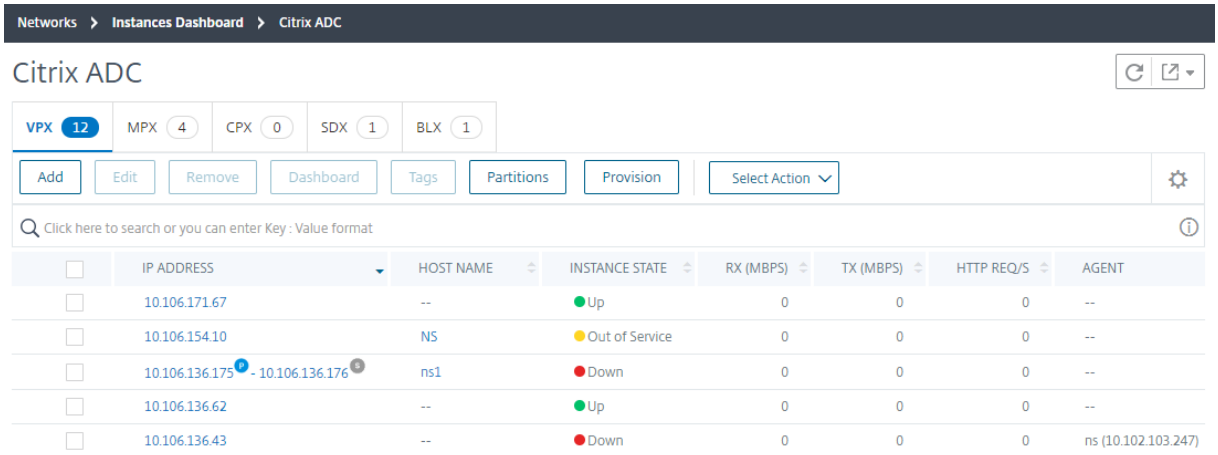
   如果在 Citrix ADM 上只配置了一个代理，则默认情况下选择该代理。

10. 单击确定。



从 **Citrix ADM** 访问实例图形用户界面

1. 导航到 网络 **>** 实例 > **Citrix ADC**。
2. 选择要访问的实例类型（例如，VPX、MPX、CPX、SDX 或 BLX）。
3. 单击所需的 Citrix ADC IP 地址或主机名。



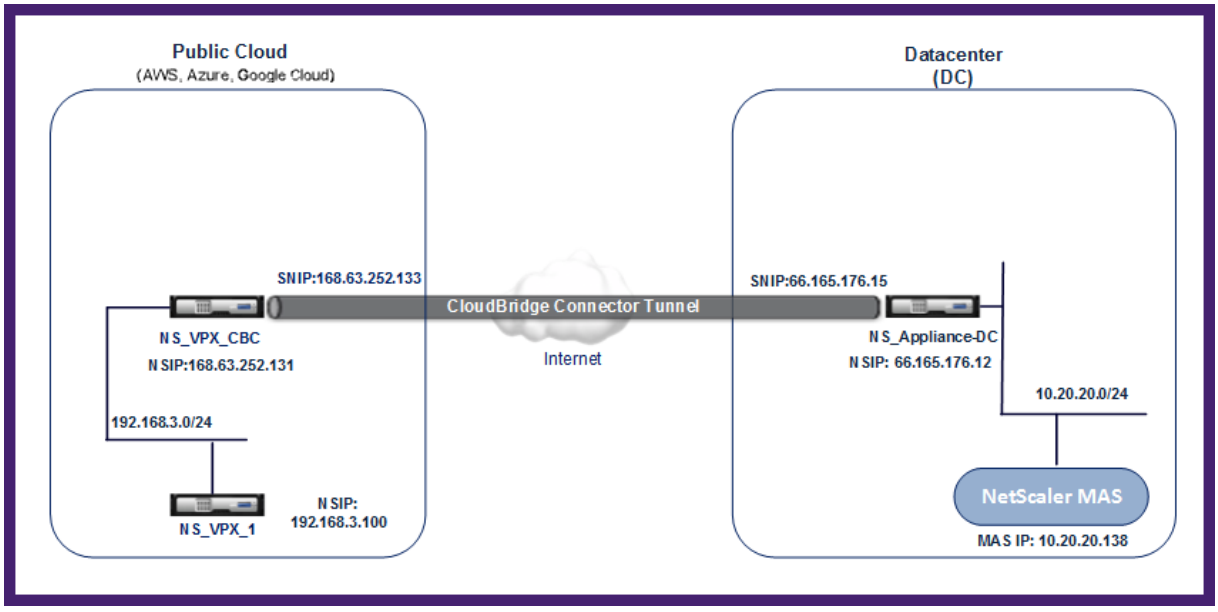
选定实例的 GUI 将显示在弹出窗口中。

将部署在云中的 **Citrix ADC VPX** 实例添加到 **Citrix ADM**

April 23, 2021

您可以使用 Citrix ADM 管理和监视部署在公有云（如 Amazon Web Services (AWS) 或微软 Azure）上的 Citrix ADC VPX 实例。您需要在 Citrix ADM 和部署在公有云上的 Citrix ADC VPX 实例之间建立第 3 层连接。要建立第 3 层连接，您可以使用 Citrix CloudBridge 连接器、Citrix SD-WAN、直接连接到 AWS、Azure 中的 VPN 或第三方连接器（如 Equinix）等解决方案。

以下示例拓扑使用 Citrix CloudBridge Connector 在 Citrix ADM 和云中部署的 Citrix ADC VPX 实例之间实现第 3 层连接。

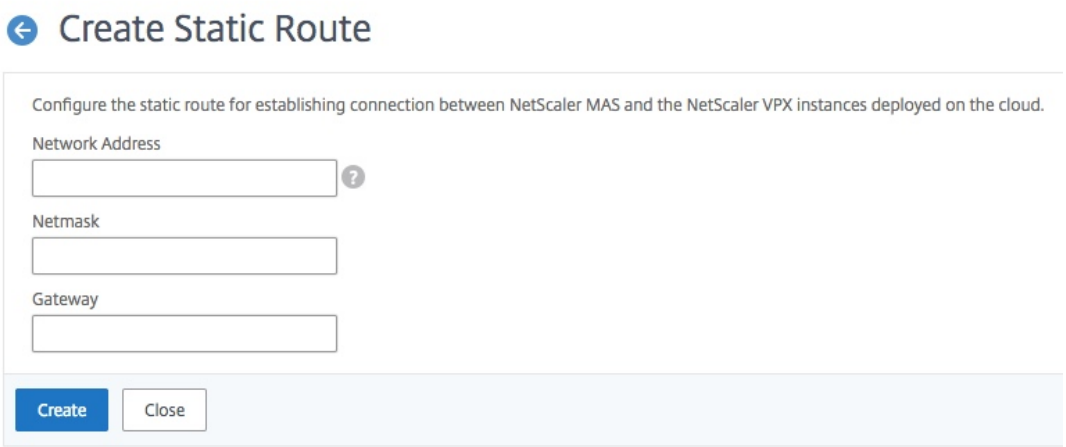


Citrix CloudBridge Connector 隧道在数据中心 DC 的 Citrix ADC 设备 NS_Appliance DC 和公有云中的 Citrix

ADC 虚拟设备 (VPX) NS_VPX_CBC 之间建立。NS_ 应用程序直流和 NS_VPX_CBC 可实现 Citrix ADM 与部署在公有云中的 Citrix ADC VPX 实例 NS_1 之间的通信。建立通信后，您可以在 Citrix ADM 中发现 NS_VPX_1。

要配置此拓扑，请执行以下操作：

1. 在公有云中安装、配置和启动 Citrix ADC VPX 实例。
   - 相关说明，请参阅在 AWS 上安装 Citrix ADC VPX。
   - 相关说明，请参阅在微软 Azure 上安装 Citrix ADC VPX。
2. 部署和配置 Citrix ADC 物理设备，或在数据中心的虚拟化平台上预配和配置 Citrix ADC 虚拟设备 (VPX)。
   - 相关说明，请参阅在 Citrix Hypervisor 上安装 Citrix ADC VPX 实例。
   - 相关说明，请参阅在 VMware ESXi 上安装 Citrix 虚拟设备。
   - 相关说明，请参阅在微软 Hyper-V 上安装 Citrix ADC 虚拟设备。
3. 在数据中心和公有云之间配置 Citrix CloudBridge Connector。相关说明，请参阅配置 Citrix CloudBridge Connector。
4. 配置用于在 Citrix ADM 和部署在云中的 Citrix ADC VPX 实例之间建立连接的静态路由，如下所示：
   a) 登录到 Citrix ADM。
   b) 导航到 **“系统” > “静态路由”**，然后单击 “ 添加”。



   c) 在 “ 网络地址” 字段中，输入要通过连接器从 Citrix ADM 建立静态路由的网络地址。
   d) 在 “ 网络掩码” 字段中，输入网络的网络掩码。
   e) 在 **Gateway** 字段中，输入网关的地址。
5. 通过指定公有云中 Citrix ADC VPX 实例的 IP 地址范围，将 Citrix ADC VPX 云实例添加到 Citrix ADM。有关详细说明，请 将实例添加到 Citrix ADM。

在虚拟服务器上管理许可并启用分析

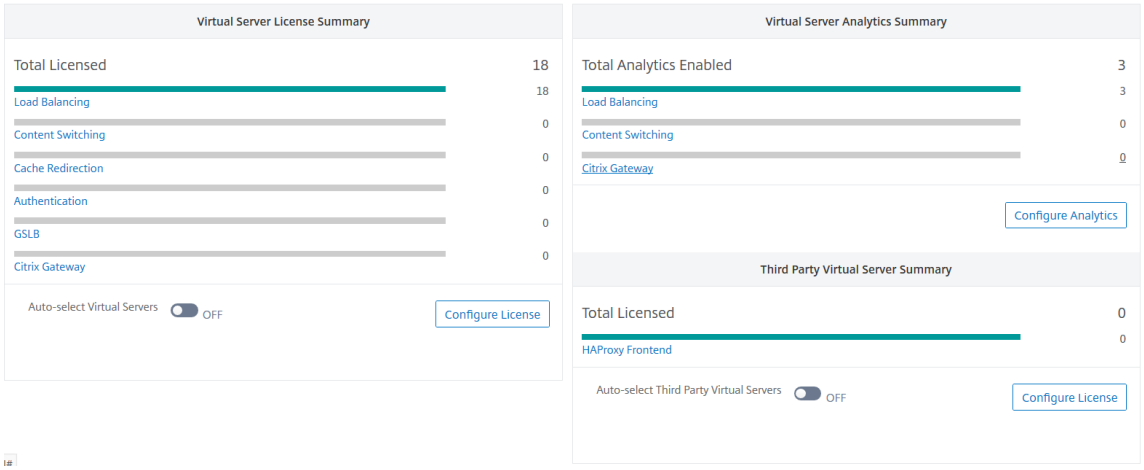
April 23, 2021

> 注意
>
> 以下启用分析的信息和过程仅适用于 Citrix ADM 版本为 **13.0** 版本 **41.x** 或更高版本时。如果您的 Citrix ADM 版本早于 **13.0** 版本 **36.27**，请参阅启用分析。

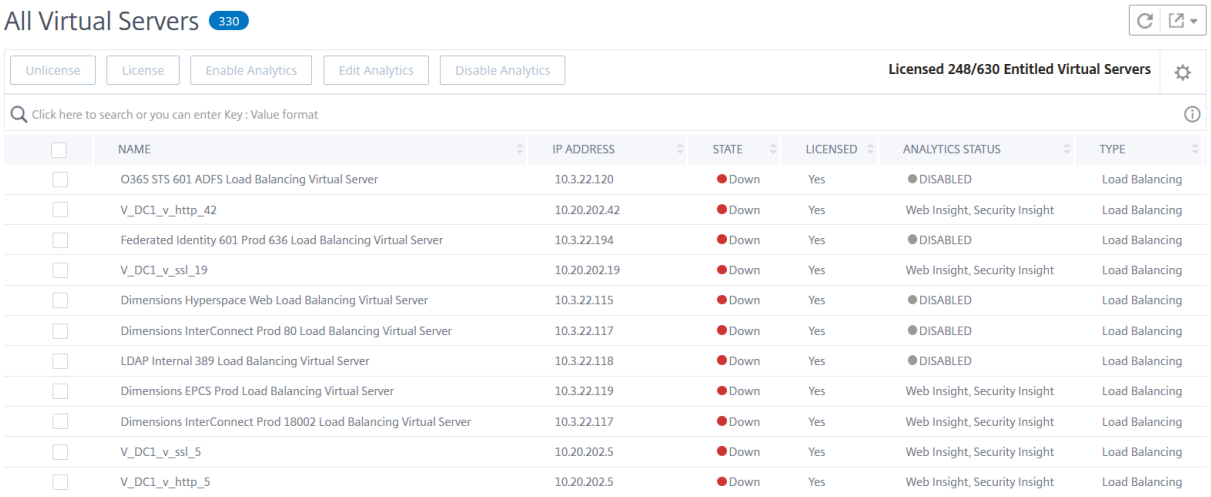
简化了启用分析的过程。现在，您可以在单个工作流中授予虚拟服务器许可并启用分析。

导航至 “ 系统” > “ 许可和分析”，以：

- 查看 虚拟服务器许可摘要
- 查看 虚拟服务器分析摘要



单击 “ 配置许可证” 或 “ 配置分析” 时，将显示 “ 所有虚拟服务器” 页。



在 所有虚拟服务器页面上，您可以：

- 为未许可的虚拟服务器应用许可证

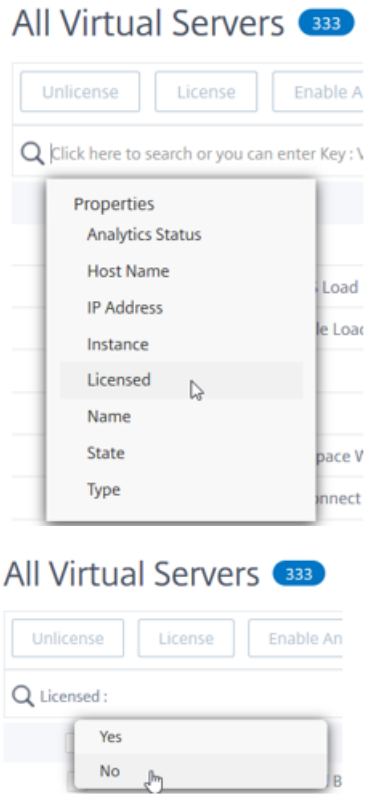
- 删除许可虚拟服务器的许可证
- 在许可虚拟服务器上启用分析
- 编辑分析
- 禁用分析

> 注意
>
> 用于启用分析的支持虚拟服务器包括负载平衡、内容交换和 Citrix Gateway。

管理虚拟服务器上的许可

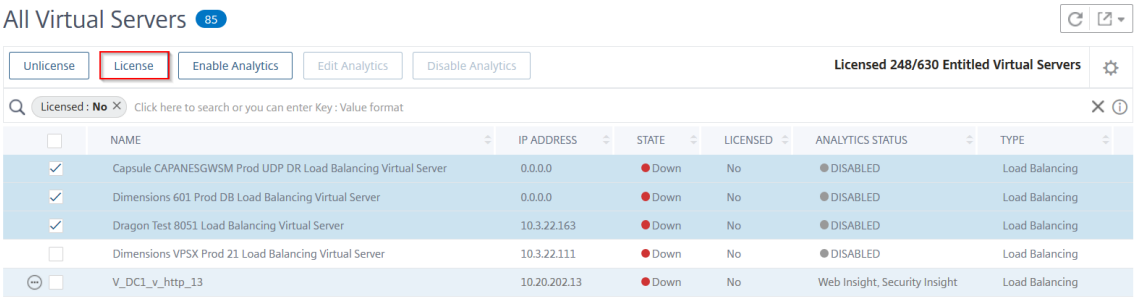
要对虚拟服务器进行许可，请从 所有虚拟服务器页面执行以下操作：

1. 单击搜索栏，选择 “ 许可”，然后选择 “ 否”。



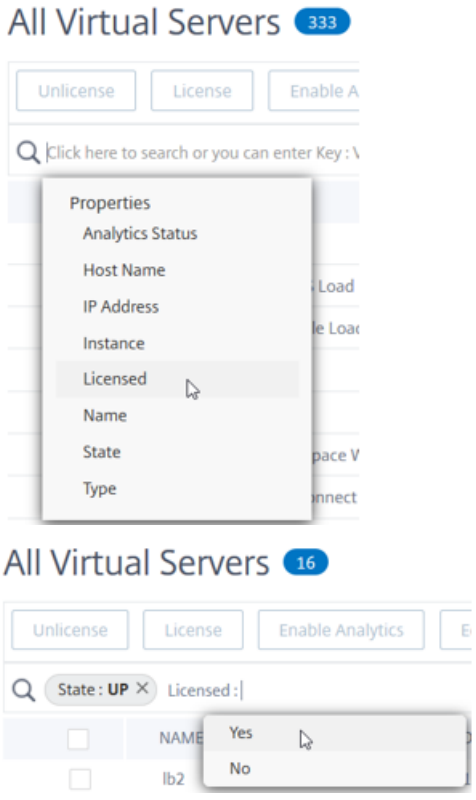
   现在应用筛选器，并且仅显示未许可的虚拟服务器。

2. 选择虚拟服务器，然后单击 许可证。

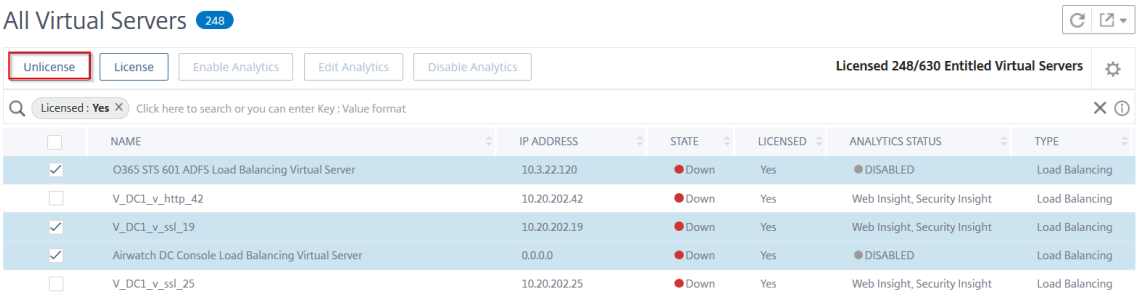


要取消虚拟服务器的许可，请从 所有虚拟服务器页面执行以下操作：

1. 单击搜索栏，选择 “ 许可”，然后选择 “ 是”。



2. 选择虚拟服务器，然后单击 “ 取消许可证”。



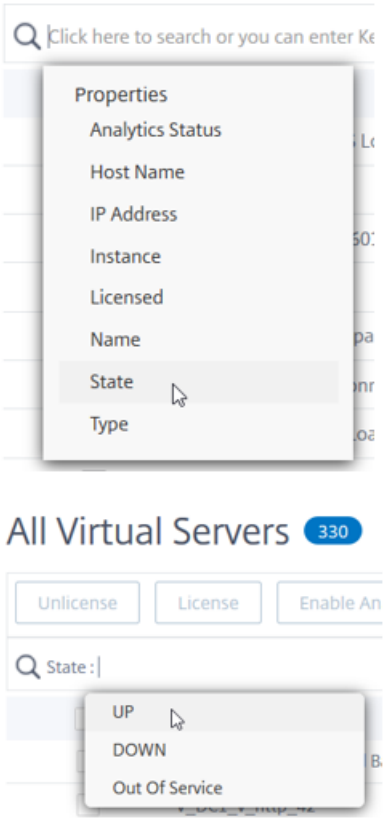
启用分析

以下是为虚拟服务器启用分析的先决条件：

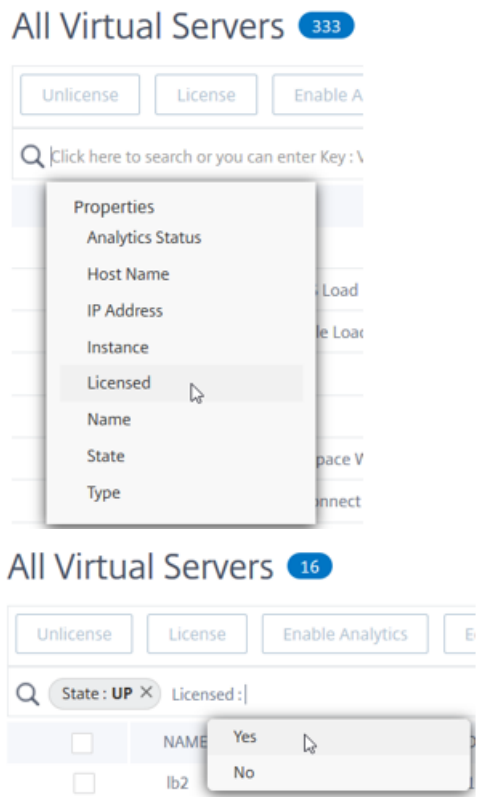
- 确保虚拟服务器已获得许可
- 确保分析状态处于禁用状态
- 确保虚拟服务器处于运行状态

您可以筛选结果以标识先决条件中提到的虚拟服务器。

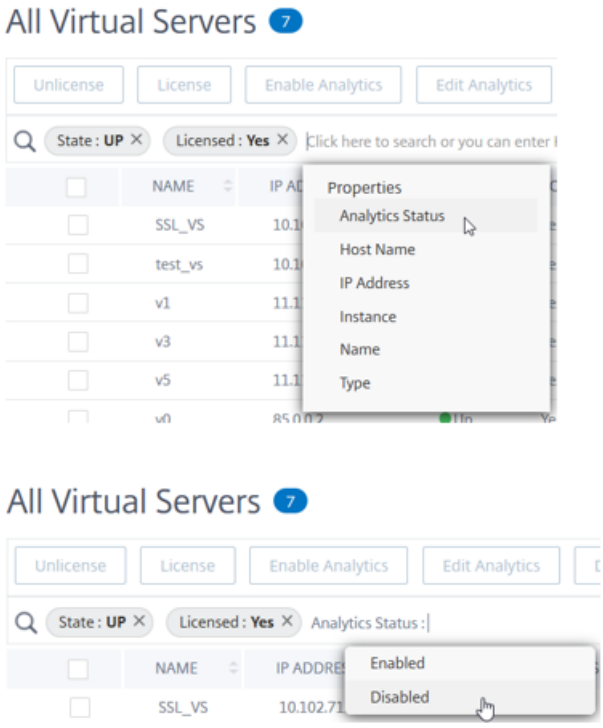
1. 单击搜索栏并选择状态，然后选择 **UP**（运行）。



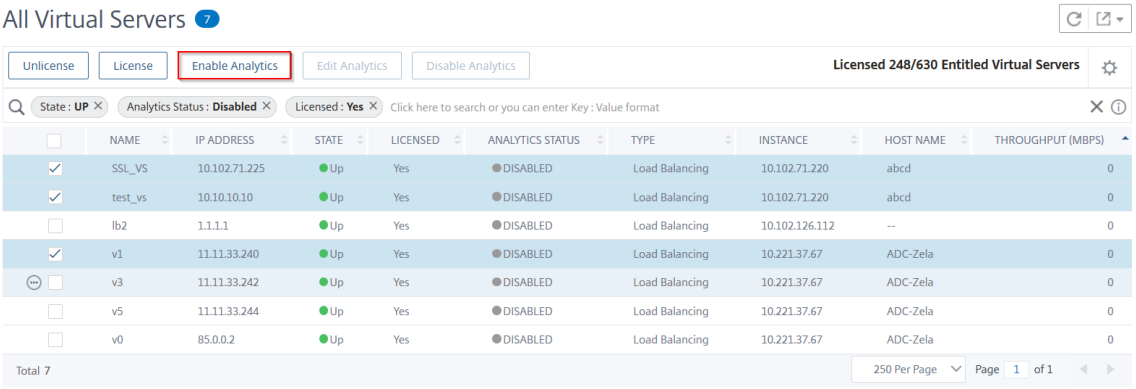
2. 单击搜索栏并选择许可，然后选择是。



3. 单击搜索栏并选择 分析状态”，然后选择 已禁用”。



4. 应用筛选器后，选择虚拟服务器，然后单击启用分析。



> 注意
>
> 或者，您也可以为特定实例启用分析：
>
> 1. 导航到 “**网络**” > “**实例**” > “**Citrix ADC**”，然后选择实例类型。例如，VPX。
>
> 1. 选择实例，然**后从选择操作**列表中选择**配置分析**
>
> 1. 在“在虚拟服务器上配置分析”页上，选择虚拟服务器，然后单击**启用分析**。

5. 在 启用分析窗口中：

   a) 选择见解类型（Web 见解或安全见解）

   b) 选择 **Logstream** 作为传输模式

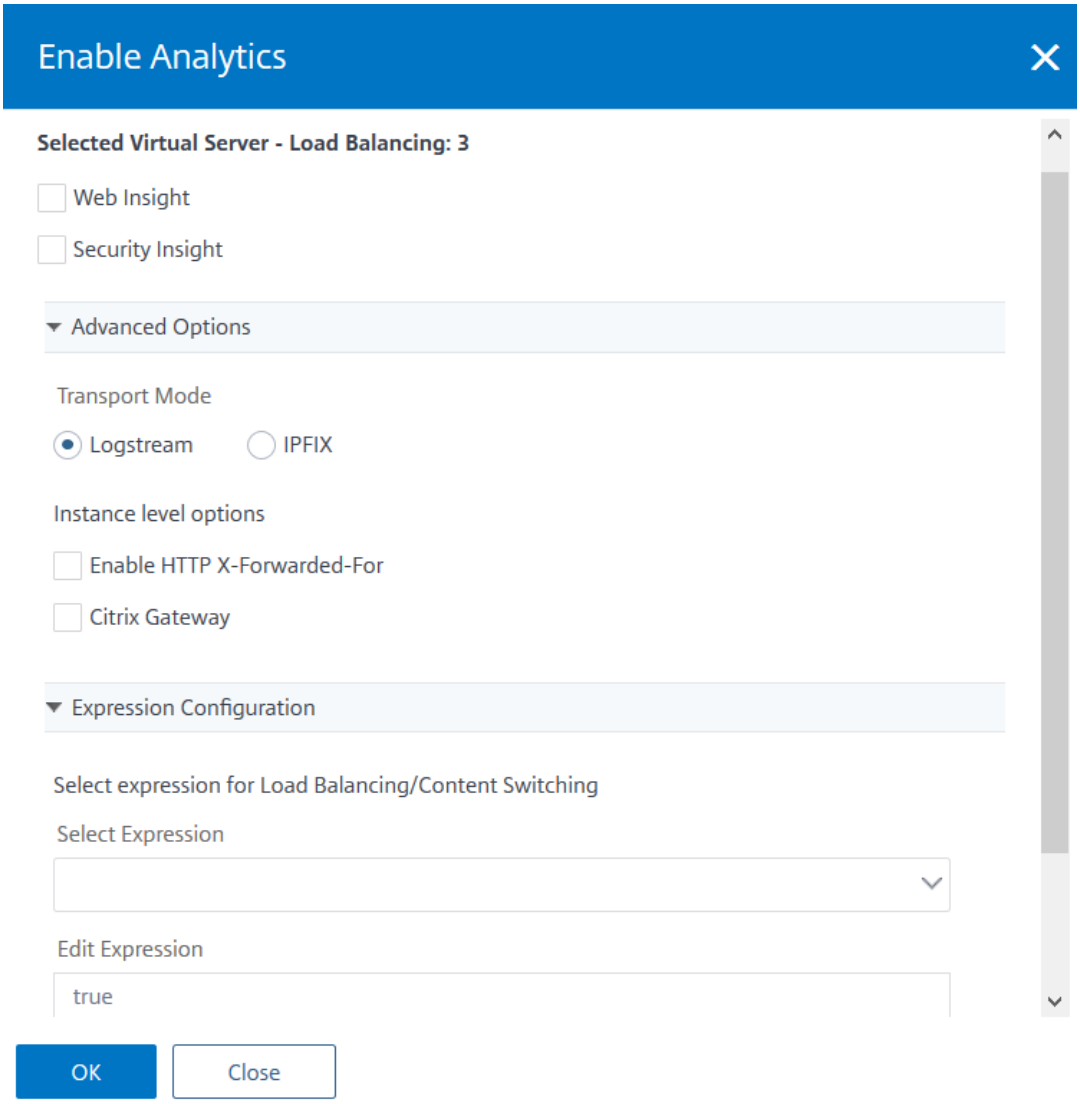
   > 注意
   >
   > 对于 Citrix ADC 12.0 或更低版本，**IPFIX** 是传输模式的默认选项。对于 Citrix ADC 12.0 或更高版本，您可以选择日志流或 **IPFIX** 作为传输模式。
   >
   > 有关 IPFIX 和日志流的详细信息，请参阅 日志流概述。

   c) 在 实例级别选项下：

   - 启用 **HTTP X-Forwar** d.For-选择此选项可通过 HTTP 代理或负载均衡器标识客户端和应用程序之间连接的 IP 地址。
   - **Citrix Gateway** -选择此选项可查看 Citrix Gateway 的分析。

   d) 默认情况下，表达式为 true

   e) 单击 **OK**（确定）



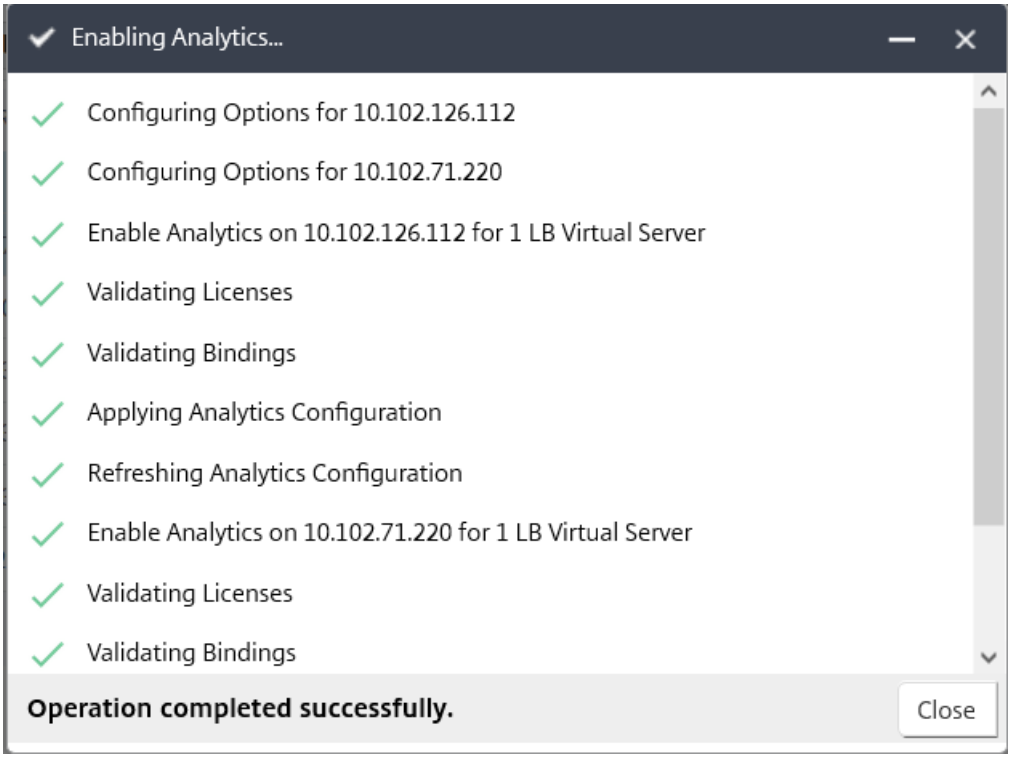
注意

- 如果选择未获得许可的虚拟服务器，则 Citrix ADM 首先许可这些虚拟服务器，然后启用分析

- 对于管理员分区，只支持 **Web Insight**

- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示一条错误消息。

单击 确定”后，Citrix ADM 将处理在所选虚拟服务器上启用分析。



> 注意
>
> Citrix ADM 对日志流使用 Citrix ADC 截取和用于 IPFIX 的 NSIP。如果在 Citrix ADM 代理和 Citrix ADC 实例之间启用了防火墙，请确保打开以下端口以使 Citrix ADM 能够收集 AppFlow 流量：
>
> | 传输模式 | 源 IP | 类型 | 端口 |
> |———| ———-|———|—-|
> | IPFIX | NSIP | UDP | 4739|
> | 日志流 | SNIP | TCP | 5557|

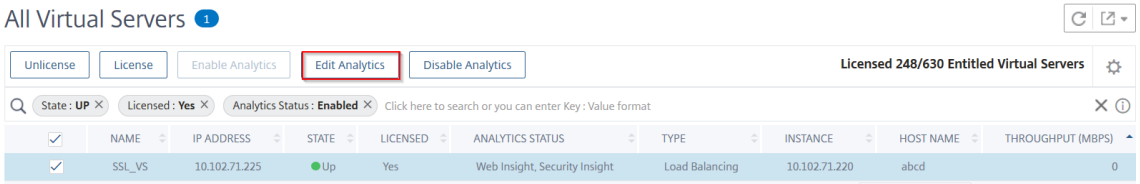
编辑分析

要编辑虚拟服务器上的分析，请执行以下操作：

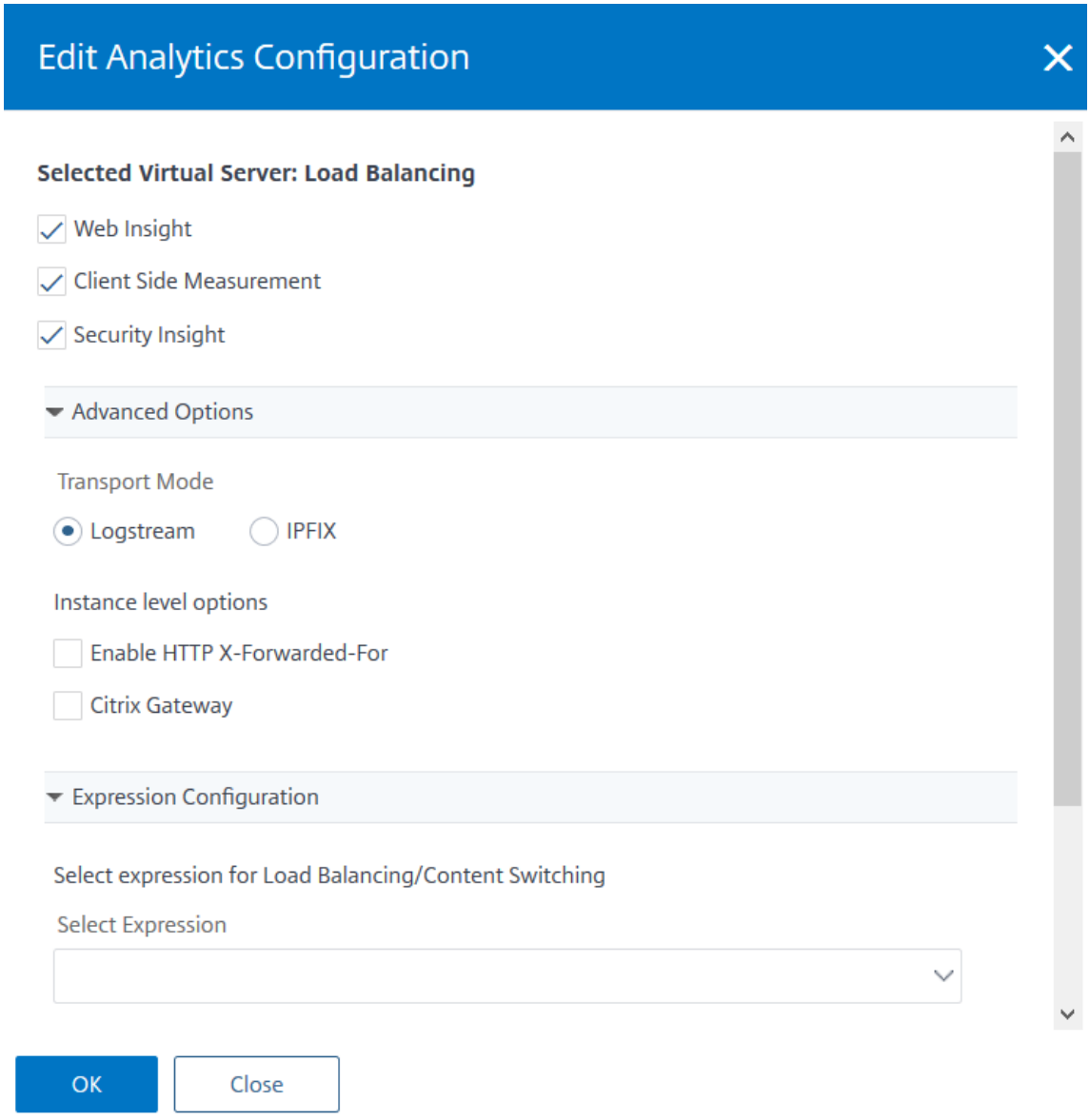
1. 选择虚拟服务器

   > 注意
   >
   > 或者，您也可以编辑特定实例的分析：
   >
   > ```
   > 1. 导航到 “ **网络** ” > “ **实例** ” > “ **Citrix ADC** ”，然后选择实例类型。例如，VPX。
   >
   > 1. 选择实例，然后单击 **编辑分析**。
   > ```

2. 单击 编辑分析



3. 编辑要在“编 辑分析配置窗口中应用的参数
4. 单击确定。

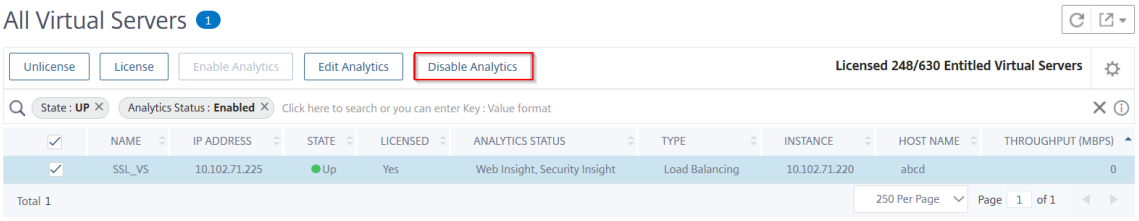


禁用分析

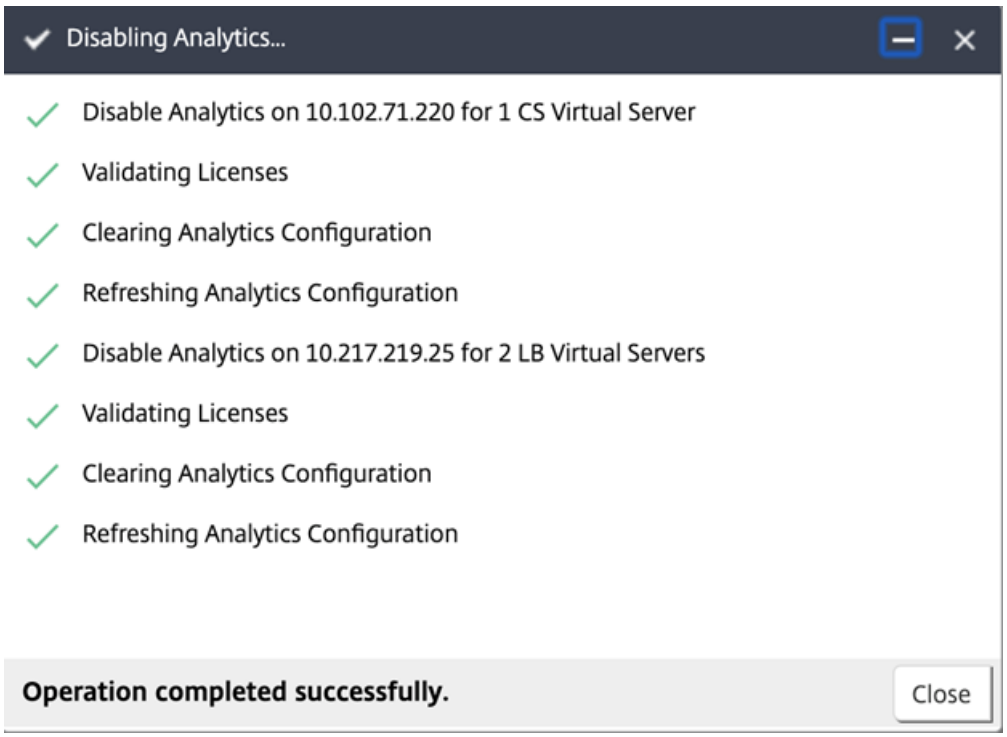
要在所选虚拟服务器上禁用分析：

1. 选择虚拟服务器

2. 单击 禁用分析



Citrix ADM 禁用选定虚拟服务器上的分析



下表介绍了支持 IPFIX 和日志流作为传输模式的 Citrix ADM 的功能：

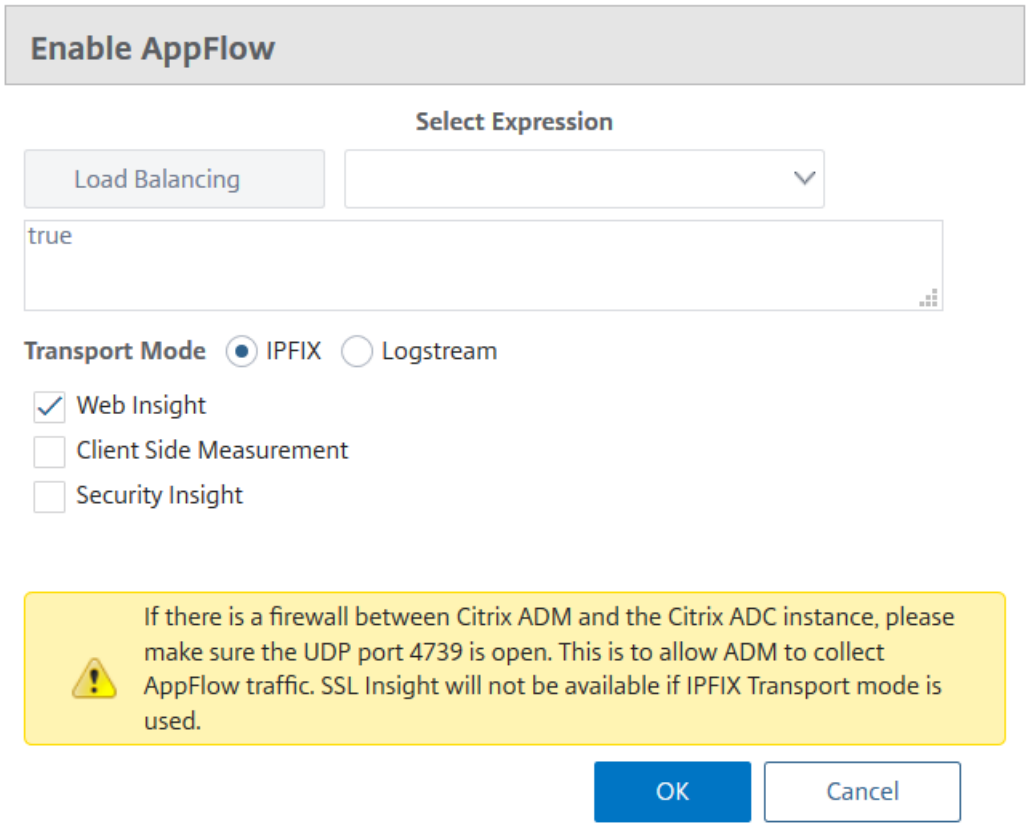
功能	IPFIX	Logstream（日志流）
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•

功能	IPFIX	Logstream（日志流）
客户端衡量标准	•	•
Syslog/Auditlog	•	•

在虚拟服务器上启用分析，以便更早的构建

要在虚拟服务器上为 **Citrix ADM 13.0** 启用分析，请执行以下操作：

1. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC**”，然后选择要启用分析的 Citrix ADC 实例。
2. 从实例列表中，选择一个实例。
3. 从 **“选择操作”** 列表中，选择 “ 配置分析”。
4. 在应用程序列表中，选择虚拟服务器，然后单击 启用 **AppFlow**。
5. 在 “ 启用 **AppFlow** ” 字段中，键入 true，并根据要启用的分析，选择 “安全智能分析” 或 “Web 智能分析”，或者选择两者。

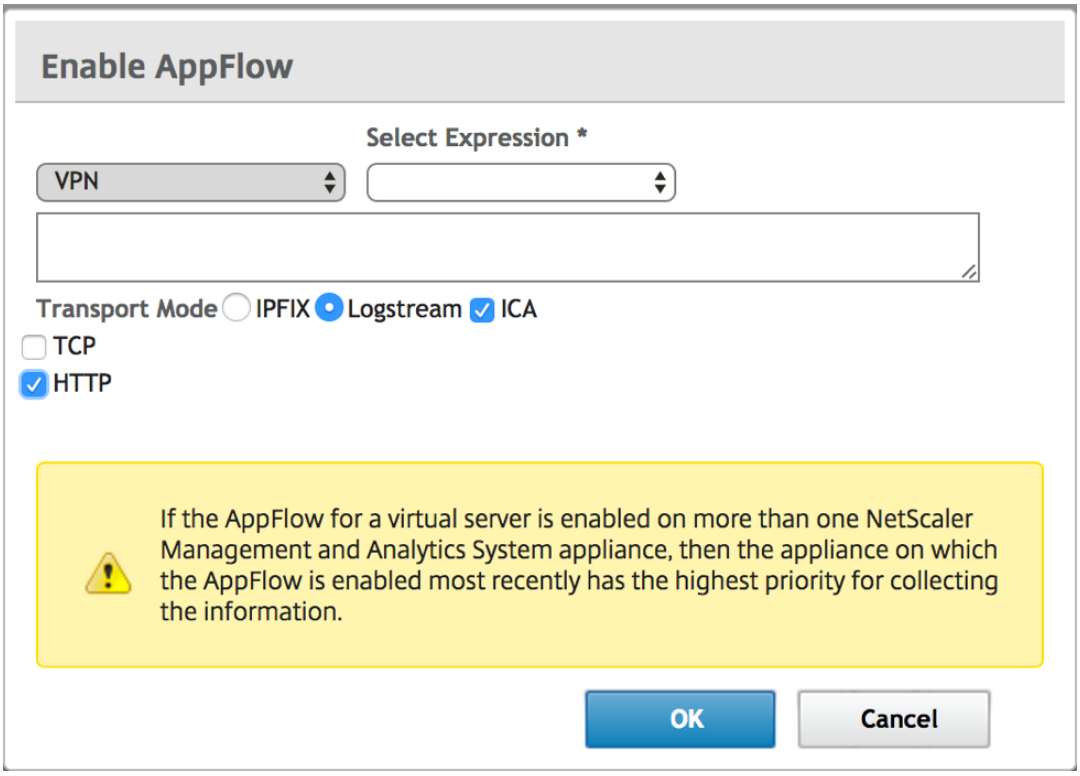


> 注意
>
> Citrix ADM 对日志流使用 Citrix ADC 截取和用于 IPFIX 的 NSIP。如果在 Citrix ADM 和 Citrix ADC 实

> 例之间启用了防火墙，请确保打开以下端口以使 Citrix ADM 能够收集 AppFlow 流量：

传输模式	源 IP	类型	端口
IPFIX	NSIP	UDP	4739
Logstream（日志流）	SNIP	TCP	5557

- 对于 HDX Insight 和 Gateway Insight，在单击启用 AppFlow 时，必须选择在 Citrix ADC 实例上配置的 VPN 虚拟服务器，然后相应地选中协议 ICA 或 HTTP 复选框。



- 对于 TCP 智能分析，导航到 “ 系统” > “ 分析设置” > “ 配置功能”，然后选择 “ 启用 **TCP** 智能分析”。
- 对于 Video Insight，您必须在 Citrix ADC 设备上进行配置更改。有关如何启用视频洞察分析的更多详细信息，请参阅 Video Insight。
- 对于广域网洞察：
  - 导航到 基础架构 **>** 实例 **> Citrix SD-WAN WO**，然后选择数据中心 WAN 优化设备。
  - 从 操作列表中，选择 启用智能分析。
  - 根据需要选择以下参数：
    * HDX Insight 地理数据收集：与 Google Geo API 共享客户端 IP 地址。
    * AppFlow：开始从 WAN 优化实例收集数据。

- TCP 和 WANOpt：提供 TCP 和 WANOpt 见解报告。
- HDX：提供 HDX Insight 报告。
- 仅适用于 HDX 的 TCP：仅提供适用于 HDX Insight 报告的 TCP。

您可以选择 AppFlow 传输模式到 **IPFIX** 或 **Logstream**，同时在 Citrix ADM 中发现的 Citrix ADC 实例上启用 AppFlow。有关 IPFIX 和日志流的详细信息，请参阅 日志流概述。

下表介绍了支持 IPFIX 和日志流作为传输模式的 Citrix ADM 的功能：

功能	IPFIX	Logstream（日志流）
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

您还可以使用 Citrix ADM 中的“启用 Web 智能分析”选项启用或禁用 Web 智能分析通信的处理。如果您不想监视 Web 智能分析通信，则可以禁用该选项。Citrix ADM 不会处理来自托管实例上虚拟服务器的 Web 智能分析流量。

配置 NTP 服务器

April 23, 2021

您可以在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

要在 **Citrix ADM** 上配置 **NTP** 服务器：

1. 在 ADM GUI 中，导航到 **“系统” > “管理”**。在“ 系统管理”页的“ 网络配置”下，单击“ **NTP** 服务器”。然后单击添加。
2. 在 **Create NTP Server**（创建 NTP 服务器）页面上，输入以下详细信息：

- **Server Name/IP Address**（服务器名称/IP 地址）– 输入 NTP 服务器的域名或 IP 地址。添加了 NTP 服务器后无法更改名称或 IP 地址。
- **Minimum Poll Interval**（最小轮询时间间隔）– 指定传输的 NTP 消息之间的最小时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最小轮询时间间隔是 64 秒（可以表示为 2^6），则输入 6。
- **Maximum Poll Interval**（最大轮询时间间隔）– 指定传输的 NTP 消息之间的最大时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最大轮询时间间隔是 256 秒（可以表示为 2^8），则输入 8。
- **Key Identifier**（密钥标识符）- 输入可以用于 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择 “Autokey”（自动密钥），请勿添加密钥标识符。
- **Autokey**（自动密钥）- 如果希望 NTP 服务器使用公钥身份验证，请选择 **Autokey**（自动密钥）。如果要添加密钥标识符，请勿选择。
- **Preferred**（首选）– 如果希望将此 NTP 服务器指定为进行时钟同步的首选服务器，请选择此选项。这仅在配置多个服务器时适用。

3. 单击创建。

要在 **Citrix ADM** 上启用 **NTP** 同步，请执行以下操作：

1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器）。
2. 单击 **NTP** 同步，然后选中 启用 **NTP** 同步复选框。
3. 单击确定。

配置系统设置

April 23, 2021

在开始使用 Citrix ADM 管理和监视实例和应用程序之前，建议您配置一些系统设置，以确保 Citrix ADM 服务器的最佳性能。

配置系统警报

配置系统警报，以确保您了解任何关键或主要的系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。对于有些警报类别（例如 cpuUsageHigh 或 memoryUsageHigh），您可以为每项设置阈值并定义严重性（例如 “Critical”（严重）或 “Major”（重大））。对于有些类别（例如 inventoryFailed 或 loginFailure），只能定义严重性。当警报类别（例如 MemoryUsageHigh）超出阈值时，或发生与警报类别对应的事件（例如登录失败）时，系统中将记录一条消息，您可以将该消息作为 syslog 消息查看。

要配置系统警报，请执行以下操作：

1. 导航到 **“系统” > “SNMP**”，然后单击右上角的 “ 警报” 选项卡。

2. 选择要配置的警报，然后单击 “ 编辑”。
3. 在 “ 配置警报” 页面上，选择警报严重性，然后设置阈值。
4. 要查看超过阈值或发生事件的警报，请导航到 **“**系统**” > “**审核**”** ，然后单击 “ **Syslog** 消息”。

配置系统通知

您可以为各种系统相关功能选择用户组发送通知。您可以在 Citrix ADM 中设置通知服务器，还可以配置电子邮件和短消息服务 (SMS) Gateway 服务器以向用户发送电子邮件和文本通知。这可确保您将收到任何系统级活动（例如，用户登录或系统重新启动）通知。

要配置系统通知，请执行以下操作：

1. 导航到 **“**系统**” > “**管理**”**。在 “ 系统管理” 页的 “ 事件通知” 下，单击 “ 配置事件通知和摘要**” > “**事件通知”。
2. 在 “ 配置系统通知设置” 页上，选择 Citrix ADM 生成的事件的类别或类别。
3. 然后，配置电子邮件服务器或 SMS 服务器以通过电子邮件或/和 SMS 接收通知。

配置系统修剪设置

要限制存储在 Citrix ADM 服务器数据库中的报告数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

要配置系统修剪设置，请执行以下操作：

1. 导航到 **System**（系统）**> System Administration**（系统管理）。在 “ 数据修剪” 下，单击 “ 系统和实例数据修剪”。
2. 在 “ 系统” 页中，指定保留数据的天数，然后单击 “保 存”。

配置实例系统日志修剪设置

要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定将从 Citrix ADM 中删除通用系统日志数据的天数。

要配置实例系统日志清除设置，请执行以下操作：

1. 定位至 **“**系统**” > “**管理**” > “**数据修剪”。
2. 单击 系统和实例数据修剪 **>** 实例系统日志。
3. 在 “ 配置实例系统日志修剪设置**”** 页中，在 保留系统日志通用数据字段中指定 **1** 到 **180** 之间的天数。
4. 单击保存。

配置实例事件修剪设置

要限制存储在 Citrix ADM 服务器数据库中的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

要配置实例事件修剪设置，请执行以下操作：

1. 导航到 **“系统” > “管理”**。
2. 在 “ 系统管理” 页面的 “ 数据修剪” 下，单击 “ 系统和实例数据修剪”。
3. 在 “数 据修剪” 页中，单击 “ 实例事件”。
4. 在 要保留的数据 **(天)** 字段中，输入要在 Citrix ADM 服务器上保留数据的时间间隔，以天为单位，然后单击保存。

配置系统备份设置

Citrix ADM 每天在 00:30 时间自动备份系统。默认情况下，它保存三个备份文件。您可能希望保留更多数量的系统备份。您还可以加密备份文件。您还可以选择在外部服务器上保存备份。

要配置系统备份设置，请执行以下操作：

1. 导航到 **“系统” > “管理”**。
2. 在 “ 备份” 下，单击 “ 配置系统和实例备份”。
3. 单击 系统，然后在 “ 配置系统备份设置” 页上，指定所需的值。

配置实例备份设置

如果备份 Citrix ADC 实例的当前状态，则可以在实例变得不稳定时使用备份文件恢复稳定性。在执行升级之前这样做尤其重要。默认情况下，每 12 小时进行一次备份，且有三个备份文件保留在系统中。

要配置实例备份设置：

1. 导航到 **“系统” > “管理”**。
2. 在 “ 备份” 下，单击 “ 配置系统和实例备份”。
3. 单击 实例，在 配置实例备份设置下，然后指定所需的值。

启用或禁用 **ADM** 功能

作为管理员，您可以在 **“系统” > “管理” > “可配置功能”** 页中启用或禁用以下功能：

- 代理故障切换 -代理故障切换可能发生在具有两个或多个活动代理的站点上。当代理在站点中处于非活动状态（关闭状态）时，Citrix ADM 服务将与其他活动代理重新分配非活动代理的 ADC 实例。有关详细信息，请参阅为多站点部署配置内部部署代理。

- 实体轮询网络函数 -实体是附加到 ADC 实例的策略、虚拟服务器、服务或操作。默认情况下，Citrix ADM 每 60 分钟自动轮询配置的网络功能实体。有关详细信息，请参阅轮询概述。
- 实例备份 — 备份 Citrix ADC 实例的当前状态，稍后使用备份的文件将 ADC 实例恢复到相同状态。有关详细信息，请参阅备份和还原 Citrix ADC 实例。
- 实例配置审核 -跨托管 Citrix ADC 实例监控配置更改，排除配置错误并恢复未保存的配置。有关详细信息，请参阅创建审计模板。
- 实例事件 -事件表示在托管 Citrix ADC 实例上发生的事件或错误。Citrix ADM 中接收的事件显示在 “ 事件摘要” 页面（**“网络” > “事件”**）中，所有活动事件都显示在 “事件消息” 页面（**“网络” > “事件” > “事件消息”**）中。有关详细信息，请参阅事件。
- 实例网络报告-您可以在全局级别为实例生成报告。此外，适用于虚拟服务器和网络接口等实体。有关详细信息，请参阅网络报告。
- 实例 **SSL** 证书 -Citrix ADM 提供了在所有托管 Citrix ADC 实例中安装的 SSL 证书的集中视图。有关详细信息，请参阅SSL 仪表板。
- 实例系统日志 -如果您已将设备配置为将所有系统日志消息重定向到 Citrix ADM，则可以监视在 Citrix ADC 实例上生成的系统日志事件。

要启用功能，请执行以下步骤：

1. 从列表中选择要启用的功能。
2. Click **Enable**。

> 重要信息：
>
> 如果禁用某个功能，则用户无法执行与该功能关联的操作。

将 Citrix ADM 与 ServiceNow 实例集成

April 23, 2021

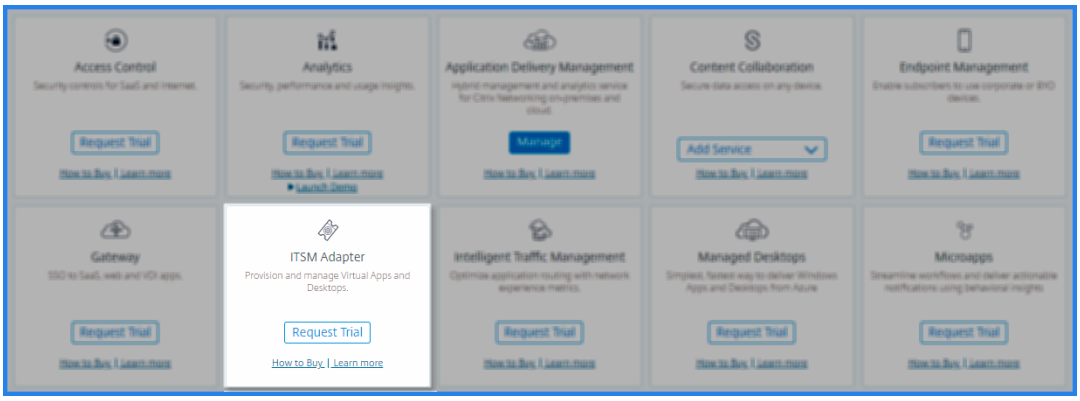
如果要为 Citrix ADC 事件和 ADM 事件启用 ServiceNow 通知，则必须将 Citrix ADM 与 ServiceNow 实例集成。要将 ADM 与 ServiceNow 实例集成，请使用Citrix ITSM 连接器。ITSM 连接器建立 Citrix ADM 与 ServiceNow 实例之间的通信。有关详细信息，请参阅ITSM 适配器的工作原理。

执行以下步骤，使用 ITSM 连接器将 Citrix ADM 与 ServiceNow 集成：

> 重要
>
> 信息：在开始之前，请确保使用管理员凭据配置客户身份。有关详细信息，请参阅配置客户身份。

1. 在 Citrix Cloud 中订阅 **ITSM** 适配器服务

a) 在 **ITSM** 适配器磁贴上，单击 请求试用。



b) 导航到 身份访问和管理 > **API** 访问”，并记下 客户端 **ID** 和 客户端密钥信息。

2. 使用管理员凭据登录到您的 ServiceNow 实例，然后执行以下步骤：

   a) 转到 ServiceNow 应用商店。下载并安装 C **itrix ITSM** 连接器。

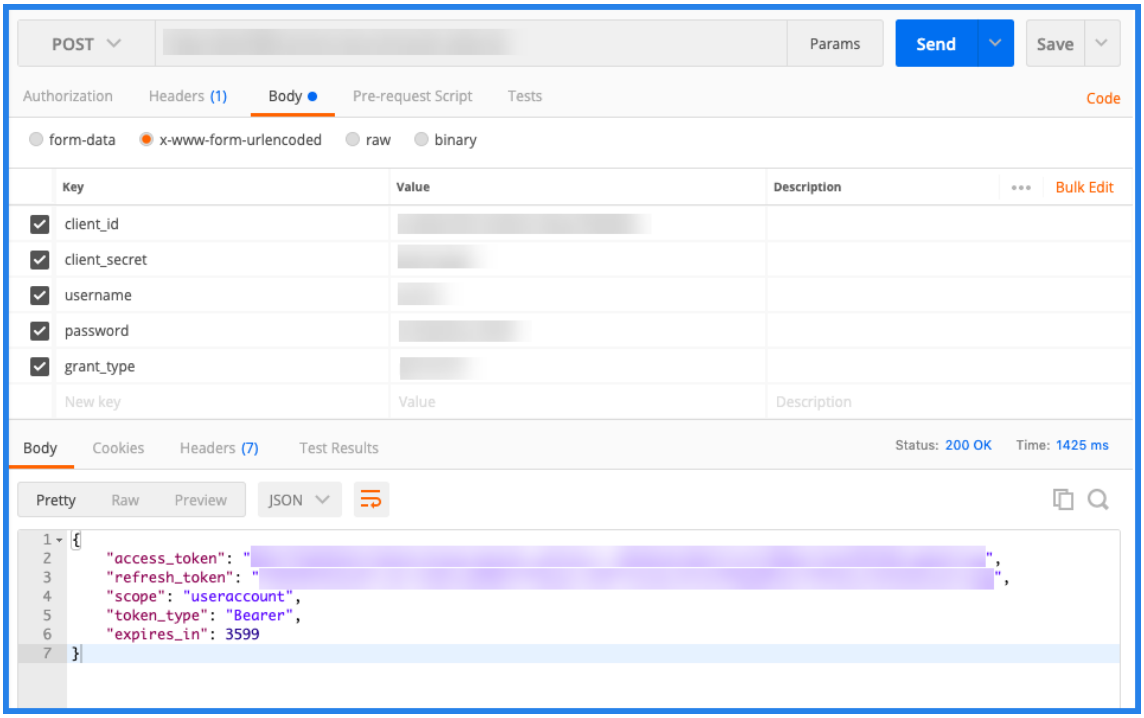
   b) 在 **Citrix ITSM** 连接器窗格上，选择 主页，然后单击 身份验证。键入您从 Citrix Cloud 中记录的客户端 ID 和密钥。

   c) 测试连接。

   d) 保存配置。此时将显示 Service Now 的确认信息，指示连接处于活动状态。

3. 创建端点以访问 ServiceNow 实例。请参阅 为客户端创建终端节点以访问实例。

4. 使用客户端 ID 和客户端密码获取访问和刷新令牌。请参阅 OAuth 令牌。

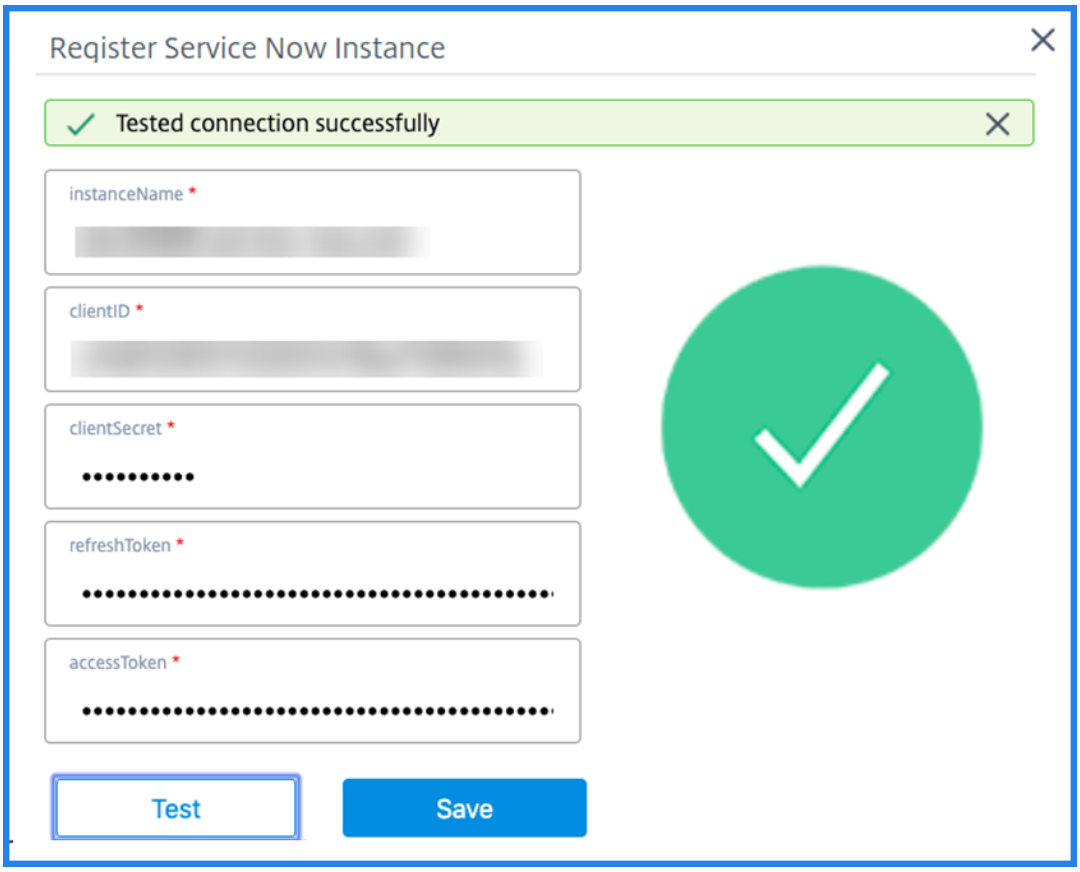


5. 在 ITSM 适配器中，添加 ServiceNow 实例：

   a) 在管理选项卡中，选择 “添加 ServiceNow 实例”。

   b) 指定 实例名称、客户端 **ID**、客户端密钥、刷新令牌和 访问令牌。

   c) 单击 测试。



   ServiceNow 实例现在已连接到 ITSM 适配器服务。

   d) 成功测试连接后，单击保存以添加 ServiceNow 实例。

6. 在 Citrix ADM 中测试 ServiceNow 票证的自动生成。

   a) 登录到 Citrix ADM。

   b) 导航到 **“系统” > “通知”**，然后选择 “ 服务 **Now**”。

   c) 从列表中选择 ServiceNow 配置文件。

   d) 单击测试以自动生成 ServiceNow 票证并验证配置。

   如果要在 Citrix ADM GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。

在 ITSM 适配器上注册 ServiceNoW 实例后，您可以在 Citrix ADM GUI 中为以下事件设置 ServiceNoW 通知：

> 重要
>
> ServiceNow 云支持此功能。

- **Citrix ADC** 事件：Citrix ADM 可以从选定托管 Citrix ADC 实例中为选定的一组 Citrix ADC 事件生成 ServiceNoW 事件。

  要从托管实例发送 Citrix ADC 事件的 ServiceNow 通知，必须配置事件规则并将规则操作分配为发送 **ServiceNow** 通知。

  通过导航到 “ 网络” > “ 事件” **>** “规则”，在 **ADM** 上创建事件规则。有关详细信息，请参阅发送 ServiceNow 通知。

- **SSL** 证书和 **ADM** 许可证事件：Citrix ADM 可以为 SSL 证书过期和 ADM 许可证过期事件生成 ServiceNow 事件。

  要发送 SSL 证书到期的 ServiceNow 通知，请参阅SSL 证书到期。

  要发送 ADM 许可证到期的 ServiceNow 通知，请参阅Citrix ADM 许可证到期。

导出或计划导出报告

April 23, 2021

在 Citrix ADM 中，您可以导出所选 Citrix ADM 功能的综合报告。此报告为您概述了实例、分区之间的映射以及相应的详细信息。

Citrix ADM 在各个 ADM 功能下显示特定于功能的计划导出报告，您可以查看、编辑或删除这些报告。例如，要查看 Citrix ADC 实例的导出报告，请导航到 **“网络” > “实例” > “Citrix ADC** ”，然后单击 “导出” 图标。您可以以 PDF、JPEG、PNG 和 CSV 文件格式导出这些报告。

在 “ 导出报告” 中，您可以执行以下操作：

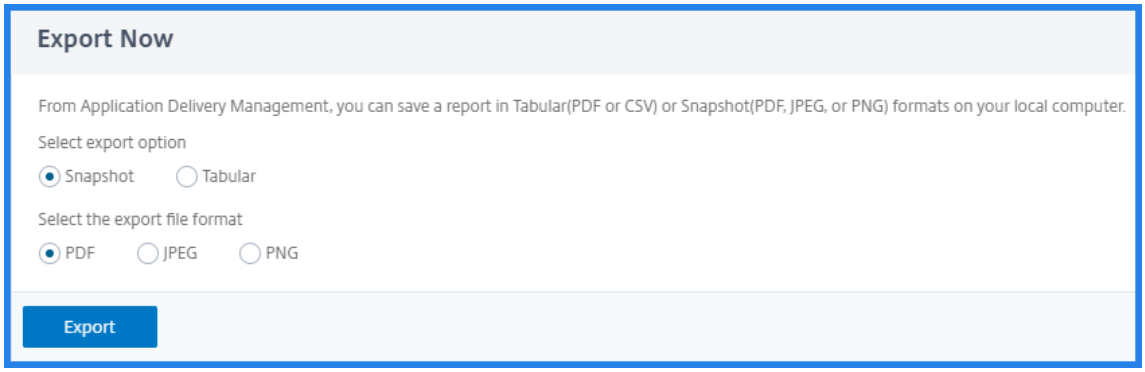
- 将报告导出到本地计算机
- 计划导出报告
- 查看、编辑或删除计划的导出报告

导出报告

要将报告从 ADM 导出到本地计算机，请执行以下步骤：

1. 单击页面右上角的导出图标。
2. 选择 “ 立即导出”。
3. 选择以下导出选项之一：
   - 快照 -此选项将 ADM 报告导出为快照。

- 表格式-此选项以表格格式导出 ADM 报告。您还可以选择以表格格式导出的数据记录数

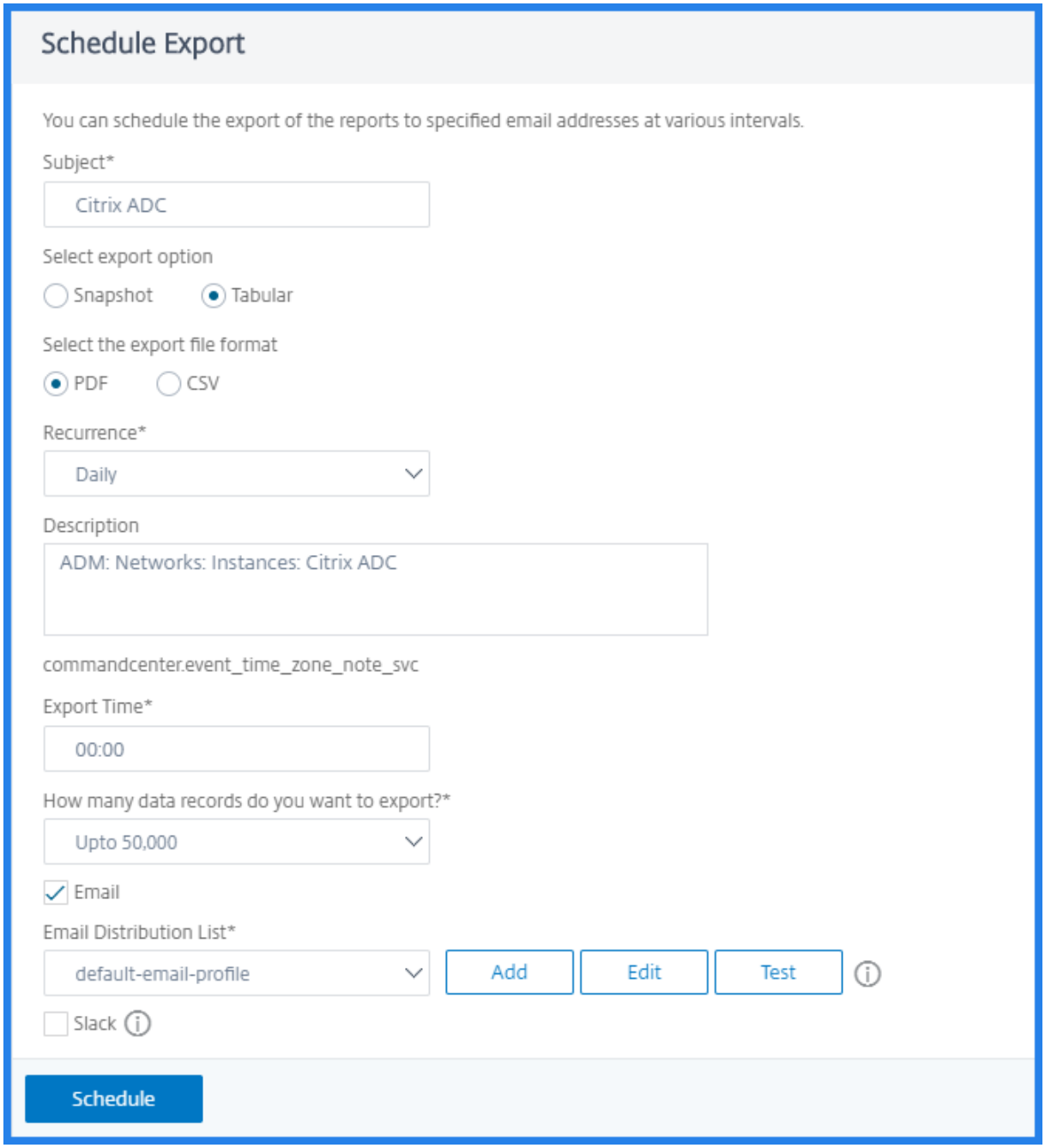


4. 选择要在本地计算机上保存报告的文件格式。
5. 单击导出。

计划导出报告

要定期调度导出报告，请指定重复时间间隔。Citrix ADM 将导出的报告发送到配置的电子邮件或松弛配置文件。

1. 单击页面右上角的导出图标。
2. 选择 “ 计划导出” 并指定以下内容：
   - 主题 -默认情况下，此字段会自动填充所选要素名称。但是，您可以使用有意义的标题重写它。
   - 导出选项 -以快照或表格格式导出 ADM 报告。您还可以选择以表格格式导出的数据记录数
   - 格式 -选择要在配置的电子邮件或松弛配置文件上接收报告的文件格式。
   - 循环 -从列表中选择 “ 每日”、“ 每周” 或 “每 月”。
   - 说明 -为报表指定有意义的描述。
   - 导出时间 -指定要导出报表的时间。
   - 电子邮件 - 选中复选框，然后从列表框中选择配置文件。如果要添加配置文件，请单击 添加。
   - **Slack** - 选中复选框，然后从列表框中选择配置文件。如果要添加配置文件，请单击 添加。
3. 单击 **Schedule**（计划）。



查看和编辑计划的导出报告

要查看导出报告，请执行以下操作：

1. 单击页面右上角的导出图标。

   “ 导出报告”页显示所有特定于功能的导出报告。

2. 选择要编辑的报告，然后单击 编辑。

升级

April 23, 2021

每个 Citrix ADM 版本都提供了新的和更新的功能，并增强了功能。Citrix 建议您将 Citrix ADM 升级到最新版本，以利用新功能和错误修复。[发行说明 ()] 随附的每个版本发布中都包含了增强功能、已知问题和错误修复的全面列表。在开始升级之前，了解许可框架以及可以使用的许可证类型也很重要。有关 Citrix ADM 许可信息，请参阅许可。

升级路径信息也可在中找到 Citrix 升级指南。

升级准备

从 Citrix ADM 下载页面下载升级程序包，然后按照本文中的说明将系统升级到最新的 13.0 版本。升级过程开始后，ADM 将重新启动，并在升级完成时终止和重新连接现有连接。现有配置将保留，但在升级成功完成之前，Citrix ADM 不会处理任何数据。

升级到 **13.0** 之前的注意事项：

- 如果从版本 11.1 或版本 12.0 56.x 升级以及以前的版本，请执行以下步骤：
  1. 从现有版本升级到 12.0 版本 57.24。
  2. 升级到版本 12.1 的最新版本。
  3. 升级到版本 13.0。
- 如果从 12.0 版本 57.24 及更高版本升级，请先升级到 12.1，然后升级到 13.0。
- 如果从 12.1 升级，则可以直接升级到 13.0。
- 如果升级到 13.0 67.xx 及更高版本，请先升级到 13.0 64.xx，然后升级到 13.0 67.xx 及更高版本，以获得更好的用户体验。

升级到 **13.0 67.xx** 及更高版本之前需要注意的重要事项

将 ADM 软件升级到 13.0 67.xx 及更高版本时，ADM 数据库也会迁移。发生这种数据迁移是因为 ADM 现在使用 PostgreSQL 版本 10.11。

> 注意
>
> 不支持降级 ADM 软件。不要试图降级。

建议的预防措施：

- 如果要升级到 13.0 67.xx 及更高版本，请拍摄 Citrix ADM 服务器的快照。
- 在升级之前备份 Citrix ADM 服务器。
- 升级后，您可能需要重新建立 Citrix ADM 服务器和托管实例之间的连接。如果继续，会有确认提示向您警告连接可能失败。

- 对于高可用性设置中的 Citrix ADM 服务器，升级时，不要对任何一个节点进行任何配置更改。

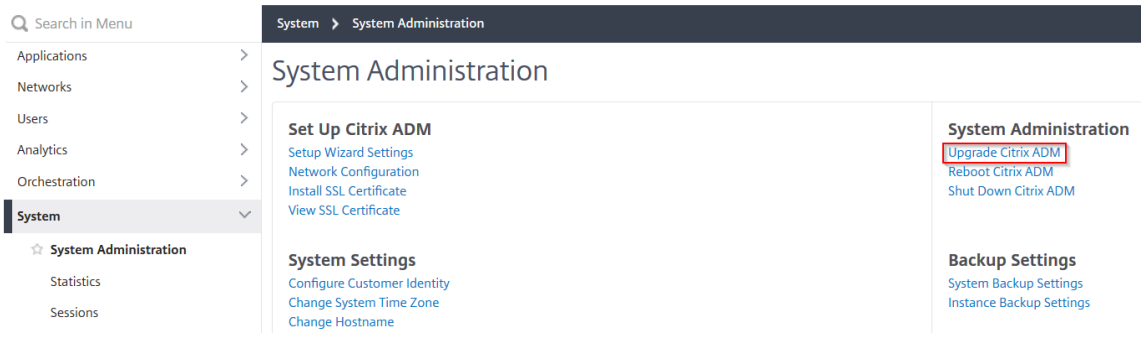
  > 警告
  >
  > 在升级过程成功完成之前，请勿刷新浏览器。检查 GUI 以了解完成升级的大概时间。

- 升级后，活动节点可以在高可用性对中进行更改。

升级单个 **Citrix ADM** 服务器

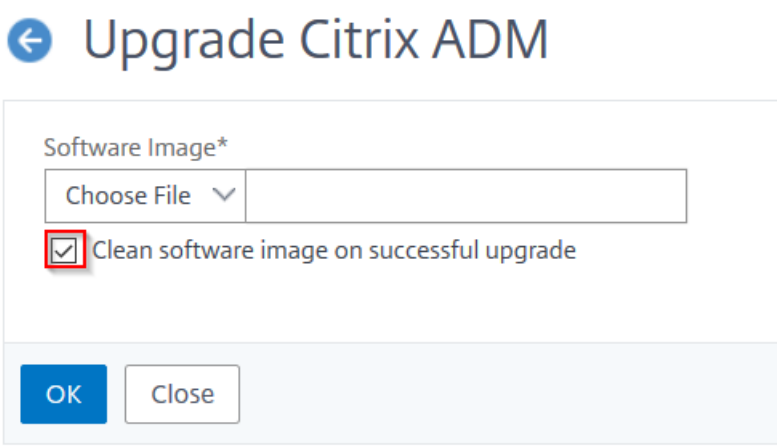
要升级单个 **Citrix ADM** 服务器，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到“系统”>“系统管理”。在系统管理子标题下，单击 升级 **Citrix ADM**。

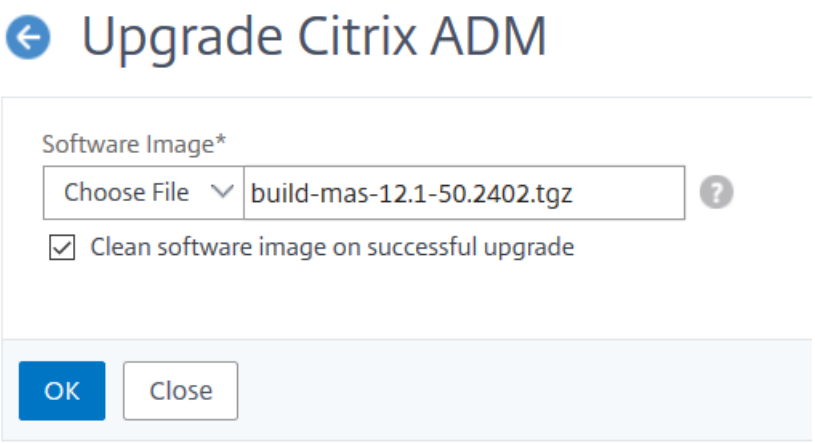


3. 在升级 **Citrix ADM** 页面上，选中成功升级时清理软件映像复选框以在升级后删除映像文件。选择此选项会在升级时自动删除 Citrix ADM 映像文件。

   > 注意
   >
   > 此选项默认处于选中状态。如果在开始升级过程之前未选中此复选框，则必须手动删除映像。



4. 然后，您可以通过选择“本地计算机”或“设备”来上传新图像文件。构建文件必须存在于 Citrix ADM 虚拟设备上。



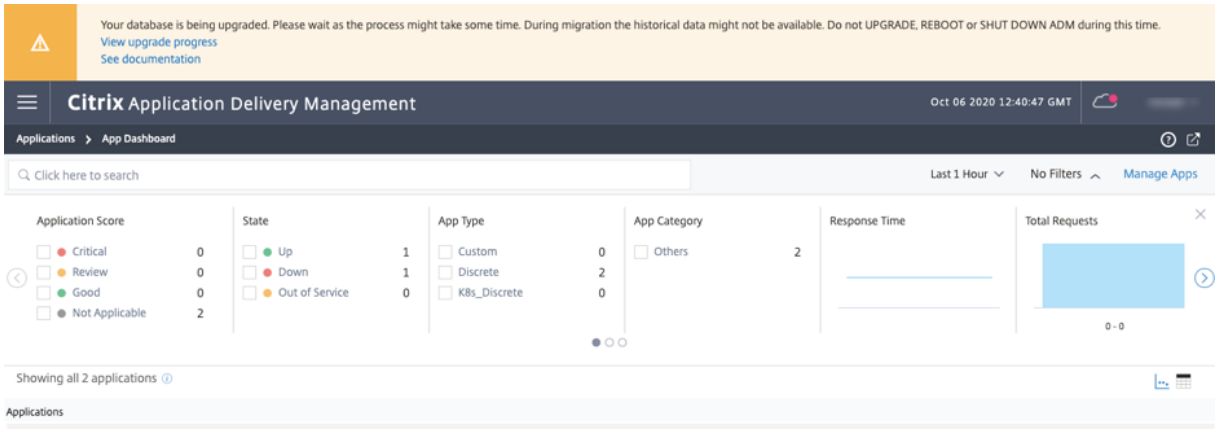
5. 单击 “ 确定”。

   此时将显示 “确认” 对话框。单击是。

   升级过程开始。以下屏幕截图显示了 13.0 64.35 和以前版本的升级过程。

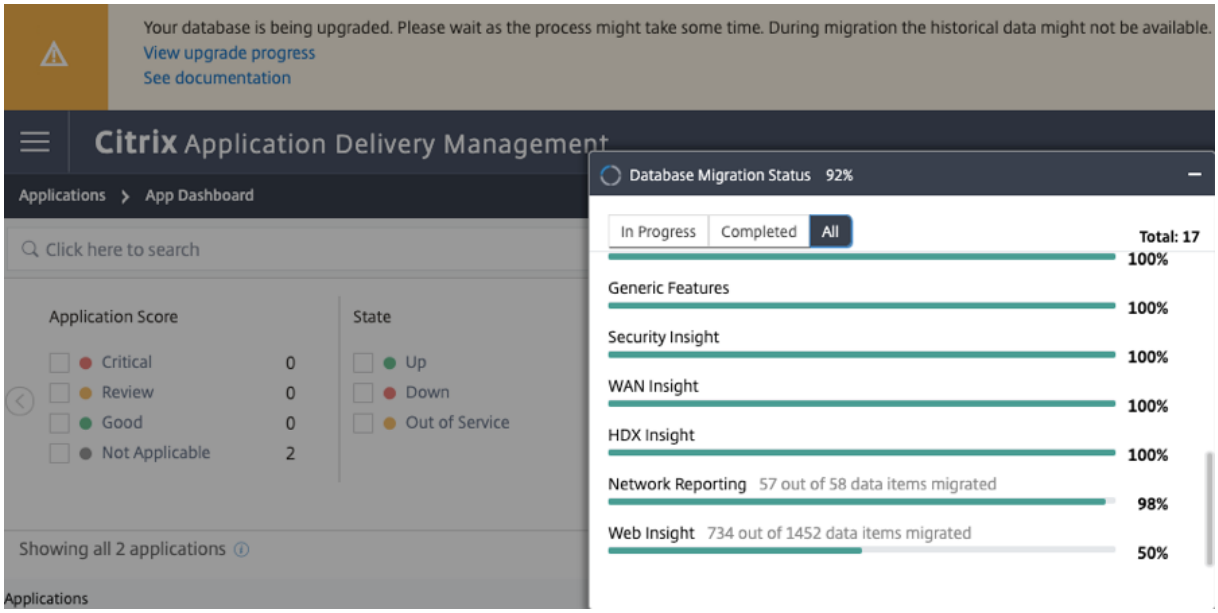
   以下屏幕截图显示了 13.0 67.xx 及更高版本的升级过程。

迁移配置后，您可以登录到 ADM GUI。登录后，历史数据开始在后台迁移，同时您可以继续使用 ADM。



在历史数据迁移期间，某些旧数据可能不可用。迁移数据库所需的时间取决于数据的大小和表的数量。

您可以使用 ADM GUI 监视数据库迁移。单击 查看升级进度，将显示 数据库迁移状态。



排查数据库迁移问题

在升级到 13.0 67.xx 及更高版本的过程中，有时 Web Insight 历史数据的迁移可能会被卡住。在这种情况下，要检查数据迁移的详细信息，请执行以下操作。

登录 ADM shell 提示符并运行以下命令以查看进度的详细信息。

```
1     cat /var/mps/log/db_upgrade/web_insight_mapping_migration_status
2
3 <!--NeedCopy-->
```

这是一个示例输出

```
1     bash-3.2# cat /var/mps/log/db_upgrade/
         web_insight_mapping_migration_status
2     Tue Oct  6 07:41:55 GMT 2020
3     157 out of 127346 done in 54 seconds
4     File
5      /var/mps/db_upgrade/hist_table_mig_data/Web_Insight/
          af_app_client_server_resp_second_l3p_d7_dump
6     bash-3.2#
7
8  <!--NeedCopy-->
```

在此示例中，`af_app_client_server_resp_second_l3p_d7` 是正在升级的条目。在 127,346 个条目中，有 157 个条目在 54 秒内被迁移。

将高可用性对从 **12.1** 版升级到 **13.0** 版

对于高可用性模式下的 Citrix ADM 服务器，可以通过访问活动节点或浮动 IP 地址进行升级。在任一服务器中启动升级过程后，两个 Citrix ADM 服务器都会自动升级到最新版本。

> 注意
>
> 如果要从 12.0 或更早版本升级高可用性对，请参阅 Citrix ADM 12.1 升级

升级 **Citrix ADM** 灾难恢复部署

升级 Citrix ADM 灾难恢复部署分为两个步骤：

- 升级主站点中以高可用性模式配置的 Citrix ADM 节点。稍后您必须升级灾难恢复节点。
- 在升级灾难恢复节点之前，请确保已升级了以高可用性部署的 Citrix ADM 服务器。

升级 **Citrix ADM** 灾难恢复节点

1. 从 Citrix 下载站点下载 Citrix ADM 升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上传到灾难恢复节点。
3. 使用 `nsrecover` 凭据登录到灾难恢复节点。
4. 导航到放置图像文件的文件夹并解压缩该文件。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Wed May 15 05:27:10 2019 from 10.252.241.103
bash-3.2# cd /var/mps/mps_images
bash-3.2# tar xvfz build-mas-13.0-36.25.tgz
```

5. 运行以下脚本：

   。/安装马斯

```
bash-3.2# ./installmas
```

为多站点部署升级内部部署代理

升级 Citrix ADM 代理部署是一个三步过程。
在升级本地代理之前，请确保您已完成以下任务：

1. 升级以高可用性部署的 Citrix ADM 服务器。
2. 升级 Citrix ADM 灾难恢复节点。

   有关详细信息，请参阅升级 Citrix ADM 灾难恢复部署。

升级本地代理

1. 从 Citrix 下载站点下载 Citrix ADM 代理升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上传到代理节点。
3. 确保您下载了正确的代理升级映像。以下是图像文件名格式的示例：

   build-masagent-13.0-48.18.tgz
4. 使用 `nsrecover` 凭据登录到本地代理。
5. 导航到放置图像文件的文件夹并解压缩该文件。

```
login as: nsrecover
Using keyboard-interactive authentication.
Password:
Last login: Thu Aug 30 08:50:48 2018 from 10.252.241.37
bash-3.2# cd /var/mps/mps_images/
bash-3.2# tar zxvf build-masagent-12.1-502.109.tgz
```

6. 运行以下脚本：

   `./installmasagent`

```
bash-3.2# ./installmasagent
```

向 **Citrix ADM** 服务器添加额外的磁盘

如果 Citrix ADM 存储需求超过默认磁盘空间（120 GB），则可以附加额外的磁盘。您可以在单服务器部署和高可用性部署中连接更多磁盘。

从版本 12.1—13.0 升级 Citrix ADM 时，您在早期版本中的其他磁盘上创建的分区保持不变。这些分区不会被删除，也不会调整它们的大小。

在升级版本中附加更多磁盘的过程保持不变。现在，您可以使用 Citrix ADM 中的新磁盘分区工具在新添加的磁盘中创建分区。您还可以使用该工具调整现有更多磁盘中的分区大小。有关如何连接更多磁盘和使用新的磁盘分区工具的详细信息，请参阅 如何将额外的磁盘附加到 Citrix ADM。

使用样书在 **OpenStack** 中置备 **Citrix ADC** 实例

从 Citrix ADM 12.1 版本 49.23 开始，OpenStack 编排工作流的体系结构已更新。此工作流现在使用 Citrix ADM 样书来配置 Citrix ADC 实例。如果从版本 12.0 或 12.1 版本 48.18 升级到 Citrix ADM 13.0，则必须运行以下迁移脚本：

```
1 /mps/scripts/migration_scripts/migrate_configurations.py
2 <!--NeedCopy-->
```

有关 `os-cs-lb-mon` 样书和迁移脚本的详细信息，请参阅 使用样书在 OpenStack 上预配 Citrix ADC VPX 实例

身份验证

April 23, 2021

用户可以通过 Citrix ADM 在内部进行身份验证，也可以通过身份验证服务器在外部对用户进行身份验证。如果使用本地身份验证，则用户必须位于 Citrix ADM 安全数据库中。如果用户通过外部身份验证，则用户 “外部名称” 必须与在身份验证服务器上注册的外部用户身份相匹配，具体取决于所选的身份验证协议。

Citrix ADM 支持通过 RADIUS、LDAP 和 TACAS 服务器进行外部身份验证。这种统一的支持提供了一个通用界面，用于验证和授权访问系统的所有本地和外部身份验证、授权和会计服务器用户。Citrix ADM 可以对用户进行身份验证，无论用户使用何种实际协议与系统进行通信。当用户尝试访问配置为外部身份验证的 Citrix ADM 实现时，请求的应用程序服务器将用户名和密码发送到 RADIUS、LDAP 或 TACAS 服务器进行身份验证。如果身份验证成功，则向用户授予对 Citrix ADM 的访问权限。

外部身份验证服务器

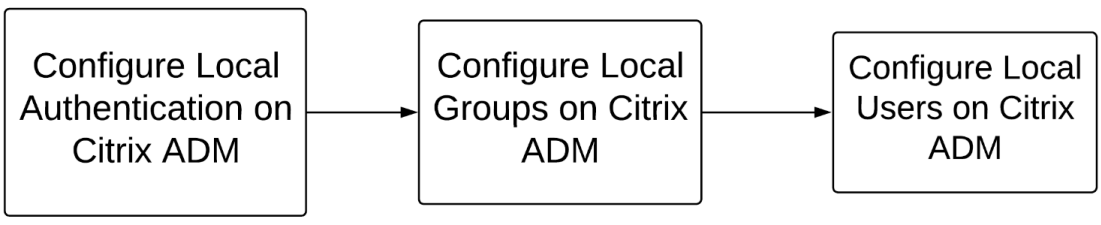
Citrix ADM 将所有身份验证、授权和审核服务请求发送到远程 RADIUS、LDAP 或 TACACS 服务器。远程身份验证、授权和审核服务器接收请求、验证请求并向 Citrix ADM 发送响应。当配置为使用远程 RADIUS、TACAS 或 LDAP 服务器进行身份验证时，Citrix ADM 将成为 RADIUS、TACAS 或 LDAP 客户端。在其中任何配置中，身份验证记录都存储在远程主机服务器数据库中。帐户名称、分配的权限和时间记帐记录也存储在每个用户的身份验证、授权和审核服务器上。

此外，您可以使用 Citrix ADM 的内部数据库在本地对用户进行身份验证。可在数据库中创建用户及其密码和默认角色条目。您还可以为特定类型的身份验证选择身份验证顺序。服务器组中的服务器列表是有序列表。除非列表中的第一个服务器不可用，否则始终使用该服务器，如果不可用，则使用列表中的下一个服务器。您可以将服务器配置为将内部数据库作为回退身份验证备份包含到已配置的身份验证、授权和审核服务器列表中。

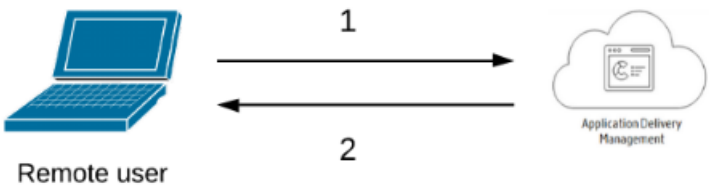
在 **Citrix ADM** 中对用户进行身份验证

您可以通过两种方式在 Citrix ADM 中对用户进行身份验证：

- 在 Citrix ADM 中配置的本地用户



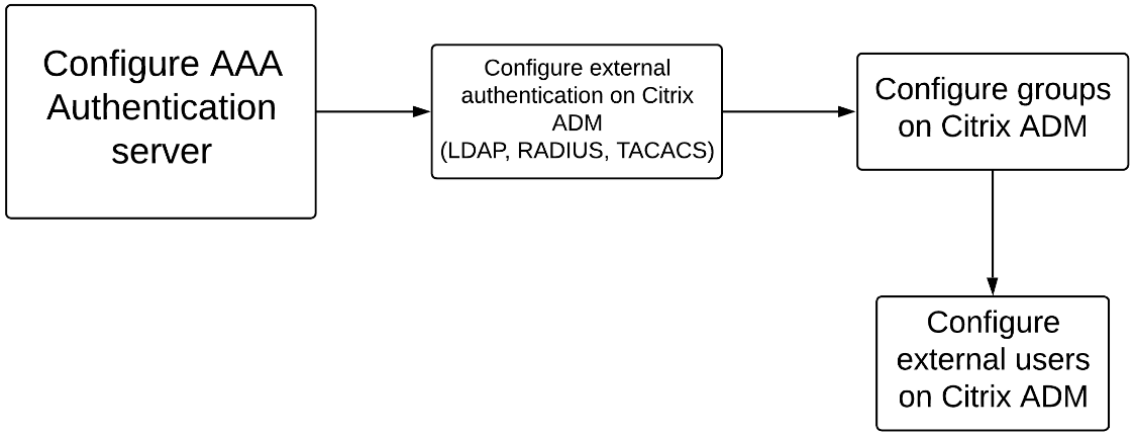
配置完成后，以下是在本地服务器中进行用户身份验证的工作流。



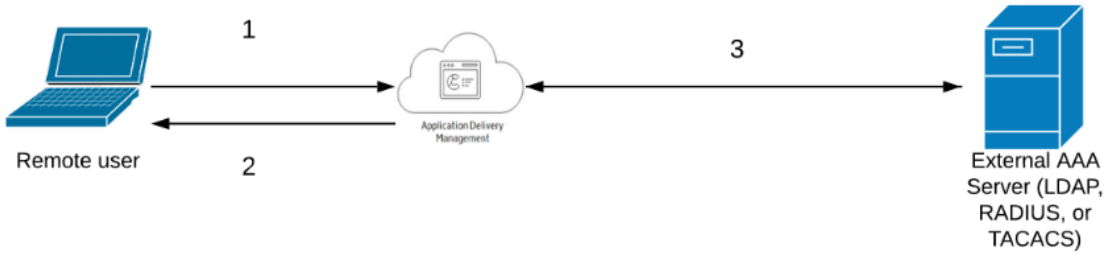
1 — 用户登录到 Citrix ADM

2 — Citrix ADM 提示用户输入凭据进行身份验证，并检查凭据是否与 ADM 数据库中的凭据匹配。

- 使用外部身份验证服务器



配置完成后，以下是外部身份验证、授权和审核服务器中用户身份验证的工作流：



1 — 用户与 Citrix ADM 连接

2 — Citrix ADM 提示用户输入凭据

3 — Citrix ADM 使用外部身份验证、授权和审核服务器验证用户凭据。如果验证成功，用户可以继续登录

在 **Citrix ADM** 中配置外部身份验证服务器

April 23, 2021

配置 LDAP、RADIUS 或 TACAS 服务器后，可以在 Citrix ADM 中添加这些服务器。

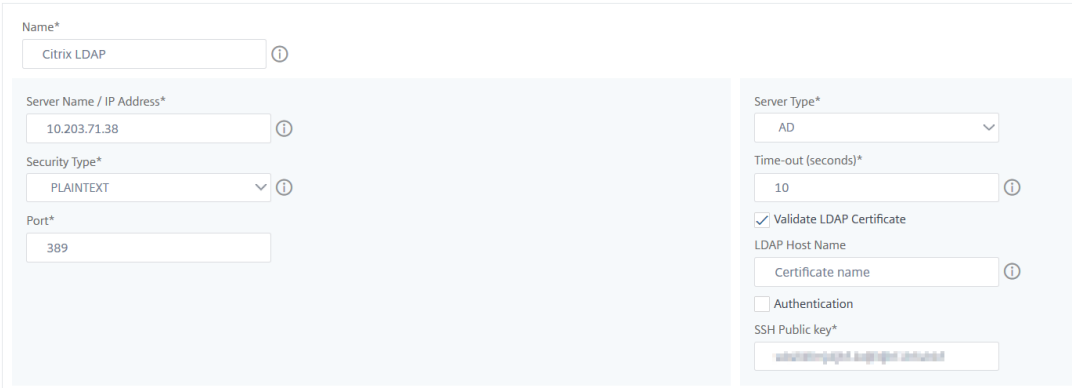
添加 **LDAP** 身份验证服务器

April 23, 2021

将 LDAP 协议与 RADIUS 和 TACAS 身份验证服务器集成时，可以使用 ADM 从分布式目录搜索和验证用户凭据。

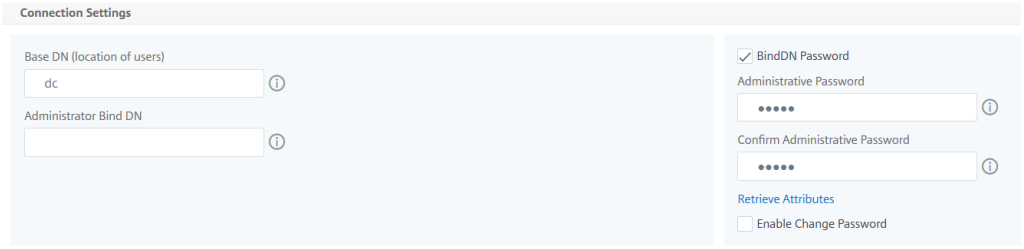
1. 导航到 “ 系统” > “ 身份验证”。
2. 选择 “ **LDAP** ” 选项卡，然后单击 “ 添加”。
3. 在 “ 创建 **LDAP** 服务器” 页上，指定以下参数：
   a) 名称 — 指定 LDAP 服务器名称
   b) 服务器名称**/IP** 地址 — 指定 LDAP IP 地址或服务器名称
   c) 安全类型 — 系统与 LDAP 服务器之间所需的通信类型。从列表中选择。如果纯文本通信不足，您可以通过选择传输层安全性 (TLS) 或 SSL 来选择加密通信
   d) 端口 — 默认情况下，端口 389 用于普通文本。您还可以为 SSL/TSL 指定端口 636
   e) 服务器类型 — 选择 Active Directory (AD) 或诺维尔目录服务 (NDS) 作为 LDAP 服务器的类型
   f) 超时（秒） — Citrix ADM 系统等待 LDAP 服务器响应的时间（以秒为单位）
   g) **LDAP** 主机名 — 选中验证 LDAP 证书复选框，并指定要在证书中输入的主机名

      清除 “ 身份验证” 选项并指定 SSH 公钥。通过基于密钥的身份验证，您现在可以通过 SSH 获取存储在 LDAP 服务器中用户对象上的公钥列表。



      在 “连接设置” 下，指定以下参数：

      i. 基本 **DN** — LDAP 服务器启动搜索的基本节点
      ii. 管理员绑定 **DN** — 用户名绑定到 LDAP 服务器。例如，admin@aaa.local。
      iii. 绑定 **DN** 密码 — 选择此选项可为身份验证提供密码
      iv. 启用更改密码 — 选择此选项可启用密码更改



在“其他设置”下，指定以下参数

i. 服务器登录名称属性 — 系统用于查询外部 LDAP 服务器或 Active Directory 的名称属性。从列表中选择相同帐户名称。

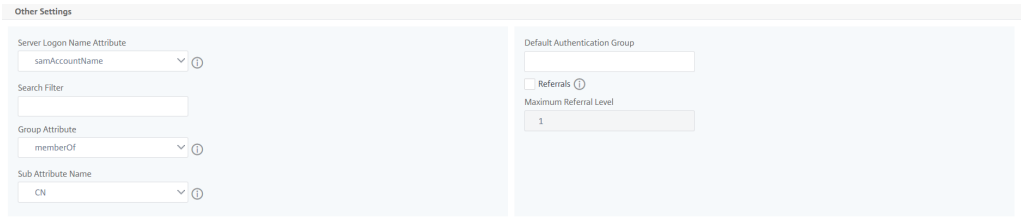
ii. 搜索筛选器 — 根据 LDAP 服务器中配置的搜索筛选器配置外部用户进行双重身份验证。例如，vpnallowed=true 使用 ldaploginame `samaccount` 和用户提供的用户名 Bob 将产生一个 LDAP 搜索字符串: &(`vpnallowed`=**`true`**)(`samaccount`=`bob`)。

> 注意
>
> 默认情况下，搜索筛选器中的值用括号括起来。

iii. 组属性 — 从列表中选择成员。

iv. 子属性名称 — 用于从 LDAP 服务器提取组的子属性名称。

v. 默认身份验证组 — 除了提取的组之外，还可以选择验证成功的默认组。



4. 单击创建。

现在已配置 LDAP 服务器。

> 注意
>
> 如果用户是 Active Directory 组成员，则该组和 Citrix ADM 上的用户名必须具有相同的 Active Directory 组成员的名称。

添加 **RADIUS** 身份验证服务器

April 23, 2021

1. 导航到“ 系统” > “ 身份验证”。

2. 选择 **RADIUS** 选项卡，然后单击 添加。

   在 “ 创建 **RADIUS** 服务器” 页上，指定以下参数：

   a) 名称 — 指定 RADIUS 服务器名称

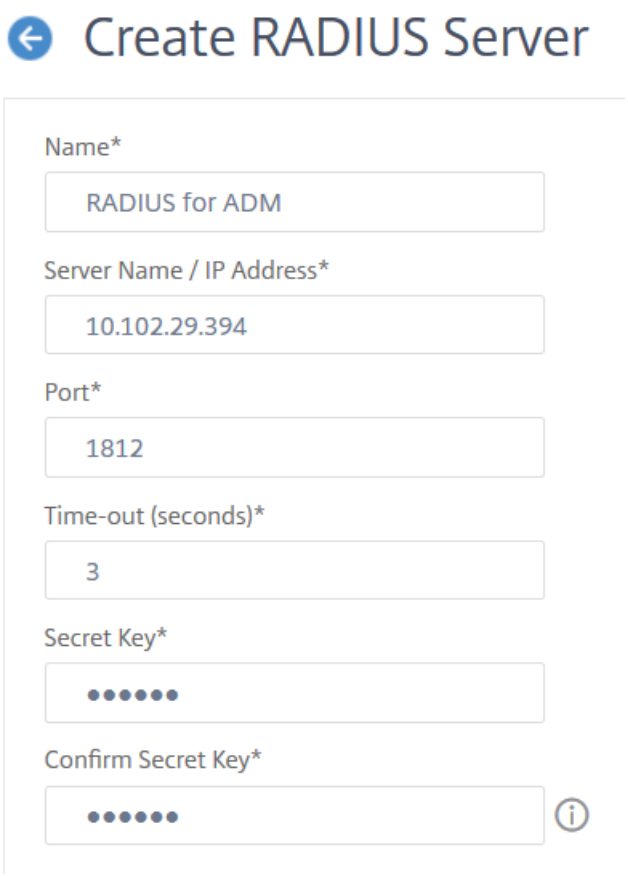
   b) 服务器名**/IP** 地址 — 指定 RADIUS 服务器 IP 地址

   c) 端口 — 指定托管 RADIUS 服务器的端口号。默认端口为 1812

   d) 超时（秒） — Citrix ADM 系统等待 RADIUS 服务器响应的时间（以秒为单位）

   e) 密钥 — 指定用于身份验证的 RADIUS 密钥

   f) 确认密钥 — 再次指定密钥进行确认



   在 “ 详细信息” 下，指定以下参数：

   i. **NAS ID** — 指定将标识符发送到 RADIUS 服务器的 ID

   ii. 组供应商标识符 — 指定用于使用 RADIUS 组抽取的供应商 ID

   iii. 组前缀 -用于 RADIUS 组抽取的 RADIUS 属性中组名称前面的字符串

   iv. 组属性类型 — 指定 RADIUS 组抽取的属性类型

   v. 组分隔符 — 用于在 RADIUS 组抽取的 RADIUS 属性中分隔组名的字符串

vi. **IP** 地址供应商标识符 — RADIUS 中的供应商 ID 表示内部网 IP。值为 0 表示属性未经供应商编码

vii. 密码供应商标识符 — RADIUS 响应中提取用户密码的供应商 ID 密码

viii. **IP** 地址属性类型 — RADIUS 要响应的远程 IP 地址属性

ix. 密码属性类型 — 要响应的 RADIUS 的密码属性

x. 密码编码 — 从列表中选择 PAP、章节、MShapv1 或 MShapv2。这表示在从系统传输到 RADIUS 服务器的 RADIUS 数据包中应如何编码密码。

xi. 默认身份验证组 — 除了提取的组之外，还可以选择验证成功的默认组

如果希望设备使用 RADIUS 服务器记录审核信息，请选择会计。

3. 单击创建。

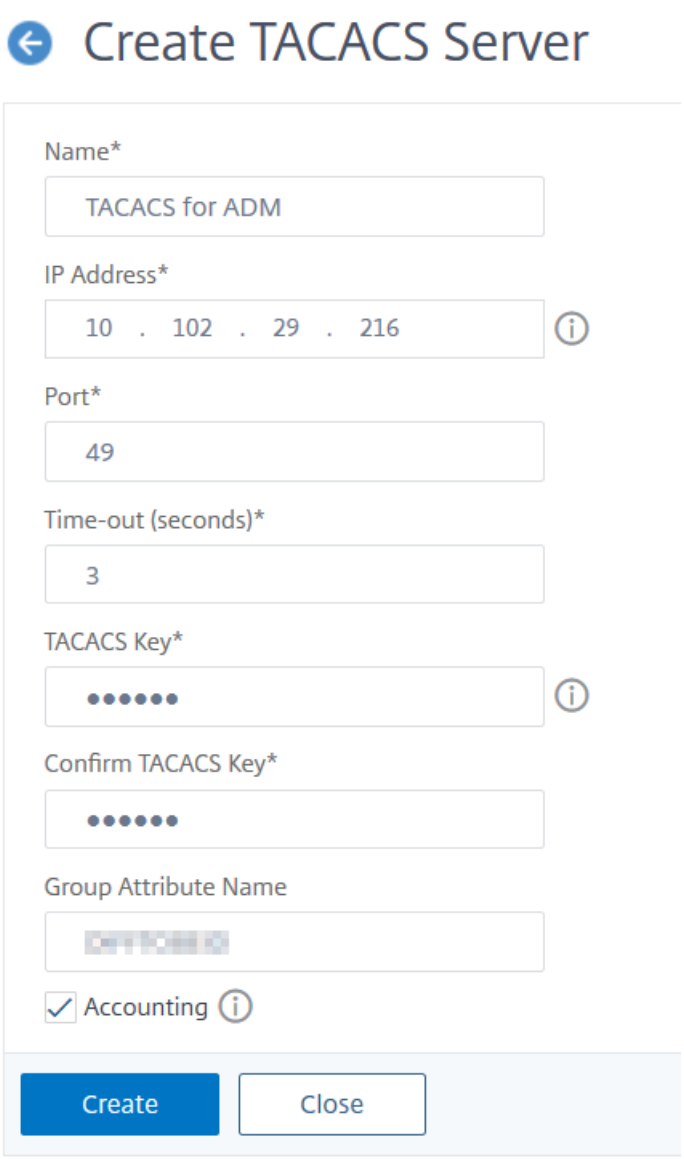
现在已配置 RADIUS 服务器。

添加 **TACAS** 身份验证服务器

April 23, 2021

1. 导航到 “ 系统” > “ 身份验证”。
2. 选择 TA **CAS** 选项卡，然后单击 添加。
3. 在 “ 创建 **TACCS** ” 页上，指定以下参数：
   a) 名称 — 指定 TACCS 服务器名称
   b) **IP** 地址 — 指定 TACCS IP 地址
   c) 端口 — 指定托管 TACCS 服务器的端口号。默认端口为 49
   d) 超时（秒） — Citrix ADM 系统等待 LDAP 服务器响应的时间（以秒为单位）
   e) **TACAS** 密钥 — 指定用于身份验证的 TACAS 密钥
   f) 确认 **TACCS** 密钥 — 再次指定 TACS 密钥进行确认
   g) 组属性名称 — 指定组名称

   如果希望设备使用 TACAS 服务器记录审 核信息，请选择会计。
4. 单击创建。



Citrix ADM 中的用户

April 23, 2021

您可以在 Citrix ADM 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，您可能希望为临时用户（例如顾问或访客）创建本地用户帐户，而无需在身份验证服务器上为这些用户创建条目。

有关配置用户的详细信息，请参阅 配置用户。

> 注意
>
> 如果用户位于 Active Directory 中，请确保 Citrix ADM 中的组名称与外部服务器上的 Active Directory 组的

> 名称相同。

Citrix ADM 中的用户组

Citrix ADM 允许您通过创建组并将用户添加到组来对用户进行身份验证和授权。一个组可以具有 “admin” 或 “只读” 权限，该组中的所有用户将获得相同的权限。

在 Citrix ADM 中：

- 组被定义为具有相似权限的用户集合
- 一个组可以具有一个或多个角色
- 用户被定义为可以根据分配的权限拥有访问权限的实体
- 用户可以属于一个或多个组

您可以在 Citrix ADM 中创建本地组，并对组中的用户使用本地身份验证。如果使用外部服务器进行身份验证，请将 Citrix ADM 上的组配置为与内部网络中的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 Citrix ADM 上该组的设置。
如果使用本地身份验证，请创建用户并将其添加到 Citrix ADM 上配置的组中。然后，用户继承这些组的设置

有关配置组和分配组权限的详细信息，请参阅 配置组。

提取身份验证服务器组

April 23, 2021

> 注意
>
> **Citrix ADM 13.0** 支持 **TA**CAS 服务器提取。

通过 Citrix ADM，您可以：

- 提取用户在外部身份验证服务器上所属的组列表。
- 将它们分配给与外部服务器上配置的组匹配的组设置。

优点：

- 您不必在 Citrix ADM 中创建用户，因为这些用户在外部服务器上进行管理。
- Citrix ADM 通过为系统上的特定应用程序分配访问特定负载平衡器虚拟服务器的组权限来执行用户授权。

启用回退和级联外部身份验证服务器

April 23, 2021

回退选项允许在外部服务器身份验证失败时接管本地身份验证。在 Citrix ADM 和外部身份验证服务器上配置的用户可以登录到 Citrix ADM，即使已配置的外部身份验证服务器已关闭或无法访问也是如此。要确保回退身份验证工作，请执行以下操作：

- 如果外部服务器关闭或无法访问，则非 NSroot 用户必须能够访问 Citrix ADM
- 必须至少添加一个外部服务器

Citrix ADM 还支持统一的身份验证、授权和记帐 (AAA) 协议系统（LDAP、RADIUS 和 TACAS）以及本地身份验证。这种统一的支持提供了一个通用界面，用于验证和授权访问系统的所有用户和外部 AAA 客户端。

无论用户要与系统通信的实际协议如何，Citrix ADM 都可以对用户进行身份验证。
级联外部身份验证服务器提供持续无故障的外部用户身份验证和授权处理。如果第一个身份验证服务器上的身份验证失败，Citrix ADM 将尝试使用第二个外部身份验证服务器对用户进行身份验证，依此类推。要启用级联身份验证，必须在 Citrix ADM 中添加外部身份验证服务器。可以添加任何类型的受支持的外部身份验证服务器（RADIUS、LDAP 和 TACACS）。

例如，假设您要添加四个外部身份验证服务器，并配置了两个 RADIUS 服务器、一个 LDAP 服务器和一个 TACAS 服务器。Citrix ADM 会根据配置尝试使用外部服务器进行身份验证。在此示例方案中，Citrix ADM 尝试执行以下操作：

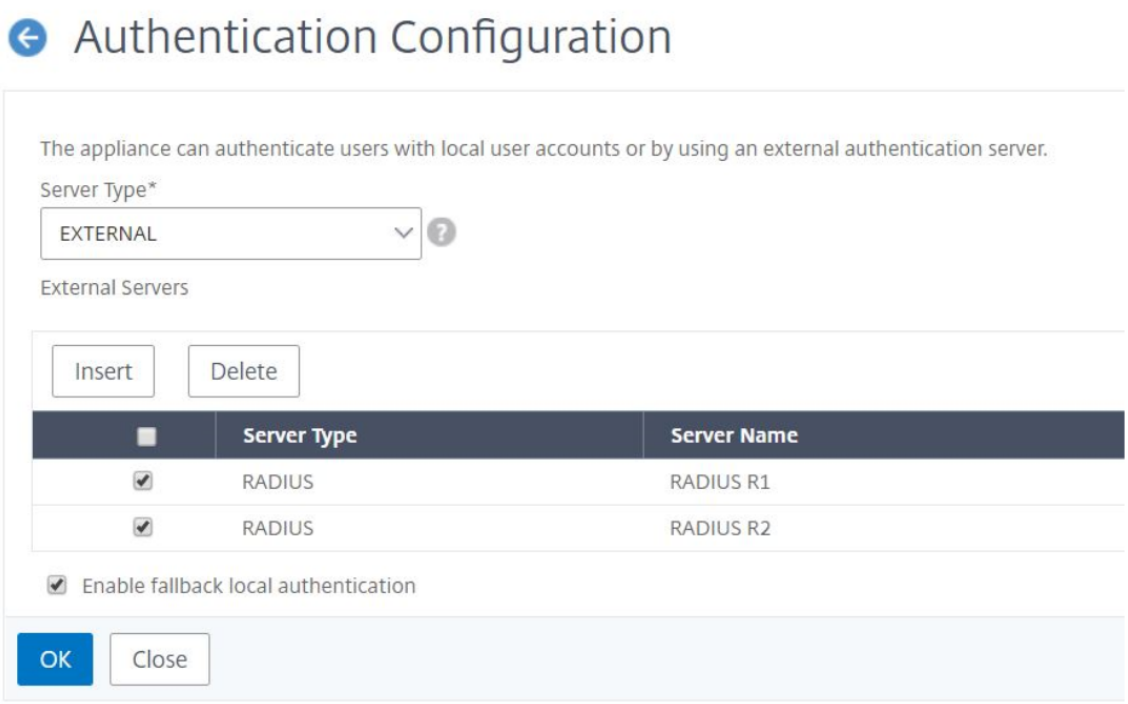
- 连接第一台 RADIUS 服务器
- 如果第一台 RADIUS 服务器的身份验证失败，请与第二台 RADIUS 服务器连接
- 连接 LDAP 服务器（如果两个 RADIUS 服务器的身份验证都失败）
- 如果 RADIUS 服务器和 LDAP 服务器的身份验证都失败，请与 TACAS 服务器连接。

> 注意
>
> 您可以在 Citrix ADM 中配置多达 32 个外部身份验证服务器。

配置回退和级联外部服务器

1. 导航到 “ 系统” > “ 身份验证”。
2. 在 “ 身份验证” 页面上，单击 “ 设置”
3. 在 “ 身份验证配置” 页上，从 “ 服务器类型” 列表中选择 “ 外部”（只能级联外部服务器）。
4. 单击 插入，然后在 “ 外部服务器” 页上，选择要级联的一个或多个身份验证服务器。
5. 如果希望在外部 身份验证失败时接管本地身份验证，请选中启用备用本地身份验证复选框。
6. 如果要捕获系统审核 日志中的外部用户组信息，请选中 “记录外部组信息” 复选框。
7. 单 击 **“**确定” 关闭页面。

   选定的服务器显示在 “外部服务器” 下：



还可以使用服务器名称旁边的图标在列表中上下移动服务器来指定身份验证顺序。

访问控制

April 23, 2021

身份验证是验证某人是否属实的过程。要执行身份验证，用户必须已经在系统中创建了一个可由身份验证机制查询的帐户，或者必须在第一次身份验证过程中创建一个帐户。Citrix Application Delivery Management (ADM) 提供了一种对本地用户和外部用户进行身份验证的方法。当本地用户在内部进行身份验证时，Citrix ADM 支持使用 RADIUS、LDAP 和 TACAS 协议进行外部身份验证。当用户尝试访问配置为外部身份验证的 Citrix ADM 时，请求的应用程序服务器将用户名和密码发送到 RADIUS、LDAP 或 TACAS 服务器进行身份验证。通过身份验证后，将使用所需的协议来识别 Citrix ADM 上的用户。

访问控制是对特定资源强制实施所需安全的过程。它是用于控制哪些人可以查看或使用计算环境中的资源的安全技术。访问控制的目的是限制计算机系统的合法用户可以执行的操作。访问控制限制了用户可以直接执行的操作以及允许代表用户运行的程序执行的操作。通过这种方式访问控制旨在防止可能导致安全漏洞的活动。访问控制假定在通过参考监视器强制实施访问控制之前已成功完成用户的身份验证。Citrix ADM 允许基于角色的细粒度访问控制 (RBAC)，通过这种控制，管理员可以根据企业中各个用户的角色向用户提供访问权限。Citrix ADM 中的 RBAC 是通过创建访问策略、角色、组和用户来实现的。

基于角色的访问控制

April 23, 2021

Citrix ADM 提供了基于角色的细粒度访问控制 (RBAC)，您可以根据企业内各个用户的角色授予访问权限。在此上下文中，访问是指能够执行特定任务，例如，查看、创建、修改或删除文件。角色是根据企业中用户的授权和职责进行定义。例如，可能允许一个用户执行所有网络操作，而另一个用户可以观察应用程序中的流量并帮助创建配置模板。

角色由策略决定。创建策略后，即可创建角色、将每个角色绑定到一个或多个策略以及为用户分配角色。您还可以为用户组分配角色。

组是拥有共同权限的用户集合。例如，管理特定数据中心的用户可以分配到一个组。角色是根据特定条件授予用户或组的身份。在 Citrix ADM 中，创建角色和策略特定于 Citrix ADC 中的 RBAC 功能。可以根据企业逐步发展的需求轻松地创建、更改或停用角色和策略，而无需单独更新每个用户的权限。

角色可以基于功能，也可以基于资源。例如，假定一个 SSL/安全管理员和一个应用程序管理员。SSL/安全管理员必须对 SSL 证书管理和监视功能具有完全访问权限，但对于系统管理操作必须具有只读访问权限。应用程序管理员必须只能访问范围内的资源。

示例：

ADC 集团负责人 Chris 是其组织中 Citrix ADM 的超级管理员。Chris 创建三个管理员角色：安全管理员、应用程序管理员和网络管理员。

安全管理员 David 必须具有 SSL 证书管理和监控的完全访问权限，但对系统管理操作也具有只读访问权限。

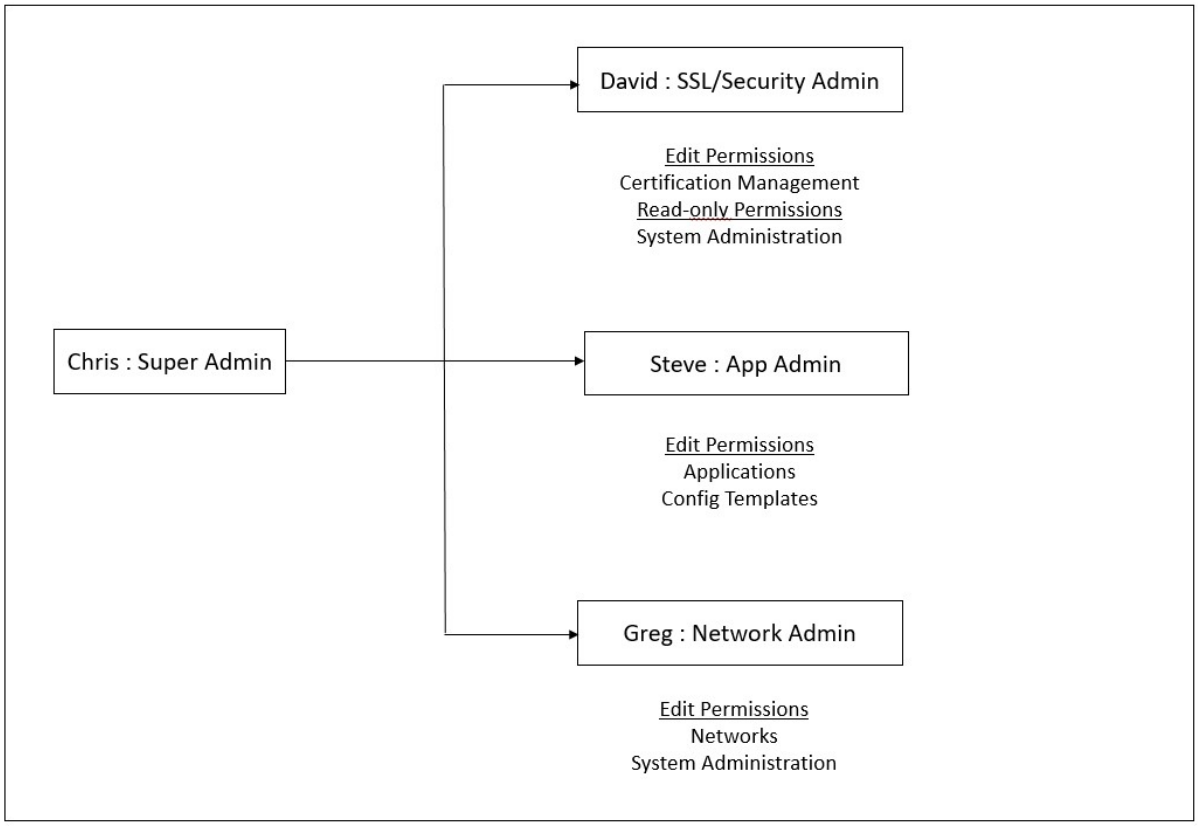
应用程序管理员 Steve 需要只对特定应用程序和特定配置模板拥有访问权限。

网络管理员 Greg 需要访问系统和网络管理的权限。

Chris 还必须为所有用户提供 RBAC，无论他们是本地还是外部用户。

Citrix ADM 用户可以在本地进行身份验证，也可以通过外部服务器（RADIUS/LDAP/TACACS）进行身份验证。RBAC 设置必须适用于所有用户，无论采用的身份验证方法是什么。

下图显示了管理员和其他用户拥有的权限以及他们在组织中的角色。



限制

以下 Citrix ADM 功能不完全支持 RBAC：

- 分析-分析模块中不完全支持 RBAC。在 Web Insight、SSL Insight、Gateway Insight、HDX Insight 和 Security Insight 分析模块中，RBAC 支持限于实例级别，不适用于应用程序级别。例如：

示例 **1**：基于实例的 RBAC（支持）

已分配了几个实例的管理员只能在 Web 智能分 析 **>** 实例下查看这些实例，而且只能在 **Web** 智能分 析 > 应 用程序下查看相应的虚拟服务器，因为 RBAC 在实例级别受支持。

示例 **2**：基于应用程序的 RBAC（不支持）

已分配了几个应用程序的管理员可以在 **Web Insight** > 应用程 序下查看所有虚拟服务器，但无法访问它们，因为 RBAC 在应用程序级别不受支持。

- 样书 — 样书不完全支持 RBAC。
  - 在 Citrix ADM 中，样书和配置包被视为单独的资源。可以单独或同时为样书和配置包提供访问权限（查看、编辑或两者）。对配置包的查看或编辑权限隐式允许用户查看样书，这对于获取配置包详细信息和创建配置包至关重要。

- 不支持特定样书或配置包的访问权限
  示例：如果实例上已有配置包，则用户可以修改目标 Citrix ADC 实例上的配置，即使他们无权访问该实例。

- 编排 -编排不支持 RBAC。

配置访问策略

April 23, 2021

访问策略定义权限。一个策略可以应用于一个用户或组，也可以应用于多个用户和多个组。Citrix Application Delivery Management (ADM) 提供了四个预定义的访问策略：

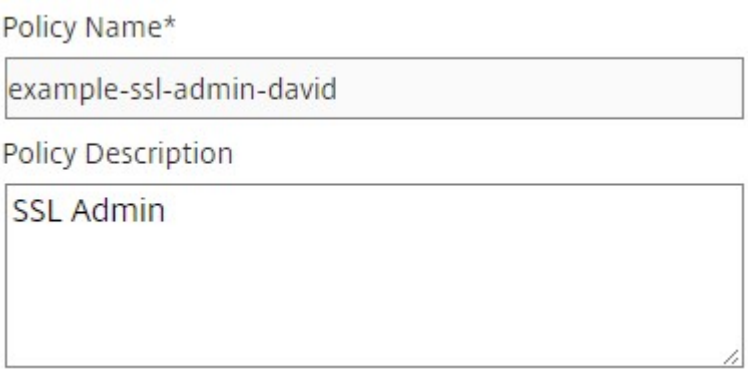
1. 行政政策. 授予对所有 Citrix ADM 功能的访问权限。用户具有查看和编辑权限，可以查看所有 Citrix ADM 内容，并可以执行所有编辑操作。即，用户可以对资源执行添加、修改和删除操作。
2. 即读政策。授予只读权限。用户可以查看 Citrix ADM 上的所有内容，但无权执行任何操作。
3. 应用程序管理员策略。授予用于访问 Citrix ADM 中应用程序功能的管理权限。绑定到此策略的用户可以添加、修改和删除自定义应用程序，并可以启用或禁用服务、服务组和各种虚拟服务器，例如，内容交换、缓存重定向和 HAProxy 虚拟服务器。
4. 制定政策。授予对应用程序功能的只读权限。绑定到此策略的用户可以查看应用程序，但不能执行任何添加、修改或删除、启用或禁用操作。

> 注意不能编辑预定义策略。

您还可以创建自己（用户定义）的策略。

要创建用户定义访问策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 用户管理” > “ 访问策略”。
2. 单击添加。
3. 在 策略名称字段中，输入策略的名称，然后在策略描述字段中输入 描述。



“ 权限部分列出了所有 Citrix ADM 功能，以及用于指定只读、启用禁用或编辑访问的选项。

4. 单击 (+) 图标将每个功能组展开为多个功能。

   a) 选中功能名称旁边的权限复选框以向用户授予权限。

      - 查看：此选项允许用户查看 Citrix ADM 中的功能。
      - 启用-禁用：此选项仅适用于允许在 Citrix ADM 上启用或禁用操作的 网络功能功能。用户可以启用或禁用该功能。而且，用户还可以执行“立 即投票操作。

        向用户授予“ 启用-禁用”权限时，也会授予“ 查看”权限。您不能取消选择此选项。

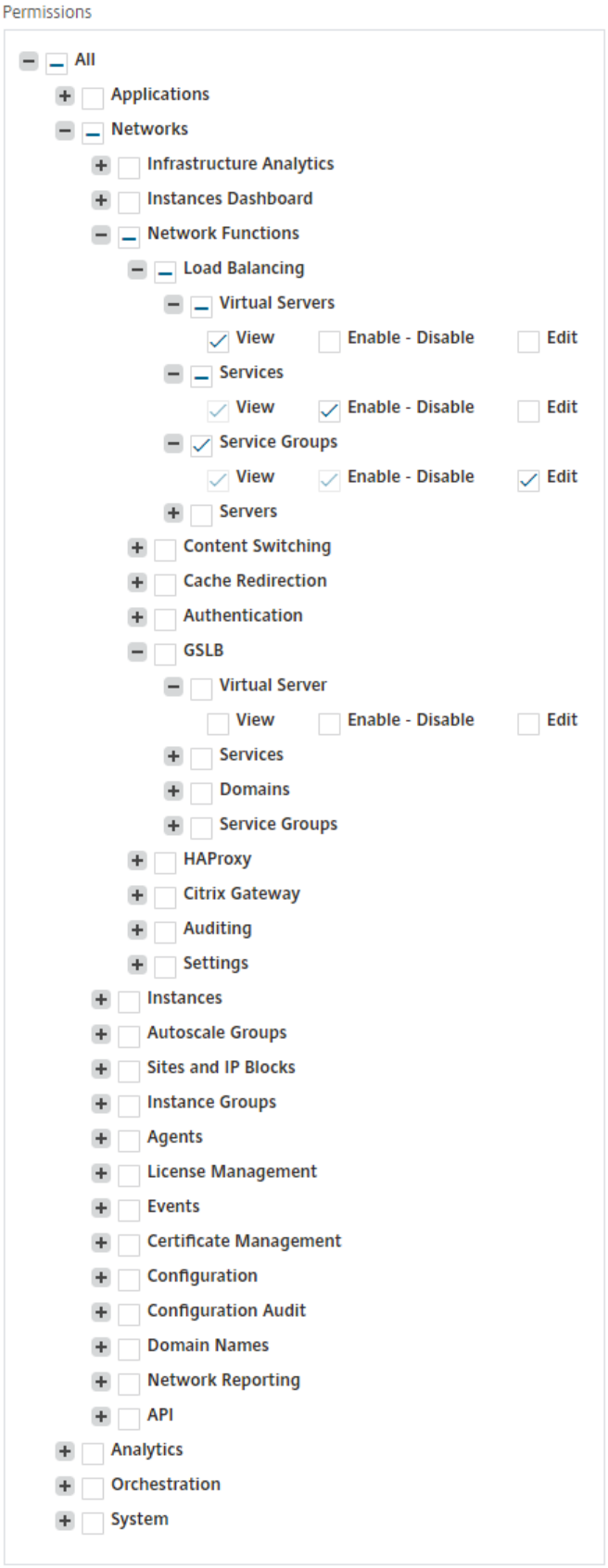
      - 编辑：此选项授予用户的完全访问权限。用户可以修改功能及其功能。

        如果授予“编辑”权限，则会同时授予 查看权限和 启用-禁用权限。您不能取消选择自动选择的选项。

   如果选中功能复选框，则会选择该功能的所有权限。

   > 注意：
   >
   > 展开负载平衡和 GSLB 以查看更多配置选项。

在下图中，负载平衡功能的配置选项具有不同的权限：



“查 看” 权限授予用户使用 虚拟服务器功能。用户可以在 Citrix ADM 中查看负载平衡虚拟服务器。要查看虚拟服务器，请导航到 “网 络 > 网络功能 > 负载平衡”，然后选择 虚拟服务器选项卡。

向用户授予 服务功能的 启用-禁用权限。此权限还授予 “查 看” 权限。用户可以启用或禁用绑定到负载平衡虚拟服务器的服务。此外，用户可以对服务执行 立即投票操作。要启用或禁用服务，请导航到 “网络” > 网络功能 > 负载平衡”，然后选择 服务选项卡。

> 注意：
>
> 如果用户具有 “ 启用-禁用” 权限，则对服务的启用或禁用操作将在以下页面中受到限制：
>
> a) 导航到 “ 网络” > “ 网络功能”。
>
> b) 选择虚拟服务器，然后单击 配置。
>
> c) 选择 “负 载平衡虚拟服务器服务绑定” 页。如果选择 启用或 “禁用”，此页将显示一条错误消息。

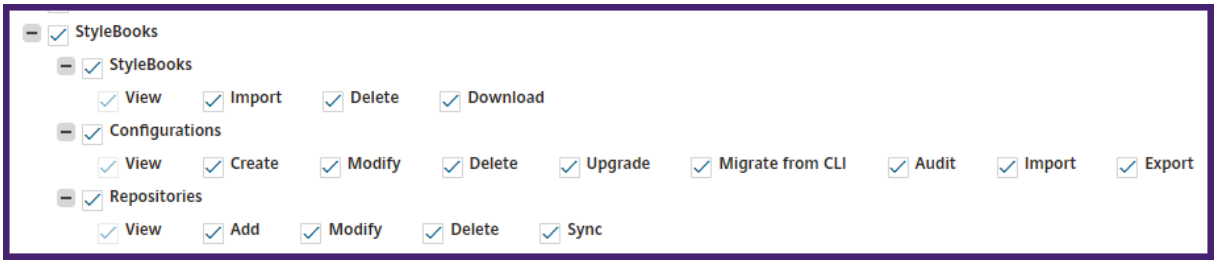
“ 编辑” 权限授予用户使用 “ 服务组” 功能。此权限授予授予 查看和 启用-禁用” 权限的完全访问权限。用户可以修改绑定到负载平衡虚拟服务器的服务组。要编辑服务组，请导航到 “网 络 > 网络功能 > 负载平衡”，然后选择服务组选项卡。

5. 单击创建。

向用户授予样书权限

您可以创建访问策略来授予样书权限，例如导入、删除、下载等。

> 注意：
>
> 当您授予其他样书权限时，将自动启用 “查看” 权限。



配置组

April 23, 2021

在 Citrix ADM 中，组可以具有功能级别和资源级别的访问权限。例如，一组用户可能只能访问选定的 Citrix ADC 实例；另一组只能访问选定的几个应用程序，依此类推。

创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。该组中的所有用户都在 Citrix ADM 中分配相同的访问权限。

您可以在网络功能实体的各个级别管理 Citrix ADM 中的用户访问权限。您可以在实体级别动态为用户或组分配特定权限。

Citrix ADM 将虚拟服务器、服务、服务组和服务器视为网络功能实体。

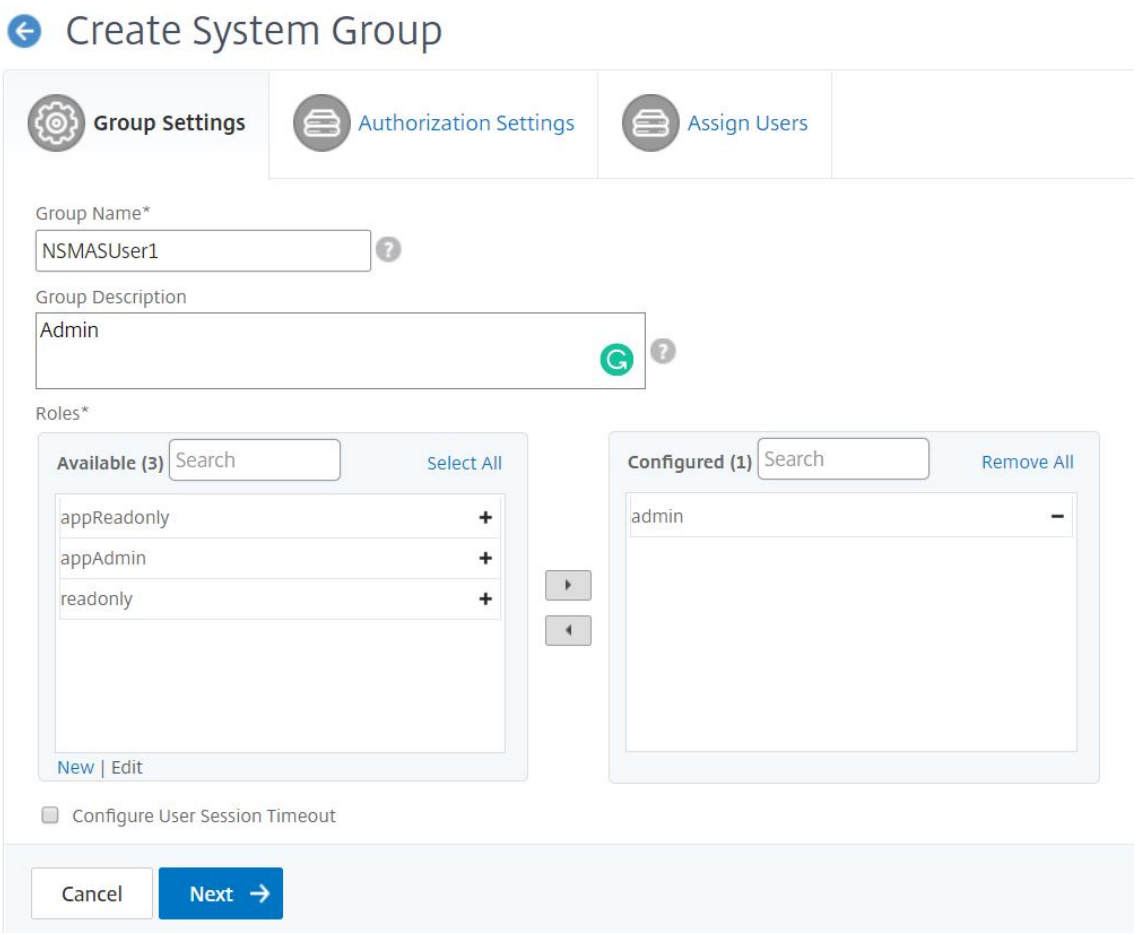
- 虚拟服务器（应用程序） -负载平衡 (lb)、GSLB、上下文切换 (CS)、缓存重定向 (CR)、身份验证 (Auth) 和 Citrix Gateway (VPN)
- 服务 -负载平衡和 GSLB 服务
- 服务组 -负载平衡和 GSLB 服务组
- 服务器 -负载平衡服务器

创建用户组

1. 在 Citrix ADM 中，导航到 系统 > 用户管理 > 组。
2. 单击添加。

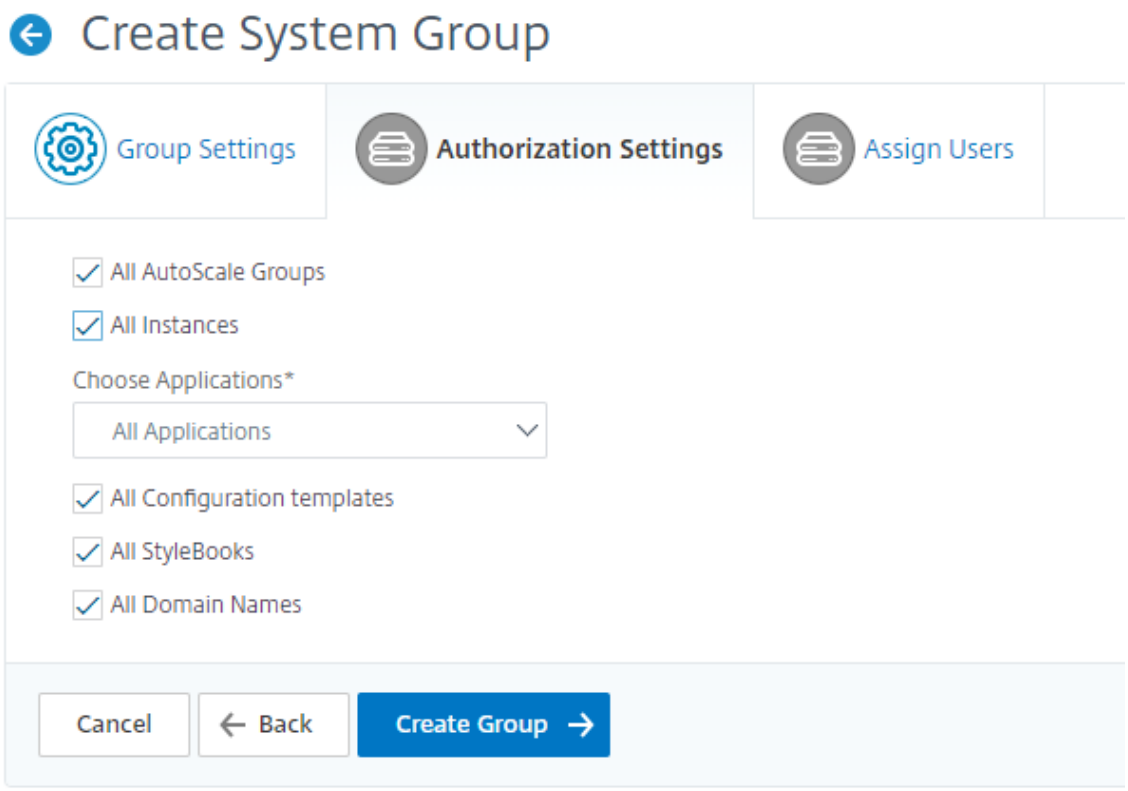
   此时将显示 创建系统组页面。
3. 在 组名称字段中，输入组的名称。
4. 在“组说明”字段中，键入组的说明。提供组的良好描述有助于您以更好的方式了解组的作用和职能。
5. 在“ 角色”部分中，将一个或多个角色添加或移动到“ 已配置”列表中。

   > 注意：
   > 在“可 用”列表下，您可以单击“ 新建”或“ 编辑”，然后创建或修改角色。或者，您可以导航到“ 系统”>“ 用户管理”>“用 户”，然后创建或修改用户。



6. 单击“ 下一步”。在“ 授权设置”选项卡上，您可以为以下资源提供授权设置：

   - 自动缩放组
   - 实例
   - 应用程序
   - 配置模板
   - 样本
   - 配置包
   - 域名



您可能希望从用户可以访问的类别中选择特定资源。

自动缩放组：

如果要选择用户可以查看或管理的特定自动缩放组，请执行以下步骤：

a) 清除 所有自动扩展组复选框，然后单击 添加自动扩展组。

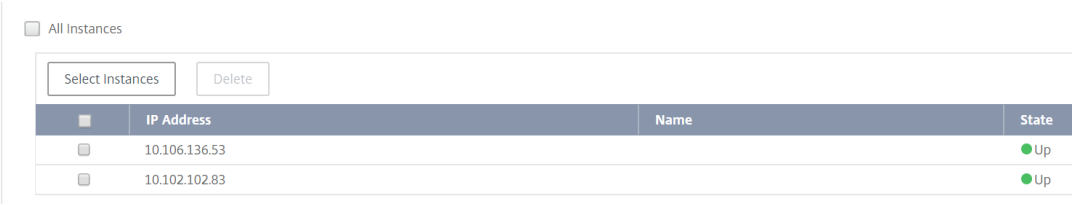
b) 从列表中选择所需的“自动缩放”组，然后单击“ 确定”。

实例：

如果要选择用户可以查看或管理的特定实例，请执行以下步骤：

a) 清除 所有实例复选框，然后单击 选择实例。

b) 从列表中选择所需的实例，然后单击“ 确定”。



应用程序**：**

“ 选择应用程序**”** 列表允许您向用户授予所需应用程序的访问权限。

您可以授予对应用程序的访问权限，而无需选择应用程序的实例。因为应用程序独立于其实例以授予用户访问权限。

当您授予用户对应用程序的访问权限时，无论选择何种实例，用户都有权仅访问该应用程序。

此列表为您提供以下选项：

- 所有应用程序：默认情况下选择此选项。它会添加 Citrix ADM 中存在的所有应用程序。
- 所选实例的所有应用程序：仅当您从 所有实例” 类别中选择实例时，才会显示此选项。它会添加所选实例上存在的所有应用程序。
- 特定应用程序：此选项允许您添加希望用户访问的必需应用程序。单击 添加应用程序”，然后从列表中选择所需的应用程序。
- 选择单个实体类型：此选项允许您选择特定类型的网络函数实体和相应实体。

  您可以添加单个实体，也可以选择所需实体类型下的所有实体，以向用户授予访问权限。

  “ 应用于绑定实体也” 选项授权绑定到选定实体类型的实体。例如，如果选择某个应用程序并选择 “ 同时应用于绑定实体”，Citrix ADM 将授权绑定到所选应用程序的所有实体。

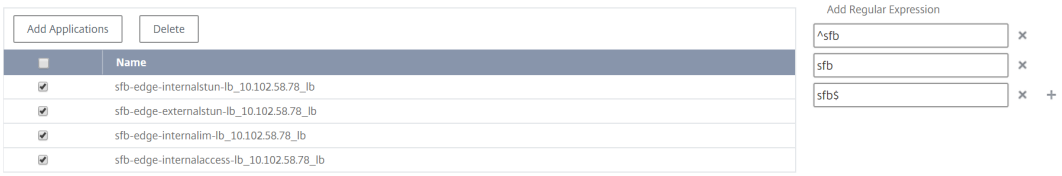
  > 注意：如果要授权绑定实体，请
  >
  > 确保只选择了一个实体类型。

您可以使用正则表达式搜索和添加满足组的正则表达式条件的网络函数实体。指定的正则表达式表达式将保留在 Citrix ADM 中。要添加正则表达式，请执行以下步骤：

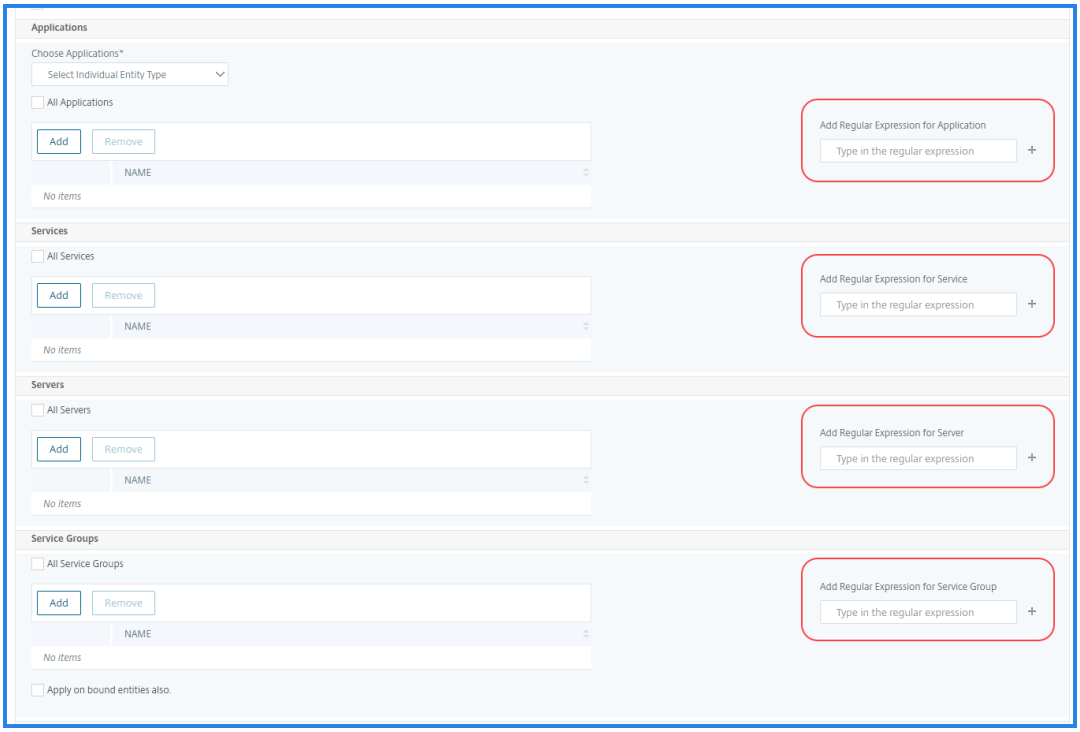
a) 单击 添加正则表达式。

b) 在文本框中指定正则表达式。

下图说明了在选择 “ 特定应用程序” 选项时如何使用正则表达式添加应用程序：



下图说明了在选择 **“选择单个实体类型”** 选项时如何使用正则表达式添加网络函数实体：



如果要添加更多正则表达式，请单击 **+** 图标。

> 注意
>
> 正则表达式仅匹配服务器实体类型的 服务器名称，而不匹配服务器 IP 地址。

如果为发现的 实体选择了“应用于绑定实体也”选项，则用户可以自动访问绑定到发现实体的实体。

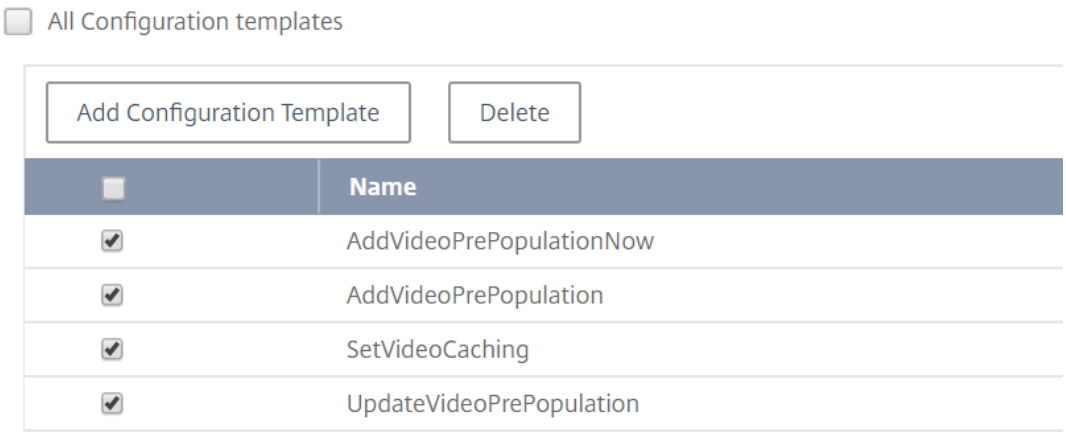
正则表达式存储在系统中以更新授权范围。当新实体与其实体类型的正则表达式匹配时，Citrix ADM 会将授权范围更新为新实体。

配置模板：

如果要选择用户可以查看或管理的特定配置模板，请执行以下步骤：

a) 清除 所有配置模板复选框，然后单击 添加配置模板。

b) 从列表中选择所需的模板，然后单击 “ 确定”。



样本：

如果要选择用户可以查看或管理的特定样书，请执行以下步骤：

a) 清除 所有样本复选框，然后单击 将样本添加到组。您可以选择单个样书，也可以指定筛选器查询来授权样书。

如果要选择单个样书，请从“单个样书”窗格中选择样本，然后单击保存所选内容。

如果要使用查询来搜索样书，请选择自定义过滤器窗格。查询是键值对的字符串，其中键是 `name`、`namespace` 和 `version`。

您还可以使用正则表达式作为值来搜索和添加符合组正则表达式条件的样书。用于搜索样书的自定义筛选器查询同时支持 `And` 和 `Or` 操作。

示例：

```
1 name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
     version=1.0
2 <!--NeedCopy-->
```

此查询列出了满足以下条件的样书：

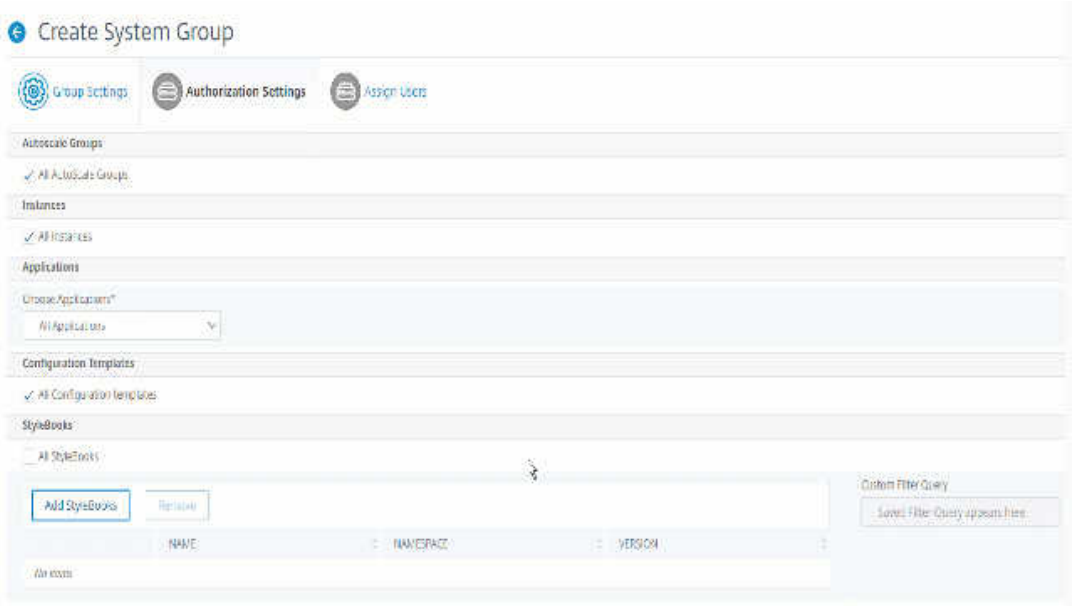
- 样书名称是 `lb-mon` 或 `lb`。
- 样书名称空间是 `com.citrix.adc.stylebooks`。
- 样书版本是 `1.0`。

在为键表达式定义的值表达式之间使用 `Or` 操作。

示例：

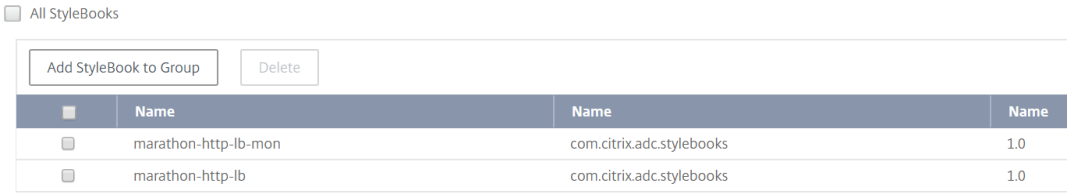
- `name=lb-mon|lb` 查询是有效的。它返回名称为 `lb-mon` 或 `lb` 的样书。
- `name=lb-mon | version=1.0` 查询无效。

按 `Enter` 以查看搜索结果，然后单击 保存查询。



保存的查询将显示在 自定义筛选器查询中。根据保存的查询，ADM 为用户提供对这些样书的访问权限。

b) 从列表中选择所需的样本，然后单击 确定”。

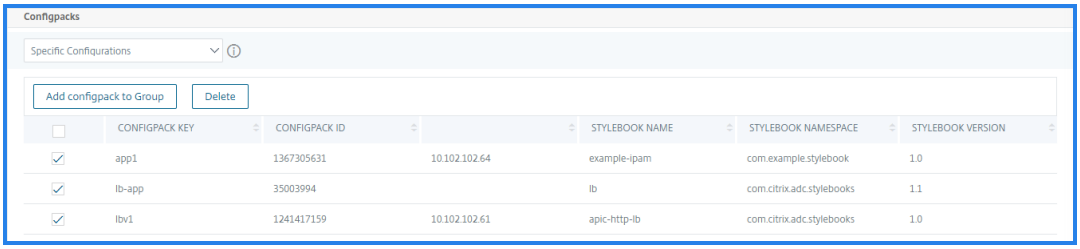


您可以在创建组并将用户添加到该组时选择所需的样本。当用户选择允许的样本时，也会选择所有相关样本。

配置包：

在 **Configpack** 中，选择以下选项之一：

- 所有配置：默认情况下，此选项处于选中状态。它添加了 ADM 中的所有配置包。
- 所选样书的所有配置：此选项添加所选样书的所有配置包。
- 特定配置：此选项允许您添加所需的配置包。



您可以在创建组并将用户添加到该组时选择所需的配置包。

域名：

如果要选择用户可以查看或管理的特定域名，请执行以下步骤：

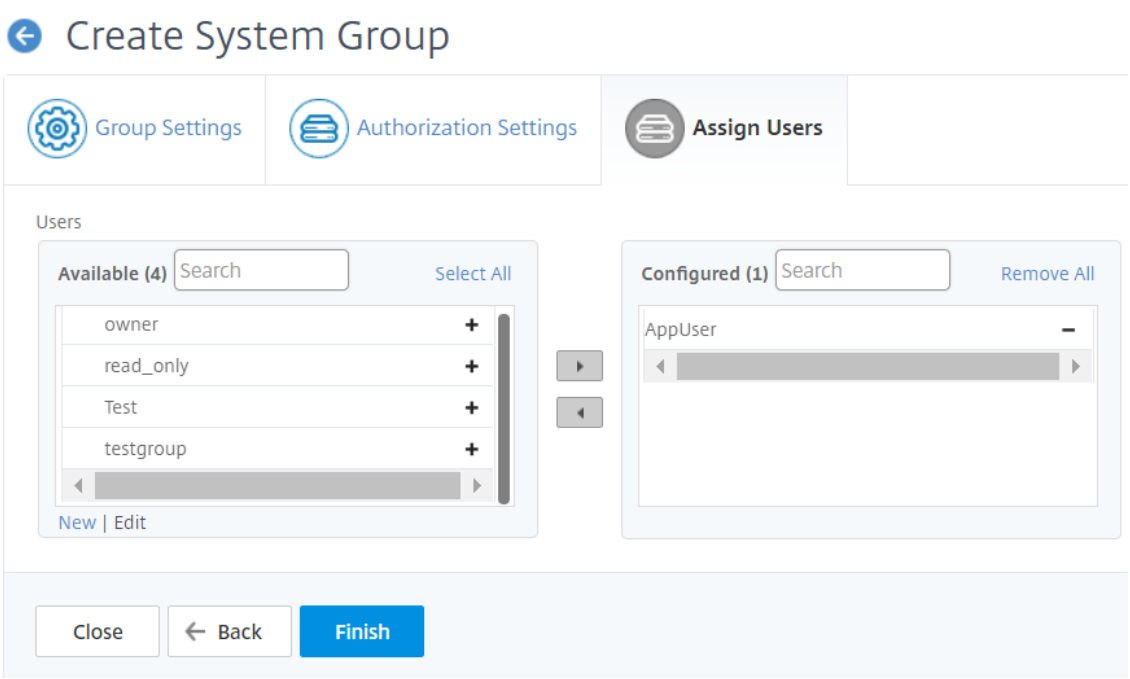
a) 清除“ 所有域名” 复选框，然后单击“ 添加域名”。

b) 从列表中选择所需的域名，然后单击“ 确定”。

7. 单击创建组。

8. 在“ 分配用户” 部分，在“ 可用” 列表中选择用户，然后将用户添加到“ 已配置” 列表中。

> 注意
>
> 您还可以通过单击“ 新建” 来添加用户。



9. 单击完成。

跨多个网络功能实体管理用户访问

作为管理员，您可以在 Citrix ADM 中网络功能实体的各个级别管理用户访问。而且，您可以使用正则表达式过滤器在实体级别动态分配特定权限给用户或组。

本文档介绍如何在实体级别定义用户授权。

在开始之前，请创建一个组。有关详细信息，请参阅在 Citrix ADM 上配置组。

使用方案：

考虑在同一台服务器上托管一个或多个应用程序（虚拟服务器）的情况。超级管理员（George）希望仅授予 Steve（应用程序管理员）对 Appp1 的访问权限，而不授予托管服务器的访问权限。

下表说明了此环境，其中服务器 A 承载应用程序应用程序 1 和应用程序-2。

主机服务器	应用程序（虚拟服务器）	服务	服务组
服务器 A	App1	App-service-1	App-service-group-1
服务器 A	App2	App-service-2	App-service-group-2

> 注意：
>
> Citrix ADM 将虚拟服务器、服务、服务组和服务器视为网络功能实体。实体类型虚拟服务器称为应用程序。

要为网络功能实体分配用户权限，George 按如下方式定义用户授权：

1. 导航到 **“帐户” > “用户管理” > “组”** ，然后添加组。
2. 在 授权设置选项卡中，选择选择应用程序。
3. 选择 **“**选择单个实体类型”。
4. 选择 “ 所有应用程序” 实体类型，然后从可用列表中添加 Appp-1 实体。
5. 单击创建组。
6. 在 分配用户中，选择需要权限的用户。在这种情况下，乔治选择史蒂夫的用户配置文件。
7. 单击完成。

使用此授权设置，Steve 只能管理 Appp-1，而不能管理其他网络功能实体。

> 注意：
>
> 确保清除 “ 同时应用于绑定实体” 选项。否则，Citrix ADM 授予对绑定到 Appp-1 的所有网络功能实体的访问权限。因此，也授予对托管服务器的访问权限。

超级管理员可以为每个实体类型指定正则表达式 (正则表达式)。正则表达式存储在系统中以更新用户授权范围。当新实体与其实体类型的正则表达式匹配时，Citrix ADM 可以动态授予用户访问特定网络功能实体的权限。

要动态授予用户权限，超级管理员可以在 “ 授权设置” 选项卡中添加正则表达式。

在这种情况下，George 添加 App* 为应用程序实体类型的正则表达式，并且符合正则表达式条件的应用程序将显示在列表中。使用此授权设置，Steve 可以访问与 App* 正则表达式匹配的所有应用程序。但是，他的访问仅限于不对托管服务器的应用程序。

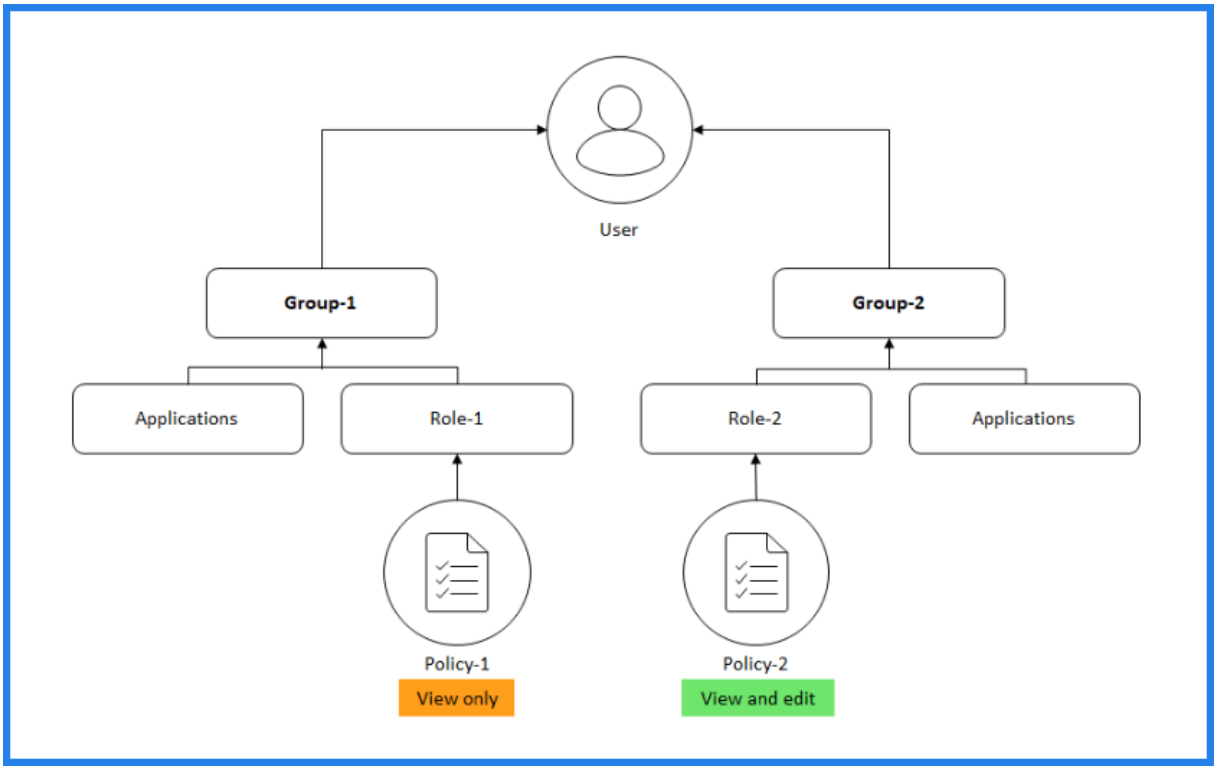
用户访问权限如何根据授权范围进行更改

当管理员将用户添加到具有不同访问策略设置的组时，该用户将被映射到多个授权作用域和访问策略。

在这种情况下，ADM 根据特定授权范围授予用户对应用程序的访问权限。

考虑分配给具有两个策略策略 1 和策略 2 的组的用户。

- 策略 **1** — 仅查看应用程序的权限。
- 策略 **2** — 查看和编辑应用程序权限。



用户可以查看策略 1 中指定的应用程序。此外，此用户还可以查看和编辑策略 2 中指定的应用程序。对组 1 应用程序的编辑访问受到限制，因为它不在组 1 授权范围内。

将 **Citrix ADM** 从 **12.0** 升级到更高版本时的 **RBAC** 映射

将 Citrix ADM 从 12.0 升级到 13.0 时，在创建组时看不到提供“读写”或“读取”权限的选项。这些权限已替换为“角色和访问策略”，使用这些策略可以更加灵活地为用户提供基于角色的权限。下表显示了 12.0 版中的权限如何映射到 13.0 版：

12.0	仅允许应用程序	13.0
admin read-write	假	`admin`
admin read-write	真	`appAdmin`
admin read-only	假	`readonly`
admin read-only	真	`appReadonly`

配置角色

April 23, 2021

在 Citrix Application Delivery Management (ADM) 中，每个角色都绑定到一个或多个访问策略。您可以在策略与角色之间定义一对一、一对多和多对多关系。您可以将一个角色绑定到多个策略，也可以将多个角色绑定到一个策略。

例如，一个角色可能绑定到两个策略，其中一个策略定义对一个功能的访问权限，另一个策略定义对另一个功能的访问权限。一个策略可能授予在 Citrix ADM 中添加 Citrix ADC 实例的权限，另一个策略可能授予创建和部署样本以及配置 Citrix ADC 实例的权限。

如果多个策略定义对某一个功能的编辑和只读权限，则编辑权限优先。

Citrix ADM 提供了四个预定义角色：

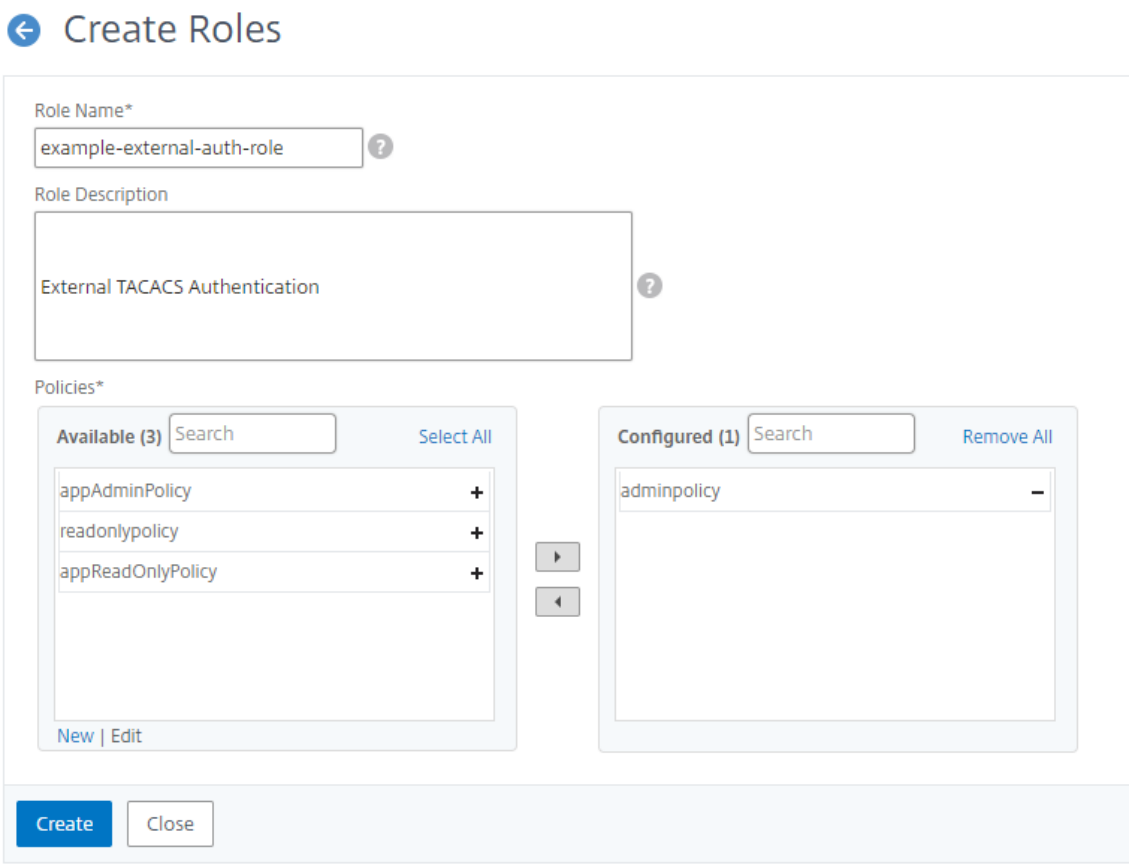
- 管理员。可以访问所有 Citrix ADM 功能。（此角色绑定到 adminpolicy。）
- 只读。拥有只读访问权限。（此角色绑定到 readonlypolicy。）
- 应用程序管理员。仅对 Citrix ADM 中的应用程序功能具有管理访问权限。（此角色绑定到 appAdminPolicy。）
- 仅限于捕获。对应用程序功能拥有只读访问权限。（此角色绑定到 appReadOnlyPolicy。）

> 注意不能编辑预定义角色。

您还可以创建自己（用户定义）的角色。

要创建角色并为其分配策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 用户管理” > “ 角色”。
2. 单击添加。
3. 在 “ 角色名称” 字段中，输入角色的名称，并在 “ 角色描述” 字段中提供说明（可选）。
4. 在 “ 策略” 部分，将一个或多个策略添加或移动到 “ 已配置” 列表中。



5. 单击创建。

配置用户

April 23, 2021

默认情况下，Citrix Application Delivery Management (ADM) 有一个用户：

nsroot - root 用户 (nsroot) 具有设备的完全管理权限。nsroot 用户是 Citrix ADM 的超级管理员。

您可以创建其他用户，方法是为其配置帐户。将新用户添加到 Citrix ADM 时，可以通过分配相应的组、角色和策略来定义用户的权限。

可以将用户分配到组并将组绑定到角色。您可以在用户、组、角色和访问策略之间定义一对一、一对多或多对多关系。可将一个用户分配到多个组。一个组可以有多个角色，多个组可以有相同角色。

要在 **Citrix ADM** 中配置用户，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 用户管理” > “用 户”。
2. 单击添加。

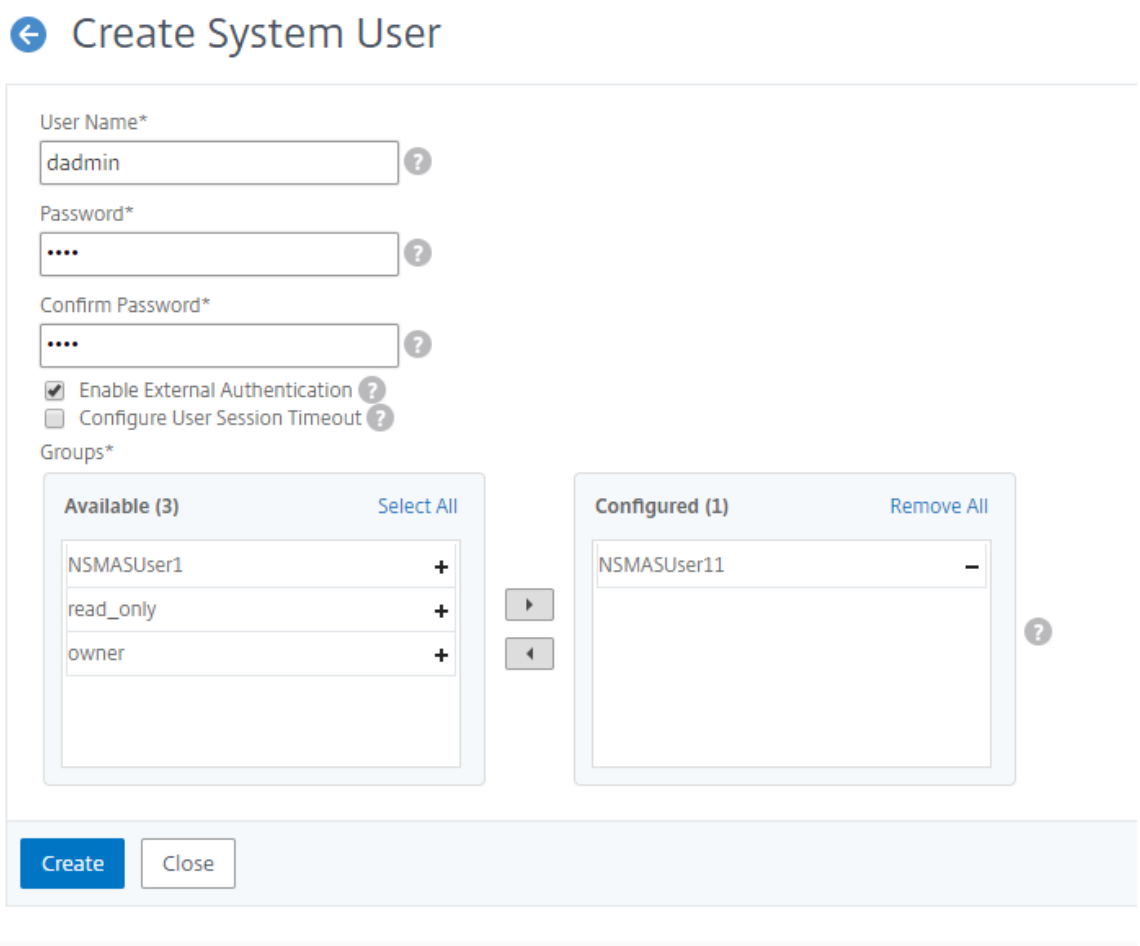
3. 输入以下详细信息：

   a) 用户名。用户的名称

   b) 密码。用户登录到 Citrix ADM 的密码

4. （可选）选择 启用外部身份验证，以便可以通过外部身份验证服务器对用户进行身份验证。

5. 如果已创建组并希望将用户分配给组，请在 “ 组” 部分中将一个或多个组从 “ 可用” 列表移动到 “已 配置” 列表。



6. 单击创建。

应用程序

April 23, 2021

Citrix ADM 的应用程序分析和管理功能使您能够通过以应用为中心的方法监视应用程序。这种方法可以帮助您：

- 检查分数并分析应用程序的整体性能
- 检查服务器或客户端是否存在任何问题

- 检测应用程序流量中的异常情况并采取纠正措施

> 注意
>
> 应用程序是指在实例上配置的一个或多个虚拟服务器 (Citrix ADC)。

您可以监视应用程序的持续时间，例如 1 小时、1 天、1 周和 1 个月。

必备条件

- 确保您已在 Citrix ADM 中添加了 Citrix ADC 实例
- 确保您拥有适用于您的 Citrix ADC 实例的有效许可证。有关详细信息，请参阅许可。
- 确保已为虚拟服务器应用许可证。有关详细信息，请参阅管理虚拟服务器上的许可。

应用程序概述

应用程序可以是：

- 离散应用
- 自定义应用程序
- 微服务应用程序（k8s_ 离散）

离散应用

所有获得许可的虚拟服务器都称为离散应用程序。

自定义应用程序

一个类别下的虚拟服务器称为自定义应用程序。作为管理员，您必须根据类别添加自定义应用程序。然后，您可以通过仪表板管理和监视应用程序。您可以轻松监视分组在一个类别下的特定应用程序。

例如，您可以为数据中心 1 创建类别并添加其 ADC 实例。为数据中心定义类别并添加实例后，应用程序仪表板将显示为单独的类别，其中包括与数据中心相关的所有应用程序 1。

注意事项

- 添加到自定义应用程序的离散应用程序将从离散应用程序中删除。
- 所有未添加到任何类别的应用程序都可以作为 **“其他”**。
- 默认情况下，Citrix ADM 允许您为最多 2 个应用程序添加许可证。根据您的许可证，您可以为要监视的应用程序选择并应用许可证。

微服务应用

在 Kubernetes 集群中，Citrix 为 Citrix ADC MPX（硬件）、Citrix ADC VPX（虚拟化）和 Citrix ADC CPX（容器化）提供了 Ingress Controller。有关详细信息，请参阅Citrix Ingress Controller。

使用 Citrix ADC CPX 实例配置的离散应用程序称为微服务应用程序。

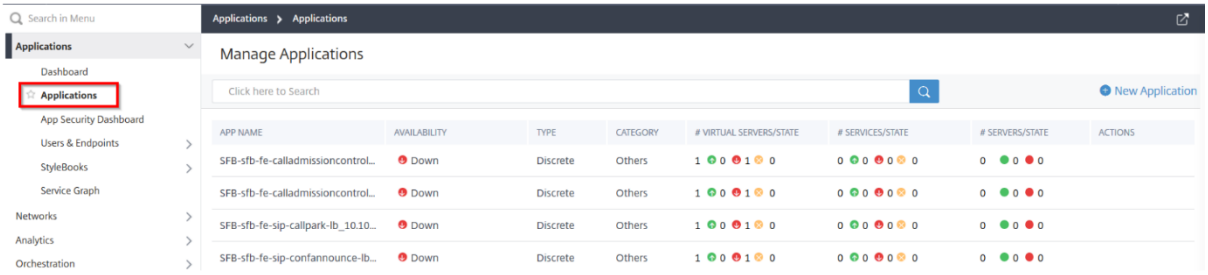
应用程序管理和应用程序仪表板

April 23, 2021

Citrix ADM 使您能够从“应用程序”页面管理应用程序，并从“ 仪表板”页面查看 应用程序详细信息。

管理应用程序

使 用 **“**应用程序”页可以查看所有自定义和离散应用程序。



在“ 应用程序”页中，作为管理员，您可以执行以下操作：

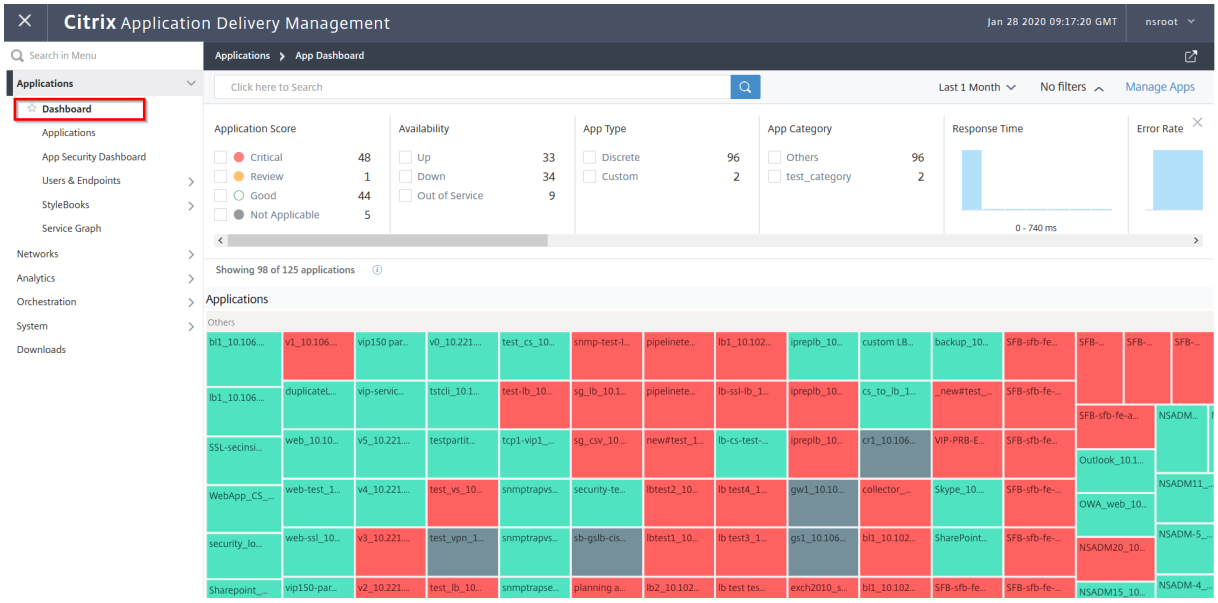
- 添加应用程序
- 查看应用程序详细信息，如应用程序名称、应用程序类别、关联的虚拟服务器、关联的服务等。
- 编辑或删除自定义应用程序

添加、编辑或删除应用程序后，详细信息将立即反映在“应用程序”页中。

有关详细信息，请参阅管理应用程序。

应用程序仪表板

导航至“ 应用程序”>“ 仪表板”，以表格视图或图形视图中查看应用程序列表。



只有在应用程序开始填充数据后，所有应用程序才会显示在仪表板中。在仪表板中，单击应用程序以查看应用程序性能的详细信息。有关详细信息，请参阅应用程序详细信息。

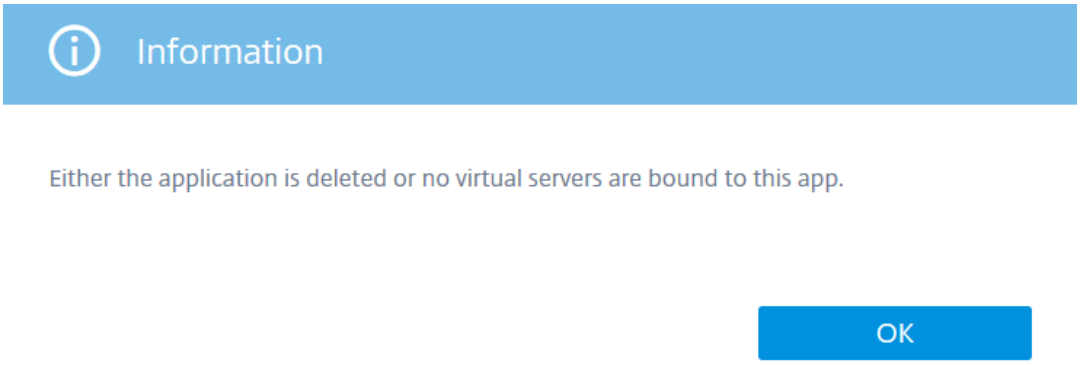
如果即使持续时间大约 10 到 15 分钟后仍未显示应用程序分析，请执行应用仪表板疑难中的故障排除步骤。

与早期仪表板相比，新仪表板行为的更新

- 添加或编辑自定义应用程序后，可能需要几分钟才能在仪表板中反映该应用程序。
- 如果删除自定义应用程序，仪表板仍会显示已删除的应用程序，直到 ADM 拥有其分析数据（最长为 1 个月的持续时间）。

  假设您在 2020 年 1 月 2 日创建了应用程序并于 2020 年 1 月 4 日删除了该应用程序的情况。在此情景中：

  - 当您选择过去 1 天、1 周和 1 个月的时间持续时间时，仪表板仍然可以在 2020 年 1 月 4 日显示已删除的应用程序。
  - 当您选择过去 1 周和 1 个月的时间持续时间时，仪表板仍然可以在 2020 年 1 月 5 日显示已删除的应用程序。
  - 当持续时间超过应用程序删除日期时，应用程序不会显示在仪表板中。也就是说，在 2020 年 1 月 6 日（最后 1 天）、2020 年 1 月 12 日（最后 1 周）和 2020 年 2 月 5 日（最后 1 个月）之后（最后 1 个月）不显示仪表板。
  - 从仪表板中单击已删除的应用程序时，将显示以下消息。

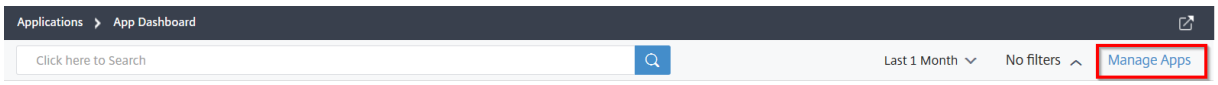


> 注意
>
> 添加应用程序后，如果关联的 Citrix ADC 实例处于关闭状态、无法使用或因临时网络故障而无法访问：
>
> -与 ADC 实例关联的应用程序仅在“应用程 序”页面中可见，但在仪表板中不可见。
>
> -ADC 实例启动并运行后，应用程序将显示在仪表板中。

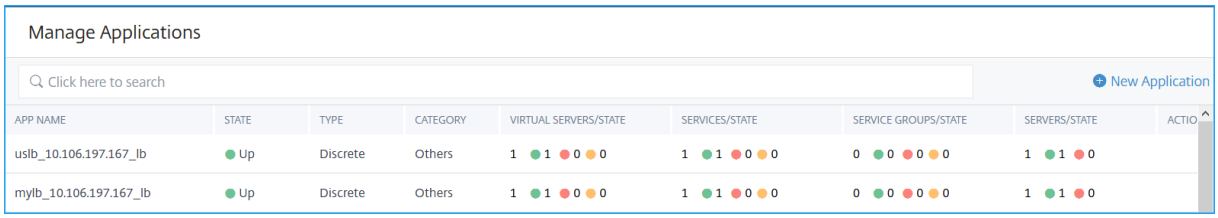
管理应用程序

April 23, 2021

在仪表板中，单击“ 管理应用程序”以查看应用程序详细信息以及添加、编辑或删除自定义应用程序。



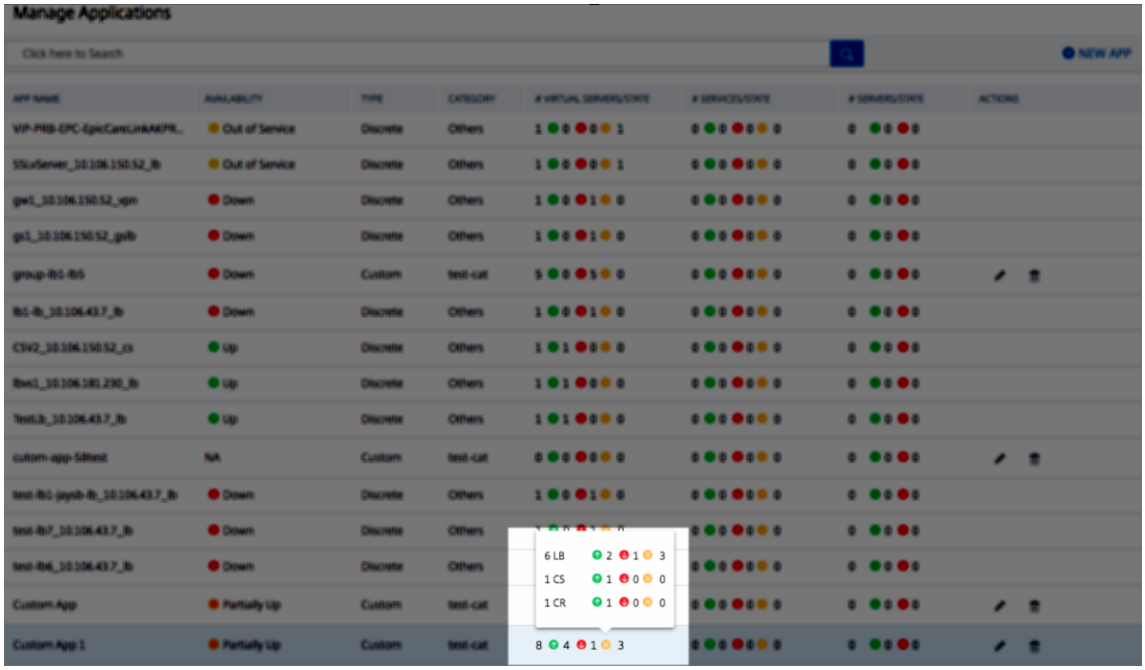
查看应用程序详细信息



- 应用程序名称 — 表示应用程序名称
- 可用性 — 表示应用程序的当前可用性，如“ 启动”、“关 闭”、“ 部分启动”、“停 止服务”和“ **NA**”
  - 启动 — 与应用程序关联的所有虚拟服务器均为“启动”。
  - 关闭 — 与应用程序关联的所有虚拟服务器均为关闭
  - 部分启动 — 与应用程序关联的一个虚拟机处于关闭状态或停止服务状态

  - 不服务 — 与应用程序关联的所有虚拟服务器都停用
  - **NA** — 没有为应用程序配置虚拟服务器

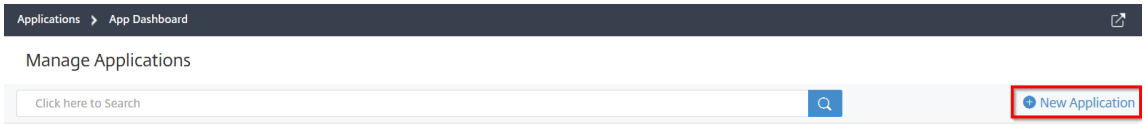
- 类型 — 表示应用程序是属于“自定义”还是“离散”
- 类别 — 表示分组的应用程序类别
- 虚拟服务器/状态 — 表示配置的虚拟服务器总数以及所有虚拟服务器的当前状态。将鼠标指针悬停以查看详细信息，如虚拟服务器总数、虚拟服务器类型和虚拟服务器状态



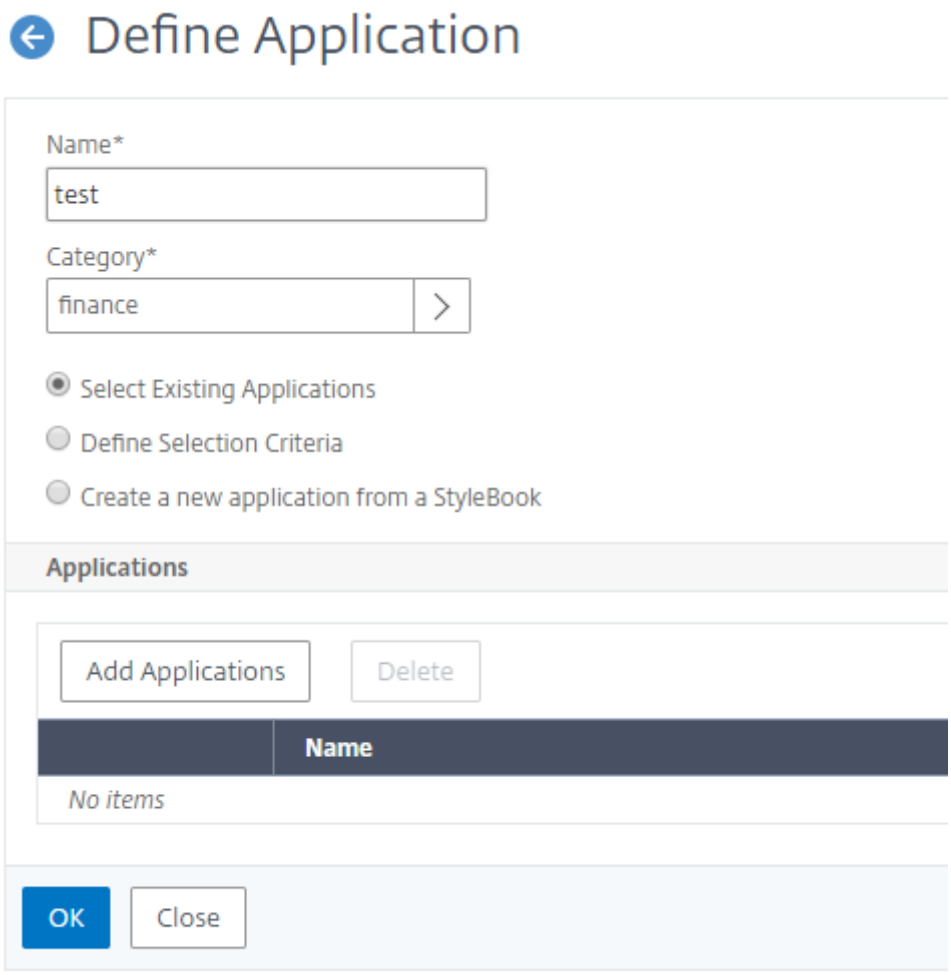
- 服务/状态 — 表示配置的总服务和所有服务的当前状态
- 服务组/状态 — 表示已配置的服务组总数和所有服务组的状态
- 服务器/状态 — 表示为应用程序配置的服务器总数以及所有服务器的当前状态
- 操作 — 允许您编辑或删除自定义应用程序

添加应用程序

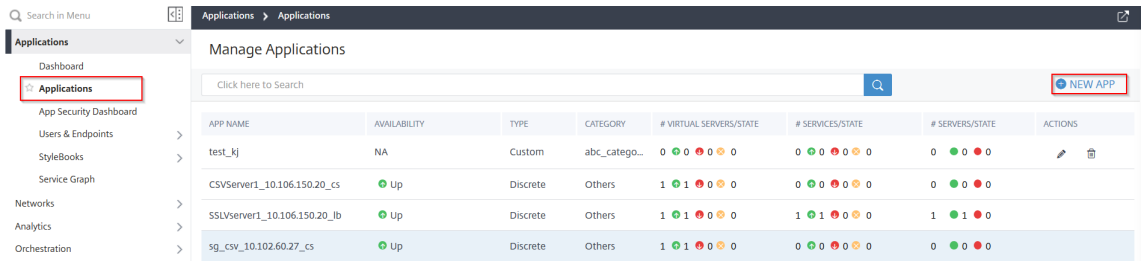
1. 单击“ 新建应用程序”以创建新应用程序



此时将显示“ 定义应用程序”页



> 注意
>
> 您还可以单击“ 应用程序”，然后选择“ 新建应用程序”以添加新的应用程序



2. 设置以下参数：

字段	说明
名称	自定义应用程序的名称。例如，LB_TEST。

字段	说明
类别	您可以对应用程序进行分组的类别。单击以获取“应用程序类别”页面。选择类别，然后单击选择。要添加类别，请执行以下操作： 1. 单击添加。 2. 输入您选择的名称。 3. 单击“创建”
Select Existing Applications（选择现有应用程序）	使您可以选择添加到 Citrix ADC 实例的现有应用程序。
添加应用程序	显示在实例上配置的所有虚拟服务器。从列表中选择应用程序，然后单击确定。
Define Selection Criteria（定义选择条件）	该选项用于按虚拟服务器范围或按源服务器/服务 IP 地址范围定义应用程序。
	- 服务器。指定运行应用程序的服务器或服务 IP 地址、服务器名称或后端服务器的端口。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。
	- 虚拟服务器。您可以指定以下任一项：虚拟服务器 IP 地址、虚拟服务器名称或运行应用程序的后端服务器的端口。可以输入一个 IP 地址、一个 IP 地址范围或以逗号分隔的两者组合。例如，可以输入 10.102.29.20, 10.102.43.10-60, 10.216.43.45。
从样本创建新应用程序	使您能够使用样本创建应用程序。有关详细信息，请参阅使用样本创建应用程序。

a) 单击确定。

> 注意
>
> 目前，应用程序控制板仅支持负载平衡和内容交换虚拟服务器。

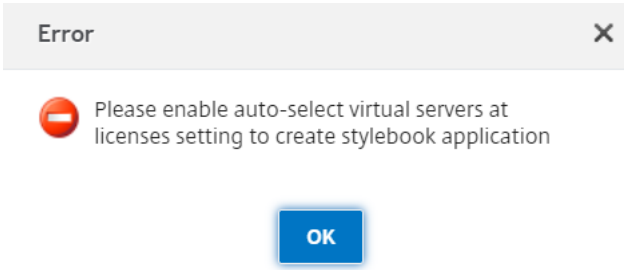
应用程序控制板现在与类别一起显示，所有应用程序都分组在下方。

如果为自定以应用程序选择从样本创建新应用程序选项，则必须允许 Citrix ADM 自动选择要授权的虚拟服务器。要为虚拟服务器启用自动选择：

a) 导航到 系统 > 许可和分析。

b) 在虚拟服务器许可摘要下，单击自动选择虚拟服务器并自动选择不可寻址的虚拟服务器以启用。

如果不启用这些选项，将显示以下错误消息。



使用样本创建应用程序

要使用样本创建应用程序，请执行以下操作：

1. 在 Citrix ADM 中，导航到应用程序 > 控制板，然后单击定义自定义应用程序以创建自定义应用程序。
2. 在定义应用程序页面中，在名称字段中键入应用程序的名称。
3. 从 Category（类别）部分中选择应用程序类别。Citrix ADM 允许您定义类别以对用户定义的应用程序进行分组。如有必要，您还可以添加更多类别。
4. 单击以选择从样本创建新应用程序，然后单击确定。

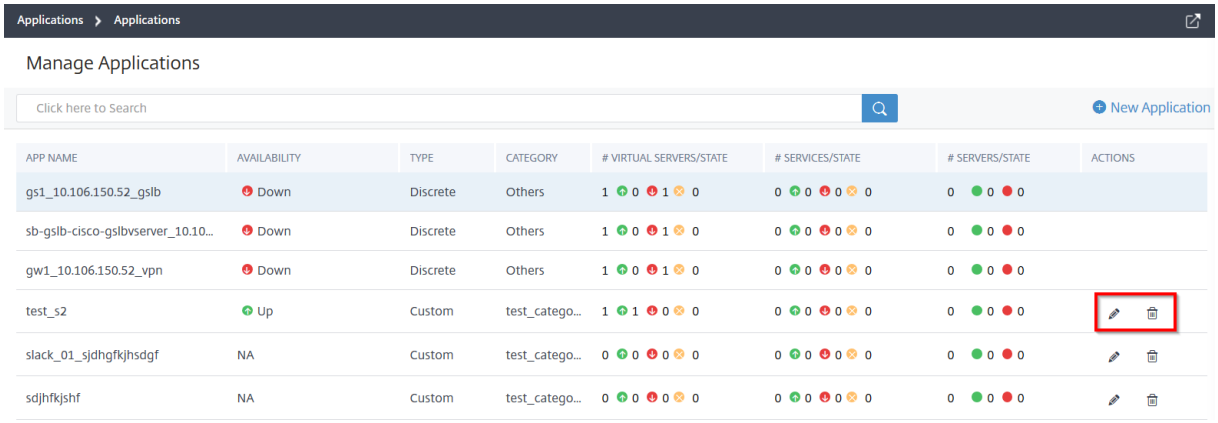
   此时将显示选择样本页面。此页面包含 Citrix ADM 中可用的所有默认样本。
5. 选择样本。
   此时将显示配置详细信息页面。
6. 在样本中键入所有参数的值。您也可以单击“查看定义”以查看样本的构造，然后再使用样本。

   有关详细信息，请参阅使用默认样本。
7. 单击创建。

   您还可以单击 干运行以检查 Citrix ADM 尝试在选定的 Citrix ADC 实例上创建的配置。此选项仅用于测试目的，以查看对配置的最终检查。即使“试运行”选项成功，所选 Citrix ADC 上的实际配置仍可能由于各种原因（IP 冲突、无法访问实例等）而失败。

编辑或删除应用程序

在“ 应用程序”页中，可以编辑或删除自定义应用程序。单击编辑按钮编辑应用程序，然后单击删除按钮删除应用程序。



导出应用程序控制板和安全控制板的报告

Citrix ADM 允许您拍摄当前应用程序仪表板的快照并将其导出为报表。在频繁的时间间隔内，应用管理员可能需要使用这些报告来更新应用使用情况和性能损失。

使用此功能，管理员可以将此数据提取为.png、.jpeg 或.pdf 报表。

> 注意
>
> 与 Citrix ADM 中的其他报表导出选项不同，您只能将应用程序控制板和安全控制板报表导出为.pdf 或.png 文件。目前不支持.csv 格式。

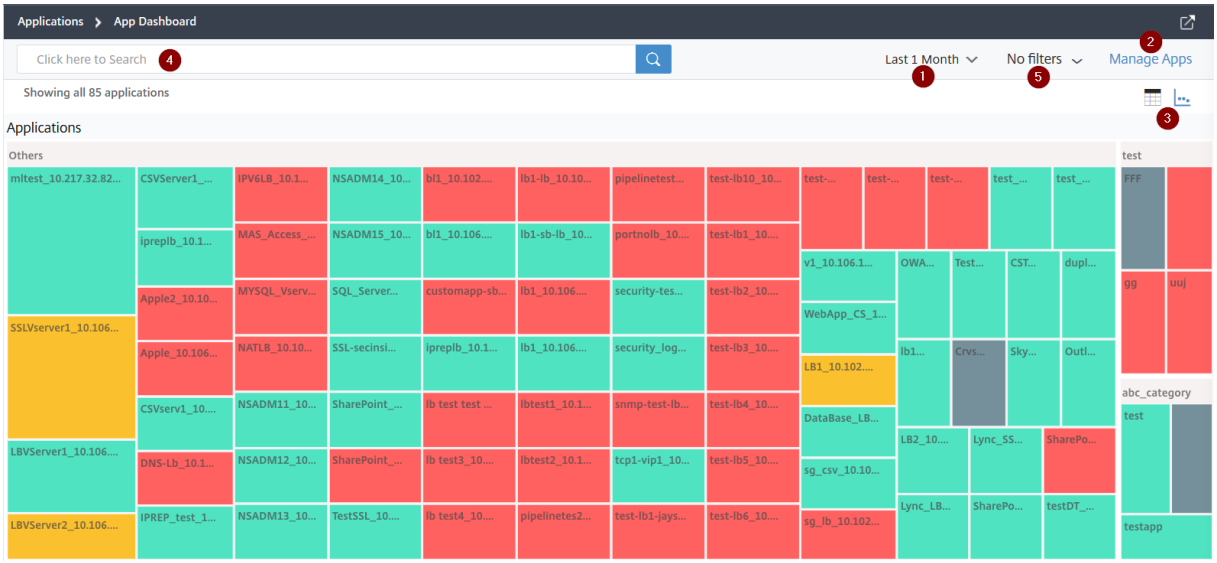
报告将下载到您的系统中。在“应用程序仪表板”和“应用程序安全仪表板”页面中，您还可以导航到二级页面并将其导出为报表。目前，您一次只能下载一个应用程序的报告。

应用程序仪表板概述

April 23, 2021

应用程序仪表板显示“ 其他”下的离散应用程序以及分组在各自类别下的自定义应用程序。

导航到应用程序 > 控制板以查看应用程序控制板。



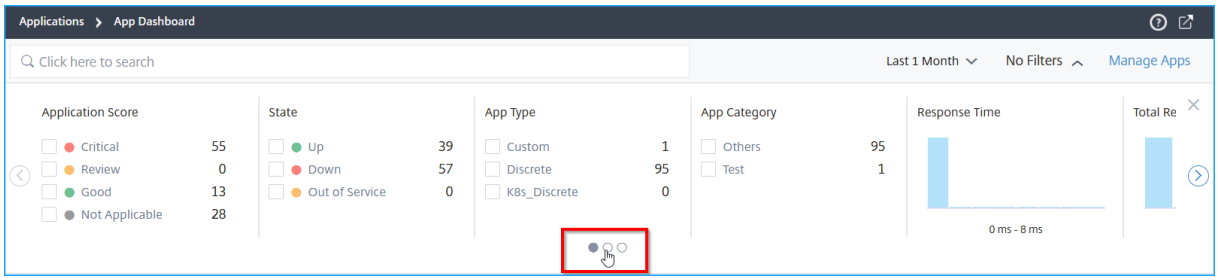
1 — 显示选定时间持续时间的应用程序详细信息，如 1 小时、1 天、1 周和 1 个月。

2 — 使您能够管理应用程序和添加新应用程序

3 — 使您能够在表视图或图形视图中查看应用程序

4 — 使您能够使用搜索栏搜索应用程序

5 — 使您能够应用筛选器来查看应用程序。单击查看详细信息。

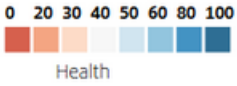


您可以选择旋转木马滑块，使您可以轻松访问所有选项。

可以执行以下操作：

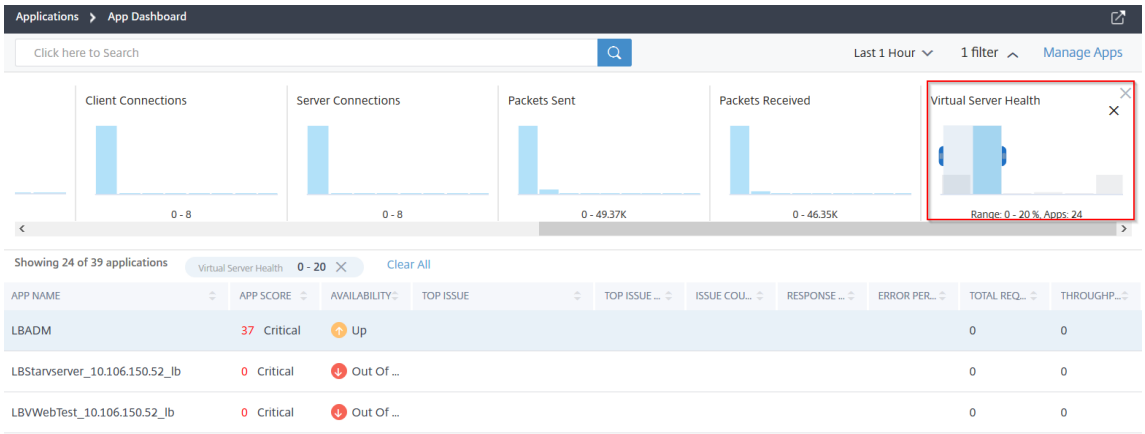
- 选择以查看基于分数的应用程序。
  - 关键 — 应用程序得分介于 0 到小于 40 之间
  - 公平 — 申请分数介于 40 和小于 75 之间
  - 好 — 申请分数大于 75
  - 不适用 — 未为应用程序配置虚拟服务器

    下表描述了早期应用分数与当前应用分数之间的差异。

申请分数（关键、评论、良好、不适用）	应用程序分数（早期视图与颜色图例）
分数计算为 **100** 减去所有应用程序当前问题的点球得分	分数计算为 **100 —**（应用程序服务器资源 **+ Citrix ADC** 系统资源）
应用程序以 红色（关键）、橙色（审查）、绿色（好）和 ** 灰色（不适用）** 等颜色显示应用程序	应用程序显示在颜色图例中。 

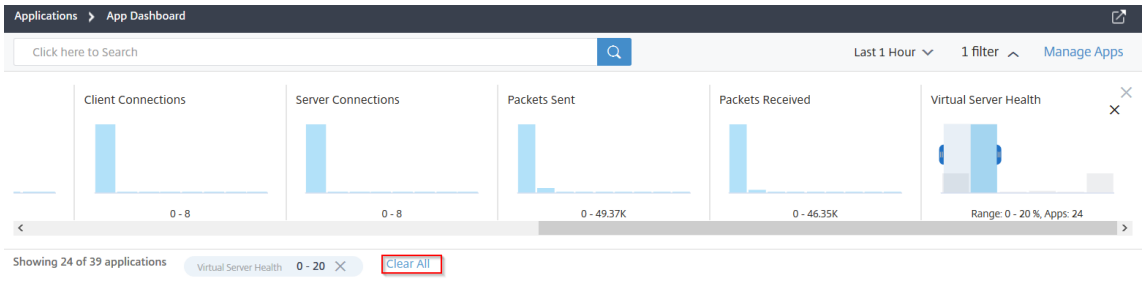
- 选择此选项可根据应用程序状态（如“启动”、“关闭”和“停止服务”）查看应用程序
- 选择此选项可根据应用程序类型（如离散或自定义）查看应用程序
- 选择以查看基于下面分组的类别的应用程序
- 拖动直方图以应用筛选器并查看应用程序。

  例如，如果要查看虚拟服务器运行状况介于 0 到 20 之间的应用程序，请拖动虚拟服务器运行状况直方图以筛选结果。



> 注意
>
> 您也可以单击直方图以显示相关应用程序。

单击 全部清除以清除应用的筛选器。

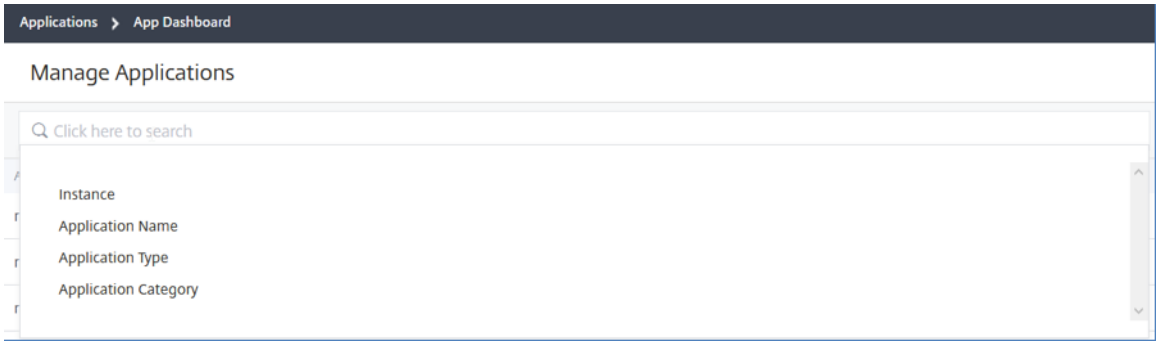


以下是您可以应用筛选器的应用程序摘要：

- 响应时间 — 显示应用程序收到的平均响应时间的直方图
- 错误率 — 显示应用程序 5xx 错误的平均误差百分比的直方图
- 请求总数 — 显示应用程序接收的请求总数的直方图
- 吞吐量 — 显示应用程序处理的总网络吞吐量的直方图
- 数据量 — 显示应用程序处理的总数据的直方图。数据量由应用程序的总请求字节和响应字节计算。
- 客户端连接 — 显示应用程序建立的平均客户端连接的直方图
- 服务器连接 — 显示应用程序建立的平均服务器连接的直方图
- 已发送的数据包 — 显示应用程序发送的数据包总数的直方图
- 收到的数据包 — 显示应用程序接收的数据包总数的直方图
- 虚拟服务器运行状况 — 显示分数范围 0% 到 100% 之间的应用程序总数的直方图。虚拟服务器运行状况是与应用程序关联的活动服务的 (%)。例如，如果虚拟服务器配置了 2 个服务，且其中一个服务低于，则分数为 50%。

使用搜索栏搜索和筛选结果

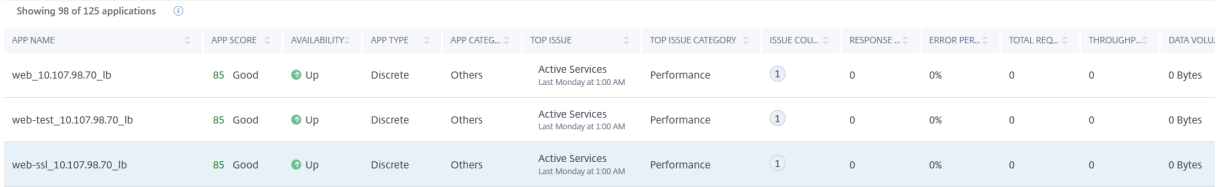
您可以将鼠标指针放在搜索栏上，然后选择类别以优化搜索。



查看应用程序

April 23, 2021

默认情况下，应用程序仪表板显示所有应用程序。根据您的需求，您可以使用筛选器选项来查看应用程序。



仪表板显示以下应用程序详细信息：

- 应用程序名称 — 表示应用程序名称
- 应用程序得分 **—** 表示应用程序得分和状态，如 “ 严重”、“ 良好”、“ 公平” 和 “ 不适用”
- 可用性 — 表示应用程序的当前可用性，如 “ 启动”、“关 闭”、“ 部分启动”、“停 止服务” 和 “ **NA**”
  - 启动 — 与应用程序关联的所有虚拟服务器均为 “启动”。
  - 关闭 — 与应用程序关联的所有虚拟服务器均为 “关闭”。
  - 部分启动 — 与应用程序关联的一个虚拟机处于 “关闭” 或 “不服务” 状态。
  - 不服务 — 与应用程序关联的所有虚拟服务器都停用。
  - **NA** — 没有为应用程序配置虚拟服务器。
- 顶级问题 — 表示应用程序上具有最大错误计数的问题
- 顶级问题类别 — 表示问题的类别
- 问题计数 — 表示应用程序的总问题计数
- 响应时间 — 表示应用程序响应的平均响应时间
- 错误百分比 — 表示应用程序 5xx 错误的总错误百分比

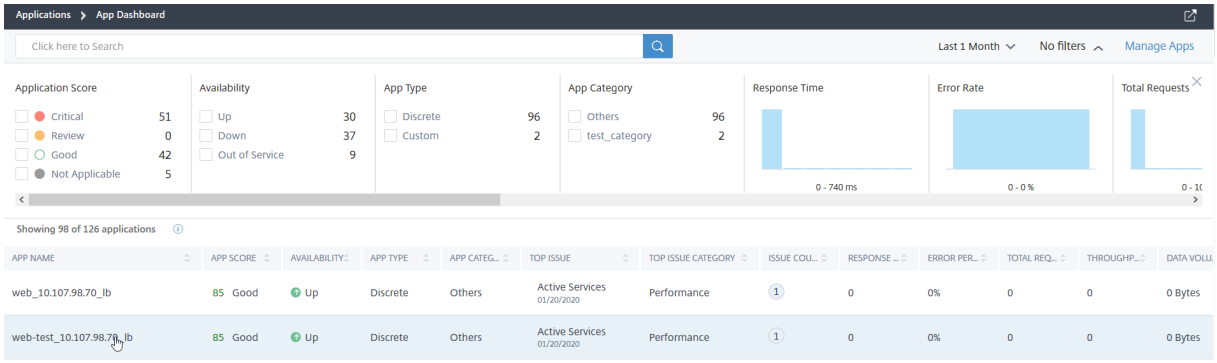
  > 注意
  >
  > 仅针对 **Citrix ADC 13.0** 或更高版本显示 5xx 错误百分比度量。对于早期版本，该值显示为 **0**。

- 请求总数 — 表示应用程序接收的请求总数
- 吞吐量 — 表示应用程序的总网络吞吐量。吞吐量由虚拟服务器的 Rq 字节/秒 + Res 字节/秒计算
- 数据量 — 表示应用程序处理的总数据
- 客户端连接 — 表示应用程序建立的平均客户端连接
- 服务器连接 — 表示应用程序建立的平均服务器连接

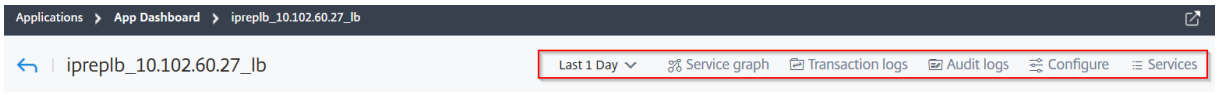
应用程序详细信息

April 23, 2021

单击仪表板中的应用程序可向下钻取以获取更多详细信息。



将显示选定的应用程序页面。

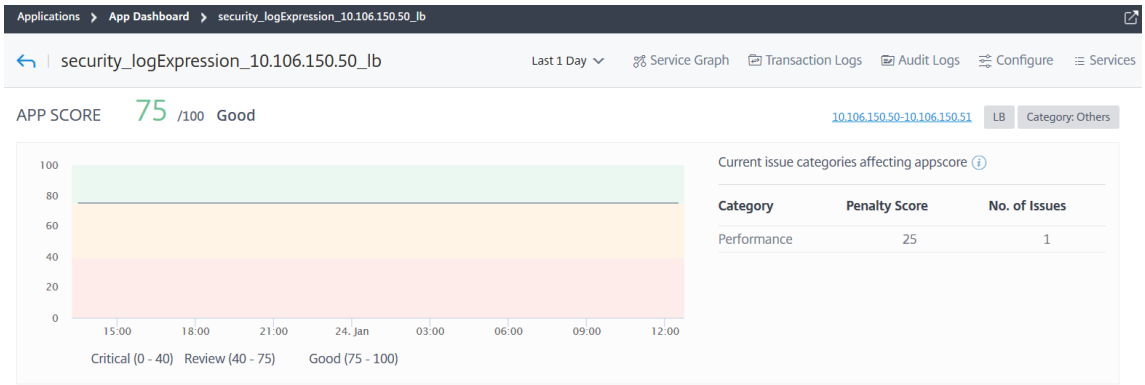


从应用程序详细信息页面：

- 从列表中选择时间持续时间以查看特定时间持续时间的详细信息
- 单击 服务图表可查看所选应用程序的服务图表。有关详细信息，请参阅应用程序的服务图。
- 单击 事务日志查看 5xx 错误的详细交易记录
- 单击 审计日志查看详细的审计日志信息
- 单击 “ 配置” 查看或编辑应用程序的服务和服务组配置
- 单击 “ 服务” 查看绑定到应用程序的服务

选择时间持续时间后，将显示以下应用程序详细信息：

- 应用程序分数 — 选定时间持续时间的应用程序分数。最终得分计算为 **100** 减去总罚款。



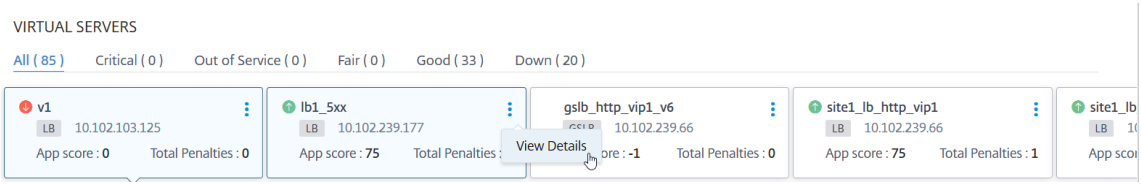
此仪表板还允许您查看影响应用程序分数的当前问题。您可以在问题下查看问题详细信息。

- 虚拟服务器 —

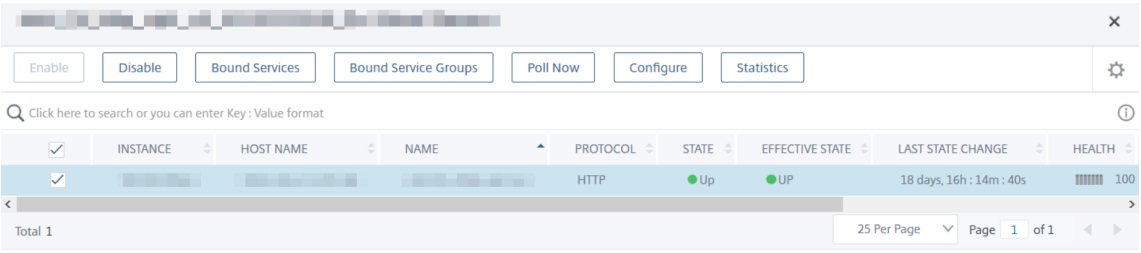
> 注意
>
> 仅对自定义应用程序显示 “ 虚拟服务器” 部分。对于离散应用程序，请单击 **IP** 地址以查看虚拟服务器的详

> 细信息。

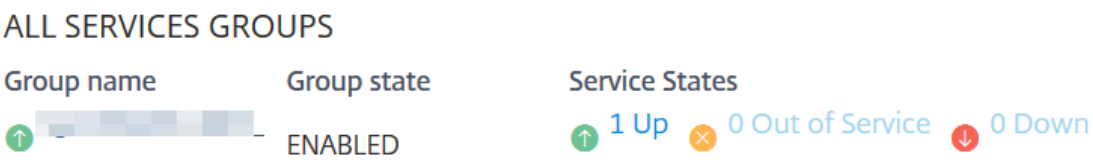
显示与自定义应用程序关联的所有虚拟服务器



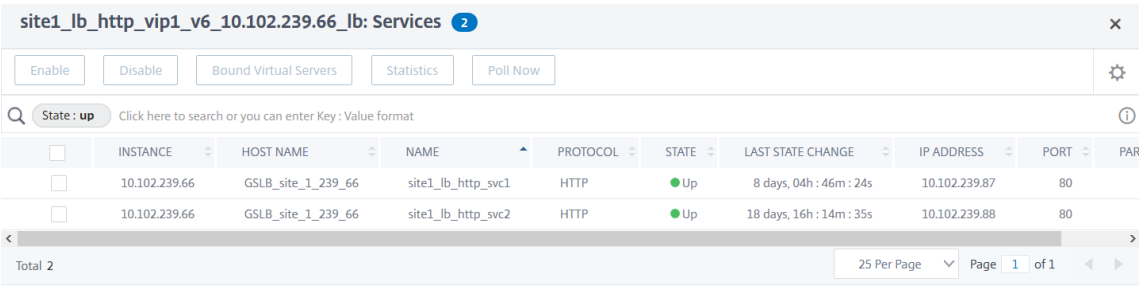
单击 查看详细信息查看和管理虚拟服务器设置。



- 所有服务 — 绑定到应用程序的服务



单击查看服务详细信息并管理服务设置



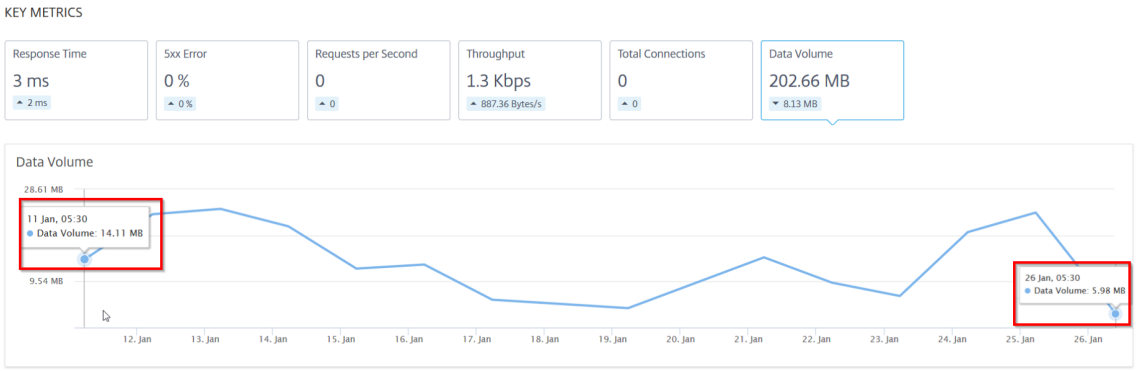
- 关键度量 — 应用程序度量详细信息，如 应用程序响应时间、错误百分比、每秒请求量、吞吐量、总连接量和数据量。对于与 SSL 相关的应用程序，将显示更多指标详细信息，例如会话命中、加密字节率、解密字节率和创建的新 **SSL** 会话。

> 注意
>
> 仅针对 **Citrix ADC 13.0** 或更高版本显示 5xx 错误百分比度量。对于早期版本，该值显示为 **0**。

在每个指标中，您可以查看所选时间持续时间的平均值和差值。差值计算为 第一个值减去所选时间持续时间的最后一个值。

您可以在所选时间持续时间内以图形格式查看以下实例指标：

下图是数据卷的示例，所选时间持续时间为 1 个月。值 202.66 MB 是 1 个月持续时间的总数据卷，值 8.13 MB 是差值。在图形中，第一个值为 14.11，最后一个值为 5.98。差值为 14.11-5.98 = 8.13 MB。



对于与 SSL 相关的应用程序，您可以查看以下更多指标：

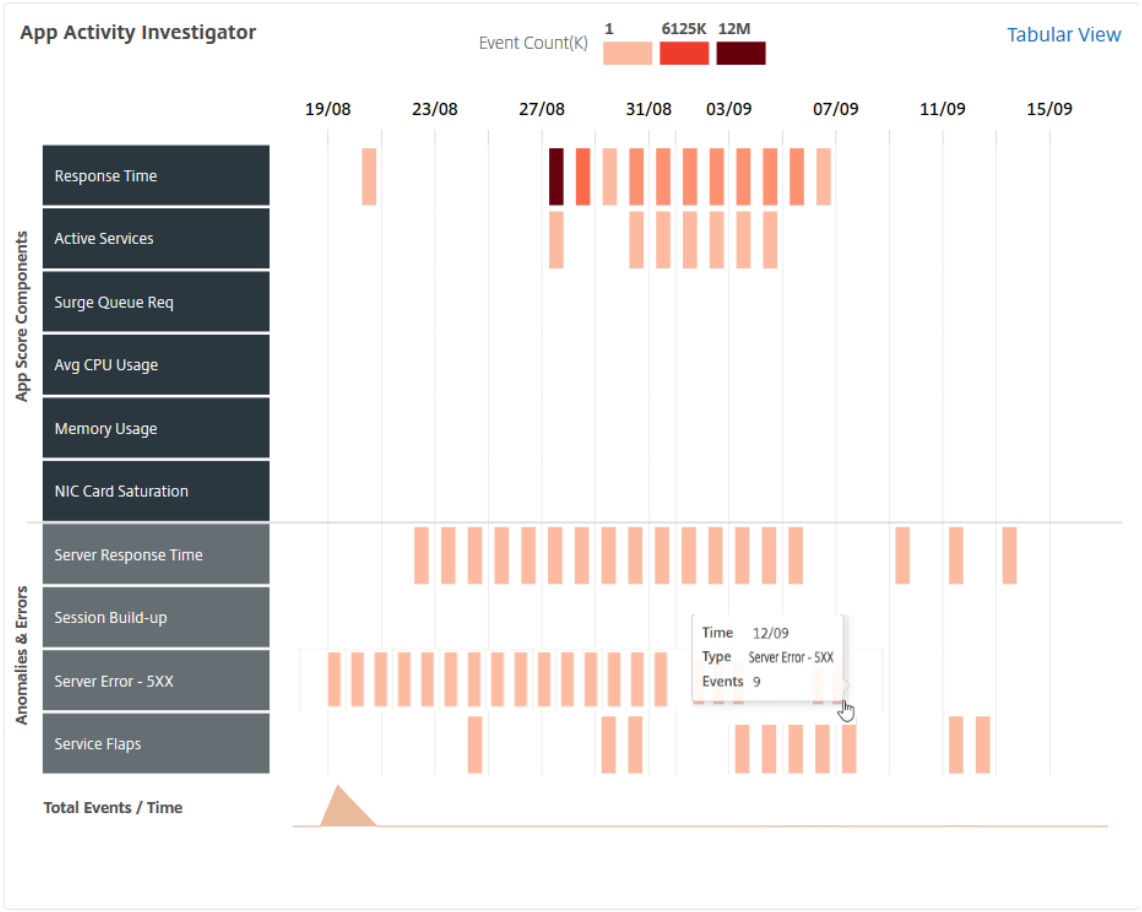
- 问题 — 适用于选定应用程序的问题。您可以查看以下问题及其类别：

性能	实例运行状况	配置	系统资源
响应时间	Average CPU Usage (平均 CPU 使用率)	不稳定的服务器	不正确的持久性类型
活动服务	内存使用率	异常大的 HTTP 数据包	NIC Card Saturation (NIC 卡饱和度)
低会话重复使用		TCP 重新组装队列限制命中	
外科队列累积			
SSL 实时流量			
会话累积			
服务襟翼			

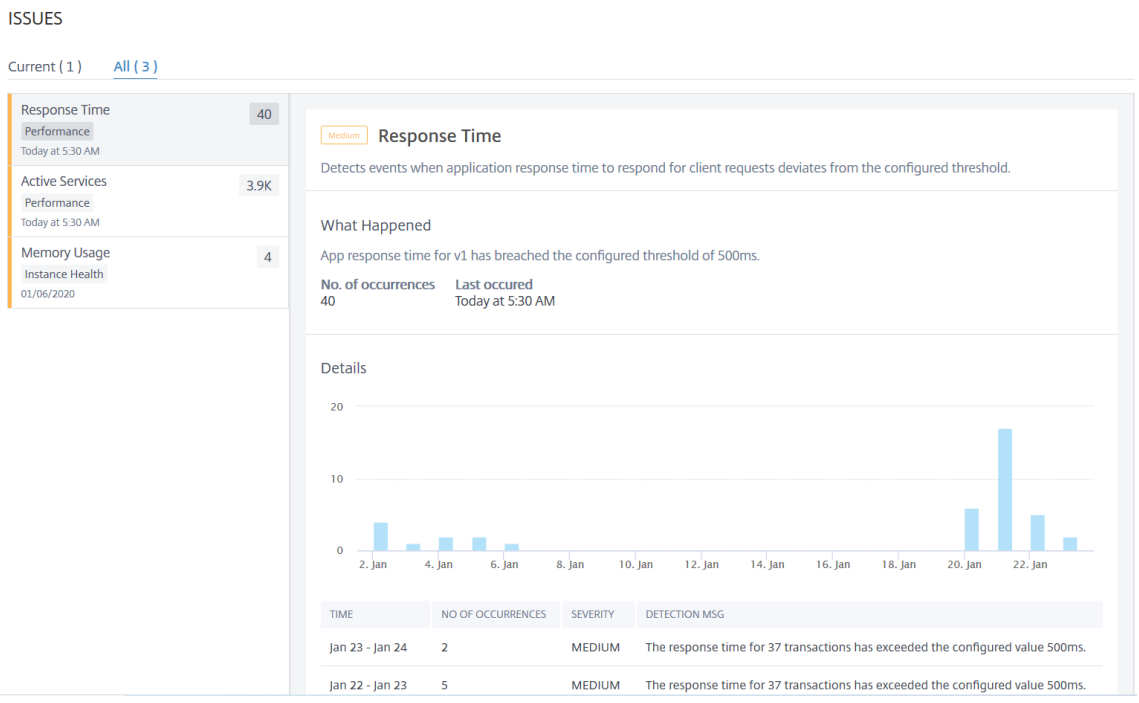
单击每个问题以检查详细信息，例如检测消息、问题发生的时间、建议的操作和详细信息。

有关详细信息，请参阅用于应用程序分析的性能指标。

下图是“应用程序活动调查器”页面的早期视图：

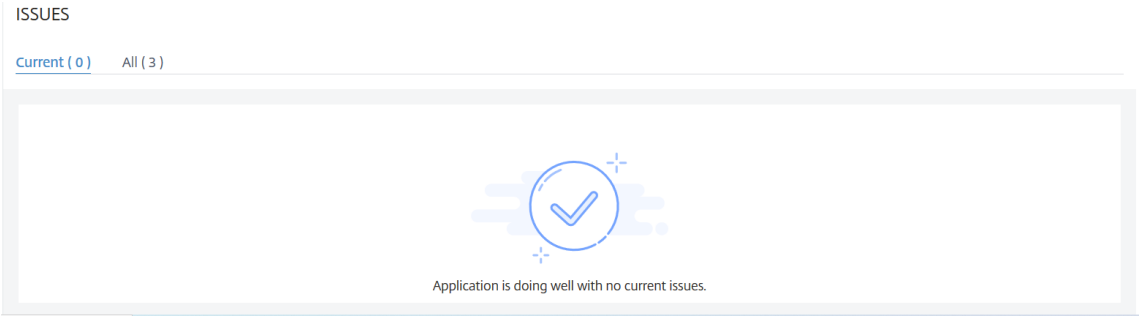


现在，您可以在“问题”部分查看所有 问题，以及您可以在“ 应用活动调查器”页面中查看的类别。

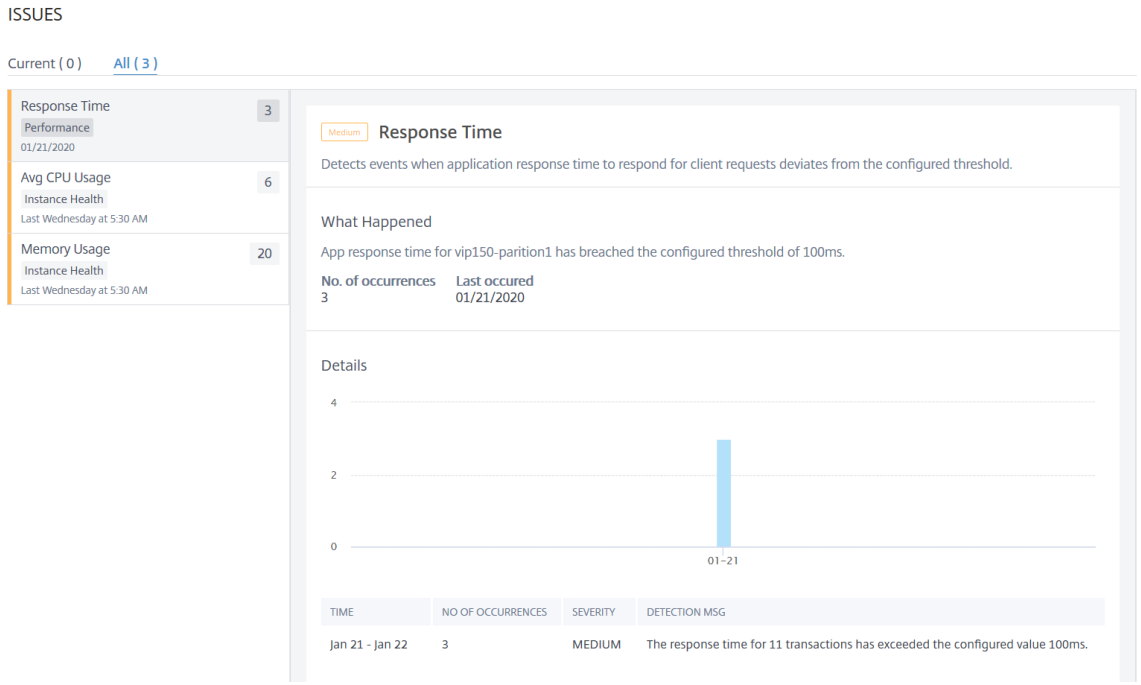


- 在“ 当前”选项卡中显示的问题是指所选时间持续时间的应用程序问题。
- “全 部”选项卡中显示的问题是指总的应用程序问题。

以下示例是持续 1 天的应用程序问题。“当 前”选项卡表示当前没有影响应用程序分数的问题。



“全 部”选项卡显示在 1 天持续时间内检测到的问题总数。



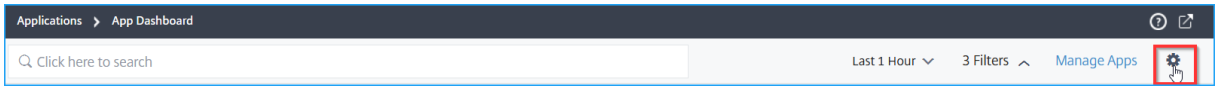
选择应用评分组件并设置阈值

April 23, 2021

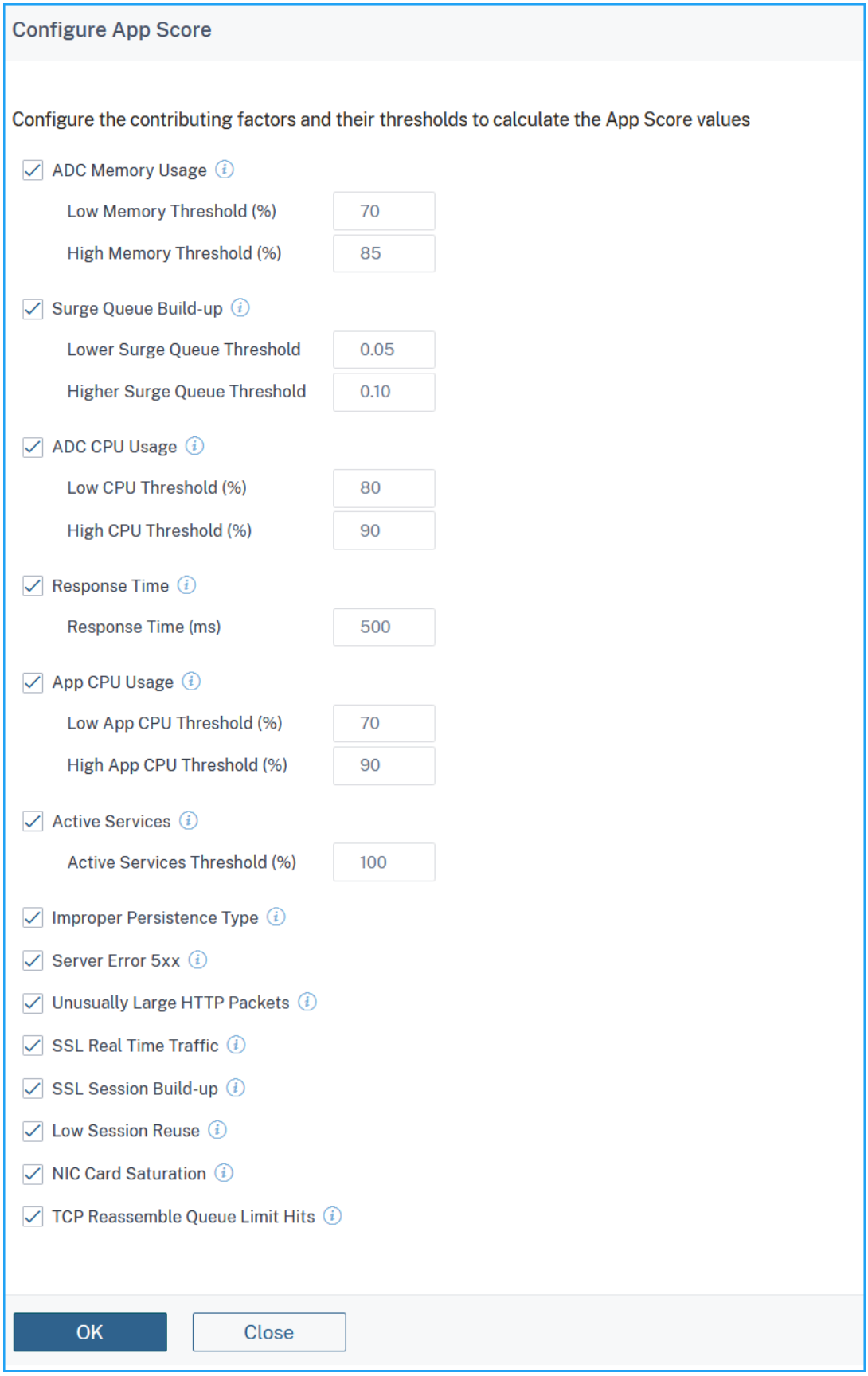
在 应用程序控制面板中，作为管理员，您可以决定选择组件并为应用程序分数计算配置阈值。App Score 是定义以下内容的评分系统：

- 应用程序的表现如何
- 应用程序在响应能力方面表现是否良好

导航到 应用程序 > 仪表板，然后选择设置图标。



在“ 配置应用程序分数”页面中，您可以选择组件并配置阈值以确定应用程序的最终得分。



应用程序分数计算基于以下组成部分：

应用评分组件	用户配置的阈值	说明
ADC 内存使用情况	是	Citrix ADC 实例中总内存使用量的低阈值和高阈值
激增队列积累	是	队列中需要响应的总激增请求的低阈值和高阈值。
ADC CPU 使用率	是	Citrix ADC 实例中总 CPU 使用率的低阈值和高阈值。
响应时间	是	发送请求数据包与从虚拟服务器上配置的服务接收第一个响应数据包之间的时间间隔。
应用程序 CPU 使用	是	应用程序总 CPU 使用率的低阈值和高阈值。
活动服务	是	绑定到虚拟服务器的服务必须处于活动状态的百分比阈值。
不正确的持久性类型	否	指示虚拟服务器上的持久性使用率是否低。
服务器错误 (5xx)	否	指示 Web 服务器是否响应 5xx 错误。
异常大的 HTTP 数据包	否	如果具有 HTTP 标头大小的 HTTP 消息超过 Citrix ADC 实例中的配置值，则指示出现次数。
SSL 实时流量	否	分析 SSL 流量以识别实时流量，并建议最佳配置设置以改善延迟。
SSL 会话积累	否	表示会话在一段时间内积累，这可能会导致 Citrix ADC 实例中的这些会话占用大量内存。
低会话重复使用	否	指示 Citrix ADC 实例重复使用的实际会话数是否较少。
NIC 卡饱和	否	表示接口丢弃的数据包总数。
TCP 重新组装队列限制命中	否	指示 TCP 连接上的无序数据包是否超过配置的无序数据包队列大小。

默认情况下，所有组件都已启用。如果禁用任何组件，Citrix ADM 仅根据选定的组件执行最终应用程序得分计算。

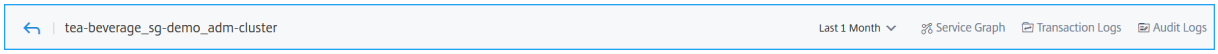
> 注意
>
> 您还可以继续配置阈值，方法是导航到 **Analytics >** 设置，然后单击 配置应用程序分数。

微服务应用的应用程序详情

April 23, 2021

单击仪表板中的微服务应用程序可向下钻取更多详细信息。

将显示选定的应用程序页面。

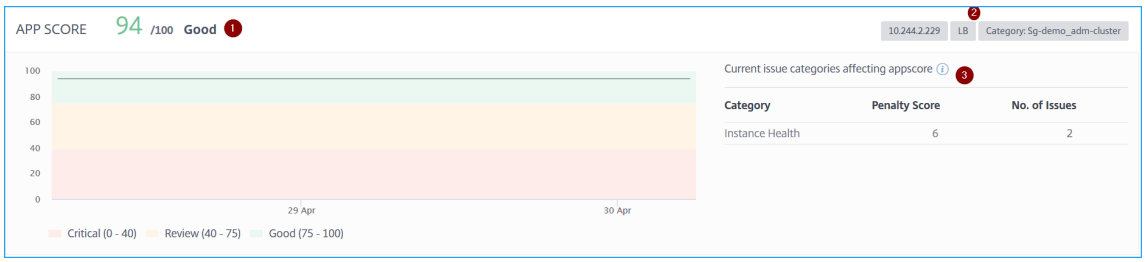


从应用程序详细信息页面：

- 从列表中选择时间持续时间以查看特定时间持续时间的详细信息
- 单击 服务图表可查看所选应用程序的服务图表。有关详细信息，请参阅应用程序的服务图。
- 点击 事务日志 查看所选应用程序的详细交易
- 单击 审计日志查看详细的审计日志信息

选择时间持续时间后，将显示以下应用程序详细信息：

- 应用程序分数 — 选定时间持续时间的应用程序分数。您还可以查看当前的申请问题，这被称为基于问题类别的适用罚款分数。最终得分计算为 **100** 减去总罚款。

  1 — 表示当前应用得分

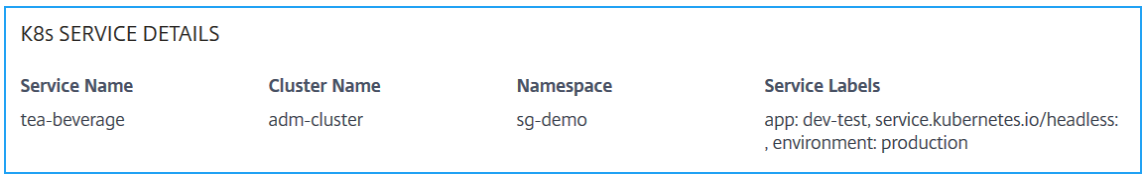
  2 — 表示 CPX IP 地址、应用程序类型（例如负载平衡或内容切换）以及托管服务的服务命名空间和集群名称

  3 — 表示影响当前应用程序分数的问题

  此仪表板还允许您查看影响应用程序分数的当前问题。您可以在问题下查看问题详细信息。

- **K8s** 服务详细信息

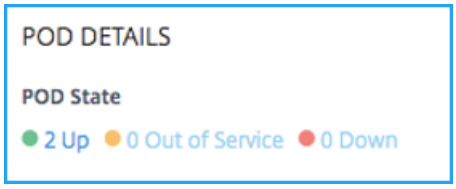
  您可以查看以下详细信息：



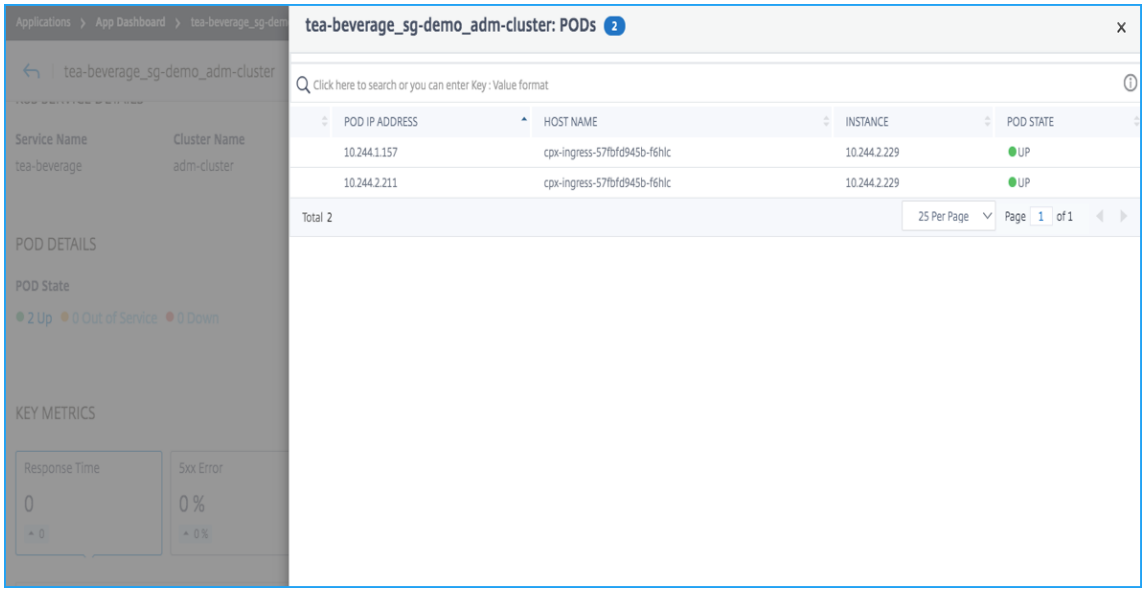
- 服务名称 — 服务名称
- 集群名称 — 托管服务的集群名称
- 命名空间 — 分配给服务的命名空间
- 服务标签 — 分配给服务的服务标签

- **Pod** 详情

  pod 是托管在 Kubernetes 集群中的一组容器。在 Pod 中，您可以部署多个容器化应用程序。每个 Pod 都与一个 IP 地址关联。



  点击窗格状态以查看详细信息

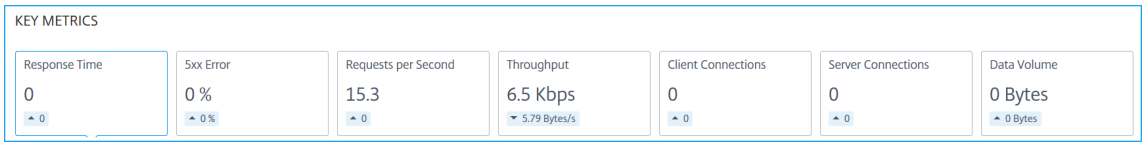


  - **Pod IP** 地址 — 表示 Pod IP 地址
  - 主机名 — 表示分配给容器的主机名
  - 实例 — 表示 Citrix ADC CPX IP 地址
  - **POD** 状态 — 表示 pod 的当前状态

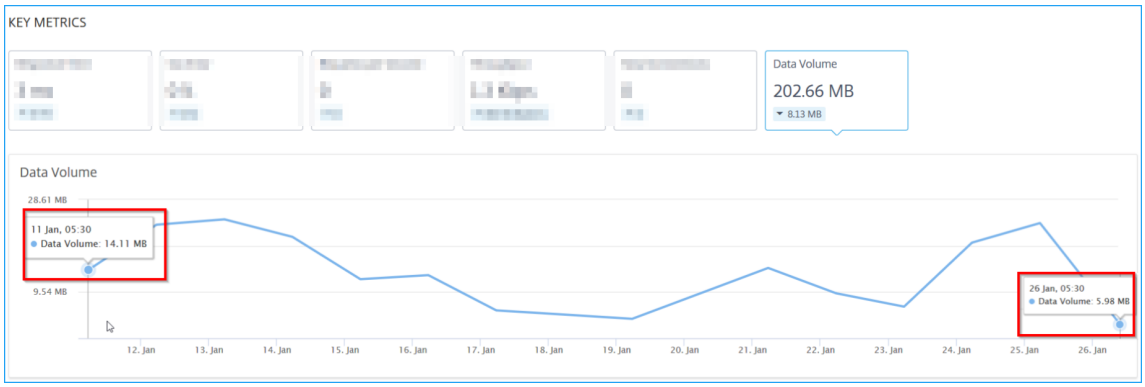
- 关键指标 — 显示关键指标详细信息，例如响应时间、**5xx** 错误、每秒请求数、吞吐量、客户端连接、服务器连接和数据量。

  在每个指标中，您可以查看所选时间持续时间的平均值和差值。差值计算为 第一个值减去所选时间持续时间的最后一个值。

  您可以在所选时间持续时间内以图形格式查看以下实例指标：



  下图是数据量的示例，选定的持续时间为 1 个月。值 202.66 MB 是 1 个月持续时间的总数据卷，值 8.13 MB 是差值。在图形中，第一个值为 14.11，最后一个值为 5.98。差值为 14.11-5.98 = 8.13 MB。

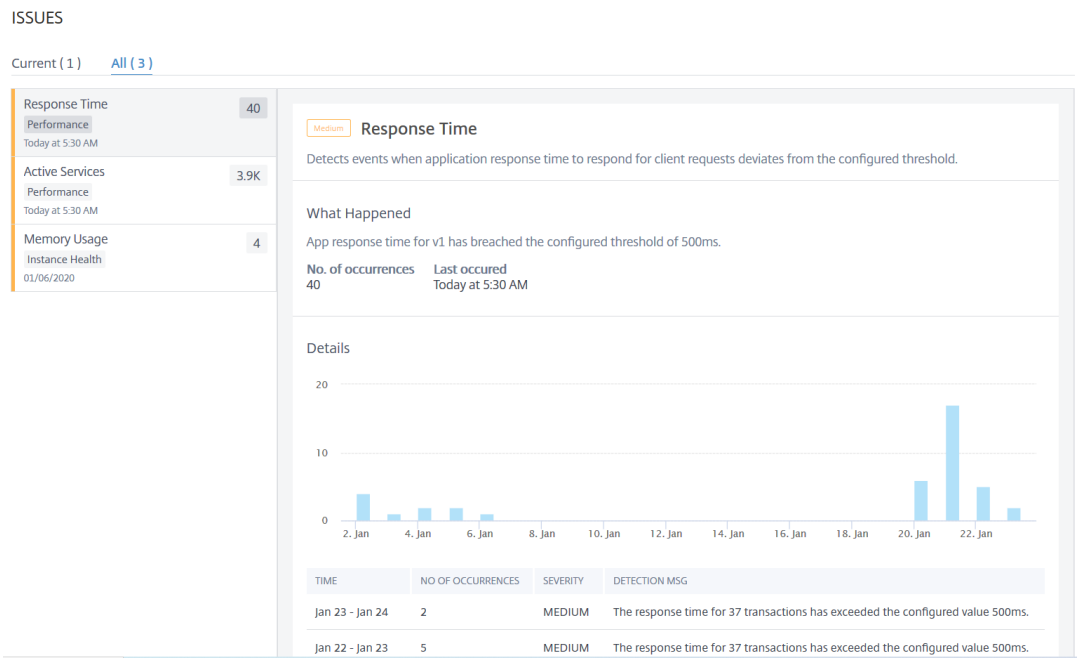


- 问题 — 适用于选定应用程序的问题。您可以查看以下问题及其类别：

性能	实例运行状况	配置	系统资源
响应时间	Average CPU Usage (平均 CPU 使用率)	高 5xx 响应	不正确的持久性类型
低会话重复使用	内存使用率	异常大的 HTTP 数据包	NIC Card Saturation (NIC 卡饱和度)
外科队列累积		TCP 重新组装队列限制命中	
SSL 实时流量			

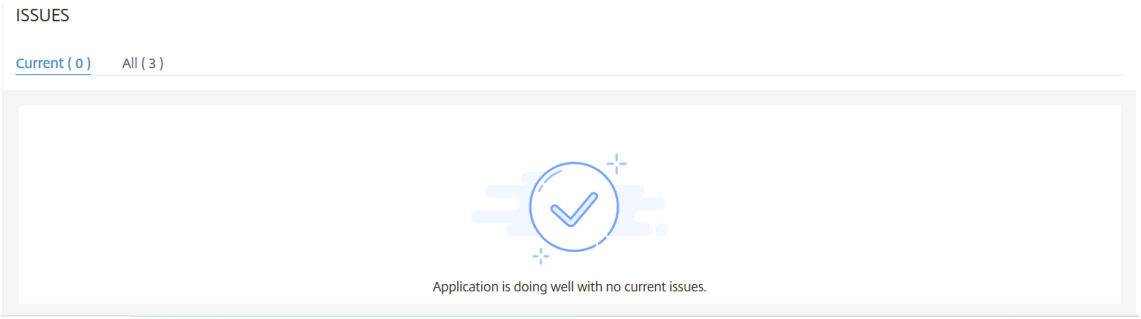
  单击每个问题可查看以下信息：

  - 总发生次数
  - 解决问题的建议操作
  - 问题详细信息，例如时间、服务名称、总发生率、严重性和检测消息

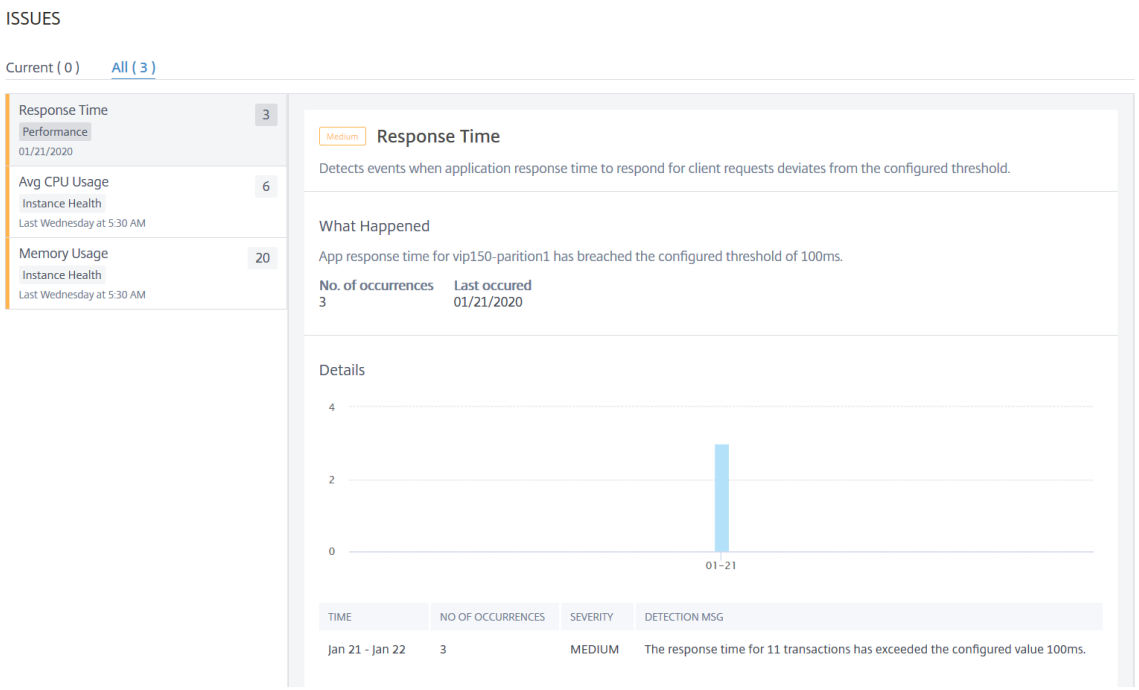


- 在“ 当前”选项卡中显示的问题是指所选时间持续时间的应用程序问题。
- “全 部”选项卡中显示的问题是指总的应用程序问题。

以下示例是持续 1 天的应用程序问题。“当 前”选项卡表示当前没有影响应用程序分数的问题。



“全 部”选项卡显示在 1 天持续时间内检测到的问题总数。



Web Insight 仪表板

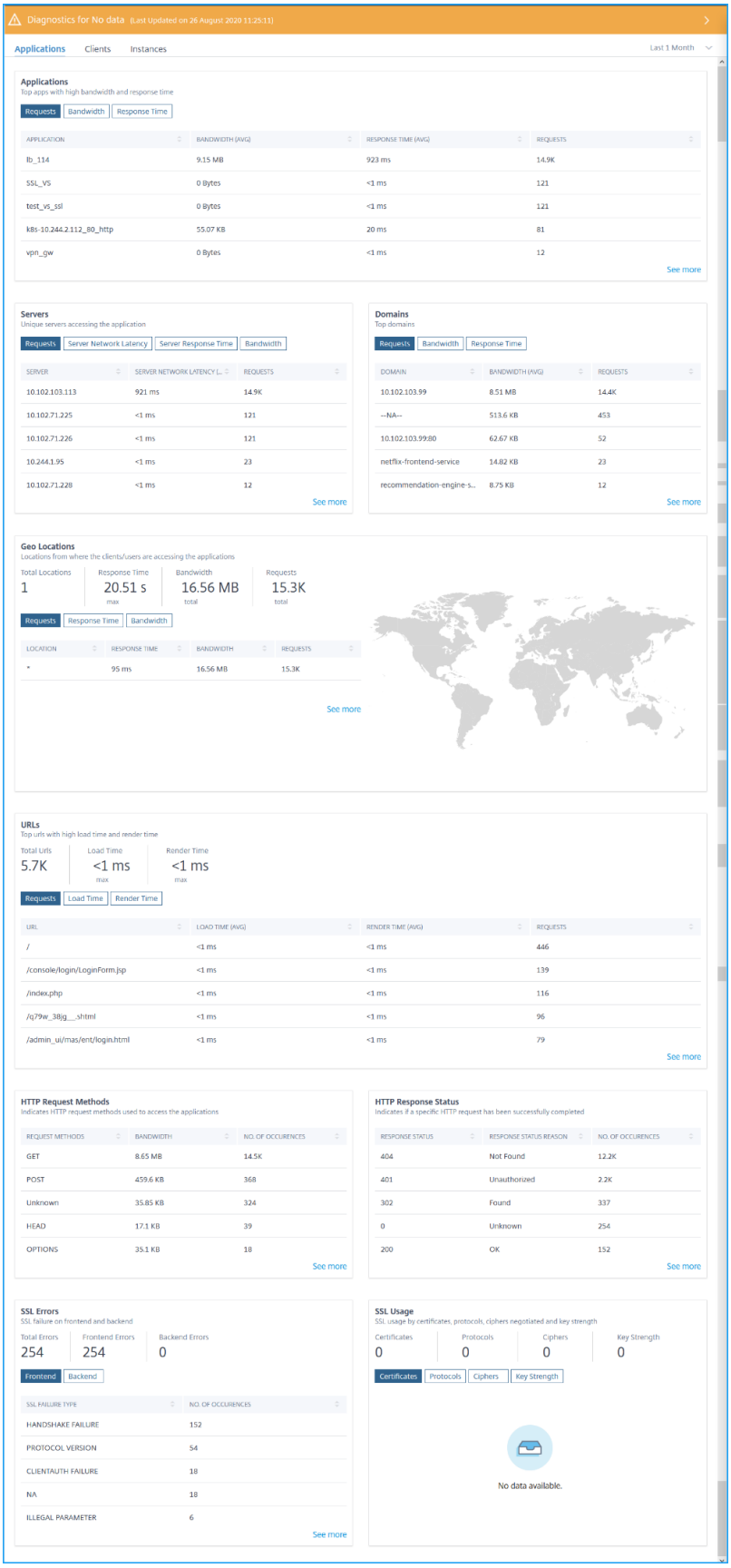
April 23, 2021

改进的 Web Insight 功能得到了增强，并提供了对 Web 应用程序、客户端和 Citrix ADC 实例的详细指标的可见性。这种改进的 Web Insight 使您能够从性能和使用情况的角度评估和可视化整个应用程序。作为管理员，您可以查看以下内容的 Web Insight：

- 一个应用程序。导航到 应用程序 **>** 仪表板，单击应用程序，然后选择 **Web Insight** 选项卡以查看详细指标。有关详细信息，请参阅应用使用分析。
- 所有应用程序。导航到 应用程序 **> Web Insight** ，然后单击每个选项卡（应用程序、客户端、实例）以查看以下指标：

应用程序	客户	实例
应用程序	客户	实例指标
服务器	地理位置	应用程序
域	HTTP 请求方法	域
地理位置	HTTP 响应状态	URL
URL	URL	HTTP 请求方法
HTTP 请求方法	操作系统	HTTP 响应状态

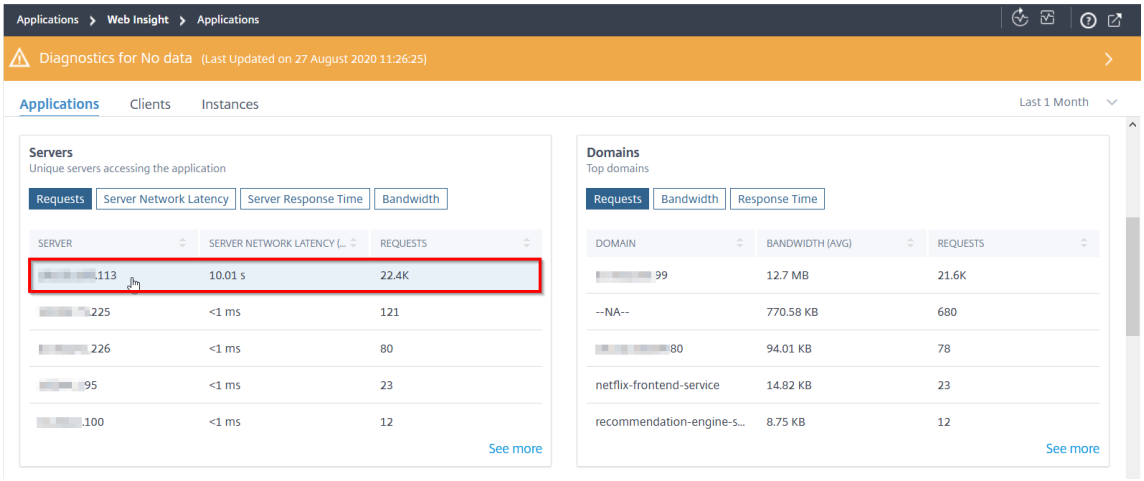
应用程序	客户	实例
HTTP 响应状态	浏览器	客户
SSL 错误	SSL 错误	服务器
SSL 使用	SSL 使用	操作系统
		浏览器



在每个指标中，您可以查看前 5 个结果。您可以单击进一步向下钻取以分析问题并更快地执行故障排除操作。

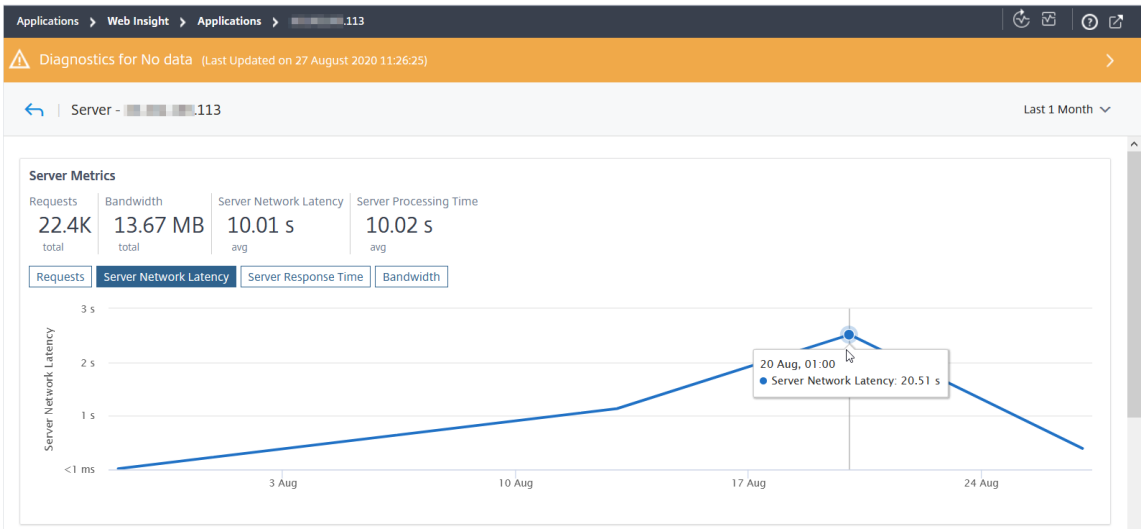
例如，考虑您想要分析服务器网络延迟 1 个月的持续时间，并决定是扩展还是缩小生产环境。要分析这个：

1. 从列表中选择过去 1 个月，然后从 应用程序选项卡中选择，向下滚动到服务 器，然后单击服务器。



将显示所选服务器的度量详细信息。

2. 选择“ 服务器网络延迟”选项卡以分析延迟。



平均延迟表示 10.01 秒，从图表中，您可以分析过去 1 个月的服务器网络延迟似乎很高。作为管理员，您可以决定扩展生产环境。

有关 Web Insight 用例的更多信息，请参阅 Web Insight。

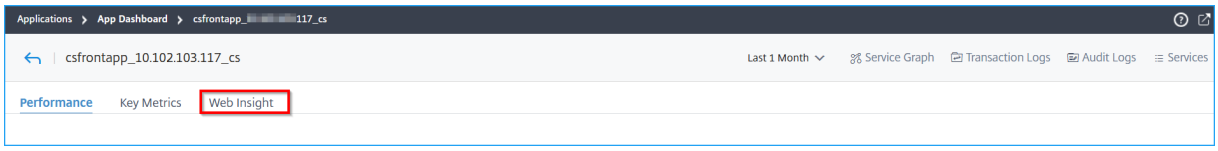
应用使用率分析

April 23, 2021

应用程序所有者必须能够从性能和使用情况的角度评估和可视化整个应用程序。

通过即兴应用 程序控制面板，您可以一起查看所有应用程序性能和使用率指标。单击应用程序时，除了现有的应用程序性能指标外，**Web Insight** 选项卡将显示有助于您的指标详细信息：

- 了解应用程序使用情况。
- 将任何性能偏差与使用量指标相关联。



注意

对于每个指标，您可以查看指示最大值和总值的选项。例如：

Client network latency

1 ms

max

- 所选持续时间内的最大客户端网络延迟。考虑一下，客户端 1 = 30 毫秒、客户端 2 = 15 毫秒、客户端 3 = 3 毫秒的网络延迟。在这种情况下，客户端网络延迟显示 30 毫秒。

Bandwidth

164.54 MB

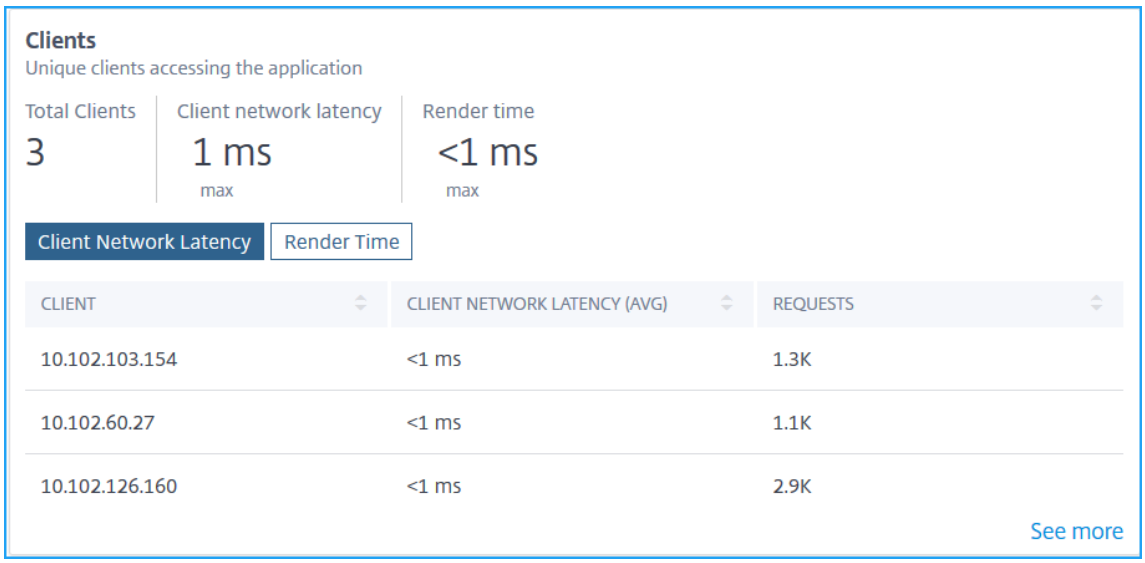
total

- 在所选持续时间内，所有可用客户端/服务器使用的总带宽。考虑客户端 1 = 30 MB 的带宽消耗，客户端 2 = 45 MB，客户端 3 = 40 MB。

  在这种情况下，带宽显示（30 MB + 45 MB +40 MB）= 115 MB。

以下是您可以从“ 使用情况”选项卡中查看的 Web Insight 指标：

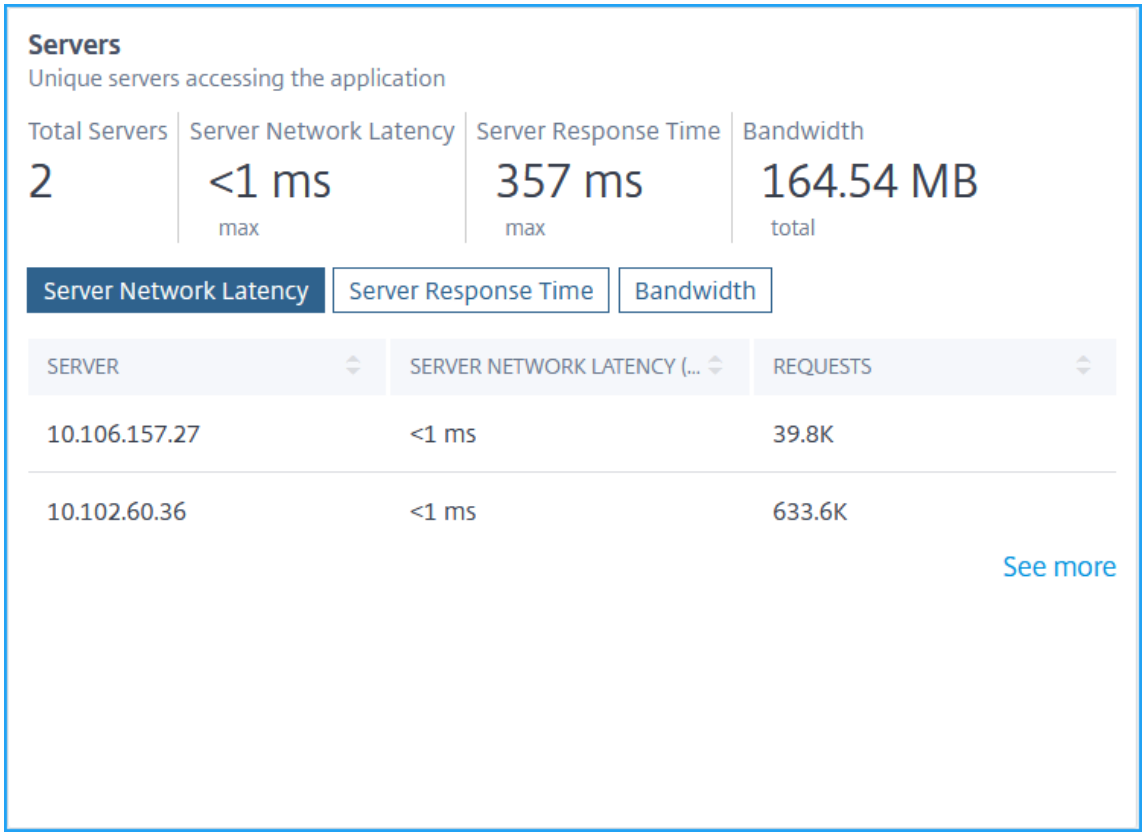
- 客户端 — 为访问应用程序的客户显示见解：



  - 客户端总数 — 显示访问应用程序的客户端总数。
  - 客户端网络延迟 — 显示从客户端到 Citrix ADC 的网络延迟。单击“ 客户端网络延迟”选项卡以查看：

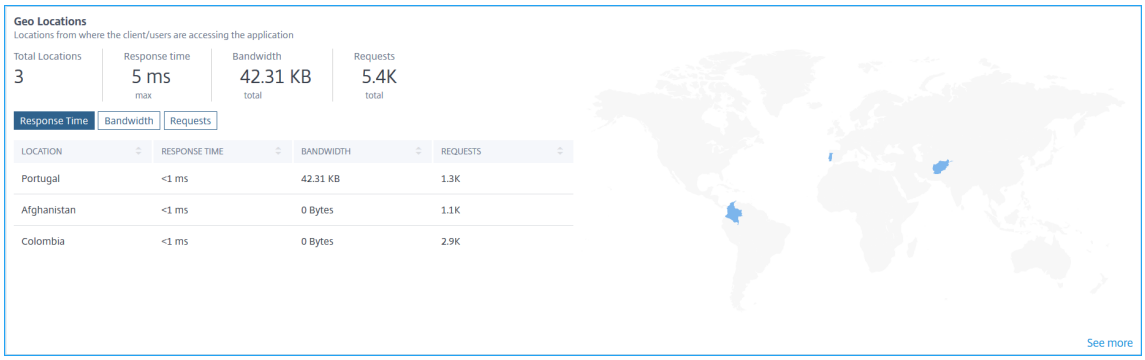
    * 客户端 — 客户端 IP 地址。
    * 客户端网络延迟 **(avg)** — 来自客户端的平均网络延迟。
    * 请求 — 来自客户端的请求总数。
  - 渲染时间 — 显示渲染服务器响应所花费的时间。单击 渲染时间选项卡以查看：
    * 客户端 — 客户端 IP 地址。
    * 渲染时间 **(avg)** — 来自客户端的平均渲染时间。
    * 请求 — 来自客户端的请求总数。

- 服务器 — 显示访问应用程序的服务器的见解：



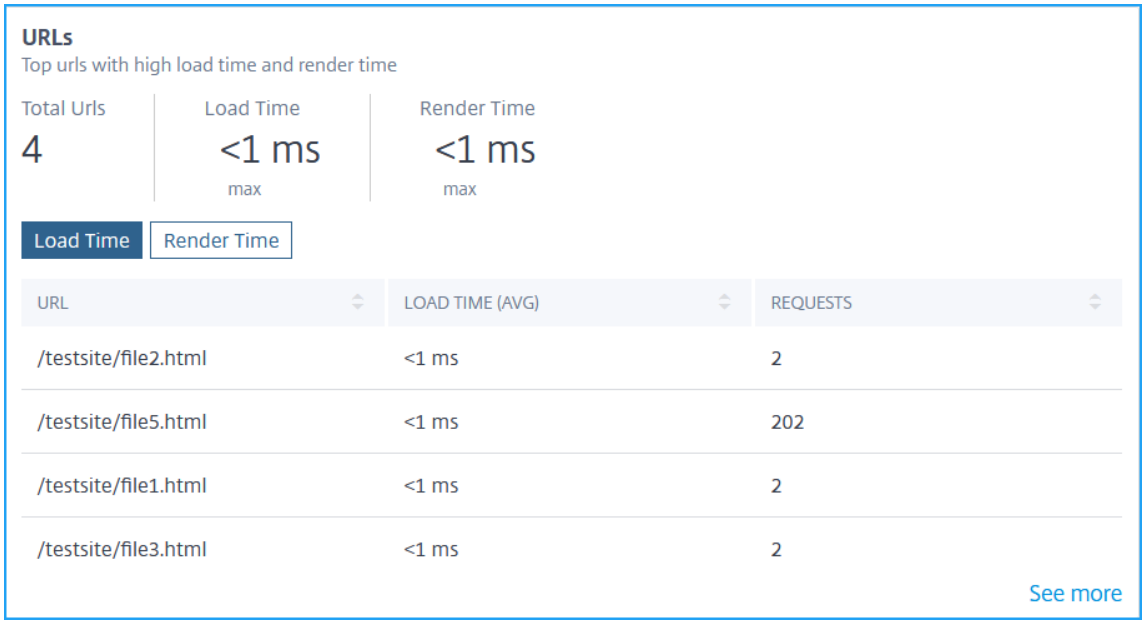
  - 服务器总数 — 显示访问应用程序的服务器总数。
  - 服务器网络延迟 — 显示从服务器到 Citrix ADC 的网络延迟。单击 服务器网络延迟选项卡以查看：
    * 服务器 — 服务器 IP 地址。
    * 服务器网络延迟 **(avg)** — 来自服务器的平均网络延迟。
    * 请求 — 来自服务器的请求总数。
  - 服务器响应时间 — 显示服务器响应请求所花费的时间。单击 服务器响应时间选项卡以查看：
    * 服务器 — 服务器 IP 地址。

        * 响应时间 **(avg)** — 来自服务器的平均响应时间。
        * 请求 — 来自服务器的请求总数。
    - 带宽 — 显示服务器消耗的总带宽。单击 带宽选项卡以查看：
        * 服务器 — 服务器 IP 地址。
        * 带宽 — 服务器消耗的总带宽。
        * 请求 — 来自服务器的请求总数。
- 地理位置 — 显示从特定位置访问应用程序的客户的见解：

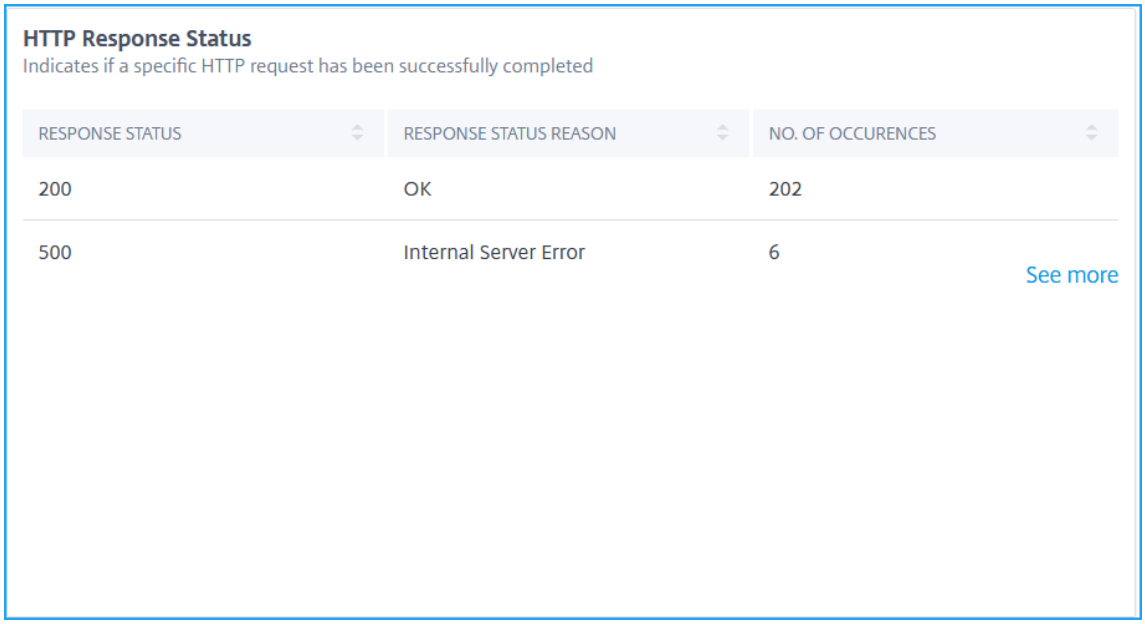


    - 总位置 — 显示访问应用程序的客户端总位置。
    - 响应时间 — 显示来自客户端位置的响应时间。
    - 带宽 — 显示所有位置的客户端消耗的总带宽。
    - 请求 — 显示来自所有客户端位置的请求总数。

      单击每个选项卡以查看：
        * 位置 — 位置名称。
        * 响应时间 — 来自客户端位置的平均响应时间。
        * 带宽 — 从客户端位置消耗的带宽。
        * 请求 — 来自客户端位置的请求总数。
- **URL** — 显示高负载和渲染时间的 URL 的见解：

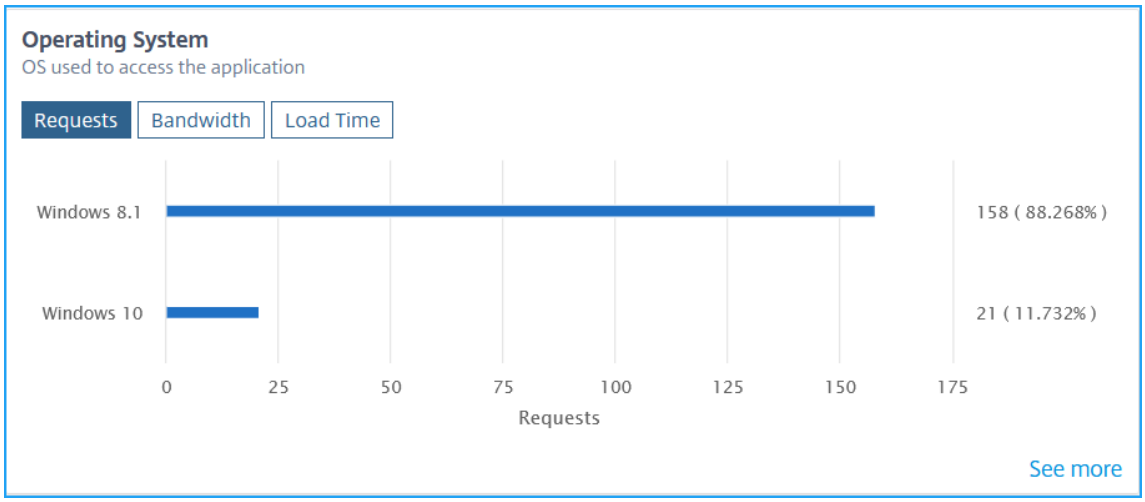


  - **URL** 总数 — 显示总 URL。
  - 加载时间 — 显示加载 URL 所花费的时间。单击加 载时间选项卡查看：
    - **URL** — URL 名称。
    - 加载时间 **(**平均值**)** — 加载 URL 的平均时间。
    - 请求 — 来自 URL 的请求总数。
  - 渲染时间 — 显示渲染和显示 URL 所花费的时间。单击 渲染时间选项卡以查看：
    - **URL** — URL 名称。
    - 渲染时间 **(avg)** — 渲染 URL 的平均时间。
    - 请求 — 来自 URL 的请求总数。
- **HTTP** 响应状态 — 显示特定已完成 HTTP 请求的见解。



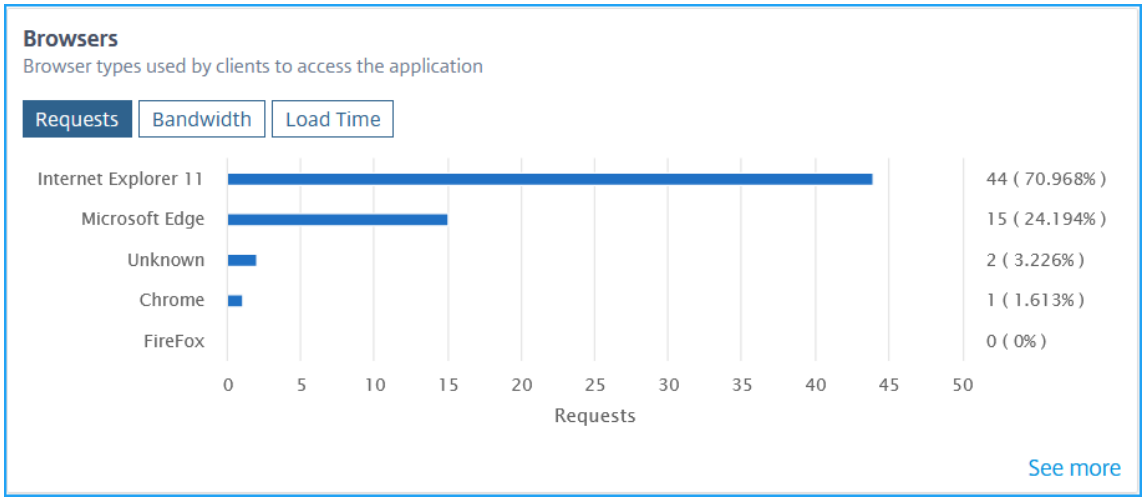
  - 响应状态 — 显示响应代码，如 2xx、4xx、5xx 等。
  - 响应状态原因 — 显示响应原因，例如内部服务器错误、未找到等。
  - 发生次数 — 显示出现的总次数。

- 操作系统 — 显示访问应用程序的操作系统的见解。



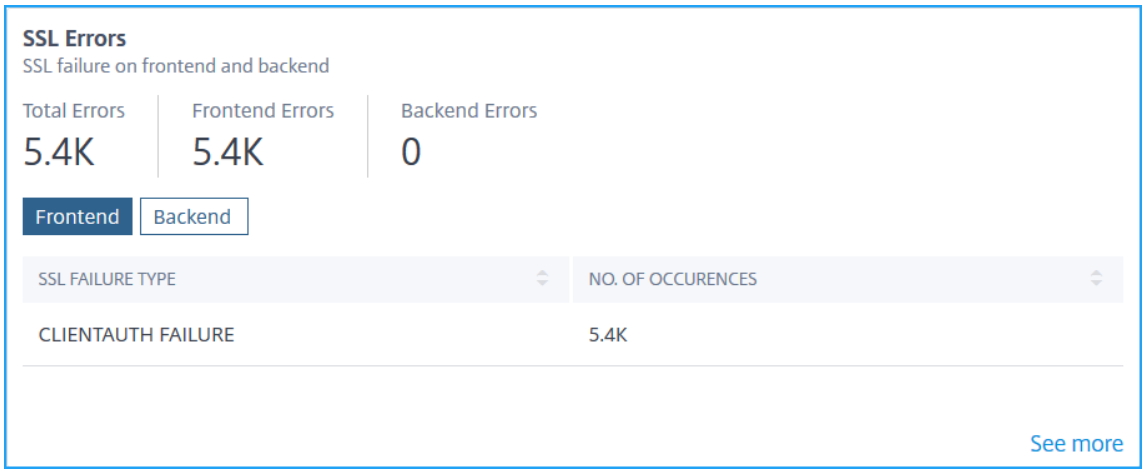
  - 请求 — 显示来自每个操作系统的请求总数。
  - 带宽 — 显示每个操作系统消耗的总带宽。
  - 加载时间 — 显示从服务器加载每个操作系统所花费的总时间。

- 浏览器 — 显示客户端用于访问应用程序的浏览器类型的见解。



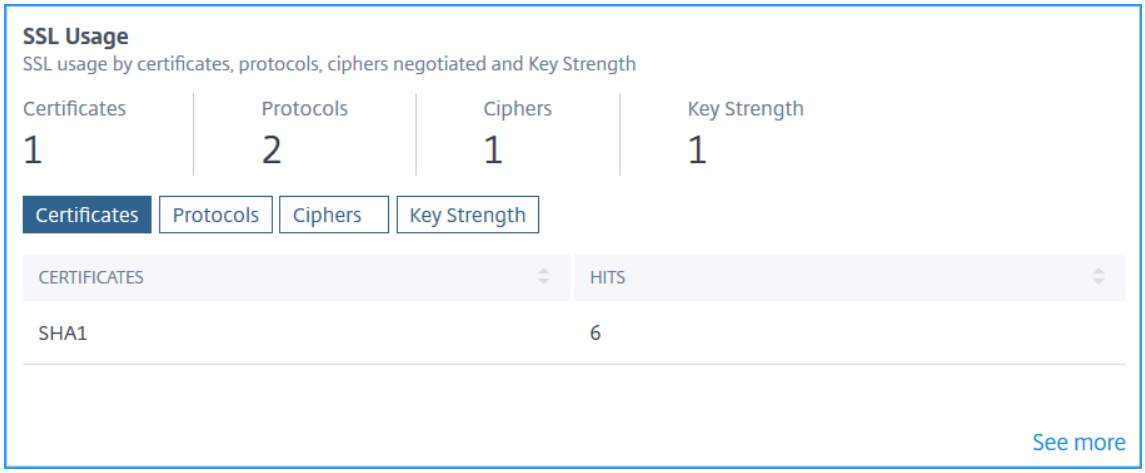
  - 请求 — 显示来自每个浏览器的请求总数。
  - 带宽 — 显示每个浏览器消耗的总带宽。
  - 加载时间 — 显示浏览器从服务器加载所花费的总时间。

- **SSL** 错误 — 显示来自前端服务器和后端服务器的 SSL 错误的见解。



  - 错误总数 — 显示 SSL 错误发生的总数。
  - 前端 — 显示来自前端服务器的 SSL 错误总数。单击前端选项卡以查看 SSL 错误类型和总出现次数。
  - 后端 — 显示来自后端服务器的 SSL 错误总数。单击 后端选项卡可查看 SSL 错误类型和总出现次数。

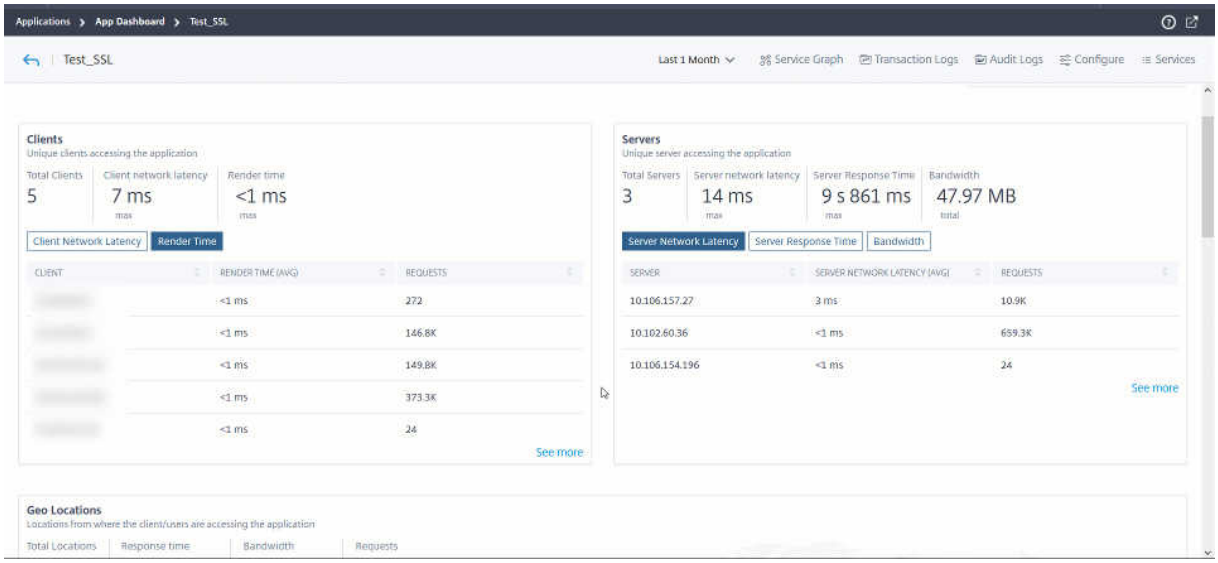
- **SSL** 使用情况 — 显示 SSL 使用情况的见解，例如 SSL 证书、协议、密码和密钥强度。



- 证书 — 显示 SSL 证书的总数。单击 证书选项卡以查看证书名称和总命中数。
- 协议 — 显示 SSL 协议的总数。单击 协议选项卡可查看 SSL/TLS 协议的详细信息和总命中。
- 密码 — 显示密码总数。单击 密码选项卡可查看每个密码套件名称和总命中数的详细信息。
- 关键强度 — 显示 SSL 证书中使用的总密钥强度。单击关 键力量选项卡可查看每个关键强度和总命中的详细信息。

以图形格式查看指标详情

对于每个指标，您可以通过单击查看更多选项以图形格式查 看更多详细信息。单击 **>** 以图形格式查看详细信息。



单击查 看更多选项后，您可以查看每个指标的详细信息：

洞察名称	指标	说明
客户	客户	表示客户端列表

	渲染时间 (AVG)	表示客户端呈现服务器响应所花费的平均时间
	客户端网络延迟 (AVG)	表示从客户端到 Citrix ADC 实例的平均网络延迟
	请求	表示来自客户端的请求总数
服务器	服务器	表示服务器列表
	服务器处理时间 (AVG)	表示服务器处理请求所花费的平均时间
	服务器网络延迟 (AVG)	表示从服务器到 Citrix ADC 实例的平均网络延迟
	访问量	表示服务器收到的总点击
地理位置	位置	表示客户位置
	响应时间	表示来自客户端位置的总响应时间
	Bandwidth（带宽）	表示从该位置消耗的总带宽
	请求	表示来自该位置的请求总数
URL	渲染时间 (AVG)	表示从服务器加载页面所需的平均时间
	加载时间 (AVG)	表示 URL 渲染和显示所需的平均时间
	访问量	表示来自 URL 的总点击
HTTP 响应状态	名称	表示响应状态名称，例如 “确定”、“未找到”、“内部服务器错误” 等
	答复状态	表示从服务器收到的响应状态代码，例如 200、400、500 等
	访问量	表示响应代码的总点击
	Bandwidth（带宽）	表示消耗的总带宽
操作系统	操作系统	表示操作系统名称，例如 Windows、MAC
	加载时间	表示从服务器加载操作系统所花费的总时间
	Bandwidth（带宽）	表示操作系统消耗的总带宽
	请求	表示来自操作系统的请求总数
浏览器	浏览器	表示浏览器名称，例如 Mozilla Firefox、Chrome 等
	加载时间	表示浏览器从服务器加载所花费的总时间
	Bandwidth（带宽）	表示浏览器消耗的总带宽
	请求	表示浏览器的请求总数
SSL 错误	SSL 失败类型	表示错误名称，例如 CLIENTAUTH 失败
	发生	表示 SSL 错误的总发生次数
SSL 使用情况	表示协议名称和版本，例如 TLS、SSL
	点击	表示协议的总点击

有关 Web Insight 使用案例的更多信息，请参阅 Web Insight。

应用仪表板疑难

April 23, 2021

在应用控制板中添加应用程序后，仪表板会立即显示应用程序的基本配置详细信息。应用程序分析详细信息（例如应用得分、关键指标和问题）在几分钟内开始填充（约 10 到 15 分钟）。有关详细信息，请参阅应用程序。

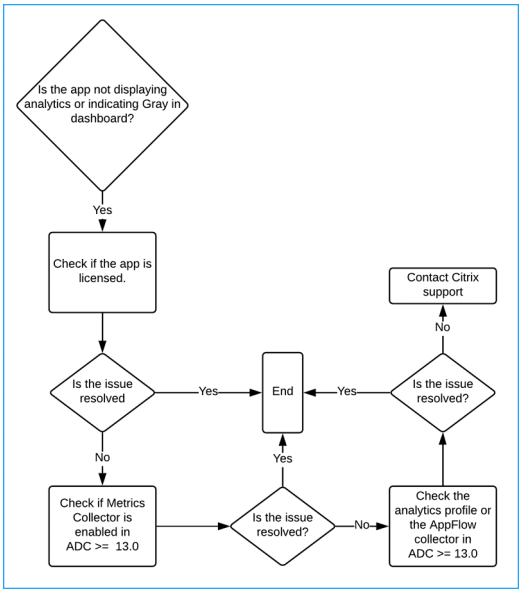
您必须确保 Citrix ADC 实例的指标数据流（AppFlow 收集器或 Analytics 配置文件）没有问题。您可以在本文档中获取有关 AppFlow 收集器和分析配置文件的更多信息

本文档介绍了在以下情况下需要执行的故障排除步骤：

- 单击应用程序，即使在上述持续时间（10-15 分钟）之后，选定应用程序的分析也不会显示所需的数据。
- CS 或 LB 应用程序始终在应用程序控制面板中显示灰色（不适用状态）。

> 注意
>
> 本文档中提到的故障排除过程仅适用于 内容切换和 负载平衡虚拟服务器。

故障排除场



应用程序已许可

您必须确保应用程序是否已获得许可。

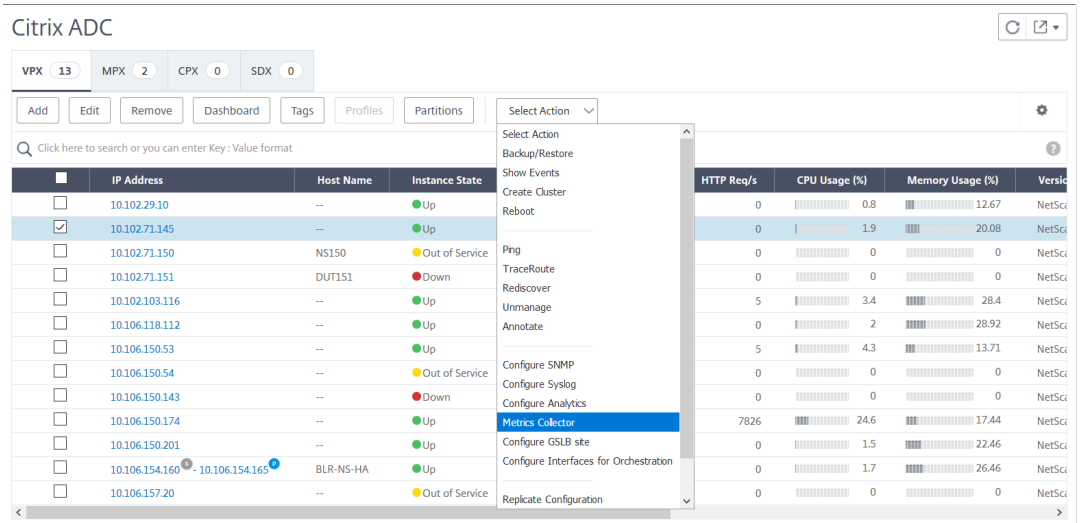
- **ADM** 服务 -导航到 帐户 **>** 订阅，然后验证应用程序是否在 虚拟服务器许可证摘要下获得许可。如果应用程序未获得许可，请参阅 在虚拟服务器上管理许可并启用分析 以许可使用虚拟服务器。
- **ADM** 本地 — 导航到 “ 系统**” > “**许可和分析”，然后验证应用程序是否在 虚拟服务器许可证摘要下获得许可。如果应用程序未获得许可，请参阅 在虚拟服务器上管理许可并启用分析 以许可使用虚拟服务器。

指标收集器已启用

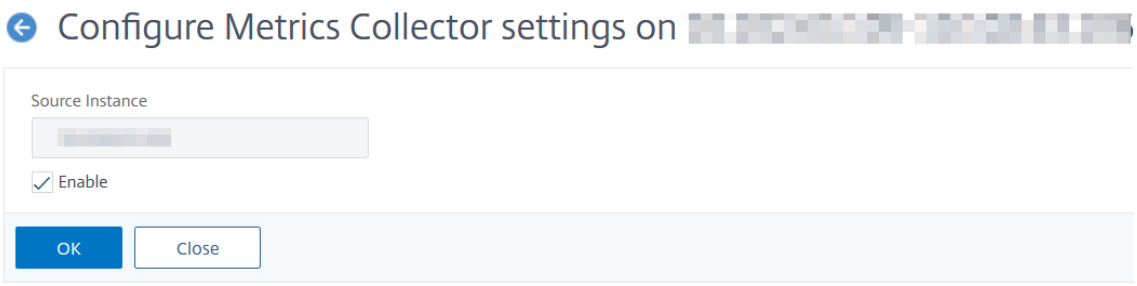
您必须确保是否在 Citrix ADC 实例中启用了 指标收集器。

对于 Citrix ADC 13.0 或更高版本，在 ADM 中成功添加 ADC 实例后，默认情况下会启用指标收集器。要确保衡量指标收集器是否已启用：

1. 导航到 网络 **>** 实例。在实例下，选择实例类型（例如 Citrix ADC VPX）。
2. 选择 Citrix ADC 实例。
   a) 在选择操作列表中，选择指标收集器。



3. 在配置指标收集器设置页面上，确保是否已选中启用选项。如果未选中，请选择启用选项并单击确定。



启用指标收集器后，如果仍然无法查看数据，请验证：

- 内部版本 **47.x** 之前的 Citrix ADC 实例版本 13.0 中的AppFlow 收集器。
- Citrix ADC 实例内部版本 **47.x** 或更高版本中的分析档案。

Citrix ADC 实例早期构建

在 Citrix ADC 中：

1. 运行以下命令以确保收集器是否已启动并在端口 5563 上运行：

```
sh appflow collector af_collector_rest_<adm_receiver_ip>
```

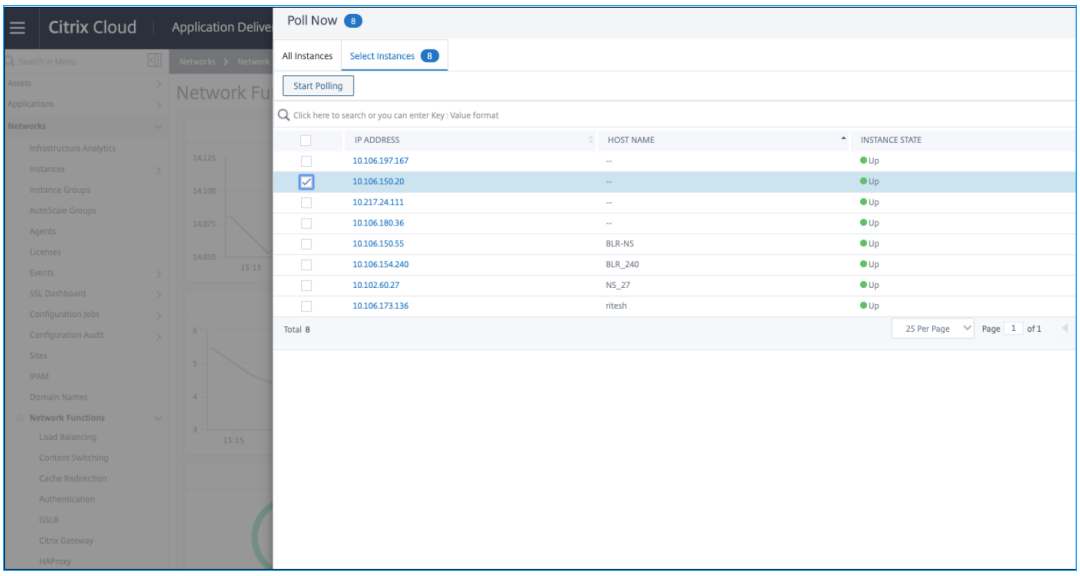


```
> sh appflow collector af_collector_rest_10.102.103.114
1) Name: af_collector_rest_10.102.103.114
IPv4 address: 10.102.103.114
Port: 5563
Netprofile:
Transport: rest
State: UP
Done
```

2. 如果没有可用的收集器，请在 Citrix ADM 中执行实例手动轮询。

   a) 导航到网络 **>** 网络功能 **>** 立即投票

   b) 选择实例，然后单击 开始轮询。



   如果轮询失败，请从 ADM 中删除 ADC 实例，然后再次添加 ADC 实例。添加 ADC 实例时，收集器会添加到 ADC 上。

如果收集器指示关闭状态：

1. 确保是否配置了 SNIP。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   如果未配置 SNIP，则必须配置 SNIP。有关详细信息，请参阅配置 SNIP。

2. 如果 ADC 实例可以访问 ADM，请确保这一点。

   你可以通过执行 ping 测试来验证。运行 `ping -S <SNIP> <adm_receiver_ip>`

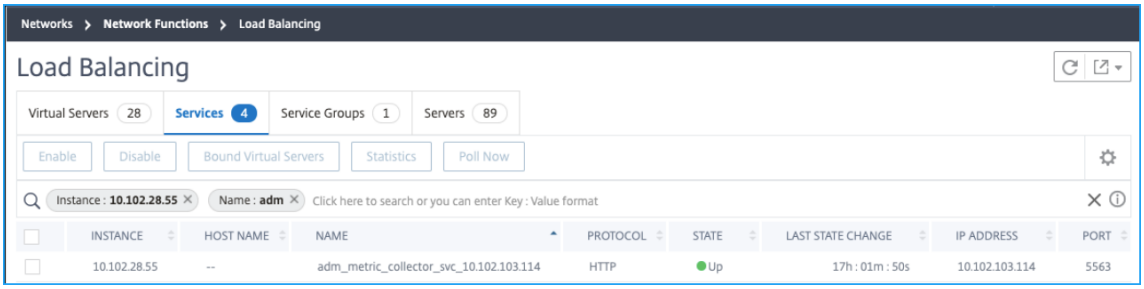

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

Citrix ADC 实例稍后构建

在 Citrix ADM 中，确保指标收集器服务可用：

1. 导航到网 络 **>** 网络功能 **>** 负载平衡 **>** 服务。
2. 在搜索栏上，按 实例：（**IP** 地址）和 名称：**ADM** 进行筛选。
3. 确保 `adm_metric_collector_svc_<adm_receiver ip>` 是否可用。IP 地址可以是 ADM 管理 IP 或代理 IP。

   确保此服务处于启动状态并在端口 5563 上运行。



如果仍然无法查看数据，请确保收集器服务绑定到 Citrix ADC 中的时间序列分析配置文件。

1. 登录 Citrix ADC
2. 运行以下命令：

   `sh analytics profile ns_analytics_time_series_profile`

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```


如果收集器指示关闭状态：

1. 确保是否配置了 SNIP。

```
> sh ip | grep SNIP
2)  10.106.150.34    0              SNIP            Active   Enabled  Enabled  NA       Enabled
```

   如果未配置 SNIP，则必须配置 SNIP。有关详细信息，请参阅配置 SNIP。

2. 如果 ADC 实例可以访问 ADM，请确保这一点。

   你可以通过执行 ping 测试来验证。运行 `ping -S <SNIP> <adm_receiver_ip>`

```
> ping -S 10.106.150.34 10.102.103.114
PING 10.102.103.114 (10.102.103.114) from 10.106.150.34: 56 data bytes
64 bytes from 10.102.103.114: icmp_seq=0 ttl=62 time=0.770 ms
64 bytes from 10.102.103.114: icmp_seq=1 ttl=62 time=0.446 ms
64 bytes from 10.102.103.114: icmp_seq=2 ttl=62 time=0.402 ms
```

3. 确保通过 telnet 的流量连接能够连接该服务。

```
root@ns# telnet 10.102.103.114 5563
Trying 10.102.103.114...
Connected to 10.102.103.114.
Escape character is '^]'.
^]
telnet> q
Connection closed.
```

   如果 telnet 能够连接服务，则存在防火墙并阻止指标数据流。你必须解决防火墙阻止问题。

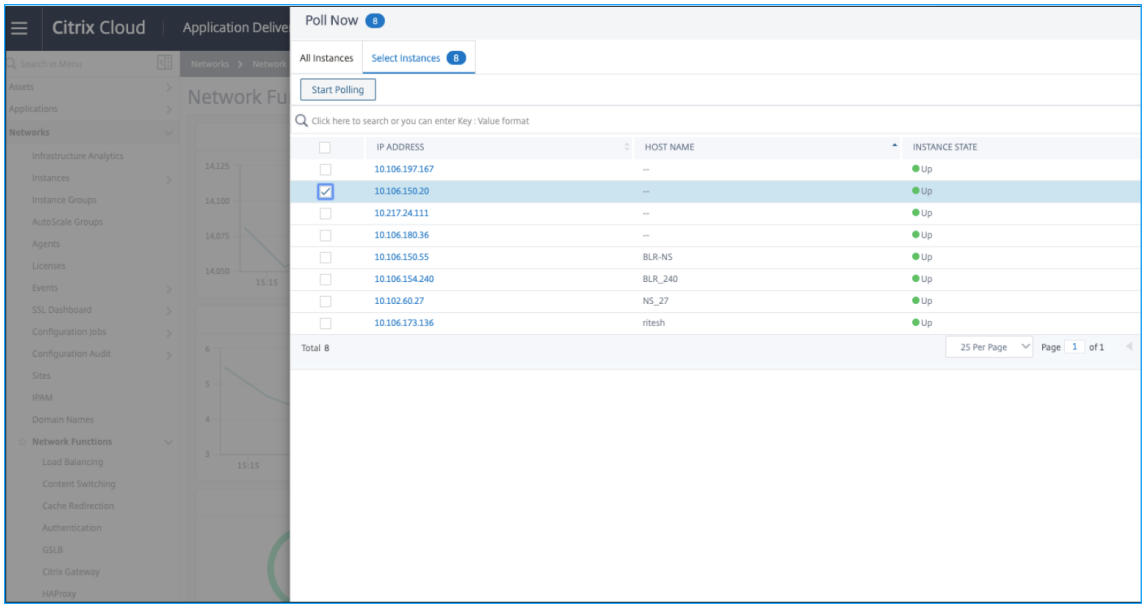
如果 Citrix ADC 中没有收集器服务绑定到时间序列分析配置文件，则收集器将显示为空白。

```
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector:
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

您必须在 Citrix ADM 中执行实例手动轮询。

1. 导航到网络 **>** 网络功能 **>** 立即投票

2. 选择实例，然后单击 开始轮询。



如果轮询失败，请使用以下命令直接在 Citrix ADC 实例添加收集器服务：

```
add service adm_metric_collector_svc_<adm_receiver_ip> <adm_receiver_ip
> HTTP 5563

unset analyticsprofile ns_analytics_time_series_profile -collectors

set analytics profile ns_analytics_time_series_profile -collectors
adm_metric_collector_svc_<adm_receiver_ip> -metrics enabled -events
enabled
```

分析时序配置文件已更新。

```
> add service adm_metric_collector_svc_10.102.103.114 10.102.103.114 HTTP 5563
 Done
> unset analyticsprofile ns_analytics_time_series_profile  -collectors
 Done
> set analytics profile ns_analytics_time_series_profile -collectors adm_metric_collector_svc_10.102.103.114 -metrics enab
 Done
> sh analytics profile ns_analytics_time_series_profile
1)  Name: ns_analytics_time_series_profile
    Collector: adm_metric_collector_svc_10.102.103.114
    Profile-type: timeseries
        Output Mode: avro
        Metrics: ENABLED
        Events: ENABLED
        Auditlog: DISABLED
    Reference Count: 0
 Done
```

如果在执行所有提到的故障排除步骤之后，问题仍然存在，请联系 **Citrix** 支持。

为应用程序分析创建阈值和警报

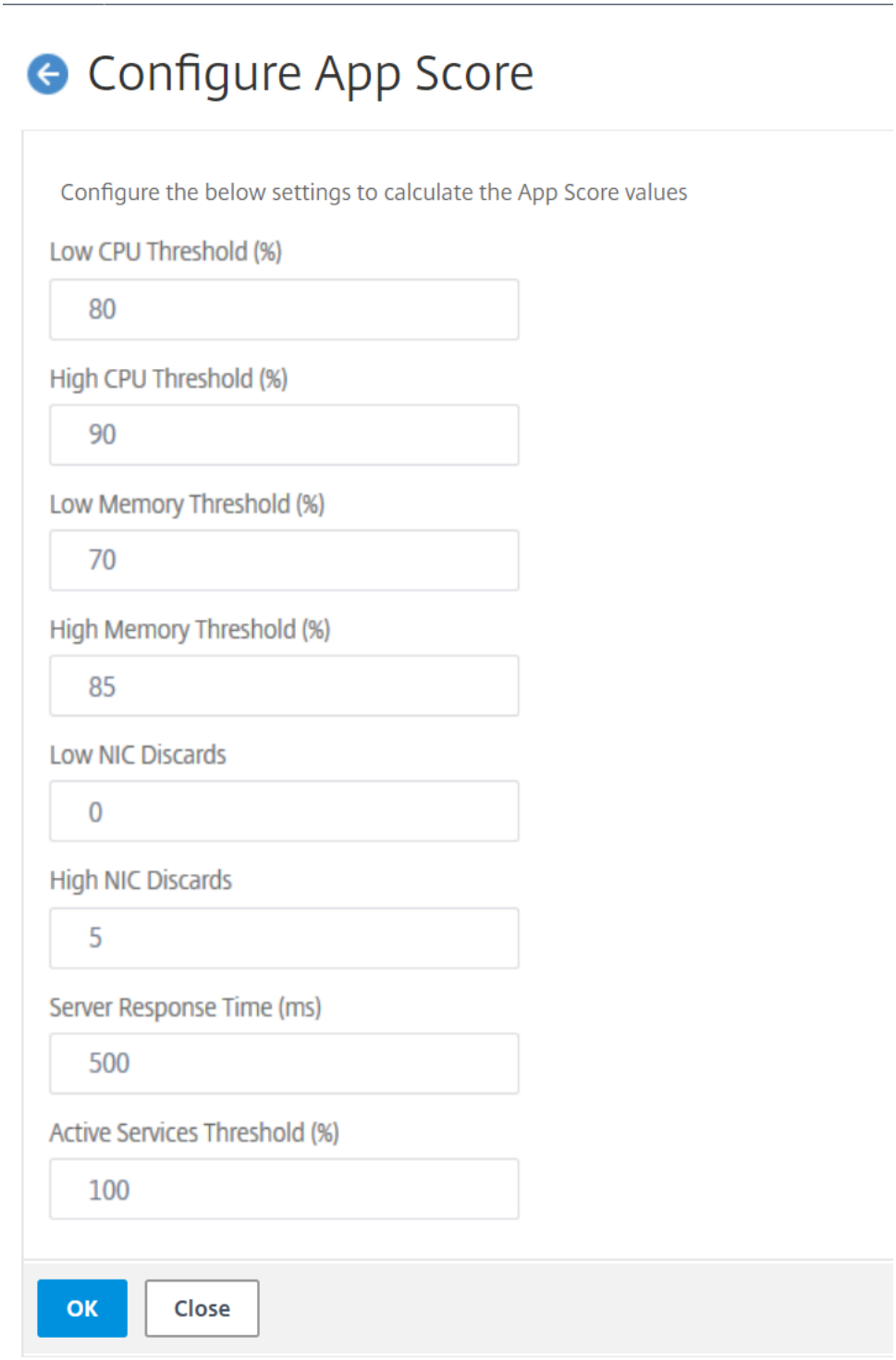
April 23, 2021

通过 Citrix ADM 上的应用程序分析，您可以监视通过 Citrix ADC 实例传递的各种类型的流量。Citrix ADM 允许您在以下计数器上设置阈值，以监视流量和应用程序分数。

您可以配置阈值并监视 CPU、内存、NIC 丢弃和响应时间的应用分数。

要在 **Citrix ADM** 中配置应用程序分数，请执行以下操作：

1. 在 Citrix ADM 中，导航到 分析 > 设置。
2. 在 设置”页上，单击 配置应用程序分数。
3. 在配置应用程序分数页面上，输入以下参数的值：
    a) 低 **CPU** 阈值。Citrix ADC 实例中 CPU 总使用率的较低阈值。
    b) 高 **CPU** 阈值。Citrix ADC 实例中 CPU 总使用率的较高阈值。
    c) 内存阈值低。Citrix ADC 实例中总内存使用量的较低阈值。
    d) 内存阈值高。Citrix ADC 实例中总内存使用量的较高阈值。
    e) 低网卡会丢弃 **SLA**。接口丢弃的数据包的较低阈值。
    f) 高网卡放弃 **SLA**。接口丢弃的数据包的较高阈值。
    g) 响应时间。发送请求数据包与从虚拟服务器上配置的服务接收第一个响应数据包之间的时间间隔。在 Citrix ADM 中配置的默认值为 500 毫秒。
    h) 活动服务阈值。绑定到虚拟服务器的服务必须处于活动状态的百分比阈值。



4. 单击确定。

Intelligent App Analytics

April 23, 2021

Intelligent App Analytics 使您能够使用机器学习和基于规则的算法识别应用性能问题。Citrix ADM 的智能应用分析功能：

- 提供一个简单且可扩展的解决方案，用于监视和故障排除通过 Citrix ADC 实例交付的应用程序。
- 监视所有级别的应用程序，以缩短故障排除问题的周转时间，并提高应用程序的整体正常运行时间。

在典型的部署中，将使用数千个服务器来满足用户的数据需求。发送到这些服务器的流量由 Citrix ADC 设备上配置的虚拟服务器进行负载平衡和监视。每个虚拟服务器均绑定到多个表示后端服务器的服务。在此类部署中，智能应用分析功能可帮助您：

- 在中断和其他事件期间监视、管理和做出决策
- 监视为应用程序配置的虚拟服务器和服务
- 显示有关虚拟服务器和服务的重要信息，以便您可以根据需要更改配置，以实现应用程序的最佳性能。

当您扩大组织服务器场时，很难跟踪与服务器上收到的大量流量相关的问题，并缩小到所需的故障排除范围。

当应用程序正在运行并接收大量流量时，可能会出现各种问题。您可以通过导航到 **“**应用程序**” > “**仪表板**”**，选择一个应用程序，然后向下滚动查看 **“**问题**”** 部分中的问题来查看应用程序分析的性能指标。

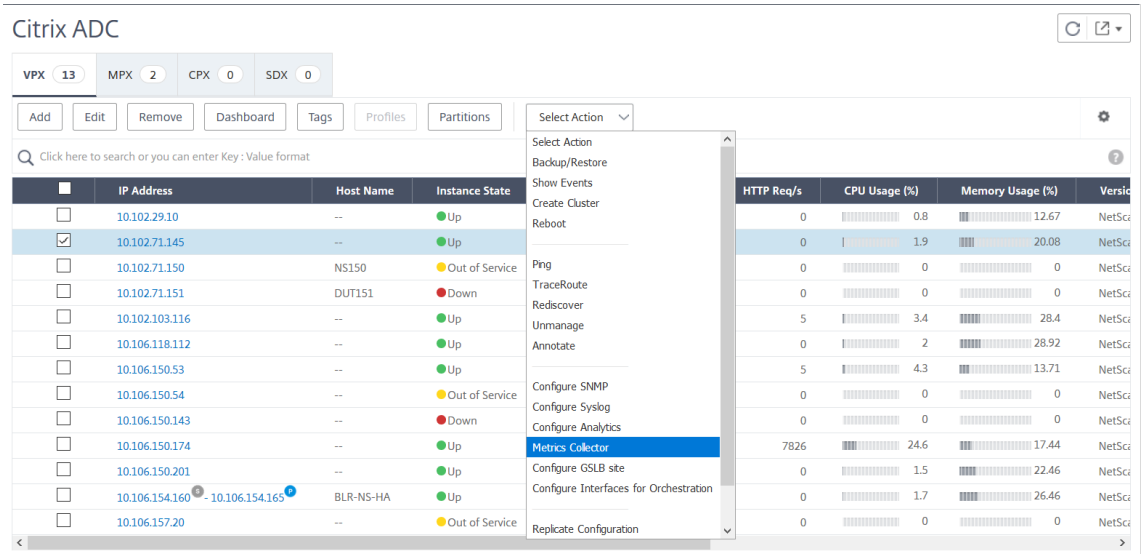
配置智能应用分析

April 23, 2021

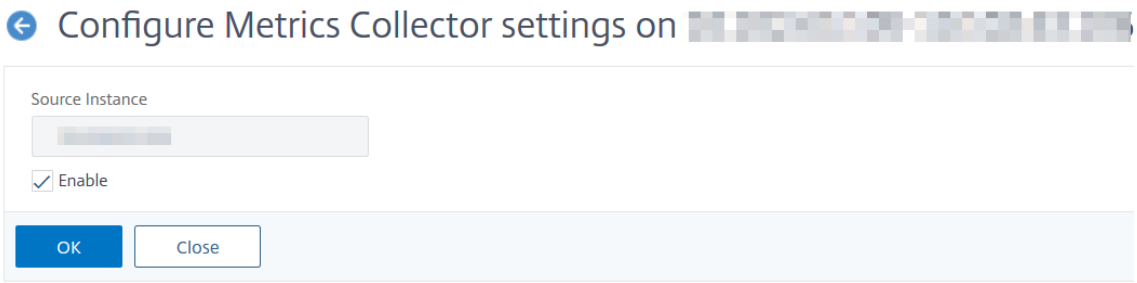
智能应用分析功能仅在 **Citrix ADC 12.1.50.x** 或更高版本中受支持。度量收集器将 Citrix ADC 计数器数据推送到 Citrix ADM，用于检测应用程序问题。要使用智能应用程序分析功能，必须在每个 Citrix ADC 实例上配置指标收集器。默认情况下，将在 Citrix ADC 上启用 度量收集器，同时将实例添加到 Citrix ADM。

要确保 衡量指标收集器是否已启用：

1. 导航到 “ 网络” > “实 例” > “ **Citrix ADC** ”，然后选择要监视的实例类型（例如，Citrix ADC VPX）。
2. 选择 Citrix ADC 实例。
3. 在选择操作列表中，选择指标收集器。



4. 在“ 配置度量收集器设置”页上，默认情况下选中“ 启用”选项。如果未选择此选项，请确保选择“ 启用”选项，然后单击“ 确定”。



> 注意
>
> 要查看 服务器错误及其 详细 **Web** 事务处理的异常情况，必须 分析 在虚拟服务器上启用。

用于应用程序分析的性能指标

April 23, 2021

您可以查看性能指标及其在 Citrix ADC Web 应用程序中出现的类别。要查看这些指标，您必须确保启用分析和 度量收集器 ADC 实例：

启 用分析和指标收集器后，您可以通过导航到“应用程序”>“ 仪表板”，选择一个应用程序，然后向下滚动到“ 问题”部分来查看以下指标：

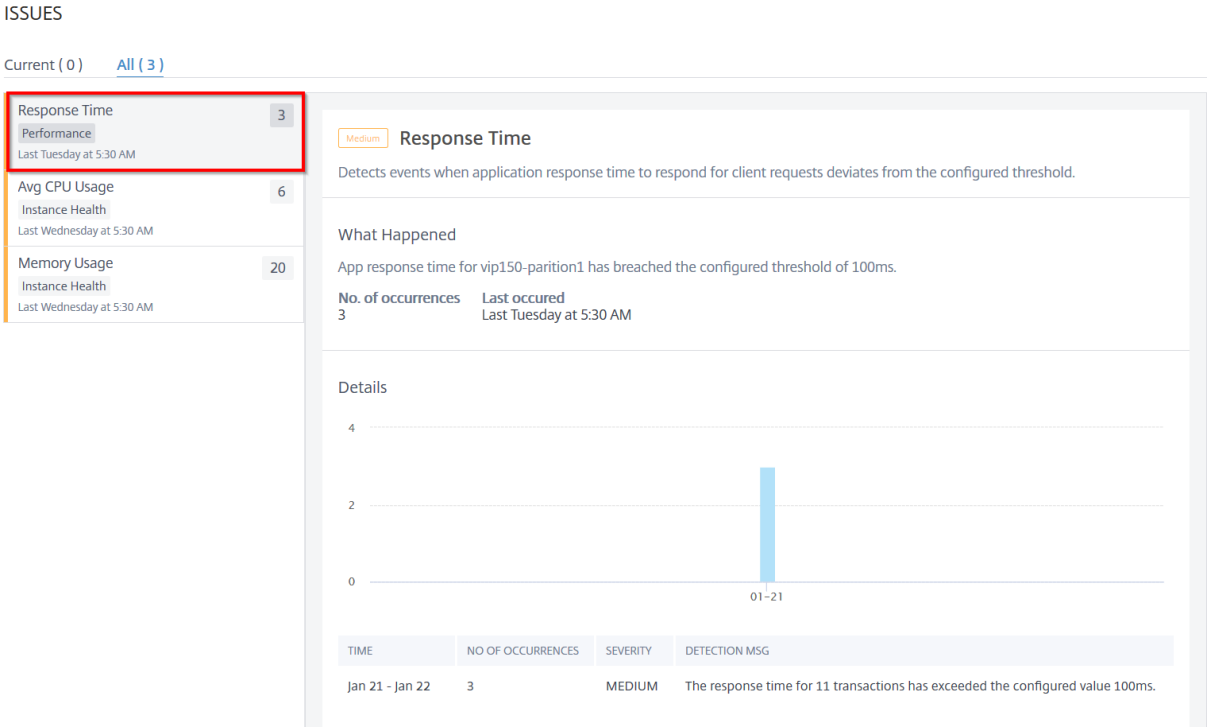
- 响应时间
- 活动服务
- Average CPU Usage（平均 CPU 使用率）

- 内存使用率
- NIC Card Saturation（NIC 卡饱和度）
- 服务摆动
- 低会话重复使用率
- 不正确的持久性类型
- 不稳定的服务器 (5xx)
- SSL 实时流量
- 异常大的 HTTP 数据包
- TCP 重组队列限制命中
- 浪涌队列累积

响应时间

April 23, 2021

当应用程序响应客户端请求的响应时间偏离配置的阈值时，此问题将检测到。单击 响应时间选项卡查看问题详细信息。



在“ 详细信息”下，您可以查看：

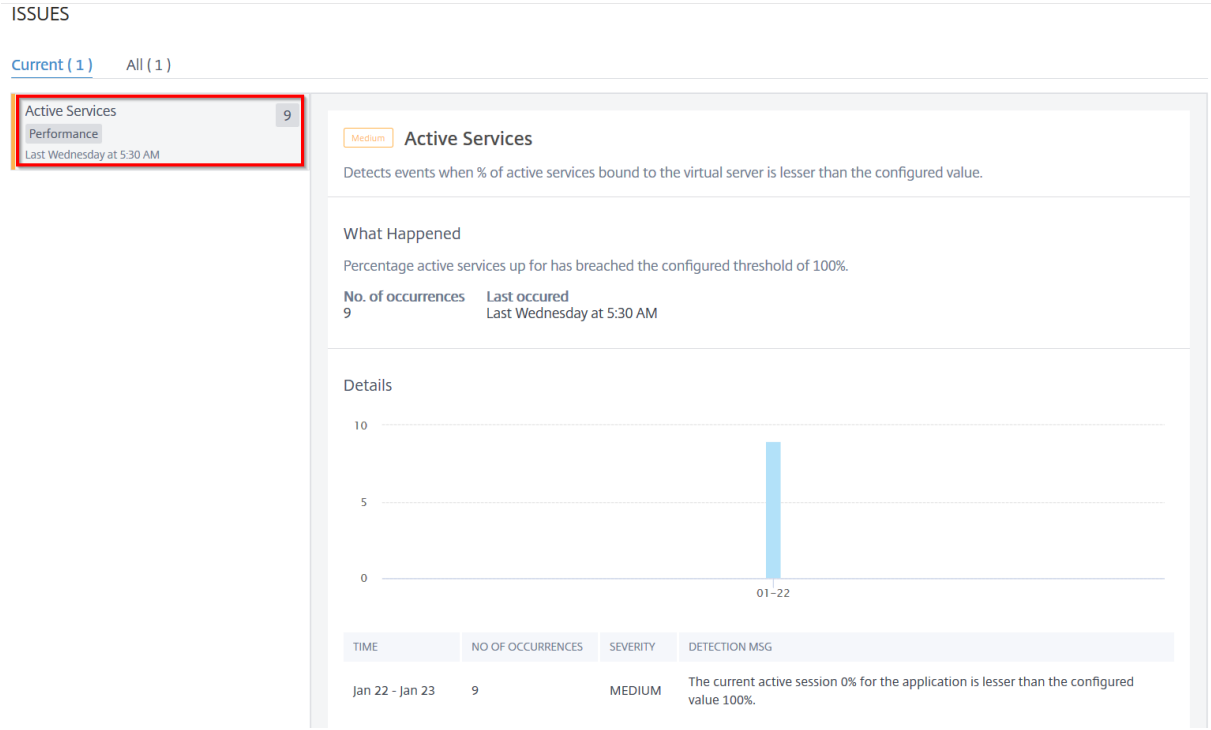
- 指示选定时间内总事件的图形。单击以应用过滤器和查看详细信息

- 问题发生时
- 选定时间的总出现次数
- 问题严重性，如低、中和高
- 指示总事务响应时间超过配置阈值的检测消息

活动服务

April 23, 2021

当绑定到虚拟服务器的活动服务的百分比小于配置的阈值时，会检测此问题。单击 活动服务选项卡查看问题详细信息。



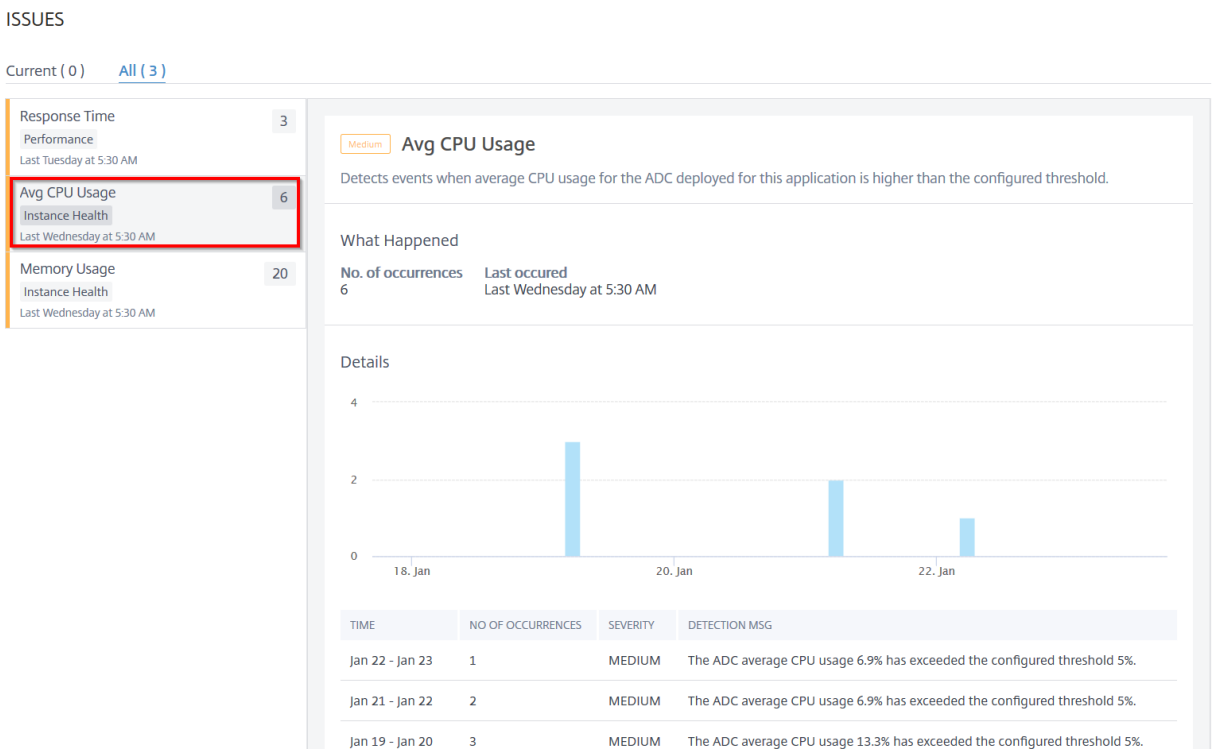
在“ 详细信息”下，您可以查看：

- 指示选定时间持续时间内总事件的图形。单击以应用过滤器和查看详细信息
- 问题发生时
- 选定时间持续时间的总出现次数
- 问题严重性，如低、中和高
- 指示活动服务会话百分比和已配置阈值的检测消息

Average CPU Usage（平均 CPU 使用率）

April 23, 2021

此问题将检测到此应用程序的 ADC CPU 使用率超过配置的阈值。单击“ 平均 **CPU** 使用率”选项卡查看问题详细信息。



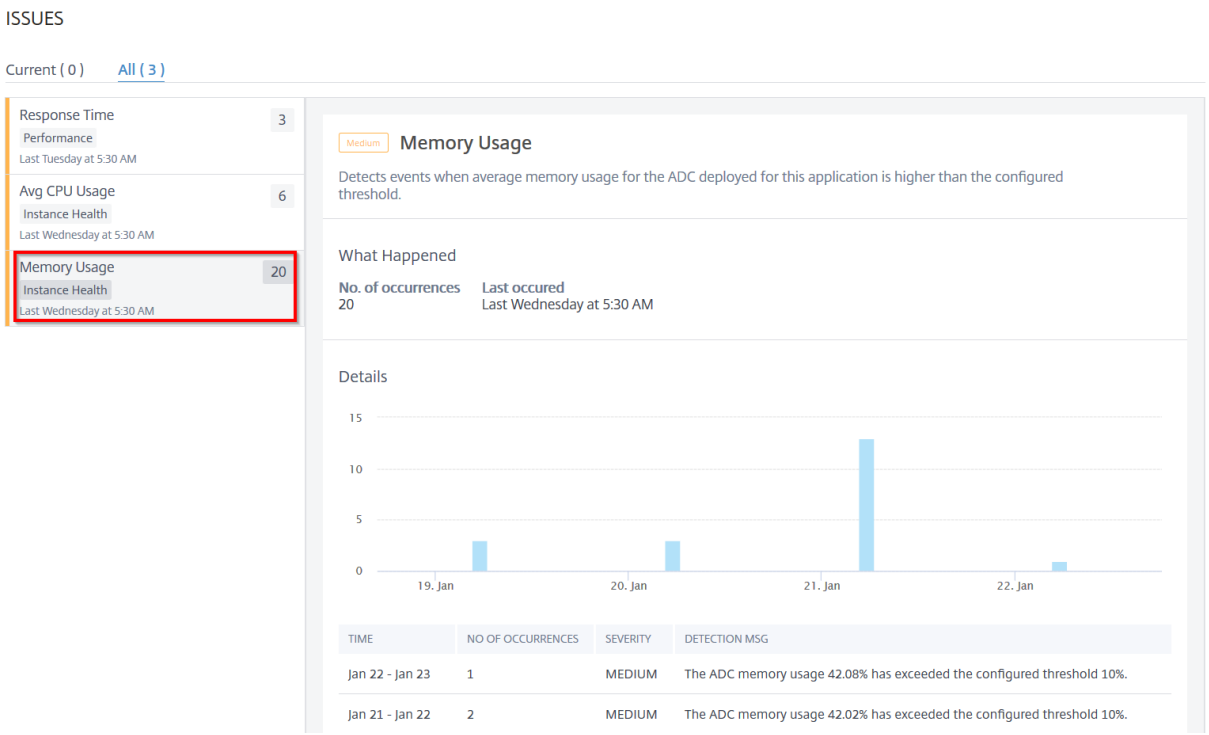
在“ 详细信息”下，您可以查看：

- 指示选定时间持续时间内总事件的图形。单击以应用过滤器和查看详细信息
- 问题发生时
- 选定时间持续时间的总出现次数
- 问题严重性，如低、中和高
- 指示 ADC 平均 CPU 使用率% 和配置阈值的检测消息

内存使用率

April 23, 2021

此问题将检测到此应用程序的 ADC 内存使用量超过配置的阈值。单击内 存使用情况选项卡查看问题详细信息。



在“详细信息”下，您可以查看：

- 指示选定时间持续时间内总事件的图形。单击以应用过滤器和查看详细信息
- 问题发生时
- 选定时间持续时间的总出现次数
- 问题严重性，如低、中和高
- 指示 ADC 平均内存使用率% 和配置阈值的检测消息

服务摆动

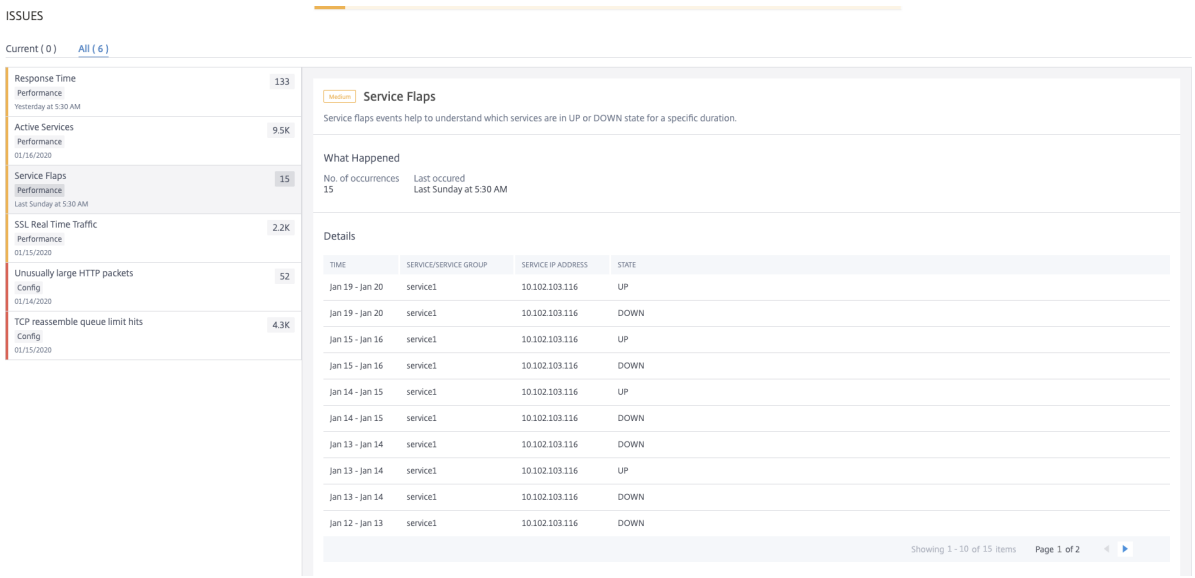
April 23, 2021

作为网络管理员，您必须确保应用程序的最佳可用性。当存在任何网络问题或配置问题时，应用程序服务器的状态和可用性可能会影响整体性能。

使用服务摆动事件，您可以识别存在问题的应用程序。服务摆动事件还可以帮助您：

- 了解特定持续时间内哪项服务处于“关闭”状态
- 了解特定持续时间内有多少服务处于“UP”或“关闭”状态

单击“服务翼”选项卡以查看服务翼详细信息。



您可以查看详细信息，例如发生次数和上次发生时间。

在“ 详细信息”下，您可以查看：

- 服务摆动异常发生的时间
- 服务/服务组名称
- 服务 IP 地址
- 当前服务状态

不稳定的服务器

April 23, 2021

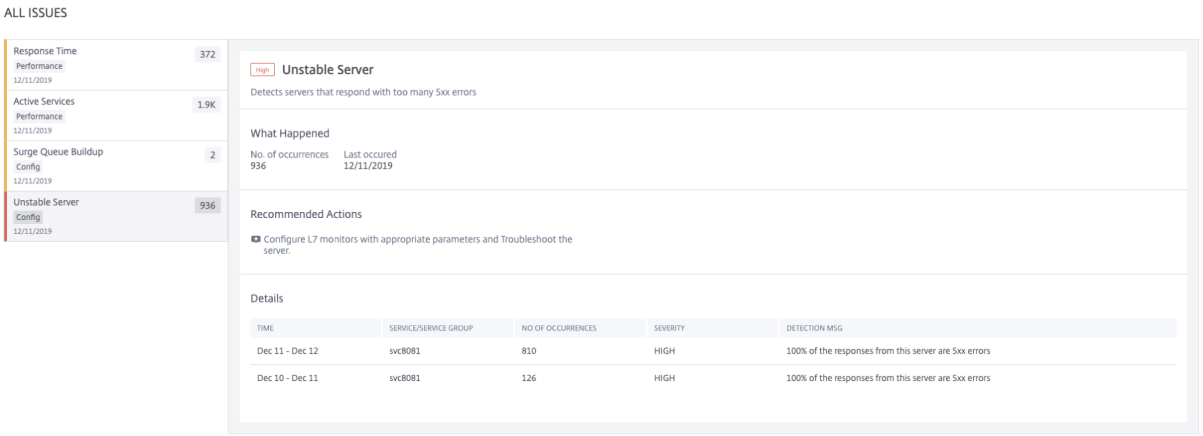
在某些情况下，Web 服务器在由于无效请求、临时重载或服务器维护等原因无法处理请求时使用状态代码作出响应。这些错误随错误代码一起显示，这些代码定义了错误的各种情况。例如，

- **502** 错误 **Gateway**
  服务器充当网关或代理，并收到来自上游服务器的无效响应。
- **503** 服务不可用
  服务器当前不可用。服务器可能已过载或由于进行维护而关闭。
- **504 Gateway** 超时
  服务器充当网关或代理，未收到来自上游服务器的及时响应。

这些可能是临时条件，但有时您必须在 Web 服务器上实施纠正措施，以使网页建立并可用。

使用“ 不稳定服务器”指示器，您可以查看这些故障，并就纠正措施做出决策，以解决问题，并确保客户端请求得到满足，网页始终可用。

选择“ 不稳定服务器”选项卡以查看问题详细信息。



解决问题的 建议操作包括：

- 为响应 5xx 错误的服务器配置适当的参数 L7 监视器。监视器是跟踪服务运行状况的实体。设备使用绑定到每项服务的监视程序定期探测服务器。如果服务器在指定的响应超时内没有响应，并且指定的探测器失败，则该服务将被标记为“关闭”。然后，设备将在其余服务之间执行负载平衡。有关配置监视器的详细信息，请参阅 自定义监视器
- 对服务器进行故障排除

在“ 详细信息”下，您可以查看：

- 发生不稳定服务器异常的时间
- 服务/服务组名称
- 总发生次数
- 异常严重性，如高、低和中
- 检测消息指示此服务报告 5xx 错误的响应百分比

有关服务器错误 Web 事务处理的详细信息，请参阅 针对服务器错误的 Web 事务分析

会话累积

April 23, 2021

对于所有安全事务，Citrix ADC 对第一个事务执行 SSL 卸载过程，然后根据会话重复使用配置存储 SSL 会话。

根据流量速率，会话累积可能会在一段时间内发生，这可能导致 Citrix ADC 中的这些会话占用大量内存。

会话累积事件会提醒管理员，并提供解决此事件的建议操作。单击“会 话生成”选项卡以查看问题详细信息

在“ 详细信息”下，您可以查看：

- 会话累积异常发生的时间
- 虚拟服务器名称
- 异常严重性，如高、低和中
- 该消息指示虚拟服务器中可用的 SSL 会话数量为 **X**，当前配置的超时会话中每秒有 **Y** 个 SSL 握手。

修复此异常的建议操作是减少会话超时或禁用会话重用。有关详细信息，请参阅会话超时。

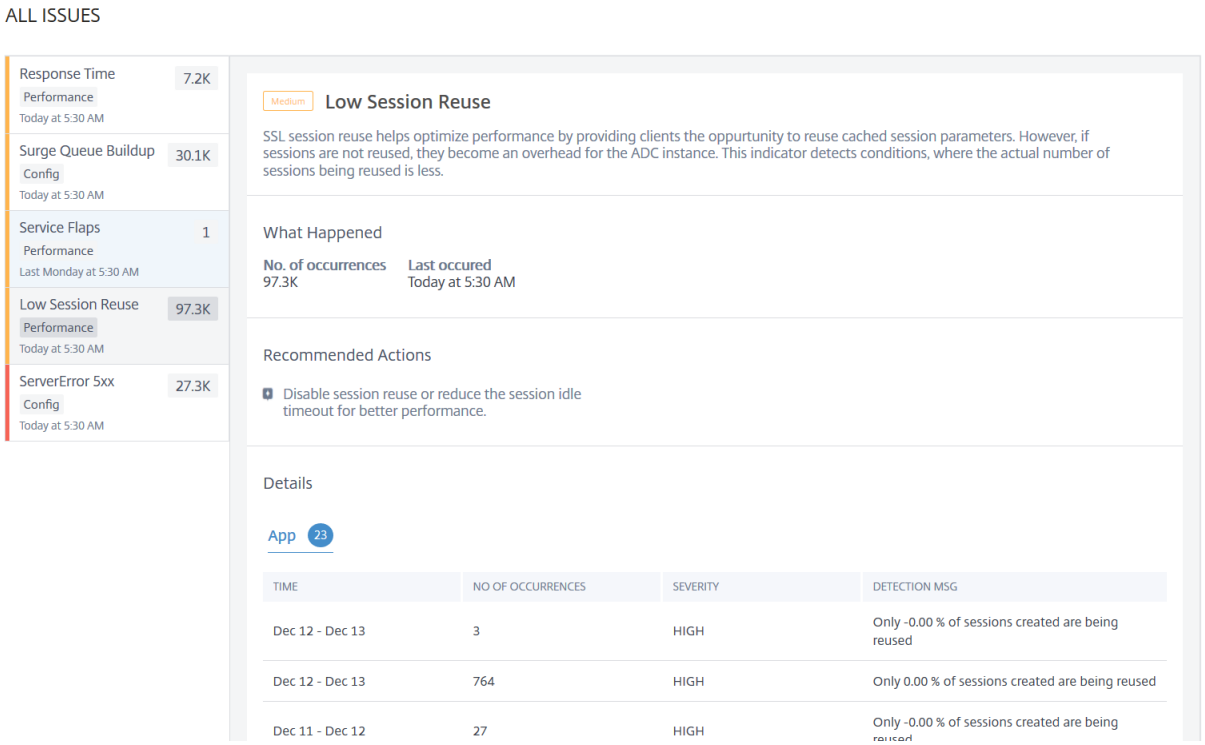
低会话重复使用

April 23, 2021

Citrix ADC 实例通过从服务器卸载 SSL 握手过程来处理 SSL 事务。从服务器收到响应后，Citrix ADC 实例将完成与客户端的安全事务。使用缓存的会话参数，Citrix ADC 实例将完成连续请求的 SSL 握手过程。

如果这些会话未被重复使用，则会成为 Citrix ADC 实例的开销。使用 低会话重复使用指示器，您可以确定实际重复使用的会话数是否较少。

单击 “ 低会话重复使用” 选项卡查看问题详细信息。



解决问题的 建议操作是禁用会话重复使用或减少会话超时。有关详细信息，请参阅会话重复使用。

在 “ 详细信息” 下，您可以查看：

- 会话重复使用率低的应用程序总数

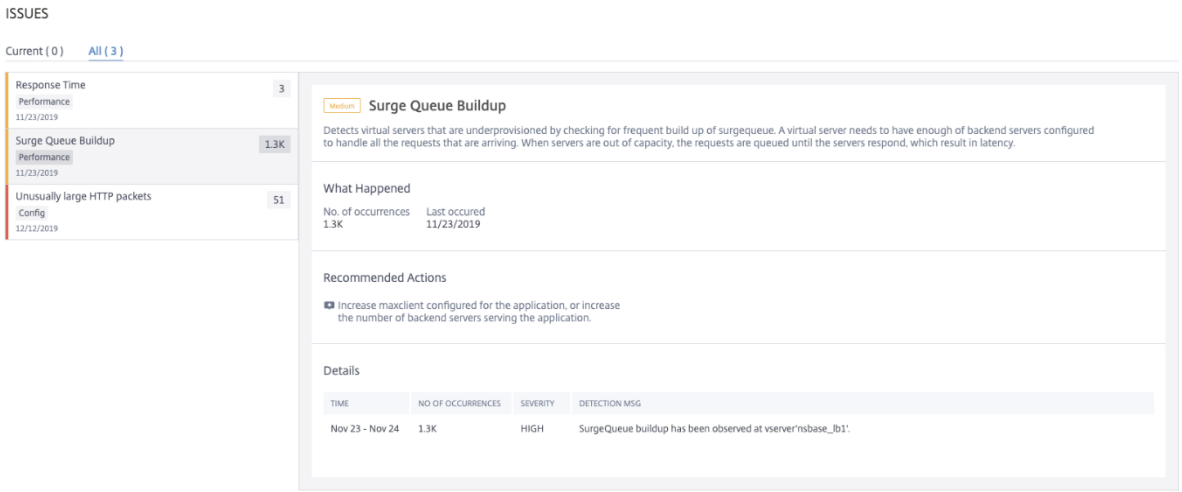
- 发生低会话重复使用异常的时间
- 总发生次数
- 异常严重性，如高、低和中
- 检测消息指示只有% 已配置的会话正在重复使用

浪涌队列累积

April 23, 2021

当服务器收到大量请求时，服务器对客户端的响应变得缓慢。通常，重载也会导致客户端收到错误页面。虚拟服务器需要配置足够的后端服务器来处理传入的请求。

使用 浪涌队列累积指示器，您可以查看具有浪涌队列累积的虚拟服务器。单击 “ 浪涌队列累积” 选项卡以查看问题详细信息。



解决问题的 建议操作包括：

- 增加客户端连接数限制。有关详细信息，请参阅设置客户端连接数量的限制。
- 增加后端服务器以满足应用程序请求

在 “ 详细信息” 下，您可以查看：

- 浪涌队列积累异常发生的时间
- 总发生次数
- 异常严重性，如高、低和中
- 指示虚拟服务器上浪涌队列累积的检测消息

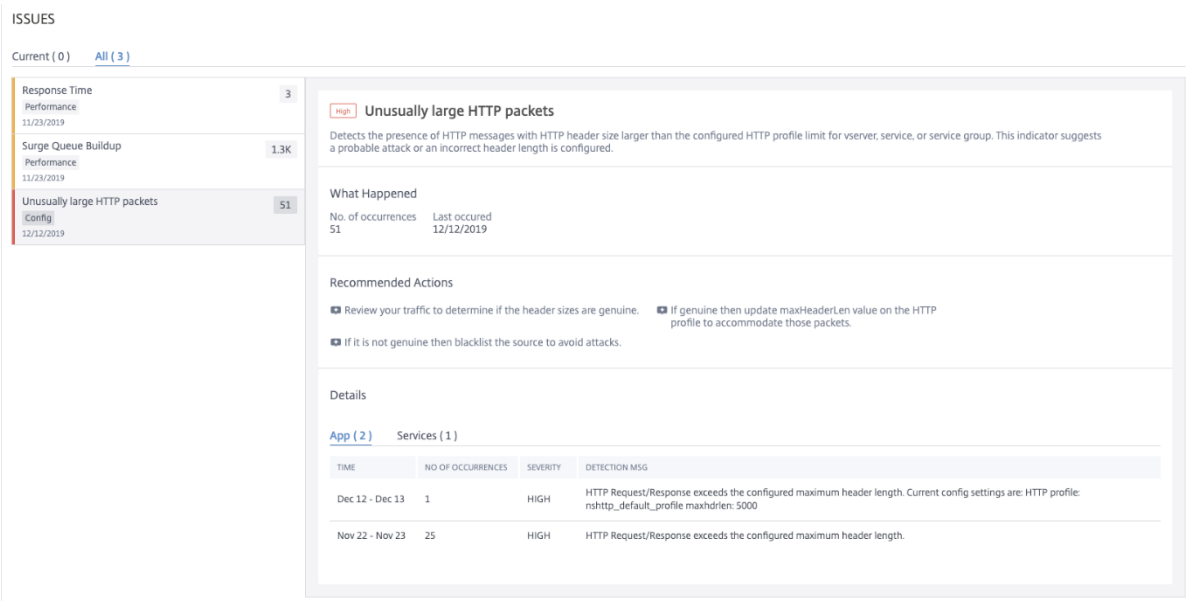
异常大的 **HTTP** 数据包

April 23, 2021

HTTP 事务在客户端和服务器之间使用请求响应消息。在请求和响应消息中，HTTP 标头是 HTTP 协议中显示的值。您可以在虚拟服务器、服务或服务组中配置 HTTP 标头长度，以避免 4xx 错误

当 HTTP 请求/响应超过最大标头长度时，它可能是可能的攻击。使用 异常大的 **HTTP** 数据包指示器，您可以查看具有 HTTP 标头大小的 HTTP 消息超过配置值的情况。

单击 异常大的 **HTTP** 数据包选项卡查看问题详细信息。



解决问题的 建议操作包括：

- 查看流量以确定报头大小是真实的。如果标头大小是真实的，则更新 HTTP 配置文件上的标头值。有关详细信息，请参阅缓冲区溢出检查。
- 如果标头大小不是真实的，请阻止列出来源以避免攻击。

在“ 详细信息”下，您可以查看：

- 发生异常的时间
- 总发生次数
- 异常严重性，如高、低和中
- 指示在虚拟服务器、服务器或服务组上配置的当前 HTTP 标头长度的检测消息

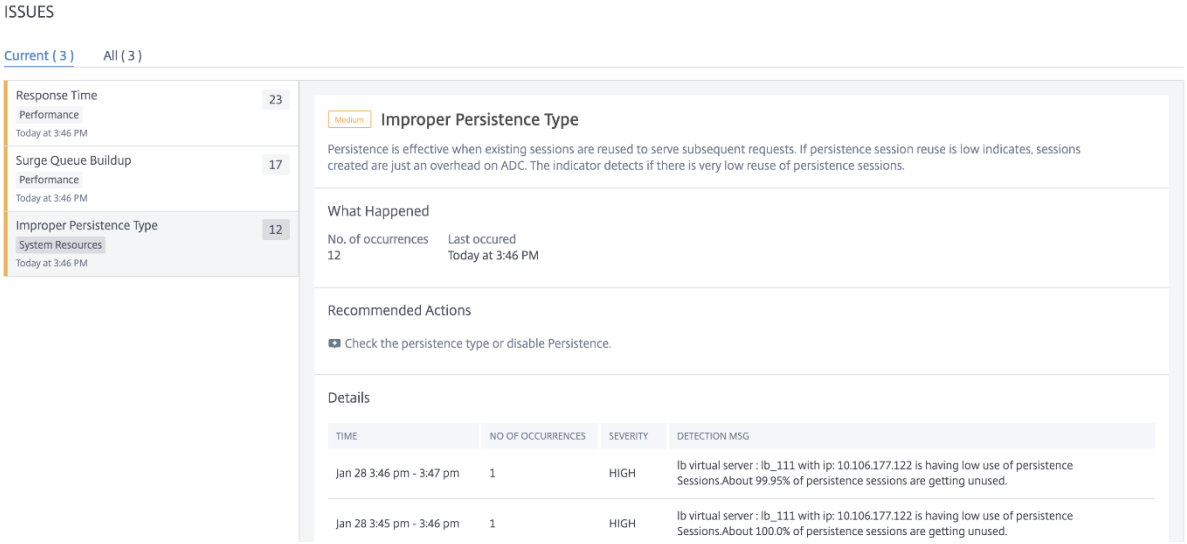
不正确的持久性类型

April 23, 2021

如果您要在由虚拟服务器表示的服务器上保持连接状态（例如，电子商务中使用的连接），必须对该虚拟服务器配置持久性。然后，设备将使用配置的负载平衡方法进行初始选择服务器，但将所有后续请求从同一客户端转发到同一服务器。

当重复使用现有会话来处理后续请求时，持久性会有效。如果持久性会话重复使用率较低，则在 ADC 上创建的会话只是一个开销。

使用 不正确的持久性类型指示器，您可以确定虚拟服务器上的持久性使用率是否较低。单击 不正确的持久性类型选项卡以查看问题详细信息。



解决问题的 建议操作是检查持久性类型或禁用持久性。有关详细信息，请参阅持久性设置。

在“ 详细信息”下，您可以查看：

- 发生异常的时间
- 总发生次数
- 异常严重性，如高、低和中
- 指示未使用会话百分比的检测消息

TCP 重新组装队列限制命中

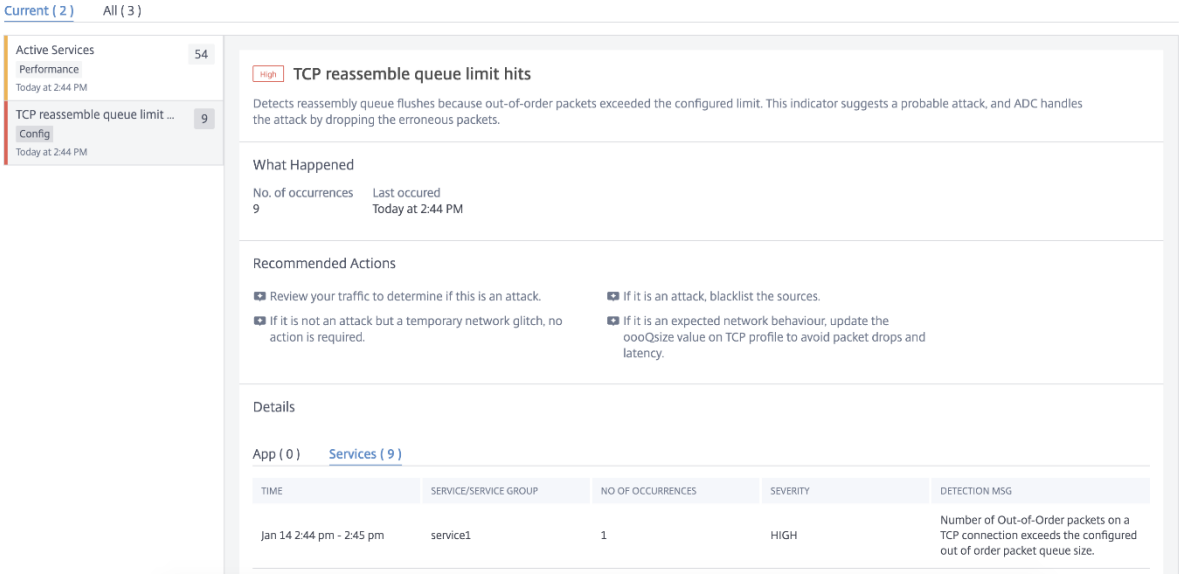
April 23, 2021

TCP 维护一个无序队列，以将 OOO 数据包保留在 TCP 通信中。如果队列大小很长时间需要将数据包保存在运行时内存中，则此设置会影响 Citrix ADC 内存。

根据网络和应用程序特征，此队列大小需要处于优化水平。

使用 **TCP** 重新组装队列限制命中指示器，您可以查看 TCP 连接上的无序数据包是否超过配置的无序数据包队列大小。

单击 **TCP** 重新装配队列限制命中选项卡查看问题详细信息。



解决问题的 建议操作包括：

- 查看流量并阻止列出来源（如果是攻击）
- 如果此行为是预期的网络行为，则更新 TCP 配置文件上的无序数据包大小值。有关详细信息，请参阅TCP 优化。
- 如果只是一个临时的网络故障，则不需要进一步的操作

在“ 详细信息”下，您可以查看：

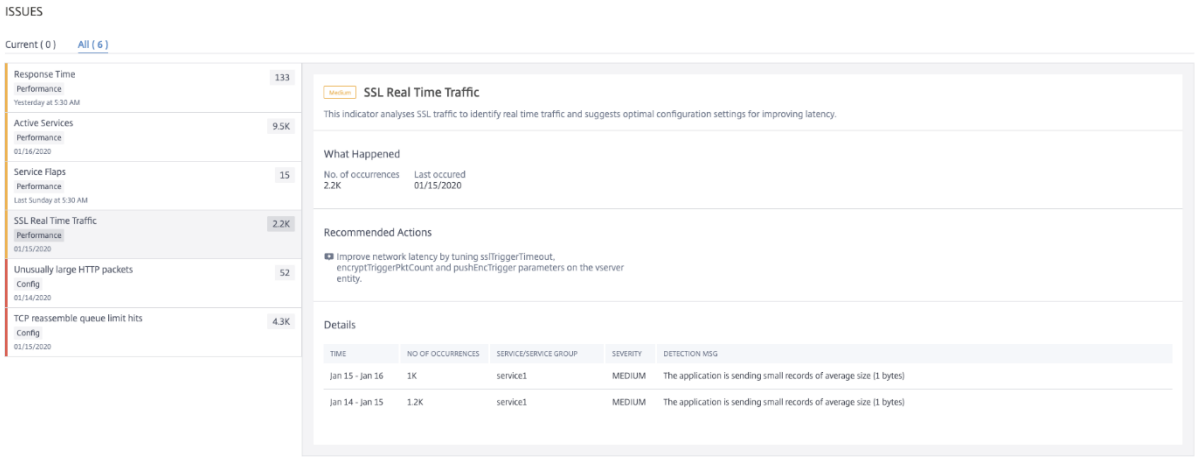
- 发生异常的时间
- 总发生次数
- 异常严重性，如低、中和高
- 指示当前 TCP 配置文件和 OOQSize 设置的检测消息

SSL 实时流量

April 23, 2021

在 Citrix ADC 实例中，您可以使用 SSL 配置文件来处理 SSL 流量。SSL 配置文件包含虚拟服务器、服务和服务组的某些 SSL 参数。**SSL** 实时流量指示器分析 **SSL** 流量，以确定实时流量，并为改善延迟提供最佳配置设置建议。

单击 **SSL** 实时流量选项卡查看问题详细信息。



解决问题的 建议措施是通过更新 SSL 参数来改善网络延迟。有关详细信息，请参阅全局 SSL 参数。

在“ 详细信息”下，您可以查看：

- 发生异常的时间
- 服务/服务组名称
- 异常严重性，如低、中和高
- 应用程序上具有当前设置的检测消息

应用程序安全控制面板

April 23, 2021

应用程序安全控制面板提供了已发现/许可应用程序的安全度量概览。此控制板显示已发现/许可应用程序的安全攻击信息，例如同步攻击、小窗口攻击、DNS 洪水攻击等。

要查看应用程序安全控制板上的安全指标，请执行以下操作：

1. 导航到 应用程序 > 应用程序安全控制面板。
2. 从“实例”列表中选择实例 IP 地址。

   报告包含每个应用程序的以下信息：

   - 威胁指数。一个单位数评级系统，用于指示应用程序攻击的严重程度。应用程序上的攻击越严重，该应用程序的威胁指数越高。值范围介于 1 到 7 之间。

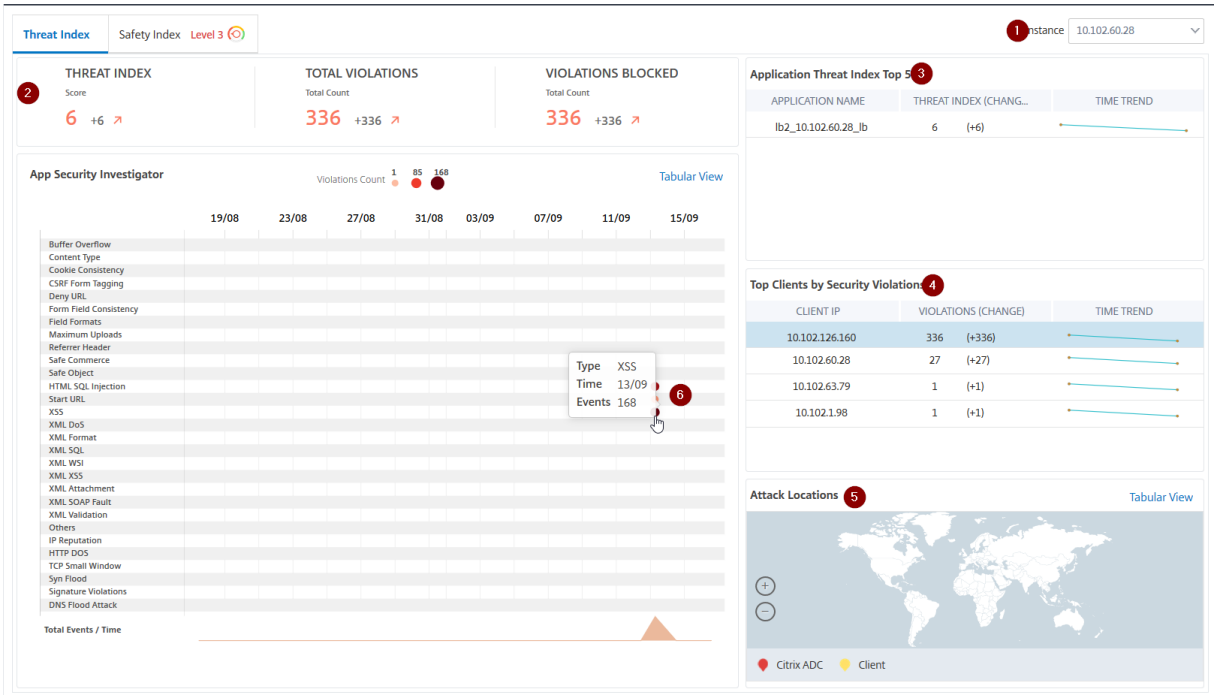
     威胁指数基于攻击信息。与攻击相关的信息（如违规类型、攻击类别、位置和客户端详细信息）可以深入了解应用程序的攻击。只有在发生违规或攻击时，才会向 Citrix ADM 发送违规信息。大量违反和漏洞会导致较高的威胁指数值。

- 安全指数。一个单位数评级系统，用于指示您配置 Citrix ADC 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数越高。值范围介于 1 到 7 之间。

  安全指标同时考虑应用程序防火墙配置和 Citrix ADC 系统安全配置。为了获得较高的安全指数值，两个配置都必须强健。例如，如果进行了严格的应用程序防火墙检查，但没有提供 Citrix ADC 系统安全措施（例如 `nsroot` 用户的强密码），则应用程序将被分配一个较低的安全指数值。

您可以查看 应用安全调查员上报告的差异。

威胁索引详细信息



1 -显示您可以查看其详细信息的 Citrix ADC 实例 IP 地址。

2 -显示威胁指数分数、发生的违规总数和阻止的违规总数等详细信息。

3 -显示所选实例的虚拟服务器。

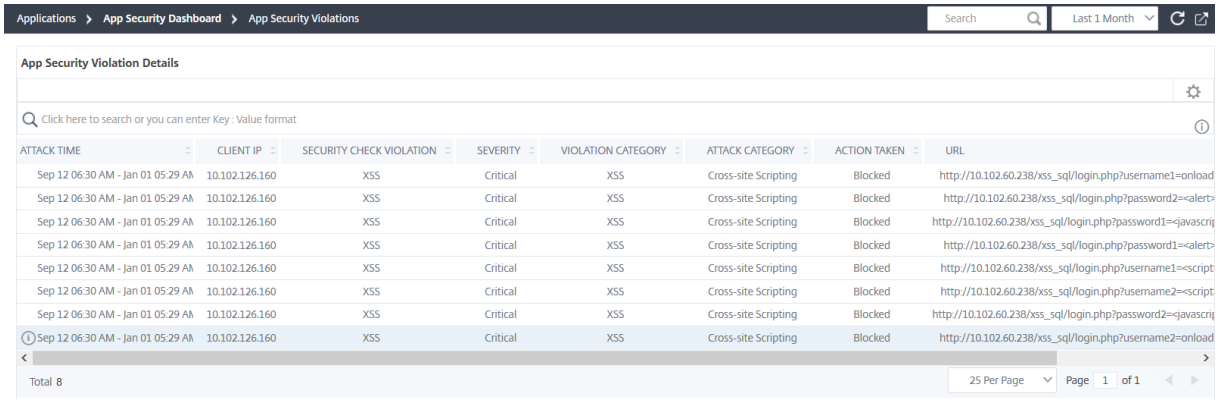
4 -显示基于客户端的安全违规。将显示每个客户端的“应用安全调查器”图形。您可以单击每个客户端 IP 以查看结果。

5 -在地图视图和表格视图中显示违规。

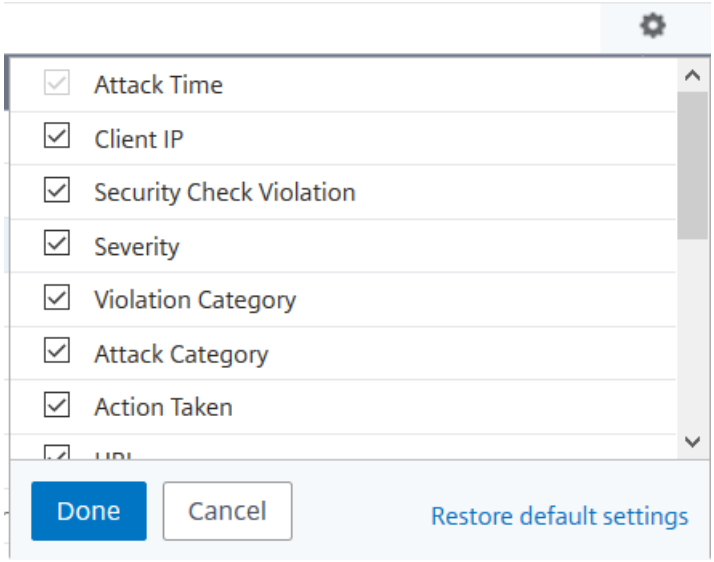
6 -显示违规详细信息。将鼠标指针悬停在图形上时，将显示违规类型、攻击时间和总事件等详细信息。

单击气泡图时，详细信息将显示在 应用程序安全违规详细信息页面中。例如，如果要进一步查看跨站点脚本（跨站点脚本）违规的详细信息，请在 应用程序安全调查器中单击为 **XSS** 填充的图表。

显示应用程序安全违例详细信息，包括攻击时间、攻击类别、严重程度、URL 等违例详细信息。



您还可以单击设置选项以选择要显示的选项。



安全指数详细信息

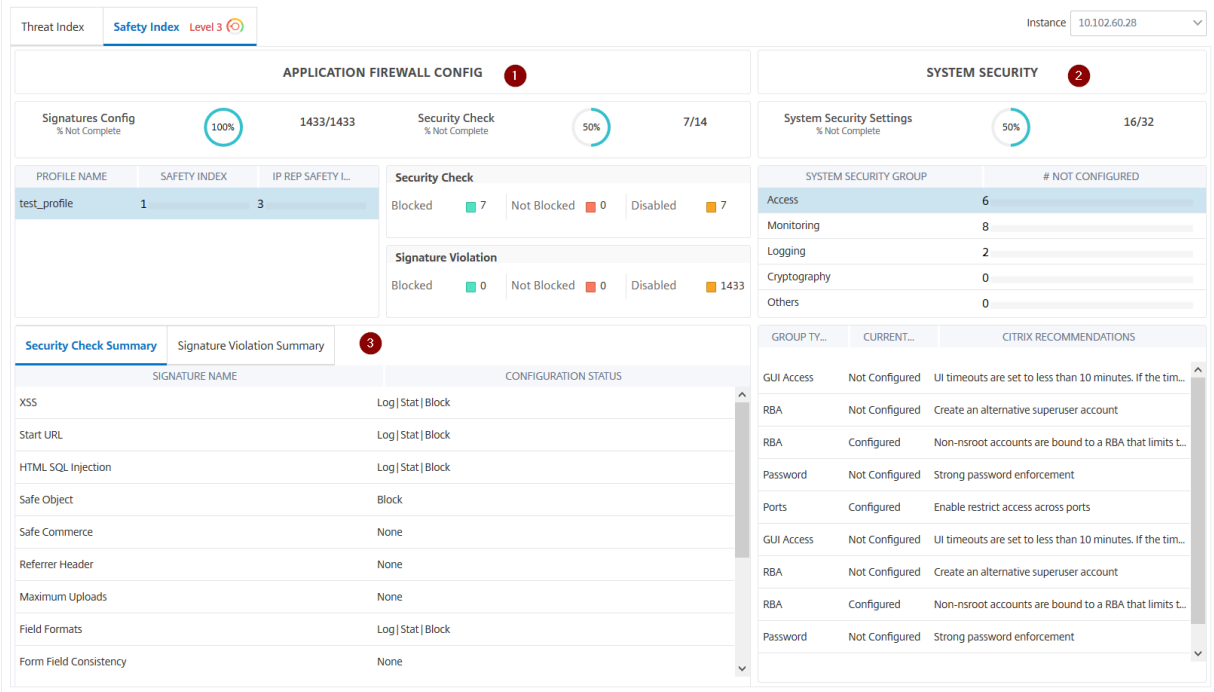
查看了应用程序面临的威胁后，您希望确定哪些应用程序安全配置正在实施，以及该应用程序缺少哪些配置。您可以通过深入查看应用程序安全指数摘要来获取此信息。

安全指数摘要为您提供有关以下安全配置的有效性：

- 应用防火墙配置。显示多少签名和安全实体未配置。
- **Citrix ADM** 系统安全。显示多少系统安全设置未配置。

要查看 安全索引详细信息，请选择虚拟服务器/应用程序，然后单击 安全索引选项卡。

将显示详细信息。



1 -显示应用程序防火墙配置的详细信息。

2 -显示系统安全性的详细信息。单击每个安全组以获取有关当前状态和 Citrix 建议的详细信息。

3 -显示安全检查和签名违规的摘要。

您还可以通过安全见解为虚拟服务器启用，然后导航到分析 > 安全见解，查看威胁环境摘要。有关安全索引使用案例的详细信息，请参阅 安全见解

服务图表

April 23, 2021

Citrix ADM 中的服务图功能使您能够以图形表示形式监视所有服务。此功能还允许您查看服务的详细分析和可操作指标。您可以查看以下内容的服务图：

- 跨所有 Citrix ADC 实例配置的应用程序
- Kubernetes 应用程序
- 3 层 Web 应用程序

跨所有 **Citrix ADC** 实例的应用程序的服务图

通过全球服务图功能，您可以获得 `clients to infrastructure to application` 视图的整体可视化。在此单窗格服务图视图中，作为管理员，您可以：

- 了解用户从哪个区域访问特定应用程序（3 层 Web 应用程序和微服务应用程序）
- 可视化处理客户端请求的基础架构（Citrix ADC 实例）视图
- 了解问题是来自客户端、基础架构还是应用程序
- 进一步深入解决问题

导航到 应用程序 **>** 服务图表，然后单击 全局选项卡以查看：

- 从客户端到后端服务器连接的所有应用程序的端到端
- 连接到各自数据中心的所有 Citrix ADC 实例

  > 注意
  >
  > 只有在拥有 GSLB 应用程序时，才能查看数据中心。

- 客户端指标信息
- Citrix ADC 指标信息
- 所有具有离散应用程序、定制应用程序和离散微服务应用程序的 Citrix ADC 实例
- 属于自定义应用程序、离散应用程序和微服务应用的前 4 个低分应用
- 排名前 4 位低分虚拟服务器的指标信息
- 应用程序（离散应用程序、自定义应用程序和微服务应用程序）状态如 “ 严重”、“ 评论”、“ 良好” 和 “ 不适用”

有关详细信息，请参阅服务图中应用程序的整体视图。

Kubernetes 应用程序的服务图

导航到 应用程序 **>** 服务图表，然后单击 微服务选项卡以查看：

- 确保端到端应用程序的整体性能
- 识别应用程序不同组件之间的相互依赖关系造成的瓶颈
- 收集有关应用程序不同组件的依赖关系的见解
- 监视 Kubernetes 群集内的服务
- 监视哪些服务存在问题
- 检查导致性能问题的因素
- 查看服务 HTTP 事务的详细可见性
- 分析 HTTP、TCP 和 SSL 指标

通过在 Citrix ADM 中可视化这些指标，您可以分析问题的根本原因并更快地采取必要的故障排除操作。服务图表将应用程序显示到各种组件服务中。在 Kubernetes 群集内运行的这些服务可以与应用程序内外的各种组件进行通信。要开始操作，请参阅设置服务图表。

3 层 **Web** 应用程序的服务图

导航到 应用程序 **>** 服务图表，然后单击 **Web** 应用程序选项卡以查看：

- 有关如何配置应用程序的详细信息（使用内容交换虚拟服务器和负载平衡虚拟服务器）

  对于 GSLB 应用程序，您可以查看数据中心、ADC 实例、CS 和 LB 虚拟服务器。
- 从客户端到服务的端到端交易
- 客户端访问应用程序的位置
- 处理客户端请求的数据中心名称和关联的数据中心 Citrix ADC 指标（仅适用于 GSLB 应用程序）
- 客户端、服务和虚拟服务器的度量详细信息
- 如果错误来自客户端或服务
- 服务状态，如 “ 严重”、“ 审查” 和 “正 常”。Citrix ADM 根据服务响应时间和错误计数显示服务状态。
  - 严重（红色） -指示平均服务响应时间 > 200 毫秒，错误计数 > 0
  - 查看（橙色） -指示平均服务响应时间 > 200 毫秒或错误计数 > 0 的时间
  - 良好（绿色） -表示无错误，平均服务响应时间小于 200 ms
- 客户端状态，如 “ 严重”、“ 审核” 和 “正 常”。Citrix ADM 根据客户端网络延迟和错误计数显示客户端状态。
  - 严重（红色）-指示平均客户端网络延迟时间 > 200 毫秒，错误计数 > 0
  - 查看（橙色） -指示客户端网络平均延迟 > 200 ms 或错误计数 > 0 时
  - 良好（绿色） -表示没有错误，客户端网络平均延迟小于 200 ms
- 虚拟服务器状态，如 “ 严重”、“ 审查” 和 “正 常”。Citrix ADM 根据应用程序分数显示虚拟服务器状态。
  - 严重（红色） -指示应用程序分数小于 40 的时间
  - 评论（橙色） -指示应用得分介于 40 到 75 之间时
  - 良好（绿色） -指示应用程序分数大于 75

注意事项：

- 服务图中仅显示负载平衡、内容切换和 GSLB 虚拟服务器。
- 如果没有将虚拟服务器绑定到自定义应用程序，则详细信息在应用程序的服务图中不可见。
- 只有在虚拟服务器和 Web 应用程序之间发生活动事务时，才能在服务图中查看客户端和服务的度量。

- 如果虚拟服务器和 Web 应用程序之间没有活动事务处理，则只能根据配置数据（如负载平衡、内容切换、GSLB 虚拟服务器和服务）在服务图中查看详细信息。
- 如果对应用程序配置进行了任何更改，则可能需要 10 分钟才能反映在服务图中。

有关详细信息，请参阅应用程序的服务图。

设置服务图表

April 23, 2021

软件要求

库贝内特斯分布	库贝内特斯版	容器网络接口 (CNI)	CPX 版本	CIC 版本	Citrix ADM 版本	Citrix ADM 代理版本
开源代码	v1.16.3	法兰绒、印花布或运河	13.0—41.28 或更高版本	1.5.25 或更高版本	13.0—47.22 或更高版本	13.0—47.22 或更高版本

您可以使用各种 部署拓扑 配置 Kubernetes 集群，下表提供了服务图中支持的拓扑：

拓扑	服务图支持
单层或统一入口	是
双层	是
云	是的，但是图表中未显示云负载均衡器
服务网格精简版	是
服务网格	是
负载均衡器类型的服务	否
NodePort 类型的服务	否

要在 Citrix ADM 中完成服务图的设置，请单击为 Kubernetes 集群配置的拓扑类型，然后完成上述步骤：

- 单层或统一入口拓扑
- 双层或服务网状精简版拓扑
- 服务网状拓扑

> 注意
>
> 为双层和服务网格精简版拓扑设置服务图的过程保持不变。

准备工作

您可以使用以下方案查看服务图表：

- Citrix ADM 和 Kubernetes 群集位于同一网络上（例如，托管在同一 Citrix Hypervisor 上的 Citrix ADM 和 Kubernetes 群集）。
- Citrix ADM 和库伯内特斯群集在另一个网络上。在这种情况下，您必须配置 本地代理 并在网络上注册代理，其中 Kubernetes 群集托管。

单层或统一入口拓扑

请确保您具有：

- 使用单层或统一入口拓扑配置 Kubernetes 集群。
- 在 Citrix ADM 中中添加了 VPX、MPX、SDX、BLX 实例 并启用了 **Web Insight**。
- 已 库贝内特斯群集 在 Citrix ADM 中添加。

双层或服务网状精简版拓扑

请确保您具有：

- 使用任何一种支持的拓扑配置了 Kubernetes 集群。
- 在 Citrix ADM 静态路由 上配置以启用 Citrix ADM 和 Citrix ADC CPX 之间的通信。

  > 注意
  >
  > 如果已将 Citrix ADM 作为微服务部署在同一群集中，则可以忽略此过程。

- 从 GitHub 仓库下载了 示例部署文件。
- 在 CPX YAML 文件中添加了 必需的参数，以确保在 Citrix ADM 成功注册 CPX。
- 在 Citrix ADM 中添加了VPX、MPX、SDX 或 BLX 实例。
- 在 Citrix ADM 中添加了库贝内特斯群集。
- 已部署 微服务应用示例.
- 已部署 Citrix ADC CPX 和 向 ADM 注册 CPX （仅适用于双层体系结构）
- 已启 自动选择虚拟服务器 用可授权虚拟服务器。
- 为 Citrix ADM 代理启用 Web 事务和 TCP 事务设置 并设置为全部以获取 HTTP 和 TCP 事务。
- 发送 流量 到微服务。

服务网状拓扑

请确保您具有：

- 使用以下任何一种服务网状拓扑配置 Kubernetes 集群版本 `1.14.0`：
  - Citrix ADC CPX 作为 Istio 的侧车代理
  - Citrix ADC 作为 Istio 的入口网关

  有关详细信息，请参阅Citrix ADC Istio 适配器部署架构。
- 启用了 `admissionregistration.k8s.io/v1beta1` API。您可以使用以下命令验证 API：

  ```
  kubectl api-versions | grep admissionregistration.k8s.io/v1beta1
  ```

  以下输出表示 API 已启用：

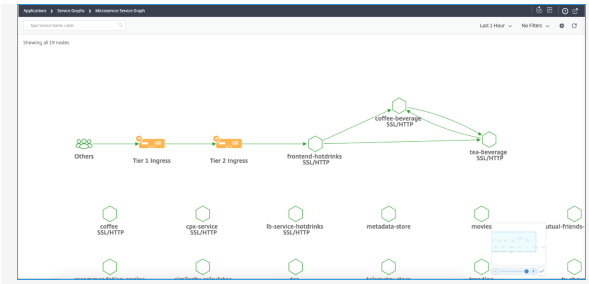
  ```
  admissionregistration.k8s.io/v1beta1
  ```
- 安装了 Istio `istio v.1.3.0`。
- 安装了 Helm 版本 3.x。
- 在 Citrix ADM 静态路由 上配置以启用 Citrix ADM 和 Citrix ADC CPX 之间的通信。

  > 注意
  >
  > 如果已将 Citrix ADM 代理作为微服务部署在同一群集中，则可以忽略此过程。
- 配置了 必需的参数 以填充服务网格拓扑数据。
- 已部署 示例应用.
- 在 Citrix ADM 中添加了库贝内特斯群集。
- 已启 自动选择虚拟服务器 用可授权虚拟服务器。
- 为 Citrix ADM 代理启用 Web 事务和 TCP 事务设置 并设置为全部以获取 HTTP 和 TCP 事务。
- 发送 流量 到微服务。

在服务图中查看详细信息

April 23, 2021

在 Citrix ADM 中，导航到 应用程序 **>** 服务图 **> Kubernetes** 服务图，然后从列表中选择持续时间以查看服务图详细信息。

两级/服务网格 lite 拓扑	单一级/统一入端拓扑
	

- 第 **1** 层入口 — Kubernetes 集群内的 Citrix Ingress Controller 在 Kubernetes 集群之外配置 Citrix ADC 实例（VPX/MPX/SDX/BLX）。
- 第 **2** 层入口 — Citrix Ingress Controller 与 Kubernetes 集群内的 Citrix ADC CPX 实例一起作为侧车运行。
- 入口 — 显示所有其他部署拓扑。

服务图表面板

1 -显示组件服务如何通信的应用程序的端到端网络图

2 — 指示特定时间持续时间内命中和错误的图形

3 — 搜索栏搜索服务

4 — 选择时间持续时间的时间列表

5 -将筛选器应用于显示服务

6 — 设置图标

7 — 放大和缩小视图

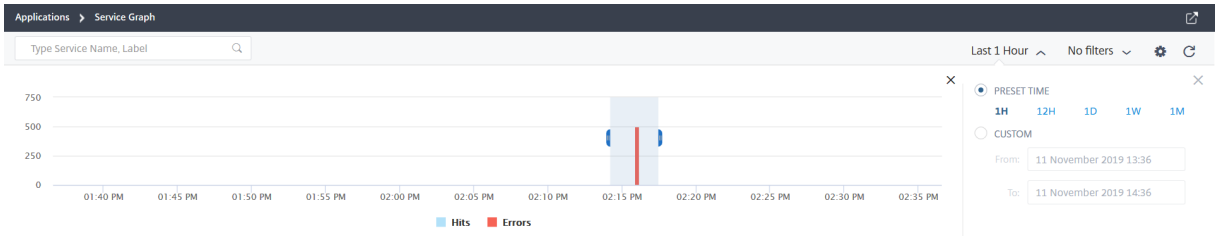
8 — 图表视图或表格视图

根据选定的时间持续时间，您可以查看服务图表。

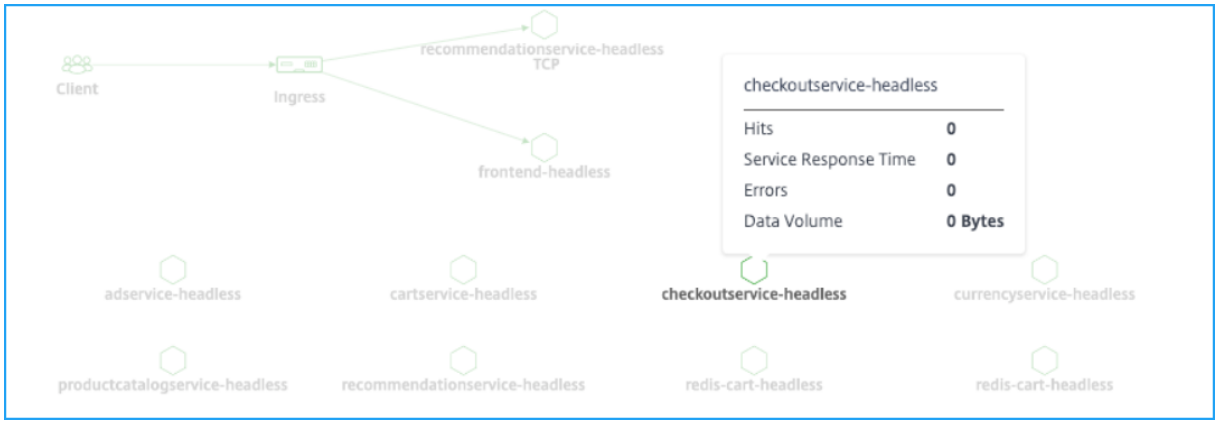
服务图标	说明
	边宽表示点击次数。边缘宽度越大，表示点击次数越高。
	带警告图标的服务表示服务存在错误。
	带秒表图标的服务表示该服务存在延迟或响应时间问题。
	具有秒表和警告图标的服务表明该服务同时存在错误和延迟/响应时间问题。

> 注意
>
> 如果服务没有警告或秒表图标，则表示服务存在“点击”的异常或阈值违反。

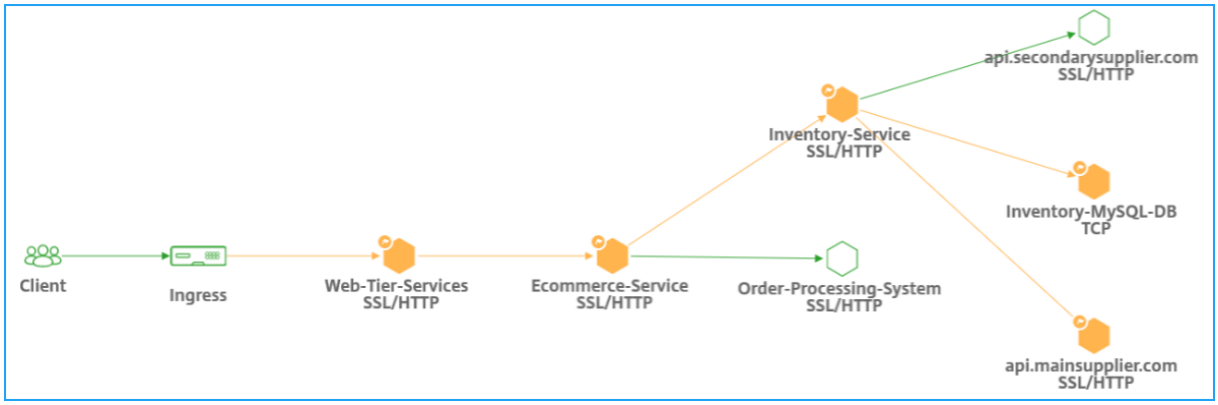
根据选定的时间持续时间，您可以查看服务图表。从图表中选择指示点击的时间段，以便进一步向下钻取以获取更多信息。



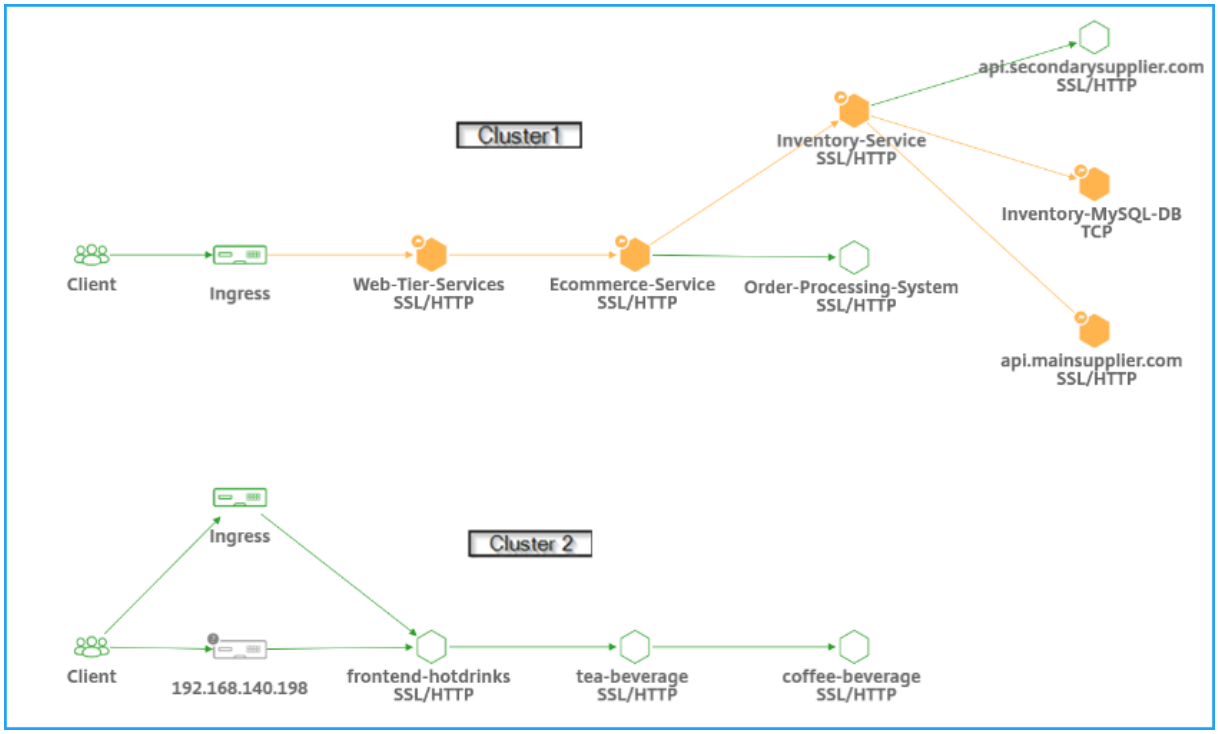
> 注意
>
> 如果 Citrix ADM 未收到活动事务，则只能查看由 Citrix ADC 实例进行负载平衡的服务。将鼠标指针悬停在服务上时，所有指标都显示为 0。



此时将显示服务图以及服务使用的协议。请考虑您的 Kubernetes 群集中运行以下服务，如图所示：



> 注意
>
> 如果您在编排 > **Kubernetes** > 群集中添加了多个群集，则可以查看与每个群集关联的服务。



您可以查看服务的以下状态：

- 严重（红色） -指示平均服务响应时间 > 200 毫秒，错误计数 > 0
- 查看（橙色） -指示平均服务响应时间 > 200 毫秒或错误计数 > 0 的时间
- 良好（绿色） -表示无错误，平均服务响应时间小于 200 ms

以下是使您能够识别服务使用的协议的协议：

- **TCP** — 表示服务正在使用 TCP 协议。
- **SSL**、**HTTP** — 表示服务正在使用通过 HTTP 协议的 SSL。
- **SSL**、**TCP** — 表示服务正在使用基于 TCP 的 SSL 协议。

> 注意
>
> 没有协议的服务表示服务正在使用 HTTP 协议。

使用表格视图查看关键指标趋势

使用表格视图，您可以看到：

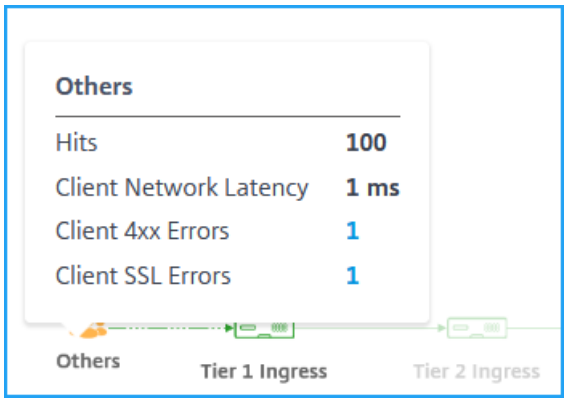
- 该服务的关键指标
- 源服务到目标服务之间的关键指标

作为管理员，使用这些关键指标，您可以分析所选时间持续时间内黄金信号的趋势。

查看客户端度量

您可以查看客户端从哪个位置访问该服务。作为管理员，您可以直观显示客户端指标并分析客户端发生的问题。

将鼠标指针悬停在客户端区域上以查看指标。



- 点击量 -表示客户端收到的总点击量。
- 客户端网络延迟 -表示平均客户端网络延迟。
- 客户端 **4xx** 错误 -表示客户端 4xx 错误总数。
- 客户端 **SSL** 错误 -表示客户端 SSL 错误总数。

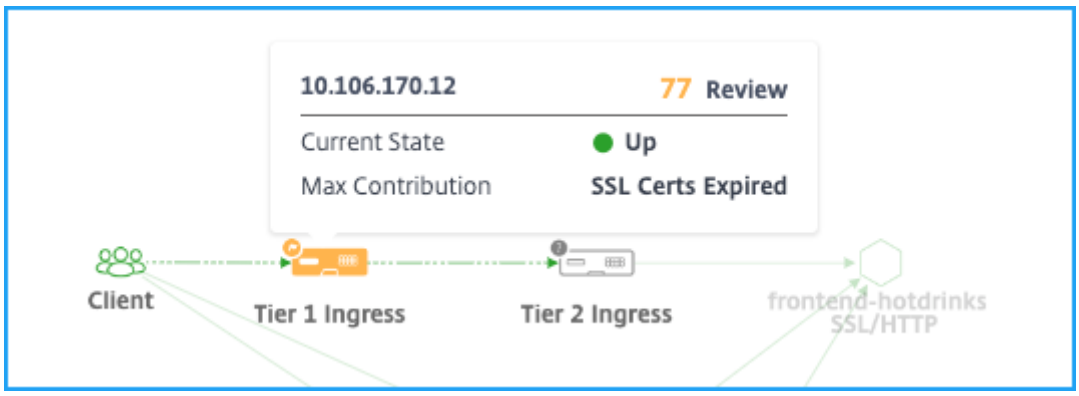
Citrix ADM 中的 **IP** 块 -如果客户端使用公有 IP 地址，Citrix ADM 可以识别客户端位置。Citrix ADM 具有其内置位置 CSV 文件，该文件与基于客户端 IP 地址范围的位置匹配。

只有将 IP 地址添加到 Citrix ADM 服务器时，Citrix ADM 才能识别具有私有 IP 地址的客户端位置。例如，如果客户端 IP 地址位于与城市 A 关联的私有 IP 地址范围内，Citrix ADM 会识别此客户端的流量来自城市 A。

有关详细信息，请参阅创建私有 IP 块。

查看入口量度

您可以查看 Kubernetes 集群中使用的入口类型。



- Citrix ADC IP 地址及其分数
- 当前状态 — 指示 Citrix ADC 实例是启动、关闭还是不在状态
- 最大贡献 — 指示影响实例分数的问题

对于单层拓扑，您只能查看单个 **Ingress**。

单击 **Ingress** 可进一步向下钻取详细信息。有关详细信息，请参阅查看入口详细信息以解决问题。

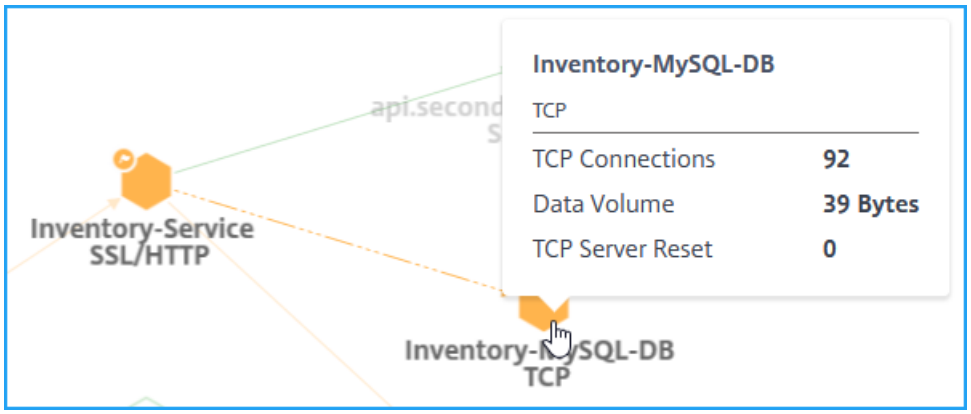
查看 **TCP** 和 **SSL** 指标

使用 TCP 和 SSL 度量，您可以执行以下操作：

- 查看服务之间的 TCP 连接详细信息
- 确定 TCP 相关问题是来自源服务还是来自目标服务
- 查看 SSL 错误是来自源服务还是目标服务
- 查看 SSL 服务使用的 SSL 协议版本

TCP 指标

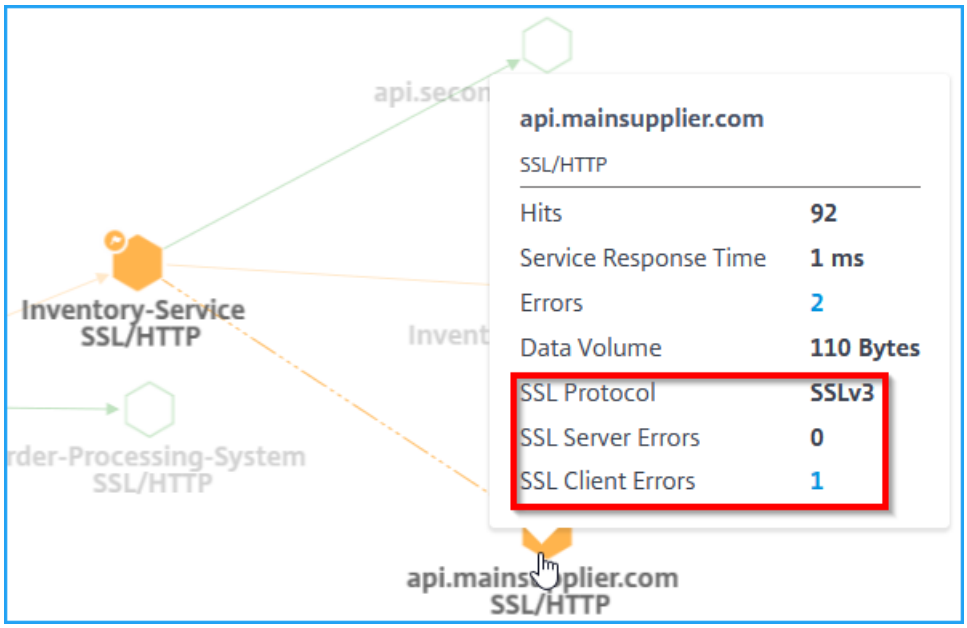
将鼠标指针悬停在 TCP 服务或其关联的传入服务上，以查看 TCP 指标。



- **TCP** 连接 — 服务之间建立的总连接
- 数据量 — 服务处理的总数据
- **TCP** 服务器重置 — 从服务器启动的 TCP 重置总数

SSL 指标

将鼠标指针悬停在使用 SSL 协议查看 SSL 度量的服务上。



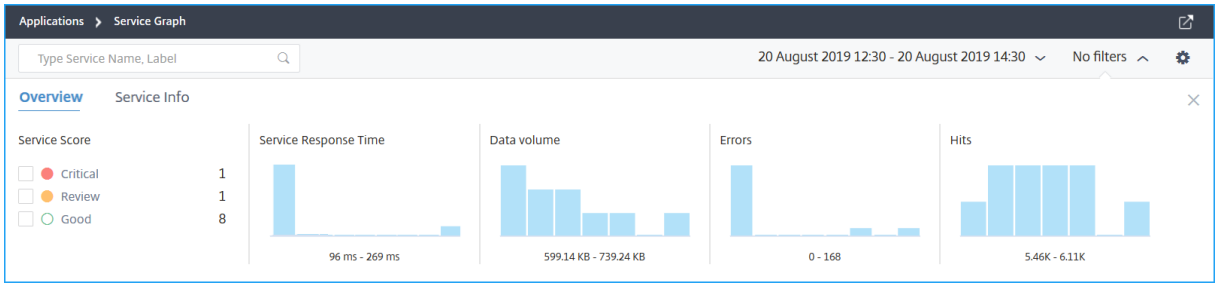
- **SSL** 服务器错误 — 指示来自服务器的 SSL 错误总数。（例如，SSL 证书未知）
- **SSL** 协议 — 指示服务使用的 SSL 协议版本
- **SSL** 客户端错误 -指明来自客户端的 SSL 错误总数。（例如，SSL 客户端身份验证错误）

查看服务详细信息

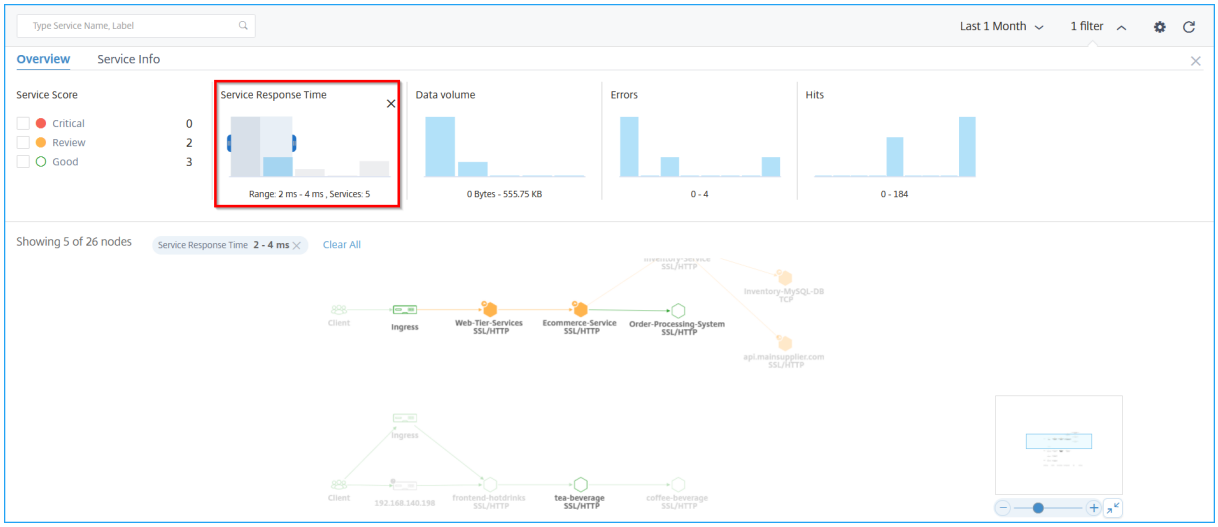
单击服务，然后选择 查看详细信息以查看服务详细信息。有关详细信息，请参阅查看服务详细信息。

应用筛选器

您可以应用筛选器来查看特定服务信息。单击 无筛选器” 列表以获取筛选器选项。

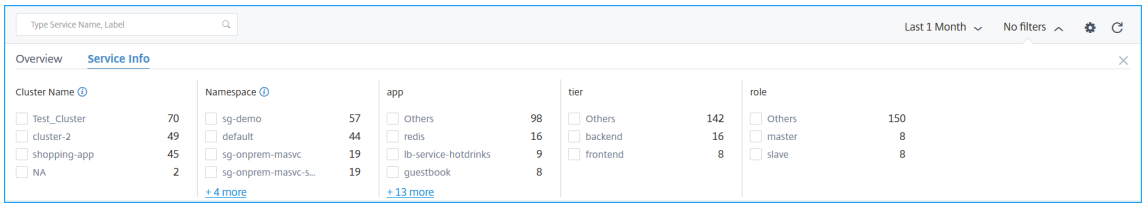


例如，如果要查看延迟小于 150 毫秒的服务，请单击 服务响应时间下的条形图以显示结果。



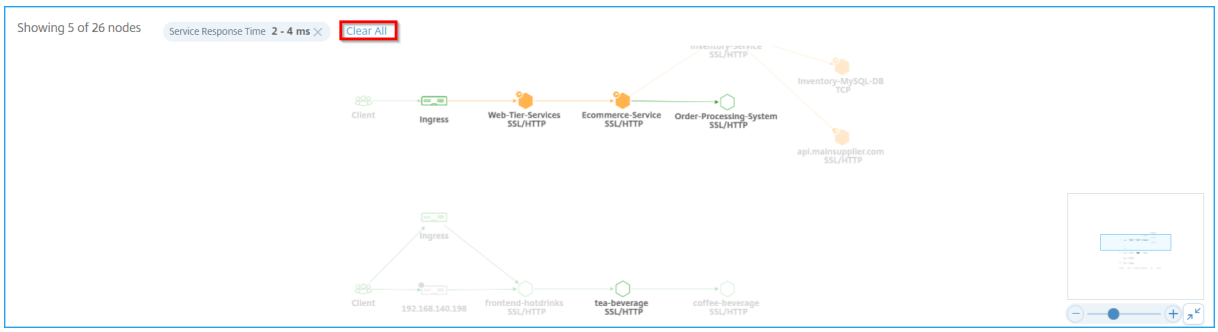
单击“ 服务信息”以选择并应用以下筛选器：

- 群集 — 显示适用于所选集群的所有服务。
- 命名空间 — 显示适用于所选命名空间的所有服务。

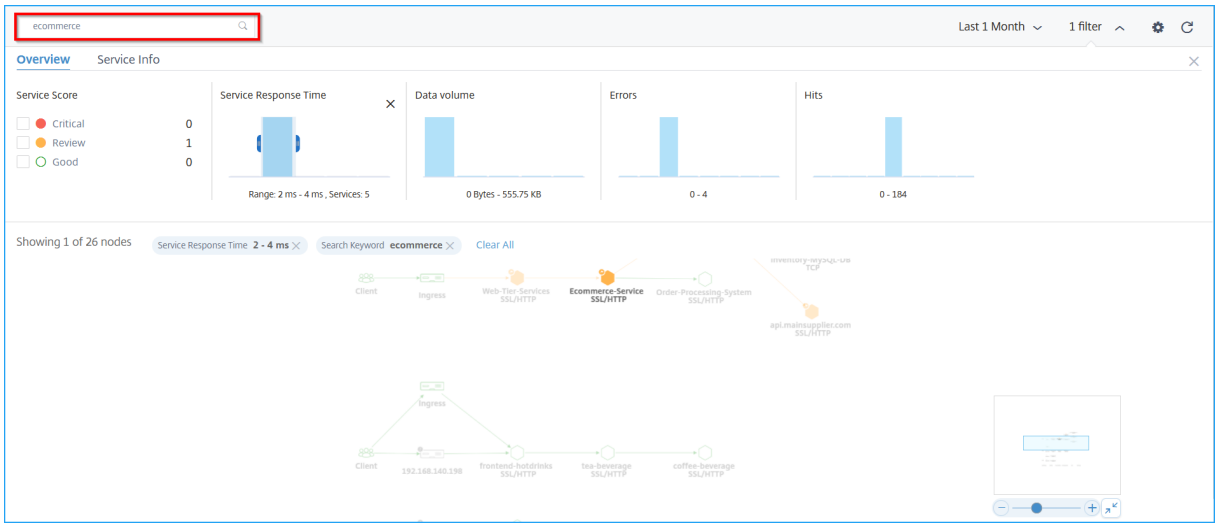


> 注意
>
> 根据 Kubernetes 服务定义 YAML 中为服务配置的标签，您还可以查看更多过滤器选项。

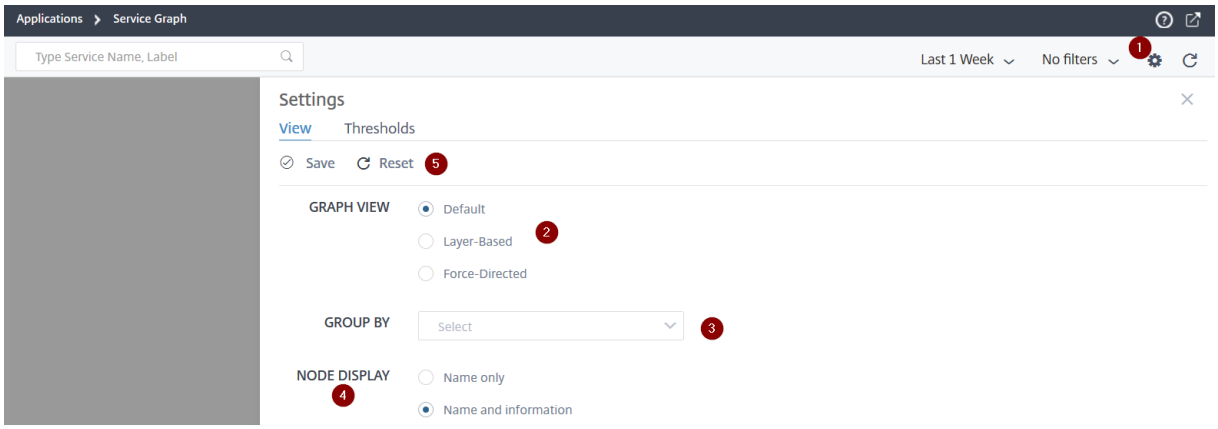
单击 全部清除以清除所有筛选器。



或者，也可以使用搜索文本框并键入服务名称，以在服务图表上显示结果。



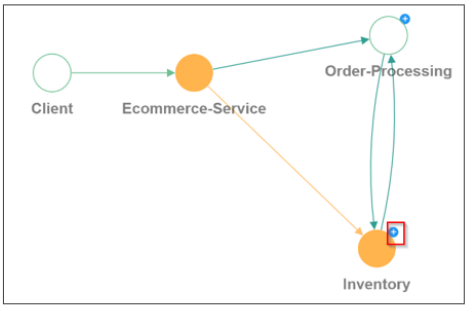
使用设置选项



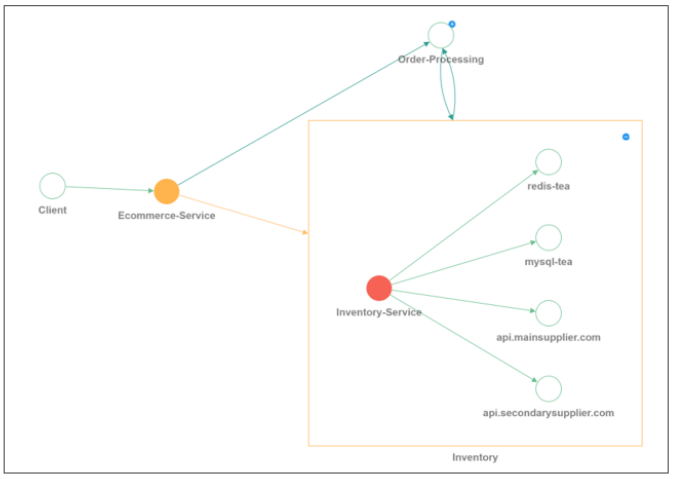
1 — 设置图标

2 — 将服务图显示为默认视图、基于图层视图或强制定向视图的选项

3 — 从列表中选择选项以查看基于类别的服务。从列表中选择一个类别后，单击图表上的 **+** 以查看所有服务



Collapsed view



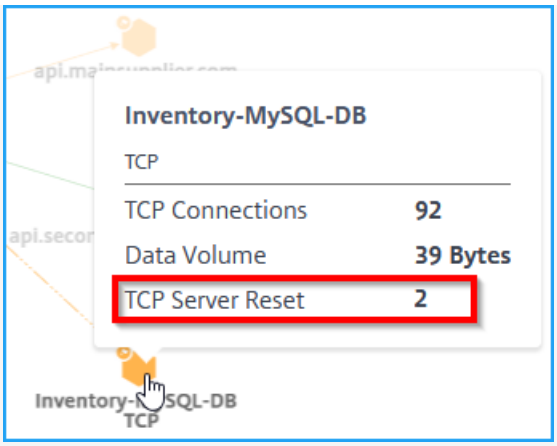
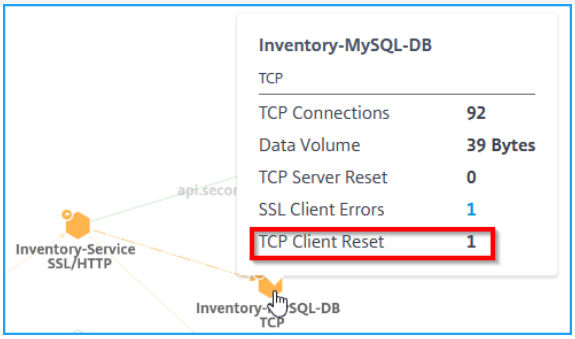
Expanded view

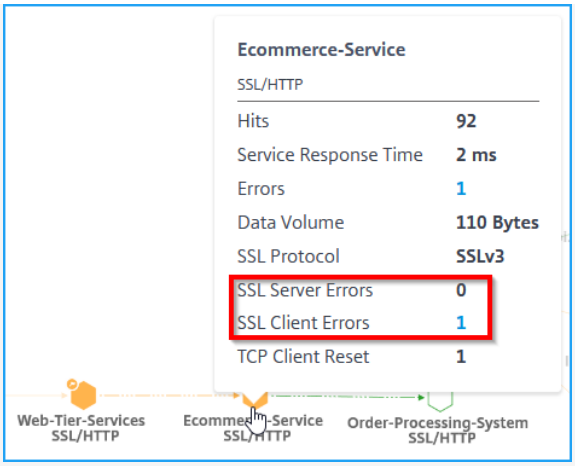
4 — 使您可以选择要如何显示服务的选项。

5 -用于保存设置或重置为默认设置的选项。

分析错误

将鼠标指针悬停在指示错误的服务上。

错误	说明
	**TCP** 服务器重置指示从服务器启动的总 TCP 重置。
	**TCP** 客户端重置指示客户端启动的总 TCP 重置。

错误	说明
	SSL 客户端错误指示来自客户端的 SSL 错误总数。（例如，SSL 客户端身份验证错误）。
	SSL 服务器错误指示来自服务器的 SSL 错误总数。（例如，SSL 证书未知）

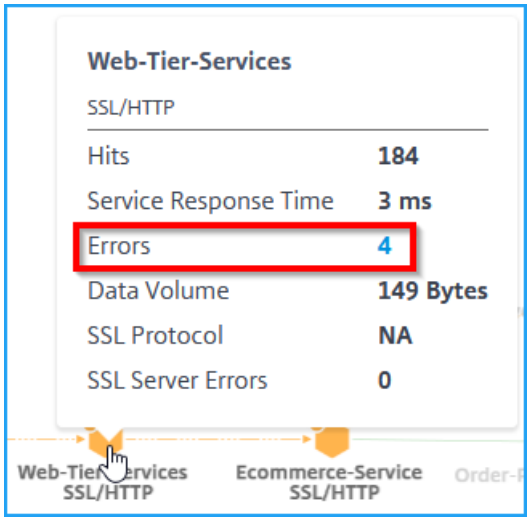
注意

- 如果客户端错误计数为 **1** 或更高，则任何服务中都会显示客户端错误计数（不考虑协议类型）。
- 显示的任何服务的客户端错误计数表明错误来自客户端。

查看 **HTTP** 事务详细信息

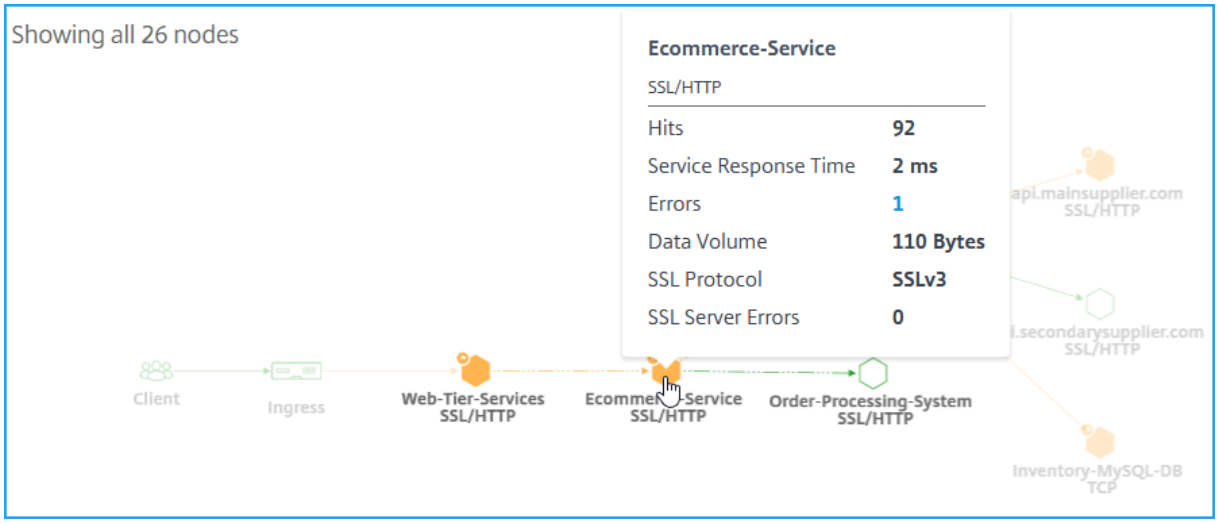
注意

您可以通过将鼠标指针悬停在错误服务上，然后单击问题计数来查看错误。

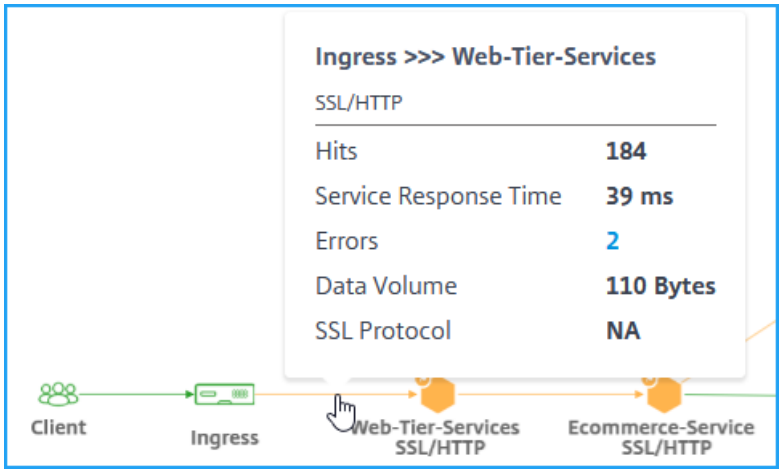


根据图像中显示的示例，您可以查看应用程序的端到端网络图，其中显示组件服务的通信方式。

当您将鼠标指针悬停在 电子商务服务上时，您可以查看 电子商务服务的指标详细信息。



Citrix ADM 还允许您查看入口和服务之间的事务详细信息。悬停鼠标指针可查看入口和服务之间的详细信息，如总错误、平均服务响应时间等。



命中 — 指示服务接收的命中总数。

服务响应时间 — 指示从服务响应时间到第一个字节 (TTFB) 所花费的平均响应时间。

错误 — 表示总错误，如 4xx、5xx 等。

数据量 — 指示服务处理的数据总量。

SSL 协议 — 表示 SSL 协议版本。

单击 **Ingress** 和 服务之间的箭头以查看详细的交易记录。

有关详细信息，请参阅查看 Web 事务的分析。

在服务图中配置阈值

April 23, 2021

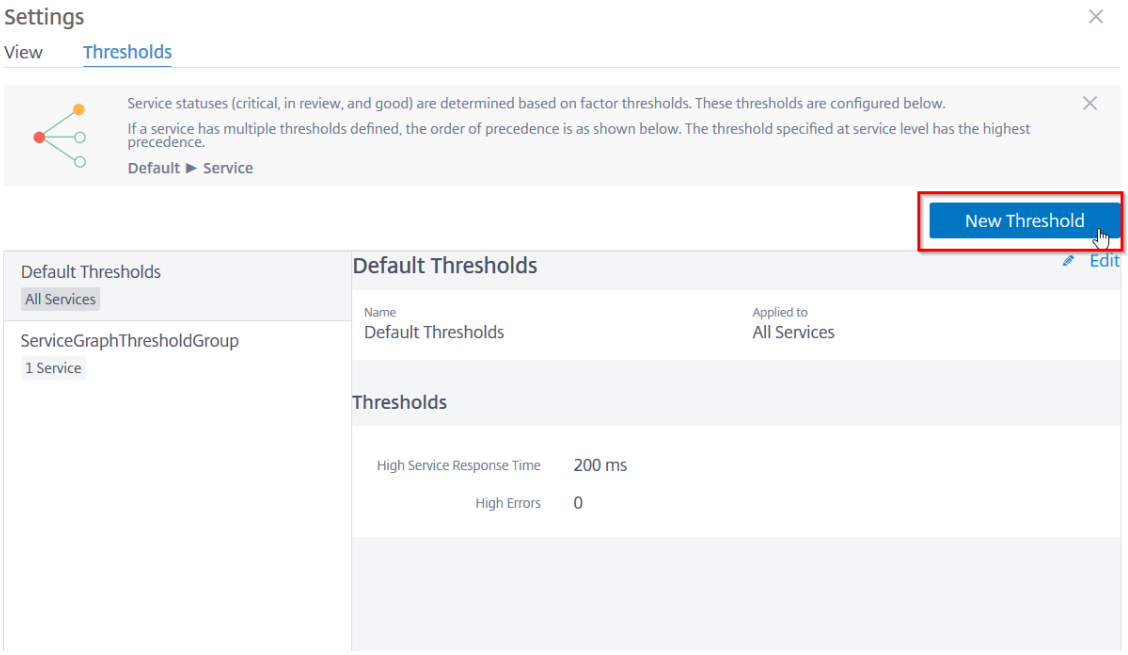
作为管理员，您可以为 Kubernetes 服务配置阈值。Citrix ADM 根据服务响应时间和错误计数显示服务状态（“严重”、“审查”和“良好”）。默认情况下，您可以查看应用于所有服务的 默认阈值（服务响应时间 = 200 毫秒，错误计数 = 0）。

> 注意
>
> 您不能删除默认阈值。

要配置新阈值，请执行以下操作：

在服务图中：

1. 单击设置图标并选择 阈值选项卡。
2. 单击 新阈值可配置新阈值。

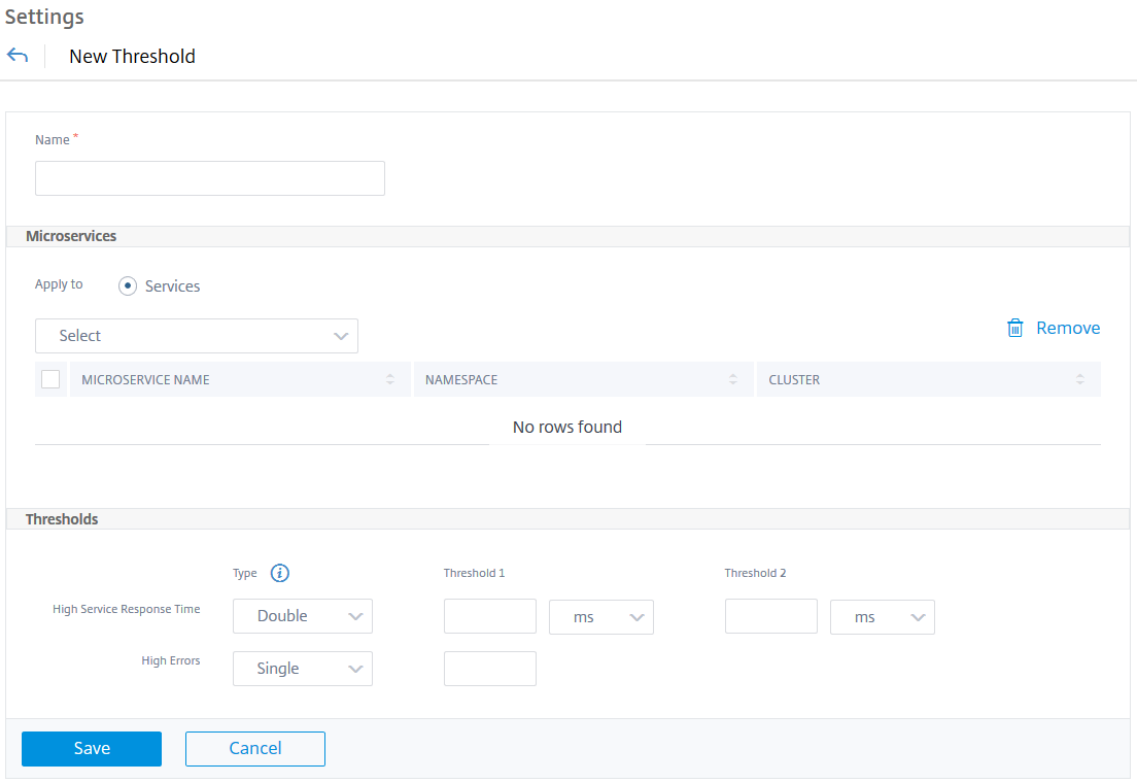


此时将显示“ 新阈值”页。

3. 配置以下参数：
   a) 名称 — 指定阈值的名称。
   b) 在 微服务下，选择要应用阈值的服务
   c) 在 阈值下，为高响应时间和高误差选择 单或 双精度
   d) 指定阈值。

> 注意
>
> 如果选择双重阈值，请确保：
>
> - 阈值 1 小于阈值 2 值。例如，如果将阈值 1 配置为 250 毫秒，则阈值 2 必须为 251 毫秒或更高。
> - 阈值 1 不得与阈值 2 值相同。

4. 单击保存。



阈值已成功创建。您可以在“阈值”页中查看 阈值详细信息。

单一阈值

配置单个阈值时，Citrix ADM：

- 将当前值与配置的阈值进行比较
- 根据超出的阈值计算总罚款
- 根据罚金计算显示服务得分和服务状态

双阈值

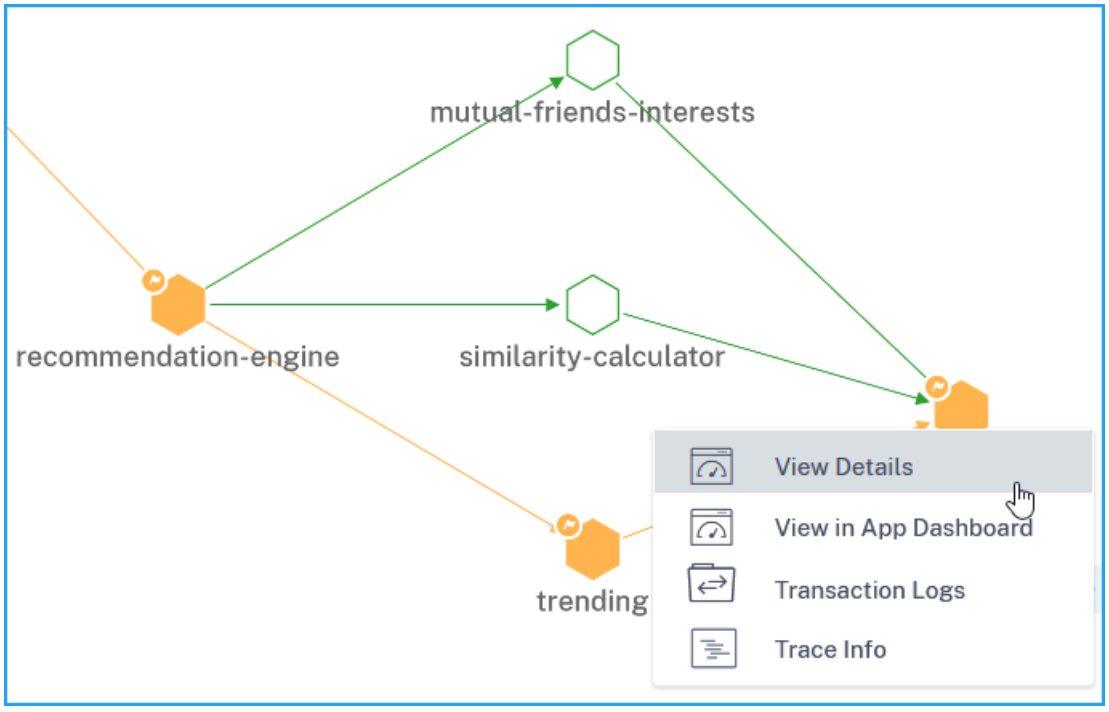
配置双重阈值时，Citrix ADM：

- 将当前值与配置的阈值进行比较
- 检查当前值是否为：
  - 低于阈值 1
  - 在阈值 1 和阈值 2 之间
  - 大于阈值 2
- 根据超出的阈值计算总罚款
- 根据罚金计算显示服务得分和服务状态

查看服务详细信息

April 23, 2021

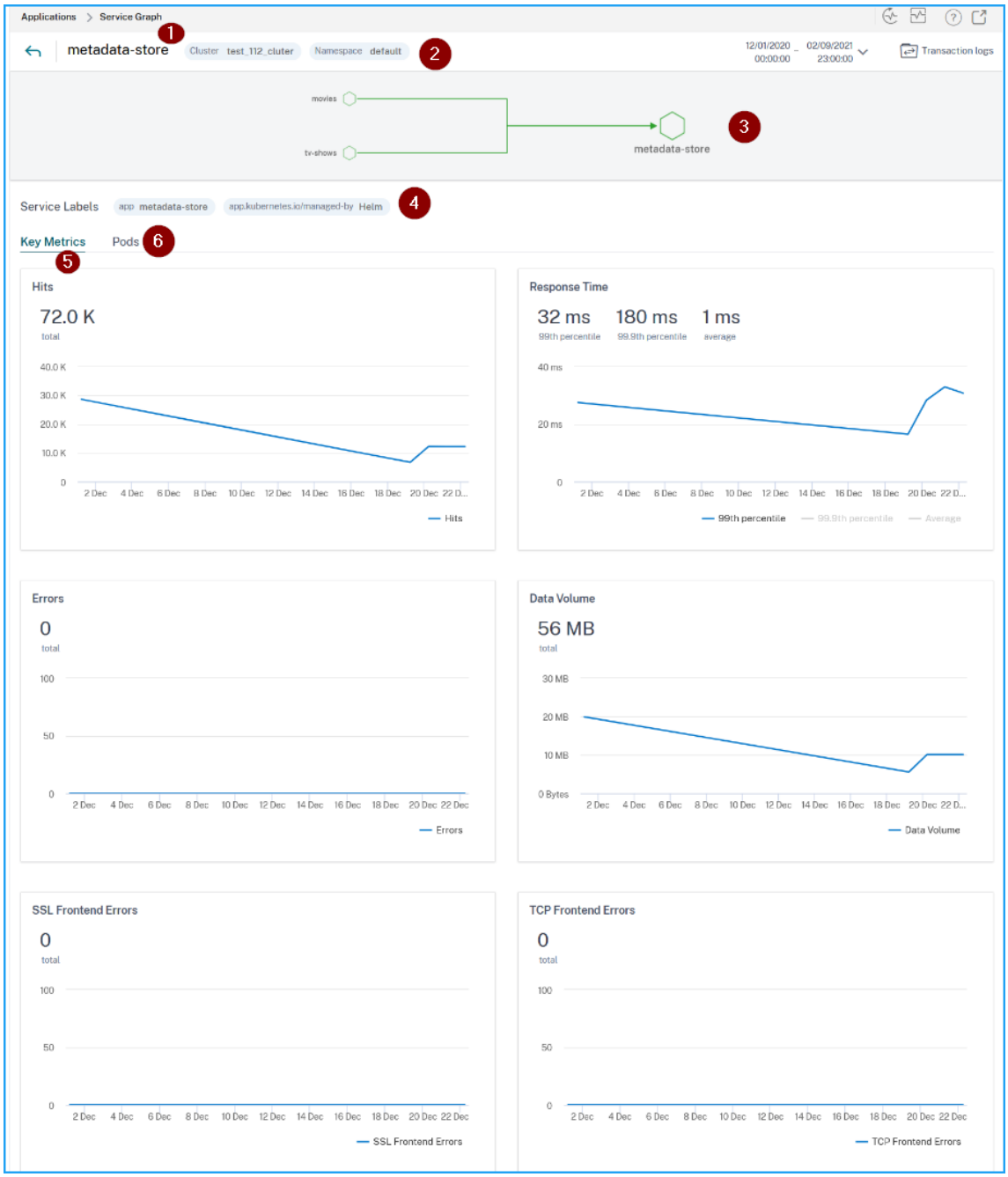
单击服务，然后选择 查看详细信息。



使用服务详细信息页面，您可以查看：

- 托管服务的群集名称 (1)
- 服务的命名空间和服务标签 (2) (4)

- 与选定服务连接的所有相关的传入和传出服务 (3)
- 以图表格式提供服务关键指标，例如点击、响应时间、错误、数据量、SSL 前端错误和 TCP 前端错误 (5)。
- 与服务关联的后端 Pod (6)。



使用这些关键指标趋势，您可以分析服务在特定时间持续时间内的执行情况。

“ 响应时间”指标使您能够查看：

- **99** 百分位数 — 表示选定持续时间内 99%的请求不到 32 毫秒（根据示例图像）。

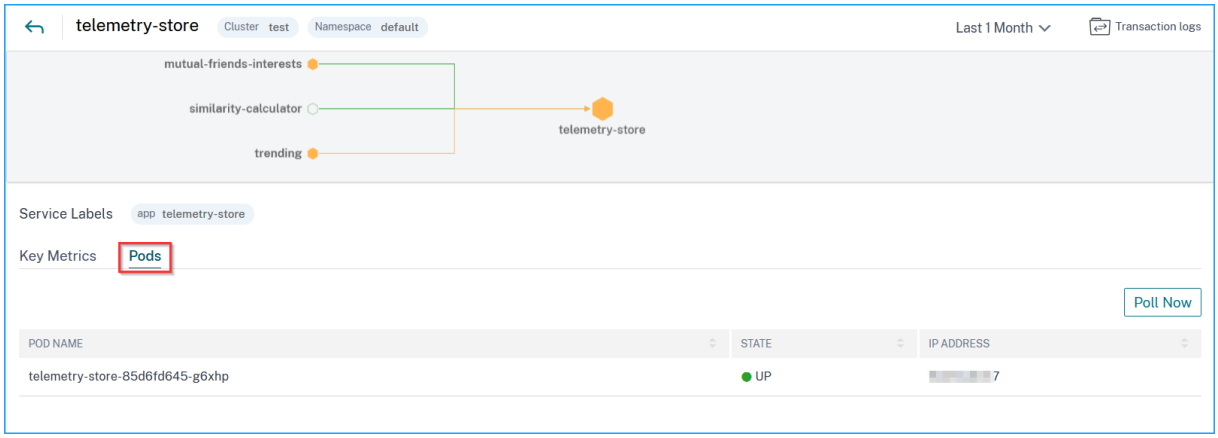
- 平均值 — 表示服务的平均响应时间
- **99.9**% -表示来自服务的最长响应时间

指标详情

指标	说明
访问量	服务收到的请求总数
错误	来自服务的 HTTP 错误总数
服务响应时间	从服务响应时间到第一个字节 (TTFB) 所用的平均响应时间。
数据量	服务处理的总数据量
SSL 前端错误	来自该服务的 SSL 前端错误总数。例如：SSL 客户端失败
SSL 后端错误	来自该服务的 SSL 后端错误总数。例如：SSL 客户端错误
TCP 后端错误	来自该服务的 TCP 后端错误总数。例如：TCP 服务器重置
TCP 前端错误	来自该服务的 TCP 前端错误总数。例如：TCP 客户端重置

查看后端 **pod** 详细信息

单击 **Pod** 选项卡以查看与服务关联的后端 Pod。

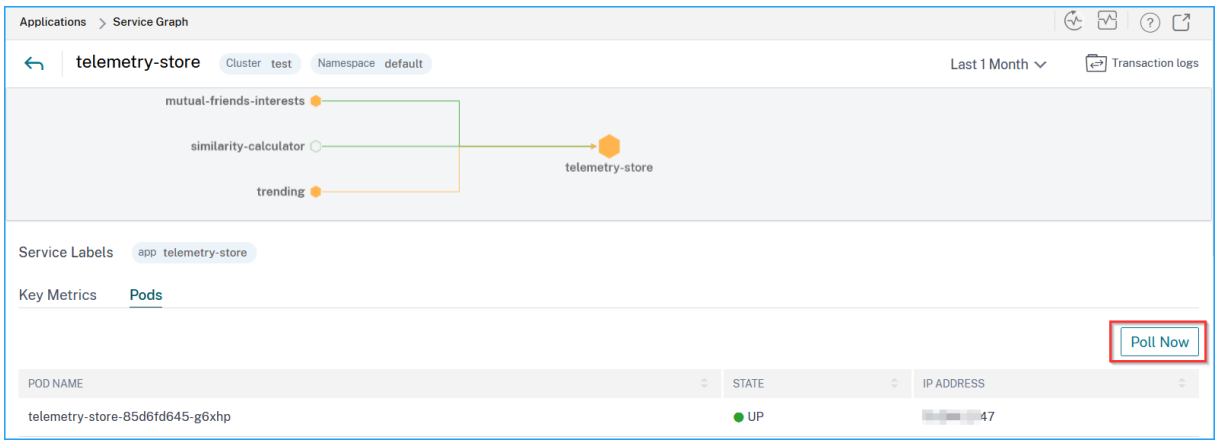


- **Pod** 名称 — 表示 pod 名称
- 状态 — 表示 Pod 是在运行（启动）还是未运行（关闭）。

- **IP** 地址 — 表示 pod 的 IP 地址

使用 **“立即轮询”** 选项获取 **Pod** 状态

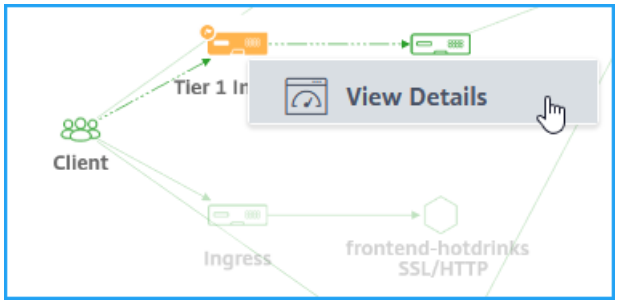
立即轮询选项可从集群中获取最新的 Pod 状态。



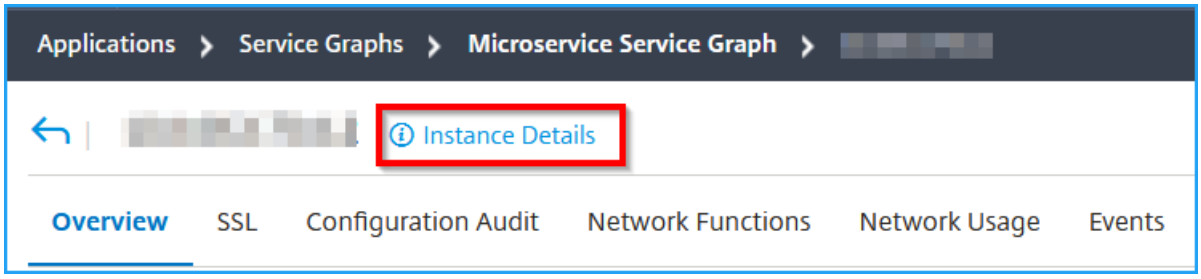
查看入口详细信息以解决问题

April 23, 2021

在服务图中，单击入口并选择 查看详细信息以可视化为 Kubernetes 集群配置的 Citrix ADC 实例的详细信息。



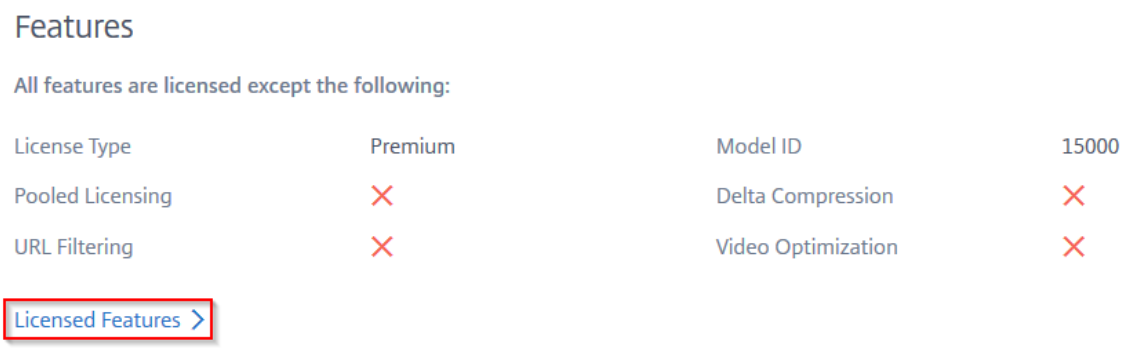
单击 “ 实例详细信息” 以查看详细信息。



将显示以下详细信息：

- 信息 -实例详细信息，例如实例类型、部署类型、版本、型号等。

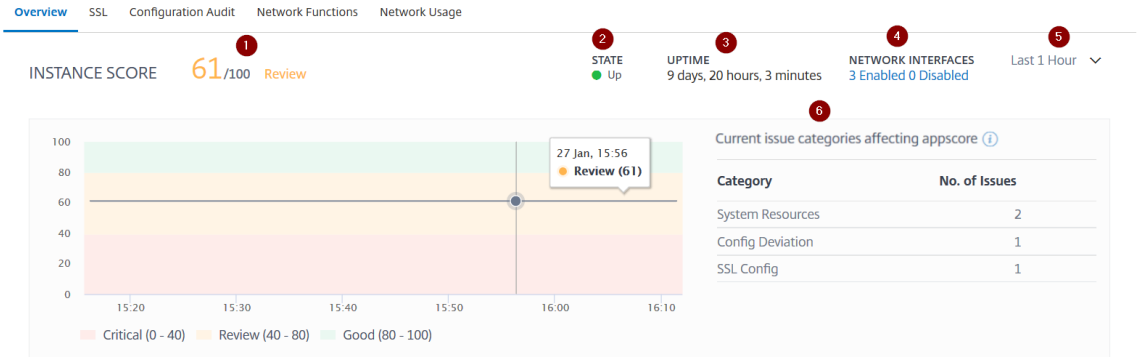
- 功能 — 默认情况下，显示未获许可的功能。单击 “ 许可功能” 以查看已许可的功能。



- 模式 — 默认情况下，将显示在实例上禁用的所有模式。单击 查看启用模式可查看实例上已启用的模式。

实例仪表板显示实例概述，您可以在其中查看以下详细信息：

- 实例分数

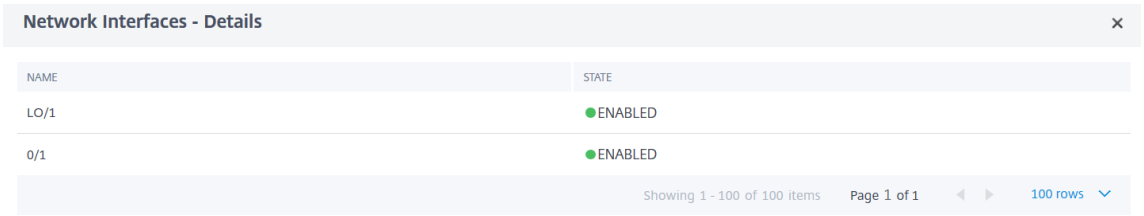


1 — 表示所选时间持续时间内的当前 Citrix ADC 实例得分。最终得分计算为 **100** 减去总处罚。图形显示选定时间持续时间的分数范围。

2 — 表示 Citrix ADC 实例的当前状态，例如启动、关闭和不服务。

3 — 表示 Citrix ADC 实例启动并运行的持续时间。

4 — 表示为实例启用和禁用的网络接口总数。单击查看详细信息，如网络接口名称和状态（已启用或已禁用）。



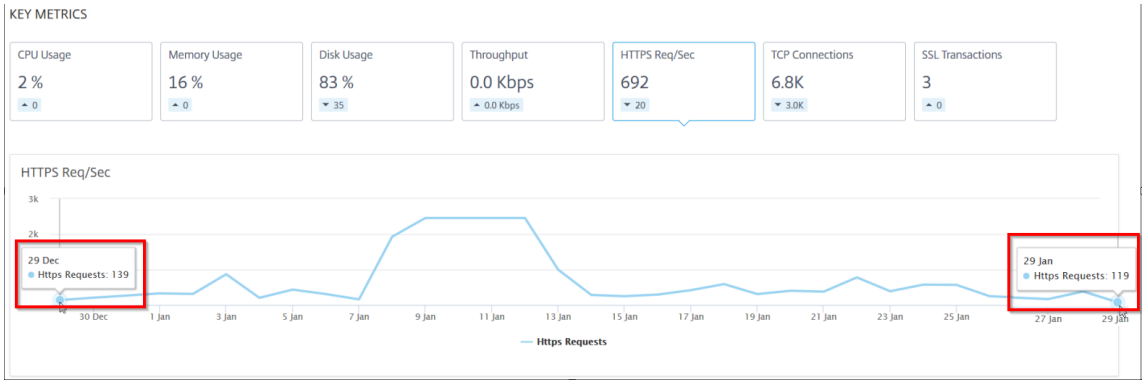
5 — 从列表中选择时间持续时间以查看实例详细信息。

6 — 显示 ADC 实例的总问题和问题类别。

- 关键指标

  单击每个选项卡以查看详细信息。在每个指标中，您可以查看所选时间的平均值和差值。

  下图是 HTTPS Req/Sec 的示例，选定的持续时间为过去 1 个月。值 **692** 是过去 1 个月持续时间的平均 HTTPS Req/秒，值 **20** 是差值。在图形中，第一个值为 **139** ，最后一个值为 **119**。差值为 **139-119 = 20**。



  您可以在所选时间持续时间内以图形格式查看以下实例指标：

  - **CPU** 使用率 — 在所选持续时间内实例的平均 CPU%（对于数据包 CPU 和管理 CPU 都显示）。
  - 内存使用率 — 在选定持续时间内实例的平均内存使用率%。
  - 磁盘使用率 — 选定持续时间内实例的平均磁盘空间%。
  - 吞吐量 — 实例在所选持续时间内处理的平均网络吞吐量。
  - **HTTPS** 请求/秒 — 实例在所选持续时间内收到的平均 HTTPS 请求。
  - **TCP** 连接 — 客户端和服务器在所选持续时间内建立的平均 TCP 连接。
  - **SSL** 事务 — 实例在所选持续时间内处理的平均 SSL 事务。

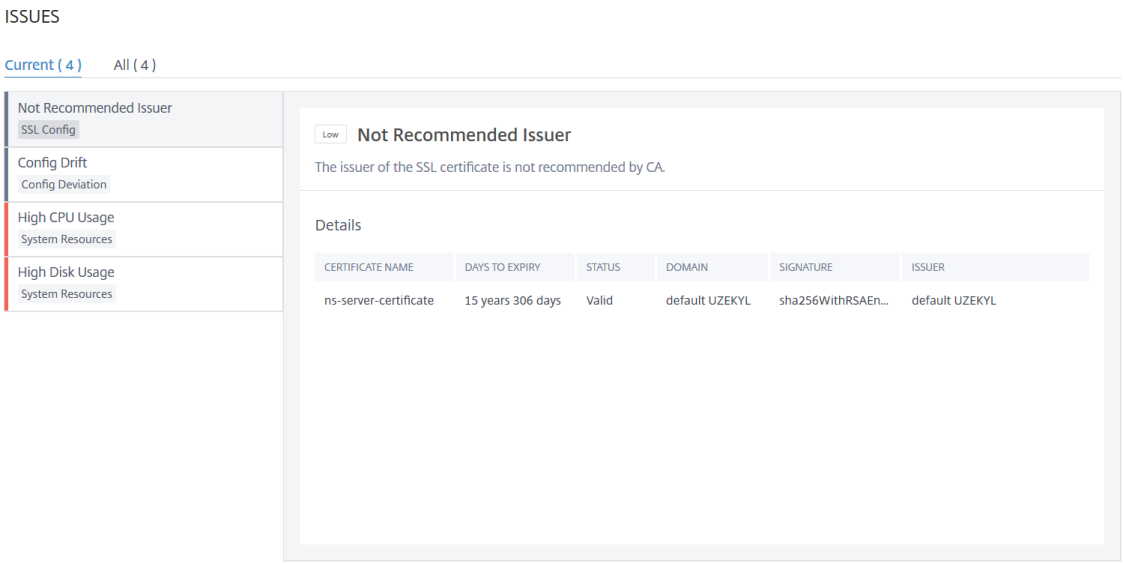
- 问题

  您可以查看 Citrix ADC 实例中出现的以下问题：

问题类别	说明	问题
系统资源	显示与 Citrix ADC 系统资源相关的所有问题，例如 CPU、内存、磁盘使用情况等。	- 高 CPU 使用率
		- 高内存使用率
		- 高磁盘使用率
		- SSL 卡故障
		- 电源故障
		- 磁盘错误

问题类别	说明	问题
		- 闪光错误
		- 网卡丢弃
SSL 配置	显示与 Citrix ADC 实例上的 SSL 配置相关的所有问题。	-SSL 证书已过期
		- 不推荐发行人
		- 不推荐算法
		- 不推荐密钥强度
配置偏差	显示与 Citrix ADC 实例中应用的配置作业相关的所有问题。	-配置漂移
		- 运行与模板
容量问题	显示 ADC 容量问题。ADM 每五分钟从 ADC 实例轮询一次这些事件，并显示数据包丢失或速率限制计数器增量（如果存在）。这些问题根据以下容量参数进行分类。	- 已达到吞吐量限制
		- 已达到 PE CPU 限制
		- 已达到 PPS 限制
		- SSL 吞吐率限制
		- SSL TPS 费率限制
网络连接	显示实例中出现的操作问题。	有关详细信息，请参阅使用新指标增强的基础架构分析。

单击每个选项卡以分析问题并进行故障排除。例如，假设某个实例在所选时间持续时间内存在以下错误：



- 当前选项卡显示影响实例分数的当前 ADC 操作问题。
- “ 全部” 选项卡显示在选定持续时间内检测到的所有问题。

分布式跟踪

April 23, 2021

在服务图中，可以使用分布式跟踪视图来执行以下操作：

- 分析整体服务性能。
- 可视化选定服务与其相互依赖服务之间的通信流。
- 确定哪些服务指示错误并排除错误服务的故障
- 查看所选服务及其每个相互依赖服务之间的交易详细信息。

必备条件

要查看服务的跟踪信息，您必须：

- 确保应用程序维护以下跟踪标头，同时发送任何东西流量：

- x-request-id
- x-b3-traceid
- x-b3-spanid
- x-b3-parentspanid
- x-b3-sampled
- x-b3-flags
- x-ot-span-context

- 对于 **1.7.23** 之前的 **CIC** 内部版本，请使用 `NS_DISTRIBUTED_TRACING` 和值 `yes` 更新 CPX YAML 文件

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: cpx-ingress
spec:
  selector:
    matchLabels:
      app: cpx-ingress
  replicas: 1
  template:
    metadata:
      name: cpx-ingress
      labels:
        app: cpx-ingress
      annotations:
    spec:
      serviceAccountName: cpx-ingress-k8s-role
      containers:
        - name: cpx-ingress
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-47.103"
          securityContext:
             privileged: true
          env:
          - name: "EULA"
            value: "yes"
          - name: "KUBERNETES_TASK_ID"
            value: ""
          - name: "NS_MGMT_SERVER"
            value: "192.168.0.1"
          - name: "NS_MGMT_FINGER_PRINT"
            value: "12:12:AB:CD:EA:72:E3:10:47:CD:AF:AG:C3:B7:82:6O:97:3D:E2:5D"
          - name: "NS_HTTP_PORT"
            value: "9080"
          - name: "NS_HTTPS_PORT"
            value: 9443"
          - name: "LOGSTREAM_COLLECTOR_IP"
            value: "192.168.0.1"
          imagePullPolicy: Always
```

- 对于 **1.7.23** 之后的 **CIC** 内部版本，您必须使用 ConfigMap。

  ConfigMaps 允许您将配置与 Pod 分开，并使工作负载可移植。使用 ConfigMaps，您可以轻松更改和管理工作负载配置，并减少将配置数据硬编码到 pod 规范的需要。

  借助 ConfigMap 支持，您可以在保持 Citrix 入口控制器容器运行的同时自动更新配置。更新后不需要重新启动 Pod。有关详细信息，请参阅ConfigMap 对入口控制器的支持。

  使用 ConfigMap，您可以启用或禁用分布式跟踪、事件、审核日志等。要使用 ConfigMap：

  1. 使用所需的参数创建 YAML 文件。

     以下示例 YAML 文件已启用分布式跟踪并禁用审计日志、事件和事务等其他变量：


```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'false'
      events:
        enable: 'false'
    transactions:
      enable: 'false'
      port: 5557
<!--NeedCopy-->
```

> 注意
>
> 您可以为 Samplingrate 提供介于 0 到 100 之间的值。Citrix ADM 显示提到的跟踪事务数量。

2. 使用以下命令部署 ConfigMap：

```
kubectl create -f <configmap-yaml>.yaml
```

3. 编辑 CPX YAML 文件并使用 envFrom 或 args 以指定以下参数：

```
envFrom:
 - configMapRef:
     name: cic-configmap
<!--NeedCopy-->
```

或


```
args:
   - --configmap
     default/cic-configmap
```

4. 如果要更改任何变量的值，请在 ConfigMap 中编辑这些值。在此示例中，所有其他变量都从 **false** 更改为 **true**。

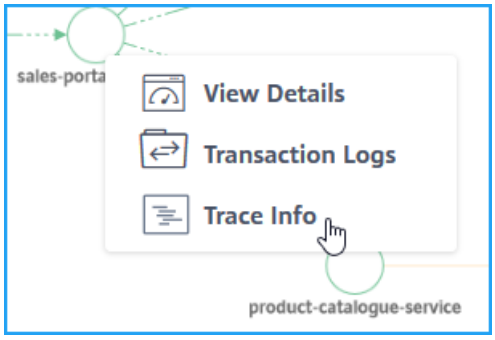
```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cic-configmap
  namespace: default
data:
  LOGLEVEL: 'debug'
  NS_PROTOCOL: 'http'
  NS_PORT: '80'
  NS_HTTP2_SERVER_SIDE: 'ON'
  NS_ANALYTICS_CONFIG:
    distributed_tracing:
      enable: 'true'
      samplingrate: 100
    endpoint:
      server: <ADM-AgentIP> / <ADM-AppserverIP>
    timeseries:
      port: 5563
      metrics:
        enable: 'true'
        mode: 'avro'
      auditlogs:
        enable: 'true'
      events:
        enable: 'true'
    transactions:
      enable: 'true'
      port: 5557
  <!--NeedCopy-->
```

5. 使用以下命令重新应用 ConfigMap：

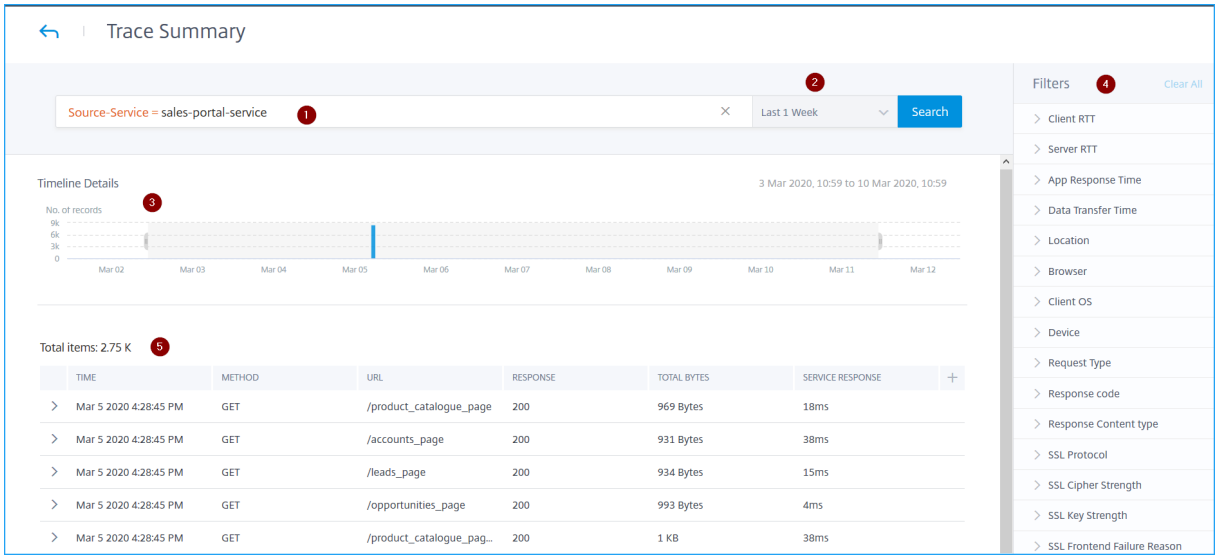
```
kubectl apply -f <yaml-file>.yaml
```

查看服务跟踪详细信息

在服务图表中，单击服务，然后选择 跟踪信息。



此时将显示所选服务的“跟踪摘要”页。



跟踪汇总显示：

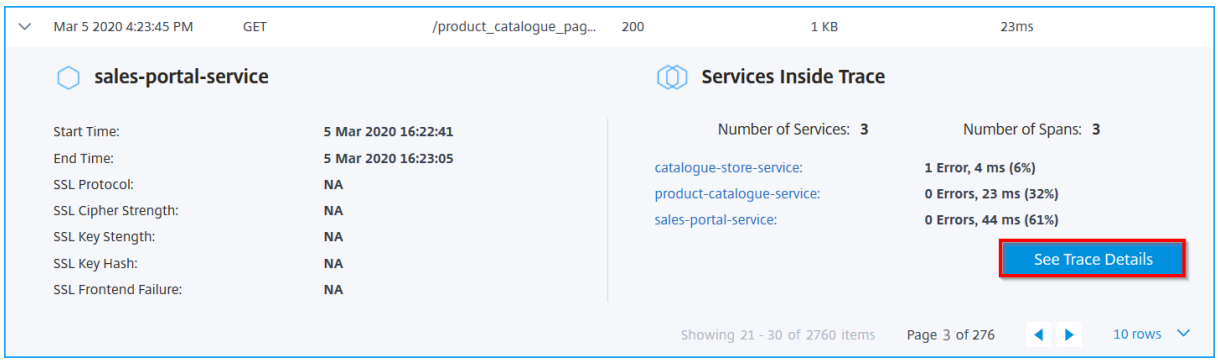
- 一种高级搜索，使您能够通过搜索包含建议和运算符的事务 (1)。有关详细信息，请参阅高级搜索。
- 使您可以选择时间持续时间（如 1 小时、12 小时、1 天、1 周、1 个月和自定义时间 (2)）的时间持续时间列表。
- 使用“时间轴详细信息”图形，您可以拖动并选择以显示特定时间持续时间 (3) 的结果。
- “筛选器”面板，您可以从每个指标中选择选项 (4)。
- 所选服务的交易详细信息 (5)。

查看交易详情

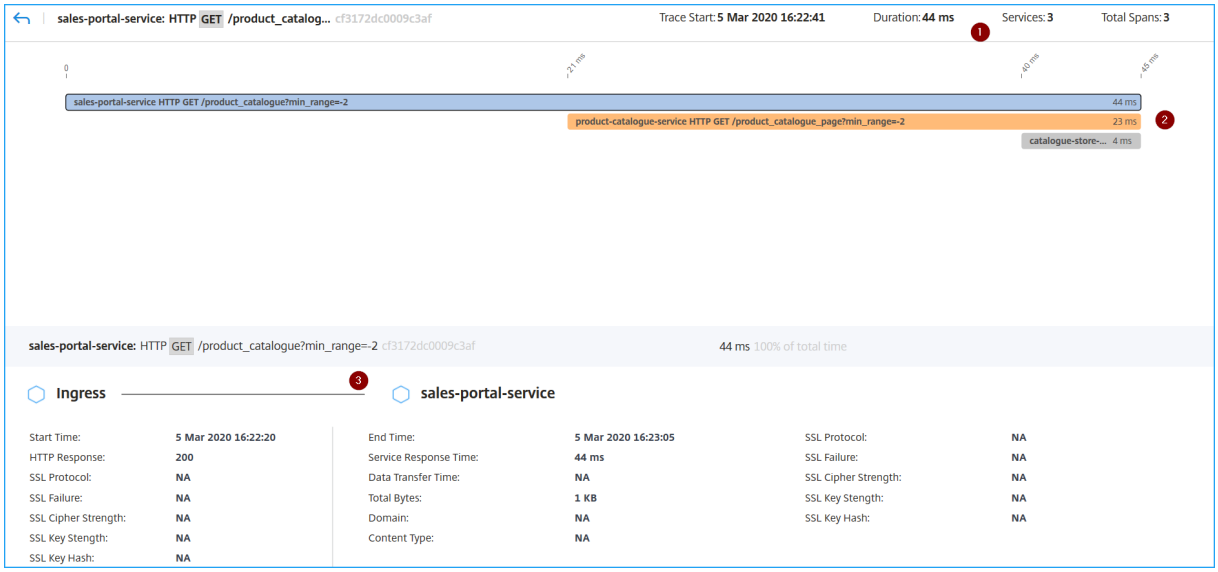
单击交易记录可向下钻取以获取详细信息。您可以查看所选服务的交易详细信息，例如：

- 开始时间
- 结束时间
- SSL 指标
- 与相互依赖的服务进行通信（以及每个服务的错误和响应时间）。

以下示例指示来自的错误 `catalogue-store-service`。单击 查看跟踪详细信息了解更多详细信息。



此时将显示“跟踪详细信息”页。

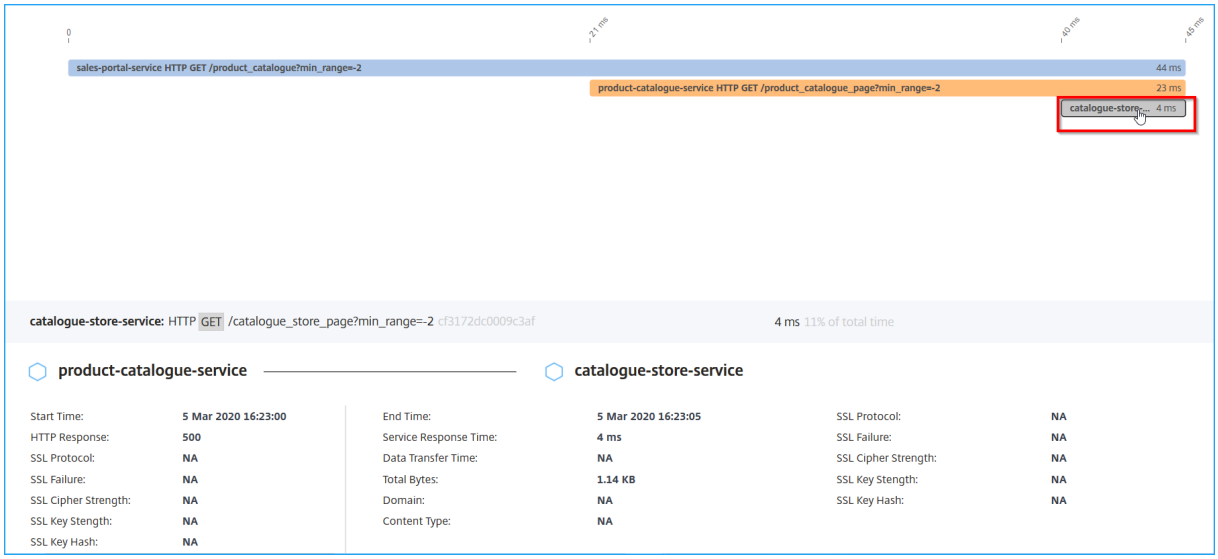


1 — 显示事务的开始时间、响应时间、总服务和总跨度。

2 — 显示已与其相互依赖服务进行通信的所选服务的详细信息。您可以单击每个交易记录以查看详细信息。

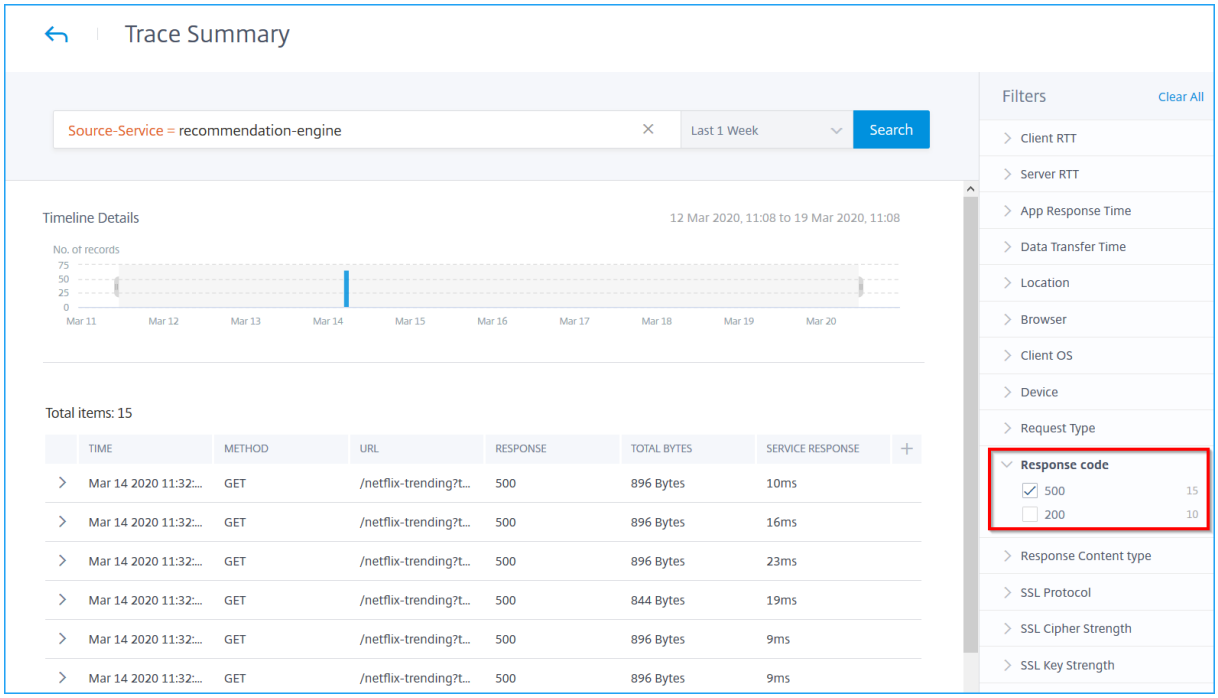
3 — 显示每个服务的交易详细信息。

根据示例图像，`catalogue-store-service` 指出了错误。单击可用的交易记录 `catalogue-store-service`。



之间的事务详细信息，product-catalogue-service 并将 HTTP 响应 catalogue-store-service 指示为 500。有了这些详细信息，作为管理员，您可以分析错误的服务并将其 product-catalogue-service 作为解决方案进行故障排除。

您还可以通过从“筛选 器”面板下的每个度量中选择选项来筛选结果。例如，如果要查看所有 5xx 交易记录，请单击 响应代码并选择 **500**。



- 客户端 **RTT**：数据包从客户端传输的时间持续时间。
- 服务器 **RTT**：数据包从服务器传输的时间持续时间。
- 应用程序响应时间：应用程序平均响应时间

- 数据传输时间：数据传输大小以及从/到服务发生传输的速率。
- 位置：客户端位置
- 浏览器：客户端使用的浏览器类型。例如：铬，火狐。
- 客户端操作系统：基于浏览器中的用户代理详细信息的客户端操作系统。
- 设备：基于浏览器中的用户代理详细信息的设备。例如：平板电脑、手机。
- 请求类型：事务处理请求类型。例如：GET。
- 响应代码：从服务器接收的响应代码。例如：501、404、200
- 响应内容类型：事务处理内容类型。如果客户端请求是文本 /html，则来自服务器的响应必须是文本 /html。
- **SSL** 协议：客户端使用的 SSL 协议版本。例如：SSLv3。
- **SSL** 密码强度：基于 SSL 证书密钥大小（如高、中和低）的密码强度。
- **SSL** 密钥强度：SSL 密码强度是根据 SSL 证书密钥大小计算的。密钥长度定义了 SSL 算法的安全性。例如：2048
- **SSL** 前端失败原因：前端 SSL 握手错误消息。例如：SSL 客户端失败

查看服务图中部分或无数据的诊断详细信息

April 23, 2021

在 Citrix ADM 中完成所需的服务图 配置 并添加 Kubernetes 集群后，服务图将开始填充数据。在某些情况下，您可能会注意到服务图显示部分数据或不显示数据。部分数据或服务图中没有数据的一些可能原因包括：

- 未配置静态路由
- Kubernetes 集群状态已关闭
- CPX 注册失败
- CPX 虚拟服务器未获得许可
- 未设置阻止服务图加载所有数据的所需分析配置

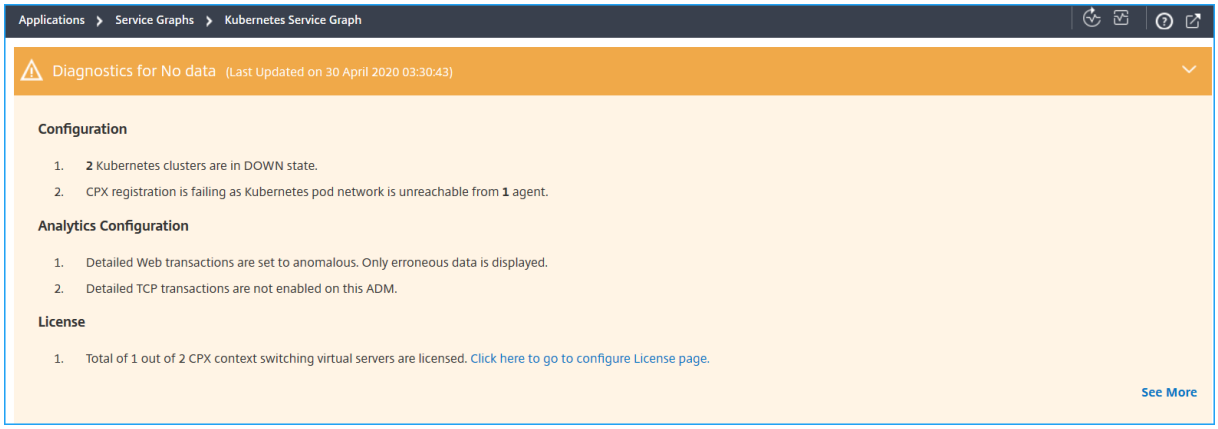
作为管理员，当您看到服务图显示部分数据或没有数据时，您可能会发现很难分析原因。使用服务图表页面中的诊断信息，您可以查看解决部分数据或无数据问题的可能原因和所需操作。

在 Citrix ADM 中，导航到 应用程序 > 服务图表，然后单击 微服务选项卡。

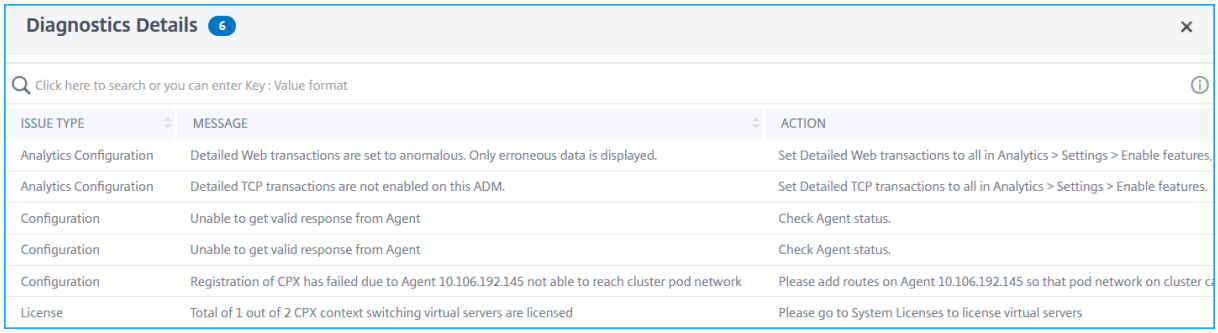
没有数据的诊断

如果服务图表未显示任何数据，则会显示以下诊断消息。

单击 **>** 查看详细信息。您可以查看服务图表未显示任何数据的可能原因。下图是服务图中没有数据的示例。



单击查看更多以查看问题的详细信息。

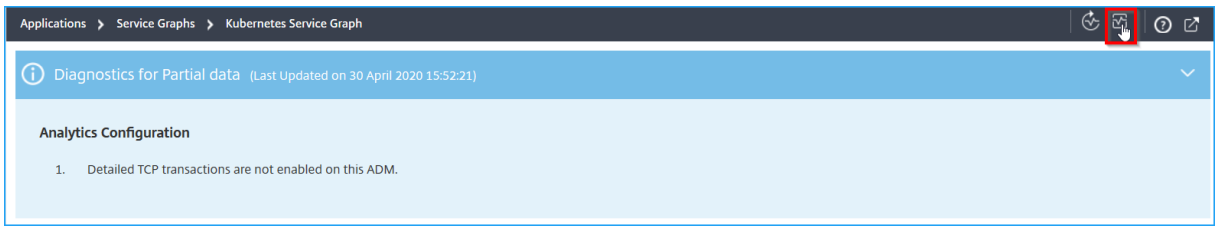


- 问题类型 — 指示问题是由配置、分析配置还是许可发生。
- 消息 — 指示导致问题的原因。
- 操作 — 指示必须执行哪些操作才能对问题进行故障排除。

部分数据的诊断

如果服务图仅显示部分数据，请单击显示诊断按钮以查看诊断信息。

以下示例表示 TCP 事务处理已禁用。

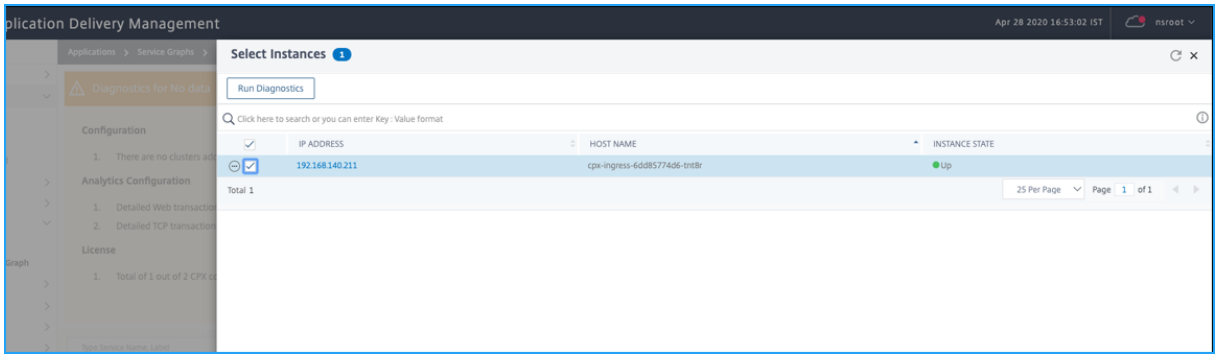


对于此示例，您必须导航到 **Analytics** > 设置，将 **TCP** 交易设置启用全部。

故障排除

作为管理员，使用这些诊断消息，您可以验证这些问题并尝试解决这些问题。排除故障后，Citrix ADM 会定期自动运行定期诊断检查。诊断检查完成后，服务图中的部分数据或无数据问题将得到解决。

您也可以单击 运行诊断程序，选择 **CPX** 实例，然后单击 运行诊断程序。



有关更多故障排除方案，请参阅 常见问题解答。

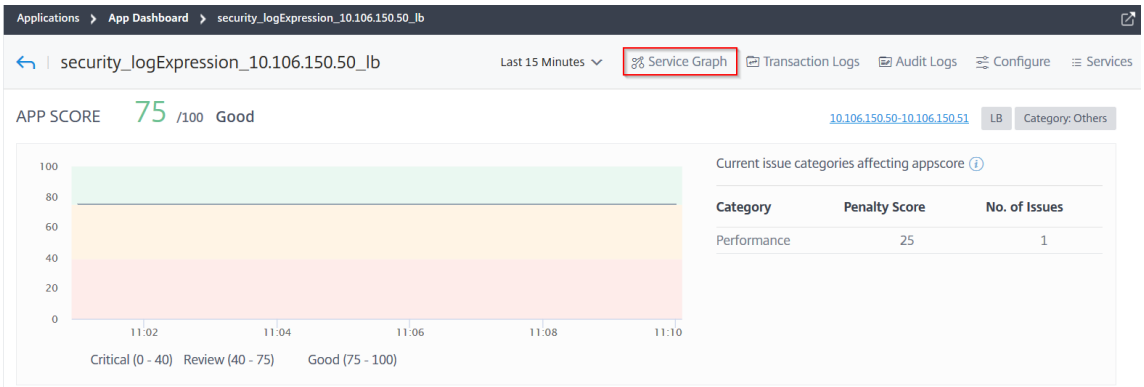
应用程序的服务图

April 23, 2021

要查看应用程序的服务图表，请执行以下操作：

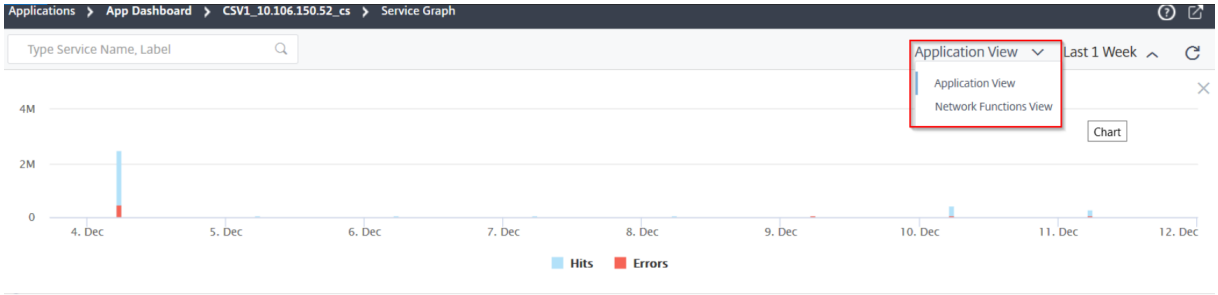
1. 定位至 “ 应用程序” > “ 控制面板”。
2. 选择一个应用程序。

   此时将显示应用程序详细信息页面。
3. 选择时间持续时间，然后单击 服务图表。

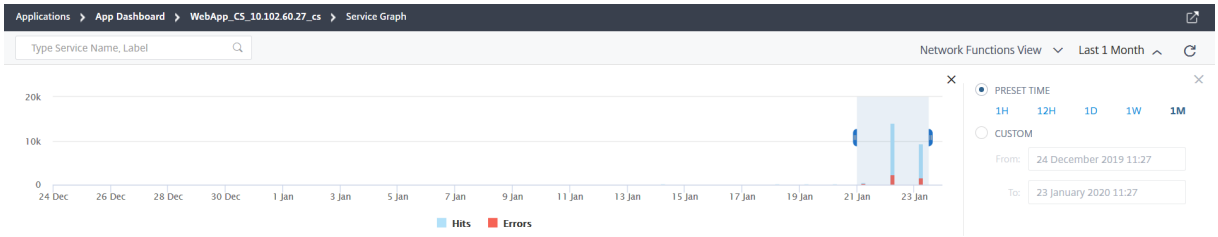


此时将显示所选应用程序的服务图表页面。

您可以在 “ 应用程序视图” 或 “网络功能视图” 中查看服务图。

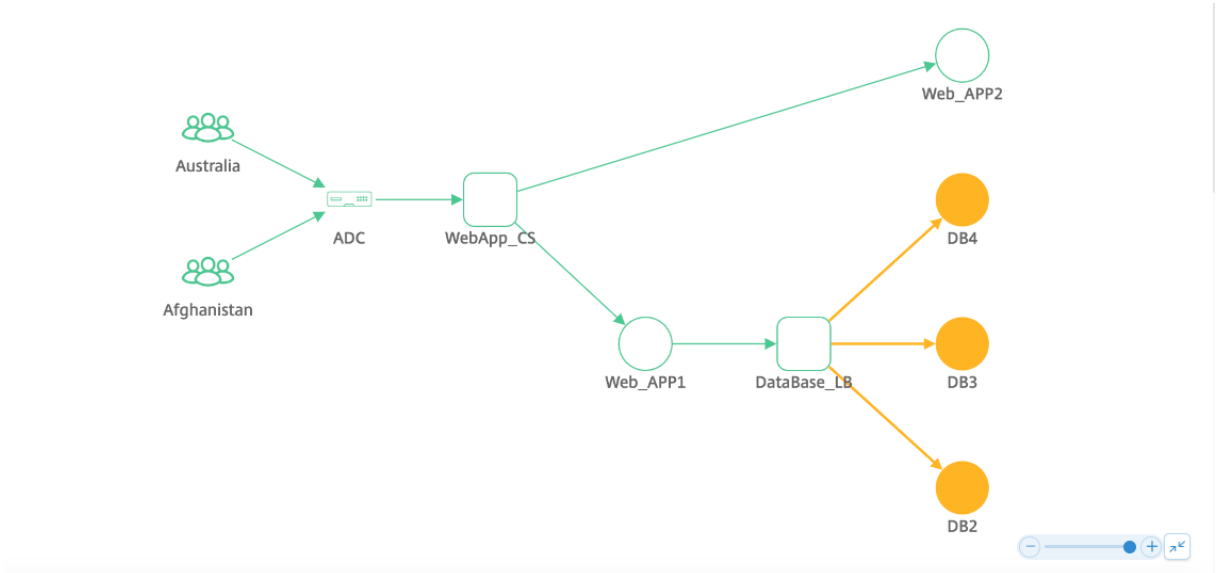


您还可以拖动并选择命中和错误以修改结果。



应用程序视图

显示应用程序配置的概述。在此视图中，您可以直观地显示客户端、ADC 和 Web 应用程序之间的通信。

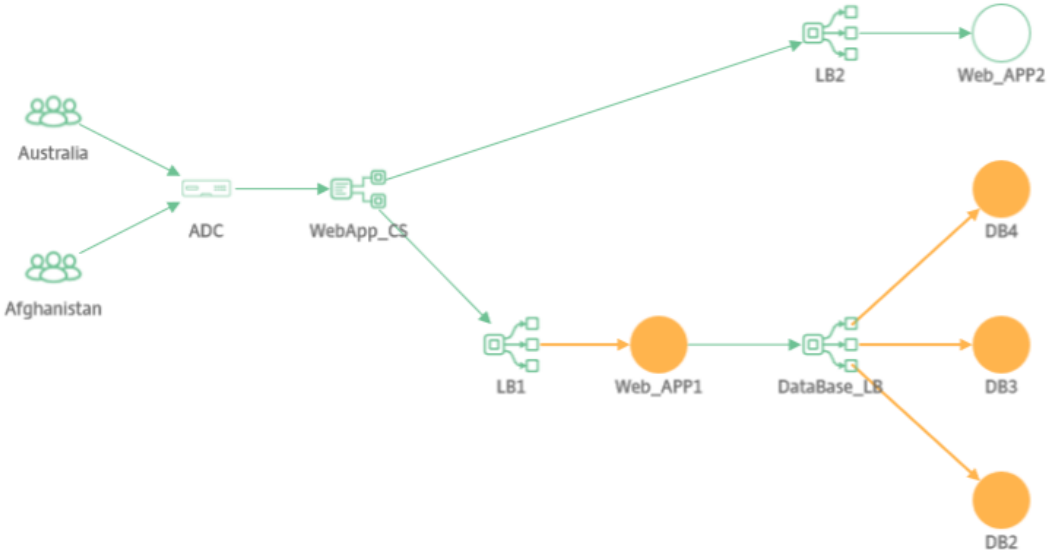


网络函数视图

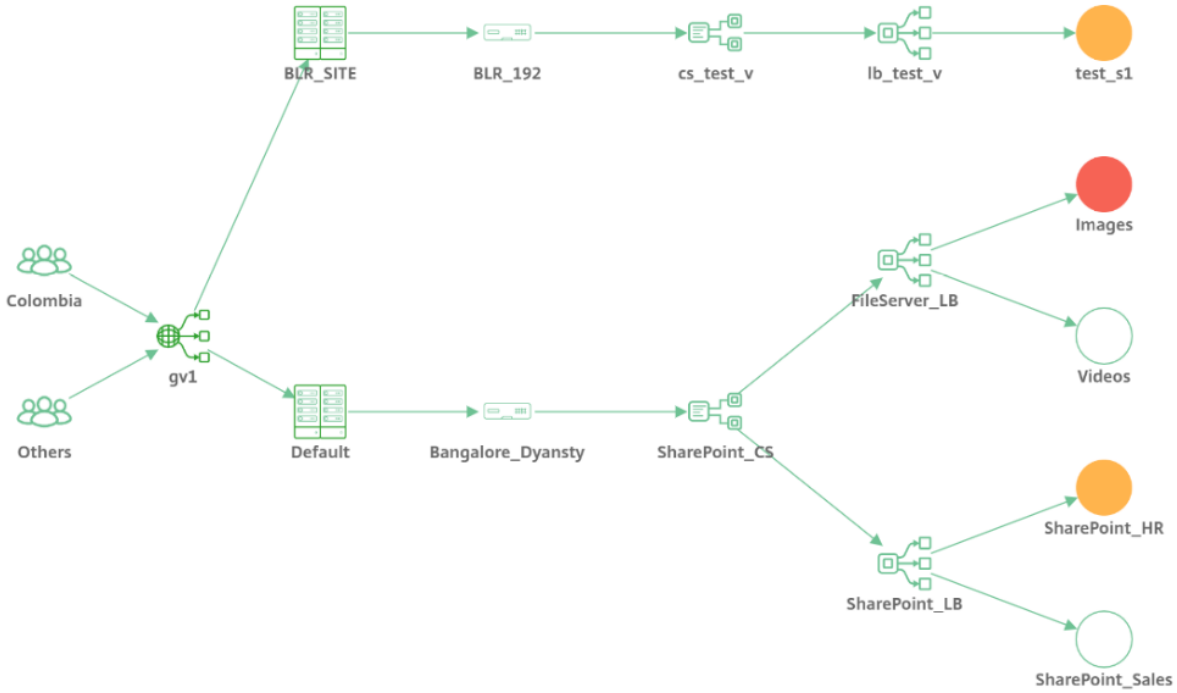
显示与应用程序关联的虚拟服务器。在此视图中，您可以直观显示 ADC 是否正在与以下内容进行通信：

- 内容切换虚拟服务器以访问应用程序
- 负载平衡虚拟服务器以访问应用程序

- 用于访问应用程序的内容交换和负载平衡虚拟服务器



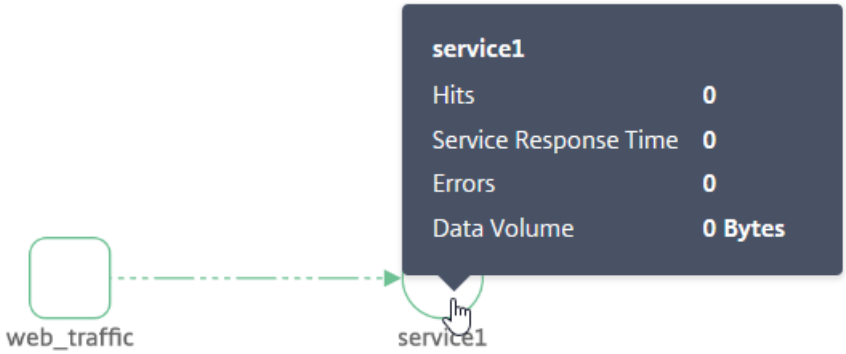
对于 GSLB 应用程序，详细信息与数据中心和 Citrix ADC 一起显示。



无活动事务处理的服务图视图

如果 ADC 和 Web 应用程序之间没有发生活动事务，则服务图表仅显示应用程序的基本配置（不包括客户端和 ADC）。

将鼠标指针悬停在服务或虚拟服务器上时，由于没有事务，所有度量的详细信息将显示为 0。

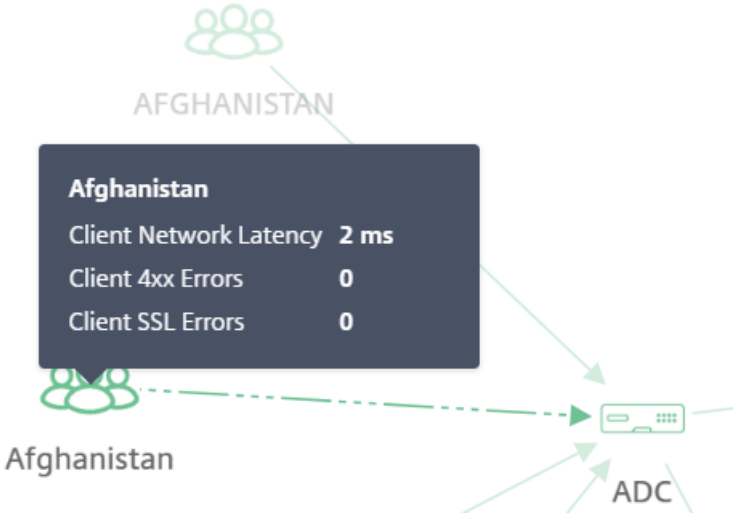


分析指标

将鼠标指针悬停在每个服务上，可在“应用程序视图”或“网络功能视图”中查看度量详细信息。

客户端指标

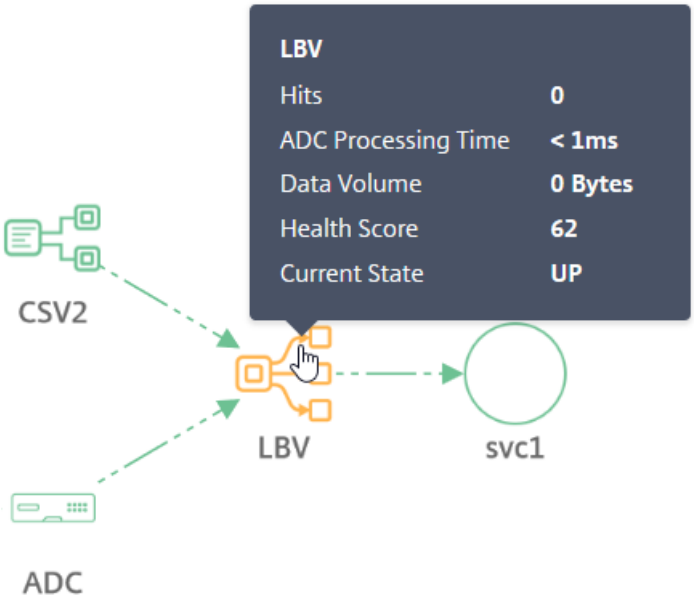
将鼠标指针悬停在客户端上以查看客户端指标。



- 客户端网络延迟 — 指示来自客户端的网络延迟。
- 客户端 **4xx** 错误 — 表示客户端发生的 4xx 个错误总数。
- 客户端 **SSL** 错误 — 指示来自客户端的 SSL 错误总数。

网络功能指标

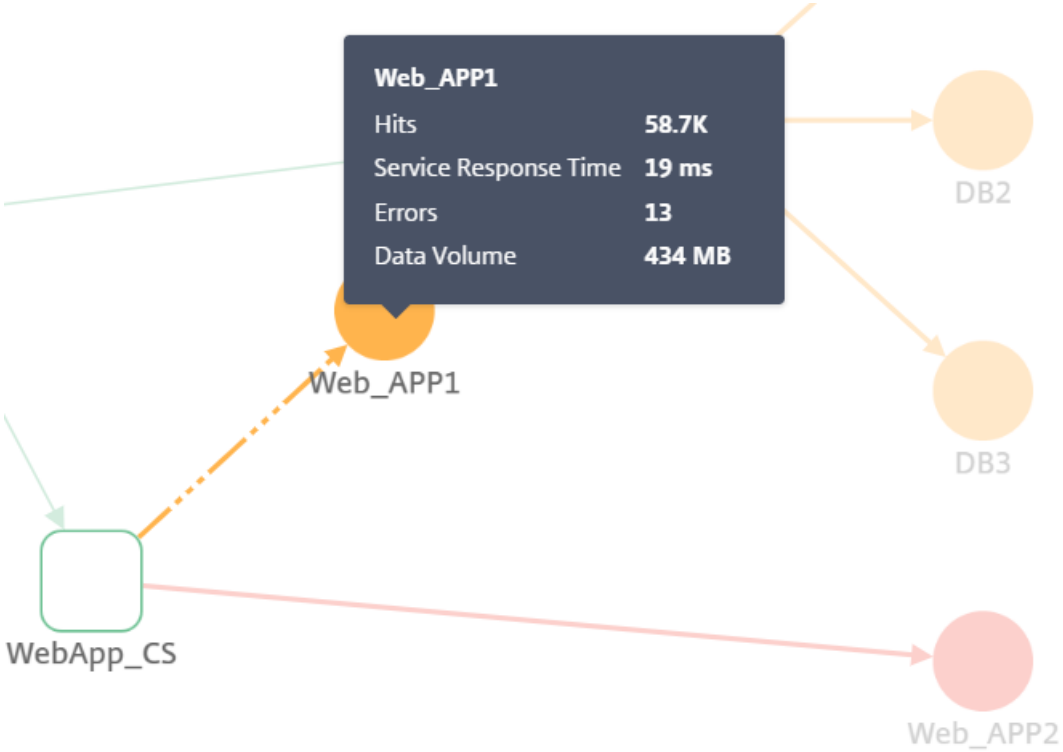
将鼠标指针悬停在负载平衡或内容切换服务上以查看指标详细信息。



- 命中 — 指示虚拟服务器接收的命中总数
- **ADC** 处理时间 — 指示 ADC 实例的平均处理时间
- 数据量 — 指示虚拟服务器处理的总数据量
- 健康评分 — 指示应用程序得分
- 当前状态 — 指示虚拟服务器的当前状态

服务指标

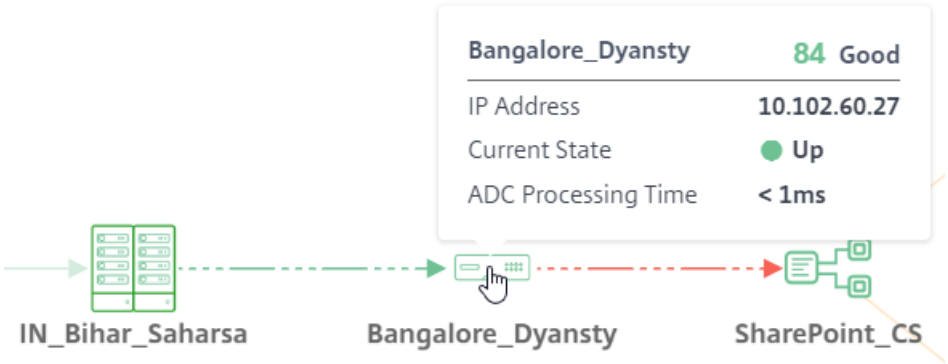
将鼠标指针悬停在服务（Web 应用程序）上以查看指标



- 命中 — 指示服务接收的命中总数
- 服务响应时间 — 指示服务的平均响应时间
- 错误 — 表示服务发生的总错误
- 数据量 — 表示服务处理的总数据

Citrix ADC 指标（仅适用于 **GSLB** 应用程序）

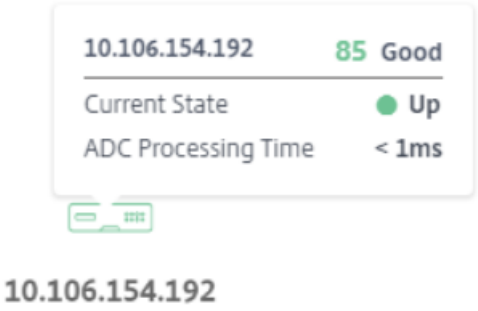
将鼠标指针悬停在 ADC 上以查看指标。



- 显示主机名和当前 ADC 分数。分数是根据不同的 Citrix ADC 潜在问题计算的。有关详细信息，请参阅实例分数。
- **IP** 地址 — 表示 Citrix ADC IP 地址

- 当前状态 — 表示 Citrix ADC 状态，如 “启动”、“关闭” 或 “停止服务”
- **ADC** 处理时间 — 表示 ADC 实例的平均处理时间

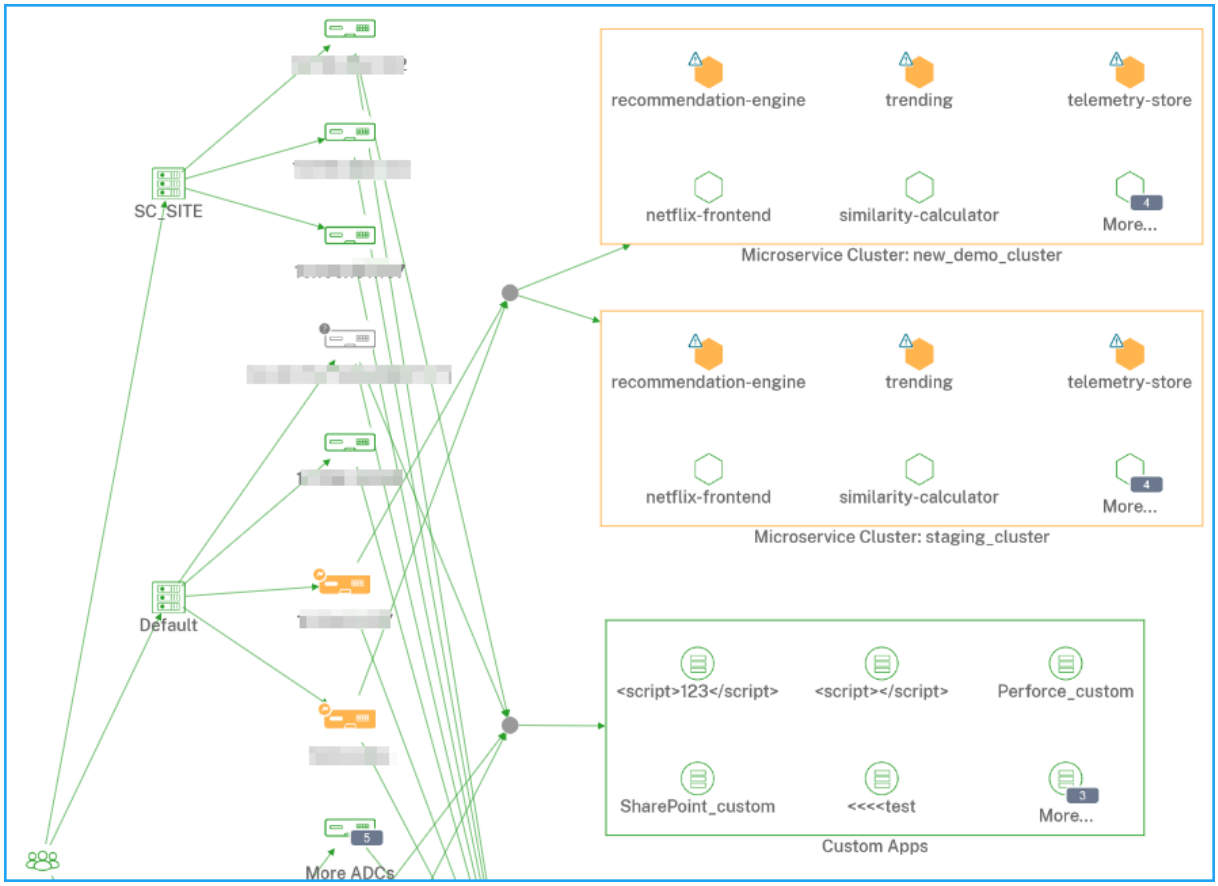
> 注意
>
> 如果未将主机名分配给 Citrix ADC：
>
> -显示的是思杰 ADC IP 地址而不是主机名。
>
> -在指标中，不显示 Citrix ADC IP 地址信息。



服务图中所有应用程序的整体视图

April 23, 2021

导航到应用程序 > 服务图表，然后单击全局。



服务图显示所选持续时间内的以下内容：

- 用户访问特定应用程序的区域

托管 Citrix ADC 实例的数据中心

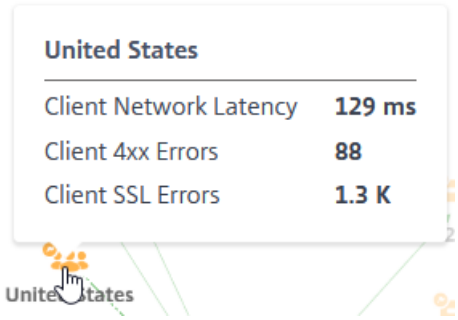
- 来自所有 Citrix ADC 实例的离散应用程序总数

  > 注意
  >
  > 如果 Citrix ADC 实例没有离散应用程序，则从 Citrix ADC 实例向离散虚拟服务器的箭头边缘不可见

- 来自所有 Citrix ADC 实例的自定义应用程序总数
- Citrix ADC CPX 实例中的微服务应用程序总数

查看客户端度量

将鼠标指针悬停在客户端区域上以查看指标。



- 客户端网络延迟 -表示平均客户端网络延迟。
- 客户端 **4xx** 错误 -表示客户端 4xx 错误总数。
- 客户端 **SSL** 错误 -表示客户端 SSL 错误总数。

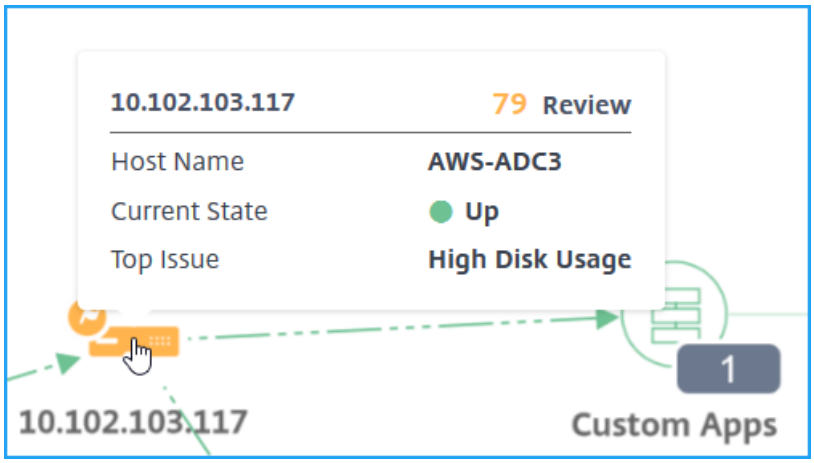
查看 **Citrix ADC** 详细信息

通过服务图表，您可以查看：

- 数据中心与其 Citrix ADC 实例总数进行分组
- 只有来自每个数据中心的前 4 个低分 Citrix ADC 实例

单击 更多 **AD** C 可通过选择相应的状态（“严重”、“查看”、“良好” 和 “不适用”）选项卡来查看所有 Citrix ADC 实例。

将鼠标指针悬停在 Citrix ADC 实例上以查看指标。



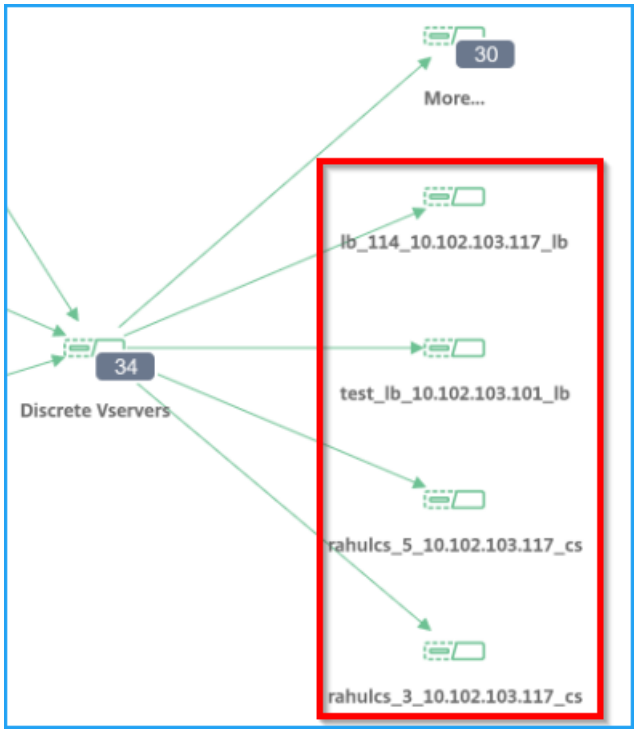
您可以查看：

- Citrix ADC 实例 IP 地址和分数
- 主机名 — 表示分配给 Citrix ADC 实例的主机名
- 当前状态 — 指示 Citrix ADC 实例的当前状态，例如 “启动”、“关闭”、“不服务”。
- 热门问题 — 表示影响当前 Citrix ADC 分数的首要问题

单击 **Citrix ADC** 实例可查看实例详细信息，例如实例得分、关键指标和与 ADC 实例相关的问题。有关详细信息，请参阅在基础架构分析中查看实例详细信息。

查看离散应用

服务图表显示前 4 个得分低的离散应用程序。



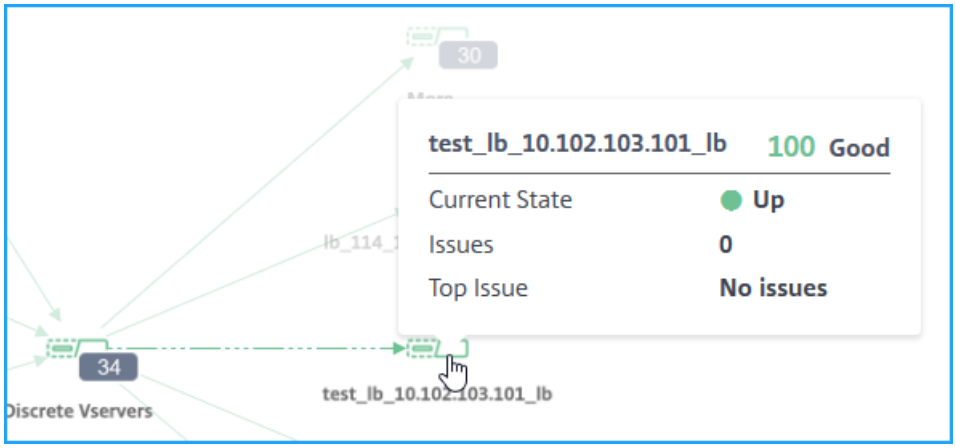
考虑一下您有以下离散应用程序：

应用程序名称	Citrix ADC	应用程序分数	应用状态
App1	10.102.29.50	35（严重）	运行
App2	10.102.29.90	100（不错）	关闭
应用程序 3	10.102.32.40	49（评论）	运行
App4	10.102.113.208	92 (不错)	关闭
App5	10.102.25.25	86 (不错)	运行
App6	10.102.29.41	77 (不错)	运行
App7	10.102.29.102	41（评论）	运行

在这种情况下，您可以将应用程序 1、应用程序 3、应用程序 6 和应用程序 7 视为服务图中评分最低的 4 个应用程序。

同样，您还可以查看 自定义和 微服务应用程序的四大低分应用程序。

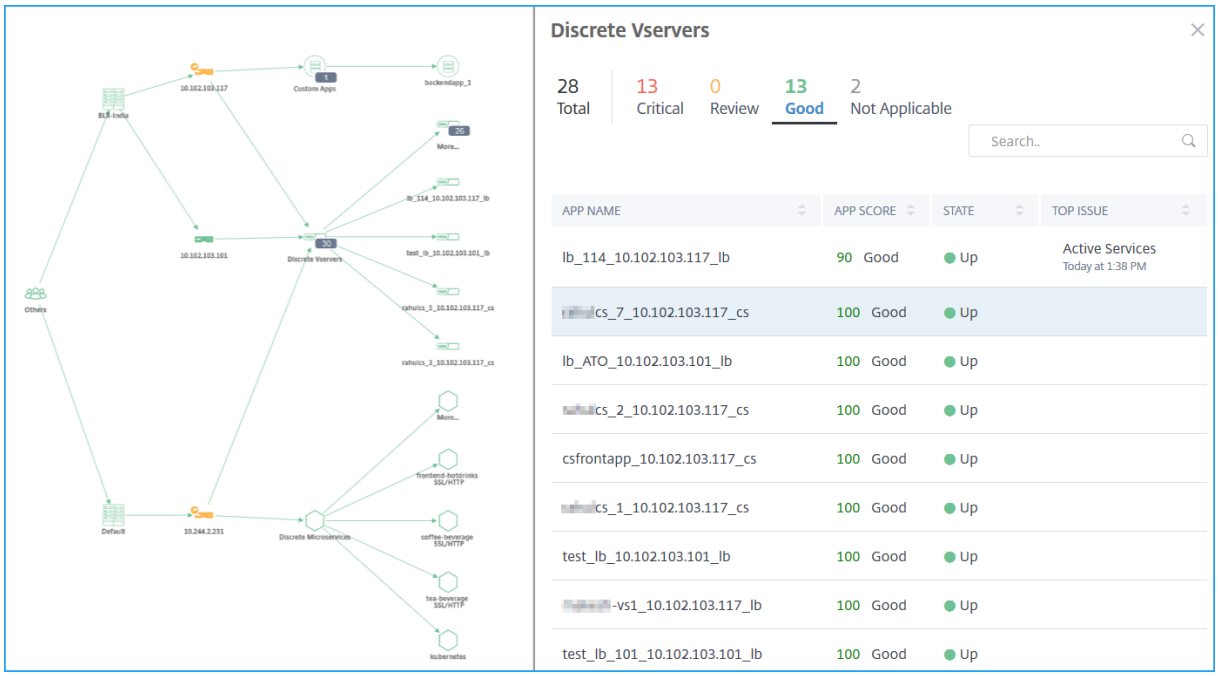
将鼠标指针悬停在服务上以查看指标信息。



您可以查看：

- 应用程序名称和分数
- 当前状态 — 表示应用程序的当前状态，例如向上或关闭
- 问题 — 表示适用于应用程序的总问题
- 热门问题 — 表示影响整体应用程序得分的首要问题

单击 更多以查看所有离散应用程序。将显示“离散虚拟服务器”页面，如下图所示：

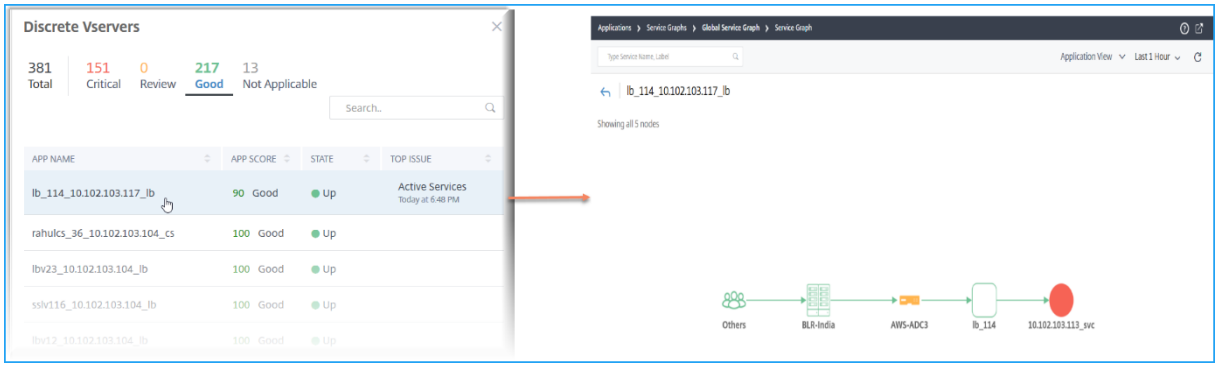


虚拟服务器将根据状态显示。

- 总计 — 离散应用程序总数
- 关键 — 应用得分在 0 到 <40 之间
- 评论 — 应用程序得分在 40 到 <75 之间

- 好 -应用得分 > 75
- 不适用 — 应用程序不绑定到任何虚拟服务器

您可以单击每个选项卡以查看虚拟服务器。单击应用程序时，将显示所选应用程序的服务图表。



有关详细信息，请参阅应用程序的服务图。

查看微服务应用程序

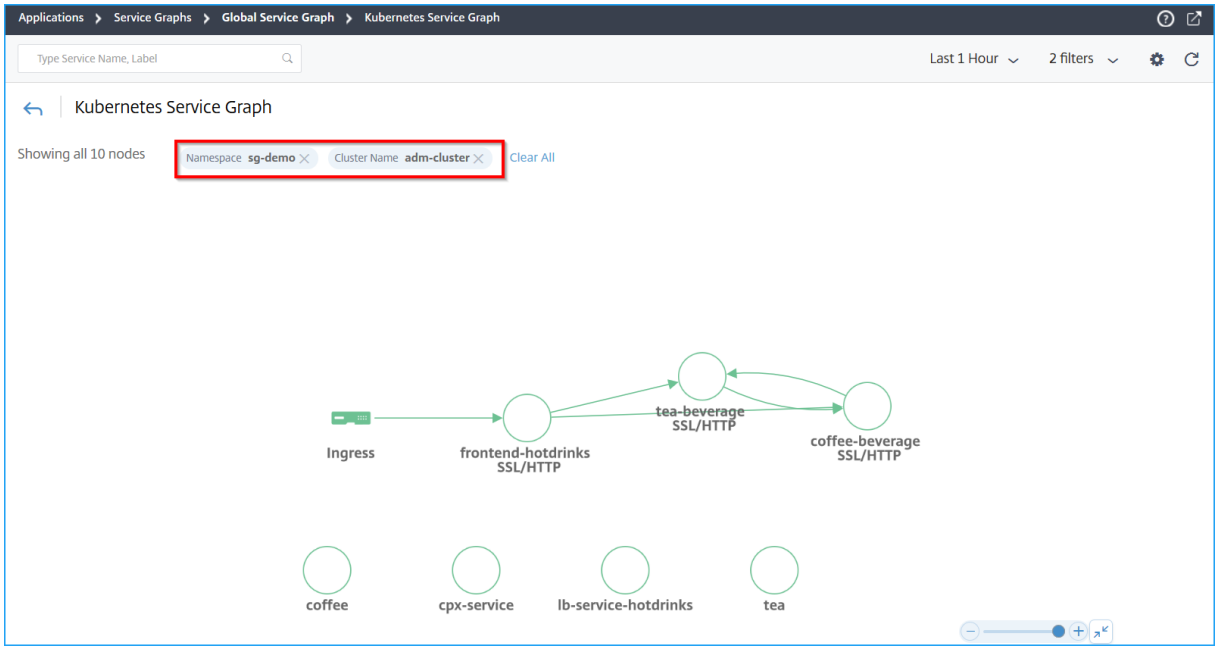
服务图还显示属于 Kubernetes 集群的所有微服务应用程序。将鼠标指针悬停在服务上以查看指标详细信息。

您可以查看：

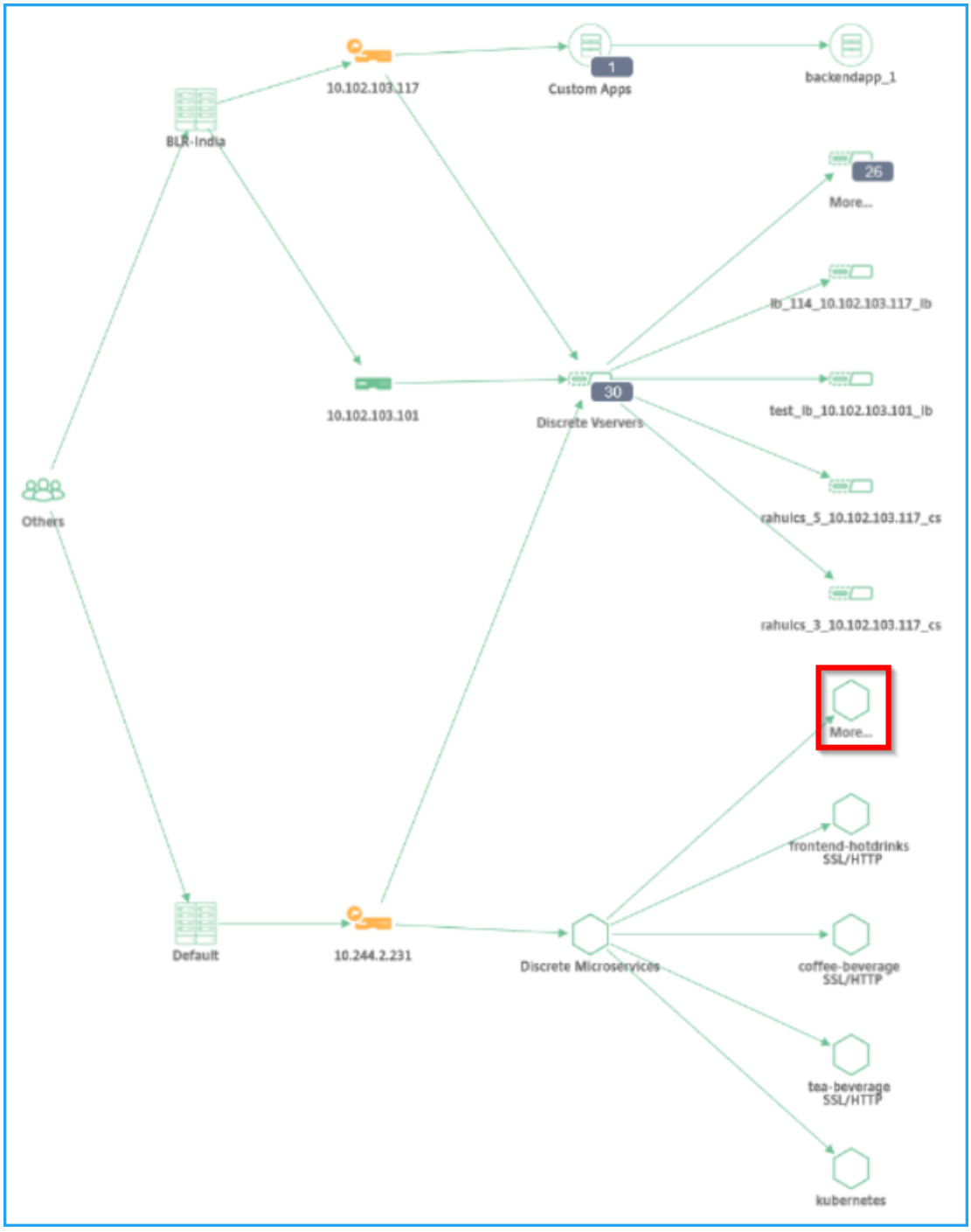
- 服务名称
- 服务使用的协议，例如 SSL、HTTP、TCP、SSL
- 点击量 — 服务收到的点击总数
- 服务响应时间 — 从服务获得的平均响应时间。

  （响应时间 = 客户端 RTT + 请求最后一个字节 — 请求第一个字节）
- 错误 — 总错误，例如 4xx、5xx 等
- 数据量 — 服务处理的数据总量
- 命名空间 — 服务的命名空间
- 集群名称 — 托管服务的集群名称
- **SSL** 服务器错误 — 来自该服务的 SSL 错误总数

单击服务时，将显示所选服务的 Kubernetes 服务图以及应用的服务命名空间和集群名称筛选器。



单击 更多以查看包含所有服务的 Kubernetes 服务图。有关 Kubernetes 服务图的更多信息，请参阅 云原生应用程序的服务图。



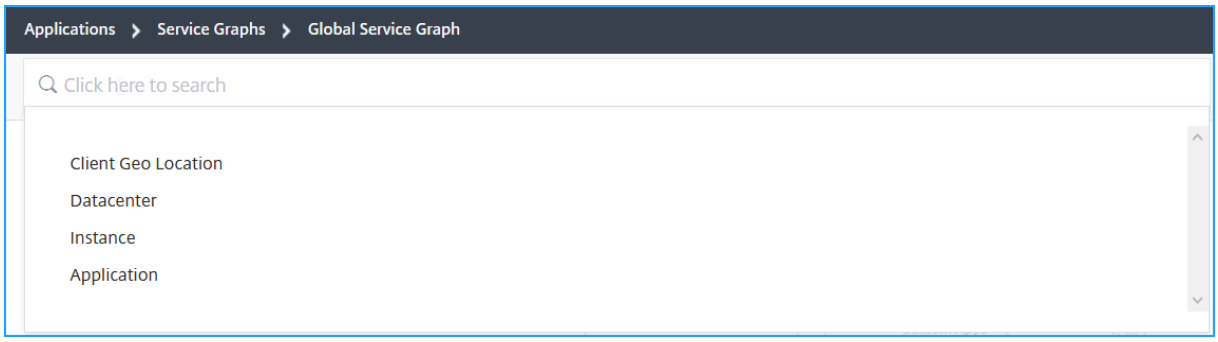
用于筛选结果的搜索栏

您可以使用搜索栏筛选结果。作为管理员，此搜索栏使您能够在以下情况下快速缩小到特定实例/客户端/应用程序/数据中心：

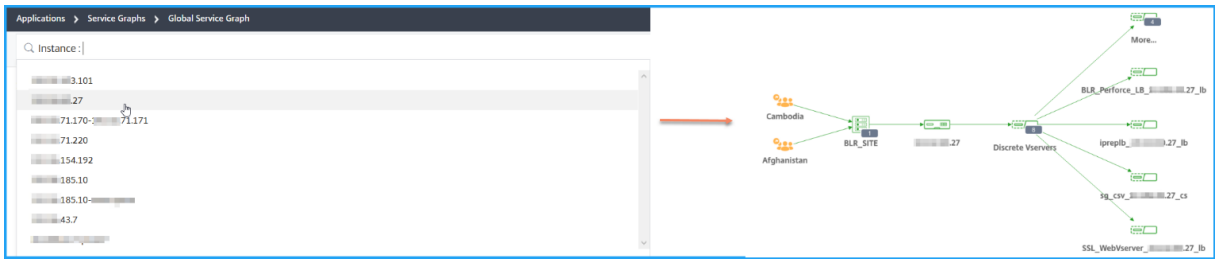
- 拥有许多数据中心的大型企业

- 为每个数据中心配置了许多 Citrix ADC 实例
- 配置了通过每个 Citrix ADC 实例部署或访问的许多应用
- 客户端从不同位置访问应用程序

将鼠标指针放在搜索栏上，然后选择要创建筛选器的类别。



例如，如果您想查看特定 ADC 实例，请从搜索栏中选择 实例，然后选择实例 IP 地址。全局服务图显示所选实例及其关联的应用程序、数据中心和客户端位置。



样本

April 23, 2021

样本简化了为应用程序管理复杂的 Citrix ADC 配置的任务。样本是可用于创建和管理 Citrix ADC 配置的模板。您可以创建样本来配置 Citrix ADC 的特定功能，也可以设计样本来为企业应用程序部署（如 Microsoft Exchange 或 Lync）创建配置。

样本非常符合 DevOps 团队实践的基础结构即代码原则，其中，配置是声明性且版本受控的。配置还是重复使用的，并作为整体部署。样本具有以下优点：

- 声明式：样本是用声明式语法而不是命令式语法编写的。样书允许您专注于描述配置的结果或“所需状态”，而不是关于如何在特定 Citrix ADC 实例上实现配置的分步说明。Citrix Application Delivery Management (ADM) 计算 Citrix ADC 上的现有状态与您指定的所需状态之间的差异，并对基础结构进行必要的编辑。由于样本使用用 YAML 编写的声明语法，因此样本的组件可以按任意顺序指定，Citrix ADM 根据其计算的依赖关系确定正确的顺序。
- 原子：使用样书部署配置时，将部署完整配置或不部署任何配置，这可确保基础结构始终处于一致状态。

- 版本化：样本具有名称、命名空间和版本号，使其与系统中任何其他样本进行唯一区分。对样本进行任何修改均需要更新其版本号（或者其名称或命名空间）以维护此唯一特征。此外，通过版本更新可以维护同一样本的多个版本。
- 可组合：定义样本后，样本可用作构建其他样本的单元。您可以避免重复使用配置的公用模式。此外，通过它您还可以在您的组织中建立标准构建块。由于样本是版本化的，因此，对现有样本进行更改会产生新的样本，从而确保绝不会意外破坏依赖样本。
- 以应用为中心：样本可用于定义完整应用程序的 Citrix ADC 配置。可以使用参数提取应用程序的配置。因此，通过样书创建配置的用户可以与一个简单的界面进行交互，该界面包括填充几个参数，以创建可能是复杂的 Citrix ADC 配置。基于样本创建的配置不绑定到基础结构。因此，可以在一个或多个 Citrix ADC 上部署单个配置，也可以在实例之间移动。
- 自动生成的 **UI**：在使用 Citrix ADM GUI 完成配置时，Citrix ADM 自动生成用于填充样本参数的 UI 表单。样本作者无需了解新的 GUI 语言或单独创建 UI 页面和表单。
- **API** 驱动：使用 Citrix ADM GUI 或通过 REST API 支持所有配置操作。可以在同步模式或异步模式下使用 API。除了配置任务外，通过样本 API 还可以在运行时发现任何样本的架构（参数说明）。

可以使用一个样本创建多个配置。每个配置都保存为一个配置包。例如，假设有一个定义典型 HTTP 负载平衡应用程序配置的样本。您可以使用负载平衡实体的值创建配置，并在 Citrix ADC 实例上执行该配置。此配置保存为一个配置包。您可以使用同一样书创建具有不同值的另一个配置，并在相同或不同的 Citrix ADC 实例上执行该配置。即为此配置创建一个新配置包。配置包保存在 Citrix ADM 上和执行配置的 Citrix ADC 实例上。

您可以使用 Citrix ADM 随附的默认样本为部署创建配置，也可以设计您自己的样本并将其导入 Citrix ADM。您可以使用样本通过使用 Citrix ADM GUI 或使用 API 来创建配置。

本文档包含以下信息：

- 如何查看样本
- 默认样本
- 为业务应用程序开发的样本
- 自定义样本
- 样本中的 API
- 样本语法

样本组

April 23, 2021

Citrix Application Delivery Management (ADM) 中有两个样本组。它们是默认样本和自定义样本。无论是默认样本还是自定义样本，样本都是公共样本或私有样本。在 Citrix ADM 中，您可以查看系统中存在的所有样本，无论其类型或可见性状态如何。您还可以查看样本之间如何连接的图形显示。

本文档介绍了不同类型的样本。此外，它还介绍了您可以对 Citrix ADM 的样本执行的以下操作：

- 下载自定义样本并进行修改，或根据现有样本创建样本。
- 隐藏 ADM 默认样本。
- 从 Citrix ADM 中删除自定义样本。
- 将标签添加到样书中。

默认和自定义样本

- 默认样本是 Citrix ADM 随附的样本，它们允许您创建可在 Citrix ADC 实例上部署的配置。您无法删除默认样本，但可以从 ADM GUI 中隐藏它们。
- 自定义样本是您自己导入到 Citrix ADM 的样本。

默认样本和自定义样本都可以是公有样本，也可以是私有样本。

公共和私人样本

您可以从中创建配置包的样书可以归类为 公共样书。也就是说，它们都可以直接用于从 Citrix ADM GUI 和 API 创建配置。

但是，某些样本用作其他样本的构建块。此类样本被标记为 私有。私有样书不能直接用于从 Citrix ADM GUI 创建配置包。但是，您仍然可以在 Citrix ADM 上显示和查看这些样本。要将任何自定义样本标记为 私有，请将样本中的私有属性设置为 **true**。您仍然可以使用私有样书使用 Citrix ADM API 创建配置包。

标记为私有样本的示例

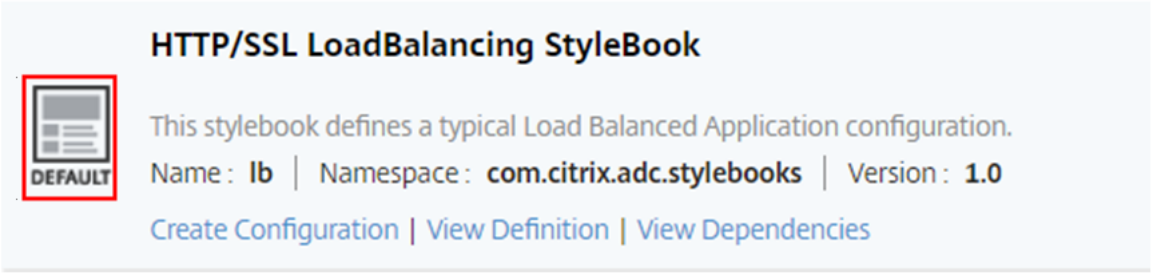
```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: |
    This StyleBook defines a simple load balancing configuration and is
        a building block to build other load balancing configurations.
schema-version: "1.0"
private: true
<!--NeedCopy-->
```

查看样本

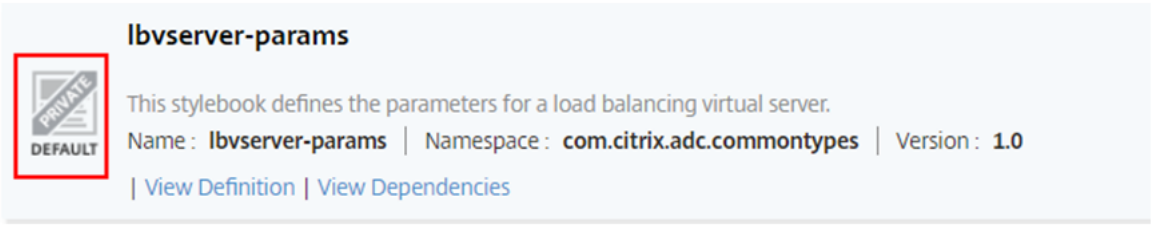
Citrix ADM 中的样本数量-默认和私有样本数量都在增加。您可能需要搜索要访问的特定样本。您可能还需要单独查看这两种类型的样本。

在 Citrix ADM 中，导航到 应用程序 > 样本时，可以查看系统中存在的样本列表。

默认公用样本面板上有以下图标：

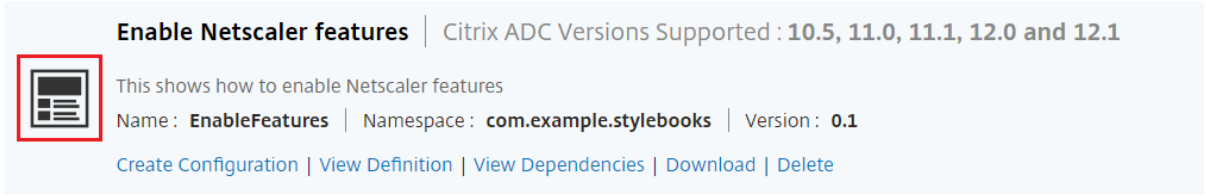


默认私有样本有一个将其声明为私有样本的图标：

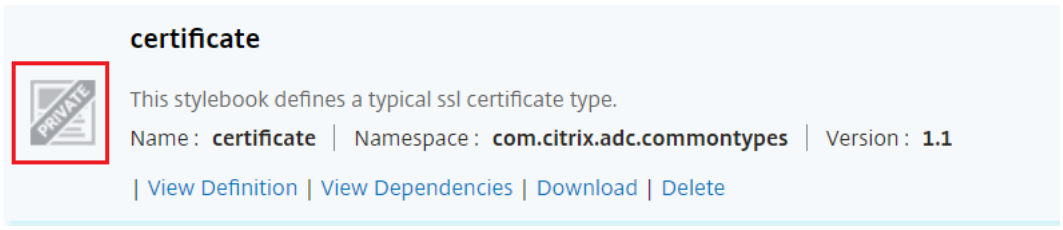


虽然您可以查看私有样书的定义和依赖关系，但不能使用 GUI 从私有样书创建配置包。私有样本的主要目的是将其用作另一个样本的构建块。使用构建块样本鼓励重复使用常见的配置模式。

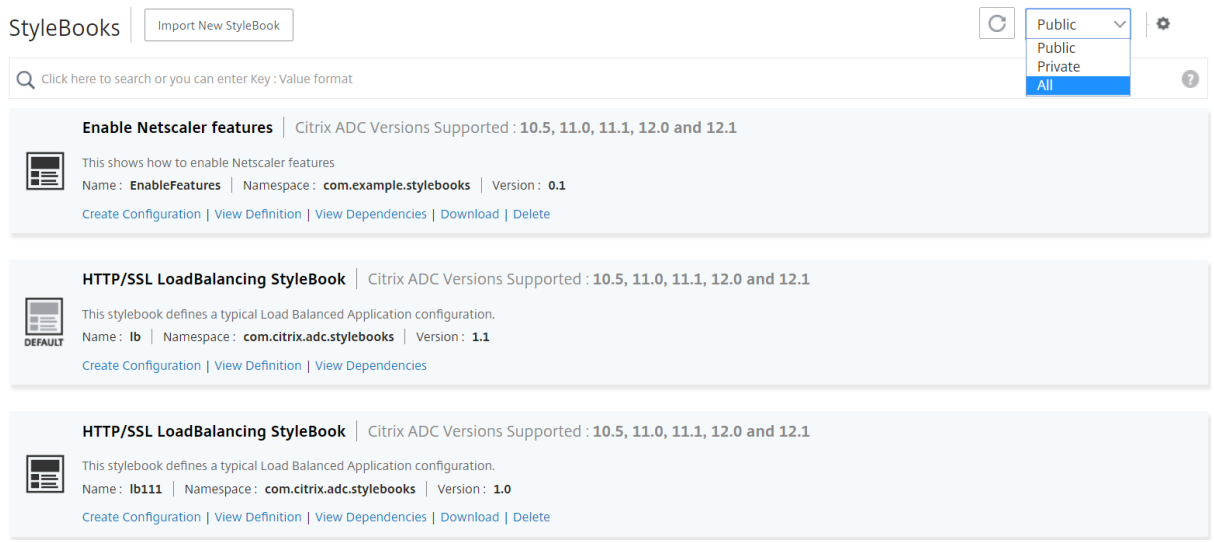
自定义公用样本具有不同的图标，如下图所示：



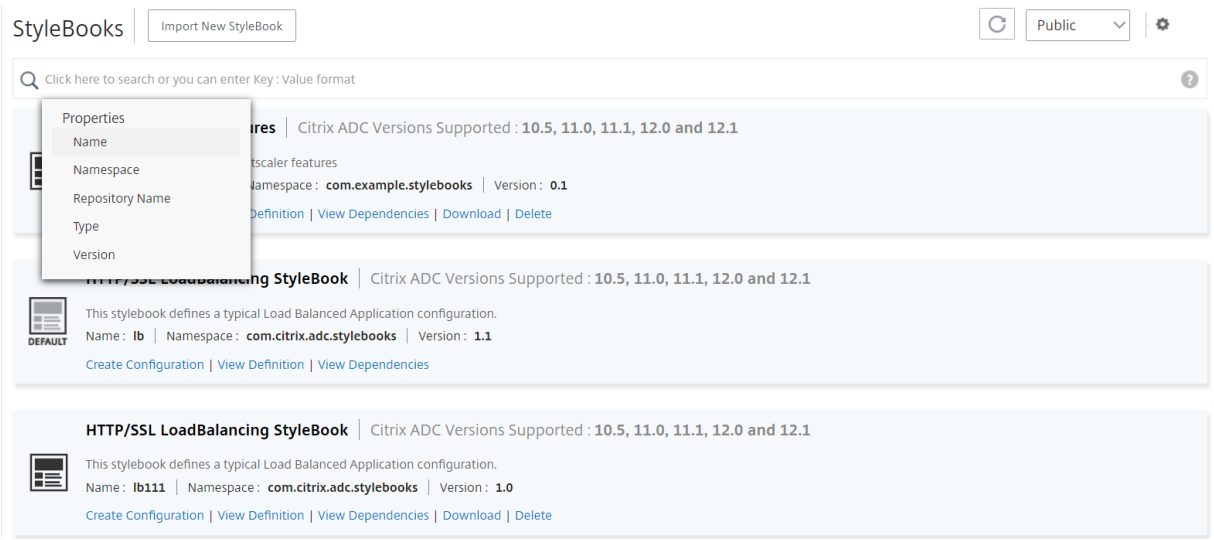
虽然自定义私有样本显示以下图标：



在页面右上角，您可以看到选择要查看的样本类型的选项。有三个选项-全部样本、公共样本或私有样本。单击其中一个选项。



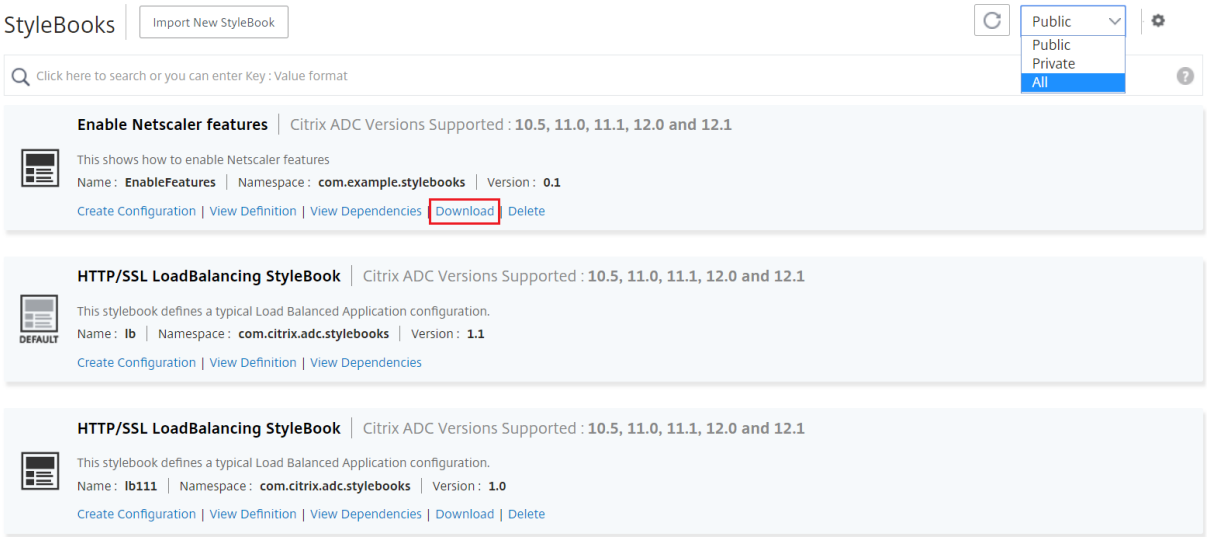
您也可以通过单击搜索图标来搜索特定样本。您可以按名称、命名空间和版本属性或这些选项的组合进行搜索。搜索操作不区分大小写。



下载自定义样本

要从 Citrix ADM 下载自定义样书，请导航到 应用程序 > 样书 > 配置。在右侧面板上显示的样本列表中，选中下载自定义样本的选项。单击下载。如果样书具有相关的自定义样书，则可以在下载的捆绑包中包含相关样书。

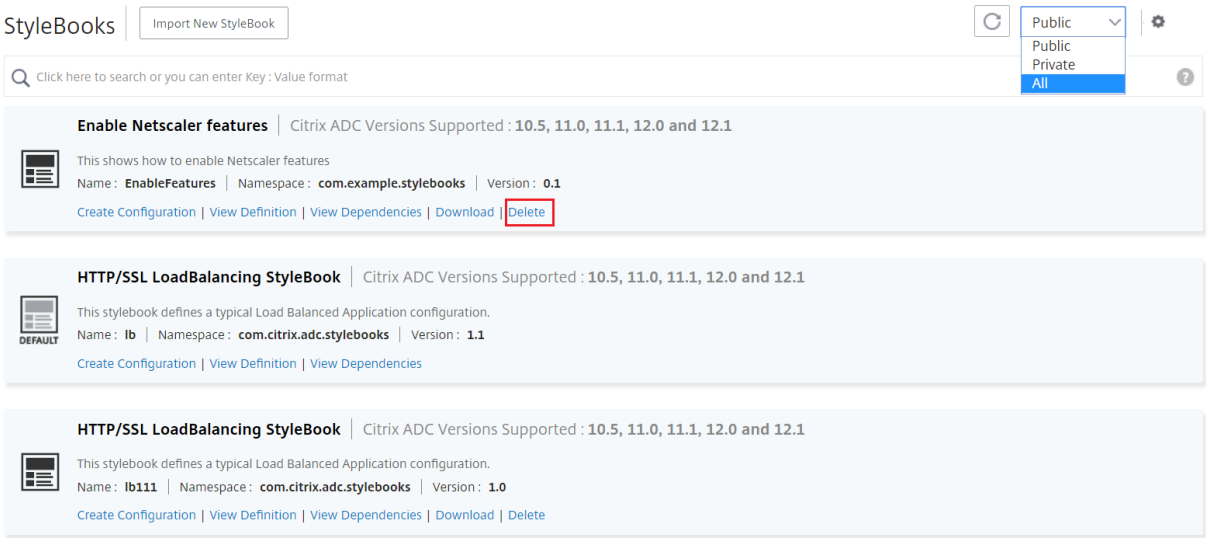
> 注意
>
> 您可以下载标记为公共或私有的自定义样本。

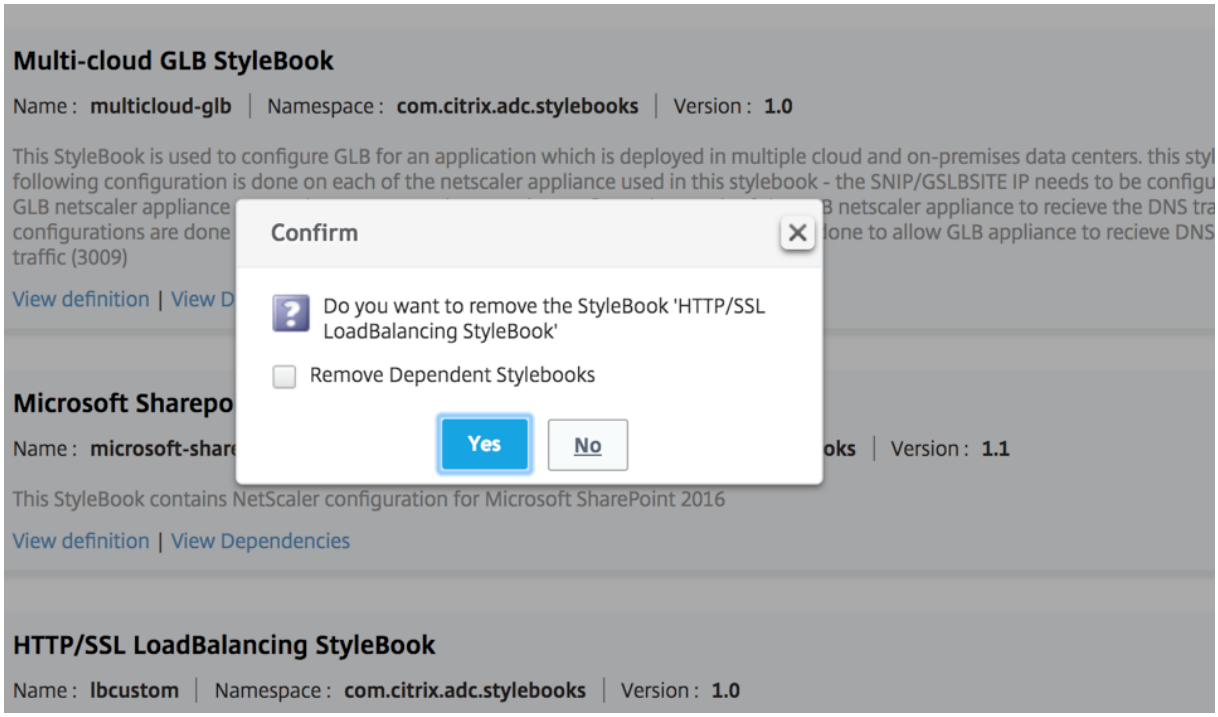


> 注意
>
> 您无法下载 Citrix ADM 默认样本。您可以查看它们的定义和依赖关系。为此，请单击样书面板上的 查看定义和查看依赖关系链接。

删除自定义样本

您也可以通过单击“删除”按钮 删除自定义样本。弹出窗口会提示您确认是否要从 Citrix ADM 中删除样本。如果样书使用其他自定义样书，则可以通过选中复选框来选择删除此类样书。





> 注意
>
> 如果自定义样书在 Citrix ADM 中具有相关样书，请不要删除该样书。否则，它会破坏现有的样书。

查看样本依赖关系

样本一个重要的强大功能是它们可以用作其他样本的构建块。您可以将样本导入到另一个样本中。导入的样书被声明为类型，并由第二个样书的组件或参数使用。您可以研究 Citrix ADM 中的现有默认样本，了解如何在另一个样本之上构建一个样本。

Citrix ADM 允许您查看样本之间如何连接的图形显示。此表示方式对于使用其他样书作为构建块构建的复杂样书尤其有用。通过查看依赖关系图，可以看到多个样本之间的关系和依赖关系。

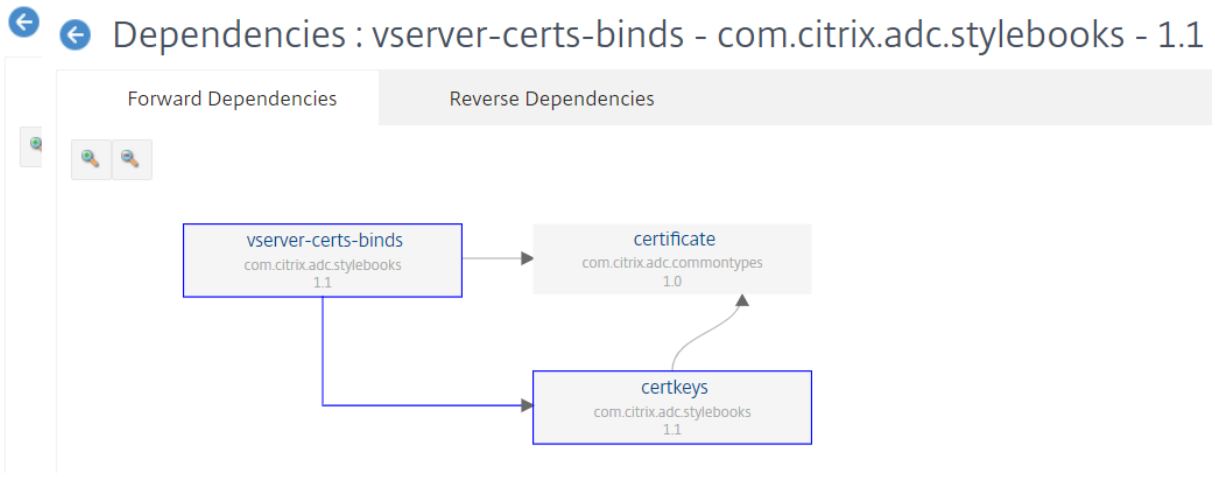
其他样书使用的样书无法从系统中删除，因为它会破坏现有的样书。使用依存关系图显示，您可以识别哪些样本阻止删除样本。

查看样本依赖关系

在 Citrix ADM 中，导航到 应用程序 > 样本。“ 样书” 页面显示可供您在 Citrix ADM 中使用的所有样书。向下滚动并找到您的样本。样书磁贴会显示创建配置、查看样书定义和查看样书依赖关系的链接。单击 查看依赖关系。

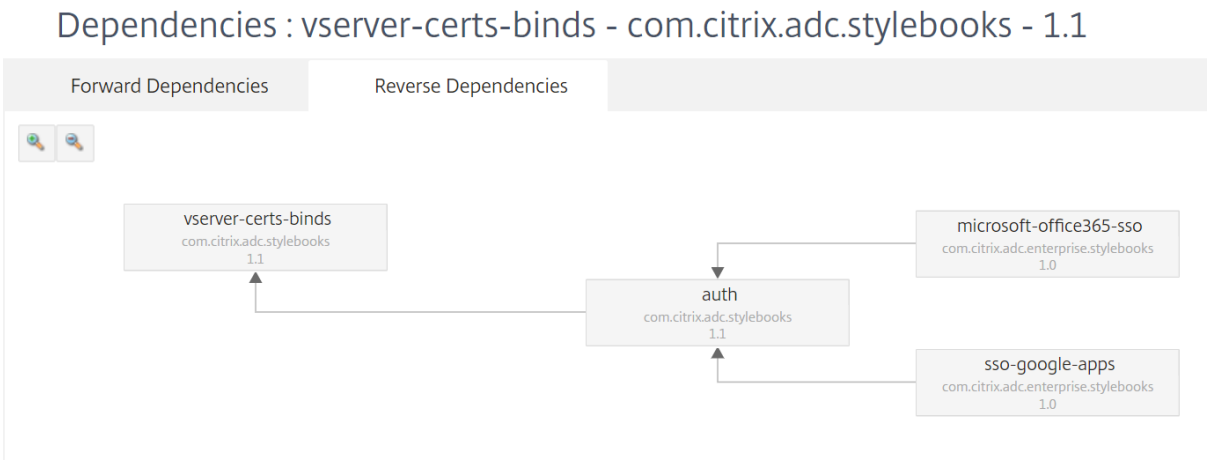
转发依赖关系

“向 前依赖关系选项卡允许您查看样本正在使用的不同默认样本。按照箭头查找样本正在使用的样本。当您将鼠标指向其中一个箭头时，箭头和相互连接的样本会突出显示。您还可以单击样本名称以查看该样本的定义。



反向依赖关系

“ 反向依赖关系选项卡允许您以图形方式查看使用样本的样本。如果按照箭头进行操作，您可以看到显示屏中的所有样书都指向您的样书。有些样本可能直接使用样本，有些样本可能正在通过其他样本使用样本。



根据配置包审核 **ADC** 配置

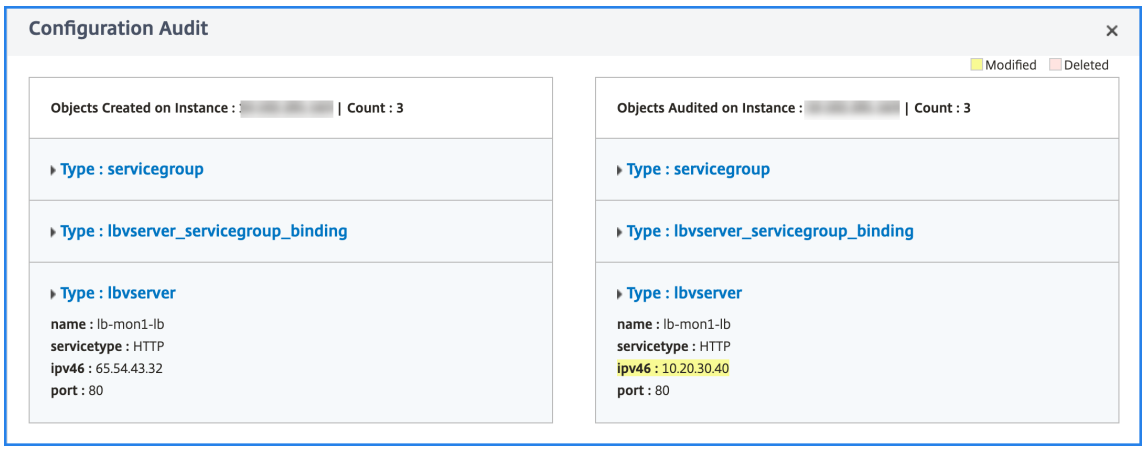
您可以将样书配置包所做的更改与当前 ADC 配置进行比较。通过此比较，您可以执行以下操作：

- 检测样书配置包和 ADC 配置之间的配置偏移。
- 识别 ADC 上没有反映配置包所做更改的任何修改和删除的对象。

要将配置包更改与 ADC 配置进行比较，请执行以下操作。

1. 导航到 应用程序 > 样本 > 配置。
2. 单击 配置审核。

   “配置审计”页显示创建和审计的对象。

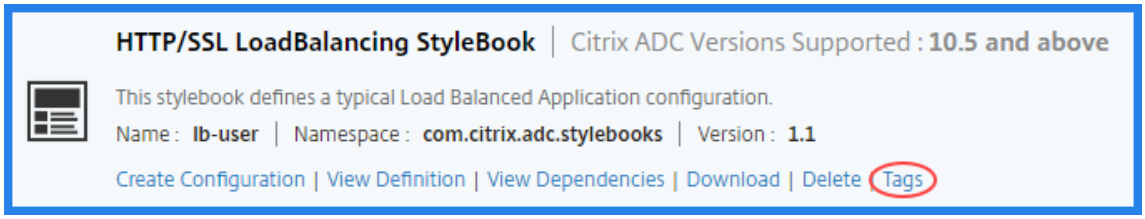


为样书创建标签

您可以将标签添加到 Citrix ADM 中的任何样书。标签是键值对，允许您使用不同的条件对样书进行分组。您可以在 Citrix ADM 中搜索或筛选样书时使用这些标签。

要向样书添加标签，请执行以下操作：

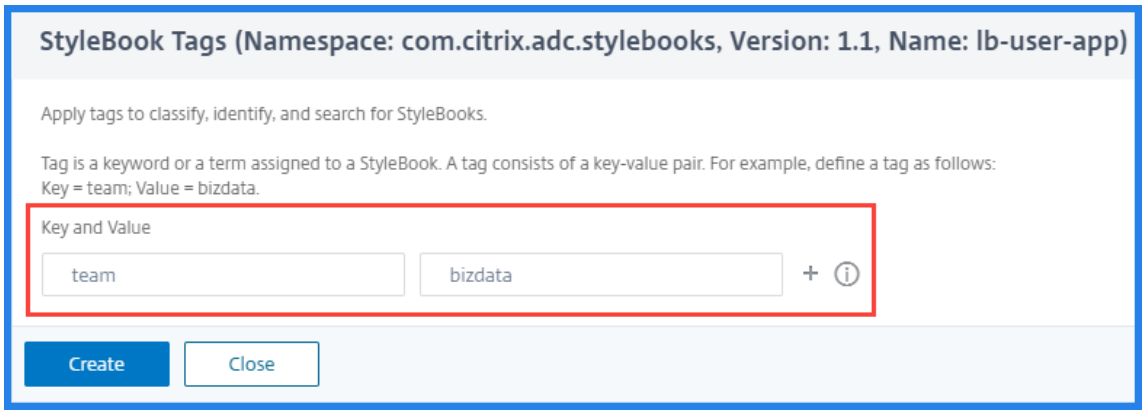
1. 导航到 应用程序 > 样本。
2. 在要为其添加 标签的样书上选择标签。



您可以向所有类型的样书添加标签。

3. 指定有助于筛选样本的所需 键和 值信息。

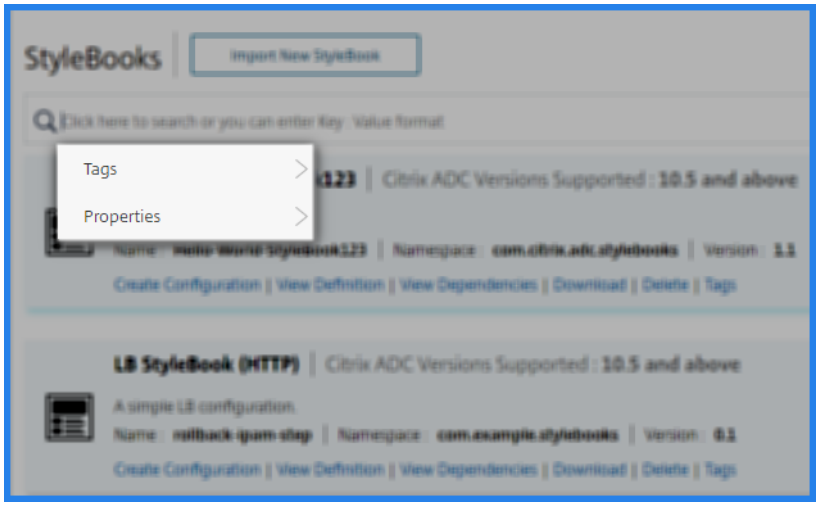
例如，键 = 团队和值 = Bizdata



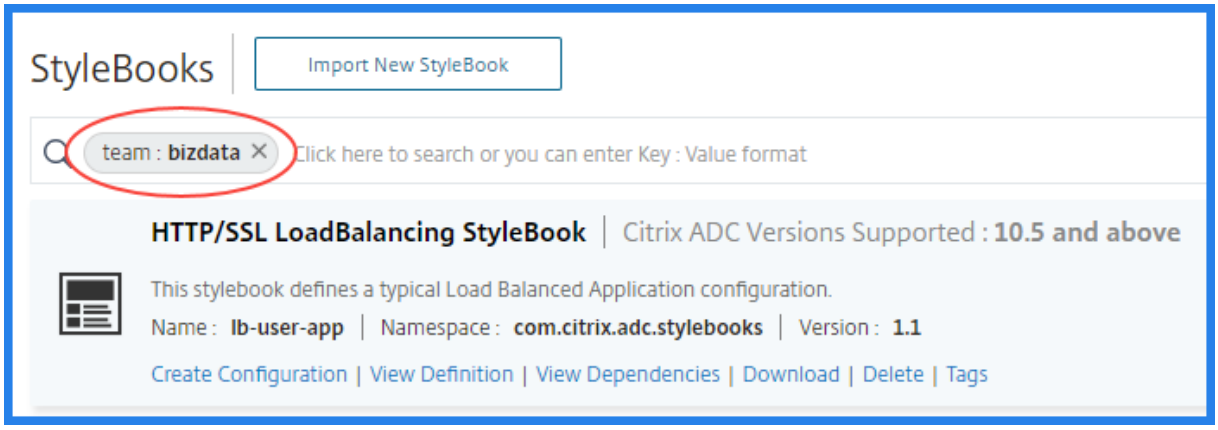
要添加更多标签，请单击 **+**。

4. 单击创建。

要使用标签过滤样书，请在搜索栏中单击“ 标签”，然后从列表中选择键和值。将显示与指定标签匹配的样书。



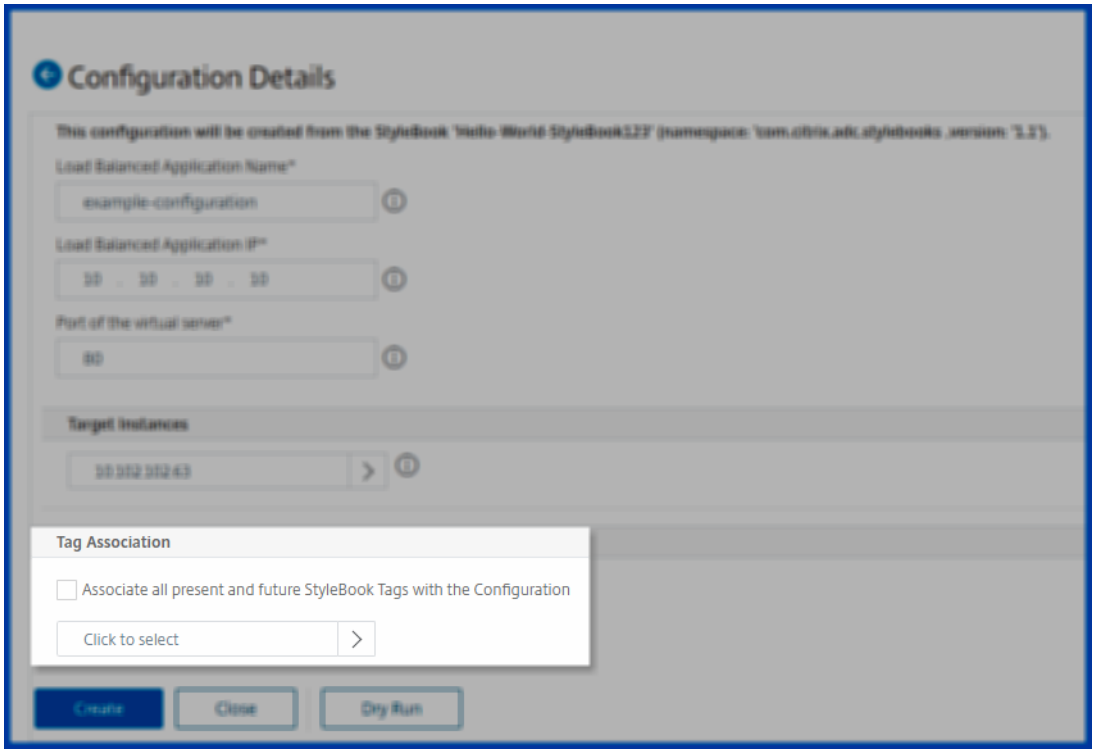
以下是搜索带有标签的样书的示例，其中包括 `key=team` 和 `value=bizdata`：



您可以将样书标签与其配置包相关联。因此，您可以使用样书标签本身搜索配置包。

创建配置包时，请使用“ 标签关联”部分中的以下选项之一：

- 将所有现在和未来的样书标签与配置关联 — 此选项将所有样书标签关联到配置包。它还可以确保将来可能添加到样书中的新标签关联起来。
- 选择标签 — 此选项显示所选样书的标签。您可以选择所需的样书标签并与配置包关联。



从 **GitHub** 存储库导入和同步样书

April 23, 2021

考虑使用 CI/CD 进程进行开发的场景。或者，您正在管理 GitHub 中的所有应用程序源代码和部署对象的场景。

在 GitHub 存储库中，您可能创建了多个样本来部署 Citrix ADC 配置和管理这些样本。Citrix 应用程序和交付管理 (ADM) 中也需要这些样本。现在，您可以直接将这些样本导入到 Citrix ADM 中。您无需从 GitHub 手动复制它们，然后将它们上传到 Citrix ADM 中，也无需手动同步 ADM 和 GitHub 中的文件。

现在，您可以在 Citrix ADM 中定义代表 GitHub 存储库的存储库。提供 GitHub 存储库 URL 以及您在 GitHub 中创建的用户名和密码（或 API 令牌）。这意味着，只有在 GitHub 中拥有有效帐户的授权用户才能导入和同步样本。

创建存储库后，您可以将 Citrix ADM 与您的 GitHub 存储库同步。Citrix ADM 连接到 GitHub 并导入在该存储库中找到的样本。然后，ADM 验证样本并将其添加到 Citrix ADM 中的样本列表中。如果样本无法验证，则不会添加到 Citrix ADM 中。更正错误并将更新版本提交到 GitHub 存储库中。稍后，您可以尝试将它们导入或将它们再次同步到 Citrix ADM 中。

> 注意
>
> - 样书文件可以从 GitHub 存储库的任何分支导入和同步。
> - 您可以导入和同步具有与其关联的相关样本的样本。

> - 必须从 Citrix ADM GUI 或 API 手动启动 GitHub 存储库中的样本同步。也就是说，目前，样本的导入和同步不会基于 GitHub 提交活动自动进行。

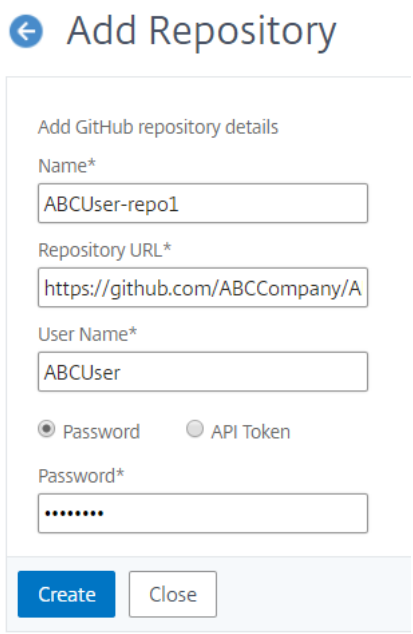
添加存储库并从 **GitHub** 存储库导入样书

在开始之前，请确保您在 GitHub 中有一个有效的帐户。

您可以从 GitHub 存储库中的任何文件夹将样书文件导入 ADM。

1. 在 Citrix ADM 中，导航到 应用程序 > 样本 > 存储库。
2. 单击添加。在 添加存储库窗口中，输入以下参数：
   - 名称。键入存储库的名称。此名称可以与 GitHub 中的存储库名称相同，也可以与其他名称相同。
   - 存储库 **URL**。键入 GitHub 存储库 URL。
   - 用户名和密码。键入用于访问 GitHub 帐户的用户名和密码。

   > 注意
   >
   > 您还可以提供 API 令牌来代替密码。API 令牌可以通过 HTTPS 使用代替 GitHub 的密码。有关如何为 GitHub 存储库创建 API 令牌的信息，请参阅的 GitHub 文档 创建个人访问令牌。
3. 单击创建。



   在 Citrix ADM 中创建存储库。
4. 要导入或同步样本，请在 “存储库” 页面中选择存 储库，然后单击 同步。

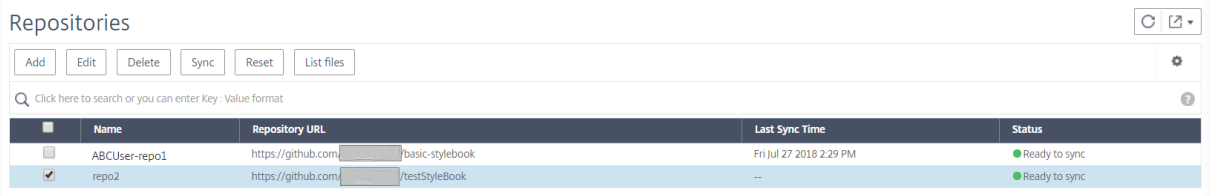
您可以在这里使用的其他操作是：

- 编辑。您可以编辑存储库 URL、用户名和密码（或 API 令牌）。

- 删除。您可以删除存储库以及 Citrix ADM 中存在的所有样本，这些样本是之前从该 GitHub 存储库导入的。

  > 注意
  >
  > 如果某个存储库具有与其关联的 ConfigPack 的任何样本，则无法从 Citrix ADM 中删除该存储库。首先，删除这些样本的所有配置包。您可以稍后从 Citrix ADM 中删除存储库以清除该存储库中的样本。

- 重置。您可以删除 Citrix ADM 中从该存储库同步的所有样本，而无需实际删除 Citrix ADM 中的存储库条目。
- 列出文件。您可以看到 Citrix ADM 中源自 GitHub 存储库的所有样本的列表。



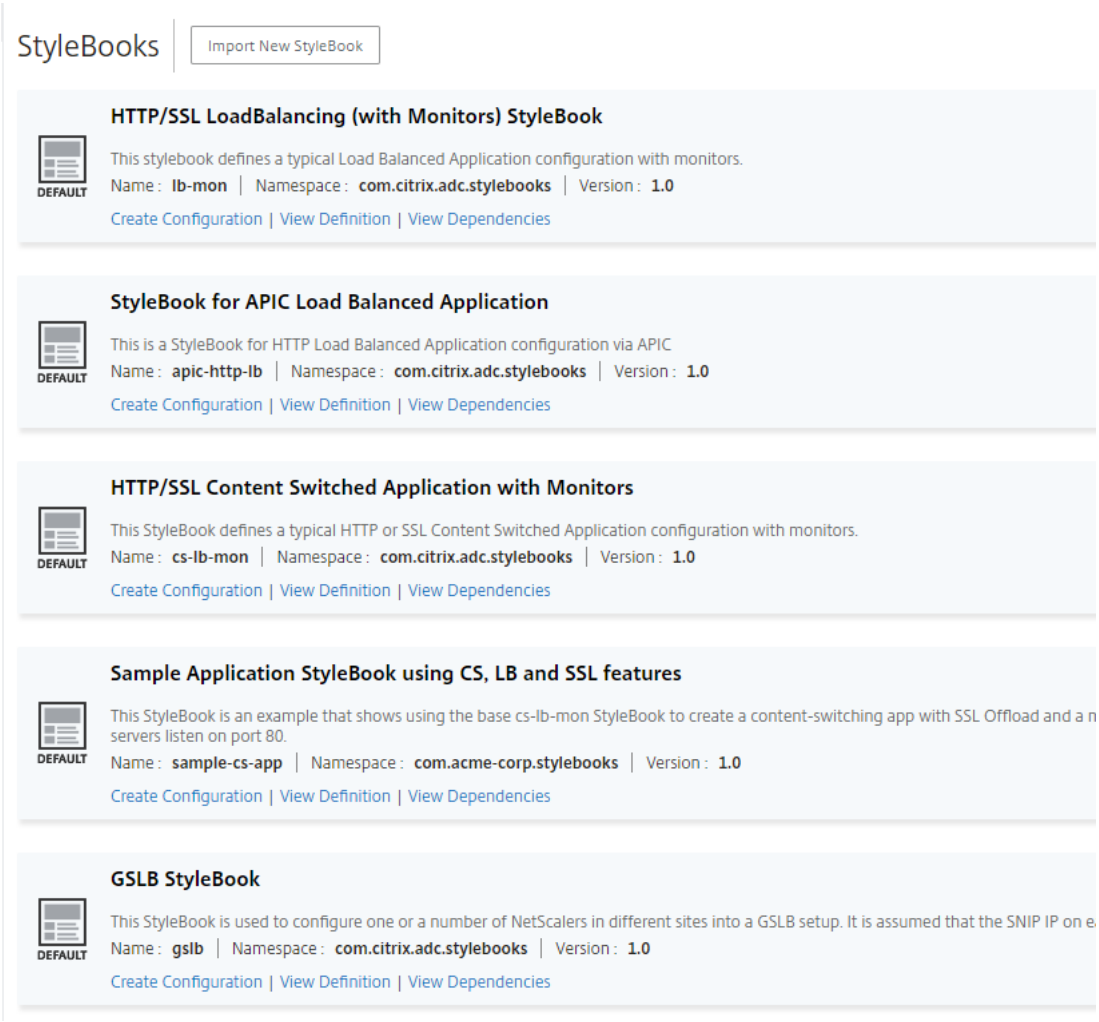
使用默认样本

April 23, 2021

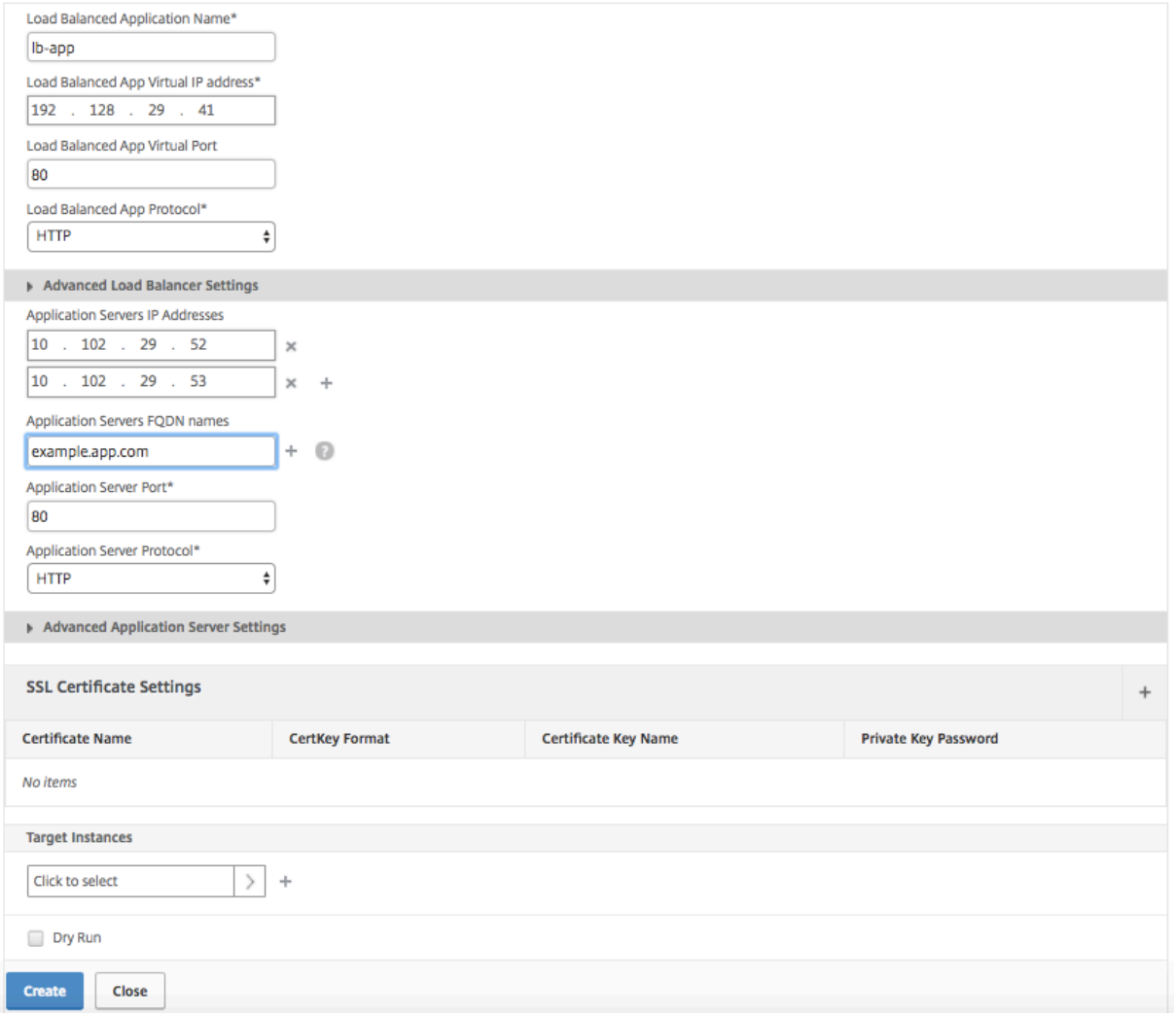
Citrix Application Delivery Management (ADM) 提供了一组默认样书。使用默认样本时，必须为样本中的参数指定值，并选择要在其中执行配置的 Citrix ADC 实例的 IP 地址。提交配置后，Citrix ADM 将验证您指定的参数值，创建配置图形，连接到 Citrix ADC 实例，并在实例上执行配置。

从默认样本创建配置

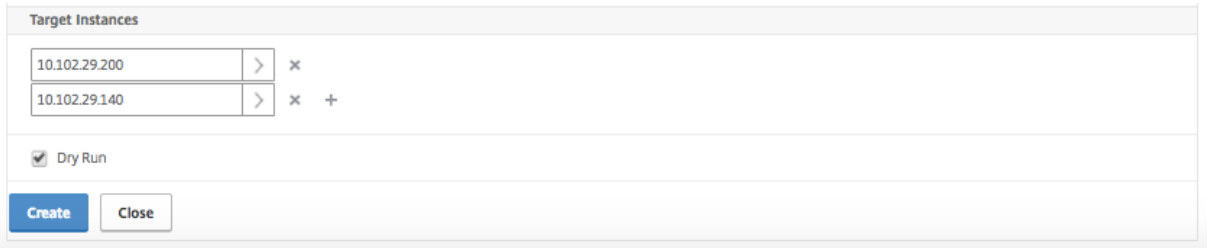
1. 导航至 “ 应用程序” > **“配置” > “**样书”。样本页面显示 Citrix ADM 中的所有样本。此列表包括默认样本和自定义样本。您可以在搜索字段中键入样本的名称，然后按 **Enter** 键。否则，你可以向下滚动列表以找到样书。



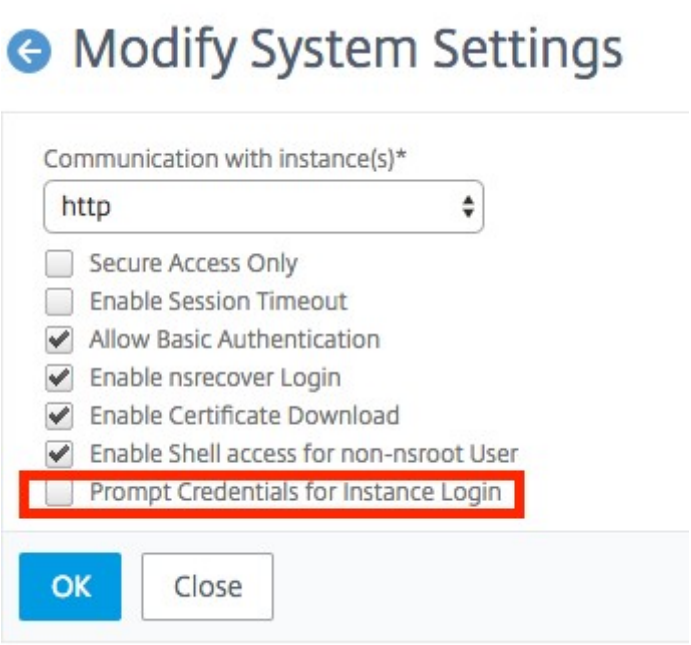
2. 单击“ 创建配置”。指定参数所需值。

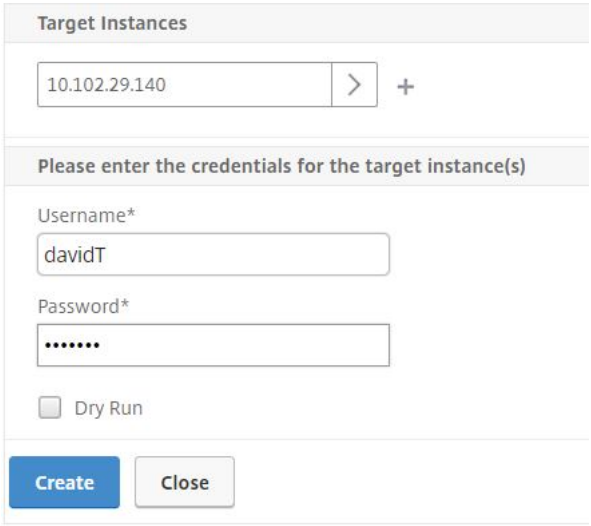


3. 在“ 目标实例”下，单击并选择要在其中执行配置的 Citrix ADC 实例的 IP 地址。如果要在多个实例上执行此配置，请单击“+”添加更多实例。

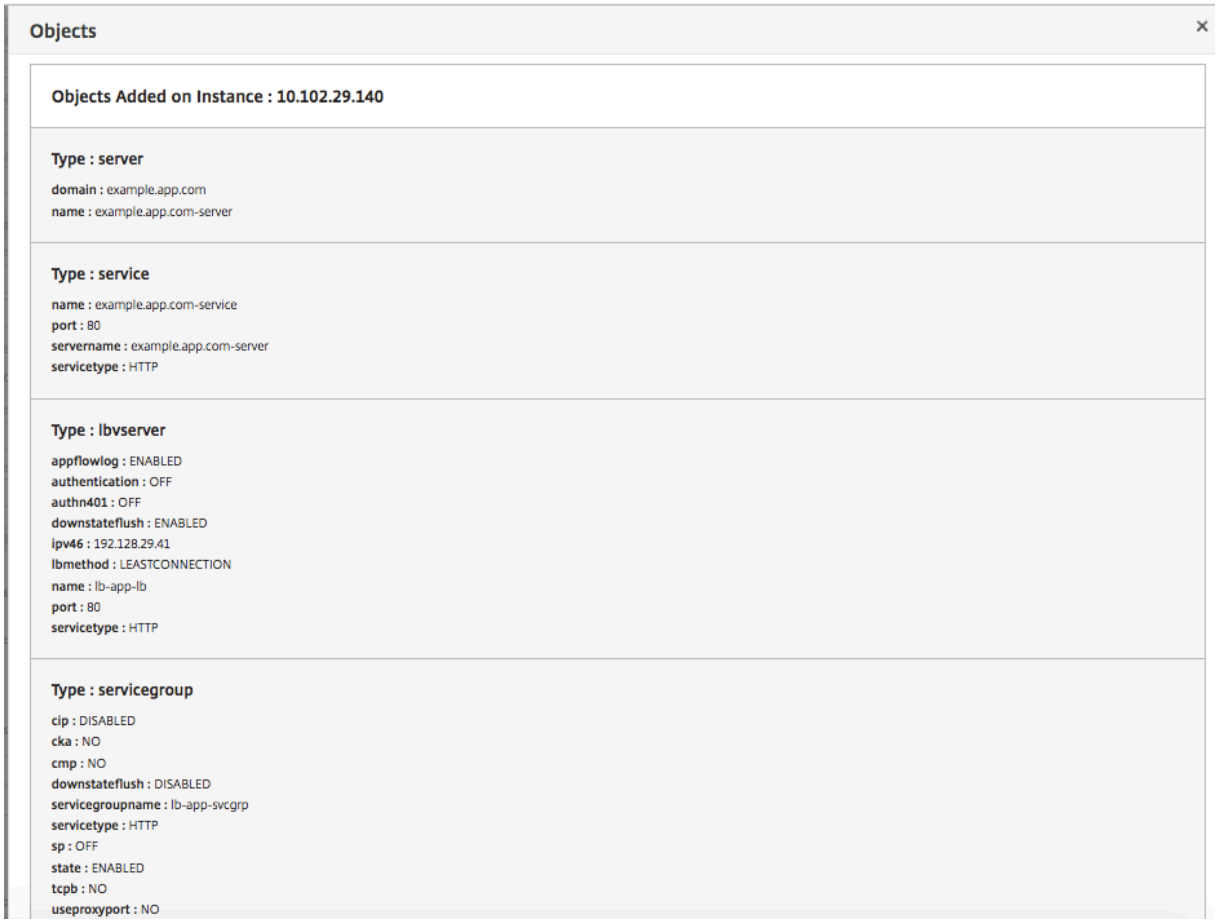


如果在 **Citrix ADM**> 系统 **>** 更改系统设置 **> **** 修改系统设置中启用了 **“**提示实例登录 ** 凭据”选项，则在执行配置中的所选 Citrix ADC 实例上的配置。否则，Citrix ADM 使用存储在实例配置文件中的实例凭据登录到实例。





如果要在 Citrix ADC 实例上执行配置之前测试或验证配置，请选择试运行，然后单击创建。如果配置有效，将显示根据您提供的值创建的对象。



4. 清除“ 干运行”复选框，然后单击“ 创建”以创建配置并在 Citrix ADC 实例上执行配置。您创建的样书配置将显示在配置列表中，如下所示。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

您现在可以使用 Citrix ADM 检查、更新或删除此配置包。

隐藏所有默认样本

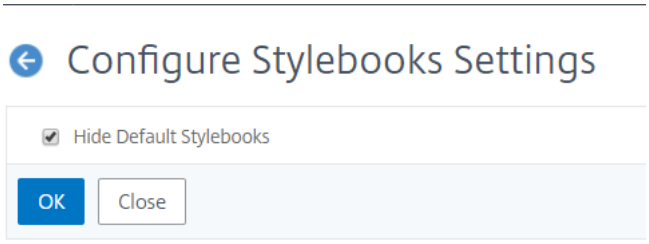
April 23, 2021

Citrix ADM 列出了 Citrix ADM 文件夹系统中存在的所有样本。样本列表包括默认和自定义样本，这些样本既可以是私有的，也可以是公有的。作为管理员，您可能希望隐藏所有默认样本。您可以允许用户仅查看和访问由您或用户构建的自定义样本。

Citrix ADM 允许您显示自定义样本，并隐藏随 Citrix ADM 一起随附的所有默认样本。提供了一个新的 GUI 选项，您可以在其中隐藏所有默认样本。

要隐藏所有默认样本：

1. 在 Citrix ADM 中，导航到 应用程序 > 配置**”** > **“**设置**”** 。
2. “ 设置**”** 页面显示默认样本是否对用户可见的信息。
3. 要隐藏默认样本，请单击右上角的编辑图标。
4. 在 配置样本设置页上，选择 隐藏默认样本选项。
5. 单击 “ 确定”。

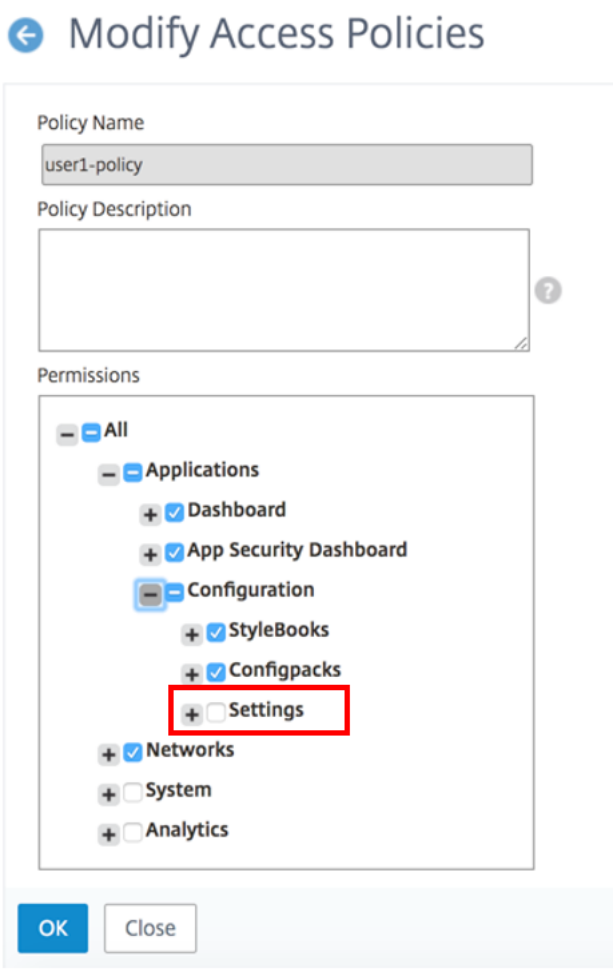


如果您没有选择使用 RBAC 功能隐藏页面，则 “ 配置样书设置” 页面仍然对用户可见。用户可能仍然可以选择取消隐藏默认样本。

要隐藏 “ 配置样书设置” 页，必须创建一个策略并将该策略分配给那些看不到默认样书的用户。

要创建 **RBAC** 策略，请执行以下操作：

1. 在 Citrix ADM 中，导航至 帐户**”** > **“**用户管理 > 访问策略”。
2. 单击 添加以创建策略。
3. 输入策略名称。
4. 在 “ 权限” 部分中，确保未选中 “ 所有” > “ 应用程序” > “ 配置**”** > **“**设置” 下，然后单击 “确定”。



创建策略后，您必须创建角色，将每个角色绑定到一个或多个策略，并将角色分配给用户组。要了解有关如何将策略与用户关联的更多信息，请参阅 配置基于角色的访问控制。

使用样本配置生成器迁移 **Citrix ADC** 应用程序配置

April 23, 2021

> 注意
>
> 此功能处于技术预览版中。

样本配置生成器用于从现有 Citrix ADC 配置创建应用程序配置样本。此功能还可自动将应用程序配置从一个 Citrix ADC 实例迁移到另一个实例。

使用配置生成器，您可以简化创建自定义样本的要求。通过此功能，您可以在无需深入了解样本语法和构造的情况下创建样本。否则，创建样本必须具备样本语法和构造的知识。

配置生成器还会创建一个在新 ADC 实例上反映相同 ADC 配置的 ConfigPack。使用此配置包，可以将一个 ADC 实例

的初始 ADC 配置复制到另一个 ADC 实例。初始配置源可以是以下之一：

- **Citrix ADC** 实例：指定托管要复制的应用程序配置的实例。

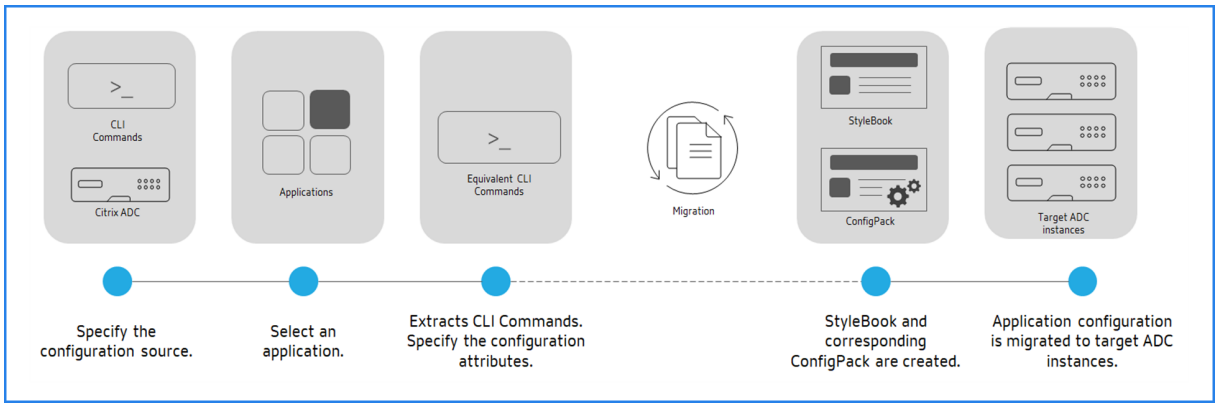
  即使您没有指定目标实例，配置生成器也会将 ADC 配置转换为样书和 ConfigPack。您可以稍后使用此配置包将 ADC 配置迁移到其他 ADC 实例。

- 一组 **CLI** 命令：从 `ns.conf` 或粘贴配置 `Application config`。

配置生成器标识源配置中嵌入的不同应用程序的列表。当您选择您感兴趣的应用程序配置时，配置生成器会提取所选应用程序的 CLI 命令集。这些 CLI 命令从源配置中提取。此外，它还标识可能需要输入的部署和配置属性。

- 部署属性 -您可以从原始配置中查看和编辑虚拟服务器、服务、服务组成员的 IP 地址和端口。
- 配置属性 -这些属性可以是在源配置中指定的口令或证书。

指定必要信息后，开始迁移或复制目标 ADC 实例上的应用程序配置。



完成应用程序创建和迁移后，将在 Citrix ADM 中创建一个 ConfigPack 及其相应的样书。此配置包表示目标 ADC 实例上的应用程序配置。要查看创建的 ConfigPack，请导航到应用程序 > 样本 > 配置。

支持的 **Citrix ADC** 功能

样本配置生成器可识别并支持源配置中的以下 Citrix ADC 功能：

- 内容交换
- 负载平衡
- 监视
- SSL 卸载
- 速率限制
- 重写
- 响应方
- Web 应用程序防火墙 (WAF)

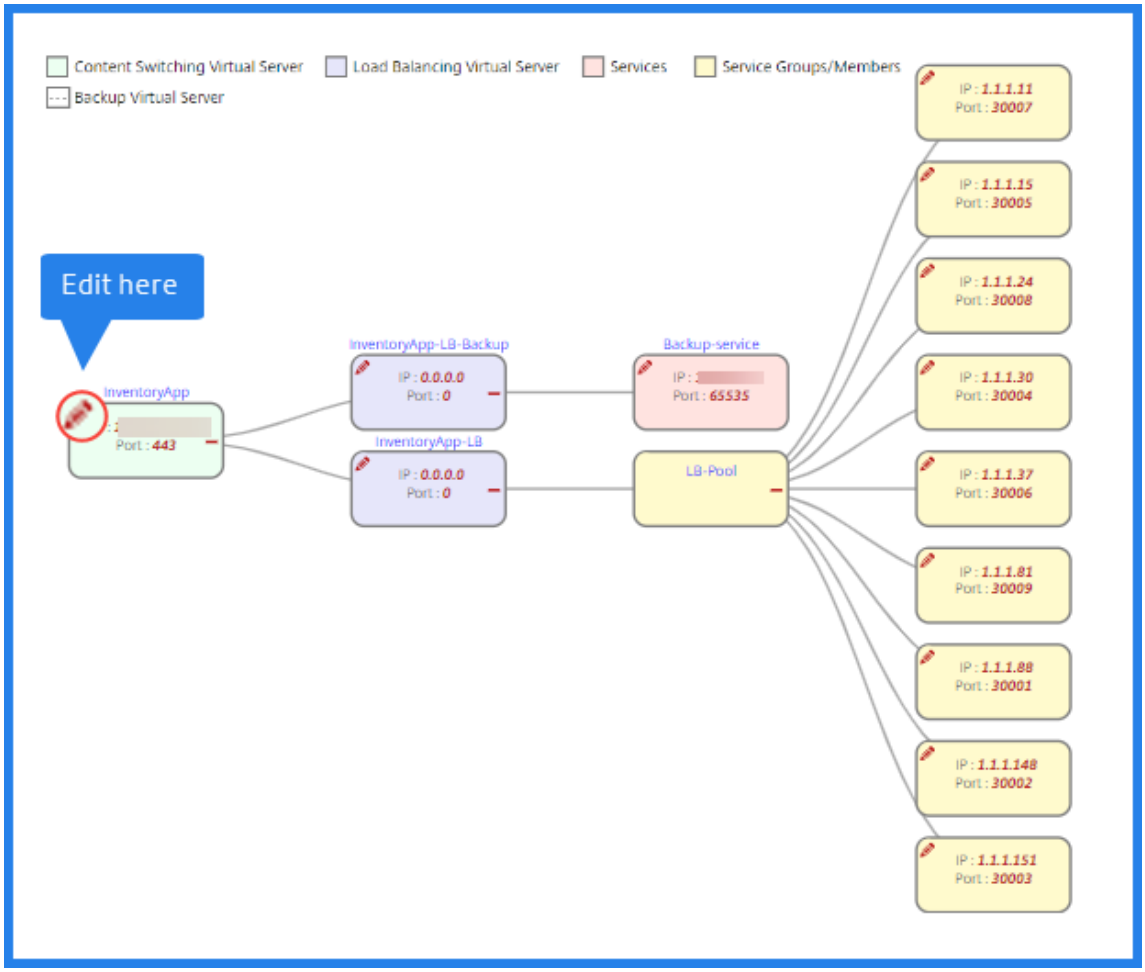
创建样本以迁移 **Citrix ADC** 应用程序配置

以下过程是创建样本，用于迁移 Citrix ADM 中的 Citrix ADC 应用程序迁移：

1. 导航到 应用程序 > 样本 > 配置。
2. 单击 迁移 **ADC** 配置。
3. 单击入门。
4. 在 指定配置中，选择配置源：
   - 从 **ADC** 导入：此选项可发现所选 ADC 实例上的活动应用程序。
   - 使用 **CLI** 命令导入：此选项分析 CLI 命令并从 CLI 命令中提取应用程序。
5. 指定要从中迁移或复制应用程序配置的 源 **ADC** 实例。
6. 指 定要迁移或复制应用程序配置的目标 **ADC** 实例。
7. 在 定义应用程序中，
   a) 在 应用程序名称中，指定应用程序的名称。
   b) 选择要迁移的虚拟服务器。
   c) 单击 “ 下一步”。
8. 在 等效 **CLI** 命令中，查看命令，然后单击 下一步。

   这些命令特定于所选应用程序配置。
9. 在 部署属性中，可以查看和编辑虚拟服务器、服务和服务组成员的 IP 地址和端口。

   要编辑 IP 地址和端口，请单击流程图中虚拟服务器、服务或服务组成员上的编辑图标。



此选项卡仅在以下情况下显示：

- 源实例和目标实例不同。
- 使用 CLI 命令导入配置。

10. 在 配置属性中，指定必要的详细信息，然后单击 下一步。

    此选项卡列出了密钥，例如用于解密密码和证书的密钥。

    > 注意：在开始迁移
    >
    > 之前，缺失或不支持的配置将显示在以下任一选项卡中：
    >
    > ** 不支持的配置
    >
    > 不支 ** 持的全局配置
    >
    > 要迁移这些配置成功，则必须在目标实例上单独应用缺失或不支持的配置。然后，单击 “ 下一步”。

11. 在 迁移中，指定所需的样书详细信息。单击 **Migrate**（迁移）。

限制

- 未标识源实例中 `responderhtmlpages` 提到的命名表达式。确保在迁移之前在目标实例 `responderhtmlpages` 上配置命名表达式和。
- 如果源具有配置 `servicegroup` 和监视绑定，如下所示：

  ```
  bind serviceGroup <Name> <Port> -monitorName <Monitor_Name>
  ```

  出现以下错误：

  ```
  1  CLI Command conversion failed: 100 - No such command [{
  2   "errorcode": 1090, "message": "No such argument [XXX]", "
        severity": "ERROR"  }
  3  ]
  4  <!--NeedCopy-->
  ```

  出现此错误的原因是 Citrix ADC 以无效的格式保存服务组和监视器之间的绑定。此问题已从 Citrix ADC 12.1.52.15 版本中修复。

SSO Google Apps 样本

April 23, 2021

Google Apps 是由谷歌开发的云计算、生产力和协作工具、软件和产品的集合。单一登录 (SSO) 使用户能够通过使用企业凭据对所有服务进行一次登录，访问其所有企业云应用程序（包括登录管理员控制台的管理员）。

通过 Citrix ADM SSO Google Apps 样书，您可以通过 Citrix ADC 实例为 Google Apps 启用 SSO。样本将 Citrix ADC 实例配置为 SAML 身份提供程序，用于对访问 Google Apps 的用户进行身份验证。

使用此样本为 Citrix ADC 实例中的 Google Apps 启用 SSO 会导致以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IdP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略
5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器

配置详细信息：

下表列出了此集成成功运行所需的最低软件版本。集成过程还将支持相同的更高版本。

产品	最低要求版本
Citrix ADC	11.0 版，高级/高级许可证

以下说明假定您已创建相应的外部或内部 DNS 条目，以将身份验证请求路由到 Citrix ADC 监控的 IP 地址。

部署 **SSO Google Apps** 样本配置：

以下任务可帮助您在您的业务网络中部署 Microsoft SSO Google Apps 样本。

部署 **SSO Google Apps** 样本

1. 在 Citrix ADM 中，导航到 “ 应用程序” > “ 配置” > “样书”。“ 样书” 页面显示可供您在 Citrix ADM 中使用的所有样书。向下滚动并找到 **SSO Google Apps** 样本. 单击 创建配置。
2. 样本将以用户界面页面形式打开，您可以在此为此样本中定义的所有参数输入值。
3. 输入以下参数的值：
    a) 应用程序名称。要在网络中部署的 SSO Google Apps 配置的名称。
    b) 验证虚拟 **IP** 地址。Google 应用 SAML IdP 策略绑定到的身份验证、授权和审核虚拟服务器使用的虚拟 IP 地址。
    c) **SAML** 规则表达式。默认情况下，使用以下 Citrix ADC 策略 (PI) 表达式：HTTP.REQ.HEADD（“引荐来源”）.CONTINES（“谷歌”）。如果您的要求不同，请使用其他表达式更新此字段。此策略表达式与应用这些 SAML SSO 设置的流量匹配，并确保推荐人标题来自 Google 域。
4. SAML IdP 设置部分允许您通过创建步骤 3 中创建的身份验证、授权和审核虚拟服务器使用的 SAML IdP 配置文件和策略，将 Citrix ADC 实例配置为 SAML 身份提供程序。
    a) **SAML** 发行者名称。在此字段中，输入身份验证虚拟服务器的公用 FQDN。示例：`https://<Citrix ADC Auth VIP>/saml/login`
    b) **SAML** 服务提供商 **(SP) ID**。（可选）Citrix ADC 身份提供程序接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。
    c) 断言消费者服务 **URL**。输入服务提供商的 URL，其中 Citrix ADC 身份提供商需要在成功用户身份验证后发送 SAML 断言。断言使用者服务 URL 可以在身份提供者服务器站点或服务提供者站点上启动。
    d) 您可以在此部分中输入其他可选字段。例如，您可以设置以下选项：
        i. SAML 绑定配置文件（默认为 “POST” 配置文件）。
        ii. 用于验证/签名 SAML 请求/响应的签名算法（默认为 “RSA-SHA1”）。
        iii. 为 SAML 请求/响应摘要哈希的方法（默认为 “SHA-1”）。
        iv. 加密算法（默认为 AES256）和其他设置。

> 注意
>
> Citrix 建议您保留默认设置，因为这些设置已经测试为与 Google Apps 兼容。

e) 您还可以启用用户属性复选框以输入用户详细信息，例如：

i. 用户属性的名称

ii. 为提取属性值进行评估的 Citrix ADC PI 表达式

iii. 用户友好的属性名称

iv. 选择用户属性的格式。

这些值包含在已发布的 SAML 断言中。您可以在 Citrix ADC 使用此样本发布的断言中包含多达五组用户属性。

5. 在 LDAP 设置部分，输入以下详细信息以验证 Google Apps 用户。要使域用户能够使用其公司电子邮件地址登录到 Citrix ADC 实例，您必须配置以下内容：

a) **LDAP**（**Active Directory**）基础。输入要允许身份验证的 Active Directory (AD) 中用户帐户所在的域的基本域名。例如 `dc=netscaler,dc=com`

b) **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，`cn=Manager,dc=netscaler,dc=com`

c) **LDAP**（**Active Directory**）绑定 **DN** 密码。输入域帐户的密码进行身份验证。

d) 您需要在本节中输入的其他一些字段如下：

i. Citrix ADC 连接到的用于对用户进行身份验证的 LDAP 服务器 IP 地址

ii. LDAP 服务器的 FQDN 名称

> 注意：
>
> 您必须至少指定上述两项中的一项-LDAP 服务器 IP 地址或 FQDN 名称。

iii. Citrix ADC 连接到的用于对用户进行身份验证的 LDAP 服务器端口（默认值为 389）。

iv. LDAP 主机名。如果验证处于打开状态（默认情况下，它处于关闭状态），则用于验证 LDAP 证书。

v. LDAP 登录名属性。用于提取登录名的默认属性是 “samAccountName。“

vi. 其他可选的其他 LDAP 设置

6. 在 SAML IdP SSL 证书部分，您可以指定 SSL 证书的详细信息：

a) 证书名称。输入 SSL 证书的名称。

b) 证书文件。从本地系统或 Citrix ADM 上的目录中选择 SSL 证书文件。

c) 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式是.pem 和.der 扩展名。

d) 证书密钥名称。输入证书私钥的名称。

e) 证书密钥文件。从本地系统或 Citrix ADM 中选择包含证书私钥的文件。

f) 私钥密码。如果您的私钥文件受密码保护，请在此字段中输入密码。

g) 您还可以启用“高级证书设置”复选框以输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。

7. 或者，如果上面输入的 SAML IdP 证书要求在 Citrix ADC 上安装 CA 公共证书，则可以选择 IdP SSL CA 证书。确保在高级设置中选择“是 CA 证书”。
8. 或者，您可以选择 SAML SP SSL 证书来指定用于验证来自 Google Apps (SAML SP) 的身份验证请求的谷歌 SSL 证书（公钥）。
9. 单击 目标实例”，然后选择要在其上部署此 Google Apps SSO 配置的 Citrix ADC 实例。单击 创建”以创建配置并在所选 Citrix ADC 实例上部署配置。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

此外，

> 提示
>
> Citrix 建议在运行实际配置之前，选择“干运行”以直观地确认样书在目标 Citrix ADC 实例上创建的配置对象。

SSO 办公室 365 样本

April 23, 2021

Microsoft™ Office 365 是 Microsoft 在订阅基础上提供的一套基于云的生产力和协作应用程序。它包括微软流行的基于服务器的应用程序，如交换、SharePoint、办公室和 Skype for Business。单点登录 (SSO) 使用户能够访问其所有企业云应用程序：

- 包括登录管理员控制台的管理员
- 使用其企业凭据对所有 Microsoft Office 365 服务进行一次性登录。

SSO Office 365 样本允许您通过 Citrix ADC 实例为 Microsoft Office 365 启用 SSO。现在，您可以将 SAML 身份验证配置为 Citrix ADC 作为 SAML 身份提供程序 (IdP)，并将 Microsoft Office 365 配置为 SAML 服务提供程序。

使用此样本在 Citrix ADC 实例中为 Microsoft Office 365 启用 SSO 涉及以下步骤：

1. 配置身份验证虚拟服务器
2. 配置 SAML IDP 策略和配置文件
3. 将策略和配置文件绑定到身份验证虚拟服务器
4. 在实例上配置 LDAP 身份验证服务器和策略

5. 将 LDAP 身份验证服务器和策略绑定到在实例上配置的身份验证虚拟服务器。

该表列出了此集成成功运行所需的最低软件版本。集成过程也应适用于相同的更高版本。

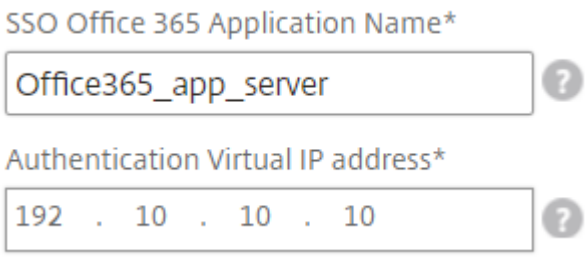
产品	最低要求版本
Citrix ADC	11.0, 高级/高级许可

以下说明假定您已经创建了相应的外部和内部 DNS 条目。这些条目对于将身份验证请求路由到 Citrix ADC 监视的 IP 地址至关重要。

以下说明可帮助您在业务网络中实施 SSO Office 365 样本。

部署 **SSO Microsoft Office 365** 样本

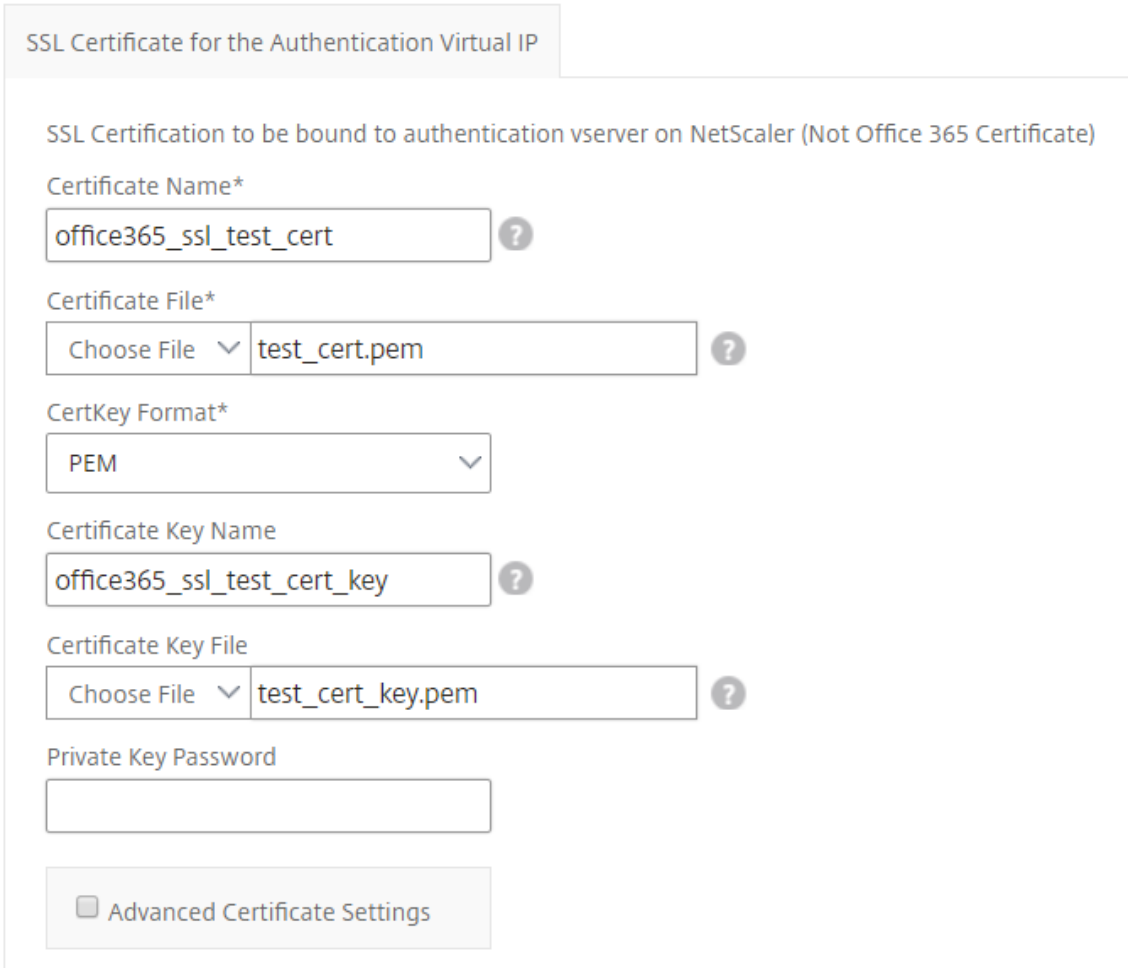
1. 在 Citrix Application Delivery Management (ADM) 中，导航到应用程序 > 样本。“ 样书” 页面显示可供您在 Citrix ADM 中使用的所有样书。向下滚动并找到 **SSO Office 365** 样本。单击 创建配置。
2. 样本将以用户界面页面形式打开，您可以在此为此样本中定义的所有参数输入值。
3. 输入以下参数的值：
   a) 应用程序名称。要在网络中部署的 SSO Microsoft Office 365 配置的名称。
   b) 验证虚拟 **IP** 地址。虚拟 IP 地址将被绑定到 Microsoft Office 365 SAML IdP 策略的 AAA 虚拟服务器使用。



4. 在 **SSL** 证书设置部分，输入 SSL 证书和证书密钥的名称。

> 注意
>
> 这不是 Office 365 服务提供商证书。此 SSL 证书绑定到 Citrix ADC 实例上的虚拟身份验证服务器。

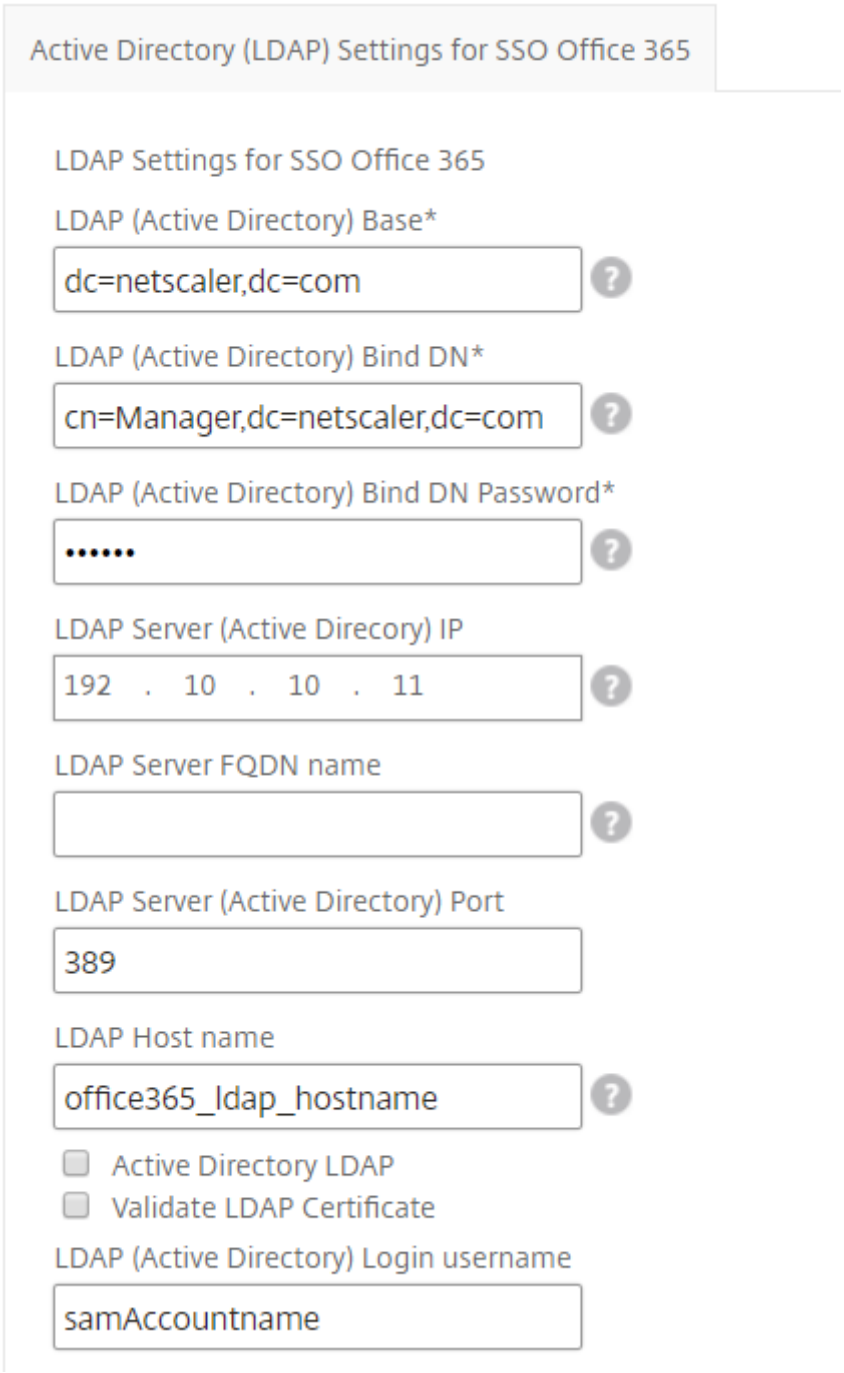
5. 从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以加载 PEM 格式的加密私钥。



6. 您还可以启用 高级证书设置” 复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。
7. （可选）如果 **SSL** 证书要求在 **Citrix ADC** 上安装 **CA** 公共证书，则可以为身份验证虚拟 IP 选中 SSL CA 证书。确保在上面的 “ 高级证书设置” 部分中选择 “是 **CA** 证书”。
8. 在 **SSO Office 365** 的 **LDAP** 设置部分中，输入以下详细信息以验证 Office 365 用户。要允许域用户使用其公司电子邮件地址登录到 Citrix ADC 实例，请配置以下内容：
   - **LDAP**（**Active Directory**）基础。输入用户帐户驻留在 Active Directory (AD) 中的域的基本域名以允许身份验证。例如，dc=netscaler,dc=com
   - **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，cn=Manager,dc=netscaler,dc=com
   - **LDAP**（**Active Directory**）绑定 **DN** 密码。输入域帐户的密码进行身份验证。
   - 您需要在本节中输入的其他一些字段如下：
     - Citrix ADC 连接到的 LDAP 服务器 IP 地址，用于对用户进行身份验证。
     - LDAP 服务器的 FQDN 名称。

> 注意：
>
> 您必须至少指定上述两项中的一项-LDAP 服务器 IP 地址或 FQDN 名称。

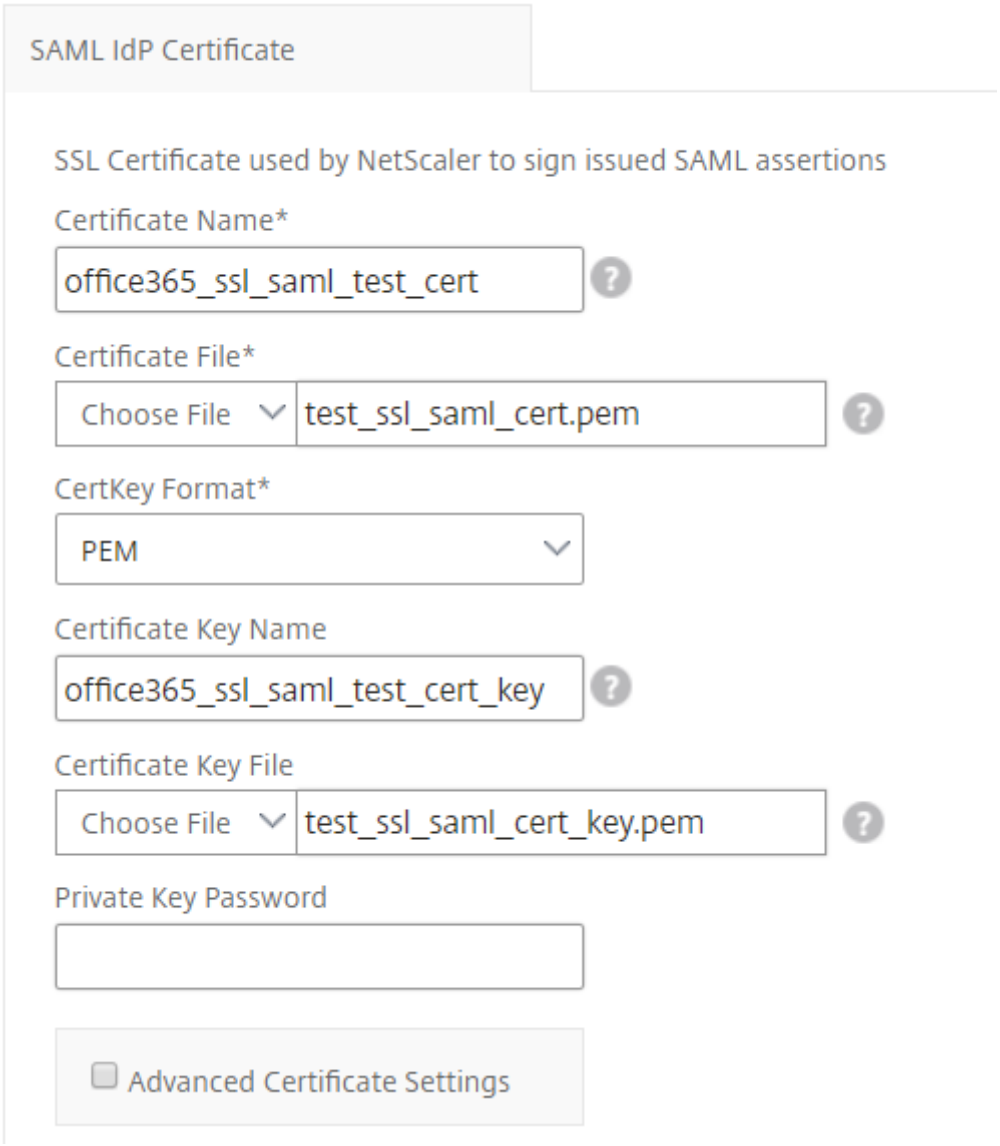
- Citrix ADC 连接到的用于对用户进行身份验证的 LDAP 服务器端口（默认值为 389）。LDAPS 使用 636。
- LDAP 主机名。如果打开了验证（默认情况下，它处于关闭状态），则使用主机名验证 LDAP 证书。
- LDAP 登录名属性。用于提取登录名的默认属性为“三帐户名称”。“
- 其他可选的其他 LDAP 设置。



9. 在 **SAML IdP** 证书部分，可以指定用于 SAML 断言的 SSL 证书的详细信息。
   - 证书名称。输入 SSL 证书的名称。
   - 证书文件。从本地系统的目录中选择 SSL 证书文件。
   - 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式为.pem 和.der 文件扩展名。
   - 证书密钥名称。输入证书私钥的名称。

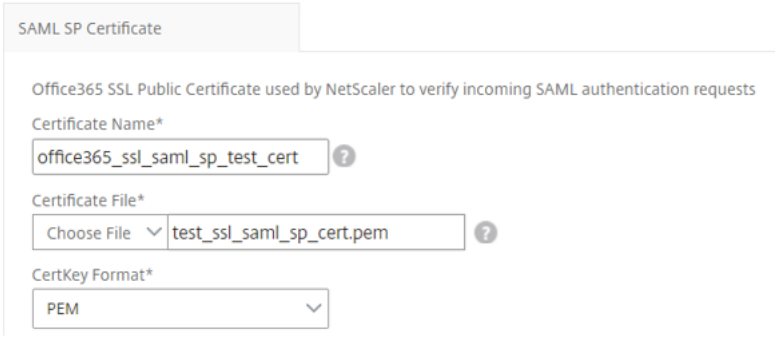
- 证书密钥文件。从本地系统中选择包含证书私钥的文件。
- 私钥密码。键入用于保护私钥文件的密码。

您还可以启用 高级证书设置”复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。



10. 或者，如果上面输入的 **SAML IdP** 证书要求在 Citrix ADC 上安装 CA 公共证书，则可以选择 SAML IdP CA 证书。确保在上面的 “ 高级证书设置” 部分中选择了 “是 CA 证书”。
11. 在 **SAML SP** 证书部分中，输入 Office 365 SSL 公共证书的以下详细信息。Citrix ADC 实例使用此证书来验证传入的 SAML 身份验证请求。
    - 证书名称。键入 SSL 证书的名称。
    - 证书文件。从本地系统的目录中选择 SSL 证书文件。

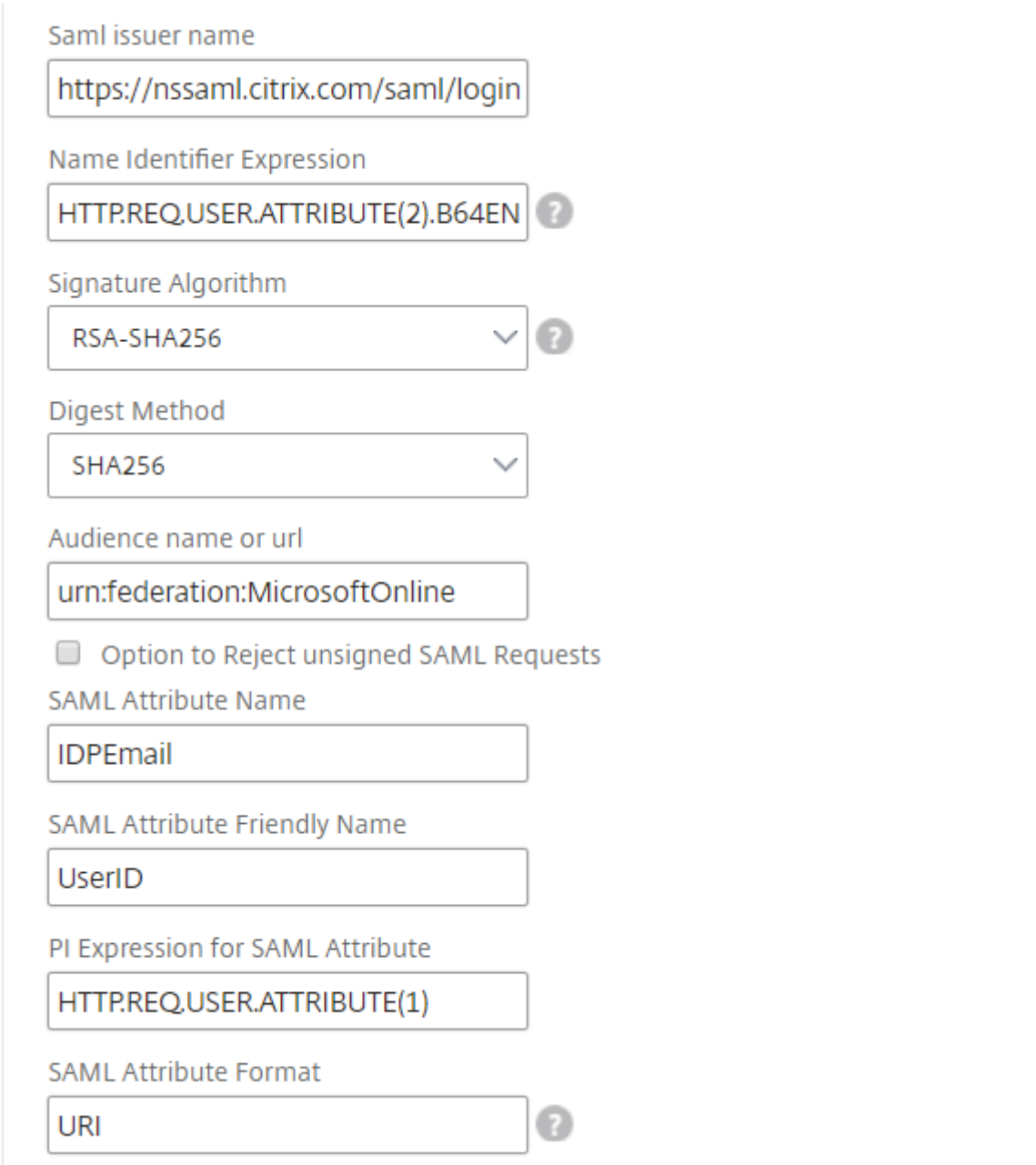
- 证书密钥格式。从下拉列表框中选择证书和私有密钥文件的格式。支持的格式为.pem 和.der 文件扩展名。
- 您还可以启用 高级证书设置”复选框。您可以在此输入详细信息，例如证书到期通知期限，启用或禁用证书到期监视器。



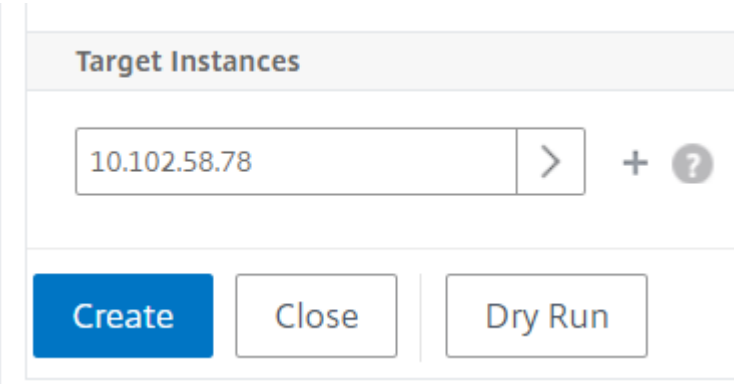
12. 通过“ **SAML Idp** 设置”部分，您可以将 Citrix ADC 实例配置为 SAML 身份提供程序，方法是创建由步骤 3 中创建的 AAA 虚拟服务器使用的 SAML IDP 配置文件和策略。
    - **SAML** 发行者名称。在此字段中，键入身份验证虚拟服务器的公用 FQDN。示例：`https://<Citrix ADC Auth VIP>/saml/login`
    - 名称标识符表达式。键入 Citrix ADC 表达式，该表达式将进行评估，以提取 SAML 断言中发送的 SAML 名称标识符。示例：`"HTTP.REQ.USER.ATTRIBUTE(2).B64ENCODE"`
    - 签名算法：选择验证/签名 SAML 请求/响应的算法（默认为“RSA-SHA256”）。
    - 摘要方法。选择用于摘要 SAML 请求/响应的哈希的方法（默认为“SHA256”）。
    - 受众姓名。键入代表服务提供商（Microsoft Office 365）的实体名称或 URL。
    - **SAML** 服务提供商 **(SP) ID**。（可选）Citrix ADC 身份提供程序接受来自与此 ID 匹配的颁发者名称的 SAML 身份验证请求。
    - 断言消费者服务 **URL**。输入服务提供商的 URL，其中 Citrix ADC 身份提供商需要在成功用户身份验证后发送 SAML 断言。断言使用者服务 URL 可以在身份提供者服务器站点或服务提供者站点上启动。
    - 您可以在此部分中输入其他可选字段。例如，您可以设置以下选项：
      - **SAML** 属性名称。SAML 断言中发送的用户属性的名称。
      - **SAML** 属性友好名称。SAML 断言中发送的用户属性的友好名称。
      - **SAML** 属性的 **PI** 表达式。默认情况下，使用以下 Citrix ADC 策略 (PI) 表达式：HTTP.REQ.USER.ATTRIBUTE(1)。此字段指定从 LDAP 服务器 (mail) 发送的第一个用户属性作为 SAML 身份验证属性。
      - 选择用户属性的格式。

    这些值包含在已发布的 SAML 断言中。

> 提示
>
> Citrix 建议您保留默认设置，因为这些设置已经测试可与 Microsoft Office 365 应用程序配合使用。



13. 单击 目标实例，然后选择要在其上部署此 Microsoft Office 365 SSO 配置的 Citrix ADC 实例。单击 创建” 以创建配置并在所选 Citrix ADC 实例上部署配置。



> 提示
>
> Citrix 建议在执行实际配置之前，选择干运行以查看样书在目标 Citrix ADC 实例上创建的配置对象。

Microsoft Skype for Business 样本

April 23, 2021

Skype for Business 2015 应用程序的运行需要依赖于多个外部组件。Skype for Business 网络由多个系统组成，例如，服务器及其操作系统、数据库、身份验证和授权系统、网络系统和基础结构以及电话 PBX 系统。Skype for Business Server 2015 有两个版本：标准版和企业版。主要差别是对高可用性功能的支持，只有企业版中提供这些功能。要实现高可用性，必须为池部署多个前端服务器，以及必须镜像 SQL 服务器。

通过企业版部署，可以创建多个具有不同角色的服务器。

主要组件

Skype for Business 2015 应用程序中的主要组件如下：

- 前端服务器
- 边缘服务器
- Director 服务器
- 数据库 (SQL) 服务器

前端服务器

在 Skype for Business 应用程序中，前端服务器是您的网络中的核心服务器。它为用户身份验证、注册、联机状态、通讯簿、A/V 会议、应用程序共享、即时消息和网络会议提供链接和服务。如果您要部署 Skype for Business 2015 企业版，则拓扑通常至少包含两个在具有数据库服务器的前端池中平衡负载的前端服务器，该数据库服务器托管存放 Skype for Business 数据库的 SQL 服务器实例。

边缘服务器

如果未登录到组织的内部网络的外部用户需要能够与内部用户进行交互，则必须为 Skype for Business 部署边缘服务器。这些外部用户可能是经过身份验证的匿名远程用户、联盟的合作伙伴或其他移动客户。

Skype For Business 边缘服务器中有四种类型的角色：

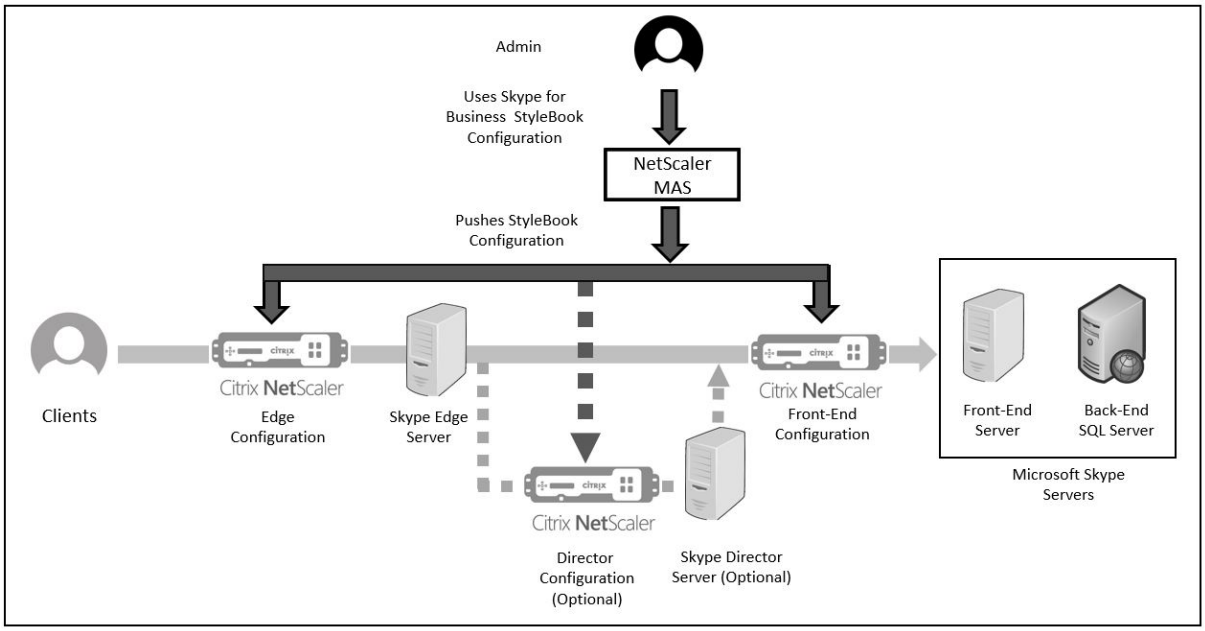
- 接入边缘处理 SIP 流量并验证外部连接，允许远程连接并允许联合连接
- Web Conferencing（网络会议），用于处理数据会议数据包以及允许外部用户访问 Skype for Business
- A/V Conferencing（A/V 会议），用于处理 A/V 会议数据包，以及将音频和视频、应用程序共享和文件传输扩展到外部用户
- XMPP Proxy（XMPP 代理），用于处理 XMPP 数据包，以及允许基于 XMPP 的服务器或客户端连接到 Skype for Business。

Director 服务器

在 Skype for Business 2015 中 Director 服务器的主要功能是对端点进行身份验证，以及将用户“导向”至包含其帐户的池。在 Skype for Business 2015 中，尽管 Director 是独立服务器上完全专用的特定角色，但它是可选服务器。这样，可以更加轻松地部署或删除配置，从而方便实现安全性。

存在多个池的情况下，Director 非常有用，因为它们为端点身份验证提供单点联系。此外，对于远程用户，Director 用作边缘池与前端池之间的附加跃点，从而添加了额外的一层保护来抵御攻击。

下图以图解方式表示了 Skype 服务器在网络中的部署：



在企业中配置 **Citrix ADC** 实例

下表列出了下面的说明中包含的示例配置中使用的 IP 地址：

Skype for Business 服务器	虚拟 IP 地址	服务器 IP 地址	Citrix ADC 实例
边缘服务器	外部 VIP - 192.20.20.20	192.20.21；	10.102.29.141
	内部 VIP - 10.10.10.20	十一月十二日	
前端服务器	10.10.10.10	十一月十一日；	10.102.29.60
Director 服务器	10.10.10.30	10.10.31；	10.102.29.93

配置前端服务器

1. 在 Citrix Application Delivery Management (ADM) 中，导航到应用程序 > 配置，然后单击新建。“ 选择样本页面显示了 Citrix ADM 中可供您使用的所有样本。向下滚动并选择 **Microsoft Skype for Business 2015** 样本。样本将以用户界面页面形式打开，您可以在此为此样本中定义的所有参数输入值。
2. 在 边缘服务器部分中，输入网络中所有边缘服务器的以下虚拟 IP (VIP) 地址和 IP 地址。
   a) 将用于访问边缘、网络会议边缘和 A/V 边缘的边缘服务器的外部 VIP 地址和 IP 地址。
   b) 将连接到内部网络的边缘服务器的内部 VIP 地址和 IP 地址。
   c) 您的网络中的两个外部和两个内部边缘服务器。
3. 在前端服务器部分中，输入要为 Skype for Business 前端服务器创建的虚拟前端服务器 (VIP) 的 IP 地址。此外，输入网络中所有 Skype for Business 前端服务器的 IP 地址。
4. 在 **Director Server**（Director 服务器）部分中，输入要为 Skype for Business 应用程序创建的 Director 服务器的虚拟 IP 地址 (VIP)。此外，还输入网络中所有 Skype for Business Director 服务器的 IP 地址。至少创建两个 Director 服务器以实现高可用性。
5. **“** 高级设置**”** 部分列出了在 Citrix ADC 实例上为三台 Skype 服务器配置的所有默认端口。

下表提供了所有默认端口和协议的列表：

标签	端口	协议	说明
HTTP 端口	80	HTTP	用于在未使用 HTTPS 时从前端服务器到 Web 场 FQDN 的通信。
HTTPS 端口	443	HTTPS	用于从前端服务器到 Web 场 FQDN 的通信。
自动发现内部端口	4443	HTTPS	用于自动发现登录的 HTTPS（从反向代理）和 HTTPS 前端池间通信。
RPC 端口	135	DCOM 和远程过程调用 (RPC)	用于基于 DCOM 的操作，例如移动用户、用户复制器同步以及通讯簿同步。

标签	端口	协议	说明
SIP 端口	5061	TCP (TLS)	由前端服务器用于所有内部 SIP 通信。
SIP Focus 端口	444	HTTPS、TCP	用于 Focus（管理 Skype 会议状态的组件）与单个服务器之间的 HTTPS 通信。
SIP 组端口	5071	TCP	用于响应组应用程序的传入 SIP 请求。
SIP 应用程序共享端口	5065	TCP	用于传入 SIP 侦听请求以进行应用程序共享。
SIP 参与人员端口	5072	TCP	用于参与人员的传入 SIP 请求（即用于调用拨入式会议）。
SIP 会议公告端口	5073	TCP	用于 Skype for Business 服务器会议公告服务的传入 SIP 请求（即用于调用拨入式会议）。
SIP CallPark 端口	5075	TCP	用于 CallPark 应用程序的传入 SIP 请求。
SIP 调用允许端口	448	TCP	用于 Skype for Business 服务器带宽策略服务实施的调用允许控制。
SIP 调用允许 TURN 端口	5080	TCP	用于带宽策略服务针对音频/视频边缘 TURN 流量实施的调用允许控制。
SIP 音频测试端口	5076	TCP	用于音频测试服务的传入 SIP 请求。
HTTPS 外部端口	443	HTTPS	用于以下情况的外部端口：远程用户访问的 SIP/TLS 通信、访问内部网络会议，以及访问内部媒体和 A/V 会话的 STUN/TCP 入站和出站媒体通信。

标签	端口	协议	说明
HTTPS 内部端口	443	HTTPS	用于以下情况的内部端口：远程用户访问的 SIP/TLS 通信、访问内部网络会议，以及访问内部媒体和 A/V 会话的 STUN/TCP 入站和出站媒体通信。
SIP 外部远程访问端口	5061	TCP	用于远程用户访问或联合的 SIP/MTLS 通信的外部端口。
SIP 内部远程访问端口	5061	TCP	用于远程用户访问或联合的 SIP/MTLS 通信的内部端口。
SIP 外部 STUN UDP 端口	3478	UDP	用于 STUN/UDP 入站和出站媒体通信的外部端口。
SIP 内部 STUN UDP 端口	3478	UDP	用于 STUN/UDP 入站和出站媒体通信的内部端口。
SIP 内部 IM 端口	5062		用于通过内部防火墙传输的出站 IM 通信的 SIP/MTLS 身份验证的内部端口。
HTTP 端口	80	TCP	用于从 Director 到 Web 场 FQDN 的初始通信。
HTTPS 端口	443	HTTPS	用于从 Director 到 Web 场 FQDN 的通信。
自动发现内部端口	4443	HTTPS	用于自动发现登录的 HTTPS（从反向代理）和 HTTPS Director 池间通信。
SIP 内部端口	5061	TCP	用于服务器与客户端连接之间的内部通信。

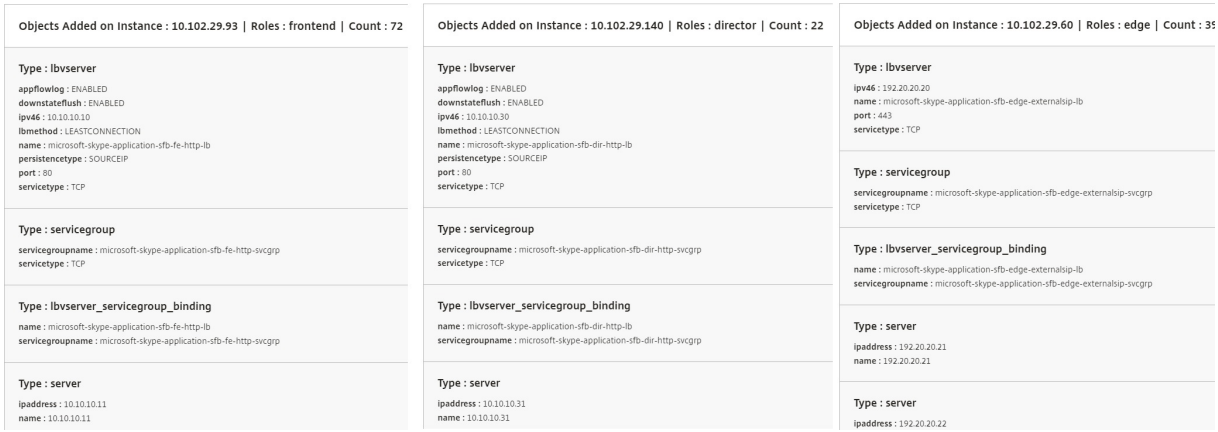
6. 在“目 标实例”部分中，选择要在其上部署三个适用于业务服务器的 Skype 的三个不同的 Citrix ADC 实例。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

7. 单击创建可在选定的 Citrix ADC 实例上创建配置。

> 提示
>
> Citrix 建议您选择干运行以检查必须在目标实例上创建的配置对象，然后再对实例执行实际配置。
>
> 成功创建配置后，样本将创建 25 个负载平衡虚拟服务器。即，对于每个端口，均定义一个负载平衡虚拟服务器以及一个服务组，且服务组绑定到负载平衡虚拟服务器。此外，该配置还将前端服务器添加为服务组成员，并将其绑定到服务组。创建的服务组成员数等于创建的前端服务器数。

下图显示了每个服务器中创建的对象：



配置 **Microsoft Exchange** 样本

April 23, 2021

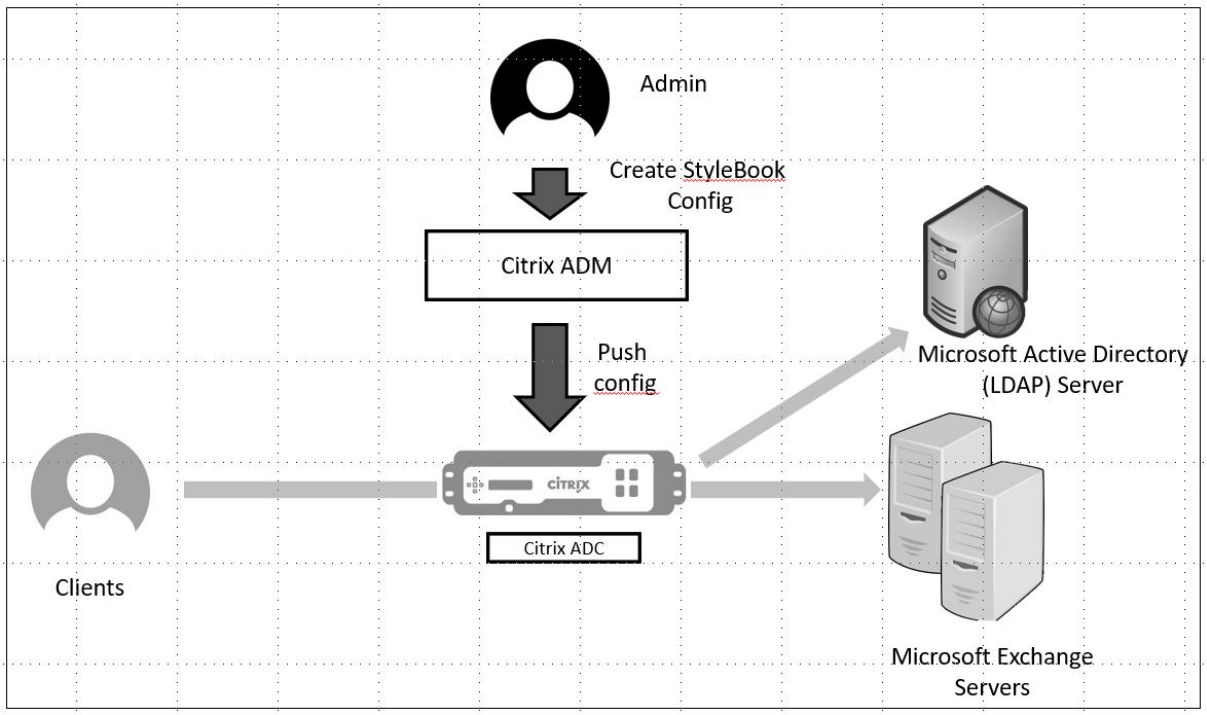
您可以使用 Microsoft Exchange 2016 样本来部署 Citrix ADC 配置，从而对您的网络中的 Microsoft Exchange 2016 企业应用程序进行优化和保护。Microsoft Exchange 2016 是关键的企业应用程序，用于为您的员工和其他利益干系人提供电子邮件、个人信息管理和消息传送服务。

使用 **Microsoft Exchange** 样本配置的 **Citrix ADC** 功能

Microsoft Exchange 2016 样书启用和配置以下 Citrix ADC 功能的 Microsoft Exchange 2016 服务器：

- 负载平衡 - 实现对多个 Exchange 服务器进行负载平衡的基本负载平衡功能
- 内容交换 - 实现对正确的负载平衡虚拟服务器进行单个 IP 访问，以及将查询重定向到正确的负载平衡虚拟服务器
- 重写 - 将用户重定向到安全页面
- SSL 卸载-将 SSL 处理卸载到 Citrix ADC，从而减少 Exchange 服务器上的负载

下图以图解方式表示了 Exchange 服务器在网络中的部署：



必备条件

- 对于基于证书的身份验证，属于网络设置一部分的所有可寻址主机均必须有可解析的域名，而不只是 IP 地址。
- 请确保可以在 Microsoft Exchange 2016 服务器中访问 SIP 端口。

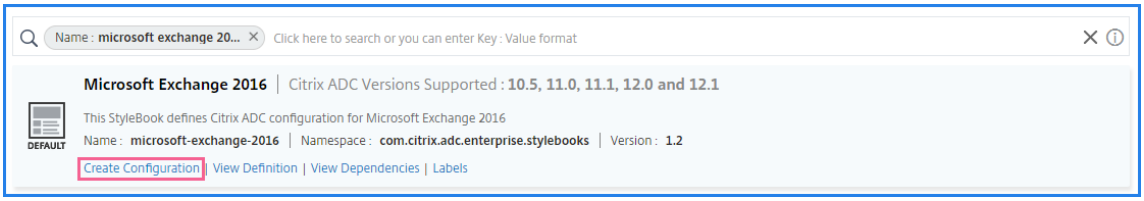
配置 **Microsoft Exchange** 样本

在您的企业中配置 Microsoft Exchange 样本以部署 Citrix ADC 配置。

配置 **Microsoft Exchange** 应用程序

1. 在 Citrix ADM 中，导航到 应用程序 > 样本。
2. 搜索 **Microsoft Exchange 2016** 样本，然后单击创建配置。

   样本以用户界面表单形式显示，您可以在此为此样本中定义的所有参数输入值。



3. 输入以下参数的详细信息：

- 交换应用程序名称-网络中的 Microsoft Exchange 应用程序的名称
- 交换 **V** IP-Citrix ADC 上的虚拟 IP 地址，用于接收 Microsoft Exchange 应用程序的客户端请求
- **Exchange Server IP** -网络中所有 Exchange 服务器的 IP 地址。

  如果要添加更多 IP 地址，请单击加号 **(+)** 图标。通常，网络中配置两个 Exchange 服务器。

4. 在“交 换证书部分中，将交换证书上载到 Citrix ADM。输入证书和密钥文件的名称，然后从本地存储器上传。您还可以提供私钥密码来加密密钥文件。

   > 注意
   >
   > 确保证书文件是 “.pem” 或 “.der” 格式。Citrix ADM 拒绝其他格式的文件。

   如果要指定证书过期详细信息或任何高级设置，请选择 高级证书设置”。

5. 在 **Exchange Active Directory** 身份验证配置部分，通过输入数据来配置 AD 设置。
   - **Active Directory** 身份验证 **V**IP-用于在 Citrix ADC 装置上创建和配置 AD (LDAP) 虚拟服务器的虚拟 IP 地址。
   - **Active Directory** 服务器 **IP**-Active Directory 域 Controller 的 IP 地址。
   - **Active Directory** 基本字符串-Active Directory 中的 LDAP 基本字符串。例如，CN=Users,DC=CTXNSSFB,DC=CO
   - **Active Directory LDAP** 绑定唯一判别名 **(DN)** -LDAP 绑定唯一判别名 (DN) 用于将此对象绑定到 LDAP 服务器 (AD)。例如 cn=Administrator,cn=Users,dc=acme,dc=com
   - **Active Directory LDAP** 绑定唯一判别名 **(DN)** 密码 -LDAP 绑定唯一判别名 (DN) 是 AD 身份验证的密码
   - **Active Directory** 用户名属性-用户名的 AD 属性。Citrix ADC 使用 LDAP 属性来查询外部 Active Directory 服务器。例如 sAMAccountName
   - **Active Directory** 组属性名称-LDAP 服务器上配置的 LDAP 组属性名称。例如，LDAP 中的组属性的“成员”。
   - **Active Directory** 子属性名称 -LDAP 服务器上配置的 LDAP 子属性名称。例如，LDAP 中的子属性的“cn”。
   - **Active Directory** 身份验证域 -用于身份验证的 AD/LDAP 域名。例如 ctxnssfb.com。
6. 在“目标实例”部分中，选择要在其上部署此 Exchange 配置的 Citrix ADC 实例。

   > 注意
   >
   > 如果要查看最近发现的 Citrix ADC 实例，请单击刷新图标。

7. 单击 创建” 以创建配置文件并在所选 Citrix ADC 实例上执行配置。

   Citrix 建议您先选择干运行以检查在目标实例上创建的配置对象，然后再对实例执行实际配置。

成功创建配置后，样本创建了一个内容交换虚拟服务器、五个负载平衡虚拟服务器和一个绑定到一个 LDAP 身份验证虚拟服务器的 LDAP 策略。此外，相应的服务组创建并绑定到负载平衡虚拟服务器。

Microsoft SharePoint 样本

April 23, 2021

Microsoft SharePoint 2016 是关键的企业应用程序，主要提供文档管理和存储系统，它是高度可配置的，且所有重要浏览器都支持它。

您可以使用 Microsoft SharePoint 2016 样本来部署 Citrix ADC 配置，从而对您的网络中的 Microsoft SharePoint 2016 企业应用程序进行优化和保护。

必备条件

- Microsoft SharePoint 2016
- Citrix ADM，版本 12.0 及更高版本
- Citrix ADC 版本 10.5 及更高版本

Microsoft SharePoint 2016 样本配置的 Citrix ADC 功能

可以使用 Microsoft SharePoint 2016 样本为 Microsoft SharePoint 2016 启用和配置以下 Citrix ADC 功能：

- 负载平衡
- 内容交换
- 响应方
- 重写
- 压缩
- 集成缓存

负载平衡

Citrix ADC 负载平衡可将请求均匀分配到后端 SharePoint 服务器。对后端服务器进行智能监视可以防止请求发送到出现故障的服务器。

SharePoint 样本配置 12 个负载平衡虚拟服务器，每个服务器专门用于按照特定类型的内容（例如，文档、图片、音频、视频及其他文件类型）对请求进行负载平衡。

SharePoint 样书现在通过配置基于 SSL 的 LB 虚拟服务器来支持 SharePoint 应用程序的 SSL 模式。确保选择 SSL 作为前端协议。请注意，虚拟端口默认设置为 443。您还可以选择 SSL 以将服务组（SharePoint 应用程序服务器）绑定到目标负载平衡虚拟服务器。请注意，后端协议默认设置为 HTTP。

内容切换

内容交换功能用于根据特定类型的 SharePoint 请求内容（例如，文档、图片及音频或视频文件）在多个负载平衡虚拟服务器之间分配客户端请求。内容交换模块将传入流量导向到可以处理相应类型的内容的最优匹配负载平衡虚拟服务器。

因此，您可以对不同类型的流量应用不同的优化策略。例如，您可能想对视频使用与文本文档不同的压缩或缓存策略。

响应方

Citrix ADC 实例的响应程序功能可用于无缝地将用户从 HTTP 重定向到 HTTPS。还可以配置响应方来提供自定义的错误页面。响应程序策略确定必须对其执行操作的请求（流量），并将每个策略绑定到负载平衡虚拟服务器。SharePoint 样本包含用于将用户从 HTTP 重定向至 HTTPS URL 的配置。

重写

重写模块用于即时修改请求/响应头、URL 或内容。此模块以内联方式进行流量处理，因此可以根据需要针对特定用例更改通信流。例如，重写可以提供对请求内容的访问，而不会公开有关 Web 站点服务器的不必要的详细信息。

在 SharePoint 样本中，重写功能用于从用户请求中删除不必要的标头。

压缩

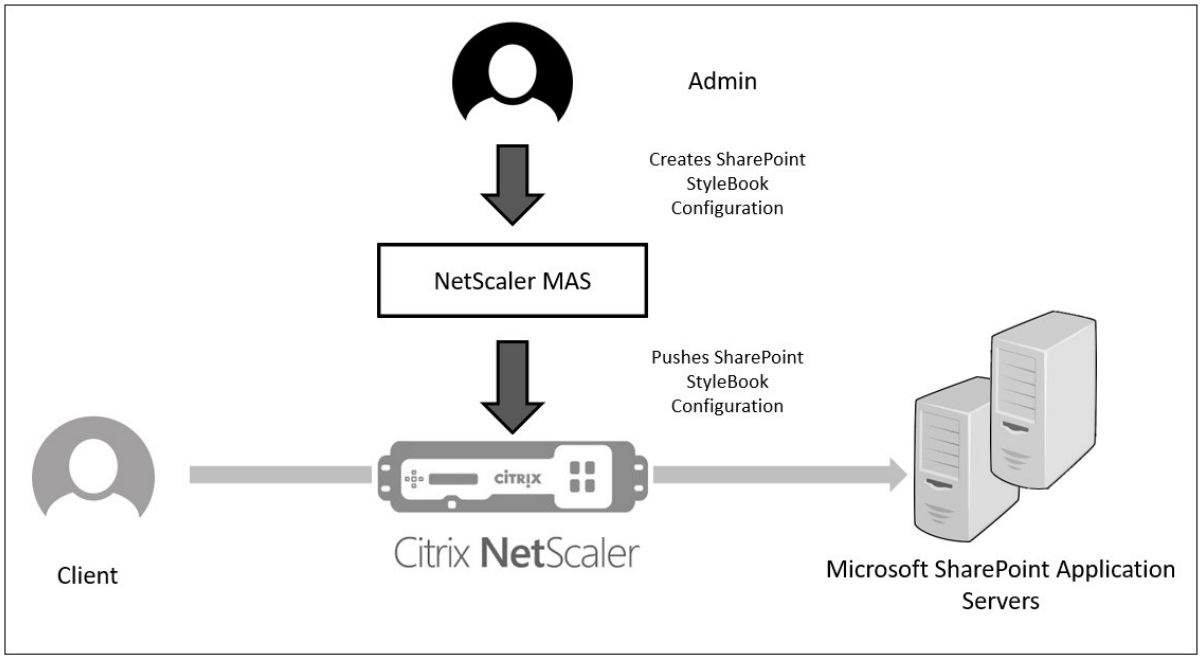
Citrix ADC 压缩引擎可识别和压缩可压缩的内容。此过程可减少数据传输时间、降低客户端的网络带宽要求，同时缩短 SharePoint 内容服务器上的 CPU 周期。Citrix ADC 实例可以压缩静态数据和动态生成的数据。它应用 GZIP 或 DEFLATE 压缩算法从服务器响应中删除无关和重复的信息，并以更加简洁和有效的格式表示原始信息。客户端浏览器解压缩数据的能力取决于它支持的算法：GZIP 或/和 DEFLATE。

Citrix ADC 实例配置为压缩 HTML、XML、纯文本、级联样式表 (CSS) 和 Microsoft Office 文档的文本，但不压缩 GIF 或 JPG 格式的图像。压缩流量的主要优势包括降低带宽成本、减少 WAN 延迟以及提高服务器性能。

集成缓存

Citrix ADC 内存中缓存可以存储 SharePoint 对象，以便快速向用户提供频繁请求的内容。缓存的内容包括下载的文档和音频、视频及图片文件。

下图以图形方式显示了 SharePoint 服务器在由 Citrix ADC 实例前端的网络中的部署，该实例使用 Citrix ADM 部署 SharePoint 样本配置。



部署 **SharePoint** 样本配置

以下任务将帮助您在您的企业网络中部署 Microsoft SharePoint 2016 样书。

若要部署微软 **SharePoint 2016** 年样书，请执行以下操作：

1. 在 Citrix ADM 中，导航到 应用程序 > 管理 > 配置”，然后单击 创建新。

   “ 选择样本页面显示了 Citrix ADM 中可供您使用的所有样本。

2. 向下滚动并选择 **Microsoft SharePoint 2016** 样本。

   > 注意
   >
   > 在 Citrix ADM 中，导航到 应用程序” > 配置” > 样本”。向下滚动以找到 微软 **SharePoint 2016** 年样书，然后单击 创建配置。

   样本将以用户界面表单形式打开，您可以在此为此样本中定义的所有参数输入值。

   输入以下参数的值：

   a) **SharePoint** 应用程序名称。要在您的网络中部署的 SharePoint 配置的名称。

   b) **SharePoint** 虚拟 **IP**。Citrix ADC 实例接收 Microsoft SharePoint 应用程序的客户端请求的虚拟 IP 地址。

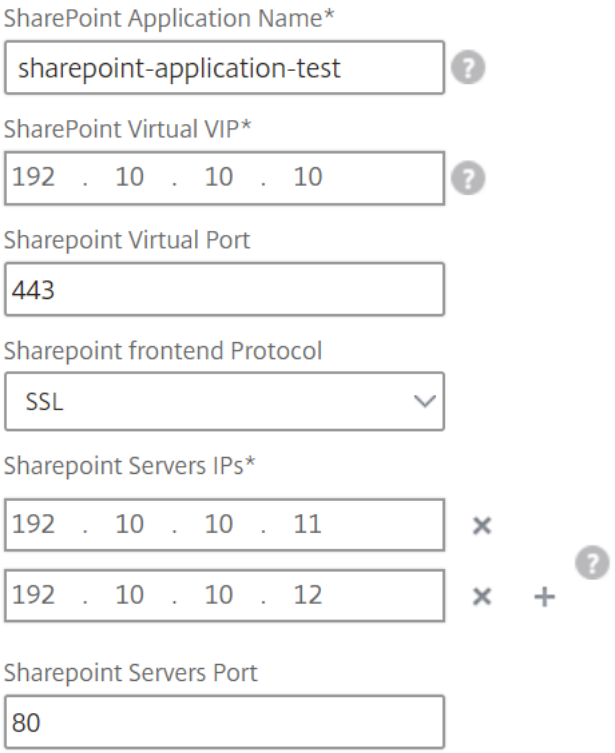
   c) **SharePoint** 虚拟端口。用户访问 SharePoint 应用程序时要使用的 TCP 端口

   d) **SharePoint** 前端协议。从下拉列表中选择 SharePoint 前端协议。可用的选项包括 HTTP 或 SSL。

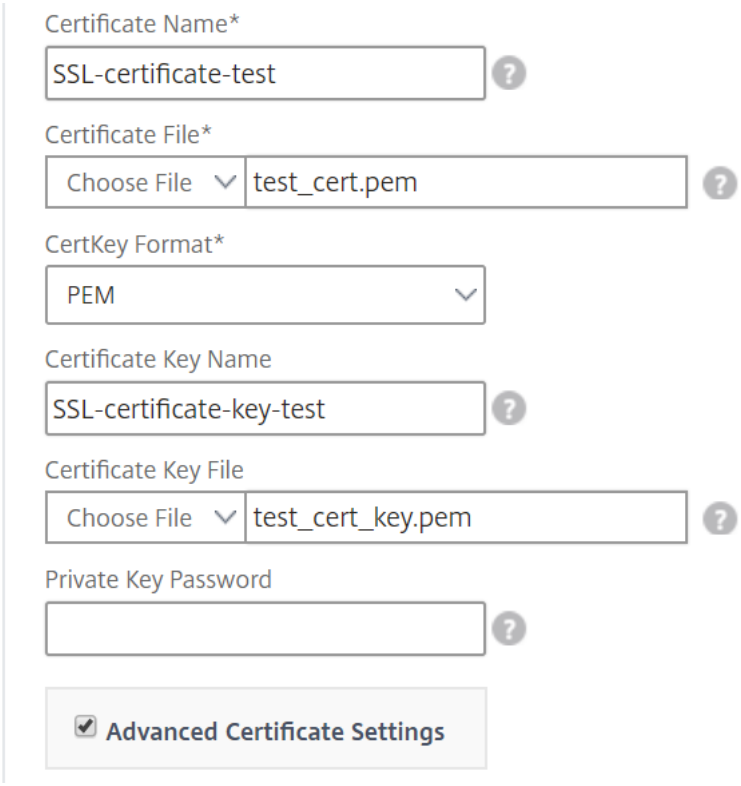
> 注意
>
> 如果选择 SSL，请确保在此样本的 SharePoint 高级设置部分中启用了“重写配置”参数。

e) **SharePoint** 服务器 **IP**。网络中所有 SharePoint 服务器的 IP 地址。

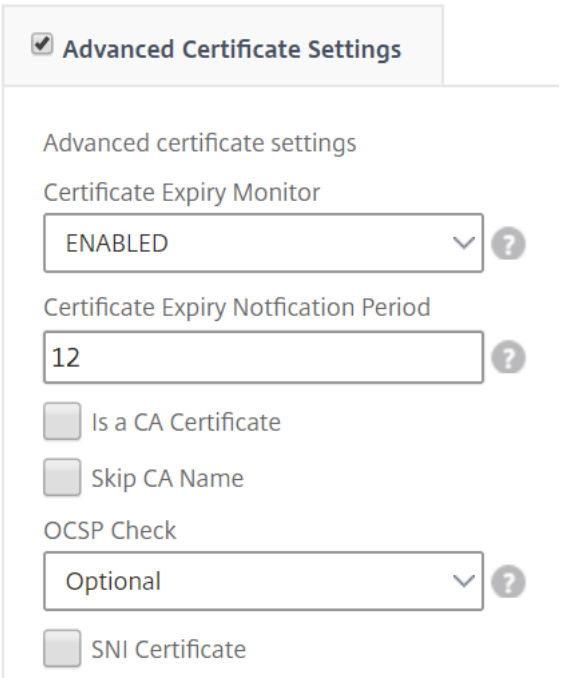
f) **SharePoint** 服务器端口。SharePoint 服务器使用的 TCP 端口号。默认情况下，此端口号为 80。您可以根据需要编辑此值，但请确保可以在 Microsoft SharePoint 2016 服务器上访问此端口。



3. 在 **SSL** 证书设置部分中，单击“+”以输入 SSL 证书的名称、证书密钥，然后从本地存储文件夹中选择相应的文件。



4. （可选）单击 高级证书设置以启用或禁用 SSL 证书到期监视。如果启用证书过期监视，请设置天数，以便 Citrix ADM 在证书即将过期的这几天后发出警报。您还可以选择将 OCSP 检查设置为可选功能或强制功能。

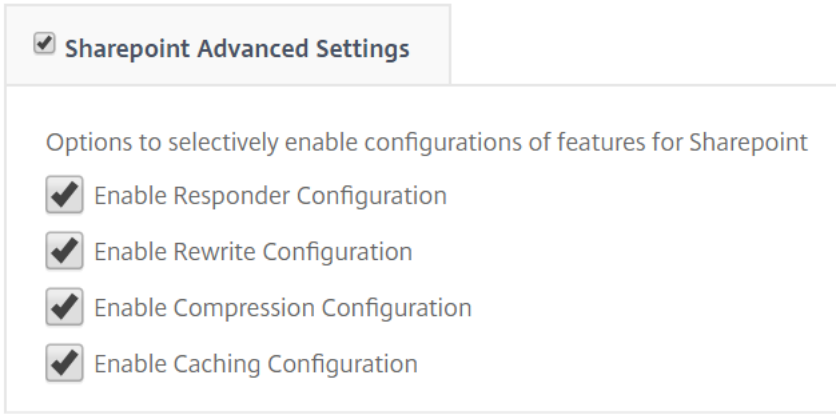


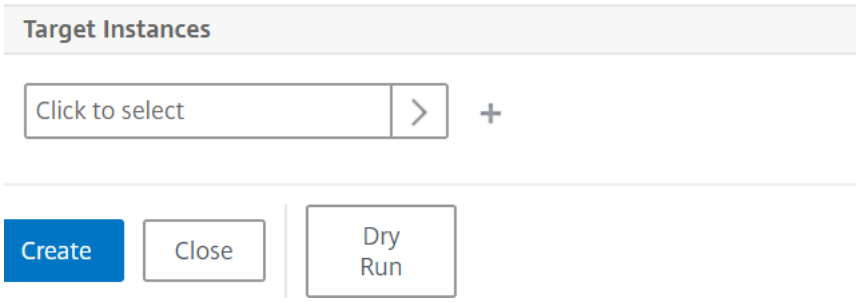
5. 通过 SharePoint 高级设置部分，您可以启用将在 Citrix ADC 实例上配置的 Citrix ADC 功能。虽然默认情况下在实例上配置负载平衡和内容交换功能，但您可以选择要在实例上配置的其他功能，即，响应方配置、重写配

置、压缩配置以及集成缓存配置。

6. 单击 目标实例，然后选择要在其上部署此 SharePoint 配置的 Citrix ADC 实例。单击 创建” 以创建配置并在所选 Citrix ADC 实例上部署配置。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。





> 注意
>
> Citrix 建议在执行实际配置之前，选择试运行以检查将在目标实例上创建的配置对象。

创建并成功部署配置后，SharePoint 样本将创建一个内容交换虚拟服务器和 12 个负载平衡虚拟服务器。它还将创建策略和服务组，并将其绑定到负载平衡虚拟服务器。创建哪些策略取决于在创建配置包的过程中在样本中选择的功能。

查看在 **Citrix ADC** 实例上定义的对象

在 Citrix ADM 上创建配置包后，您可以查看在 Citrix ADC 实例上为 SharePoint 样本创建的所有对象。导航至 “ 应用程序” > “ 管理” > “ 配置”，然后单击 “ 查看已创建的对象”。下图显示了一些已创建的对象，其中示例中指定的 IP 地址如 “从 Citrix ADM 部署 SharePoint 样本配置”。“

Type : lbvserver

appflowlog : DISABLED
backuppersistencetimeout : 20
downstateflush : DISABLED
ipv46 : 0.0.0.0
lbmethod : LEASTCONNECTION
name : sharepoint application test frontpage services lb
persistencebackup : SOURCEIP
persistencetype : COOKIEINSERT
port : 0
servicetype : HTTP
timeout : 20

Type : servicegroup

cip : DISABLED
cka : YES
cmp : NO
downstateflush : DISABLED
healthmonitor : NO
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp
servicetype : HTTP
sp : ON
state : ENABLED
tcpb : NO
useproxyport : NO
usip : NO

Type : lbvserver_servicegroup_binding

name : sharepoint-application-test-frontpage-services-lb
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.11
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.10.10.12
port : 80
servicegroupname : sharepoint-application-test-frontpage-services-svcgrp

Type : csaction

name : sharepoint-application-test-cs-frontpage-services-csaction
targetlbvserver : sharepoint-application-test-frontpage-services-lb

Type : cspolicy

action : sharepoint-application-test-cs-frontpage-services-csaction
policyname : sharepoint-application-test-cs-frontpage-services-cspol
rule : HTTP.REQ.HEADER("X-Vermeer-Content-Type").EXISTS

Type : csvserver_cspolicy_binding

name : sharepoint-application-test-cs
policyname : sharepoint-application-test-cs-frontpage-services-cspol
priority : 10

Microsoft ADFS 代理样本

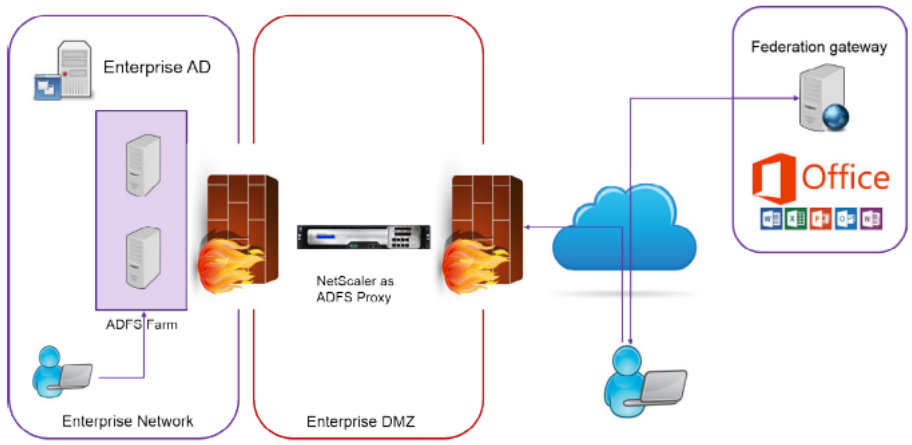
April 23, 2021

Microsoft™ ADFS 代理通过为启用内部联合的资源和云资源提供单点登录访问，发挥了重要作用。云资源的一个例子是 Office 365。ADFS 代理服务器的目的是接收请求并转发到无法从互联网访问的 ADFS 服务器。ADFS 代理是反向代理，通常驻留在组织的外围网络 (DMZ) 中。ADFS 代理在远程用户连接和应用程序访问方面起着关键作用。

Citrix ADC 具有精确的技术，可实现联合身份的安全连接、身份验证和处理。使用 Citrix ADC 作为 ADFS 代理可避免在 DMZ 中部署额外的组件。

Citrix Application Delivery Management (ADM) 中的 Microsoft ADFS 代理样本允许您在 Citrix ADC 实例上配置 ADFS 代理服务器。

下图显示了在企业 DMZ 中将 Citrix ADC 实例部署为 ADFS 代理服务器的情况。



使用 Citrix ADC 作为 ADFS 代理的好处

1. 满足负载平衡和 ADFS 代理需求
2. 支持内部和外部用户访问方案
3. 支持丰富的预身份验证方法
4. 为用户提供单点登录体验
5. 支持主动和被动协议
    a) 主动协议应用程序的示例 - Microsoft Outlook、Microsoft Skype for Business
    b) 被动协议应用程序的示例 - Microsoft Outlook Web App、Web 浏览器
6. 用于基于 DMZ 的部署的强化设备
7. 通过使用其他核心 Citrix ADC 功能增加价值
    a) 内容交换
    b) SSL 卸载
    c) 重写

d) 安全性（Citrix ADC AAA）

对于基于协议的活动方案，您可以连接到 Office 365 并提供凭据。Microsoft 联合身份验证网关代表活动协议客户端联系 ADFS 服务（通过 ADFS 代理）。然后，Gateway 使用基本身份验证 (401) 提交凭据。Citrix ADC 在访问 ADFS 服务之前处理客户端身份验证。身份验证后，ADFS 服务向联合身份验证网关提供 SAML 令牌。反过来，联合身份验证网关将令牌提交给 Office 365 以提供客户端访问。

对于被动客户端，ADFS 代理样本创建 Kerberos 约束委派 (KCD) 用户帐户。KCD 帐户是连接到 ADFS 服务器的 Kerberos SSO 身份验证所必需的。样本还会生成 LDAP 策略和会话策略。这些策略稍后会绑定到处理被动客户端身份验证的 Citrix ADC AAA 虚拟服务器。

样本还可以确保 Citrix ADC 上的 DNS 服务器配置为 ADFS。

下面的配置部分介绍了如何设置 Citrix ADC 以处理基于主动和被动协议的客户端身份验证。

配置详细信息

下表列出了成功部署此集成所需的最低软件版本。

产品	最低要求版本
Citrix ADC	11.0, 高级/高级许可

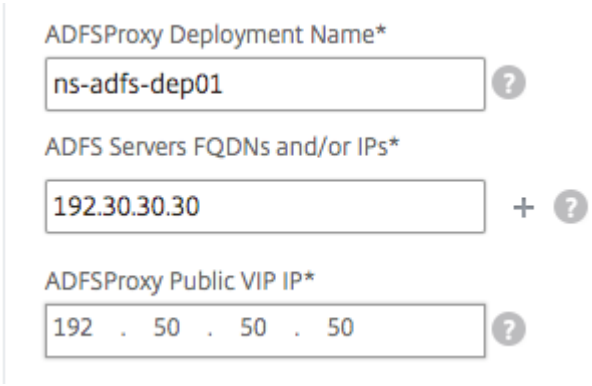
以下说明假定您已经创建了相应的外部和内部 DNS 条目。

从 **Citrix ADM** 部署 **Microsoft ADFS** 代理样本配置

在您的业务网络中实施 Microsoft ADFS 代理样本时，以下说明可以帮助您。

部署 **Microsoft ADFS** 代理样本

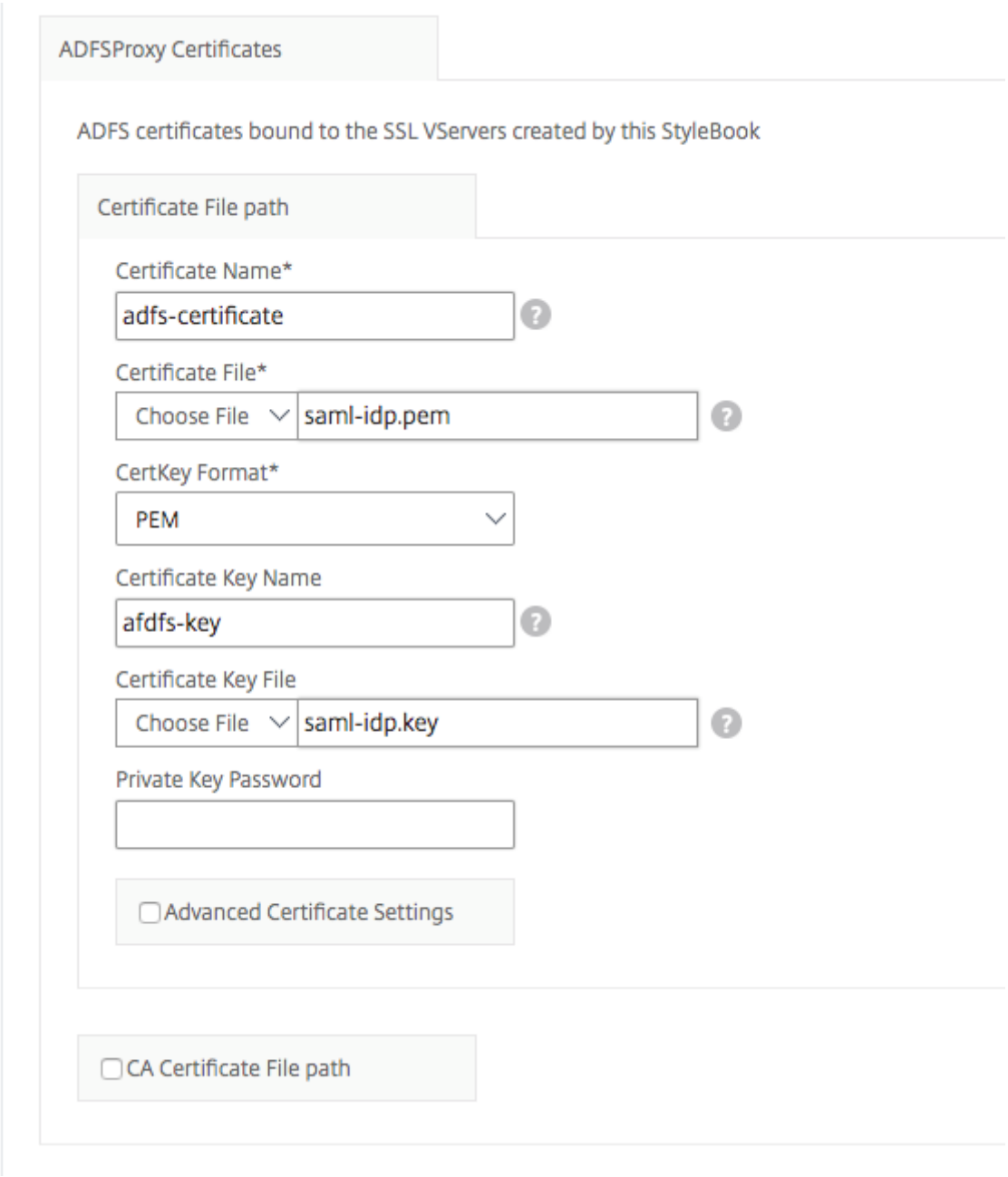
1. 在 Citrix ADM 中，导航到 应用程序 > 样本。“ 样书”页面显示可供您在 Citrix ADM 中使用的所有样书。
2. 向下滚动并查找 **Microsoft ADFS** 代理样本。单击 创建配置。样本
   以用户界面页的形式打开，您可以在该页面上键入此样本中定义的所有参数的值。
3. 键入以下参数的值：
   a) **ADFS** 代理部署名称。为网络中部署的 ADFS 代理配置选择一个名称。
   b) **ADFS** 服务器 **FQDN** 或 **IP**。键入网络中所有 ADFS 服务器的 IP 地址或 FQDN（域名）。
   c) **ADFS** 代理公共 **VIP IP**. 键入作为 ADFS 代理服务器执行的 Citrix ADC 上的公用虚拟 IP 地址。



4. 在 **ADFS** 代理证书”部分中，键入 SSL 证书和证书密钥的详细信息。

   此 SSL 证书绑定到在 Citrix ADC 实例上创建的所有虚拟服务器。

   从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以加载.pem 格式的加密私钥。



您还可以启用 高级证书设置”复选框。在这里，您可以键入详细信息，例如证书到期通知期限、启用或禁用证书到期监视器。

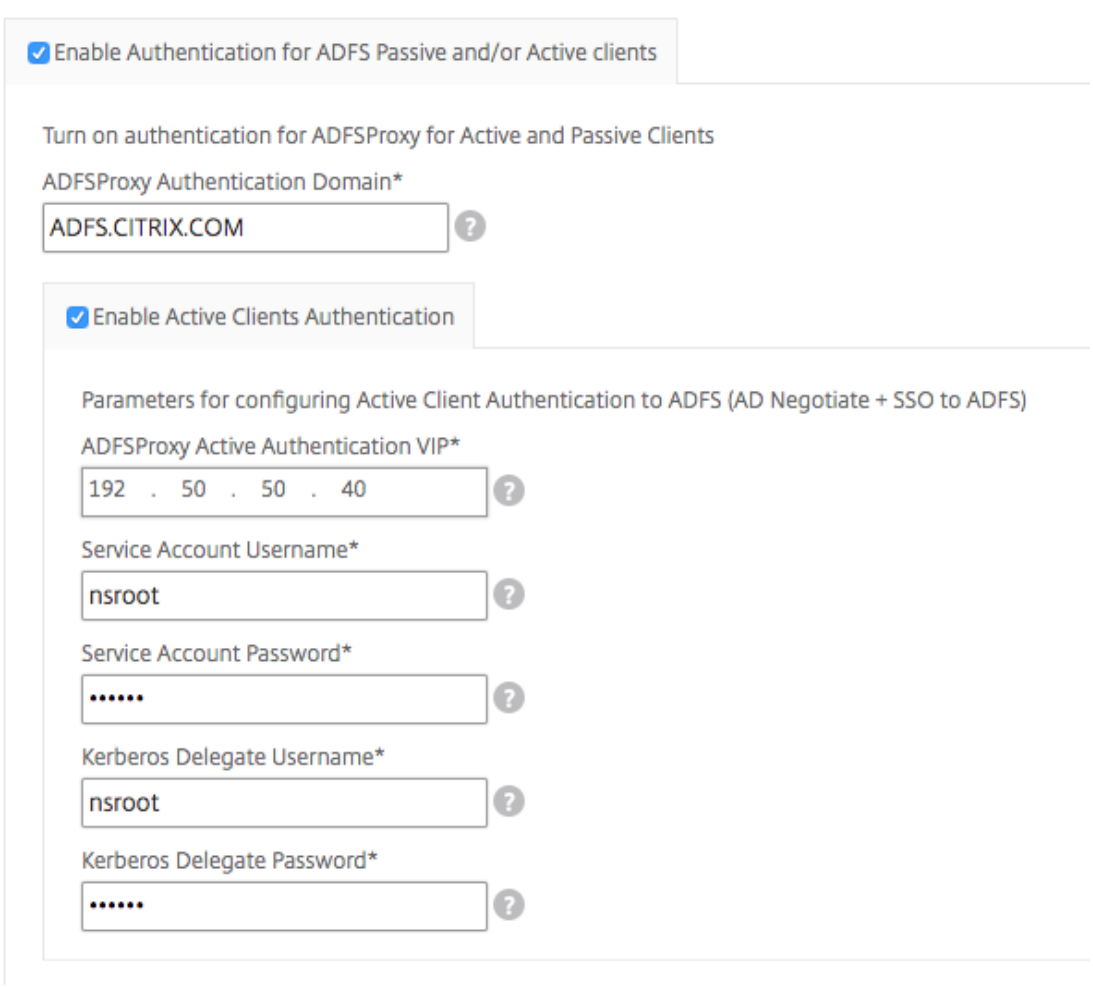
5. （可选）如果 **SSL** 证书要求在 Citrix ADC 上安装 CA 公共证书，则可以选中 SSL CA 证书复选框。确保在 “ 高级证书设置” 部分中选择 “是 CA 证书”。
6. 为主动客户端和被动客户端启用身份验证。键入用于用户身份验证的 Active Directory 中使用的 DNS 域名。然后，您可以为主动客户端或被动客户端配置身份验证，或者两者都配置身份验证。
7. 键入以下详细信息以启用活动客户端的身份验证：

> ** 注
>
> 意：** 配置对活动客户端的支持是可选的。

a) **ADFS** 代理活动身份验证 **VIP**. 键入 Citrix ADC 实例上虚拟身份验证服务器的虚拟 IP 地址，其中活动客户端将被重定向以进行身份验证。

b) 服务帐户用户名。键入 Citrix ADC 用于在 Active Directory 中对用户进行身份验证的服务帐户用户名。

c) 服务帐户密码。键入 Citrix ADC 用于在 Active Directory 中对用户进行身份验证的密码。



8. 通过启用相应的选项并配置 LDAP 设置，为被动客户端配置身份验证。

> ** 注
>
> 意：** 配置对被动客户端的支持是可选的。

键入以下详细信息以启用被动客户端的身份验证：

a) **LDAP**（**Active Directory**）基础。键入用户帐户驻留在 Active Directory (AD) 中的域的基本域名以允许身份验证。例如，dc=netscaler,dc=com

b) **LDAP**（**Active Directory**）绑定 **DN**。添加具有浏览 AD 树权限的域帐户（使用电子邮件地址以便于配置）。例如，cn=Manager,dc=netscaler,dc=com

c) **LDAP**（**Active Directory**）绑定 **DN** 密码。键入域帐户的密码进行身份验证。

您必须在本节中键入的值的其他几个字段如下：

d) **LDAP** 服务器（**Active Directory**）**IP**。键入 Active Directory 服务器的 IP 地址，以便 AD 身份验证正常工作。

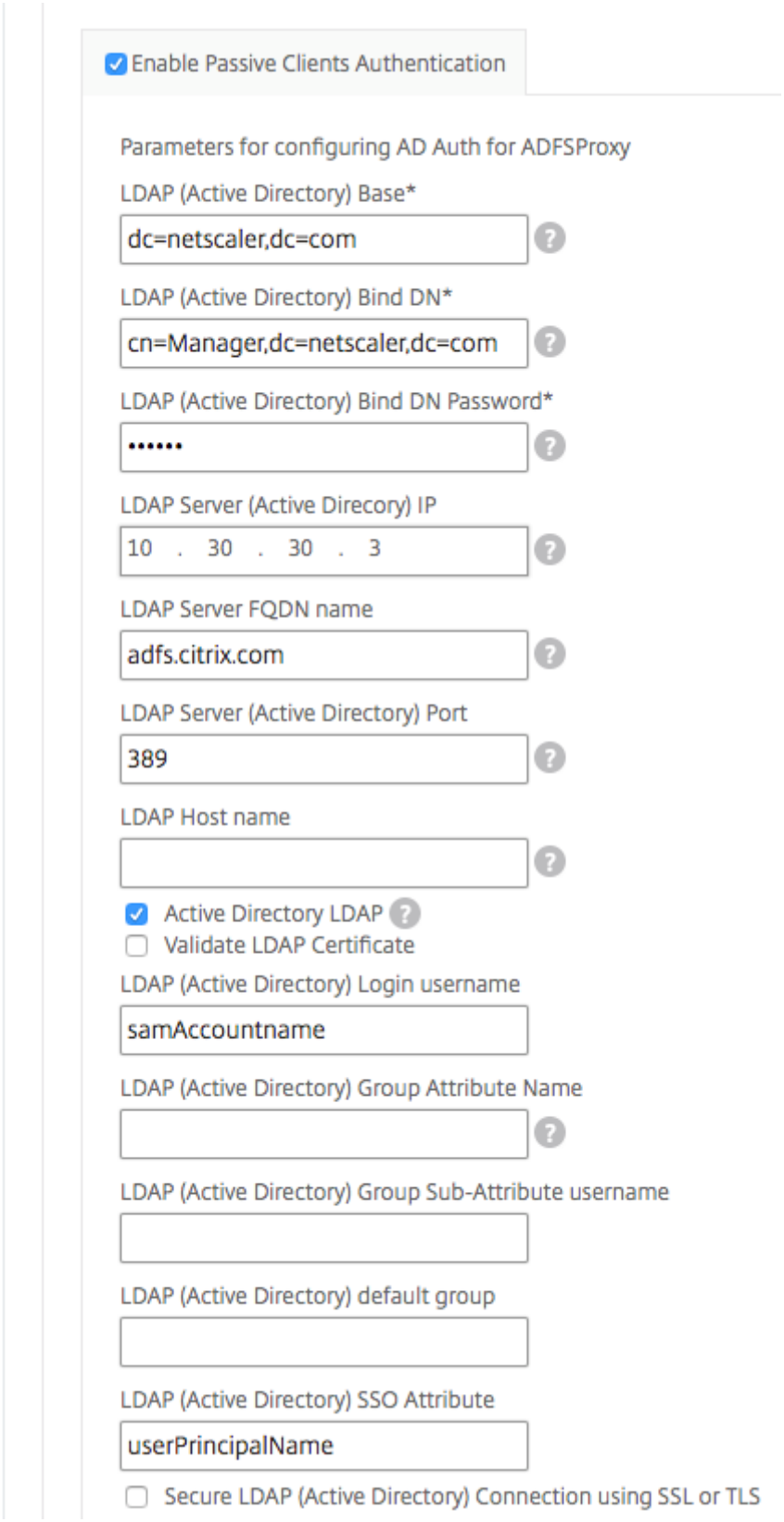
e) **LDAP** 服务器 **FQDN** 名称。键入 Active Directory 服务器的 FQDN 名称。FQDN 名称是可选的。提供步骤 1 中的 IP 地址或 FQDN 名称。

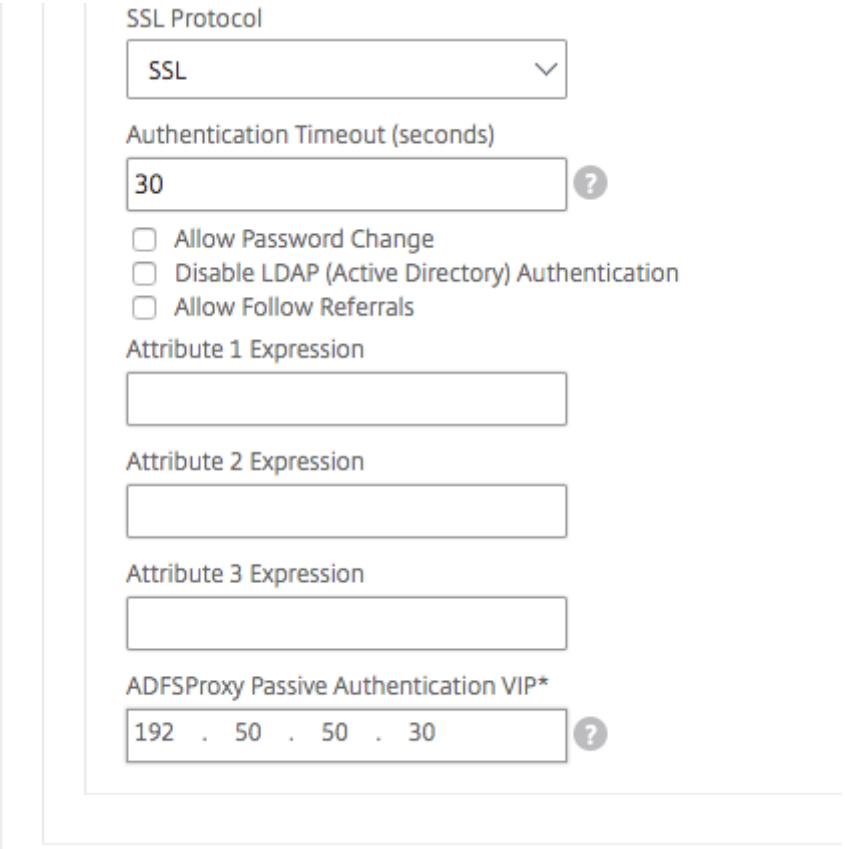
f) **LDAP** 服务器 **Active Directory** 端口。默认情况下，LDAP 协议的 TCP 和 UDP 端口为 389，而安全 LDAP 的 TCP 端口为 636。

g) **LDAP**（**Active Directory**）登录用户名。键入用户名为 “三帐户名称”。“

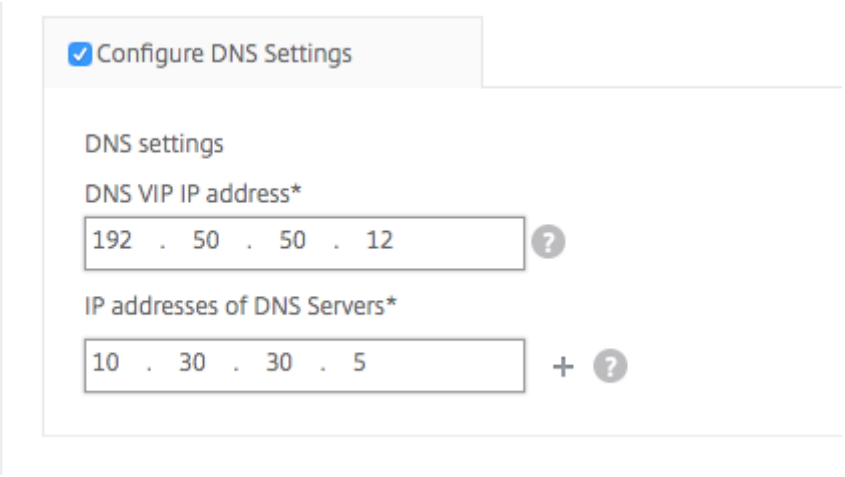
h) **ADFS** 代理被动身份验证 **VIP**. 键入被动客户端的 ADFS 代理虚拟服务器的 IP 地址。

> 注意
>
> 标有 “*” 的字段是必填字段。

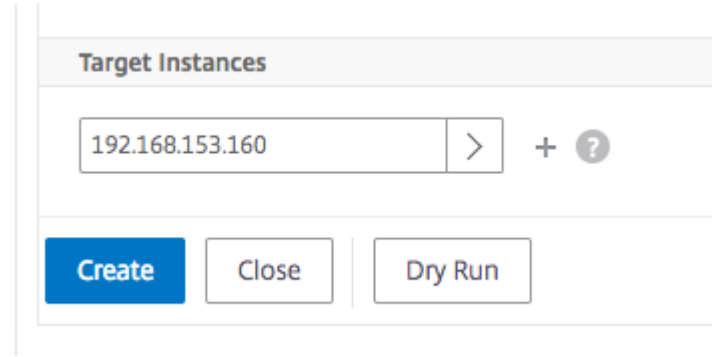




9. 您也可以为 DNS 服务器配置 DNS VIP。



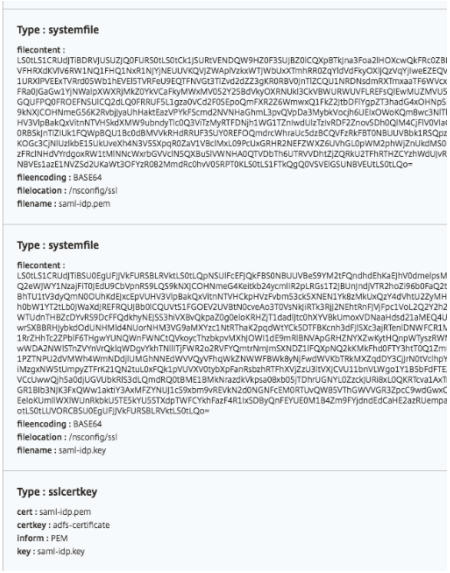
10. 单击 目标实例，然后选择要部署此 Microsoft ADFS 代理配置的 Citrix ADC 实例。单击 创建” 以创建配置并在所选 Citrix ADC 实例上部署配置。



> 注意
>
> Citrix 建议在执行实际配置之前，选择试运行。您可以首先查看样本在目标 Citrix ADC 实例上创建的配置对象。然后，您可以单击 **Create** 以在选定的实例上部署配置。

已创建的对象

在 Citrix ADC 实例上部署 ADFS 代理配置时，将创建多个配置对象。下图显示创建的对象的列表。



Objects Added on Instance : 192.168.153.160 | Count : 57

Type : nsfeature

Meta Properties
action : **enable**

feature : cs lb ssl rewrite aaa

Type : lbvserver

ipv46 : 192.50.50.12
name : ns-adfs-dep01-adfs-dns
port : 53
servicetype : DNS

Type : service

ip : 10.30.30.5
name : ns-adfs-dep01-dns-svc-1
port : 53
servicetype : DNS

Type : lbvserver_service_binding

name : ns-adfs-dep01-adfs-dns
servicename : ns-adfs-dep01-dns-svc-1

Type : authenticationnegotiateaction

domain : ADFS.CITRIX.COM
domainuser : nsroot
domainuserpasswd : nsroot
name : ns-adfs-dep01-negotiate-action

Type : authenticationpolicy

action : ns-adfs-dep01-negotiate-action
name : ns-adfs-dep01-negotiate-policy
rule : true

Type : aaakcdaccount

delegateduser : nsroot
kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
kcdpassword : nsroot
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-auth401-kcd-
name : ns-adfs-dep01-adfs-auth401-tmsession-action
persistentcookie : ON
persistentcookievalidity : 3
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-auth401-tmsession-action
name : ns-adfs-dep01-adfs-auth401-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.40
maxloginattempts : 255
name : ns-adfs-dep01-adfs-auth401-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-auth401-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-negotiate-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-auth401-auth-vserver
policy : ns-adfs-dep01-adfs-auth401-tmsession-policy
priority : 10

Type : authenticationldapaction

authentication : ENABLED
authtimeout : 30
followreferrals : OFF
ldapbase : dc=netscaler,dc=com
ldapbinddn : cn=Manager,dc=netscaler,dc=com
ldapbinddnpassword : nsroot
ldaploginname : samAccountname
name : ns-adfs-dep01-ldap-action
passwdchange : DISABLED
sectype : PLAINTEXT
serverip : 10.30.30.3
serverport : 389
ssonameattribute : userPrincipalName
svrtype : AD
validateservercert : NO

Type : authenticationpolicy

action : ns-adfs-dep01-ldap-action
name : ns-adfs-dep01-ldap-policy
rule : true

Type : aaakcdaccount

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
realmstr : ADFS.CITRIX.COM

Type : tmsessionaction

kcdaccount : ns-adfs-dep01-adfs-ldap-kcd-acc
name : ns-adfs-dep01-adfs-ldap-tmsession-action
persistentcookie : OFF
sso : ON

Type : tmsessionpolicy

action : ns-adfs-dep01-adfs-ldap-tmsession-action
name : ns-adfs-dep01-adfs-ldap-tmsession-policy
rule : ns_true

Type : authenticationvserver

authenticationdomain : ADFS.CITRIX.COM
failedlogintimeout : 1
ipv46 : 192.50.50.30
maxloginattempts : 255
name : ns-adfs-dep01-adfs-ldap-auth-vserver
port : 443
servicetype : SSL

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-adfs-ldap-auth-vserver

Type : authenticationvserver_authenticationpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-ldap-policy
priority : 10

Type : authenticationvserver_tmsessionpolicy_binding

name : ns-adfs-dep01-adfs-ldap-auth-vserver
policy : ns-adfs-dep01-adfs-ldap-tmsession-policy
priority : 10

Type : csvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-cs
port : 443
servicetype : SSL

Type : lbvserver

ipv46 : 192.50.50.50
name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
port : 445
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : server

ipaddress : 192.30.30.30
name : 192.30.30.30

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-federationproxy-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") || HTTP.REQ.URL.CONTAINS("/federa

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-federationproxy-cspol
priority : 9800

Type : lbvserver

appflowlog : ENABLED
authentication : ON
authenticationhost : ADFS.CITRIX.COM
authn401 : OFF
authnvsname : ns-adfs-dep01-adfs-ldap-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
port : 446
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-passive-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
rule : HTTP.REQ.URL.CONTAINS("/adfs/ls/auth/integrated") || HTTP.REQ.URL.CONTAINS("/adfs/ls/wia")

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-passive-cspol
priority : 9900

Type : lbvserver

appflowlog : ENABLED
authentication : OFF
authn401 : ON
authnvsname : ns-adfs-dep01-adfs-auth401-auth-vserver
downstateflush : ENABLED
ipv46 : 192.50.50.50
lbmethod : LEASTCONNECTION
name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
port : 444
servicetype : SSL

Type : servicegroup

servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp
servicetype : SSL

Type : lbvserver_servicegroup_binding

name : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : servicegroup_servicegroupmember_binding

ip : 192.30.30.30
port : 443
servicegroupname : ns-adfs-dep01-ns-adfs-dep01-adfs-active-svcgrp

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : csaction

name : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
targetlbvserver : ns-adfs-dep01-ns-adfs-dep01-adfs-active-lb

Type : cspolicy

action : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-csaction
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
rule : true

Type : csvserver_cspolicy_binding

name : ns-adfs-dep01-cs
policyname : ns-adfs-dep01-cs-ns-adfs-dep01-adfs-active-cspol
priority : 10000

Type : sslvserver_sslcertkey_binding

certkeyname : adfs-certificate
vservername : ns-adfs-dep01-cs

Type : rewritepolicylabel

labelname : ns-adfs-dep01-request-rewritepolicylabel
transform : HTTP_REQ

Type : rewritepolicylabel

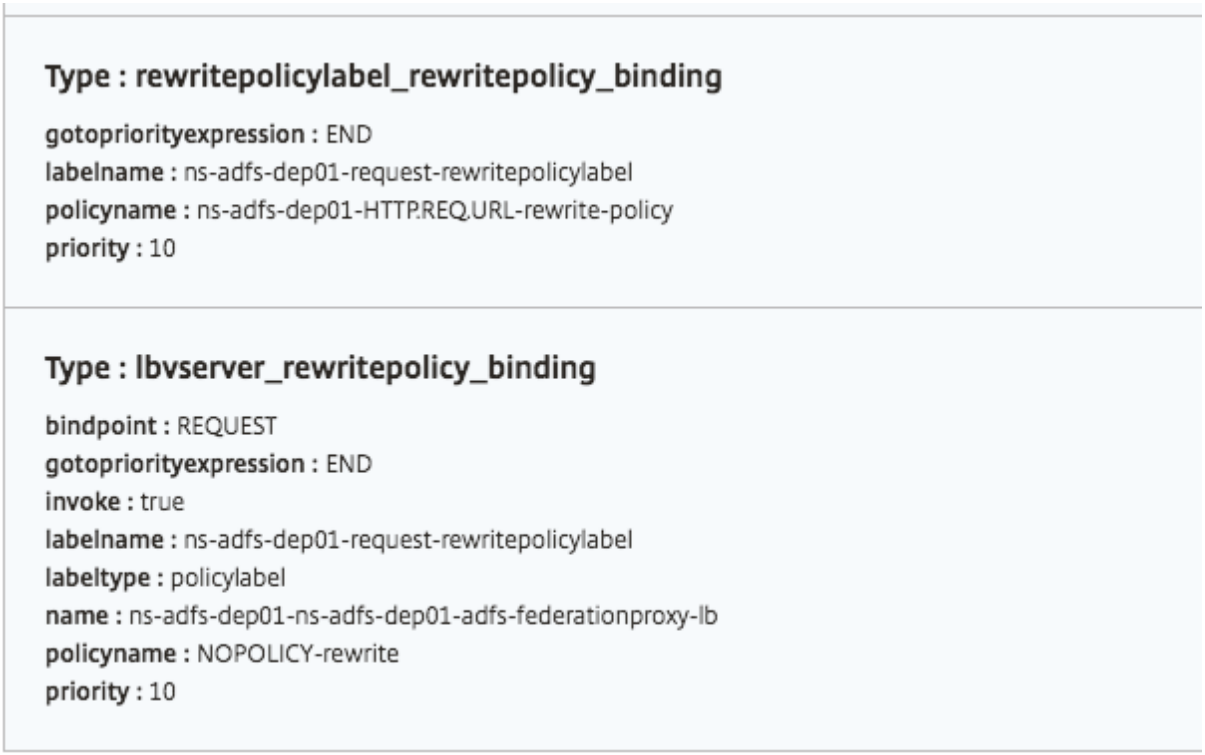
labelname : ns-adfs-dep01-response-rewritepolicylabel
transform : HTTP_RES

Type : rewriteaction

name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
stringbuilderexpr : "/adfs/services/trust/proxymex"
target : HTTP.REQ.URL
type : REPLACE

Type : rewritepolicy

action : ns-adfs-dep01-HTTP.REQ.URL-rewrite-action
name : ns-adfs-dep01-HTTP.REQ.URL-rewrite-policy
rule : HTTP.REQ.URL.CONTAINS("/adfs/services/trust") && (!HTTP.REQ.URL.CONTAINS("/trust/proxymex"))



Oracle 电子商务样书

April 23, 2021

Oracle 电子商务套件是最全面的集成式全球业务应用程序套件。此套件使组织能够做出更好的决策、降低成本和提高性能，并由以下应用程序组成。

- 企业资源规划 (ERP)
- 客户关系管理 (CRM)
- 供应链管理 (SCM)

这些计算机应用程序由 Oracle 开发或购买。Oracle 电子商务套件 12.2 样本允许您在选定的 Citrix ADC 实例上部署配置。

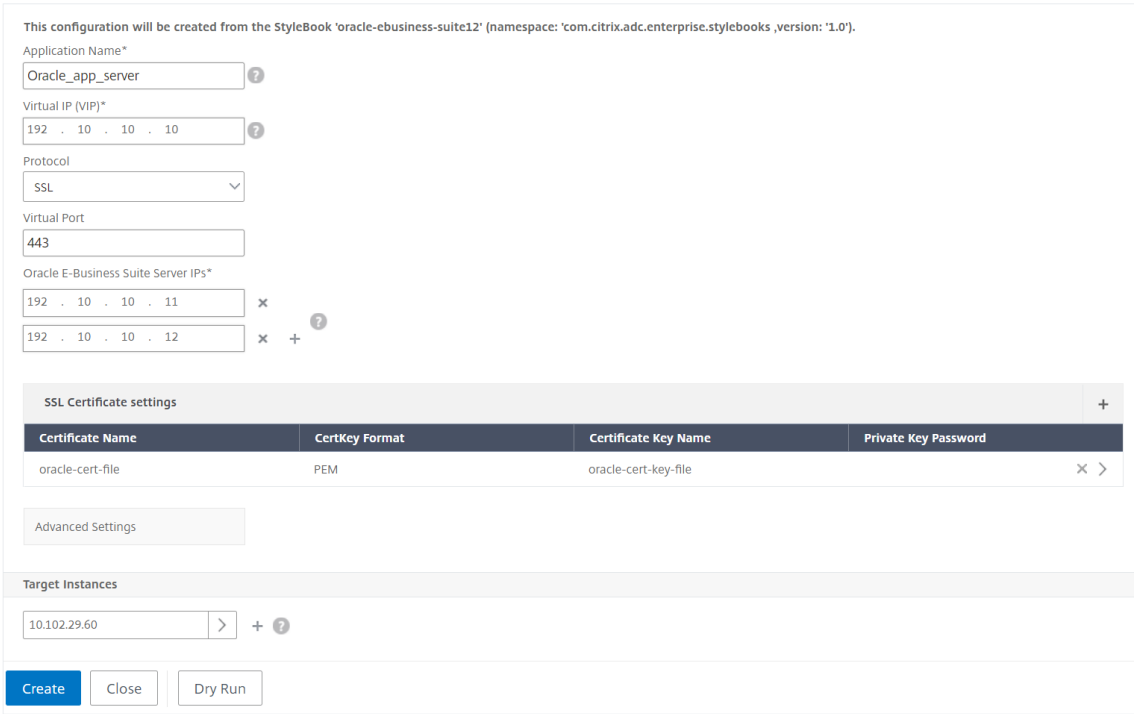
此样本创建包含负载平衡虚拟服务器、服务组和服务列表的负载平衡配置。它还将服务绑定至服务组，并将服务组绑定至虚拟服务器。您可以通过选择 SSL 并从本地系统提供 SSL 文件和密钥文件来选择加密通信。

为 **Oracle** 电子商务套件 **12.2** 创建配置的步骤

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “应用程 序” > **“**配置**” > “**样书”。样本页面显示 Citrix ADM 中可用的所有样本。向下滚动并选择 **Oracle** 电子商务套件 **12.2**。您还可以使用搜索选项搜索样本。

2. 单击样本面板中的 创建配置。
3. 在负载平衡器设置部分中键入负载平衡器应用程序的名称和虚拟 IP 地址。
4. 选择所需的协议。这里有两个选项-HTTP 和 HTTPS/SSL。您也可以键入端口号。
5. 键入网络中要进行负载平衡的所有 Oracle 电子商务套件应用程序服务器的 IP 地址。单击 **+** 添加更多服务器 IP 地址。
6. 在 **SSL** 证书设置部分，从本地存储中选择相应的文件。您还可以启用 高级证书设置”复选框。在这里，您可以配置更多详细信息，例如证书到期通知期限。您还可以启用或禁用证书过期监视器。

   选择必须在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。



> 提示
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。刷新图标当前仅在 Citrix ADM 上可用。

Citrix StoreFront 样书

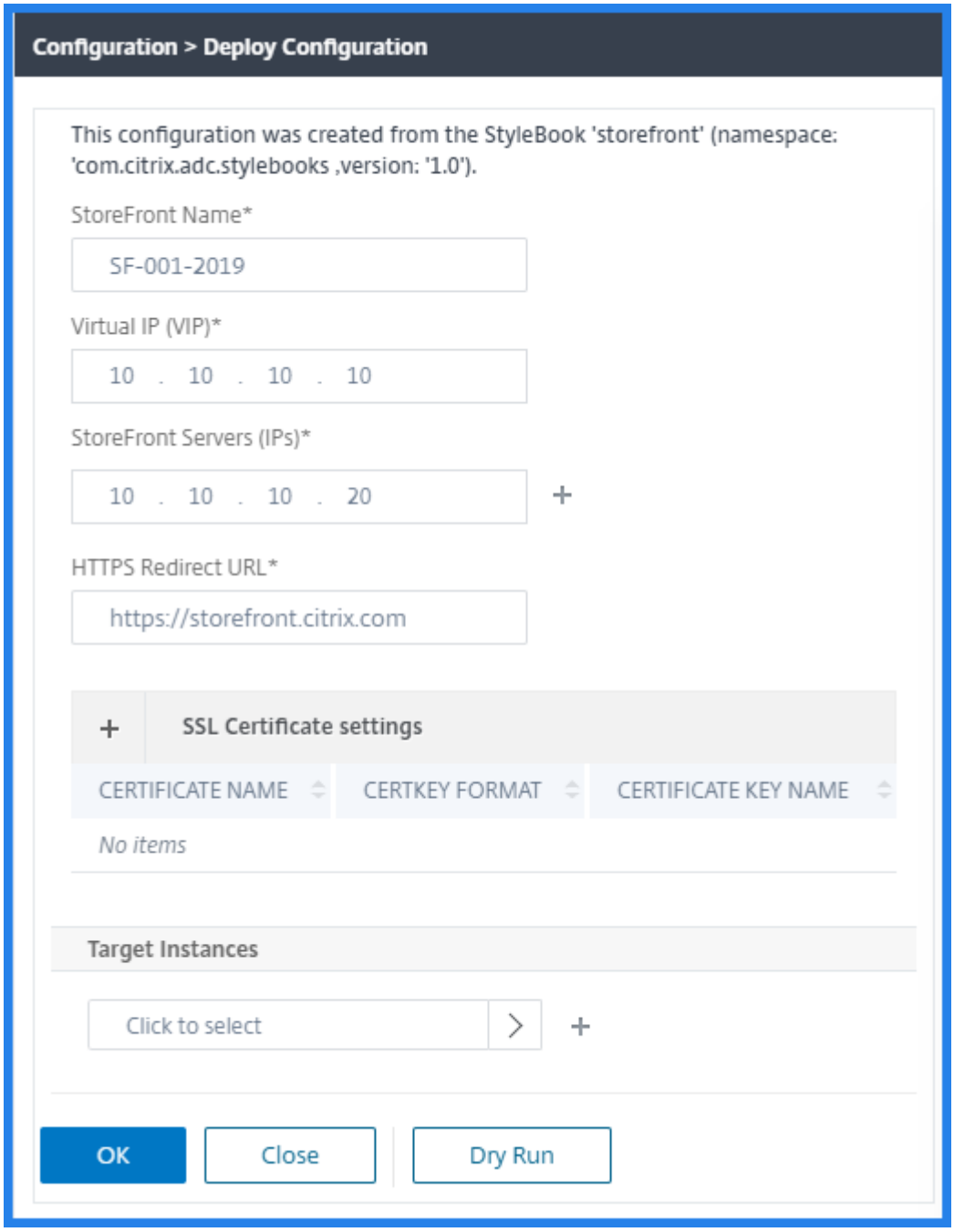
April 23, 2021

StoreFront 是一个企业应用商店，它将 Citrix Virtual Apps and Desktops 站点中的应用程序和桌面聚合到一个供用户使用的单个应用商店中。StoreFront 对托管资源站点的用户进行身份验证，并管理用户访问的应用程序存储和桌面。它托管您的企业应用程序存储，从而允许用户自助访问您提供给他们的应用程序和桌面。

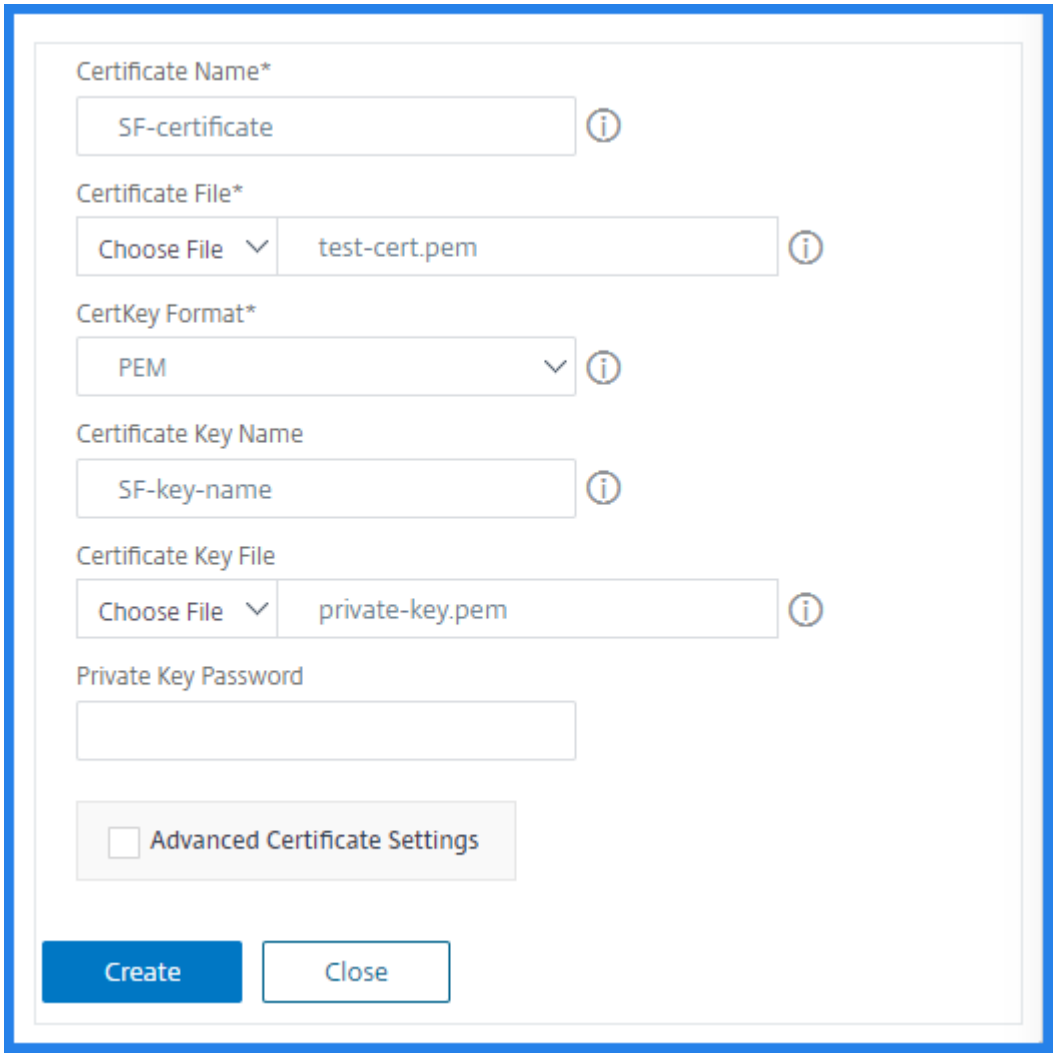
此样书定义了 StoreFront 服务器的 Citrix ADC 配置。使用此样书，您可以将 StoreFront 服务器配置为所需的 Citrix ADC 实例。您可以通过选择 SSL 并从本地系统提供 SSL 文件和密钥文件来选择加密通信。

为 **Citrix StoreFront** 应用程序创建配置

1. 在 Citrix ADM GUI 中，导航到 **“应用程序” > “样书”**。
2. 在搜索栏中，使用 “名 称” 属性和搜索 `Citrix StoreFront`。
3. 在 Citrix StoreFront 样书上，单击创建配置。
4. 指定以下详细信息：
    - **StoreFront** 名称：指定 StoreFront 名称。StoreFront 配置包使用相同的 StoreFront 名称创建。
    - 虚拟 **IP (VIP)**：指定 Citrix ADC 实例接收客户端请求的虚拟 IP 地址。
    - **StoreFront** 服务器：指定要使用 Citrix ADC 实例配置的 StoreFront 服务器的 IP 地址。
    - **HTTPS** 重定向 **URL**：指定 HTTPS 请求重定向到的 HTTPS URL。



5. 在 **SSL** 证书设置部分，输入 SSL 证书和证书密钥的名称。
6. 从本地存储文件夹中选择相应的文件。您还可以键入私钥密码以指定 PEM 格式的加密私钥。



7. 您还可以启用 高级证书设置”复选框。您可以在此处输入详细信息，例如证书到期通知期限、启用或禁用证书到期监视器。
8. 可选，如果 **SSL** 证书要求在 **Citrix ADC** 上安装 **CA** 公共证书，则为身份验证虚拟 **IP** 复选框选择 SSL CA 证书。确保在 “ 高级证书设置” 部分中选择 “是 CA 证书”。
9. 单击创建。
10. 单击 目标实例，然后选择要在其上配置 StoreFront 服务器的 Citrix ADC 实例。
11. 单击 创建” 以创建配置并在所选 Citrix ADC 实例上部署配置。

创建和使用自定义样本

April 23, 2021

您可以为部署编写自己的样本，将其导入 Citrix Application Delivery Management (ADM)，然后创建配置对象。还可以使用 API 根据您的样本创建配置。

本文档包含以下信息：

准备工作

开始创建样本之前，请确保您了解以下内容：

- NITRO API。有关详细信息，请参阅Nitro API 文档。
- YAML

样本文件使用 YAML 格式。有关 YAML 格式的信息，请参见 YAML 语法。

下面是创建样本时必须了解的 YAML 准则列表：

- YAML 区分大小写。
- YAML 要求使用正确的行首缩进。
- 使用 <spacebar> 键创建正确的缩进。不 <tab> 要使用密钥。使用<tab> 键会在将样本导入 MA 服务时产生编译错误。
- 请勿在字符串两边加引号。仅当字符串包含标点符号（破折号、冒号等）时才在字符串两边加引号。如果要将数字解释为字符串，请在数字两边加引号或使用样本的内置函数 str()。
- YES/Yes/yes/Y/y/NO/no/No/n/N、ON/On/on/OFF/Off/off 和 TRUE/true/truthy/FALSE/False/-false/falsely 这样的文字被视为布尔值，分别等同于是和否。要将它们解释为字符串，请在其两边加引号。例如：
  - “YES”
  - “否”
  - “真”
  - “假”等。

> 注意
>
> 将样本文件导入 Citrix ADM 之前，建议您验证文件是否符合 YAML 格式。Citrix 建议您使用样本中的内置 YAML 验证程序来验证和导入 YAML 内容。
>
> 配置样本时，您只能使用支持创建和删除操作的 Nitro 配置资源（POST 和 DELETE HTTP 方法）。有关详细信息，请参阅 Nitro API 文档。

样本解析

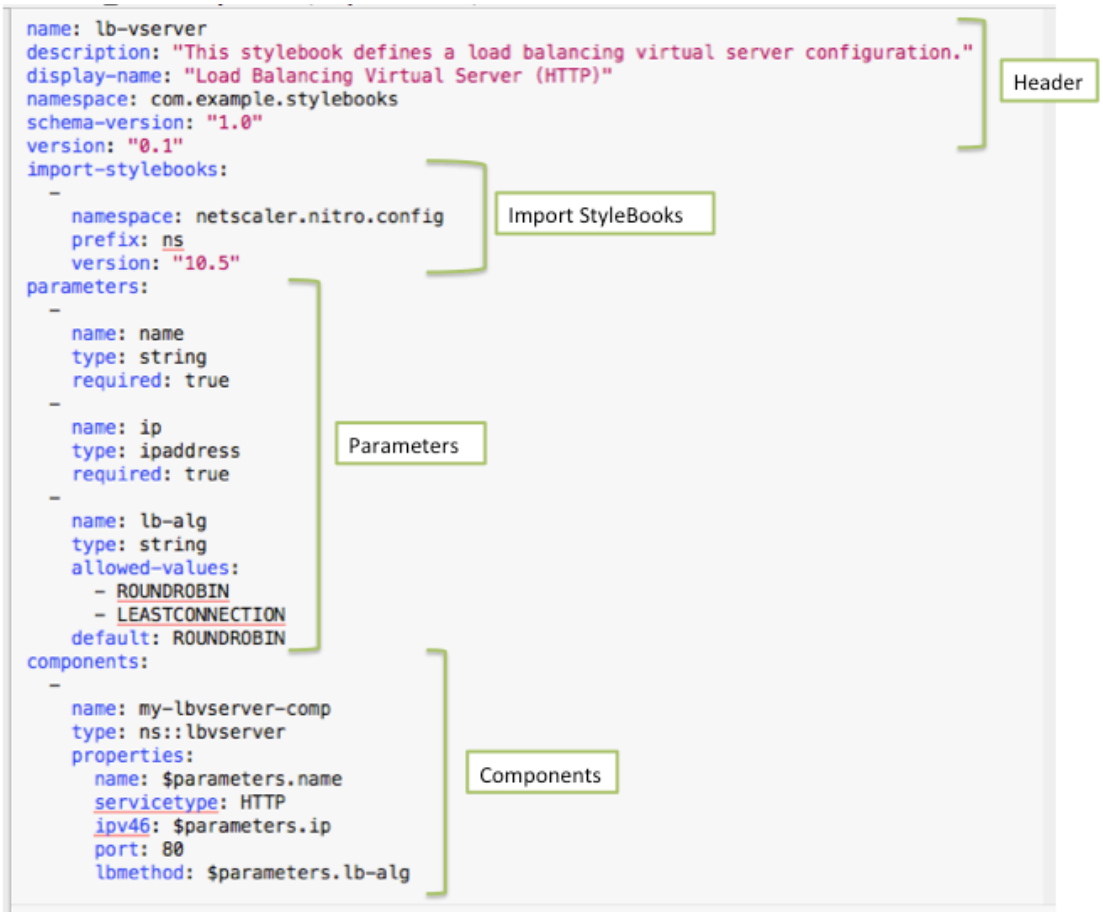
编写样本要求您了解样本的语法、句法和结构。典型的样本包含以下部分：

- 标题：此部分允许您定义样本的标识并描述它的作用。这是必需的部分。

- 导入样本：此部分用于声明要在当前样本中引用哪个其他样本。需要导入 Citrix ADC NITRO 配置样本或其他样本才能编写样本。这是必需的部分。
- 参数：此部分用于定义样本中所需的参数以创建配置。它描述样书接收的输入。这是可选部分。
- 组件：此部分允许您定义样本为特定配置创建的实体（配置对象）。此部分被视为样本的核心。组件通常使用 parameters 部分中提供的输入来改写样本生成的配置。这是可选部分。

  样书可以包含参数部分或组件部分，也可以同时包含两者。如果要定义其他样本可以使用的一组参数，可以使用仅含 parameters 部分的样本。这有利于在一组样本之间重用参数组。如果要在样本中指定属性值，而不是定义参数来接收用户输入，可以使用仅含 components 部分的样本。
- 输出：参数部分定义样本的输入时，此可选部分定义其输出。在此可选输出部分，可以指定要向基于此样本创建配置的用户和导入此样本的其他样本呈现的组件。之后，用户和导入样本可以引用呈现的组件的属性。
- 操作：样本可能包含一个可选部分，用于在作为样本一部分的任何虚拟服务器上启用 Citrix ADM 中的分析。

下图显示了一个简单的样本概况。



以下示例帮助您了解样本的语法和结构，以及如何编写复杂程度不断增加的样本。

- 创建负载平衡虚拟服务器的样本
- 创建基本负载平衡配置的样本

- 创建复合样本
- 使用 GUI 属性自定义样本

创建负载平衡虚拟服务器的样本

April 23, 2021

在此示例中，设计一个创建协议类型为 HTTP 且侦听端口 80 的负载平衡虚拟服务器的基本样本。虚拟服务器名称、IP 地址和负载平衡方法参数接受用户定义的值，即它们是样本的参数。

标题

样书的前六行构成标头部分。在此示例中，标头部分编写如下：

```
name: lb-vserver
description: This StyleBook defines a load balancing virtual server
   configuration.
display-name: Load Balancing Virtual Server (HTTP)
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

标头部分包含以下详细信息：

- **name**：此样本的名称。
- **description**：定义此样本做什么的说明。此描述将显示在 Citrix ADM 上。
- 显示名称：Citrix ADM 上显示的样本的描述性名称。
- **namespace**：样本的唯一标识符的命名空间形式部分，以避免发生名称冲突。
- **schema-version**：在此版本中，其值总是 “1.0”。
- **version**：样本的版本号。可以在更新样本时更改版本号。

name、**namespace** 和 **version** 组合在系统中唯一标识样书。Citrix ADM 中不能有两个具有相同名称、命名空间和版本组合的样本。但可以有两个 name 和 version 相同但 namespace 不同或 namespace 和 version 相同但 name 不同的样本。

> 注意
>
> 假定您已更新您的样本，且您有更新的 version 号。现在，如果您要在其他样本中引用（即您要导入）此样本，请务必也在其他样本中更新 version 号，以便它们使用正确版本的导入样本。

导入样本

标头后面的部分称为 “import-stylebooks”。在此部分中，必须在当前样书中声明要引用的任何其他样书的 namespace 和 version 号。这样可以导入并重用其他样书，而不是在您自己的样书中重新构建相同的配置。

在此示例中，import-stylebooks 部分编写如下：

```
import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
<!--NeedCopy-->
```

直接使用任何一个 NITRO 配置对象的每个样本都必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 Citrix ADC NITRO 类型，例如 Lbvserver。由于支持 10.5 及更高版本的软件版本，您可以使用样本在运行 10.5 及更高版本的任何 Citrix ADC 实例上创建和运行配置。

import-stylebooks 部分中使用的前缀是指代命名空间和版本组合的简写。在此示例中，ns 是指版本为 10.5 的 netscaler.nitro.config。在样本的后面部分，并非使用命名空间和版本来指代被导入样本，可以使用上述示例中选择的前缀字符串，例如 ns。

样本中使用的版本是 Citrix ADC NITRO 版本。基于 Nitro 版本 X 的样本可用于配置 X 或更高版本的任何 Citrix ADC。

> 注意
>
> 为确保您的样本可用于配置 10.5 或更高版本的任何 Citrix ADC 实例，Citrix 建议您在直接使用 Nitro 内置样本的样本中导入 Nitro 10.5 命名空间（命名空间：netscaler.nitro.config，版本：10.5）。

重要的是，导入其他样本的样本必须基于与其导入的样本相同或更高版本的 Nitro 版本。例如，基于 Nitro 10.5 的样本不能依赖或使用或导入基于 11.1 的样本。但是，基于版本 11.1 的样本可以导入基于小于 11.1 的任何版本的样本。

也可能是一个样书根本不导入 Nitro 命名空间。这意味着样本不需要直接定义 Nitro 组件，但可以导入（取决于）定义 Nitro 组件的样本。导入其他样本的样本始终获取其依赖关系层次结构中的最高 Nitro 版本，因此可用于配置该版本或更高版本的 Citrix ADC。

参数

parameters 部分用于声明样本中需要的所有参数。作为样本开发人员，您必须决定您希望样本的用户要指定哪些输入。在此示例中，构建的样本要求其用户提供虚拟服务器的名称、其 IP 地址以及负载平衡方法。

parameters 部分类似如下：

```
parameters:
 -
  name: name
  type: string
```



```
  label: Application Name
  description: Name of the application configuration.
  required: true

-
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: Application VIP that the clients access.
  required: true

-
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the load balancing algorithm (method) used for
     load balancing client request between the application servers.
  allowed-values:
   - ROUNDROBIN
   - LEASTCONNECTION
   default: ROUNDROBIN
<!--NeedCopy-->
```

> 注意
>
> 如果不提供参数的标签，则 Citrix ADM 在显示此参数时使用名称属性。必须始终为参数定义标签，以便控制参数在 Citrix ADM 中的显示方式。
>
> 但使用 API 时，参数由其 name 指定。

在此部分中，声明了三个参数，它们以其 **name** 属性值来指示 - **name** 表示虚拟服务器名称，**ip** 表示虚拟服务器的 IP 地址，以及 **lb-alg** 表示负载平衡方法。

- 类型。这些参数可以采用的值的类型。例如，name 和 lb-alg 可以接收字符串值，ip 值必须属于 IP 地址类型。样本中的参数可以是以下任何内置类型：
- 字符串。字符数组。如果未指定长度，则字符串值可以接收任何数量的字符。但是，可以使用 min-length 和 max-length 属性限制字符串类型的长度。
- 号码。整数。可以使用 min-value 和 max-value 属性指定此类型可以接收的最小数和最大数。
- 布尔值。可以是真的，也可以是假的。另外请注意，所有文字都被 YAML 视为布尔值（例如 Yes 或 No）。
- **IP** 地址。表示有效 IPv4 或 IPv6 地址的字符串。
- **TCP** 端口。介于 0 到 65535 之间的数字，表示 TCP 或 UDP 端口。
- 密码。不透明/秘密字符串值。当 Citrix ADM 显示此参数的值时，它将显示为星号 (*****)。
- 证书文件。证书文件。
- 密钥文件。证书私钥文件。
- 文件。此类型的参数要求用户上传文件，例如证书或密钥文件。

- 对象。由多个元素组成，每个元素都是一个参数。此类型可以用于对一个父参数下多个相关参数进行分组。
- 需要。指出参数是强制参数还是可选参数。如果设置为 true，表示参数是必需的，用户必须在使用此样本创建配置时提供此参数值。默认情况下，所有参数都是可选的。在此示例中，**name** 和 **ip** 是必需参数，而 **lb-alg** 是一个可选参数，其默认值为 “ROUNDROBIN”。“

可使用 **default** 属性为可选参数分配默认值。创建配置时，如果用户未指定值，则使用默认值。例如，**lb-alg** 参数的默认值是 ROUNDROBIN。

可使用 **allowed-values** 属性来定义用户创建配置时可从中选择的特定值。在此示例中，为 **lb-alg** 参数指定了两个值 - ROUNDROBIN 和 LEASTCONNECTION。

当您导入样本并使用它时，Citrix ADM 会显示一个包含这三个参数的表单。显示的 name 和 ip 字段用于输入字符串和 IP 地址类型的值，lb-alg 字段显示为下拉列表，在其中 ROUNDROBIN 选为默认值。

> 注意
>
> 除了内置类型外，参数的类型还可以是另一个样本。这就是重用其他样本中定义的参数的方式。

组件

此样本的最后一部分称为 components 部分，它被视为样本中最重要的部分。在此部分，定义必须由样本创建的配置对象。

例如，必须按如下所示编写 components 部分：

```
components:
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

此示例仅包含一个组件。组件的主要属性是 name、type 和 properties。组件的类型确定此组件提供哪些属性。组件有两种类型：

- 内置类型。此类型由系统提供，您不必定义它，例如，NITRO 实体类型为 “lbvserver” 或 “服务组”。在此实例中，使用的是内置组件类型。
- 复合类型。此类型是您创建并导入到 Citrix ADM 中的样书或 Citrix ADM 附带的默认样书。您可以在中了解有关复合样本的详细信息创建复合样书。

在此示例中，您定义了一个名为 **lbvserver-comp** 的组件。此组件的类型为 **ns lbvserver**（内置硝基类型），其中“ns”是引用命名空间 netscaler.nit.config 和版本 10.5 的前缀，而“lbvserver”是此命名空间中的硝基资源。

此处定义的 **properties** 是“lbvserver”资源的属性。要了解有关所有可用 Citrix ADC Nitro 资源及其属性的详细信息，请参阅Citrix ADC NITRO REST API 文档。

此部分中的属性包括“lbvserver”资源的必需属性，用于为这些属性指定值。在此示例中，为 servicetype 和 port 指定静态值，而 name、ipv46 和 lbmethod 属性从输入参数获取其值。在样书的其余部分中，可以使用 **$parameters.<parameter-name>** 表示法（例如 **$parameters.ip**）来引用在 parameters 部分定义的参数名称。

> 注意
>
> 按照惯例，前缀“ns”始终用于在“导入样书”部分中指定 Citrix ADC Nitro 命名空间。尽管这不是必需的，但 Citrix 建议在您自己的样本中采用相同的约定以保持一致性。

构建您的样本

现在已定义了此样本的所有必要部分，将它们全部汇聚在一起即可构建您的第一个样本。将样本内容复制并粘贴到一个文本编辑器，然后将文件保存为 **lb-vserver.yaml**。Citrix 建议您使用样本中的内置 YAML 验证程序来验证和导入 YAML 内容。

lb-vserver.yaml 文件的完整内容再现如下：

```
name: lb-vserver
namespace: com.example.stylebook
version: "1.0"
display-name: Load Balancing Virtual Server (HTTP)
description: "This stylebook defines a very simple load balancing HTTP
    virtual server configuration"
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
 -
  namespace: com.citrix.adc.stylebooks
  version: "1.0"
  prefix: stlb

parameters:
 -
  name: name
  label: "Application Name"
```



```
  description: "Give a name to the application configuration."
  type: string
  required: true
 -
  name: vip-ipaddress
  label: "Load Balancer IP Address"
  description: "The Application VIP that clients access"
  type: ipaddress
  required: true
 -
  name: lb-alg
  label: LB Algorithm
  description: Load Balancing Algorithm
  type: string
  default: ROUNDROBIN
  allowed-values:
   - ROUNDROBIN
   - LEAST-CONNECTION

components:
 -
  name: lbvserver-comp
  description: This StyleBook component (a Builtin Nitro StyleBook)
     builds a Citrix ADC load balancing virtual server configuration
     object.
  type: ns::lbvserver
  properties:
   name: $parameters.name
   ipv46: $parameters.vip-ipaddress
   lbmethod: $parameters.lb-alg
   servicetype: HTTP
   port: 80
<!--NeedCopy-->
```

要开始使用样本创建配置，您必须将其导入 Citrix ADM，然后使用它。有关详细信息，请参阅 如何使用用户定义的样本。

还可以将此样本导入其他样本（使用 import-stylebooks 构造）。或者，可以修改此样本以包含更多参数和组件，如下一节中所述。

创建基本负载平衡配置的样本

April 23, 2021

在上一个示例中，您已构建了一个基本样本来创建负载平衡虚拟服务器。可以用不同的名称保存此样本，然后对其更新以包含用于基本负载平衡配置的其他参数和组件。将此样本文件保存为 **basic-lb-config.yaml**。

在本节中，将设计一个新样本，用于创建由负载平衡虚拟服务器、服务组和一组服务组成的负载平衡配置。它还将服务绑定至服务组，并将服务组绑定至虚拟服务器。

标题

要构建此样本，必须先更新标头部分。此部分与为负载平衡虚拟服务器样本创建的标头部分类似。在标头部分中，将 **name** 值更改为 basic-lb-config。此外，更新 **description** 和 **display-name** 以适当说明此样本。不必更改 **namespace** 和 **version** 值。因为已更改了名称，所以 name、namespace 和 version 组合构成了此样本在系统中的唯一标识符。

```
name: basic-lb-config
description: This StyleBook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

导入样本

import-stylebooks 部分保持不变。它引用 netscaler.nitro.config 命名空间以使用 Nitro 配置对象。

```
import-stylebooks:
 -
 namespace: netscaler.nitro.config
 prefix: ns
 version: "10.5"
<!--NeedCopy-->
```

参数

必须更新 parameters 部分以添加两个其他参数来定义一组服务或服务器以及服务侦听的端口。前三个参数 name、ip 和 lb-alg 保持不变。

```
parameters:
 -
 name: name
 type: string
 label: Application Name
```



```
 description: Name of the application configuration
 required: true
  -
   name: ip
   type: ipaddress
   label: Application Virtual IP (VIP)
   description: Application VIP that the clients access
   required: true
  -
   name: lb-alg
   type: string
   label: LoadBalancing Algorithm
   description: Choose the load balancing algorithm used for load
       balancing client requests between the application servers.
     allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
      default: ROUNDROBIN
  -
   name: svc-servers
   type: ipaddress[]
   label: Application Server IPs
   description: The IP addresses of all the servers of this application
   required: true
  -
   name: svc-port
   type: tcp-port
   label: Server Port
   description: The TCP port open on the application servers to receive
       requests.
   default: 80
<!--NeedCopy-->
```

在此示例中，添加参数 **svc-servers** 以接受代表应用程序后端服务器的服务的 IP 地址列表。这是必需参数，由 **required: true** 指明。第二个参数 **svc-port** 表示服务器侦听的端口号。如果用户未指定，svc-port 参数的默认端口号是 80。

组件

必须还要更新 components 部分以定义其他组件，以便它们可以使用两个新参数并构建完整的负载平衡配置。

例如，必须按如下所示编写 components 部分：

```
components:
 -
```



```
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg

components:
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
   name: $parameters.name + "-svcgrp"
   servicetype: HTTP

components:
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $parent.parent.properties.name
   servicegroupname: $parent.properties.name
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

在此示例中，原始组件 **lbvserver-comp**（来自前面的示例）现在有一个名为 **svcg-comp** 的子组件。而且，**svcg-comp** 组件中有两个子组件。通过在一个组件里面嵌套另一个组件，嵌套的组件可以通过引用父组件中的属性来创建配置对象。嵌套的组件可以为父组件中创建的每个对象创建一个或多个对象。

svcg-comp 组件用于通过使用为资源“服务组”属性提供的值在 Citrix ADC 实例上创建服务组。在此示例中，为 servicetype 指定静态值，而 name 从输入参数获取其值。您可以通过使用 ****$** 参数部分中定义的参数名称。**name + “-svcgrp”** 表示法来 ****** 引用参数名称，其中-svcgrp 附加（连接）到用户定义的名称。

组件 **svcg-comp** 有两个子组件，**lbvserver-svg-binding-comp** 和 **members-svcg-comp**。

第一个子组件 **lbvserver-svg-binding-comp** 用于在由其父组件创建的服务组和由父组件创建的负载平衡虚拟服务

器 (lbvserver) 之间绑定配置对象。$parent 表示法（也称为父引用）用于引用父组件中的实体。例如，服务组名称：**$parent.** 属性**.name** 指由父组件 **svcg-comp** 创建的服务组，名称：**$ parent .parent**。属性名称指由父组件创建的虚拟服务器 服务器**-**比赛。

成员 **svcg** 组件用于将服务列表之间的配置对象绑定到父组件创建的服务组。创建多个绑定配置对象是通过使用样书的重复构造迭代参数 **svc-servers** 中指定的一组服务器来完成。在迭代过程中，此样书组件为服务组中的每个服务（在 **repeat-item** 构造中被称为 srv）创建类型为 **servicegroup_servicegroupmember_binding** 的 Nitro 配置对象，并将每个 Nitro 配置对象中的 **ip** 属性设置为对应服务器的 IP 地址。

通常，您可以使用组件中 的重复项和重复项结构来使该组件构建同一类型的多个配置对象。您可以将变量名指定给 重复项结构，例如 srv，以指定迭代中的当前值。此变量名称在相同组件或子组件的属性中作为 **$<varname>**（例如 $srv）来引用。

在上述示例中，使用了在组件中相互嵌套组件来轻松构造此配置。在此特殊情况下，嵌套组件不是唯一的配置构建方式。您可以在没有嵌套的情况下实现相同的结果，如下所示：

```
components:
 -
  name: members-svcg-comp
  type: ns::servicegroup_servicegroupmember_binding
  repeat: $parameters.svc-servers
  repeat-item: srv
  properties:
   ip: $srv
   port: str($parameters.svc-port)
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-svg-binding-comp
  type: ns::lbvserver_servicegroup_binding
  properties:
   name: $components.lbvserver-comp.properties.name
   servicegroupname: $components.svcg-comp.properties.name
 -
  name: lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name + "-lb"
   servicetype: HTTP
   ipv46: $parameters.ip
   port: 80
   lbmethod: $parameters.lb-alg
 -
  name: svcg-comp
  type: ns::servicegroup
  properties:
```



```
30    name: $parameters.name + "-svcgrp"
31    servicetype: HTTP
32  <!--NeedCopy-->
```

在这里，所有组件都处于相同级别（也就是说，它们不嵌套），但实现的结果（生成的 Citrix ADC 配置）与之前使用的嵌套组件相同。此外，样本中组件的声明顺序不影响配置对象的创建顺序。在此示例中，组件 **svcg-comp** 和 **lbvserver-comp** 尽管最后声明，但必须在构建第二个组件 **lbvserver-svg-bindingcomp** 之前构建，因为在第二个组件中存在对这些组件的前向引用。

> 注意
>
> 按约定，样本的名称、parameters、substitutions、components 和 outputs 采用小写。如果它们包含多个词语，词语以 “-” 字符分隔。例如 “lb-bindings”、“app-name”、“rewrite-config” 等。另一个约定是为组件名称添加后缀 “-comp” 字符串。

输出

可以添加到新样本的最后一个部分是 outputs 部分，在其中指定在此样本用于创建配置后，此样本向其用户呈现的内容（或在其他样本中）。例如，可以在 outputs 部分指定要呈现将由此样本创建的 lbvserver 和 servicegroup 配置对象。

```
1  outputs:
2   -
3    name: lbvserver-comp
4    value: $components.lbvserver-comp
5    description: The component that builds the Nitro lbvserver
        configuration object
6   -
7    name: servicegroup-comp
8    value: $components.svcg-comp
9    description: The component that builds the Nitro servicegroup
        configuration object
10 <!--NeedCopy-->
```

样书的 outputs 部分是可选的。样书不必返回输出。但是，如果将一些内部组件作为输出返回，导入此样本的任何样本就可以有更大的灵活性，这在创建复合样本时可以看到。

> 注意
>
> 最好在 outputs 部分呈现样本的整个组件，而不仅仅是组件的单个属性（例如，呈现整个 $components.lbvserver-comp，而不仅仅是名称 $components.lbvserver-comp.properties.name）。另外在输出中添加说明，解释特定输出表示的内容。

构建您的样本

现在已定义了此样本的所有必要部分，将它们全部汇聚在一起即可构建您的第二个样本。已将此样本文件保存为 **basic-lb-config.yaml**。Citrix 建议您使用样书页中的内置 YAML 验证程序来验证和导入 YAML 内容。

basic-lb-config.yaml 文件的完整内容再现如下：

```
name: basic-lb-config
namespace: com.example.stylebooks
version: "0.1"
display-name: Load Balancing Configuration
description: This StyleBook defines a simple load balancing
   configuration.
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "10.5"
  prefix: ns
parameters:
 -
  name: name
  type: string
  label: Application Name
  description: Give a name to the application configuration.
  required: true
 -
  name: ip
  type: ipaddress
  label: Application Virtual IP (VIP)
  description: The Application VIP that clients access
  required: true
 -
  name: lb-alg
  type: string
  label: LoadBalancing Algorithm
  description: Choose the loadbalancing algorithm (method) used for
     loadbalancing client requests between the application servers.
  allowed-values:
     - ROUNDROBIN
     - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: svc-servers
  type: ipaddress[]
```



```
38    label: Application Server IPs
39    description: The IP addresses of all the servers of this application
40    required: true
41
42  components:
43   -
44    name: lbvserver-comp
45    type: ns::lbvserver
46    properties:
47     name: $parameters.name + "-lb"
48     servicetype: HTTP
49     ipv46: $parameters.ip
50     port: 80
51     lbmethod: $parameters.lb-alg
52   -
53    name: svcg-comp
54    type: ns::servicegroup
55    properties:
56      servicegroupname: $parameters.name + "-svcgrp"
57      servicetype: HTTP
58
59   -
60    name: lbvserver-svg-binding-comp
61    type: ns::lbvserver_servicegroup_binding
62    properties:
63     name: $components.lbvserver-comp.properties.name
64     servicegroupname: $components.svcg-comp.properties.servicegroupname
65   -
66    name: members-svcg-comp
67    type: ns::servicegroup_servicegroupmember_binding
68    repeat: $parameters.svc-servers
69    repeat-item: srv
70    properties:
71     ip: $srv
72     port: 80
73     servicegroupname: $components.svcg-comp.properties.servicegroupname
74  outputs:
75  -
76    name: lbvserver-comp
77    value: $components.lbvserver-comp
78    description: The component that builds the Nitro lbvserver
         configuration object
79  -
80    name: servicegroup-comp
81    value: $components.svcg-comp
```



```
82    description: The component that builds the Nitro servicegroup
         configuration object
83  <!--NeedCopy-->
```

要开始使用样本创建配置，您必须将其导入 Citrix ADM，然后使用它。有关详细信息，请参阅 如何使用用户定义的样本。

还可以将此样本导入其他样本并使用其属性，如下一节中所述。

创建复合样本

April 23, 2021

样本一个重要的强大功能是它们可以用作其他样本的构建块。样本可以导入到另一个样本中，它可以被称为第二个样本的组件使用的类型，类似于 Nitro 内置样本。

例如，您可以使用上一节中构建的 基本 **lb-config** 样书来构建另一个名为 复合示例的样书。要使用 “basic-lb-config” 样本，必须在新样本的 import-stylebooks 部分将其导入。

构建您的样本

新样本类似如下：

```
1  name: composite-example
2  namespace: com.example.stylebooks
3  version: "0.1"
4  display-name: Load Balancing Virtual Server (HTTP/RoundRobin)
5  description: This StyleBook defines a RoundRobin load balancing
      configuration with a monitor.
6  schema-version: "1.0"
7  import-stylebooks:
8    -
9     namespace: netscaler.nitro.config
10    version: "10.5"
11    prefix: ns
12   -
13    namespace: com.example.stylebooks
14    version: "0.1"
15    prefix: stlb
16 parameters:
17   -
18     name: name
19     type: string
20     label: Application Name
```



```
21      description: Give a name to the application configuration.
22      required: true
23    -
24      name: ip
25      type: ipaddress
26      label: Application Virtual IP (VIP)
27      description: The Application VIP that clients access
28      required: true
29    -
30      name: svc-servers
31      type: ipaddress[]
32      label: Application Server IPs
33      description: The IP addresses of all the servers of this
           application
34      required: true
35
36    -
37      name: response-code
38      type: string[]
39      label: List of Response Codes
40      description: List of Response Codes - Provide a list of response
           codes in integer.
41
42  components:
43    -
44      name: basic-lb-comp
45      type: stlb::basic-lb-config
46      description: This component's type is another StyleBook that builds
           the NetScaler lbvserver, servicegroups and services
           configuration objects.
47      properties:
48       name: $parameters.name
49       ip: $parameters.ip
50       svc-servers: $parameters.svc-servers
51    -
52       name: monit-comp
53       type: ns::lbmonitor
54       description: This component is a basic Nitro type (a Builtin
           StyleBook) that builds the NetScaler monitor configuration
           object.
55       properties:
56         monitorname: $parameters.name + "-mon"
57         type: HTTP
58         respcode: $parameters.response-code
59         httprequest: "'GET /'"
```



```
60          lrtm: ENABLED
61          secure: "YES"
62
63        components:
64           -
65             name: monit-svcgrp-bind-comp
66             type: ns::servicegroup_lbmonitor_binding
67             properties:
68               servicegroupname: $components.basic-lb-comp.outputs.
                    servicegroup-comp.properties.servicegroupname
69               monitor_name: $parent.properties.monitorname
70  <!--NeedCopy-->
```

在 import-stylebooks 部分，使用 basic-lb-config 样本的命名空间和版本将其导入，引用时加前缀 “stlb”。

在 components 部分，定义了两个组件。第一个组件是 **stlb::** 基本 **lb-config** 类型，其中 “基本 lb-config” 是您在中创建的样本的名称创建基本负载平衡配置的样本。为此组件定义的数据对应于 basic-lb-config 样本中声明的必需参数。但是，您可以使用样本的任何参数（必填参数和可选参数）。而不是重新构建 lbvserver、服务组以及服务和服务组绑定，而是导入样本作为组件执行所有这些操作的样本，并使用它在新样本中创建这些配置对象。

样书添加第二个组件 “monit-comp”（使用 Nitro 资源 “lbmonitor”（内置样书）的属性）来创建监视器配置对象。它还有子组件 “monit-svcgrp-bind-comp” 用来创建绑定配置对象，该对象将监视器绑定到第一个组件中创建的服务组。由于在 “基本 Lb-config” 样本中创建的服务组组件作为输出显示，因此此样本可以使用表达 式 **$** 组件**.basents.lb-comp.outputs.Servicegroup-comp** 访问它。此示例说明导入样本如何能够使用 outputs 部分来访问原本无法访问的被导入样本中的组件。

接下来，将样本内容复制并粘贴到文本编辑器，然后将该文件另存为 合成，**example.yaml**。在 Citrix ADM 中导入文件之前，请确保验证 YAML 内容。然后，将其导入 Citrix ADM 并使用此样本创建一个或多个配置。

Citrix 建议您使用样本中的内置 YAML 验证程序来验证和导入 YAML 内容。

在自定义样本中使用 **GUI** 属性

April 23, 2021

您可以在样书的参数部分中添加 GUI 属性，以便在 Citrix Application Delivery Management (ADM) 上显示时使字段直观。

示例。您可以使用 label 属性为参数添加描述性名称，并使用描述属性为此参数添加工具提示。

```
1  name: ip
2  label: Virtual Server IP Address
3  description: IP address of the virtual server that represents the load
      balanced application.
```



```
type: ipaddress
required: true
<!--NeedCopy-->
```

示例。如果您有类型对象的参数，则可以使用 **gui** 属性定义布局。在此示例中，布局是字段以两列显示的可折叠对象。

```
name: svcg-advanced
label: Advanced Application Server Settings
type: object
required: false
gui:
 collapse_pane: true
 columns: 2
<!--NeedCopy-->
```

示例。Citrix ADM 上的某些样书仅用作其他样书的构建块。而且，您可能不希望用户直接从这些样本创建配置。因为这些样本将用作其他样本的一部分。将样本标记为专用，以确保样本未直接用于在 Citrix ADM GUI 中创建配置。

```
name: basic-lb-config
description: This stylebook defines a simple load balancing
   configuration.
display-name: Load Balancing Configuration
namespace: com.example.stylebooks
private: true
schema-version: "1.0"
version: "0.1"
<!--NeedCopy-->
```

导入自定义样书

April 23, 2021

构建样本后，必须将其导入 Citrix Application Delivery Management (ADM) 才能使用它。Citrix ADM 允许您以 YAML 形式导入单个样本或多个样本 YAML 文件作为.zip、.tgz 或.gz 形式的捆绑包导入。Citrix ADM 系统在导入时验证您的样本。样书现在可用于创建配置。

Citrix ADM 还具有内置的 YAML 编辑器，您可以使用该编辑器来撰写样本 YAML 内容。YAML 编辑器允许您从 Citrix ADM GUI 本身验证 YAML 构造。您无需为这些验证检查使用单独的工具。内容根据 YAML 标准进行验证，并突出显示任何偏差。然后，您可以更正内容并尝试将样本导入 Citrix ADM。内置的 YAML 编辑器在编写自己的样本时提供了两个优势。

- 颜色编码。编辑器显示按照 YAML 指南解析的样书内容，颜色编码可帮助您轻松区分键和 YAML 内容中定义的值。

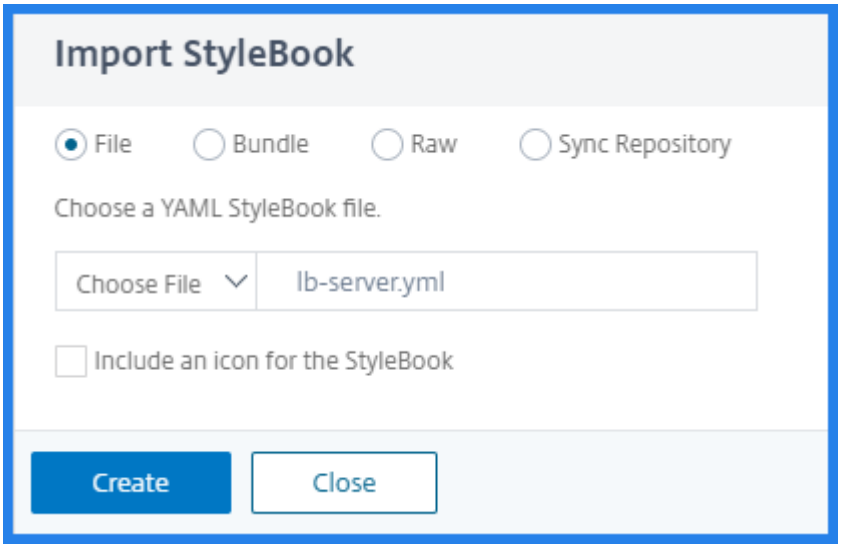
- **YAML** 验证。在您输入时，系统会验证内容是否存在任何 YAML 错误，并且任何偏差都会立即突出显示。此验证允许您在 ADM 中导入样书之前编写符合 YAML 准则的文本。

> 注意
>
> 目前，编辑器根据 YAML 准则验证内容。它不验证代码的正确性和印刷错误。

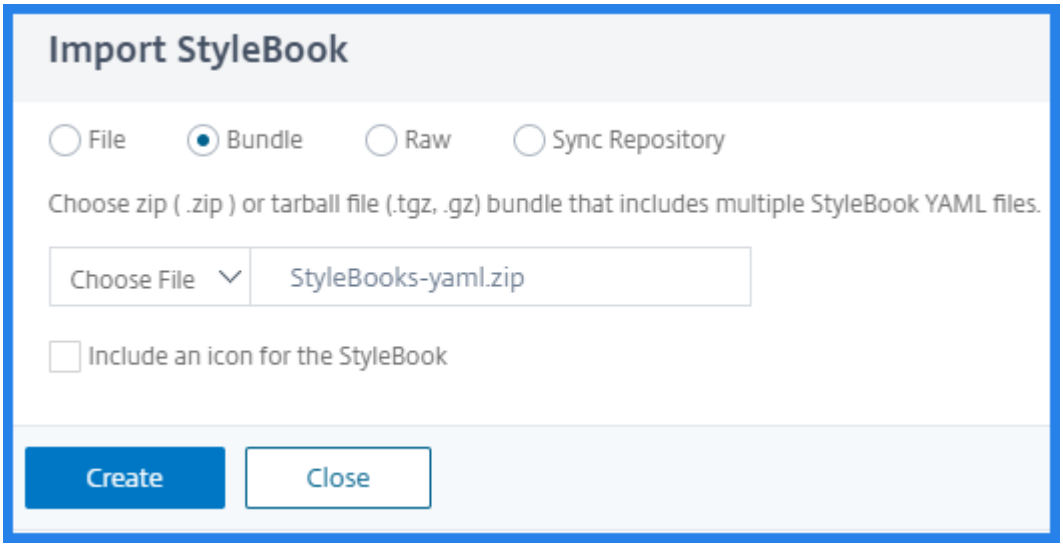
导入样书

1. 在 Citrix ADM 中，导航到 应用程序 > 配置 > 样本”，然后单击 导入新样本。
2. 单击以下选项之一以导入样书。
   - 文件 -从本地存储中选择所需的文件或文件捆绑包。

     > 注意
     >
     > 在此示例中，导入您在中创建的 `lb-vserver.yml` 样书 用于创建负载平衡虚拟服务器的样本。

   - 捆绑 -Citrix ADM 允许您以 YAML 格式导入多个样本。您可以导入多个以压缩 (.zip) 格式或压缩 (.tgz, .gz) 格式压缩的 YAML 样书文件。



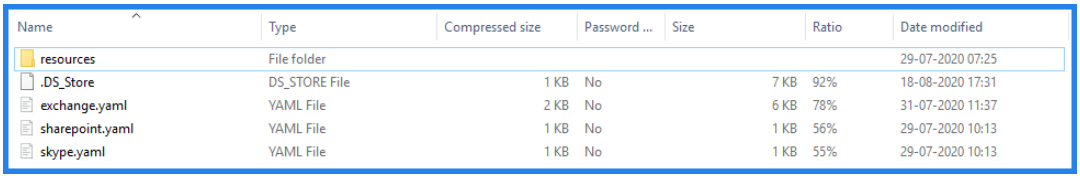
现在，您可以在捆绑包中的每个样书中添加图标。确保包含 PNG、GIF 或 JPEG 格式的图标的资源文件夹。如果图标文件名与样书名称匹配，则图标会自动映射到样书。否则，请执行以下操作：

a) 将 `icon_mapping.json` 文件添加到资源文件夹中。

b) 按如下方式映射 `icon_mapping.json` 文件中的样书和图标：

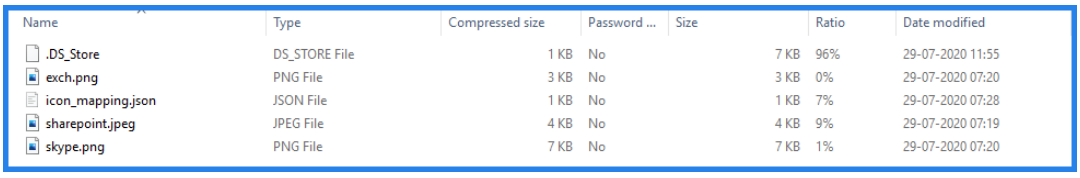
```
<StyleBook file name> : <icon file name>
<!--NeedCopy-->
```

以下是示例样书捆绑包：



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
resources	File folder					29-07-2020 07:25
.DS_Store	DS_STORE File	1 KB	No	7 KB	92%	18-08-2020 17:31
exchange.yaml	YAML File	2 KB	No	6 KB	78%	31-07-2020 11:37
sharepoint.yaml	YAML File	1 KB	No	1 KB	56%	29-07-2020 10:13
skype.yaml	YAML File	1 KB	No	1 KB	55%	29-07-2020 10:13

`resources` 文件夹包含所需的图标。



Name	Type	Compressed size	Password ...	Size	Ratio	Date modified
.DS_Store	DS_STORE File	1 KB	No	7 KB	96%	29-07-2020 11:55
exch.png	PNG File	3 KB	No	3 KB	0%	29-07-2020 07:20
icon_mapping.json	JSON File	1 KB	No	1 KB	7%	29-07-2020 07:28
sharepoint.jpeg	JPEG File	4 KB	No	4 KB	9%	29-07-2020 07:19
skype.png	PNG File	7 KB	No	7 KB	1%	29-07-2020 07:20

在此示例中，`sharepoint.yaml` 和 `skype.yaml` 文件分别自动映射到 `sharepoint.jpeg` 和 `skype.png`。

要映射 `exchange.yaml` 到 `exch.png`，请在 `icon_mapping.json` 文件中指定以下内容：

```
{

"exchange.yaml":"exch.png"
 }
```



```
5
6   <!--NeedCopy-->
```

如果指定 `defaulticon` 条目，则样书将映射到默认图标，除非它们映射到其他图标。

```
1   defaulticon: <icon file name>
2   <!--NeedCopy-->
```

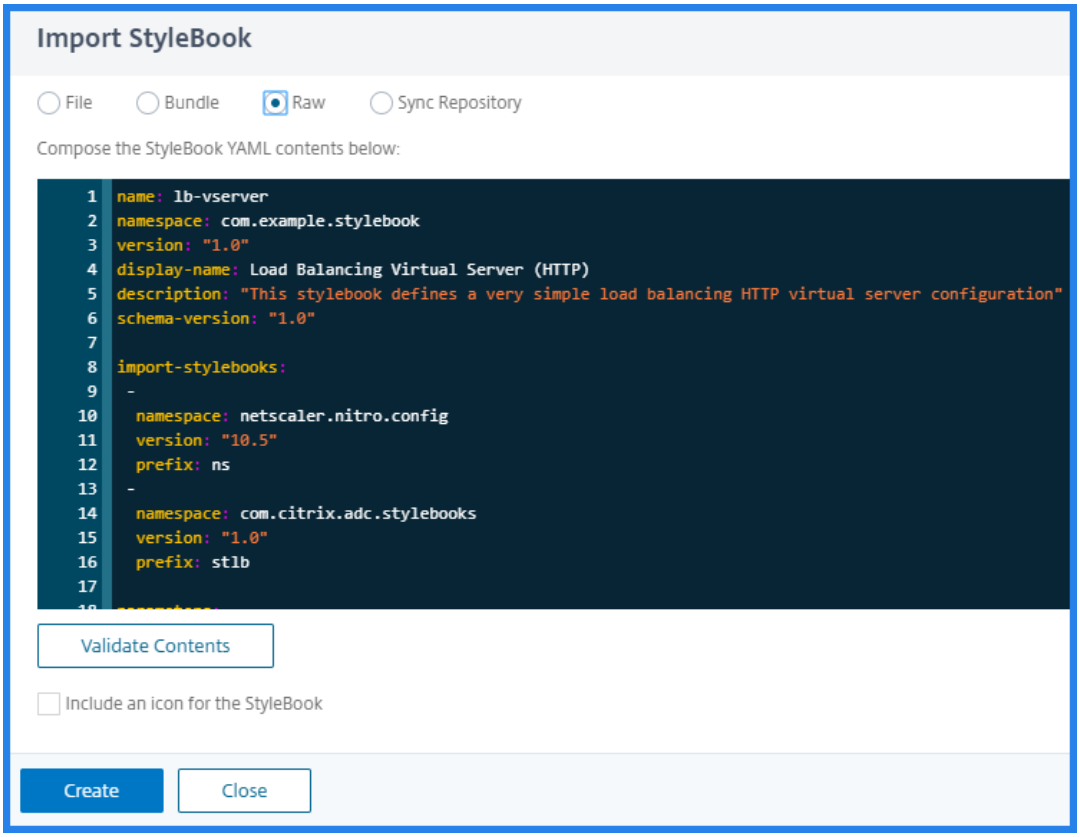
在 应用程序 **>** 样书中，导入的样书随映射的图标一起显示。

- **Raw** -在 YAML 编辑器中撰写样本的内容。

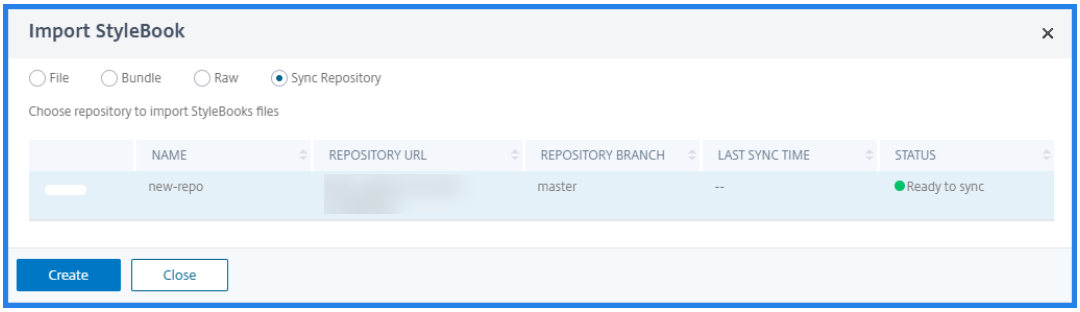
  您可以验证样书内容以检查样书语法错误。要验证样书内容，请单击 验证内容。

  > 注意
  >
  > 在撰写样书时，请确保了解以下概念：
  >
  > - NITRO API
  > - YAML

  有关如何编写自己的样本的更多信息，请参阅如何创建您自己的样本。



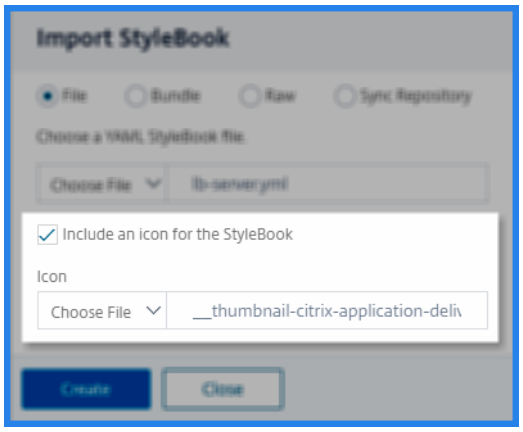
- 同步存储库 -此选项列出添加到 ADM 的存储库。选择要与 ADM 同步的存储库。



> 注意
>
> 您还可以将样书 YAML 文件中的内容复制并粘贴到 YAML 编辑器中。

3. 可选，选择样书的图标。

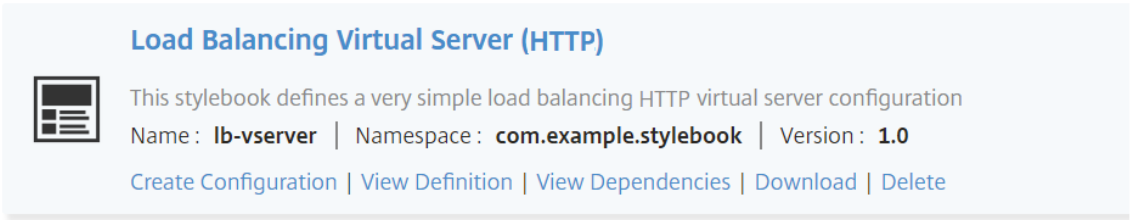
   在 “ 应用程序” > “样书” 中，导入的样书将显示带有此图标。



4. 单击创建。

   Citrix ADM 现在根据样本语法验证样本是否存在所有语法和语义错误。如果存在任何错误，则不会将样本导入到 Citrix ADM 中。

   如果没有错误，则样书将成功导入并在 样书页面上列出。您可以通过在样本的标题部分中定义的显示名称来识别样本。



> 注意
>
> 如果要导入文件包，Citrix ADM 会解压缩压缩文件夹并验证所有样本。
> 即使一个样本文件未通过验证测试，也不会导入捆绑包。

有关样本语法和不同构造和属性语法的更多信息，请参阅样本语法。

5. 单击 创建配置链接可通过此样书创建配置。

   样本将以用户界面页面形式打开，您可以在此为此样本中定义的所有参数输入值。

6. 指定参数所需值。

   在下面的例子中，

   a) 指定 应用程序名称和 负载均衡器 **IP** 地址必填字段。

   b) 从列表中选择负载平衡算法。默认情况下，将选择 “ **ROUNDROBIN** ”。

   ![示 例 配 置 部 署] (/en-us/citrix-application-delivery-management-software/media/nmas-stylebooks-yaml-editor-4.png)

7. 在 目标实例下，选择要在其中部署配置的 Citrix ADC 实例的 IP 地址。

   您还可以根据需要指定任意数量的目标实例，在多个 Citrix ADC 上部署配置。

8. 如果要在部署配置之前在 Citrix ADC (NITRO) 配置对象进行测试，请单击 “ 干运行”。

   如果配置有效，则会根据指定的值创建配置对象。

   在此示例中，样书只创建一个类型的对象 `lbvserver`。此负载平衡服务器是此基本示例样书中定义的唯一组件。

   稍后，单击 创建以在选定的 Citrix ADC 实例上部署配置。

成功部署配置后，“配置” 页面中将显示一个新的 配置包。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

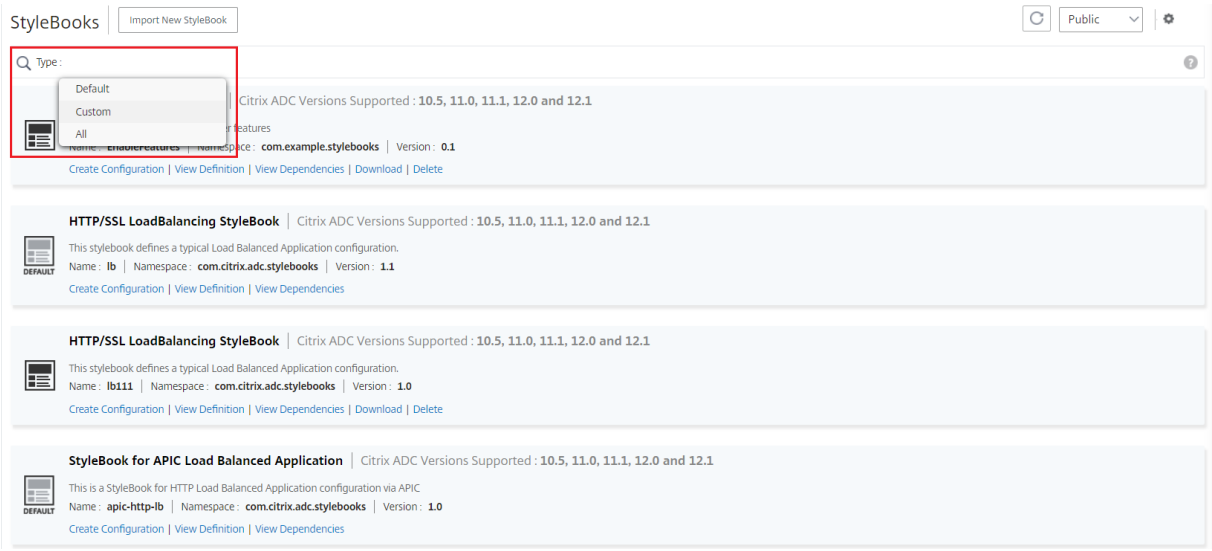
搜索自定义样本

Citrix ADM 现在允许您根据样本类型搜索样本。也就是说，您现在可以搜索默认样本或自定义样本。当您必须在许多默认样书中搜索用户定义的样书时，此选项尤其有用。

搜索自定义样本

1. 在 Citrix ADM 中，导航到 应用程序 > 配置 > 样本。
2. 单击右上角的搜索图标。
3. 在搜索栏中，选择 “ 类型”，然后从子列表中选择 “ 自定义”。

4. Citrix ADM 仅显示用户定义的样本。



创建和编辑配置包

April 23, 2021

在 Citrix Application Delivery Management (ADM) 中，您可以从样书创建配置包。此外，配置包与创建它的样书相关联。配置包的更新是通过与其绑定的样书进行的。

创建配置包

执行以下操作以从样书创建配置包：

1. 导航到 应用程序 > 样书 > 配置。
2. 单击添加。
3. 在 选择样书中，选择要从中创建配置包的所需样书。

   此页面将样书分类为默认样书和自定义样书。选择相应的选项卡以查找所需的样书。
4. 指定所需的详细信息，例如应用程序名称、IP 地址、端口或协议类型。

   图形用户界面字段因样书而异于另一个样书。
5. 在 目标实例中，选择要运行配置的实例或实例组。

   > 注意：
   >
   > 您可以通过根据需要指定任意数量的目标实例，在多个 Citrix ADC 上部署配置。

6. 单击试运行。

   “对 象” 页面显示已创建、修改或从 Citrix ADC 实例中删除的对象。

7. 单击 “创建”

   配置包将显示在 样书 **>** 配置页面中。

如果要编辑现有配置包，请选择配置包，然后单击 编辑。

更改配置包的样书

有时，您需要更新样书以添加功能或修复问题。如果您已经使用旧的样书创建了配置包，则可能需要更新它们以使用新的更新后的样书。要使用新的样书，请更改配置包的现有样书。

考虑在 **ADC** 实例上部署基本负载均衡器配置的样本书示例。而且，您可以从此样书中创建配置包 CP1。

如果要使用基本负载均衡器配置来配置监视器，则需要新的样书。因此，请创建 **Example-lb-mon** 样书，其中包括配置监视器以及基本负载均衡器配置的功能。

创建样书后，请更新现有配置包 CP1 以添加一些监视器。为此，请执行以下操作：

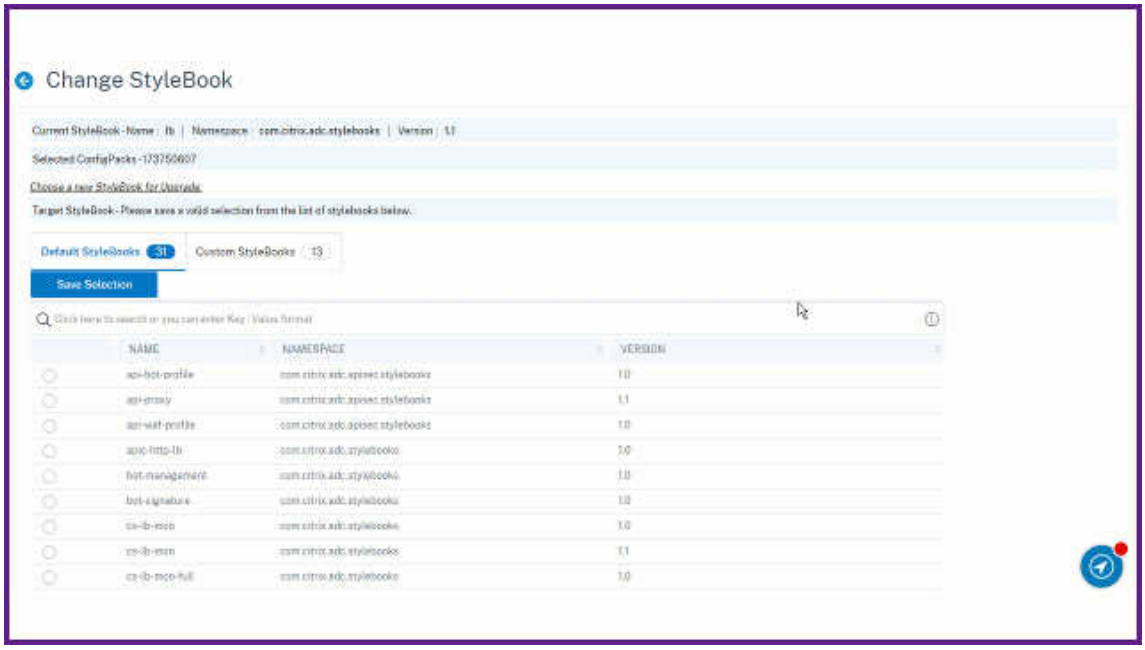
1. 导航到 应用程序 **>** 样书 **>** 配置。
2. 选择要更改样书的配置包。

   在此示例中，从列表中选择 CP1。

3. 单击 “ 更改样书”。
4. 从列表中选择所需的样书。然后，单击 “ 保存选择”。
5. 单击 **Change**（更改）。

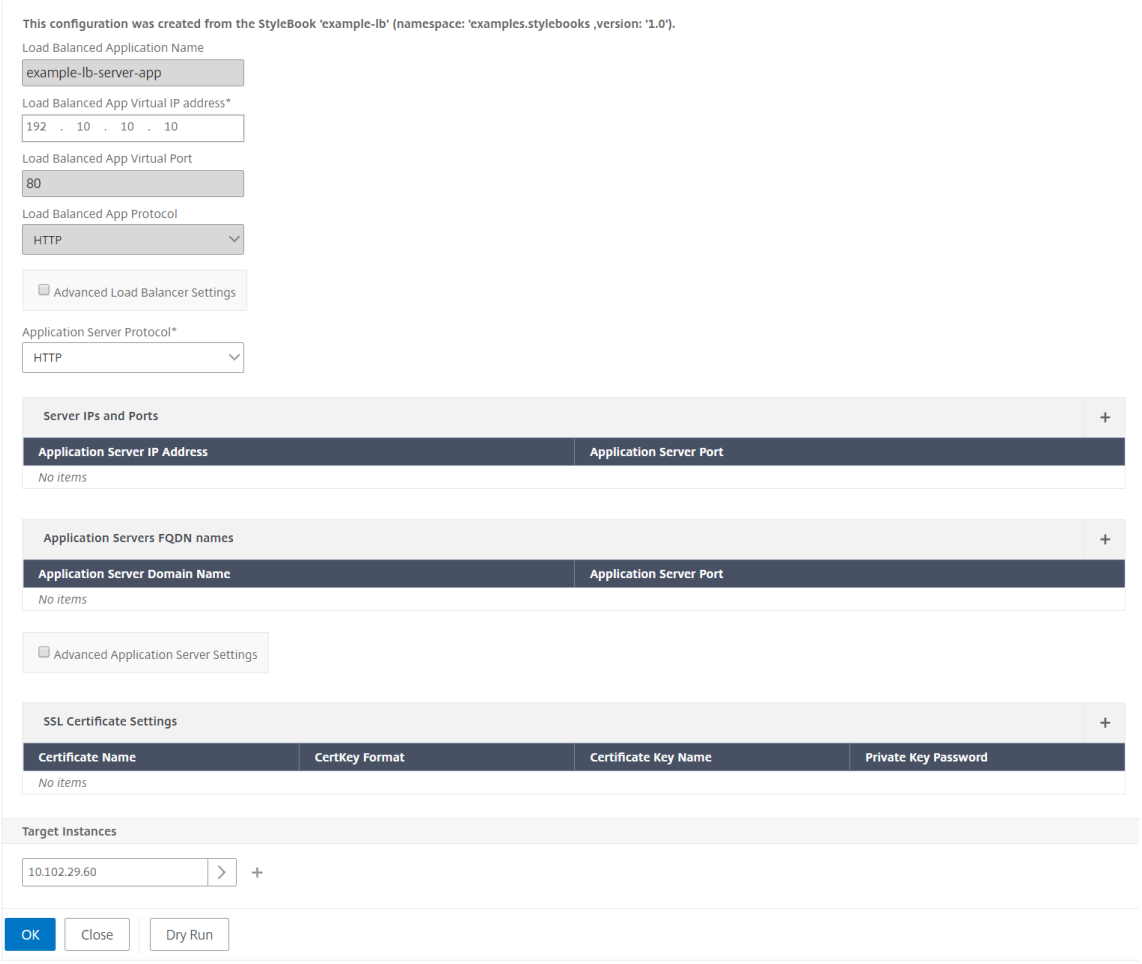
   在此示例中，从列表中选择 例子**-lb-mon** 。

   更改配置包的样书时，新样书中的参数可能具有与现有样书不同的结构。如果参数结构与之前的样书类似，则参数的值将自动保留在各自的字段中。否则，只有两个样书之间具有相同结构的参数才会被传输。例如，相同的参数名称、类型、参数父级等。

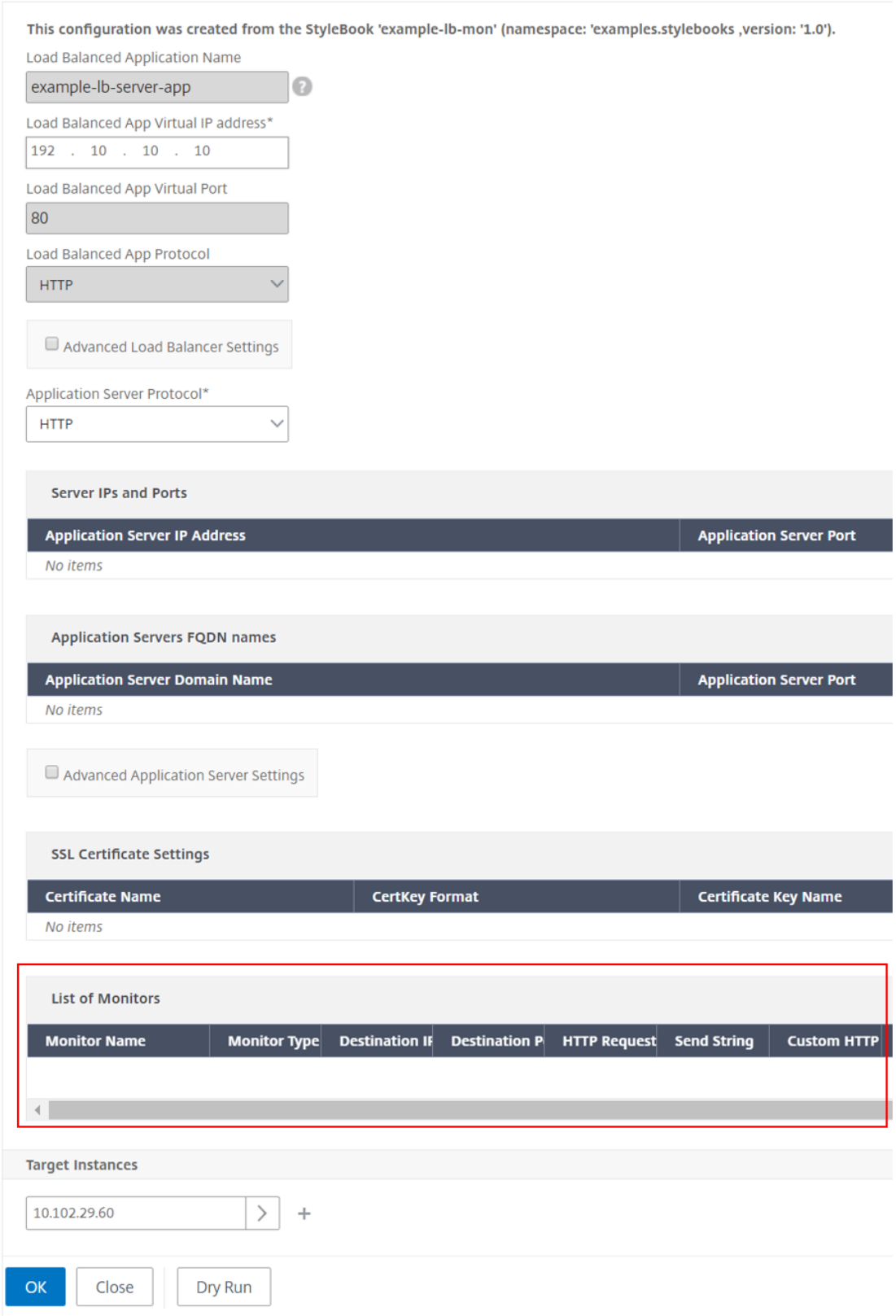


如果在新样书中添加了新的必需参数，则在更改样书之后，必须手动指定此类参数的值。

在此示例中，示 例 **lb** 样书的配置页面上显示的参数如下：



新示 例**-lb-mon** 样书的配置页面上显示的参数如下：



在这种情况下，样书会保留基本负载均衡器配置的旧值，因为新的样书没有更改现有参数。而且，它只添加了新

的参数。对于监视器参数，请手动指定所需的值。

6. 在 目标实例中，查看选定的实例并根据需要更新列表。
7. 单击试运行。

   “对 象”页面显示已创建、修改或从 Citrix ADC 实例中删除的对象。

8. 单击确定。

   在 样书 **>** 配置页面中，样书名称列显示所选配置包的新样书名称。在这种情况下，它会显示示 例-**lb-mon**。

更改具有多个配置包的样书

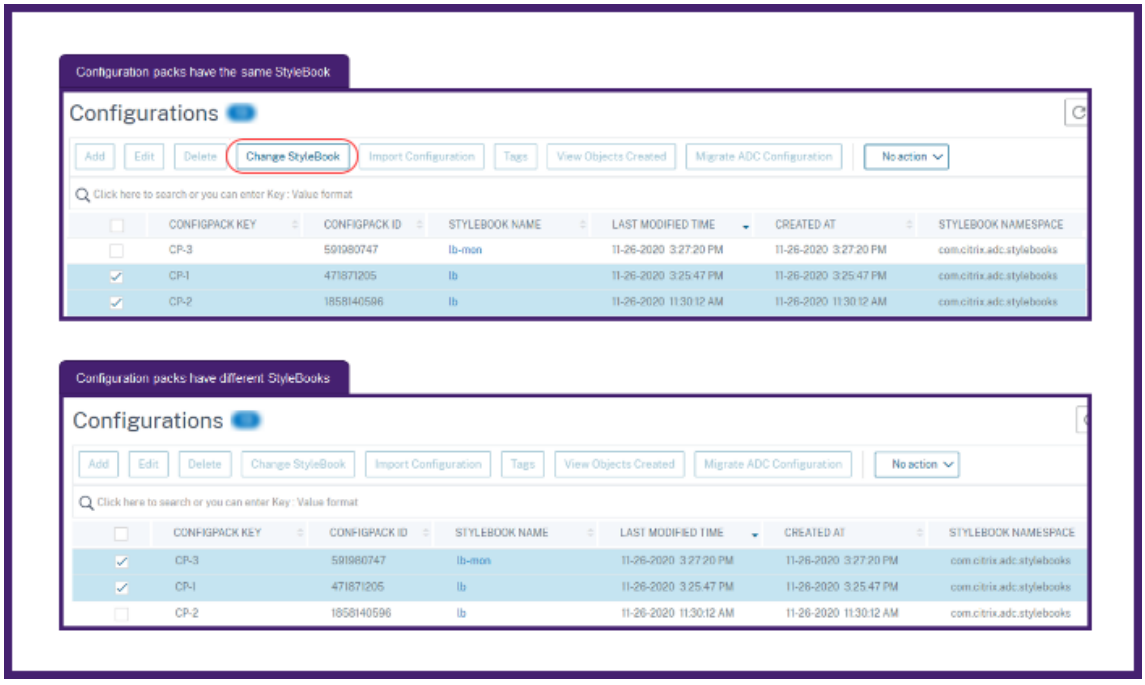
当您更改具有多个配置包的现有样书时，请执行以下操作：

1. 将新的样书导入 ADM。

   通常，新样书的名称和命名空间相同，版本高于现有样书。但是，如果名称、命名空间或版本不同，则可以跳过此步骤。

2. 更改与现有样书关联的配置包的样书。

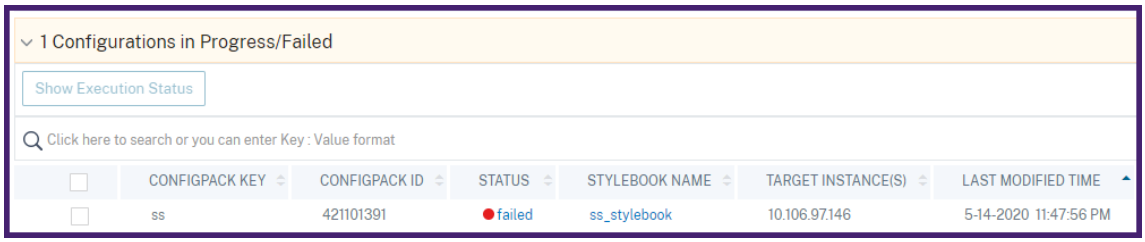
   只有当选定的配置包与同一 样书关联时，才能选择更改样书。



对于选定的配置包，当满足以下条件时，ADM 将成功更改样书：

- 所选样书中必须包含现有样书的所有配置参数。
- 选定样书中的新参数是可选的。

要查看所选配置包的进度，请在“配置”页面 中选择 **“正在进行中/失败的 配置”**。



3. 一旦所有配置包都绑定到新的样书，将旧的样书从 ADM 中删除。

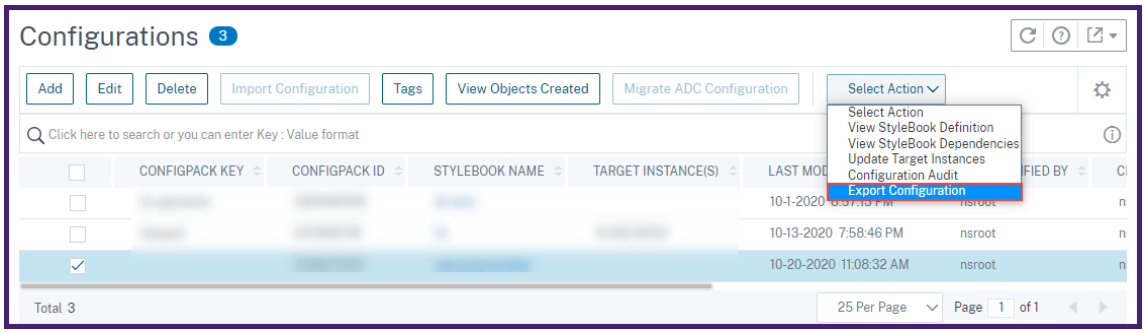
导出或导入配置包

您可以像样书一样导出或导入配置包。使用此功能，您可以随时将样书配置共享到另一台 ADM 服务器。导出配置包时，`tgz` 或 `zip` 捆绑包下载到本地计算机。此捆绑包包含一个 JSON 文件，其中包含配置包中定义的所有参数。

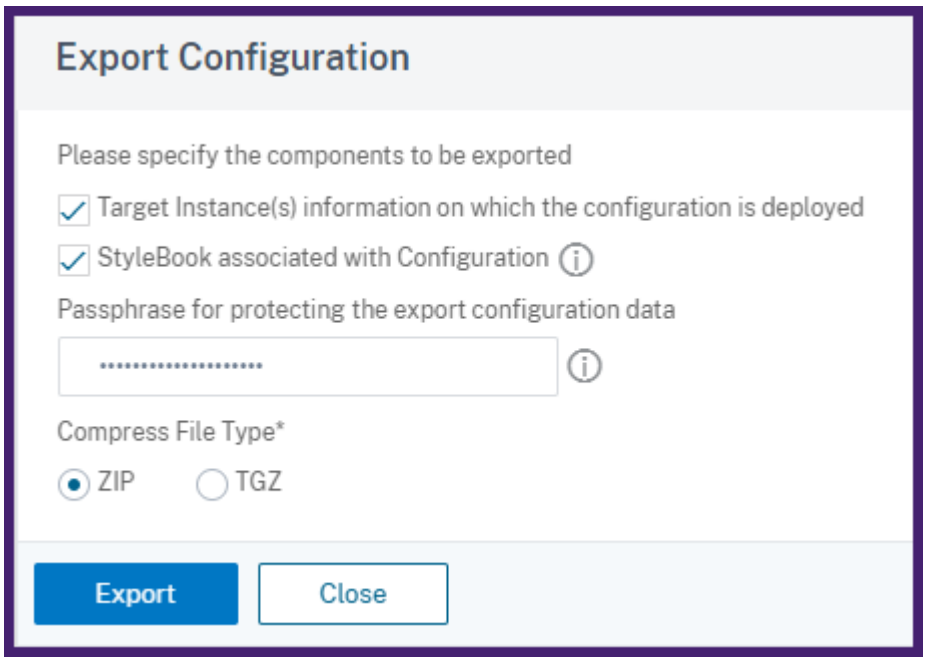
导出配置

执行以下操作以导出配置包：

1. 导航到 应用程序 **>** 样书 **>** 配置。
2. 选择要导出的配置包。
3. 在 选择操作中，选择 导出配置。



4. 在 “ 导出配置” 窗格中，指定以下内容：
   - 部署配置的目标实例信息：选择此选项可在导出捆绑包中包含目标实例的信息。
   - 与配置关联的样书：选择此选项可将样书包含在导出包中。
   - 用于保护导出配置数据的密码：指定用于加密导出包的密码短语。此密码短语可保护配置包的敏感数据。
   - 压缩文件类型：选择 **ZIP** 或 **TGZ** 文件类型。



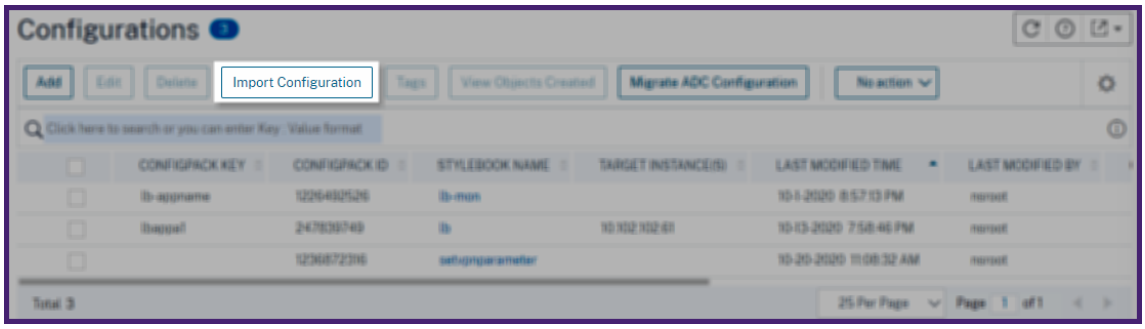
5. 单击导出。

   将导出包保存在本地计算机上。

导入配置

您可以将配置包从本地计算机导入其他 ADM 服务器。要导入配置包，请执行以下操作：

1. 导航到 应用程序 **>** 样书 **>** 配置。
2. 选择 导入配置。



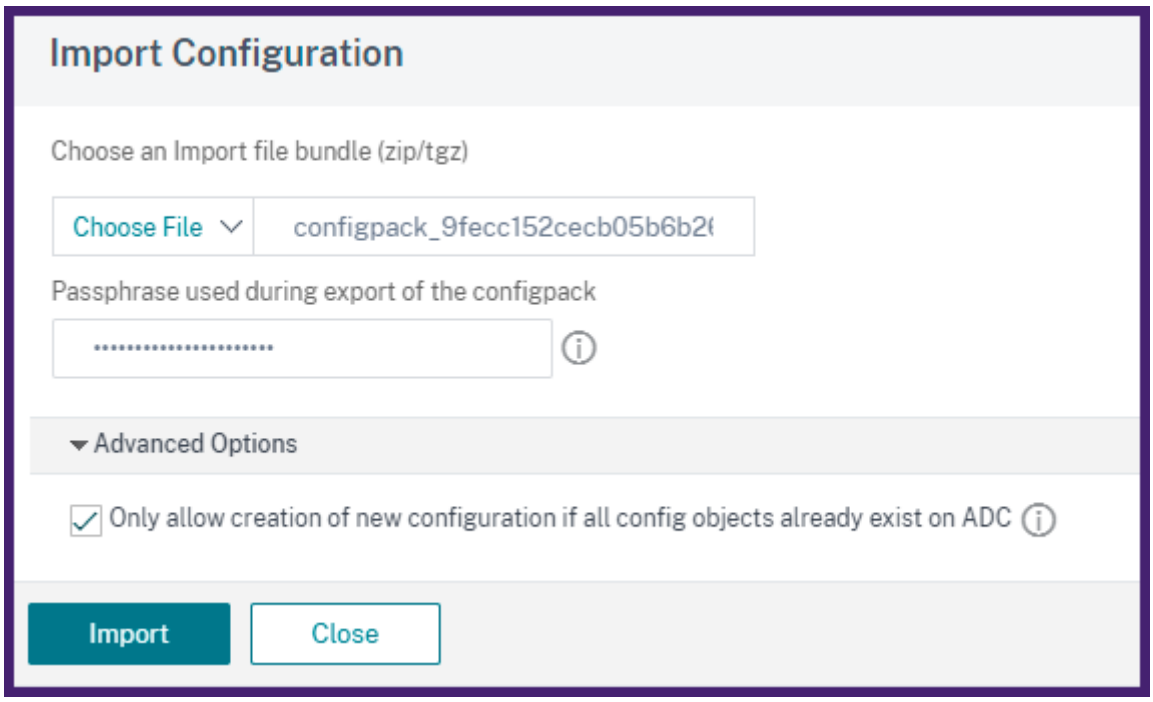
3. 从计算机中选择导入文件包。
4. 使用您在导出期间指定的密码短语。
5. 可选，在“高级选项”中，选择“ 仅允许创建新配置”（如果 **ADC** 上已存在所有配置对象）。

   此选项不会更改已在 ADC 实例上创建的对象。

   考虑您在两台 ADM 服务器中添加了相同的 ADC 实例。而且，您希望将配置包从一台 ADM 服务器迁移到另一台服务器。使用此选项可在不更改 ADC 实例上的配置对象的情况下导入配置包。

> 重要
>
> 信息：要使用此选项，请确保指定的配置捆绑包含目标实例信息。请参阅导出配置。
>
> 只有当目标实例上都存在所有对象时，此选项才迁移配置。

6. 单击导入。



导入配置包时，ADM 将验证以下内容：

- 关联的样书：如果关联的样书不在 ADM 中，它将导入样书和配置包。
- 目标实例：检查目标实例并在指定的目标实例上部署配置。如果 ADM 中没有提到的 ADC 实例，则导入配置包时不包含目标实例。
- 源 **ADM**：如果要在同一台 ADM 服务器上导入配置包，则选定的捆绑包将更新现有的配置包。

构建您的样本

示 例磅样书的完整内容如下供您参考：

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
    application
schema-version: "1.0"
import-stylebooks:
```



```
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

示 例**-lb-mon** 样书的完整内容如下供参考：

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
```



```
    type: cmtypes::monitor[]
substitutions:
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
  -
    name: monitors-comp
    type: cmtypes::monitor
    condition: $parameters.monitors
    repeat: $parameters.monitors
    repeat-item: mon
    repeat-index: ndx
    description: Builds a list of Citrix ADC monitor objects and binds
       them to the servicegroup of this LB config
    properties-default-sources:
      - $mon
    properties:
        monitorname: $substitutions.mon-name($parameters.lb-appname,
           $mon.monitorname)
    components:
      -
        name: monitor-svcg-binding-comp
        condition:  $parameters.svc-servers
        type: ns::servicegroup_lbmonitor_binding
        properties:
          servicegroupname: $components.lb-comp.outputs.servicegroup.
             properties.servicegroupname
          monitor_name: $parent.properties.monitorname
<!--NeedCopy-->
```

创建样本以将文件上传到 **Citrix ADM**

April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 样本允许您通过使用 Citrix ADM GUI 或 API 创建 Citrix ADC 配置，在将任何类型的文件从本地文件系统上传到 Citrix ADC 实例时，这些配置可能包括其他内容。这些文件可

以是示例证书文件或地理定位文件。您还可以指定要上传这些文件的目录。

样本配置

以下是描述如何在 Citrix ADC 实例上上传地理位置文件的示例样本。地理文件通常用于 GSLB 配置中，用于根据地理位置定义静态邻近：

构建您的样书**-1**

```
name: upload-geolocations
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
-
 namespace: netscaler.nitro.config
 version: "11.1"
 prefix: ns

parameters:
-
 name: locationfile
 label: Location File
 description: The system file path of the geolocation file on Citrix
    ADM
 type: file
 required: true

components:
-
 name: upload-file-comp
 type: ns::systemfile
 properties:
    filename: $parameters.locationfile.filename
    filelocation: "/var/netscaler/inbuilt_db/"
    filecontent: base64.encode($parameters.locationfile.contents)
<!--NeedCopy-->
```


> ** 注
>
> 意 ** 此示例中使用的参数是类型文件。您可以在 Citrix ADM 中导入此样本并使用它上传地理定位文件。

此样本要求该文件已经存在于 Citrix ADM 中（例如，您已经使用 scp 等实用程序将其复制到 Citrix ADM）。

如果要通过 Citrix ADM 将文件上传到 Citrix ADC 而不首先将其复制到 Citrix ADM 文件系统，则可以构建一个样本，其中包含两个“字符串”参数，一个用于指定要在 Citrix ADC 上使用的文件名，另一个用于指定文件，然后在上传文件组件中使用这两个参数。以下是用于上传地理位置文件的备用样本：

构建您的样本**-2**

```
name: upload-geolocations-alt
namespace: com.citrix.adc.stylebooks.samples
version: "1.0"
display-name: GeoLocation File Upload
description: This StyleBook is used to upload a geolocation file to
   Citrix ADC
schema-version: "1.0"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  version: "11.1"
  prefix: ns

parameters:
 -
  name: filename
  label: Location Filename
  description: The name of the location file on the Citrix ADC
  type: string
  required: true
 -
  name: filecontents
  label: Location File Contents
  description: The contents of the location file
  type: string
  required: true

components:
 -
  name: upload-file-comp
  type: ns::systemfile
  properties:
```



```
    filename: $parameters.filename
    filelocation: "/var/Citrix ADC/inbuilt_db/"
    filecontent: base64.encode($parameters.filecontents)
<!--NeedCopy-->
```

创建配置以上传文件

以下过程在选定的 Citrix ADC 实例上创建配置，该配置将使用上述第一个样本上传地理定位文件。

要创建上载文件的配置，请执行以下操作：

1. 在 Citrix ADM 中，导航到 应用程序 > 配置”，然后单击 创建新。“选择样本” 页面显示 Citrix ADM 中可用的所有样本。向下滚动并选择您导入的样本。

   样本参数显示为用户界面页面，允许您输入此样本中定义的所有参数的值。

2. 在基本负载平衡器设置部分输入负载平衡器的名称和虚拟 IP 地址。
3. 在 “ 位置文件” 部分中，输入文件的名称或位置。

   > 注意：
   >
   > 确保在 Citrix ADM 中，文件仅位于当前租户的文件夹下。使用任何文件传输协议将文件复制到 Citrix ADM 文件系统。

4. 在访问目标实例之前，可能会要求您提供用户凭据。
5. 选择需要在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。

> 注意：
>
> Citrix 建议您选择干运行以检查在目标实例上创建的配置对象，然后再对实例执行实际配置。

成功创建配置包后，该文件将保存在 Citrix ADC 实例文件系统中的位置：/var/netscaler/inbuilt_db/

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。

使用 **Citrix ADM API** 创建配置包

您还可以使用 Citrix ADM API 创建将文件上传到所选 Citrix ADC 实例的配置包。有关如何使用 API 的更多信息，请参阅如何使用 API 创建配置以上载任何文件类型。

创建样本以将 **SSL** 证书和证书密钥文件上传到 **Citrix ADM**

April 23, 2021

创建使用 SSL 协议的样本配置时，必须上载样本参数所需的 SSL 证书文件和证书密钥文件。样书允许您使用 Citrix ADM GUI 直接从本地系统上传 SSL 文件和密钥文件。您还可以使用 Citrix ADM API 上载已由 Citrix ADM 管理的证书文件和密钥文件。

样本配置

本文档帮助您创建自己的样本- 负载平衡虚拟服务器 **(SSL)**，其中包含
用于上传 SSL 证书和密钥文件的组件。此处作为示例提供的样本在所选 Citrix ADC 实例上创建基本的负载平衡虚拟服务器配置。该配置使用 SSL 协议。要使用此样本创建配置，您必须提供虚拟服务器的名称和 IP 地址，选择负载平衡方法参数，然后上传虚拟服务器的证书文件和证书密钥文件，或者使用已经存在的证书文件和证书密钥文件存在于 Citrix ADM 中。这些内容在 parameters 部分中指定，如下所示：

```
parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
  description: "The file name of the SSL certificate file"
  type: certfile
 -
  name: key
  label: "SSL Certificate Key File"
  description: "The file name of the server certificate's private key
     file"
  type: keyfile
<!--NeedCopy-->
```

然后在样本的 components 部分中创建两个组件，如下所示。my-lbvserver-comp 组件的类型为 ns::lbvserver，其中：

- “ns” 是指代在 import-stylebooks 部分中指定的内置命名空间 netscaler.nitro.config 和版本 10.5 的前缀。
- lbvserver 是此命名空间中的内置样本。它对应于同名的 Citrix ADC NITRO 负载平衡虚拟服务器资源。

第二个组件 “lbvser-证书-复合” 类型为 stlb vser-证书-绑定。前缀 “stlb” 指代在样本的 import-stylebooks 部分中指定的命名空间 com.citrix.adc.stylebooks 和版本 1.0。如果 com.citrix.adc.stylebooks 命名空间可以视为文件夹，则 vserver-certs-binds 是该文件夹中的另一个样本（或文件）。位于命名空间 “com.citrix.adc. 样本” 中的样本将作为 Citrix ADM 的一部分发送。

用户定义样本使用的 “v 服务器 cers-binds” 样本允许您通过将证书和密钥文件上传到目标 Citrix ADC 实例，并配置证书和密钥文件绑定到相应的虚拟服务器，轻松配置证书。此组件的属性是-lb 虚拟服务器的名称以及创建配置包时提供的 SSL 证书的名称。

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  properties:
   name: $parameters.name
   servicetype: SSL
   ipv46: $parameters.ip
   port: 443
   lbmethod: $parameters.lb-alg
 -
  name: lbvserver-certificate-comp
  type: stlb::vserver-certs-binds
  description: Binds lbvserver with server certificate
  properties:
   vserver-name: $components.my-lbvserver-comp.properties.name
   certificates:
    -
     cert-name: $parameters.name + "-lb-cert"
     cert-file: $parameters.certificate
     ssl-inform: PEM
     key-name: $parameters.name + "-key"
     key-file: $parameters.key
<!--NeedCopy-->
```

使用 API 基于此类样本创建配置时，只使用文件名（而不是完整文件路径）。这些文件预计已在 Citrix ADM 上的证书和密钥文件夹中可用。上载的 SSL 证书文件和 SSL 证书密钥文件分别存储在 Citrix ADM 中的目录 /var/mps/tenants/…/ns_ssl_certs 和 /var/mps/tenants/…/ns_ssl_keys 中。

创建配置以上传 **SSL** 文件

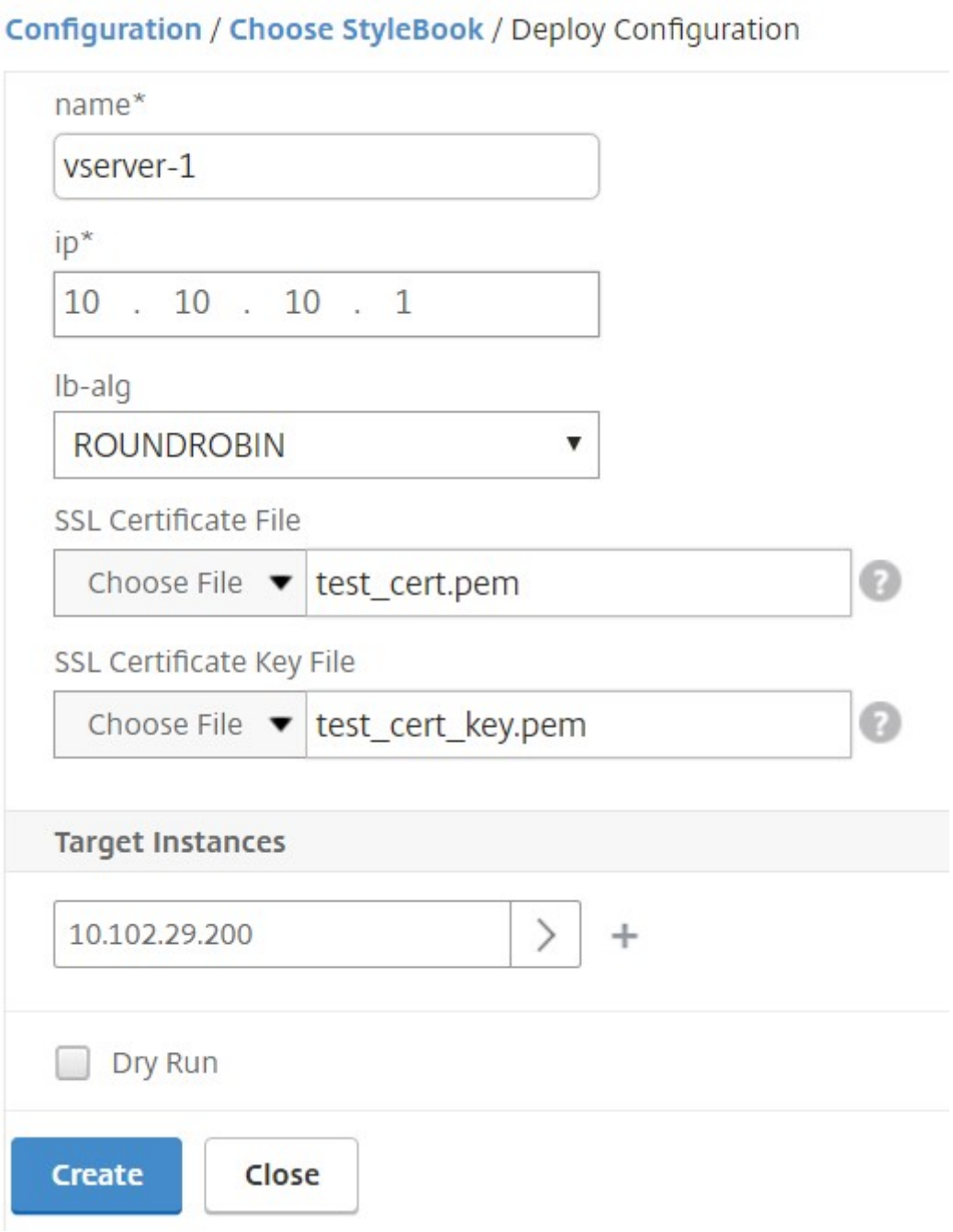
以下过程使用上述指定的样本中的 SSL 协议在所选 Citrix ADC 实例上创建基本负载平衡虚拟服务器配置。您可以使用此过程在 Citrix ADM 中上载 SSL 证书文件和证书密钥文件。

创建配置用于上载文件

1. 在 Citrix ADM 中，导航到 应用程序 > 配置**” > “**样本。“ 样书” 页面显示 Citrix ADM 中可用的所有样书。
2. 向下滚动并选择 负载平衡虚拟服务器 **(SSL)** 或在搜索字段中键入负载平衡虚拟服务器 **(SSL)** ，然后按 **Enter** 键。
3. 单击样本面板中的 创建配置链接。

   样本参数显示为用户界面页面，允许您输入此样本中定义的所有参数的值。
4. 在基本负载平衡器设置部分输入负载平衡器的名称和虚拟 IP 地址。
5. 在 **SSL** 证书设置部分，从本地存储文件夹中选择相应的文件。或者，您也可以选择 Citrix ADM 本身上存在的文件。
6. 选择需要在其上创建配置的目标 Citrix ADC 实例，然后单击 创建”。

> 注意
>
> 您还可以单击刷新图标，将 Citrix ADM 中最近发现的 Citrix ADC 实例添加到此窗口中的可用实例列表中。



注意

在 Citrix ADM 中，以下默认样本（作为 Citrix ADM 的一部分发送）使您能够通过上传 SSL 证书和密钥来创建 SSL 支持。

- HTTP/SSL 负载平衡样本 (lb)
- HTTP/SSL 负载平衡（具有监视器）样本 (lb-mon)
- HTTP/SSL 内容交换应用程序（具有监视器）(cs-lb-mon)

> • 使用 CS、LB 和 SSL 功能的示例应用程序样本 (sample-cs-app)
>
> 您还可以创建自己的样本，以上面的样本中所述的同一方式利用 SSL 证书

构建您的样本

lb-vserver-ssl.yaml 文件的完整内容如下所示：

```
name: lb-vserver-ssl
description: "This stylebook defines a load balancing virtual server
   configuration."
display-name: "Load Balancing Virtual Server (SSL)"
namespace: com.example.ssl.stylebooks
schema-version: "1.0"
version: "0.1"

import-stylebooks:
 -
  namespace: netscaler.nitro.config
  prefix: ns
  version: "10.5"
 -
  namespace: com.citrix.adc.stylebooks
  prefix: stlb
  version: "1.0"

parameters:
 -
  name: name
  type: string
  required: true
 -
  name: ip
  type: ipaddress
  required: true
 -
  name: lb-alg
  type: string
  allowed-values:
    - ROUNDROBIN
    - LEASTCONNECTION
  default: ROUNDROBIN
 -
  name: certificate
  label: "SSL Certificate File"
```



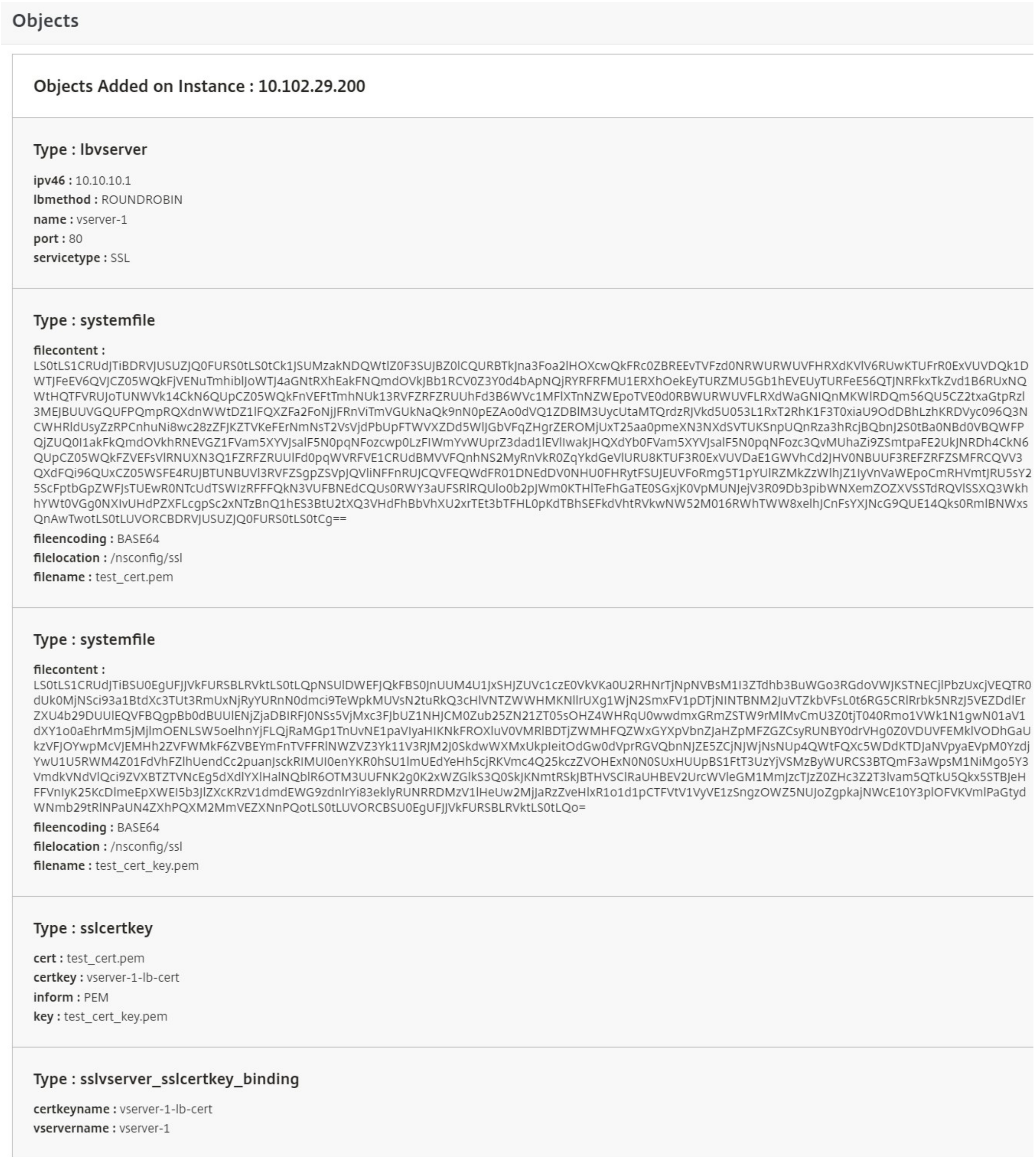
```
37    description: "The file name of the SSL certificate file"
38    type: certfile
39   -
40    name: key
41    label: "SSL Certificate Key File"
42    description: "The file name of the server certificate's private key
          file"
43    type: keyfile
44
45  components:
46   -
47    name: my-lbvserver-comp
48    type: ns::lbvserver
49    properties:
50      name: $parameters.name
51      servicetype: SSL
52      ipv46: $parameters.ip
53      port: 443
54      lbmethod: $parameters.lb-alg
55   -
56    name: lbvserver-certificate-comp
57    type: stlb::vserver-certs-binds
58    description: Binds lbvserver with server certificate
59    properties:
60     vserver-name: $ components.my-lbvserver-comp.properties.name
61     certificates:
62      -
63       cert-name: $parameters.name + "-lb-cert"
64       cert-file: $parameters.certificate
65       ssl-inform: PEM
66       key-name: $parameters.name + "-key"
67       key-file: $parameters.key
68  <!--NeedCopy-->
```

使用 **Citrix ADM API** 创建配置包

您还可以使用 Citrix ADM API 创建将证书和密钥文件上传到所选 Citrix ADC 实例的配置包。有关如何使用 API 的详细信息，请参阅如何使用 API 创建配置以上传证书和密钥文件。

查看在 **Citrix ADC** 实例上定义的对象

在 Citrix ADM 上创建样书配置包后，单击 查看创建的对象以显示在目标 Citrix ADC 实例上创建的所有 Citrix ADC 对象



在样本中定义的虚拟服务器上启用分析并配置警报

April 23, 2021

您可以使用操作构造配置 Citrix ADM 分析，以收集由作为样书一部分的任何虚拟服务器组件处理的所有或部分流量事务的应用程序流记录。还可以使用此构造来配置警报，以深入了解虚拟服务器管理的流量。

以下示例显示了样本的 operations 部分：

```
operations:
  analytics:
   -
    name: lbvserver-ops
    properties:
    target: $components.basic-lb-comp.outputs.lbvserver
    filter: HTTP.REQ.URL.CONTAINS("catalog")
   -
    alarms:
     -
      name: lbvserver-alarm
      properties:
      target: $outputs.lbvserver
      email-profile: $parameters.emailprofile
      sms-profile: "NetScalerSMS"

    rules:
     -
      metric: "total_requests"
      operator: "greaterthan"
      value: 25
      period-unit: $parameters.period
     -
       metric: "total_bytes"
       operator: "lessthan"
       value: 60
       period-unit: "day"
<!--NeedCopy-->
```

分析部分中的属性用于指示 Citrix ADM 分析功能在由目标属性标识的虚拟服务器组件上收集应用程序流记录。您还可以选择指定一个过滤器属性，该过滤器属性接受 Citrix ADC 策略表达式，以筛选在虚拟服务器上收集应用程序流记录的请求。

从此样书创建配置包时，Citrix ADM Analytics 功能将配置为收集在创建配置包过程中创建虚拟服务器时指定的 appflow 记录。

alarms 部分的属性用于设置阈值，以在由目标属性标识的虚拟服务器上生成警报并发送通知。在上述示例中，email-profile 属性和 sms-profile 属性用于指定应向哪里发送通知。rules 部分定义阈值。例如，如果虚拟服务器处理的请求总数超过 25 并在用户定义的期间，即设置警报并发送通知。“period-unit” 指定触发警报的频率。它可以采取日、小时或每周的值。

可以在比较指标值与阈值时使用以下运算符：

- “greaterthan” 表示 “>”

- “lessthan” 表示 “<”
- “greaterthanequal” 表示 “>=”
- “lessthanequal” 表示 “<=”

请注意，样本使用 API 名称作为指标，而不是 Citrix ADM 分析 GUI 上显示的名称。

要了解如何查看和分析在虚拟服务器上收集的数据，这些数据是作为配置包的一部分创建的，请参阅 Citrix ADM Analytics 文档。

实例角色

April 23, 2021

在 Citrix Application Delivery Management (ADM) 中，可能存在一种情况：您必须为单个应用程序配置多个 Citrix ADC 实例，但每个 ADC 实例需要在其上部署不同的配置。这种情况下的一个示例是默认的 Microsoft Skype for Business 样本。

样书目前支持创建配置包并在多个 Citrix ADC 实例上应用相同配置的功能。在所有 ADC 实例上配置相同的情况下，可以称为对称配置。

现在，借助 StyleBooks 的 “实例角色” 功能，您可以创建不对称配置，即可应用于多个 ADC 实例的配置包，但在不同的 ADC 实例上使用不同的配置。

当使用带实例角色的样书功能创建配置包时，可以为配置包中的每个 ADC 实例分配不同的角色。此角色决定 ADC 实例将接收的配置包的配置对象。

注意事项：

- 样本中的一组实例角色是在创建样本时定义的。
- 创建或更新配置包时，角色会分配给特定 ADC 实例。

目标角色部分

在样书中引入了一个名为 “目标角色” 的新部分，其中声明了样书支持的所有角色。

此部分通常放在样书的 “导入样书” 部分之后和参数部分之前。

在以下样书示例中，在 “目标角色” 部分中定义了两个角色-A 和 B。

```
target-roles:

  -
   name: A
   name: B
     min-targets: 2
     max-targets: 5
```



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

您可以看到角色 B 还定义了两个可选子属性，即最小目标和最大目标。

尽管这两个子属性是可选的，但最小目标指定在使用此样书创建配置包时应分配此角色的 ADC 实例的最小强制数量，而 max-target 则指定创建时可分配此角色的 ADC 实例的最大数量来自此样书的配置包。

如果未指定这些子属性，则可以为该角色配置的 ADC 实例数量没有限制。如果最小目标 = 0，则与该角色关联的配置是可选的，如果最小目标 = 1，则该配置是必需的，并且至少需要为该角色配置一个 ADC 实例。

角色“默认”

除了明确定义的角色之外，还有一个所有样本都具有的隐式角色，并且该角色被称为默认角色。此角色可以像样本中的任何其他角色一样使用。创建配置包时，如果没有为 ADC 实例分配特定角色，则该实例将隐式分配给“默认”角色。实例现在将接收由具有“默认”角色的组件生成的任何配置对象。

具有角色的组件

定义样书可以支持的角色（包括角色“默认”）后，可以在样书的组件部分中使用这些角色。如果希望仅在发挥特定角色的 ADC 实例上部署组件，则可以将角色属性指定为组件的一部分，如以下组件示例所示：

```
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
<!--NeedCopy-->
```

在上面的示例中，组件生成一个“lbvserver”，该“lbvserver”将在扮演角色 A 的实例上部署。请注意，组件的角色属性是一个列表，可以为组件分配多个角色。这些角色将在样书的“目标角色”部分中声明。

注意：如果样书中的某个组件未指定角色属性，则无论其角色如何，都会在所有 Citrix ADC 实例上创建由该组件生成的配置对象。您可以有效地使用此功能创建可应用于配置包的所有实例的配置对象。

让我们假设有一个定义了两个角色的样书-A 和 B，其中包含四个组件。

- 组件 C1 具有角色 A 和 B
- 组件 C2 具有作用 B
- 组件 C3 没有定义任何角色
- 组件 C4 具有“默认”的角色

本样本的组成部分转载如下：

```
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
<!--NeedCopy-->
```

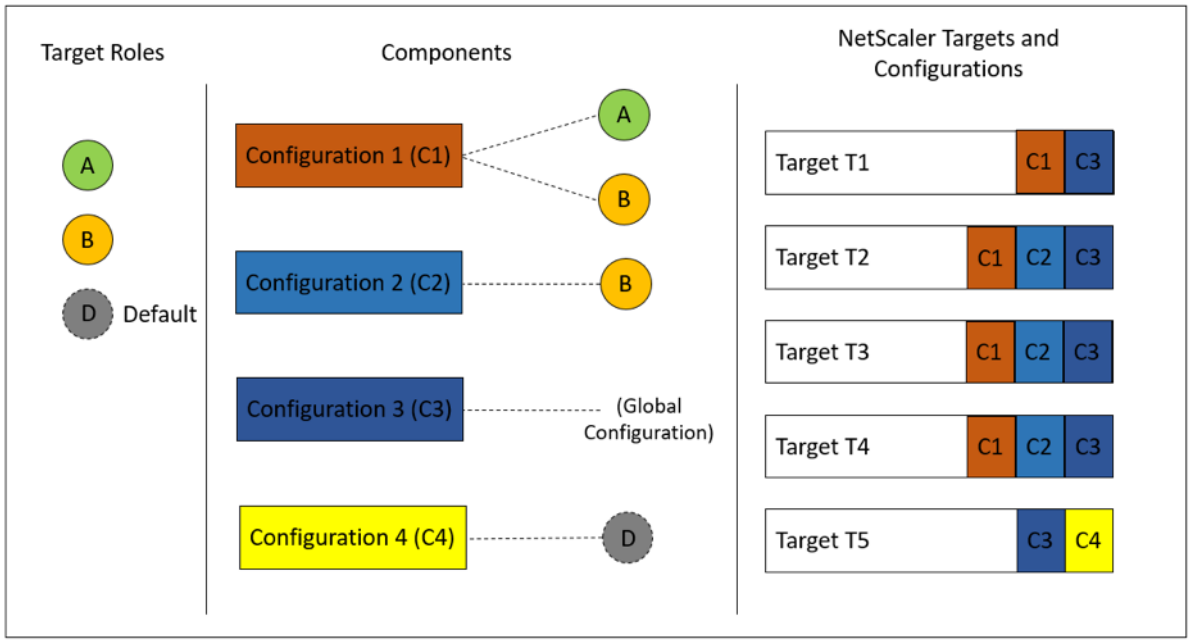
请注意，组件 C3 没有定义角色，这意味着组件将部署在所有实例上，无论其角色如何。另一方面，组件 C4 具有“默

认”角色，这意味着它应用于没有分配明确角色的任何实例。

现在，考虑您想使用此样书创建一个配置包，然后将其部署在五个 ADC 实例上。在此阶段，您可以通过以下方式将角色分配给实例：

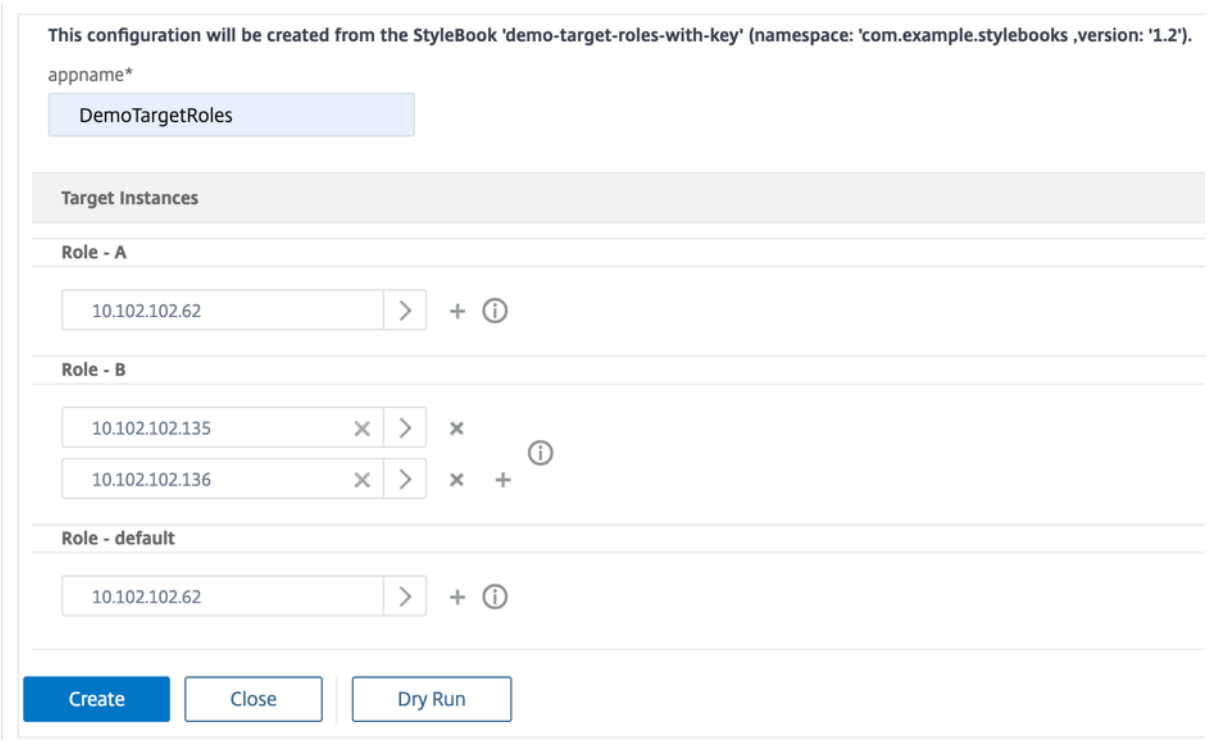
- 角色 A 分配给实例 T1、T2、T3 和 T4
- 角色 B 分配给实例 T2、T3 和 T4
- 实例 T5 未分配任何角色

下图总结了角色分配，并显示了每个 ADC 实例将收到的结果配置：



请注意，组件 C3 部署在所有实例上，而不考虑角色如何，因为此组件没有角色属性。

下图显示了创建示例配置包时角色的分配：



在创建配置包时，您还可以使用 “Dry Run” 功能来查看和验证角色分配的正确性以及将在每个 ADC 实例上创建的配置对象。

构建您的样本

样本 “演示目标角色” 的全部内容如下：

```
---
name: demo-target-roles
namespace: com.example.stylebooks
version: "1.2"
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
parameters:
  -
    name: appname
    type: string
    required: true
    key: true
target-roles:
  -
```

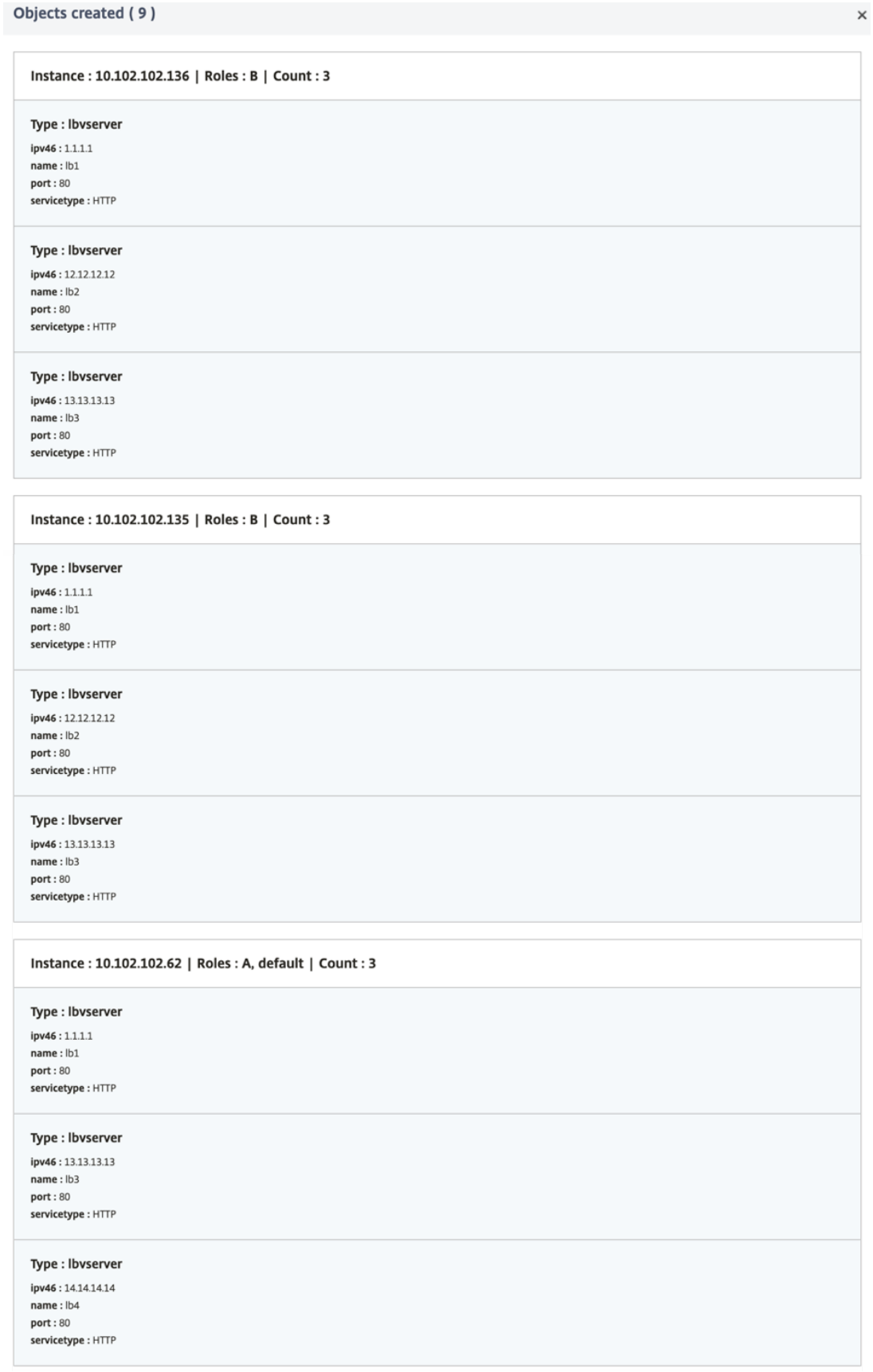


```
    name: A
  -
    name: B
    min-targets: 2
    max-targets: 5
components:
  -
    name: C1
    type: ns::lbvserver
    roles:
      - A
      - B
    properties:
      name: lb1
      servicetype: HTTP
      ipv46: 1.1.1.1
      port: 80
  -
    name: C2
    type: ns::lbvserver
    roles:
      - B
    properties:
      name: lb2
      servicetype: HTTP
      ipv46: 12.12.12.12
      port: 80
  -
    name: C3
    type: ns::lbvserver
    properties:
      name: lb3
      servicetype: HTTP
      ipv46: 13.13.13.13
      port: 80
  -
    name: C4
    type: ns::lbvserver
    roles:
      - default
    properties:
      name: lb4
      servicetype: HTTP
      ipv46: 14.14.14.14
      port: 80
```



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

下图显示了为示例配置包创建的对象：



使用 **API**

使用 REST API 时，您可以在创建或更新配置包时为每个 ADC 实例指定角色，如下所示。在“目标”块中，指定要在其上部署单个组件的特定 Citrix ADC 实例的 UUID。

```
"targets": [
            {

             "id": "<ADC-UUID>",
             "roles": ["A"]
             }
 ,
           ]
<!--NeedCopy-->
```

我们提供了一个完整的示例 REST API 供您参考。

POST /<ADM-IP>/stylebook/nitro/v1/config/stylebooks/com.example.stylebooks/1.2/demo-target-roles/configpacks

```
{

  "configpack": {

     "parameters": {

     "appname": "app1"
     }
 ,
     "targets": [
        {

          "id": "f53c35c3-a6bc-4619-b4b4-ad7ab6a94ddb",
        "roles": ["A"]
         }
 ,
        {

          "id": "c08caa1c-1011-48aa-b8c7-9aed1cd38ed0",
          "roles": ["A", "B"]
         }
 ,
        {

          "id": "88ac90cb-a5cb-445b-8617-f83d0ef6174e",
          "roles": ["A", "B"]
```



```
          }
  ,
         {

           "id": "bf7b0f74-7a83-4856-86f4-dcc951d3141e",
           "roles": ["A", "B"]
          }
  ,
         {

           "id": "fa5d97ab-ca29-4adf-b451-06e7a234e3da",
           "roles": ["default"]
          }

       ]
      }

  }

<!--NeedCopy-->
```

创建样书以执行非 **CRUD** 操作

April 23, 2021

样本通过计算 Citrix ADC 实例上的必要配置对象来管理 Citrix ADC 配置。每次创建或更新 ConfigPack 时，都会从实例中添加、更新或删除这些对象。这是当您指定 “所需的状态” 时的情况。

但是，某些 Citrix ADC 配置对象支持创建、更新或删除（CRUD 操作）以外的其他一些操作。例如，负载平衡器对象 (lbvserver) 或 Citrix ADC 功能对象 (ns 功能) 可以支持 “启用” 或 “禁用” 操作。同样，Citrix ADC 证书密钥支持 “链接” 和 “取消链接” 操作，以将证书链接到另一个证书或取消链接。对 Citrix ADC 对象的这些操作称为非 CRUD 操作。本节介绍如何使用样本对支持它们的配置对象执行非 CRUD 操作。

> 注意
>
> 配置对象之间的绑定（例如，将证书键绑定到 lbvserver）不被视为非 CRUD 操作。这是因为 Nitro 绑定本身就表示为配置对象。创建和删除这些对象与任何其他 Citrix ADC 配置对象一样。

支持非 **CRUD** 操作

在组件中添加一个名为 “元属性” 的新构造，其级别与 “属性” 构造相同。此结构当前支持的唯一属性称为 “action” 此属性可以采用该配置对象支持的 “启用” 或 “禁用” 等值。


```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
  meta-properties
   action: enable
  properties:
    name: $parameters.name
    servicetype: HTTP
    ipv46: $parameters.ip
    port: 80
    lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

在上面的例子中，“my-lbvser-comp” 组件类型为 “ns⊠ lbvserver。“ “ns” 是指在导入样式书部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀。“lbvserver” 是此命名空间中的 NITRO 资源。作为隐式操作，lbvserver 首先由样本创建；然后对其执行 “启用” 操作。

元属性中指定的操作仅在创建 ConfigPack 期间对配置对象执行。对配置包的更新不执行非 CRUD 操作。

> ** 注
>
> 意 ** 操作属性的值不能是动态评估的样本表达式。

将样书的配置包迁移到另一个样书

April 23, 2021

在 Citrix Application Delivery Management (ADM) 中，配置包始终绑定到从中创建配置包的样书。对配置包的任何更新只能通过配置包绑定到的样书来完成。Citrix ADM 现在允许您将现有配置包迁移到新的样书。新的样书可以是绑定到配置包的当前样书的更原始版本。或者，您也可以将配置包迁移到完全不同的样书中。

例如，您创建了一个名为 **exam-lb** 的样本。此样本用于在 Citrix ADC 实例上部署基本负载平衡器配置。您在 Citrix ADC 实例上通过此样书创建了配置包 CP1。稍后，您意识到样本不包含监视配置。因此，您现在创建了一个名为 例子 **lb-mon** 的样本。此样本具有与 exam-lb 样本相同的负载平衡器配置，但增加了配置监视器的功能。

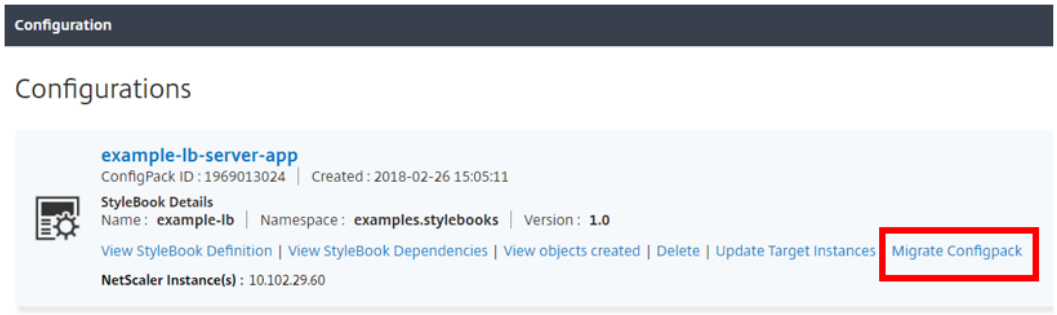
现在，您想更新在配置包 CP1 中创建的现有配置以添加一些监视器。以前，您必须删除配置包 CP1，然后从新的样书中创建配置包 CP2 才能将监视器添加到配置中。删除 CP1 会导致删除在一个或多个 Citrix ADC 实例上的配置包 CP1 中创建的所有配置。之前，您必须通过为所有参数键入值，通过新的样书重新创建新的配置包。

相反，您现在可以将现有配置包 CP1 迁移到新的示例-lb-mon 样书。您的新样本可以配置显示器监视器的详细信息。只有那些与监视器相关的配置对象才会添加到部署配置包的 Citrix ADC 实例中。您现在只需提供显示器的详细信息。在未更改的 Citrix ADC 实例上部署的现有配置不受影响。

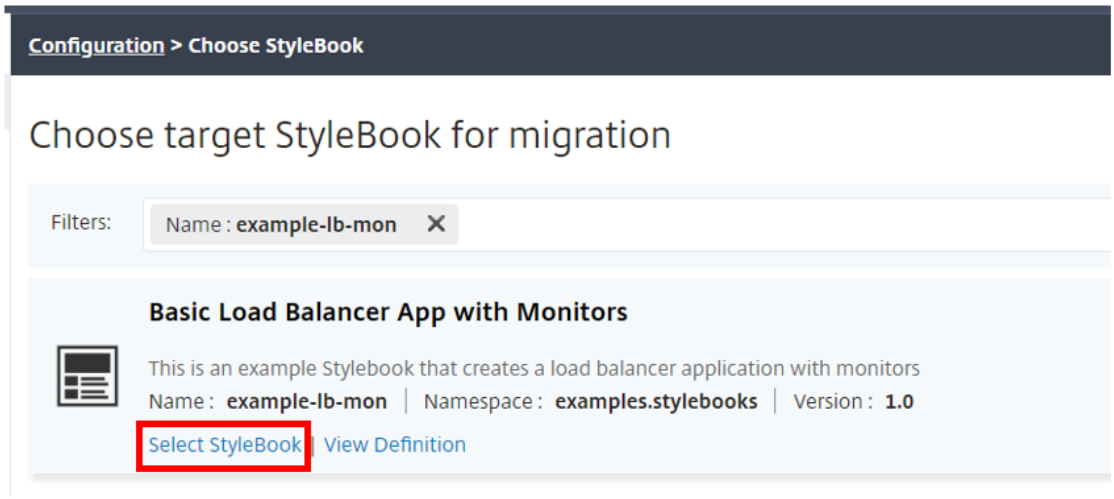
迁移配置包

将使用 **example-lb** 样书创建的配置包迁移到示例**-lb-mon** 样书

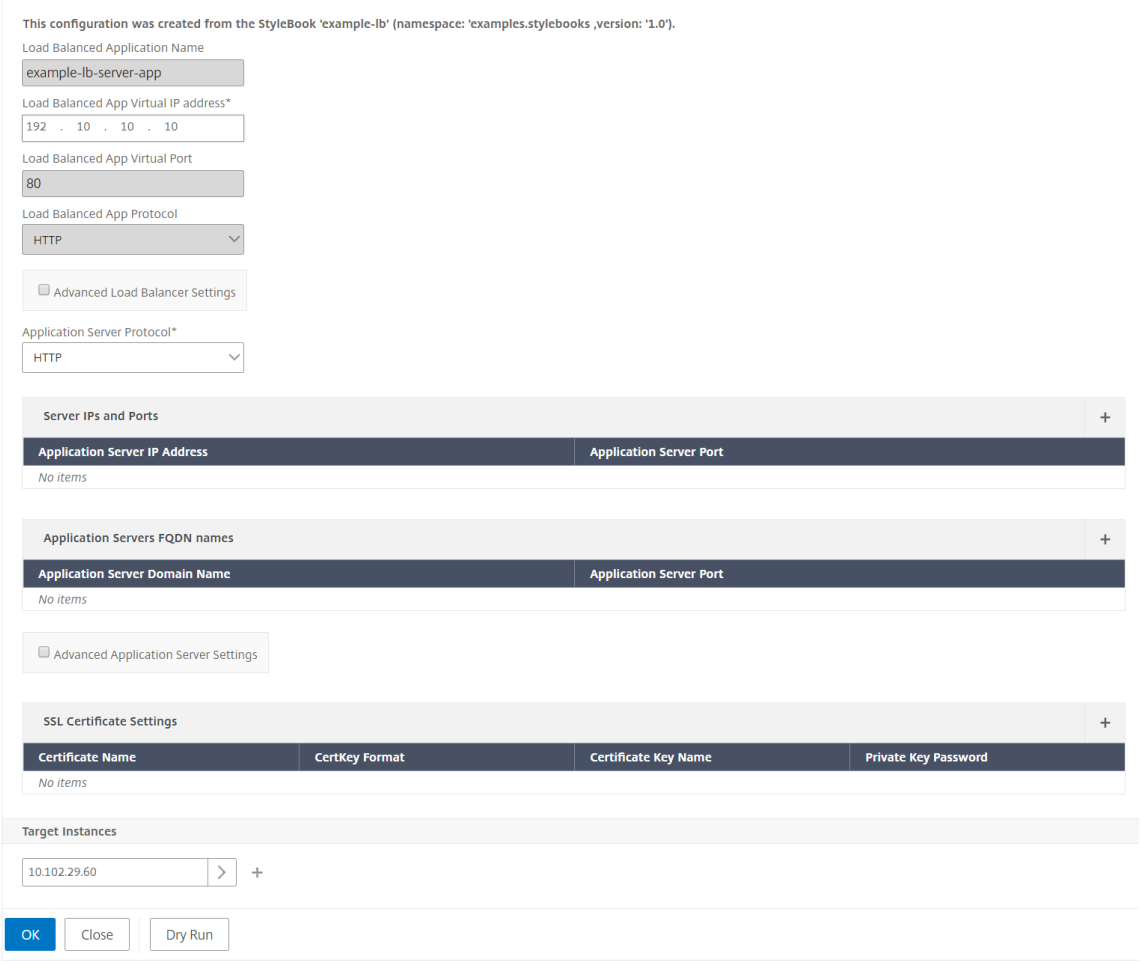
1. 在 Citrix ADM 中，导航到 应用程序 > 配置。“ 配置”页面显示系统中存在的所有配置包。
2. 向下滚动以 查找先前创建的示例磅配置包，然后单击 迁移 **Configpack**。



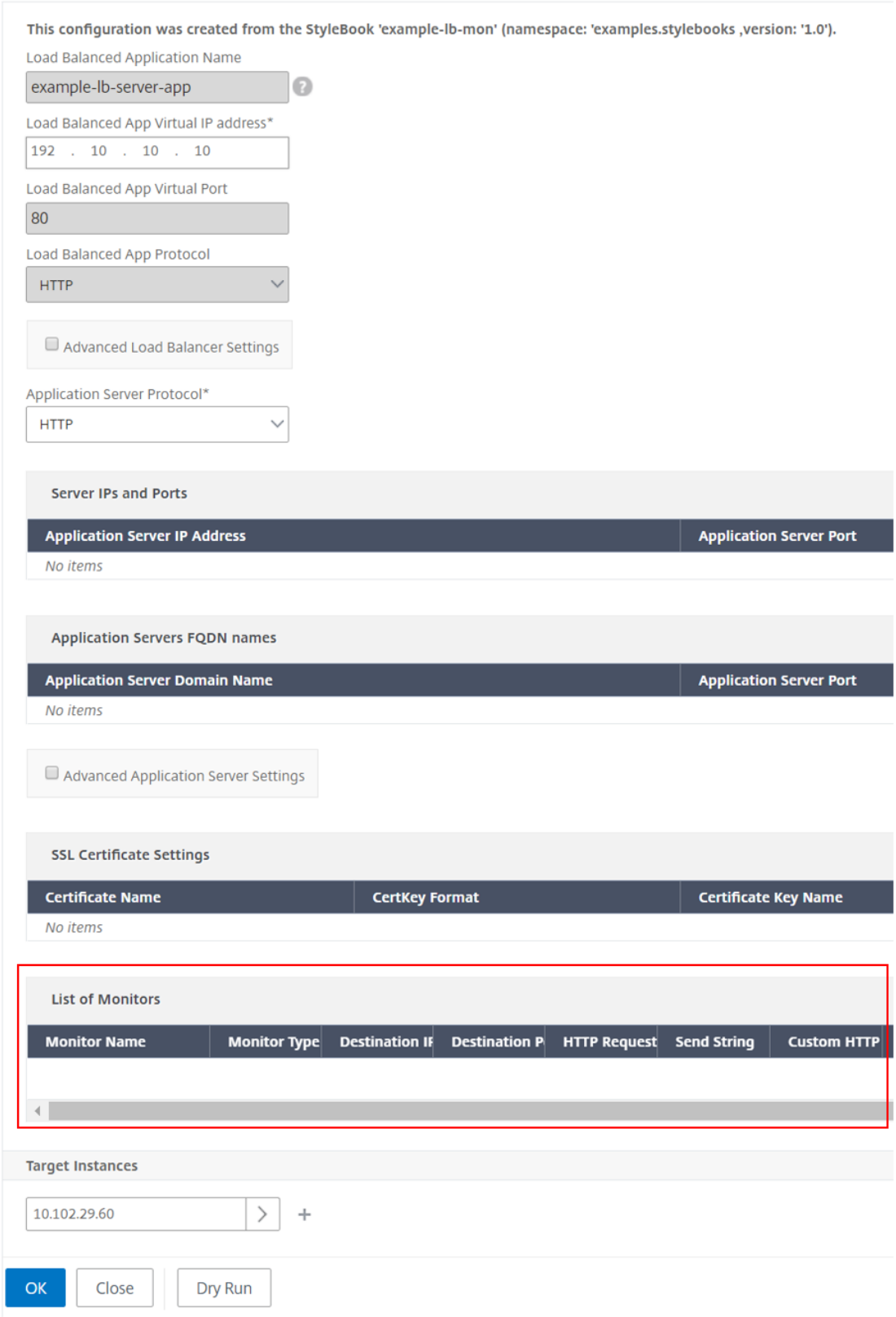
3. “ 选择要迁移的目标样本页面将打开，其中列出 Citrix ADM 中可用的所有样本。向下滚动以 查找示例 **Lb-mon** 样本，然后单击 选择样本。您也可以通过键入示例 lb-mon 来搜索样本。



如果从一个样本迁移到另一个样本，则两个样本中的所有参数可能不具有相同的结构。如果参数结构相似，则前面的值将自动保留在参数字段中。新样本中的一些参数可能是新的，或者它们的结构可能发生变化。在这种情况下，您必须手动填写样本参数的值。例如，下图显示了示例 lb 样本的参数。



下图显示了将配置包迁移到 example-lb-mon 样书后的参数。



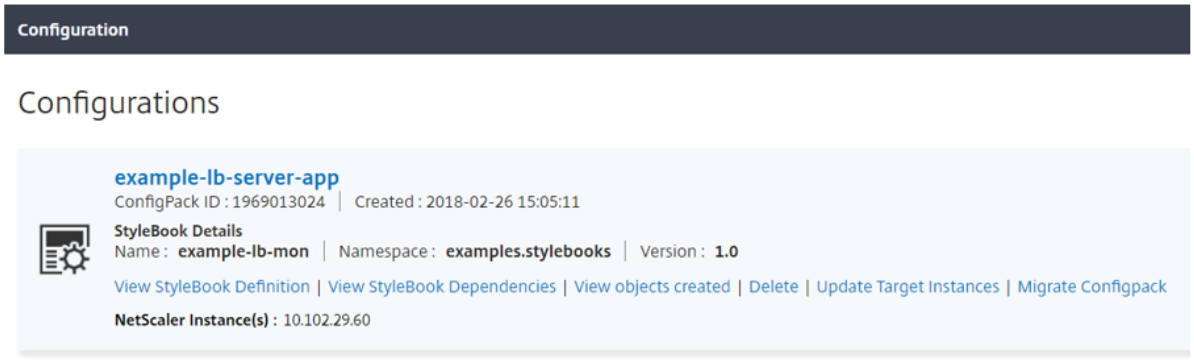
在这种情况下，您可以看到样本保留了基本负载平衡器配置的较旧值。但是，必须手动键入监视器参数的值。

4. 键入用于在实例上创建监视器的新参数的值。
5. 在 目标实例” 下，单击并选择要在其中运行配置的 Citrix ADC 实例的 IP 地址。请注意，您可以根据需要指定任意数量的目标实例，在多个 Citrix ADC 上部署配置。
6. 单击试运行。“对 象页面显示将新创建、修改或从 Citrix ADC 实例中删除的对象。
7. 单击 创建可创建或更新所选实例的配置。如果目标实例是新的，则会创建配置包。否则，将更新实例上部署的现有配置。

> 注意：
>
> 您还可以单击刷新图标以添加最近发现的 Citrix ADC 实例。因此，这些实例在此窗口的实例列表中立即可用。刷新图标当前仅在 Citrix ADM 上可用。

您还可以将配置包从一个版本的样书迁移到下一个版本。在这里，您可能还必须键入新版本中存在的任何新必需参数的值。您还可以将配置包迁移到旧版本的样书。在这种情况下，将删除旧样本中不存在的额外参数。“对 象页面显示从配置中删除的任何对象。

成功迁移后，ConfigPack 将绑定到新的样本。



您可以看到配置包的名称和配置包 ID 与之前相同。但是 Citrix ADM 将样本名称更新为样本名称从样本 lb 。

构建您的样本

下面提供了示 例**-lb** 样书的完整内容供您参考：

```
name: example-lb
namespace: examples.stylebooks
version: "1.0"
display-name: Basic Load Balancer App
description: This is an example StyleBook that creates a load balancer
    application
schema-version: "1.0"
import-stylebooks:
  -
    namespace: com.citrix.adc.stylebooks
```



```
    prefix: stlb
    version: "1.0"
parameters-default-sources:
  - stlb::lb
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
<!--NeedCopy-->
```

示 例 **lb-mon** 样本的全部内容如下，供您参考：

```
name: example-lb-mon
namespace: examples.stylebooks
version: "1.0"
description: This is an example StyleBook that creates a load balancer
   application with monitors
display-name: Basic Load Balancer App with Monitors
schema-version: "1.0"
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    prefix: ns
    version: "10.5"
  -
    namespace: com.citrix.adc.stylebooks
    prefix: stlb
    version: "1.0"
  -
    namespace: com.citrix.adc.commontypes
    prefix: cmtypes
    version: "1.0"
parameters-default-sources:
  - stlb::lb
parameters:
  -
    name: monitors
    label: "List of Monitors"
    description: "List of Monitors to monitor Application Servers"
    type: cmtypes::monitor[]
substitutions:
```



```
  mon-name(appname, monname): $appname + "-mon-" + $monname
components:
  -
    name: lb-comp
    type: stlb::lb
    description: Uses the default lb StyleBook to build the typical lb
       configuration objects
    properties-default-sources:
      - $parameters
  -
    name: monitors-comp
    type: cmtypes::monitor
    condition: $parameters.monitors
    repeat: $parameters.monitors
    repeat-item: mon
    repeat-index: ndx
    description: Builds a list of Citrix ADC monitor objects and binds
       them to the servicegroup of this LB config
    properties-default-sources:
      - $mon
    properties:
        monitorname: $substitutions.mon-name($parameters.lb-appname,
           $mon.monitorname)
    components:
      -
        name: monitor-svcg-binding-comp
        condition:  $parameters.svc-servers
        type: ns::servicegroup_lbmonitor_binding
        properties:
          servicegroupname: $components.lb-comp.outputs.servicegroup.
             properties.servicegroupname
          monitor_name: $parent.properties.monitorname
<!--NeedCopy-->
```

使用 **API** 从样本创建配置

April 23, 2021

构建样本后，您必须将其导入到 Citrix Application Delivery Management (ADM)，以便使用 Citrix ADM 或 Citrix ADM API 来使用样本。Citrix ADM 会在导入样本时验证样本，如果验证成功，样本将显示在 Citrix ADM 样本目录中，可用于创建配置。

现在可以使用样本 API 基于此样本创建配置。您可以使用任何工具（如 curl 命令行工具或邮递员铬浏览器扩展）将 HTTP 请求发送到 Citrix ADM。

示例 **1**

考虑您在中创建的 “lb-vserver” 样本用于创建负载平衡虚拟服务器的样本。使用 REST API 从此样书创建配置包，如下所示：

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks

<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "lb1",
      "ip": "10.102.117.31"
     }
 ,
    "target_devices":
    [
      {

        "id": "deecee30-f478-4446-9741-a85041903410"
       }

    ]
 }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，ID（例如 deecee30-f478-4446-9741-a85041903410）是在其中创建 IP 地址为 10.102.117.31 的负载平衡虚拟服务器 lb1 的 Citrix ADC 实例的实例 ID。从 Citrix ADM 中检索到 Citrix ADC 实例的实例 ID。

要获取由 Citrix ADM 管理的实例的 ID，可以使用 Citrix ADM API。例如，要检索 IP 地址为 192.168.153.160 的 Citrix ADC 实例的实例 ID，您可以使用以下 API：

```
GET https://<MAS-IP>/nitro/v1/config/ns?filter=ip_address
    :192.168.153.160
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

在有效负载中，响应包含 ID：

```
200
OK
Content-Type: application/json
{

  "errorcode": 0,
  "message": "Done",
  "operation": "get",
  "resourceType": "ns",
  "username": "nsroot",
  "tenant_name": "Owner",
  "resourceName": "",
  "ns":
  [
    {

    "is_grace": "false",
    "hostname": "",
    "std_bw_config": "0",
    "gateway_deployment": "false",
    …"id": "deecee30-f478-4446-9741-a85041903410",
    ...
    }

 ]
 }

<!--NeedCopy-->
```

如果成功创建了配置包，您将收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
```



```
{

  "configpack":
  {

    "config_id": "1460806080"
   }

 }

<!--NeedCopy-->
```

您已经创建了第一个使用 id 1460806080 唯一标识的配置包。可以使用此 ID 查询、更新或删除该配置。

示例 **2**

您可以使用相同的样书创建另一个配置包并在相同或不同的 Citrix ADC 实例上执行该配置包。在此示例中，创建另一个配置并为虚拟服务器提供不同的名称和 IP 地址，另外还指定 LEASTCONNECTION 作为负载平衡方法。在两个 Citrix ADC 实例上部署此配置。

HTTP 请求如下：

```
POST

https://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/lb-vserver/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "lb2",
      "ip": "10.102.117.32",
      "lb-alg": "LEASTCONNECTION"
     }
 ,
    "target_devices"
```



```
    [
     {
 "id": "deecee30-f478-4446-9741-a85041903410" }
 ,
     {
 "id": "debecc60-d589-4557-8632-a74032802412" }

    ]
   }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，在由 ID deecee30-f478-4446-9741-a85041903410 和 debecc60-d589-4557-8632-a74032802412 表示的两个 Citrix ADC 实例上创建 IP 地址为 10.102.117.32 的负载平衡虚拟服务器 lb2。

成功创建配置包后，将收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

   "configpack":
  {

     "config_id": "1657696292"
   }

 }

<!--NeedCopy-->
```

这个新的配置包具有不同的 ID 165769629。您可以通过使用此 ID 更新或删除此配置。

示例 3

考虑您在中创建的“基本 Lb-config”样本用于创建基本负载平衡配置的样本。使用 REST API 从此样书创建配置包，如下所示：

```
POST

http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.example
    .stylebooks/0.1/basic-lb-config/configpacks
<!--NeedCopy-->
```



```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters":
    {

      "name": "myapp",
      "ip": "10.70.122.25",
      "svc-servers":
      ["192.168.100.11","192.168.100.12"],
       "svc-port": 8080
     }
 ,
    "target_devices":
    [
     {

      "id": "deecee30-f478-4446-9741-a85041903410"
      }
 ,
     {

      "id": "debecc60-d589-4557-8632-a74032802412"
      }

    ]
   }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，负载平衡配置在两个 Citrix ADC 实例上执行。您可以登录到这些 Citrix ADC 实例，以验证是否创建了绑定了两个服务的虚拟服务器和服务组。

示例 **4**

考虑您在中创建的复合样本合成 示例创建复合样本**/en-us/citrix-application-delivery-management-software/current-release/stylebooks/how-to-create-custom-stylebooks/create-composite-**

stylebook.html[()]。使用 REST API 从此样书创建配置包，如下所示：

```
POST http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack":
  {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53"]
     }
 ,
    "target_devices":
    [
    {

      "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
    {

      "id": "debecc60-d589-4557-8632-a74032802412"
     }

    ]
  }

 }

<!--NeedCopy-->
```

在此 HTTP 请求中，将在两个由其 ID 表示的 Citrix ADC 实例上创建配置。如果您登录到 Citrix ADC 实例，则可以查看导入到 “复合示例” 样本中的 “基本 lb-config” 样本创建的配置对象。您还可以看到名为 “myapp-mon” 的新 HTTP 监视器，它属于 “composite-example” 样书的一部分。

成功创建配置包后，将收到以下 HTTP 响应：


```
200 OK
Content-Type: application/json{

  "configpack": {

    "config_id": "4917276817"
   }

 }

<!--NeedCopy-->
```

更新配置

要更新此配置，例如，通过向负载平衡虚拟服务器 myapp 添加具有 IP 地址 10.102.29.54 的新后端服务器，请使用 API 更新配置包，如下所示：

```
PUT http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

  "configpack": {

    "parameters": {

      "name": "myapp",
      "ip": "2.2.2.2",
      "svc-servers": ["10.102.29.52","10.102.29.53","10.102.29.54"]
   }
 ,
  "target_devices":
  [
    {

    "id": "deecee30-f478-4446-9741-a85041903410"
     }
 ,
  {

    "id": "debecc60-d589-4557-8632-a74032802412"
```



```
    }

]
 }

 }

<!--NeedCopy-->
```

成功更新配置包后，将收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config-id": "4917276817"
   }

 }

<!--NeedCopy-->
```

删除配置

要删除此配置（从所有 Citrix ADC 实例中），您可以使用 API 删除配置包，如下所示：

```
DELETE http://<MAS-DNS-or-IP>/stylebook/nitro/v1/config/stylebooks/com.
   example.stylebooks/0.1/composite-example/configpacks/4917276817
<!--NeedCopy-->
```

```
Accept: application/json
<!--NeedCopy-->
```

成功删除配置包后，将收到以下 HTTP 响应：

```
200 OK
Content-Type: application/json
{

   "configpack": {

     "config_id": "4917276817"
```



```
    }

 }

<!--NeedCopy-->
```

您可以登录 Citrix ADC 实例并验证是否已删除属于此配置包的所有配置对象。

如果要从特定 Citrix ADC 实例而不是从所有实例中删除配置，请使用上述更新配置包操作并更改 JSON 负载中的“target_devices”属性以删除特定的 Citrix ADC 实例 ID。

使用 **API** 创建配置以上传证书和密钥文件

April 23, 2021

可使用样本 API 基于此样本创建配置。您可以使用任何工具（如 curl 命令行工具或 Postman Chrome 浏览器扩展）将 HTTP 请求发送到 Citrix Application Delivery Management (ADM)。

考虑您为在中上传证书和密钥文件而创建的样本示例如何创建样本以将 SSL 证书和证书密钥文件上传到 Citrix ADM。使用 REST API 从此样书创建配置包，如下所示：

```
POST

https://<MAS_IP_Address>/stylebook/nitro/v1/config/stylebooks/com.
   citrix.adc.stylebooks/1.0/lb-mon/configpacks?mode=async
<!--NeedCopy-->
```

```
Content-Type: application/jsonAccept: application/json {

   "configpack": {

       "parameters": {

           "lb-appname": "lbmon",
           "lb-virtual-ip": "13.1.11.10",
           "lb-virtual-port": "80",
           "lb-service-type": "HTTP",
           "svc-service-type": "HTTP",
           "svc-servers": [
               {

                   "ip": "14.1.1.15",
                   "port": "80"         }
```



```
17
18        ],
19             "certificates": [
20                 {
21
22                     "cert-name": "server_cert",
23                     "cert-file": "server_cert.pem",
24                     "ssl-inform": "PEM",
25                     "key-name": "server_key",
26                     "key-file": "server_key.pem",
27                     "cert-password": "secret",
28                     "cert-advanced": {
29
30                         "is-ca-cert": false,
31                         "skip-ca-name": false
32             }
33
34           }
35
36        ],
37             "lb-advanced": {
38
39                 "flush-on-state-down": "ENABLED",
40                 "auth-params": {
41
42                     "authentication": "OFF",
43                     "authentication-http-401": "OFF"
44           }
45   ,
46                 "appflow-log": "ENABLED",
47                 "algorithm": "LEASTCONNECTION"
48         }
49   ,
50             "svcg-advanced": {
51
52                 "svc-client-ip": "DISABLED",
53                 "svc-use-source-ip": "NO",
54                 "svc-use-proxy-port": "NO",
55                 "svc-surge-protection": "OFF",
56                 "svc-client-keepalive": "NO",
57                 "svc-tcp-buffering": "NO",
58                 "svc-compression": "NO",
59                 "svc-state": "ENABLED",
60                 "svc-downstate-flush": "DISABLED",
61                 "svc-enable-health-monitor": "NO"
```



```
        }

      }
  ,
        "targets": [
            {

                "id": "8c158e7a-0087-423f-91b0-0ccf16de552a"
        }

     ]
    }

  }

<!--NeedCopy-->
```

此配置包通过使用 id 8c158e7a-0087-423F-91b0-0ccf16de552a 进行唯一标识。可以使用此 ID 查询、更新或删除该配置。成功更新配置包后，证书和密钥文件将上载到 Citrix ADM 文件系统。

使用 **API** 创建配置以上传任何文件类型

April 23, 2021

您还可以使用 Citrix Application Delivery Management (ADM) API 创建将文件上传到所选 Citrix ADC 实例的配置包。

考虑您为上传中任何类型的文件而创建的样书示例如何创建样书以将文件上载到 Citrix ADC MA 服务。如上述主题中的示例所示，创建配置包并将参数“放置文件”的值指定为 Citrix ADM 上位置文件的文件路径。
使用 REST API 从此样书创建配置包，如下所示：

```
POST

https://<mas_ip>/stylebook/nitro/v1/config/stylebooks/com.citrix.adc.
    stylebooks.samples/1.0/upload-geolocations/configpacks
<!--NeedCopy-->
```

```
Content-Type: application/json
Accept: application/json
{

   "configpack":
   {
```



```
7
8        "parameters": {
9
10          "locationfile": "/var/mps/tenants/root/files/ /
             custom_geolocations.csv"
11       }
12   ,
13        "targets": [
14          {
15
16              "id": "5e540839-cd6c-437e-ac53-7d49bc2602b5"
17          }
18
19      ]
20     }
21
22   }
23
24 <!--NeedCopy-->
```

使用 **API** 导入自定义样本

April 23, 2021

您现在可以使用样本 API 将自定义样本导入到 Citrix Application Delivery Management (ADM) 中。使用 REST API 从此样书创建配置包，如卷曲命令行工具或 Postman chrome 浏览器扩展程序等任何工具中的如下所示。例如，您可以导入名为 exam-lb 的样本，该样本可用于在 Citrix ADC 实例上创建负载平衡器配置。

```
1  HTTP Method: POST
2  URL: http://<mas-ip>/stylebook/nitro/v1/config/stylebooks
3  Headers:
4  Content-Type: application/json
5  Accept: application/json
6  RequestBody:
7  {
8
9         "stylebook":
10   {
11
12      "file_name": "example-lb.yaml",
13      "source": "<base64-contents>",
14      "encoding": "base64"
```



```
    }

  }

<!--NeedCopy-->
```

其中，“源”属性的值是样书文件内容的 base64 编码。您可以将样书文件的 YAML 内容粘贴到联机工具中，例如，https://www.browserling.com/tools/file-to-base64 获取 base64 字符串，然后可以将其用作上述“source”属性的值。

使用此 API 调用，您还可以在一个 API 操作中上传包含多个样本文件的压缩 tarball 文件（.tgz 文件）。为此，只需将 file_name 属性更改为.tgz 文件名，将源属性的值更改为.tgz 文件内容的 base64 编码。

在工具中成功运行 API 后，您会收到以下响应，指示样本已导入 Citrix ADM。

```
200 OK
<!--NeedCopy-->
```

响应正文：

```
{


  "stylebook":
{


    "name": "example-lb",

    "namespace": "com.example.stylebook",

    "version": "1.0"

   }


  }

<!--NeedCopy-->
```

使用 **API** 下载自定义样本

April 23, 2021

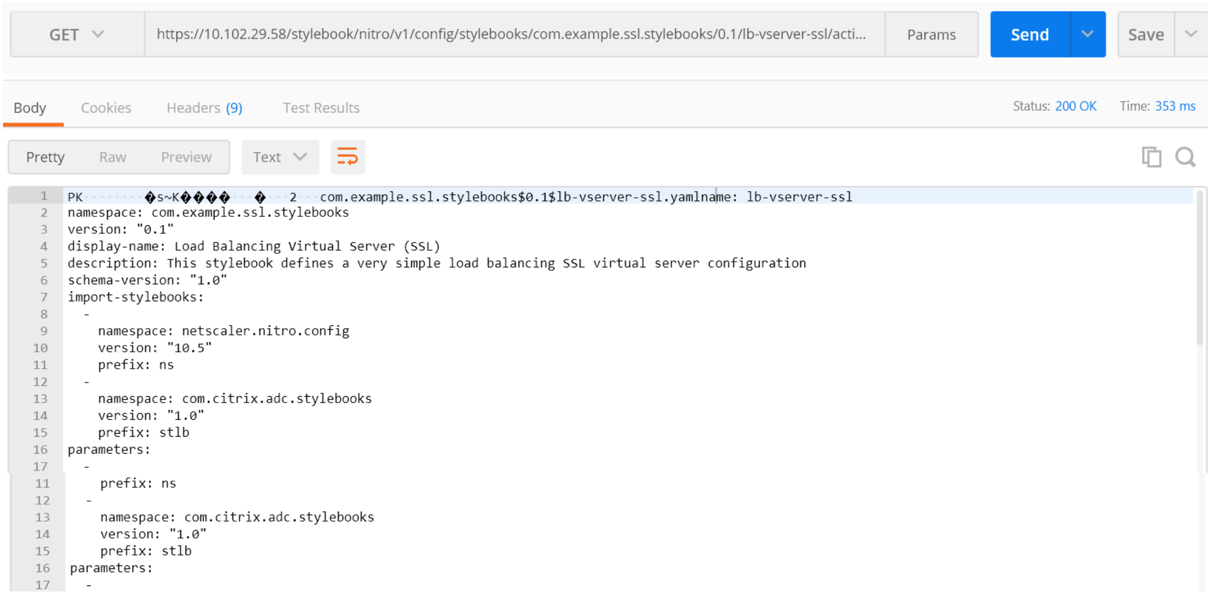
您可以通过提供以下样书 REST API 来下载自定义样书：

```
GET

https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>/actions/download
<!--NeedCopy-->
```

对 IP 地址、名称、版本和命名空间字段进行修改后，您可以在任何工具（如 curl 命令行工具或 Postman Chrome 浏览器扩展）中运行 API。

```
GET

https://10.102.29.58/stylebook/nitro/v1/config/stylebooks/com.example.
    ssl.stylebooks/0.1/lb-vserver-ssl/actions/download`
<!--NeedCopy-->
```

将下载.yaml 格式的样本。



使用 **API** 删除自定义样本

April 23, 2021

您可以通过提供以下样本 REST API 删除自定义样本：

```
DELETE

```



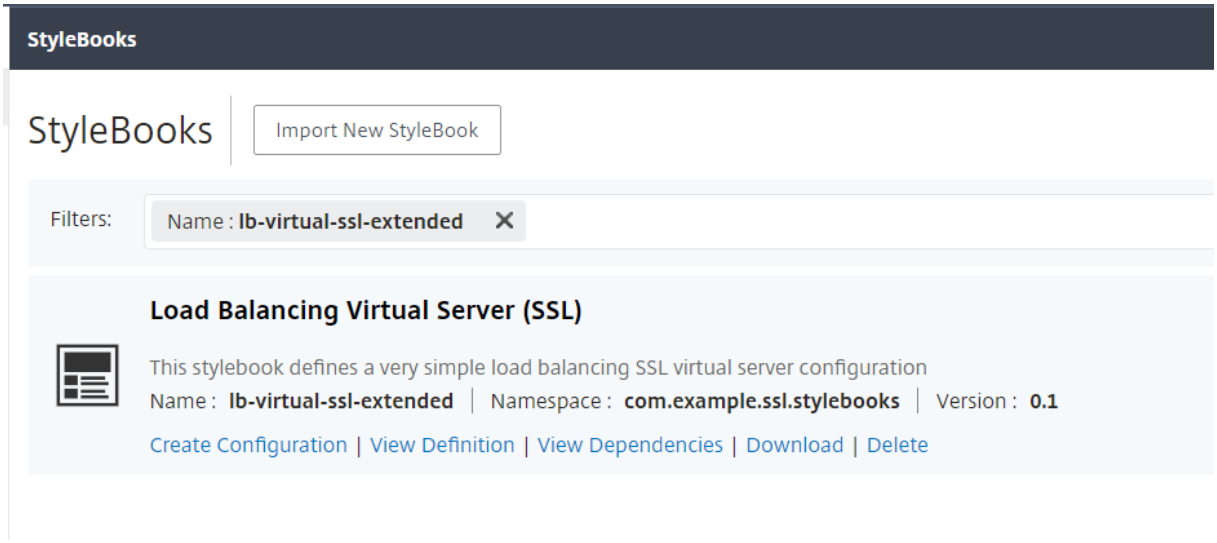
```
https://<MAS_IP>/stylebook/nitro/v1/config/stylebooks/<NAMESPACE>/<
    VERSION>/<NAME>?dependencies=true
<!--NeedCopy-->
```

如果 URL 中没有提供依赖关系查询参数或其值设置为 false，则不会删除样本依赖关系（仅删除样本本身）。

当您收到的 HTTP 响应状态代码为 200 时，这意味着自定义样书（及其依赖关系）已从 Citrix ADM 中成功删除。

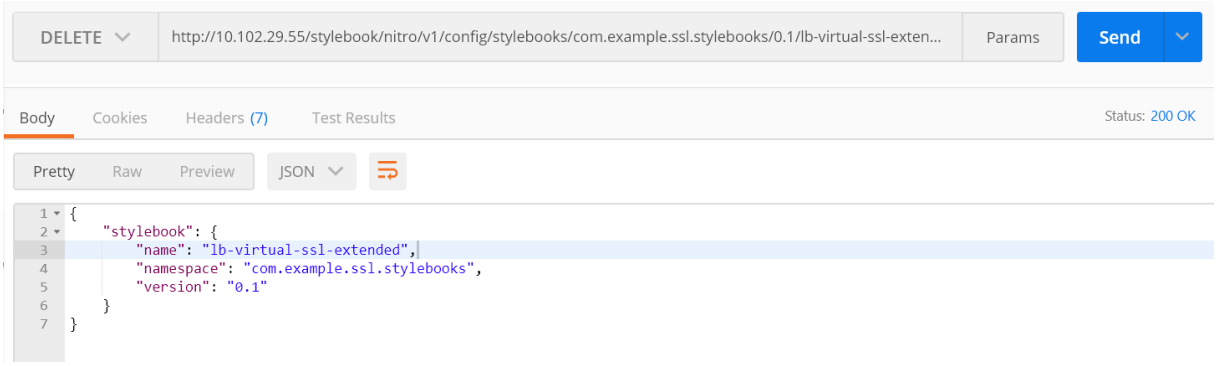
> 注意
>
> 您不能删除具有其他样本的 MA 服务中依赖于它的自定义样本。

例如，假定您在 Citrix ADM 中创建了名为 “lb-虚拟 ssl-扩展” 的样本。您后来决定删除该样本。

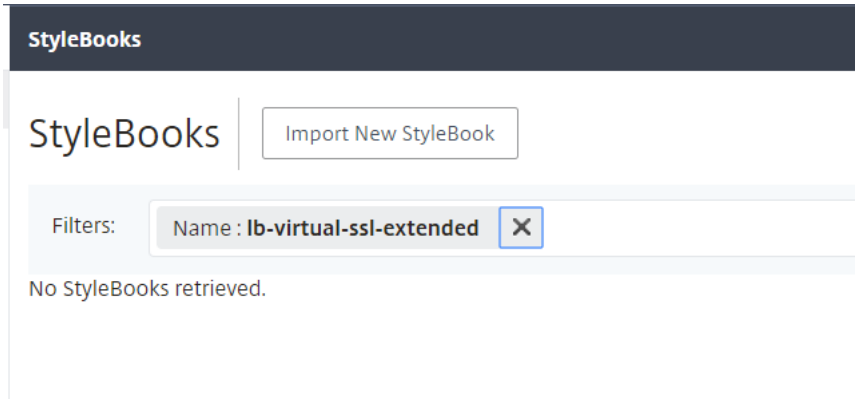


对 IP 地址、名称、版本和命名空间字段进行修改后，您可以在任何工具（如 curl 命令行工具或 Postman Chrome 浏览器扩展）中运行 API。

删 除https://10.102.29.55/stylebook/nitro/v1/config/stylebooks/com.example.ssl.stylebooks/0.1/lb-virtual-ssl-extended?dependencies=false



样本将从 Citrix ADM 中删除。



样本语法

April 23, 2021

您可以设计自己的样本，将其导入到 Citrix Application Delivery Management (ADM)，然后使用它们通过使用 Citrix ADM GUI 或使用 API 创建配置。为了能够创建您自己的样本，必须先了解您可以使用的不同构造和属性的语法和句法。

本文档介绍了创建样本时可以使用的不同构造和引用。

单击下表中的部分、构造或引用名称可查看详细信息。

标题	导入样本
参数	参数-默认源构造
替换	组件
可选属性	帮助程序组件
属性默认源	嵌套组件
条件构造	重复构造
重复条件构造	输出
嵌套重复	父引用
参数引用	替换引用
元件参考	操作
变量引用	警报
分析	内置函数
表达式	依赖性检测
原位内插	

> 注意
>
> 定义重复项、重复索引或替代函数的参数时，不要使用以下保留字命名用户定义的变量 $<var-name>
>
> - stylebook、parameters、substitutions、components、properties、outputs、parent、self、operations、analytics、alarms
> - repeat-item、repeat-item-0、repeat-item-1、repeat-item-2
> - repeat-index、repeat-index-0、repeat-index-1、repeat-index-2
> - default
> - roles、role、targets、target
> - context、parent-context、parent_context

有关如何设计自己的样本的信息和示例，请参阅如何创建您自己的样本。

标题

April 23, 2021

样书的前六行构成标头部分。此部分用于定义样本的标识，以及介绍它做什么。这是必需的部分。

下表介绍标头部分的属性：

属性	说明
—	—
name	用于标识样本的名称。此属性是必需的。
display-name	样本的描述性名称。此名称将显示在 Citrix ADM GUI 上。这是可选属性。
description	描述文本定义了此样书的作用。此描述将显示在 ADM 图形用户界面上。这是可选属性。注意：这是一个 HTML 片段，您可以使用 HTML 标签来自定义标题或使用带有 URL 或嵌入图像的标 <img> 签插入图像。
author	创建样本的作者个人或组织。这是可选属性。
namespace	命名空间构成样本的唯一标识符的一部分，以避免发生名称冲突。命名空间可以是任何字符串，但良好的做法是用它来表示创建和拥有一组样本的公司、部门或单位。例如，您可以使用以下格式：<company>.<department>.<unit>.stylebooks。这是必需属性。
version	样本的版本号。可以在更新样本时更改版本号。不同版本的样本可以共存在一起。这是必需属性。
schema-version	样本架构的版本。它采用 Citrix ADM 的当前版本中的值 “1.0”。这是必需属性。
private	如果此属性设置为 true，则样本不会显示在 Citrix ADM GUI 上。对于构建用于其他样本的块且不打算由用户直接使用的样本，这是很有用的设置。这是可选属性。其默认值为 false。

示例：

```
1     name: lb
2     description: "This stylebook defines a sample load balancing
     configuration."
```



```
    display-name: "Load Balancing StyleBook (HTTP)"
    author: Mike Smith (ACME Infra team)
    namespace: com.example.stylebooks
    schema-version: "1.0"
    version: "0.1"
<!--NeedCopy-->
```

name、namespace 和 version 组合在系统中唯一标识样本。Citrix ADM 中不能有两个具有相同名称、命名空间和版本组合的样本。但可以有两个 name 和 version 相同但 namespace 不同或 namespace 和 version 相同但 name 不同的样本。

导入样本

April 23, 2021

这是样本的第二个部分，在此部分可以声明要在当前样本中引用哪个其他样本。这样可以导入并重用其他样书，而不是在您自己的样书中重新构建相同的配置。这是必需的部分。

必须在当前样本中声明要引用的样本的 **namespace** 和 **version** 号。直接使用任何一个 NITRO 配置对象的每个样本都必须引用 netscaler.nitro.config 命名空间。此命名空间包含所有 Citrix ADC NITRO 类型，例如 lbvserver 服务或监视器。支持 Citrix ADC 10.5 及更高版本的样本，这意味着您可以使用样本在运行 10.5 或更高版本的任何 Citrix ADC 实例上创建和运行配置。

import-stylebooks 部分中使用的 **prefix** 属性是指代命名空间和版本组合的简写。例如，“ns” 前缀可以用于指代命名空间 netscaler.nitro.config 和版本 10.5。在样书的后面部分中，不必每次要引用具有此命名空间和版本的样书时使用命名空间和版本，只需将所选前缀字符串与样书名称一起使用即可唯一标识它。

示例：

```
    import-stylebooks:
     -
       namespace: netscaler.nitro.config
       version: "10.5"
       prefix: ns
    -
     namespace: com.acme.stylebooks
      version: "0.1"
      prefix: stlb
<!--NeedCopy-->
```

在上述示例中，定义的第一个前缀名为 ns，它指代命名空间 netscaler.nitro.config 和版本 10.5。定义的第二个前缀名为 stlb，它指代命名空间 com.acme.stylebooks 和版本 0.1。

定义了前缀后，每次要引用属于一个特定命名空间和版本的类型或样本时，可以使用表示法 **<namespace-shorthand>::<type-name>**。例如，**ns::lbvserver** 指代在命名空间 netscaler.nitro.config（版本 10.5）中定义的类型 lbvserver。

同样，如果要引用 com.acme.stylebooks 命名空间中版本为 “0.1” 的样本，可以使用表示法 **stlb::<stylebook-name>**。

> 注意
>
> 按照惯例，前缀 “ns” 用于指 Citrix ADC 的 NITRO 命名空间。

参数

April 23, 2021

在此部分可以定义样本中用于创建配置所需的所有参数。它描述样本接收的输入。尽管此部分是可选的，但大多数样书可能需要一个。您可以考虑参数部分为使用样书在 Citrix ADC 实例上创建配置的用户定义字段。

将样书导入 Citrix ADM 并使用它创建配置时，GUI 使用样书的这一部分来显示表单。此表单接受定义的参数值的输入。

以下部分介绍了需要为本节中的每个参数指定的属性：

‘name’

要定义的参数的名称。可以指定字母数字名称。

名称必须以字母表开头，并且可以包含更多的字母、数字、连字符 (-) 或下划线 (_)。

在编写样书时，您可以使用此 “name” 属性通过使用表示法 $ 参数来引用其他部分中的参数。<name>。

强制性？是

‘label’

在 ADM GUI 中显示为此参数的名称的字符串。

强制性？否

‘description’

说明参数用途的帮助字符串。当用户单击此参数的帮助图标时，ADM GUI 将显示此文本。

强制性？否

‘type’

这些参数可以接收的值类型。参数可以是以
下内置类型之一：

- string：字符数组。如果未指定长度，则字符串值可以接收任何数量的字符。但是，可以使用 min-length 和 max-length 属性限制字符串类型的长度。
- `number`：一个整数。可以使用 min-value 和 max-value 属性指定此类型可以接收的最小数和最大数。
- **`boolean`**：可以是真的也可以是假的。YAML 将所有文字视为布尔值（例如，是或否）。
- `ipaddress`：表示有效的 IPv4 或 IPv6 地址的字符串。
- `tcp-port`：介于 0 到 65535 之间的数字，表示 TCP 或 UDP 端口。
- `password`：表示不透明/密码字符串值。当 ADM GUI 显示此参数的值时，它将显示为星号 (*****)。
- `certfile`：表示证书文件。使用 ADM GUI 创建样书配置时，此值允许您直接从本地系统上传文件。上传的证书文件存储在 ADM 的 `/var/mps/tenants/\<tenant_path>/ns_ssl_certs` 目录中。

  证书文件将添加到 ADM 管理的证书列表中。
- `keyfile`：表示证书密钥文件。使用 ADM GUI 创建样书配置时，此值允许您直接从本地系统上传文件。上传的证书文件存储在 ADM 的 `/var/mps/tenants/\<tenant_path>/ns_ssl_keys` 目录中。

  证书密钥文件将添加到 ADM 管理的证书密钥列表中。
- `file`：代表一个文件。
- `object`：当您想要将多个相关参数分组到父元素下时，将使用此类型。将类型的父参数指定为 “对象”。类型为 “object” 的参数可以有嵌套的 “parameters” 部分以描述其包含的参数。
- `another StyleBook`：当您使用此类型的参数时，此参数期望其值以表示其类型的样书中定义的参数的形式。

参数也可以包含具有类型列表的 `type`。为此，请在文字末尾添加 `[]`。例如，如果 `type` 属性为 `string[]`，则此参数将字符串列表作为输入。可以在使用此样书创建配置时为此参数提供一个、两个或多个字符串。

强制性？ 是

‘network’

对于 `type: ipaddress`，您可以指定从 ADM IPAM 网络自动分配 IP 地址的 `network` 属性。

创建样书配置时，ADM 会从 `network` 属性中自动分配 IP 地址。

示例：

```
1       name: virtual-ip
2       label: "Load Balancer IP Address"
3       type: ipaddress
```



```
        network: "network-1"
        required: true
<!--NeedCopy-->
```

在此示例中，virtual-ip 字段自动分配来自 network-1 的 IP 地址。删除配置后，IP 地址将释放回网络。

‘dynamic-allocation’

dynamic-allocation 属性将添加到 type:ipaddress 的参数定义中。使用此属性动态列出 ADM IPAM 网络。此属性可以采用 **true** 或 **false** 作为输入。对于 type: ipaddress，指定 dynamic-allocation: **true** 属性以动态列出 ADM 中的 ADM IPAM 网络。在配置包创建窗体中，您可以执行以下操作：

1. 从列表中选择所需的 IPAM 网络。
2. 指定要从所选 IPAM 网络分配的 IP 地址。

   如果未指定 IP 地址，ADM 将自动分配来自所选 IPAM 网络的 IP 地址。

示例：

```
  -
    name: virtual-ip
    label: "Load Balancer IP Address"
    type: ipaddress
    dynamic-allocation: true
    required: true
<!--NeedCopy-->
```

在此示例中，virtual-ip 字段列出了 ADM 中的 ADM IPAM 网络。从列表中选择一个网络以从网络中自动分配 IP 地址。删除配置后，IP 地址将释放回网络。

‘key’

指定 true 或 false 指示此参数是否是样本的主要参数。

样本只能有一个定义为 “key” 参数的参数。

当您从同一样书（在相同或不同的 ADC 实例上）创建
不同的配置时，每个配置都有此
参数的不同/唯一值。

默认值为 false。

强制性？否

‘required’

指定 true 或 false 指示参数是必需的还是可选的。如果
设置为 true，则该参数是必需的，用户在创建配置时必须为此
参数提供值。

ADM GUI 强制用户为此参数提供有效值。

默认值为 false。

强制性? 否

‘allowed-values’

类型设置为 “string” 时，此属性用于定义参数的有效值列表。

从 ADM GUI 创建配置时，系统会提示用户从此列表中选择参数值。

> 注意
>
> 如果要将列表值显示为单选选项，请设置 [layout](#layout) 属性。

示例 **1**:

```
-
       name: ipaddress
       type: string
       allowed-values:
             -  SOURCEIP
             -  DEST IP
             -  NONE
<!--NeedCopy-->
```

示例 **2**:

```
-
       name: TCP Port
       type: tcp-port
       allowed-values:
             -  80
             -  81
             -  8080
<!--NeedCopy-->
```

示例 **3**:

tcp-ports 的列表，其中列表的每个元素只能在 allowed-values 中指定的值。


```
-
      name: tcpports
      type: tcp-port[]
      allowed-values:
            -  80
            -  81
            -  8080
            -  8081
<!--NeedCopy-->
```

强制性? 否

‘default’

此属性用于为可选参数指定默认值。当用户在未指定值的情况下创建配置时，将使用默认值。

如果满足以下条件，则参数不具任何值：

- 该参数没有默认值。
- 用户没有为参数提供值。

示例 **1**：

```
-
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

示例 **2**：

要列出参数的默认值，请执行以下操作：

```
-
      name: protocols
      type: string[]
      default:
            -  TCP
            -  UDP
            -  IP
<!--NeedCopy-->
```

示例 **3**：

```
-
```



```
      name: timeout
      type: number
      default: 20
<!--NeedCopy-->
```

示例 **4**:

```
-
      name: tcpport
      type: tcp-port
      default: 20
<!--NeedCopy-->
```

强制性? 否

‘pattern’

当参数的类型为 “string 时，使用此属性定义此
参数的有效值的模式（正则表达式）。“

示例:

```
-
      name: appname
      type: string
      pattern: "[a-z]+"
<!--NeedCopy-->
```

强制性? 否

‘min-value’

使用此属性可定义 `number` 或 `tcp-port` 类型参数的最小值。

示例:

```
-
      name: audio-port
      type: tcp-port
      min-value: 5000
<!--NeedCopy-->
```

`min-value` 数字可能是负数。但是，`min-value`（对于 `tcp-port`）必须是正数。

强制性? 否

‘max-value’

使用此属性可定义类型 `number` 或
`tcp-port` 的参数的最大值。

确保最大值大于最小值（如果已定义）。

示例：

```
-
       name: audio-port
       type: tcp-port
       min-value: 5000
       max-value: 15000
<!--NeedCopy-->
```

强制性？否

‘min-length’

使用此属性可定义
类型为 “string” 的参数所接受的值的最小长度。“

确保定义为值的字符的最小长度大于或等于零。

示例：

```
-
       name: appname
       type: string
       min-length: 3
<!--NeedCopy-->
```

强制性？否

‘max-length’

使用此属性可以定义
类型为 “string 的参数所接受的值的最大长度。“

确保值的最大长度大于或等于在 `min-length` 中定义的字符的长度。

示例：

```
-
       name: appname
       type: string
```



```
        max-length: 64
<!--NeedCopy-->
```

强制性？否

‘min-items’

此属性用于定义列表参数中的最小项目数。

确保最小商品数量大于或等于零。

示例：

```
-
        name: server-ips
        type: ipaddress[]
        min-items: 2
<!--NeedCopy-->
```

强制性？否

‘max-items’

使用此属性可定义作为
列表的参数中的最大项数。

确保最大商品数量大于最小商品数（如果已定义）。

示例：

```
-
        name: server-ips
        type: ipaddress[]
        min-items: 2
        max-items: 250
<!--NeedCopy-->
```

强制性？否

‘Gui’

使用此属性可在 ADM GUI 中自定义参数的布局。

强制性？否

‘columns’

此属性是 gui 属性的子属性。使用此属性可定义要在 ADM GUI 中显示 type: object[] 参数的列数。

强制性？否

‘updatable’

此属性是 gui 属性的子属性。使用此属性可指定在创建配置后是否可以更新参数。仅在字符串、布尔值或数字等简单参数类型上设置此属性。

如果该值设置为 **false**，则在更新配置时，参数字段将显示为灰色。

强制性？否

‘collapse_pane’

此属性是 gui 属性的子属性。使用此属性可指定定义此对象参数布局的窗格是否可折叠。

如果值设置为 true，则用户可以展开或折叠此父参数下方的子参数。

示例：

```
gui:

 collapse_pane: true

 columns: 2
<!--NeedCopy-->
```

完整的 parameters 部分示例：

```
parameters:

   -

      name: name

      label: Name

      description: Name of the application

      type: string

      required: true

   -
```



```
16
17        name: ip
18
19        label: IP Address
20
21        description: The virtual IP address used for this application
22
23        type: ipaddress
24
25        required: true
26
27    -
28
29        name: svc-servers
30
31        label: Servers
32
33        type: object[]
34
35        required: true
36
37        parameters:
38
39          -
40
41                name: svc-ip
42
43                label: Server IP
44
45                description: The IP address of the server
46
47                type: ipaddress
48
49                required: true
50
51          -
52
53                name: svc-port
54
55                label: Server Port
56
57                description: The TCP port of the server
58
59                type: tcp-port
60
```



```
                default: 80

        -

                name: lb-alg

                label: LoadBalancing Algorithm

                type: string

                allowed-values:

                   - ROUNDROBIN

                   - LEASTCONNECTION

                default: ROUNDROBIN

        -

                name: enable-healthcheck

                label: Enable HealthCheck?

                type: boolean

                default: true
<!--NeedCopy-->
```

下面的示例定义前面的部分中说明的所有列表属性和值：

```
        -
                name: features-list

                type: string[]

                min-length: 1

                max-length: 3

                min-items: 1

                max-items: 3

                pattern: "[A-Z]+"
```



```
15
16                allowed-values:
17
18                  - SP
19
20                  - LB
21
22                  - CS
23
24                default:
25
26                  - LB
27  <!--NeedCopy-->
```

‘layout’

此属性是 gui 属性的子属性。使用此属性可以将列表值显示为单选按钮。在样书定义的参数部分中将 layout 属性设置为 radio。它适用于具有 [allowed-values](#allowed-values) 属性的参数。创建配置包时，ADM GUI 将列表中的值显示为 allowed-values 单选按钮。

示例:

```
1  -
2      gui:
3          layout: radio
4      allowed-values:
5          - One
6          - Two
7          - Three
8  <!--NeedCopy-->
```

“一”、“二” 和 “三” 值在 ADM GUI 中显示为单选按钮。

‘dependent-parameters’

此属性是 gui 属性的子属性。它根据在另一个参数中指定的值动态控制参数的外观或其初始值在样书配置窗体中。

在控制参数在表单上的行为的源参数上指定此属性。您可以包含多个控制其他参数的条件。例如，源参数 protocol 可以具有依赖参数 certificate，该参数仅在 protocol 参数值为 SSL 时才会显示。

每个条件都可以具有以下属性:

- **target-parameter**：指定此条件适用的目标参数。
- **matching-values**：指定触发操作的源参数的值列表。

- **action**：对目标参数指定以下操作之一：
  - read-only：该参数为只读。
  - show：如果参数被隐藏，则该参数将显示在窗体中。
  - hide：该参数将从表单中删除。
  - set-value：参数值被设置为值属性中指定的值。
- **value**：如果操作为 set-value，则为目标参数的值。

当用户输入与源参数上的指定值匹配时，目标参数的外观或值将根据指定的操作而发生变化。

示例：

```
-
   name: lb-virtual-port
   label: "Load Balanced App Virtual Port"
   description: "TCP port representing the Load Balanced application"
   type: tcp-port
   gui:
     updatable: false
     dependent-parameters:
           -
             matching-values:
               - 80
             target-parameter: $parameters.lb-service-type
             action: set-value
             allowed-values:
             - HTTP
             - TCP
             - UDP

   default: 80

<!--NeedCopy-->
```

在此示例中，依赖参数在 lb-virtual-port 参数（源参数）下指定。

当源参数值设置为 80 时，lb-service-type 参数将触发 set-value 操作。因此，允许用户选择以下选项之一：

- HTTP
- TCP
- UDP

参数-默认源构造

April 23, 2021

可以使用此构造来重用其他样本中的参数定义。

假设这样一个场景：一个参数或一组参数在多个样本中重复使用。为了避免重新定义这些参数，每次要创建新样本时，可以将其定义一次，然后使用 **parameters-default-sources** 构造将其定义导入需要这些参数的样本。

例如，如果多个样本需要配置虚拟 IP，可能必须在创建的每个新样本中定义与虚拟 IP 有关的相同参数。但是可以创建一个单独的样本（例如，名为 “vip-params”），在其中定义与其有关的所有参数，如以下示例中所示：

```
1       -
2       name: vip-params
3       namespace: com.acme.commontypes
4       version: "1.0"
5       description: This StyleBook defines a typical virtual IP config.
6       private: true
7       schema-version: "1.0"
8       parameters:
9         -
10            name: lb-appname
11            label: Load Balanced Application Name
12           description: Name of the Load Balanced application
13            type: string
14            required: true
15        -
16            name: lb-virtual-ip
17            label: Load Balanced App Virtual IP address
18            description: Virtual IP address representing the Load
      Balanced application
19            type: ipaddress
20            required: true
21        -
22            name: lb-virtual-port
23            label: Load Balanced App Virtual Port
24            description: TCP port representing the Load Balanced
      application
25            type: tcp-port
26            default: 80
27        -
28            name: lb-service-type
29            label: Load Balanced App Protocol
30            description: Protocol used for the Load Balanced application
      .
```



```
            type: string
            default: HTTP
            required: true
            allowed-values:
                 - HTTP
                 - SSL
                 - TCP
<!--NeedCopy-->
```

之后可以创建利用这些参数的其他样本。下面是这样一个样本示例。

```
    -
    name: acme-biz-app
    namespace: com.acme.stylebooks
    version: "1.0"
    description: This stylebook defines the Citrix ADC configuration
   for Biz App
    schema-version: "1.0"
    import-stylebooks:
      -
        namespace: com.acme.commontypes
        prefix: cmtypes
        version: "1.0"
    parameters-default-sources:
         - cmtypes::vip-params
    parameters:
        -
          name: monitorname
          label: Monitor Name
          description: Name of the monitor
          type: string
          required: true
        -
          name: type
          label: Monitor Type
          description: Type of the monitor
          type: string
          required: true
          allowed-values:
            - PING
            - TCP
            - HTTP
            - HTTP-ECV
            - TCP-ECV
            - HTTP-INLINE
```



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

在 acme-biz-app 样本中，首先通过使用 “import-stylebooks” 部分导入 vip-params 样本的命名空间和版本。然后添加 **parameters-default-sources** 构造，并指定样本名称，即 vip-params。这与在此样本中直接定义 vip-params 样本的参数效果一样。

由于 parameters-default-sources 是一个列表，且列表中的每个项目都需要是一个样本，因此可以包括多个样本中的参数。

除了包括其他样本中的参数外，还可以使用 parameters 部分定义您自己的参数。样本的完整参数列表是从其他样本中添加的参数和此样本中定义的参数的组合。因此，表达式 **$parameters** 是指此参数组合。

请注意，如果一个参数在导入的样本和当前样本中都定义了，则当前样本中的定义覆盖从其他样本导入的定义。可以在需要时自定义一些导入参数，同时按原样使用其余导入参数，有效利用这一点。

parameters-default-sources 构造还可以用于嵌套的参数中，如下所示：

```
parameters:
    -
      name: vip-details
      label: Virtual IP details
      description: Details of the Virtual IP
      type: object
      required: true
      parameters-default-sources:
              - cmtypes::vip-params
<!--NeedCopy-->
```

这与在此样本中将 vip-params 样本的参数直接作为 vip-details 参数的子参数添加类似。

替换

April 23, 2021

substitutions 部分用于定义可在样本其余部分使用的复杂表达式的简写名称，以使样本更加清晰。在样本中多次重复使用相同表达式或值（例如，一个常数值）时，它们也很有用。通过为此值使用替换名称，您可以在需要更改此值时只更新替换值，而不是在样本中出现的每一处更新它（这很容易出错）。

替换还用于定义值之间的映射，如本文档中后面的示例中所述。

列表中的每个替换都由一个关键字和一个值组成。值可以是简单值、表达式、函数或映射。

在以下示例中，定义了两个替换。第一个替换是可以用作 8181 的简写名称的 “http-port”。通过使用替换，可以在样本的其余部分以 **$substitutions.http-port** 引用它，而不是使用 8181。

替换：

http-port: 8181

这让您可以为端口号指定助记名称，并在样本中的一个地方定义此端口号，无论它被使用多少次。如果要将端口号修改为 8080，可以在替换部分修改它，该更改将在使用助记名称 http-port 的任何位置生效。以下示例说明了如何在组件中使用替换。

```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: HTTP
          ipv46: $parameters.ip
          port: \*\*$substitutions.http-port\*\*
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

替换也可以是复杂的表达式。以下示例说明了两个替换如何使用表达式。

```
substitutions:
  app-rule: HTTP.REQ.HEADER("X-Test-Application").EXISTS
  app-name: str("acme-") + $parameters.name + str("-app")
<!--NeedCopy-->
```

替换表达式还可以使用现有替换表达式，如以下示例中所示。

```
substitutions:
  http-port: 8181
  app-name: str("acme-") + $parameters.name + str($substitutions.http-
   port) + str("-app")
<!--NeedCopy-->
```

替换的另一个有用功能是映射，即可以将关键字映射到值。下面是一个映射替换示例。

```
substitutions:
    secure-port:
        true: int("443")
        false: int("80")
    secure-protocol:
        true: SSL
        false: HTTP
<!--NeedCopy-->
```

以下示例说明了如何使用映射 secure-port 和 secure-protocol。


```
components:
 -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
          name: $parameters.name + "-lb"
          servicetype: $substitutions.secure-protocol[$parameters.is-
    secure]
          ipv46: $parameters.ip
          port: $substitutions.secure-port[$parameters.is-secure]
          lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

这意味着，如果样本的用户将布尔值 “true” 指定为参数是安全的，或者在 Citrix ADM GUI 中选择了与此参数对应的复选框，则此组件的服务类型属性将分配值 **SSL** ，并且端口属性为分配了值 **443**。但是，如果用户为此参数指定 “false” 或清除 Citrix ADM GUI 中的相应复选框，则会为服务类型属性分配值 **HTTP** ，并为端口分配值 **80**。

以下示例说明了如何将替换用作函数。替换函数可以接受一个或多个参数。参数应属于简单类型，例如，字符串、数字、IP 地址、布尔值和其他类型。

替换：

form-lb-name(name): $name + “-lb”

在这个例子中，我们定义了一个替代函数 “form-lb-name”，该函数采用名为 “name” 的字符串参数，** 并使用它创建一个新字符串，该字符串后缀为 name 参数中的字符串。使用此替换函数的表达式可以编写如下：

$substitutions.form-lb-name(“my”)

此表达式返回 “my-lb”

看看另外一个示例：

替换：

cspol-priority(priority): 10100 - 100 * $priority

替换 cspol-priority 是一个函数，它接收名为 priority 的参数，并使用它来计算值。在样本的其余部分，可以使用此替换，如以下示例中所示：

```
components:
  -
    name: cspolicy-binding-comp
    type: ns::csvserver_cspolicy_binding
    condition: not $parameters.is-default
    properties:
         name: $parameters.csvserver-name
         policyname: $components.cspolicy-comp.properties.policyname
```



```
          priority: $substitutions.cspol-priority($parameters.pool.
    priority)
<!--NeedCopy-->
```

替换也可以由键和值组成。值可以是简单值、表达式、函数、映射、列表或字典。

以下是名为 'slist' 的替代示例，其值为列表：

```
substitutions:
  slist:
    - a
    - b
    - c
<!--NeedCopy-->
```

替换的值还可以是键值对字典，如以下示例中所示，这是名为 "sdict" 的替换：

```
substitutions:
  sdict:
    a: 1
    b: 2
    c: 3
<!--NeedCopy-->
```

您可以组合列表和字典来创建更加复杂的属性。例如，一个名为 "slistofdict" 的替换返回键值对列表。

```
  slistofdict:
    -
      a: $parameters.cs1.lb1.port
      b: $parameters.cs1.lb2.port
    -
      a: $parameters.cs2.lb1.port
      b: $parameters.cs2.lb2.port
<!--NeedCopy-->
```

但是，在以下示例中，名为 "sdictoflist" 的替换返回一个键值对，其中值本身是另一个列表。

```
  sdictoflist:
    a:
      - 1
      - 2
    b:
      - 3
      - 4
<!--NeedCopy-->
```


在组件中，这些替换可以用于 condition、properties、repeat、repeat-condition 构造中。

以下组件示例显示了如何使用替换指定属性：

```
    properties:
      a: $substitutions.slist
      b: $substitutions.sdict
      c: $substitutions.slistofdict
      d: $substitutions.sdictoflist
<!--NeedCopy-->
```

定义其值是列表或字典的替换的用例是当您配置一个内容交换虚拟服务器和多个负载平衡虚拟服务器时。由于绑定到同一 cs 虚拟服务器的所有 lb 虚拟服务器可能有相同的配置，因此，您可以使用替换列表和字典来构建此配置以避免对每个 lb 虚拟服务器重复使用该配置。

以下示例显示 cs-lb-mon 样本中用于创建内容交换虚拟服务器配置的替换和组件。构建 cs-lb-mon 样本的属性时，复杂的替换 “lb-properties” 指定与 cs 虚拟服务器关联的 lb 虚拟服务器的属性。“lb-properties” 替换是一个函数，接受名称、服务类型、虚拟 IP 地址、端口和服务器作为参数，并生成键值对作为值。在 “cs-pools” 组件中，我们将此替换的值指定给每个池的 lb-pool 参数。

```
substitutions:
  cs-port[]:
    true: int("80")
    false: int("443")
  lb-properties(name, servicetype, vip, port, servers):
    lb-appname: $name
    lb-service-type: $servicetype
    lb-virtual-ip: $vip
    lb-virtual-port: $port
    svc-servers: $servers
    svc-service-type: $servicetype
    monitors:
      -
        monitorname: $name
        type: PING
        interval: $parameters.monitor-interval
        interval_units: SEC
        retries: 3
components:
  -
    name: cs-pools
    type: stlb::cs-lb-mon
    description: | Updates the cs-lb-mon configuration with the
    different pools provided. Each pool with rule result in a dummy LB
    vserver, cs action, cs policy, and csvserver_cspolicy_binding
    configuration.
```



```
24      condition: $parameters.server-pools
25      repeat: $parameters.server-pools
26      repeat-item: pool
27      repeat-condition: $pool.rule
28      repeat-index: ndx
29      properties:
30        appname: $parameters.appname + "-cs"
31        cs-virtual-ip: $parameters.vip
32        cs-virtual-port: $substitutions.cs-port($parameters.protocol == "
      HTTP")
33        cs-service-type: $parameters.protocol
34        pools:
35          -
36            lb-pool: $substitutions.lb-properties($pool.pool-name, "HTTP"
      , "0.0.0.0", 0, $pool.servers)
37            rule: $pool.rule
38            priority: $ndx + 1
39  <!--NeedCopy-->
```

替代映射：

您可以创建将键映射到值的替换。例如，假设这样一个场景：您想要定义要用于每个协议（键）的默认端口（值）。对于此任务，按如下所示编写替换映射。

```
1  substitutions:
2       port:
3            HTTP: 80
4            DNS: 53
5            SSL: 443
6  <!--NeedCopy-->
```

在此示例中，HTTP 映射到 80，DNS 映射到 53，SSL 映射到 443。要检索作为参数提供的特定协议的端口，请使用表达式

$ 替换。端口 [$ 参数。协议]

该表达式根据用户指定的协议返回值。

- 如果键为 HTTP，则表达式返回 80
- 如果键为 DNS，则表达式返回 53
- 如果键为 SSL，则表达式返回 443
- 如果映射中没有键，则该表达式不返回任何值

组件

April 23, 2021

样本中的 components 构造被视为样本中最重要的部分。在此部分，定义必须要创建的配置对象。通过使用此构造，可以构建相同类型的一个或多个配置对象。

components 构造使用 parameters 部分中提供的输入来改写样本生成的配置。这是一个可选部分，尽管大多数样本都有一个 components 部分。

下表介绍了组件的主要属性。

属性	说明
—	—
名称	组件的名称。可以指定字母数字名称。名称必须以字母开头，可以包括其他字母、数字、连字符 (-) 或下划线 (_)。
description	样本中此组件的角色的说明。
type	类型确定此组件提供哪些属性。组件有两种类型：内置类型：此类型由系统提供，您不必定义它，例如，NITRO 实体类型 “lbvserver” 或 “服务组”。“ 当组件具有内置类型属性时，它会在 Citrix ADC 上创建该类型的配置对象。例如，如果某个组件引用内置类型 “lbvserver”，则此组件将在作为配置目标的 Citrix ADC 实例上创建一个负载平衡虚拟服务器。复合类型：此类型是指您创建并导入到 Citrix ADM 中的现有样书。当组件具有复合类型属性时，它会在作为配置目标的 Citrix ADC 实例上创建所有配置对象（在引用样本中指定）。这让您可以组合多个样本，其中每个样本创建最终配置的一部分。有关复合样本的更多信息，请参阅创建复合样本。
properties	可以用于组件类型属性的子属性。组件的有效属性由其类型决定。对于内置类型，有效属性是对应的 Nitro 对象的属性。对于其类型是另一个样本的组件（即复合类型），属性对应于该样本中定义的参数。

示例：

```
components:
   -
     name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
         name: $parameters.name
         servicetype: HTTP
         ipv46: $parameters.ip
         port: 80
         lbmethod: $parameters.lb-alg
<!--NeedCopy-->
```

在此示例中，定义了名为 my-lbvserver-comp 的组件。此组件的类型为 ns::lbvserver（内置类型），其中 “ns” 是指代在 import-stylebooks 部分中指定的命名空间 netscaler.nitro.config 和版本 10.5 的前缀，“lbvserver” 是此命名空间中的 NITRO 资源。

此部分中的属性包括 “lbvserver” 资源的四个必需属性和一个可选属性 (lbmethod)，您可以为这些属性指定值。在此示例中，为 servicetype 和 port 指定静态值，而 name、ipv46 和 lbmethod 属性从输入参数获取其值。使用 $parameters.<name> 表示法（例如 $parameters.ip）来引用在 parameters 部分定义的参数名称。

> 注意
>
> NITRO 资源类型的属性名称（其组件属性）必须使用小写。否则，样本导入将失败。

帮助程序组件

April 23, 2021

样本中 components 部分的主要用途是通过 Nitro 内置类型或创建实际配置对象的另一个样本来生成配置对象。帮助程序组件本身不会生成配置对象。帮助程序组件接收来自其他部分（例如，参数对象、其他组件的属性或其他组件的输出）的输入，并将其传输到其他表单中。以后，其他组件可以使用这些内容来生成实际配置对象。帮助程序组件的类型有两种：对象类型或不包含组件部分的另一个样本。

以下示例显示了样本的片段，该片段用于在 Citrix ADC 实例上创建具有监视器（lb-mon-comp）的负载平衡服务器。

```
parameters:
  -
    name: appname
    type: string
  -
    name: ips
    type: ipaddress[]
  -
    name: vip
    type: ipaddress

components:
  -
    name: help-comp
    type: cmtypes::server-ip-port-params
    repeat:
      repeat-list: $parameters.ips
      repeat-item: server-ip
    properties:
      ip: $server-ip
      port: 80
 -
    name: lb-mon-comp
    type: stlb::lb-mon
    properties:
```



```
26        lb-appname: $parameters.appname
27        lb-virtual-ip: $parameters.vip
28        lb-virtual-port: 80
29        lb-service-type: HTTP
30        svc-service-type: HTTP
31        svc-servers: $components.help-comp.properties
32  <!--NeedCopy-->
```

parameters 部分允许您输入应用程序的名称和负载平衡服务器的 IP 地址。在 lb-mon-comp 组件部分中，lb-mon 样本的 svc-servers 参数要求为对象列表，其中每项都有两个子参数：ip 和 port。

但是，此样本的 parameters 部分仅通过 $parameters.ips 接受服务器 IP。该样本假定所有服务器都在端口 80 上运行。要使用 lb-mon 样本创建负载平衡配置，必须将 $parameters.ips 传输到对象列表。这是通过使用帮助程序组件（上述示例中的 help-comp）来实现的。help-comp 组件的类型为 server-ip-port-params 样本。此样本没有任何组件。因此，它不会创建任何配置对象。help-comp 基于 $parameters.ips 创建重复列表，并为 $parameters.ips 的每项构造由 ip 和 port（设置为静态 80）组成的对象。因此，help-comp 将 IP 地址列表传输到对象列表，以后可以在 lb-mon-comp 中使用该对象列表来分配 svc-servers 属性。help-comp 的结果即分配给 lb-mon-comp 的 svc-servers 属性。

可选属性

April 23, 2021

在有些情况下，组件的一个属性从一个表达式接收其值，表达式可以是简单表达式（例如参数引用），也可以是较复杂的表达式。在组件中设置此属性值是可选的。可以选择仅当表达式返回实际值时设置该属性值，否则可以选择不设置此属性。

例如，假设要设置的其中一个属性是其类型为 ns::lbvserver 的组件的 lbmethod（负载平衡算法）。属性 lbmethod 的值取自用户提供的一个参数值，如下所示：

```
1  components
2    -
3        name: lbvserver_comp
4        type: ns::lbvserver
5        properties:
6          name: $parameters.lb-appname + "-lb"
7          servicetype: $parameters.lb-service-type
8          ipv46: $parameters.lb-virtual-ip
9          port: 80
10         lbmethod: $parameters.lb-advanced.algorithm
11 <!--NeedCopy-->
```


现在，考虑参数 **lb-**高级 **d.** 算法是一个可选参数。而且，如果用户没有为此参数提供值，因为该参数是可选的，则表达式 **$** 参数 **s.lb-**高级 **d.** 算法将计算为空值。因此，为 lbmethod 属性传递的值无效。为了避免这种情况，可以在属性名称后面添加后缀 “?” 将属性标注为可选，如下所示：

```
components
   -
     name: lbvserver_comp
     type: ns::lbvserver
     properties:
       name: $parameters.lb-appname + "-lb"
       servicetype: $parameters.lb-service-type
       ipv46: $parameters.lb-virtual-ip
       port: 80
       lbmethod?: $parameters.lb-advanced.algorithm
<!--NeedCopy-->
```

使用 “? “如果右侧的表达式计算为什么，则忽略该属性，在这种情况下，这将等同于定义如下的组件：

```
components
  -
    name: lbvserver_comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb-appname + "-lb"
      servicetype: $parameters.lb-service-type
      ipv46: $parameters.lb-virtual-ip
      port: 80
<!--NeedCopy-->
```

由于 **lbmethod** 是可选的，忽略它后，此组件仍是有效组件。请注意，如果在 lbmethod 的类型 “ns::lbvserver” 中定义了默认值，则 lbmethod 可能采用其默认值。

属性-默认源构造

April 23, 2021

properties-default-sources 构造类似于 parameters-default-sources 构造。parameters-default-sources 构造允许在样本中重用（来自其他样本的）现有参数，properties-default-sources 构造允许用户根据现有来源指定组件的属性。

组件的属性可以分布在样本的多个部分中。例如，属性可能来自对象参数、返回对象的替换、其他组件的属性或其他组件的输出。在此类情况下，您需要在组件的定义中重新定义在样本的其他部分中出现的属性。显然，这是多余的，且可

能会导致出错。为了解决此问题，可以使用 properties-default-sources 构造。properties-default-sources 构造是一个列表，其中每项均标识组件的一些属性的一个来源。

例如，假定一个创建 lbvserver 配置的组件。此组件应按以下所示定义 lbvserver 的属性。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties:
      name: $parameters.lb.name
      ipv46: $parameters.lb.ipv46
      port: $parameters.lb.port
      servicetype: $parameters.lb.servicetype
      lbmethod: $parameters.lb.lbmethod
<!--NeedCopy-->
```

在上述示例中，看到 components 部分中定义的所有属性的值均取自 $parameters.lb 对象。尽管它们取自一个来源，但在样本中再次定义了属性。此外，如果向 $parameters.lb 对象添加与 lbvserver 的配置相关的新子参数，您需要更新 lb-comp 组件以添加与新子参数对应的新属性。

为了避免重新定义属性以及为了提取某个组件的所有相关属性而无需明确在 properties 部分中列出它们，可以使用 properties-default-sources 构造。上述示例可以编写如下。

```
parameters:
  -
    name: lb
    type: ns::lbvserver
components:
  -
    name: lb-comp
    type: ns::lbvserver
    properties-default-sources:
      - $parameters.lb
<!--NeedCopy-->
```

在上述示例中，通过使用 properties-default-sources 构造，减小了组件定义的规模，这样，您可以简明地定义组件。此外，每当组件的属性的来源更改时，更改会自动反映出来。例如，在 $parameters.lb 对象中添加新属性“persistencetype”时，由于 persistencetype 是 lbvserver 的属性，因此，默认情况下，此属性添加到 lb-comp 的配置。因此，properties-default-sources 构造提供了定义组件的动态接口，而无需担心组件的属性的来源发生的更改。

计算组件的属性

本节讨论如果在组件中使用 properties-default-sources 构造，如何提取属性。首先，样本编译器根据组件的类型（在上述示例中为 lbvserver）标识组件的属性列表。然后，编译器按这些属性的定义顺序（在组件的 properties-default-sources 部分中）从多个来源中提取它们。如果某个属性存在于多个来源中，则出现在最后一个来源中的该属性的优先级高于其他来源中的该属性。最后，可以在组件的 properties 部分中覆盖使用 properties-default-sources 构造提取的属性。请务必注意，components 部分的定义至少应有一个 properties-default-sources 部分或一个 properties 部分。可以有两者。

嵌套组件

April 23, 2021

通过在一个组件中嵌套另一个组件，嵌套的组件可以通过引用父组件创建的配置对象或上下文来创建其配置对象。嵌套的组件可以为父组件中创建的每个对象创建一个或多个对象。在一个组件中嵌套另一个组件并不表示创建的配置对象之间有任何关系。嵌套是一种简化组件的任务以在父组件的现有上下文中构造配置对象的方式。

示例：

```
components:
 -
  name: my-lbvserver-comp
  type: ns::lbvserver
   properties:
      name: $parameters.name + "-lb"
      servicetype: HTTP
      ipv46: $parameters.ip
      port: 80
      lbmethod: $parameters.lb-alg
      components:
        -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
            name: $parameters.name + "-svcgrp"
            servicetype: HTTP
         components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                name: $parent.parent.properties.name
                servicegroupname: $parent.properties.name
```



```
                    -
                      name: members-svcg-comp
                      type: ns::servicegroup_servicegroupmember_binding
                      repeat:
                        repeat-list: $parameters.svc-servers
                        repeat-item: srv
                      properties:
                        ip: $srv
                        port: str($parameters.svc-port)
                        servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

在此示例中，使用了多层嵌套。组件 my-lbvserver-comp 有一个名为 my-svcg-comp 的子组件。而且 my-svcg-comp 组件里面有两个子组件。my-svcg-comp 组件用于在 Citrix ADC 实例上创建服务组配置对象，方法是为内置 NITRO 资源类型“服务组”的属性提供值。“ my-svcg 组件的第一个子组件 lbvserver-svg-binding-comp 用于将其父组件创建的服务组绑定到父组件的父组件创建的负载平衡虚拟服务器 (lbvserver)。$parent 表示法（也称为父引用）用于引用父组件中的实体。第二个子组件 members-svcg-comp 用于将一组服务绑定到父组件创建的服务组。绑定是通过使用样本的重复构造迭代为参数 svc-servers 指定的一组服务来完成。有关重复构造的信息，请参阅 重复构造。

还可以在不使用组件嵌套的情况下创建相同配置对象。有关详细信息和示例，请参阅用于创建基本负载平衡配置的样本。

条件构造

April 23, 2021

可以使用 condition 构造使组件成为有条件的组件。condition 构造的值是求值结果为 true 或 false 的布尔表达式。如果条件为 true，则使用该组件构建其配置对象。如果条件为 false，则跳过该组件，不通过它创建配置对象。布尔表达式通常基于参数值。

示例：

```
components:
      -
        name: servicegroup-comp
        type: ns::servicegroup
        condition: $parameters.svc-server-ips
        properties:
              name: $parameters.name + "-svcgrp"
              servicetype: HTTP
<!--NeedCopy-->
```


在此示例中，如果用户为可选参数 svc-server-ips 指定一个值，则样本引擎将处理组件 servicegroup-comp。如果条件为 false，即如果用户没有为此参数提供值，则系统为此参数指定空值，且求值结果为 false，那么样本引擎将忽略此组件，且不创建服务组。

请注意，布尔表达式可以基于样本中支持的任何有效表达式（例如，另一个组件是否存在，或一个参数是否有特定值）。

以下示例在条件求值结果为 true 时构建 NITRO 类型 ns::systemfile 的配置对象。

示例：

```
1       components
2            -
3              name: pem_key_files
4              type: ns::systemfile
5              condition: "$components.der-certificate-files-comp or
      $components.pem-certificate-files-comp"
6              properties:
7                     filecontent: $certificate.keyfile.contents
8                     fileencoding: "BASE64"
9                     filelocation: "/nsconfig/ssl"
10                    filename: $certificate.keyfile.filename
11 <!--NeedCopy-->
```

在此示例中，条件是一个复杂的 “OR” 表达式，只有在样书中的其他两个组件已经处理（未跳过）时，才希望样书才创建此配置对象，从而在组件之间创建依赖关系。

重复构造

April 23, 2021

可以使用组件的重复构造来构建多个相同类型的配置对象。

在下面的示例中，**members-svcg-comp** 组件用于将一组服务绑定到父组件创建的服务组。为了创建将每个服务器绑定到服务组的配置对象，请使用重复构造来迭代为参数 **svc-servers** 指定的服务列表。在迭代过程中，组件为服务组中的每个服务（在重复项结构中称为 srv）创建一个类型为服务组服务组成员绑定的 NITRO 对象，并在每个 NITRO 中设置 **ip** 属性对象设置为相应服务的 IP 地址。

示例：

```
1  components:
2    -
3        name: my-lbvserver-comp
4        type: ns::lbvserver
5        properties:
6             name: $parameters.name + "-lb"
```



```
            servicetype: HTTP
            ipv46: $parameters.ip
            port: 80
            lbmethod: $parameters.lb-alg
          components:
                -
                  name: my-svcg-comp
                  type: ns::servicegroup
                  properties:
                       name: $parameters.name + "-svcgrp"
                       servicetype: HTTP
                  components:
                        -
                        name: lbvserver-svg-binding-comp
                        type: ns::lbvserver\servicegroup\binding
                        properties:
                              name: $parent.parent.properties.name
                              servicegroupname: $parent.properties.
    name
                        -
                        name: members-svcg-comp
                        type: ns::servicegroup\servicegroupmember\
    binding
                        repeat:
                          repeat-list: $parameters.svc-servers
                          repeat-item: srv
                        properties:
                               ip: $srv
                               port: $parameters.svc-port
                               servicegroupname: $parent.properties.
    name
<!--NeedCopy-->
```

重复项本身就是一个对象，重 复列表和重 复项是重复对象的属性。

- repeat-list 是必需属性，它标识组件迭代的列表。
- repeat-item 是可选的，用于为迭代中的当前项目指定友好名称。

如果未指定，可以使用表达式 **$repeat-item** 访问当前项目。上述示例中的最后一个组件还可以编写如下：

```
          -
          name: members-svcg-comp
          type: ns::servicegroup_servicegroupmember_binding
          repeat:
            repeat-list: $parameters.svc-servers
          properties:
```



```
                ip: $repeat-item
                port: $parameters.svc-port
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

除了能够引用当前项目白色遍历列表之外，还可以使用 重复索引引用列表中项目的当前索引。在以下示例中，重复索引用于基于当前索引计算端口号：

```
            name: services
            type: ns::service
            repeat:
               repeat-list: $parameters.app-services
               repeat-item: srv
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + repeat-index
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

与重复项结构类似，您可以指定不同的变量名称来引用迭代的当前索引。上述示例与以下示例等同：

```
    -
            name: services
            type: ns::service
            repeat:
               repeat-list: $parameters.app-services
               repeat-item: srv
               repeat-index: idx
            properties:
                ip: $parameters.app-ip
                port: $parameters.base-port + $idx
                servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

重复条件构造

April 23, 2021

在重复构造的每个迭代中都对 repeat-condition 构造求值，并由结果确定是在相应迭代中构建配置对象，还是移至下一个迭代。以下示例说明了 repeat-condition 构造的使用：

示例：


```
components
    -
       name: der-key-files-comp
       type: ns::systemfile
       repeat:
       repeat-list: $parameters.certificates
       repeat-item: certificate
         repeat-condition: $certificate.ssl-inform == DER
         properties:
          filecontent: base64($certificate.keyfile.contents)
          fileencoding: BASE64
          filelocation: /nsconfig/ssl
          filename: $certificate.keyfile.file
<!--NeedCopy-->
```

在此示例中，der-key-files-comp 组件迭代用户提供的所有证书，但仅构建与采用 DER 编码的证书对应的配置对象。在每个迭代中，都对 repeat-condition 表达式求值来测试证书编码是否属于类型 DER。如果不属于类型 DER，则不在当前迭代中构建配置对象，且迭代移至列表中的下一个证书。

嵌套重复

April 23, 2021

使用嵌套的重复构造时，根据组件的定义，一个组件中可以有多个重复构造。假定一个嵌套的重复有两个级别。对于外层列表（第一个 repeat-list）中的每个元素，您可以为内层列表（第二个 repeat-list）的所有元素创建一个重复列表。样本编译器最多支持三个嵌套的重复。每个重复级别都有与之关联的 repeat-item 和 repeat-index 属性。repeat-item 和 repeat-index 属性是可选的。此外，每个重复还可以指定 repeat-condition。

示例：

```
parameters:
  -
       name: vips
       type: ipaddress[]
  -
       name: vip-ports
       type: tcp-port[]
components:
  -
       name: lbvservers-comp
       type: ns::lbvserver
       repeat:
```



```
13          repeat-list: $parameters.vips
14          repeat-item: ip
15          repeat:
16               repeat-list: $parameters.vip-ports
17               repeat-item: port
18       properties:
19          name: str("lb-") + str($ip) + '-' + str($port)
20          servicetype: HTTP
21          ipv46: $ip
22          port: $port
23 <!--NeedCopy-->
```

在上述示例中，对于 $parameters.vips 中的每项，均对 $parameters.vip-ports 的所有项进行迭代。因此，对于 $parameters.vips 中指定的每个 IP 地址，均为 $parameters.vip-ports 中指定的所有端口创建 lbvserver 配置对象。properties 部分定义对象的名称，并以 “lb” 作为 IP 地址和端口的组合的前缀。因此，对于每个迭代，$ip + $port 均定义 IP 地址和端口号的唯一组合。

如果未提供 repeat-item 属性，则编译器将为其生成默认值。repeat-item 的默认值为：分别对应每个重复级别的 $repeat-item、$repeat-item-1、$repeat-item-2。同样，如果未提供 repeat-index 属性，则编译器将为其生成默认值。repeat-index 的默认值为：分别对应每个重复级别的 $repeat-index、$repeat-index-1 和 $repeat-index-2。

以下示例说明了嵌套的重复对象中没有 repeat-item 和 repeat-index 属性时的命名约定。

示例：

```
1  components:
2  -
3       name: lbvservers-comp
4       type: ns::lbvserver
5       repeat:
6           repeat-list: $parameters.vips
7           repeat:
8              repeat-list: $parameters.vip-ports
9       properties:
10         name: str("lb-") + str($repeat-item) + '-' + str($repeat-item
       -1)
11          servicetype: HTTP
12          ipv46: $repeat-item
13          port: $repeat-item-1
14 <!--NeedCopy-->
```


输出

April 23, 2021

在 outputs 部分，指定样本成功完成创建所有配置对象后向其用户呈现的内容。样书的 outputs 部分是可选的。样书不必返回输出。但是，如果将一些内部组件作为输出返回，导入它的任何样本就可以有更大的灵活性，这在创建复合样本时可以看到。

下表介绍了 outputs 部分中使用的属性。

属性	说明	强制
名称	与您要呈现的配置对象对应的输出的名称。	是
description	描述输出的文本字符串。	否
value	此属性指定如何提取样本返回的值。	是

示例：

```
outputs:
 -
   name: lbvserver
   description: LBVServer component
   value: $components.my-lbvserver-comp
 -
   name: svc-grp
     description: ServiceGroup name
     value: $components.my-svcg.properties.name
<!--NeedCopy-->
```

在此示例中，呈现将由样本创建的 **lbvserver** 组件和服务组名称。名为 **lbvserver** 的输出的值是组件 **my-lbvserver-comp**。同样，名为 **svc-grp** 的输出的值是组件 **my-svcg** 创建的服务组的名称。

参数引用

April 23, 2021

在组件构造中，通过使用符号来引用参数部分中定义 $parameters.<parametername> 的参数。如

果 <parametername> 本身包含参数（当类型是对象时）$parameters.<parametername>.<sub-parametername>，则必须使用符号等。

示例：

```
parameters:
  -
    name: name
    label: Name
    type: string
    required: true
     -
      name: vip
      label: Virtual IP and Port
      type: object
      required: true
      parameters:
        -
          name: ip
          label: Virtual IP
          description: The Virtual IP Address
          type: ipaddress
          required: true
            -
              name: port
              label: The Virtual Port
              description: The TCP port for the Virtual IP
              type: tcp-port
              default: 80
components:
  -
    name: my-lbvserver-comp
    type: ns::lbvserver
    properties:
       name: $parameters.name
       servicetype: HTTP
       ipv46: $parameters.vip.ip
       port: $parameters.vip.port
<!--NeedCopy-->
```

父引用

April 23, 2021

如果您正在使用 嵌套组件，则可以使用 $ parent 符号来引用父组件。如果父组件使用重复构造构建多个配置对象，且在每个迭代中，子组件构建其他配置对象，那么 $parent 表示法始终引用父组件的当前迭代。例如，$parent.properties.name 引用父组件的当前迭代中构建的配置对象的 name 属性。

示例：

```
components:
 -
   name: my-lbvserver-comp
   type: ns::lbvserver
   properties:
     name: $parameters.name + "-lb"
     servicetype: HTTP
     ipv46: $parameters.ip
     port: 80
     lbmethod: $parameters.lb-alg
     components:
       -
         name: my-svcg-comp
         type: ns::servicegroup
         properties:
           name: $parameters.name + "-svcgrp"
           servicetype: HTTP
           components:
            -
              name: lbvserver-svg-binding-comp
              type: ns::lbvserver_servicegroup_binding
              properties:
                 name: $parent.parent.properties.name
                 servicegroupname: $parent.properties.name
                   -
                     name: members-svcg-comp
                     type: ns::servicegroup_servicegroupmember_binding
                     repeat: $parameters.svc-servers
                     repeat-item: srv
                     properties:
                       ip: $srv
                       port: str($parameters.svc-port)
                       servicegroupname: $parent.properties.name
<!--NeedCopy-->
```

还可以通过访问父组件的父组件的属性，在组件的层次结构中一直向上导航到顶层组件。例如，组件 **lbvserver-svg-binding-comp** 的属性名称通过使用 **$parent .parent** 表示法从其父代的父代（**my-lbvserver-comp** 组件）的属性名称中获取其值。

元件参考

April 23, 2021

在组件结构中，通过使用组件引用样书中的顶级组件 **$components.<componentname>** 符号。如果顶层组件中有嵌套的组件，则使用 **$components.<componentname>.components.<component-name>** 表示法来引用它们，依此类推。

示例：

```
components:
 -
    name: my-lbvserver-comp
     type: ns::lbvserver
     properties:
           name: $parameters.name + "-lb"
           servicetype: HTTP
           ipv46: $parameters.ip
           port: 80
           lbmethod: $parameters.lb-alg
  -
     name: my-svcg-comp
     type: ns::servicegroup
     properties:
          name: $parameters.name + "-svcgrp"
          servicetype: HTTP
 -
     name: members-svcg-comp
     type: ns::servicegroup_servicegroupmember_binding
     repeat: $parameters.svc-servers
     repeat-item: srv
     properties:
        ip: $srv
          port: str($parameters.svc-port)
          servicegroupname: $components.my-svcg-comp.properties.name
 -
     name: lbvserver-svg-binding-comp
     type: ns::lbvserver_servicegroup_binding
     properties:
            name: $components.my-lbvserver-comp.properties.name
            servicegroupname: $components.my-svcg-comp.properties.name
<!--NeedCopy-->
```

在此示例中，必须先构建组件 **my-svcg-comp** 和 **my-lbvserver-comp**，再构建最后一个组件 **lbvserver-**

svg-binding-comp，因为在这最后一个组件中有对这些组件的引用。这些引用通过使用由 **$components.<componentname>** 表示的 components 引用来提供。

替换引用

April 23, 2021

在“组件”部分或“操作”部分中，通过使用 **$substitutions.<substitution-name>** 符号来引用替代部分中定义的替代。例如，**$substitutions.http-port**。

如果替换是映射，则可以将映射中的元素称为 **$substitutions.<substitutions-name>[<map-key>]**。例如 **$substitutions.protocol-map[$parameters.port]**。

变量引用

April 23, 2021

在 components 中使用 repeat 和 repeat-item 构造来构建多个配置对象时，可以为 repeat-item 构造指定变量名称。然后，可以使用符号在该组件的属性或子组件中引用此变量 **$\<varname\>**。注意，在组件中使用重复构造时没有使用 repeat-item 构造，可以使用名为 $repeat-item 的默认变量来访问迭代项。

示例：

```
components:
  -
    name: server-members-comp
    type: ns::server
    condition: $parameters.svc-server-domain-names
    repeat: $parameters.svc-server-domain-names
    repeat-item: server-name
    properties:
      name: $server-name + "-server"
      domain: $server-name
    components:
      -
         name: service-members-comp
         type: ns::service
         properties:
           name: $server-name + "-service"
           servername: $parent.properties.name
           servicetype: $parameters.svc-service-type
           port: $parameters.svc-server-port
```



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

在上面的示例中，为 repeat-item 构造指定了变量名称 server-name。此变量名称在同一组件的属性以及子组件中都引用 **$\<varname\>**。

操作

April 23, 2021

操作是样本中的一个可选部分。在本节中，您可以配置 Citrix Application Delivery Management (ADM) 分析，以收集有关所有或部分流量事务的 AppFlow 记录。使用样本在 Citrix ADC 实例上创建的虚拟服务器处理这些流量事务。在本节中，您还可以将 Citrix ADM 配置为在虚拟服务器上满足某些流量条件时触发警报。

您可以通过样本配置 Citrix ADM，从以下列出的各种 Citrix ADM 见解收集流量统计信息：

- Web Insight
- Security Insight
- HDX Insight
- Citrix Gateway 洞察。

支持的虚拟服务器包括负载平衡、内容交换和 VPN 虚拟服务器。

启用 Web Insight 和 Security Insight 或其中一个功能，以便在负载平衡或内容交换虚拟服务器上进行分析。但是，对于 VPN 虚拟服务器，您必须同时启用 HDX Insight 和 Citrix Gateway 智能分析或其中一个。

通过样书在 Citrix ADC 实例上启用的任何 Citrix ADM Insight 都使用 IPFIX 协议 (AppFlow) 将实例中的数据发送到 Citrix ADC。

此外，启用 Web Insight 时，将在负载平衡和内容交换虚拟服务器上启用客户端测量。启用客户端测量后，ADM 通过 HTML 注入捕获 HTML 页面的加载时间和渲染时间指标。使用这些指标，管理员可以识别 L7 延迟问题。

示例 **1**：

以下示例说明如何在样书中编写操作部分，以便在 VPN 虚拟服务器上同时启用 HDX Insight 能分析和 Citrix Gateway 智能分析：

```
name: simple-vpn-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable hdxinsight and gatewayinsight on
   a VPN vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
```



```
    version: "10.5"
    prefix: ns
components:
    -
        name: vpnvserver-comp
        type: ns::vpnvserver
        properties:
            name: str("vpn-") + str($current-target.ip)
            servicetype: SSL
            ipv46: 1.1.21.37
            port: 443
operations:
    analytics:
        -
            name: comp-ops
            properties:
                target: $components.vpnvserver-comp
                filter: "true"
                insights:
                  -
                  type: hdxinsight**
                   -
                     type: gatewayinsight
outputs:
  -
    name: myvpns
    value: $components.vpnvserver-comp
<!--NeedCopy-->
```

示例 **2**:

以下示例演示如何在样本中编写操作部分，以便在负载平衡虚拟服务器上同时启用 Web Insight 和 Security Insight:

```
name: simple-lb-ops
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
description: Test StyleBook to enable webinsight and securityinsight on
    LB vserver
import-stylebooks:
  -
    namespace: netscaler.nitro.config
    version: "10.5"
    prefix: ns
components:
```



```
12      -
13          name: lbvserver-comp
14          type: ns::lbvserver
15          properties:
16              name: str("lb-") + str($current-target.ip)
17              servicetype: HTTP
18              ipv46: 1.1.21.37
19              port: 80
20  operations:
21      analytics:
22          -
23              name: comp-ops
24              properties:
25                  target: $components.lbvserver-comp
26                  filter: "true"
27                   insights:
28                   -
29                    type: webinsight
30                     -
31                    type: securityinsight
32  outputs:
33    -
34      name: mylbs
35      value: $components.lbvserver-comp
36  <!--NeedCopy-->
```

分析

April 23, 2021

operations 部分的 analytics 子部分的结构与 components 部分类似。分析部分中的每个元素都用于为样书创建的一个或多个虚拟服务器配置 Citrix ADM 分析功能。

analytics 部分中的元素具有以下属性：

属性	说明	强制
名称	analytics 元素的名称。	是
description	说明此元素是什么的文本字符串。	否
condition	布尔表达式。此 condition 求值结果为 false 时，将跳过整个 analytics 元素。	否

属性	说明	强制
重复	迭代列表。	否
repeat-condition	布尔表达式。如果该表达式的求值结果为 false，则将跳过当前迭代。	否
repeat-item	当前迭代中项目的名称。	否
repeat-index	当前迭代的索引值的名称。	否
properties	analytics 的属性列表。	是
target	列表中的其中一个属性。目标表达式是在 Citrix ADC 上配置的虚拟服务器的名称，将为其收集分析。	是
filter	列表中的其中一个属性。此属性的值是 Citrix ADC 高级策略表达式，用于筛选要为其收集分析的虚拟服务器上的请求。默认情况下，收集通过虚拟服务器的所有通信的分析数据。	否

示例：

```
operations:

  analytics:

    -

    name: lbvserver-ops-comp

    properties:

    target: $components-basic-lb-comp.outputs.lbvserver-name

    filter: HTTP.REQ.URL.CONTAINS("catalog")
<!--NeedCopy-->
```

分析部分中的每个属性用于指示 Citrix ADM 分析功能配置 Citrix ADC 实例，以便在由目标属性标识的虚拟服务器上收集应用程序流记录。

警报

April 23, 2021

operations 部分的 alarms 子部分的结构与 analytics 子部分类似，属性与 analytics 子部分相同。唯一的区别是 properties 属性。有关所有属性（属性属性除外）的列表，请参阅 分析。

alarms 子部分中具有以下属性：

属性	说明	强制
target	计算为虚拟服务器名称的表达式，该表达式在 Citrix ADC 上配置，并为其配置了警报。	是
email-profile	在 Citrix ADM Analytics 功能中定义的电子邮件配置文件的名称，其中包含要在触发警报时通知的电子邮件地址列表。	否（必须定义 email-profile 或 sms-profile）
sms-profile	在 Citrix ADM Analytics 功能中定义的 SMS 配置文件的名称，该配置文件包含要在触发警报时通知的调用号码列表。	否（必须定义 email-profile 或 sms-profile）
rules	定义将会为 target 属性定义的虚拟服务器触发警报的条件的规则列表。	是
metric	规则的属性。要跟踪与 Citrix ADC 虚拟服务器相关的度量的名称。	是
operator	规则的属性。运算符用于将指标与值比较。有效运算符为 “greaterthan” 和 “lessthan”。	是
value	规则的属性。通过使用运算符将指标与其比较的阈值。如果指标值超过此阈值，则触发关联的警报。	是
period-unit	规则的属性。满足警报规则时向用户发出警报的频率。其值可以是天、小时或周。这表示，如果满足规则，则每个 period-unit 发送一次警报（例如，一天一次）。	是

下表提供了与 Citrix ADC 虚拟服务器相关的跟踪度量的列表。

Counters（计数器）| 说明 | 详细解除 |Citrix ADM 计算
|—|—|—|—|
| 对于 VPN 虚拟服务器：|
total_requests|VPN 会话启动总数 | 在用户指定的时间间隔内在此 VPN 虚拟服务器上启动的活动会话总数。| 单调递增的计数器，在每次新会话启动时递增 |
app_count	VPN 应用程序启动计数	在用户指定的时间间隔内在此 VPN 虚拟服务器上启动的唯一 VPN 应用程序总数。	单调递增的计数器，基于每次新应用程序启动
app_launch_duration	VPN 应用程序启动持续时间	启动应用程序所用平均时间（以毫秒为单位）	基于在此 VPN 虚拟服务器上启动的所有 VPN 应用程序的启动持续时间计算得出的平均值
其他虚拟服务器（CS、LB、身份验证、GSLB）	
Total_Request| 请求数	请求数	自上次设备重新启动以来或创建虚拟服务器以最近为准的虚拟服务器上的客户端请求数。| 单调递增计数器，每次向此虚拟服务器发出新请求时递增。|
总字节	字节	在指定时间间隔内从虚拟服务器传输到 Citrix ADM 的总字节数。	单调增加计数器以考虑此虚拟服务器提供的总字节数。
应用程序 _ 响应 _ 时间	响应时间	虚拟服务器的平均响应时间。	此虚拟服务器自设备上次重新启动（或创建虚拟服务器）以来收到的所有请求的响应时间的平均值（以最后者为准）。

样本中的 alarms 部分示例：

```
operations:
alarms:
 -
  name:lbvserver_alarm
  properties:
  target: $outputs.lbvserver
  email-profile: $parameters.emailprofile
  sms-profile: "NetScalerSMS"
     rules:
      -
        metric: "total_requests"
        operator: "greaterthan"
        value: 25
        period-unit: weekly
        -
          metric: "total_bytes"
          operator: "lessthan"
          value: 1024
          period-unit: day

<!--NeedCopy-->
```


表达式

April 23, 2021

样书最强大的功能之一是使用表达式。可以在各种方案中使用样本表达式来计算动态值。以下示例是将参数值与文字字符串连接的表达式。

示例：

```
$parameters.appname + "-mon"
<!--NeedCopy-->
```

此表达式检索名为 appname 的参数，并将其与字符串连接 -mon。

支持以下类型的表达式：

算术表达式

- 添加 (+)
- Subtraction (-)
- 乘法 (*)
- 司 (/)
- 模数 (%)

示例：

- 添加两个数字：$parameters.a + $parameters.b
- 乘以两个数字：$parameters.a * 10
- 在一个数字除以另一个数字后查找剩余数字：

15%10 5 中的结果

字符串表达

- 连接两个字符串 (+)

示例：

连接两个字符串：str(“app-“) + $parameters.appname

列出表达式

合并两个列表 (+)

示例：

- 连接两个列表：$parameters.external-servers + $parameters.internal-servers
- 如果 `$parameters.ports-1` 为 [80, 81]，`$parameters.port-2` 为 [81, 82]，则 `$parameters.ports-1 + $parameters.ports-2` 将显示为列表 [80, 81, 81, 82]。

关系表达式

- **==**：测试两个操作数是否相等，如果两个操作数相等则返回 true，否则返回 false。
- **!=**：测试两个操作数是否不同，如果两个操作数不同，则返回 true，否则返回 false。
- **>**：如果第一个操作数大于第二个操作数，则返回 true，否则返回 false。
- **>=**：如果第一个操作数大于或等于第二个操作数，则返回 true，否则返回 false。
- **<**：如果第一个操作数小于第二个操作数，则返回 true，否则返回 false。
- **<=**：如果第一个操作数小于或等于第二个操作数，则返回 true，否则返回 false。

示例：

- 使用平等运算符：`$parameters.name = = "abcd"`
- 不等式运算符的使用：`$parameters.name != "default"`
- 其他关系运算符示例
  - 10 > 9
  - 10 >= 10
  - 0 < 9
  - 10 <= 9
  - 10 == 10
  - 10 != 1

逻辑表达式-布尔值

- 和：逻辑的‘和’运算符。如果两个操作数为 true，则结果为 true，否则为 false。
- 或者：逻辑的‘或’运算符。如果其中一个操作数为 true，则结果为 true，否则为 false。
- 不：一元运算符。如果操作数为 true，则结果为 false，而相反。
- 在: 测试第一个参数是否为第二个参数的子字符串
- 在：测试项目是否为列表的一部分

> 注意
>
> 您可以将字符串转换为数字并将数字转换为字符串的类型转换表达式。同样，您可以将 `tcp-port` 转换为数字，IP 地址可以转换为字符串。
>
> 在任何运算符之前和之后使用分隔符。可以使用以下分隔符：

> - 在运算符之前：space、tab、comma、(、)、[、]
> - 在运算符之后：space、tab、(、[
>
> 例如：
>
> - abc + def
> - 100 % 10
> - 10 > 9

逐字字符串表达式

当字符串中的特殊字符必须采用文字形式时，可以使用逐字字符串。这些字符串可以包含转义字符、反斜杠、引号、括号、空格、括号等。在逐字字符串中，特殊角色的通常解释被跳过。字符串中的所有字符都以其文字形式保留。

在样书中，您可以使用逐字字符串将 Citrix ADC 策略表达式包含在其文本形式中。策略表达式通常包含特殊字符。如果没有逐字字符串，你必须通过将字符串分成子字符串来转义特殊字符。

要创建逐字字符串，请将字符串封装在特殊字符之间，如下所示：

```
~{
 string }
 ~
<!--NeedCopy-->
```

您可以在样书的任何位置使用逐字字符串。

> 注意请
>
> 勿在输入字符串中使用字符 } ~ 的序列，因为此序列表示逐字字符串的结尾。

示例：

```
 ~{
 HTTP.REQ.COOKIE.VALUE("jsessionid") ALT HTTP.REQ.URL.BEFORE_STR("=").
    AFTER_STR(";jsessionid=") ALT HTTP.REQ.URL.AFTER_STR(";jsessionid="
    ) }
 ~
<!--NeedCopy-->
```

目标表达式

在样书定义中，您可以使用 $current-target 表达式来引用当前目标 ADC 实例。要特别引用目标 ADC 实例的 IP 地址，请按如下方式使用此表达式：

```
$current-target.ip
```



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

示例:

```
components:
 -
  name: lb-comp
  type: ns::lbvserver
  properties:
    name: $current-target.ip + "-lbvserver"
<!--NeedCopy-->
```

在此示例中，使用目标 ADC 实例的 IP 地址构造的 `lbvserver` 的名称。

表达式类型验证

StyleBook 引擎允许在编译时进行更强的类型检查，也就是说，编写样书时使用的表达式是在导入样书本身的过程中验证的，而不是在创建配置包时进行验证。

对参数、替换、组件、组件属性、组件输出、用户定义变量（repeat-item、repeat-index、替代函数的参数）等的所有引用都经过验证，以确定它们的存在和类型。

类型检查示例:

在以下示例中，`lbvserver` StyleBook 的端口属性的预期类型为 `tcp-port`。在 Citrix Application Delivery Management (ADM) 中，类型验证在编译时（导入时）进行。编译器发现该字符串并且 `tcp-port` 不兼容类型，因此，样书编译器显示错误，导入或迁移样书失败。

```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: str("80")
      servicetype: HTTP
<!--NeedCopy-->
```

要成功编译此样书，请在编译器中将以下内容声明为数字:

```
port: 80
```

标记无效表达式的示例:

在早期版本中，当将无效表达式分配给属性名称时，编译器未检测到无效表达式，并允许将样本导入 Citrix ADM。现在，如果将此样书导入 Citrix ADM，编译器将识别此类无效表达式并对其进行标记。因此，样书无法导入到 Citrix ADM。

在此示例中，分配给 lb-sg-binding-comp 组件中 name 属性的表达式为：$components.lbvserver-comp.properties.lbvservername。但是，组件 lbvserver-comp 中没有调用 lbvservername 的属性。在早期的 Citrix ADM 版本中，编译器将允许此表达式并成功导入该表达式。当用户要使用此样本创建配置包时，实际上会失败。但是现在，在导入过程中会识别此类错误，并且样本不会导入到 Citrix ADM。手动更正此类错误并导入样书。

```
Components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.lbvservername
      servicegroupname: $components.sg-comp.properties.servicegroupname
<!--NeedCopy-->
```

为列表建立索引

现在，可以直接为列表中的项目建立索引来访问它们：

表达式	说明
$components.test-lbs[0]	引用 test-lbs 组件中的第一个项目
$components.test-lbs[0].properties.p1	引用 test-lbs 组件中的第一个项目的属性 p1

`$components.lbcomps[0].outputs.servicegroups[1].properties.servicegroupname`	指 `servicegroups` 组件中第二个项目的属性 `servicegroupname`，它是 `lbcomps` 组件的第一项的输出

原位内插

April 27, 2021

现在可以替换字符串中使用样本表达式的部分。样书编译器对这些字符串表达式进行求值时，字符串中使用样书表达式的部分将替换为表达式的值。要在字符串中包括样书表达式，我们使用以下表示法：

"…%{…}%…"

其中，"%{" 和 "}%" 之间包括的字符构成样书表达式。这些表达式称为 "原位内插"。

例如，字符串 "lb-%{$parameters.appname}%-svc" 是包含原位内插样本表达式的字符串表达式。字符串表达式的值取决于内插表达式的值。假定为 **$parameters.appname** 分配了 app1。然后，字符串表达式的计算结果为 **lb-app1-svc**。这就允许不在字符串表达式中对值进行硬编码，而是根据用户定义的值求值。

原位内插的一个实际用例是在样本中参数化策略表达式。假设这样一个场景：您要编写一个策略表达式，用于检查 HTTP URL 是否包含特定的单词，例如 "jpeg"。

为此，您可以编写如下所示的策略表达式："HTTP.REQ.URL.CONTAINS(\"jpeg\")"。

现在，如果您要参数化 HTTP URL 中的对象，可以在样本中添加字符串参数，例如 $parameters.url-object。应基于此参数编写策略表达式。为此，应使用字符串连接来达到效果。该表达式类似如下：

str("HTTP.REQ.URL.CONTAINS(\"" + $parameters.url-object + "\")")

如果为 $parameter.url-object 分配 "csv"，则上述表达式的求值结果将为 "HTTP.REQ.URL.CONTAINS(\"csv\")"。但是，此表达式不易阅读。为了使此参数化形式易于阅读和理解，可以使用原位内插。

现在，包含原位内插的表达式为：

str("HTTP.REQ.URL.CONTAINS(%{quotewrap($parameters.url-object)}%)")

在上述表达式中，使用了一个在 $parameters.url-object 值两边添加内部引号的内插表达式。此表达式的结果与上述表达式相同，但它更加直观且更接近实际结果。

内插中允许的类型

您可以在内插中使用生成以下类型值的表达式：boolean、number、tcp-port、ipaddress 和 string。内插替换为结果时，生成的值会自动转换为字符串。

字符串表达式可以有 0、1 个或更多内插。在顺序内插中，字符串表达式的不同部分可以替换为不同的样本表达式。例如，如果 $parameters.appname 为 “app1” 且 $parameters.vip 为 “1.1.1.1”，字符串 lb-%{$parameters.appname}%-%{$parameters.vip}% 返回 “lb-app1-1.1.1.1”

字符串表达式还支持嵌套内插。即，内插表达式可以嵌套在另一个内插表达式中，以便一个表达式的值可以作为另一个表达式的输入。

例如，假定字符串 “%{lb-%{$parameters.port + 1}%}%”

如果 $parameters.port 为 80，内部字符串 **%{$parameters.port + 1}%** 将返回 lb-81。此处，此表达式嵌套在另一个内插表达式中。

下表介绍了不同类型的内插，并提供了示例和相应的结果。示例中使用的参数值为：

- $parameters.appname: “lb1”
- $parameters.vip: “1.1.1.1”
- $parameters.n1: 1
- $parameters.n2: 3

简单内插

表达式	结果
—	—
lb-%{$parameters.appname}%-def	lb-lb1-def

自动类型转换

表达式	结果
—	—
lb-%{1}%	lb-1
lb-%{$parameters.vip}%	lb-1.1.1.1
lb-%{true}%	lb-True

顺序内插

表达式	结果
—	—
%{$parameters.appname}%-%{str($parameters.appname)}%	lb1-lb1
lb-%{1}%-%{2}%	lb-1-2

嵌套内插

表达式	结果
—	—
%{abc-%{$parameters.n1 + 1}%}%	abc-2
str(“%{abc-%{$parameters.n1}%}%-%{$parameters.n2}%”)	bc-1-3

包含 **quotewrap** 的内插

表达式	结果
—	—
str(“%{quotewrap(abcd)}%”)	”abcd|
str(“%{quotewrap(https://)} %+HTTP.REQ.HOSTNAME+HTTP.REQ.URL")	”<https://"+HTTP.REQ.HOST NAME+HTTP.REQ.URL

内插中的转义字符

如果字符 “%{” 或 “}%” 是字符串的一部分，您必须提供 “\” 作为转义字符以便样书编译器不会将它们视为内插标记。

示例：

str(“%{\%{ + str($parameters.vip) + }\%}%”) returns “%{1.1.1.1}%” if $parameters.vip is 1.1.1.1

下表介绍了另外一些表达式及其结果：

类别	表达式	结果
—	—	—
转义内插	str(“%{str($parameters.n1) + }%}%”)	1}%
	lb-%{str($parameters.n1) + }%}%	lb-1}%
	”%{str($parameters.n1) + \”\}\%\”}%”	1}%

内置函数

April 23, 2021

样本中的表达式可以利用内置函数。

例如，您可以使用内置函数 `str()` 将数字转换为字符串。

```
str($parameters.order)
```


或者，你可以使用内置函数 **int**() 将字符串转换为整数。

```
int($parameters.priority)
```

下面是样本表达式中支持的内置函数列表以及这些函数的用法示例。

str()

str() 函数将输入参数转换为字符串值。

允许的参数类型：

- string
- number
- TCP-port
- **boolean**
- IP address

示例：

- "set-"+ str(10) 函数返回 "set-10"。
- str(10) 函数返回 10。
- str(1.1.1.1) 函数返回 1.1.1.1。
- str(T rue) 函数返回 "T rue"。
- str(ADM) 函数返回 "mas"。

int()

int() 函数接受字符串、数字、IP 地址或 tcpport 作为参数并返回一个整数。

示例：

- **int**("10") 函数返回 10。
- **int**(10) 函数返回 10。
- **int**(ip('0.0.4.1')) 函数返回 1025。

bool()

bool() 函数将任何类型作为参数。如果参数值为 **false**、空值或不存在，则此函数返回 **false**。

否则，它会返回 **true**。

示例：

- bool(**true**) 函数返回 **true**。
- bool(**false**) 函数返回 **false**。
- 如果 $parameters.a 为 **false**、空值或不存在，bool($parameters.a) 函数将返回 **false**。

len()

`len()` 函数将字符串或列表作为参数，并返回字符串中的字符数或列表中的项目数。

示例 **1**：

如果按以下所示定义 substitution：

```
items: ["123", "abc", "xyz"]
```

`len($substitutions.items)` 函数返回 3

示例 **2**：

`len("Citrix ADM")` 函数返回 10。

示例 **3**：

如果 `$parameters.vips` 有值 `['1.1.1.1', '1.1.1.2', '1.1.1.3']`，则 `len($parameters.vips)` 函数返回 3。

min()

`min()` 函数接受列表或一系列数字或 `tcp-ports` 作为参数，然后返回最小的项目。

包含一系列编号/**TCP** 端口的示例：

- `min(80, 100, 1000)` 函数返回 80。
- `min(-20, 100, 400)` 函数返回 -20。
- `min(-80, -20, -10)` 函数返回 -80。
- `min(0, 100, -400)` 函数返回 -400。

包含编号/**tcp** 端口列表的示例：

- 支持 `$parameters.ports` 是一个列表，`tcp-ports` 具有以下值：`[80, 81, 8080]`。

  `min($parameters.ports)` 函数返回 80。

max()

`max()` 函数接受列表或一系列数字或 `tcp-ports` 作为参数，然后返回最大的项目。

包含一系列编号/**TCP** 端口的示例：

- `max(80, 100, 1000)` 函数返回 1000。
- `max(-20, 100, 400)` 函数返回 400。
- `max(-80, -20, -10)` 函数返回 -10。
- `max(0, 100, -400)` 函数返回 100。

包含编号/**tcp** 端口列表的示例：

- 支持 `$parameters.ports` 是 `tcp-ports` 的列表，具有值：`[80, 81, 8080]`。

  `max($parameters.ports)` 函数返回 `8080`。

bin()

`bin()` 函数将数字作为参数，并返回一个以二进制格式表示数字的字符串。

表达式示例：

`bin(100)` 函数返回 `0b1100100`。

oct()

`oct()` 函数将数字作为参数，并返回一个字符串，该字符串以八进制格式表示该数字。

表达式示例：

`oct(100)` 函数返回 `0144`。

hex()

`hex()` 函数接受一个数字作为参数，并返回一个小写字符串，该字符串表示十六进制格式的数字。

表达式示例：

`hex(100)` 函数返回 `0x64`。

lower()

`lower()` 函数接受一个字符串作为参数，并以小写形式返回相同的字符串。

示例：

`lower("ADM")` 函数返回 `adm`。

upper()

`upper()` 函数接受一个字符串作为参数，并以大写形式返回相同的字符串。

示例：

`upper("Citrix ADM")` 函数返回 `CITRIX ADM`。

sum()

sum() 函数接受数字列表或 tcpports 作为参数并返回列表中数字的总和。

示例 **1**：

如果按如下方式定义替
代：替代：

```
list-of-numbers = [11, 22, 55]
```

sum($substitutions.list-of-numbers) 函数返回 88。

示例 **2**：

如果 $parameters.ports 是 [80, 81, 82]，则 sum($parameters.ports) 函数返回 243。

pow()

pow() 函数接受两个数字作为参数，并返回一个数字，该数字表示第一个参数提出到第二个幂的参数。

示例：

pow(3,2) 函数返回 9。

ip()

ip() 函数采用整数、字符串或 IP 地址作为参数，并根据输入值返回 IP 地址。

示例：

- 在 ip 函数中指定 IP 地址：

  ip(3.1.1.1) 函数返回 3.1.1.1。

- 在 ip 函数中指定一个字符串：

  ip('2.1.1.1') 函数返回 2.1.1.1

- 在 ip 函数中指定一个整数：

  - ip(12) 函数返回 0.0.0.12。
  - 当您在 ip 函数中将整数指定为字符串时，它会返回输入的等效 IP 地址。

    ip('1025') 函数返回 0.0.4.1。

  此函数还支持整数加减操作，并返回生成的 IP 地址。

  - 加法：ip(1025)+ ip(12) 函数返回 0.0.4.13。
  - 减法：ip('1025')- ip(12) 函数返回 0.0.3.245。
  - 合并加减：ip('1.1.1.1')+ ip('1.1.1.1')- ip(2) 返回 2.2.2.0。

base64.encode()

`base64.encode()` 函数接受一个字符串参数并返回 base64 编码的字符串。

示例：

`base64.encode("abcd")` 函数返回 `YWJjZA==`。

base64.decode()

`base64.decode` 函数将 base64 编码的字符串作为参数并返回解码的字符串。

示例：

`base64.decode("YWJjZA==")` 函数返回 `abcd`。

存在 ()

`exists()` 函数接受任何类型的参数并返回布尔值。如果输入有任何值，则返回值为 `True`。如果输入参数没有值（即没有值），返回值为 `False`。

假设 `$parameters.monitor` 是一个可选参数。如果在创建配置包时为此参数提供值，则存在 (`$parameters.monitor`) 函数返回 `True`。

否则，它会返回 `False`。

筛选器 ()

`filter()` 函数有两个参数。

参数 1：接收一个参数并返回布尔值的 substitution 函数。

参数 2：列表。

传递给第一个参数中的替代函数时，
该函数返回每个元素计算结果为 `True` 的原始列表的一个子集。

示例：

假定按如下所示定义了 substitution 函数。

substitutions:

```
x(a): $a != 81
```

如果输入值不等于 81，此函数返回 True。否则，它会返回 `False`。

假设 `$parameters.ports` 为 `[81, 80, 81, 89]`。

`filter($substitutions.x, $parameters.ports)` 通过从列表中删除 81 的所有实例返回 `[80, 89]`。

如果-然后-否则 ()

函数 `if-then-else()` 需要三个参数。

参数 1：布尔表达式

参数 2：任何表达式

参数 3：任何表达式（可选）

如果参数 1 中的表达式的计算结果为 `True`，则函数返回作为参数 2 提供的表达式的值。

否则，如果提供了参数 3，该函数返回参数 3 中的表达式的值。

如果未提供参数 3，则函数返回 `no`。

示例 **1**：

如果 `$parameters.servicetype` 有值 `HTTP`，则 `if-then-else($parameters.servicetype == HTTP, 80, 443)` 函数返回 `80`。否则，函数返回 `443`。

示例 **2**：

如果 `$parameters.servicetype` 有值 `HTTP`，`if-then-else($parameters.servicetype == HTTP, $parameters.hport, $parameters.sport)` 函数返回 `$parameters.hport` 的值。

否则，函数返回 `$parameters.sport` 的值。

示例 **3**：

如果 `$parameters.servicetype` 有值 `HTTP`，则 `if-then-else($parameters.servicetype == HTTP, 80)` 返回 `80`。

否则，该函数不返回任何值。

连接 ()

`join()` 函数有两个参数：

参数 1：数字、`tcp-ports`、字符串或 IP 地址列表

参数 2：分隔符字符串（可选）

此函数将作为参数 1 提供的列表中的元素连接到一个字符串中，其中每个元素由作为参数 2 提供的分隔符字符串分隔。如果未提供参数 2，则列表中的元素将作为一个字符串连接。

示例：

- `$parameters.ports` 是 `[81, 82, 83]`。
  - 使用分隔符参数：

    `join($parameters.ports, '-')` 函数返回 `81-82-83`。

- 没有分隔符参数：

  `join($parameters.ports)` 函数返回 818283。

split()

`split()` 函数根据指定的分隔符将输入字符串拆分为多个列表。如果未指定或空白 (`''`) 分隔符，则此函数将空格视为分隔符并将字符串拆分为列表。

示例**:**

- `split('Example_string_split', 's')` 函数返回 `['Example_','tring_','plit']`。
- `split('Example string split')` 函数返回 `['Example','string','split']`。
- `split('Example string split', '')` 函数返回 `['Example','string','split']`。
- `split('Example string')` 函数返回 `['Example','string']`。

  此函数将连续空格视为一个空间。

地图 ()

`map()` 函数需要两个参数；

参数 1：任何函数

参数 2：元素列表。

该函数返回一个列表，其中列表中的每个元素都是将 `map()` 函数（参数 1）应用于参数二中的相应元素的结果。

参数 1 中允许的函数：

- 采用一个参数的内置函数：

  `base64.encode, base64.decode, bin, bool, exists, hex, int, ip, len, lower, upper, oct, quotewrap, str, trim, upper, url.encode, url.decode`

- 至少接收一个参数的 substitution 函数。

示例：

假设 $parameters.nums 为 `[81, 82, 83]`。

- 使用内置函数 str 的 map

  `map(str, $parameters.nums)` 函数返回 `["81", "82", "83"]`

  map 函数的结果是字符串列表，其中的每个元素是对输入列表 ($parameters.nums) 中的对应元素应用 str 函数计算所得的字符串。

- 使用 substitution 函数的 map

- substitutions:

  ```
  add-10(port): $port + 10
  ```

- 表达式：

  `map($substitutions.add-10, $parameters.nums)` 函数返回数字列表：`[ 91, 92, 93 ]`

这个 map 函数的结果是一个数字列表，每个元素都是通过对输入列表（`$parameters.nums`）中的相应元素应用替代函数 `$substitutions.add-10` 来计算的。

报价包装 ()

`quotewrap()` 函数接受一个字符串作为参数，并在输入值之前和之后添加双引号字符后返回一个字符串。

示例：

`quotewrap("ADM")` 函数返回 `"mas"`

替换 ()

`replace()` 函数有三个参数：

参数 1：字符串

参数 2：字符串或列表

参数 3：字符串（可选）

该函数将参数一中出现的所有参数二替换为参数三。

如果未提供参数 3，则将从参数 1 中删除所有出现的参数 2（换句话说，用空字符串替换）。

将一个子字符串替换为另一个字符串：

- `replace('abcdef', 'def', 'xyz')` 函数返回 `abcxyz`。

  所有出现的 `def` 都将替换为 `xyz`。

- `replace('abcdefabc', 'def')` 返回 `abcabc`。

  由于没有第三个参数，`def` 将从结果字符串中删除。

指定要在字符串中替换的字符列表。

```
$parameters.spl_chars = ['@', '##', '!', '%']
```

此列表包含必须在输入字符串中替换的值。

`replace('An##example@to%replace!characters', $parameters.spl_chars, '_')` 函数返回 `An_example_to_replace_characters`。

输出字符串具有下划线 (_) 而不是 `$parameters.spl_chars` 列表中指定的字符。

修剪 ()

trim() 函数返回一个字符串，其中将从输入字符串中删除前导和尾随空格。

示例：

trim('abc ') 函数返回 abc。

截断 ()

truncate() 函数有两个参数：

参数 1：字符串

参数 2：数字

该函数返回参数一中的输入字符串截断为参数二中指定的长度的字符串。

示例：

truncate('Citrix ADM', 6) 返回 Citrix。

distinct()

distinct() 函数从列表输入中提取唯一项目。

示例：
如果 $parameters.input_list 是 ['ADM', 'ADC', 'VPX', 'ADC', 'ADM', 'CPX']，则 distinct($parameters.input_list) 函数返回 ['ADM', 'ADC', 'VPX', 'CPX']。

url.encode()

url.encode() 函数返回一个字符串，其中根据 RFC 3986 使用 ASCII 字符集转换字符串。

示例：

url.encode("a/b/c") 函数返回 a%2Fb%2Fc。

url.decode()

url.decode() 函数返回一个字符串，其中 URL 编码的参数根据 RFC 3986 解码为常规字符串。

示例：

url.decode("a%2Fb%2Fc") 函数返回 a/b/c。

is-ipv4()

`is-ipv4()` 函数将 IP 地址作为参数，如果 IP 地址为 IPv4 格式，则返回布尔值 `True`。

`is-ipv4(10.10.10.10)` 函数返回 `True`

is-ipv6()

该 `is-ipv6()` 函数将 IP 地址作为参数，`True` 如果 IP 地址为 IPv6 格式，则返回布尔值。

`is-ipv6(2001:DB8::)` 函数返回 `True`

startswith()

`startswith()` 函数确定字符串是否以给定的前缀开头。此函数需要两个强制的字符串参数。

```
startswith(str, sub_str)
```

当字符串 (`str`) 以子字符串 (`sub_str`) 开头时，此函数返回 `True`。

示例：

- `startswith('Citrix', 'Ci')` 函数返回 `True`。
- `startswith('Citrix', 'iC')` 函数返回 `False`
- `startswith('Citrix', 'Ab')` 函数返回 `False`

endswith()

`endswith()` 函数确定字符串是否以给定的后缀结尾。此函数需要两个强制的字符串参数。

```
endswith(str, sub_str)
```

当字符串 (`str`) 以子字符串 (`sub_str`) 结尾时，此函数返回 `True`。

示例：

- `endswith('Citrix', 'ix')` 函数返回 `True`。
- `endswith('Citrix', 'Ix')` 函数返回 `False`。
- `endswith('Citrix', 'ab')` 函数返回 `False`。

contains()

`contains()` 函数确定字符串是否包含给定的子字符串。此函数需要两个强制的字符串参数。

```
contains(str, sub_str)
```

当子字符串 (`sub_str`) 包含在字符串 `str`) 中的任何位置时，此函数返回 `True`。

示例：

- `contains('Citrix', 'tri')` 函数返回 `True`。
- `contains('Citrix', 'Ci')` 函数返回 `True`。
- `contains('Citrix', 'ti')` 函数返回 `False`

substring()

使用 `substring()` 函数从字符串中提取子字符串。

```
substring(str, start_index, end_index)
```

此函数需要两个强制参数和一个可选的整数参数。

- `str` （必填）
- `start_index` （必填）
- `end_index` (可选)

此函数返回位于指定索引位置之间的字符串 (`str`) 中的子字符串。如果不指定结束索引位置，函数会将子字符串从起始索引提取到字符串末尾。

> 注意
>
> 指定时 `end_index`，子字符串将排除 `end_index` 位置上的字符。

示例:

- `substring('Citrix', 2)` 函数返回 `trix`
- `substring('Citrix', 10)` 函数返回 (")

  在此示例中，函数返回一个空字符串，因为它的 `start_index` 位置无效。
- `substring('Citrix', 2, 4)` 函数返回 `tr`

  在此示例中，函数提取介于 2 到 4 个索引位置之间的字符。
- `substring('Citrix', -3)` 函数返回 `rix`

  如果要提取字符串末尾的字符，请为 `start_index` 参数指定负值。

  在此示例中，函数提取包含字符串中最后三个字符的子字符串。

依赖性检测

April 23, 2021

样本中的组件可以引用同一样本中的其他组件的属性或部分。组件本身是完整的块，它们的编写顺序可能与必须执行的顺序不同。样本编译器会检查组件的编写顺序，然后按逻辑顺序执行这些组件。

示例:


```
components:
  -
    name: lbvserver-comp
    type: ns::lbvserver
    properties:
      name: mylb
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
 -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
      name: $components.lbvserver-comp.properties.name
      servicegroupname: $components.sg-comp.properties.servicegroupname
-
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: HTTP
<!--NeedCopy-->
```

在上面的例子中，定义了三个组件- **lbvser-comp**，**lb-sg-**绑定**-**复合和 **sg-comp**。执行此样本时，先创建 lbvserver-comp。lb-sg-binding-comp 引用 lbvserver-comp 属性，但尽管它是样本中定义的第二个组件，但不能接下来创建它。这是因为 lb-sg-binding-comp 还依赖也要创建的 sg-comp。因此，编译器对组件重新排序以使组件的依赖项按组件的创建时间进行解析，然后执行此重新排序的组件列表。上述样本的执行顺序为：lbvserver-comp、sg-comp 和 lb-sg-binding-comp。

这样，样本的作者不必担心组件的正确顺序。组件可以按任何顺序显示。编译器根据组件相互引用的情况计算组件的正确执行顺序。请注意，此依赖项检测和重新排序也适用于 substitutions 和 outputs 部分。

循环依赖项

由于组件可能会引用其他组件，因此可能会在样本的定义中引入依赖项循环。例如，如果组件 A 引用组件 B 中定义的一个属性，而后者也引用组件 A 中定义的一个属性。这种依赖项称为循环依赖项。循环依赖项无法自动解析。样本的作者应该手动更新更正样本定义以消除此类循环依赖项。编译器能够识别循环依赖项（如果存在）并报告。

以下示例显示了组件的循环依赖项：

```
components:
  -
    name: lbvserver-comp
```



```
    type: ns::lbvserver
    properties:
      name: $components.lb-sg-binding-comp.properties.name
      ipv46: 10.102.190.15
      port: 80
      servicetype: HTTP
  -
    name: lb-sg-binding-comp
    type: ns::lbvserver_servicegroup_binding
    condition: $parameters.create-binding
    properties:
     name: mylb
      servicegroupname: $components.sg-comp.properties.servicegroupname
  -
    name: sg-comp
    type: ns::servicegroup
    properties:
      servicegroupname: mysg
      servicetype: $components.lbvserver-comp.properties.servicetype
<!--NeedCopy-->
```

** 在上面的例子中，有三个组成部分：**lbvser-comp、lb-sg-绑定-复合和 sg-comp。** 此处，在这些组件之间形成了依赖项循环，这无法自动解析。因此，无法执行此样本。样本编译器检测到此问题并阻止样本导入 Citrix ADM。

实例管理

April 23, 2021

实例是 Citrix Application Delivery Controller (ADC) 设备，您可以使用 Citrix Application Delivery Management (ADM) 管理、监视和故障排除。您必须将实例添加到 Citrix ADM 才能对其进行监视。可以在设置 Citrix ADM 或更高版本时添加实例。将实例添加到 Citrix ADM 后，系统会持续轮询这些实例，以收集以后可用于解决问题或作为报告数据的信息。

实例可以分组为静态组或私有 IP 块。当您想要运行特定任务（如配置作业等）时，静态实例组非常有用。私有 IP 块根据实例的地理位置对实例进行分组。

添加实例

您可以在首次设置 Citrix ADM 服务器时或以后添加实例。要添加实例，您必须指定每个 Citrix ADC 实例的主机名或 IP 地址，或指定 IP 地址范围。

要了解如何将实例添加到 Citrix ADM，请参阅 将实例添加到 Citrix ADM。

将实例添加到 Citrix ADM 服务器时，服务器会隐式地将自身添加为实例的陷阱目标，并收集实例的清单。要了解更多信息，请参阅Citrix ADM 如何发现实例。

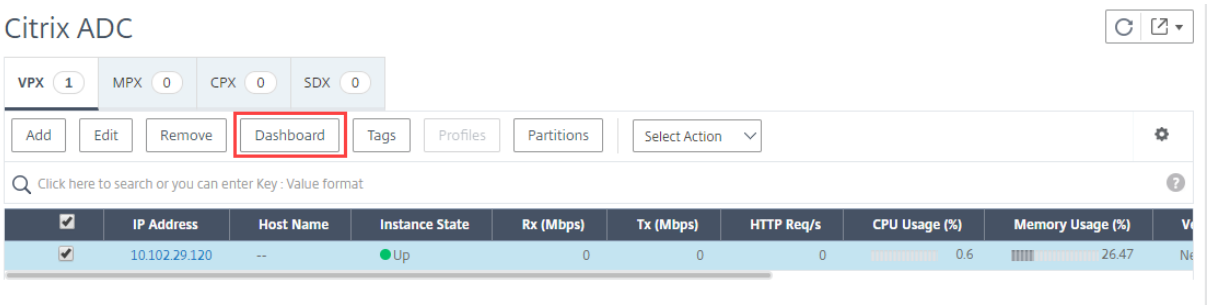
添加实例后，您可以通过导航到 “ 网络” > “ 仪表板” 并单击 “ 所有实例” 来将其删除。在 “实例” 页面上，选择要删除的实例，然后单击 删除”。

如何使用实例仪表板

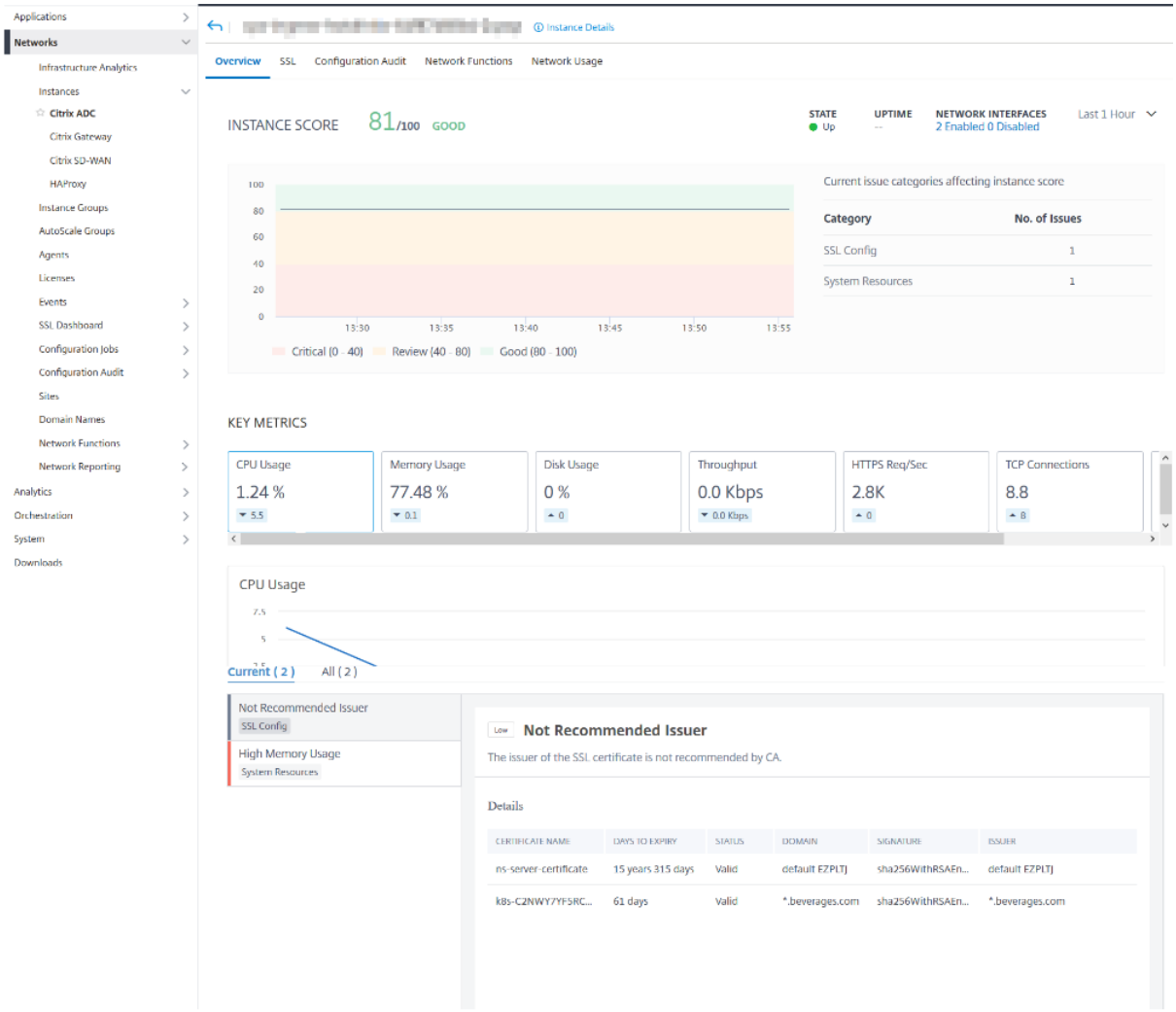
Citrix ADM 中的每个实例控制板以表格和图形格式显示所选实例的数据。轮询过程中从实例收集的数据将显示在控制板上。

默认情况下，每分钟轮询托管实例以进行数据收集。使用 NITRO 调用持续收集状态、每秒 HTTP 请求、CPU 使用率、内存使用率和吞吐量等统计信息。作为管理员，您可以在单个页面上查看所有这些收集的数据，确定实例中的问题，并立即采取措施来纠正这些问题。

要查看特定实例的仪表板，请导航到 “ 网络” > “ 实例”。从摘要中选择实例类型，然后选择要查看的实例，然后单击 仪表板。



下图概述了每个实例控制板上显示的各种数据：



- 概述。概述选项卡显示所选实例的 CPU 和内存使用情况。您还可以查看实例生成的事件和吞吐量数据。此处还显示特定于实例的信息，例如 IP 地址、其硬件和 LOM 版本、配置文件详细信息、序列号、联系人等。通过进一步向下滚动，您所选实例上可用的许可功能及其上配置的模式。

  有关详细信息，请参阅实例详细信息。

- **SSL** 控制板。您可以使用每个实例仪表板上的 SSL 选项卡查看或监视所选实例的 SSL 证书、SSL 虚拟服务器和 SSL 协议的详细信息。您可以点击图形中的“数字”以显示更多详细信息。

- 配置审核。您可以使用配置审核选项卡查看所选实例上发生的所有配置更改。仪表板上的 **NetScaler** 配置保存状态和 **NetScaler** 配置漂移图显示了有关保存的配置更改的高级别详细信息。

- 网络功能。使用网络功能控制板，您可以监视在所选 Citrix ADC 实例上配置的实体的状态。您可以查看显示客户端连接、吞吐量和服务器连接等数据的虚拟服务器的图形。

- 网络使用情况。您可以在网络使用情况选项卡上查看所选实例的网络性能数据。您可以显示一小时、一天、一周或一个月的报告。时间轴滑块功能可用于自定义正在生成的网络报告的持续时间。默认情况下，仅显示八个报告，但您可以单击屏幕右下角的“加号”图标来添加其他绩效报告。

监控全球分布的站点

April 23, 2021

作为网络管理员，您可能必须监视和管理部署在不同地理位置的网络实例。但是，在分布在地理位置上的数据中心管理网络实例时，要衡量网络的要求并不容易。

Citrix Application Delivery Management (ADM) 中的地理地图为您提供站点的图形表示，并按地理位置细分网络监控体验。通过 Geomap，您可以按位置呈现网络实例分布，并监视网络问题。

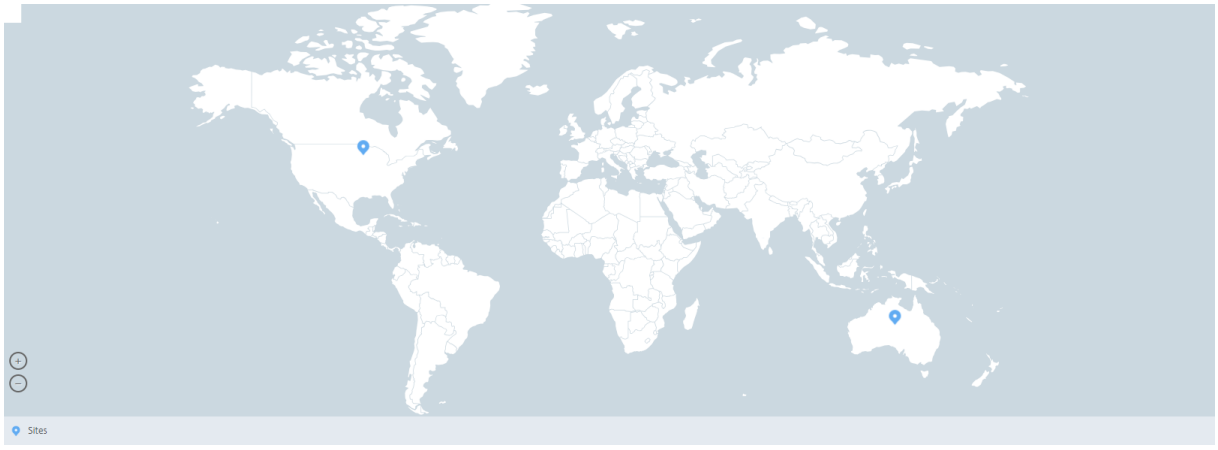
以下部分介绍如何监控 Citrix ADM 中的数据中心。

Citrix ADM 站点是特定地理位置中的 Citrix 应用程序 Delivery Controller (ADC) 实例的逻辑分组。例如，当一个站点被分配给 Amazon Web Services (AWS) 时，另一个站点可能被分配给 Azure™。还有一个网站托管在租户的前提。Citrix ADM 管理和监视连接到所有站点的所有 Citrix ADC 实例。您可以使用 Citrix ADM 监视和收集系统日志、AppFlow、SNMP 以及来自托管实例的任何此类数据。

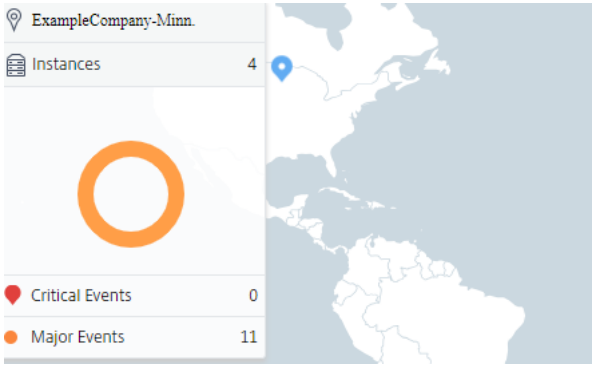
Citrix ADM 中的地理地图为您提供站点的图形表示。Geomaps 还会按地理分解您的网络监视体验。通过地理图，您可以按位置可视化您的网络实例分布并监视所有网络问题。您可以导航到 “ 网络” > “ 仪表板” 页面，以获得在世界地图上创建的站点的可视化表示。

用例

一家领先的移动运营商公司 Explecompany 正在依靠私人服务提供商托管他们的资源和应用程序。该公司已经有两个基地-一个位于美国明尼阿波利斯，另一个位于澳大利亚的爱丽斯泉。在此图中，您可以看到两个标记代表两个现有站点。

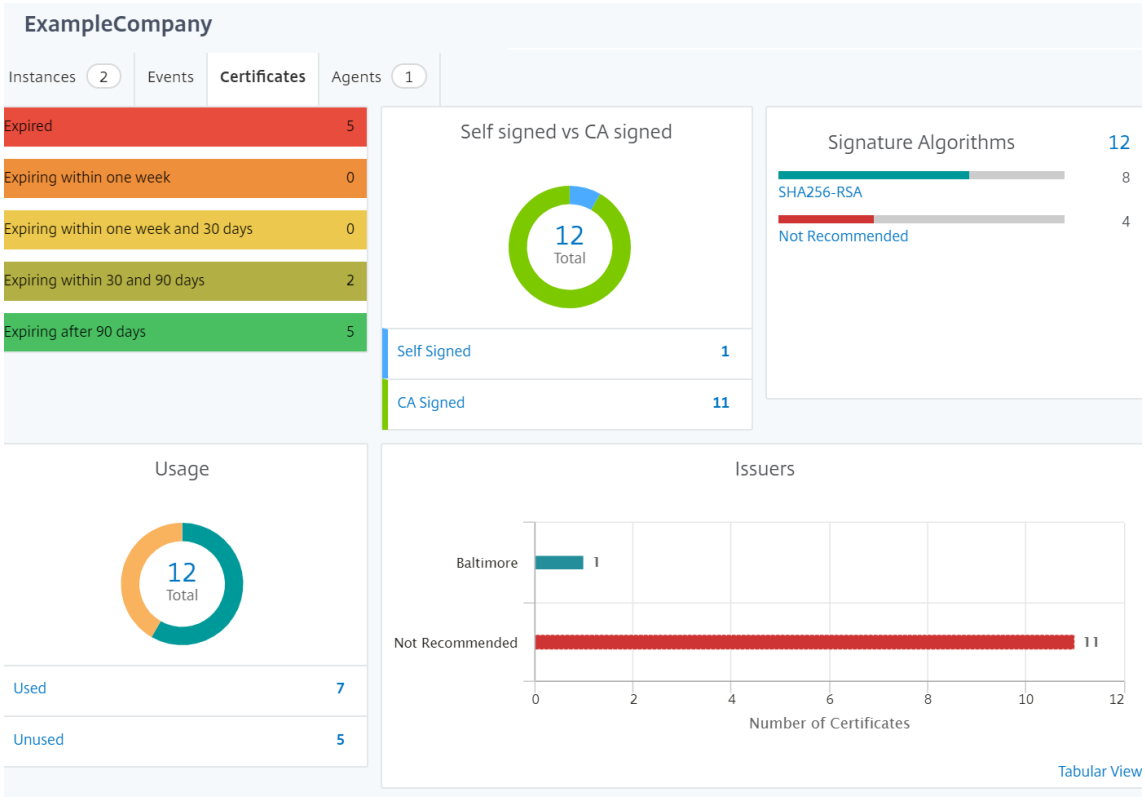


标记还会显示一个数字，显示每个站点中的应用程序数。您可以单击这些标记以了解有关每个站点的详细信息。



单击选项卡以查看详细信息：

- “实例选项卡：在此选项卡中查看以下内容：
  - 每个网络实例的 IP 地址
  - 实例的类型
  - 它们上的关键事件数
  - 在 Citrix ADC 实例上引发的重大事件和所有事件。
- 事件选项卡：查看在实例上引发的关键事件和重要事件的列表。
- “证书选项卡：在此选项卡中查看以下内容：
  - 所有实例的证书列表
  - 到期状态
  - 重要信息和正在使用的许多证书的前 10 个实例。
- **Agent** 选项卡：查看绑定实例的代理列表。



配置地理地图

考试组织决定在印度班加罗尔创建第三个网站。该公司希望通过将一些不太重要的内部 IT 应用程序卸载到班加罗尔办公室来测试云。该公司决定使用 AWS 云计算服务。

作为管理员，您必须首先创建站点，然后在 Citrix ADM 中添加 Citrix ADC 实例。您还必须将实例添加到站点、添加代理并将代理绑定到站点。然后，Citrix ADM 会识别 Citrix ADC 实例和代理所属的站点。

有关添加 Citrix ADC 实例的更多信息，请参阅添加实例。

要创建站点，请执行以下操作：

在 Citrix ADM 中添加实例之前创建站点。通过提供位置信息，您可以精确地定位站点。

导航到“网络”>“站点”，然后单击“添加”。

1. 在“创建站点”页中，指定以下信息：

   a) 站点类型：选择 数据中心。

   > 注意
   >
   > 站点可以作为主数据中心或分支。相应地选择。

   b) 类型：从列表中选择 AWS 作为云提供商。

> 注意相应
>
> 选中“ 使用现有 **VPC** 作为站点” 框。

c) 站点名称：键入站点的名称。

d) 城市：键入城市。

e) 邮政编码：键入邮政编码。

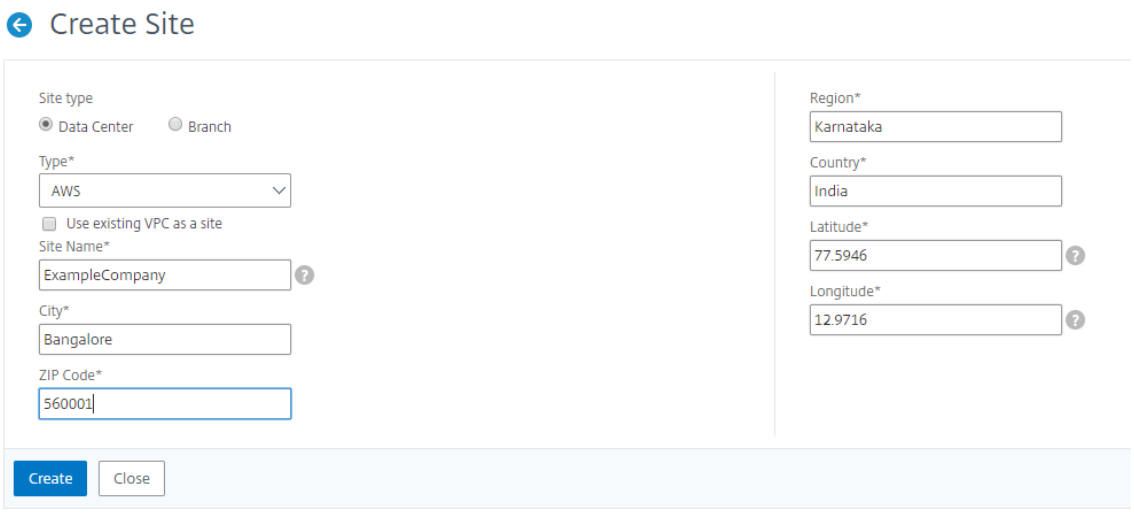
f) 区域：键入区域。

g) 国家/地区：键入国家/地区

h) 纬度：键入位置的纬度。

i) 经度：键入位置的经度。

2. 单击创建。

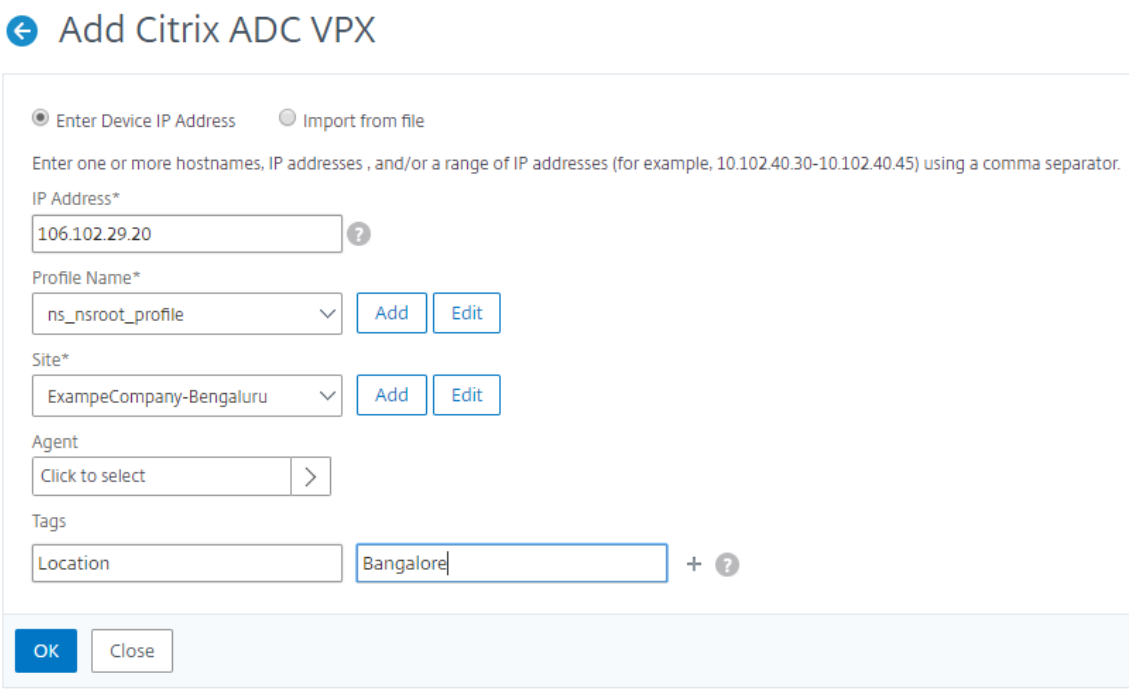


要添加实例并选择站点，请执行以下操作：

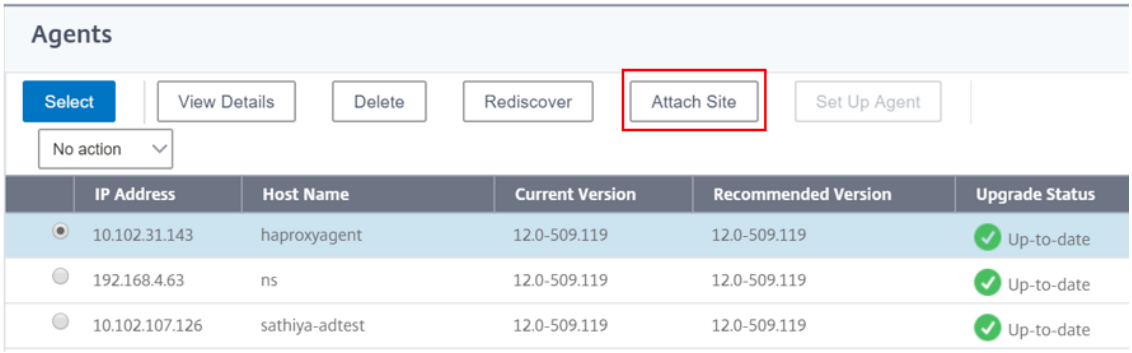
创建站点后，您必须在 Citrix ADM 中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

创建站点后，您必须在 Citrix ADM 中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

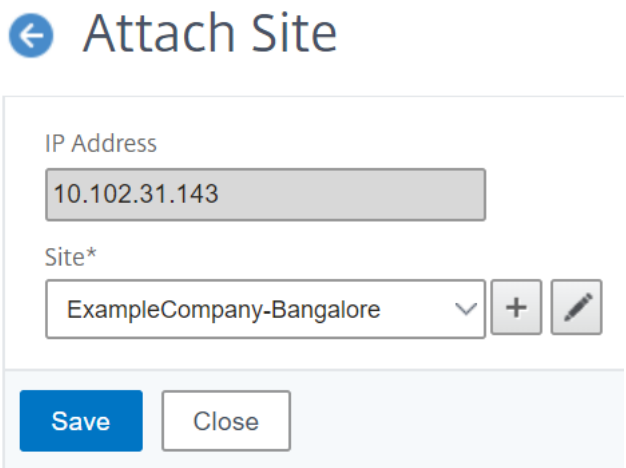
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例”。
2. 选择要创建的实例类型，然后单击 添加。
3. 在 添加 **Citrix ADC VPX** 页面上，键入 IP 地址并从列表中选择配置文件。
4. 从列表中选择站点。您可以单击 “ 站点” 字段旁边的 + 号来创建站点，或单击 “编辑” 图标以更改默认站点的详细信息。
5. 单击向右箭头，然后从显示的列表中选择座席。



6. 选择代理后，您必须将代理与站点关联。此步骤允许代理绑定到站点。选择代理，然后单击 “ 附加站点”。



1. 从列表中选择站点，然后单击 保存”。

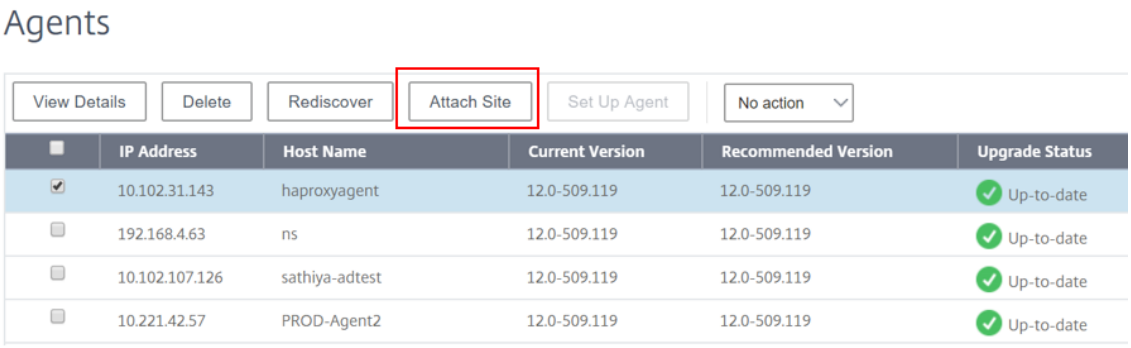


1. 单击确定。

您也可以通过导航到 “ 网络” > “代理” 将 代理附加到站点。

要将 **Citrix ADM** 代理与站点关联，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 代理”。
2. 选择代理，然后单击 “ 附加站点”。



1. 您可以关联网站并单击 保存”。

Citrix ADM 开始监视在班加罗尔站点中添加的 Citrix ADC 实例以及其他两个站点中的实例。

如何创建标签并分配给实例

April 23, 2021

现在，Citrix Application Delivery Management (ADM) 允许您将 Citrix 应用程序 Delivery Controller (ADC) 实例与标签相关联。标签是您可以分配给实例的关键字或单词术语。这些标签添加了有关实例的一些其他信息。标签可以被视为有助于描述实例的元数据。标签允许您根据这些特定关键字对实例进行分类和搜索。您还可以将多个标签分配给单个实例。

以下使用案例可帮助您了解实例的标记如何帮助您更好地监控实例。

- 使用案例 **1**：您可以创建标签来标识英国的所有实例。在这里，您可以创建一个标签，密钥为 “国家/地区”，值为 “UK”。“ 此标签可以帮助您搜索和监控英国境内的所有这些实例。
- 使用案例 **2**：您要搜索处于临时环境中的实例。在这里，您可以创建一个标签，其中密钥为 “目的”，值为 “Staging_NS。“ 此标记可帮助您将正在暂存环境中使用的所有实例与运行客户端请求的实例隔离开来。
- 使用案例 **3**：考虑一种情况，您想要查找位于英国 “Swindon” 区域并由您（David T）拥有的 Citrix ADC 实例列表。您可以为所有这些要求创建标签，然后将其分配给满足这些条件的所有实例。

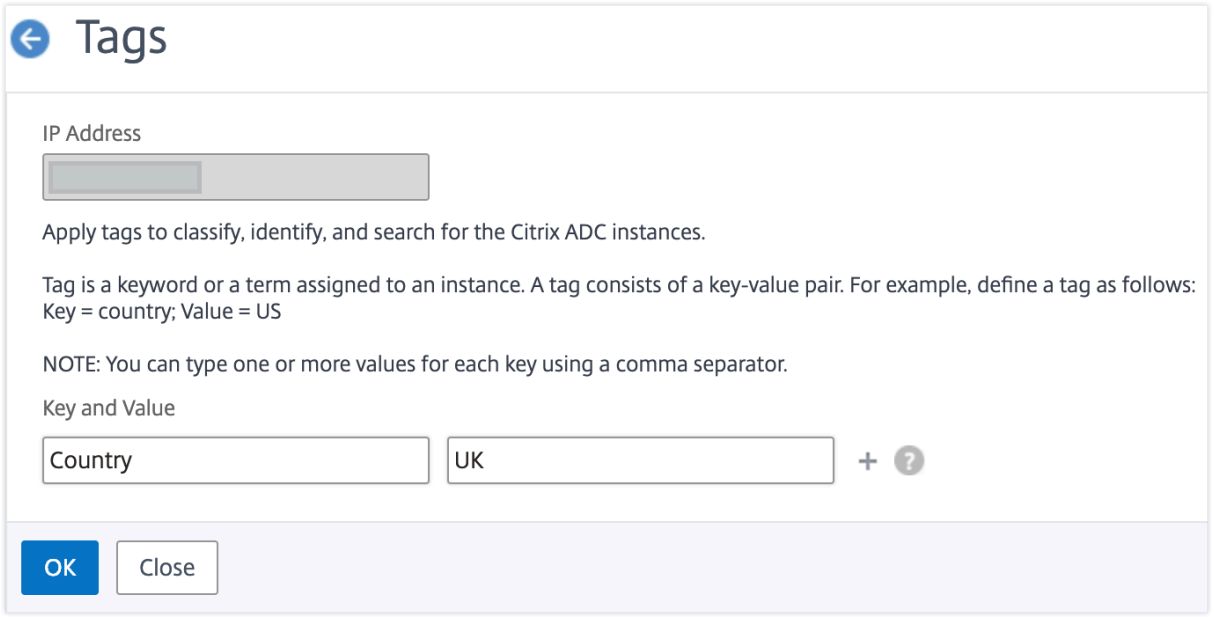
要为 **Citrix ADC VPX** 实例分配标签，请执行以下操作：

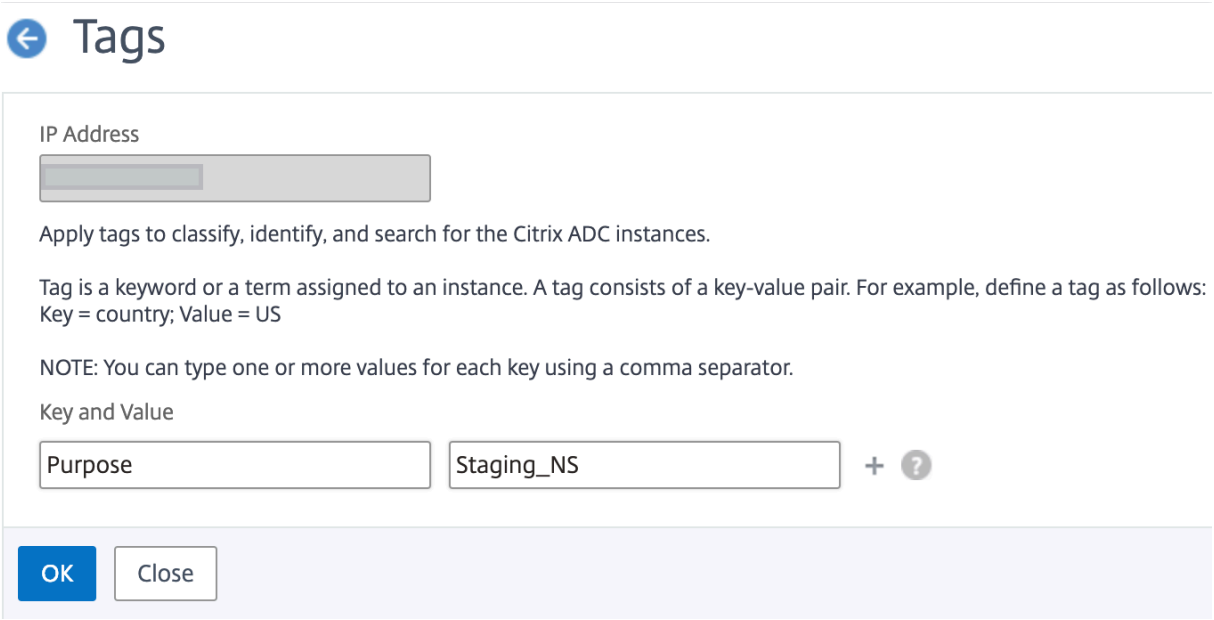
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例” > “ **Citrix ADC**”。
2. 选择 C **itrix ADC VPX** 选项卡。

3. 选择所需的 Citrix VPX。
4. 单击 “ 标签”。
5. 创建标签，然后单击 “ 确定”。

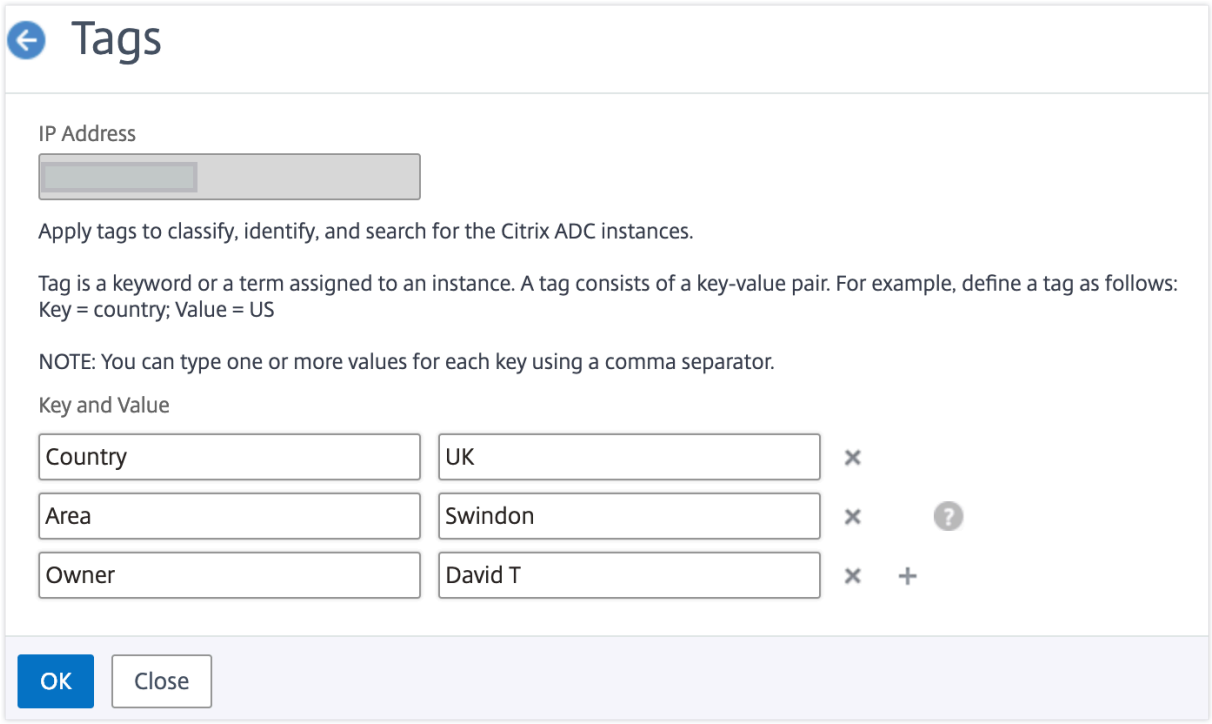
出现的 标签窗口允许您通过为您创建的每个关键字分配值来创建自己的 “键值” 对。

例如，以下图像显示了创建的几个关键字及其值。您可以添加自己的关键字并为每个关键字键入一个值。



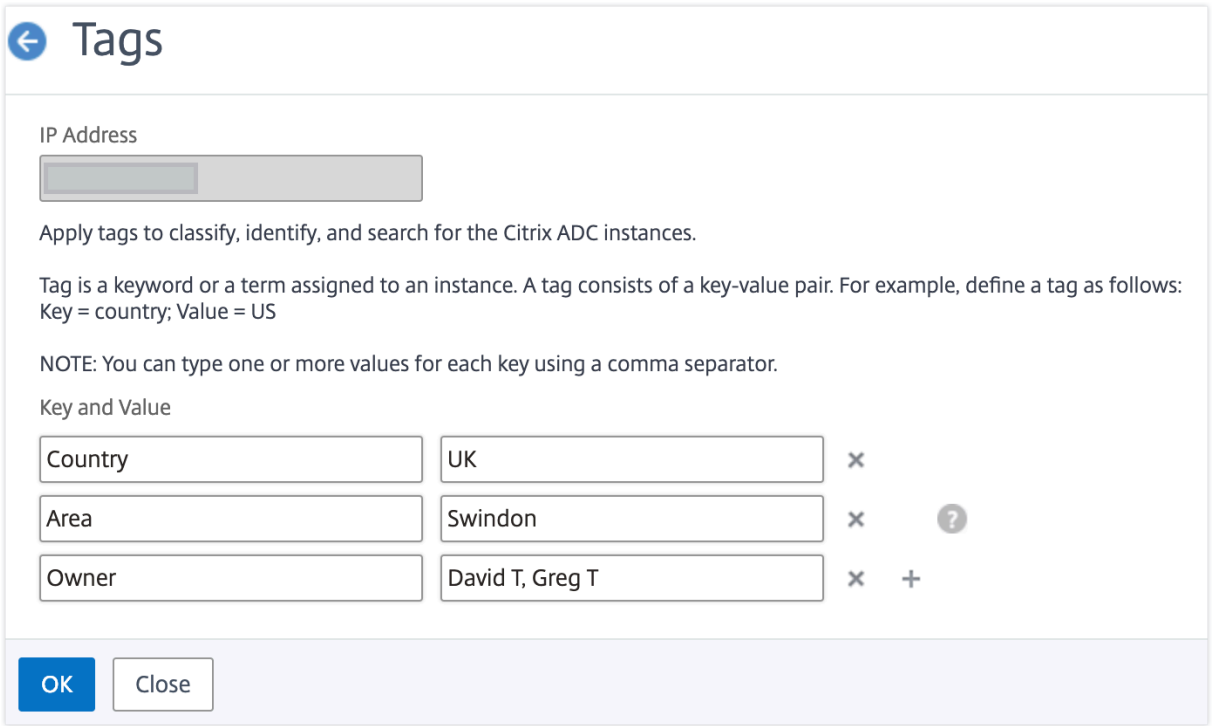


您也可以通过点击 “+” 添加多个标签。“ 通过添加多个有意义的标签，您可以高效地搜索实例。



您可以通过用逗号分隔来向关键字添加多个值。

例如，您将管理员角色分配给另一个同事 Greg T. 您可以添加他的名字，用逗号分隔。添加多个名称可帮助您按其中一个名称或两个名称进行搜索。Citrix ADM 将逗号分隔的值识别为两个不同的值。



要了解有关如何根据标签搜索实例的更多信息，请参阅 如何使用标签和属性的值搜索实例。

> 注意
>
> 您以后可以添加新标签或删除现有标签。您创建的标签数量没有限制。

如何使用标签和属性的值搜索实例

April 23, 2021

可能存在 Citrix Application Delivery Management (ADM) 管理许多 Citrix ADC 实例的情况。作为管理员，您可能希望灵活地根据特定参数搜索实例清单。Citrix ADM 现在提供了改进的搜索功能，可根据您在搜索字段中定义的参数搜索 Citrix ADC 实例子集。您可以根据两个条件（标签和属性）搜索实例。

- 标签。标签是可以分配给 Citrix ADC 实例的术语或关键字，以添加有关 Citrix ADC 实例的一些其他说明。现在，您可以将您的 Citrix ADC 实例与标签相关联。这些标签可用于更好地识别和搜索 Citrix ADC 实例。
- 属性。在 Citrix ADM 中添加的每个 Citrix ADC 实例都有一些与该实例关联的默认参数或属性。例如，每个实例都有自己的主机名、IP 地址、版本、主机 ID、硬件型号 ID 等。您可以通过为这些属性中的任何一个指定值来搜索实例。

例如，请考虑一种情况，您希望查找位于版本 12.0 且处于 UP 状态的 Citrix ADC 实例列表。此处，实例的版本和状态由默认属性定义。

除了实例的 12.0 版本和 UP 状态外，您还可以搜索您拥有的那些实例。您可以创建一个 “所有者” 标签并为该标签分配一个值 “David T”。有关如何创建和分配标签的更多信息，请参阅 如何创建标签并分配给实例。

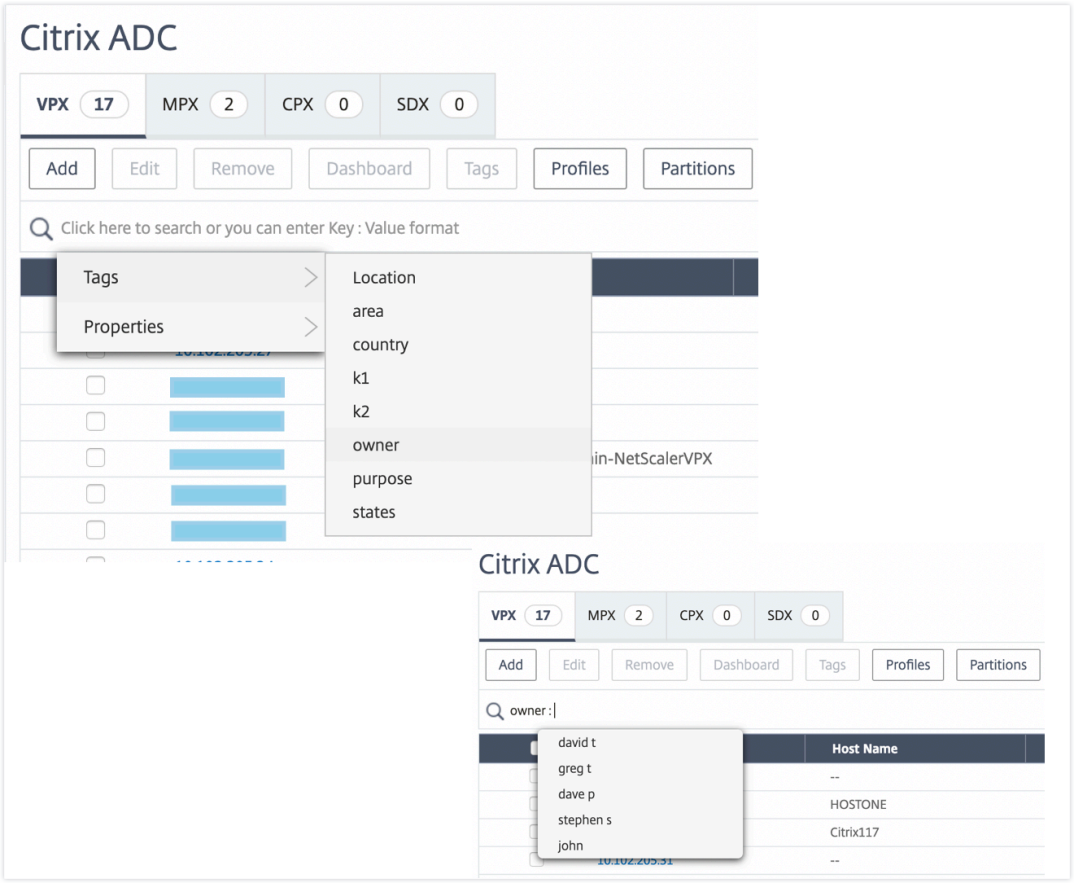
您可以使用标签和属性的组合来创建自己的搜索条件。

搜索 **Citrix ADC VPX** 实例

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ” > “ **VPX** ” 选项卡。
2. 单击搜索字段。您可以通过使用 “标签” 或 “属性” 或 “属性” 来创建搜索表达式。

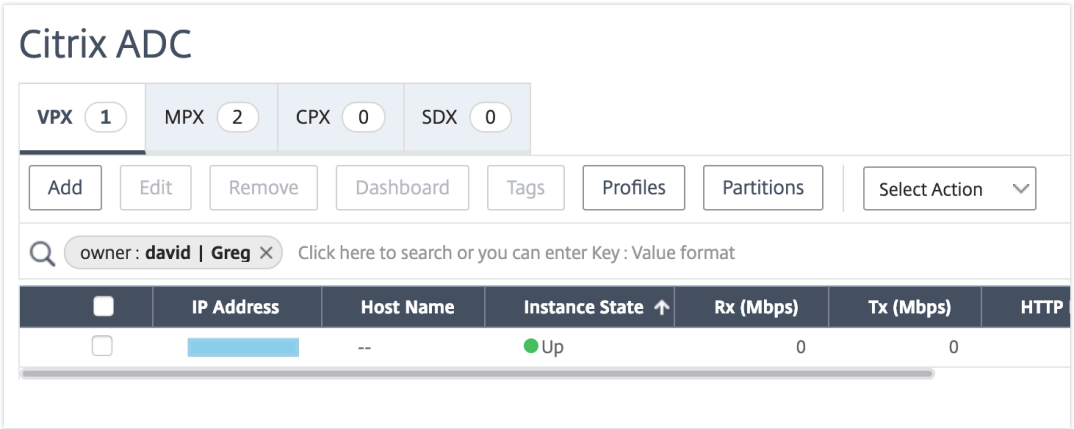
   以下示例说明了如何有效地使用搜索表达式搜索实例。

   a) 选择 “ 标签” 选项，然后选择 “ 所有者”。选择 “大卫 T.”

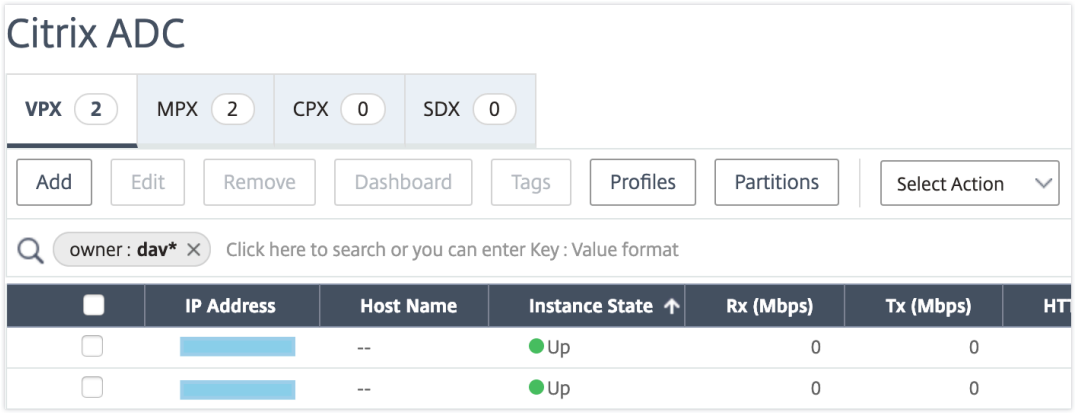


Citrix ADM 支持搜索表达式中的正则表达式和通配符。

b) 您可以使用正则表达式进一步展开搜索条件。例如，您希望搜索 David 或 Stephen 拥有的实例。在这种情况下，您可以通过使用 “|” 表达式分隔值来键入值。



c) 您还可以使用通配符替换或表示一个或多个字符。例如，您可以键入 `Dav*` 以搜索 David T 和 Dave P。



> 注意：有
>
> 关正则表达式和通配符及其使用方法的详细信息，请单击搜索栏中的“信息”图标。

管理 **Citrix ADC** 实例的管理分区

April 23, 2021

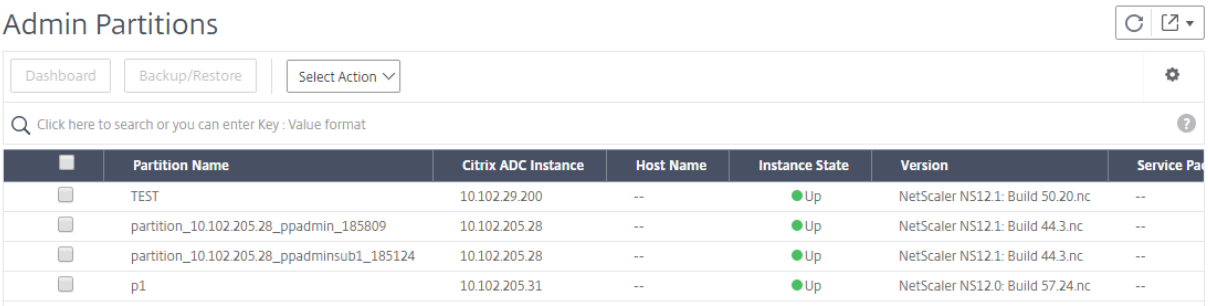
您可以在 Citrix 应用程序 Delivery Controller (ADC) 实例上配置管理分区，以便在同一 Citrix ADC 实例上为组织中的不同组分配不同的分区。可以分配一个网络管理员来管理多个 Citrix ADC 实例上的多个分区。

Citrix Application Delivery Management (ADM) 提供了从单个控制台管理员拥有的所有分区的无缝方式。您可以在不中断其他分区配置的情况下管理这些分区。

要允许多个用户管理不同的管理分区，您必须创建组，然后将用户和分区分配给这些组。每个用户只能查看和管理用户所属的组中的分区。每个管理分区都被视为 Citrix ADM 中的一个实例。当您发现 Citrix ADC 实例时，在该 Citrix ADC 实例上配置的管理分区会自动添加到系统中。

请考虑您有两个 Citrix VPX 实例，并在每个实例上配置了两个分区。例如，Citrix ADC 实例 10.102.216.49 具有分区 1、分区 2 和分区 3，而 Citrix ADC 实例 10.102.29.120 具有 p1 和 p2，如下图所示。

要查看分区，请导航到网络 **>** 实例 **> Citrix ADC > VPX**，然后单击 分区。



您可以为用户分配以下分区：10.102.29.120 分区和 10.102.216.49 分区 1 分区。而且，您可以分配用户 p2 来管理分区 10.102.29.80 分区、10.102.49 分区 2 分区和 10.102.216.49 分区 3 分区。

之后，必须创建两个用户 user-p1 和 user-p2，且必须将用户分配到为其创建的组。

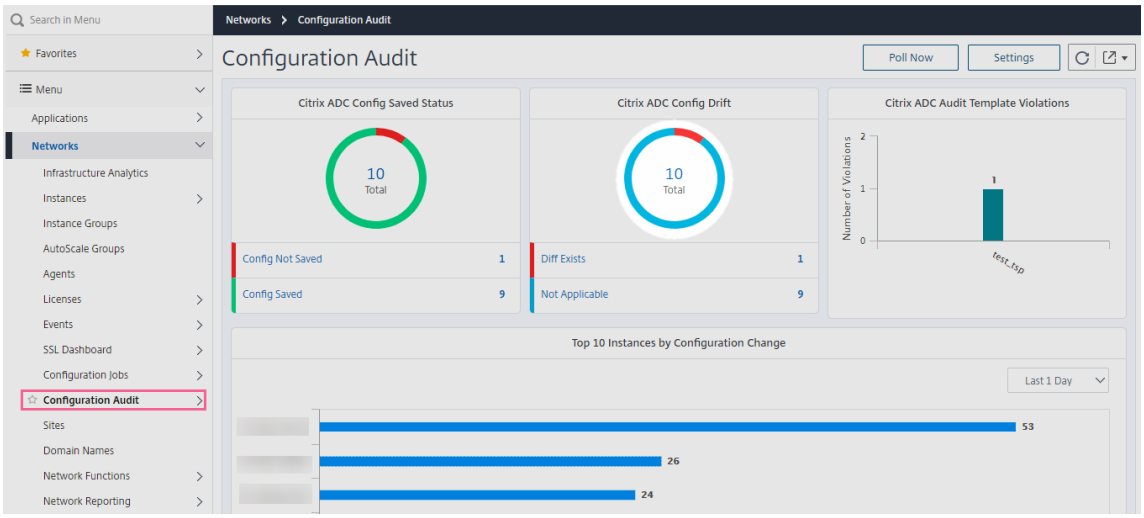
首先，您必须创建两个具有适当权限的组（例如：管理员权限），并在每个组中包含所需的管理员分区实例。例如，创建系统组分区-管理员，然后将 Citrix ADC 管理分区 10.102.29.120-p1 和 10.102.216.49 分区 1 添加到此组中。同时创建系统组分区-管理员，并将 Citrix ADC 管理分区 10.102.29.120-p2、10.102.216.49-分区 2 和 10.102.216.49 分区 3 添加到此组中。

创建管理分区后，您还可以使用修订历史记录差异功能和管理分区的审计模板功能进行审计

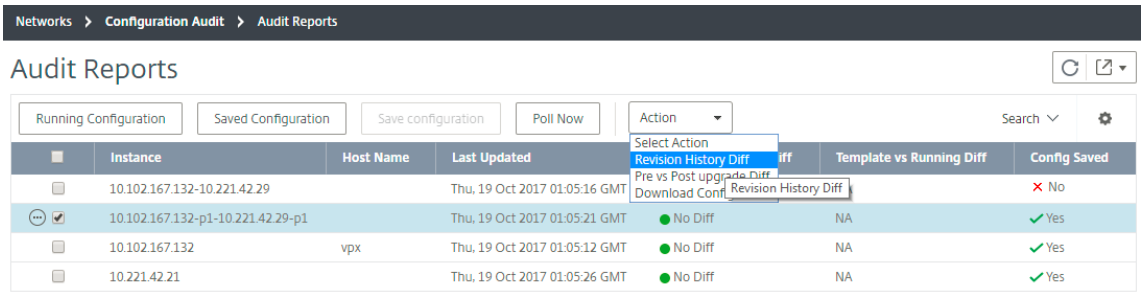
管理分区的修订历史记录差异允许您查看分区 Citrix ADC 实例的五个最新配置文件之间的差异。您可以将配置文件相互比较（例如配置修订版本-1 与配置修订版本-2）或与当前运行/保存的配置与配置修订版本进行比较。除了配置的差异外，还显示了校正配置。您可以将所有更正命令导出到本地文件夹并更正配置。

要查看版本历史记录差异，请执行以下操作：

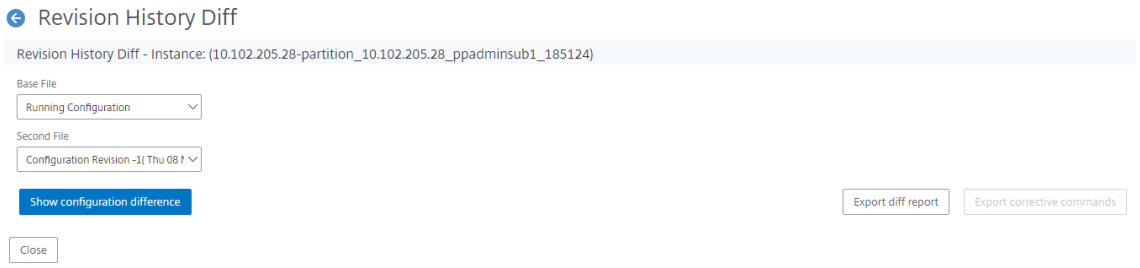
1. 导航到 网络 **>** 配置审计。在表示实例配置状态的圆环图中单击。在打开的 “ 审计报告” 页中，单击已分区的 Citrix ADC 实例。



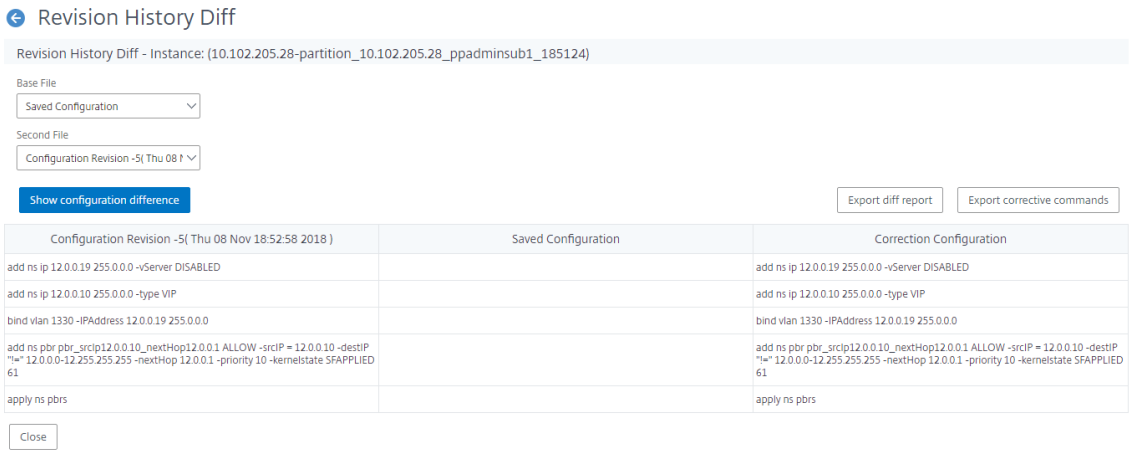
2. 在 “ 操作” 菜单中，单击 “ 修订历史记录比较”。



3. 在 修订历史记录差异页面上，选择要比较的文件。例如，将保存的配置与配置修订版-1 进行比较，然后单击 显示配置差异。



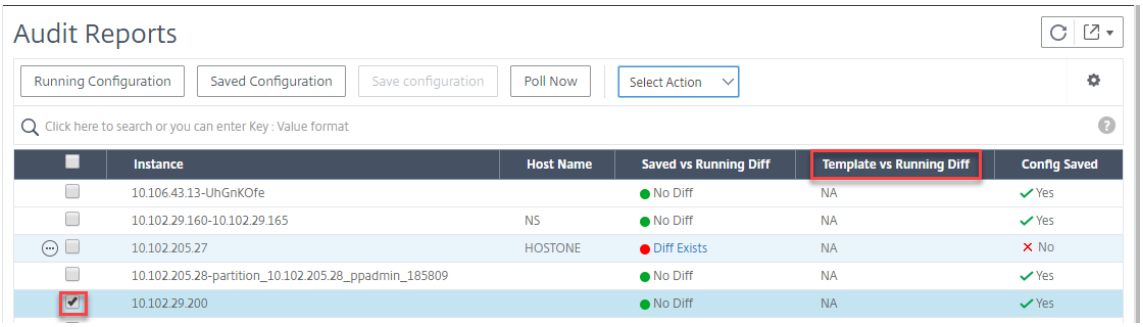
4. 然后，您可以查看所选分区 Citrix ADC 实例的五个最新配置文件之间的差异，如下所示。您还可以查看更正配置命令并将这些更正命令导出到本地文件夹。这些纠正命令是需要在基础文件上运行的命令，以使配置到所需状态（用于比较的配置文件）。



分区的审核模板允许您创建自定义配置模板并将其与分区实例关联。具有审计模板的实例运行配置中的任何变化都显示在“审计 报告”页的“ 模板与运行比较”列中。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。

要查看模板与运行差异，请执行以下操作：

1. 在 审计报告页面中，单击已分区的 Citrix ADC 实例。

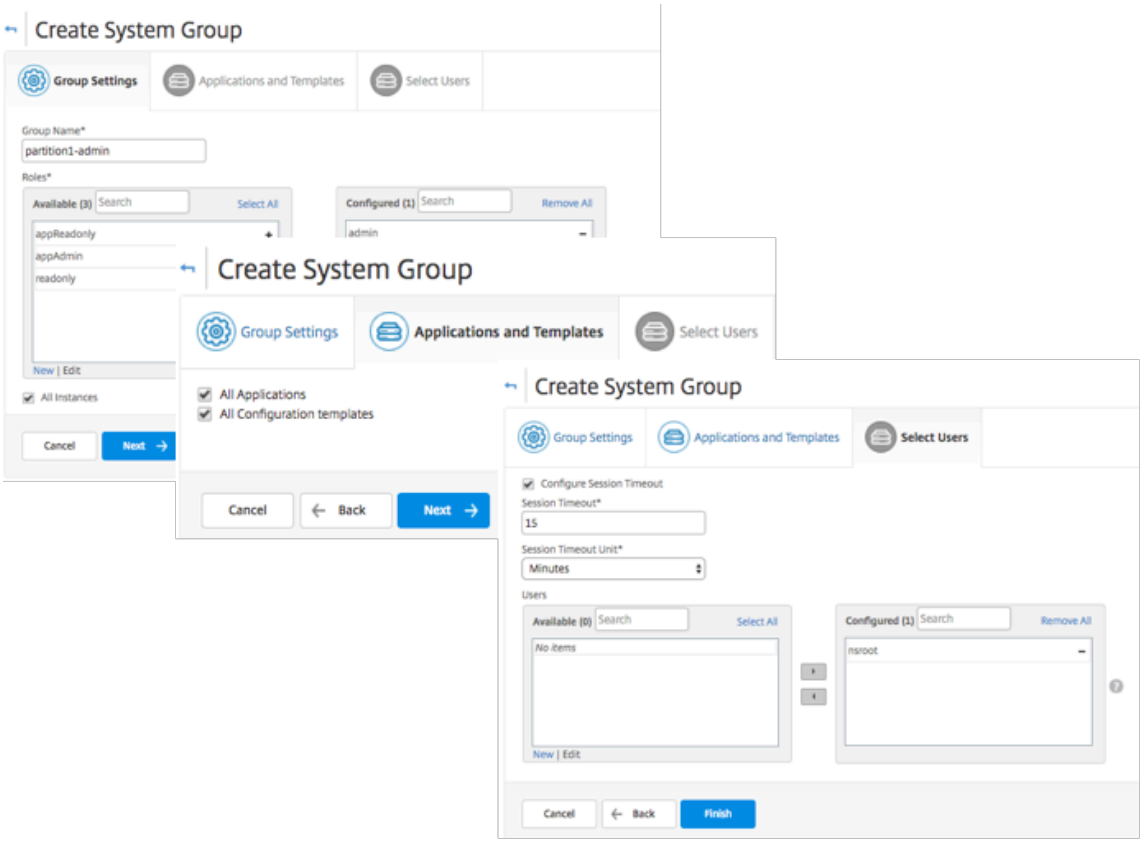


2. 如果审核模板与运行差异之间存在任何差异，则差异将显示为超链接。单击超链接可查看差异（如果存在）。除了配置的差异外，还显示了校正配置。您还可以将所有更正命令导出到本地文件夹并更正配置。

要创建组，请执行以下操作：

1. 导航到 系统 > 用户管理 > 组，然后单击 添加。

2. 在“ 创建系统用户” 页中，指定以下内容：
   - “组设置” 选项卡：输入组名称和角色权限。要允许访问特定实例，请清除 **“所有实例”** 复选框，然后在 **“选择实例”** 页面上选择您的实例。
   - “应用程序和模板” 选项卡：您可以选择在所有应用程序和配置模板中使用此组。
   - 选择用户选项卡：选择要添加到此组的用户。您可以单击 **“可用”** 表格中的 **“新建”** 链接以创建新用户。（可选）配置会话超时，在此可以配置用户可以保持活动状态的时间期限。
3. 单击完成。



要创建用户：

1. 导航到系统 **>** 用户管理 **>** 用户，然后单击 添加。
2. 在“创建系统用户” 页上，指定用户名和密码。（可选）您可以启用外部身份验证以及配置会话超时。
3. 通过将 “可用” 列表中的组名称添加到 “已配置” 列表，将用户分配到组。
4. 单击创建。

现在注销并使用 user-p1 凭据登录。只能查看和管理为您分配的管理分区以进行管理和监视。

创建 **Citrix ADC** 高可用性对

April 23, 2021

Citrix ADC 高可用性 (HA) 对可在停机或网络故障期间提供不间断的操作。您可以使用 Citrix ADM 创建一对高可用性 ADC 实例。有关详细信息，请参阅Citrix ADC 高可用性。

要在 Citrix ADM 中创建一对高可用性 ADC 实例，请执行以下步骤：

1. 导航到 网络 **>** 实例 **> Citrix ADC**。
2. 从列表中选择要用来创建 HA 对的 ADC 实例。

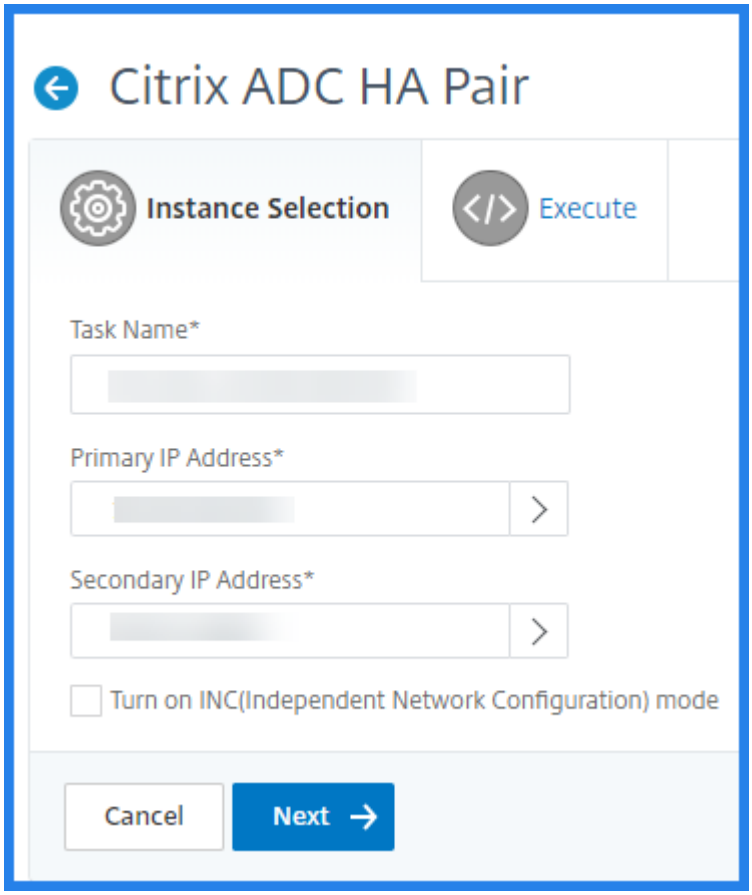
   选定的实例将成为 HA 对中的主实例。
3. 单击“选择 操作**” > “**创建高可用性对”。
4. 在 实例选择中，执行以下步骤：

   a) 在 辅助 **IP** 地址中，单击以选择辅助实例。

   b) 选择要在 HA 对中配置为辅助的 ADC 实例。

   c) 可选，如果在两个子 网中有 **HA** 对实例，请选择打开 **INC**（独立网络配置）模式。

   d) 单击 “ 下一步”。



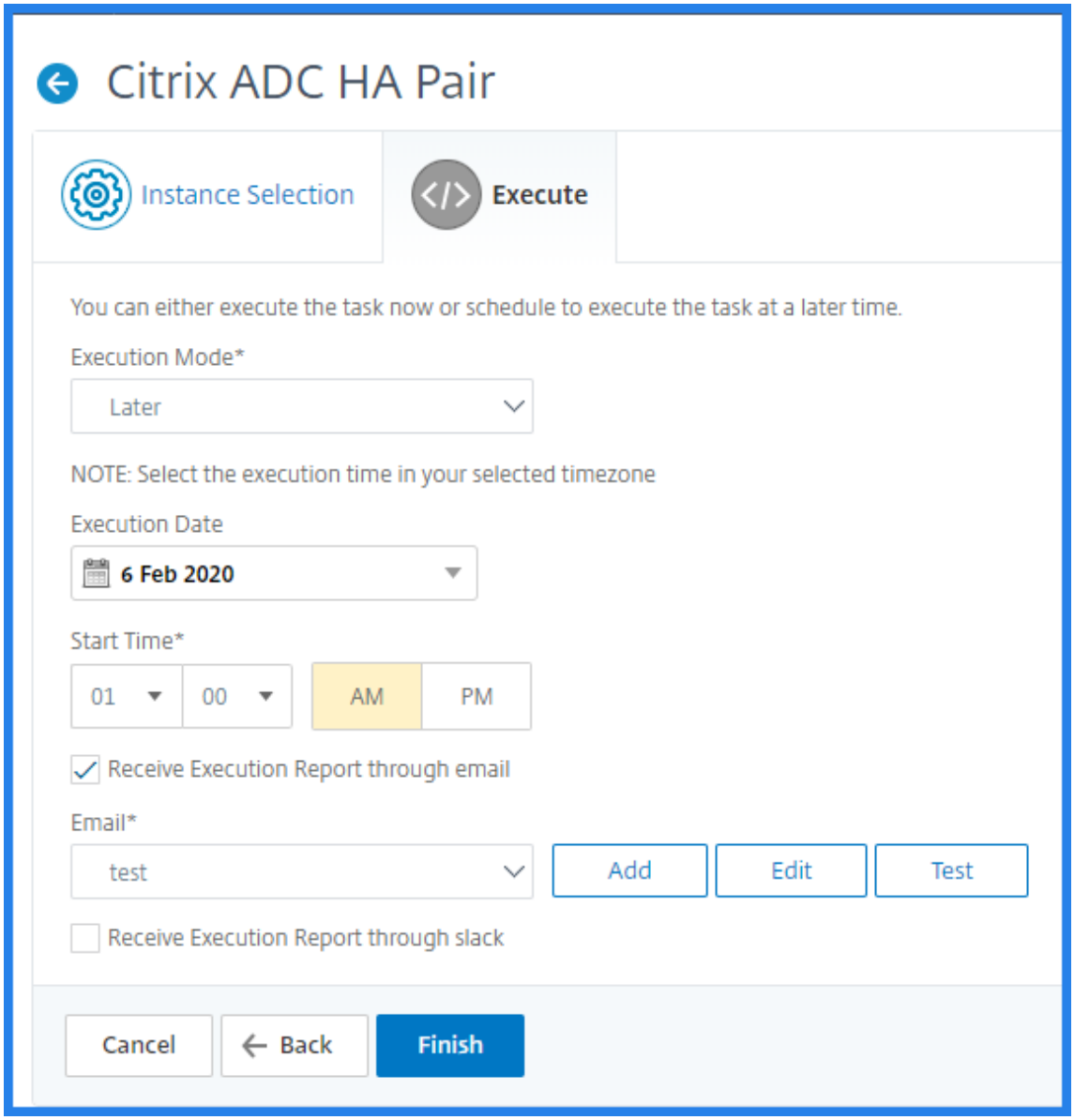
5. 在“ 执行” 中，您可以决定立即或稍后创建 HA 对。

   a) 在“ 执行模式” 中，选择以下执行模式之一：

      - 现在 -选择此选项立即创建 HA 对。
      - 稍后 -选择此选项可在特定日期和时间创建 HA 对。

   b) 如果在执行模式列表中选择了以后，请在要运行此任务时选择执行日期和开始时间。

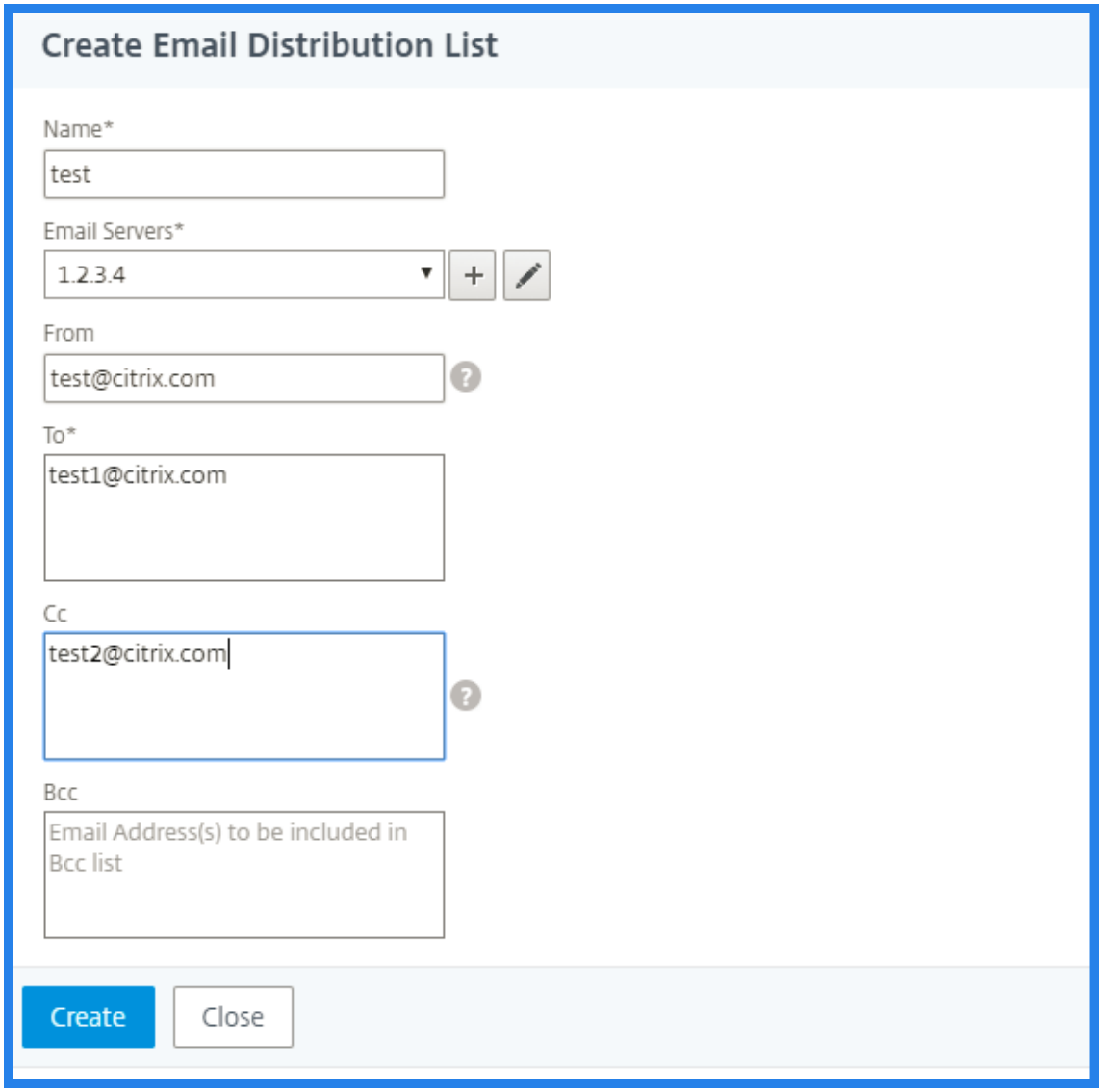
      > ** 注
      >
      > 意：** 执行时间显示在 Citrix ADM 中设置的时区中。



您可以通过以下方式接收此任务的执行报告：

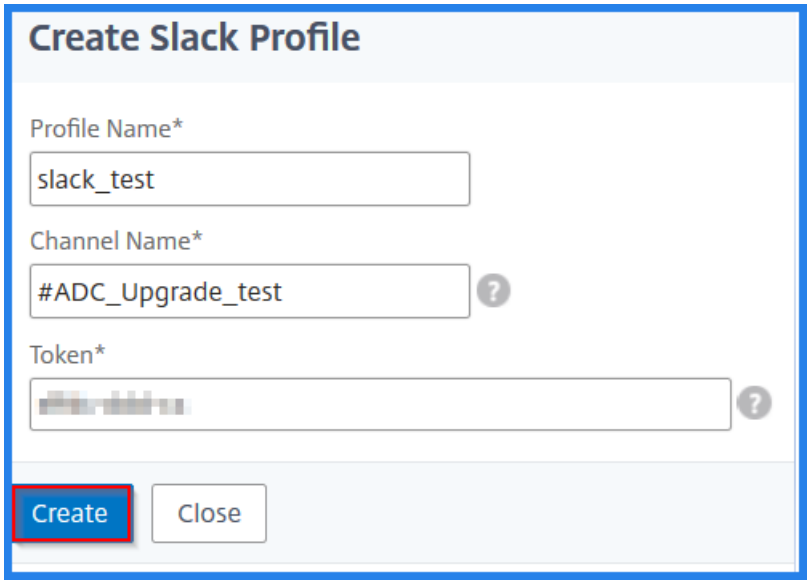
- 电子邮件 -从列表中选择电子邮件分发。

  要添加通讯组列表，请单击 添加。指定添加通讯组列表所需的参数，然后单击 创建。



- **Slack** -从列表中选择 Slack 配置文件。

  要添加 “Slack” 配置文件，请单击 “ 添加”。指定 配置式名称、频道名称和 令牌，然后单击 创建。



备份和还原 **Citrix ADC** 实例

April 23, 2021

您可以备份 Citrix ADC 实例的当前状态，然后使用备份的文件将其恢复到相同的状态。在升级实例之前或出于预防原因，始终备份实例。稳定系统的备份使您能够将其恢复到稳定点，如果系统变得不稳定。

有多种方法可以在 Citrix ADC 实例上执行备份和恢复。您可以使用 GUI 和 CLI 手动备份和还原 Citrix ADC 配置。您还可以使用 Citrix ADM 执行自动备份和手动恢复。

Citrix ADM 使用 NITRO 调用和安全外壳 (SSH) 和安全拷贝 (SCP) 协议备份托管 Citrix ADC 实例的当前状态。

Citrix ADM 创建完整备份并恢复以下 Citrix ADC 实例类型：

- Citrix SDX
- Citrix VPX
- Citrix MPX
- Citrix BLX

有关详细信息，请参阅 [备份和还原 ADC 实例。](https://docs.citrix.com/en-us/citrix-adc/12-1/system/basic-operations/backup-restore-citrix-adc-appliance.html)

> 注意
>
> - 确保 Citrix ADM 配置文件具有备份和还原 ADC 实例的管理员访问权限。
> - 在 Citrix ADM 中，您无法在 Citrix ADC 群集上执行备份和还原操作。

> - 不能使用从一个实例创建的备份文件来还原另一个实例。

备份的文件作为压缩的 TAR 文件存储在以下目录中：

```
/var/mps/tenants/root/device_backup/
<!--NeedCopy-->
```

为避免由于磁盘空间不可用而引起的问题，您可以在此目录中每个 ADC 实例最多保存 50 个备份文件。

要备份和还原 Citrix ADC 实例，必须首先在 Citrix ADM 上配置备份设置。配置设置后，您可以选择单个 Citrix ADC 实例或多个实例，并在这些实例中创建配置文件的备份。如有必要，您还可以使用这些备份的文件还原 Citrix ADC 实例。

配置实例备份设置

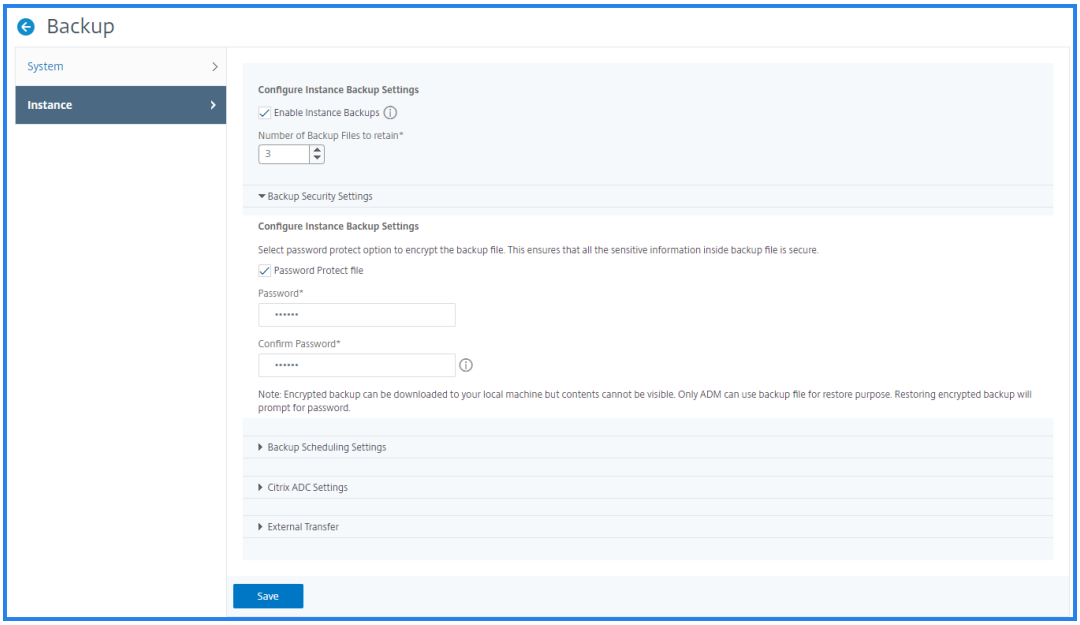
使用 “ 实例备份设置” 页可以配置 Citrix ADM 上的设置，以备份选定的 Citrix ADC 实例或多个实例：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 管理”。
2. 在 备份中，选择 配置系统和实例备份。
3. 选择 实例并指定以下内容：
   - 启用实例备份：默认情况下，Citrix ADM 处于启用状态，以备份 Citrix ADC 实例。如果您不想创建实例的备份文件，请清除此选项。
   - 密码保护文件：（可选）选择密码保护选项以加密备份文件。加密备份文件可确保备份文件中的所有敏感信息都是安全的。

     > 注意
     >
     > 您可以将加密的备份文件下载到本地计算机，但无法使用 Citrix ADM GUI 或任何文本编辑器打开该文件。该文件可以单独由 Citrix ADM 检索和使用。还原加密的备份文件时，系统会提示您提供密码。但您可以在您的系统上打开未加密的备份文件。

   - 要保留的备份文件数：指定要在 Citrix ADM 中保留的备份文件数。每个 ADC 实例最多可保留 50 个备份文件。默认是三个备份文件。

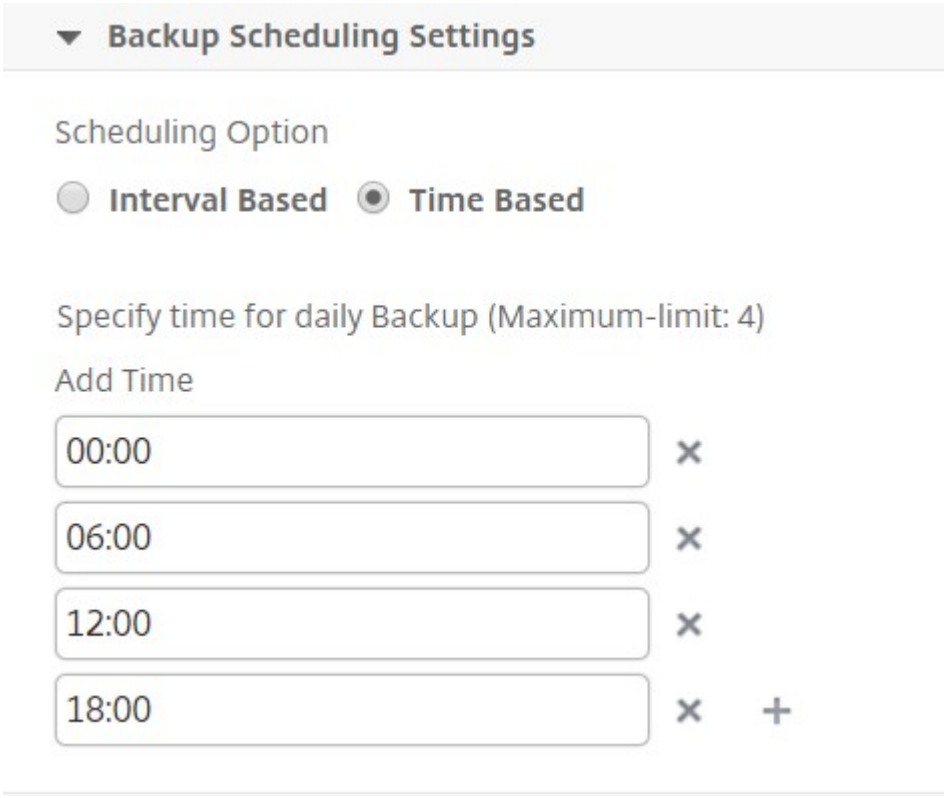
     > 注意
     >
     > 每个备份文件都会考虑到一些存储要求。Citrix 建议您根据您的要求在 Citrix ADM 上存储最佳数量的 Citrix ADC 备份文件。



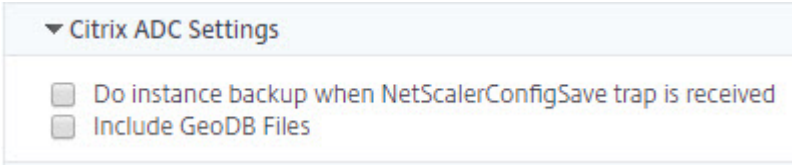
- 备份计划设置：（可选）有两个选项可用于创建备份文件，但一次只能使用一个选项：

  a) 默认的备份计划选项是“基于间隔的。“ 在指定的时间间隔过后，将在 Citrix ADM 中创建一个备份文件。默认备份时间间隔是 12 小时。

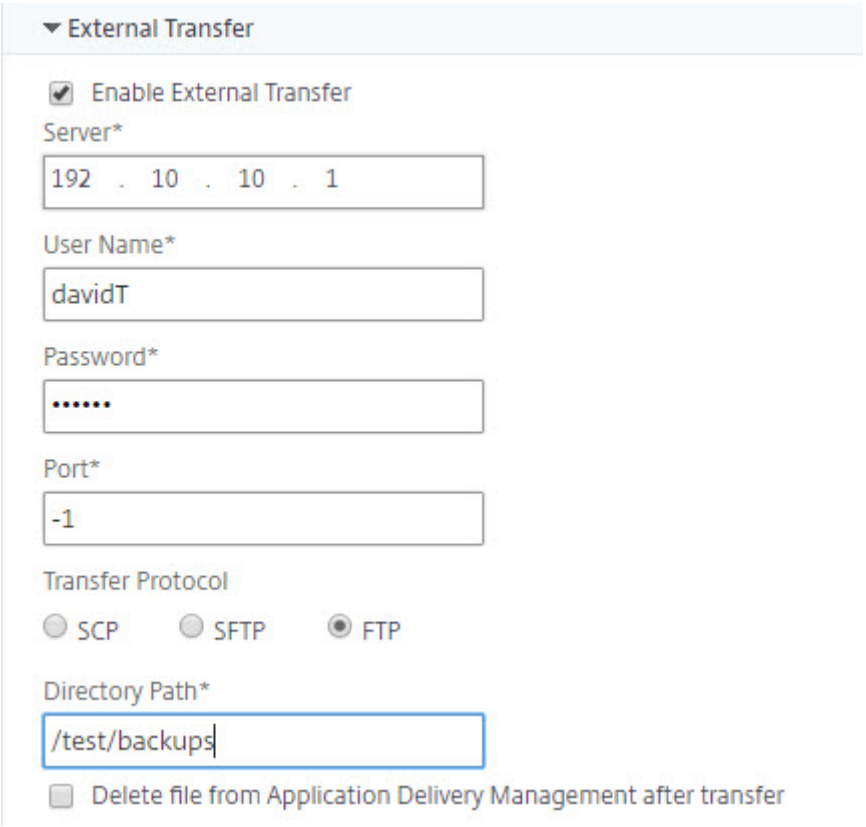
  b) 您还可以将定时备份的类型更改为“基于时间”。“ 在此选项中，以 `hours:minutes` 格式指定在指定时间备份实例的时间。Citrix ADM 允许在实例上进行最多四次每日备份。



- **Citrix ADC** 设置：（可选）默认情况下，Citrix ADM 在收到 “NetScalerconfigSave” 陷阱时不会创建备份文件。但是，只要 Citrix ADC 实例向 Citrix ADM 发送 “NetScalerconfigSave” 陷阱，您可以启用此选项来创建备份文件。每次保存实例上的配置时，Citrix ADC 实例都会发送 “NetScalerconfigSave”。
- 地理数据库文件：（可选）默认情况下，Citrix ADM 不备份地理数据库文件。您也可以启用该选项以创建这些文件的备份。



- 外部传输：（可选）Citrix ADM 允许您将 Citrix ADC 实例备份文件传输到外部位置：
  a) 指定位置的 IP 地址。
  b) 指定要将备份文件传输到的外部服务器的用户名和密码。
  c) 指定传输协议和端口号。
  d) 您可以指定必须存储文件的目录路径。
  e) 可选，还可以在将备份文件传输到外部服务器后从 Citrix ADM 中删除备份文件。



> 注意
>
> 当任何选定的 Citrix ADC 实例出现备份失败时，Citrix ADM 会向自身发送 SNMP 陷阱或系统日志通知。

使用 **Citrix ADM** 为选定的 **Citrix ADC** 实例创建备份

如果要备份选定的 Citrix ADC 实例或多个实例，请执行以下任务：

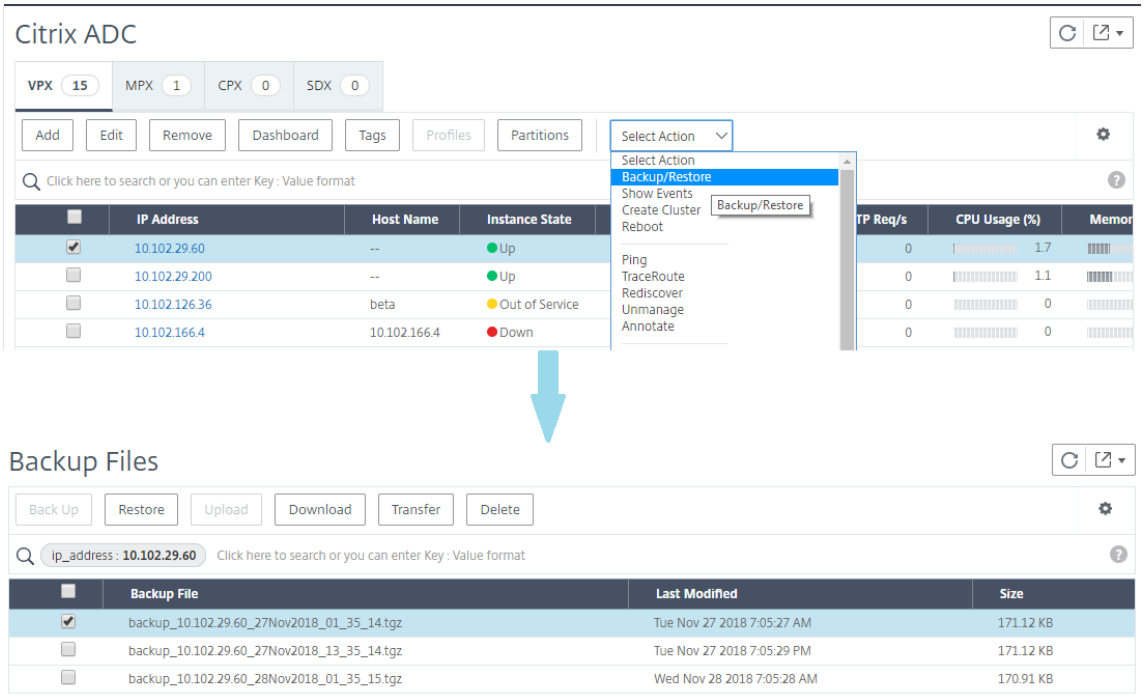
1. 在 Citrix ADM 中，导航到“网络”>“实例”。在“实例”下，选择要在屏幕上显示的实例类型（例如 Citrix VPX）。
2. 选择要备份的实例。
   - 对于 MPX、VPX 和 BLX 实例，请从“选择 操作”列表中选择“备份/恢复”。
   - 对于 SDX 实例，请单击 备份/恢复。
3. 在“备份文件”页上，单击“备份”。
4. 您可以指定是否加密备份文件以提高安全性。您可以输入密码，也可以使用之前在实例备份设置页面上指定的全局密码。
5. 单击 继续。

使用 **Citrix ADM** 还原 **Citrix ADC** 实例

> 注意：
>
> 如果在 HA 对中有 Citrix ADC 实例，则需要注意以下事项：
>
> - 还原创建备份文件的同一实例。例如，让我们考虑从 HA 对的主实例中获取备份的情况。在还原过程中，确保您正在还原相同的实例，即使它不再是主实例也是如此。
> - 当您在主 ADC 实例上启动还原过程时，您无法访问主实例，并且辅助实例将更改为 **STAYSECONDARY**。在主实例上完成还原过程后，辅助 ADC 实例将从 **STAYSECONDARY** 模式更改为 **ENABLED** 模式，并再次成为高可用性对的一部分。在恢复过程完成之前，主实例可能会出现停机时间。

执行此任务可通过使用您之前创建的备份文件还原 Citrix ADC 实例：

1. 导航到“网络”>“实例”，选择要还原的实例，然后单击“查看备份”。
2. 在“备份文件”页上，选择包含要还原的设置的备份文件，然后单击还原。



使用 **Citrix ADM** 恢复 **Citrix ADC SDX** 装置

在 Citrix ADM 中，Citrix ADC SDX 装置的备份包括以下内容：

- 设备上托管的 Citrix ADC 实例
- SVM SSL 证书和密钥
- 实例删除设置（XML 格式）
- 实例备份设置（XML 格式）
- SSL 证书轮询设置（XML 格式）
- 支持虚拟机数据库文件
- SDX 上存在的设备的 Citrix ADC 配置文件
- Citrix ADC 构建映像
- Citrix ADC XVA 映像，这些图像存储在以下位置：
  `/var/mps/sdx_images/`
- SDX 单捆绑包映像 (SVM+XS)
- 第三方实例映像（如果已置备）

将您的 Citrix ADC SDX 装置恢复到备份文件中可用的配置。在设备还原过程中，会删除整个当前配置。

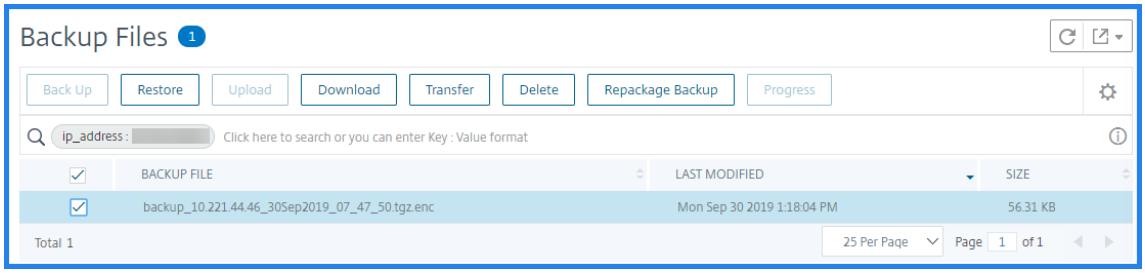
如果要通过使用其他 Citrix ADC SDX 装置的备份还原 Citrix ADC SDX 装置，请确保添加许可证并将设备的管理服务网络设置配置为与备份文件中的设置相匹配，然后再开始还原过程。

在恢复 SDX 装置之前，请确保备份的 SDX 装置平台变体与装置相同。不能从另一个平台变体还原。

> 注意：
>
> 在恢复 SDX RMA 装置之前，请确保备份版本与 RMA 版本相同或更高。

要从备份文件中恢复 SDX 装置，请执行以下操作：

1. 在 Citrix ADM GUI 中，导航到 **“网络” > “实例” > “Citrix ADC”**。
2. 单击 “ 备份/恢复”。
3. 选择要还原的同一实例的备份文件。
4. 单击 “ 重新打包备份”。



   备份 SDX 设备时，XVA 文件和映像将单独存储，以节省网络带宽和磁盘空间。因此，在恢复 SDX 装置之前，必须重新打包备份的文件。

   重新打包备份文件时，备份文件将所有备份文件包括在一起，以恢复 SDX 设备。重新打包的备份文件可确保 SDX 设备的成功恢复。

5. 选择重新打包的备份文件，然后单击 还原”。

强制故障切换到辅助 **Citrix ADC** 实例

April 23, 2021

例如，如果需要替换或升级主 Citrix 应用程序 Delivery Controller (ADC) 实例，则可能希望强制执行故障切换。可以从主要实例或辅助实例强制执行故障转移。对主要实例强制执行故障转移时，主要实例变为辅助实例，而辅助实例变为主要实例。仅当主要实例可以确定辅助实例处于 “UP”（运行）状态时才有可能执行强制故障转移。

强制故障转移不会传播，也不会同步。要在执行强制故障转移后查看同步状态，可以查看实例的状态。

在下列任何一种情况下，强制故障转移会失败：

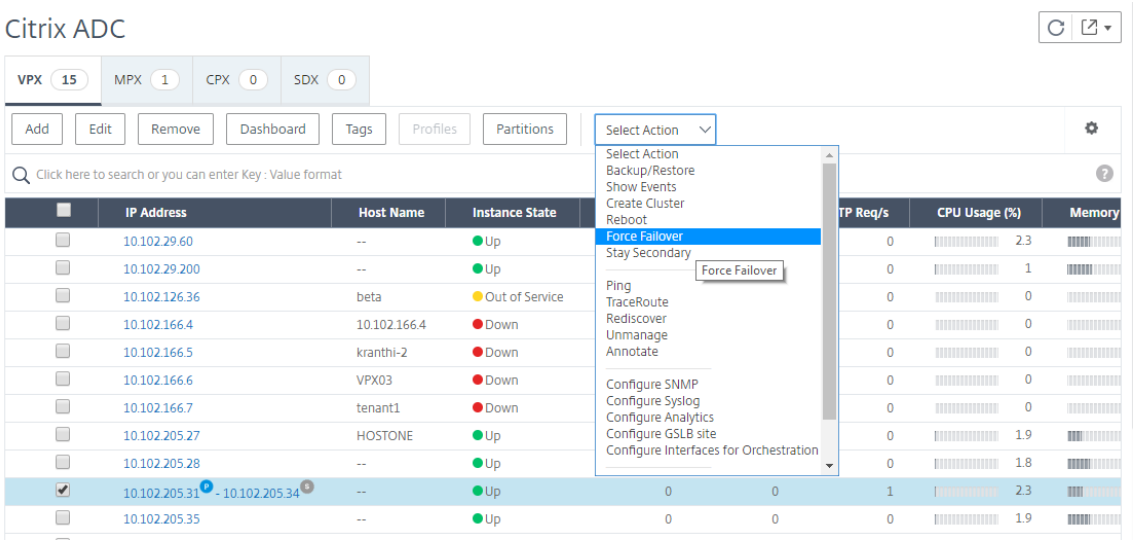
- 在独立的系统上强制执行故障转移。
- 辅助实例处于禁用或非活动状态。如果辅助实例处于非活动状态，必须等待其状态变为 “UP”（运行）时才能强制执行故障转移。
- 辅助实例配置为保持辅助状态。

如果在运行强制故障切换命令时检测到潜在问题，Citrix ADC 实例将显示一条警告消息。该消息包括触发警告的信息，并在继续之前要求确认。

可以对主要实例或辅助实例强制执行故障转移。

要使用 **Citrix ADM** 强制故障切换到辅助 **Citrix ADC** 实例，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 网络 **>** 实例 **> Citrix ADC > VPX** 选项卡，然后选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 从 “ 操作” 菜单中，选择 “ 强制故障切换**”**。
4. 单击 **Yes**（是）确认强制执行故障转移操作。



强制辅助 **Citrix ADC** 实例保持辅助实例

April 23, 2021

在 HA 设置中，辅助节点可以被强制保持辅助状态，无论主节点的状态为何。

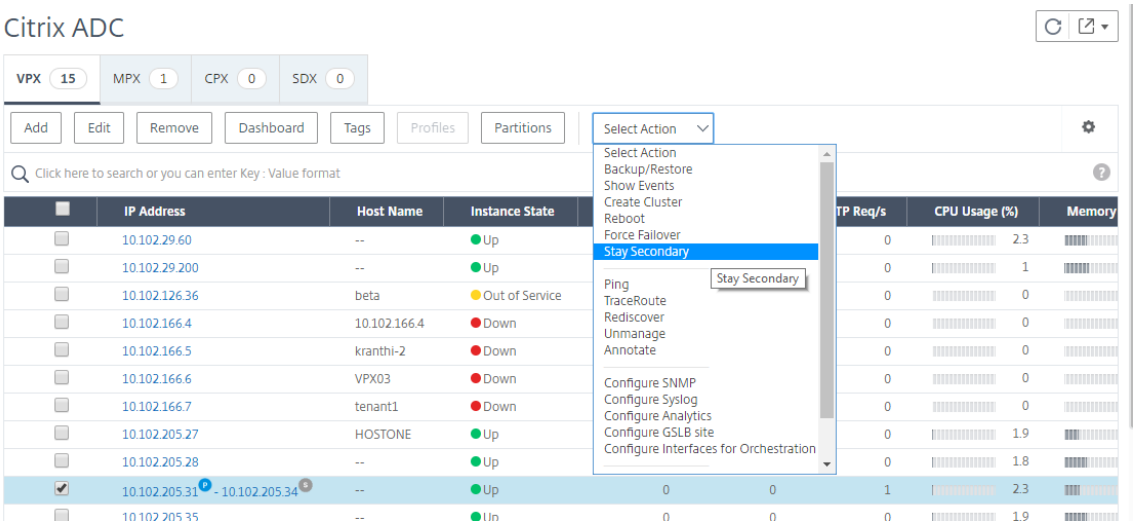
例如，假定主节点需要升级，该过程需要数秒。升级期间，主节点可能会关闭几秒钟，但您不希望辅助节点接管。即使在主节点中检测到故障，您也希望它仍然是辅助节点。

强制辅助节点保持辅助节点时，即使主节点关闭，它仍保持辅助节点。此外，如果强制使 HA 对中一个节点状态保持辅助状态，它将不会参与 HA 状态计算机转换。该节点的状态显示为 STAYSECONDARY。

> 注意
>
> 强制系统保持辅助状态时，强制过程不会传播或同步。它仅影响对其运行命令的节点。

要使用 **Citrix ADM** 配置辅助 **Citrix ADC** 实例保持辅助实例，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ” > “ **VPX** ” 选项卡，然后选择一个实例。
2. 从所选实例类型下方列出的实例中选择 HA 设置中的实例。
3. 从 “ 操作” 菜单中，选择 “ 保持次要”。
4. 单击 **Yes**（是）确认执行 “Stay Secondary”（保持辅助状态）操作。



创建实例组

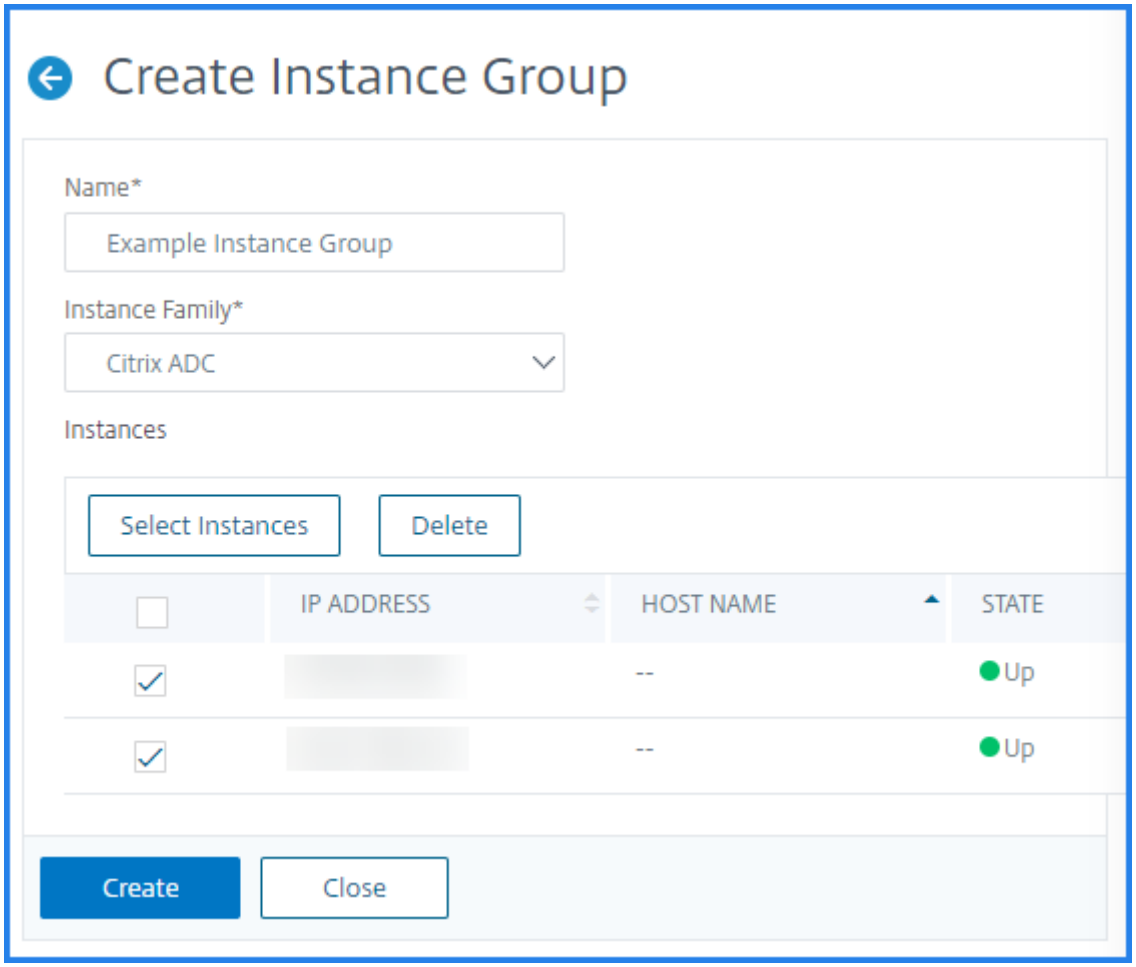
April 23, 2021

要创建实例组，必须首先将所有 Citrix ADC 实例添加到 Citrix ADM 中。成功添加实例后，基于实例系列创建实例组。创建一组实例可帮助您同时在分组实例上升级、备份或还原。

使用 **Citrix ADM** 创建实例组

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例组”，然后单击 “ 添加”。
2. 为您的实例组指定一个名称，然后从 “实 例系列” 列表中选择 **Citrix ADC** 。
3. 单击 选择实例。在 选择实例页面上，选择要分组的实例，然后单击 选择。

   该表列出了所选实例及其详细信息。如果要从组中删除任何实例，请从表中选择该实例，然后单击 “ 删除”。
4. 单击创建。



使用 **ADM** 在 **SDX** 上预配 **ADC VPX** 实例

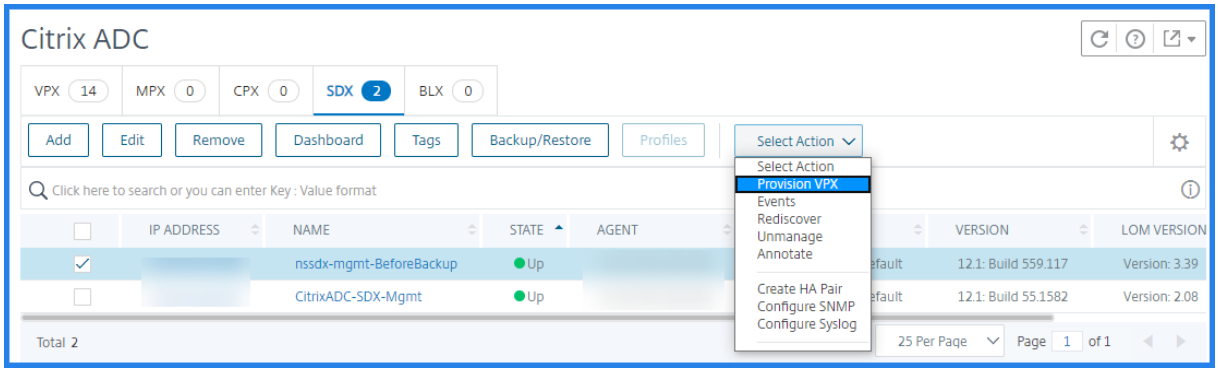
April 23, 2021

您可以使用 Citrix ADM 在 SDX 设备上配置一个或多个 ADC VPX 实例。您可以部署的实例数量取决于您购买的许可证。如果添加的实例数等于许可证中指定的数量，则 ADM 将限制您置备更多 Citrix ADC 实例。

在开始之前，请确保在 ADM 中添加要预配 VPX 实例的 SDX 实例。

要配置 VPX 实例，请执行以下操作：

1. 导航到 网络 **>** 实例 **> Citrix ADC**。
2. 在 **SDX** 选项卡中，选择要预配 VPX 实例的 SDX 实例。
3. 在 选择操作中，选择 置备 **VPX**。

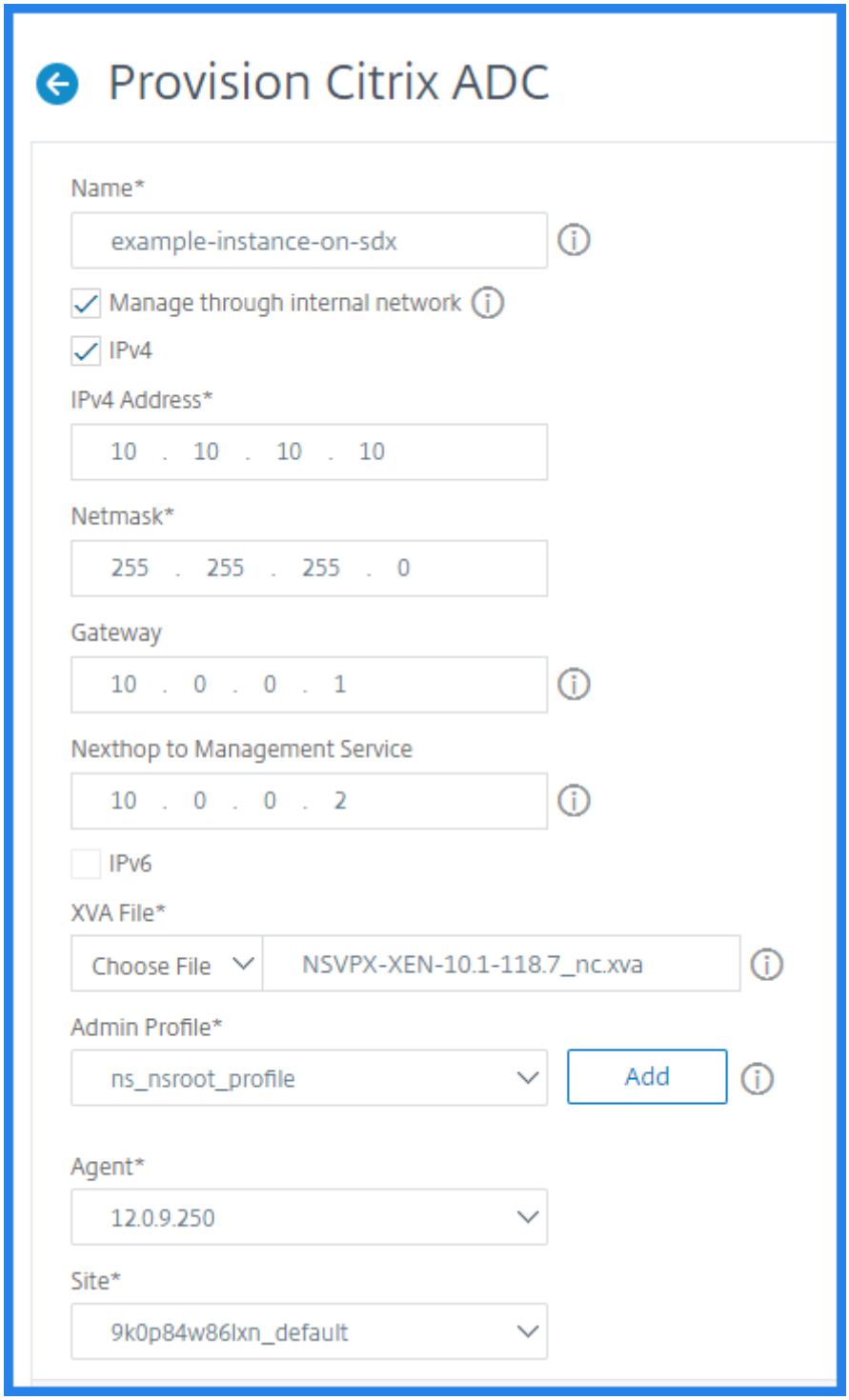


步骤 **1-**添加 **VPX** 实例

ADM 使用以下信息在 SDX 设备中配置 VPX 实例：

- 名称 -为 ADC 实例指定名称。
- 在 SDX 和 VPX 之间建立通信网络。为此，请从列表中选择所需的选项：
  - 通过内部网络进行管理 -此选项为 ADM 和 VPX 实例之间的通信建立内部网络。
  - **IP** 地址 -您可以选择 **IPv4** 或 **IPv6** 地址或两者来管理 Citrix VPX 实例。VPX 实例只能有一个管理 IP（也称为 Citrix ADC IP）。您无法删除 Citrix ADC IP 地址。

    对于所选选项，为 IP 地址分配子网掩码、默认网关和下一跳到 ADM 服务器。
- **XVA** 文件 -选择要从中预配 VPX 实例的 XVA 文件。使用以下选项之一选择 XVA 文件。
  - 本地 -从本地计算机中选择 XVA 文件。
  - 设备 -从 ADM 文件浏览器中选择 XVA 文件。
- 管理员配置文件-此配置文件提供对配置 VPX 实例的访使用此配置文件，ADM 将从实例中检索配置数据。如果必须添加配置文件，请单击 添加。
- **Agent** -选择要与实例关联的代理
- 站点 -选择要添加实例的站点。



步骤 **2-**分配许可证

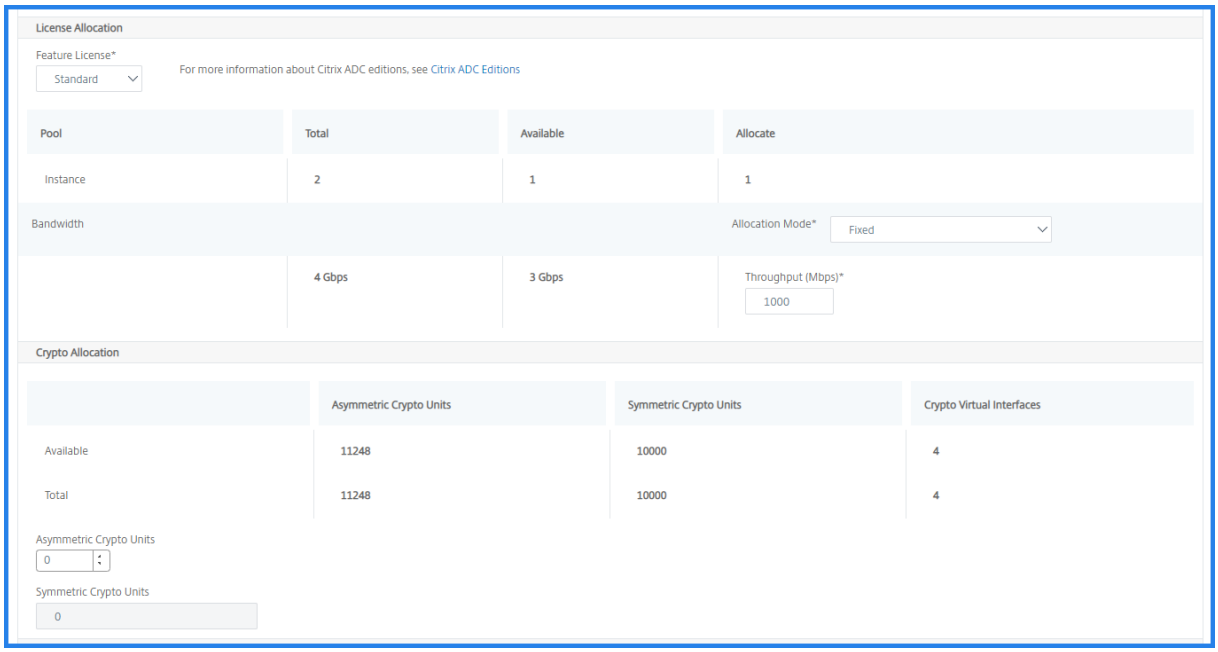
在“ 许可证分配**”** 部分中，指定 VPX 许可证。您可以使用标准、高级和高级许可证。

- 分配模式 -您可以为带宽池选择 固定或突发模式。

如果选择 突发模式，则可以在达到固定带宽时使用额外的带宽。

- 吞吐量 -将总吞吐量（以 Mbps 为单位）分配给实例。

> 注意
>
> 为 SDX 设备上的 Citrix Secure Web Gateway (SWG) 实例单独购买许可证（适用于 Secure Web Gateway 的 SDX 双实例附加包）。此实例包不同于 SDX 平台许可证或 SDX 实例包。
>
> 有关更多信息，请参阅 在 SDX 设备上部署 Citrix Secure Web Gateway 实例。



从 SDX 12.0 57.19 版本开始，管理加密容量的界面发生了变化。有关详细信息，请参阅管理加密容量。

步骤 **3-**分配资源

在 “ 资源分配” 部分中，将资源分配给 VPX 实例以维护流量。

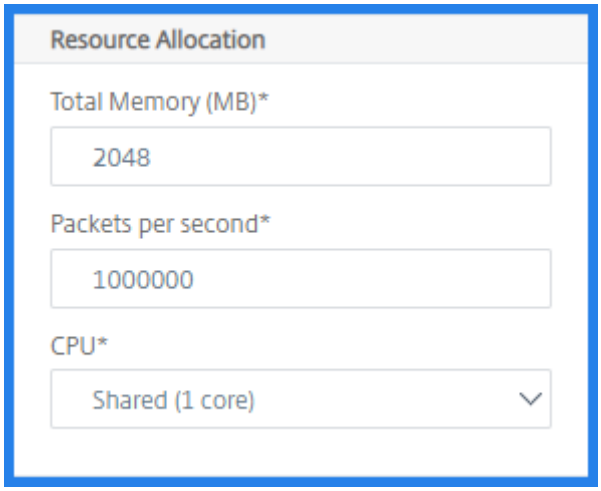
- 总内存 **(MB)** -为实例分配总内存。最小值为 2048 MB。
- 每秒数据包数-指定每秒要传输的数据包数。
- **CPU** -指定实例的 CPU 内核数。您可以使用共享或专用 CPU 内核。

  当您为实例选择共享内核时，其他实例可以在资源短缺时使用共享内核。

  重新启动重新分配 CPU 核心的实例，以避免任何性能下降。

  如果您使用的是 SDX 25000xx 平台，则最多可以为实例分配 16 个内核。此外，如果您使用的是 SDX 2500xxx 平台，则最多可以为实例分配 11 个内核。

> 注意
>
> 对于实例，您配置的最大吞吐量为 180 Gbps。



下表列出了支持的 VPX、单一 Bungle 映像版本以及您可以分配给实例的核心数量：

平台名称	核心总数	可用于 VPX 预配的核心总数	可分配给单个实例的最大核心数
SDX 8015、SDX 8400 和 SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500 和 SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540 和 SDX 11542	12	10	5
SDX 17500、SDX 19500 和 SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550 和 SDX 21550	12	10	5

平台名称	核心总数	可用于 VPX 预配的核心总数	可分配给单个实例的最大核心数
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080 和 SDX 14100	12	10	5
SDX 22040、SDX 22060、SDX 22080、SDX 22100 和 SDX 22120	16	14	7
SDX 24100 和 SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G 和 SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS 和 SDX 14100。FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S 和 SDX 14100 40S	12	10	5
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16（如果版本为 11.1-51.x 或更高版本）；9（如果版本为 11.1-50.x 或更低；所有版本为 11.0 和 10.5）
SDX 26100、26160、26200、26250	28	26	13

平台名称	核心总数	可用于 VPX 预配的核心总数	可分配给单个实例的最大核心数
15000-50G	16	14	7

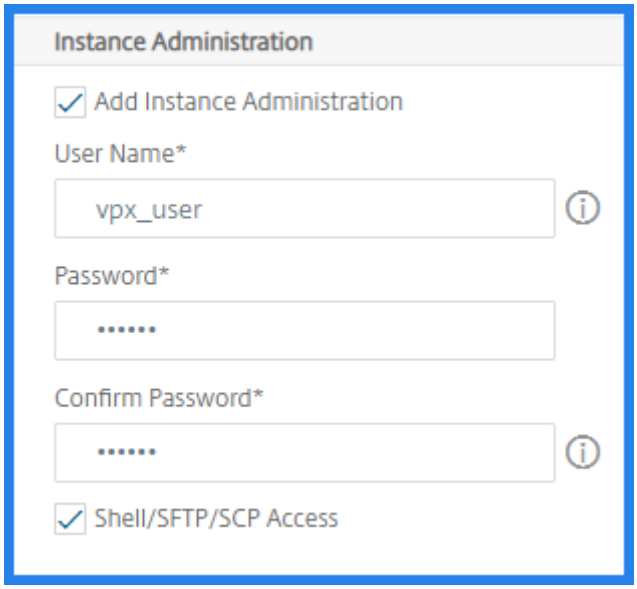
> 注意
>
> 在 SDX 26xxx 平台上，最多可以为 VPX 实例分配 26 个 CPU 内核。如果为实例分配了加密单元，则核心的最大数量取决于加密单元和数据接口的数量。
>
> 例如，如果您为实例分配 24000 个加密单元，则可以为实例分配 24 个 CPU 核心和最多两个数据接口。SDX 设备将数据接口和加密单元视为 PCI 设备。对于 26000 个加密单元，VPX 实例配置失败，因为没有添加数据接口的空间。

步骤 **4-**添加实例管理

您可以为 VPX 实例创建管理员用户。为此，请在 “ 实例管理” 部分中选择添加实例管理。

指定以下详细信息：

- 用户名：Citrix ADC 实例管理员的用户名。此用户具有超级用户访问权限，但无权访问联网命令来配置 VLAN 和接口。
- 密码：指定用户名的密码。
- S@@**hell/Sftp/Scp** 访问：Citrix ADC 实例管理员允许的访问权限。此选项默认处于选中状态。



步骤 **5-**指定网络设置

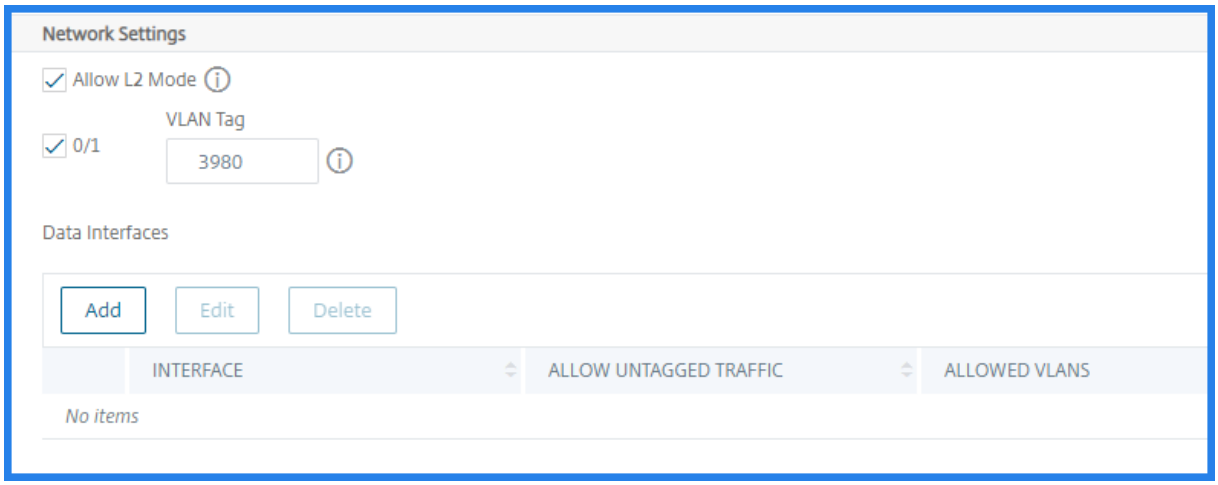
为实例选择所需的网络设置：

- 在网络设置下允许 **L2** 模式 -您可以在 Citrix ADC 实例上允许 L2 模式。在网络设置下选择允许 L2 模式。在登录实例并启用 L2 模式之前。有关详细信息，请参阅在 Citrix ADC 实例上允许使用 L2 模式。

  > 注意：
  >
  > 如果您为实例禁用 L2 模式，则必须登录该实例并从该实例禁用 L2 模式。否则，它可能会导致在重新启动实例后所有其他 Citrix ADC 模式被禁用。

- **0/1** -在 **VLAN** 标记中，为管理接口指定 VLAN ID。
- **0/2** -在 **VLAN** 标记中，为管理接口指定 VLAN ID。

默认情况下，接口 **0/1** 和 **0/2** 处于选中状态。



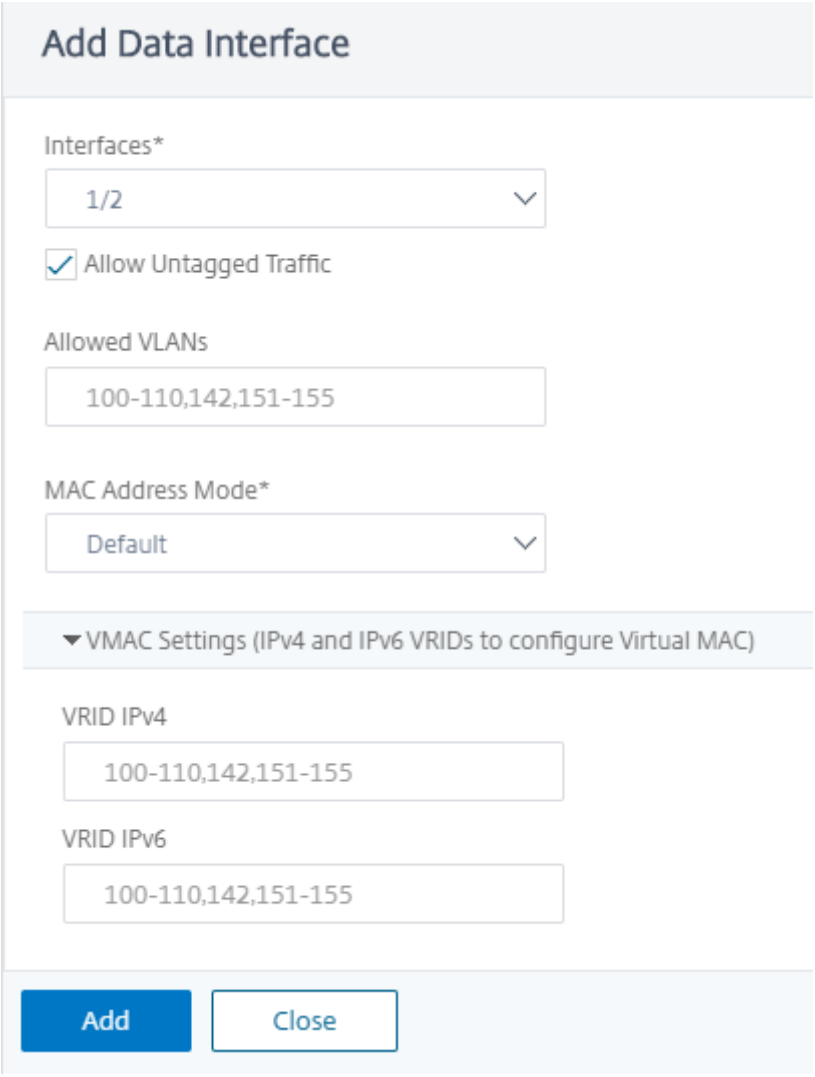
在 数据接口中，单击 添加以添加数据接口并指定以下内容：

- 接口 -从列表中选择接口。

  > 注意：
  >
  > 添加到实例的接口的接口 ID 不一定与 SDX 设备上的物理接口编号相对应。
  >
  > 例如，与实例 1 关联的第一个接口是 SDX 接口 1/4，当您查看该实例中的接口设置时，它显示为接口 1/1。此接口表示它是您与 instance-1 关联的第一个接口。

- 允许的 **VLAN** -指定可与 Citrix ADC 实例关联的 VLAN ID 列表。
- **MAC** 地址模式 -为实例分配 MAC 地址。选择以下选项之一：
  - 默认 -Citrix Workspace 分配 MAC 地址。
  - 自定义 -选择此模式可指定覆盖生成的 MAC 地址的 MAC 地址。
  - 已生成-使用之前设置的基本 MAC 地址生成 MAC 地址。有关设置基本 MAC 地址的信息，请参阅 为接口分配 MAC 地址。
- **VMAC** 设置（用于配置虚拟 **MAC** 的 **IPv4** 和 **IPv6 vRID**）
  - **VRID IPv4** - 标识 VMAC 的 IPv4 VRID。可能的值：1—255。有关详细信息，请参阅在接口上配置 VMacs。

– VRID IPv6 - 标识 VMAC 的 IPv6 VRID。可能的值：1—255。有关详细信息，请参阅在接口上配置 VMacs。



单击添加。

步骤 6-指定管理 VLAN 设置

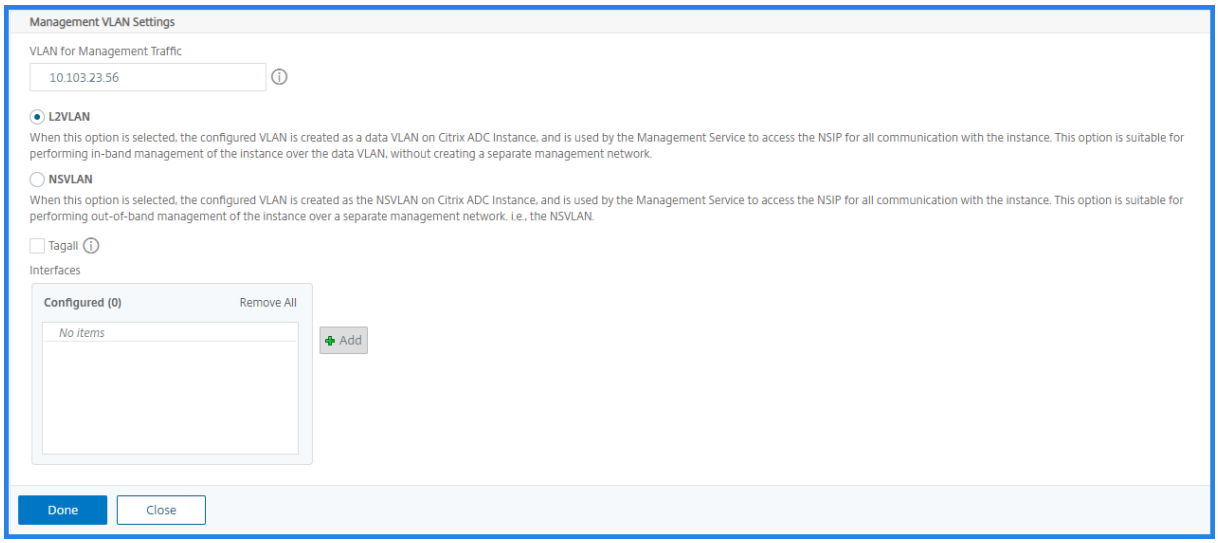
VPX 实例的管理服务和管理地址 (NSIP) 位于同一子网中，通信通过管理接口进行。

如果管理服务和实例位于不同的子网中，请在配置 VPX 实例时指定 VLAN ID。因此，当实例处于活动状态时，可通过网络访问该实例。

如果您的部署要求 NSIP 只能在配置 VPX 实例时通过选定的接口访问，请选择 **NSVLAN**。而且，NSIP 变得无法通过其他接口访问。

- HA 检测信号仅在属于 NSVLAN 的接口上发送。
- 只能从 VPX XVA 内部版本 9.3-53.4 及更高版本中配置 NSVLAN。

> 重要
>
> - 置备 VPX 实例后，您无法更改此设置。
> - 如果未选择 **NSVLAN**，**VPX** 实例上的 **`clear config full`** 命令将删除 **VLAN** 配置。

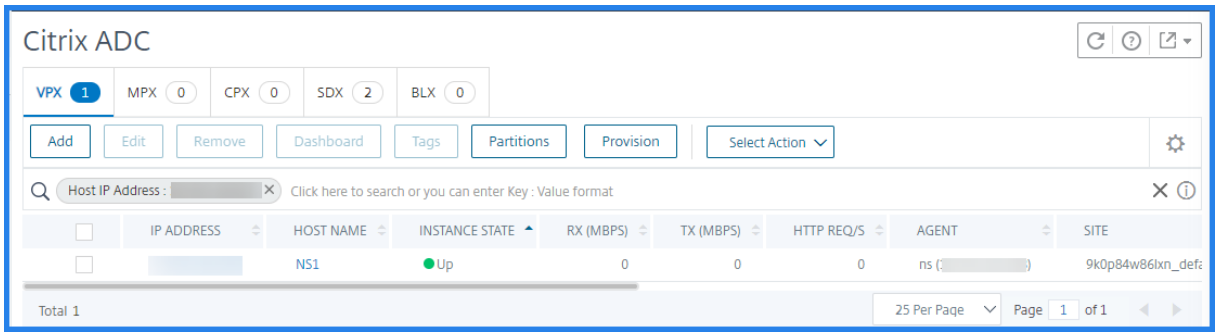


单击“ 完成”以配置 VPX 实例。

查看预配置的 **VPX** 实例

要查看新配置的实例，请执行以下操作：

1. 导航到 网络 **>** 实例 **> Citrix ADC**。
2. 在 **VPX** 选项卡中，按 主机 **IP** 地址属性搜索实例，然后为其指定 SDX 实例 IP。



重新发现多个 **Citrix VPX** 实例

April 23, 2021

您可以在 Citrix 应用程序交付管理 (ADM) 设置中重新发现多个 Citrix VPX 实例。此外，如果要查看多个 Citrix VPX 实例的最新状态和配置，则可以重新发现这些实例。Citrix ADM 服务器将重新发现所有 Citrix VPX 实例，并检查 Citrix 应用程序 Delivery Controller (ADC) 实例是否可访问。

要重新发现多个 **Citrix VPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 服务器的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。默认管理员凭据为 `nsroot` 和 `nsroot`。
3. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ” > “ **VPX** ” 选项卡，然后选择要重新发现的实例。
4. 在 “ 选择操作” 菜单中，单击 “ 重新发现”。
5. 当显示运行 “重新发现” 实用程序的确认消息时，单击 是”。

   屏幕将报告每个 Citrix VPX 实例的重新发现进度。

取消管理实例

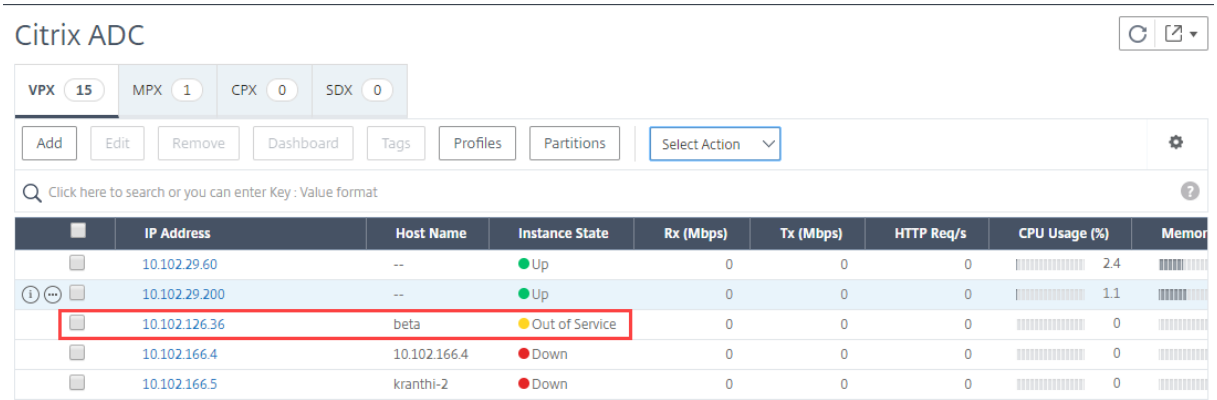
April 23, 2021

如果要停止 Citrix Application Delivery Management (ADM) 和网络中的实例之间的信息交换，则可以取消管理这些实例。

要取消管理实例，请执行以下操作：

导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ” > “ **VPX** ” 选项卡。在实例列表中，右键单击某个实例，然后选择取 消管理，或选择该实例，然后从 **“**选择操作” 列表中选择 “取 消管理”。

所选实例的状态将更改为 “ 停止服务”，如下图所示。



实例不再由 Citrix ADM 管理，也不再与 Citrix ADM 交换数据。

跟踪到实例的路由

April 23, 2021

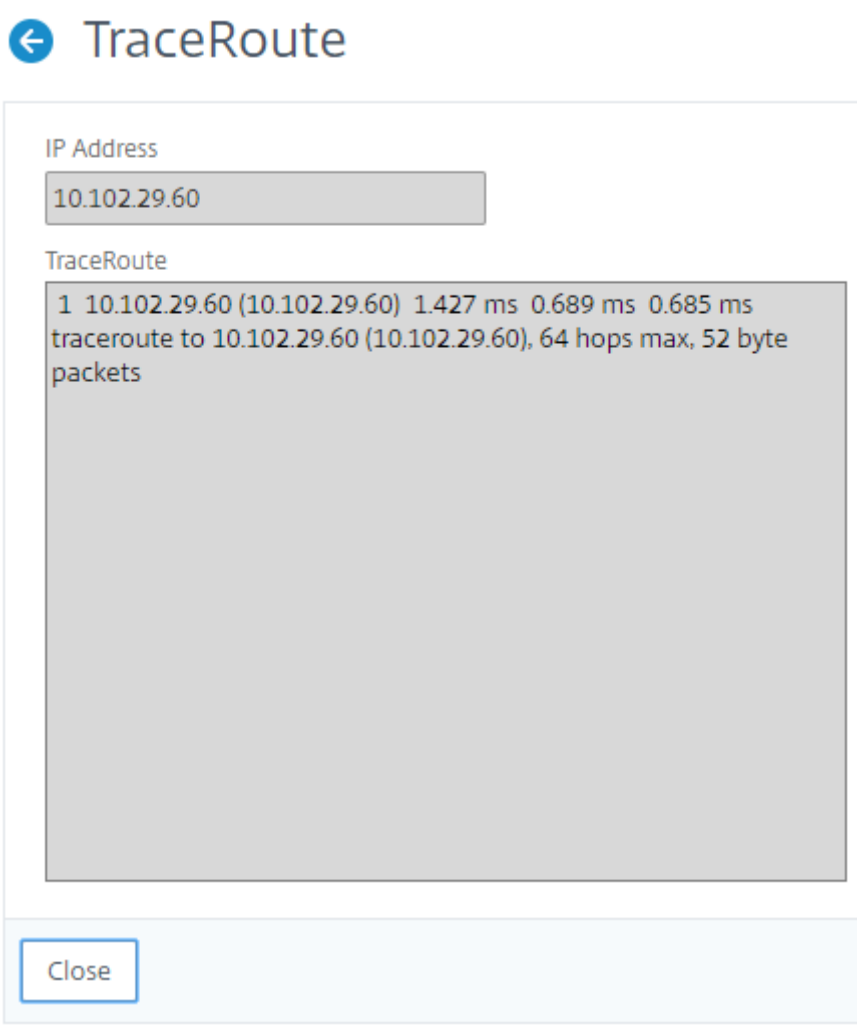
通过跟踪数据包从 Citrix Application Delivery Management (ADM) 到实例的路由，您可以找到到达实例所需的跳数等信息。Traceroute 会跟踪数据包从源到目标的路径。它显示网络跃点列表以及路由中每个实体的主机名和 IP 地址。

Traceroute 也记录数据包从一个跃点传输到另一个跃点所用时间。如果在数据包传输中有任何中断，Traceroute 会显示问题所在位置。

要跟踪实例的路由，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例” > “ **Citrix ADC** ” > “ **VPX** ” 选项卡。
2. 在实例列表中，右键单击某个实例，然后选择 T **racerOute** 或选择该实例，然后从 “ 选择操作” 菜单中单击 T **racerUte**。

TraceRoute 消息框显示到实例的路由以及每跳消耗的时间量（以毫秒为单位）。



事件

April 23, 2021

将 Citrix 应用程序 Delivery Controller (ADC) 实例的 IP 地址添加到 Citrix Application Delivery Management (ADM) 时，Citrix ADM 会发送一个 NITRO 调用，并隐式地将自身添加为实例接收陷阱或事件的陷阱目标。

事件表示托管 Citrix ADC 实例上发生的事件或错误。例如，当发生系统故障或配置更改时，系统会在 Citrix ADM 服务器上生成并记录事件。Citrix ADM 中接收的事件显示在“事件摘要”页面（“网络”>“ 事件”）中，所有活动事件都显示在“事件消息”页面（“网络”>“ 事件**”>“**事件消息”）中。

Citrix ADM 还会检查实例上生成的事件，以形成不同严重性级别的警报。然后，这些警报将显示为消息，其中一些可能需要立即注意。例如，系统故障可以归类为“严重”事件严重性，需要立即解决。

可以配置规则以监视特定事件。规则使监控跨 Citrix ADC 基础架构生成的事件变得更加轻松，这些事件可能很多。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、Citrix ADC 实例、类别、故障对象、配置命令和消息。

您还可以确保在特定时间间隔内为某个事件触发多个通知，直到事件被清除。作为额外措施，您可以使用特定的主题行和用户消息自定义电子邮件，然后上传附件。

使用事件控制板

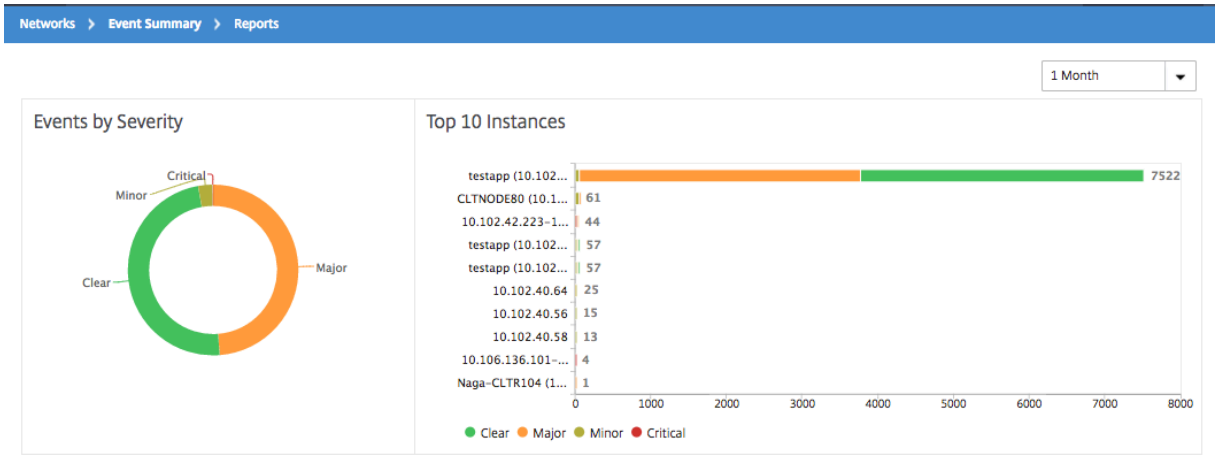
April 23, 2021

作为网络管理员，您可以查看 Citrix 应用程序 Delivery Controller (ADC) 实例上的配置更改、登录条件、硬件故障、阈值违规和实体状态更改等详细信息，以及特定实例上的事件及其严重性。您可以使用 Citrix Application Delivery Management (ADM) 的事件仪表板查看为所有 Citrix ADC 实例上的关键事件严重性详细信息生成的报告。

要查看事件控制板上的详细信息：

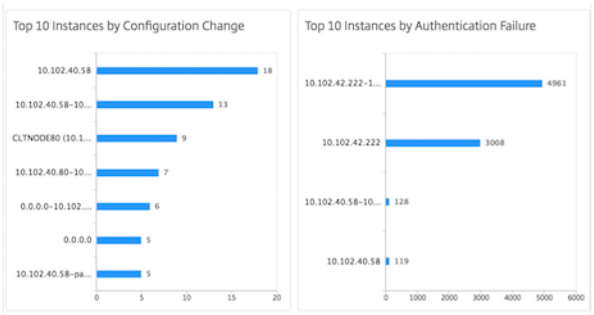
导航到 网络 > 事件 > 报表。

控制板上的“Top 10 Devices”（前 10 位的设备）图中显示按实例上生成的事件数排在前 10 位的实例的报告。您可以单击图表上的实例以查看事件严重性的更多详细信息。

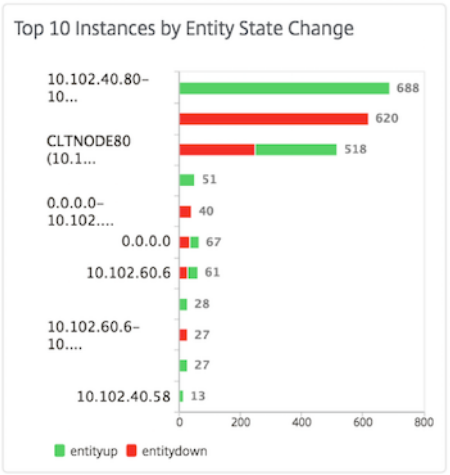


可以通过导航到 Citrix ADC 实例类型（网络 > 事件 > 报告 > **Citrix ADC/Citrix ADC SDX/Citrix ADC SD-WAN WO**）查看更多详细信息，以查看以下内容：

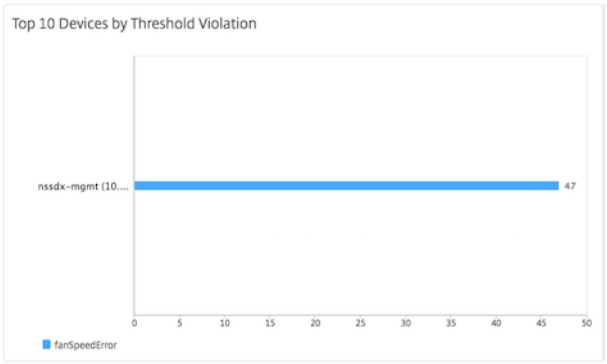
- Top 10 devices by hardware failure（按硬件故障排在前 10 位的设备）
- Top 10 devices by configuration change（按配置变更排在前 10 位的设备）
- Top 10 devices by authentication failure（按身份验证失败排在前 10 位的设备）



- Top 10 devices by entity state changes（按实体状态变化排在前 10 位的设备）



- Top 10 devices by threshold violation（按阈值违反排在前 10 位的设备）



设置事件的活动年龄

April 23, 2021

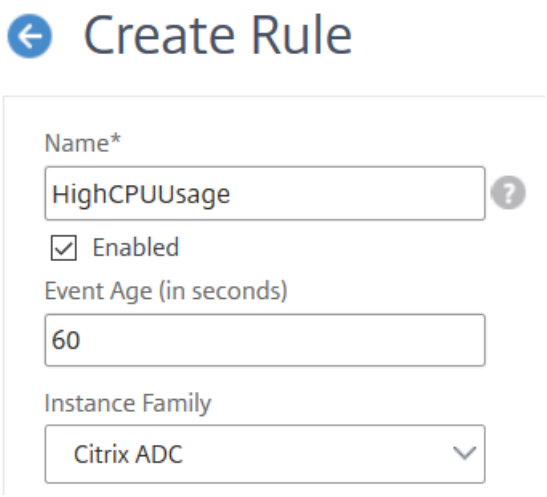
您可以设置事件时间选项以指定时间间隔（以秒为单位）。Citrix ADM 会监视装置，直到设置的持续时间，并且仅当事件时间超过设定的持续时间时才会生成事件。

> 注意：
>
> 事件时间的最小值为 60 秒。如果将 “事 件时间” 字段保留为空，则事件发生后立即应用事件规则。

例如，假设您希望管理各种 ADC 设备，并在任何虚拟服务器停机 60 秒或更长时收到电子邮件通知。您可以创建具有必要筛选器的事件规则，并将规则的事件期限设置为 60 秒。然后，每当虚拟服务器停机 60 秒或更长时间时，您都会收到一封电子邮件通知，其中包含实体名称、状态更改和时间等详细信息。

要在 **Citrix ADM** 中设置事件期限，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 事件” > “ 规则”，然后单击 “ 添加”。
2. 在 **Create Rule**（创建规则）页面上，设置规则参数。
3. 指定事件期限（以秒为单位）。



确保在“ 类别”部分中设置所有共同相关陷阱，并在设置事件年龄时在“严 重性”部分中设置相应的严重性。在前面的示例中，选择 `entityup`、`entitydown` 和 `entityofs` 陷阱。

计划事件筛选器

April 23, 2021

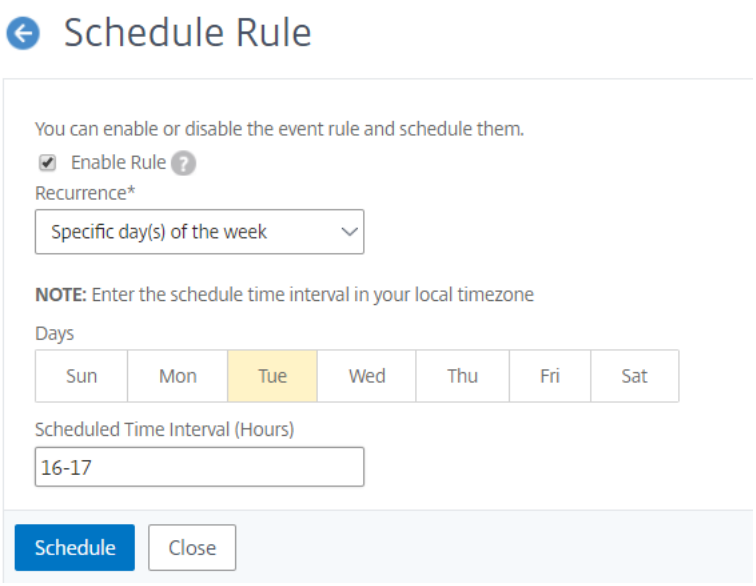
为规则创建筛选器后，如果不希望 Citrix Application Delivery Management (ADM) 服务器在每次生成的事件满足筛选条件时发送通知，则可以将筛选器安排为仅在特定时间间隔（如每日、每周或每月）触发。

例如，如果为实例上的不同应用程序计划了在不同时间进行系统维持活动，实例可能会生成多个警报。

如果您为这些警报配置了筛选器并为这些筛选器启用了电子邮件通知，则在 Citrix ADM 收到这些陷阱时，服务器会发送大量电子邮件通知。如果希望服务器仅在特定的时间段发送这些电子邮件通知，可以通过计划过滤器来实现。

要使用 **Citrix ADM** 调度筛选器，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 事件” > “ 规则”。
2. 选择要为其计划过滤器的规则，并单击 **View Schedule**（查看计划）。
3. 在 **Scheduled Rule**（计划的规则）页面上，单击 **Schedule**（计划）并指定以下参数：
   - 启用规则 — 选中此复选框可启用计划事件规则。
   - **Recurrence**（定期循环）- 计划规则的时间间隔。选择一周中的特定日期或一个月中的特定日期。
   - 天数：选择要运行规则的星期几。您可以选择多天。
   - 日期：键入日期。可以键入多个日期作为逗号分隔值。
   - 计划时间间隔（小时） -小时，计划规则的时间（使用 24 小时格式）。
4. 单击 **Schedule**（计划）。



为事件设置重复电子邮件通知

April 23, 2021

为了确保所有严重事件都被解决且没有重要电子邮件通知丢失，可以选择为满足所选择条件的事件规则发送重复的电子邮件通知。例如，如果为涉及磁盘故障的实例创建了事件规则，并希望在问题解决之前一直收到通知，可以选择接收有关那些事件的重复电子邮件通知。

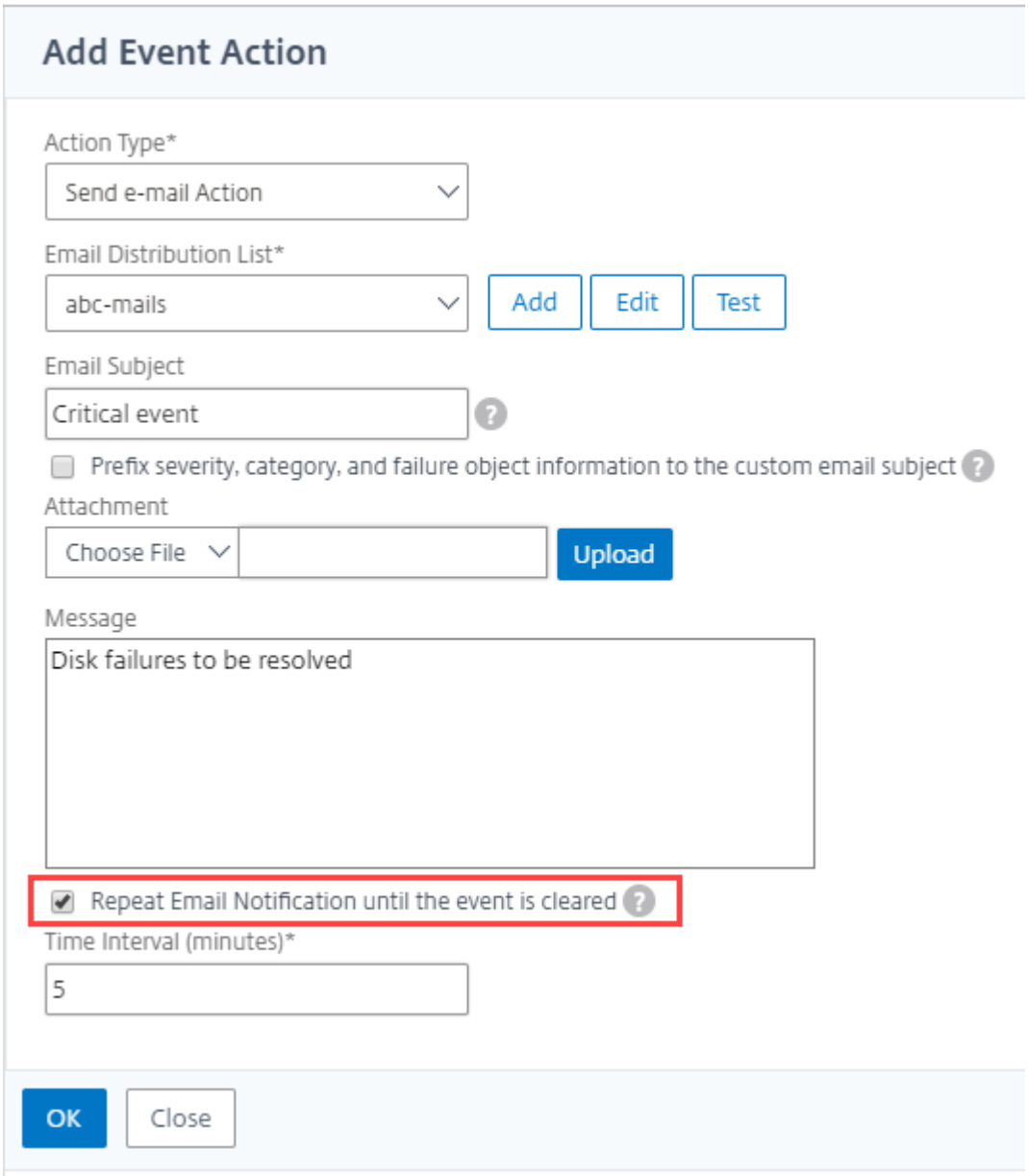
这些电子邮件通知会按预定义的时间间隔重复发送，直到收件人确认看到通知或事件规则被清除。

> 注意
>
> 只有当存在等效的“清除”陷阱集并从 Citrix 应用程序 Delivery Controller (ADC) 实例发送时，才能自动清除事件。
>
> 要手动清除事件，可以执行以下操作：
>
> - 导航到 网络” > “活动” > “活动摘要”，选择一个 类别，然后在类别中选择一个活动，然后单击 清除”。
> - 或者，导航到 “网络” > “事件” > “事件消息”。选择一个实例类型，然后从下面的网格中选择一个事件，然后单击 清除”。

要设置来自 **Citrix ADM** 的重复电子邮件通知，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “ 网络” > “ 事件” > “ 规则”，然后单击 “ 添加” 以创建规则。
2. 在 **Create Rule**（创建规则）页面上，设置规则参数。
3. 在 事件规则操作下，单击 添加操作。然后，从 操作类型” 下拉列表中选择 “发送电子邮件操作” 并选择电子邮件通讯组列表。

4. 您还可以在传入事件满足配置的规则时添加自定义的主题行和用户消息，以及将附件上载到您的电子邮件。
5. 选中 **Repeat Email Notification until the event is cleared**（重复发送电子邮件通知，直到事件被清除）复选框。



隐藏事件

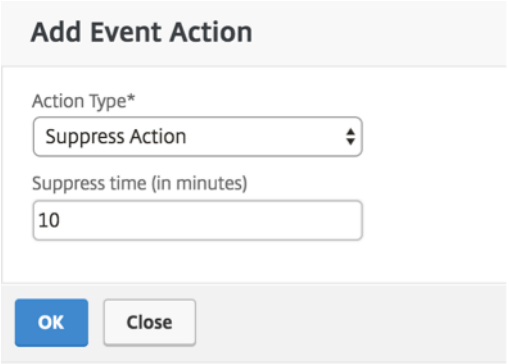
April 23, 2021

选择“隐藏操作”事件操作时，可以配置一个时间段（以分钟为单位），该时段将隐藏或删除某个事件。可以最短阻止事件 1 分钟。

> 注意：
>
> 您还可以将禁止时间配置为 0 分钟，这意味着无限时间。如果未指定任何持续时间，Citrix ADM 将隐藏时间视为零，并且永远不会过期。

要通过使用 **Citrix ADM** 隐藏事件，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “ 网络” > “ 事件” > “ 规则”。单击添加。
2. 指定创建规则所需的所有参数。
3. 在 **Event Rule Actions**（事件规则操作）下方，单击 **Add Action**（添加操作）为事件分配通知操作。
4. 在添加事件操作页面上，从操作类型下拉列表中选择隐藏操作，然后指定必须禁止事件的时间段（以分钟为单位）。
5. 单击确定。



创建事件规则

April 23, 2021

可以配置规则以监视特定事件。通过规则，可以更轻松地监视在您的基础架构中生成的大量事件。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。您可以创建筛选器的条件包括：严重性、Citrix Application Delivery Controller (Citrix ADC) 实例、类别、故障对象、配置命令和消息。

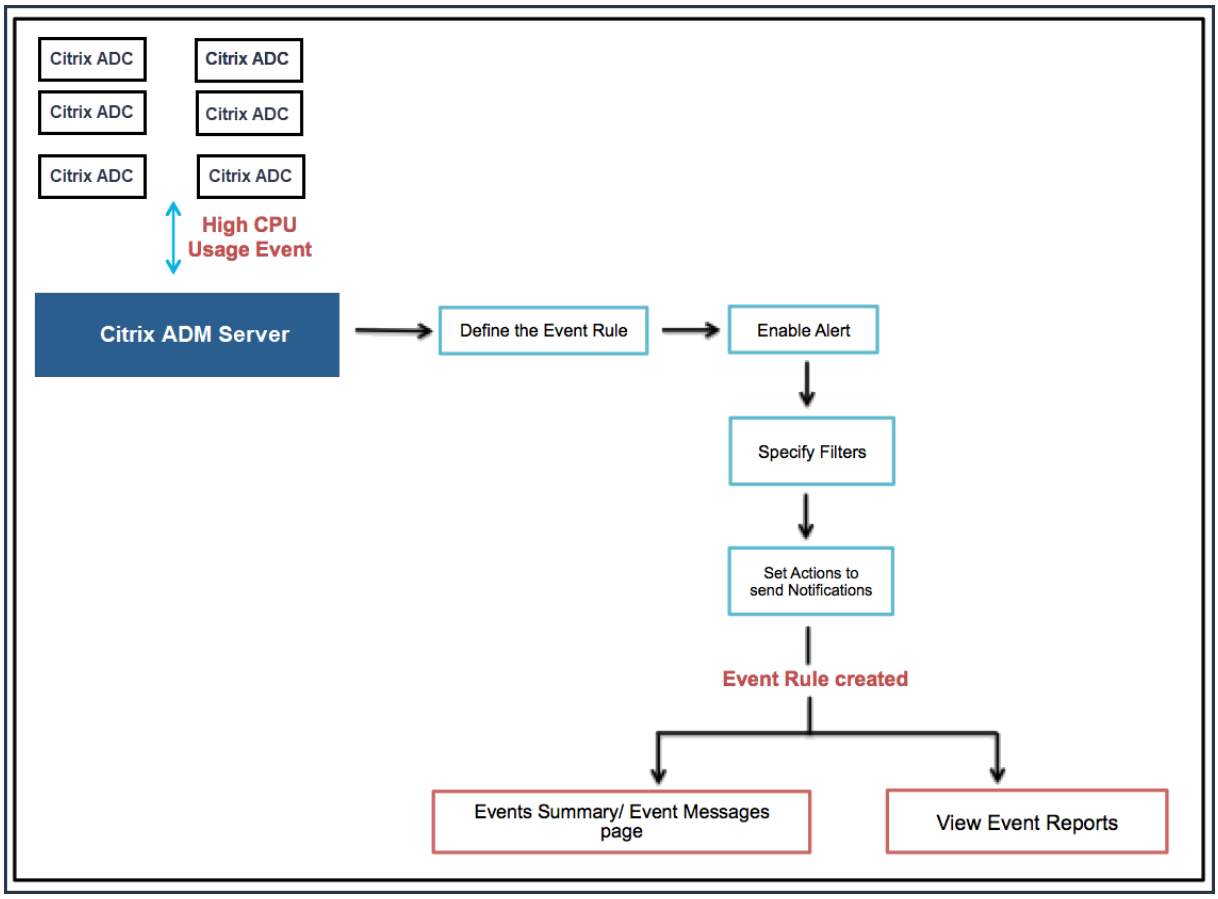
可以为事件分配以下操作：

- 发送电子邮件操作：发送与筛选条件匹配的事件的电子邮件。
- 发送陷阱操作：向外部陷阱目标发送或转发 SNMP 陷阱
- 运行命令操作：当传入事件满足配置的规则时运行命令。
- 执行作业操作：运行作业适用于与您指定的筛选条件匹配的事件。
- 隐藏操作：在特定时间段内禁止删除事件。

- 发送 **Slack** 通知：针对符合筛选条件的事件，在配置的 Slack 通道上发送通知。
- 发送寻呼工作通知：根据与筛选条件匹配的事件的 PageRatch 配置发送事件通知。
- 发送 **ServiceNow** 通知：为符合筛选条件的事件自动生成 ServiceNow 事件。

有关详细信息，请参阅添加事件规则操作。

您还可以设置以指定的时间间隔重新发送通知，直到清除了事件。您还可以使用特定的主题行、用户消息和附件自定义电子邮件。



例如，作为管理员，如果特定 Citrix ADC 实例的“高 CPU 使用率”事件可能会导致 Citrix ADC 实例中断，则您可能希望监视这些事件。可以执行以下操作：

- 创建一个规则来监视实例，并指定在发生“CPU 使用率高”类别中的事件时向您发送电子邮件通知的操作。
- 安排规则在特定时间运行，例如在上午 11 点到晚上 11 点之间运行，以便不会在每次生成事件时通知您。

配置事件规则涉及以下任务：

1. 定义规则
2. 选择规则检测的事件的严重性
3. 指定事件的类别
4. 指定应用规则的 Citrix ADC 实例

5. 选择失败对象
6. 指定高级筛选器
7. 指定规则检测到事件时采取的操作

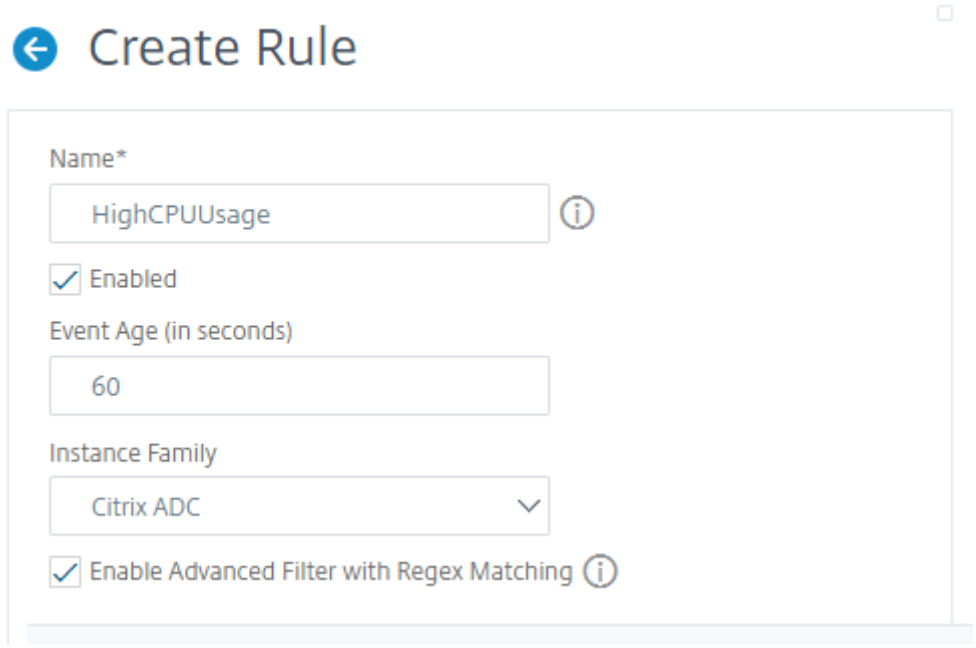
步骤 **1-**定义事件规则

导航到 网络 > 事件 > 规则”，然后单击 添加。如果要启用规则，请选中 启用规则复选框。

您可以设置“事 件时间”选项以指定 Citrix ADM 刷新事件规则的时间间隔（以秒为单位）。

> 注意：
>
> 事件时间的最小值为 60 秒。如果将“事 件时间”字段保留为空，则事件发生后立即应用事件规则。

根据上述示例，每次 Citrix ADC 实例发生“CPU 使用率高”事件时，您可能希望收到电子邮件通知。您可以将事件期限设置为 60 秒，以便每次 Citrix ADC 实例具有 60 秒或更长时间的“CPU 使用率高”事件时，您都会收到包含事件详细信息的电子邮件通知。



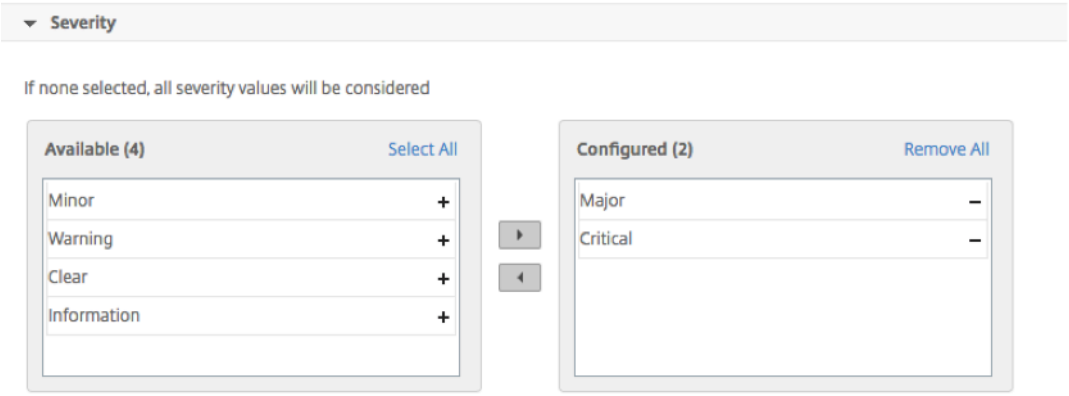
您还可以按 实例系列筛选事件规则，以跟踪 Citrix ADM 从中接收事件的 Citrix ADC 实例。

如果要包含星号 (*) 模式匹配以外的正则表达式，请选择 启用使用正则表达式匹配的高级筛选器。

步骤 **2-**选择事件的严重性

可以创建使用默认严重性设置的事件规则。“Severity”（严重性）指定要为其添加事件规则的事件的当前严重性。

可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）、Clear（清除）及 Information（信息）。

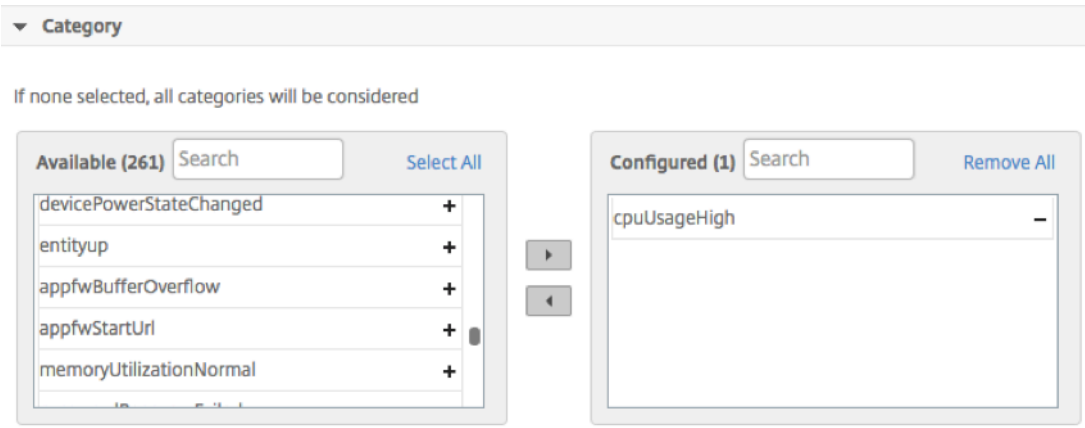


> 注意
>
> 您可以为一般事件和高级特定事件配置严重性。要修改 Citrix ADM 上管理的 Citrix ADC 实例的事件严重性，请导航至 网络 > 事件设置。选择要为其配置事件严重性的类别，然后单击配置严重性。分配新的严重性级别，然后单击确定”。

步骤 **3-**指定事件类别

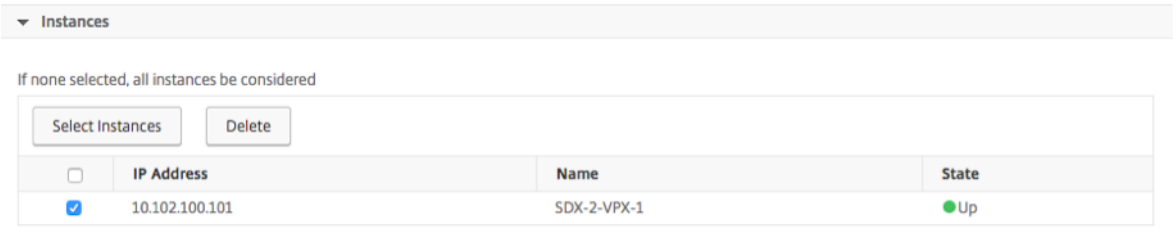
您可以指定 Citrix ADC 实例生成的事件的类别或类别。所有类别都在 Citrix ADC 实例上创建。然后，这些类别将使用 Citrix ADM 进行映射，该 ADM 可用于定义事件规则。选择要考虑的类别，然后将其从 可用表移动到 已配置表。

在上述示例中，您需要从显示的表中选择 “cpuUsageHigh” 作为事件类别。



步骤 **4-**指定 **Citrix ADC** 实例

选择要为其定义事件规则的 Citrix ADC 实例的 IP 地址。在 “实 例” 部分，单击 “ 选择实例”。在 “选 择实例页面中，选择您的实例，然后单击 “选 择。



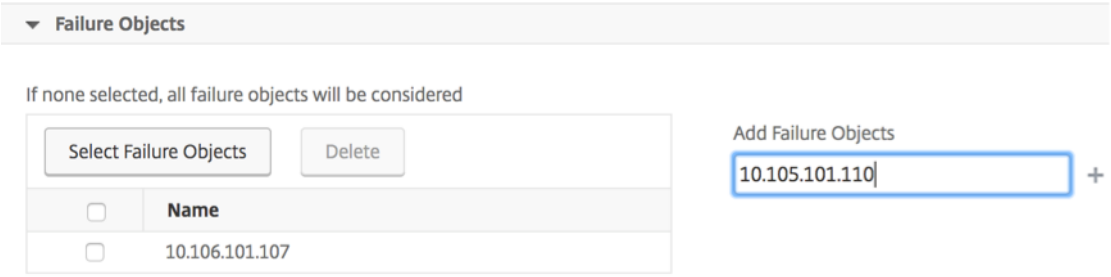
步骤 **5**-选择失败对象

您可以从提供的列表中选择失败对象，也可以添加已为其生成事件的失败对象。您还可以指定正则表达式来添加失败对象。根据指定的正则表达式，失败对象会自动添加到列表中。失败对象是已为其生成事件的实体实例或计数器。

> 重要信息：
>
> 要使用正则表达式列出失败对象，请在中选择 启用具有正则表达式匹配的高级筛选器 [步骤 1()]。

失败对象会影响事件的处理方式，并确保它反映通知的确切问题。使用此过滤器，您可以快速跟踪故障对象上的问题并确定问题的原因。例如，如果用户有登录问题，则此处的失败对象是用户名或密码，例如 `nsroot`。

此列表可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、证书相关事件的证书名称等。

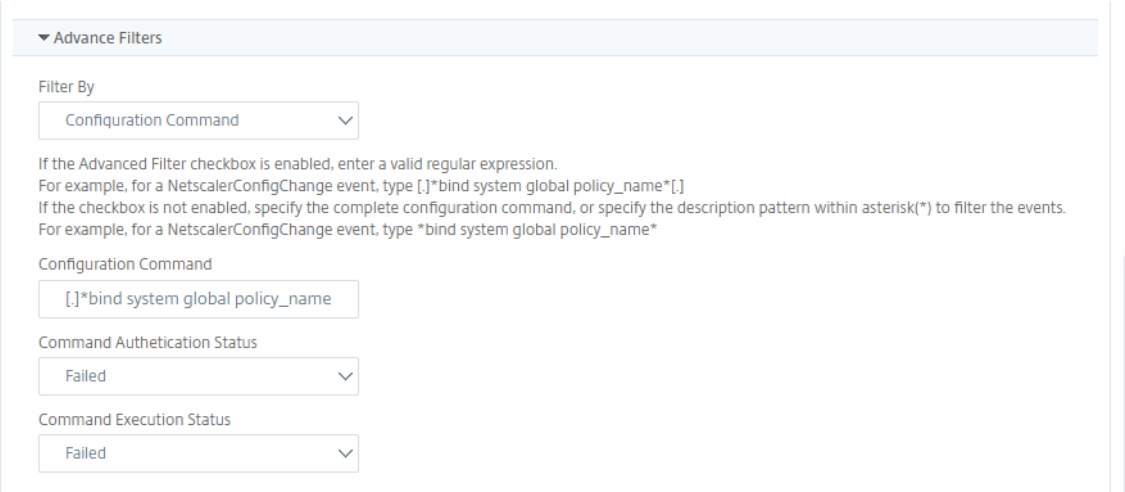


步骤 **6**-指定高级筛选器

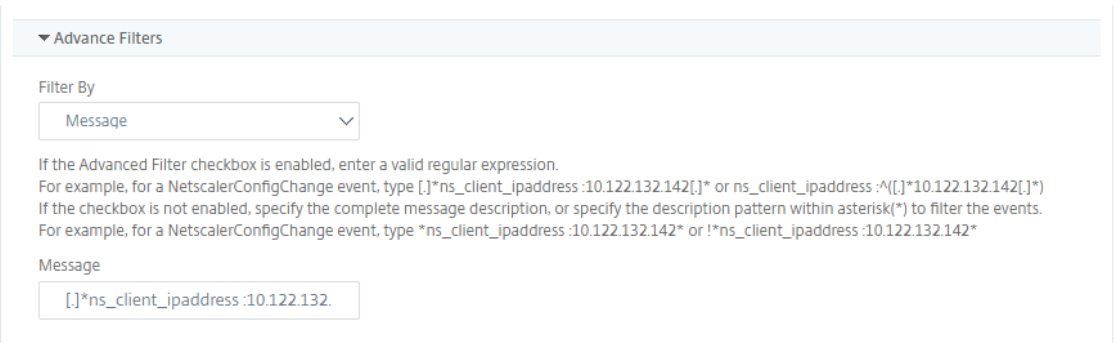
您可以按以下内容进一步过滤事件规则：

- 配置命令 -可以指定完整的配置命令，也可以指定正则表达式来筛选事件。

  您可以根据命令的身份验证状态和/或其执行状态进一步筛选事件规则。例如，对于 `NetscalerConfigChange event`，键入 `[.]*bind system global policy_name[.]*`。



- 消息-您可以指定完整的消息说明，或者指定正则表达式来筛选事件。
  例如，对于某个 `NetscalerConfigChange` 事件，键入 `[.]*ns_client_ipaddress :10.122.132.142[.]* or ns_client_ipaddress :^([.]*10.122.132.142[.]*)`。



步骤 7-添加事件规则操作

您可以添加事件规则操作来为事件分配通知操作。当某个事件满足您在上面设置的已定义过滤条件时，将会发送或执行这些通知。您可以添加以下事件操作：

- 发送电子邮件操作
- Send Trap Action（发送陷阱操作）
- Run Command Action（运行命令操作）
- 运行作业操作
- Suppress Action（阻止操作）
- 发送 Slack 通知
- 发送 PageerTuty 通知
- 发送 ServiceNow 通知

设置电子邮件事件规则操作

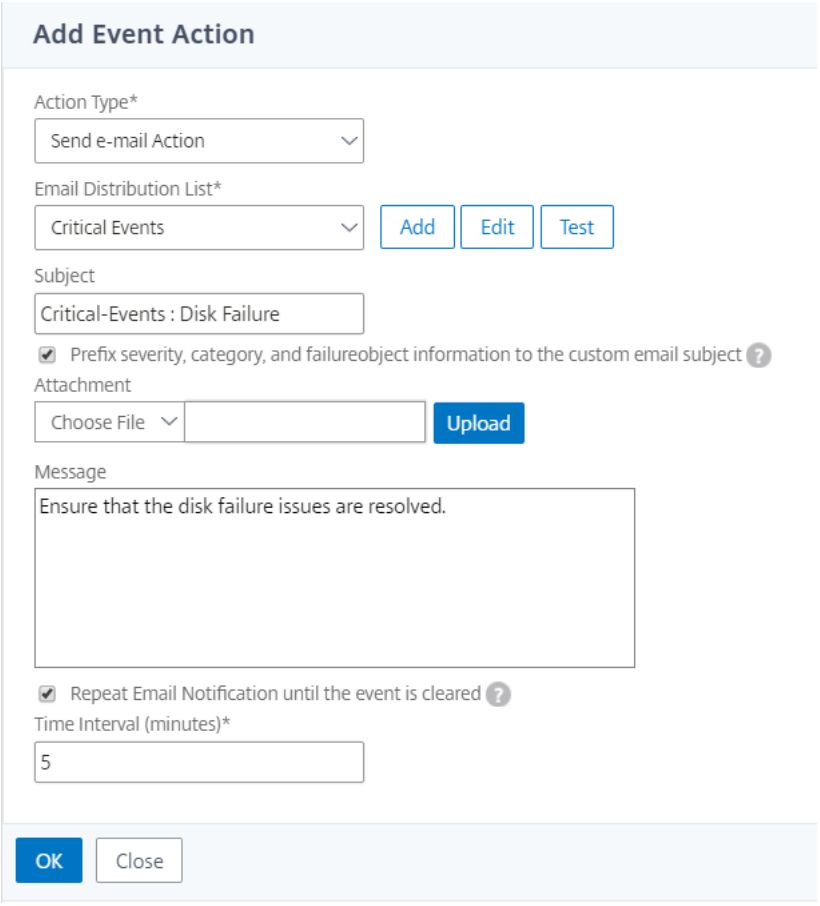
选择“发送电子邮件操作”事件操作类型时，当事件满足定义的筛选条件时，将触发电子邮件。您需要通过提供邮件服务器或邮件配置文件详细信息来创建电子邮件通讯组列表，也可以选择先前创建的电子邮件通讯组列表。

由于 Citrix ADM 中配置了大量虚拟服务器，因此您每天可能会收到大量电子邮件。电子邮件具有默认主题行，提供有关事件严重性、事件类别和失败对象的信息。但主题行不包含有关这些事件来源的虚拟服务器名称的任何信息。您现在可以选择包含一些附加信息，如受影响实体的名称，即失败对象的名称。

您还可以添加自定义主题行和用户消息，并在传入事件与配置的规则匹配时将附件上传到电子邮件。

在发送事件通知的电子邮件时，您可能希望发送测试电子邮件来测试配置的设置。“测试”按钮现在允许您在配置电子邮件服务器、关联的分布式列表和其他设置后发送测试电子邮件。此功能可确保设置正常工作。

您还可以通过选中“重复电子邮件通知 直到事件被清除为止”复选框来发送符合所选条件的事件规则的重复电子邮件通知，确保所有关键事件都已得到处理，并且不会遗漏重要的电子邮件通知。例如，如果为涉及磁盘故障的实例创建了事件规则，并希望在问题解决之前一直收到通知，可以选择接收有关那些事件的重复电子邮件通知。



设置陷阱事件规则操作

选择 发送陷阱操作”事件操作类型时，SNMP 陷阱将被发送或转发到外部陷阱目标。通过定义陷阱通讯组列表（或陷阱目标和陷阱配置文件详细信息），当事件满足定义的过滤条件时，陷阱消息将发送到特定陷阱侦听器。

设置运行命令操作

选择 “ 运行命令操作” 事件操作时，可以为符合特定筛选条件的事件创建可在 Citrix ADM 上运行的命令或脚本。

您还可以为 运行命令操作” 脚本设置以下参数：

参数	说明
$source	此参数对应于接收的事件的源 IP 地址。
$category	此参数对应于过滤器类别下定义的陷阱类型。
$entity	此参数对应于已为其生成事件的实体实例或计数器。它可以包含所有阈值相关事件的计数器名称、所有实体相关事件的实体名称、所有证书相关事件的证书名称。
$severity	此参数对应于事件的严重性。
$failureobj	失败对象影响事件的处理方式，并确保失败对象反映通知的确切问题。这可以用于快速追查问题以及确定失败的原因，而不是仅仅报告原始事件。

> 注意
>
> 在命令执行过程中，这些参数将替换为实际值。

例如，假设您要在负载平衡虚拟服务器状态为 “关 闭” 时设置 run 命令操作。作为管理员，您可能需要考虑通过添加另一个虚拟服务器来提供快速的解决方法。在 Citrix ADM 中，您可以执行以下操作：

- 编写脚本 (.sh) 文件。

  以下是一个示例脚本 (.sh) 文件：

```
#!/bin/sh
source=$1
failureobj=$2
payload='{
"params":{
"warning":"YES" }
,"lbvserver":{
"name":"'$failureobj'","servicetype":"HTTP","ipv46":"x.x.x.x","
   port":"80","td":"","m":"IP","state":"ENABLED","rhistate":"
   PASSIVE","appflowlog":"ENABLED","
bypassaaaa":"NO","retainconnectionsoncluster":"NO","comment":"" }
 }
'
url="http://$source/nitro/v1/config/lbvserver"
```



```
curl --insecure -basic -u nsroot:nsroot -H "Content-type:
    application/json" -X POST -d $payload $url

<!--NeedCopy-->
```

- 将.sh 文件保存在 Citrix ADM 代理上的任何永久位置。例如 /var。
- 在 Citrix ADM 中提供要在满足规则条件时运行的.sh 文件位置。

要设置用于创建新虚拟服务器的 “ 运行命令” 操作，请执行以下操作：

1. 定义规则
2. 选择事件的严重性
3. 选择事件类别 实体
4. 选择配置了虚拟服务器的实例
5. 为虚拟服务器选择或创建故障对象
6. 在 事件规则操作” 下，单击 添加操作” 并从 操作类型” 列表中选择 “运行命令操作”。
7. 在 命令执行列表下，单击 添加。

   此时将显示 “创建命令通讯组列表” 页。

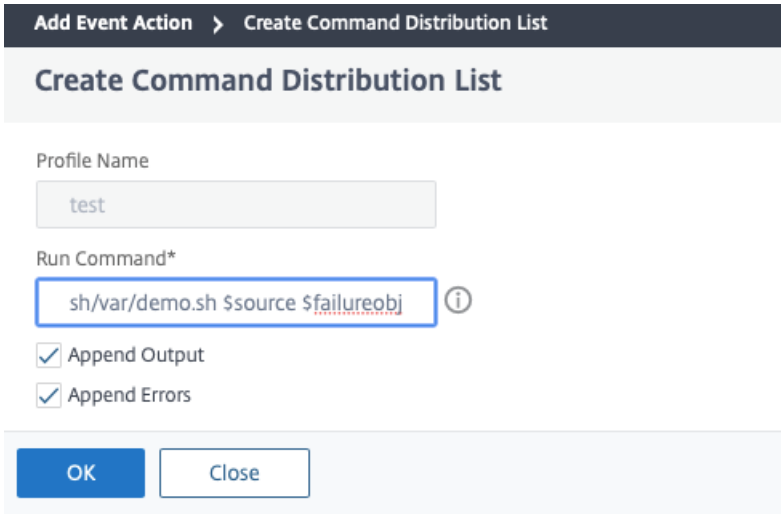
   a) 在 配置文件名称中，指定您选择的名称

   b) 在 运行命令中，指定必须在其中运行脚本的 Citrix ADM 代理位置。例如：/sh/var/demo.sh $source $failureobj。

   c) 选择 “ 追加输出” 和 “ 追加错误”

   > 注意
   >
   > 如果要在 **Citrix ADM** 服务器日志文件中运行命令脚本时存储输出和生成的错误（如果有），则可以启用追加输出” 和 “追加错误” 选项。如果不启用这些选项，Citrix ADM 会丢弃运行命令脚本时生成的所有输出和错误。

   d) 单击创建。
8. 在 添加事件操作” 页面中，单击 确定。

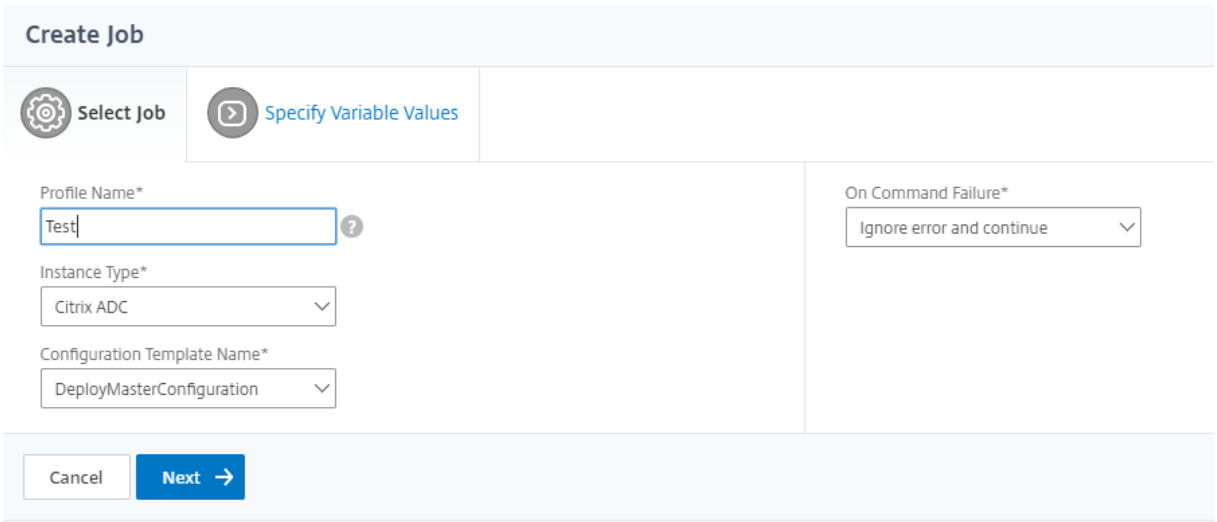


> 注意
>
> 如果要在 **Citrix ADM** 服务器日志文件中运行命令脚本时存储输出和生成的错误（如果有），则可以启用追加输出”和“追加错误”选项。如果不启用这些选项，Citrix ADM 会丢弃运行命令脚本时生成的所有输出和错误。

设置 **Execute** 作业操作

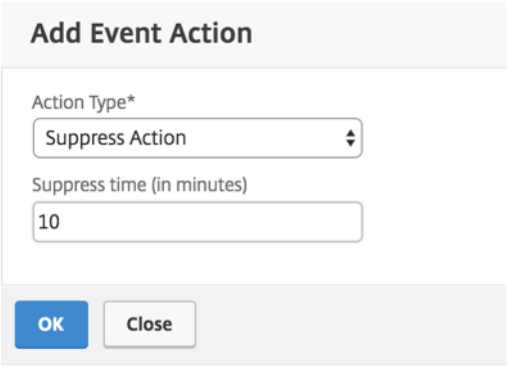
通过创建包含配置作业的配置文件，作业将作为内置作业或自定义作业运行，适用于 Citrix ADC、Citrix ADC SDX 和 Citrix SD-WAN WO 实例，以满足您指定的筛选条件的事件和警报。

1. 在 事件规则操作下，单击 添加操作，然后从 操作类型下拉列表中选择执行作业操作。
2. 在事件满足定义的筛选条件时，使用要运行的作业创建配置文件。
3. 创建作业时，指定配置文件名称、实例类型、配置模板以及作业上的命令失败时要执行的操作。
4. 根据选定的实例类型和所选配置模板，指定变量值，然后单击“ 完成”创建作业。



设置隐藏操作

选择 禁止操作” 事件操作时，可以配置禁止或删除事件的时间段（以分钟为单位）。可以最短阻止事件 1 分钟。



设置来自 **Citrix ADM** 的 **Slack** 通知

通过在 Citrix ADM GUI 中提供配置文件名称和 Webhook URL 来配置所需的 Slack 通道。然后将事件通知发送到此频道。您可以配置多个 Slack 频道来接收这些通知

1. 在 Citrix ADM 中，导航到 “网络” > “事件” > “规则”，然后单击 “添加” 以创建规则。
2. 在 “ 创建规则” 页上，设置规则参数，如严重性和类别。选择需要监视的实例以及故障对象。
3. 在事件规则操作下，单击添加操作。然后，从 “操作类型” 列表中选择 “发送 **Slack** 通知”，然后选择 “ **Slack** 配置文件列表**”**。
4. 您还可以通过单击 “Slack 配置文件列表” 字段旁的 添加来添加 **Slack** 配置文件列表。
5. 键入以下参数以创建配置文件列表：
   a) 配置文件名称。键入要在 Citrix ADM 上配置的配置文件列表的名称
   b) 频道名称。键入要向其发送事件通知的 Slack 频道的名称。
   c) **Webhook URL**。键入您之前输入的频道的 Webhook URL。传入的网络挂钩是将来自外部来源的消息发布到 Slack 的一种简单方法。URL 在内部链接到频道名称，所有事件通知都会发送到此 URL，以便在指定的 Slack 频道上发布。webhook 的一个示例如下：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK
6. 单击 “ 创建”，然后在 “ 添加事件操作” 窗口中单击 “ 确定”。

> 注意
>
> 您还可以通过导航到 “ 系统” > “ 通知” > “Slack 配置文件” 来添加 “ **Slack** 配置文件”。单击 添加并创建配置文件，如前面部分所述。

您可以查看已创建的 Slack 配置文件的状态。

现在已创建具有适当过滤器和定义明确的事件规则操作的事件规则。

设置来自 **Citrix ADM** 的 **PagerDuty** 通知

您可以在 Citrix ADM 中添加 PagerDuty 配置文件作为选项，以根据您的 PagerDuty 配置监视事件通知。PagerDuty 让您可以通过电子邮件、短信、推送通知和调用注册号码配置通知。

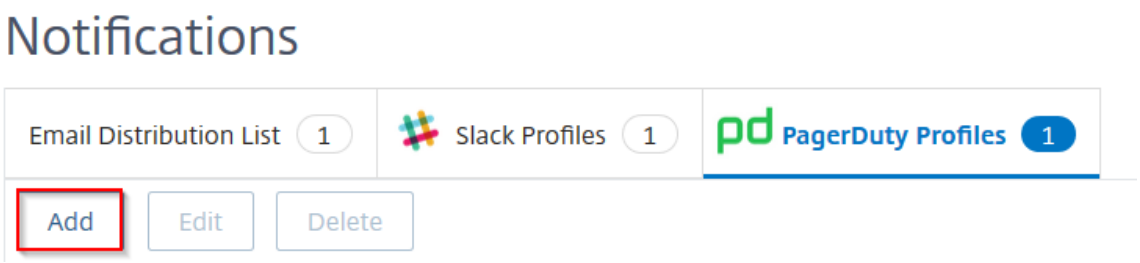
在 Citrix ADM 中添加 PagerDuty 配置文件之前，请确保您已完成了 PagerDuty 中所需的配置。有关详细信息，请参阅PagerDuty 文档。

可以选择您的 PagerDuty 配置文件作为获取以下功能通知的选项之一：

- 事件 — 为 Citrix ADC 实例生成的事件列表。
- 许可证 — 当前处于活动状态、即将过期等许可证的列表。
- **SSL** 证书 — 添加到 Citrix ADC 实例的 SSL 证书列表。

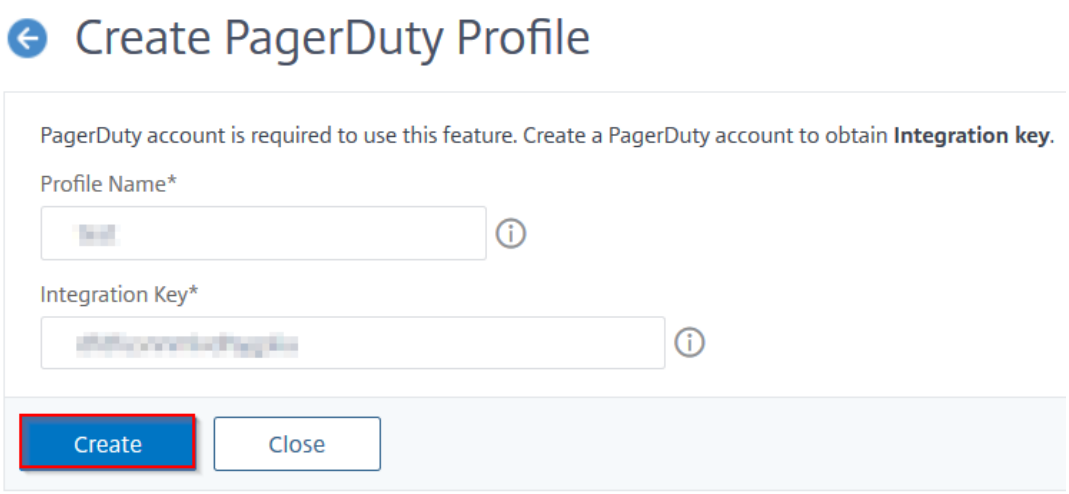
要在 **ADM** 中添加 **PagerDuty** 配置文件，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 定位至 “ 系统” > “ 通知” > “ 寻呼服务配置文件”。
3. 单击 “ 添加” 以创建新的配置文件。



4. 在 “创建 PagerDuty 配置文件” 页面中：
   a) 提供您选择的配置文件名称。
   b) 输入 集成密钥。

      可以从您的 PagerDuty 门户网站获取集成密钥。
   c) 单击创建。



使用案例：

考虑一个情况下，您：

- 想要发送通知到您的 PagerDuty 配置文件。
- 已将调用调用配置为 PagerDuty 中接收通知的选项。
- 希望获取 Citrix ADC 事件的调用通话警报。

要配置：

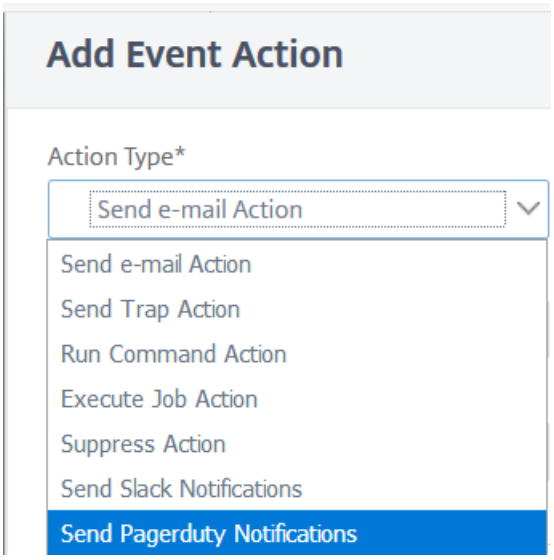
a) 导航到 事件 > 规则”

b) 在 创建规则页面上，配置所有其他参数以创建规则。

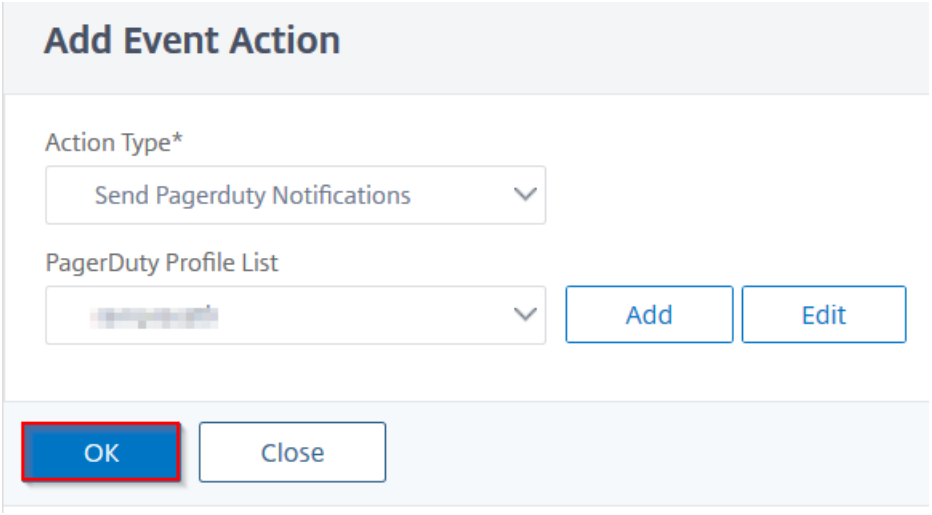
c) 在 创建规则操作” 下，单击 添加操作”。

此时将显示 添加事件操作” 页面。

i. 在操作类型下，选择发送 **PagerDuty** 通知。



ii. 选择您的 PagerDuty 配置文件，然后单击确定。



配置完成后，每当为 Citrix ADC 实例生成新事件时，您都会收到一个调用。通过调用，您可以决定：

- 确认事件
- 将其标记为已解决
- 升级到另一个团队成员

从 **Citrix ADM** 自动生成 **ServiceNow** 事件

可以通过在 Citrix ADM GUI 上选择 ServiceNow 配置文件，为 Citrix ADM 事件自动生成 ServiceNow 事件。必须在 Citrix ADM 中选择 ServiceNow 配置文件才能配置事件规则。

在配置事件规则以自动生成 ServiceNoW 事件之前，请将 Citrix ADM 与 ServiceNow 实例集成。有关详细信息，请参阅为 ServiceNow 配置 ITSM 适配器。

要配置事件规则，请导航到 事件 > 规则。

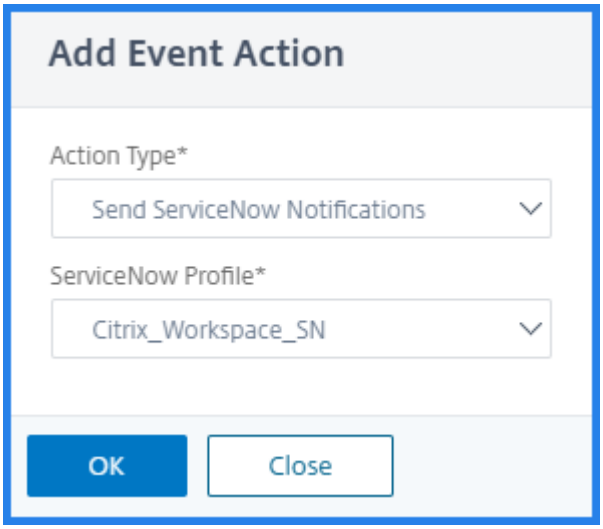
1. 在 创建规则页面上，配置所有其他参数以创建规则。
2. 在 创建规则操作” 下，单击 添加操作”。

   此时将显示 添加事件操作” 页面。

   a) 在 操作类型” 中，选择 发送服务立即通知”。

   b) 在 **ServiceNow** 配置文件中，从列表中选择 **Citrix_Workspace_SN** 配置文件。

   c) 单击确定。



修改 **Citrix ADC** 实例上发生的事件的报告严重性

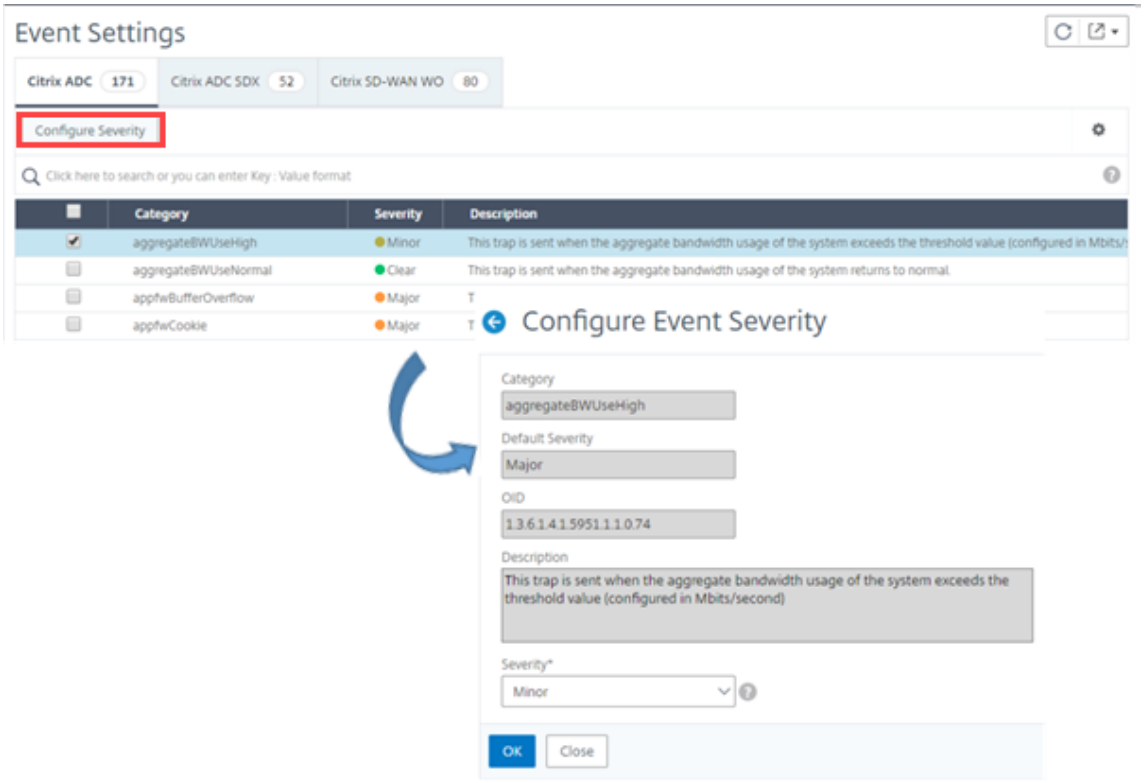
April 23, 2021

您可以管理您的所有设备上生成的事件的报告，以便可以查看有关特定实例上特定事件的事件详细信息，以及根据事件严重性查看报告。可以创建使用默认严重性设置的事件规则，并可以更改严重性设置。可以为一般事件和企业特定的事件配置严重性。

可以定义以下级别的严重性：Critical（严重）、Major（重大）、Minor（较小）、Warning（警告）及 Clear（清除）。

要修改事件严重性：

1. 导航到 网络 **>** 事件 **>** 事件设置。
2. 单击要修改的 Citrix 应用程序 Delivery Controller (ADC) 实例类型的选项卡。然后，从列表中选择类别，然后单击 配置严重性。
3. 在 **Configure Event Severity**（配置事件严重性）中，从下拉列表中选择严重级别。
4. 单击确定。

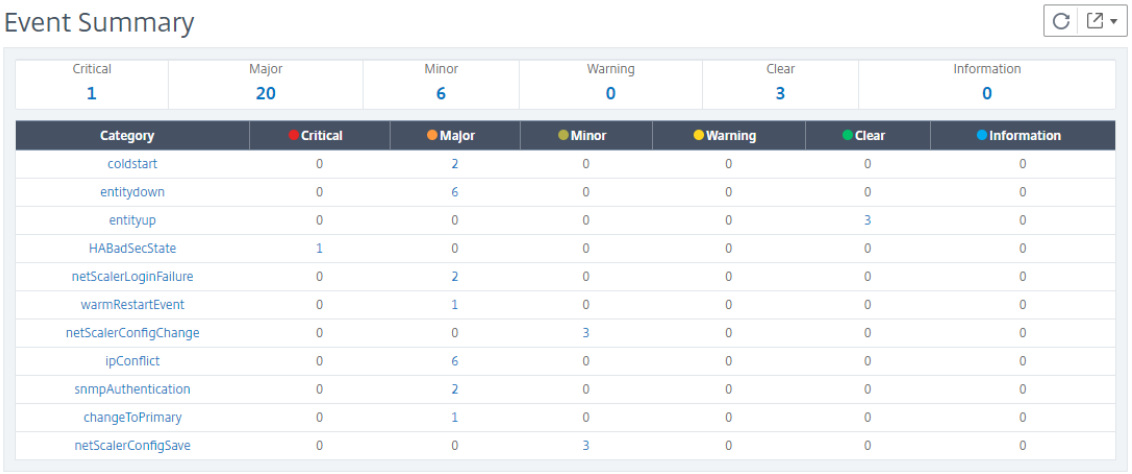


查看事件摘要

April 23, 2021

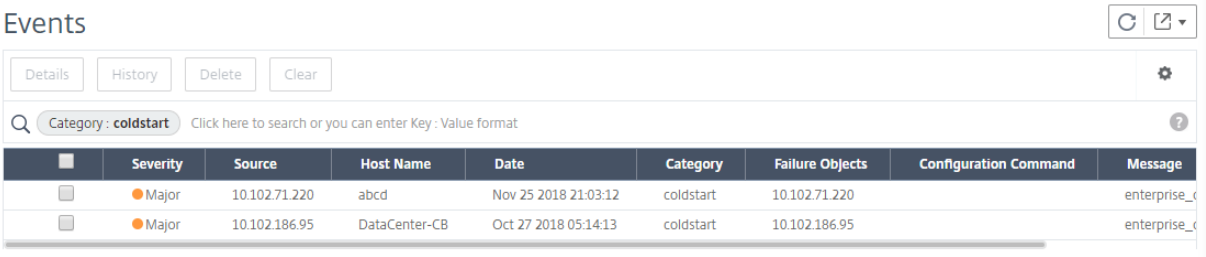
现在，您可以查看“事件摘要”页面，以监视 Citrix Application Delivery Management (ADM) 服务器上收到的事件和陷阱。导航到“ 网络”>“ 事件”。“Events Summary”（事件摘要）页面以表格形式显示以下信息：

- **Citrix ADM** 收到的所有事件的摘要。事件按类别列出，不同的严重性显示在不同的列中：“Critical”（严重）、“Major”（重大）、“Minor”（较小）、“Warning”（警告）、“Clear”（清除）和“Information”（信息）。例如，当 Citrix 应用程序 Delivery Controller (ADC) 实例关闭并停止向 Citrix ADM 服务器发送信息时，将发生严重事件。在活动期间，系统会向管理员发送通知，解释实例关闭的原因、关闭的时间等。然后，该事件记录在“Events Summary”（事件摘要）页面上，您可以在该页面上查看摘要并访问事件的详细信息。



- 每个类别收到的陷阱数量。收到的陷阱数，按严重性分类。默认情况下，从 Citrix ADC 实例发送到 Citrix ADM 的每个陷阱都具有分配的严重性，但作为网络管理员，您可以在 Citrix ADM GUI 中指定其严重性。

如果单击类别类型或陷阱，则会进入
事件页面，在该页面上预先选择类别和严重性等筛选器。此页显示有关事件的详细信息，例如 Citrix ADC 实例的 IP 地址和主机名、接收陷阱的日期、类别、故障对象、配置命令运行以及消息通知。



显示事件严重性和 **SNMP** 陷阱详细信息

April 23, 2021

在 Citrix Application Delivery Management (ADM) 中创建事件及其设置时，可以立即在“事件摘要”页面上查看事件。同样，您可以在基础架构仪表板上查看和监视添加到 Citrix ADCitrix ADM 服务器的所有 Citrix 应用程序 Delivery Controller (ADC) 实例的运行状况、正常运行时间、型号和版本。

在“基础结构”控制板上，您现在可以掩盖不相关的值，以便更轻松地查看和监视信息，如严重程度、运行状况、正常运行时间、型号和 Citrix ADC 实例版本。

例如，具有严重严 重性级别的事件可能很少发生。但是，如果您的网络上发生严重事件，您可能想要对事件的发生地点和时间进一步进行调查、故障排除和监视。如果您选择“Critical”（严重）以外的所有严重级别，则图形将仅显示发生的严重事件。此外，通过单击该图表，您将进入 基于严重性的事件页面，在该页面中，您可以查看有关在您选择的持续时间内发生严重事件的所有详细信息：实例来源、日期、类别和在重要事件发生时发送的消息通知。

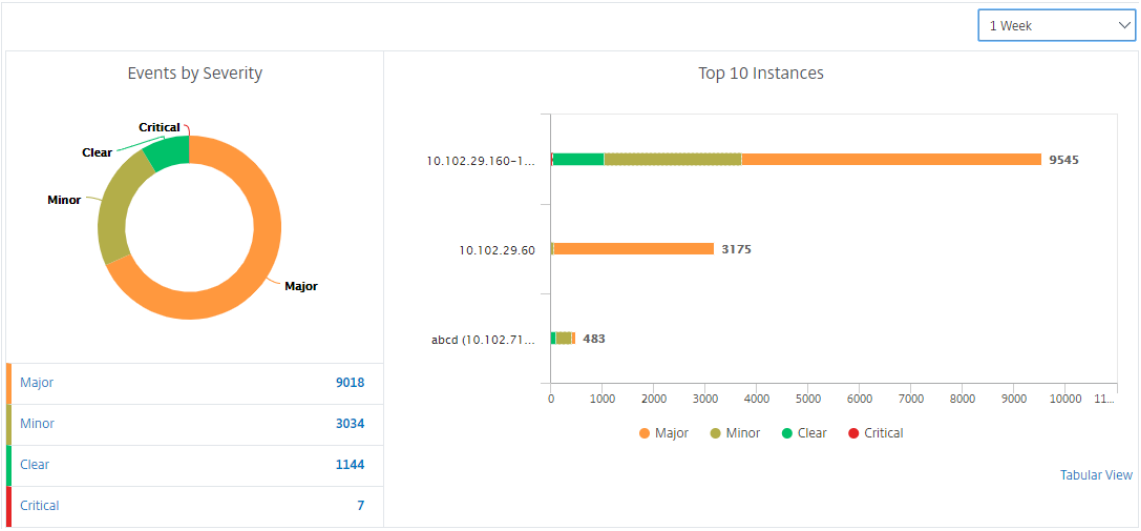
同样，您可以在仪表板上查看 Citrix VPX 实例的运行状况。您可以屏蔽实例已启动并运行的时间段，只显示实例停止工作的时间段。通过单击图表，您将进入该实例的页面，其中已应用 了不服务筛选器，并查看详细信息，如主机名、每秒接收的 HTTP 请求数、CPU 使用率等。您还可以选择实例并查看特定 Citrix 实例的仪表板以了解更多详细信息。

要在 **Citrix ADM** 中按严重性选择特定事件，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到 网络 **>** 仪表板。

   或者，

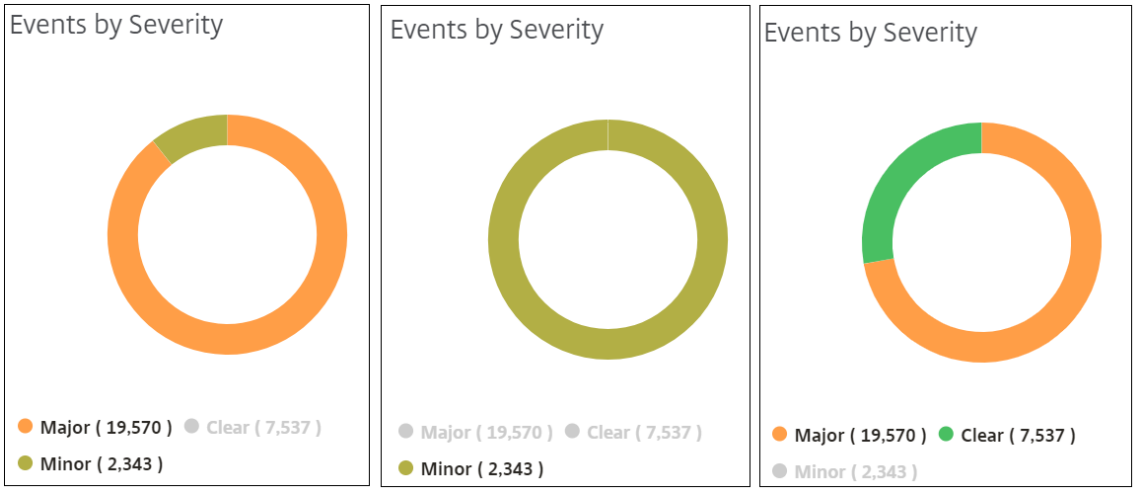
   导航到 网络 **>** 事件 **>** 报告。
3. 从页面右上角的菜单中，选择要按严重程度查看事件的持续时间。



4. “ 按严重程度列出的事件” 圆环图显示按严重程度显示所有事件的可视化表示。不同类型的事件以不同的彩色部分表示，每个部分的长度对应于该严重性类型的事件总数。
5. 您可以单击圆环图表上的每个部分以显示相应的 基于严重性的事件页面，该页面显示所选持续时间内所选严重性的以下详细信息：

   - 实例源
   - 事件日期
   - Citrix ADC 实例生成的事件类别
   - 发送的消息通知

   > 注意
   >
   > 在甜甜圈图下方，您可以看到图表中表示的严重性列表。默认情况下，圆环图显示所有严重性类型的所有事件，因此，列表中的所有严重性类型均突出显示。您可以切换严重性类型以更加轻松地查看和监视您选择的严重性。



要查看 **Citrix ADM** 上的 **Citrix ADC SNMP** 陷阱详细信息，请执行以下操作：

现在，您可以在“ 事件设置”页面上查看从 Citrix ADM 服务器上的托管 Citrix ADC 实例收到的每个 SNMP 陷阱的详细信息。导航到“ 网络”>“ 事件”**>“**事件设置”。对于从您的实例接收的特定陷阱，您可以以表格形式查看以下详细信息：

- 类别 -指定事件所属实例的类别。
- 严重性 -事件的严重性由颜色及其严重性类型表示。
- 说明 -指定与事件关联的消息。

例如，一个陷阱类别为 **MonResptimeoutlowThh** 的事件，陷阱的描述显示为 **“**当监视器探测的响应超时回到正常状态（小于设置的阈值）时，会发送此陷阱。”

查看和导出 **Citrix ADC syslog** 消息

April 23, 2021

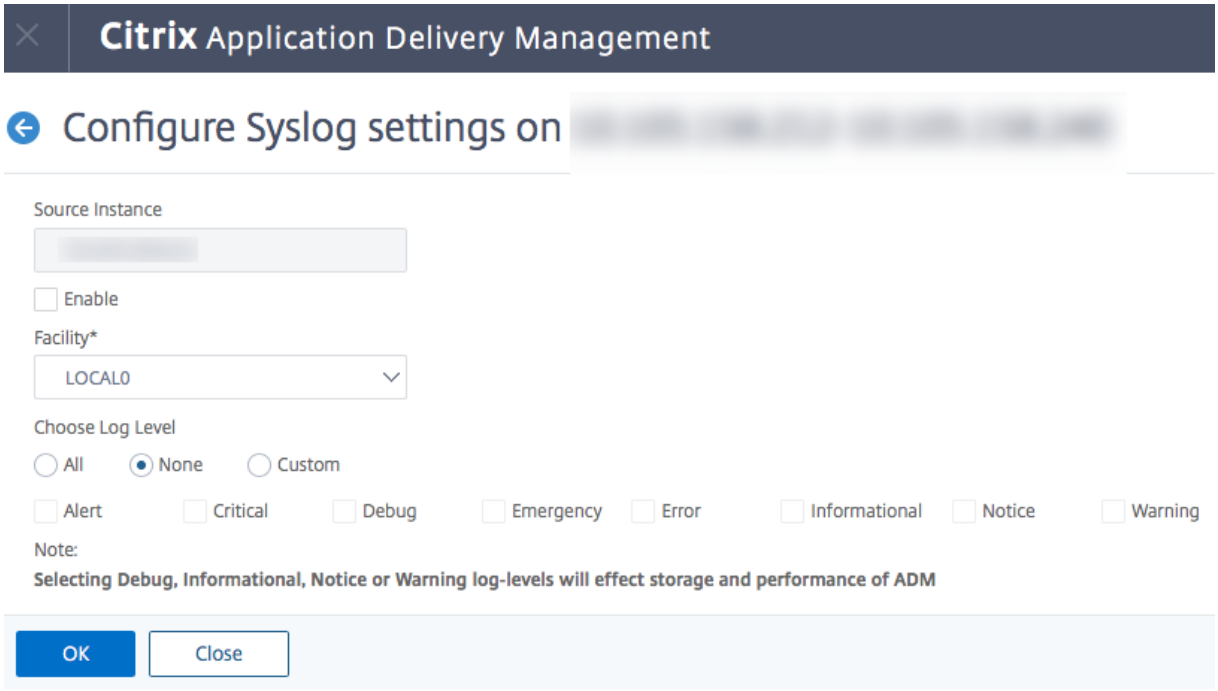
通过 ADM 软件，您可以监控在 Citrix 应用程序 Delivery Controller (ADC) 实例上生成的 syslog 事件。为此，您必须将 ADM 配置为 Citrix ADC 实例的 syslog 服务器。配置 ADM 后，所有系统日志消息都将从 ADC 实例重定向到 ADM。

将 **ADM** 配置为 **syslog** 服务器

请按照以下步骤将 ADM 配置为 syslog 服务器：

1. 在 ADM GUI 中，导航到 **“网络”>“实例”**。
2. 选择希望从中收集并在 Citrix ADM 中显示系统日志消息的 Citrix ADC 实例。
3. 在 选择操作列表中，选择 配置系统日志。
4. Click **Enable**。

5. 在 设施点下拉列表中，选择一个本地或用户级设施点。
6. 为 syslog 消息选择所需的日志级别。
7. 单击 “ 确定”。

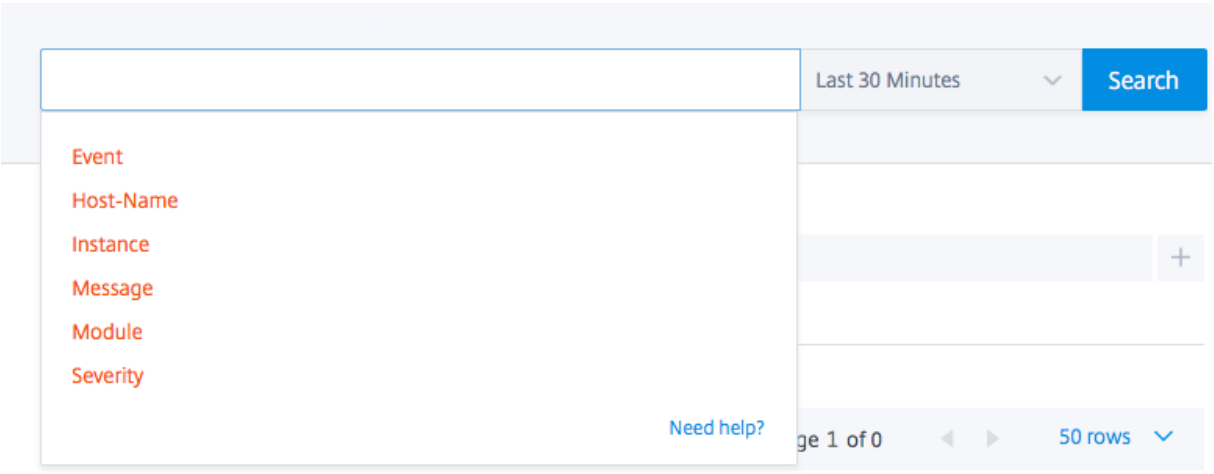


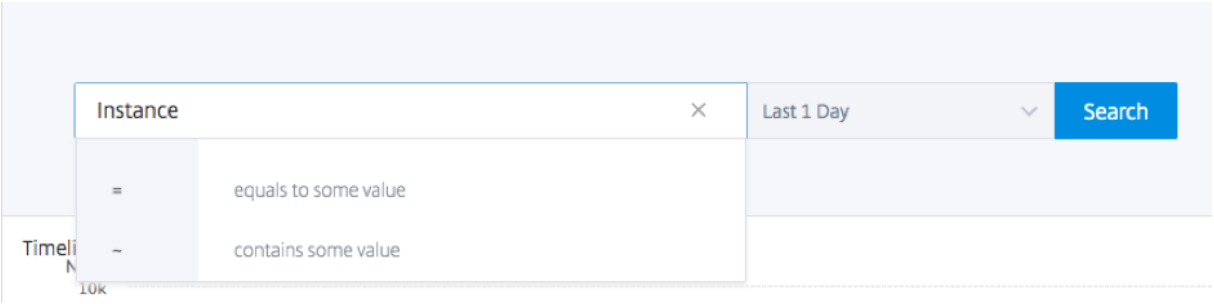
这些步骤配置 Citrix ADC 实例中的所有 syslog 命令，Citrix ADM 开始接收系统日志消息。

查看和搜索 **syslog** 消息

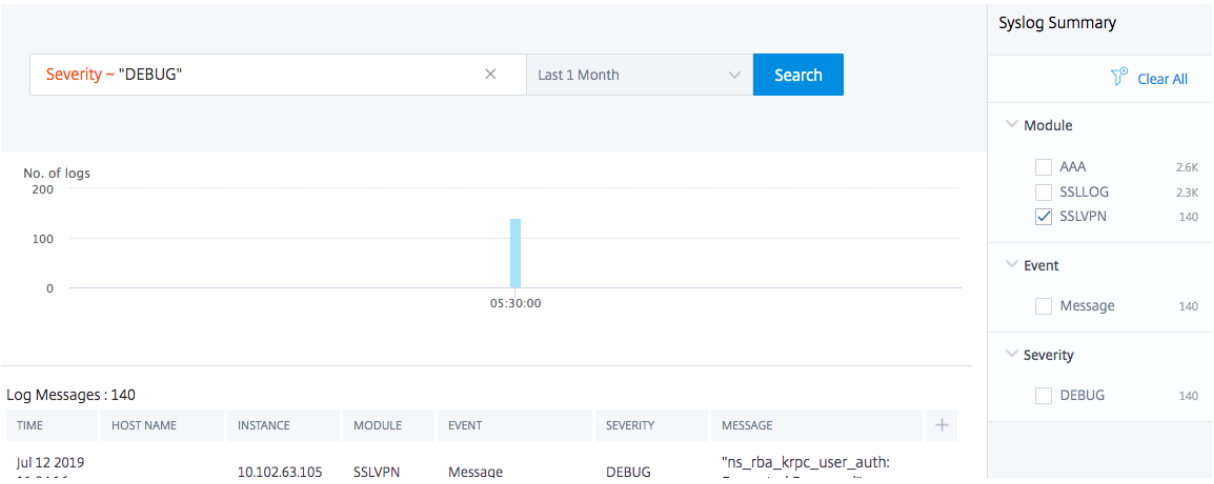
您可以查看在托管 Citrix ADC 实例上生成的所有 syslog 消息。syslog 消息集中存储在数据库中，可在 “ 网络**” > “**事件**” > “**系统日志消息” 下获取，以供审核使用。您可以合并这些日志记录信息，然后从收集的数据中派生报告以进行分析。

此外，您可以使用过滤器来缩小 syslog 消息的搜索结果范围，并实时查找您要查找的内容。单击 需要帮助**?** 打开内置搜索帮助。





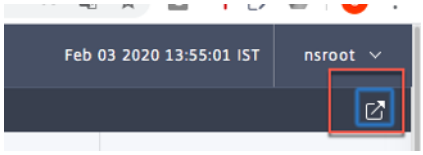
接下来，添加搜索词。对于某些类别，将显示预填充的搜索词列表。默认情况下，搜索时间为 1 天。您可以通过单击向下箭头更改时间和日期范围。您可以通过从“ 系统日志摘要”窗格中选择选项来进一步缩小搜索范围。



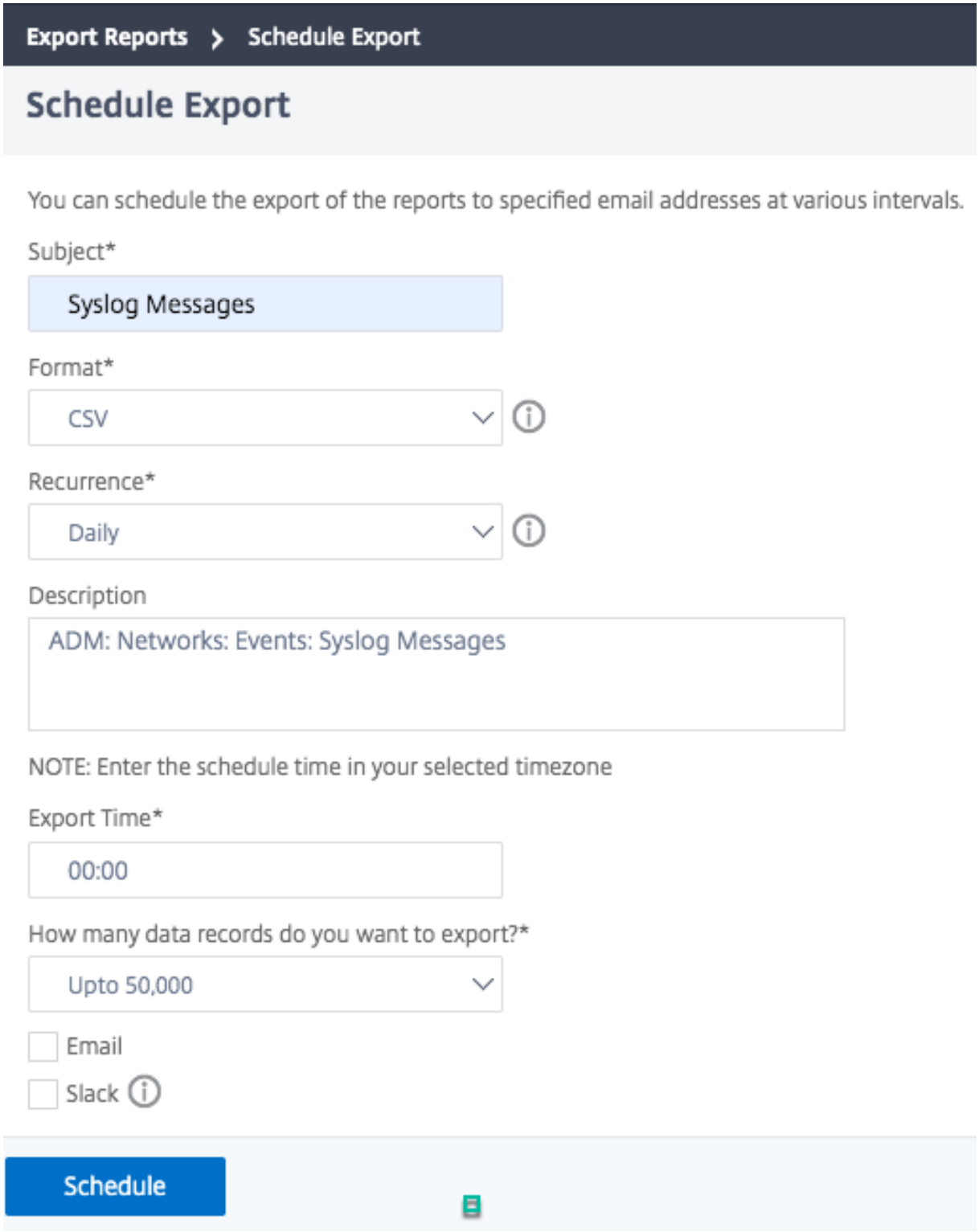
导出和安排 **syslog** 消息

通过安排导出服务器上收到的所有 syslog 消息，您可以在不登录 ADM 的情况下查看 syslog 消息。您可以将在 ADC 实例上生成的系统日志消息导出为 PDF、CSV、PNG 和 JPEG 格式。您可以安排在不同的时间间隔将这些报告导出到指定的电子邮件地址或 Slack 帐户。

要导出和计划日志消息，请单击右上角的箭头图标。



- 要导出日志消息，请单击 “ 导出报告” > “立即导出”，选择所需的格式，然后单击 “ 导出”。
- 要计划系统日志消息的导出，请单击 导出报告 > 计划报告，然后设置所需的参数。您可以通过电子邮件或 Slack 接收报告。



禁止系统日志消息

April 23, 2021

当配置为 syslog 服务器时，Citrix Application Delivery Management (ADM) 会收到配置的 Citrix 应用程序 Delivery Controller (ADC) 实例发送给它的所有 syslog 消息。可能有大量您可能不想看到的消息。例如，您可能不希望看到所有信息级别的消息。现在您可以丢弃其中一些您不感兴趣的 syslog 消息。您可以通过设置一些筛选器来抑制进入 Citrix ADM 的某些系统日志消息。Citrix ADM 会删除符合条件的所有消息。这些删除的消息不会显示在 Citrix ADM GUI 上，这些消息也不会存储在客户的 Citrix ADM 数据库中。

您可以通过设置一些筛选器来禁止某些记录的 syslog 消息进入 Citrix ADM。用于阻止 syslog 消息的两个过滤器是严重性和设施。您还可以禁止来自特定 Citrix ADC 实例或多个实例的消息。您还可以为 Citrix ADM 提供用于搜索和禁止消息的文本模式。Citrix ADM 会删除符合条件的所有消息。这些删除的消息不会显示在 Citrix ADM GUI 上，这些消息也不会存储在客户数据库中。因此，在存储服务器上节省了大量空间。

阻止 syslog 消息的一些用例如下：

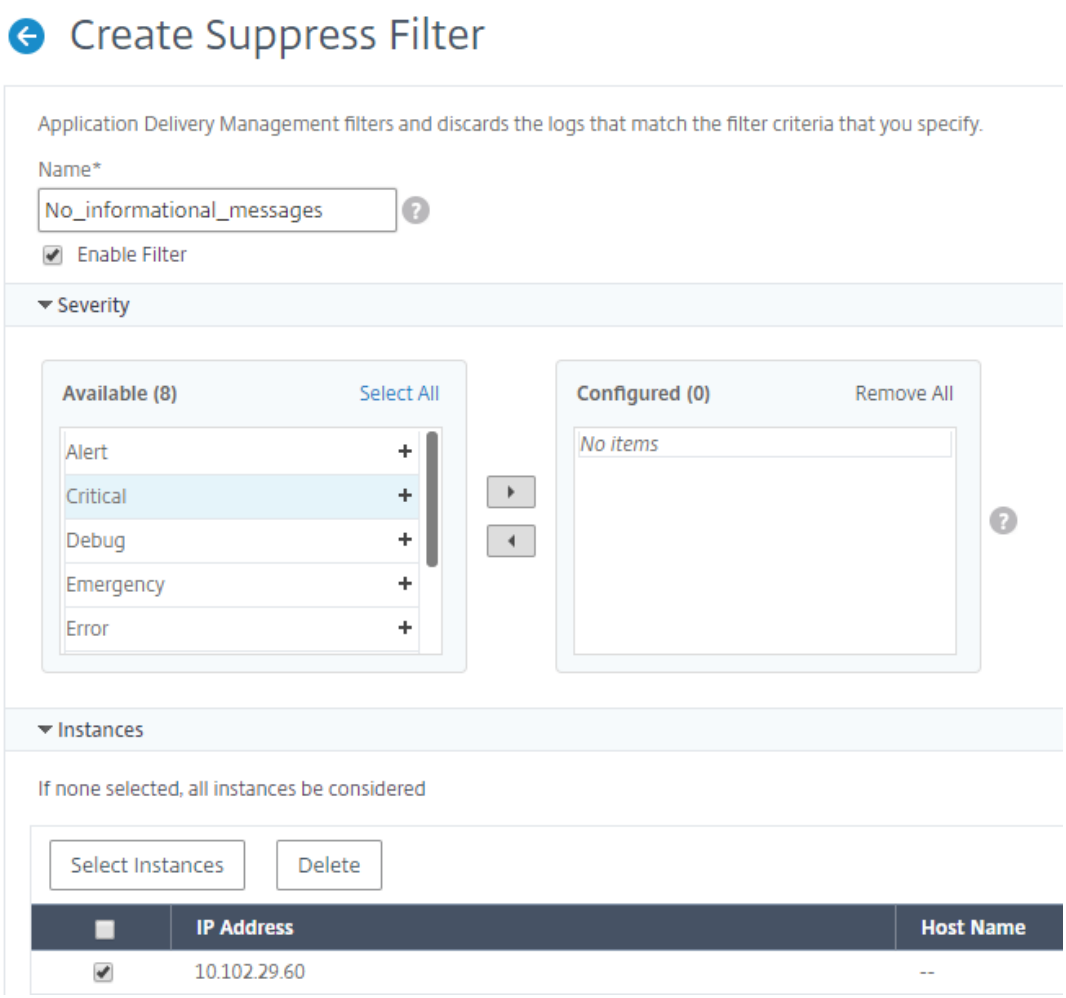
- 如果您要忽略所有信息级别消息，则阻止级别 6（信息）
- 如果您仅要记录防火墙错误状况，则阻止级别 3（错误）以外的所有级别

通过创建筛选器禁止 **syslog** 消息

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 事件” > “ 系统日志消息” > “ 禁止筛选器”。
2. 在 “ 创建隐藏过滤器” 页上，更新以下信息：
   a) 名称 -键入筛选器的名称。

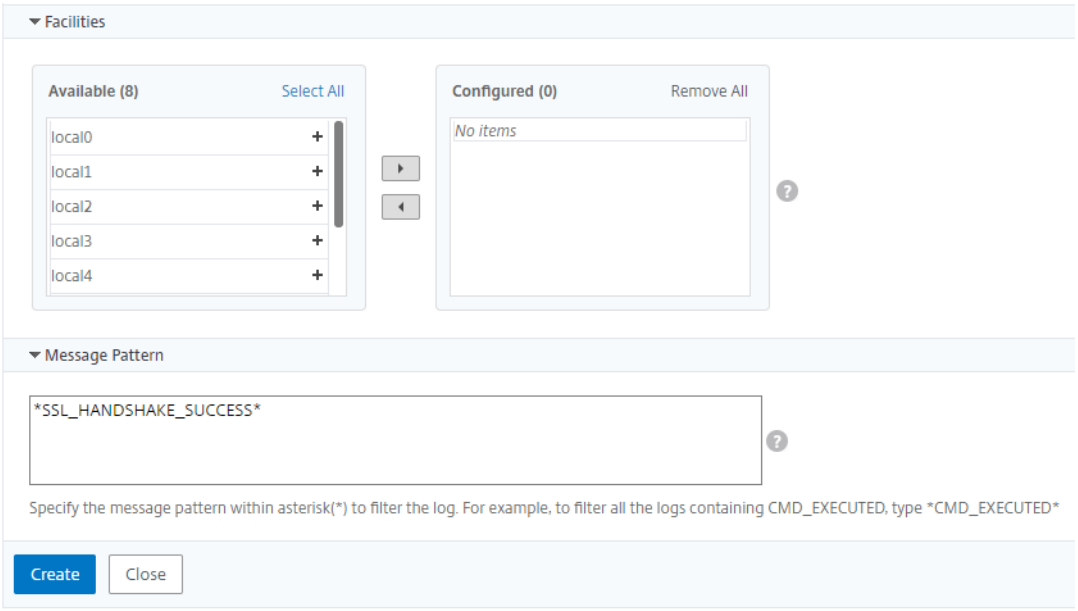
   > 注意：
   >
   > 如果不同用户对多个 Citrix ADC 实例具有不同的访问权限，则必须为不同的实例创建不同的筛选器，因为用户只能看到他们有权访问所有实例的那些筛选器。

   b) 严重性 -选择并添加必须禁止消息的日志级别。例如，如果您不想查看传入的任何信息消息，则可以选择 “Informational”（信息）以阻止这些消息。
   c) 实例 -选择已配置 syslog 消息的 Citrix ADC 实例。



d) 协作室 -根据生成消息的源选择要隐藏消息的协作室。

e) 消息模式 -您还可以键入一个由星号 (*) 包围的文本模式来隐藏消息。将在消息中搜索该文本模式字符串，并阻止包含此模式的那些消息。



禁用过滤器

要允许在 Citrix ADM 上查看消息，必须禁用筛选器。

1. 导航到 “ 网络” > “ 事件” > “ **Syslog** 消息” > “ 禁止筛选器”，然后在 “ 禁止筛选器” 页面上，选择筛选器，然后单击 “ 编辑”。
2. 在 “ 配置禁止筛选器” 页上，清除 “ 启用筛选器” 复选框以禁用筛选器。

配置实例事件的修剪设置

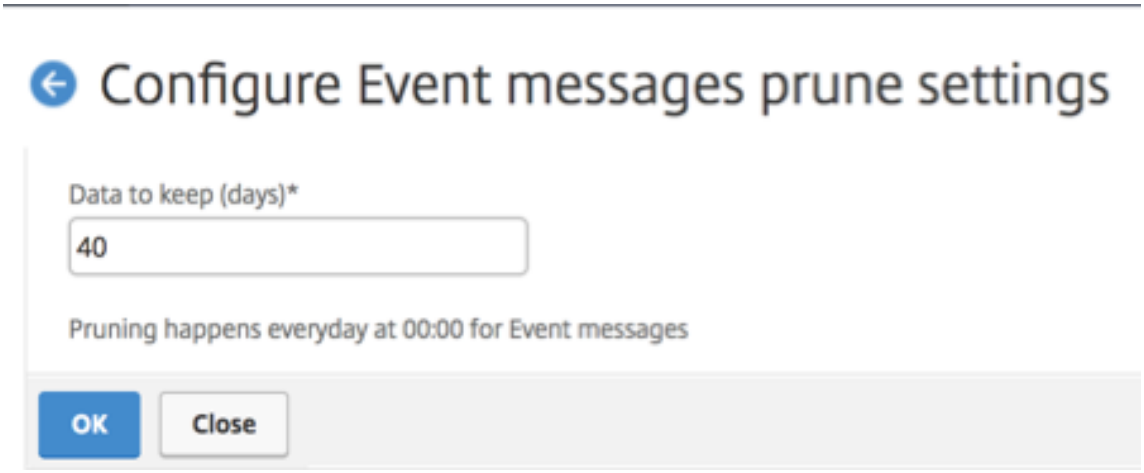
April 23, 2021

由 Citrix 应用程序交付管理 (ADM) 服务器管理的 Citrix 应用程序 Delivery Controller (ADC) 实例不断发送事件消息数据以存储在 Citrix ADM 上。您可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

> 注意
>
> 您可以指定的值不能超过 40 天或少于 1 天。

要配置实例事件的修剪设置，请执行以下操作：

1. 导航到 “系统” > “系统管理”。
2. 在 “修剪设置” 下，单击 “实例 事件修剪设置”。
3. 输入要在 Citrix ADM 服务器上保留数据的时间间隔（以天为单位），然后单击 **“**确定”。



SSL 证书管理

April 23, 2021

任何需要处理机密或敏感信息的组织或个人网站都必须拥有 SSL 证书。Web 服务器上的 SSL 证书有助于保证 Web 服务器对连接客户端的真实性。它不仅验证网站的身份，还有助于生成会话密钥，该密钥稍后用于整个会话的加密。

安全套接字层 (SSL) 证书是任何 SSL 交易的一部分，是标识公司（域）或个人的数字数据表单 (X509)。证书具有公钥组成部分，想要启动与服务器的安全事务的任何客户端都可以看见该组成部分。相应的私钥安全地驻留在 Citrix 应用程序 Delivery Controller (ADC) 设备上，用于完成非对称密钥（或公钥）加密和解密。

Citrix Application Delivery Management (ADM) 为您提供了一个统一的控制台，用于自动安装、更新、删除、链接和下载 SSL 证书。它有助于保持网站的声誉和客户的信任。Citrix ADM 现在可以为您简化证书管理的各个方面。通过统一的控制台，您可以配置自动化策略，以确保根据组织 IT 策略建议的发布者、关键强度、协议和算法。通过这样做，您可以密切关注未使用或即将过期的证书。

您可以通过以下任何一种方式获取 SSL 证书和密钥：

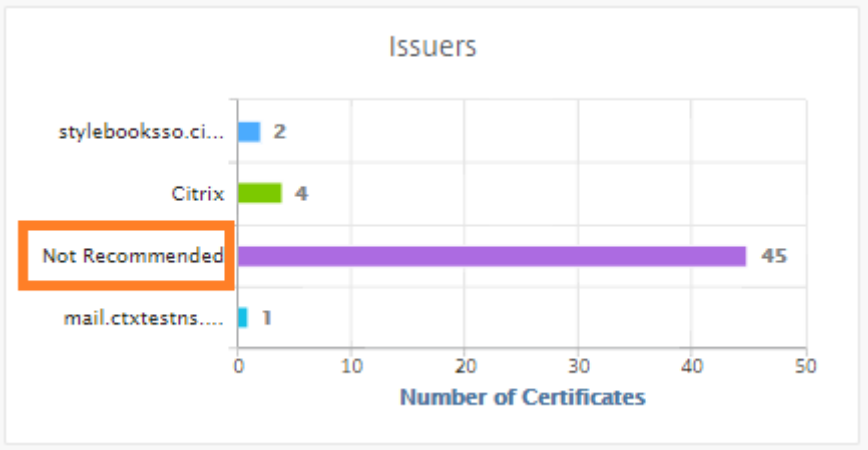
- 来自授权证书颁发机构 (CA)，例如威瑞信
- 通过在 Citrix ADC 设备上生成新的 SSL 证书和密钥

企业 SSL 策略设置

每个企业都有自己的 SSL 策略，并定义了所有 SSL 证书必须遵守的要求。安全性一直是所有企业用户的首要任务之一，因此 SSL 设置起着重要作用。

例如，ABC 公司要求所有证书必须具有最低关键强度为 2,048 位及以上。证书必须由受信任的 CA 或颁发机构授权。管理员必须检查所有此类 SSL 参数，以确保证书遵守公司策略。手动验证每个证书是一项乏味的工作。为了克服这种情况，Citrix ADM 可帮助您配置企业 SSL 策略设置，并显示带有“不推荐”标签的任何不合规证书。

您可以在 SSL 控制面板上查看不合规（不推荐）证书的摘要。

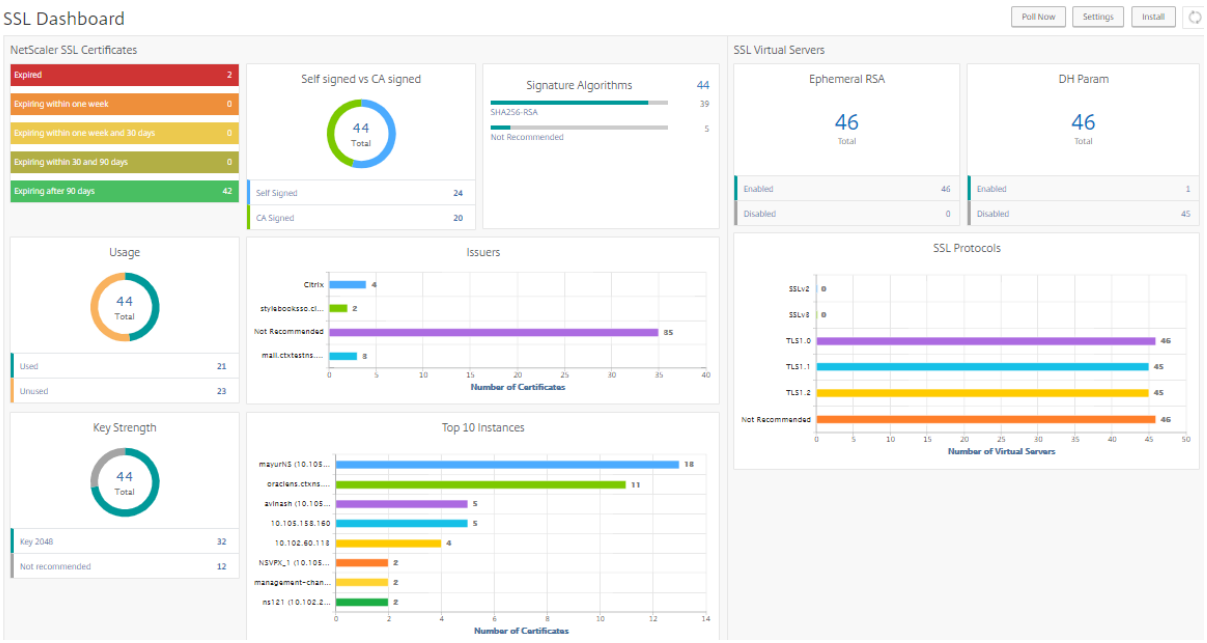


> 注意
>
> “不推荐”证书根据不同的参数进行分类，您可以在相关组件中查看它们。

Citrix ADM 证书的工作原理

SSL 仪表板为您提供了在不同 Citrix ADC 实例上安装的所有 SSL 证书的直观演示。SSL 仪表板包括 Citrix ADC 实例上安装的每个证书的以下信息。它根据以下内容进行分类：

- 自签名与 **CA** 签名。自签名与 CA 签名部分可帮助您将证书分离为自签名证书和 CA 签名证书。
- 签名算法。本节根据用于加密的签名算法分离 SSL 证书。
- 用法。本节根据使用的和未使用的证书将 SSL 证书隔离开来。未使用的证书需要特别关注，因为它们可能错过了绑定到虚拟服务器。
- 发行人。本节根据证书的颁发者对 SSL 证书进行分离。
- 关键力量。本节根据私钥的密钥强度分离 SSL 证书。
- 前 **10** 个实例。本节根据安装的 SSL 证书数量提供前 10 个 Citrix ADC 实例的详细信息。



SSL 证书管理使用案例

以下使用案例描述了如何使用 SSL 证书跨多个 Citrix ADC 实例管理和监控证书。

安装 **SSL** 证书

想象一下，您有一个 Citrix ADC 实例队列，您必须在其上部署所需的 SSL 证书。Citrix ADM 为您提供了一个统一的控制台，用于一次尝试在多个 Citrix ADC 实例之间部署 SSL 证书。

例如，您可能希望在一个或多个 Citrix ADC 实例上安装一些 SSL 证书。使用此方法，您可以尽量减少在每个 Citrix ADC 实例上安装 SSL 证书的手动干预。您可以跨一个或多个 Citrix ADC 实例批量安装 SSL 证书。

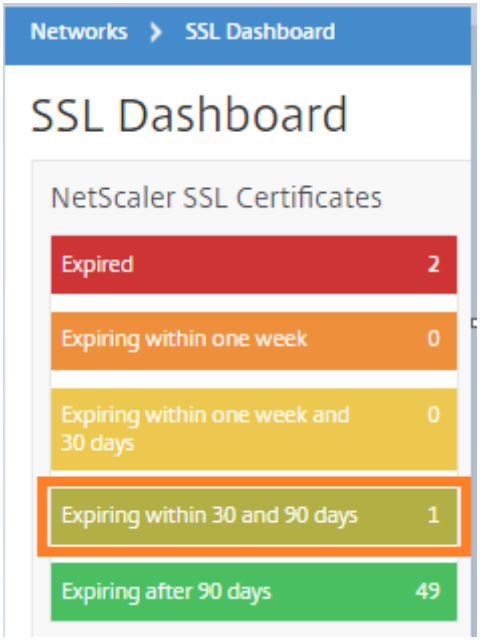
要获取 SSL 证书的摘要，请登录 **Citrix ADM**，然后导航到 “ 网络**” > “SSL** 控制面板”。

证书到期的通知设置

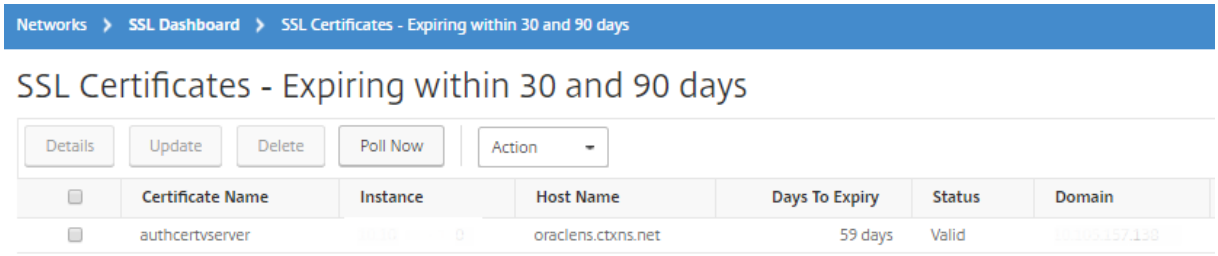
在此使用案例中，您可能跨多个 Citrix ADC 实例拥有许多证书，跟踪每个证书的到期时间将成为开销。手动跟踪每个证书并在证书到期之前对其进行更新是一项繁琐的工作。要避免这种情况，您可以将 Citrix ADM 配置为将通知或警报发送到已配置的电子邮件、寻呼机、Slack 或 ServiceNoW 配置文件。通过这种方式，您可以在到期日之前及时了解证书的到期日并续订证书。

例如，您可能忘记跟踪即将到期的证书。证书过期会导致服务中断，这可能会影响用户的许多应用程序。使用 ADM 证书到期通知设置，您可以避免此类不可预见的情况。

您可以在 **SSL** 控制面板上查看摘要并跟踪即将到期的证书。



要查看任何持续时间内即将到期的证书的报告，您可以单击磁贴以获取该窗口中即将到期的所有此类证书的详细信息。



证书续期

您现在可以续订 Citrix ADM 的证书。您可以续订现有证书，也可以根据以下内容创建证书：

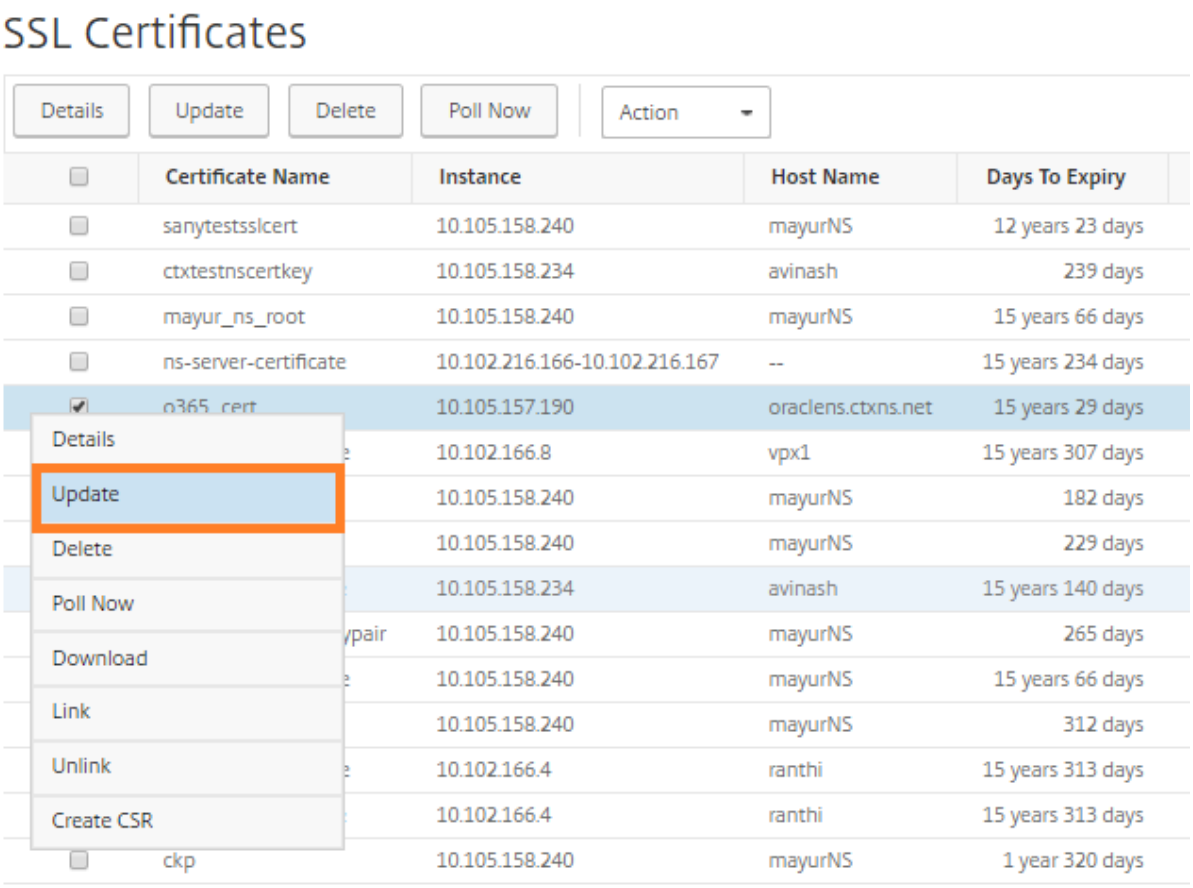
更新现有证书

在此使用案例中，您必须在收到证书颁发机构 (CA) 的续订证书后更新现有证书。现在，您可以从 Citrix ADM 更新现有证书，而无需登录 Citrix ADC 实例。

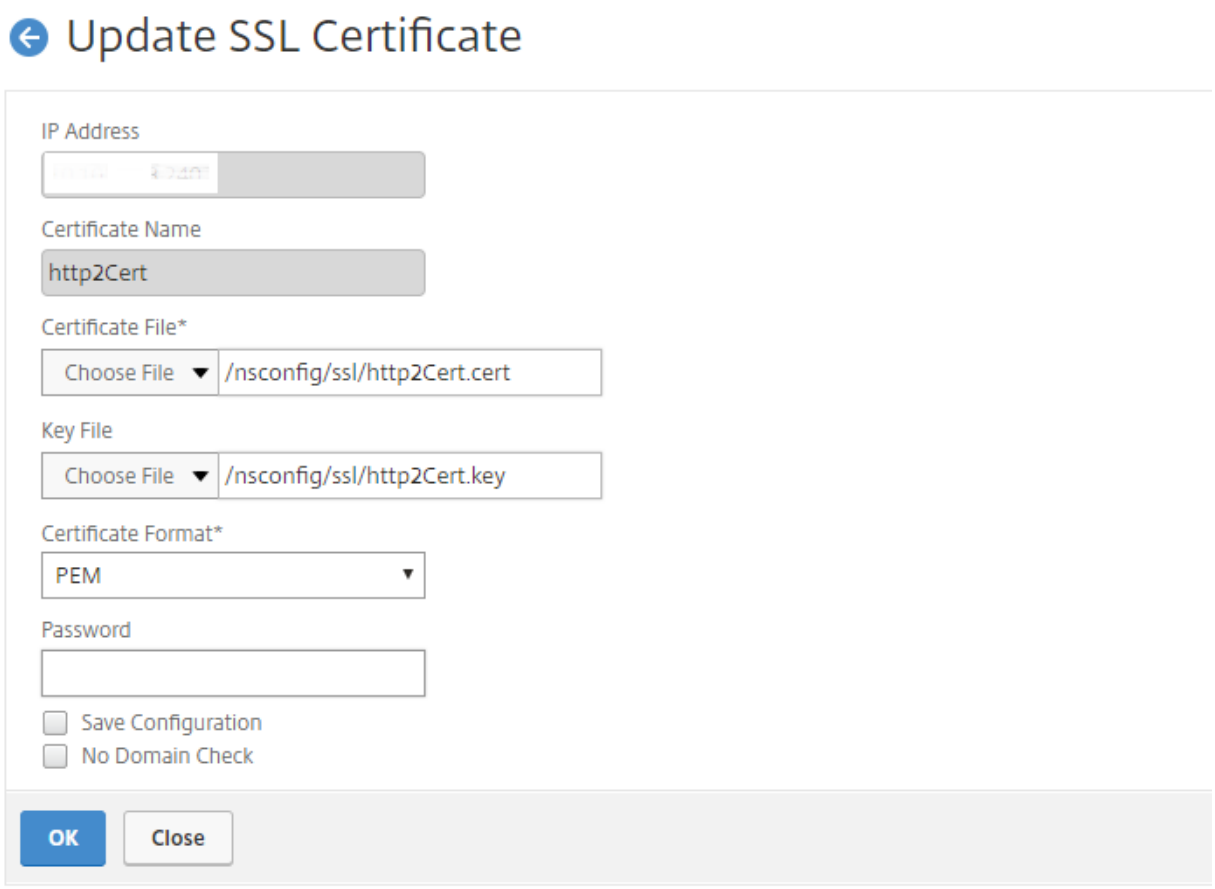
例如，现有证书可能会有一些更改或修改。CA 颁发续订的证书。您现在可以从 Citrix ADM 更新 SSL 证书，而不是转到 Citrix ADC 设备。

要更新任何证书，请登录 Citrix ADM，然后导航到 网络 **> SSL** 仪表板。

选择要更新的证书，然后单击 更新。



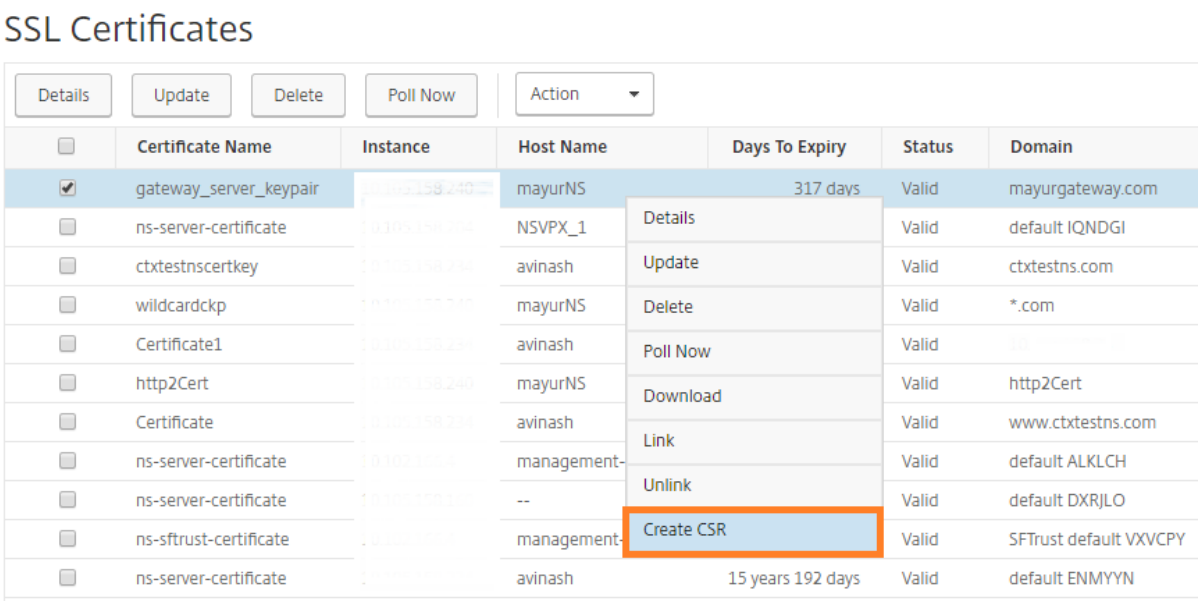
您可以选择更新 Citrix ADM 所选证书的相关字段。



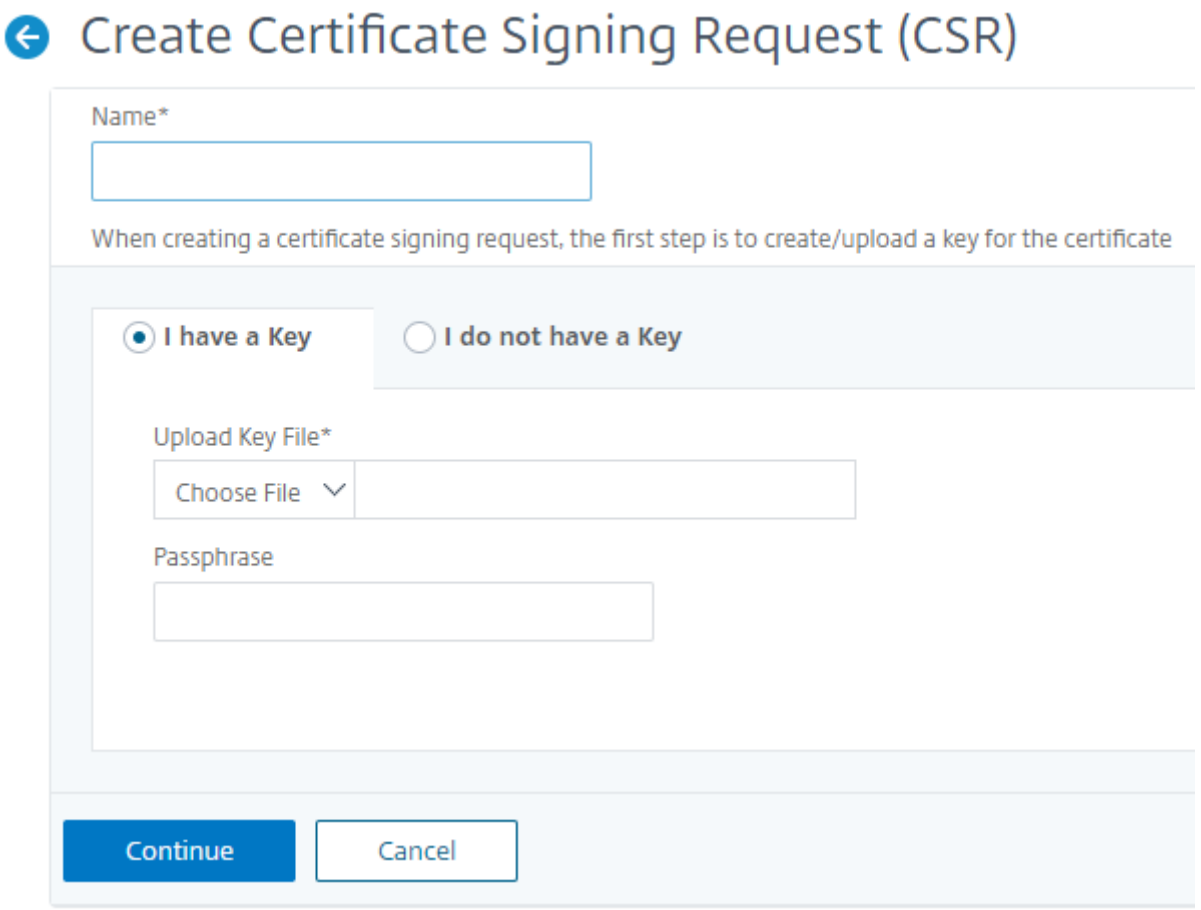
创建证书签名请求

想象一下，其中一个 SSL 证书不符合组织策略的使用案例。您想从证书颁发机构获得新证书。您现在可以从 Citrix ADM 生成证书签名请求 (CSR)。可以将 CSR 和公钥发送到 CA 以获取 SSL 证书。

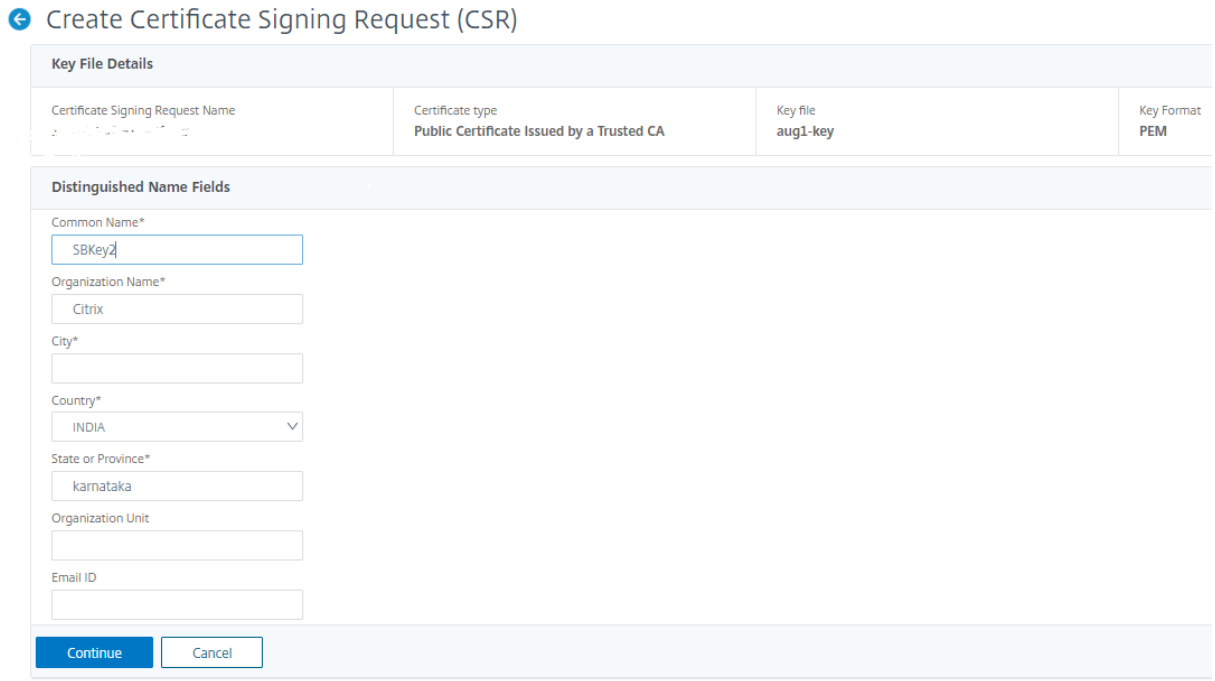
要确定并创建 CSR，请选择所需的证书，然后单击 创建 **CSR**。



您需要有一个公钥或私钥值对。要上传密钥，请单击“ 选择文件”，然后从列表中进行选择。要创建密钥，请选择“ 我没有 **Key”** 选项，然后指定相关参数。

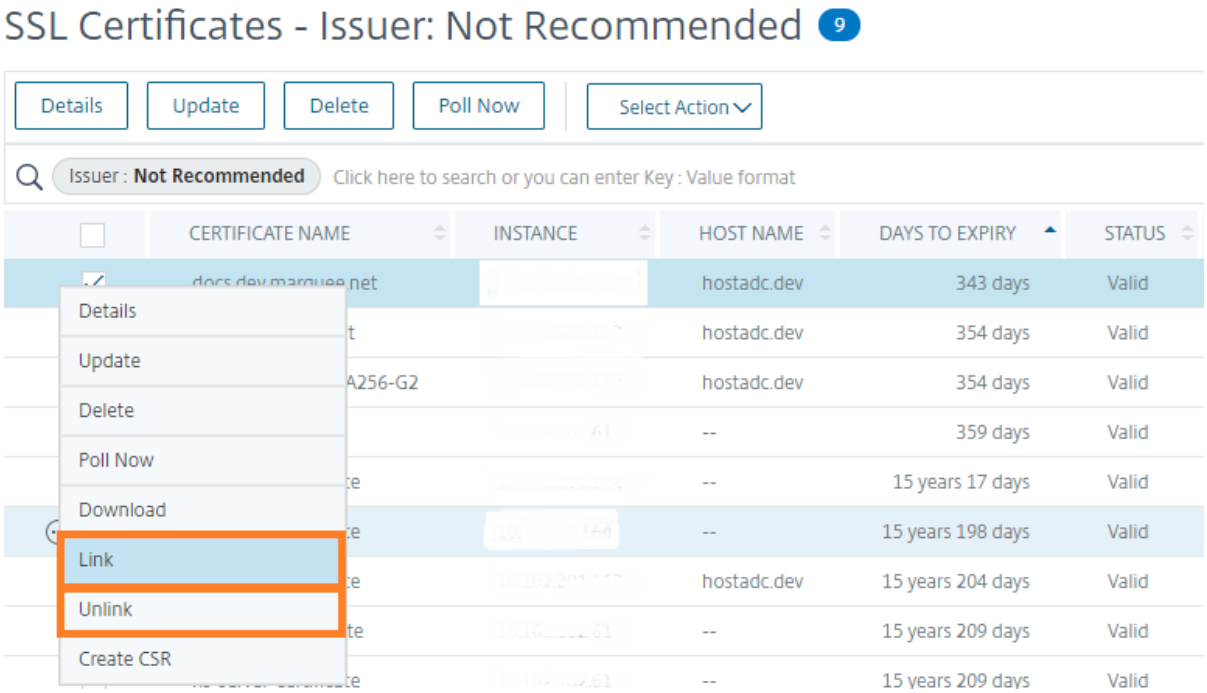


提供所选密钥（如公用名称、组织名称、城市、国家/地区、州、组织单位和电子邮件 ID）的更多详细信息，以创建 CSR。



链接和取消链接 **SSL** 证书

您可以将多个 SSL 证书相互绑定以创建证书捆绑包。要将证书链接到另一个证书，第一个证书的颁发者必须匹配第二个证书的域。

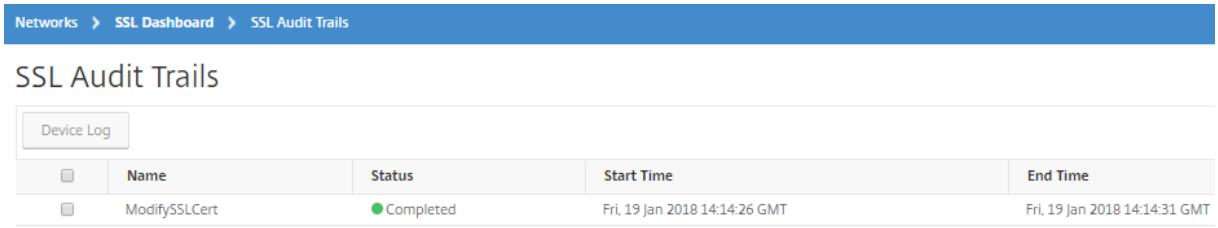


审核日志

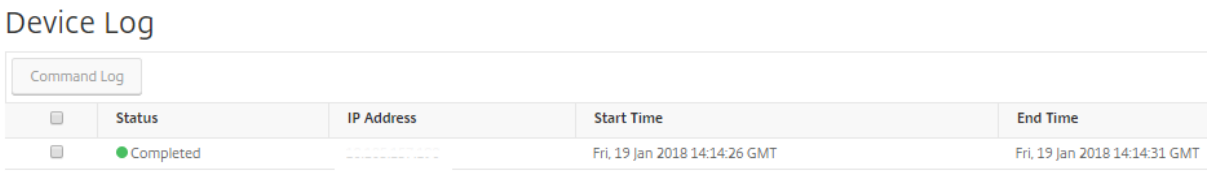
审核日志是 Citrix ADM 生成的文本日志文件的集合。它显示了通过将 Citrix ADM 添加、修改和更改的 SSL 证书的历史记录到特定 Citrix ADC 设备。审核日志还显示 Citrix ADC 设备的 IP 地址、状态、开始时间和特定操作的结束时间。

在此示例中，您可能需要验证特定证书在一段时间内发生的更改。而且，您可以选择通过设备日志和命令日志查看证书更改的历史记录。

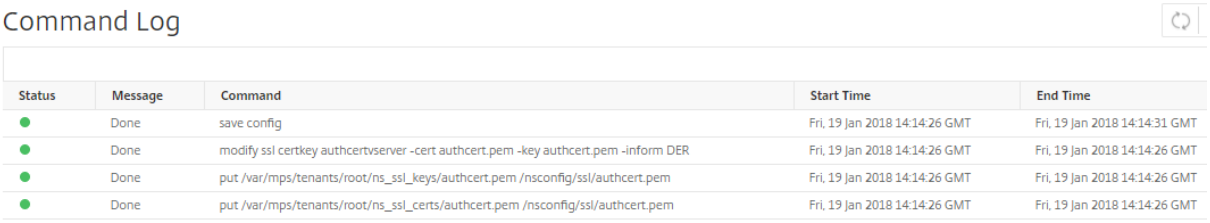
要确定 SSL 证书的信息，请在 **SSL** 控制面板上单击 审核日志。应用程序摘要包括启动时间和结束时间的 SSL 证书状态。



要确定特定 SSL 证书的 Citrix ADC 设备的信息，请选择所选的相关证书复选框。单击 设备日志。



要查看命令类型和消息的信息，请单击 命令日志。



使用 **SSL** 仪表板

April 23, 2021

您可以使用 Citrix Application Delivery Management (ADM) 中的 SSL 证书仪表板查看有助于跟踪证书颁发者、关键优势和签名算法的图形。SSL 证书控制板还显示指示以下信息的图形：

- 证书过期前的天数
- 已使用证书和未使用证书的数量
- 自签名证书和 CA 签名证书的数量
- 颁发者数

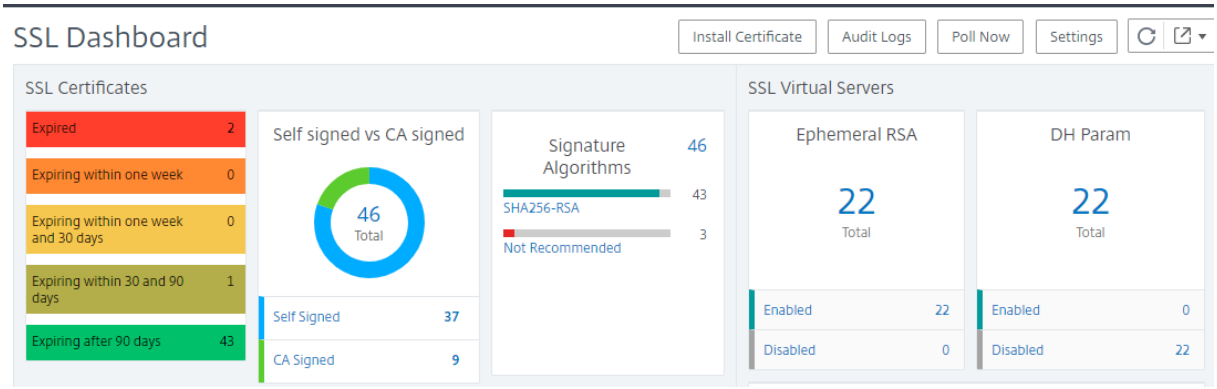
- 签名算法
- SSL 协议
- 按使用的证书数排在前 10 位的实例

监视 **SSL** 证书

如果您的公司已定义了某些 SSL 证书要求（例如所有证书的最小密钥强度必须为 2048 位且受信任的 CA 颁发机构必须对其进行授权），则可以使用 Citrix ADM 上的 SSL 仪表板监视您的证书。

在另一个示例中，您可能已上传了新证书，但忘记将其绑定到虚拟服务器。SSL 控制板会突出显示正在使用或未使用的 SSL 证书。在 “ 使用情况” 部分，您可以看到已安装的证书数以及正在使用的证书数。您可以进一步单击图形，查看证书名称、正在使用证书的实例、其有效性、签名算法等。

要在 Citrix ADM 中监视 SSL 证书，请导航到 “网络” > “ **SSL** 仪表板”。



Citrix ADM 允许您轮询 SSL 证书，并立即将实例的所有 SSL 证书添加到 Citrix ADM 中。为此，

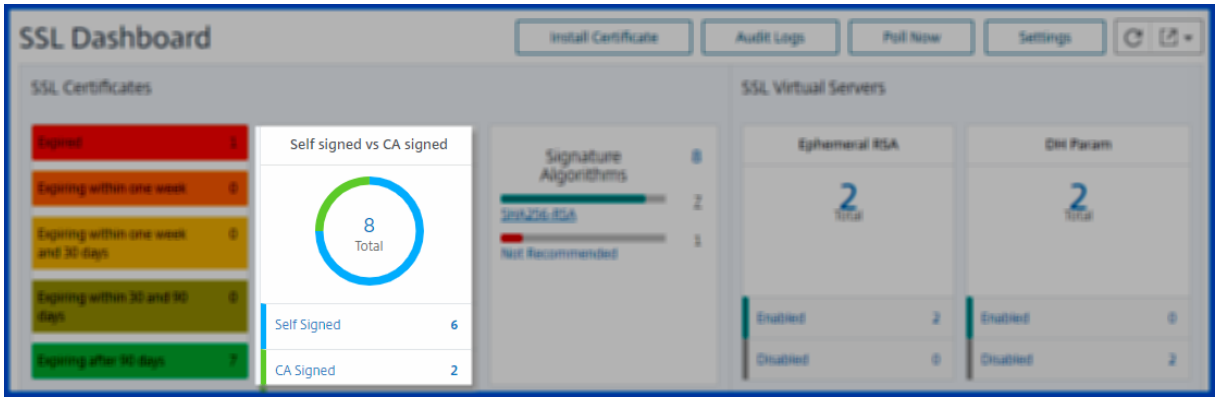
1. 导航到 “ 网络” > “**SSL** 仪表板”。
2. 单击 立即轮询。

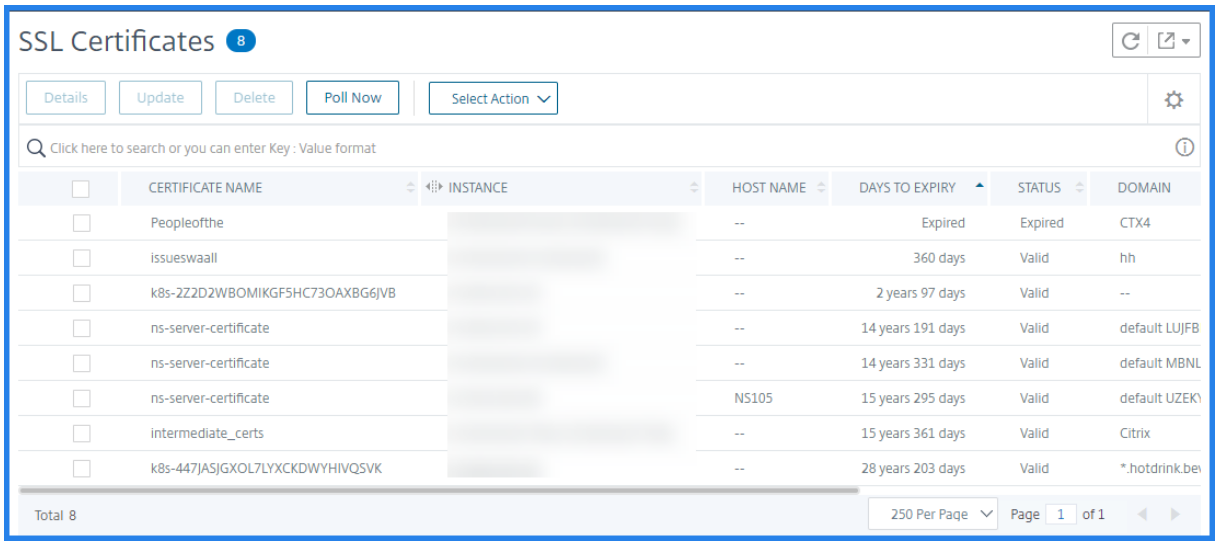
   在 “ 立即轮询” 页面上，您可以轮询所有托管 ADC 实例，也可以选择特定实例。
3. 单击 开始轮询。

在 **SSL** 仪表板中，您可以监视 ADC SSL 证书、SSL 虚拟服务器和 SSL 协议。

您可以单击仪表板上的指标以查看与 SSL 证书、SSL 虚拟服务器或 SSL 协议相关的详细信息。

例如，当您单击仪表板上 自签名与 **CA** 签名下的数字时，ADM GUI 将显示 Citrix ADC 实例上的所有 SSL 证书。





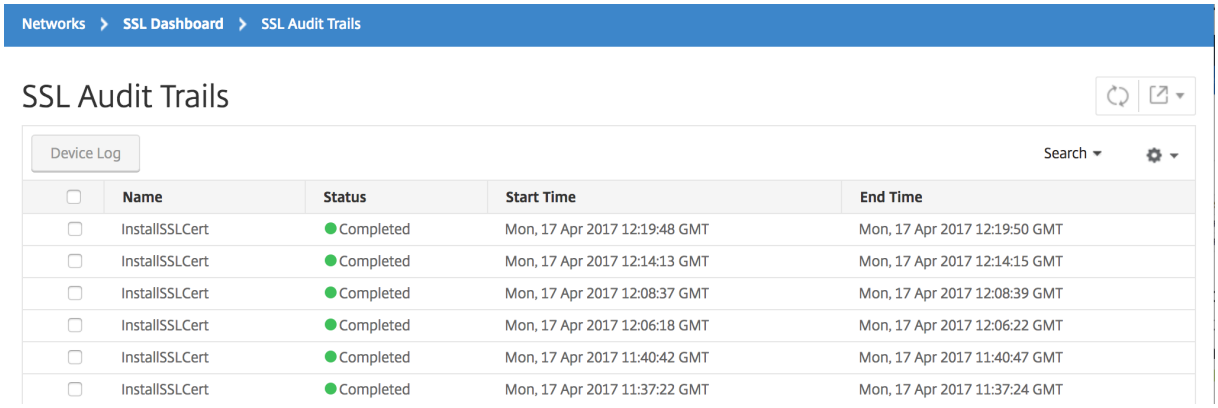
Citrix ADM SSL 仪表板还显示了虚拟服务器上运行的 SSL 协议的分布情况。作为管理员，您可以指定要通过 SSL 策略监视的协议，有关更多信息，请参阅配置 SSL 策略。支持的协议包括 SSLV2、SSLV3、TLS 1.0、TLS 1.1、TLS 1.2 和 TLS 1.3。虚拟服务器上使用的 SSL 协议以条形图格式显示。单击特定协议将显示使用该协议的虚拟服务器的列表。

在 SSL 仪表板上启用或禁用 Diffie-Hellman (DH) 或短暂 RSA 密钥后，会出现一个圆环图。即使服务器证书不支持导出客户端，使用这些密钥也可以与导出客户端进行安全通信，就像使用 1024 位证书一样。单击相应的图表将显示启用 DH 或临时 RSA 密钥的虚拟服务器的列表。

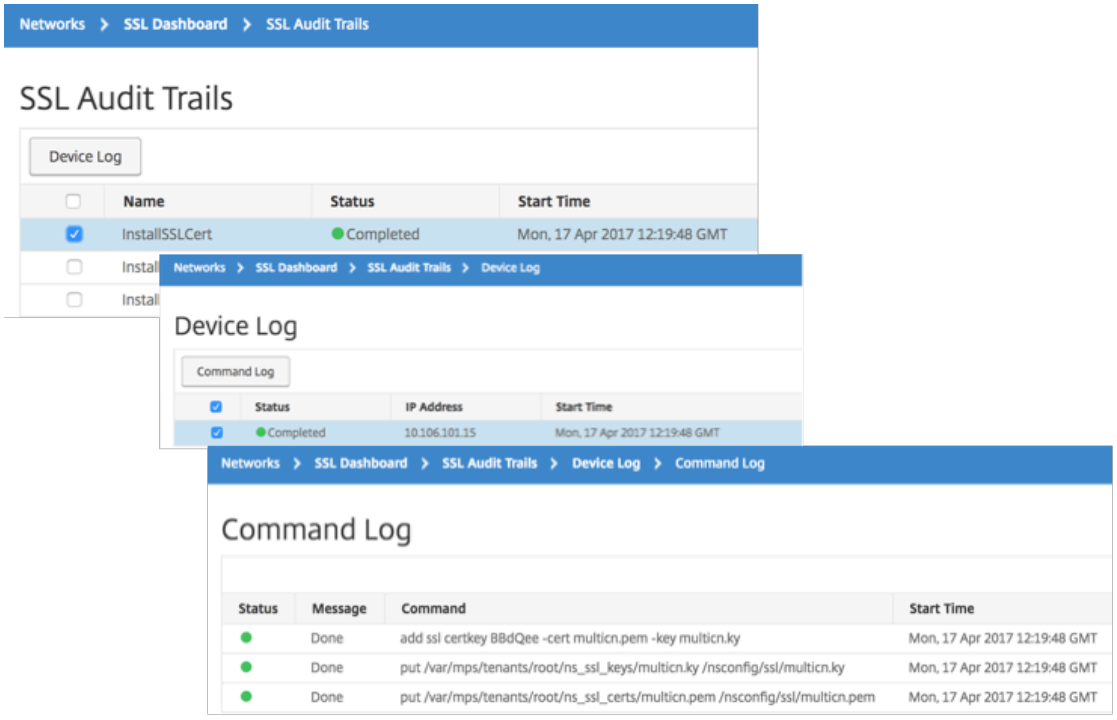
查看 **SSL** 证书的审核追踪

您现在可以在 Citrix ADM 上查看 SSL 证书的日志详细信息。日志详细信息显示在 Citrix ADM 上使用 SSL 证书执行的操作，例如：安装 SSL 证书、链接和取消链接 SSL 证书、更新 SSL 证书和删除 SSL 证书。监视具有多个所有者的应用程序上进行的 SSL 证书更改时，审核追踪信息很有用。

要查看使用 SSL 证书在 Citrix ADM 上执行的特定操作的审核日志，请导航到 “ 网络” > “ **SSL** 仪表板” >，然后单击 “ 审核日志”。



对于使用 SSL 证书执行的特定操作，您可以查看其状态、开始时间和结束时间。此外，您可以查看在其上执行操作的实例以及在该实例上运行的命令。



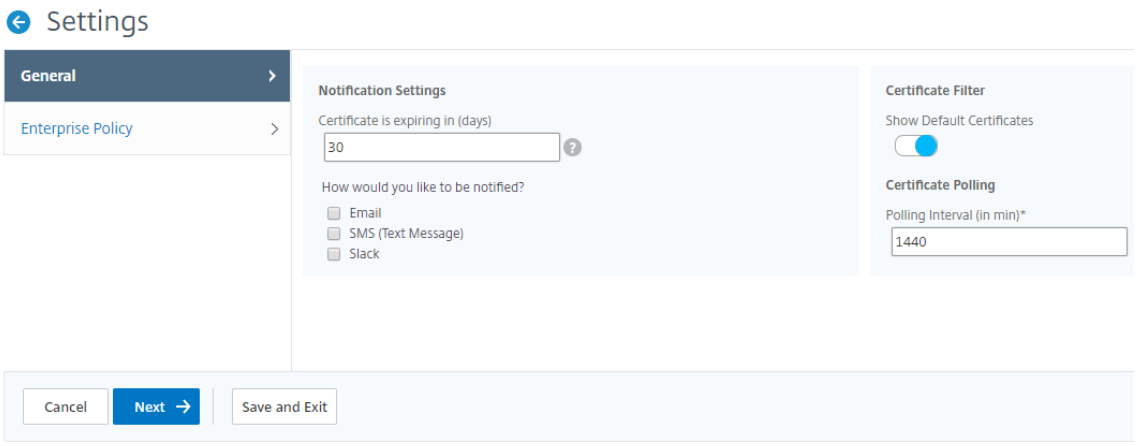
排除 **SSL** 仪表板上的默认 **Citrix ADC** 证书

Citrix ADM 允许您显示或隐藏根据您的首选项显示在 SSL 控制板图表上的默认 Citrix ADC 证书。默认情况下，所有证书都显示在 SSL 控制板上，包括默认证书。

要在 SSL 控制板上显示或隐藏默认证书，请执行以下操作：

1. 在 Citrix ADM GUI 中导航到 网络 > **SSL** 控制板。
2. 在 “ **SSL** 仪表板” 页面上，单击 “ 设置”。
3. 在 设置页面上，选择 常规。

4. 键入证书过期的天数以接收有关证书到期的通知。
5. 选择通知方法并创建相应的配置文件。
6. 在 “ 证书筛选器” 部分，清除 “ 显示默认证书” 复选框，然后单击 “ 保存并退出”。



查看、上传和下载 **SSL** 文件

要查看 Citrix ADM 上的 SSL 文件，请导航到 网络 **> SSL** 仪表板 **> Citrix ADM** 上的 **SSL** 文件。

在此页中，您可以在 Citrix ADM 上查看、上载和下载以下文件：

- SSL 证书
- SSL 密钥
- SSL CSR

要查看和下载 Citrix ADC 实例上的 SSL 文件，请导航到 **“网络” > “SSL** 仪表板” **> “Citrix ADC** 上的 **SSL** 文件”。

> 重要
>
> 要启用从 ADC 实例下载 SSL 文件，请启用实 例 **SSL** 证书功能。有关详细信息，请参阅启用或禁用 ADM 功能。

设置 **SSL** 证书到期通知

April 23, 2021

作为安全管理员，您可以设置通知，以便在证书即将过期时通知您，并包括有关哪些 Citrix 应用程序 Delivery Controller (ADC) 实例使用这些证书的信息。通过启用通知，您可以及时续订您的 SSL 证书。

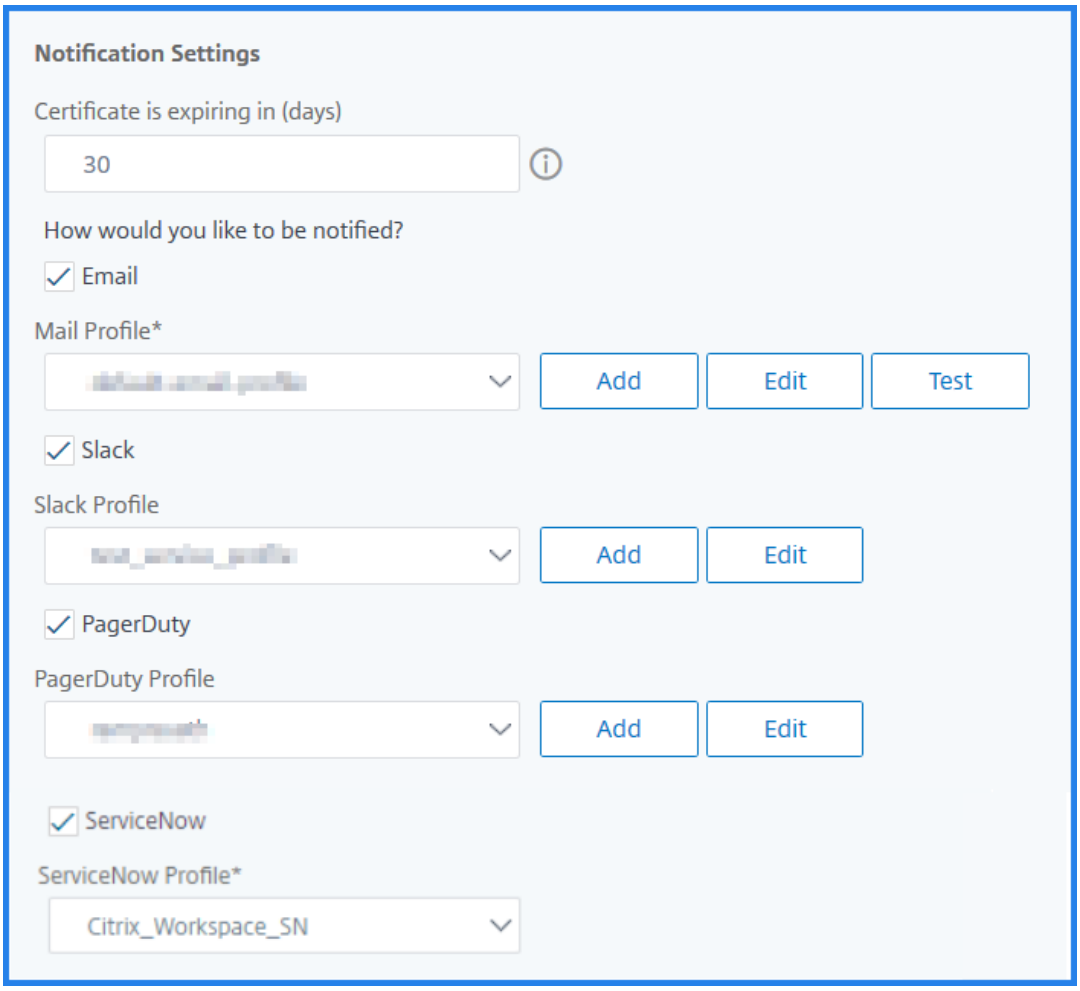
例如，您可以设置在您的证书即将过期前的 30 天向电子邮件通讯组列表发送电子邮件通知。

要设置来自 **Citrix ADM** 的通知，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 网络 **> SSL** 仪表板。

2. 在 **SSL** 控制面板页面上，单击 设置。
3. 在 “ **SSL** 设置” 页上，单击 “编 辑” 图标。
4. 在 **Notification Settings**（通知设置）部分，指定要何时（过期日期前的天数）发送通知。
5. 选择要发送的通知类型。从下拉菜单中选择通知类型和通讯组列表。通知类型如下：
   - **Email**（电子邮件）- 指定邮件服务器和配置文件详细信息。证书要过期时将触发电子邮件。
   - **SMS** - 指定短信服务 (SMS) 服务器和配置文件详细信息。证书要过期时将触发 SMS 消息。
   - **Slack** -指定 Slack 配置文件详细信息。
   - 寻呼服务警报 -指定寻呼服务配置文件。根据您的 PagerDuty 门户中配置的通知设置，当您的证书即将过期时会发送通知。
   - **ServiceNow** -当您的证书即将过期时，会向默认的 ServiceNow 配置文件发送通知。

     > 重要信息：
     >
     > 确保 Citrix 云 ITSM 适配器已配置为服务 Now 并与 Citrix ADM 集成。有关详细信息，请参阅将 Citrix ADM 与 ServiceNow 实例集成。



6. 单击 “ 保存并退出”。

现在，当您的 SSL 证书到期时，Citrix ADM 将 SSL 证书过期陷阱发送到外部陷阱目标服务器。满足以下两个条件时，Citrix ADM 会发送陷阱：

- 您已在 SSL 控制板设置页面中配置了证书过期的天数。
- 您已添加陷阱目标。

您可以通过导航到 “ 系统**” > “SNMP” > “**陷阱目标**”** 来设置陷阱目的地。键入发送陷阱的目标 SNMP 服务器的 IP 地址。输入端口号并键入 “public”（不含引号）作为团体字符串。

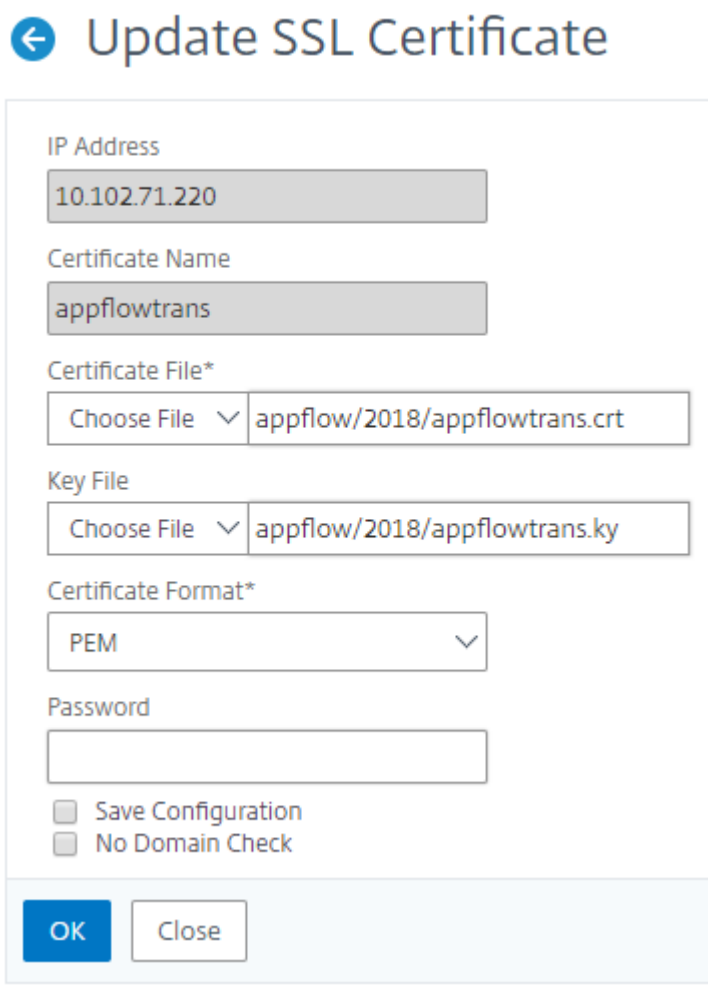
更新已安装的证书

April 23, 2021

从证书颁发机构 (CA) 收到续订的证书后，您可以从 Citrix Application Delivery Management (ADM) 更新现有证书，而无需登录到单个 Citrix 应用程序 Delivery Controller (ADC) 实例。

要从 **Citrix ADM** 更新 **SSL** 证书、密钥或两者，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > **SSL** 控制板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 在 **SSL Certificates**（SSL 证书）页面上，选择证书并单击 **Update**（更新）。或者，单击 SSL 证书查看其详细信息，然后单击 **SSL** 证书页右上角的 更新。
4. 在 **Update SSL Certificate**（更新 SSL 证书）页面上，对证书和/或密钥进行所需的修改，并单击 **OK**（确定）。



在 **Citrix ADC** 实例上安装 **SSL** 证书

April 23, 2021

在 Citrix 应用程序 Delivery Controller (ADC) 实例上安装 SSL 证书之前，请确保证书由受信任的 CA 颁发。此外，请确保证书密钥的密钥强度为 2048 位或更高，并使用安全签名算法对密钥进行签名。

要从另一个 **Citrix ADC** 实例安装 **SSL** 证书，请执行以下操作：

您还可以从选定的 Citrix ADC 实例导入证书，并从 Citrix Application Delivery Management (ADM) GUI 将其应用到其他目标 Citrix ADC 实例。

1. 导航到 “ 网络” > “ **SSL** 仪表板”。
2. 在 SSL 控制板的右上角，单击 安装。
3. 在 “在 **Citrix ADC** 实例上安装 **SSL** 证书” 页上，指定以下参数：

a) 证书源选

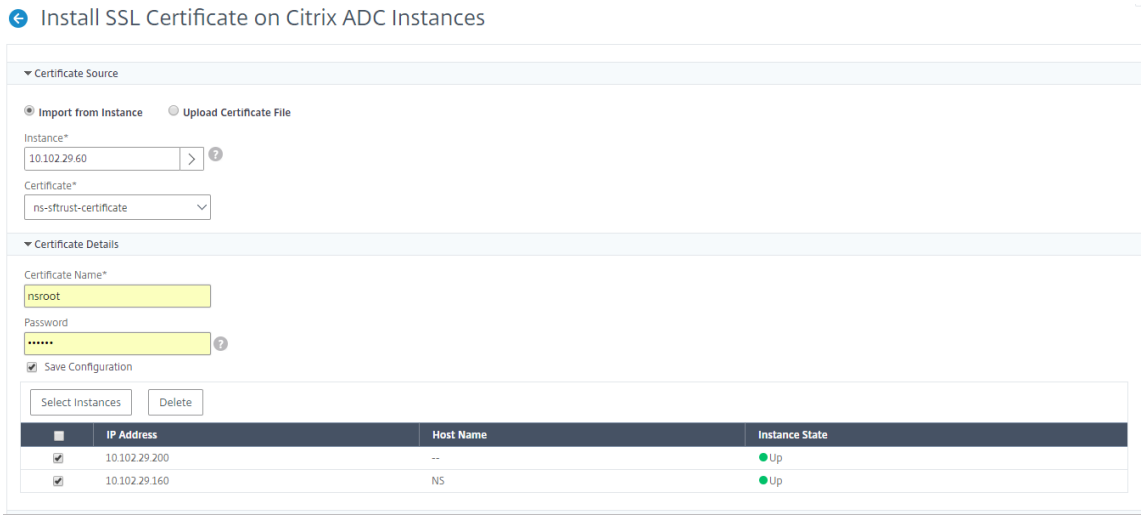
择要 从实例导入的选项。

- 选择要从中导入证书的 实例。
- 从实例上所有 SSL 证书文件的列表中选择证书。

b) 证书详细信息

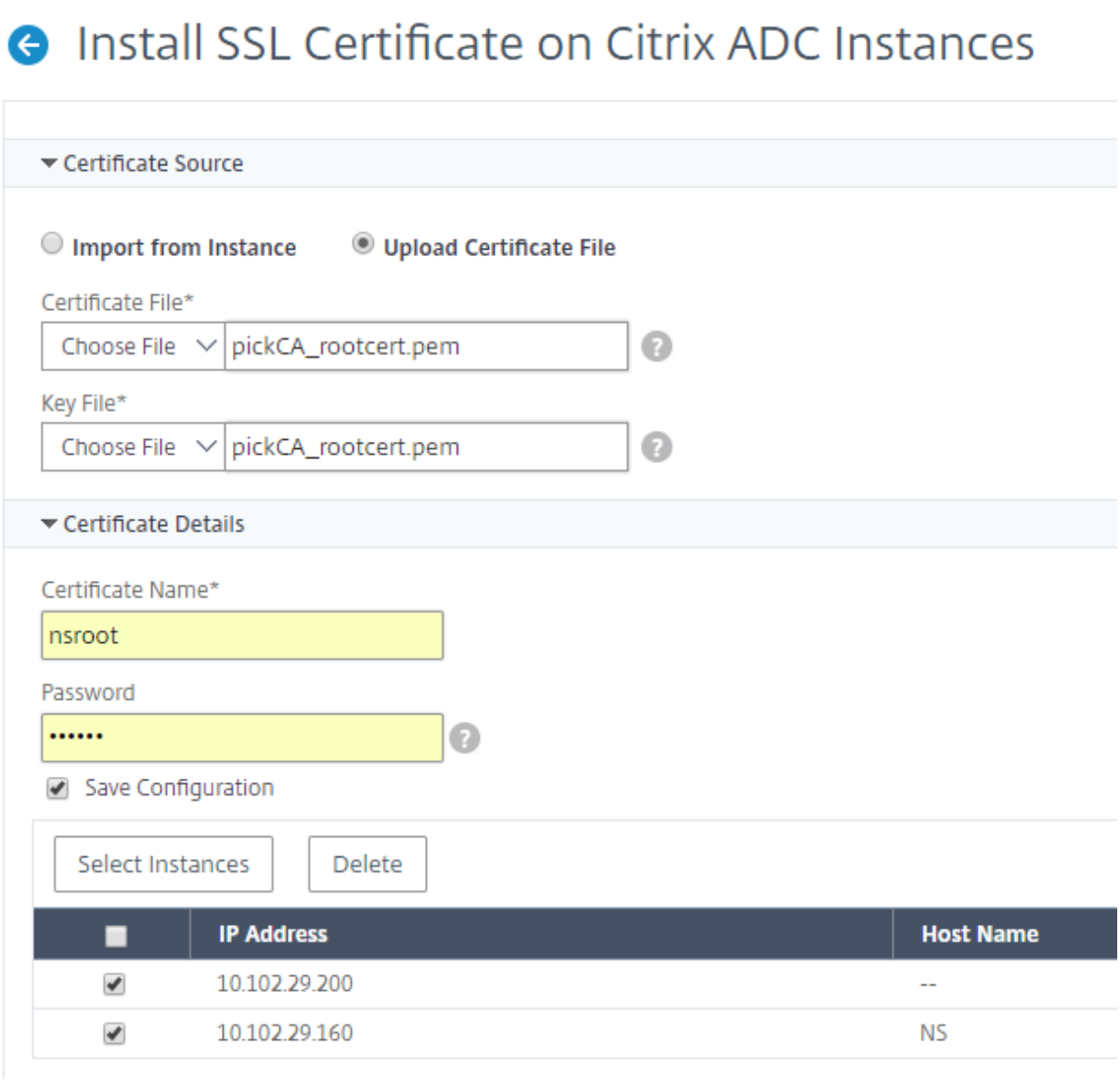
- 证书名称。指定证书密钥的名称。
- 密码。用于加密私钥的密码。可以使用此选项上载加密的私钥。

4. 单击 选择实例以选择要在其上安装证书的 Citrix ADC 实例。
5. 单击确定。



要从 **Citrix ADM** 安装 **SSL** 证书，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > **SSL** 控制板。
2. 在控制板的右上角，单击 **Install**（安装）。
3. 在“在 **Citrix ADC** 实例上安装 **SSL** 证书”页上，选择“ 上载证书文件”并指定以下参数：
   - 证书文件 -通过选择本 地（您的本地计算机）或 设备（证书文件必须存在于 Citrix ADM 虚拟实例上）来上传 SSL 证书文件。
   - **Key File**（密钥文件）- 上载密钥文件。
   - **Certificate Name**（证书名称）– 指定证书密钥的名称。
   - **Password**（密码）- 用于对私钥进行加密的密码。可以使用此选项上载加密的私钥。
   - 选择实例 -选择要在其上安装证书的 Citrix ADM 实例。
4. 若要保存配置以供将来使用，请选中 保存配置复选框。
5. 单击确定。



创建证书签名请求 **(CSR)**

April 23, 2021

证书签名请求 (CSR) 是将在其中使用证书的服务器上生成的加密文本块。它包含将包含在证书中的信息，例如您组织的名称、公用名（域名）、区/县和国家/地区。

要使用 **Citrix ADM** 创建 **CSR**，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “ 网络” > “ **SSL** 仪表板”。
2. 单击任何图形以查看已安装 SSL 证书的列表，然后选择要为其创建 CSR 的证书，然后从选择 操作列表中选择创建 **CSR** 。

3. 在 **Create Certificate Signing Request (CSR)**（创建证书签名请求 (CSR)）页面上，为 CSR 指定名称。
4. 执行以下操作之一：
   - **Upload a key**（上载密钥）- 选择 **I have a Key**（我有密钥）选项。要上传密钥文件，请选择本 地（您的本地计算机）或 设备（密钥文件必须存在于 Citrix ADM 虚拟实例上）。
   - 创建密钥 -选择我没有密钥选项，然后指定以下参数：

加密算法	Type of key（密钥类型）。例如 RSA。
Key File Name（密钥文件名称）	存储 RSA 密钥的文件的名称。
密钥大小	密钥大小（以位为单位）。
Public Exponent Value（公共指数值）	从提供的下拉列表中选择 **3** 或 **F4** 。此值属于创建 RSA 密钥所需的密码算法的一部分。
Key Format（密钥格式）	默认情况下，选择 PEM。PEM 是建议的 SSL 证书密钥格式。
PEM Encoding Algorithm（**PEM** 编码算法）	在下拉列表中，选择要用于加密生成的 RSA 密钥的算法（**DES** 或 **DES3**）。如果选择此算法，则需要提供 PEM 密码。
PEM Passphrase（**PEM** 密码）	如果选择了 “PEM Encoding Algorithm”（PEM 编码算法），请输入密码。
Confirm PEM Passphrase（确认 **PEM** 密码）	确认 PEM 密码。

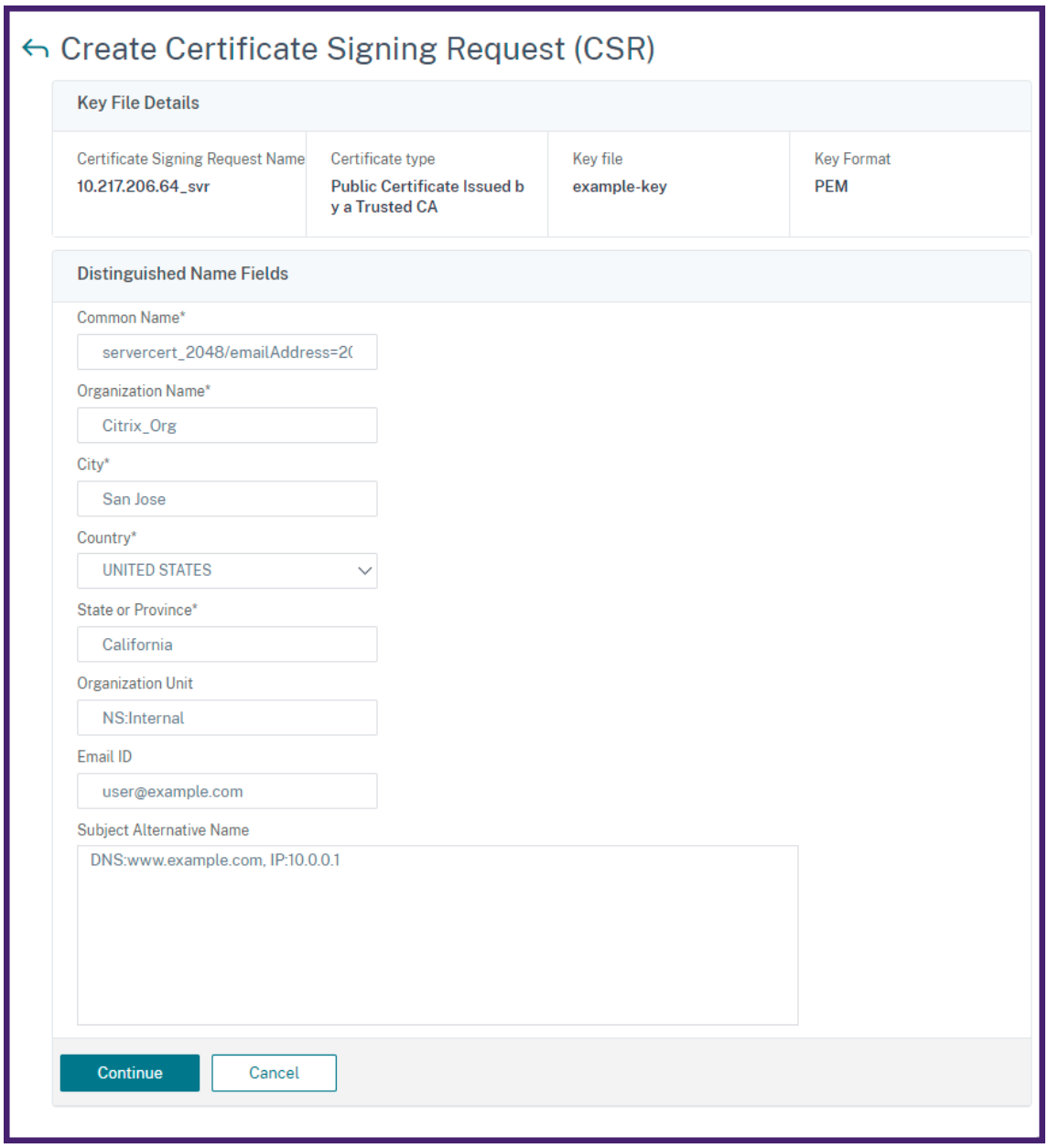
5. 单击继续。
6. 在下一页中，提供更多详细信息。

   大多数字段都有从所选证书的主题提取的默认值。主题包含公用名、组织名称、省/市/自治区和国家/地区之类的详细信息。

   在 “主 题备用名称” 字段中，您可以使用单个证书指定多个值，例如域名和 IP 地址。主题备选名称可帮助您使用单个证书保护多个域的安全。

   按以下格式指定域名和 IP 地址：

```
DNS:<Domain name>, IP:<IP address>
<!--NeedCopy-->
```

在这个例子中，它可以保护 `10.0.0.1` 和 `www.example.com`。

查看字段，然后单击 继续。

> 注意
>
> 大多数 CA 接受通过电子邮件提交证书。CA 将向您提交 CSR 的电子邮件地址返回有效证书。

链接和取消链接 **SSL** 证书

April 23, 2021

可以将多个证书链接在一起来创建证书捆绑包。要将证书链接到另一个证书，第一个证书的颁发者必须匹配第二个证书的域。例如，如果要将证书 A 链接到证书 B，证书 A 的“颁发者”必须匹配证书 B 的“域”。

要使用 **Citrix ADM** 将一个 **SSL** 证书链接到另一个证书，请执行以下操作：

1. 在 Citrix Application Delivery Management (ADM) 中，导航到 “ 网络” > “ **SSL** 仪表板”。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择要链接的证书，然后从 **Action**（操作）下拉列表中选择 **Link**（链接）。
4. 从匹配的证书列表中选择要链接到的证书，然后单击 **OK**（确定）。

> 注意
>
> 如果未找到匹配的证书，将显示以下消息：No certificate found to link（未找到证书进行链接）。

要使用 **Citrix ADM** 取消 **SSL** 证书的链接，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > **SSL** 控制板。
2. 单击任何一个图形以查看 SSL 证书列表。
3. 选择链接的任一已链接证书，然后从 **Action**（操作）下拉列表中选择 **Unlink**（取消链接）。
4. 单击确定。

> 注意
>
> 如果所选证书未链接到另一个证书，将显示以下消息：Certificate does not have any CA link（证书没有任何 CA 链接）。

配置企业策略

April 23, 2021

您可以在 Citrix Application Delivery Management (ADM) 中配置企业策略并添加所有受信任的 CA、安全签名算法，并为证书密钥选择建议的密钥强度。如果 Citrix 应用程序 Delivery Controller (ADC) 实例上安装的任何证书尚未添加到企业策略中，则 SSL 证书仪表板会将这些证书的颁发者显示为 “ 不推荐”。

此外，如果证书密钥强度与企业策略中建议的密钥强度不匹配，则 SSL 证书仪表板会将这些密钥的强度显示为 “ 不推荐”。

要在 **Citrix ADM** 上配置企业策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 基础架构” > “ **SSL** 仪表板”，然后单击 “ 设置”。
2. 在 “SSL 设置” 页面上，单击 “ 编辑” 图标以添加所有受信任的 CA、安全的签名算法，并为证书和密钥选择建议的密钥强度。
3. 单击 **Save**（保存）以保存企业策略。

轮询来自 **Citrix ADC** 实例的 **SSL** 证书

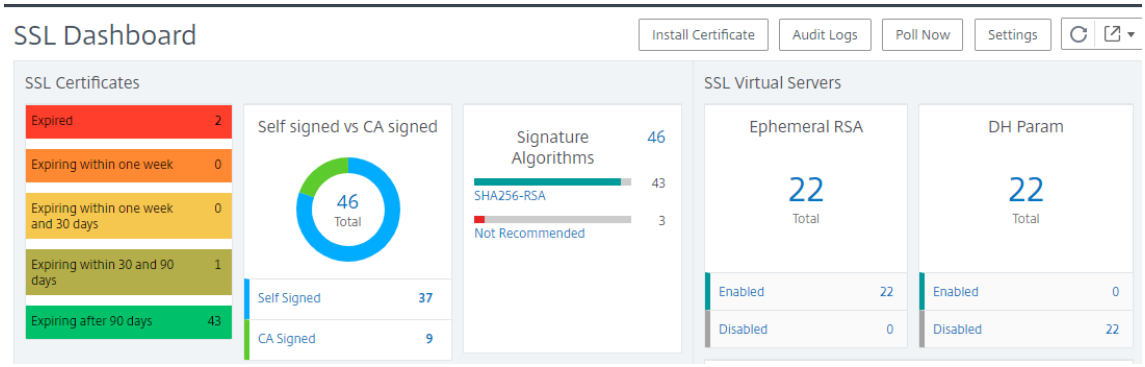
April 23, 2021

通过使用 NITRO 调用和安全拷贝 (SCP) 协议，Citrix Application Delivery Management (ADM) 每 24 小时自动轮询一次 SSL 证书。您还可以手动轮询 SSL 证书，以发现 Citrix 应用程序 Delivery Controller (ADC) 实例上新添加的 SSL 证书。轮询所有 Citrix ADC 实例 SSL 证书会给网络带来沉重负载。

您可以只手动轮询一个或多个选定实例的 SSL 证书，而不是轮询所有 Citrix ADC 实例 SSL 证书。

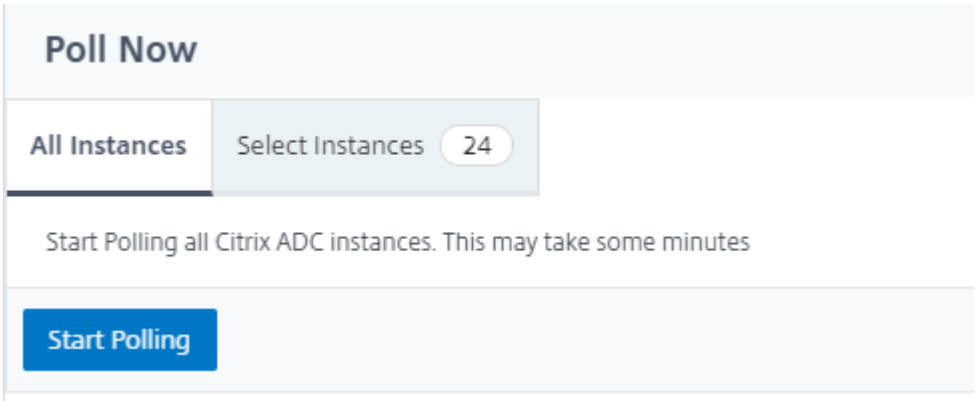
要在 **Citrix ADC** 实例上轮询 **SSL** 证书，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > **SSL** 控制板。
2. 在 **SSL** 仪表板页面的右上角，单击 立即轮询。

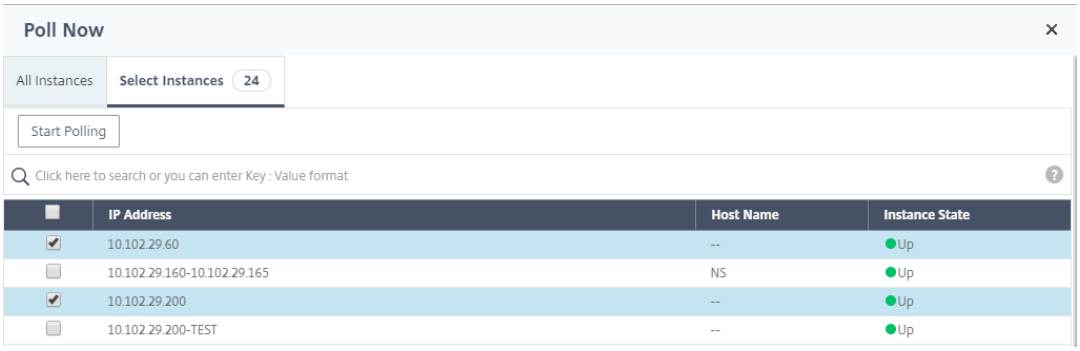


3. 此时会弹出 “立 即轮询页面，您可以选择轮询网络中的所有 Citrix ADC 实例或轮询选定实例。

   a) 要轮询所有 Citrix ADC 实例的 SLL 证书，请选择 所有实例” 选项卡，然后单击 开始轮询。



   b) 要轮询特定实例，请选择 选择实例选项卡，从列表中选择实例，然后单击 立即轮询。



配置 IP 地址管理 (IPAM)

April 23, 2021

ADM IPAM 让您能够在 ADM 托管配置中自动分配和释放 IP 地址。您可以从使用以下 IP 提供程序定义的网络或 IP 范围分配 IP：

- ADM 内置 IPAM 提供程序。
- 信息布鲁 IPAM 解决方案。有关详细信息，请参阅 DDI 信息。

目前，您可以在以下位置使用 ADM IPAM：

- 样书：创建配置时自动将 IP 分配到虚拟服务器。
- **Kubernetes** 入口：自动为 Kubernetes 群集中的入口配置分配虚拟 IP 地址。

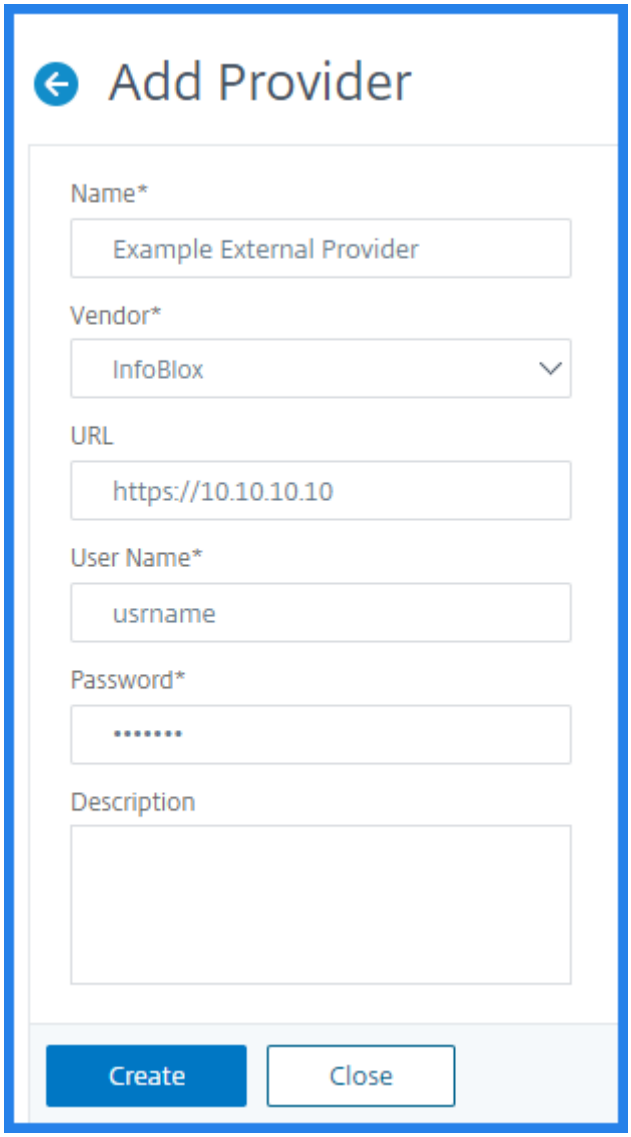
您还可以跟踪 ADM 管理的每个网络或 IP 范围内的已分配和可用 IP 地址。

添加外部 IP 地址提供程序

ADM 具有内置 IPAM 提供程序来管理 IP 和 IP 范围。如果要在 ADM 中添加外部 IP 提供程序解决方案，请执行以下步骤：

1. 导航到 **“网络” > “IPAM”**。
2. 在 提供程序中，单击 添加。
3. 指定以下详细信息以添加 IP 提供程序：
    - 名称 - 指定要在 ADM 中使用的 IP 提供程序名称。
    - 供应商 -从列表中选择 IP 地址供应商。
    - **URL** -指定在 ADM 环境中分配 IP 地址的 IPAM 解决方案的 URL。
    - 用户名 -指定登录 IPAM 解决方案的用户名。
    - 密码 -指定登录 IPAM 解决方案的密码。

4. 单击添加。



添加网络

添加网络以将 IPAM 与 ADM 托管配置结合使用。

1. 导航到 **“网络” > “IPAM”**。
2. 在 网络中，单击 添加。
3. 指定以下详细信息：
   - 网络名称 -指定网络名称以标识 ADM 中的网络。
   - 提供程序 -从列表中选择提供程序。

     此列表显示在 ADM 中添加的提供程序。

- 网络类型 -根据您的要求从列表中选择 **IP** 范围或 **CIDR** 。
- 网络值 -指定网络值。

  > 注意
  >
  > ADM IPAM 仅支持 IPv4 地址。

  对于 **IP** 范围，请按以下格式指定网络值：

  ```
  <first-IP-address>-<last-IP-address>
  <!--NeedCopy-->
  ```

  示例:

  ```
  10.0.0.20-10.0.0.100
  <!--NeedCopy-->
  ```

  对于 **CIDR**，请按以下格式指定网络值：

  ```
  <IP-address>/<subnet-mask>
  <!--NeedCopy-->
  ```

  示例:

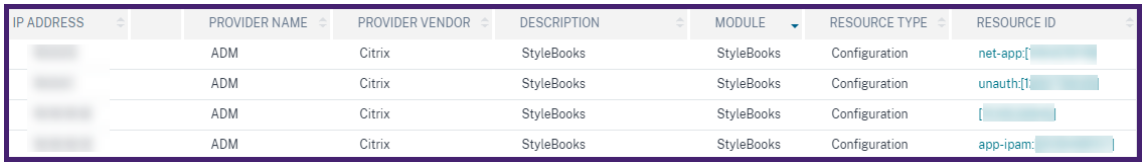
  ```
  10.70.124.0/24
  <!--NeedCopy-->
  ```

4. 单击创建。

查看分配的 **IP** 地址

要查看有关从 IPAM 网络分配的 IP 地址的更多详细信息，请执行以下步骤：

1. 导航到 **“网络” > “IPAM”**。
2. 在 网络选项卡中，单击 查看所有已分配的 **IP**。



IP ADDRESS	PROVIDER NAME	PROVIDER VENDOR	DESCRIPTION	MODULE	RESOURCE TYPE	RESOURCE ID
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	net-app:[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	unauth:[1
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	[
[redacted]	ADM	Citrix	StyleBooks	StyleBooks	Configuration	app-ipam:

此窗格显示 IP 地址、提供商名称、提供商供应商和描述。它还显示保留此 IP 地址的资源详细信息：

- 模块：显示保留 IP 地址的 ADM 模块。例如，如果 IP 地址由样书保留，则此列将样书显示为模块。
- 资源类型：显示该模块中的资源类型。对于样书模块，只有配置资源类型使用 IPAM 网络。
- 资源 **ID**：显示带链接的资源 ID。单击此链接可访问使用 IP 地址的资源。对于配置资源类型，资源 ID 显示为配置包 ID。

> 注意：
>
> 如果要释放 IP 地址，请选择要释放的 IP 地址，然后单击 释放已分配的 **IP**。

配置作业

April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 配置管理流程可确保在网络中的多个 Citrix 应用程序 Delivery Controller (ADC) 实例之间正确复制配置更改、系统升级和其他维护活动。

Citrix ADM 允许您创建配置作业，以帮助您作为一项任务在多台设备上轻松执行所有这些活动。配置作业和模板将最重复的管理任务简化为 Citrix ADM 上的单个任务。配置作业包含可以在一个或多个托管设备上运行的一组配置命令。

配置作业可以使用 SSH 命令执行配置命令，也可以使用 SCP 将文件副本从本地存储复制到另一个设备，例如，可以计划 HA 故障转移或 HA 升级。

您可以在 Citrix ADM 中使用以下四个选项之一来创建配置作业。使用其中一个创建可重复使用的命令和指令来源，用于系统运行配置作业。

1. 配置模板
2. 实例
3. 文件
4. 录制和播放

配置模板

您可以在创建作业并将一组配置命令另存为模板的同时创建配置模板。在“Create Jobs”（创建作业）页面上保存这些模板时，它们会自动显示在“Create Template”（创建模板）页面上。

> 注意：
> 对于默认配置模板，“ 重命名”选项处于禁用状态。但是，您可以重命名自定义配置模板。

您可以使用以下模板之一：

配置编辑器：您可以使用配置编辑器键入 CLI 命令，将配置另存为模板，然后使用它配置作业。

内置模板：您可以从配置模板列表中进行选择。这些模板提供了 CLI 命令的语法，并允许您为变量指定值。下表中列出了内置模板及其说明。可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，可以使用内置模板选项计划作业来配置 syslog 服务器。您还可以选择立即运行作业或安排在稍后阶段运行作业。

实例

您可以对运行 Citrix ADC 11.0 版及更高版本的 Citrix SDX 实例执行单捆绑升级。要执行单捆绑升级，请使用 Citrix ADM 中的内置任务。您还可以通过提取运行配置或保存的配置并在另一个同类型的 Citrix ADC 实例上运行命令来升级 Citrix ADC 实例。这样，您可以在一个实例上复制另一个实例的配置。

文件

您可以从本地计算机上载配置文件并创建作业。

使用文件的优势

- 您可以使用任何文本文件来创建可重用的配置命令源。
- 不需要进行任何种类的格式设置。
- 文件可以保存在您的本地计算机上。

您可以创建并保存新文件，也可以导入现有文件，然后运行命令。

录制和播放

使用创建作业，您可以输入自己的 CLI 命令，也可以使用录制和播放按钮从 Citrix ADC 会话中获取命令。运行作业时，选定实例上 ns.conf 中的更改将被记录并复制到 Citrix ADM。

相关文章

- 如何在配置作业中使用 SCP (put) 命令
- 如何在配置作业中使用变量
- 如何从更正命令创建配置作业
- 如何使用配置模板创建审计模板
- 如何使用录制和播放来创建配置作业
- 如何在 Citrix ADM 上使用主配置模板

创建配置作业

April 23, 2021

作业是可以在一个或多个托管实例上创建并运行的一组配置命令。您可以创建作业以在网络上跨实例进在多个实例上复制配置行配置更改，录制和播放配置任务使用 Citrix Application Delivery Management (ADM) GUI 并将其转换为 CLI 命令。

您可以使用 Citrix ADM 的配置作业功能创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

要在 **Citrix ADM** 上创建配置作业，请执行以下操作：

1. 导航到 **“网络” > “配置作业”**。
2. 单击 创建作业。
3. 在 创建作业页上的 选择配置选项卡下，指定作业名称并从列表中选择 实例类型。
4. 在 配置源列表中，选择要创建的配置作业模板。为选定模板添加命令。
   - 您可以输入命令，也可以从保存的配置模板导入现有命令。
   - 在配置作业中创建作业时，还可以在配置编辑器中添加不同类型的多个模板。
   - 从 “ 配置源” 列表中，选择不同的模板，然后将模板拖到配置编辑器中。模板类型可以是 配置模板、内置模板、主配置、录制和播放、实例和 文件。

   > 注意
   >
   > 如果首次添加 `Deploy Master Configuration Job` 模板，请添加不同类型的模板，则整个作业模板将变为 `Master Configuration` 类型。

   您还可以在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。您还可以在编辑配置作业时重新排列命令行并重新排序。

   您可以定义变量，使您能够为这些参数分配不同的值或跨多个实例运行作业。您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。单击 “预览变量” 选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。

   您可以为配置编辑器上的每个命令自定义回滚命令。要指定自定义命令，请启用自定义回滚选项。

   > ** 重
   >
   > 要说明要使自定义回滚生效，请完成创建作业” 向导。在执行” 选项卡中，从命令 失败列表中选择 “回滚成功命令 ** 选项。

5. 在 “ 选择实例” 选项卡中，选择要运行配置审核的实例。
   a) 在 Citrix ADC 高可用性对中，您可以在主节点或辅助节点的本地运行配置作业。选择要在哪个节点上运行作业。
      - 在主节点上执行 -选择此选项可仅在主节点上运行作业。
      - 在辅助节点上执行 -选择此选项可仅在辅助节点上运行作业。

      您还可以选择主节点和辅助节点来运行同一配置作业。如果未选择主节点或辅助节点，配置作业将自动在主节点上运行。
6. 在 “指定变量值” 选项卡中，有两个选项：
   a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
   b) 输入已为所有实例定义的变量的公用值

c) 单击下一步。

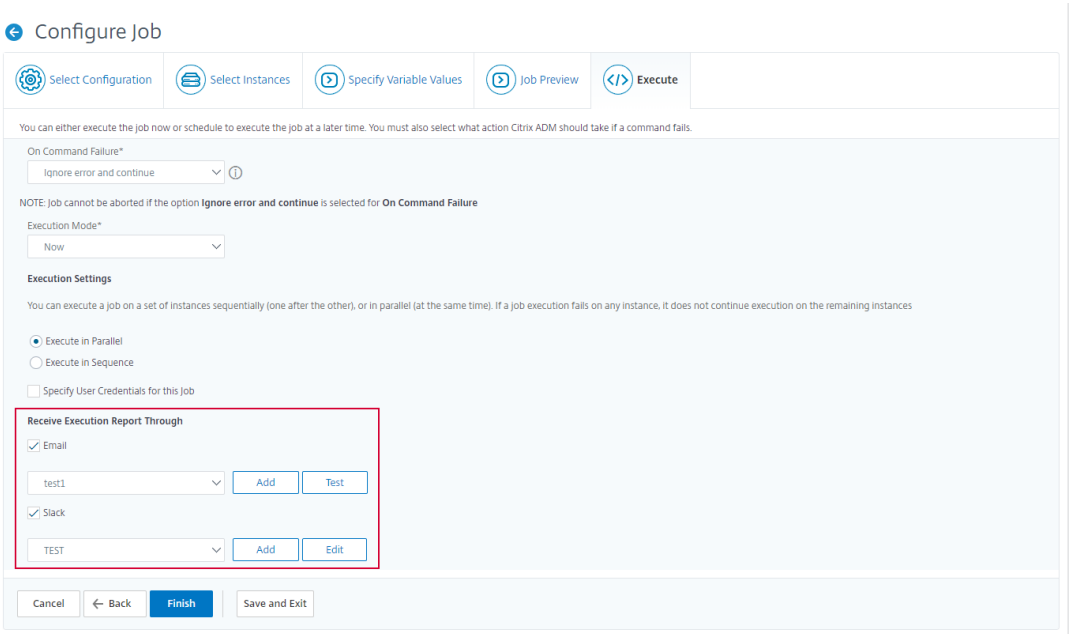
要发送任务的电子邮件和 **Slack** 通知，请执行以下操作：

现在，每次运行或计划作业时，都会发送电子邮件和 Slack 通知。通知包括作业成功或失败等详细信息以及相关详细信息。

1. 导航到 “ 网络” > “配置作业”。
2. 选择要启用电子邮件和 Slack 通知的作业，然后单击 编辑。
3. 在 执行” 选项卡中，转到 通过接收执行报告窗格：
   - 选中 电子邮件复选框，然后选择要向其发送执行报告的电子邮件通讯组列表。

     如果要添加电子邮件通讯组列表，请单击 添加并指定电子邮件服务器详细信息。
   - 选中 **Slack** 复选框，然后选择要向其发送执行报告的松弛通道。

     如果要添加 Slack 配置文件，请单击 添加并指定所需 Slack 频道的 配置文件名称、频道名称和 令牌。



4. 单击完成。

要发送任务的电子邮件和 **Slack** 通知，请执行以下操作：

现在，每次运行或计划作业时，都会发送电子邮件和 Slack 通知。通知包括作业成功或失败等详细信息以及相关详细信息。

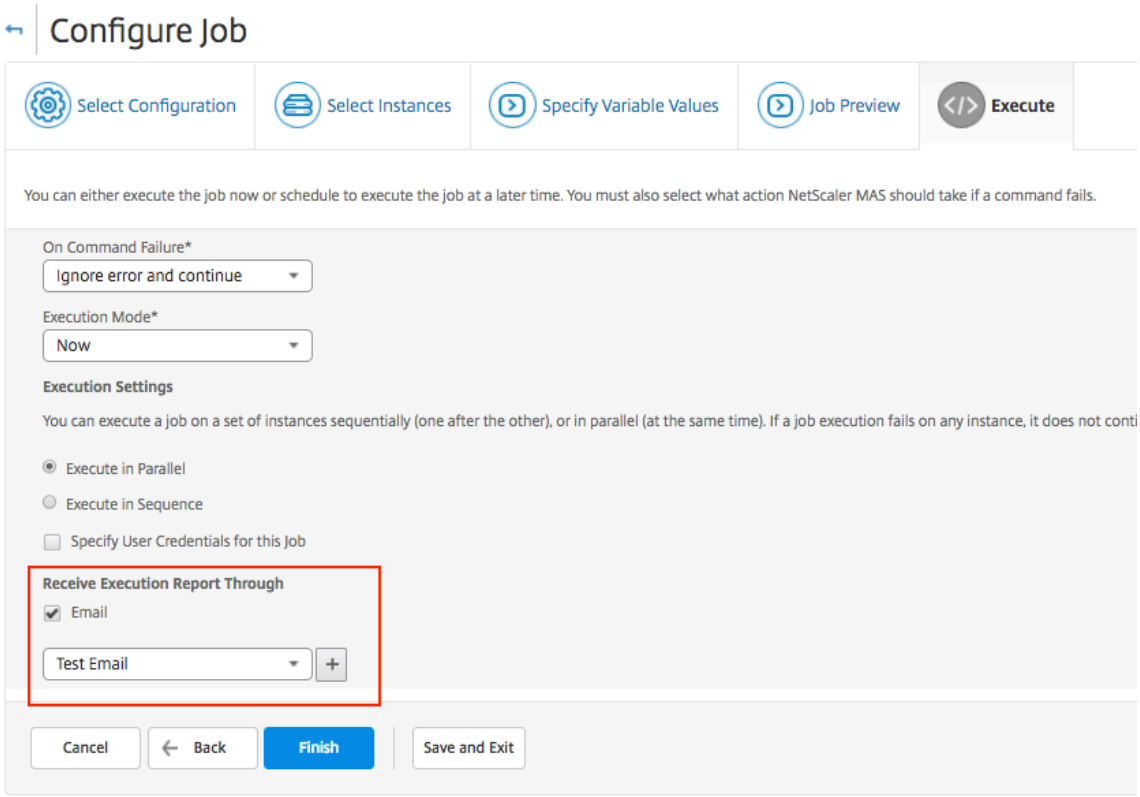
1. 导航到 “ 网络” > “配置作业”。
2. 选择要启用电子邮件和 Slack 通知的作业，然后单击 编辑。
3. 在 执行” 选项卡中，转到 通过接收执行报告窗格：

- 选中 电子邮件复选框，然后选择要向其发送执行报告的电子邮件通讯组列表。

  如果要添加电子邮件通讯组列表，请单击 添加并指定电子邮件服务器详细信息。

- 选中 **Slack** 复选框，然后选择要向其发送执行报告的松弛通道。

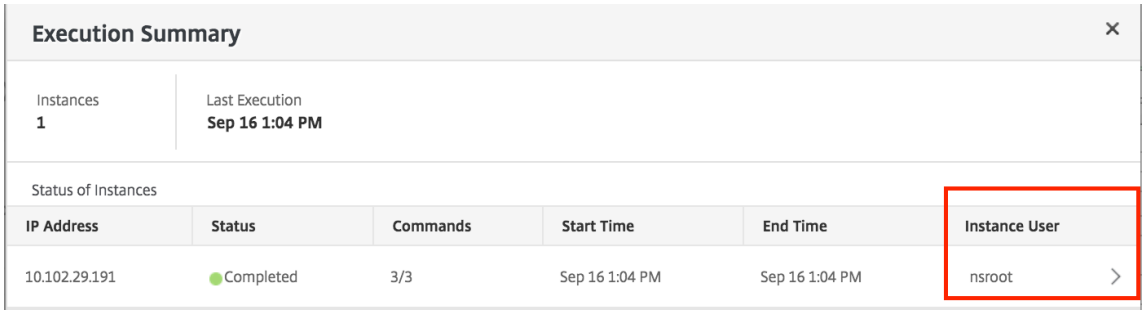
  如果要添加 Slack 配置文件，请单击 添加并指定所需 Slack 频道的 配置文件名称、频道名称和 令牌。



4. 单击完成。

要查看执行摘要详细信息，请执行以下操作：

1. 导航到 “ 网络” > “ 配置作业”。
2. 选择要查看执行摘要的作业，然后单击 详细信息。
3. 单击 “ 执行摘要” 以查看：
   - 运行作业的实例的状态
   - 这些命令在作业上运行
   - 作业的开始和结束时间，以及
   - 实例用户的名称



使用录制和播放创建配置作业

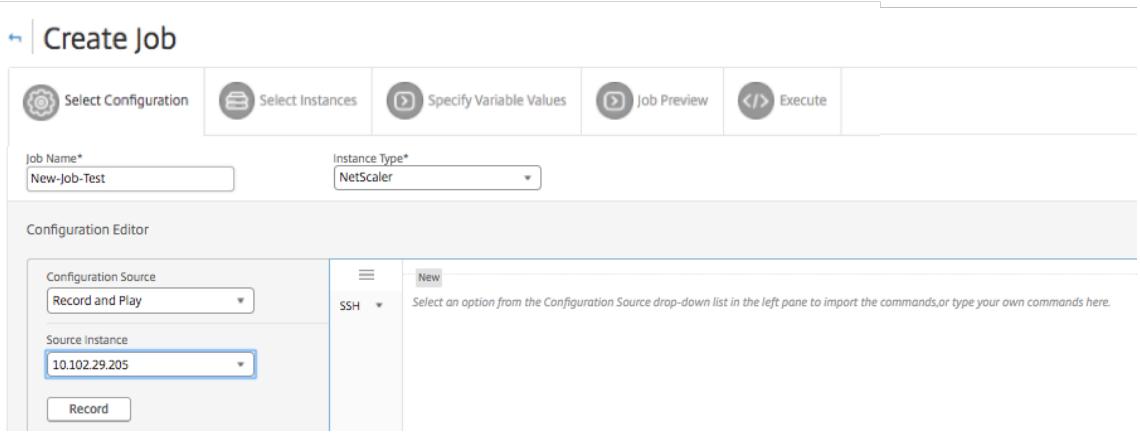
April 23, 2021

如果您习惯于使用 Citrix ADC GUI 配置 Citrix ADC 实例，有时会发现很难调用确切的 CLI 命令来创建配置任务并在多个 Citrix ADC 实例上运行该任务。

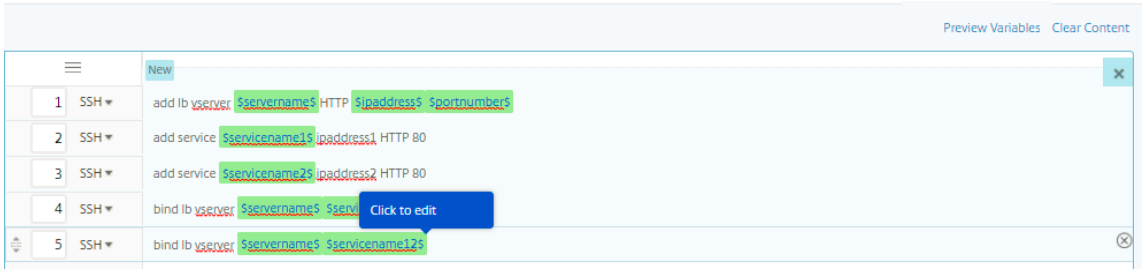
通过 Citrix ADM，您可以记录使用 Citrix ADC 实例的 GUI 执行的配置任务，并将其转换为 CLI 命令。之后可以使用这些 CLI 命令创建配置任务，并在多个实例上运行此任务。

录制 **GUI** 配置并将其转换为配置任务

1. 导航到 **Networks**（网络）> **Configuration Jobs**（配置作业），然后单击 **Create Job**（创建作业）。
2. 指定作业名称和实例类型。
3. 从 配置源列表中，选择 录制并播放”，然后选择要从中录制配置的源实例。单击 **Record**（录制）。

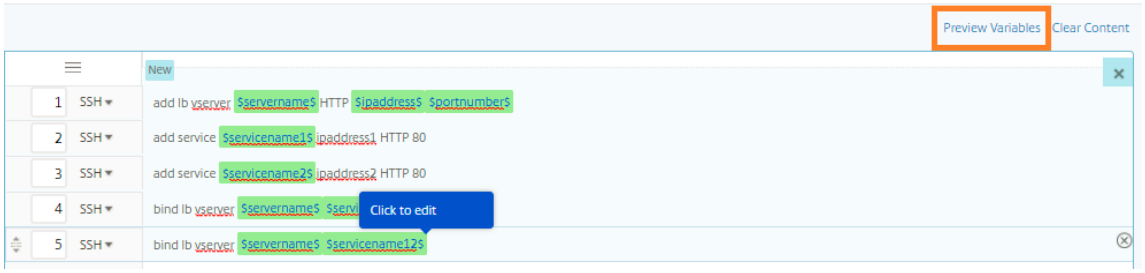


4. 将打开 **Citrix ADC** 图形用户界面。配置您希望配置任务包含的功能和设置。然后，关闭 Citrix ADC GUI 窗口，然后单击 配置编辑器中的 停止。在左侧窗格中，命令显示为链接。将命令拖动到右侧窗格中，然后单击 下一步。

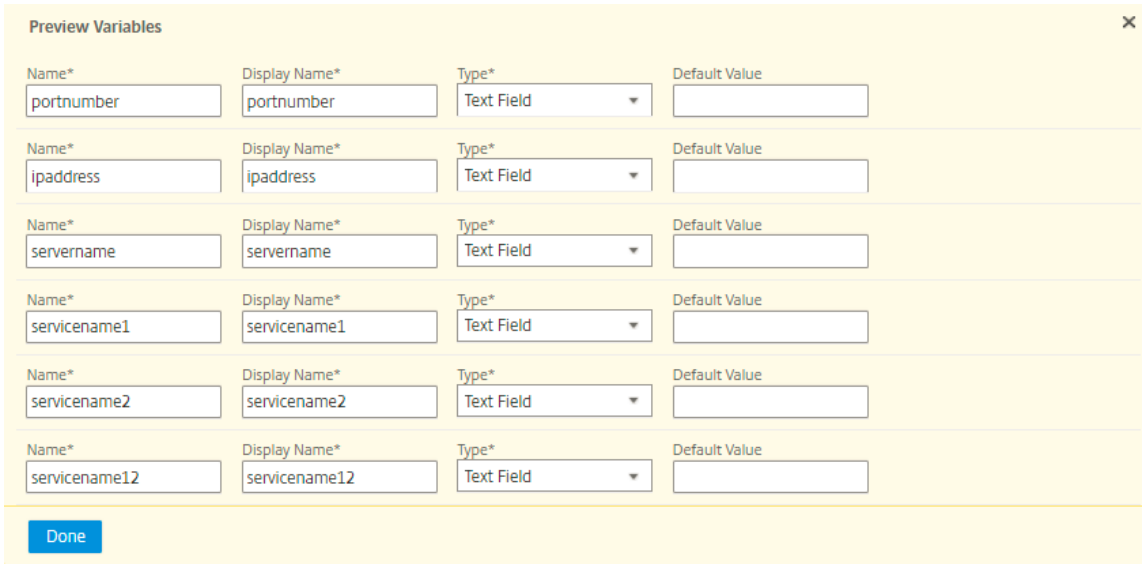


然后，您可以根据需要在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。

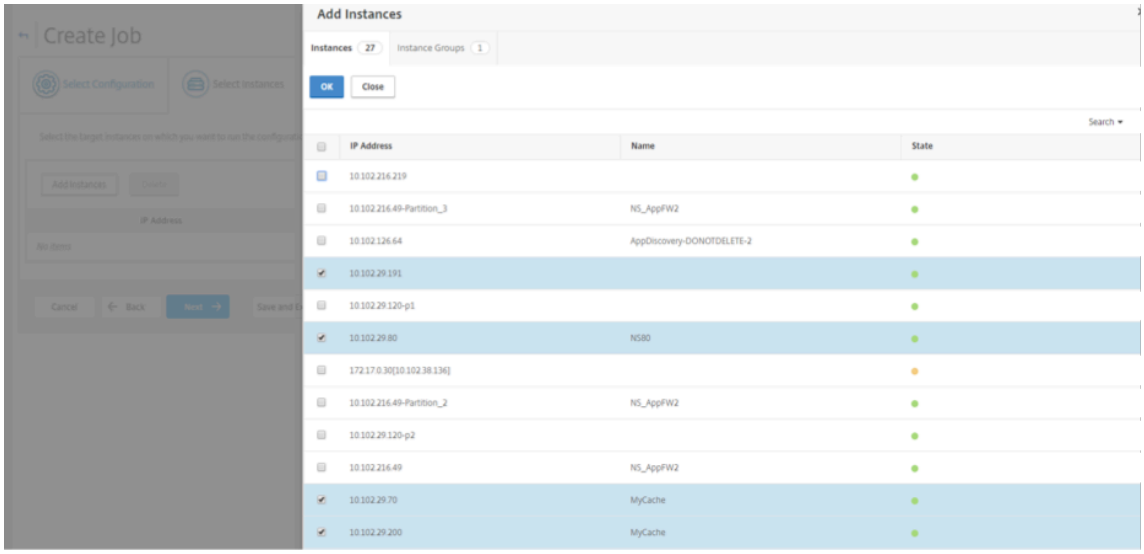
5. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
6. 执行以下操作之一以查看单个统一视图中的所有变量：
   - 创建配置作业时，导航到 **“网络” > “配置作业”**，选择 “ 创建作业”。在 创建作业页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **“网络” > “配置作业”**，选择 “作业名称”，然后单击 “ 编辑”。在 配置作业页面上，您可以查看创建配置作业时添加的所有变量。
7. 然后，您可以单击预览变量选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



8. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完成” 按钮。



9. 单击添加实例，然后选择要在其上运行配置作业的实例。单击“确定”，然后单击“下一步”。



10. 如果在命令中指定了变量，请在“指定变量值”选项卡上，选择以下选项之一以指定实例的变量：

    - 上传变量值的输入文件：单击下载输入密钥文件下载输入文件。在输入文件中，输入已在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
    - 所有实例的公用变量值：输入变量值。变量因选定的模板而不同。

    包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上传的这些输入文件。

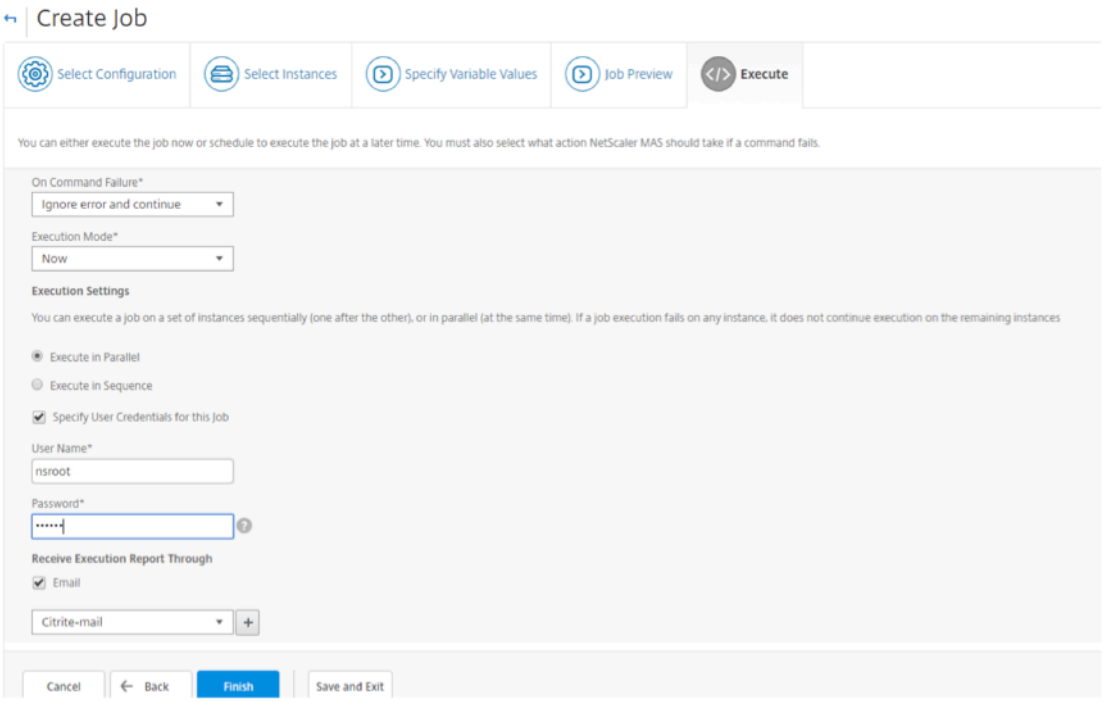
    要在创建配置作业时查看运行配置作业，请导航到网络 **>** 配置作业，然后单击创建作业。在 创建任务页面中。在指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

    要在编辑配置作业时查看已运行的配置作业，请导航到网络 **>** 配置作业，选择作业名称，然后单击编辑。在 配置作业页面的 指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）.10. 在“作 业预览”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

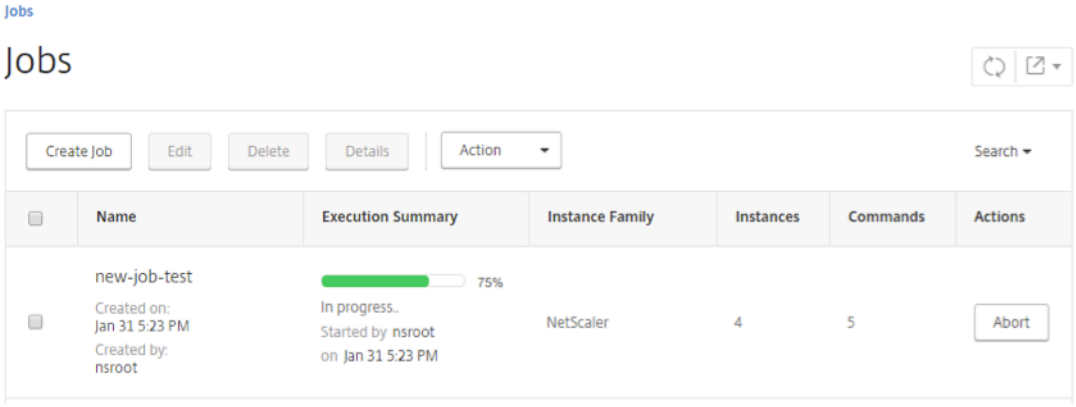
11. 在作业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

12. 在执行选项卡上，您可以选择立即运行作业或计划稍后运行作业。您还可以选择如果命令失败，Citrix ADM 必须采取的操作。

    您还可以选择允许授权用户在托管实例上运行作业，也可以选择是否发送有关作业成功还是失败的电子邮件通知以及其他详细信息。



13. 在“作 业页面上，您可以查看所有实例上的配置任务执行进度。



使用配置作业将配置从一个实例复制到多个实例

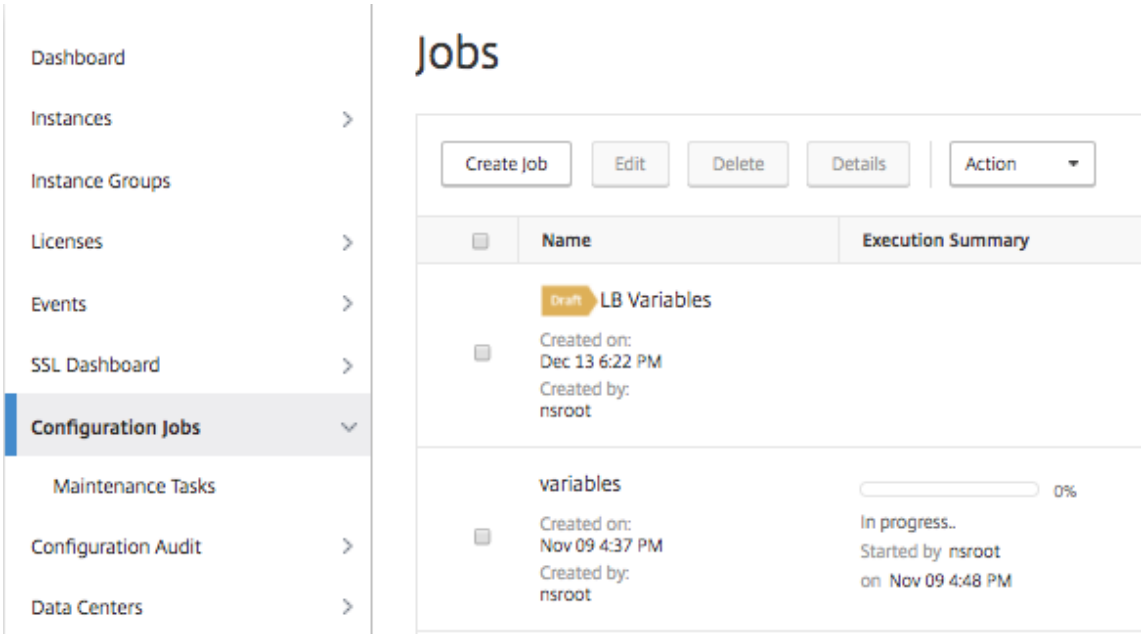
April 23, 2021

您可以使用 Citrix ADM 的配置作业功能从 Citrix ADC 实例中提取特定配置并将其复制到多个实例上。

例如，您可能已在 Citrix ADC 实例上为您的部署配置了负载平衡和前端优化 (FEO)。但是，现在您只想将 FEO 配置复制到其他 Citrix ADC 实例。

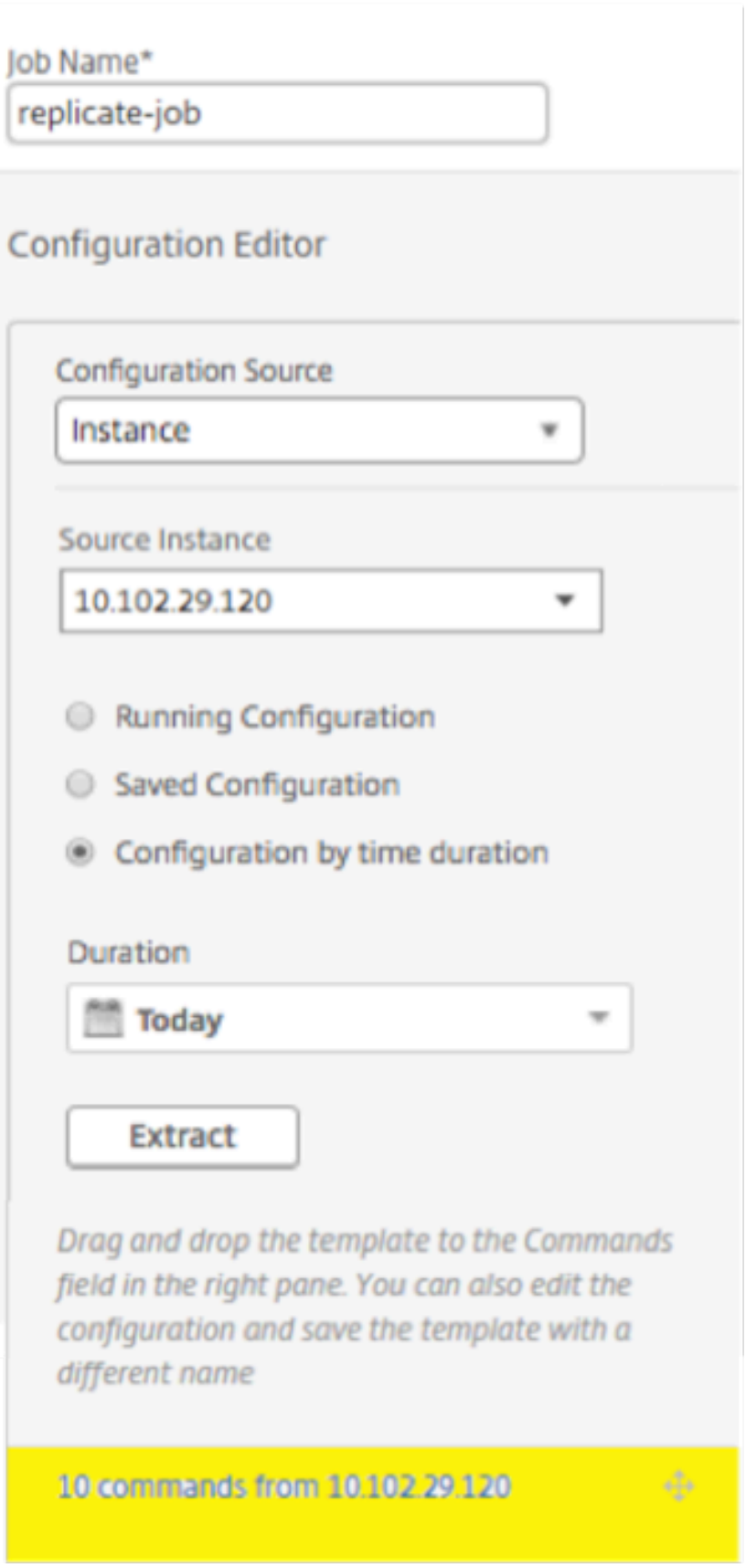
要检索配置并将其从一个实例复制到其他 **Citrix ADC** 实例，请执行以下操作：

1. 导航到 **Networks**（网络）> **Configuration Jobs**（配置作业），然后单击 **Create Job**（创建作业）。



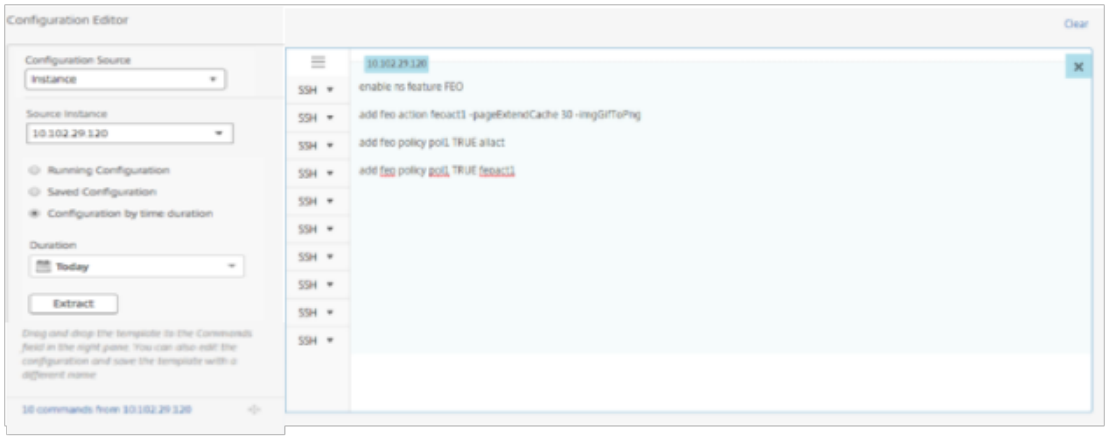
2. 指定作业名称和实例类型。
3. 选择 实例作为 配置源，然后选择要复制其配置的源实例。选择要提取的配置类型。如果您选择“按时间持续时间配置”，设置运行此配置的时间段，然后单击 提取”。

   在您选择的持续时间内，该实例上运行的命令数将显示在屏幕上，如下图所示。



4. 将命令拖动到右侧窗格中的 “ 命令” 字段中。

仅保留与 FEO 有关的命令，手动删除与负载平衡有关的命令，或与任何其他配置有关的命令，然后单击 **Next**（下一步）。



5. 单击 添加实例，然后添加要应用 FEO 配置的实例。单击 “ 确定”，然后单击 “ 下一步”。
6. 如果在命令中指定了变量，请在 “Specify Variable Values”（指定变量值）选项卡上单击 **Download Input Key File**（下载输入密钥文件）。在下载的文件中，为变量指定值，然后将文件上载到 Citrix ADM。
7. 在 “作 业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
8. 在执行选项卡上，单击完成以在选定的 Citrix ADC 实例上运行作业。

在配置作业中使用变量

April 23, 2021

配置作业是一组配置命令，您可以在一个或多个托管实例上运行。当您在多个实例上运行相同的配置时，您可能希望为配置中使用的参数使用不同的值。您可以定义变量，使您能够为这些参数分配不同的值或跨多个实例运行作业。

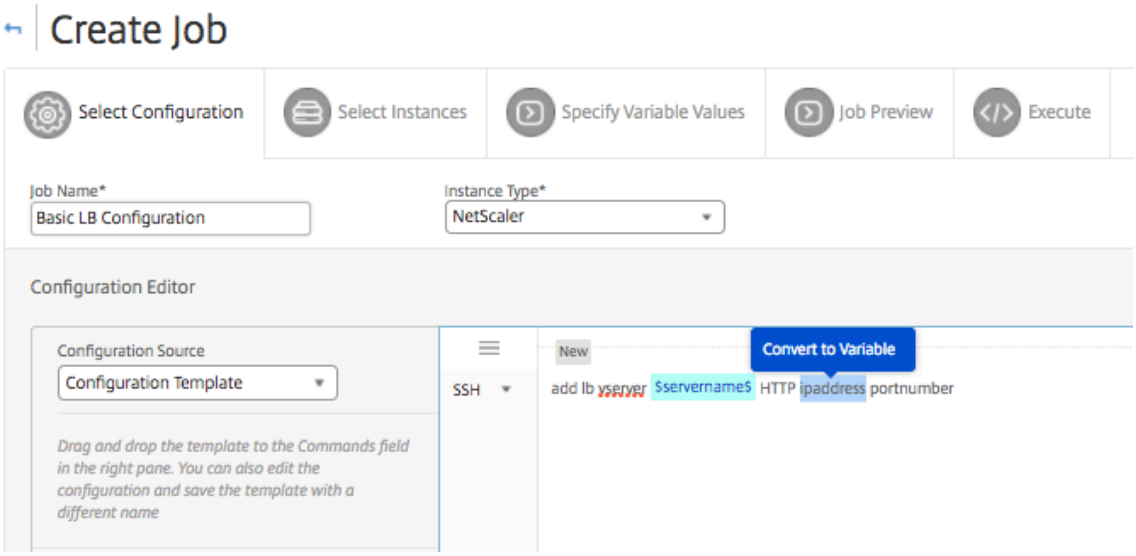
例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。现在，您可能希望两个实例上的配置相同，但虚拟服务器和服务名称和 IP 地址的值不同。您可以使用配置作业功能来实现这一点，即使有变量来定义虚拟服务器和服务名称和 IP 地址。

在此示例中，使用了以下命令和变量：

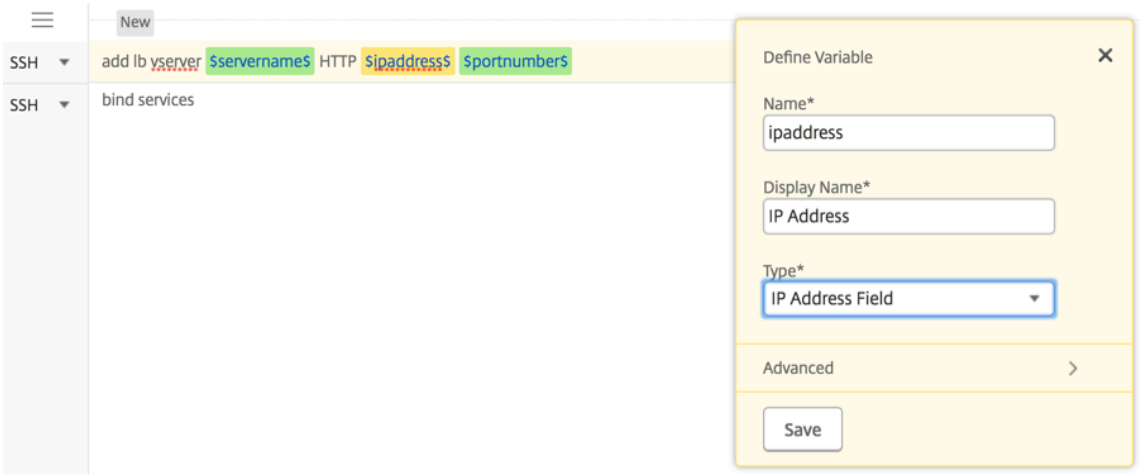
```
add lb vserver <servername> HTTP <ipaddress> <portnumber>

add service <servicename1> <ipaddress1> HTTP 80

add service <servicename2> <ipaddress2> HTTP 80

bind lb vserver <servername> <servicename1>

bind lb vserver <servername> <servicename2>
```

要通过在 **Citrix ADM** 中定义变量来创建配置作业，请执行以下操作：

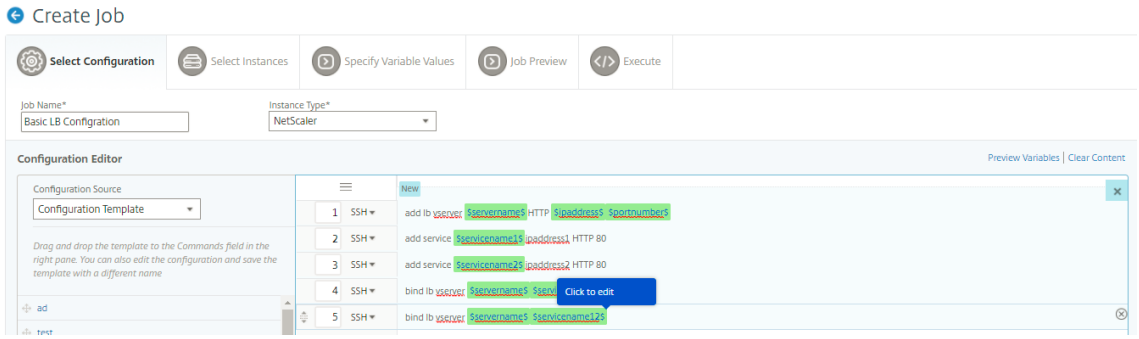
1. 导航到 “ 网络” > “ 配置作业”。
2. 单击 创建作业。
3. 在 “ 创建作业” 页上，选择自定义作业参数，如作业的名称、实例类型和配置类型。
4. 在 “Configuration Editor”（配置编辑器）中，键入命令以添加一个负载平衡虚拟服务器、两个服务以及将服务绑定到虚拟服务器。双击以选择要转换为变量的值，然后单击 转换为变量。例如，选择负载平衡服务器的 IP 地址 `*ipaddress*`，然后单击转换为变量，如下图所示。



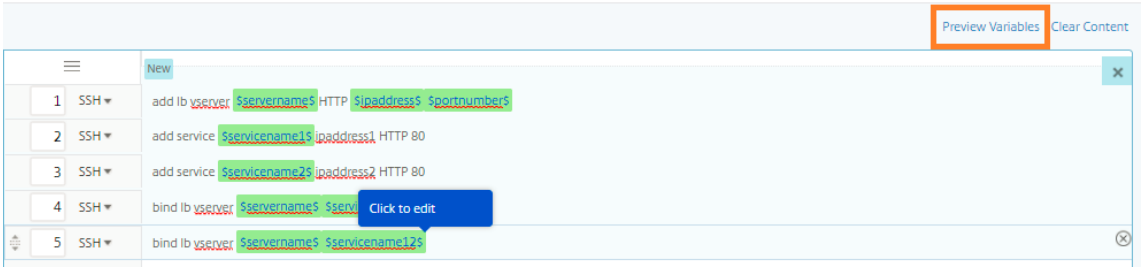
5. 看到美元符号包含变量的值后，单击变量以进一步指定变量的详细信息，例如名称、显示名称和类型。如果要进一步为变量指定默认值，也可以单击 高级” 选项。单击 保存，然后单击 下一步。



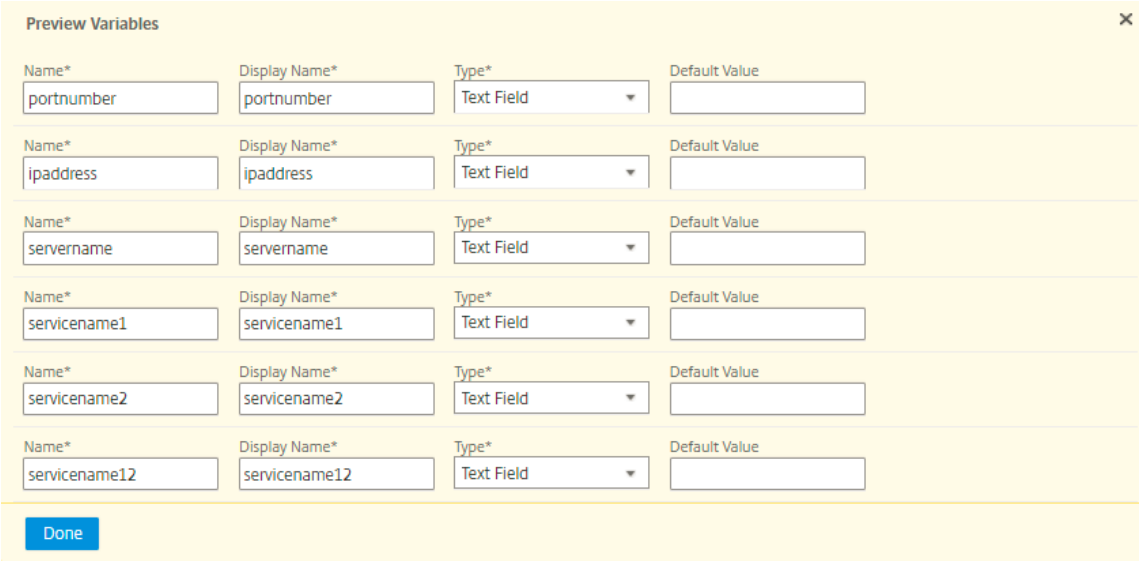
键入命令的其余部分，并定义所有变量。



6. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
7. 执行以下操作之一以查看单个统一视图中的所有变量：
   - 创建配置作业时，导航到 **“网络” > “配置作业”**，选择 “ 创建作业”。在 创建作业页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **“网络” > “配置作业”**，选择 “作业名称”，然后单击 “ 编辑”。在 配置作业页面上，您可以查看创建配置作业时添加的所有变量。
8. 然后，您可以单击预览变量选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



9. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完成” 按钮。

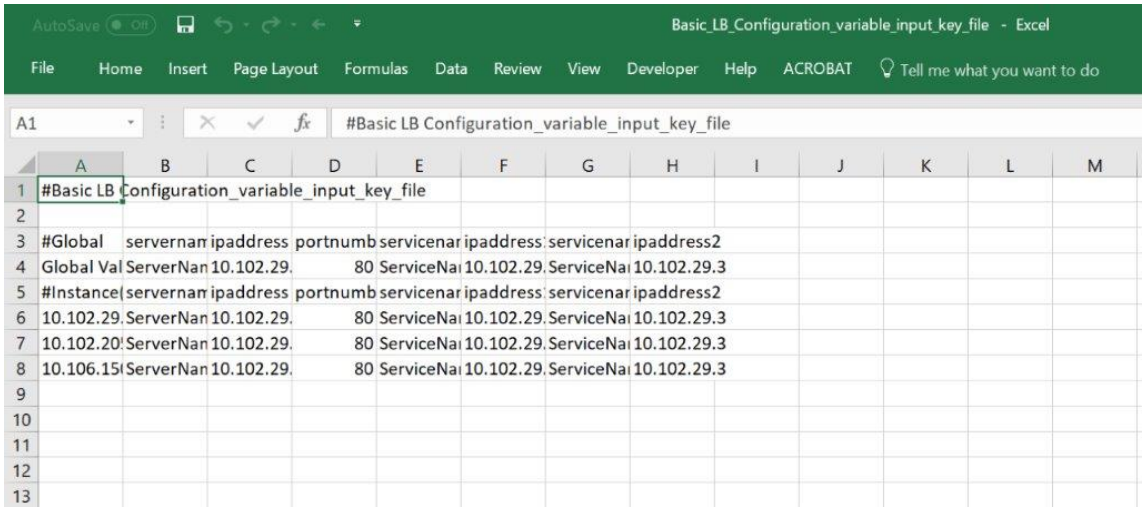


10. 然后，您可以根据需要在配置编辑器中重新排列和重新排序命令。您可以通过拖放命令行将命令从一行移动到另一行。您也可以通过简单地更改文本框中的命令行号，将命令行从一行移动或重新排列到任何目标行。
11. 选择要对其运行配置作业的实例。
12. 在“ 指定变量值”选项卡中，选择“ 上载变量值的输入文件”选项，然后单击“ 下载输入密钥文件”。在我们的示例中，您将需要指定每个实例上的服务器名称、服务器和服务的 IP 地址、端口号以及服务名称。保存文件并将其上载。如果未准确定义您的值，系统可能会抛出错误。
13. 输入密钥文件将下载到本地系统中，您可以通过为之前选择的每个 Citrix ADC 实例指定变量值进行编辑，然后单击“ 上传”将输入密钥文件上载到 Citrix ADM。单击下一步。输入密钥文件将下载到本地系统，您可以通过为之前选择的每个 Citrix ADC 实例指定变量值来对其进行编辑。

    > 注意在输入密钥文件中，变量定义在三个级别：
    >
    > - 全局级别
    > - 实例组级别
    > - 实例级别

    全局变量是应用于所有实例的变量值。实例组级别变量值应用于组中定义的所有实例。实例级别变量值仅应用于特定实例。

    Citrix ADM 给予实例级别值的第一优先级。如果没有为单个实例的变量提供任何值，Citrix ADM 将使用在组级别提供的值。如果在组级别没有提供任何值，Citrix ADM 将使用在全局级别提供的可变值。如果为所有三个级别的变量提供输入，Citrix ADM 将使用实例级别值作为默认值。
14. 单击“ 上载”将输入密钥文件上载到 Citrix ADM。单击下一步。



> 重要
>
> 从 Mac 上传 CSV 文件时，Mac 会使用分号而不是逗号存储 CSV 文件。这将导致配置失败，当您上传输入文件并运行作业。如果您使用的是 Mac，请使用文本编辑器进行必要的更改，然后上传文件。

15. 您还可以为所有实例提供公用变量值，然后单击 **“上传”** 将输入密钥文件上传到 **Citrix ADM**。

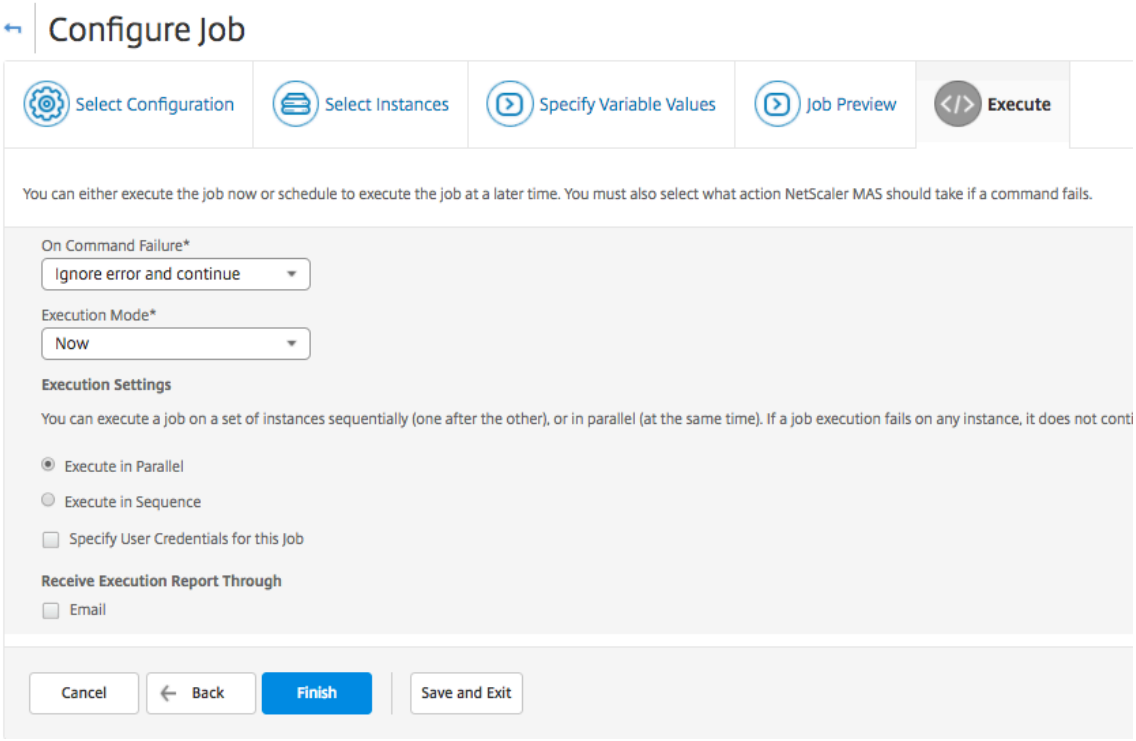
    包含变量值的键输入文件在配置作业中保留（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上传的这些输入文件。

    要在创建配置作业时查看运行配置作业，请导航到网络 **>** 配置作业，然后单击创建作业。在 创建任务页面中。在指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

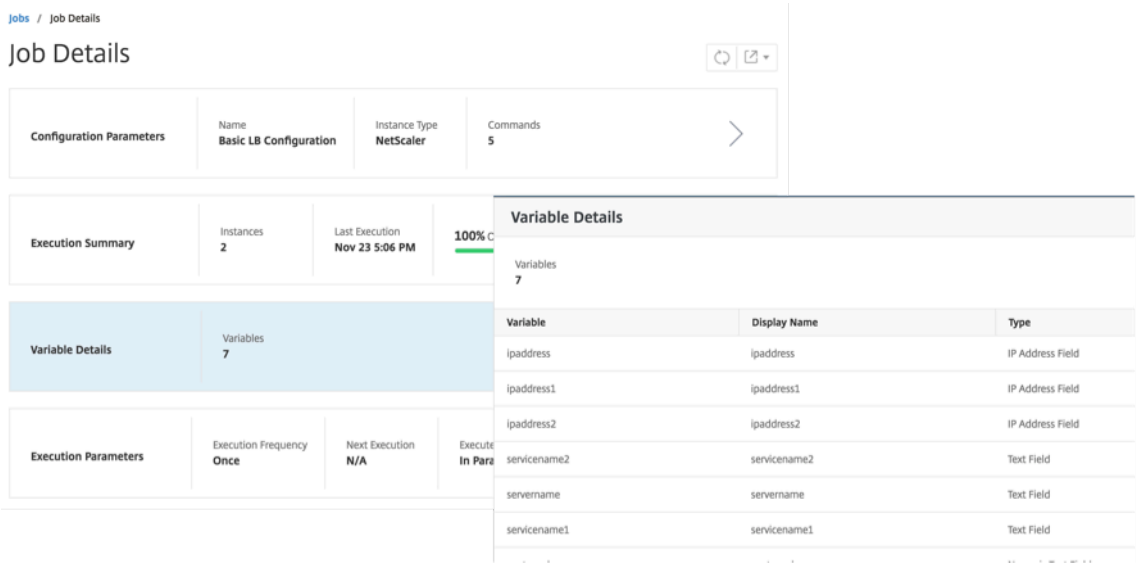
    要在编辑配置作业时查看已运行的配置作业，请导航到网络 **>** 配置作业，选择作业名称，然后单击编辑。在 配置作业页面的 指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

16. 在“作 业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

17. 在 “ 执行” 选项卡中，您可以选择立即运行作业，也可以将其安排在以后运行。您还可以选择如果命令失败以及如果要发送有关作业成功或失败的电子邮件通知以及其他详细信息，Citrix ADM 必须采取的操作。



配置并运行作业后，您可以通过导航到 “ 网络” > “配置 作业” 并选择刚刚配置的作业来查看作业详细信息。单击 详细信息，然后单击 变量详细信息以查看添加到作业的变量列表。



> 注意
>
> 当您保存作业并退出时，或者安排作业在稍后时间点运行时，Citrix ADM 将保留为 STE **P 5** 中的变量提供的值。

通过更正命令创建配置作业

April 23, 2021

您可以使用 Citrix Application Delivery Management (ADM) 中的审核模板功能监视托管 Citrix ADC 实例中的配置更改，并对配置错误进行故障排除。

使用审核模板来审核配置更改的典型工作流包括以下步骤

1. 使用一组有效/预期的 Citrix ADC 命令创建审核模板，用于审核实例配置。
2. 选择要运行审核模板的 Citrix ADC 实例，以检查正在运行的配置和预期的配置之间是否存在差异。
3. 了解差别/更正命令，并利用 “Create Job”（创建作业）功能使实例的配置进入期望状态

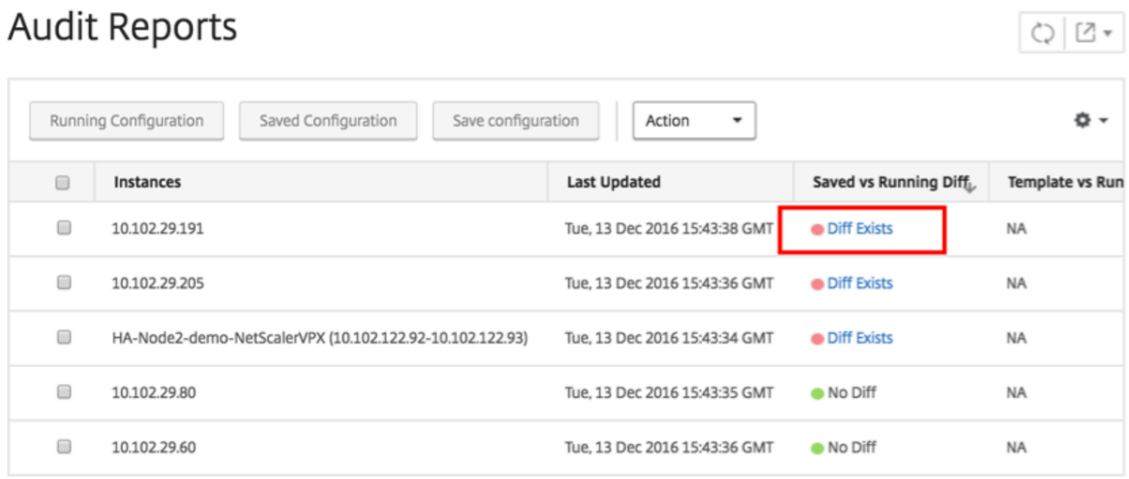
考虑一种情况，即多个管理员正在管理五个 Citrix ADC 实例。所有这些管理员在需要任何更改时更新现有实例配置。超级管理员想要确保，无论其他管理员做了什么更改，一组特定的重要配置保持不变。对于此使用案例，超级管理员将创建一个预期在 Citrix ADC 实例上存在的配置模板，并针对这些实例运行该模板。Citrix ADM 将审核模板配置与正在运行的配置进行比较，并在配置 审核控制板上报告任何不匹配情况。

如果您注意到某些实例的配置发生了更改，则可以使用 Citrix ADM 纠正命令功能创建配置作业，其中包含针对特定 Citrix ADC 实例的修改和更正配置命令。

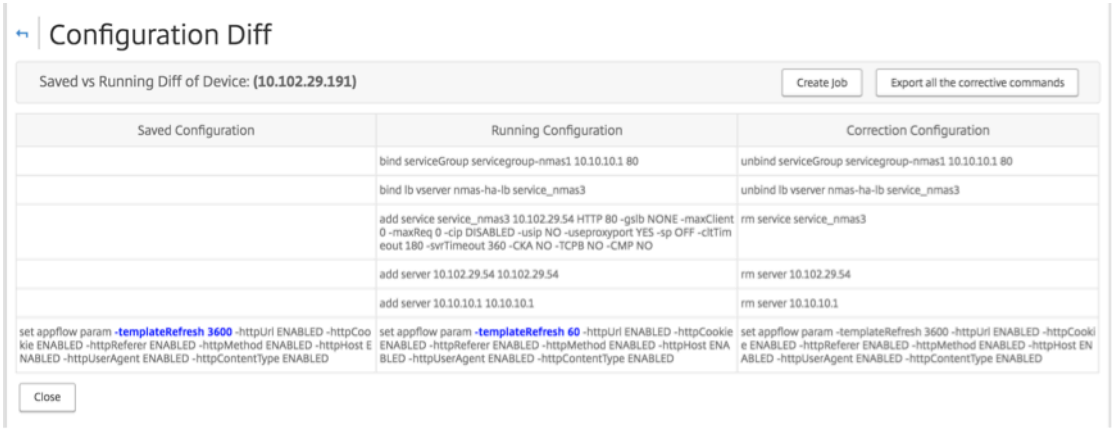
如果审核模板配置和正在运行的配置之间存在任何差异，则 审核报告页面上将显示 “差异 存在状态消息。单击 差异退出链接将转到 配置差异页面，您可以在其中查看纠正命令。您还可以使用这些纠正命令创建配置作业，然后在特定 Citrix ADC 实例上运行该作业，以使它们恢复到所需的配置。

使用 **Citrix ADM** 上的更正命令创建配置作业

1. 导航至 “ 网络” > “ 配置审核”。
2. 在 配置审核页面上，单击两个圆环图中的任意一个以访问 审核报告页面。
3. 单击要更正配置命令的实例的 “ 比较存在” 链接（在表中的 “已保存与正在运行的比较” 列下）。此时将显示 配置差异页面，其中列出了该实例的 “已保存配置”、“正在运行的配置” 和 “更正配置” 之间的差异。



4. 单击 创建作业以转到 创建作业页面，在该页面上预先填充了纠正命令。有关如何创建配置作业的说明，请参阅 如何在 Citrix ADM 上创建配置作业。



将运行和保存的配置从一个 **Citrix ADC** 实例复制到另一个实例

April 23, 2021

May 24, 2018

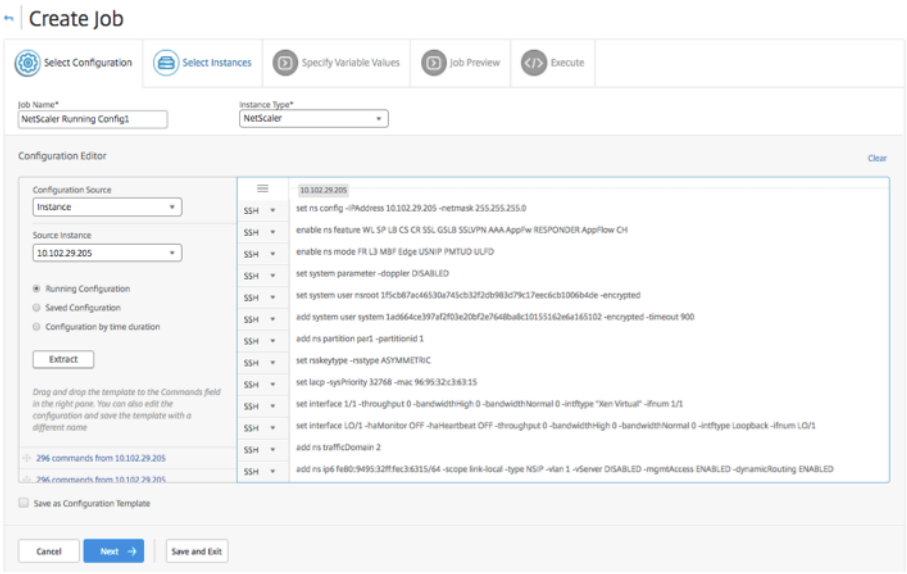
现在，您可以在其他实例上复制 Citrix ADC 实例的配置。在 Citrix ADM 中配置作业时，请选择一个实例作为配置源，然后选择所选实例的正在运行或保存的配置。

例如，当您选择 “正在 运行的配置并单击 提取时，Citrix ADM 会向选定的 Citrix ADC 实例发送请求以查找正在运行的配置，并将其显示为模板。您可以将模板拖到右侧窗格的命令字段中。您可以修改命令、参数和实例。

要将一个实例的运行和保存的配置命令复制到 **Citrix ADM** 上的另一个实例，请执行以下操作：

1. 导航到 “ 网络” > “ 配置作业”，然后单击 “ 创建作业”。
2. 指定作业名称和实例类型。例如，将 *Citrix ADC* 运行配置 *1* 指定为作业的名称，将实例类型指定为 *Citrix ADC*。

3. 选择 实例作为 配置源，选择要在其他实例上复制其配置的源实例。
4. 你会看到以下三个选项：
   - Running Configuration（正在运行的配置）
   - Saved Configuration（保存的配置）
   - Configuration by time duration（按持续时间的配置）
5. 选择 “ 运行配置”，然后单击 “ 提取”。将显示在该实例上运行的正在运行的配置命令的数量。



6. 拖动右侧窗格的 命令字段中的命令。
7. 您可以在 “Commands”（命令）字段中编辑命令。例如，如果提取的命令要设置 Citrix ADC 实例。这可能包括添加分区、设置负载平衡、将负载平衡服务器绑定到服务等。您可能需要编辑命令，以设置没有分区的新 Citrix ADC 实例。因此，要删除分区，请手动删除与创建分区相关的命令，然后单击 “ 下一步”。
8. 单击 添加实例”，然后添加要应用正在运行的配置命令的实例。单击 确定，然后单击 下一步。
9. 如果在命令中指定了变量，请在 指定变量值选项卡上单击 下载输入密钥文件。在下载的文件中，为变量指定值，然后将文件上载到 Citrix ADM。
10. 在 “作 业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。

11. 在 “ 执行” 选项卡中，您可以选择立即运行作业，也可以将其安排在以后运行。您还可以选择 Citrix ADM 必须采取的操作，命令失败，以及是否要发送有关作业成功或失败的电子邮件通知以及其他详细信息。

重用运行配置作业

April 23, 2021

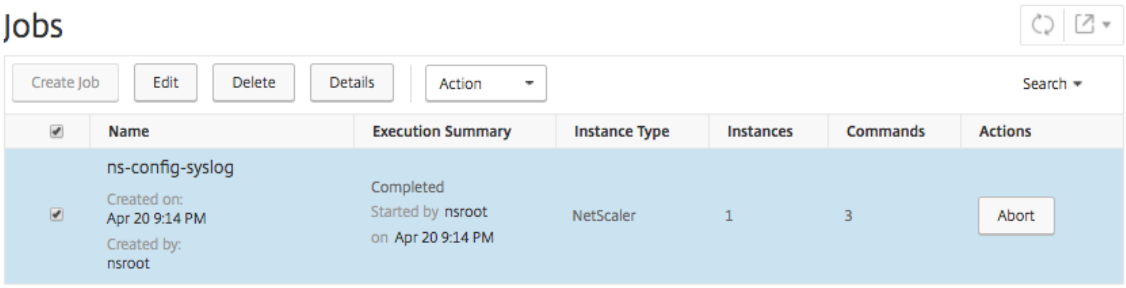
配置作业允许您创建一组配置命令，您可以在一个或多个托管实例上运行。还可以在修改作业中的命令、参数、配置来源及实例后，运行同一组保存的配置作业。当必须在不同的实例上运行相同的命令集或作业遇到错误并停止进一步执行时，这很有用。

Citrix Application Delivery Management (ADM) 提供了再次运行已完成的作业的功能。使用此功能，完全运行的作业可以在不更改作业名称的情况下再次运行。

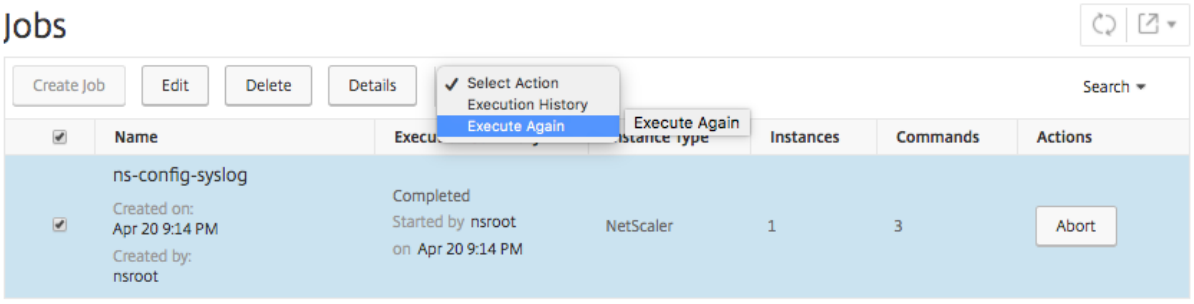
> 注意：您只能重新执行在执行模式为“现在”时运行的那些作业。

要编辑已完成的作业，请执行以下操作：

1. 在 Citrix ADM 主页中，导航到 网络 **>** 配置作业。
2. 在“作 业页面中，选择显示“执行摘要”为“已完成”的作业，然后单击 编辑。还可以编辑计划的配置作业。
3. 在 **Configure Job**（配置作业）页面上，可以看到“Job Name”（作业名称）和“Instance type”（实例类型）都是不可编辑。可以修改其他字段（例如，配置来源）、添加实例、编辑变量值以及设置执行设置。
4. 单击 完成再次运行配置作业。



> 注意
>
> 您还可以选择作业，然后再次单击 执行以运行作业，而不修改任何源、实例和命令。当您必须在相同的实例上运行同一组命令时，这很有用。有时，作业可能会遇到来自服务器端的暂时错误，并且您可能需要再次运行作业。



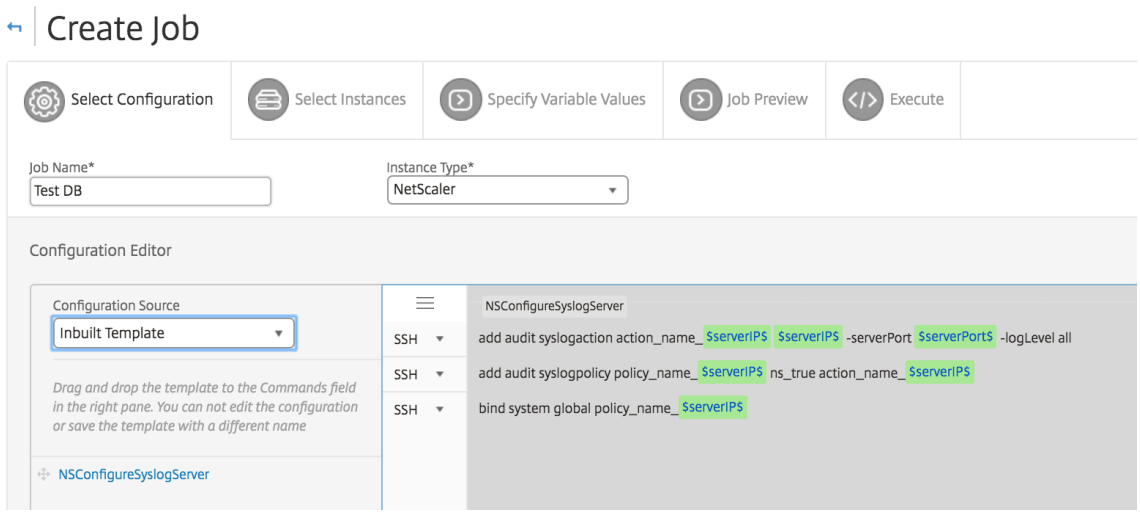
安排使用内置模板创建的作业

April 23, 2021

可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，使用内置模板选项调度作业以配置 syslog 服务器。您还可以选择立即运行作业，或者安排在稍后阶段运行作业。

使用 **Citrix Application Delivery Management (ADM)** 中的内置模板来安排作业

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业”，然后单击 “ 创建作业”。
2. 在 创建作业页上的 选择配置选项卡上，指定 作业名称并从下拉列表中选择 实例类型。
3. 从 配置源下拉列表中选择内置模板。将 ***NSConfigureSyslogServer** 命令拖到右窗格中，然后单击 下一步。

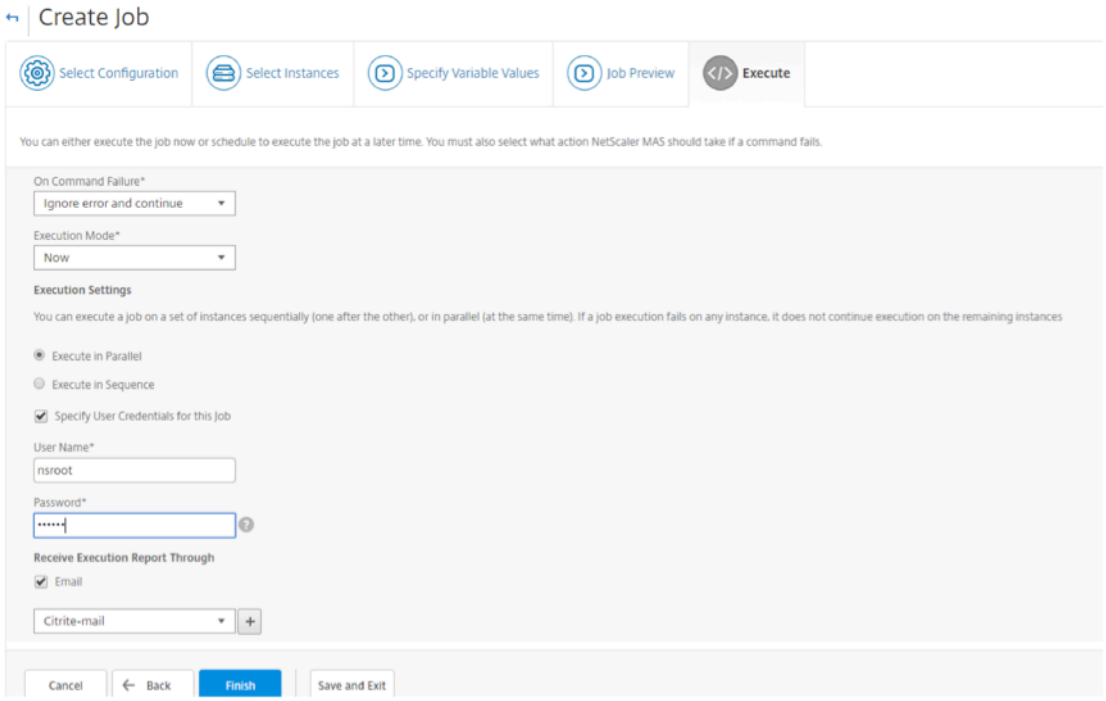


4. 在 选择实例选项卡上，单击 添加实例”，选择要在其上运行作业的实例，然后单 击“确定”。
5. 单击下一步。在 **Specify Variable Values**（指定变量值）选项卡中，选择以下选项之一来为您的实例指定变量：
   - 输入文件中的变量值 -下载输入文件以输入您在命令中定义的变量的值。然后，将文件上载到 Citrix ADM 服务器。
   - **Common variable values for all instances**（用于所有实例的公用变量值）- 指定 syslog 服务器 IP 地址和端口。
6. 在“作 业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
7. 单击下一步。
8. 在 执行” 选项卡上，设置以下条件：
   - 命令失败时- 如果命令失败，则可以选择忽略错误并继续运行作业或停止进一步执行作业。从下拉列表中选择要运行的操作。
   - 执行模式 -您可以立即运行作业，也可以安排稍后运行作业。如果要稍后安排作业，则必须指定该作业的执行频率设置。从下拉列表中选择希望作业遵从的计划。

9. 您还可以通过在执行设置下选择所需的方法，按顺序或并行在一组实例上运行作业。如果在任一实例上作业执行失败，它不会继续在其余实例上运行。

   您可以选择允许授权用户在托管实例上运行作业。还可以发送关于作业成功或失败的电子邮件通知以及其他详细信息。

10. 单击完成。



使用维护作业升级 **Citrix ADC SDX** 实例

April 23, 2021

您可以对运行 Citrix ADC 11.0 版及更高版本的 Citrix ADC SDX 实例执行单捆绑升级。要执行单捆绑升级，请使用 Citrix ADM 中的内置任务。使用此内置任务，您可以升级 Citrix ADC SDX 管理服务、Citrix Hypervisor 以及 Citrix Hypervisor 的补充包和修补程序。

要使用 **Citrix ADM** 升级 **Citrix ADC SDX** 实例，请执行以下操作：

1. 导航到 网络 **>** 配置作业 **>** 维护作业。
2. 单击 创建作业。在 创建作业页面中，选择 升级 **Citrix ADC SDX** 内置任务以升级 Citrix ADC SDX 实例。单击继续。
3. 在升级 **Citrix ADC** 设备页面的实例选择选项卡中，指定作业名称，然后单击添加实例。
4. 选择要升级的目标实例或实例组。

5. 添加 Citrix ADC 实例或实例组后，单击下一步以启动所选实例的升级前验证。屏幕将报告每个 Citrix ADC 实例的预验证进度。
6. 在修改升级 **Citrix ADC** 设备页面上，选择升级选项卡。从 **“软件映像”** 下拉菜单中，选择 **“本地计算机”** 或 **“设备”**（构建文件必须存在于 **Citrix ADM** 上）。
7. 您还可以查看是否有任何实例存在验证前升级错误。这些错误以消息形式显示。这些消息显示与磁盘空间、硬盘驱动器和用户自定义项相关的错误。如果您不想继续处理预验证升级检查失败的实例，可以删除这些实例。要删除实例，请选择实例，然后单击删除。
8. 在“计划任务”选项卡上，您还可以设置执行详细信息，您可以立即执行升级过程或计划在以后的日期执行升级过程。您还可以选择备份 Citrix ADC SDX 实例、通过电子邮件接收执行报告或对 HA 中的节点执行两阶段升级。

HA 中节点的两阶段升级使您可以选择立即执行升级，也可以安排一个接一个更新节点的时间。在两个节点成功升级之前，禁用节点的同步和传播。

为 **Citrix SD-WAN WANOP** 实例创建配置作业

April 23, 2021

作业是可以在一个或多个托管实例上创建并计划的一组配置命令。对于 Citrix SD-WAN WANOP 实例，可以使用以下选项创建作业：

- 配置模板：您可以使用配置编辑器键入 CLI 命令，将配置另存为模板，然后使用它配置作业。
- 内置模板：您可以从配置模板列表中进行选择。这些模板提供了 CLI 命令的语法，并允许您为变量指定值。下表中列出了内置模板及其说明。
- 文件：您可以从本地计算机上载配置文件并创建作业。

创建作业后，您可以选择立即运行作业或计划稍后运行作业。还可以设置执行频率

内置模板	说明
EnableCloudBridgeWANOpt	启用通过 Citrix SD-WAN 设备的流量。
DisableCloudBridgeWANOpt	禁用通过 Citrix SD-WAN 设备的流量。
RestartCloudBridgeWANOpt	重新启动 Citrix SD-WAN WANOP 设备。
RestoreConfig	还原 Citrix SD-WAN WANOP 设备的配置。
AddLink	通过创建或定义链接，SD-WAN WANOP 设备可以防止链接上的拥塞和丢失，并执行流量调整。可以定义通过链接发送或接收的最大带宽，还可以指定是 LAN 端流量还是 WAN 端流量。
ConfigureBandwidth	设置带宽限制和其他带宽管理设置。

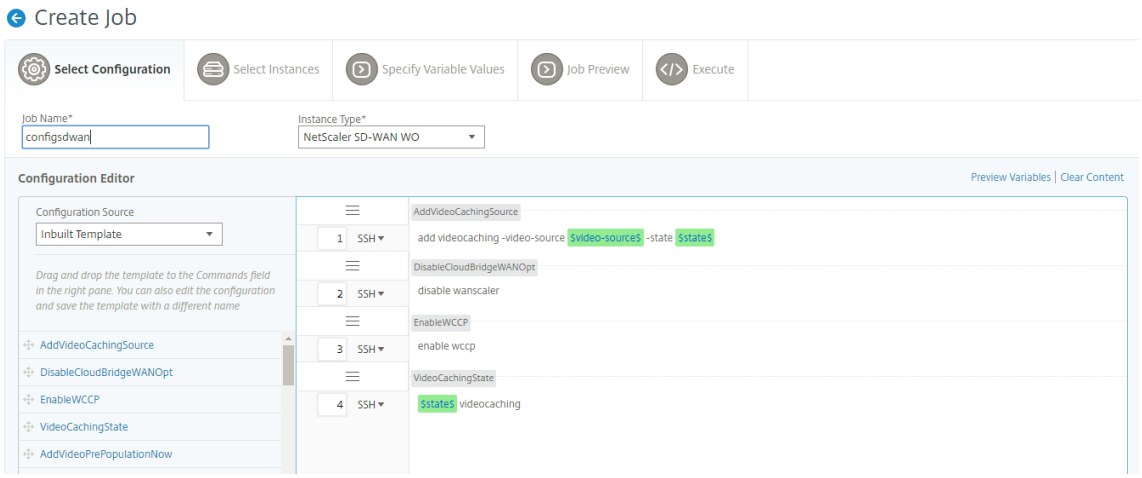
内置模板	说明
AddUser	添加新用户，可以为其分配权限。
AddUserAdvancedPlatform	添加新用户使您能够分配 AddUser 模板中不可用的权限。
AddService-class	使用一个或多个服务类筛选器为 Citrix SD-WAN WANOP 设备创建服务类并将其启用。
SetApplication	设置应用程序分类器定义。
AddorRemoveVideoCachingPorts	添加或删除视频源可以用于发送或接收数据的端口号。默认端口为 80。
RemoveVideoCachingSource	删除一个或多个视频缓存源。指定视频源 IP 地址或域名。
RemoveAllVideoCaching	删除所有可用视频缓存源。
VideoCachingState	启用或禁用 Citrix SD-WAN WANOP 设备上的视频缓存功能。
ClearVideoCaching	清除视频缓存或视频缓存统计信息。
SetVideoCaching	设置缓存对象的最大大小。超过此限制的对象不会缓存。默认情况下，最大缓存对象大小为 100 MB。
AddVideoCachingSource	添加视频源的 IP 地址或域名。包括用于为该源启用或禁用视频缓存的选项。
ConfigureRemoteLicenseServer	配置集中式许可证服务器。指定许可证服务器型号、IP 地址和端口号。
ConfigureLocalLicenseServer	将许可证服务器位置设为本地。
InstallCACert	在 Citrix SD-WAN WANOP 设备上安装 CA 证书。指定证书名称、文件名和密钥库密码。
InstallCombinedCerKey	安装组合的 SSL 证书-密钥对文件。
InstallSeperateCertKey	将 SSL 证书和密钥作为单独的文件进行安装。
EnableWCCP	启用 WCCP 部署模式。
AddWCCPServiceGroup	为 Citrix SD-WAN WANOP 设备添加新的 WCCP 服务组定义。
DisableWCCP	禁用 WCCP 部署模式。
AddTrafficShapingPolicy	为 Citrix SD-WAN 装置创建流量调整策略。该策略控制网络带宽。

内置模板	说明
SetTrafficShapingPolicy	修改 Citrix SD-WAN 设备的流量调整策略。该策略控制网络带宽。
AddVideoPrePopulation	创建视频预填充条目，让您可以提前下载和缓存视频。还可以指定何时缓存视频。
UpdateVideoPrePopulation	修改视频预填充条目，该条目指定何时缓存视频。
AddVideoPrePopulationNow	配置视频预填充，让您可以立即下载和缓存视频。您可以控制从 URL 下载和缓存视频的方式。
VideoPrePopulationState	更改、开始、更新或删除视频预填充。
ConfigureSyslogServer	设置 syslog 服务器的 IP 地址和端口号。
ConfigureAlert	配置警报级别。

要为 **Citrix SD-WAN WANOP** 实例创建配置作业，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业”，然后单击 “ 创建作业”。
2. 在 创建作业页上的 选择配置选项卡下，指定 作业名称。
3. 在实例类型字段中，选择 **Citrix SD-WAN WO** 。
4. 在 “ 配置源” 下拉列表中，选择创建作业的选项。

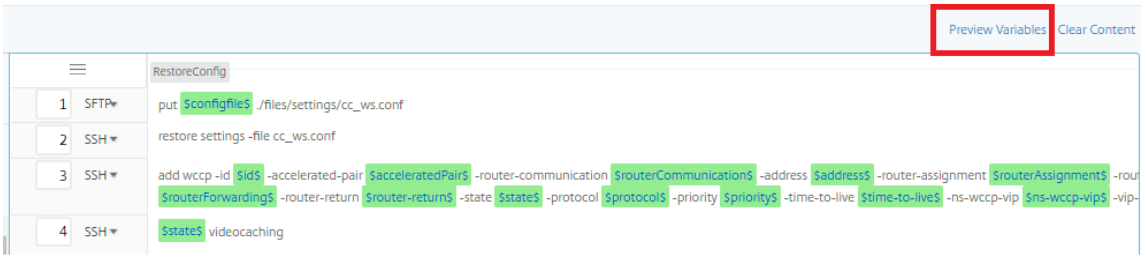
   > 注意
   >
   > 选择 另存为配置模板”，然后指定一个名称以将配置另存为模板并重复使用。



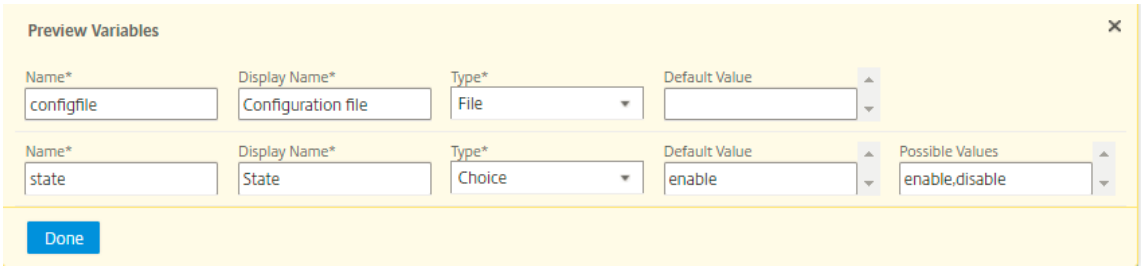
5. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
6. 执行以下操作之一以查看单个统一视图中的所有变量：

- 创建配置作业时，导航到 **“网络” > “配置作业”**，选择 “ 创建作业”。在 创建作业页面上，您可以查看创建配置作业时添加的所有变量。
- 编辑配置作业时，导航到 **“网络” > “配置作业”**，选择 “作业名称”，然后单击 “ 编辑”。在 配置作业页面上，您可以查看创建配置作业时添加的所有变量。

7. 然后，您可以单击预览变量选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。

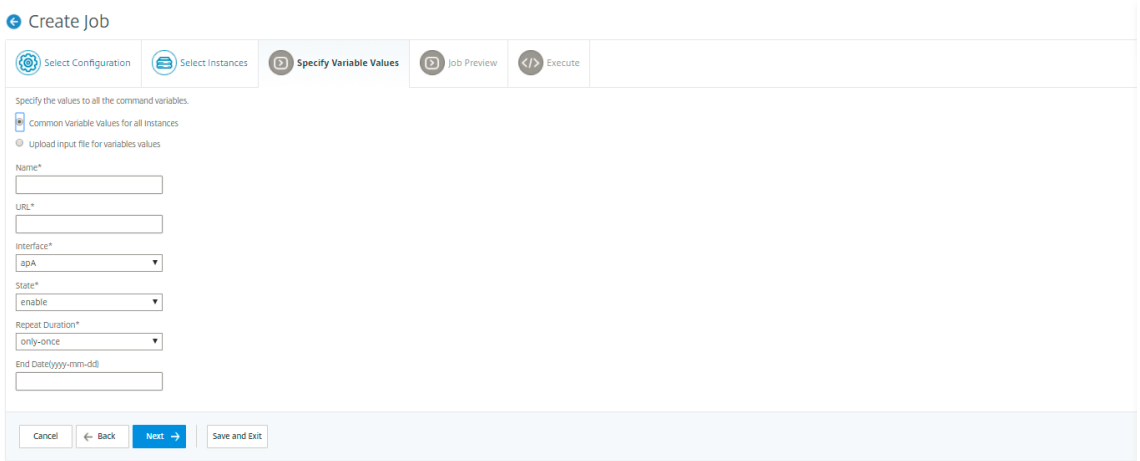


8. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完成” 按钮。



9. 单击下一步，然后在选择实例选项卡上，单击添加实例。选择要在其上运行作业的实例，然后单击 “确定”**。
10. 单击下一步，然后在指定变量值选项卡上，选择以下选项之一以指定实例的变量：

- 上传变量值的输入文件：单击下载输入密钥文件下载输入文件。在输入文件中，输入已在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
- 所有实例的公用变量值：输入变量值。变量因选定的模板而不同。

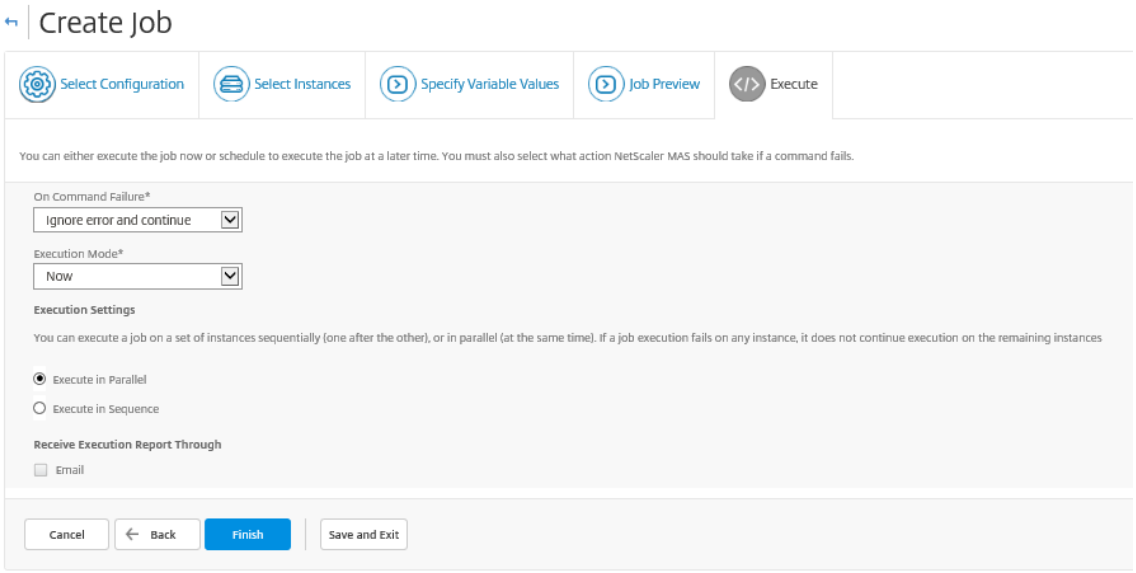


包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上传的这些输入文件。

要在创建配置作业时查看运行配置作业，请导航到 “ 网络**” > “**配置作业”，然后单击 “ 创建作业”。在 “创建作业” 页中。在指定变量值选项卡上，选择所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

要在编辑配置作业时查看已运行的配置作业，请导航到 网络 **>** 配置作业，选择作业名称，然后单击编 辑。在配置作业页面的指定变量值选项卡上，选择所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）

11. 单击 下一步，在 作业预览选项卡上，您可以评估和验证要作为作业运行的命令。
12. 单击 “下 一步”，在 执行” 选项卡上，设置以下条件：
    - 命令失败：如果命令失败，该怎么办：忽略错误并继续执行作业，或停止进一步执行作业。从下拉列表中选择操作。
    - 执行模式：立即运行作业，或安排稍后执行。如果计划以后执行，必须为作业指定执行频率设置。从 执行频率下拉列表中选择您希望作业遵循的计划。



13. 在 执行设置下，选择按顺序运行作业（一个接一个）或并行（同时）运行作业。
14. 要将作业执行报告通过电子邮件发送到收件人列表，请选中 “ 接收执行报告通过” 部分中的 “ 电子邮件” 复选框。从显示的下拉列表中选择电子邮件通讯组列表。要创建电子邮件通讯组列表，请单击 **+** 图标并输入收件人的电子邮件地址和电子邮件服务器详细信息。
15. 单击完成。

使用主配置模板

April 23, 2021

使用主配置模板是在多个 Citrix ADC 实例上创建和部署主配置的灵活选项。

作为管理员，您可能需要更改配置并将许可证、证书和其他文件保存在 ADC 实例上。您可以将新配置保存为主配置模板（.conf 文件）。

要从 ADC 实例保存主配置模板，您可以执行以下操作之一：

- 在命令提示符处，输入 **save ns** 配置。配置将保存在实例的闪存中的 /nsconfig/ns.conf 文件中。
- 从实例的 GUI 中，导航到 “ 诊断” > “ 查看配置”。选择您要保存的配置种类。例如，如果要保存实例的保存配置，请选择 已保存的配置 n。单击 “ 将文本保存到文件” 链接将 “ns.conf” 文件保存到本地计算机上。

当您在创建作业时使用 “DeploMasterConfiguration” 配置模板部署主配置模板时，可以通过添加更多命令、修改现有命令以及在输入文件中提供不同的变量值，为每个特定 ADC 实例进一步自定义该模板。

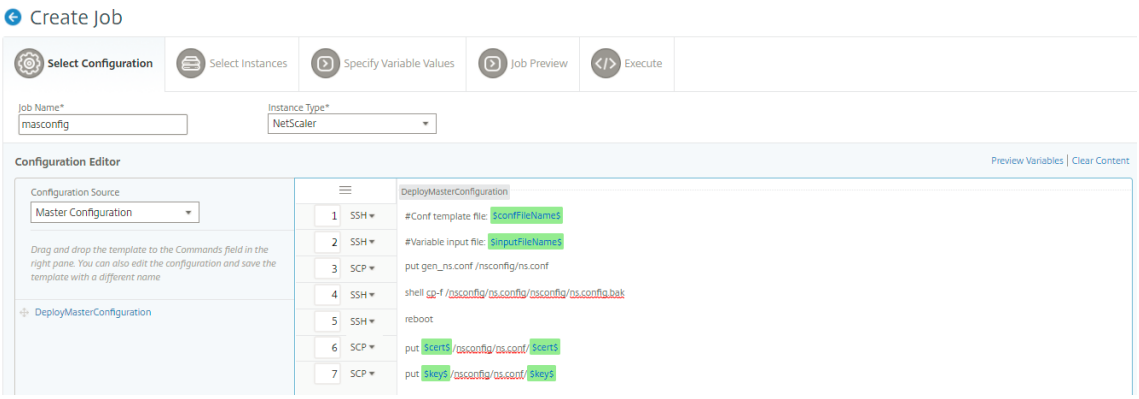
例如，作为管理员，您可能希望除 ns.conf 文件外将证书密钥上传到 ADC 实例，并在这些实例上部署主配置。

> 重要
>
> 您无法在 Citrix ADC CPX 实例、集群中配置的实例或分区 ADC 实例上使用 DeployMasterConfiguration 模板运行配置作业。

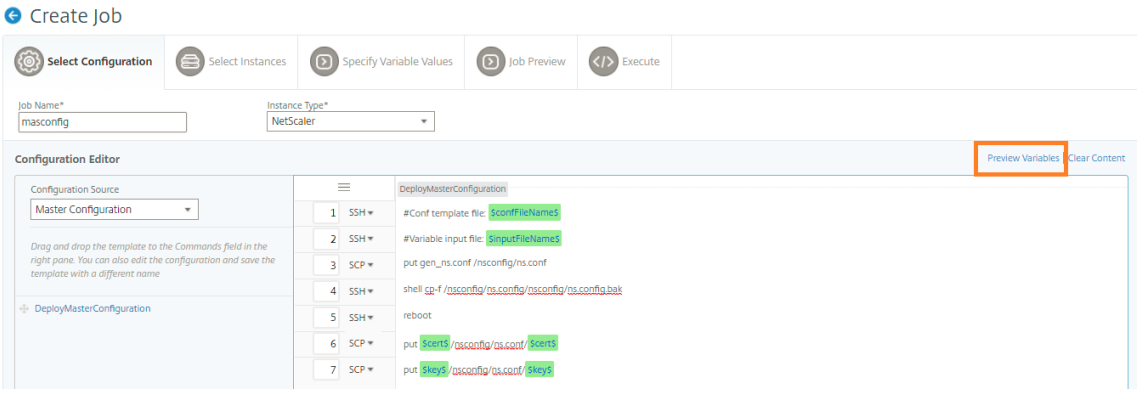
要使用 **Citrix ADM** 上的主配置配置模板创建配置作业，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “网络” > “ 配置作业”，然后单击 “创建作业”。
2. 在 创建作业页上的 选择配置选项卡上，指定 作业名称并从下拉列表中选择 实例类型。
3. 从 配置源下拉列表中选择主配置。将 DeployMasterConfiguration 模板的命令拖动到右侧窗格中。您也可以在右侧窗格中添加、修改或删除命令。单击 “下一步”。

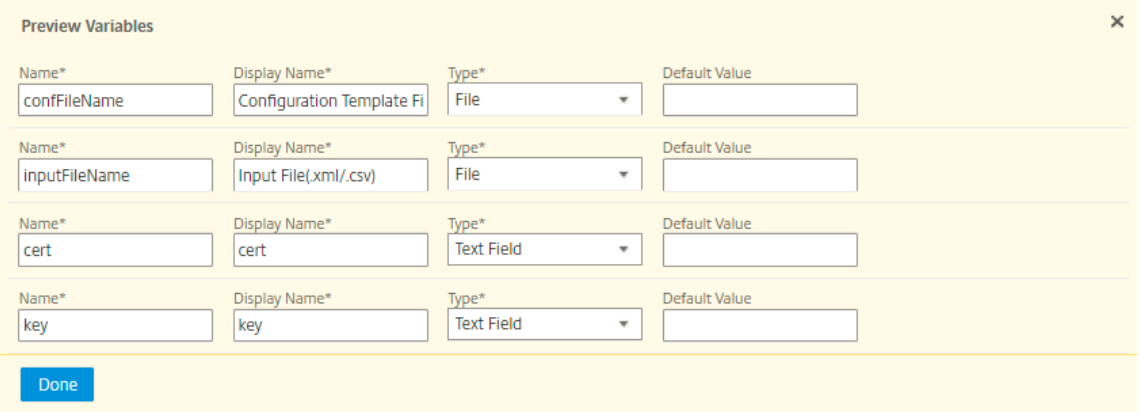
   > 注意
   >
   > 您可以添加 ***put*** 命令以将输入文件添加到模板中。在我们的示例中，除了配置模板文件和变量输入文件之外，我们还必须上传证书和密钥文件。



4. 您可以在单个合并视图中查看在创建或编辑配置作业时定义的所有变量。
5. 执行以下操作之一以查看单个统一视图中的所有变量：
   - 创建配置作业时，导航到 **“网络” > “配置作业”**，选择 “ 创建作业”。在 创建作业页面上，您可以查看创建配置作业时添加的所有变量。
   - 编辑配置作业时，导航到 **“网络” > “配置作业”**，选择 “作业名称”，然后单击 “ 编辑”。在 配置作业页面上，您可以查看创建配置作业时添加的所有变量。
6. 然后，您可以单击预览变量选项卡，在创建或编辑配置作业时定义的单个合并视图中预览变量。



7. 将出现一个新的弹出窗口，并以表格格式显示变量的所有参数，如名称、显示名称、类型和默认值。您还可以编辑和修改这些参数。在编辑或修改任何参数后，单击 完成” 按钮。



8. 选择要在其上运行配置作业的实例，然后单击 下一步”。
9. 在 指定变量值选项卡上，上传以下内容：
   - 配置模板文件 **(.conf)** -上载从 ADC 实例中提取的.conf 文件。
   - 上传输入文件 **(.xml/csv)** -使用您在命令中定义的变量值上传输入文件。

   此处提供了一个示例 xml 文件供您使用。确保 xml 文件包含与您正在使用的 ADC 实例相对应的详细信息。

```
1 <?xml version="1.0" encoding="UTF-8" ?>
2
```

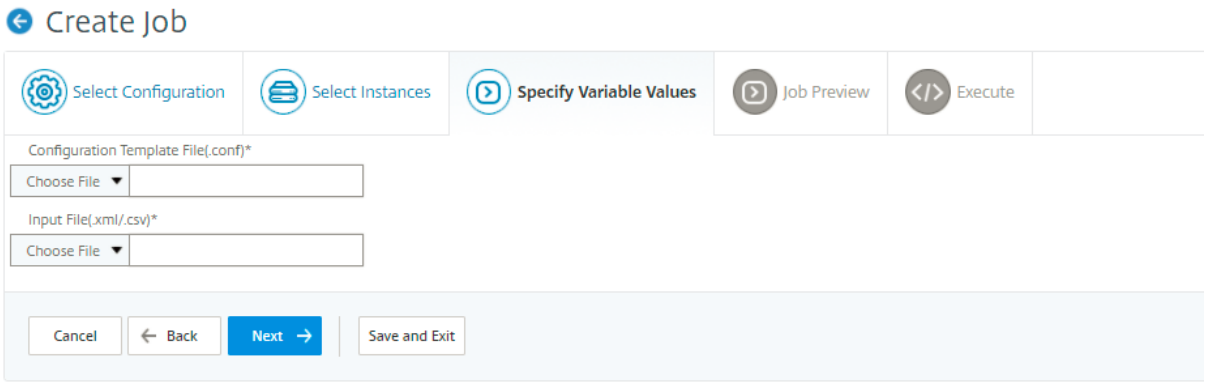


```
<properties>

<!--

Provide inputs for all the parameters defined in the master config
    file.

-  global. This tag contains all the common parameters and value.

-  devicegroup. This tag contains all the instance group specific
   parameters and values.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence
   over the instance group. The instance group specific parameters
    value will take precedence over global parameters in the
   execution.

-  name. This attribute represents the name of the instance group.

-  device. This tag contains all the instance specific parameters
   and value.

If the same parameters are defined in global and instance tags,
   the instance specific parameters value will take precedence in
   the execution.

-  name. This attribute represents the IP Address of the instance.
    Host name is not supported for the attibute.

HA pair should be represented as <primaryip>-<secondaryip>.
   Example 10.102.2.1-10.102.2.2

In the template file, the parameter name must be specified within
   the dollar sign,Example: $NSIP$, $CC_Trap_Dest$ and parameters
   names are case sensitive.
-->

<global>

</global>
<devicegroup name="BLR_DEVS">
</devicegroup>
<device name="10.106.101.209">
<param name="IP" value="10.106.101.209"/>
```



```
</device>

<!-- HA PAIR-->
<!--<device name="10.102.43.154-10.102.43.155">
<param name="NSIP" value="10.102.43.154"/>
<param name="HostName" value="NS43HA"/>
<param name="LBSERVER" value="haserver43http"/>
<param name="SNMPTrapDest" value="10.102.43.130"/>
</device>-->
</properties>

<!--NeedCopy-->
```

10. 单击 **Next**（下一步）。

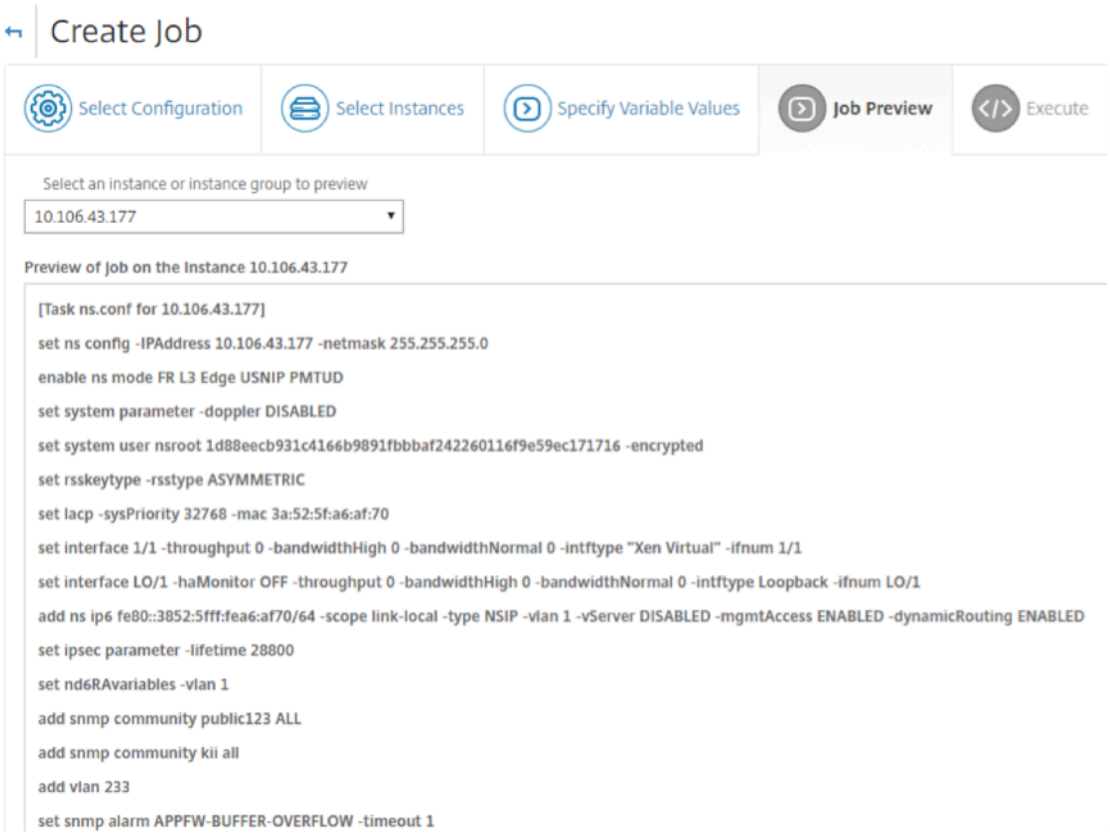


包含变量值的输入文件将保留在配置作业中（具有相同的文件名）。您可以查看和编辑创建或编辑配置作业时先前使用和上传的这些输入文件。

要在创建配置作业时查看运行配置作业，请导航到网络 **>** 配置作业，然后单击创建作业。在 创建任务页面中。在 指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

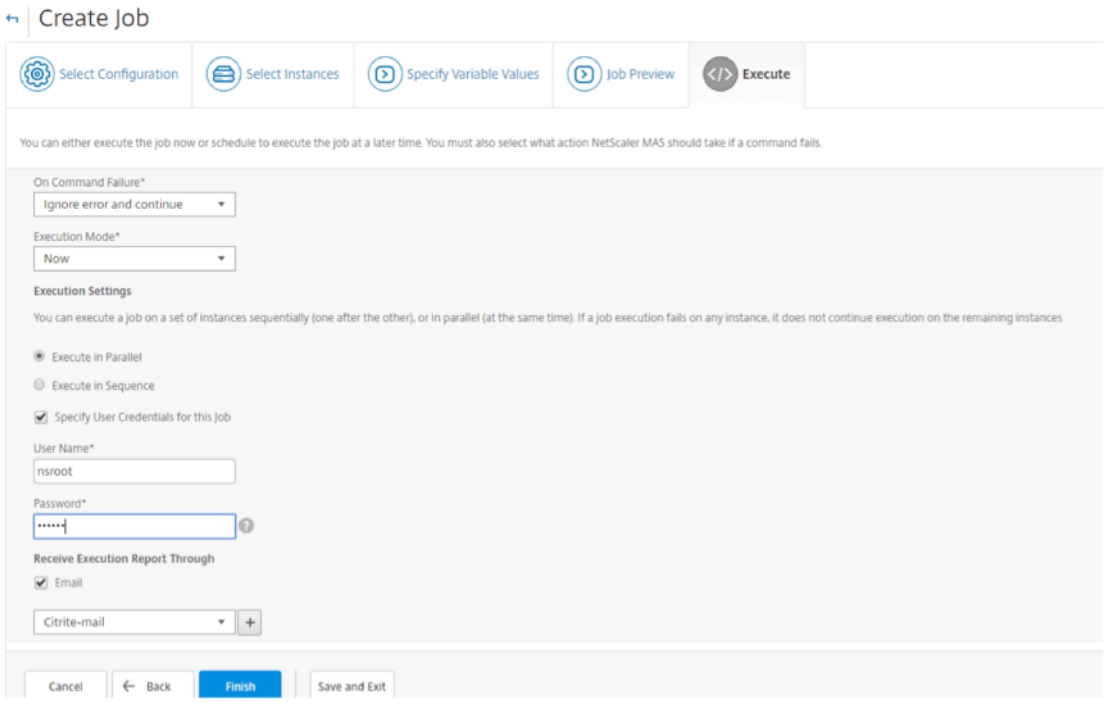
要在编辑配置作业时查看已运行的配置作业，请导航到网络 **>** 配置作业，选择作业名称，然后单击编辑。在 配置作业页面的 指定变量值选项卡上，选择 所有实例的公用变量值选项以查看上传的文件。要编辑输入文件，请下载输入文件，然后编辑和上传文件（保持相同的文件名）。

1. 在“作 业预览选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令，然后单击 下一步。

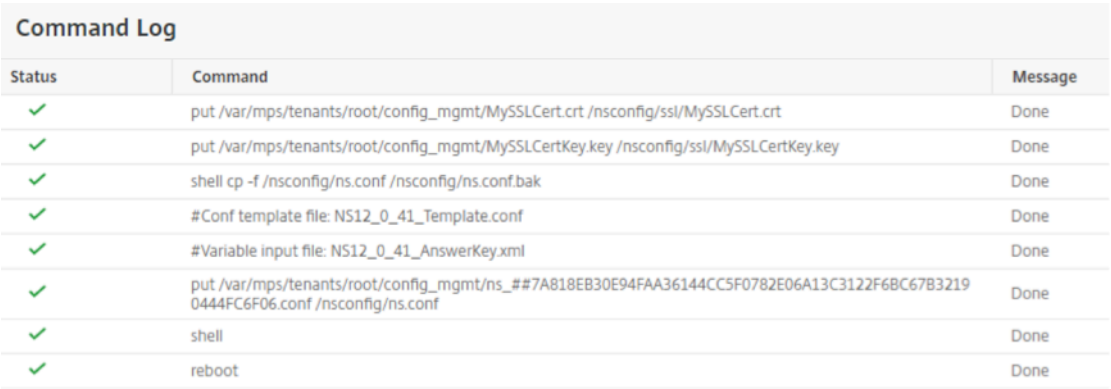


2. 在“执行”选项卡上，您可以选择立即运行作业或计划稍后运行作业。您还可以选择如果命令失败，Citrix ADM 必须采取的操作。

   您还可以选择允许授权用户在托管实例上运行作业，也可以选择是否发送有关作业成功还是失败的电子邮件通知以及其他详细信息。



运行作业后，您可以通过导航到网络 > 配置作业并选择配置的作业来查看作业详细信息。单击详细信息，然后单击执行摘要以查看作业的详细信息。单击实例可查看命令日志以查看在作业上运行的命令。



Command Log

Status	Command	Message
✓	put /var/mps/tenants/root/config_mgmt/MySSLCert.crt /nsconfig/ssl/MySSLCert.crt	Done
✓	put /var/mps/tenants/root/config_mgmt/MySSLCertKey.key /nsconfig/ssl/MySSLCertKey.key	Done
✓	shell cp -f /nsconfig/ns.conf /nsconfig/ns.conf.bak	Done
✓	#Conf template file: NS12_0_41_Template.conf	Done
✓	#Variable input file: NS12_0_41_AnswerKey.xml	Done
✓	put /var/mps/tenants/root/config_mgmt/ns_##7A818EB30E94FAA36144CC5F0782E06A13C3122F6BC67B32190444FC6F06.conf /nsconfig/ns.conf	Done
✓	shell	Done
✓	reboot	Done

使用作业升级 **Citrix ADC** 实例

April 23, 2021

您可以使用 Citrix Application Delivery Management (ADM) 升级一个或多个 Citrix ADC 实例。在升级实例之前，您必须了解许可证框架和许可证类型。

通过创建维护作业升级 Citrix ADC 实例时，请对要升级的实例执行预验证检查。

1. 检查自定义项 -备份您的自定义项并从实例中删除它们。您可以在实例升级后重新应用备份的自定义项。

2. 检查磁盘使用情况 -如果 /var 文件夹的空间小于 6 GB，且 /flash 文件夹的空间小于 200 MB，请清理磁盘空间。检查以下文件夹路径以清理磁盘空间：
   - /var/nstrace
   - /var/log
   - /var/nslog
   - /var/tmp/support
   - /var/core
   - /var/crash
   - /var/nsinstall
   - /var/netscaler/nsbackup
3. 检查磁盘硬件问题 -解决硬件问题（如果有）。

您可以分两个阶段升级 ADC HA 对：

1. 创建升级作业并立即在其中一个节点上运行，或稍后安排。
2. 安排稍后在其余节点上运行升级作业。确保在初始节点升级后安排此作业。

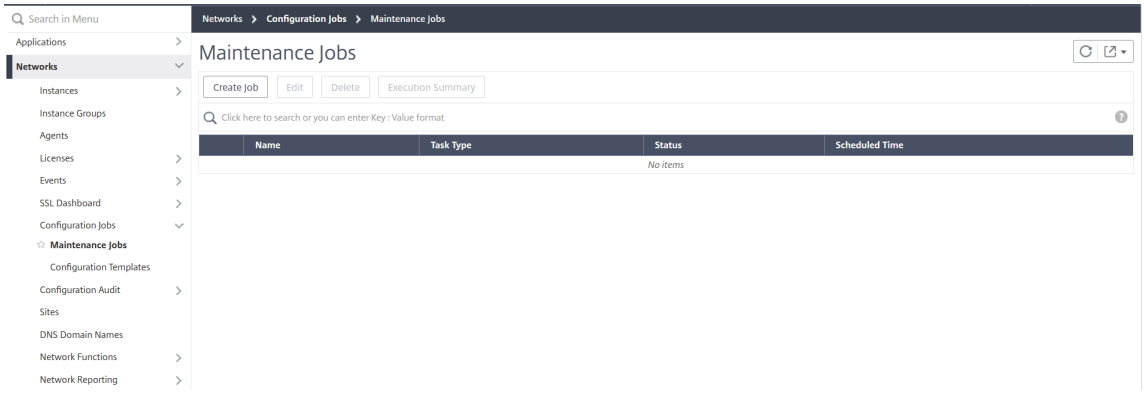
升级 ADC HA 对时，请注意以下事项：

- 首先升级辅助节点。
- 在两个节点成功升级之前，禁用节点的同步和传播。
- 成功升级 HA 对后，执行历史记录中会显示一条错误消息。如果 HA 对中的节点位于不同的版本或版本上，则会显示此消息。此消息表示禁用主节点和辅助节点之间的同步。

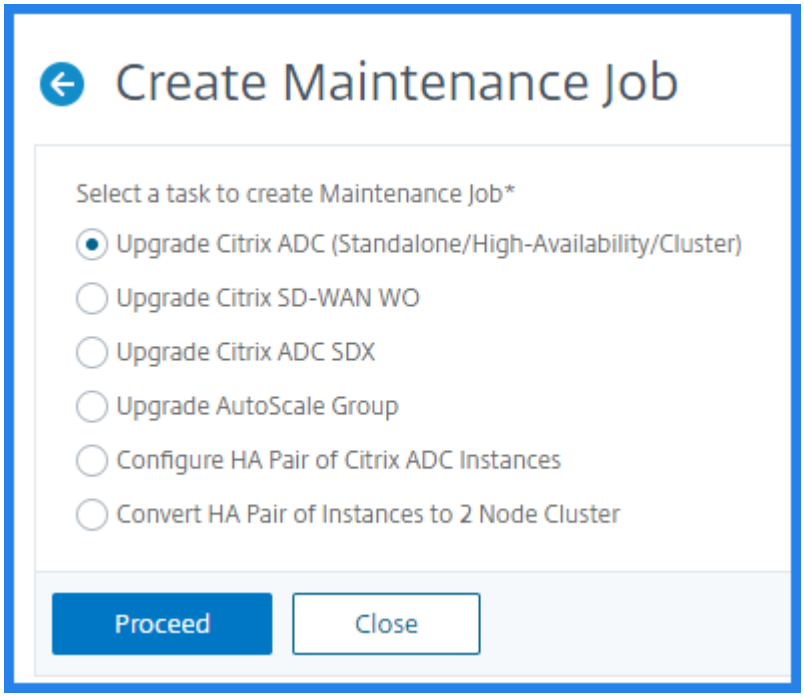
升级 ADC 群集时，ADM 仅对指定实例执行升级前验证。升级之前，请检查并解决群集节点上的自定义、磁盘使用情况和硬件问题。

创建升级维护作业以升级 **ADC** 实例

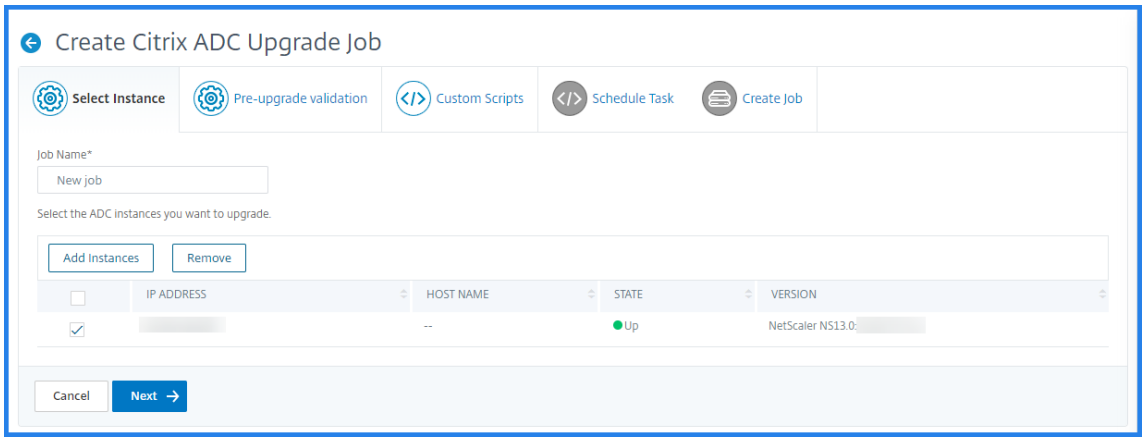
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业” > “ 维护作业”。单击 创建作业按钮。



2. 在 创建维护作业中，选择 升级 **Citrix ADC**（独立/高可用性/群集），然后单击 继续。



3. 在选 择实例中，键入您选择的 作业名称的名称。
4. 单击 添加实例以添加要升级的 ADC 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。
   - 要升级群集，请指定群集 IP 地址。



5. 单击 下一步开始对所选实例进行升级前验证。

   升级前验证选项卡显示失败的实例。您可以删除失败的实例，然后单击 下一步。

   如果实例上的磁盘空间不足，则可以检查并清理磁盘空间。请参阅清理 ADC 磁盘空间。

   > 重要信息：
   >
   > 如果指定群集 IP 地址，ADM 仅对指定实例而不在其他群集节点上执行升级前验证。

6. 可选，在 自定义脚本中，指定要在实例升级之前和之后运行的脚本。使用以下方法之一来运行命令：

   自定义脚本用于检查 ADC 实例升级之前和之后的更改。例如：

   - 升级前后的实例版本。
   - 升级前后接口、高可用性节点、虚拟服务器和服务的状态。
   - 虚拟服务器和服务的统计信息。
   - 动态路由。

   实例升级有多个阶段。现在，您可以指定这些脚本在以下阶段运行：

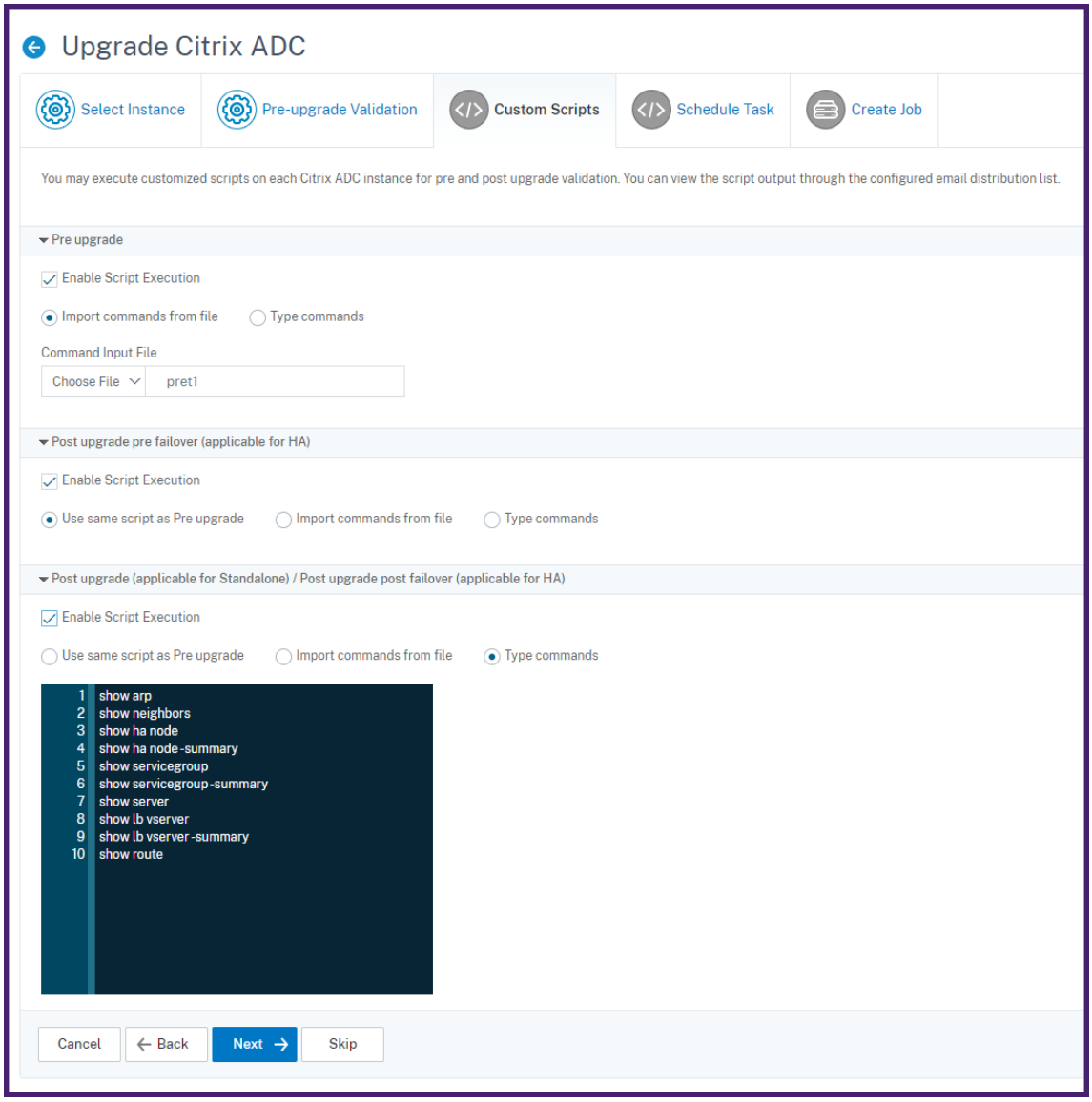
   - 升级前：指定的脚本在升级实例之前运行。
   - 升级后故障转移前（适用于 **HA**）：此阶段仅适用于高可用性部署。指定的脚本在升级节点之后但在其故障转移之前运行。
   - 升级后（适用于独立版）**/**故障转移后升级后（适用于 **HA**）：指定的脚本在独立部署中升级实例后运行。在高可用性部署中，脚本在升级节点及其故障切换后运行。

   > 注意：
   >
   > 确保在所需阶段启用脚本执行。否则，指定的脚本将不会运行。

   您可以直接在 ADM GUI 中导入脚本文件或键入命令。

   - 从文件导入命令：从本地计算机中选择命令输入文件。
   - 键入命令：直接在 GUI 上输入命令。

   在升级后阶段，您可以使用升级前阶段中指定的相同脚本。



7. 在 计划任务中，选择以下选项之一：

   - 立即升级 -升级作业将立即运行。
   - 稍后计划 -选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

     如果要分两个阶段升级 ADC HA 对，请选择对 **HA** 中的节点执行两阶段升级。

     如果要升级 HA 对中的另一个实例，请指定 执行日期和 开始时间。

8. 在 创建作业中，指定以下详细信息：

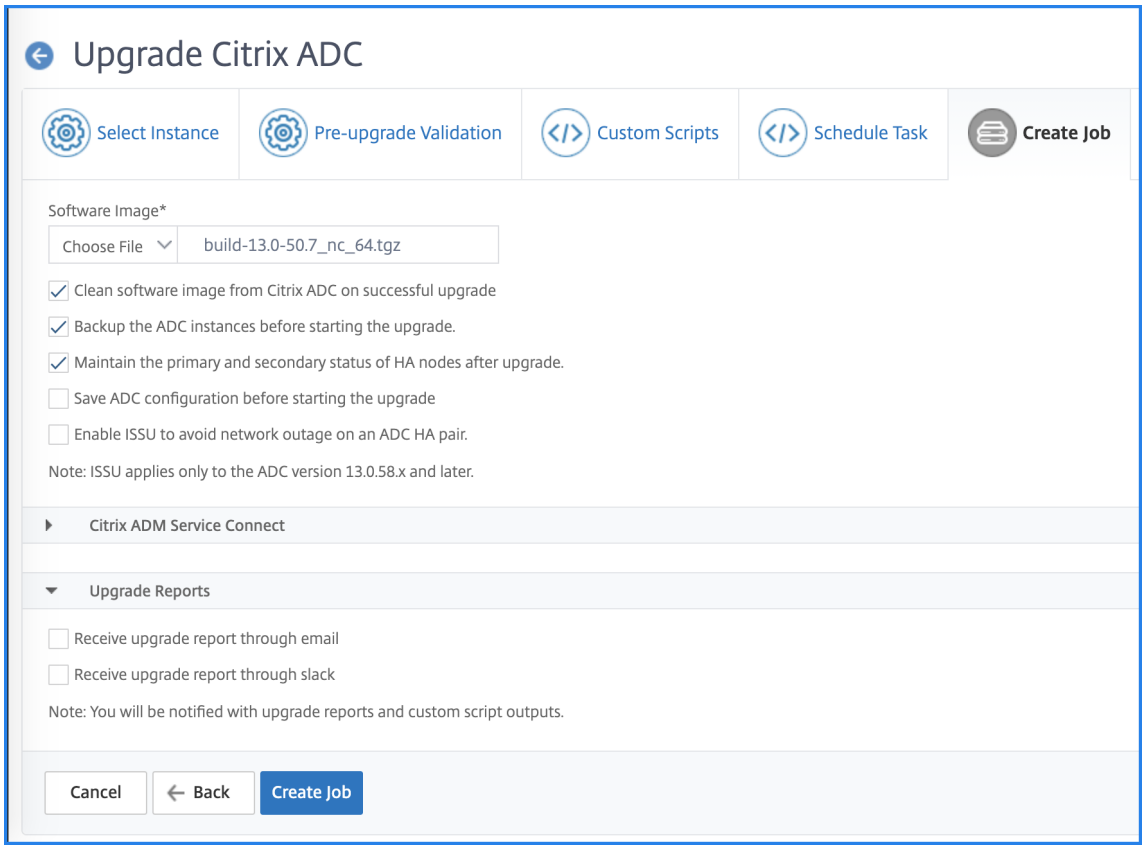
   a) 从 “ 软件映像” 列表中选择以下选项之一：

      - 本地 -从本地计算机中选择实例升级文件。
      - 装置 -从 ADM 文件浏览器中选择实例升级文件。ADM GUI 显示存在于的实例文件 `/var/mps/mps_images`。

b) 指定要将图像上传到实例的时间：

- 立即上传 -选择此选项可立即上传图片。但是，升级作业将在计划的时间运行。
- 执行时上传 -选择此选项可在升级作业执行时上传映像。

- 成功升级时从 **Citrix ADC** 清除软件映像-选择此选项可在实例升级后清除 ADC 实例中上传的映像。
- 在开始升级之前备份 **ADC** 实例。-创建所选 ADC 实例的备份。
- 升级后保持 **HA** 节点的主和辅助状态：如果希望升级任务在每个节点升级后启动故障转移，请选择此选项。通过这种方式，升级作业将保持节点的主和次要状态。
- 在开始升级之前保存 **ADC** 配置-升级 ADC 实例之前保存正在运行的 ADC 配置。
- 使 **ISSU** 能够避免 **ADC HA** 对上的网络中断 -ISSU 确保 ADC 高可用性对的零停机升级。此选项提供了在升级期间支持现有连接的迁移功能。因此，您可以在不停机的情况下升级 ADC HA 对。以分钟为单位指定 ISSU 迁移超时。
- 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
- 通过松弛接收执行报告-以松弛的方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。



9. 单击 创建作业。

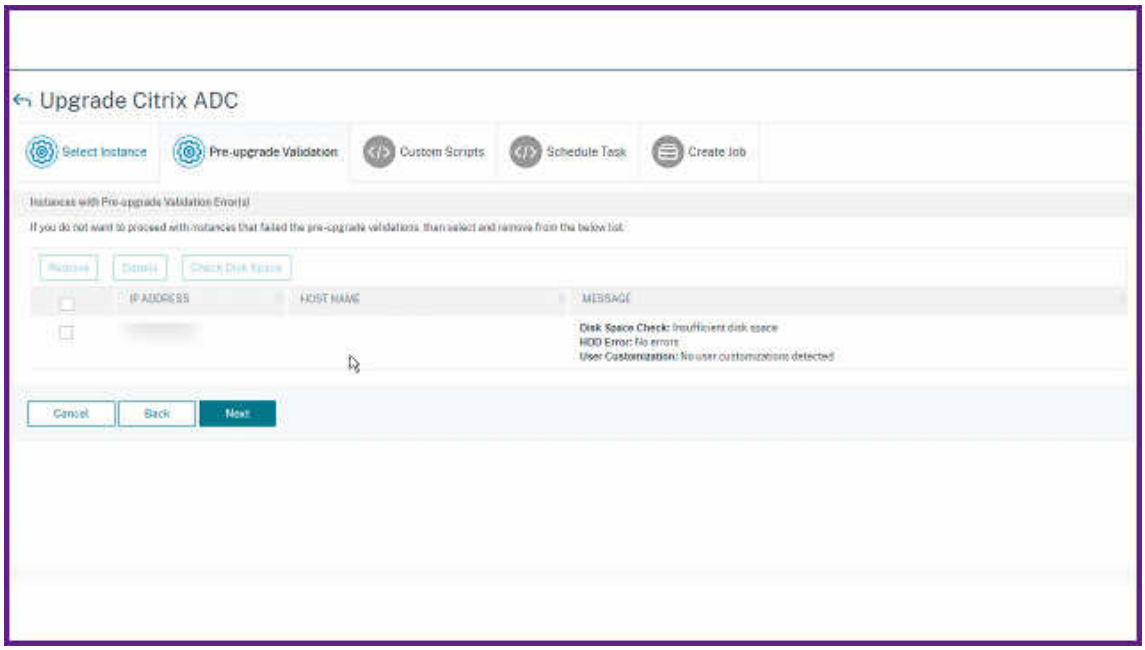
升级作业将显示在 网络 **>** 配置作业 **>** 维护作业中。编辑现有作业时，如果必填字段已填充，则可以切换到任何选项卡。例如，如果您位于“ 选择配置”选项卡中，则可以切换到“ 作业预览”选项卡。

清理 **ADC** 磁盘空间

如果您在升级 ADC 实例时遇到磁盘空间不足的问题，请从 ADM GUI 本身清理磁盘空间。

1. 在 升级前验证选项卡中，选择存在磁盘空间问题的实例。
2. 选择 检查磁盘空间。

   此窗格显示实例空间不足的磁盘。它还显示磁盘上已使用和可用的内存量。
3. 在 检查磁盘空间窗格中，选择需要清理的实例。
4. 单击“ 磁盘清理”。



5. 选择要删除的文件。
6. 点击 删除

下载 **ADC** 升级作业的综合差异报告

如果指定了自定义脚本，则可以下载 ADC 升级作业的差异报告。差异报告包含升级前脚本和升级后脚本输出之间的差异。使用此报告，您可以确定升级后 ADC 实例发生了哪些更改。

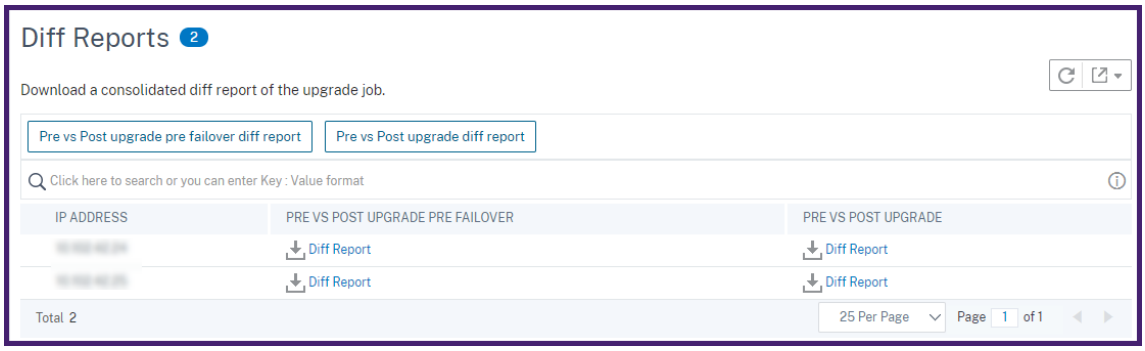
> 注意：
>
> 只有在升级前和升级后阶段指定了相同脚本时，才会生成差异报告。

要下载升级作业的差异报告，请执行以下操作：

1. 导航到 网络 **>** 配置作业 **>** 维护作业。
2. 选择要下载差异报告的升级作业。
3. 单击 差异报表。
4. 在 差异报告中，下载所选升级作业的合并差异报告。

   在此页面中，您可以下载以下任何差异报告类型：

   - 升级前与升级后的故障转移前差异报告
   - 升级前与升级后差异报告



使用配置模板创建审计模板

April 23, 2021

现在，您可以使用先前保存为配置模板的配置命令来创建可应用于特定 Citrix ADC 实例的审核模板。创建审计模板时，您可以将之前保存的配置模板拖到 Commands 字段中，然后编辑模板以满足您的要求。然后，您可以将审核模板应用于特定的 Citrix ADC 实例。Citrix ADM 将这些实例与审计模板进行比较，并报告任何不匹配。此过程可帮助您发现错误并及时对其进行纠正。

您可以在创建作业并将一组配置命令另存为模板的同时创建配置模板。在“ 创建作业”页面上保存这些模板时，它们将自动显示在“ 创建模板”页面上。

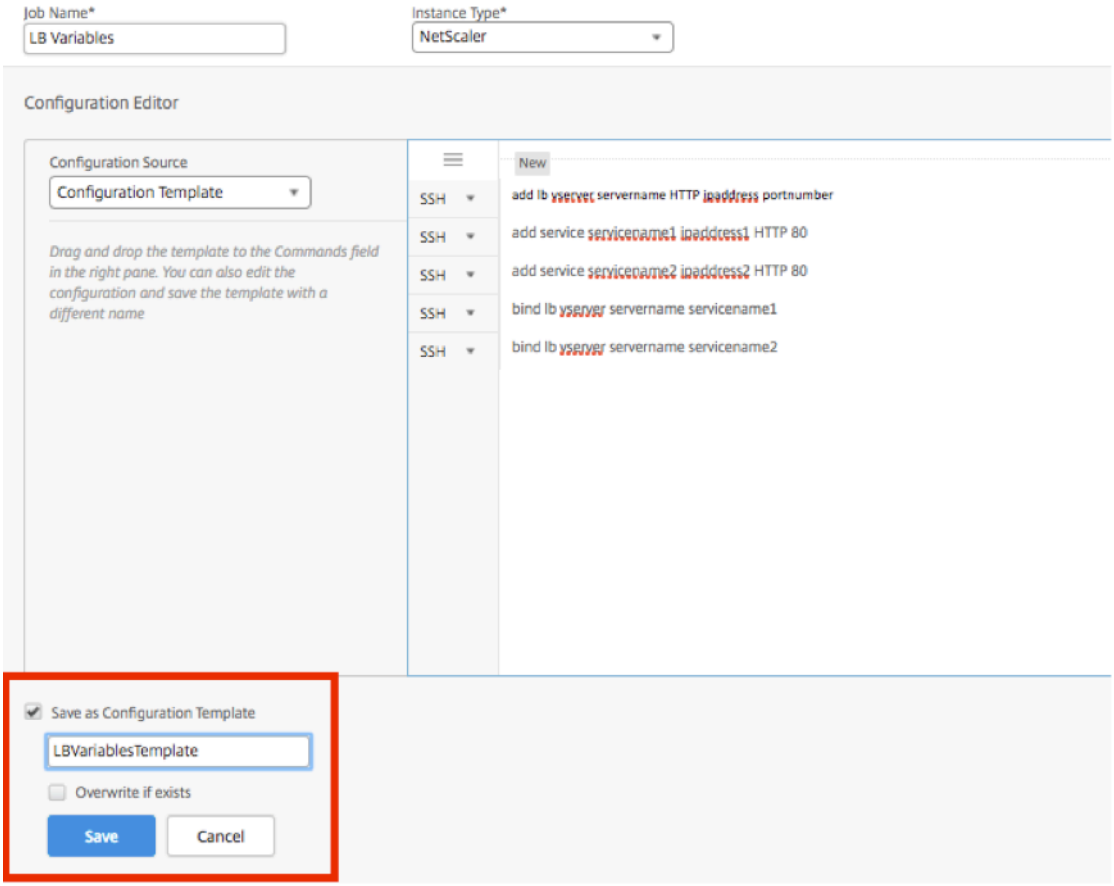
例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。

此示例使用以下命令：

```
add lb vserver >servername> HTTP <ipaddress portnumber>

add service <servicename1 ipaddress1> HTTP 80

add service <servicename2 ipaddress2> HTTP 80

bind lb vserver <servername servicename1>

bind lb vserver <servername servicename2>
```

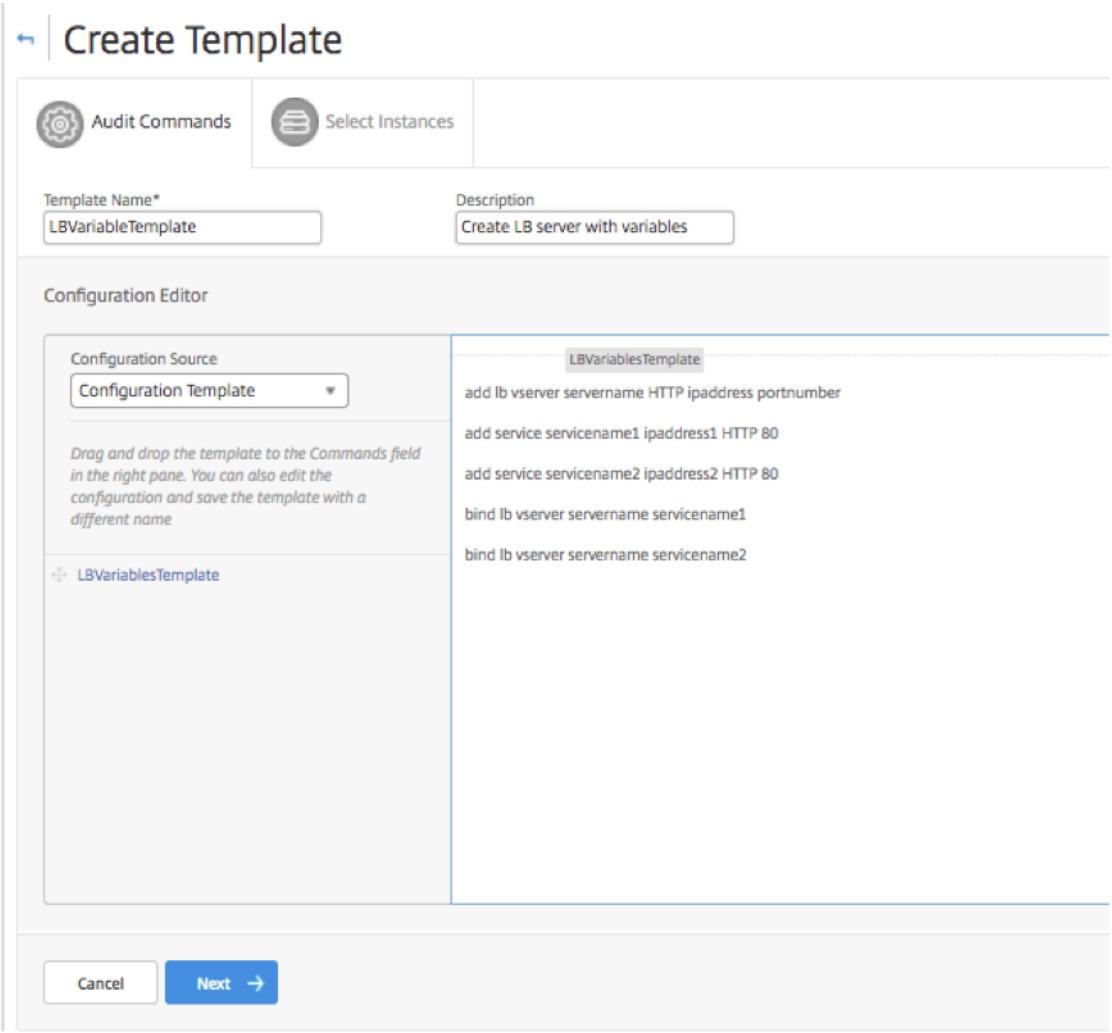

要在 **Citrix ADM** 中保存配置模板，请执行以下操作：

1. 导航到 “ 网络” > “ 配置作业”，然后单击 “ 创建作业”。
2. 在 创建任务页面上，指定作业名称和实例类型。
3. 选择 配置模板作为配置源，然后在 命令字段中输入诸如上例中的命令。
4. 选中 另存为配置模板复选框，然后为模板指定名称。您可以选择覆盖已有的其他同名模板。
5. 单击保存。



要使用配置模板在 **Citrix ADM** 中创建审核模板，请执行以下操作：

1. 导航到 “ 网络” > “ 配置审计” > “ 审计模板”，然后单击 “ 添加”。
2. 在 创建模板页面上，指定模板名称的名称，然后输入描述。
3. 从 “ 配置源” 列表中，选择 “ 配置模板”，然后将模板拖到右侧窗格的 “命令” 字段中。您也可以编辑配置并使用另一个名称保存模板。单击 “ 下一步”。
4. 在选择实例选项卡上，单击 **“添加实例”** 并添加要在其上运行配置的实例。单击确定。
5. 单击完成。



审核模板显示在 “Audit Templates”（审核模板）列表中，每 12 小时根据指定实例的配置运行一次。

在配置作业中使用 **SCP**（放置）命令

April 23, 2021

您可以使用 Citrix ADM 的 “配置作业” 功能来创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。作业是可以在一个或多个托管实例上创建并运行的一组配置命令。例如，您可以使用配置作业进行设备升级。

Citrix ADM 中的配置作业使用安全外壳 (SSH) 命令来配置实例，您可以配置配置作业以使用安全拷贝 (SCP) 安全地传输文件。SCP 基于 SSH 协议。可以包含在配置作业中的 **SCP** 命令之一是 “put” 命令。您可以在配置作业中使用 “put” 命令将存储在系统本地目录中的一个或多个文件上传或传输到 Citrix ADM，然后传输到 Citrix ADC 实例上的一个或多个目录。

> 注意文件将上载到 Citrix ADM，然后将其复制（放置）到选定的 Citrix ADC 实例。上载的文件存储在 Citrix ADM 中，只有在删除作业时才会删除。对于计划稍后运行的作业来说，这是必要的。

该命令语法如下：

```
put <local_filename> <remote_path/remote_filename>
```

其中，

<local_filename> 是要上载的本地文件的名称。

<remote_path/remote_filename> 是远程目录的路径，以及将文件复制到该目录时要分配给该文件的名称。

创建配置作业时，可以将本地和远程文件名参数转换为变量。这样，您可以在每次运行作业时为同一组 Citrix ADC 实例分配不同的文件给这些参数。此外，在一个作业中的多个位置使用某个文件时，如果您要重命名文件，可以重新定义变量，而不是在所有位置更改文件名。

要使用 **put** 命令在配置作业中上载文件，请执行以下操作：

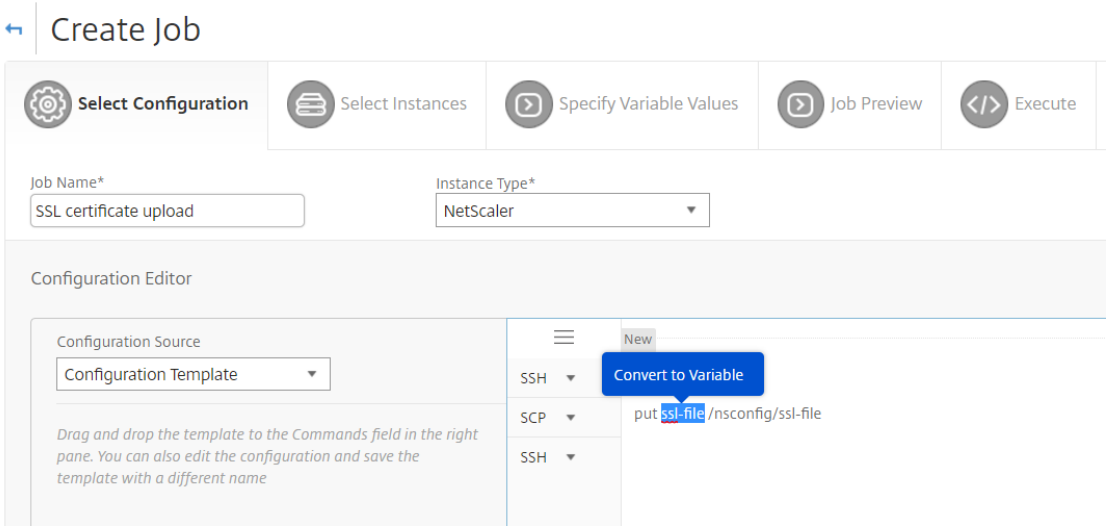
1. 导航到 “ 网络” > “ 配置作业”。
2. 在 “作 业页上，单击 创建作业。
3. 在 创建作业页面上，在 “作业名称” 字段中输入作业的名称，然后在 配置编辑器窗格中输入 “put” 命令。

   例如，如果要创建将本地系统上保存的 SSL 证书文件复制到多个 Citrix ADC 实例的配置作业，则可以添加使用变量而不是特定文件名称的 “放置” 命令，然后将变量类型定义为 “file”。

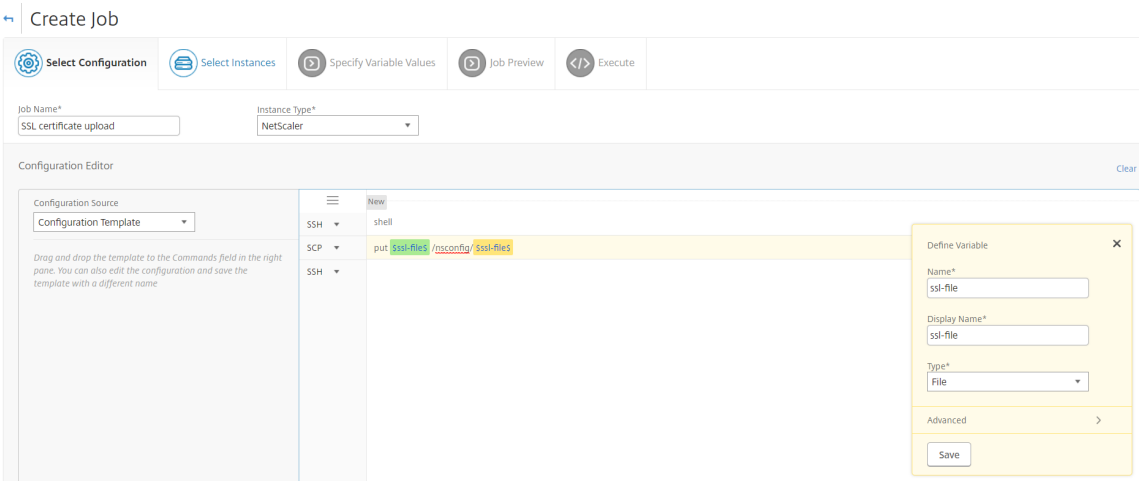
   ```
   put ssl-file /nsconfig/ssl-file
   ```

   在此示例中，

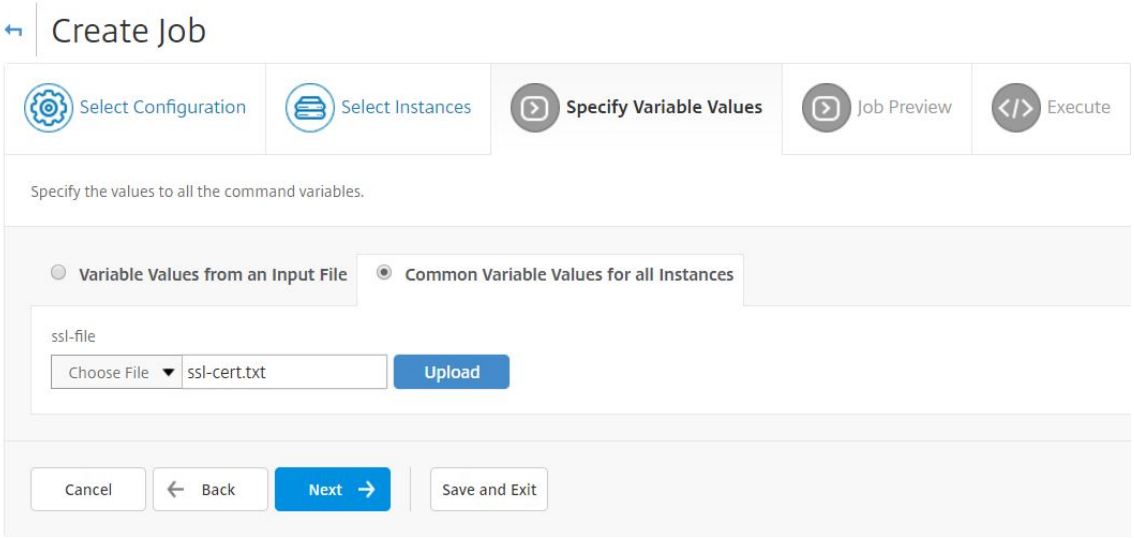
   - `ssl-file` -这是必须在 Citrix ADC 实例中上传的文件的名称。
   - `/nsconfig/ssl-file` - 这是任务执行后实例上用于放置 `ssl-file` 的目标文件夹。
4. 在输入的命令中，选择要转换为变量的文件名，然后单击转换为变量，如下图所示。



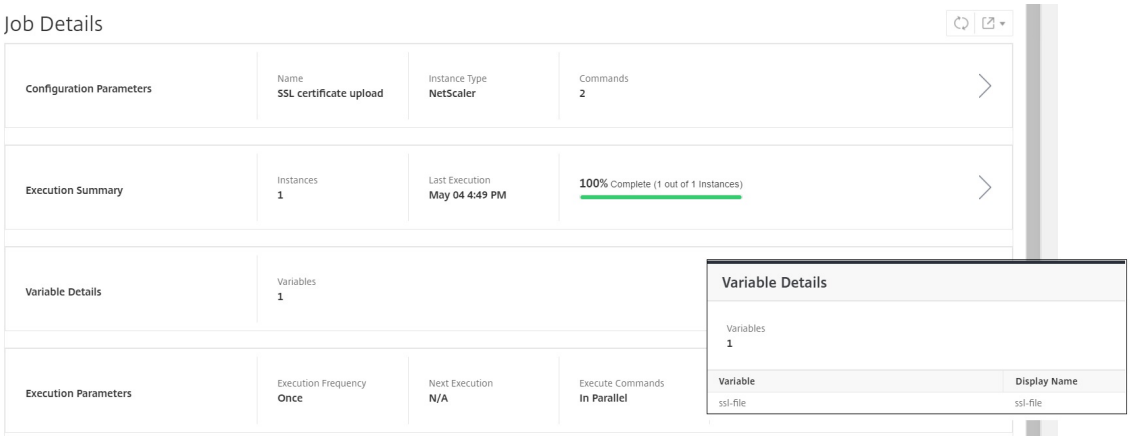
5. 验证文件名是否用美元符号括起来（表示它现在是一个变量），然后单击该变量。
6. 指定变量的详细信息，例如名称、显示名称和类型。
7. 从 类型下拉列表中，选择 文件。单击保存。将变量声明为“文件”类型允许您将文件上传到 Citrix ADM。



8. 单击“下一步”，然后选择要将文件复制到的 Citrix ADC 实例。
9. 在“ 指定变量值”选项卡上，选择 所有实例的公用变量值部分，从系统上的本地存储中选择文件，单击“上传”将文件上载到 Citrix ADM，然后单击“下一步”。



10. 在“作业预览”选项卡上，您可以评估和验证要在每个实例或实例组上运行的命令。
11. 在执行选项卡上，您可以立即运行作业，也可以将其安排在以后运行。您还可以选择如果命令失败，Citrix ADM 必须采取的操作。您还可以创建电子邮件通知以接收有关作业成功或失败以及其他详细信息的通知。单击完成。
12. 您可以通过导航到网络 > 配置作业，然后选择配置的作业来查看作业详细信息。单击“ 详细信息”，然后单击“变量详细信息”列出添加到作业的变量。



重新计划通过使用内置模板配置的作业

April 23, 2021

您可以使用 Citrix Application Delivery Management (ADM) 中的内置模板重新计划作业。例如，您可以更改 Citrix ADM 在命令失败时必须执行的操作。如果之前选择了忽略错误并继续，可以将其更改为在命令失败时回滚所有成功的命令。

重新计划通过使用 **Citrix ADM** 中的内置模板配置的作业

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业”。
2. 选择要编辑的作业，添加或删除实例、指定变量值，然后更改执行操作和设置。
3. 单击 **Finish**（完成）重新计划作业。

> 注意
>
> 您还可以选择作业，然后单击 “ 再次执行” 以运行作业，而不修改任何源、实例和命令。当您必须在相同的实例上运行相同的命令集时，此功能非常有用。有时，作业可能会遇到来自服务器端的暂时错误，并且您可能需要再次运行作业。

在配置作业中重复使用配置审计模板

April 23, 2021

作为管理员，您现在可以在创建作业并运行配置审核时将配置命令保存为一组可重用的配置模板。在配置作业中创建和保存的配置模板在配置审核中可用于创建可应用于特定 Citrix ADC 实例的审核模板。同样，可以在 “Configuration Jobs”（配置作业）中访问在 “Configuration Audit”（配置审核）模块中创建的审核模板，以便可以将模板作为配置

作业运行。现在，在模板中所做的任何更改在 “Configuration Jobs”（配置作业）模块和 “Configuration Audit”（配置审核）模块中均可见。

以前，必须为同一配置单独创建配置作业模板和配置审核模板，并将其保存为不同的文件。这导致在创建和维护模板时所做工作量加倍。

Citrix Application Delivery Management (ADM) 允许您将此模板保存在系统中，以便在配置作业中也可用审核模板。现在可以使用审核模板创建配置作业。这样，可以在配置作业与配置审核之间互换使用模板。

例如，假定一个基本的负载平衡配置，在该配置中，您添加一个负载平衡虚拟服务器、添加两个服务以及将服务绑定到虚拟服务器。

此示例使用以下命令：

```
add lb vserver servername HTTP ipaddress portnumber

add service servicename1 ipaddress1 HTTP 80

add service servicename2 ipaddress2 HTTP 80

bind lb vserver servername servicename1

bind lb vserver servername servicename2
<!--NeedCopy-->
```

在 **“Configuration Audit”**（配置审核）中创建模板并在 **“Configuration Jobs”**（配置作业）中重用该模板

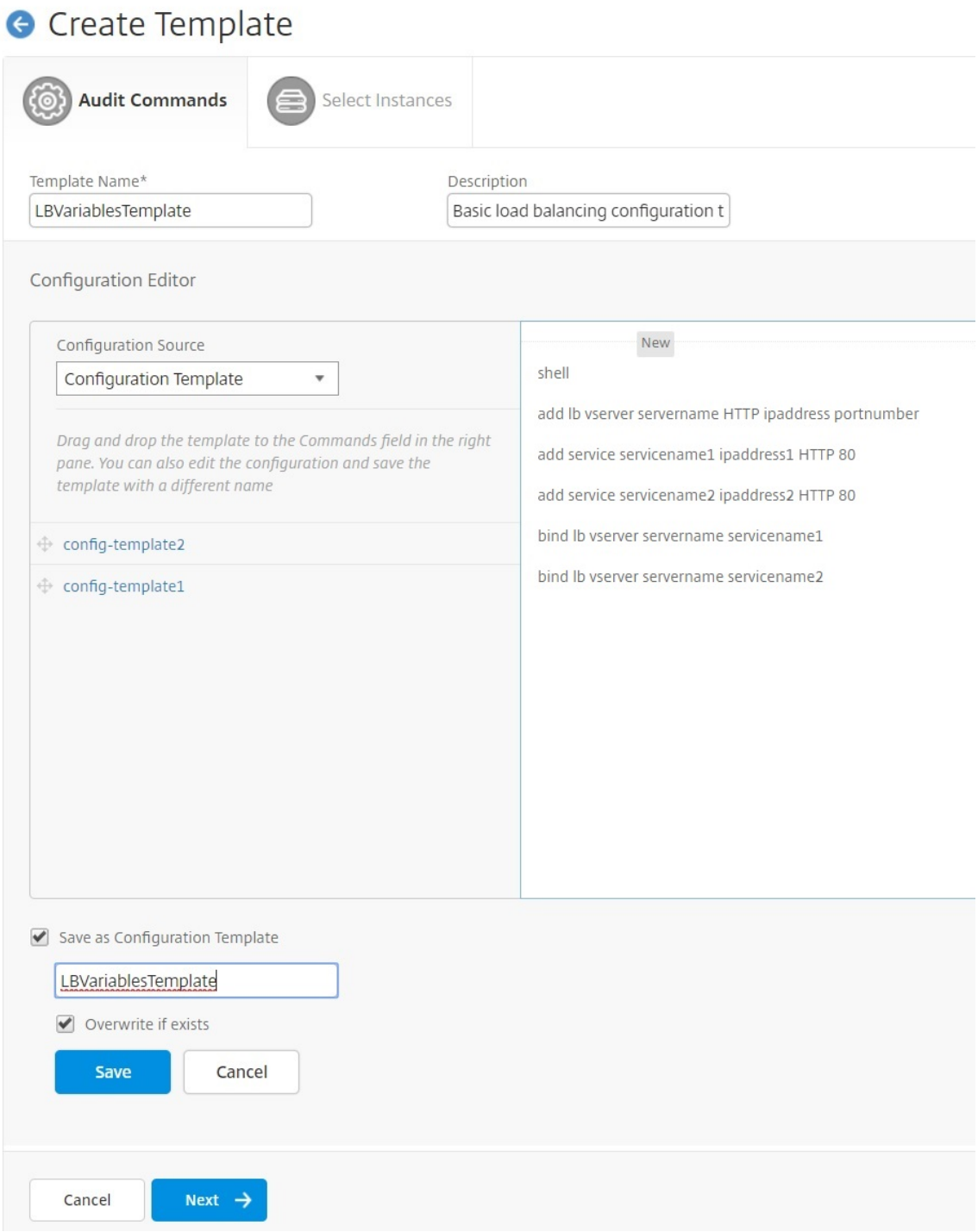
执行以下任务，在配置审核模块上创建模板，并在配置作业模块中重复使用相同的模板。

要创建审计模板，请执行以下操作：

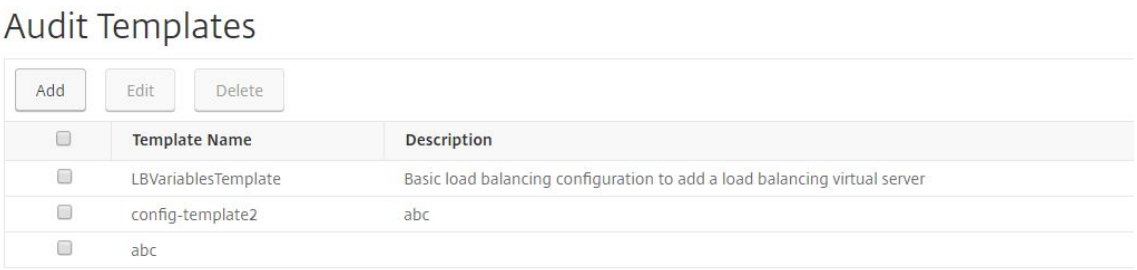
1. 在 Citrix ADM 中，导航到网络 **>** 配置审核 **>** 审核模板，然后单击添加。
2. 在 “创建模板” 页面上，指定模板名称。您还可以在 描述字段中添加有关模板的更多信息。
3. 在 命令窗格中，输入示例中的命令。
4. 选中另存为配置模板复选框并为模板指定一个名称，例如，您可以将此模板命名为 “lbVariableStemPlate。“ 您可以选择覆盖已有的其他同名模板。

   > 注意：审计模板名称可以与配置模板名称相同。

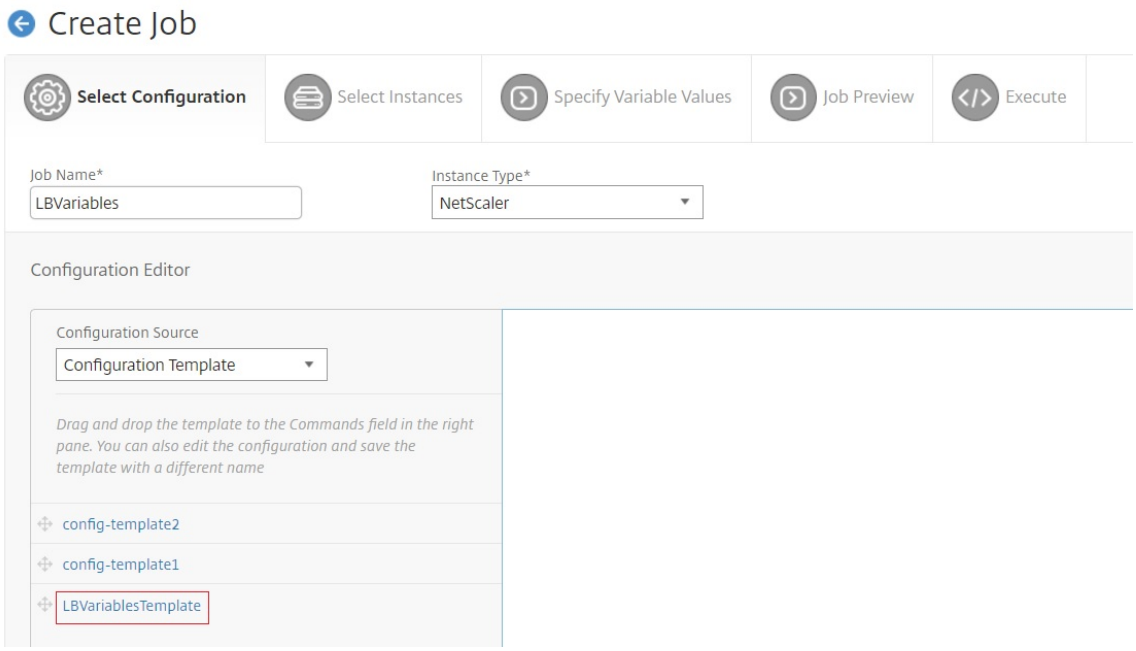
5. 单击 “保存”，然后单击 “ 下一步”。



6. 单击下一步。
7. 在“选择实例”选项卡中，选择要在其上运行这些配置命令的 **Citrix ADC** 实例，然后单击“完成”。新模板现在显示在审核模板列表中。

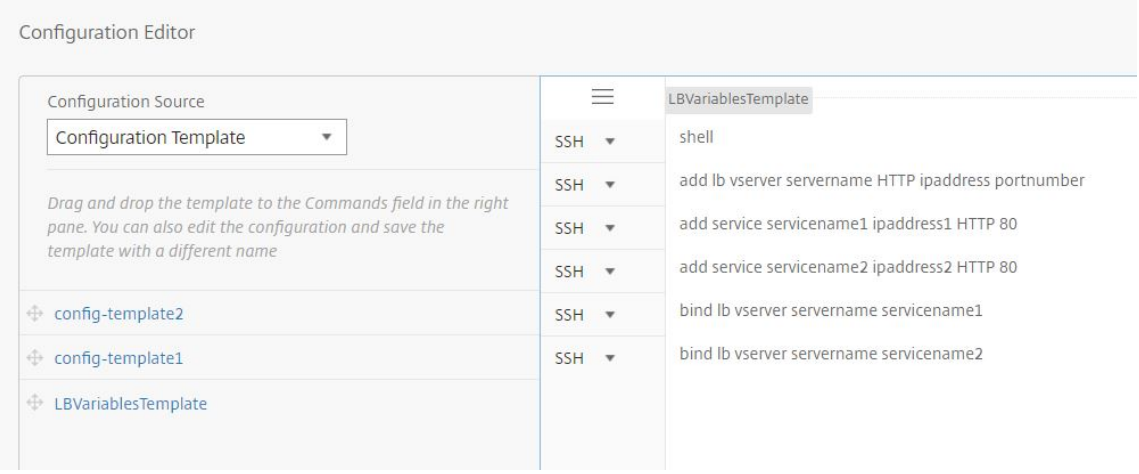


8. 如果要运行这些配置命令，请导航到 网络 **>** 配置作业，然后单击 创建作业。您之前创建的审核模板将作为配置模板列出。



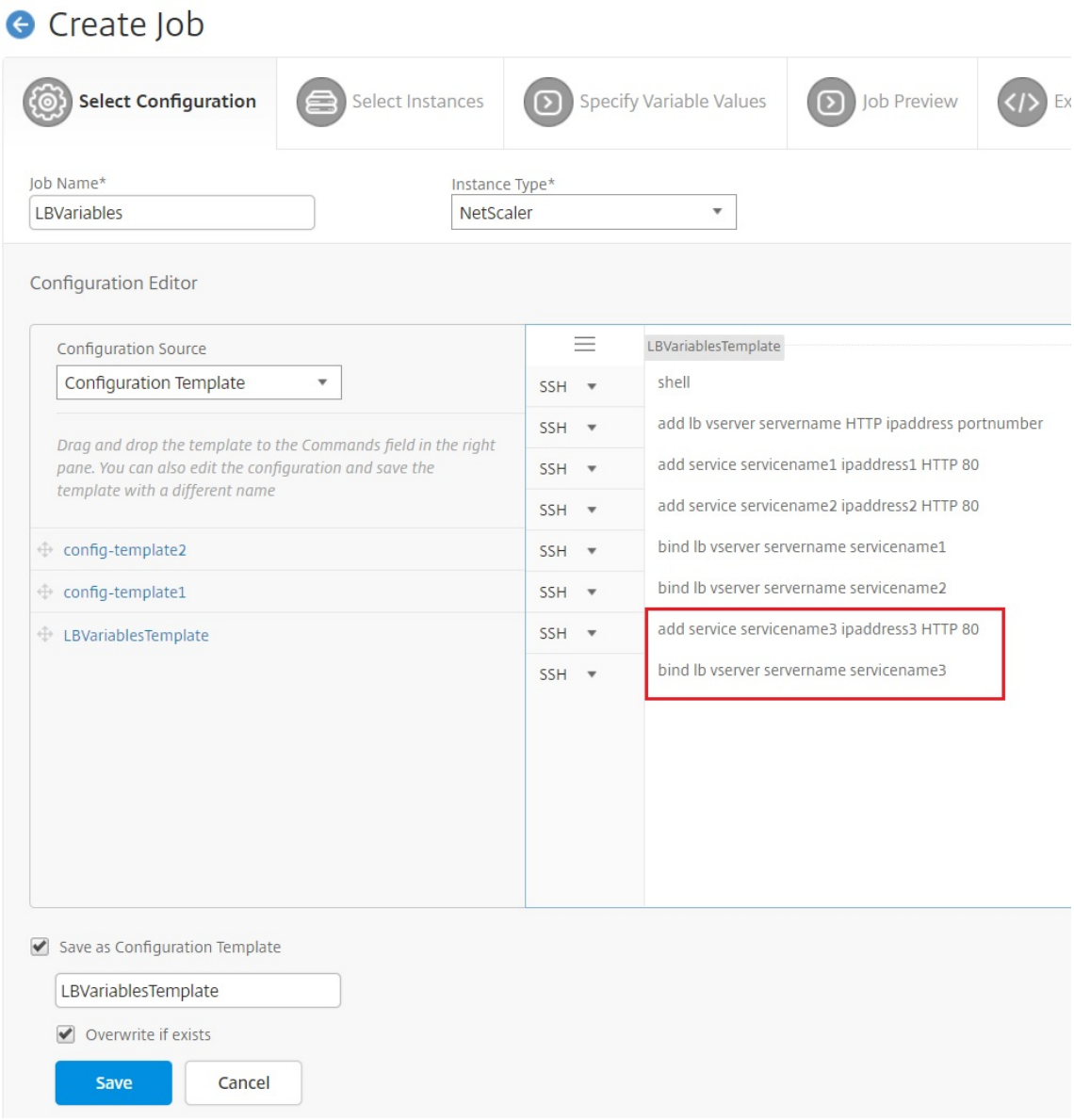
要在配置作业中重复使用审核模板，请执行以下操**:**

1. 输入作业的名称并选择实例类型，然后将模板拖到命令窗格中。

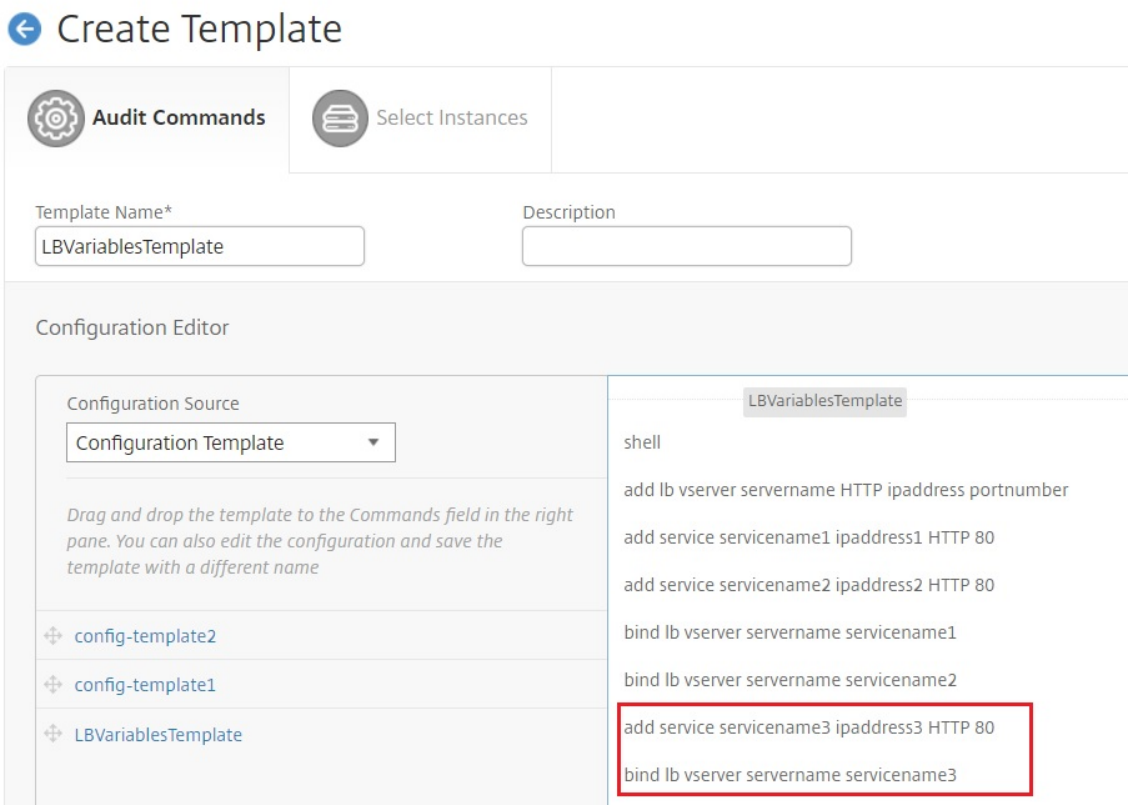


创建配置作业时，可以将本地和远程文件名参数转换为变量。这样，您可以在每次运行作业时为同一组 Citrix ADC 实例分配不同的文件给这些参数。

2. 在您输入的命令中，选择要转换为变量的文件名，然后单击转换为变量。
3. 在 选择实例选项卡中，选择要在其上运行这些命令的实例。
4. 如果您在命令中指定了任何变量，请在 指定变量值选项卡中，选择以下选项之一以为您的实例指定变量：
   - 输入文件中的变量值-下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器。
   - Common variable values for all instances（用于所有实例的公用变量值）- 指定 syslog 服务器 IP 地址和端口。
5. 在“作业预览”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令，然后单击“下一步”。
6. 在“执行”选项卡中，单击“完成”运行配置作业。现在，如果您要将另一个服务添加到此负载平衡服务器，并将该服务绑定到该服务器，可以在命令页面上编辑命令并将其保存。



7. 导航到 审计模板，然后单击 添加。
8. 将 “lbVariablestemPlate” 模板拖到命令窗格中。您可以看到该模板中已更新了新命令。



审核模板显示在 “Audit Templates”（审核模板）列表中，每 12 小时根据指定实例的配置运行一次。您现在可以创建模板，并在 “Configuration Jobs”（配置作业）模块与 “Configuration Audit”（配置审核）模块之间重用这些模板。

导入和导出配置模板

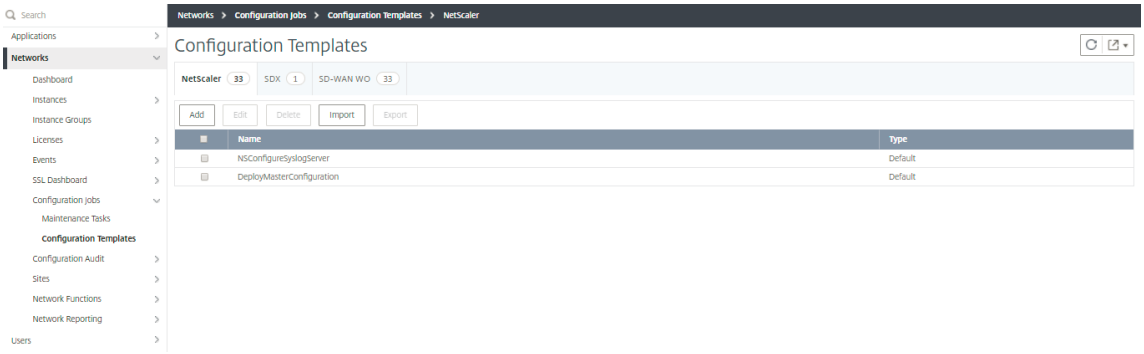
April 23, 2021

您可以从任何 Citrix Application Delivery Management (ADM) 导出配置模板。您还可以在将来随时将文件导入到同一个或另一个 Citrix ADM 中。配置模板数据（如配置命令、变量定义和参数）不会丢失。

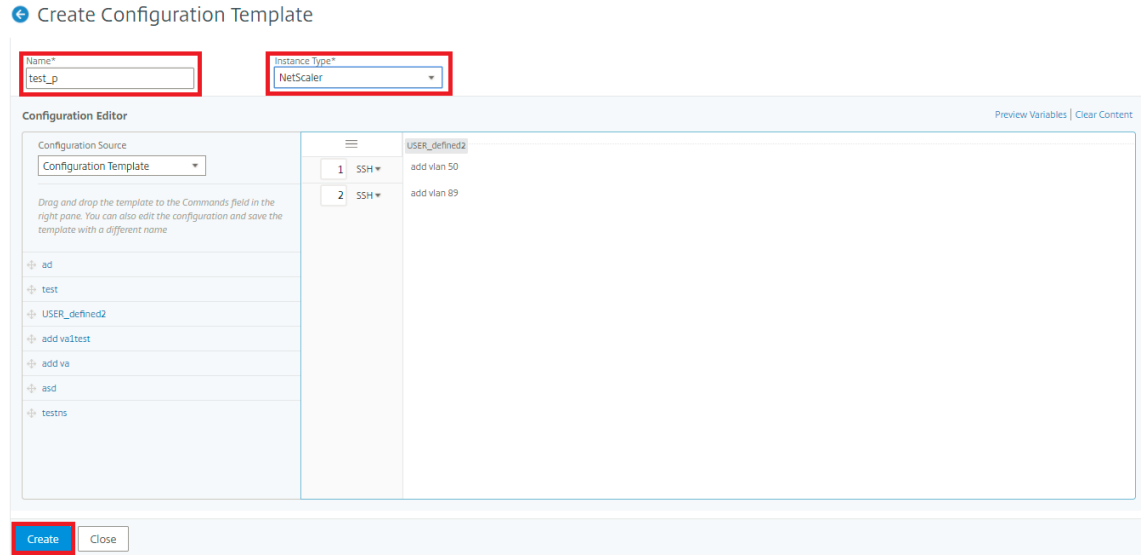
您可以将配置模板导出为 **.json** 文件格式，并将其保存在本地文件夹中。您可以导入配置模板。**json** 文件添加到 Citrix ADM 中。此文件可能是新文件，也可能是从相同或其他 Citrix ADM 导出的文件。

要导出配置模板，请执行以下操作：

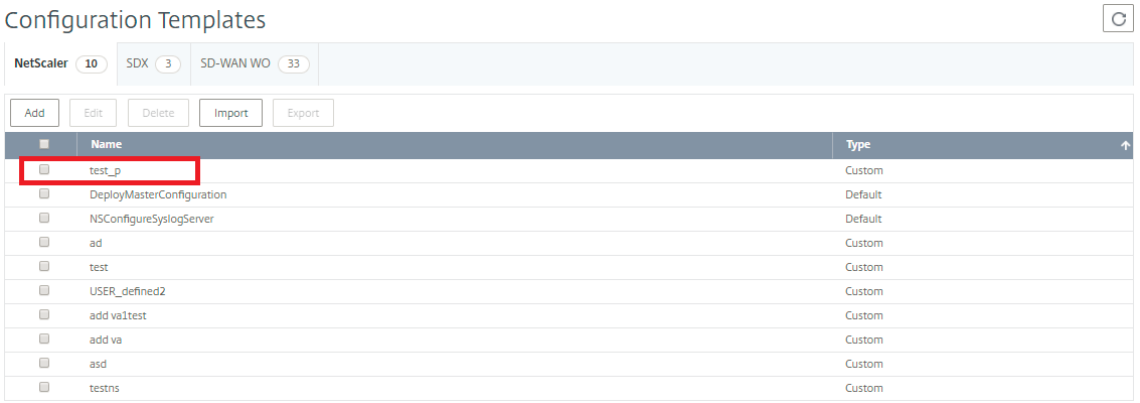
1. 导航到 **“网络” > “配置作业” > “配置模板”**。
2. 单击 添加按钮创建配置模板。



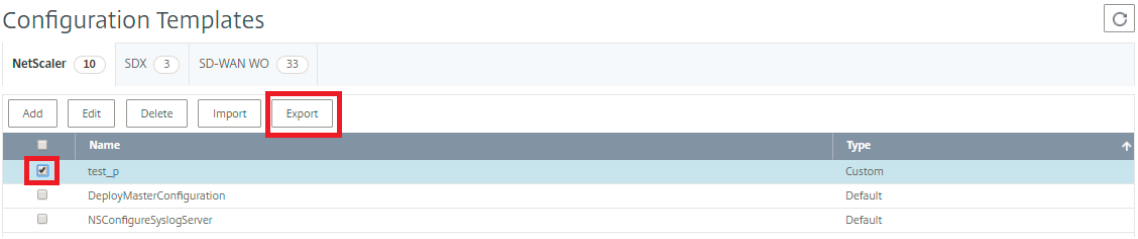
3. 在 创建配置模板页面上，指定配置模板名称，然后选择实例类型。在 配置编辑器下，从下拉菜单中选择配置源作为配置模板。您可以将现有配置模板拖到配置编辑器中。单击创建。



4. 导航到 **“网络” > “配置作业” > “配置模板”** 以查看在配置模板列表中创建的模板。



5. 选择新创建的配置模板，然后单击 导出按钮。

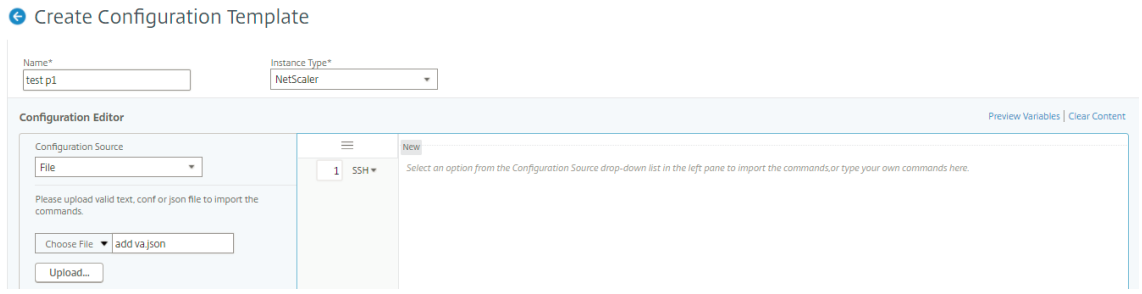


相应的配置模板以 **.json** 格式在本地系统上下载。

要导入配置模板，请执行以下操作：

1. 导航到 **“网络” > “配置作业” > “配置模板”**，然后单击 “ 导入” 按钮。选择您拥有的路径。配置模板的 **json** 文件并上传.**json** 文件。强烈建议上传. 已导出的 **json** 文件。

2. 您还可以使用配置编辑器上的 文件选项导入配置模板。
3. 从 配置编辑器的下拉菜单中选择 文件。
4. 选择选择文件 (.**json** 文件）并上传配置模板。**json** 文件。



> 注意
>
> - 每个新导入的模板都存储一个新的 id 字符串。
> - 仅当文件保存在中时，才能导入配置模板。**JSON** 格式。如果从本地系统导入 **.json** 文件以外的配置模板，则会显示错误并导入文件失败。

维护作业

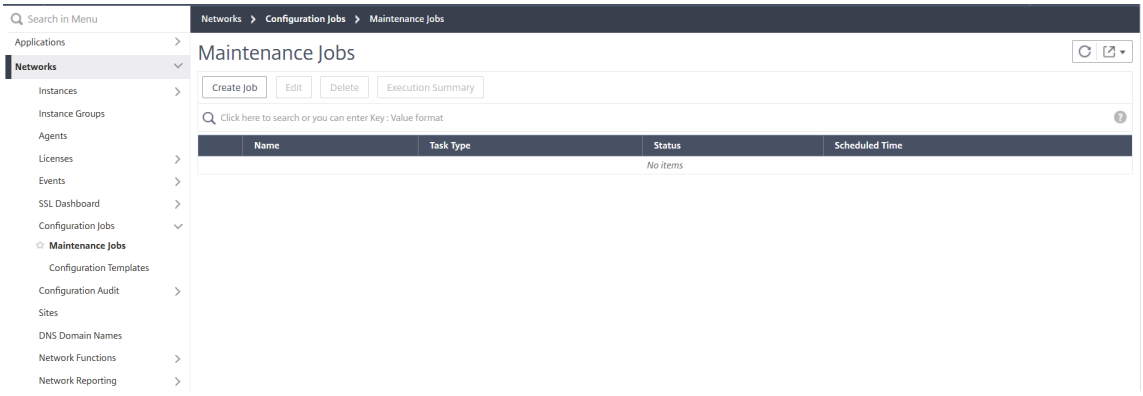
April 23, 2021

您可以使用 Citrix ADM 创建以下维护作业。然后，您可以在特定日期和时间安排维护作业。

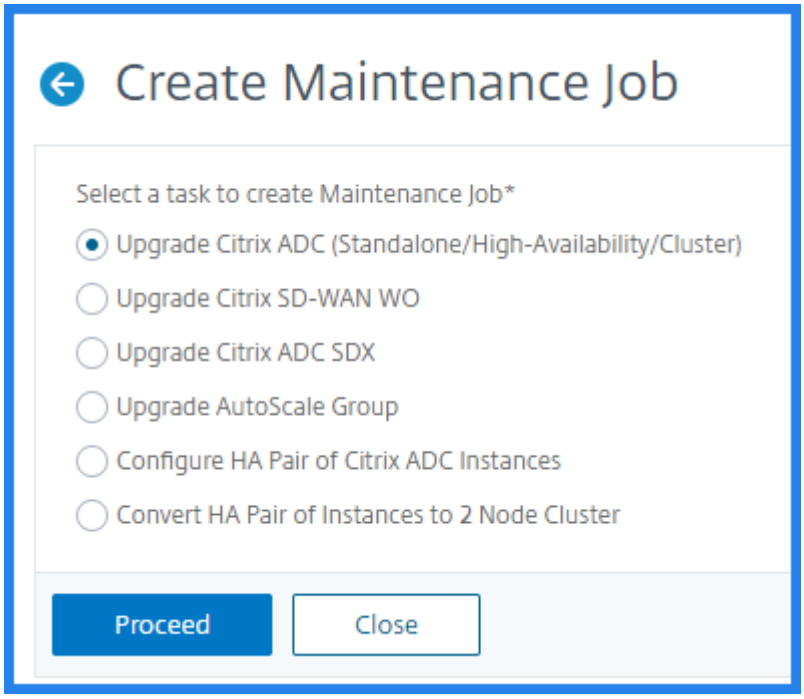
- 升级 Citrix ADC 实例
- 升级 Citrix ADC SD WAN WO 实例
- 升级 Citrix ADC SDX 实例
- 升级自动扩展组中的 Citrix ADC 实例
- 配置 Citrix ADC 实例的高可用性对
- 将 HA 实例对转换为双节点群集

计划升级 **Citrix ADC** 实例

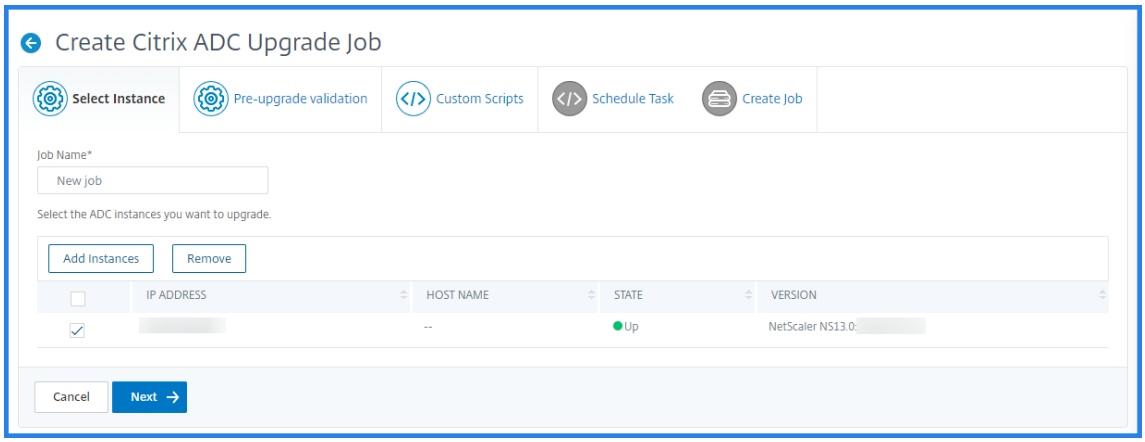
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业” > “ 维护作业”。单击 创建作业按钮。



2. 在 创建维护作业中，选择 升级 **Citrix ADC**（独立/高可用性/群集），然后单击 继续。



3. 在选 择实例中，键入您选择的 作业名称的名称。
4. 单击 添加实例以添加要升级的 ADC 实例。
   - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
   - 要升级群集，请指定群集 IP 地址。

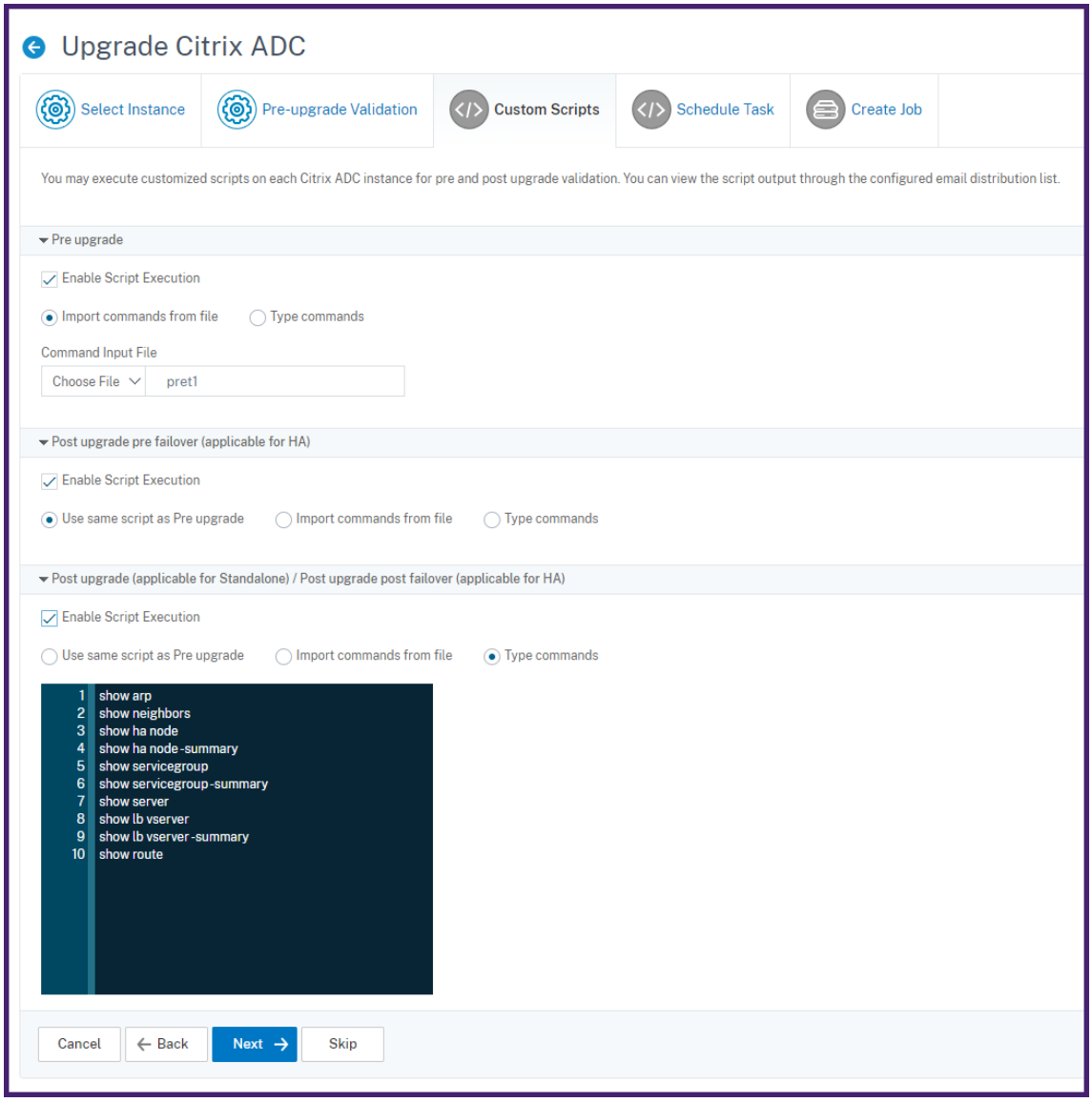


5. 单击 下一步开始对所选实例进行升级前验证。

   升级前验证选项卡显示失败的实例。删除失败的实例，然后单击 “ 下一步”。

   > 重要信息：
   >
   > 如果指定群集 IP 地址，ADM 仅对指定实例而不在其他群集节点上执行升级前验证。

6. 可选，在 自定义脚本中，指定要在实例升级之前和之后运行的脚本。使用以下方法之一来运行命令：
   - 从文件导入命令 -从本地计算机中选择命令输入文件。
   - 键入命令 -直接在 GUI 上输入命令。



您可以使用自定义脚本来检查实例升级之前和之后的更改。例如：

- 升级前后的实例版本。
- 升级前后接口、高可用性节点、虚拟服务器和服务的状态。
- 虚拟服务器和服务的统计信息。
- 动态路由。

7. 在 计划任务中，选择以下选项之一：

   - 立即升级 -升级作业将立即运行。
   - 稍后计划 -选择此选项可以稍后运行此升级作业。当您要升级实例 时，请指定执行日期和开始时间。

     如果要分两个阶段升级 ADC HA 对，请选择对 **HA** 中的节点执行两阶段升级。

     如果要升级 HA 对中的另一个实例，请指定 执行日期和 开始时间。

8. 在 创建作业中，指定以下详细信息：

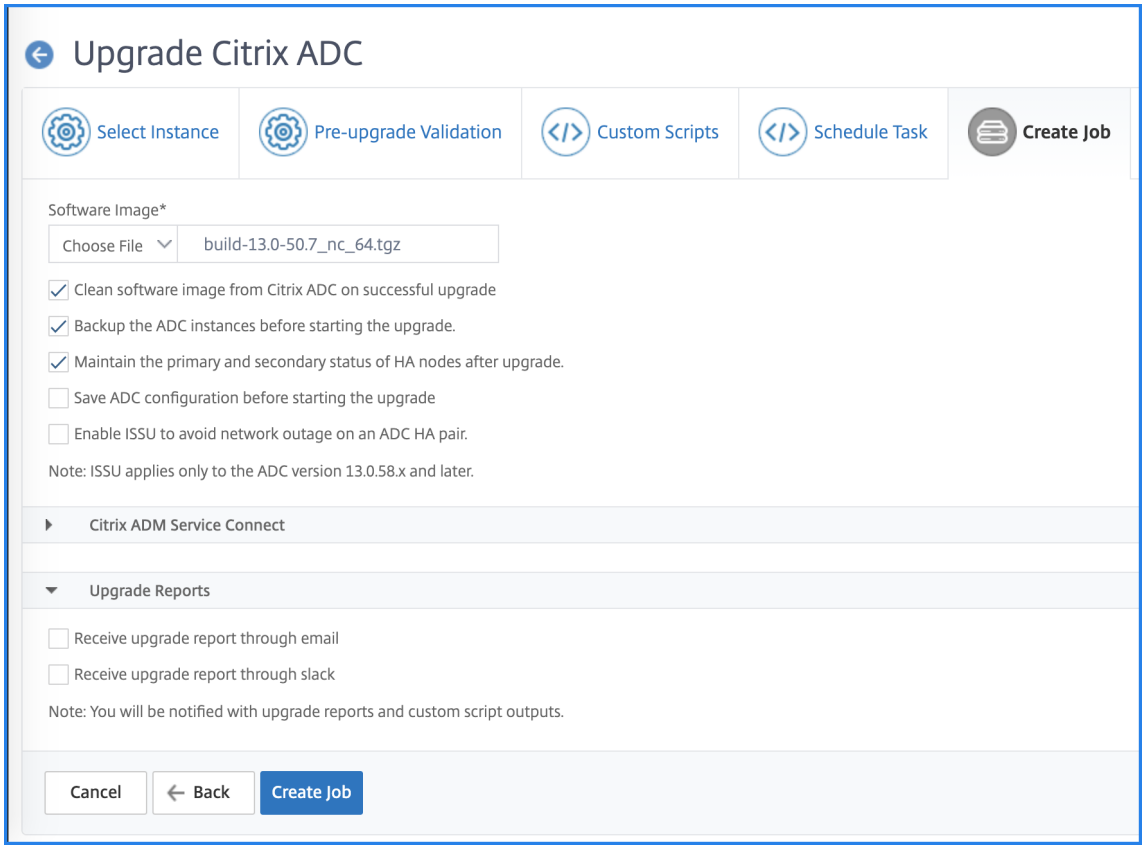
   a) 从 “ 软件映像” 列表中选择以下选项之一：

      - 本地 -从本地计算机中选择实例升级文件。
      - 装置 -从 ADM 文件浏览器中选择实例升级文件。ADM GUI 显示存在于的实例文件 `/var/mps/mps_images`。

   b) 指定要将图像上传到实例的时间：

      - 立即上传 -选择此选项可立即上传图片。但是，升级作业将在计划的时间运行。
      - 执行时上传 -选择此选项可在升级作业执行时上传映像。

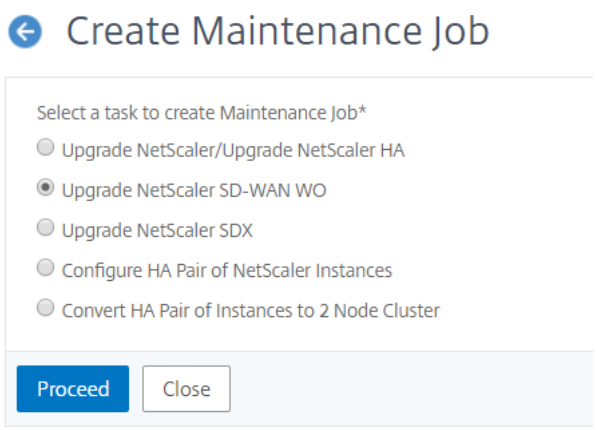
   - 成功升级时从 **Citrix ADC** 清除软件映像**-**选择此选项可在实例升级后清除 ADC 实例中上传的映像。
   - 在开始升级之前备份 **ADC** 实例。-创建所选 ADC 实例的备份。
   - 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
   - 通过松弛接收执行报告**-**以松弛的方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。



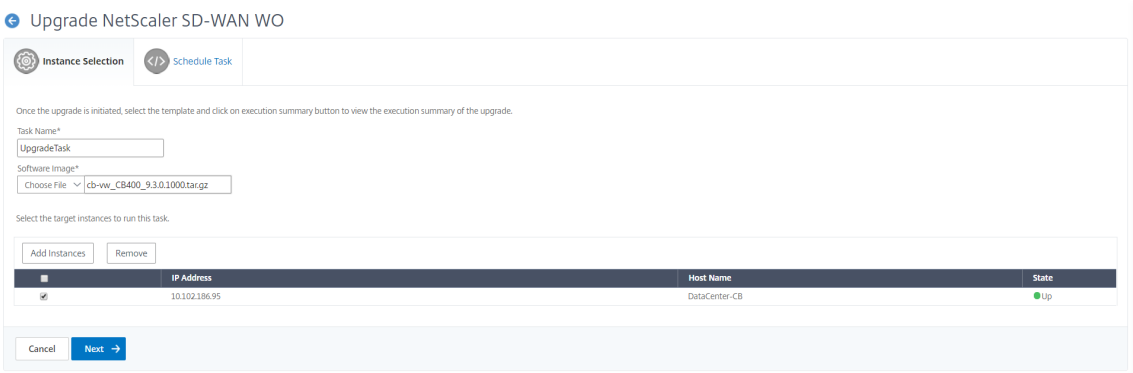
9. 单击 创建作业。

计划升级 **Citrix ADC SD-WO** 实例

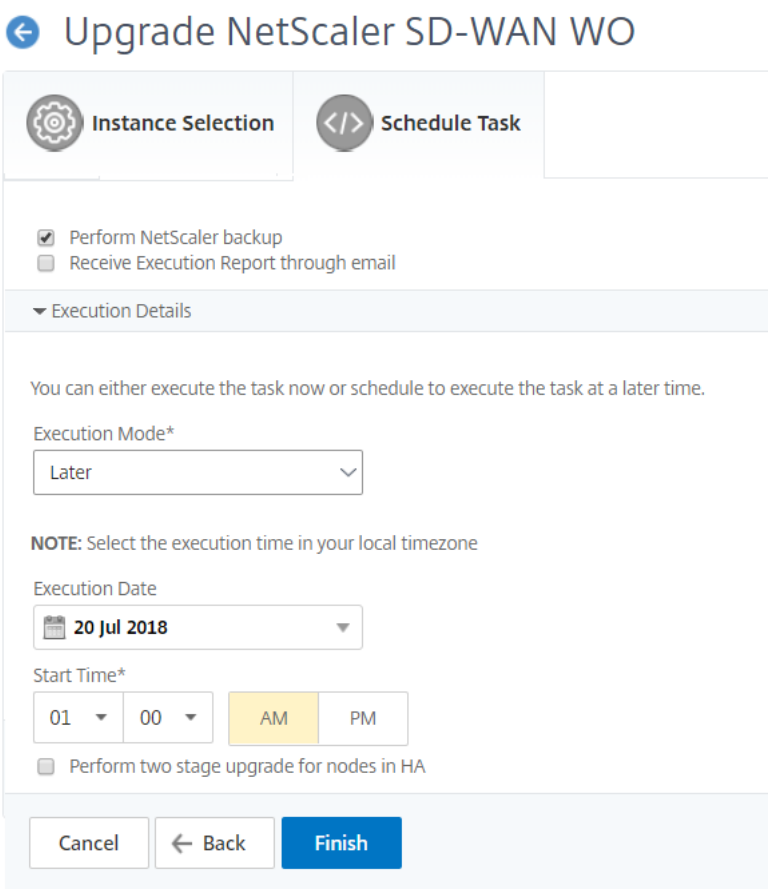
1. 导航至 “ 网络” > “ 配置作业” > “ 维护作业”。单击 “ 创建作业” 按钮。
2. 在 “ 创建维护作业” 页上，选择 “ 升级 **Citrix ADC SD-WAN WO** ”，然后单击 “ 继续”。



3. 在 “ 升级 **Citrix ADC SD-WAN WO** ” 页上的 “ 实例选择” 选项卡中，添加 任务名称。从 “软件映像” 列表中，选择 “本地计算机” 或 “设备”（构建文件必须存在于 Citrix ADM 虚拟设备上）。添加要在其上运行升级过程的 Citrix ADC SD-WO 实例。单击下一步。



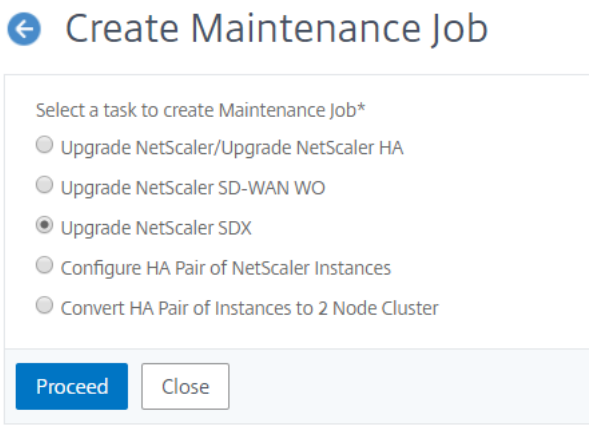
4. 要立即升级 Citrix ADC SD-WAN WO 实例，请从 “ 执行模式” 列表中选择 “ 立即”。单击完成。
5. 要稍后升级 Citrix ADC SD-WAN WO 实例，请从 “执行模式” 列表中选择 “ 稍后”。然后，您可以选择升级 Citrix ADC SD-WO 实例的执行日期和开始时间。
6. 您可以启用电子邮件通知，以接收升级 Citrix ADC SD-WAN WO 实例的执行报告。单击 “通 过电子邮件接收执行报告” 复选框以启用电子邮件通知。
7. 选择 **+** 图标以创建电子邮件通讯组列表。



8. 在“创建电子邮件通讯组列表”页上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在**“发件人”**框中，添加要从中发送邮件的电子邮件地址。在“收件 人”框中，添加要向其发送邮件的电子邮件地址。您还可以添加一个或多个要向其发送邮件副本和副本的电子邮件地址，而不会在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成配置过程。

计划升级 **Citrix ADC SDX** 实例

1. 在 Citrix ADM 中，导航到“网络”>“配置作业”>“维护作业”。单击“创建作业”按钮。
2. 在 创建维护作业页上，选择 升级 **Citrix ADC SDX** ”，然后单击 继续。



3. 在 “ 升级 **Citrix ADC SDX** 装置” 页上的 “ 实例选择” 选项卡中，添加 任务名称。从 “软件映像” 列表中，选择 “本地计算机” 或 “设备”（构建文件必须存在于 Citrix ADM 虚拟设备上）。添加要在其上运行升级过程的 Citrix ADC SDX 实例。单击下一步。
4. 您可以启用电子邮件通知，以接收升级 Citrix ADC SDX 实例的执行报告。单击 “通 过电子邮件接收执行报告” 复选框以启用电子邮件通知。
5. 选择 **+** 图标以创建电子邮件通讯组列表。
6. 要立即升级 Citrix ADC SDX 实例，请从 “ 执行模式” 列表中选择 “ 立即”。单击完成。
7. 要稍后升级 Citrix ADC SDX 实例，请从 “ 执行模式” 列表中选择 “ 稍后”。然后，您可以选择用于升级 Citrix ADC SDX 实例的执行日期和开始时间。
8. 在 “ 创建电子邮件通讯组列表” 页上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在 **“**发件人**”** 框中，添加要从中发送邮件的电子邮件地址。在 “收件 人” 框中，添加要向其发送邮件的电子邮件地址。您还可以添加一个或多个要向其发送邮件副本和副本的电子邮件地址，而不会在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成配置过程。

计划升级自动扩展组

执行以下步骤来升级属于 Autoscale 组的云服务中的所有实例：

1. 在 Citrix ADM 中，导航到 网络 **>** 配置作业 **>** 维护作业。单击 创建作业按钮。
2. 在 创建维护作业页上，选择 升级自动缩放组”，然后单击 继续。
3. 在 升级设置选项卡中：
   a) 选择要升级的 自动缩放组。
   b) 在 映像” 中，选择 Citrix ADC 版本。此映像是自动缩放组中 Citrix ADC 实例的现有版本。
   c) 在 **Citrix ADC** 映像中，浏览要升级到的 Citrix ADC 版本文件。

      如果您选中 优雅升级”，则升级任务将等待指定的消耗连接期过期。

d) 单击下一步。

4. 在 计划任务选项卡中：

   a) 从 “执行模式” 列表中选择以下选项之一：

      - 现在：立即启动 Citrix ADC 实例升级。
      - 稍后：以后启动 Citrix ADC 实例升级。

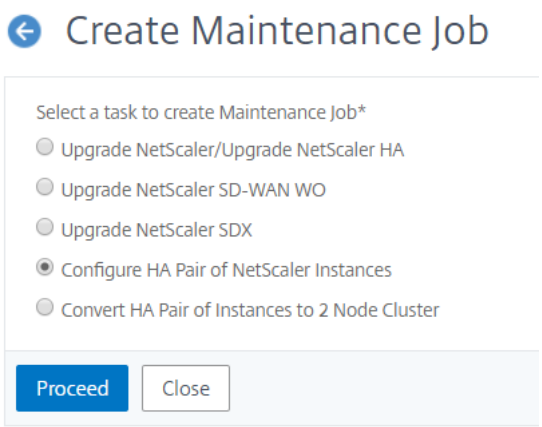
   b) 如果选择 “以 后选项，请在要启动升级任务时选择 “执行日期” 和 “开始时间”。

   您还可以启用电子邮件和松弛通知，以接收升级 Autoscale 组的执行报告。单击 “通 过电子邮件接收执行报告复选框和 “通 过松弛接收执行报告复选框以启用通知。

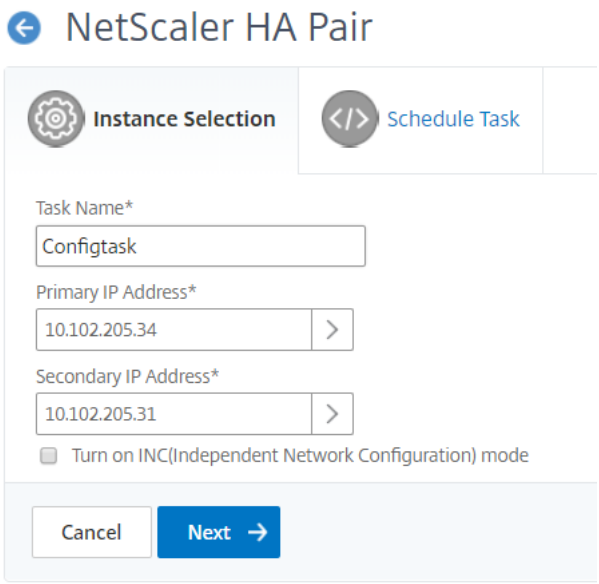
5. 单击完成。

计划配置 **Citrix ADC** 实例的高可用性对

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业” > “ 维护作业”。单击 “ 创建作业” 按钮。
2. 在 “ 创建维护作业” 页上，选择 “ 配置 **Citrix ADC** 实例的高可用性对”，然后单击 “ 继续”。



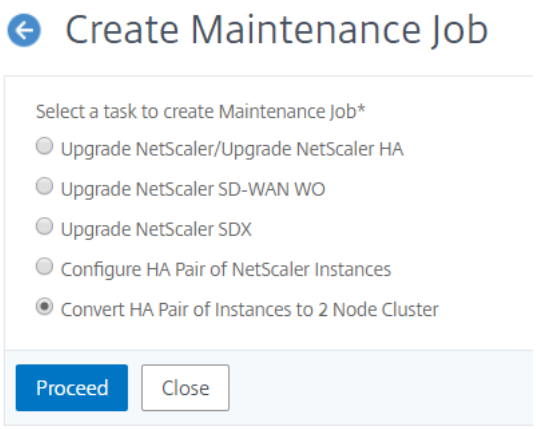
3. 在 **Citrix ADC HA** 对页面上的 “ 实例选择” 选项卡中，添加 任务名称。输入主 IP 地址和辅助地址，然后单击下一步。



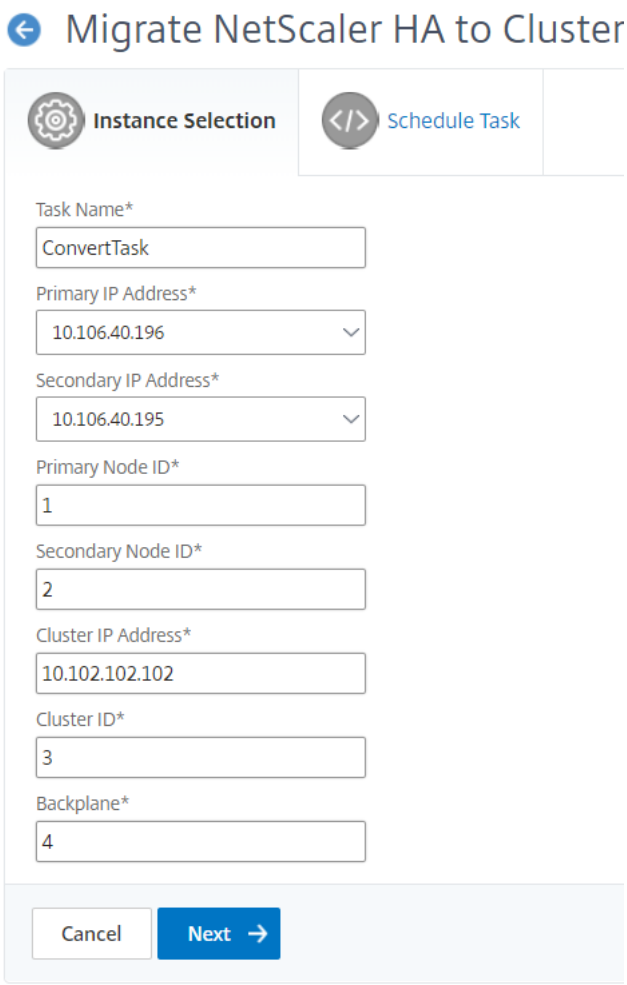
4. 在“计 划任务” 选项卡上，您可以选择现在或稍后配置 Citrix ADC HA 对。
5. 要立即配置 Citrix ADC HA 对，请从 “ 执行模式” 列表中选择 “ 立即”。您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击 “通 过电子邮件接收执行报告” 复选框以启用电子邮件通知。
6. 要以后配置 Citrix ADC HA 对，请从 “ 执行模式” 列表中选择 “ 稍后”。然后，您可以选择电子执行日期和开始时间。您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击 “通 过电子邮件接收执行报告” 复选框以启用电子邮件通知。
7. 选择 **+** 图标以创建电子邮件通讯组列表。
8. 在 “ 创建电子邮件通讯组列表” 页上，指定电子邮件通讯组列表的 名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在 **“**发件人**”** 框中，添加要从中发送邮件的电子邮件地址。在 “收件 人” 框中，添加要向其发送邮件的电子邮件地址。您还可以添加一个或多个要向其发送邮件副本和副本的电子邮件地址，而不会在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成配置过程。

计划将 **HA** 实例对转换为群集

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置作业” > “ 维护作业”。单击 “ 创建作业” 按钮。
2. 在 “ 创建维护作业” 页上，选择 “ 将 **HA** 实例对转换为 **2** 节点集群”，然后单击 “ 继续”。



3. 在“将 **Citrix ADC HA** 迁移到集群”页上的“ 实例选择**”** 选项卡中，添加 任务名称。指定主 IP 地址、辅助地址、主节点 ID、辅助节点 ID、群集 IP 地址、群集 ID 和底板。单击“ 下一步”。



4. 在“计 划任务”选项卡上，您可以选择立即或稍后将 Citrix ADC HA 迁移到群集。
5. 要以后配置 Citrix ADC HA 对，请从“ 执行模式”列表中选择“ 稍后”。然后，您可以选择执行日期和开始时间。

您可以启用电子邮件通知，以接收 Citrix ADC HA 对的执行报告。单击“通 过电子邮件接收执行报告”复选框以启用电子邮件通知。

6. 选择 **+** 图标以创建电子邮件通讯组列表。
7. 在“ 创建电子邮件通讯组列表”页上，指定电子邮件通讯组列表的名称。添加用于向电子邮件服务器发送电子邮件通知的 SMTP 邮件服务器。在**“**发件人**”**框中，添加要从中发送邮件的电子邮件地址。在“收件 人”框中，添加要向其发送邮件的电子邮件地址。您还可以添加一个或多个要向其发送邮件副本和副本的电子邮件地址，而不会在邮件或副本中显示这些地址。单击创建。创建电子邮件通讯组列表后，单击 完成以完成配置过程。

配置审核

April 23, 2021

本文档包括：

- 创建审计模板
- 查看审计报告
- 审核实例上的配置更改
- 获取有关网络配置的配置建议
- 如何轮询 Citrix ADC 实例的配置审核

创建审计模板

April 23, 2021

您希望确保某些配置运行在特定实例上以获得网络的最佳性能。您还希望监视跨托管 Citrix 应用程序 Delivery Controller (ADC) 实例的配置更改，排除配置错误，并在系统突然关闭后恢复未保存的配置。您可以使用要在某些实例上审核的特定配置创建审核模板。Citrix Application Delivery Management (Citrix ADM) 会将这些实例与审计模板进行比较，并报告配置中存在不匹配的情况。每当出现配置不匹配时，Citrix ADM 都会生成配置差异报告，使您能够进行故障排除和纠正不需要的配置更改。

您可以通过以下方式自动运行审核模板：

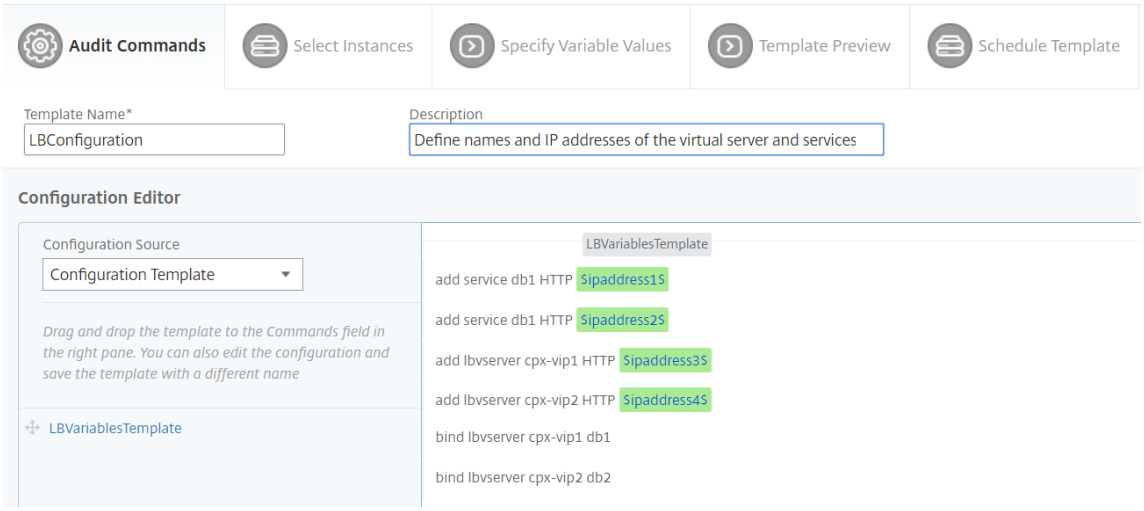
- 安排模板必须运行的时间
- 设置 Citrix ADM 必须运行模板的频率。您可以每天、在一周中的特定日期或在一个月中的特定日期运行模板。

此外，您还可以选择将 Citrix ADM 生成的差异报告发送到可以配置的指定电子邮件地址。通过此选项，您的用户可以将报告作为邮件附件接收，并且用户无需登录到 Citrix ADM 即可手动导出报告。

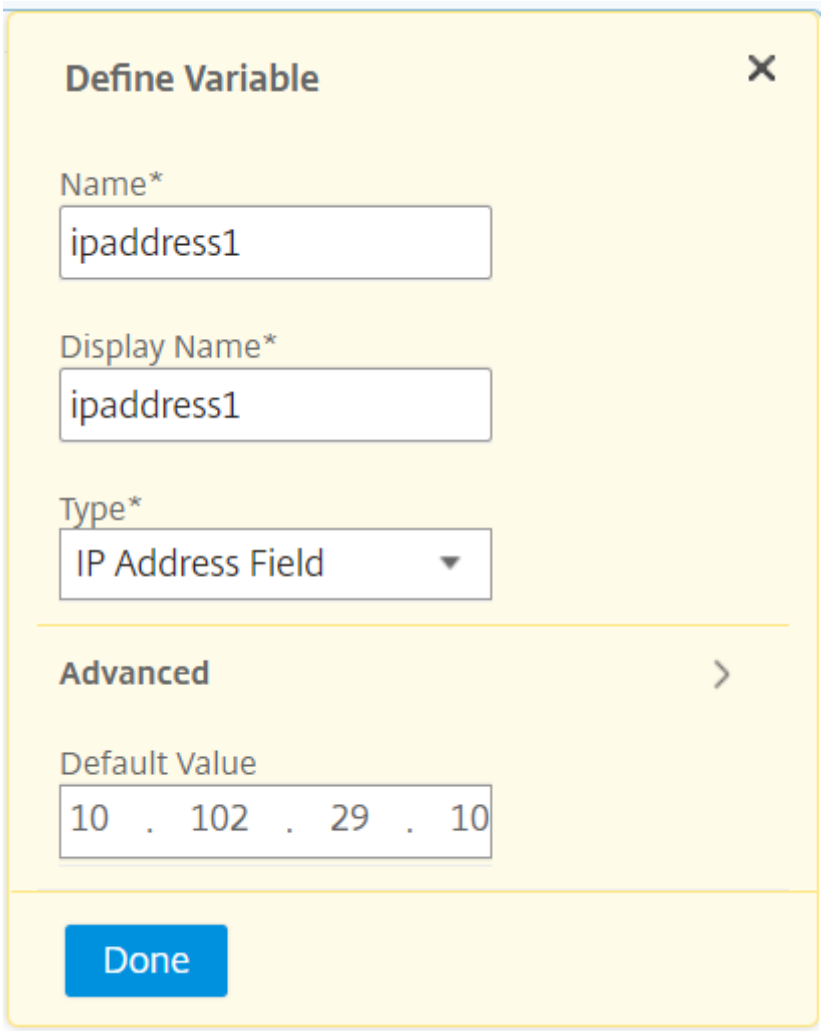
> 注意：
>
> 对于默认配置模板，“ 重命名” 选项处于禁用状态。但是，您可以重命名自定义配置模板。

要创建审计模板，请执行以下操作：

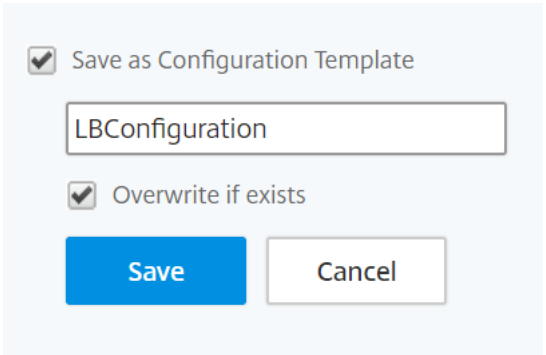
1. 导航到 “网络” > “配置审计” > “审计模板”，然后单击 “添加”。
2. 在 “创建模板” 页和 “审计命令” 选项卡中，指定模板名称及其说明。
3. 在 配置编辑器页面中，键入命令并将命令另存为配置模板。您也可以将现有模板从左窗格拖动到编辑器。
4. 选择要转换为变量的值，然后单击转换为变量。例如，选择负载平衡服务器 “ip 地址 1” 的 IP 地址，然后单击 “转换为变量”。该变量现在用 “$” 括起来，如下图所示。



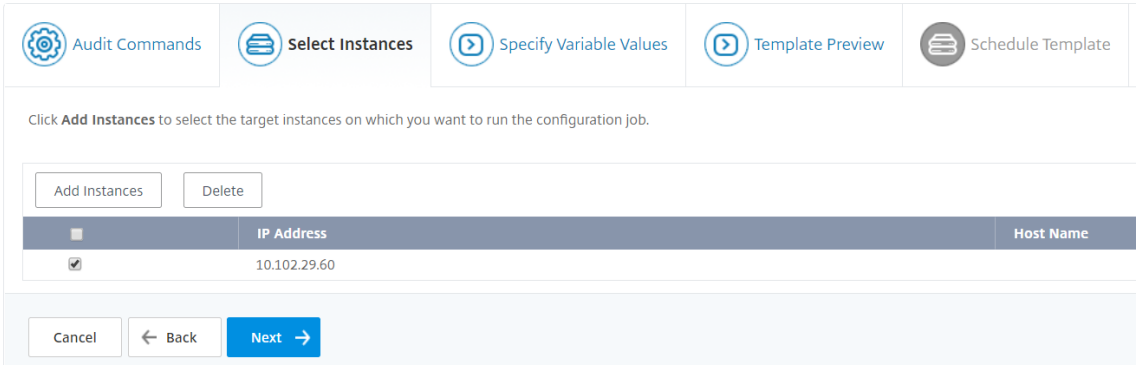
在 “定 义变量窗口中，设置此变量的属性-名称、显示名称和变量的类型。如果要进一步指定变量的默认值，请单击 “高级” 选项。



您还可以将命令另存为配置模板。



5. 单击保存，然后单击下一步。
6. 在 “ 选择实例” 选项卡中，选择要对其运行配置审核的实例，然后单击 “ 下一步”。

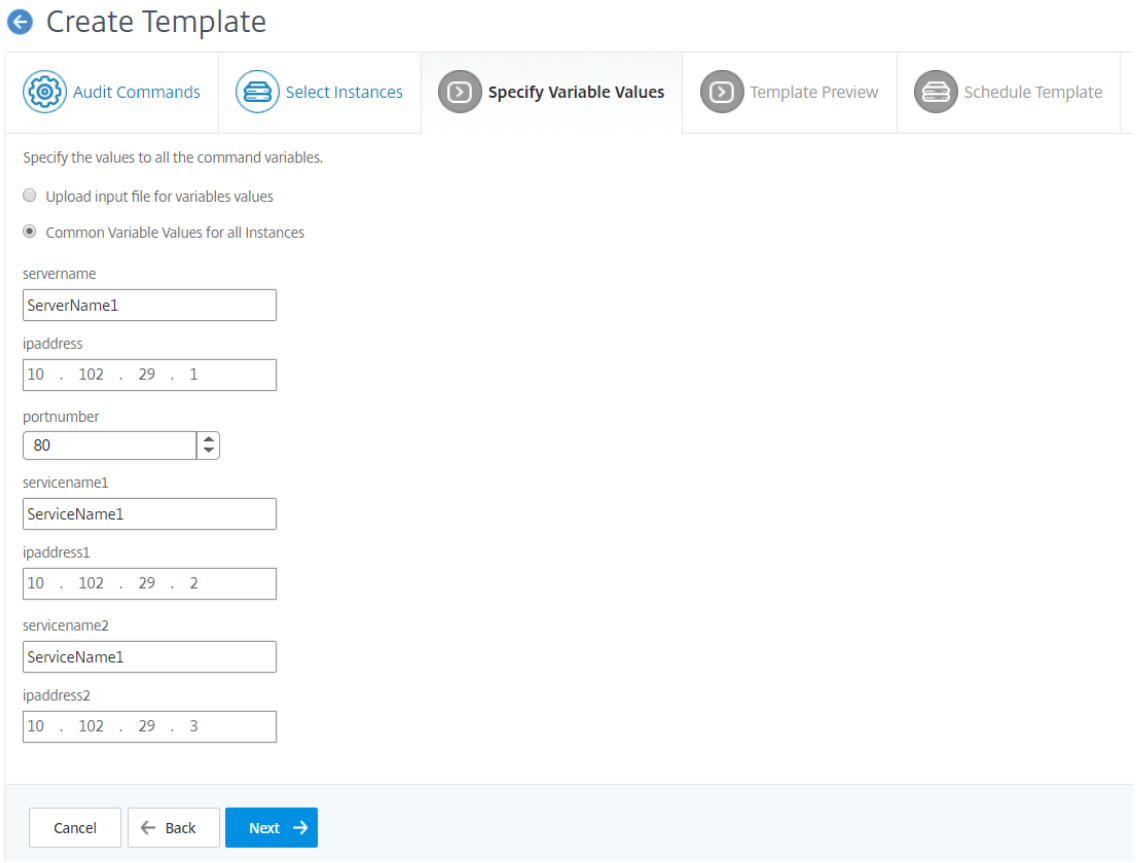


7. 在“指定变量值”选项卡中，有两个选项：

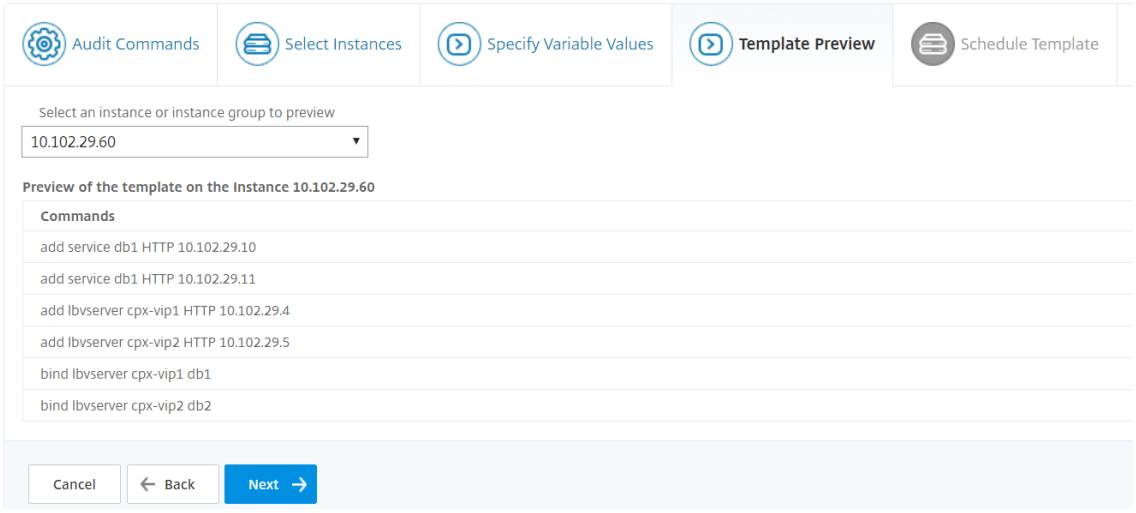
   a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器

   b) 输入已为所有实例定义的变量的公用值

8. 单击下一步。



9. 在“ 模板预览”选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令。单击下一步。



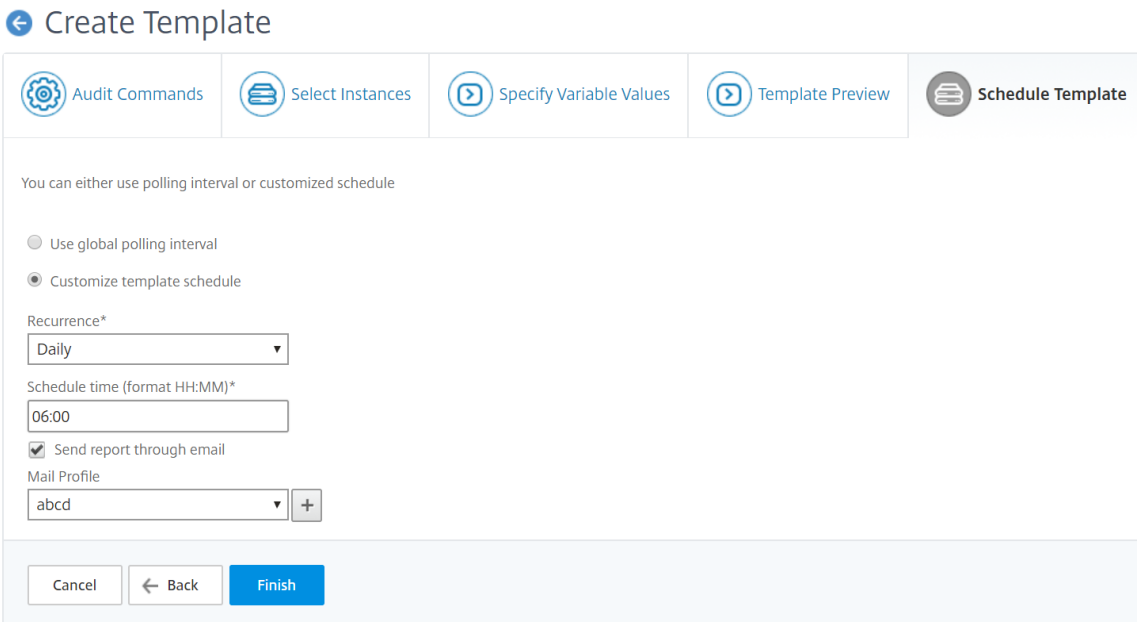
10. 在“计 划模板选项卡中，您有以下选项来计划模板的运行并配置邮件地址以发送差异报告。

    - 使用全局轮询间隔。选择此选项可在 Citrix ADM 上全局配置的时间在实例上运行模板。

      > 注意
      >
      > 要在 Citrix ADM 中配置全局轮询间隔，请导航到 网络”> 配置审核”**>**“审核模板”，然后单击全局轮询间隔”。在轮询间隔字段中，输入 Citrix ADM 必须全局轮询实例的分钟数。

    - 自定义模板计划。使用此选项可配置需要运行模板的时间和频率
    - 通过电子邮件发送报告。使用此选项可以配置必须将差异报告作为邮件附件发送到的邮件配置文件。

11. 单击完成。



审计模板将显示在“ 审计模板”列表中，并在计划的时间针对指定实例中的配置运行。

查看审计报告

April 23, 2021

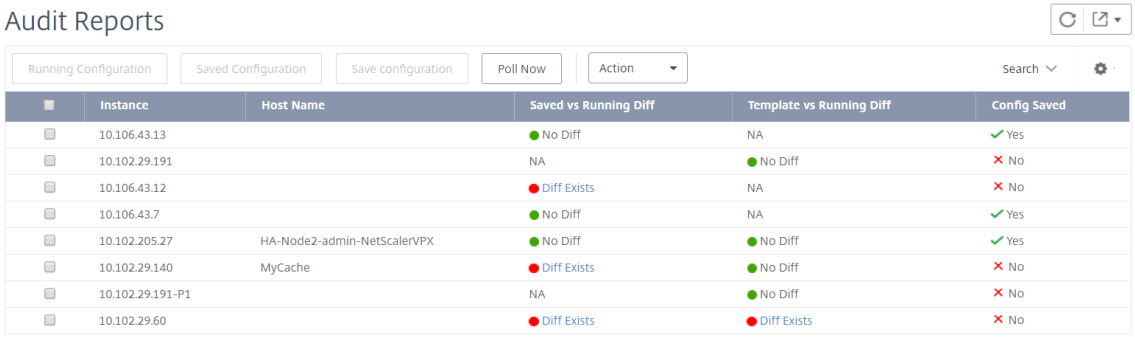
Citrix Application Delivery Management (Citrix ADM) 允许您在配置审核部分查看和下载配置审核差异报告。使用配置审核部分，您可以在所有实例和每个实例中导出摘要报告，还允许您为每个实例-模板对导出粒度差异报告。

“审计模板”列表中显示的审计模板将在计划时间针对指定实例中的配置运行。“ 配置审核”仪表板上的 **“NetScaler** 配置漂移”图表显示了针对未保存配置保存的配置更改的高级别详细信息。单击 **NetScaler** 配置漂移图表时，随后的“审计报告”页将显示一个实例列表，其中显示“差异存在”和“无差异”。“ 您可以下载 Citrix ADM 显示的差异报告。

Citrix ADM 还提供了一个选项，用于计划将差异报告自动导出为邮件附件。有关如何计划导出报告的详细信息，请参阅创建审计模板。

要导出配置审核报告，请执行以下操作：

1. 在 Citrix ADM 中，导航到“ 网络”>“ 配置审核”。
2. 在“ 配置审核”页上，单击 **NetScaler** 配置漂移图表内部的。
3. “ 审核报告页面列出了具有差异的实例。此页面还显示其运行配置没有任何区别的实例列表。

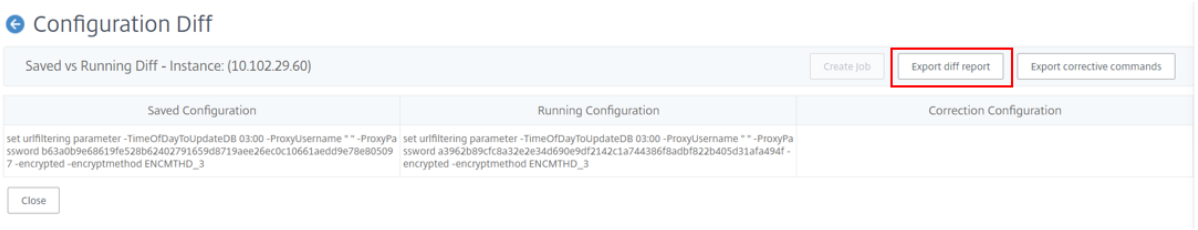


在图像中，您可以看到对于某些实例，差异仅存在于“ 保存与运行比较”中，对于某些实例，差异仅存在于“ 模板与运行比较”中。对于某些情况下，保存与运行差异和 模板与运行差异都存在差异。

已保存与正在运行的比较

您可以查看实例上保存的配置与该实例上当前运行的配置之间的差异报告。例如，单击“ 已保存与运行差异”下的实例的差异存在。

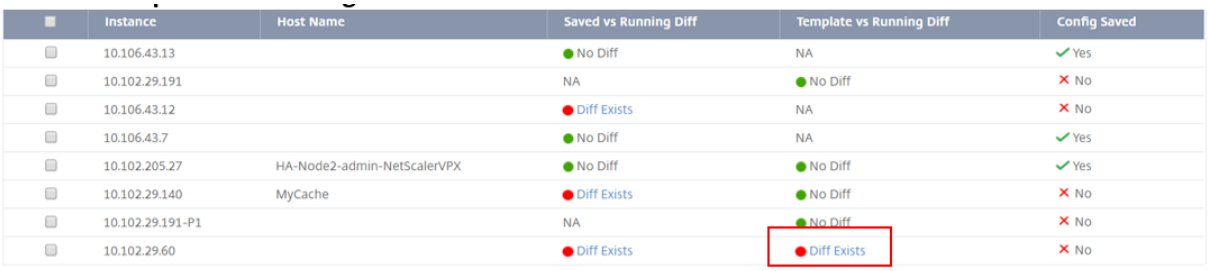
在这里，您可以看到针对该实例运行配置差异的已保存配置的报告。



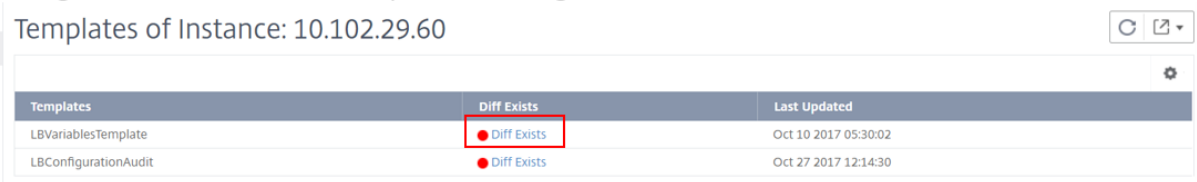
单击 导出差异报告可下载差异报告的.csv 文件。也可以单击 “ 导出更正命令” 将命令导出到.txt 文件。然后，您可以从配置作业对关联的 Citrix ADM 实例运行命令，以更正该实例中的配置。

模板与运行比较

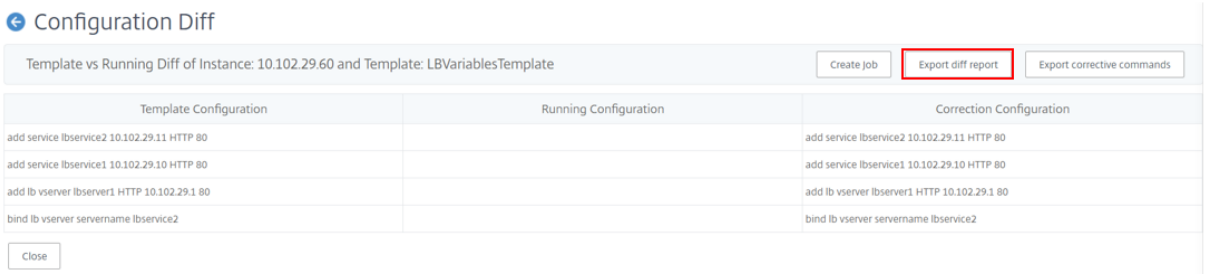
“ 模板与运行比较” 包括所有模板，而 “ 保存与运行比较” 是默认模板。您可以查看模板和运行配置之间存在的差异。例如，单击 “ 模板与运行比较” 下的其中一个实例的比较存在。



现在，您可以看到两个模板显示差异，Citrix ADM 实例的配置与模板正在查找的配置不同。



再次单击 “比较存在”。下图显示了模板要查找的配置以及空白的运行配置，因为尚未配置或删除此类命令。您还可以查看更正配置或要运行的命令来更正配置。

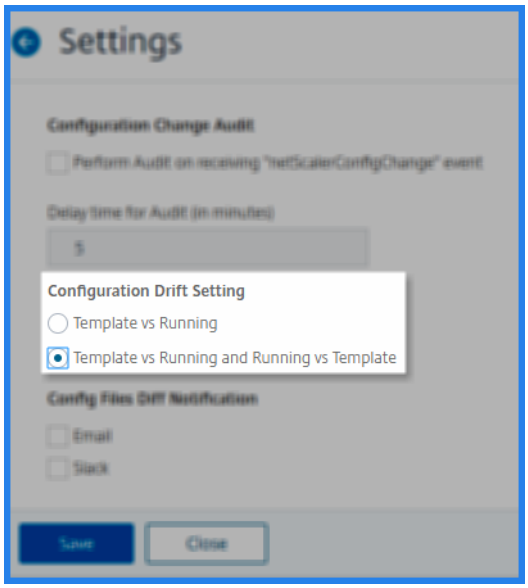


您还可以使用 “模板” 与 “运行” 和 “运行” 与 “模板漂移” 设置，以两种方式比较配置：

- 将审计模板配置与实例上的运行配置进行比较。

- 将实例上的运行配置与审计模板进行比较。

默认情况下，“模板与运行漂移”设置处于选中状态。要修改漂移 设置，请从 ADM GUI 中选择“ 配置审计”页中的“设置”。



单击 导出差异报告可下载差异报告的.csv 文件。也可以单击“ 导出更正命令”将命令导出到.txt 文件。然后，您可以在 CLI 中运行命令以更正该实例中的配置。

下图显示了下载到系统的.csv diff 示例文件：

#Template vs Running Diff of Instance: 10.102.29.60 and Template: LBVariablesTemplate		
Template Configuration	Running Configuration	Correction Configuration
add service lbservice2 10.102.29.11 HTTP 80		add service lbservice2 10.102.29.11 HTTP 80
add service lbservice1 10.102.29.10 HTTP 80		add service lbservice1 10.102.29.10 HTTP 80
add lb vserver lbserver1 HTTP 10.102.29.1 80		add lb vserver lbserver1 HTTP 10.102.29.1 80
bind lb vserver servername lbservice2		bind lb vserver servername lbservice2

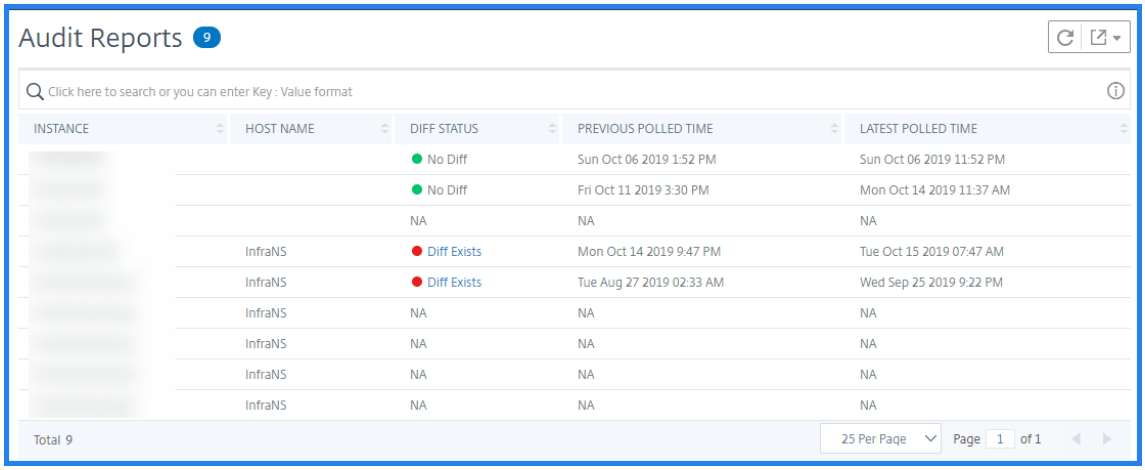
查看文件状态审核报告

使用 **Citrix ADC** 文件状态图表，您可以监控 `nsconfig` 文件夹中是否添加、修改或删除了任何文件。例如：如果在 ADC 实例上更新了许可证文件，您可以检查上次更新此文件的时间并采取相应的措施。

要导出 Citrix ADC 实例的文件状态审核报告，请执行以下操作：

1. 在 Citrix ADM 中，导航到“ 网络”>“ 配置审核”。
2. 在 配置审核页面上，单击 **Citrix ADC** 文件状态图表。

   “ 审核报告页面列出了具有差异状态的实例。



比 较状态是根据 上一轮询时间到最近轮询时间之间的时间间隔计算的。“ 比较状态” 可以是以下选项之一：

- 比较存在-此状态表示自上一轮询时间以来，实例文件 nsconfig夹中的文件发生了更改。要查看文件上已更改的内容，请单击 “ 比较存在”。

  ![nsconfig 文件夹中存在差异](/en-us/citrix-application-delivery-management-software/media/config-audit-file-status-diff.png)

- 无比较 -此状态表示文件 nsconfig 夹中的文件自上次轮询时间以来没有更改。
- **NA** -此状态表示监视文件状态不适用。当 Citrix ADM 不轮询实例时，会显示此状态。例如，当新添加实例或实例状态处于非活动状态时，实例不会进行轮询。

跨实例审核配置更改

April 23, 2021

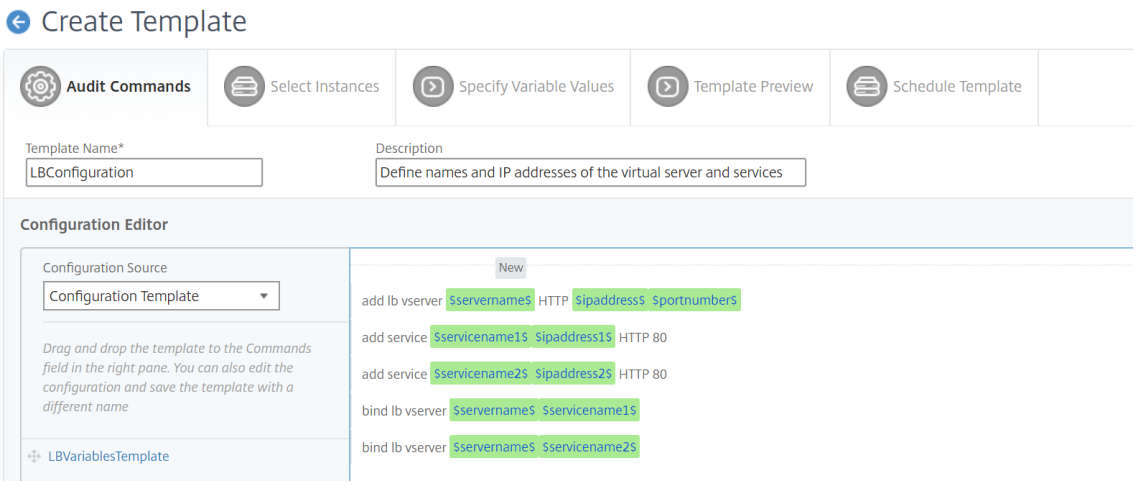
您希望确保某些配置运行在特定实例上以获得网络的最佳性能。您还希望监视跨托管 Citrix 应用程序 Delivery Controller (ADC) 实例的配置更改，排除配置错误，并在系统突然关闭后恢复未保存的配置。您可以使用要在某些实例上运行的特定配置创建审计模板。Citrix Application Delivery Management (Citrix ADM) 将这些实例与审核模板进行比较，并报告配置中存在不匹配的情况。这样，就可以对错误进行故障排除并纠正。

您可以通过安排模板必须运行的时间来自动运行审计模板。您还可以设置 Citrix ADM 必须运行模板的频率。您可以每天、在一周中的特定日期或在一个月中的特定日期运行模板。您还可以选择将 Citrix ADM 生成的差异报告发送到可以配置的指定电子邮件地址。通过此选项，您的用户将以邮件附件形式收到报告，并且用户无需登录到 Citrix ADM 手动检查报告。

要创建审计模板，请执行以下操作：

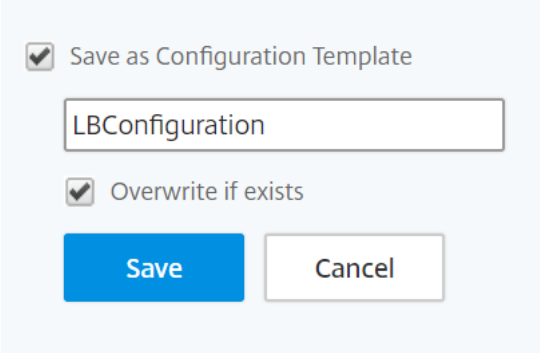
1. 导航到网络 **>** 配置审核 **>** 审计模板，然后单击添加。
2. 在 “创建模板” 页和 “审计命令” 选项卡中，指定模板名称及其说明。

3. 在 配置编辑器中，键入命令并将命令另存为配置模板。您还可以从编辑器的左侧窗格中拖动现有模板。
4. 选择要转换为变量的值，然后单击转换为变量。例如，选择负载平衡服务器的 IP 地址 `ipaddress`，然后单击转换为变量，如下图所示。

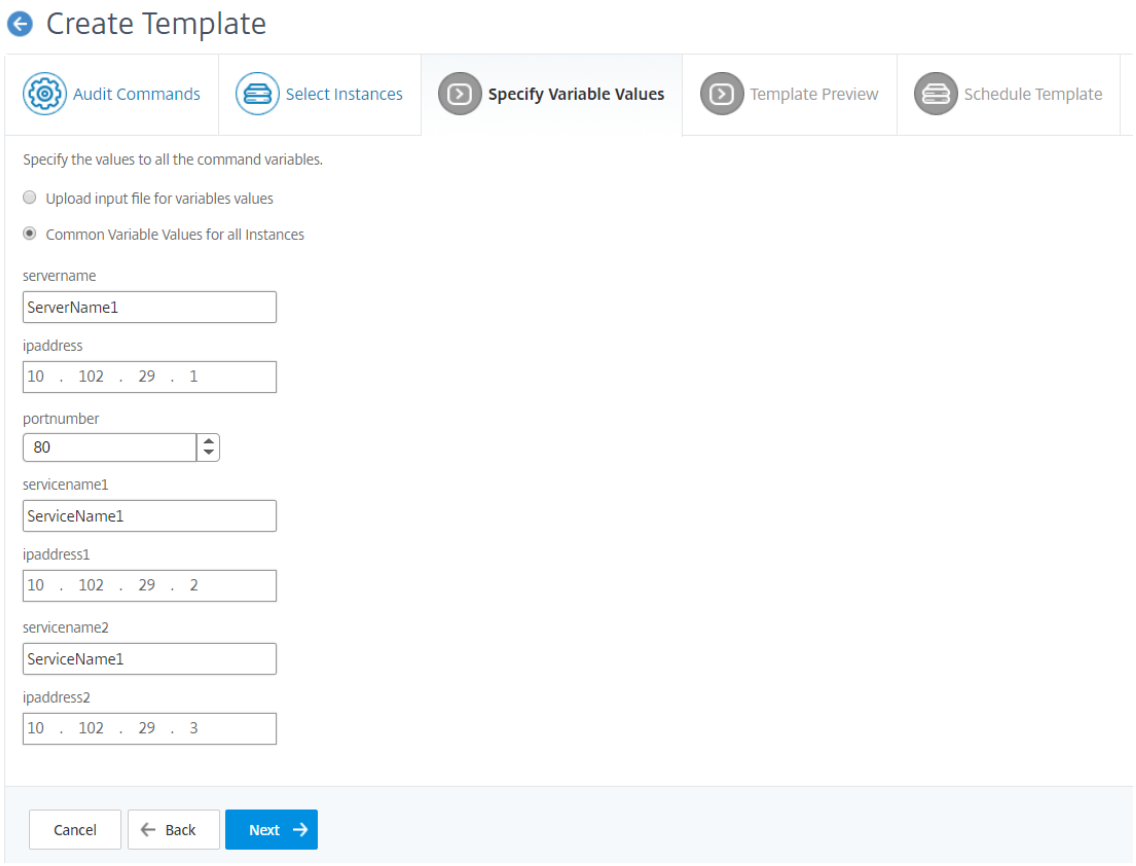


如果要进一步指定变量的默认值，请单击“高级”选项。

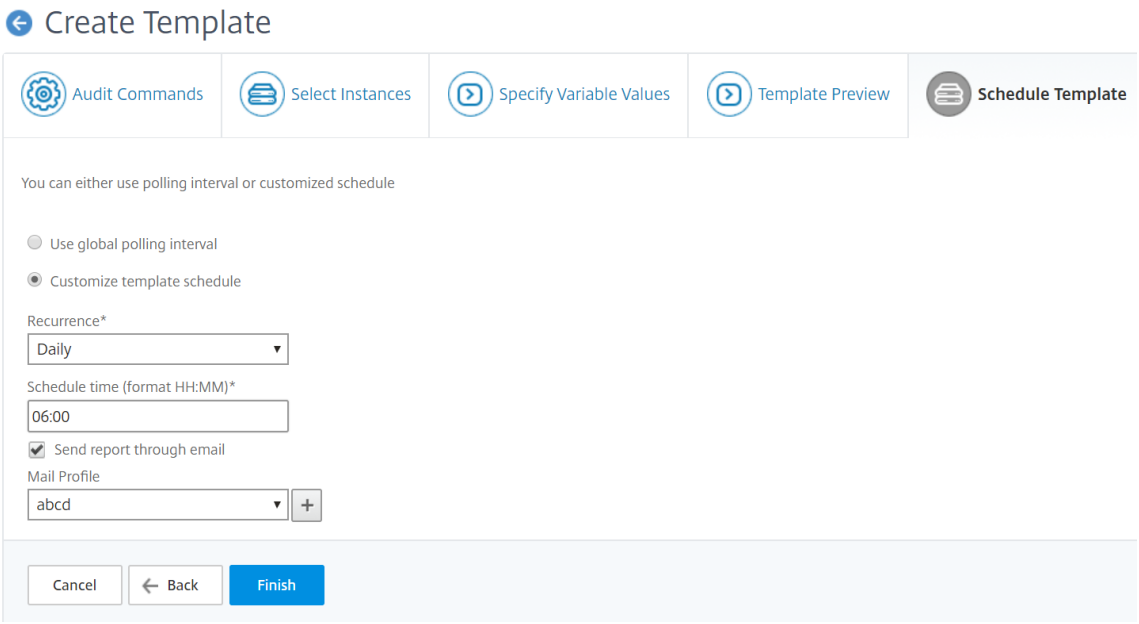
您还可以将命令另存为配置模板。



5. 单击保存，然后单击下一步。
6. 在选 择实例选项卡中，选择要在其上运行配置审核的实例。
7. 在“指定变量值”选项卡中，有两个选项：
   a) 下载输入文件以输入您在命令中定义的变量的值，然后将文件上载到 Citrix ADM 服务器
   b) 输入已为所有实例定义的变量的公用值
8. 单击下一步。



9. 在“ 模板预览” 选项卡中，您可以评估和验证要在每个实例或实例组上运行的命令。单击下一步。
10. 在“计 划模板选项卡中，您有三个选项可以自动运行模板和邮件地址以发送差异报告。
    - 使用全局轮询间隔。选择此选项可在 Citrix ADM 上全局配置的时间在实例上运行模板
    - 自定义模板计划。使用此选项可配置需要运行模板的时间和频率
    - 通过电子邮件发送报告。使用此选项可以配置必须将差异报告作为邮件附件发送到的邮件配置文件。
11. 单击完成。

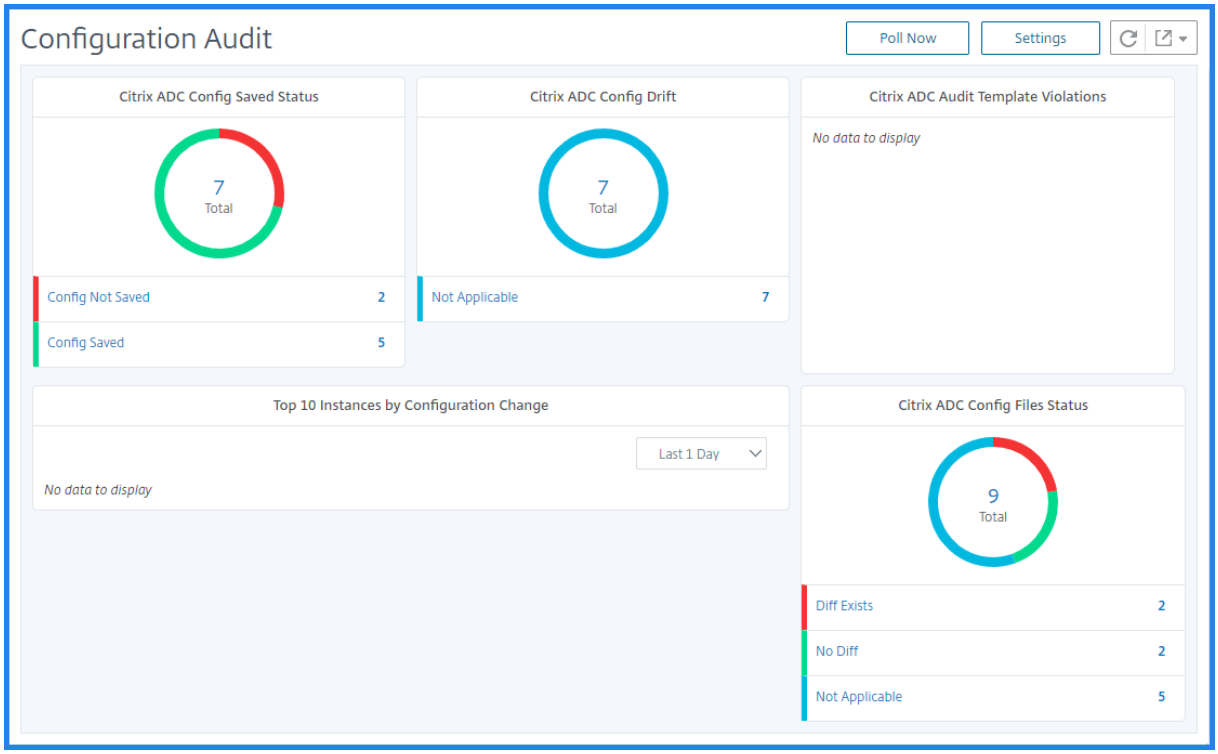


审核模板将显示在审核模板列表中，并在计划时间针对指定实例中的配置运行。

查看配置更改的详细信息

您还可以使用“配置审核”控制板查看有关配置更改的高级别详细信息，例如：

- 按配置更改排列的前十个实例
- 已保存和未保存的配置数
- 在文件 `nsconfig` 夹中添加、删除或修改的文件

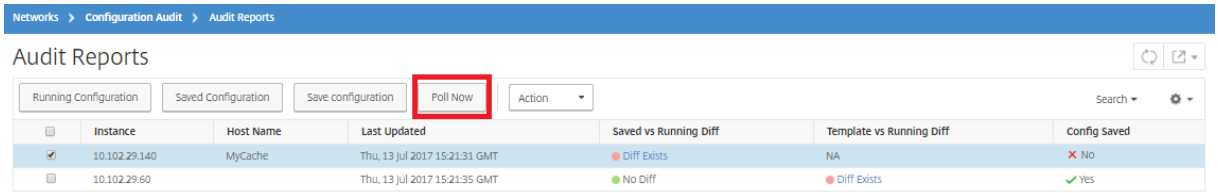


Citrix ADM 还允许您手动轮询配置审核，并立即将实例的所有配置审核添加到 Citrix ADM 中。为此，请导航到 “ 网络” > “配置审核”，单击 “立 即轮询”，弹出式页面 “立 即轮询” 将为您提供轮询网络中的所有 Citrix ADC 实例的选项，或轮询所选实例。

还可以对实例强制执行审核。要执行此操作，请单击以下任一图表：

- **Citrix ADC** 配置已保存状态
- **Citrix ADC** 配置漂移

在 审核报告页面上，选择实例，然后在 操作” 列表中选择 立即轮询。



Citrix ADC 配置文件状态图表提供文件 `nsconfig` 夹中存在的 Citrix ADC 文件的状态。Citrix ADM 记录和比较文件 `nsconfig` 夹内文件中的更改，并显示差异。请参阅查看文件状态审核报告。

设置配置审核通知

1. 导航至 “ 网络” > “ 配置审核”。
2. 在 配置审核页上，单击 设置。
3. 在 **Notification Settings**（通知设置）页面上，单击 **Edit**（编辑）图标以启用通知设置。

4. 选中 **Enabled**（已启用）复选框，然后从下拉列表中选择电子邮件通讯组列表。还可以单击 **+** 图标并指定电子邮件服务器详细信息来创建电子邮件通讯组列表。

获取有关网络配置的配置建议

April 23, 2021

您可以使用最佳配置设置 Citrix 应用程序 Delivery Controller (ADC) 实例，以便在应用程序上实现最佳性能。但是，某些配置可能不是标准配置，这可能会影响应用程序的性能。

为了帮助您优化应用程序性能，Citrix Application Delivery Management (Citrix ADM) 会分析 Citrix ADC 实例配置并为您提供建议。您可以应用 Citrix ADM 中的推荐配置。

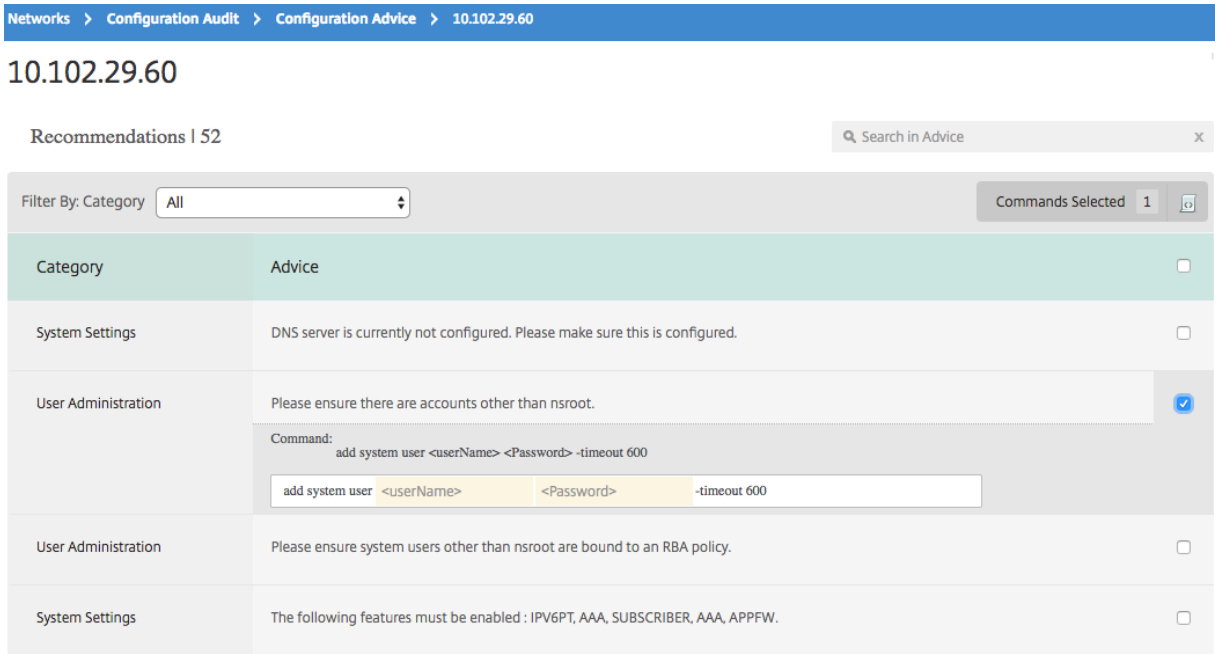
要分析 **Citrix ADC** 实例，请执行以下操作：

1. 导航至 “ 网络” > “ 配置审计” > “ 配置建议”。
2. 执行以下操作之一：

   - 单击 **Upload Configuration File**（上载配置文件）并上载网络实例的配置文件。

   -单击 “ 选择设备”，然后选择要分析的 Citrix ADC 实例。

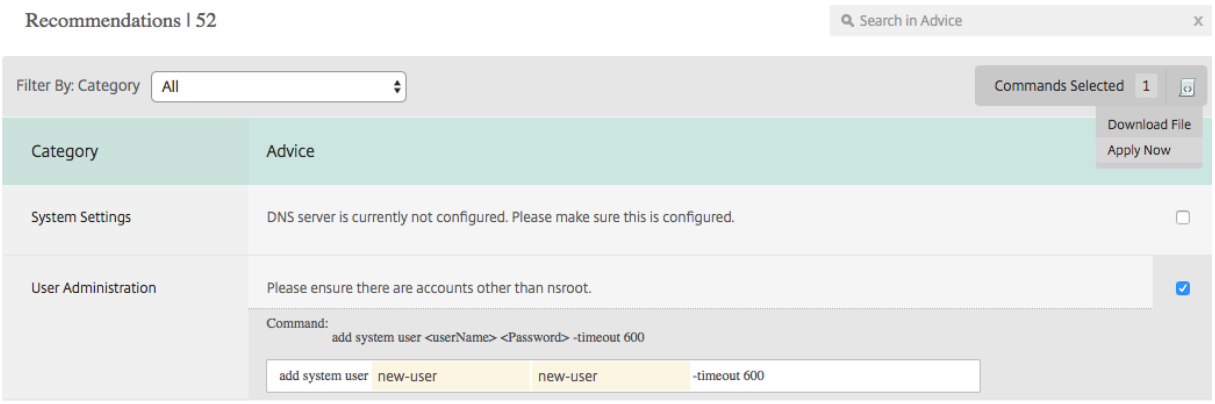
Citrix ADM 将分析实例上的配置，并提供配置建议的列表，如下图所示。单击配置建议旁边的复选框可以查看更正命令。



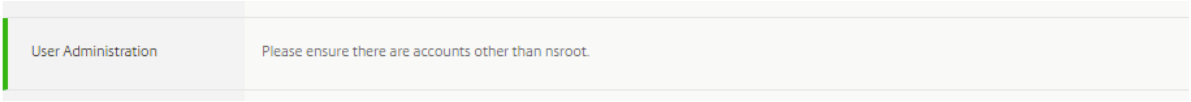
如果要更新配置，请在纠正命令中指定变量的值，然后单击 立即应用，如下图所示。

> 注意此处列出
>
> 的命令只是建议。具有读写权限的用户或许能够使用此功能编辑任何命令。确保向您认为不能编辑命令的用户授予有限的特权访问权限。

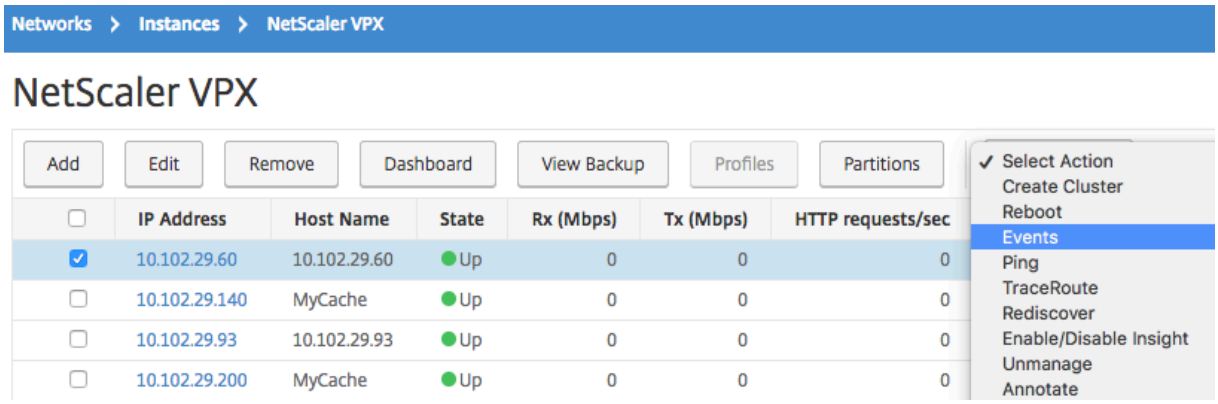
10.102.29.60



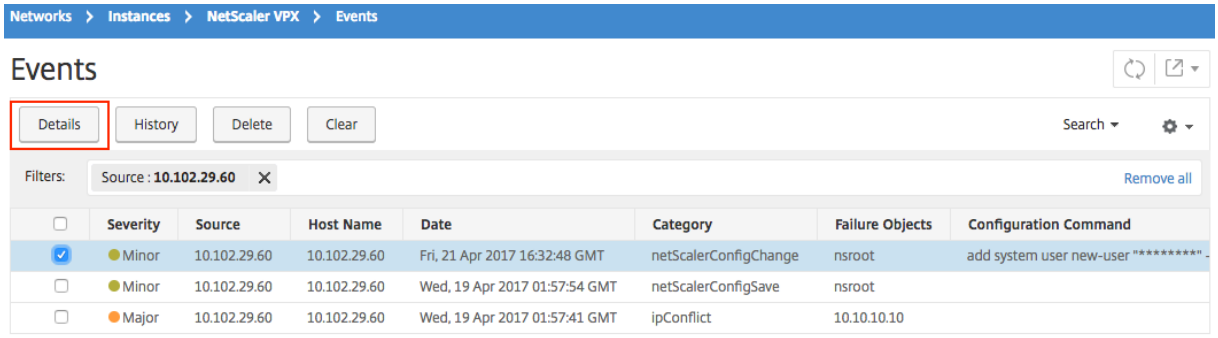
在网络实例上成功运行了命令后，建议旁边的复选框会消失。



如果要查看在网络实例上运行的命令的详细信息，请导航到网络 **>** 实例 **>** **<Instance_Type\>**，选择实例的 IP 地址，然后单击 操作下拉列表中的 事件。



在“事 件页面上，您可以查看配置更改的详细信息。



对 **Citrix ADC** 实例的轮询配置审核

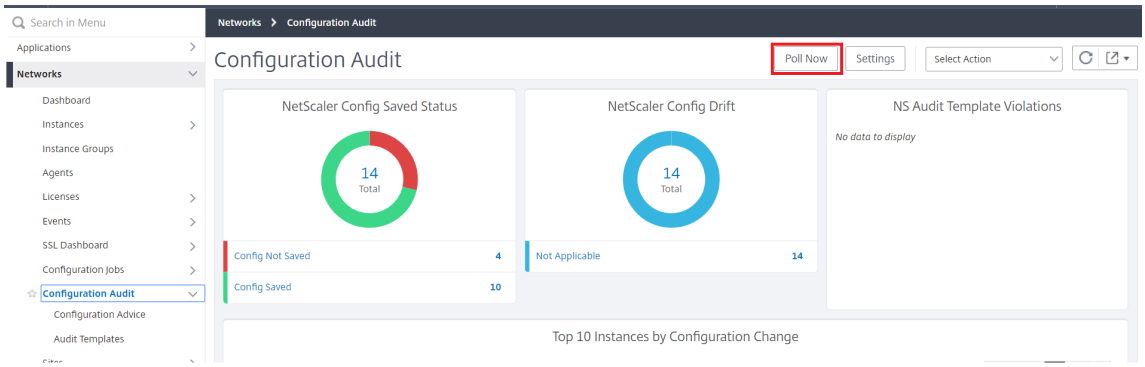
April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 每 10 小时自动轮询一次配置审核，以查找在 Citrix 应用程序 Delivery Controller (ADC) 实例上发生的配置更改。您还可以手动轮询配置审核以发现最近的更改，但轮询所有 Citrix ADC 实例配置会给网络带来沉重负载。

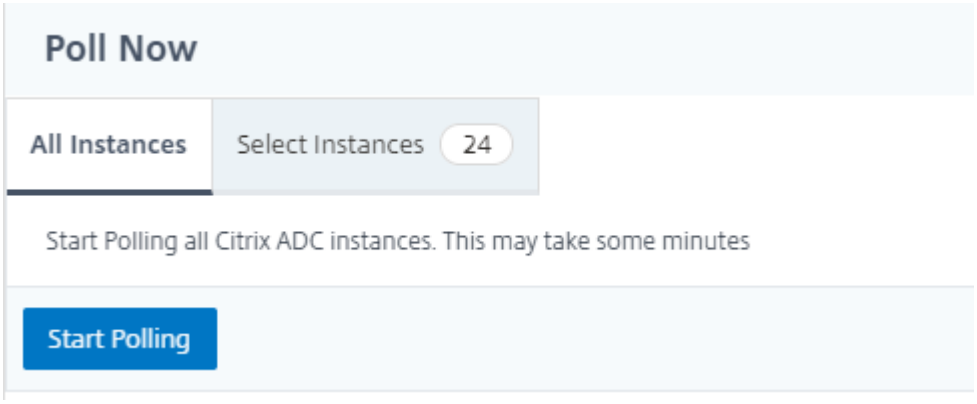
您可以只手动轮询一个或多个选定实例的配置审核，而不是轮询整个 Citrix ADC 实例配置审核。

要轮询 **Citrix ADC** 实例的配置审核，请执行以下操作：

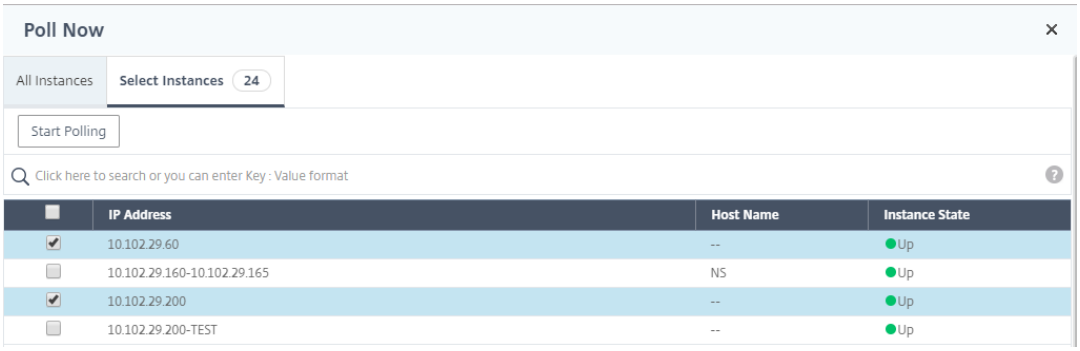
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置审核”。
2. 在 配置审核页上的右上角，单击 立即轮询。



3. 此时会弹出 “立 即轮询页面，您可以选择轮询网络中的所有 Citrix ADC 实例或轮询选定实例。
   a) 要轮询所有 Citrix ADC 实例，请选择 所有实例选项卡，然后单击 开始轮询。



b) 要轮询特定实例，请选择 选择实例选项卡，从列表中选择实例，然后单击立即轮询。



为 **ConfigChange SNMP** 陷阱生成配置审核差异

April 23, 2021

每当网络中的 Citrix 应用程序 Delivery Controller (ADC) 实例中的配置发生更改时，配置文件都会更新。实例会将配置更改 SNMP 陷阱发送到 Citrix Application Delivery Management (Citrix ADM)。当实例发送 ConfigChange SNMP 陷阱时，您可以启用 Citrix ADM 对该实例执行配置审核。

如果审核模板配置和正在运行的配置之间存在任何差异，则审核报告页面上将显示“差异存在状态消息。单击差异退出链接将转到配置差异页面，您可以在其中查看纠正命令。您可以使用这些纠正命令创建配置作业并在特定 Citrix ADC 实例上运行配置作业。运行配置作业时，实例将返回到所需的配置。有关如何通过更正命令创建配置作业的详细信息，请参阅 如何从 Citrix ADM 上的更正命令创建配置作业。

要在接收 **ConfigChange SNMP** 陷阱时运行配置审核模板，请执行以下操作：

Citrix ADM 允许您启用在 Citrix ADM 中运行配置审核模板的选项。

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 配置审核”。
2. 单击 “ 配置审计” 页上的 “设置”。
3. 单击 “ 配置更改审计设置” 部分中的编辑图标。

4. 选中接收 **netScalerConfigChange** 事件时执行配置审核复选框。

> 注意
>
> 这是所有实例的全局设置。Citrix ADM 会对将来收到 NetScalerConfig 更改 SNMP 陷阱的每个实例执行配置审核。

1. 在 运行审计模板的时间延迟（以分钟为单位）字段中，键入分钟。Citrix ADM 在此时间延迟之后在 Citrix ADC 实例上运行配置审核模板，当它接收到该实例的 ConfigChange SNMP 陷阱时。

网络功能

April 23, 2021

使用网络功能功能，您可以监视在托管 Citrix 应用程序 Delivery Controller (ADC) 实例上配置的实体的状态。您可以查看统计信息，例如，事务详细信息、连接详细信息以及负载平衡虚拟服务器的吞吐量。您还可以在计划维护时启用或禁用实体。

“Network Functions”（网络功能）控制板为您提供以下图形：

- 客户端连接数最高的前 5 位虚拟服务器
- 服务器连接数最高的前 5 位虚拟服务器
- 吞吐量（MB/秒）最大的前 5 位虚拟服务器
- 吞吐量（MB/秒）最小的前 5 位虚拟服务器
- 虚拟服务器最多的前 5 位实例
- 虚拟服务器的状态
- 负载平衡虚拟服务器的运行状况
- 协议

为负载平衡实体生成报告

April 23, 2021

Citrix Application Delivery Management (ADM) 允许您查看所有级别的 Citrix 应用程序 Delivery Controller (ADC) 实例实体的报告。您可以在 Citrix ADM > 网络功能中下载两种类型的报告-合并报告和单个报告。

合并报告：您可以下载并查看 Citrix ADC 实例上管理的所有实体的合并报告或汇总报告。

通过此报告，您可以从高级视图查看 Citrix ADC 实例、分区和网络中存在的相应负载平衡实体（虚拟服务器、服务组和服务）之间的映射。

下图显示了一个汇总报告示例。

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing				
[redacted]	[redacted]		Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:
[redacted]	[redacted]		Load Balancing	ADM-Test-LB3#10.1.1.3:80			
[redacted]	[redacted]		Load Balancing	334-lb#1.33.2.2:80			
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b1a9-26ca3			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8404-b5b6			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-99e1-6703			33f97d16-0413-4e6e-9f3d-8
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[redacted]	[redacted]	Load Balancing				
[redacted]	[redacted]		Load Balancing				

合并报告的格式为 CSV 格式。每列中的条目说明如下：

- **NetScaler IP** 地址：报告中显示了 Citrix ADC 实例的 IP 地址
- **NetScaler** 主机名：主机名显示在报告中。
- 分区：显示管理分区的 IP 地址
- 虚拟服务器 <name_of_the_virtual_server>: #virtual_IP_address: 端口号
- 服务: <name_of_the_service> #service-IP 地址: 端口 _ 号码
- **Service Groups**: <name_of_service_group>#server_member1_IP_address:port,server_member2_IP_addr

> 注意
>
> - 如果没有主机名，则显示对应的 IP 地址。
> - 空白列表示未为该 Citrix ADC 实例配置相应的实体。

单个报告：您还可以下载和查看所有实例和实体的独立报告。例如，您可以仅下载负载平衡虚拟服务器、负载平衡服务或负载平衡服务组的报告。

Citrix ADM 允许您立即下载报告。您还可以计划在每天、每周或每月的某个固定时间生成报告。

生成组合负载平衡报告

1. 在 Citrix ADM 中，导航到网 络 > 网络功能 > 负载平衡。
2. 在 “ 负载平衡” 页上，单击  。
3. 在打开的 “ 导出” 页面上，您有两个选项可以查看报告：
   a) 选择 “ 立即导出” 选项卡，然后单击 “ 确定”。

      合并报告将下载到您的系统上。

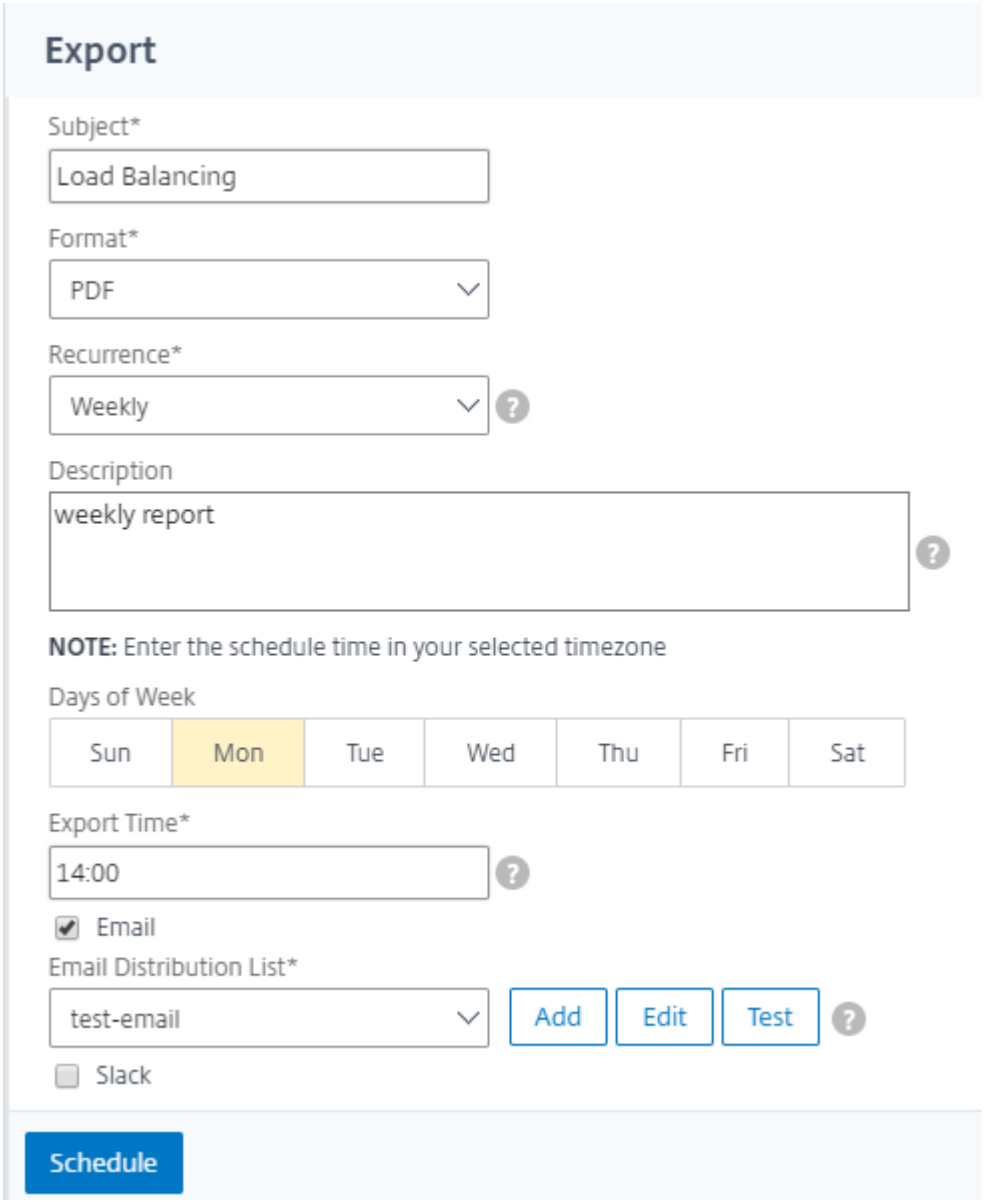
   b) 选择 计划报告选项卡以安排定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

      i. 重复 -从下拉列表框中选择 “ 每日”、“ 每周” 或 “每 月”。

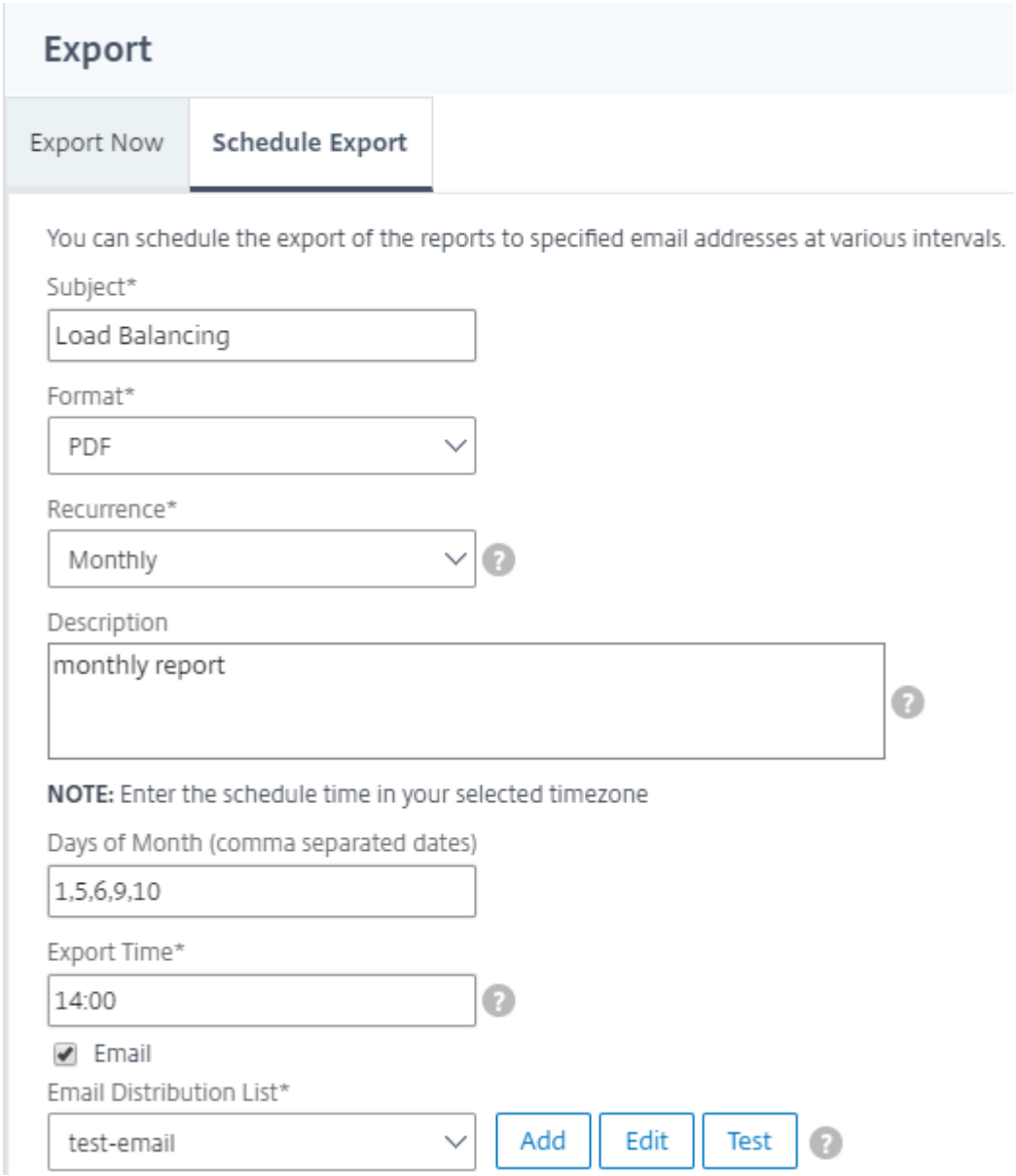
ii. 重复时间 -以 24 小时格式输入时间为小时: 分钟。

iii. 电子邮件配置文件 -从下拉列表框中选择配置文件，或单击 + 创建电子邮件配置文件。

> 注意
>
> 如果您选择 每周定期”，请确保您选择要计划报表的工作日。



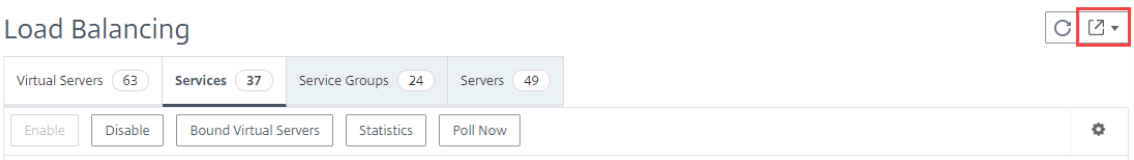
> 注意
>
> 如果选择 每月重复，请确保输入希望报告以逗号分隔的所有日期。



生成单个负载平衡实体报告

您可以为与实例关联的特定类型的实体生成并导出单个报告。例如，假定这样一个场景：您要查看网络中所有负载平衡服务的列表。

1. 在 Citrix ADM 中，导航到网 络 > 网络功能 > 负载平衡 **>** 服务。
2. 在 服务页面上，单击右上角的 导出按钮。



a) 如果要 在此时生成和查看报告，请选择 **“**立即导出” 选项卡。

b) 选择 “ 计划导出” 以计划定期生成和导出报告。

> 注意
>
> 只能以邮件附件形式下载报告或导出报告。您无法在 Citrix ADM GUI 上查看报告。

导出或计划导出网络函数报告

April 23, 2021

您可以为 Citrix Application Delivery Management (ADM) 中的选定网络功能生成综合报告，例如负载平衡、内容交换、缓存重定向、全局服务器负载平衡 (GSLB)、身份验证和 Citrix 网关。此报告允许您从高级视图了解 Citrix ADC 实例、分区和网络中存在的相应绑定实体（虚拟服务器、服务组和服务）之间的映射。您可以以.csv 文件格式导出这些报告。

报告显示以下虚拟服务器数据：

- NetScaler IP 地址
- 主机名
- 分区数据
- 虚拟服务器名称
- 虚拟服务器的类型
- 虚拟服务器
- 目标 LB 虚拟服务器

> 注意：
>
> 对于内容切换和缓存重定向虚拟服务器，目标 LB 虚拟服务器列列列出所有 LB 服务器，即默认服务器和基于策略的服务器。
>
> - 服务名称
> - 服务组名称

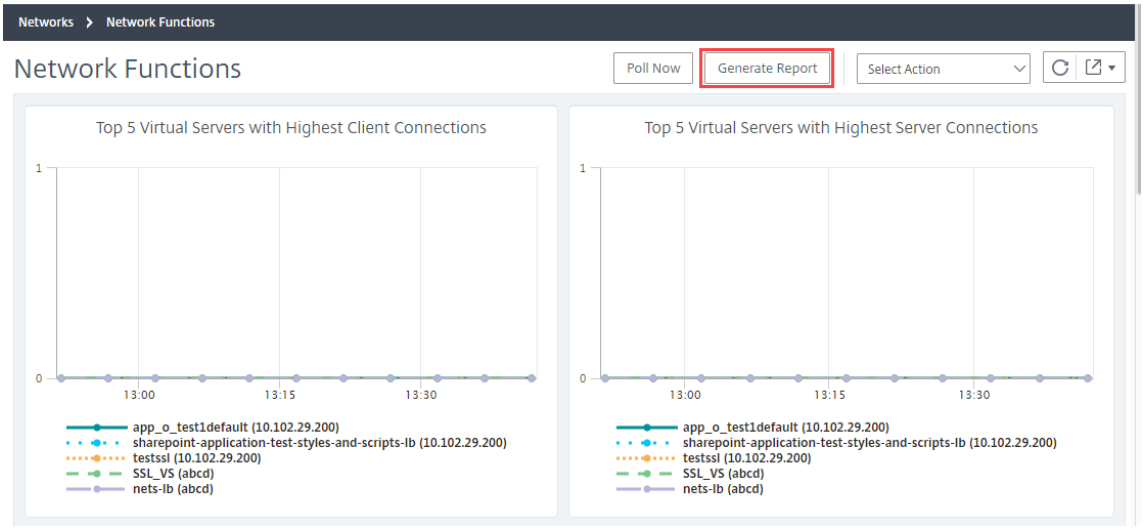
您可以安排以不同的时间间隔将这些报告导出到指定的电子邮件地址。

> 注意
>
> - 对于 GSLB 虚拟服务器，网络功能报告仅显示 GSLB 虚拟服务器和相关服务。
> - 对于内容切换和缓存重定向虚拟服务器，报告仅显示与关联的 LB 服务器的绑定。
> - 此报告中未列出 SSL 虚拟服务器，因为 Citrix ADM 上未维护单独的 SSL 虚拟服务器列表。
> - 当生成新报告时，旧报告将自动从您的帐户中清除。

- 您无法为 HAProxy 生成网络函数报告。

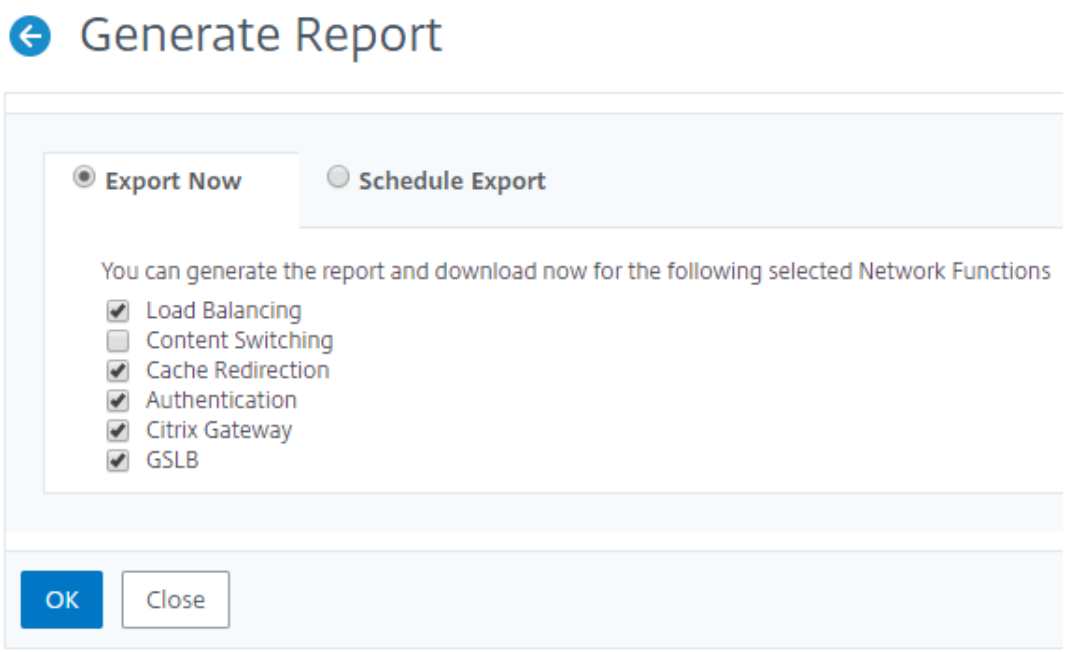
要导出和计划网络函数报告，请执行以下操作：

1. 导航到网络 **>** 网络功能。
2. 在“网络功能”页面的右窗格中，单击页面右上角的“生成报告”。



3. 在 生成报告页面上，您有以下 2 个选项：

   a) 选择“ 立即导出”选项卡，然后单击“ 确定”。报告将下载到您的系统。



下图显示了网络函数报告的示例。

Citrix ADC IP Address	Citrix ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
	beta		Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing				
			Load Balancing	lb11-lb#11.1.2.2:80			lb11-svcgrp#3.4.4.4-3.4.4.4:80
			Load Balancing	ADM-Test-LB3#10.1.1.3:80			
			Load Balancing	334-lb#1.33.2.2:80			
			Load Balancing				
			Load Balancing				
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-7bfbca74-07fb-45b6-b			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
			Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
			Load Balancing				

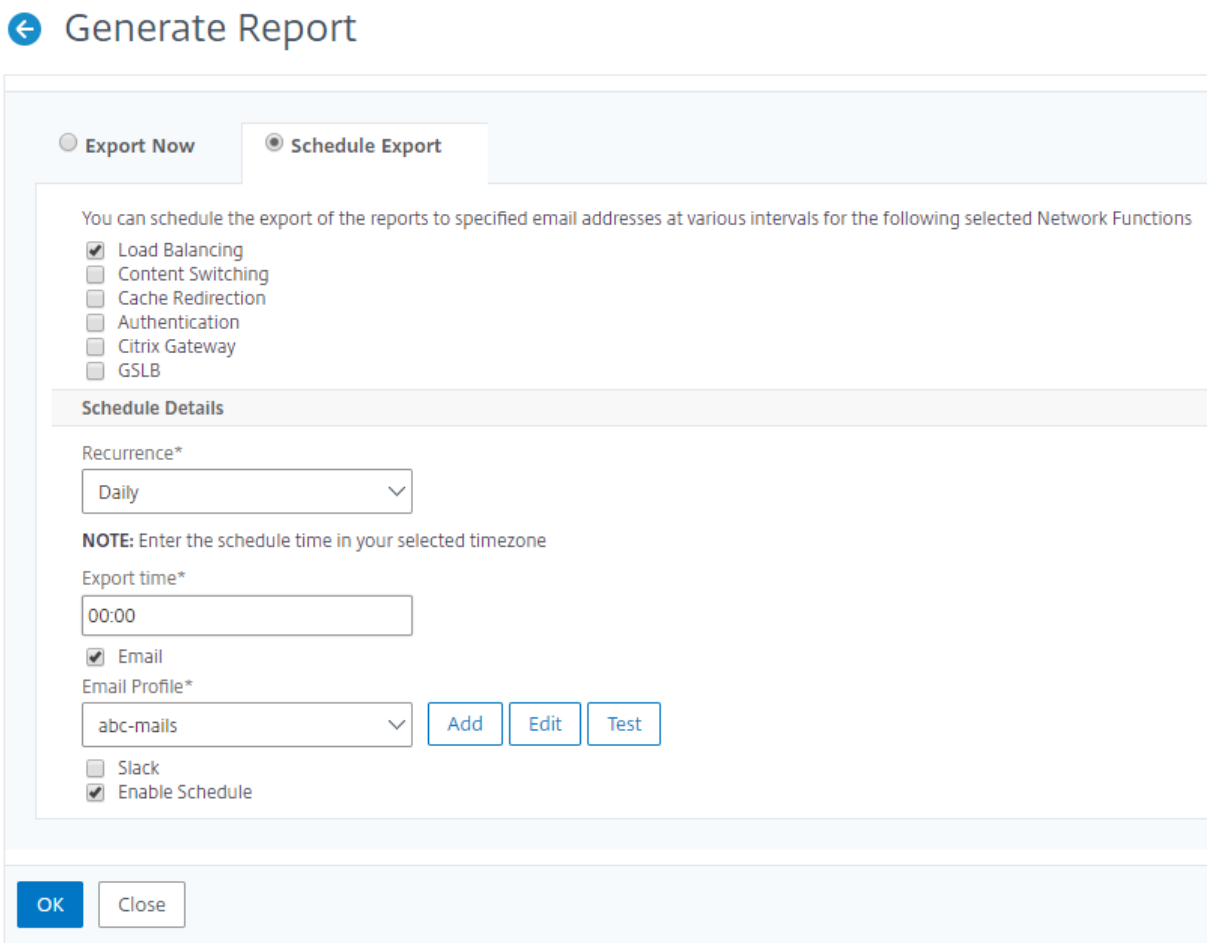
b) 选择“计划报告”选项卡，以计划定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

i. 重复-从下拉列表框中选择“每日”、“每周”或“每月”。

ii. 循环时间-以 24 小时格式输入时间为小时：分钟。

iii. 电子邮件配置文件-从下拉列表框中选择配置文件，或单击 **+** 创建电子邮件配置文件。

单击 启用计划以计划您的报告，然后单击 确定。通过单击 启用计划复选框，您可以生成选定的报告。



网络报告

April 23, 2021

您可以通过监视 Citrix Application Delivery Management (Citrix ADM) 上的网络报告来优化资源使用情况。您可能有包含许多部署在多个位置的应用程序的分布式部署。为了确保应用程序的最佳性能，您还部署了多个 Citrix Application Delivery Controller (Citrix ADC) 实例来平衡负载、内容交换或压缩流量。网络性能会影响应用程序性能。要继续保持应用程序的性能，您必须定期监控网络性能，并确保所有资源都得到最佳使用。

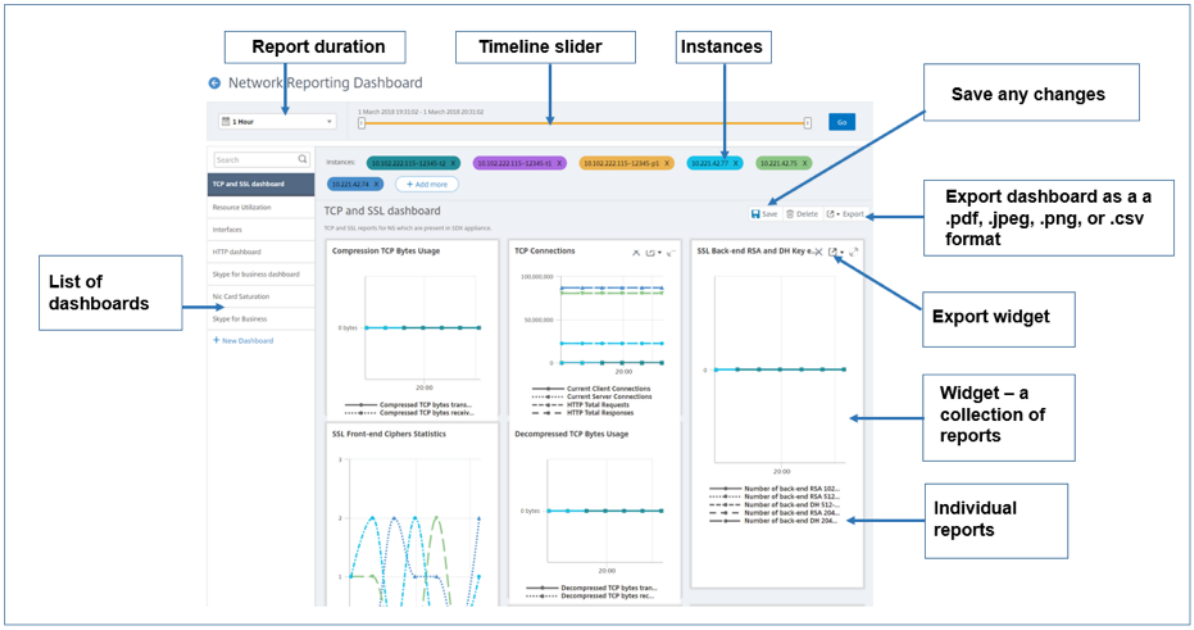
现在，Citrix ADM 不仅可以为全局级别的实例生成报告，还可以为虚拟服务器和网络接口等实体生成报告。实例系列由 Citrix ADC 和 SD-WAN 实例组成。您可以为其生成报告的虚拟服务器如下所示：

- 负载平衡服务器、服务和服务组
- 内容交换服务器
- 缓存重定向服务器
- 全局服务负载平衡 (GSLB)
- 身份验证
- Citrix Gateway

Citrix ADM 中的网络报告控制板是一个高度可定制的。现在，您可以为各种实例、虚拟服务器和其他实体创建多个控制板。

网络报告控制板

下图显示了控制板中的各种功能：

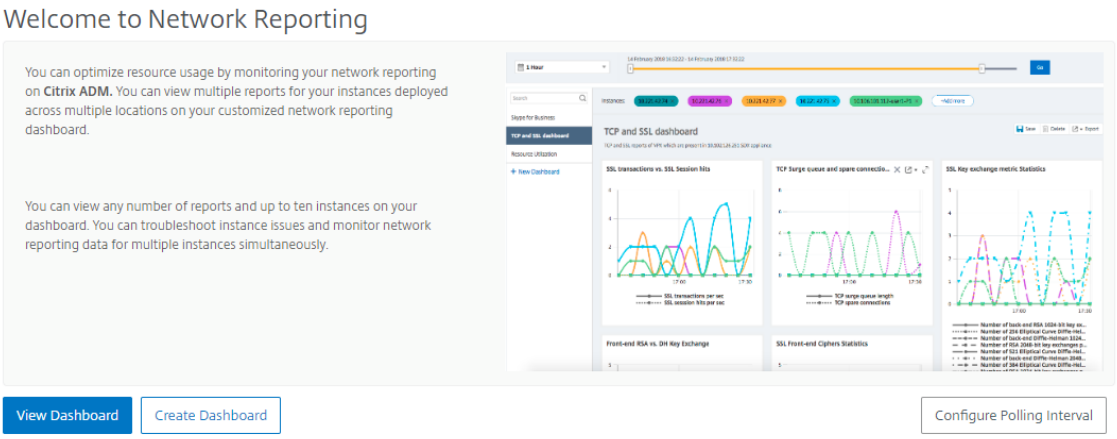


- 左侧面板列出了在 Citrix ADM 中创建的所有自定义控制板。您可以单击其中一个以查看控制面板所组成的各种报告。例如，TCP 和 SSL 控制板包含与 TCP 和 SSL 协议相关的各种报告。
- 您可以使用多个微件自定义每个仪表板以显示各种报告。小组件表示控制板上的报表，即更多相关报表的集合。例如，压缩 TCP 字节使用情况报告包含每秒传输和接收的压缩 TCP 字节的报告。
- 您可以显示一小时、一天、一周或一个月的报告。此外，您现在可以使用时间轴滑块选项自定义在 Citrix ADM 上生成的报告的持续时间。
- 您可以点击 “X” 删除报告。您也可以将报告导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。您还可以安排必须生成报告的时间和重复的时间。您还可以配置必须向其发送报告的电子邮件通讯组列表。
- 控制板顶部的 “实例” 部分列出了生成报告的所有实例的 IP 地址。
- 您可以通过单击 “X” 删除实例，也可以向报告添加更多实例。但是，目前 Citrix ADM 允许您查看 10 个实例的报告。
- 您还可以将整个控制板导出为.pdf、.jpeg、.png 或.csv 格式到您的系统。必须保存对控制板所做的任何更改。单击保存保存更改。

以下部分详细介绍了创建控制板、生成报表和导出报表的任务。

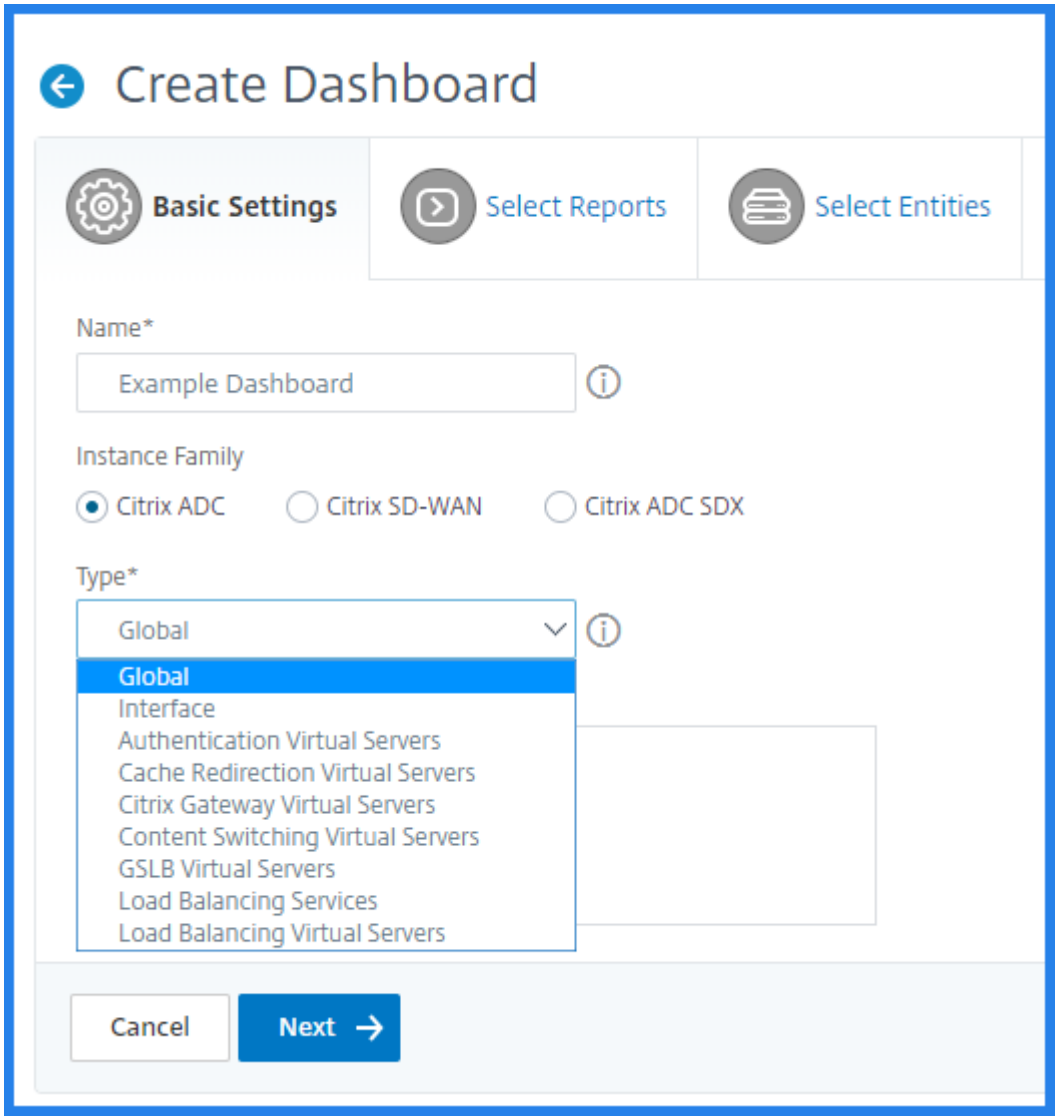
要查看或创建控制板，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “网 络” > “ 网络报告”。



2. 要查看现有控制板，请单击 查看控制板。“网络报表仪表 板页将打开，您可以在其中查看所有控制板和报表小组件。

3. 要创建控制板，请单击 创建控制板。此时将打开 “创建控制板” 页面。



4. 在“基本设置”选项卡中，输入以下详细信息：

   a) 名称。键入控制板的名称。

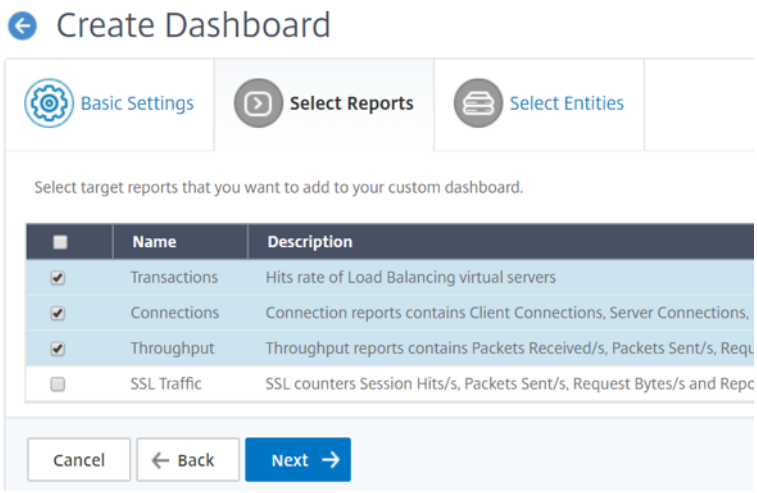
   b) 实例系列。选择实例类型 - Citrix ADC、Citrix SD-WAN 或 Citrix ADC SDX。

   c) 类型。选择要为其生成报告的实体类型。在此示例中，选择负载平衡虚拟服务器。

   d) 说明。键入控制板的有意义的描述。

5. 单击“ 下一步”。

6. 在 选择报告选项卡中，选择所需的报告。在此示例中，您可以选择事务、连接和吞吐量。单击下一步。



1. 在 “ 选择实体” 选项卡中，单击 “ 添加”。

   根据 “基本设置” 选项卡中选定的实体类型，将出现一个窗口，其中 包含实体列表。在此示例中，将显示 **“选择 LB** 虚拟服务器窗口。

2. 选择要监视的实体。

3. 单击创建。

控制板即会创建，并显示您选择的所有报表。

> 注意
>
> 目前，无法保存您对图例或筛选器所做的任何更改。

导出网络报告

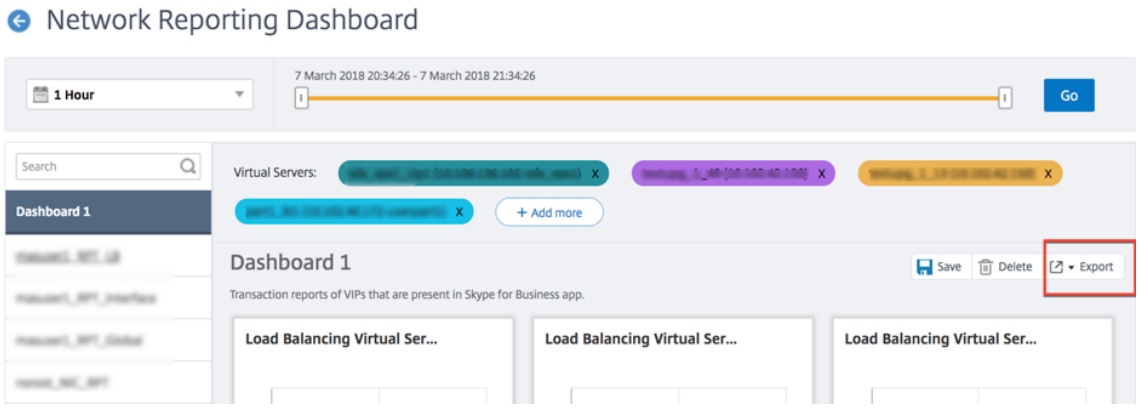
虽然您可以以.pdf、.png、.jpeg 或.csv 格式导出小组件报告，但您只能以.pdf、.jpeg 或.png 格式导出整个控制板。

> 注意
>
> 如果您具有只读权限，则无法在 Citrix ADM 中导出报表。您需要具有编辑权限才能在 Citrix ADM 中创建文件并

> 能够导出该文件。

要导出控制板报告，请执行以下操作：

1. 导航至 “ 网络” > “ 网络报告”
2. 单击 查看控制板以查看您已创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，单击 控制板 **1**。
4. 单击页面右上角的导出按钮。
5. 在 **“**立即导出” 选项卡下，选择所需的格式，然后单击 “ 导出”。



在 导出页面上，您可以执行以下操作之一：

6. 选择立即导出选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
7. 选择 计划导出选项卡。安排每天、每周或每月报告，并通过电子邮件或松弛消息发送报告。

   您可以定期安排导出 “ 网络报告” 仪表板页面。例如，您可以设置一个选项，以便在特定时间的前一小时内每周生成控制板报告。然后每周生成报告，并显示控制板的状态。如果用户设置，报告将覆盖时间和日期戳。

> 注意
>
> - 如果选择 “每周重复”，请确保选择了要计划报告的工作日。
> - 如果选择每月重复”，请确保输入希望以逗号分隔的报告计划的所有天数。

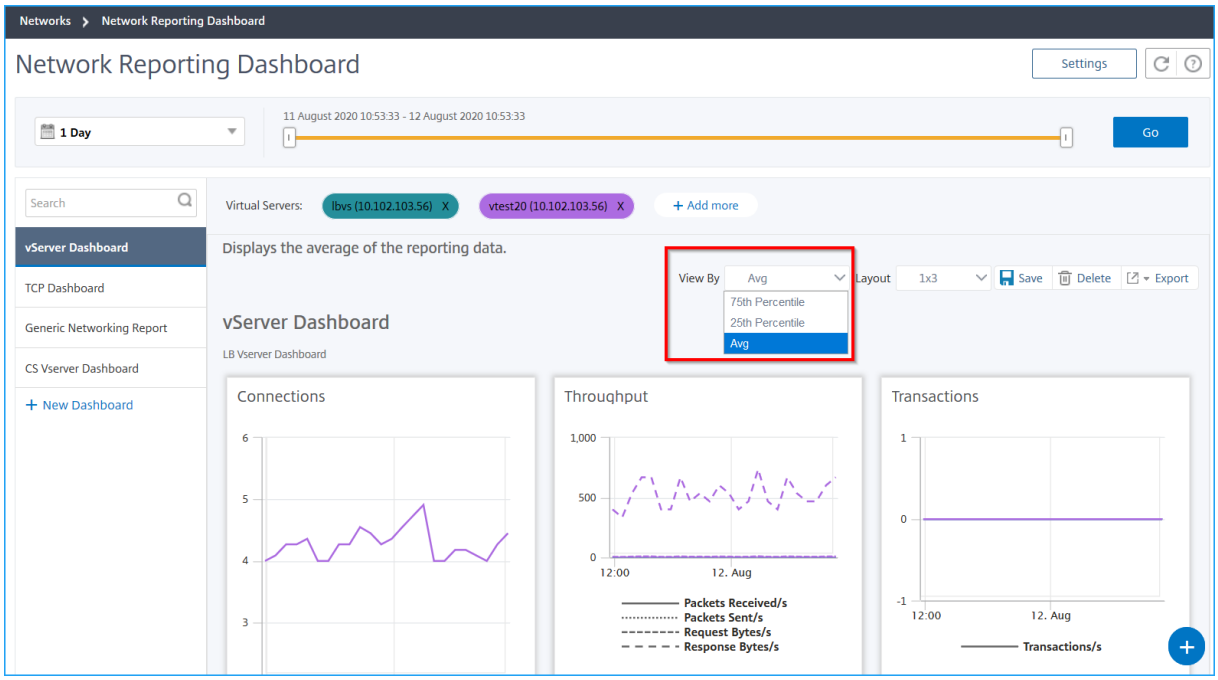
安排网络报告时，您可以通过在 “主题” 字段中输入文本字符串来自定义报告的标 题。在计划时间创建的报告的名称为此字符串。

例如，对于来自特定虚拟服务器的网络报告，可以键入主题为 “身份验证报告-10.106.118.120”，其中 10.106.118.120 是被监视虚拟服务器的 IP 地址。

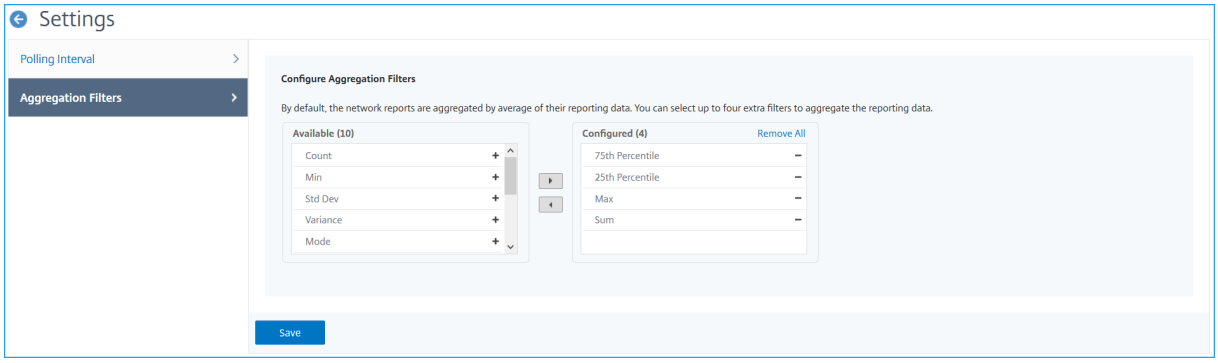
> 注意
>
> 目前，此选项仅在计划导出报告时可用。立即导出标题时，无法将标题添加到报表中。

通过应用聚合查看网络报告数据

您可以将聚合应用于网络性能数据，并在仪表板上查看应用程序性能。您还可以根据自己的要求导出结果。使用应用于数据的这些聚合，您可以分析并确保是否所有资源都得到最佳利用。导航到“ 网络”**>**“网络报告”，然后选择持续时间 1 天或更长时间以获取“ 查看依据”选项。



在现有平均数据中，您可以通过从“ 查看依据”列表中选择选项来应用聚合。应用聚合时，仪表板中的每个指标的数据都会更新。单击 设置并选择 聚合筛选器。



以下是您可以添加的聚合：

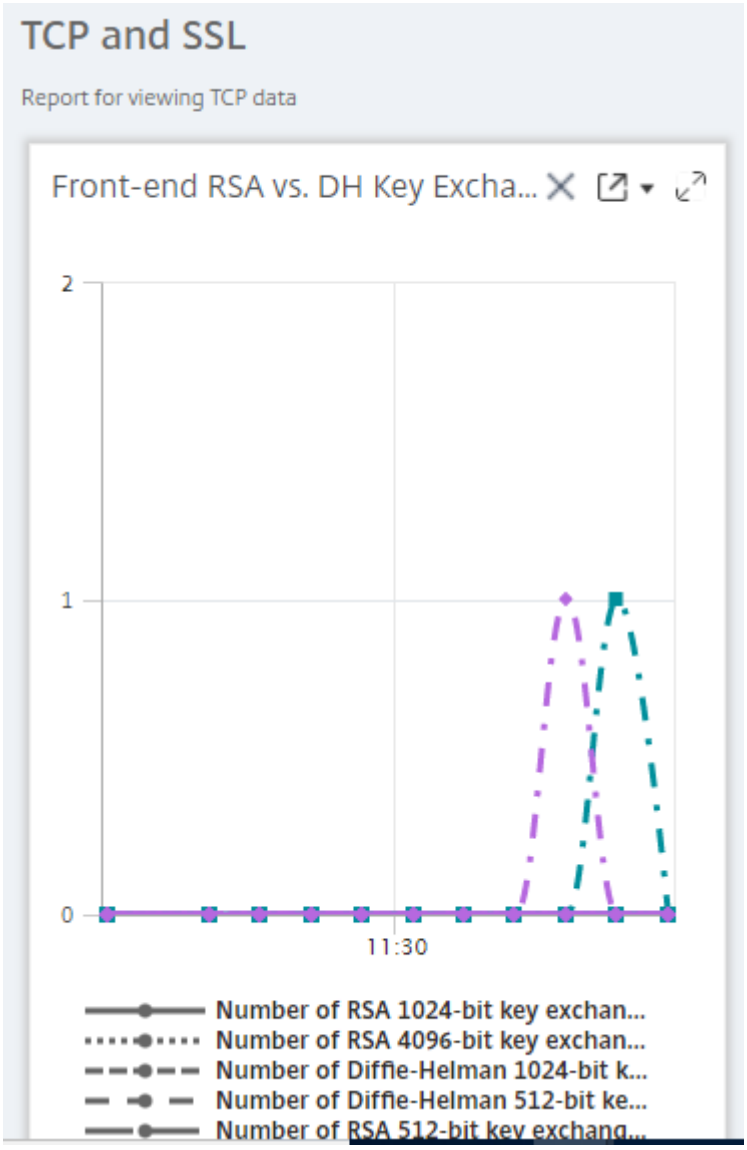
- 计数
- 最大
- 最小
- 求和
- Std 开发

- 差异
- 模式
- 中位数
- 第 25 个百分位数
- 第 75 个百分位
- 第 95 个百分位
- 99 个百分位数
- 第一个
- 最后一个

您最多可以向仪表板添加 4 个聚合选项。添加聚合选项后，Citrix ADM 大约需要 1 小时才能为所选聚合选项生成报告。

要导出小组件报表，请执行以下操作：

1. 导航到网 络 > 网络报告。
2. 单击 查看控制板以查看您已创建的所有控制板。
3. 在左窗格中，单击控制板。在此示例中，还单击 **Skype for Business**。
4. 选择一个小组件。例如，选择 负载平衡虚拟服务器事务。
5. 单击页面右上角的导出按钮
6. 在 **“**立即导出” 选项卡下，选择所需的格式，然后单击 “ 导出”。



如何在 **Citrix ADM** 上管理网络报告的阈值

要监视 Citrix ADC 实例的状态，您可以在计数器上设置阈值，并在超过阈值时接收通知。在 Citrix ADM 上，您可以配置阈值以及查看、编辑和删除阈值。

例如，当内容交换虚拟服务器的 Connections 计数器达到指定值时，您可以收到电子邮件通知。您可以为特定实例类型定义阈值。您还可以从所选实例中选择要为特定计数器指标生成的报告。

当计数器的值超过或低于阈值（由规则指定）时，将生成指定严重性的事件以表示与性能有关的问题。计数器值恢复到您认为正常的值时，将清除事件。可通过导航到 “ 网络” > “事 件” > “报告” 来查看这些事件。在 “报告” 页面上，您可以单击 按严重性划分的事件圆环以按其严重性查看事件。

您还可以将操作与阈值关联，例如在超过阈值时发送电子邮件或 SMS 消息。

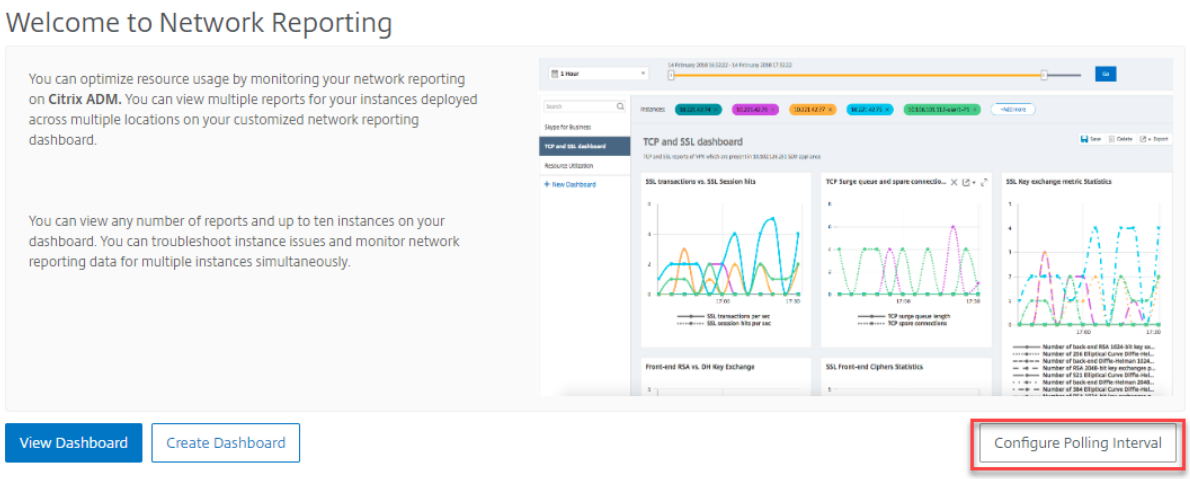
要创建阈值，请执行以下操作：

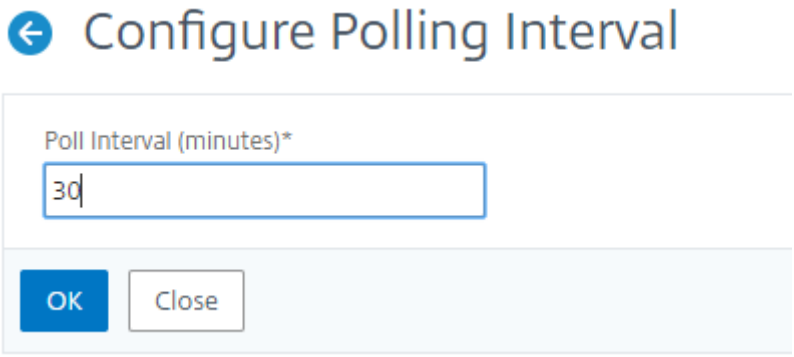
1. 在 Citrix ADM 中，导航到“网 络”>“ 网络报告”>“ 阈值”。在 **Thresholds**（阈值）下方单击 **Add**（添加）。
2. 在 创建阈值页上，指定以下详细信息：
   - 名称。阈值的名称。
   - 实例类型。选择 Citrix ADC 或 Citrix SD-WAN WO。
   - 报告名称。提供有关此阈值的信息的性能报告的名称。
3. 您还可以设置规则以指定生成或清除事件的时间。您可以在 配置规则部分下指定以下详细信息：
   - 度量。选择要为其设置阈值的度量。
   - 比较器。选择一个比较器以检查监视的值是否大于或等于或小于或等于阈值。
   - 阈值。键入计算事件严重性的值。例如，您可能希望在当前客户端连接的监视值达到 80% 时生成事件严重性为严重的事件。在此情况下，键入 80 作为阈值。您可以通过导航到“ 网络”>“事件”>“ 报告”来查看“严重严重性”事件。在“报告”页面上，您可以单击 按严重性划分的事件圆环以按其严重性查看事件。
   - 清除值。键入指示何时清除该值的值。例如，您可能希望在监视的值达到 50% 时清除当前客户端连接阈值。在此情况下，键入 50 作为清除值。
   - 事件严重性。选择要为阈值设置的安全级别。
4. 选择要为其设置阈值的一个或多个实例的 IP 地址。
5. 您还可以添加 活动消息。键入您希望在达到阈值时显示的消息。Citrix ADM 会将监视值和阈值追加到此消息。
6. 选择启用启用阈值以生成警报。
7. 或者，您可以配置 操作，例如电子邮件或 Slack 通知，或同时配置电子邮件和 Slack 通知。
8. 单击创建。

为网络报告设置性能轮询时间间隔

默认情况下，每 5 分钟 NITRO 调用收集一次性能数据用于网络报告。ADM 检索实例统计信息，例如计数器信息，并根据每分钟、每小时、每天或每周进行汇总。可以在预定义的报告中查看此汇总数据。

要设置性能轮询间隔，请导航到“网 络”>“ 网络报告”，然后单击“配置轮询间隔”。轮询时间间隔不能低于 5 分钟，也不能超过 60 分钟。





配置网络报告修剪设置

您可以在 Citrix ADM 中配置网络报告数据的清除间隔。此设置限制了 Citrix ADM 服务器数据库中存储的网络报告数据量。默认情况下，每 24 小时（01.00 小时）对报告历史数据的网络进行修剪。

> 注意
>
> 您可以指定的值不能超过 90 天或少于 1 天。

使用 **ADM** 审核日志管理和监视您的基础架构

April 23, 2021

您可以使用 Citrix ADM 服务跟踪 ADM 管理的 ADC 实例上生成的 ADM 和系统日志事件上的所有事件。这些消息可以帮助您管理和监控您的基础架构。但是，只有在您查看日志消息时，日志消息才是一个很好的信息来源，ADM 简化了日志消息的审阅方式。

您可以使用筛选器搜索 ADM 系统日志和审核日志消息。这些过滤器有助于缩小您的结果范围，并确切找到您正在寻找的内容和实时。内置的搜索帮助指导您筛选日志。另一种查看日志消息的方法是以 PDF、CSV、PNG 和 JPEG 格式导

出日志消息。您可以计划以各种时间间隔将这些报告导出到指定的电子邮件地址。

您可以从 ADM GUI 中查看以下类型的日志消息：

- 与 ADC 实例相关的审核日志
- ADM 相关审核日志
- 应用程序审核日志

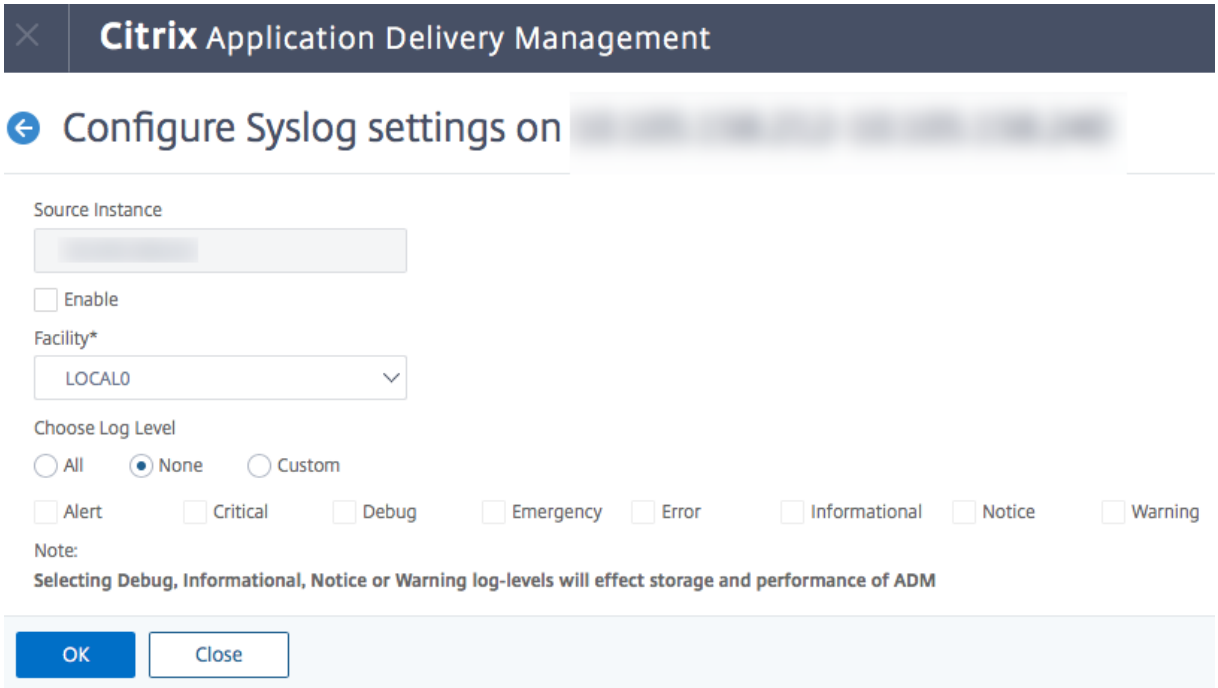
与 **ADC** 实例相关的审核日志

在从 ADM 查看与 ADC 实例相关的系统日志消息之前，先将 Citrix ADM 服务配置为 Citrix ADC 实例的系统日志服务器。配置完成后，所有 syslog 消息都将从实例重定向到 ADM。

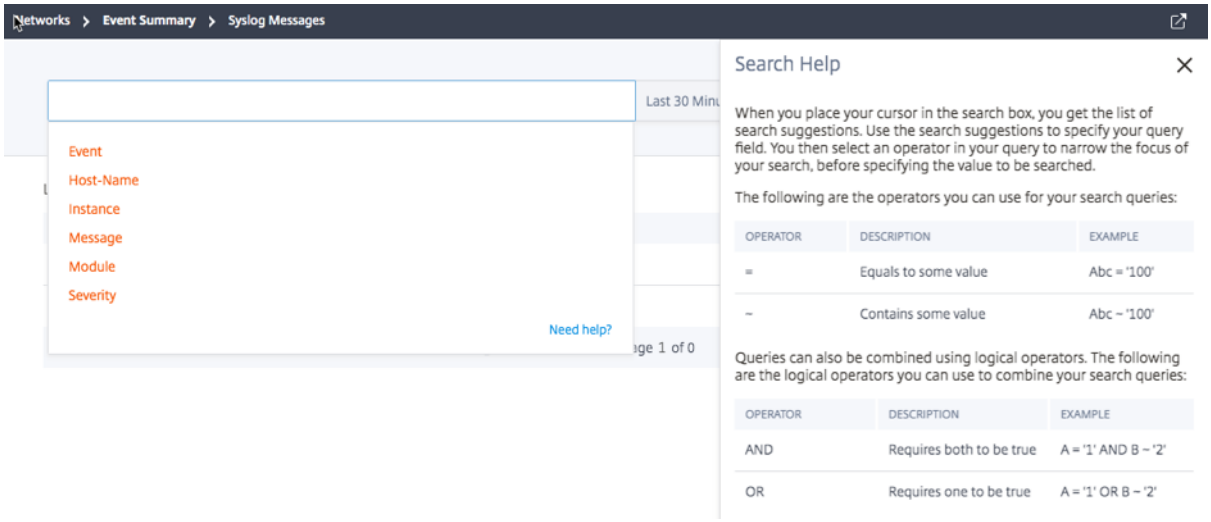
将 **ADM** 服务配置为系统日志服务器

请按照以下步骤将 ADM 配置为 syslog 服务器：

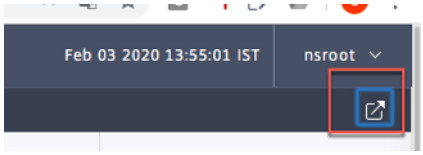
1. 在 ADM GUI 中，导航到 **“网络” > “实例”**。
2. 选择希望从中收集并在 Citrix ADM 中显示系统日志消息的 Citrix ADC 实例。
3. 在 选择操作列表中，选择 配置系统日志。
4. Click **Enable**。
5. 在 设施点下拉列表中，选择一个本地或用户级设施点。
6. 为 syslog 消息选择所需的日志级别。
7. 单击 “ 确定”。



这些步骤配置 Citrix ADC 实例中的所有 syslog 命令，Citrix ADM 开始接收系统日志消息。您可以通过导航到 **“网络” > “事件” > “系统日志消息”** 来查看消息。单击 需要帮助**?** 打开内置搜索帮助。有关详细信息，请参阅查看和导出系统日志消息。



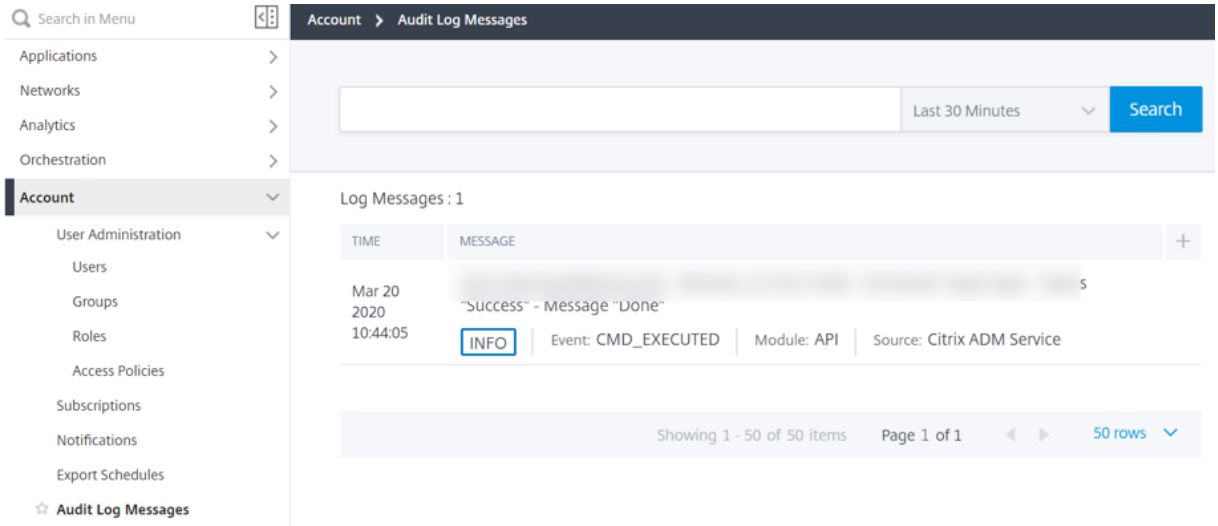
要导出日志消息，请单击右上角的箭头图标。



接下来，单击 “ 立即导出” 或 “ 计划导出”。有关详细信息，请参阅查看和导出系统日志消息。

ADM 相关审核日志

根据预配置的规则，ADM 会为上的所有事件生成审核日志消息，从而帮助您监控基础架构的运行状况。要查看 ADM 中存在的所有审核日志消息，请导航到 **“系统” > “审核日志消息”**。

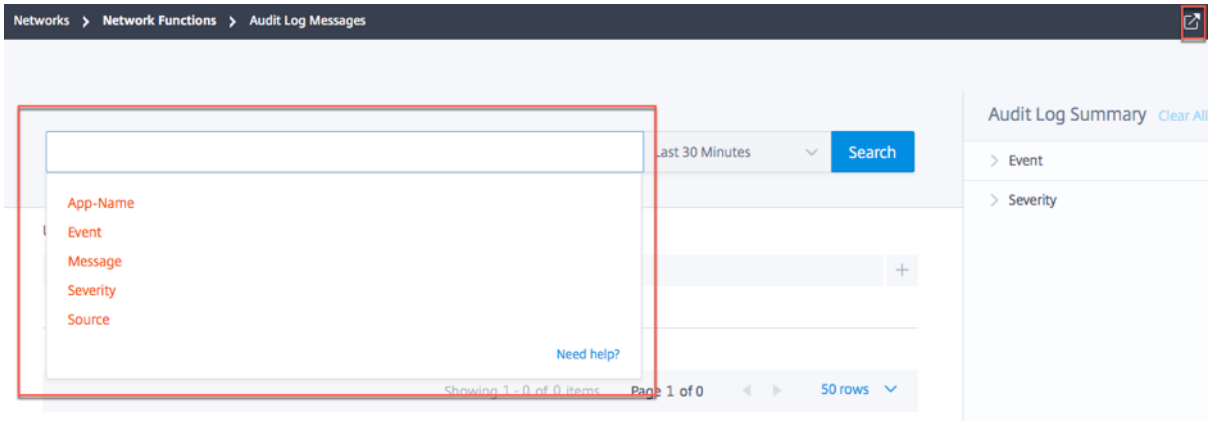


要导出日志消息，请单击右上角的箭头图标。

与应用程序相关的审核日志

您可以查看所有 ADM 应用程序或特定应用程序的审核日志消息。

- 要查看 ADM 中存在的所有应用程序的所有审核日志消息，请导航到 **“网络”-> “网络功能” > “审核”**。



- 要查看 ADM 中任何特定应用程序的审核日志消息，请导航至 **“应用程序” > “仪表板” > “双击虚拟服务器” > “审核日志”**。

分析

April 23, 2021

Citrix ADM 分析功能提供了一种简单且可扩展的方法，用于查看各种 Citrix ADC 见解，以分析和改进应用程序性能。您可以在 Citrix ADM 上同时使用一个或多个分析功能。

下表介绍了 Citrix ADM 上支持的各种分析功能：

分析功能	说明
Web Insight	Web Insight 支持对企业 Web 应用程序的可见性，并允许您监视 Citrix ADC 中的所有 Web 应用程序。作为管理员，您可以看到应用程序的集成和实时监控。
HDX Insight	HDX Insight 为通过 Citrix ADC 的 ICA 流量提供端到端的可见性。通过 HDX Insight，您可以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性能问题故障排除。

分析功能	说明
Gateway Insight	Gateway Insight 提供了所有用户在登录 Citrix Gateway 关时遇到的故障的可见性（无论访问模式如何）。
Security Insight	Security Insight 提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。
SSL Insight	SSL 智能分析提供了对安全 Web 事务 (HTTPS) 的可见性，并允许您监视 Citrix ADC 中的所有安全 Web 应用程序。作为管理员，您可以看到安全 Web 事务的集成、实时和历史监控。
TCP Insight	TCP Insight 提供了一个简单且可扩展的解决方案，用于监控 Citrix ADC 实例中使用的优化技术和拥塞控制策略（或算法）的指标，以避免数据传输中的网络拥塞。
Video Insight	Video Insight 功能提供了一个简单且可扩展的解决方案，用于监控 Citrix ADC 设备所使用的视频优化技术的指标，从而改善客户体验和运营效率。
WAN Insight	通过 WAN Insight 分析，管理员可以轻松监视数据中心与分支 WAN 优化设备之间传输的加速和未加速 WAN 流量。WAN Insight 还提供了网络上的客户端、应用程序和分支机构的可见性，以帮助有效地排除网络问题。

许可证要求

April 23, 2021

下表介绍了用于查看 Citrix ADM 上各种分析报告的 Citrix ADC 实例的许可要求：

Citrix ADM 分析功能	Citrix ADC 许可证要求
Web Insight	所有 Citrix ADC 许可证版本（标准/高级/高级）都支持 Citrix ADM 上的 Web 洞察报告。
HDX Insight	Citrix ADM 上的 HDX Insight 报告受到以下任何 Citrix ADC 许可证的支持：高级版（用于报告小于 1 小时）或高级版（用于无限制报告）。注意不支持标准许可证版本。

Citrix ADM 分析功能	Citrix ADC 许可证要求
Security Insight	Citrix ADM 上的安全洞察报告受到高级版或具有应用防火墙的高级版许可证的支持。注意不支持标准许可证版本和独立应用防火墙许可证。
SSL Insight	所有 Citrix ADC 许可证版本（标准/高级/高级）都支持 Citrix ADM 上的 SSL 智能分析报告。
Gateway Insight	Citrix ADM 上的网关智能分析报告受到以下任何 Citrix ADC 许可证的支持：高级版（用于报告小于 1 小时）或高级版（用于无限制报告）。注意不支持标准许可证版本。
TCP Insight	所有 Citrix ADC 许可证版本（标准/高级/高级）都支持 TCP 智能分析报告。
Video Insight	Citrix ADM 的视频洞察报告受到 Citrix ADC 高级版（VPX-T 1000 系列，VPX-T）支持。
WAN Insight	Citrix SD-WAN WO 版（广域网优化版）支持 Citrix ADM 的广域网洞察报告。

日志流概述

April 23, 2021

Citrix ADC 实例生成 AppFlow 记录，并且是数据中心中所有应用程序流量的中心控制点。IPFIX 和日志流是将这些 AppFlow 记录从 Citrix ADC 实例传输到 Citrix ADM 的协议。有关详细信息，请参阅AppFlow。

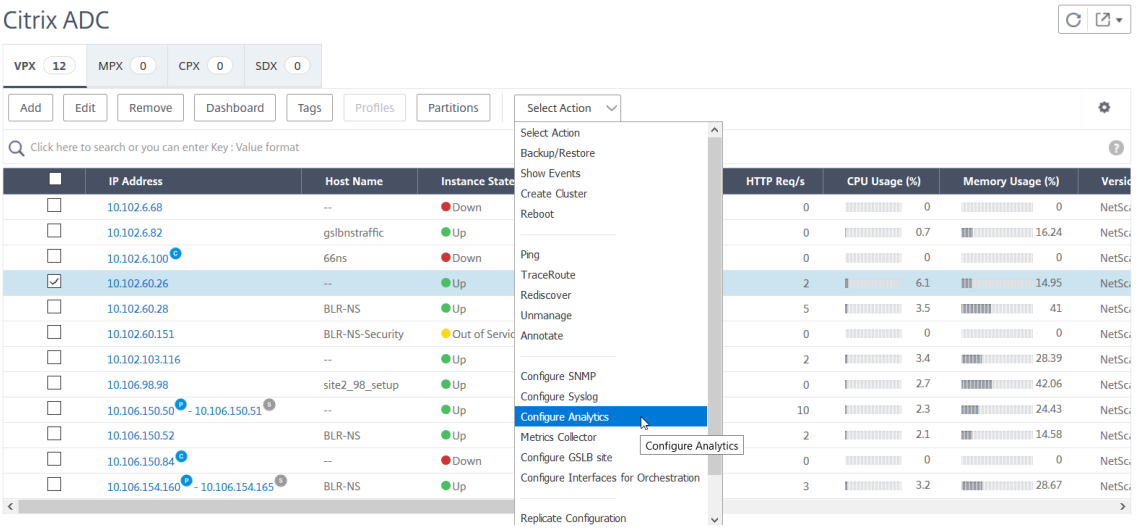
- IPFIX 是 RFC 5101 中定义的一个打开式互联网工程任务组 (IETF) 标准。IPFIX 使用 UDP 协议，该协议是用于单向数据流的不可靠传输协议。由于 IPFIX 使用 UDP 协议，因此遵守 IPFIX 标准可以在 Citrix ADM 中处理更多资源。
- Logstream 是 Citrix 拥有的协议，用作传输模式之一，可将分析日志数据从 Citrix ADC 实例高效传输到 Citrix ADM。Logstream 使用可靠的 TCP 协议，在处理数据时需要较少的资源。

对于 **11.1 Build 47.14** 与 **11.1 Build 62.8** 之间的 Citrix ADC，Logstream 是启用 Web Insight (HTTP) 的默认传输模式，IPFIX 是启用其他见解的唯一传输模式。对于从 **12.0** 开始到最新版本的 **Citrix ADC** 版本，您可以选择日志流或 **IPFIX** 作为传输模式。

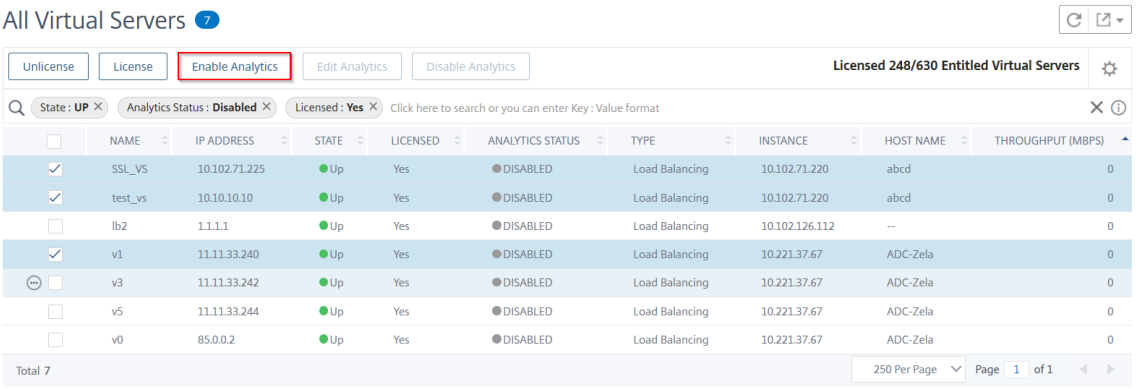
启用日志流作为传输模式

1. 导航到 网络 **>** 实例，然后选择要启用分析的 ADC 实例。

2. 从选择操作列表中，选择配置分析。



3. 选择虚拟服务器，然后单击启用分析。



4. 在 启用分析窗口中：

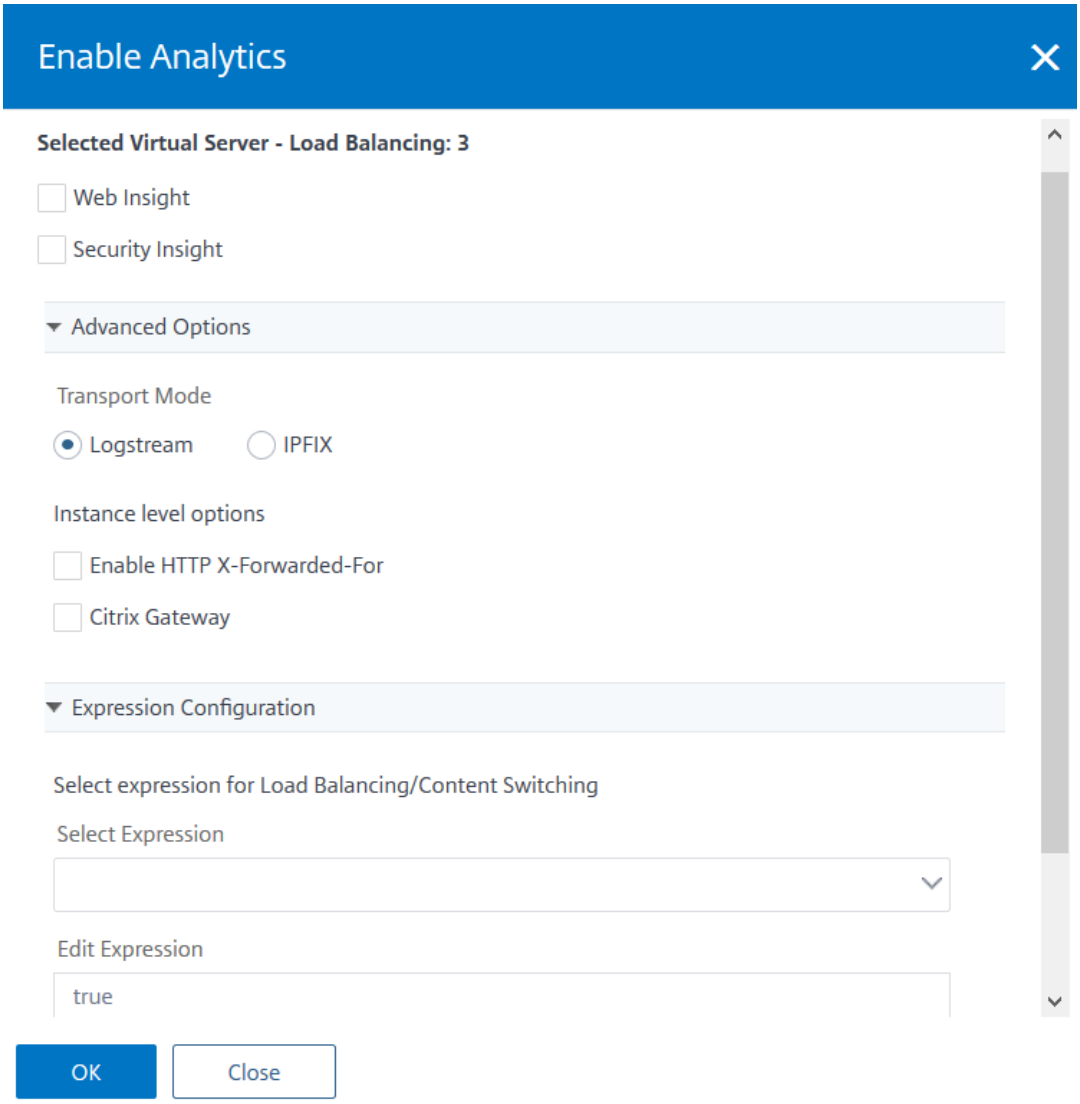
   a) 选择见解类型（Web 见解或安全见解）

   b) 选择 **Logstream** 作为传输模式

   > 注意
   >
   > 对于 **11.1 Build 47.14** 与 **11.1 Build 62.8** 之间的 Citrix ADC，Logstream 是启用 Web Insight (HTTP) 的默认传输模式，IPFIX 是启用其他见解的唯一传输模式。对于从 **12.0** 开始到最新版本的 **Citrix ADC** 版本，您可以选择日志流或 **IPFIX** 作为传输模式。

   c) 默认情况下，表达式为 true

   d) 单击 **OK**（确定）



注意

- 如果选择未获得许可的虚拟服务器，则 Citrix ADM 首先许可这些虚拟服务器，然后启用分析

- 对于管理员分区，只支持 **Web Insight**

- 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。显示错误消息

下表介绍了支持日志流作为传输模式的 Citrix ADM 的功能：

功能	IPFIX	Logstream（日志流）
Web Insight	•	•
Security Insight	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

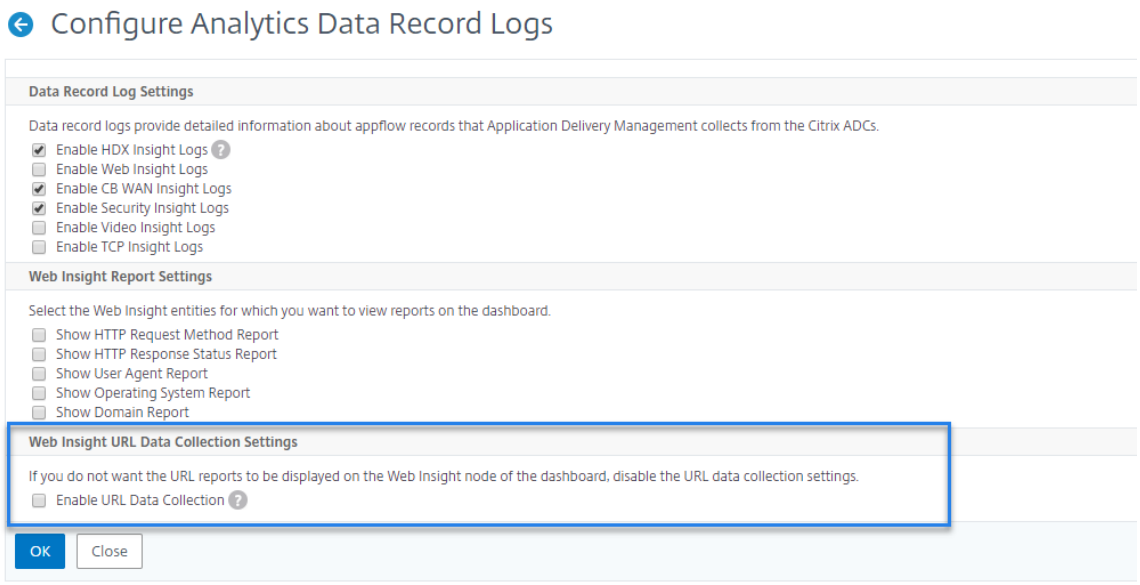
禁用 **URL** 数据收集

April 23, 2021

如果您不希望在 Citrix Application Delivery Management (ADM) 中仪表板的 Web 智能分析节点上显示 URL 报告，则可以禁用 URL 数据收集。

禁用来自 **Citrix ADM** 的 **URL** 数据收集的步骤

1. 在 Citrix ADM 中，导航到 “ 分析” > “ 设置”，然后单击 “ 配置分析数据记录日志”。
2. 在 **Web Insight URL Data Collection Settings**（Web 洞察 URL 数据收集设置）部分，如果 **Enable URL Data Collection**（启用 URL 数据收集）选项已选中，请清除该复选框。
3. 单击确定。



创建阈值和警报

April 23, 2021

您可以设置阈值和警报以监视 Citrix ADC 实例的状态。可以设置计数器阈值以及监视实例和托管实例上的实体。

当计数器的值超过阈值时，Citrix Application Delivery Management (ADM) 会生成一个事件来表示与性能相关的问题。如果计数器值符合在阈值中指定的清除值，即会清除事件，这意味着特定阈值已回到其正常状态。

还可以为阈值关联操作。操作包括发送警报、电子邮件或 SMS 通知。当超过阈值时，Citrix ADM 会自动执行您定义的操作，例如启用警报和发送电子邮件或 SMS 通知。

要使用 **Citrix ADM** 创建阈值和警报，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 > 设置 > 阈值。在 **Thresholds**（阈值）下方单击 **Add**（添加）。
2. 在 “ 创建阈值” 页上，指定以下详细信息：
    - **Name**（名称）- 用于配置阈值的名称。
    - 流量类型 — 要为其配置阈值的流量类型。
    - **Entity**（实体）- 要为其配置阈值的类别或资源类型。
    - **Reference Key**（引用键）- 根据选择的流量类型和实体自动生成的值。
    - **Duration**（持续时间）- 要为其配置阈值的时间间隔。
    - 配置规则 — 要为其配置阈值的度量的规则。

- 通知设置 -启用阈值并在超过阈值时通过电子邮件、松弛或短信等各种渠道接收通知。

3. 单击创建。

对于 HDX Insight，还可以设置多个阈值，以便仅当违反了配置的阈值中的所有实体时才生成警报。

配置自适应阈值

April 23, 2021

自适应阈值功能为每个 URL 的最大命中数设置阈值。如果 URL 的最大命中数大于为该 URL 设置的阈值，则会向外部 syslog 服务器发送 syslog 消息。阈值时间间隔可以是天或周。

阈值计算方式如下：

阈值 = 最大命中数 **x** 阈值乘数

其中：

- 最大命中数是 URL 的最大命中数。
- 阈值系数是您定义的整数值（默认值：2）。

使用 **Citrix ADM** 创建自适应阈值

1. 在 Citrix ADM 中，导航到 “ 分析” > “ 设置” > “ 自适应阈值”，然后单击 “ 添加”。
2. 在 “ 自适应阈值” 页上，指定以下参数：
    - **Name**（名称）- 阈值名称
    - **Entity**（实体）- URL
    - **Duration**（持续时间）- 阈值的持续时间（天或周）
    - 阈值乘数-用户定义的整数，该整数与指定 URL 的最大命中计数相乘，以获取 URL 的自适应阈值。

配置数据库持久性

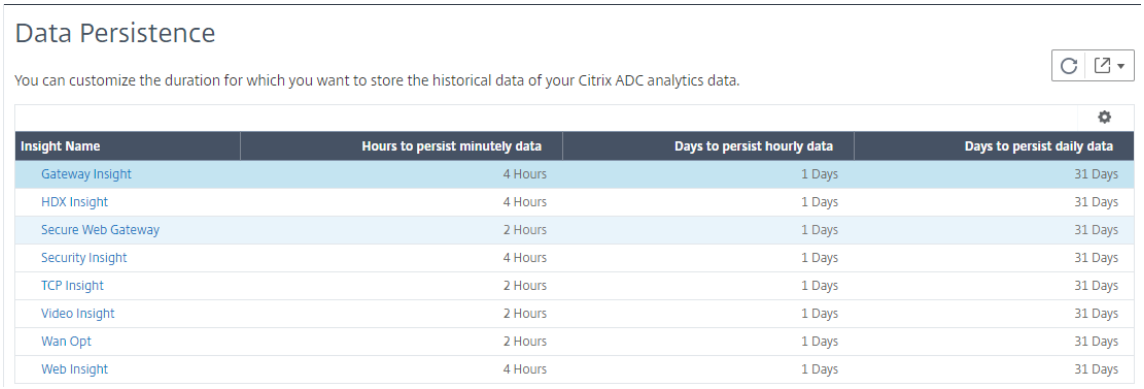
April 23, 2021

在 Citrix Application Delivery Management (ADM) 中配置数据库持久性允许您自定义要存储 Citrix ADC 分析数据的历史数据的持续时间。您可以为分析的历史数据选择以下数据库持久性类型：

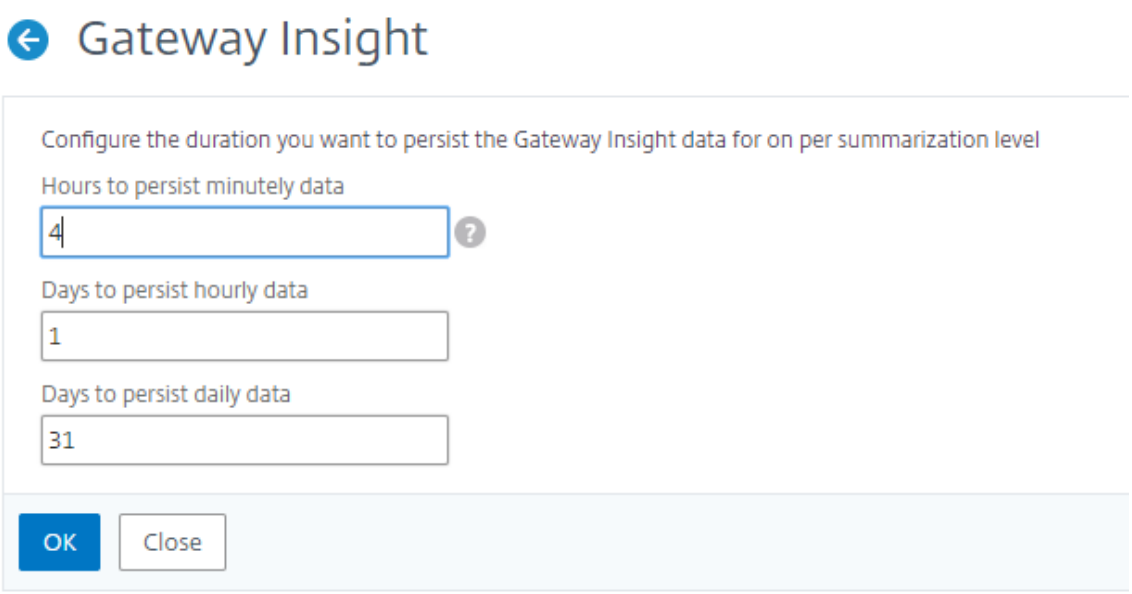
- Hours to persist minutely data（保持每分钟数据的小时数）
- Days to persist hourly data（保持每小时数据的天数）
- Days to persist daily data（保持每日数据的天数）

配置数据库持久性

1. 导航到 > 分析 > 设置 > 数据库持久性。
2. 单击要配置数据库持久性的智能分析类型。



3. 指定要在 Citrix ADM 上保留智能分析数据的持续时间。例如，对于 Gateway Insight，可以将分析的每分钟历史数据存储 2 小时，或将每小时数据存储 1 天。



针对分析的自助诊断

April 23, 2021

Citrix Application Delivery Management (ADM) 执行自助诊断，以确定托管实例上的许可证和配置问题，以满足以下分析功能：

- Web Insight
- HDX Insight
- Gateway Insight
- Security Insight
- SSL 转发代理分析

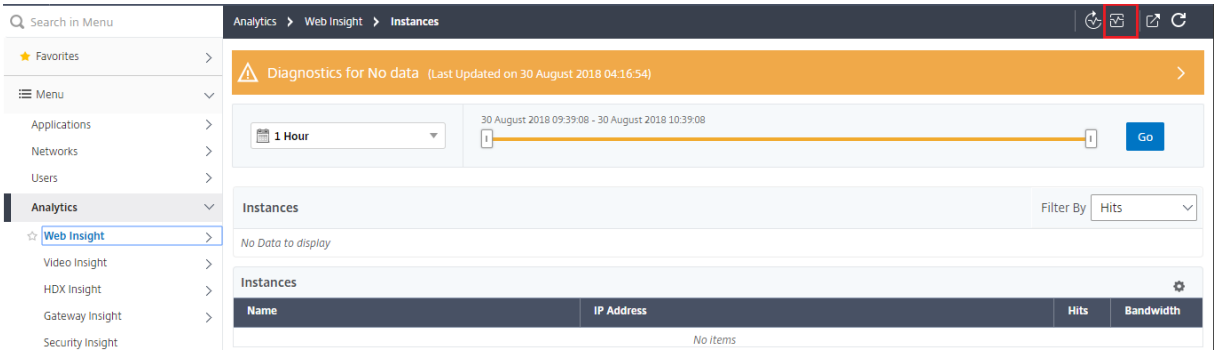
自助诊断程序每 12 小时运行一次，如果发现每个指定分析功能的问题，则会生成一份诊断报告。诊断报告提供了问题的来源、问题的类型以及解决问题的纠正措施。自助诊断可帮助您更快地识别问题并进行故障排除。

例如，如果虚拟服务器上未绑定 AppFlow 策略或虚拟服务器未获得许可，则 Citrix ADM 不会获取所需的 Web 智能分析监视数据。自助诊断程序可识别问题并生成诊断报告。您可以查看诊断报告以检查问题并执行更正操作。

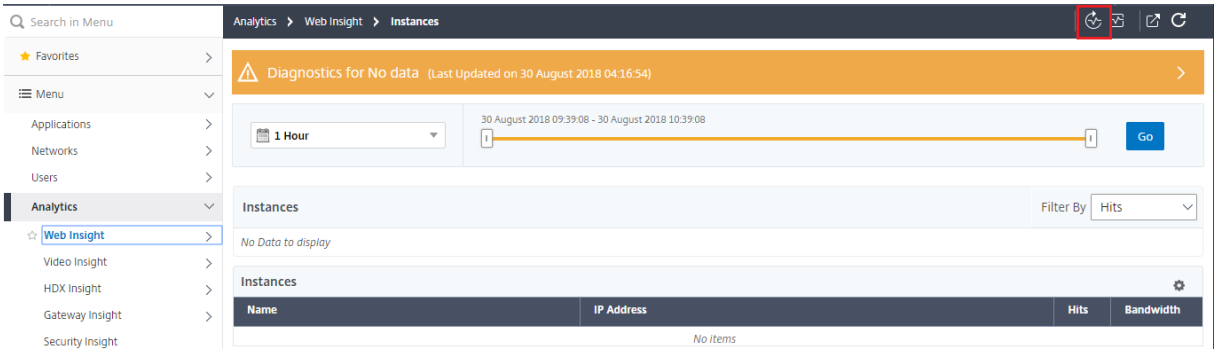
查看诊断报告

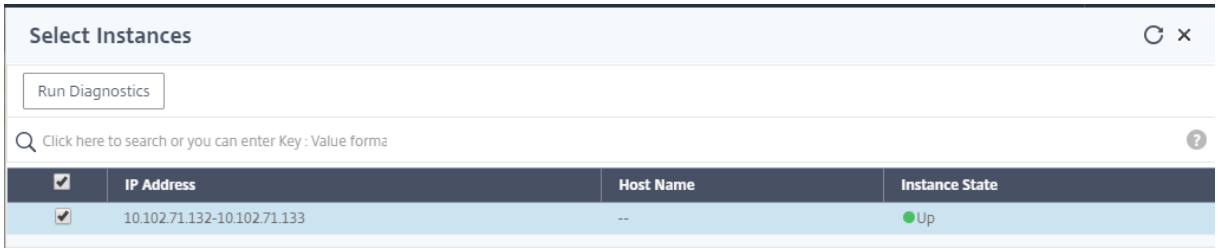
要查看指定分析功能的诊断报告，您需要转到 Citrix ADM 仪表板中的相应分析节点。

例如，要查看 Web 智能分析的诊断报告，请导航到 **“分析” > “Web** 智能分析”。在 “Web 智能分析” 页面上，选择 “显示诊断” 图标。



如果要检查问题，也可以运行即时诊断程序。单击 运行诊断程序。选择实例并选择 运行诊断程序。





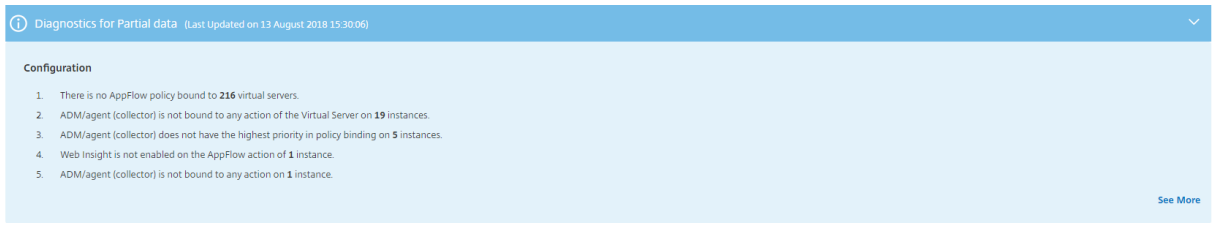
分析诊断报告

自助诊断程序根据问题的严重程度以橙色或蓝色背景显示诊断报告。

橙色背景的诊断报告表明临界程度高于蓝色背景。

例如，在您的 Citrix ADC 实例上配置了五台虚拟服务器。如果尚未在任何虚拟服务器上启用 AppFlow 参数，则 Citrix ADM 不会收到用于分析的 Web 智能分析和安全智能分析通信。自助诊断程序将配置问题确定为严重问题。您可以在 Web 智能分析和安全分析功能中看到橙色背景诊断报告。

如果您在其中一台虚拟服务器上启用了 AppFlow，则 Citrix ADM 会收到数据进行分析。您可以在蓝色背景下看到诊断报告，因为至少有一个虚拟服务器正在发送流量进行分析。

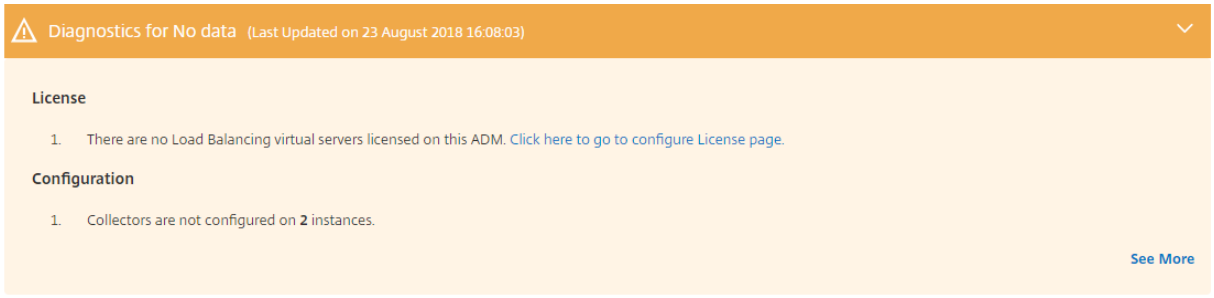


> 重要提示：自助诊断程序不检查流量。它只检查与托管实例上的指定分析功能相关联的许可证或配置问题。有时，您看不到任何分析数据，因为没有活动流量通过虚拟服务器。

诊断报告包含一个摘要页面和一个详细信息页面。

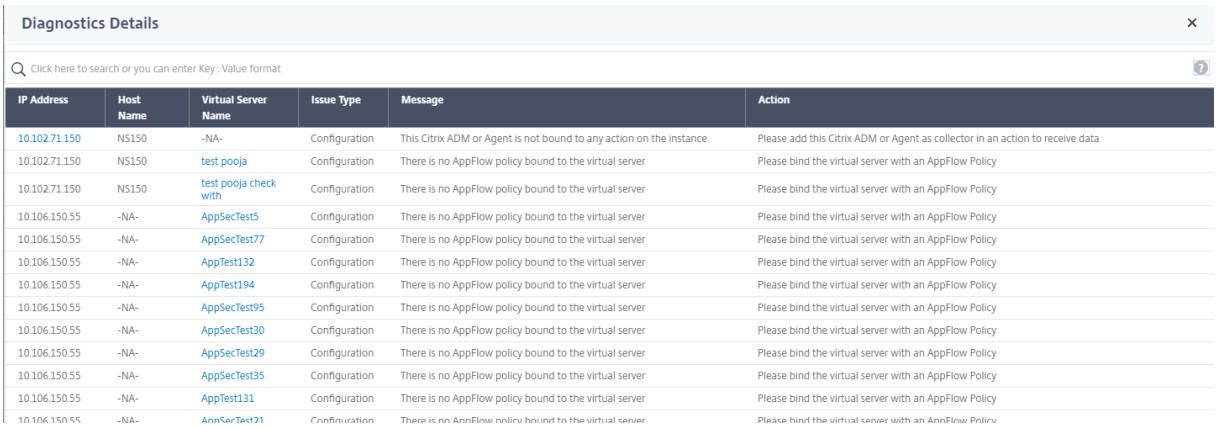
摘要页面概述了许可证或配置问题类型。该页面可能包含指向相关配置页的超链接。

例如，如果 Citrix ADM 上没有许可的负载平衡虚拟服务器，则摘要页面将提供一个超链接，用于指向“ 系统许可证”页面。

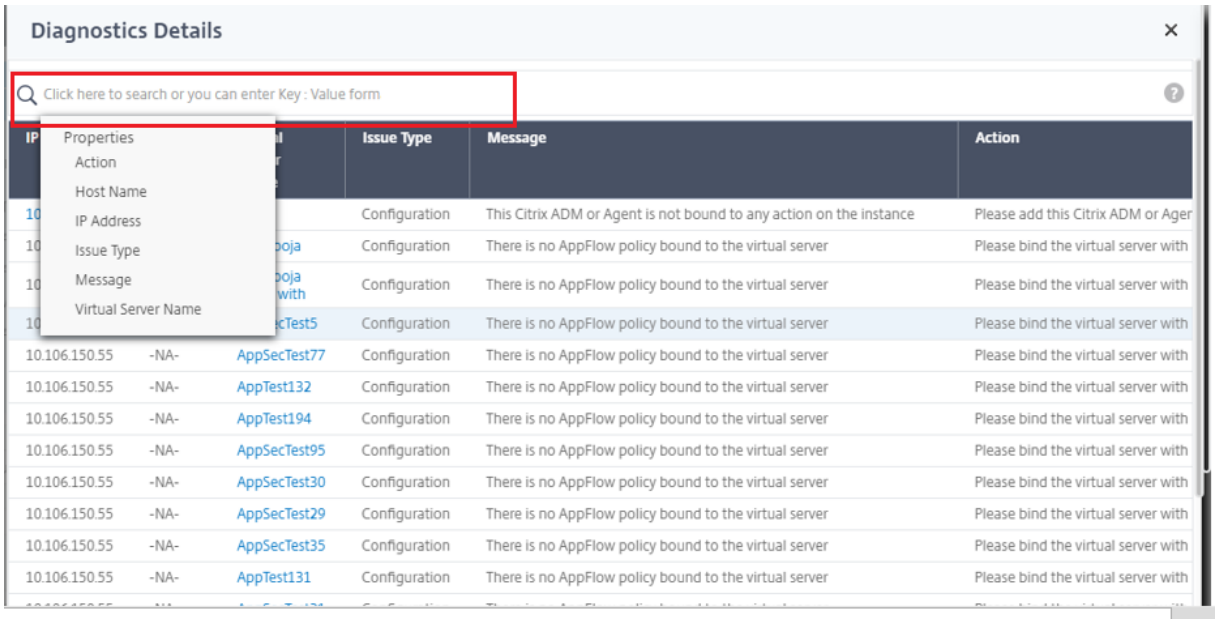


要查看有关问题的详细信息，请单击摘要页面上的查看详细信息。

详细信息页面提供有关问题的完整信息，并建议您需要执行的操作。您可以单击针对每个问题的超链接来配置托管实例或虚拟服务器。



您还可以根据操作、主机名、IP 地址和问题类型等搜索问题。



解决问题后，您需要运行即时诊断以生成最新的诊断报告。

Web Insight

April 23, 2021

通过 Web Insight，管理员可以监视 Citrix ADC 实例提供的所有 Web 应用程序。作为管理员，您可以从 Citrix ADC 实例获得对应用程序的集成实时监视。Web Insight 提供客户端网络延迟和服务器响应时间等重要信息，确保监控和提高应用程序性能。从 Citrix ADC 实例处理的每个 HTTP HTTPS 事务中捕获用于分析的数据。通过分析数据，您可以分析环境中 Citrix ADC 实例、应用程序、URL、客户端和服务器的性能。

以下是您可以使用 Web 智能分析查看数据的一些使用案例：

- 访问 SharePoint 等应用程序时遇到高延迟的客户端列表
- 在一个小时内打击最多的顶级应用程序
- 从客户端访问的应用程序和 URL 列表
- 特定客户端使用的操作系统和浏览器
- 发送与错误相关响应最多的应用程序或服务器
- 一个特定客户端的辅助功能问题
- 来自特定客户端的少数或所有应用程序的可访问性问题
- 来自特定客户端和后端服务器的应用程序的页面很少
- 从特定客户端和后端服务器访问应用程序时速度很慢

您可以为选定实例上的特定虚拟服务器启用 Web Insight，以监视 Web 应用程序上的流量。然后，Web 见解功能提供 Citrix ADM 中虚拟服务器的统计信息。

要启用 Web Insight：

如果您的 Citrix ADM 是 **13.0** 版本 **41.x** 版本：

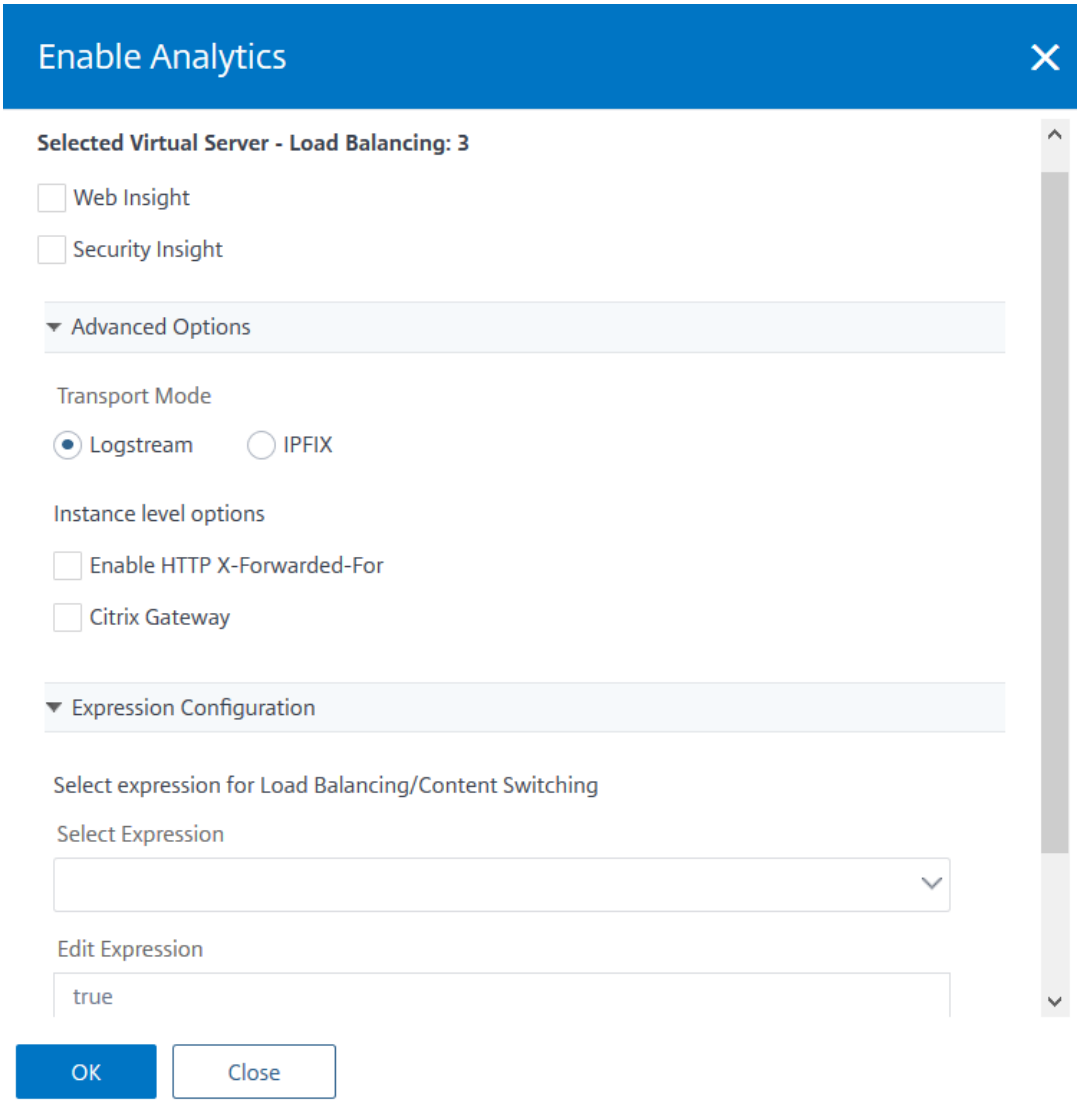
1. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC**”，然后选择实例类型。例如，VPX。
2. 选择实例，然后从 “ 选择操作” 列表中单击 “ 配置分析”。
3. 在在虚拟服务器上配置 **Analytics** 页面上，选择虚拟服务器，然后单击启用 **Analytics**。
4. 在 启用分析窗口中：
   a) 选择 **Web Insight**
   b) 选择 **Logstream** 作为传输模式

   > 注意
   >
   > 对于 Citrix ADC 12.0 或更低版本，**IPFIX** 是传输模式的默认选项。对于 Citrix ADC 12.0 或更高

> 版本，您可以选择日志流或 **IPFIX** 作为传输模式。
>
> 有关 IPFIX 和日志流的详细信息，请参阅 日志流概述。

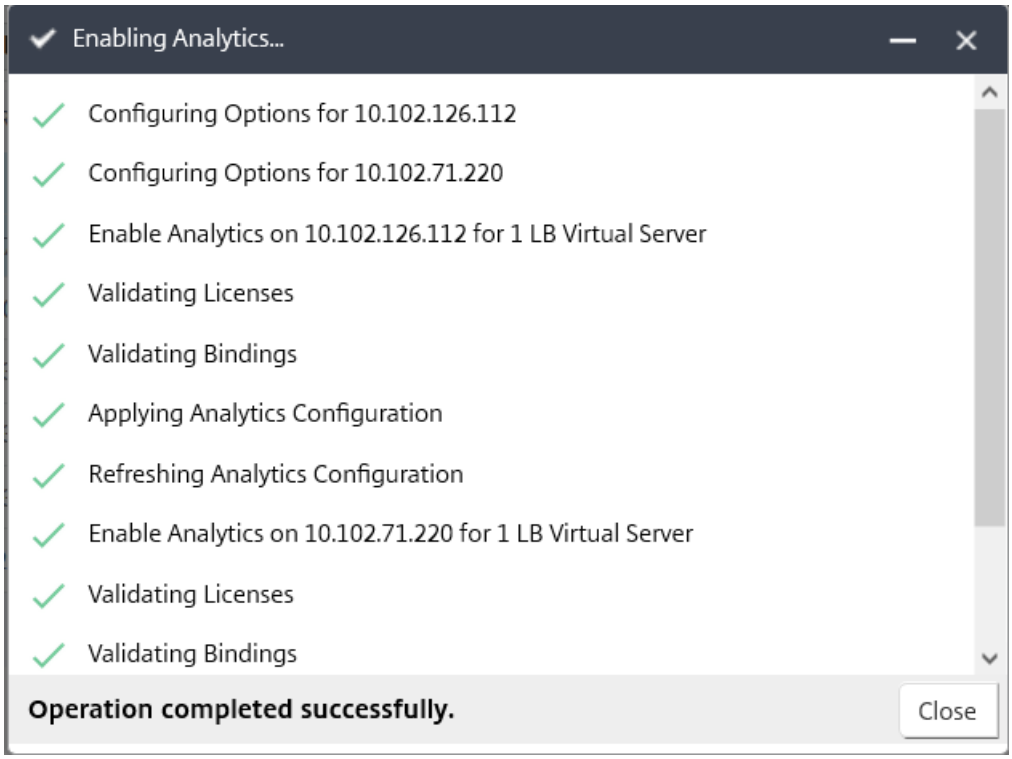
c) 默认情况下，表达式为 true

d) 单击 **OK**（确定）



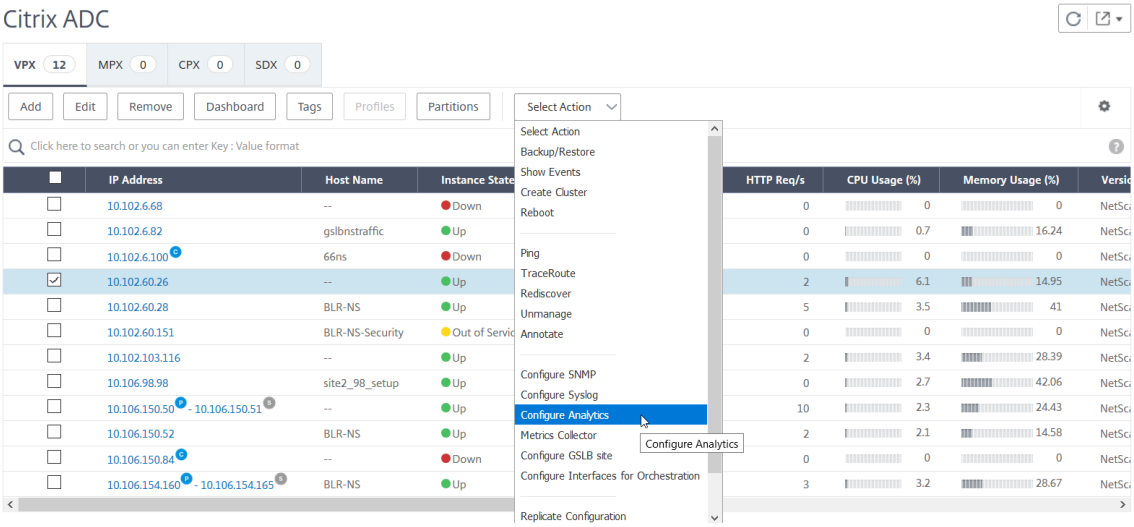
> 注意
>
> ```
> - 如果选择未获得许可的虚拟服务器，则 Citrix ADM 首先许可这些虚拟服务器，然后启用分析
>
> - 对于管理员分区，只支持 **Web Insight**
>
> - 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无法启用分析。将显示一条错误消息。
> ```


单击 确定”后，Citrix ADM 将处理在所选虚拟服务器上启用分析。



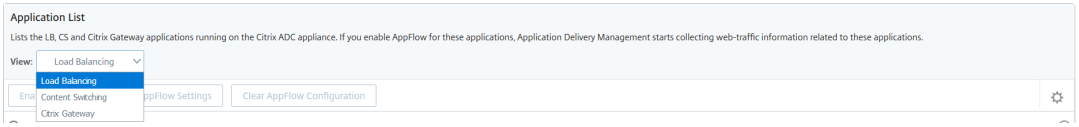
如果您的 Citrix ADM 是 **13.0** 版本 **36.27**：

1. 导航到网络 > 实例 > **Citrix ADC**，然后选择要在其上启用分析的 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。

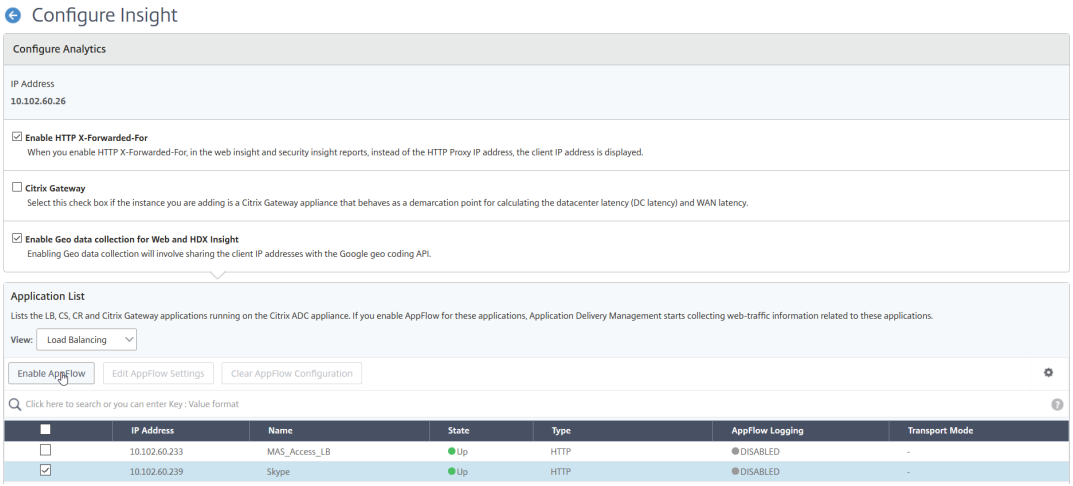


3. 在 “ 配置智能分析” 页上：

   a) 为负载平衡或内容切换选择 应用程序列表。



b) 选择虚拟服务器，然后单击 启用 **AppFlow**。

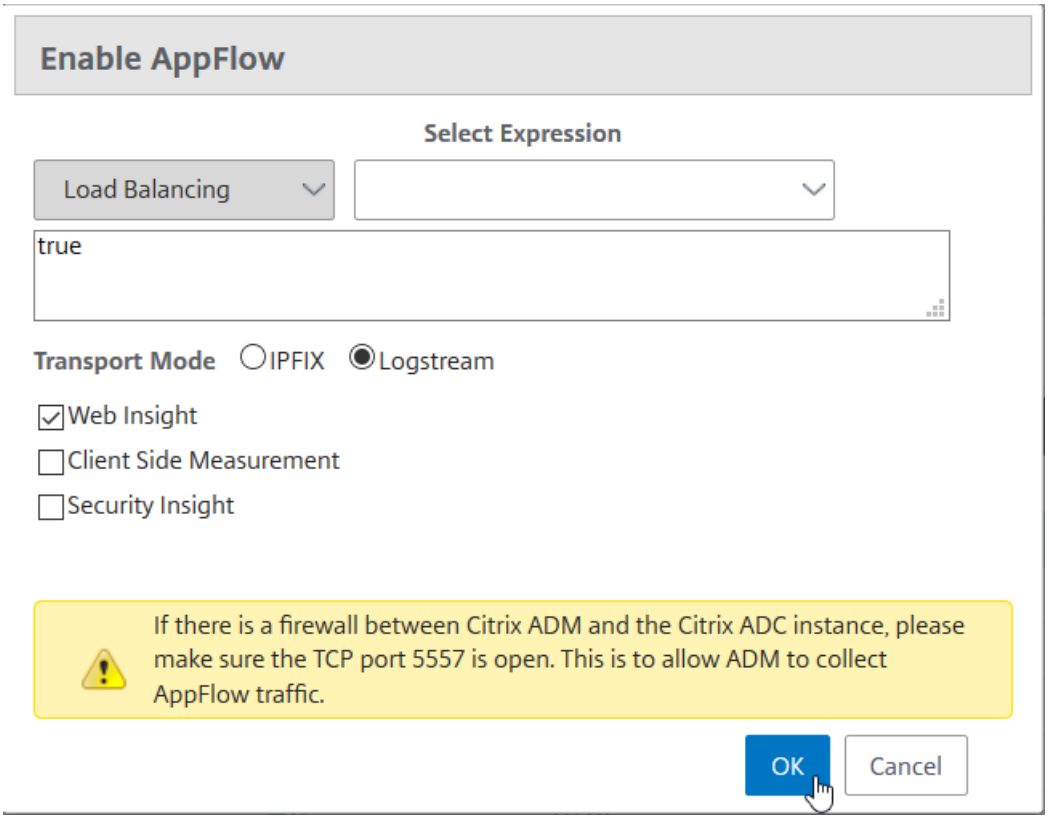


4. 在“启用 AppFlow”对话框中：

   - 在文本框中输入 **true**
   - 选择 日志流作为传输模式

     > 注意：Citrix 建议您选择日志流作为传输模式

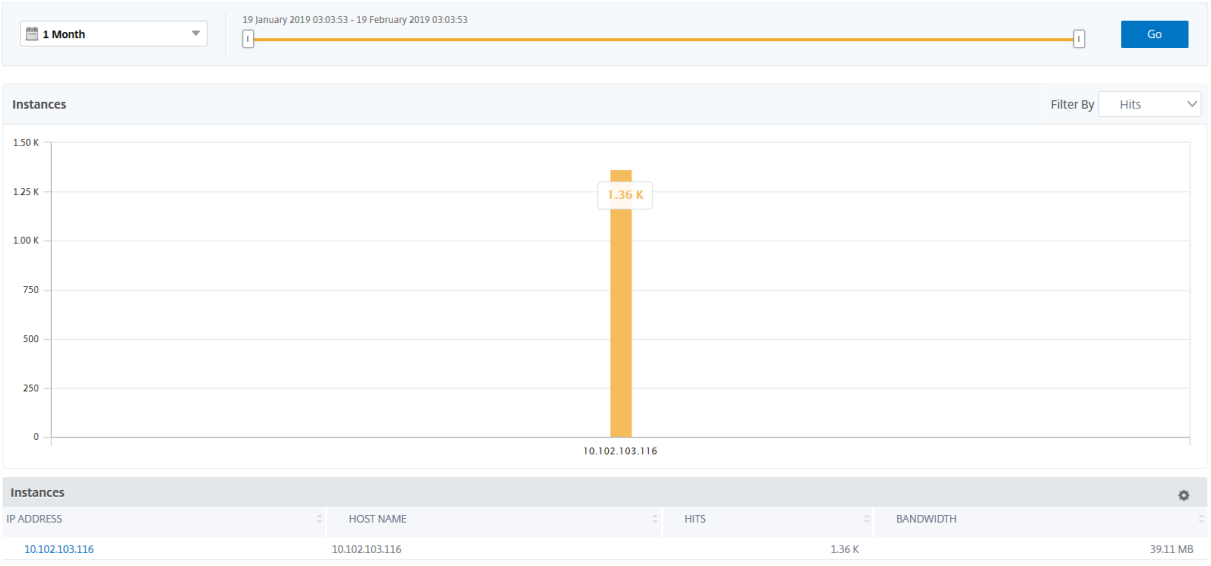
   - 选择“ **Web** 智能分析”，然后单击“ 确定”。



分析 **Web** 应用程序问题

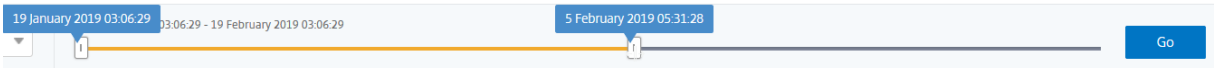
管理员需要确定的常见问题之一是延迟问题。作为管理员，您需要查找延迟问题是来自服务器网络、客户端网络还是服务器响应时间。使用 Citrix ADM，您可以通过导航到分析 > **Web Insight** 来识别此信息。

导航到分析 > **Web Insight** 时，它会显示通过 Web 智能分析启用的 Citrix ADC 实例。您可以查看实例的详细信息，例如 IP 地址、主机名、总命中次数和带宽。



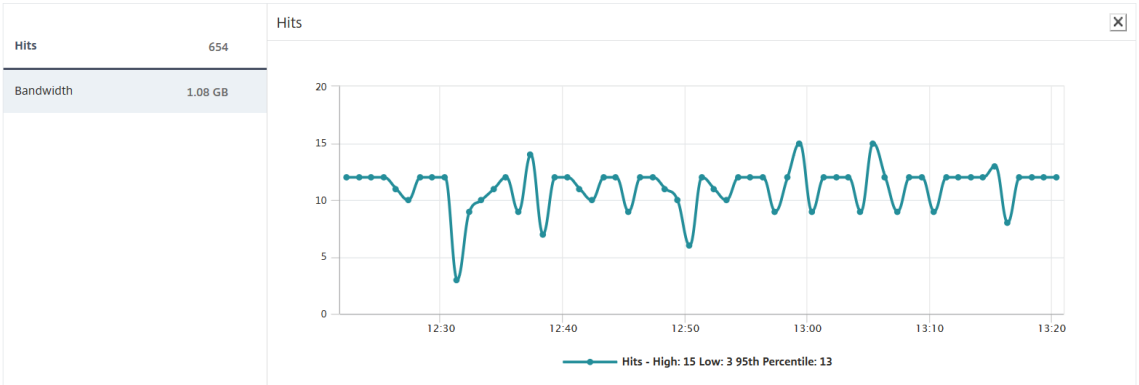
使用列表，您可以选择时间持续时间以查看实例的见解。

您还可以使用滑块自定义时间持续时间，然后单击 转到以显示结果。

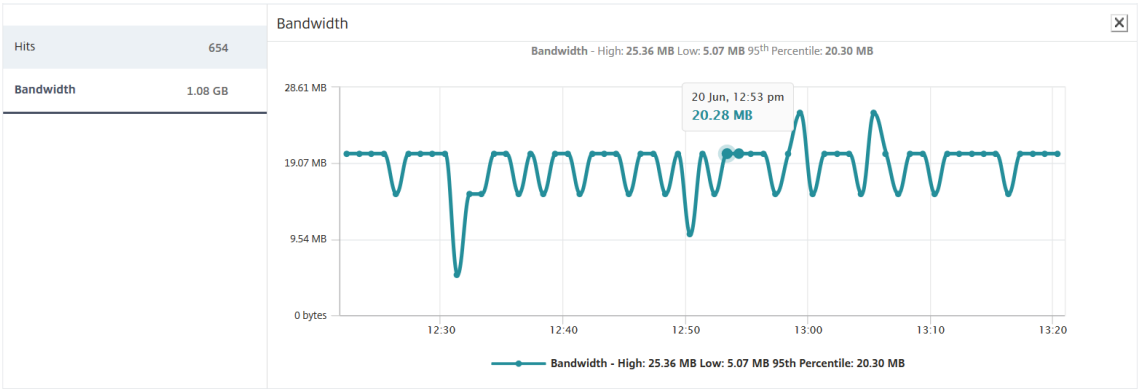


当您单击实例的图表或 IP 地址时，将显示有关该实例的详细信息。您可以查看以下内容的见解：

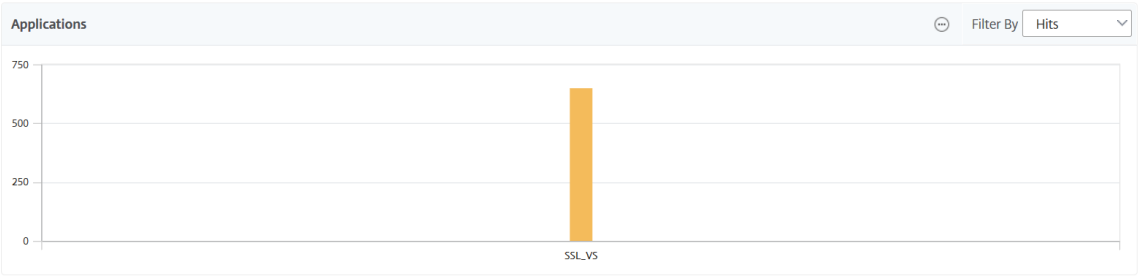
- 点击总数



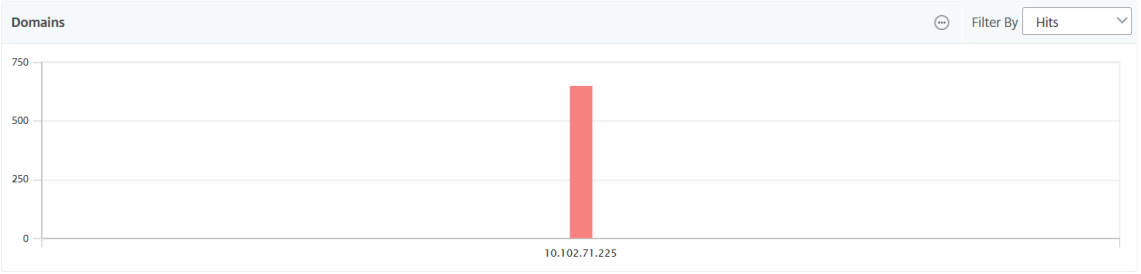
- **Bandwidth**（带宽）



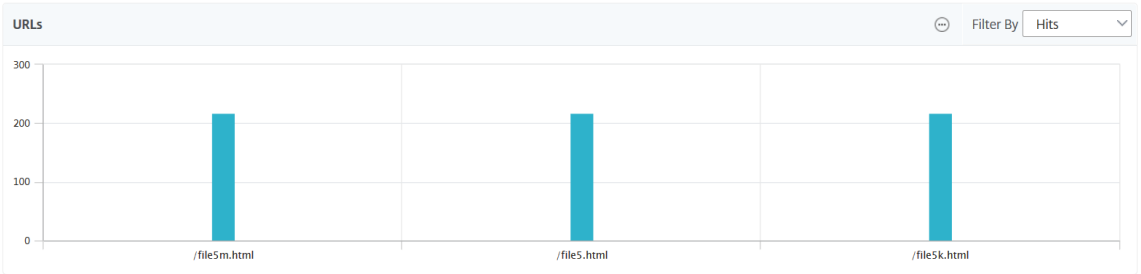
- 应用程序



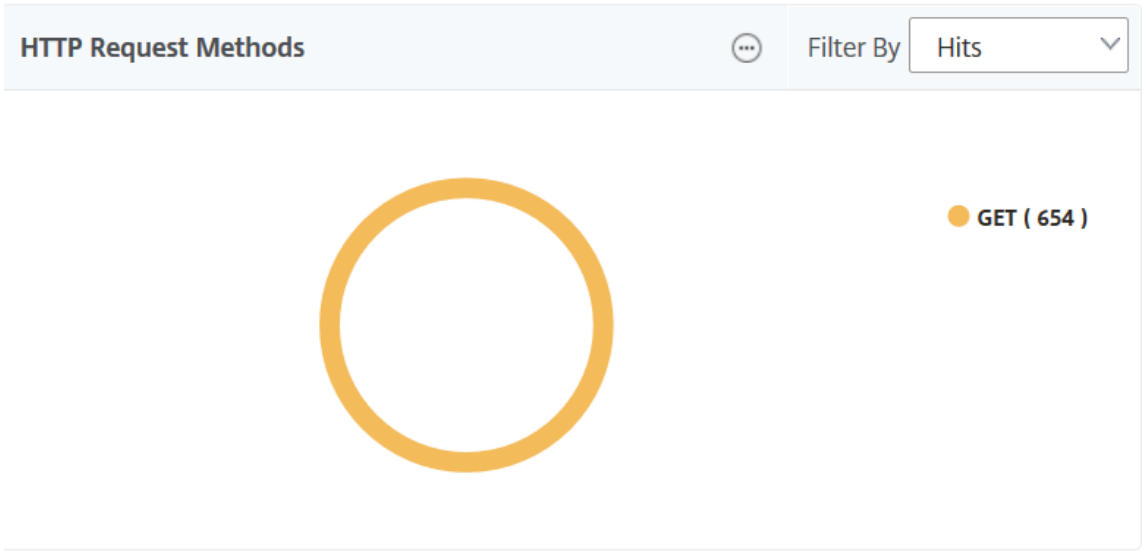
- 域



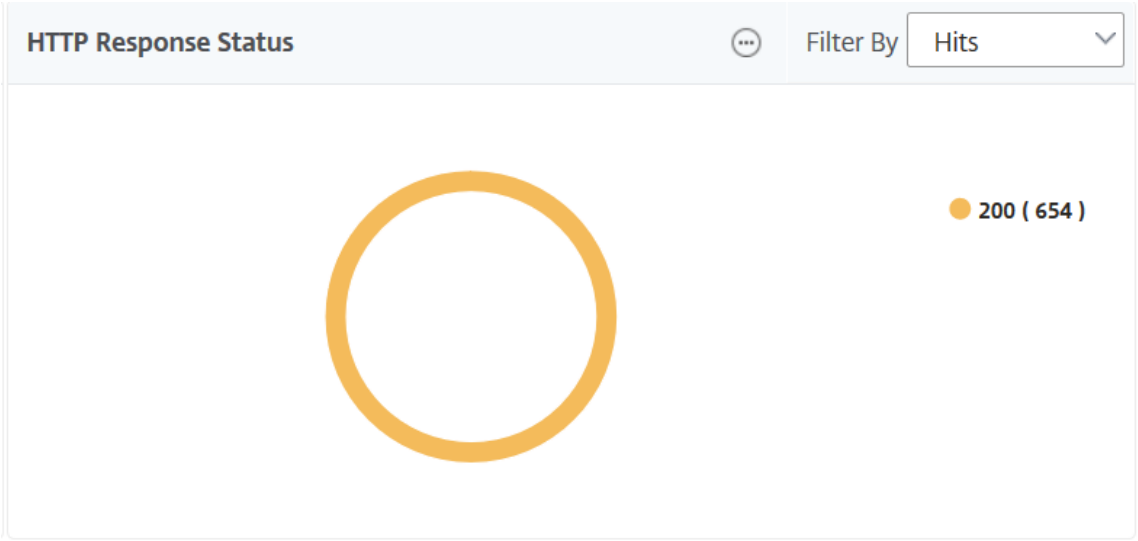
- **URL**



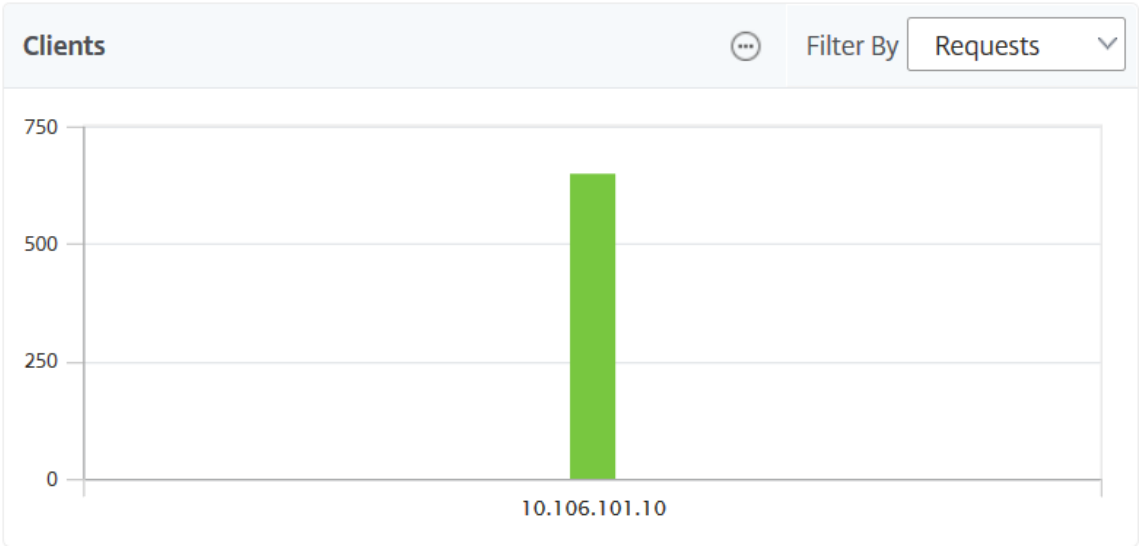
- **HTTP** 请求方法



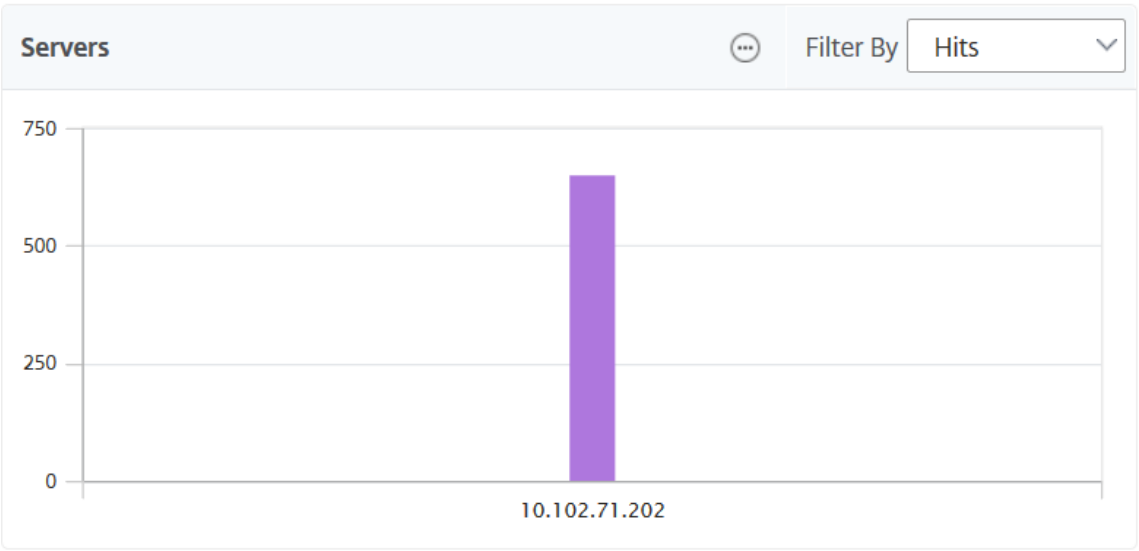
- **HTTP** 响应状态



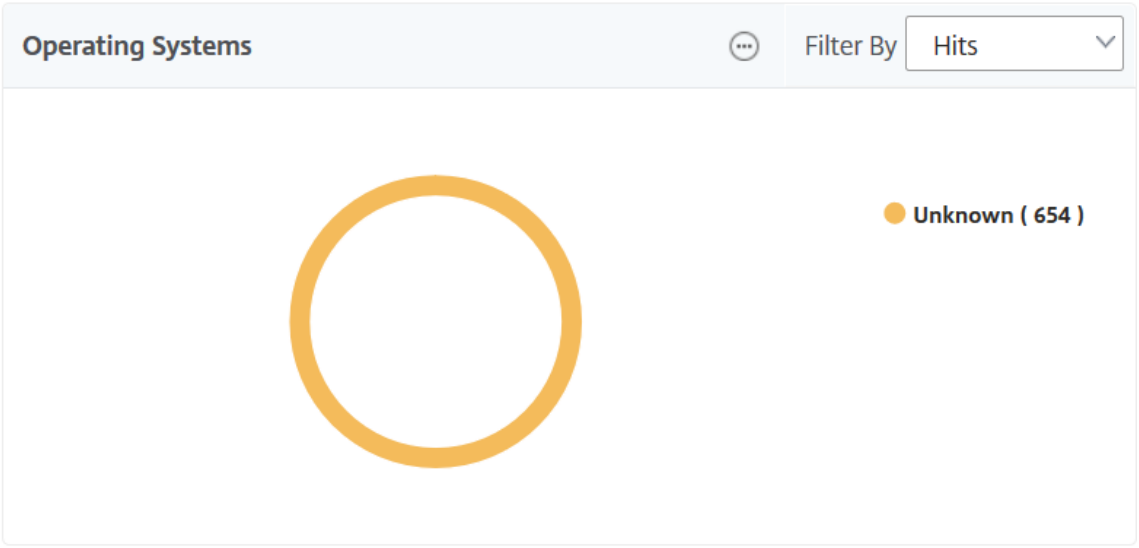
- 客户



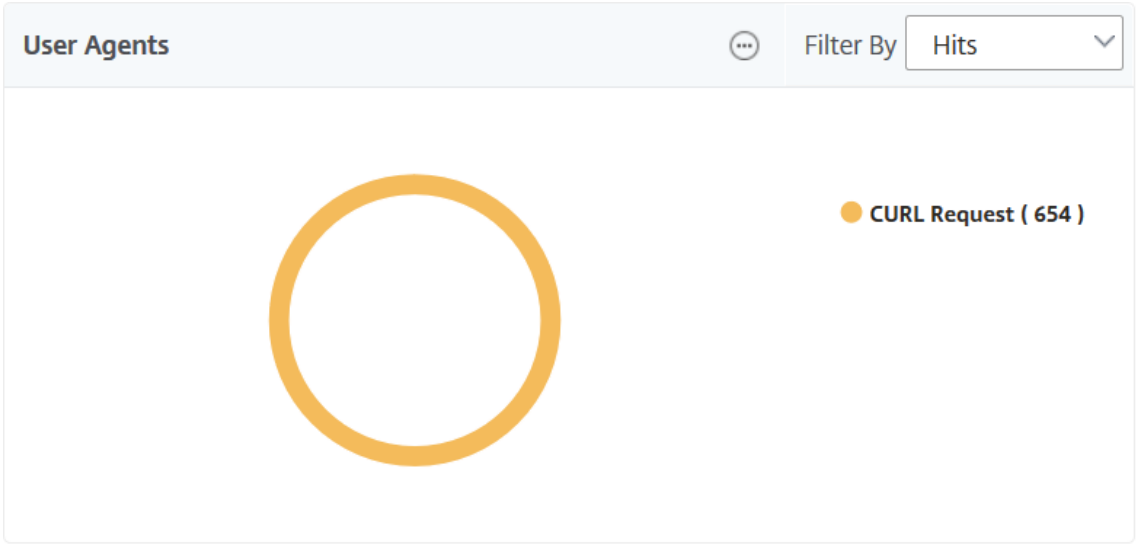
- 服务器



- 操作系统

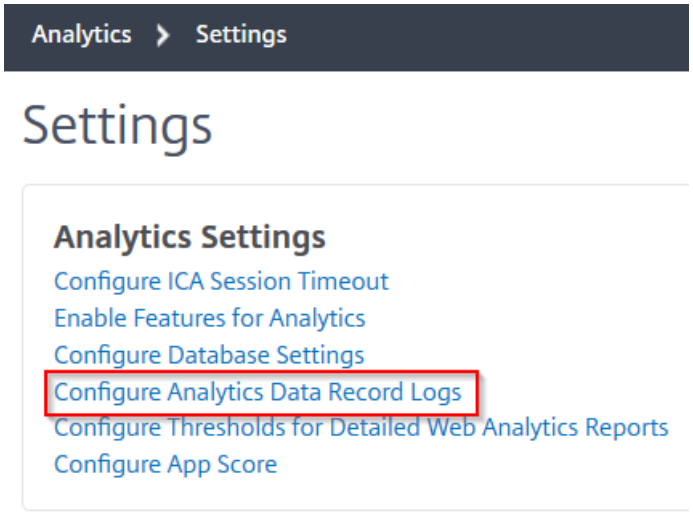


- **User Agents**（用户代理）

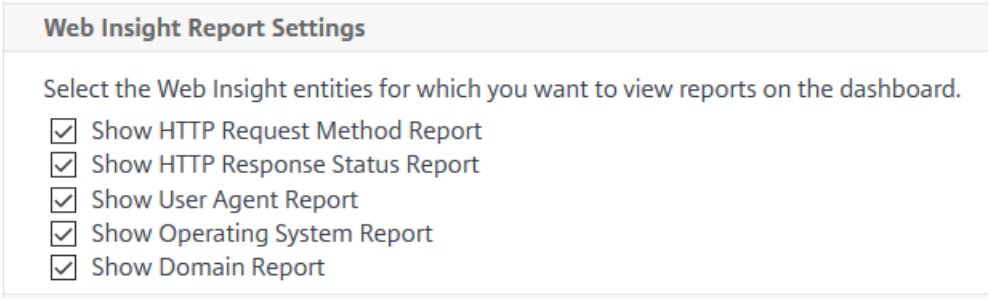


您还可以选择要在 GUI 上查看其报表的 **Web** 智能分析实体。

1. 导航到分析 > **Web Insight** > 设置。
2. 单击配置分析数据记录日志。



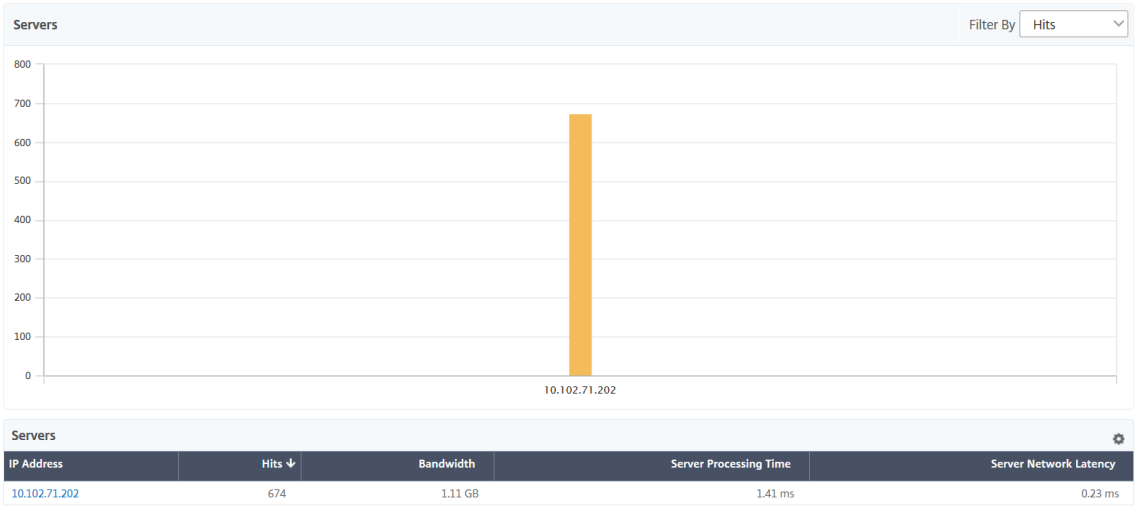
3. 在 **Web Insight** 报告设置下，选择要在 GUI 上查看报表的实体。



4. 单击确定。

要向下钻取进一步分析，您可以单击 GUI 中 “Web Insight” 下的每个洞察分类。例如，如果要检查已配置服务器的问题：

1. 导航到分析 > **Web Insight** > 服务器。
2. “服务器” 页面随所有已配置的服务器一起显示。
3. 单击图表中的 IP 地址。您也可以单击表中的 IP 地址。



此时将显示所选服务器的详细分析视图。从此视图中，您可以检查多个见解，例如：

- 服务器接收的点击总数
- Bandwidth（带宽）
- 服务器处理时间
- 服务器网络延迟
- 为服务器配置的虚拟服务器
- 访问服务器的客户端总数
- 服务器提供的响应代码总数

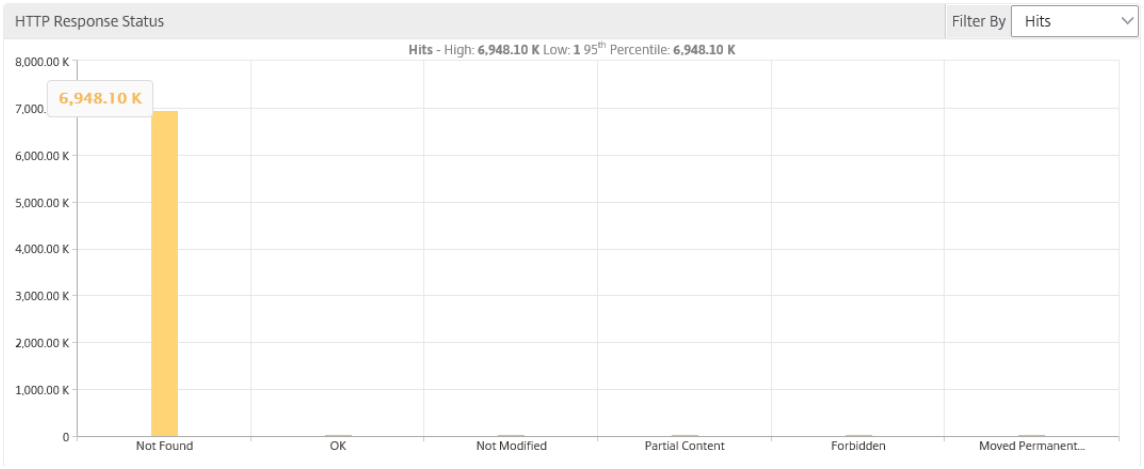
使用案例 **1-**内部服务器错误

考虑您的用户遇到 Web 应用程序无法访问错误 500 的情况。错误 500（未找到）是 HTTP 响应状态错误，指示 Web 服务器上的问题，但服务器没有明确说明问题。要确定并深入查看实际问题：

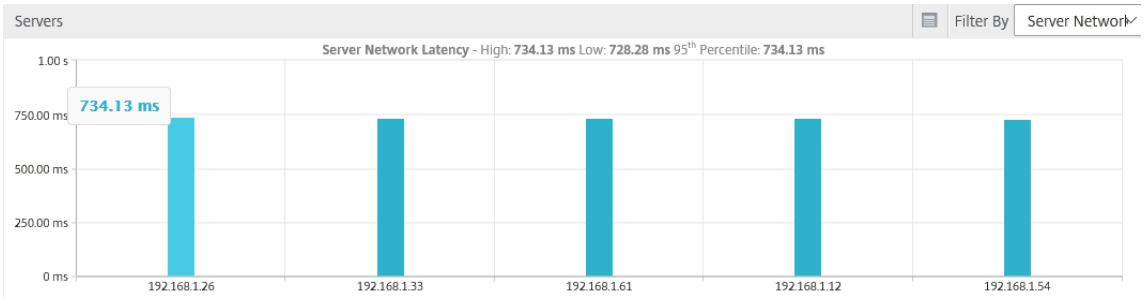
1. 导航到分析 > **Web Insight** > 响应状态。

   显示控制板页面。控制板为您提供了可用于分析所处理 HTTP 事务的成功和失败的指标。

2. 单击图表上的未找到。



3. 向下滚动以查看服务器图形，然后从筛选方式列表中选择服务器网络延迟。



该图表表明每个应用程序服务器在检索 Web 应用程序时都存在问题，因此 Web 服务器的响应时间会增加。问题可能是 Web 服务器没有响应来自任何服务器的任何请求。

使用案例 **2-**用户访问 **Web** 应用程序时遇到缓慢

考虑一种情况，即您的 Web 应用程序通过 10 个不同的 Web 服务器托管。当多个用户同时访问应用程序时，一个或多个用户可能会遇到应用程序缓慢。作为管理员，您必须分析以下情况以了解问题的根本原因：

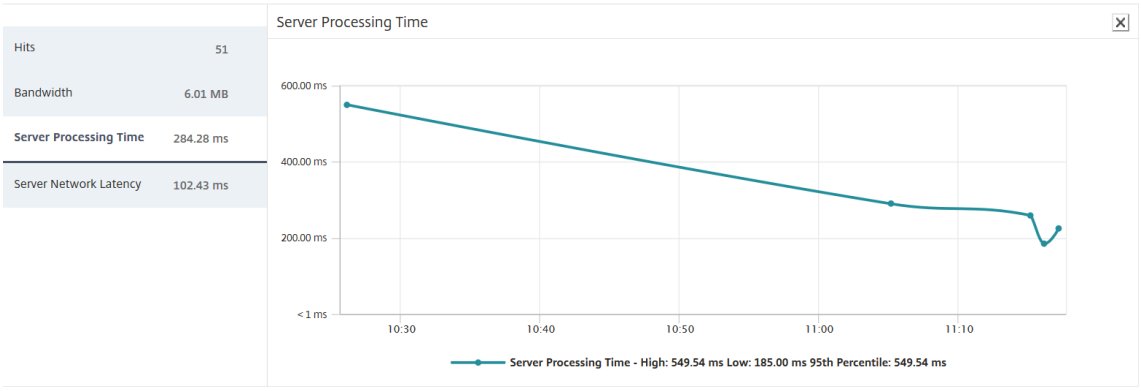
方案 **1-**服务器处理时间：

当多个请求同时触及 10 个 Web 服务器时，加载请求所花费的时间因以下因素而异：

- 队列中的请求数。
- 每个请求用于处理 HTTP 事务的带宽。

  服务器图可帮助您了解每台服务器对于服务器处理的请求的处理时间。同样，应用程序图显示每个 HTTP 事务的命中、响应时间和占用的带宽。

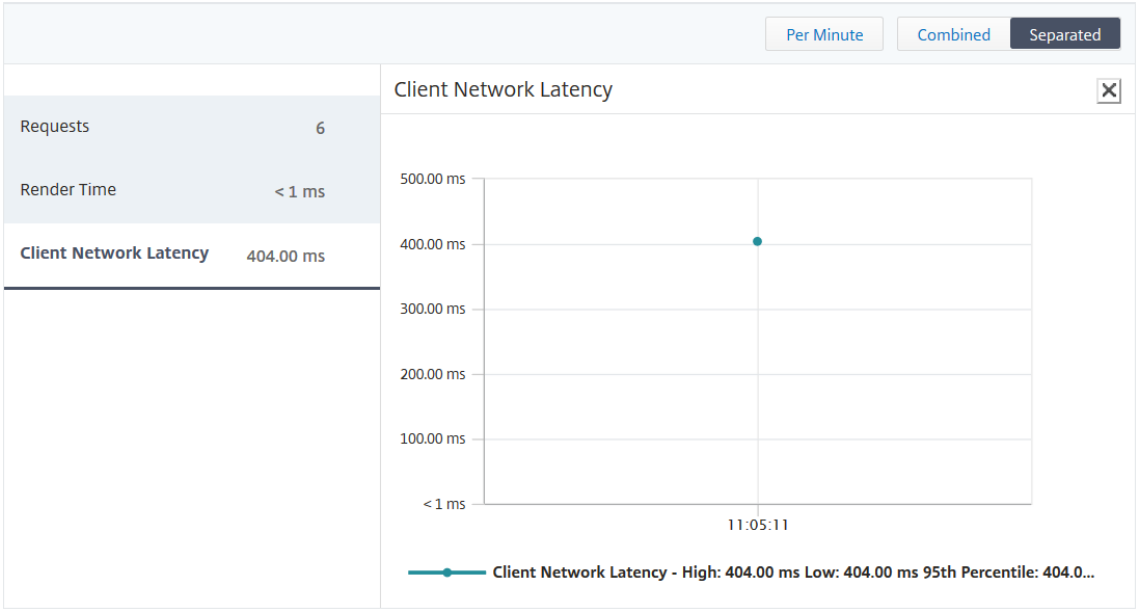
1. 导航到分析 > **Web Insight** > 服务器。
2. 从图表中选择服务器。
3. 单击服务器处理时间以分析服务器的处理时间。



场景 **2-**客户端延迟：

应用程序的响应时间和点击总数可能是应用程序访问缓慢的原因。您可以检查客户端网络延迟并分析客户端网络延迟的指标。要分析根本原因，请执行以下操作：

1. 导航到分析 > **Web Insight** > 客户端。
2. 从图表中选择客户端。
3. 单击客户端网络延迟分析高延迟。



在此示例中，作为管理员，您可以看到问题的根本原因来自客户端网络，因为客户端网络延迟表示高。

使用案例 **3-**访问 **Web** 应用程序的缓慢

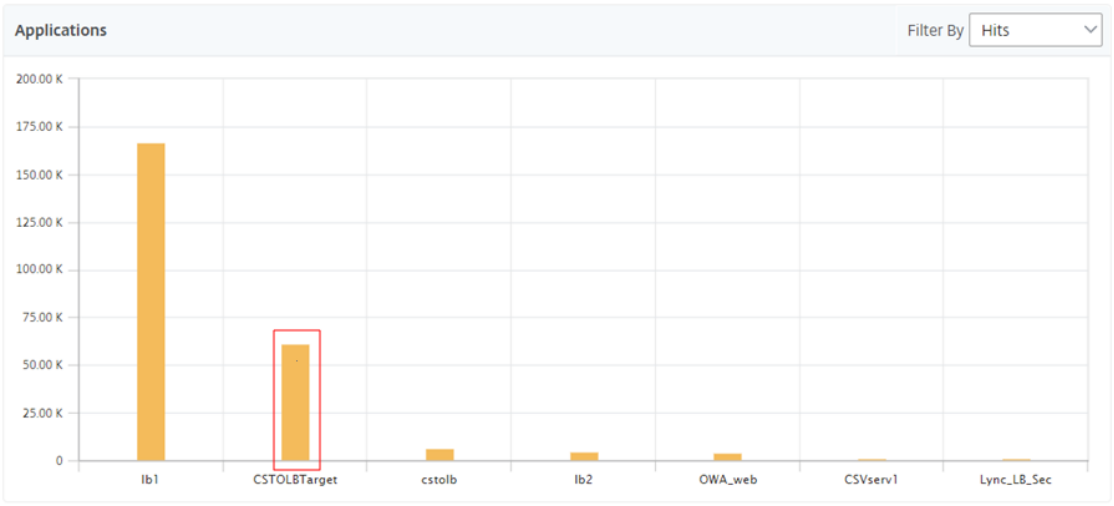
考虑一种情况，即您拥有适用于 Windows 用户的 Web 服务器和适用于 Mac 用户的 Web 服务器，并且您的用户报告访问 Web 应用程序的速度缓慢。作为管理员，您知道您拥有：

- 为 Windows 用户配置了内容交换虚拟服务器。

- 为 Mac 用户配置了内容交换虚拟服务器。
- 配置绑定到虚拟服务器的关联服务，以便基于 Windows 和 Mac 用户重定向请求。

要分析 Web 应用程序缓慢问题的根本原因，请执行以下操作：

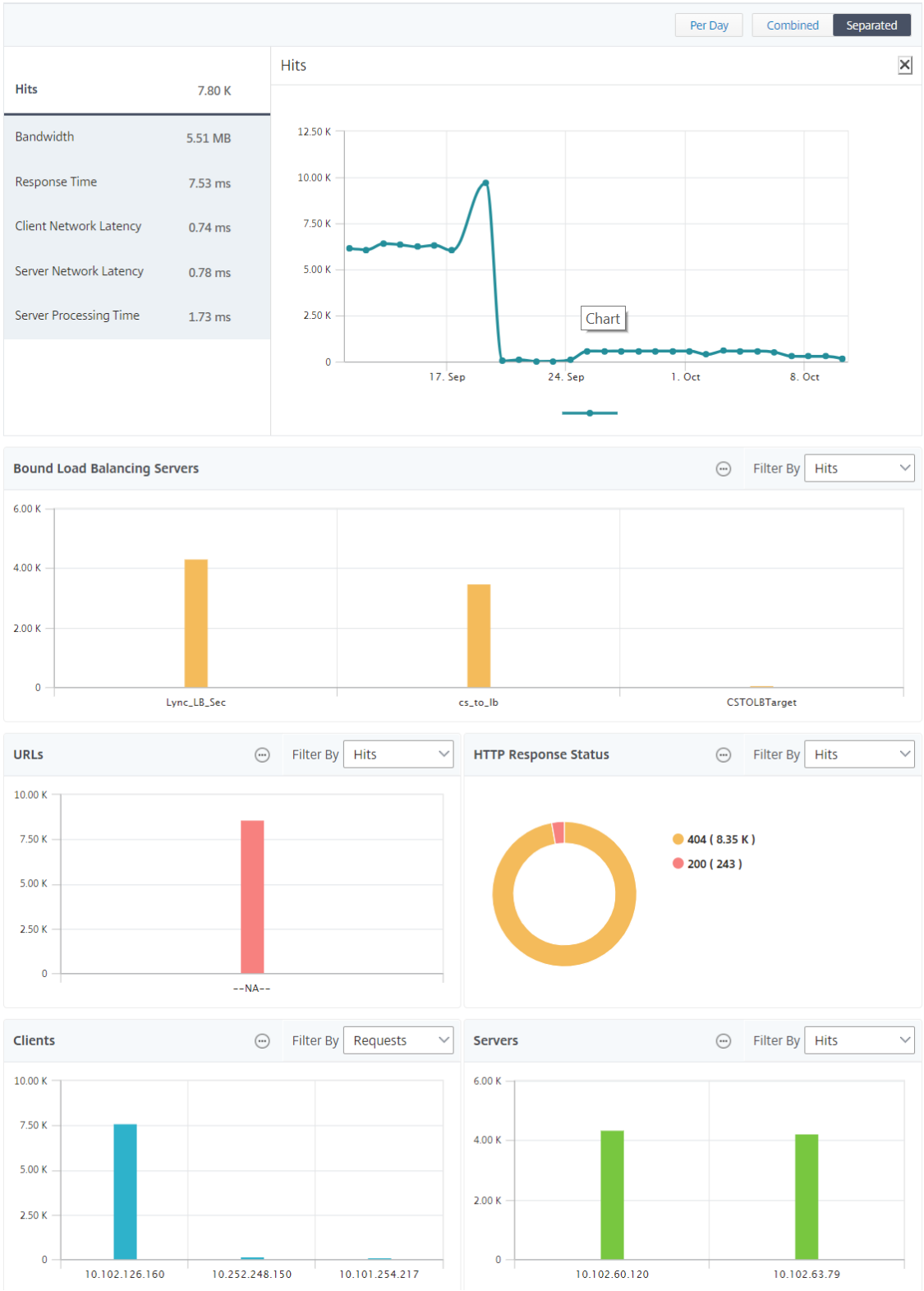
1. 导航到分析 > **Web Insight** > 应用程序
2. 选择内容交换虚拟服务器。
   例如，映像中的 “CstolbTarget” 应用程序是绑定到其他负载平衡虚拟服务器的内容交换虚拟服务器



Applications

Name	Hits	Bandwidth	Response Time
lb1	167.05 K	136.74 MB	0.74 ms
CSTOLBTarget	61.06 K	60.14 MB	8.66 ms
cstolb	6.61 K	4.80 MB	374.97 ms
lb2	4.83 K	3.61 MB	0.67 ms
OWA_web	4.31 K	3.27 MB	3.21 ms
CSVserv1	291	184.82 KB	157.12 ms
Lync_LB_Sec	10	12.63 KB	86.43 ms

3. 单击内容交换虚拟服务器以查看其他负载平衡虚拟服务器。也可以单击表中的应用程序名称。



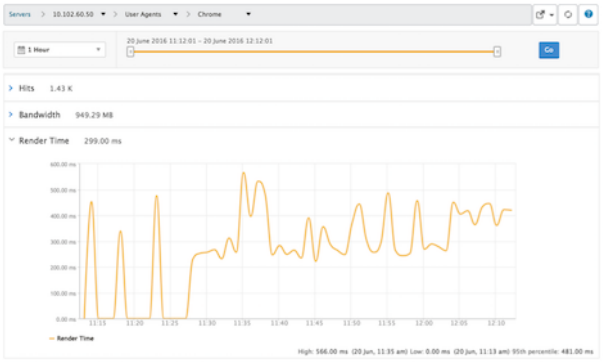
您可以进一步单击绑定的负载平衡服务器以查看这些应用程序的 Web 智能分析详细信息。

分析浏览器和操作系统的见解

可以使用 Web Insight 来帮助您区分 L7 延迟问题，并了解移动设备使用情况。作为管理员，见解可以帮助您了解整个用户群的不同操作系统使用情况。

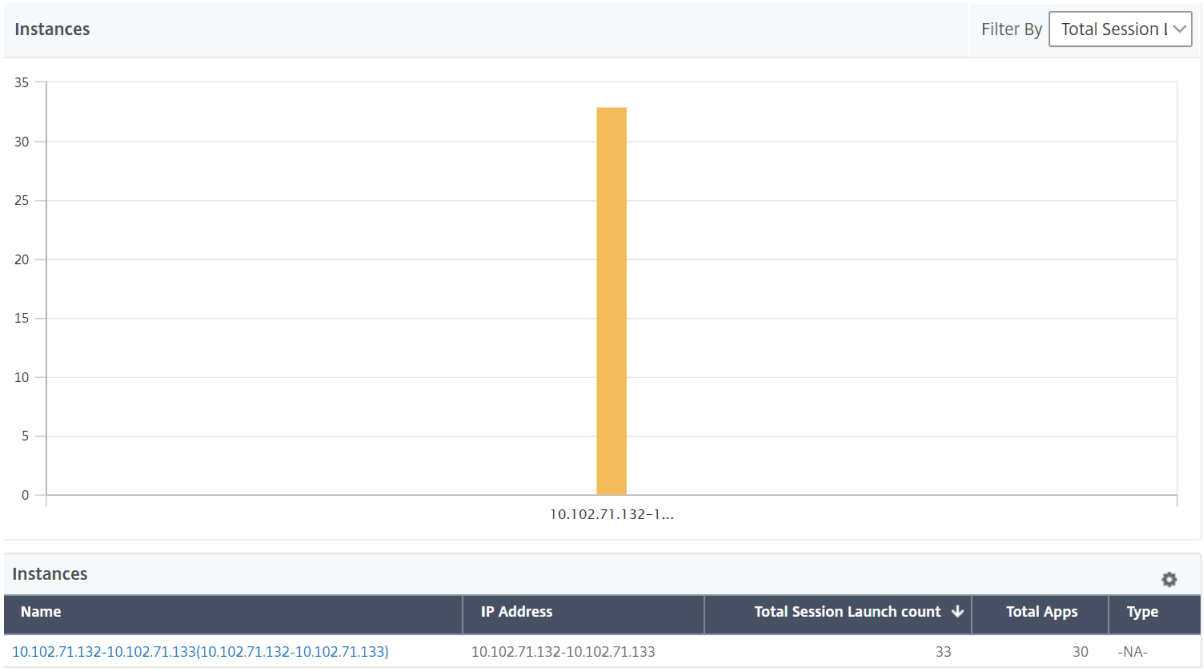
导航到分析 > **Web Insight** > 操作系统，了解用户访问速度缓慢的原因，以及是否由于某些浏览器之间的不兼容。还可以查看某些客户端上在使用哪些操作系统，以及在访问哪些浏览器。您可以比较不同浏览器之间的渲染时间，然后进一步深入查看特定浏览器，以确定哪些应用程序页面与该浏览器的最长渲染时间相关联。

例如，您可以选择 **Google Chrome** ，然后查看特定应用程序的不同 URL 页面的相应渲染时间。

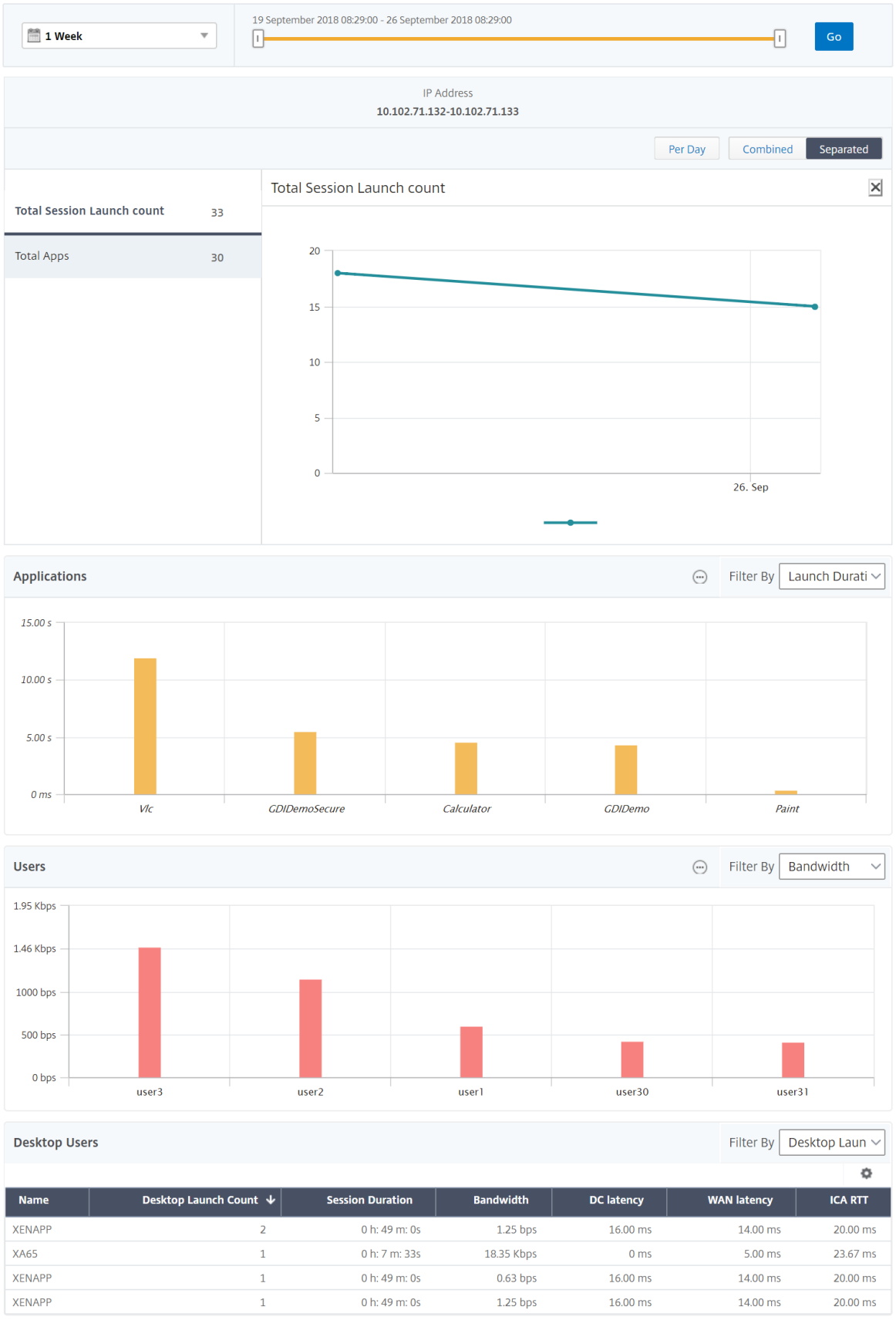


在高可用性模式下部署的 **Citrix ADC** 实例

Citrix ADM 为在高可用性模式下部署的 ADC 实例提供报告。所有分析都支持高可用性模式下实例的汇总报告。



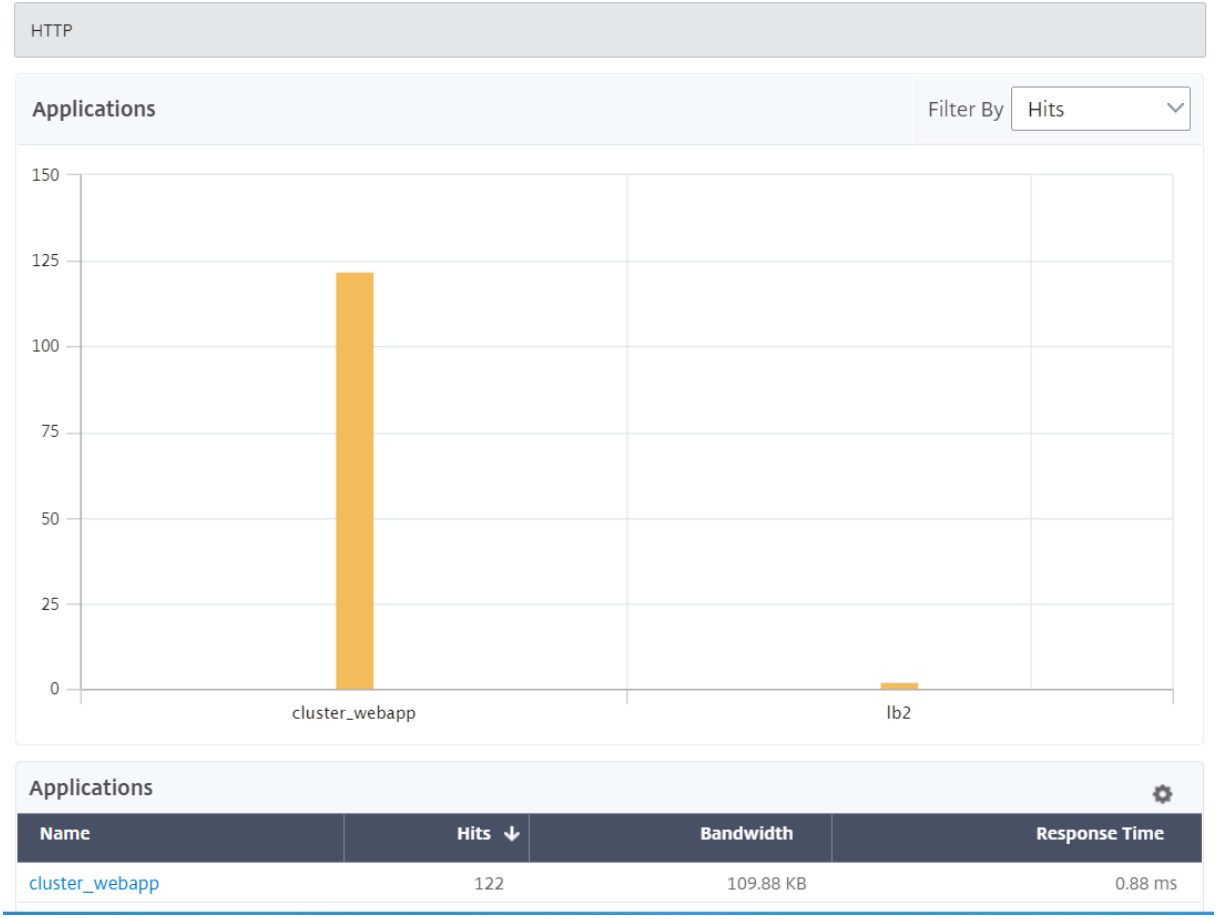
您可以单击处于高可用性的实例的名称以查看更多详细信息。



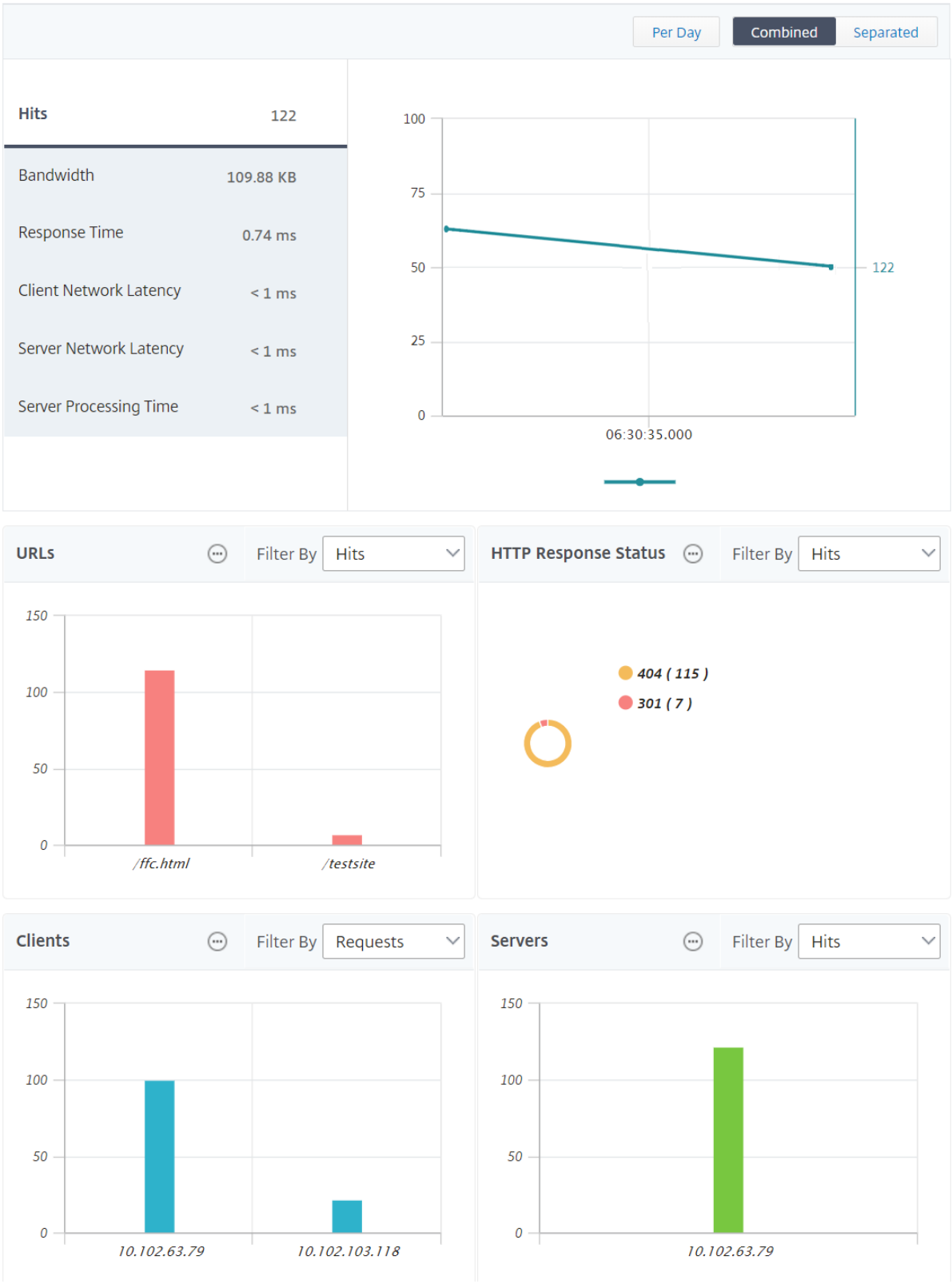
Name	Desktop Launch Count	Session Duration	Bandwidth	DC latency	WAN latency	ICA RTT
XENAPP	2	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms
XA65	1	0 h: 7 m: 33s	18.35 Kbps	0 ms	5.00 ms	23.67 ms
XENAPP	1	0 h: 49 m: 0s	0.63 bps	16.00 ms	14.00 ms	20.00 ms
XENAPP	1	0 h: 49 m: 0s	1.25 bps	16.00 ms	14.00 ms	20.00 ms

以群集模式部署的 **Citrix ADC** 实例

Citrix ADM 为在群集模式下部署的 ADC 实例提供报告。所有分析都支持群集模式下的实例的聚合报告。



您还可以单击 **CLIP** 主机名以查看有关在集群模式下部署的 ADC 实例的所有详细信息。



> 注意
>
> - 升级到 Citrix ADM 12.1 版本 503.x 之前以前收集的所有数据在数据保留之前仍显示为独立报告。
> - 对于在群集模式下部署的 ADC 实例，观察域 ID/ 观察域名将替换为 CLIP 主机名和 CLIP。以前收集的所有数据都将继续报告观察域 ID/观察域名。

Web Insight 地理地图配置

Citrix ADM 中的地理地图功能显示了地图上不同地理位置的 Web 应用程序的使用情况。管理员可以使用此信息了解应用程序使用趋势和容量规划。

Geo map 提供了有关特定于国家/地区、州和城市的以下指标的信息：

- 点击总数：访问应用程序的总次数。
- 带宽：服务客户端请求时消耗的总带宽
- 响应时间：向客户端请求发送响应所用的平均时间。

Geommap 提供的信息可用于解决以下几个使用案例：

- 访问应用程序的客户端数最大的区域
- 响应时间最长的区域
- 消耗最多带宽的区域

Citrix ADM 为您提供了一个选项来配置私有 IP 地址或公有 IP 地址的地理地图。

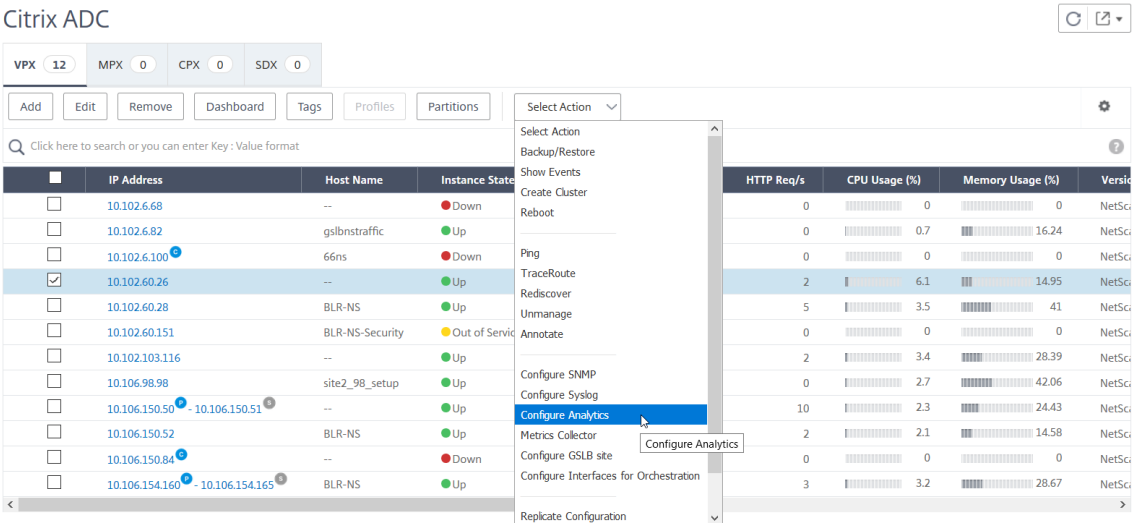
为私有 **IP** 地址配置地理地图

> 注意
>
> 仅当您的 Citrix ADM 为 **13.0** 版本 **36.27** 或更早版本时，以下过程才适用。对于 Citrix ADM **13.0** 版本 **41.x** 或更高版本，在启用 Web 智能分析时自动启用地理数据收集。

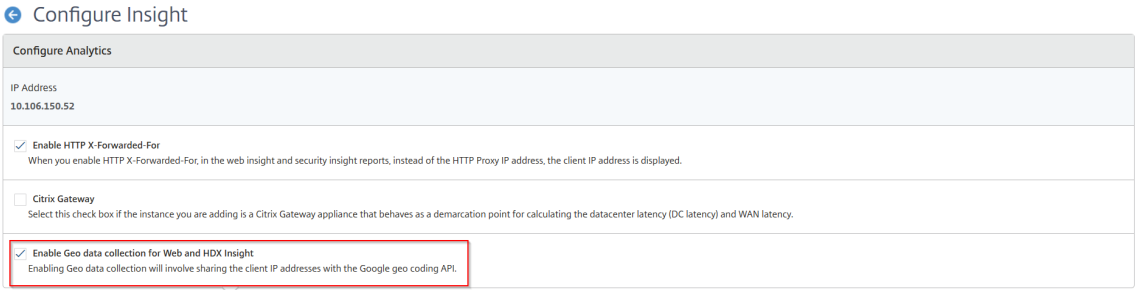
要查看来自地理映射上私有 IP 地址的 Web 应用程序流量，必须首先创建私有 IP 地址块，然后启用地理数据收集。

要启用地理数据收集，请执行以下操作：

1. 导航到网络 > 实例 > **Citrix ADC**，然后选择 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。



3. 在配置 **Insight** 页面上，选择为 **Web** 和 **HDX Insight** 启用地理数据收集。



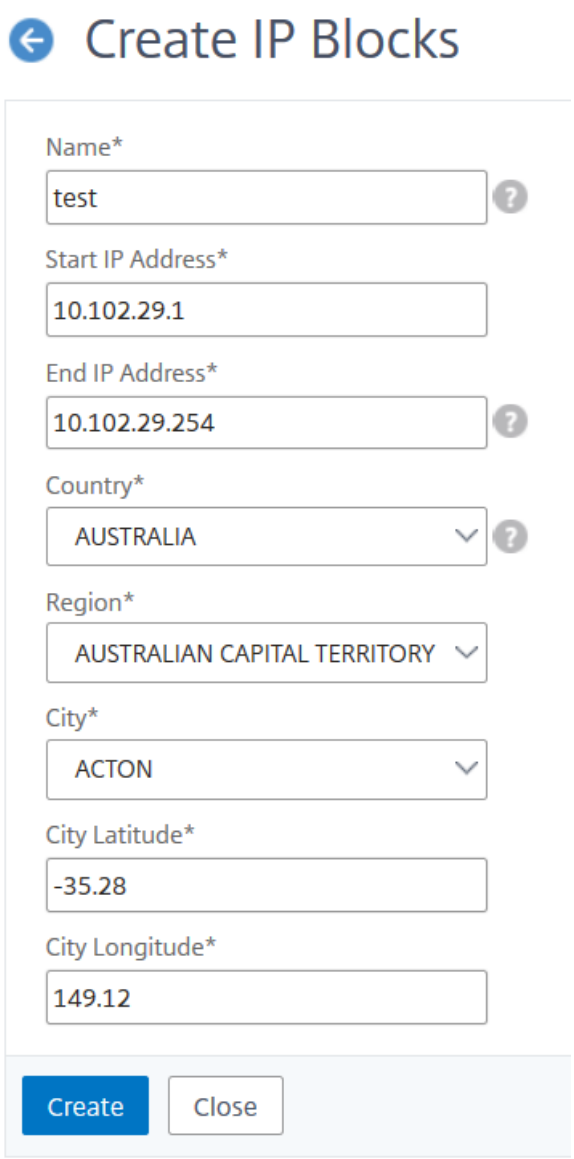
创建私有 **IP** 块

将客户端私有 IP 地址添加到 Citrix ADM 服务器时，Citrix ADM 可以识别客户端的位置。例如，如果客户端的 IP 地址属于与 City A 相关联的私有 IP 地址块的范围内，Citrix ADM 会识别此客户端的流量来自 A 城市。

要创建 IP 块，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 > 设置 > **IP** 块，然后单击添加。
2. 在创建 **IP** 块页面中，指定以下参数：
   - 名称。指定专用 IP 块的名称
   - 启动 **IP** 地址。指定 IP 块的最低 IP 地址范围。
   - 结束 **IP** 地址。指定 IP 块的最大 IP 地址范围。
   - 国家。从列表中选择国家/地区。
   - 区域。根据国家/地区，该地区是自动填充的，但您可以选择您的地区。
   - 城市。根据区域，该城市是自动填充的，但您可以选择您的城市。
   - 城市纬度和城市经度。根据您选择的城市，纬度和经度会自动填充。

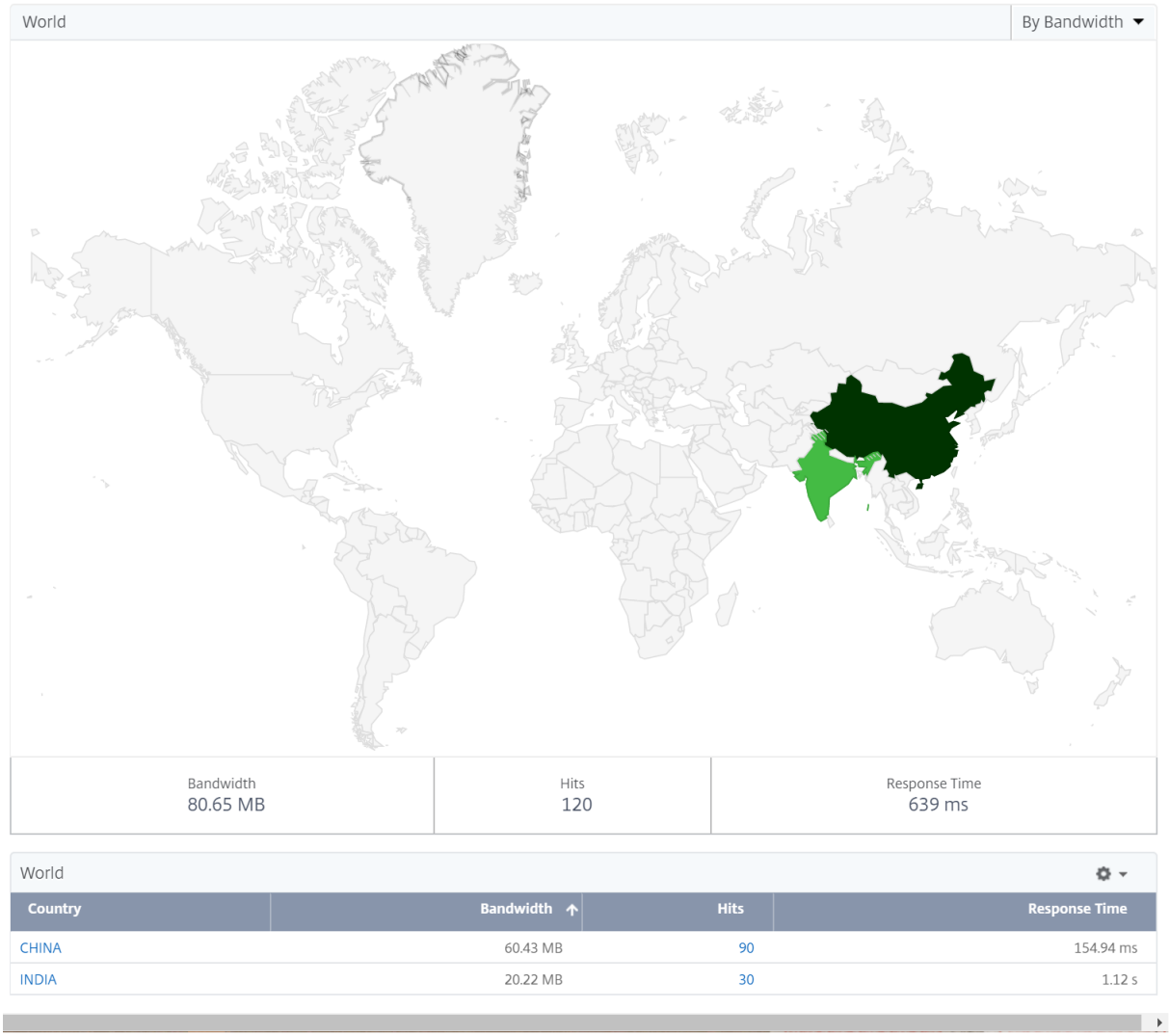
3. 单击 **Create**（创建）完成。



公共 **IP** 块

如果客户端使用公有 IP 地址，Citrix ADM 还可以识别客户端的位置。Citrix ADM 具有其内置位置 CSV 文件，该文件与基于客户端 IP 地址范围的位置匹配。对于使用公有 IP 块，唯一的要求是必须从配置智能分析页面启用启用地理数据收集。

> 注意
>
> Citrix ADM 需要互联网连接才能显示特定地理位置的地理地图。还需要互联网连接才能以.pdf、.png 或.jpg 格式导出 GeoMap。



要导出此控制板的报告，请执行以下操作：

要导出此页面的报告，请单击此页面右上角的 导出图标。在 导出页面上，您可以执行以下操作之一：

1. 选择立即导出选项卡。查看并保存 PDF、JPEG、PNG 或 CSV 格式的报告。
2. 选择 计划导出选项卡。每天、每周或每月安排报告，并通过电子邮件或松弛消息发送报告。

> 注意
>
> - 如果您选择 每周定期”，请确保您选择要计划报表的工作日。
> - 如果选择 每月重复，请确保输入希望报告以逗号分隔的所有日期。

配置阈值

您可以创建阈值，并在阈值超出时获得通知。在典型部署中，您可以将阈值设置为：

- 跟踪各种应用程序指标

- 促进规划
- 每当应用程序度量值超过设定阈值时收到通知

要配置阈值：

1. 导航到分析 > 设置 > 阈值。
2. 在阈值页面上，单击添加。

   此时将显示创建阈值页面。
3. 指定以下详细信息：

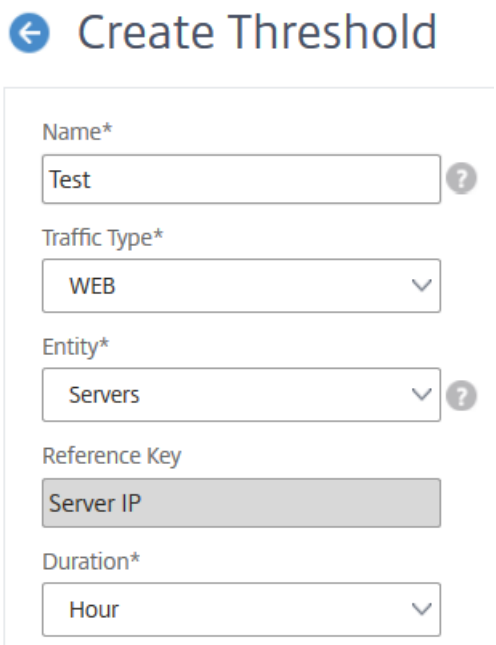
   a) 名称 -指定用于创建事件的名称。

   b) 通信类型 -从列表中选择 WEB。

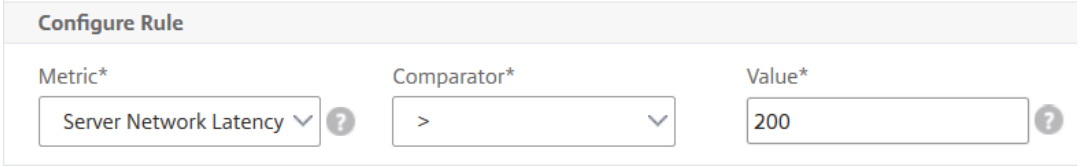
   c) 实体 -从列表中选择类别或资源类型。默认情况下，选择“应用程序”作为实体。

   d) 引用键 -根据您选择的流量类型和实体自动生成引用键。

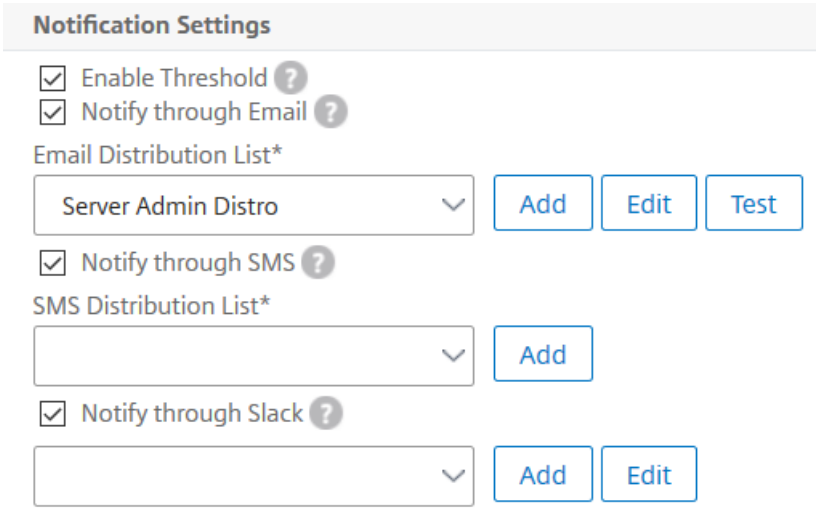
   e) 持续时间-从列表中选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。



   f) 在配置规则部分，通过选择指标和所需的比较器来创建规则，并提供阈值。



   g) 在通知设置部分中，选择启用阈值和要获取警报的警报模式。



4. 单击创建。

排除 **Web** 智能分析问题

有关详细信息，请参阅故障排除文档 排除 Web 智能分析问题。

排除 **Web** 智能分析问题

April 23, 2021

借助 Citrix ADM Web 智能分析仪表板，您可以直观地显示应用程序使用情况，并监视 Citrix ADC 实例所服务的所有 Web 应用程序。使用 Web 智能分析，ADC 实例将 HTTP 和 SSL 事务数据发送到配置为 AppFlow 收集器的 ADM。AppFlow 是用于识别和收集网络基础架构中的应用程序和事务数据的流导出标准。

本文档帮助您解决常见的 Web Insight 部署问题。

与 **Citrix ADM Web** 智能分析仪表板报告相关的问题

如果 ADM Web 智能分析仪表板（**ADM GUI >** 分析 **> Web** 智能分析）无法显示报告，则问题可能是以下问题之一：

- Web 智能分析配置问题
- Citrix ADC 和 Citrix ADM 之间的连接问题
- 计数器问题
- 许可证问题
- 观察点 ID 问题
- 缺少 AppFlow 参数问题

配置问题：**Citrix ADM Web** 智能分析不显示报告

请完成以下步骤来解决此问题：

1. 确保在 Citrix ADC 实例中启用了 AppFlow 功能。有关详细信息，请参阅启用 AppFlow。
2. 检查 ADC 实例中的 Web 智能分析配置：
   a) 运行 `show running | grep -i <appflow_policy>` 命令以检查策略上的 Web Insight 配置。确保绑定类型为 `REQUEST`。例如：`bind lb vserver afsanity -policy afp -priority 100 -type REQUEST`
   b) 运行 `show appflow action` 命令以检查 Web Insight 配置的操作。确保已启用该 `-webinsight` 选项
   c) 适当检查 `appflowlog` LB/CS/CR 虚拟服务器中的参数。确保启用此参数。

Citrix ADC 和 **Citrix ADM** 之间的连接问题：**Citrix ADM Web** 智能分析不显示报告

请完成以下步骤来解决此问题：

1. 检查 Citrix ADC 中的应用流收集器状态。有关详细信息，请参阅如何检查 Citrix ADC 和 AppFlow 收集器之间的连接状态。
2. 在 ADC GUI 上，检查 AppFlow 策略是否获得命中。运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中情况。您还可以导航到 GUI 中的 **“系统” > “AppFlow” > “**策略”，以检查 AppFlow 策略命中。
3. 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

计数器问题：**Citrix ADM Web** 智能分析不显示报告

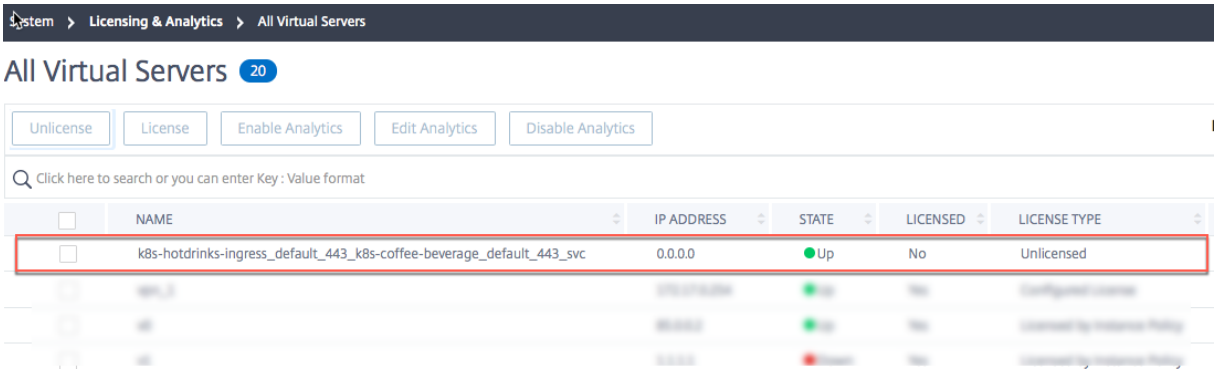
请完成以下步骤来解决此问题：

1. 确保没有 AppFlow 配置和连接问题。有关详细信息，请参阅本主题中的解决方案部分，了解 Citrix ADC 和 Citrix ADM 之间的配置问题和连接问题。
2. 在 ADC 实例上，在 shell 提示符下，运行 `nsconmsg -g appflow_tmpl -d current` 命令并检查以下计数器：
   - `appflow_tmpl_v4_l7_clt2ns_complete`
   - `appflow_tmpl_v4_l7_srvr2ns_complete`
   - `appflow_tmpl_v46_ulfd_client_eot`
   - `appflow_tmpl_v46_ulfd_server_eot`

   如果任何计数器丢失，请跟踪 ADC 实例。接下来，确认事务已完成，并且正在从源服务器提供响应。如果事务是正确的，并且某些计数器丢失，请提交一个错误。

许可证问题：**Citrix ADM Web** 智能分析不显示报告

出现此问题时，要查看 Web Insight 报告的特定虚拟服务器的许可证显示在 “ 系统” > “许可证和分析” > “配置许可证” 下。



请完成以下步骤来解决此问题：

1. 在 ADC 实例中，确保 AppFlow 策略命中增加，并且实例正在将 AppFlow 记录发送到 ADM
2. 检查相应的虚拟服务器是否已获得许可。如果虚拟服务器未获得许可，ADM 会丢弃 AppFlow 记录。因此，不会显示 Web 智能分析报告。

观察点 **ID** 问题：**Citrix ADM Web** 智能分析不显示报告

出现此问题的原因是观察点 ID 不唯一。

> 注意：
> 观测点 ID 是要从中导出 AppFlow 记录的 Citrix ADC 的标识符。默认情况下，Citrix ADC IP 是观测点 ID。

请完成以下步骤来解决此问题：

1. 在 ADC 实例中，确保 AppFlow 策略命中增加，并且实例正在将 AppFlow 记录结束到 ADM。
2. 检查相应的虚拟服务器是否获得许可。
3. 确保配置不会从一个 ADC 实例复制到另一个实例。复制时，配置可能会产生导出程序 ID 问题，从而导致 ADM 删除 AppFlow 记录。
4. 登录 ADC 实例并运行 `unset appflow param -observationpointId` 命令。

缺少 **AppFlow** 参数问题：**Citrix ADM Web** 智能分析不显示报告

出现此问题的原因是 ADM 丢失 AppFlow 记录由于缺少数据。

请完成以下步骤来解决此问题：

1. 确保在 ADC 实例中，AppFlow 策略命中不断增加，并且实例正在将 AppFlow 记录结束到 ADM。
2. 检查相应的虚拟服务器是否获得许可。
3. 确保配置不会从一个 ADC 实例复制到另一个实例。复制时，配置可能会产生导出程序 ID 问题，从而导致 ADM 删除 AppFlow 记录。

4. 确保在 ADC 实例上启用了以下 AppFlow 参数：
   a) `HTTP method logging`
   b) `HTTP domain name logging`
   c) `HTTP URL logging`
   d) `HTTP host logging`
   e) `HTTP Content-Type header logging`

Citrix ADM Web 智能分析杂项问题

- 问题：在 HTTP 客户端上，启用 AppFlow 时不会加载页面。
- 解决方案：完成以下步骤来解决此问题：

  1. 在 AppFlow 操作命令中，禁用“页面跟踪”功能 `set appflow action <name> -pageTracing disable`。此操作对功能没有影响。

  如果问题未解决，请执行以下步骤：

  1. 在同一操作中，取消设置要 `clientsidemeasurement` 素 `set appflow action <name> -clientsidemeasurements disable`。如果此步骤解决了问题，请捕获 ADC 实例上的跟踪并提交错误。

- 问题：启用 AppFlow 时，ADC 装置崩溃。
- 解决方案：完成以下步骤来解决此问题：

如果回溯跟踪 (BT) 具有 AppFlow 功能，则问题可能出在 AppFlow 功能中。如果 BT 位于特定于功能的代码中，则问题可能在于那些使用 AppFlow 向收集器发送数据的功能。
在后一种情况下，禁用任何特定于功能的 AppFlow 配置并验证。请勿在全局禁用 AppFlow 功能，因为此步骤不会对此问题提供太多的见解。

使用计数器进行故障排除

检查以下 AppFlow 计数器是否存在任何 AppFlow 或 Web 智能分析相关问题。

Counter	说明
`appflow_tot_record_drop`	由于收集器无效而丢弃的 AppFlow 记录。通常情况下，收集器配置发生变化，并且现有连接使用旧的收集器配置。
`lstream_tot_trans_written`	此计数器必须为要记录的每个事务递增。
`lstream_sent`	此计数器为发送的每个事务日志增加。

HDX Insight

April 23, 2021

HDX 智能分析为通过 Citrix ADC 传输到 Citrix Virtual Apps 和桌面的 HDX 流量提供端到端的可视性。它还让管理员能够查看实时客户端和网络延迟指标、历史报告和端到端性能数据，以及对性能问题进行故障排除。实时和历史可见性数据的可用性使 Citrix Application Delivery Management (ADM) 能够支持各种使用案例。

要显示任何数据，您需要在 Citrix Gateway 虚拟服务器上启用 AppFlow。AppFlow 可以通过 IPFIX 协议或日志流方法传递。

> 注意
>
> 要允许记录 ICA 往返行程时间计算，请启用以下策略设置：

- ICA 往返行程计算
- ICA 往返行程计算间隔
- 空闲连接的 ICA 往返行程计算

如果单击单个用户，则可以看到该用户在所选时间范围内创建的每个 HDX 会话，无论是活动的还是终止的。其他信息包括会话期间消耗的几个延迟统计信息和带宽。您还可以从各个虚拟通道（如音频、打印机映射和客户端驱动器映射）获取带宽信息。

> 注意：
>
> 创建组时，您可以将角色分配给组，提供对组的应用程序级访问权限，并将用户分配到组。Citrix ADM 分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有关组和向组分配用户的详细信息，请参阅 配置组。

您还可以导航到 **HDX Insight** > 应用程序，然后单击 启动持续时间以查看应用程序启动所花费的时间。您还可以通过导航到 **HDX Insight->** 用户查看所有连接用户的用户代理。

> 注意 HDX 分析支持在软件版本 12.0 上运行的 Citrix ADC 实例中配置的管理分区。

下列瘦客户端支持 HDX Insight：

- 基于 WYSE Windows 的瘦客户端
- 基于 WYSE Linux 的瘦客户机
- 基于 WYSE ThinOS 的瘦客户端
- 基于 10Zig Ubuntu 的瘦客户机

找出低性能问题的根本原因

场景 **1**

用户在访问 Citrix Virtual Apps and Desktops 时遇到延迟。

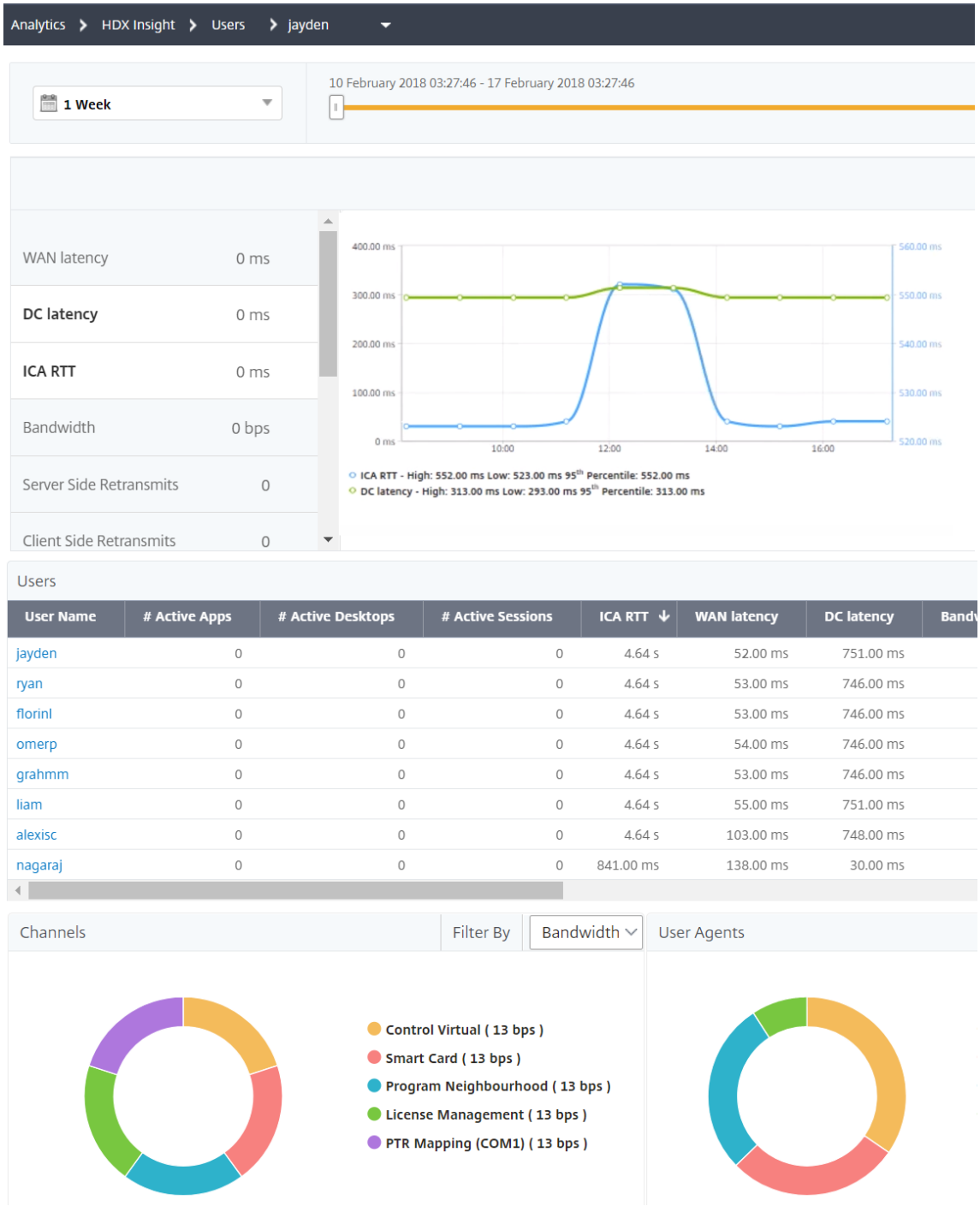
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟或客户端网络延迟造成。

为了找出问题的根本原因，请分析下列指标：

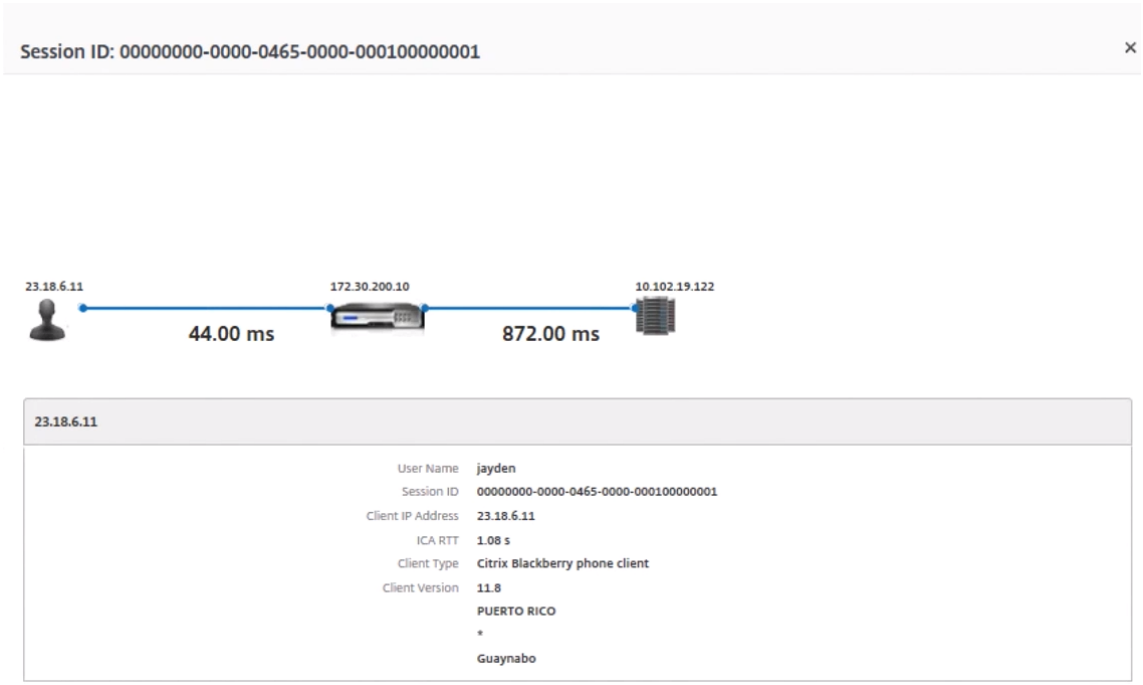
- WAN 延迟
- DC 延迟
- 主机延迟

要查看客户端度量，请执行以下操作：

1. 在“分析”选项卡上，导航到“**HDX Insight** 能分析”>“用户”。
2. 向下滚动并选择用户名，然后从列表中选择句点。期间可以是一天、一周、一个月，甚至可以自定义要查看数据的期间。
3. 图表以图形形式显示用户在指定时间段内的 ICA RTT 和 DC 延迟值。



4. 在“当前会话”表中，将鼠标悬停在 **RTT** 值上，并记下主机延迟、DC 延迟和 WAN 延迟值。
5. 在“当前会话”表中，单击跳图符号以显示有关客户端与服务器之间连接的信息，包括延迟值。



摘要

在此示例中，**DC** 延迟为 751 毫秒，**WAN** 延迟为 52 毫秒，主机延迟为 6 秒。这表示由于服务器网络导致的平均延迟，用户正在遇到延迟。

方案 **2**

用户在 Citrix 虚拟应用程序或桌面上启动应用程序时遇到延迟

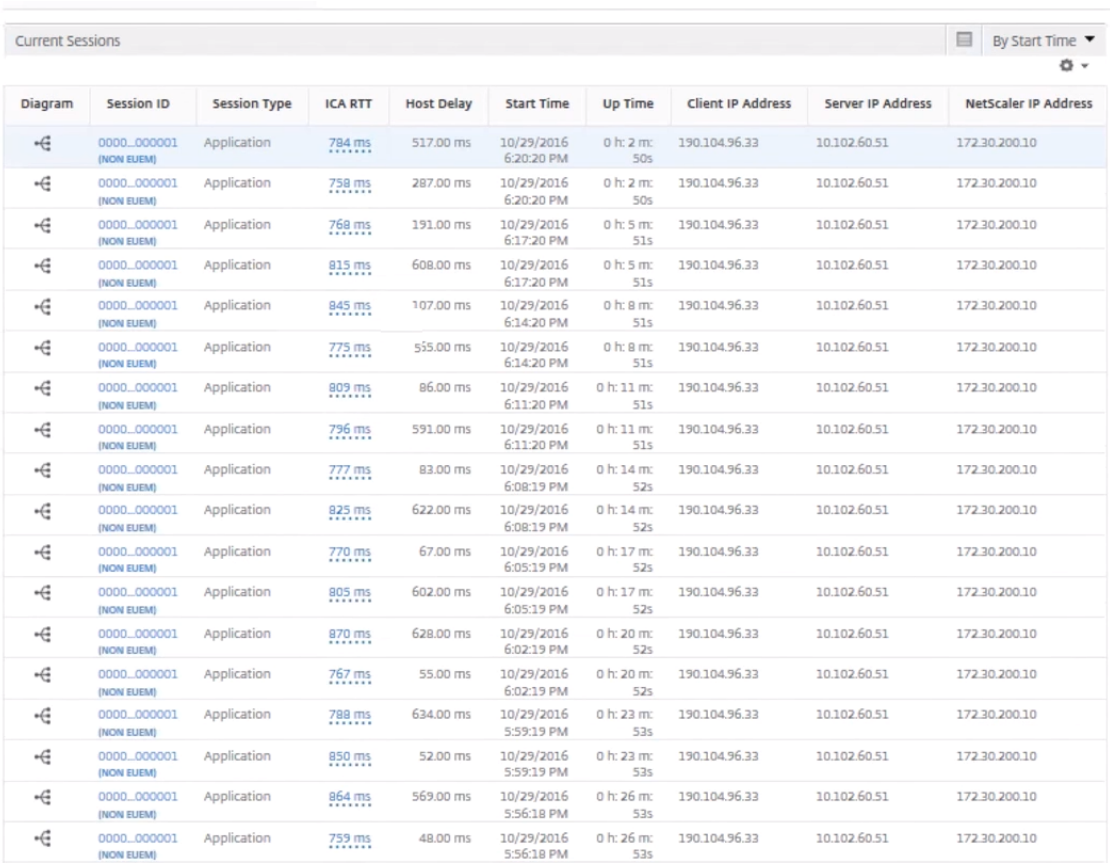
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟、客户端网络延迟或应用程序启动所用时间造成。

为了找出问题的根本原因，请分析下列指标：

- WAN 延迟
- DC latency（DC 延迟）
- 主机延迟

要查看用户度量：

1. 在“ 分析” 选项卡上，导航到 “ **HDX Insight** 能分析” > “ 用户**”**。
2. 向下滚动并单击用户名。
3. 在图形表示中，记下特定会话的 WAN 延迟、DC 延迟和 RTT 值。
4. 在“当 前会话” 表中，请注意主机延迟很高。



Current Sessions — By Start Time

Diagram	Session ID	Session Type	ICA RTT	Host Delay	Start Time	Up Time	Client IP Address	Server IP Address	NetScaler IP Address
	0000...000001 (NON EUEM)	Application	784 ms	517.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	758 ms	287.00 ms	10/29/2016 6:20:20 PM	0 h: 2 m: 50s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	768 ms	191.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	815 ms	608.00 ms	10/29/2016 6:17:20 PM	0 h: 5 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	845 ms	107.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	775 ms	555.00 ms	10/29/2016 6:14:20 PM	0 h: 8 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	809 ms	86.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	796 ms	591.00 ms	10/29/2016 6:11:20 PM	0 h: 11 m: 51s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	777 ms	83.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	825 ms	622.00 ms	10/29/2016 6:08:19 PM	0 h: 14 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	770 ms	67.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	805 ms	602.00 ms	10/29/2016 6:05:19 PM	0 h: 17 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	870 ms	628.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	767 ms	55.00 ms	10/29/2016 6:02:19 PM	0 h: 20 m: 52s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	788 ms	634.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	850 ms	52.00 ms	10/29/2016 5:59:19 PM	0 h: 23 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	864 ms	569.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10
	0000...000001 (NON EUEM)	Application	759 ms	48.00 ms	10/29/2016 5:56:18 PM	0 h: 26 m: 53s	190.104.96.33	10.102.60.51	172.30.200.10

摘要

在此示例中，**DC** 延迟为 1 毫秒，**WAN** 延迟为 12 毫秒，但主机延迟为 517 毫秒。高 RTT 且直流和 WAN 延迟较低，表示主机服务器上出现应用程序错误。

> 注意：如果您使用的是运行软件 11.1 版本 51.21 或更高版本的 Citrix ADM，则 HDX Insight 还会显示更多用户指标，例如 WAN 抖动和服务器端重新传输。要查看这些指标，请导航到分析 > **HDX Insight** > 用户，然后选择一个用户名。用户指标将显示在图旁边的表中。

用于 **HDX Insight** 的地理图

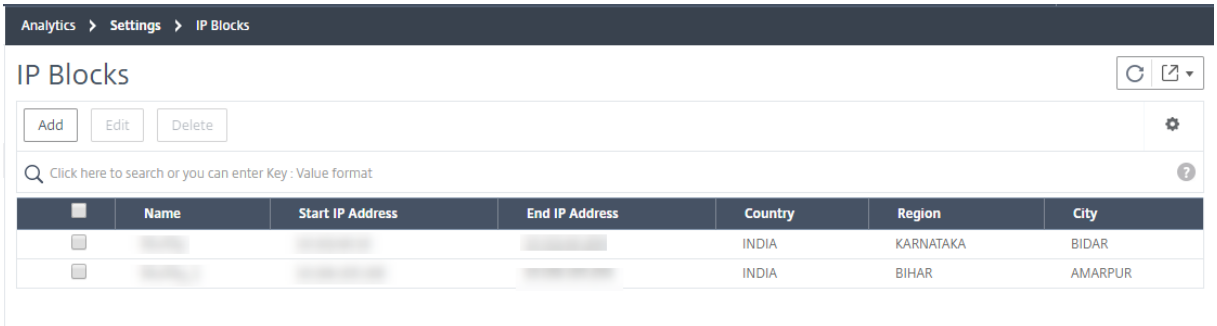
Citrix ADM 地理图功能显示地图上不同地理位置的应用程序使用情况。管理员可以使用此信息来了解应用程序在各地理位置使用情况的趋势。

您可以通过指定位置的专用 IP 范围（起始和终止 IP 地址），将 Citrix ADM 配置为显示特定地理位置或 LAN 的地理位置。

您还可以在 HDX Insight 中查看地理位置地图中的历史和活动用户的详细信息。导航到 “ 分析 ” > “ **HDX Insight** 能分析 ”，然后在地图的 “ 世界 ” 部分，单击要查看其详细信息的国家或地区。您可以按城市和省/自治区/直辖市进一步深入查看信息。

要为数据中心配置地理图，请执行以下操作：

在 “ 分析 ” 选项卡上，导航到 “ 设置 ” > “ **IP** 块 ” 以配置特定位置的地理地图。



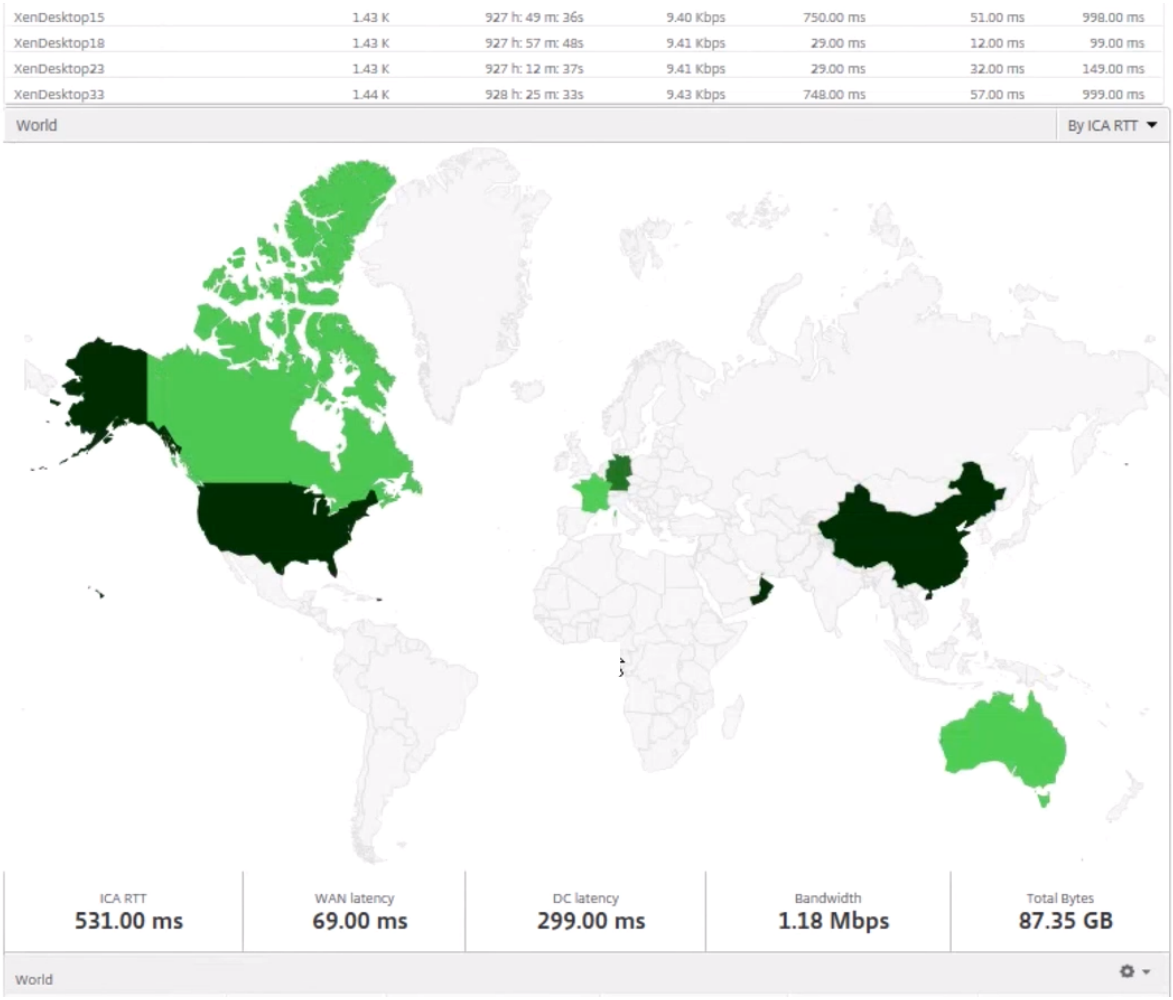
用例

假设这样一个场景：组织 ABC 有 2 个分支机构：一个在圣克拉拉，另一个在印度。

圣克拉拉用户使用 Sclara.x.com 上的 Citrix Gateway 设备访问 VPN 流量。印度用户使用位于印度.x.com 的 Citrix Gateway 设备访问 VPN 流量。

在一个特殊的时间间隔（例如 10 AM 到 5 PM），圣克拉拉的用户连接到 SClara.x.com 来访问 VPN 流量。大多数用户访问相同的 Citrix Gateway，从而导致连接到 VPN 的延迟，因此某些用户连接到 India.x.com 而不是 Sclara.x.com。

分析流量的 Citrix ADC 管理员可以使用地理地图功能来显示圣克拉拉办公室的流量。该地图显示圣克拉拉办公室的响应时间很长，因为圣克拉拉办公室只有一个 Citrix Gateway 设备，用户可以通过该设备访问 VPN 流量。因此，管理员可能会决定安装另一个 Citrix Gateway，以便用户有两个本地 Citrix 网关设备来访问 VPN。



限制

如果 Citrix ADC 实例具有高级许可证，则不会触发 Citrix ADM 上为 HDX Insight 能分析设置的阈值，因为分析数据只收集 1 小时。

启用 **HDX Insight** 数据收集

April 23, 2021

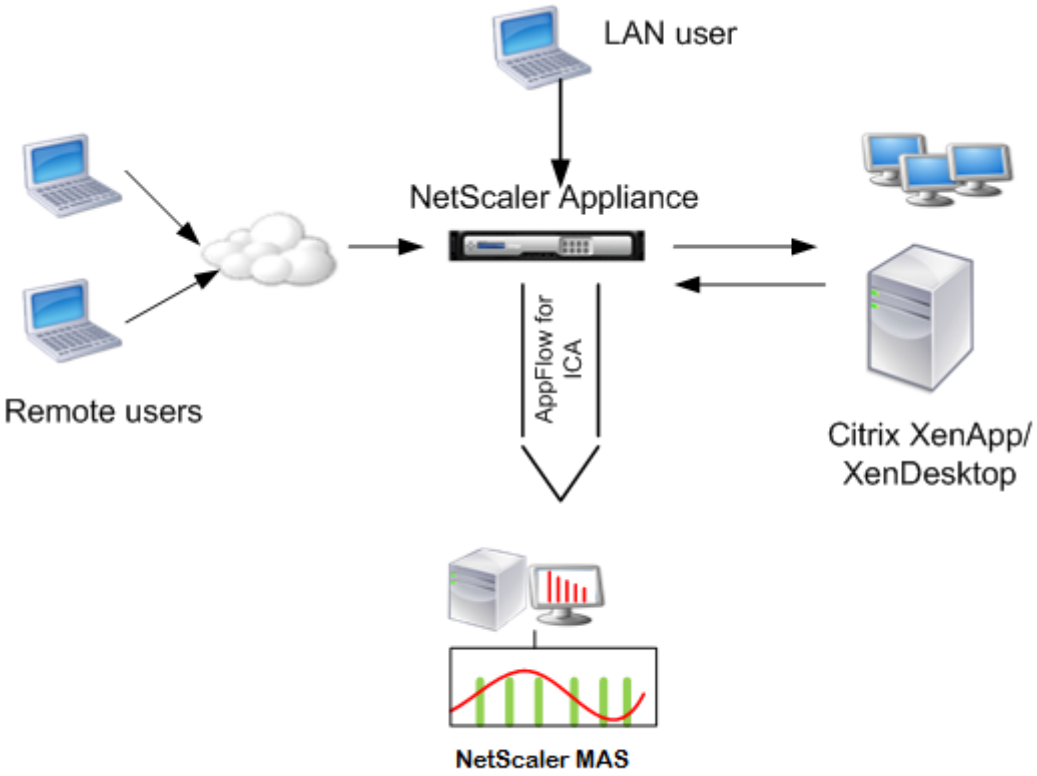
HDX Insight 通过 Citrix ADC 实例或 Citrix SD-WAN 设备传递的 ICA 流量提供前所未有的端到端可见性，使 IT 部门能够提供卓越的用户体验，并且是 Citrix Application Delivery Management (ADM) 分析的一部分。HDX Insight 为网络、虚拟桌面、应用程序和应用程序结构提供引人注目且强大的商业智能和故障分析功能。HDX Insight 可以即时鉴别分类用户问题、收集有关虚拟桌面连接的数据、生成 AppFlow 记录并将其呈现为可视报告。

Citrix ADC 中启用数据收集的配置与设备在部署拓扑中的位置不同。

启用数据收集以监视在 **LAN** 用户模式下部署的 **Citrix ADC**

访问 Citrix 虚拟应用程序和桌面应用程序的外部用户必须在 Citrix Gateway 上对自己进行身份验证。但是，内部用户可能不需要重定向到 Citrix Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便将请求重定向到 Citrix ADC 设备。

要克服这些挑战，并让 LAN 用户直接连接到 Citrix 虚拟应用程序和桌面应用程序，您可以通过配置缓存重定向虚拟服务器（该服务器充当 Citrix 网关设备上的 SOCTS 代理）以 LAN 用户模式部署 Citrix ADC 设备。



> 注意： Citrix ADM 和 Citrix Gateway 设备位于同一子网中。

要监视在此模式下部署的 Citrix ADC 装置，请首先将 Citrix ADC 装置添加到 NetScaler 智能分析清单中，启用 AppFlow，然后在仪表板上查看报告。

将 Citrix ADC 装置添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。

> 注意
>
> - 在 ADC 实例上，您可以导航到 系统 **> AppFlow >** 收集器，以检查收集器（即 Citrix ADM）是否已启动。Citrix ADC 实例使用 NSIP 将 AppFlow 记录发送到 Citrix ADM。但实例使用其 SNIP 来验证与 Citrix ADM 的连通性。因此，请确保在实例上配置了 SNIP。
> - 无法使用 Citrix ADM 配置实用程序在局域网用户模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。
> - 有关策略表达式的信息，请参见策略和表达式。

要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 添加转发代理缓存重定向虚拟服务器并提供代理 IP 和端口，指定服务类型为 HDX。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

示例

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
   cltTimeout 180
<!--NeedCopy-->
```

> 注意：如果使用 Citrix Gateway 设备访问 LAN 网络，请添加一个操作，以便由匹配 VPN 流量的策略应用。

```
add vpn trafficAction <name> <qual> [-HDX ( ON or OFF )]

add vpn trafficPolicy <name> <rule> <action>
<!--NeedCopy-->
```

示例

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. 将 Citrix ADM 添加为 Citrix ADC 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```


Example:

“‘

添加应用程序流收集器我的洞察-IP 地址 192.168.1.101

“‘

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action <name> -collectors <string>
```

示例:

```
add appflow action act -collectors MyInsight
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例:

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

示例:

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注意
>
> 类型的值必须是 ICA 流量的 ICA _REQ_ 覆盖或 ICA _REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

示例:

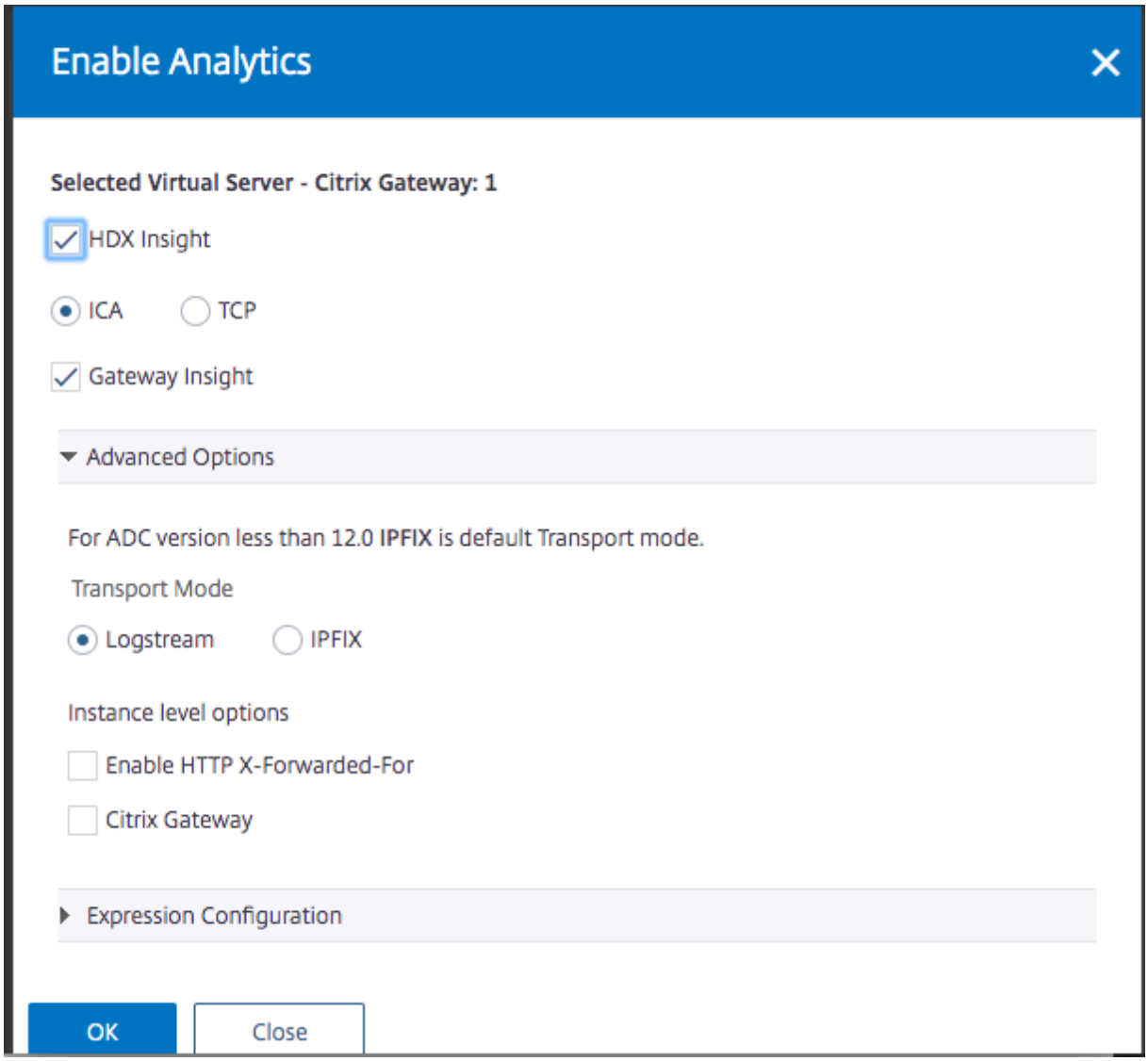
```
set appflow param -flowRecordInterval 60
```

8. 保存配置。类型：`save ns config`

为在单跳模式下部署的 **Citrix Gateway** 装置启用数据收集

在单跳模式下部署 Citrix Gateway 时，它位于网络的边缘。网关实例提供到桌面交付基础结构的代理 ICA 连接。单跳是最简单和最常见的部署。如果外部用户尝试访问组织中的内部网络，则单跳模式可提供安全性。
在单跳模式下，用户通过虚拟专用网络 (VPN) 访问 Citrix ADC 设备。

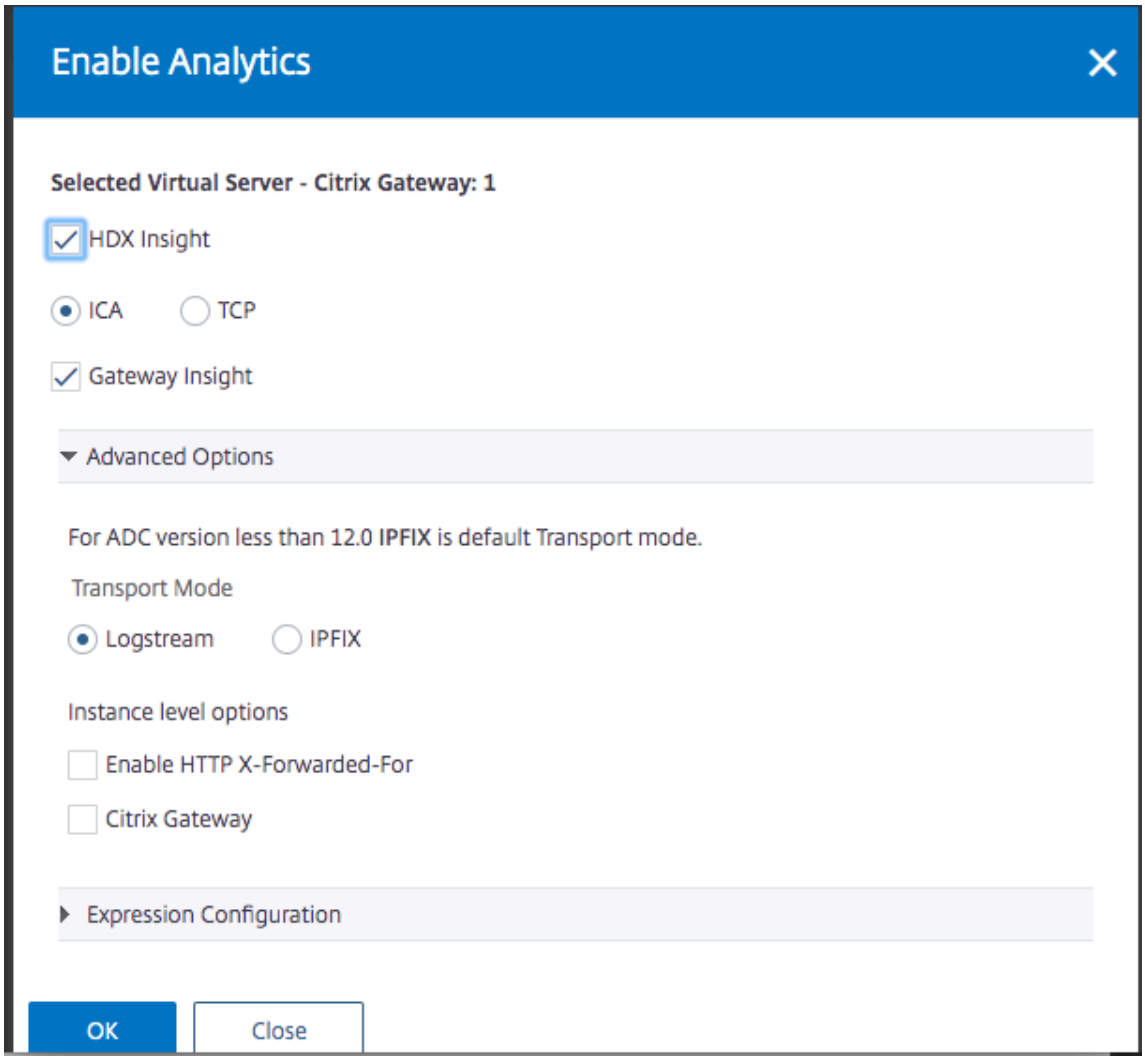
要开始收集报告，必须将 Citrix Gateway 设备添加到 Citrix Application Delivery Management (ADM) 清单中，并在 ADM 上启用 AppFlow。



要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到 “ 网络” > “ 实例”，然后选择要启用分析的 Citrix ADC 实例。
4. 从选择操作列表中，选择配置分析。

5. 选择 VPN 虚拟服务器，然后单击 启用分析。
6. 选择 “ **HDX Insight** ”，然后选择 “ **ICA**”。
7. 单击确定。



> 注意
>
> 在单跳模式下启用 AppFlow 时，以下命令将在后台运行。此处显式指定这些命令是为了进行故障排除。

```
- add appflow collector <name> -IPAddress <ip_addr>

- add appflow action <name> -collectors <string>

- set appflow param -flowRecordInterval <secs>

- disable ns feature AppFlow

- enable ns feature AppFlow
```

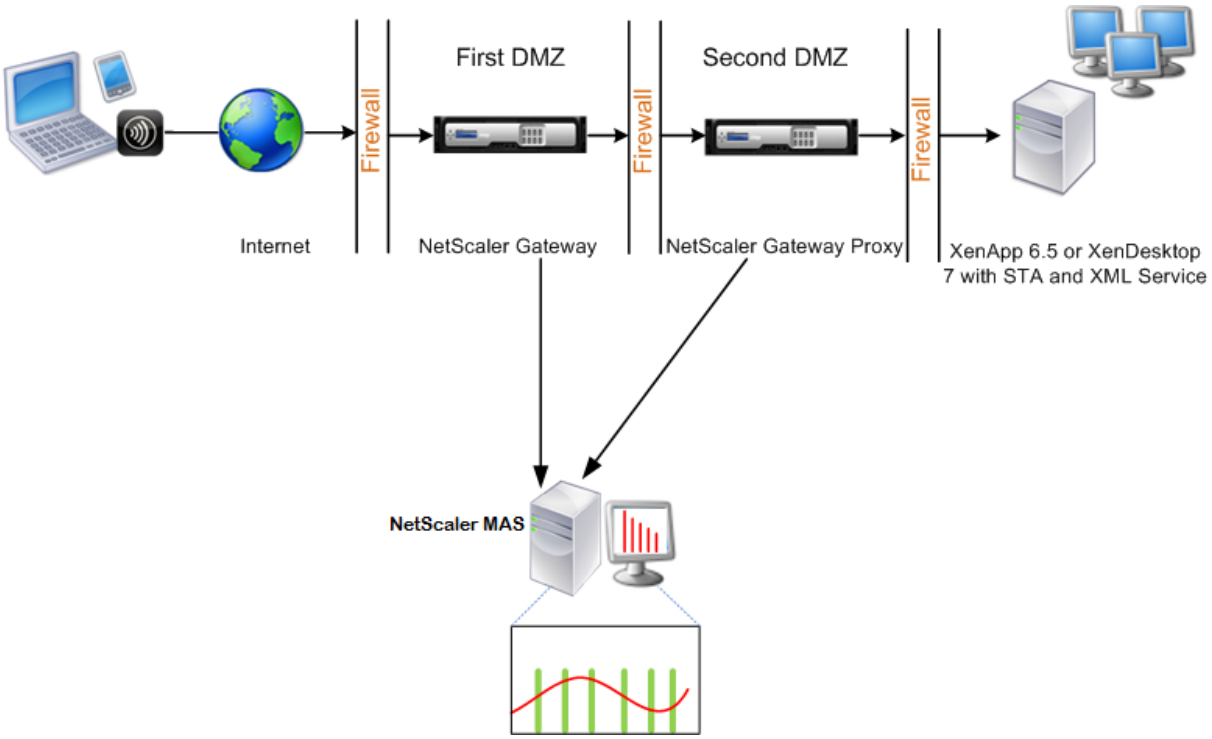


```
10
11 -  add appflow policy <name> <rule> <expression>
12
13 -  set appflow policy <name> -rule <expression>
14
15 -  bind vpn vserver <vsname> -policy <string> -type <type> -priority <
      positive_integer>
16
17 -  set vpn vserver <name> -appflowLog ENABLED
18
19 -  save ns config
```

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则 Citrix ADM 上仍会显示剩余的 HDX Insight 数据。

为在双跳模式下部署的 **Citrix Gateway** 装置启用数据收集

Citrix Gateway 双跳模式为组织的内部网络提供额外的保护，因为攻击者需要穿透多个安全区域或非军事区域 (DMZ) 才能访问安全网络中的服务器。如果要分析 ICA 连接通过的跃点数（Citrix Gateway 装置），以及有关每个 TCP 连接上延迟的详细信息，以及它如何与客户端感知到的总 ICA 延迟展开，则必须安装 Citrix ADM，以便 Citrix 网关装置报告这些生命统计数据。



第一个 DMZ 中的 Citrix Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 Citrix 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 Citrix 网关充当 Citrix Gateway 代理设备。此 Citrix Gateway 使 ICA 流量能够遍历第二个 DMZ，以完成与服务器场的用户连接。

Citrix ADM 可以部署在属于第一个 DMZ 中 Citrix Gateway 设备的子网中，也可以部署在属于 Citrix 网关设备第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 Citrix ADM 和 Citrix 网关部署在同一子网中。

在双跳模式下，Citrix ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 Citrix Gateway 装置添加到 Citrix ADM 清单并启用数据收集后，每个装置都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 Citrix ADM 识别哪个装置正在导出记录，每个装置都会使用跳数指定，并使用连接链 ID 指定每个连接。跳数表示通信从客户端流向服务器的 Citrix Gateway 设备数。连接链 ID 表示客户端与服务器之间的端到端连接。

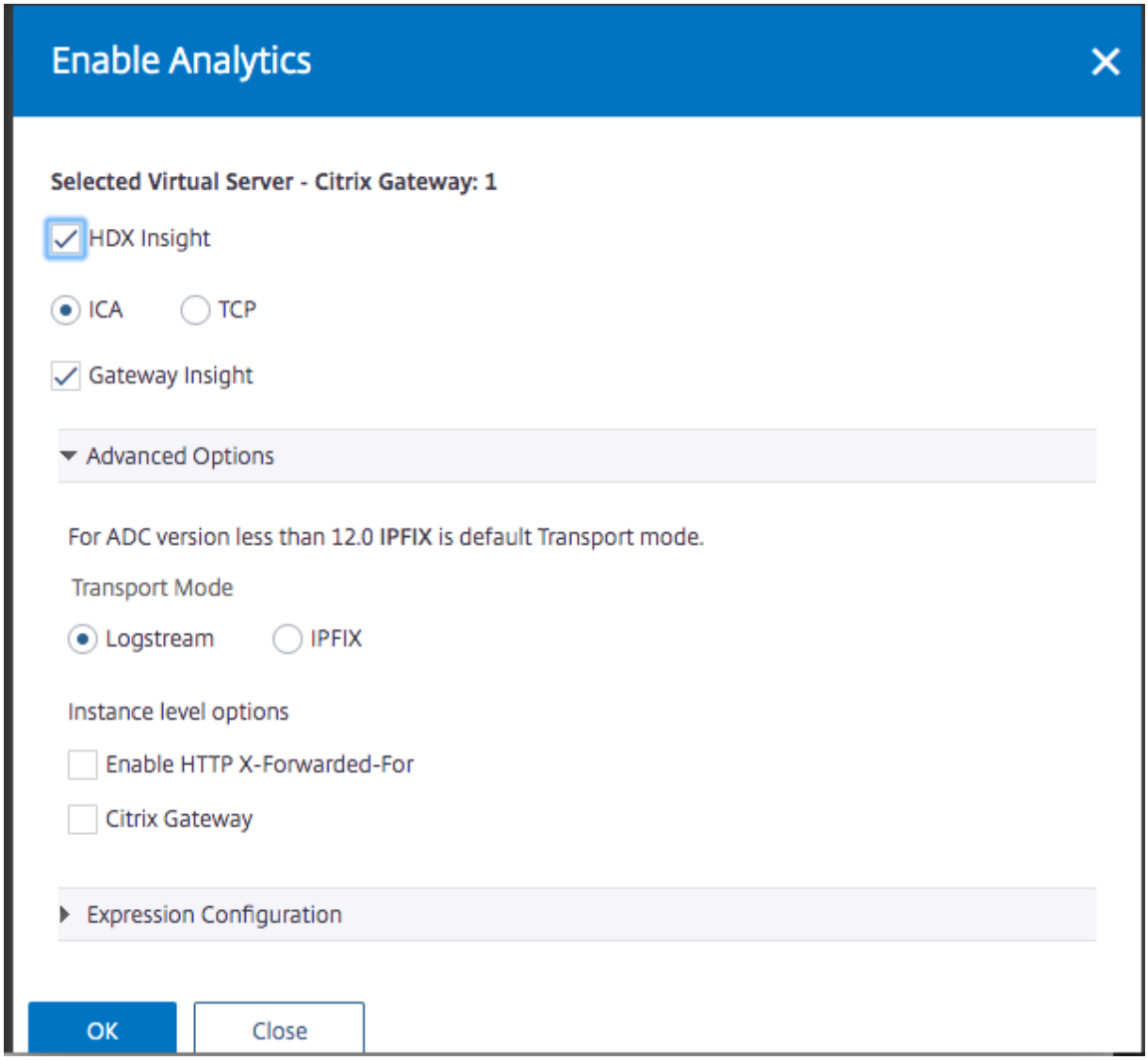
Citrix ADM 使用跳数和连接链 ID 来共同关联来自 Citrix Gateway 设备的数据并生成报告。

要监视在此模式下部署的 Citrix Gateway 装置，必须首先将 Citrix Gateway 添加到 Citrix ADM 清单中，启用 Citrix ADM 上的 AppFlow，然后在 Citrix ADM 仪表板上查看报告。

在用于最佳网关的虚拟服务器上配置 **HDX Insight**

在用于最佳网关的虚拟服务器上配置 HDX Insight 能分析的步骤：

1. 导航到 “ 网络” > “ 实例”，然后选择要启用分析的 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。
3. 选择为身份验证配置的 VPN 虚拟服务器，然后单击 启用分析。
4. 选择 “ **HDX Insight** ”，然后选择 “ **ICA**”。
5. 根据需要选择其他高级选项。
6. 单击确定。
7. 在另一个 VPN 虚拟服务器上重复步骤 3 到步骤 6。



在 **Citrix ADM** 上启用数据收集

如果启用 Citrix ADM 开始从两个装置收集 ICA 详细信息，则收集的详细信息将是冗余的。即两个设备报告相同的指标。若要克服此情况，您必须在第一个 Citrix Gateway 设备之一上启用 ICA 的 AppFlow，然后在第二个装置上启用 TCP 的 AppFlow。通过这样做，其中一个装置导出 ICA AppFlow 记录，另一个装置则导出 TCP AppFlow 记录。这还节省解析 ICA 通信的处理时间。

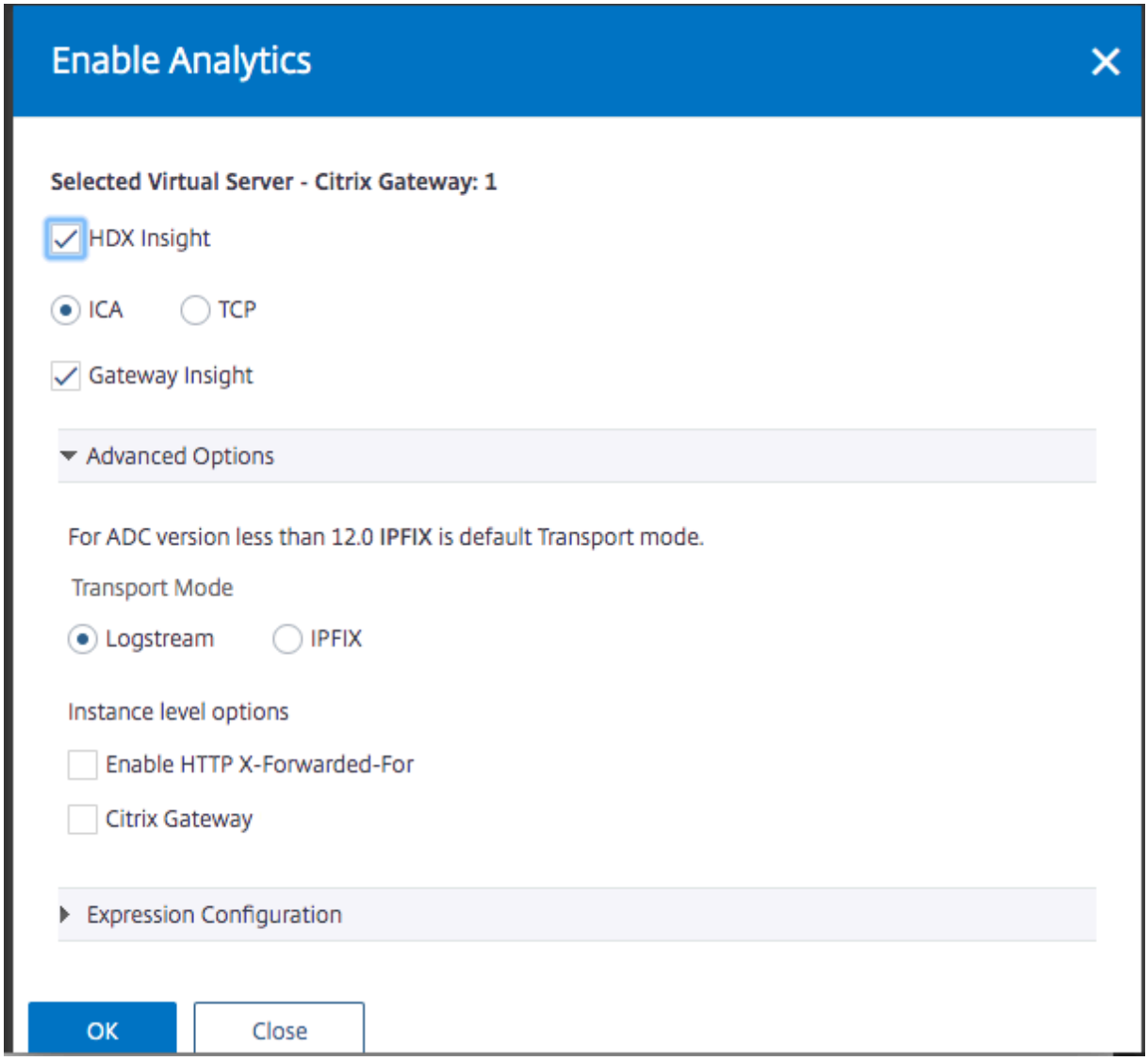
要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到 “ 网络” > “ 实例”，然后选择要启用分析的 Citrix ADC 实例。
4. 从选择操作列表中，选择配置分析。

5. 选择 VPN 虚拟服务器，然后单击 启用分析。
6. 选择 “ **HDX Insight** 分析”，然后分别为 **ICA** 流量或 **TCP** 流量选择 ICA 或 TCP 流量。

> 注意
>
> 如果未为 Citrix ADC 设备上的相应服务或服务组启用 AppFlow 日志记录，则 Citrix ADM 仪表板也不会显示记录，即使 “智能分析” 列显示 “已启用” 也是如此。

7. 单击确定。



配置 **Citrix Gateway** 设备以导出数据

安装 CCitrix Gateway 设备后，必须在 Citrix 网关设备上配置以下设置，以便将报告导出到 Citrix ADM：

- 在第一个和第二个 DMZ 中将 Citrix Gateway 设备的虚拟服务器配置为彼此通信。

- 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。
- 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
- 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。
- 启用其中一个 Citrix Gateway 设备以导出 ICA 记录
- 启用其他 Citrix Gateway 设备以导出 TCP 记录：
- 在两个 Citrix Gateway 设备上启用连接链接。

使用命令行界面配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 虚拟服务器配置为与第二个 DMZ 中的 Citrix Gateway 虚拟服务器进行通信。

```
add vpn nextHopServer <name> <nextHopIP> <nextHopPort> [-secure (
    ON or OFF)] [-imgGifToPng]

add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
```

2. 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。在第一个 DMZ 中的 Citrix Gateway 上运行以下命令：

```
bind vpn vserver <name> -nextHopServer <name>

bind vpn vserver vs1 -nextHopServer nh1
```

3. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点和 AppFlow。

```
set vpn vserver <name> [- doubleHop ( ENABLED or DISABLED )] [-
    appflowLog ( ENABLED or DISABLED )]

set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
```

4. 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。

```
set vpn vserver <name> [-authentication (ON or OFF)]

set vpn vserver vs -authentication OFF
```

5. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn1 -policy appflowpol1 -priority 101 -type
    OTHERTCP_REQUEST
```


6. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

```
bind vpn vserver <name> [-policy <string> -priority <
    positive_integer>] [-type <type>]

bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
    ICA_REQUEST
```

7. 在两个 Citrix Gateway 设备上启用连接链接：

```
set appFlow param [-connectionChaining (ENABLED or DISABLED)]

set appflow param -connectionChaining ENABLED
```

使用配置实用程序配置 **Citrix Gateway**

1. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix 网关绑定到第一个 DMZ 中的 Citrix 网关。
   a) 在“配置”选项卡上展开 **Citrix Gateway** ，然后单击“虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在高级组中展开已发布的应用程序。
   c) 单击下一跳服务器并将下一跳服务器绑定到第二个 Citrix Gateway 设备。
2. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
   a) 在“配置”选项卡上展开 **Citrix Gateway** ，然后单击“虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。
   c) 展开更多内容，选择双跳，然后单击确定。
3. 在第二个 DMZ 中 Citrix Gateway 关上的虚拟服务器上禁用身份验证。
   a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器
   b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。
   c) 展开“更多”，然后清除“启用身份验证”。
4. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。
   a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器
   b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。
   c) 单击 + 图标，然后从“选择策略”列表中选择“**AppFlow**”，然后从“ 选择类型”列表中选择“其他 **TCP** 请求”。
   d) 单击 继续。
   e) 添加策略绑定，并单击 **Close**（关闭）。

5. 启用其他 Citrix Gateway 设备以导出 ICA 记录：
   a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器
   b) 在右窗格中，双击虚拟服务器，然后在高级组中
      展开策略。
   c) 单击 + 图标，然后从 “选择策略” 列表中选择 “AppFlow”，然后从 “CHOSE 类型” 列表中选择 “其他 **TCP** 请求”。
   d) 单击 继续。
   e) 添加策略绑定，并单击 **Close**（关闭）。
6. 在两个 Citrix Gateway 设备上启用连接链接。
   a) 在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Appflow**。
   b) 在右窗格中的 “设置” 组中，双击 “更改应用程序流设置”。
   c) 选择 **Connection Chaining**（连接链）并单击 **OK**（确定）。
7. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix 网关绑定到第一个 DMZ 中的 Citrix 网关。
   a) 在 “配置” 选项卡上展开 **Citrix Gateway**，然后单击 “虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在高级组中展开已发布的应用程序。
   c) 单击下一跳服务器，然后将下一跳服务器绑定到第二台 Citrix Gateway 设备。
8. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
   a) 在 “配置” 选项卡上展开 **Citrix Gateway**，然后单击 “虚拟服务器”。
   b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。
   c) 展开 “更多”，选择 “双跳”，然后单击 “确定”。
9. 在第二个 DMZ 中 Citrix Gateway 关上的虚拟服务器上禁用身份验证。
   a) 在配置选项卡上，展开 Citrix Gateway 并单击虚拟服务器
   b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。
   c) 展开 “更多”，然后清除 “启用身份验证”。
10. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。
    a) 在 “配置” 选项卡上展开 **Citrix Gateway**，然后单击 “虚拟服务器”。
    b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。
    c) 单击 **+** 图标，然后从 “选择策略” 列表中选择 “AppFlow”，然后从 “ 选择类型” 列表中选择 “其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

11. 启用其他 Citrix Gateway 设备以导出 ICA 记录。

a) 在 “配置” 选项卡上展开 **Citrix Gateway**，然后单击 “虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 **+** 图标，然后从 **“选择策略”** 列表中选择 “AppFlow”，然后从 “ 选择类型” 列表中选择 “其他 **TCP** 请求”。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

12. 在两个 Citrix Gateway 设备上启用连接链接。

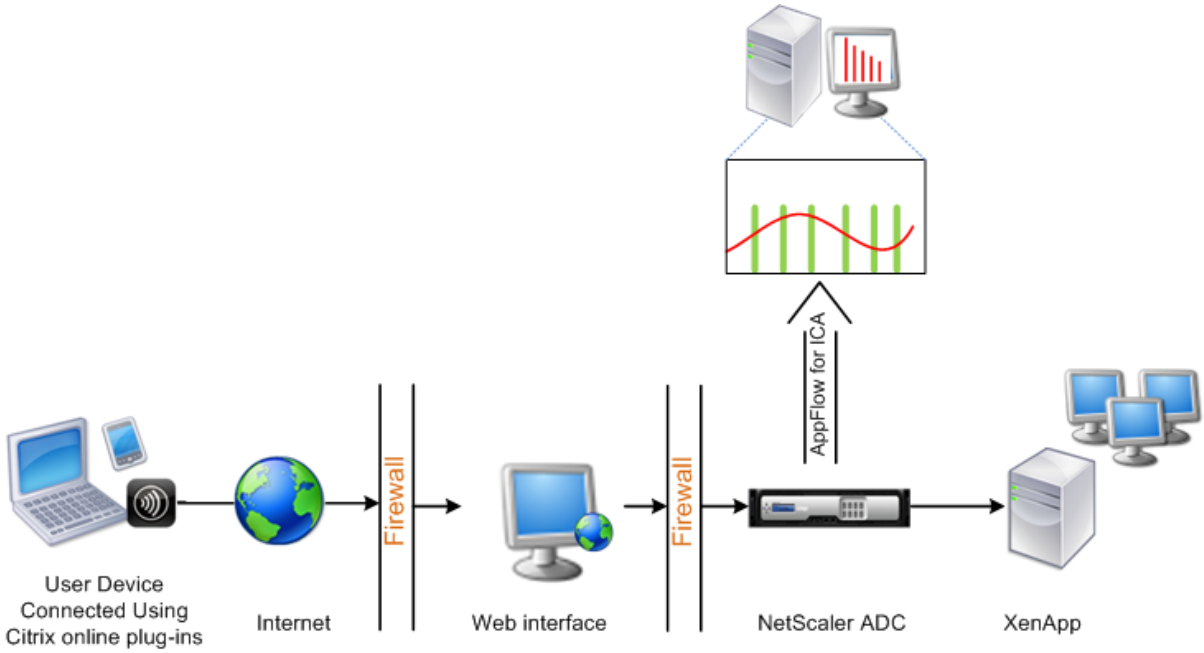
启用数据收集以监控在透明模式下部署的 Citrix ADC

当以透明模式部署 Citrix ADC 时，客户端可以直接访问服务器，而无需干预虚拟服务器。如果在 Citrix 虚拟应用程序和桌面环境中以透明模式部署了 Citrix ADC 装置，则 ICA 流量不会通过 VPN 传输。

将 Citrix ADC 添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。启用数据收集依赖于设备和模式。在这种情况下，您必须在每个 Citrix ADC 设备上添加 Citrix ADM 作为 AppFlow 收集器，并且必须配置 AppFlow 策略以收集流经设备的所有或特定 ICA 流量。

> 注意
>
> - 无法使用 Citrix ADM 配置实用程序在透明模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。
> - 有关策略表达式的信息，请参见策略和表达式。

下图显示了在透明模式下部署 Citrix ADM Citrix ADC 时的网络部署情况：



要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 指定 Citrix ADC 设备侦听通信的 ICA 端口。

```
set ns param --icaPorts <port>...
```

示例：

```
set ns param -icaPorts 2598 1494
```

> 注意
>
> - 可以使用此命令最多指定 10 个端口。
> - 默认端口号为 2598。可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 Citrix ADC 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
```

> 注意：要查看 Citrix ADC 设备上配置的 AppFlow 收集器，请使用 **show appflow** 收集器命令。

4. 创建 AppFlow 操作，并将收集器与该操作关联。


```
add appflow action <name> -collectors <string> ...
```

示例：

添加 AppFlow 动作行为收集器 myInsight

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
```

示例：

```
add appflow policy pol true act
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
```

> 注意
>
> **type** 的值必须是 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
```

示例：

```
set appflow param -flowRecordInterval 60
```

8. 保存配置。类型：`save ns config`

‘‘‘

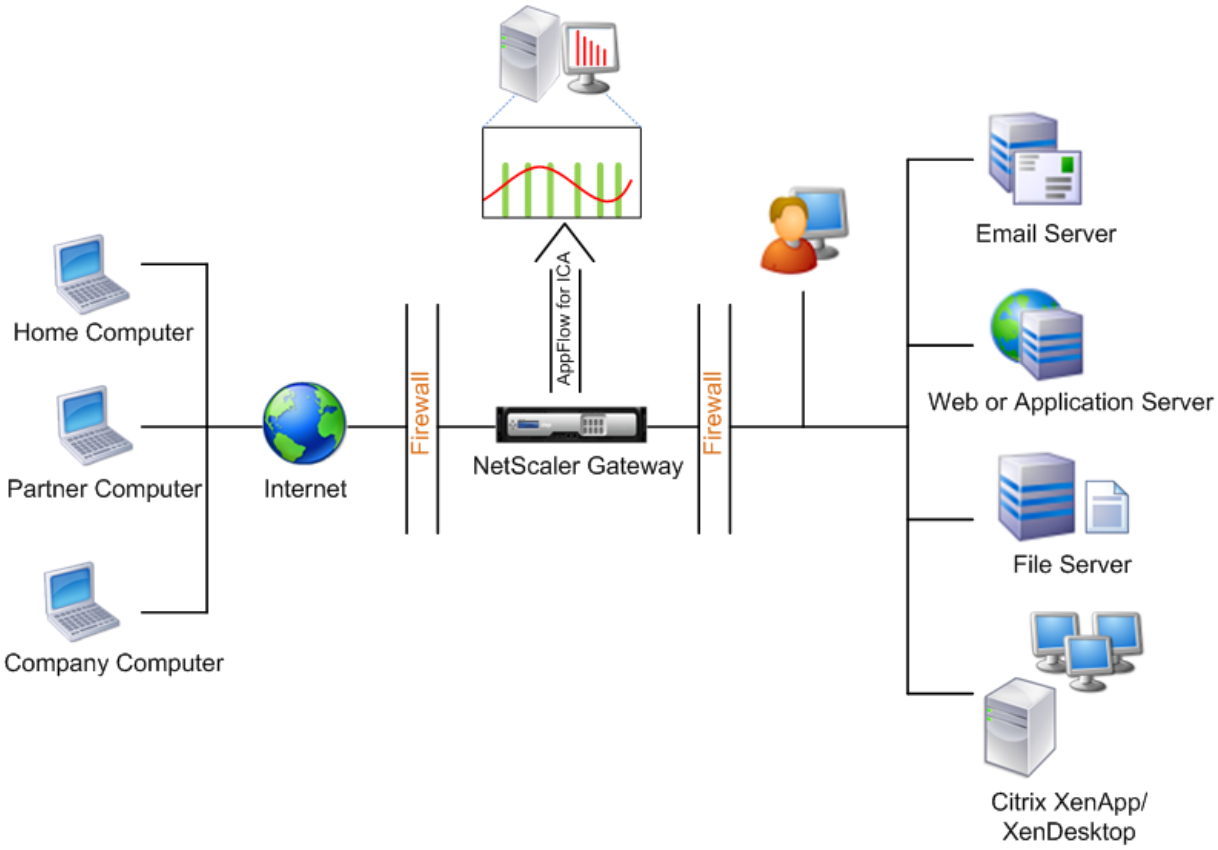
为在单跳模式下部署的 **Citrix Gateway** 装置启用数据收集

April 23, 2021

在单跳模式下部署 Citrix Gateway 时，它位于网络的边缘。网关实例提供到桌面交付基础结构的代理 ICA 连接。单跳是最简单和最常见的部署。如果外部用户尝试访问组织中的内部网络，则单跳模式可提供安全性。

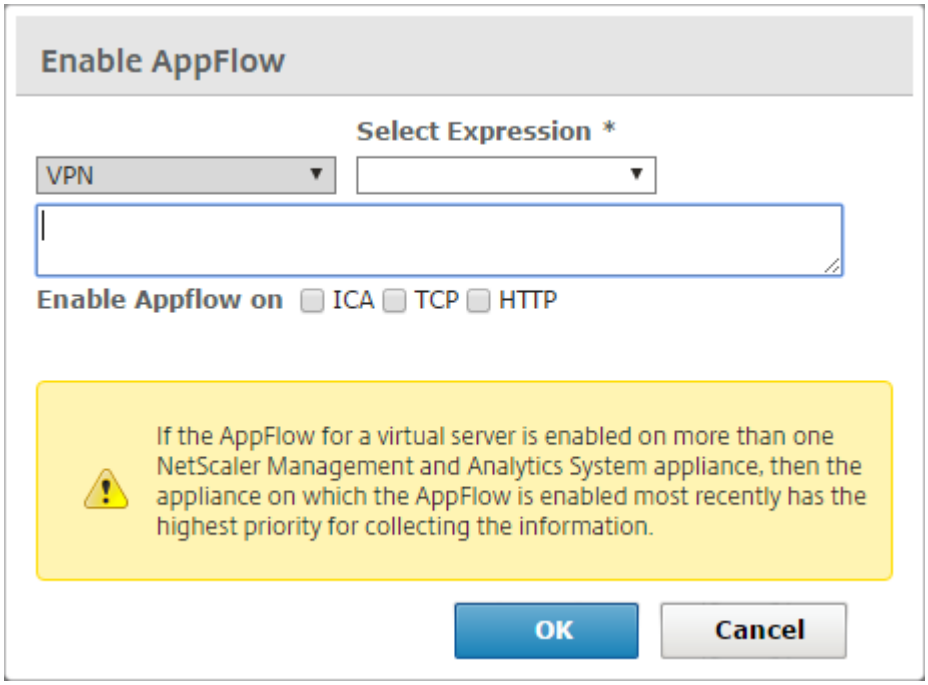
在单跳模式下，用户通过虚拟专用网络 (VPN) 访问 Citrix ADC 设备。

要开始收集报告，必须将 Citrix Gateway 设备添加到 Citrix Application Delivery Management (ADM) 清单中，并在 ADM 上启用 AppFlow。



要从 **ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到基础设施 > 实例，然后选择要启用分析的 Citrix ADC 实例。
2. 从 操作列表中，选择 启用/禁用智能分析。
3. 选择 **VPN** 虚拟服务器，然后单击 启用 **AppFlow**。
4. 在启用 **AppFlow** 字段中，键入 **true**，然后选择 **ICA**。
5. 单击确定。



注意

在单跳模式下启用 AppFlow 时，以下命令将在后台运行。此处显式指定这些命令是为了进行故障排除。

- `add appflow collector \<name\> -IPAddress \<ip\\_addr\>`
- `add appflow action \<name\> -collectors \<string\>`
- `set appflow param -flowRecordInterval \<secs\>`
- `disable ns feature AppFlow`
- `enable ns feature AppFlow`
- `add appflow policy \<name\> \<rule\> \<expression\>`
- `set appflow policy \<name\> -rule \<expression\>`
- `bind vpn vserver \<vsname\> -policy \<string\> -type \<type\> >- priority \<positive\\_integer\>`
- `set vpn vserver \<name\> -appflowLog ENABLED`
- `save ns config`

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则 Citrix ADM 上仍会显示剩余的 HDX Insight 数据。

启用数据收集以监视在透明模式下部署的 Citrix ADC

April 23, 2021

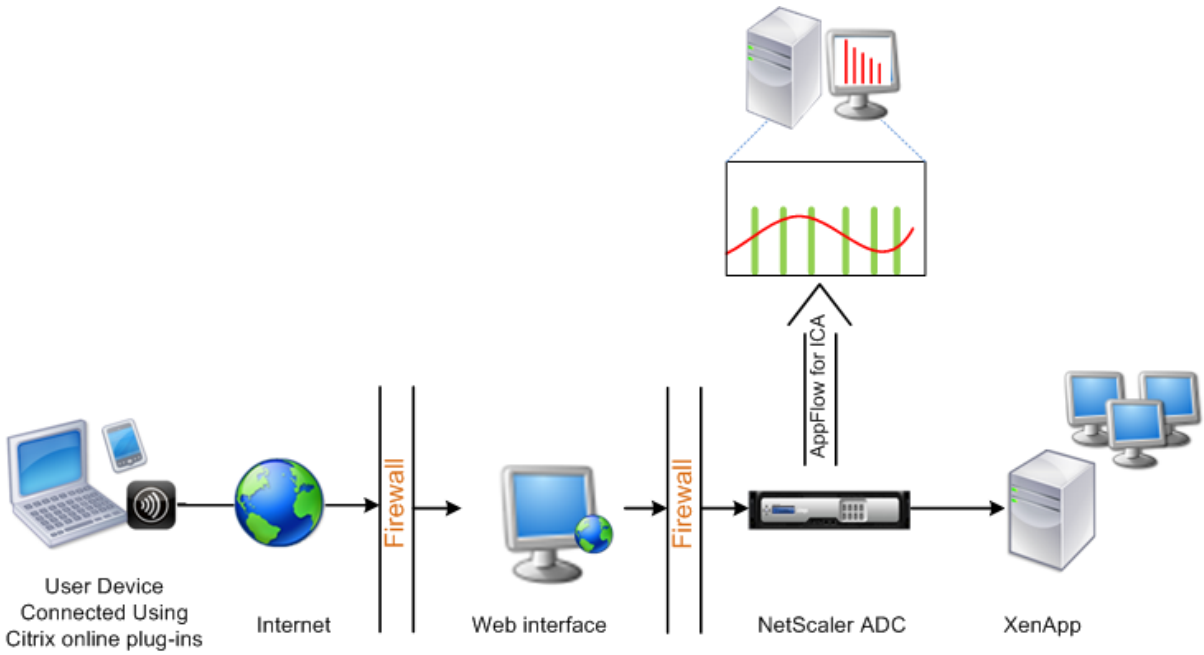
当以透明模式部署 Citrix ADC 时，客户端可以直接访问服务器，而无需干预虚拟服务器。如果在 Citrix Virtual Apps

and Desktops 环境中以透明模式部署了 Citrix ADC，则 ICA 流量不会通过 VPN 传输。

将 Citrix ADC 添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。启用数据收集依赖于设备和模式。在这种情况下，您必须将 Citrix ADM 添加为每个 Citrix ADC 实例上的 AppFlow 收集器，并且必须配置 AppFlow 策略以收集通过设备流的所有或特定 ICA 流量。

> 注意
>
> - 无法使用 Citrix ADM 配置实用程序在透明模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅命令参考。
> - 有关策略表达式的信息，请参见策略和表达式。

下图显示了在透明模式下部署 Citrix ADM Citrix ADC 时的网络部署情况：



要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 指定 Citrix ADC 设备侦听通信的 ICA 端口。

```
set ns param --icaPorts <port>...
<!--NeedCopy-->
```

示例：

```
set ns param -icaPorts 2598 1494
<!--NeedCopy-->
```


> 注意
>
> - 可以使用此命令最多指定 10 个端口。
> - 默认端口号为 2598。可以根据需要修改端口号。

3. 将 NetScaler Insight Center 添加为 Citrix ADC 实例上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

> 注意要查看在 Citrix ADC 实例上配置的 AppFlow 收集器，请使用 **show appflow** 收集器命令。

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action <name> -collectors <string> ...
<!--NeedCopy-->
```

示例：

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy <policyname> <rule> <action>
<!--NeedCopy-->
```

示例：

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global <policyname> <priority> -type <type>
<!--NeedCopy-->
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```


> 注意
>
> **type** 的值必须是 ICA_REQ_OVERRIDE 或 ICA_REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 保存配置。

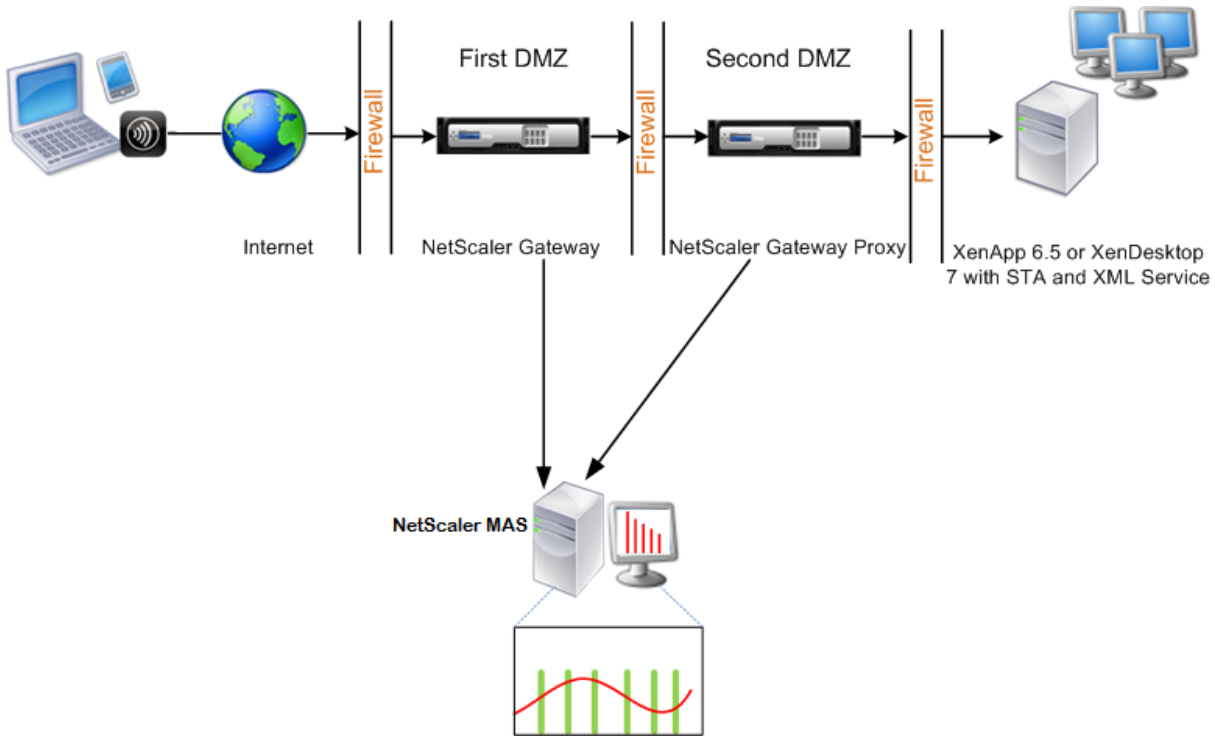
```
save ns config
<!--NeedCopy-->
```

为在双跳模式下部署的 **Citrix Gateway** 装置启用数据收集

April 23, 2021

Citrix Gateway 双跃点模式为组织的内部网络提供额外的保护，因为攻击者需要穿透多个安全区域或非军事区 (DMZ) 才能访问安全网络中的服务器。如果要分析 ICA 连接通过的跳数（Citrix Gateway 装置），以及有关每个 TCP 连接上延迟的详细信息，以及它如何与客户端感知到的 ICA 总延迟进行展览，则必须安装 Citrix ADM，以便 Citrix Gateway 装置报告这些生命统计数据。

图 3. Citrix ADM 在双跃点模式下部署



第一个 DMZ 中的 Citrix Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 Citrix 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 Citrix 网关充当 Citrix Gateway 代理设备。此 Citrix Gateway 使 ICA 流量能够遍历第二个 DMZ，以完成与服务器场的用户连接。

Citrix ADM 可以部署在属于第一个 DMZ 中 Citrix Gateway 设备的子网中，也可以部署在属于 Citrix 网关设备第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 Citrix ADM 和 Citrix 网关部署在同一子网中。

在双跳模式下，Citrix ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 Citrix Gateway 设备添加到 Citrix ADM 清单并启用数据收集后，每台设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 Citrix ADM 识别哪个装置正在导出记录，每个装置都会使用跳数指定，并使用连接链 ID 指定每个连接。跳数表示通信从客户端流向服务器的 Citrix Gateway 设备数。连接链 ID 表示客户端与服务器之间的端到端连接。

Citrix ADM 使用跳数和连接链 ID 来共同关联来自 Citrix Gateway 设备的数据并生成报告。

要监视在此模式下部署的 Citrix Gateway 装置，必须首先将 Citrix Gateway 添加到 Citrix ADM 清单中，启用 Citrix ADM 上的 AppFlow，然后在 Citrix ADM 仪表板上查看报告。

在 **Citrix ADM** 上启用数据收集

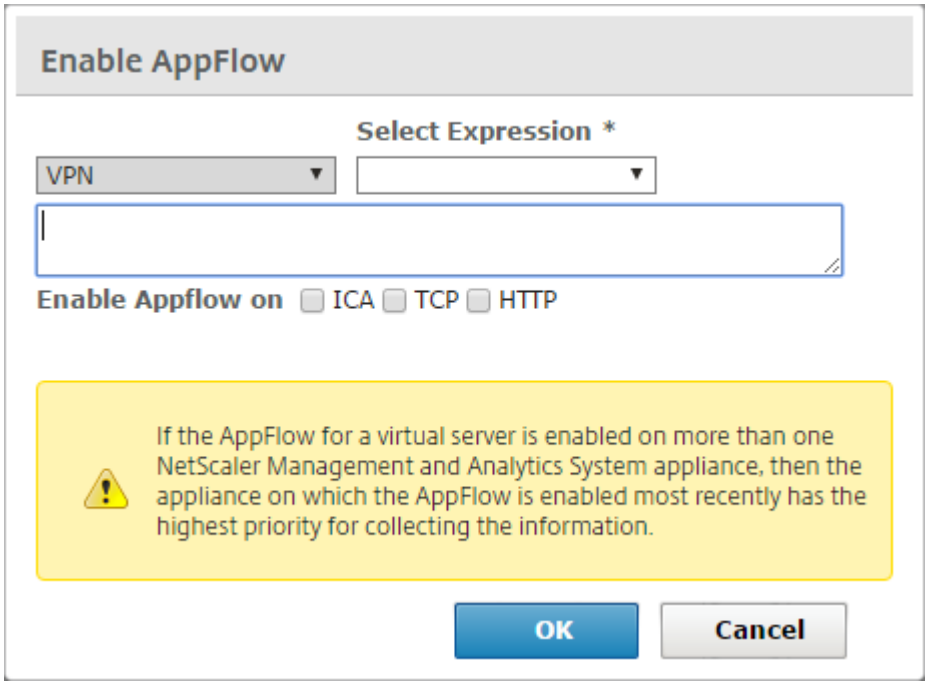
如果启用 Citrix ADM 开始从两个装置收集 ICA 详细信息，则收集的详细信息将是冗余的。即两个设备报告相同的指标。若要克服此情况，您必须在第一个 Citrix Gateway 设备之一上启用 ICA 的 AppFlow，然后在第二个装置上启用 TCP 的 AppFlow。通过这样做，其中一个装置导出 ICA AppFlow 记录，另一个装置则导出 TCP AppFlow 记录。这还节省解析 ICA 通信的处理时间。

要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到 基础架构 **>** 实例，然后选择要启用分析的 Citrix ADC 实例。
2. 从 操作列表中，选择 启用**/**禁用智能分析。
3. 选择 VPN 虚拟服务器，然后单击启用 **AppFlow**。
4. 在 启用 **AppFlow** 字段中，键入 **true**，然后分别为 **ICA** 流量选择 **ICA/** TCP 流量。

   > 注意
   >
   > 如果未为 Citrix ADC 设备上的服务或服务组启用 AppFlow 日志记录，Citrix ADM 仪表板不会显示记录，即使 Insight 列显示已启用。

5. 单击确定。



配置 **Citrix Gateway** 设备以导出数据

安装 CCitrix Gateway 设备后，必须在 Citrix 网关设备上配置以下设置，以便将报告导出到 Citrix ADM：

- 在第一个和第二个 DMZ 中将 Citrix Gateway 设备的虚拟服务器配置为彼此通信。
- 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。
- 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。
- 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。
- 启用其中一个 Citrix Gateway 设备以导出 ICA 记录
- 启用其他 Citrix Gateway 设备以导出 TCP 记录：
- 在两个 Citrix Gateway 设备上启用连接链接。

使用命令行界面配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 虚拟服务器配置为与第二个 DMZ 中的 Citrix Gateway 虚拟服务器进行通信。

   添加 **VPN** 下一个服务器 <name> <nextHopIP> <nextHopPort> [**-**安全 (开 |OFF)] [**-imgGifToPng**] …

   ```
   1 add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
   2 <!--NeedCopy-->
   ```

2. 将第二个 DMZ 中的 Citrix Gateway 虚拟服务器绑定到第一个 DMZ 中的 Citrix Gateway 虚拟服务器。在第一个 DMZ 中的 Citrix Gateway 上运行以下命令：

绑定 **VPN** 虚拟服务器 **<name> -**下一个服务器 <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点和 AppFlow。

   设置 **VPN** 虚拟服务器 <name> [**-**双跳 (已启用) | 已禁用)] [**-**应用程序流日志（已启用 |DISABLED)]

```
set vpn vserver vpnhop2  -doubleHop ENABLED  -appFlowLog ENABLED
<!--NeedCopy-->
```

4. 在第二个 DMZ 中的 Citrix Gateway 虚拟服务器上禁用身份验证。

   set vpn vserver<name> [**-authentication** (ON|OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。

   bind vpn vserver<name> [**-policy** <string> **-priority** <positive_integer>] [**-type** <type>]

```
bind vpn vserver vpn1 -policy appflowpol1 -priority 101  -type
   OTHERTCP_REQUEST
<!--NeedCopy-->
```

6. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

   bind vpn vserver<name> [**-policy** <string> **-priority** <positive_integer>] [**-type** <type>]

```
bind vpn vserver vpn2 -policy appflowpol1 -priority 101 -type
   ICA_REQUEST
<!--NeedCopy-->
```

7. 在两个 Citrix Gateway 设备上启用连接链接：

设置应用程序流参数 [**-**连接链接（已启用）　　DISABLED)]

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

使用配置实用程序配置 **Citrix Gateway**：

1. 将第一个 DMZ 中的 Citrix Gateway 配置为与第二个 DMZ 中的 Citrix Gateway 进行通信，并将第二个 DMZ 中的 Citrix 网关绑定到第一个 DMZ 中的 Citrix 网关。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开已发布的应用程序。

c) 单击下一跳服务器并将下一跳服务器绑定到第二个 Citrix Gateway 设备。

2. 在第二个 DMZ 中的 Citrix Gateway 上启用双跃点。

a) 在“配置”选项卡上展开 **Citrix Gateway**，然后单击“虚拟服务器”。

b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展开 **More**（更多），选择 **Double Hop**（双跃点）并单击 **OK**（确定）。

3. 在第二个 DMZ 中 Citrix Gateway 关上的虚拟服务器上禁用身份验证。

a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器

b) 在右窗格中，双击虚拟服务器，然后在基本设置组中单击编辑图标。

c) 展开“更多”，然后清除“启用身份验证”。

4. 启用其中一个 Citrix Gateway 设备以导出 TCP 记录。

a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 + 图标，然后从选择策略列表中选择 **AppFlow**，然后从选择类型下拉列表中选择其他 **TCP** 请求。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

5. 启用其他 Citrix Gateway 设备以导出 ICA 记录：

a) 在配置选项卡上，展开 **Citrix Gateway** 并单击虚拟服务器

b) 在右窗格中，双击虚拟服务器，然后在高级组中展开策略。

c) 单击 + 图标，然后从选择策略下拉列表中选择 **AppFlow**，然后从选择类型下拉列表中选择其他 **TCP** 请求。

d) 单击 继续。

e) 添加策略绑定，并单击 **Close**（关闭）。

6. 在两个 Citrix Gateway 设备上启用连接链接。

a) 在配置选项卡上，导航到系统 **> Appflow**。

b) 在右侧窗格的“设置”组中，单击“更改 **Appflow** 设置”。

c) 选择 **Connection Chaining**（连接链）并单击 **OK**（确定）。

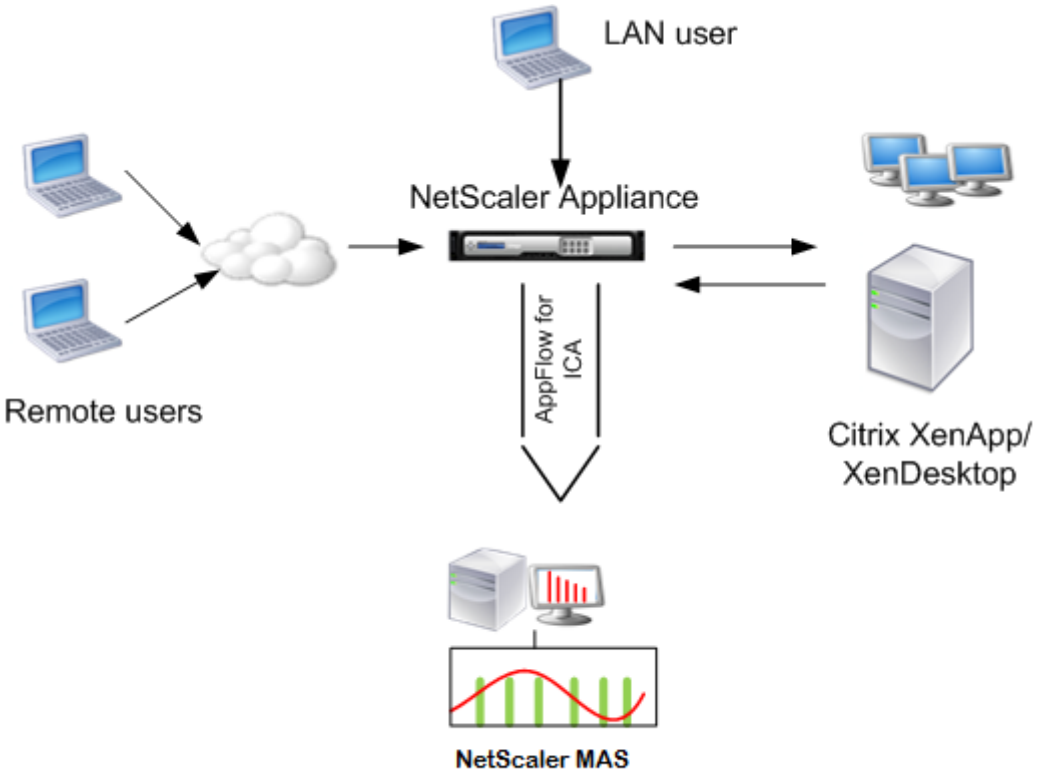
启用数据收集以监视在 **LAN** 用户模式下部署的 **Citrix ADC**

April 23, 2021

访问 Citrix 虚拟应用程序或桌面应用程序的外部用户必须在 Citrix Gateway 上对自己进行身份验证。但是，内部用户可能不需要重定向到 Citrix Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便将请求重定向到 Citrix ADC 设备。

要克服这些挑战，并让 LAN 用户直接连接到 Citrix Virtual Apps and Desktops 应用程序，您可以通过配置缓存重定向虚拟服务器（该服务器充当 Citrix 网关设备上的 SOCTS 代理）以 LAN 用户模式部署 Citrix ADC 设备。

图 4. 在局域网用户模式下部署的 Citrix ADM



注意： Citrix ADM 和 Citrix Gateway 设备位于同一子网中。

要监视在此模式下部署的 Citrix ADC 装置，请首先将 Citrix ADC 装置添加到 NetScaler 智能分析清单中，启用 AppFlow，然后在仪表板上查看报告。

将 Citrix ADC 装置添加到 Citrix ADM 清单后，必须为数据收集启用 AppFlow。

> 注意
>
> - 无法使用 Citrix ADM 配置实用程序在局域网用户模式下部署的 Citrix ADC 上启用数据收集。
> - 有关命令及其用法的详细信息，请参阅“命令参考”。

- 有关策略表达式的信息，请参阅“策略和表达式”。

要使用命令行界面在 **Citrix ADC** 装置上配置数据收集，请执行以下操作：

在命令提示窗口中执行以下操作：

1. 登录设备。
2. 添加转发代理缓存重定向虚拟服务器并提供代理 IP 和端口，指定服务类型为 HDX。

```
add cr vserver <name> <servicetype> [<ipaddress> <port>] [-
   cacheType <cachetype>] [ - cltTimeout <secs>]
<!--NeedCopy-->
```

示例：

```
add cr vserver cr1 HDX 10.12.2.2 443  - cacheType FORWARD  -
   cltTimeout 180
<!--NeedCopy-->
```

注意：如果您使用 Citrix Gateway 设备访问 LAN 网络，请添加要由匹配 VPN 流量的策略应用的操作。

```
add vpn trafficAction** <name> <qual> [-HDX ( ON | OFF )]

add vpn trafficPolicy** <name> <rule> <action>
<!--NeedCopy-->
```

示例：

```
add vpn trafficAction act1 tcp -HDX ON

add vpn trafficPolicy pol1 "REQ.IP.DESTIP == 10.102.69.17" act1
<!--NeedCopy-->
```

3. 将 Citrix ADM 添加为 Citrix ADC 设备上的 AppFlow 收集器。

```
add appflow collector** <name> \*\*-IPAddress\*\* <ip_addr>
<!--NeedCopy-->
```

示例：

```
add appflow collector MyInsight -IPAddress 192.168.1.101
<!--NeedCopy-->
```

4. 创建 AppFlow 操作，并将收集器与该操作关联。

```
add appflow action** <name> \*\*-collectors\*\* <string> ...
<!--NeedCopy-->
```


示例：

```
add appflow action act -collectors MyInsight
<!--NeedCopy-->
```

5. 创建 AppFlow 策略以指定用于生成流量的规则。

```
add appflow policy** <policyname> <rule> <action>
<!--NeedCopy-->
```

示例：

```
add appflow policy pol true act
<!--NeedCopy-->
```

6. 将 AppFlow 策略绑定到全局绑定点。

```
bind appflow global** <policyname> <priority> \*\*-type\*\* <type>
<!--NeedCopy-->
```

示例：

```
bind appflow global pol 1 -type ICA_REQ_DEFAULT
<!--NeedCopy-->
```

> 注意
>
> 类型的值必须是 ICA 流量的 ICA _REQ_ 覆盖或 ICA _REQ_DEFAULT 才能应用于 ICA 流量。

7. 将 AppFlow 的 flowRecordInterval 参数值设置为 60 秒。

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

示例：

```
set appflow param -flowRecordInterval 60
<!--NeedCopy-->
```

8. 保存配置。

```
save ns config
<!--NeedCopy-->
```


为 **HDX Insight** 创建阈值并配置警报

April 23, 2021

通过 Citrix Application Delivery Management (ADM) 的 HDX HDX Insight 功能，您可以监视通过 Citrix ADC 实例的 HDX 流量。Citrix ADM 允许您在用于监视智能分析通信量的各种计数器上设置阈值。您还可以在 Citrix ADM 中配置规则和创建警报。

HDX 流量类型与各种实体（如应用程序、桌面、网关、许可证和用户）相关联。每个实体都可以包含与其关联的不同指标。例如，应用程序实体与各种点击、应用程序消耗的带宽和服务器的响应时间相关联。用户实体可以与用户使用的 WAN 延迟、DC 延迟、ICA RTT 和带宽相关联。

Citrix ADM 中 HDX Insight 能分析的阈值管理允许您在超过设置的阈值时主动创建规则并配置警报。现在，此阈值管理已扩展到配置一组阈值规则。现在，您可以监视组而不是单个规则。阈值规则组包含一个或多个用户定义的阈值规则，用于从实体（如用户、应用程序和桌面）中选择的度量。每个规则都会根据您在创建规则时输入的预期值进行监视。对于用户实体，阈值组也可以与地理位置相关联。

仅当违反了配置的阈值组中的所有规则时，才会在 Citrix ADM 上生成警报。例如，您可以以一个阈值组的形式监视应用程序的总会话启动次数和应用程序启动次数。仅当两个规则都被违反时，才会生成警报。这允许您在实体上设置更逼真的阈值。

下面列出了几个示例：

- 阈值规则 1：用户（实体）的 ICA RTT（指标）必须 <= 100 毫秒
- 阈值规则 2：用户（实体）的 WAN 延迟（指标）必须 <= 100 毫秒

阈值组的示例可以是：{阈值规则 1 + 阈值规则 2}

要创建规则，必须首先选择要监视的实体。然后在创建规则时选择指标。例如，您可以选择应用程序实体，然后选择总会话启动计数或应用程序启动计数。您可以为实体和量度的每个组合创建一个规则。使用提供的比较器（>、<、>= 和 <=）并为每个指标键入阈值。

> 注意
>
> 如果不想监视单个组中的多个实体，则必须为每个实体创建单独的阈值规则组。

当计数器的值超过阈值时，Citrix ADM 会生成一个事件来表示违反阈值，并为每个事件创建警报。

您必须配置接收警报的方式。您可以启用在 Citrix ADM 上显示警报和/或在移动设备上以电子邮件或 SMS 形式接收警报。对于最后两个操作，您必须在 Citrix ADM 上配置电子邮件服务器或 SMS 服务器。

阈值组也可以绑定到地理位置，以便对用户实体进行地理特定监视。

示例使用案例

ABC Inc. 是一家全球性的公司，在 50 多个国家设有办事处。该公司有两个数据中心，一个位于新加坡，另一个位于加利福尼亚州，负责托管 Citrix Virtual Apps and Desktops。公司的员工使用 Citrix 网关和基于 Citrix GSLB 的重

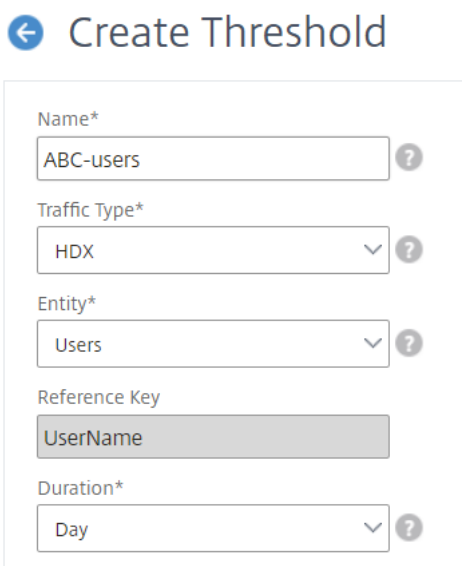
定向访问全球各地的 Citrix Virtual Apps and Desktops。ABC 公司的 Citrix Virtual Apps and Desktops 管理员 Eric 希望跟踪其所有办公室的用户体验，以优化应用程序和桌面交付，随时随地访问。Eric 还希望检查用户体验指标，如 ICA RTT，延迟，并主动提出任何偏差。

ABC Inc. 的用户有一个分布式的存在。有些用户位于数据中心附近，有些用户位于远离数据中心的地方。随着用户群的分布广泛，指标和相应的阈值也因这些位置而异。例如，靠近数据中心的位置的 ICA RTT 可能是 5—10 ms，而远程位置的 ICA RTT 可能是 100 ms 左右。

借助 HDX Insight 的阈值规则组管理，Eric 可以为每个位置设置特定于地理位置的阈值规则组，并通过电子邮件或短信向每个区域发出违规警报。Eric 还能够将对阈值规则组中多个指标的跟踪结合起来，并将根本原因缩小到容量问题（如果有）。Eric 现在能够主动跟踪任何偏差，而不必担心手动查看所有 Citrix Virtual Apps and Desktops 产品组合指标的复杂性。

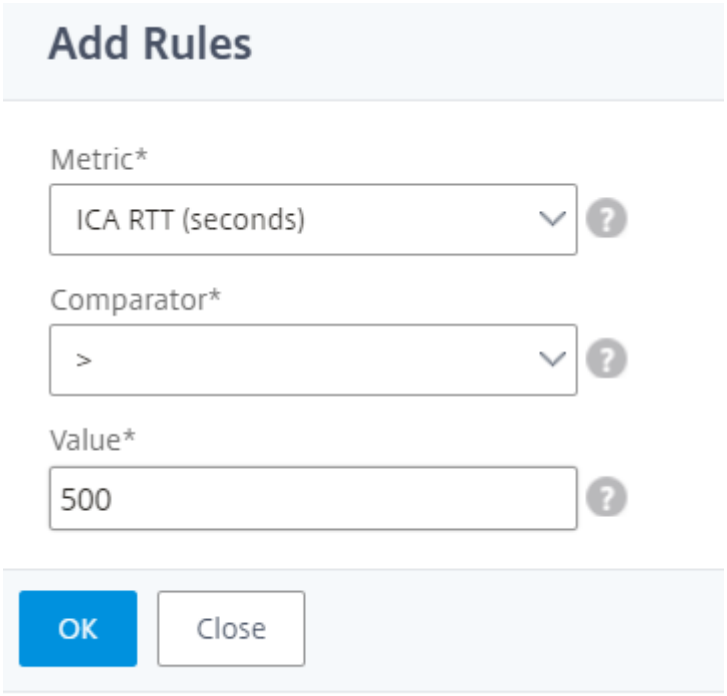
要使用 **Citrix ADM** 创建阈值规则组并为 **HDX Insight** 配置警报，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “分析” > “ 设置” > “ 阈值”。在打开的阈值页面上，单击添加。
2. 在 **Create Thresholds and Alerts**（创建阈值和警报）页面上，指定以下详细信息：
   a) 名称。键入用于创建 Citrix ADM 为其生成警报的事件的名称。
   b) 流量类型。从列表框中，选择 HDX。
   c) 实体。从列表框中，选择类别或资源类型。您之前选择的每种流量类型的实体不同。
   d) 引用键。将根据您选择的流量类型和实体自动生成引用密钥。
   e) 持续时间。从列表框中，选择要监视实体的时间间隔。您可以监视实体一小时、一天或一周的持续时间。

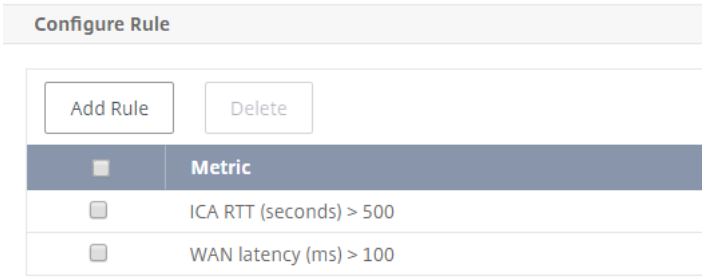


3. 为所有实体创建阈值规则组：

   对于 HDX 通信，您必须通过单击 添加规则来创建规则。输入打开的 “ 添加规则” 弹出窗口中的值。

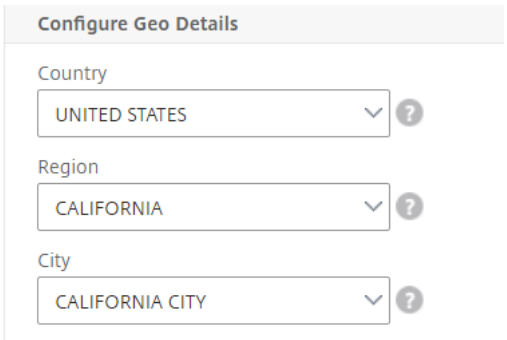


您可以创建多个规则来监视每个实体。在一个组中创建多个规则允许您将实体作为一组阈值规则而不是单个规则来监视。单击确定关闭窗口。



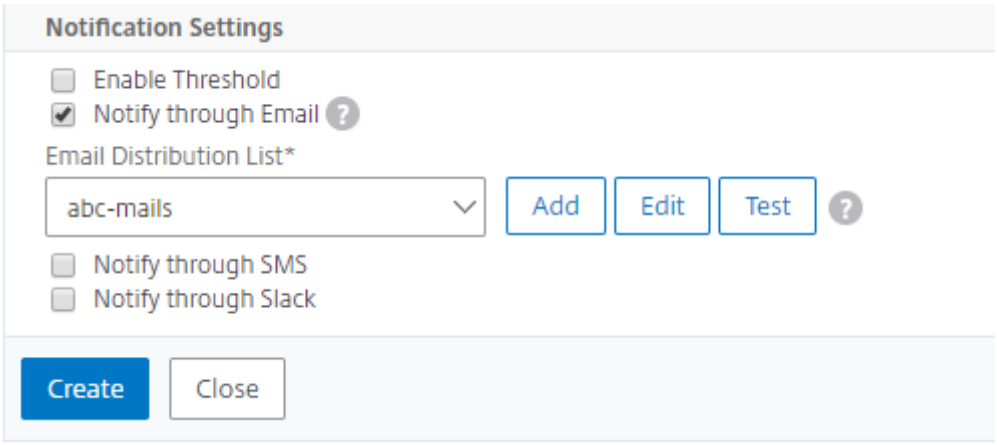
4. 配置用户实体的地理位置标记

   或者，您可以在配置地理详细信息部分为用户实体创建基于位置的警示。下图显示了创建基于地理位置的标记以监视美国西海岸用户 WAN 延迟性能的示例。



5. 单击启用阈值以允许 Citrix ADM 开始监视实体。

6.（可选）配置操作，如电子邮件通知和 SMS 通知。



7. 单击创建以创建阈值规则组。

查看 **HDX Insight** 报告和指标

April 23, 2021

HDX Insight 提供与 Citrix ADC 实例上 HDX 流量相关的报告和指标的完整可见性。

您可以查看任何选定实体的 HDX 指标。视图中包括以下类别的实体：

- 用户：显示在选定时间间隔内访问 Citrix 虚拟应用程序或桌面的所有用户的报告。
- 应用程序：显示应用程序总数的报告，以及所有相关信息，如在指定时间间隔内启动应用程序的总次数。
- 实例：显示用作传入流量网关的 Citrix ADC 实例的报告。
- 桌面：显示在选定时间范围内使用的桌面的报告。
- 许可证：显示在指定时间段内使用的 SSL VPN 许可证总数的报告。

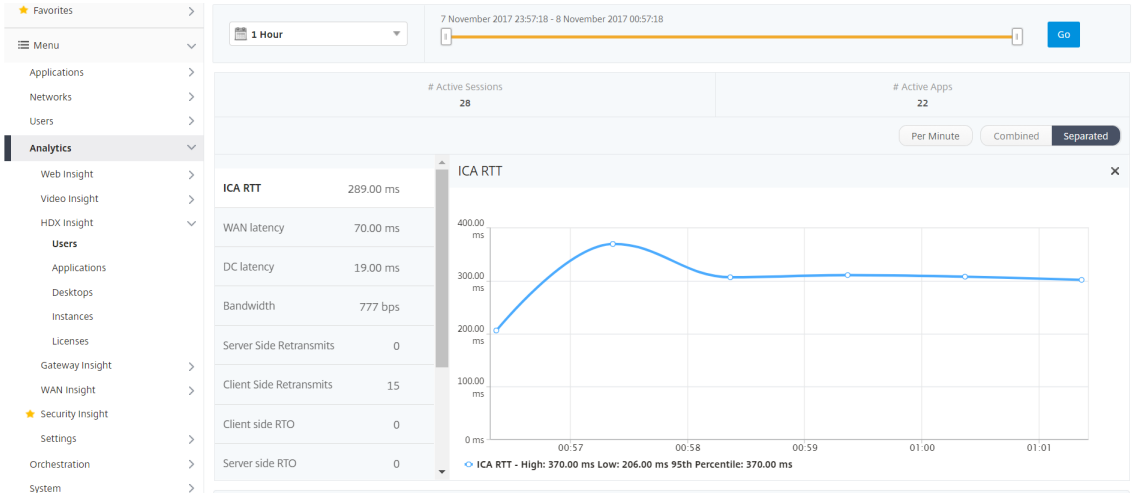
> 注意
>
> “许可证”值不适用于 Citrix SD-WAN 设备。

用户查看报告和指标

此视图中的报告和衡量指标按 Citrix Virtual Apps 和桌面用户显示。

要导航到用户视图，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户



用户视图报告和度量由以下部分组成：

- Summary View（摘要视图）
- Per User View（每个用户视图）
- Per User Session View（每个用户会话视图）

Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有用户的报告。除非另有指定，否则此视图中的所有指标/报告都会显示所选时间段内与其对应的值。

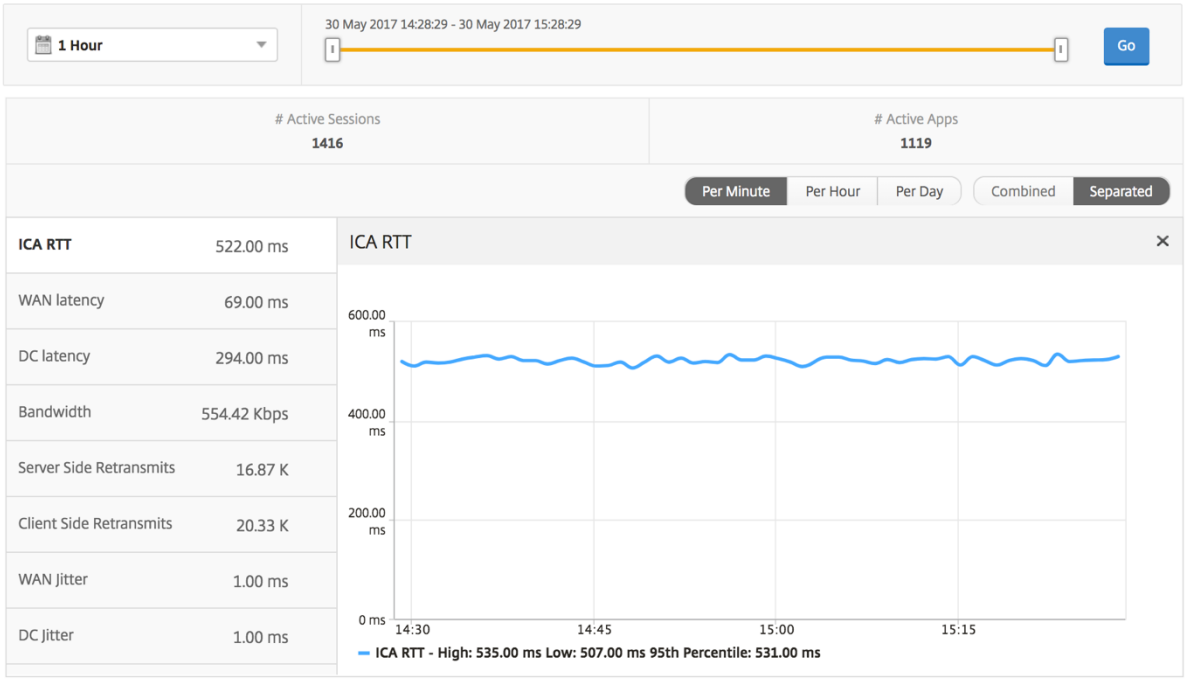
要更改选定时间段，请执行以下操作：

1. 使用时间段列表或时间滑块设置所需的时间间隔。
2. 单击转到。

折线图

指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。

指标	说明
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



用户摘要报告

下面是与此报告特定相关的指标。

指标	说明
活动会话数	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Total App Launch Count（应用程序启动总数）	在选定的时间段内用户启动的应用程序总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。

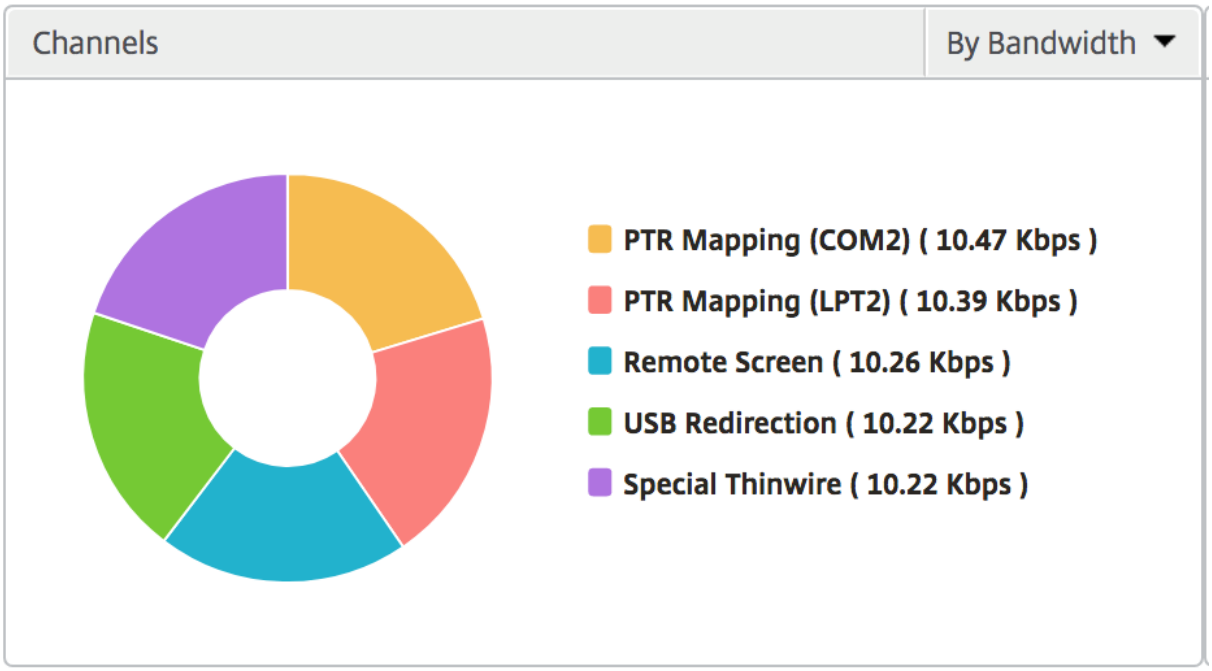
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

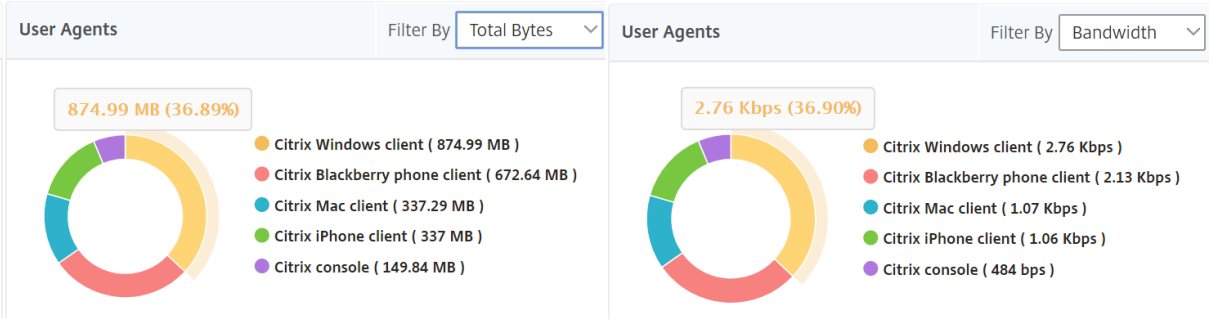
通道

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。

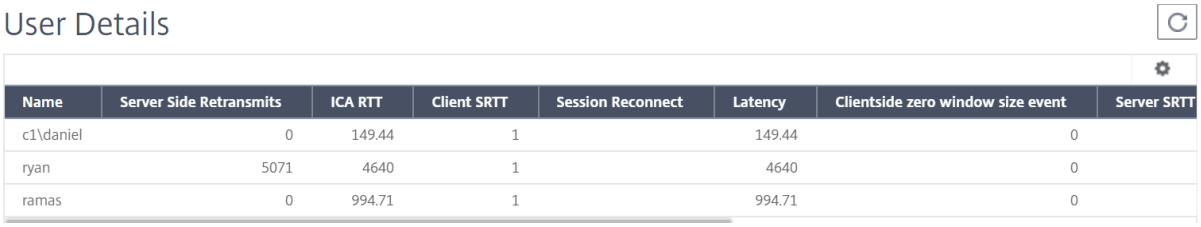


用户代理

用户代理以甜圈图表的形式表示每个接收器客户端使用的总带宽/总字节。图表中的每个彩色段代表一个接收器客户端。段的长度取决于在该接收器客户端上启动其应用程序的用户数。您还可以按带宽或总字节对指标进行排序。



单击每个段可查看使用该接收器客户端的用户详细信息。



Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

阈值违规计数

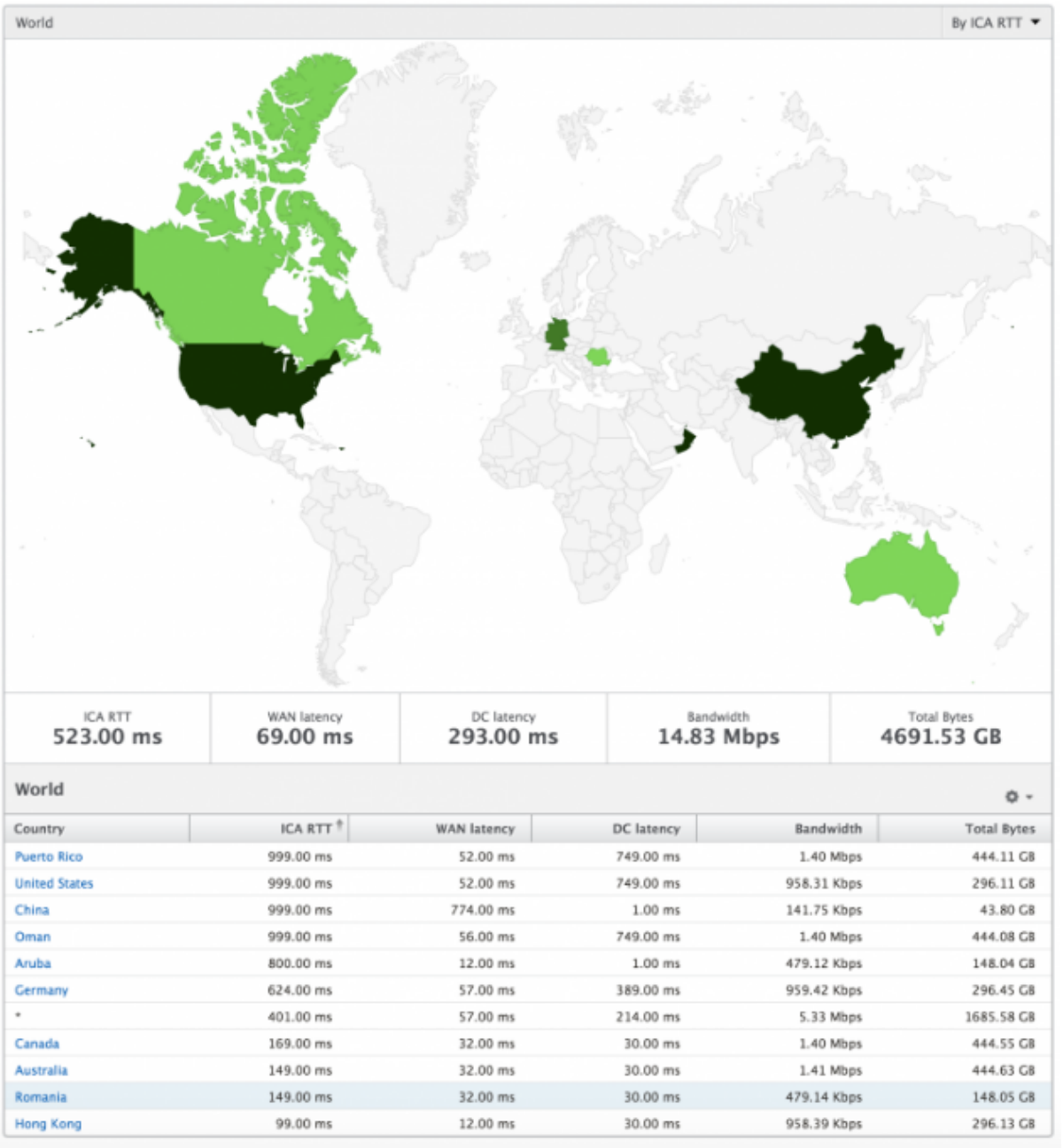
阈值违反计数指标表示在选定时间段内违反的阈值计数。

世界地图

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以查看系统的世界视图，向下钻取到特定国家/地区，进一步深入到城市，也可以通过单击该区域即可。管理员可以进一步向下钻取以按城市和州查看信息。从 Citrix ADM 12.0 及更高版本中，您可以深入查看从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

每用户视图

“Per User View”（每个实例视图）提供任何特定的选定用户的详细最终用户体验报告。

要导航到特定用户的度量，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户。
3. 从“User Summary Report”（用户摘要报告）部分中选择特定用户。

折线图

折线图显示在选定时间段内特定的选定用户的所有指标摘要。

当前/终止的会话报告

此报告与选定用户的所有当前/已终止用户会话有关。这些指标可以按开始时间、会话重新连接数和 ACR 计数排序。

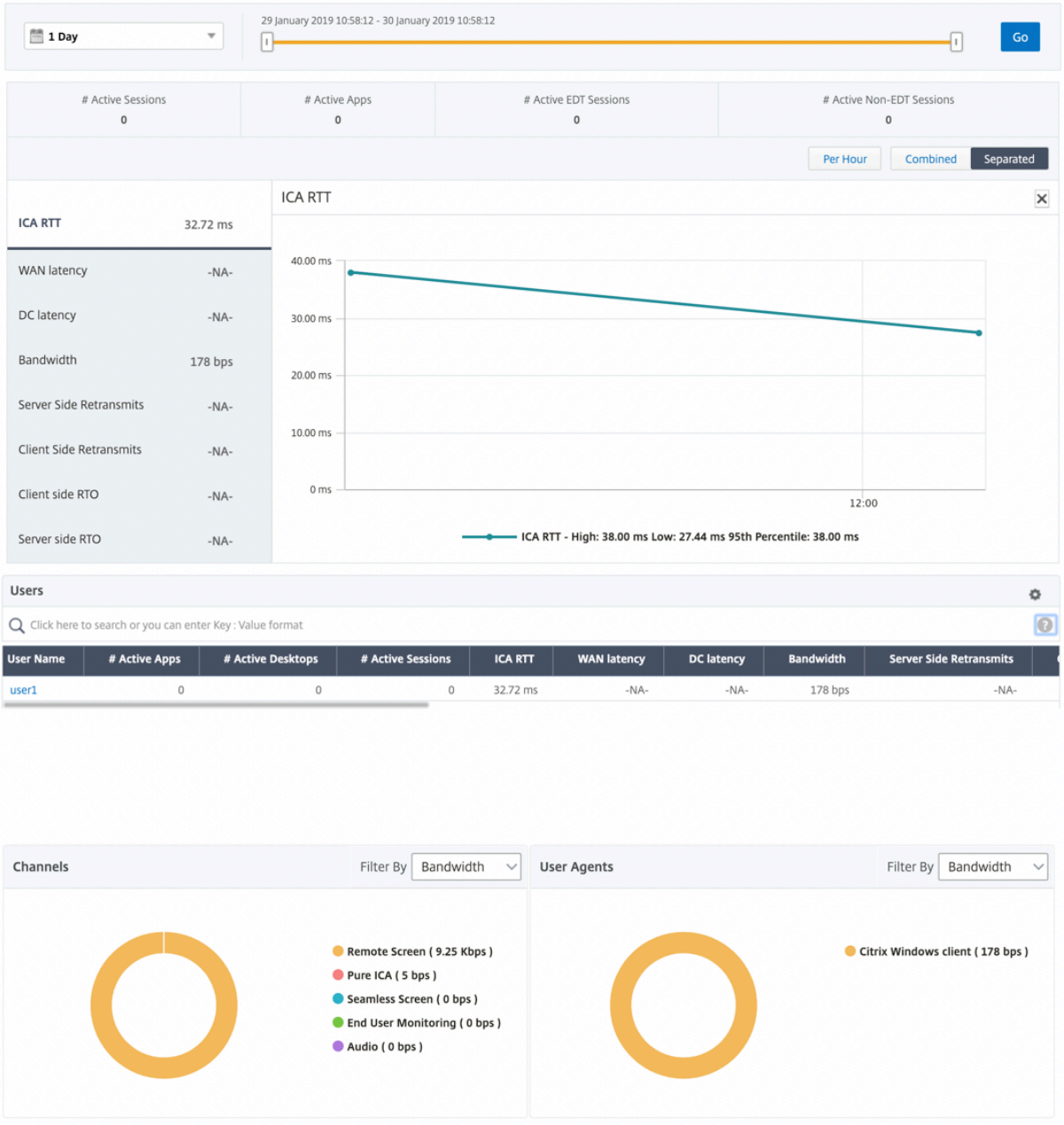
指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。

指标	说明
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。

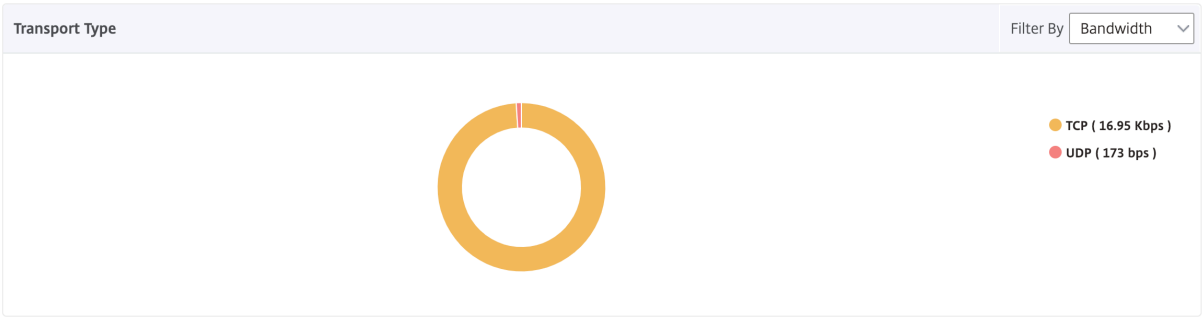
支持 **HDX** 洞察中的 **EDT**

Citrix Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示针对 HDX 智能分析的分析。也就是说，ADM 现在同时支持 UDP 和 TCP 协议。对 Citrix Gateway 的 EDT 支持可确保为运行 Citrix Receiver 的用户提供高清晰度的虚拟桌面会话中用户体验。

HDX Insight 现在将 EDT 会话数和非 EDT 会话数作为活动会话报告的一部分显示。“用户” (Users) 表格显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传、RTO 等衡量指标，以及当前从 TCP 堆栈计算时确实具有 EDT 会话的用户不可用。因此，它们显示为 “NA”。



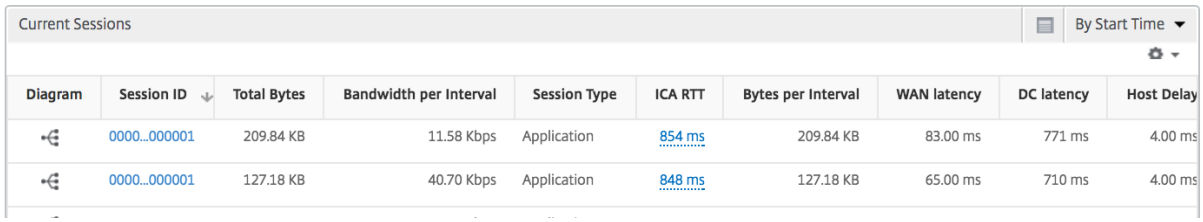
引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。

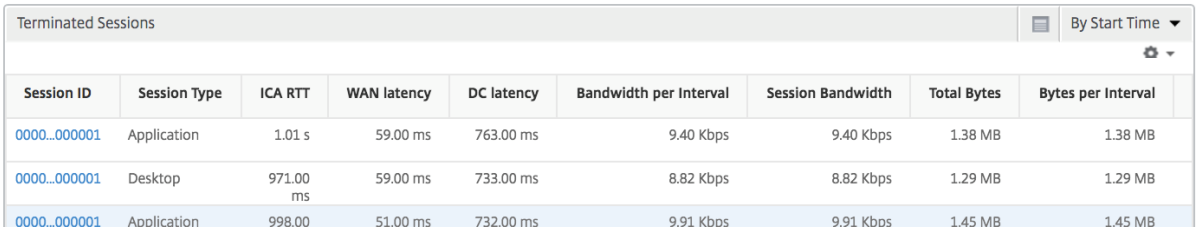


> 注意：从版本 12.1 版本 50.28 开始的 Citrix ADM 支持 HDX Insight 能分析中的
>
> EDT，并且在版本 12.1 版本 49.23 开始的 ADC 实例上可用。

Citrix ADM 12.0 及更高版本中提供的 **HDX Insight** 分析指标：

L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
L7 Server-side Latency（L7 服务器端延迟）	Citrix ADC 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。

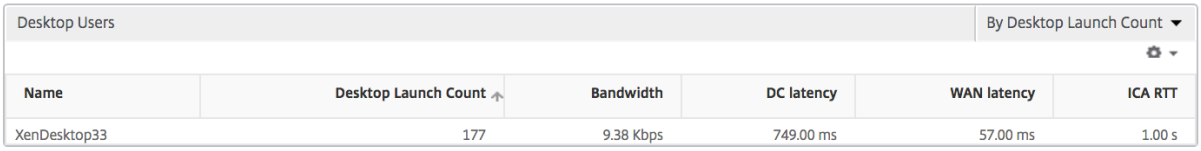




桌面用户

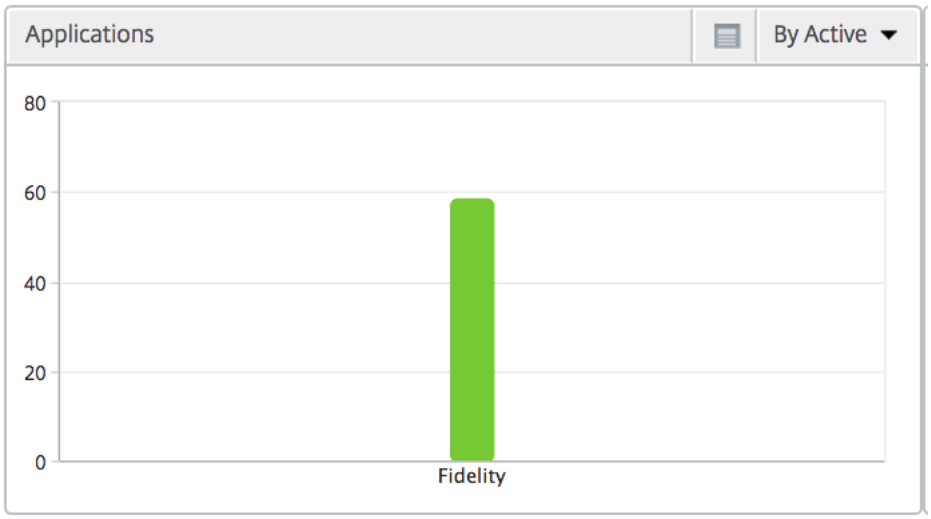
此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN Latency（WAN 延迟）	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。



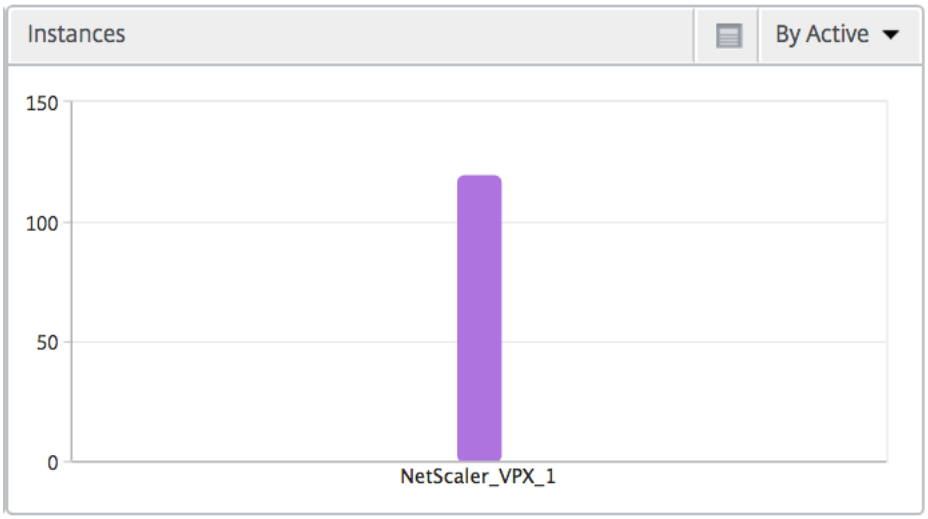
应用程序

一个条形图，表示按活动状态、总会话启动次数、总应用程序启动次数和启动持续时间排序的应用程序。



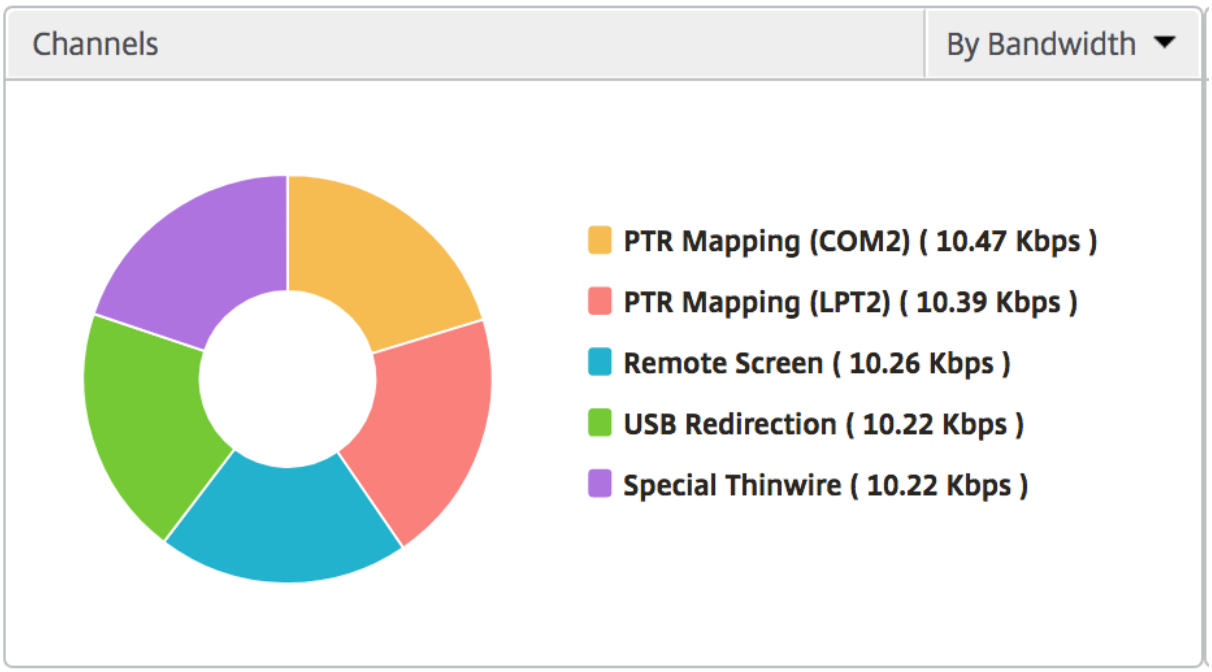
实例

表示按活动应用程序和总应用程序排序的 Citrix ADC 实例的条形图



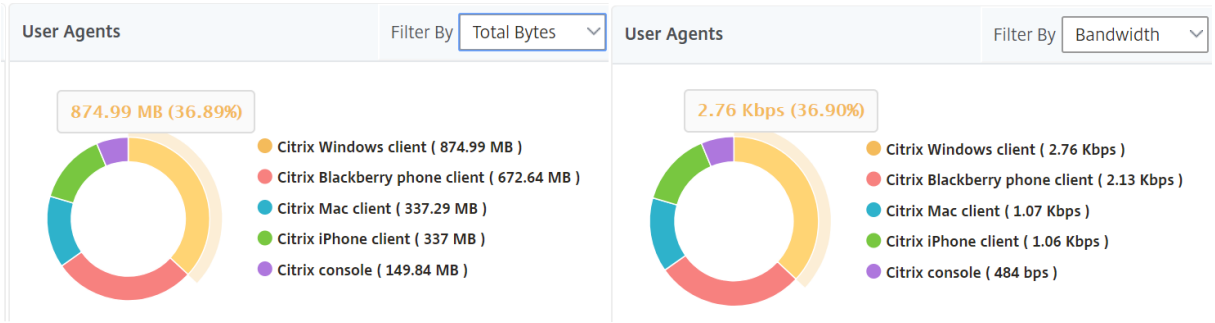
通道

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



用户代理

“User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



每用户会话视图

“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

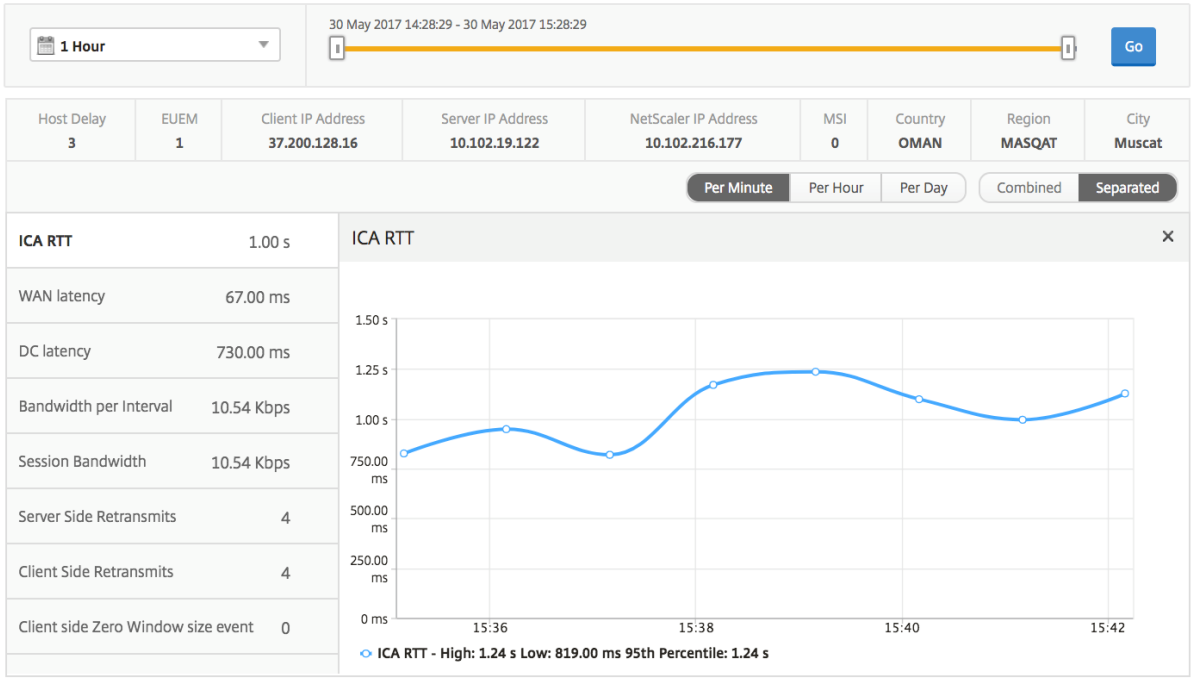
要查看选定用户会话的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或终止的会话列中选择会话。

时间线图

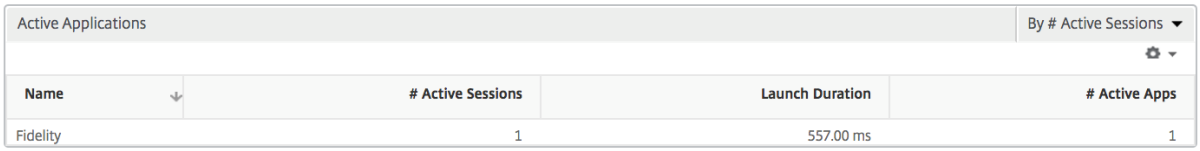
指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



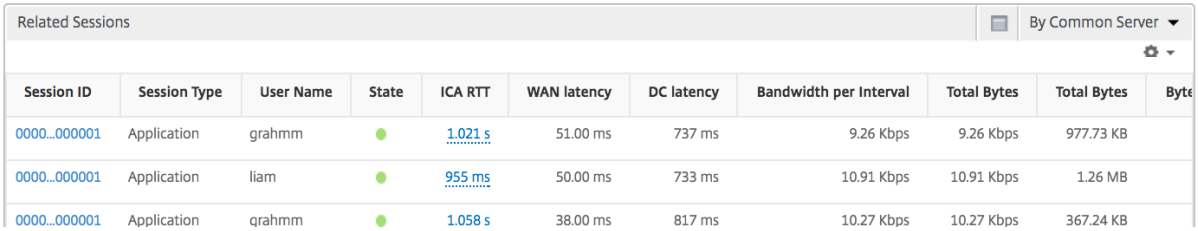
活动应用程序

“活动应用程序”部分显示选定用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间排序。



相关会议

“Related Sessions”（相关会话）部分显示选定用户的会话的相关会话。可以选择该关系作为公用服务器或通用 Citrix ADC。



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

“Application”（应用程序）视图报告和指标

此视图中的报告和衡量指标侧重于 Citrix Virtual Apps。

要定位至 **“**应用程序**”** 视图，请执行以下操作：

1. 导航到 “ 分析” > “ **HDX Insight** ” > “ 应用程序”。

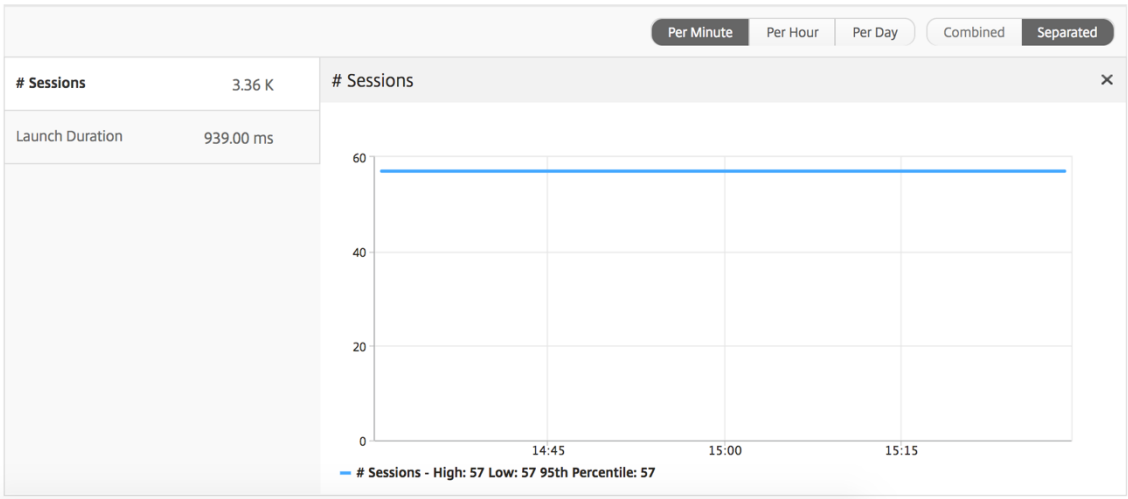
Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有应用程序的报告。

除非明确提及，否则所有指标/报告将具有与所选时间段相对应的值。

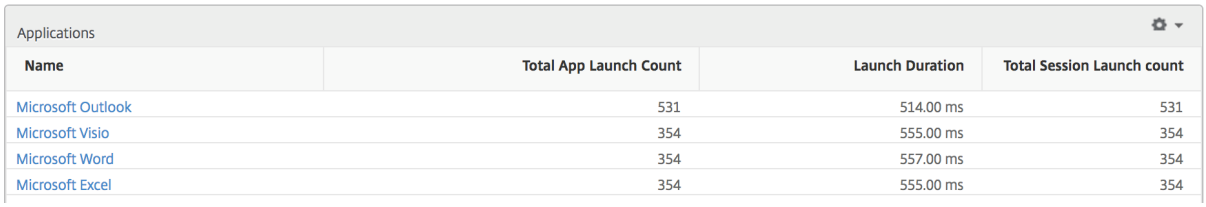
折线图

指标	说明
会话数	在给定时间间隔内的会话总数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。



应用程序摘要报告

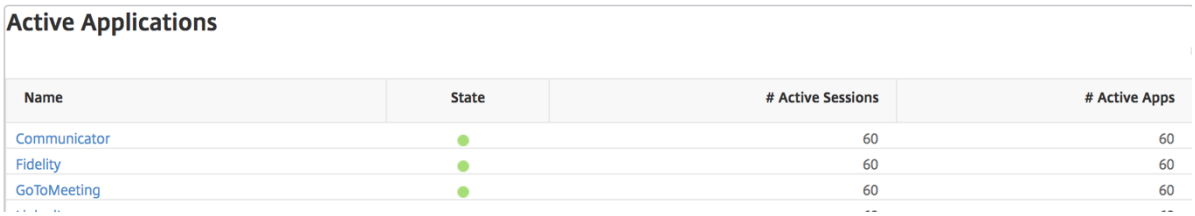
指标	说明
名称	Citrix 虚拟应用程序的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内的活动 Citrix 虚拟应用程序会话总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix 虚拟应用程序总数。
Launch Duration（启动持续时间）	启动 Citrix 虚拟应用程序所需的平均时间。



Name	Total App Launch Count	Launch Duration	Total Session Launch count
Microsoft Outlook	531	514.00 ms	531
Microsoft Visio	354	555.00 ms	354
Microsoft Word	354	557.00 ms	354
Microsoft Excel	354	555.00 ms	354

活动应用程序报告

指标	说明
名称	Citrix 虚拟应用程序的名称。
状态	显示应用程序的状态：绿色-活动，红色-非活动
# Active Sessions（活动会话数）	在给定时间间隔内使用此应用程序的活动用户会话数。
# Active Apps（活动应用程序数）	此应用程序的活动会话数。

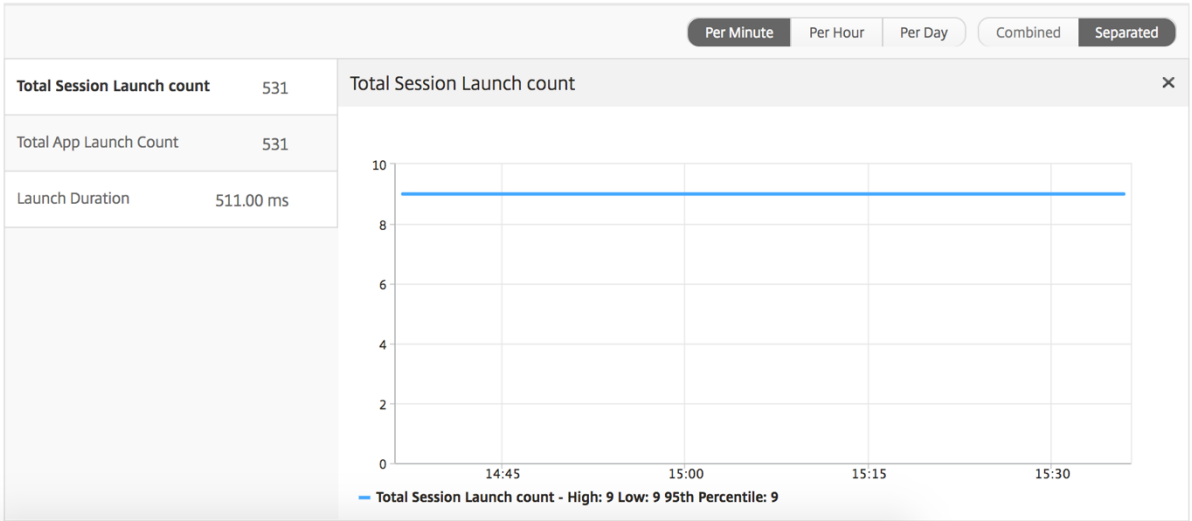


阈值报告

阈值报告表示在选定期间内将 实体选为应用程序的超过阈值计数。有关详细信息，请参阅如何创建阈值。

折线图

指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。



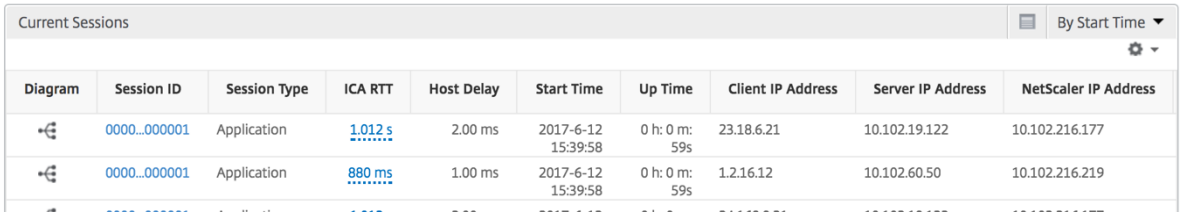
当前会话报告

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。

指标	说明
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。

指标	说明
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
用户名	访问此特定 Citrix 虚拟应用程序的用户的用户名。
会话 ID	Citrix 虚拟应用程序会话的唯一标识符。
会话类型	将为 “Application”（应用程序）。
状态	会话状态：绿色表示活动，红色表示处于活动状态。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于 “L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。

指标	说明
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
L7 Server-side Latency（L7 服务器端延迟）	Citrix ADC 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。



每个应用程序会话视图

“Per Application Session View”（每个应用程序会话视图）显示特定的选定应用程序会话的报告。

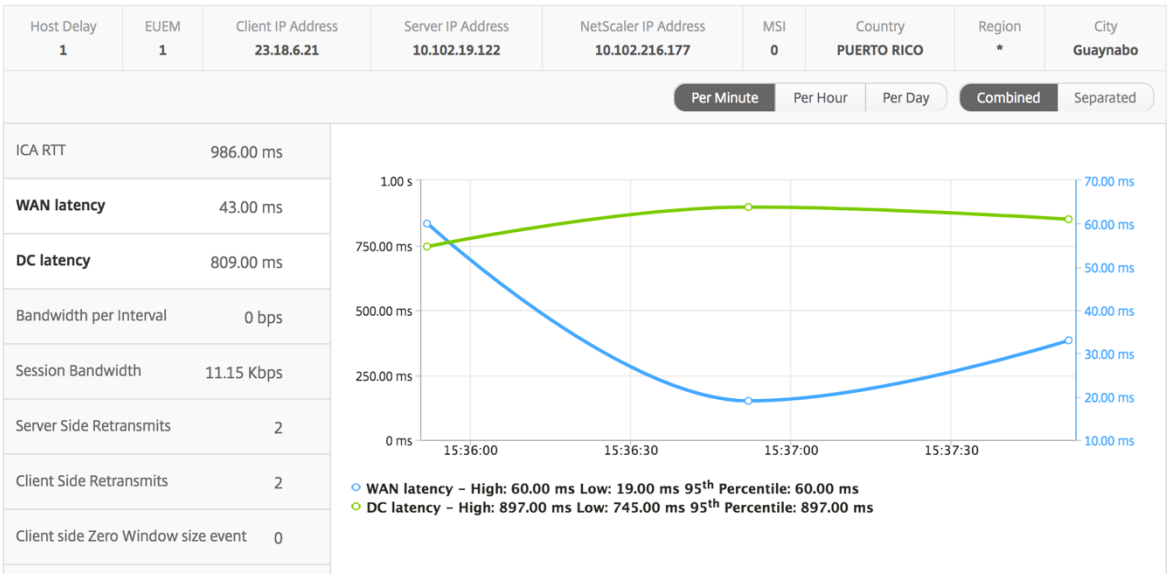
要查看会话报告，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 “ 分析” > “ **HDX Insight** ” > “ 应用程序”。
3. 从 “Application Summary Report”（应用程序摘要报告）中选择特定用户。
4. 从当前会话报告中选择会话。

折线图

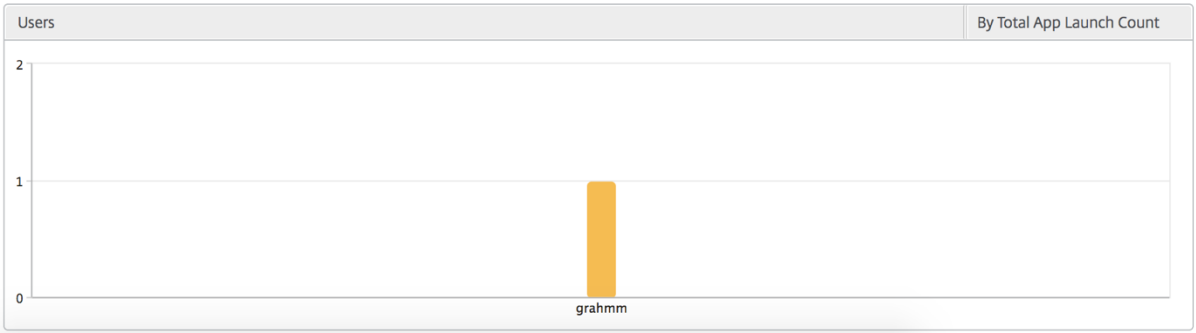
指标	说明
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。

指标	说明
Server side Zero Window size event（服务器端零窗口大小事件）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



用户条形图

用户条形图表示登录此特定应用程序的用户。



“Desktop”（桌面）视图报告和指标

此视图中的报告和衡量指标侧重于 Citrix Virtual Desktops。

要导航到桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 分析 > **HDX Insight** > 桌面。

Summary View（摘要视图）

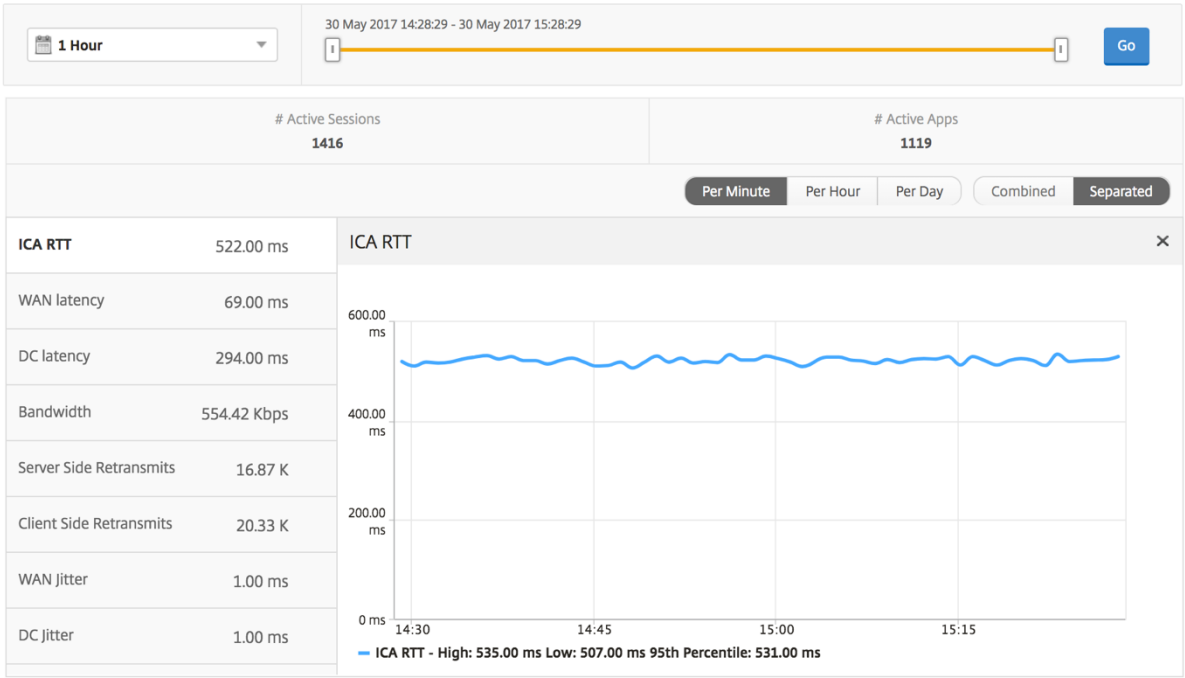
摘要视图显示在选定时间轴内登录的所有 Citrix Virtual Desktops 的报告。

除非明确提及，否则所有指标/报告将具有与所选时间段相对应的值。

折线图

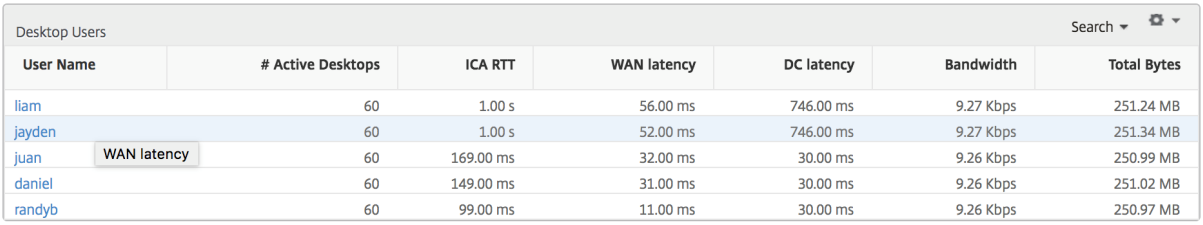
指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。

指标	说明
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



桌面摘要报告

指标	说明
活动会话	在指定时间间隔内的活动 Citrix 虚拟桌面会话总数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。



阈值报告

阈值报告表示在选定期间内将 实体选为桌面时所超过的阈值计数。有关详细信息，请参阅如何创建阈值。

每个桌面视图

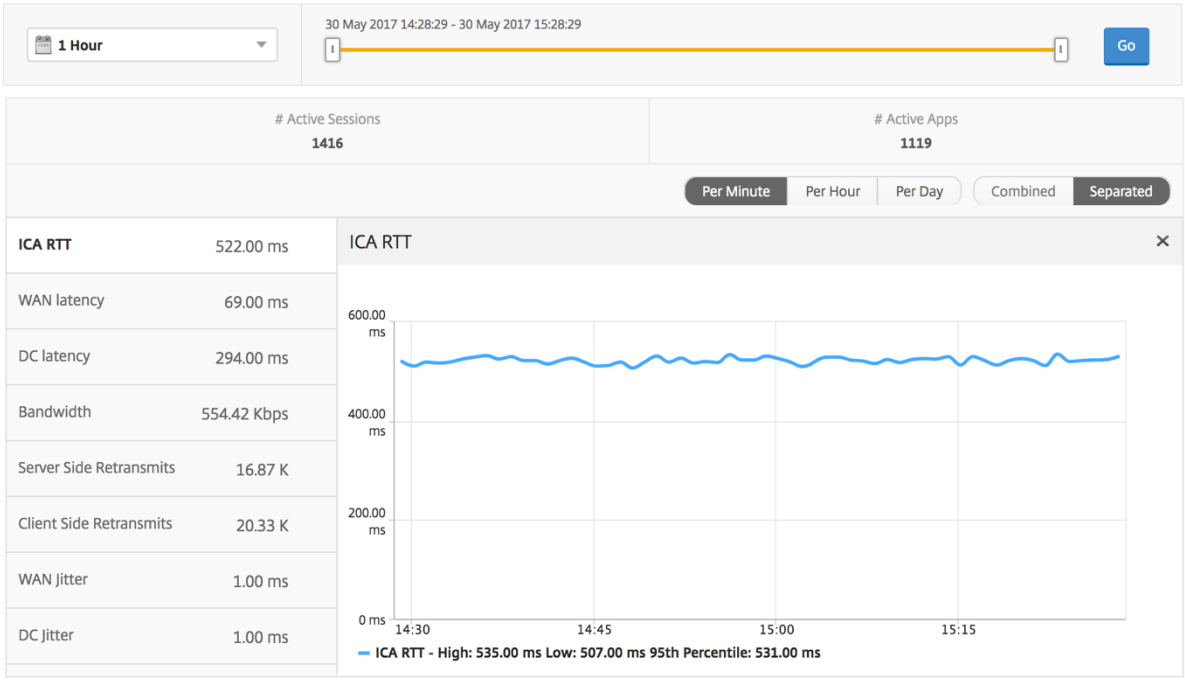
每个桌面视图提供了选定 Citrix 虚拟桌面的详细最终用户体验报告。

要导航到特定的桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 **“分析” > “HDX Insight” > “桌面”**。
3. 从 桌面摘要报告中选择特定桌面。

折线图

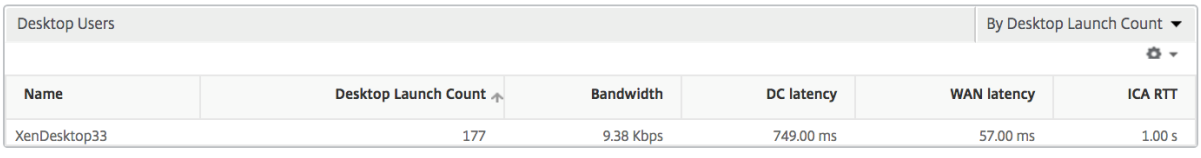
指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



桌面用户报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN Latency（WAN 延迟）	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

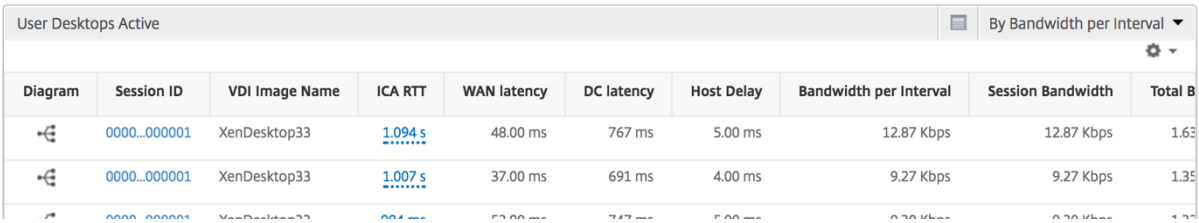


用户桌面活动/非活动报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。

指标	说明
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称
Diagram（示意图）	



每个桌面会话视图

每个桌面会话视图提供特定选定 Citrix 虚拟桌面会话的报告。

要导航到桌面会话视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 **“分析” > “HDX Insight” > “桌面”**。
3. 从桌面 摘要报告中选择特定桌面。
4. 从当前会话报告中选择会话。

时间线图

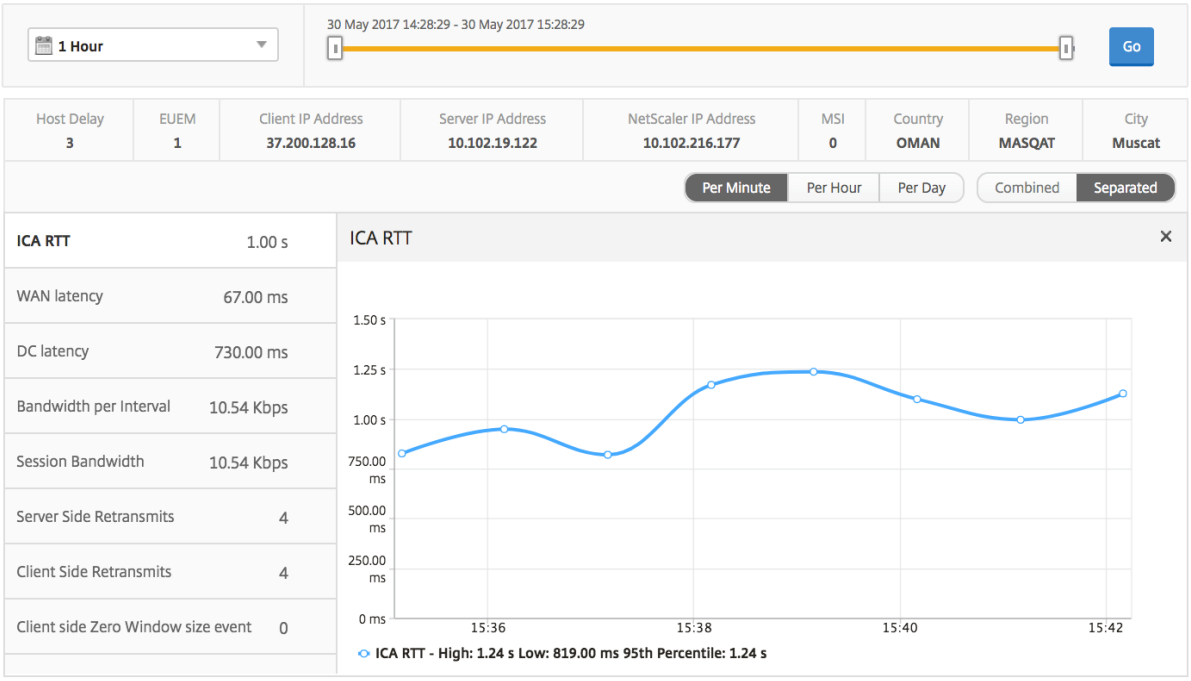
“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

要查看选定用户会话的度量，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到分析 > **HDX Insight** > 用户。
3. 从用户摘要报告部分选择特定用户。
4. 从当前会话或终止的会话列中选择会话。

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。

指标	说明
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。

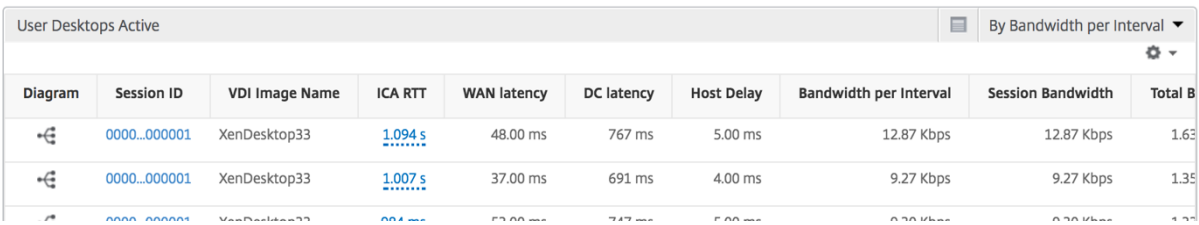


相关桌面会话报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。

指标	说明
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。



“Instance”（实例）视图报告和指标

实例视图中的报告和指标侧重于 Citrix ADC 实例。

要导航到 **“实例”** 视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 **“分析” > “HDX Insight” > “实例”**。

实例视图报告和指标由以下部分组成：

- Instance Summary View（实例摘要视图）
- Per Instance View（每个实例视图）

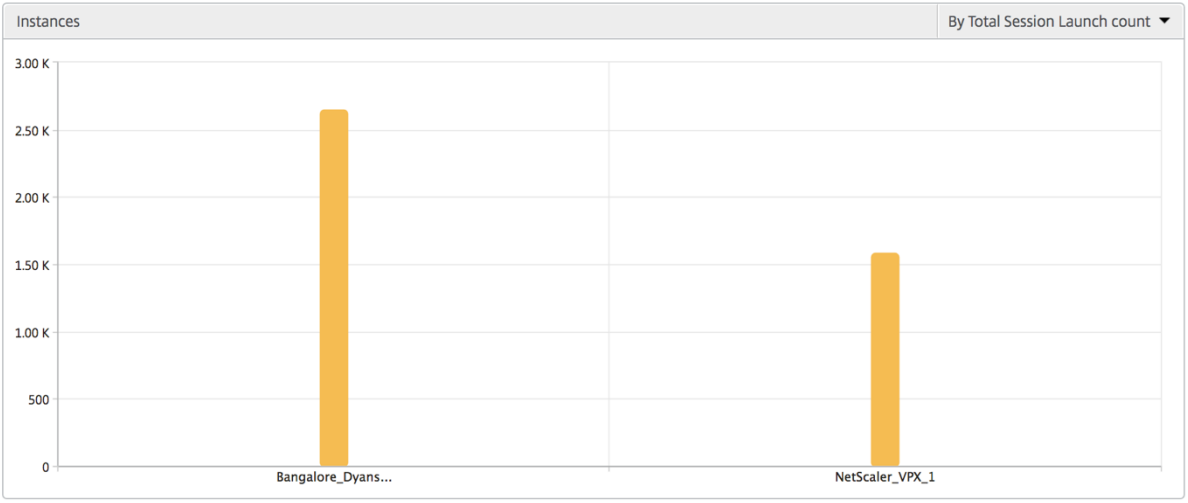
实例摘要视图

此视图称为摘要视图，因为它显示了添加到 Citrix ADM 的所有 Citrix ADC 实例的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

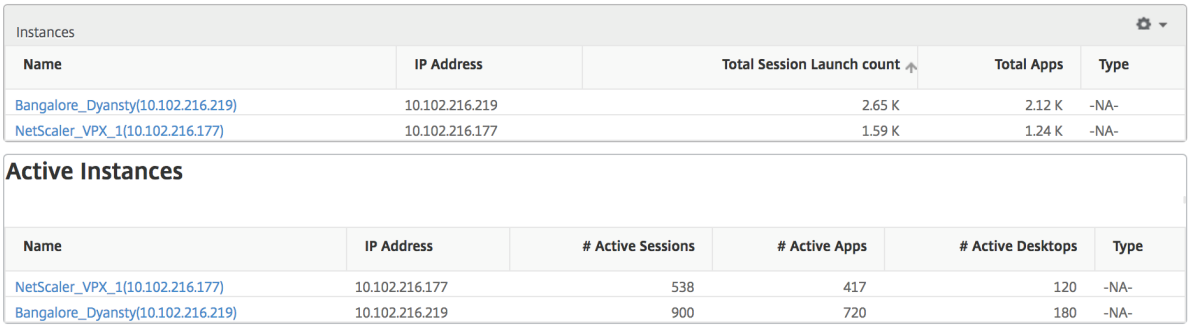
实例条形图

此图形显示实例与总会话启动计数的比较	可从图表画布右上角的列表中选择的应用程序总数。



实例/活动实例摘要报告

指标	说明
名称	Citrix ADC 实例的主机名。
IP 地址	NetScaler IP 地址。
Total Session Launch Count（会话启动总数）	在给定时间间隔内创建的唯一用户会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用

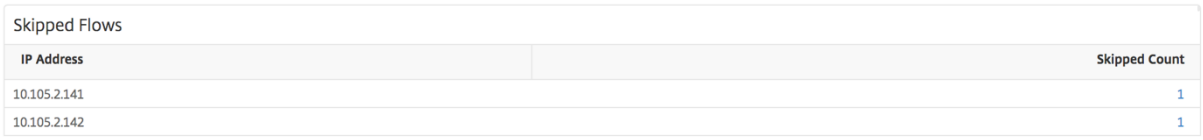


阈值报告

阈值报告表示在选定时间段内将实体选为实例的违反阈值计数。有关详细信息，请参阅如何创建阈值。

跳过的流

跳过的流是跳过解析 ICA 连接的记录。这可能是由于多种原因造成的，例如使用不受支持的 Citrix Virtual Apps 和桌面版本、不受支持的接收器或接收器类型版本等。此表显示了 IP 地址和跳过的流计数。这些接收器可能不是列入白名单的接收器的一部分。因此，这些会话将从监视中跳过。



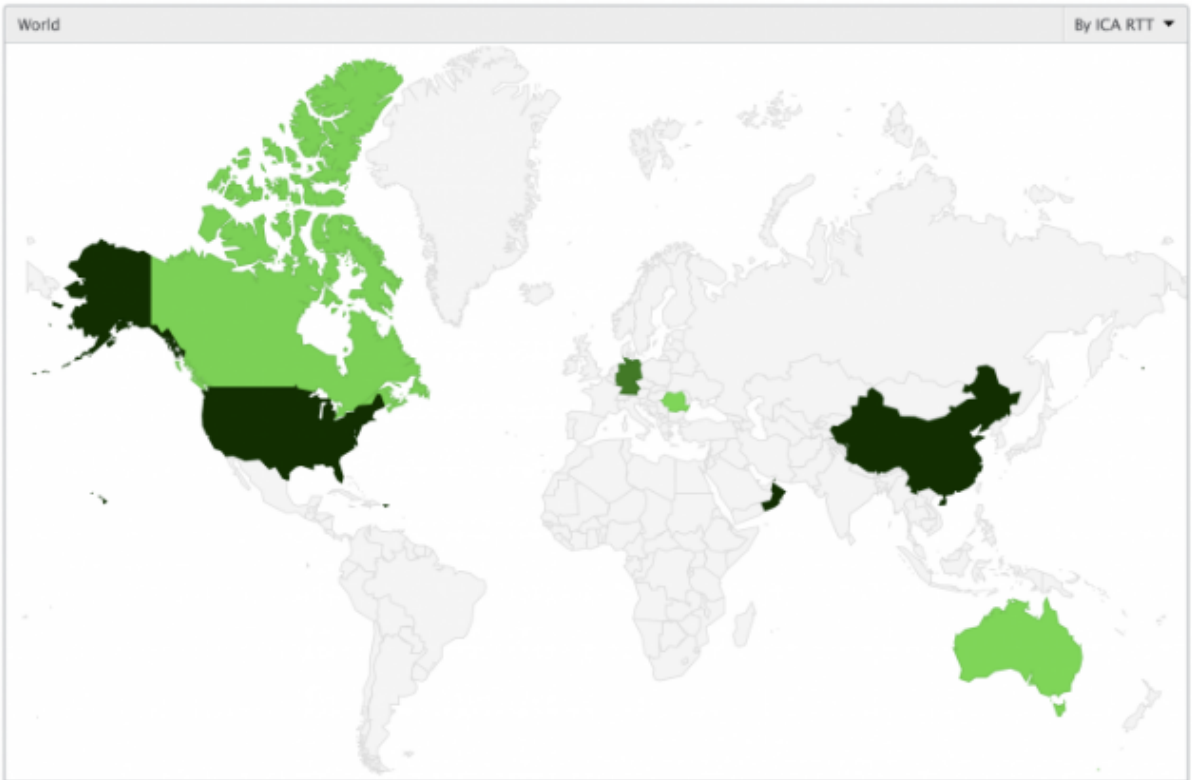
世界观

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市，以及只需单击区域即可。管理员可以进一步向下钻取以按城市和州查看信息。从 Citrix ADM 12.0 及更高版本中，您可以深入查看从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT

- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



World

Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

每个实例视图

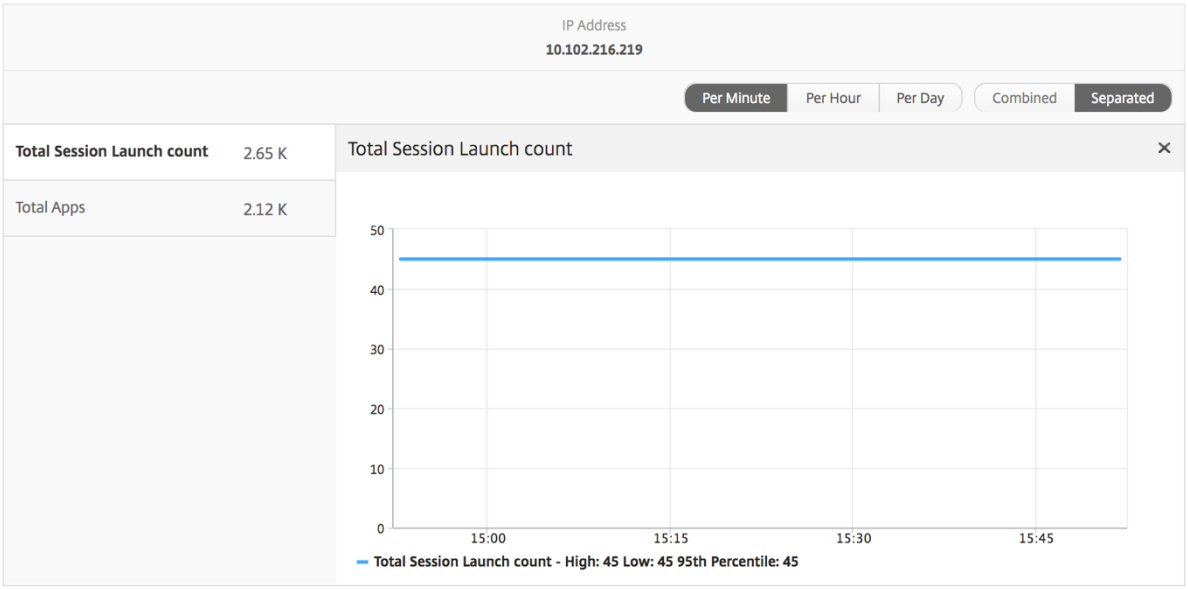
每个实例视图为特定选定的 Citrix ADC 实例提供详细的最终用户体验报告。

要导航到实例视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 **“分析” > “HDX Insight” > “实例”**。
3. 从 “实例 摘要报告” 中选择特定实例。

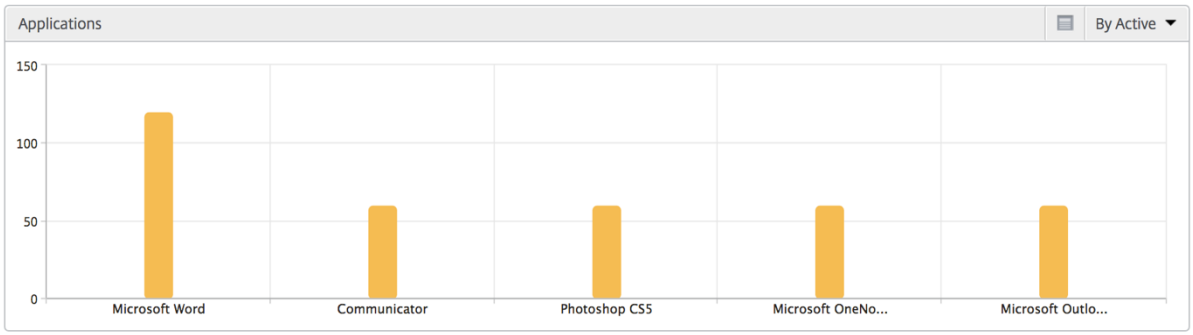
折线图

指标	说明
IP 地址	此项表示选定实例的 NetScaler IP 地址。
Total Session Launch count（会话启动总数）	在给定时间间隔内的活动 Citrix 虚拟应用程序会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。



“Applications”（应用程序）条形图

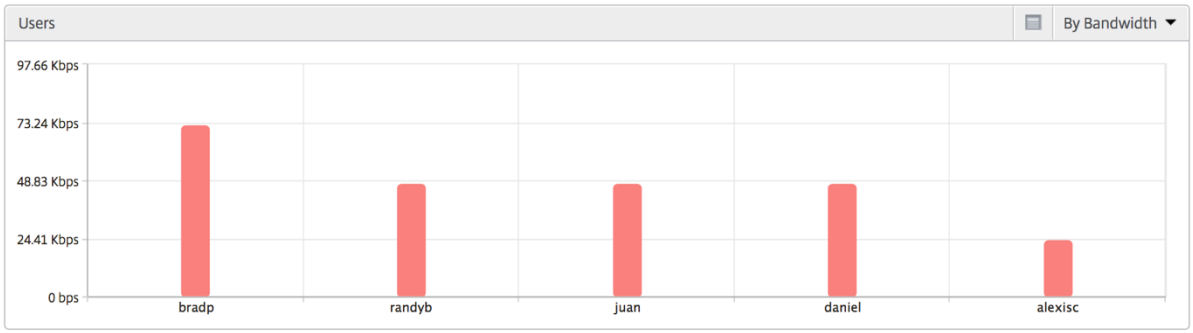
根据以下条件显示前 5 个应用程序-按活动应用程序、总会话启动次数、总应用程序启动次数或启动持续时间。



“Users”（用户）条形图

“Users”（用户）条形图基于以下条件显示排在前 5 位的用户

- Bandwidth（带宽）
- WAN 延迟
- DC 延迟
- ICA RTT

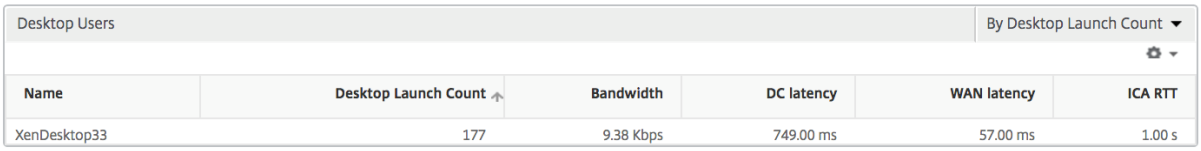


桌面用户报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN Latency（WAN 延迟）	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。

指标	说明
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

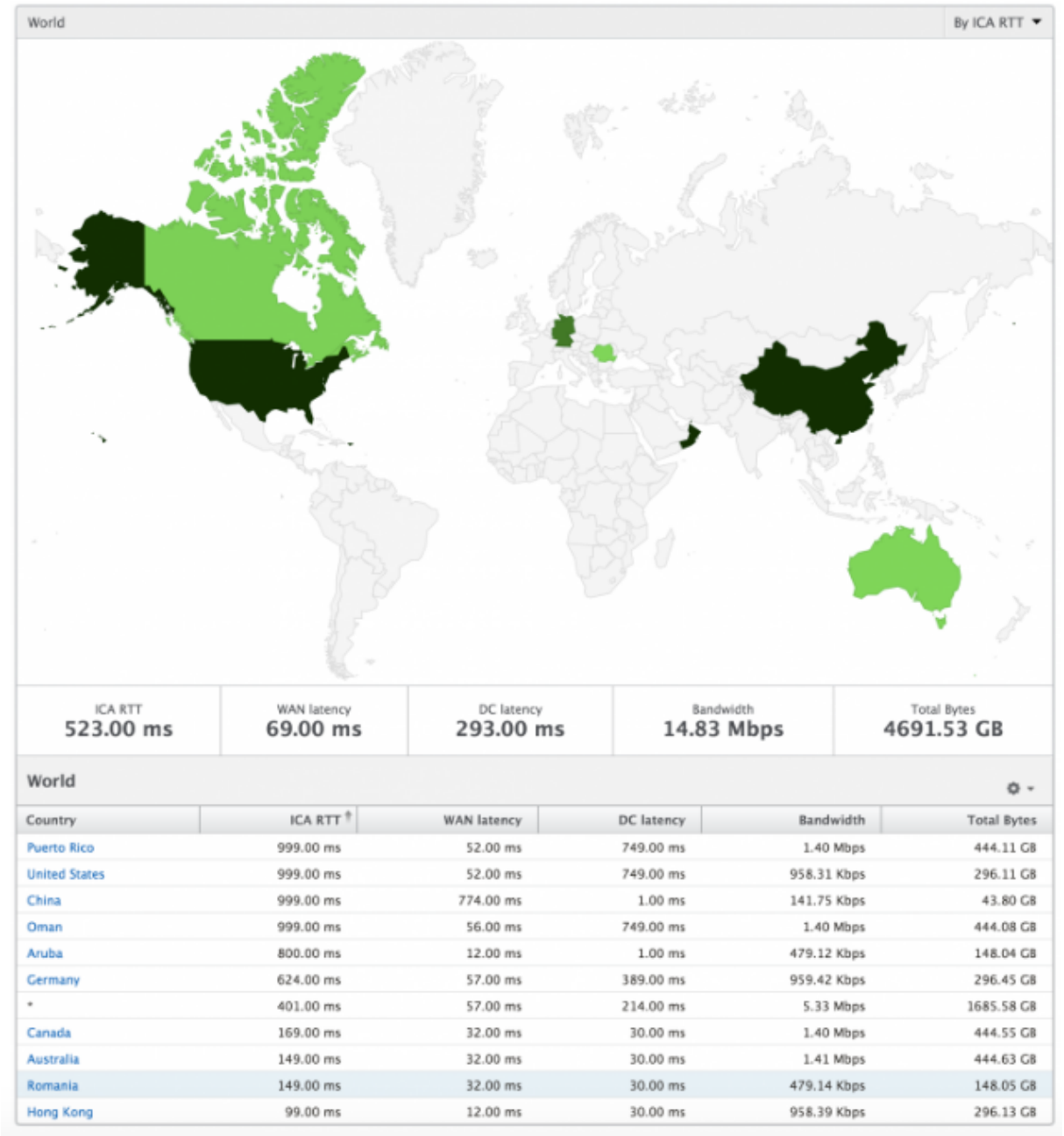


世界观

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市以及通过单击区域。管理员可以按城市和省/自治区/直辖市进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

许可证查看报告和指标

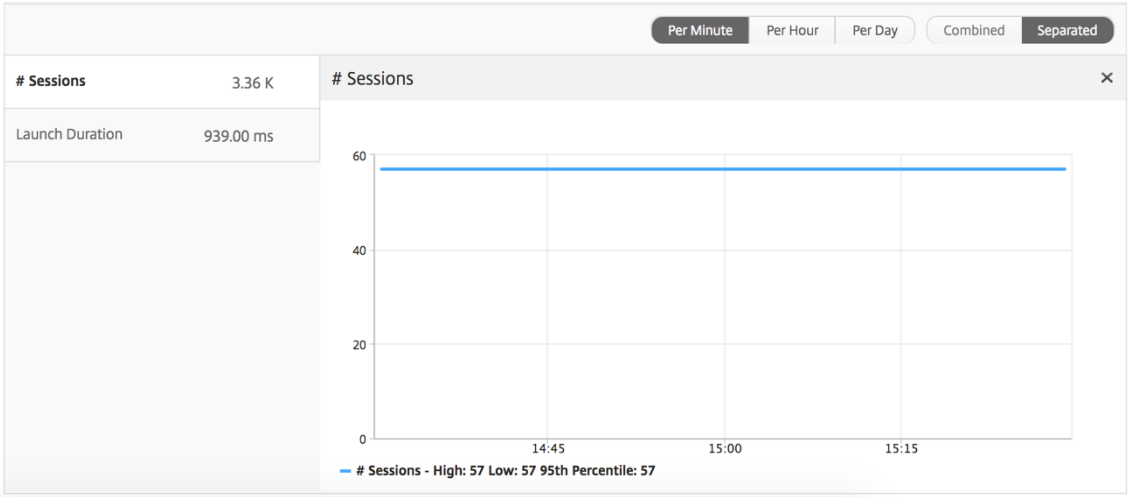
许可证视图提供了有 Citrix Gateway 许可证信息的详细信息。

要导航到 **“许可证”** 视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 Citrix ADM。
2. 导航到 **“分析” > “HDX Insight” > “许可证”**。

折线图

指标	说明
正在使用的许可证	在选定时间轴内使用的 Citrix Gateway CCU 许可证。每个计数均表示用户会话数。这与用户启动的应用程序和桌面会话无关。
Total licenses（许可证总数）	可供客户使用的 Citrix Gateway CCU 许可证总数。



阈值报告

阈值报告表示在选定期间内将实体选为许可证的违反阈值计数。有关详细信息，请参阅如何创建阈值。

“Application”（应用程序）视图报告和指标

April 23, 2021

此视图中的报告和衡量指标侧重于 Citrix Virtual Apps。

要定位至 **“**应用程序**”** 视图，请执行以下操作：

1. 导航到 “ 分析” > “ **HDX Insight** ” > “ 应用程序”。

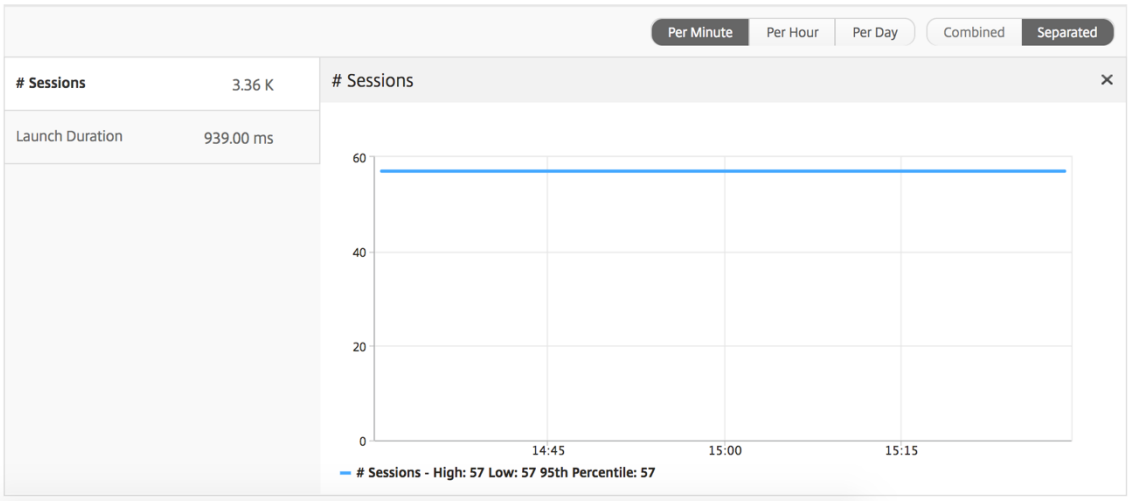
Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有应用程序的报告。

除非明确提及，否则下面所有指标/报告在选定时间段内都有与之对应的值。

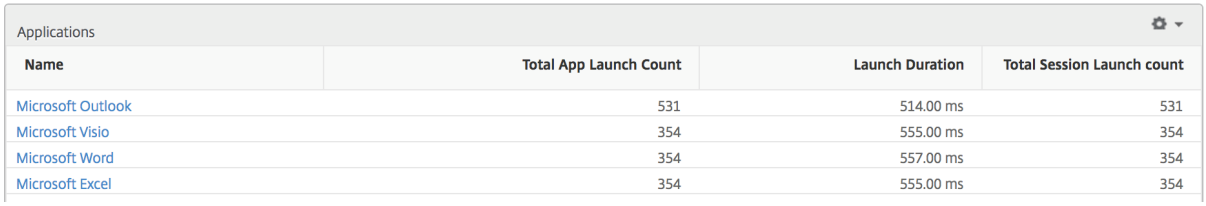
折线图

指标	说明
会话数	在给定时间间隔内的会话总数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。



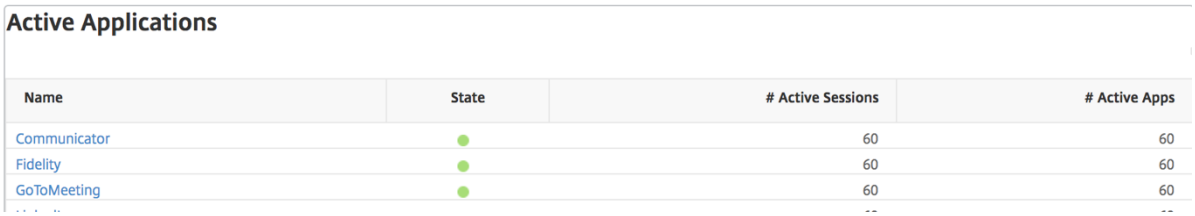
应用程序摘要报告

指标	说明
名称	Citrix 虚拟应用程序的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内的活动 Citrix 虚拟应用程序会话总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix 虚拟应用程序总数。
Launch Duration（启动持续时间）	启动 Citrix 虚拟应用程序所需的平均时间。



活动应用程序报告

指标	说明
名称	Citrix 虚拟应用程序的名称。
状态	显示应用程序的状态：绿色-活动，红色-非活动
# Active Sessions（活动会话数）	在给定时间间隔内使用此应用程序的活动用户会话数。
# Active Apps（活动应用程序数）	此应用程序的活动会话数。

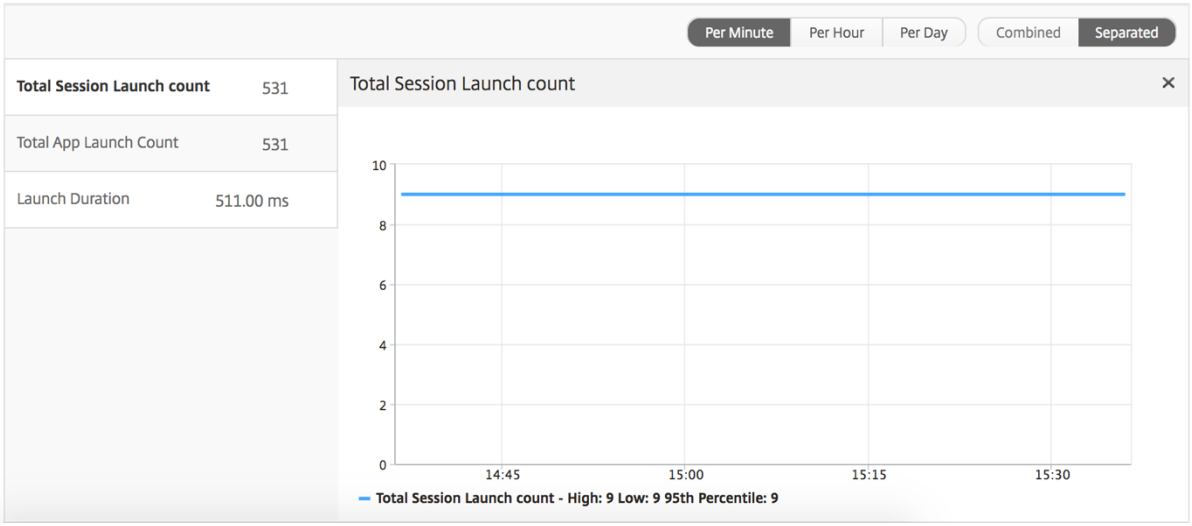


阈值报告

阈值报告表示在选定期间内将 实体选为应用程序的超过阈值计数。 有关更多信息，请参阅 如何创建阈值和警报。

折线图

指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Launch Duration（启动持续时间）	启动应用程序所用平均时间。

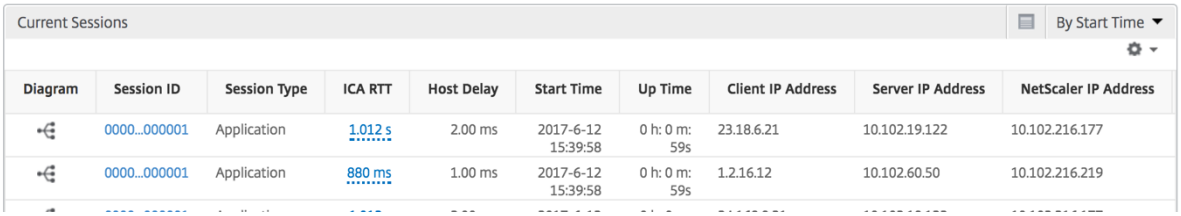


当前会话报告

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。

指标	说明
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
用户名	访问此特定 Citrix 虚拟应用程序的用户的用户名。
会话 ID	Citrix 虚拟应用程序会话的唯一标识符。
会话类型	将为 “Application”（应用程序）。
状态	会话状态：绿色表示活动，红色表示处于活动状态。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。

指标	说明
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。
L7 Server-side Latency（L7 服务器端延迟）	Citrix ADC 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。此衡量指标在传输路径中存在的非 Citrix 设备中非常有用。



每个应用程序会话视图

“Per Application Session View”（每个应用程序会话视图）显示特定的选定应用程序会话的报告。

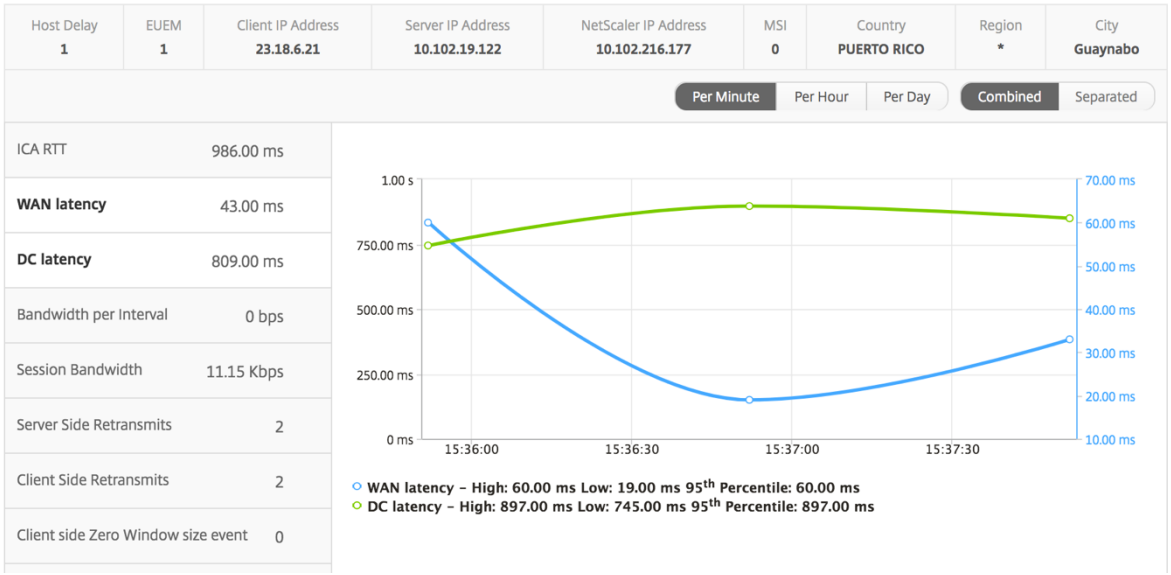
要查看会话报告，请执行以下操作：

1. 导航到“分析”>“**HDX Insight**”>“应用程序”。
2. 从“Application Summary Report”（应用程序摘要报告）中选择特定用户。
3. 从当前会话报告中选择会话。

折线图

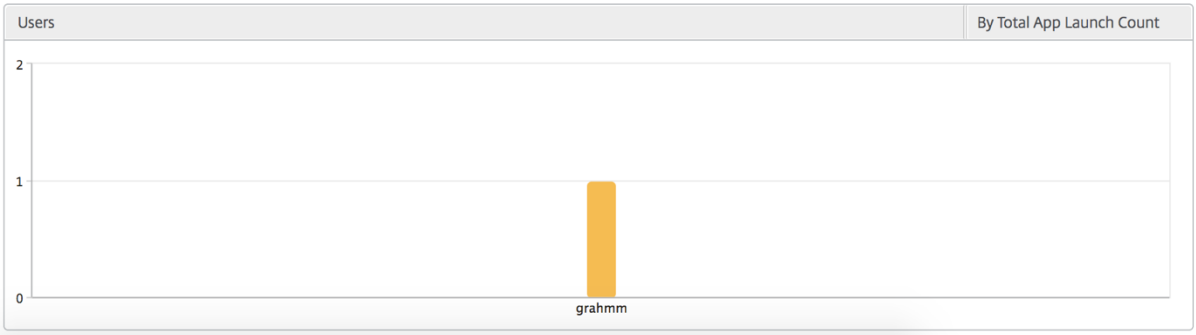
指标	说明
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

指标	说明
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
Server side Zero Window size event（服务器端零窗口大小事件）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。



用户条形图

用户条形图表示登录此特定应用程序的用户。



“Desktop”（桌面）视图报告和指标

April 23, 2021

此视图中的报告和衡量指标侧重于 Citrix Virtual Desktops。

要导航到桌面视图，请执行以下操作：

1. 导航到 分析 > **HDX Insight** > 桌面。

Summary View（摘要视图）

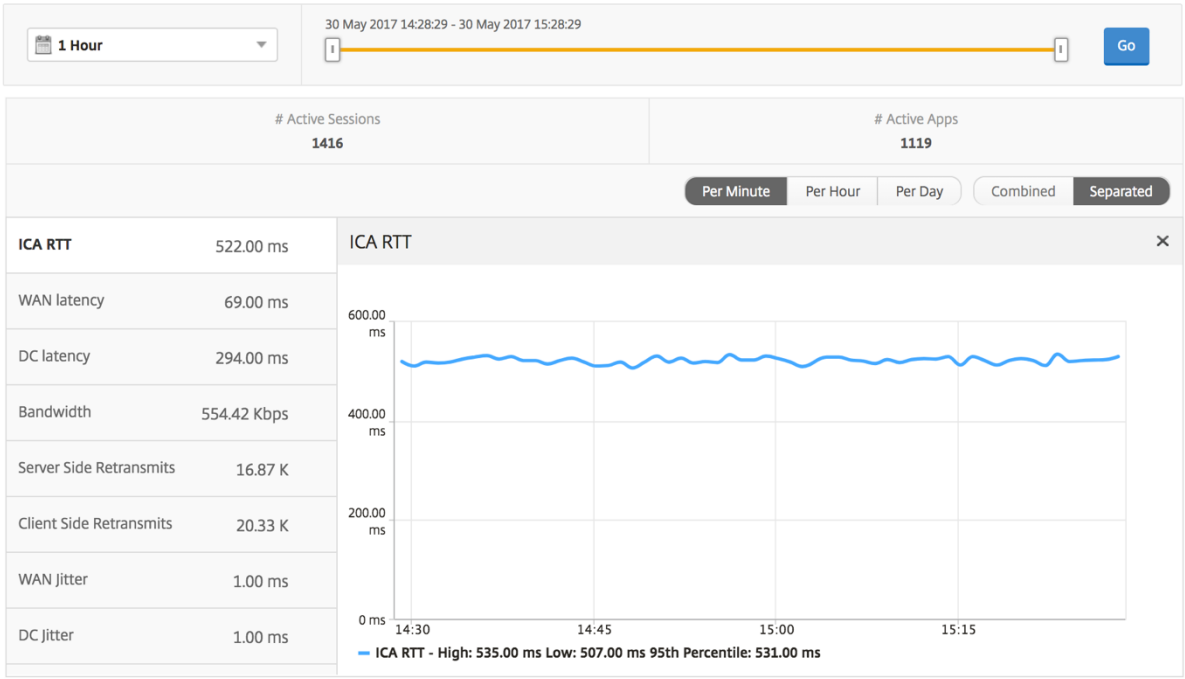
摘要视图显示在选定时间轴内登录的所有 Citrix Virtual Desktops 的报告。

除非明确提及，否则所有指标/报告将具有与所选时间段相对应的值。

折线图

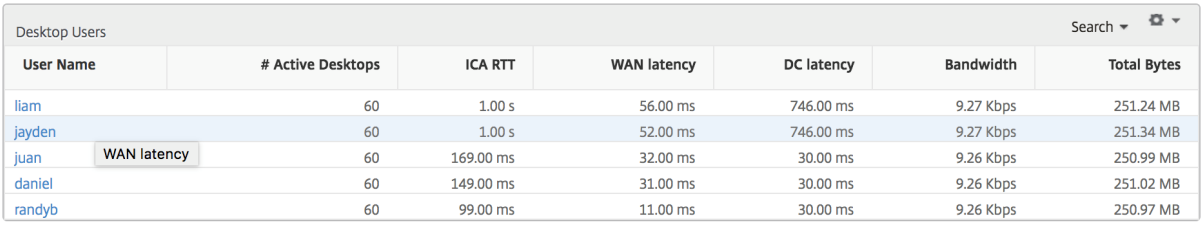
指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。

指标	说明
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



桌面摘要报告

指标	说明
活动会话	在指定时间间隔内的活动 Citrix 虚拟桌面会话总数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。



阈值报告

阈值报告表示在选定期间内将 实体选为桌面时所超过的阈值计数。 有关更多信息，请参阅 如何创建阈值和警报。

每台桌面视图

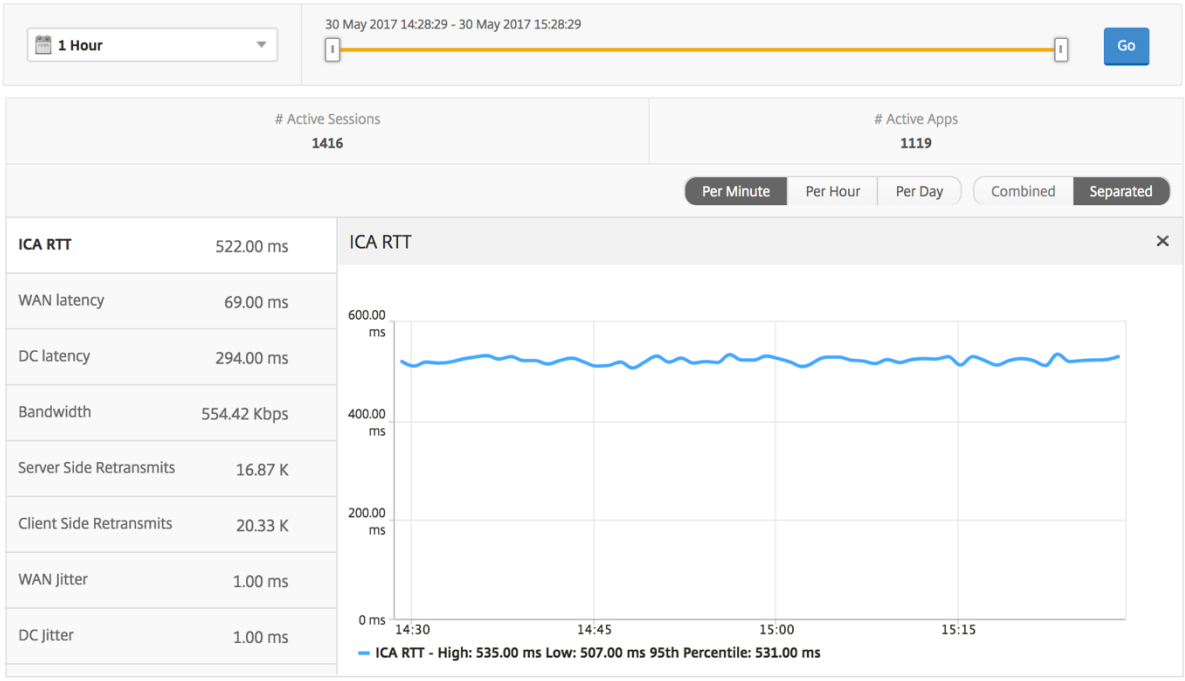
每个桌面视图提供了选定 Citrix 虚拟桌面的详细最终用户体验报告。

要导航到特定的桌面视图，请执行以下操作：

1. 导航到 **“分析” > “HDX Insight” > “桌面”**。
2. 从 桌面摘要报告中选择特定桌面。

折线图

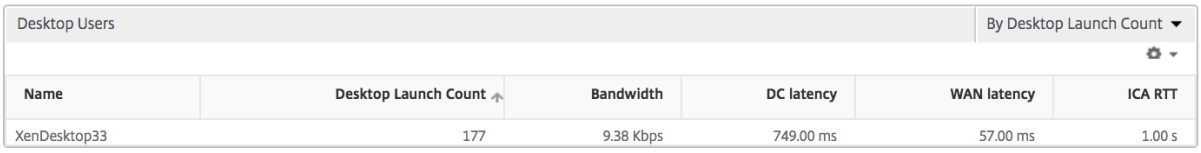
指标	说明
活动会话数	此数字表示活动的 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



“Desktop Users”（桌面用户）报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN Latency（WAN 延迟）	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程序或桌面进行交互时遇到的屏幕滞后。

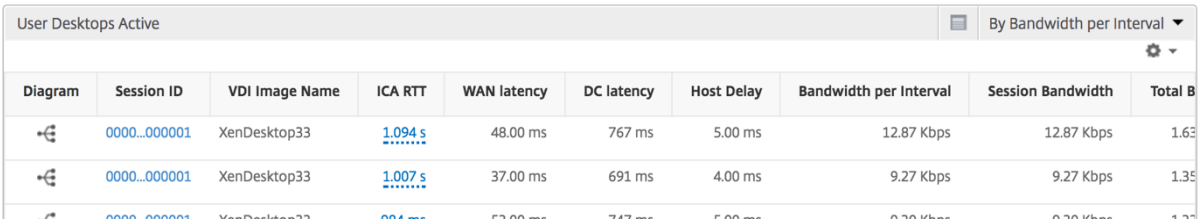


用户桌面活动/非活动报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。

指标	说明
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在分别与 Citrix Virtual Apps 用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称
Diagram（示意图）	



每个桌面会话视图

每个桌面会话视图提供特定选定 Citrix 虚拟桌面会话的报告。

要导航到桌面会话视图，请执行以下操作：

1. 导航到 分析 > **HDX Insight** > 桌面。
2. 从桌面 摘要报告中选择特定桌面。
3. 从当前会话报告中选择会话。

时间线图

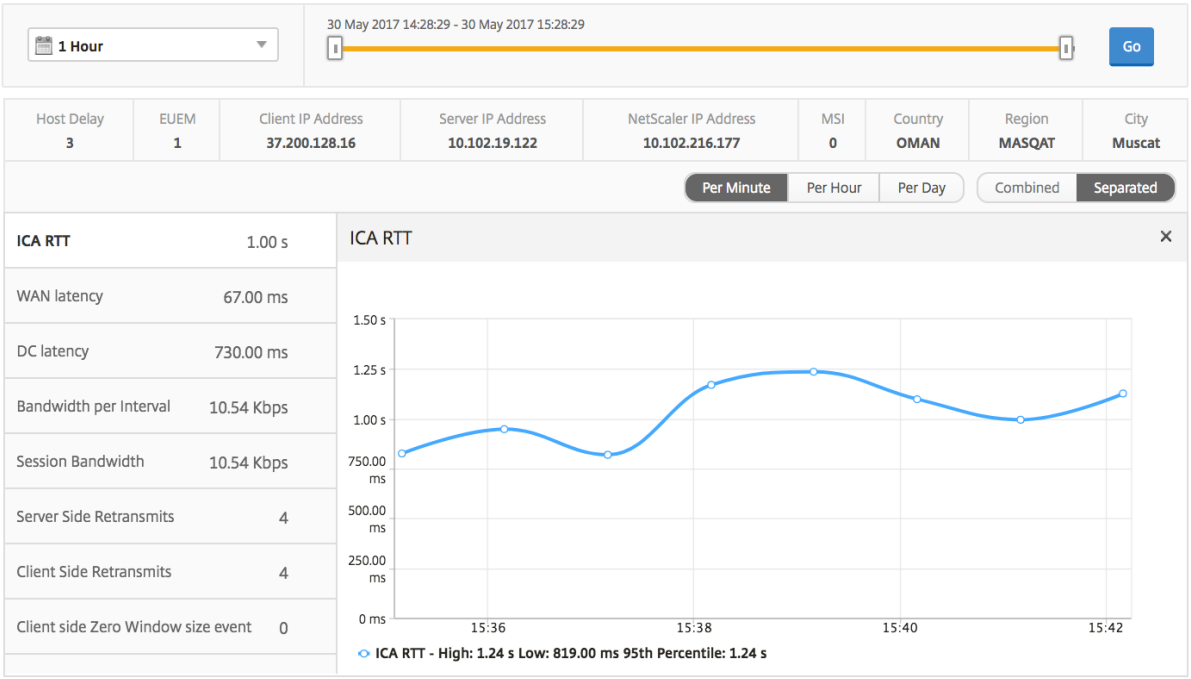
“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

要查看选定用户会话的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或终止的会话列中选择会话。

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix 虚拟应用程序和桌面上的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。

指标	说明
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。

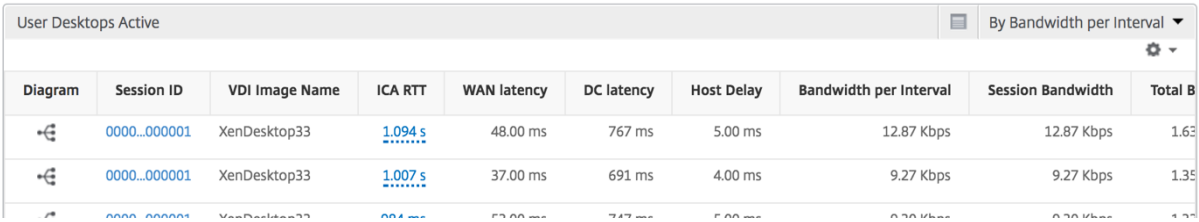


相关桌面会话报告

以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix ADC Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。

指标	说明
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接发生重新传输超时的次数。
VDI Image Name（VDI 映像名称）	用户连接到的 Citrix 虚拟桌面的名称



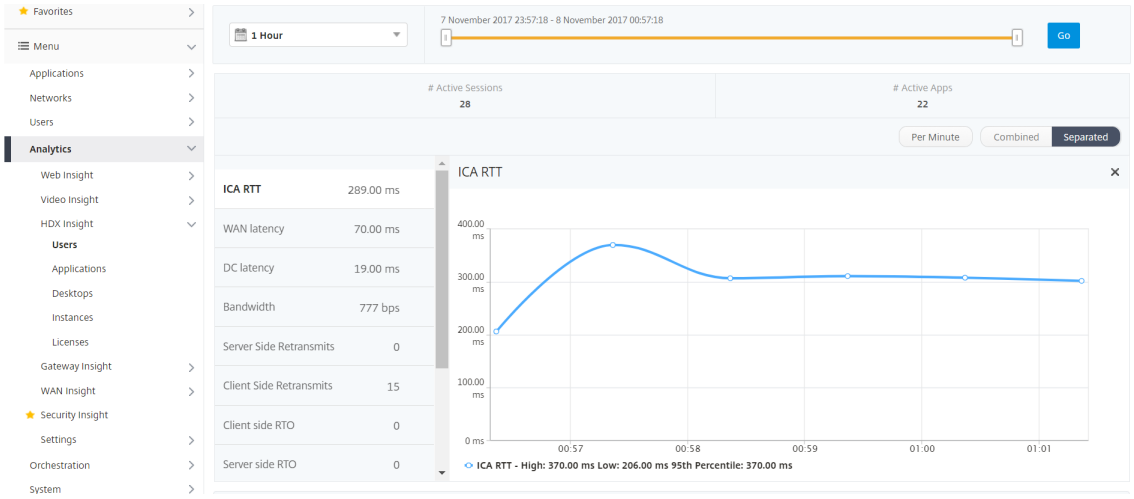
“User”（用户）视图报告和指标

April 23, 2021

此视图中的报告和衡量指标按 Citrix Virtual Apps 和桌面用户显示。

要导航到 **“用户”** 视图，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户



Summary View（摘要视图）

“Summary View”（摘要视图）显示在选定时间线内登录的所有用户的报告。除非另有指定，否则此视图中的所有指标/报告都会显示所选时间段内与其对应的值。

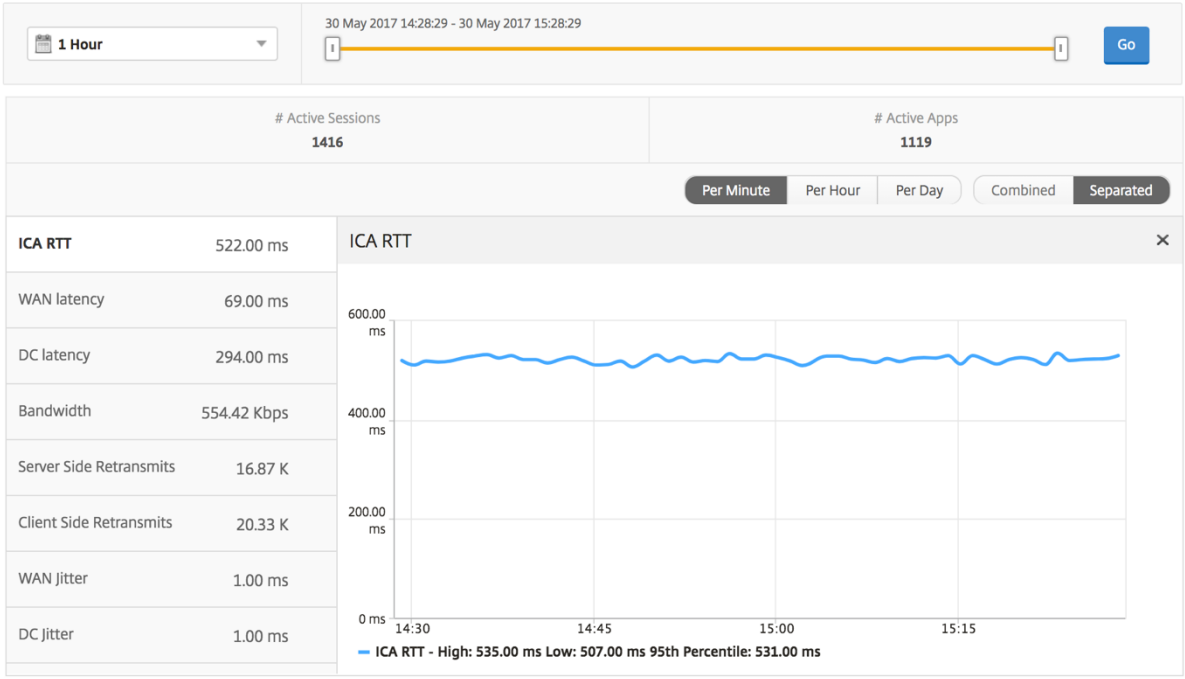
要更改选定时间段，请执行以下操作：

1. 使用时间段列表或时间滑块设置所需的时间间隔。
2. 单击转到。

折线图

指标	说明
活动会话数	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。

指标	说明
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



用户摘要报告

下面是与此报告特定相关的指标。

指标	说明
活动会话数	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Total App Launch Count（应用程序启动总数）	在选定的时间段内用户启动的应用程序总数。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。

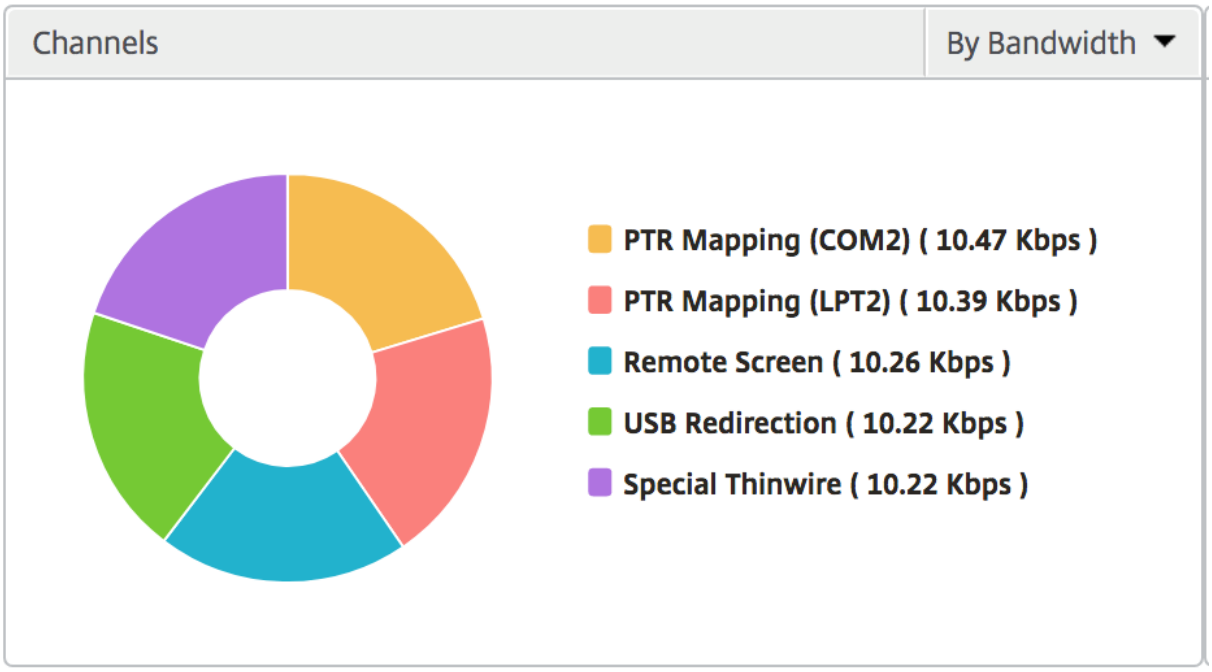
Users

Search

User Name	# Active Apps	# Active Desktops	# Active Sessions	ICA RTT	WAN latency	DC latency	Bandwidth	Server Side Retransmits	Cl
liam	59	59	118	999.00 ms	57.00 ms	751.00 ms	47.25 Kbps	3.74 K	
jayden	59	59	118	999.00 ms	52.00 ms	751.00 ms	47.06 Kbps	3.71 K	
florinl	59	0	59	997.00 ms	52.00 ms	754.00 ms	23.66 Kbps	1.88 K	
ramas	59	0	59	997.00 ms	778.00 ms	1.00 ms	7.03 Kbps	0	
omerp	59	0	59	997.00 ms	57.00 ms	754.00 ms	23.80 Kbps	1.89 K	
grahmm	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.80 Kbps	1.89 K	
ryan	59	0	59	997.00 ms	53.00 ms	754.00 ms	23.69 Kbps	1.88 K	
rajivs	59	0	59	801.00 ms	11.00 ms	1.00 ms	23.97 Kbps	0	
alexisc	117	0	118	622.00 ms	56.00 ms	392.00 ms	47.67 Kbps	1.88 K	
juan	59	59	118	169.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
lennoxl	59	0	59	169.00 ms	31.00 ms	30.00 ms	23.86 Kbps	0	
daniel	59	59	118	149.00 ms	31.00 ms	29.00 ms	47.72 Kbps	0	
woojunek	58	0	59	149.00 ms	31.00 ms	30.00 ms	23.85 Kbps	0	
parkerf	59	0	59	149.00 ms	31.00 ms	30.00 ms	23.88 Kbps	0	
randyb	59	59	118	99.00 ms	11.00 ms	29.00 ms	47.71 Kbps	0	
bradp	177	0	177	74.00 ms	27.00 ms	1.00 ms	71.75 Kbps	0	

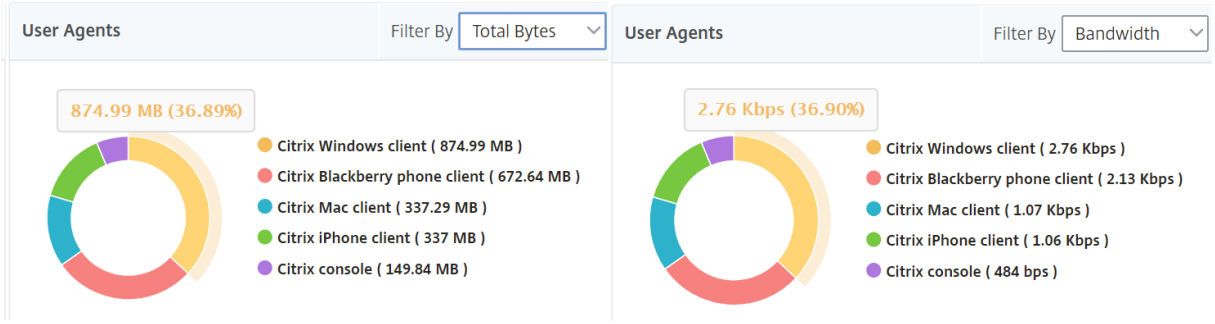
通道

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



用户代理

“User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



阈值违规计数

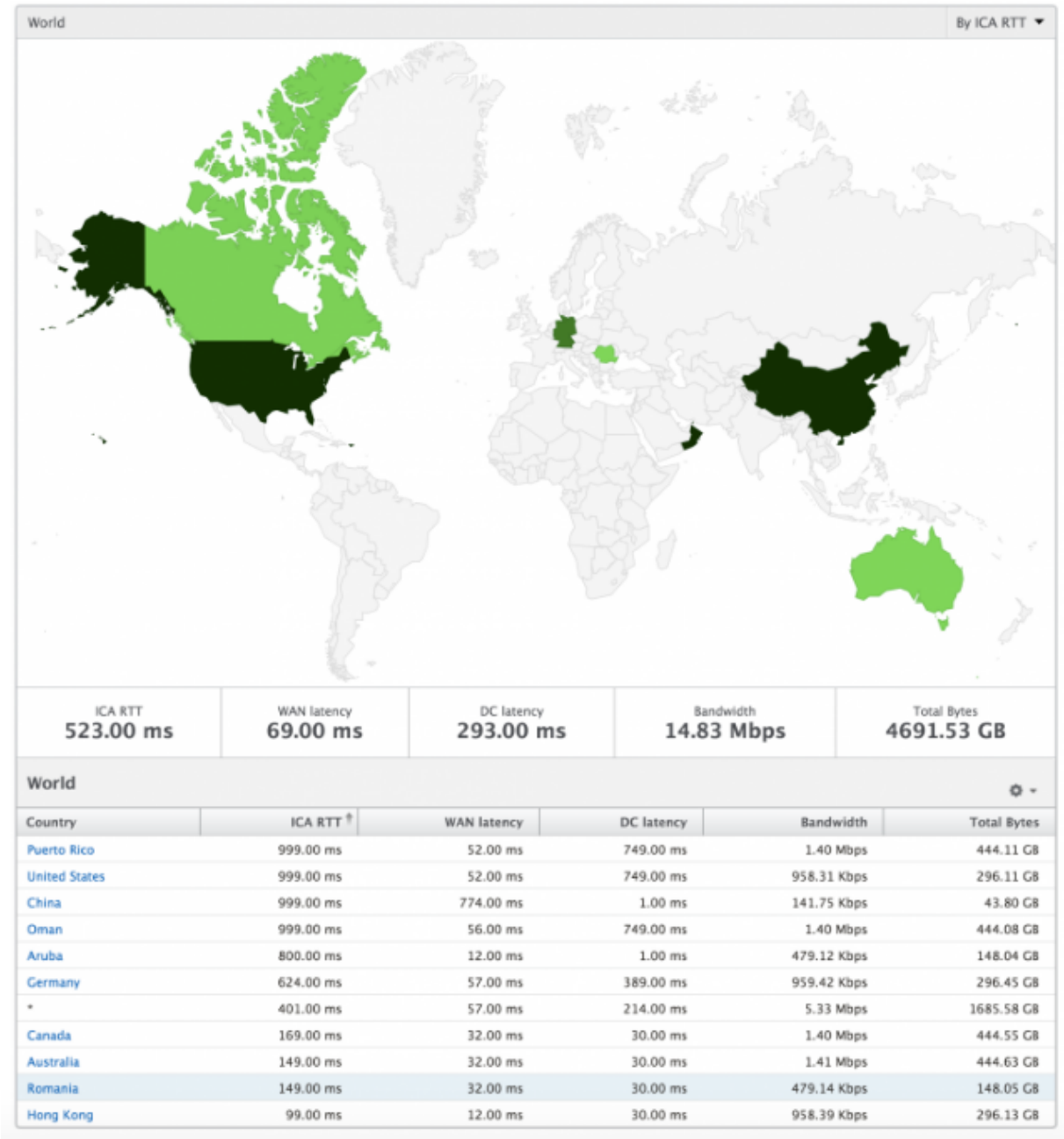
阈值违反计数指标表示在选定时间段内违反的阈值计数。有关详细信息，请参阅如何创建阈值和警报。

世界地图

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市以及通过单击区域。管理员可以按城市和省/自治区/直辖市进一步深入查看信息。从 Citrix ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

每个用户视图

“Per User View”（每个实例视图）提供任何特定的选定用户的详细最终用户体验报告。

要导航到特定用户的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从“User Summary Report”（用户摘要报告）部分中选择特定用户。

折线图

折线图显示在选定时间段内特定的选定用户的所有指标摘要。

当前/终止的会话报告

此报告与选定用户的所有当前/已终止用户会话有关。这些指标可以按开始时间、会话重新连接数和 ACR 计数排序。

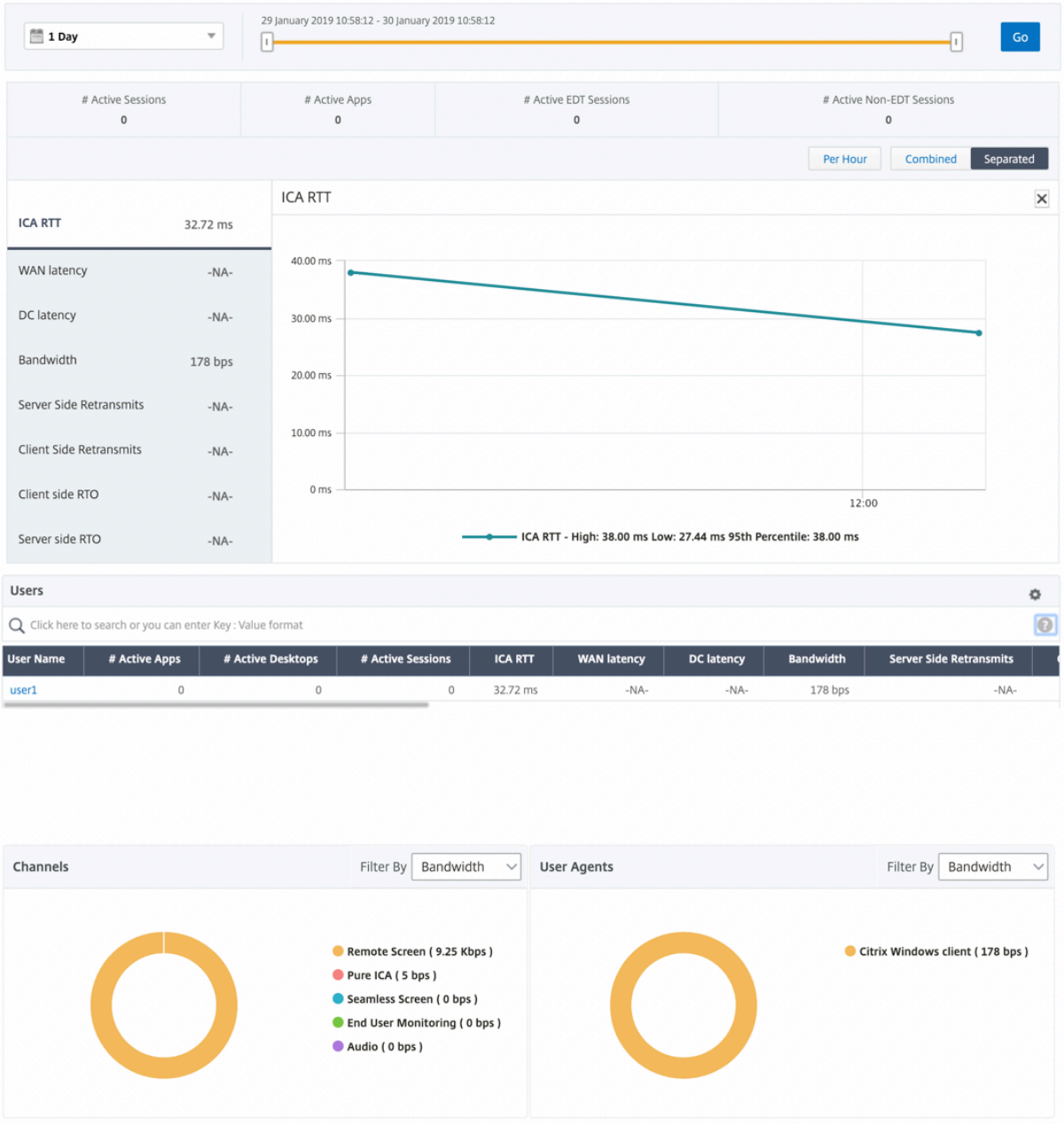
指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	由服务器网络引起的通过 Citrix ADC 的 ICA 流量的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
开始时间	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix 虚拟应用程序服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	接收器类型-Citrix Windows 客户端等
客户端版本	Receiver 版本。
MSI	布尔值（是/否）。指示会话是否是多流 ICA。
Session Reconnects（会话重新连接数）	重新连接会话的次数。
ACR Counts（ACR 计数）	客户端自动为用户重新连接已断开连接的会话的总次数。
User Access Type（用户访问类型）	显示 ICA 会话的访问模式。例如，Citrix Gateway 用户/透明模式。
国家/地区	建立会话时所在的国家/地区。
地理区域	建立会话时所在的区域。
城市	建立会话时所在的城市。
USB Status（USB 状态）	活动/非活动 - 绿色/红色。

指标	说明
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。例如，ICA 会话超时、用户终止了会话。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。

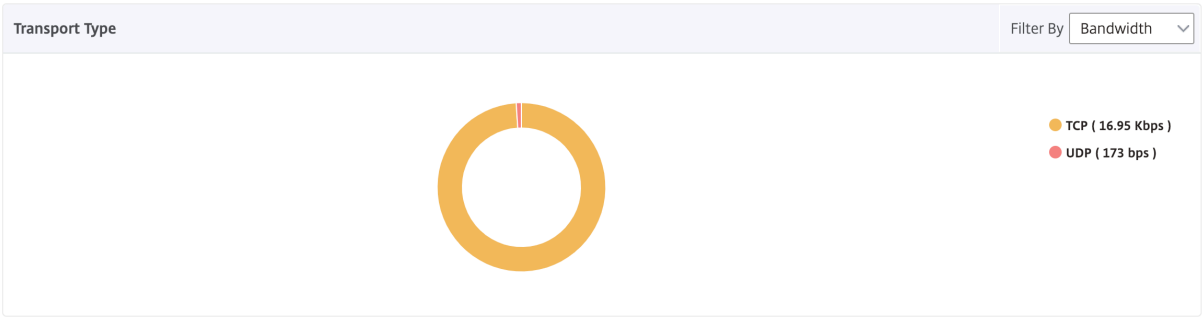
支持 **HDX** 洞察中的 **EDT**

Citrix Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示针对 HDX 智能分析的分析。也就是说，ADM 现在同时支持 UDP 和 TCP 协议。对 Citrix Gateway 的 EDT 支持可确保为运行 Citrix Receiver 的用户提供高清晰度的虚拟桌面会话中用户体验。

HDX Insight 现在将 EDT 会话数和非 EDT 会话数作为活动会话报告的一部分显示。“用户” (Users) 表格显示系统中所有用户的详细报告。该表显示了 WAN 延迟、DC 延迟、重传和 RTO 等指标。这些指标中的某些指标不适用于具有 EDT 会话的用户，因为它们是从 TCP 堆栈计算的。因此，它们显示为 “NA”。

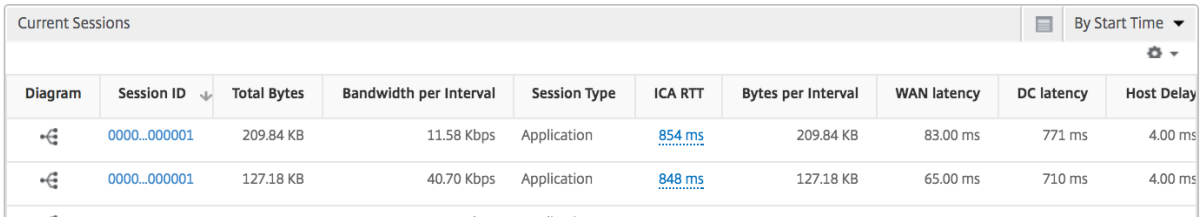


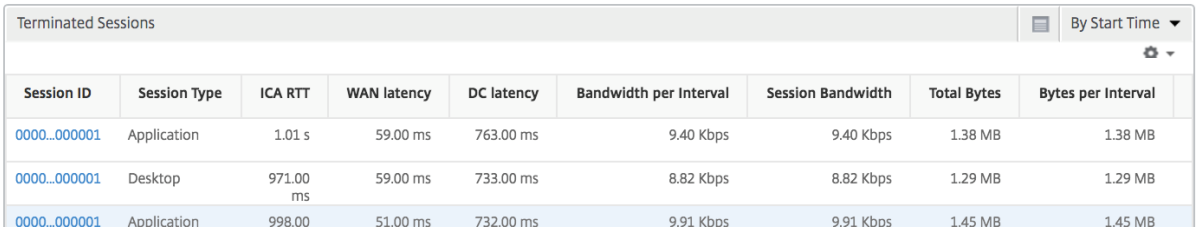
引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。



Citrix ADM 12.0 及更高版本中提供的 **HDX Insight** 分析指标：

L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 Citrix ADC 实例之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
L7 Server-side Latency（L7 服务器端延迟）	Citrix ADC 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	系统处于“L7 latency breached”（已违反 L7 延迟）状态时，L7 延迟的平均值。
L7 Threshold Breach Count（L7 阈值违反计数）	发生 L7 阈值违反的次数。

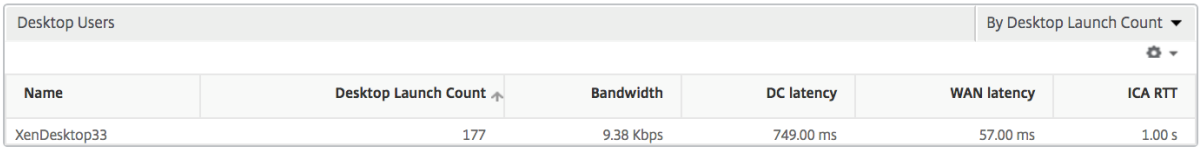




Desktop Users（桌面用户）

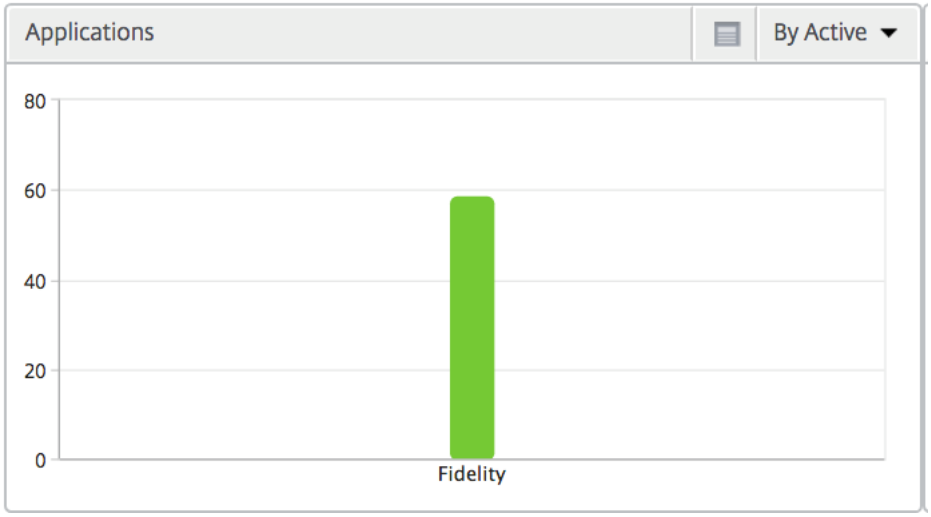
此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。



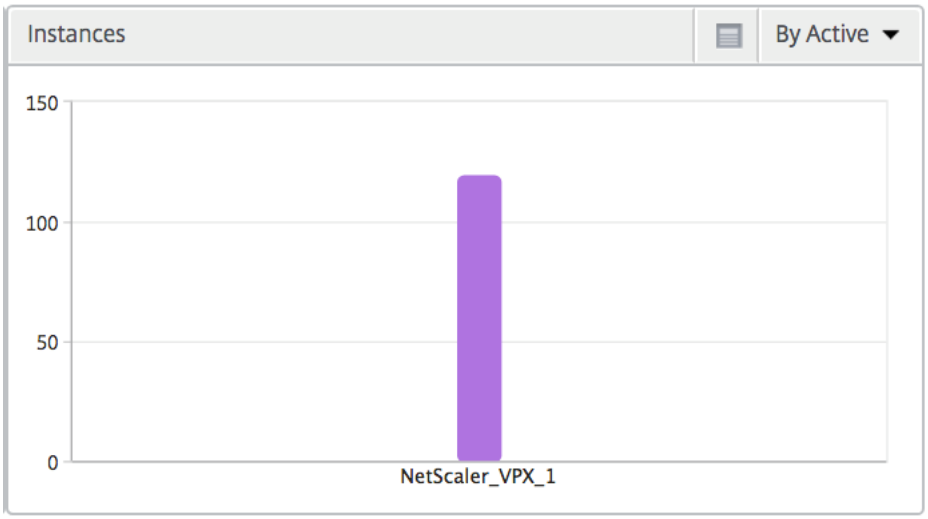
应用程序

一个条形图，表示按活动状态、总会话启动次数、总应用程序启动次数和启动持续时间排序的应用程序。



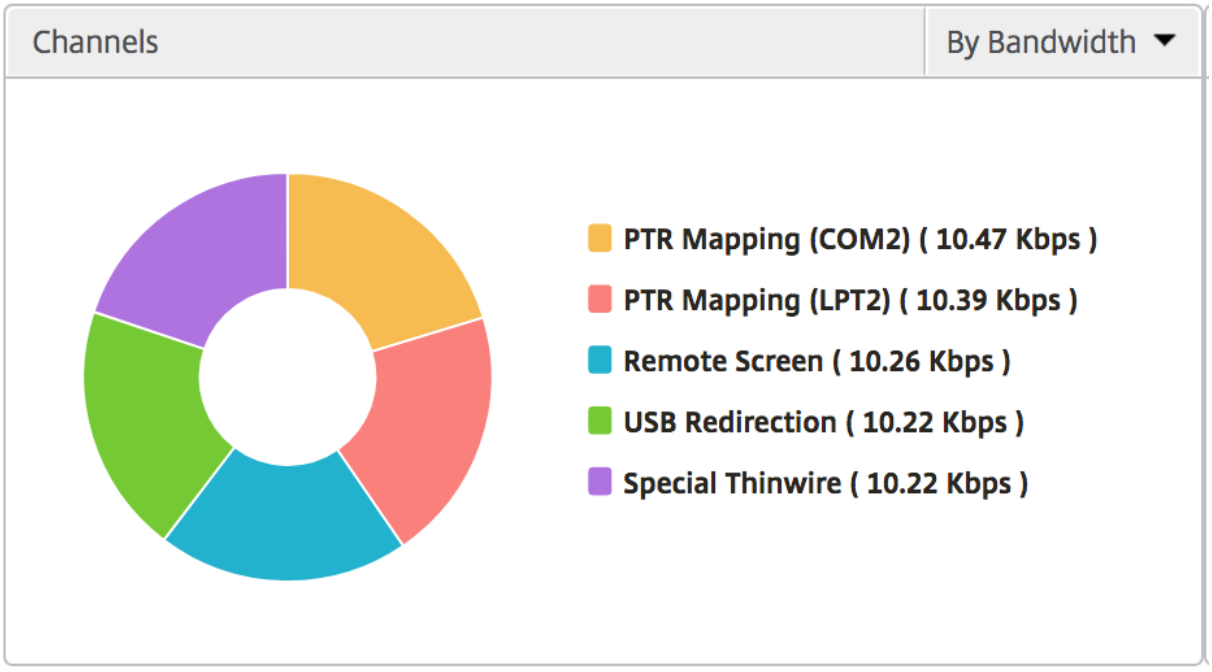
实例

表示按活动应用程序和总应用程序排序的 Citrix ADC 实例的条形图



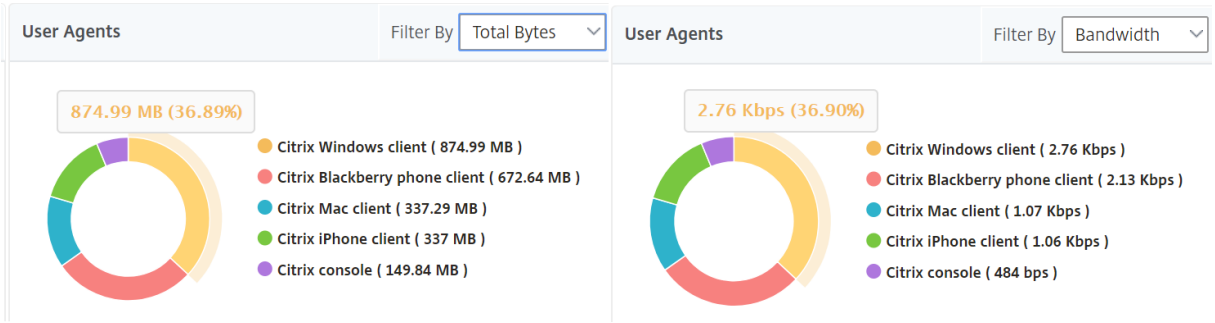
通道

“Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



用户代理

“User Agents”（用户代理）以环形图的形式表示每个端点占用的总带宽/总字节数。您还可以按带宽或总字节数对指标排序。



每用户会话视图

“Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

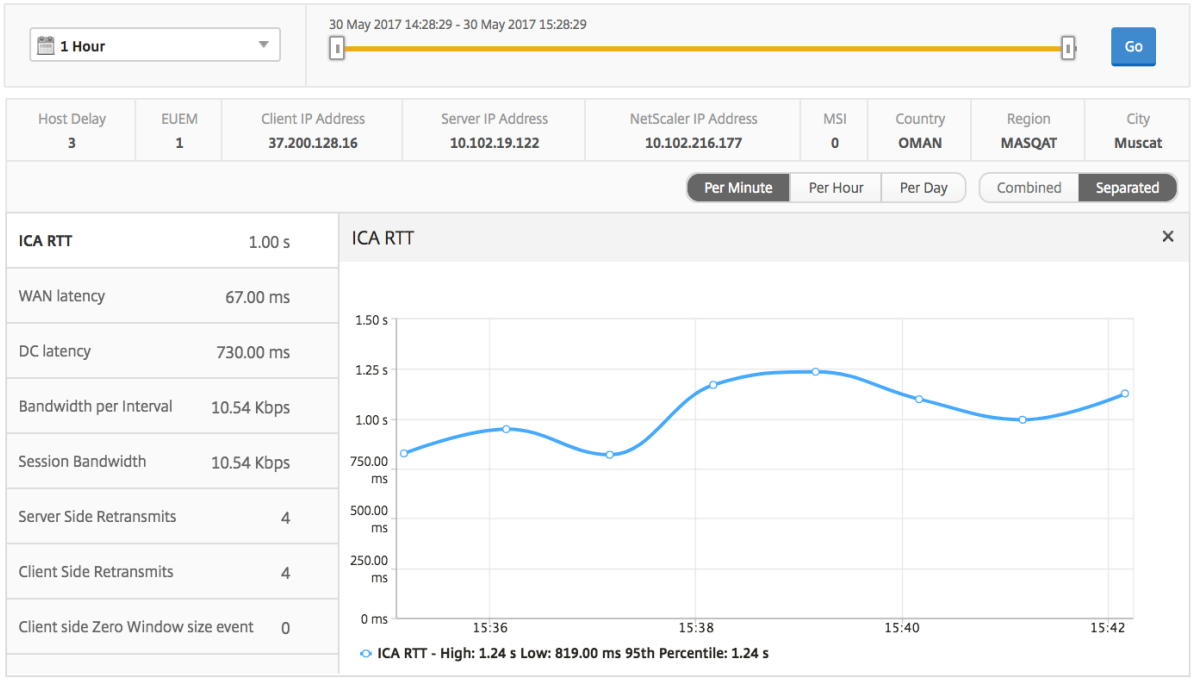
要查看选定用户会话的度量，请执行以下操作：

1. 导航到分析 > **HDX Insight** > 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或终止的会话列中选择会话。

时间线图

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix 虚拟应用程序会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Server Side Retransmits（服务器端重新传输数）	在 Citrix ADC 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	在 Citrix ADC 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。

指标	说明
Client side fast RTO（客户端快速 RTO）	Citrix ADC 与最终用户之间的连接发生重新传输超时的次数。
Server side fast RTO（服务器端快速 RTO）	Citrix ADC 和后端服务器之间的连接上发生重新传输超时的次数。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。

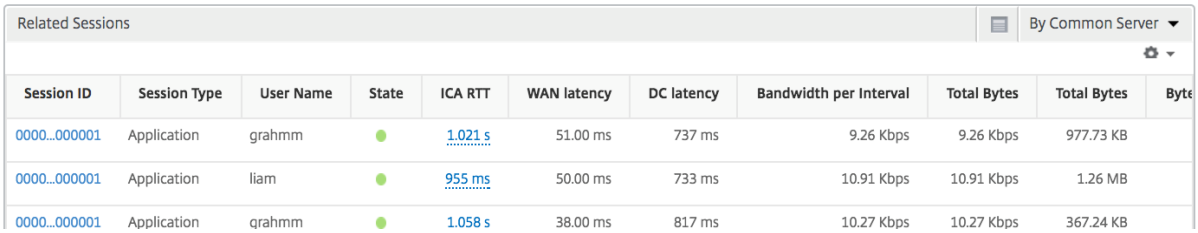


活动应用程序

“ 活动应用程序” 部分显示选定用户的活动应用程序。这些应用程序还可以按活动会话数和启动持续时间排序。

相关会议

“Related Sessions”（相关会话）部分显示选定用户的会话的相关会话。可以选择该关系作为公用服务器或通用 Citrix ADC。



Session ID	Session Type	User Name	State	ICA RTT	WAN latency	DC latency	Bandwidth per Interval	Total Bytes	Total Bytes	Byte
0000...000001	Application	grahmm		1.021 s	51.00 ms	737 ms	9.26 Kbps	9.26 Kbps	977.73 KB	
0000...000001	Application	liam		955 ms	50.00 ms	733 ms	10.91 Kbps	10.91 Kbps	1.26 MB	
0000...000001	Application	grahmm		1.058 s	38.00 ms	817 ms	10.27 Kbps	10.27 Kbps	367.24 KB	

“Instance”（实例）视图报告和指标

April 23, 2021

实例视图中的报告和指标侧重于 Citrix ADC 实例。

要导航到实例视图，请执行以下操作：

1. 导航到 分析 > **HDX Insight** > 实例。

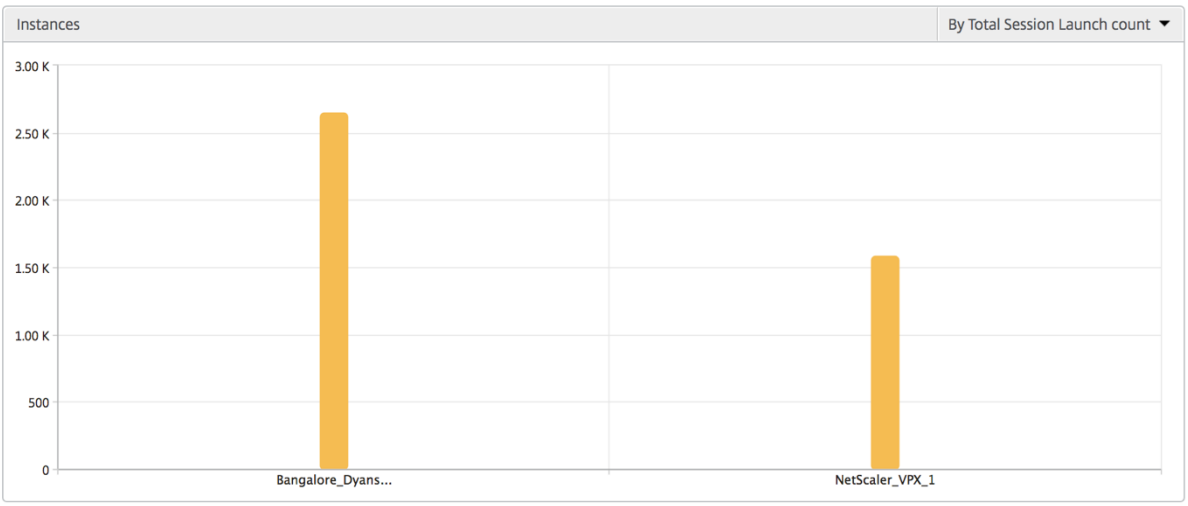
实例摘要视图

此视图称为摘要视图，因为它显示了添加到 Citrix ADM 的所有 Citrix ADC 实例的报告。

除非明确提及，否则所有指标/报告将具有与所选时间段相对应的值。

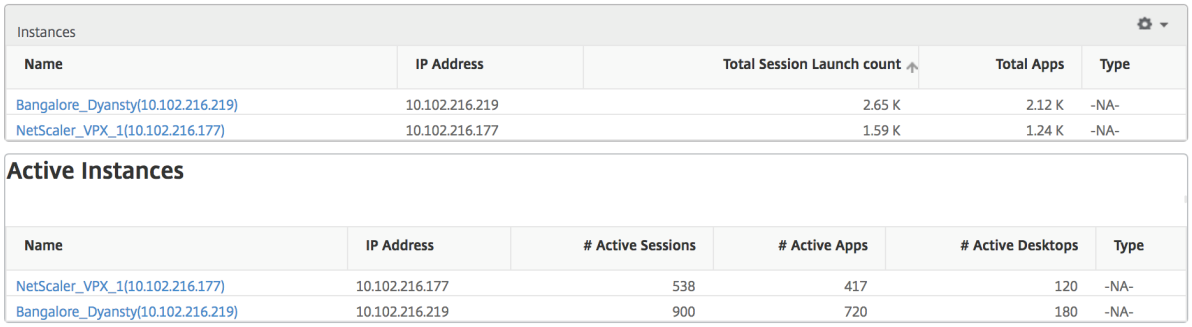
实例条形图

此图形显示实例与会话总启动计数和应用程序总数的比较，这些实例可从图形画布右上角的列表中选择。



实例/活动实例摘要报告

指标	说明
名称	Citrix ADC 实例的主机名。
IP 地址	NetScaler IP 地址。
Total Session Launch Count（会话启动总数）	在给定时间间隔内创建的唯一用户会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。
类型	不适用



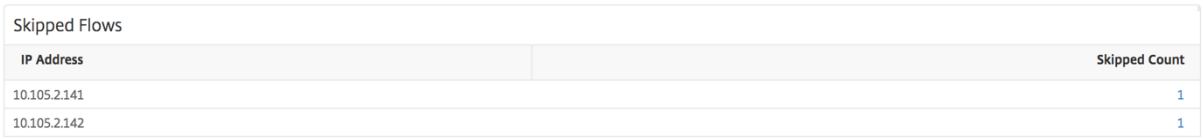
阈值报告

阈值报告表示在选定时间段内将实体选为实例的违反阈值计数。 有关更多信息，请参阅 如何创建阈值和警报。

跳过的流

跳过的流是跳过解析 ICA 连接的记录。出现这种情况的原因可能是多种，例如使用不受支持的 Citrix Virtual Apps and Desktops 版本、不受支持的接收器或接收器类型版本等。此表显示 IP 地址和跳过的流计数。这些接收器可能不是列入白名单的接收器的一部分。因此，这些会话将从监视中跳过。

请参阅 错误！对于 ICA 解析相关问题的详细信息，超链接引用无效。

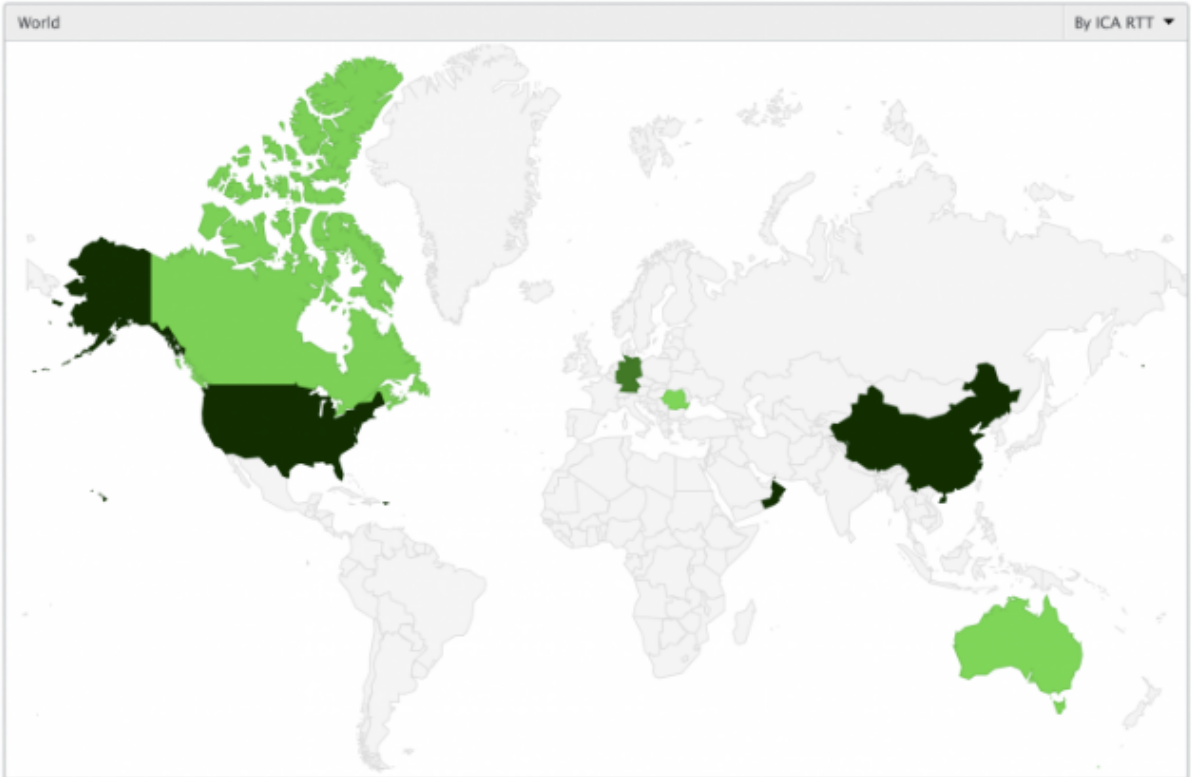


世界观

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市以及通过单击区域。管理员可以进一步向下钻取以按城市和州查看信息。从 Citrix ADC 12.0 及更高版本中，您可以深入查看从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



World

Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

每个实例视图

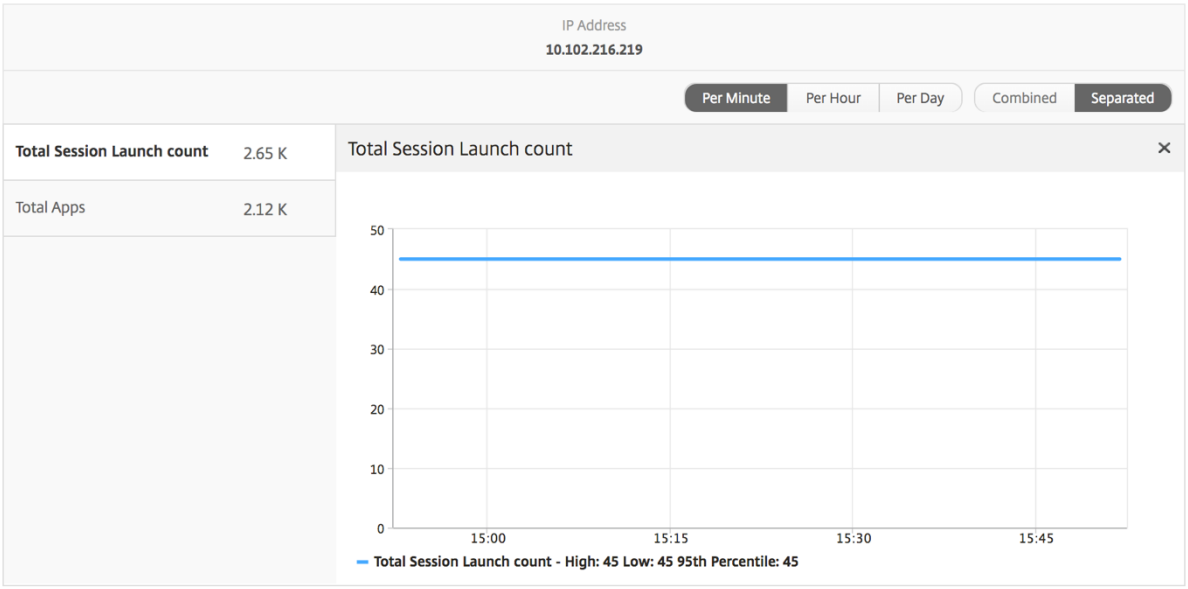
每个实例视图为特定选定的 Citrix ADC 实例提供详细的最终用户体验报告。

要导航到实例视图，请执行以下操作：

1. 导航到 分析 > **HDX Insight** > 实例。
2. 从“实例 摘要报告”中选择特定实例。

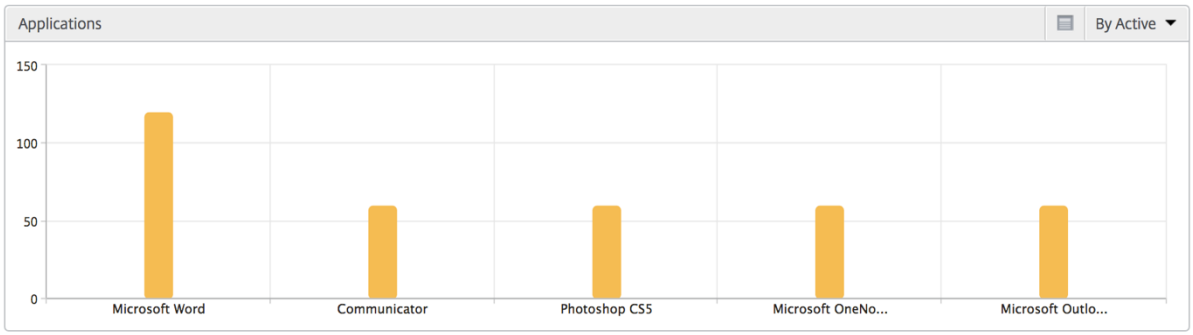
折线图

指标	说明
IP 地址	此项表示选定实例的 NetScaler IP 地址。
Total Session Launch count（会话启动总数）	在给定时间间隔内的活动 Citrix 虚拟应用程序会话总数。
Total Apps（总应用程序数）	在给定时间间隔内启动的唯一应用程序总数。



“Applications”（应用程序）条形图

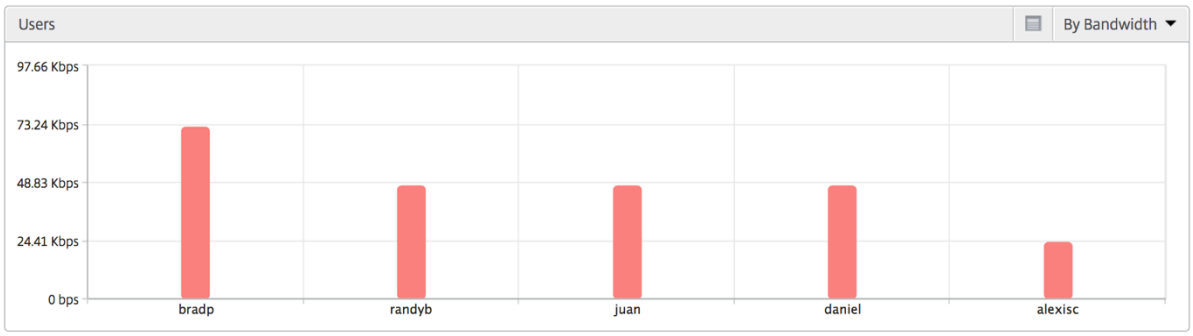
根据以下条件显示前 5 个应用程序-按活动应用程序、总会话启动次数、总应用程序启动次数或启动持续时间。



“Users”（用户）条形图

“Users”（用户）条形图基于以下条件显示排在前 5 位的用户

- Bandwidth（带宽）
- WAN 延迟
- DC 延迟
- ICA RTT

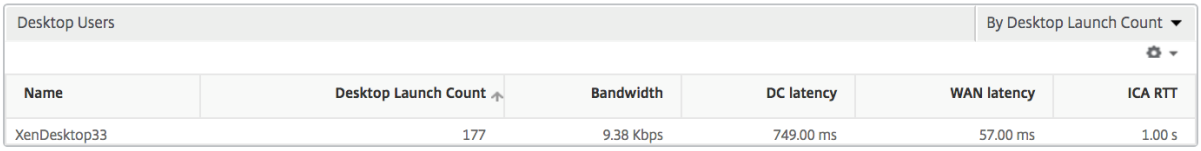


“Desktop Users”（桌面用户）报告

此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix 虚拟桌面的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在选定的时间间隔内端到端通信所用的每秒字节总数。
DC latency（DC 延迟）	网络的服务器端导致的延迟。也就是说，从 Citrix ADC 到后端服务器。
WAN Latency（WAN 延迟）	网络的客户端导致的延迟。也就是说，从 Citrix ADC 到最终用户。

指标	说明
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。

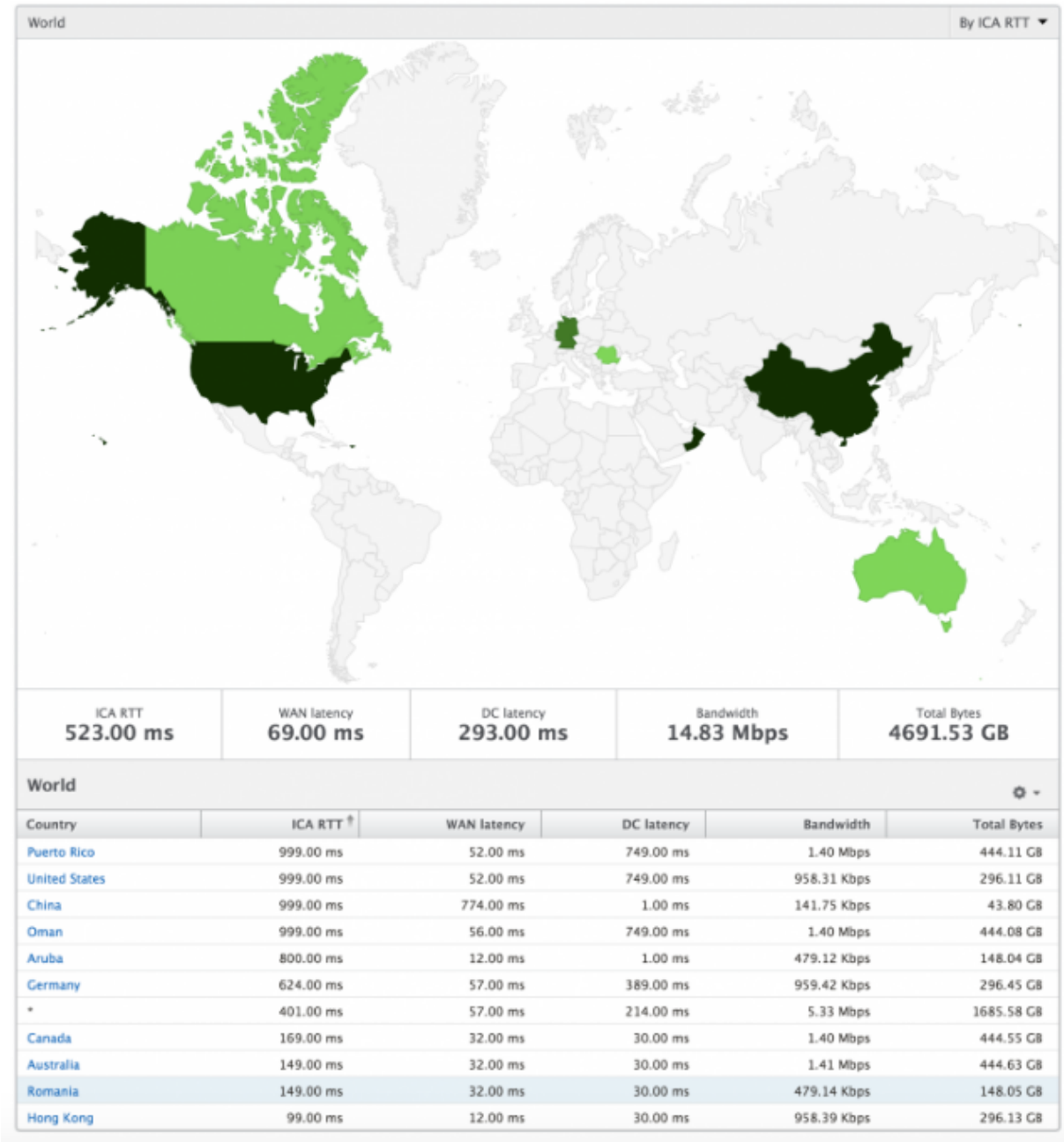


世界观

通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以看到系统的“世界”视图，通过单击该区域向下钻取到特定国家/地区和进一步深入城市。管理员可以进一步向下钻取以按城市和州查看信息。从 Citrix ADM 12.0 及更高版本中，您可以深入查看从地理位置连接的用户。

以下详细信息可以在 HDX 洞察的世界地图上查看，每个度量的密度以热图的形式显示：

- ICA RTT
- WAN 延迟
- DC 延迟
- Bandwidth（带宽）
- Total Bytes（总字节数）



Country	ICA RTT	WAN latency	DC latency	Bandwidth	Total Bytes
Puerto Rico	999.00 ms	52.00 ms	749.00 ms	1.40 Mbps	444.11 GB
United States	999.00 ms	52.00 ms	749.00 ms	958.31 Kbps	296.11 GB
China	999.00 ms	774.00 ms	1.00 ms	141.75 Kbps	43.80 GB
Oman	999.00 ms	56.00 ms	749.00 ms	1.40 Mbps	444.08 GB
Aruba	800.00 ms	12.00 ms	1.00 ms	479.12 Kbps	148.04 GB
Germany	624.00 ms	57.00 ms	389.00 ms	959.42 Kbps	296.45 GB
*	401.00 ms	57.00 ms	214.00 ms	5.33 Mbps	1685.58 GB
Canada	169.00 ms	32.00 ms	30.00 ms	1.40 Mbps	444.55 GB
Australia	149.00 ms	32.00 ms	30.00 ms	1.41 Mbps	444.63 GB
Romania	149.00 ms	32.00 ms	30.00 ms	479.14 Kbps	148.05 GB
Hong Kong	99.00 ms	12.00 ms	30.00 ms	958.39 Kbps	296.13 GB

“License”（许可证）视图报告和指标

April 23, 2021

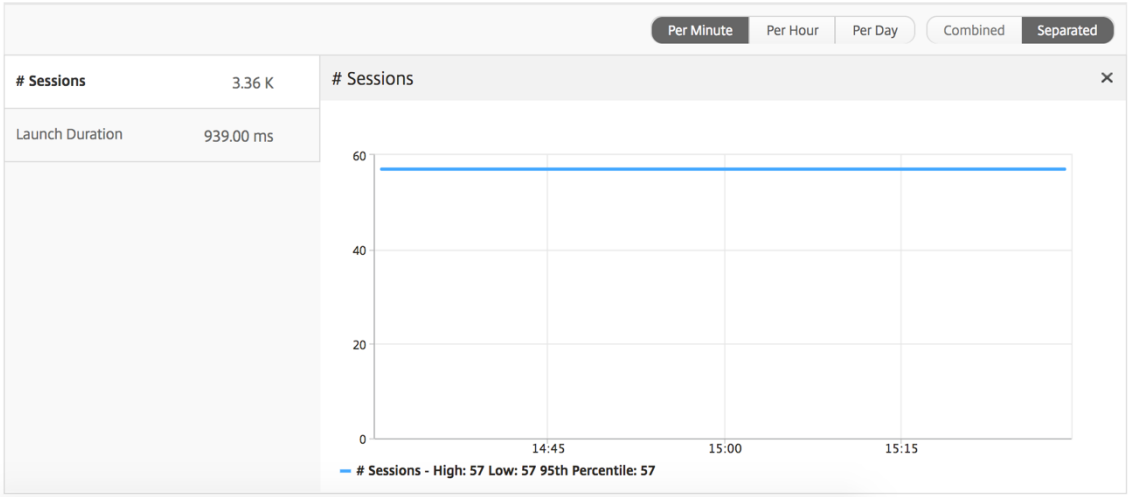
许可证视图提供了有 Citrix Gateway 许可证信息的详细信息。

要导航到许可证视图，请执行以下操作：

1. 导航到 分析 > **HDX Insight** > 许可证。

折线图

指标	说明
正在使用的许可证	在选定时间轴内使用的 Citrix Gateway CCU 许可证。每个计数均表示用户会话数。这与用户启动的应用程序和桌面会话无关。
Total licenses（许可证总数）	可供客户使用的 Citrix Gateway CCU 许可证总数。



阈值报告

阈值报告表示在选定期间内将实体选为许可证的违反阈值计数。 有关更多信息，请参阅 如何创建阈值和警报。

对 **HDX Insight** 问题进行故障排除

April 23, 2021

如果 HDX Insight 解决方案无法按预期运行，则问题可能与以下情况之一有关。请参阅相应部分中的清单以进行故障排除。

- HDX Insight 配置。
- Citrix ADC 和 Citrix ADM 之间的连接。
- 在 Citrix ADC 中为 HDX/ICA 流量生成记录。
- Citrix ADM 中记录的人口。

HDX Insight 配置清单

- 确保在 Citrix ADC 中启用了 AppFlow 功能。有关详细信息，请参阅启用 AppFlow。
- 检查 Citrix ADC 运行配置中的 HDX Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查 HDX Insight 配置。确保绑定类型为 ICA 请求。例如;

  ```
  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  ```

  对于透明模式，绑定类型必须为 ICA_REQ_DEFAULT。例如;

  ```
  bind appflow global afp 100 END -type ICA_REQ_DEFAULT
  ```

- 对于单跳/访问网关或双跳部署，请确保 HDX Insight AppFlow 策略绑定到 VPN 虚拟服务器，其中 HDX/ICA 流量正在流动。
- 对于透明模式或局域网用户模式，请确保设置 ICA 端口 1494 和 2598。
- 已为 Access Gateway 或双跳部署启用 Citrix Gateway 或 VPN 虚拟服务器中的检查 `appflowlog` 参数。有关详细信息，请参阅为虚拟服务器启用 AppFlow。
- 选中双跳 Citrix ADC 中已启用“连接链接”。有关详细信息，请参阅配置 Citrix Gateway 设备以导出数据。
- HA 故障转移后，如果 HDX Insight 详细信息被跳过解析，请检查 ICA 参数“启用重建故障转移”是否已启用。有关详细信息，请参阅Citrix ADC 高可用性对的会话可靠性。

Citrix ADC 与 Citrix ADM 之间的连接检查表

- 检查 Citrix ADC 中的应用流收集器状态。有关详细信息，请参阅如何检查 Citrix ADC 和 AppFlow 收集器之间的连接状态。
- 检查 HDX Insight AppFlow 策略命中。

  运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中情况。

  您还可以导航到 GUI 中的 **“系统” > “AppFlow” > “**策略”，以检查 AppFlow 策略命中。

- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

在 Citrix ADC 核对表中为 HDX/ICA 流量生成记录

运行命令 `tail -f /var/log/ns.log | grep -i "default ICA Message"` 进行日志验证。根据生成的日志，您可以使用此信息进行故障排除。

- 日志：已跳过解析 **ICA** 连接-此主机不支持 **HDX Insight** 能分析

  原因：Citrix Virtual Apps and Desktops 版本不受支持

  解决办法：将 Citrix Virtual Apps and Desktops 服务器升级到受支持的版本。

- 日志：**Client type received 0x53, NOT SUPPORTED**

  原因：Citrix Workspace 版本不受支持

  解决方案：将 Citrix Workspace 升级到支持的版本。有关详细信息，请参阅Citrix Workspace 应用程序。

- 日志：来自扩展数据包的错误-跳过此流的所有 **hdx** 处理

  原因：解压缩 ICA 通信时出现问题

  解决方案：在建立新会话之前，此 ICA 会话没有可用的报告。

- 日志：无效的转换：**NS_ICCA_ST_** 流程**/INIT/NS_ICCA_EVT_** 无效**-> NS_ICCA_ST_UNINIT”**

  原因：解析 ICA 握手时出现问题

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：缺少欧盟 **ICA RTT**

  原因：无法解析最终用户体验监控通道数据

  解决方案：确保在 Citrix Virtual Apps and Desktops 服务器上启动了最终用户体验监视服务。确保您使用的是 Citrix Workspace 应用程序受支持的版本。

- 日志：无效的通道报头

  原因：无法识别通道报头

  解决方案：在建立新会话之前，此特定 ICA 会话没有可用的报告。

- 日志：跳过代码

  如果您看到以下跳过代码的任何值，则会跳过分析智能分析详细信息。

  > 跳过代码 0 表示记录已成功从 Citrix ADC 导出。

跳过代码	错误消息	错误原因
100	非正常错误为空的错误	处理 ICA 片段时出错，可能是由于内存条件
101	非法错误，无效，有效，有效	收到的握手命令无效
102	非法错误减少参数数据	为 V3 扩展器初始化指定的参数无效
103	现有的错误，还原的开头	无法正确初始化 V3 扩展器
104	非法错误还原参数字节	字节不足，无法将编码器分配给通道
105	无效通道	ICA 通道号码无效
106	无效解码器	为通道指定的解码器无效

跳过代码	错误消息	错误原因
107	无效的两个参数	在 Thinwire 通道上指定的参数计数无效
108	错误解码器，无效，两者解码器	薄线通道的解码器无效
109	非正确的错误解码器	没有为通道定义解码器
110	NS_ICA_ERR_REDUC_V3_EXPAN	无法扩展通道数据
111	NS_ICA_ERR_REDUC_BYTES_V3_扩展器	扩展器错误：占用的字节超过可用字节数
112	非法错误，还原字节字节字节	错误：未压缩的数据溢出
113	非法错误减少无效的 CMD	未定义的扩展器命令
114	孔中的空间	处理拆分 CGP 帧时出错
115	公司名单上的名称	NSB 分配错误 — 由于内存不足的情况
116	记忆还原有的数据	扩展器上下文的内存分配错误
117	网络服务器上的服务器	旧服务器，不支持功能块
118	非法错误，多种错误	数据包的 Init 请求被碎片化，无法处理
119	不同类型的名称	ICA 功能初始化错误
120	支持服务	主机不支持 MSI 功能。表示 XenApp 版本低于 6.5 或 XenDesktop 版本低于 5.0
121	无效的计算机	遇到无效的 CGP 命令
122	缺少信道字节的信道字节	通道上的字节不足
123	通道数据	EUEM、控制或无缝通道上的数据不正确
124	非法错误无效、纯净、CMD	处理纯 ICA 通道数据时收到的命令无效
125	NS_ICA_ERR_INVALID_PURE_LEN	处理纯 ICA 通道数据时遇到的长度无效
126	无效、纯净、无效、无效	处理 PURE ICA 通道数据时遇到的长度无效
127	数据无效的数据	从客户端收到的数据长度无效
128	不同的情况下，有些信息	MSI GUID 大小出现错误

跳过代码	错误消息	错误原因
129	无效通道报头	检测到无效的通道报头
130	重新连接 ID	检索重新连接的会话失败
131	重新连接时，禁用重新连接	禁用 SR 时出错
132	NS_ICA_ERR_REDUC_NOT_V3	不支持的 ICA 减速器版本
133	禁用了空间压缩	压缩已禁用，主机不支持
134	不同文件的名称	无法识别 ICA 或 CGP 协议，在不正确的接收器中看到
135	无效签名	ICA 签名或魔术字符串不正确
136	原始工具	解析 ICA 握手数据包时出错
137	不完整的问题	握手时收到的数据包不完整
138	非常重要的错误，也可以使用大号	ICA 帧太大，超过 1460 字节
139	正确的错误转发	转发 ICA 数据时出错
140	最大孔	无法处理 CGP 命令，因为它被拆分超出支持的限制
141	组装框架	无法正确重新组装 ICA 帧
142	NS_ICA_ERR_UNSUPPORTED_F	已跳过此接收器（客户端）的 ICA 解析，因为它不在允许列表中
143	查找重新连接 ID	无法检测客户端重新连接 cookie 的解析状态
144	重新连接 ID	客户端重新连接后检测到无效的重新连接 cookie 长度
145	NS_ICA_ERR_INVALID_RECONNECT_ID	客户端重新连接 cookie 错过了所需的约束
146	客户端版本无效	从客户端接收的接收器版本字符串无效
147	不知道客户端产品编码	从客户端收到的商品编码无效
148	NS_ICA_ERR_V3_HDR_CORRUP	通道长度扩展后无效
149	特殊薄线	解压缩错误
150	无缝密封的字节	遇到无缝命令的字节不足
151	以后字节为单位	遇到 EUEM 命令的字节不足
152	无缝无效事件	无缝通道解析的无效事件

跳过代码	错误消息	错误原因
153	无效事件	CTRL 通道解析的事件无效
154	无效事件	EUEM 通道解析的事件无效
155	无效事件	USB 通道解析的事件无效
156	无效事件	纯通道解析的无效事件
157	无效事件	虚拟通道解析的事件无效
158	错误事件无效	ICA 数据解析的事件无效
159	无效事件	CGP 数据解析的事件无效
160	基本加密无效状态	基本加密中的 crypt 命令的状态无效
161	加密密码无效	基本加密中的 crypt 命令无效
162	无效状态	RC5 加密中的地密命令的状态无效
163	加密密码无效	RC5 加密中的密码命令无效
164	有关的信息，有关信息	RC5 加密/解密中的错误
165	数据加密工具	RC5 加密/解密中的错误
166	NS_ICA_ERR_SERVER_NOT_RE	VDA 不支持减速器版本 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	客户端不支持减速器版本 3
168	以后字节为单位	ICA 握手中意外的字节数
169	NS_ICA_ERR_HIGHER_RECONSEQ	对等帖子重新连接的 CGP 恢复序列号较高
170	不存在的问题	重新连接后无法恢复 ICA 解析状态
171	解析的问题	分析智能分析通道数据时出错
172	应用程序	从 Insight 渠道数据解析应用详细信息时出错
173	有关的信息	从智能分析通道数据中分析 ACR 详细信息时出错
174	会话结束	从 Insight 通道数据解析会话结束详细信息时出错
175	不适用于不适用于不适用于不适用的情况	由于缺少 Insight 通道支持，在服务节点上跳过 ICA 解析
176	客户端上的客户端	客户端不支持 NSAP
177	服务器上的服务器	VDA 不支持 NSAP

跳过代码	错误消息	错误原因
178	失败的问题	NSAP 数据协商时出错
179	NS_ICA_ERR_SN_RECONNECT_TKT_FAIL	获取服务节点中的票证时出错重新连接服务节点
180	高级别咨询委员会	在服务节点中收到较高的重新连接序列号时出错
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NSAP_VC	禁用 HDX Insight 时出错

示例日志：

```
Jan 9 22:57:02 <local0.notice> 10.106.40.223 01/09/2020:22:57:02 GMT ns-223
 0-PPE-2 : default ICA Message 1234 0 : "Session setup data send: Session
GUID [57af35043e624abab409f5e6af7fd22c], Client IP/Port [10.105.232.40/52314],
 Server IP/Port [10.106.40.215/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:56:49 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [WIN2K12
-215], Ctx Flags [0x8820220228], Track Flags [0x1775010c3fc], Skip Code [0]
"

Jan 9 22:55:41 <local0.notice> 10.106.40.223 01/09/2020:22:55:41 GMT ns-223
 0-PPE-0 : default ICA Message 156 0 : "Skipping ICA flow: Session GUID
[4e3a91175ebcbe686baf175eec7e0200], Client IP/Port [10.105.232.40/60059],
Server IP/Port [10.106.40.219/2598], MSI Client Cookie [Non-MSI], Session
 setup time [01/09/2020:22:55:39 GMT], Client Type [0x0052], Receiver
Version [19.12.0.23], User [user1], Client [10.105.232.40], Server [10.106.40.219],
 Ctx Flags [0x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

错误计数器

捕获各种计数器 ICA 解析。下表列出了用于 ICA 解析的各种计数器。

运行命令 `nsconmsg -g hdx -d statswt0` 查看计数器详细信息。

HDX 计数器名称	用途	类别（统计数据/错误/诊断）
高清/高清/高清	指示 NS 检测到的纯 ICA 连接总数。每当检测到基于客户端 PCB 上的 ICA 签名的 ICA 连接时，会递增。	统计数据

HDX 计数器名称	用途	类别（统计数据/错误/诊断）
高密度计算机	指示 NS 检测到的 CGP 连接总数（会话可靠性打开）。每当检测到基于客户端 PCB 上的 CGP 签名的 CGP 连接时，会递增。	统计数据
高清数据库中的数据库中的数据库	指示 NS 检测到的 UDP ICA 连接总数	统计数据
数据库中的数据库中的数据库	指示 NS 检测到的 NSAP 支持连接的总数	统计数据
高清过程中的跳过	指示由于 ICA 或 CGP 签名无效而被解析器跳过的 ICA 连接数量。	统计数据
高清数据库中的活动数据库	当时的活动 ED/CGP/ICA 连接总数。	统计数据
高级管理系统的高级管理系统	当时的活动 ED/CGPP/ICA NSAP 连接总数。	统计数据
已禁用高级应用程序流	AppFlow 因禁用 AppFlow 而从会话中分离的实例总数	统计/诊断
透明用户	透明用户访问总数	统计/诊断
用户	访问网关用户访问总数	统计/诊断
用户	局域网用户模式访问总数	统计/诊断
高清基本数据	指示使用基本加密的 ICA 连接数	统计/诊断
高级数据	指示使用基于 RC5 的高级加密的 ICA 连接数	统计/诊断
在客户端上进行分类	客户端具有 Citrix SD-WAN 的 CGP/ICA 连接总数	统计/诊断
服务器端的服务器	具有 Citrix SD-WAN 服务器端的 CGP/ICA 连接总数	统计/诊断
已重新连接会话	未出现任何 Citrix ADC 错误的客户端重新连接请求总数	统计/诊断
被拒绝的主机重新连接	客户端拒绝的重新连接请求的主机总数	统计/诊断
可用的高清晰度	指示具有最终用户体验监视频道可用的连接数。要收集 ICA RTT 等统计信息，需要最终用户体验监控渠道。	统计/诊断

HDX 计数器名称	用途	类别（统计数据/错误/诊断）
已禁用的高清错误	使用 nsapimgr 旋钮禁用会话可靠性。会话不适用于此会话。	错误
高清错误跳过无微米	XA/XD 服务器缺少 MSI 功能。这表示较旧的服务器版本，HDX Insight 将跳过此连接。	错误
高清服务器跳过服务器	旧的不受支持的服务器版本	错误
高清错误白名单	客户端接收器不在允许列表中，HDX Insight 会跳过此连接	错误
已禁用高清摄像头通道	通过 SmartAccess 策略禁用的 NS_ICCA_CAM_ 通道总数	诊断
已禁用高清频道	通过 SmartAccess 策略禁用 NS_ICCA_USB_ 通道的总数	诊断
已禁用高清通道	通过 SmartAccess 策略禁用 NS_ICCA_Clip_ 通道的总数	诊断
已禁用高清频道	通过 SmartAccess 策略禁用 NS_ICCA_CCM_ 通道的总数	诊断
已禁用高清频道	通过 SmartAccess 策略禁用 NS_ICCA_CDM_ 通道的总数	诊断
hdx_sm_ica_com1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICCA_COM1_ 通道总数	诊断
hdx_sm_ica_com2_channel_di	通过 SmartAccess 策略禁用 NS_ICCA_COM2_ 通道的总数	诊断
已禁用高清通道	通过 SmartAccess 策略禁用 NS_ICCA_CPM_ 通道的总数	诊断
hdx_sm_ica_lpt1_channel_disa	通过 SmartAccess 策略禁用 NS_ICA_LPT1_ 通道的总数	诊断
hdx_sm_ica_lpt2_channel_disabled	通过 SmartAccess 策略禁用 NS_ICA_LPT2_ 通道的总数	诊断
禁用了多个数据库	通过 SmartAccess 策略禁用 MSI 的情况总数	诊断
已禁用高清文件通道	通过 SmartAccess 策略禁用 NS_ICCA_ 文件通道的总数	诊断
接受设备	接受的 USB 设备总数	诊断

HDX 计数器名称	用途	类别（统计数据/错误/诊断）
拒绝设备	拒绝的 USB 设备总数	诊断
设置终端节点	USB 端点重置总数	诊断
设备的设备	重置 USB 设备的总数	诊断
高清设备	已停止的 USB 设备总数	诊断
设备响应	来自已停止 USB 设备的响应总数	诊断
设备已经消失了	USB 设备总数	诊断
已停止设备	已停止的 USB 设备总数	诊断

nstrace 验证

检查 CFLOW 协议以查看从 Citrix ADC 中传出的所有 AppFlow 记录。

Citrix ADM 核对表中的记录填写

- 运行命令 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: ica_"` 并检查日志以确认 Citrix ADM 正在接收 AppFlow 记录。
- 确认已将 Citrix ADC 实例添加到 Citrix ADM 中。
- 验证 Citrix 网关 /VPN 虚拟服务器是否在 Citrix ADM 中获得许可。
- 确保为双跳启用了多跳参数设置。
- 确保已清除 Citrix Gateway 在双跃点部署中的第二跃点。

在联系 **Citrix** 技术支持之前

为了快速解决问题，请确保在联系 Citrix 技术支持之前具有以下信息：

- 部署和网络拓扑的详细信息。
- Citrix ADC 和 Citrix ADM 版本。
- Citrix Virtual Apps and Desktops 服务器版本。
- 客户端接收器版本。
- 发生问题时的活动 ICA 会话数。
- 通过在 Citrix ADC `show techsupport` 命令提示符下运行命令捕获的技术支持包。
- 为 Citrix ADM 捕获的技术支持包。

- 在所有 Citrix ADC 上捕获的数据包跟踪。
  要启动数据包跟踪，请键入，`start nstrace -size 0'`
  要停止数据包跟踪，请键入、`stop nstrace`
- 通过运行 `show arp` 命令收集系统 ARP 表中的条目。

已知问题

有关 HDX Insight 的已知问题，请参阅 Citrix ADC 发行说明。

Gateway Insight

April 23, 2021

在 Citrix Gateway 部署中，查看用户的访问详细信息对于解决访问失败问题至关重要。作为网络管理员，您想知道用户何时无法登录到 Citrix Gateway，并希望了解用户活动以及登录失败的原因。除非用户发送解决请求，否则此信息通常不可用。

Gateway Insight 提供了所有用户在登录 Citrix Gateway 关时遇到的故障的可见性（无论访问模式如何）。可以查看所有可用用户列表，以及任何给定时间的活动用户数、活动会话数及所有用户使用的字节数和许可证数。可以查看某个用户的端点分析 (EPA)、身份验证、单点登录 (SSO) 及应用程序启动失败。还可以查看某个用户的活动会话和已终止会话的详细信息。

通过 Gateway Insight 还可以查看虚拟应用程序的应用程序启动失败的原因。这可提高您对任何登录或应用程序启动失败问题进行故障排除的能力。您可以查看启动的应用程序数、总会话数和活动会话数、总字节数以及应用程序消耗的带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

您可以查看与 Citrix Gateway 设备关联的所有网关在任何给定时间使用的网关数、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活动的详细信息。

所有日志消息都存储在 Citrix ADM 数据库中，因此您可以查看任何时间段的错误详细信息。还可以查看登录失败摘要，并确定在登录过程的什么阶段发生了失败。

注意事项

- 以下部署支持 Gateway Insight：
  - Access Gateway
  - Unified Gateway
- Citrix ADM 版本和内部版本必须与 Citrix Gateway 设备的版本和内部版本相同或晚。
- 可以查看具有高级许可证的 Citrix ADC 实例的一小时网关智能分析报告。高级许可证是必须查看超过一小时的网关智能分析报告。

限制

- 当身份验证方法配置为基于证书的身份验证时，Citrix Gateway 网关不支持 Gateway Insight。
- 对于 Gateway Insight 报告，Citrix ADC 设备不提供地理位置信息。
- 在 HDX Insight“Users”（用户）控制板上只能看到虚拟 ICA 应用程序和桌面的成功用户登录、延迟及应用程序级别详细信息。
- 在双跳模式下，第二个 DMZ 中 Citrix Gateway 设备故障的可见性不可用。
- 远程桌面协议 (RDP) 桌面访问问题不会报告。
- 以下身份验证类型支持网关智能分析。如果使用这些身份验证类型以外的其他身份验证类型，您可能会在网关智能分析中看到一些不一致之处。
  - 本地
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - 本机 OTP

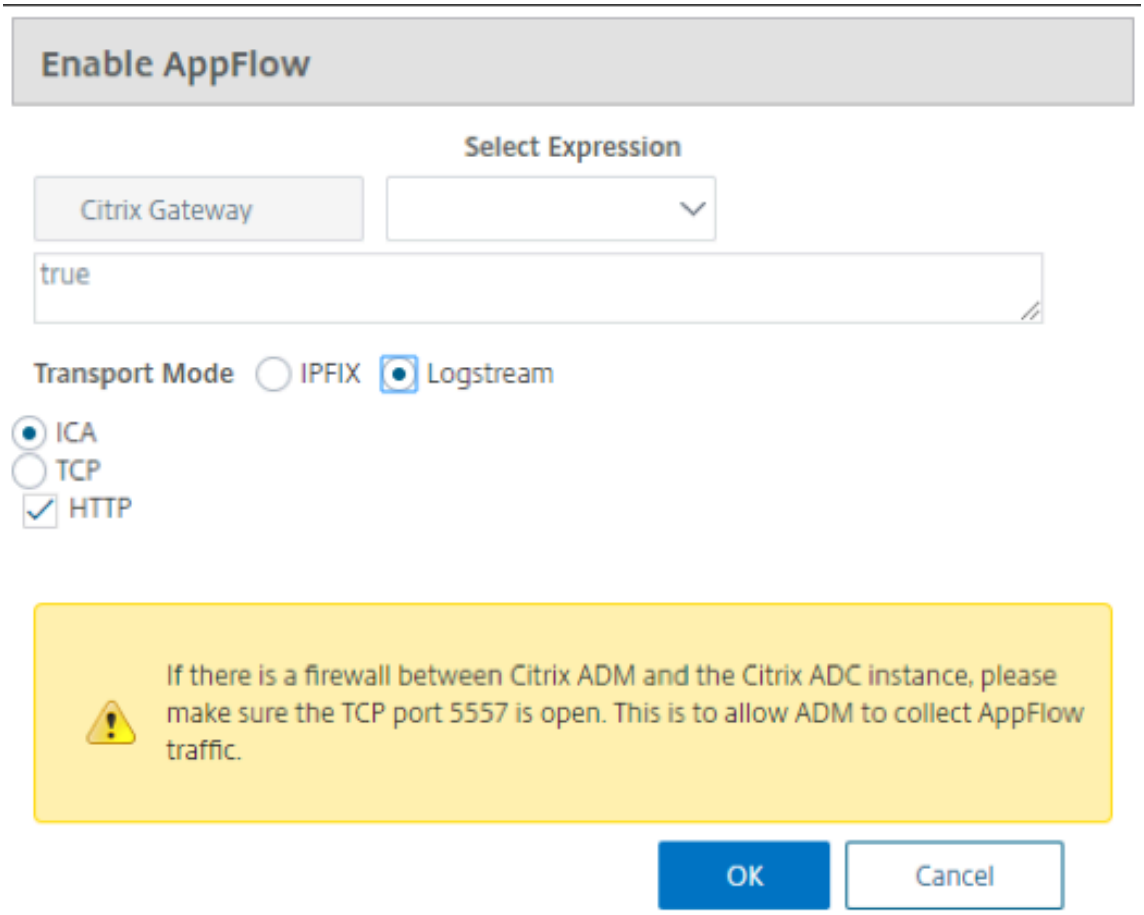
启用网关洞察

要为您的 Citrix 网关设备启用网关智能分析，必须首先将 Citrix 网关设备添加到 Citrix ADM 中。然后必须为表示 VPN 应用程序的虚拟服务器启用 AppFlow。有关将设备添加到 Citrix ADM 的信息，请参阅添加设备。

> 注意
>
> 要查看 Citrix ADM 中的端点分析 (EPA) 故障，必须在 Citrix Gateway 设备上启用AppFlow 身份验证、授权和审核用户名 日志记录。

如果您的 Citrix ADM 是 **13.0** 版本 **36.27**，则可以执行以下过程来启用 Gateway 洞察：

1. 导航到 **“网络” > “实例”**，然后选择要为其启用 **AppFlow** 的实例。
2. 从选择操作列表中，选择配置分析。
3. 在 “ 配置智能分析” 页的 “ 配置分析” 下，选择 **Citrix Gateway**。
4. 选择虚拟服务器，然后单击 启用 **AppFlow**。
5. 在启用 **AppFlow** 屏幕上的选择表达式列表中，单击 “真”。
6. 在 传输模式旁边，选中 日志流复选框。

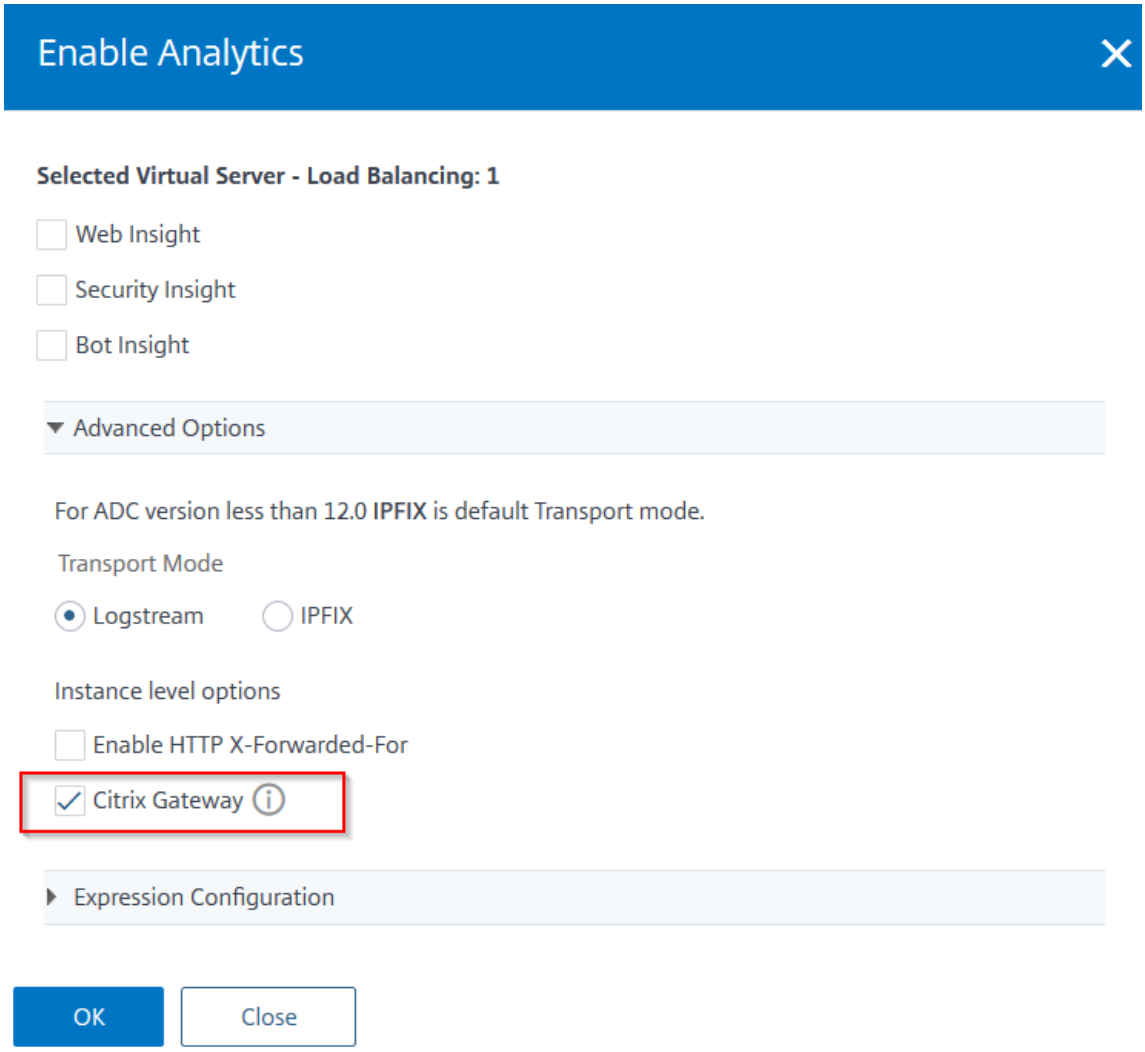


> 注意
>
> 您可以选择 **IPFIX** 或 日志流作为传输模式。
>
> 有关 **IPFIX** 和 **Logstream** 的更多信息，请参阅 日志流概述。

7. 单击确定。

对于 **Citrix ADM** 版本 **13.0** 版本 **41.x** 或更高版本

1. 导航到 “ 网络” > “实例”，然后选择实例。
2. 从选择操作列表中，选择配置分析。
3. 选择虚拟服务器，然后单击启用分析。
4. 在 “ 高级选项” 下：
   a) 选择 日志流
   b) 选择 **Citrix Gateway**
5. 单击确定。



使用 **GUI** 在 **Citrix Gateway** 设备上启用 **AppFlow** 身份验证、授权和审核用户名记录

1. 导航到配置 **>** 系统 **> AppFlow >** 设置，然后单击更改 **AppFlow** 设置。
2. 在配置 **AppFlow** 设置屏幕中，选择 **AAA** 用户名，然后单击确定。

查看网关智能分析报告

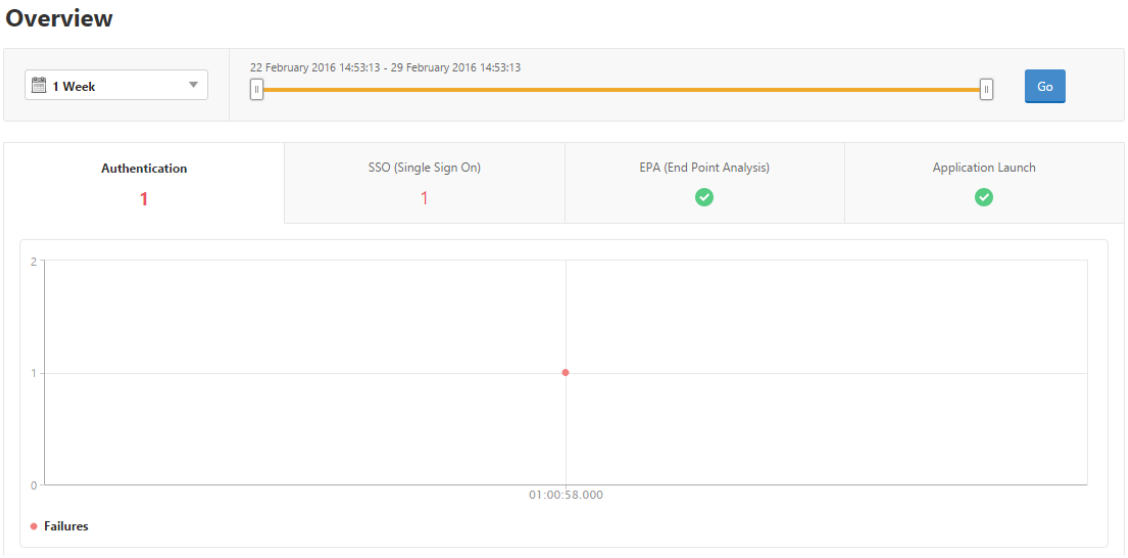
在 Citrix ADM 中，您可以查看与 Citrix Gateway 设备关联的所有用户、应用程序和网关的报告，还可以查看特定用户、应用程序或网关的详细信息。在“ 概述”部分，您可以查看 EPA、SSO、身份验证和应用程序启动失败。还可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。

> 注意
>
> 创建组时，您可以为组分配角色、提供对组的应用程序级别访问权限以及将用户分配给组。Citrix ADM 分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有

> 关组和向组分配用户的详细信息，请参阅 配置组。

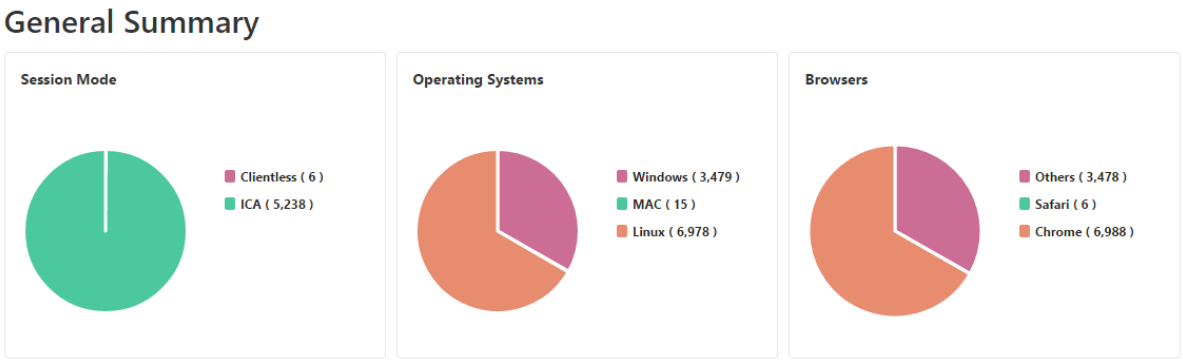
查看 **EPA**、**SSO**、身份验证、授权和应用程序启动失败

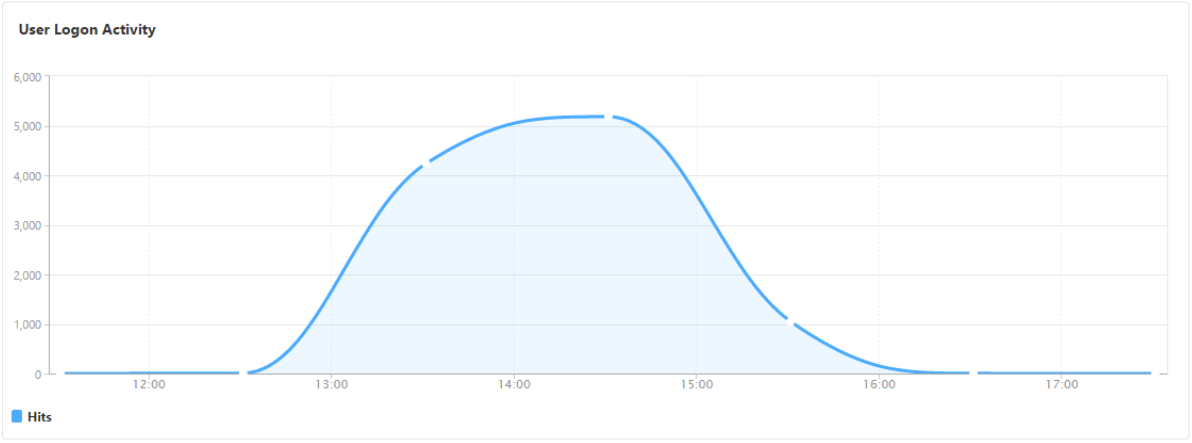
1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 单击 “EPA (End Point Analysis)”（EPA(端点分析)）、“Authentication”（身份验证）、“Authorization”（授权）、“SSO (Single Sign On)”（SSO(单点登录)）或 “Application Launch”（应用程序启动）选项卡以显示失败详细信息。



查看会话模式、客户端及用户数摘要

在 Citrix ADM 中，导航到分析 **> Gateway Insight**，向下滚动以查看报告。





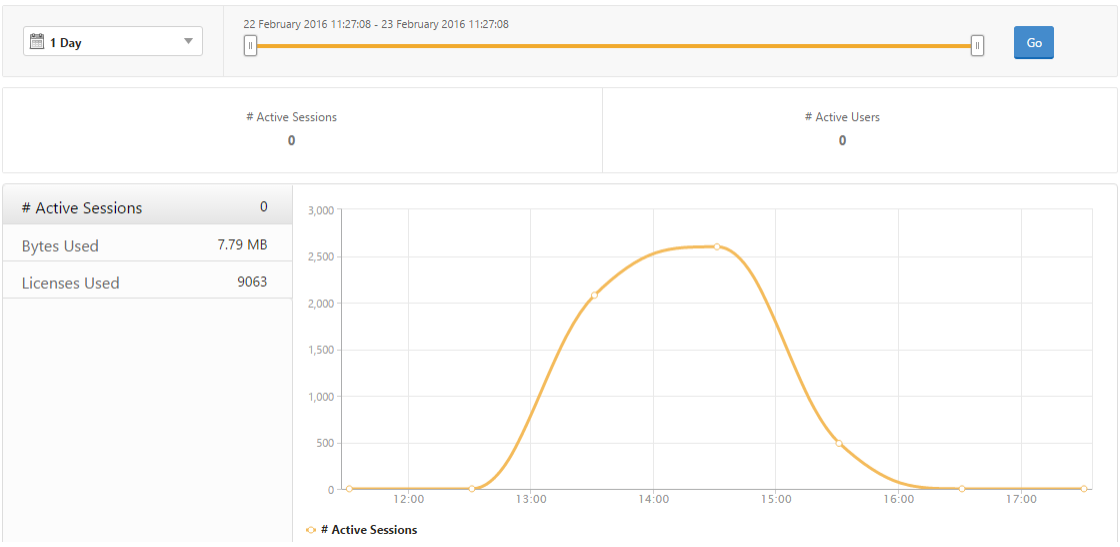
查看用户的网关智能分析报告

您可以查看以下内容的报告：

- 与 Citrix Gateway 设备关联的所有用户。
- 用户的 EPA、身份验证、SSO 和应用程序启动失败。
- 用户的活动和已终止会话的详细信息。
- 会话模式的类型，如全通道、无客户端 VPN 和 ICA 代理。

查看用户详细信息

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight >** 用户。
2. 选择要查看用户详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。
3. 您可以查看该时段内所有用户使用的活动用户数、活动会话数、字节数和许可证。

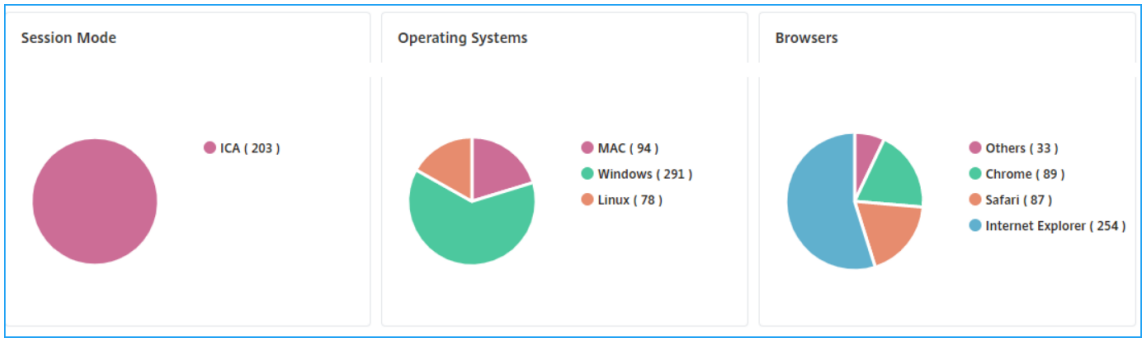


向下滚动可查看可用用户和活动用户列表。

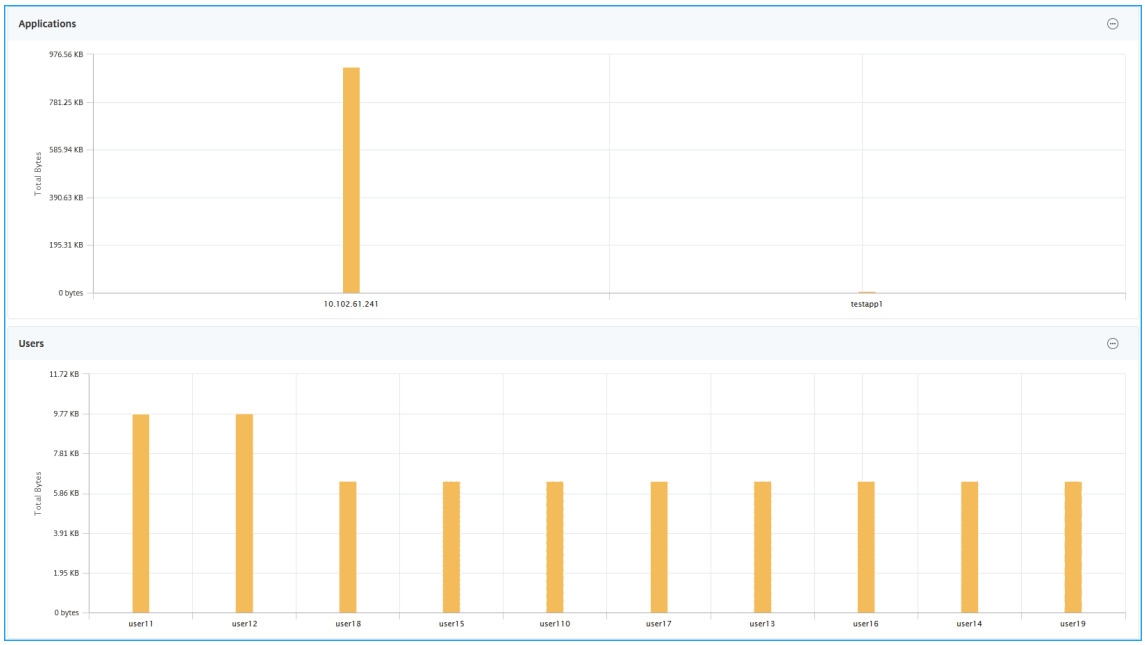
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

在“用户”或“活动用户”选项卡上，单击用户可查看以下用户详细信息：

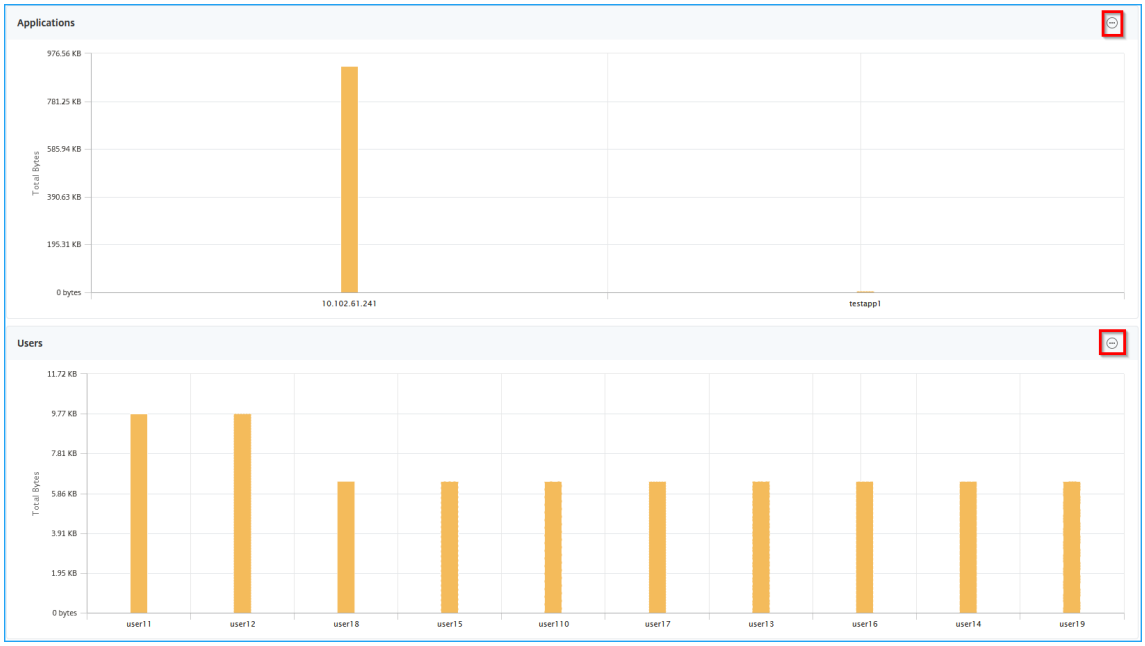
- 用户详细信息 -您可以查看与 ADC Gateway 设备关联的每个用户的见解。导航到 **Analytics** > **Gateway Insight** > 用户，然后单击用户以查看选定用户的见解，例如会话模式、操作系统和浏览器。



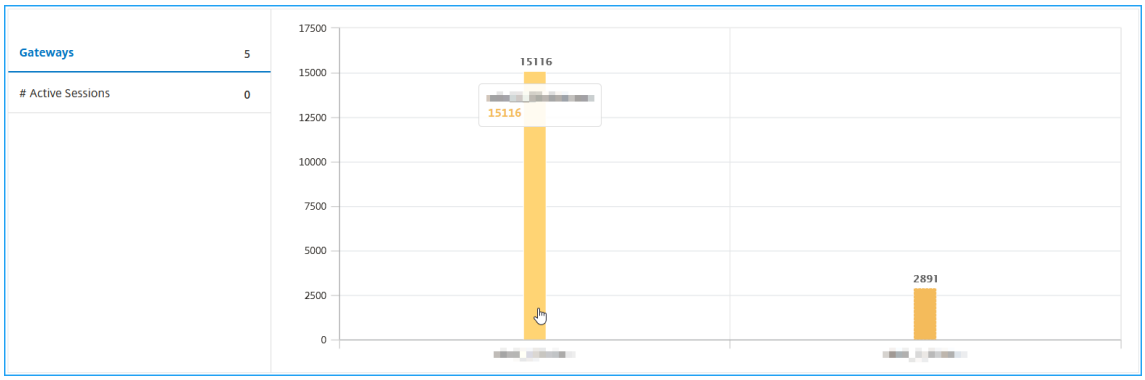
- 选定网关的用户和应用程序 -导航到 **Analytics** > **Gateway Insight**> 网关，然后单击网关域名以查看与所选网关关联的前 10 个应用程序和前 10 名用户。



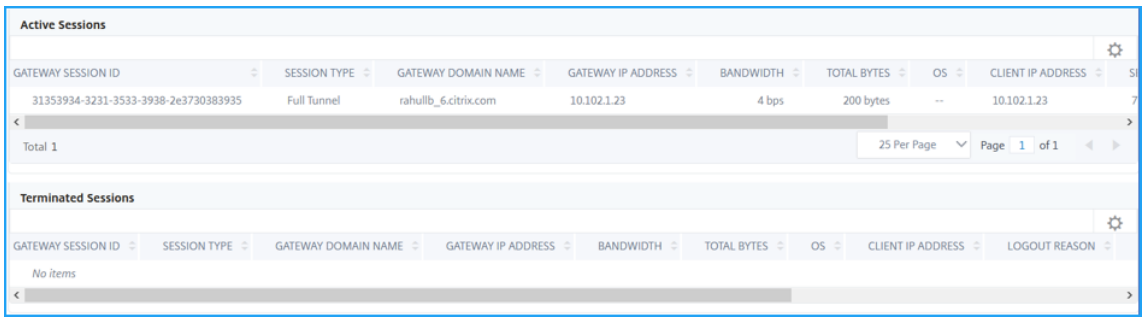
- 查看应用程序和用户的更多选项 — 对于 10 个以上的应用程序和用户，您可以单击应用程序和用户中的更多图标以查看与所选网关关联的所有用户和应用程序详细信息。



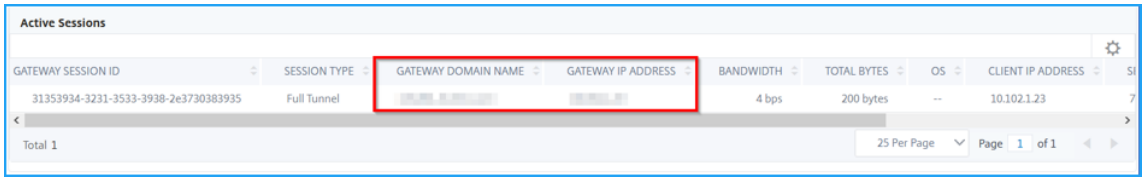
- 通过单击条形图查看详细信息 — 单击条形图时，可以查看相关详细信息。例如，导航到 **Analytics > Gateway Insight >** 网关，然后单击网关条形图以查看网关详细信息。



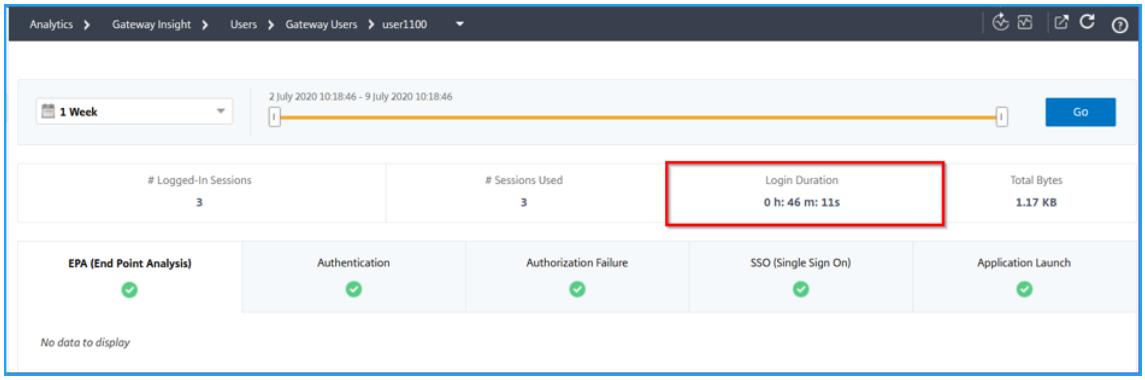
- 用户 活动会话和 已终止的会话。



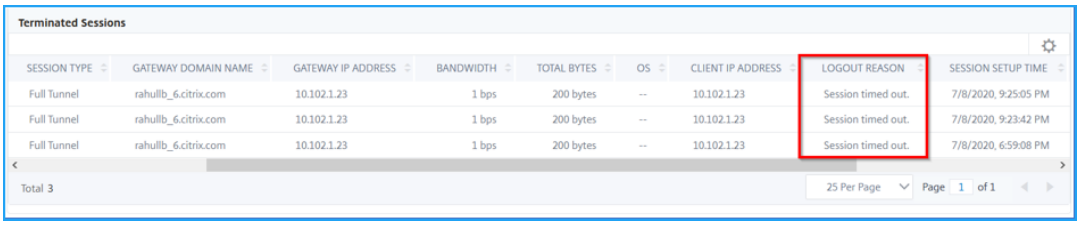
- 活动会话中的网关域名和网关 IP 地址。



- 用户登录持续时间。



- 用户注销会话的原因。注销的原因可能是：
  - 会话超时
  - 由于内部错误而注销
  - 由于非活动会话超时而注销
  - 用户已注销
  - 管理员已停止会话



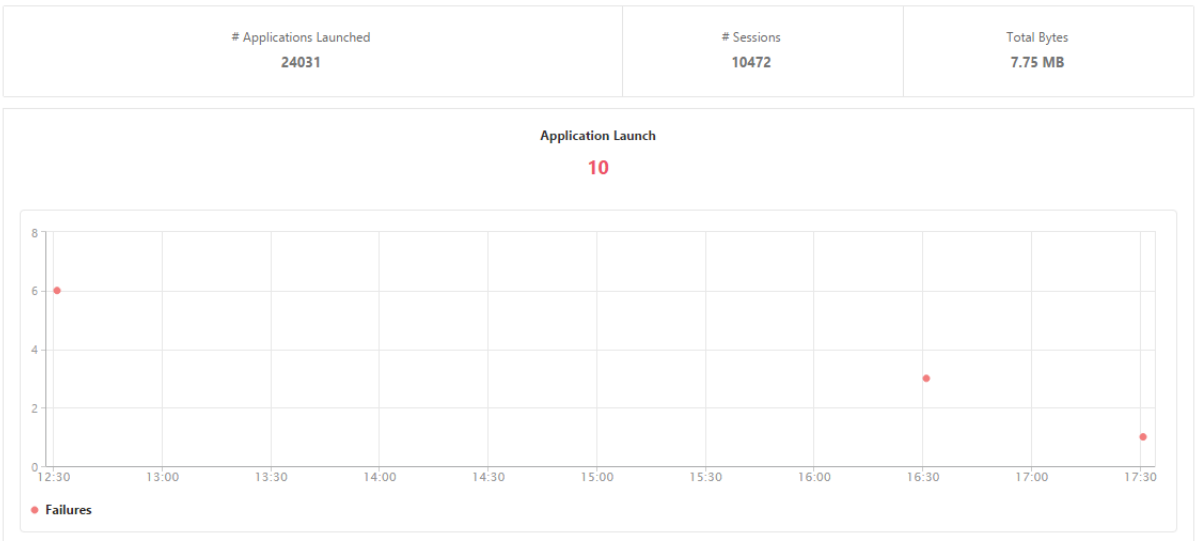
查看应用程序的网关智能分析报告

您可以查看启动的应用程序数、总会话和活动会话数、应用程序消耗的总字节数和带宽。可以查看应用程序的用户、会话、带宽和启动错误的详细信息。

查看应用程序详细信息

1. 在 Citrix ADM 中，导航到 分析 **> Gateway Insight >** 应用程序。
2. 选择要查看应用程序详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在，您可以查看启动的应用程序数、总会话和活动会话数、应用程序消耗的总字节数和带宽。



向下滚动可查看 ICA 和其他应用程序使用的会话数、带宽及总字节数。

Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	3972	52 bps	3.79 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB

在其他应用程序选项卡上，您可以单击名称列中的应用程序以显示该应用程序的详细信息。

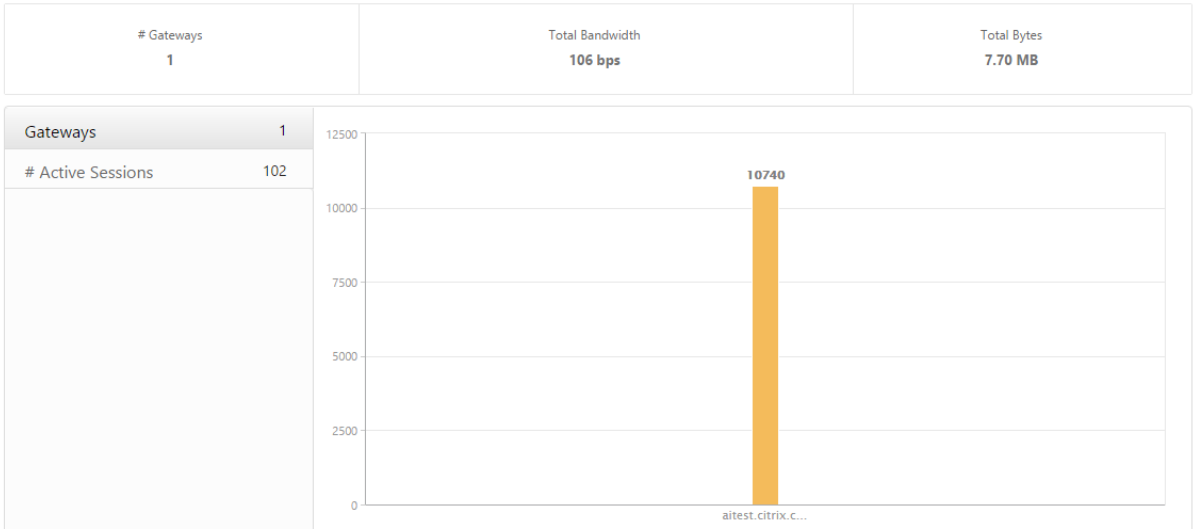
查看网关智能分析报告

您可以查看与 Citrix Gateway 设备关联的所有网关在任何给定时间使用的网关数、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其登录活动的详细信息。

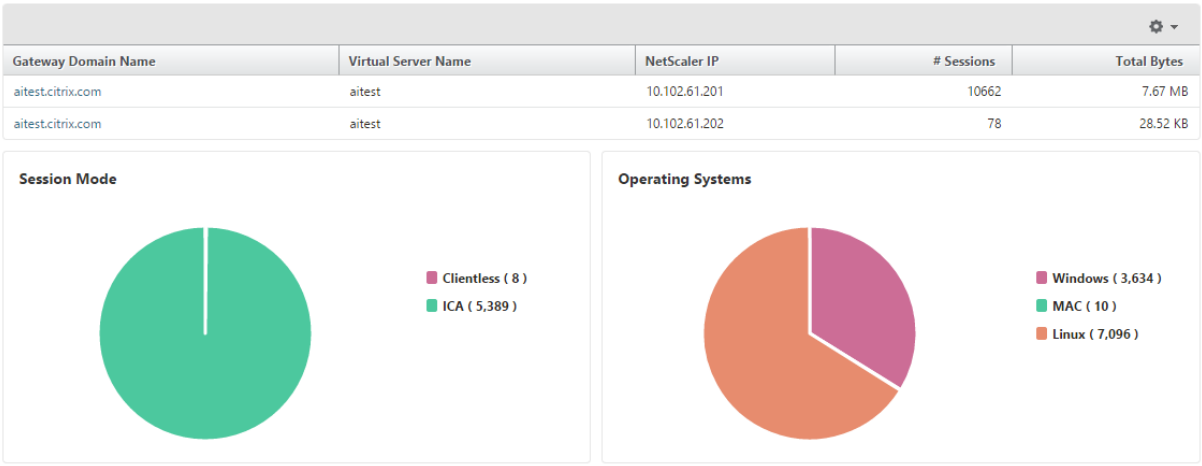
查看网关详细信息

1. 在 **Citrix ADM** 中，导航到 **“分析” > “网关智能分析” > “网关”**。
2. 选择要查看网关详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

现在，您可以查看与 Citrix Gateway 设备关联的所有网关在任何给定时间使用的网关数、活动会话数、总字节数和带宽。



向下滚动可查看网关详细信息，例如，“Gateway Domain Name”（网关域名）、“Virtual Server Name”（虚拟服务器名称）、NetScaler IP 地址、会话模式及“Total Bytes”（总字节数）。



您可以单击 Gateway 域名列中的 **Gateway**，以显示网关的 EPA、身份验证、单点登录和应用程序启动失败以及其他详细信息。

导出报告

您可以在本地计算机上以 PDF、JPEG、PNG 或 CSV 格式将 GUI 中显示的所有详细信息保存网关智能分析报告。您还可以计划以各种时间间隔将报告导出到指定的电子邮件地址。

> 注意
>
> - 具有只读访问权限的用户不能导出报告。
> - 仅当 Citrix ADM 具有互联网连接时，才会导出地理地图报告。

导出报告

1. 在控制板选项卡上的右窗格中，单击导出按钮。
2. 在 立即导出”下，选择所需的格式，然后单击 导出”。

要计划导出：

1. 在控制板选项卡上的右窗格中，单击导出按钮。
2. 在计划导出下，指定详细信息，然后单击计划。

要添加电子邮件服务器或电子邮件通讯组列表，请执行以下操作：

1. 在配置选项卡上，导航到系统 > 通知 > 电子邮件。
2. 在右窗格中，选择“ 电子邮件服务器”以添加电子邮件服务器，或选择“ 电子邮件通讯组列表”以创建电子邮件通讯组列表。
3. 指定详细信息，然后单击创建。

要导出整个网关智能分析控制板：

1. 在控制板选项卡上的右窗格中，单击导出按钮。
2. 在立即导出下，选择 **PDF** 格式，然后单击导出。

网关智能分析使用案例

以下使用案例演示了如何使用网关智能分析来了解用户在 Citrix 网关设备上的访问详细信息、应用程序和网关。

用户无法登录到 **Citrix Gateway** 设备或内部 **Web** 服务器

您是 Citrix Gateway 管理员通过 Citrix ADM 监视 Citrix 网关装置，并希望了解用户无法登录的原因，或者在登录过程的哪个阶段发生了故障。

Citrix ADM 使您能够在登录过程的以下阶段查看用户登录错误详细信息：

- 身份验证
- 端点分析 (EPA)
- 单点登录

在 Citrix ADM 中，您可以搜索特定用户，然后查看该用户的所有详细信息。

要搜索用户，请执行以下操作：

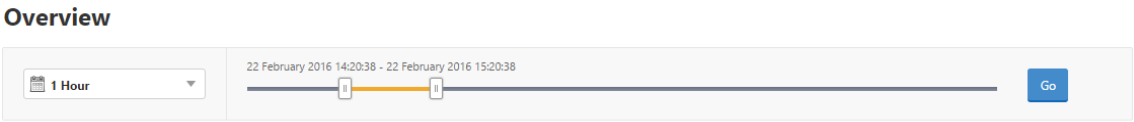
在 Citrix ADM 中，导航到分析 **> Gateway Insight**，然后在搜索用户文本框中指定要搜索的用户。

身份验证失败

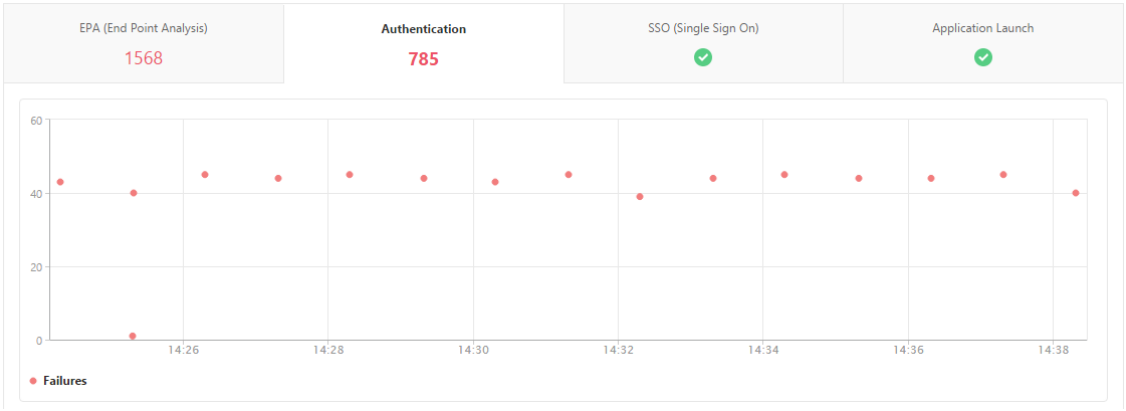
可以查看身份验证错误，例如，凭据错误或身份验证服务器没有响应。您还可以查看身份验证失败的因素。

要查看验证失败的详细信息，请执行以下操作：

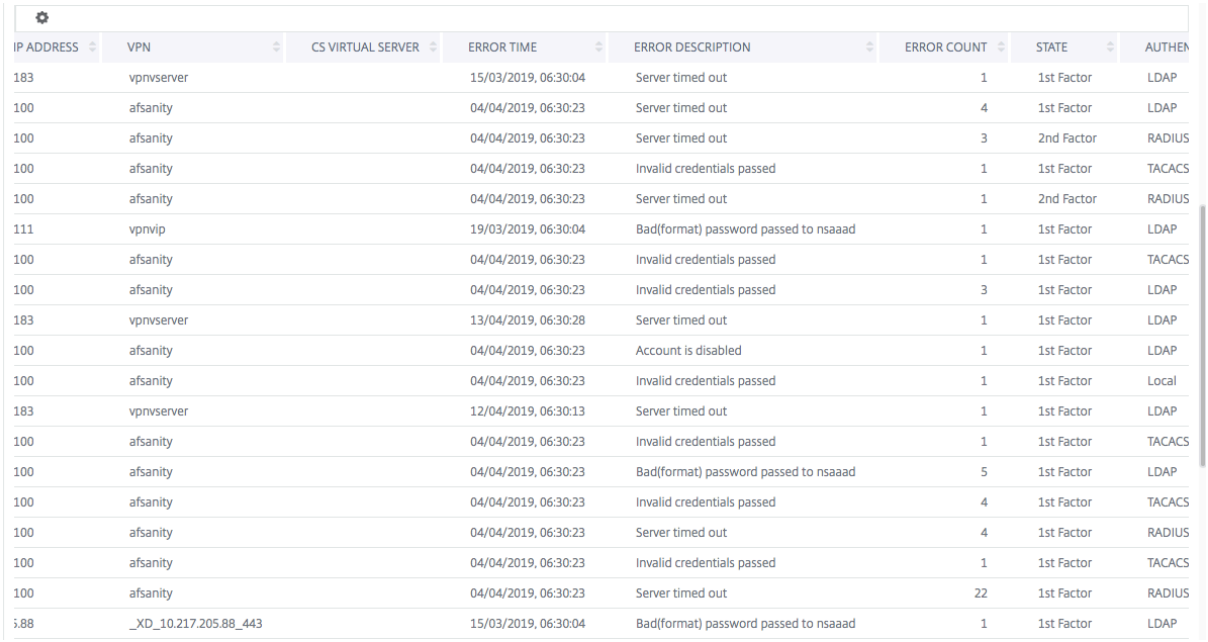
1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在概述部分中，选择要查看身份验证错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击身份验证选项卡。您可以在失败图表中查看任何给定时间的身份验证错误数。



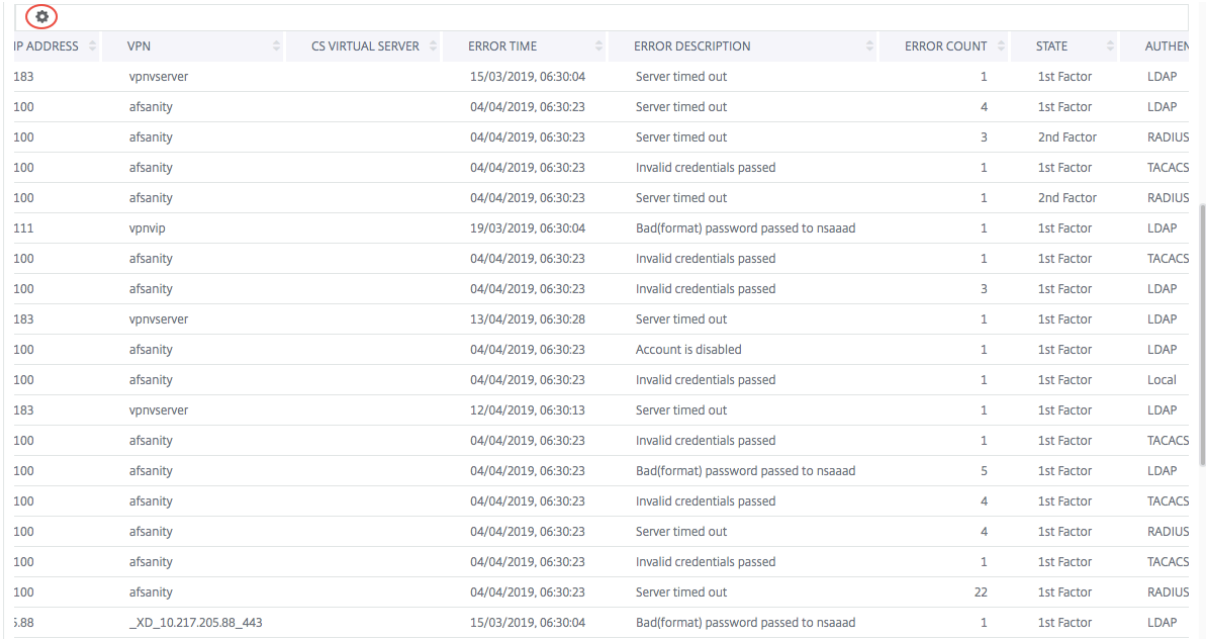
在同一选项卡上的表中向下滚动可查看每个身份验证错误的详细信息，例如，**Username**（用户名）、**Client IP Address**（客户端 **IP** 地址）、**Error Time**（错误时间）、**Authentication Type**（身份验证类型）、**Authentication Server IP Address**（身份验证服务器 **IP** 地址）及其他信息。表中的“ 错误说明”列显示登录失败的原因，“ 状态”列显示出现故障的第 n 个因子。



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

您可以单击“用户 名”列中的用户以显示该用户的身份验证错误和其他详细信息。

您可以使用以下屏幕截图中所示的设置图标自定义表以添加或删除列。



IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR TIME	ERROR DESCRIPTION	ERROR COUNT	STATE	AUTHEN
183	vpnvserver		15/03/2019, 06:30:04	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Server timed out	3	2nd Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	1	2nd Factor	RADIUS
111	vpnvip		19/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	3	1st Factor	LDAP
183	vpnvserver		13/04/2019, 06:30:28	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Account is disabled	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	Local
183	vpnvserver		12/04/2019, 06:30:13	Server timed out	1	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Bad(format) password passed to nsaaad	5	1st Factor	LDAP
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	4	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	4	1st Factor	RADIUS
100	afsanity		04/04/2019, 06:30:23	Invalid credentials passed	1	1st Factor	TACACS
100	afsanity		04/04/2019, 06:30:23	Server timed out	22	1st Factor	RADIUS
.88	_XD_10.217.205.88_443		15/03/2019, 06:30:04	Bad(format) password passed to nsaaad	1	1st Factor	LDAP

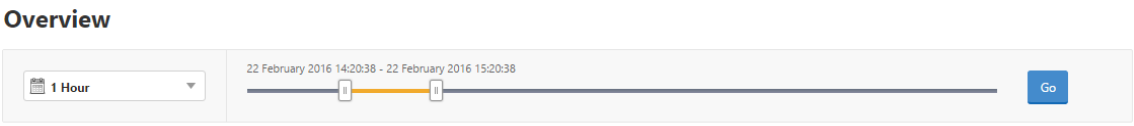
环保局失败

可以查看身份验证前阶段或身份验证后阶段的 EPA 失败。

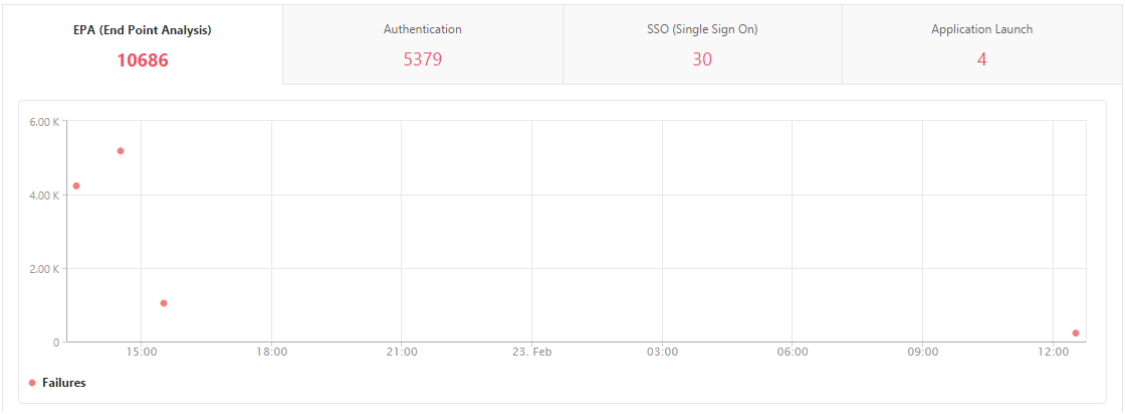
要查看 **EPA** 失败详细信息，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。

2. 在“Overview”（概览）部分中，选择要查看 EPA 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击 **EPA**（终点分析）选项卡。您可以在故障图中查看任何给定时间的 EPA 错误数。



在同一选项卡上的表中向下滚动可查看每个 EPA 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Gateway IP Address**（网关 **IP** 地址）、**VPN**、**Error Time**（错误时间）、**Policy Name**（策略名称）、**Gateway Domain Name**（网关域名）及其他信息。表中 **Error Description**（错误说明）列显示 EPA 失败的原因，**Policy Name**（策略名称）列显示导致失败的策略。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

您可以单击“用户 名”列中的用户以显示该用户的 EPA 错误和其他详细信息。

您可以使用下面的屏幕截图中所示的向下箭头自定义表以添加或删除列。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	Policy Name	EPA Method	Gateway Domain Name
user1097	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1098	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1491	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1633	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 3:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user17	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user1774	10.102.61.201	10.102.61.200	10.102.61.210	aitest	2/22/2016, 2:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com
user197	10.102.61.201	10.144.2.35	10.102.61.210	aitest	2/22/2016, 1:30:54 PM	Post auth failed, no quar...	1	postauth_act		aitest.citrix.com

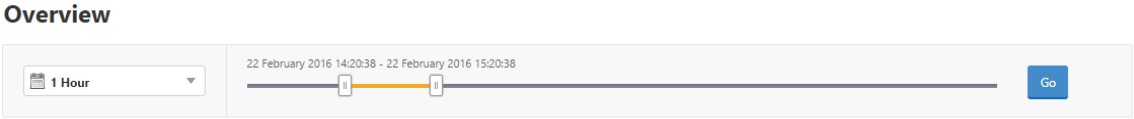
> 注意
>
> 当“客户端安全”表达式配置为 VPN 会话策略规则时，Citrix Gateway 不会报告 EPA 故障。

SSO 故障

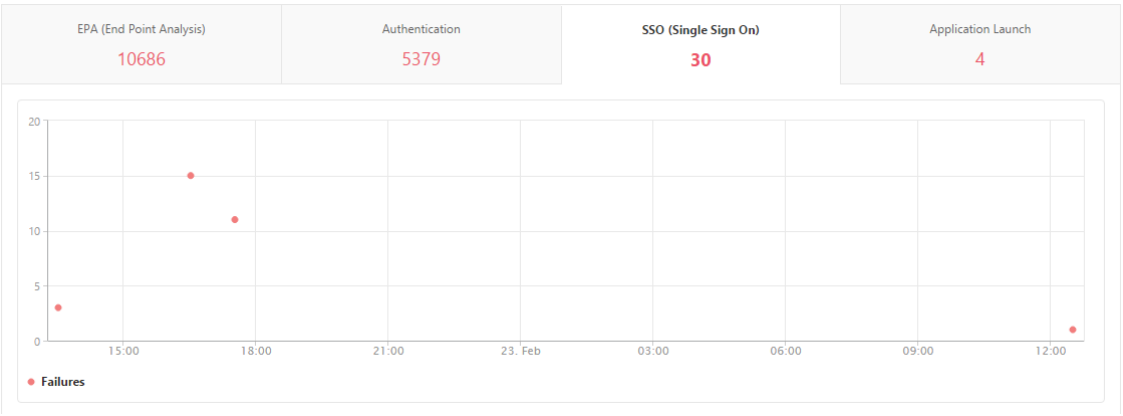
您可以查看通过 Citrix Gateway 设备访问任何应用程序的用户在任何阶段的所有 SSO 故障。

要查看 **SSO** 故障详细信息，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在“Overview”（概览）部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击 **SSO**（单次登录）选项卡。可以在“Failures”（失败）图中查看任何给定时间的 SSO 错误数。

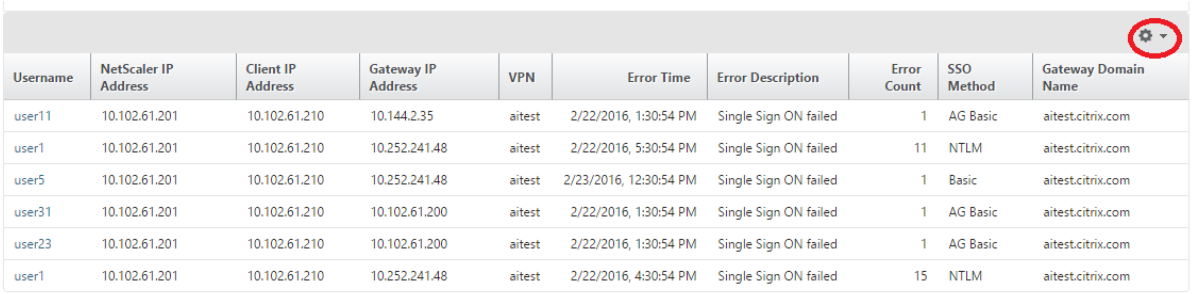


在同一选项卡上的表中向下滚动可查看每个 SSO 错误的详细信息，例如，**Username**（用户名）、**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）及其他信息。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

您可以单击“用户 名”列中的用户以显示该用户的 SSO 错误和其他详细信息。

您可以使用下面的屏幕截图中所示的向下箭头自定义表以添加或删除列。



Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	Error Time	Error Description	Error Count	SSO Method	Gateway Domain Name
user11	10.102.61.201	10.102.61.210	10.144.2.35	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 5:30:54 PM	Single Sign ON failed	11	NTLM	aitest.citrix.com
user5	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/23/2016, 12:30:54 PM	Single Sign ON failed	1	Basic	aitest.citrix.com
user31	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user23	10.102.61.201	10.102.61.210	10.102.61.200	aitest	2/22/2016, 1:30:54 PM	Single Sign ON failed	1	AG Basic	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	2/22/2016, 4:30:54 PM	Single Sign ON failed	15	NTLM	aitest.citrix.com

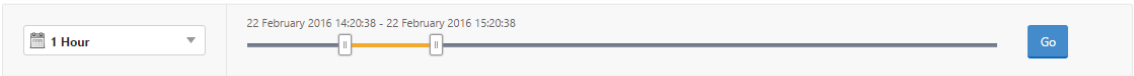
成功登录到 **Citrix Gateway** 后，用户将无法启动任何虚拟应用程序

对于应用程序启动失败，您可以了解原因，例如无法访问的安全票证颁发机构 (STA) 或 Citrix 虚拟应用程序服务器或 STA 票证无效。可以查看错误发生的时间、错误的详细信息以及 STA 验证失败的资源。

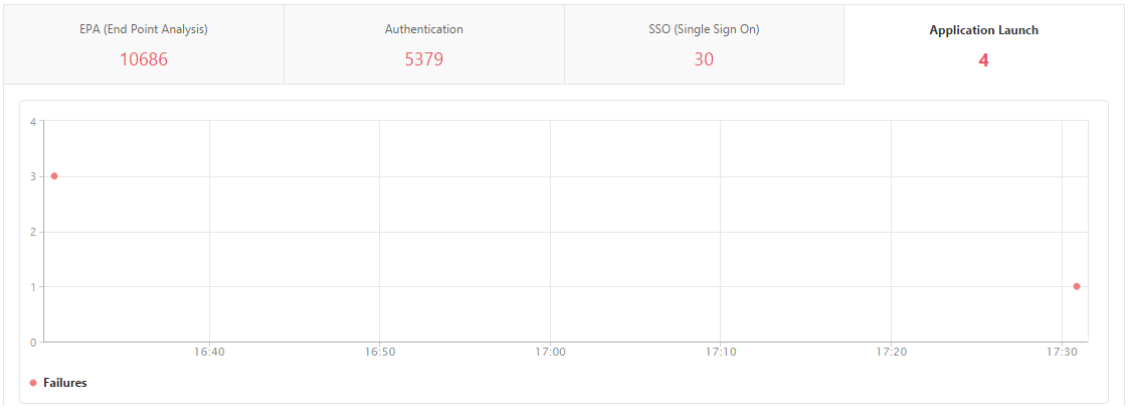
查看应用程序启动失败的详细信息：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在 **Overview**（概览）部分中，选择要查看 SSO 错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。

   Overview

3. 单击应用程序启动选项卡。您可以在失败图表中查看任何给定时间的应用程序启动失败次数。



在同一选项卡上的表中向下滚动可查看每个应用程序启动错误的详细信息，例如，**NetScaler IP Address**（**NetScaler IP** 地址）、**Error Time**（错误时间）、**Error Description**（错误说明）、**Resource Name**（资源名称）、**Gateway Domain Name**（网关域名）及其他信息。表中的 **Error Description**（错误说明）列显示 STA 服务器的 IP 地址，**Resource Name**（资源名称）列显示 STA 验证失败的资源的详细信息。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

您可以单击“用户 名”列中的用户以显示该用户的应用程序启动错误和其他详细信息。

您可以使用下面的屏幕截图中所示的向下箭头自定义表以添加或删除列。

Username	NetScaler IP Address	Client IP Address	Gateway IP Address	VPN	STA IP Address	Error Time	Error Description	Error Count	Resource Name	Gateway Domain Name
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 5:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	c.go-mpulse.net	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	code.jquery.com	aitest.citrix.com
user1	10.102.61.201	10.102.61.210	10.252.241.48	aitest	-NA-	2/22/2016, 4:30:54 PM	Gateway timed out (HTTP c...	1	cdn.kendostatic.com	aitest.citrix.com

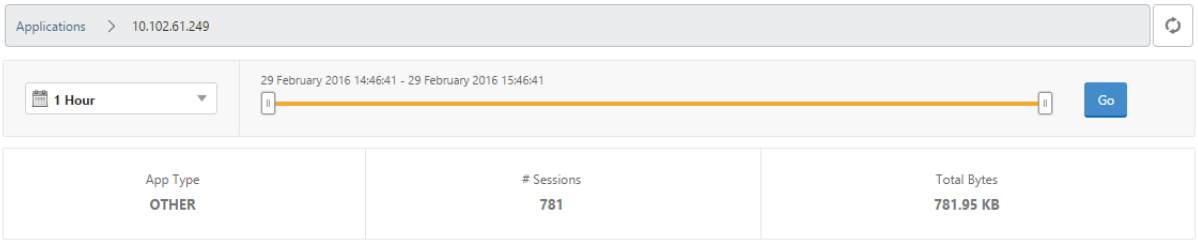
成功启动新应用程序后，用户希望查看该应用程序占用的总字节和带宽

成功启动新应用程序后，可以在 Citrix ADM 中查看该应用程序占用的总字节和带宽。

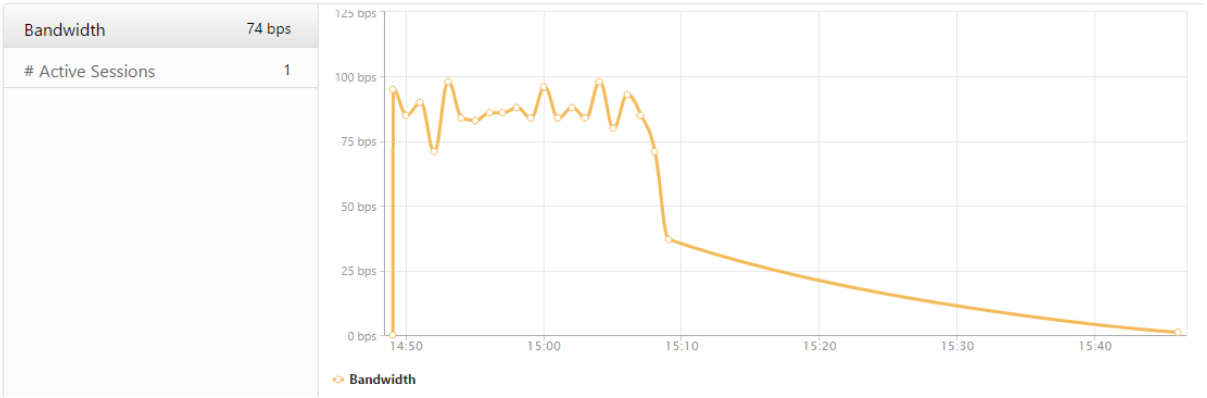
要查看应用程序消耗的总字节和带宽，请执行以下操作：

在 Citrix ADM 中，导航到分析 **> Gateway Insight >** 应用程序，向下滚动，然后在其他应用程序选项卡上单击要查看详细信息的应用程序。

可以查看该应用程序使用的会话数和总字节数。



还可以查看该应用程序使用的带宽。

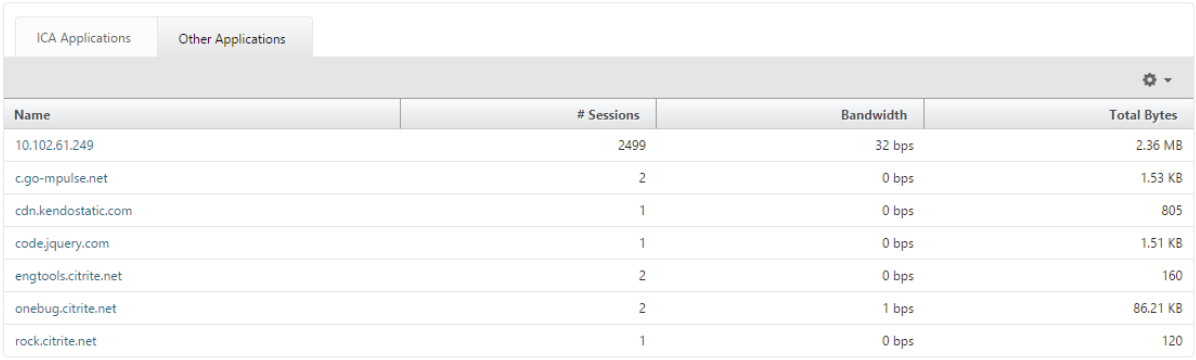


用户已成功登录到 **Citrix Gateway**，但无法访问内部网络中的某些网络资源

通过 Gateway Insight，可以确定用户是否有权访问网络资源。还可以查看导致失败的策略的名称。

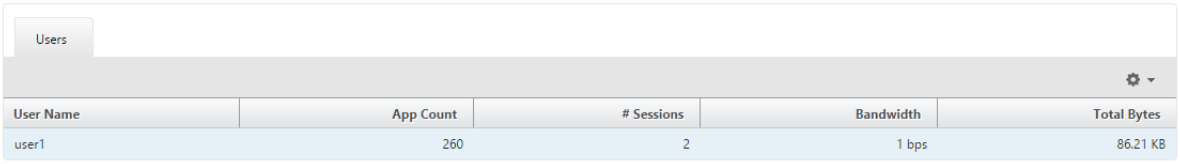
要查看资源的用户访问权限，请执行以下操作：

1. 在 Citrix ADM 中，导航到 **“分析” > “网关洞察” > “应用程序”**。
2. 在出现的屏幕上，向下滚动，然后在 其他应用程序选项卡上，选择用户无法登录的应用程序。



Name	# Sessions	Bandwidth	Total Bytes
10.102.61.249	2499	32 bps	2.36 MB
c.go-mpulse.net	2	0 bps	1.53 KB
cdn.kendostatic.com	1	0 bps	805
code.jquery.com	1	0 bps	1.51 KB
engtools.citrite.net	2	0 bps	160
onebug.citrite.net	2	1 bps	86.21 KB
rock.citrite.net	1	0 bps	120

在出现的屏幕上向下滚动，并在“用户”表中显示有权访问该应用程序的所有用户。



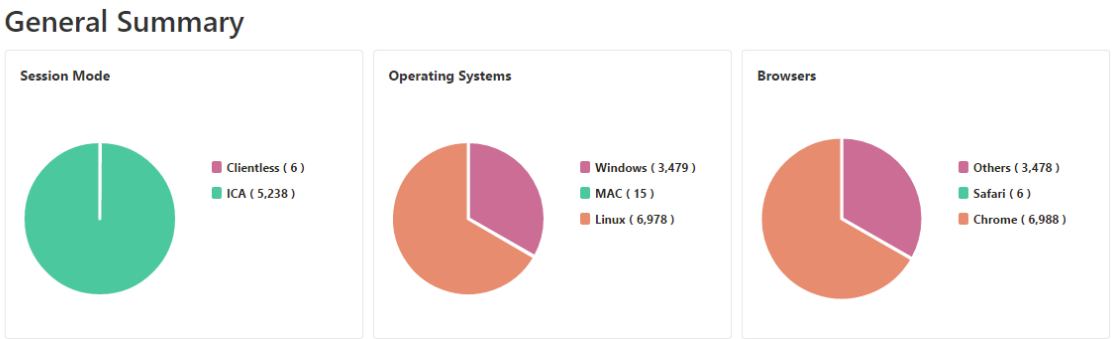
User Name	App Count	# Sessions	Bandwidth	Total Bytes
user1	260	2	1 bps	86.21 KB

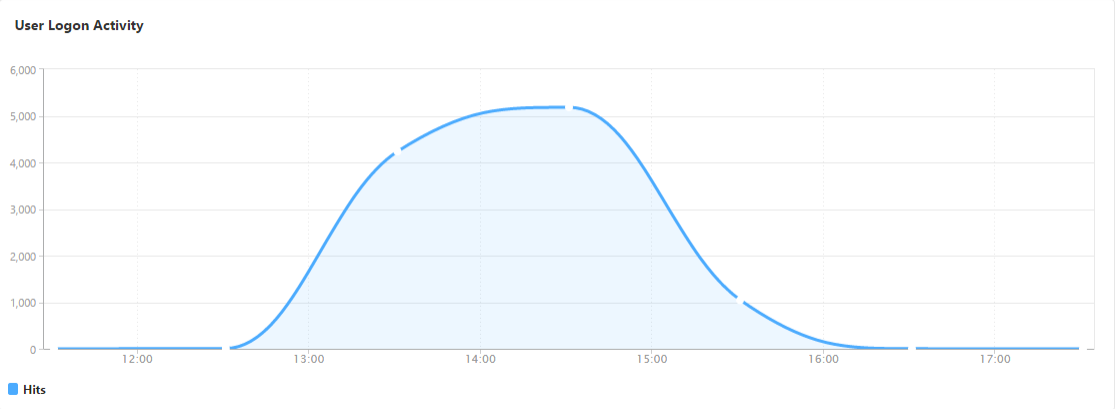
不同的用户可能正在使用不同的 **Citrix Gateway** 部署，也可能通过不同的访问模式登录到 **Citrix** 网关。管理员必须能够查看有关部署类型和访问模式的详细信息

通过 Gateway Insight，可以查看用户用于登录的不同会话模式、客户端类型及每小时登录用户数的摘要。您还可以确定用户的部署是统一网关还是传统的 Citrix Gateway 部署。对于 Unified Gateway 部署，可以查看内容交换虚拟服务器名称和 IP 地址及 VPN 虚拟服务器名称。

要查看会话模式、客户端类型和登录用户数的摘要，请执行以下操作：

1. 在 Citrix ADM 中，导航到分析 **> Gateway Insight**。
2. 在概述部分中，向下滚动以查看会话模式、操作系统、浏览器和用户登录活动图表显示用户用于登录的不同会话模式、客户端类型以及每小时登录的用户数。





排除网关智能分析问题

April 23, 2021

如果网关智能分析解决方案无法按预期运行，则问题可能出在以下情况之一。请参阅相应部分中的清单以进行故障排除。

- 网关智能分析配置。
- Citrix ADC 和 Citrix ADM 之间的连接问题。
- 在 Citrix ADC 中生成记录。
- 在 Citrix ADM 中进行验证。

Gateway Insight 配置清单

- 确保 Citrix ADC 设备中启用了 AppFlow 功能。有关详细信息，请参阅启用 AppFlow。
- 检查 Citrix ADC 运行配置中的 Gateway Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查网关智能分析配置。确保绑定类型为请求。例如;

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type REQUEST
  2  <!--NeedCopy-->
  ```

  Gateway Insight 也需要绑定类型 OTHERTCP_REQUEST。

  ```
  1  bind vpn vserver afsanity -policy afp -priority 100 -type
     OTHERTCP_REQUEST
  2  <!--NeedCopy-->
  ```

- 对于单跳、接入网关或 Unified Gateway 部署，请确保网关智能分析 AppFlow 策略绑定到 VPN 虚拟服务器，其中 VPN 流量正在流动。有关详细信息，请参阅启用 HDX Insight 数据收集。

- 对于双跳，必须在两个跳上配置 Gateway Insight。
- 在 Citrix 网关 /VPN 虚拟服务器中检查 `appflowlog` 参数。有关详细信息，请参阅为虚拟服务器启用 AppFlow。

Citrix ADC 与 Citrix ADM 之间的连接检查表

- 检查 Citrix ADC 中的应用流收集器状态。有关详细信息，请参阅如何检查 Citrix ADC 和 AppFlow 收集器之间的连接状态。
- 检查 Gateway Insight AppFlow 策略命中。

  运行命令 `show appflow policy <policy_name>` 以检查 AppFlow 策略命中情况。

  您还可以导航到 GUI 中的 **“系统” > “AppFlow” > “**策略”，以检查 AppFlow 策略命中。
- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

Citrix ADC 核对清单中的记录生成

- 运行 `nsconmsg -d stats -g ai_tot` 命令并检查 Citrix ADC 中的统计数据增量。
- 捕获 `nstrace logs` 并检查 CFLOW 数据包以确认 Citrix ADC 导出 AppFlow 记录。

  > 注意：
  >
  > 只有 IPFIX 才需要使用 `nstrace logs`。对于 Logstream，nstrace 日志不确认 ADC 设备是否导出了 AppFlow 记录。

在 Citrix ADM 中验证记录

- 运行 `tail -f /var/mps/log/mps_afdecoder.log | grep -i "Data Record: vpn_"` 命令以检查日志以确认 Citrix ADM 正在接收 AppFlow 记录。
- 确保 Citrix ADC 实例已添加到 Citrix ADM。
- 确保 Citrix Gateway/VPN 虚拟服务器已在 Citrix ADM 中获得许可。

在 Citrix ADM 中验证 Logstream 日志

可以使用以下方法验证 Citrix ADM 接收的 Logstream 数据：

- 在 **Citrix ADM** 中启用数据记录记录

  启用后，可以在 /var/mps/log/mps_afdecoder.log 中看到日志
- 启用 **ULFD** 库日志记录

  运行以下命令 `/mps/decoder_enable_debug`

这些日志在 /var/ulflog/libulfd.log 中捕获

您可以使用 /mps/decoder_disable_debug 命令禁用日志记录

Gateway Insight 计数器

以下 Gateway Insight 计数器可用。

- ai_tot_preauth_epa_export
- ai_tot_auth_export
- ai_tot_auth_session_id_update_export
- ai_tot_postauth_epa_export
- ai_tot_vpn_update_export
- ai_tot_ica_fileinfo_export
- ai_tot_app_launch_failure
- ai_tot_logout_export
- ai_tot_skip_appflow_export
- ai_tot_sso_appflow_export
- ai_tot_authz_appflow_export
- ai_tot_appflow_pol_eval_failure
- ai_tot_vpn_export_state_mismatch
- ai_tot_appflow_disabled
- ai_ot_appflow_pol_eval_in_gwinsight
- ai_ot_app_launch_ 成功

Citrix ADC 日志中的 AppFlow 记录

从版本 13.0 版本开始，您可以检查 Citrix ADC 日志以确认 AppFlow 记录是否导出。默认日志级别 syslogparams 捕获所有错误和信息日志。如果找不到有关错误的线索，请启用包括 DEBUG 在 syslogparams 内的所有日志级别以捕获甚至 DEBUG 日志。

示例日志

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 147 0 : "
    GwInsight: Sent auth record Func=ns_sslvpn_export_auth_data Username
    =<name> Clientip=<ip>:<port> Destip=0:80 SessSeq=0 Sessid=<sessid>
    Gwip=<ip>:443 StatusCode=0 CSappid=0 CSAppname=(null) VPNfqdn=<
    vpnfqdn> Authtype=3 EPAid=(null) AuthStage=1 AuthDuration=309
    AuthAgent=<auth_server_ip> Groupname= Policyname=<name>
    CurfactorPolname=<name> NextfactorPolname= CSecExpr= Devicetype
    =16777219 Deviceid=0 email="
```



```
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 143 0 : "GwInsight
    : Func=ns_aaa_copy_email_id_to_vpn_record input hash_attrs_len is
    zero"
<local0.err> … GMT 0-PPE-0 : default SSLVPN Message 148 0 : "GwInsight
    : Func=update_session_appflow_collector pcb or session is NULL"
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 165 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<> Clientip=<ip>:<port> Destip
    =<ip>:80 SessSeq=1 Sessid=<sessid> Gwip=<ip>:443 StatusCode=0
    CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=0 SessState
    =2 SessMode=2 IIP=0 AppByteCount=0 ReqURL=/Citrix/Store
Web BackendServername= SSOurl= email="
SSO logs:
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 463 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=1
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 582 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=3
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 513 0 : "
    GwInsight: Sent session update record Func=
    ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
    Destip=<ip>:80 SessSeq=2 Sessid=<sessid> Gwip=<ip>:443 StatusCode
    =150 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=2
    SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
    BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

```
<local0.info> … GMT 0-PPE-0 : default SSLVPN Message 29796 0 : "
    GwInsight: Sent session update record Func=
```



```
      ns_sslvpn_send_update_record Username=<name> Clientip=<ip>:<port>
      Destip=<ip>:443 SessSeq=c Sessid=<sessid> Gwip=<ip>:443 StatusCode
      =155 CSappid=0 CSAppname=(null) VPNfqdn=<fqdn> SSOAuthMethod=6
      SessState=4 SessMode=3 IIP=0 AppByteCount=0 ReqURL=
      BackendServername=<> SSOurl= email="
<!--NeedCopy-->
```

联系 **Citrix** 技术支持

为了快速解决问题，请确保在联系 Citrix 技术支持之前具有以下信息：

- 部署和网络拓扑的详细信息。
- Citrix ADC 和 Citrix ADM 版本。
- 适用于 Citrix ADC 和 Citrix ADM 的技术支持包。
- `nstrace` 在问题期间捕获。

已知问题

有关网关智能分析的已知问题，请参阅 Citrix ADC 发行说明。

Security Insight

April 23, 2021

> 注意
>
> 如果 Citrix ADM 版本早于 **13.0-79.x**，则可以通过导航至 **Analytics** > 安全性 > 安全洞察来查看安全洞察。对于版本 **13.0-79.x** 或更高版本，您可以导航到 **Analytics** > 安全性 > 安全违规 > 应用程序概述，然后单击应用程序细分依据下的 ****WAF**** ，查看 WAF 违规详细 ** 信息。

面向 Internet 的 Web 和 Web 服务应用程序越来越易受攻击。为了保护应用程序不受攻击，需要了解过去、现在及将来的威胁的本质和范围、有关攻击的实时可操作数据以及有关防范措施的建议。Security Insight 提供单窗格解决方案来帮助您评估应用程序安全状态，并采取更正措施来保护应用程序的安全。

> 注意
>
> Citrix Application Delivery Management (ADM) 支持安全洞察，Citrix ADC 设备在版本 11.0 版本 65.31 及更高版本上运行。

安全洞察的工作原理

Security Insight 是基于控制板的直观安全分析解决方案，让您可以完全了解与应用程序关联的威胁环境。安全洞察包含在 Citrix ADM 中，并根据您的应用程序防火墙和 Citrix ADC 系统安全配置定期生成报告。报告包含每个应用程序的

以下信息：

- 威胁指数。一个单位数评级系统，指示应用程序攻击的严重程度，无论应用程序是否受到 Citrix ADC 设备的保护。应用程序上的攻击越严重，该应用程序的威胁指数越高。值的范围是 1 到 7。

  威胁指数基于攻击信息。攻击相关的信息（例如，违反类型、攻击类别、位置和客户端详细信息）让您可以了解应用程序上的攻击。只有在发生违规或攻击时，才会向 Citrix ADM 发送违规信息。许多漏洞和漏洞导致了高威胁指数值。

- 安全指数。一个单位数评级系统，用于指示您配置 Citrix ADC 实例以保护应用程序免受外部威胁和漏洞的安全性。应用程序的安全风险越低，安全指数越高。值的范围是 1 到 7。

  安全指标同时考虑应用程序防火墙配置和 Citrix ADC 系统安全配置。为了获得较高的安全指数值，两个配置都必须强健。例如，如果进行了严格的应用程序防火墙检查，但尚未采用 Citrix ADC 系统安全措施（例如 `nsroot` 用户的强密码），则应用程序将被分配一个较低的安全指数值。

- 可操作信息。降低威胁指数和提高安全指数所需的信息，从而显著提高了应用程序的安全性。例如，可以查看有关违反、应用程序防火墙和其他安全功能的现有和缺少的安全配置以及应用程序被攻击速率等的信息。

配置安全智能分析

Citrix ADM 支持来自所有已配置应用程序防火墙的 Citrix ADC 实例的安全智能分析。

要在 ADC 实例上配置安全洞察，请首先配置应用程序防火墙配置文件和应用程序防火墙策略。尽管随后可以在全局范围内绑定应用程序防火墙策略，但 Citrix 建议将该策略绑定到虚拟服务器。

要查看 Citrix ADM 上的分析，请在实例上启用 AppFlow 功能，配置 AppFlow 收集器、操作和策略，并在全局范围内绑定策略。此外，尽管您随后可以在全局范围内绑定应用程序防火墙策略，但 Citrix 建议将该策略绑定到虚拟服务器。Citrix 还建议您使用 Citrix ADM 在 ADC 实例上部署 AppFlow 配置。配置收集器时，必须指定要在其上监视报表的 Citrix ADM 服务器的 IP 地址。

要在 **Citrix ADC** 实例上配置安全洞察，请执行以下操作：

1. 运行以下命令来配置应用程序防火墙配置文件和策略，并全局绑定应用程序防火墙策略，或将应用程序防火墙策略绑定到负载平衡虚拟服务器。

   添加 **appfw** 配置文件 <name> [**-**默认值（基本 | 高级）]

   设置应用程序配置文件 <name> [**-**启动动作 <startURLAction>…]

   添加应用程序策略 <name> <rule> <profileName>

   绑定应用程序全局 <policyName> <priority>

   或者，

   绑定 **lb** 虚拟服务器 <lb vserver> **-**策略名称 <policy> **-**优先级 <priority>

   ```
   add appfw profile pr_appfw -defaults advanced
   set  appfw profile pr_appfw -startURLaction log stats learn
   ```



```
add appfw policy pr_appfw_pol "HTTP.REQ.HEADER("Host").EXISTS"
    pr_appfw
bind appfw global pr_appfw_pol 1
or,
bind lb vserver outlook  - policyName pr_appfw_pol  - priority  “20
    ”
<!--NeedCopy-->
```

2. 运行以下命令来启用 AppFlow 功能、配置 AppFlow 收集器、操作及策略，并全局绑定策略，或将策略绑定到负载平衡虚拟服务器：

   添加应用程序流收集器 <name> **-IP** 地址 <ipaddress>

   设置应用程序流参数 [**-**安全见解记录间隔 <secs>] [**-**安全见解流量 (已启用) | DISABLED)]

   添加应用程序流操作 <name> **-**收集器 <string>

   add appflow policy <name> <rule> <action>

   bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

   或者，

   绑定 **lb** 虚拟服务器 <vserver> **-**策略名称 <policy> **-**优先级 <priority>

```
add appflow collector col -IPAddress 10.102.63.85
set appflow param  -SecurityInsightRecordInterval 600 -
    SecurityInsightTraffic ENABLED
add appflow action act1 -collectors col
add appflow action af_action_Sap_10.102.63.85 -collectors col
add appflow policy pol1 true act1
add appflow policy af_policy_Sap_10.102.63.85 true
    af_action_Sap_10.102.63.85
bind appflow global pol1 1 END -type REQ_DEFAULT
or,
bind lb vserver Sap  - policyName af_action_Sap_10.102.63.85  -
    priority  “20”
<!--NeedCopy-->
```

要从 **Citrix ADM** 启用安全洞察，请执行以下操作：

如果您的 Citrix ADM 是 **13.0** 版本 **41.x** 版本：

1. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC**”，然后选择实例类型。例如，VPX。
2. 选择实例，然后从 “ 选择操作” 列表中单击 “ 配置分析”。
3. 在 “在 虚拟服务器上配置分析” 页上，选择虚拟服务器，然后单击 启用分析。
4. 在 启用分析窗口中：

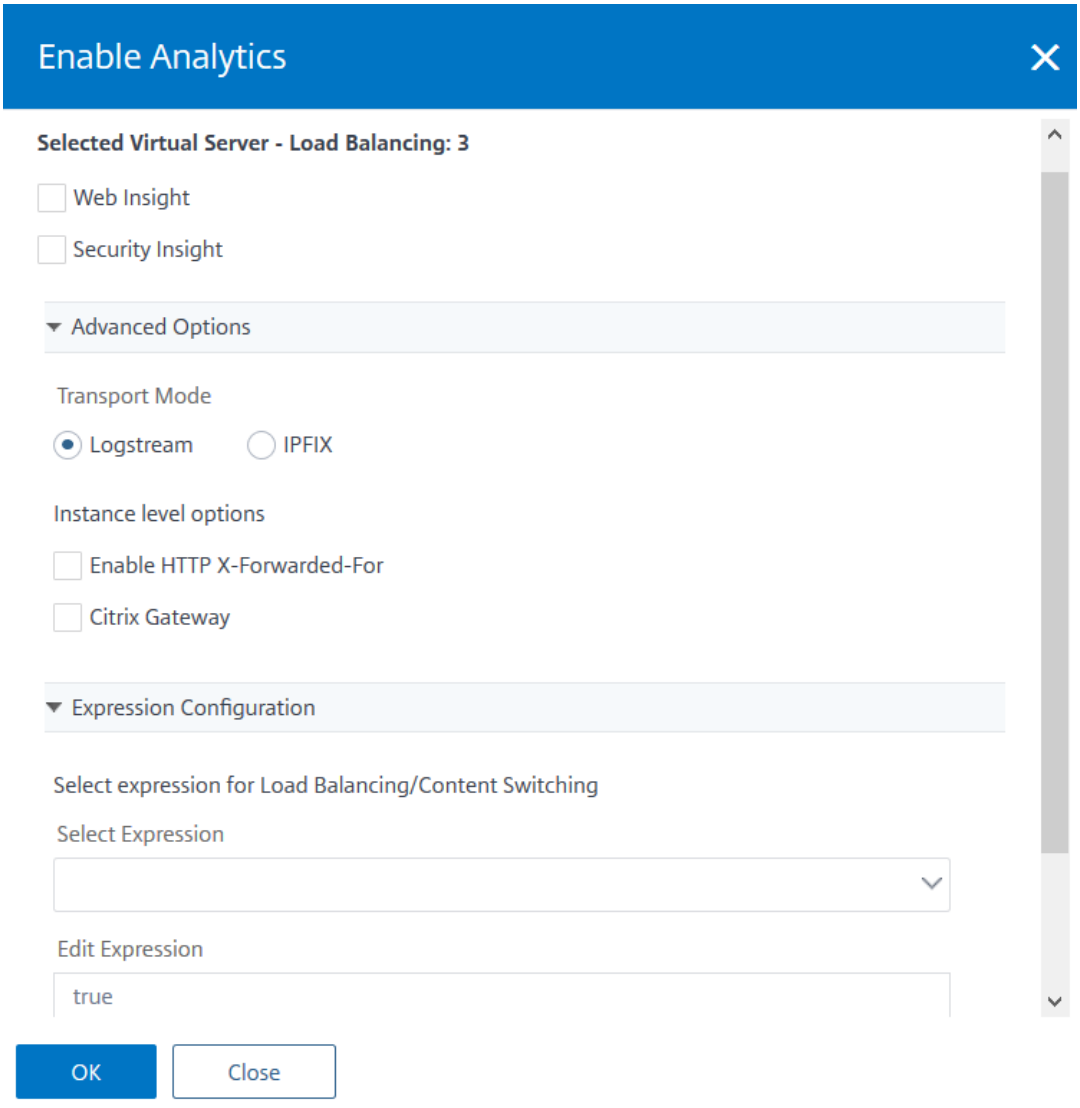
a) 选择 **Security Insight**

b) 选择 **Logstream** 作为传输模式

> 注意
>
> 对于 Citrix ADC 12.0 或更低版本，**IPFIX** 是传输模式的默认选项。对于 Citrix ADC 12.0 或更高版本，您可以选择日志流或 **IPFIX** 作为传输模式。
>
> 有关 IPFIX 和日志流的详细信息，请参阅 日志流概述。

c) 默认情况下，表达式为 true

d) 单击 **OK**（确定）

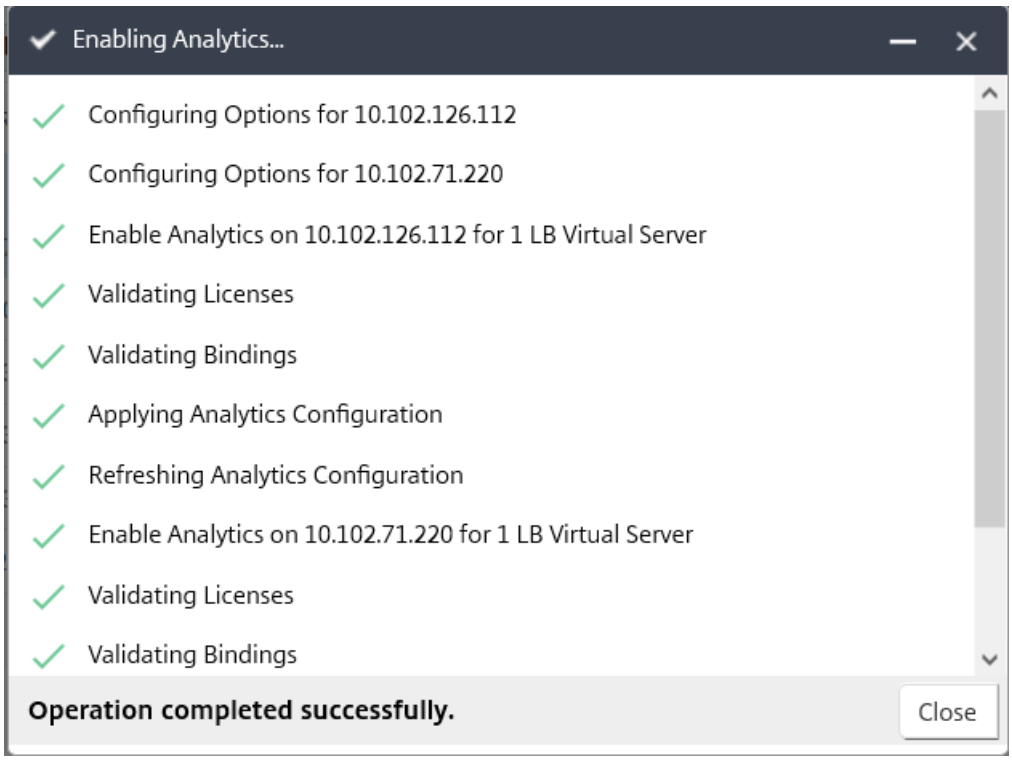


> 注意
>
> ```
> 1    - 如果选择未获得许可的虚拟服务器，则 Citrix ADM 首先
> ```



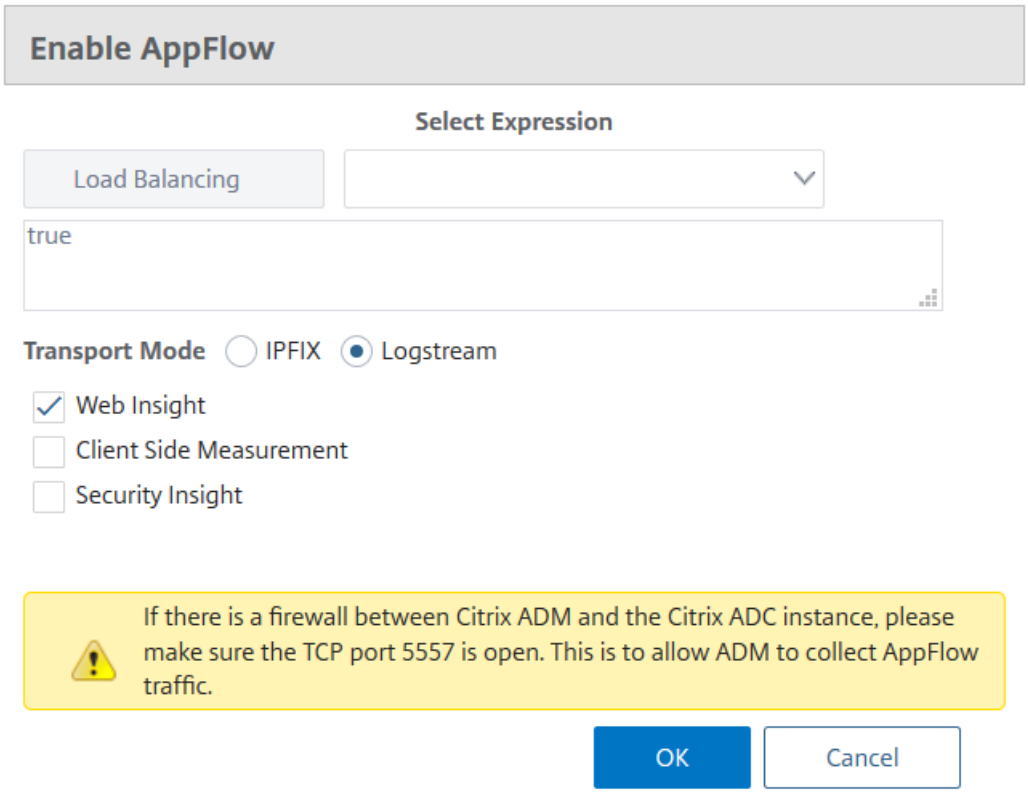
```
        许可这些虚拟服务器，然后启用分析
2
3       - 对于管理员分区，只支持 **Web Insight**
4
5       - 对于缓存重定向、身份验证和 GSLB 等虚拟服务器，您无
          法启用分析。将显示一条错误消息。
```

单击 确定”后，Citrix ADM 将处理在所选虚拟服务器上启用分析。



如果您的 Citrix ADM 是 **13.0** 版本 **36.27**:

1. 导航到 “ 网络” > “ 实例”，然后选择要启用 AppFlow 的 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。
3. 选择虚拟服务器，然后单击 启用 **AppFlow**。
4. 在 “ 启用 **AppFlow** ” 字段中，键入 **true**，然后选择 “ 安全智能分析”。
5. 单击 “ 确定”。



> 注意：
>
> 创建组时，您可以将角色分配给组，提供对组的应用程序级访问权限，并将用户分配到组。Citrix ADM 分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有关组和向组分配用户的详细信息，请参阅 配置组。

查看安全智能分析报告的地理位置

安全智能分析报告包括客户端请求源自的确切地理位置。您可以查看 Citrix ADM 中的地理位置。Citrix ADC 中内置的地理数据库文件包含大多数公有 IP 地址。该文件位于 Citrix ADC 中的位置 /变量/网络扩展器/内置数据库处。

要启用地理位置，请执行以下操作：

运行以下命令以启用地理位置日志记录及采用 CEF 格式的日志记录：

- 添加位置文件 <Complete path with the DB filename>
- **set appfw settings -geoLocationLogging ON**
- **set appfw settings -CEFLogging ON**

如果地理数据库文件中没有任何 IP 地址，则可以添加该地理位置的 IP 地址。除 IP 地址外，您还可以添加城市/州/国家/地区名称以及每个位置的纬度和经度坐标。

使用文本编辑器（如 vi 编辑器）打开 geo 数据库文件，并为每个位置添加一个条目。

该条目必须采用以下格式：


```
\<start IP\>,\<end IP\>,,\<country\>,\<state\>,,\<city\>,,longitude,latitude
```

例如，

```
4.17.142.224,4.17.142.239,,US,New York,,Harrison,,73.7304,41.0568
<!--NeedCopy-->
```

知识产权信誉

可以使用 NetScaler Insight Center 来监视和管理您的传入流量的 IP 信誉。可以配置策略以将更多 IP 添加为恶意 IP，并创建自定义的阻止列表。

要了解有关配置和使用 IP 信誉的信息，请参阅 IP 信誉。

监控 **IP** 信誉

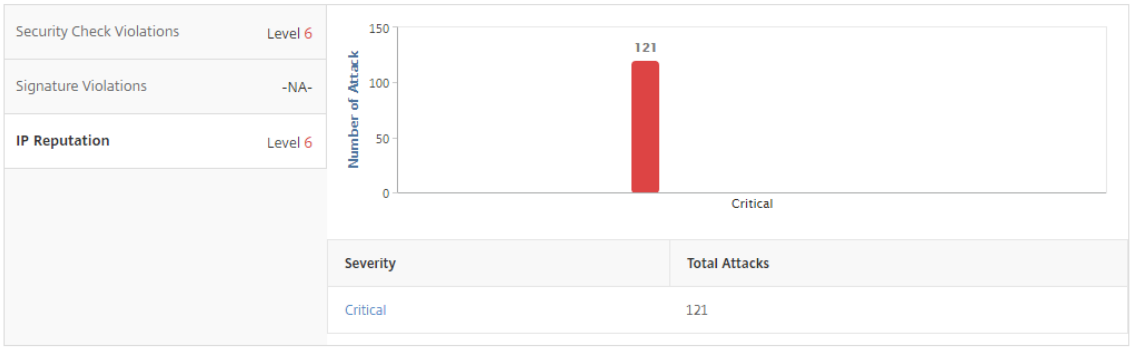
IP 信誉功能提供有关恶意 IP 地址的攻击相关信息。例如，它报告有关客户端 IP 地址的 IP 信誉分数、IP 信誉类别、IP 信誉攻击时间、设备 IP 及详细信息。

IP 信誉分数指示与 IP 地址关联的风险。该分数范围如下：

IP 信誉分数	风险级别
1–20	高风险
21–40	可疑
41–60	中等风险
61–80	低风险
81–100	可信

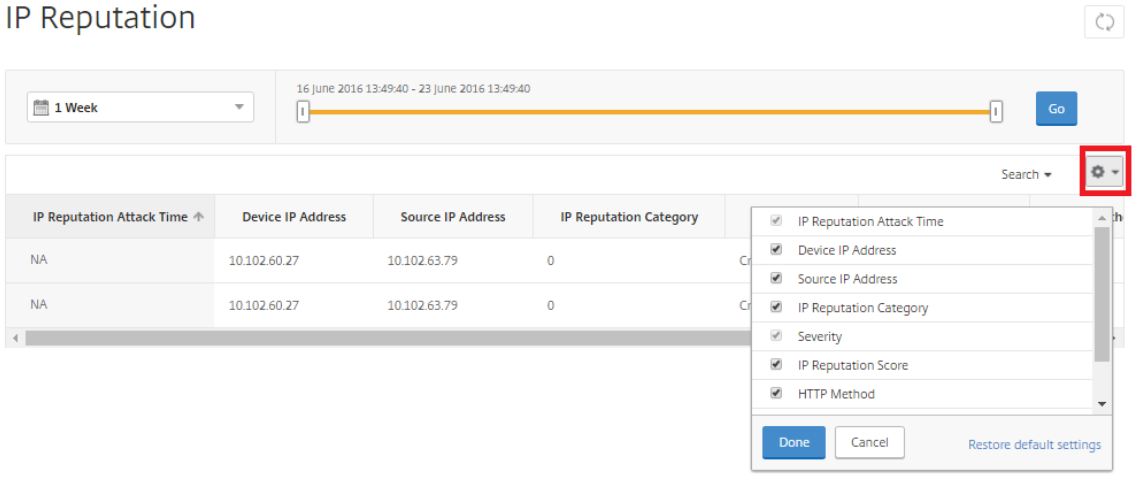
要监视 **IP** 信誉，请执行以下操作：

1. 导航到 “ 分析” > “ 安全智能分析”，然后选择要监视的应用程序。
2. 在威胁索引选项卡中，选择 **IP** 信誉。



3. 选择严重性以显示该级别的攻击的更多详细信息。您可以单击条形图或图表下方的表格中。
4. 选择要查看详细信息的时间段。可以使用时间滑块来进一步自定义所选时间段。然后，单击 **Go**（继续）。

5. 要自定义显示，请单击设置按钮。



阈值

您可以设置应用程序的安全指数和威胁指数的阈值，以及在 Security Insight 中查看这些阈值。

要设置阈值，请执行以下操作：

1. 导航至 “ 分析” > “ 设置” > “ 阈值”，然后选择 “ 添加”。

2. 在“流量类型”字段中选择 通信类型作为 安全性，并在其他相应字段（如名称、持续时间和实体）中输入所需信息。
3. 在“ 配置规则”部分中，使用“度量”、“比较器”和“值”字段来设置阈值。

   例如，“Threat Index”（威胁指数）“>”“5”
4. 在“通 知设置”中，选择通知类型。
5. 单击创建。

要查看违反阈值，请执行以下操作：

1. 导航到“ 分析”>“ 安全智能分析”>“ 设备”，然后选择 Citrix ADC 实例。
2. 在“ 应用程序”部分，您可以在“阈值违规”列中查看每个虚拟服务器发生的 阈值违规次数。

安全洞察使用案例

以下用例说明了如何使用 Security Insight 来评估应用程序面临的威胁以及改进安全措施。

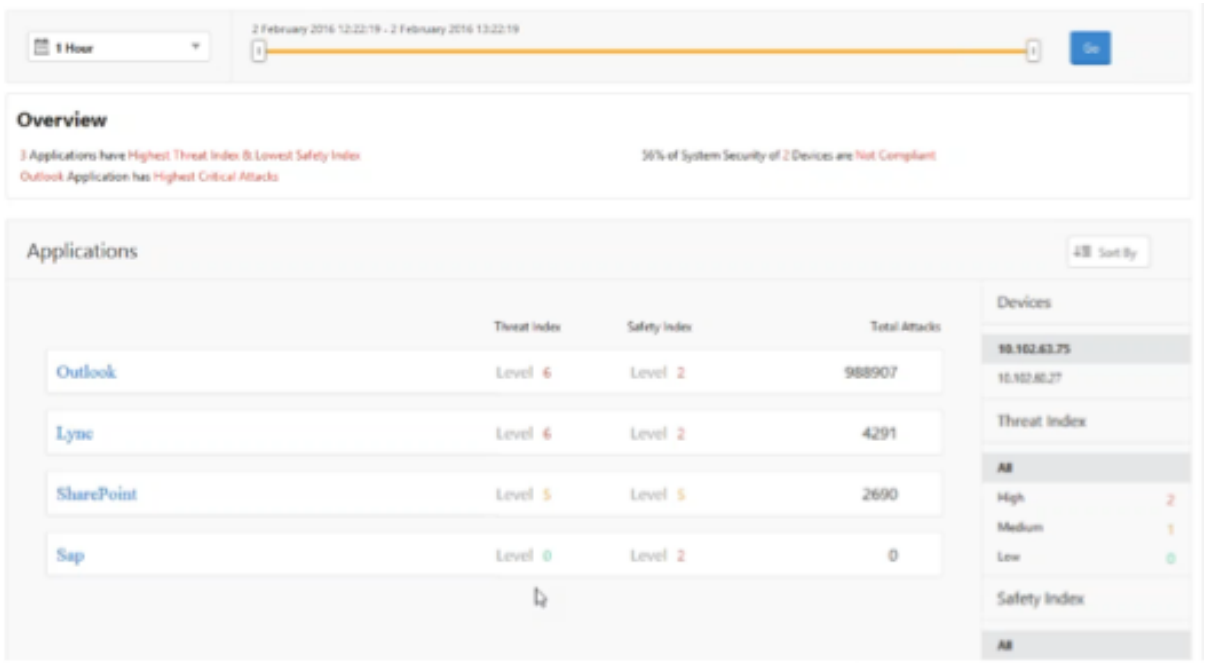
获取有关威胁环境的概述

在此使用案例中，您有一组可能遭受攻击的应用程序，并且您已将 Citrix ADM 配置为监视威胁环境。需要频繁查看应用程序可能经受的任何攻击的威胁指数、安全指数以及类型和严重性，以便可以首先关注最需要注意的应用程序。安全洞察仪表板提供了应用程序在您选择的一段时间内以及所选 Citrix ADC 设备所遇到的威胁的摘要。它显示应用程序列表、它们的威胁指数和安全指数以及在所选时间段的攻击总数。

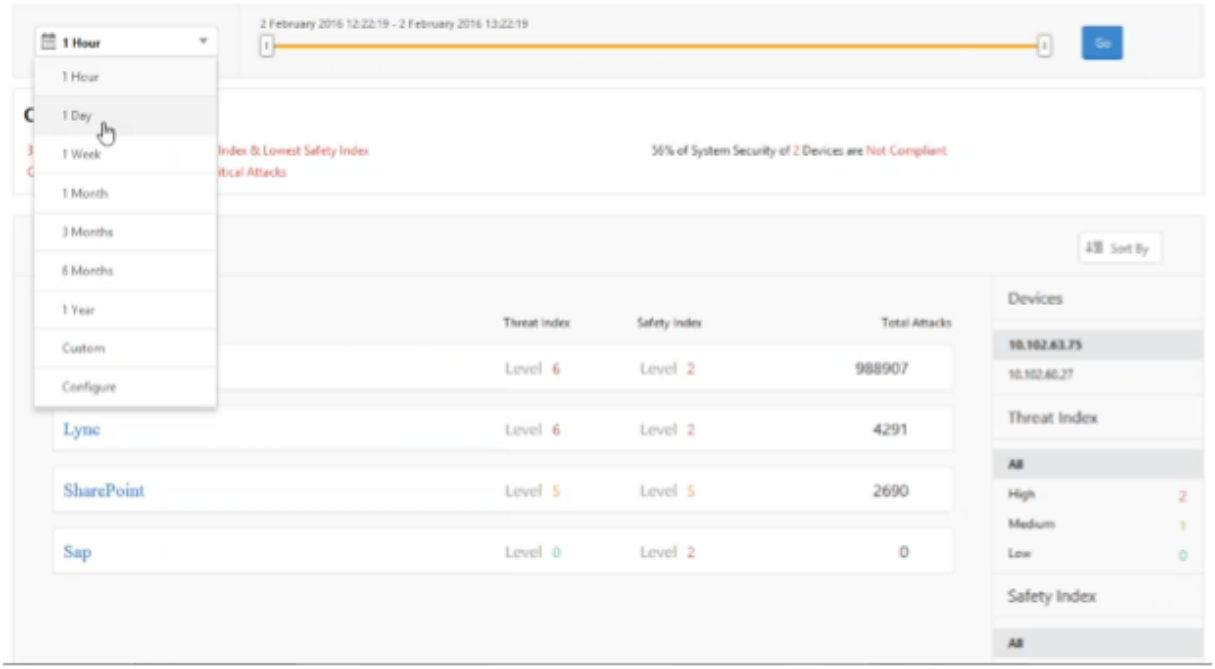
例如，你可能正在监视 Microsoft Outlook、Microsoft Lync、SharePoint 和 SAP 应用程序，你可能需要查看这些应用程序的威胁环境摘要。

要获取威胁环境的摘要，请登录到 **Citrix ADM**，然后导航到 **“**分析**” > “**安全智能分析**”**。

此时将显示每个应用程序的主要信息。默认时间段是 1 小时。



要查看不同时段的信息，请从左上角的列表中选择一个时段。



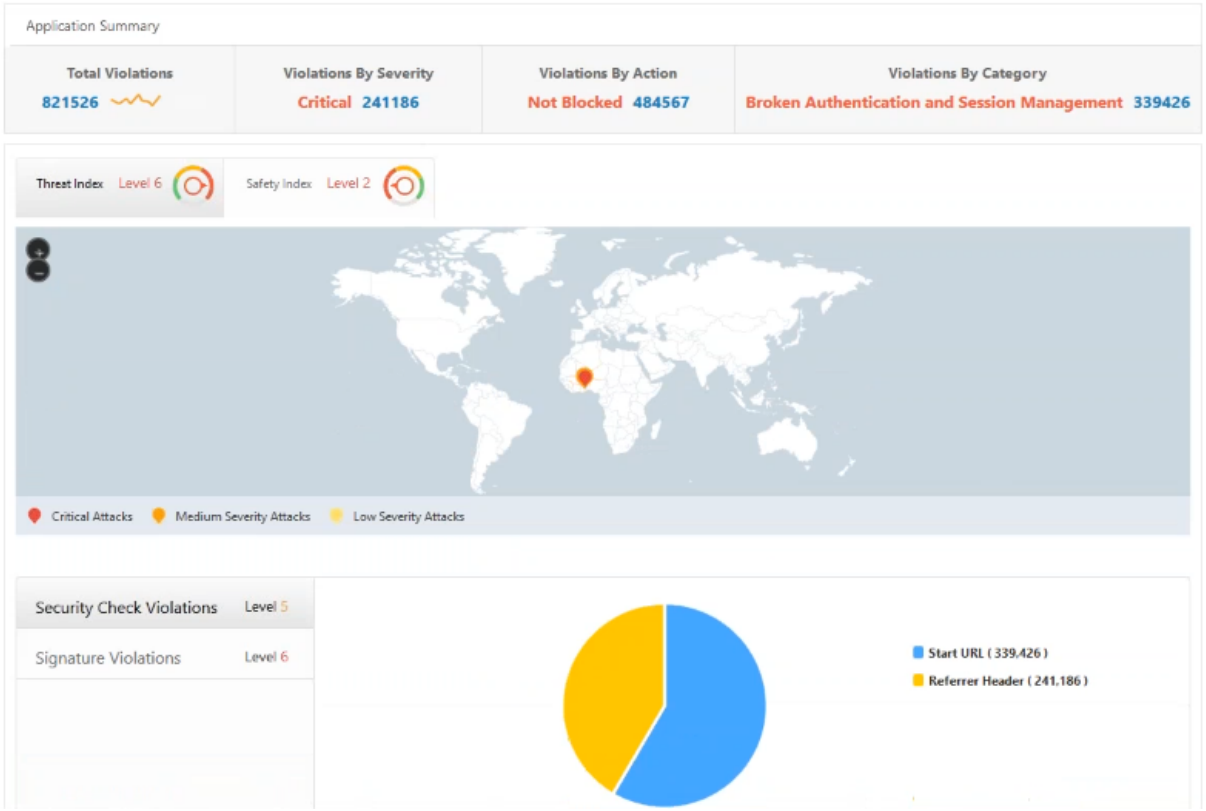
要查看其他 Citrix ADC 实例的摘要，请在“ 设备”下单击 Citrix ADC 实例的 IP 地址。要按给定列对应用程序列表排序，请单击列标题。

确定应用程序的威胁风险

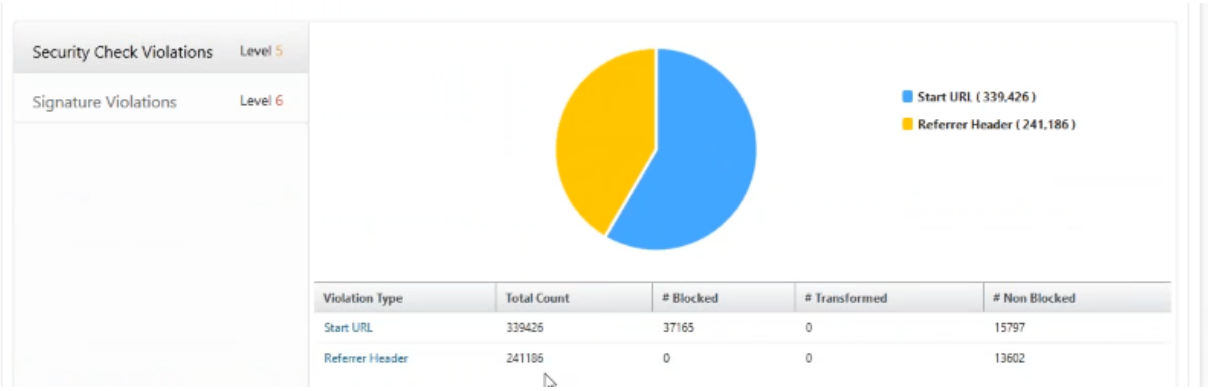
要在“安全智能分析”仪表板上识别具有高威胁指数和低安全指数的应用程序，您希望在决定保护这些威胁风险之前确定威胁风险。即，您希望确定降低了其指数值的攻击的类型和严重性。可以通过查看应用程序摘要来确定应用程序面临的威胁。

在此示例中，Microsoft Outlook 的威胁指数值是 6，您希望知道哪些因素导致此高威胁指数。

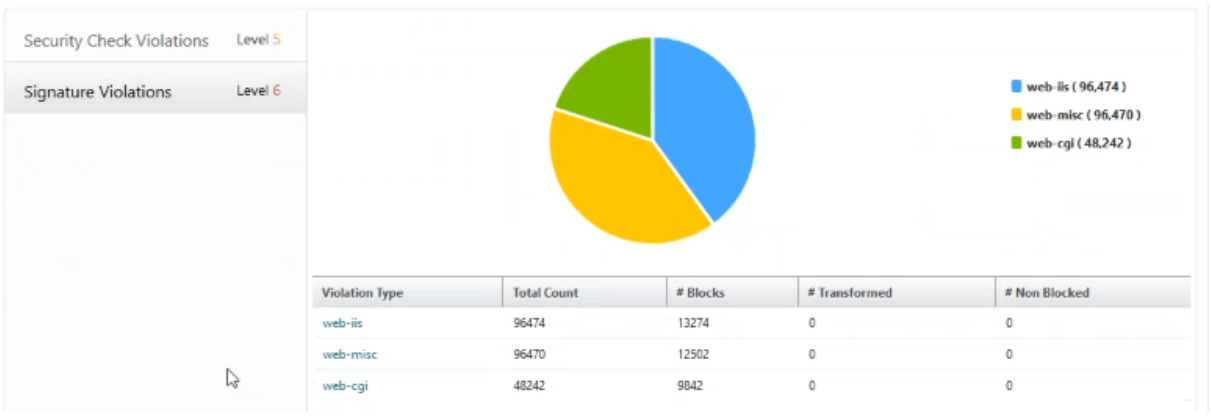
要确定 Microsoft Outlook 面临的威胁，请在 **Security Insight**（安全见解）控制板上，单击 **Outlook**。应用程序摘要包含标识服务器地理位置的地图。



单击 **Threat Index**（威胁指数）**> Security Check Violations**（安全检查违反），并查看显示的违反信息。



单击 签名违规并查看显示的违规信息。

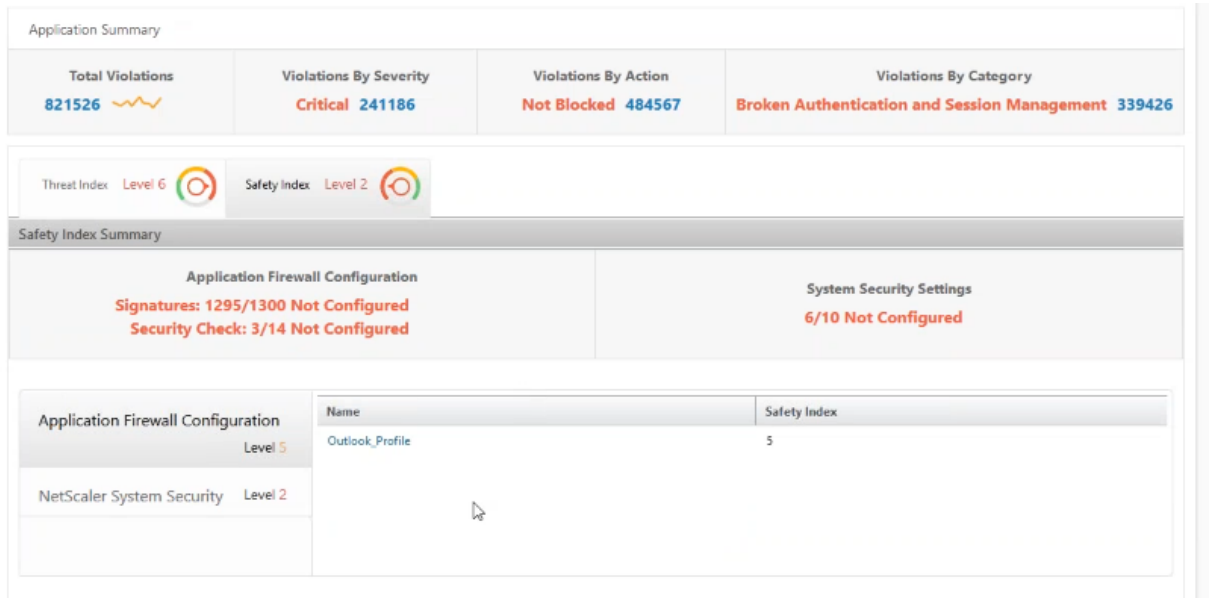


确定应用程序的现有和缺少的安全配置

查看了应用程序面临的威胁后，您希望确定哪些应用程序安全配置正在实施，以及该应用程序缺少哪些配置。可以深度查看应用程序的安全指数摘要来获取此信息。

安全指数摘要为您提供有关以下安全配置的有效性：

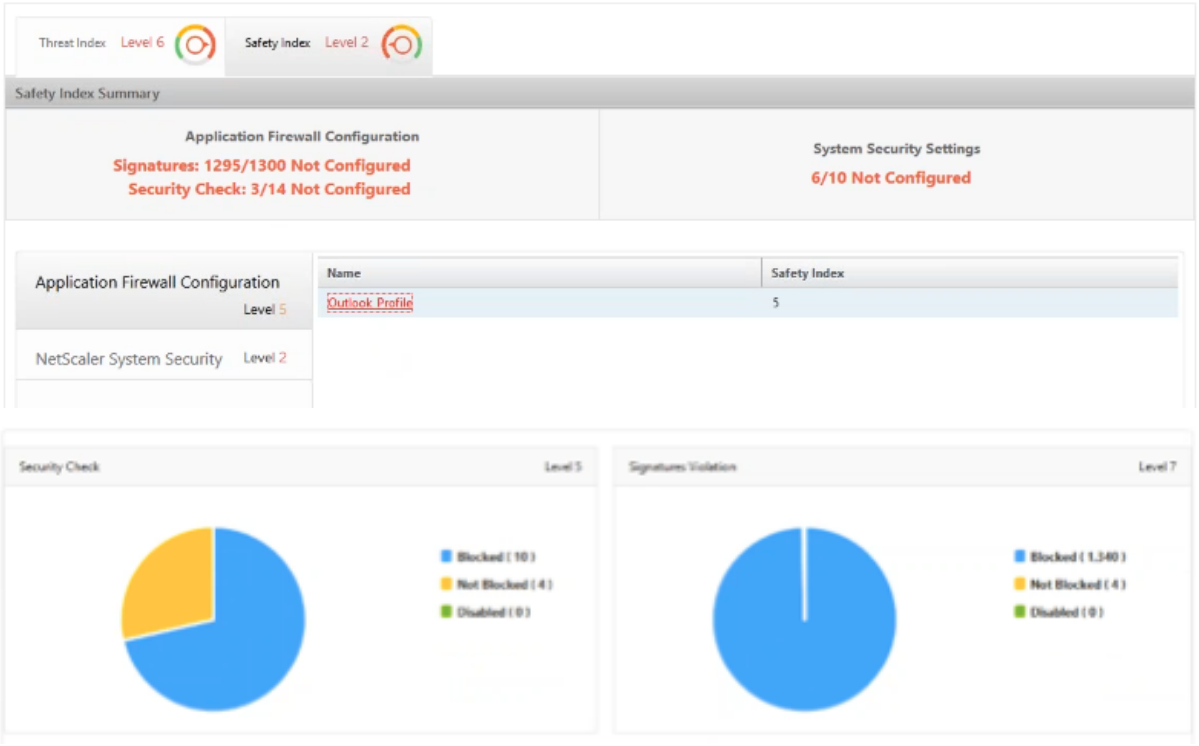
- 应用程序防火墙配置。显示多少签名和安全实体未配置。
- **NetScaler** 系统安全。显示多少系统安全设置未配置。



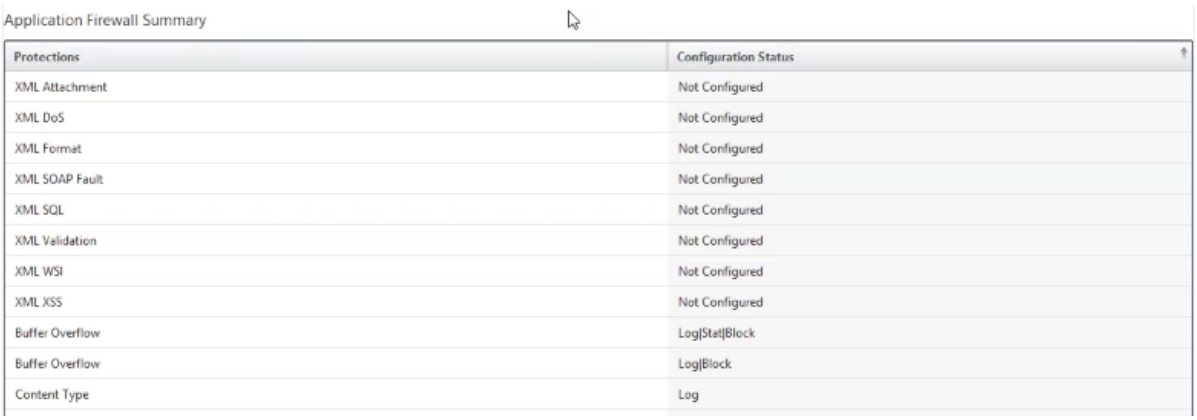
在之前的用例中，您查看了 Microsoft Outlook 面临的威胁，它的威胁指数值为 6。现在，您希望知道 Outlook 有哪些安全配置正在实施，以及可以添加哪些配置来改进其威胁指数。

在 **Security Insight**（安全见解）控制板上，单击 **Outlook**，然后单击 **Safety Index**（安全指数）选项卡。查看 **Safety Index Summary**（安全指数摘要）区域提供的信息。

在 **Application Firewall Configuration**（应用程序防火墙配置）节点上，单击 **Outlook_Profile** 并查看饼图中的安全检查和签名违反信息。



查看应用程序防火墙摘要表中每个保护类型的配置状态。要按列对表排序，请单击列标题。

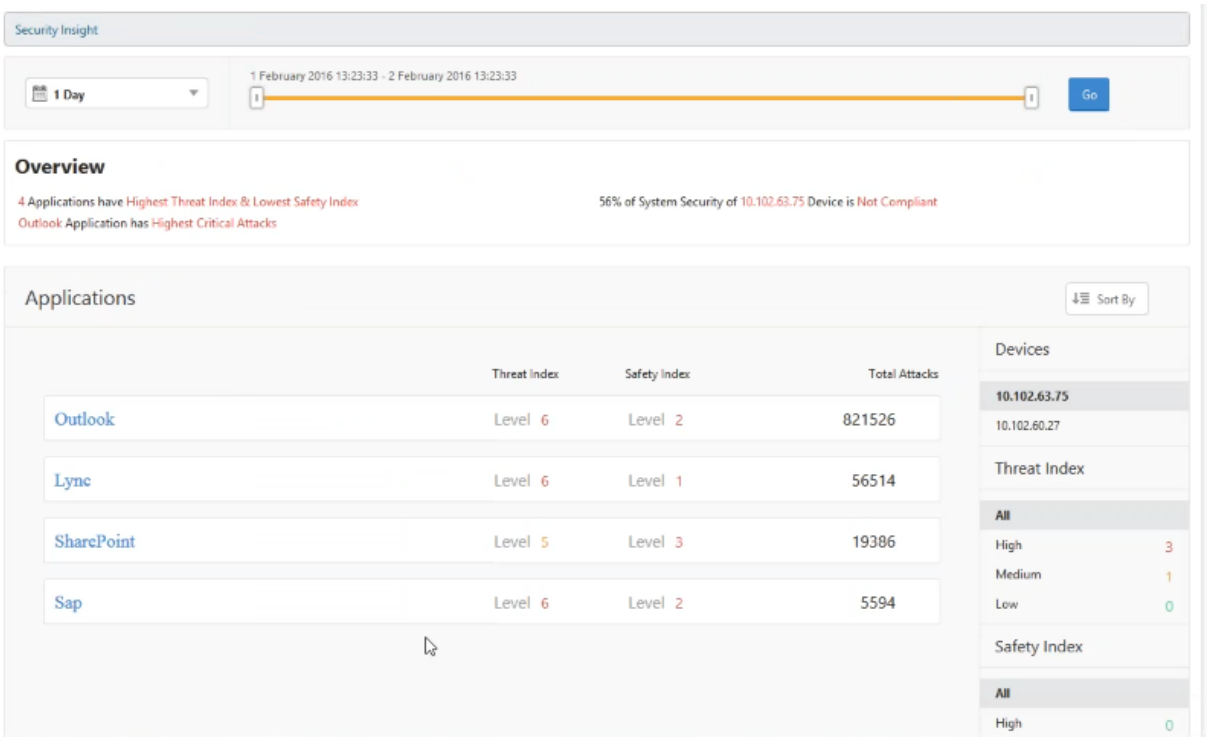


单击 **NetScaler System Security**（NetScaler 系统安全）节点，并查看系统安全设置和 Citrix 建议以改进应用程序安全指数。

确定需要立即关注的应用程序

需要立即注意的应用程序是那些具有较高威胁指数和较低安全指数的应用程序。

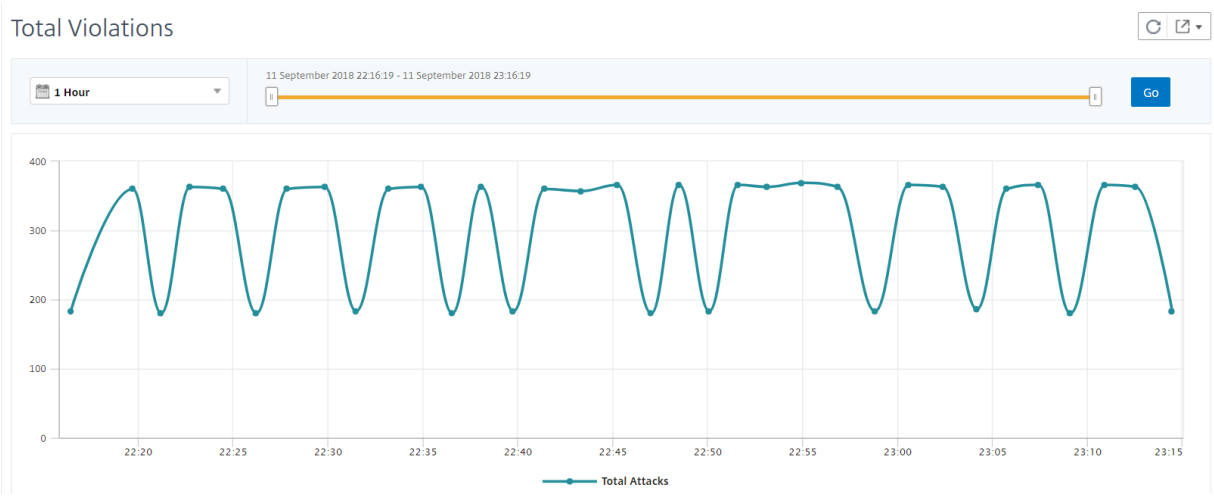
在此示例中，Microsoft Outlook 和 Microsoft Lync 都具有较高威胁指数值 6，但在两个安全指数中，Lync 的安全指数较低。因此，可能必须先将注意力放在 Lync 上，然后再改进 Outlook 的威胁环境。



确定给定时间内的攻击次数

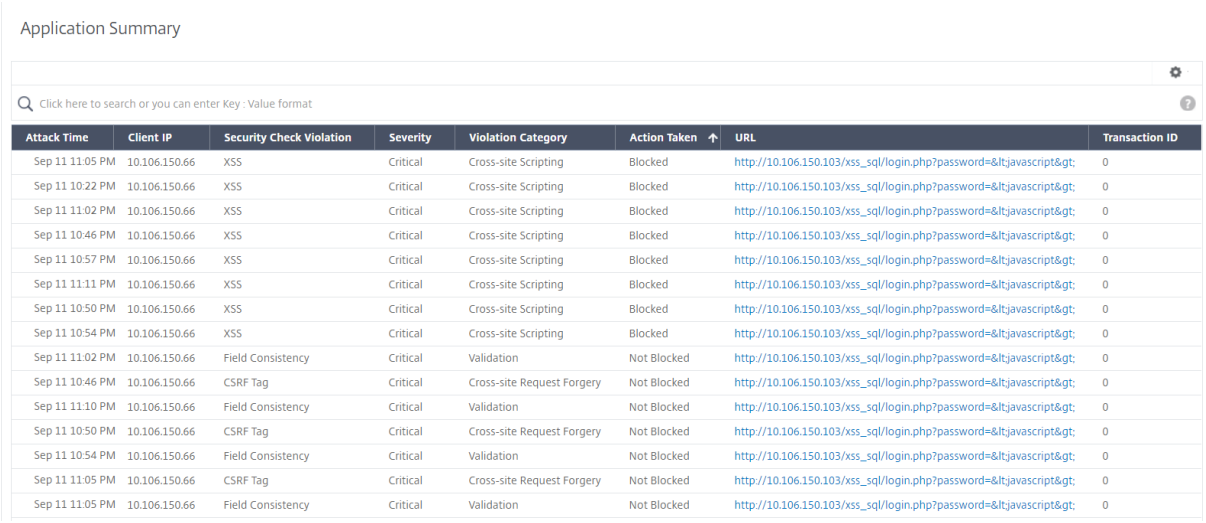
您可能希望确定在给定时间点给定应用程序上发生了多少攻击，或者您可能希望研究特定时间段的攻击速率。

在 **Security Insight** 页面上，单击任何应用程序，然后在 应用程序摘要中单击违规数量。“违规总数”页面以图形方式显示攻击时间为 1 小时、1 天、1 周和 1 个月。



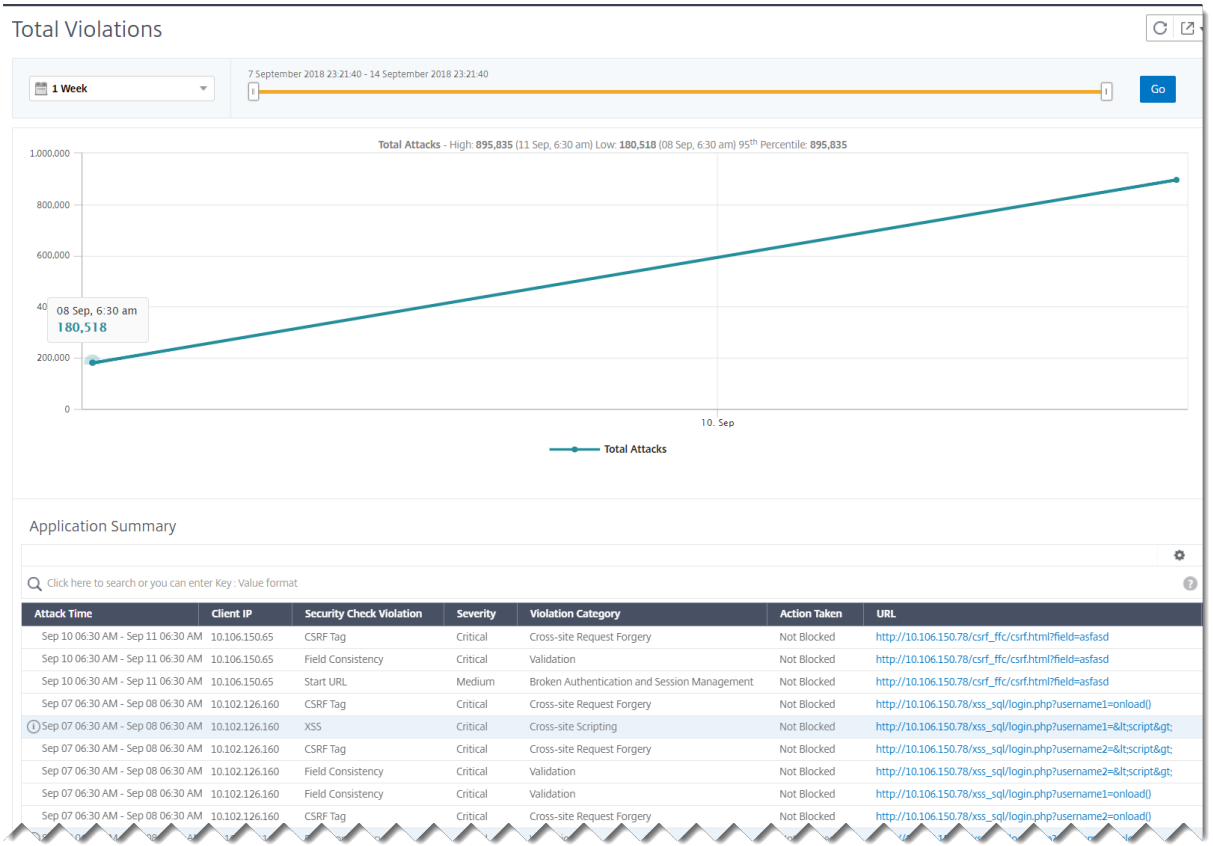
“应用程序摘要”表提供了有关攻击的详细信息。其中一些内容如下：

- 攻击时间
- 发生攻击的客户端的 IP 地址
- 严重性
- 违反行为的类别
- 发起攻击的 URL 以及其他详细信息。



Attack Time	Client IP	Security Check Violation	Severity	Violation Category	Action Taken	URL	Transaction ID
Sep 11 11:05 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:22 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:57 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:11 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	XSS	Critical	Cross-site Scripting	Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:02 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:46 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:10 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:50 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 10:54 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	CSRF Tag	Critical	Cross-site Request Forgery	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0
Sep 11 11:05 PM	10.106.150.66	Field Consistency	Critical	Validation	Not Blocked	http://10.106.150.103/xss_sql/login.php?password=<javascript>	0

虽然您始终可以在每小时报告中查看攻击时间（如图所示），但现在您可以查看聚合报告的攻击时间范围，即使是每日或每周报告也是如此。如果您从时间段列表中选择“1 天”，安全智能分析报告将显示所有已聚合的攻击，攻击时间显示在 1 小时范围内。如果您选择“1 周”或“1 个月”，则所有攻击将被汇总，攻击时间显示在一天范围内。

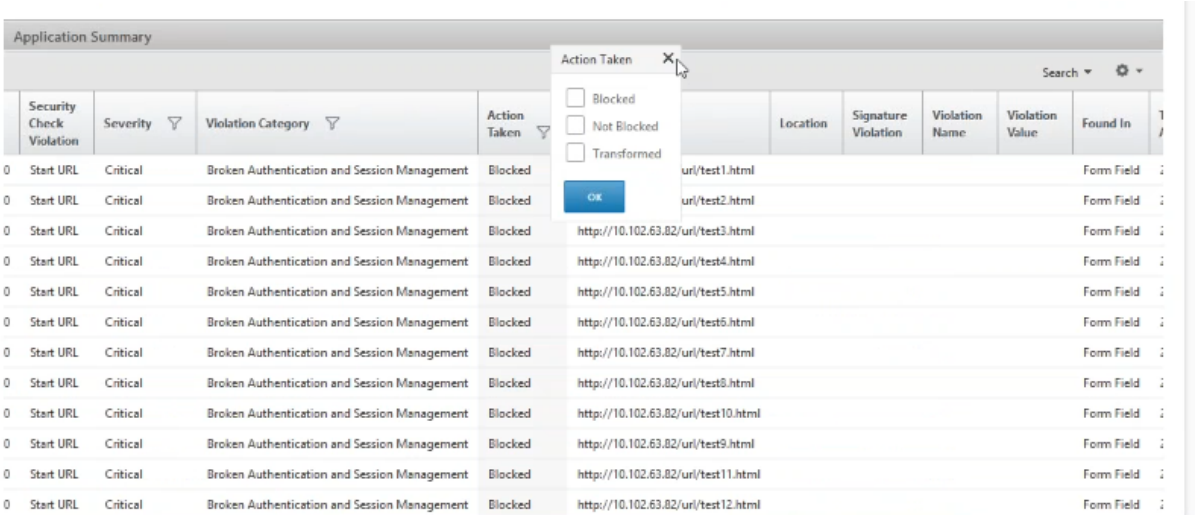


获取有关安全漏洞的详细信息

您可能希望查看应用程序攻击的列表，并深入了解攻击的类型和严重性、Citrix ADC 实例采取的操作、请求的资源以及攻击的来源。

例如，您可能希望确定 Microsoft Lync 上多少攻击被阻止了、请求了什么资源以及来源的 IP 地址。

在 安全智能分析仪表板上，单击 **Lync >** 总违规。在表中，单击 **Action Taken**（采取的操作）列标题中的过滤器图标，然后选择 **Blocked**（被阻止）。



有关请求的资源的信息，请查看 **URL** 列。有关攻击来源的信息，请查看 **Client IP**（客户端 IP）列。

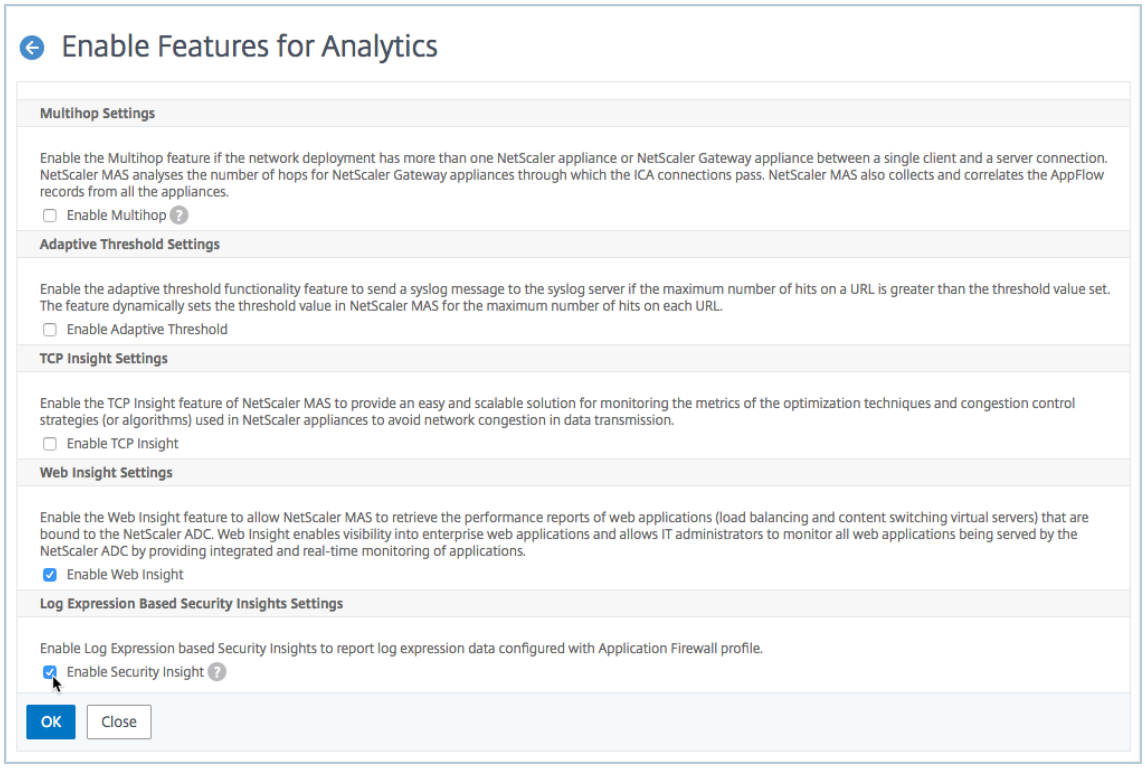
查看日志表达式详细信息

Citrix ADC 实例使用配置为“应用程序防火墙”配置文件的日志表达式对企业中应用程序的攻击采取措施。在安全智能分析中，您可以查看为 Citrix ADC 实例使用的日志表达式返回的值。这些值包括请求标头、请求正文等。除了日志表达式值之外，您还可以查看日志表达式名称和在应用程序防火墙配置文件中定义的日志表达式的注释，Citrix ADC 实例用于对攻击执行操作。

必备条件

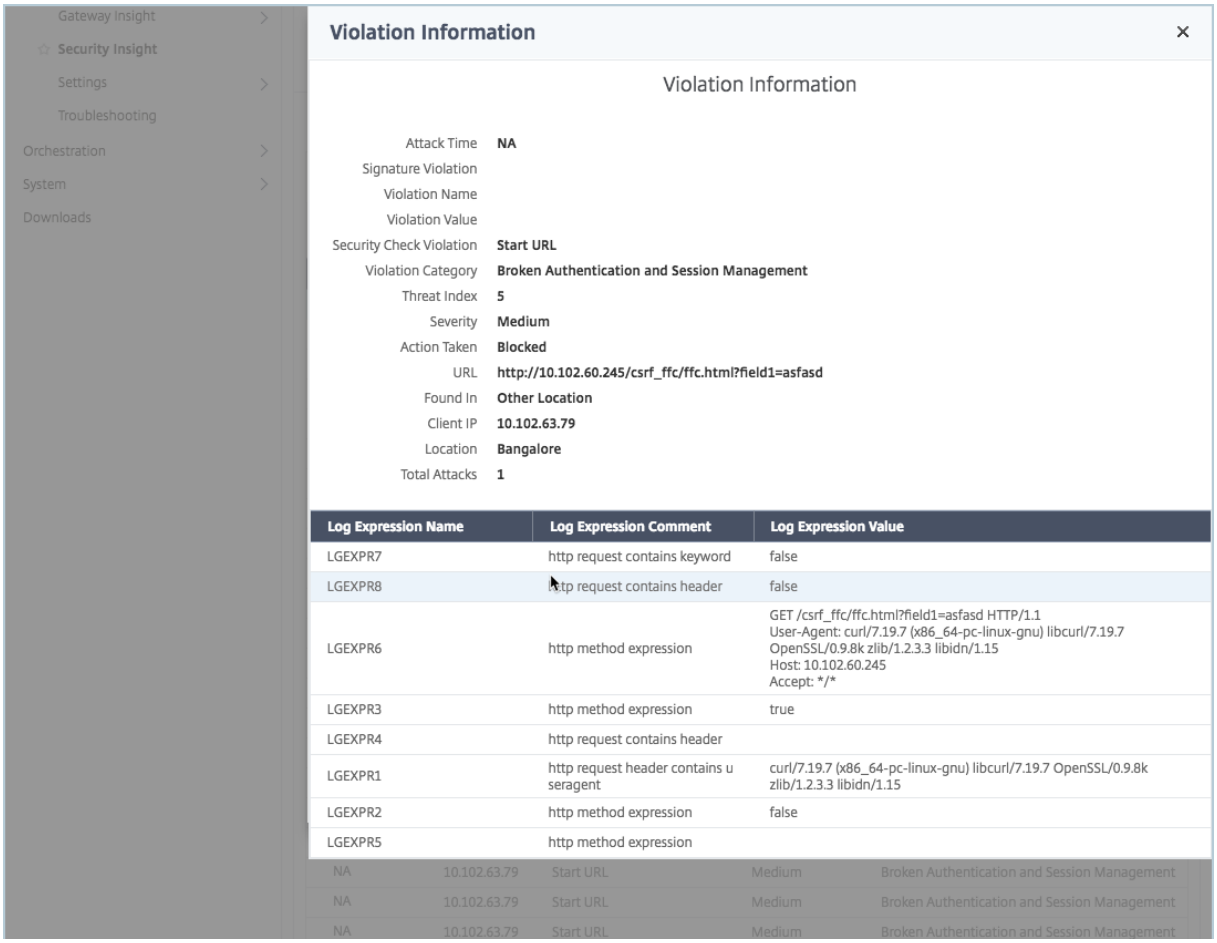
确保您：

- 在应用程序防火墙配置文件中配置日志表达式。有关详细信息，请参阅应用程序防火墙。
- 在 Citrix ADM 中启用基于日志表达式的安全见解设置。请执行以下操作：
  1. 导航到 **Analytics >** 设置，然后单击 启用分析功能。
  2. 在“启用分析功能”页中，选择“ 基于日志表达式的安全智能分析设置”部分下的“启用安全智能分析”，然后单 击 **“**确定”。



例如，您可能希望查看由 Citrix ADC 实例返回的日志表达式的值，用于针对企业中的 Microsoft Lync 攻击采取的操作。

在安全智能分析控制板上，导航到 **Lync >** 总冲突。在 “ 应用程序摘要**”** 表中，单击 URL 可在 “违规信息” 页中查看 违规的完整详细信息，包括日志表达式名称、注释以及 Citrix ADC 实例为操作返回的值。



突出显示 **Web** 应用程序防火墙 **(WAF)** 的违规模式

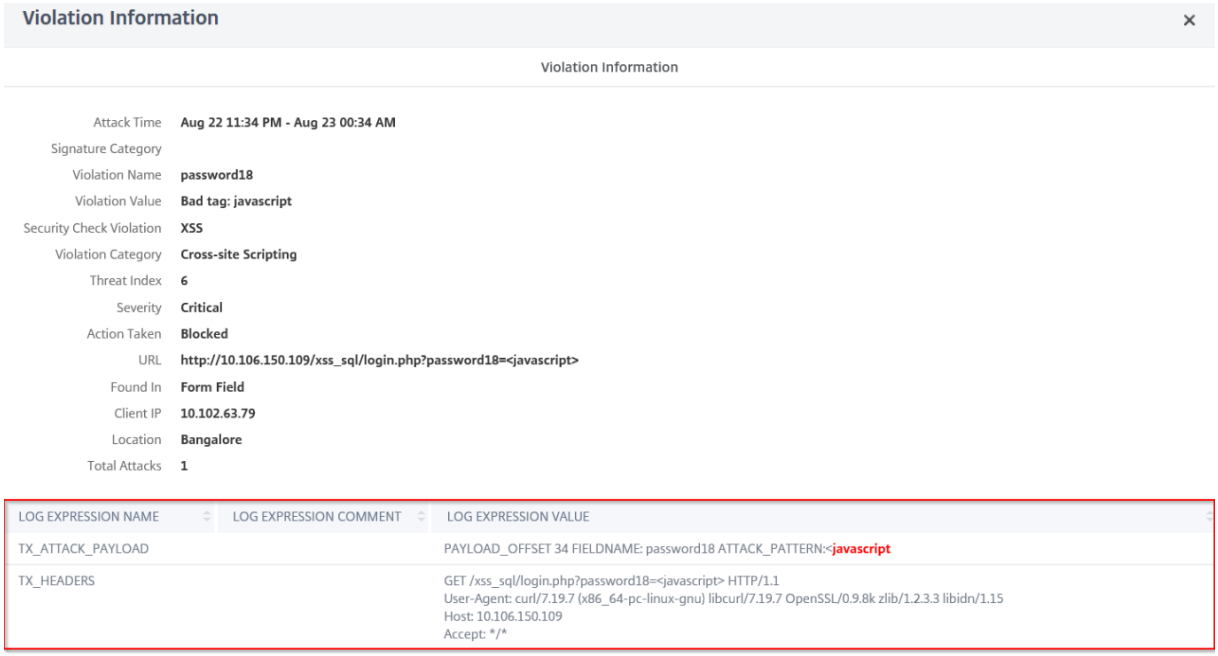
现在，您可以获取攻击的详细信息，例如 HTTP 标头和 HTTP 有效负载，以对攻击进行故障排除或分析。要获取攻击的详细信息，必须使用以下命令更新应用程序防火墙配置文件中的 “VerboseLogLevel”：

`Set appfw profile <profile_name> -VerboseLogLevel (pattern|patternPayload|patternPayloadHdr)`

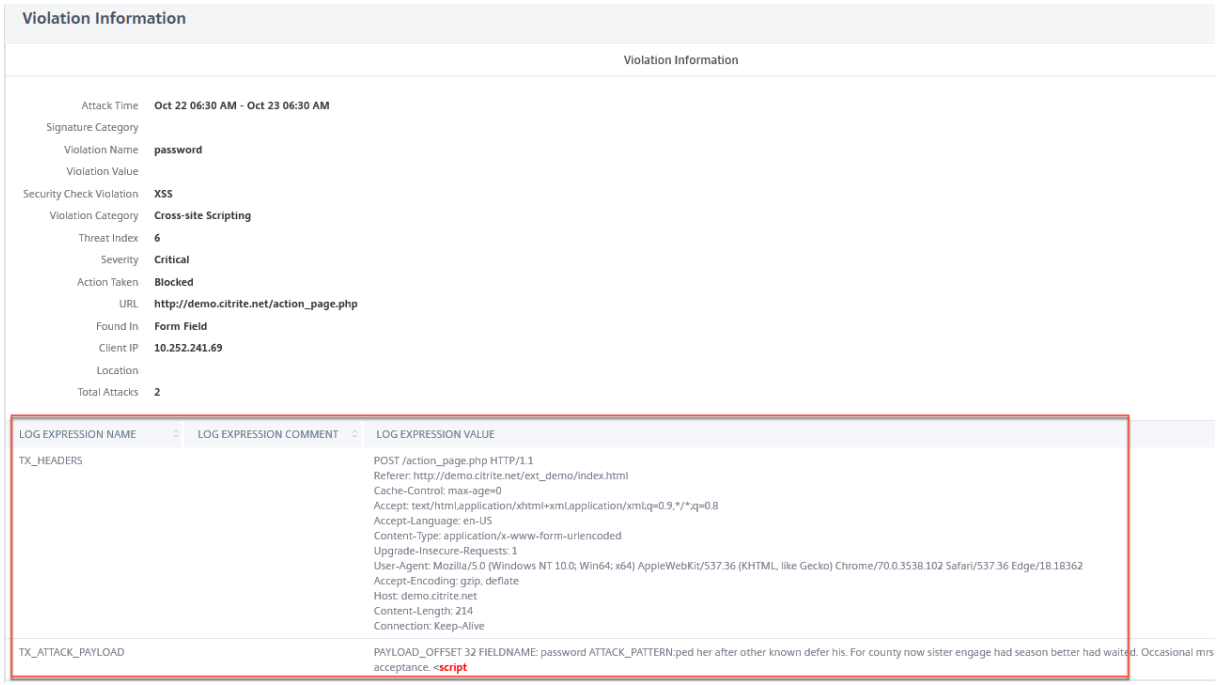
- `pattern` -仅记录违规模式
- `patternPayload` -记录攻击模式前的违规模式 + 150 字节字段元素值
- `patternPayloadHdr` -违规模式 + 攻击模式之前的 150 字节字段元素值 + HTTP 请求标头被记录

根据 “详细日志级别” 配置，Citrix ADM 显示详细的日志表达式记录。

下图是一个突出显示 GET 请求的攻击模式的示例：



下图是突出显示 POST 请求的攻击模式的示例：



在这两个例子中：

- 字段名称是指攻击模式的相应字段名称。
- 有效载荷偏移是指实际有效载荷中的攻击偏移。
- 攻击模式突出显示攻击模式，并在值中包含 150 字节的前缀有效负载。

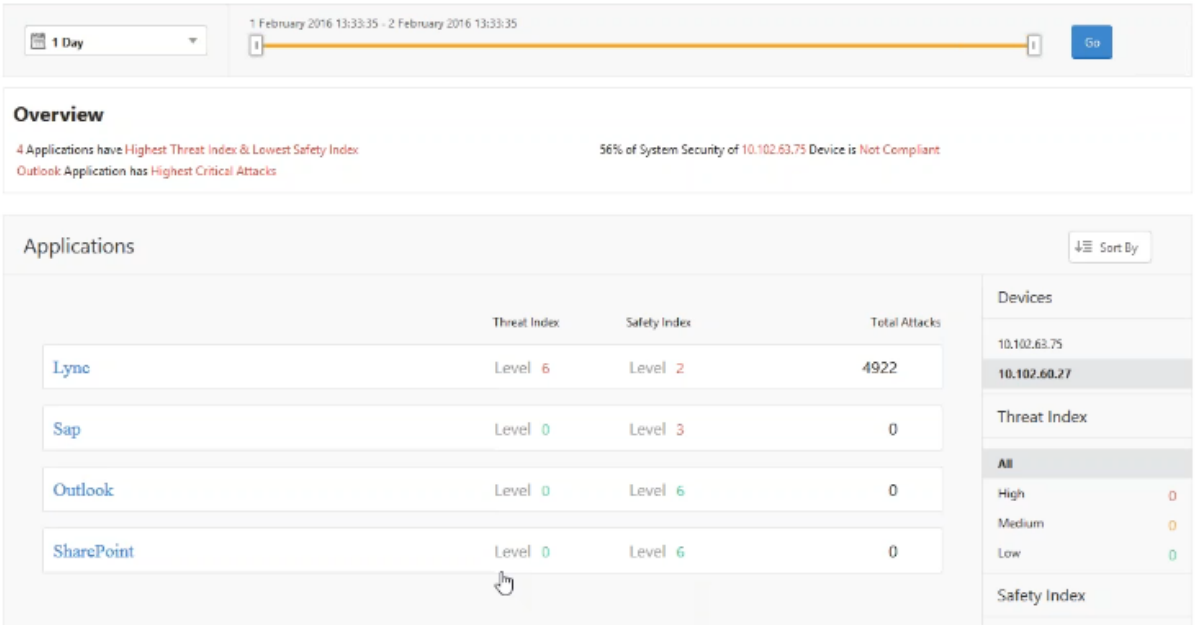
有关在 Citrix ADC 中配置详细日志级别的详细信息，请参阅 易于使用 Web App Firewall 日志进行故障排除。

在部署配置之前确定安全指数

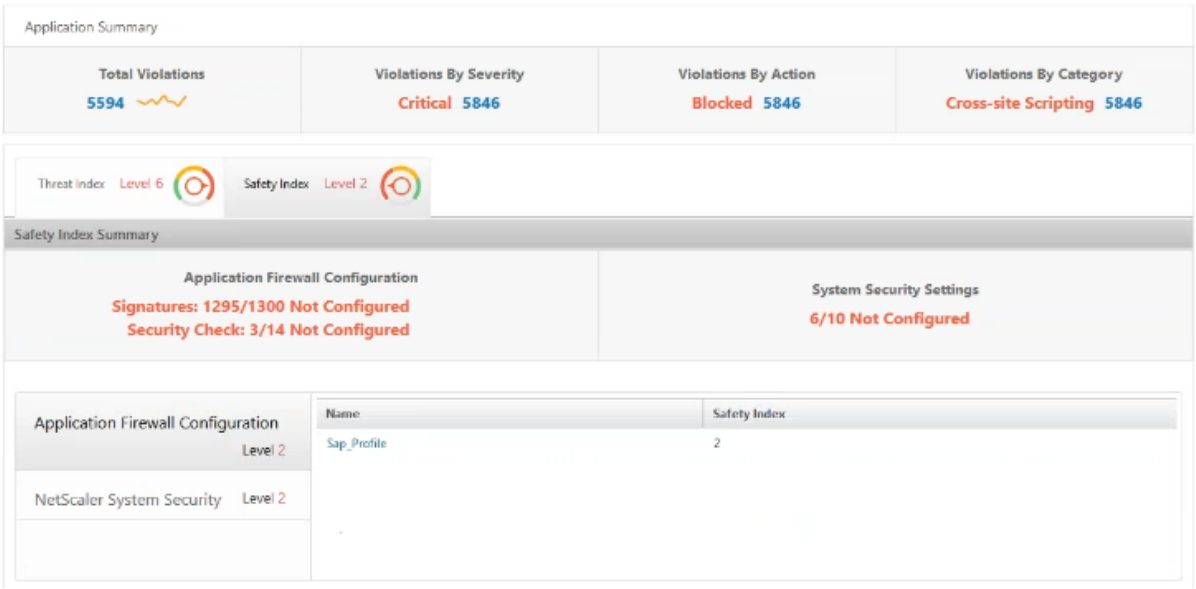
在 Citrix ADC 实例上部署安全配置后，会发生安全漏洞，但您可能希望在部署安全配置之前评估安全配置的有效性。

例如，您可能需要评估具有 10.102.60.27 IP 地址的 Citrix ADC 实例上 SAP 应用程序配置的安全索引。

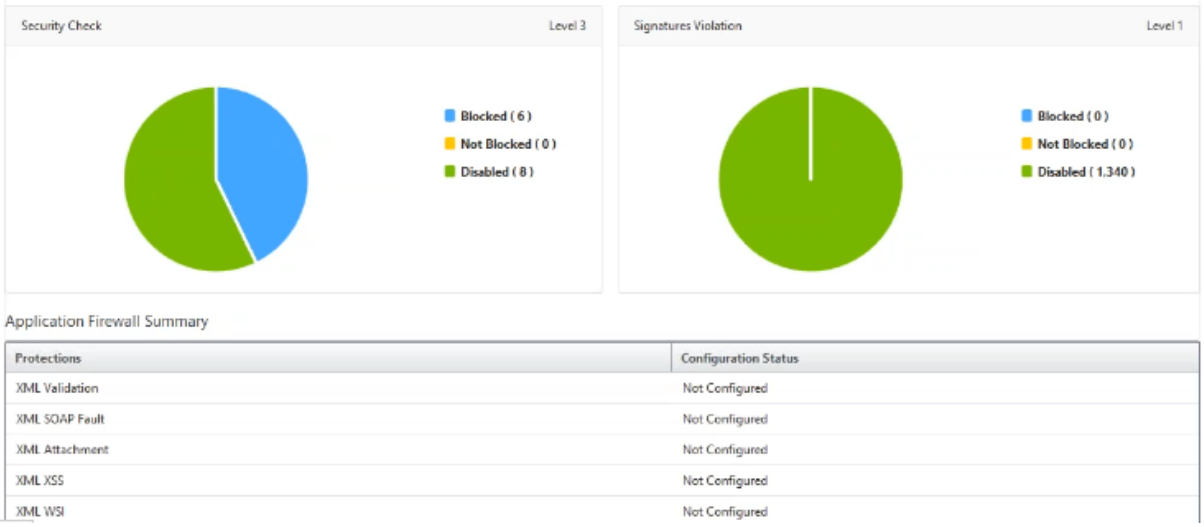
在“ 安全智能分析”仪表板上的“ 设备”下，单击您配置的 Citrix ADC 实例的 IP 地址。可以看到威胁指数和攻击总数都是 0。威胁指数直接反映应用程序上攻击的数量和类型。攻击数为零表示应用程序没有面临任何威胁。



单击 **Sap > Safety Index**（安全指数）**> SAP_Profile**，并评估显示的安全指数信息。



在应用程序防火墙摘要中，可以查看不同保护设置的配置状态。如果一个设置被设置为日志或如果一个设置未配置，则为应用程序分配较低的安全指数。



机器人

April 23, 2021

> 注意
>
> 如果您的 Citrix ADM 版本早于 **13.0-79.x**，则可以通过导航至 **Analytics** > 安全 > 机器人洞察来查看机器人洞察。对于版本 **13.0-79.x** 或更高版本，您可以导航到 **Analytics** > 安全 > 安全违规 > 应用程序概述，然后单击应用程序细分依据下的机器人来查看机器人详细信息。

机器人是一种软件程序，它以比人类快得多的速度自动执行某些操作。超过 35% 的 Web 流量由机器人组成，80% 的组织遭受机器人攻击。他们可以与网页交互、提交表单、单击链接、扫描文本或下载内容。机器人可以在社交媒体平台上访问视频、发表评论和推文。有些机器人甚至可以与人类用户进行基本对话。这些被称为聊天机器人。

执行需要或有用的服务（如客户服务、聊天机器人、搜索引擎爬虫程序）的机器人被称为良好的机器人。某些恶意机器人可以从网站上刮取或下载内容、窃取用户凭据、传播垃圾邮件内容以及执行各种其他类型的网络攻击。这些恶意机器人被称为坏机器人。识别错误的机器人并保护您的设备免受高级安全攻击至关重要。您可以使用机器人管理系统来实现这一点。

有关机器人的更多信息，请参阅机器人管理。

在 **Citrix ADC** 中配置机器人检测技术

在 Citrix ADC 中，您可以配置机器人检测技术来检测传入的机器人流量。以下是您在 Citrix ADC 实例中配置的机器人技术：

- 允许列表。此规则包含 URL 和策略表达式的列表，用于评估是否有一组特定的好机器人可以访问您的 Web 资源。
- 阻止列表。此规则包含 URL 和策略表达式的列表，用于评估一组特定的坏机器人是否可以访问您的网站。

- **IP** 信誉。此规则检测传入的机器人流量是否为恶意 IP 地址。
- 设备指纹识别。此规则检测传入的机器人流量是否在传入的客户机器人流量的传入请求标头和浏览器属性中具有设备指纹 ID。
- 速率限制。此规则速率限制来自同一客户端的多个请求。
- 签名。此规则根据特征码检测检测检测检测并阻止机器人。它还可以防止未经授权的 URL 刮取网站、强制登录以及探测漏洞的机器人。
- 机器人陷阱。此规则检测到访问网页上启用的脚本的机器人。
- **TPS**。如果请求的最大数量和请求的增加百分比超过了配置的时间间隔，此规则将传入流量检测为机器人。

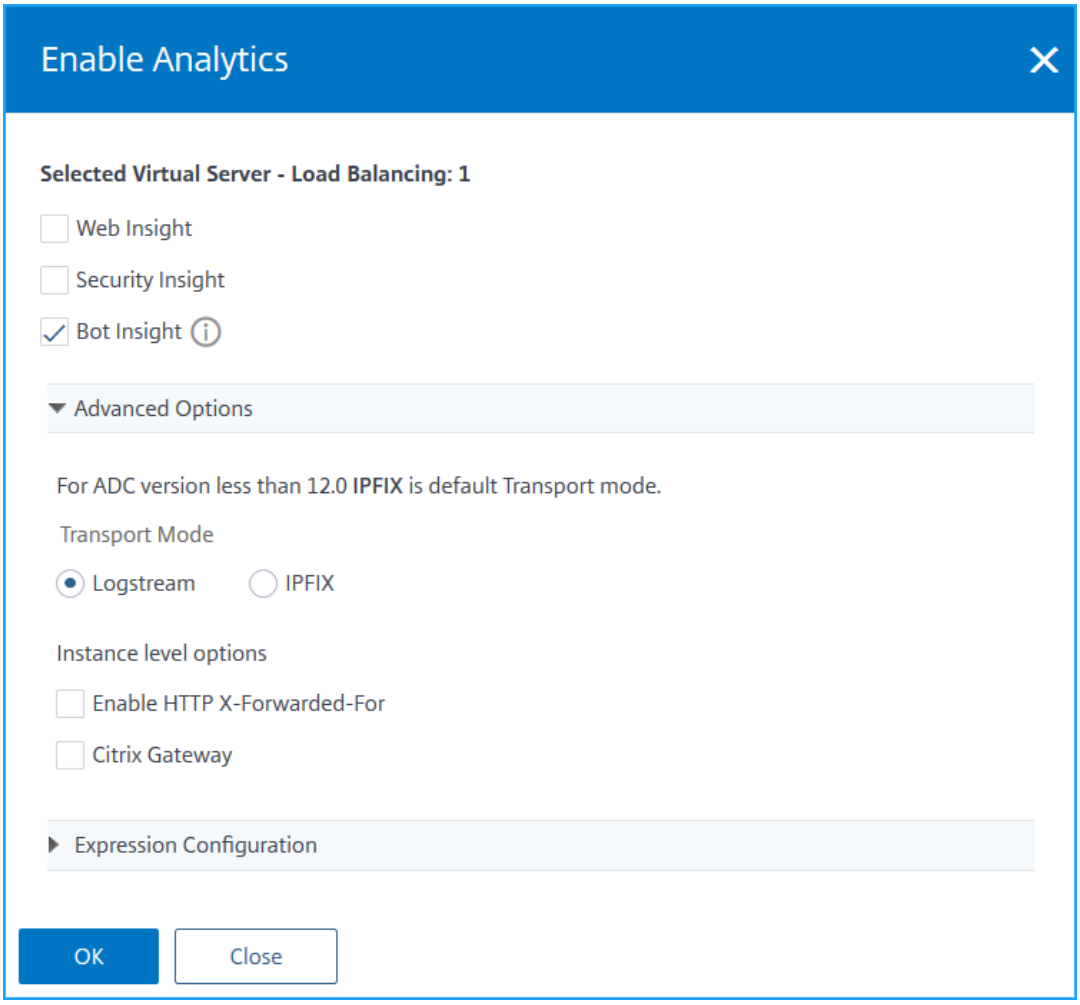
有关配置机器人管理的详细信息，请参阅 配置机器人管理。

在 **Citrix ADM** 中使用机器人见解

在 Citrix ADC 中配置机器人管理后，必须在虚拟服务器上启用 机器人见解功能，以查看 Citrix ADM 中的见解。

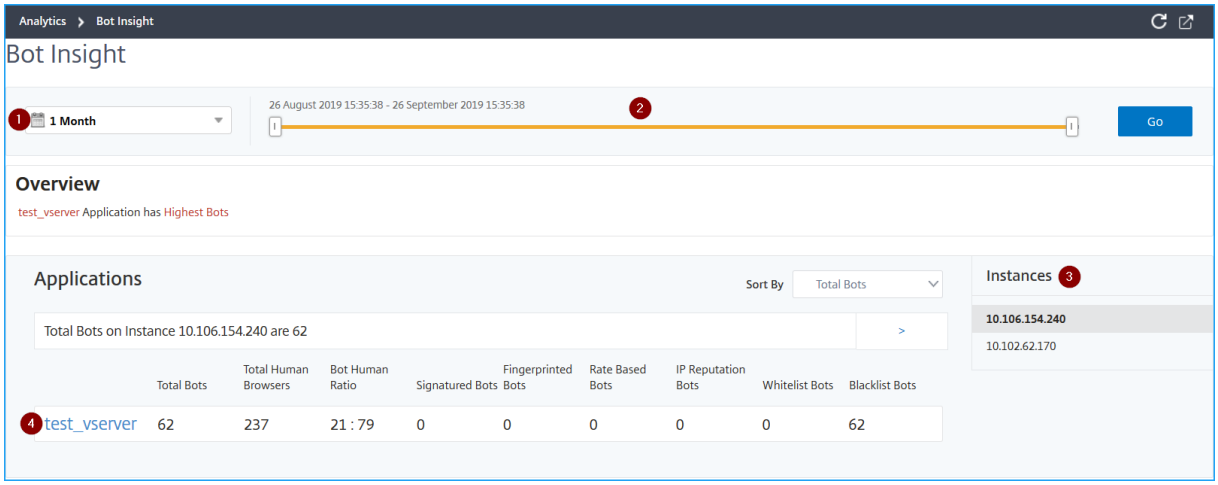
要启用机器人见解，请执行以下操作：

1. 导航到网络 > 实例 > **Citrix ADC** 并选择实例类型。例如，VPX。
2. 选择实例，然后从选择操作列表中选择配置分析。
3. 选择虚拟服务器，然后单击启用分析。
4. 在 启用分析窗口中：
    a) 选择机器人见解
    b) 在高级选项下，选择日志流。



c) 单击确定。

启用机器人见解功能后，导航到分析 > 机器人见解。



1 -查看机器人详细信息的时间列表

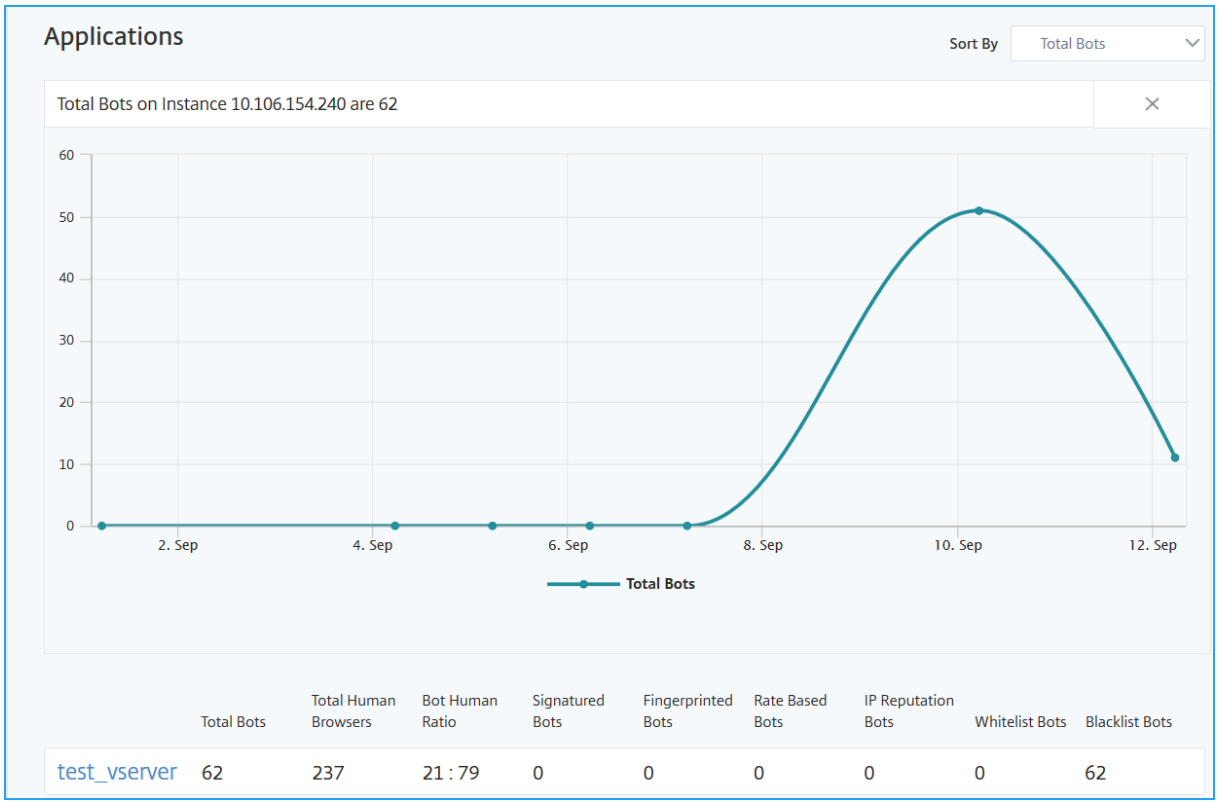
2 — 拖动滑块以选择特定的时间范围，然后单击转到以显示自定义结果

3 — 受机器人影响的实例总数

4 — 具有总自动程序攻击的选定实例的虚拟服务器

- 机器人总数 — 表示为虚拟服务器找到的机器人攻击总数（包括所有机器人类别）。
- 人类浏览器总数 — 表示访问虚拟服务器的人类用户总数。
- 机器人员比率 — 指示访问虚拟服务器的人员用户与机器人之间的比率。
- 签名机器人、指纹机器人、基于速率的机器人、**IP** 信誉机器人、允许列表机器人和 阻止列表机器人-根据配置的机器人类别指示发生的机器人攻击总数。有关机器人类别的更多信息，请参阅在 Citrix ADC 中配置机器人检测技术。

5 -单击 **>** 以图形格式查看机器人详细信息。

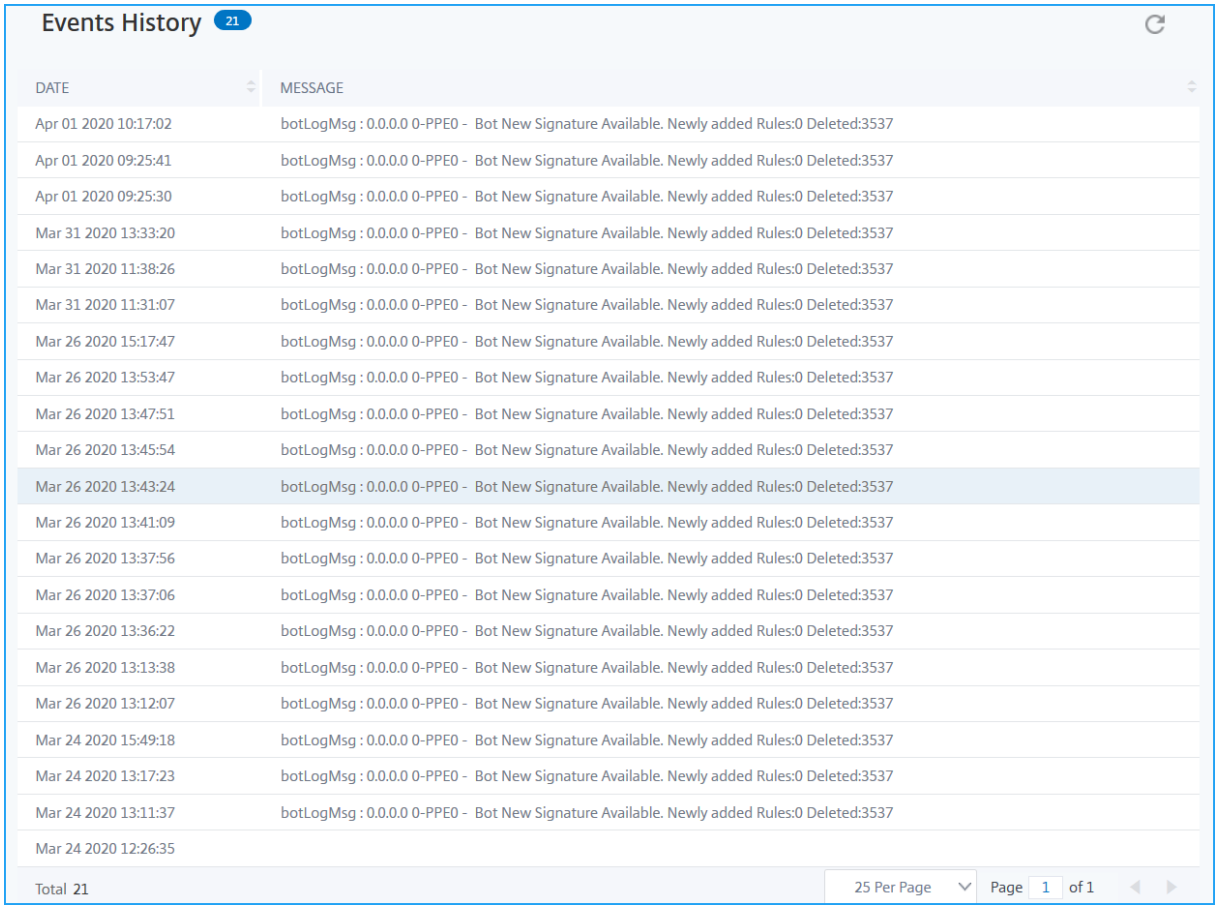


查看事件历史记录

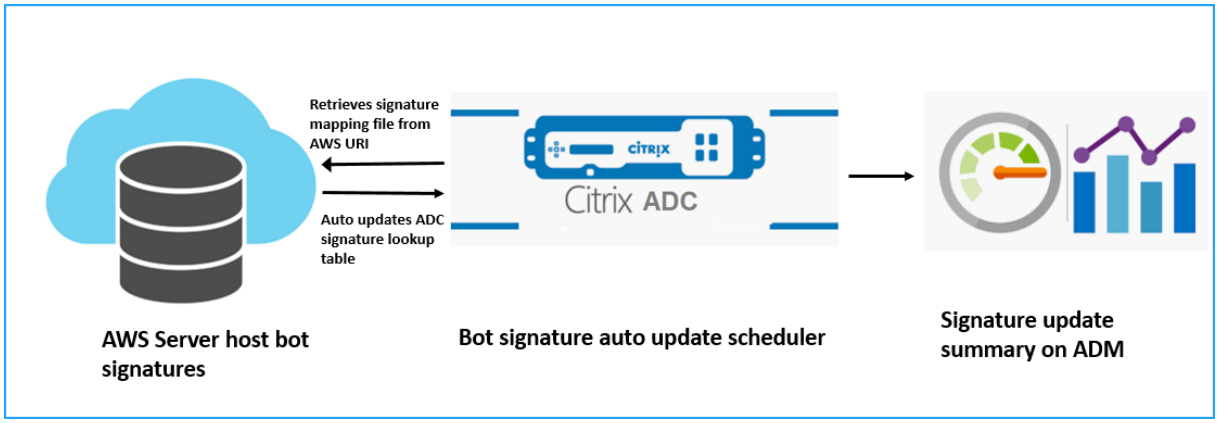
在以下情况下，您可以在 事件历史记录中查看机器人特征码更新：

- 在 Citrix ADC 实例中添加了新的机器人签名。
- 在 Citrix ADC 实例中更新现有的机器人特征码。

您可以在机器人洞察页面中选择时间持续时间以查看事件历史记录。



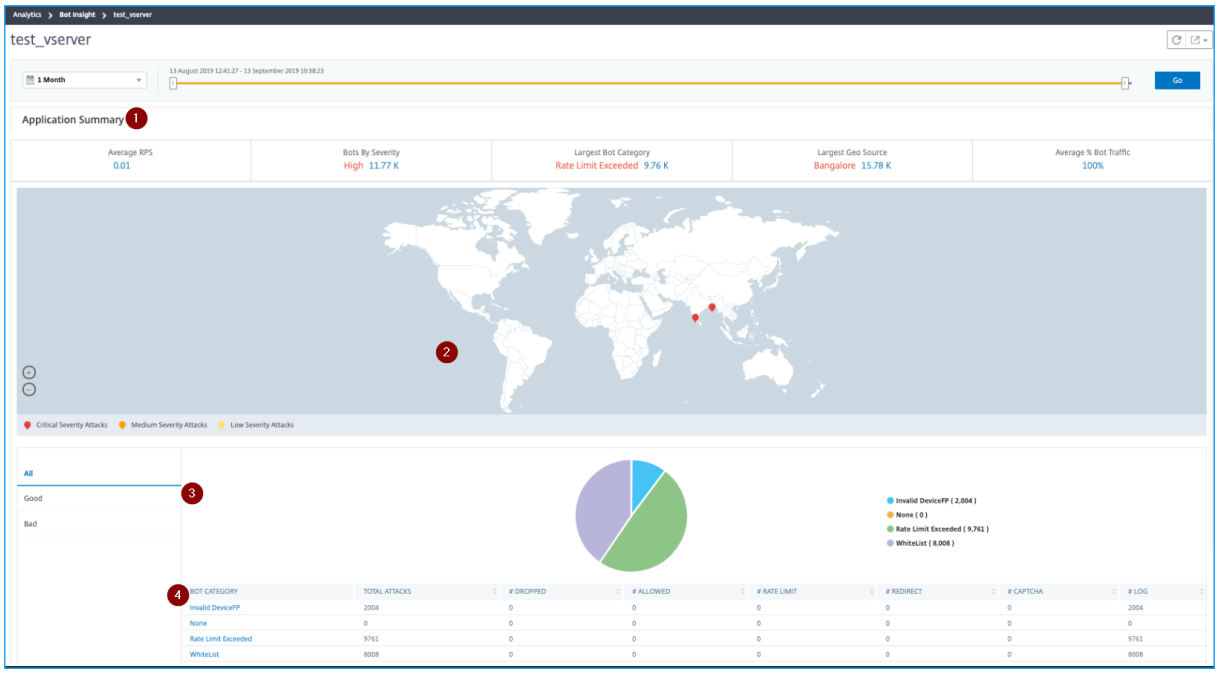
下图显示了如何从 AWS 云中检索机器人签名、在 Citrix ADC 上更新以及在 Citrix ADM 上查看特征码更新摘要。



1. 机器人签名自动更新调度程序从 AWS URI 中检索映射文件。
2. 使用 ADC 装置中的现有签名检查映射文件中的最新签名。
3. 从 AWS 下载新签名并验证签名完整性。
4. 使用机器人签名文件中的新签名更新现有机器人签名。
5. 生成 SNMP 警报并将特征码更新摘要发送到 Citrix ADM。

查看机器人

单击虚拟服务器以查看 应用程序摘要。



1 — 提供应用程序摘要详细信息，例如：

- 平均 **RPS** — 表示虚拟服务器上收到的平均每秒机器人事务请求 (RPS)。
- 按严重性划分的机器人 — 表示基于严重性发生的机器人事务最高。严重性根据致命、高、中和低进行分类。

  例如，如果虚拟服务器具有 11770 个高严重性机器人和 1550 个致命严重性机器人，则 Citrix ADM 在按严重程度划分的机器人下显示致命 **1.55 K**。
- 最大机器人类别 — 表示基于机器人类别发生的机器人攻击最高。

  例如，如果虚拟服务器有 8000 个阻止列出的机器人、5000 个允许列出的机器人和 10000 个超出速率限制的机器人，则 Citrix ADM 将在 最大机器人类别下显示 超过 **10 K** 的速率限制。
- 最大地理源 — 表示基于区域发生的机器人攻击最高。

  例如，如果虚拟服务器在圣克拉拉有 5000 个机器人攻击，伦敦有 7000 个机器人攻击，班加罗尔有 9000 个机器人攻击，那么 Citrix ADM 在最大地理源下显示班加罗尔 **9 K**。
- 平均机器人流量百分比 — 表示人类机器人比率。

2 — 根据地图视图中的位置显示机器人攻击的严重性

3 — 显示机器人攻击的类型（“好”、“坏”和“全部”）

4 — 显示机器人攻击总数以及相应的配置操作。例如，如果您已配置：

- IP 地址范围 (192.140.14.9 到 192.140.14.254) 作为阻止列表机器人，并选择删除作为这些 IP 地址范围的操作

- IP 范围 (192.140.15.4 到 192.140.15.254) 作为阻止列表机器人，并选择创建日志消息作为这些 IP 范围的操作

  在这种情况下，Citrix ADM 显示：

  - 区块列出的机器人总数
  - 丢弃下的机器人总数
  - 日志下的机器人总数

查看验证码机器人

在网页中，CaptChaS 旨在识别传入流量是来自人类还是自动机器人。要查看 Citrix ADM 中的验证码活动，必须将验证码配置为 Citrix ADC 实例中的 IP 信誉和设备指纹检测技术的自动程序操作。有关详细信息，请参阅机器人管理。

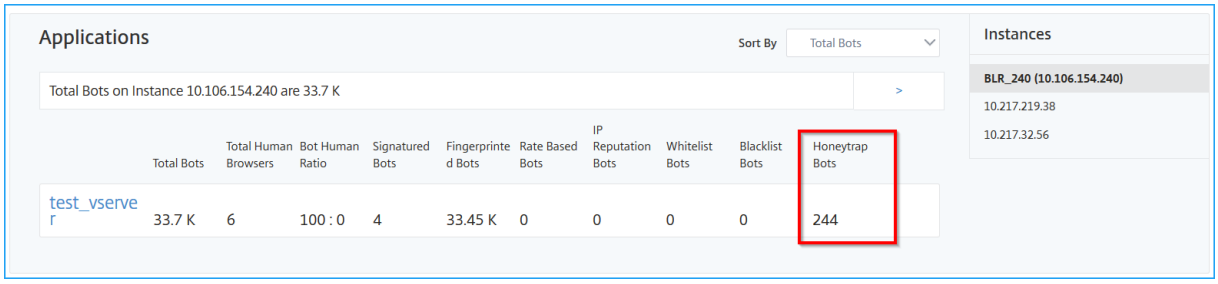
以下是 Citrix ADM 在机器人洞察中显示的验证码活动：

- 超过验证码尝试次数 — 表示登录失败后所做的最大验证码尝试次数
- 验证码客户端静音 **—** 表示丢弃或重定向的客户端请求数，因为这些请求早些时候在 **CAPTCHA** 挑战中被检测为坏机器人
- 人类 — 表示从人类用户执行的验证码条目
- 验证码响应无效 — 表示 Citrix ADC 发送验证码挑战时从机器人或人类收到的错误验证码响应的数量

BOT CATEGORY	TOTAL ATTACKS	# DROPPED	# CAPTCHA	# ALLOWED	# RATE LIMIT	# REDIRECT	# LOG
Captcha Attempts Exceeded	11	11	0	0	0	0	0
Captcha Client Muted	2	0	0	0	0	2	0
Crawler	36	36	0	0	0	0	0
Feed Fetcher	8	8	0	0	0	0	0
Human	0	0	0	0	0	0	0
Invalid Captcha Response	48	33	8	0	0	0	7
Marketing	262	262	0	0	0	0	0
NULL	1	0	0	0	0	0	1
Scraper	33	33	0	0	0	0	0
Search Engine	155	155	0	0	0	0	0
Site Monitor	57	57	0	0	0	0	0
Tool	82	82	0	0	0	0	0
Uncategorized	0	0	0	0	0	0	0

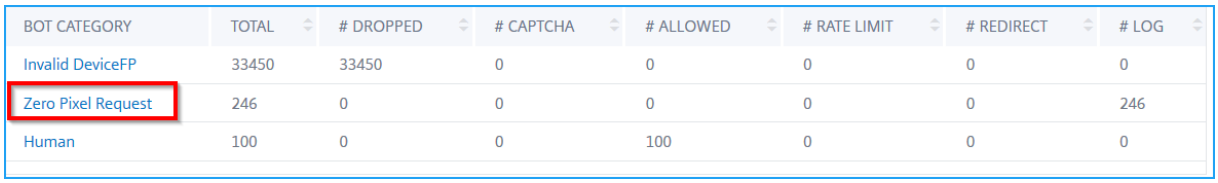
查看机器人陷阱机器人

要在 Citrix ADM 中查看机器人陷阱，必须在 Citrix ADC 实例中配置机器人陷阱。有关详细信息，请参阅机器人管理。



为了识别机器人陷阱，在网页中启用了一个脚本，这个脚本对人类隐藏，但不会对机器人隐藏。当机器人访问此脚本时，Citrix ADM 会识别并报告机器人陷阱。

单击虚拟服务器并选择 零像素请求

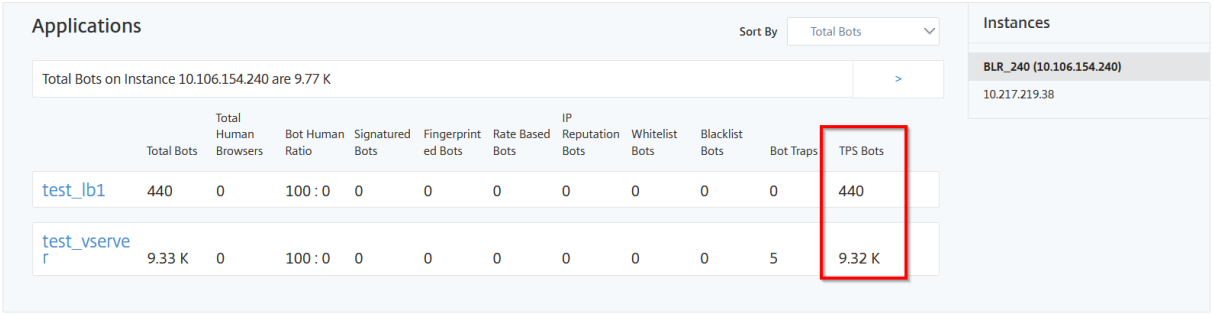


查看 **TPS** 机器人

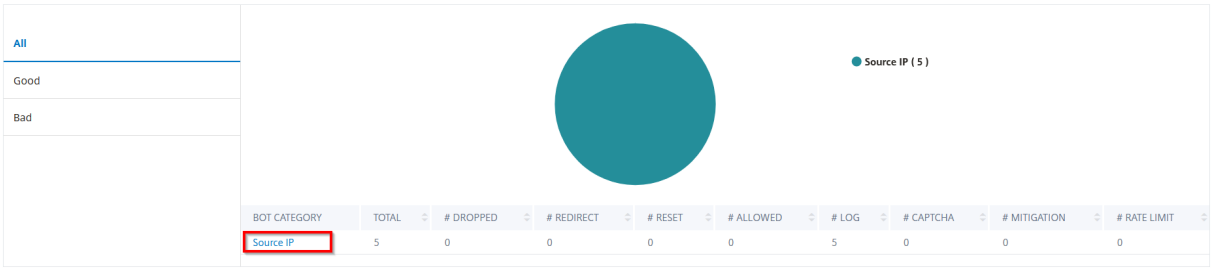
以下是您可以在 Citrix ADM 中查看的 TPS 机器人类别：

- 源 IP
- 地理位置
- 主机
- URL

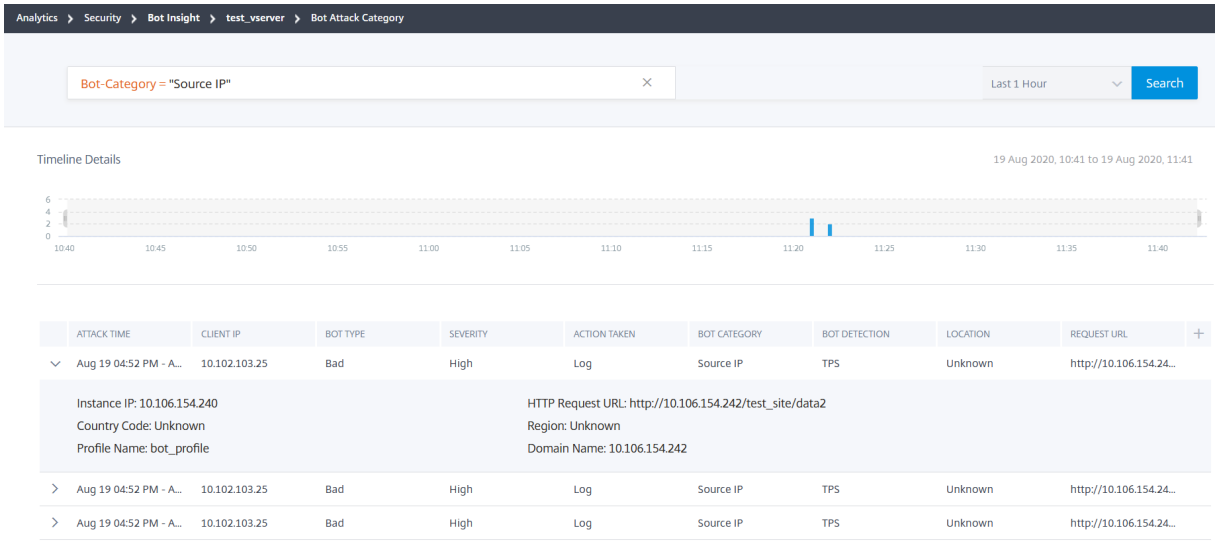
单击虚拟服务器以查看 TPS 机器人。



单击 **TPS** 机器人类别以查看机器人详细信息。



此时将显示详细信息页面。



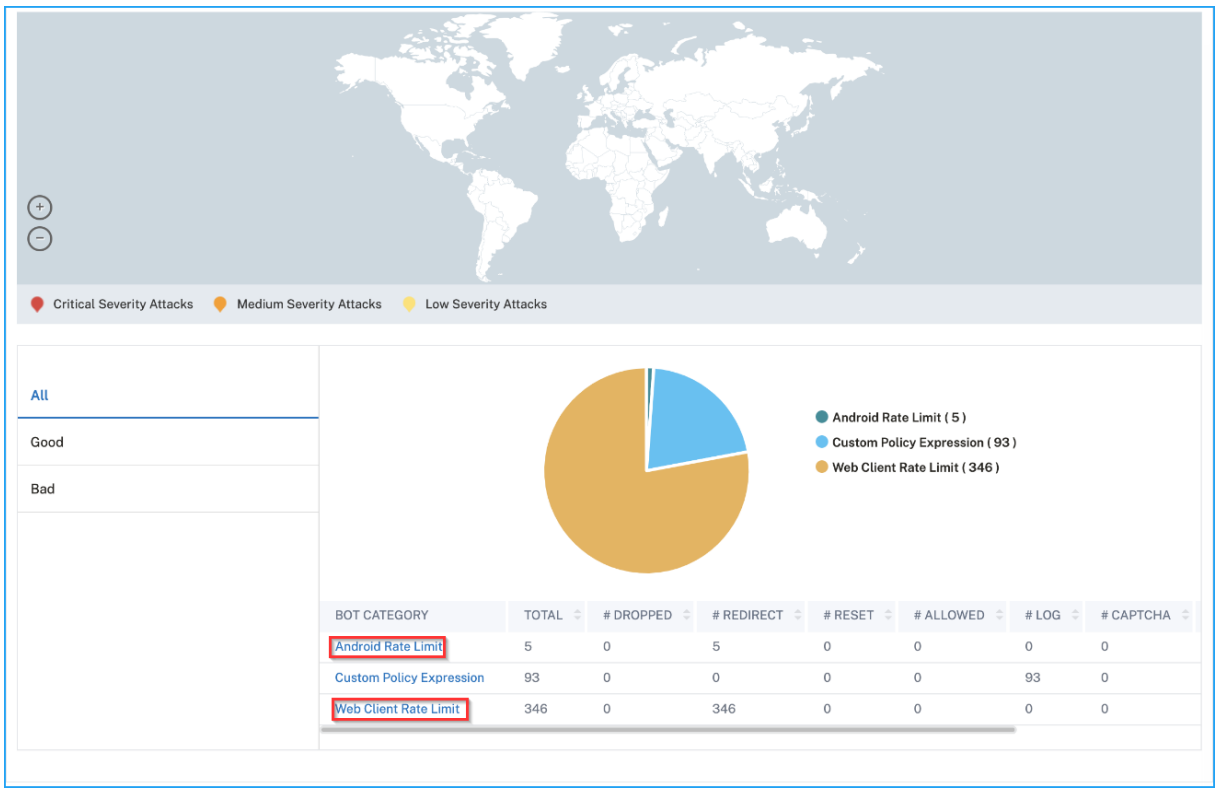
查看移动 **(Android)** 应用程序的机器人类别

要查看适用于移动 (Android) 应用程序的机器人，必须在 Citrix ADC 中配置指纹检测技术。有关详细信息，请参阅为移动应用程序配置设备指纹技术。

在 Citrix ADC 中配置设置后，您可以在 Citrix ADM 中查看以下机器人类别：

- Web 客户端费率限制
- Android 费率限制
- Web 客户端设备
- Android 设备

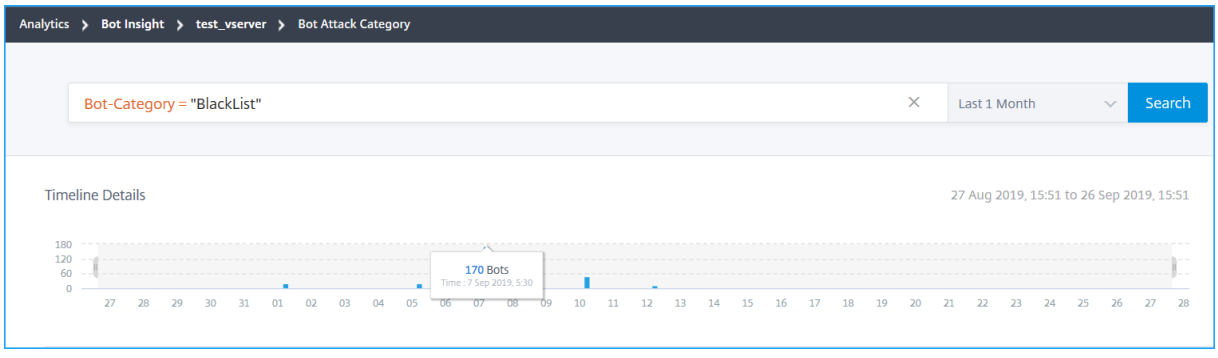
单击虚拟服务器以查看适用于移动应用程序的机器人类别。



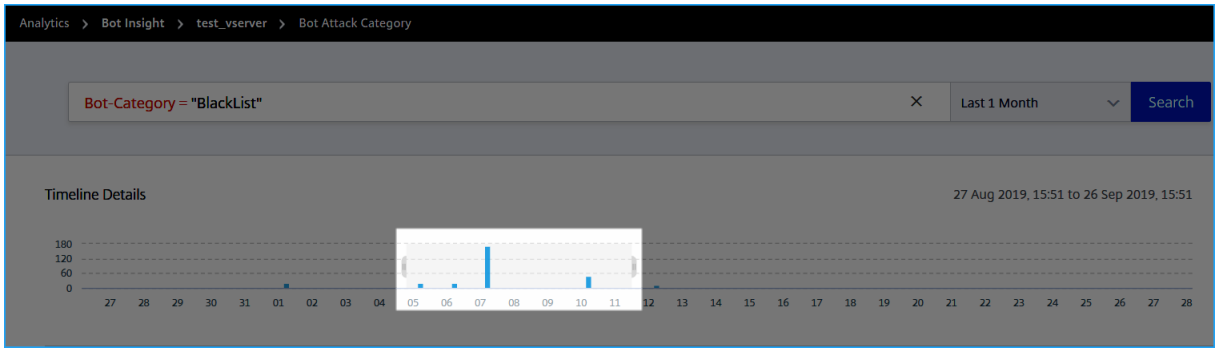
查看机器人详细信息

要进一步深入了解详细信息，请单击机器人类别下的机器人攻击类型。例如，如果要查看阻止列出的机器人攻击的详细信息，请单击机器人类别下的阻止列表。

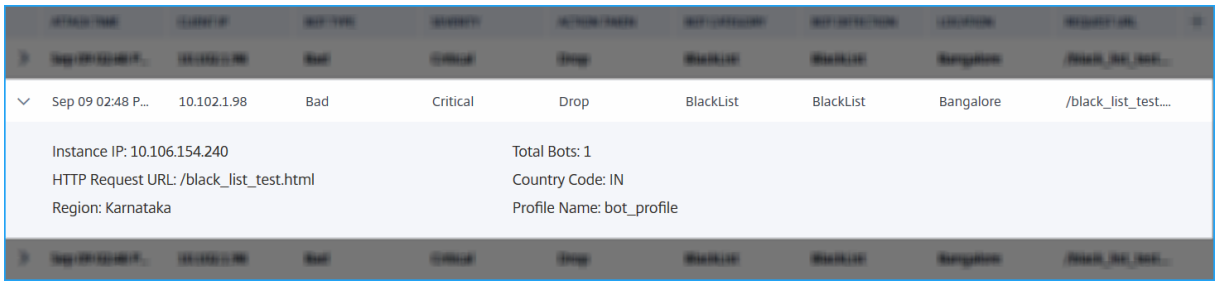
将显示攻击时间和机器人攻击总数等详细信息。



您还可以拖动条形图来选择要随机器人攻击显示的特定时间范围。



要获取有关机器人攻击的其他信息，请单击展开。



- 实例 **IP** — 表示 Citrix ADC 实例 IP 地址
- 机器人总数 — 表示该特定时间内发生的机器人攻击总数
- **HTTP** 请求 **URL** — 表示配置为阻止列出的 URL
- 国家代码 — 指示发生机器人攻击的国家/地区
- 区域 — 指示发生自动程序攻击的区域
- 配置文件名称 — 指示您在配置过程中提供的配置文件名称

高级搜索

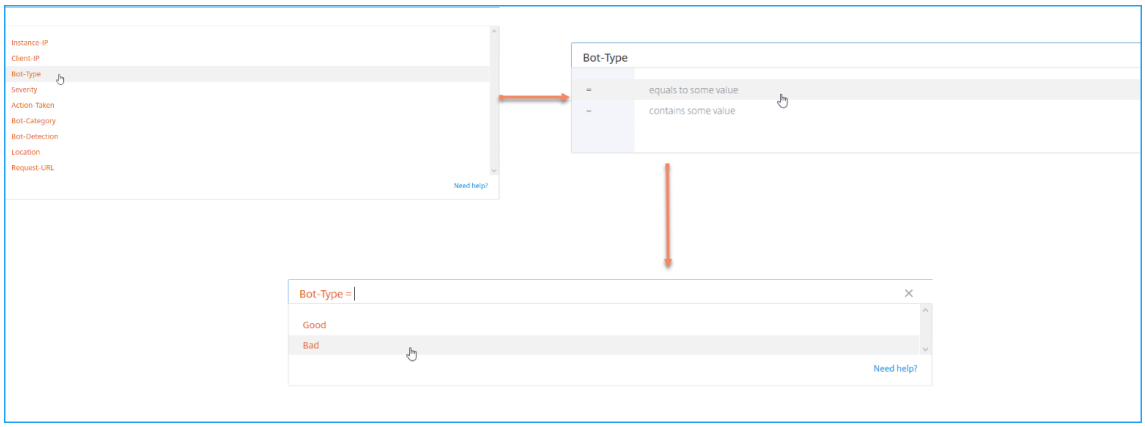
您还可以使用搜索文本框和时间持续时间列表，从中可以根据您的要求查看机器人详细信息。单击搜索框时，搜索框将为您提供以下搜索建议列表。

- 实例 **IP** — Citrix ADC 实例 IP 地址
- 客户端 **IP** - 客户端 IP 地址
- 机器人类型 — 机器人类型，如好或坏
- 严重性 — 机器人攻击的严重性
- 采取的操作 **—** 在机器人攻击之后采取的操作，如 **“**删除**”**、**“**无操作**”**、**“**重定向”
- 机器人类别 — 机器人攻击的类别，例如阻止列表、允许列表、指纹等。根据类别，您可以将机器人操作与其关联
- 机器人检测 — 您在 Citrix ADC 实例上配置的机器人检测类型（阻止列表、允许列表等）

- 位置 — 机器人攻击发生的地区/国家
- 请求 **URL** - 具有可能的机器人攻击的 URL

您也可以在搜索查询中使用运算符来缩小搜索焦点。例如，如果您想查看所有坏机器人：

1. 单击搜索框并选择机器人类型
2. 再次单击搜索框并选择运算符 **=**
3. 再次单击搜索框并选择错误
4. 单击搜索以显示结果



查看应用程序安全违规详细信息

April 23, 2021

暴露于互联网的 Web 应用程序已经容易受到严重攻击。Citrix ADM 使您能够显示可操作的违规详细信息，以保护应用程序免受攻击。导航到 **Analytics** > 安全 > 安全违规，以获取单窗格解决方案，以便：

- 通过全面了解安全洞察和机器人洞察中相关的威胁详细信息，可视化应用程序
- 根据 网络、机器人和 **WAF** 等类别访问应用程序安全违规
- 采取纠正措施保护应用程序的安全

“ 安全违规” 页面有以下选项：

- 应用程序概述 — 显示具有完全违规、WAF 和 Bot 违规总数、按国家/地区划分的违规等的应用程序的概览。有关详细信息，请参阅应用程序概述。
- 所有违规 — 显示应用程序安全违规详细信息。有关详细信息，请参阅所有违规。

必备条件

确保是否已启用 度量收集器。默认情况下，在 Citrix ADC 实例上启用 度量收集器。有关详细信息，请参阅配置智能应用分析。

SSL Insight

April 23, 2021

SSL Insight 提供对安全 Web 事务 (HTTPS) 的可见性，并允许 IT 管理员通过对安全 Web 事务提供集成的实时和历史性监视来监视 Citrix ADC 提供服务的所有安全 Web 应用程序。通过此功能，管理员可以评估以下内容：

- 确定配置更改对客户使用情况的影响：管理员可以了解进行配置更改（如关闭 SSLv3 或删除 RC4-MD5 等密码）对客户端的影响。这可以通过评估此协议和密码的历史事务数据来完成。
- 量化客户端性能：管理员可以根据使用的 SSL 密码/协议或协商的证书了解对应用程序响应时间的影响。
- 应用程序安全性：评估是否有任何应用程序在低安全性协议、密码或弱密钥强度上运行事务。

如果在 Citrix ADC 实例上启用 SSL 分析，则会记录和记录每个 SSL 事务的 SSL 统计信息。这些统计信息显示 SSL 流的详细信息。此外，每个成功的连接都会由 Citrix Application Delivery Management (ADM) 分析记录和显示。

SSL Insight 提供以下关键信息，这些信息由 Citrix ADM 分析显示：

- 协商的 SSL 协议版本
- 协商的密码和密码强度
- 使用的证书的签名哈希算法
- 证书类型和大小
- SSL 前端和后端错误

> 注意
>
> 对于成功的 SSL 连接，SSL AppFlow 日志记录会在每个事务结束时进行。

必备条件

- 要配置 SSL 智能分析的 Citrix ADC 实例必须运行 Citrix ADC 软件版本 11.1 51.21 及更高版本。在运行 11.1 51.21 的 ADC 实例上运行以下命令，以启用日志流作为 SSL 智能分析的传输类型。

1. `enable ns mode ulfd`
2. `add ulfd server <IP Address of the ADM>`

   对于运行 12.0 及以上版本的 ADC 实例，请选择日志流作为传输类型，同时从 ADM 启用 AppFlow。

- Citrix ADM 版本和内部版本必须等于或高于 Citrix ADC 版本和内部版本。例如，如果您已安装 Citrix ADM 11.1 版本 61.7，请确保已安装 Citrix ADC 11.1 版本 60.14 或更早版本。

配置 **SSL Insight**

如果您启用了以下元素，则 SSL Insight 指标包含在 Web Insight 报告中：

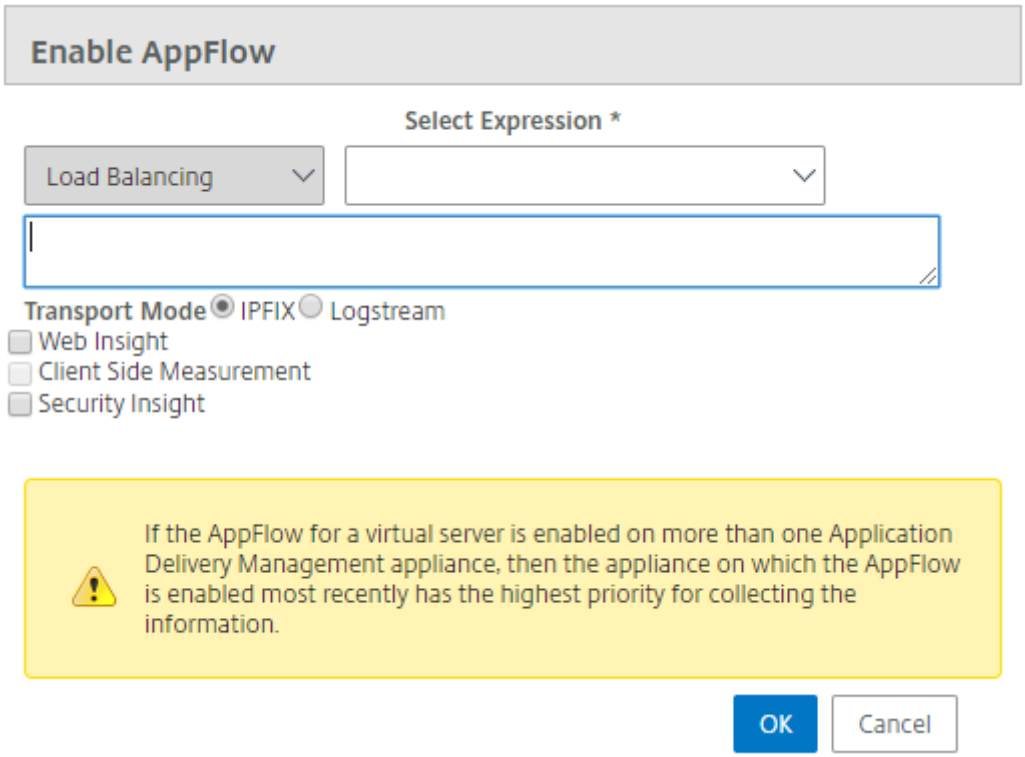
- 在每个 Citrix ADC 实例上启用 Web 智能分析的 AppFlow。
- 在每个 Citrix ADC 实例上启用 ULFD 模式。
- 在每个 Citrix ADC 实例上启用所需的 AppFlow 参数。

启用 **AppFlow** 功能

> 注意
>
> 您可以从 Citrix ADM 或每个 Citrix ADC 实例启用 AppFlow 功能。

要从 **Citrix ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到 **“网络” > “实例”**，然后选择要启用分析的 **Citrix ADC** 实例。
2. 从选择操作列表中，选择配置分析。
3. 选择虚拟服务器，然后单击 启用 **AppFlow**。
4. 在 “启用 AppFlow” 字段中，键入 **true**，然后选择 “ **Web** 智能分析”。
5. 在每个 Citrix ADC 实例上重复步骤 3 到步骤 6。
6. 单击确定。



> 注意
>
> 如果虚拟服务器的运行状态不是“UP”（运行），则无法在虚拟服务器上启用数据收集。

要使用 **Citrix ADC GUI** 启用 **AppFlow** 功能，请执行以下操作：

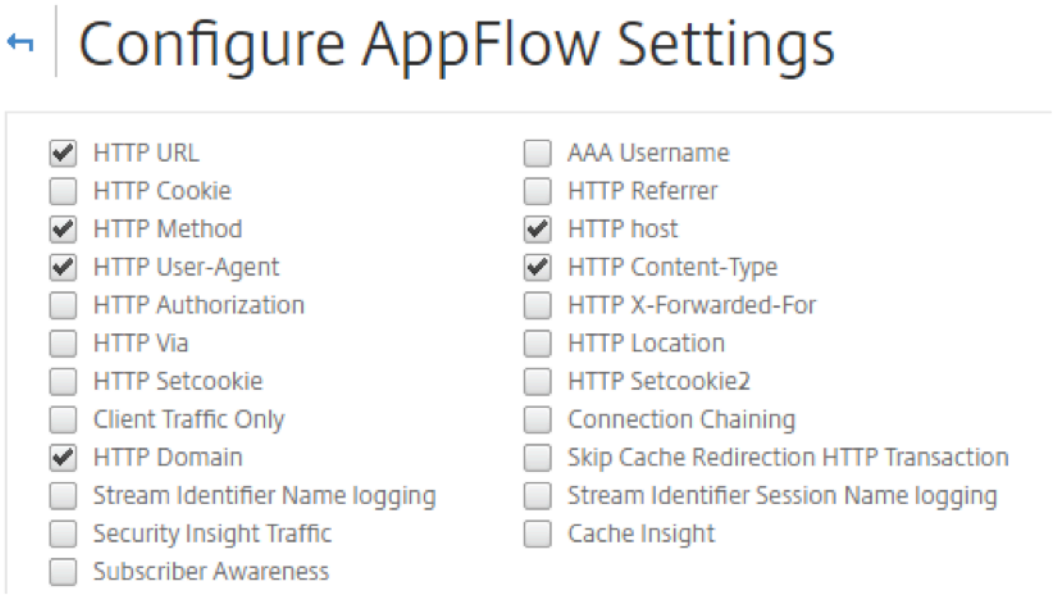
在 Citrix ADC 实例的 GUI 中，导航到 “ 配置” **>** “系统” **>** “设置”，单击 “配 置高级功能”，然后选择 “ **AppFlow**”。

启用 **SSL** 智能分析参数

在每个 Citrix ADC 实例上，您必须启用某些 HTTP 参数才能在 Citrix ADM 中显示 SSL 智能分析记录。

要从 **Citrix ADC** 配置实用程序启用 **SSL** 智能分析参数，请执行以下操作：

1. 导航到配置 > 系统 > **AppFlow**，然后单击更改应用流程设置。
2. 选中以下复选框：**HTTP** 域、**HTTP** 主机、**HTTP** 方法、**HTTP URL**、**HTTP** 用户代理、**HTTP** 内容类型。
3. 单击确定。



查看 **SSL** 智能分析度量

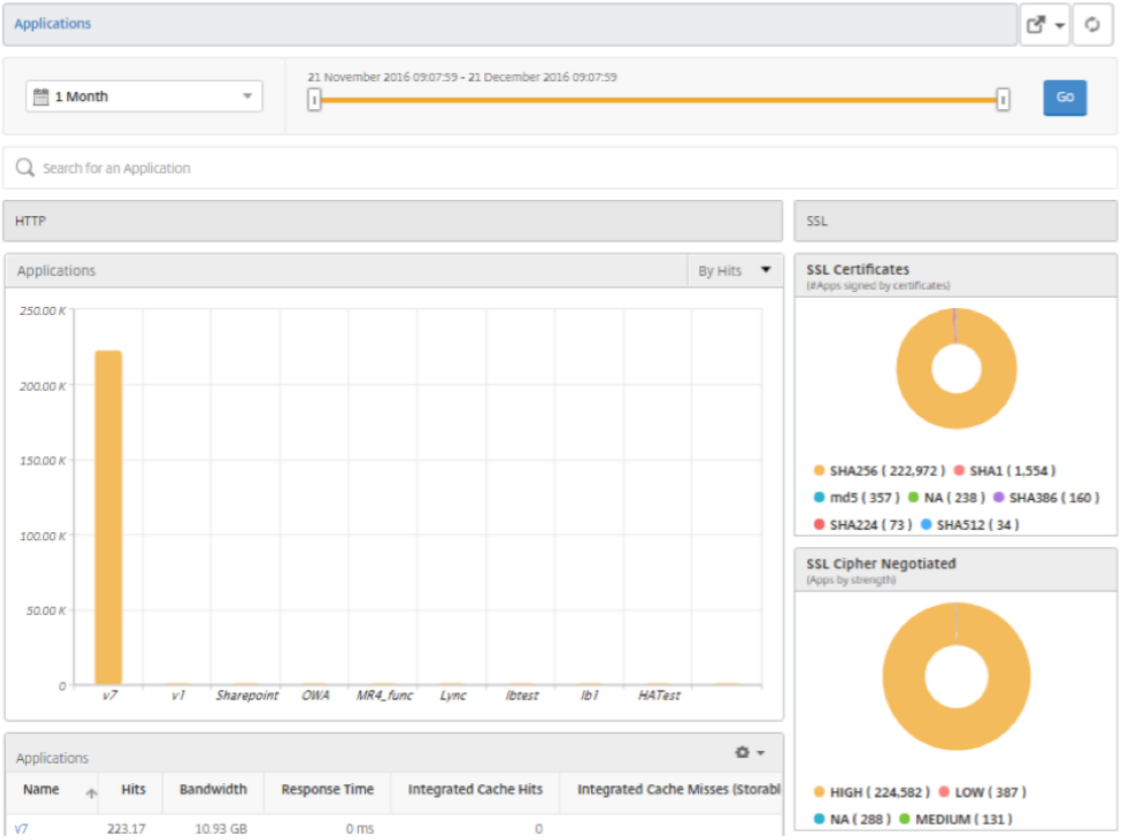
Citrix ADM 中的 SSL 智能分析度量提供了 Citrix ADC 实例所服务的 SSL 事务性能的详细视图。您可以在客户端、服务器或应用程序级别查看 SSL Insight 指标，以及查看 SSL 成功和失败事务的指标。借助这些指标，您可以分析和优化 **Citrix ADC HTTPS** 设置和 SSL 证书设置，并跟踪性能问题。

> 注意：
>
> 创建组时，您可以将角色分配给组，提供对组的应用程序级访问权限，并将用户分配到组。Citrix ADM 分析现在支持基于虚拟 IP 地址的授权。您的用户现在只能看到他们被授权的应用程序（虚拟服务器）的所有见解报告。有关组和向组分配用户的详细信息，请参阅 配置组。

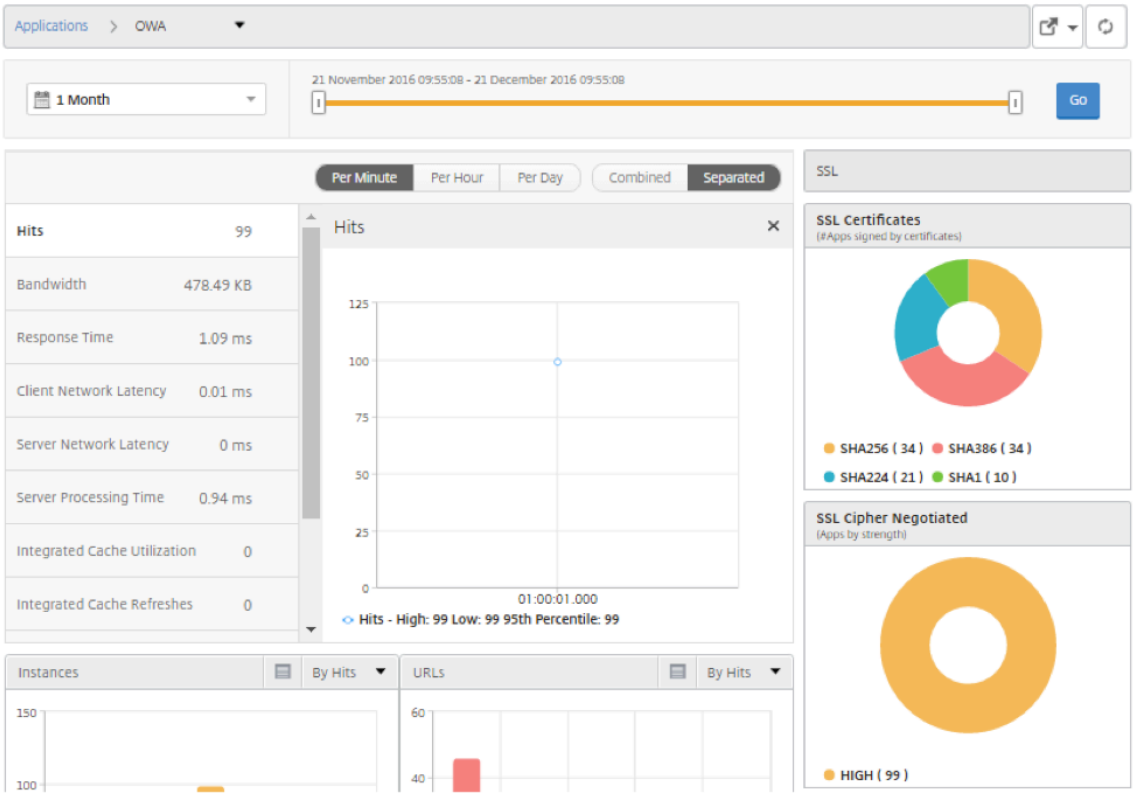
要在 **Citrix ADM** 中监视 **SSL** 智能分析度量，请执行以下操作：

1. 在 “ 分析” 选项卡上，导航到 Web Insight，然后单击 “客户 端”、“ 服务器” 或 “应用 程序” 节点，以分别显示有关客户端、服务器或应用程序的度量。
2. 在左上角窗格中，从期间列表中选择要显示其指标的时间范围。可以使用时间范围滑块自定义时间范围。单击转到。
3. SSL Insight 指标将以饼图形式显示，您可以单击这些图表以了解更多详细信息。

> 注意
>
> 饼图显示所有应用程序、客户端或服务器的度量。



4. 要显示特定应用程序、客户端或服务器的详细信息，请单击条形图上的相应值。



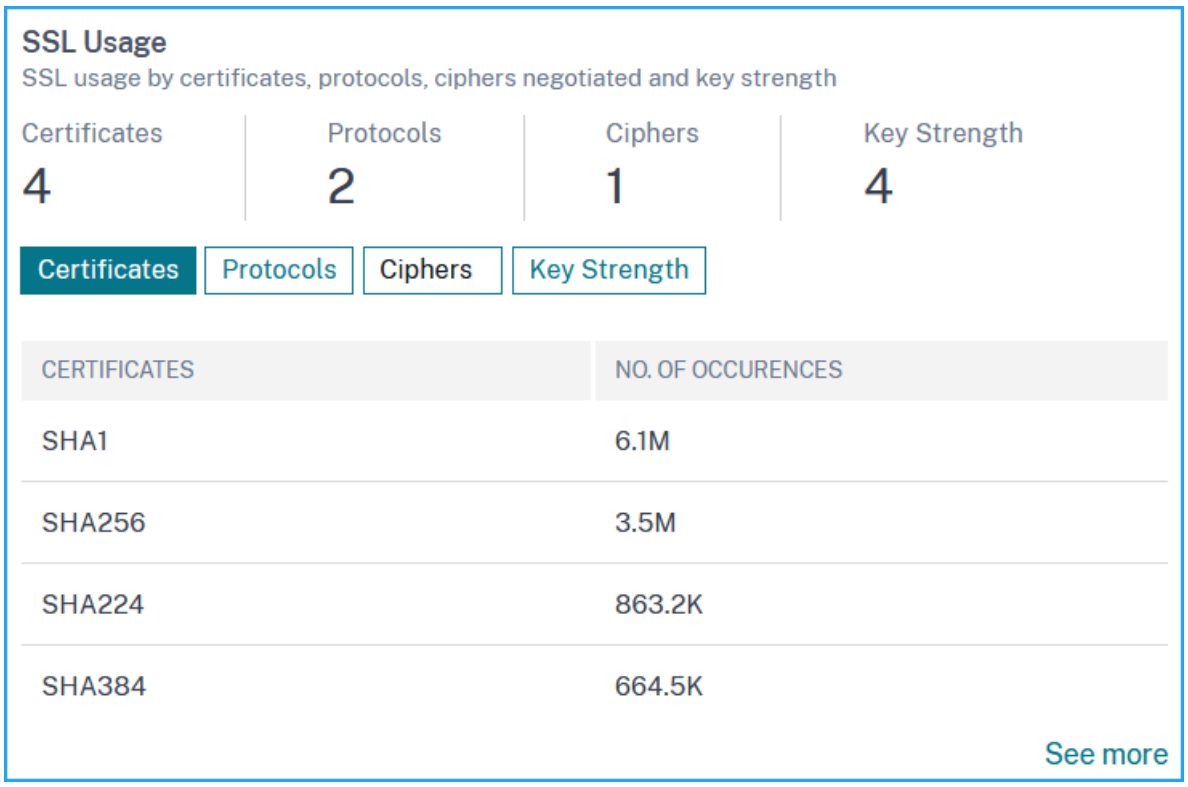
5. 要查看失败的 SSL 事务，请在“SSL”部分中选择单选按钮。

使用案例：获取应用程序、客户端或服务器的 **SSL** 事务概览

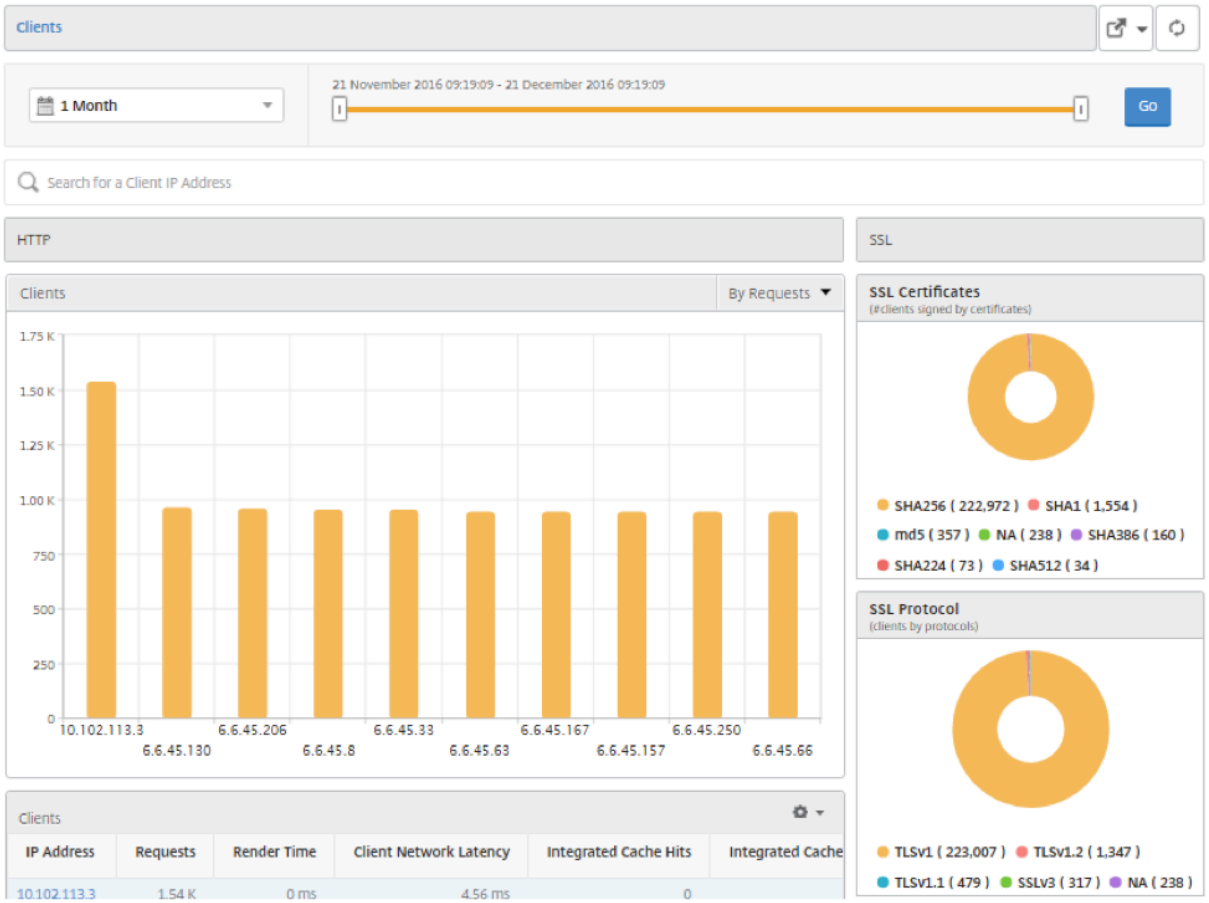
以下用例说明了如何使用 SSL Insight 来评估应用程序、客户端和服务器中的各种 SSL 参数的使用情况，以及改进安全措施。

请考虑您有一组使用 SSL 事务 (HTTPS) 进行通信的应用程序，并且您已将 Citrix ADM 配置为监视 SSL 组件。您可能需要频繁查看应用程序，以便可以首先关注最需要注意的应用程序。SSL 见解仪表板提供了应用程序在您选择的一段时间内以及针对所选 Citrix ADC 设备使用的各种 SSL 参数的摘要。具体如下：

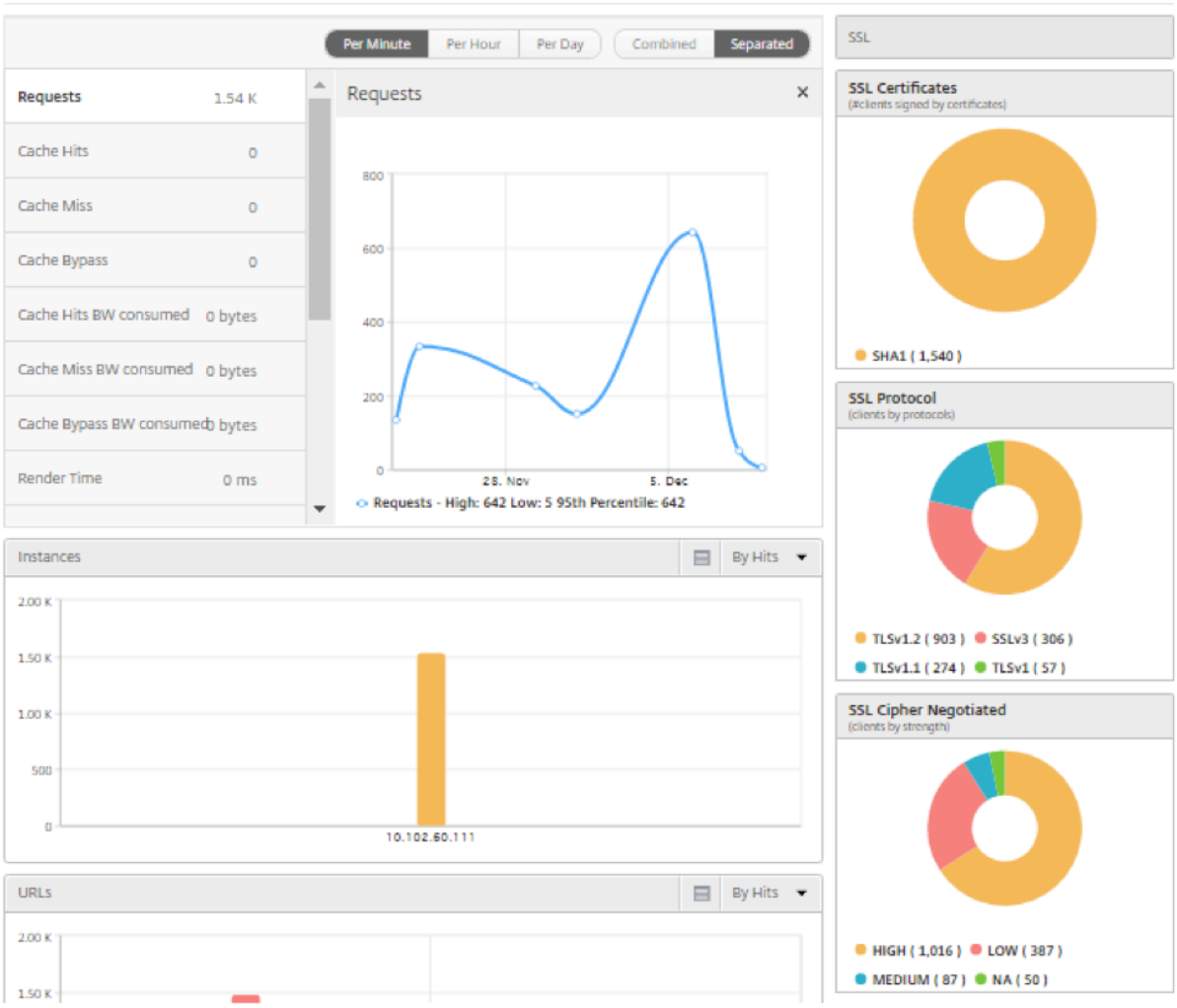
- SSL Certificates（SSL 证书）
- SSL Protocols（SSL 协议）
- SSL Cipher Negotiated（协商的 SSL 密码）
- SSL Key Strength（SSL 密钥强度）
- SSL 失败 — 前端
- SSL 失败 — 后端



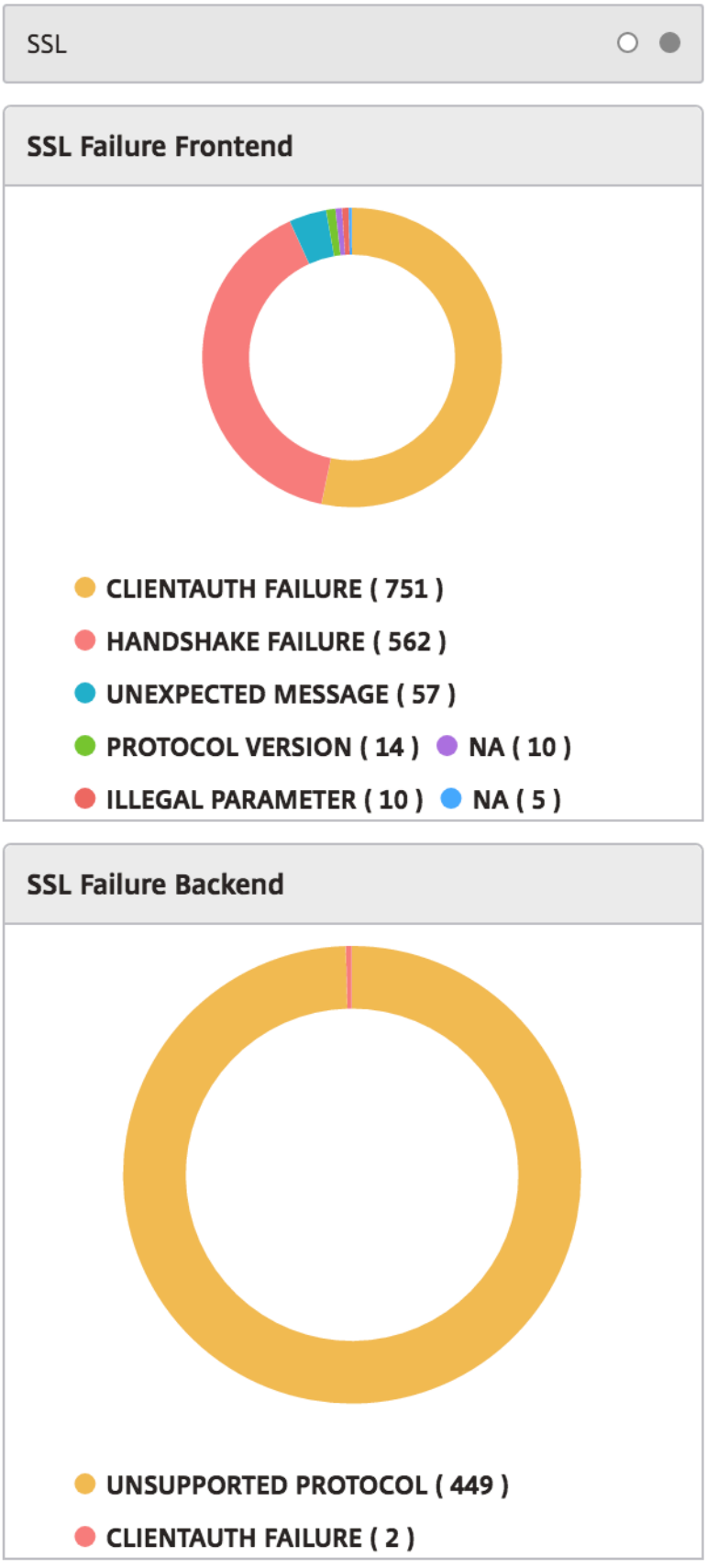
在以下示例中，您可以看到客户端列表（按其 IP 地址标识）和每个客户端的 SSL 命中数。此外，在右侧，可以看到所有客户端的 SSL 参数。



要显示某个客户端的 SSL 详细信息，请在条形图中或在图形下面的表中选择该客户端。在以下示例中，所选客户端的事务使用 SHA1 SSL 证书和四个主要协议：TLSV1.3、TLSV1.2、TLSV1.1、TLSV1 和 SSLv3。您还可以看到协商了各种强度的密码。颜色编码指示 SSL 协议的强度，为您提供有关弱密码和强密码的信息。



同样，要查看有关失败的 SSL 事务的信息，请选择 **SSL** 部分上的单选按钮。SSL 前端和后端故障分别显示在两个饼图中。在以下示例中，您可以查看主要的后端 SSL 错误是握手失败和主要前端 SSL 错误是非法参数。



TCP Insight

April 23, 2021

Citrix Application Delivery Management (ADM) 的 TCP Insight 功能提供了一个简单且可扩展的解决方案，用于监视 Citrix ADC 设备中使用的优化技术和拥塞控制策略（或算法）的衡量指标，以避免数据传输中的网络拥堵。此功能使用“TCP 速度报告”功能，即衡量在采用和不采用 TCP 优化的情况下的 TCP 文件下载或上载性能。

您可以查看关键的 传输层指标（如数据量、吞吐量和速度），并使用该信息衡量 Citrix ADC 实例提供的流量并验证 TCP 优化的优势。为上述指标提供了按流方向（从客户端到 Citrix ADC，从 Citrix ADC 到源服务器）、TCP 端口和虚拟局域网的细分。

必备条件

在开始配置 TCP Insight 功能之前，请务必满足以下必备条件：

- Citrix ADC 实例正在软件版本 11.1 版本 51.21 或更高版本上运行。
- 您已安装在软件版本 11.1 版本 51.21 或更高版本上运行的 Citrix ADM。
- 为应用程序配置的所有虚拟服务器都已获得许可，以便在 Citrix ADM 上进行管理和监视。
  有关 Citrix ADM 许可的信息，请参阅 许可。

启用 **TCP Insight**

您必须在 Citrix ADM 上启用该功能，然后才能查看 TCP 智能分析度量。

要启用 **TCP** 见解：

1. 在 Web 浏览器中，键入 Citrix ADM 虚拟设备的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到分析 > 设置，然后单击启用分析功能。
4. 在启用分析功能页面上，选择启用 **TCP Insight**。
5. 在确认窗口中，单击确定。

查看 **Citrix ADM** 中的 **TCP** 智能分析度量

在 Citrix ADM 中启用 TCP Insight 后，您可以查看关键传输层信息，如流量模式（Internet 或移动数据）、数据量、吞吐量、接口、端口、平均上传速度、平均下载速度。

要在 **Citrix ADM** 中显示 **TCP** 智能分析度量，请执行以下操作：

导航到 **Analytics**（分析）> **TCP Insight**。

您可以将鼠标指针悬停在条形图上，以查看相应传输技术的数据量。此外，您还可以在图形下面的表中查看数据量和其他指标。

> 注意您可以使用表中的设置图标自定义图表中显示的指标。您还可以选择指标所属的时间段，以及使用时间滑块调整时间段。

您还可以通过从 **“ TCP 智能分析”** 列表中进行选择，查看接口、端口和比特率等指标。

用例

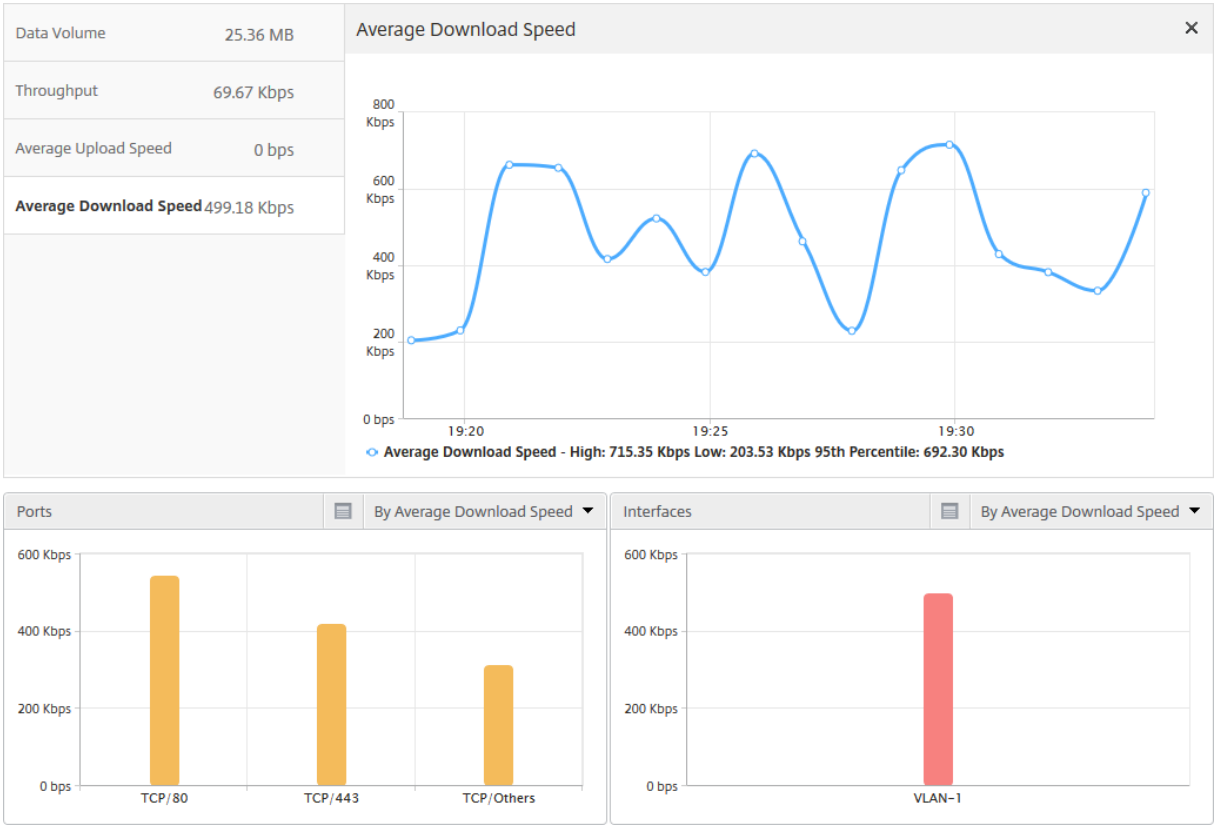
以下使用案例说明了在 Citrix ADC 装置上使用 TCP 智能分析的一些方法：

- 评估 TCP 优化的好处
- 调整 TCP 参数
- 衡量 TCP 优化对流量的影响

评估 **TCP** 优化的好处

Citrix ADC TCP 优化实际上对移动（无线电）或企业网络（互联网）有多大好处。您可以查看通过 TCP 进行的数据传输的速度，以及比较未优化性能和优化性能。这些衡量指标按下载和上载方向（始终在无线/客户端上）以及按不同的目标端口（HTTP (80) 和 HTTPS (443)）单独显示。
通过检查 TCP Insight 指标，您可以量化通过优化 TCP 流获得的速度提升。

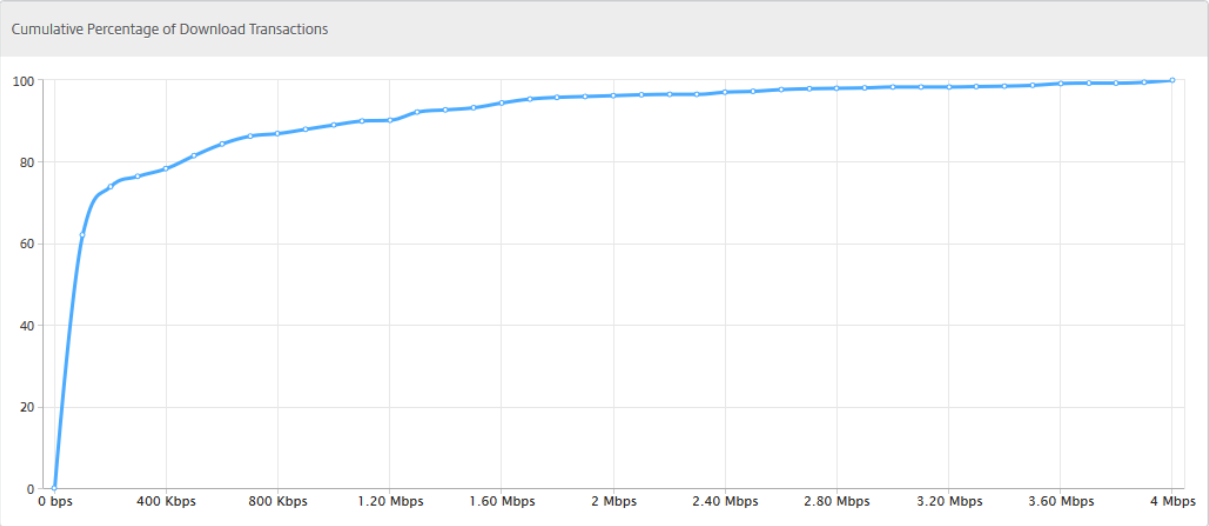
要查看这些参数的摘要，请登录 Citrix ADM 并单击 **TCP Insight** 选项卡。然后单击 **Sides**（端）并从条形图或图形下面的表中选择 **Internet** 或 **Radio**（无线）。



调整 **TCP** 参数

使用不同的 TCP 配置文件对同一流量可能会产生不同的输出。在这种情况下，您可能需要查看和比较 Citrix ADC 运行不同 TCP 优化配置文件的周期的速度测量值。您可以使用结果来调整 TCP 参数以提高传输速度，以及创建用于在特定的客户网络中实现最佳的用户感受体验的 TCP 配置文件。

要查看报告，请登录到 Citrix ADM。然后，在 **TCP Insight** 选项卡上，单击 比特率，然后从条形图或图表下方的表中选择所需的比特率。

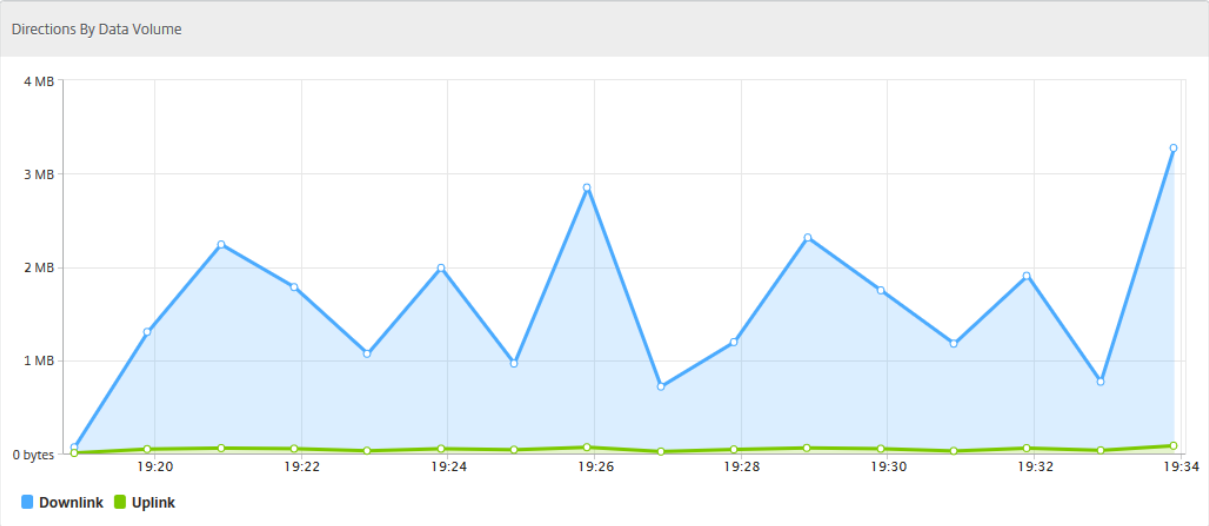


衡量 **TCP** 优化对流量的影响

Citrix ADC 实例处理的 IP 层数据容量/吞吐量测量可在不同时间段之间进行比较，以评估 TCP 优化对用户数据消耗的影响。可以按网络的各端（无线端和 Internet 端）、不同的流量段（按不同的接口或虚拟 LAN 区分）、每个方向（下行链路和上行链路）以及不同的目标端口（HTTP 和 HTTPS）单独应用衡量指标。可以使用比较来确认 TCP 优化是否促使订阅方使用更多数据。

有关衡量指标的摘要，请登录 Citrix ADM，在 **TCP Insight** 选项卡中，单击 **Sides**（端），然后从条形图或图形下面的表中选择 **Internet** 或 **Radio**（无线）。

您也可以从时间列表中选择不同的时间范围。可以使用时间范围滑块自定义时间范围。



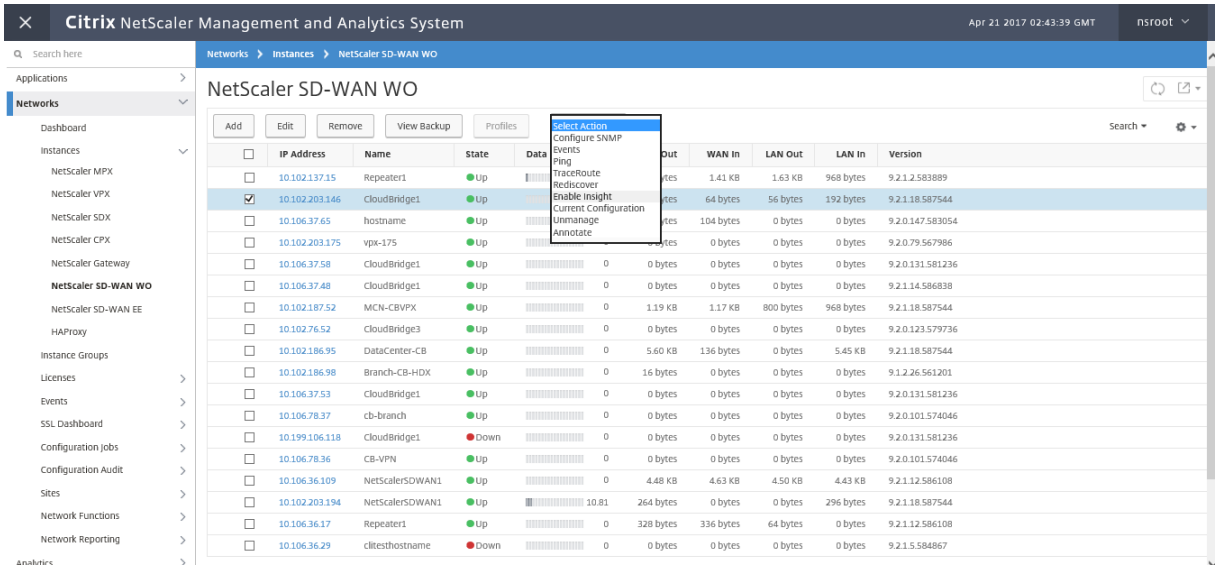
WAN Insight

April 23, 2021

Citrix SD-WAN 优化 (WO) 设备通过提高数据中心和分支站点之间网络中的数据流效率，优化了通过广域网交付许多应用程序的情况。

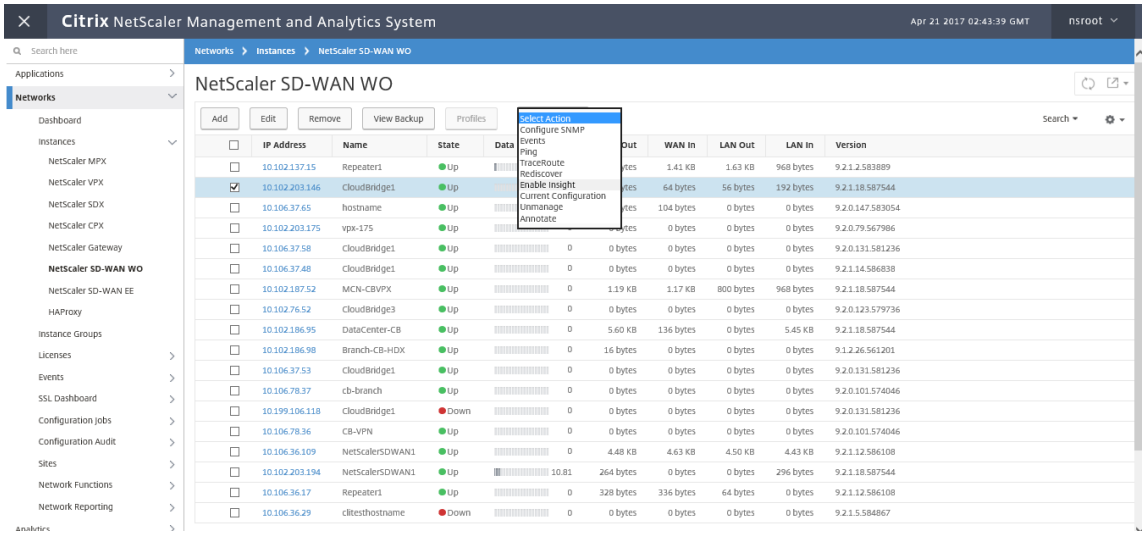
WAN Insight 分析使管理员能够轻松监控数据中心和分支广域网优化设备之间的加速和未加速的 WAN 流量。WAN Insight 提供了网络上的客户端、应用程序和分支机构的可见性，帮助有效地排除网络问题。实时报告和历史报告使您能够主动解决问题（如果有的话）。

通过在数据中心 WAN 优化设备上启用分析功能，Citrix ADM 能够收集数据并为数据中心和分支广域网优化设备提供报告和统计信息。



要在 **WAN** 优化设备上启用分析：

1. 导航到 网络 > 实例 > **Citrix SD-WAN**，然后选择 SD-WAN 实例。

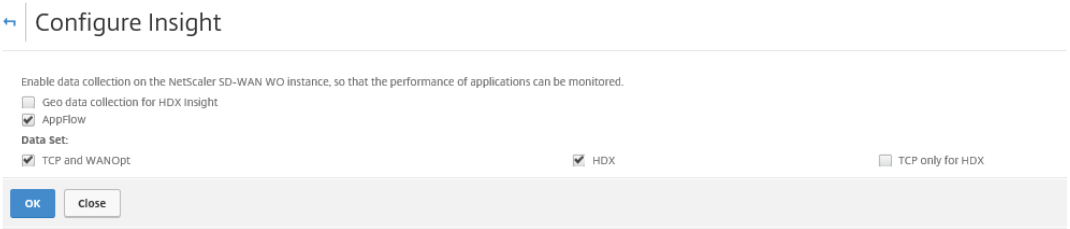


2. 从 **“选择操作”** 列表中，选择 “配置分析”。
3. 根据需要选择以下参数：

   -用 于 **HDX Insight** 的地理数据收集：与谷歌地理 API 共享客户端 IP 地址。

   - **AppFlow**：开始从广域网优化实例收集数据。

     - **TCP** 和 **Wanopt**：提供 **TCP** 和 **Wanopt** Insight 报告。
     - **HDX**：提供 HDX Insight 报告。
     - **TCP** 仅适用于 **HDX**：仅为 HDX Insight 报告提供 TCP。



4. 单击确定。

要查看 **WAN** 见解报告，请执行以下操作：

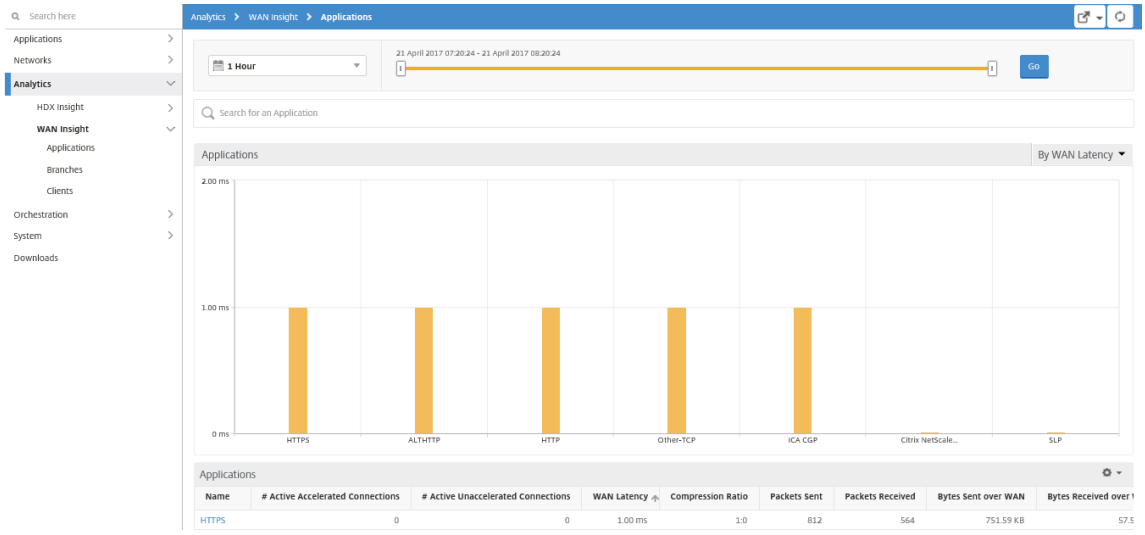
1. 导航到分析 > **WAN** 见解。

   > 注意
   >
   > 只有在将 SD-WO 实例添加到 Citrix ADM 后，才可见 WAN 智能分析选项。

您可以查看以下报告：

- 应用程序 -显示所选持续时间内所有应用程序的使用情况和性能统计信息。
- 分支机构 -显示所有 WAN 优化分支机构设备的使用情况和性能统计信息。

- 客户端 -显示每个分支中访问 WAN 优化设备的所有客户端的使用情况和性能统计信息。



显示以下指标：

指标	说明
Active Accelerated Connections（活动加速连接）	加速的活动 WAN 连接数。
Active Unaccelerated Connections（活动未加速连接）	未加速的活动 WAN 连接数。
WAN 延迟	用户与应用程序交互时遇到的延迟（以毫秒为单位）。
Compression Ratio（压缩比）	在选定持续时间内，分支办公室和数据中心设备之间的数据压缩比率。
Packets Sent（发送的数据包数）	在选定的持续时间内 WAN 优化设备通过网络发送的数据包数。
Packets Received（接收的数据包数）	在选定的持续时间内 WAN 优化设备从网络接收的数据包数。
Bytes Sent over WAN（通过 WAN 发送的字节数）	Citrix WAN 优化设备在选定持续时间内通过 WAN 发送的字节数。
Bytes Received over WAN（通过 WAN 接收的字节数）	在选定的持续时间内 WAN 优化设备从 WAN 接收的字节数。
LAN RTO	在选定的持续时间内 WAN 优化设备向 LAN 重新传输超时的次数。
WAN RTO	在选定的持续时间内 WAN 优化设备向 WAN 重新传输超时的次数。
Retransmit Packets (LAN)（重新传输数据包 (LAN)）	在选定的持续时间内 WAN 优化设备向 LAN 网络重新传输的数据包数。

指标	说明
Retransmit Packets (WAN)（重新传输数据包 (WAN)）	在选定的持续时间内 WAN 优化设备向 WAN 网络重新传输的数据包数。

Video Insight

April 23, 2021

Video Insight 功能提供了一个简单且可扩展的解决方案，用于监视 Citrix ADC 设备使用的视频优化技术的指标，从而改善客户体验和运营效率，从而提供以下优势：

- 在高峰时段出现拥堵时管理网络。
- 改进视频播放连贯性并降低视频停顿。
- 支持新的视频服务方案（例如 Binge-on 视频服务）。
- 支持客户选择持续性最佳的视频质量。
- 为订阅方提供一致的用户体验。

在优化视频流量的同时，Citrix ADC 设备使用特殊机制来动态调节视频比特速率，并使用随机采样技术来估算优化技术节省的成本。有关 Citrix ADC 视频优化功能的详细信息，请参阅 视频优化。将 Citrix ADC 装置与 Citrix Application Delivery Management (ADM) 集成后，它会从通过 Citrix ADC 装置流动的视频数据中收集关键信息。您可以使用此信息比较 ABR 视频流量的优化性能和未优化性能，以及确定由于优化产生的节省等。

> 注意
>
> Citrix ADM 中提供的未优化会话的统计信息与您在 Citrix ADC 设备中选择的随机采样会话相对应。有关随机采样的详细信息，请参阅视频优化。

Citrix ADM 中的视频洞察提供了以下类型的视频流量的指标：

- 通过 HTTP 进行的渐进式下载 (PD) 视频
- 通过 HTTP 进行的 ABR 视频
- 通过 HTTPS 进行的 ABR 视频
- 通过 QUIC 进行的 YouTube ABR 视频

配置 Video Insight

> 注意
>
> 使用 Citrix ADC 高级许可证的 Citrix ADC 实例支持视频分析。Citrix ADC 高级许可证受到 Citrix ADC 电信平

> 台（VPX T1000 和 VPX-T）的支持。

要在 Citrix ADC 实例上配置视频洞察，请首先启用 AppFlow 功能，配置 AppFlow 收集器、操作和策略，然后全局绑定策略。配置收集器时，必须指定要监视报告的 Citrix ADM 服务器的 IP 地址。

要在 Citrix ADC 实例上配置视频洞察，请运行以下命令来配置 AppFlow 配置文件和策略，并在全局范围内绑定 AppFlow 策略。

add appflow collector <name> **-IPAddress** <ipaddress> **-port** <port_number> **-Transport** logstream

设置应用程序流参数 -启用视频洞察

add appflow action <name> **-collectors** <string> **-videoAnalytics** ENABLED

add appflow policy <name> <rule> <action>

bind appflow global <policyName> <priority> [<gotoPriorityExpression>] [**-type** <type>]

enable ns mode `ulfd`

enable feature AppFlow

示例

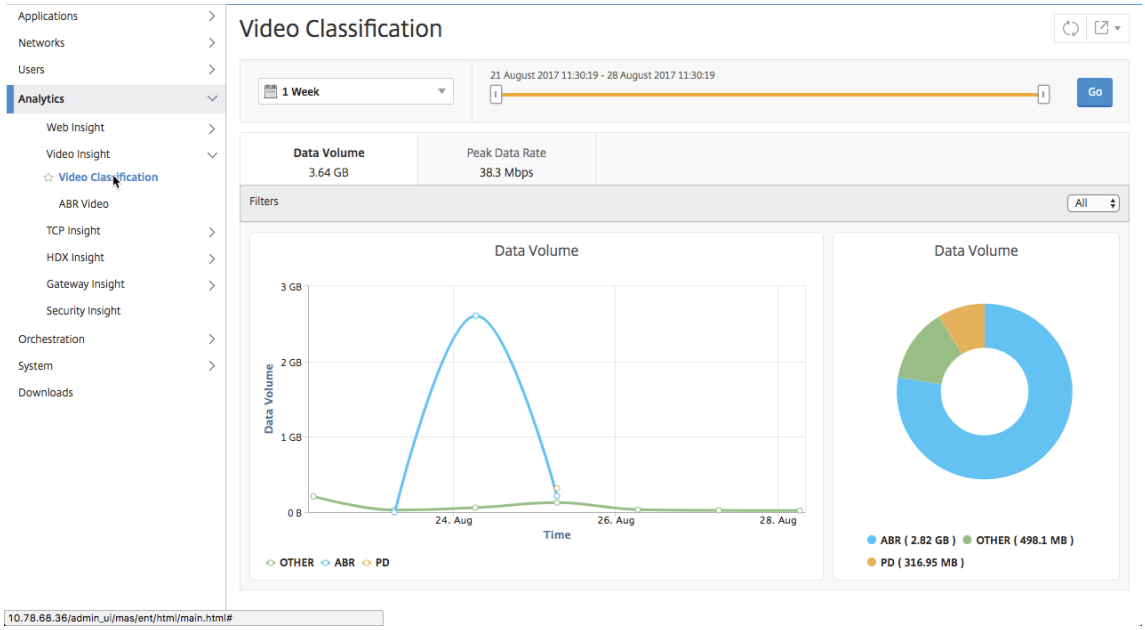
```
add appflow collector col1 -IPAddress 10.106.76.15 -port 5557 -
   Transport logstream
set appflow param -videoInsight ENABLED
add appflow action act1 -collectors col1 -videoAnalytics ENABLED
add appflow policy appol true act1
bind appflow global appol 1
enable ns mode ulfd
enable feature appflow
<!--NeedCopy-->
```

在 **Citrix ADM** 中查看视频智能分析度量

在 Citrix ADM 中启用“视频洞察”后，您可以查看视频优化指标，如视频分类、数据量、峰值数据速率和 ABR 视频播放。这些指标可帮助您分析您的网络和优化视频，以改进订阅方体验、操作效率及其他性能条件。

要在 **Citrix ADM** 中查看视频智能分析度量，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 虚拟设备的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 导航到 **Analytics**（分析）**> Video Insight**。



> 注意
>
> 图表中 OTE 图例提供 的值代表视频流量中的非 ABR 和非 PD 数据，具体取决于您选择的筛选器：
>
> - 全部 — 视频流量中非 ABR（HTTP、HTTPS 和 QUIC）和非 PD（HTTP）数据的总和。
> - **HTTP** — 视频流量中非 ABR 和非 PD 数据的总和。
> - **HTTPS** — 视频流量中非 ABR 视频数据的总和。
> - **QUIC** — 视频流量中非 ABR 视频数据的总和。

查看网络效率

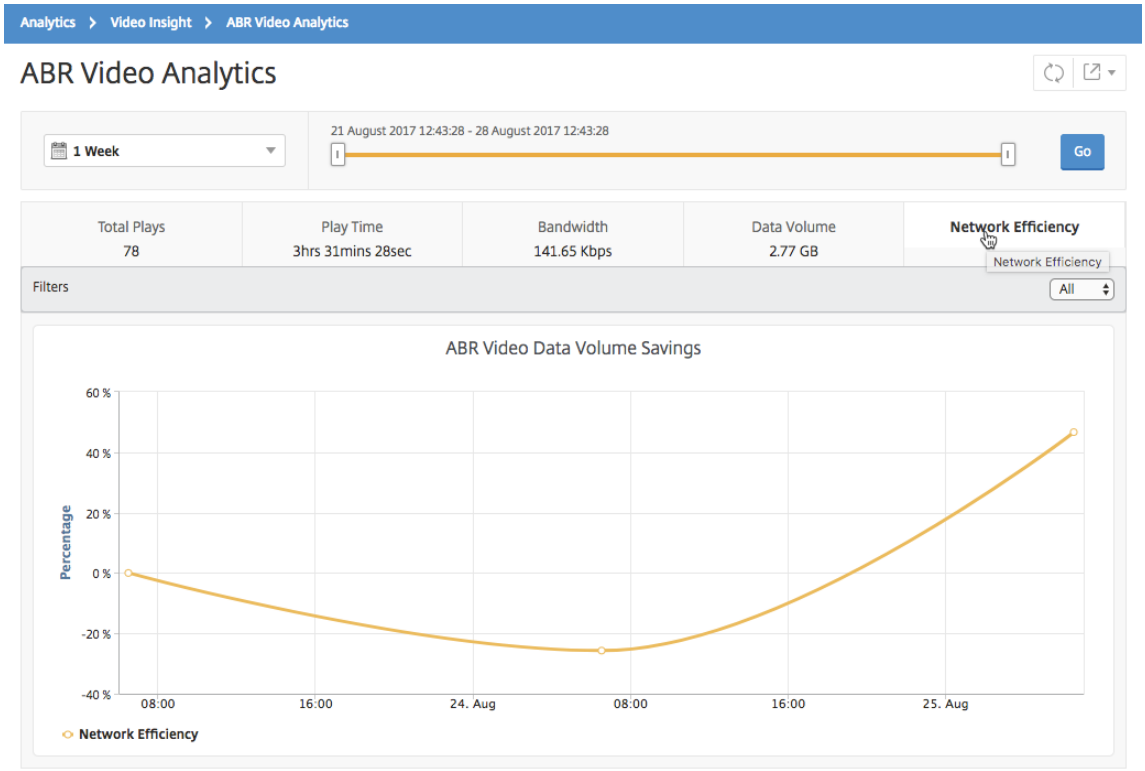
April 23, 2021

对于给定时间范围，Citrix Application Delivery Management (ADM) 提供了一个图表，其中显示了时间范围内优化视频会话与未优化视频会话的比率。它还显示通过优化节省的带宽百分比。节省的带宽百分比的计算公式如下：

节省的带宽百分比 = 优化 **ABR** 视频数据量平均值 **/** 未优化 **ABR** 视频数据量平均值。

要查看优化节省的带宽百分比，请执行以下操作：

1. 导航到分析 **>** 视频见解，然后单击 **ABR** 视频。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（继续），并选择 **Network Efficiency**（网络效率）选项卡。



比较优化和未优化 **ABR** 视频使用的数据量

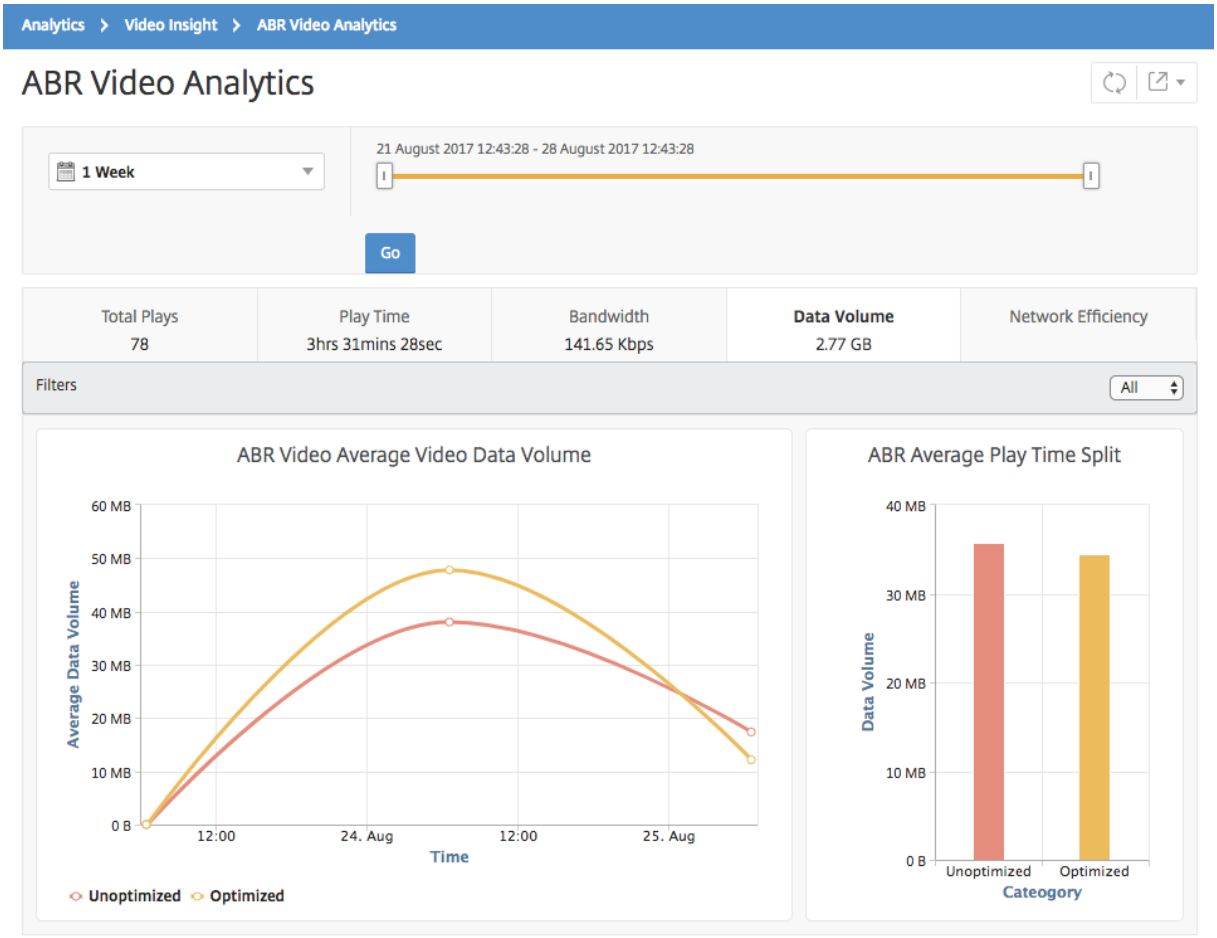
April 23, 2021

在给定时间范围内，Citrix Application Delivery Management (ADM) 会显示优化和未优化的 ABR 视频所使用的数据量，以便您可以比较这两个卷。

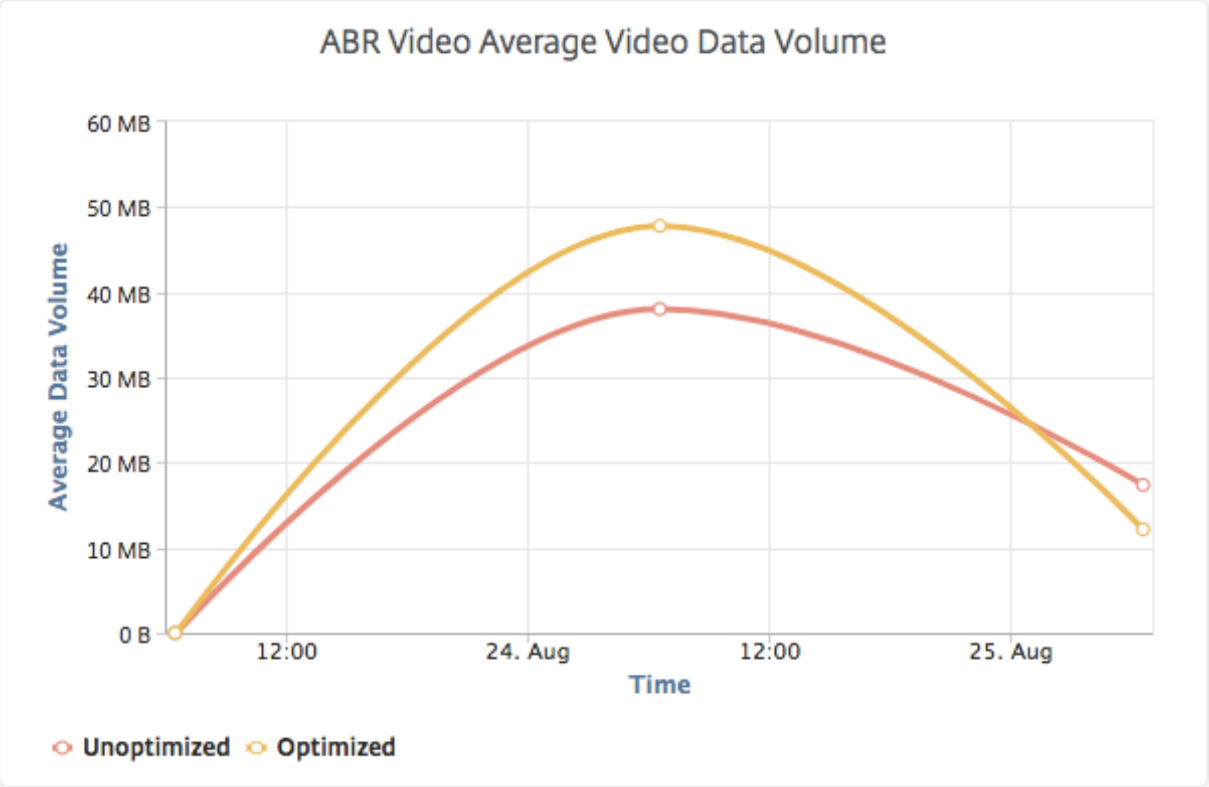
要查看 ABR 视频使用的数据量，请执行以下操作：

1. 导航到分析 **>** 视频见解，然后单击 **ABR** 视频。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（继续），并选择 **Data Volume**（数据量）选项卡。

您可以使用 **Filters**（过滤器）列表选择 HTTP、HTTPS 或 QUIC ABR 视频。



Data Volume（数据量）选项卡提供折线图和饼图，描述 ABR 视频使用的平均数据量，以及在选定的时间范围内在您的网络中优化和未优化 ABR 视频占用的数据量。您可以将鼠标指针悬停在折线图上以查看特定时间范围内使用的平均数据量：



查看流式传输的视频类型和网络消耗的数据量

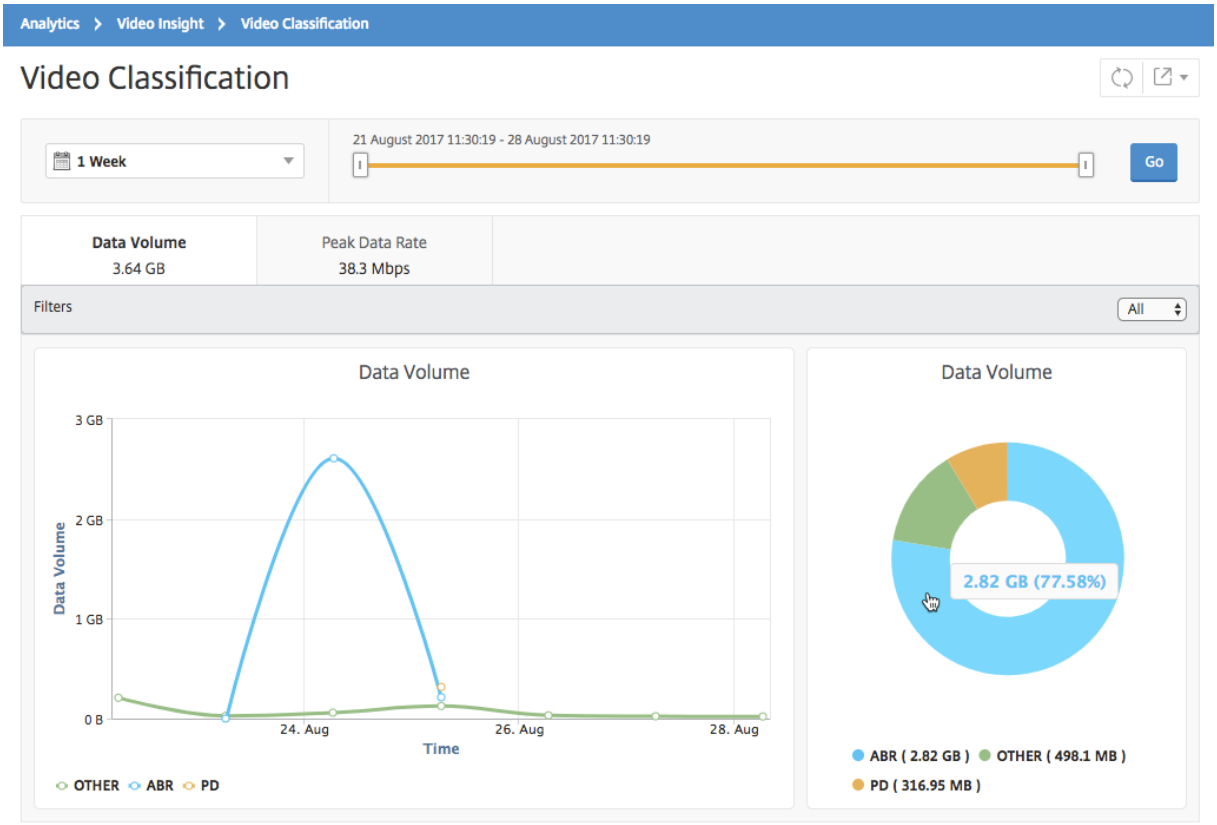
April 23, 2021

Citrix ADC 设备可检测网络中加密或未加密的视频流量以及视频流的类型（PD 或 ABR）。Citrix Application Delivery Management (ADM) 显示这些指标以及视频流量在定义的时间范围内消耗的数据量。

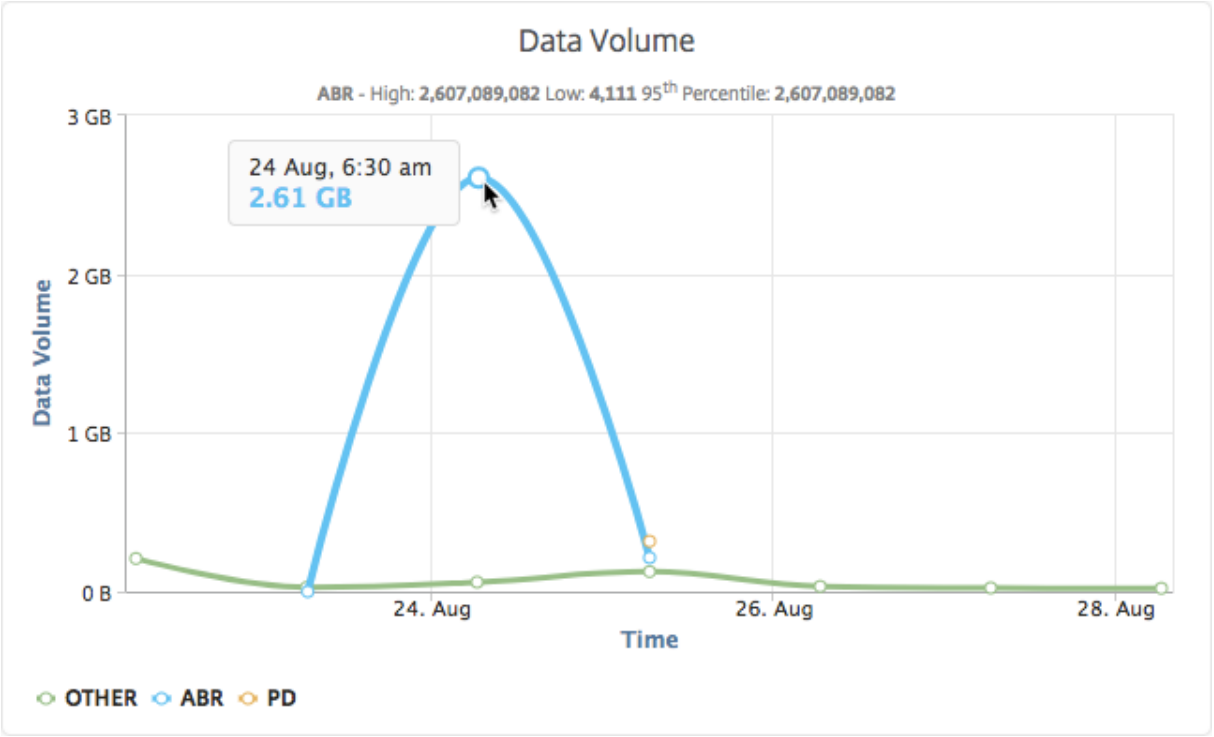
要查看视频类型和消耗的数据量，请执行以下操作：

1. 导航到分析 **>** 视频见解，然后单击视频分类。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击转到。

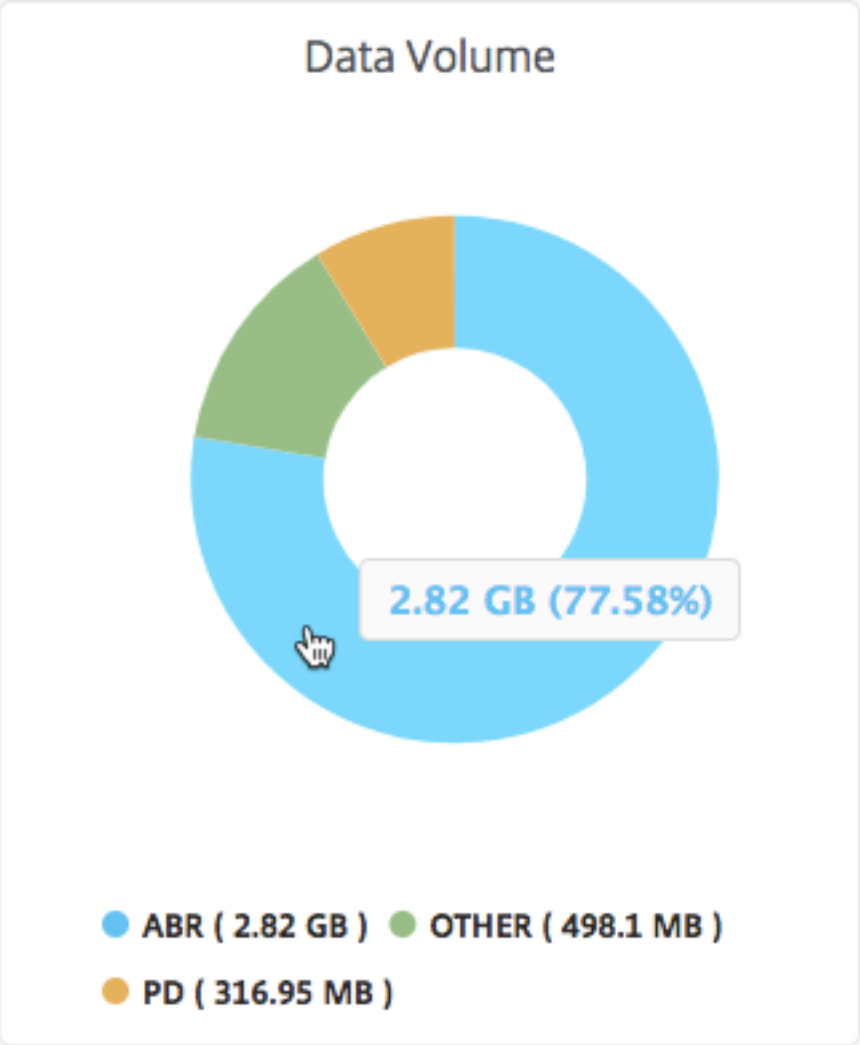
您可以使用 筛选器列表选择 HTTP、HTTPS 或 QUIC 流量。



Data Volume（数据量）选项卡提供折线图和饼图，显示从您的网络中通过流技术推送的视频流量类型，以及您的网络使用的数据量。您可以将鼠标指针悬停在折线图上以查看特定时间范围内使用的数据：



此外，您还可以将鼠标指针悬停在饼图上以查看特定类型的视频流量使用的数据量的百分比。



比较 **ABR** 视频的优化和未优化播放时间

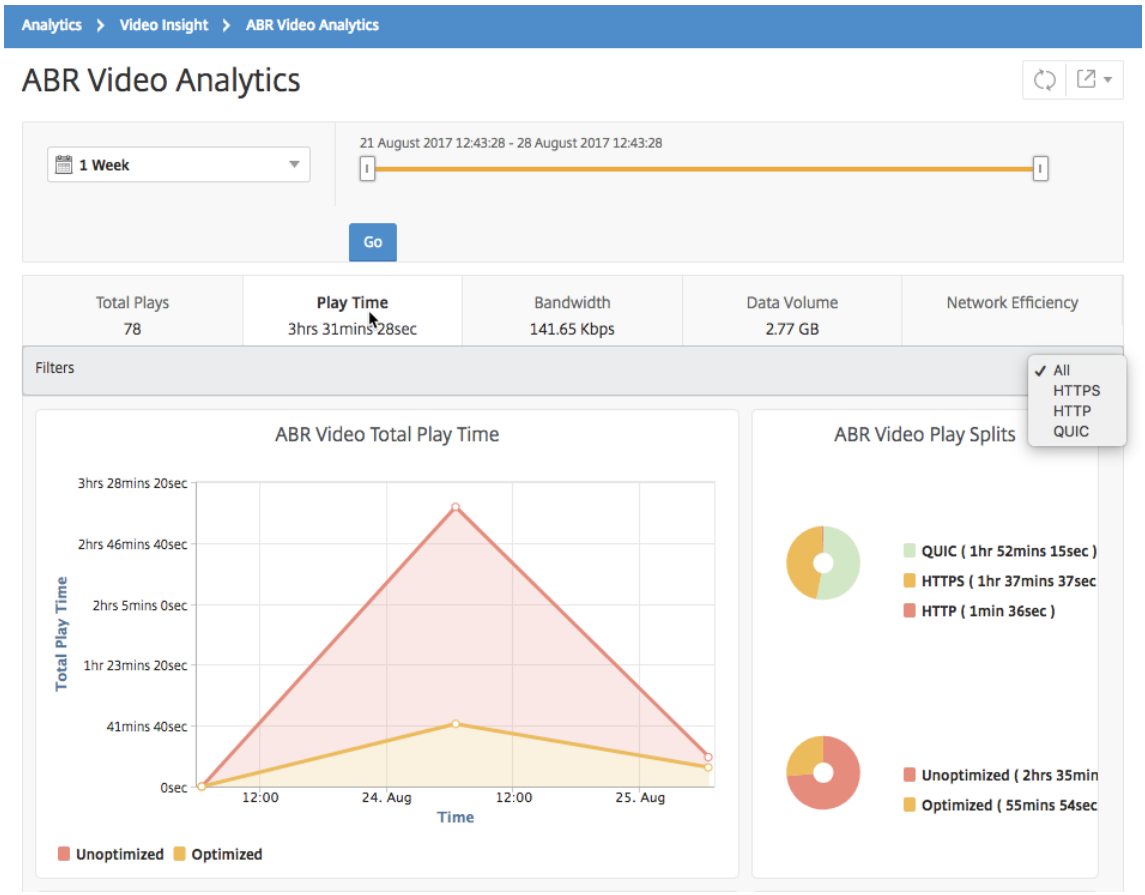
April 23, 2021

在给定时间范围内，Citrix Application Delivery Management (ADM) 提供 ABR 视频的播放时间，并使您能够比较网络中优化和未优化 ABR 视频的播放时间。

要查看播放时间，请执行以下操作：

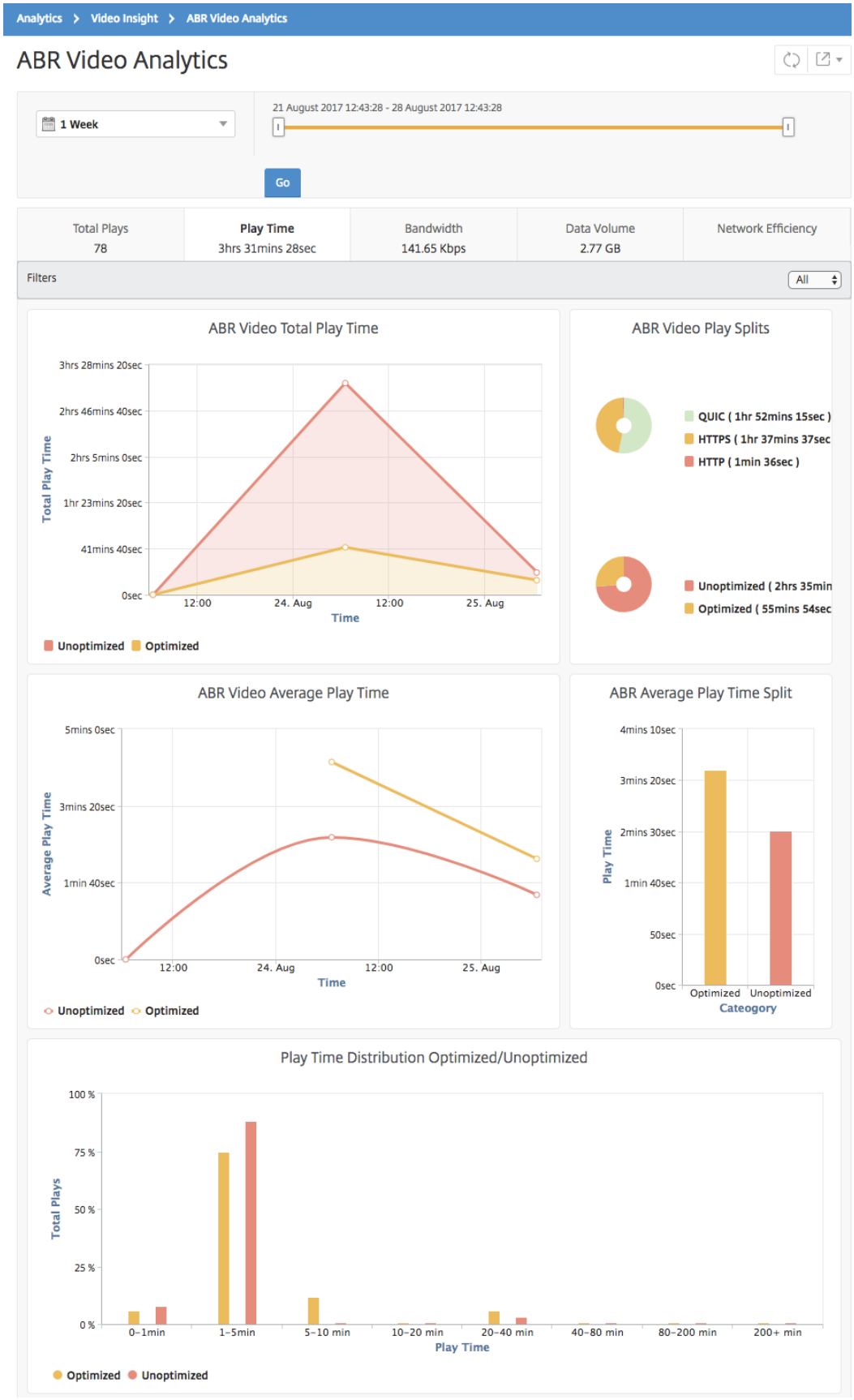
1. 导航到分析 **>** 视频见解，然后单击 **ABR** 视频。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（转到），并选择 **Play Time**（播放时间）选项卡。

您可以使用 **Filters**（过滤器）列表选择 HTTP、HTTPS 或 QUIC ABR 视频。



对于选定的时间范围，**Play Time**（播放时间）选项卡提供折线图和饼图，描述以下内容：

- 在您的网络中 ABR 视频的总播放时间
- 在选定时间范围内，优化和未优化的 ABR 视频播放的总播放时间
- 加密和未加密 ABR 视频的总播放时间
- ABR 视频的平均播放时间
- ABR 视频的优化播放和未优化播放的平均播放时间
- 加密和未加密 ABR 视频的平均播放时间
- 优化和未优化 ABR 视频之间的播放时间分布



比较优化和未优化 **ABR** 视频的带宽消耗

April 23, 2021

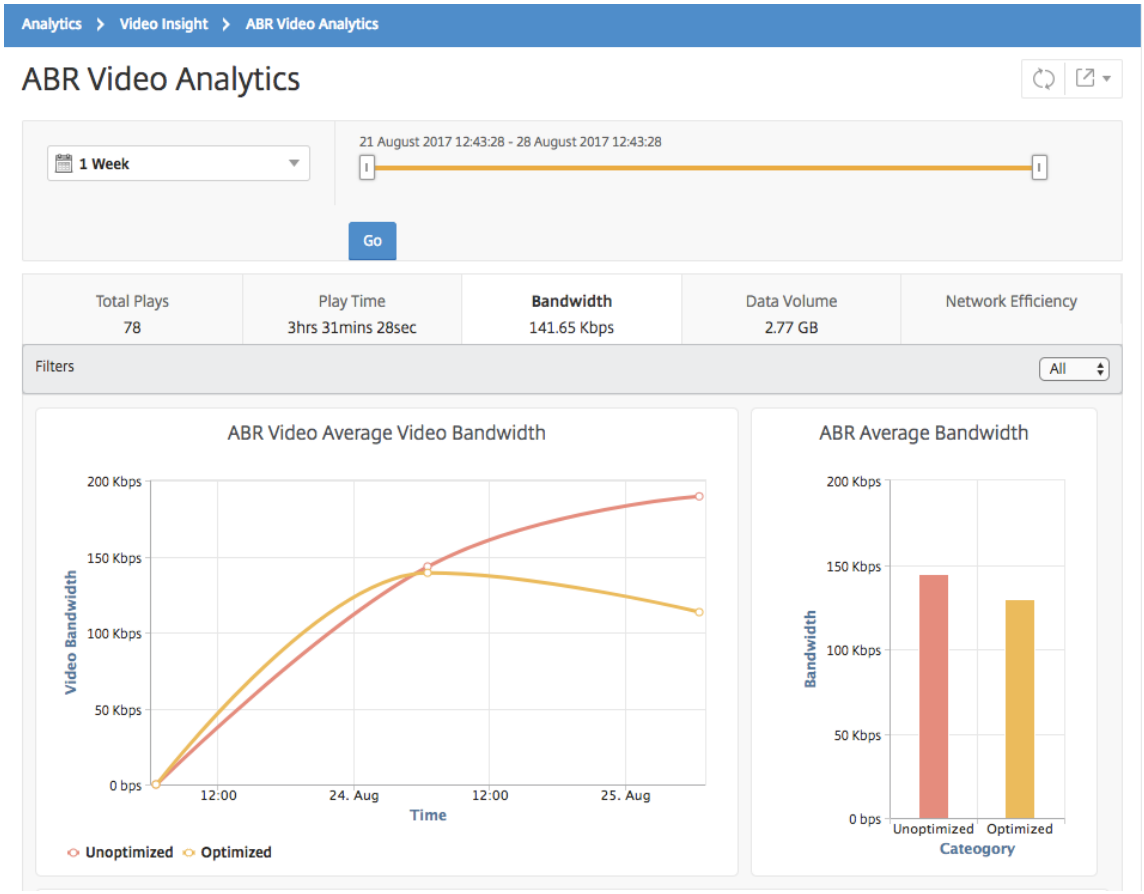
在给定的时间范围内，Citrix Application Delivery Management (ADM) 提供 ABR 视频的优化和未优化所消耗的带宽，还使您能够根据以下内容比较网络中优化和未优化 ABR 视频消耗的带宽：

- Play Time（播放时间）
- Data Volume（数据量）

要查看带宽消耗：

1. 导航到分析 **>** 视频见解，然后单击 **ABR** 视频分析。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（转到），并选择 **Bandwidth**（带宽）选项卡。

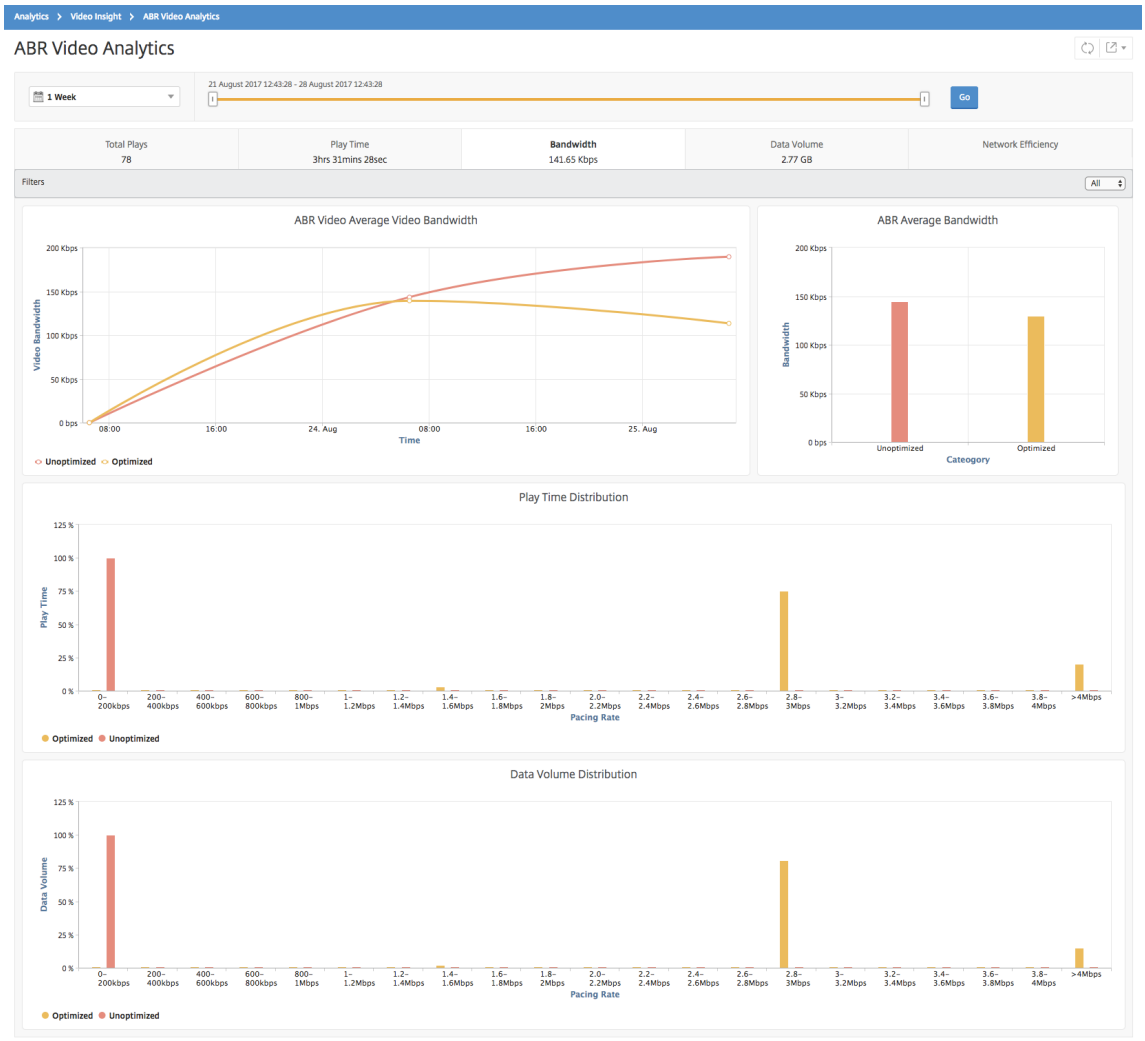
   您可以使用 筛选器列表选择 HTTP、HTTPS 或 QUIC ABR 视频。



对于选定的时间范围，**Bandwidth**（带宽）选项卡提供折线图和饼图，描述以下内容：

- 优化和未优化 ABR 视频占用的平均带宽。

- 基于优化和未优化 ABR 视频之间的播放时间分布占用的带宽。
- 基于优化和未优化 ABR 视频之间分布的数据量占用的带宽。



比较优化和未优化的 **ABR** 视频播放次数

April 23, 2021

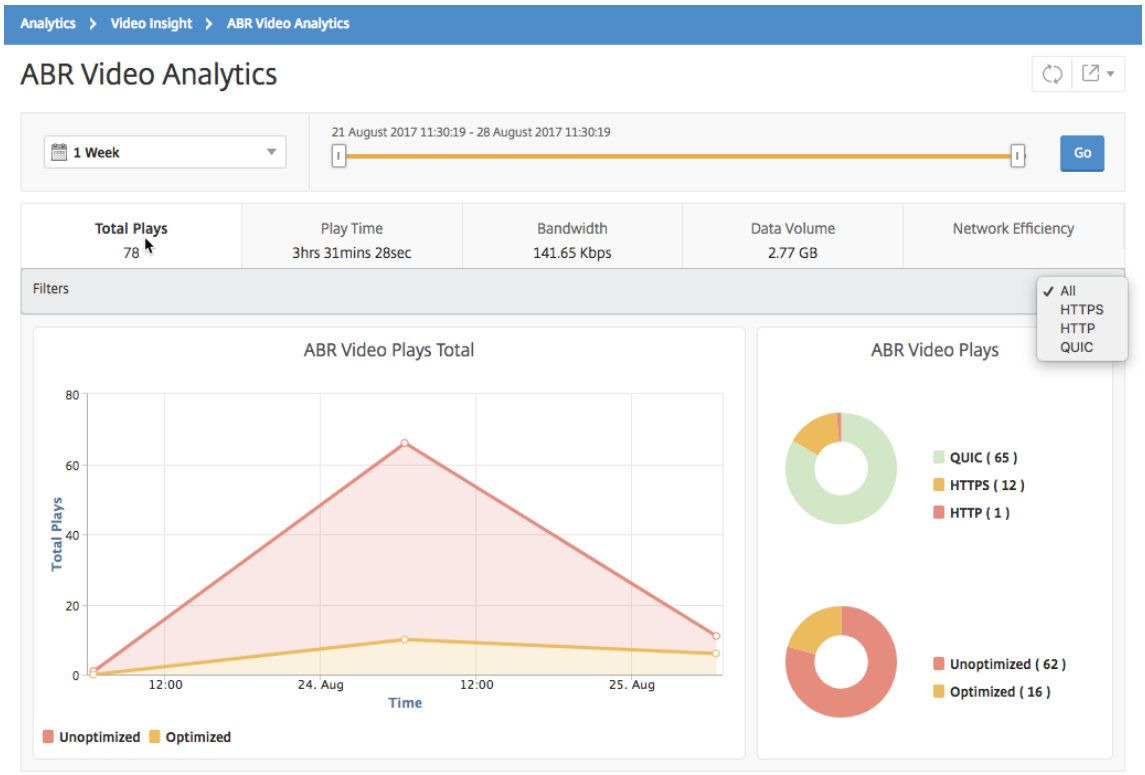
在给定时间范围内，Citrix Application Delivery Management (ADM) 会显示 ABR 视频的播放次数，并使您能够比较网络中优化和未优化播放次数。

要查看播放次数，请执行以下操作：

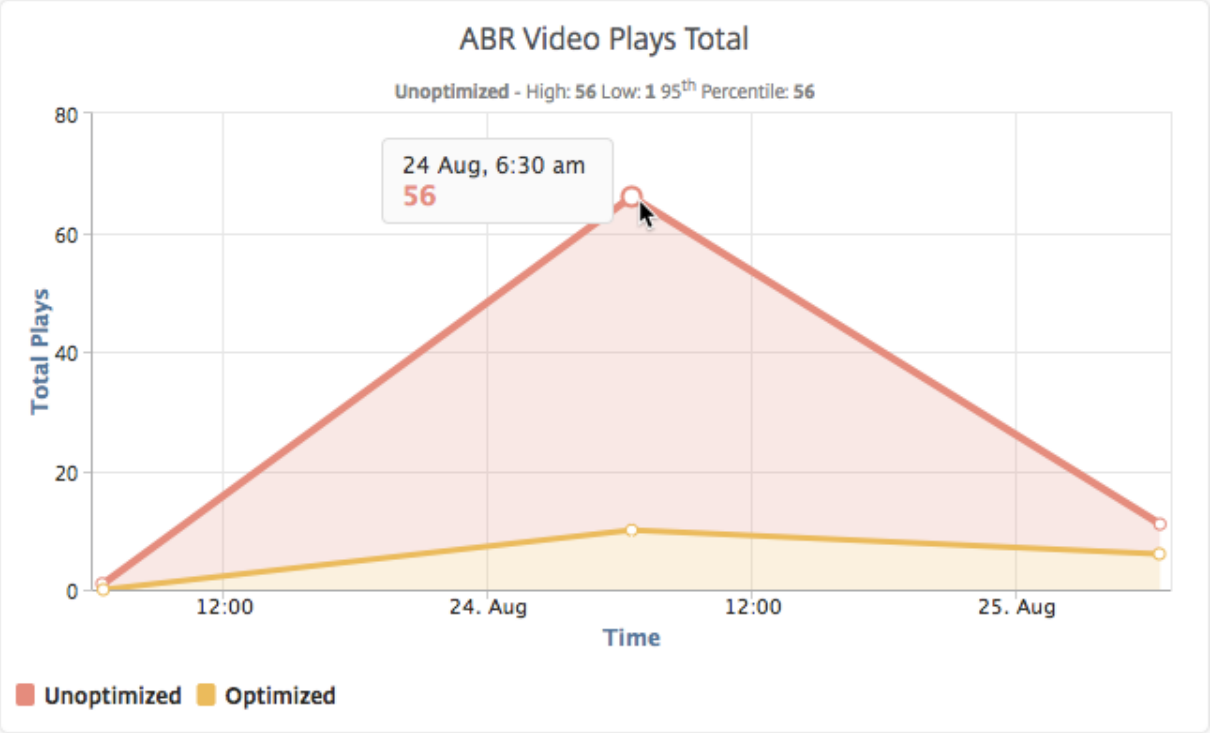
1. 导航到分析 **>** 视频见解，然后单击 **ABR** 视频分析。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。

3. 单击 **Go**（转到），并选择 **# of Plays**（播放数）选项卡。

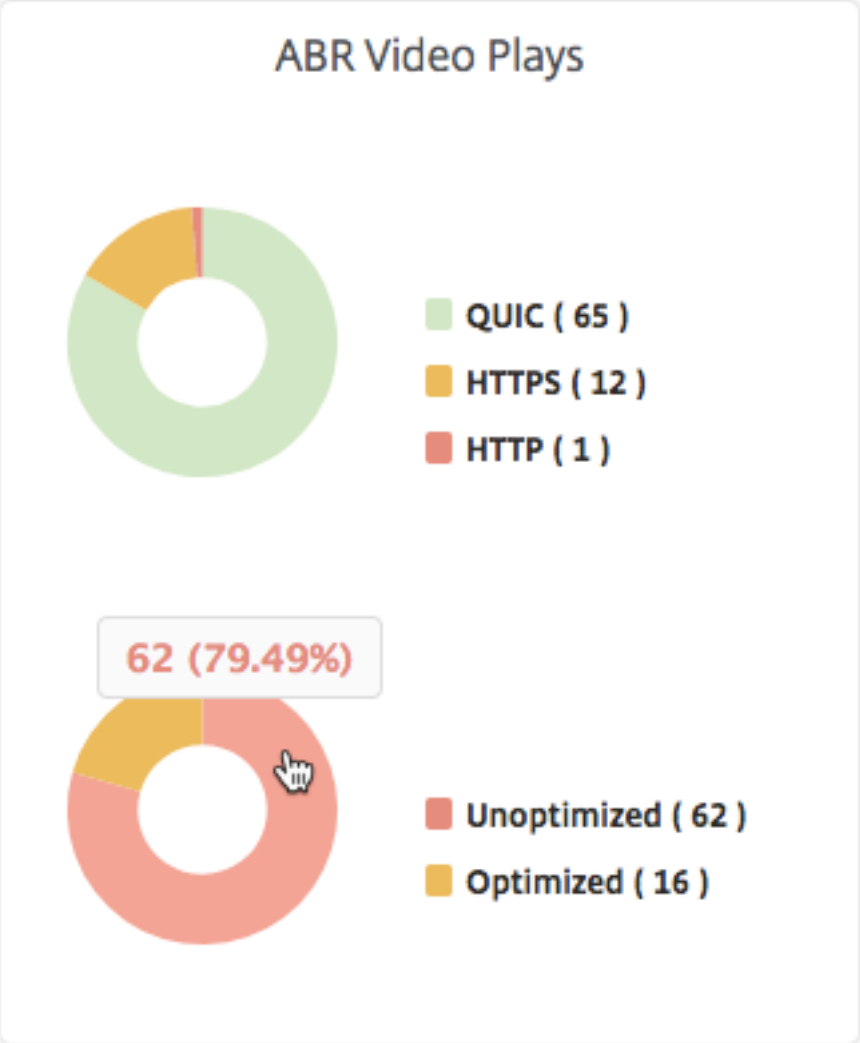
   您可以使用 **Filters**（过滤器）列表选择 HTTP、HTTPS 或 QUIC ABR 视频。



# of Plays（播放数）选项卡提供折线图和饼图，描述在您的网络中 ABR 视频的播放数，以及在选定的时间范围内在您的网络中 ABR 视频的优化和未优化播放数。您可以将鼠标指针悬停在折线图上以查看特定时间范围内的播放数：



此外，您还可以将鼠标指针悬停在饼图上以显示在选定的时间范围内优化和未优化播放的百分比以及加密和未加密 ABR 视频的百分比。



查看特定时间范围内的峰值数据速率

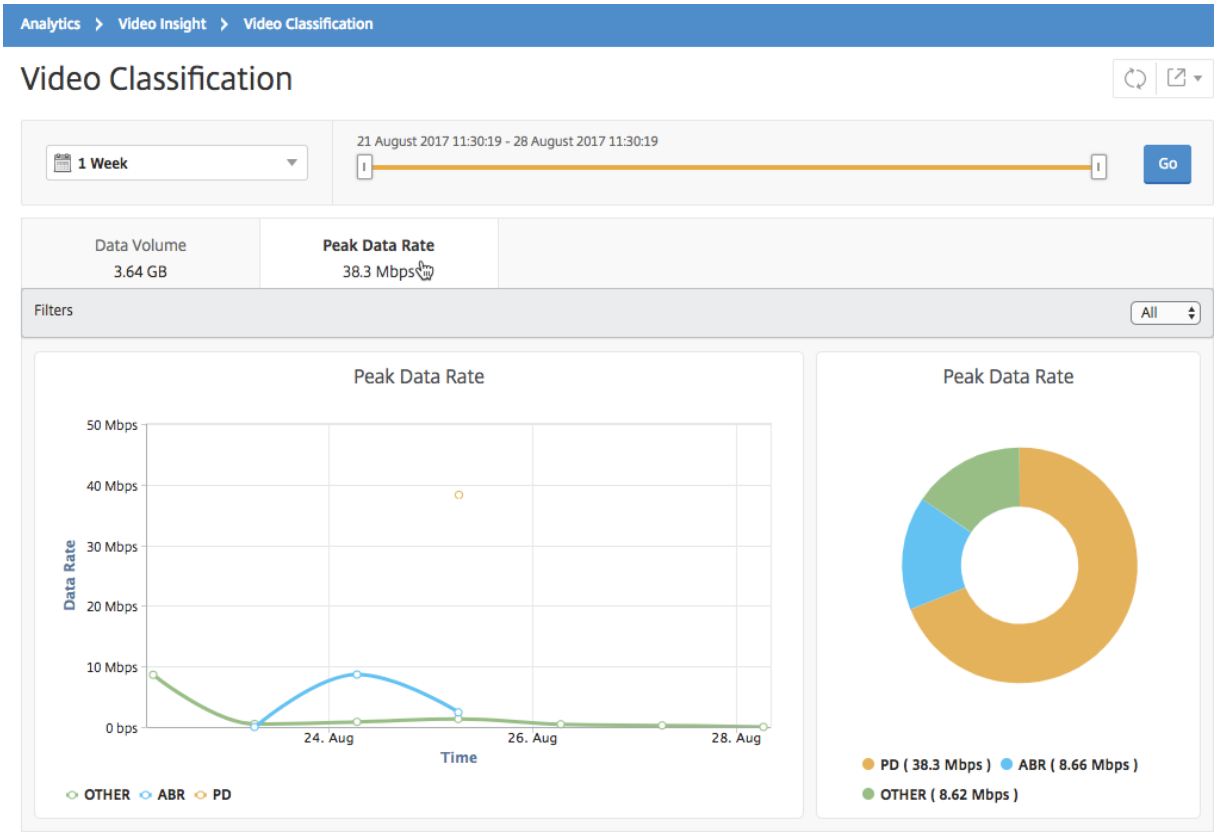
April 23, 2021

Citrix Application Delivery Management (ADM) 显示网络中视频流量的峰值吞吐量或数据速率。

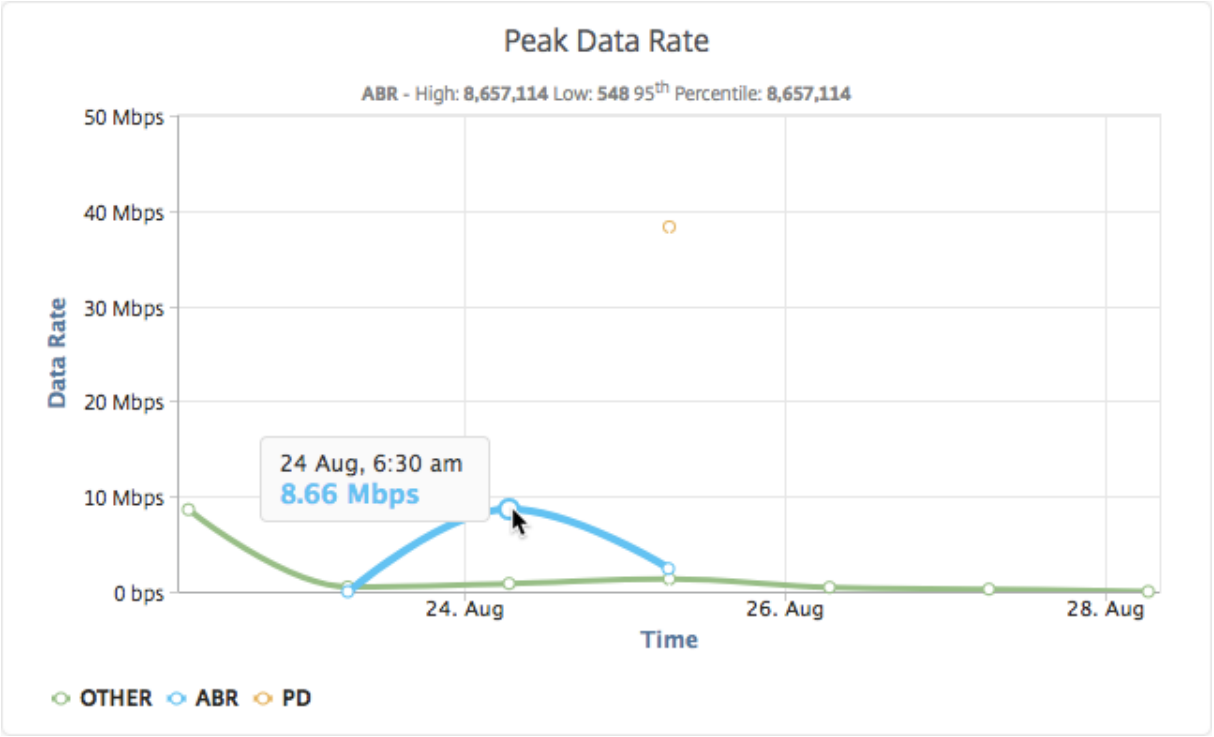
要查看视频流量的峰值数据速率，请执行以下操作：

1. 导航到分析 **>** 视频见解，然后单击视频分类。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（继续），并选择 **Peak Data Rate**（高峰数据速率）选项卡。

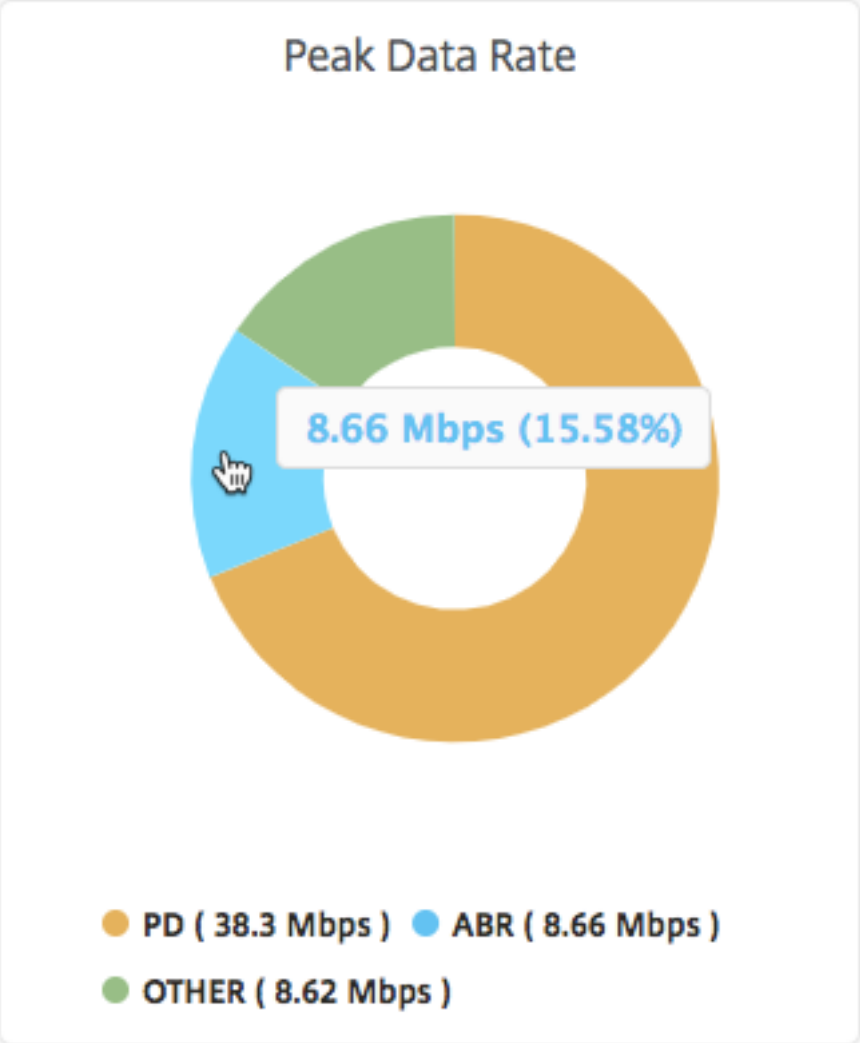
您可以使用 筛选器列表选择 HTTP、HTTPS 或 QUIC 流量。



Peak Data Rate（高峰数据速率）选项卡提供折线图和饼图，显示选定时间范围内从您的网络中通过流技术推送的视频流量类型的高峰数据速率，以及您的网络中视频流量的高峰数据速率。您可以将鼠标指针悬停在折线图上以显示特定时间范围内的高峰数据速率。



此外，您还可以将鼠标指针悬停在饼图上以显示选定时间范围内通过流技术推送的视频流量类型使用的高峰数据速率的百分比。



SSL 转发代理分析

April 23, 2021

位于企业网络边缘的 Citrix ADC 设备充当互联网代理。该设备可以在透明代理模式或显式代理模式下操作，提供拦截 Internet 流量（包括 HTTPS）的控制功能。拦截、跳过或阻止任何请求的决定是基于设备上配置的策略做出的。用户在登录企业网络之前会进行身份验证。所有请求和响应都会标记到用户，且用户活动会记录在设备中。有关详细信息，请参阅 Citrix SSL 转发代理。

将 Citrix Application Delivery Management (ADM) 与 Citrix ADC 装置集成时，会使用日志流将记录的用户活动和装置上的后续记录导出到 Citrix ADM。Citrix ADM 会整理和提供有关用户活动的信息，例如，所访问的 Web 站点和所占用的带宽。它还报告带宽使用和检测到的威胁，例如，恶意软件和钓鱼网站。您可以使用这些关键指标监视您的网络，并对 Citrix ADC 设备采取纠正措施。

要将 **Citrix ADC** 装置与 **Citrix ADM** 集成，请执行以下操作：

1. 在 Citrix ADC 设备上，配置 SSL 转发代理时，启用分析并提供要用于分析的 Citrix ADM 实例的详细信息。
2. 在 Citrix ADM 中，将 Citrix ADC 装置作为实例添加到 Citrix ADM 中。有关详细信息，请参阅将实例添加到 Citrix ADM。

控制板

April 23, 2021

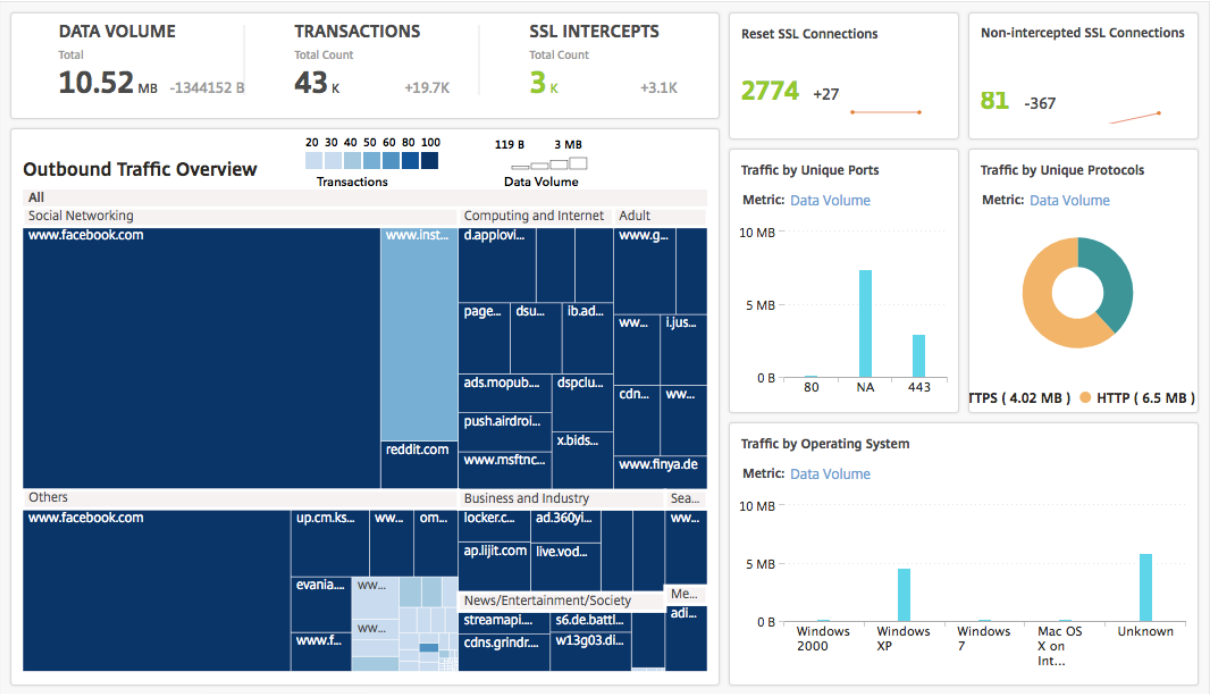
Citrix Application Delivery Management (ADM) 提供两个控制板，即出 站流量控制板和 用户控制板。这些控制板显示多个图表，这些图表汇总了从企业网络访问的 Web 站点或应用程序，以及您的网络中的用户执行的活动。

出站流量控制面板

出 站流量控制面板提供从网络访问的 URL 或域的摘要。它按事务数或 URL 或域使用的数据量提供所有 URL 或域的历史视图。
它还提供详细信息，例如：

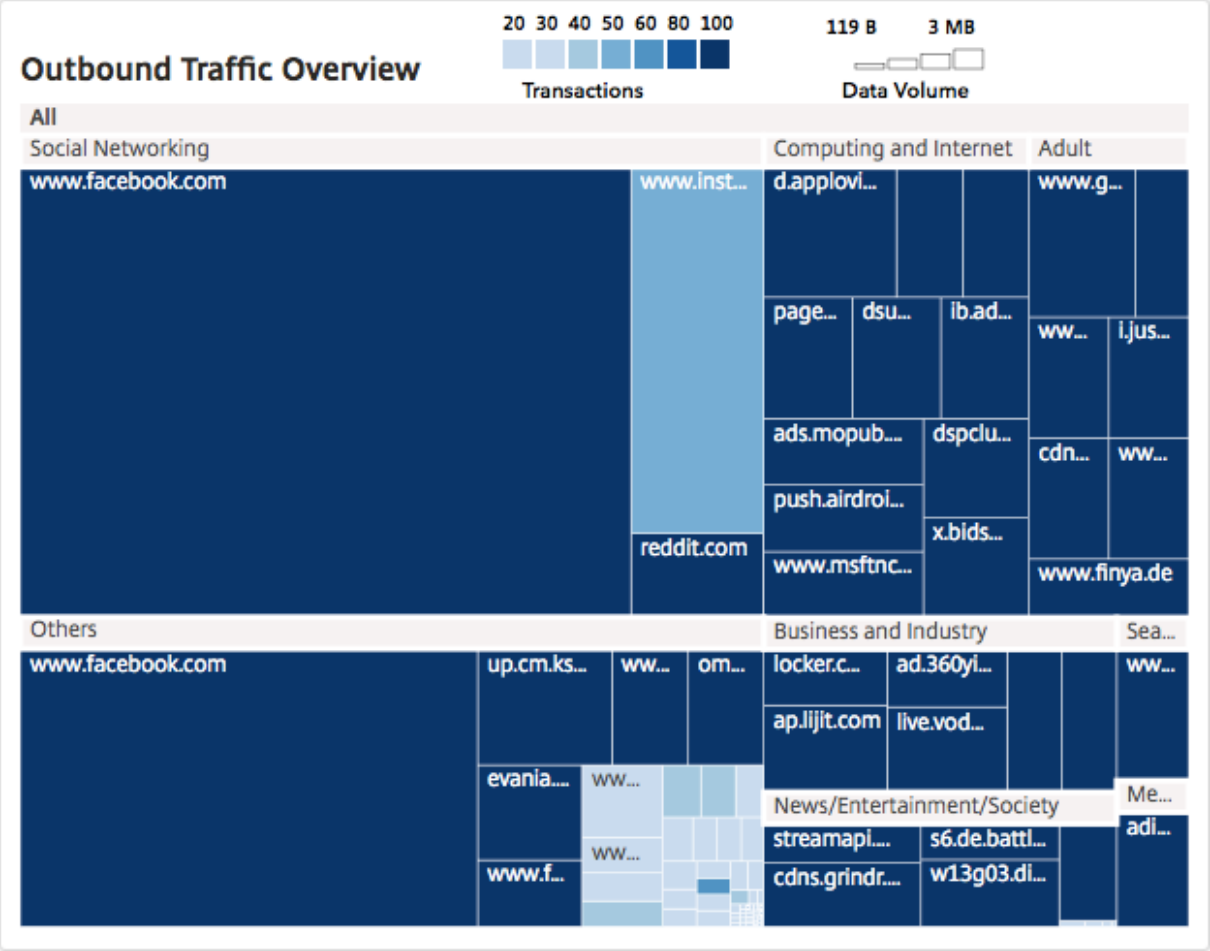
1. 从您的网络访问的 URL 或域占用的带宽量。
2. 从您的网络访问 URL 和域时发生的事务数。
3. 事务期间 Citrix ADC 设备截获的 SSL 连接数。
4. 在事务期间，Citrix ADC 设备未拦截的 SSL 连接数。
5. 事务期间 Citrix ADC 装置重置的 SSL 连接数。
6. 传输的 Web 流量，基于用于传输流量的端口、Web 流量使用的协议以及用于传输流量的客户端操作系统。

要访问出站流量控制面板，请导航到应用程序 **>** 出站流量控制面板。



查看来自网络的出站流量

出站流量控制面板包括出站流量概览窗格。在出站流量概览窗格中，Citrix ADM 将访问的 URL 或域分组为类别，如购物、新闻、社交网络等。出站流量概览窗格将从网络访问的 URL 或域显示为 URL 类别中的节点。节点的大小对应于访问 URL 或域时使用的数据量。节点的颜色指示访问 URL 或域时发生的事务数。



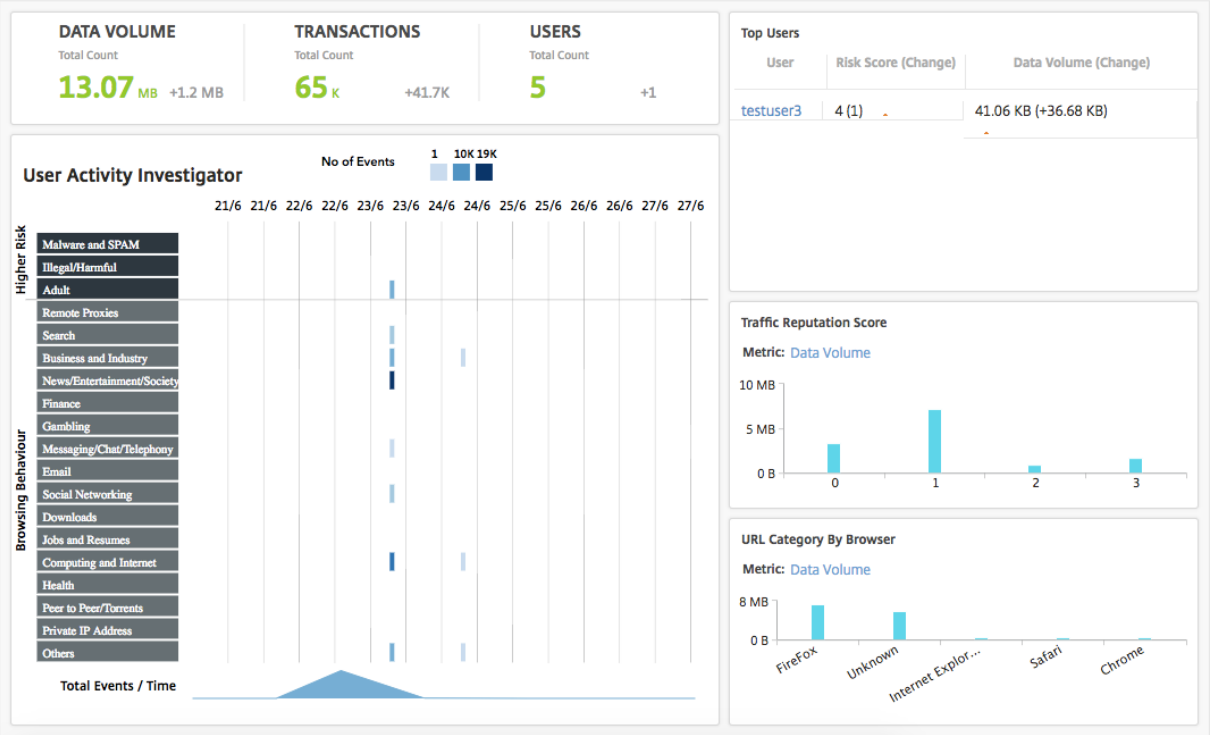
您可以单击类别来筛选图表，以显示指定时间范围内与类别相关的详细信息。

用户控制板

用户控制板显示企业中用户执行的活动的摘要。它提供一些主要指标，可以用来确定以下内容：

1. 您企业中的用户的浏览行为。
2. 您企业中的用户访问的 URL 类别。
3. 排名前五位的用户，基于其风险分数和其占用的带宽。有关风险分数的详细信息，请参阅“风险分数”。
4. 用于访问 URL 或域的浏览器。
5. 用户生成的 Web 流量，基于流量信誉分数。

要访问用户控制板，请导航到用户 **>** 控制板。

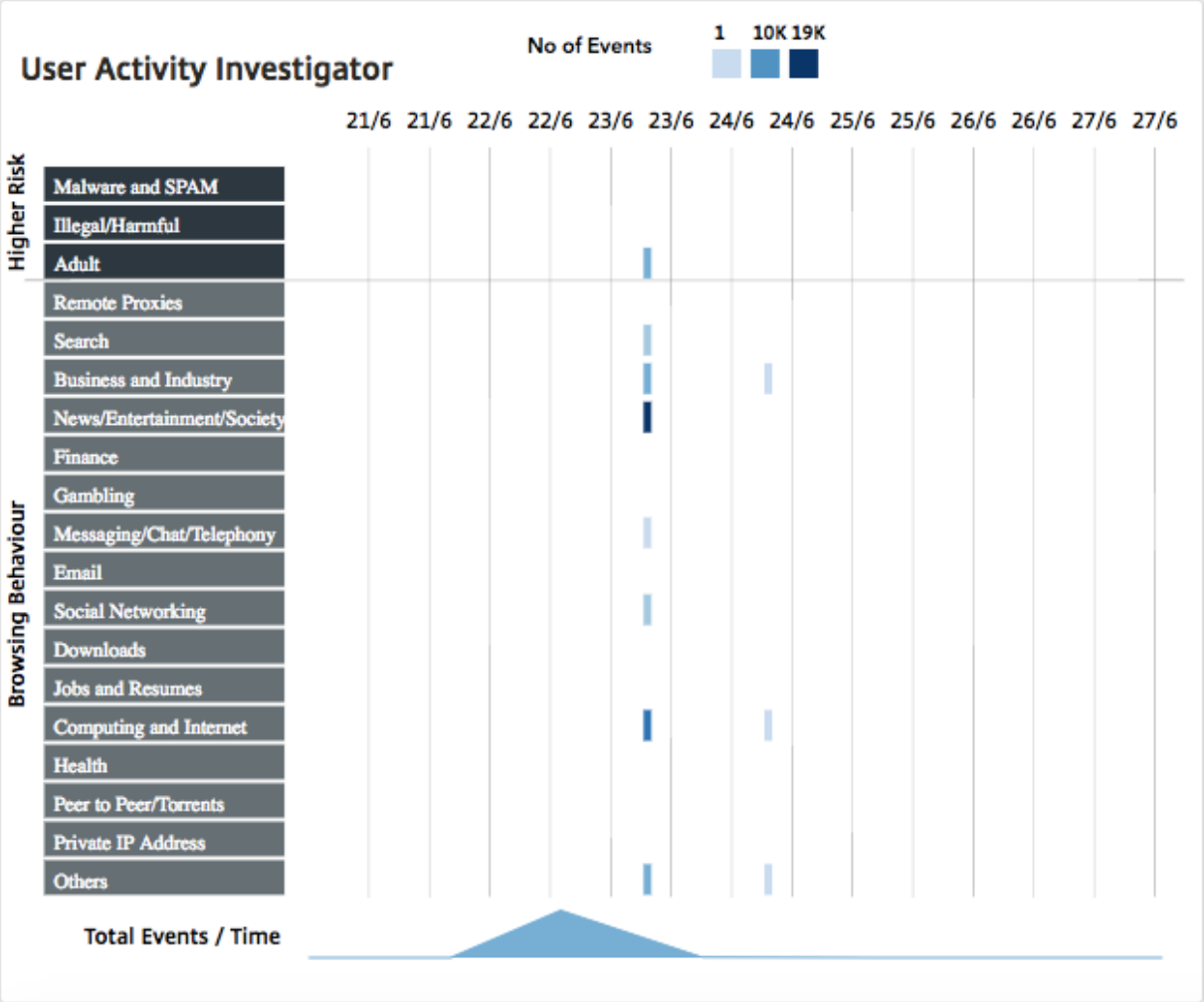


您可以单击排名前几位的用户窗格中的某个用户来过滤图表，以显示该用户在指定的时间范围内执行的 Web 活动的详细信息。

用户活动调查员

用户控制板包括一个用户活动调查器窗格，显示用户执行的各种 Web 活动。它显示在选定的时间范围内用户访问的 URL 类别，以及每个 URL 类别触发的各种事件。您可以单击事件以获取事务记录级别的详细信息。

用户活动调查器按 URL 类别显示关键信息，例如用户的浏览行为、用户的高风险活动以及触发的事件。事件以矩形图形式显示在图表中。如果选定的持续时间是一小时，则每个图例以一分钟的时间间隔进行汇总，如果选定的持续时间是一天，则每个图例以一小时的时间间隔进行汇总。



这些图例会进行汇总，并按照发生的事件数进行颜色编码。可以将鼠标指针悬停在图例上来显示选定图例的详细信息，例如，时间和汇总的事件数。您可以通过从时间段列表中选择一个时间来自定义图形的时间段。

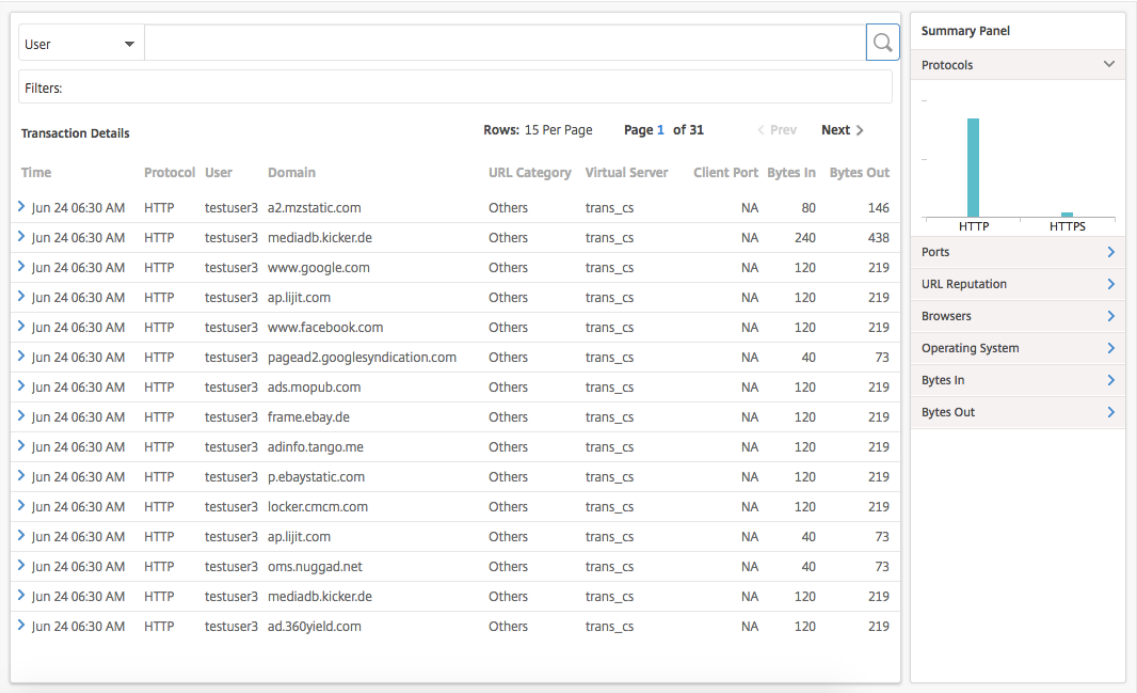
您可以单击事件以进一步向下钻取事务记录的详细信息。

用户事务

“User Transactions”（用户事务）页面显示您网络中的用户事务的详细信息。它提供事务级别详细信息，例如：

1. 事务的发生时间
2. 用于事务的协议
3. 用户名
4. 用户访问的域
5. URL 类别
6. 用于拦截事务的代理服务器

7. 客户端端口详细信息
8. 输入字节数
9. 输出字节数



Summary Panel（摘要面板）

Summary Panel（摘要面板）显示 **Transaction Details**（事务详细信息）窗格中可见的事务的所有指标。可以在此面板中选择或取消选择指标来在 **Transaction Details**（事务详细信息）窗格中对事务排序和查看事务。**Summary Panel**（摘要面板）显示以下指标：

指标	说明
协议	事务中使用的协议
端口	用于事务的端口
URL 信誉	URL 信誉分数
浏览器	用于事务的浏览器
操作系统	用于事务的操作系统
输入字节数	通过 Citrix ADC 设备接收的数据量。
输出字节数	通过 Citrix ADC 设备发送的数据量。

风险分数

风险评分是 Citrix ADM 中用于确定与企业中用户相关的风险的评分系统。Citrix ADM 根据 Citrix ADC 设备为网络中的用户访问的 URL 分配的 URL 信誉分数来分配风险分数。有关 URL 信誉分数的信息，请参阅 URL 信誉分数。下表介绍了 Citrix ADM 分配的风险评分。

风险分数	说明
1	用户的 Web 活动没有发现威胁或没有异常。
2	用户的 Web 活动没有发现威胁或没有异常，但用户正在访问没有 URL 信誉分数的“未知站点”。
3	在用户的 Web 活动未检测到威胁，但用户尝试访问的站点潜在易受攻击或与潜在易受攻击的站点关联。
4	潜在易受害的用户。
5	用户的 Web 活动异常，用户已访问已知的恶意站点。

用例

April 23, 2021

监视 **SSL** 拦截

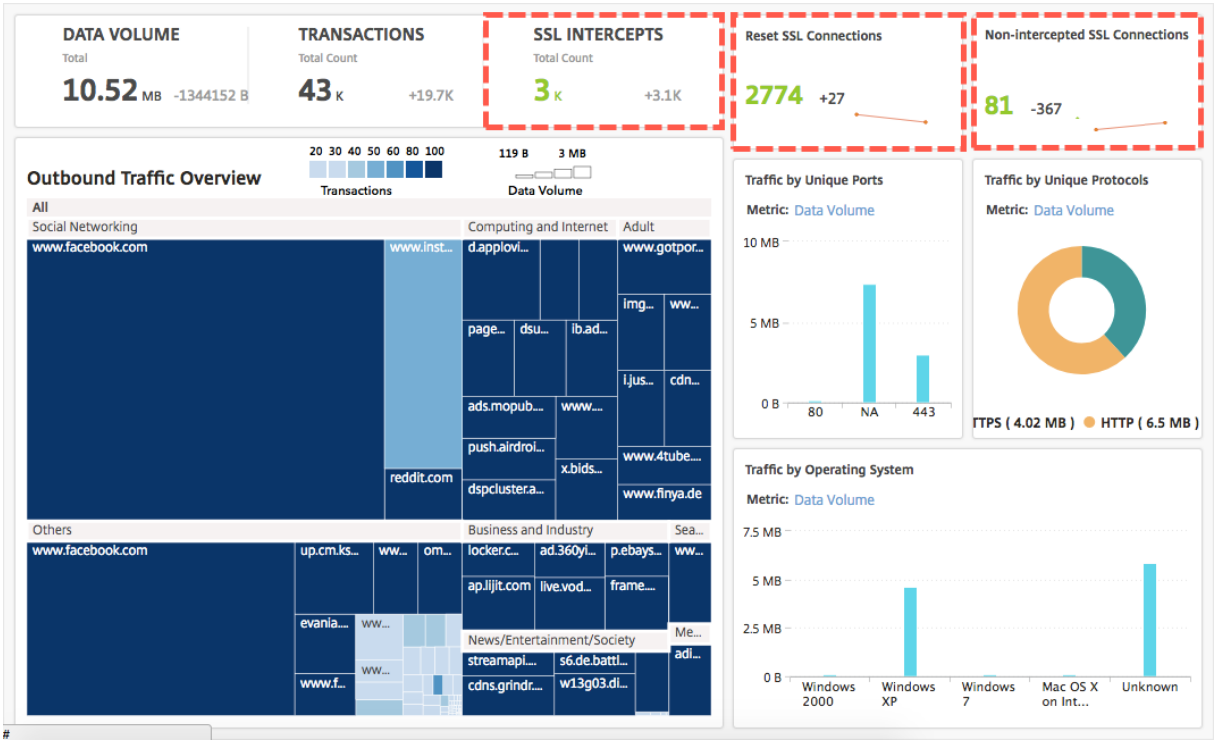
使用 Citrix ADC 装置，您可以检查加密的出站流量。您可以根据在设备上配置的策略拦截、绕过或阻止任何 HTTPS 请求。Citrix Application Delivery Management (ADM) 提供了有关所选时间范围内 出站流量控制板中 SSL 连接的以下详细信息：

- Citrix ADC 设备截获、未截获和重置的 SSL 连接数
- SSL 连接的事务详细信息

使用这些详细信息，您可以进一步微调 Citrix ADC 设备上的策略，以有效地检查加密的出站流量。有关详细信息，请参阅Citrix SSL 转发代理。

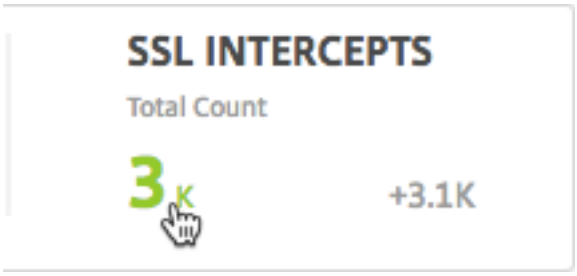
要显示拦截、未拦截和重置的 **SSL** 连接数，请执行以下操作：

导航到应用程序 **>** 出站流量控制面板。“Outboard Traffic Dashboard”（出站流量控制板）将显示拦截、未拦截和重置的 SSL 连接数。

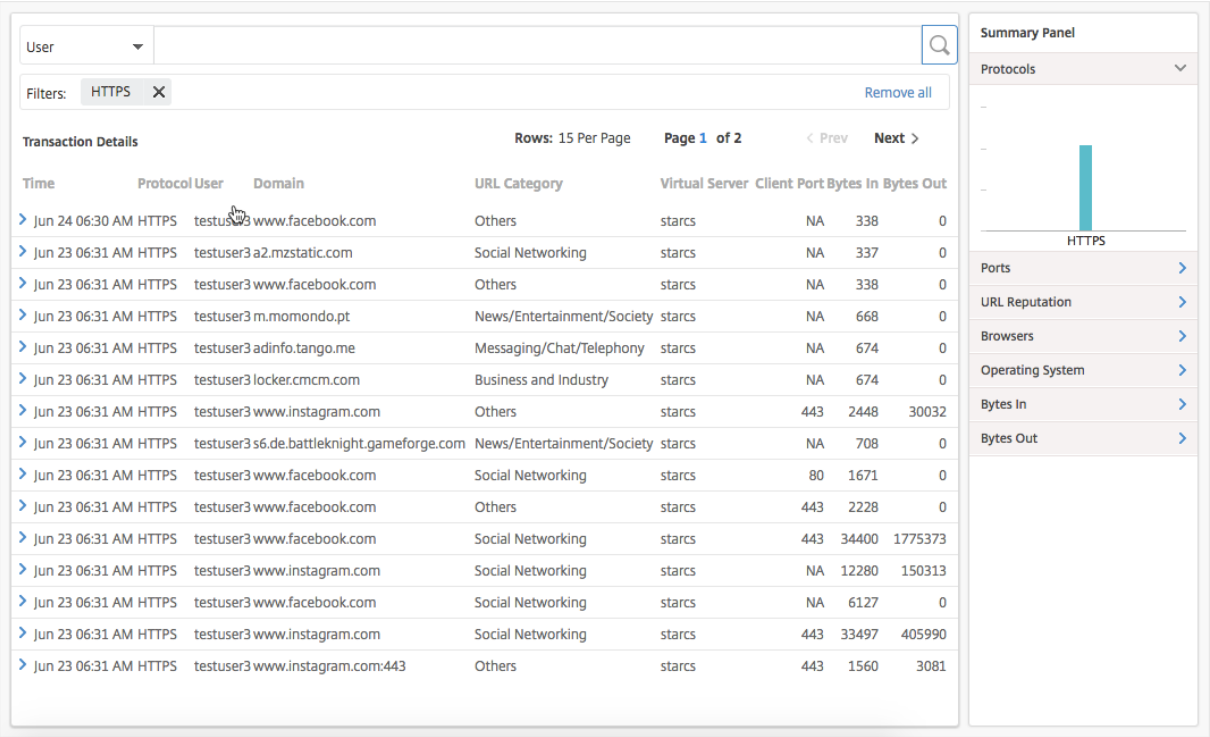


要显示拦截的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **SSL INTERCEPTS**（SSL 拦截）部分中的总计数。



在选定时间范围内拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。

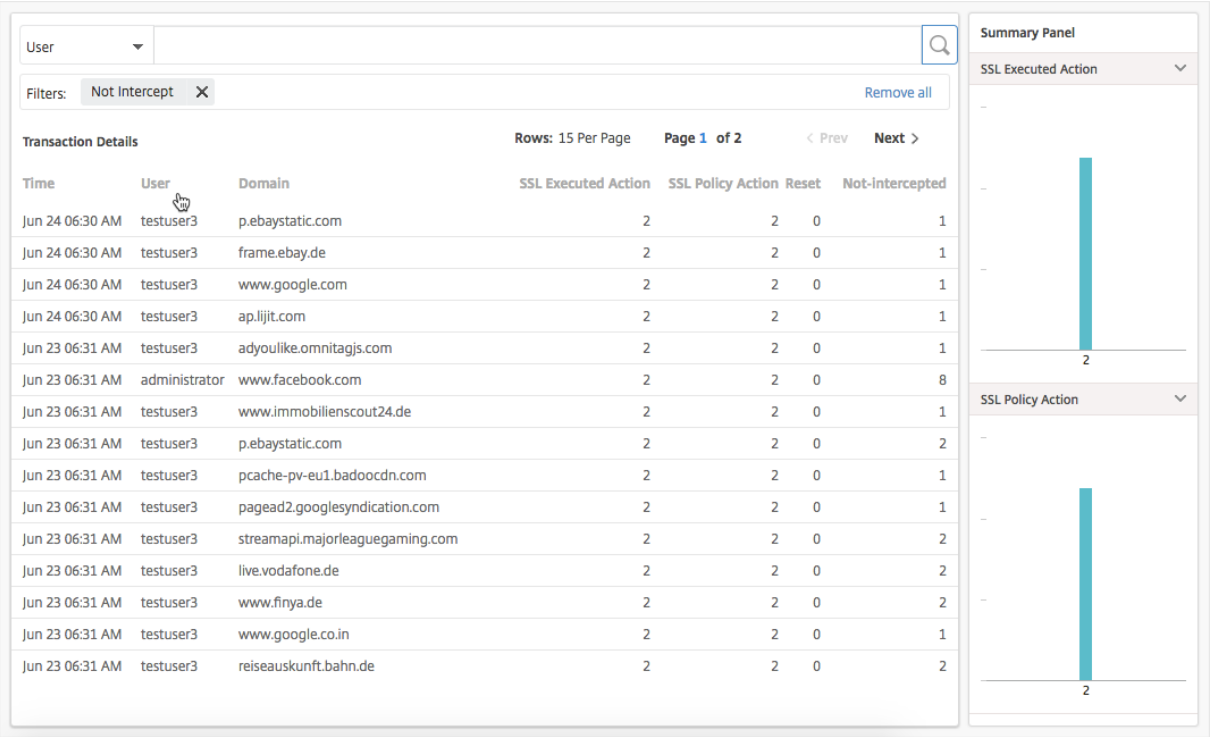


您可以进一步按用户和 URL 类别过滤事务详细信息。

要查看未拦截流量的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **Not-intercepted SSL Connections**（未拦截 SSL 连接）部分中的总计数。

在选定时间范围内流量未被拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。

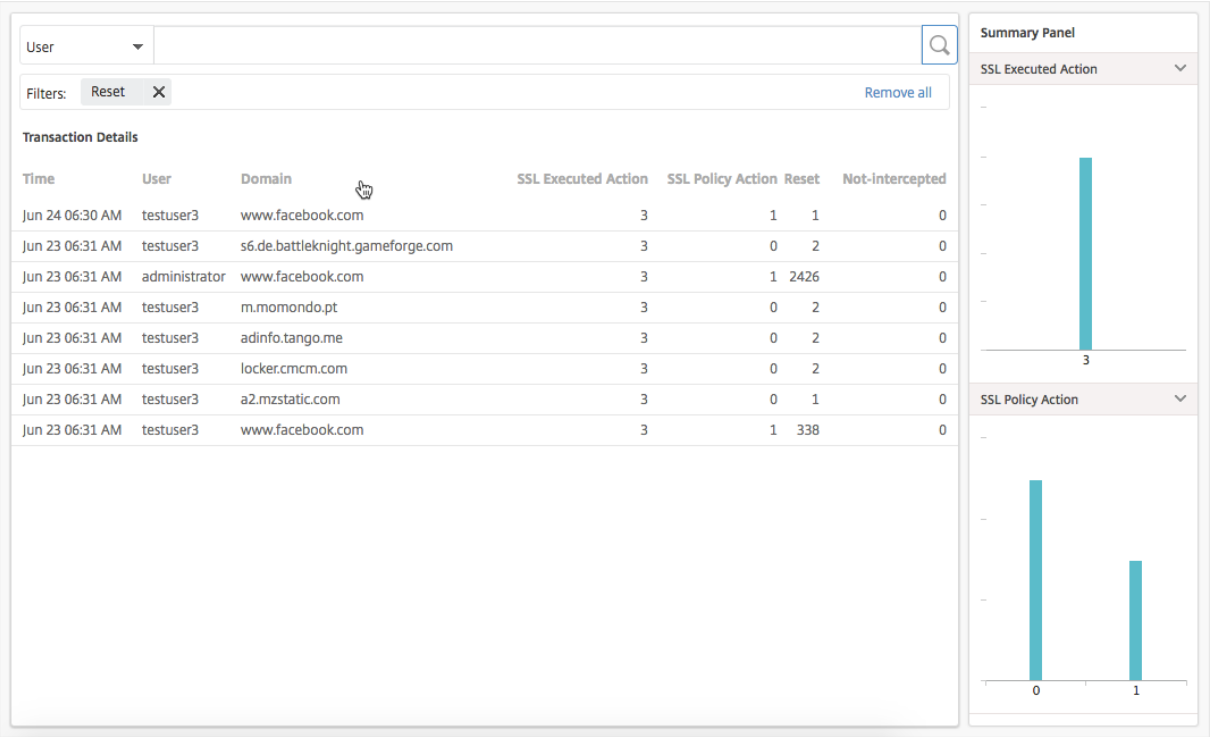


您可以进一步按用户和 URL 类别过滤事务详细信息。

要显示重置的 **SSL** 连接的事务详细信息，请执行以下操作：

1. 导航到应用程序 **>** 出站流量控制面板。
2. 在 **Outboard Traffic Dashboard**（出站流量控制板）上，单击 **Reset SSL Connections**（重置 SSL 连接）部分中的总计数。

在选定时间范围内流量未被拦截的 SSL 连接的事务详细信息将显示在 **Transaction Details**（事务详细信息）页面上。



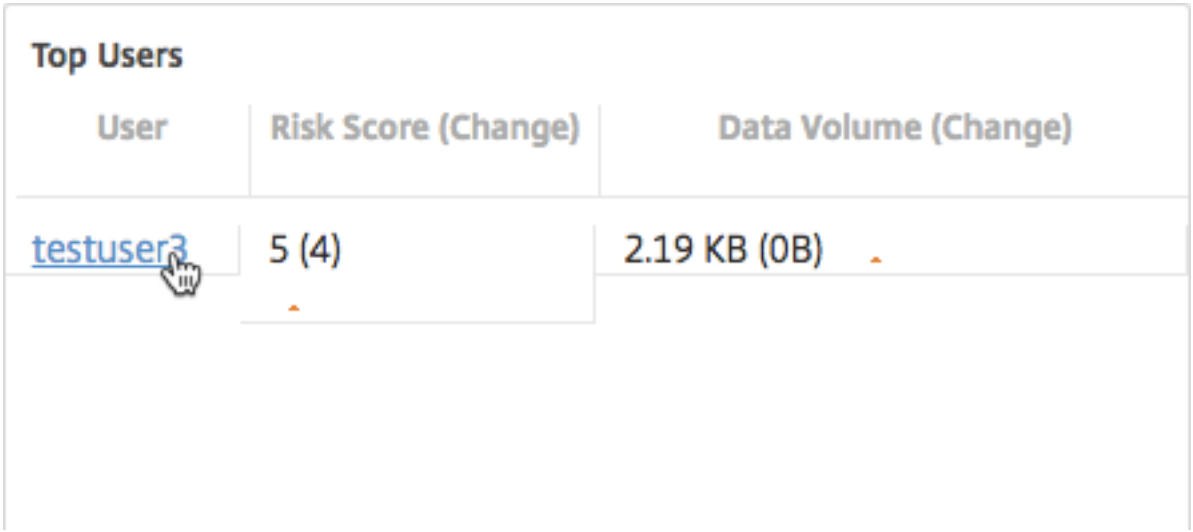
您可以进一步按用户和 URL 类别过滤事务详细信息。

检查终端节点

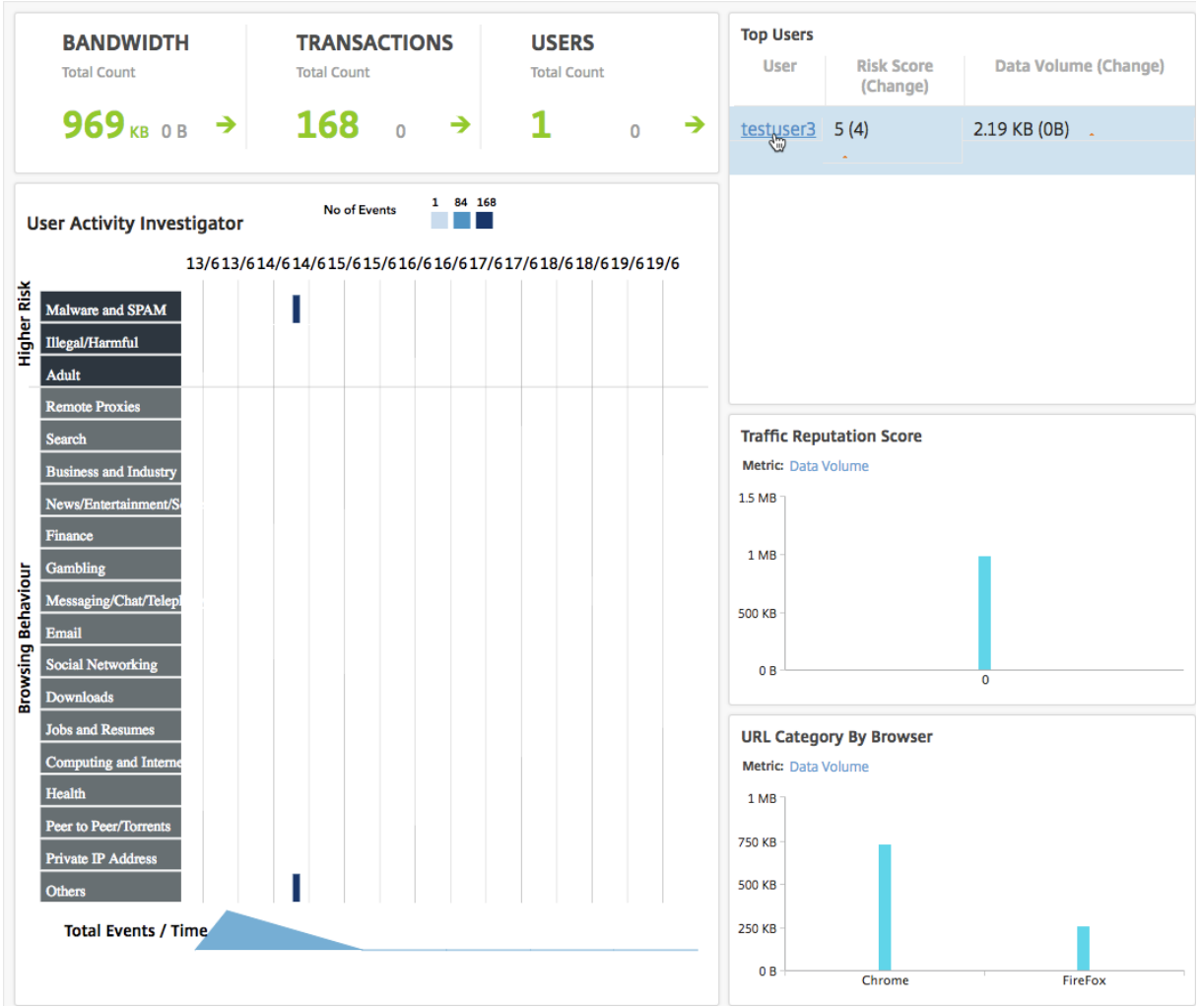
您在 Citrix ADC 设备上配置的策略指定设备如何记录企业中执行的所有用户活动。Citrix ADM 提供了关键指标，可用于确定：

1. 您企业中的用户的浏览行为。
2. 您企业中的用户访问的 URL 类别。
3. 排名前五位的用户，基于其风险分数和其占用的带宽。有关风险评分的更多信息，请参阅 风险分数。
4. 用于访问 URL 或域的浏览器。
5. 用户生成的 Web 流量，基于流量信誉分数。

例如，如果具有用户 ID testuser3 的用户不断访问企业中的恶意软件相关站点，Citrix ADM 将该用户识别为高风险活动用户，并分配更高的风险评分。testuser3 信息显示在 用户控制板的顶级用户部分。



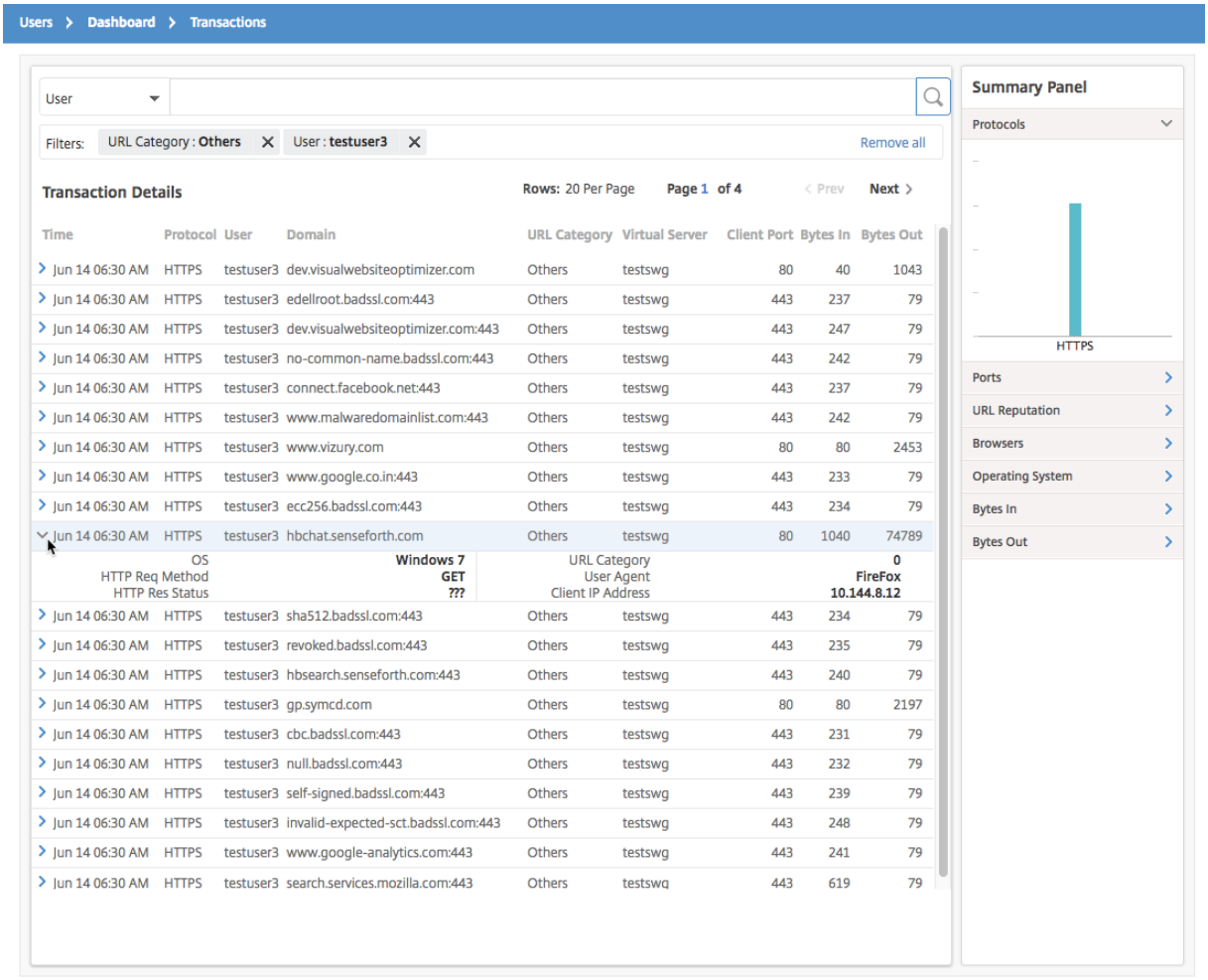
您可以单击 testuser3 来过滤 **User Dashboard**（用户控制板）以显示与 testuser3 有关的主要指标。



在 **User Activity Investigator**（用户活动调查器）窗格中，testuser3 的高风险活动以各自 URL 类别中的事件形

式显示。

您可以将鼠标悬停在事件上以显示事件数，也可以单击事件来调查事件期间发生的事务。

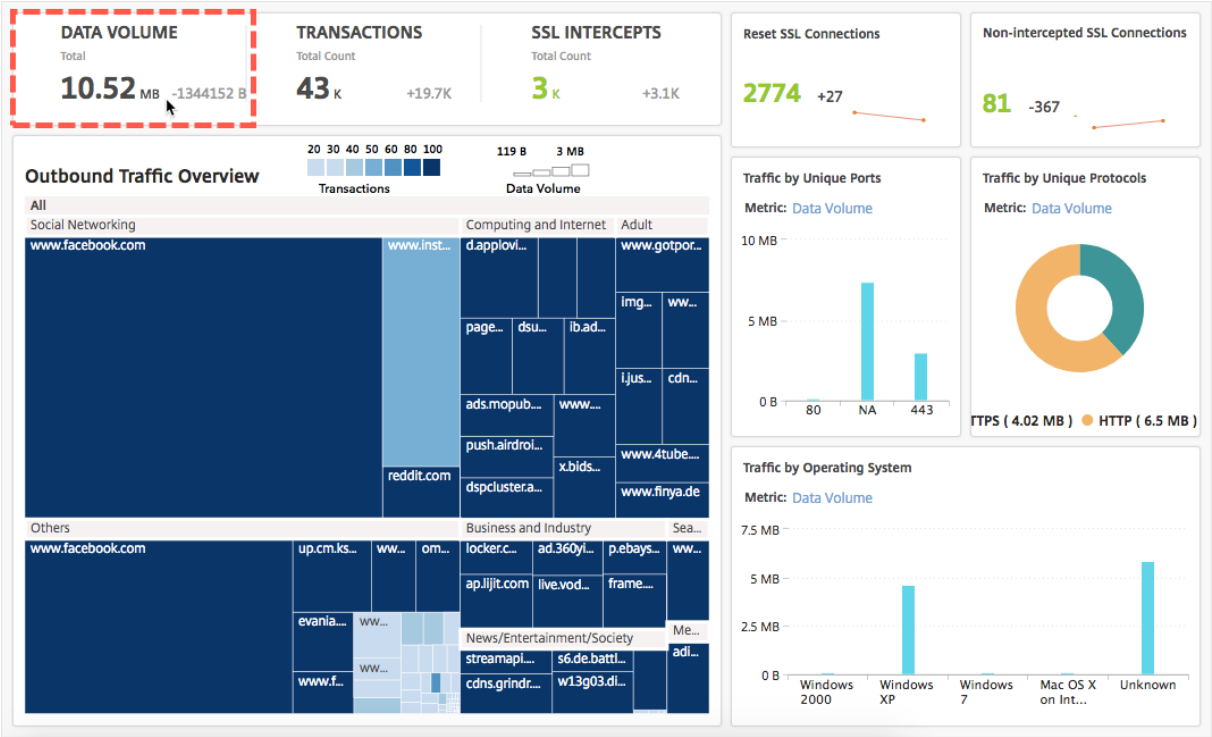


利用此信息，您可以确定系统是否感染了恶意软件，也可以了解用户的带宽消耗模式并微调 Citrix ADC 策略。有关详细信息，请参阅Citrix SSL 转发代理文档。

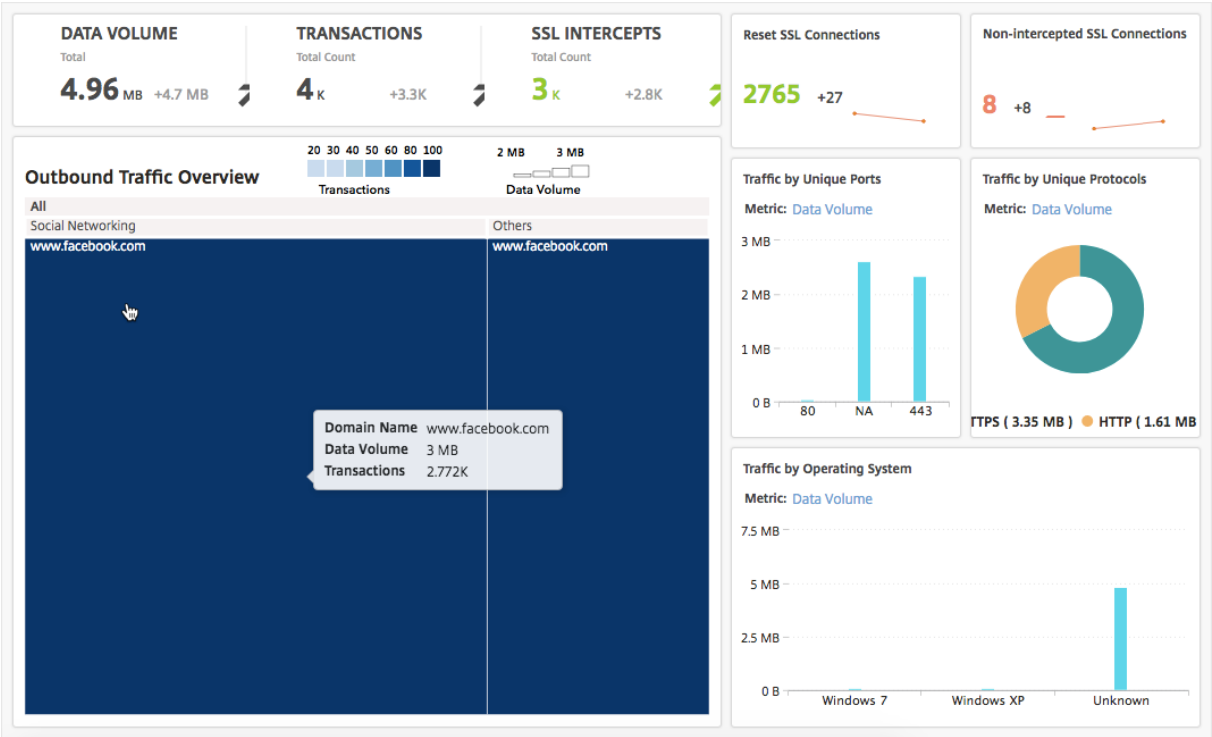
报告带宽消耗

Outbound Traffic Dashboard（出站流量控制板）和 **User Dashboard**（用户控制板）显示多个图表，这些图表汇总了从企业网络访问的 Web 站点或应用程序，以及您的网络中的用户执行的活动。

Outbound Traffic Dashboard（出站流量控制板）提供了从您的网络访问的 URL 或域占用的数据量的详细信息。导航到 **Applications**（应用程序）**> Outbound Traffic Dashboard**（出站流量控制板），其中数据量详细信息显示在 **Data Volume**（数据量）部分中。

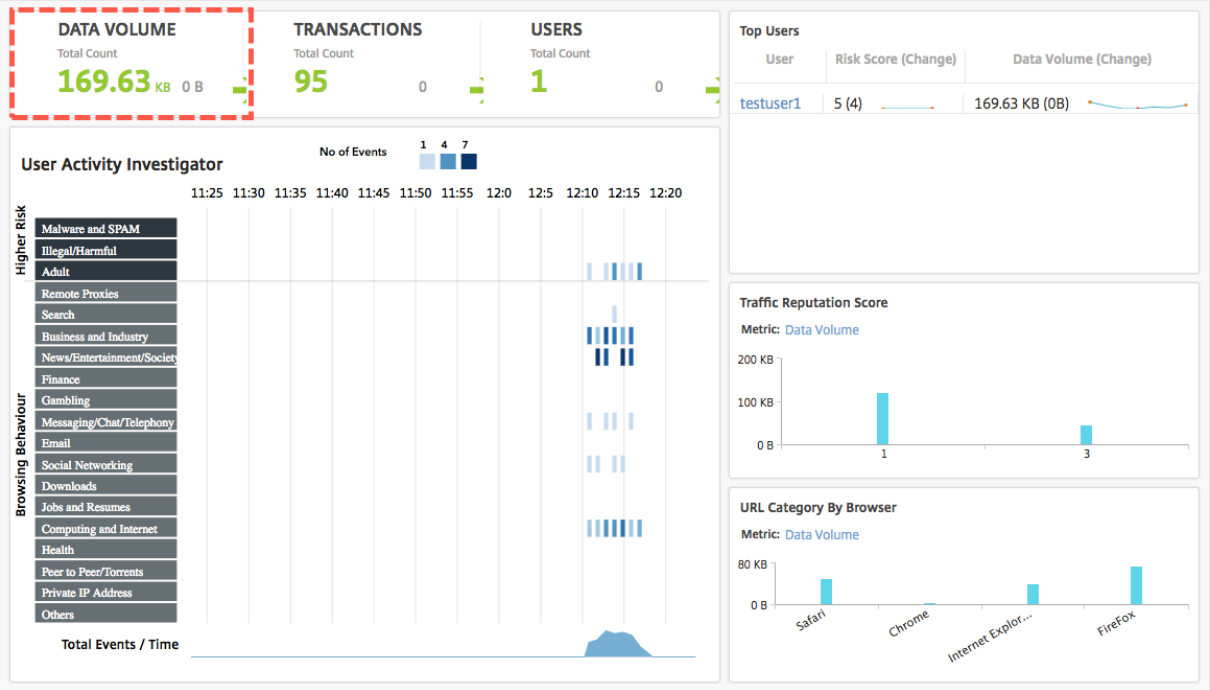


在 **Outbound Traffic Overview**（出站流量控制板）窗格中，单击域或 URL 以显示该域或 URL 占用的数据量的详细信息。

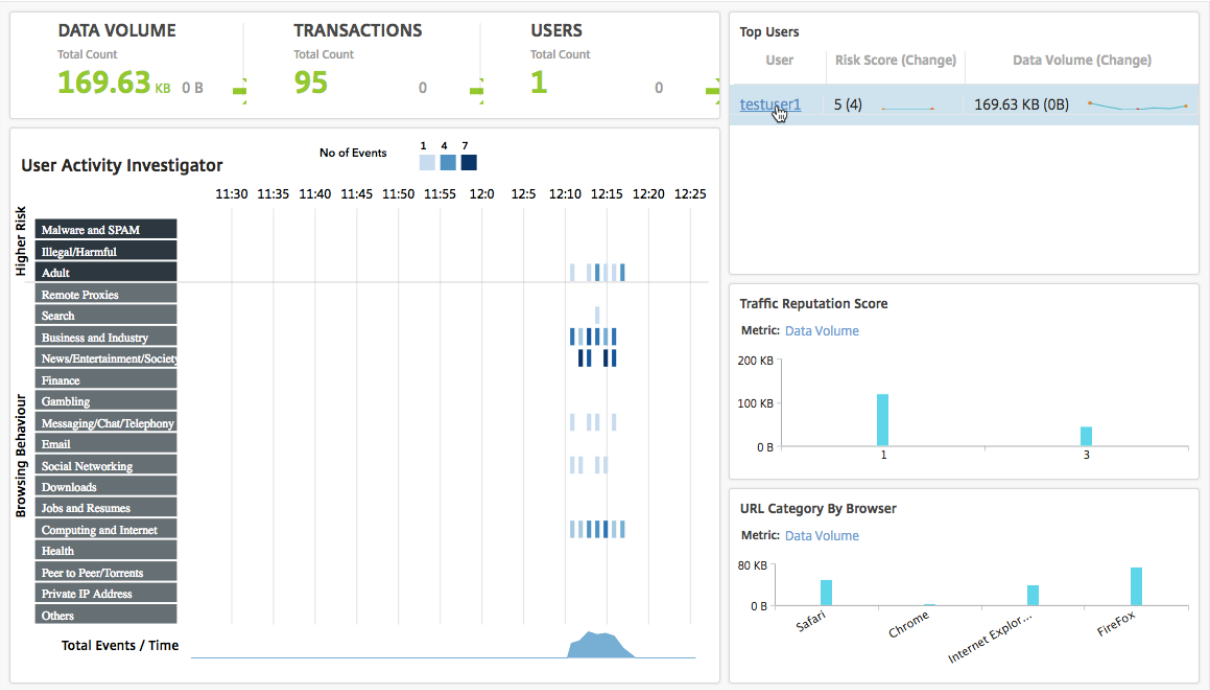


User Dashboard（用户控制板）提供了有关您网络中的用户占用的带宽的详细信息。导航到 **Users**（用户）> **Dashboard**（控制板）以在 **User Dashboard**（用户控制板）的 **DATA VOLUME**（数据量）部分中显示用户占用

的带宽的详细信息。



您可以从 **Top Users**（排名前几位的用户）部分选择用户来查看该用户占用的带宽的详细信息。**DATA VOLUME**（数据量）部分和图表中的其他主要指标将按选定用户过滤。



通过使用这些详细信息，您可以了解带宽占用量和占用的原因。例如，如果用户正在访问社交网站并导致大量带宽消耗，则管理员可以访问 Citrix ADC 设备并配置 URL 列表功能以控制对网站的访问。有关详细信息，请参阅使用案例：使用自定义 URL 集过滤主题。

查看出站流量分布

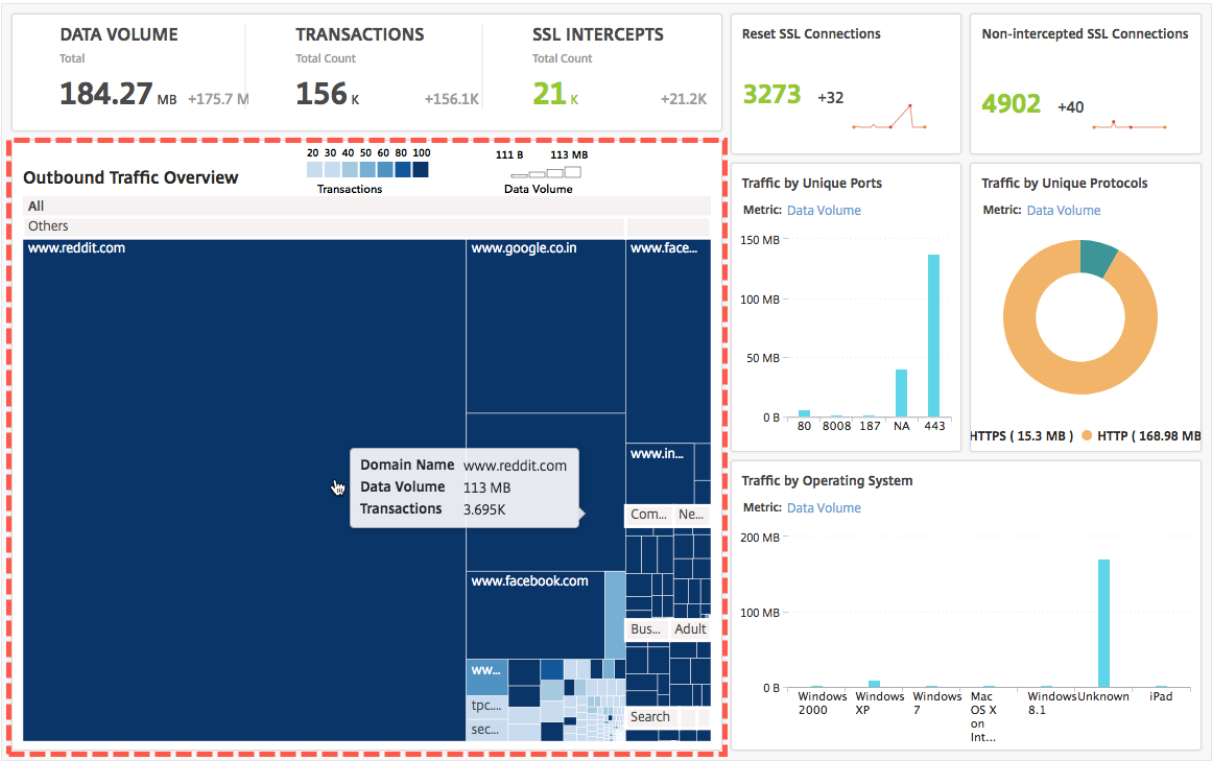
Citrix ADC 设备提供 URL 分类和筛选功能，您可以使用这些功能对从网络访问的 URL 进行分类。在 Citrix ADM 中，出站流量控制面板包括出站流量概览窗格。在 **Outbound Traffic Overview**（出站流量概览）窗格中，Citrix ADM 将访问的 URL 或域分组为不同类别（例如，Shopping（购物）、News（新闻）、Mobile（移动）等）以显示您网络中的出站流量分布。对于选定的时间范围，您可以单击 URL 以了解以下内容：

1. 访问该 URL 占用的带宽
2. 访问该 URL 时发生的事务
3. 访问该 URL 时拦截、未拦截和重置的 SSL 连接数

通过此信息，您可以了解出站流量模式并制定更正决策，例如，是否阻止特定 URL。

要查看出站流量分布，请执行以下操作：

导航到应用程序 **>** 出站流量控制面板。外部流量控制面板在 " 出站流量概览 " 窗格中显示 URL：



如果您要查看特定 URL 的详细信息，请选择该 URL。

使用此信息，您可以了解出站流量模式并使用在 Citrix ADC 设备上配置的 URL 筛选器控制网络流量。有关详细信息，请参阅URL 过滤。

调配

April 23, 2021

在软件定义网络连接 (SDN) 中，软件应用程序控制器管理网络及其活动，而不是管理支持网络的硬件。也就是说，SDN 允许网络管理员使用基于软件的集中式管理工具将物理网络连接虚拟化为逻辑网络连接并管理网络服务。SDN 让网络工程师和管理员可以快速响应不断变化的业务要求。

SDN 比较有名的优势是流量可编程性、更大的灵活性、创建策略驱动的网络监督能力以及实施网络自动化，下面列出了 SDN 一些特别的优势：

- 集中式网络置备
- 将网络安全性提高到粒度级
- 降低了运行成本
- 提高了云提取的级别
- 保证了内容交付
- 缩短了网络停机时间

Citrix Application Delivery Management (ADM) 通过与不同供应商的 SDN 控制器集成，支持企业网络中的 SDN。Citrix ADM 同时支持 VMware NSX 管理器和思科应用策略基础架构控制器 (APIC)。

VMware NSX Manager

Citrix ADM 与 VMware 网络虚拟化平台集成，可自动执行 Citrix ADC 服务的部署、配置和管理。此集成抽象出了与物理网络拓扑相关的传统复杂性，使 vSPhere/vCenter 管理员能够更快地以编程方式部署 Citrix ADC 服务。

VMware NSX Manager 呈现逻辑防火墙、交换机、路由器、端口及其他网络连接元素，从而能够在各种虚拟机管理程序、云管理系统和关联的网络硬件之间构成虚拟网络连接。此外，它还支持外部网络连接和安全服务。

Citrix ADM 的云编排功能支持将 Citrix ADC 产品与 VMware NSX 的集成，并提供以下功能：

- 能够在服务插入过程中将预置备的 VPX 按需分配给特定 Edge 网关。
- 能够通过在 NSX 环境内运行的实例上的应用程序模板配置 Citrix ADC 的高级功能（如 SSL 和 CS）以及基本负载平衡。
- 能够从某个 Edge Gateway 取消分配 VPX，作为服务删除的一部分，并将相同的 VPX 重新分配给另一个 Edge Gateway。
- 能够从 vCenter 控制台快速部署 Citrix ADC 功能，作为应用程序所需的所有基础架构的部署工作流程的一部分。

优势：

- 在应用程序部署工作流中，自动按需分配新 ADC 服务

- 通过应用程序模板，简化了应用程序特定的高级 ADC 功能的配置
- 多租户职责分离和自助服务消费模式，同时为云管理员提供单点控制
- 更轻松地与 Citrix ADM API 集成，这有助于支持意外的未来使用。

有关如何在 Citrix ADM 上配置 VMware NSX 管理器的详细信息，请参阅 将 Citrix ADC 设备与 VMware NSX 管理器集成。

Cisco ACI 混合模式

Cisco ACI 1.3 版 (2f) 中引入了混合模式支持。在混合模式下，您可以通过应用程序策略基础架构控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委派给 Citrix ADM，后者充当 APIC 中的设备管理器。

混合模式器件封装和 Citrix ADM 支持 Citrix ADC 混合模式解决方案。需要在 APIC 中上载混合模式设备包。有关详细信息，请参阅 在思科 ACI 混合模式下使用 Citrix ADM 实现 Citrix ADC 自动化。

开放式堆栈：集成 **Citrix ADC** 实例

April 23, 2021

Citrix Application Delivery Management (ADM) 的云编排功能支持 Citrix ADC 产品与 OpenStack 平台的集成。通过将此功能与 OpenStack 平台结合使用，OpenStack 用户可以使用 Citrix ADC 的负载平衡功能 (LBaaS)。之后，OpenStack 用户可以从 Citrix ADC 实例中的 OpenStack 部署其负载均衡器配置。

以下各节简要介绍了 Citrix ADM 和 OpenStack 集成工作流中的功能。

Citrix ADC 驱动器用于开放式堆栈中子 **LBA**

OpenStack Neutron LBAS 插件包括 Citrix ADC 驱动程序，该驱动程序使 OpenStack 能够与 Citrix ADM 进行通信。OpenStack 使用此驱动程序将通过 LBaaS API 完成的任何负载均衡配置转发到 Citrix ADM，Citrix ADM 将在所需的 Citrix ADC 实例上创建负载均衡器配置。OpenStack 还使用驱动程序定期调用 Citrix ADM，以从 Citrix ADC 检索所有负载平衡配置的不同实体（如 VIP 和池）的状态。用于 OpenStack 平台的 Citrix ADC 驱动程序软件与 Citrix ADM 捆绑在一起。要下载并安装驱动程序，必须首先安装 Citrix ADM 并启动应用程序。

相互注册 **Citrix ADM** 和 **OpenStack**

您必须首先在 Citrix ADM 上注册 OpenStack 信息。指定 OpenStack Controller IP 地址和云管理用户凭据，以及 OpenStack Citrix ADC 驱动程序用户凭据。稍后可以在中子配置文件 (中子.conf) 的 Citrix ADC_ 驱动程序部分指定相同的登录凭据，以便 OpenStack 中的 Citrix ADC 驱动程序可以在 LB 配置期间连接到 Citrix ADM。

在 OpenStack 和 Citrix ADM 相互注册后，两者都可以相互通信。此外，OpenStack 用户可以使用其在 OpenStack 中的现有凭据登录到 Citrix ADM 用户界面，以检查其 LB 配置在 Citrix ADC 中的执行情况。

OpenStack 中的租户

在 OpenStack 中，租户也称为项目。租户是一组用户；租户或项目也可以定义为一组分配给隔离用户组的资源（计算、网络和存储等）。

放置策略

放置策略可以灵活地决定用户创建的每个负载均衡器配置中使用的 Citrix ADC 实例。或者，Citrix ADM 还提供了一个基于 OpenStack 租户分配 Citrix ADC 实例的选项。

服务包

服务包是将策略/SLA、设备或自动置备配置规范及租户/放置策略关联在一起的捆绑包。服务包通常是以提供给租户的隔离策略进行定义。

下面是与服务包相关的一些要点：

- 租户不能属于多个服务包。
- 多个租户可以与相同的服务包关联。
- 在设置为自动配置的服务包中，只能从一种平台类型（在 SDX 平台上或 OpenStack 计算平台上）创建虚拟 Citrix ADC 实例。

LBaaS V1 和 LBaaS V2 支持的功能

虽然 OpenStack 中的 LBaaS V1 驱动程序支持从 OpenStack Horizon 用户界面进行操作，但 LBaaS V2 驱动程序仅支持命令行操作。

下面的列表显示了 OpenStack 上 LBaaS V1 和 LBaaS V2 支持的功能：

- LBaaS V1
  - 负载平衡
- LBaaS V2
  - 负载平衡
  - SSL 使用 OpenStack 中的密钥管理器 巴比肯管理的证书卸载
  - 证书捆绑包（包括中间证书颁发机构）
  - SNI 支持

本文档提供关于以下内容的信息：

- 用例场景
- Citrix ADM 集成与 OpenStack 工作流程

- 必备条件
- Citrix ADM 和 OpenStack 中的预配置任务
- 使用 Horizon 对 LBaaS V1 进行配置的步骤
- 使用命令行对 LBaaS V2 进行配置的步骤
- 在 OpenStack 上手动配置 Citrix ADC VPX 实例
- 将 Citrix ADM 与 OpenStack 加热服务集成
- 监控 Citrix ADM 中的 OpenStack 应用程序

用例场景

以下用例场景解释了 Citrix ADM 与 OpenStack 平台集成的工作流程：

企业 Example-Cloud-Provider 已使用 OpenStack 组件来设置一个云，为其租户提供基础结构。Steve 是此云提供商的管理员，而 Tom 是 Example-Cloud-Provider 的云基础结构的租户。汤姆的组织，例如，Sportsonline.com，需要两个服务器 S1 和 S1，而汤姆还需要一个专用的 Citrix ADC 设备来平衡 OpenStack 平台上的服务器 S1 和 S2 之间的流量。

为了满足这一要求，史蒂夫必须同时安装和配置 OpenStack 和 Citrix ADM，并为彼此兼容做好准备。Steve 必须在 OpenStack 中创建名为 Example-SportsOnline 的租户帐户，然后为该租户帐户分配资源。Steve 还必须为 Example-SportsOnline 创建不同的登录凭据（用户）用于管理器其资源和配置。Tom 现在可以在 OpenStack 上创建两个服务器 S1 和 S2 以管理其组织中的流量。

史蒂夫必须注册 OpenStack 的详细信息与 Citrix ADM, 并在 OpenStack 网络组件中配置 Citrix ADC LBaaS 驱动程序, 中子. 注册完成后，Citrix ADM 将显示 OpenStack 中所有租户的详细信息。史蒂夫可以从列表中选择希望 Citrix ADC LBaaS 功能的示例体育在线，并将 Tom 配置为 Citrix ADM 中的负载均衡器配置分配给他的专用 Citrix ADC。

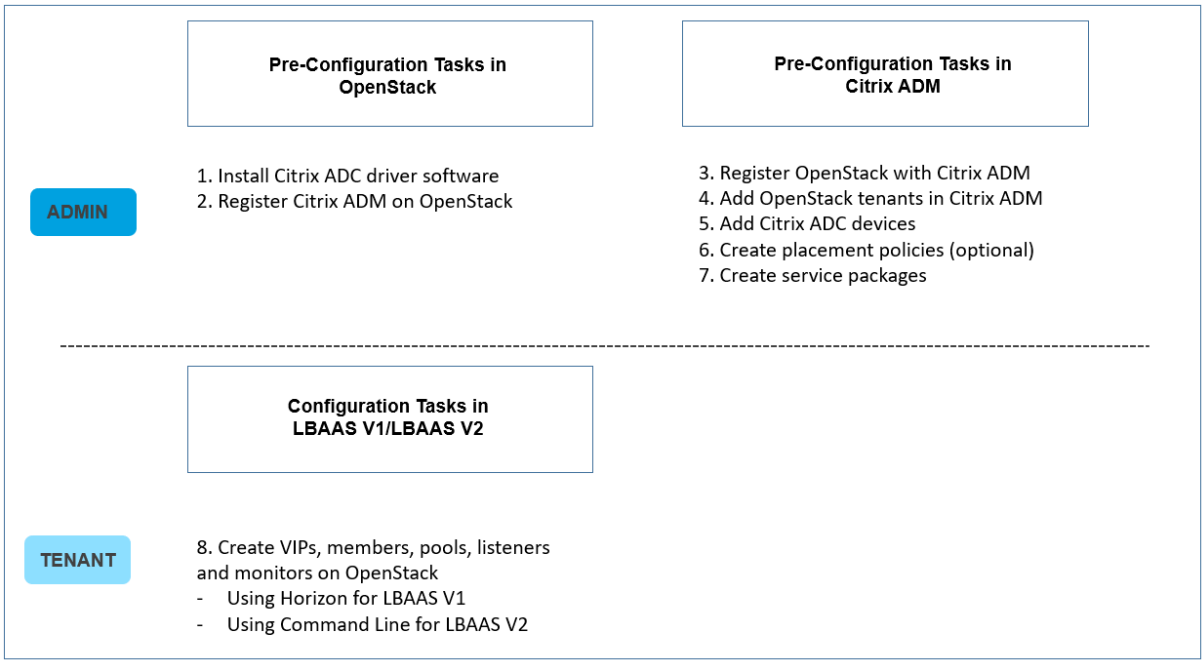
为此，Steve 可以使用 Citrix ADM 用户界面在 OpenStack 的计算层（Nova）上配置 Citrix ADC VPX 实例，也可以使 MAS 按需自动配置 Citrix ADC VPX 实例，当 Tom 在 OpenStack 中进行 LB 配置时。在任何一种情况下，Citrix ADM 都会管理 VPX 实例。为了实现这一目标，Steve 在 Citrix ADM 中创建了一个服务包，并定义了 SLA 中与 Tom 商定的服务包中的条件。例如，Steve 选择“专用”隔离策略来提供专用实例用于为 Tom 提供负载平衡器配置。即，Steve 在服务包中为 Tom 选择非共享实例。然后，他将许多 Citrix ADC VPX 实例分配给服务包，并将示例体育联机以及需要专用 Citrix ADC 和服务包的其他租户关联起来。因此，当 Tom 执行其第一个负载均衡器配置时，Citrix ADM 会将服务包中的一个 Citrix ADC VPX 实例分配给示例体育 Online，并将其配置部署到该 Citrix ADC 中。

Tom 现在可以通过使用 OpenStack LBaaS/UI 创建池、虚拟 IP (VIP) 及运行状况监视器来创建负载平衡配置。OpenStack 中的池和 VIP 在 Citrix ADC 实例上作为服务组和虚拟服务器进行部署。Tom 还可以创建运行状况监视器来监视服务器，并将应用程序流量仅发送到那些在任何时间点处于启动状态并可从 Citrix ADC 访问的服务器。

在 OpenStack 中创建的负载平衡配置现在已在 Citrix ADC 实例上实施。完全配置后，Citrix ADC VPX 实例接管负载平衡功能，并开始接受应用程序流量并平衡 Tom 创建的服务器 S1 和 S2 之间的流量。

Citrix ADM 集成与 OpenStack 工作流程

下面的流程图说明了在配置 LBaaS V1 和 LBaaS V2 时需要遵循的工作流。



必备条件

April 23, 2021

在将 Citrix ADC 虚拟实例与 OpenStack 平台集成之前，请确保满足以下要求：

Citrix ADM 和 OpenStack 软件要求

- Citrix ADM 13.0 安装在受支持的 Hypervisor 工作站上，该工作站符合最低硬件要求系统。
- OpenStack 组件已安装并正在运行。
- Citrix ADM 13.0 支持以下 OpenStack 版本- 牛顿、奥卡塔、派克和 皇后区。

Citrix ADM 硬件要求

确保 OpenStack 服务器上有以下虚拟计算资源以安装 Citrix ADC 虚拟实例：

组件	要求
RAM	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

> 注意
>
> 考虑到主机上没有其他虚拟机运行，指定的内存和硬盘要求用于在 OpenStack 平台上部署 Citrix ADM。OpenStack 的硬件要求取决于其上运行的虚拟机数量。

Citrix ADM 和 OpenStack 中的预配置任务

April 23, 2021

本节将帮助您在配置 Citrix Application Delivery Management (ADM) 和 OpenStack 之前执行预配置任务。

安装 Citrix ADM

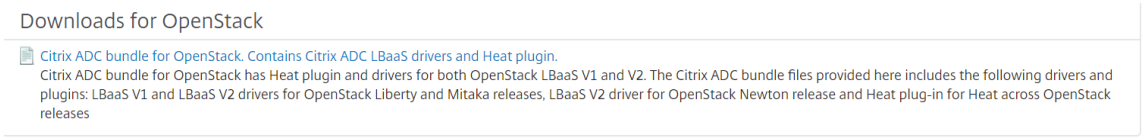
在受支持的 Hypervisor 上安装 Citrix ADM。有关如何下载和安装 Citrix ADM 的详细信息，请参阅 部署 Citrix ADM。

安装 Citrix ADC 驱动程序软件并在 OpenStack 上注册 Citrix ADM

从 Citrix ADM 下载页面下载适用于 OpenStack 的 Citrix ADC 捆绑包。

要使用 **Citrix ADM GUI** 在 **OpenStack** 平台上安装 **Citrix ADC** 驱动程序，请执行以下操作：

1. 在 Citrix ADM 中，单击 下载。Citrix ADM 中的“下 载”页面为您提供下载 **Citrix ADC** 捆绑包的链接，该软件适用于 牛顿、**Ocata** 和 Pike**O** penStack 版本所需的 OpenStack 软件。
2. 将最新的 Citrix ADC 捆绑 tar 文件下载到 OpenStack 控制器中的临时目录（例如 /tmp）。该捆绑包包括适用于所有 OpenStack 版本的 LBaaas V2 驱动程序和热插件。



3. 运行以下命令，从 Citrix ADC 驱动程序 tar 文件中提取文件：

```
tar -xvzf <name_of_tar_file>
```


4. 如果您有 OpenStack <Release Name> 安装程序，请在提示符下键入以下命令：

   ```
   cd <Release Name>
   ```

   示例：

   ```
   cd Newton
   ```

5. 运行以下命令来安装驱动程序并指定 Citrix ADM IP 地址、在向 Citrix ADM 注册 OpenStack 时配置的 Citrix ADC 驱动程序密码以及协议：

   ```
   ./install.sh --ip=<NetScaler_MAS_IP> --password=<password> --protocol=<protocol> --neutron-lbaas-path <neutron-lbaas-directory-path>
   ```

   单节点 **OpenStack** 设置示例：

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/opt/stack/neutron-lbaas
   ```

   多节点 **OpenStack** 设置示例：

   ```
   ./install.sh --ip=10.102.29.90 --password=xxxx --protocol=HTTP --neutron-lbaas-path=/usr/lib/python2.7/site-packages
   ```

   > 注意
   >
   > 提供系统 `neutron-lbaas` 目录的路径是可选的。提供该路径可以帮助脚本找到驱动程序。
   >
   > 在 OpenStack 上成功注册 Citrix ADM 后，您还可以使用 OpenStack 用户凭据登录到 Citrix ADM。
   >
   > 在 OpenStack 上成功注册 Citrix ADM 后，重新启动 OpenStack 中子服务。

在 **Citrix ADM** 中注册 **OpenStack**

要使用 **Citrix ADM GUI** 将 **OpenStack** 注册到 **Citrix ADM**，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “编排” > “云编排” > “**OpenStack**”。
2. 单击 配置打开堆栈设置。
3. 在 “ 配置 **OpenStack** 设置” 页中，可以设置用于在 Citrix ADM 中配置 OpenStack 的参数。此处有两个选项 -“Default”（默认）和 “Customized”（自定义）。

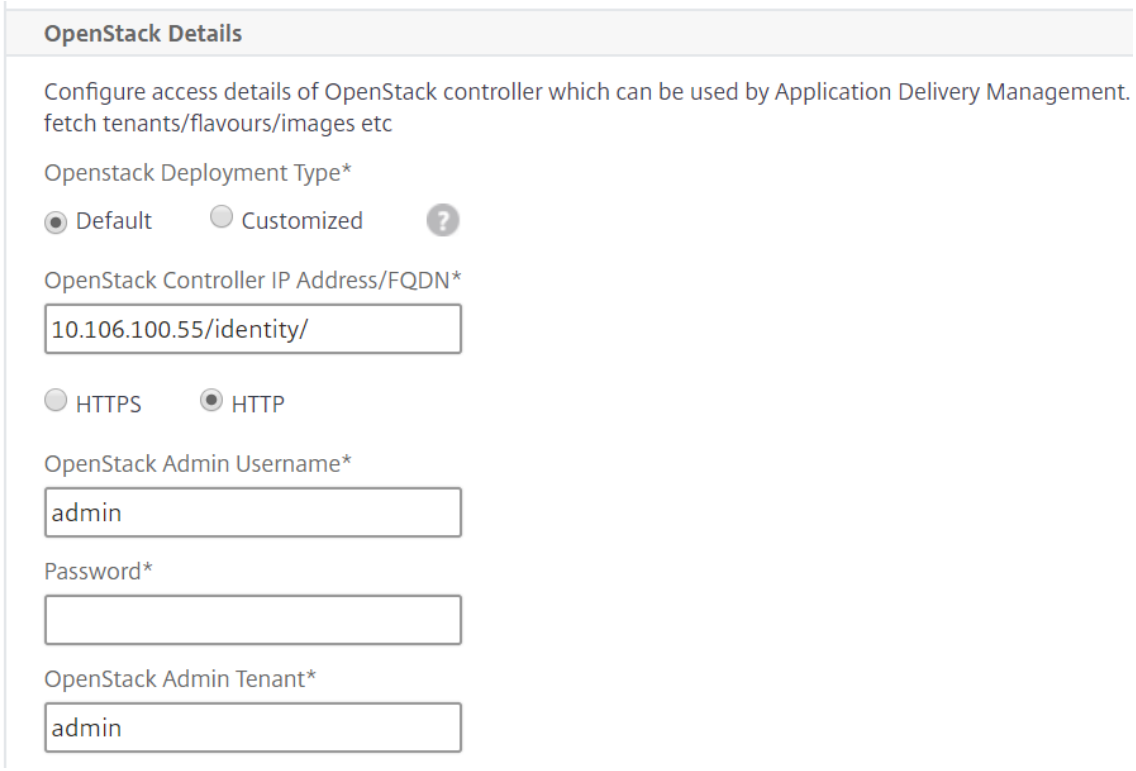
   对于牛顿和 **Ocata** 版本的 OpenStack，您可以使用默认部署类型或自定义部署类型。但是，对于派克版本，您必须使用自定义部署类型向 Citrix ADM 注册 OpenStack。

   - 默认部署类型

     如果 OpenStack 服务正在默认端口上运行，请选择默认值。例如，Neutron 服务的默认端口是 9696，Keystone 服务的默认端口是 5000。

1. OpenStack 控制器 IP 地址-OpenStack 控制器的 IP 地址（**KeyStone** 服务和 **Neutron** 服务都可以在此 IP 地址上访问）。例如，输入 IP 地址 10.102.205.23。

2. OpenStack 管理员用户名-OpenStack 控制器的管理用户名。例如，输入 admin1。
3. Password（密码）- OpenStack 控制器的管理用户的密码。
4. OpenStack 管理租户-管理租户在 OpenStack 上的名称。例如，输入 admin。

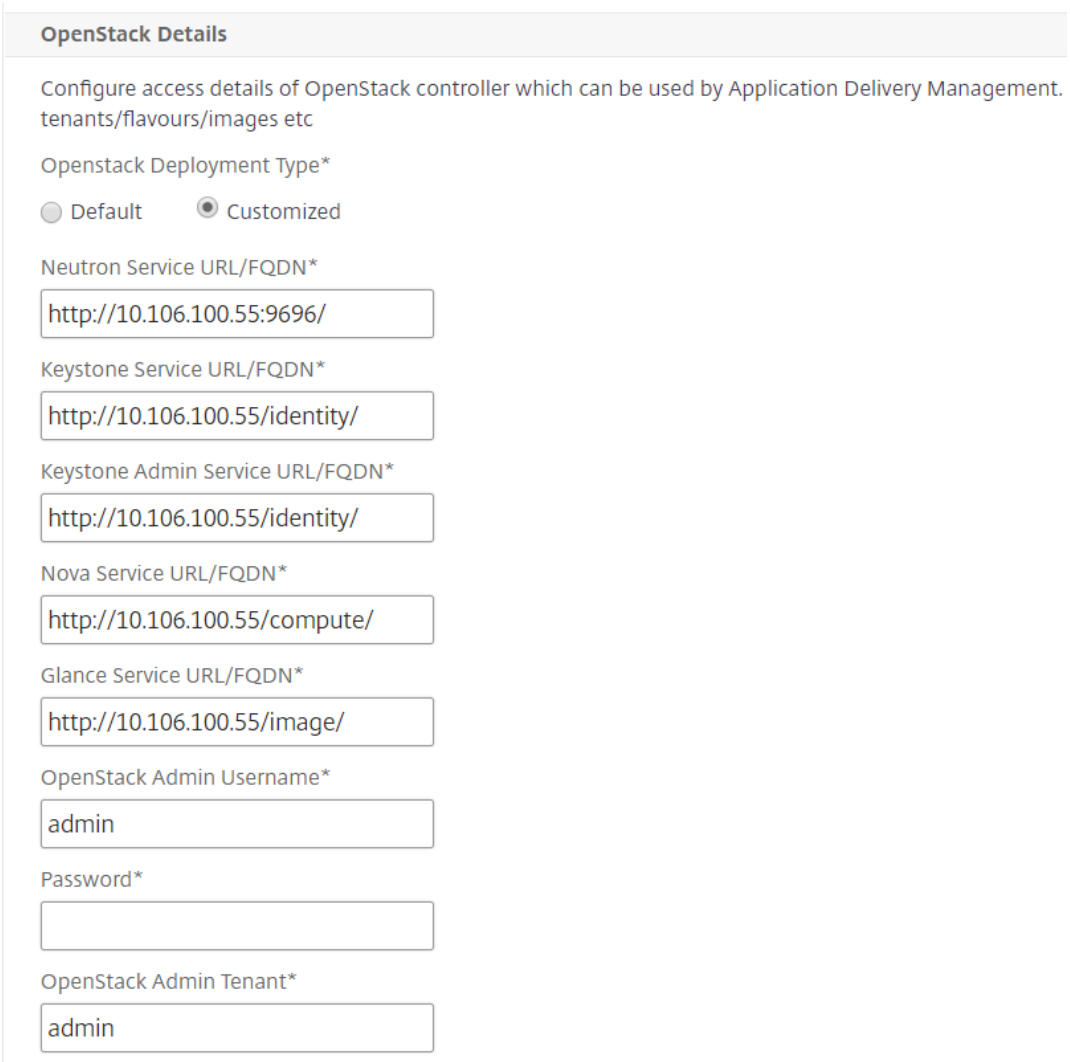


- 自定义部署类型

  如果 OpenStack 服务运行在与默认端口不同的端口上，请选择部署类型为“自定义”。如果这些服务在不同的端口上运行，请在此处指定它们。向 Citrix ADM 注册 **OpenStack** 牛顿和 **Ocata** 版本与注册 OpenStack 派克版本不同。

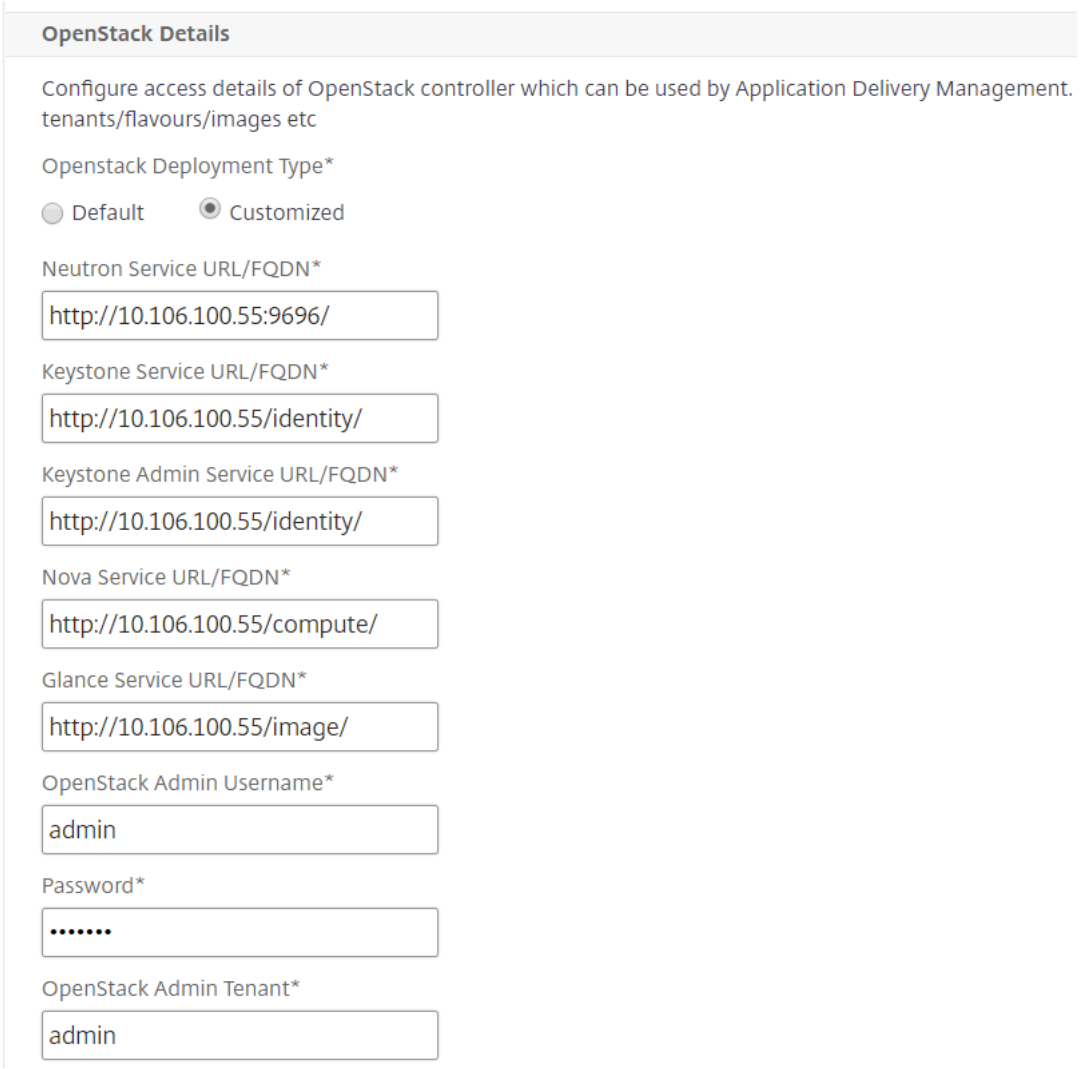
  牛顿和奥卡塔版本的 **OpenStack**：

  1. 如果您正在注册 OpenStack 的牛顿版本，请指定各种 OpenStack 服务的端口号。
  2. 按照您之前在 默认设置中指定的那样，指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名。

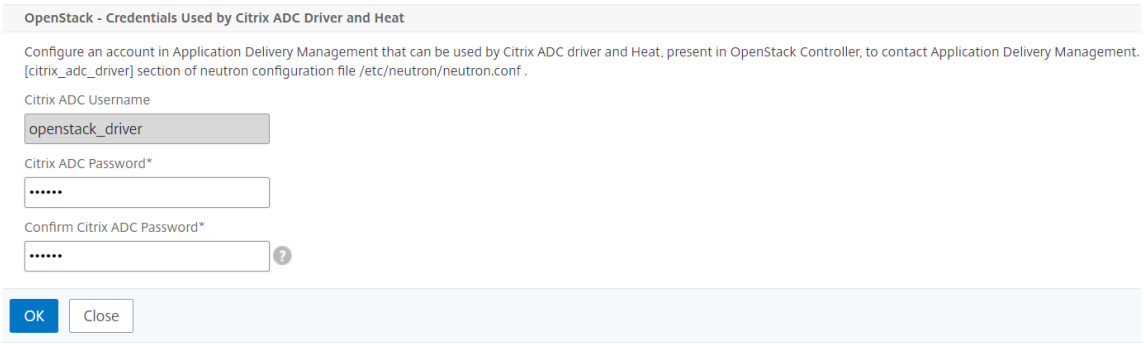


派克发布的开放堆栈：

如果您正在注册 OpenStack 的派克版本，请输入 OpenStack 服务的详细信息，如下图所示。您还必须在默认设置中指定 OpenStack 管理员用户名、密码和 OpenStack 管理员租户用户名。



1. 在 **OpenStack** 中子 **LBaaS-Citrix ADC** 驱动程序使用的凭据部分中，为 OpenStack Citrix ADC 驱动程序用户帐户设置 Citrix ADC 驱动程序密码。Citrix ADM 使用这些凭据对来自 OpenStack Citrix ADC 驱动程序的调用进行身份验证。在 OpenStack 控制器中运行 Citrix ADC 驱动程序安装脚本时，必须指定相同的密码。



2. 单击确定。

在 **OpenStack** 上创建租户

在 OpenStack 中创建项目或租户，将用户添加到项目或租户，并为所有用户分配角色。OpenStack 中的身份服务 **KeyStone** 为每个 OpenStack 服务提供身份验证服务。身份验证服务使用域、项目（租户）、用户和角色组合。

有关如何创建项目以及在 OpenStack 中执行其他任务的详细信息，请参阅中的 OpenStack 文档http://docs.openstack.org/。

添加 **OpenStack** 租户

1. 在 Citrix ADM 中，导航到编排 > 云编排 > **OpenStack** >**OpenStack** 租户，然后单击添加。
2. 在 **Add OpenStack Tenants**（添加 OpenStack 租户）页面上，单击 **+Add**（+ 添加），然后选择 OpenStack 租户。
3. 单击 “ 确定”。

根据在集成 OpenStack 时是使用预置备的实例还是自动置备实例，执行以下两个任务之一：

- 预置 Citrix ADC 设备
- 在 OpenStack 上自动配置 Citrix ADC VPX 设备

预配 **Citrix ADC** 设备

根据在集成 OpenStack 时是使用预置备的实例还是自动置备实例，执行以下两个任务之一：

- 预置 Citrix ADC 设备
- 在 OpenStack 上自动配置 Citrix ADC VPX 设备

预配置 **Citrix ADC** 设备

在任何 Hypervisor 平台（如 Citrix Hypervisor、KVM 或 ESX）上安装 Citrix ADC 设备，然后将该实例添加到 Citrix ADM 中。然后，Citrix ADM 管理此设备，该设备负载均衡服务器中的流量。

要在 **Citrix ADM** 中添加现有的 **Citrix ADC VPX** 实例，请执行以下操作：

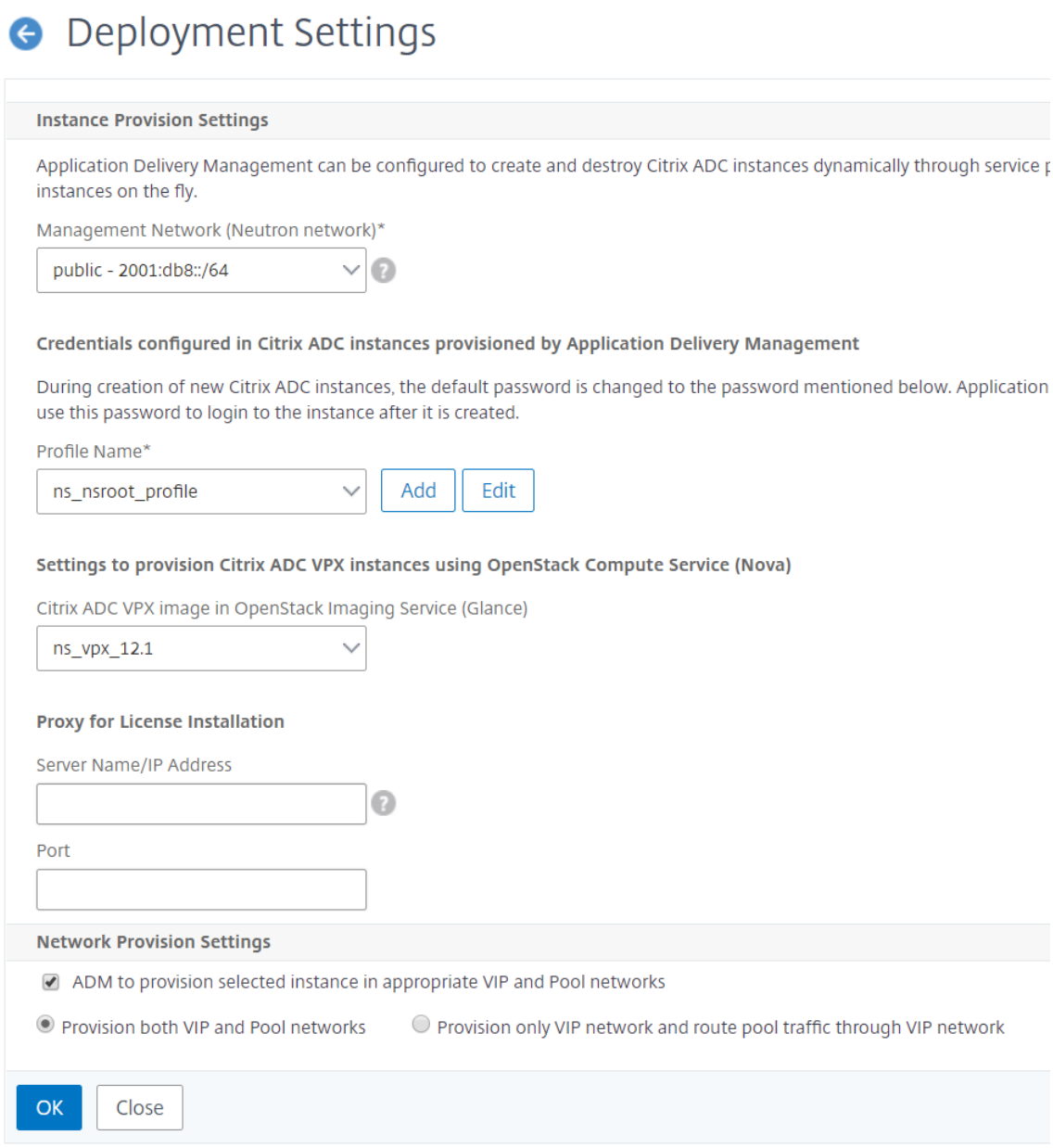
1. 在 Citrix ADM 中，导航到 “基础架构” > “实例” > “**Citrix ADC VPX**”，然后单击 “添加”。
2. 在 “添加 **Citrix ADC VPX**” 页上，指定 Citrix ADC VPX 实例的 IP 地址，然后从 “配置文件名称**”** 列表中选择一个实例配置文件。实例配置文件包含用于登录到 Citrix ADC VPX 的凭据。还可以单击 + 图标创建新实例配置文件。单击确定。

自动配置 **Citrix ADC** 设备

从 Citrix 下载页面下载所需的 Citrix ADC 实例映像，然后通过 OpenStack 映像服务一览上传它。在将实例分配给租户时，使您可以按需配置 Citrix ADC 实例。

要在 **OpenStack** 上自动置备 **Citrix ADC VPX** 设备，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 编排” > “ 云编排” > “ **OpenStack**”。
2. 单击 “部署设置”。
3. 设置以下参数：
   a) 管理网络-选择 OpenStack 上的管理网络，自动配置的 Citrix ADC VPX 连接到该网络。
   b) Profile Name（配置文件名称）- 从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
   c) 许可证-提供用于许可新的自动置备 Citrix ADC 实例的 Citrix ADM 许可证访问代码。Citrix ADM 在管理网络中的 OpenStack 计算上配置 Citrix ADC 实例，然后使用指定的许可证代码在这些实例上触发许可证安装。然后，Citrix ADC 实例使用此处指定的许可证访问代码从 Citrix 网站下载许可证文件。
   d) Citrix ADC VPX 映像概览-选择用于创建 Citrix ADC VPX 实例的 OpenStack 概览中可用的 Citrix ADC VPX 映像。
   e) 代理设置-提供用于安装许可证的 Citrix ADC 代理服务器的详细信息。如果 Citrix ADC 无法通过管理网络直接访问互联网，则可能需要这样做。
4. 单击确定。



在 **Citrix ADM** 中创建服务包

要在 **Citrix ADM** 中为租户创建服务包，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 编排” > “ 云编排” > “ **OpenStack** ” > “ 服务包”，然后单击 “ 添加”。
2. 在 “ 服务包” 页上指定以下参数：
   a) Name（名称）- 服务包的名称。例如，输入 SVC-PKG-GOLD。
   b) Citrix ADC 实例分配-在服务包中定义的实例分配类型，Citrix ADC 实例资源分配给租户。选择 专用。有关策略的详细信息，请参阅 服务包隔离策略。

c) Citrix ADC 实例预配-选择 现有实例以将现有 Citrix ADC 实例分配给租户。如果要在配置期间创建 Citrix ADC 实例，请选择 按需创建实例。

d) Citrix ADC 实例类型-选择 **Citrix ADC VPX**。

> 注意：
>
> 选择 Citrix ADC VPX 以分配在 SDX 平台上托管的预配置 Citrix ADC 实例。

3. 单击 “ 继续” 将租户与服务包关联。

> 注意：如果要在 ** 高可用性模式下部署 Citrix ADC 实例，则
>
> 启用预配 ** 置 Citrix ADC 实例对以实现高可用性。

4. 在 分配实例部分中，单击 添加，然后选择要分配给租户的 Citrix ADC 实例，然后单击 继续。
5. 在 分配 **OpenStack** 租户**/**放置策略部分的 **OpenStack** 租户下，单击 添加，然后选择租户。
6. 单击 **Continue**（继续），然后单击 **Done**（完成）。

> 注意：
>
> 如果未找到策略，则会恢复回退机制，并且 Citrix ADM 会根据租户分配 Citrix ADC 实例。如果租户不是任何服务包的一部分，Citrix ADM 将显示一条错误消息，指出：” 租户 <admin> 不是任何服务包的一部分，并且没有默认的服务包。“

创建放置策略（可选）

隔离策略不仅仅基于租户。可以创建灵活的放置策略，这些策略不仅基于租户名称或 ID，而且也基于其他自定义属性。

要在 **Citrix ADM** 中为租户创建放置策略，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 编排**” > “**云编排” > “**OpenStack**” > “放置策略”，然后单击 “添加”。
2. 在 **Add Placement Policy**（添加放置策略）页面上，设置以下参数：
   a) Name（名称）- 键入放置策略的名称
   b) Sample Expressions（示例表达式）- 从列表中选择示例表达式。这些示例有助于构建放置策略。
   c) Expression（表达式）- 根据在前面的字段中选择的示例表达式，在此字段中填充一个布尔表达式。根据需要编辑字段名称。
3. 单击确定。

通过客户端网络启用从 **Citrix ADC** 实例到后端服务器的流量

默认情况下，在 OpenStack 编排工作流中，Citrix ADC 实例会动态绑定到负载均衡器或客户端网络以及成员或服务器网络。

在某些部署中，服务器也可以通过客户端网络访问，并且可以通过客户端 Gateway 进行路由。在这种情况下，Citrix ADC 实例不需要绑定到服务器网络，但只需将它们绑定到客户端网络。

执行以下设置以配置通过客户端 Gateway 的流量。

导航到 “ 编排” > “ 云编排” > “ **OpenStack** ” > “ 部署设置”，然后选择 “ 仅预配 **VIP** 网络和通过 **VIP** 网络路由池流量” 选项。

然后，Citrix ADM 通过在客户端网络中添加 SNIP 来将 Citrix ADC 实例配置到客户端网络，并将进一步添加到客户端网络 Gateway 的默认路由。这使实例能够通过客户端 Gateway 访问服务器。

Citrix ADC SDX 平台上部署的自动配置 **Citrix ADC VPX** 设备

在 Citrix ADM 中添加 Citrix ADC SDX 平台，以便 Citrix ADM 按需在此平台上配置实例。

要自动监控部署在 **Citrix ADC SDX** 平台上的 **Citrix ADC** 实例，请执行以下操作：

1. 在 Citrix ADM GUI 中，导航到 “网络” > “实例” > “**Citrix ADC SDX**”，然后单击 “添加” 以添加 Citrix ADC SDX 平台。
2. 导航到 编排 > 云编排 > **OpenStack** > 部署设置。
3. 在 “管理网络” 部分中，选择 OpenStack 上自动置备的 Citrix ADC SDX 连接到的管理网络。
    a) 在配置文件名称中，从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
    b) 单击确定。
4. 要在 OpenStack 中配置 Citrix ADC SDX 平台，请导航到编排 > 云编排 >**OpenStack**> 服务包。
    a) 单击 “添加” 创建新的服务包。
    b) 输入服务包的名称。
    c) 在 **Citrix ADC** 实例分配字段中，选择专用。
    d) 在 **Citrix ADC** 实例置备字段中，选择按需创建实例，然后在自动配置平台字段中，选择 **Citrix ADC SDX**。
    e) 默认情况下，仅在 Citrix ADC SDX 平台上预配 Citrix ADC VPX 实例。
    f) 单击 继续。
    g) 在 “自动置备设置” 部分，设置 “资源” 属性。
        i. 吞吐量字段。输入 1000 Mbps。
        ii. **Citrix ADC** 版本字段。从列表中，选择上显示的正确版本的 Citrix ADC VPX 映像 Citrix ADC SDX 平台。
    h) 在 **Citrix ADC SDX** 平台部分中，单击添加以将 SDX 平台添加到服务包中。

i) 单击 继续。

j) 在配置 **OpenStack** 租户部分中，单击添加以添加租户。您还可以通过单击“新建”来添加新租户。

k) 单击完成。

5. LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

使用地平线配置 **LBaaS V1**

April 23, 2021

Tom 现在可以登录 OpenStack Horizon 门户，创建 LBaaS 池，并选择此池的所有成员所在的子网。Tom 必须添加虚拟 IP (VIP) 地址并将此 VIP 分配给他创建的池。Tom 还可以在命令行上或通过 API 执行此操作。Tom 服务器的外部客户端可以连接到托管在分配的 Citrix ADC 上的此 VIP 地址，Citrix ADC 会将所有请求分发给已配置端口上的池成员。

LBaaS 池成员是添加到所选池的已负载平衡的服务器。Tom 可以为其中每个成员分配权重和端口。

运行状况监视器用于观察池的所有成员的运行状况和良好运行状态。Tom 可以在 OpenStack 中指定延迟、超时和重试限制来创建运行状况监视模板，此外还可以指定方法、URL 路径以及成功时的预期 HTTP 代码。创建监视器后，Tom 必须将监视器与之前创建的池关联。

有关如何在 OpenStack 中创建池以及其他 LBaaS 配置任务的详细信息，请参阅 开放式堆栈文档。

> 重要
>
> OpenStack 的 Liberty 版本不支持 LBaaS V1。有关详细信息，请参阅 开放式堆栈发行说明。

使用命令行配置 **LBaaS V2**

April 23, 2021

L **Baas V2** 支持 **SSL** 卸载，包括巴比肯管理的证书、证书捆绑包（包括中间证书颁发机构）、SNI 支持以及常规负载均衡功能。LBaas V2 仅支持用于运行配置任务的命令行界面。LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。

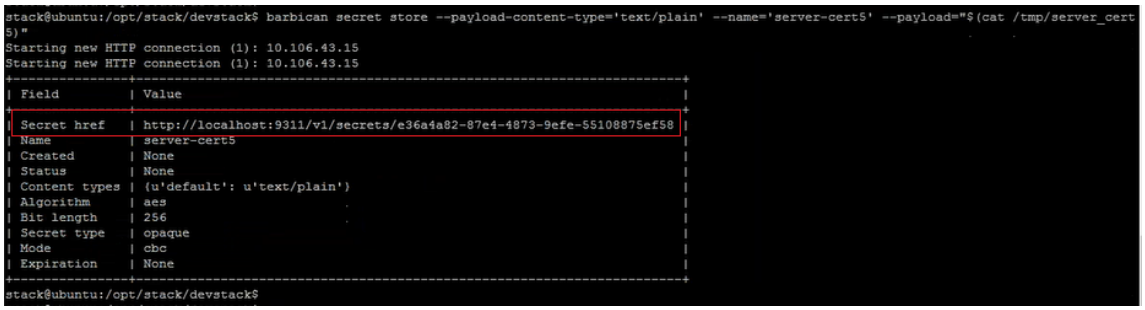
> 注意
>
> 当您需要 SSL 卸载功能时，将证书和密钥上传到 巴比肯服务。如果支持 SSL 卸载，请执行步骤 1、2 和 3，否则继续创建负载均衡器、侦听器、池和成员。[步骤 4()]

1. 使用以下命令将证书上传到 巴比肯服务：

```
barbican secret store --payload-content-type <content_type> --name
    <certificate_name> --payload<certificate_location>
<!--NeedCopy-->
```


示例：

```
barbican secret store --payload-content-type='text/plain' --name='
    hp_server_certificate' --payload=" hp_server/tmp/
    server_certificate"
<!--NeedCopy-->
```



2. 使用以下命令将密钥上传到 **Barbican** 服务：

```
barbican secret store --payload-content-type <content_type> --name
     <key_name> --payload<key_location>
<!--NeedCopy-->
```

示例：

```
barbican secret store -- payload-content-type='text/plain' --name=
    'shp_server_key' --payload="hp-server/tmp/server_key"
<!--NeedCopy-->
```

> 注意
>
> 当你运行这两个 **Barbican** 命令来加载证书和密钥时，Secret href 字段会提供一个位置或 URL。这是安装了 OpenStack 的系统上存储证书和密钥的位置。在步骤 3 中在 **Barbican** 服务上创建容器时，复制这些链接并将这些链接作为参数提供。

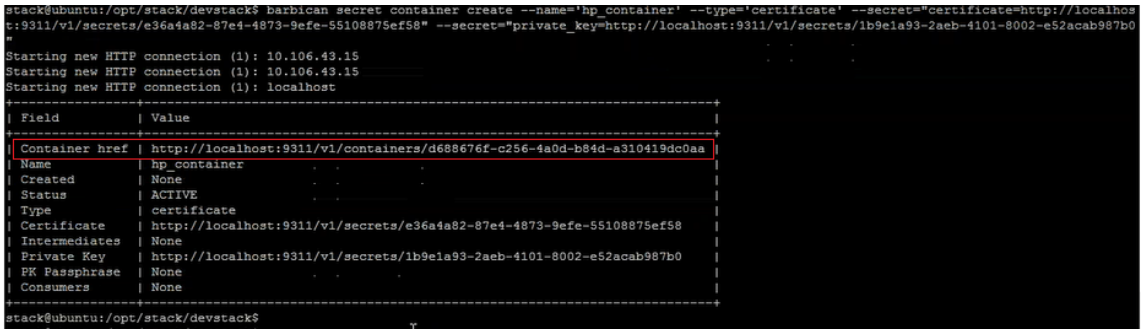
3. 使用以下命令在 **Barbican** 服务中创建容器以存储证书和密钥：

   在命令中，替换为上传证书时从 Secret href 字段获得的 URL。同样，将替换为上传密钥时从 Secret href 字段获得的 URL。


```
barbican secret container create --name<container_name> --type<
    container_type> --secret<certificate_url> --secret<key_url>
<!--NeedCopy-->
```

示例：

```
barbican secret container create --name='hp_container' --type='
    certificate' --secret="`certificate=http://localhost:9311/v1/
    secrets/e36a4a82-87e4-4873-9efe-55108875ef58 --secret="
    private_key=http://localhost:9311/v1/secrets/1b9e1a93-2aeb
    -4101-8002-e52acab987b0`"
<!--NeedCopy-->
```



请复制容器 href 值。在步骤 6 中创建侦听器时必须提供指向容器的链接。

4. 在 OpenStack 中设置环境变量。通过这些变量，OpenStack 客户端命令可以与 OpenStack 服务通信。

   示例：

   export OS_PASSWORD-hp

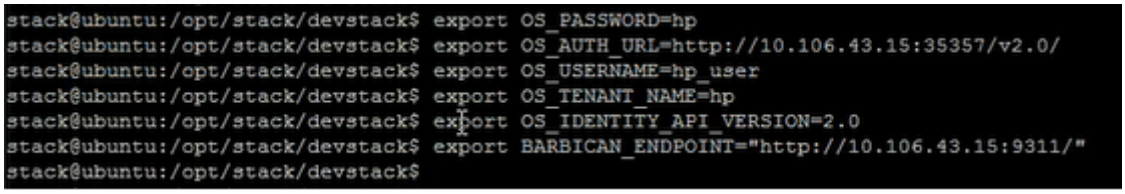
   export OS_AUTH_URL=http://10.106.43.15:35357/v2.0/

   export OS_USERNAME=hp_user

   export OS_TENANT_NAME=hp

   export OS_IDENTITY_API_VERSION=2.0

   export BARBICAN_ENDPOINT="http://10.106.43.15:9311/"



> 注意
>
> 在运行其他命令之前为每个 SSH 会话设置这些变量。有关 OpenStack 环境变量的详细信息，请参阅 开放式堆栈环境变量。

5. 使用以下命令创建负载均衡器：

```
neutron lbaas-loadbalancer-create --name <loadbalancer-name>  <
    subnet-name> --provider <netscaler>
<!--NeedCopy-->
```

示例：

```
neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --
    provider netscaler
<!--NeedCopy-->
```

```
stack@ubuntu:/opt/stack/devstack$ neutron lbaas-loadbalancer-create --name hp-lb-test hp-sub1 --provider netscaler
Created a new loadbalancer:
+---------------------+--------------------------------------+
| Field               | Value                                |
+---------------------+--------------------------------------+
| admin_state_up      | True                                 |
| description         |                                      |
| id                  | 746d730b-3b63-418f-a816-d8dd5472963c |
| listeners           |                                      |
| name                | hp-lb-test                           |
| operating_status    | OFFLINE                              |
| provider            | netscaler                            |
| provisioning_status | PENDING_CREATE                       |
| tenant_id           | 0f30b93cd0cd4482b92d033e1628aa8f     |
| vip_address         | 15.0.0.27                            |
| vip_port_id         | 36636748-15c1-4ec3-9328-496ee74e64fc |
| vip_subnet_id       | 0bb433c4-4b90-4de0-803f-9df92aa46ac4 |
+---------------------+--------------------------------------+
stack@ubuntu:/opt/stack/devstack$
```

成功创建负载平衡器后，状态从 PENDING_CREATE 变为 ACTIVE。

```
+--------------------------------------+------------+-------------+---------------------+-----------+
| id                                   | name       | vip_address | provisioning_status | provider  |
+--------------------------------------+------------+-------------+---------------------+-----------+
| 0d5e8e17-41c2-41bb-aab5-2b3f8f5af4c5 | hp-lb8     | 15.0.0.25   | ACTIVE              | netscaler |
| 1092f752-aa25-4262-aacc-014725fe2921 | hp_lb3     | 15.0.0.19   | ACTIVE              | netscaler |
| 41dbe490-6d9c-4ce5-8d88-bb55953f5961 | hp-lb7     | 15.0.0.24   | ACTIVE              | netscaler |
| 746d730b-3b63-418f-a816-d8dd5472963c | hp-lb-test | 15.0.0.27   | ACTIVE              | netscaler |
| 9d65f6a4-5be5-44fd-a4bd-0808084557b0 | hp-lb1     | 15.0.0.18   | ACTIVE              | netscaler |
| cf8ee4b7-a9f5-41c5-a76a-cd2520e0a7a3 | hp-lb6     | 15.0.0.23   | ACTIVE              | netscaler |
| f7f7dd6e-28eb-40f2-b26c-e541138c6a06 | hp-lb4     | 15.0.0.20   | ERROR               | netscaler |
+--------------------------------------+------------+-------------+---------------------+-----------+
```

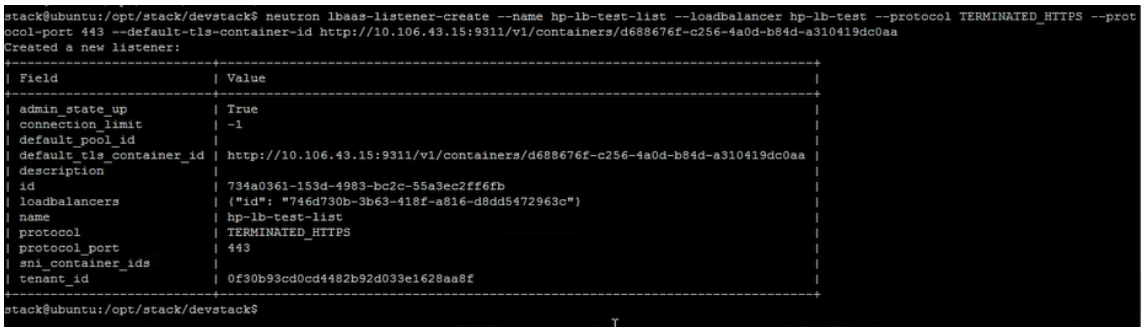
6. 使用以下命令创建监听器：

```
neutron lbaas-listener-create --loadbalancer <loadbalancer-name>
    --name <listener-name> --protocol <protocol_type> --protocol-
    port <port_number> --default-tls-container-id<container_url>
<!--NeedCopy-->
```

示例：


```
neutron lbaas-listener-create --name hp-lb-test-list  --
    loadbalancer hp-lb-test --protocol TERMINATED_HTTPS --protocol-
    port 443 --default-tls-container-id `http://10.106.43.15:9311/
    v1/containers/d688676f-c256-4a0d-b84d-a310419dc0aa`
<!--NeedCopy-->
```

> 注意
>
> 如果您正在创建没有 SSL 卸载支持的侦听器，请运行以下命令而不向容器提供位置：
>
> `neutron lbaas-listener-create --loadbalancer <loadbalancer-name> --name <listener-name> --protocol <protocol_type> --protocol-port <port_number>`

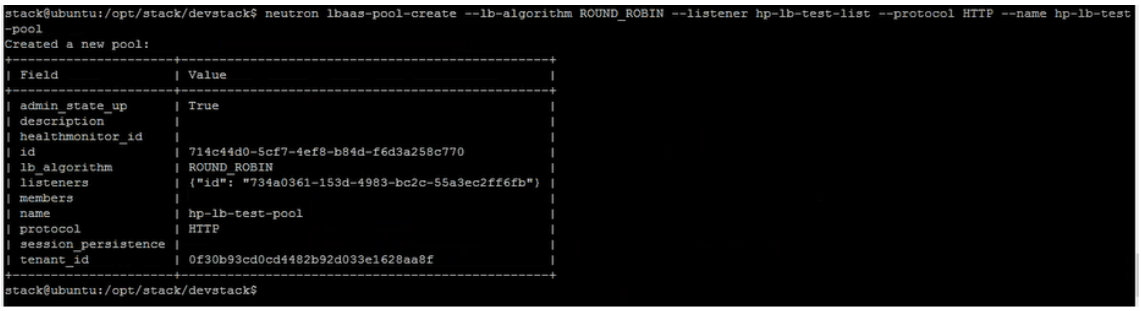


7. 使用以下命令创建池：

```
neutron lbaas-pool-create --lb-algorithm <algorithm_type> --
    listener <listener-name> --protocol <protocol_type> --name <
    pool-name>
<!--NeedCopy-->
```

示例：

```
neutron lbaas-pool-create --lb-algorithm LEAST_CONNECTIONS --
    listener demolistener --protocol http --name demopool
<!--NeedCopy-->
```

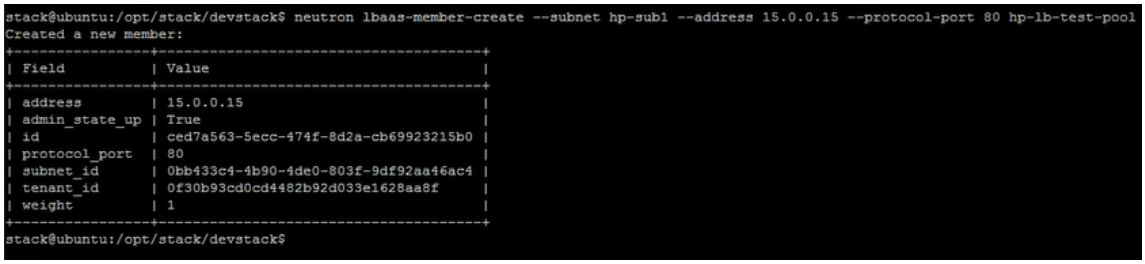


8. 使用以下命令创建成员：


```
neutron lbaas-member-create  --subnet <subnet-name> --address <ip-address of the web server> --protocol-port <port_number>  <pool-name>
<!--NeedCopy-->
```

示例：

```
neutron lbaas-member-create --subnet hp-sub1 --address 15.0.0.15 --protocol-port 80 hp-lb-test-pool
<!--NeedCopy-->
```



监控 **Citrix ADM** 中的 **OpenStack** 应用程序

您的租户可以使用其 OpenStack 凭据登录到 Citrix Application Delivery Management (ADM)，以监视从任何浏览器从 OpenStack 创建的 VIP 和池。URL 必须采用以下格式：

`http://<mas_ip>/<admin_ui>/mas/ent/html/cc_tenant_main.html`

其中 `mas-ip-address` 是在 OpenStack 中注册的 Citrix ADM IP 地址。

> 注意
>
> - OpenStack VIP 对应于 Citrix ADM 中的虚拟服务器。
> - OpenStack 池对应于 Citrix ADM 中的服务组。
> - OpenStack 池成员对应于 Citrix ADM 中的服务组成员。

配置第 **7** 层内容交换

April 23, 2021

Citrix Application Delivery Management (ADM) 与 OpenStack 协调，在 Citrix ADC 实例上配置第 7 层 (L7) 交换或基于内容的交换功能。内容交换与简单的负载平衡不同，因为特定类型的请求可以导向到特定服务器。在 OpenStack 中使用 Citrix ADC 实例作为提供程序创建 L7 配置时，Citrix ADM 会分配一个 Citrix ADC 实例，并部署与 L7 配置对应的内容交换和响应器配置。然后，Citrix ADC 实例可以根据请求的应用层特征分发和负载平衡用户请求。

OpenStack 7 层 (L7) 负载平衡功能组合了负载平衡和内容交换，可针对特定类型内容提供优化交付。这只运行适用于内容的策略，从而提高了负载均衡器的性能。7 层负载平衡还有利于提高应用程序基础结构的效率。由于能够根据类型、URI 或数据分开内容，因此能够在应用程序基础结构中优化物理资源的分配。例如，浏览到 http://example-sports.com/about-us 的最终用户由托管有关公司和服务的内容的服务器池提供服务，而浏览到 http://example-sports.com/shopping-cart-football 的用户则由另一个服务器池提供服务，允许用户进行在线购买。

在 L7 交换中，负载平衡器实现为内容交换虚拟服务器，该服务器接受来自用户的 HTTP 请求，并将请求分发到应用程序服务器。L7 交换或内容交换允许您通过单点进入来访问各种后端服务（例如，不仅有 Web 应用程序、Web 服务门户、Web 邮件，而且有移动管理、不同语言的内容等）。即，您可以为您向用户提供的所有服务提供一个公用 IP 地址。

与较低级别的负载平衡不同，7 层交换不要求池中的所有服务器具有相同的内容。使用 L7 交换的负载平衡器配置假定不同池中的应用程序或后端服务器具有不同的内容。L7 交换可以根据 URI、主机、HTTP 标头或应用程序消息中的任何其他内容导向请求。应用程序服务器基本上服务于特定类型的内容。例如，一台服务器只能提供图像，另一台服务器可能运行服务器端脚本语言，如 PHP 和 ASP，另一台服务器可以提供 HTML、CSS 和 JavaScript 等静态内容。

L7 规则

以下属性在规则中定义，用于评估流量，它们将与规则中定义的值进行比较：

- 主机名：将 HTTP 请求中的主机名与规则中的 value 参数进行比较。例如 www.example-sports.com。
- path：HTTP URI 的路径部分将与规则中的值参数进行比较。例如，“www.example-体育/购物车/足球/html”
- file_type：URI 的最后一部分将与规则中的值参数进行比较。例如，txt、html、jpg、PNG、xls 等。
- header：主要参数中定义的标头将与规则中的值参数进行比较。
- cookie：主要参数指定的 cookie 将与规则中的值参数进行比较。cookie request-header 字段值包含存储的 URL 信息的名称和值对；常规语法如下 - Cookie: name=value。例如，正在寻找一个名为 “存储” 的 cookie 的规则，其值以 “足球-” 开头将如下所示：类型 = Cookie，比较类型 = 开始，键 = 商店值 = 足球-。

比较类型

评估流量时，L7 策略将以下表达式与规则中定义的属性进行比较。

- regex：Perl 类型正则表达式匹配
- starts_with：字符串开头
- ends_with：字符串结尾
- contains：字符串包含
- equal_to：字符串等于

> 注意
>
> 主机名、路径、标题和 Cookie 属性支持所有比较类型，但 file_type 属性仅支持正则表达式和 equal_to。

L7 策略

L7 策略处理传入 HTTP 流量，当匹配策略中定义的所有规则时返回 “true” 值。

在任何 L7 策略中，所有规则都通过 AND 运算符以逻辑方式连接在一起。请求必须匹配所有规则，策略才会返回 “true” 值。负载平衡器采取的操作基于策略返回的值。您可以创建具有相同操作的另一个策略，在规则之间实现逻辑 OR 运算。

例如，您可以创建一个策略，在此策略中，传入 HTTP 请求可以包含词语 “EXAMPLE-SPORTS”、“SPORTS-FOOTBALL” 或 “EXAMPLE-FOOTBALL”，以便负载平衡器可以采取合适的操作将这些请求转发到 Example-sports ecommerce 公司的服务器池，从而为请求的内容提供服务。您可以创建另一个策略，它采取相同操作但匹配 “example-sports”、“example-sports-football” 或 “example-football”。如果用户发送的 HTTP 请求包含这六个关键字中的任何一个，负载平衡器都将请求转发到 Example-Sports 服务器。

根据策略中定义的规则，L7 策略可以采取以下任何操作：

- 重定向到池 - 将请求转发到与 L7 策略关联的规则标识的应用程序服务器。即，您可以创建一个应用程序规则以根据域名将请求定向到特定负载平衡器池。例如，您可以创建一个规则，将针对 example-football.com 的一些请求定向到 pool_1，将针对 example-sports-online_purchase.com 的其他请求定向到 pool_2。
- 重定向到 URL - 向客户端发送位置响应头包含新位置的重定向 HTTP 响应。浏览器使用新位置更新地址栏并发出新请求。用例很多。例如，如果 Web 站点地址发生变化，您可以将请求重定向到新地址，而不是丢弃。或者，在 Web 站点维护期间，您可以将用户重定向到只读站点。
- 拒绝 - 拒绝请求且不采取任何进一步操作。例如，您可以返回 401 未经授权的响应，以拒绝访问受限网页的用户。

内容交换配置包括内容交换虚拟服务器、负载平衡设置（包括负载平衡服务器和服务）以及内容交换策略。创建内容交换虚拟服务器和策略后，应将每个策略绑定到内容交换虚拟服务器。将策略绑定到内容交换虚拟服务器时，应指定目标负载平衡虚拟服务器。请求到达内容交换虚拟服务器时，该虚拟服务器将关联的内容交换策略应用于该请求。策略的优先级定义绑定到内容交换虚拟服务器的策略的评估顺序。

可以将具有侦听器 ID 的任何池分配为流量转移到的默认虚拟服务器池。池与侦听器松散绑定在一起，仅通过实现 L7 策略与侦听器关联。还可以直接在负载平衡器下创建池，无需绑定到侦听器。在这种情况下，池创建时处于 “pending_create” 状态。由于 L7 策略与侦听器紧密绑定在一起，因此必须创建并实现包含池 ID 的 L7 策略，池才能处于 “active” 状态并开始接收流量请求。

一个池可以由多个 L7 策略提供服务，但在至少附加了一个策略时保持 “active” 状态。删除最后一个策略后，池返回到 “pending_create” 状态，直到创建了另一个策略并与之关联。如果删除池本身，则原本由它接收的所有 HTTP 请求都重定向到默认池。

OpenStack L7 策略和 Citrix ADC 实体之间的映射

OpenStack	Citrix ADC 实体	说明
操作为 REDIRECT_TO_POOL 的 L7 策略	内容交换策略 > 内容交换操作	Citrix ADM 创建一个内容交换策略，该策略绑定到内容交换虚拟服务器，并与内容交换操作相关联，该操作指定应用程序服务器的目标池，以便检索内容并向用户呈现。
操作为 REDIRECT_TO_URL 的 L7 策略	响应方策略 > 响应方操作	Citrix ADM 创建一个响应程序策略，该策略绑定到内容交换虚拟服务器，并与响应程序操作关联，该操作指定要向用户显示的目标 URL。
操作为 REJECT 的 L7 策略	响应方策略 > 丢弃请求	Citrix ADM 创建一个响应程序策略，该策略绑定到内容交换虚拟服务器，并与删除请求的响应程序操作相关联。

如果评估为 “true” 的 L7 策略操作将流量重定向到处于 “create_ 挂起” 状态的池，则 Citrix ADM 将实现指定池以及负载平衡虚拟服务器。Citrix ADM 从 L7 策略中创建内容交换策略，并使用相应的内容交换操作将请求重定向到与该池关联的负载平衡虚拟服务器。如果第二个 L7 策略重定向到同一池，Citrix ADM 将创建内容交换策略和内容交换操作，以将流量重定向到与池关联的现有负载平衡虚拟服务器。

策略定位

OpenStack 中对 L7 策略的评估由其优先级确定。在 OpenStack 中，默认情况下，按策略的创建顺序为其分配优先级。第一个创建的策略编号为 1，后续创建的策略连续编号。但您可以更改策略的优先级，为其分配不同的优先级。策略始终按其优先级顺序进行评估。首先运行与特定请求匹配的第一个策略。

创建策略时，应注意以下事项：

- 如果为新策略分配的优先级与某个现有策略相同，则新策略采用该优先级。现有策略的优先级将会降低。如有必要，还可以降低其他策略的优先级以保持策略的评估顺序。
- 如果创建新策略时未指定位置，则新策略将只是附加到列表中。
- 如果创建新策略时为其分配的位置大于列表中已有的策略数，则新策略将附加到列表中，即，新策略的优先级将始终为下一个可用优先级。例如，假定有三个策略 A、B 和 C，优先级为 1、2 和 3，如果创建一个策略并为其分配优先级 8，则新策略的优先级将变为 4。
- 如果向列表添加策略或从列表中删除策略，则策略位置值将从 1 重新排序，而不会跳过数字。例如，假定策略 A、B、C 和 D 的位置值为 1、2、3 和 4，如果从列表中删除策略 B，则策略 C 现在排在第二个位置，策略 D 排在第三个位置。

在 Citrix ADM 中，始终存在与优先级为 1 的 csvserver 关联的默认策略。此默认策略指定 lbvserver 在任何给定时间点处理的 TCP 连接数。因此，当在 Citrix ADC 中创建相应的响应程序策略和内容交换策略时，它们的优先级总是高于相应 L7 策略的优先级 1。例如，如果 L7 策略的优先级为 1，则创建的内容交换策略的优先级为 2。同样，如果 L7 策略的优先级为 2，则创建的响应方策略的优先级为 3。

在 OpenStack 中，首先评估 “拒绝” 或 “redirect_to_url” 策略，然后评估 “redirect_to_pool 策略。在 Citrix ADC 实例中，始终首先评估响应程序策略，以删除请求或向用户提供重定向的 Web 地址，最后评估内容切换策略。如果内容交换策略和响应方策略相互排斥，则此评估顺序通常不会导致出现任何冲突。也就是说，两个 L7 策略不能具有相同的表达式。派生表达式将添加到响应程序和内容切换策略中，以避免此类冲突。例如，编写一个表达式用于拒绝发送到 “sports-football.com” 的所有请求，编写另一个表达式用于允许发送到 “example-sports-football.com” 的请求。创建 L7 策略以使拒绝请求的所有响应方策略排列在评估列表顶部，后面依次接着用于 Web 定向的响应方策略和内容交换策略。

在 Citrix ADM 中，始终存在与优先级为 1 的 csvserver 关联的默认策略。此默认策略指定 lbvserver 在任何给定时间点处理的 TCP 连接数。因此，当在 Citrix ADC 中创建相应的响应程序策略和内容交换策略时，它们的优先级总是高于相应 L7 策略的优先级 1。例如，如果 L7 策略的优先级为 1，则创建的内容交换策略的优先级为 2。同样，如果 L7 策略的优先级为 2，则创建的响应方策略的优先级为 3。

在 OpenStack 中，首先评估 “拒绝” 或 “redirect_to_url” 策略，然后评估 “redirect_to_pool 策略。在 Citrix ADC 中，始终首先评估响应程序策略，以删除请求或向用户提供重定向的 Web 地址，最后评估内容切换策略。如果内容交换策略和响应方策略相互排斥，则此评估顺序通常不会导致出现任何冲突。也就是说，没有两个 L7 策略具有类似的表达式。响应程序和内容切换策略中会添加类似的派生表达式，以避免此类冲突。例如，编写一个表达式用于拒绝发送到 “sports-football.com” 的所有请求，编写另一个表达式用于允许发送到 “example-sports-football.com” 的请求。创建 L7 策略以使拒绝请求的所有响应方策略排列在评估列表顶部，后面依次接着用于 Web 定向的响应方策略和内容交换策略。

配置任务

通过 Neutron LBaaS 命令执行 L7 策略和操作实现。

在 OpenStack 中设置环境变量并创建负载平衡器（例如 LB1）。成功创建负载平衡器后，创建侦听器和池（例如 L1、P1 和 P2），并向池添加成员和监视器。例如，P1 是 L1 的默认池，P2 是绑定到 LB1 的池并管理应用程序服务器。

有关如何使用命令行配置 LBaaS V2 的详细信息，请参阅 使用命令行配置 LBaaS V2。

以下命令创建策略并定义特定操作：

创建用于丢弃请求的 **L7** 策略

```
neutron lbaas-l7policy-create --name <L7 policy name> --listener <listener name
    > --action <action-name>
```

示例：

neutron lbaas-l7policy-create –name policy11 –action REJECT –listener L1

上述命令创建响应方策略 policy11 并将其绑定到内容交换服务器以拒绝请求。由于没有为此策略创建规则，因此策略的评估结果为 “false” 并拒绝请求。

创建用于将请求重定向到特定 **URL** 的 **L7** 策略

```
1 中子 lbas-l7 策略创建-名称 <L7 policy name>-侦听器 <listener name>-操作
    <action-name>-重定向-url <redirect-url>
```

示例：

中子计划策略创建-名称策略 12-操作重定向 _TO_URL-侦听器管理员列表 1-重定向 URL http://example-sports/about-us.html

上述命令创建响应方操作以将请求重定向到 URL、创建具有操作的响应方策略以及将此策略绑定到内容交换虚拟服务器。

```
1 中子拉巴斯-l7 规则创建 — 类型主机名称 — 比较型包含 — 值 <value-
    string> <L7 policy name>
2
3 中子拉巴斯-l7 规则创建 — 类型路径 — 比较型包含 — 值 <value-string> <
    L7 policy name>
```

可以使用 AND 运算符连接上述两个规则为响应方策略派生表达式。

创建用于将请求重定向到池的 **L7** 策略

```
1 中子 lbas-l7 策略创建 — 名称 <L7 policy name> — 侦听器 <listener name
    > — 操作 <action-name> — 重定向池 <redirect-pool>
```

示例：

neutron lbaas-l7policy-create –name policy13 –action REDIRECT_TO_POOL –listener admin-list1 –redirect-pool admin-pool2

如果这是第一个 L7 策略，则上述命令将 P2 与 LB1 一起实现、创建内容交换重定向操作以及将请求重定向到 LB1。如果 P2 已存在，则该命令将创建内容交换重定向操作以及将请求重定向到 LB1。

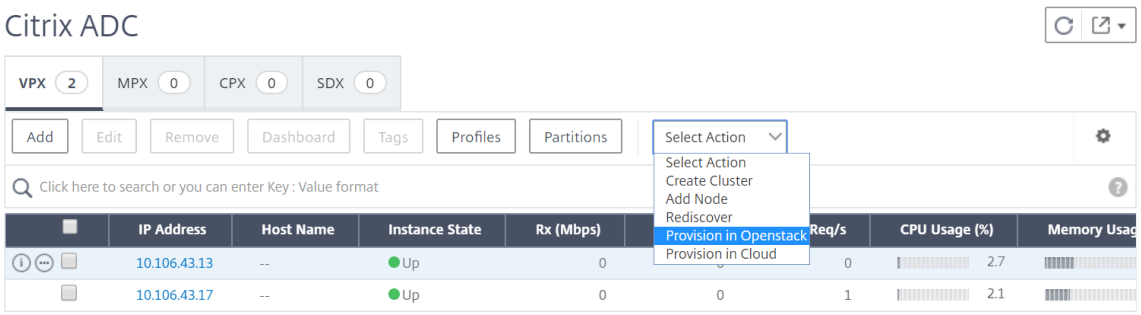
在 **OpenStack** 上手动 **Provisioning Citrix ADC VPX** 实例

April 23, 2021

出于安全原因，在少数企业网络中，Citrix ADC VPX 实例无法连接到 Citrix 许可证服务器以自动下载许可证。在这种情况下，您需要在 OpenStack 平台上手动部署 Citrix ADC VPX 实例。使用从 Citrix 收到的许可证访问代码，下载相应的 Citrix ADC VPX 许可证并将其保存在本地系统中。

要在 **OpenStack** 上手动置备 **Citrix ADC VPX** 实例，请执行以下操作：

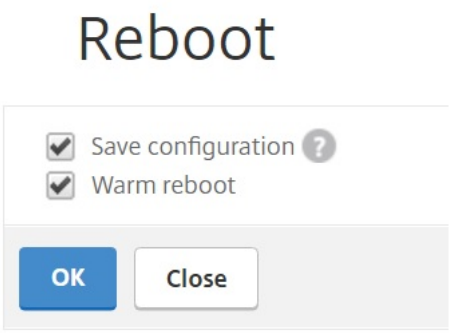
1. 在 OpenStack 上安装 Citrix ADC 驱动程序软件并注册思杰应用程序交付管理 (ADM)
    a) 在 Citrix ADM 中，导航到 “ 编排” > “ 云编排” > “ **OpenStack**”。
    b) 单击 配置打开堆栈设置。在 “ 配置 **OpenStack** 设置” 页中，可以设置用于在 Citrix ADM 中配置 OpenStack 的参数。你在这里有两个选择- 默认和 自定义。
    c) 如果 OpenStack 服务在默认端口上运行，选择 **Default**（默认）。
2. 导航到 编排 > 云编排 > **OpenStack**，然后单击 部署设置。
    a) 管理网络 -选择 OpenStack 上的管理网络，自动配置的 Citrix ADC VPX 连接到该网络。
    b) 配置文件名称 -从下拉列表中选择配置文件。Citrix ADM 使用此配置文件中包含的密码配置新的自动置备的 Citrix ADC VPX 实例。
    c) Citrix ADC VPX 映像概览-选择用于创建 Citrix ADC VPX 实例的 OpenStack 概览中可用的 Citrix ADC VPX 映像。该下拉列表将仅显示 OpenStack Glance 中已有的那些映像。
3. 在 Citrix ADM 中，导航到 “ 编排” > “ 云编排” > “ **OpenStack** ” > “ 服务包”，然后单击 “ 添加”。
4. 在 “ 服务包” 页上指定以下参数：
    a) 名称 -服务包的名称。例如，输入 SVC-PKG-GOLD。
    b) **Citrix ADC** 实例分配 -选择 专用或 分区作为服务包中定义的实例分配类型。
    c) **Citrix ADC** 实例预配 -选择 按需创建实例以在配置期间创建 Citrix ADC 实例。
    d) 自动配置平台 -选择 **OpenStack** 计算。默认情况下，将选择 Citrix ADC VPX 作为实例类型。
    e) 分配 **OpenStack** 租户/放置策略-部分的 OpenStack 租户下，单击 添加，然后选择租户。
    f) 单击 **Continue**（继续），然后单击 **Done**（完成）。
5. 导航到 “ 系统” > “ 系统管理” > “ 更改系统设置”，然后从下拉列表中选择 **http** 。
6. 导航到 “ 网络” > “ 实例” > “ **Citrix ADC VPX**”。
7. 在 **Citrix ADC VPX** 页中，单击 管理下拉列表，然后选择 预配设备。



a) 在“ 设备预配”页面上，输入设备的名称，然后选择您在上一步中创建的服务包。

b) 单击确定。

8. 导航到 编排 > 云编排 >**OpenStack** > 请求选项卡。选择请求，然后单击“ 任务”以查看任务。当任务的状态更改为“ 已完成”时，这意味着 Citrix ADC VPX 是在 Citrix ADM 中置备的。
9. 导航到“网络”>“实例”>“**Citrix ADC VPX** ”，检查 Citrix ADC VPX 实例是否显示在 Citrix ADC VPX 页中。
10. 单击 Citrix ADC VPX 实例。当 Citrix ADC VPX 实例在浏览器窗口中打开时，请登录到该实例。导航到“ 配置”>“ 系统”>“ 许可证”，然后手动添加新许可证。有关如何添加新许可证的详细信息，请参阅Citrix ADC 许可概述。
11. 重新启动 Citrix ADC VPX 实例。



12. 几分钟后，您可以登录到 OpenStack，并在系统 > 实例中，您可以看到 Citrix ADC VPX 实例部署在 OpenStack 上。
13. LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

使用样书在 **OpenStack** 上预配 **Citrix ADC VPX** 实例

April 23, 2021

在 OpenStack 编排工作流中，Citrix Application Delivery Management (ADM) 现在使用 `os-cs-lb-mon` 样书在分配给 OpenStack 租户的 Citrix ADC 实例上部署 LBaaS 配置。将为 OpenStack 用户创建的每个负载均衡器创建一个配置包。

在 OpenStack 工作流程中使用样书进行配置可提供以下好处：

- 通过查看所有配置对象，更好地可视化。
- 通过回滚实现可靠性。
- 支持各种 Citrix ADC 实例类型（Citrix ADC HA、分区、VPX、CPX 和其他）。
- 通过使用自己的样书为 OpenStack 租户部署配置进行自定义。

作为 **Citrix ADM** 管理员，导航到 **“应用程序” > “配置”** 以查看在 **Citrix ADC** 实例上部署的配置包。
您可以执行以下任务：

- 滚动以查看为负载均衡器部署的 `os-cs-lb-mon` 配置包。
- 单击 `os-cs-lb-mon` 样书面板上的查 看定义以检查实例上部署的配置。
- 单击 查看对象可查看在实例上部署的 Citrix ADC 对象或实体的列表。

使用样书 **Provisioning** 实例之前的注意事项

从 Citrix ADM 12.1 版本 49.23 开始，OpenStack 编排工作流的体系结构已更新。此工作流现在使用 Citrix ADM 样书来配置 Citrix ADC 实例。如果要从版本 12.0 或版本 12.1 版本 48.18 升级到 Citrix ADM 12.1 版本 49.23，则必须运行以下迁移脚本：

```
/mps/scripts/migration_scripts/migrate_configurations.py
<!--NeedCopy-->
```

- 运行迁移脚本会创建与现有 OpenStack 配置相对应的 `os-cs-lb-mon` 样书的配置包。
- 如果您从这些早期版本中部署了 OpenStack 配置，则必须运行此迁移脚本。
- 只有在运行版本 12.1 build 49.23 的迁移脚本之后，才能使用 `os-cs-lb-mon` 样书在实例上部署新配置。
- 在运行迁移脚本之前，从 OpenStack 尝试的所有配置都会失败。

> 注意
>
> - 运行迁移脚本后，无法降级到 Citrix ADM 的先前版本。
> - 确保您已将用于 OpenStack LBaaas V2 的 Citrix ADC 驱动程序升级到最新版本。使用与最新的 Citrix ADM 13.0 版本一起提供的 Citrix ADC 捆绑包文件。

LBaaS V2 API 实施通过 Neutron LBaaS 命令执行。连接到任何 Neutron 客户端并运行配置任务。有关如何运行配置命令的更多信息，请参阅使用命令行配置 LBaaS V2。

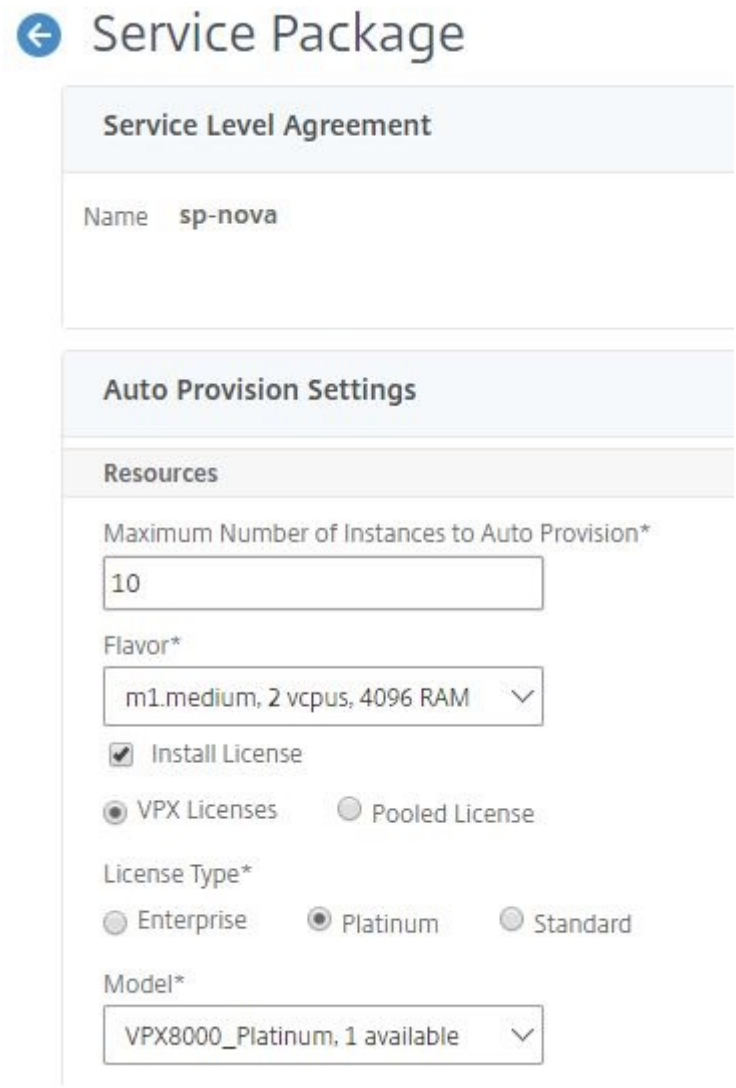
VPX 签入和签出许可证以及 **OpenStack** 环境的池许可证支持

April 23, 2021

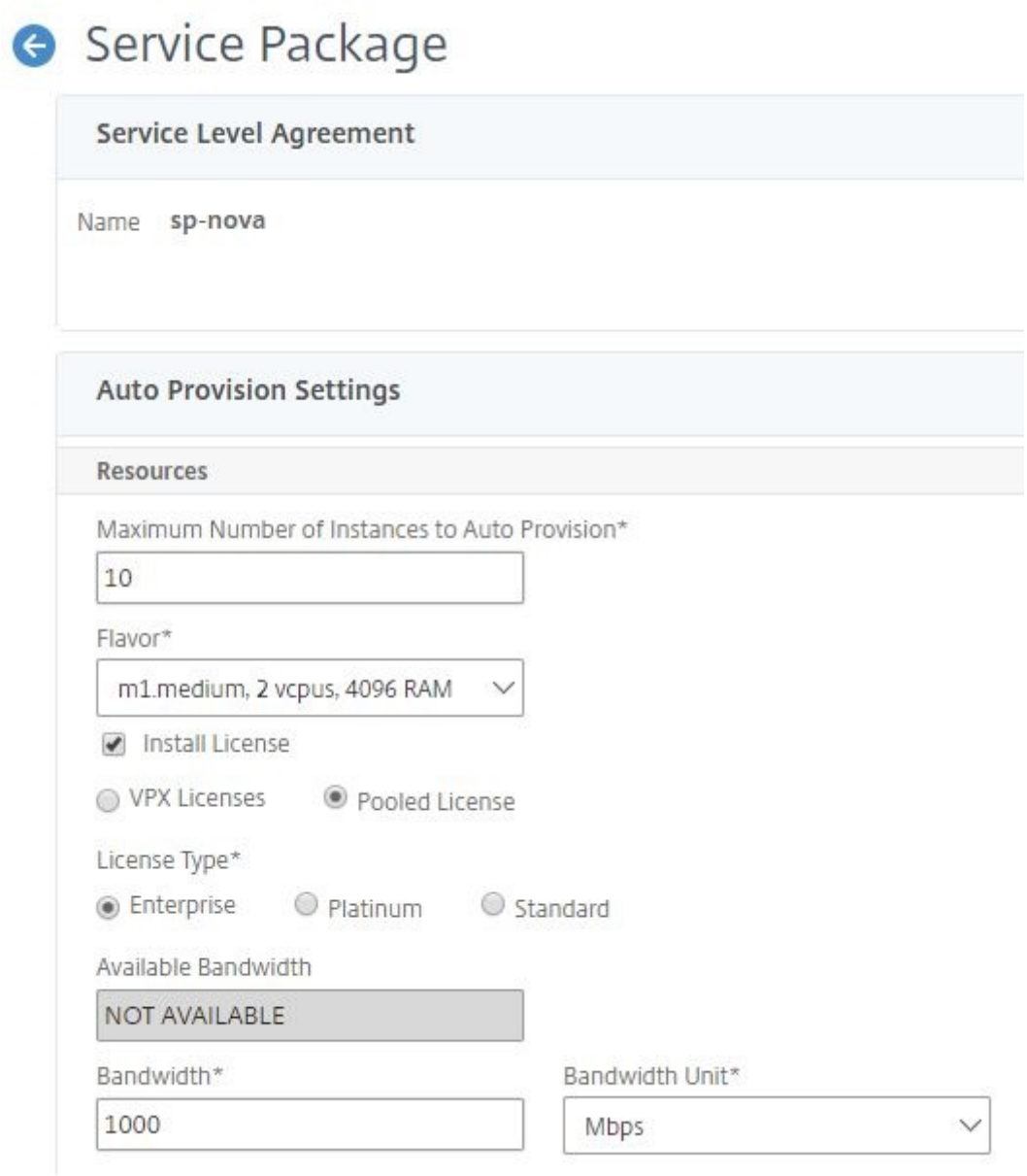
在 OpenStack 编排工作流中，当您选择使用 O **penStack** 计算的服务包时，思杰应用程序交付管理 (ADM) 会根据需要创建 Citrix ADC VPX 实例。现在，Citrix ADM 中业务流程功能中的服务包页面得到了增强，以提供在按需创建的 Citrix ADC VPX 实例上安装所需的许可证。提供的许可证可以是 VPX 签入和签出许可证，也可以是合并许可证。

要使用此功能，必须首先在 Citrix ADM 中上载许可证，然后创建使用 OpenStack 计算的服务包。

- 如果是签入和签出许可证，则可以从各种可用许可证中选择要安装的许可证。



- 如果是池许可证，则可以同时选择要安装的带宽和许可证版本的类型。



每当您以 Citrix ADM 作为提供程序部署第一个负载均衡器时，Citrix ADM 都会创建 Citrix ADC VPX 实例，并将服务包中指定的许可证安装到新创建的实例。

此外，当您删除现有负载平衡实例时，不再需要该实例。实例已停用，并将许可证返回到 Citrix ADM。这样可以优化使用 Citrix ADM 中提供的许可证。

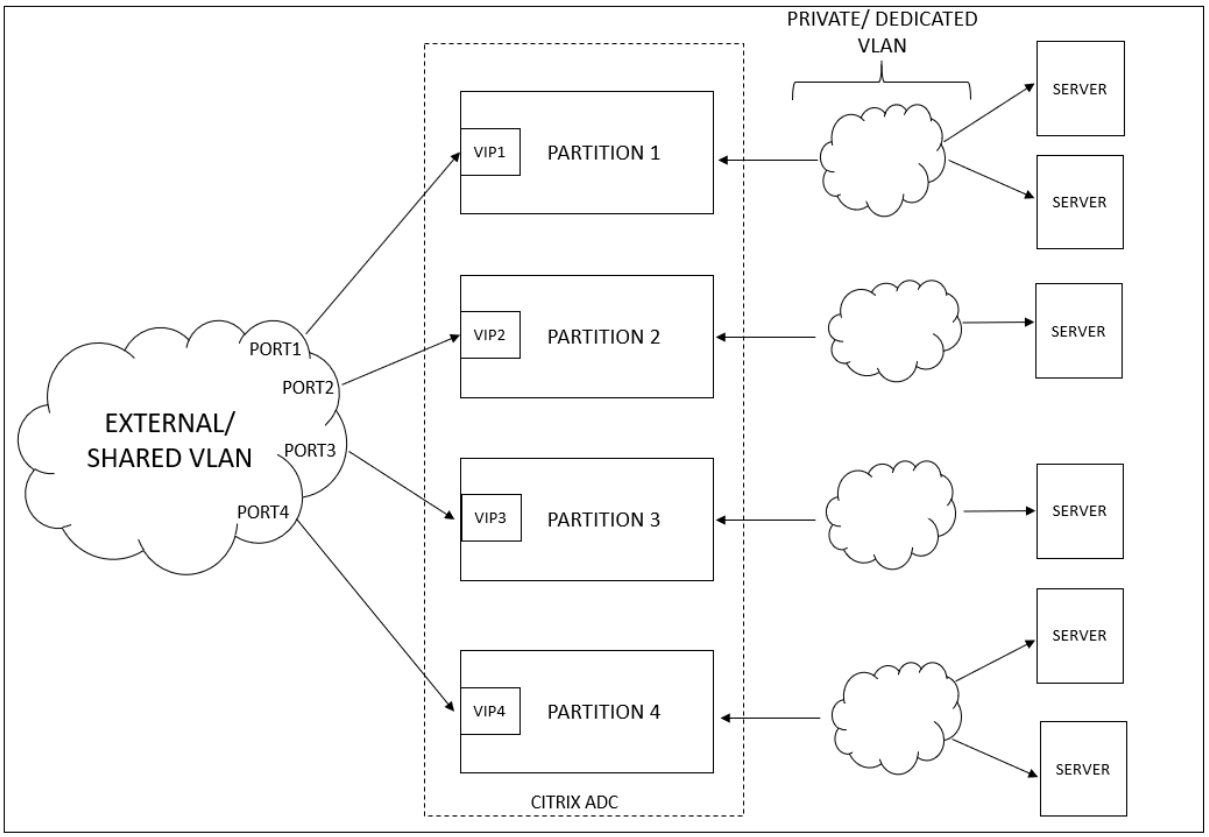
> 注意：
>
> 在高可用性模式下部署 Citrix ADM 时，请考虑将许可证上载到当前活动或主 Citrix ADM MAS-HA-1。当您部署第一个请求并且 Citrix ADM 创建 Citrix ADC VPX 实例时，该实例将从 MAS-HA-1 中签出所需的许可证。在稍后的时间点，假定没有许可证的辅助 Citrix ADM MAS-HA-2 现在处于活动状态。ADC VPX 实例现在无法从 MAS-HA-2 签出许可证，因此无法为新用户创建该实例。

> 在这种情况下，请确保 MAS-HA-1 处于 UP 状态并且现在是当前主节点。也就是说，手动故障切换 Citrix ADM 从 MAS-HA-2 到 MAS-HA-1。之后，您必须重新尝试从 OpenStack 进行配置，并使用适当的许可证重新创建实例。有关 Citrix ADM 高可用性部署中许可证支持的详细信息，请参阅 高可用性。

对管理分区的共享 **VLAN** 支持

April 23, 2021

对于从专用网络连接的租户，Citrix Application Delivery Management (ADM) 支持隔离策略，以便每个租户都拥有自己的专用分区、专用 VLAN 和专用服务器。对于从公用网络连接的租户，专用虚拟 LAN 会要求使用太多的 IP 地址。共享虚拟 LAN 通过在每个分区上创建一个虚拟 IP 地址，由此创建一个单一 IP 子网，避免了此问题

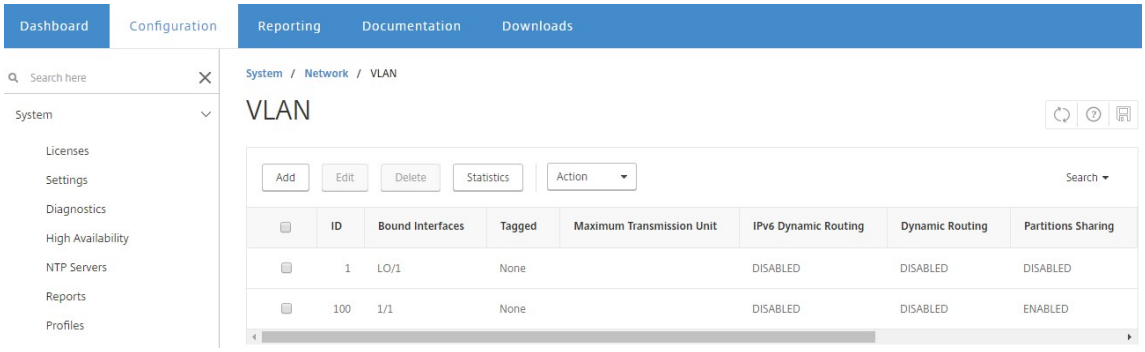


租户配置 VIP 或侦听程序时，系统会在 Citrix ADC 设备中为该租户创建管理分区。所有负载平衡器配置都会被推送到创建的管理分区。如果租户使用共享网络或外部网络创建负载平衡器，那么将会添加该网络的虚拟 LAN，并启用共享功能。当不同租户使用同一共享网络创建其负载均衡器时，VLAN 不会再次添加到 Citrix ADC 中，但 VLAN 也会绑定到第二个分区。因此，使用相同共享网络的任何租户都将获得绑定到相同虚拟 LAN 的分区。

Citrix ADM 支持虚拟目标 MAC 地址。租户共享 VLAN 时，Citrix ADM 会为 Citrix ADC 设备上的分区分配不同的 MAC 地址。这样就可以在多个分区之间或所有租户和所有通信域之间共享虚拟 LAN。

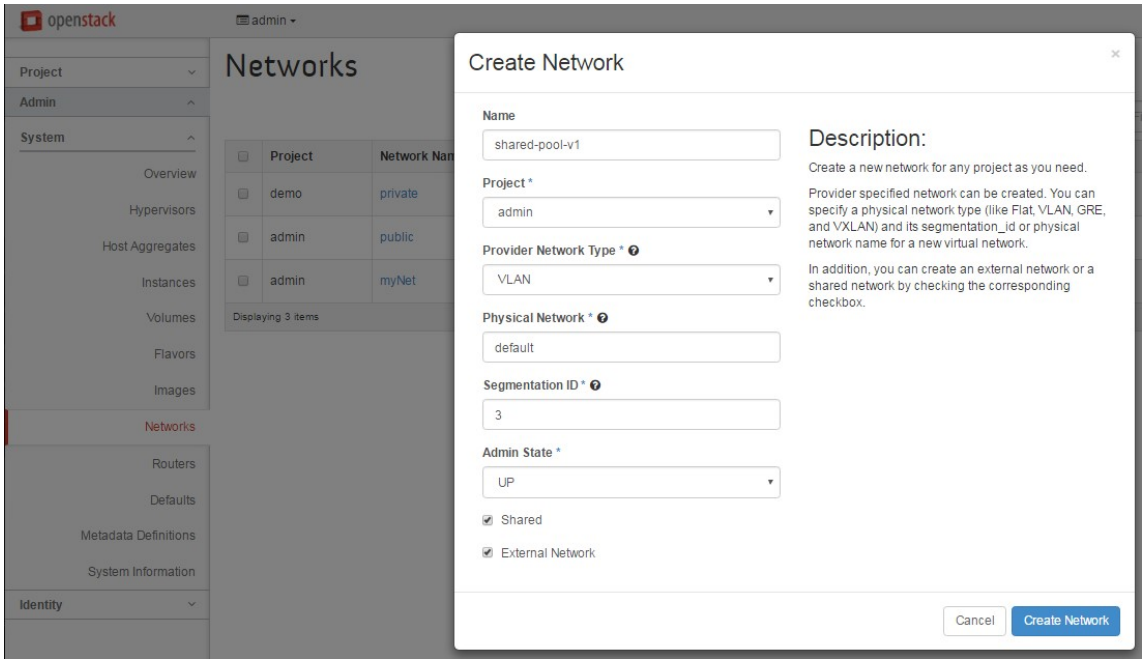
从 **Citrix ADC** 实例配置共享 **VLAN**

1. 在 Citrix ADC 实例中，导航到 “ 配置” > “ 系统” > “ 网络” > “ **VLAN**”，选择一个 VLAN 配置文件，然后单击 “ 编辑” 以设置分区共享参数。
2. 在 配置 **VLAN** 页面上，选中 分区共享复选框。
3. 单击确定。



从 **OpenStack** 调配配置共享虚拟 **LAN**

1. 在 OpenStack 中，导航到 管理 > 系统 > 网络，然后单击 创建网络。
2. 在 **Create Network**（创建网络）中，设置以下参数：
   a) Name（名称）- 输入网络的名称
   b) Project（项目）- 从下拉列表中选择项目
   c) 提供商网络类型-从下拉列表中选择 **VLAN** 。这定义虚拟网络建立为虚拟 LAN。
   d) Physical Network（物理网络）- 此处选择默认物理网络。可以编辑此项。
   e) Admin State（管理状态）- 默认情况下，网络的管理状态是 “UP”（运行）
   f) 选择 **Shared**（共享）和 **External Network**（外部网络）定义共享虚拟 LAN 且虚拟 LAN 使用外部网络。
3. 单击 **Create Network**（创建网络）。



试用许可工作流程

April 23, 2021

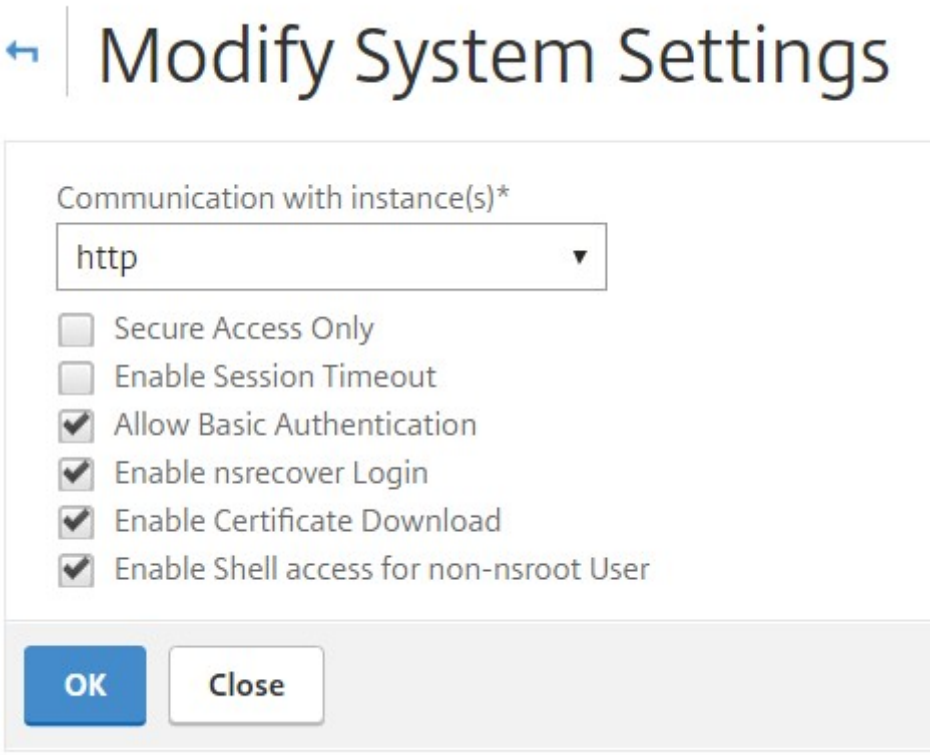
在使用 OpenStack 编排自动置备 Citrix ADC VPX 实例期间，Citrix Application Delivery Management (ADM) 使用 OpenStack 计算启动 Citrix ADC VPX 实例。新置备的 Citrix ADC VPX 实例在设置过程中联系 Citrix 许可门户，并使用许可证访问代码自动下载和安装许可证文件。

试用版许可证

技术支持人员在现场安装 Citrix ADM 和 Citrix ADC VPX 设备时使用试用许可证。适用于 Citrix ADC VPX 的试用或评估许可证的有效期为 90 天。如果需要评估多个 Citrix ADC 或在 90 天后延长测试，则需要申请新的评估许可证。Citrix ADM 为您提供了替代解决方案，而不是自动安装试用许可证文件。您可以手动下载许可证文件并将其安装到 Citrix ADC VPX 上，以完成实例的安装。

如果 Citrix ADC VPX 无法连接到互联网，请将 Citrix ADM 配置为充当 Citrix 许可门户的代理服务器，然后安装许可证文件。

具有试用许可证的 Citrix ADC VPX 实例只能在 HTTP 上与 Citrix ADM 进行通信。要在 Citrix ADM 中配置 HTTP 通信，请导航到“系统**”>“**系统管理”，然后单击“更改系统设置”。从下拉列表中选择 **http** 以设置通信方法，然后单击确定。



与开放式加热服务集成

April 23, 2021

OpenStack Neutron LBaaS 面向应用程序支持核心负载平衡服务，例如，负载平衡、SSL 卸载和内容交换。LBAS 通过 REST API 进行管理，而且该 API 允许租户进行 REST 调用以创建、更新和删除 LBAS 对象。由于 LBaaS 提供负载平衡服务，因此在编排过程中不允许使用更高级的 Citrix ADC 功能。Citrix ADC 加热插件克服了这一限制。

Heat 调配服务

通过 OpenStack Heat 调配服务可以基于模板部署复杂的云应用程序。Heat 调配模板 (HOT) 以文本文件方式描述云应用程序的基础结构，用户可读写这些文件，且版本控制工具可以管理这些文件。编写这些模板使用的是结构化语言 YAML。HOT 模板允许您创建大多数的 OpenStack 资源类型，以及指定在其中定义的资源之间的关系。借助 Citrix ADC 热插件，您可以在任何 Citrix ADC 实例上配置高级应用程序交付 Controller (ADC) 功能。

Citrix ADC 样书

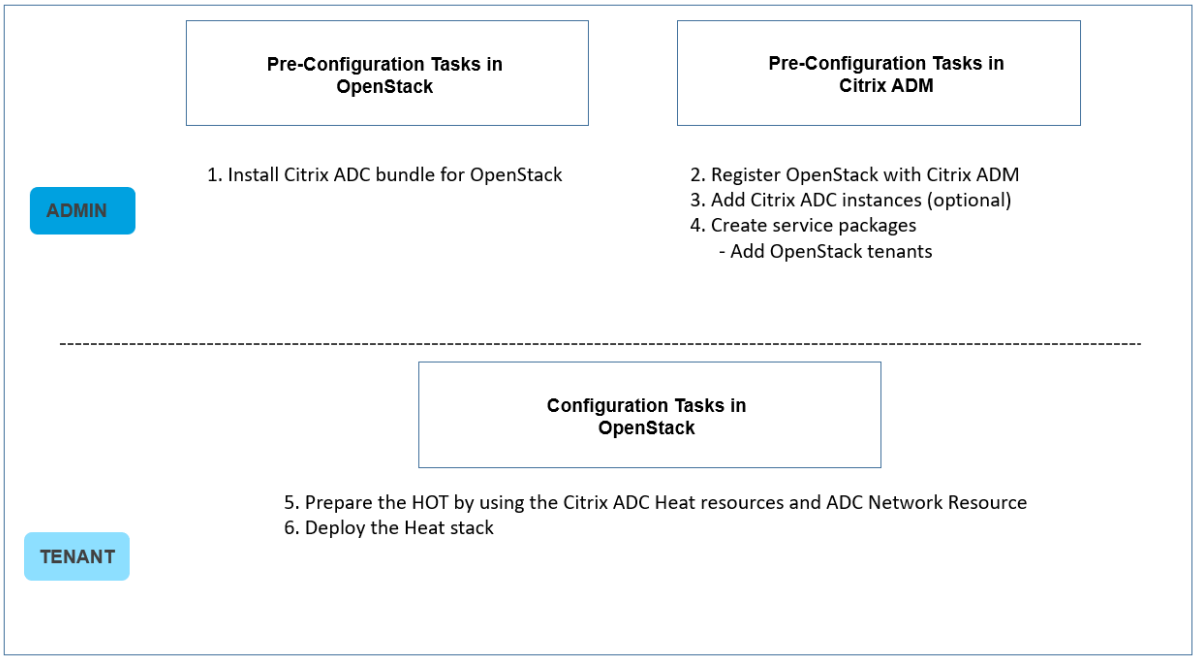
Citrix Application Delivery Management (ADM) 样书可用于创建和配置 Citrix ADC 功能。与 Heat 模板一样，样书也是使用 YAML 编写的。可以为每个功能创建单独的样书，并且可以使用单个样书在多个 Citrix ADC 实例上部署

配置。

在 Citrix ADC 与 OpenStack 集成期间，Citrix ADM 将所有 Citrix ADM 样书作为加热服务中的资源发布。这包括 Citrix ADM 附带的样书和用户在稍后时间点创建的样书。“热量” 模板允许您使用这些样书资源配置 Citrix ADC 的高级功能。

使用热配置 **Citrix ADC** 实例的工作流

以下流程图说明了部署 Heat 堆栈的工作流：



以云管理员身份执行以下任务：

要在 **OpenStack** 中配置热服务，请执行以下操作：

1. 下载适用于 OpenStack 的 Citrix ADC 软件包

   在 OpenStack 中安装 Citrix ADC 软件包。在 Citrix ADM 中，导航到 “下 载” 并下载 Citrix ADC 驱动程序包，解开包，然后将捆绑包中的 “热量” 文件夹的内容复制到 OpenStack 中的 “热量” 资源目录中。目录路径如下：/选项/堆叠/加热/加热/引擎/资源/网络规模器 _ 资源

2. 在 heat.conf 文件中创建一个部分 “netscaler_plugin”，并更新该部分中的以下参数：

   [网络扩展器插件]

   a) 当通信是 HTTP 时，参数将按如下方式更新：

      NMAS_BASE_URI=<http://10.146.103.45:80>

      NMAS_USERNAME=

      NMAS_PASSWORD=

b) 当通信是 https 时，参数将按如下方式更新：

NMAS_BASE_URI=https://common_name_used_in_certificate

NMAS_USERNAME=<openstack_driver_username

NMAS_PASSWORD=<openstack_driver_password>

SSL_CERT_VERIFY=<True_or_False>

CERT_FILE_PATH=<path_of_the_certificate_file>

如果用户将 ssl_cert_ 验证设置为 “False”，Citrix ADM 会在请求调用中发送验证 = False，这将禁用 SSL 证书验证。如果将 SSL_cert_ 验证设置为 “True” 并且存在证件路径条目，则 Citrix ADM 会在请求的验证参数中发送此路径，否则 Citrix ADM 会发送 “验证” = True。

> 注意
>
> ：要在 “高可用性” 模式下部署 Citrix ADM，请在热.conf 文件中更新以下参数：
>
> NMAS_BAS_URI = <IP address of the front-end virtual server>

3. 在 OpenStack 中重新启动加热服务。

在 OpenStack 中重新启动 Citrix ADC 加热服务时，所有定义的 Citrix ADM 样书都将作为资源导入到热量中。此外，Citrix ADC 网络资源和证书资源将作为 Citrix ADC 热量资源导入 OpenStack。

4. 注册 Citrix ADM 与 OpenStack.

a) 在 Citrix ADM 中，导航到 编排 > 云编排 > **OpenStack**，然后单击 配置 **OpenStack** 设置。

b) 在 配置 **OpenStack** 设置页面中，可以设置用于配置 OpenStack 的参数。此处有两个选项：“Default”（默认）和 “Customized”（自定义）。

c) 如果 OpenStack 服务在 默认端口上运行，请选择默认值。输入以下参数：

i. OpenStack 控制器 IP 地址

ii. 管理员用户名

iii. 密码

iv. 开放式堆栈管理租户

v. Citrix ADC 驱动程序和热密码

> 注意
>
> 这与您在加热.conf 文件中输入的密码（NMAS_ 密码）相同。

5. 创建服务包并与租户定义 SLA。

在 OpenStack 注册期间，在 Citrix ADM 中为每个用户创建租户，并且租户信息由 LBaaS 驱动程序和热插件使用。“热量” 插件使用此信息与 Citrix ADM 联系，将样书作为热量资源导入 OpenStack 中。

> 注意：有
>
> 关在 Citrix ADM 和 OpenStack 中创建服务包和其他预配置任务的详细信息，请参阅 [将 Citrix ADM 与 OpenStack 平台集成 ()]。

6. 注意 Citrix ADM 中的所有相关样书都作为资源导入到 OpenStack Heat 中。此外，请观察 Citrix ADC 网络资源和 Citrix ADC 证书资源已作为资源导入 OpenStack 热量。

   > 注意
   >
   > 目前，您只能使用 Citrix ADM 附带的样书。

   您的租户现在可以在 OpenStack 中创建 Heat 模板、输入所需 Heat 参数的值以及部署 Heat 堆栈。部署热量堆栈后，配置将推送到 Citrix ADM，并配置所需的 Citrix ADC 实例。

要准备热模板并启动热堆栈，请执行以下操作：

1. 在 OpenStack 中，租户可以使用 Heat 资源创建 Heat 调配模板 (HOT)。
2. 在 OpenStack Horizon 中，租户管理员可以导航到 “项目” > “编排” > “堆栈” 以创建热量模板并启动热量堆栈。有两种方法可以创建 HOT：

   - 文件 -从本地目录中选择更新的模板
   - 直接输入 -从窗口中的模板复制并粘贴 YAML 内容

   > 注意：成功部署堆栈
   >
   > 后，租户可以使用更改堆栈模板更新堆栈。但不能修改创建堆栈时最初提供的子网信息和虚拟 IP 地址 (VIP)。

   租户部署堆栈后，导航到 “编排” > “云编排” > “**OpenStack**” > “**Citrix ADM** 中的请求”，以观察任务列表。此外，导航到 Citrix ADM 中的应用程序 > 配置以观察 Citrix ADC 实例以样书配置包的形式成功配置。

Citrix ADM 样书的示例：

下图显示了如何构建 Citrix ADM 样书的示例，并简要说明了这些组件。有关 Citrix ADM 样书以及如何使用随附的样书的详细信息，请参阅 样本。


```
name: lb-vserver
description: "This stylebook defines a load balancing virtual server configuration."
display-name: "Load Balancing Virtual Server (HTTP)"
namespace: com.example.stylebooks
schema-version: "1.0"
version: "0.1"
import-stylebooks:
   -
      namespace: netscaler.nitro.config
      prefix: ns
      version: "10.5"
parameters:
       -
      name: name
      type: string
      required: true
      -
      name: ip
      type: ipaddress
      required: true
     -
      name: lb-alg
      type: string
      allowed-values:
        - ROUNDROBIN
        - LEASTCONNECTION
      default: ROUNDROBIN
components:
   -
      name: my-lbvserver-comp
      type: ns::lbvserver
      properties:
          name: $parameters.name
          servicetype: HTTP
          ipv46: $parameters.ip
          port: 80
          lbmethod: $parameters.lb-alg
```

header

StyleBooks imported

parameters

components

热模板示例：

下图显示了 YAML 中定义的“热量”模板的结构，并指向作为“热量”资源导入的样书资源和 Citrix ADC 网络资源。

```
heat_template_version: '2015-10-15'
parameter_groups:
- description: servers
  label: servers
  parameters: [server_ips, server_port]
- description: vip ip
  label: VIP IP
  parameters: [lb-virtual-ip, lb-virtual-port, lb-service-type]
- description: lb-appname
  parameters: [lb-appname]
parameters:
  lb-appname: {description: This is the lb-name, label: LB-NAME, type: string}
  lb-service-type:
    constraints:
    - allowed_values: [HTTP, SSL, TCP, UDP, ANY]
    default: HTTP
    description: This is lb-service-type
    label: Service-type
    type: string
  lb-virtual-ip: {description: This is LB vip, label: VIP, type: string}
  lb-virtual-port: {description: This is virtual port, label: Virtual-port, type: string}
  server_ips: {description: Ip address of servers, label: IP of server, type: comma_delimited_list}
  server_port: {description: Port of server, label: Server port, type: string}
resources:
  sb_config:
    properties:
      lb-appname: {get_param: lb-appname}
      lb-service-type: {get_param: lb-service-type}
      lb-virtual-ip: {get_param: lb-virtual-ip}
      lb-virtual-port: {get_param: lb-virtual-port}
      mas_device_handle:
        get_attr: [network_resource_NS, mas_device_handle]
      svc-servers:
        repeat:
          for_each:
            ipvar%: {get_param: server_ips}
          template:
            ip: ipvar%
            port: {get_param: server_port}
    type: Citrix::NetScaler::Stylebook_com_citrix_adc_stylebooks_1_0_lb
  network_resource_NS:
    properties:
      subnets: [c07d727c-37a6-493a-ab4e-b96d9ddab560]
    type: Citrix::NetScaler::NetscalerNetworkConfigurator
```

version of the Heat template

parameter groups - declares the input parameter groups and order

parameter groups - declares the input parameters

resources - declares template resources; in this example declares the StyleBook resources

resources - declares template resources; in this example declares the NetScaler network resources

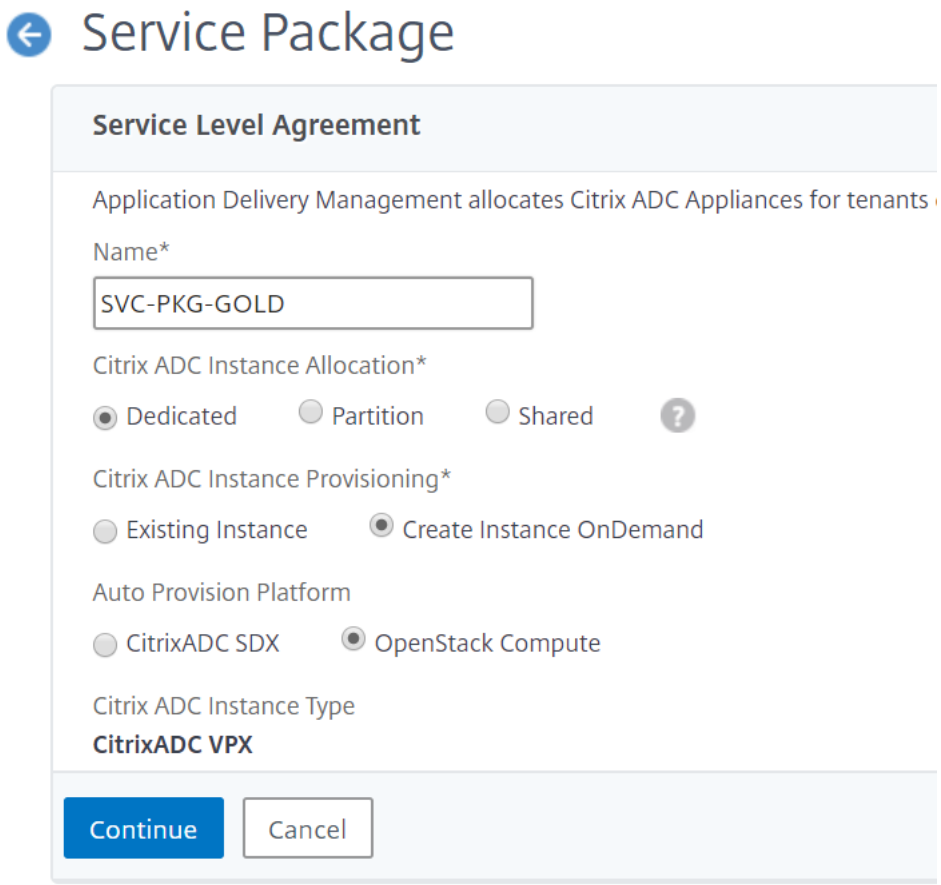
有关 Heat 服务以及如何创建模板的详细信息，请参阅开放式堆栈热量文档。

服务包隔离策略

April 23, 2021

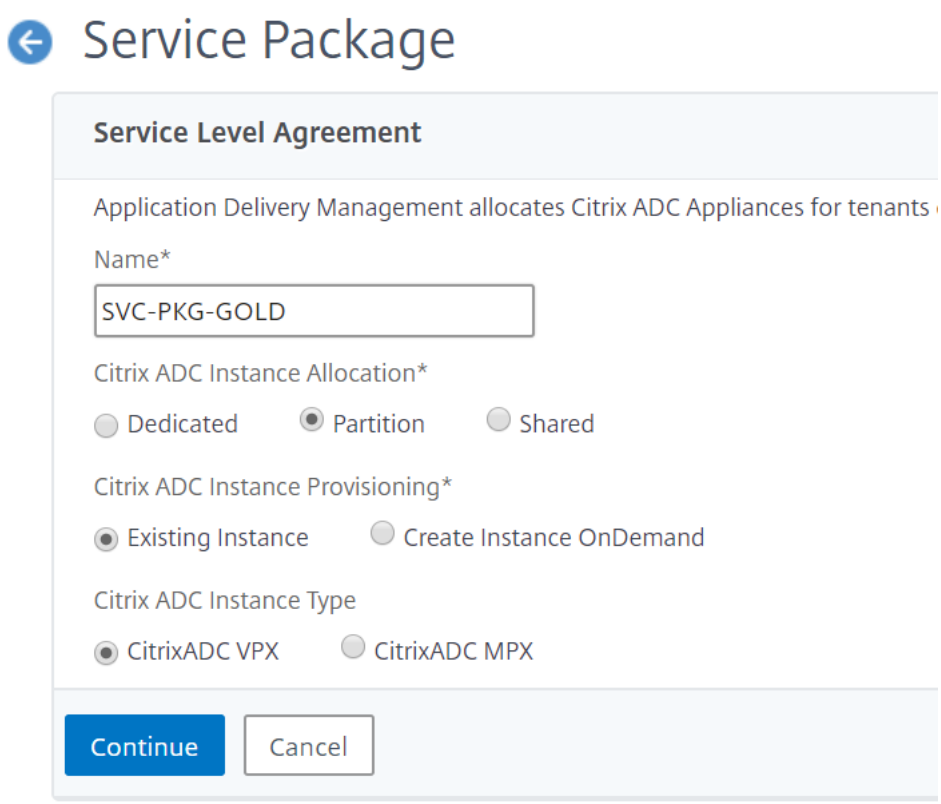
专用隔离策略

与专用策略的 Citrix Application Delivery Management (ADM) 服务包关联的每个租户都会从属于此服务包的实例中分配一个 Citrix ADC 实例。此分配的 Citrix ADC 实例不与其他租户共享。



分区隔离策略

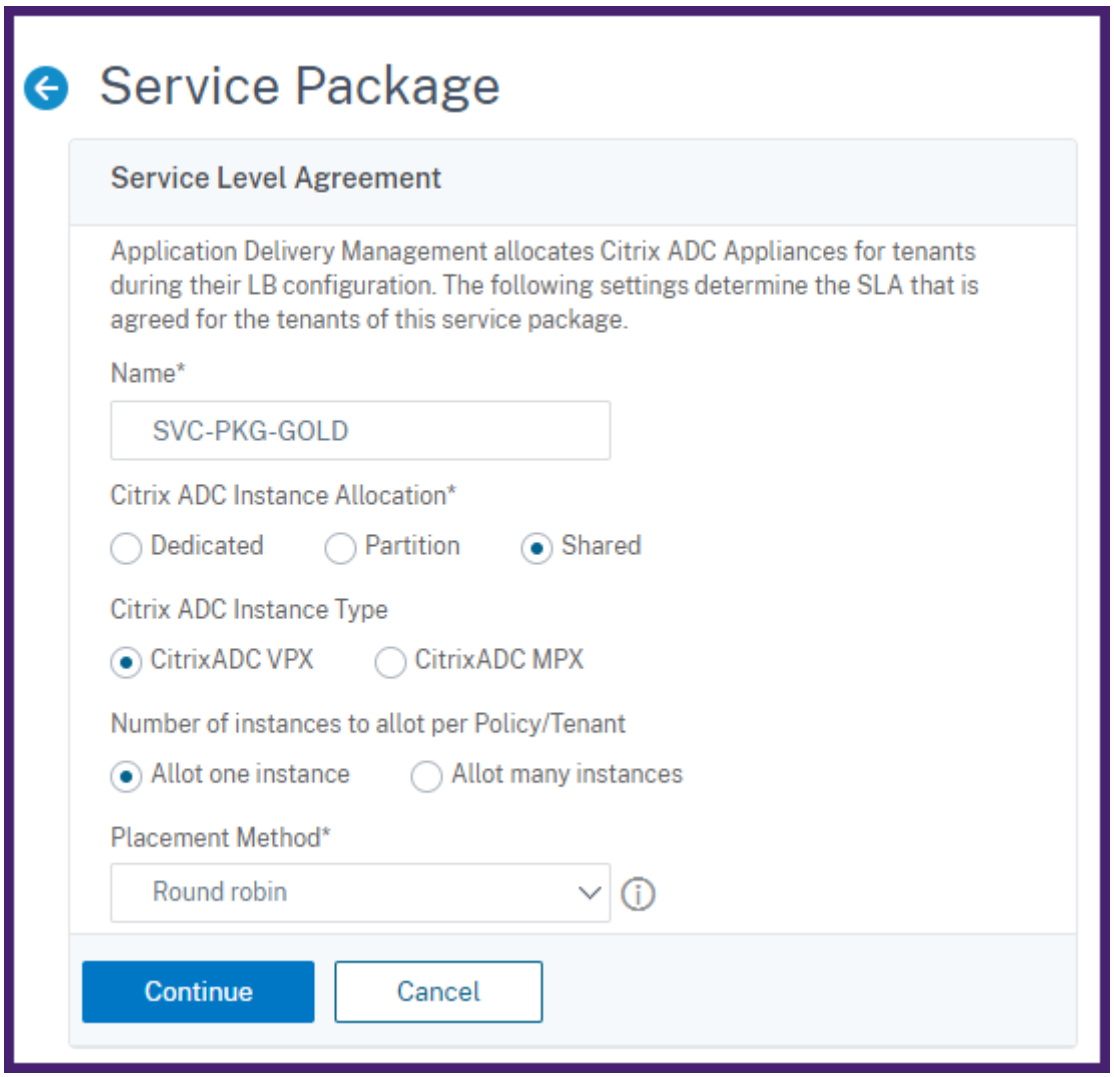
与分区策略的服务包关联的每个租户都会分配一个属于服务包的 Citrix ADC 实例的专用逻辑管理分区。



共享隔离策略

与服务包关联的租户共享作为服务包一部分的 Citrix ADC 实例。租户的所有配置都分配给一个 Citrix ADC 实例。在此模式下，多个租户的配置可以托管在同一 Citrix ADC 实例上。您可以选择 **Citrix ADC VPX** 或 **Citrix ADC MPX** 作为设备类型。您可以选择仅为服务包分配一个 Citrix ADC 实例或多个实例。也就是说，多个租户可以共享 Citrix ADC 设备的一个或多个虚拟实例。

> 注意：
>
> 将服务包中的 Citrix ADC SDX 实例仅作为 Citrix ADC VPX 实例添加为 Citrix ADC SDX 实例，因为思杰 ADC SDX 具有预配置的 Citrix ADC VPX。



> 注意
>
> 您还可以创建灵活的放置策略，其中策略不仅基于租户名称或 ID，还基于其他自定义属性。有关灵活放置策略的详细信息，请参阅基于策略的灵活设备分配。

灵活的基于策略的设备分配

April 23, 2021

Citrix Application Delivery Management (ADM) 会根据与租户商定的 SLA 将 Citrix ADC 虚拟实例分配给租户。为租户分配虚拟实例会在实例和租户之间建立一对一的关系，此时只能为租户分配数据中心里的一个服务包。

有些情况下，租户可能需要多个实例，或者实例分配可能不是基于作为条件的租户，而是基于其他因素，例如，网络 ID 或应用程序。在这种情况下，Citrix ADM 允许您根据用户定义的表达式精确定义放置策略，以便将负载均衡器配置分配给其中一个托管实例。

放置策略可以灵活地决定用户创建的每个负载均衡器配置中使用的 Citrix ADC 实例。Citrix ADM 中的灵活放置策略为基于租户分配 Citrix ADC 实例的现有方法提供了一个附加选项。

> 注意
>
> 您可以手动为租户分配实例，也可以基于创建的表达式使用放置策略来分配实例。不能对单个服务包同步使用这两个方法。

放置策略是基于对主要 LBaaS 配置对象（例如池和负载平衡器）的属性定义布尔表达式。Citrix ADM 中的放置策略用户界面提供了预定义的表达式，您可以从中进行选择，以定义自定义策略。可以针对不同的表达式创建多个放置策略。因此，每个租户可以有多个按租户要求定义的设备。

必须先选择表达式以匹配以后必须配置的根对象。对于 LBaaS V1，根对象可以是池对象；对于 LBaaS V2，根对象可以是负载平衡器对象。因此，LBaaas V1 和 V2 API 都支持基于 Citrix ADM 策略的放置。之后这些放置策略与服务包关联。根对象放置在实例中后，模型中连续的对象都会添加在该实例中。

例如，池配置对象可以有以下属性：

- tenant_id
- 名称
- description
- protocol
- lb_method
- subnet_id
- subname_name
- admin_state_up
- status
- network_id
- network_type
- segmentation_id
- subnet_cidr
- subnet_gateway_ip

下面的示例中显示了一些使用池属性为策略定义表达式的表达式：

1. 基于池名称的策略表达式

```
config["pools"]["name"] =="high-end-pool"
<!--NeedCopy-->
```

2. 基于池子网名称的策略表达式


```
config ["pools"]["subnet_name"] == "us-west-payment-subnet1"
<!--NeedCopy-->
```

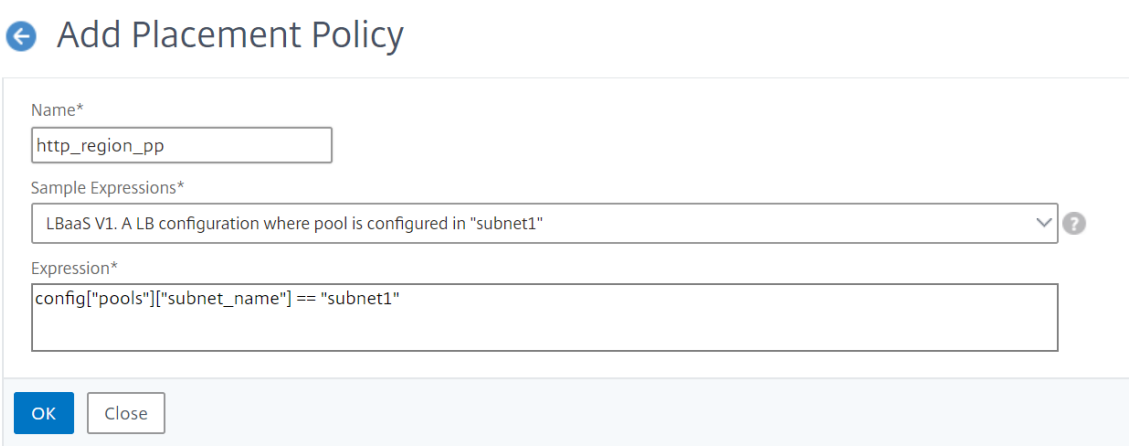
3. 基于负载均衡器子网名称的策略表达式

```
config["loadbalancers"]["subnet_name"] == "mas-subnet"
<!--NeedCopy-->
```

添加放置策略

1. 在 Citrix ADM 主页中，导航到 “ 编排**” > “**云编排” > “放置策略”，然后单击 “添加”。
2. 在 **Add Placement Policy**（添加放置策略）页面上，设置以下参数：
   a) Name（名称）- 键入放置策略的名称
   b) Frequently Used Expressions（常用表达式）- 从下拉列表中选择表达式。
   c) Expression（表达式）- 根据在前面的字段中选择的表达式，在此字段中填充一个逻辑（布尔）表达式。根据需要编辑字段名称。

> 注意：创建多个策略
>
> 时，请确保这些策略彼此独占。



3. 单击确定。
4. 导航到 编排 > 云编排 > **OpenStack** > 服务包，然后单击 添加。
5. 在 “ 服务包” 页上，设置以下参数：
   a) 名称-键入服务包的名称
   b) 隔离策略-选择 共享策略

      在共享隔离策略中，租户的负载平衡器配置与分配给该租户的设备中其他租户的负载平衡器配置共存。

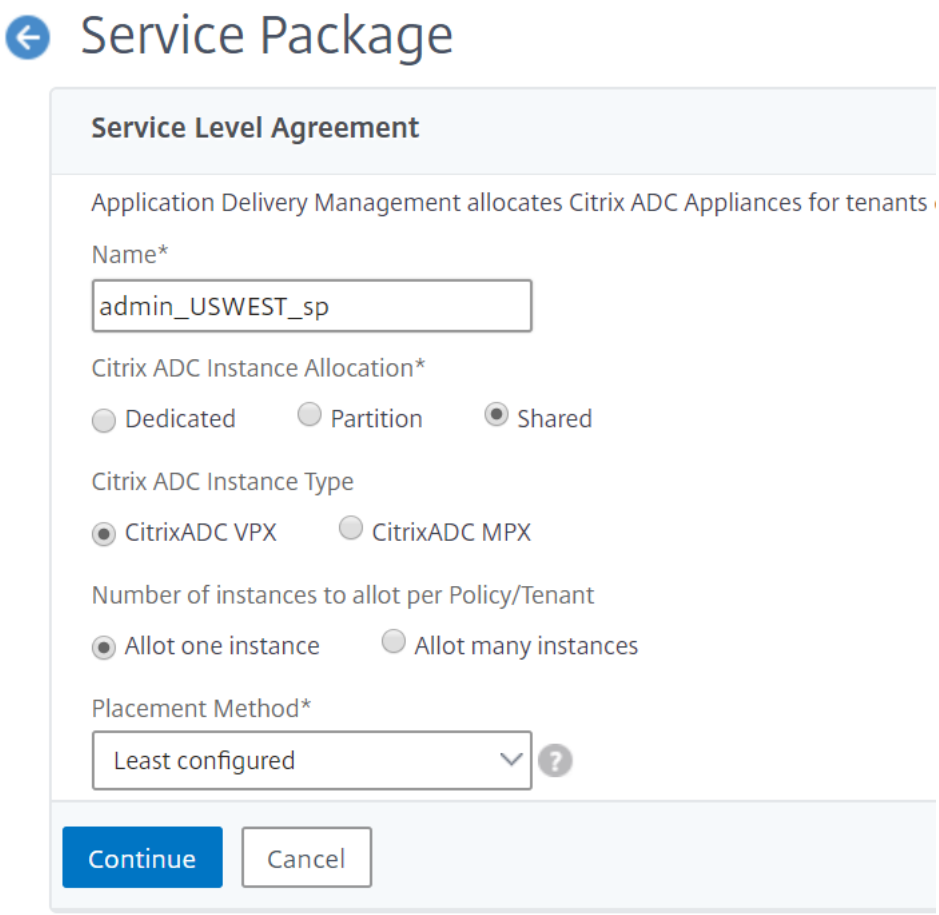
c) 设备类型-选择预置备的 **Citrix ADC VPX** 或 **Citrix ADC MPX**

如果希望租户的所有负载平衡器配置绑定到一个设备，请选择 **Allot one device**（分配一个设备）。如果希望租户的每个负载平衡器配置根据放置策略分发在数个设备上，请选择 **Allot many devices**（分配多个设备）。

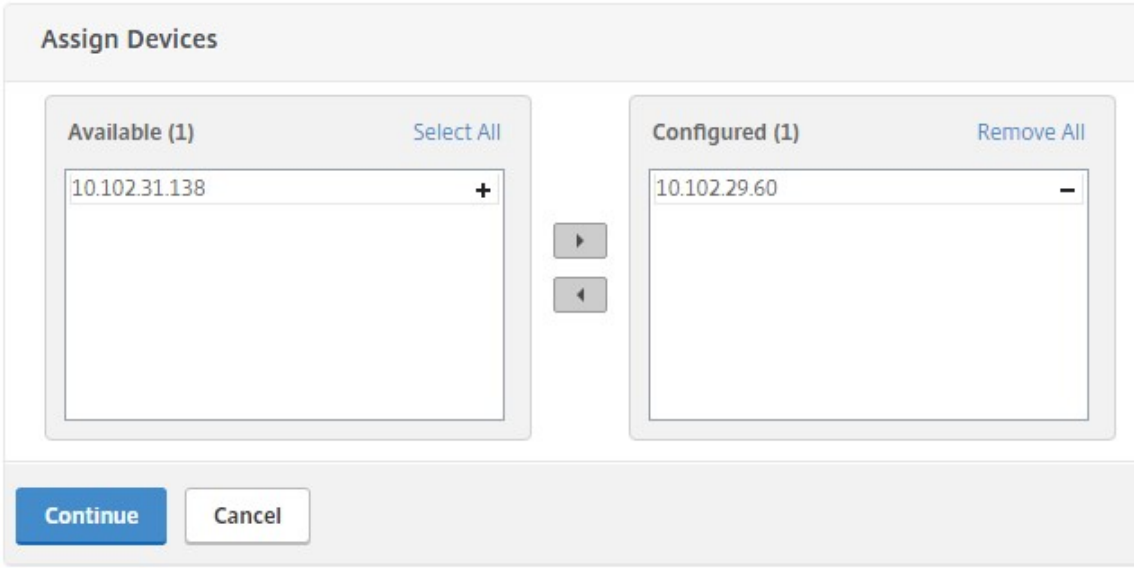
> 注意：必须将
>
> Citrix ADC SDX 作为仅在服务包中添加为 Citrix ADC VPX 实例，因为 Citrix ADC SDX 在其上配置了 Citrix ADC VPX。

d) 放置方法-选择 最不配置

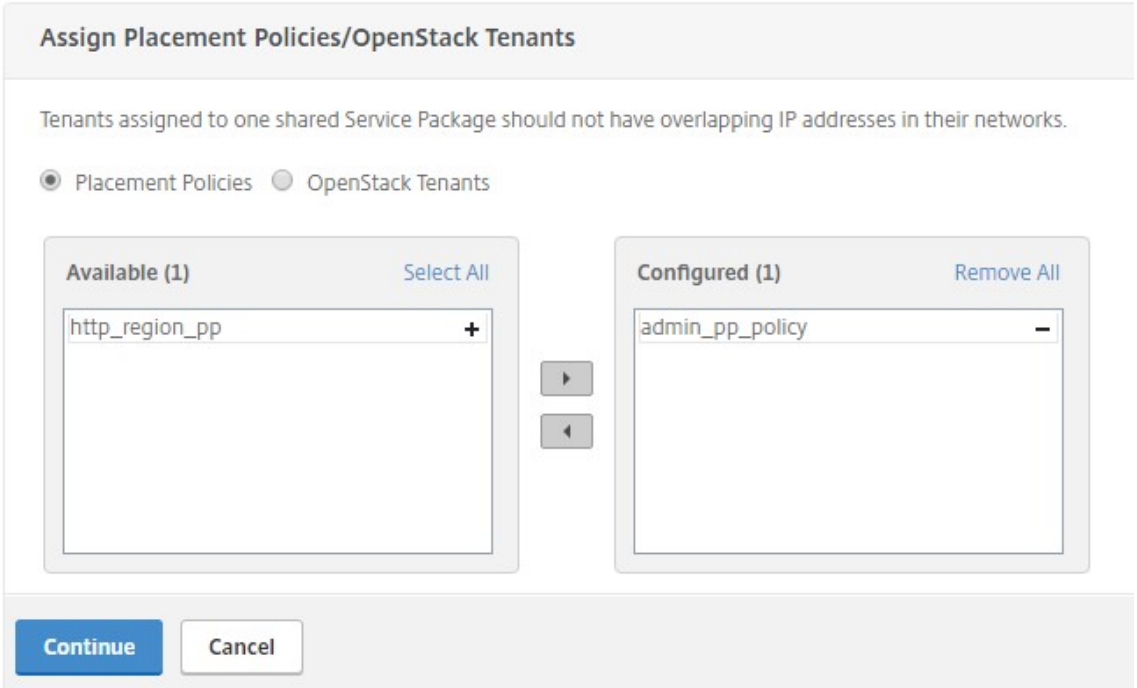
选择“最少配置”时，将选择在该时间点配置的池成员数量最少的 Citrix ADC 实例作为租户的设备。



6. 单击继续。
7. 在“分配设备”部分，将可用的 Citrix ADC 设备添加到已配置的设备列表中。



8. 单击继续。
9. 在 分配置放置策略/**OpenStack** 租户部分中，添加您之前创建的放置策略。



> 注意：
>
> 如果未找到策略，则会恢复回退机制，并且 Citrix ADM 会根据租户分配 Citrix ADC 实例。如果租户不是任何服务包的一部分，Citrix ADM 将显示一条错误消息，提示
>
> “租户不 `admin` 是任何服务包的一部分，也没有默认的服务包”。

10. 单击 **Continue**（继续），然后单击 **Done**（完成）。

NSX 管理器：手动 Provisioning Citrix ADC 实例

April 23, 2021

Citrix Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动执行 Citrix ADC 服务的部署、配置和管理。此集成抽象出了与物理网络拓扑相关的传统复杂性，使 vSPhere/vCenter 管理员能够更快地以编程方式部署 Citrix ADC 服务。

本文提供了必须在 VMware NSX 管理器和 Citrix ADM 上执行的任务列表。

> 注意：
>
> 确保已安装并配置适用于 vSphere 6.2 及更高版本的 VMware NSX，并且已创建必须进行负载平衡的边缘网关、DLR 和虚拟机。

必备条件

- 在满足最低要求的硬件上安装 VMware ESXi 4.1 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 在满足最低系统要求的管理工作站上安装 VMware 开放式虚拟化格式工具（VMware ESXi 4.1 版需要）。
- 在任何支持的虚拟机管理程序上安装 Citrix ADM。

  有关在任何支持的虚拟机管理程序上安装 Citrix ADM 版本 13.0 的任务，请参阅 部署 Citrix ADM。

VMware ESXi 硬件要求

下表列出了 VMware ESXi 服务器上安装 Citrix ADM 虚拟设备所需的虚拟计算资源。

组件	要求
RAM	8 GB
虚拟 CPU	8
存储空间	500 GB
虚拟网络接口	1
吞吐量	1 Gbps

> 注意：

> 上面指定的内存和硬盘要求用于在 VMware ESXi 服务器上部署 Citrix ADM（考虑到主机上没有其他虚拟机）。对 VMware ESXi 服务器的硬件要求取决于在其中运行的虚拟机数。

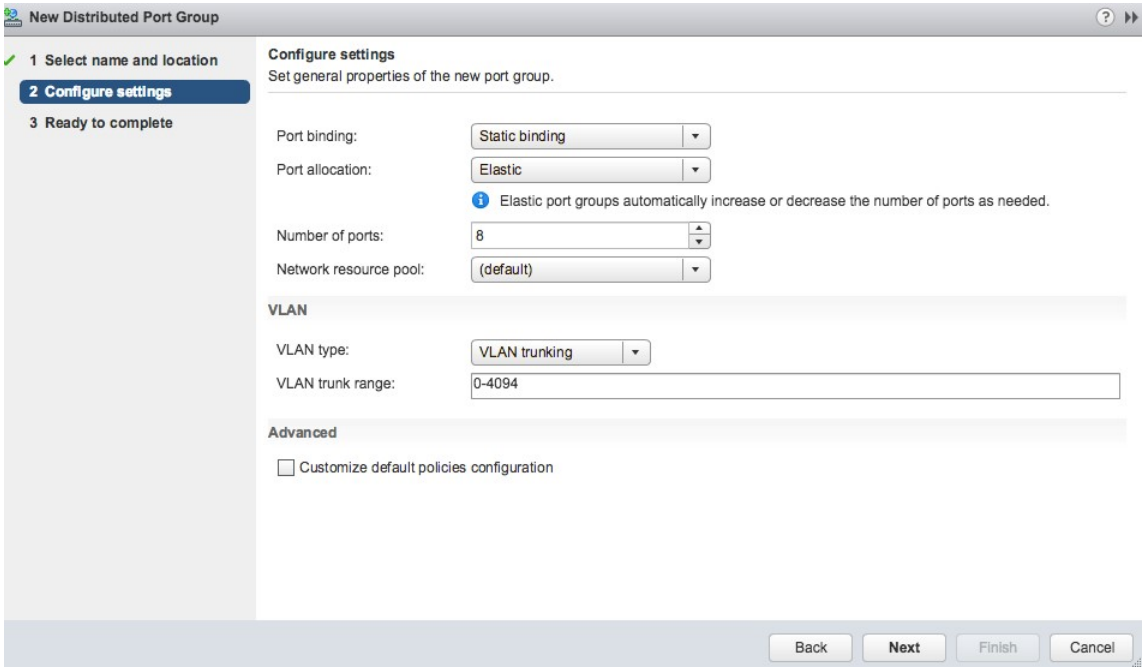
配置 **VMware NSX**

- 创建具有不同容量的 Citrix ADC VPX 实例池，这些实例将添加到不同服务包中。

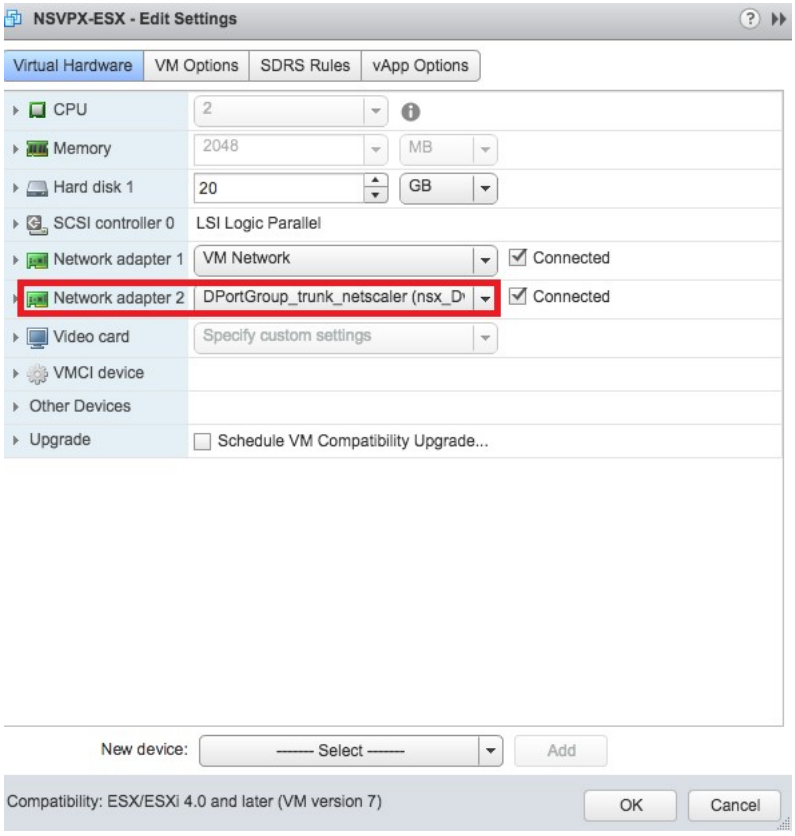
例如：

- 创建五个 VPX1000（1 Gbps）的 Citrix ADC VPX 实例。这些实例添加到金牌级服务包。
- 创建五个 VPX10（10 Mbps）的 Citrix ADC VPX 实例。这些实例添加到铜牌级服务包。

1. 在 vSphere Client 中，导航到 **Networking**（网络连接），创建类型为虚拟 LAN 的 Trunk 端口组，且设定范围（例如 101-105）（甚至可以提供全范围，但仅为所需的虚拟 LAN 创建类型为虚拟 LAN 的端口组）。

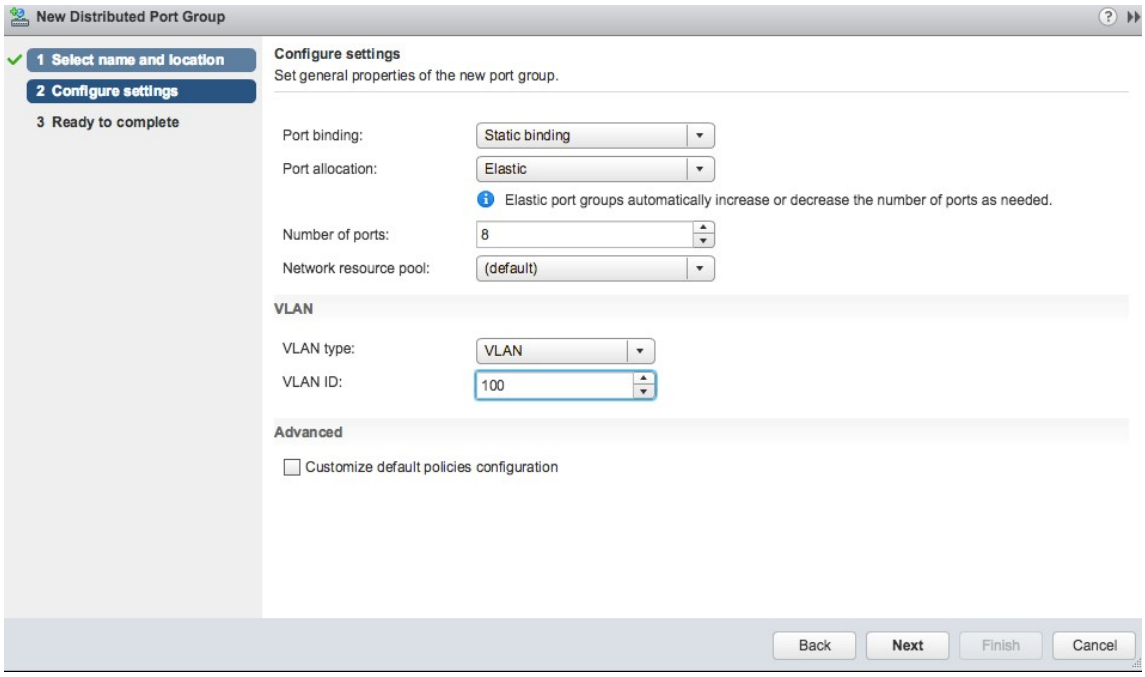


2. 为每个 Citrix ADC VPX 实例创建一个新接口，并将其连接到上面创建的 VLAN 范围中继端口组。



3. 在 vSphere Client 中，导航到 **Networking**（网络连接），创建类型为虚拟 LAN 的端口组。

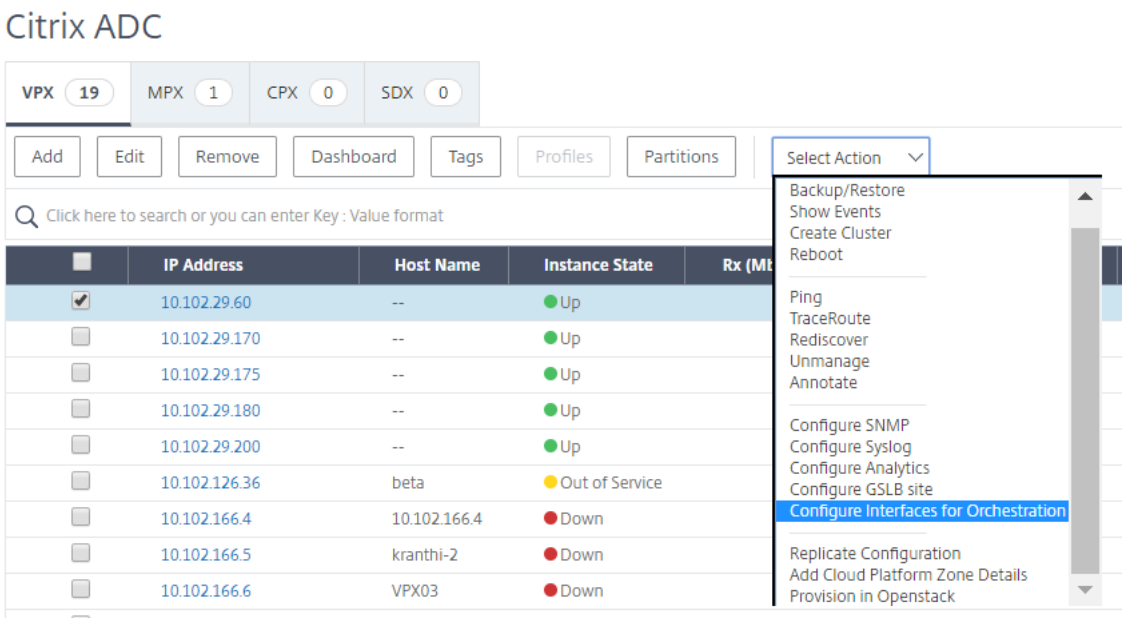
   例如，如果创建了范围是 101-105 的初始 Trunk 端口组，则创建五个虚拟 LAN 端口组（每个虚拟 LAN 一个端口组），即虚拟 LAN 101 一个端口组，虚拟 LAN 102 另一个端口组，依次类推，直至虚拟 LAN 105。



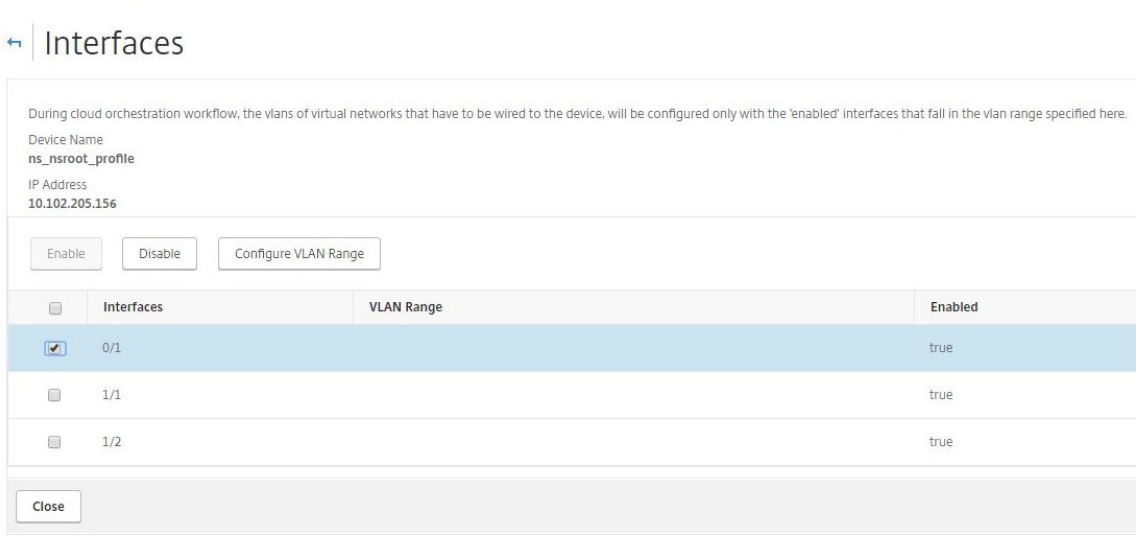
在 **Citrix ADM** 中添加 **Citrix ADC VPX** 实例

在 Citrix ADM 中添加 Citrix ADC VPX 实例，并为每个设备指定中继组的 VLAN 范围。

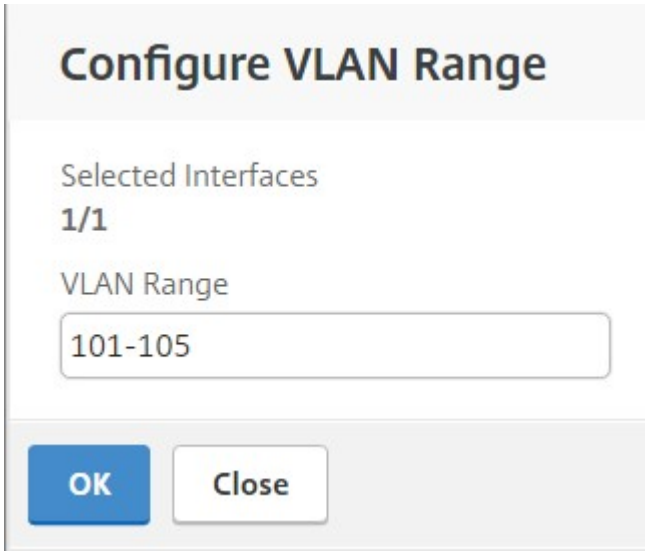
1. 在 Citrix ADM 中，导航到 “ 基础架构” > “ 实例” > “ **Citrix ADC VPX**”，然后单击 “ 添加”。
2. 在 “ 添加 **Citrix ADC VPX** ” 页上，指定实例的主机名、每个实例的 IP 地址或 IP 地址范围，然后从 “P**rofile** 名称” 列表中选择实例配置文件。还可以单击 + 图标创建新实例配置文件。
3. 单击 “ 确定”。
4. 从 Citrix ADC VPX 页面的列表中选择新添加的 **Citrix ADC VPX** 实例，然后单击 操作字段中的向下箭头按钮。选择 **Configure Interfaces for Orchestration**（为调配配置接口）。



5. 在 “ 接口” 页面上，选择管理接口，然后单击 “ 禁用” 以禁止 VLAN 绑定到管理接口。



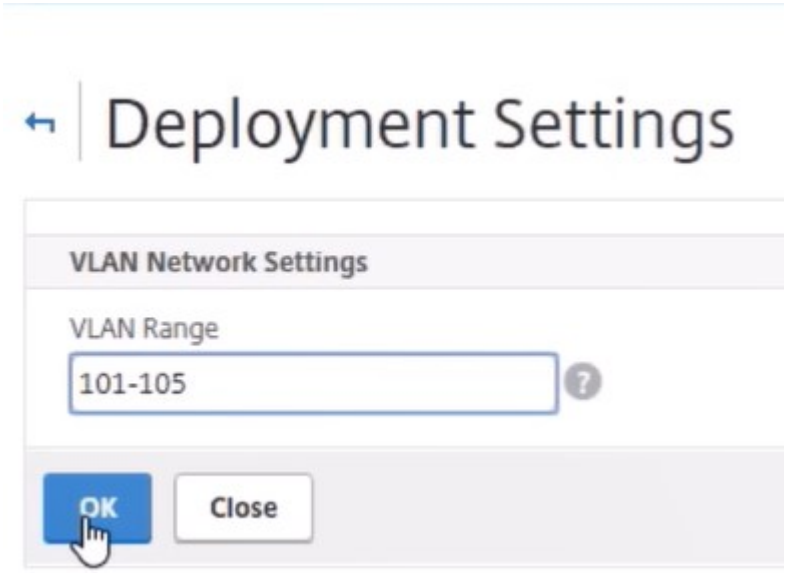
6. 在 “ 接口” 页面上，选择所需的接口，然后单击 “ 配置 **VLAN** 范围”。
7. 输入 NSX Manager 中配置的 VLAN 范围，单 击确定，然后单击 关闭。



在 **Citrix ADM** 中注册 **VMware NSX** 管理器

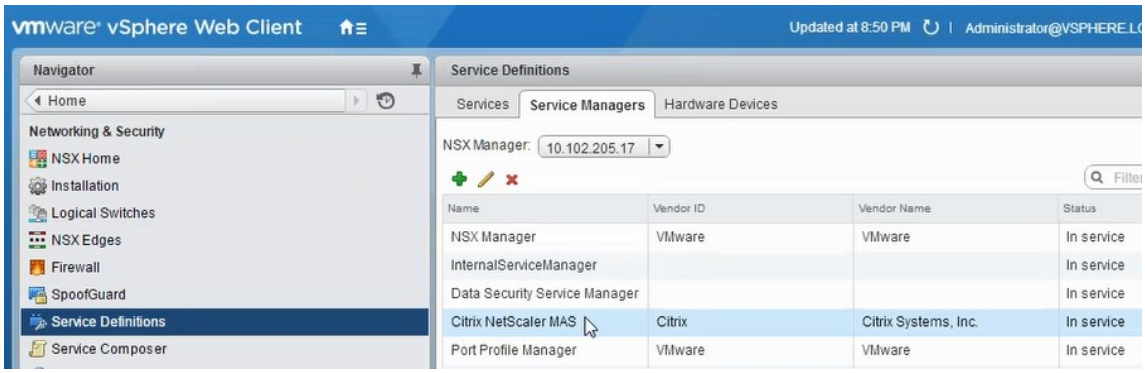
在 Citrix ADM 中注册 VMware NSX 管理器，以便在它们之间创建通信通道。

1. 在 **Citrix ADM** 中，从下拉列表中导航到 **“**编排” > “SDN 编排**” > “**VMware NSX 管理器**”**，然后单击 **“**配置 NSX 管理器设置**”**。
2. 在 “ 配置 **NSX** 管理器设置” 页上，设置以下参数：
   a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
   b) NSX 管理器用户名-NSX 管理器的管理用户名。
   c) Password（密码）- NSX Manager 的管理用户的密码。
3. 在 NSX Manager 使用的 **Citrix ADM** 帐户部分中，为 **NSX Manager** 设置 Citrix ADC 驱动程序用户名和密码。Citrix ADM 使用这些登录凭据对来自 NSX 管理器的负载均衡器配置请求进行身份验证。
4. 单击 “ 确定”。
5. 导航到 “ 编排” > “ 系统” > “ 部署设置”。提供在 Trunk 端口组中配置的虚拟 LAN 范围。



6. 登录到 vSphere Web 客户端上的 NSX 管理器，然后导航到 “ 服务定义” > “ 服务管理器”。

   您可以将 Citrix Citrix ADM 作为服务管理器之一进行查看。这表示注册成功，并在 NSX 管理器和 Citrix ADM 之间建立了通信通道。

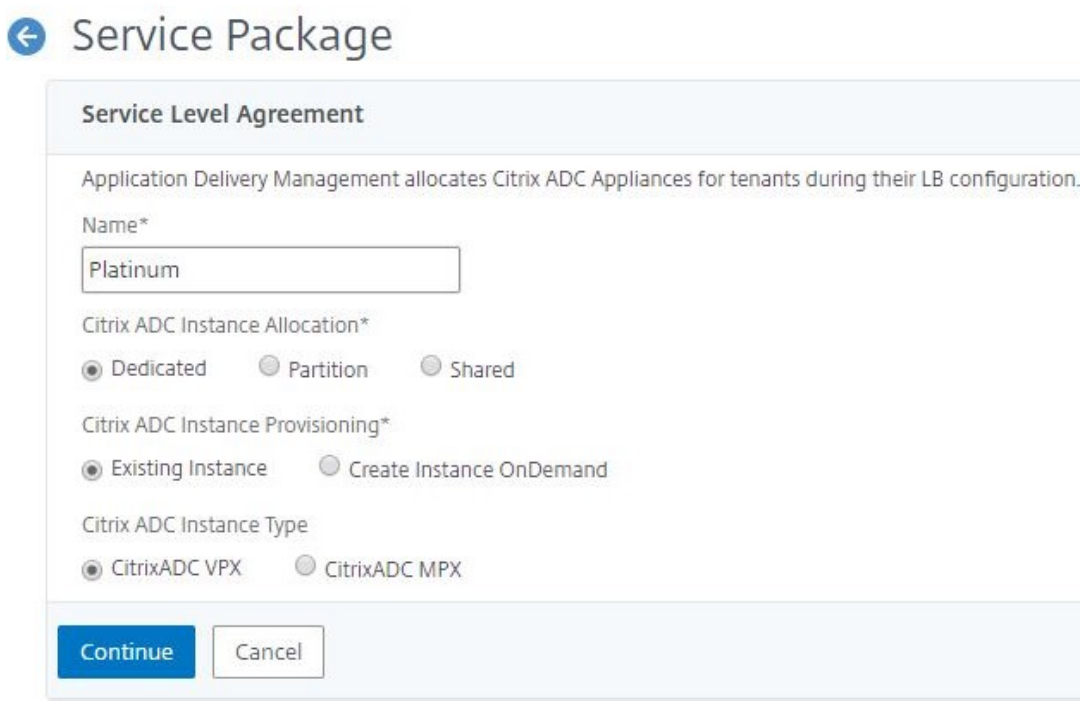


在 **Citrix ADM** 中创建服务包

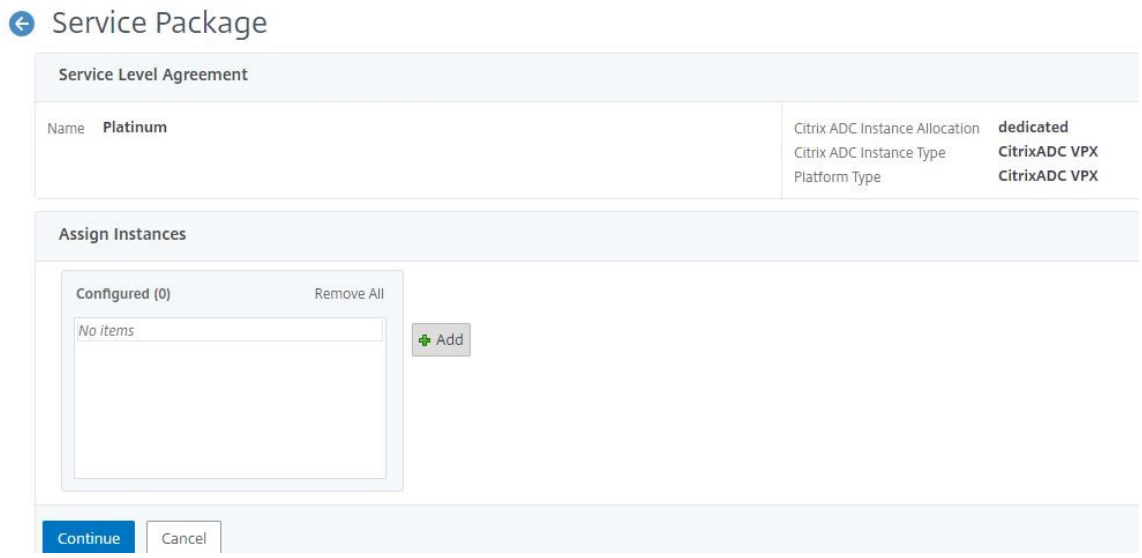
1. 在 Citrix ADM 中，导航到 “编排” > “**SDN** 编排” > “**VMware NSX** 管理器” > “ 服务包”，然后单击 “ 添加” 以添加新的服务包。
2. 在 “ 服务包” 页上的 “ 基本设置” 部分，设置以下参数：
   a) Name（名称）- 键入服务包的名称
   b) Isolation Policy（隔离策略）- 默认情况下，隔离策略设置为 “Dedicated”（专用）
   c) 设备类型 — 默认情况下，设备类型设置为 Citrix ADC VPX

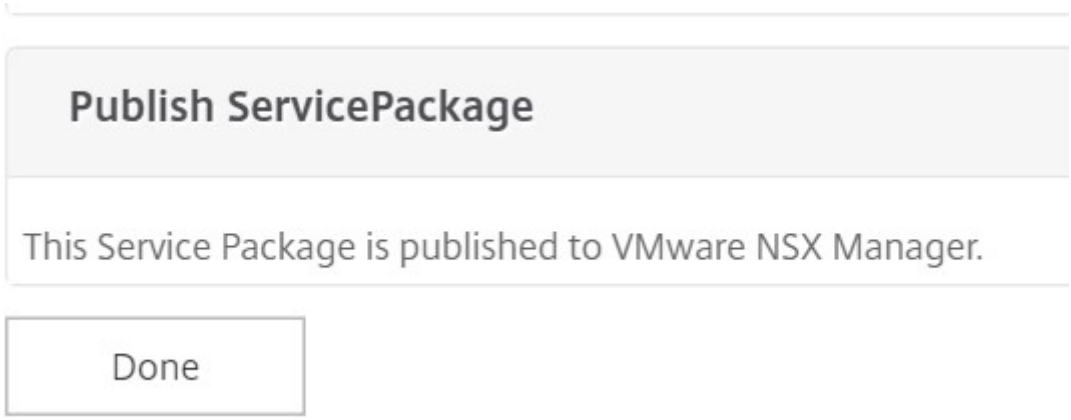
   > 注意
   >
   > 这些值在此版本中默认设置，您无法修改它们。

d) 单击继续。



3. 在“ 分配设备” 部分，选择此程序包的预置 VPX，然后单击“ 继续”。
4. 在“ 发布服务包” 部分中，单击“ 继续” 以将服务包发布到 VMware NSX，然后单击“ 完成”。





此过程在 NSX Manager 中配置服务包。服务可以添加多个设备，并且多个边缘可以使用相同的服务包将 Citrix ADC VPX 实例卸载到 Citrix ADM。

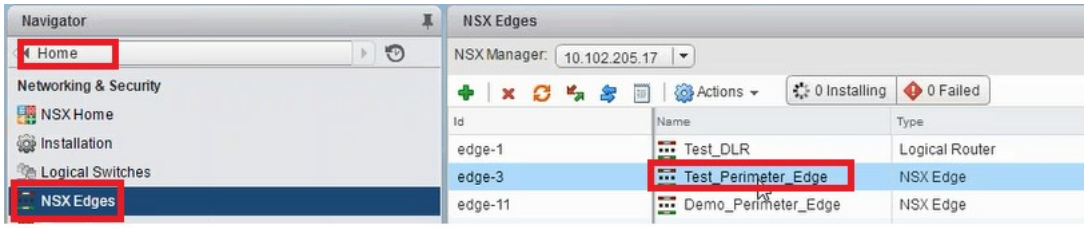
5. 登录到 vSphere Web 客户端上的 NSX 管理器，然后导航到 “ 服务定义” > “ 服务”。

   您可以看到 Citrix ADM 服务包已注册。

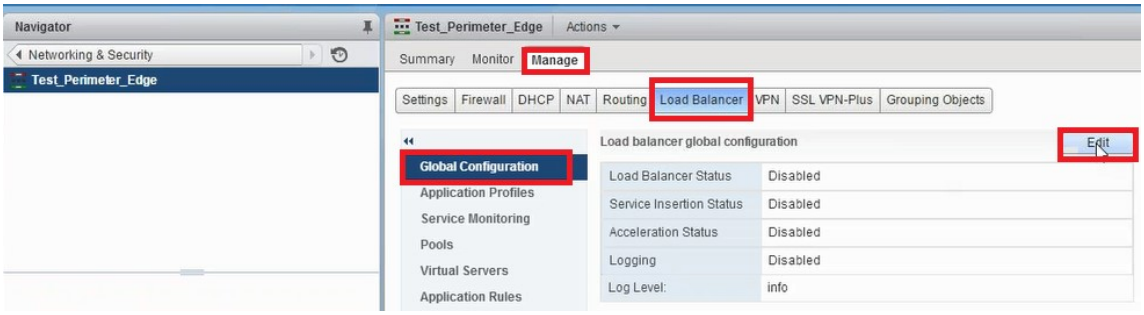
为边界执行负载平衡器服务插入

在先前创建的 NSX Edge Gateway 上执行负载平衡器服务插入（将负载平衡功能从 NSX LB 卸载到 Citrix ADC）。

1. 在 NSX Manager 中，导航到 “ 主页” > “ **NSX** 边缘”，然后选择已配置的边缘 Gateway。

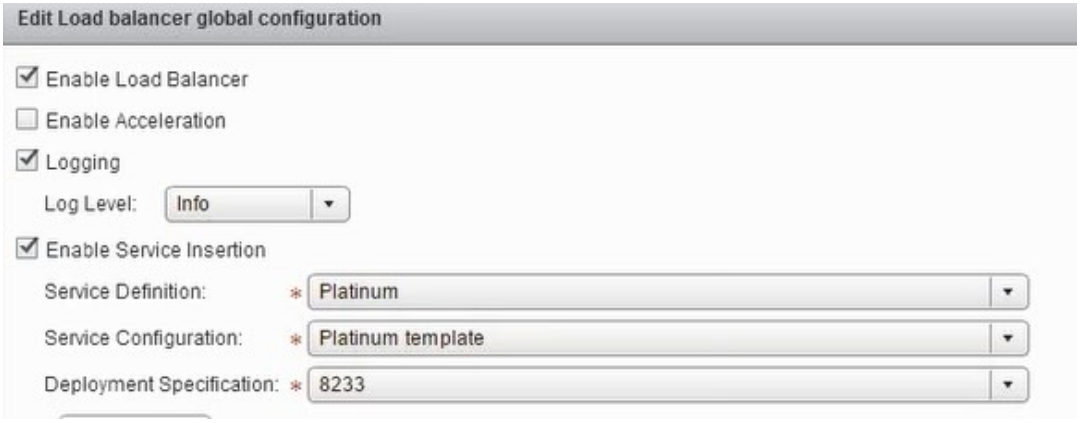


2. 单击 管理，然后在 负载均衡器选项卡上，选择 全局配置，然后单击 编辑。

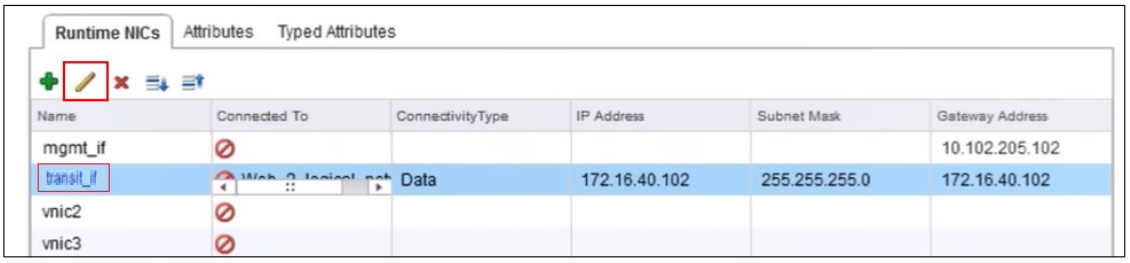


3. 选择 启用负载均衡器、日志记录、启用服务插入以启用它们。

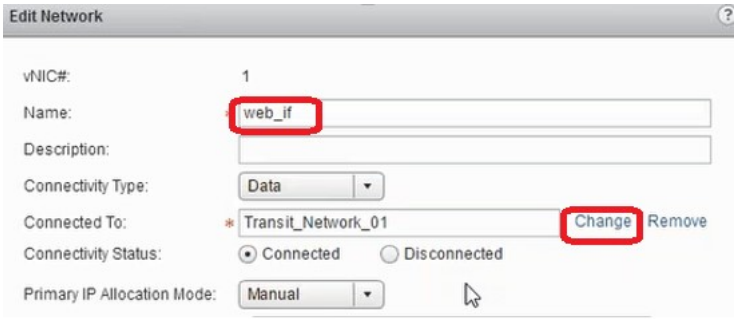
   a) 在 服务定义中，选择在 Citrix ADM 中创建并发布到 NSX 管理器的服务包。



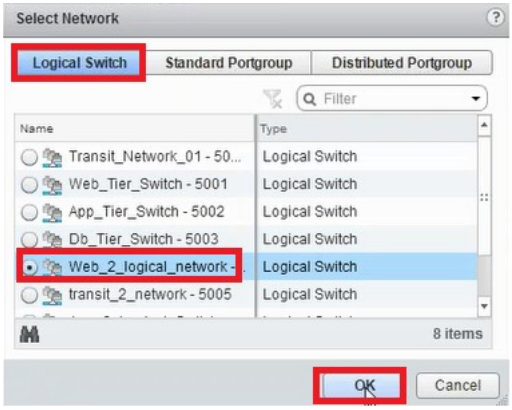
4. 选择现有的运行时网卡，然后单击“编辑”图标以编辑在分配 Citrix ADC VPX 时必须连接的运行时 NIC。



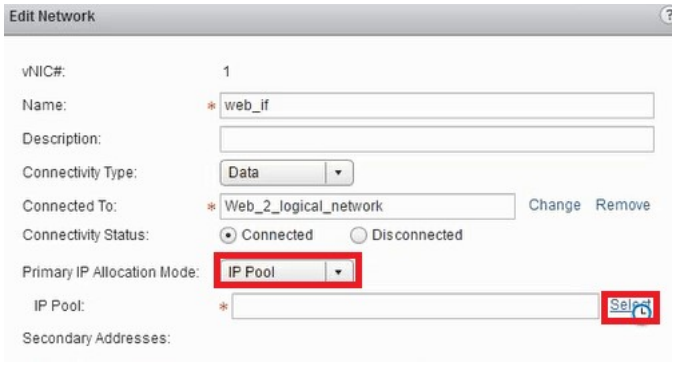
5. 编辑 NIC 的名称，将连接类型指定为 数据，然后单击 更改。



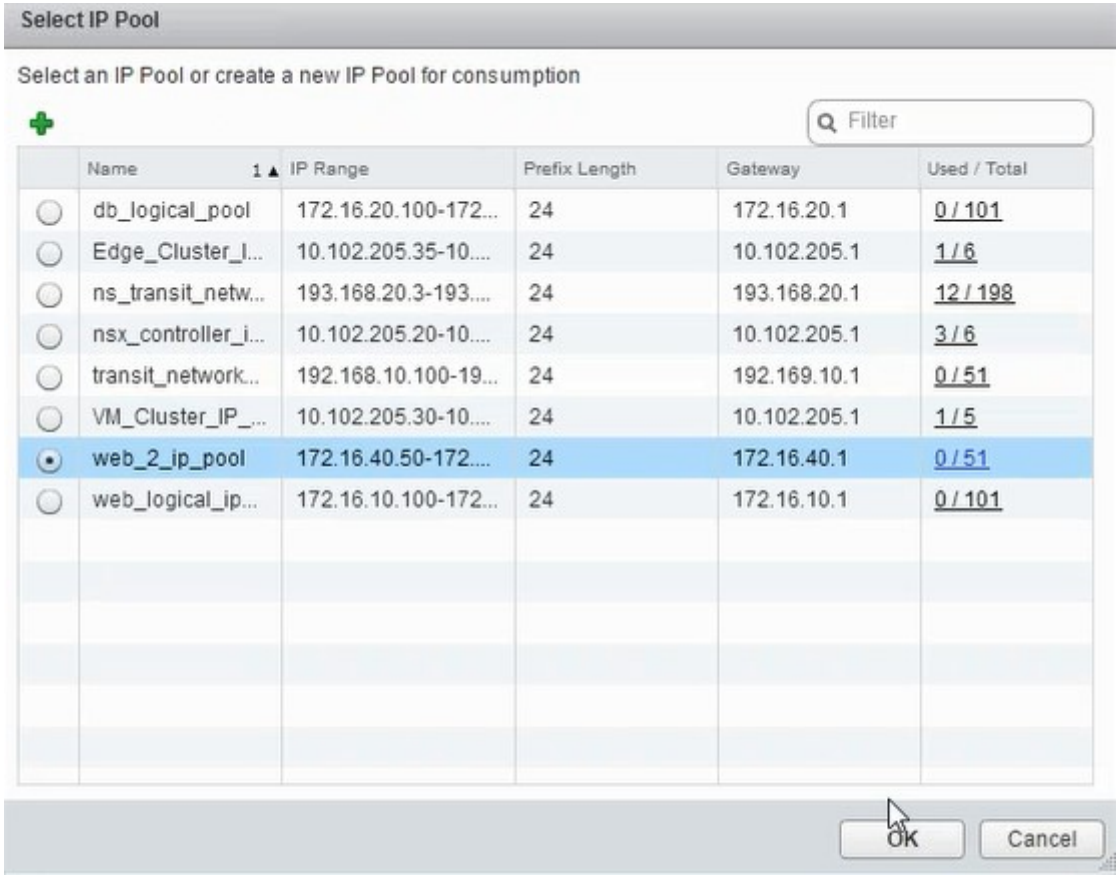
6. 选择适当的 Web 逻辑交换机。



7. 在 主 **IP** 分配模式下，从下拉列表中选择 IP 池，然后单击 IP 池字段上的向下箭头按钮。



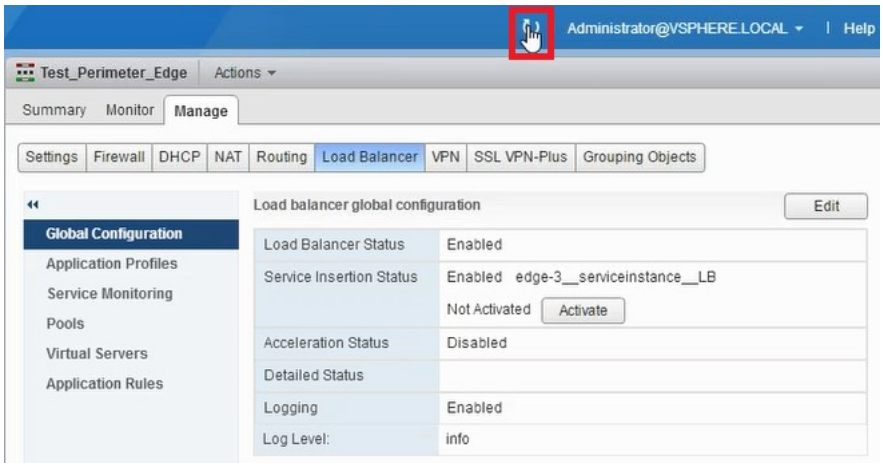
8. 在 “选 择 **IP** 池” 窗口中，选择相应的 IP 池，然后单击 “ 确定”。

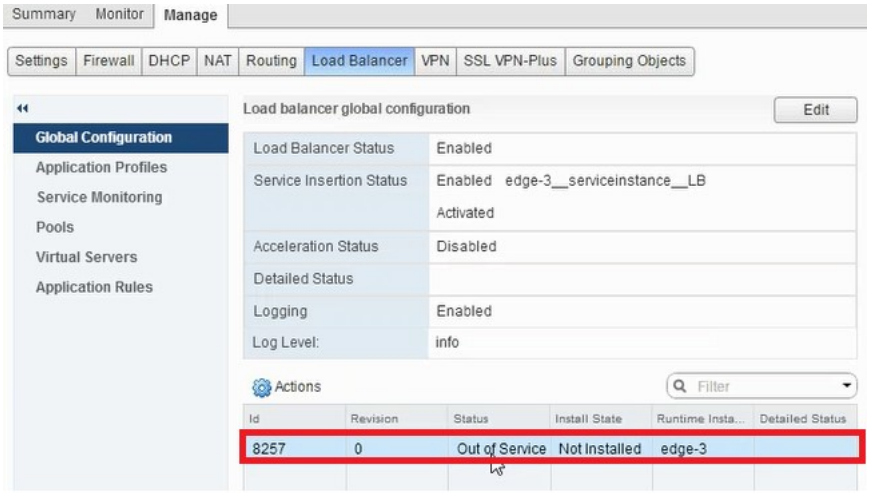


在 Citrix ADC VPX 装置中获取 IP 地址并将其设置为源净 IP 地址。在 NSX Manager 中创建一个 L2 网关以将 VXLAN 映射到虚拟 LAN。

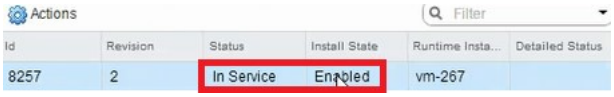
> 注意：
>
> 所有数据接口都作为运行时 NIC 连接，它们是 DLR 接口的一部分。

9. 刷新视图以查看运行时间的创建。





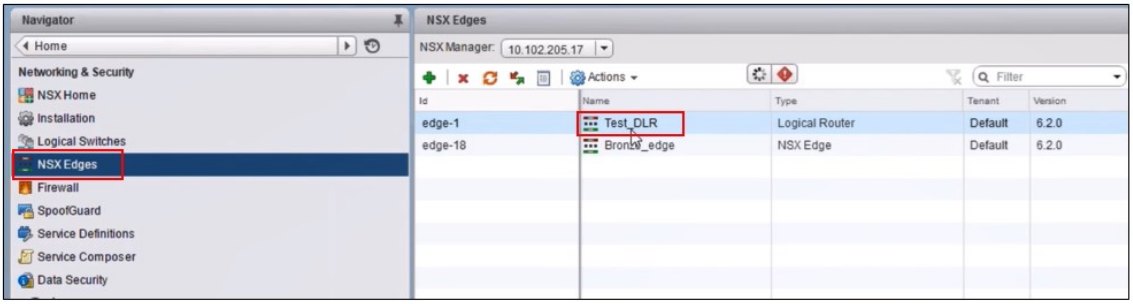
10. VM 启动后，“状态” 的值将更改为 “正 在服务”，“安装状态” 的值更改为 **“**已启用**”**。



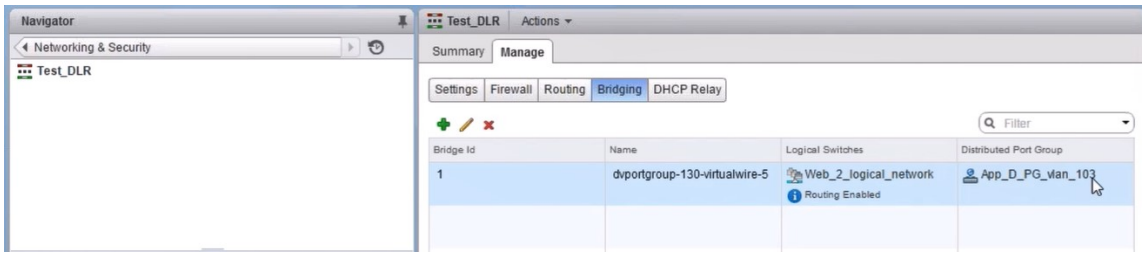
> 注意：
>
> 在 Citrix ADM 中，导航到 “业务 流程” > “ 请求” 以查看 LB 服务插入完成的进度详细信息。

在 **NSX Manager** 中查看 **L2** 网关

1. 登录到 vSphere Web 客户端上的 NSX 管理器，导航到 **NSX** 边缘，然后选择已创建的 DLR。



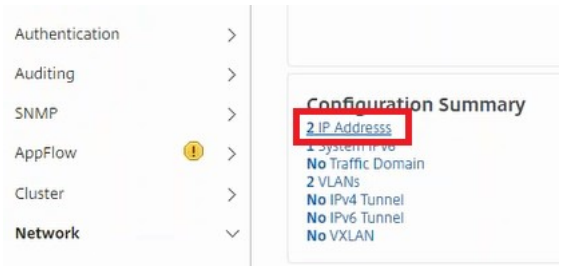
2. 在 DLR 页面中，导航到 “ 管理” > “ 桥接”。可以看到列表中显示的 L2 网关。



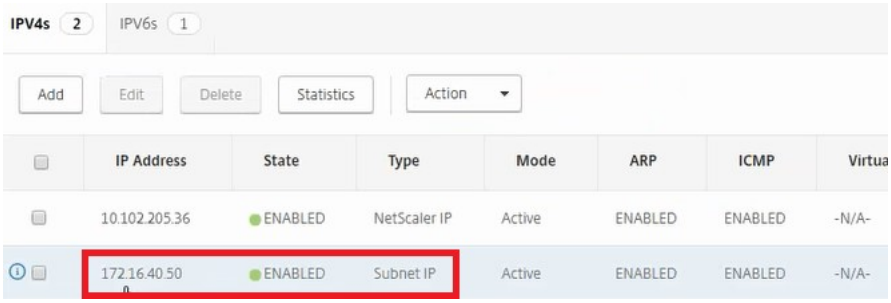
> 注意为每个数据接口创建
>
> 一个 L2 Gateway。

查看分配的 **Citrix ADC**

1. 使用 Citrix ADM 中显示的 IP 地址登录到 Citrix ADC VPX 实例。然后，导航到 “ 配置” > “ 系统” > “ 网络”。在右侧窗格中，可以看到添加了两个 IP 地址。单击 IP 地址超链接可以查看详细信息。



子网 IP 地址与 NSX 中添加的 Web Interface 的 IP 地址相同。



2. 导航到 “ 配置” > “ 系统” > “ 许可证” 以查看应用于此实例的许可证。

使用样书配置 **Citrix ADC VPX** 实例

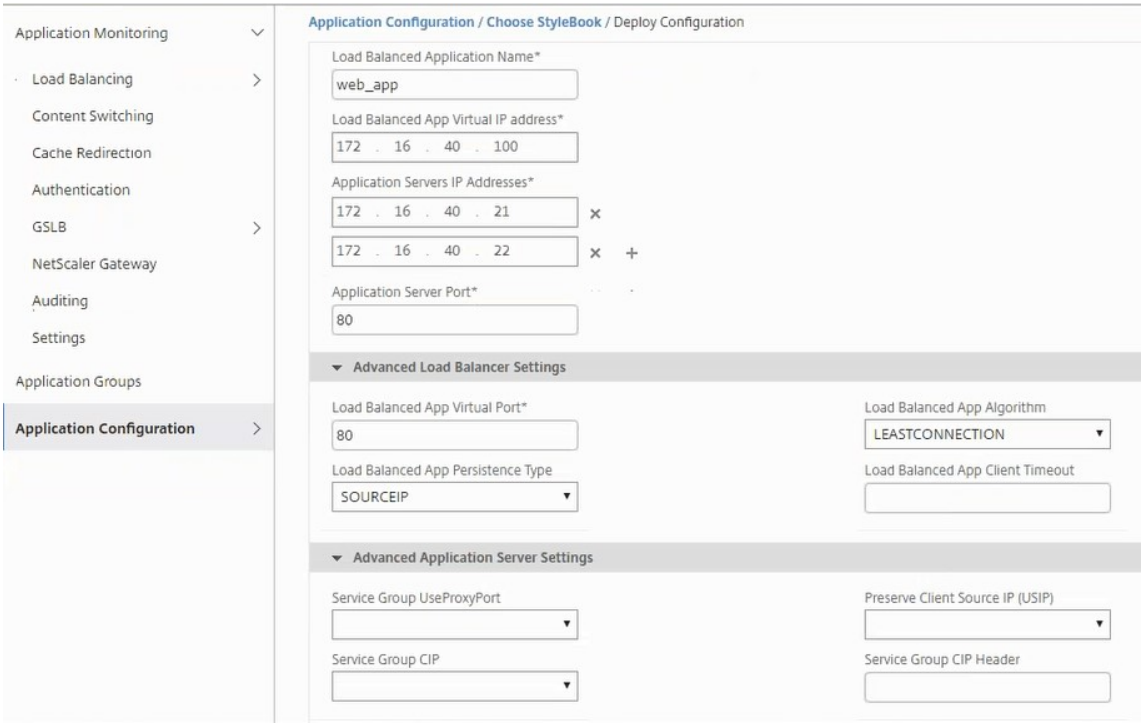
1. 在 Citrix ADM 中，导航到 “编排” > “**SDN** 编排” > “配置 **NSX** 管理器” > “ 边缘网关”。

   记下分配给必须通过样书应用负载平衡配置的相应 Edge 网关的 Citrix ADC 实例 IP。

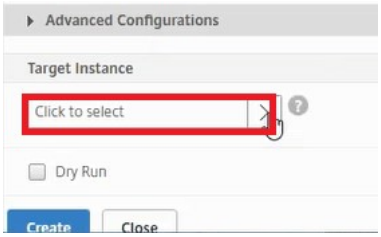
2. 创建一本新的样书。导航到 应用程序 > 配置，导入样书，然后从列表中选择样书。

   要创建新的样书，请参阅 创建自己的样书。

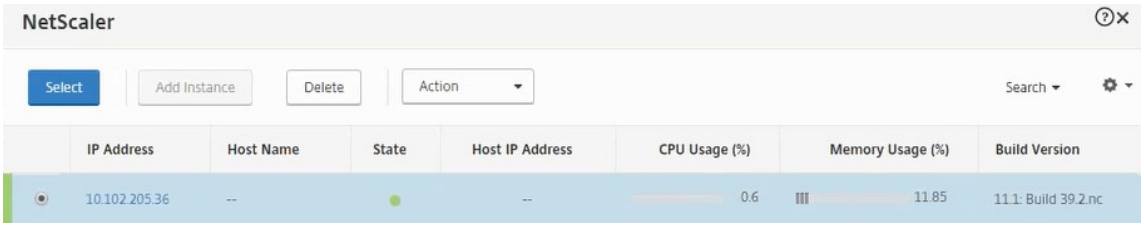
3. 为所有所需参数指定值。



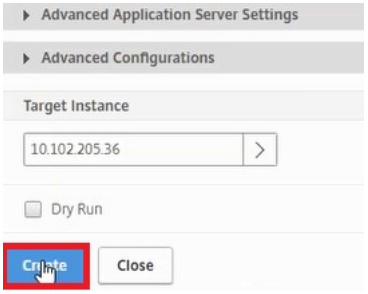
4. 指定要在其上运行这些配置设置的 Citrix ADC VPX 实例。



5. 选择前面说明的 IP 实例，然后单击 “ 选择”。

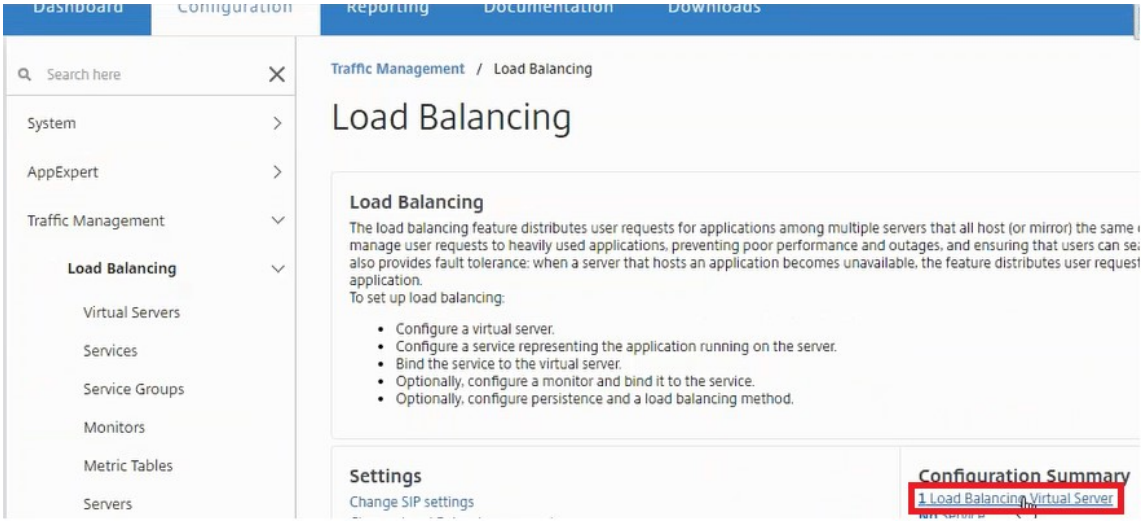


6. 单击 创建可在选定的设备上应用配置。

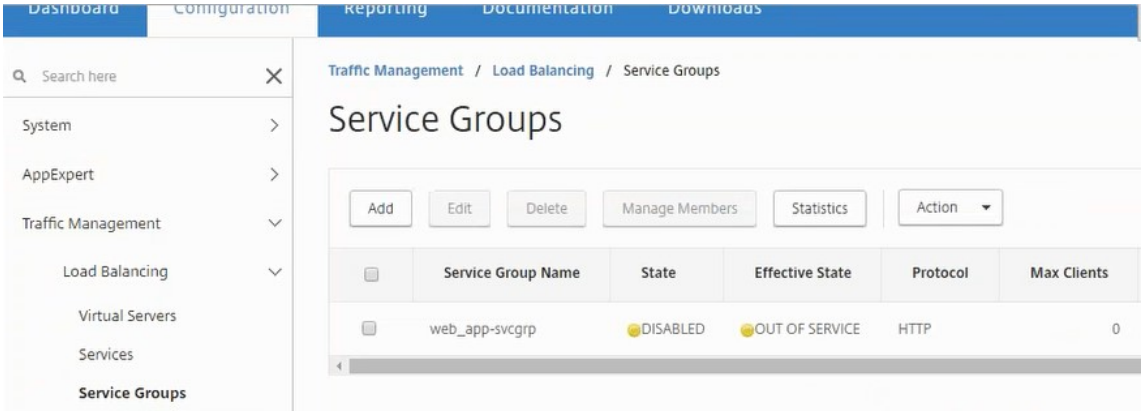


查看负载平衡器配置

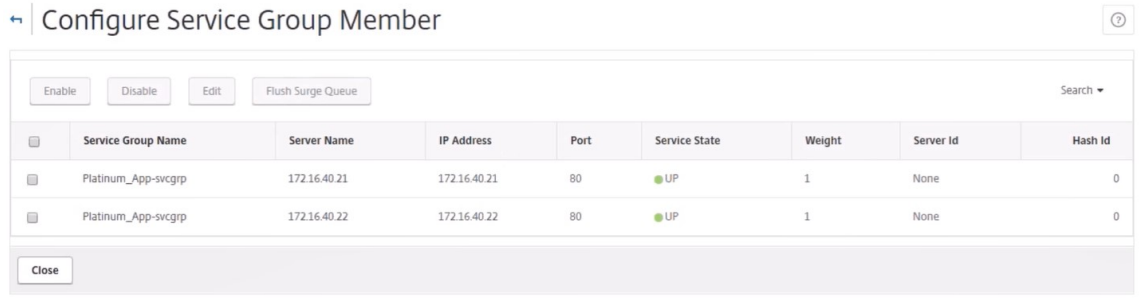
1. 登录到 Citrix ADC VPX 实例，导航到 “ 配置” > “ 流量管理” > “ 负载平衡” 以查看创建的负载平衡虚拟服务器。



还可以查看创建的服务组。



2. 选择服务组，然后单击 管理成员。**Configure Service Group Member**（配置服务组成员）页面显示与服务组关联的成员。

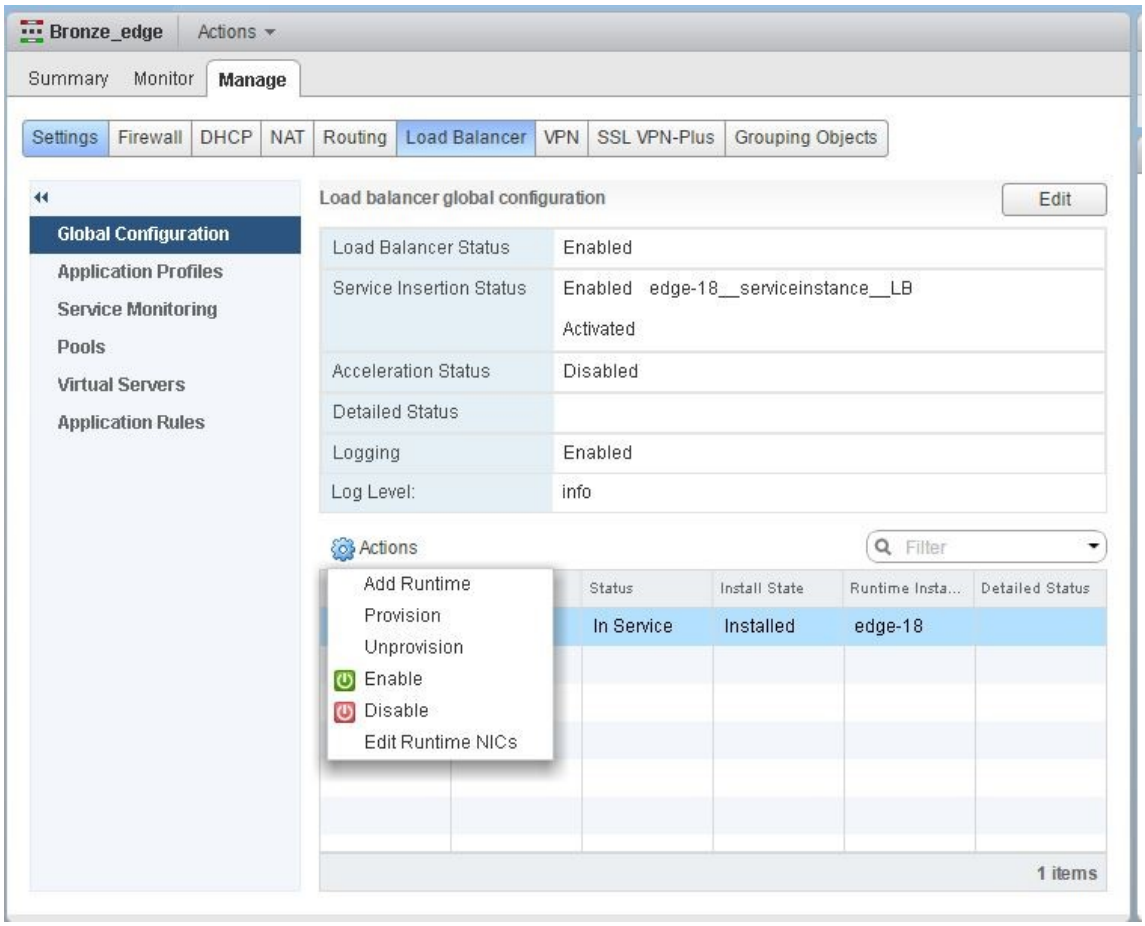


删除负载平衡器服务

1. 在 Citrix ADM 中，导航到 “应用程 序” > “ 配置”，然后单击 “ **X** ” 图标以删除应用程序配置。

2. 登录到 vSphere Web 客户端上的 NSX 管理器，然后导航到 Citrix ADC VPX 实例所连接的边缘 Gateway。
3. 导航到 “ 管理” > “ 负载均衡器” > “ 全局配置”，右键单击运行时条目，然后单击 “ 取消置备”。

   > 注意：
   >
   > Citrix ADM 中的 Edge 网关对应于 NSX Manager 中的运行时条目。



   Citrix ADC VPX 实例已停止服务。

4. 在 Citrix ADM 中，导航到 “编排” > “**SDN** 编排” > “配置 **NSX** 管理器” > “ 边缘网关”。确认 Edge 网关与所删除实例的各个映射是否不存在。

NSX 管理器：自动 **Provisioning Citrix ADC** 实例

April 23, 2021

概述

Citrix Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动执行 Citrix ADC 服务的部署、配置和管理。此集成抽象出了与物理网络拓扑相关的传统复杂性，使 vSPhere/vCenter 管理员能够更快地以编程方式部署 Citrix ADC 服务。

在 VMware NSX 管理器上插入和删除负载平衡服务期间，Citrix ADM 会动态配置和销毁 Citrix ADC 实例。此动态 Provisioning 要求在 Citrix ADM 中自动分配 Citrix ADC VPX 许可证。将 Citrix ADC 许可证上载到 Citrix ADM 时，Citrix ADM 将执行许可证服务器的角色。

必备条件

> 注意
>
> 仅适用于 **vSphere 6.1** 或更早版本的 **VMware NSX** 支持此集成。

- Citrix ADM, 版本 13.0 设置在高可用性和安装在 ESX 上.
- Citrix ADC VPX，版本 13.0
- 适用于 Citrix ADC VPX 实例的 Citrix ADC VPX 许可证，版本 13.0
- 在满足最低要求的硬件上安装 VMware ESXi 4.1 版或更高版本。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 在满足最低系统要求的管理工作站上安装 VMware 开放式虚拟化格式工具（VMware ESXi 4.1 版需要）。

Citrix ADM 和 **Citrix ADC** 实例的高可用性部署

要置备 Citrix ADM HA 设置，请安装从 Citrix 下载站点下载的 Citrix ADM 映像文件。有关如何置备 Citrix ADM HA 设置的详细信息，请参阅 在高可用性中部署 Citrix ADM。

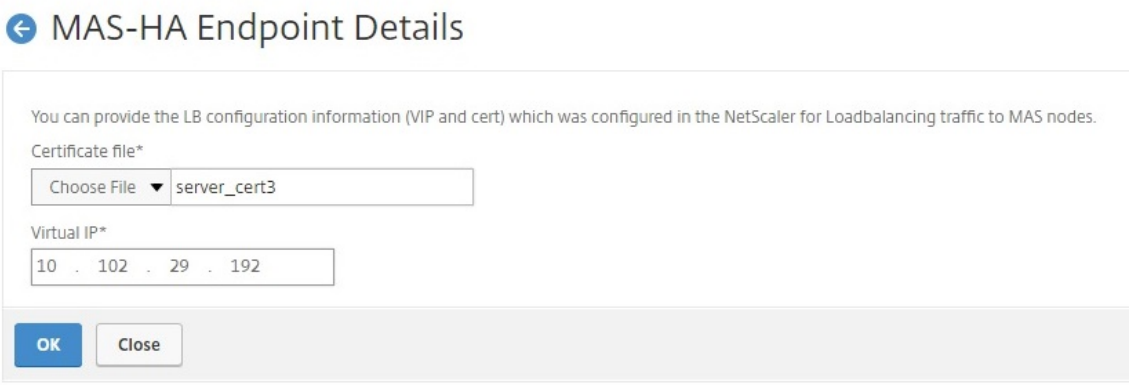
设置 **Citrix ADM HA** 端点详细信息

要将 VMware NSX 管理器与在 HA 模式下部署的 Citrix ADM 集成，必须首先输入负载平衡 Citrix ADC 实例的虚拟 IP 地址。您还必须将 Citrix ADC 负载平衡虚拟服务器上存在的证书文件上载到 Citrix ADM 文件系统。

要在 **Citrix ADM** 中提供负载平衡配置信息，请执行以下操作：

1. 在 Citrix ADM HA 节点中，导航到 “ 系统” > “ 部署”。
2. 单击右上角的 **HA** 设置，然后在 **MAS-HA** 设置页面中，单击 **MAS-HA** 端点详细信息。

3. 在 **MAS-HA** 端点详细信息页面上，上载负载平衡 Citrix ADC 实例上已存在的相同证书。
4. 输入负载平衡 Citrix ADC 实例的虚拟 IP 地址，然后单 击确定。



在 **Citrix ADM** 中注册 **VMware NSX** 管理器

在设置两个 Citrix ADM 服务器以高可用性时，这两个服务器节点处于主动-被动模式。登录到主 Citrix ADM 服务器节点，将 VMware NSX 管理器注册到 HA 中的 Citrix ADM，以便在它们之间创建通信通道。

要将 **VMware NSX** 管理器注册到 **HA** 中的 **Citrix ADM**，请执行以下操作：

1. 在主 Citrix ADM 服务器节点中，导航到 “ 编排” > “ **SDN** 编排” > “ **VMware NSX** 管理器”。
2. 单击 配置 **NSX** 管理器设置。
3. 在 “ 配置 **NSX** 管理器设置” 页上，设置以下参数：
    a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
    b) NSX 管理器用户名-NSX 管理器的管理用户名。
    c) Password（密码）- NSX Manager 的管理用户的密码。
4. 在 NSX 管理器使用的 Citrix ADM 帐户部分中，设置 NSX 管理器的 Citrix ADC 驱动程序密码。
5. 单击 “ 确定”。

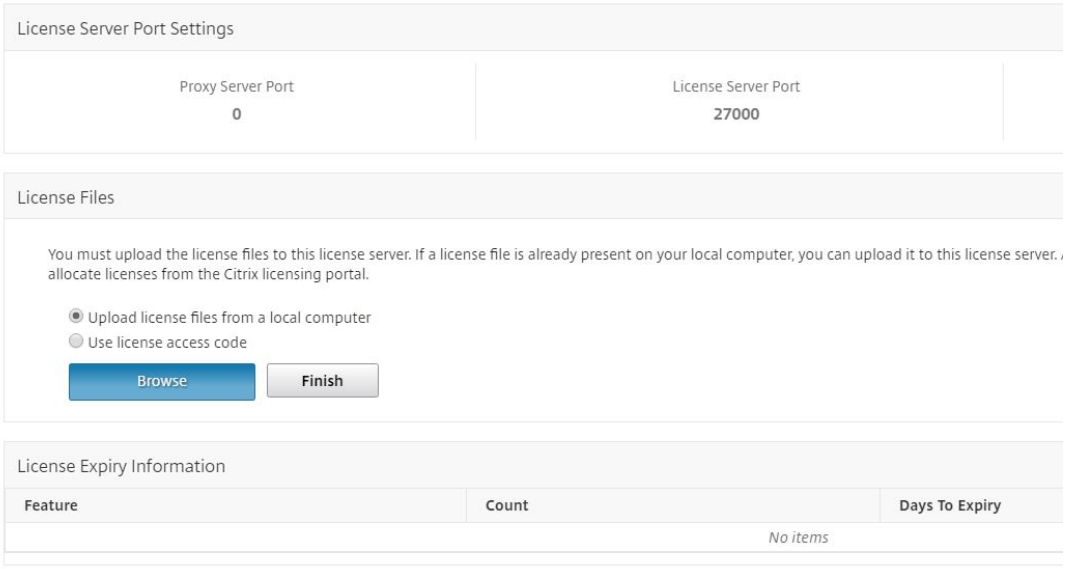
在 **Citrix ADM** 中上传许可证

将 Citrix ADC VPX 许可证上传到 Citrix ADM，以便 Citrix ADM 可以在与 NSX 进行编排期间自动向实例分配许可证。

要在 **Citrix ADM** 上安装许可证文件，请执行以下操作：

1. 在 Citrix ADM 中，导航到 网络 > 许可证。
2. 在 “ 许可证文件” 部分，选择以下选项之一：
   a) 从本地计算机上传许可证文件-如果本地计算机上已存在许可证文件，则可以将其上传到 Citrix ADM。要添加许可证文件，请单击 浏览并选择要添加的许可证文件 (.lic)。然后单击 “ 完成”。
   b) 使用许可证访问代码 -Citrix 通过电子邮件发送您购买的许可证访问代码。要添加许可证文件，请在文本框中输入许可证访问代码，然后单击 获取许可证。

> 注意：您可以随
>
> 时从许可证设置向 Citrix ADM 添加更多许可证。



在 **Citrix ADM** 中上传 **Citrix ADC VPX** 映像

将 Citrix ADC 映像添加到 Citrix ADM 中，以便 Citrix ADM 使用服务包中定义的这些映像。

要在 **Citrix ADM** 中上载 **Citrix ADC VPX** 映像，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 编排” > “ **SDN** 编排” > “ **VMware NSX** 管理器” > “ **ESX NSVPX** 映像”。
2. 单击 “ 上传”，然后从本地存储文件夹中选择 Citrix ADC VPX zip 包。

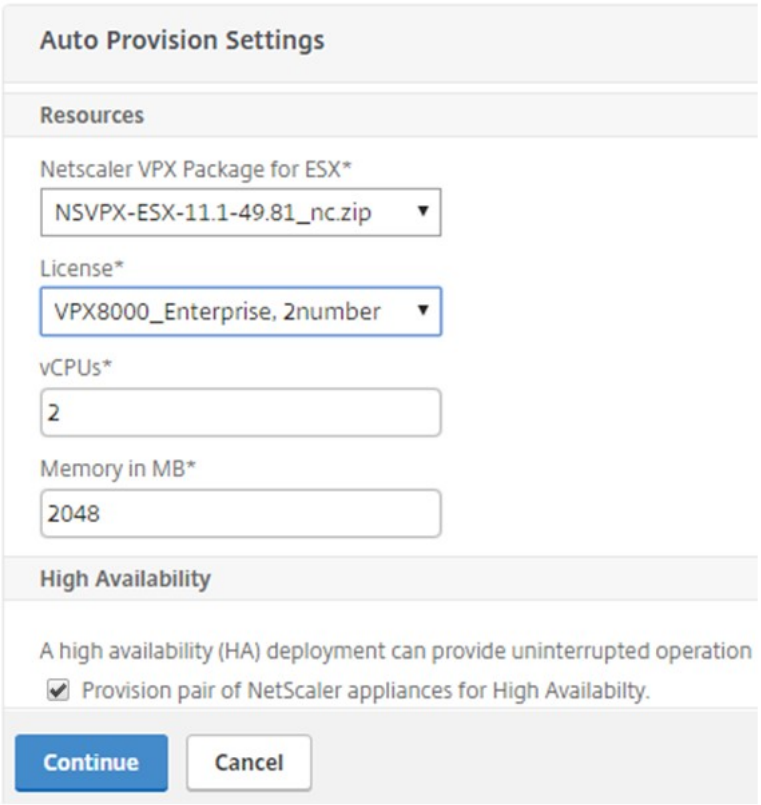
在 **Citrix ADM** 中创建服务包

在 Citrix ADM 中创建服务包以定义 SLA 集，该集指示如何分配 Citrix ADC 资源。

要在 **Citrix ADM** 中创建服务包，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 编排” > “ **SDN** 编排” > “ **VMware NSX** 管理器” > “ 服务包”，然后单击 “ 添加” 以添加新的服务包。
2. 在 “ 服务包” 页上的 “ 基本设置” 部分，设置以下参数：
   a) Name（名称）- 服务包的名称
   b) 隔离策略-选择 专用
   c) Citrix ADC 实例预配-选择 按需创建实例
   d) 自动配置平台-选择 思特利 **xADC SDX**
   e) 单击 “ 继续”
3. 在 “ 自动配置设置” 部分中，选择最近上传的 Citrix ADC VPX zip 包以将其部署到 NSX 平台上，选择相应的许可证，然后单击 “ 继续”。

> 注意：
>
> 在 “ 高可用性” 部分中，选中该复选框以为 HA 置备 Citrix ADC 实例。



> 注意
>
> 上图所示列表框中显示的许可证名称 VPx8000_Advanced，2 是一个示例，解释如下：
>
> - VPX-许可证是部署 Citrix ADC VPX 实例

> - 8000 - 可占用的带宽为 8 GB
> - 高级-Citrix 提供三种类型的许可证-标准许可证、高级许可证和高级许可证
> - 2 个数字-使用此许可证可以部署两个 Citrix ADC VPX 实例
>
> “许可证” 列表框中显示的许可证名称取决于您从 Citrix 购买的许可证。

4. 单击继续。
5. 服务包发布到 NSX 管理器。在 NSX Manager 中，导航到 “ 服务定义” > “ 服务管理器”。您可以将 Citrix ADM 作为服务管理器之一进行查看。这表示注册成功，并在 NSX 管理器和 Citrix ADM 之间建立了双向通信。

> 注意：
>
> 对于高可用性部署中的 Citrix ADM，许可证仅在 Citrix ADM 许可证服务器节点中上传。Citrix ADM 节点处于主动-被动模式。

为边界执行负载平衡器服务插入

在现有 NSX Edge 网关上执行负载平衡器服务插入，即将负载平衡功能从 NSX 负载均衡器卸载到 Citrix ADC。

要在 **NSX Edge** 网关上插入负载平衡服务，请执行以下操作：

1. 在 NSX Manager 中，导航到 “ 主页” > “ 网络和安全” > “ **NSX** 边缘”，然后双击以选择已配置的边缘 Gateway。
2. 单击 管理，然后在 负载均衡器选项卡上，选择 全局配置，然后单击 编辑。
3. 选择 “ 启用负载均衡器” 和 “ 启用服务插入” 以启用它们。
4. 在 服务定义中，选择发布到 NSX Manager 的服务包。
5. 为管理接口配置一个虚拟 NIC，为数据接口配置一个或多个虚拟 NIC。相应地为管理和数据选择网络。

> 注意：在主 IP 分配模式下选
>
> 择 IP 池选项。Citrix ADM 不支持手动或 DHCP 分配 IP 地址。

6. 单击刷新图标可查看运行时间的创建。

> 注意：
>
> 由于您要在 HA 部署中部署两个 Citrix ADC VPX 实例，因此在 NSX 管理器中会创建两个运行时间。
>
> 您可能需要刷新屏幕才能查看屏幕上显示的运行时间。

7. 选择运行时间，单击 操作，然后从弹出式菜单中选择 安装。如果是 HA，则还对另一个运行时重复此操作。
8. 当两个虚拟机启动时，状态的值将更改为 “正在服务中”，安装状态的值更改为 “已启用”。“

> 注意
>
> 您可能需要刷新屏幕才能查看状态的更改。

9. 在 Citrix ADM 中，导航到“业务 流程”>“ 请求”以查看服务插入完成的进度详细信息。您可以看到 Citrix ADM 发出了创建和更新运行时间的请求。更新运行时间后，选择请求，然后单击“ 任务”按钮以查看是否已在 NSX 管理器中添加了 Citrix ADM。

   对于 HA，在 Citrix ADM 中将有两个请求创建和更新两个运行时间。更新了两个运行时间后，请选择两个请求，然后单击“ 任务”按钮，以查看 NSX Manager 中是否添加了两个 Citrix ADM HA 节点。

10. 在 Citrix ADM 中，导航到“ 编排”>“ **SDN** 编排”>“ **VMware NSX** 管理器”>“ 边缘网关”。在右侧面板中，您可以查看是否已将 Citrix ADC VPX 添加到 NSX 边缘网关中。

    对于高可用性，您可以看到在 NSX 边缘网关中添加了两个处于高可用性模式的 Citrix ADC VPX 实例。

11. 在 Citrix ADM 中，导航到“ 网络”>“ 许可证”>“**VPX** 许可证”。选择 Citrix ADC VPX 许可证和您已安装的版本。

    处于 HA 模式的 Citrix ADC VPX 实例使用两个许可证，状态将显示在屏幕上，如下所示。

    服务插入完成后，您可以使用样书通过以下两种方法之一配置 Citrix ADC 实例：

    - 在 VMware NSX 管理器 GUI 中在 Citrix ADC VPX 上配置负载平衡服务
    - 在 Citrix ADM GUI 中在 Citrix ADC VPX 上配置负载平衡服务

在 **VMware NSX** 管理器 **GUI** 中在 **Citrix ADC VPX** 上配置负载平衡服务

执行以下任务以使用内置样书在 NSX Edge 网关设备上启用负载平衡服务的配置。

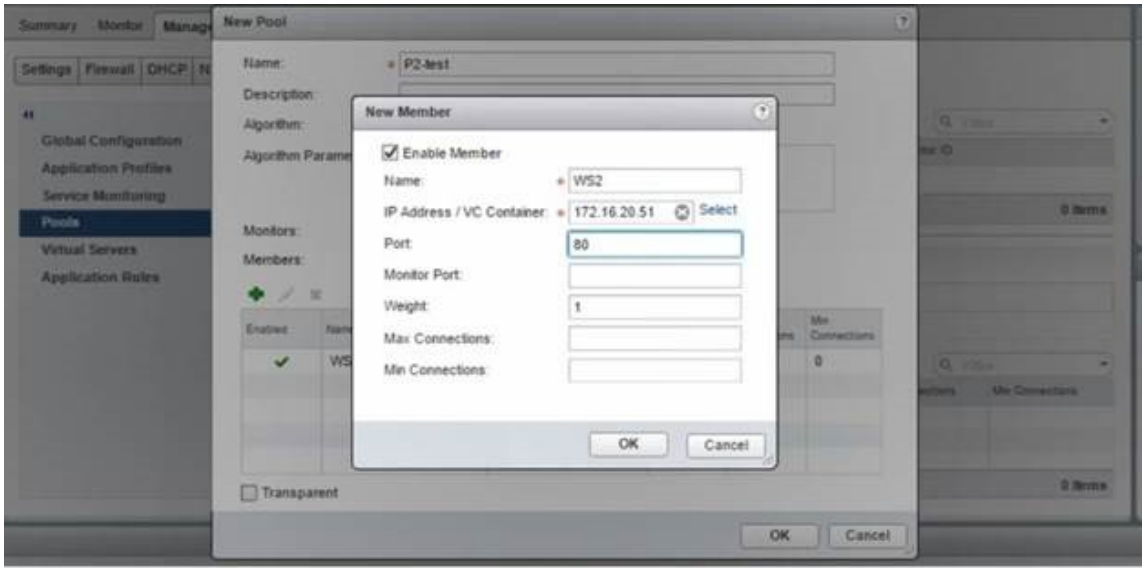
在 NSX Manager 中，导航到“ 主页”>“ 网络和安全”>“ **NSX** 边缘”，然后双击以选择已配置的边缘 Gateway。

创建池和池成员

创建服务器池和不同容量的成员。

1. 单击 “ 管理”，然后在 “ 负载均衡器” 选项卡上，选择 “ 池”，然后单击 “**+**” 图标添加新池，并设置以下参数：
   a) Name（名称）- 新池的名称
   b) Algorithm（算法）- 从下拉列表中选择算法，将基于该算法选择池。
   c) Monitors（监视器）- 确保服务监视器设置为 default_http_monitor
   d) Members（成员）- 单击 “+” 以向池添加成员，并在 “New Member”（新成员）窗口中输入必要的参数。
      i. Name（名称）- 成员的名称
      ii. IP Address/ VC Container（IP 地址/VC 容器）- 单击 “Select”（选择）以从可用列表中选择对象或输入对象的 IP 地址。
2. 单击 “ 确定”。

   根据需要添加任意数量的成员。



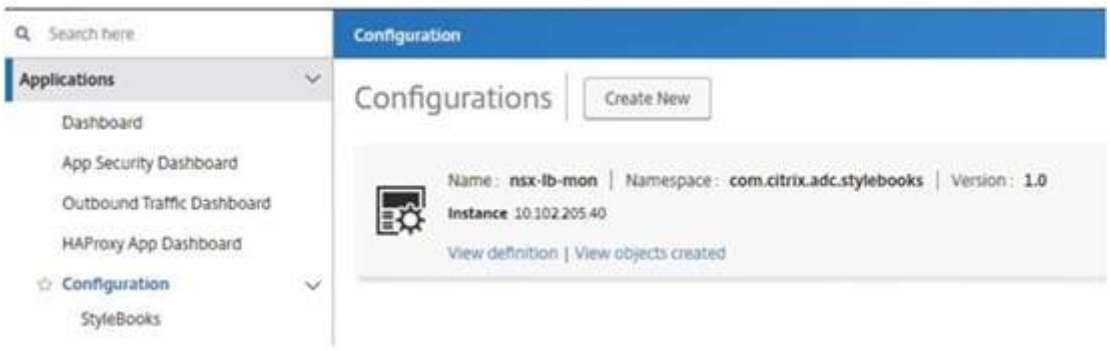
创建虚拟服务器

创建一组虚拟服务器，并为每个虚拟服务器分配一个池。

1. 单击 “ 管理”，然后在 “负载均衡器” 选项卡上，选择 “ 虚拟服务器”，然后单击 “**+**” 图标添加虚拟服务器，并设置以下参数：
   a) 应用程序配置文件-默认情况下，显示在 Citrix ADM 中创建的服务配置文件。
   b) Name（名称）- 虚拟服务器的名称。
   c) IP Address（IP 地址）- 单击 “Select”（选择）以选择现有的 IP 地址池或创建新的 IP 地址池。

d) Default pool（默认池）- 从下拉列表中选择默认池。

2. 单击 “ 确定”。
3. 在 Citrix ADM 中，导航到 “业务 流程” > “ 请求”，以查看在一个或多个选定 Citrix ADC 实例上完成服务创建的进度详细信息。
4. 在 Citrix ADM 中，导航到 应用程序 > 配置，然后检查 `nsx-lb-mon` 配置包是否已创建。



在 **Citrix ADM GUI** 中在 **Citrix ADC VPX** 上配置负载平衡服务

使用 Citrix ADM 样书在 Citrix ADC 实例上部署负载均衡器配置。对于 HA，配置部署在 HA 中的两个 Citrix ADC 实例上。

要通过样书创建配置包，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 应用程序” > “ 配置” > “ 创建新”，然后从列表中选择 **HTTP/SSL** 负载平衡（带监视器）样书。样书将以用户界面页面形式打开，您在此为此样书中定义的所有参数输入值。
2. 为所有所需参数指定值。
3. 选择在 NSX 环境中预配置的目标 Citrix ADC VPX 实例，然后单击 创建以在选定的设备上应用配置。对于 HA 部署，请选择处于 HA 模式的实例。

验证在 **Citrix ADC VPX** 实例中创建虚拟服务器和服务组

您可以查看是否通过登录到 Citrix ADC VPX 实例来创建服务组和虚拟服务器。

要查看服务组和虚拟服务器，请执行以下操作：

1. 登录到 Citrix ADC VPX 实例。对于 HA 部署，您必须登录到处于 HA 状态的两个 Citrix ADC 实例。
2. 导航到 “ 配置” > “ 系统” > “ 网络”。在右侧窗格中，可以查看添加的 IP 地址。单击 IP 地址超链接可以查看详细信息。您可以看到子网 IP 地址与在 NSX 中添加的 Web Interface 的 IP 地址相同。
3. 接下来，导航到 流量管理 > 负载平衡 > 虚拟服务器，然后查看虚拟服务器的详细信息。
4. 接下来，导航到 服务组并查看服务组详细信息。
5. 最后，导航到 “ 配置” > “ 系统” > “ 许可证” 以查看应用于此实例的许可证。

删除负载平衡服务

如果在 NSX 管理器上部署的 Citrix ADC VPX 实例上不再需要负载平衡服务，则可以删除之前执行的服务插入。

要删除配置和服务插入：

1. 在 Citrix ADM 中，导航到 “ 应用程序” > “ 配置”，选择创建的应用程序配置，然后单击 “X” 图标删除配置。
2. 在 NSX 管理器中，导航到 Citrix ADC VPX 实例所连接的边缘 Gateway。导航到 管理 > 负载均衡器 > G**lobal** 配置，右键单击运行时条目，然后单击 取消置备。将是虚拟机停止工作。
3. 在 Citrix ADM 中，导航到 “ 编排” > “ 云编排” > “ 边缘网关”。确保没有将 Edge 网关与已删除的实例相应映射。

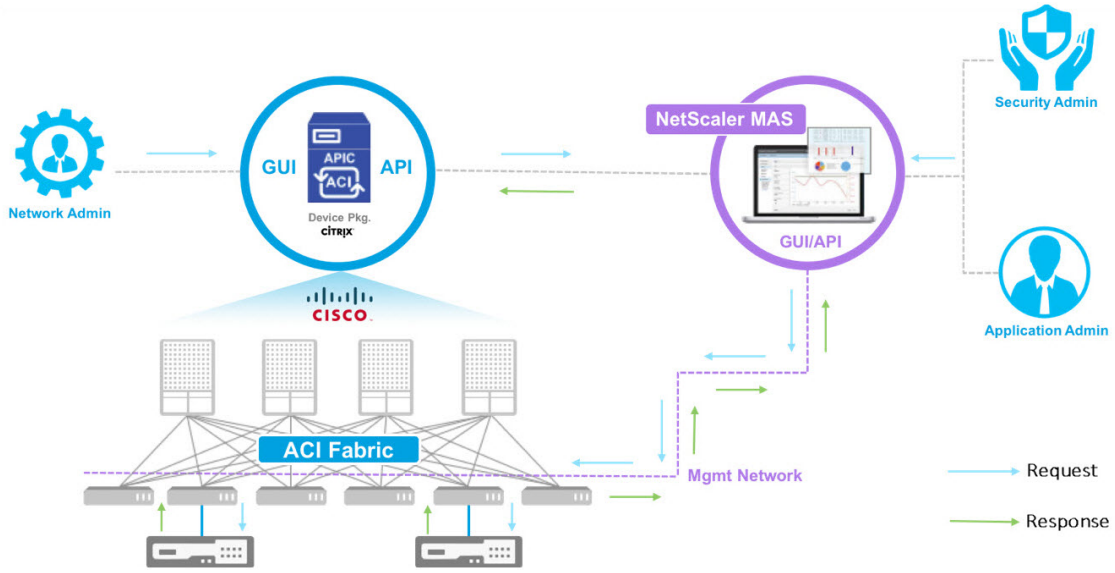
在思科 **ACI** 混合模式下使用 **Citrix ADM** 实现 **Citrix ADC** 自动化

April 23, 2021

Cisco ACI 1.3 版 (2f) 中引入了混合模式支持。在混合模式下，您可以通过应用程序策略基础架构控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委派给 Citrix Application Delivery Management (ADM)，后者充当 APIC 中的设备管理器。

混合模式器件封装和 Citrix ADM 支持 Citrix ADC 混合模式解决方案。需要在 APIC 中上载混合模式设备包。此软件包提供来自 Citrix ADC 的所有网络 L2-L3 可配置实体。应用程序奇偶校验由样书从 Citrix ADM 映射到 APIC。也就是说，样书充当给定应用程序的 L2-L3 配置和 L4-L7 配置之间的引用。在配置适用于 Citrix ADC 的 APIC 中的网络实体时，必须提供样书名称。

下图概述了混合模式解决方案中的 Citrix ADC：



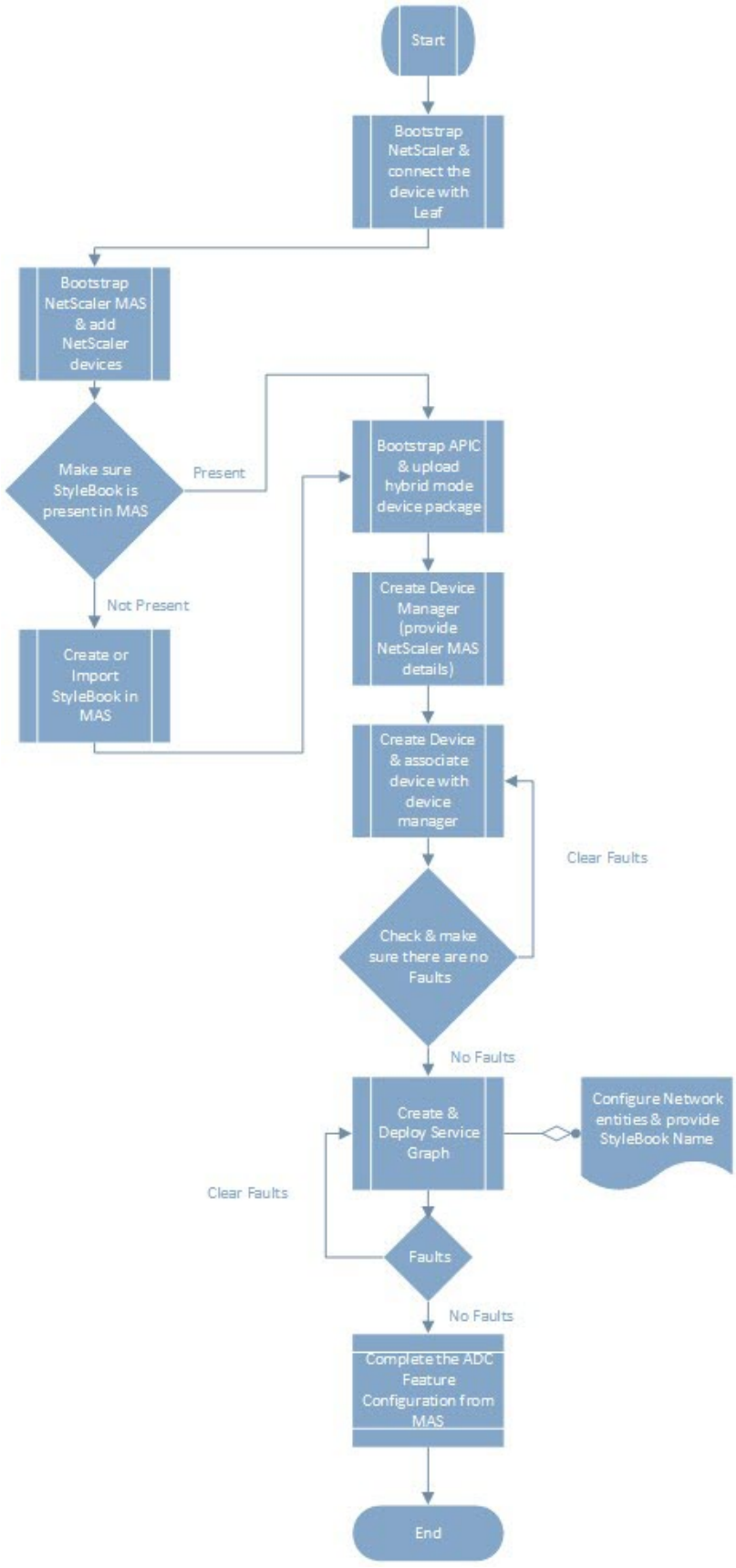
在混合模式下，Citrix ADC 配置分两个阶段执行：

1. 从 Cisco APIC 进行网络交换

2. 通过 Citrix ADM 完成配置

对于任何给定的应用程序，在 Cisco APIC 中进行服务图创建和部署过程中，网络管理员必须提供网络特定的详细信息，例如 IP 地址、端口、虚拟 LAN（自动）等。然后通过设备包将这些配置详细信息推送到 Citrix ADM，Citrix ADM 在内部处理这些详细信息并配置 Citrix ADC。应用程序管理员通过在 Citrix ADM 中使用样书创建应用程序与 ADC 相关的配置，然后将这些配置从 Citrix ADM 推送到 Citrix ADC。思科 APIC 和 Citrix ADM 通过管理网络与 ADC 进行通信。

下图显示了混合解决方案中的 Citrix ADC 工作流：



必备条件

April 23, 2021

请确保：

- 您拥有 Cisco ACI 组件和 Citrix ADC 的概念知识。
  - 有关 Cisco ACI 及其组件的详细信息，请参阅以下产品文档：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html。
  - 有关 Citrix ADC 的详细信息，请参阅 Citrix ADC 产品文档：http://docs.citrix.com/。
- 已设置并配置所有所需的 Cisco ACI 组件，包括数据中心里的 Cisco APIC。有关 Cisco ACI 及其组件的详细信息，请参阅以下产品文档：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html。
- 您已安装 Citrix ADC 11.1 或更高版本。
- 您已在思科 ACI 中配置了 Citrix ADC，以便可以使用思科 APIC 对它们进行管理。
- 您已在您的环境中部署了 Citrix Application Delivery Management (ADM)。有关详细信息，请参阅 Citrix ADM 13.0。
- 建立了从 APIC 到 Citrix ADM 和 ADC 的管理连接。
- 请记录：
  - 用于管理和数据路径连接的连接接口和 IP 地址。
  - 叶交换机详细信息：Citrix ADC IP 地址、端口、接口等。

> 注意
>
> 在此版本中，混合模式解决方案在单一上下文中支持 Citrix ADC，即不支持管理分区。

使用思科 **APIC** 和 **Citrix ADM** 在混合模式下配置 **Citrix ADC**

April 23, 2021

执行以下任务，通过使用思科 APIC 和思杰应用程序交付管理 (ADM) 在混合模式下配置 Citrix ADC：

1. 将结构中的 Citrix ADC 实例添加到 Citrix ADM 中。相关说明，请参阅将实例添加到 Citrix ADM。
2. 使用 Citrix ADM 为应用程序创建样书。相关说明，请参阅使用 Citrix ADM 为应用程序创建样书。
3. 将 Citrix ADC 混合模式设备包导入思科 APIC。有关说明，请参阅将 Citrix ADC 混合模式设备包导入思科 APIC

4. 在思科 APIC 中将 Citrix ADM 添加为设备管理器。有关说明，请参阅在思科 APIC 中将 Citrix ADM 添加为设备管理器
5. 使用思科 APIC 在思科 ACI 中添加 Citrix ADC 设备。有关说明，请参阅在思科 ACI 中将 Citrix ADC 作为设备添加
6. 创建和部署服务图模板。有关说明，请参阅创建和部署服务图
7. 在 Citrix ADM 中使用样书配置 L4-L7 参数。有关说明，请参阅使用 Citrix ADM 中的样书配置 L4-L7 参数
8. Cisco APIC 中的附加或分离端点事件。有关详细信息，请参阅从 APIC 附加或分离端点事件。

使用 **Citrix ADM** 为应用程序创建样书

April 23, 2021

样书是一种配置模板，您可以使用它为任何应用程序创建和管理 Citrix ADC 配置。您可以创建用于配置特定 Citrix ADC 功能的样书，例如负载平衡、SSL 卸载或内容切换。可以设计样书以创建针对企业应用程序部署（例如 Microsoft Exchange 或 Lync）的配置。有关详细信息，请参阅 样本。

您可以为您的应用程序创建自己的样书，也可以修改和使用随 Citrix Application Delivery Management (ADM) 附带的 APIC-HTTP-LB 样书。

要在 Citrix ADM 中为您的应用程序创建自己的样书，请参阅 如何创建您自己的样本。

创建样书时，请务必遵循样书中的 APIC 服务图模型。也就是说，适用于任何应用程序的 APIC 服务图遵循通过 ADC 功能连接的使用者和提供商模型。使用者和提供商以端点组 (EPG) 表示，是一对一的关系。在样书中也必须遵循相同的模型，其中提供商 EPG 必须以服务组表示，每个端点以服务组的成员表示。ADC 功能节点必须由虚拟服务器（例如，负载平衡虚拟服务器）表示，虚拟服务器与服务组之前必须是一对一的关系。

这基本上体现了服务图的本质，让您可以处理来自 APIC 的附加或分离事件，其中附加事件是将端点绑定到对应的服务组，分离事件是对其取消绑定。必须确保服务图和样书是对等的，以实现从网络 L2-L3 到 ADC 功能 L4-l7 配置的无缝自动化。

将 **Citrix ADC** 混合模式设备封装导入思科 **APIC**

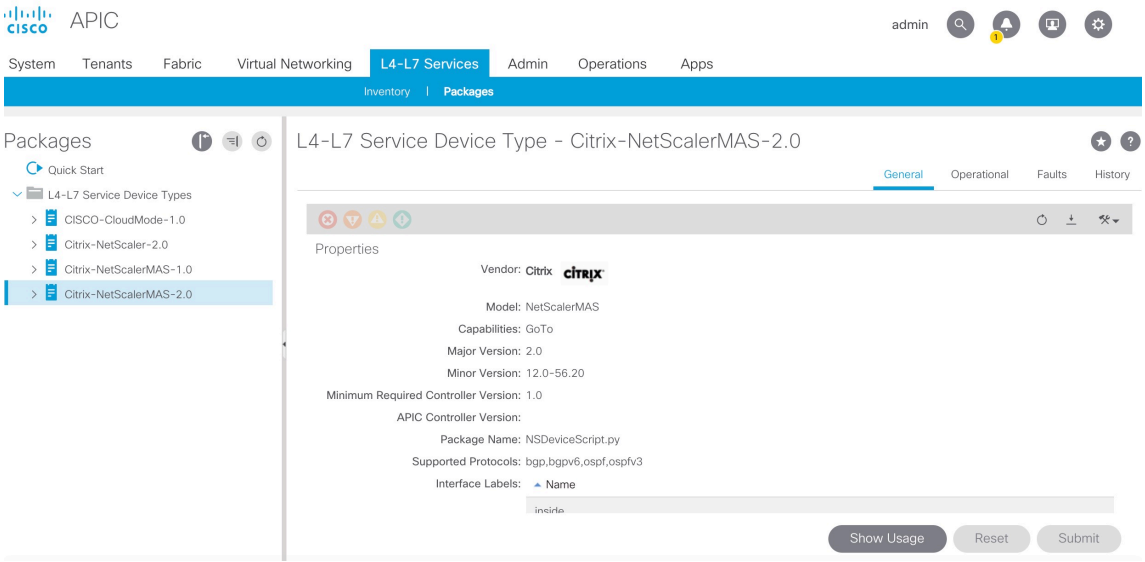
April 23, 2021

与完全托管模式相比，混合模式设备包是轻型包。通过设备型号只能提供 L2-L3 网络参数。器件型号中只定义了一个通用 ADC 功能，以及基于结构中 Citrix ADC 部署的四个功能配置文件（例如，单臂和双臂，RHI 相同）。混合模式设备包名称是 **NetScaler** 混合模式设备包 **12.0** 版本 **56.20**。在中搜索混合模式设备包 Citrix 下载站点，下载它，然后将设备包导入 APIC。

> 注意
>
> 混合模式设备包可以与完全托管模式设备包共存。

要使用 **APIC GUI** 将混合模式设备包导入 **APIC**，请执行以下操作：

1. 在菜单栏上，单击 “ **L4-L7** 服务” 选项卡，然后选择 “ 程序包” 面板。
2. 在 导航窗格中，右键单击 **L4-L7** 设备类型，然后选择 导入设备包。
3. 在 “ 导入设备包” 对话框中，单击 “ 浏览” 以选择下载的 Citrix ADC 混合模式设备包。
4. 单击 **Submit**（提交）。
   成功将设备包导入 APIC 后，可以在 “ 导航” 窗格中单击设备名称来查看设备包的详细信息。



> 重要
>
> 导入设备包后，请确保 APIC 中没有故障。可以单击 “Device Types”（设备类型）窗口中的 **Faults**（故障）选项卡查看故障。

在思科 **APIC** 中将 **Citrix ADM** 添加为设备管理器

April 23, 2021

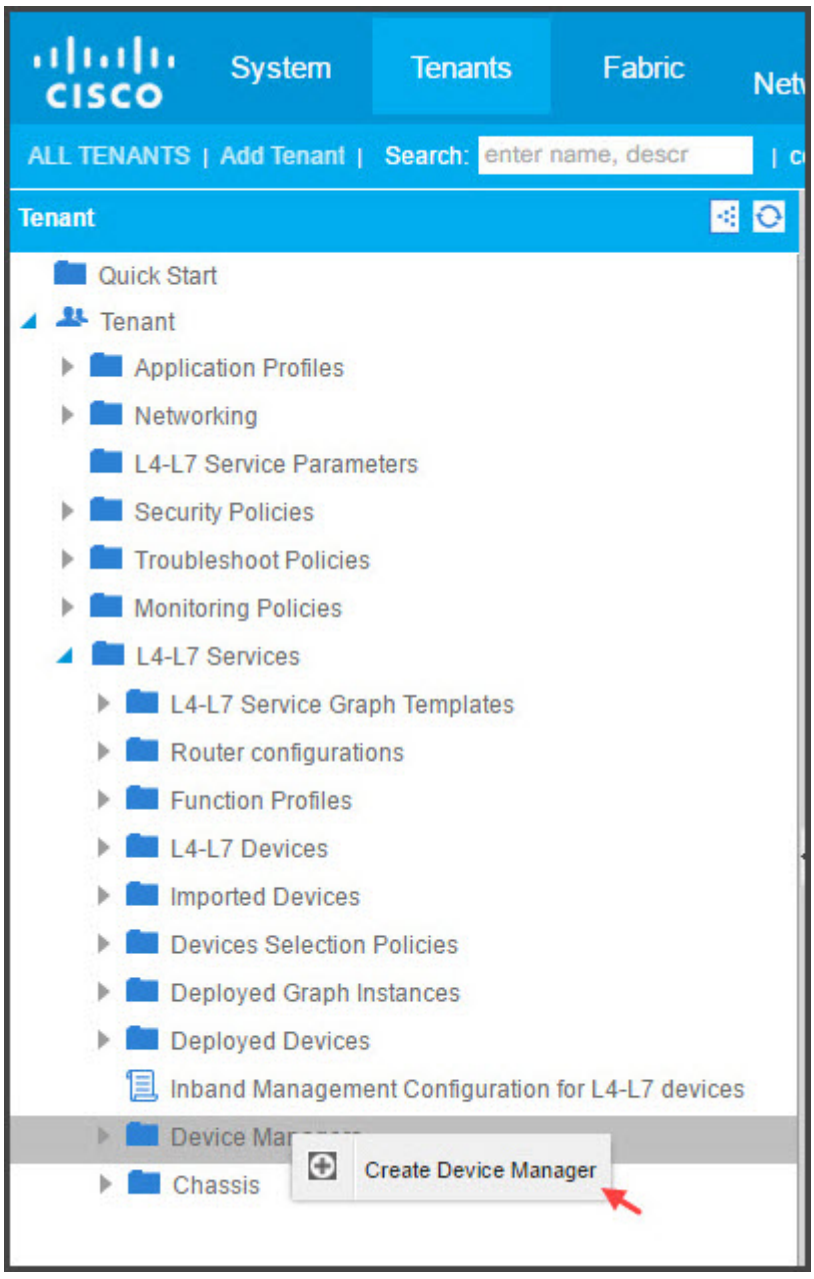
May 24, 2018

思杰应用程序交付管理 (ADM) 充当 Cisrix ACI 上部署的 Citrix ADC 的集中设备管理器。您需要在思科 APIC 中将 Citrix ADM 添加为设备管理器。

要使用 **APIC GUI** 将 **Citrix ADM** 添加为设备管理器，请执行以下操作：

1. 在菜单栏上，转到 **“租户” > “所有租户”**。

2. 在 “ 工作” 窗格中，双击租户的名称。
3. 在 导航窗格中，选择 ***** 租户名称 *** > L4-L7** 服务。
4. 右键单击 “ 设备管理器”，然后单击 “ 创建设备管理器”。

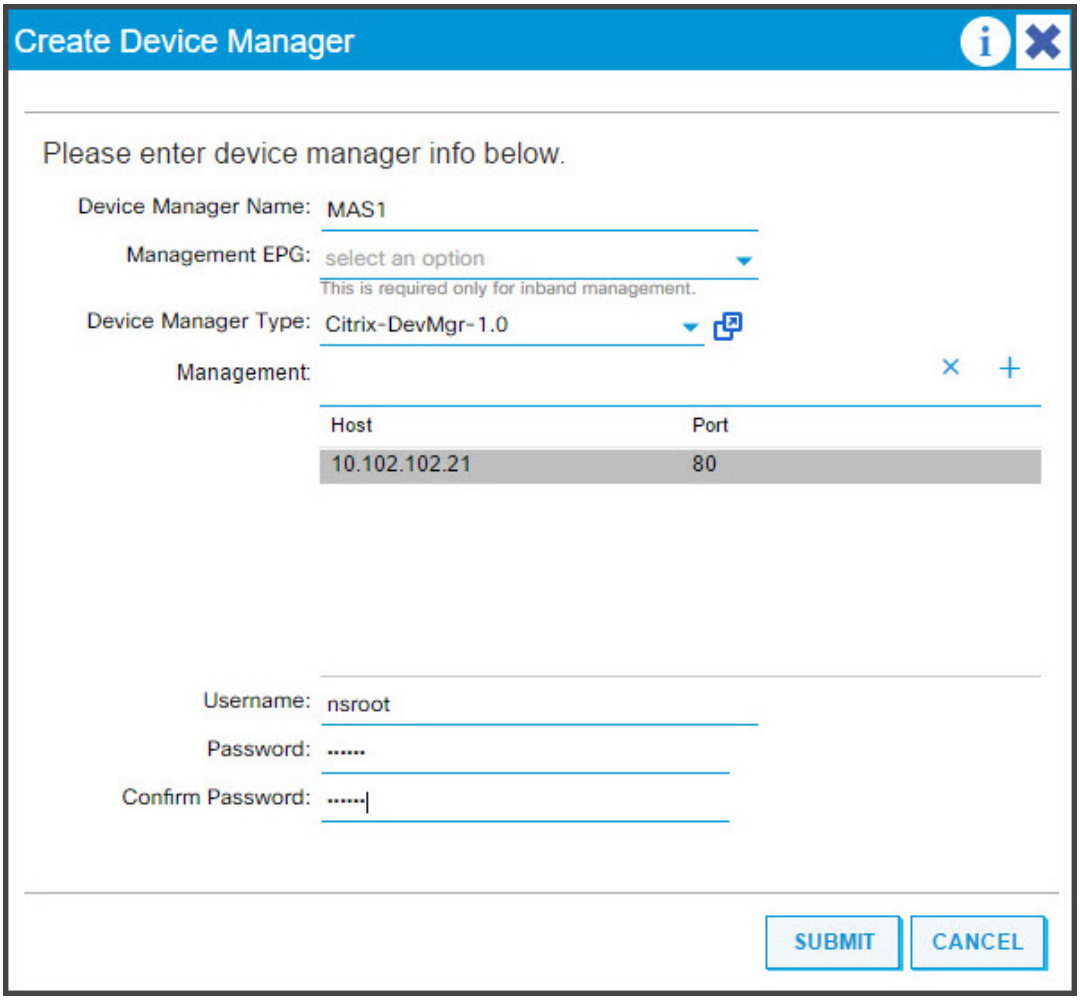


5. 在 “ 创建设备管理器” 对话框中，执行以下操作：
   a) 在 “ 设备管理器名称” 字段中，输入要注册为设备管理器的 Citrix ADM 部署的名称。
   b) 在 **Management EPG**（管理 EPG）下拉列表中，选择管理 EPG。
   c) 在 **Device Manager Type**（设备管理器类型）下拉列表中，选择 **Citrix-DevMgr-1.0**。
   d) 在 管理字段中，单击 **+** 并添加 Citrix ADM 部署的 IP 地址和端口详细信息。

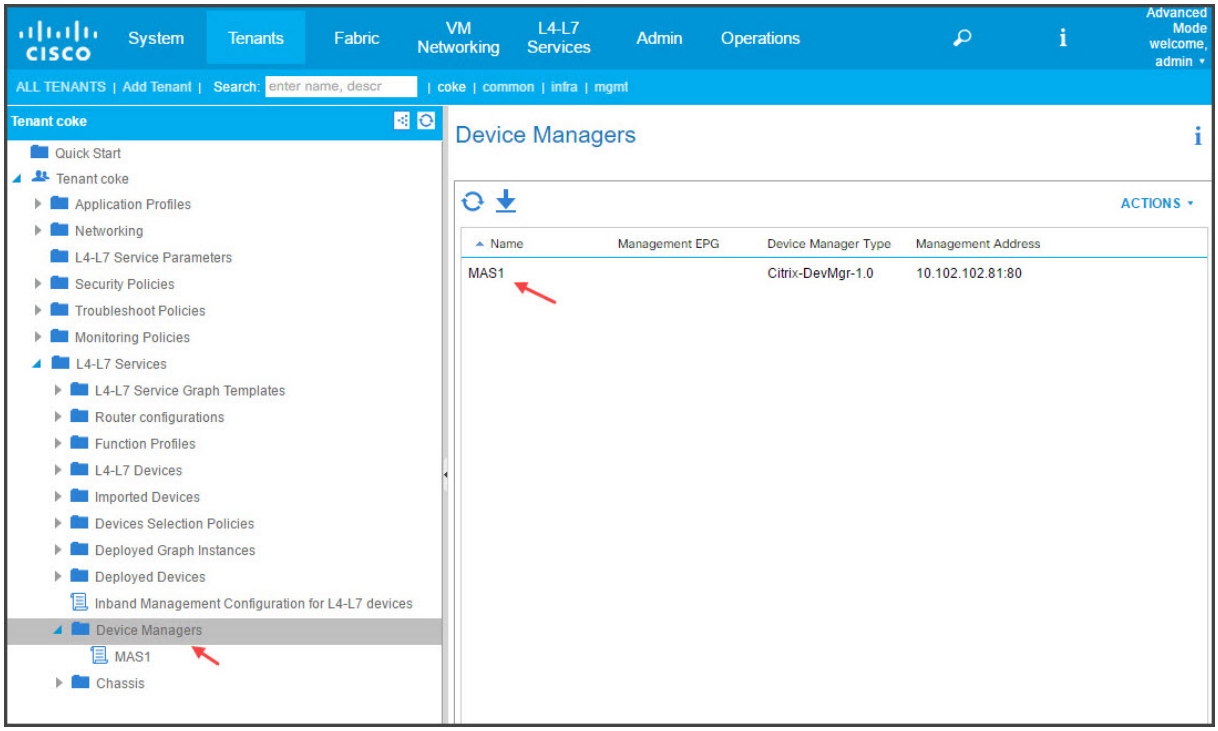
e) 在 **“用户名”** 字段中，输入访问 **Citrix ADM** 的用户名。

f) 在 “ 密码” 和 “ 确认密码” 字段中，输入访问 Citrix ADM 的密码。

g) 单击 **SUBMIT**（提交）。



一旦 Citrix ADM 在 APIC 中成功注册为设备管理器，便会添加设备管理器并显示在 “ 导航” 窗格中。要查看注册的设备管理器，请在导航窗格中转到 ***** 租户名称 *** > L4-L7** 服务 **>** 设备管理器。



> 注意
>
> 确保 Cisco APIC 和 Citrix ADM 之间没有连接问题，并且您提供的凭据与用于访问 Citrix ADM 的相同。还需确保帐户具有管理员权限。
>
> 重要
>
> 导入设备包后，请确保 APIC 中没有故障。可以单击“Device Types”（设备类型）窗口中的 **Faults**（故障）选项卡查看故障。

您还可以使用 API 将 Citrix ADM 注册为设备管理器。以下是示例 XML 有效负载，展示了如何使用 API 将 Citrix ADM 添加为设备管理器。

```
<polUni>
<gvTenant name="coke">
<vnsDevMgr name="MAS1">
<vnsRsDevMgrToMDevMgr tDn="uni/infra/mDevMgr-Citrix-DevMgr-1.0" />
<vnsCMgmts name="devMgmt" host="10.102.102.81" port="80"/>
<vnsCCred name="username" value="nsroot"/>
< 虚拟机密码名称 = "密码" 值 =" * ( “/****
</vnsDevMgr>
</fvTenant>
</polUni>
```


使用 **APIC** 将 **Citrix ADC** 添加为思科 **ACI** 中的设备

April 23, 2021

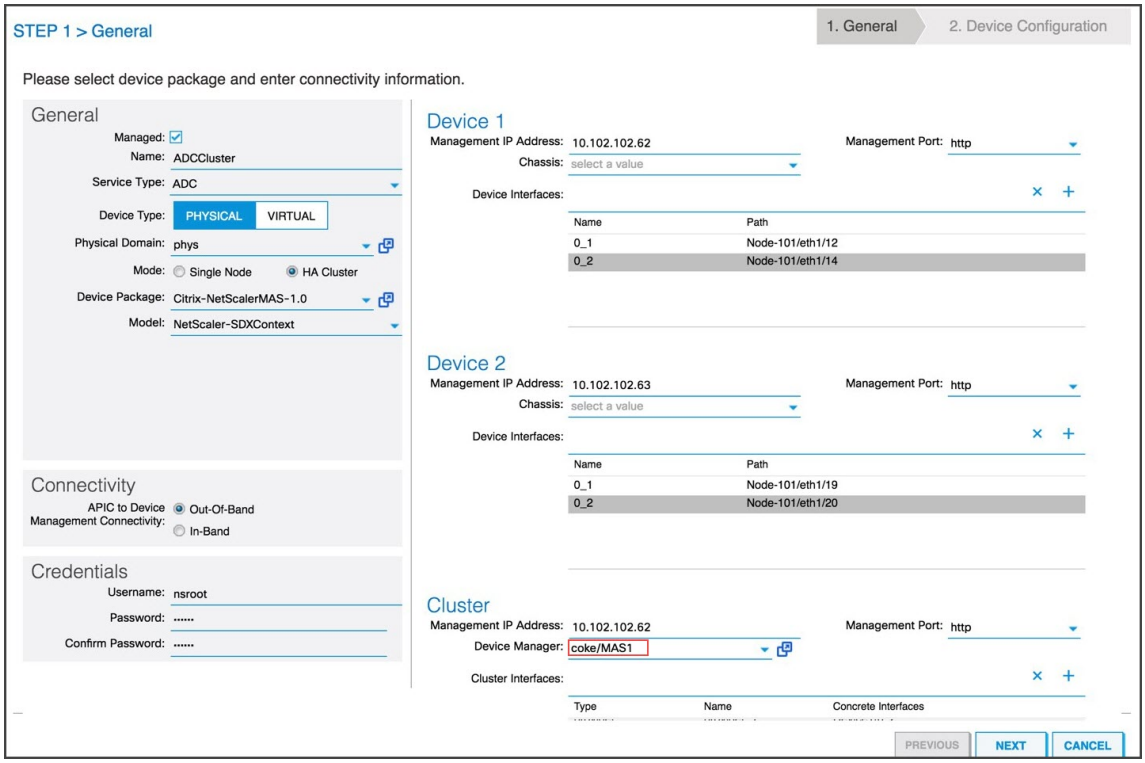
您需要将 Citrix ADC 作为 L4-L7 设备添加到 APIC 以实现网络自动化。APIC 根据部署的服务图，在 Leaf 和 Citrix ADC 设备之间执行网络拼接。需要配置设备配置的基本设置，例如配置管理 IP 地址、设备管理器和凭据。

要使用 **APIC GUI** 将 **Citrix ADC** 注册为 **APIC** 中的设备，请执行以下操作：

1. 在菜单栏上，转到 **“租户” > “**所有租户”。
2. 在 “ 工作” 窗格中，双击租户的名称。
3. 在 导航窗格中，选择 ***tenant_name* > L4-L7 Services > L4-L7 Devices**。
4. 在 “工作” 窗格中，选择 **“操作” > “**创建 **L4-L7** 设备”。
5. 在 “ 创建 **L4-L7** 设备” 对话框的 “ 常规” 部分，执行以下操作：
   a) 选中 “ 托管” 复选框。
   b) 在 “名 称” 字段中，输入设备的名称。
   c) 在 **Service Type**（服务类型）下拉列表中，选择 **ADC**。
   d) 在 **Device Type**（设备类型）字段中，选择 **Physical**（物理）。

   > 注意：请
   >
   > 确保对于 VMware ESX，选择 “虚拟” 并关联相应的虚拟机管理器 (VMM) 域。

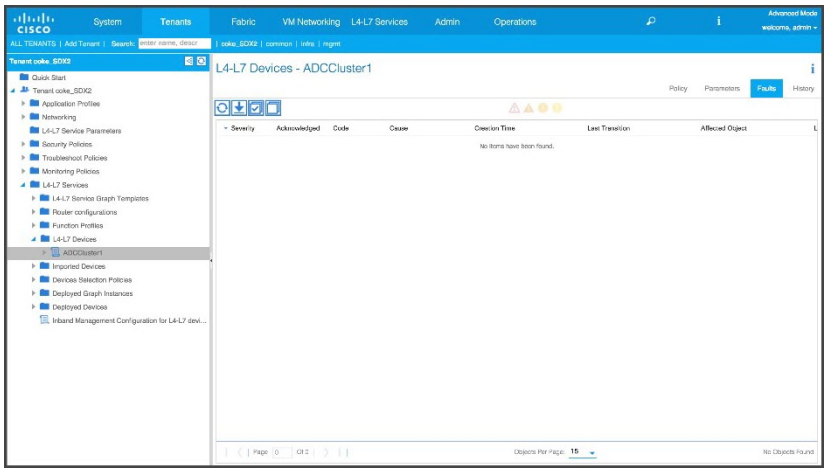
   e) 在 **Physical Domain**（物理域）下拉列表中，选择物理域。
   f) 在 “ 模式” 字段中，根据您的要求选择 单节点或 **HA** 群集。
   g) 在 “ 设备包” 下拉列表中，选择 **Citrix** 网络扩展器**-1.0**。
   h) 在 “ 型号” 下拉列表中，选择设备型号。例如，思杰 ADC-MPX 或思杰 ADC-VPX。
6. 在 **Connectivity**（连接）部分的 **APIC to Device Management Connectivity**（APIC 到设备管理连接）字段中，根据 NetScaler 在结构中的配置方式，选择 **Out-Of-Band**（带外）或 **In-Band**（带内）。
7. 在 “ 凭据” 部分中，指定用于访问设备的用户名和密码。
8. 在 “ 设备 **1** ” 和 “ 设备 **2** ” 部分，分别完成与管理相关的配置。
9. 在 “ 群集” 部分中，完成群集的管理相关配置。确保在 “设 备管理器” 下拉列表中，选择在 在思科 APIC 中将 Citrix ADM 添加为设备管理器



10. 单击“ 下一步”。此时将显示“Device Configuration”（设备配置）页面。混合模式设备包不提供设备和群集特定的配置详细信息，例如高可用性、启用/禁用功能和模式以及有关 NTP、SNMP 和 SNMP 警报等的配置。这些配置必须通过使用 Citrix ADM 完成。

11. 单击“ 完成”。成功在 APIC 中注册了设备后，设备会添加并显示在“Navigation”（导航）窗格中。要查看已注册的设备，请在导航窗格中转到 ***tenant_name* > L4-L7 Services > L4-L7 Devices > device_name**。

> 重要
>
> 注册设备后，请确保 APIC 中没有故障。您可以通过单击“ 工作”窗格中的“ 故障”选项卡查看错误。



您还可以使用 API 注册 Citrix ADC 设备。下面是添加 L4-L7 设备的示例 XML 有效负载：


```
<polUni>

<gvTenant name="coke">

<vnsLDevVipname="ADCCluster1"funcType="GoTo" svcType="ADC">

<vnsRsMDevAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0" />

<vnsRsALDevToPhysDomP tDn="uni/phys-phys"/>

<vnsCMgmt name="devMgmt"host="10.102.102.67"port="80"/>

<vnsCCred name="username" value="nsroot"/>

<vnsCCredSecret name="password" value="****"/>

<vnsRsALDevToDevMgr tnVnsDevMgrName="MAS1"/>

<vnsCDev name="ADC1" devCtxLbl="C1">

<vnsCIf name="1_1">

<vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/33]"/>

</vnsCIf>

<vnsCIf name="1_2">

<vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/35]"/>

</vnsCIf>

<vnsCMgmt name="devMgmt" host="10.102.102.65" port="80"/>

<vnsCCred name="username" value="nsroot"/>

<vnsCCredSecret name="password" value="****"/>

</vnsCDev>

<vnsCDev name="ADC2" devCtxLbl="C1">

<vnsCIf name="1_1">

<vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/34]"/>
```



```
46
47  </vnsCIf>
48
49  <vnsCIf name="1_2">
50
51  <vnsRsCIfPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/36]"/>
52
53  </vnsCIf>
54
55  <vnsCMgmt name="devMgmt" host="10.102.102.66" port="80"/>
56
57  <vnsCCred name="username" value="nsroot"/>
58
59  <vnsCCredSecret name="password" value="****"/>
60
61  </vnsCDev>
62
63  <vnsLIf name="outside">
```

</vnsLIf>

</VNSLDV

</fvTenant>

</polUni>

创建和部署服务图

April 23, 2021

您必须在 APIC 中使用思科 APIC 服务图模板来创建和部署 Citrix ADC。请务必在创建和部署服务图时使用 ADC 功能配置文件。

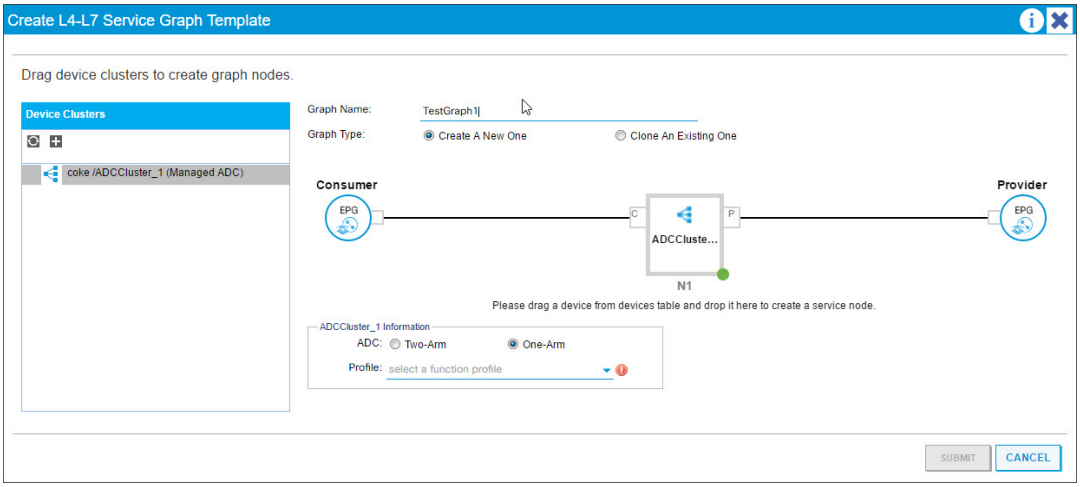
在 APIC 中配置图形后，APIC 根据功能定义、与结构的设备连接以及配置为图形部署一部分的实体来自动完成设备配置。作为创建服务图的一部分，APIC 还自动完成网络配置（例如虚拟 LAN 分配及其绑定），在您从 APIC 删除图形后，该配置会立即被删除。

服务图以两层或多层应用程序表示，它们之间插入适当的服务功能。按照合同，在源和目标 EPG 之间插入服务图。

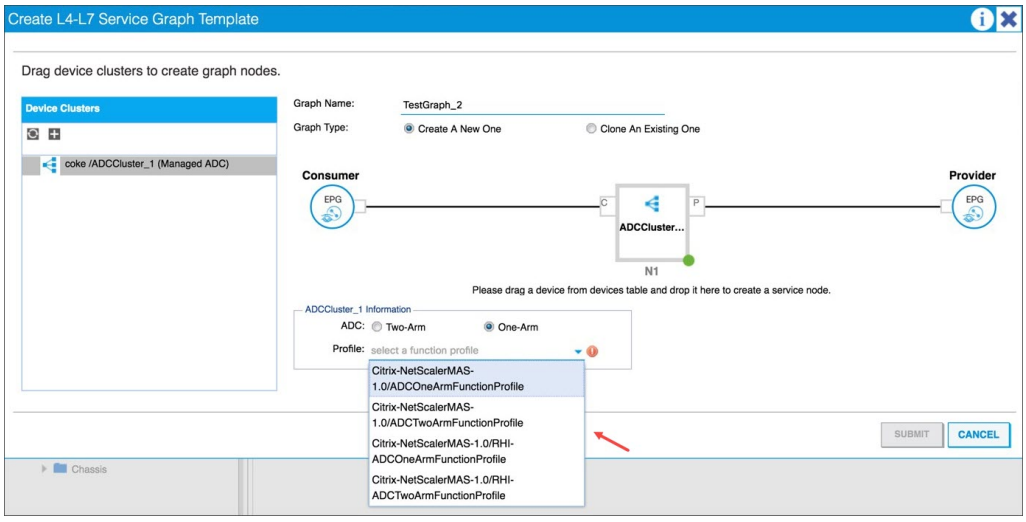
要使用 **APIC GUI** 创建服务图，请执行以下操作：

1. 在菜单栏上，转到 **“租户” > “**所有租户”。
2. 在 “ 工作” 窗格中，双击租户的名称。
3. 在 导航窗格中，选择 **tenant_name > L4-L7 服务 > L4-L7 服务图形模板 **。

4. 在 “ 工作” 窗格中，选择 **“操作” > “**创建 **L4-L7** 服务图模板”。
5. 在 “ 创建 **L4-L7** 服务图模板” 对话框的 “设备群集” 部分中，选择一个设备群集，然后执行以下操作：
   a) 在 **Graph Name**（图形名称）字段中，输入服务图模板的名称。
   b) 在 **Graph Type**（图形类型）字段中，选择 **Create A New One**（创建一个新图）。
   c) 在 **Device Cluster**（设备群集）部分，将设备拖放在使用者端点组和提供商端点组之间以创建服务节点。

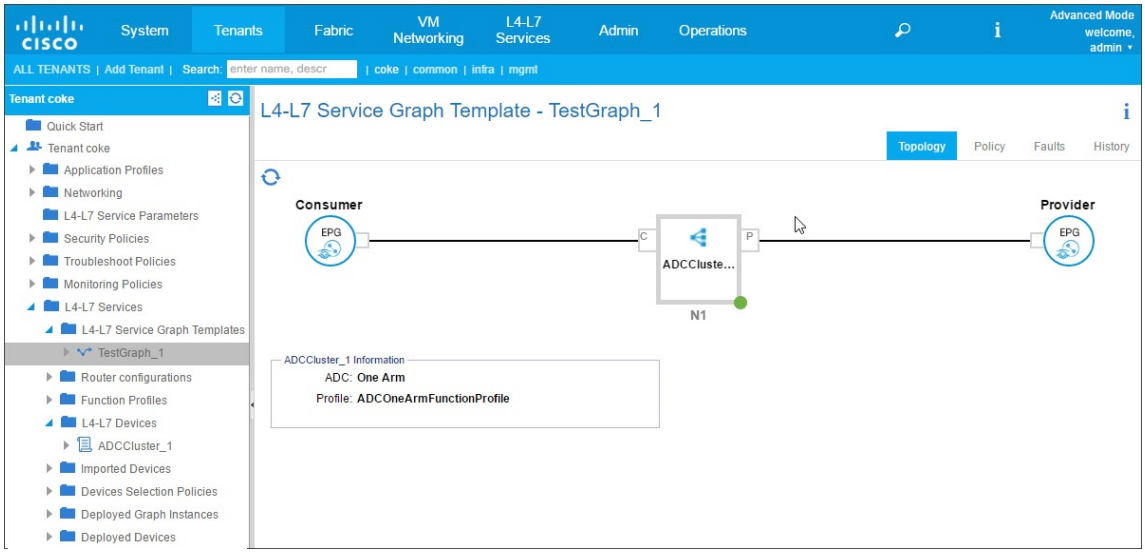


   d) 在 <***L4-L7device_name information***> 部分，执行以下操作：
      i. 在 **ADC** 字段中，选择 单臂或 双臂，具体取决于在结构中部署 Citrix ADC 的方式。
      ii. 在 “ 配置文件” 下拉列表中，选择设备包中提供的功能配置文件。



      iii. 单击 **SUBMIT**（提交）。
6. 在 “导 航” 窗格中，单击服务图模板。屏幕上将显示服务图模板的图形拓扑。

> 注意
>
> Cisco APIC 支持连接器的概念，这些连接器在 ADC 群集节点中可见。连接器定义网络流量方向和设备脚本，该脚本根据连接是外部还是内部，动态将分配的虚拟 LAN 绑定到虚拟 IP (VIP) 或子网 IP (SNIP) 地址。此外，虚拟 LAN 还绑定到用于入站流量和出站流量的特定接口。

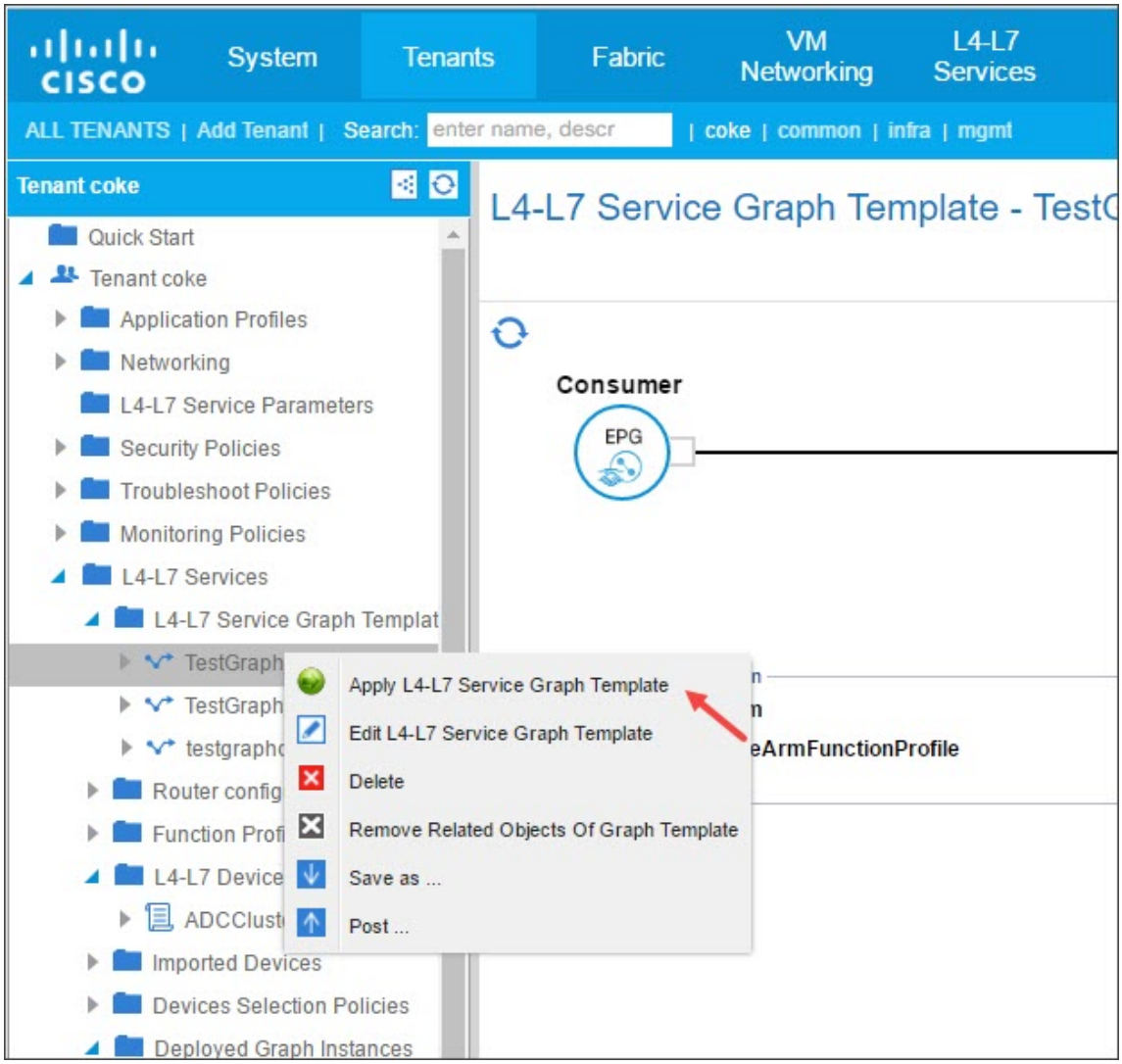


将服务图模板应用于端点组

创建了服务图模板后，需要使用 APIC GUI 来应用创建的服务图模板。

要应用服务图模板，请执行以下操作：

1. 在菜单栏上，转到 **“租户” > “所有租户”**。
2. 在 “ 工作” 窗格中，双击租户的名称。
3. 在导航窗格中，选择 **tenant_name > L4-L7 服务 > L4-L7 服务图形模板 **。
4. 右键单击 模板名称，然后单击 应用 **L4-L7** 服务图模板。

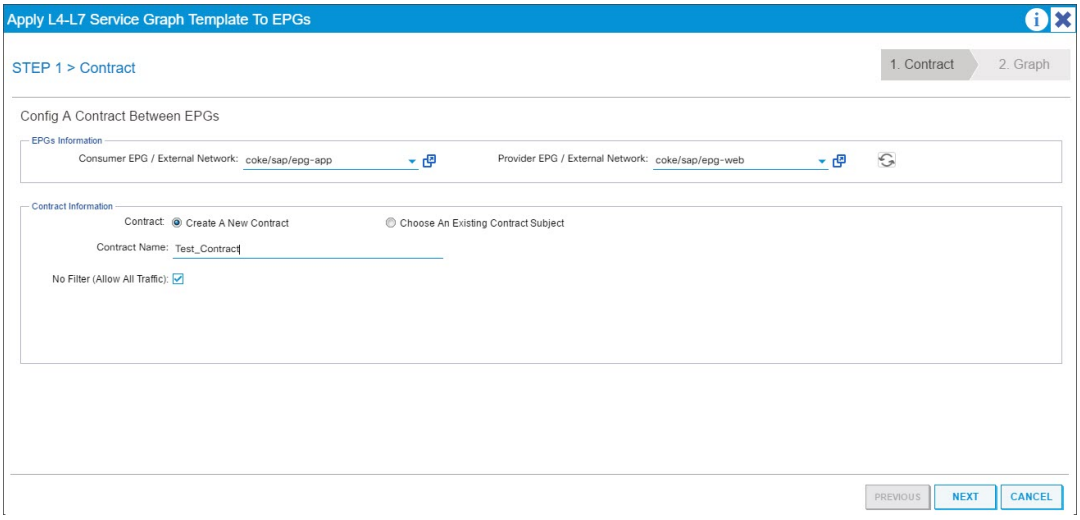


5. 在“将 **L4-L7** 服务图模板应用于 **EPG** ”对话框的“ **EPG** 信息”部分中，填写以下字段：

   a) 在 **Consumer EPG/External Network**（使用者 EPG/外部网络）下拉列表中，选择使用者端点组。

   b) 在 **Provider EPG/External Network**（提供商 EPG/外部网络）下拉列表中，选择提供商端点组。

   c) 在 **Contract Information**（合同信息）部分，完成适当的字段。合同信息与 Cisco APIC 特定相关，并作为与 EPG 关联的安全策略的一部分进行配置。



d) 单击“ 下一步”。

e) 在“ 图形模板”下拉列表中，选择您创建的服务图形模板。

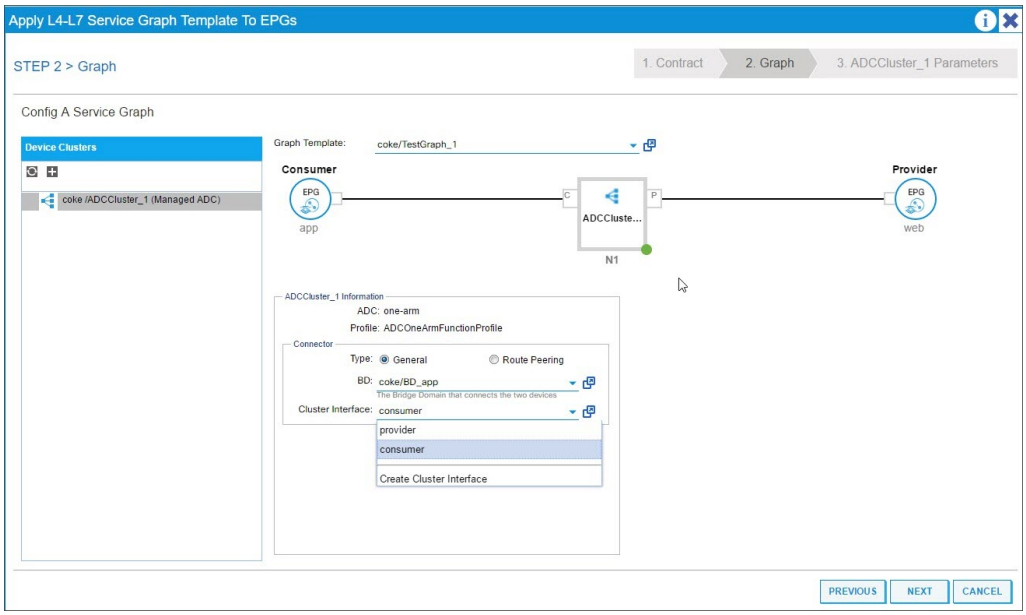
f) 在“ 连接器”部分，执行以下操作：

i. 在 类型字段中，选择常规。

ii. 在 **BD** 下拉列表中，选择网桥域。连接器详细信息属于包含在 Cisco APIC 基础结构模型中的桥接域的一部分。

iii. 在 **Cluster Interface**（群集接口）下拉列表中，为所选桥接域选择适当的群集接口。

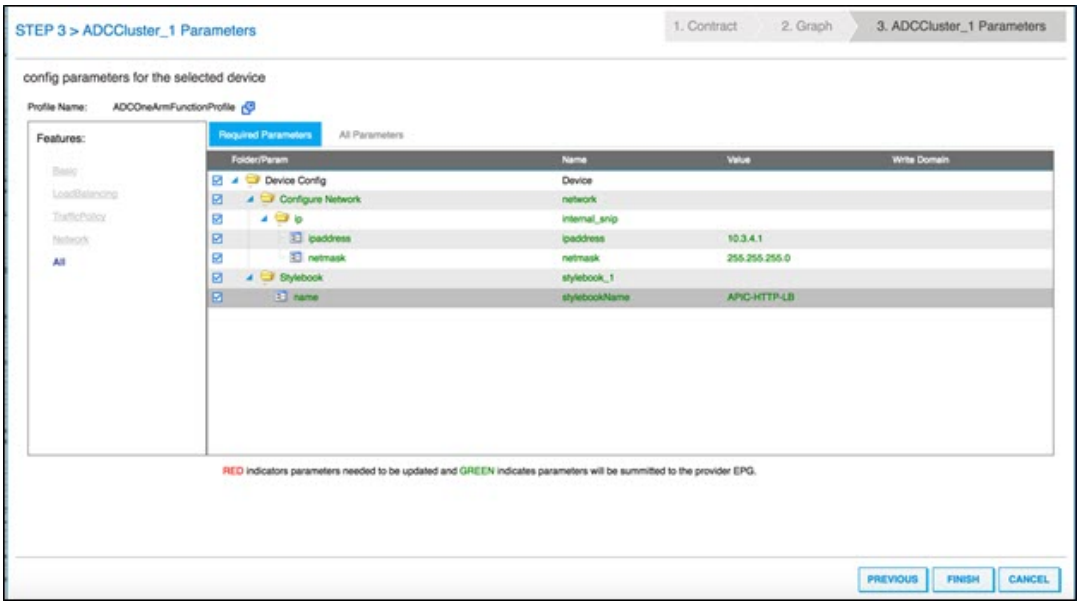
Cisco APIC 根据所选服务图模板的要求，将选定的网桥域用于 Citrix ADC 设备与结构之间的数据路径流量。



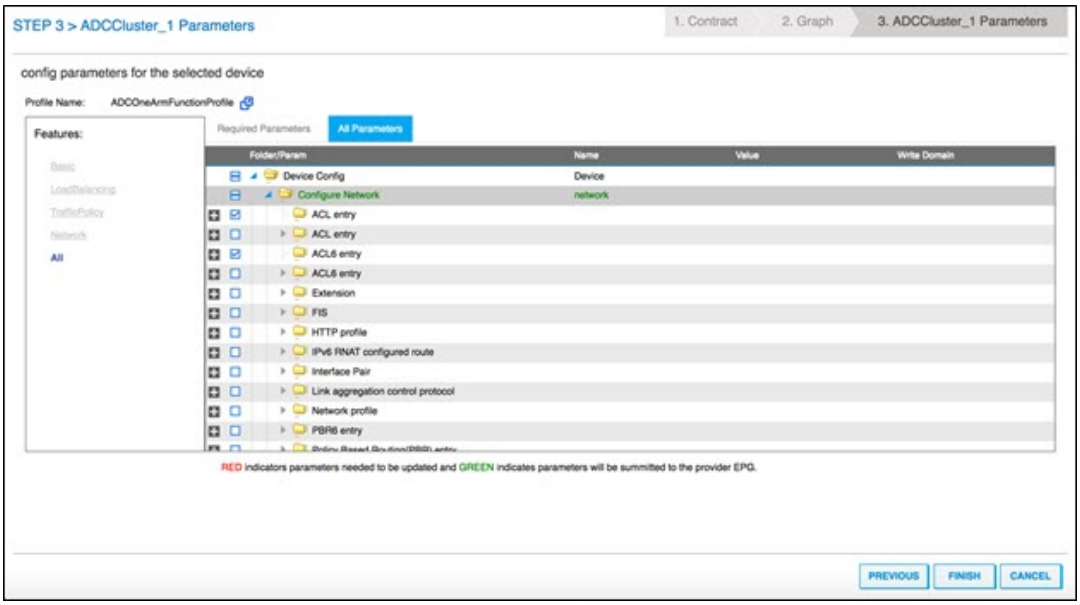
iv. 单击“ 下一步”。

在“参数”屏幕上的“必需参数”选项卡上，输入 L2-L3 的特定详细信息，如配置文件规定的 IP 地址。其他主要参数是样书名称。它可以是 Citrix **Application Delivery Management (ADM)** 中提供的内置样书 **APIC-HTTP-LB**，也可以提供在 使用 Citrix ADM 为应用程序创建样书

> 注意
>
> 样书名称将服务图形详细信息与使用 Citrix ADM 为给定应用程序创建的 L4-L7 配置链接起来。



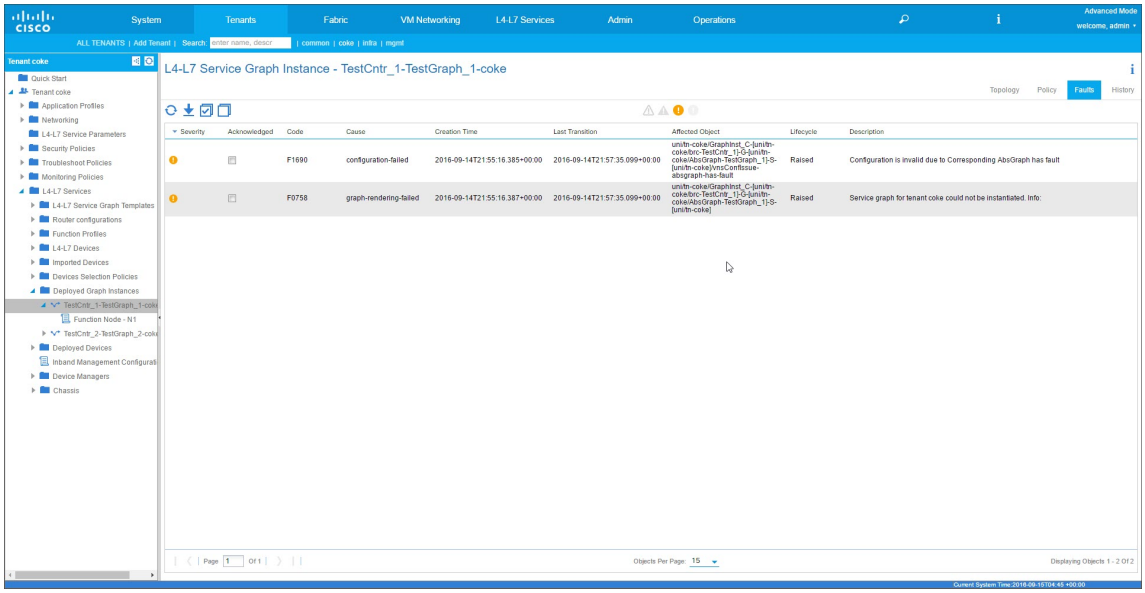
Cisco APIC GUI 允许根据功能（例如负载平衡）过滤参数。可以在 **Required Parameters**（所需参数）选项卡中查看和设置所有必要参数，可以在 **All Parameters**（所有参数）选项卡中查看和设置与功能有关的所有其他参数。



> 注意
>
> 默认情况下，内置单臂配置文件要求提供 SNIP 详细信息，例如 IP 地址和网络掩码。可以在 Cisco APIC GUI 中单击 **All Parameters**（所有参数）并展开 **Configure Network**（配置网络）树来查看其他网络连接参数。这将列出 Citrix ADC 支持的所有网络参数。可以从 Cisco APIC GUI 实例化任何实体，并为列出的属性提供值。

6. 单击完成。

> 重要
>
> 应用服务图模板后，请确保部署的图形中没有故障。您可以通过单击“ 工作”窗格中的“ 故障”选项卡查看错误。



作为服务图形部署的一部分，混合模式设备包将配置详细信息从 Cisco APIC 推送到 Citrix ADM。Citrix ADM 在内部将这些配置处理到相应的 Citrix ADC，并将响应返回到 APIC。成功的图形部署将没有任何故障，并且 Citrix ADC 已成功地与相应图形的结构联网。

APIC 支持使用 API 以不同的方法来配置和部署图形，图形部署包括对 APIC 特定的一些构造的依赖项，例如租户、合同、虚拟 LAN 和命名空间。

下面的示例方法说明了其中一个方法，即利用 APIC 的 API 来创建和部署 L4-L7 图，假定已在 APIC 中配置 APIC 特定的工件。

> 重要
>
> 请务必将这些 XML 有效负载用作参考，并在您的环境中使用 XML 之前对其进行适当的更改。

下面是一个使用 API 创建和部署服务图的示例：

a) 创建 AppProfile

b) 创建服务图详细信息

c) 将服务图附加到合同

下面是一个用于创建 AppProfile 的示例 XML 有效负载。应用程序配置文件包含 EPG，提供程序 EPG 包含 Citrix ADC 特定的实体、属性及其值。在以下示例 XML 有效负载中，使用一组属性和样书名称创建 Citrix ADC 特定的网络实体（如 NSIP）。

```
<polUni>
    <fvTenant name="coke">
        <!-- Application Profile -->
        <fvAp dn="uni/tn-coke/ap-sap" name="sap">
            <!-- EPG 1  -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-web" name="web">
                <fvRsBd tnFvBDName="BD_web" />
                <!-- --------- CONFIG PAYLOAD ---------------- -->
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Network" name=
    "Network">
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip1">
                        <vnsParamInst key="ipaddress" name="ip1"
    value="110.110.110.2"/>
                        <vnsParamInst key="netmask" name="netmask1
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
                    <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="nsip" name="
    snip2">
                        <vnsParamInst key="ipaddress" name="ip2"
    value="220.220.220.2"/>
                        <vnsParamInst key="netmask" name="netmask2
    " value="255.255.255.0"/>
                        <vnsParamInst key="type" name="tye" value=
    "SNIP"/>
                        <vnsParamInst key="dynamicrouting" name="
    dynamicrouting" value="DISABLED"/>
                        <vnsParamInst key="hostroute" name="
    hostroute" value="DISABLED"/>
                    </vnsFolderInst>
```



```
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="Stylebook"
    name="stylebook_1">
                    <vnsParamInst name="stylebookName" key="name"
    value="APIC-HTTP-LB"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    internal_network" name="internal_network">
                    <vnsCfgRelInst name="internal_network_key" key
    ="internal_network_key" targetName="Network/snip1"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="
    external_network" name="external_network">
                    <vnsCfgRelInst name="external_network_key" key
    ="external_network_key" targetName="Network/snip2"/>
                </vnsFolderInst>
                <vnsFolderInst ctrctNameOrLbl="Ctrct1"
    graphNameOrLbl="Graph1" nodeNameOrLbl="ADC" key="mFCngStylebook
    " name="mFCngStylebook_1">
                    <vnsCfgRelInst name="Stylebook_key" key="
    Stylebook_key" targetName="stylebook_1"/>
                </vnsFolderInst>
                <!-- ------- END CONFIG PAYLOAD -------------- -->
                <fvSubnet ip="110.110.110.110/24" scope="shared"/>
                <fvRsProv tnVzBrCPName="Ctrct1"></fvRsProv>
                <fvRsDomAtt tDn="uni/phys-sepg" />
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/38]" encap="vlan-3703" instrImedcy="immediate"/>
            </fvAEPg>
            <!-- EPG 2 -->
            <fvAEPg dn="uni/tn-coke/ap-sap/epg-app"  name="app">
                <fvRsCons tnVzBrCPName="Ctrct1"/>
                <fvRsBd tnFvBDName="BD_app" />
                <fvSubnet ip="220.220.220.220/24" scope="shared"/>
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep
    -[eth1/37]" encap="vlan-3704" instrImedcy="immediate"/>
                <fvRsDomAtt tDn="uni/phys-sepg" />
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```


下面是一个用于创建服务图详细信息的示例 XML 有效负载：

```
<polUni>
    <fvTenant name="coke">
        <vnsAbsGraph name = "Graph1">
            <vnsAbsTermNodeProv name = "Input1">
                <vnsAbsTermConn name = "C1"></vnsAbsTermConn>
            </vnsAbsTermNodeProv>
            <vnsAbsNode name="ADC" funcType="GoTo">
                <vnsAbsFuncConn name = "outside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-external" />
                </vnsAbsFuncConn>
                <vnsAbsFuncConn name = "inside" attNotify="true">
                    <vnsRsMConnAtt tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction/mConn-internal" />
                </vnsAbsFuncConn>
                <vnsRsNodeToMFunc tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/mFunc-ADCFunction"/>
                <vnsRsDefaultScopeToTerm tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/outtmnl"/>
                <vnsRsNodeToAbsFuncProf tDn="uni/infra/mDev-Citrix-NetScalerMAS-1.0/absFuncProfContr/absFuncProfGrp-ADCOneArmServiceProfileGroup/absFuncProf-ADCOneArmFunctionProfile"/>
                <vnsRsNodeToLDev tDn="uni/tn-coke/lDevVip-ADCCluster1"/>
            </vnsAbsNode>
            <vnsAbsTermNodeCon name = "Output1">
                <vnsAbsTermConn name = "C6"></vnsAbsTermConn>
            </vnsAbsTermNodeCon>
            <vnsAbsConnection name = "CON1">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeCon-Output1/AbsTConn" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-outside" />
            </vnsAbsConnection>
            <vnsAbsConnection name = "CON2">
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsNode-ADC/AbsFConn-inside" />
                <vnsRsAbsConnectionConns tDn="uni/tn-coke/AbsGraph-Graph1/AbsTermNodeProv-Input1/AbsTConn" />
            </vnsAbsConnection>
```

```
        </vnsAbsGraph>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

下面是一个用于将服务图附加到合同的示例 XML 有效负载：

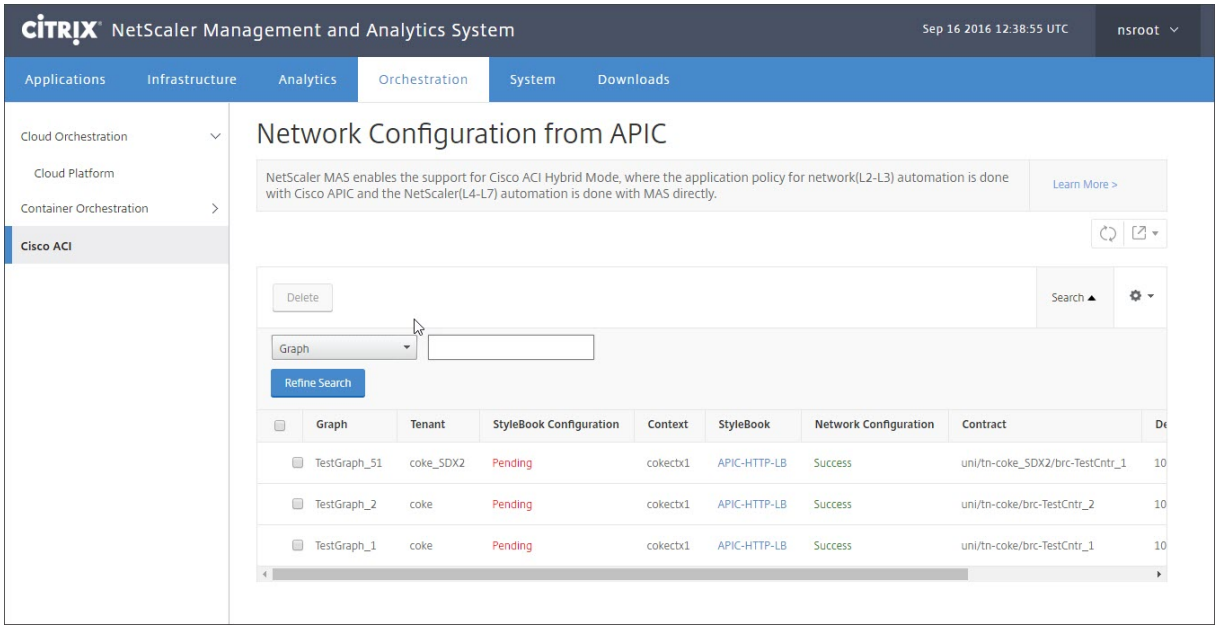
```
<polUni>
    <fvTenant name="coke">
        <vzBrCP name="Ctrct1">
            <vzSubj name="http">
                <vzRsSubjGraphAtt tnVnsAbsGraphName="Graph1"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
<!--NeedCopy-->
```

使用样书配置来自 **Citrix ADM** 的 **L4-L7** 参数

April 23, 2021

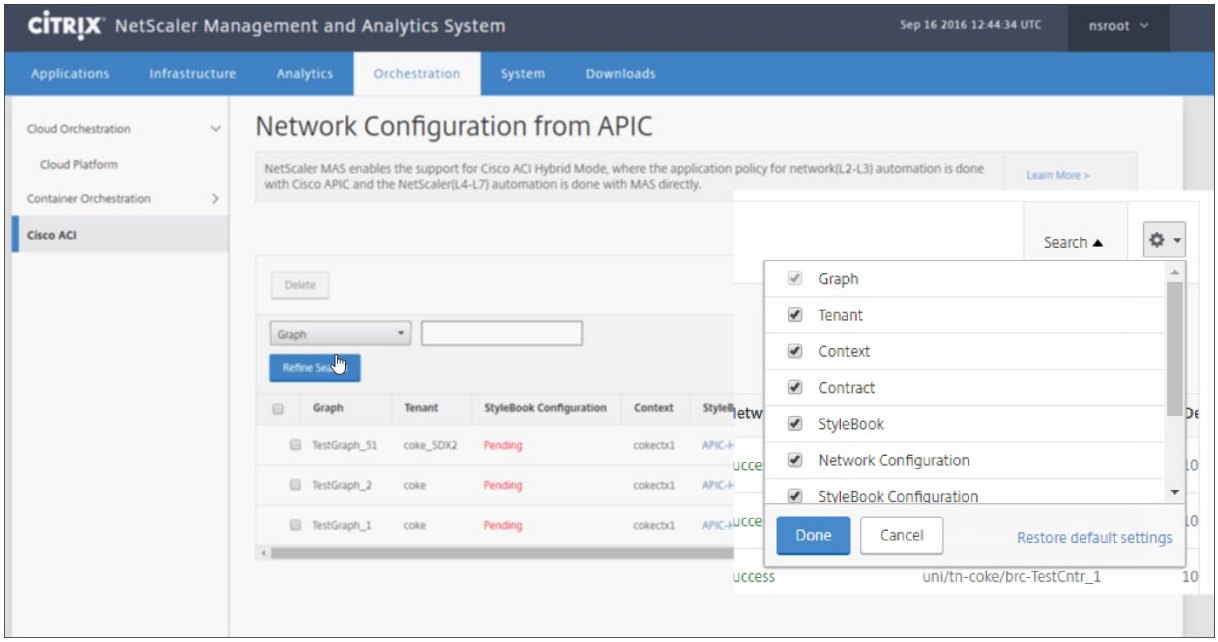
May 24, 2018

在 Citrix Application Delivery Management (ADM) 中，您可以在 “业务 流程” 选项卡上的 C **isco ACI** 下查看已部署的服务图表详细信息。表格视图中显示服务图详细信息，例如图形名称、租户名称、上下文、样书名称及网络配置状态。



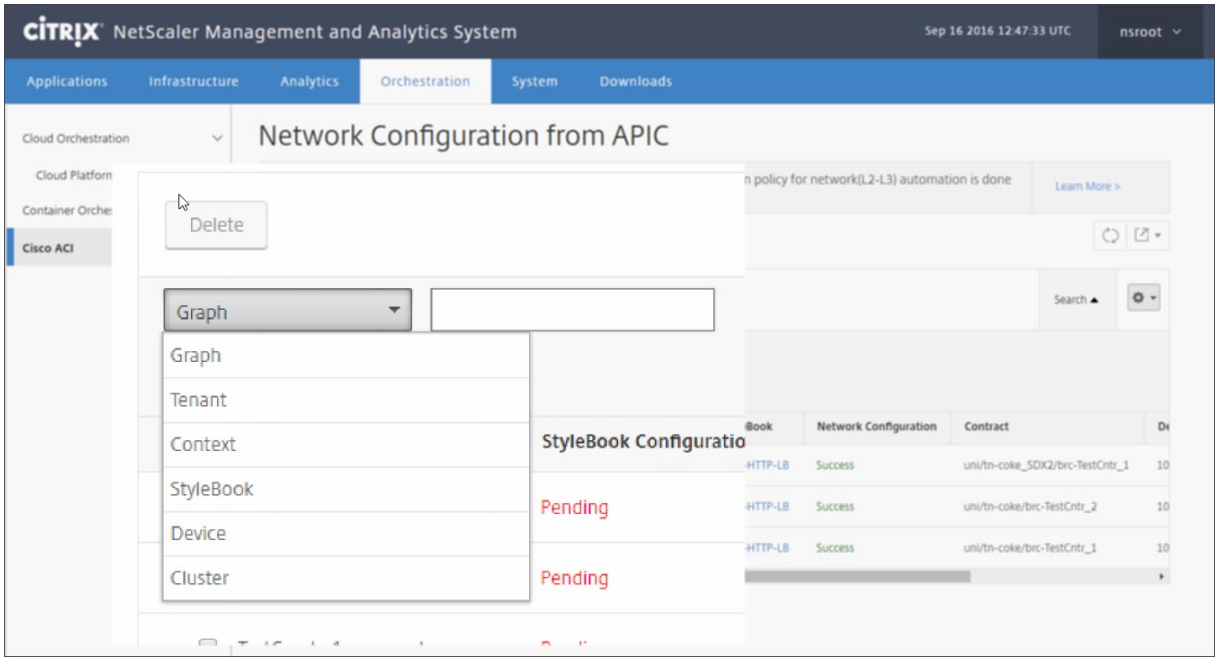
> 注意
>
> 如果从 Cisco APIC 删除了图形，对应的配置将从设备中删除，包括 L4-L7 配置。

此外，表格视图允许您对表中显示的任何列进行排序，以及使用 “Search”（搜索）选项过滤数据。还可以从列的下拉列表中选择或取消选择列名来自定义列详细信息：



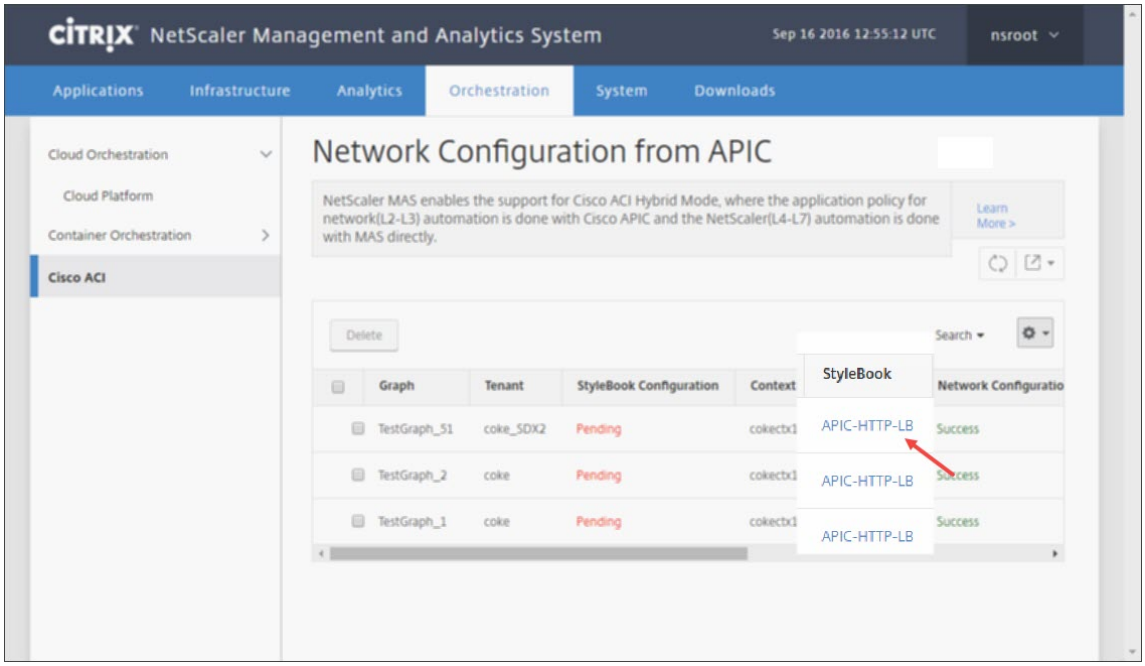
此外，可以单击 **Search**（搜索）按钮并使用搜索选项来过滤数据。可以从下拉框中选择任何列并输入对应的值来过滤表中显示的数据。

> 注意
>
> 搜索功能区分大小写，您必须提供精确的搜索条件。

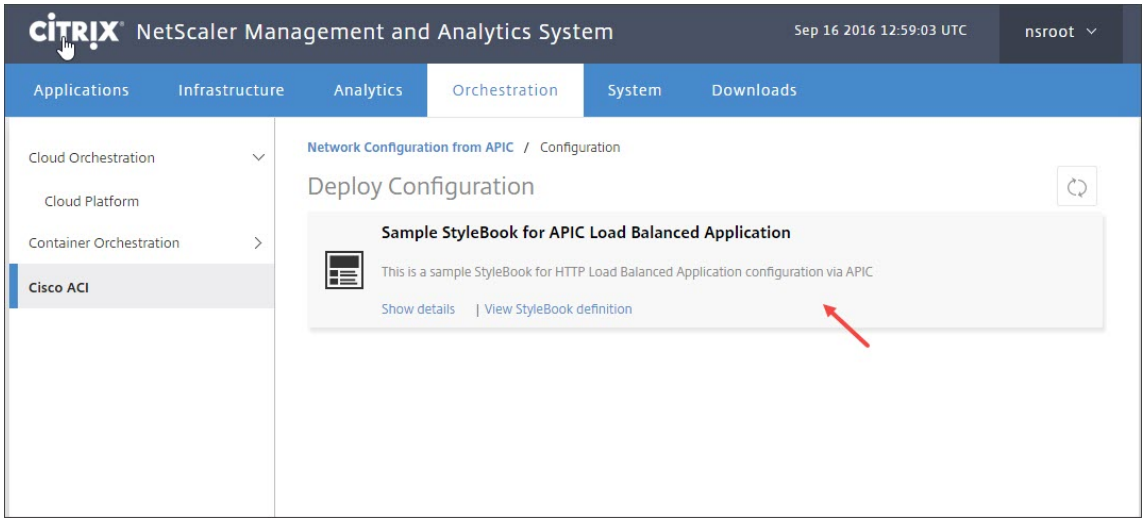


要在 Citrix ADM 中使用样书部署 L4-L7 配置，请执行以下操作：

1. 单击在表格视图中显示为 URL 的样书名称。



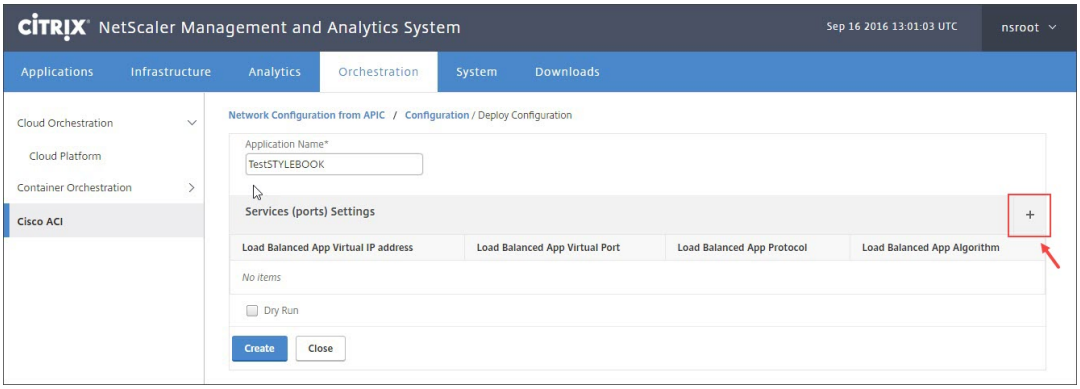
2. 在“配置”窗口中，双击 样书。



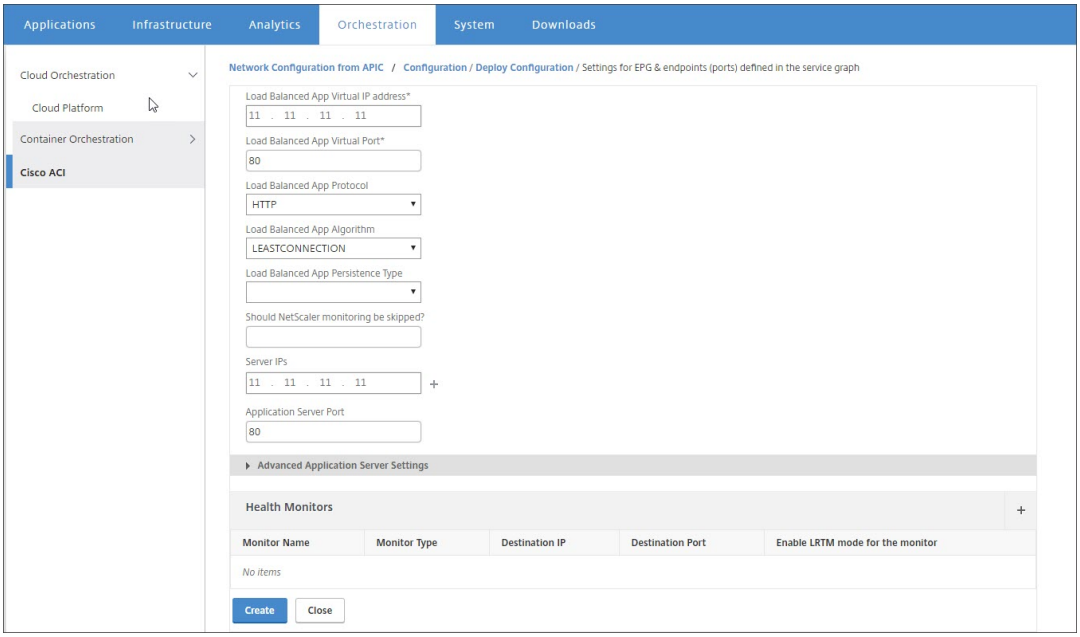
3. 在 “Deploy Configuration”（部署配置）窗口中，执行以下操作：

   a) 在 **Application Name**（应用程序名称）字段中，输入与 APIC 中应用程序的服务图对应的 ADC 功能配置的名称。

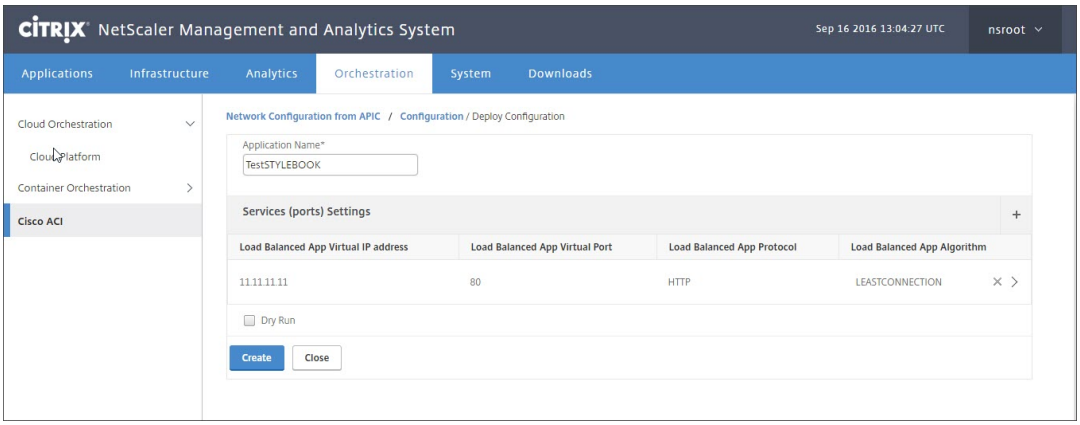
   b) 在 “Service (ports) Settings”（服务 (端口) 设置）部分，单击 **+**。



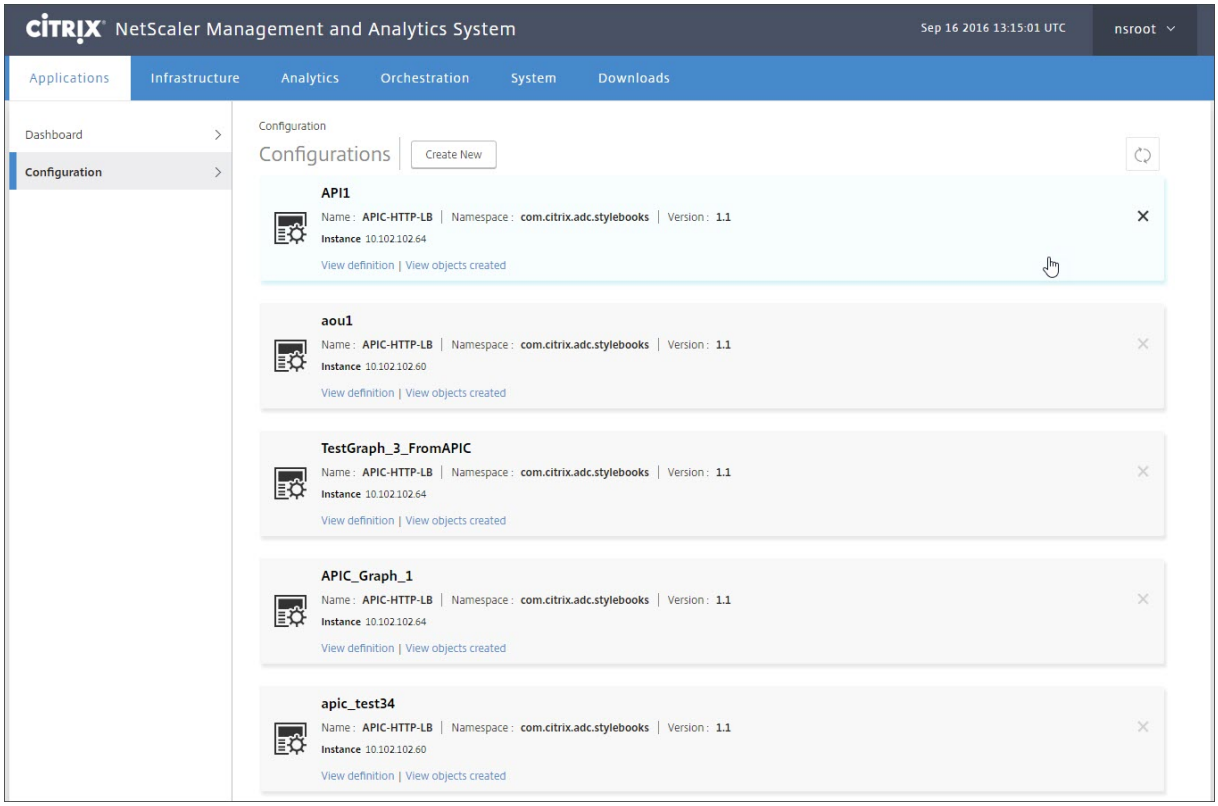
   c) 在 服务图形窗口中定义的 **EPG** 和端点（端口）的设置中，输入从样书填充的参数值，然后单击 创建。



d) 单击创建。



在 Citrix ADM 中部署样书中指定的 L4-L7 配置。可以导航到 **Application**（应用程序）**> Configuration**（配置），在 **Application**（应用程序）选项卡中查看样书配置。



从 **APIC** 附加和分离端点事件

April 23, 2021

混合模式解决方案隐式处理 Cisco APIC 中的附加或分离端点事件。当 Cisco APIC 触发连接终端节点事件时，Citrix Application Delivery Management (ADM) 中的样书会自动触发服务组服务组成员绑定，并且在分离终端节点事件期间解除绑定。

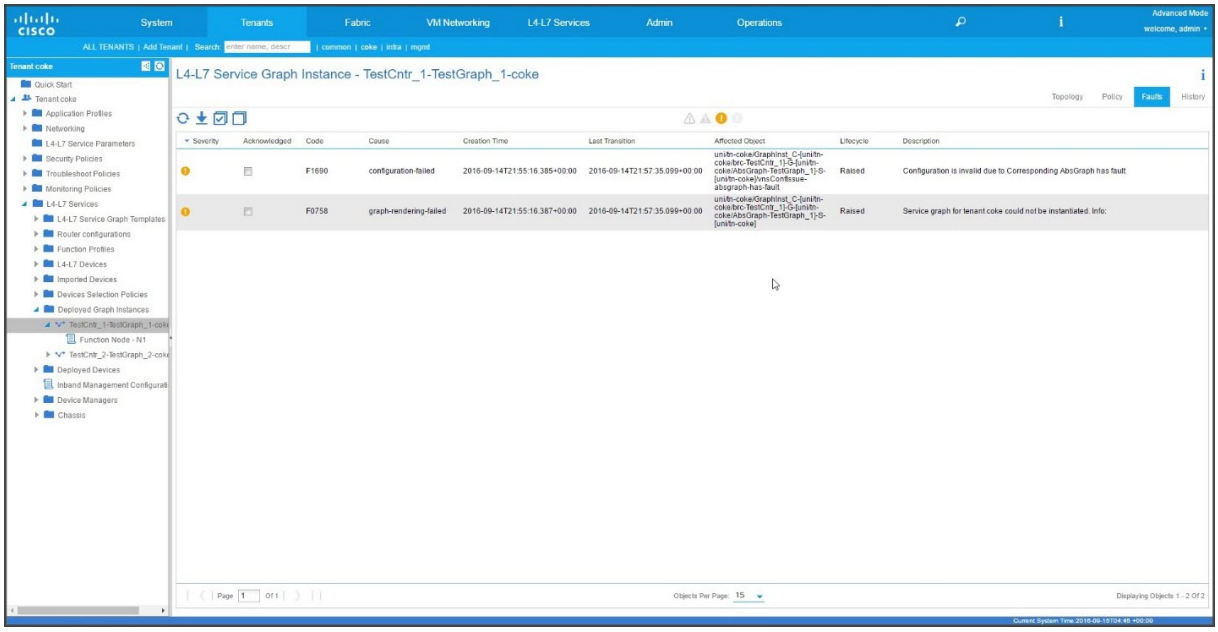
此外，如果在 Cisco APIC 中触发连接或分离终端节点事件之前尚未在 Cisco ADM 中部署 L4-L7 配置，则解决方案将在数据库中保留连接 IP 地址。在通过样书创建了服务组后，这些 IP 地址被绑定到对应的服务组。

APIC 故障报告

April 23, 2021

在 Cisco ACI 中部署 Citrix ADC 设备包时，思科 APIC 会报告任何故障。可以查看 APIC 任何级别（例如，设备、租户、EPG 或服务图）的故障报告。下面的屏幕截图显示了设备级别的故障报告。有关故障的更多信息，请参阅 http://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/1-x/faults/guide/b_APIC_Faults_Errors/b_IFC_Faults_Errors_chapter_01.html。

选择任何 APIC 实体并单击 **Faults**（故障）选项卡可显示 APIC 针对该实体报告的故障。



由 **Citrix ADM** 生成的日志

April 23, 2021

Citrix Application Delivery Management (ADM) 提供了大量的日志记录，可帮助解决问题。生成的日志 (**admin.log**) 位于：**/var/controlcenter/log/**

您可以登录到 Citrix ADM，然后使用命令行管理程序导航到 Citrix ADM 目录结构。以下是用于 APIC 图形部署的 Citrix ADM 日志的示例片段。

```
    2016-06-29 10:58:33,816 DEBUG APIC Config  = {
(0, '', 5230): {
'dn': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'state': 1, 'transaction': 0, 'ackedstate': 0, 'tenant': 'coke_SDX2', 'ctxName': 'cokectx1', 'value': {
(10, '', 'ADCHybridMode_1_Consumer_1'): {
'state': 1, 'transaction': 0, 'cifs': {
'ADCHybridMode_1_Device_1': '1_1' }
, 'ackedstate': 0 }
, (7, '', '2129920_32778'): {
'state': 1, 'tag': 273, 'type': 1, 'ackedstate': 0, 'transaction': 0 }
, (1, '', 5790): {
'transaction': 0, 'ackedstate': 0, 'value': {
(3, 'ADCFunction', 'N1'): {
```



```
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'mFCngNetwork', 'mFCngnetwork'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Network_key', 'network_key'): {
'state': 1, 'transaction': 0, 'target': 'network', 'ackedstate': 0 }
 }
 }
, (4, 'internal_network', 'internal_network'): {
'connector': 'provider', 'state': 1, 'transaction': 0, 'ackedstate':
   0, 'value': {
(6, 'internal_network_key', 'internal_network_key'): {
'state': 1, 'transaction': 0, 'target': 'network/internal_snip', '
   ackedstate': 0 }
 }
 }
, (2, 'external', 'consumer'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': '
   ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
, (4, 'mFCngStylebook', 'mFCngStylebook'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(6, 'Stylebook_key', 'Stylebook_key'): {
'state': 1, 'transaction': 0, 'target': 'stylebook_1', 'ackedstate': 0
    }
 }
 }
, (2, 'internal', 'provider'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(9, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'target': '
   ADCHybridMode_1_Consumer_1_2129920_32778', 'ackedstate': 0 }
 }
 }
 }
 }
 }
, 'state': 1, 'absGraph': 'HybridModeGraph_1', 'rn': u'vGrp-[uni/tn-
   coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-
   coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, (4, 'Network', 'network'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(4, 'nsip', 'internal_snip'): {
```



```
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'type', 'type'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'SNIP' }
, (5, 'hostroute', 'hostroute'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'DISABLED' }
, (5, 'ipaddress', 'ipaddress'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '10.1.1.1' }
, (5, 'dynamicrouting', 'dynamicRouting'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'ENABLED' }
, (5, 'netmask', 'netmask'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': '255.255.255.0
   ' }
 }
 }
 }
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'state': 1, 'transaction': 0, 'vif': 'ADCHybridMode_1_Consumer_1', '
   ackedstate': 0, 'encap': '2129920_32778' }
, (4, 'Stylebook', 'stylebook_1'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
    }
 }
 }
 }
, 'txid': 10000 }
 }

   2016-06-29 10:58:33,816 DEBUG get Graph Return details = {
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[
   uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-
   coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-
   HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', '
   graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', '
   graphInstanceId': 5790 }

   2016-06-29 10:58:33,827 DEBUG SUCCESS created track 2.0
   2016-06-29 10:58:33,833 DEBUG SUCCESS updated track with new task 2
   2016-06-29 10:58:33,851 DEBUG SUCCESS updated track with new task 1
   2016-06-29 10:58:33,867 DEBUG fn_wrapper:long_operation_thread_id:<
      eventlet.greenthread.GreenThread object at 0x80aa5c7d0>
```



```
87      2016-06-29 10:58:33,867 DEBUG +++++++ Service Audit Call for Device
            Details  = 10.102.102.62 +++++++++++++++++
88      2016-06-29 10:58:33,867 DEBUG Inside APIC Cred Col If = 2
89      2016-06-29 10:58:33,867 DEBUG Host name from device =
           ADCHybridMode_1
        "InProgress","message":null,"replication_status":"","target":"
           10.102.102.81","operation":"POST","entity_type":"apic","
           entity_id":null }
91    }
92
93      2016-06-29 10:58:44,141 DEBUG  Save config  Response = {
94    "errorcode": 0, "message": "Done", "severity": "NONE"  }
95
96      2016-06-29 10:58:44,141 DEBUG +++++++++ getContextAwareFlag = True
97      2016-06-29 10:58:44,141 DEBUG +++++ get context tenant name from
           Config ++++++
98      2016-06-29 10:58:44,141 DEBUG +++++ getContextTenantName = {
99    'state': 1, 'ctxName': 'cokectx1', 'tenant': 'coke_SDX2', 'vdev': 5230
          }
100   ++++++
101     2016-06-29 10:58:44,142 DEBUG Service health details = {
102   }
103   collection length = 0
104     2016-06-29 10:58:44,142 DEBUG Count details Total = 0 Up = 0 Down =
            0
105     2016-06-29 10:58:44,142 DEBUG Health Score details Up = 0
106     2016-06-29 10:58:44,142 DEBUG Service HEALTH final collection  = {
107   ((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')): {
108   'faults': [], 'state': 0, 'health': ([(0, '', 5230), (1, '', 5790),
          (3, 'ADCFunction', 'N1')], 0) }
109   }
110
111     2016-06-29 10:58:44,142 DEBUG ++++++getServiceHealth Fault List =
           []
112     2016-06-29 10:58:44,142 DEBUG Service HEALTH final response  = {
113   'devs': 'ADCHybridMode_1_Device_1', 'faults': [], 'state': 0, 'health'
          : [([(0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1')], 0)] }
114
115     2016-06-29 10:58:44,236 DEBUG RESPONSE from NSLOGOUT = {
116   "errorcode": 0, "message": "Done", "severity": "NONE"  }
117   , sessionId = ##
          D2EAFA7CFCD73119E6C5E78D8BCB2E842829C971C1DC7E99850949DAE0029F2191B5E7EDF2764
118     2016-06-29 10:58:44,237 DEBUG +++++ Faults respCol   = {
119   '10.102.102.62': {
```



```
'10.102.102.62': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
    u'NONE', 'operation_name': 'add_op' }
 }
, (7, '', '2129920_32778'): {
'vlan': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
    u'NONE', 'operation_name': 'add_op' }
 }
, (((0, '', 5230), (1, '', 5790), (3, 'ADCFunction', 'N1'), (2, '
   internal', 'provider')), 'nsip'): {
'vlan_nsip_binding': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
    u'NONE', 'operation_name': 'bind_op' }
 }
, (((0, '', 5230), (4, 'Network', 'network')), (4, 'nsip', '
   internal_snip')): {
'nsip': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
    u'NONE', 'operation_name': 'add_op' }
 }
, (): {
 }
, (8, '', 'ADCHybridMode_1_Consumer_1_2129920_32778'): {
'vlan_interface_binding': {
u'errorcode': 0, 'status_code': 201, u'message': u'Done', u'severity':
    u'NONE', 'operation_name': 'bind_op' }
 }
 }

   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
       = Done, statusCode = add_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
       = Done, statusCode = add_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = bind_op,
      erMsg = Done, statusCode = bind_op
   2016-06-29 10:58:44,237 DEBUG Fault details oprName = add_op, erMsg
       = Done, statusCode = add_op
   2016-06-29 10:58:44,238 DEBUG Fault details oprName = bind_op,
      erMsg = Done, statusCode = bind_op
   2016-06-29 10:58:44,238 DEBUG ++++++++++++++ ServiceAudit response
      = {
'faults': [], 'state': 0, 'health': [] }

   2016-06-29 10:58:44,238 DEBUG APIC Graph Details = {
```



```
'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', (1, '', 5790): {
'state': 1, 'graphrn': u'vGrp-[uni/tn-coke_SDX2/GraphInst_C-[uni/tn-coke_SDX2/brc-TestCntr_3]-G-[uni/tn-coke_SDX2/AbsGraph-HybridModeGraph_1]-S-[uni/tn-coke_SDX2]]' }
, 'tenantName': 'coke_SDX2', 'StyleBookName': 'APIC-HTTP-LB', 'graphInstanceName': 'HybridModeGraph_1', 'context': 'cokectx1', 'graphInstanceId': 5790 }

    2016-06-29 10:58:44,242 DEBUG Journal Processing: Database task: create apic_graph
    2016-06-29 10:58:44,264 DEBUG SUCCESS created task 2
    2016-06-29 10:58:44,269 DEBUG SUCCESS updated track with new task 2
    2016-06-29 10:58:44,308 DEBUG +++++++ get IP and Connector collection from Config with type 22 for attach & detach event ++++++
    2016-06-29 10:58:44,308 DEBUG ----- connector with IP List = {
0: [], 1: [], 3: [] }

    2016-06-29 10:58:44,308 DEBUG ----- attachIpList = [] dettachIpList = []
    2016-06-29 10:58:44,308 DEBUG ----- In _attachDettachIps attachIpList = [] dettachIpList = []
    2016-06-29 10:58:44,312 DEBUG ----- In _attachDettachIps row = {
'deviceIP': u'10.102.102.62', 'responseToAPIC': None, 'graphDN': u'uni/vDev-[uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1]-tn-[uni/tn-coke_SDX2]-ctx-cokectx1', 'apicGraphState': None, 'serviceGroupName': None, 'configPackId': None, 'tenantName': u'coke_SDX2', 'styleBookName': u'APIC-HTTP-LB', 'graphInstanceName': u'HybridModeGraph_1', 'context': u'cokectx1', 'serviceGroupPort': None, 'graphInstanceId': 5790, 'createDate': None, 'serviceGroupIP': None }

<!--NeedCopy-->
```

混合模式设备包生成的日志

April 23, 2021

Citrix ADC 混合模式设备包生成与配置相关的日志和监视相关的日志。生成的日志位于 **/data/devicescript/Citrix.NetScalerMAS.1.0/logs**。

下面是 Cisco APIC 的 **debug.log** 的示例代码段：


```
    2016-06-28 03:06:53.879767 DEBUG Thread-20 18723 [10.102.102.62,
       24063] Device manager details ip = 10.102.102.81, port = 80
    2016-06-28 03:06:53.879856 DEBUG Thread-20 18724 [10.102.102.62,
       24063] ++++++++++++++ serviceAudit  request ++++++++++++++++
    2016-06-28 03:06:53.879929 DEBUG Thread-20 18725 [10.102.102.62,
       24063] ++++++++++ getStyleBookObjects ++++++++++++
    2016-06-28 03:06:53.879995 DEBUG Thread-20 18726 [10.102.102.62,
       24063] NMAS collection A3 = (4, 'Stylebook', 'stylebook_1') B3 =
        {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': {
(5, 'name', 'stylebookName'): {
'state': 1, 'transaction': 0, 'ackedstate': 0, 'value': 'APIC-HTTP-LB'
    }
 }
 }

    2016-06-28 03:06:53.880045 DEBUG Thread-20 18727 [10.102.102.62,
       24063] NMAS collection styleBookName= APIC-HTTP-LB
    2016-06-28 03:06:53.880093 DEBUG Thread-20 18728 [10.102.102.62,
       24063] NMAS collection retCol= {
'Stylebook': 'APIC-HTTP-LB', 'tuple': ((0, '', 5230), (4, 'Stylebook',
    'stylebook_1')) }

    2016-06-28 03:06:53.880140 DEBUG Thread-20 18729 [10.102.102.62,
       24063]  ++++ devMgrStyleBookUrl = http://10.102.102.81/stylebook
       /nitro/v1/config/stylebooks/com.citrix.adc.stylebooks/1.1/APIC-
       HTTP-LB
    2016-06-28 03:06:54.135240 DEBUG Thread-20 18730 [10.102.102.62,
       24063]  ++++ Response from styleBookresCode serviceAudit = {
u'stylebook': {
u'uses_builtin_namespaces': {
u'netscaler.nitro.config': u'10.5' }
, u'name': u'APIC-HTTP-LB', u'used_by_stylebooks': [], u'namespace': u
   'com.citrix.adc.stylebooks', u'source': u'---\nname: APIC-HTTP-LB\
   nnamespace: com.citrix.adc.stylebooks\nversion: "1.1"\ndisplay-name
   : "Sample StyleBook for APIC Load Balanced Application"\
   ndescription: "This is a sample StyleBook for HTTP Load Balanced
   Application configuration via APIC"\nschema-version: "1.0"\nimport-
   stylebooks: \n  - \n    namespace: netscaler.nitro.config\n
   prefix: ns\n    version: "10.5"\n  - \n    namespace: "com.citrix.
   adc.stylebooks"\n    prefix: "stlb"\n    version: "1.1"\nparameters
   -default-sources:\n  - stlb::APIC-ROOT\nsubstitutions:\n  lb-name(
   appname, port): $appname + "-" + str($port) + "-lb"\n  sg-name(
   appname, port): $appname + "-" + str($port) + "-sg"\n
```



```
        healthmonitor[]:\n    true: "NO"\n    false: "YES"\ncomponents: \n
         - \n    name: lbvserver\n    type: ns::lbvserver\n    repeat:
        $parameters.app-services\n    repeat-item: app\n    properties: \
        n      name: $substitutions.lb-name($parameters.appname, $app.
        virtual-port)\n      ipv46: $app.virtual-ip\n      port: $app.
        virtual-port\n      servicetype: $app.protocol\n      lbmethod?:
        $app.algorithm\n      persistencetype?: $app.persistence\n  - \n
         name: svcgrp\n    type: ns::servicegroup\n    repeat: $parameters.
        app-services\n    repeat-item: app\n    properties: \n      name:
        $substitutions.sg-name($parameters.appname, $app.virtual-port)\
        n      servicetype: $app.protocol\n      useproxyport?: $app.sg-
        advanced.useproxyport\n      usip?: $app.sg-advanced.usip\n
        cip?: $app.sg-advanced.cip\n      cipheader?: $app.sg-advanced.
        cipheader\n      healthmonitor?: $substitutions.healthmonitor($app.
        skip_healthmonitor)\n    components: \n      -\n        name:
        lbvserver-svg-binding\n        type: ns::
        lbvserver_servicegroup_binding\n        properties: \n
        name: $substitutions.lb-name($parameters.appname, $app.virtual-port
        )\n          servicegroupname: $parent.properties.name\n      - \
        n        name: svg-members\n        type: ns::
        servicegroup_servicegroupmember_binding\n        condition: $app.
        server-ips\n        repeat: $app.server-ips\n        repeat-item:
        serverip\n        properties: \n          ip: $serverip\n
        port: $app.server-port\n          servicegroupname: $parent.
        properties.name\noutputs: \n  - \n    name: lbvservers\n    value:
        $components.lbvserver\n  - \n    name: servicegroups\n    value:
        $components.svcgrp', u'version': u'1.1', u'uses_stylebooks': [{
21  u'version': u'1.1', u'namespace': u'com.citrix.adc.stylebooks', u'name
        ': u'APIC-ROOT' }
22  ] }
23   }
24
25      2016-06-28 03:06:54.359142 DEBUG Thread-20 18731 [10.102.102.62,
           24063]  ++++ Dev Mgr request details devMgrUrl = http://
           10.102.102.81/admin/v1/apic
26      2016-06-28 03:06:54.359221 DEBUG Thread-20 18732 [10.102.102.62,
           24063]  ++++ Response from Device Mgr serviceAudit = {
27  "APIC":[] }
28
29      2016-06-28 03:06:54.359266 DEBUG Thread-20 18733 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response = {
30  "APIC":[] }
31
32      2016-06-28 03:06:54.359306 DEBUG Thread-20 18734 [10.102.102.62,
           24063] ++++++++++++++ serviceAudit response headers content type
```



```
          = application/json; charset=utf-8
33      2016-06-28 03:06:54.359394 DEBUG Thread-20 18735 [10.102.102.62,
          24063] ++++++++++++++ serviceAudit response headers = {
34  'content-length': '11', 'job_id': 'ctxt-f4db2883-e42c-4262-a35f-04628
      c4ad5ea', 'x-content-type-options': 'nosniff', 'transfer-encoding':
       'chunked', 'connection': 'close', 'date': 'Wed, 29 Jun 2016
      10:58:33 GMT', 'x-frame-options': 'SAMEORIGIN', 'content-type': '
      application/json; charset=utf-8' }
35
36      2016-06-28 03:06:54.359480 DEBUG Thread-20 18736 [10.102.102.62,
          24063] ++++++++++++++ pollingURL = http://10.102.102.81/admin/v1
          /journalcontexts/ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea
37      2016-06-28 03:06:54.359713 DEBUG Thread-20 18737 [10.102.102.62,
          24063] ++++++++++++++ pollingStatus = True, pollingTime = 0
38      2016-06-28 03:06:54.483228 DEBUG Thread-20 18738 [10.102.102.62,
          24063] ++++++++++++++ pollingResponse json = {
39  u'journalcontext': {
40  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
       u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': None, u'
      target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
      -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
41   }
42
43      2016-06-28 03:07:04.493074 DEBUG Thread-20 18739 [10.102.102.62,
          24063] ++++++++++++++ pollingStatus = True, pollingTime = 1
44      2016-06-28 03:07:04.587595 DEBUG Thread-20 18767 [10.102.102.62,
          24063] ++++++++++++++ pollingResponse json = {
45  u'journalcontext': {
46  u'status': u'In Progress', u'scopes': [], u'entity_id': None, u'name':
       u'Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
      service_name': u'admin', u'start_time': u'2016-06-29T10
      :58:33.760565', u'is_default': u'false', u'end_time': None, u'
      target': u'10.102.102.81', u'message': None, u'id': u'ctxt-f4db2883
      -e42c-4262-a35f-04628c4ad5ea', u'replication_status': u'' }
47   }
48
49      2016-06-28 03:07:14.597812 DEBUG Thread-20 18790 [10.102.102.62,
          24063] ++++++++++++++ pollingStatus = True, pollingTime = 2
50      2016-06-28 03:07:14.692590 DEBUG Thread-20 18791 [10.102.102.62,
          24063] ++++++++++++++ pollingResponse json = {
51  u'journalcontext': {
52  u'status': u'Finished', u'scopes': [], u'entity_id': None, u'name': u'
      Create apic', u'operation': u'POST', u'entity_type': u'apic', u'
```



```
        service_name': u'admin', u'start_time': u'2016-06-29T10
        :58:33.760565', u'is_default': u'false', u'end_time': u'2016-06-29
        T10:58:44.486919', u'target': u'10.102.102.81', u'message': u'Done'
        , u'id': u'ctxt-f4db2883-e42c-4262-a35f-04628c4ad5ea', u'
        replication_status': u'' }
53    }
54
55      2016-06-28 03:07:14.692932 DEBUG Thread-20 18793 [10.102.102.62,
           24063] Attempts 1
56      2016-06-28 03:07:14.693031 DEBUG Thread-20 18794 [10.102.102.62,
           24063] Cluster (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1', (0,
            '', 5230)), transaction: 0
57      2016-06-28 03:07:14.693147 DEBUG Thread-20 18795 [10.102.102.62,
           24063] Attempts for {
58    'name': 'ADCHybridMode_1', 'host': '10.102.102.62', 'virtual': False,
        'devs': {
59    'ADCHybridMode_1_Device_1': {
60    'state': 0, 'virtual': False, 'manager': {
61    'hosts': {
62    '10.102.102.81': {
63    'port': 80 }
64     }
65    , 'name': 'NMAS_1', 'creds': {
66    'username': 'nsroot', 'password': '<hidden>' }
67     }
68    , 'version': '11.0', 'host': '10.102.102.62', 'port': 80, 'creds': {
69    'username': 'nsroot', 'password': '<hidden>' }
70     }
71     }
72    , 'manager': {
73    'hosts': {
74    '10.102.102.81': {
75    'port': 80 }
76     }
77    , 'name': 'NMAS_1', 'creds': {
78    'username': 'nsroot', 'password': '<hidden>' }
79     }
80    , 'contextaware': True, 'port': 80, 'creds': {
81    'username': 'nsroot', 'password': '<hidden>' }
82     }
83     is 0
84      2016-06-28 03:07:14.693339 DEBUG Thread-20 18796 [10.102.102.62,
           24063] Deleting (u'uni/tn-coke_SDX2/lDevVip-ADCHybridMode_1',
           (0, '', 5230))
85      2016-06-28 03:07:14.693379 DEBUG Thread-20 18797 [10.102.102.62,
```



```
          24063] pending: False, delete: False, txId: None
86      2016-06-28 03:07:14.693517 DEBUG Thread-20 18798 [10.102.102.62,
          24063] Faults: []
87      2016-06-28 03:07:14.693558 DEBUG Thread-20 18799 [10.102.102.62,
          24063] Health: []
88      2016-06-28 03:07:14.693914 DEBUG Thread-20 18800 [10.102.102.62,
          24063] Send num: 761, type: 220, len: 382
89  <!--NeedCopy-->
```

Citrix ADC 设备封装，采用思科 ACI 云协调器模式

April 23, 2021

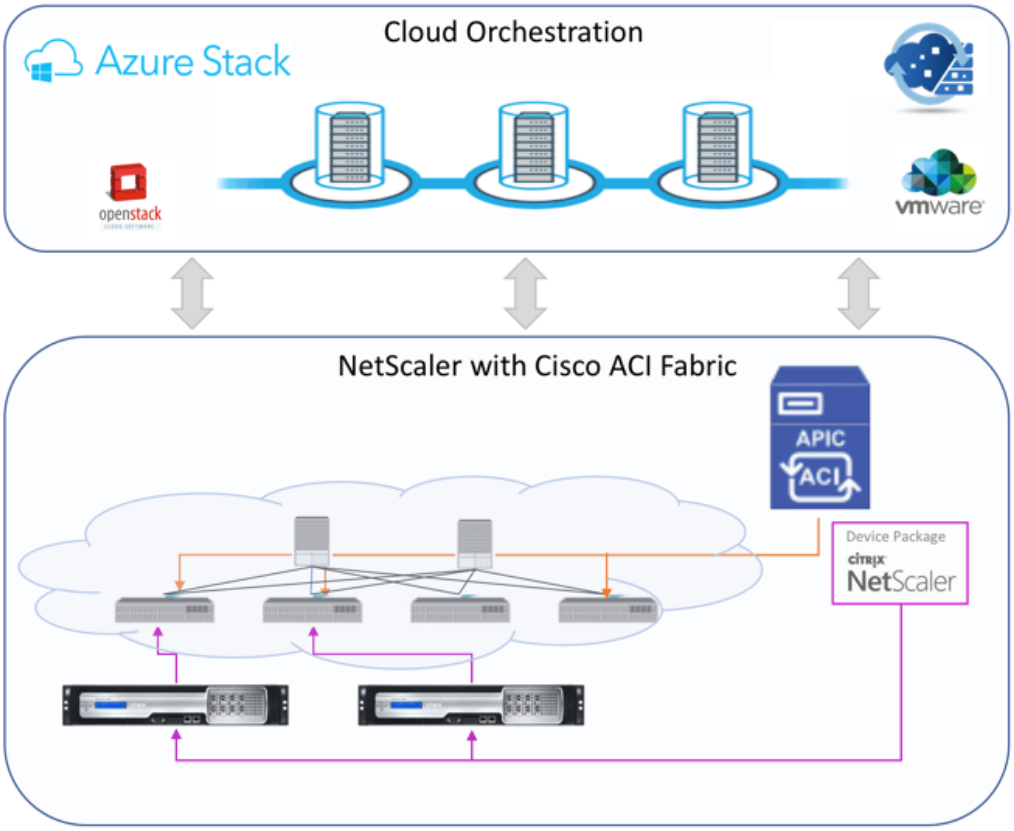
借助应用策略基础架构控制器 (APIC) 3.1 版 Citrix Citrix ADC 和思科 ACI 扩展了联合集成产品组合，以提供满足客户需求的新解决方案。新的集成模式 ACI 云协调器模式 ** 通过标准化参数抽象配置复杂性，简化了 L4-L7 集成。该解决方案可以无缝地实现 L4-L7 服务的自动化，实现敏捷应用部署、操作灵活性和简单性的目标。

使用 Citrix ADC 解决方案的思科 ACI 云协调器模式提供以下优势：

- L4-L7 服务的自动化减少了人为错误。
- Cisco ACI 解决方案的预构建集成可帮助您缩短部署时间，并提高应用程序（如 Web 应用程序、虚拟机和 SQL）的性能。
- 跨物理和虚拟网络组件对 Web 应用程序、虚拟机和 SQL 等应用程序的运行状况进行完全集成的可见性。

ACI 云协调器模式现在为您提供了更多选择，以便直接使用新的简化 APIC GUI，或者根据您的喜好选择任何云协调器，如思科云中心、Windows Azure 包、OpenStack、vRealize 或其他任何云协调器。这一新更改是通过将一组 ADC 属性公开为 ADC 架构来实现的。这些属性在设备包函数配置文件中映射。您可以在由云协 Provisioning 器（Cisco 云中心或无线应用协议 (WAP)）预配 ADC 服务时为这些属性提供值。

下图概述了云编排解决方案中的 Citrix ADC：

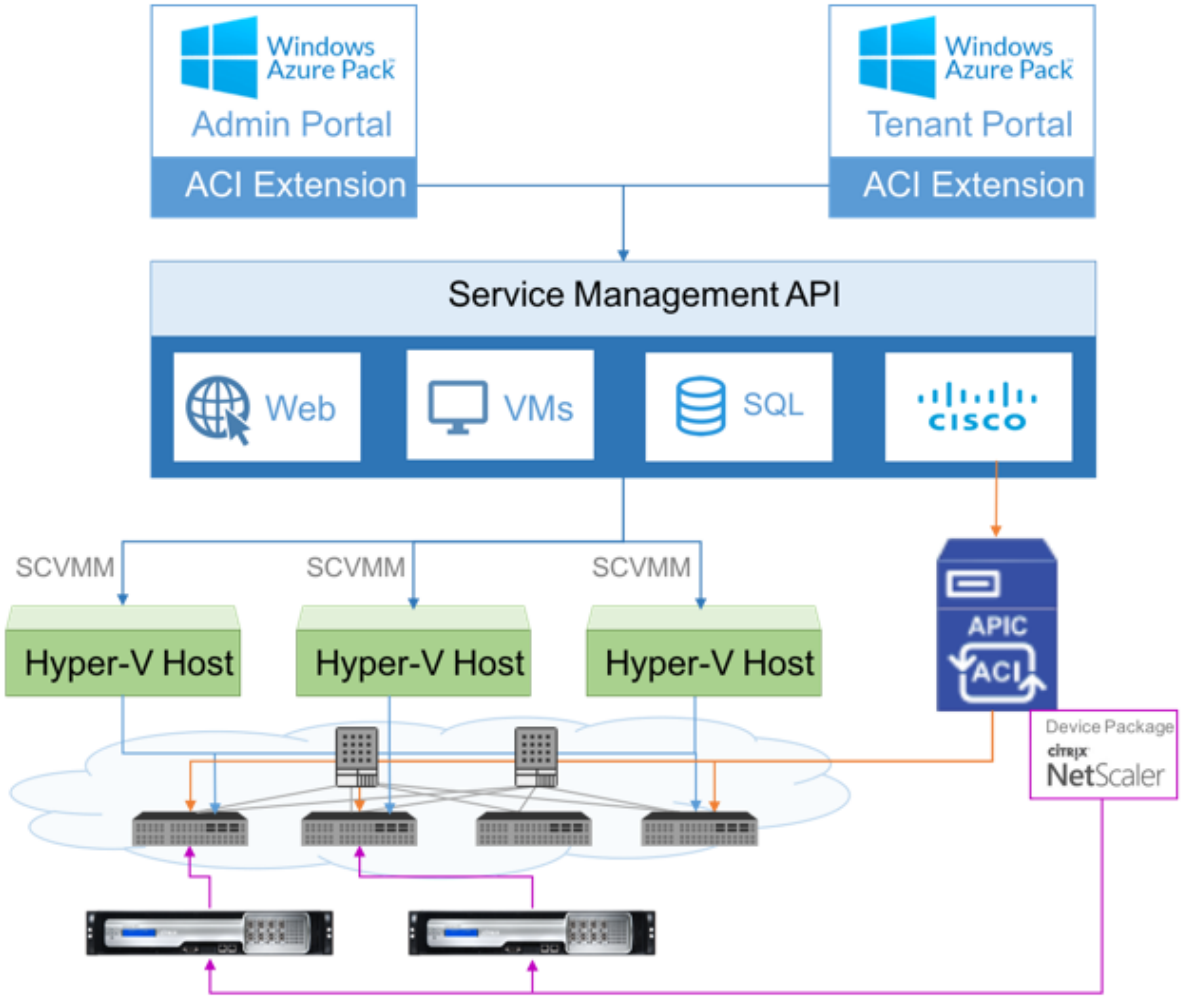


使用 Microsoft Azure 包的云编排器模式解决方案涉及许多集成点，例如 Azure 包到思科 APIC、思科 APIC 到系统中心虚拟机管理器 (SCVMM)，思科 APIC 到 Citrix ADC。作为私有云中的租户，您可以启用 NAT、配置网络服务以及添加负载均衡器。

Azure Pack 支持租户和管理员门户，每个门户都有自己的一组可以执行的操作。

- 作为管理员，您可以执行 ACI 注册、VIP 范围、Citrix ADC 设备与虚拟机云关联以及租户用户帐户创建等管理任务。
- 作为租户，您可以执行诸如登录 Azure 包租户门户以及配置网络、网桥域和虚拟路由和转发 (VRF) 等任务，还可以使用 Citrix ADC 负载平衡和 RNAT 功能。

下图概述了云模式解决方案中的 Azure 包：



> 重要
>
> - 云管理员可以使用 APIC 支持的 L4-L7 架构，任何其他更改都可以由 APIC 管理员直接在 APIC 中完成。这样，您就可以与支持的功能集相同地配置和部署 Citrix ADC。
> - 租户可以为同一网络部署具有不同端口的多个 VIP 地址。您必须确保 IP 和端口组合是唯一的。
> - Citrix ADC 设备包仅支持单上下文部署。每个租户都会获得一个专用的 Citrix ADC 实例。
> - 无线应用协议 (WAP) 支持 Citrix ADC MPX 装置和 Citrix ADC VPX 装置（包括部署在 Citrix ADC SDX 平台上的 Citrix ADC VPX 实例）。

云编排器模式设备包支持完全托管模式和服务管理器模式。完全托管模式包支持各种功能配置文件，例如简单负载平衡、内容切换、SSL 卸载和其他配置文件。这些功能配置文件涵盖了 Citrix ADC 的完整功能集和部署模式。同样，服务管理器模式设备包支持使用 APIC 对 Citrix ADC 进行单臂和双臂配置和部署。Citrix Application Delivery Management (ADM) 充当 APIC 的服务管理器，您可以使用 Citrix ADM 配置 Citrix ADC L4-L7 参数。

> 注意
>
> 在服务管理器模式（混合模式）中，不能重复使用或重新分配 Citrix ADC 设备中已存在的同一服务器 IP 地址。

云编排器模式功能配置文件包含一组映射到 APIC ADC 架构的参数，协调器使用这些参数。云协调器提供 ADC 参数的值（VIP，同时通过 APIC Provisioning Citrix ADC）。协调器与 APIC 的 API 进行通信，并将 ADC 的特定详细信息作为特定功能配置文件的有效负载的一部分传递。在内部，APIC 提取值并将其传递给在内部配置 Citrix ADC 的设备包。

有关 Cisco APIC 支持的 ADC 架构完整列表的详细信息，请参阅 思科 APIC 第 4 层到第 7 层服务部署指南，版本 3.1(1)。

完全托管模式设备包支持以下功能配置文件：

1. LB-HTTP-One-Arm-ProfileCM
2. LB-HTTP-Two-Arm-ProfileCM
3. LB-HTTP-Two-Arm-ServiceBackendProfileCM
4. CS-HTTP-LB-Service-ProfileCM
5. CS-SSL-LB-Service-ProfileCM
6. LB-SSL-ProfileCM
7. SSLVServerProfileInlineModeCM
8. WebVServerProfileWithRHICM
9. WebInlineVServerProfileWithRHICM
10. WebAnywhereVServerProfileWithRHIC
11. SSLVServerProfileForAnywhereModeCM
12. SSLAnywhereServerProfileCM
13. WebVServerProfileCM
14. WebInlineVServerProfileCM
15. WebAnywhereVServerProfileCM
16. CSLBServerProfileCM
17. GSLBServerProfileCM
18. CMPServerProfileCM
19. CRServerProfileC
20. DNSServerProfileCM
21. DSServerProfileCM
22. ICServerProfileCM

23. SSLVPNServerProfileCM
24. AppFWServerProfileCM
25. AAAServerProfileCM
26. AAASyslogServerProfileCM
27. IPv6WebInlineVServerProfileCM

服务管理模式设备包支持以下云模式功能配置文件：

1. ADCOneArmFunctionProfileCM
2. AADCTwoArmFunctionProfileCM
3. RHI-ADCOneArmFunctionProfileCM
4. RHI-ADCTwoArmFunctionProfileCM

Citrix ADC 支持上述功能配置文件。APIC 在 ADC 架构中支持这些参数的子集。如果函数配置文件中存在 Cisco ACI 不支持的属性，则必须克隆云 Orchestrator 模式函数配置文件，并提供 APIC 所有不支持的属性的值，并且必须保存这些属性。稍后，协调器可以使用新克隆的函数配置文件。

Citrix 云模式设备包支持 Citrix ADC 12.0，服务管理器模式也使用 Citrix ADM 12.0。设备包已将型号版本从 1.0 更改为 2.0，可用作新安装。由于机型版本已更改，云 Orchestrator 模式设备包无法从以前的设备包版本升级。

云编排器模式设备包也可用于常规部署。该软件包不要求用户通过任何云协调器置备 Citrix ADC。该设备包只与 APIC 和 APIC 兼容与云编排器。

管理 **Citrix ADM** 中的 **Kubernetes** 入口配置

April 23, 2021

Kubernetes (K8s) 是一个开源容器编排平台，可自动执行云原生应用程序的部署、扩展和管理。

Kubernetes 提供了入口功能，允许群集外部的客户端流量访问 Kubernetes 群集内运行的应用程序的微服务。ADC 实例可以充当 Kubernetes 群集内运行的应用程序的入口。ADC 实例可以负载平衡和内容将北南流量从客户端路由到 Kubernetes 群集内的任何微服务。

> 注意
>
> - Citrix ADM 支持 Kubernetes 版本 1.14 及更高版本的群集上的入口功能。
> - Citrix ADM 支持 Citrix ADC VPX 和 MPX 装置作为入口设备。
> - 在 Kubernetes 环境中，Citrix ADC 实例仅对 “NodePort” 服务类型进行负载平衡。

您可以将多个 ADC 实例配置为充当同一群集或不同群集或命名空间上的入口设备。配置实例后，您可以根据入口策略将每个实例分配给不同的应用程序。

您可以使用 Kubernetes `kubectl` 或 API 创建和部署入口配置。您还可以配置和部署来自 Citrix ADM 的入口。

您可以在 ADM 中指定 Kubernetes 集成的以下方面：

- 群集 — 您可以注册或取消注册 ADM 可以为其部署入口配置的 Kubernetes 群集。在 Citrix ADM 中注册群集时，请指定 Kubernetes API 服务器信息。然后，选择可以访问 Kubernetes 群集并部署入口配置的 ADM 代理。
- 策略 — 入口策略用于根据群集或命名空间选择 ADC 实例以部署入口配置。在添加策略时指定集群、站点和实例信息。
- 入口配置 — 此配置是 Kubernetes 入口配置，其中包括内容切换规则和微服务及其端口的相应 URL 路径。您还可以使用 Kubernetes 秘密资源指定 SSL/TLS 证书（在 ADC 实例上卸载 SSL 处理）。

Citrix ADM 使用入口策略自动将入口配置映射到 ADC 实例。

对于每个成功的入口配置，Citrix ADM 会生成一个样书配置包。ConfigPack 表示应用于 ADC 实例的 ADC 配置，该 ADC 配置与入口配置相对应。要查看配置包，请导航到 **“应用程序” > “样书” > “配置”**。

准备工作

要在 Kubernetes 群集上使用 Citrix ADC 实例作为入口设备，请确保具备以下功能：

- 库贝内特斯集群到位。
- 在 Citrix ADM 中注册的库贝内特斯群集。

使用秘密令牌配置 **Citrix ADM** 以管理 **Kubernetes** 群集

为了使 Citrix ADM 能够接收来自 Kubernetes 的事件，您需要在库贝内特斯中为 Citrix ADM 创建一个服务帐户。此外，使用群集中必要的 RBAC 权限配置服务帐户。

1. 为 Citrix ADM 创建服务帐户。例如，服务帐户名称可以是 `citrixadm-sa`。要创建服务帐户，请参阅 使用多个服务帐户。
2. 使用 `cluster-admin` 角色绑定 Citrix ADM 服务帐户。此绑定将 `ClusterRole` 跨群集授予服务帐户。以下是将 `cluster-admin` 角色绑定到服务帐户的示例命令。

   ```
   kubectl create clusterrolebinding citrixadm-sa-admin --clusterrole
      =cluster-admin --serviceaccount=default:citrixadm-sa
   <!--NeedCopy-->
   ```

   将 Citrix ADM 服务帐户绑定到 `cluster-admin` 角色后，服务帐户具有群集范围的访问权限。有关更多信息，请参阅 [`kubectl` create `clusterrolebinding`](https://kubernetes.io/docs/reference/access-authn-authz/rbac/#kubectl-create-clusterrolebinding)。

3. 从创建的服务帐户获取令牌。

   例如，运行以下命令查看 `citrixadm-sa` 服务帐户的令牌：


```
kubectl describe sa citrixadm-sa
<!--NeedCopy-->
```

4. 运行以下命令以获取令牌的密钥字符串：

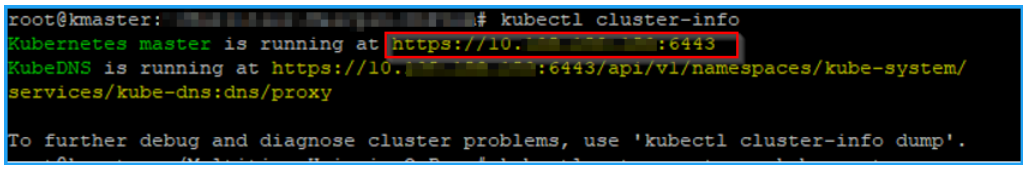
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

在 **Citrix ADM** 中添加 **Kubernetes** 群集

配置 Citrix ADM 代理并配置静态路由后，必须在 Citrix ADM 中注册 Kubernetes 群集。

要注册 Kubernetes 群集，请执行以下操作：

1. 使用管理员凭据登录到 Citrix ADM。
2. 导航到调配 > **Kubernetes** > 群集。
   此时将显示“集群”页面。
3. 单击添加。
4. 在 添加群集页面中，指定以下参数：
   a) 名称 -指定您选择的名称。
   b) **API** 服务器 **URL** -您可以从 Kubernetes 主节点获取 API 服务器 URL 详细信息。
      i. 在 Kubernetes 主节点上，运行命令 `kubectl cluster-info`。



      ii. 输入显示的 **Kubernetes** 主服务器正在运行的 URL。
   c) 身份验证令牌 -指定在您时获得的身份验证令牌字符串将 Citrix ADM 配置为管理库伯内特群集。验证 Kubernetes 集群和 Citrix ADM 之间的通信访问需要使用身份验证令牌。要生成身份验证令牌，请执行以下操作：
      i. 在 Kubernetes 主节点上，运行以下命令：

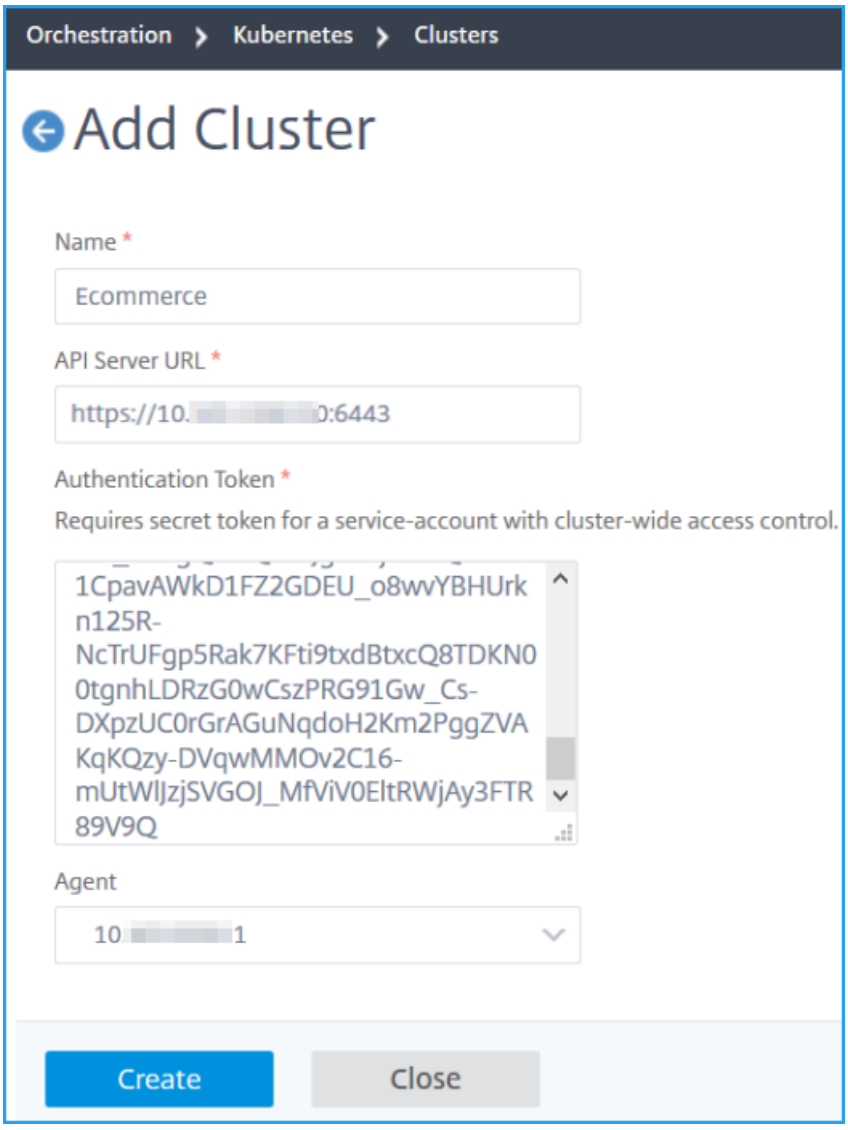
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

      ii. 复制生成的令牌并将其粘贴为身份验证令牌

      有关详细信息，请参阅 Kubernetes文档。

d) 从列表中选择座席。

e) 单击创建。



定义入口策略

入口策略根据入口群集或命名空间决定使用哪个 Citrix ADC 部署入口配置。

1. 导航到调配 **> Kubernetes >** 策略。
2. 单击 添加以创建策略。

   a) 指定策略名称。

   b) 定义在 Kubernetes 群集上部署入口配置的条件。这些条件通常基于入口群集和命名空间。

   c) 在“基础结构”小组中,

- 站点 -从列表中选择站点。
- 实例 -从列表中选择 ADC 实例。

站点和 实例列表根据 条件面板中的群集选择填充选项。

这些列表显示与使用 Kubernetes 群集配置的 Citrix ADM 代理相关联的站点或实例。

d) 在 “ 选择网络” 中，选择 ADM 将虚拟 IP 地址自动分配给入口配置的网络。

此列表显示在 “网 络**” > “IPAM**” 中创建的网络。

e) 单击创建。

部署入口配置

您可以使用 Kubernetes `kubectl`、Kubernetes API 或其他工具部署入口配置。您还可以直接从 Citrix ADM 部署入口配置。

1. 导航到 “ 编排**” > “**库贝内特斯**” > “**入口”。
2. 单击添加。
3. 在 创建入口字段中，指定以下详细信息：
   a) 指定入口的名称。
   b) 在 群集中，选择要在其上部署入口的 Kubernetes 群集。
   c) 从列表中选择 集群命名空间。此字段列出指定 Kubernetes 群集中存在的命名空间。
   d) 可选，选择 自动分配前端 **IP** 地址。
   e) 从列表 中选择入口协议。如果选择 **HTTPS**，请指定 **TLS** 密码。

   此密钥嵌入了嵌入 HTTPS 证书和私钥的 Kubernetes 密钥资源。

   HTTPS 入口需要在 Kubernetes 群集上配置基于 TLS 的密码。指定 `tls.crt` 要分别包含服务器证书和证书密钥的和 `tls.key` 字段。
   f) 对于内容路由，请指定以下详细信息：
      - **URL** 路径 -指定与 Kubernetes 服务和端口关联的路径。
      - **Kubernetes** 服务 -指定所需的服务。
      - 端口 -指定服务端口。
      - **LB** 方法 -为所选 Kubernetes 服务选择首选的负载平衡方法。

        选定的方法使用适当的注释更新入口规范。例如，如果选择 **ROUDROBIN** 方法，则 Citrix 注释将如下所示：

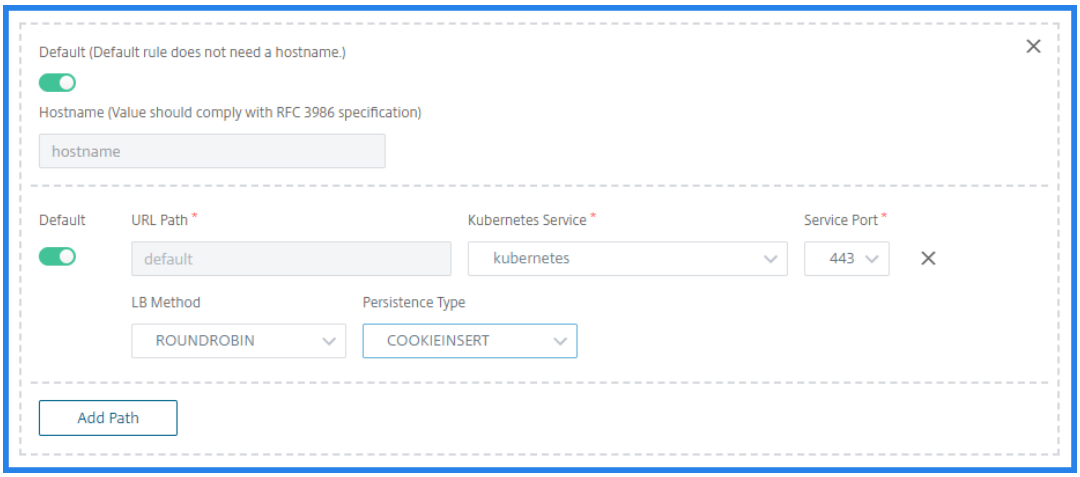
```
1  "lbmethod":"ROUNDROBIN"
2  <!--NeedCopy-->
```


- 持久性类型 -为所选 Kubernetes 服务选择首选的负载平衡持久性类型。

  选定的持久性类型使用适当的注释更新入口规范。例如，如果选择 **Cookie** 插入，则 Citrix 注释将如下所示：

```
"persistenceType":"COOKIEINSERT"
<!--NeedCopy-->
```

单击 添加” 以向入口配置添加更多 URL 路径和端口。



部署后，入口配置会根据以下内容将客户端流量重定向到特定服务：

- 请求的 URL 路径和端口。
- 定义的 LB 方法和持久性类型。

> 注意：在入口配置中使用的
>
> Kubernetes 服务应为节点端口类型。

g) 可选，请指定 入口说明。

h) 单击 “ 部署”。

如果要在部署之前查看配置，请单击 生成入口规范。指定的入口配置以 YAML 格式显示。查看配置后，单击 部署”。

> 注意
>
> 将许可证应用于使用入口配置创建的虚拟服务器。要应用许可证，请执行以下步骤：
>
> 1. 转到 “系统” > “许可和分析”。
> 2. 在 “ 虚拟服务器许可证摘要” 下，启用 自动选择虚拟服务器。

Citrix ADC 池容量

April 23, 2021

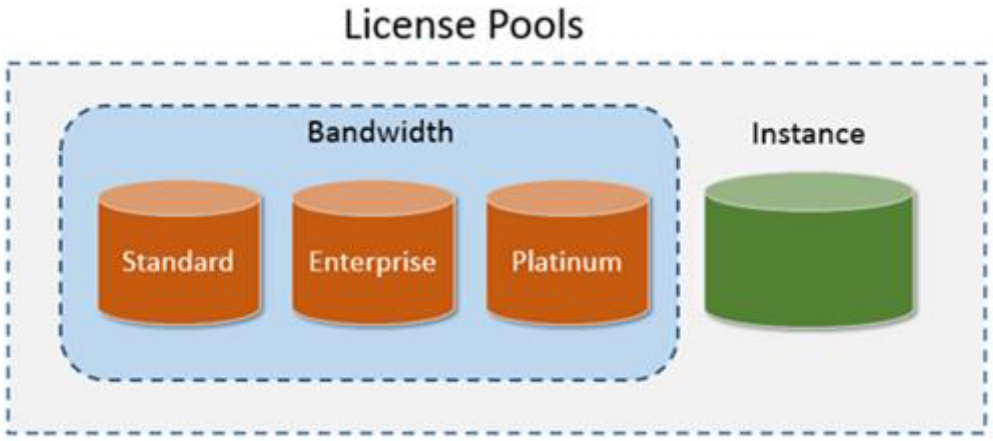
Citrix ADC 池容量允许您跨不同 ADC 外形共享带宽或实例许可证。对于基于虚拟 CPU 订阅的实例，您可以跨实例共享虚拟 CPU 许可证。将此池容量用于数据中心或公有云中的实例。当实例不再需要资源时，它会将分配的容量检查回公共池中。将释放的容量重用于需要资源的其他 ADC 实例。

您可以使用池许可来最大限度地提高带宽利用率，方法是确保为实例分配必要的带宽，而不会超过其需要。在运行时增加或减少分配给实例的带宽，而不影响流量。使用池容量许可证，您可以自动执行实例 Provisioning。

Citrix ADC 池容量许可的工作原理

Citrix ADC 池容量具有以下组件：

- Citrix ADC 实例，可分类为：
  - 零容量硬件
  - 独立 VPX 实例或 CPX 实例或 BLX 实例
- 带宽池
- 实例池
- 配置为许可证服务器的 Citrix ADM



零容量硬件

当通过 Citrix ADC 池容量进行管理时，MPX 和 SDX 实例称为“零容量硬件”，因为这些实例在从带宽和实例池中检出资源之前无法正常工作。因此，这些平台也称为 MPX-Z 和 SDX-Z 装置。

零容量硬件需要平台许可证才能从公共池中检出带宽和实例许可证。但是，您不能将 Citrix ADC 池容量用于另一个 Citrix ADC 硬件实例。

> 注意
>
> MPX 实例不需要实例许可证订阅。有关 MPX 和 SDX 实例支持的池容量，请参阅本页的表 1。有关不同 MPX 和 SDX 外形规格的许可证要求，请参阅表 5。

管理和安装平台许可证

您必须通过使用硬件序列号或许可证访问代码手动安装平台许可证。安装平台许可证后，它将被锁定到硬件上，无法按需在 Citrix ADC 硬件实例之间共享。但是，您可以手动将平台许可证移动到另一个 Citrix ADC 硬件实例。

运行 ADC 软件版本 11.1 的 ADC MPX 实例构建 54.14 或更高版本，运行 11.1 的 ADC SDX 实例构建 58.13 或更高版本支持 ADC 池容量。有关详细信息，请参阅 表 **1**。**MPX** 和 **SDX** 实例支持的池容量。

独立 **Citrix ADC VPX** 实例

运行 Citrix ADC 软件版本 11.1 版本版本 54.14 及更高版本的 Citrix ADC VPX 实例支持集容量：

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM

在以下虚拟机管理程序和云平台上运行 Citrix ADC 软件版本 12.0 版本 51.24 及更高版本的 Citrix ADC VPX 实例支持集容量：

- Microsoft Hyper-V
- AWS
- Microsoft Azure

> 注意
>
> 要启用 Citrix ADM 与 Microsoft Azure 或 AWS 之间的通信，必须配置 IPSEC 隧道。 有关更多信息，请参阅 将部署在云中的 Citrix ADC VPX 实例添加到 Citrix ADM。
>
> 与零容量硬件不同，VPX 不需要平台许可证。为了处理流量，它必须从池中签出带宽和实例许可证。

独立 **Citrix ADC CPX** 实例

部署在 Docker 主机上的 Citrix ADC CPX 实例支持集容量。与零容量硬件不同，CPX 不需要平台许可证。单个 CPX 实例消耗高达 1 Gbps 吞吐量，仅检出 1 个实例，而许可证池中没有带宽。例如，假设您有 20 个 CPX 实例，带宽池为 20 Gbps。如果其中一个 CPX 实例消耗 500 Mbps 的吞吐量，则其余 19 个 CPX 实例的带宽池将保持 20 Gbps。

如果同一 CPX 实例开始消耗 1500 Mbps 的吞吐量，则其余 19 个 CPX 实例的带宽池有 19.5 Gbps。

对于池许可，您只能以 10 Mbps 的倍数添加更多带宽。

独立 **Citrix ADC BLX** 实例

Citrix ADC BLX 实例支持池容量许可证。Citrix ADC BLX 实例不需要平台许可证。要处理流量，Citrix ADC BLX 实例必须从池中签出带宽和实例许可证。

带宽池

带宽池是 Citrix ADC 实例（物理和虚拟）可共享的总带宽。带宽池包含每个软件版本（标准版、高级版和高级版）的单独池。给定的 Citrix ADC 实例不能同时检出来自不同池的带宽。可从其签出带宽的带宽池取决于为其许可的软件版本。

实例池

实例池定义了可通过 Citrix ADC 池容量管理的 VPX 实例、CPX 实例或 BLX 实例的数量，或 SDX-Z 实例中 VPX 实例的数量。

从池中签出时，许可证会解锁 MPX-Z、SDX-Z、VPX、CPX 和 BLX 实例的资源，包括 CPU/PE、SSL 核心、每秒数据包和带宽。

> 注意
>
> SDX-Z 的管理服务不使用实例。

Citrix ADM 许可证服务器

Citrix ADC 池容量使用配置为许可证服务器的 Citrix ADM 来管理池容量许可证：带宽池许可证和实例池许可证。您可以使用 Citrix ADM 软件来管理无需 ADM 许可证的池容量许可证。

从带宽和实例池中签出许可证时，零容量硬件上的 Citrix ADC 外形规格和硬件型号决定

- Citrix ADC 实例在正常工作之前必须检出的最小带宽和实例数。
- Citrix ADC 可以检出的最大带宽和实例数。
- 每个带宽签出的最低带宽单位。最小带宽单位是 Citrix ADC 必须从池中检出的最小带宽单位。任何签出都必须是最低带宽单位的整数倍数。例如，如果 Citrix ADC 的最小带宽单位为 1 Gbps，则可以检出 100 Gbps，但不能检出 200 Mbps 或 150.5 Gbps。最小带宽单位与最小带宽要求不同。Citrix ADC 实例只有在获得至少最小带宽许可后才能运行。一旦达到最低带宽，实例可以使用最小带宽单位检查更多带宽。

表 1、2、3 和 4 总结了所有支持的 Citrix ADC 实例的最大带宽/实例、最小带宽/实例和最小带宽单位。表 5 总结了所有受支持的 Citrix ADC 实例的不同外形规格的许可证要求：

表 **1. MPX** 和 **SDX** 实例支持的池容量

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例	最大实例数	最小带宽单位
MPX 5900Z	10	1	不适用	不适用	1 Gbps
MPX 8005Z	15	5	不适用	不适用	1 Gbps
MPX 8900Z	33	5	不适用	不适用	1 Gbps

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例	最大实例数	最小带宽单位
MPX 14000Z 系列	100	20	不适用	不适用	1 Gbps
MPX 14000Z 40G 系列	100	20	不适用	不适用	1 Gbps
MPX 14000Z FIPS 系列	100	20	不适用	不适用	1 Gbps
MPX 14000Z 40S 系列	100	20	不适用	不适用	1 Gbps
MPX 15000Z 系列	120	20	不适用	不适用	1 Gbps
MPX 15000Z 50G 系列	120	20	不适用	不适用	1 Gbps
MPX 115XX 系列	42	15	不适用	不适用	1 Gbps
MPX 22000Z 系列	120	40	不适用	不适用	1 Gbps
MPX 24000Z 系列	150	100	不适用	不适用	1 Gbps
MPX 25000Z 40G	200	100	不适用	不适用	1 Gbps
MPX 25000ZA	200	100	不适用	不适用	1 Gbps
MPX 26000Z 系列	200	100	不适用	不适用	1 Gbps
MPX 26000Z 100G 系列	200	100	不适用	不适用	1 Gbps
MPX 26000Z 50S 系列	200	100	不适用	不适用	1 Gbps
SDX 8015Z	15	2	1	5	1 Gbps
SDX 8900Z	33	10	2	7	1 Gbps
SDX 115XX 系列	42	8	2	20	1 Gbps

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例	最大实例数	最小带宽单位
SDX 14000Z 系列	100	10	2	25	1 Gbps
SDX 14000Z 40G 系列	100	10	2	25	1 Gbps
SDX 14000Z 40S 系列	100	10	2	25	1 Gbps
SDX 14000Z FIPS 系列	100	10	2	25	1 Gbps
SDX 15000Z 50G	120	10	2（注意：低于 13.0 47.x 的版本有 5 个实例）	55	1 Gbps
SDX 15000Z	120	10	2 注意：5 个实例适用于低于 13.0 47.x 的版本）	55	1 Gbps
SDX 22000Z 系列	120	20	20	80	1 Gbps
SDX 25000Z 40G	200	50	10	115	1 Gbps
SDX 25000ZA	200	50	10	115	1 Gbps
SDX 26000Z 100G	200	50	10	115	1 Gbps
SDX 26000Z	200	50	10	115	1 Gbps
SDX 26000Z 50S	200	50	10	115	1 Gbps
SDX 24000Z 系列	150	50	10	80	1 Gbps

> 注意：
>
> 最低带宽和实例适用于运行以下及更高版本的 SDX 实例：11.1 64.x、12.0 63.x、12.1 54.x 和 13.0 41.x。
>
> 最低购买数量与最低系统要求不同。

表 **2. CPX** 实例支持的池容量

产品系列	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例	最大实例数	最小带宽单位
CPX	10	10	1	1	10 Mbps

表 **3.** 虚拟机管理程序和云服务上的 **VPX** 实例支持的池容量

虚拟机管理程序 /云服务	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例	最大实例数	最小带宽单位
Citrix Hypervisor	40 Gbps	10 Mbps	1	1	10 Mbps
VMware ESXI	100 Gbps	10 Mbps	1	1	10 Mbps
Linux KVM	100 Gbps	10 Mbps	1	1	10 Mbps
Microsoft Hyper-V	3 Gbps	10 Mbps	1	1	10 Mbps
AWS	30 Gbps	10 Mbps	1	1	10 Mbps
Azure	10 Gbps	10 Mbps	1	1	10 Mbps

> 注意：
>
> 最小采购数量不同于最低系统要求。

表 **4. BLX** 实例支持的池容量

产品系列	最大带宽 (Gbps)	最小带宽 (Mbps)	最小实例	最大实例数	最小带宽单位
BLX	100	10	1	1	10 Mbps

有关支持 BLX 实例的平台的更多信息，请参阅 支持的 Linux 平台。

表 **5.** 不同外形规格的许可证要求

产品系列	零容量硬件购买	带宽和版本订阅	实例订阅
MPX	需要许可证	需要许可证	-
SDX	需要许可证	需要许可证	需要许可证

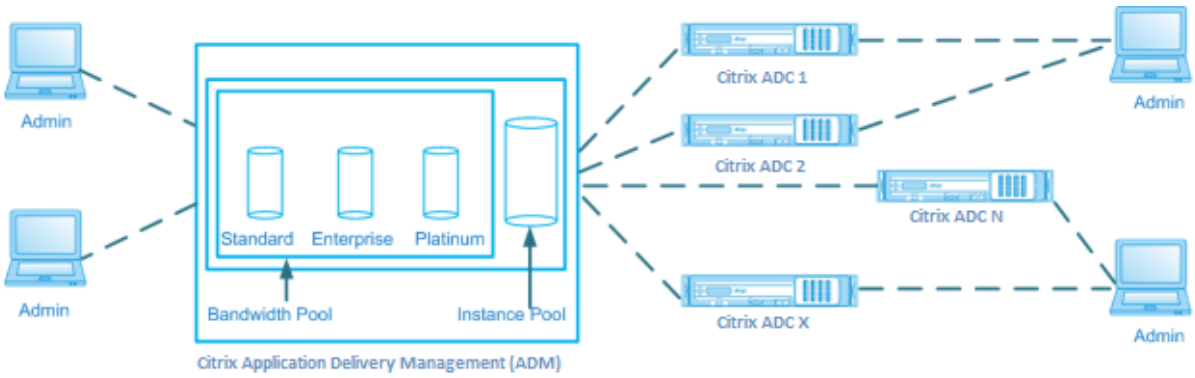
产品系列	零容量硬件购买	带宽和版本订阅	实例订阅
VPX	-	需要许可证	需要许可证
CPX	-	-	需要许可证
BLX	-	需要许可证	需要许可证

配置 **Citrix ADC** 池容量

April 23, 2021

要使用 ADC 池容量，请将 Citrix ADM 配置为所需 ADC 实例的许可证服务器。ADC 实例从 ADM 签入和签出许可证。您可以在 ADM GUI 中执行以下任务：

- 将池容量许可证文件（带宽和实例池）上传到许可证服务器。
- 根据需要将许可证池中的许可证分配给 Citrix ADC 实例。
- 根据实例的最小和最大容量，查看来自 Citrix ADC 实例（MPX-Z /SDX-Z/VPX/BLX）的许可证。
- 为 Citrix ADC FIPS 实例配置池容量以签入或签出许可证。



支持的硬件和软件版本

有关池容量支持的硬件和软件版本，请参阅 Citrix ADC 池容量。

ADC 池容量状态

池容量状态指示 ADC 实例的许可证要求。配置了池容量的 ADC 实例显示以下状态之一：

- 最佳：实例以适当的许可证容量运行。
- 容量不匹配：实例运行的容量小于用户配置的容量。

- **Grace**：实例在宽限许可证上运行。
- 宽限和不匹配：实例正在宽限运行，但容量小于用户配置的容量。
- 不可用：实例未向 ADM 注册以进行管理，或者从 ADM 到实例的 NITRO 通信无法正常工作。
- 未分配：实例中未分配许可证。

步骤 **1-**在 **ADM** 中应用许可证

1. 在 Citrix ADM 中，导航到 网络 > 许可证。
2. 在 许可证文件部分，选择 添加许可证文件”，然后选择以下选项之一：
   - 从本地计算机上传许可证文件。如果本地计算机上已存在许可证文件，则可以将其上传到 ADM。
   - 使用许可证访问代码。指定从 Citrix 购买的许可证的许可证访问代码。然后，选择 获取许可证。然后选择完成”。

   > 注意：您可以随
   >
   > 时从许可证 设置向 ADM 添加更多许可证。
3. 单击完成。

   许可证文件将添加到 ADM 中。“ 许可证到期信息” 选项卡列出 ADM 中存在的许可证以及到期的剩余天数。
4. 在 许可证文件中，选择要应用的许可证文件，然后单击 应用许可证。

   此操作使 ADC 实例能够将选定的许可证用作池容量。

步骤 **2-**将 **Citrix ADM** 注册为许可证服务器

要将 ADM 注册为 Citrix ADC 实例的许可证服务器，请执行以下步骤之一：

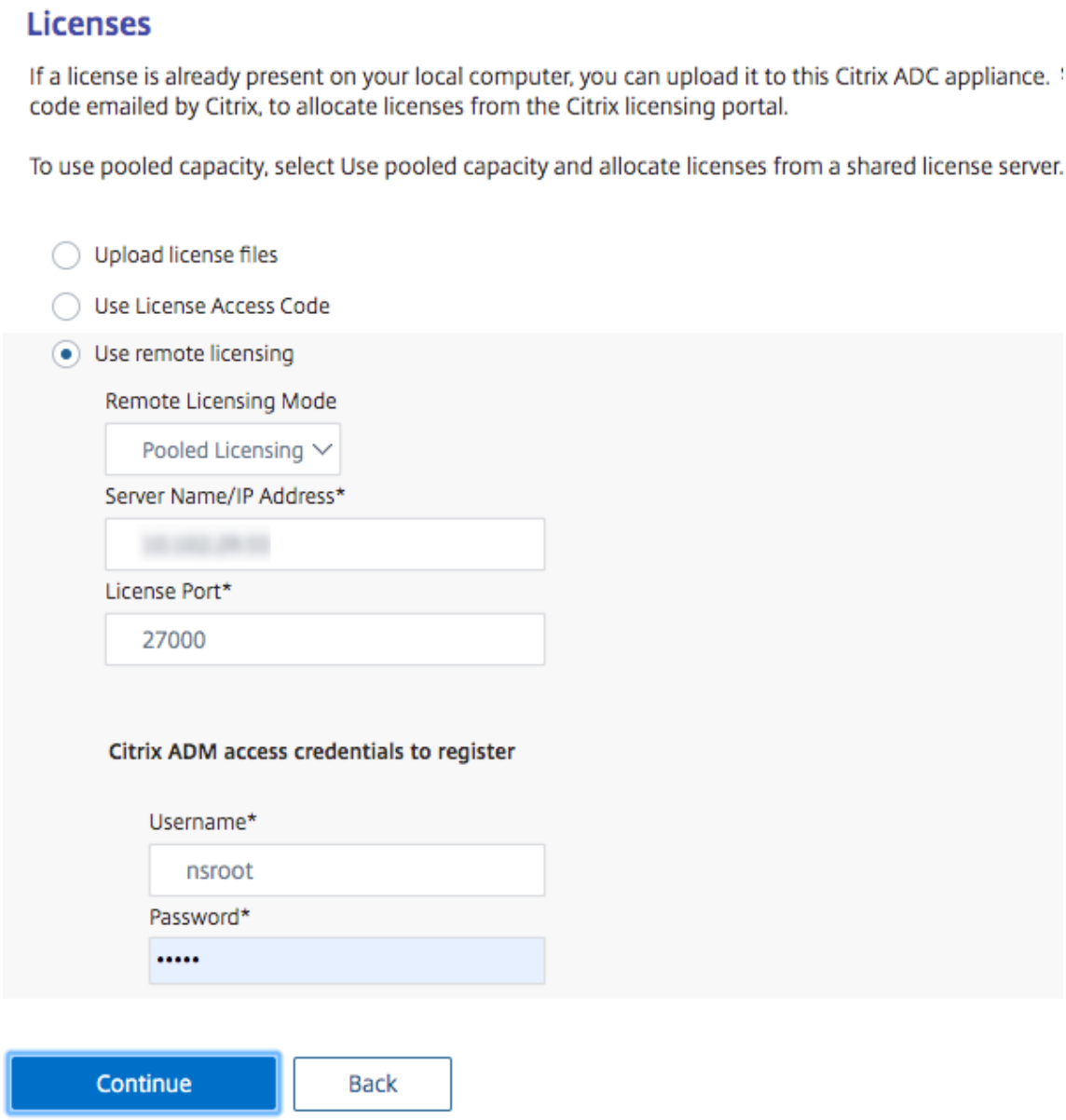
- 使用图形用户界面
- 使用 CLI

使用 **GUI** 将 **ADM** 注册为许可证服务器

在 ADM GUI 中，将 ADM 服务器注册为许可证服务器。

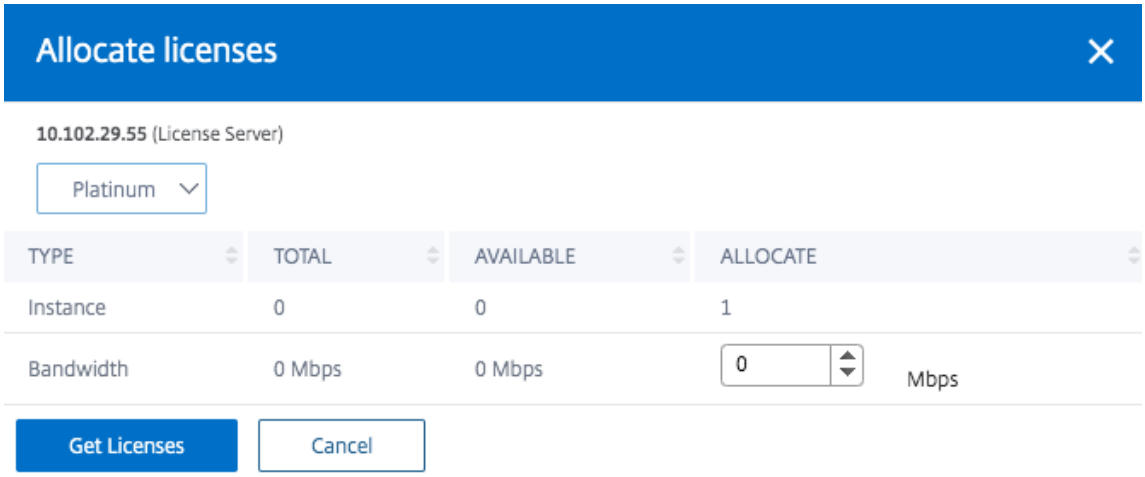
1. 登录到 Citrix ADC GUI。
2. 导航到 系统 > 许可证 > 管理许可证。
3. 单击 “ 添加新许可证”。
4. 选择 使用远程许可”，然后从列表中选择远程许可模式。
5. 在 “ 服务器名称**/IP** 地址” 字段中，指定 ADM 服务器的 IP 地址。

6. 选择“向 **Citrix ADM** 注册”。
7. 输入 ADM 凭据以向 Citrix ADM 注册实例，然后单击 继续。



8. 在 分配许可证中，选择许可证版本并指定所需的带宽。

   首次在 Citrix ADC 中分配许可证。您可以稍后从 ADM GUI 更改或释放许可证分配。



9. 单击获取许可证。

> 重要
>
> 如果您更改许可证版本，则热重新启动实例。在您重新启动实例之前，配置更改才会生效。

使用 **CLI** 将 **ADM** 添加为许可证服务器

如果 ADC 实例没有 GUI，请使用以下 CLI 命令将 ADM 服务器添加为许可证服务器：

1. 登录到 ADC 控制台。
2. 添加 ADM 服务器 IP 地址：

```
1 > add ns licenseserver <adm-server-IP-address> -port <adm-server-
    port-number>
2 <!--NeedCopy-->
```

3. 查看许可证服务器中可用的许可证带宽：

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```

4. 从所需的许可证版本中分配许可证带宽：

```
1 > set ns capacity -unit gbps -bandwidth <specify-license-bandwidth
    > edition <specify-license-edition>
2 <!--NeedCopy-->
```

许可证版本可以是 标准版、企业版或 白金版。

> 重要信息：如果您更改许可证版本，则 “
>
> 热” 重新启动实例。


```
reboot -w
```

在您重新启动实例之前，配置更改才会生效。

步骤 3-将池许可证分配给 ADC 实例

要从 ADM GUI 分配池容量许可证，请执行以下操作：

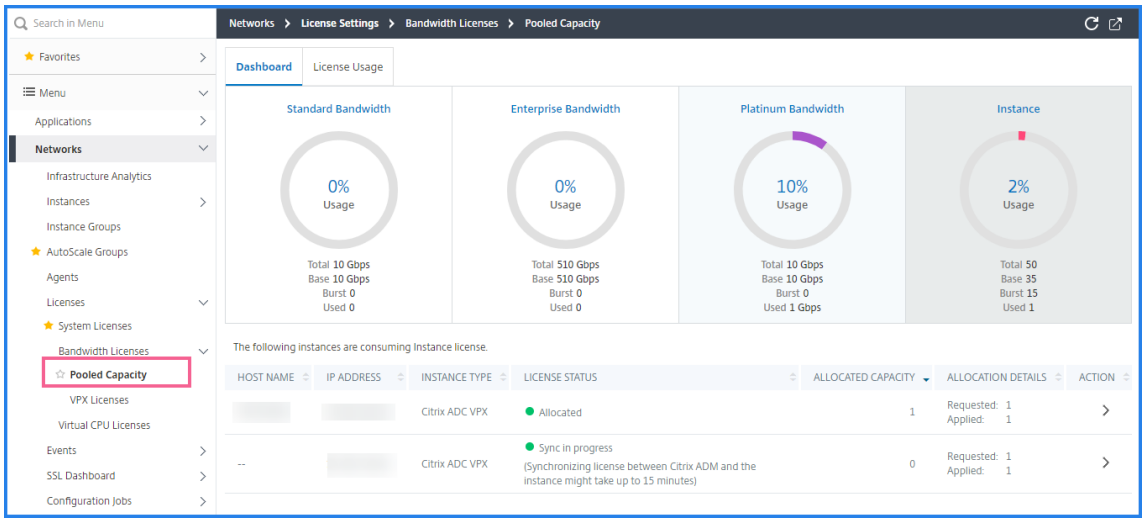
1. 登录到 Citrix ADM。
2. 导航至 **“网络” > “许可证” > “带宽许可证” > “池容量”**。

   仅当您将 FIPS 实例许可证上传到 ADM 时，才会显示 FIPS 实例容量。
3. 单击要管理的许可证池。

   注意：

   “已 分配容量” 字段不会立即反映更改的带宽。带宽更改在 ADC 热重启后生效。

   在 “ 分配详细信息” 中，当您更改实例的带宽分配时，将更新 “ 请求” 和 “ 应用” 字段。
4. 单击 **>** 按钮，从可用实例列表中选择 ADC 实例。



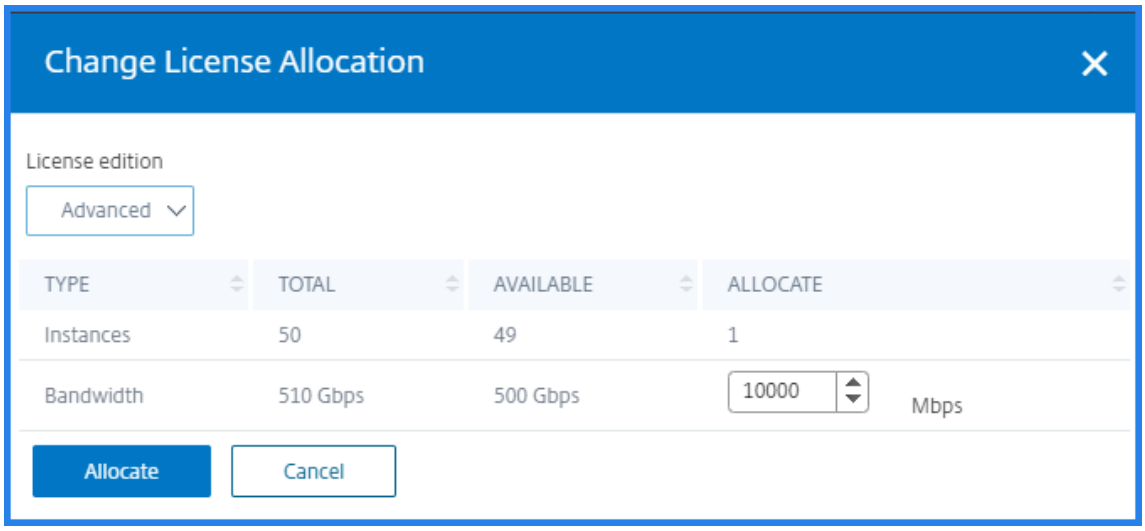
许可证状态列显示相应的许可证分配状态消息。

注意：

非托管实例选项卡显示在 Citrix ADM 中发现但未管理的实例。

5. 单击 “ 更改分配” 或 “ 发布分配” 以修改许可证分配。
6. 此时将显示一个弹出窗口，其中包含许可证服务器中的可用许可证。

7. 您可以通过设置“分配”列表选项来选择实例的带宽或实例分配。进行选择后，单击 分配”。
8. 您也可以从“更改许可证 分配”窗口的列表选项中更改已分配的许可证版本。



> 注意：如果您更改许可证版本，则
>
> 热重新启动实例。

在 **ADC** 实例上配置池容量

您可以在以下 ADC 实例上配置池容量许可证：

- ADC MPX-Z 实例
- ADC VPX 实例
- ADC 高可用性对

Citrix ADC MPX-Z 实例

MPX-Z 是支持集容量的 ADC MPX 装置。MPX-Z 支持高级版、高级版或标准版许可证的带宽池。

MPX-Z 需要平台许可证才能连接到许可证服务器。您可以通过以下任一方式安装 MPX-Z 平台许可证：

- 从本地计算机上传许可证文件。
- 使用实例的硬件序列号。
- 实例 GUI 的“ 系统” > “ 许可证” 部分中的许可证访问代码。

如果删除 MPX-Z 平台许可证，则会禁用存储容量功能。实例许可证将被释放到许可证服务器。

您可以动态修改 MPX-Z 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重新启动实例时，它会自动签出其配置容量所需的池许可证。

Citrix ADC VPX 实例

启用池容量的 ADC VPX 实例可以从带宽池（高级/高级/标准版）中检出许可证。您可以使用 ADC GUI 从许可证服务器签出许可证。

您可以动态修改 VPX 实例的带宽，而无需重新启动。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重新启动实例时，配置的池容量许可证将自动从 ADM 服务器中签出。

Citrix ADC 高可用性对

在开始之前，请确保 ADM 服务器配置为许可证服务器。有关详细信息，请参阅将 ADM 配置为许可证服务器。

将带宽分配给 ADC HA 对时，Citrix ADM 会将相同的带宽检出到主实例和辅助实例。如果将 10 Mbps 带宽分配给 ADC HA 对，ADM 将执行以下操作：

1. 将 20 Mbps 带宽检出到高可用性对。
2. 为 HA 对中的每个实例分配 10 Mbps。

要将池许可证分配给 ADC HA 对，请参阅将池许可证分配给 ADC 实例。

“池容量”页分别显示实例及其分配的容量。如果您更改或释放主实例的带宽，辅助实例带宽会自动与主实例同步。但是，如果您更改或释放辅助实例带宽，则不会发生同步。

仅将 **ADM** 服务器配置为池许可证服务器

April 23, 2021

作为管理员，您只能将 ADM 服务器配置为池许可证服务器。使用此配置，ADM 服务器仅接收来自 ADC 实例的许可数据。

有时，您可能需要限制 ADC 实例的数据离开监管区域的监管要求。在这种情况下，您可以在监管区域中部署 ADM 内部服务器的本地实例，以使用管理、监控和分析功能。当您遵循相同的方法使用池许可证功能时，必须在各种 ADM 许可证服务器之间拆分池许可证。此方法无法让您灵活地在全球部署的 ADC 实例之间分配池许可证。

因此，只将 ADM 服务器配置为池许可证服务器。ADM 服务器仅接收来自所有 ADC 实例的许可数据。因此，您可以遵守监管要求，并在全球部署的 ADC 实例之间动态分配池容量许可证。

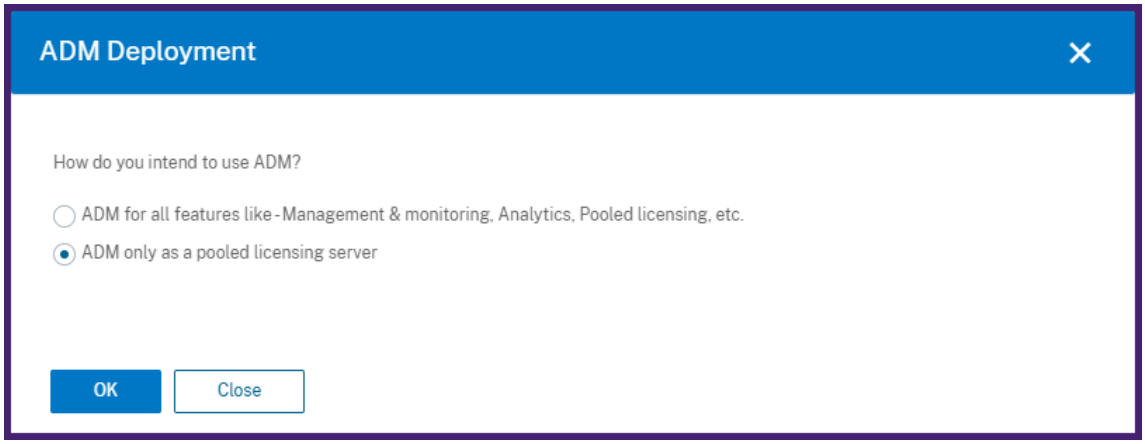
本文档介绍如何仅将 ADM 服务器配置为池许可证服务器。

如何仅将 **ADM** 服务器配置为池许可证服务器

在开始之前，请确保没有向 ADM 服务器添加 ADC 实例。仅在完成步骤 4 后添加 ADC 实例。

要仅为池许可证服务器配置 ADM 服务器，请执行以下操作：

1. 导航到 **“系统” > “管理”**。
2. 在 “ 系统配置” 部分中，选择 “ 系统部署”。
3. 在 **ADM** 部署中，选择 仅 **ADM** 作为池许可服务器。



4. 单击确定。

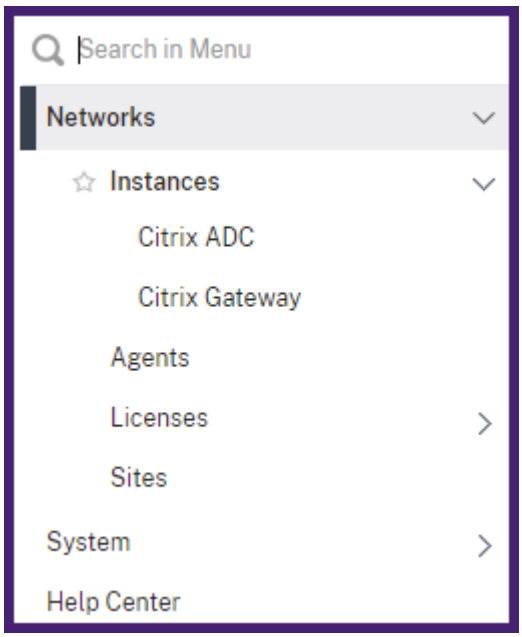
   此操作仅保留池许可功能并禁用以下 ADM 功能：

   - ADM 备份
   - 事件管理
   - SSL 证书管理
   - 网络报告
   - 网络功能
   - 配置审核

   > 注意
   >
   > 默认情况下，ADM 分析功能处于禁用状态。如果已启用此功能，请务必禁用该功能。

   在确认框中，单击 是。

   ADM GUI 现在只显示池许可功能。而且，剩余的功能不会显示。



5. 仅为许可功能配置 ADM 后，请在 网络 **>** 实例页面中添加 **ADC** 实例。

> 注意
>
> - 您可以在一个或多个 ADM 服务器中添加 ADC 实例。当您更改此类 ADC 实例的密码时，请确保更新发现该实例的所有 ADM 服务器上的密码。
> - 用户仍然可以在 ADM GUI 中对禁用功能执行某些操作。例如，事件轮询和 ADC 备份。作为超级管理员，如果要限制此类操作，请使用适当的访问策略禁用其他管理员的用户访问权限。有关详细信息，请参阅在 Citrix ADM 上配置访问策略。

将 **Citrix ADC VPX** 中的永久许可证升级到 **Citrix ADC** 池容量

April 23, 2021

具有永久许可证的 Citrix ADC VPX 装置可升级到 Citrix ADC 池容量许可证。通过升级到 Citrix ADC 池容量许可证，您可以根据需要将许可证池中的许可证分配给 Citrix ADC VPX 装置。您还可以为在高可用性模式下配置的 Citrix ADC 实例配置 Citrix ADC 池容量许可证。要在高可用性模式下为 Citrix ADC VPX 实例配置 Citrix ADC 池容量许可证，请参阅将 Citrix ADC VPX 高可用性对中的永久许可证升级到 Citrix ADC 池容量。

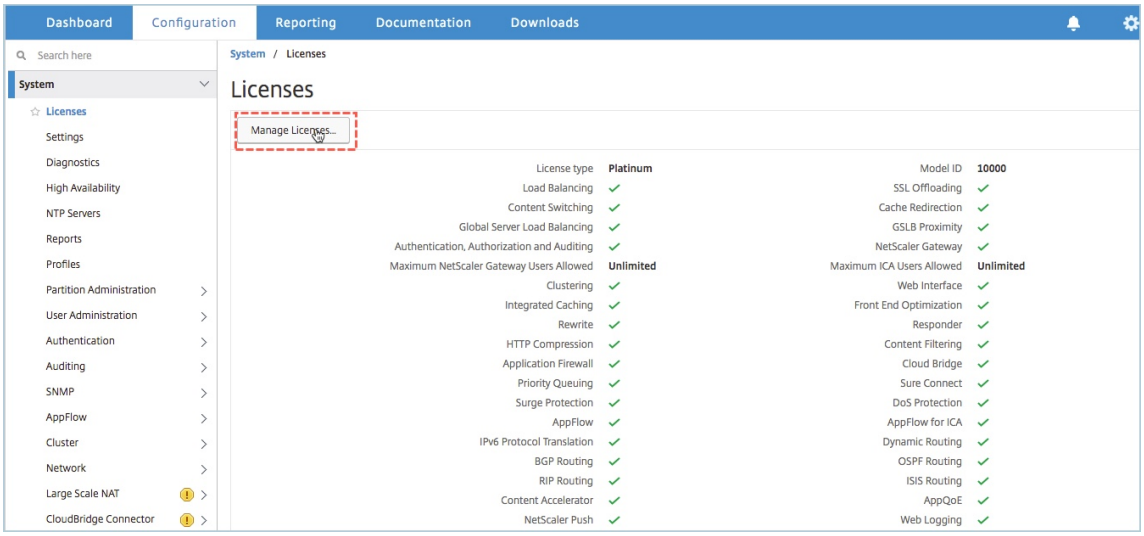
必备条件

确保将 Citrix ADC VPX 装置升级到 12.0.56.x 版本。

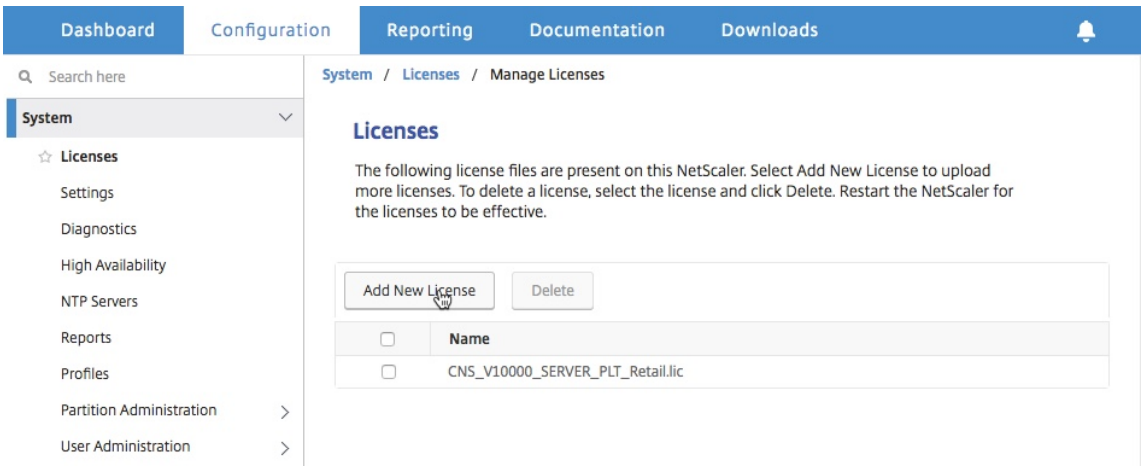
要升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADC VPX 设备的 IP 地址，如 http://192.168.100.1。

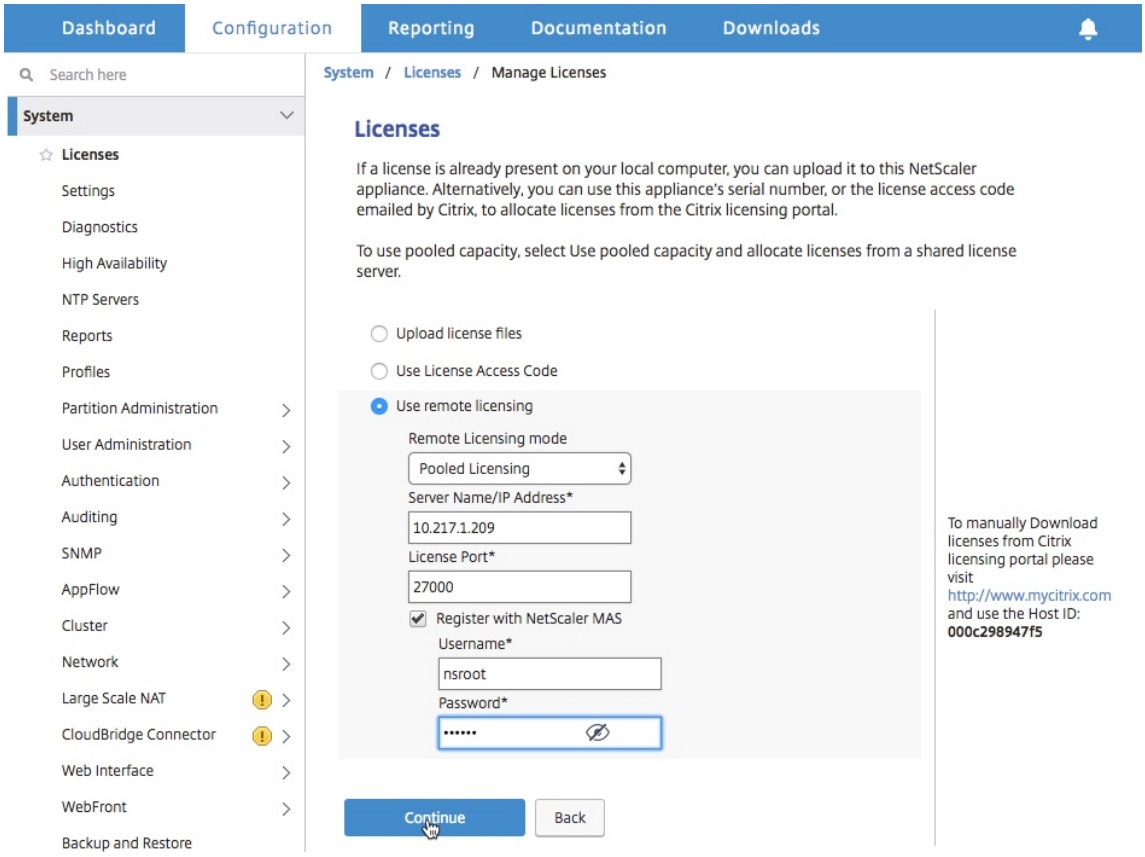
2. 在 “ 用户名 ” 和 “ 密码 ” 字段中，键入管理员凭据。
3. 在 “ 欢迎使用 ” 页面上，单击 “ 继续 ”。
4. 在 “配置 ” 选项卡上，导航到 **“系统” > “**许可证 ”，然后单击 “ 管理许可证 ”。



5. 在 “ 许可证 ” 页面上，单击 “ 添加新许可证 ”。



6. 在 “ 许可证 ” 页面上，选择 “ 使用远程许可 ”，然后执行以下操作：



a) 在 远程授权模式下拉列表中，选择 池授权。

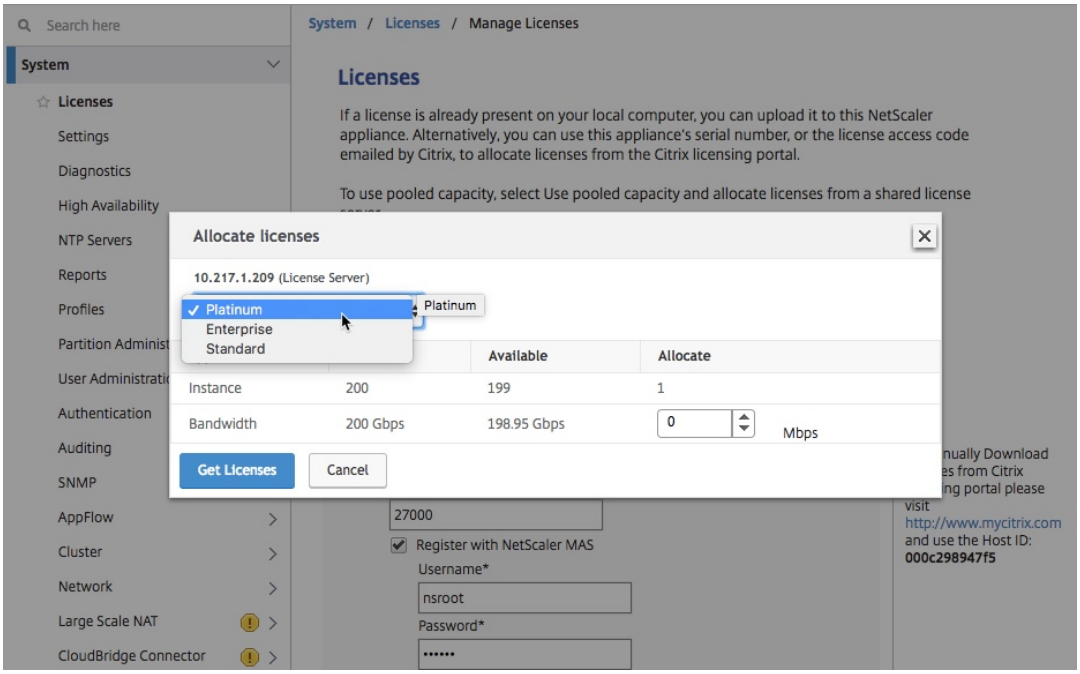
b) 在 “ 服务器名称 **/IP** 地址” 字段中，输入许可证服务器的详细信息。

c) 如果要通过 **ADM** 管理实例的池许可证，请确保选中 **“向 Citrix ADM** 注册” 复选框并输入 Citrix ADM 凭证。

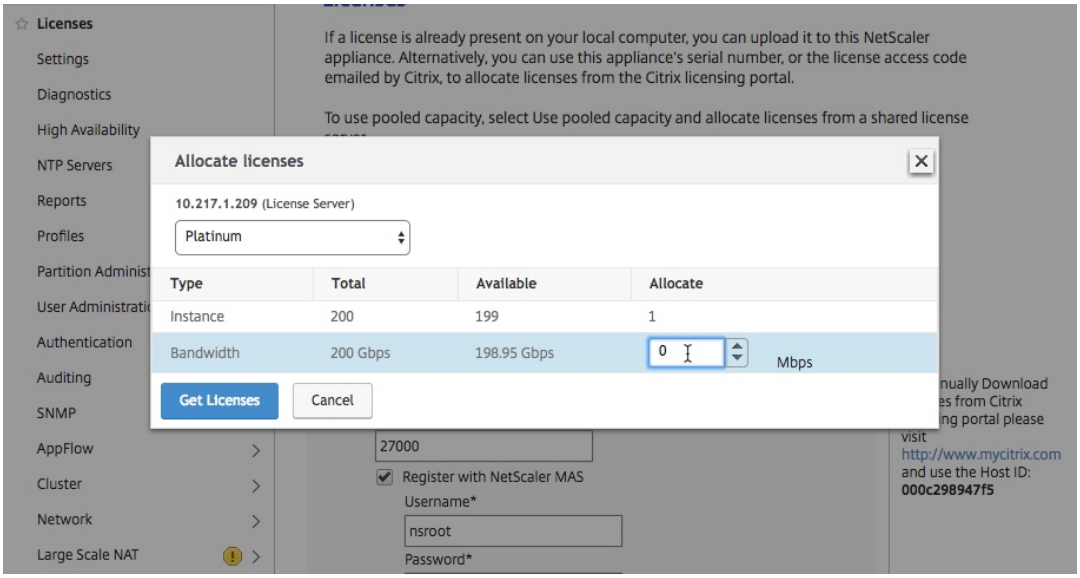
d) 单击继续。

7. 在 “ 分配许可证” 窗口中，执行以下操作：

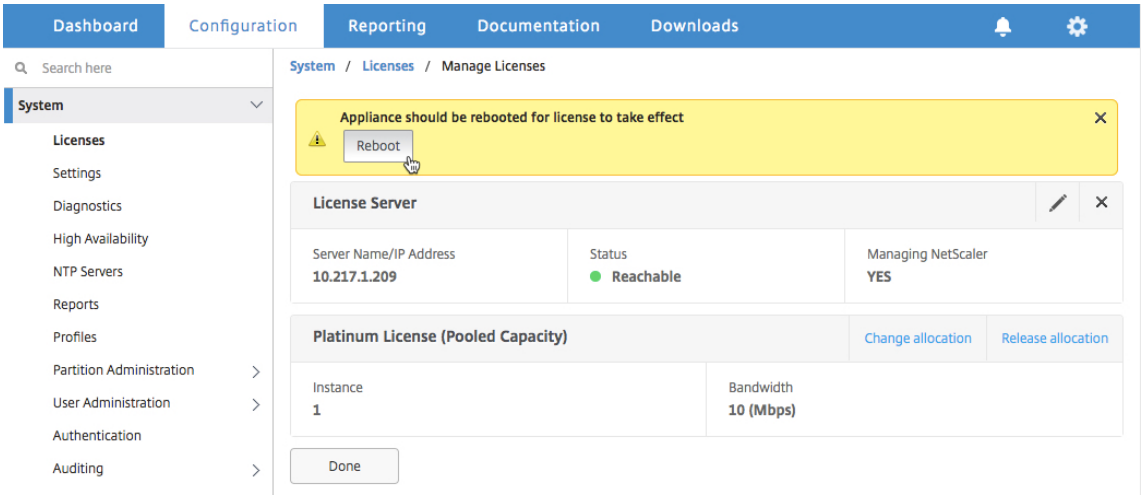
a) 从下拉列表中选择许可证版本。



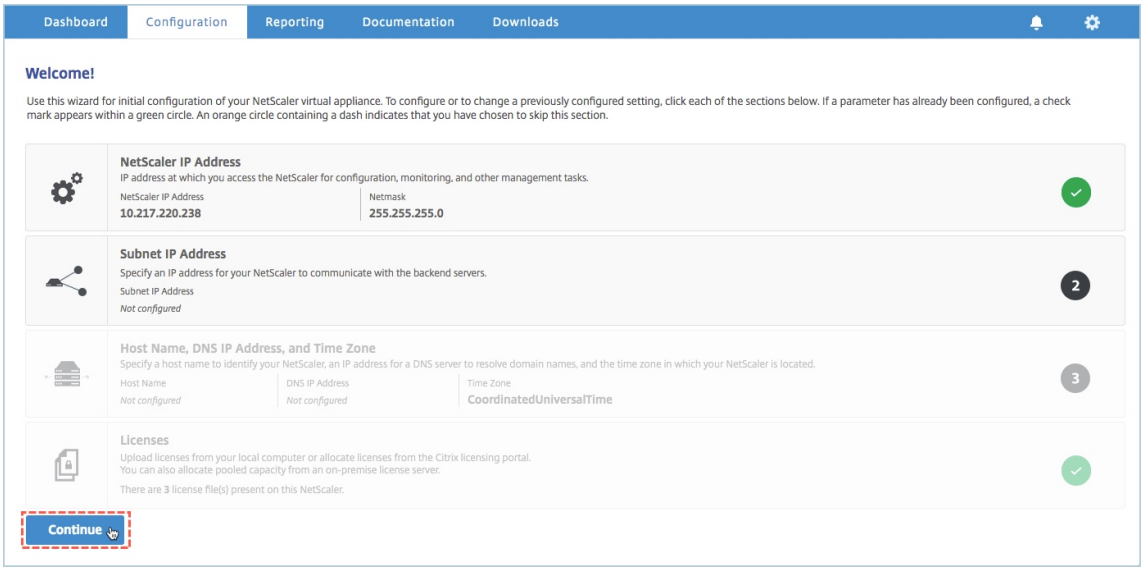
b) 从 “分配” 菜单将带宽分配 给 Citrix ADC 装置，然后单击 “ 获取许可证”。



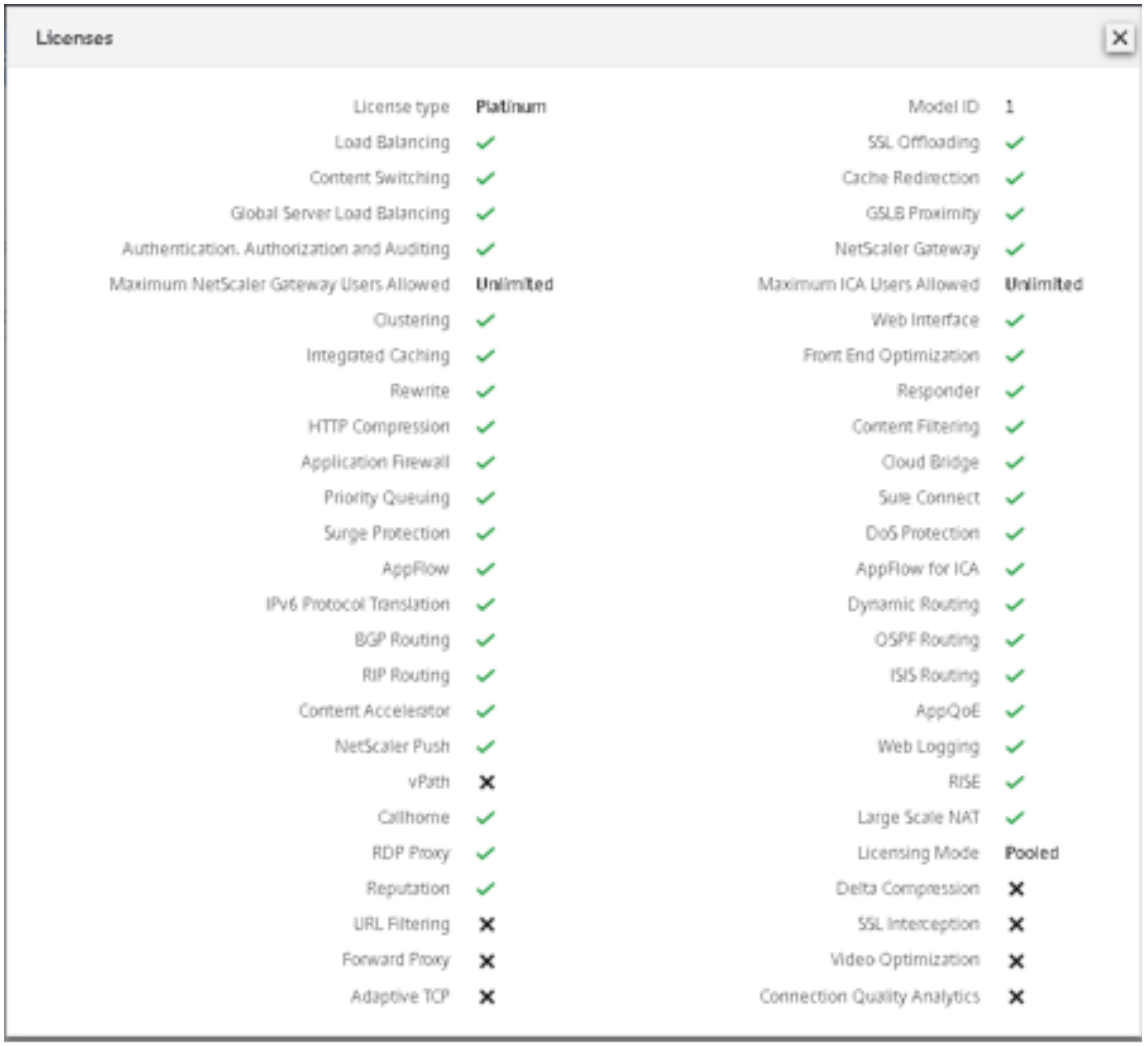
8. 出现提示时，单击 重新启动以重新启动装置。



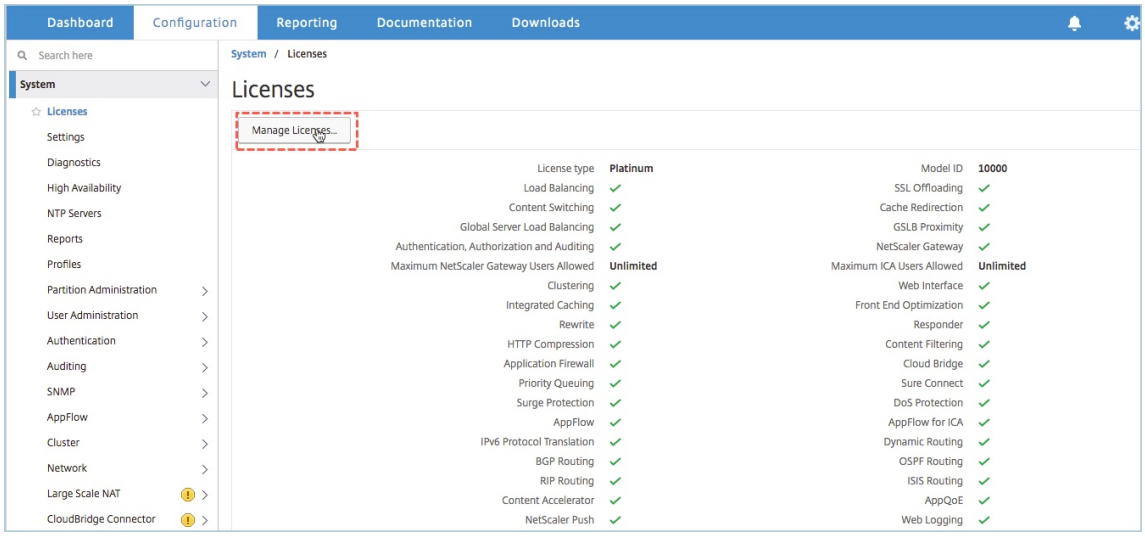
9. 在“确认”对话框中，单击“ 是”。
10. 一旦 Citrix ADC VPX 装置重新启动，请登录到 Citrix ADC VPX 装置。在“ 欢迎使用”页面上，单击“ 继续”。



许可证页面显示 Citrix ADC VPX 设备上许可的所有功能。单击 **X**。



11. 导航到 **“系统” > “许可证”**，然后单击 “ 管理许可证”。



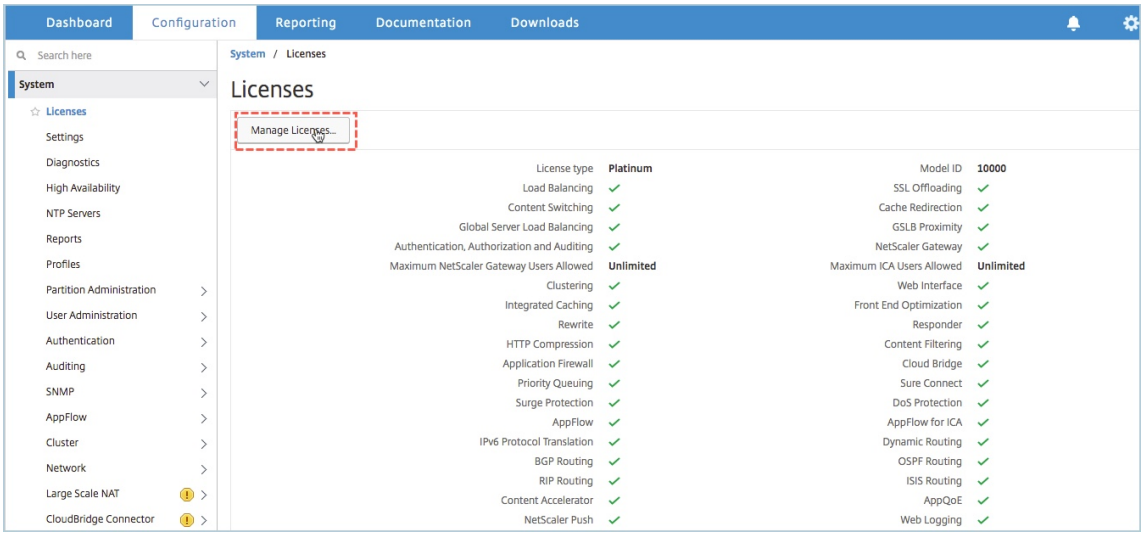
在 “ 管理许可证” 页面上，可以查看许可证服务器、许可证版本和分配带宽的详细信息。

将 **Citrix ADC VPX** 高可用性对中的永久许可证升级到 **Citrix ADC** 池容量

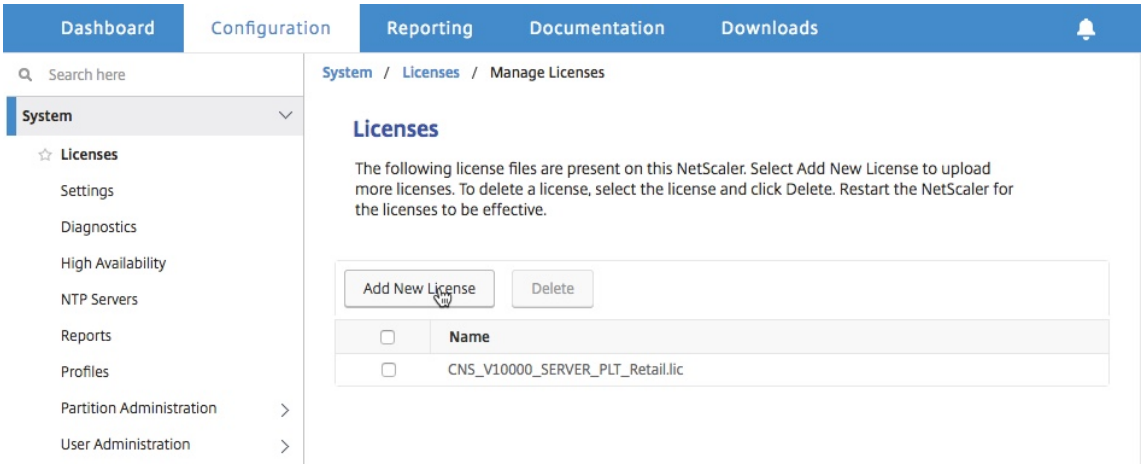
对于在高可用性模式下配置的 Citrix ADC VPX 装置，您必须在 HA 对中的主要和辅助 Citrix ADC 实例上配置 Citrix ADC 池容量。您需要将相同容量的许可证分配给 HA 对中的主 Citrix ADC 实例和辅助实例。例如，如果您希望高可用性对中的每个实例提供 1 Gbps 容量，则需要从公共池中分配 2 Gbps 容量，以便您可以为高可用性对中的主要和辅助 Citrix ADC 实例分配 1 Gbps 容量。

要将现有的 **Citrix ADC VPX HA** 设置升级到 **Citrix ADC** 池容量，请执行以下操作：

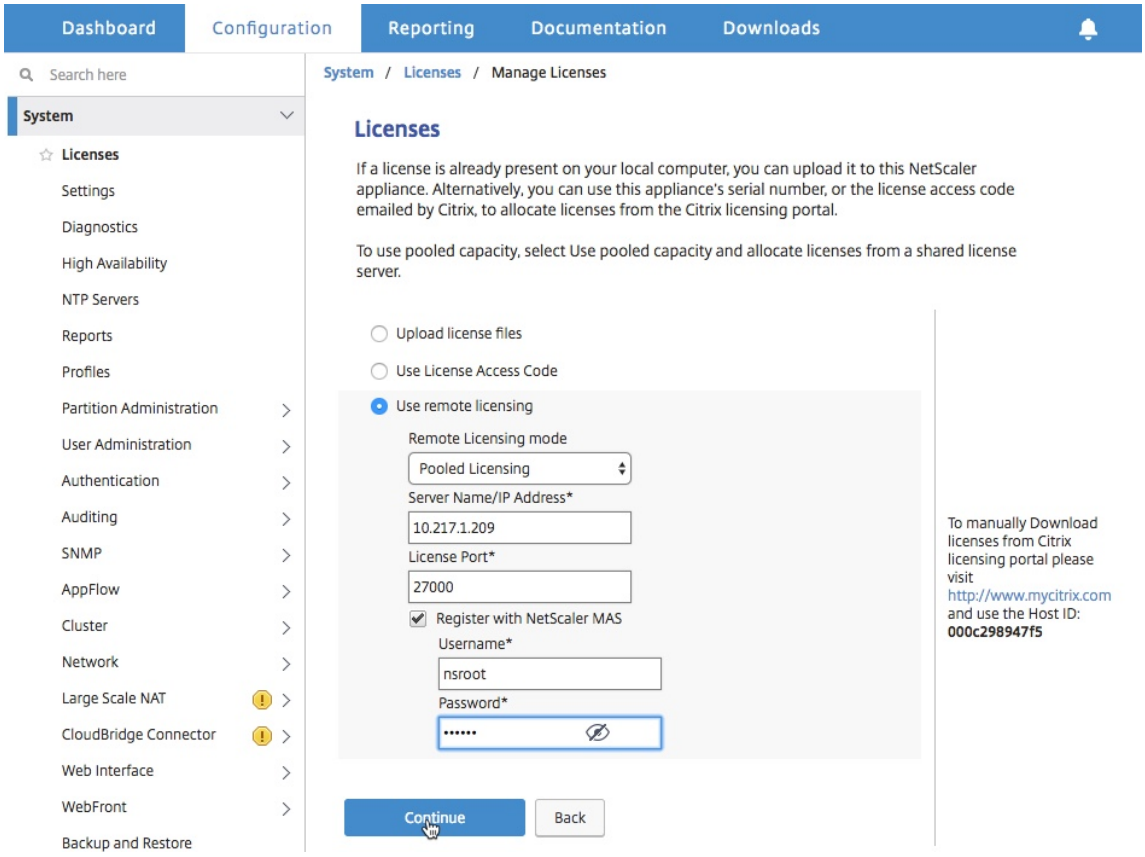
1. 登录到主 Citrix ADC VPX 实例。在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，如 `http://192.168.100.1`。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎使用”页面上，单击“继续”。
4. 在配置选项卡上，导航到 系统 > 许可证，然后单击 管理许可证。



5. 在“许可证”页面上，单击“添加新许可证”。



6. 在“许可证”页面上，选择“使用远程许可”，然后执行以下操作：



a) 在 远程授权模式下拉列表中，选择 池授权。

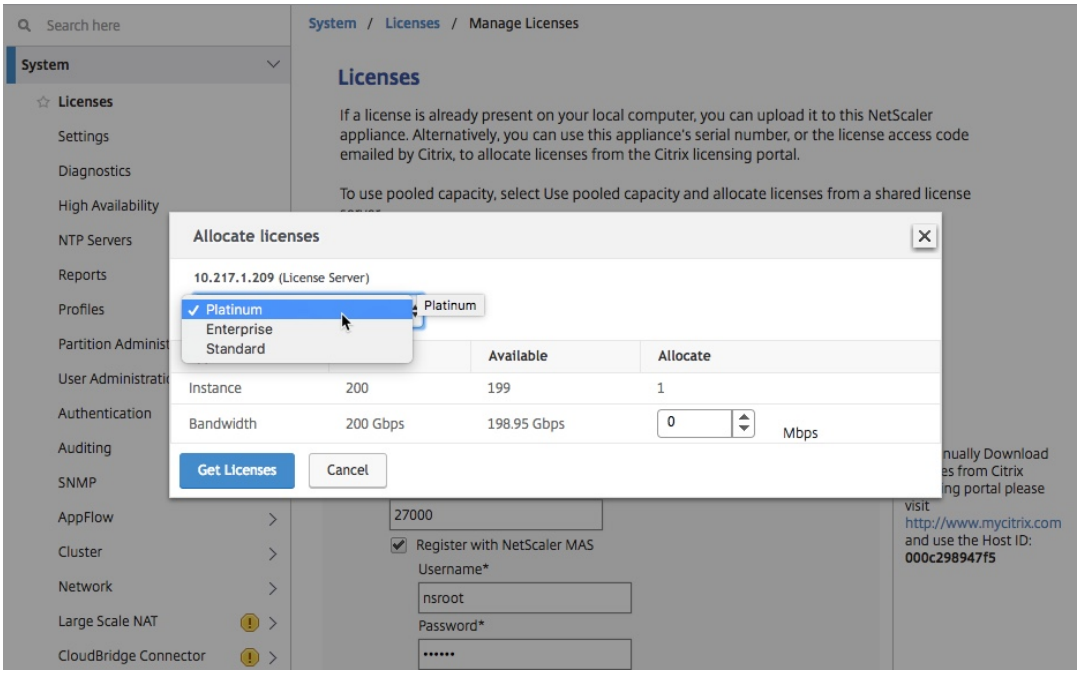
b) 在 “ 服务器名称 **/IP** 地址” 字段中，输入许可证服务器的详细信息。

c) 如果要通过 **Citrix ADM** 管理实例的池许可证，请确保选中 **“向 Citrix ADM** 注册” 复选框并输入 ADM 凭证。

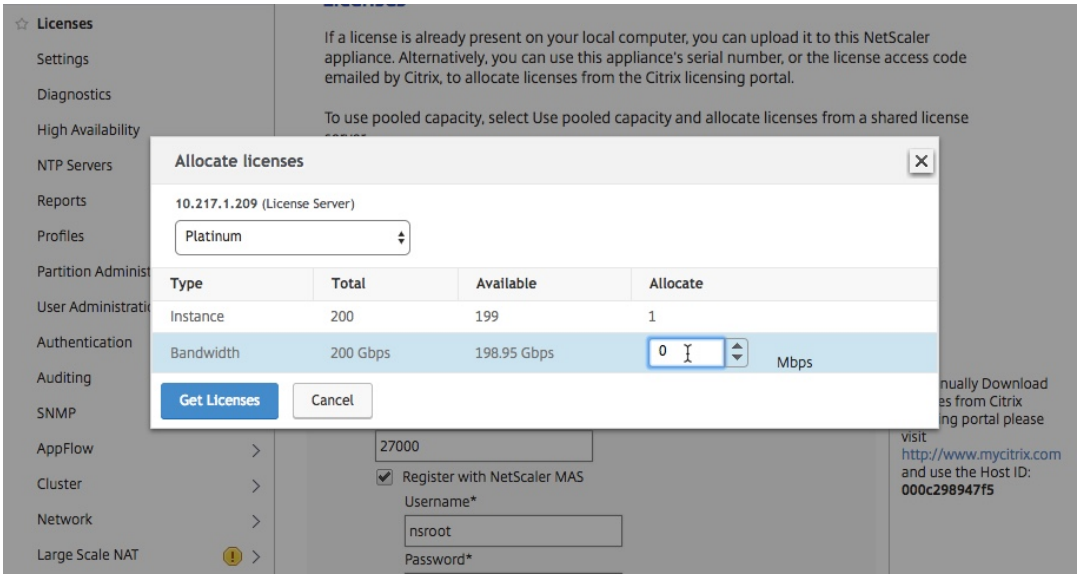
d) 单击继续。

7. 在 “ 分配许可证” 窗口中，执行以下操作：

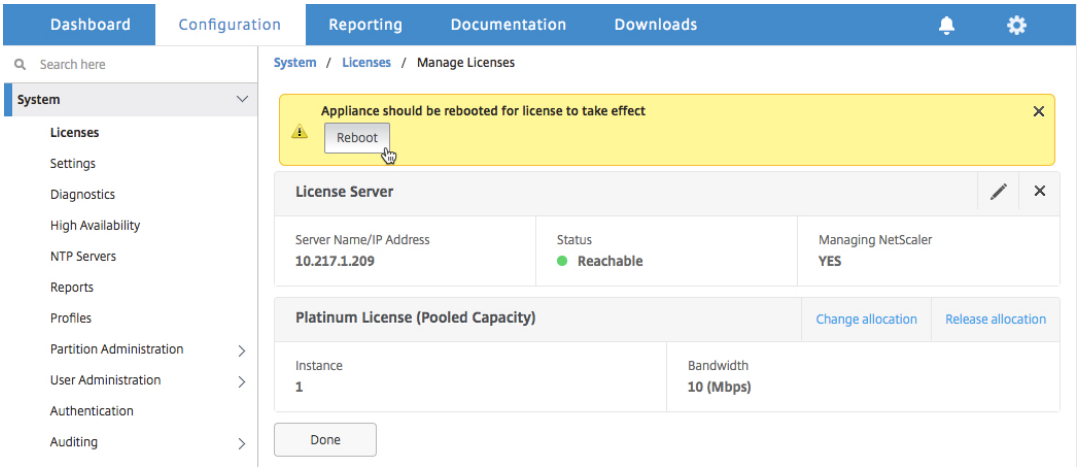
a) 从下拉列表中选择许可证版本。



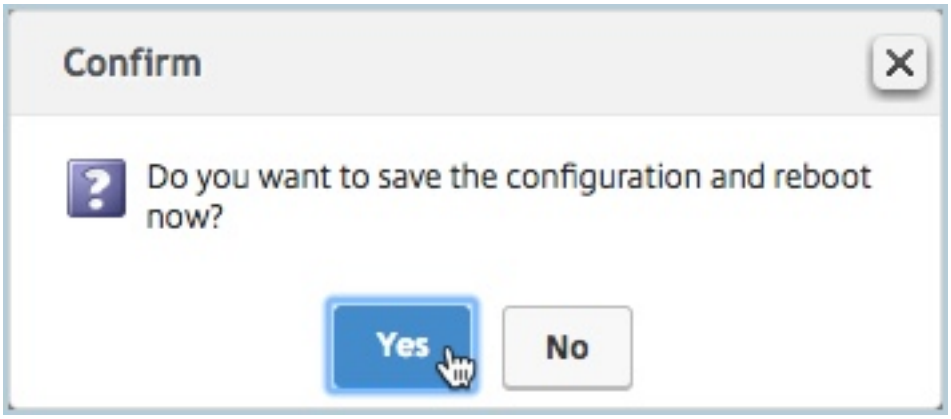
b) 从“分配”菜单将带宽分配 给 Citrix ADC 装置，然后单击“ 获取许可证”。



c) 出现提示时，单击“ 重新启动”以热重新启动主 Citrix ADC VPX 装置。



8. 在“确认”对话框中，单击“是”。



Citrix ADC VPX 装置将重新启动。

主 Citrix ADC VPX 装置重新启动后，辅助 Citrix ADC VPX 装置将成为 HA 设置中新的主 Citrix ADC VPX 装置。

9. 登录到新的主 Citrix ADC VPX 装置，然后重新启动装置。执行以下操作：

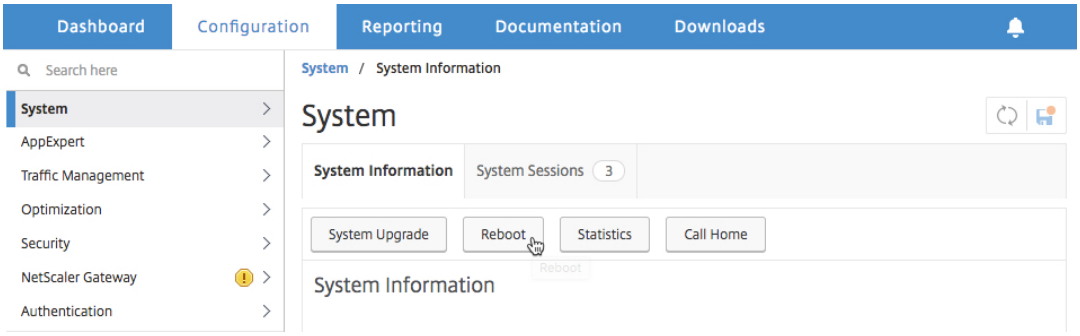
   a) 在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，如 http://192.168.100.1。

   b) 在“用户名”和“密码”字段中，键入管理员凭据。

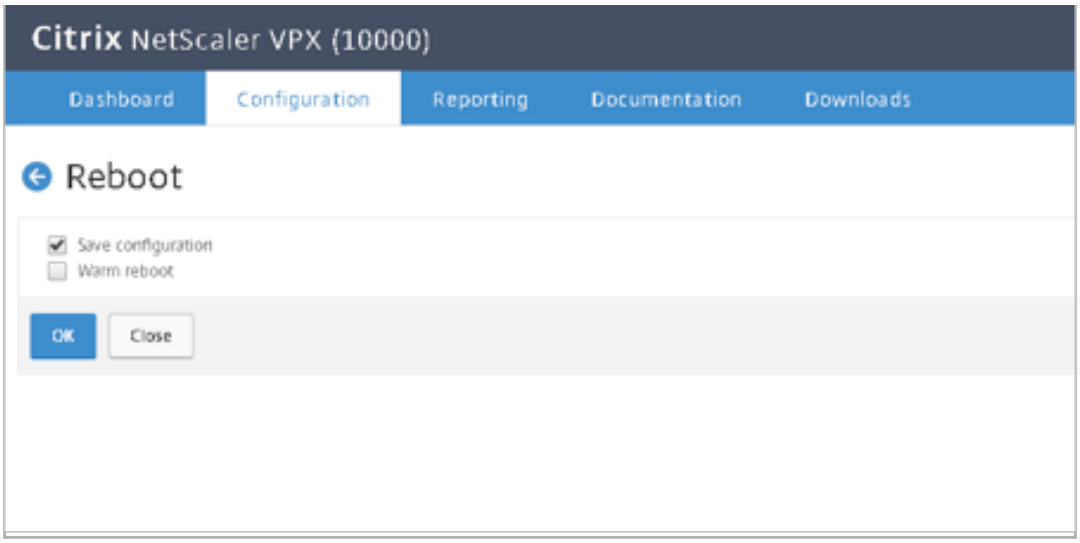
   c) 在“欢迎使用”页面上，单击“继续”。

   d) 在 配置选项卡上，单击 系统。

   e) 在“系统”页面上，单击“重新启动”。



f) 在 “ 重新启动” 页面上，选择 “ 热重新启动”，然后单击 “ 确定”。



处于高可用性模式的 Citrix ADC VPX 设备现已升级到 Citrix ADC 池容量许可证。

10. 要验证处于 HA 可用性模式的 Citrix ADC VPX 设备是否已升级到 Citrix ADC 池容量许可证，请登录到主 VPX 设备和辅助 VPX 设备，然后执行以下操作：

    a) 在 “ 欢迎使用” 页面上，单击 “ 继续”。

    b) 在 “配置” 选项卡上，导航到 **“系统” > “**许可证”，然后单击 “ 管理许可证”。在 “ 管理许可证” 页面上，可以查看许可证服务器、许可证版本和分配带宽的详细信息。

将 **Citrix ADC MPX** 中的永久许可证升级到 **Citrix ADC** 池容量

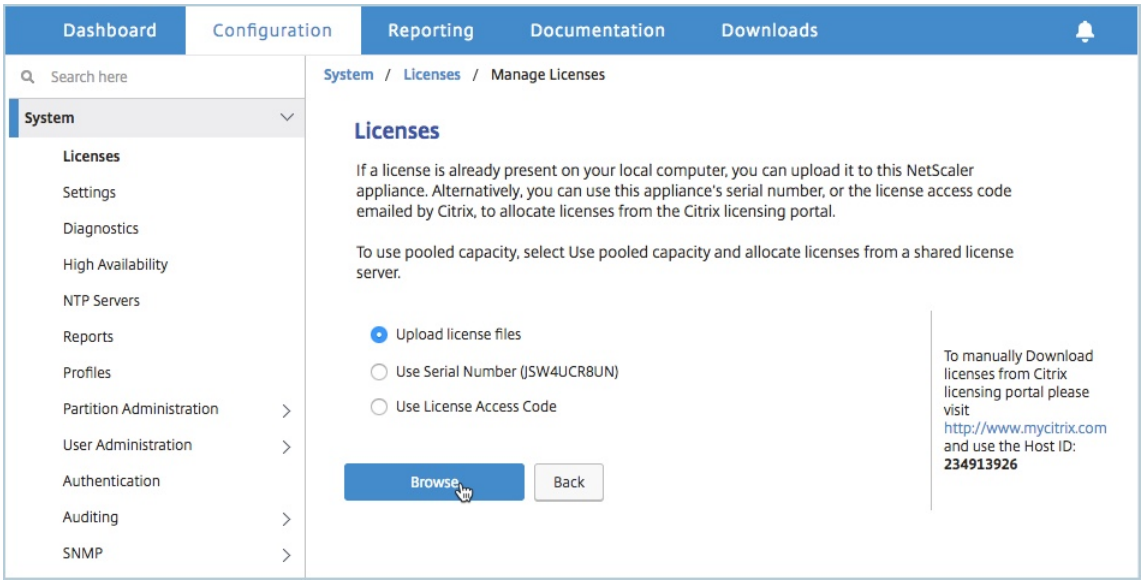
April 23, 2021

具有永久许可证的 Citrix ADC MPX 装置可升级到 Citrix ADC 池容量许可证。升级到 Citrix ADC 池容量许可证允许您按需将许可证池中的许可证分配给 Citrix ADC 设备。您还可以为在高可用性模式下配置的 Citrix ADC 实例配置 Citrix ADC 池容量许可证。要在高可用性模式下为 Citrix ADC MPX 实例配置 Citrix ADC 池容量许可证，请参阅将 Citrix ADC MPX 高可用性对中的永久许可证升级到 Citrix ADC 池容量。

> 注意
>
> 从永久许可证转换为池容量许可证是一个单向许可证授权过程。您不能将池容量许可证恢复为永久容量许可证。
>
> 重要
>
> 要将 Citrix ADC MPX 装置升级到 Citrix ADC 池容量许可证，您需要将 MPX-Z 许可证上传到该装置。

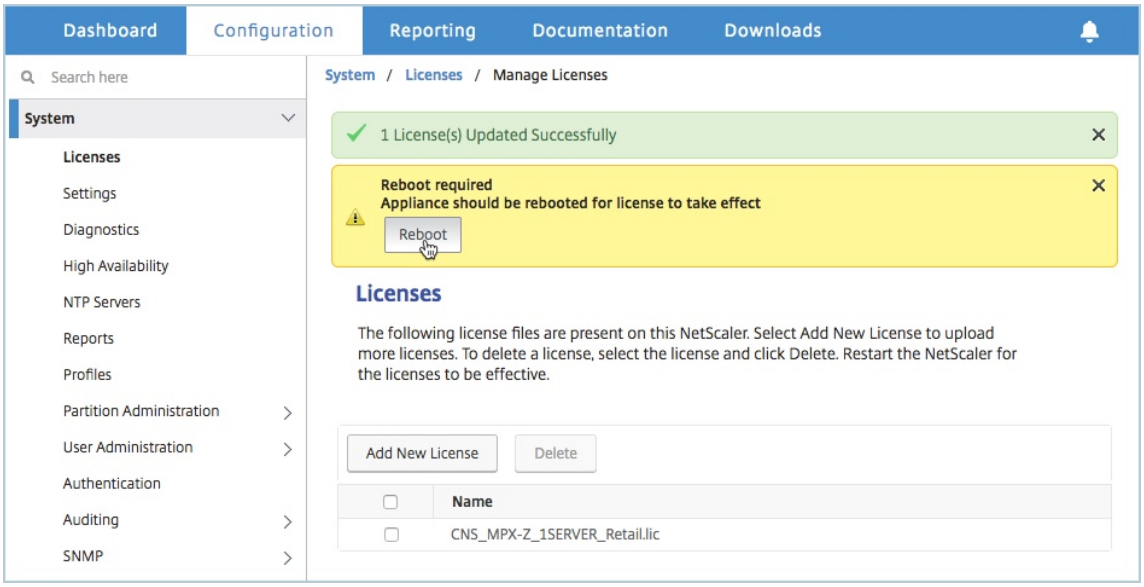
要升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，如 http://192.168.100.1。
2. 在“ 用户名” 和“ 密码” 字段中，键入管理员凭据。
3. 在“ 欢迎使用” 页面上，单击“ 继续”。
4. 上传零容量许可证（MPX-Z 许可证）。在“配置” 选项卡上，导航到“ 系统” > “ 许可证”。
5. 在详细信息窗格中，单击 管理许可证，单击添加 新许可证。
6. 在“ 许可证” 页面中，选择“ 上传许可证文件”，然后单击“ 浏览” 以从本地计算机中选择零容量许可证。

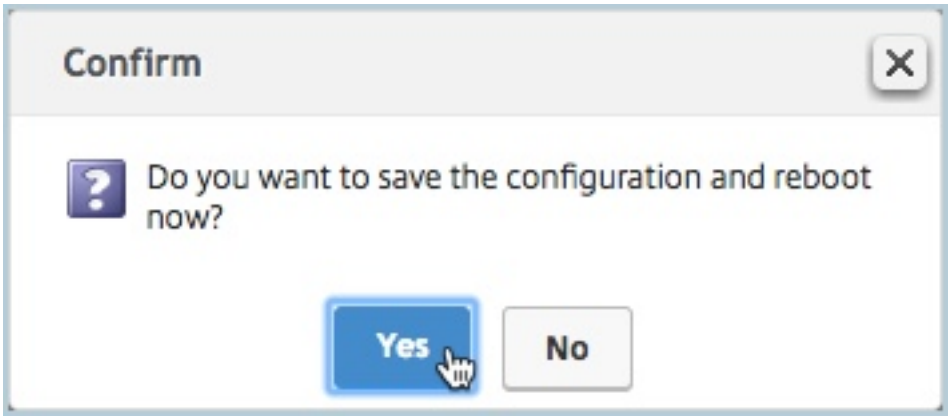


7. 上传许可证后，单击 重新启动以重新启动设备。

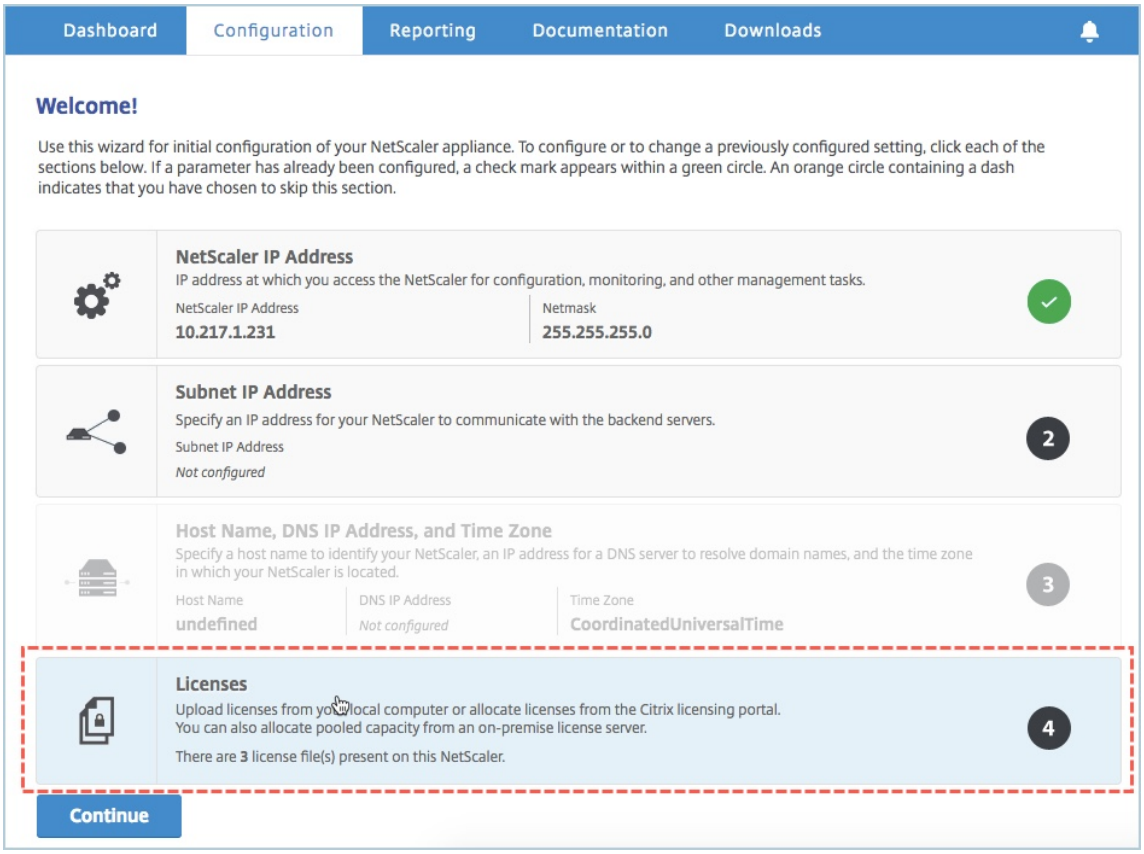
> 警告应用 MPX-Z 许可证
>
> 后，装置上包括 SSL 卸载在内的功能将变为未授权。设备停止处理 HTTPS 请求。
>
> 如果在升级之前在装置上启用了“ 仅安全访问” 选项，则无法使用 HTTPS 通过 Citrix ADM GUI 连接到装置。



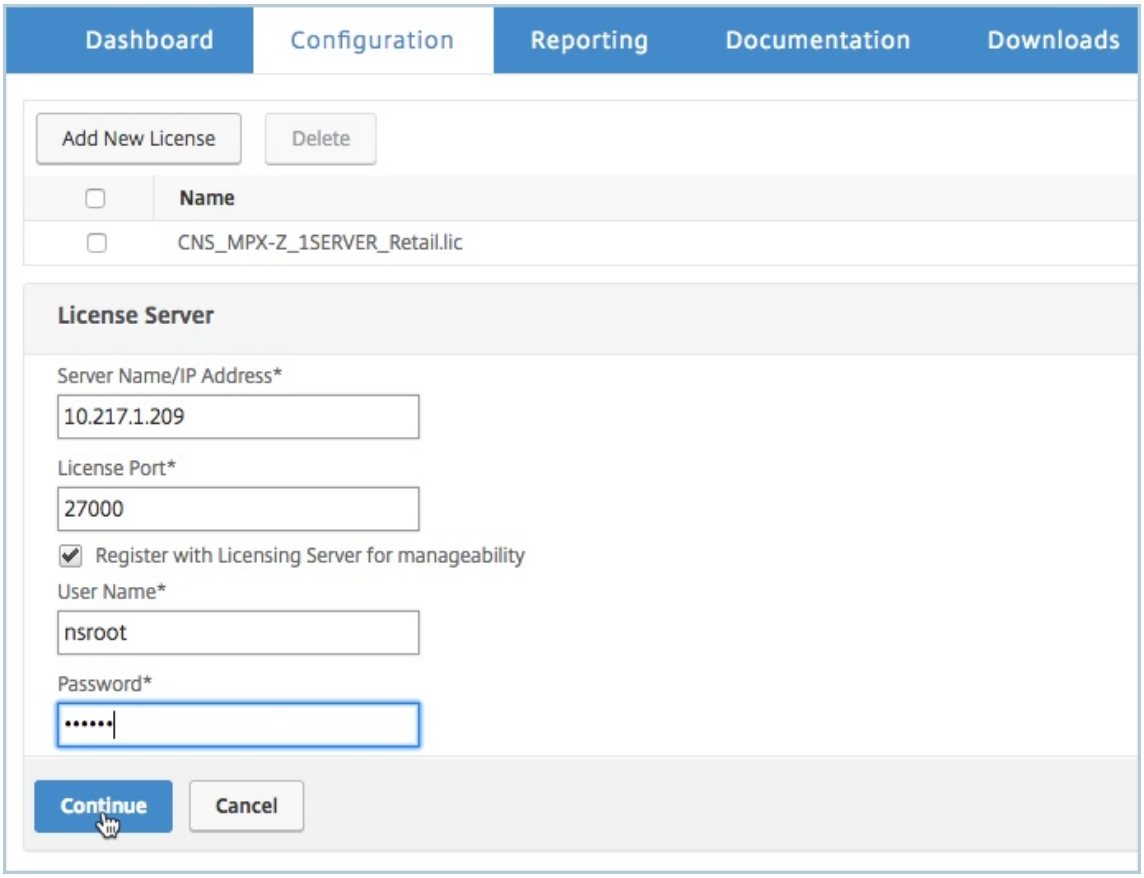
8. 在 “ 确认 ” 页上，单击 “ 是 ”。



9. 装置重新启动后，登录到装置。
10. 在欢迎页面上，单击 许可证部分。



11. 在“许可证服务器”部分中，执行以下操作：



a) 在“ 服务器名称 **/IP** 地址” 字段中，输入许可证服务器详细信息。

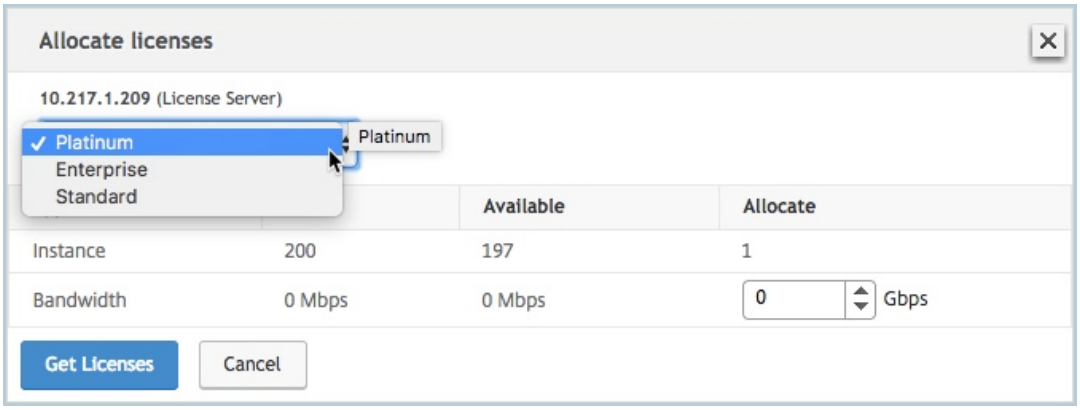
b) 在 许可证端口字段中，输入许可证服务器端口。默认值：27000。

c) 如果要通过 Citrix ADM 管理实例的池许可证，请选中向 许可服务器注册以便可管理性复选框，然后输入 ADM 凭证。

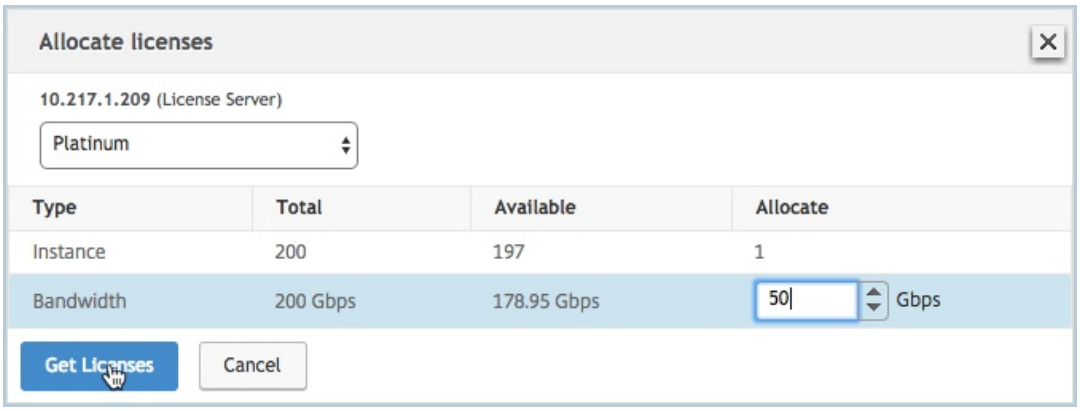
d) 单击继续。

12. 在“ 分配许可证” 窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。

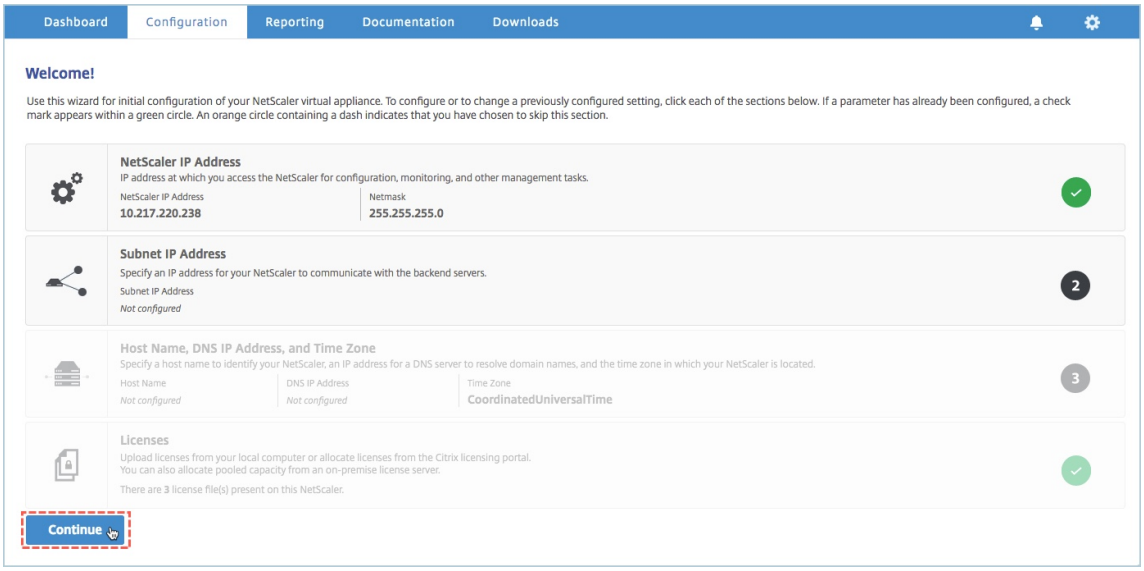


b) 从“分配”菜单将带宽分配 给 Citrix ADC 装置，然后单击 “ 获取许可证”。

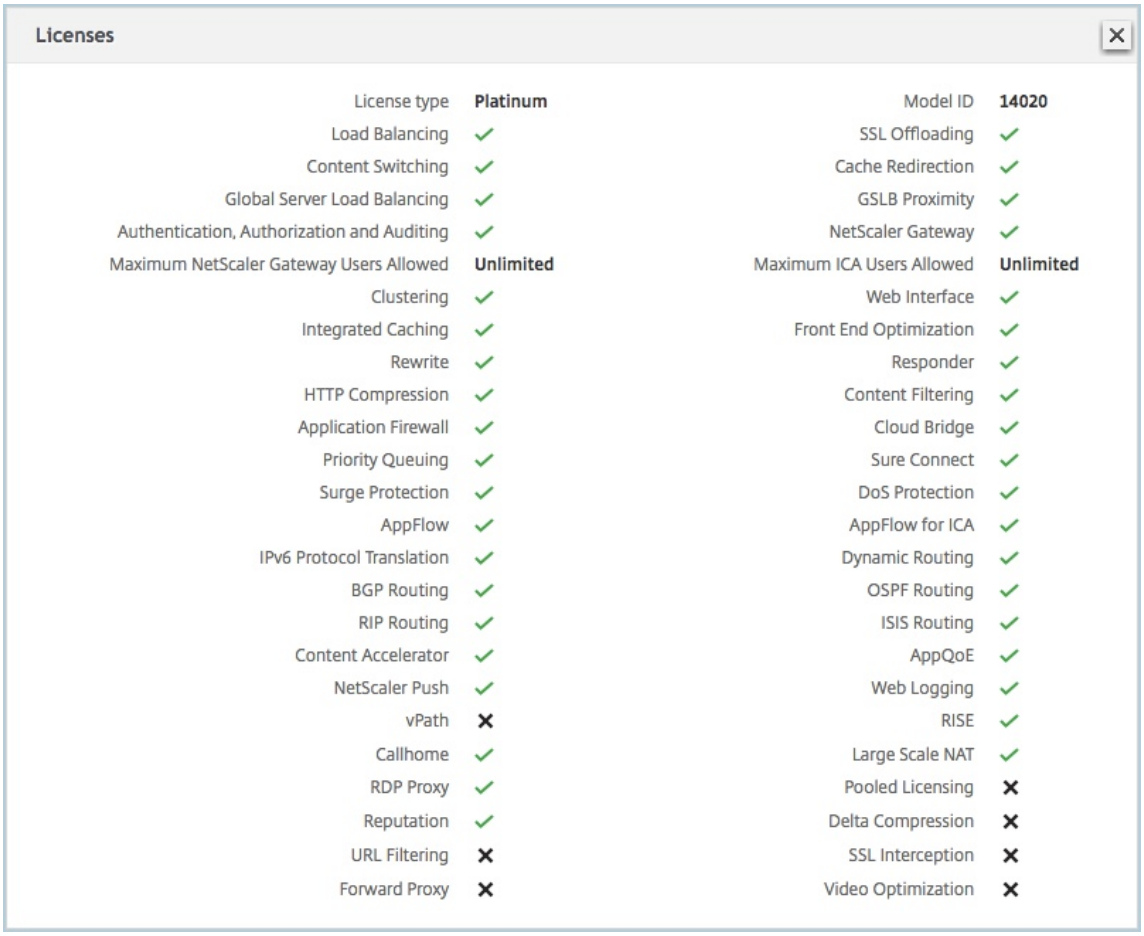


c) 出现提示时，单击 重新启动以重新启动装置。

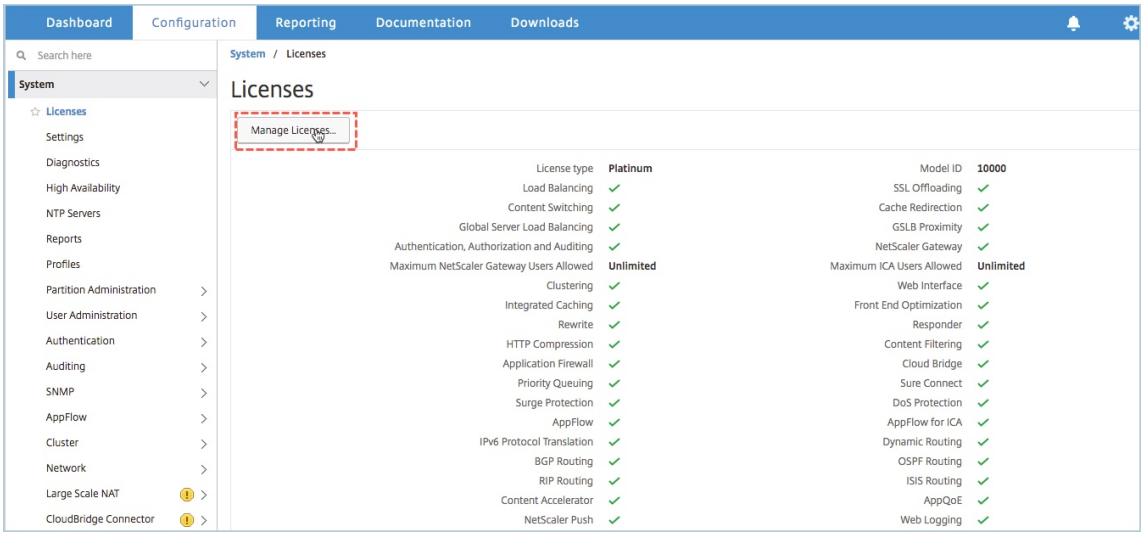
13. 一旦 Citrix ADC MPX 装置重新启动，请登录到 Citrix ADC MPX 装置。在 “ 欢迎使用”页面上，单击 “ 继续”。



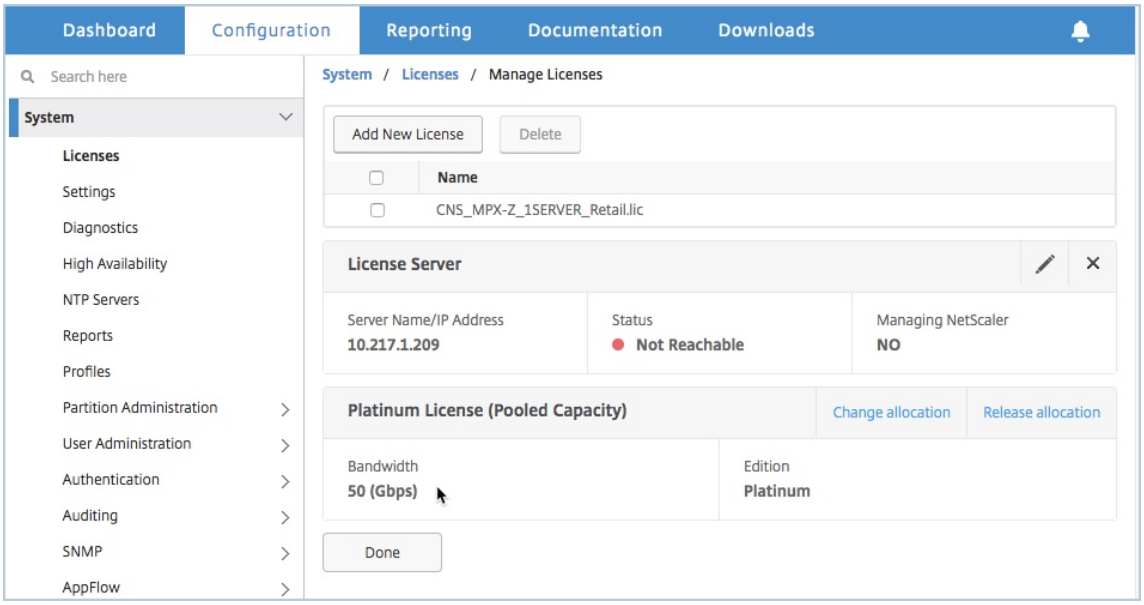
“ 许可证”页面列出了所有已许可的功能。



14. 导航到 **“系统” > “许可证”**，然后单击 “ 管理许可证”。



在 “ 管理许可证” 页面上，可以查看许可证服务器、许可证版本和分配带宽的详细信息。



将 **Citrix ADC MPX** 高可用性对中的永久许可证升级到 **Citrix ADC** 池容量

对于在高可用性模式下配置的 Citrix ADC MPX 设备，您必须在 HA 对中的主 Citrix ADC 实例和辅助 Citrix ADC 实例上配置 Citrix ADC 池容量。您需要将相同容量的许可证分配给 HA 对中的主 Citrix ADC 实例和辅助实例。例如，如果您希望高可用性对中的每个实例提供 1 Gbps 容量，则需要从公共池中分配 2 Gbps 容量，以便您可以为高可用性对中的主要和辅助 Citrix ADC 实例分配 1 Gbps 容量。

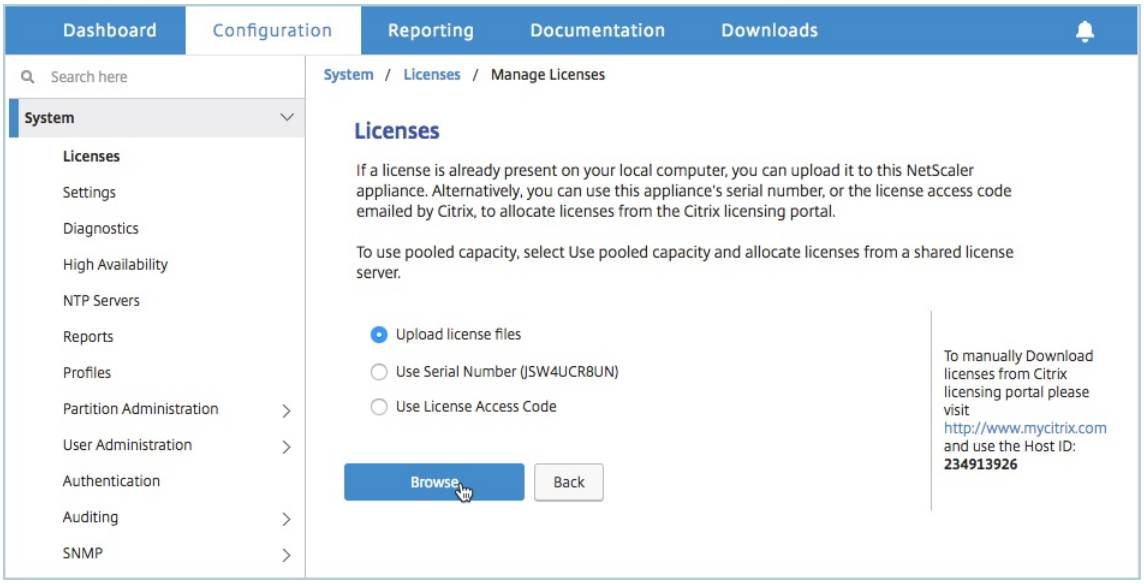
> 重要
>
> 要将 Citrix ADC MPX 装置升级为使用 Citrix ADC 池容量许可证，您需要将 MPX-Z 上传到装置。

必备条件

确保将 MPX-Z 许可证上传到 HA 对中的主实例和辅助实例。

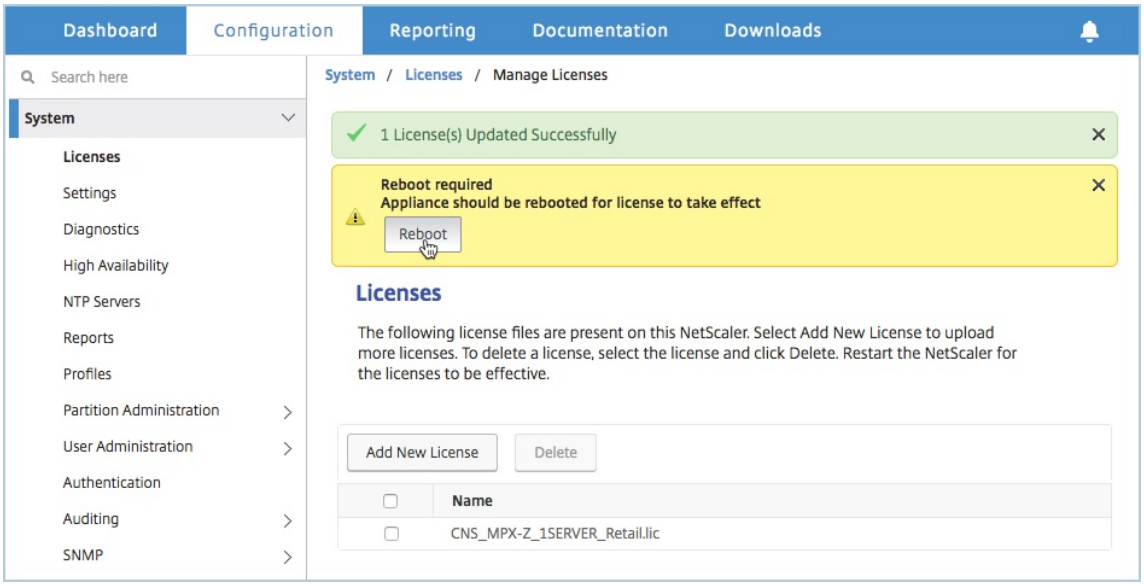
要将 **MPX-Z** 许可证上传到 **HA** 对中的 **Citrix ADC MPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入设备的 IP 地址，如 http://192.168.100.1。
2. 在“ 用户名”和“ 密码”字段中，键入管理员凭据。
3. 在“ 欢迎使用”页面上，单击“ 继续”。
4. 上传零容量许可证（MPX-Z 许可证）。在 **Configuration**（配置）选项卡上，导航到 **System**（系统）> **Licenses**（许可证）。
5. 在详细信息窗格中，单击 管理许可证，单击 添加新许可证。
6. 在“ 许可证”页面中，选择“ 上传许可证文件”，然后单击“ 浏览”以从本地计算机中选择零容量许可证。

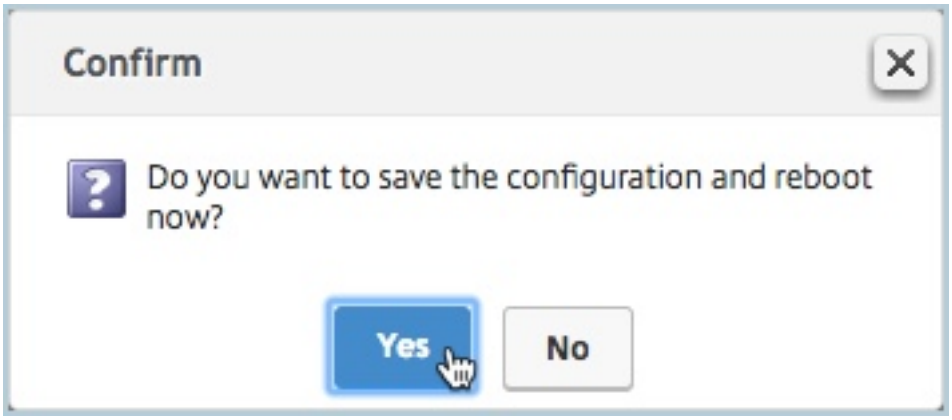


上传许可证后，系统会提示您重新启动设备。

7. 单击“ 重新启动”以重新启动装置。

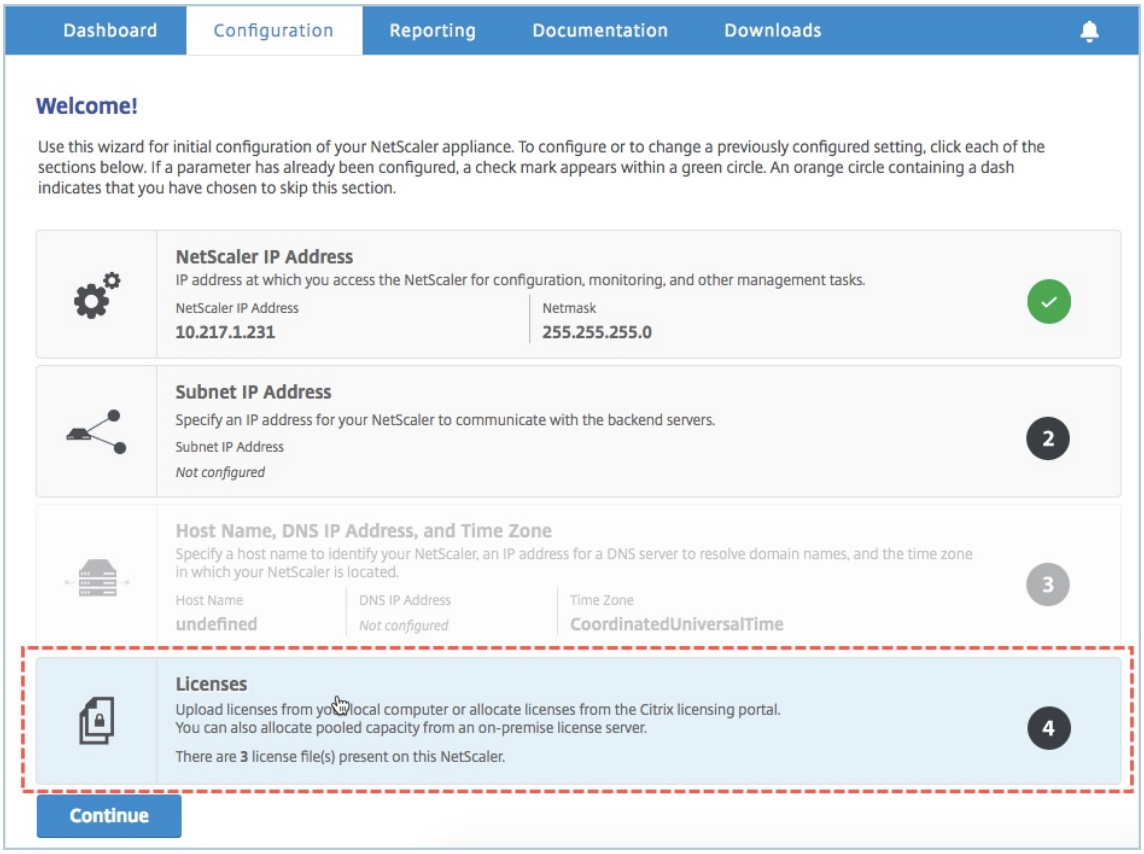


8. 在“ 确认”页上，单击“ 是”。

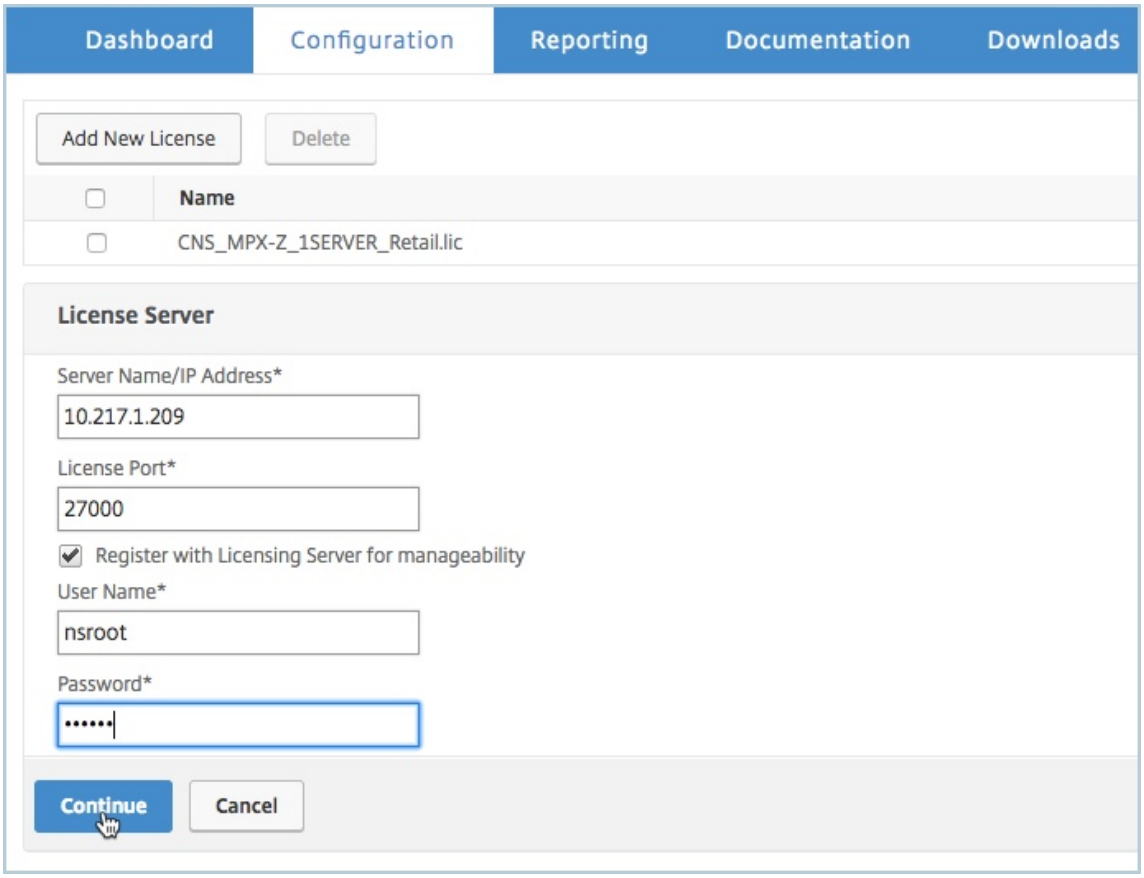


要将现有的 **HA** 设置升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 登录到辅助 Citrix ADC MPX 实例。在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，如 http://192.168.100.1。
2. 在“ 用户名”和“ 密码”字段中，键入管理员凭据。
3. 在 欢迎页面上，单击 许可证部分。



4. 在“ 许可证服务器”部分中，执行以下操作：



a) 在“ 服务器名称 **/IP** 地址” 字段中，输入许可证服务器详细信息。

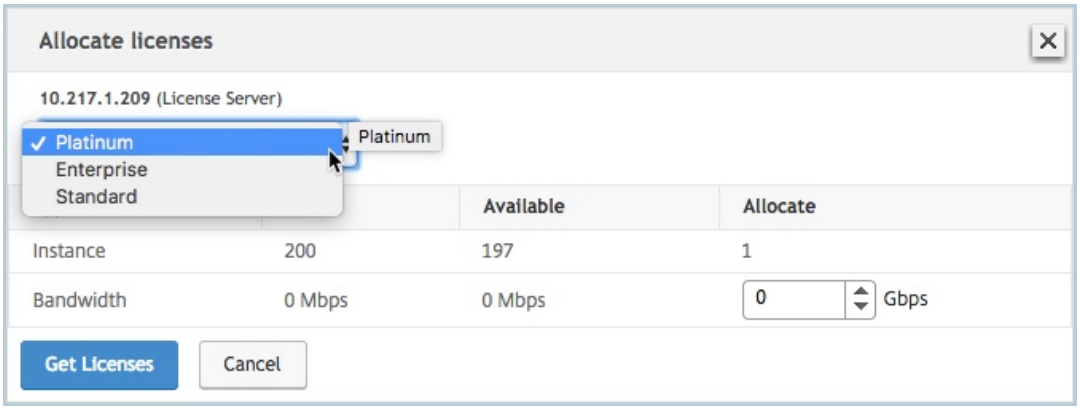
b) 在 许可证端口字段中，输入许可证服务器端口。默认值：27000。

c) 如果要通过 Citrix ADM 管理实例的池许可证，请选中向 许可服务器注册以便可管理性复选框，然后输入 ADM 凭证。

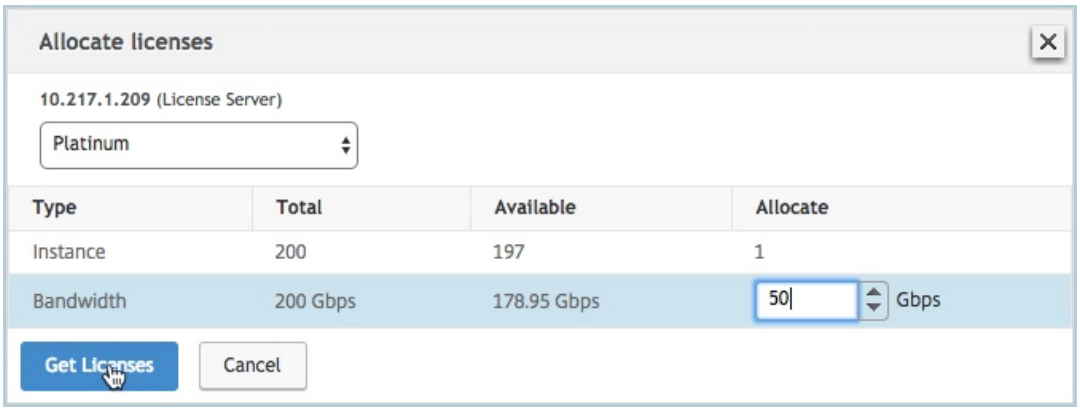
d) 单击继续。

5. 在“ 分配许可证” 窗口中，执行以下操作：

a) 从下拉列表中选择许可证版本。



b) 从“分配”菜单将带宽分配给 Citrix ADC 装置，然后单击“获取许可证”。



c) 出现提示时，单击 重新启动以重新启动装置。

辅助 Citrix ADC MPX 装置重新启动后，它将成为 HA 对中的主 Citrix ADC MPX 装置。

6. 登录现有主 Citrix ADC MPX 设备并重新启动设备。执行以下操作：

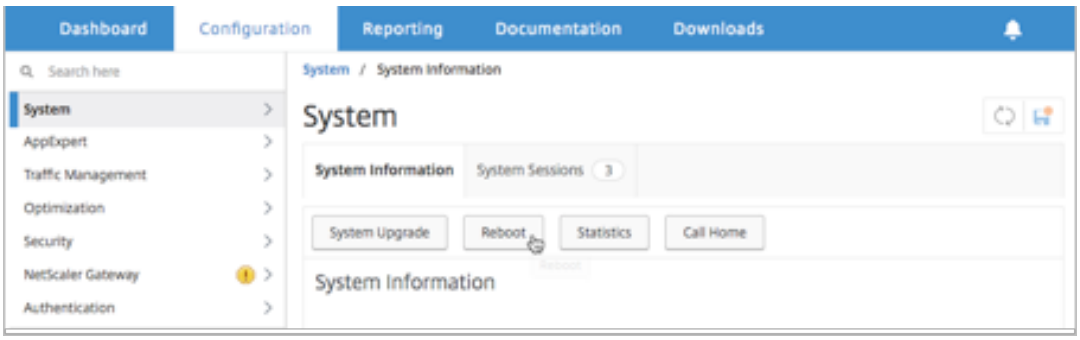
a) 在 Web 浏览器中，键入 Citrix ADC 设备的 IP 地址，如 http://192.168.100.1。

b) 在“用户名”和“密码”字段中，键入管理员凭据。

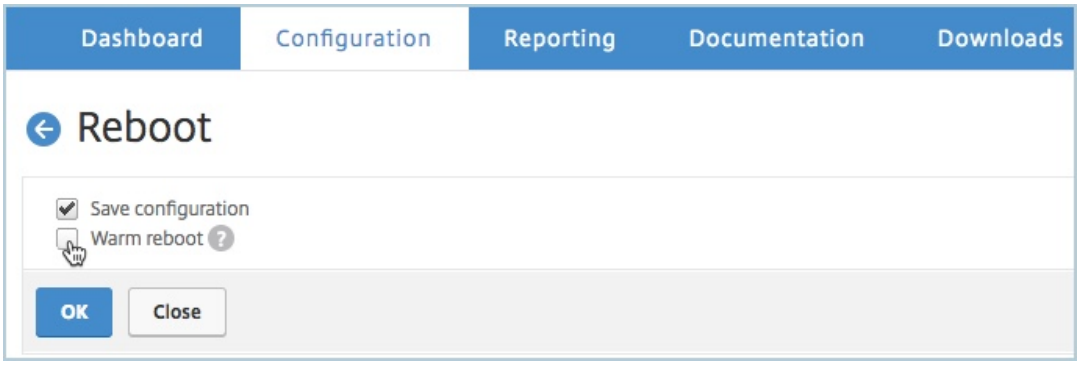
c) 在“欢迎使用”页面上，单击“继续”。

d) 在 配置选项卡上，单击 系统。

e) 在“系统”页面上，单击“重新启动”。



f) 在“重新启动”页面上，选择“热重新启动”，然后单击“确定”。



主 Citrix ADC MPX 装置重新启动后，它将成为 HA 对中的辅助 Citrix ADC MPX 装置。如果需要，您可以在 HA 对中的任何实例上使用以下命令，将 HA 对中的主实例和辅助实例更改为原始 HA 对配置：

```
> force ha failover
<!--NeedCopy-->
```

将 **Citrix ADC SDX** 中的永久许可证升级到 **Citrix ADC** 池容量

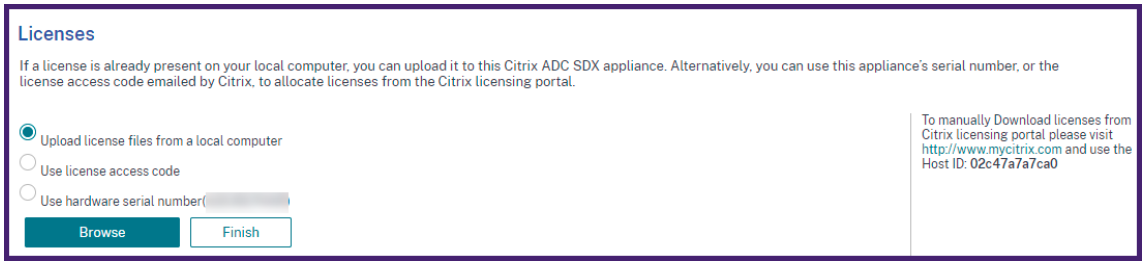
April 23, 2021

具有永久许可证的 Citrix ADC SDX 设备可以升级到 Citrix ADC 池容量许可证。升级到 Citrix ADC 池容量许可证允许您按需将许可证池中的许可证分配给 Citrix ADC 设备。您还可以为在高可用性模式下配置的 Citrix ADC 实例配置 ADC 池容量许可证。

> 注意
>
> 从永久许可证转换为池容量许可证是一个单向许可证授权过程。您不能将池容量许可证恢复为永久容量许可证。
>
> 重要
>
> - 要将 SDX 设备升级到 Citrix ADC 池容量许可证，必须将 SDX-Z 许可证上传到设备。
> - 确保您有权在 ADM 中添加 ADC 实例。

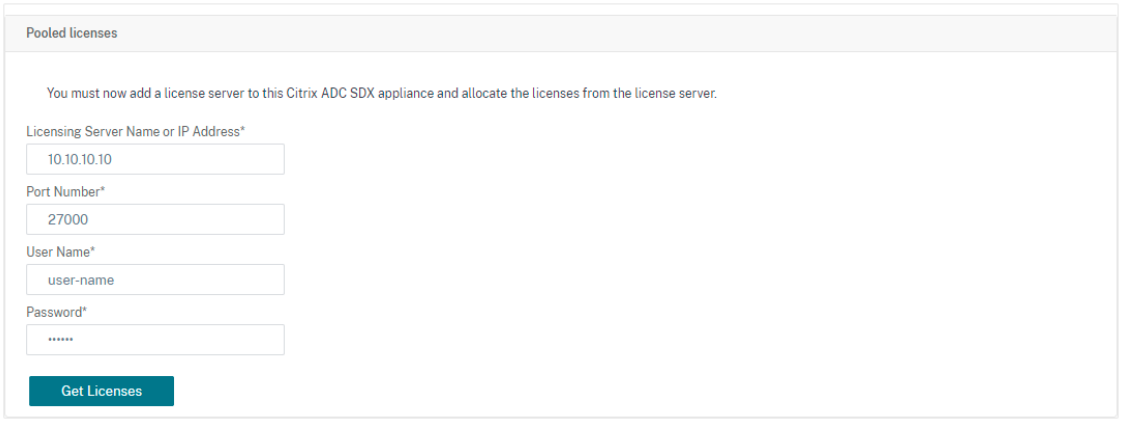
要升级到 **Citrix ADC** 池容量，请执行以下操作：

1. 在 Web 浏览器中，键入 SDX 设备的 IP 地址，例如 http://192.168.100.1。
2. 在 “ 用户名” 和 “ 密码” 字段中，键入管理员凭据。
3. 在 “ 欢迎使用” 页面上，单击 “ 继续”。
4. 上传零容量许可证。在 “配置” 选项卡上，导航到 “ 系统” > “ 许可证”。
5. 在 “ 管理许可证” 页面上，单击 “ 添加许可证文件”。
6. 在 “ 许可证” 页面中，选择 “ 从本地计算机上上传许可证文件”，然后单击 “ 浏览” 以从本地计算机中选择零容量许可证。然后，单击 “ 完成”。



成功应用零容量许可 证后，**“许可证”** 页面上将显示 **“池许可证”** 部分。

7. 在 池许可证部分中，执行以下操作：



a) 在 授权服务器名称或 **IP** 地址字段中，输入许可证服务器详细信息。

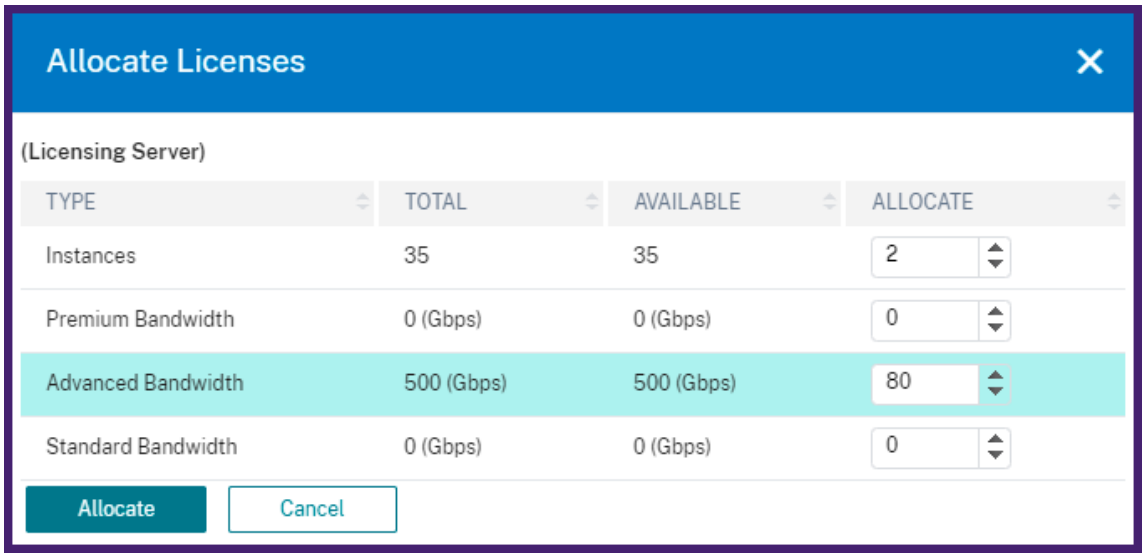
如果要将 ADM 服务器配置为许可证服务器，请指定 ADM 服务器的 IP 地址。

如果使用代理与 ADM 服务器通信，请指定 ADM 代理的 IP 地址。

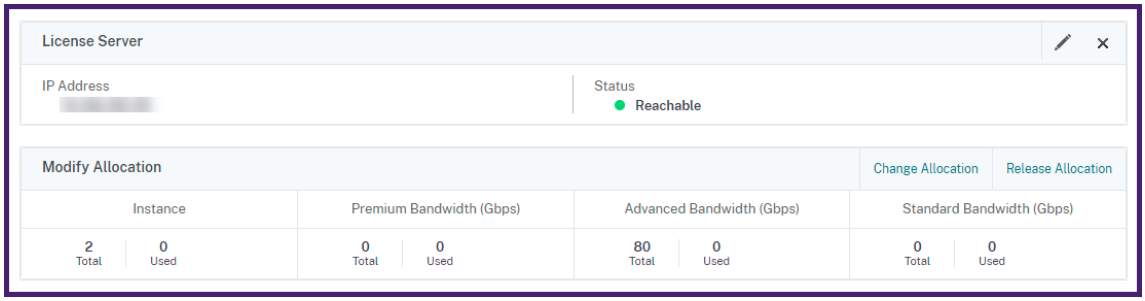
b) 在 端口号字段中，输入许可证服务器端口。默认值：27000。

c) 单击获取许可证。

8. 在 “ 分配许可证” 窗口中，指定所需的实例和带宽，然后单击 “ 分配”。



在 “ 管理许可证” 页面上，您可以查看许可证服务器、许可证版本以及池中分配的实例和带宽的详细信息。



> 注意
>
> 将永久许可证升级到池容量不需要重新启动 SDX 设备。

Citrix ADC 集群模式下的 Citrix ADC 池容量

April 23, 2021

您可以在配置为群集的 Citrix ADC 实例上配置 Citrix ADC 池容量。以下是在群集模式下在 Citrix ADC 实例上配置池容量的先决条件：

- 实例在池容量许可模式下单独运行以组成集群。
- 所有实例必须以相同的带宽运行。
- 所有实例都从同一 Citrix Application Delivery Management (ADM) 中检出了池容量。
- 除非新实例的容量和 Citrix ADM 配置与群集中现有实例的容量和 Citrix ADM 配置相同，否则无法将新实例添加到现有 Citrix ADC 群集中。

从 Citrix ADC 群集检出的任何容量都会为所有群集节点分配相同的容量，并且检出带宽 = 提供的带宽 * 节点数。

例如，如果从 Citrix ADC 群集中签出 50 Mbps 的带宽，并且该群集包括 12 个实例，则每个实例会自动收到 50 Mbps 的带宽。而且，600 Mbps 从游泳池中退出。

> 注意
>
> 如果群集中的一个或多个实例无响应，群集将继续以剩余实例的容量处理流量。

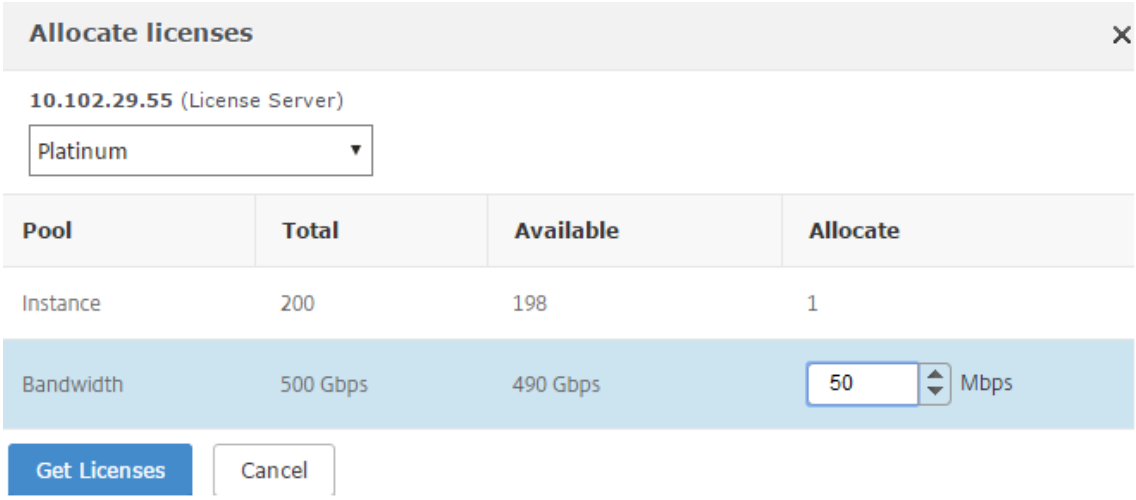
为 ADC 群集分配 ADC 池容量

将许可证分别分配给每个群集节点。因为禁用了跨群集节点传播和同步许可证的命令。

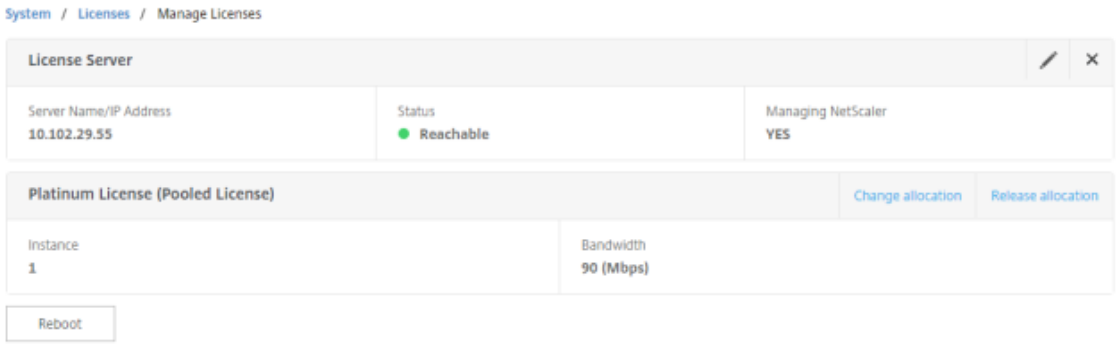
在每个群集节点上重复以下过程：

1. 在 Web 浏览器中，键入 Citrix ADC IP 地址 (NSIP)。例如 `http://192.168.100.1`。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在 “ 配置” 选项卡上，导航到 **“系统” > “许可证” > “管理许可证”**，单击 “ 添加新许可证**”**，然后选择 “ 使用池许可证”。

4. 在“服务器名称 **/IP** 地址**”** 字段中输入许可证服务器的名称或地址。
5. 如果要通过 Citrix ADM 管理实例的池许可证，请选中“向 **Citrix ADM** 注册以便可管理性”复选框，然后输入 ADM 凭证。
6. 选择许可证版本和所需的带宽，然后单击 获取许可证。

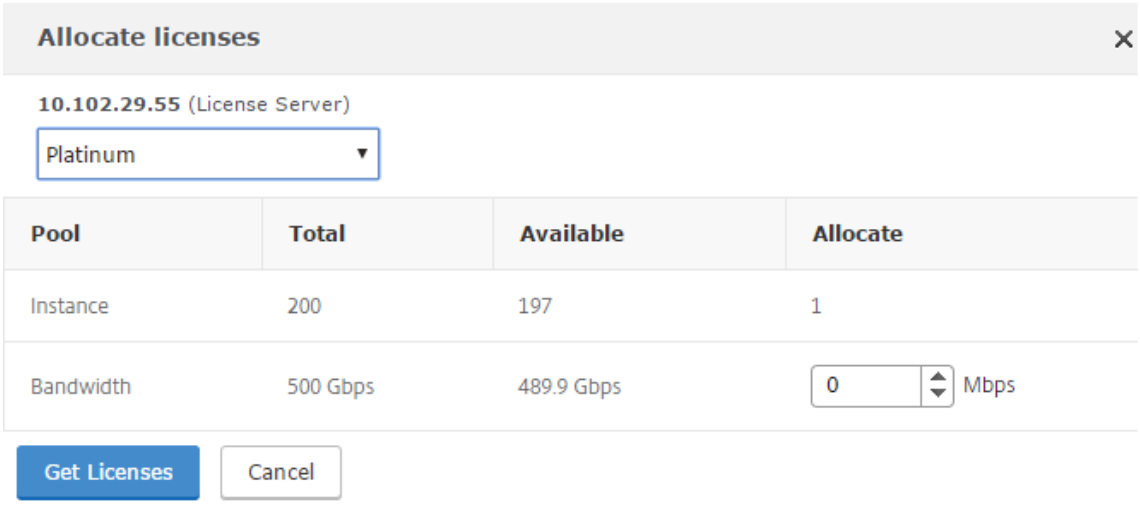


7. 您可以通过选择“更改分配”或“发布分配”来 更改或 释放许可证分配。



8. 如果单击 更改分配”，弹出窗口将显示许可证服务器上可用的许可证。

> 注意
>
> 带宽分配必须是对应尺寸规格的最低带宽单位的整数倍数。



9. 您可以从“分配”下拉列表中为 Citrix ADC 实例分 配带宽或实例。然后单击 获取许可证。
10. 您可以从弹出窗口中的下拉列表中选择许可证版本和所需的带宽。

> 注意
>
> 如果更改带宽分配，则不需要重新启动，但如果更改许可证版本，则需要热重新启动。

使用 **CLI** 将 **ADC** 池容量分配给 **ADC** 群集

将许可证分别分配给每个群集节点。因为禁用了跨群集节点传播和同步许可证的命令。

在每个群集节点上重复以下过程：

1. 在 SSH 客户端中，输入 Citrix ADC IP 地址 (NSIP)，然后使用管理员凭据登录。
2. 要添加许可服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. 要显示许可服务器上的可用许可证，请输入以下命令：

```
sh licenseserverpool
<!--NeedCopy-->
```



```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. 要为 Citrix ADC VPX 装置分配许可证，请输入以下命令：

```
set capacity  -platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

运行状况监视

April 23, 2021

许可证服务器会持续监视启用 Citrix ADC 集容量的实例的运行状况。实例定期向许可证服务器发送消息。如果连续几次未收到消息，则许可证服务器报告失去了连接。

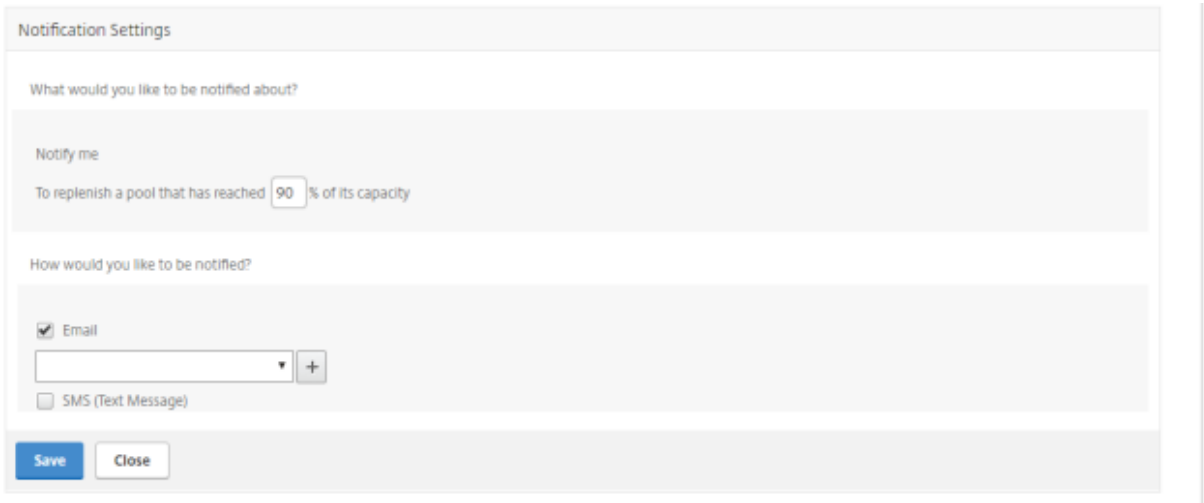
您可以创建自定义通知以补充默认的警报。

宽限期

当启用了 Citrix ADC 集容量的实例处于正常状态并且许可证服务器停止响应时，该实例将继续以当前容量运行 30 天。如果 30 天后没有恢复与许可证服务器的连接，则实例将失去其容量并停止处理流量。

通知和警报

可以通过 Citrix Application Delivery Management (ADM) 为对实例执行的任何操作启用通知。除了自定义通知设置外，默认情况下会配置以下警报。例如：要配置补充已耗尽一定百分比容量的池的警报，请导航到 “ 基础架构” > “ 许可证” > “设置” > “ 通知设置”，然后单击 “编辑” 按钮。



出现问题时的预期行为

April 23, 2021

以下是许可证服务器和 Citrix ADC 实例遇到所述问题时的预期行为：

许可证服务器停止响应

> 警告
>
> 许可证服务器没有响应。Citrix ADC 在当前容量下继续运行 30 天。30 天后，如果未恢复到许可证服务器的连接，Citrix ADC 将失去当前容量并停止处理流量。

如果许可证服务器停止响应，Citrix ADC 实例将进入宽限期，直到连接恢复为止。

启用 **Citrix ADC** 集容量的实例停止响应

如果启用了 Citrix ADC 集容量的实例停止响应，并且许可证服务器处于正常状态，则许可证服务器将在 10 分钟后检查所有 Citrix ADC 实例的许可证。实例重启时，它会发送请求，请求从许可服务器中查出所有许可证。

许可证服务器和启用 **Citrix ADC** 集容量的实例都停止响应

如果许可证服务器和启用 Citrix ADC 池容量的实例都重新启动并重新建立连接，则许可证服务器将在 10 分钟后签入其所有许可证，并且 Citrix ADC 池容量启用的实例会在重启完成后自动签出许可证。

启用 **Citrix ADC** 集容量的实例可以正常地关闭

在正常关闭过程中，您可以选择签入许可证或保留在正常关闭之前分配的许可证。如果您选择签入许可证，则 Citrix ADC 已启用池容量的实例在重新启动后将无许可。如果您选择保留许可证，则在实例关闭时将这些许可证签入许可服务器。实例重新启动后，它将与许可服务器重新建立连接，并签出保存的配置中指定的许可证。

如果系统重新启动且由于池中没有可用容量而导致签出失败，Citrix ADC 将检查 CitCitrix Application Delivery Management (ADM) 池许可证的清单并检出任何可用容量。如果 Citrix ADC 未按照配置以满容量运行，则会发出 SNMP 警报以通知用户此情况。如果带宽池中没有可用容量，则启用池容量的实例将变为未许可。

网络失去连接

> 错误消息（系统日志）
>
> 许可证服务器没有响应。

如果许可证服务器和启用 Citrix ADC 集容量的实例处于正常状态，但网络连接丢失，则这些实例将继续以其当前容量运行 30 天。30 天后，如果没有恢复与许可证服务器的连接，则实例将失去其容量并停止处理流量，且许可证服务器将签入其所有许可证。许可证服务器重新建立与 Citrix ADC 实例的连接后，这些实例将再次签出许可证。

配置池容量许可证的到期检查

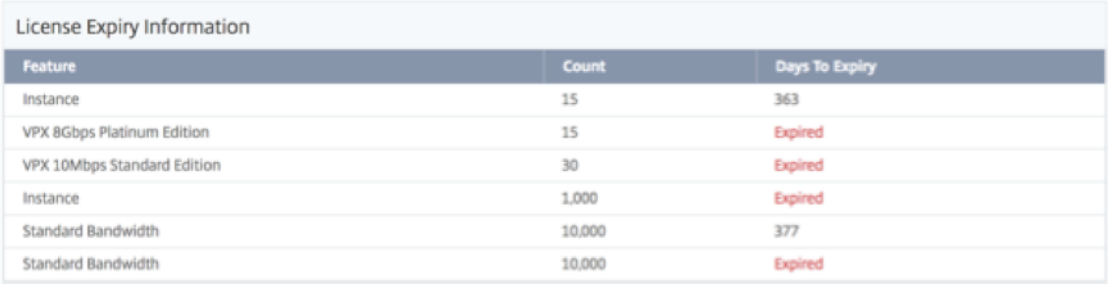
April 23, 2021

现在，您可以为 Citrix ADC 池容量许可证配置许可证到期阈值。通过设置阈值，Citrix Application Delivery Management (ADM) 在许可证即将过期时通过电子邮件或 SMS 发送通知。当 Citrix ADM 上的许可证过期时，还会发送 SNMP 陷阱和通知。

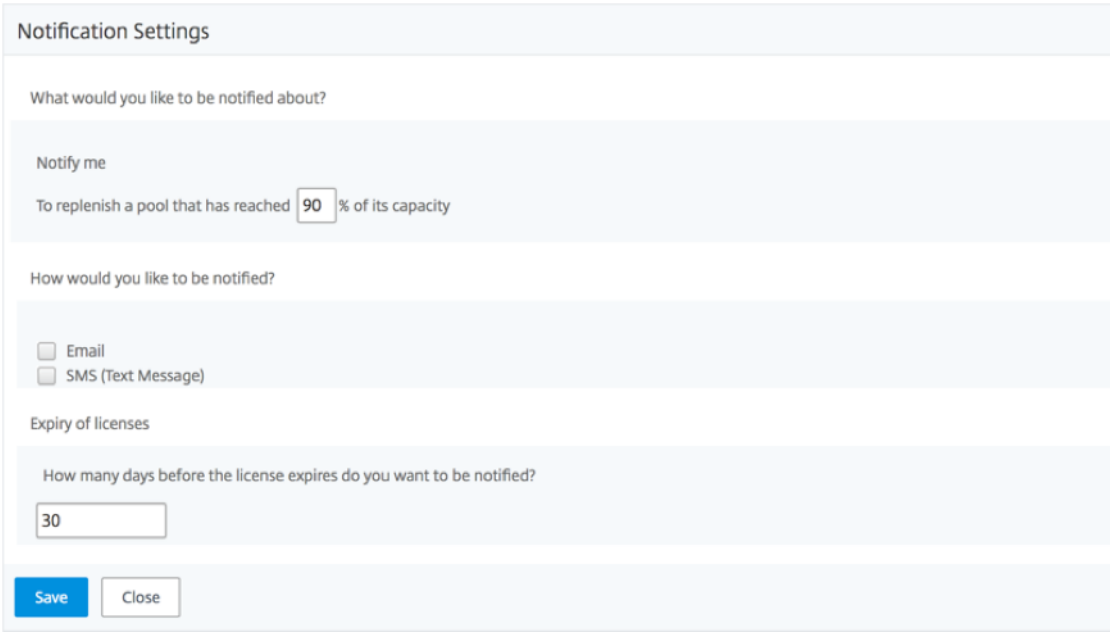
当发送许可证到期通知并且可以在 Citrix ADM 上查看此事件时，将生成一个事件。

要配置许可证到期检查，请执行以下操作：

1. 导航到“网络”>“许可证”。
2. 在“ 许可证设置”页面的“许可证到期信息”部分下，您可以找到将要过期的许可证的详细信息：
    - 功能：即将过期的许可证类型。
    - 计数：将受影响的虚拟服务器或实例的数量。
    - 到期天数：许可证到期前的天数。



3. 在“通知设置”部分，单击“ 编辑”图标并指定警报阈值。您可以设置用于通知管理员的池许可证容量的百分比。
4. 通过选中相应的复选框，选择要发送的通知类型。通知类型如下：
   a) 电子邮件配置文件：指定邮件服务器和配置文件详细信息。当您的许可证即将过期时，将触发电子邮件。
   b) **SMS** 配置文件：指定短消息服务 (SMS) 服务器和配置文件详细信息。当您的许可证即将过期时，会触发 SMS 消息。



5. 然后，根据许可证到期前的天数指定要发送通知的时间。
6. 单击保存。

> 注意
>
> 向池中添加新许可证时，Citrix ADC 实例会在其现有许可证到期时使用新许可证。

Citrix ADC VPX 签入和签出许可

April 23, 2021

您可以通过 Citrix Application Delivery Management (ADM) 按需将 VPX 许可证分配给 Citrix ADC VPX 实例。ADM 软件存储和管理许可证，许可证具有提供可扩展和自动化许可证 Provisioning 的许可证框架。在预配 Citrix ADC VPX 实例时，Citrix ADC VPX 实例可以从 Citrix ADM 中签出许可证。当实例被删除或销毁时，实例将其许可证重新检回到 Citrix ADM 软件。

必备条件

请务必满足以下必备条件：

- 您正在使用运行软件版本 12.0 的 Citrix ADC VPX 映像。
  例如：NSVPX-ESX-12.0-xx.xx_nc.zip
- 您已安装运行版本 12.0 的 Citrix ADM。
  例如：MAS-ESX-12.0-XX.xx.zip

> 注意
>
> 要通过 Citrix ADM 管理现有 VPX 许可证，您需要将许可证重新托管到 Citrix ADM。

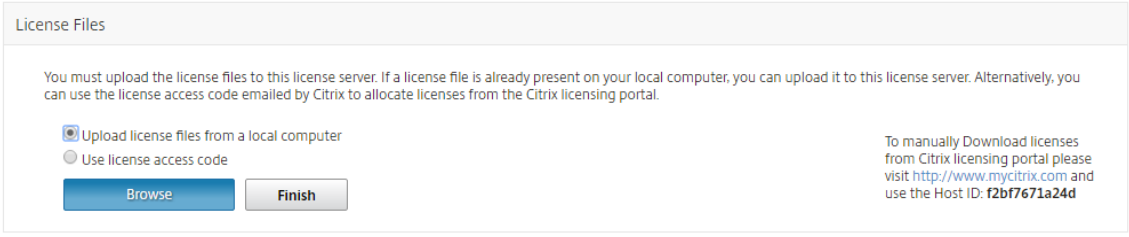
在 **Citrix ADM** 中安装许可证

> 注意：
>
> 在安装许可证之前，如果您更改了软件版本或带宽，请重新启动 Citrix ADM 虚拟设备。

要在 **Citrix ADM** 上安装许可证文件，请执行以下操作：

1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 User Name（用户名）和 Password（密码）中，输入管理员凭据。
3. 导航到 “ 网络” > “ 许可证”。
4. 在 “许可证文件” 部分，选择以下选项之一：
   - 从本地计算机上传许可证文件-如果本地计算机上已存在许可证文件，则可以将其上传到 Citrix ADM。
     要添加许可证文件，请单击 浏览，然后选择要添加的许可证文件 (.lic)。然后单击 “ 完成”。
   - 使用许可证访问代码 -Citrix 通过电子邮件发送您购买的许可证访问代码。
     要添加许可证文件，请在文本框中输入许可证访问代码，然后单击 获取许可证。

   > 注意
   >
   > 在使用许可证访问代码安装许可证之前，请确保您已连接到 Internet。



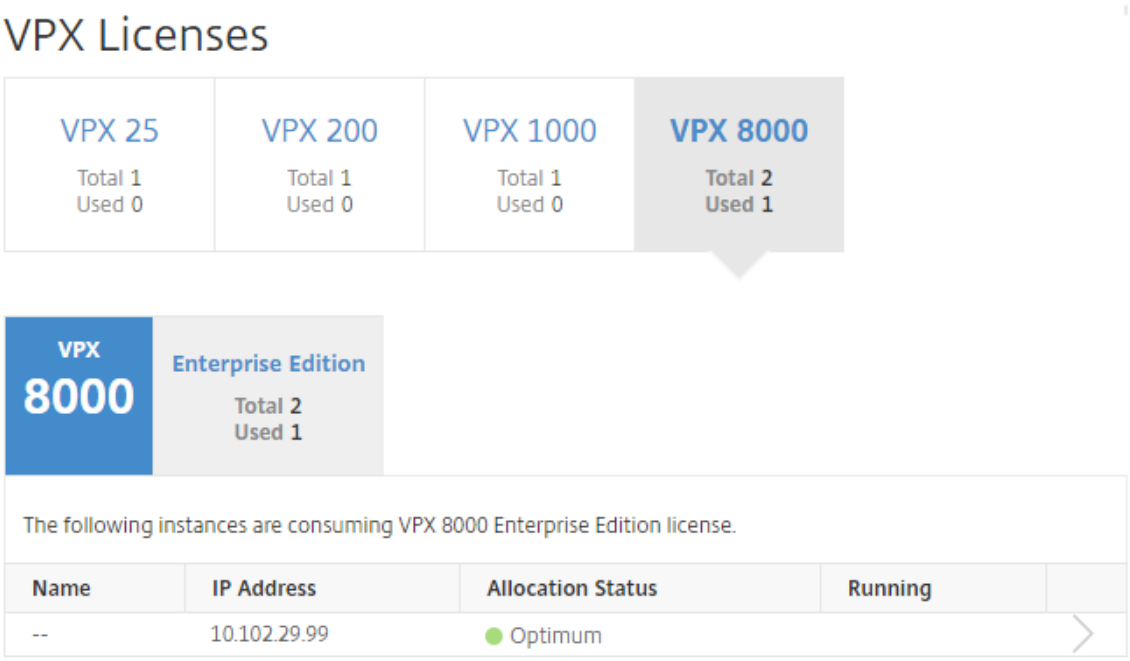
您可以随时从许可证设置向 Citrix ADM 添加更多许可证。

验证

您可以在 Citrix ADM GUI 中查看可用和已分配的许可证。

要显示许可证，请执行以下操作：

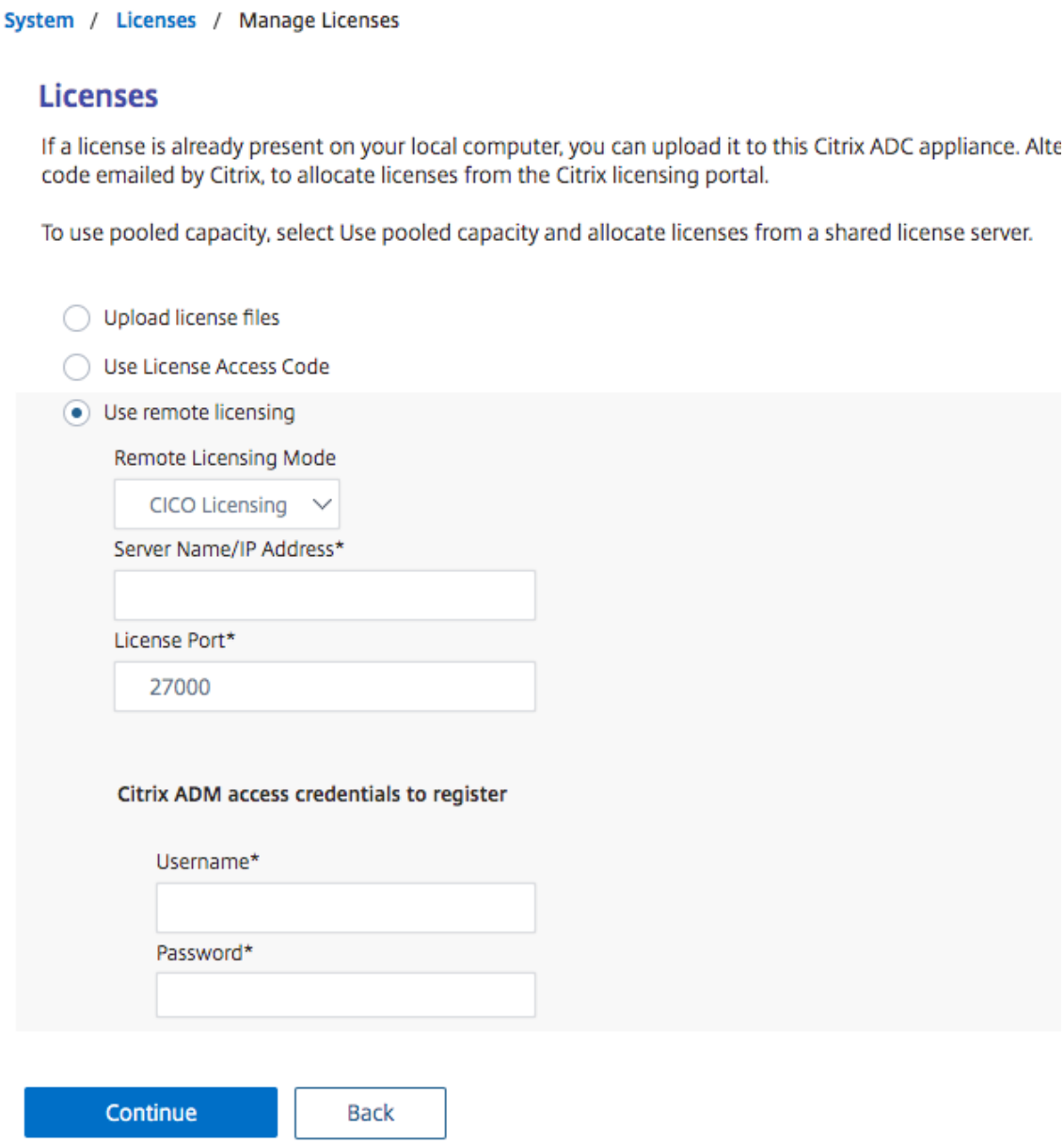
1. 在 Web 浏览器中，键入 Citrix ADM 的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“网络”>“许可证”>“**VPX** 许可证”。



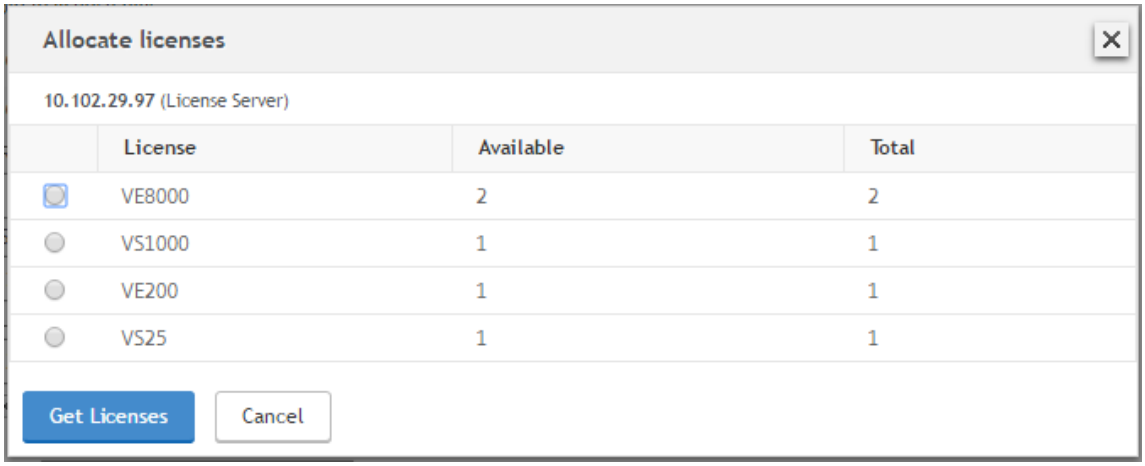
4. 您可以在可用许可证部分下的表中查看分配的许可证。

使用 **Citrix ADC GUI** 将 **VPX** 许可证分配到 **Citrix ADC VPX** 实例

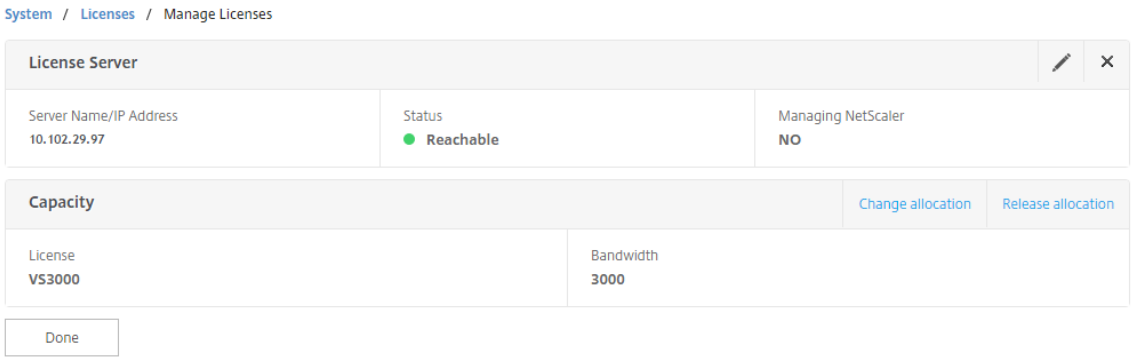
1. 在 Web 浏览器中，键入 Citrix ADC 实例的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在配置选项卡上，导航到 系统 **>** 许可证 **>** 管理许可证，单击 添加新许可证，然后选择 使用远程许可证 **> CICO** 许可证。
4. 在“服务器 名称 **/IP** 地址”字段中输入许可证服务器的详细信息。
5. 在上面屏幕的“用户名”和“密码”字段中，输入 Citrix ADM 凭据，然后单击“继续”。



6. 选择具有所需带宽的许可证版本，单击 获取许可证。



7. 单击 “ 重新启动”，您的 Citrix ADC VPX 实例将重新启动。
8. 您可以通过导航到 “ 系统” > “ 许可证” > “管理许可证”，然后选择 “更改分配” 或 “发布 ** 分配” 来更改或释放许 ** 可证分配。



9. 如果单击 更改分配”，弹出窗口将显示许可证服务器上可用的许可证。选择所需的许可证，单击 获取许可证。

使用 **Citrix ADC CLI** 将 **VPX** 许可证分配到 **Citrix ADC VPX** 实例

1. 在 SSH 客户端中，输入 Citrix ADC 实例的 IP 地址，然后使用管理员凭据登录。

2. 要添加许可服务器，请输入以下命令：

```
add ns licenseserver (<licenseServerIP> | <serverName>) [-port <
    port number >]
<!--NeedCopy-->
```

```
> add ns licenseserver 10.102.29.97 -port 27000
 Done
```

3. 要显示许可服务器上的可用许可证，请输入以下命令：

```
sh licenseserverpool
<!--NeedCopy-->
```

```
> sh licenseserverpool
        Instance Total                  : 0
        Instance Available              : 0
        Standard Bandwidth Total        : 0 Mbps
        Standard Bandwidth Availabe     : 0 Mbps
        Enterprise Bandwidth Total      : 0 Mbps
        Enterprise Bandwidth Available  : 0 Mbps
        Platinum Bandwidth Total        : 0 Mbps
        Platinum Bandwidth Available    : 0 Mbps
        VPX25S Total                    : 1
        VPX25S Available                : 1
        VPX200E Total                   : 1
        VPX200E Available               : 1
        VPX1000S Total                  : 1
        VPX1000S Available              : 1
        VPX8000E Total                  : 2
        VPX8000E Available              : 1
 Done
```

4. 要为 Citrix ADC VPX 装置分配许可证，请输入以下命令：

```
set capacity  - platform V[S/E/P][Bandwidth]
<!--NeedCopy-->
```

```
> set capacity -platform VE8000
Warning: The configuration changes will not take effect until the system is rebooted
```

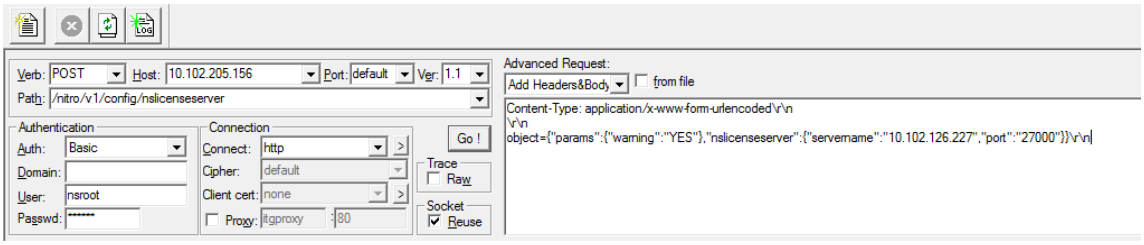
通过使用 **API** 将 **VPX** 许可证分配给 **Citrix ADC VPX** 实例

在 Web 浏览器或 API 客户端中，使用管理员凭据登录到 Citrix ADC VPX 实例。

要添加许可服务器，请执行以下操作：

1. 将请求类型设置为 “过 帐”。
2. 将路径设置为 /nitro/v1/config/nslicensingserver。
3. 按如下方式设置有效载荷：


```
content-type: application/x-www-form-urlencoded\r\n
\r\n
object= {
  “params” ;{
 warning” :” yes”  }
 ,” nslicensing server” ;{
 servername” :” <Citrix ADM IP>” ,  “port” :” 27000”  }
  }
 \r\n
<!--NeedCopy-->
```

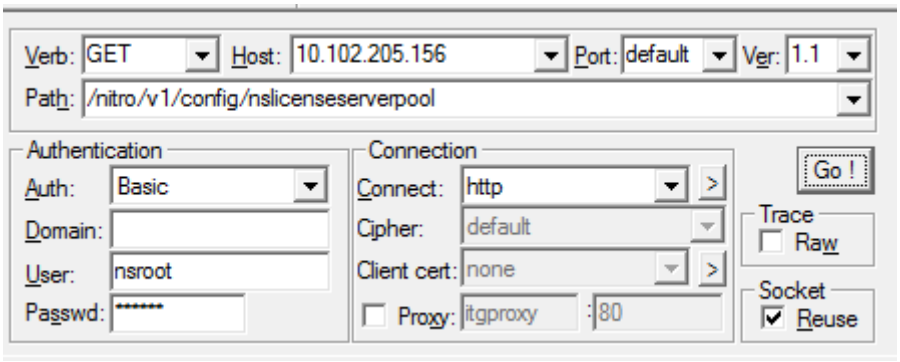


Citrix ADM 响应请求。以下示例响应显示成功。

```
RESPONSE: **********\n
HTTP/1.1 201 Created\r\n
Date: Fri, 06 Jan 2017 19:03:21 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 57\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE" }
finished.
```

要查看许可服务器上的可用许可证，请执行以下操作：

1. 将请求类型设置为 “ 获取”。
2. 将路径设置为 /nitro/v1/config/nslicenseserverpool



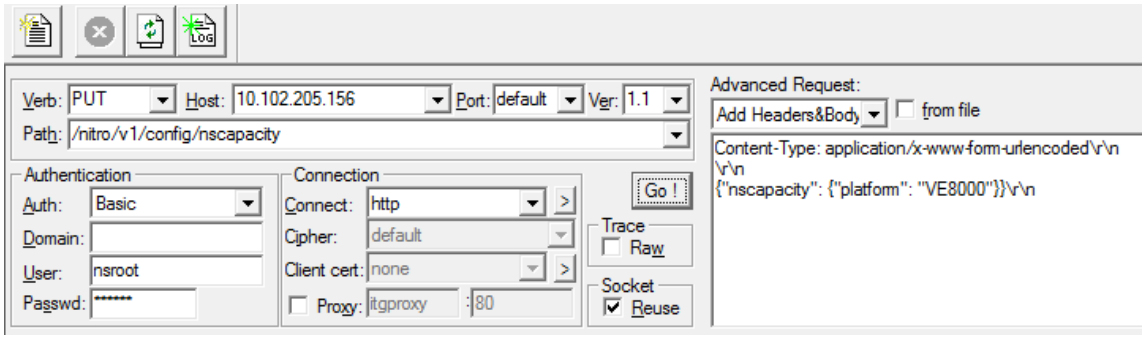
Citrix ADM 响应请求。以下示例响应显示成功，以及许可证服务器上的可用许可证列表。

RESPONSE: **********\n
HTTP/1.1 200 OK\r\n
Date: Fri, 06 Jan 2017 19:18:54 GMT\r\n
Server: Apache\r\n
Expires: Thu, 19 Nov 1981 08:52:00 GMT\r\n
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0\r\n
Pragma: no-cache\r\n
Content-Length: 1874\r\n
Content-Type: application/json; charset=utf-8\r\n
\r\n
{ "errorcode": 0, "message": "Done", "severity": "NONE", "nslicenseserverpool": { "instancetotal": 0, "instanceavailable": 0, "standardbandwidthtotal":
0, "standardbandwidthavailable": 0, "enterprisebandwidthtotal": 0, "enterprisebandwidthavailable": 0, "platinumbandwidthtotal": 0, "platinumbandwidthav
ailable": 0, "cpxinstancetotal": 0, "cpxinstanceavailable": 0, "vpx1stotal": 0, "vpx1savailable": 0, "vpx1ptotal": 0, "vpx1pavailable": 0, "vpx5stotal"
: 0, "vpx5savailable": 0, "vpx5ptotal": 0, "vpx5pavailable": 0, "vpx10stotal": 0, "vpx10savailable": 0, "vpx10etotal": 0, "vpx10eavailable": 0, "vpx10p
total": 0, "vpx10pavailable": 0, "vpx25stotal": 0, "vpx25savailable": 0, "vpx25etotal": 0, "vpx25eavailable": 0, "vpx25ptotal": 0, "vpx25pavailable": 0
, "vpx50stotal": 0, "vpx50savailable": 0, "vpx50etotal": 0, "vpx50eavailable": 0, "vpx50ptotal": 0, "vpx50pavailable": 0, "vpx100stotal": 0, "vpx100sav
ailable": 0, "vpx100etotal": 0, "vpx100eavailable": 0, "vpx100ptotal": 0, "vpx100pavailable": 0, "vpx200stotal": 0, "vpx200savailable": 0, "vpx200etota
l": 0, "vpx200eavailable": 0, "vpx200ptotal": 0, "vpx200pavailable": 0, "vpx500stotal": 0, "vpx500savailable": 0, "vpx500eto
tal": 0, "vpx500eavailable": 0, "vpx500ptotal": 0, "vpx500pavailable": 0, "vpx1000stotal": 0, "vpx1000savailable": 0, "vpx1000etotal": 0, "vpx1000eavail
able": 0, "vpx1000ptotal": 0, "vpx1000pavailable": 0, "vpx2000ptotal": 0, "vpx2000pavailable": 0, "vpx3000stotal": 0, "vpx3000savailable": 0, "vpx3000e
total": 0, "vpx3000eavailable": 0, "vpx3000ptotal": 0, "vpx3000pavailable": 0, "vpx4000ptotal": 0, "vpx4000pavailable": 0, "vpx5000stotal": 0, "vpx5000
savailable": 0, "vpx5000etotal": 0, "vpx5000eavailable": 0, "vpx5000ptotal": 0, "vpx5000pavailable": 0, "vpx8000stotal": 1, "vpx8000savailable": 1, "vp
x8000etotal": 2, "vpx8000eavailable": 1, "vpx8000ptotal": 1, "vpx8000pavailable": 1 } }
finished.

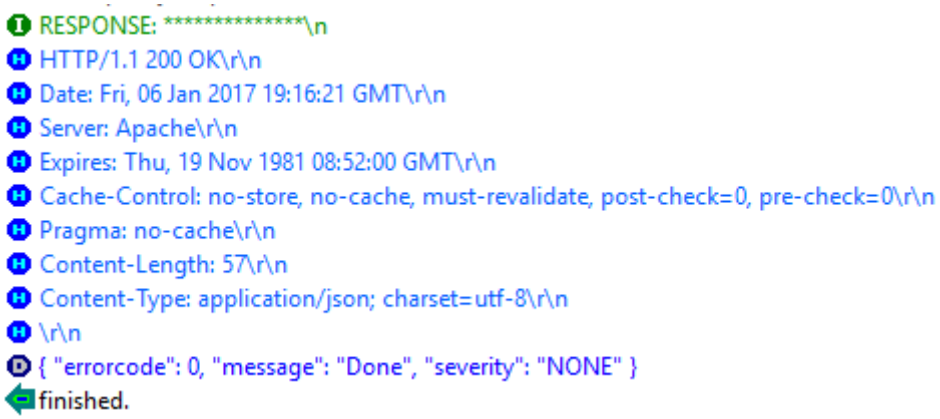
要将许可证分配给 **Citrix ADC VPX** 装置，请执行以下操作：

1. 将请求类型设置为 “过 帐”。
2. 将路径设置为 /nitro/v1/config/nscapacity。
3. 按如下方式设置有效载荷：

```
content-type: application/x-www-form-urlencoded\r\n
\r\n
{
  “nscapacity:{
  “platform” :” VE8000”  }
  }
 \r\n
<!--NeedCopy-->
```



Citrix ADM 响应请求。以下示例响应显示成功。



更新许可服务器 **IP** 地址

您可以更新 VPX 实例中的许可服务器 IP 地址，而不会对实例分配的许可证带宽和数据丢失产生任何影响。

使用 **CLI** 更新：要使用 CLI 更新许可服务器 IP 地址，请在 VPX 实例上键入以下命令：

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

此命令连接到新服务器并释放与之前许可服务器关联的资源。

使用 **GUI** 更新：要使用 GUI 更新许可服务器 IP 地址，请导航到 **“系统” > “许可证” > “管理许可证”**，单击 “ 添加新许可证” 有关详细信息，请参阅使用 Citrix ADC GUI 将 VPX 许可证分配到 Citrix ADC VPX 实例。

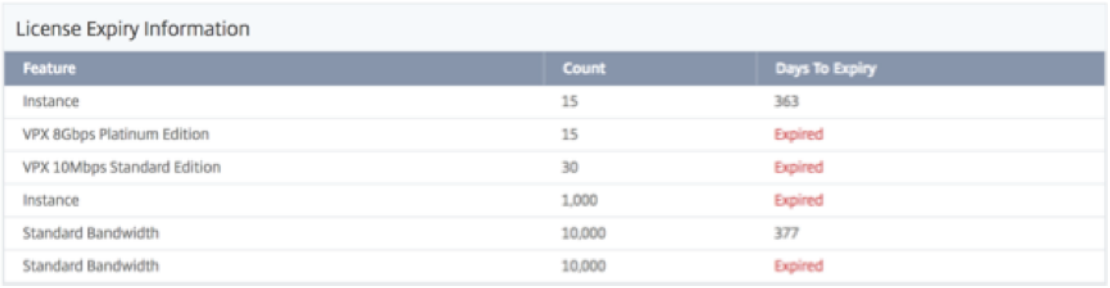
为 **Citrix ADC VPX** 登入/退出许可证配置过期检查

现在，您可以为 Citrix ADC VPX 许可证配置许可证到期阈值。通过设置阈值，Citrix ADM 在许可证即将到期时通过电子邮件或 SMS 发送通知。当 Citrix ADM 上的许可证过期时，还会发送 SNMP 陷阱和通知。

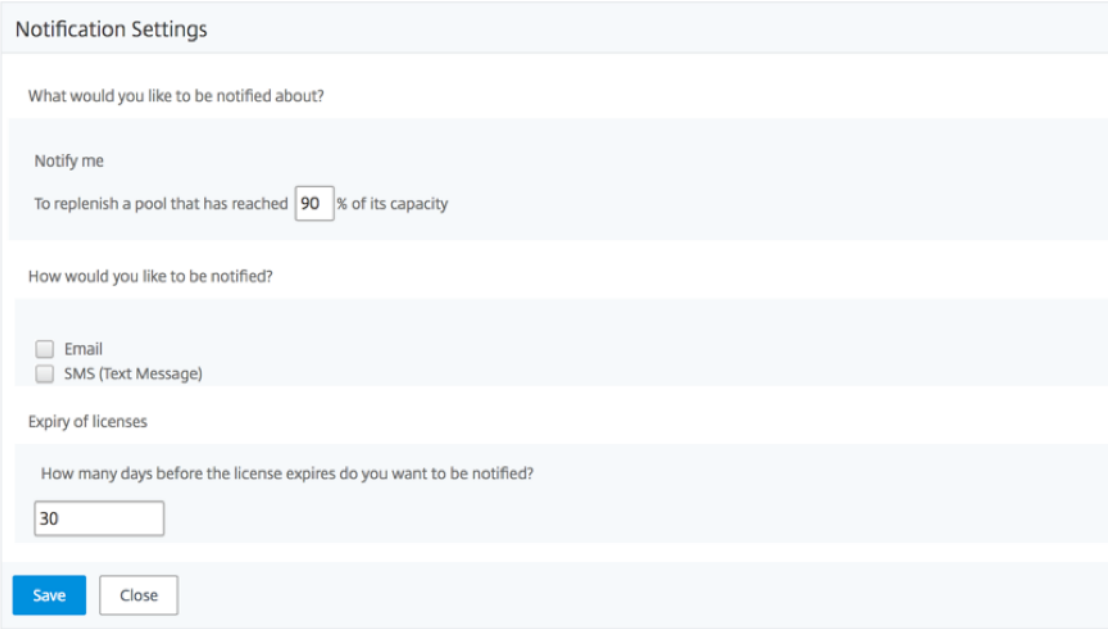
当发送许可证到期通知并且可以在 Citrix ADM 上查看此事件时，将生成一个事件。

要配置许可证到期检查，请执行以下操作：

1. 导航到 “网络” > “许可证”。
2. 在 “许可证设置” 页面的 “许可证到期信息” 部分下，您可以找到将要过期的许可证的详细信息：
    - 功能：即将过期的许可证类型。
    - 计数：受影响的虚拟服务器或实例的数量。
    - 到期天数：许可证到期前的天数。



3. 在“通知设置”部分，单击“编辑”图标并指定警报阈值。您可以设置用于通知管理员的池许可证容量的百分比。
4. 通过选中相应的复选框，选择要发送的通知类型。通知类型如下：
   a) 电子邮件配置文件：指定邮件服务器和配置文件详细信息。当您的许可证即将过期时，将触发电子邮件。
   b) **SMS** 配置文件：指定短消息服务 (SMS) 服务器和配置文件详细信息。当您的许可证即将过期时，会触发 SMS 消息。



5. 然后，根据许可证到期前的天数指定要发送通知的时间。
6. 单击保存。

Citrix ADC 虚拟 CPU 许可

April 23, 2021

像您这样的数据中心管理员正在转向更新的技术，这些技术能够简化网络功能，同时提供更低的成本和更高的可扩展性。较新的数据中心体系结构必须至少包括以下功能：

- 软件定义网络 (SDN)
- 网络功能虚拟化 (NFV)
- 网络虚拟化 (NV)
- 微型服务

此类运动还需要软件要求具有动态、灵活和敏捷性，以满足不断变化的业务需求。许可证还将由一个中央管理工具管理，并充分了解使用情况。

适用于 **Citrix ADC VPX** 的虚拟 **CPU** 许可

早些时候，Citrix ADC VPX 许可证是根据实例的带宽消耗分配的。根据所绑定的许可证版本，Citrix ADC VPX 只能使用特定的带宽和其他性能指标。要增加可用带宽，必须升级到提供更多带宽的许可证版本。在某些情况下，带宽要求可能较小，但对于其他 L7 性能（如 SSL TPS、压缩吞吐量等）的要求更高。在这种情况下，升级 Citrix ADC VPX 许可证可能不适合。但是，您可能仍然需要购买带宽较大的许可证，以解锁 CPU 密集处理所需的系统资源。Citrix ADM 现在支持根据虚拟 CPU 要求向 Citrix ADC 实例分配许可证。

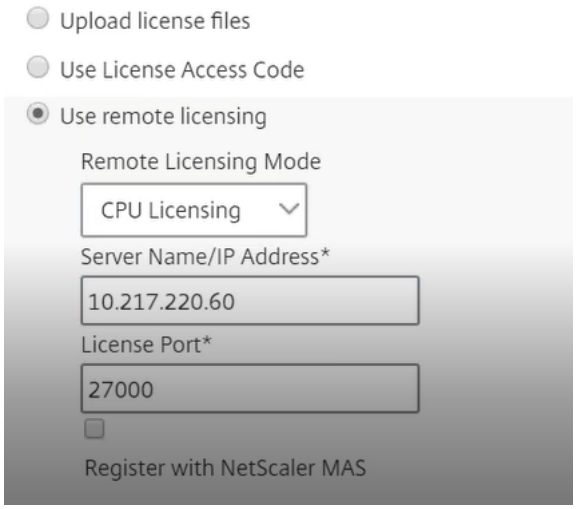
在基于 CPU 使用情况的虚拟许可功能中，许可证指定特定 Citrix ADC VPX 有权使用的 CPU 数量。因此，Citrix ADC VPX 只能从许可证服务器检出其上运行的虚拟 CPU 数量的许可证。Citrix ADC VPX 会根据系统中运行的 CPU 数量签出许可证。Citrix ADC VPX 在签出许可证时不考虑空闲 CPU。

与池许可证容量和 CICO 许可证功能类似，Citrix ADM 许可证服务器管理一组单独的虚拟 CPU 许可证。此外，为虚拟 CPU 许可证管理的三个版本是标准版、高级版和高级版。这些版本解锁了与带宽许可证版本解锁的功能集相同。

虚拟 CPU 数量可能发生变化，或许可证版本发生变化时。在这种情况下，您必须始终关闭实例，然后再发起新许可证集的请求。签出许可证后重新启动 Citrix ADC VPX。

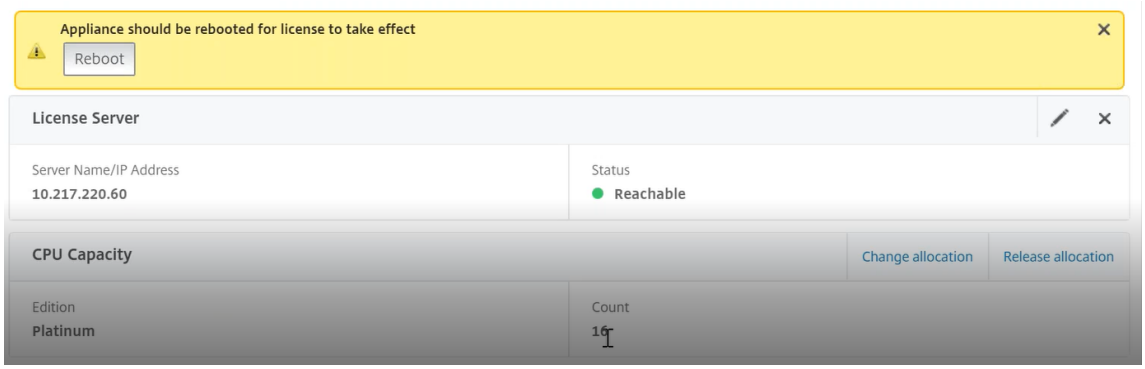
要使用 **GUI** 在 **Citrix ADC VPX** 中配置许可服务器，请执行以下操作：

1. 在 Citrix ADC VPX 中，导航到 系统 > 许可证”，然后单击 管理许可证。
2. 在 许可证页上，单击 添加新许可证。
3. 在 许可证页面上，选择 使用远程许可” 选项。
4. 从 远程许可模式” 列表中选择 CPU 许可。
5. 键入许可证服务器的 IP 地址和端口号。
6. 单击继续。



> 注意：
>
> 您必须始终将 Citrix ADM 注册到 Citrix ADC VPX 实例。如果尚未完成，请启用“向 **Citrix ADM** 注册”并键入 Citrix ADM 登录凭据。

7. 在“分 配许可证”窗口中，选择许可证类型。此窗口将显示总数和可用虚拟 CPU 以及可分配的 CPU。单击获取许可证。
8. 单击下一页上的 重新启动以申请许可证。



> 注意
>
> 您还可以释放当前许可证并从其他版本签出。例如，您已经在实例上运行标准版许可证。您可以释放该许可证，然后从高级版中签出。

使用 **CLI** 在 **Citrix ADC VPX** 许可证中配置许可服务器

在 Citrix ADC VPX 控制台中，为以下两个任务键入以下命令：

1. 要将许可服务器添加到 Citrix ADC VPX，请执行以下操作：

```
1 add licenseserver <IP address of the license server>
2 <!--NeedCopy-->
```


2. 要申请许可证，请执行以下操作：

```
set capacity -vcpu - edition premium
<!--NeedCopy-->
```

出现提示时，键入以下命令重新启动实例：

```
reboot -w
<!--NeedCopy-->
```

更新许可服务器 **IP** 地址

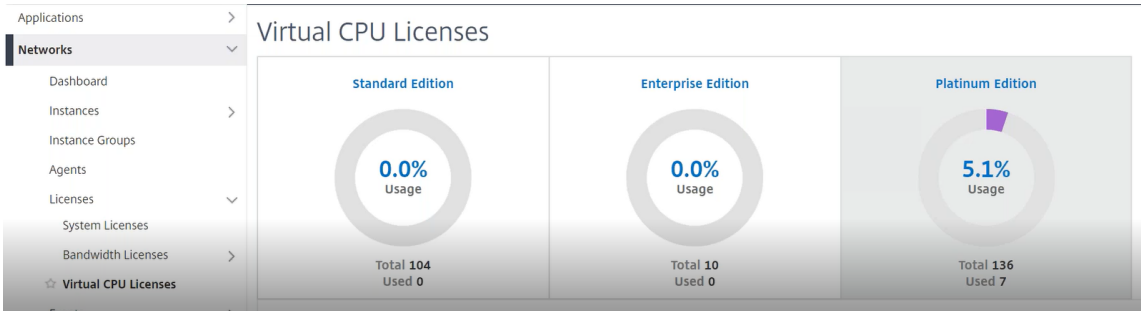
您可以更新 VPX 实例中的许可服务器 IP 地址，而不会对实例分配的许可证带宽和数据丢失产生任何影响。要更新授权服务器 IP 地址，请在 VPX 实例上键入以下命令：

```
add licenseserver <licensing server IP address> -forceUpdateIP
```

此命令连接到新服务器并释放与之前许可服务器关联的资源。

在 **Citrix ADM** 上管理虚拟 **CPU** 许可证

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 许可证” > “ 虚拟 **CPU** 许可证”。
2. 此页面显示为每种类型的许可证版本分配的许可证。
3. 单击每个圆环内的数字可查看使用此许可证的 Citrix ADC 实例。



适用于 **Citrix ADC CPX** 的虚拟 **CPU** 许可

在预配 Citrix ADC CPX 实例时，您可以根据实例上的 CPU 使用情况，将 Citrix ADC CPX 实例 Provisioning 为从许可证服务器签出许可证。

Citrix ADC CPX 依赖于在 Citrix ADM 上运行的许可证服务器来管理许可证。Citrix ADC CPX 在许可证服务器启动时从许可证服务器中签出许可证。当 Citrix ADC CPX 关闭时，许可证会签回许可证服务器。

您可以从 Docker 应用商店下载 Citrix ADC CPX。在 Docker 主机上，要下载 Citrix ADC CPX，请运行以下命令：

```
docker pull store/citrix/netscalercpx: [version]
```


CPX 许可证有三种许可证类型：

1. CPX 和 VPX 支持的虚拟 CPU 订阅许可证
2. 池容量许可证
3. CP1000 许可证仅支持 CPX 的单到多个 vCPU

要在置备 **Citrix ADC CPX** 实例的同时 **Provisioning vCPU** 订阅许可证，请执行以下操作：

指定 Citrix ADC CPX 实例使用的 vCPU 许可证数。

- 此值通过 Docker、Kubernetes 或中索斯/马拉松作为环境变量输入。
- 目标变量是 “CPX_CORES”。CPX 可以支持 1 到 16 个内核。

要指定 2 个内核，您可以执行 docker 运行命令，如下所示：

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2
2 <!--NeedCopy-->
```

Provisioning Citrix ADC CPX 实例时，请在 码头运行命令中将 Citrix ADC 许可服务器定义为环境变量，如下所示：

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> cpx:11.1
2 <!--NeedCopy-->
```

其中，

- < LS_IP 地址 > 是 *Citrix ADC* 许可服务器的 IP 地址。
- < LS_PORT > 是 *Citrix*ADC 许可服务器的端口。默认情况下，端口为 27000。

> 注意
>
> 默认情况下，Citrix ADC CPX 实例会从 vCPU 订阅池中签出许可证。如果实例使用 “n” CPU 运行，CPX 实例会检出 “n” 数量的许可证。

要在预配 **Citrix ADC CPX** 实例时 **Provisioning Citrix ADC** 池容量或 **CP1000** 许可证，请执行以下操作：

如果要使用池许可（基于带宽）或 CPX 私有池（CP1000 或基于私有池）签出 CPX 实例的许可证，则必须相应地提供环境变量。

例如，

```
1 docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
     -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
     LS_PORT> -e PLATFORM=CP1000 cpx:11.1
2 <!--NeedCopy-->
```


CP1000. 此命令触发从 CP1000 池（CPX 专用池）检出。然后，Citrix ADC CPX 实例检索为 CPX_CORES 指定的 “n” 核心数量的实例。最常见的用例是为单个实例的检出指定 n = 1。多核 CPX 使用案例检出 “n” vCPU（其中 “n” 是从 1 到 7）。

```
docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx
    -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<
    LS_PORT> -e BANDWIDTH=2000 cpx:11.1
<!--NeedCopy-->
```

集合容量。此命令从实例池中检出一个许可证，并消耗高级带宽池中的 1000 Mbps 带宽，但使 CPX 能够运行高达 2000 Mbps。在池许可中，不收费前 1000 Mbps 的费用。

> 注意：从带宽池检出时，
>
> 指定所需目标带宽的相应 vCPU 数，如下表所述：
>
> | 内核数量（vCPU）| 最大带宽 |
> |—| 1
> | 千兆位/秒 | | 2
> | 2000 兆位/秒 | | 3
> | 3500 兆位/秒 | 4
> | 5000 兆位/秒 |
> | 5 | 6500 兆位/秒
> | 6 | 8000 兆位/秒 |
> |7 | 9300 兆位/小时 |

管理 Citrix SD-WAN 实例

April 23, 2021

通过 Citrix ADM，您可以监视、管理和查看网络中的 Citrix SD-WAN 装置的分析。下面的互操作性表提供了每个 Citrix SD-WAN 平台版本当前支持哪些 Citrix ADM 功能的信息。

Citrix SD-WAN 平台版本和 Citrix ADM 功能的互操作性矩阵

平台版本	发现	配置	监视	报告（网络报告）	事件管理	HDX Insight	WAN Insight
Citrix SD-WAN WANOP	是	是	是	是	是	是	是

平台版本	发现	配置	监视	报告（网络报告）	事件管理	HDX Insight	WAN Insight
Citrix SD-WAN 东南	是	否	否	否	否	否	否
Citrix SD-WAN PE	是	否	否	否	否	是	否

Citrix SD-WAN 版本由 Citrix ADM 支持

平台版本	Citrix SD-WAN 版本	Citrix ADM 版本
Citrix SD-WAN WANOP	Citrix CloudBridge 7.4 及更高版本	Citrix ADM 11.0 及更高版本
Citrix SD-WAN 东南	Citrix SD-WAN 9.3.0 及更高版本	Citrix ADM 12.0.53.8 及更高版本
Citrix SD-WAN PE	Citrix SD-WAN 9.3.0 及更高版本	Citrix ADM 12.0.53.8 及更高版本

您可以将 Citrix SD-WAN 设备添加为 Citrix ADM 上的托管实例。有关详细信息，请参阅将实例添加到 Citrix ADM。您可以查看 Citrix SD-WAN WANOP 实例的广域网洞察、HDX 洞察、网络报告和事件报告。

Citrix ADM 允许 Citrix SD-WAN 标准版 (SE) 和企业版 (EE) 设备将自身注册为 Citrix ADM 上的托管实例。

要将 Citrix SD-WAN SE/PE/AE 设备添加到 Citrix ADM，请在 Citrix SD-WAN SE/PE/AE 设备上将 Citrix ADM 配置为 AppFlow 收集器。Citrix SD-WAN SE/PE/AE 设备将自己添加为 Citrix ADM 上的托管实例。然后，SD-WAN SE/PE/AE 设备将分析数据发送到 Citrix ADM。

您可以在每个 SD-WAN SE/PE/AE 设备上单独将 Citrix ADM 设置为 AppFlow 收集器，也可以使用 Citrix SD-WAN 中心将配置导出到受控装置。

有关详细信息，请参阅在 Citrix ADM 中添加 Citrix SD-WAN SE/PE/AE 实例。

对于 Citrix SD-WAN PE 装置，您可以查看 HDX 数据记录或多跳数据，具体取决于 AppFlow 配置。Citrix SD-WAN SE 设备仅提供多跳数据。有关详细信息，请参阅 查看 HDX Insight 报告和指标 和 查看多跳部署的分析数据。

此页提供了一些主题的快速访问链接，您可以参考这些主题，以便使用 Citrix ADM 设备来管理 SD-WAN WANOP 设备。

Citrix ADM 概述

关于 Citrix ADM

体系结构

Citrix ADM 如何发现实例

Citrix ADM 如何与托管实例进行通信

Citrix ADM 部署

使用思杰虚拟机管理程序部署 Citrix ADM

使用微软 Hyper-V 部署 Citrix ADM

使用 VMware ESXi 部署 Citrix ADM

使用 Linux KVM 服务器部署 Citrix ADM

在高可用性模式下部署 Citrix ADM

从 NetScaler Insight Center 迁移至 Citrix ADM

将 Citrix ADM 与控制器集成

实例管理

如何将实例添加到 Citrix ADM

如何在 Citrix ADM 上创建实例组

如何使用 Citrix ADM 备份和还原实例

配置管理

如何从 Citrix ADM 上的更正命令创建配置作业

如何安排使用 Citrix ADM 中的内置模板创建的作业

如何重新计划通过使用 Citrix ADM 中的内置模板配置的作业

如何重用执行的配置作业

分析

WAN Insight

HDX Insight

如何查看 Citrix SD-WAN 实例的网络报告

如何配置自适应阈值

如何为分析配置数据库汇总

如何使用 Citrix ADM 创建阈值和警报

事件管理

如何为 Citrix ADM 上的事件设置事件年龄

如何使用 Citrix ADM 调度事件筛选器

如何为 Citrix ADM 中的事件设置重复电子邮件通知

如何通过使用 Citrix ADM 隐藏事件

如何查看 Citrix SD-WAN 实例的事件报告

如何修改 Citrix ADC 实例上发生的事件的报告严重性

如何在 Citrix ADM 中查看事件摘要

如何在 Citrix ADM 的基础架构仪表板上显示 SNMP 陷阱的事件严重性和倾斜性

身份验证

如何级联外部身份验证服务器

如何添加 RADIUS 身份验证服务器

如何添加 LDAP 身份验证服务器

如何添加 TACACS 身份验证服务器

如何在 Citrix ADM 中提取身份验证服务器组

如何启用回退本地身份验证

Citrix ADM 系统

管理 Citrix ADM 系统

如何升级 Citrix ADM

如何为 Citrix ADM 生成技术支持文件

如何在单服务器部署中备份和还原您的 Citrix ADM 服务器

如何在 HA 对中备份和还原 Citrix ADM 配置

如何在 Citrix ADM 中为非默认用户启用外壳访问

如何在 Citrix ADM 上配置 NTP 服务器

如何为 Citrix ADM 配置 SSL 设置

如何为 Citrix ADM 配置系统日志清除间隔

如何查看 Citrix ADM 的审核信息

如何配置 Citrix ADM 的系统通知设置

如何监视 Citrix ADM 的 CPU、内存和磁盘使用情况

如何为 Citrix ADM 配置密码组

如何在 Citrix ADM 上创建 SNMP 陷阱、管理器和用户

如何将主机名分配给 Citrix ADM 服务器

如何配置 Citrix ADM 的系统修剪设置

如何使用 Citrix ADM 配置系统备份设置

如何在 Citrix ADM 上配置和查看系统警报

添加 **Citrix SD-WAN** 实例

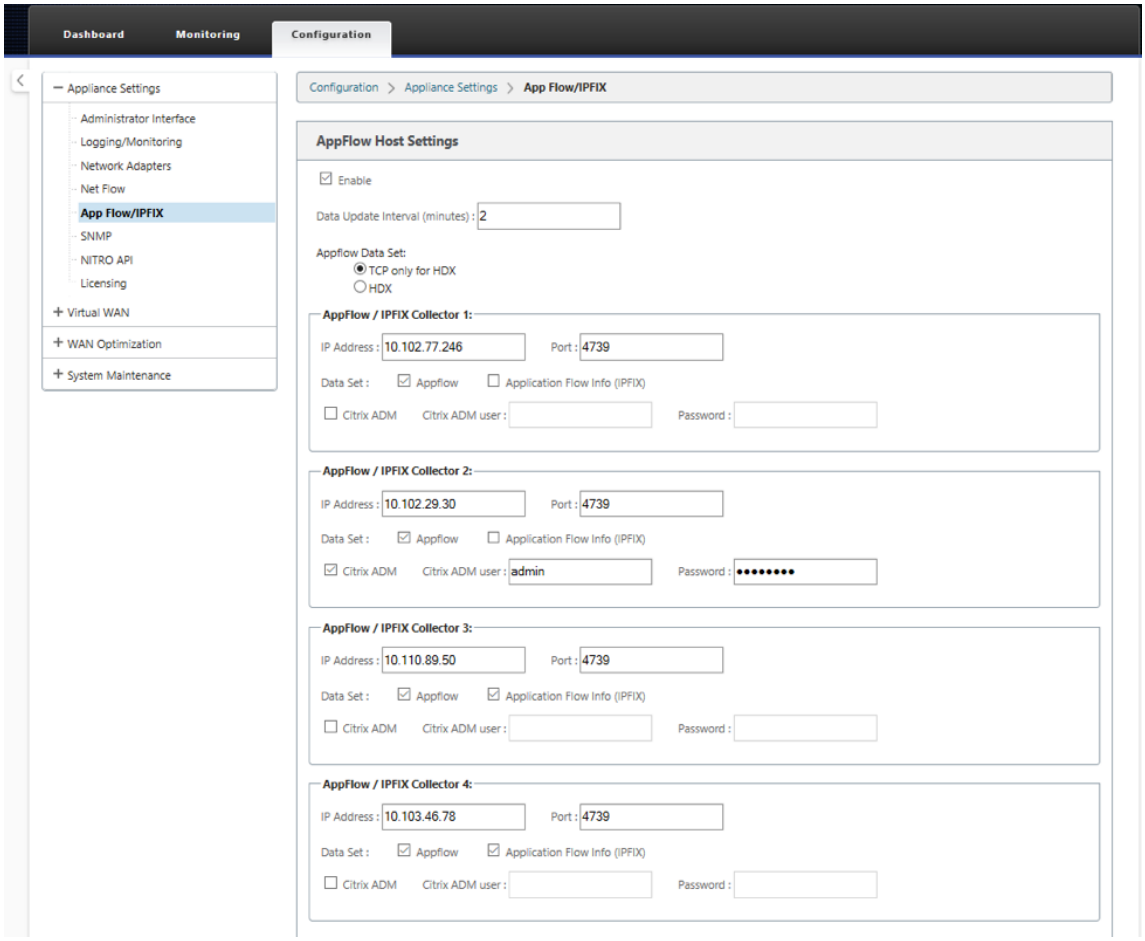
April 23, 2021

将 Citrix ADM 配置为 Citrix SD-WAN SE/PE 装置上的 AppFlow 收集器，以便在 Citrix ADM 中添加这些实例。Citrix SD-WAN SE/PE/AE 设备在 Citrix ADM 上注册为托管实例，并收集其 AppFlow 记录。对于 Citrix SD-WAN PE 装置，您可以 仅为 **HDX** 模板启用 **TCP** ，也可以启用 **HDX** 模板。仅适用于 **HDX** 模板的 **TCP** 提供多跳数据。**HDX** 模板提供 HDX 数据，应仅在数据中心设备上启用该模板。

您可以在单个 SD-WAN SE/PE/AE 设备上将 Citrix ADM 配置为 AppFlow 收集器，也可以使用 SD-WAN Center 将 Citrix ADM 配置为 AppFlow 收集器，然后将配置导出到由其管理的设备。

要将 **Citrix ADM** 配置为 **Citrix SD-WAN SE/PE/AE** 设备上的 **AppFlow** 收集器，请执行以下操作：

1. 在 SD-WAN SE/PE/AE Web 界面中，导航到 配置 > **AppFlow/IPFix**
2. 选择 “ 启用”。



3. 在“数据更新间隔”字段中，指定将 AppFlow 报告导出到 AppFlow 收集器的时间间隔（以分钟为单位）。

> 注意
>
> 如果 Citrix ADM 是 AppFlow 收集器，则数据更新间隔应为 1 分钟。

4. 执行以下操作之一：

   - 选择 **HDX**，将 HDX 见解数据发送到 AppFlow 收集器。应该在分支设备上启用此选项。
   - 选择 仅适用于 **HDX** 的 **TCP**，以将多跳数据发送到 AppFlow 收集器。

> 注意
>
> **HDX** 模板选项仅适用于 Citrix SD-WAN PE 装置，应在数据中心设备上启用该选项

5. 在“**IP** 地址”字段中，键入外部 AppFlow 收集器系统（Citrix ADM 服务器）的 IP 地址。
6. 在“端口”字段中，键入外部 AppFlow 收集器系统侦听的端口号。默认值为 4739。
7. 选中“**Citrix ADM** ”复选框，以指定 Citrix ADM 是 AppFlow 收集器。

> 注意
>
> - Citrix ADM 目前不支持 IPFIX 集合。

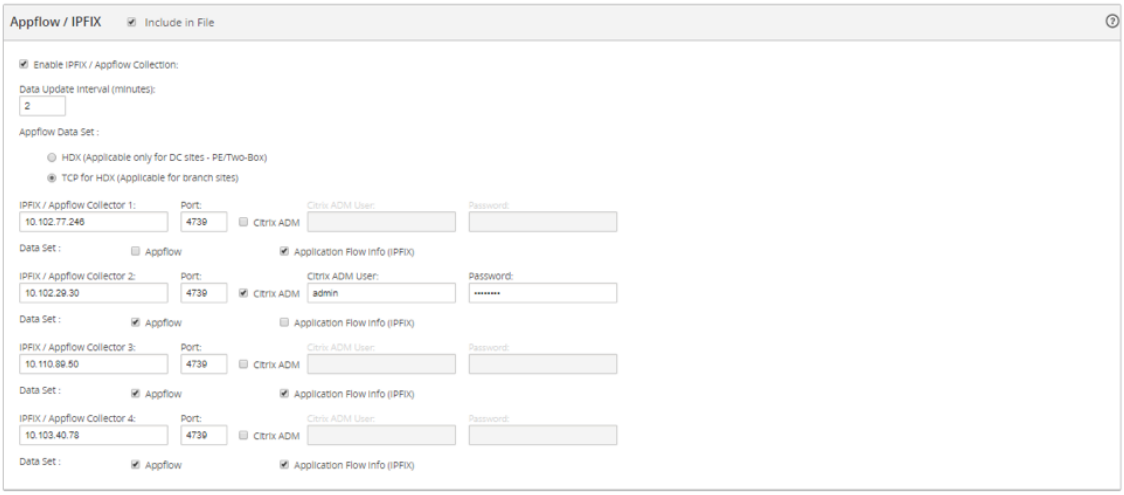
> - 最多可以添加 4 个 AppFlow 收集器。Citrix ADM 或任何支持 IPFIX 协议的 AppFlow 收集器。

8. 输入 Citrix ADM 服务器的凭据
9. 单击 应用设置。

在 Citrix ADM 上发现并列出了 Citrix SD-WAN SE/PE 装置。Citrix SD-WAN SE/PE 装置将分析数据发送到 Citrix ADM。有关详细信息，请参阅AppFlow 和 IPFIX。

要使用 **Citrix SD-WAN** 中心将 **Citrix ADM** 配置为 **AppFlow** 收集器，请执行以下操作：

1. 在 Citrix SD-WAN 中心管理用户界面中，导航到 “ 配置” > “ 装置设置”。
2. 导航到 “ **AppFlow/IPFIX** ” 部分，然后选择 “包括在文件中”。
3. 选择启用 **IPFIX/AppFlow** 集合。



4. 在 “ 数据更新 间隔” 字段中，指定将 AppFlow 报告导出到 AppFlow 收集器的时间间隔（以分钟为单位）。

> 注意
>
> 如果 Citrix ADM 是 AppFlow 收集器，则数据更新间隔应为 1 分钟。

5. 执行以下操作之一：
   - 选择 **HDX**，将 HDX 见解数据发送到 AppFlow 收集器。
   - 为 **HDX** 选择 **TCP**，将多跳见解数据发送到 AppFlow 收集器。应该在分支设备上启用此选项。

> 注意
>
> **HDX** 模板选项仅适用于 Citrix SD-WAN PE 装置，应在数据中心装置上启用该选项。

6. 在 **IPFIX AppFlow** 收集器字段中，键入外部应用流收集器系统（Citrix ADM 服务器）的 IP 地址。
7. 在 “ 端口” 字段中，键入外部 AppFlow 收集器系统侦听的端口号。默认值为 4739。
8. 选中 “ **Citrix ADM** ” 复选框以指定 Citrix ADM 是 AppFlow 收集器。
9. 输入 Citrix ADM 服务器的凭据。

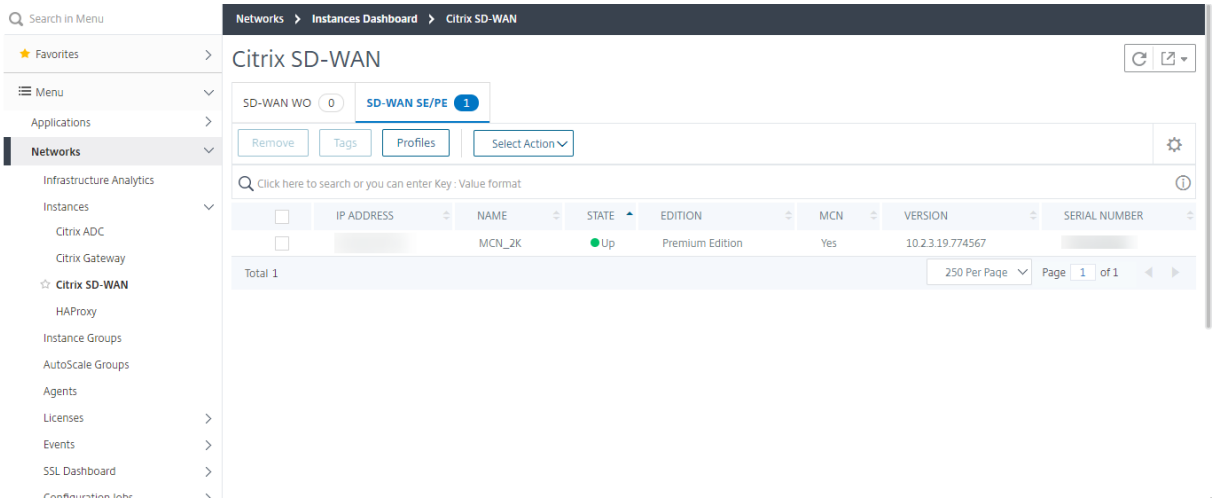
> 注意
>
> 最多可以添加 4 个 AppFlow 收集器。Citrix ADM 或任何支持 IPFIX 协议的 AppFlow 收集器。

10. 将配置保存并导出到受管设备。

    有关详细信息，请参阅如何配置装置设置并将其导出到受控装置。

有关使用 Citrix SD-WAN 中心将 Citrix ADM 配置为 AppFlow 收集器的详细信息，请参阅 AppFlow 和 IPFIX。

Citrix SD-WAN SE/PE 装置由 Citrix ADM 发现并列出。在 Citrix ADM 中发现并列出了思杰 SD-WAN SE/PE 设备。要查看发现的 Citrix SD-WAN SE/PE 设备，请在 Citrix ADM Web 界面中导航到 网络 > 实例 > **Citrix SD-WAN**，然后选择 **SD-WAN SE/PE/AE**。



您可以查看发现的设备的 IP 地址、名称、当前状态、软件版本和自身版本。还可以查看设备是否是主控制器节点 (MCN)。

您可以执行以下操作：

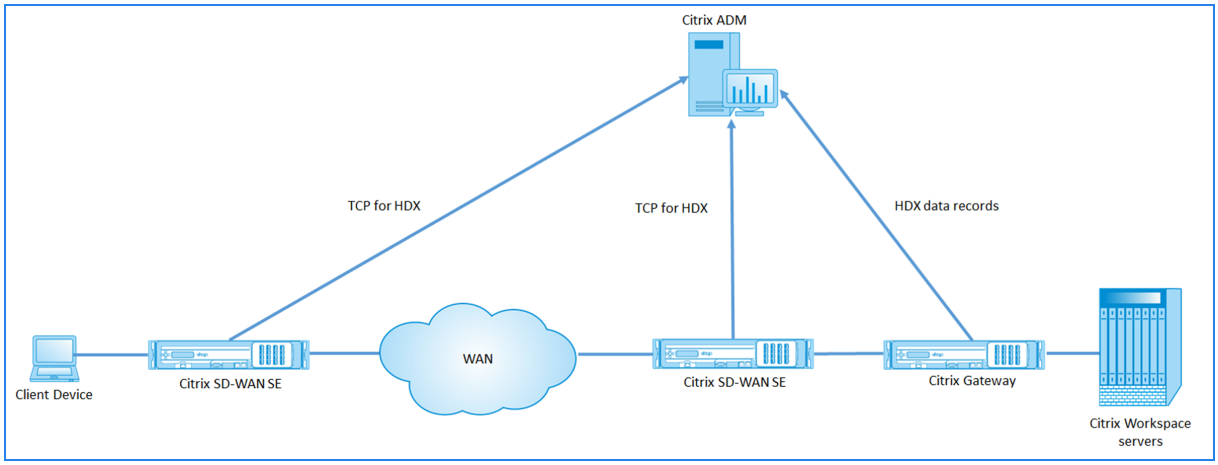
- 查看和删除实例配置文件。
- 从 Citrix ADM 中删除实例。
- 重新发现实例。

对于 Citrix SD-WAN PE 装置，您可以查看 HDX 数据记录或多跳数据，具体取决于 AppFlow 配置。Citrix SD-WAN SE 设备仅提供多跳数据。有关详细信息，请参阅 查看 HDX Insight 报告和指标 和 查看用于多跳部署的 Citrix SD-WAN 分析数据。

查看用于多跳部署的 **Citrix SD-WAN** 分析数据

April 23, 2021

在多跃点网络部署中，客户端与服务器之间有多个设备，如下图所示。在此类型的部署中，Citrix SD-WAN SE 设备和 Citrix Gateway 将添加到 Citrix ADM 中，并且启用了 AppFlow。



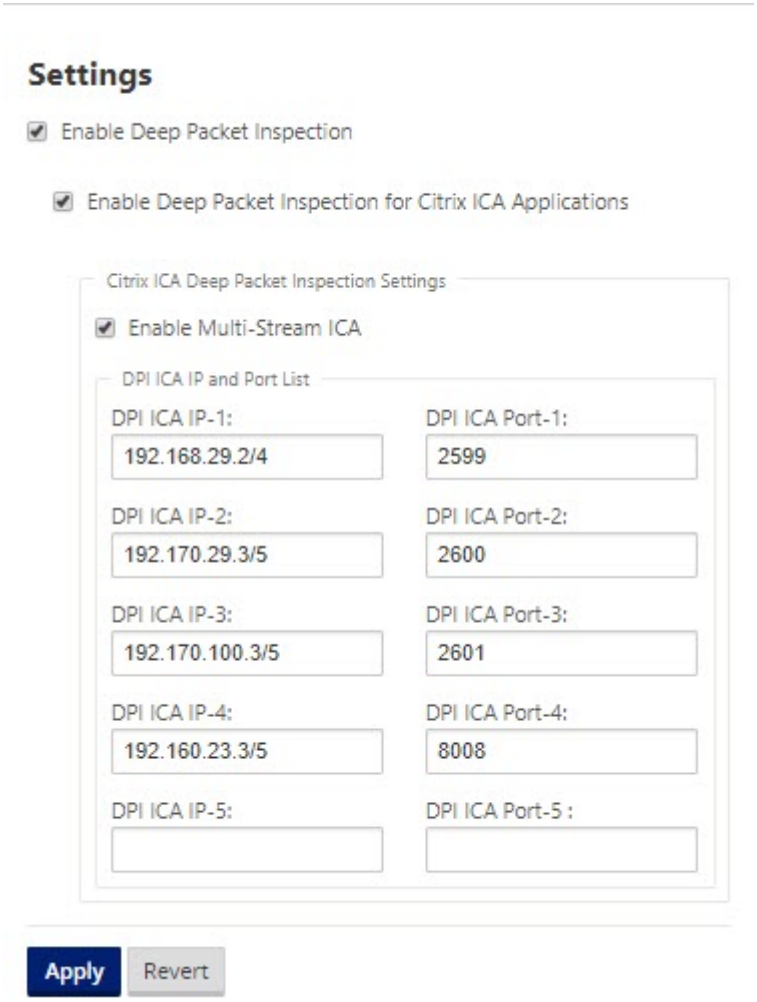
Citrix ADM 根据跳数和连接链 ID 标识其从中接收数据的装置。跃点计数表示流量从客户端传输到服务器通过的设备数。连接链 ID 表示客户端与服务器之间的端到端连接。

Citrix ADM 使用跳数和连接链 ID 来关联来自设备的数据，并生成报告。

要使 Citrix SD-WAN SE 装置将分析数据发送到 Citrix ADM，您应将 Citrix Gateway 的虚拟 IP 地址配置为 DPI ICA IP，并将 DPI ICA 端口号设置为 443。

要配置 **ICA DPI** 设置，请执行以下操作：

1. 在 Citrix SD-WAN SE 设备 UI 中，导航到 配置编辑器 > 高级 > 全局 > 应用程序 > 设置
2. 选择 “ 启用深度数据包检测” > “ 启用 **Citrix ICA** 应用程序的深度数据包检测” > “ 启用多流 **ICA**”



3. 在 **DPI ICA IP-1** 字段中，输入 Citrix Gateway 虚拟 IP 地址和前缀。
4. 在 **DPI ICA** 端口**-1** 字段中，输入端口号 443。
5. 单击 应用并使用更改管理过程将配置导出到设备。

在 Citrix ADM 中，对于每个活动的 ICA 会话，您可以在 HDX Insight 中查看会话图。会话图提供有关连接路径中的设备的详细信息。通过它们还可以深入了解网络设备与其紧邻的下一个跃点之间的客户端/服务器端延迟。通过此信息可以找出延迟的根本原因以及对性能问题进行故障排除。

Citrix SD-WAN SE 不发送 HDX 数据记录。它仅提供 “适用于 HDX 的 TCP” 信息。HDX 分析数据由网络中启用 HDX 分析的设备（例如，Citrix ADC 或 CitCitrix Gateway）提供。

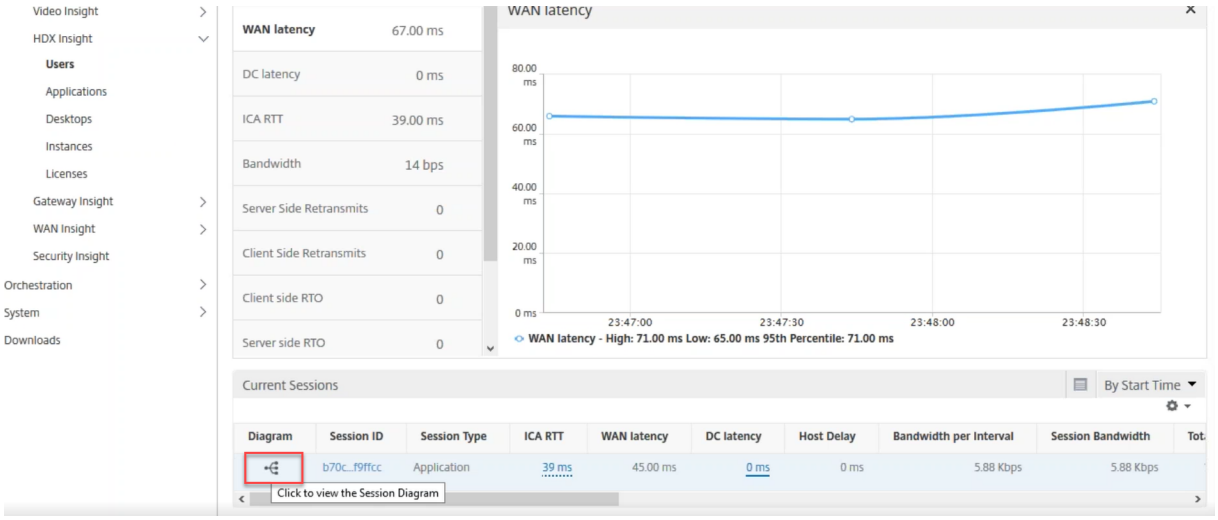
Citrix SD-WAN PE 设备可以为 HDX 数据或 HDX 洞察数据发送 TCP，具体取决于设备的 AppFlow 配置。应在数据中心设备上启用 HDX 模板。

> 注意
>
> 在多跃点部署中，请确保仅其中一个网络设备发送 HDX Insight 数据。其余网络设备可以发送 “适用于 HDX 的

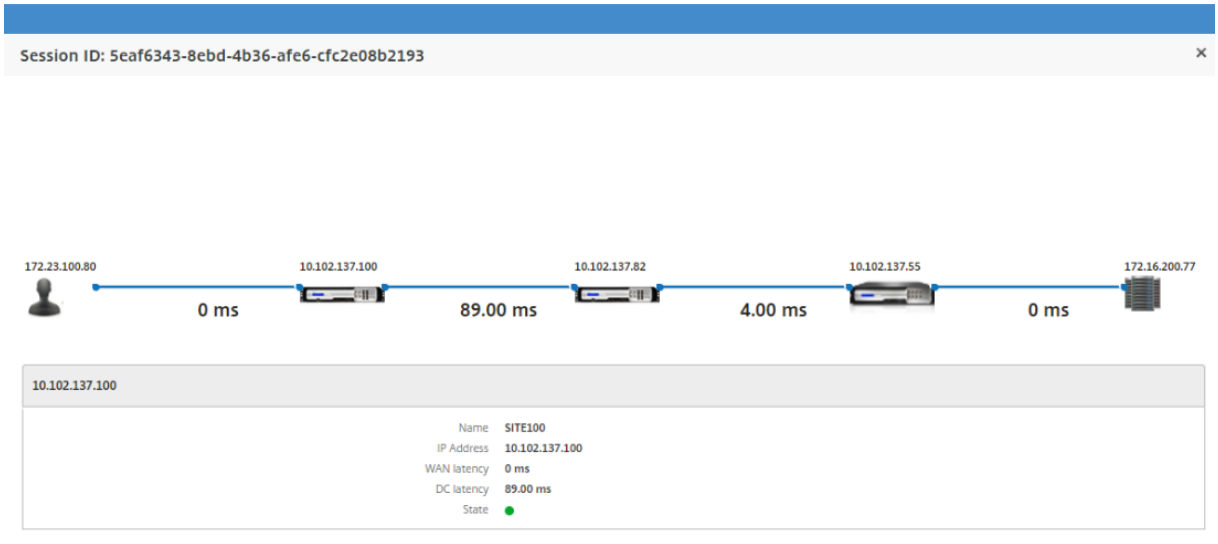
> TCP” 数据。

要查看多跳数据，请执行以下操作：

在 Citrix ADM Web 界面中，导航到 “ **HDX Insight** ” > “ 用户” > “ 当前会话” 或 “ **HDX** 智能分析” > “应用 程序” > “ 当前会话”，然后单击 “ 图” 图标。



将显示网络拓扑图。



单击任何网络元素可显示详细信息。

> 注意
>
> 显示的信息取决于选定的网络元素。

Citrix 装置将显示以下参数：

- 名称：Citrix 装置的名称。
- **IP** 地址：装置的 IP 地址。
- **WAN** 延迟：由网络的客户端造成的延迟。也就是说，从 Citrix 设备到最终用户。

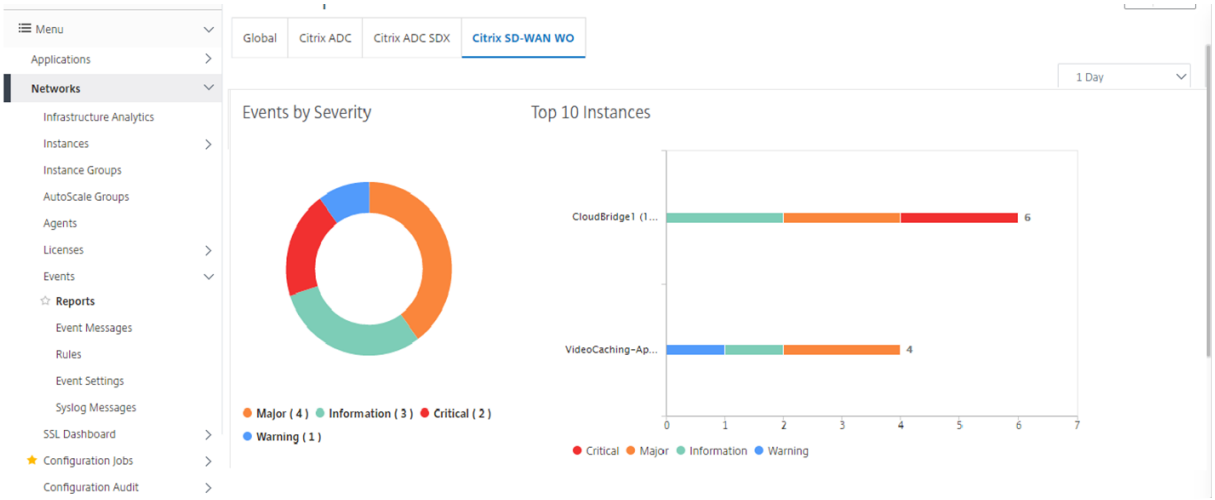
- 直流延迟：由网络的服务器端引起的延迟。也就是说，从 Citrix 设备到后端服务器。
- 状态：设备可达性状态。

查看 **Citrix SD-WAN WANOP** 实例的事件报告

April 23, 2021

您可以通过导航到 “ 网络” > “事件” > “ 报告”，然后选择 **Citrix SD-WAN WO**，以图形表示形式查看前 **10** 个 **SD-WAN** 实例的 事件。

每个实例的事件根据其严重性进行显示，您可以单击每个严重性来了解有关事件数、事件发生时间以及事件所属类别的详细信息。



查看 **Citrix SD-WAN** 实例的网络报告

April 23, 2021

您可以在 Citrix ADM 中查看与 WAN 优化网络相关的报告，使用这些数据可以排除网络问题或分析 Citrix SD-WAN WANOP 设备的行为。您可以查看过去一小时、一天、一周或一个月内 WAN 优化设备的网络统计信息的报告。

您可以查看以下报告：

报告	说明
加速	使用此报告可以分析加速流量的模式（按服务类别的 KBPS）和通过 WAN 优化设备的加速 TCP 连接数。这包括通过 WAN 优化设备进行加速的 TCP 连接数、已选择进行加速的开放和半闭合连接数以及候选半开放连接数加速度。
Pass through Connection（通过连接传送）	使用此报告可查看 WAN 优化设备的非加速连接。
Service Class（服务类别）	使用此报告可以查看基于为 WAN 优化设备定义的服务类型的发送和接收带宽节省。
应用程序	使用此报告可以查看在 WAN 优化设备上运行的应用程序的发送和接收数据卷（以每秒比特为单位）。
CPU 使用率	使用此报告可查看以百分比表示的 WAN 优化设备的 CPU 使用率。
Capacity Increase（容量增加）	使用此报告可查看 WAN 优化设备的累计发送压缩比。
Data reduction（数据减少）	使用此报告可查看以百分比表示的传输和接收带宽节省量。您还可以分别分析 WAN 优化设备的传输带宽和接收带宽节省值。
Link Utilization（链路利用率）	使用此报告可以查看 WAN 优化的传输链路利用率和接收链路利用率的百分比。
Plugin Usage（插件使用情况）	使用此报告可查看连接到 WAN 优化设备的插件数。
Packet Loss（数据包丢失）	使用此报告可查看 WAN 优化设备中定义的链路丢弃的已发送数据包和链路丢弃的接收数据包。
吞吐量	使用此报告可以查看 WAN 优化设备的链路发送卷和链路接收卷（以比特为单位）。
QoS	使用此报告可以查看 WAN 优化设备的 QOS 已发送和 QOS 接收卷（以位/秒为单位）。

要查看 **Citrix SD-WAN ANOP** 网络报告，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网 络”>“ 网络报告”>“ **Citrix SD-WAN O**”。
2. 从“报 告名称”下拉列表中选择要查看的报告。
3. 从“ 实例”下拉列表中，选择要查看其报告的 Citrix SD-WAN WANOP 实例。
4. 从持续时 间下拉列表中，选择时间间隔。
5. 单击运行。

备份 **Citrix SD-WAN** 实例

April 23, 2021

您可以备份实例的当前状态，稍后使用备份的文件将实例恢复到相同状态。在升级实例之前或出于预防原因备份实例是一种很好的做法。稳定系统的备份使您能够将系统恢复到稳定点，以防系统变得不稳定。有多种方法可以在 Citrix SD-WAN 实例上执行备份和恢复。您可以使用 GUI、CLI 进行临时备份和还原实例，也可以使用 Citrix ADM 执行备份。Citrix ADM 使用 NITRO 调用、安全外壳 (SSH) 协议和安全拷贝 (SCP) 协议备份托管 Citrix SD-WAN WANOP 实例的当前状态。

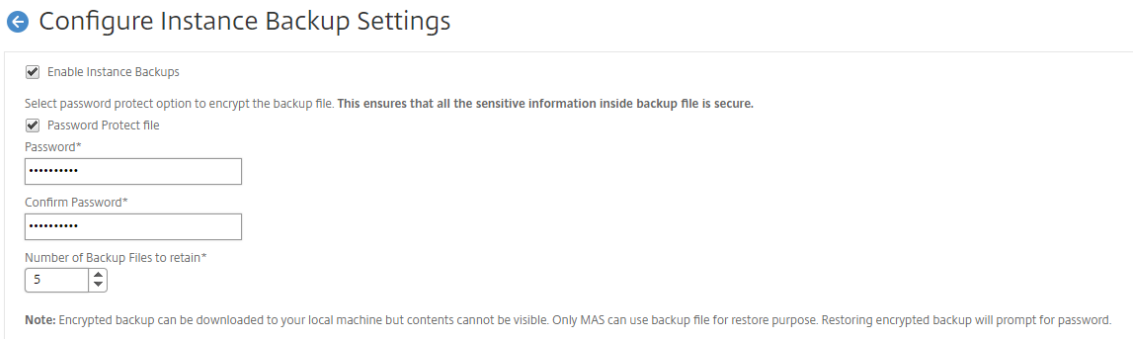
配置实例备份设置

在 Citrix ADM 中备份 Citrix SD-WAN 实例之前，必须在 Citrix ADM 上配置实例备份设置。

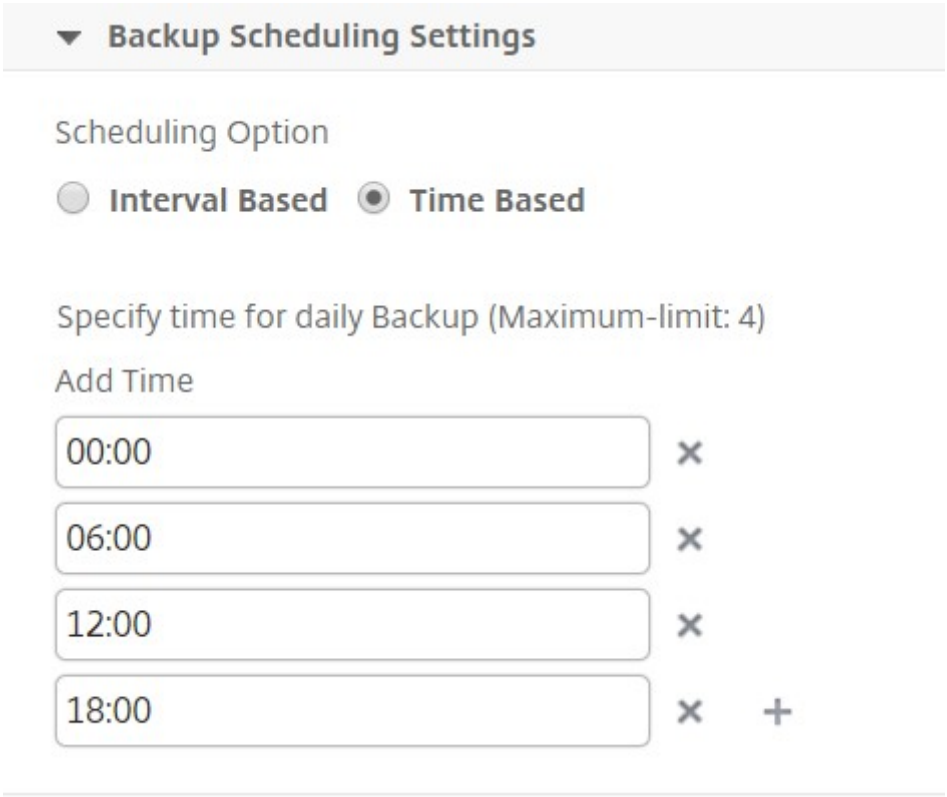
要配置实例备份设置，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 系统管理”。在右侧窗格中的 “ 备份设置” 下，选择 “ 实例备份设置”。
2. 选择 启用实例备份。默认情况下启用此选项。
3. 选择 密码保护文件以加密备份文件。加密备份文件可确保备份文件中的敏感信息是安全的。
4. 在 要重新设置的备份文件数字段中，指定要在 Citrix ADM 中保留的备份文件数。您最多可以保留 50 个备份文件。

   > 注意
   >
   > 每个备份文件都需要一些存储要求。Citrix 建议您根据您的要求在 Citrix ADM 上存储最佳数量的备份文件。

5. 设置备份计划设置。选择以下选项之一：
   - 基于时间间隔 -在指定的时间间隔过后，在 Citrix ADM 中创建备份文件。默认备份时间间隔是 12 小时。
   - 基于时间 -您可以以 “小时: 分钟” 格式指定进行备份的时间。Citrix ADM 允许在实例上进行最多四次每日备份。

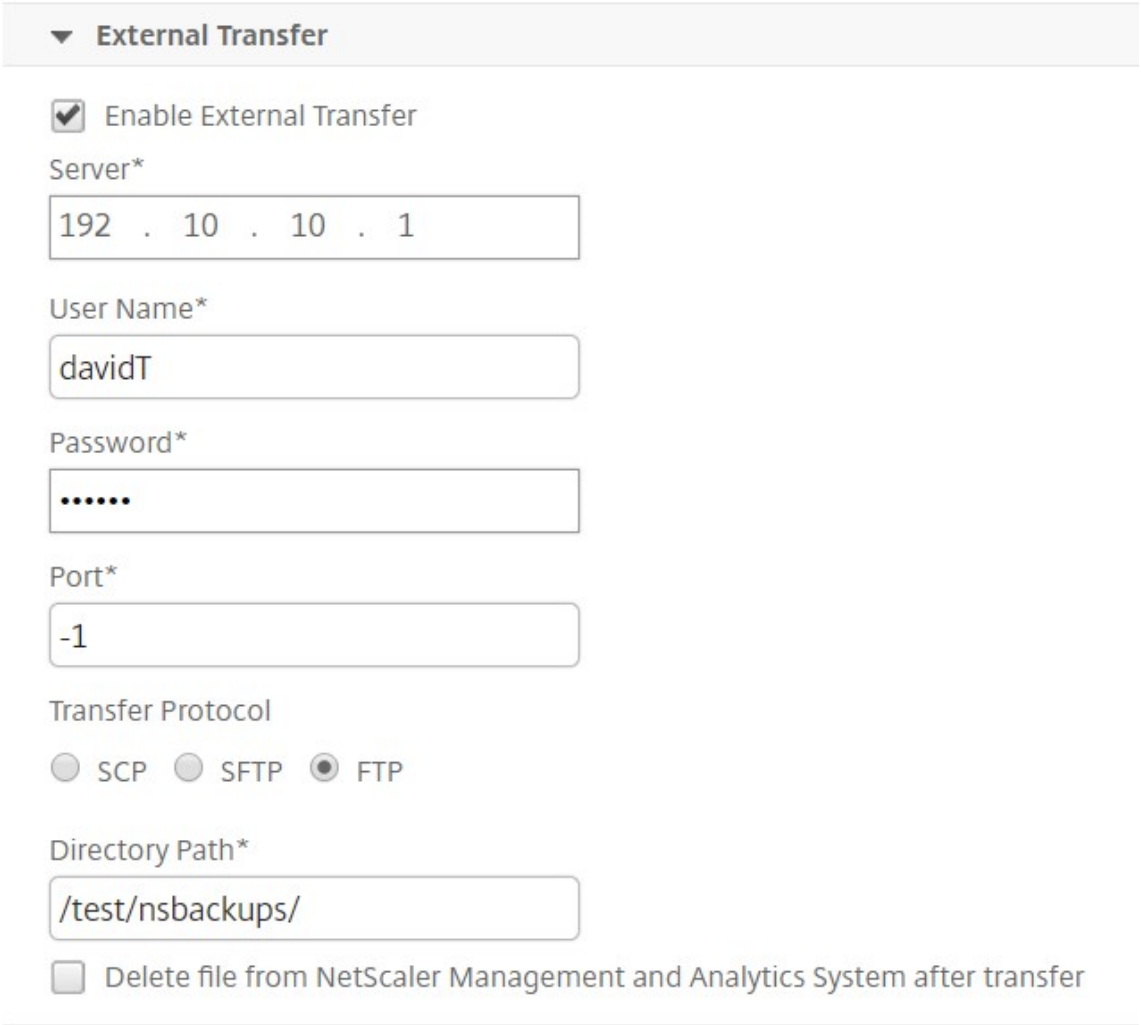


> 注意
>
> 忽略 **Citrix ADC** 设置部分；这些设置不适用于 Citrix SD-WAN 实例。

6. 选择 启用外部传输以将实例备份文件传输到外部位置。输入以下字段的值：

   - 服务器：外部服务器的 IP 地址。
   - 用户名：外部服务器的用户名
   - 密码：外部服务器的密码。
   - 端口：用于与外部服务器通信的端口号。
   - 传输协议：用于将备份文件从 Citrix ADM 传输到外部服务器的协议。

   还可以在将备份文件传输到外部服务器后从 Citrix ADM 中删除备份文件。



7. 单击确定。

> 注意
>
> 当任何选定的 Citrix SD-WAN WANOP 实例出现备份失败时，Citrix ADM 会向自身发送 SNMP 陷阱或系统日志通知。

创建 **Citrix SD-WAN** 实例的备份

为 Citrix SD-WAN WANOP 实例创建备份的过程适用于使用默认 nsroot 配置文件的管理员用户。

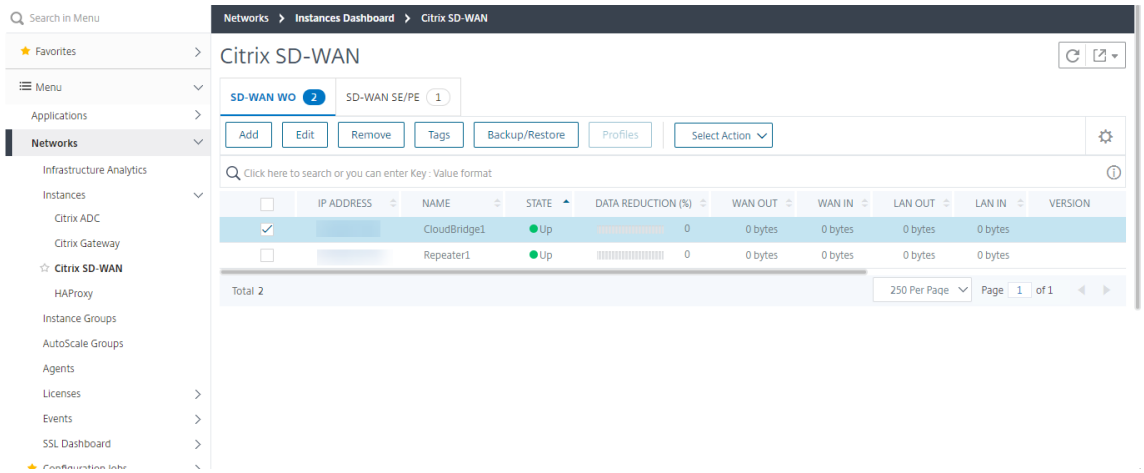
有关自定义用户如何备份 Citrix SD-WAN 实例的信息，请参阅本主题中的“为自定义用户创建 Citrix SD-WAN WANOP 实例的备份”部分。

请确保将 Citrix SD-WAN 实例添加到 Citrix ADM 中了解更多信息，请参阅 将实例添加到 Citrix ADM。

要为 **Citrix SD-WAN** 实例创建备份，请执行以下操作：

1. 在 Citrix ADM 中，导航到“网络”>“实例”>“ **Citrix SD-WAN**”。

2. 在 **SD-WAN WO** 中，选择要备份的 Citrix SD-WAN 实例，然后单击备份/还原。



3. 在“备份文件”页上，单击“备份”。
4. 使用以下任一选项对备份文件进行加密：
   - 选择 受密码保护的文件，然后输入密码以加密备份文件。
   - 选择 使用全局密码以使用您在实例备份设置页面上指定的全局密码。
5. 单击 创建备份

为自定义用户创建 **Citrix SD-WAN** 实例的备份

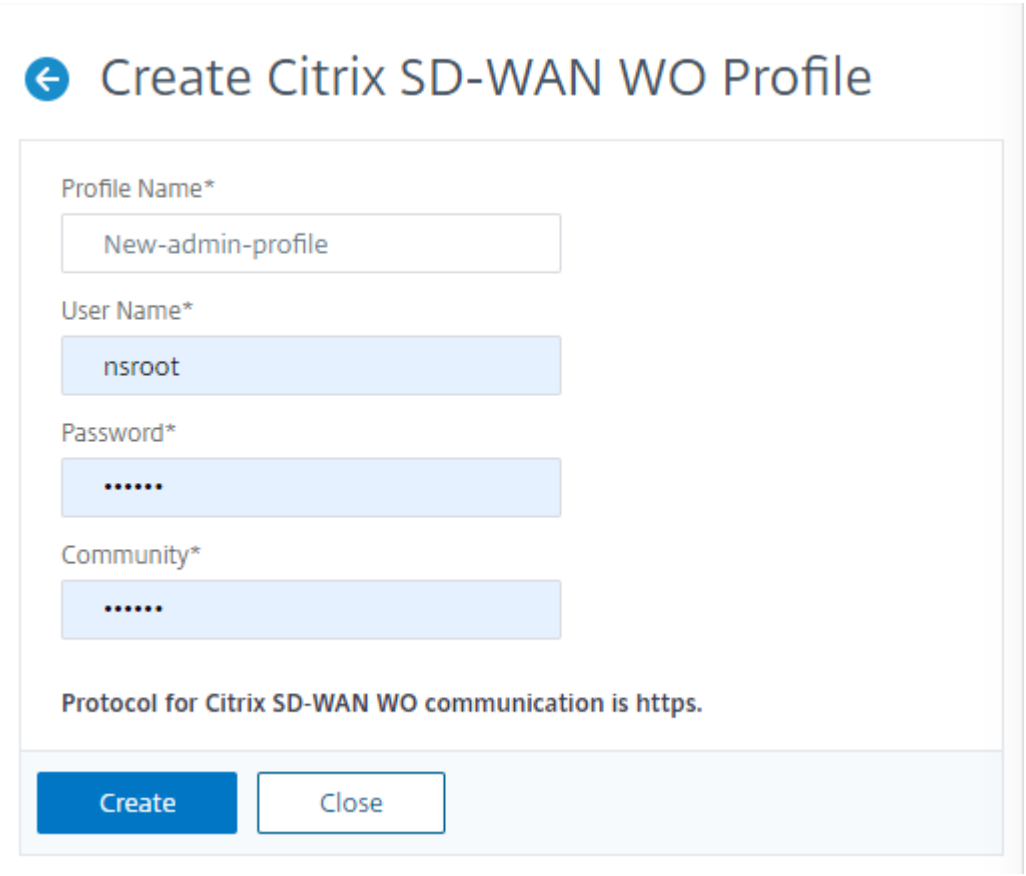
如果您已在 Citrix SD-WAN 实例中创建了具有管理员权限的自定义用户，请使用以下过程添加实例并使用 Citrix ADM 备份该实例。

自定义用户的备份操作不受支持在自定义用户的支持。

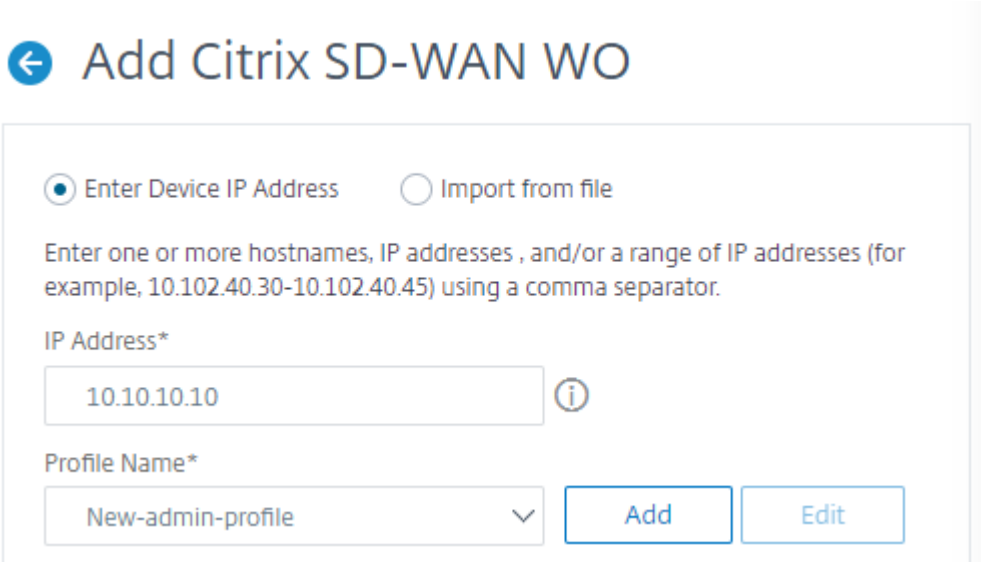
> 注意
>
> Citrix 建议您在 Citrix ADM 中创建 Citrix SD-WAN 高级平台的备份时使用默认 nsroot 配置文件。

要添加 **Citrix SD-WAN WANOP** 实例并为自定义用户执行备份，请执行以下操作：

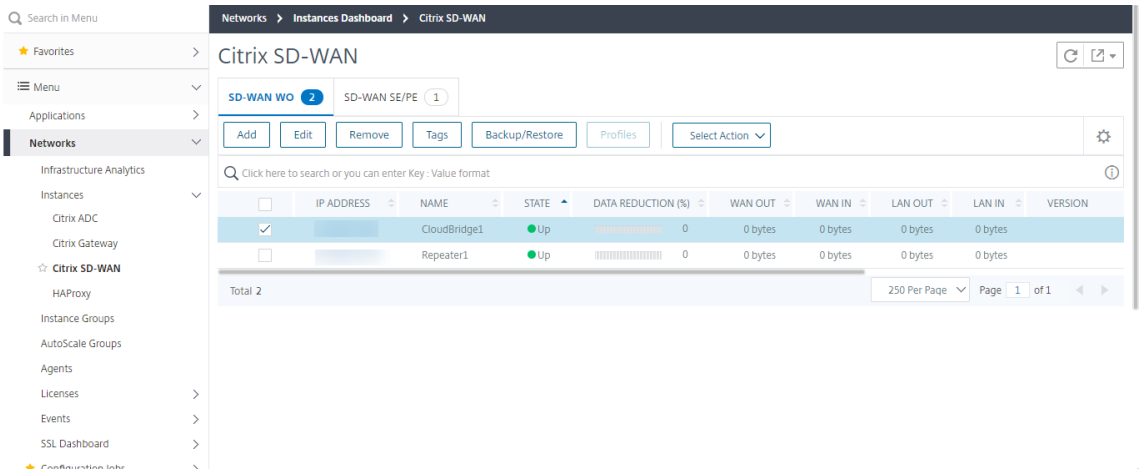
1. 在 Citrix ADM 中，导航到“网络”>“实例”>“ **Citrix SD-WAN”**，然后选择 **“SD** 广域网”。
2. 单击添加。
3. 在 **IP** 地址字段中，输入 Citrix SD-WAN 实例的 IP 地址。
4. 单击“ 配置文件名称”字段旁边的 添加以创建新的配置文件。此时将显示“ 创建 **Citrix SD-WAN WO** 配置文件”窗口。



5. 在 配置文件名字段中，输入配置文件的名称。
6. 在 用户名字段中，输入您在 SD-WAN WANOP 实例上创建的自定义用户的用户名。
7. 在 “ 密码” 字段中，输入您在 SD-WAN WANOP 实例中为自定义用户设置的密码。
8. 在 “ 社区” 字段中，输入在 SD-WAN WANOP 装置上配置的 SNMP 通信字符串。（例如：公共）
9. 单击创建。
10. 在 “ 配置文件名称” 字段中，选择新创建的配置文件，然后单击 “ 确定”。



11. 导航至“网络”>“实例”>“ **Citrix SD-WAN**”。
12. 在 **SD-WAN WO** 中，选择刚刚添加的 Citrix SD-WAN 实例，然后单击备份/还原。



13. 在“备份文件”页上，单击“备份”。
14. 使用以下任一选项对备份文件进行加密：
    - 选择 受密码保护的文件，然后输入密码以加密备份文件。
    - 选择 使用全局密码以使用您在实例备份设置页面上指定的全局密码。

    > 注意
    >
    > 您可以将加密的备份文件下载到本地计算机，但无法查看其内容。只有 Citrix ADM 可以将这些备份文件用于还原目的。恢复加密备份将提示输入密码。

15. 单击 创建备份。

> 重要
>
> ```
> 1. 对于 Citrix SD-WAN WANOP VPX 装置，Citrix ADM 仅备份 CB 代理配置文件。
> ```
>
> a) 对于高级 Citrix SD-WAN WANOP 平台，Citrix ADM 备份以下内容：·
>
> - CB 代理配置文件
>
> - NTP 配置文件
> - DNS
> - SNMPD 配置文件
> - 系统日志配置文件
> - SSL 证书、密钥和策略
> - SVM 数据库文件
> - 组件（XML 格式）
> - 资源（XML 格式）
>
> 下表中列出了各个文件夹中备份的文件。请注意，如果文件夹名称后接“*”，则备份该文件夹中的所有文件夹。
>
> | 目录 | 子目录或文件 |
> |———-|———————————————————–|
> | /br_broker/ | CB-6bbb660a/ ws.conf |
> | /etc/ | resolv.conf |
> | /mps/ | mps_devices.xml |
> | /mpsconfig/ | ssl/*, ntp.conf, snmpd.conf, syslog.conf |
> | /mpsdb/ | mpsdb_dump.sql |
> | /ns/ | NS-6cbb660a/* |
> | /var/ | mps/policy/*, mps/ssl_certs/ sdx_default_ssl_cert, mps/ssl_keys/ sdx_default_ssl_key, mps/tenants/* |

管理 **HAProxy** 实例

April 23, 2021

HAProxy 是开放源负载平衡器，可以对任何 TCP 或 HTTP 服务进行负载平衡。有关 HAProxy 的更多信息，请参阅 http://www.haproxy.org/。

Citrix Application Delivery Management（Citrix ADM）支持 HAProxy 版本 1.4.24 或更高版本。在将已预配置 HAProxy 实例的主机添加到 Citrix ADM 时，Citrix ADM 会发现主机上的 HAProxy 实例并使您能够监视这些实例。它将向您显示有关实例上 HAProxy 配置的以下类型信息：

- 前端 - 请求应该如何转发到后端。
- 后端 - 接收转发的请求的一组服务器。
- 服务器 - HAProxy 用于对流量进行负载平衡的服务器。

有关详细信息，请参阅http://www.haproxy.org/download/1.7/doc/configuration.txt。

此外，Citrix ADM 还提供了 HAProxy 应用程序仪表板，您可以在其上实时监控前端。有关详细信息，请参阅 HAProxy App Dashboard（HAProxy 应用程序控制板）。

将 **HAProxy** 实例添加到 **Citrix ADM**

April 23, 2021

在 Citrix Application Delivery Management (Citrix ADM) 中，您需要手动添加已置备 HAProxy 实例的主机的详细信息。添加这些详细信息后，Citrix ADM 会自动发现在主机上置备的 HAProxy 实例并将其添加到 Citrix ADM 清单中。它还会发现 HAProxy 实例上配置的所有前端、后端和服务器，并将前端视为发现的应用程序。

必备条件

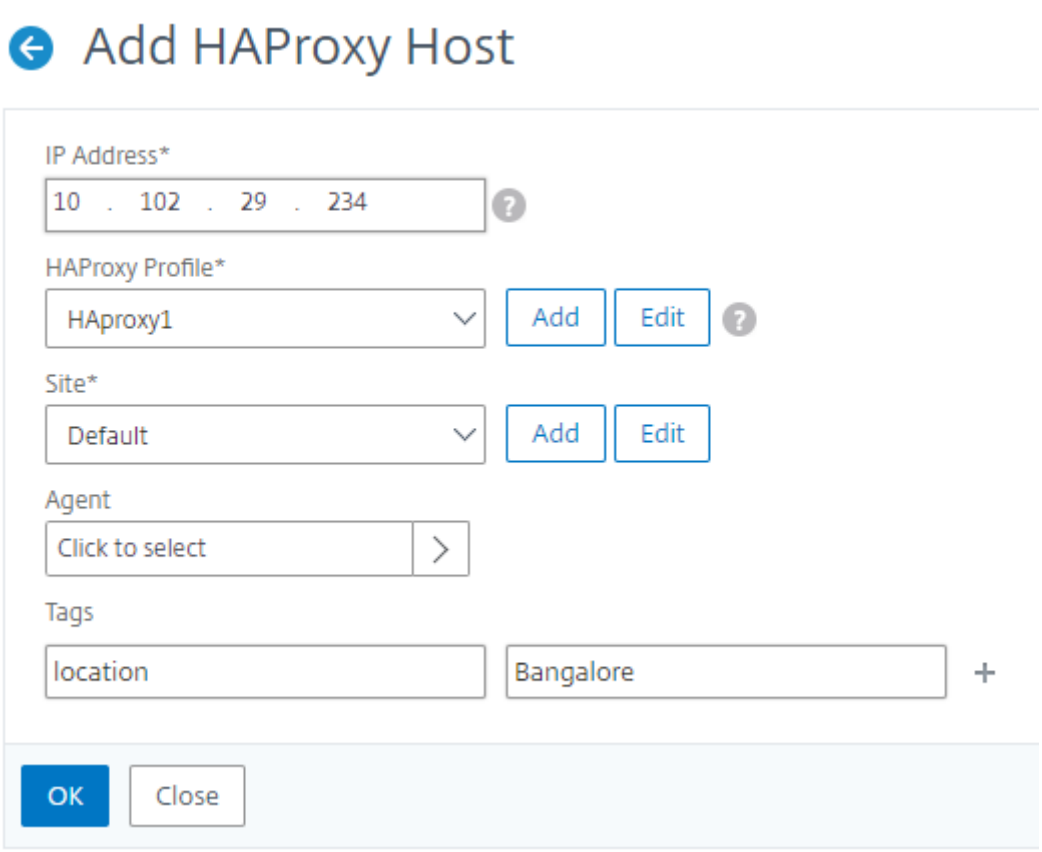
请务必执行以下操作：

- 在您的部署中的主机上部署了 HAProxy 实例。有关详细信息，请参阅http://www.haproxy.org/#docs。
- 确定并决定要在 HAProxy App 控制面板上查看应用程序统计信息的前端数量。默认情况下，“HAProxy App Dashboard”（HAProxy 应用程序控制板）显示 30 个发现的应用程序的统计信息。有关 HAProxy 应用程序仪表板的更多信息，请参阅 HAProxy App Dashboard（HAProxy 应用程序控制板）。如果要查看 30 多个已发现应用程序的统计信息，则必须购买单独的许可证。有关详细信息，请参阅第三方许可。

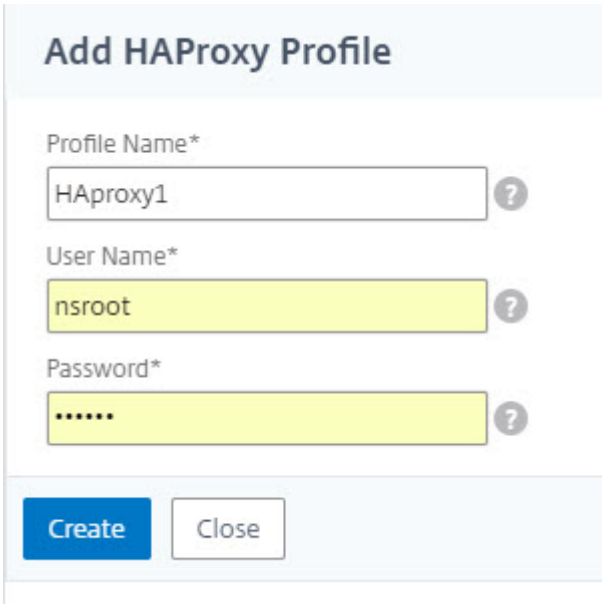
> 重要
>
> Citrix ADM 需要访问主机才能发现其中的 HAProxy 实例。您可以通过提供主机的 SSH 密钥对或使用主机密码来提供对 Citrix ADM 的访问。如果您要使用 SSH 密钥对提供访问权限，请务必在主机中生成 SSH 私钥和公钥对，并将公钥添加到主机上的授权密钥。此外，SSH 用户帐户必须具有超级用户权限。

要将 **HAProxy** 实例添加到 **Citrix ADM**，请执行以下操作：

1. 导航到 “ 网络” > “ 实例”。在 实例下，选择 **HAProxy** ，然后单击 添加。
2. 在 “ 添加 **HAProxy** 主机” 对话框中，执行以下操作：



1. 在 **IP** 地址字段中，输入已置备 HAProxy 实例的主机的 IP 地址。
    a) 在 **HAProxy** 配置文件菜单中，选择一个现有的 HAProxy 配置文件，或者创建并选择一个新的 HAProxy 配置文件。要创建 HAProxy 配置文件，请单击 添加。
        i. 在添加 **HAProxy** 配置文件对话框中，执行以下操作：



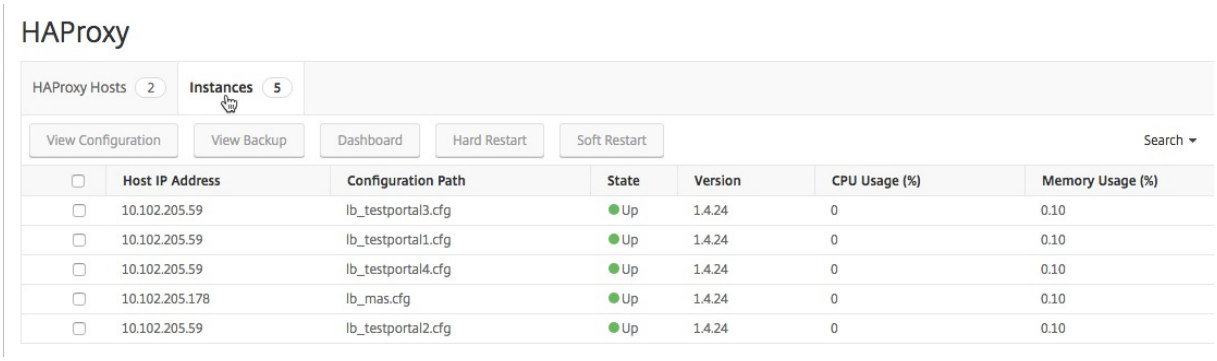
i. 在 “ 配置文件名称” 字段中，输入配置文件名称。

ii. 在 “用 户名” 和 “ 密码” 字段中，输入主机的用户凭据。

iii. 单击创建。

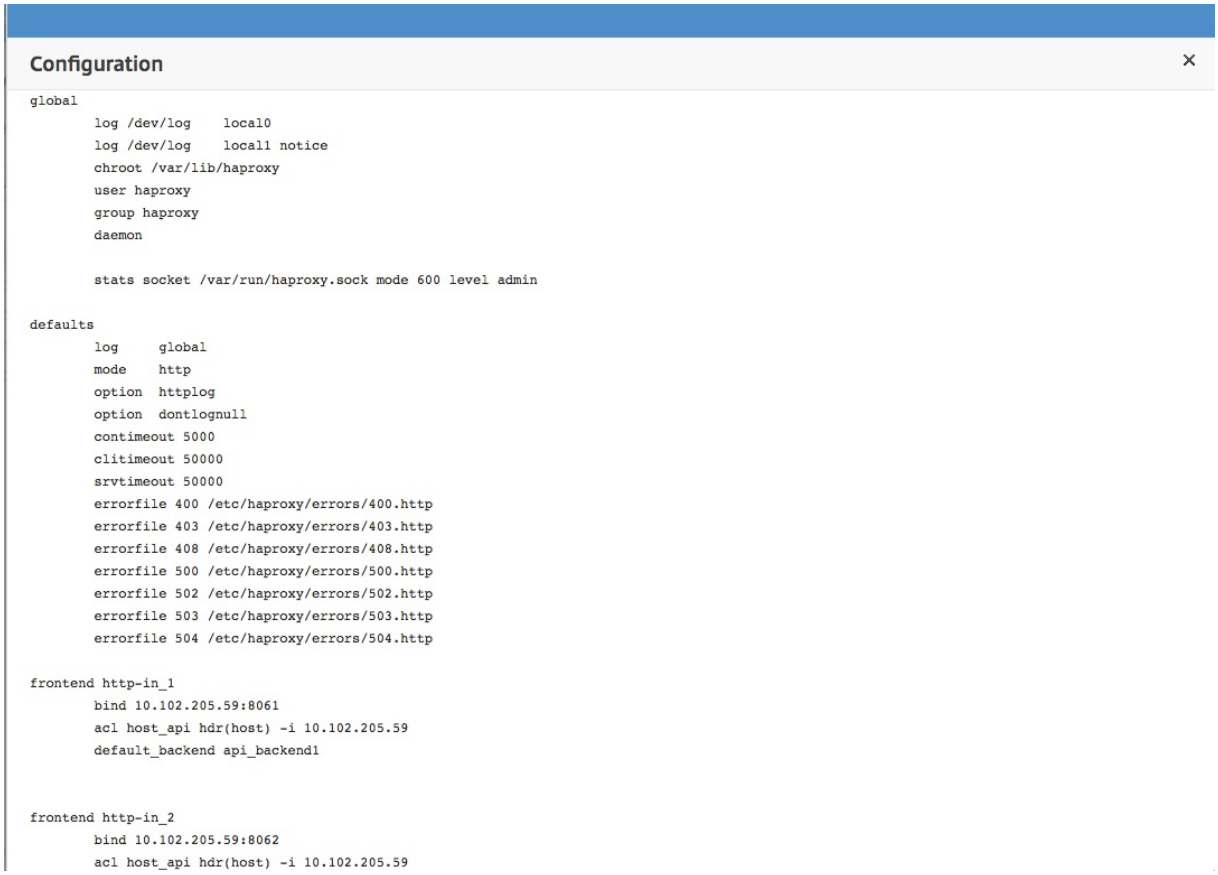
2. 从 “ 站点” 菜单中，选择 HAProxy 站点。要创建新站点并将其添加到菜单中，请单击 “ 添加”。
3. 从 “ 代理” 菜单中，选择一个代理。
4. 在 “标签” 字段中，相应地输入值。
5. 单击确定。

Citrix ADM 会发现在主机上预配置的 HAProxy 实例，您可以在 “实例” 选项卡上查看所有 HAProxy 实例。



查看 **HAProxy** 实例的配置

要查看 Citrix ADM 中 HAProxy 实例的配置，请导航到 “ 网络” > “实 例” > “ **HAProxy** ”，然后在 “实 例” 选项卡上，选择 HAProxy 实例，然后单击 “ 查看配置”。



HAProxy 应用程序控制板

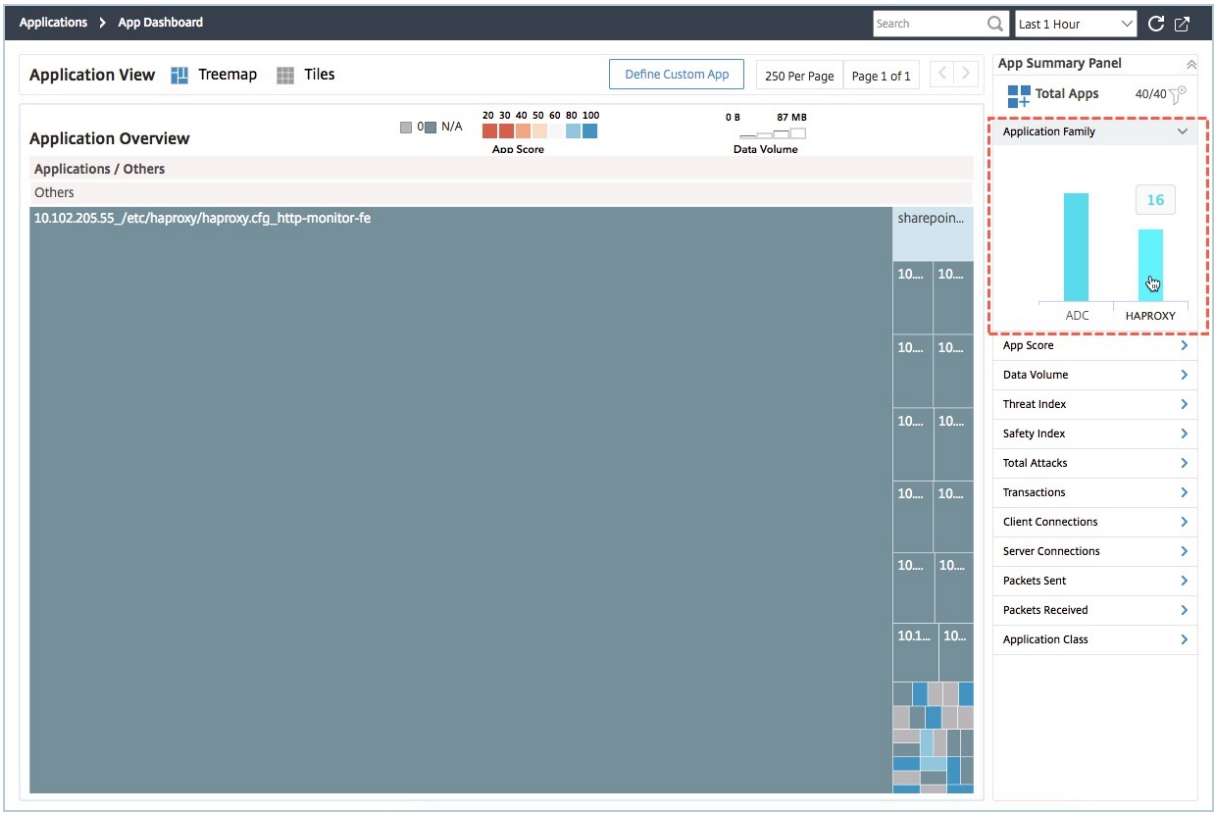
April 23, 2021

应用程序仪表板提供 Citrix 应用程序交付管理 (Citrix ADM) 监控的所有 HAProxy 前端的实时统计信息。它将前端列为离散应用程序，并提供有关应用程序的事务、吞吐量和会话信息。

> 重要
>
> 确保在 HAProxy 实例配置文件中启用了 统计信息。要启用 统计信息，请编辑 HAProxy 配置文件，然后在默认值部分之后添加一个类似于以下示例中的条目：

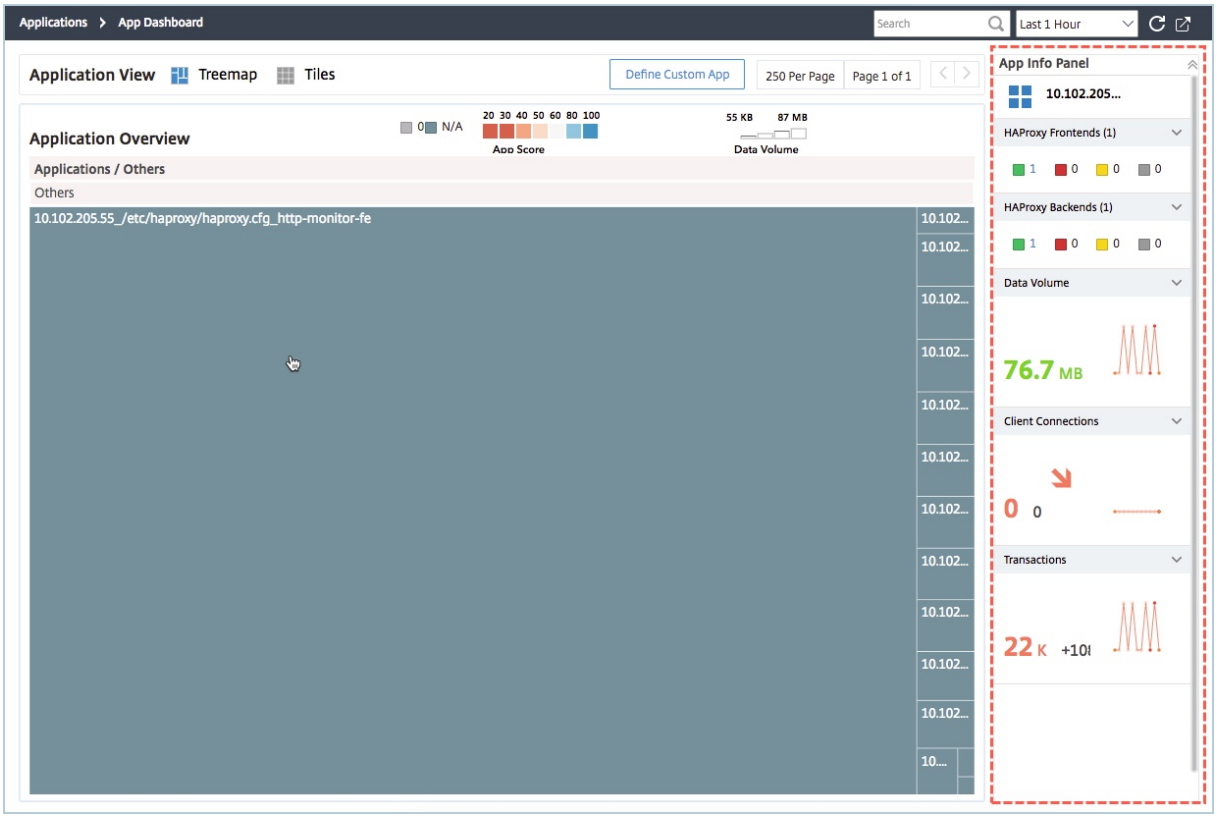
```
    listen stats :9000  # Listen on localhost:9000
    mode http
    stats enable  # Enable stats page
    stats hide-version  # Hide HAProxy version
    stats realm Haproxy\ Statistics  # Title text for popup window
    stats uri /haproxy_stats  # Stats URI
    stats auth Username:Password  # Authentication credentials
<!--NeedCopy-->
```


要访问 Citrix ADM 中应用程序仪表板上的 HAProxy 应用程序，在将 HAProxy 实例添加到 Citrix ADM 后，请导航“应用程 序”>“ 仪表板”。您可以筛选仪表板以仅显示 HAProxy 应用程序，要筛选仪表板，请选择“应用程序摘要信息面板”的“应用程 序系列”部分下显示的 **HAPROX** Y。



查看 **HAProxy** 应用程序的关键指标

向下钻取 HAProxy 应用程序时，应用程序信息面板处于第一级。该面板显示应用程序的主要指标和组件，以及其状态。例如，对于任何选定的 HAProxy 应用程序，应用程序信息面板会显示 HAProxy 前端的总数、HAProxy 后端总数、数据量、客户端连接趋势以及事务。要查看 HAProxy 应用程序的关键指标，请单击应用程序控制面板上的 **HAProxy** 应用程序磁贴。然后，应用程序信息面板将替换 应用程序摘要面板。

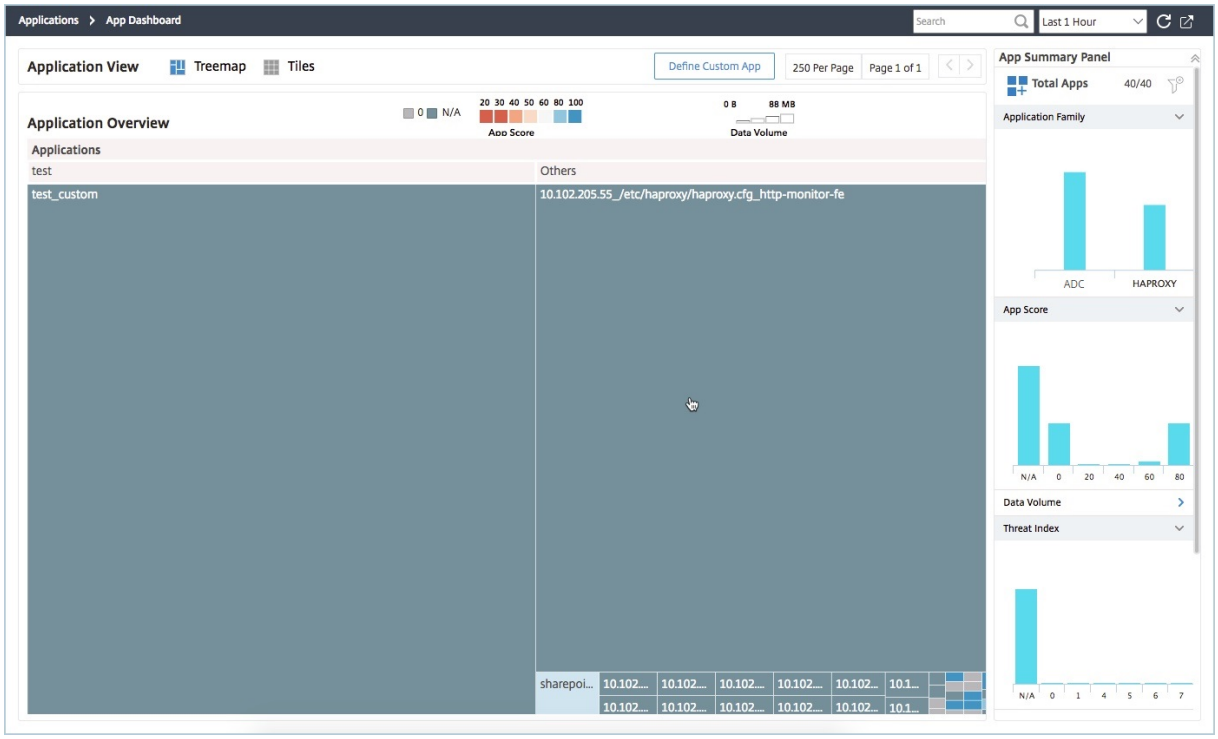


查看 **HAProxy** 应用程序的实时性能

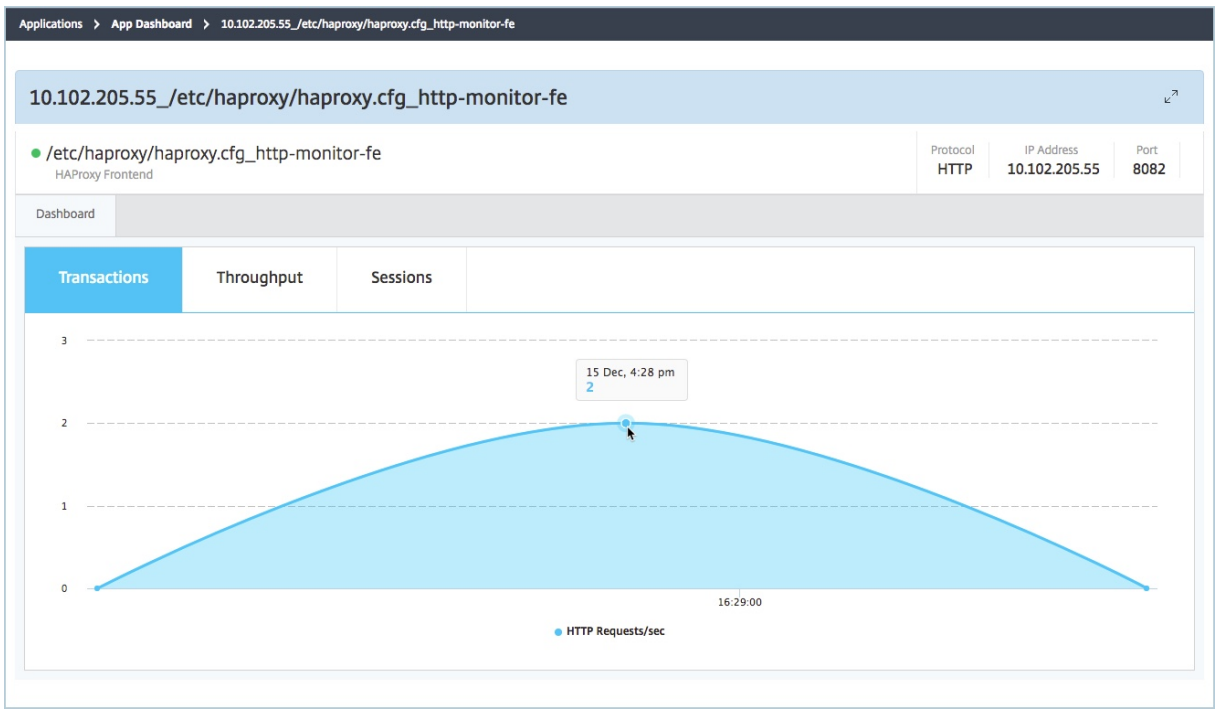
通过 Citrix ADM，您可以查看 HAProxy 应用程序的实时性能。它提供了所选 HAProxy 应用程序的以下实时详细信息：

- 交易。应用程序执行的事务。
- 吞吐量。应用程序的吞吐量。
- 会话。应用程序建立的会话数。

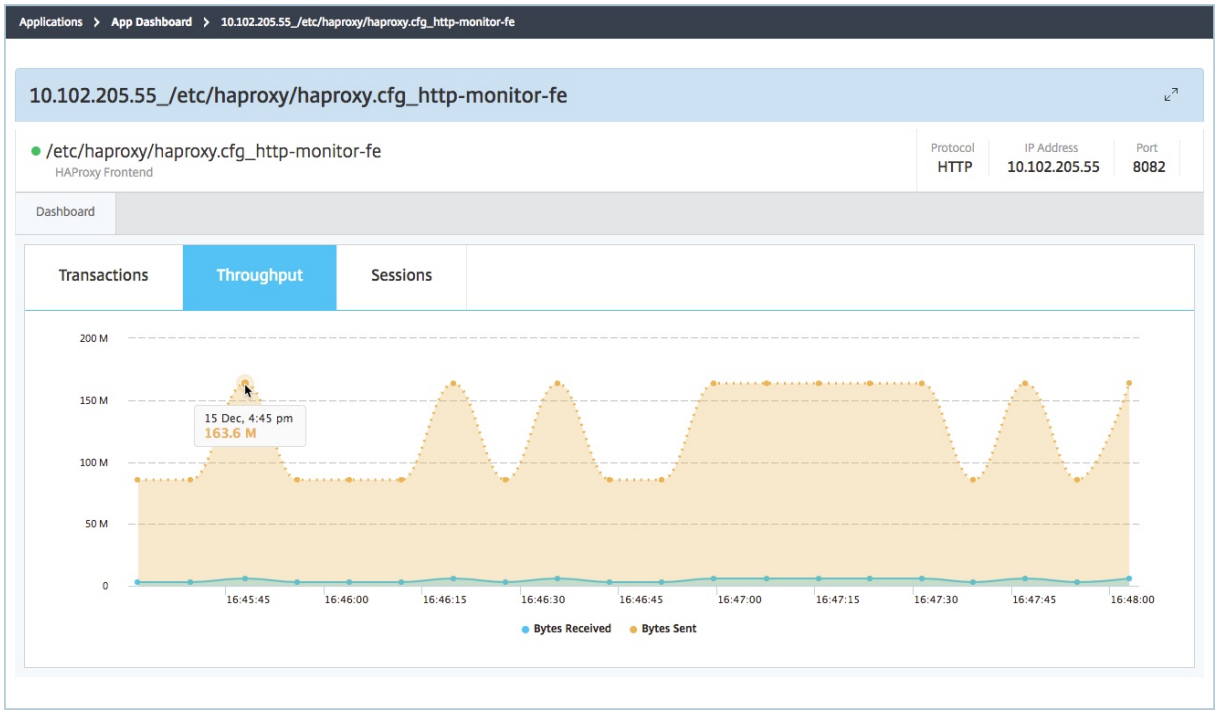
要查看 HAProxy 应用程序的实时性能，请在应 用程序仪表板上双击 HAProxy 应用程序磁贴。



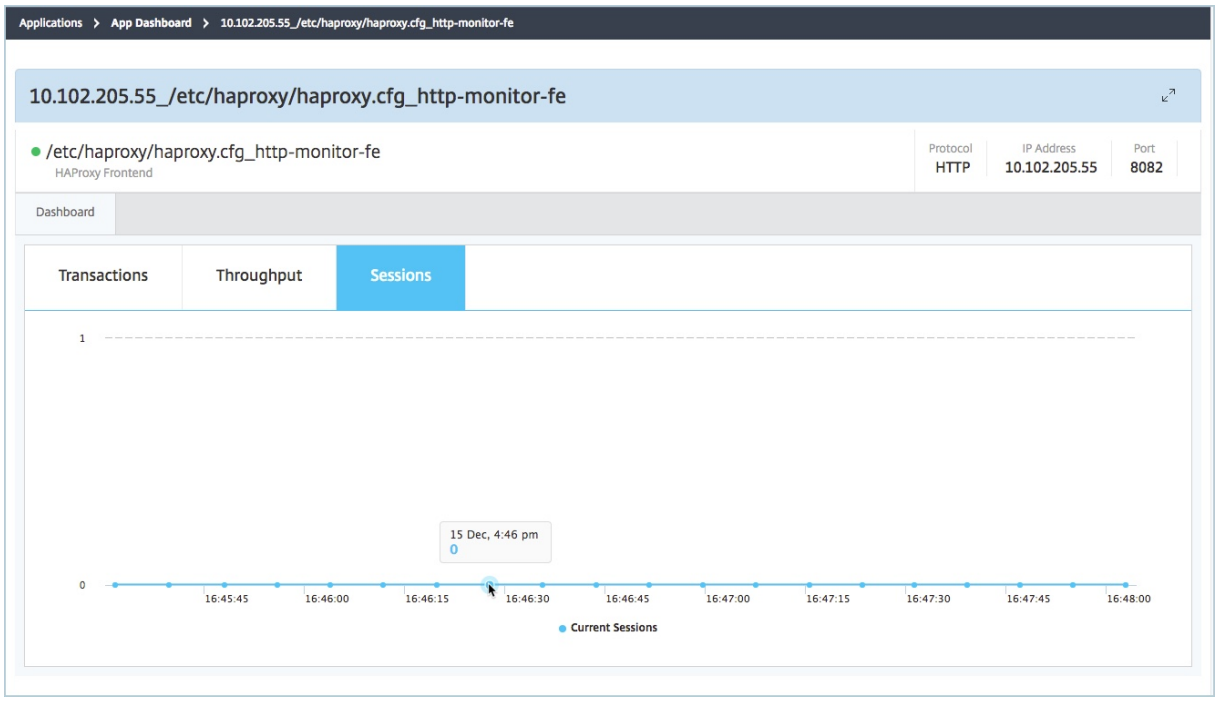
默认情况下，“事 务处理”选项卡处于选中状态，并显示应用程序执行的实时事务处理。



要查看应用程序的实时吞吐量，请单击 吞吐量选项卡。



您可以单击“会 话”选项卡以查看应用程序实时建立的会话数。

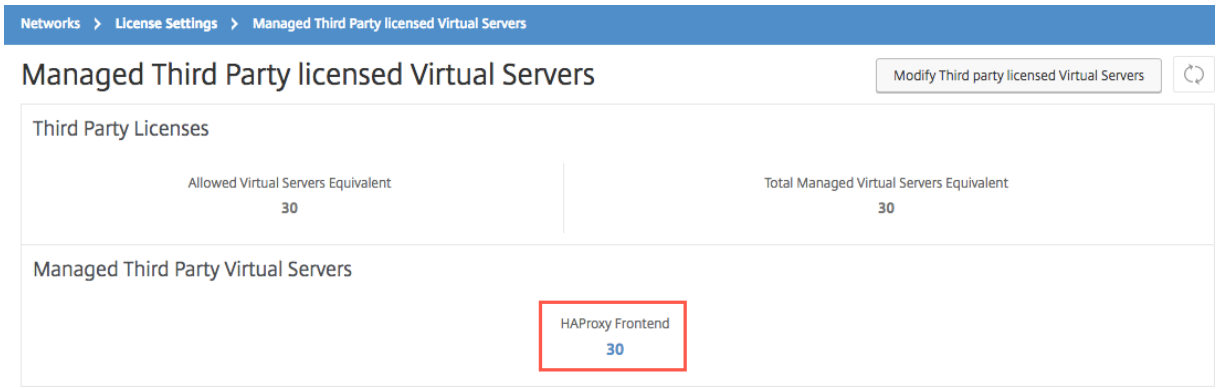


第三方许可

April 23, 2021

将主机添加到 Citrix Application Delivery Management (Citrix ADM) 后，Citrix ADM 会自动发现在主机上置备的 HAProxy 实例并将其添加到 Citrix ADM 清单中。它还会发现 HAProxy 实例上配置的所有前端、后端和服务器，并将前端视为已发现的应用程序。

您可以管理和监视所有发现的应用程序，但默认情况下，“HAProxy App Dashboard”（HAProxy 应用程序控制板）显示 30 个发现的应用程序的应用程序统计信息。有关 “HAProxy App Dashboard”（HAProxy 应用程序控制板）的详细信息，请参阅 “HAProxy App Dashboard（HAProxy 应用程序控制板）”。如果要查看 30 个以上发现的应用程序的应用程序统计信息，需要购买单独的许可证。



更多前端的许可证可以在 100 个虚拟服务器包中获得。您可以使用 Citrix ADM GUI 获取有效的许可证并安装许可证。

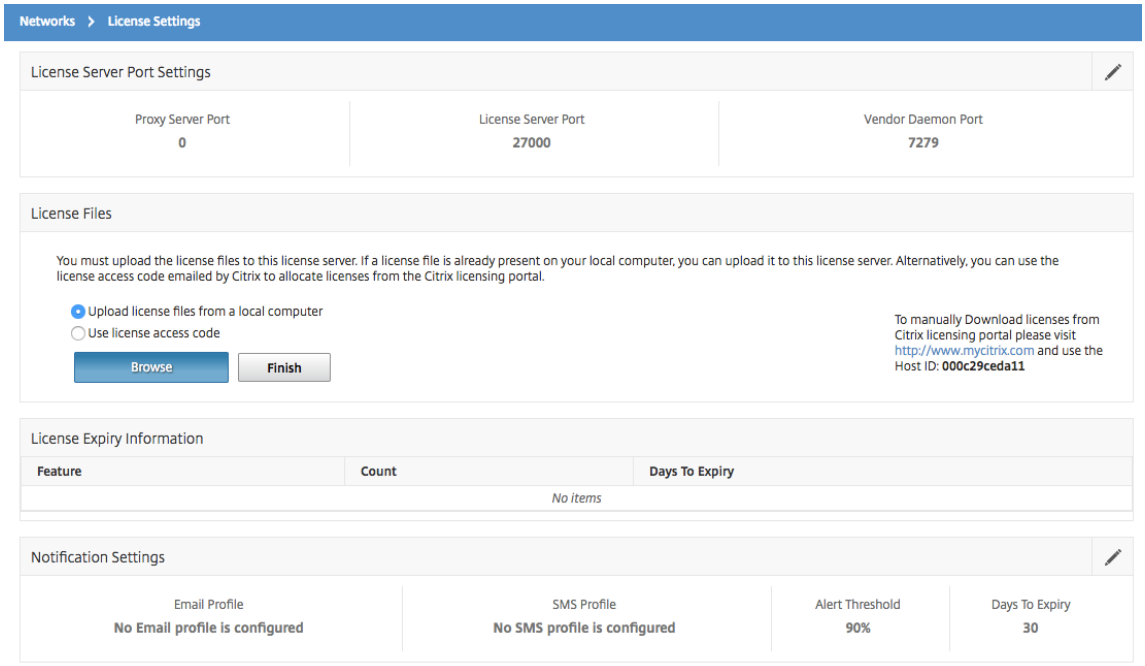
安装第三方许可证

您可以在 Citrix ADM 上安装许可证，以查看 30 多个发现的应用程序的应用程序统计信息。

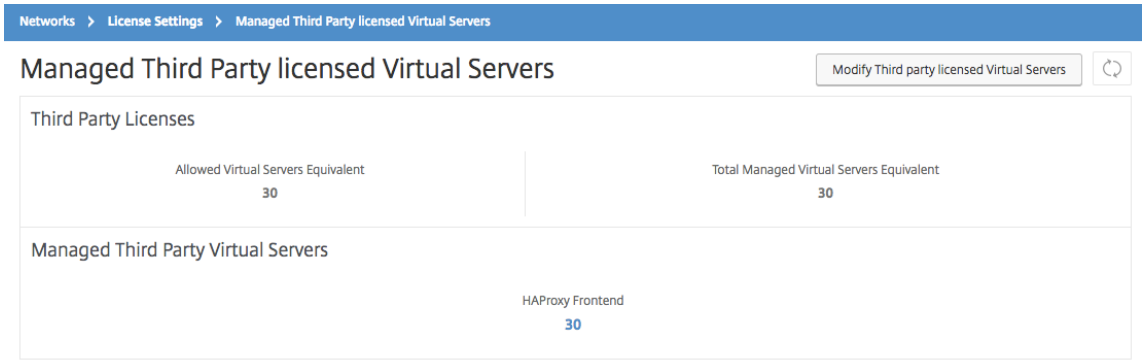
要安装许可证，请执行以下操作：

1. 导航到 “ 网络” > “ 许可证”。
2. 在 “许可证文件” 部分，选择以下选项之一：
   - 从本地计算机上载许可证文件。如果您的本地计算机上已经有许可证，请单击 “Browse”（浏览）并选择要用于分配您的许可证的许可证文件 (.lic)。单击完成。
   - 使用许可证激活码 -Citrix 通过电子邮件发送您购买的许可证密钥。在文本框中输入许可证密钥，然后单击获取许可证。

> 注意
>
> 如果选择此选项，则 Citrix ADM 必须连接到 Internet，否则必须有代理服务器可用。



您可以通过导航到 “ 网络” > “许可证” > “ 第三方许可证” 来验证 **Citrix ADM** 上安装的许可证。

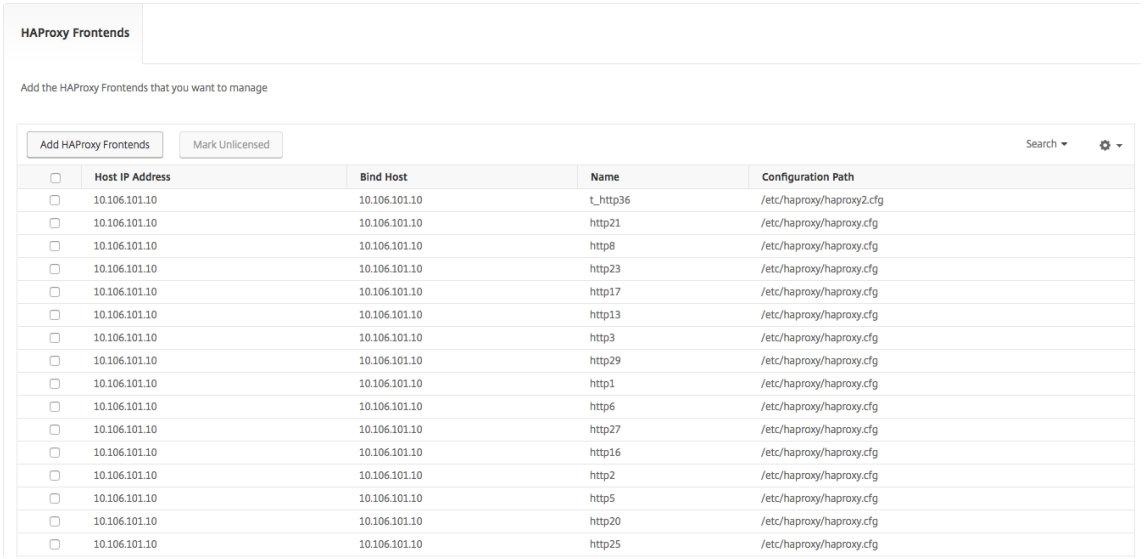


管理第三方许可证

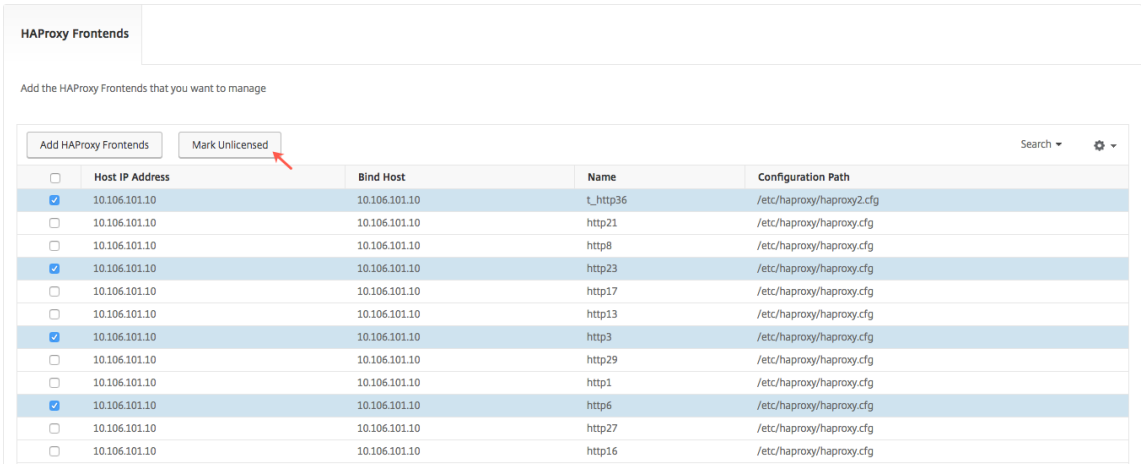
Citrix ADM 会随机选择 HAProxy 实例中发现的应用程序，并自动对其进行许可。如果您要更改选定的发现应用程序，您需要手动取消许可已许可的发现应用程序，然后将许可证分配给您要许可的发现应用程序。

要管理第三方许可证，请执行以下操作：

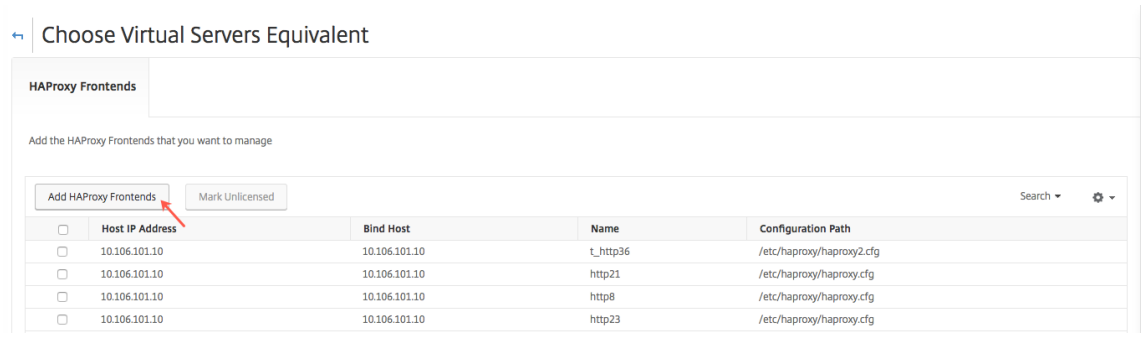
1. 导航到 网络 > 许可证 > 第三方许可证，然后单击 修改第三方许可证的虚拟服务器。仪表板显示受管理的前端。



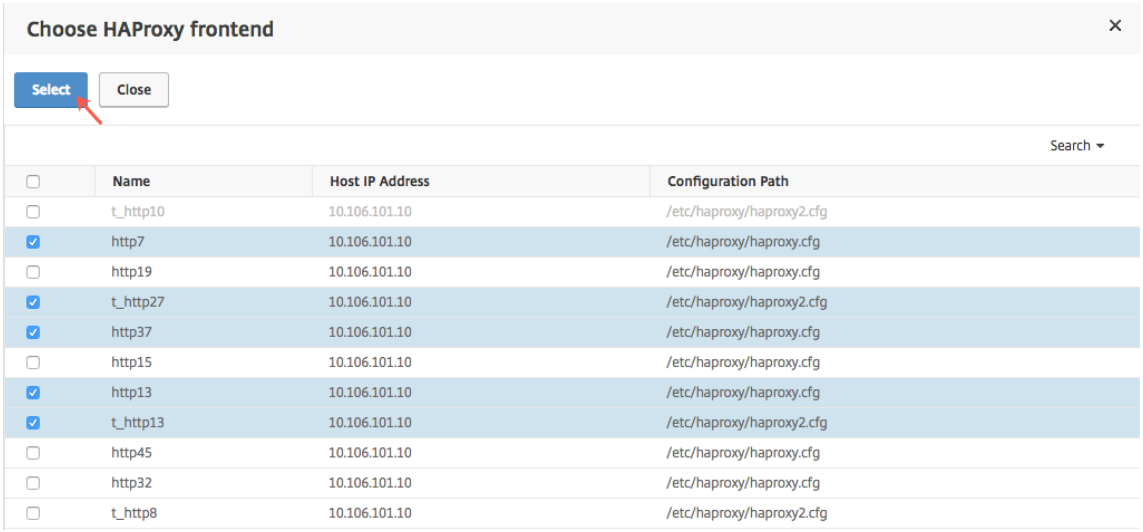
2. 从列表中选择前端“ 标记为未许可”，然后单击“ 完成”以释放许可证。



3. 释放许可证后，或者如果您已有可用的许可证，请单击 添加 **HAProxy** 前端。



4. 在“ 选择 **HAProxy** 前端”对话框中，从列表中选择未许可的前端，然后单击 **“**选择”。



5. 单击 “ 立即完成”。

基于角色的 **HAProxy** 实例访问控制

April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 使用精细的基于角色的访问控制 (RBAC) 来控制对配置对象的访问。例如，您可以创建用户并为其提供对特定 HAProxy 实例的访问权限，以及可以指定针对 “HAProxy App Dashboard”（HAProxy 应用程序控制板）的查看/只读权限。有关详细信息，请参阅Citrix ADM 中基于角色的访问控制。

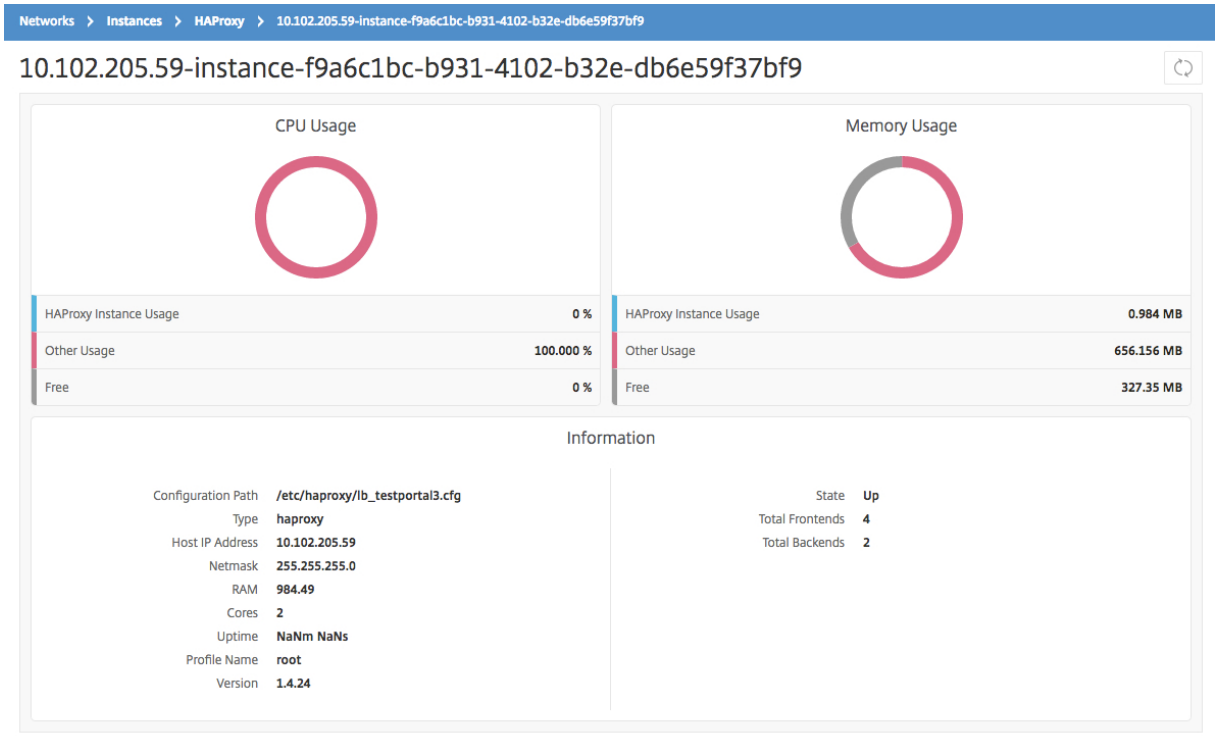
监视 **HAProxy** 实例

April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 中的 HAProxy 仪表板显示有助于跟踪 HAProxy 实例的 CPU 和内存使用情况的图形。该控制板还显示指示以下信息的图形：

- 主机上的 HAProxy 实例使用的 CPU 的百分比。
- 主机上的其他实体使用的 CPU 的百分比。
- 主机上剩余的 CPU 的百分比。
- 主机上的 HAProxy 实例使用的内存的百分比。
- 主机上的其他实体使用的内存的百分比。
- 主机上剩余的内存的百分比。

要监视 Citrix ADM 中的 HAProxy 实例，请导航到 网络 > 实 例 > **HAProxy** > 实 例选项卡，选择 HAProxy 实例，然后单击 仪表板。



查看在 **HAProxy** 实例上配置的前端的详细信息

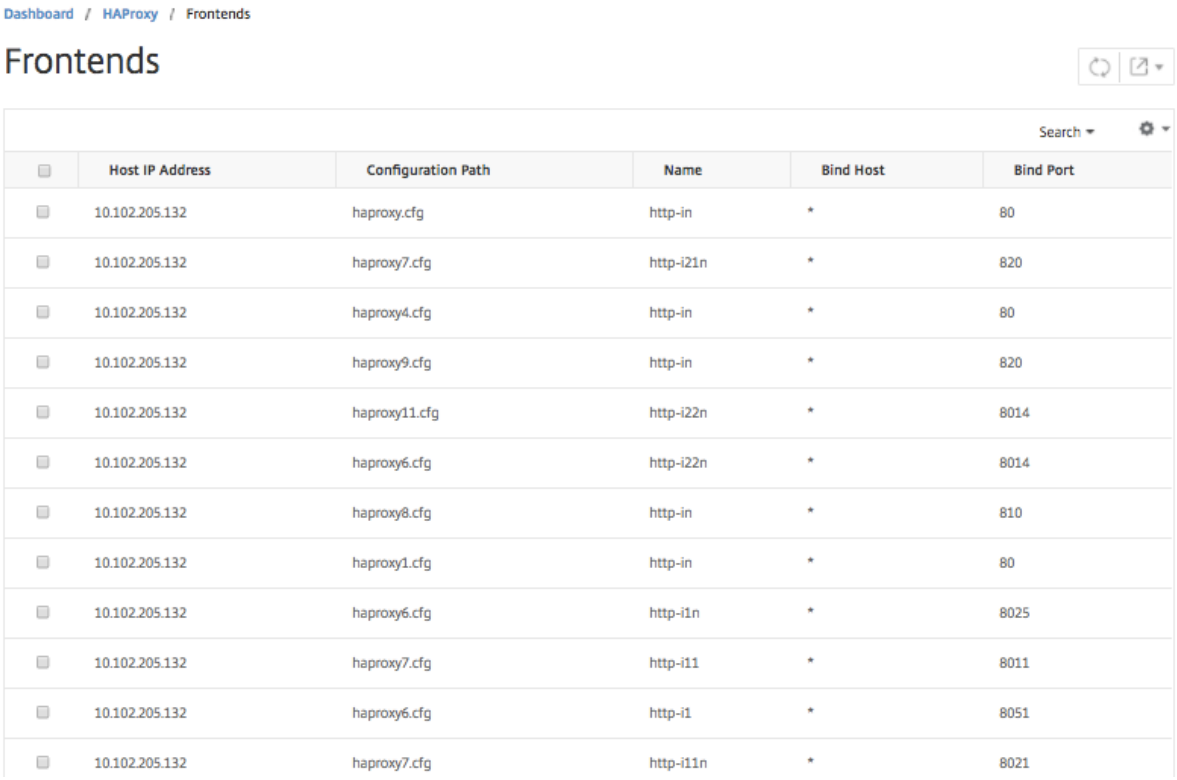
April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的前端的以下详细信息：

- 主机 **IP** 地址。主机的 IP 地址
- 配置路径。主机上 HAProxy 实例的绝对配置路径。
- 名称。处理传入流量的前端的名称。
- 绑定主机。前端绑定到的 IP 地址。
- 绑定端口。前端绑定到的端口。

要查看 **HAProxy** 实例上配置的前端，请执行以下操作：

在 Citrix ADM 中，导航到 “网 络” > “网络功能” > “**HAProxy**” > “前端”。



查看 **HAProxy** 实例上配置的后端的详细信息

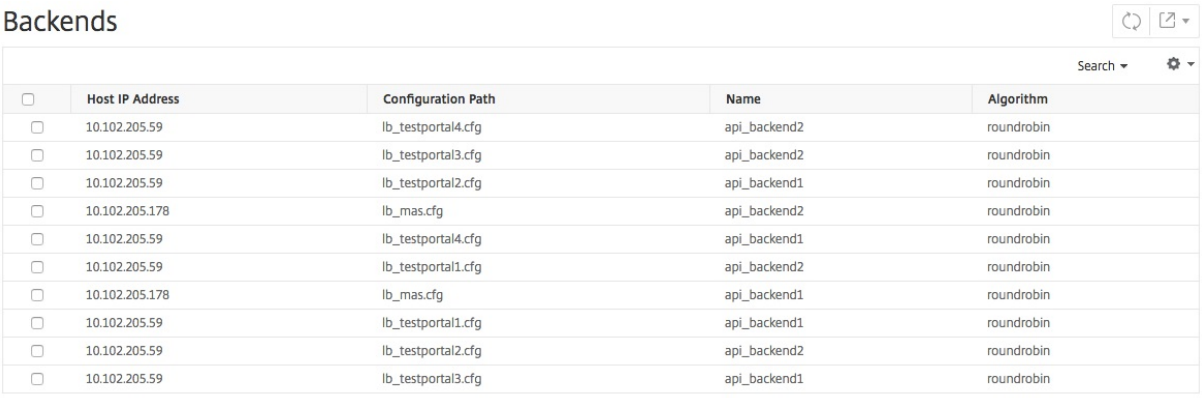
April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的后端应用程序的以下详细信息：

- 主机 **IP** 地址。主机的 IP 地址。
- 配置路径。主机上的 HAProxy 实例路径。
- 名称。将流量转发到的后端的名称。
- 算法。用于平衡流量的负载平衡算法。

要查看 **HAProxy** 实例上配置的后端，请执行以下操作：

在 Citrix ADM 中，导航到“网 络”>“ 网络功能”>“ **HAProxy** ”>“ 后端”。



查看 **HAProxy** 实例上配置的服务器的详细信息

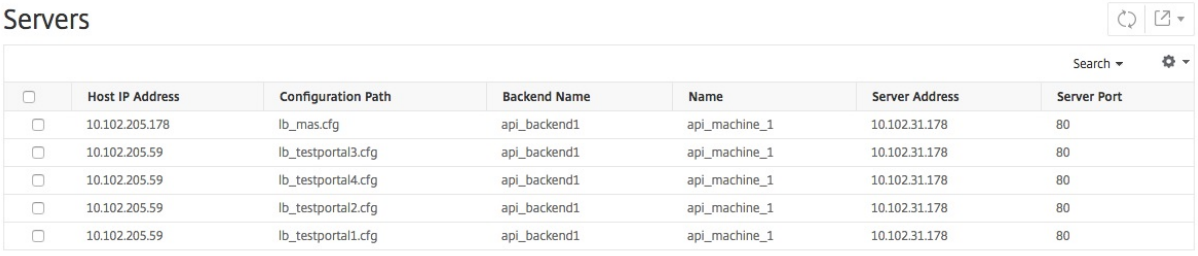
April 23, 2021

Citrix Application Delivery Management (Citrix ADM) 报告在 HAProxy 实例上配置的服务器的以下详细信息：

- 主机 **IP** 地址。主机的名称。
- 配置路径。主机上的 HAProxy 实例配置文件的绝对路径。
- 后端名称。HAProxy 配置中后端的名称。
- 名称。HAProxy 配置中服务器的名称。
- 服务器地址。服务器的 IP 地址。
- 服务器端口。服务器所使用的端口。

要查看 **HAProxy** 实例上配置的服务器，请执行以下操作：

在 Citrix ADM 中，导航到 “网 络**” > “**网络功能” > “**HAProxy**” > “服务器”。

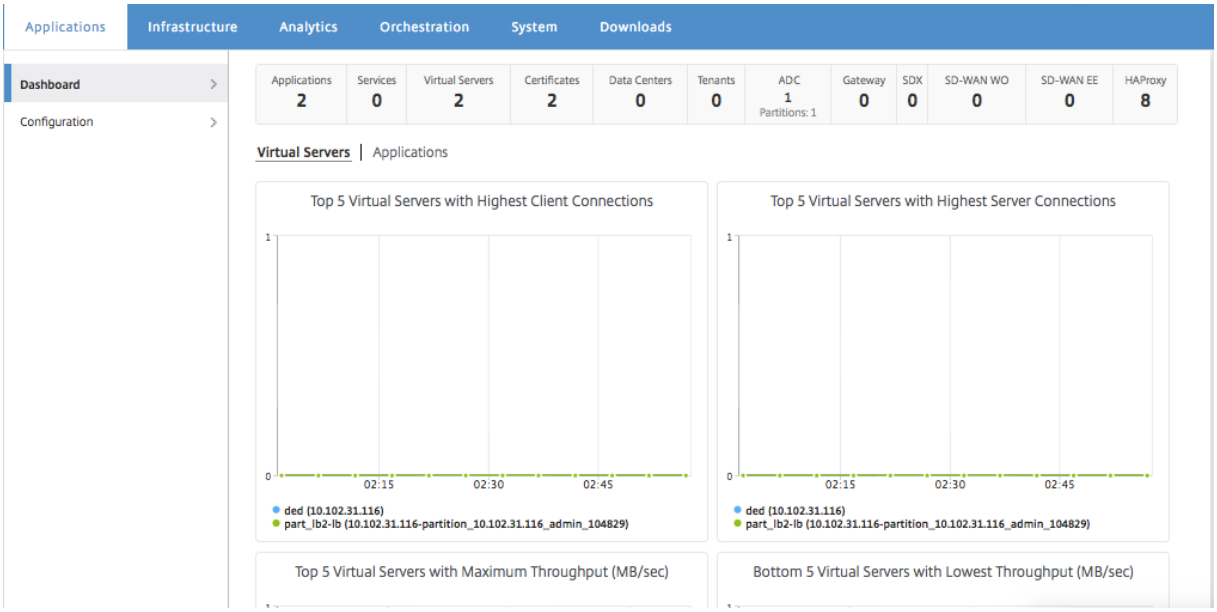


查看前端或服务器数量最多的 **HAProxy** 实例

April 23, 2021

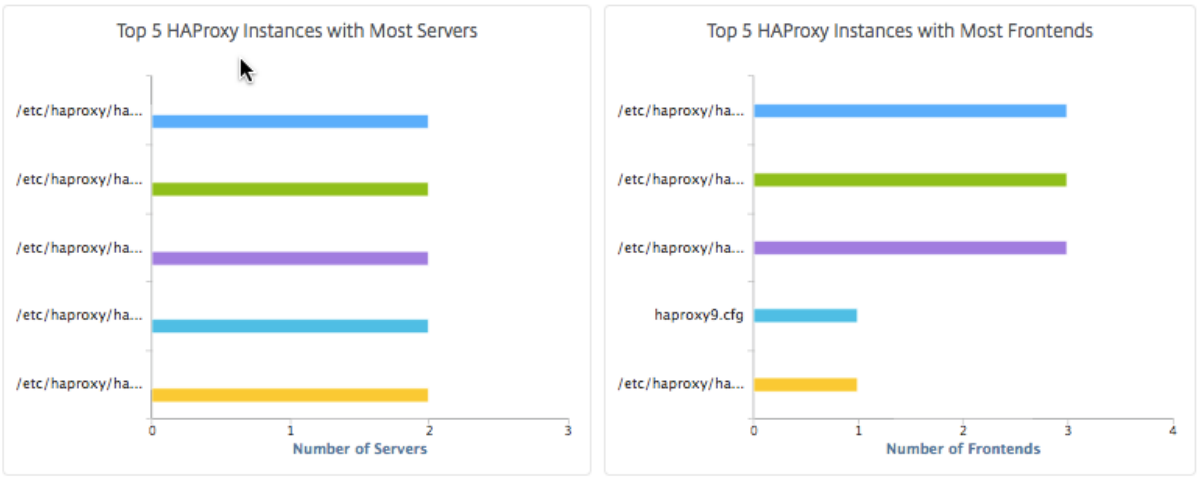
在 应用程序控制板上，Citrix 应用程序交付管理 (Citrix ADM) 显示其发现的 HAProxy 实例的数量，并列出了配置为最多的前端或服务器的五个 HAProxy 实例。

要查看应用程序仪表板，请在 Citrix ADM 中导航到 应用程序 > 仪表板。



Citrix ADM 发现的 HAProxy 实例数显示在顶行中：

要查看配置前端数量最多或服务器数量最多的前五个 HAProxy 实例的列表，请向下滚动控制面板：



重新启动 **HAProxy** 实例

April 23, 2021

要从 Citrix Application Delivery Management (Citrix ADM) GUI 重新启动 HAProxy 实例，可以选择硬重新启动或软重新启动。

硬重启

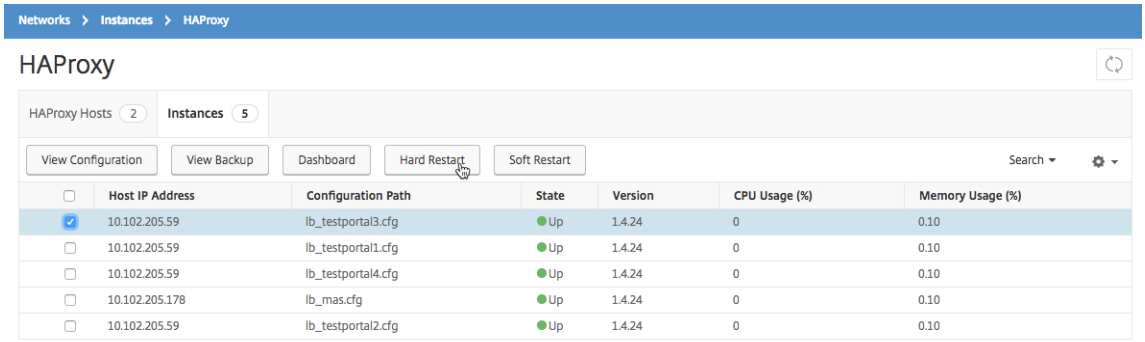
硬重新启动将终止实例上的 HAProxy 进程并关闭所有已建立的连接。重新启动后，将创建一个新的 HAProxy 进程，然后的新连接将由新的 HAProxy 进程处理。

软重启

软重新启动将取消 HAProxy 进程与侦听端口的绑定，但 HAProxy 进程会继续处理现有连接直到其关闭。将创建新 HAProxy 进程来处理新连接。

要重新启动 **HAProxy** 实例，请执行以下操作：

1. 导航到 “ 网络” > “ 实例” > “ **HAProxy** ”，然后单击 “ 实例” 选项卡。
2. 在 实例选项卡上，选择要重新启动的 HAProxy 实例。
3. 单击 硬重新启动硬重新启动 HAProxy 实例，或单击 软重新启动软重新启动 HAProxy 实例。



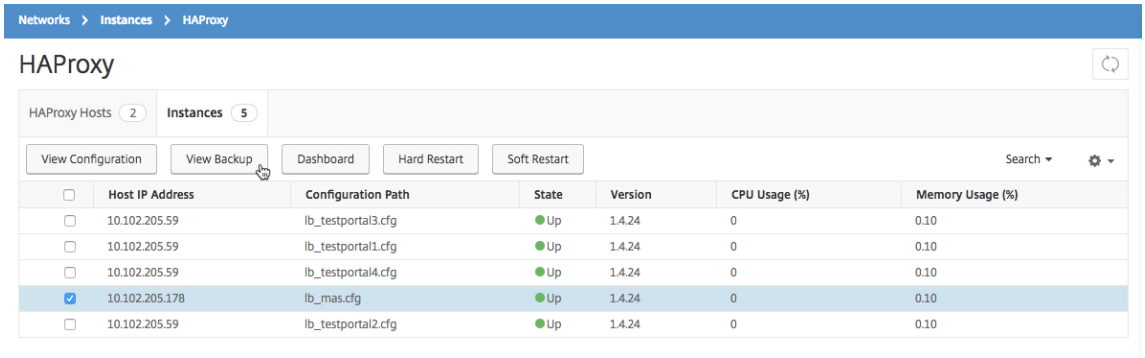
备份和还原 **HAProxy** 实例

April 23, 2021

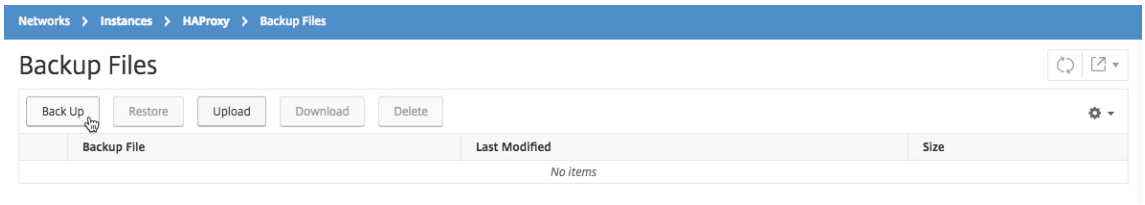
可以在 HAProxy 配置文件中备份 HAProxy 实例的当前状态。如果实例变得不稳定，您可以使用备份的文件将实例恢复到稳定状态。

要使用 **Citrix ADM** 备份 **HAProxy** 实例，请执行以下操作：

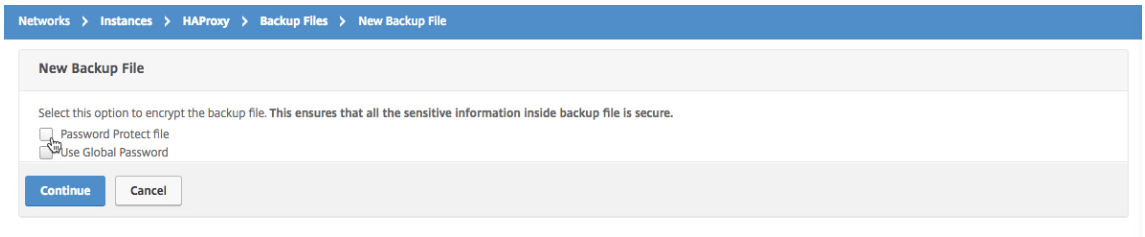
1. 在 Citrix Application Delivery Management (Citrix ADM) 中，导航到 **“网络” > “实例” > “HAProxy”**。
2. 在 **HAProxy** 页面中，单击实 例选项卡。
3. 选择要备份的 HAProxy 实例，然后单击 查看备份。



4. 在备份文件页面上，单击备份。



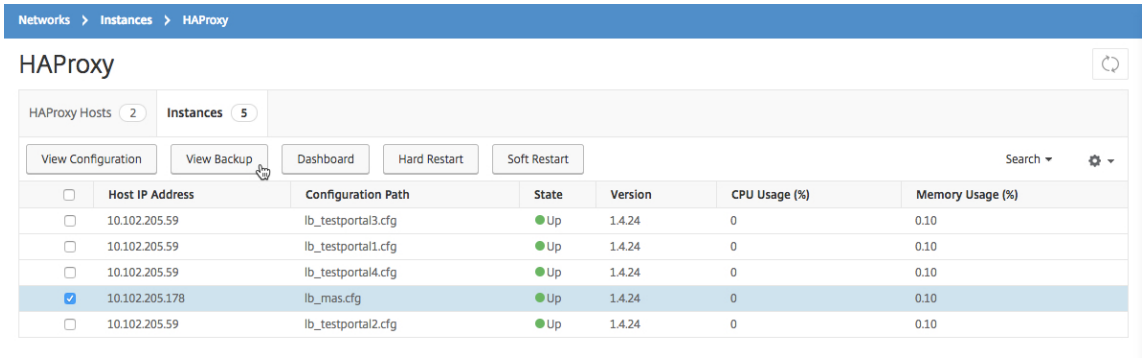
5. 您可以选择加密备份文件以提高安全性。



6. 单击继续。

要使用 **Citrix ADM** 还原实例，请执行以下操作：

1. 导航到 “ 网络” > “ 实例” > “ **HAProxy**”。
2. 在 **HAProxy** 页面上，单击实 例选项卡。
3. 选择要还原的实例，然后单击 查看备份。



4. 在 **Backup Files**（备份文件）页面上，选择要还原的备份文件，然后单击 **Restore**（还原）。

> 注意
>
> 恢复实例时，Citrix ADM 软重新启动 HAProxy 实例。

编辑 **HAProxy** 配置文件

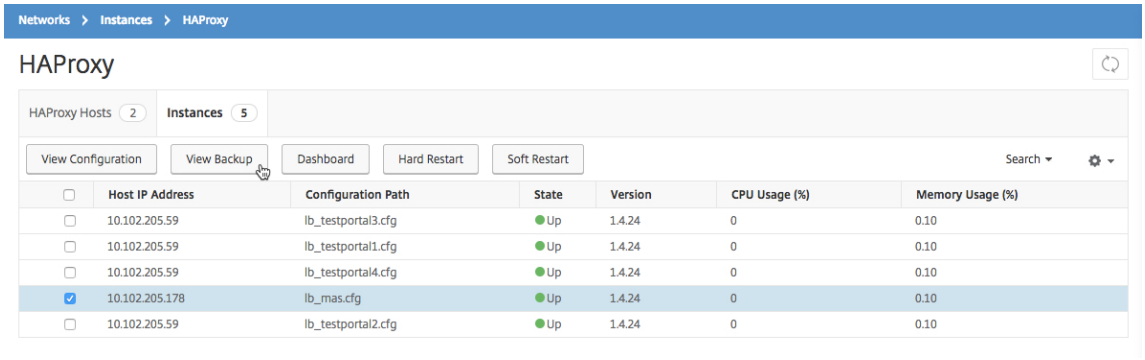
April 23, 2021

您可以更新现有 HAProxy 配置文件中的前端、后端、服务器和其他设置。要编辑 HAProxy 配置文件，请执行以下操作：

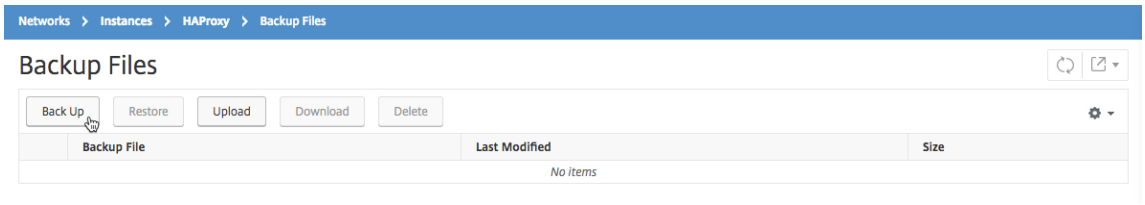
- 备份 HAProxy 配置文件。
- 下载备份 HAProxy 配置文件，然后对其进行脱机编辑。
- 将更新的 HAProxy 配置文件上传到 Citrix Application Delivery Management (Citrix ADM)
- 使用更新的备份文件还原 HAProxy 实例。

要使用 **Citrix ADM** 编辑 **HAProxy** 配置文件，请执行以下操作：

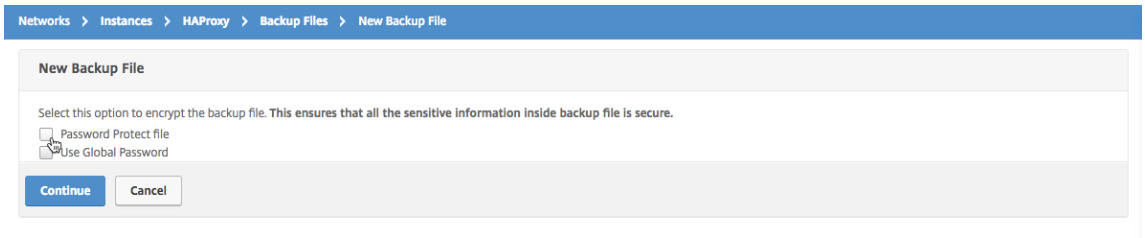
1. 在 Citrix ADM 中，导航到 “ 网络” > “ 实例” > “ **HAProxy**”。
2. 在 **HAProxy** 页面上，单击实 例选项卡。
3. 选择要备份的 HAProxy 实例，然后单击 查看备份。



4. 在 **Backup Files**（备份文件）页面上，单击 **Back Up**（备份）。

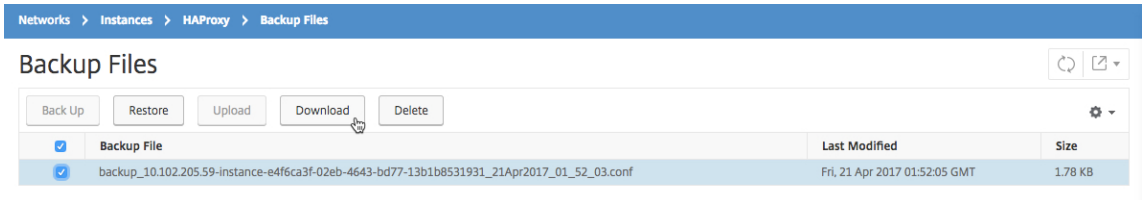


5. 单击继续。

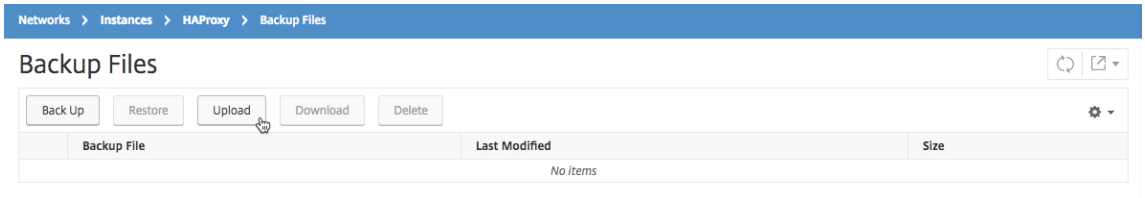


> 注意
>
> 请勿加密备份文件。

6. 在“ 备份文件” 页面上，选择备份文件，然后单击“ 下载”。



7. 使用文本编辑器，编辑 HAProxy 配置文件。
8. 在“ 备份文件” 页面上，单击“ 上传” 浏览并选择更新后的 HAProxy 配置文件。



上传更新的 HAProxy 配置文件后，它将列在“ 备份文件” 页面上。

9. 选择更新后的 HAProxy 配置文件，然后单击 恢复。

管理系统设置

April 23, 2021

下表介绍了 “ 系统” > “ 管理” 下的可用选项列表：

网络配置

网络配置	选项	说明
IP 地址、第二个 NIC、主机名和代理服务器	IP 地址	显示用于部署 Citrix ADM 的 Citrix ADM 网络配置 IP 地址详细信息
	第二个网卡	使您可以配置第二个网卡以隔离 Citrix ADM 管理访问。有关详细信息，请参阅配置双网卡以访问 Citrix ADM。
	主机名	使您能够为 Citrix ADM 分配主机名。有关详细信息，请参阅为 Citrix ADM 服务器分配主机名。
	代理服务器	使您可以将 ADM 配置为代理服务器。有关详细信息，请参阅作为 API 代理服务器的 Citrix ADM。
静态路由		使您可以配置静态路由，以在 Citrix ADM 和 Citrix ADC VPX 实例之间建立连接
NTP 服务器		确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。有关详细信息，请参阅配置 NTP 服务器。
ADM 端口信息		使您能够了解必须打开哪个端口才能在 ADM 和 ADC 或 SD-WAN 实例之间进行通信。有关详细信息，请参阅支持的端口。

系统配置

系统配置	选项	说明
系统、时区、允许的 URL 和当日消息	基本设置	使您能够修改系统设置，例如启用 `nsrecover` 登录、启用会话超时等
	时区	使您可以修改要在 Citrix ADM 中使用的时区。默认时区为 UTC
	允许的 URL 列表	使您可以配置 URL 以将不间断的请求发送到 ADM。如果没有要添加的 URL，您可以使用值 “none” 对其进行配置
	当天的消息	使您能够在 Citrix ADM 中创建欢迎消息。您可以使用此功能为自己或登录到 Citrix ADM 的用户设置提醒消息。单击 启用消息，在消息框中键入消息，然后单击 保存
查看 ADM 指纹		使您能够复制唯一的 Citrix ADM 指纹 ID 以开始使用服务图形
配置客户身份		使您能够通过仅允许经过身份验证的客户或用户访问网络来保护网络资源。有关详细信息，请参阅数据治理。
CUXIP 设置		如果选中此复选框，则收集使用情况统计信息的唯一目的是改进 GUI。收到的数据仅供 Citrix 工程师使用，不与任何人共享

系统维护

系统维护	说明
升级 Citrix ADM	使您能够通过 GUI 升级 Citrix ADM。有关详细信息，请参阅升级。
重新启动 Citrix ADM	使您能够重新启动 Citrix ADM
关闭 Citrix ADM	使您能够关闭 Citrix ADM

系统维护	说明
灾难恢复	使您能够查看灾难恢复节点信息。有关详细信息，请参阅配置灾难恢复。

数据修剪

数据修剪	选项	说明
系统和实例数据修剪	系统	使您可以限制存储在 Citrix ADM 服务器数据库中的报告数据量。有关详细信息，请参阅配置系统修剪设置。
	实例事件	允许您限制报告存储在 Citrix ADM 中的数据的事件消息
	实例系统日志	使您可以限制存储在数据库中的 syslog 数据量。有关详细信息，请参阅配置实例系统日志修剪设置。
	网络报告	允许您限制存储在 Citrix ADM 中的网络报告数据

备份

备份	选项	说明
配置系统和实例备份	系统	使您能够在执行系统备份之前配置初始备份设置。有关详细信息，请参阅系统备份设置。
	实例	使您可以在 Citrix ADM 上配置设置，以备份选定的 Citrix ADC 实例或多个实例。有关详细信息，请参阅配置实例备份设置。

事件通知

事件通知	选项	说明
配置事件通知和摘要	事件通知	您可以为多个系统相关功能选择用户组发送通知。这些系统功能按事件类别（例如 SystemReboot、StatusPoll、SystemState 等）划分。您可以将 Citrix Application Delivery Management (ADM) 配置为通过电子邮件、SMS 或 Slack 向您发送通知。这可以确保您收到任何系统级活动的通知，例如超过数据存储或备份失败。
	事件摘要	使您能够获得重要系统和功能事件的综合报告

SSL 设置

SSL 设置	说明
安装 SSL 证书	使您能够安装 SSL 证书和 SSL 密钥文件
查看 SSL 证书	使您能够查看 SSL 证书详细信息
配置 SSL 设置	有关详细信息，请参阅配置 SSL 设置。
SSL Certificates（SSL 证书）	使您能够上传、下载或删除 SSL 证书或 SSL 密钥文件
密码组	有关详细信息，请参阅配置密码组。

配置功能

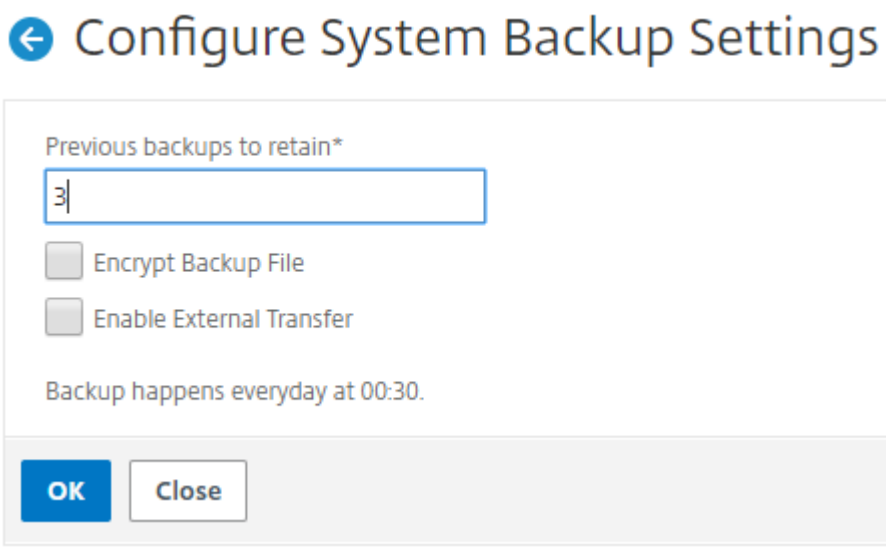
配置功能	说明
禁用或启用功能	您可以在 Citrix ADM 中启用或禁用功能。有关详细信息，请参阅启用或禁用 ADM 功能。

配置系统备份设置

April 23, 2021

在需要备份和还原 Citrix 应用程序交付管理 (ADM) 系统之前，请先设置初始系统备份设置。

1. 导航到“系统”>“系统管理”。在“备份设置”下，单击“系统备份设置”。
2. 在“ 混淆系统备份设置”页上，指定以下内容：
   - 要保留的备份数。您最多只能保留 10 个备份。
   - 加密备份文件。
   - 启用外部传输。可以将备份文件副本传输到另一个系统上作为预防措施。要还原配置时，必须首先将文件上载到 Citrix ADM 服务器，然后执行还原操作。指定服务器、用户名和密码、端口、要使用的传输协议以及目录路径。要了解有关外部传输的更多信息，请参阅将 Citrix ADM 备份文件传输到外部系统。
3. 单击确定。



配置 NTP 服务器

April 23, 2021

您可以在 Citrix Application Delivery Management (ADM) 中配置网络时间协议 (NTP) 服务器，以便将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

要在 **Citrix ADM** 上配置 **NTP** 服务器，请执行以下操作：

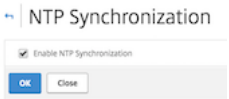
1. 导航到 **System**（系统）> **NTP Servers**（NTP 服务器），然后单击 **Add**（添加）。
2. 在 **Create NTP Server**（创建 NTP 服务器）页面上，输入以下详细信息：
   - **Server Name/IP Address**（服务器名称/IP 地址）– 输入 NTP 服务器的域名或 IP 地址。添加了 NTP 服务器后无法更改名称或 IP 地址。

- **Minimum Poll Interval**（最小轮询时间间隔）– 指定传输的 NTP 消息之间的最小时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最小轮询间隔为 64 秒（可以表示为 2^6），请输入 6。
- **Maximum Poll Interval**（最大轮询时间间隔）– 指定传输的 NTP 消息之间的最大时间间隔值，以秒为单位且是 2 的幂。例如，如果希望最大轮询时间间隔是 256 秒（可以表示为 2^8），则输入 8。
- **Key Identifier**（密钥标识符）- 输入可以用于 NTP 服务器进行对称密钥身份验证的密钥标识符。如果选择 “Autokey”（自动密钥），请勿添加密钥标识符。
- **Autokey**（自动密钥）- 如果希望 NTP 服务器使用公钥身份验证，请选择 **Autokey**（自动密钥）。如果要添加密钥标识符，请勿选择。
- **Preferred**（首选）– 如果希望将此 NTP 服务器指定为进行时钟同步的首选服务器，请选择此选项。这仅在配置多个服务器时适用。

3. 单击创建。

要在 **Citrix ADM** 上启用 **NTP** 同步，请执行以下操作：

1. 导航到 **System**（系统）**> NTP Servers**（NTP 服务器）。
2. 单击 **NTP** 同步，然后选中 启用 **NTP** 同步复选框。
3. 单击确定。



> 注意：
>
> 您可以在文件 /var/log/ntpd.log 文件的 /var/log 目录中找到 NTP 日志消息。

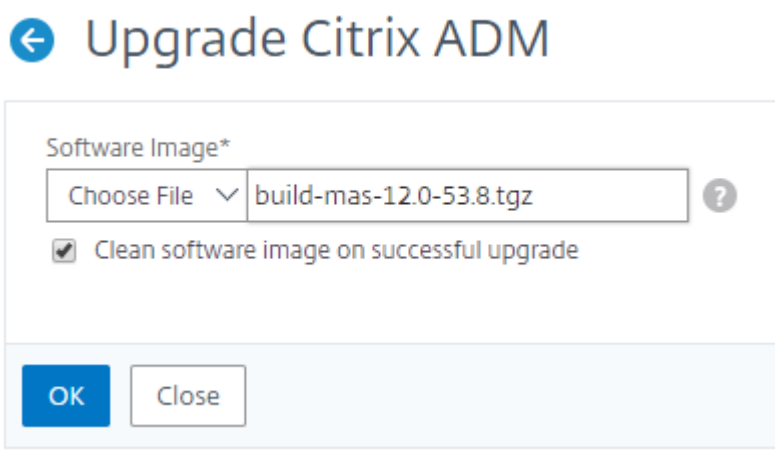
升级 Citrix ADM

April 23, 2021

每个 Citrix Application Delivery Management (ADM) 版本都提供了新的和更新的功能以及更多的功能。增强功能的完整列表在版本发布时附带的发行说明中提供。升级软件前，请花一些时间阅读发行说明。在开始升级软件前了解许可框架及许可证类型，这很重要。

要升级 **Citrix ADM**，请执行以下操作：

1. 导航到 **System**（系统）> **System Administrations**（系统管理）。在 系统管理子标题下，单击 升级 **Citrix ADM**。
2. 在升级 Citrix ADM 页面上，通过选择本 地（您的本地计算机）或 装置（证书文件必须存在于 Citrix ADM 虚拟设备上）来上传新映像文件。
   默认情况下，软件映像在成功升级后被清理。
3. 单击确定。



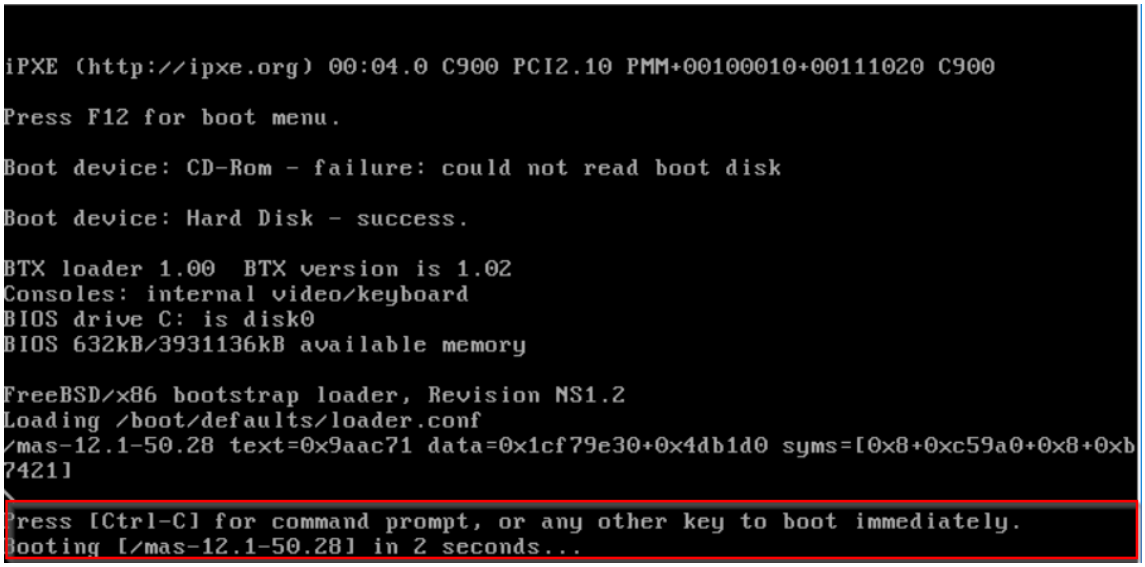
如何重置 **Citrix ADM** 的密码

April 23, 2021

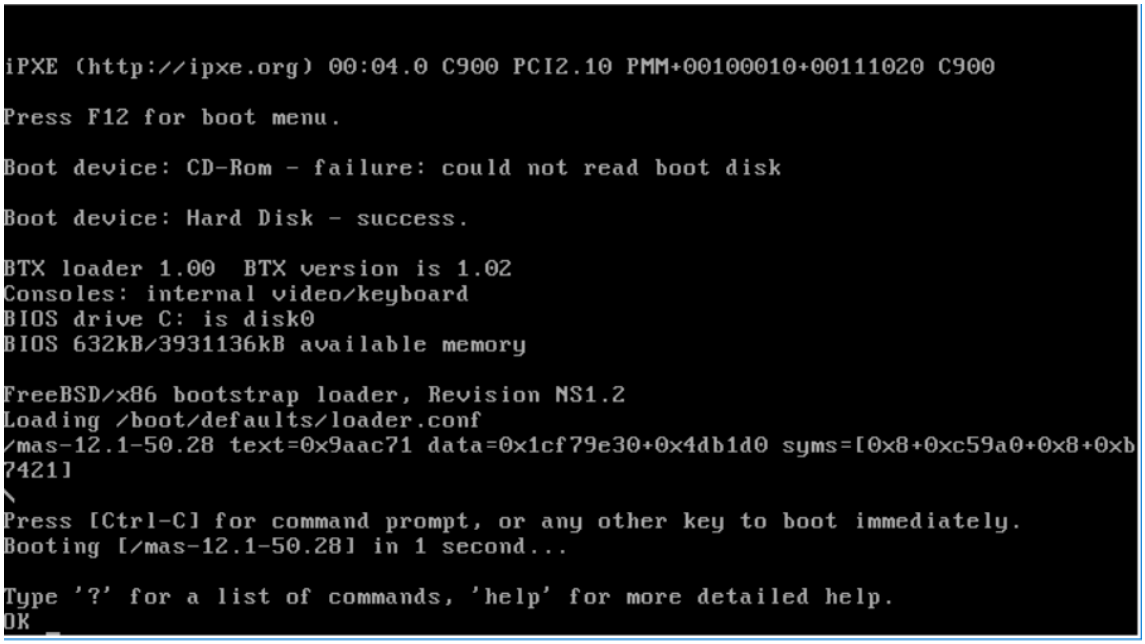
重置 Citrix ADM 密码的过程可能会因托管它的虚拟机管理程序而异。如果您已更改默认密码并希望重置为默认密码，则可以通过重新启动 Citrix ADM 节点来重置密码。

使用 **XenCenter** 的思杰虚拟机管理程序：

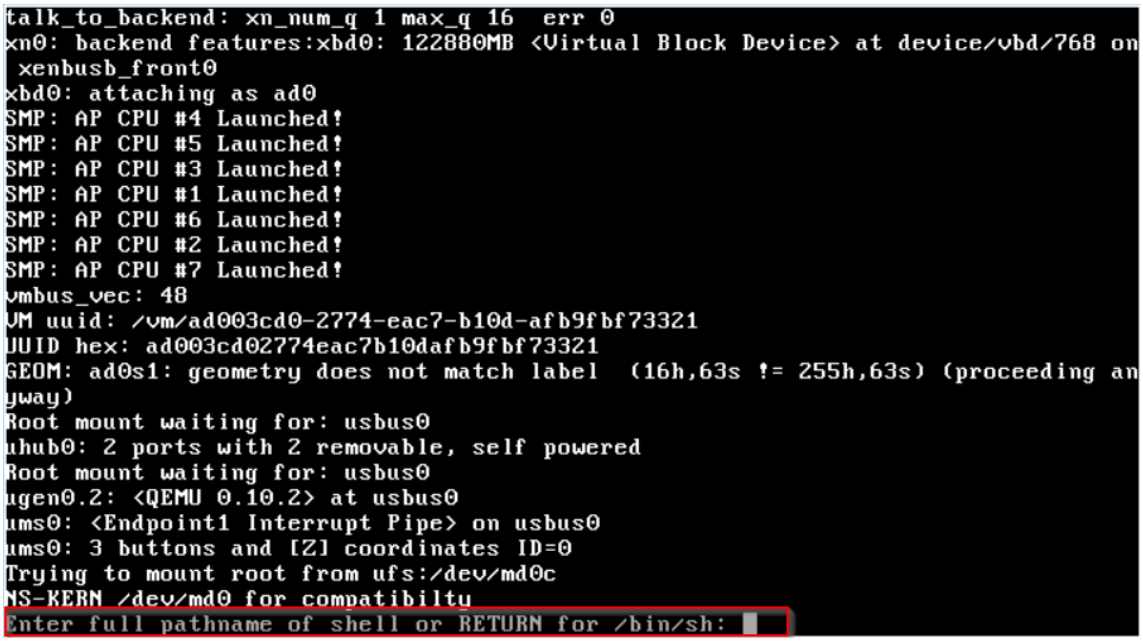
1. 使用 XenCenter 登录到 Citrix Hypervisor。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台选项卡上，按 **CTL + C** 以中断引导顺序。



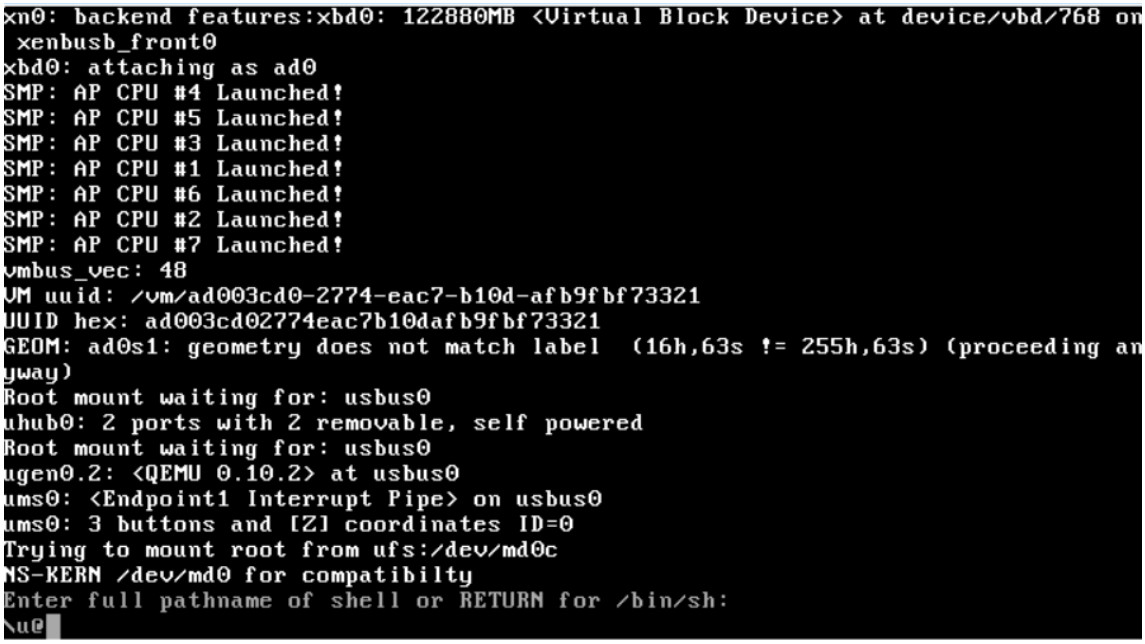
4. 在确定提示符下运行 **boot-s** 命令。



Citrix ADM 重新启动并显示以下消息：

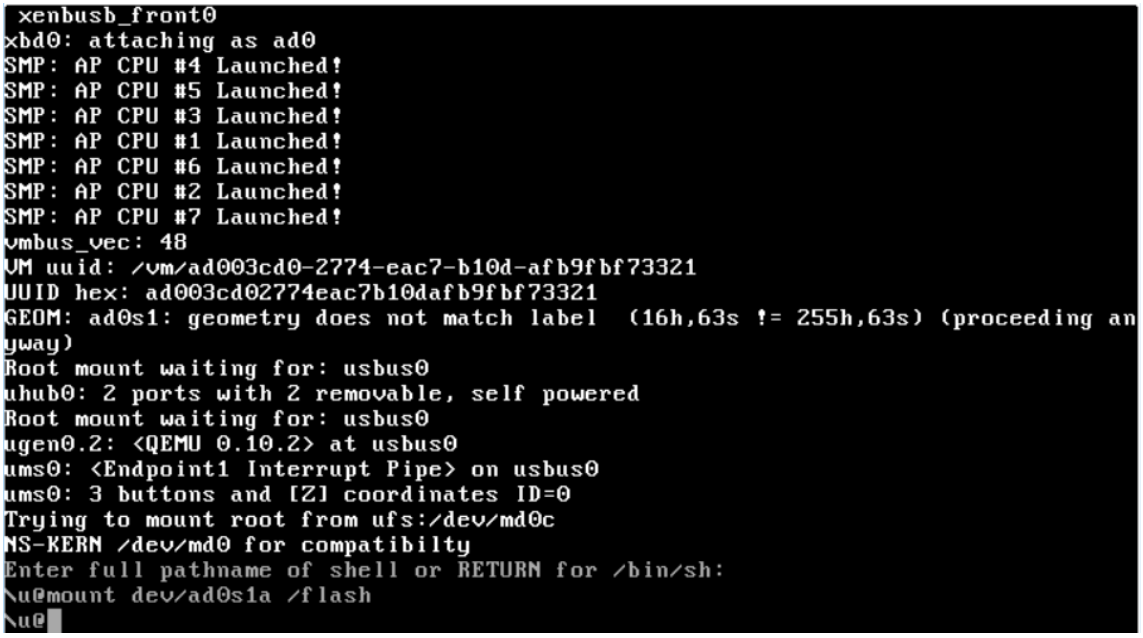


5. 按 **Enter** 键以获得 /u @ 提示。



6. 使用以下命令装载闪存分区：

```
mount dev/ad0s1a /flash
```

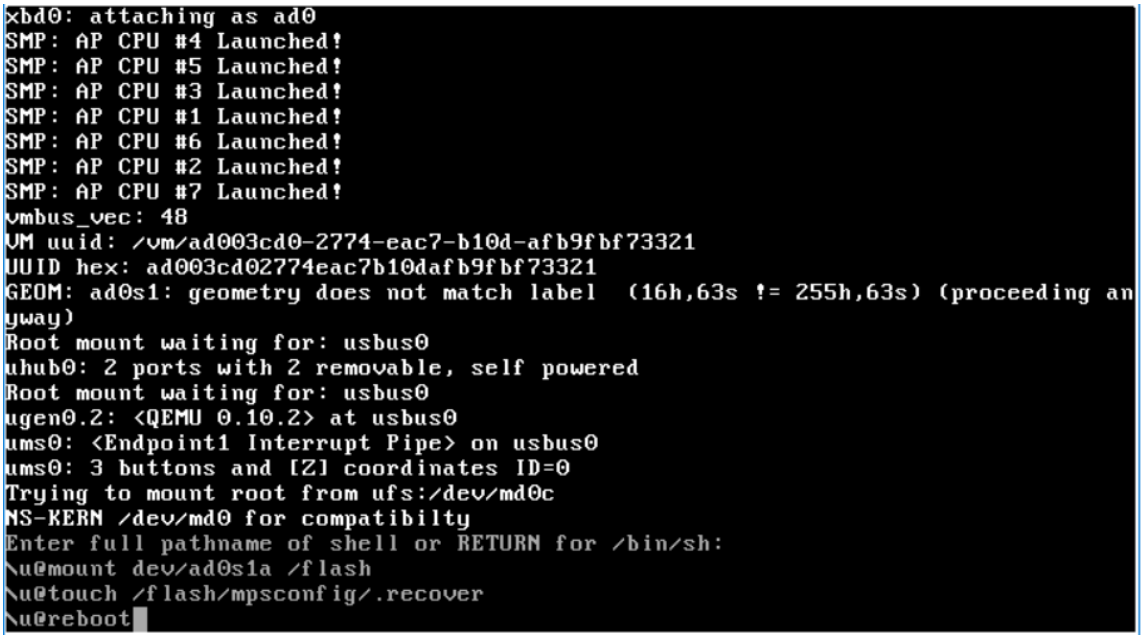



7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：

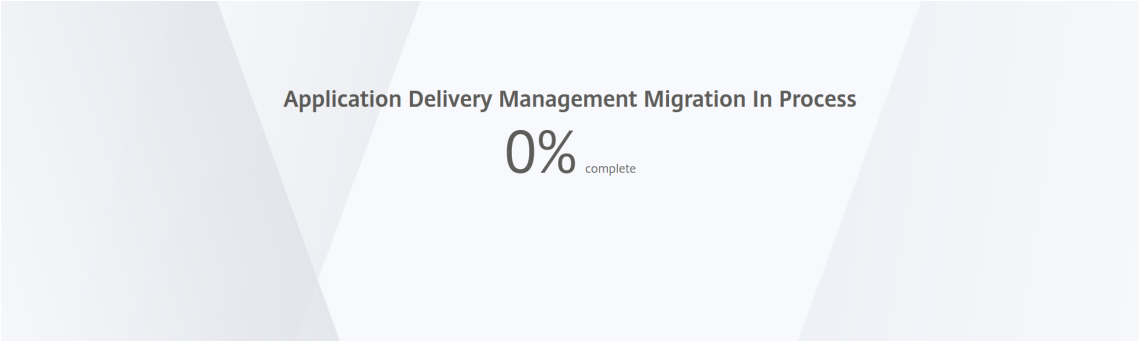
   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

10. 运行 重新启动命令以重新启动 Citrix ADM。



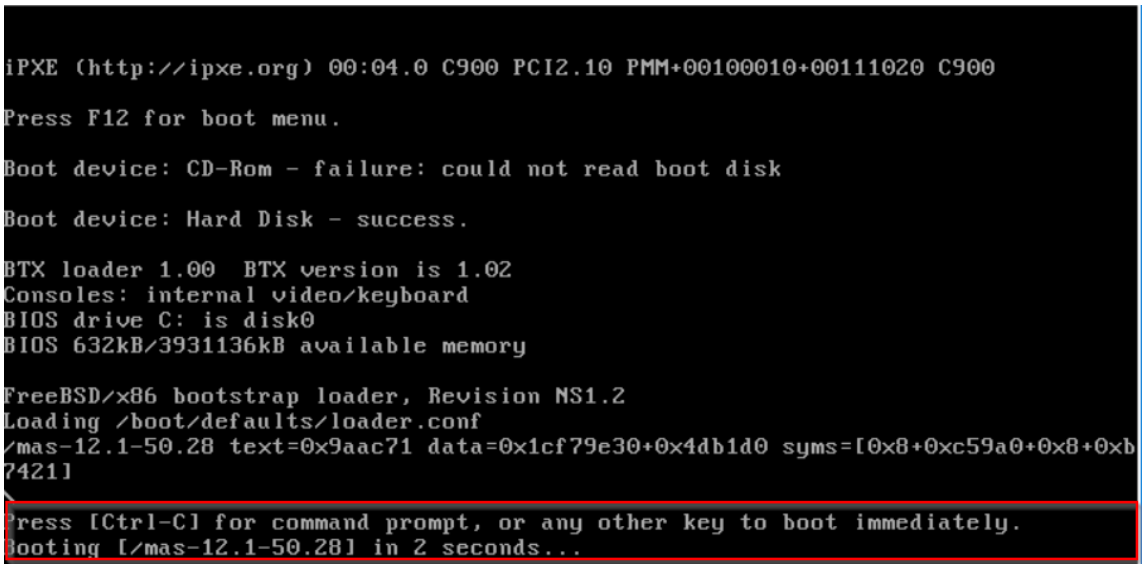
11. 访问 Citrix ADM GUI 并等待重新启动完成。



现在，您可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsroot/nsroot* 从 Hypervisor 登录。

使用 **vSphere** 的 **ESX**：

1. 使用 vSphere 登录到 ESX。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台选项卡上，按 **CTL + C** 以中断引导顺序。



4. 在确定提示符下运行 **boot-s** 命令。

   Citrix ADM 将重新启动。

5. 按 **Enter** 键以获得 /u @ 提示。
6. 使用以下命令装载闪存分区：

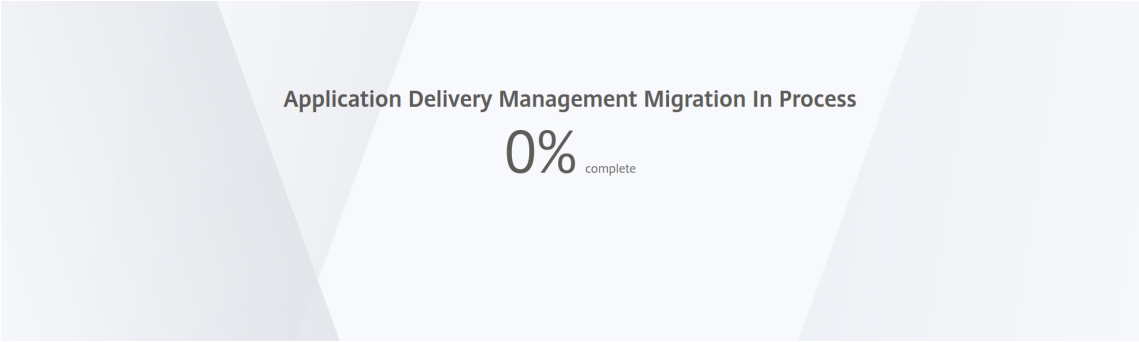
   ```
   mount dev/da0s1a /flash
   ```

7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：


```
touch /flash/mpsconfig/.recover
```

密码现在重置为默认密码。

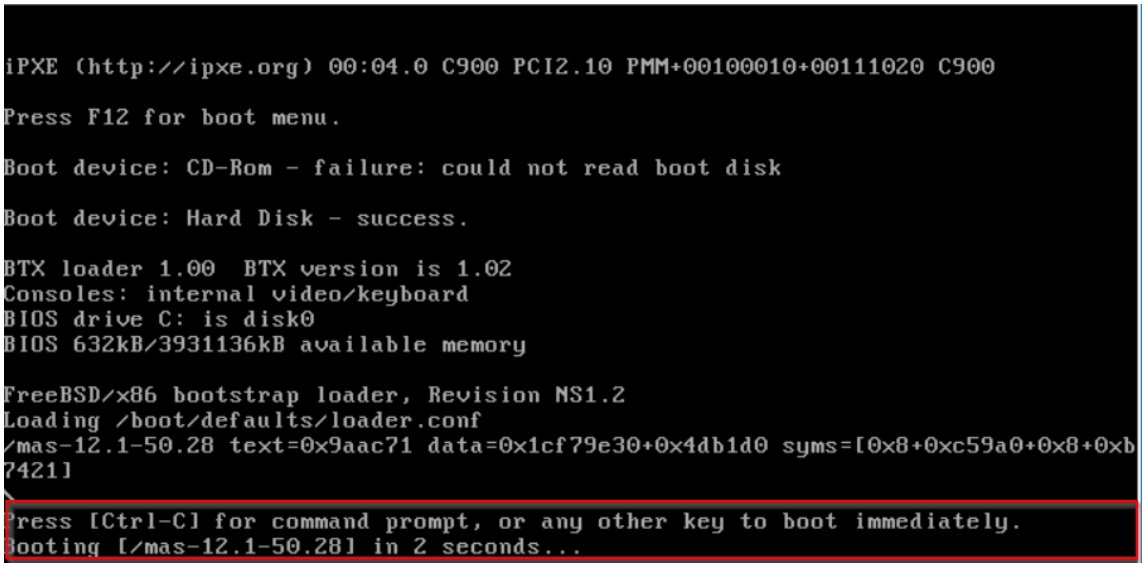
10. 运行 重新启动命令以重新启动 Citrix ADM。
11. 访问 Citrix ADM GUI 并等待重新启动完成。



您现在可以使用 nsroot/nsroot 凭据从图形用户界面登录，从 *ESX* 服务器登录。

使用 **Hyper-V** 管理器的 **Hyper-V**：

1. 使用 Hyper-v 管理器登录到 Hyper-v。
2. 选择 Citrix ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台选项卡上，按 **CTL + C** 以中断引导顺序。



4. 在确定提示符下运行 **boot-s** 命令。

   Citrix ADM 将重新启动。

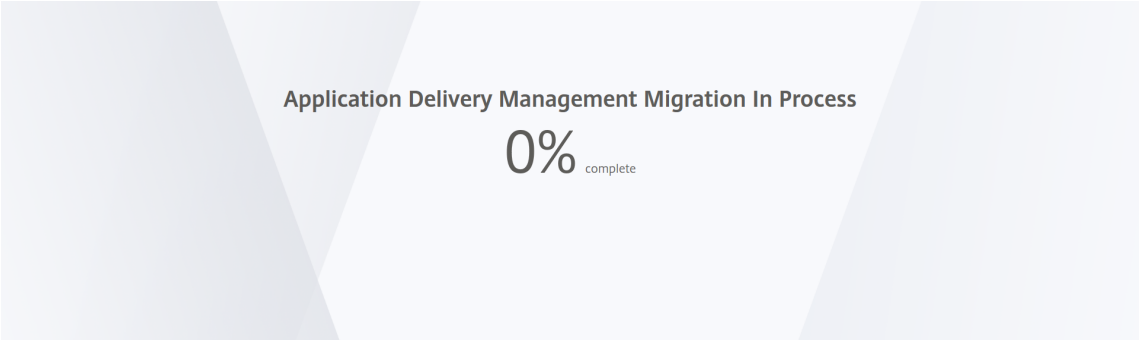
5. 按 **Enter** 键以获得 /u @ 提示。
6. 使用以下命令装载闪存分区：

```
mount dev/ad0s1a /flash
```


7. `Delete /flash/mpsconfig/master.passwd`
8. `Delete rm -rf /etc/passwd`
9. 使用以下命令创建文件：

   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。
10. 运行 重新启动命令以重新启动 Citrix ADM。
11. 访问 Citrix ADM GUI 并等待重新启动完成。



您现在可以使用 *nsroot/nsroot* 凭据从图形用户界面登录，并使用 *nsroot/nsroot* 从超级 v 管理器登录。

Linux KVM 服务器（**SSH** 到 **KVM** 服务器通过使用任何 **SSH** 客户端）：

1. 使用 SSH 客户端登录到 KVM 服务器的 Citrix ADM。
2. 重新启动 Citrix ADM。
3. 在显示加载/启动/ 默认**/**装载器**.conf** 消息后不久，按 **CTL + C** 中断启动序列。
4. 在 OK 提示符下，运行以下命令：

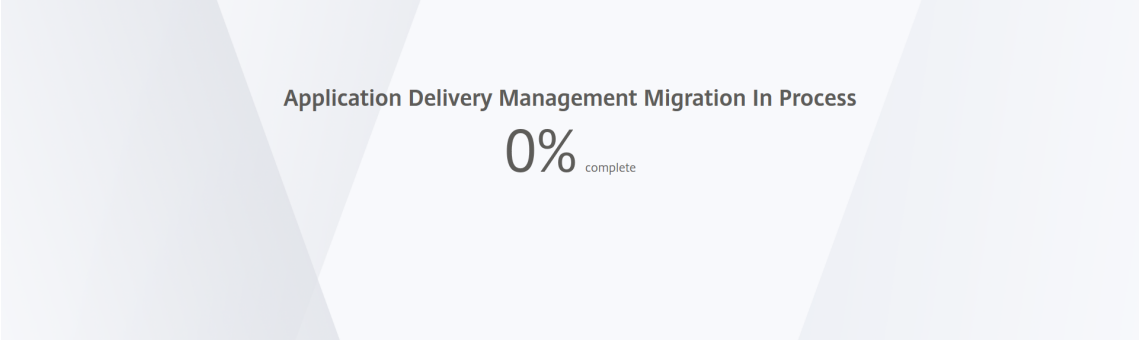
   ```
   set console='comconsole,vidconsole'
   ```
5. 运行 引导**-s** 命令以重新启动 Citrix ADM。
6. 在显示 输入 **shell** 的完整路径或返回 **/bin/sh:** 消息后，按 **Enter** 键以获得 /u @ 提示。
7. 使用以下命令装载闪存分区：

   ```
   mount dev/vtbd0s1a /flash
   ```
8. `Delete /flash/mpsconfig/master.passwd`
9. `Delete rm -rf /etc/passwd`
10. 使用以下命令创建文件：

    ```
    touch /flash/mpsconfig/.recover
    ```

    密码现在重置为默认密码。

11. 运行 重新启动命令以重新启动 Citrix ADM。
12. 访问 Citrix ADM GUI 并等待重新启动完成。



您现在可以使用 nsroot/nsroot 凭据从图形用户界面登录，并从 *SSH* 控制台登录。

配置双网卡以访问 **Citrix ADM**

April 23, 2021

您可以配置第二个网卡来隔离对 Citrix ADM 的管理访问。使用第二个 NIC 功能，您可以根据您的要求选择如何隔离通过 Citrix ADM 接收和发送的流量。

考虑一种情况下，您希望将流量隔离到：

- 将 Citrix ADM 与其托管 Citrix ADC 实例之间的所有通信集中在一个网络中。
- 在另一个网络中拥有对 Citrix ADM 的管理访问权限。

在这种情况下，作为管理员，您可以执行以下操作：

- 为 Citrix ADM 与其托管 Citrix ADC 实例之间的流量配置一个 IP 地址。
- 为管理 Citrix ADM 软件配置另一个 IP 地址，以执行软件中的所有管理任务。

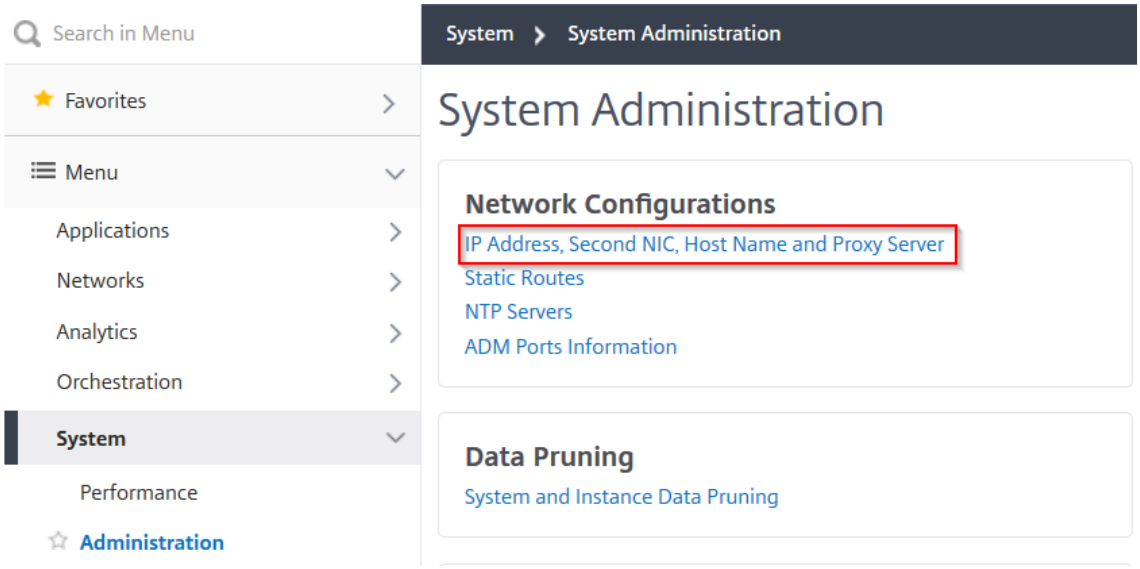
> 注意
>
> 如果将 Citrix ADM 配置为 HA 对，则在第二个 NIC 上配置的管理 IP 地址将与主节点相关联。

必备条件

- 确保已在 Hypervisor（**Citrix Hypervisor**、微软 **Hyper-V**、**Linux KVM** 或 **VMware ESXi**）上部署并配置了 **Citrix ADM 13.0** 版本 **47.x** 版本或更高版本。
- 确保已在 Hypervisor（Citrix Hypervisor、微软 Hyper-V、Linux KVM 或 VMware ESXi）上添加了第二个网卡。

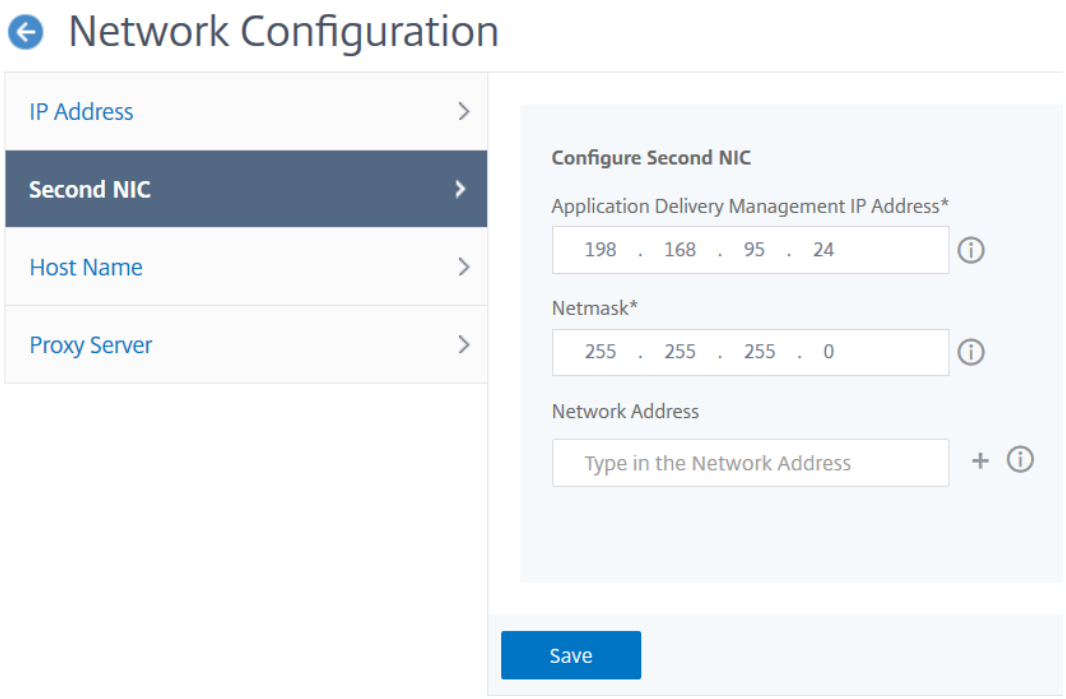
在 **Citrix ADM** 中配置第二个网卡

1. 登录到 ADM 图形用户界面。
2. 导航到 系统 > 管理。
3. 在 “ 网络配置” 下，单击 “ **IP** 地址”、“第二个 **NIC**”、“主机名” 和 “代理服务器”。



此时将显示 “ 网络配置” 页。

4. 单击第二个 NIC 选项卡并配置以下参数：
   a) 应用程序交付管理 **IP** 地址 — 输入有效的 IP 地址以访问 Citrix ADM。除了现有的管理 IP 地址之外，您可以使用此 IP 地址访问 Citrix ADM。
   b) 网络掩码 — 输入网络掩码地址以指定网络主机。默认地址为 255.255.0。
   c) 网络地址 — 输入 IP 地址以添加 Citrix ADM 的路由条目。单击 **+** 添加更多 IP 地址。此字段是可选的。
   d) 单击保存。



配置系统日志清除间隔

April 23, 2021

Syslog 是日志记录标准协议。它有两个组件：Syslog 审核模块（在 Citrix 应用程序 Delivery Controller (ADC) 实例上运行）和 Syslog 服务器，可以在 Citrix ADC 实例的底层 FreeBSD 操作系统 (OS) 上运行，也可以在远程系统上运行。SYSLOG 使用用户数据报协议 (UDP) 进行数据传输。

通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

要限制存储在数据库中的 syslog 数据量，可以指定要修剪 syslog 数据的时间间隔。您可以指定从 Citrix Application Delivery Management (ADM) 中删除以下 syslog 数据的天数：

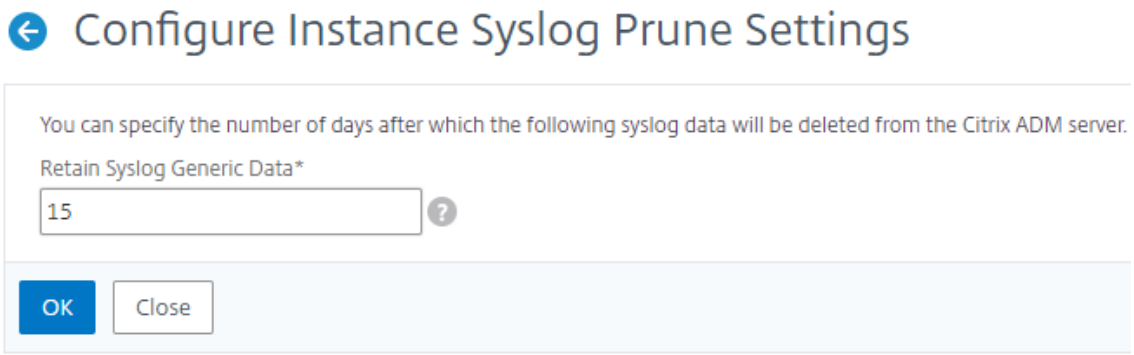
- 一般 Syslog 数据
- AppFirewall 数据
- Citrix Gateway 数据

您还可以按系统日志类型配置 Citrix Gateway 修剪间隔。此修剪间隔优先于为保留 Citrix Gateway 数据而配置的符文间隔。

要为 **Citrix ADM** 配置系统日志修剪间隔设置，请执行以下操作：

1. 导航到 **“系统” > “管理”**。在 “ 数据修剪” 下，单击 “ 系统和实例数据修剪”，然后单击 “ 实例系统日志”。

2. 在“ 配置实例系统日志修剪设置” 页中，指定 保留系统日志通用数据 **(**天**)**。键入 Citrix ADM 保留通用系统日志消息的天数。



配置系统修剪和事件修剪设置

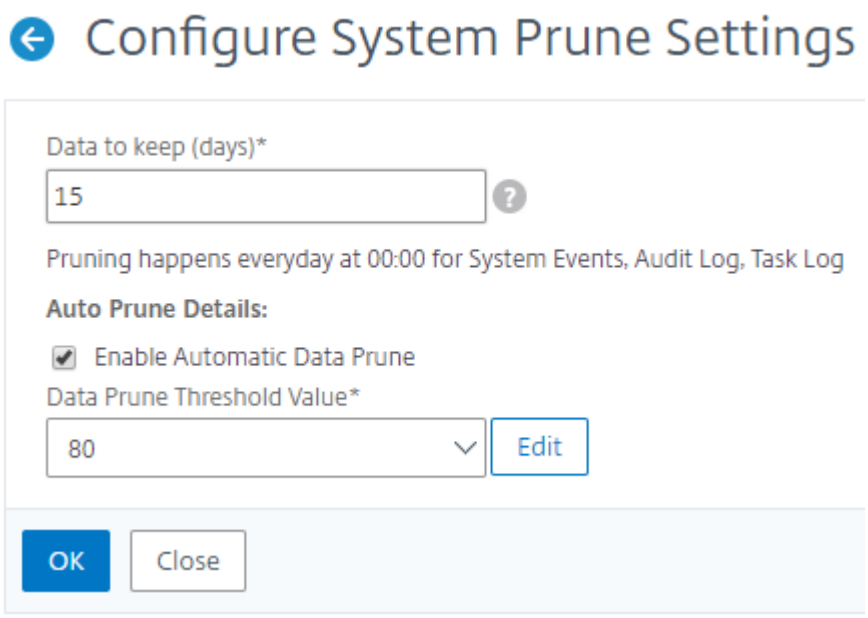
April 23, 2021

要限制存储在 Citrix Application Delivery Management (ADM) 软件数据库中的报告数据量，可以对其进行修剪。您可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

> 注意
>
> 您指定的值不能超过 30 天或少于 15 天。

要使用 **Citrix ADM** 为性能报告配置系统修剪设置，请执行以下操作：

1. 导航到 “系统” > “管理”。在 “数据修剪” 下，单击 “系统和实例数据修剪”。
2. 在 “配置系统修剪设置” 页中，指定保留数据的天数，然后单击 “确定”。

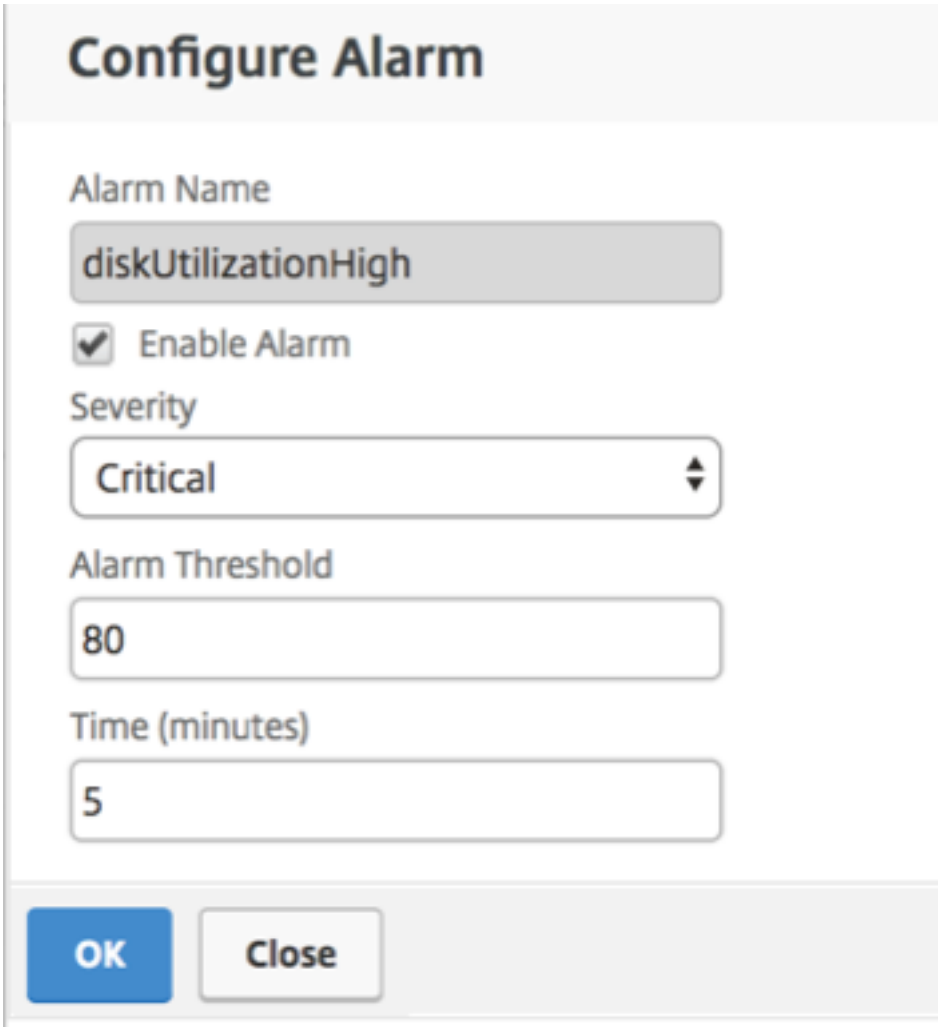


您可以通过选中“启用自动修剪数据”复选框来启用自动修剪。当磁盘使用率违反配置的 数据修剪阈值时，将触发警报并发送电子邮件。要更改磁盘空间的百分比（修剪阈值），请单击 编辑。

> 注意：在满足任何一个条件时开始修
> 剪 — 数据修剪阈值或要保留的数据 (天)。无论第一个满足，优先于另一个。

您可以配置和启用磁盘高警报（默认情况下）并指定以下内容：

- 严重性，例如，严重。
- 警报阈值。键入计算事件严重性的值。
- 时间。要触发警报的时间长度（以分钟为单位）。



使用 **Citrix ADM** 配置事件修剪设置

要限制存储在 Citrix ADM 数据库中的事件消息数据量，可以指定希望 Citrix ADM 保留网络报告数据、事件、审核日志和任务日志的时间间隔。默认情况下，此数据每 24 小时删除一次（在 00:00 点）。

- 导航到 系统 **>** 管理 **>** 数据修剪，然后单击 系统和实例数据修剪。单击 实例事件。
- 输入要在 Citrix ADM 服务器上保留数据的时间间隔（以天为单位），然后单击 “保 存”。

为非默认用户启用 **shell** 访问

April 23, 2021

您可以在 Citrix Application Delivery Management (ADM) 中为非默认用户启用 shell 访问。可以使用此功能启用和设置与实例的通信模式。

> 注意
>
> 默认情况下，对非默认用户禁用 shell 访问。

要在 **Citrix ADM** 中为非默认用户启用外壳访问，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 系统管理”。
2. 在 **System Settings**（系统设置）中，单击 **Change System Settings**（更改系统设置）。
3. 在 **Modify System Settings**（修改系统设置）页面上，配置以下参数：
   - **Communication with instances**（与实例通信）- 选择通信协议。
   - 安全访问 -启用 Citrix ADM 的安全访问。
   - **Enable Session Timeout**（启用会话超时）- 指定保留非活动会话的时间段。
   - **Allow Basic Authentication**（允许基本身份验证）- 允许管理服务接受使用基本身份验证协议提供的凭据。
   - 启用 **nsrecover** 登录 -在管理服务上启用 `nsrecover` 登录。
   - 启用证书下载 -使您能够从添加的 Citrix ADC 下载证书。
   - 为非 **nsroot** 用户启用命令行管理程序访问 — 为 Citrix ADM 中的非默认用户启用外壳访问。
   - 提示用户凭据进行实例登录 -允许用户在从 Citrix ADM 登录到实例时输入其用户凭据。
4. 单击确定。

恢复无法访问的 **Citrix ADM** 服务器

April 23, 2021

Citrix Application Delivery Management (ADM) 现在提供了一个用于执行系统数据库清理的数据库维护工具。现在，您可以启动 Citrix ADM 实用程序工具以连接到文件系统、删除一些组件并使数据库可访问。Citrix ADM 恢复脚本是一种工具，可通过清除旧的或未使用的数据库表和文件来帮助恢复文件系统中的空间。该工具可帮助您在连续步骤中浏览数据库表和文件，并显示文件系统上由相应项目占用的当前空间。选择要删除的数据库表和文件后，工具将在确认后从文件系统中删除这些表和文件。

如何将 **Citrix ADM** 数据库恢复脚本用于 **Citrix ADM** 独立部署

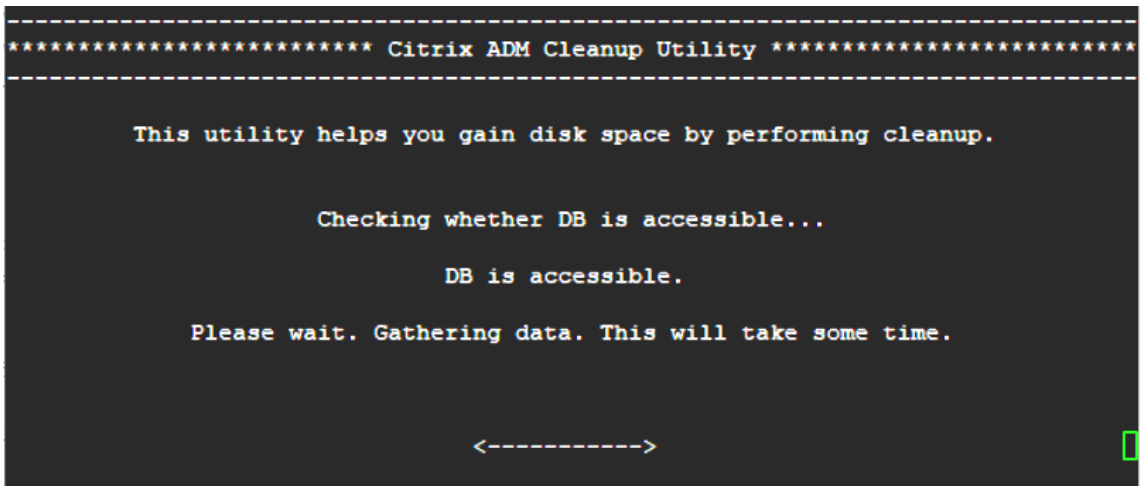
在单个服务器 Citrix ADM 部署中使用以下过程连接到文件系统、删除一些组件并使数据库可访问，然后执行恢复操作。

1. 使用 SSH 客户端或虚拟机管理程序的控制台登录到 Citrix ADM 并键入以下命令：

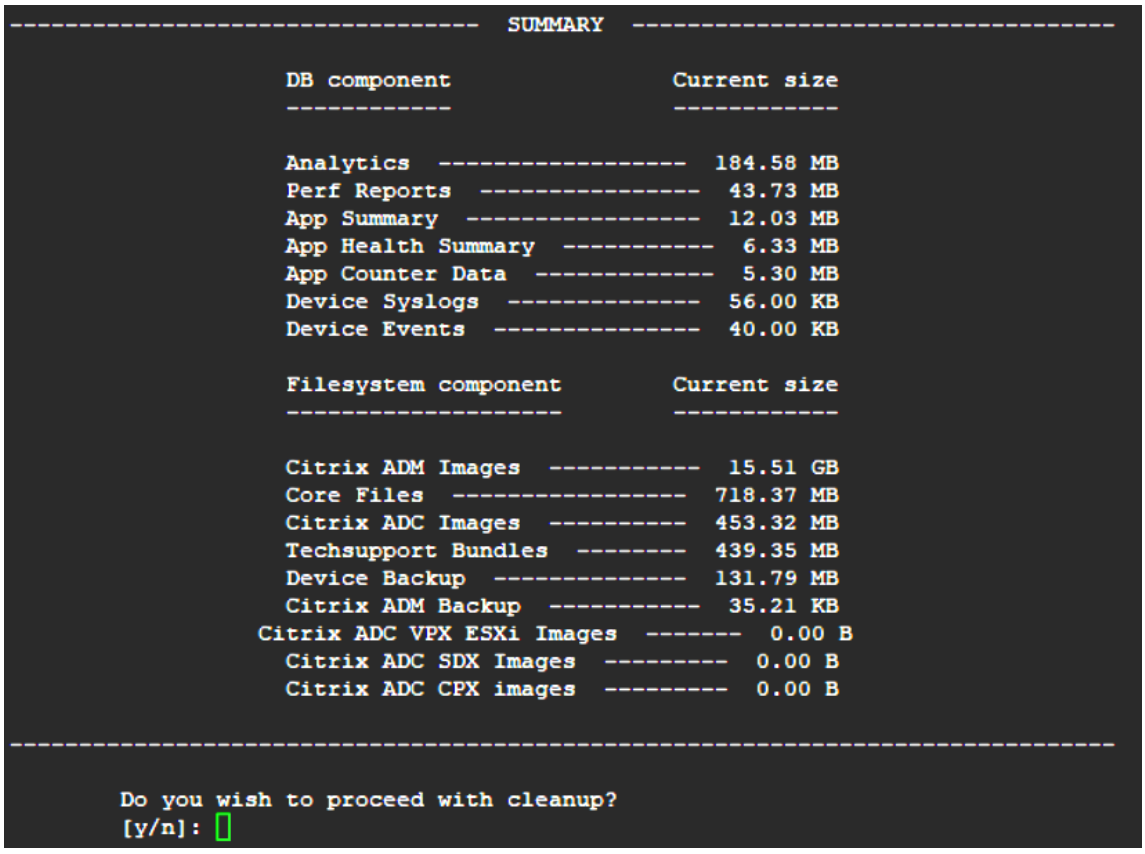
```
Last login: Fri Nov 30 09:51:19 2018 from 10.252.241.100
Have a nice daybash-3.2# /mps/mas_recovery/mas_recovery.py
```

2. 当屏幕显示停止一些 Citrix ADM 进程的警告消息时，键入 “y” 并按 **Enter** 键。

   当系统确定可以删除数据库的哪些组件而不影响系统的核心文件时，将出现以下屏幕。



3. 屏幕显示数据库中的文件列表。键入 “y”，然后按 Enter 键开始清理过程。

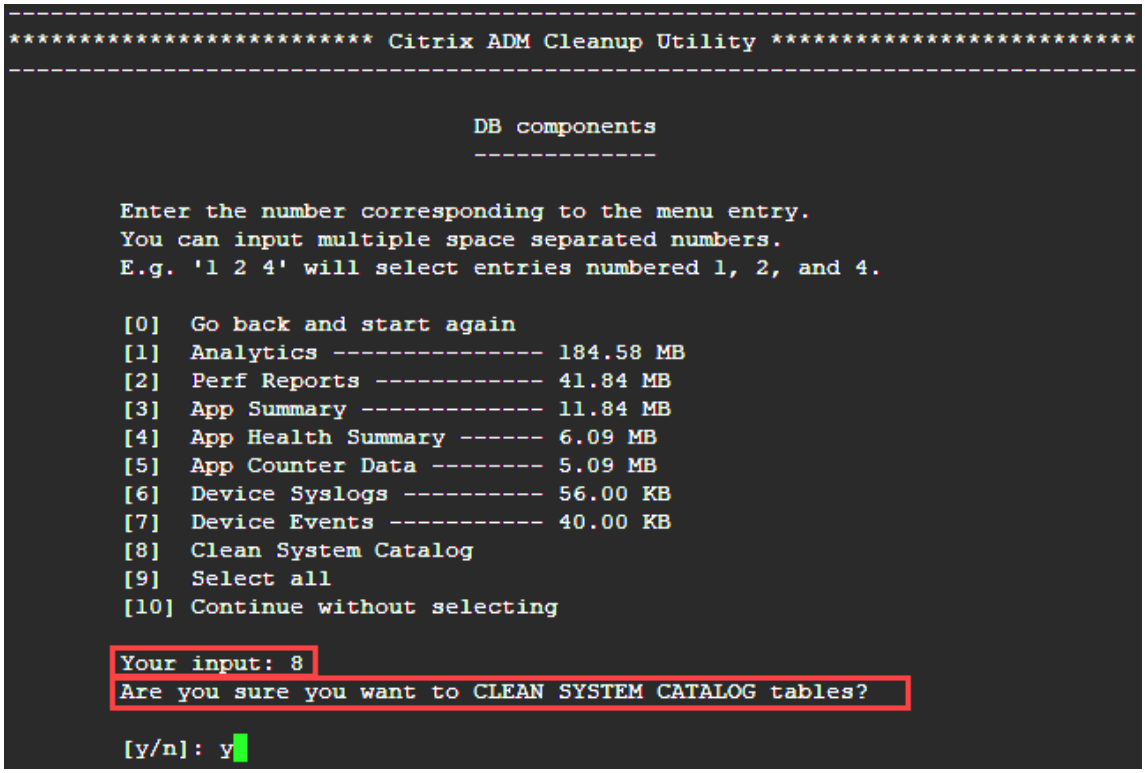


4. 您可以选择需要清理的特定数据库组件，然后键入相应的编号。按 En **ter** 键。

   例如，要执行系统目录清理，请在 数据库组件选择菜单中选择选项 8，然后键入 “y”，然后按 **Enter** 键继续清理系统目录。

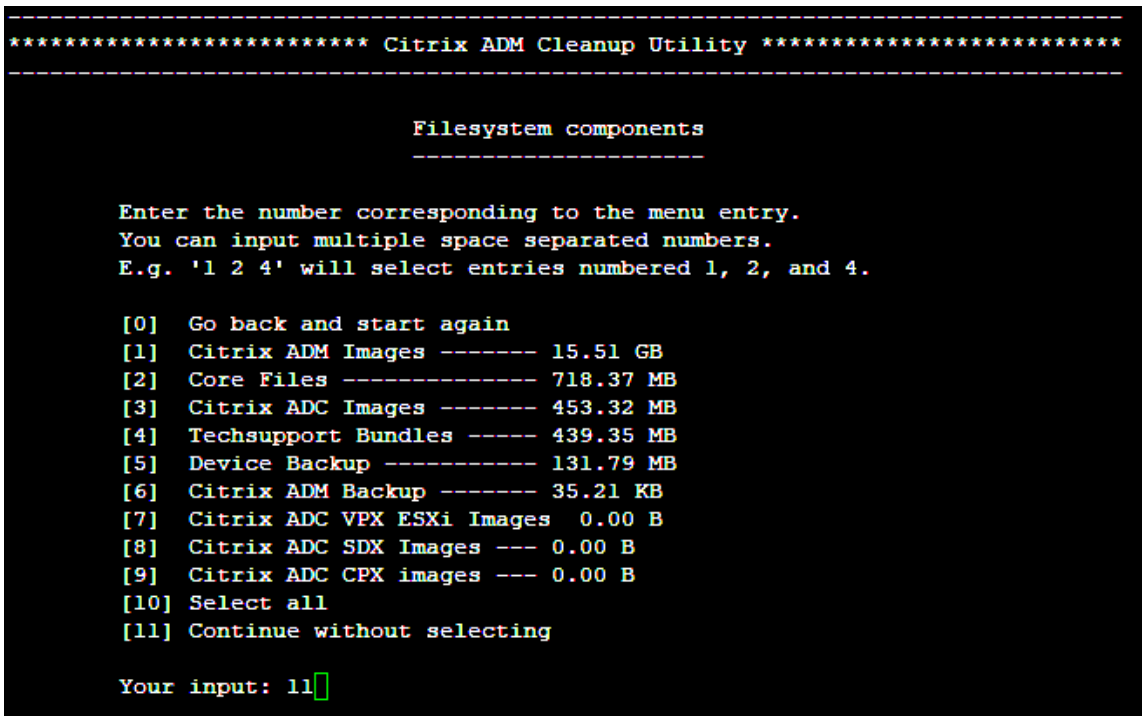
   > 注意：
   >
   > Citrix ADM 包括称为系统目录的用户表。系统目录是 Citrix ADM 数据库中的一个位置，关系数据库管理

> 系统在其中存储架构元数据，例如有关表和列以及内部记录的信息。系统目录中的表类似于常规表，它们可以随着时间的推移累积膨胀行和死行，因此需要定期清理以获得最佳性能。定期维护这些表格是一个良好的做法。该活动不仅释放了磁盘空间，而且还提高了数据库的整体性能，从而提高了 Citrix ADM 的性能。

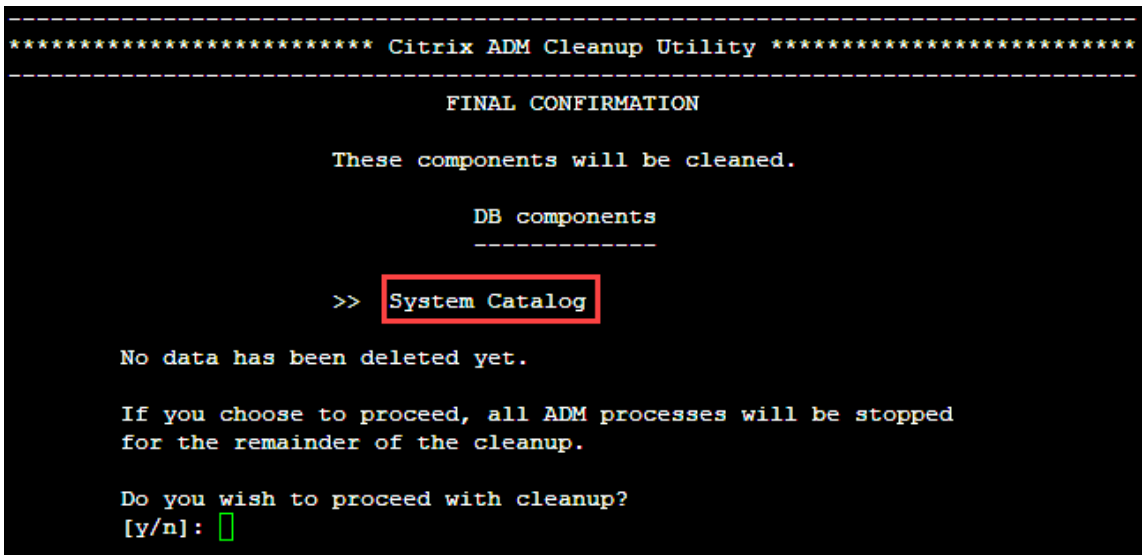


清理实用程序为您提供了清理数据库组件和文件组件的选项。您可以通过键入“1”和“9”之间的数字来选择任何文件组件，或键入“11”，然后按 Enter 键清除数据库组件。

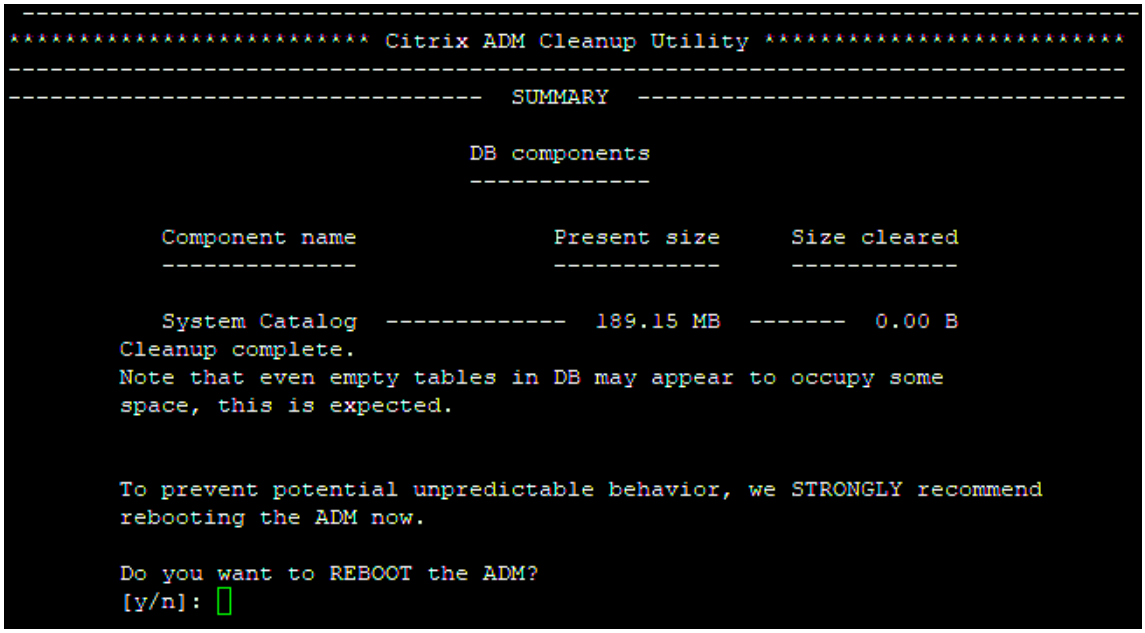
> ** 注
>
> 意 ** 数字“11”表示您尚未选择要清理的任何文件组件，并且正在继续清理之前选择的早期数据库组件。在此示例中，它是“系统目录。“



5. 键入 “y”，然后在最后确认屏幕中再次按 **Enter** 键。



系统目录将被清理，这可能需要一些时间，具体取决于系统目录中表的大小。该过程完成后，将显示摘要屏幕。



6. 键入 “y”，然后按 **Enter** 键以重新启动 Citrix ADM。

   确保在系统清理后重新启动 Citrix ADM。在 Citrix ADM 重新启动后，请等待大约 30 分钟以完成内部数据库操作。然后，您应该能够连接到 Citrix ADM 数据库。如果没有，请再次运行恢复脚本以释放更多空间。当 Citrix ADM 启动并运行时，它应按预期工作。

   > ** 注
   >
   > 意：** 清理后，系统目录表的当前大小永远不会等于零。这是因为只会从表中删除空行，并且表可能具有一些有效的条目，即使在清理后也是如此。

如何将 **Citrix ADM** 数据库恢复脚本用于 **Citrix ADM** 高可用性部署

高可用性部署中的 Citrix ADM 服务器的数据库系统处于连续同步模式。使用新的数据库恢复工具时，不需要在两个 Citrix ADM 服务器上复制该过程。

1. 使用 SSH 客户端或虚拟机管理程序的控制台登录到主节点。
2. 运行以下命令：

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. 按照步骤 2 中的步骤操作Citrix ADM 独立部署恢复脚本

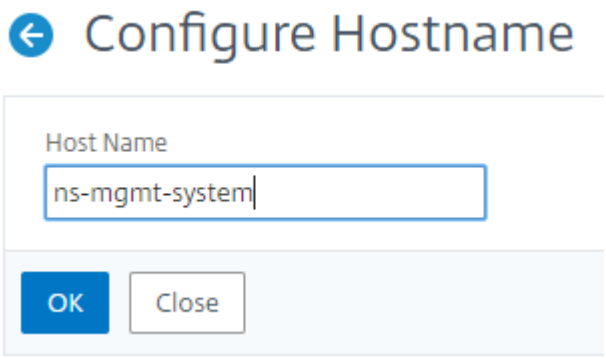
为 **Citrix ADM** 服务器分配主机名

April 23, 2021

要标识 Citrix Application Delivery Management (ADM) 服务器，可以为该服务器分配一个主机名。主机名显示在 Citrix ADM 的通用许可证上。

要为 **Citrix ADM** 服务器分配主机名，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 系统管理”。
2. 在 **System Settings**（系统设置）下方，单击 **Change Hostname**（更改主机名）。
3. 在 “ 配置主机名” 页上，输入主机名，然后单击 “ 确定”。

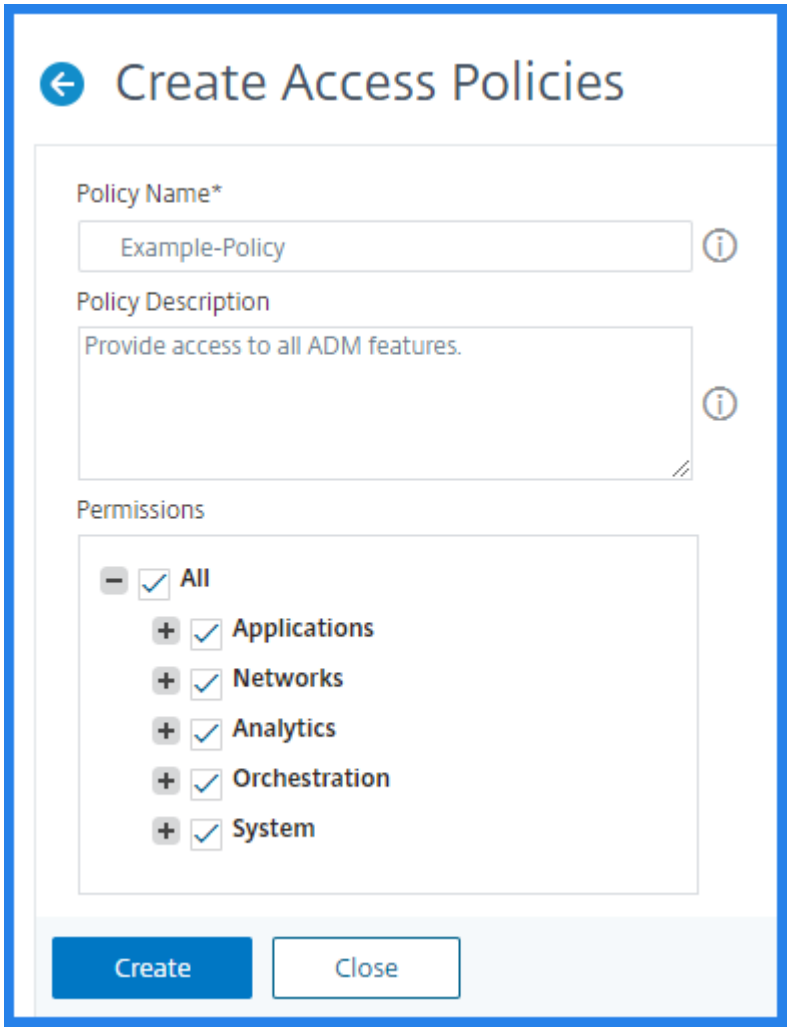


备份和还原您的 **Citrix ADM** 服务器

April 23, 2021

您可以对 Citrix ADM 服务器进行定期备份。您可以备份和还原配置文件、实例详细信息、系统数据等。

> 注意：
>
> 用户对备份和还原 ADM 服务器的访问权限受到限制。“ 系统” **>** “备份文件” 页面仅向有权访问所有 ADM 功能的用户显示。只有当用户的访问策略具有所有权限时，用户才能访问此页面。通常，超级用户可以访问所有 ADM 功能。



有关更多信息，请参阅 配置访问策略。

在升级之前，请出于预防原因备份 ADM 服务器配置文件。

备份包括以下组件：

- Citrix ADM 配置文件：
  - SNMP
  - Syslog 服务器配置文件
  - NTP 文件
  - SSL 证书
  - 控制中心文件
- Citrix ADM 服务器管理的 Citrix ADC 实例的备份。
- 配置审核模板。
- 存储在数据库中的系统数据：

  - 创建的租户和用户列表。
  - 外部身份验证服务器配置（LDAP、RADIUS 及其他）。
  - 创建的配置作业和作业模板。
- 存储在数据库中的基础结构和应用程序数据：
  - 来自添加和托管的 Citrix ADC 实例的数据。
  - 实例配置文件详细信息、版本详细信息和实例组详细信息等。
  - 管理员创建的静态应用程序（虚拟服务器组）。
- SNMP 设置。

> 注意
>
> 备份中不包括 Analytics 数据、事件、ADM 许可证和 syslog 消息。

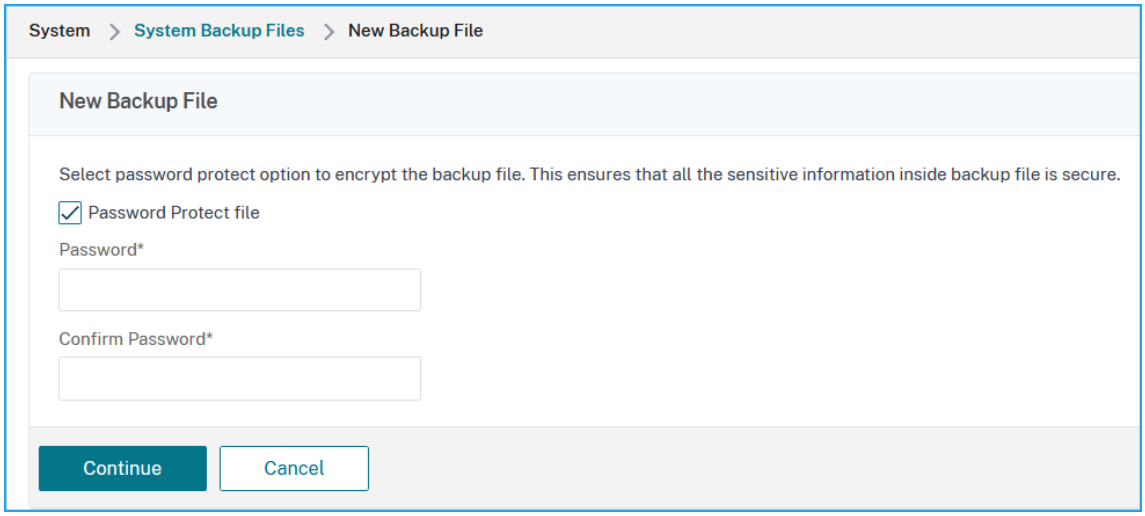
备份 **Citrix ADM** 配置

默认情况下，Citrix ADM 服务器每 24 小时（00.30 小时）备份一次配置。您还可以安排和选择备份的时间。此外，您可以将备份文件的副本移动到另一个系统。

备份以还可加密的压缩 TAR 文件进行存储。默认情况下，在服务器中保留三个备份文件。为避免任何磁盘空间不足问题，您最多可以在 Citrix ADM 服务器上存储 10 个备份文件。但是，Citrix 建议您将备份文件的某些副本存储在服务器上或将文件传输到另一个系统 作为预防措施。

要备份 **Citrix ADM** 配置，请执行以下操作：

1. 导航到 **System**（系统）> **Advanced Settings**（高级设置）> **Backup Files**（备份文件），然后单击 **Back Up**（备份）。
2. 若要加密备份文件，请选中 密码保护文件复选框，然后提供加密文件的密码。



> 注意
>
> 您也可以通过导航到“ 系统”**>**“系统备份设置”，然后选择“加密 备份文件”来设置加 密的备份文件。

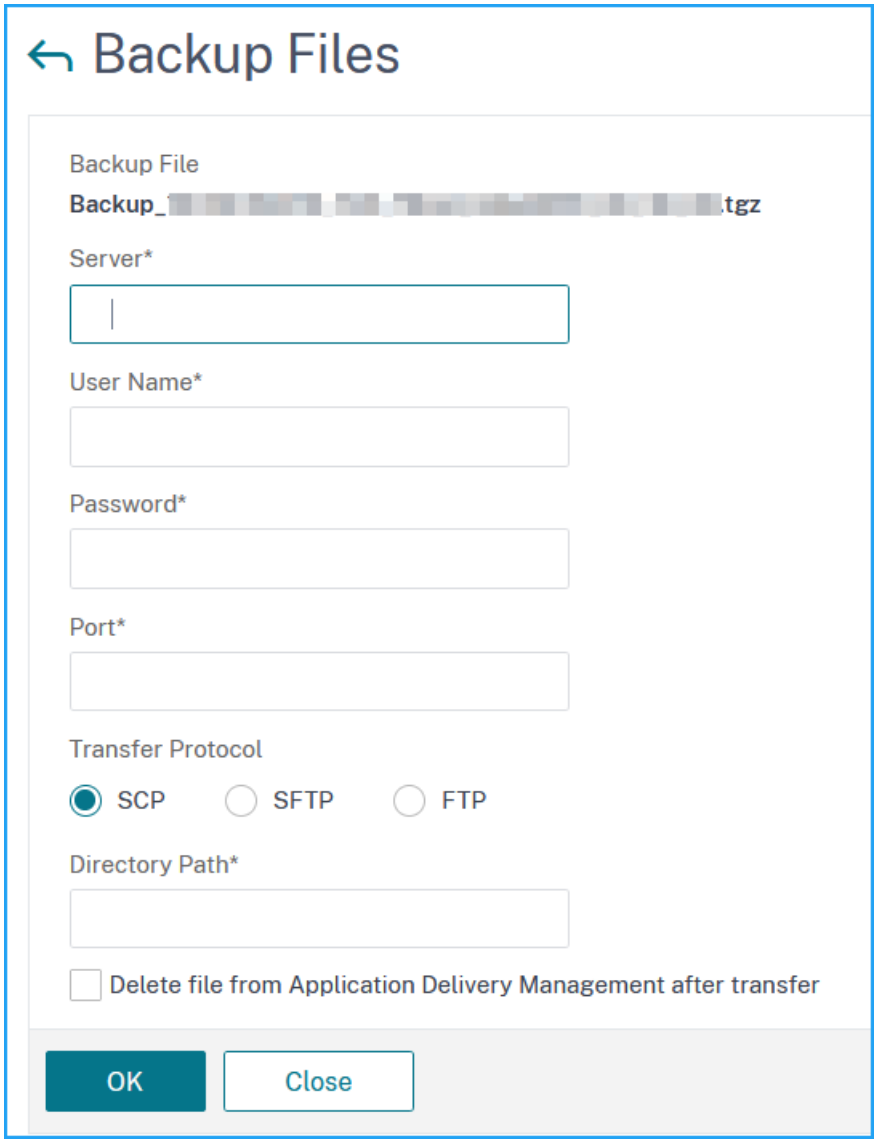
将 **Citrix ADM** 备份文件传输到外部系统

可以将备份文件副本传输到另一个系统上作为预防措施。如果要还原配置，请首先将文件上载到 Citrix ADM 服务器，然后执行恢复操作。

要传输 **Citrix ADM** 备份文件，请执行以下操作：

1. 导航到“系统”>“高级设置”>“备份文件”。
2. 选择要移动到另一个系统的备份文件，然后单击“传输”。
3. 在“ 备份文件”页上，指定以下参数：
   - 服务器 -要传输备份文件的系统的 IP 地址。
   - 用户名和密码 -要复制备份文件的新系统的用户凭据。
   - **Port**（端口）- 文件要传输到的系统的端口号。
   - **Transfer Protocol**（传输协议）- 进行备份文件传输要使用的协议。可以选择 SCP、SFTP 或 FTP 协议来传输备份文件。
   - 目录路径 -在新系统上将备份文件传输到的位置。

   或者，您也可以通过导航到“系统”**>**“系统备份设置”来
   设置外部系统详细信息。
4. 通过选中“传输后从 应用程序交付管理中删除文件”复选框，可以在传输后从 Citrix ADM 中删除备份文件。
5. 单 击“确定”进行传输。



> 注意
>
> 要在本地系统中保存备份文件的副本，请导航到“ 系统”>“ 高级设置”>“ 备份文件”，选择要复制的文件，然后单击“ 下载”。

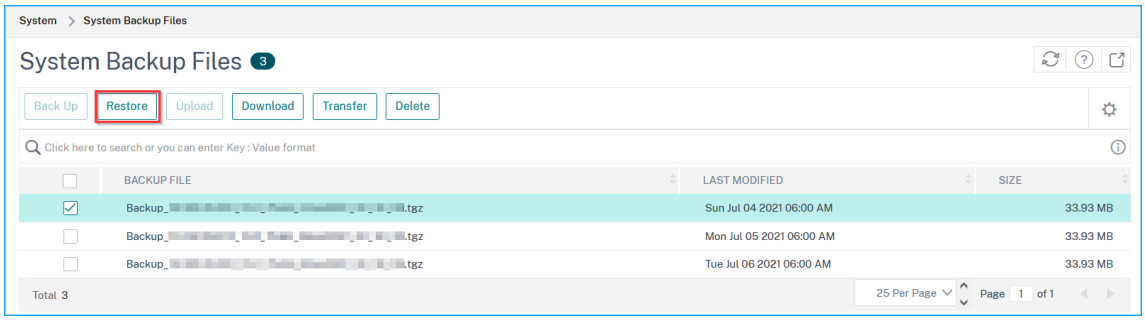
从备份文件还原 **Citrix ADM** 配置

从以前备份的文件还原 Citrix ADM 配置时，还原操作将取消备份文件的修改，然后恢复配置。还原操作会删除现有配置并将其替换为备份文件中的配置。

> 注意
>
> 如果重命名备份文件或修改备份文件内容，还原操作将失败。

要从备份文件还原 **Citrix ADM** 配置，请执行以下操作：

1. 导航到 **System**（系统）> **Advanced Settings**（高级设置）> **Backup Files**（备份文件）。
2. 选择要还原的备份文件，然后单击 **Restore**（还原）。



3. 在确认对话框中，单击 **Yes**（是）。

> 注意
>
> 要从存储在外部系统中的备份文件恢复配置，请在执行还原操作之前将备份文件上传到 ADM 服务器。要上载文件，请导航到 “ 系统” > “ 高级设置” > “ 备份文件”，然后单击 “ 上载”。

查看审计信息

April 23, 2021

Syslog 是日志记录标准协议。它有两个组件：Syslog 审核模块（在 Citrix 应用程序 Delivery Controller (ADC) 实例上运行）和 Syslog 服务器，可以在 Citrix ADC 实例的底层 FreeBSD 操作系统 (OS) 上运行，也可以在远程系统上运行。SYSLOG 使用用户数据报协议 (UDP) 进行数据传输。

通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

如果将设备配置为将 syslog 消息重定向到 Citrix Application Delivery Management (ADM)，则可以监视 Citrix ADC 设备生成的 syslog 消息。您可以安排作业以创建使用 Citrix ADM 中的插入模板功能生成不同类型的 syslog 数据的 syslog 服务器。

首先，配置实例可以向其发送日志信息的 syslog 服务器。然后，指定用于记录日志消息的日期和时间格式。

要在 **Citrix ADM** 上配置系统日志服务器，请执行以下操作：

1. 导航到 “系统” > “审核”。在 “ 配置摘要” 下，选择 “ 系统日志服务器”。也可以导航到 “ 系统” > “ 审计” > “系统日志服务器”。
2. 在 “系 统日志服务器” 页中，单击添加。
3. 在 **Create Syslog Server**（创建 Syslog 服务器）页面上，输入以下值：
   - **Name**（名称）- syslog 服务器的名称。
   - **IP Address**（IP 地址）- syslog 服务器的 IP 地址。
   - **Port**（端口）- Syslog 服务器端口。

4. 选择日志级别（All（全部）、None（无）或 Custom（自定义））。相应地选择严重级别。
5. 单击创建。

要在 **Citrix ADM** 上配置系统日志日志日期和时间格式，请执行以下操作：

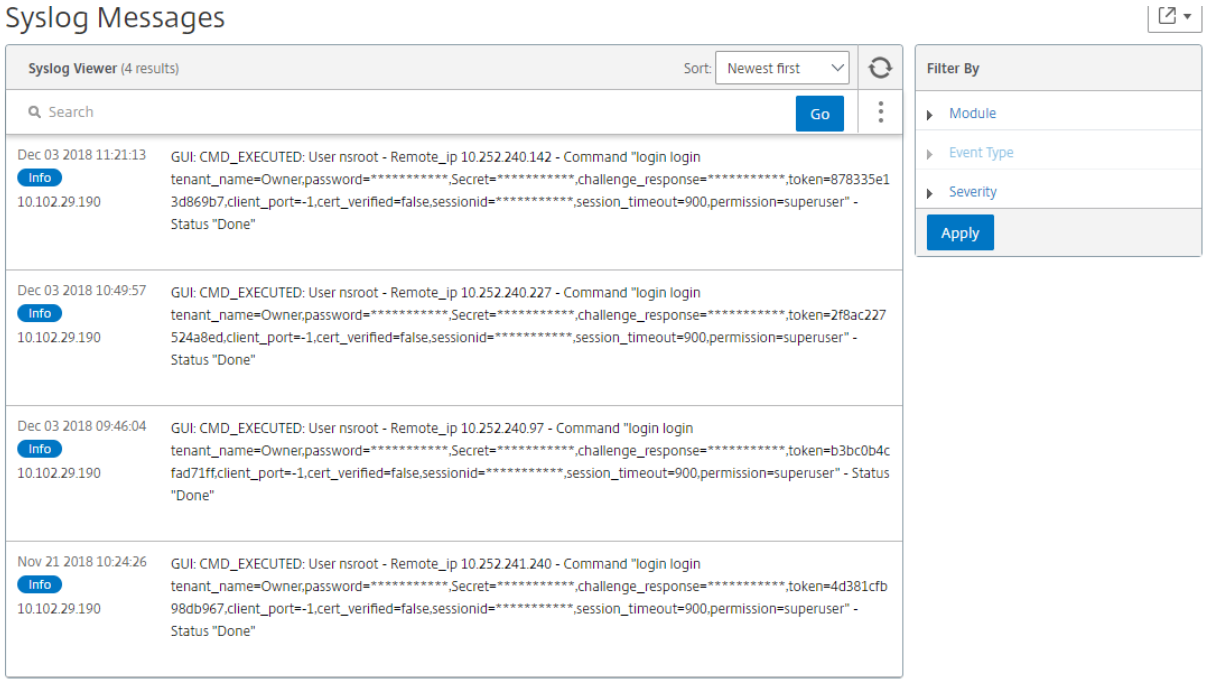
1. 导航到“系统”>“审核”。在“配置摘要”下，选择“系统日志服务器”。
2. 在“系统日志服务器”页中，选择一个系统日志服务器，然后单击系统日志参数。
3. 在 **Configure Syslog Parameters**（配置 Syslog 参数）页面上，指定日期和时间格式。
4. 单击确定。

要查看 **Citrix ADM** 上的系统日志消息，请执行以下操作：

如果您已将实例配置为将 syslog 消息重定向到 Citrix ADM 服务器，则现在可以查看在托管 Citrix ADC 实例上生成的所有 syslog 消息。系统日志消息集中存储在 Citrix ADM 服务器的数据库中，并将在系统日志查看器上提供这些消息以便进行审核。可以合并此日志记录信息，并基于收集的数据得出分析报告。

您可以按模块、事件类型和严重性过滤此信息。还可以配置 syslog 来记录不同类型的事件。

要查看系 统日志查看器，请导航到“ 系统”>“ 审核”。在“ 审计”页的“ 审计消息”下，选择“ 系统日志消息”。选择合适的过滤器以查看您的系统日志消息。



配置 SSL 设置

April 23, 2021

SSL（安全套接字层）和 TLS（传输层安全性）是常用的安全网络连接协议，它们在用户和服务器之前提供加密通信。您可以在 Citrix Application Delivery Management (ADM) 上配置 SSL 设置，并指定连接到系统的客户端类型。

要为 **Citrix ADM** 配置 **SSL** 设置，请执行以下操作：

1. 导航到 **System**（系统）> **System Administration**（系统管理）。在 **System Settings**（系统设置）下方，单击 **Configure SSL Settings**（配置 SSL 设置）。
2. 在“ **SSL** 设置”页面上，查看当前协议设置和应用于系统的密码套件。
3. 要修改协议设置，请导航到 **Edit Settings**（编辑设置）> **Protocol Settings**（协议设置），进行所需更改。
4. 要修改应用的密码套件，请导航到 **Edit Settings**（编辑设置）> **Cipher Suites**（密码套件），进行所需更改。
5. 单击 **OK**（确定），然后单击 **Close**（关闭）。

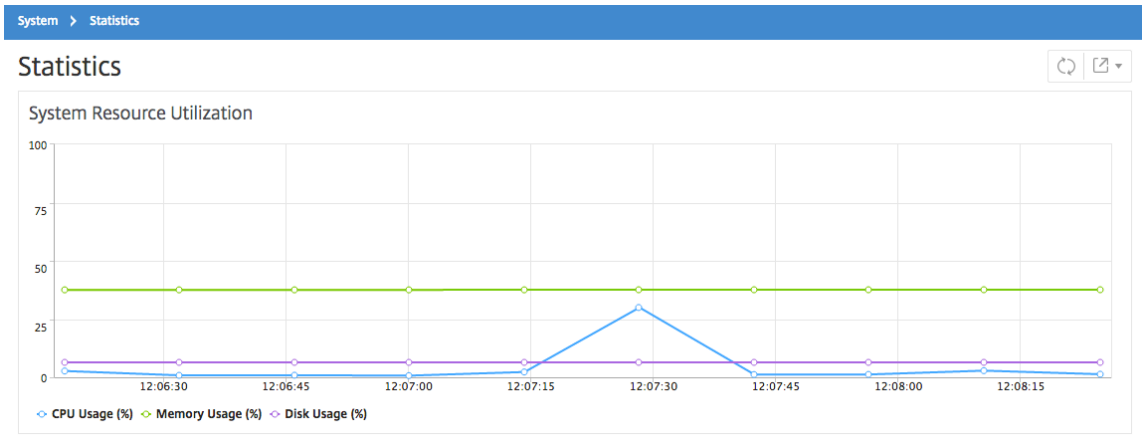
监视 **CPU**、内存和磁盘使用情况

April 23, 2021

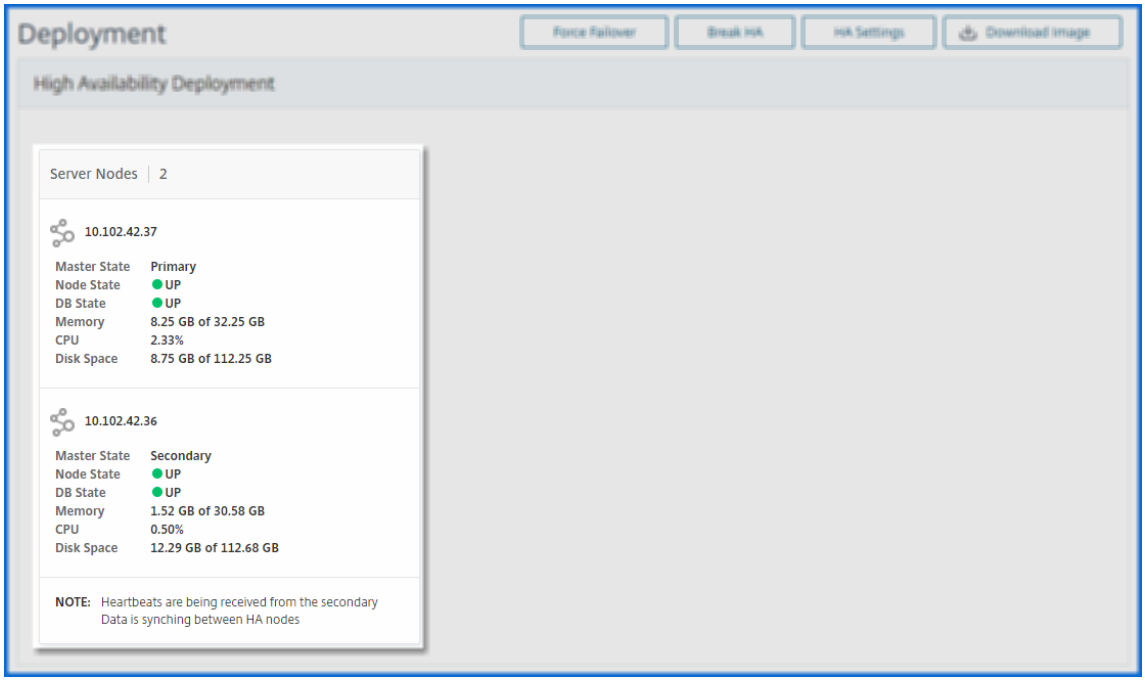
您可以使用日志和统计信息中维护的信息。此信息还显示在帮助您配置和维护 Citrix Application Delivery Management (ADM) 的报告中。

要监视 CPU、内存和磁盘使用情况，请

- 独立部署。导航到“ 系统”**>** “统计信息”。可以查看实时 CPU、内存及磁盘利用率图表。



- 高可用性部署。导航到“ 系统”> “ 部署”。内存、CPU、磁盘空间和托管实例的统计信息以数字方式显示，如下图所示：



配置通知设置

April 23, 2021

您可以选择通知类型以接收以下功能的通知：

- 事件 — 为 Citrix ADC 实例生成的事件列表。有关详细信息，请参阅添加事件规则操作。
- 许可证 — 当前处于活动状态、即将过期等许可证的列表。有关详细信息，请参阅Citrix ADM 许可证到期。
- **SSL** 证书 — 添加到 Citrix ADC 实例的 SSL 证书列表。有关详细信息，请参阅SSL 证书到期。

ADM 支持以下通知类型：

- 电子邮件
- SMS
- Slack
- 寻呼责任
- ServiceNow

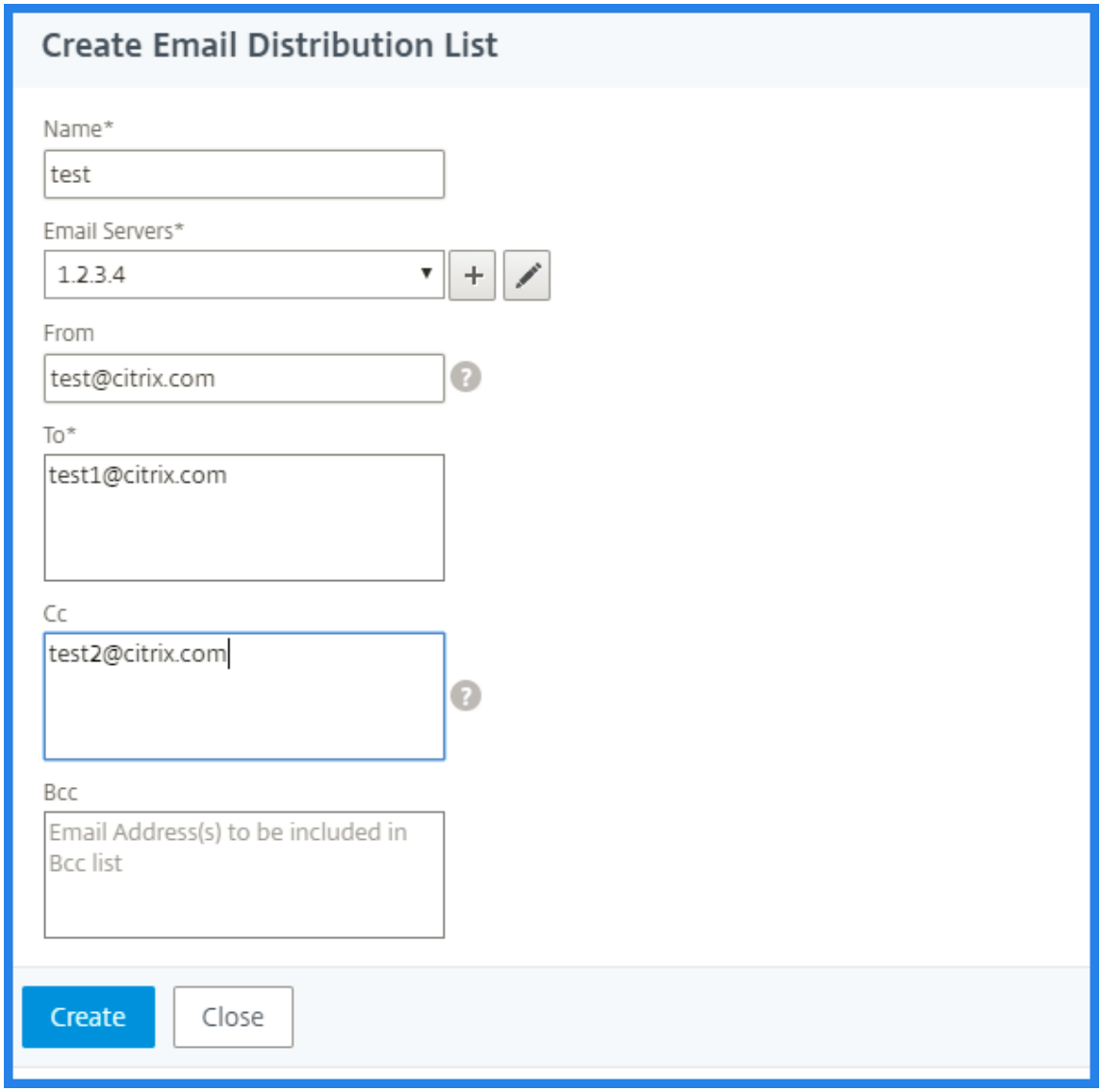
对于每种通知类型，ADM GUI 显示已配置的通讯组列表或配置文件。ADM 将通知发送到选定的通讯组列表或配置文件。

创建电子邮件通讯组列表

要接收 ADM 功能的电子邮件通知，必须添加电子邮件服务器和通讯组列表。

执行以下步骤创建电子邮件通讯组列表：

1. 导航到 **System**（系统）**> Notifications**（通知）。
2. 在 电子邮件中，单击 添加。
3. 在 创建电子邮件通讯组列表中，指定以下详细信息：
   - 名称 -指定通讯组列表名称。
   - 电子邮件服务器 -选择发送电子邮件通知的电子邮件服务器。如果要添加电子邮件服务器，请单击 “ 添加”。
   - 发件人**-**指定 **ADM** 必须从中发送消息的电子邮件地址。
   - 收件人-指定 ADM 必须向其发送消息的电子邮件地址。
   - 抄送-指定 ADM 必须向其发送邮件副本的电子邮件地址。
   - 密件抄送-指定 ADM 必须向其发送邮件副本而不显示地址的电子邮件地址。



4. 单击创建。

重复此过程以创建多个电子邮件通讯组列表。电子邮件选项卡显示 ADM 中存在的所有电子邮件通讯组列表。

创建短信通讯组列表

要接收 ADM 功能的 SMS 通知，必须添加 SMS 服务器和电话号码。

执行以下步骤配置 SMS 通知设置：

1. 导航到 **System**（系统）**> Notifications**（通知）。
2. 在 **SMS** 中，单击 添加。
3. 在 创建 **SMS** 通讯组列表中，指定以下详细信息：
    - 名称 -指定通讯组列表名称。
    - **SMS** 服务器 -选择发送 SMS 通知的 SMS 服务器。
    - 收件人-指定 ADM 必须向其发送消息的电话号码。
4. 单击创建。

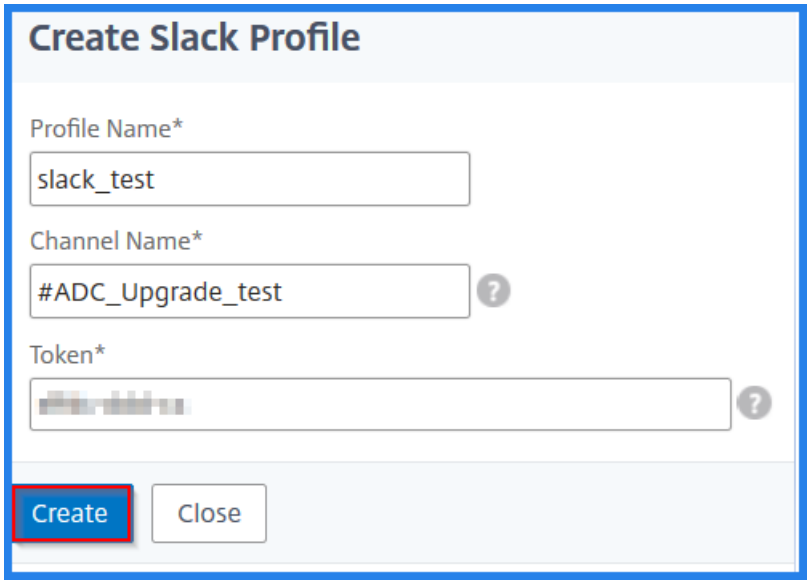
重复此过程以创建多个 SMS 通讯组列表。**SMS** 选项卡显示 ADM 中存在的所有 SMS 通讯组列表。

创建 **Slack** 配置文件

要接收 ADM 函数的 Slack 通知，必须创建松弛配置文件。

执行以下步骤来创建 “Slack” 配置文件：

1. 导航到 **System**（系统）**> Notifications**（通知）。
2. 在 “ **Slack**” 中，单击 “ 添加”。
3. 在 创建 **Slack** 配置文件中，指定以下详细信息：
    - 配置文件名称 -指定配置文件名称。此名称显示在 “Slack” 配置文件列表中。
    - 通道名称 -指定 ADM 必须向其发送通知的 Slack 通道名称。
    - **Webhook** 网址 -指定频道的网址。传入的网络挂钩是将来自外部来源的消息发布到 Slack 的一种简单方法。URL 在内部链接到频道名称。而且，所有事件通知都会发送到此 URL 上的指定 Slack 频道。webhook 的一个示例如下：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. 单击创建。

重复此过程以创建多个“Slack”配置文件。“ **Slack** ”选项卡显示 ADM 中存在的所有 Slack 配置文件。

创建寻呼服务配置文件

您可以添加 PageRor 配置文件来监视基于 PageRor 配置的事件通知。使用 PageNty，您可以通过电子邮件、短信、推送通知和电话在注册号码上配置通知。

在 Citrix ADM 中添加 PagerDuty 配置文件之前，请确保您已完成了 PagerDuty 中所需的配置。要开始使用“寻呼工作”，请参阅 PagerDuty 文档。

请执行以下步骤来创建“寻呼”配置文件：

1. 导航到 **System**（系统）**> Notifications**（通知）。
2. 在“ 寻呼值”中，单击“ 添加”。
3. 在 创建寻呼机配置文件中，指定以下详细信息：
   - 配置文件名称 -指定您选择的配置文件名称。
   - 集成密钥 -指定集成密钥。您可以从您的 PageRty 门户网站获取此密钥。
4. 单击创建。

有关更多信息，请 服务和集成 参阅 PageRty 文档中的。

重复此过程以创建多个 PageRate 配置文件。“ 寻呼工作”选项卡显示 ADM 中存在的所有寻呼工作配置文件。

查看服务 **Now** 配置文件

如果要为 Citrix ADC 事件和 ADM 事件启用服务 Now 通知，则必须使用 ITSM 连接器将 Citrix ADM 与服务 Now 集成。有关详细信息，请参阅将 Citrix ADM 与 ServiceNow 实例集成。

执行以下步骤以查看和验证 ServiceNow 配置文件：

1. 导航到 **System**（系统）**> Notifications**（通知）。
2. 在 “ 服务 **Now**” 中，从列表中选择 **Citrix** 工作空间 **_SN** 配置文件。
3. 单击测试以自动生成 ServiceNow 票证并验证配置。

   如果要在 Citrix ADM GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。

生成技术支持文件

April 23, 2021

Citrix 建议您在联系技术支持以调试问题之前，生成 Citrix Application Delivery Management (ADM) 数据和统计信息的存档。存档是可以发送给技术支持团队的 TAR 文件。

> 注意
>
> 对于高可用性模式下的 Citrix ADM 服务器，您可以从任一服务器生成技术支持文件。Citrix 建议您不要使用负载平衡虚拟服务器 IP 地址来生成技术支持文件。

要从 **Citrix ADM** 配置和发送技术支持文件，请执行以下操作：

1. 导航到 “ 系统” > “ 诊断” > “ 技术支持”，然后单击 “ 生成技术支持文件”。
2. 在 “ 生成支持文件” 页上，选择以下选项：

- 收集调试日志 — 选择此选项可收集 `afdecoder` 日志。
- 持续时间 — 输入必须收集调试日志的持续时间。如果启用了 “ 收集调试日志” 选项，您将只会看到此选项。
- **Collect Data Distribution**（收集数据分发）- 选择此选项以从数据库中收集各种各样的日志。

```
存档文件以 TAR 文件格式创建。

例如，创建的存档文件可能命名如下：    Citrix_ADM<ADM_IP_address> _
   <DDMMYY> _ _ <time_stamp> .tar.gz
```

1. 您可以通过两种方式将技术支持文件发送给支持团队：

   a) 您可以将文件从 ADM GUI 下载到本地存储器，然后使用 Web 浏览器上传到 CIS。

   b) 您还可以通过在 ADM 控制台上运行脚本将技术支持文件上传到 Citrix 智能分析服务 (CIS) 网站。

      i. 使用 SSH 登录 ADM 控制台。

      ii. 切换到命令行管理程序提示符键入：

      */mps/*收集器上传*.pl*

下面给出了完整的命令，其中包含您需要提供的属性：

```
/mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
    proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
     <sr>] [-description <description>] [-debug] <file>
<!--NeedCopy-->
```

运行 Perl 脚本的优点是，您不必将技术支持文件从 ADM 下载到本地系统，然后将其上传到 CIS。作为一个选项，您可以使用 ADM 控制台的代理直接将文件上传到 CIS。

确保您在 CIS 上有一个帐户。您可以使用 Citrix 帐户凭据将文件上传到 CIS。

如果你没有代理服务器呢？或者，如果您遇到 SSL 转发代理的一些问题，该怎么办？（如果 Perl 脚本不信任代理服务器的根证书，则会发生这种情况。）
您仍然可以将文件直接从 ADM shell 上传到 CIS。

> 注意：在 ADM 无法从控制台将文件上传到 CIS 的情况下，
>
> 您仍然可以下载该文件并通过电子邮件发送给 Citrix 技术支持团队。或者，您可以将文件从 ADM 下载到本地存储器，然后使用 Web 浏览器上传到 CIS。

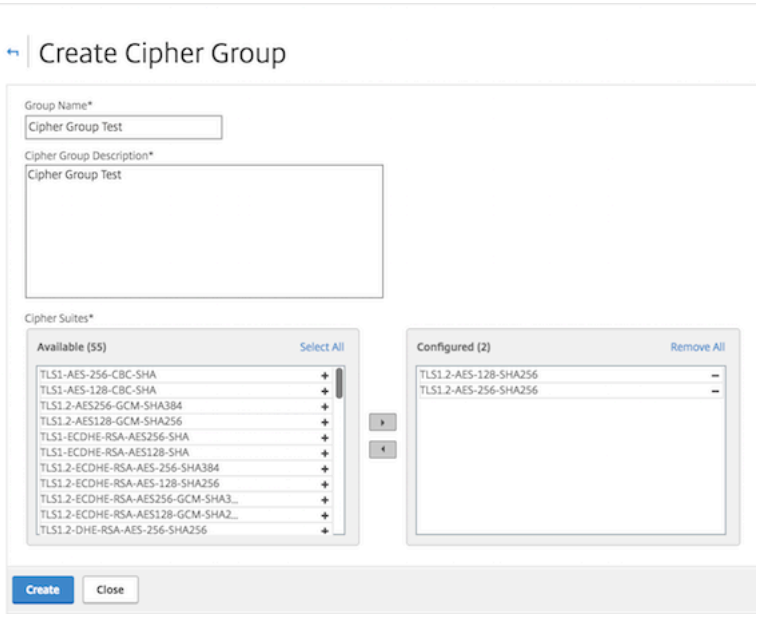
配置密码组

April 23, 2021

密码组是绑定到 Citrix 应用程序 Delivery Controller (ADC) 实例上的 SSL 虚拟服务器、服务或服务组的一组密码套件。密码套件包括协议、密钥交换 (Kx) 算法、身份验证 (Au) 算法、加密 (Enc) 算法和消息身份验证码 (Mac) 算法。

要在 **Citrix ADM** 上添加密码组，请执行以下操作：

1. 导航至 “ 系统” > “ 管理”
2. 在 “ **SSL** 设置” 下，单击 “ 密码组”
3. 单击添加。
4. 在 **Create Cipher Group**（创建密码组）页面上，输入以下详细信息：
    - **Group Name**（组名）- 密码组的名称。
    - **Cipher Group Description**（密码组说明）– 提供密码组的说明。
    - **Cipher Suites**（密码套件）– 单击 “Add”（添加）从 “Available”（可用）列表中选择密码套件，然后将所选（或全部）密码套件移至 “Configured”（已配置）列表。
5. 单击创建。



创建 **SNMP** 陷阱目标、管理者社区和用户

April 23, 2021

每当 Citrix ADM 出现异常情况时，都会生成 SNMP 陷阱。然后将陷阱发送到称为陷阱目标服务器的远程设备或 *SNMP* 陷阱目标。在此处，Citrix ADM 配置为陷阱目标。您可以从名为 SNMP 管理器的远程设备查询 *SNMP* 代理以获取特定于系统的信息。该代理随后会在管理信息库 (MIB) 搜索请求的数据，并将其发送到 SNMP 管理器。

要在 **Citrix ADM** 上创建 **SNMP** 陷阱目标，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Trap Destinations**（陷阱目标）。
2. 在 **SNMP** 陷阱下，单击 添加以创建 SNMP 陷阱，然后指定以下详细信息：
   - 版本。选择要使用的 SNMP 版本。
   - 目标服务器。陷阱目标的名称或 IP 地址。
   - **Port**（端口）。输入陷阱目的地的端口。该端口默认设置为 162。
   - 社区。指定向陷阱侦听器发送陷阱时要使用的社区字符串。
3. 单击创建。

> 注意
>
> 如果要创建 SNMP v3 陷阱目标，请指定要将陷阱绑定到的 SNMP 用户凭据。若要添加 SNMP 用户凭据，请单击 插入，然后从可用 SNMP 用户列表中添加该用户。

要创建 **SNMP** 管理器社区，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Managers**（管理器）。
2. 在 **SNMP** 管理器下，单击 添加以创建 SNMP 管理器社区，然后指定以下详细信息：
   - **SNMP** 管理器。输入 SNMP 管理器的名称或 IP 地址。
   - 社区。指定将陷阱发送到陷阱侦听器时要使用的社区字符串。
3. （可选）您可以选中 **“启用管理网络”** 复选框以指定作为 **SNMP** 管理器网络子网掩码的子网掩码。
4. 单击创建。

要创建 **SNMP** 用户，请执行以下操作：

1. 导航到 **System**（系统）> **SNMP** > **Users**（用户）。
2. 在 **SNMP** 用户下，单击 添加。
3. 输入用户名并从菜单中为用户分配安全级别。
4. 根据您分配给用户的安全级别，提供额外的身份验证协议，如身份验证协议、隐私密码和分配 SNMP 视图。

配置和查看系统警报

April 23, 2021

您可以启用和配置一组警报，以监视 Citrix Application Delivery Management (ADM) 服务器的运行状况。您必须配置系统警报，以确保您了解任何关键或主要的系统问题。例如，您可能希望在 CPU 使用率较高或存在多次登录服务器失败时收到通知。对于有些警报类别（例如 cpuUsageHigh 或 memoryUsageHigh），您可以为每项设置阈值并定义严重性（例如 “Critical”（严重）或 “Major”（重大））。对于有些类别（例如 inventoryFailed 或 loginFailure），只能定义严重性。当警报类别（例如 MemoryUsageHigh）超出阈值时，或发生与警报类别对应的事件（例如 登录失败）时，系统中将记录一条消息，您可以将该消息作为 syslog 消息查看。可以进一步设置通知以接收对应于警报设置的电子邮件或 SMS。

可以分配或修改警报的严重性。您可以分配的严重性级别包括 “严重”、“主要”、“次要”、“警告” 和 “信息性”。

考虑一种情况，您希望在备份尝试失败时监视。您可以启用 BackupFailed 警报并为其分配严重性，例如 “主要”。每当 Citrix ADM 尝试备份系统文件以及尝试失败时，都会触发警报。您可以在 Citrix ADM 上查看消息，也可以通过电子邮件或短信获取通知。

要配置警报，您必须选择备份失败警报，并将严重性级别指定为 “主要”。默认情况下，启用警报。

要使用 **Citrix ADM** 配置和查看系统警报，请执行以下操作：

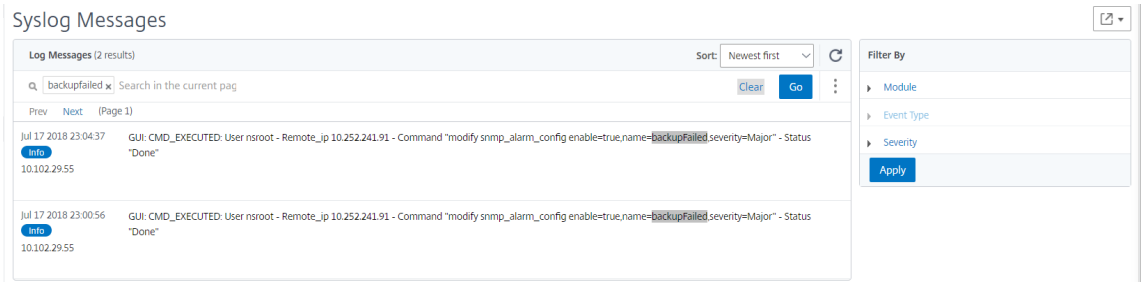
1. 导航到 **System**（系统）**> SNMP**。单击右上角的 “ 警报”。

2. 选择要配置的警报（例如，备份失败），然后单击 “ 编辑” 修改其设置。
3. 默认情况下，启用警报。指定严重性级别（例如：主要），然后单 击确定。

> 注意
>
> 对于一些警报，您无法设置阈值。
> 触发警报后，可以查看以 syslog 消息形式存在的生成事件。

要使用 **Citrix ADM** 查看由备份失败警报生成的事件，请执行以下操作：

1. 导航到 “系统” > “审核”。
2. 在 “审计” 页的 “审计消息” 下，选择 “系统日志消息”。
3. 在搜索字段中，键入警报的名称。
   在此示例中，您可以看到为失败的备份尝试生成了一个事件。



您还可以设置通知以在触发警报时向您发送电子邮件或 SMS（短信服务）文本。有关如何配置系统通知的信息，请参阅 如何配置 Citrix ADM 的系统通知设置。

作为 **API** 代理服务器的 **Citrix ADM**

April 23, 2021

除了能够接收自己的管理和分析功能的 NITRO REST API 请求之外，Citrix Application Delivery Management (Citrix ADM) 还可以作为其托管实例的 REST API 代理服务器。REST API 客户端可以将 API 请求发送到 Citrix ADM，而不是直接向托管实例发送 API 请求。Citrix ADM 可以区分它必须响应的 API 请求和它必须转发到托管实例的 API 请求。

作为 API 代理服务器，Citrix ADM 为您提供了以下好处：

- 验证 **API** 请求。Citrix ADM 根据配置的安全性和基于角色的访问控制 (RBAC) 策略验证所有 API 请求。Citrix ADM 还具有租户感知功能，并确保 API 活动不会跨越租户边界。
- 集中审核。Citrix ADM 维护与其托管实例相关的所有 API 活动的审核日志。
- 会话管理。Citrix ADM 使 API 客户端不必维护与托管实例的会话的任务。

Citrix ADM 作为 **API** 代理服务器的工作原理

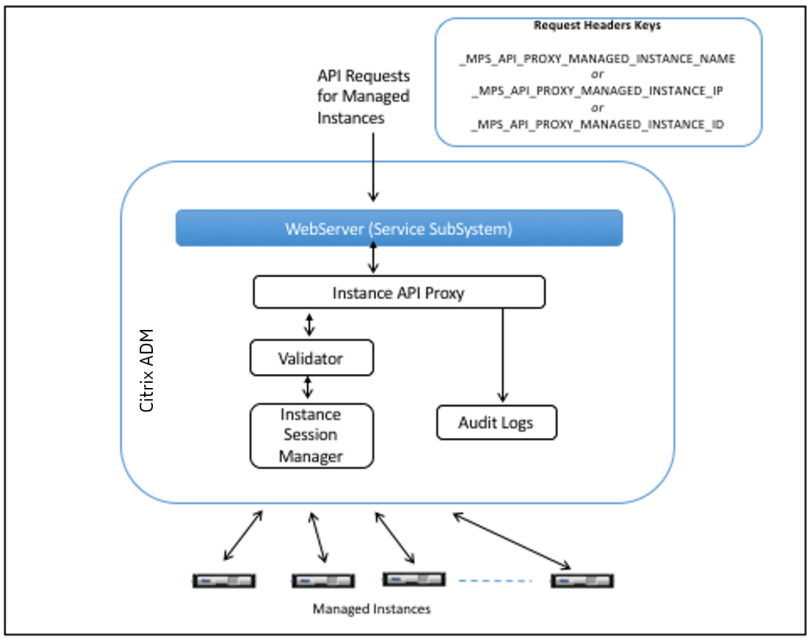
如果希望 Citrix ADM 将请求转发到托管实例，则可以将 API 客户端配置为在 API 请求中包含以下任何一个 HTTP 标头：

标题值	说明
_MPS_API_PROXY_MANAGED_INSTANCE_NAME	托管实例的名称。
_MPS_API_PROXY_MANAGED_INSTANCE_IP	托管实例的 IP 地址。
_MPS_API_PROXY_MANAGED_INSTANCE_ID	托管实例的 ID。
_MPS_API_PROXY_TIMEOUT	NITRO API 请求的超时值。以秒为单位设置超时值。当您设置代理超时时，ADM 将等待指定的持续时间，然后再超时请求。
_MPS_API_PROXY_MANAGED_INSTANCE_ 用户名	用于访问托管 ADC 实例的用户名。
_MPS_API_PROXY_MANAGED_INSTANCE_ 密码	访问托管 ADC 实例的密码。
_MPS_API_PROXY_MANAGED_INSTANCE_SESSIL	访问托管实例的会话 ID。

> 注意
>
> ：在系统 **>** 管理 **>** 系统配置 **>** 基本设置中，如果选择了实例的提示凭证登录，请务必配置托管实例的用户名和密码。或者，您还可以指定实例会话 ID。

存在这些 HTTP 标头中的任何一个可帮助 Citrix ADM 将 API 请求识别为它必须转发给托管实例的 API 请求。标头的值可帮助 Citrix ADM 识别它必须将请求转发到的托管实例。

下图中说明了此流程：



如上图所示，当请求中出现其中一个 HTTP 标头时，Citrix ADM 按如下方式处理请求：

1. 在不修改请求的情况下，Citrix ADM 会将请求转发到实例 API 代理引擎。
2. 实例 API 代理引擎将 API 请求转发至验证程序，并将 API 请求的详细信息记录在审核日志中。
3. 验证程序确保请求没有违反配置的安全策略、RBAC 策略、租赁边界等。它会执行额外的检查，例如检查以确定托管实例是否可用。

如果 API 请求有效且可以转发到托管实例，Citrix ADM 会标识由实例会话管理器维护的会话，然后将请求发送到托管实例。

> 注意：
>
> 确保禁用“提示实例登录凭据”选项。对此，请执行以下操作：
>
> 1. 导航到 **“系统” > “管理”**。
> 2. 在 系统配置中，选择 系统、时区、允许的 **URL** 和当日消息。

如何将 **Citrix ADM** 用作 **API** 代理服务器

以下示例显示了 API 客户端发送到 IP 地址为 192.0.2.5 的 Citrix ADM 服务器的 REST API 请求。需要 Citrix ADM 将请求（未更改）转发到具有 IP 地址 192.0.2.10 的托管实例。所有示例都使用 _MPS_API_PROXY_MANAGED_INSTANCE_IP 标头。

在向 Citrix ADM 发送 API 请求之前，API 客户端必须：

- 登录到 Citrix ADM
- 获取会话 ID

- 在后续 API 请求中包含会话 ID。

登录 API 请求的形式如下：

```
    POST /nitro/v1/config/login
    Content-Type: application/json

    {

        "login": {

            "username":"nsroot",
            "password":"nsroot"
          }

     }

<!--NeedCopy-->
```

Citrix ADM 通过包含会话 ID 的响应响应登录请求。以下示例响应正文显示了会话 ID：

```
{


  "errorcode": 0,

  "message": "Done",

  "operation": "add",

  "resourceType": "login",

  "username": "***********",

  "tenant_name": "Owner",

  "resourceName": "nsroot",

  "login": [

    {


      "tenant_name": "Owner",

      "permission": "superuser",
```



```
26
27        "session_timeout": "36000",
28
29        "challenge_token": "",
30
31        "username": "",
32
33        "login_type": "",
34
35        "challenge": "",
36
37        "client_ip": "",
38
39        "client_port": "-1",
40
41        "cert_verified": "false",
42
43        "sessionid": "##
      D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D",
44
45        "token": "b2f3f935e93db6a"
46       }
47
48
49    ]
50
51   }
52
53 <!--NeedCopy-->
```

示例 **1**：检索负载平衡虚拟服务器统计信息

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
1      GET /nitro/v1/stat/lbvserver
2      Content-type: application/json
3      _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4      SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5  <!--NeedCopy-->
```

其中 Cookie 标头的值是从登录 API 调用返回的会话 ID。而 _MPS_API_PROXY_MANAGED_INSTANCE_IP 的值是 ADC 的 IP 地址。

示例 **2**：创建负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
1     POST /nitro/v1/config/lbvserver/sample_lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9          "lbvserver":{
10
11             "name":"sample_lbvserver",
12             "servicetype":"HTTP",
13             "ipv46":"10.102.1.11",
14             "port":"80"
15          }
16
17      }
18
19 <!--NeedCopy-->
```

示例 **3**：修改负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
1     PUT /nitro/v1/config/lbvserver
2     Content-type: application/json
3     Accept-type: application/json
4     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
5     SESSID: ##
          D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
6
7     {
8
9        "lbvserver":{
10
11            "name":"sample_lbvserver",
12            "appflowlog":"DISABLED"
13         }
14
15      }
```



```
16
17 <!--NeedCopy-->
```

示例 **4**：删除负载平衡虚拟服务器

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
1     DELETE /nitro/v1/config/lbvserver/sample_lbvserver
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6 <!--NeedCopy-->
```

示例 **5**：在 **ADC** 上下载 **CLI** 运行配置

客户端必须向 Citrix ADM 发送以下形式的 API 请求：

```
1     GET /nitro/v1/config/nsrunningconfig
2     Accept-type: application/json
3     _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
4     SESSID: ##
         D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D
5
6 <!--NeedCopy-->
```

使用 **Citrix ADM** 在 **AWS** 中自动扩展 **Citrix ADC**

April 23, 2021

在云中高效托管应用程序涉及根据应用程序需求轻松且经济高效地管理资源。例如，假设您有一个在 AWS 上运行的电子商务门户网站。此门户有时提供巨大的折扣，在此期间，应用程序流量出现峰值。当这些产品提供期间应用程序流量增加时，必须动态扩展应用程序，因此可能还需要增加网络资源。

Citrix ADM 自动扩展功能支持在 AWS 中预 Provisioning 和自动扩展 Citrix ADC 实例。Citrix ADM 自动缩放功能会持续监视阈值参数，如内存使用率、CPU 使用率和吞吐量。您可以选择其中一个参数或多个参数进行监视。然后将这些参数值与用户配置的值进行比较。如果参数值超出限制，则相应地触发向外扩展或缩放。

Citrix ADM AutoScale 功能体系结构的设计方式是，您可以为每个 AutoScale 组配置最小和最大实例数。预设这些数字可确保您的应用程序始终正常运行。

自动扩展的好处

应用程序的高可用性。自动缩放可确保您的应用程序始终拥有适当数量的 Citrix ADC VPX 实例来处理流量需求。这是为了确保您的应用程序始终正常运行，而不考虑流量需求。

智能缩放决策和零接触配置。自动缩放可持续监视您的应用程序，并根据需求动态添加或删除 Citrix ADC 实例。当需求上升时，会自动添加实例。当需求向下高峰时，实例会自动移除。
Citrix ADC 实例的添加和删除会自动执行，使其成为零接触手动配置。

自动 **DNS** 管理。Citrix ADM AutoScale 功能提供自动 DNS 管理。每当添加新的 Citrix ADC 实例时，域名都会自动更新。

正常连接终止。在扩展过程中，Citrix ADC 实例会正常移除，避免客户端连接丢失。

更好的成本管理。自动缩放可根据需要动态增加或减少 Citrix ADC 实例。这使您能够优化所涉及的成本。您可以通过仅在需要时启动实例并在不需要时终止实例来节省资金。因此，您只需为使用的资源付费。

可观察性。可观察性是应用程序开发人员或 IT 人员监视应用程序运行状况的关键。Citrix ADM 的 AutoScale 仪表板使您能够可视化阈值参数值、自动缩放触发时间戳、事件和参与自动缩放的实例。

可支持性

目前，仅 AWS 部署支持 AutoScale 功能。

许可要求

为 Citrix AutoScale 组创建的 Citrix ADC 实例使用 Citrix ADC 高级或高级 ADC 许可证。Citrix ADC 群集功能包含在高级或高级 ADC 许可证中。

您可以选择以下方法之一来对 Citrix ADM 置备的 Citrix ADC 进行许可：

- 使用 **Citrix ADM** 中存在的 **ADC** 许可证：在创建 AutoScale 组时配置池容量、VPX 许可证或虚拟 CPU 许可证。因此，当为 AutoScale 组配置新实例时，已配置的许可证类型将自动应用于预配置的实例。
  - 池容量：将带宽分配给 Autoscale 组中的每个预配实例。确保您在 Citrix ADM 中具有预配新实例所需的可用带宽。有关详细信息，请参阅配置池容量。

    Autoscale 组中的每个 ADC 实例都会从池中签出一个实例许可证以及指定的带宽。
  - **VPX** 许可证：将 VPX 许可证应用于新预配置的实例。确保您在 Citrix ADM 中拥有必要数量的可用 VPX 许可证以置备新实例。

    预配置了 Citrix ADC VPX 实例后，该实例将从 Citrix ADM 中签出许可证。有关详细信息，请参阅Citrix ADC VPX 签入和签出许可。
  - 虚拟 **CPU** 许可证：将虚拟 CPU 许可证应用于新预配置的实例。此许可证指定授予 Citrix ADC VPX 实例的 CPU 数量。确保您在 Citrix ADM 中具有必要数量的虚拟 CPU 来置备新实例。

预配置了 Citrix ADC VPX 实例后，该实例将从 Citrix ADM 中签出虚拟 CPU 许可证。有关详细信息，请参阅Citrix ADC 虚拟 CPU 许可。

当预配置的实例被销毁或取消置备时，应用的许可证将自动返回到 Citrix ADM。

要监视已使用的许可证，请导航到 网络 > 许可证页面。

- 使用 **AWS** 订阅许可证：在创建 AutoScale 组时配置 AWS 市场中可用的 Citrix ADC 许可证。因此，当为 AutoScale 组配置新实例时，许可证将从 AWS Marketplace 获取。

AWS 术语

下表简要介绍了本文档中使用的一些自动缩放术语。

术语	说明
AWS 自动扩展组	AWS Auto Scaling 组是具有相似特征的 EC2 实例的集合，为了实例扩展和管理目的，它们被视为逻辑分组。
Amazon Machine Image (AMI)	计算机映像，提供启动实例（云中的虚拟服务器）所需的信息。
弹性计算云 (EC2)	在云中提供安全、可调整大小的计算能力的 Web 服务。它旨在为开发人员简化 Web 规模的云计算。
弹性 IP (EIP) 地址	弹性 IP 地址是专为动态云计算而设计的静态公有 IPv4 地址。您可以将弹性 IP 地址与您账户中任何 VPC 的任何实例或网络接口关联。
弹性网络接口 (ENI)	可以附加到 VPC 中的实例的虚拟网络接口。
实例类型	Amazon EC2 提供了多种实例类型，针对不同的用例进行了优化。实例类型包括 CPU、内存、存储和网络容量的各种组合，让您能够为您的应用程序灵活选择合适的资源组合。
身份识别和访问管理 (IAM) 角色	具有权限策略的 AWS 身份，这些策略确定该身份在 AWS 中可以执行哪些操作以及不能执行哪些操作。您可以使用 IAM 角色启用 EC2 实例上运行的应用程序以安全地访问 AWS 资源。
IAS 实例配置文件	提供给 AWS 中群集中置备的 Citrix ADC 实例的身份。配置文件允许实例在开始对客户端请求进行负载平衡时访问 AWS 服务。
监听器	监听程序是使用您配置的协议和端口检查连接请求的进程。您为侦听器定义的规则决定了负载平衡器如何将请求路由到一个或多个目标组中的目标。

术语	说明
NLB	网络负载平衡器。NLB 是 AWS 环境中可用的 L4 负载平衡器。
53 號公路	Route 53 是亚马逊高度可用且可扩展的云域名系统 (DNS) Web 服务。
安全组	实例的一组指定的允许入站网络连接。
子网	EC2 实例可以附加到的 VPC 的一段 IP 地址范围。您可以根据安全和操作需求创建子网来对实例进行分组。
虚拟专用云 (VPC)	用于置备 AWS 云的逻辑隔离部分的 Web 服务，在此部分您可以在您定义的虚拟网络中启动 AWS 资源。

Citrix ADC VPX 自动缩放术语

下表简要介绍了本文档中使用的某些 Citrix ADC VPX 自动缩放术语。

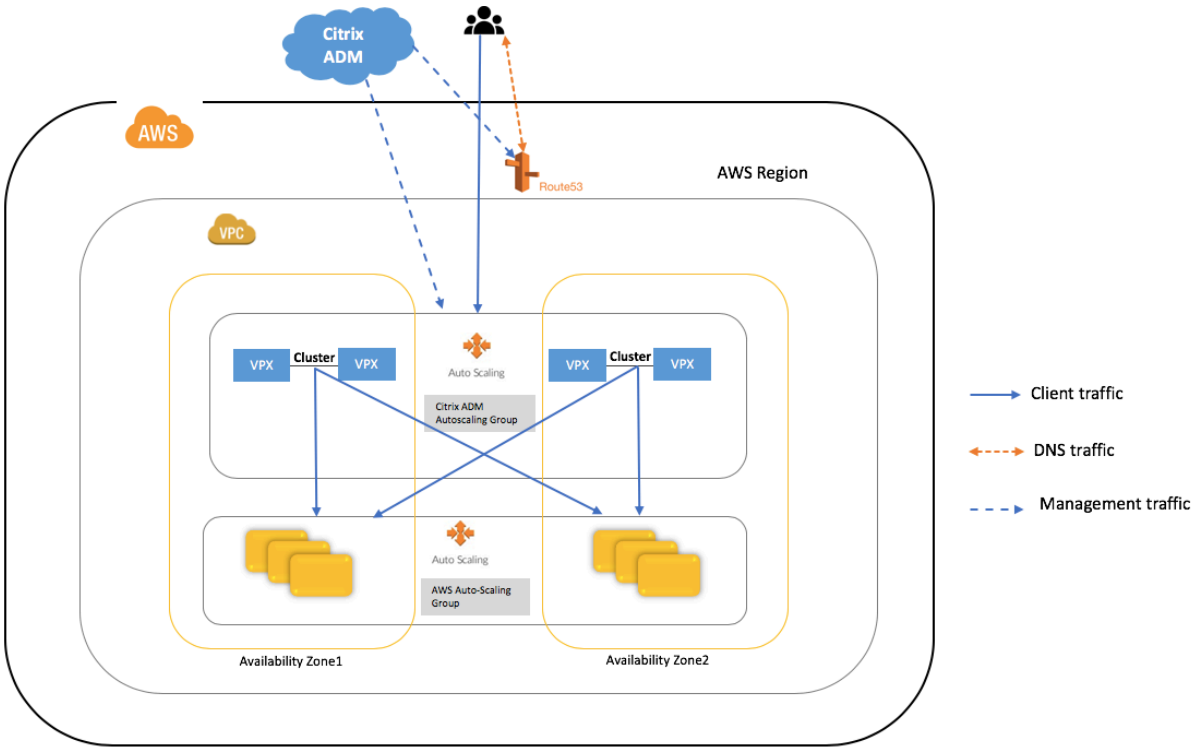
术语	说明
自动缩放组	自动缩放组是一组 Citrix ADC 实例，它们将应用程序作为单个实体进行负载平衡，并在阈值参数超出限制时触发自动缩放。Citrix ADC 实例根据 AutoScale 组配置动态向外扩展或缩减。注意： Citrix AutoScale 组在本文档中称为 AutoScale 组，而 AWS AutoScale 组则被明确称为 AWS AutoScale 组。
Citrix ADC 群集	Citrix ADC 群集是一组 Citrix ADC VPX 实例，每个实例都称为一个节点。客户端流量分布在节点之间，以提供高可用性、高吞吐量和可扩展性。
耗尽连接超时	在扩展期间，一旦选择了要取消置备的实例，Citrix ADM 将从处理到 AutoScale 组的新连接中删除该实例，并等到指定的漏出连接超时期满后才取消置备。这样就可以在取消置备前将与此实例的现有连接耗尽。如果连接在漏极连接超时到期之前耗尽，即使如此，Citrix ADM 也会等待漏极连接超时期过期，然后再开始新的评估。注意：如果连接在耗尽连接超时过期后仍未耗尽连接，Citrix ADM 将删除可能影响应用程序的实例。默认值为 5 分钟，可配置。

术语	说明
冷却时间	在横向扩展之后，冷却时间是指必须停止统计数据评估的时间。这可以在做出下一个扩展决策之前允许当前流量在当前实例集上稳定和平均值，从而确保 AutoScale 组的有机增长。默认冷却时间值为 10 分钟，可配置。注意：默认值是根据向外扩展（大约 4 分钟）后系统稳定所需的时间加上 Citrix ADC 配置和 DNS 通告时间来确定的。
标记	为每个 AutoScale 组分配了一个标签，该标签是键和值对。您可以将标签应用于资源，使您能够轻松地组织和识别资源。这些标签同时应用于 AWS 和 Citrix ADM。示例：键 = 名称，值 = Web 服务器。建议使用一组一致的标签来轻松跟踪可能属于各种组（如开发、生产、测试）的 AutoScale 组。
阈值参数	监视触发向外扩展或扩展的参数。参数为 CPU 使用率、内存使用率和吞吐量。您可以选择一个参数或多个参数进行监视。
生存时间 (TTL)	指定在必须重新查阅信息来源之前，DNS 资源记录可能被缓存的时间间隔。默认 TTL 值为 30 秒，可配置。
观看时间	缩放参数的阈值必须保持超出以便进行缩放的时间。如果在此指定时间内收集的所有样本上超过阈值，则会进行缩放。如果阈值参数在整个持续时间内保持高于最大阈值的值，则会触发向外扩展。如果阈值参数的工作值低于最小阈值，则会触发缩放。默认值为 3 分钟，可配置。

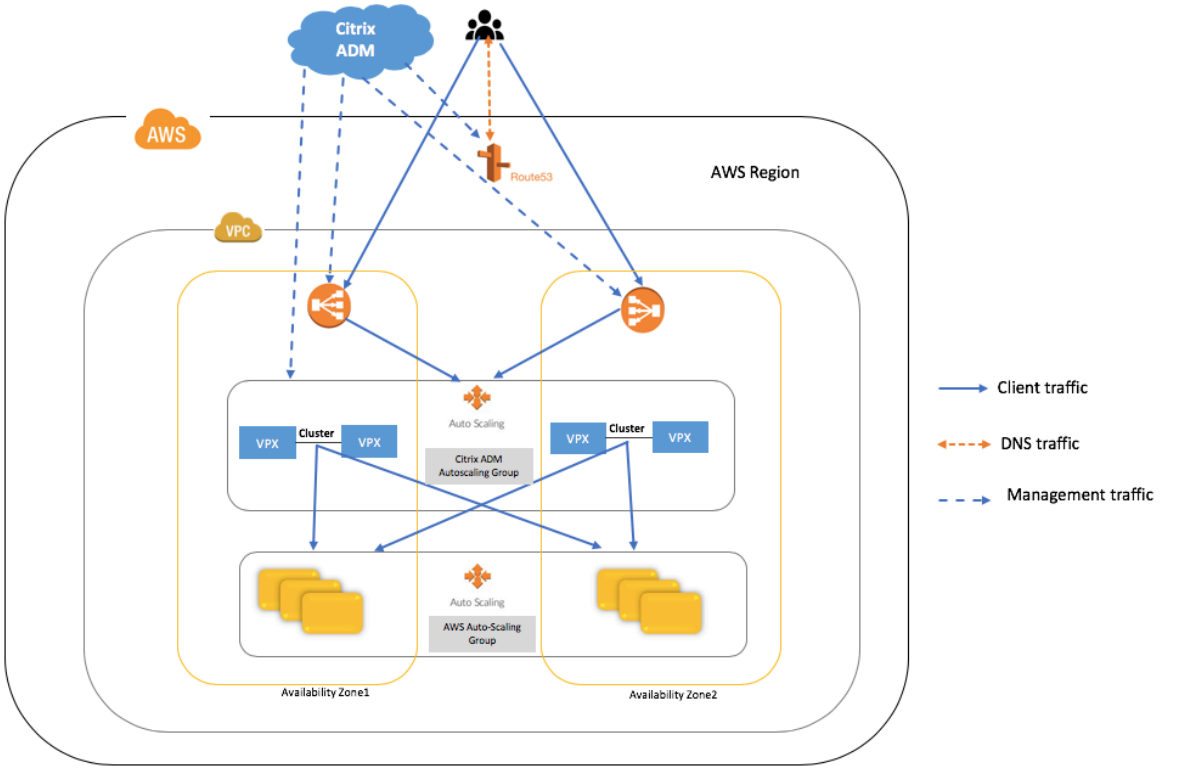
体系结构

April 23, 2021

下图说明了以 DNS 作为流量分配服务器的自动缩放功能的体系结构。



下图说明了以 NLB 作为流量分配器的自动缩放功能的体系结构。



Citrix Application Delivery Management (ADM)

Citrix Application Delivery Management 是一种基于 Web 的解决方案，用于管理部署在本地或云上的所有 Citrix ADC 部署。
您可以使用此云解决方案从单一、统一和集中的基于云的控制台管理、监控和故障排除整个全球应用程序交付基础架构。Citrix Application Delivery Management (ADM) 提供了在 Citrix ADC 部署中快速设置、部署和管理应用程序交付所需的所有功能，并对应用程序运行状况、性能和安全性进行了丰富的分析。

自动缩放组是在 Citrix ADM 中创建的，Citrix ADC VPX 实例是从 Citrix ADM 预配的。然后通过 Citrix ADM 中的样本部署应用程序。

流量分销商（**NLB** 或 **DNS/Route53**）

NLB 或 DNS/route53 用于在 AutoScale 组中的所有节点之间分配流量。有关详细信息，请参阅自动缩放流量分布模式。

Citrix ADM 与流量分销商通信，以更新前端应用程序的负载平衡虚拟服务器的应用程序域和 IP 地址。

Citrix ADM 自动缩放组

自动缩放组是一组 Citrix ADC 实例，它们将应用程序作为单个实体进行负载平衡，并根据配置的阈值参数值触发自动缩放。

Citrix ADC 群集

Citrix ADC 群集是一组 Citrix ADC VPX 实例，每个实例都称为一个节点。客户端流量分布在节点之间，以提供高可用性、高吞吐量和可扩展性。

> 注意
>
> - 自动缩放决策是在群集级别而不是在节点级别做出的。
> - 独立群集托管在不同的可用区中，因此对某些共享状态功能的支持受到限制。
>
> 持久性会话（如源 IP 持久性和除基于 cookie 的持久性之外的其他持久性会话）不能跨群集共享。但是，所有无状态功能（如负载平衡方法）在多个可用区域中按预期工作。

AWS 自动扩展组

AWS Auto Scaling 组是具有相似特征的 EC2 实例的集合，为了实例扩展和管理目的，它们被视为逻辑分组。

AWS 可用区

AWS 可用区是区域内的隔离位置。每个区域由多个可用区组成。每个可用区都属于一个区域。

流量分配模式

当您将应用程序部署迁移到云时，自动扩展将成为基础架构的一部分。当应用程序使用自动缩放进行横向扩展或扩展时，这些更改必须传播到客户端。这种传播是使用基于 DNS 或基于 NLB 的自动缩放来实现的。

基于 **NLB** 的自动缩放

在基于 NLB 的部署模式下，群集节点的分发层是 AWS 网络负载平衡器。

在基于 NLB 的自动扩展中，每个可用区仅提供一个静态 IP 地址。这是添加到 route53 的公有 IP 地址，后端 IP 地址可以是私有的。使用此公有 IP 地址时，在自动扩展期间配置的任何新 Citrix ADC 实例都会使用私有 IP 地址运行，不需要额外的公有 IP 地址。

NLB 仅支持基于 TCP 的负载平衡。如果要支持 UDP 流量，可以选择基于 DNS 的自动缩放。

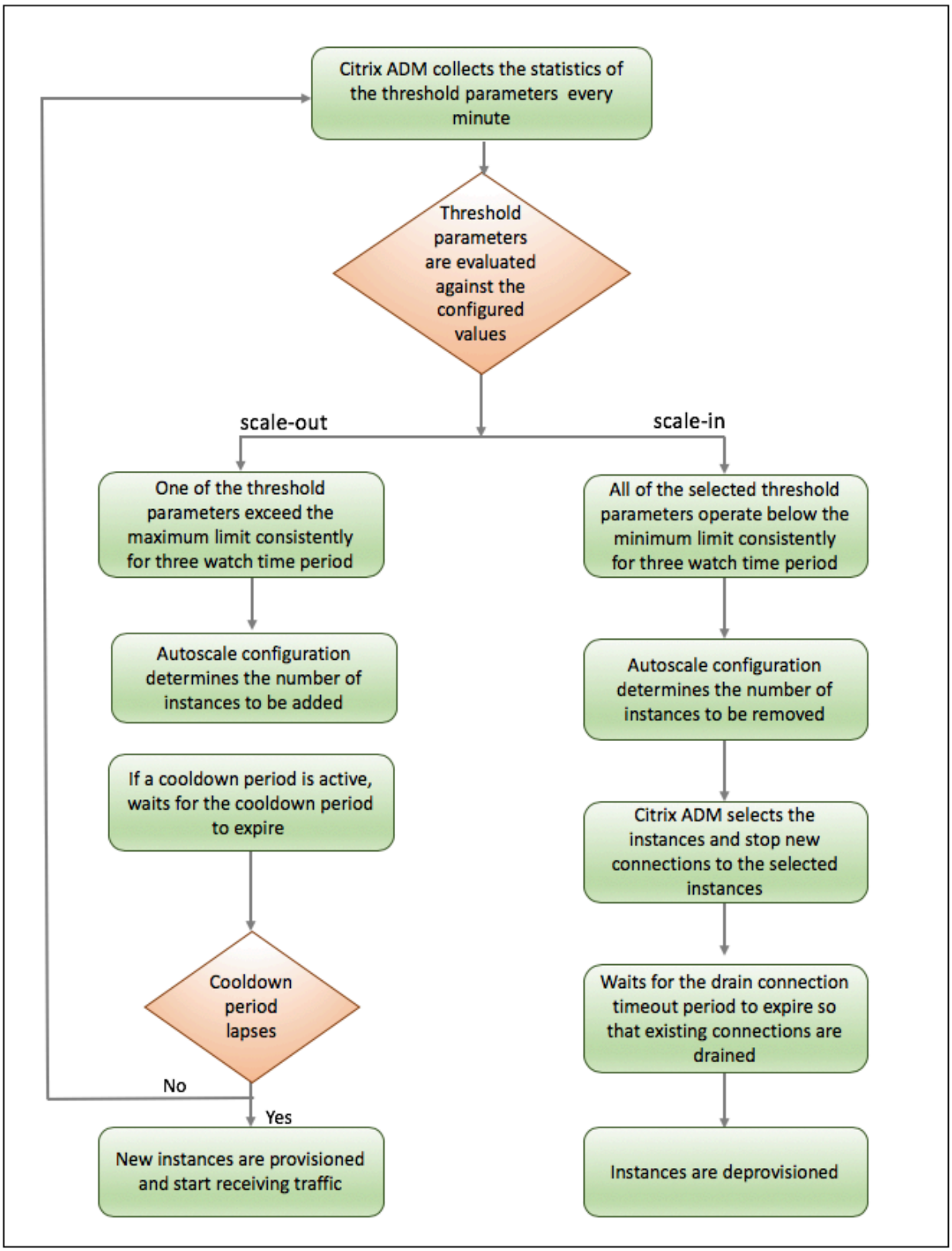
基于 **DNS** 的自动扩展

在基于 DNS 的自动扩展中，DNS 充当 Citrix ADC 群集节点的分布层。通过更新与应用程序对应的域名，扩展更改将传播到客户端。目前，DNS 提供商是 AWS Route53。

> 注意：
>
> 在基于 DNS 的自动扩展中，每个 Citrix ADC 实例都需要一个公有 IP 地址。

自动缩放的工作原理

下面的流程图说明了自动缩放工作流。



Citrix ADM 以一分钟的时间间隔从 AutoScale 预配置的群集中收集统计信息（CPU 使用率、内存使用率、吞吐量）。将根据配置阈值评估统计信息。根据统计数据是超过最大阈值还是低于最小阈值，分别触发向外扩展或向外扩展。

- 如果触发了横向扩展;
  - 已置备新节点。
  - 节点附加到群集，并且配置从群集同步到新节点。
  - 这些节点已向 Citrix ADM 注册。
  - 在 DNS/NLB 中更新新的节点 IP 地址。

部署应用程序时，`IPset` 将在每个可用区域的群集上创建，域和实例 IP 地址将在 DNS/NLB 中注册。

- 如果触发了缩放;
  - 将删除标识为删除的节点的 IP 地址。
  - 节点将与群集分离、取消置备，然后从 Citrix ADM 取消注册。

删除应用程序后，域和实例 IP 地址将从 DNS/NLB 中取消注册并删除 `IPset`。

示例

假设您已在具有以下配置的单个可用性区域中创建名为 asg_arn 的 Autoscale 组。

- 阈值参数 — 内存使用情况
- 最小限制：40
- 最大限制：85
- 观看时间 — 3 分钟
- 冷却时间 — 10 分钟
- 耗尽连接超时 — 10 分钟
- TTL 超时 — 60 秒

创建 AutoScale 组后，将从该组中收集统计信息。AutoScale 策略还会评估是否有任何 AutoScale 事件正在进行中，如果自动伸缩正在进行中，则在收集统计信息之前等待该事件完成。

ASG ID	Availability zone	Cluster IP address	CPU usage	Throughput	Memory usage	Timestamp
asg_arn	eu-west-2	192.0.2.250	55	65	92	T1
asg_arn	eu-west-2	192.0.2.250	60	50	90	T2
asg_arn	eu-west-2	192.0.2.250	59	45	80	T3
asg_arn	eu-west-2	192.0.2.250	49	75	90	T4
asg_arn	eu-west-2	192.0.2.250	63	70	93	T5
asg_arn	eu-west-2	192.0.2.250	65	80	92	T6
asg_arn	eu-west-2	192.0.2.250	65	85	75	T7
asg_arn	eu-west-2	192.0.2.250	35	70	70	.....
asg_arn	eu-west-2	192.0.2.250	55	70	70	T16
asg_arn	eu-west-2	192.0.2.250	58	55	45	T17
asg_arn	eu-west-2	192.0.2.250	59	65	30	T18
asg_arn	eu-west-2	192.0.2.250	75	45	30	T19
asg_arn	eu-west-2	192.0.2.250	46	64	25	T20
asg_arn	eu-west-2	192.0.2.250	64	65	50	T31
asg_arn	eu-west-2	192.0.2.250	64	65	60	T32
asg_arn	eu-west-2	192.0.2.250	64	65	60	T33

Scale-out event is triggered. Nodes are provisioned.

Evaluation of statistics is skipped for this availability zone from T7 –T16 as the cooldown period is in effect.

Scale-in event is triggered. Drain connection timeout in effect.

事件序列：

- T1 和 T2：内存使用量超过最大阈值限制。
- T3-内存使用率低于最大阈值限制。
- T6、T5、T4：内存使用率连续超过三个监视时间持续时间的最大阈值限制。
  - 触发向外扩展。
  - 发生节点置备。
  - 冷却时间有效。
- T7 — T16：由于冷却期已生效，此可用区域从 T7 到 T16 跳过自动缩放评估。
- T18、T19、T20-内存使用率连续超过三个监视时间持续时间的最小阈值限制。
  - 触发缩放。
  - 漏极连接超时有效。
  - IP 地址从 DNS/NLB 中解除。
- T21 — T30：由于漏极连接超时生效，此可用区域从 T21 到 T30 跳过自动缩放评估。
- T31
  - 对于基于 DNS 的自动缩放，TTL 生效。

  - 对于基于 NLB 的自动缩放，会取消配置实例。
- T32
  - 对于基于 NLB 的自动缩放，开始评估统计信息。
  - 对于基于 DNS 的自动扩展，会取消预配实例。
- T33：对于基于 DNS 的自动缩放，开始评估统计信息。

AutoScale 配置

April 23, 2021

要在 AWS 中开始自动扩展 Citrix ADC VPX 实例，您必须完成以下步骤：

1. 完成 AWS 上的所有先决条件
2. 完成 Citrix ADM 上的所有先决条件
3. 创建自动缩放组
   a) 初始化自动扩展配置
   b) 配置自动缩放参数
   c) 配置置备参数
4. 部署应用程序

AWS 的前提条件

确保完成 AWS 上的所有先决条件以使用自动缩放功能。本文档假定您已拥有 AWS 账户。

以下几个部分将帮助您在 Citrix ADM 中创建自动扩展组之前在 AWS 中执行所有必要任务。您必须完成的任务如下所示：

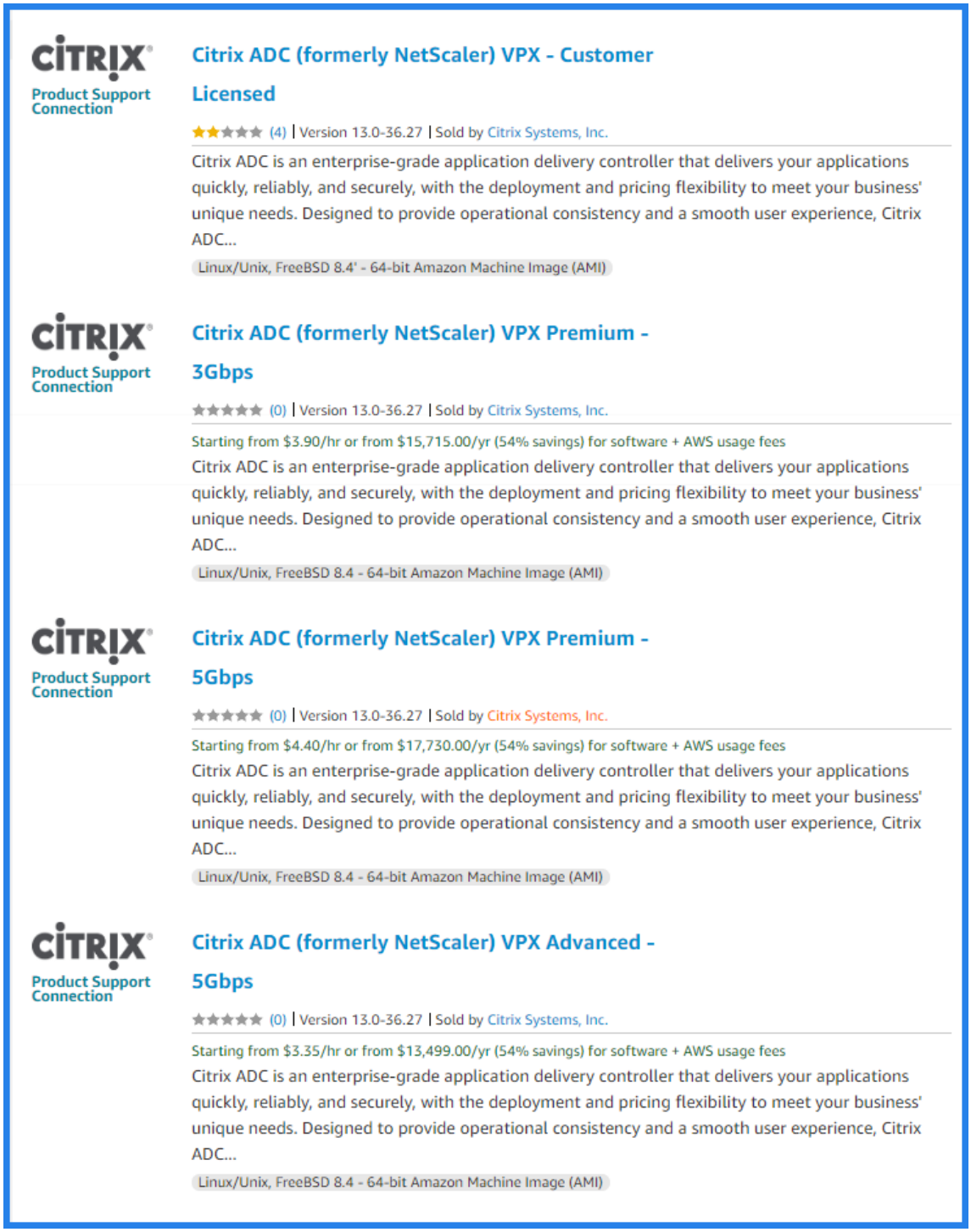
1. 订阅 AWS 上所需的 Citrix ADC VPX 实例。

2. 创建所需的虚拟私有云 (VPC) 或选择现有 VPC。
3. 定义相应的子网和安全组。
4. 创建两个身份访问管理 (IAM) 角色，一个用于 Citrix ADM，一个用于 Citrix ADC VPX 实例。
5. 为 Citrix ADM 创建用户，并将为 Citrix ADM 创建的角色分配给该用户。
6. 为用户生成访问密钥 ID 和安全访问密钥。

有关如何创建 VPC、子网和安全组的更多信息，请参阅 AWS 文档。

在 **AWS** 中订阅 **Citrix ADC VPX** 许可证

1. 转到 AWS Marketplace。
2. 使用您的凭据登录。
3. 搜索 Citrix ADC VPX 客户授权、高级版或高级版。



4. 订阅 Citrix ADC VPX 客户许可、高级版或高级版许可证。

> 注意：
>
> 如果选择客户许可版本，则自动扩展组在 Provisioning Citrix ADC 实例时会从 Citrix ADM 中签出许可证。

创建子网

在 VPC 中创建三个子网-每个子网用于管理、客户端和服务器连接。在 VPC 中为每个子网定义的范围内指定 IPv4 CIDR 块。指定希望子网驻留的可用区。在存在服务器的每个可用区中创建所有三个子网。

- 管理. 虚拟私有云 (VPC) 中专门用于管理的现有子网。Citrix ADC 联系需要互联网访问的 AWS 服务。配置 NAT Gateway 并添加路由表条目以允许从此子网访问 Internet。
- 客户端。虚拟私有云 (VPC) 中专用于客户端的现有子网。通常情况下，Citrix ADC 从互联网通过公有子网接收应用程序的客户端流量。将客户端子网与具有通往 Internet Gateway 的路由表相关联。此子网允许 Citrix ADC 接收来自互联网的应用程序流量。
- 服务器。预配应用程序服务器的服务器子网。您的所有应用程序服务器都位于此子网中，并通过此子网接收来自 Citrix ADC 的应用程序流量。

创建安全组

创建安全组以控制 Citrix ADC VPX 实例中的入站和出站流量。为要在 Citrix 自动缩放组中控制的传入和传出流量创建规则。您可以根据需要添加多个规则。

- 管理. 您帐户中专门用于管理 Citrix ADC VPX 的现有安全组。必须允许在以下 TCP 和 UDP 端口上使用入站规则。
  - TCP：80、22、443、3008–3011、4001
  - UDP：67、123、161、500、3003、4500、7000

  确保安全组允许 Citrix ADM 代理访问 VPX。
- 客户端。您帐户中专门用于 Citrix ADC VPX 实例的客户端通信的现有安全组。通常，TCP 端口 80、22 和 443 上允许入站规则。
- 服务器。您帐户中的现有安全组专用于 Citrix ADC VPX 的服务器端通信。

创建 **IAM** 角色

除了创建 IAM 角色和定义策略外，您还必须在 AWS 中创建实例配置文件。IAM 角色允许 Citrix ADM 配置 Citrix ADC 实例、创建或删除 Route53 条目。

虽然角色定义了“我可以做什么？“他们没有定义“我是谁？“ AWS EC2 使用实例配置文件作为 IAM 角色的容器。实例配置文件是 IAM 角色的容器。您可以使用此配置文件在实例启动时将角色信息传递给 EC2 实例。

当您使用控制台创建 IAM 角色时，控制台会自动创建与其对应角色同名的实例配置文件。角色提供了一种定义权限集合的机制。IAM 用户代表一个人，实例配置文件代表 EC2 实例。如果用户具有角色“A”，并且实例附加到“A”的实例配置文件，则这两个委托人可以以相同的方式访问相同的资源。

> 注意：
>
> 确保角色名称以“Citrix-ADM-”开头，实例配置文件名称以“Citrix-ADC-开头。“

为 **Citrix ADM** 创建 **IAM** 角色的步骤

创建 IAM 角色，以便您可以在用户和 Citrix 受信任的 AWS 账户之间建立信任关系。然后，创建具有 Citrix 权限的策略。

1. 在 **AWS** 中，单击 “ 服务”。在左侧导航窗格中，选择 **IAM >** 角色，然后单击 创建角色。
2. 您正在将您的 AWS 账户与 Citrix ADM 中的 AWS 账户连接起来。因此，请选择 其他 **AWS** 账户以允许 Citrix ADM 在您的 AWS 账户中执行操作。
3. 键入 12 位 Citrix ADM AWS 账户 ID。Citrix ID 为 835822366011。创建云访问配置文件时，还可以在 Citrix ADM 中找到 Citrix ID。
4. 单击权限。
5. 在 附加权限策略页中，单击 创建策略。
6. 您可以在可视化编辑器中或使用 JSON 创建和编辑策略。

   以下框中提供了 Citrix 对 Citrix ADM 的权限列表：

```
JSON
{

"Version": "2012-10-17",
"Statement": [
  {

    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:UnmonitorInstances",
      "ec2:MonitorInstances",
      "ec2:CreateKeyPair",
      "ec2:ResetInstanceAttribute",
      "ec2:ReportInstanceStatus",
      "ec2:DescribeVolumeStatus",
      "ec2:StartInstances",
      "ec2:DescribeVolumes",
      "ec2:UnassignPrivateIpAddresses",
      "ec2:DescribeKeyPairs",
      "ec2:CreateTags",
      "ec2:ResetNetworkInterfaceAttribute",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DeleteNetworkInterface",
      "ec2:RunInstances",
      "ec2:StopInstances",
      "ec2:AssignPrivateIpAddresses",
      "ec2:DescribeVolumeAttribute",
```



```
30          "ec2:DescribeInstanceCreditSpecifications",
31          "ec2:CreateNetworkInterface",
32          "ec2:DescribeImageAttribute",
33          "ec2:AssociateAddress",
34          "ec2:DescribeSubnets",
35          "ec2:DeleteKeyPair",
36          "ec2:DisassociateAddress",
37          "ec2:DescribeAddresses",
38          "ec2:DeleteTags",
39          "ec2:RunScheduledInstances",
40          "ec2:DescribeInstanceAttribute",
41          "ec2:DescribeRegions",
42          "ec2:DescribeDhcpOptions",
43          "ec2:GetConsoleOutput",
44          "ec2:DescribeNetworkInterfaces",
45          "ec2:DescribeAvailabilityZones",
46          "ec2:DescribeNetworkInterfaceAttribute",
47          "ec2:ModifyInstanceAttribute",
48          "ec2:DescribeInstanceStatus",
49          "ec2:ReleaseAddress",
50          "ec2:RebootInstances",
51          "ec2:TerminateInstances",
52          "ec2:DetachNetworkInterface",
53          "ec2:DescribeIamInstanceProfileAssociations",
54          "ec2:DescribeTags",
55          "ec2:AllocateAddress",
56          "ec2:DescribeSecurityGroups",
57          "ec2:DescribeHosts",
58          "ec2:DescribeImages",
59          "ec2:DescribeVpcs",
60          "ec2:AttachNetworkInterface",
61          "ec2:AssociateIamInstanceProfile"
62        ],
63        "Resource": "\*"
64      }
65    ,
66     {
67
68        "Sid": "VisualEditor1",
69        "Effect": "Allow",
70        "Action": [
71          "iam:GetRole",
72          "iam:PassRole"
73        ],
74        "Resource": "\*"
```



```
75      }
76    ,
77     {
78
79       "Sid": "VisualEditor2",
80       "Effect": "Allow",
81       "Action": [
82         "route53:CreateHostedZone",
83         "route53:CreateHealthCheck",
84         "route53:GetHostedZone",
85         "route53:ChangeResourceRecordSets",
86         "route53:ChangeTagsForResource",
87         "route53:DeleteHostedZone",
88         "route53:DeleteHealthCheck",
89         "route53:ListHostedZonesByName",
90         "route53:GetHealthCheckCount"
91       ],
92       "Resource": "\*"
93      }
94    ,
95     {
96
97       "Sid": "VisualEditor3",
98       "Effect": "Allow",
99       "Action": [
100        "iam:ListInstanceProfiles",
101        "iam:ListAttachedRolePolicies",
102        "iam:SimulatePrincipalPolicy"
103      ],
104      "Resource": "\*"
105     }
106   ,
107    {
108
109      "Sid": "VisualEditor4",
110      "Effect": "Allow",
111      "Action": [
112        "ec2:ReleaseAddress",
113        "elasticloadbalancing:DeleteLoadBalancer",
114        "ec2:DescribeAddresses",
115        "elasticloadbalancing:CreateListener",
116        "elasticloadbalancing:CreateLoadBalancer",
117        "elasticloadbalancing:RegisterTargets",
118        "elasticloadbalancing:CreateTargetGroup",
119        "elasticloadbalancing:DeregisterTargets",
```



```
        "ec2:DescribeSubnets",
        "elasticloadbalancing:DeleteTargetGroup",
        "elasticloadbalancing:ModifyTargetGroupAttributes",
        "ec2:AllocateAddress"
      ],
      "Resource": "*"
     }

]
 }

 }

<!--NeedCopy-->
```

7. 复制并粘贴 JSON 选项卡中的权限列表，然后单击 查看策略。
8. 在 查看策略页面中，键入策略的名称，输入描述，然后单击 创建策略。

   > 注意
   >
   > 确保名称以“思特里克斯 ADM-开头。“

9. 在 创建角色页面中，输入角色的名称。

   > 注意：
   >
   > 确保角色名称以“Citrix-ADM-开头。“

10. 单击 创建角色。

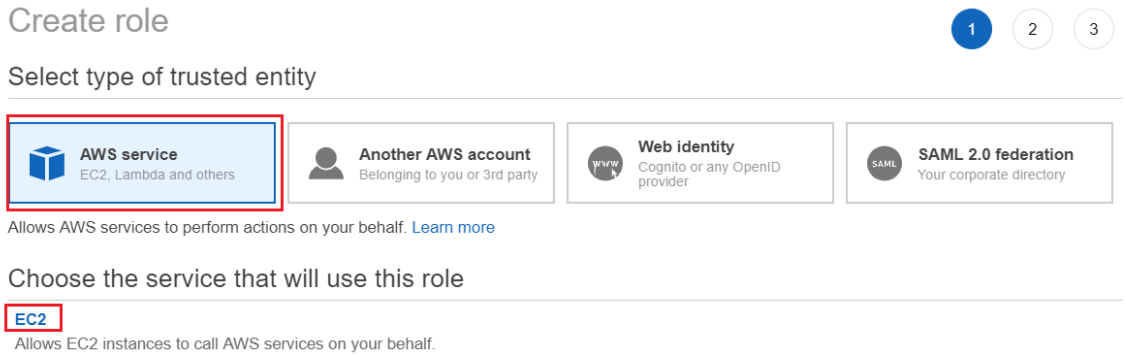
为 **Citrix ADC** 实例创建 **IAM** 角色

同样，为 Citrix ADC 创建 IAM 角色。然后，Citrix ADC 可以登录到您的 AWS 账户并执行以下操作：

- 在节点故障期间重新分配管理 IP 地址
- 监听后端服务器的 AWS 自动缩放事件等。

将策略附加到 Citrix 为 AWS 提供的访问 Citrix ADC 实例的权限。

1. 在 **AWS** 中，单击“ 服务”。在左侧导航窗格中，选择 **IAM** > 角色，然后单击 创建角色。
2. 确保选择 **AWS** 服务 > **EC2**，然后单击“ 权限”以创建实例配置文件。



3. 单击权限。
4. 在 附加权限策略页中，单击 创建策略。
5. 您可以在可视化编辑器中或使用 JSON 创建和编辑策略。

以下框中提供了 Citrix 对 Citrix ADC 实例的权限列表：

```
{

  "Version": "2012-10-17",
  "Statement": [
    {

      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "autoscaling:\*",
        "sns:\*",
        "sqs:\*",
        "cloudwatch:\*",
        "ec2:AssignPrivateIpAddresses",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DetachNetworkInterface",
        "ec2:AttachNetworkInterface",
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*"
    }

  ]
```



```
28   }
29
30 <!--NeedCopy-->
```

注册 **DNS** 域

确保您已注册 DNS 域用于托管应用程序。

评估网络中所需的弹性 IP (EIP) 数量。

所需的 EIP 数量取决于您是部署基于 DNS 的自动扩展还是基于 NLB 的自动扩展。要增加 EIP 数量，请使用 AWS 创建案例。

- 对于基于 DNS 的自动扩展，每个可用区所需的 EIP 数等于应用程序数乘以要在自动扩展组中配置的最大 VPX 实例数。
- 对于基于 NLB 的自动扩展，所需的 EIP 数等于应用程序数乘以部署应用程序的可用区数。

评估实例限制要求

评估实例限制时，请确保您还考虑到 Citrix ADC 实例的空间要求。

在 **AWS** 上安装 **Citrix ADM** 代理

Citrix ADM 代理作为 Citrix ADM 与数据中心或云中发现的实例之间的中介工作。确保您已在 AWS 中安装了 Citrix ADM 代理。在 AWS ADM 代理中添加路由，以便 ADM 在建立第 3 层连接后可以到达代理。

请按照以下步骤在 AWS 中安装的代理中添加路由：

1. 访问 AWS 上安装的 ADM 代理的控制台。
2. 在提示符下运行以下命令：

   路由添加-网络 <DMZ network> <gateway to ADM agent>

例如，“路由添加-净值 10.x.0/24 21.1.1.10”

> 注意：
>
> 在代理重新启动后，路由将被删除。此行为特定于跳过网络设置的 AWS /Azure 代理映像。

有关如何在 AWS 上安装 Citrix ADM 代理的详细信息，请参阅 在 AWS 上安装 Citrix ADM 代理

在 **AWS** 中创建路由表

添加路由表以建立从 Citrix ADC 实例到数据中心上部署的 Citrix ADM 的通信。

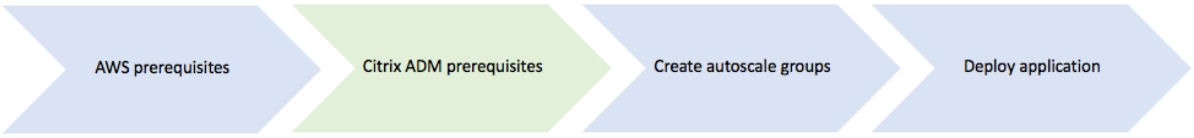
1. 登录 AWS 并导航到 路由表。

2. 在 创建路由表中，指定 **Name** 标记，然后选择要在其中部署 ADC 实例的 VPC。请参阅 创建路由表。
3. 在 子网关联中，将管理子网与部署 ADC 实例的路由表相关联。将子网与路由表关联。
4. 在 “ 路由” 中，选择 “ 编辑路由” 并指定以下详细信息：
    - 目标：指定 Citrix ADM 网络。您可以指定 Citrix ADM IP 地址或 Citrix ADM 子网。
    - 目标：选择 网络接口并指定 Citrix CloudBridge 连接器的子网。

    有关详细信息，请参阅添加路由。

Citrix ADM 的先决条件

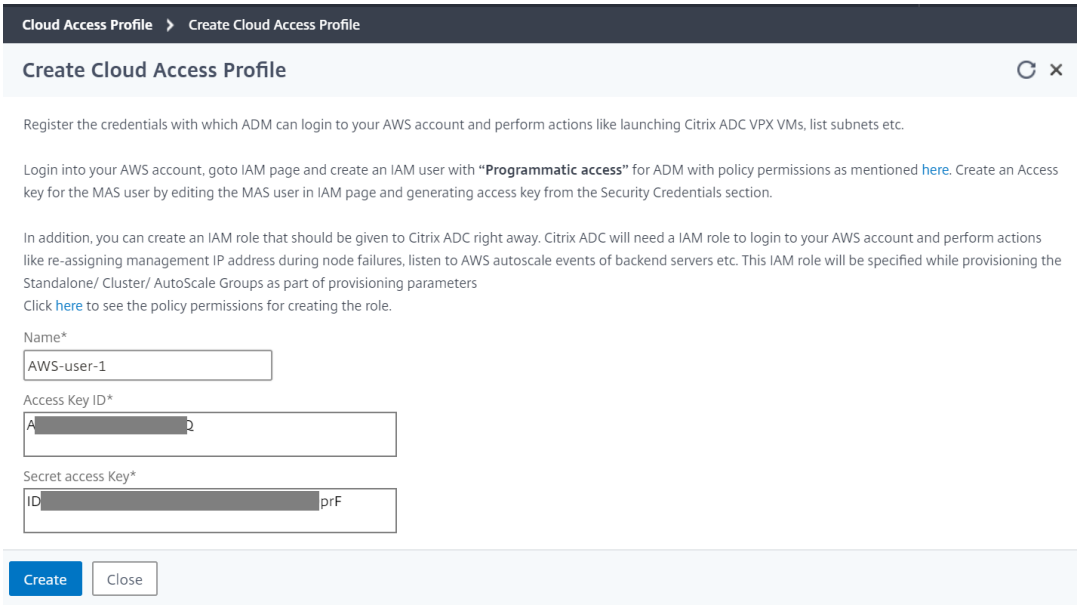
确保您已完成 Citrix ADM 上的所有先决条件，以使用 “自动缩放” 功能。



创建站点

在 Citrix ADM 中创建一个站点，然后添加与您的 AWS 角色关联的 VPC 的详细信息。

1. 在 Citrix ADM 中，导航到 网络 **>** 站点。
2. 单击添加。
3. 选择作为 AWS 的服务类型，然后启 用将现有 **VPC** 用作站点。
4. 选择云访问配置文件。
5. 如果字段中不存在云访问配置文件，请单击 添加以创建配置文件。
    a) 在 创建云访问配置文件页面中，键入要访问 AWS 的配置文件的名称。
    b) 键入与您在 **AWS** 中创建的角色相关联的访问密钥 **ID** 。
    c) 键入在 **AWS** 中为 **Citrix ADM** 创建 **IAM** 角色时生成的私有访问密钥。



与您在 AWS 中的 IAM 角色关联的 VPC 的详细信息（例如区域、VPC ID、名称和 CIDR 块）将导入到 Citrix ADM 中。

d) 单击创建。

6. 再次单击 创建以创建站点。

配置 **NTP** 服务器

确保在 Citrix ADM 上配置 NTP 服务器，以便 Citrix ADM 时钟的日期和时间设置与 AWS 上部署的 Citrix ADC 具有相同的日期和时间设置。
有关如何配置 NTP 服务器的详细信息，请参阅配置 NTP 服务器。

配置域名服务器

Citrix ADM 需要互联网连接才能连接到 AWS 上部署的 ADC 实例。在 ADM 上配置 DNS IP 地址以允许互联网连接。

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 设置 **Citrix ADM**”，然后选择 “ 网络配置”。
2. 在 网络配置页面中，输入网络中配置的 DNS 的 IP 地址。
3. 单击确定。

配置第 **3** 层连接

在 Citrix ADM 和部署在公有云上的 ADC VPX 实例之间建立第 3 层连接。要建立第 3 层连接，您可以使用 Citrix CloudBridge 连接器、Citrix SD-WAN、直接连接到 AWS、Azure 中的 VPN 或第三方连接器（如 Equinix）等解决方案。

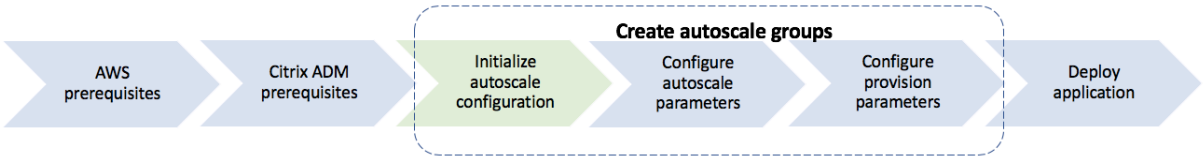
有关如何创建第 3 层连接的详细信息，请参阅 将部署在云中的 VPX 实例添加到 Citrix ADM。

在 **AWS** 上安装 **Citrix ADM** 代理

Citrix ADM 代理作为 Citrix ADM 与数据中心或云中发现的实例之间的中介工作。
有关在 AWS 上安装 Citrix ADM 代理的详细信息，请参阅 在 AWS 上安装 Citrix ADM 代理。

创建自动缩放组

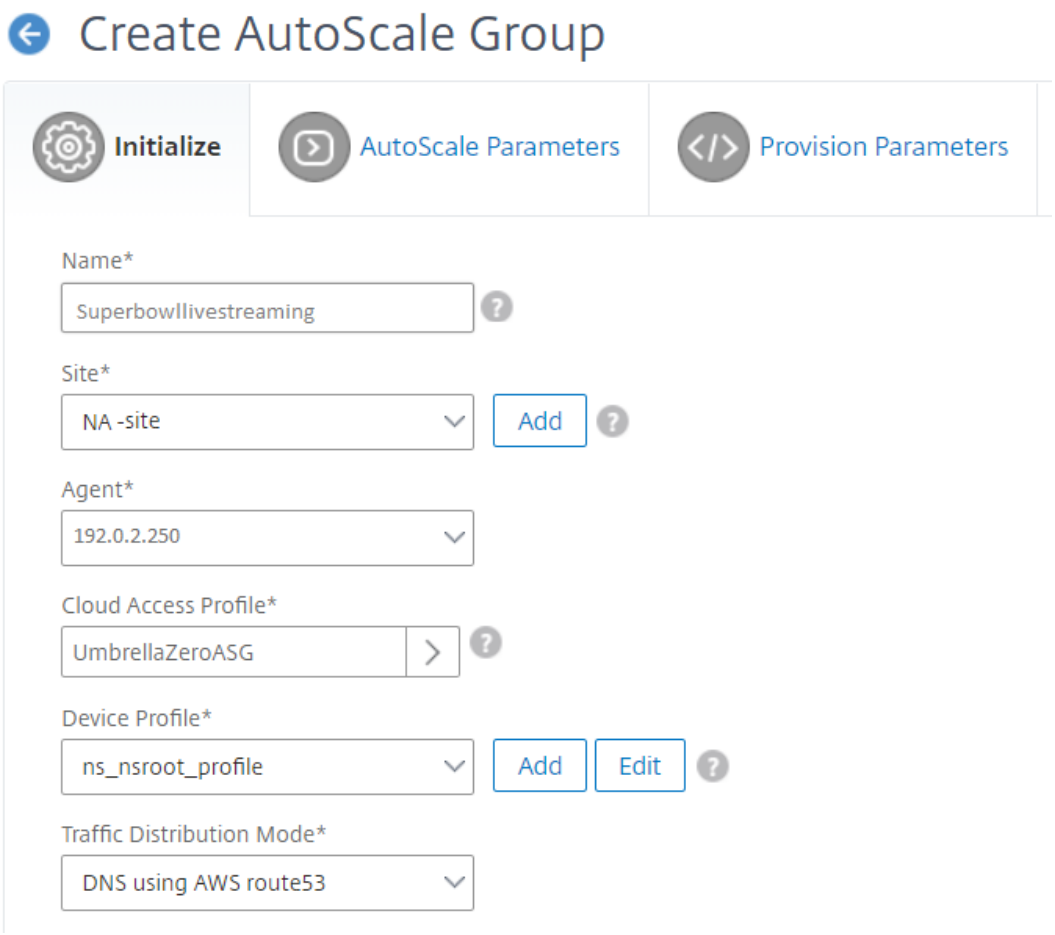
初始化自动扩展配置



1. 在 Citrix ADM 中，导航到 网络 **> AutoScale** 组。
2. 单击 添加以创建自动缩放组。此时将显示 创建 **AutoScale** 组页面。
3. 输入以下详细信息。
   - 名称。键入自动缩放组的名称。
   - 站点。选择您为在 AWS 上配置 Citrix ADC VPX 实例而创建的站点。
   - 代理选择用于管理预配置实例的 Citrix ADM 代理。
   - 云访问配置文件。选择云访问配置文件。

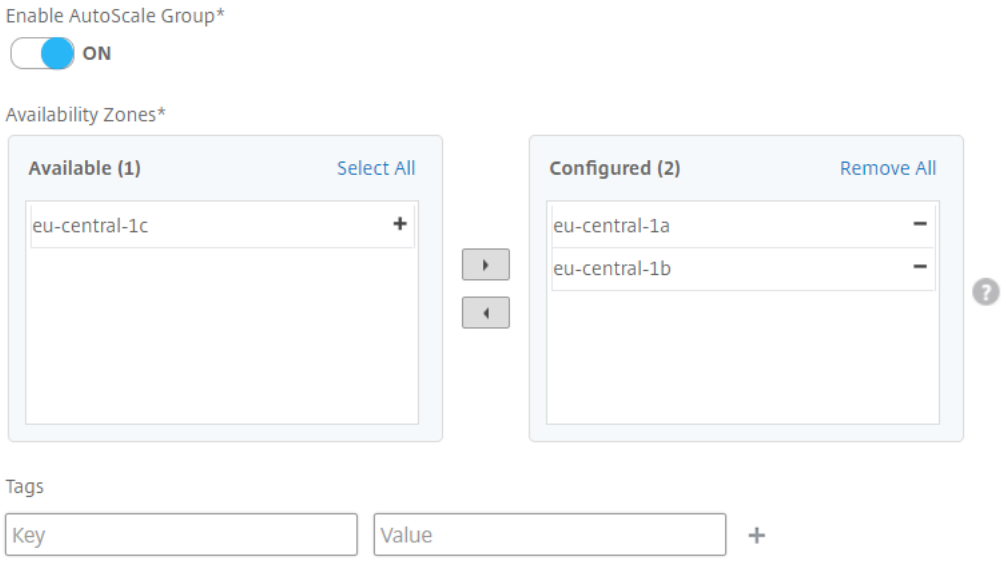
   > 注意：
   >
   > 如果字段中不存在云访问配置文件，请单击 添加以创建配置文件。
   >
   > - 键入与您在 AWS 中创建的角色相关联的 ARN。
   > - 键入您在 AWS 中创建身份和访问管理 (IAM) 角色时提供的外部 ID。根据您选择的云访问配置文件，将填充可用区。

   - 设备配置文件。从列表中选择设备配置文件。无论何时 ADM 必须登录实例，Citrix ADM 都会使用此设备配置文件。
   - 流量分配模式。使用 **NLB** 进行负载平衡选项被选为默认流量分配模式。如果应用程序正在使用 UDP 流量，则 使用 **AWS route53** 选择 **DNS**。



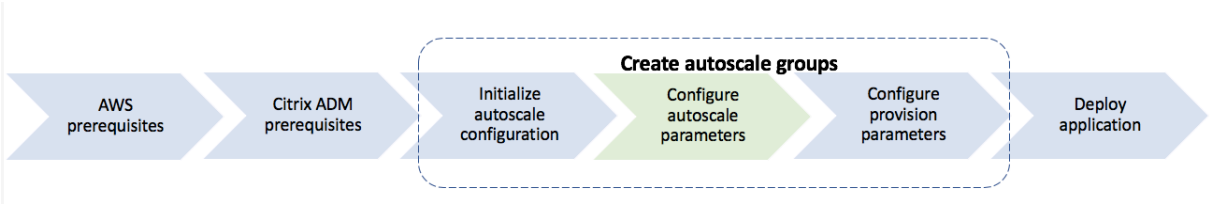
> 注意设置自动缩放配置
>
> 后，无法添加新的可用区或者无法删除现有可用区。

- 启用自动缩放组。启用或禁用 ASG 组的状态。默认情况下，此选项处于启用状态。如果禁用此选项，则不会触发自动缩放。
- 可用区域。选择要在其中创建自动缩放组的区域。根据您选择的云访问配置文件，会填充特定于该配置文件的可用区。
- 标签。键入自动缩放组标记的键值对。标签由区分大小写的键值对组成。这些标签使您能够轻松地组织和识别自动缩放组。这些标签同时应用于 AWS 和 Citrix ADM。



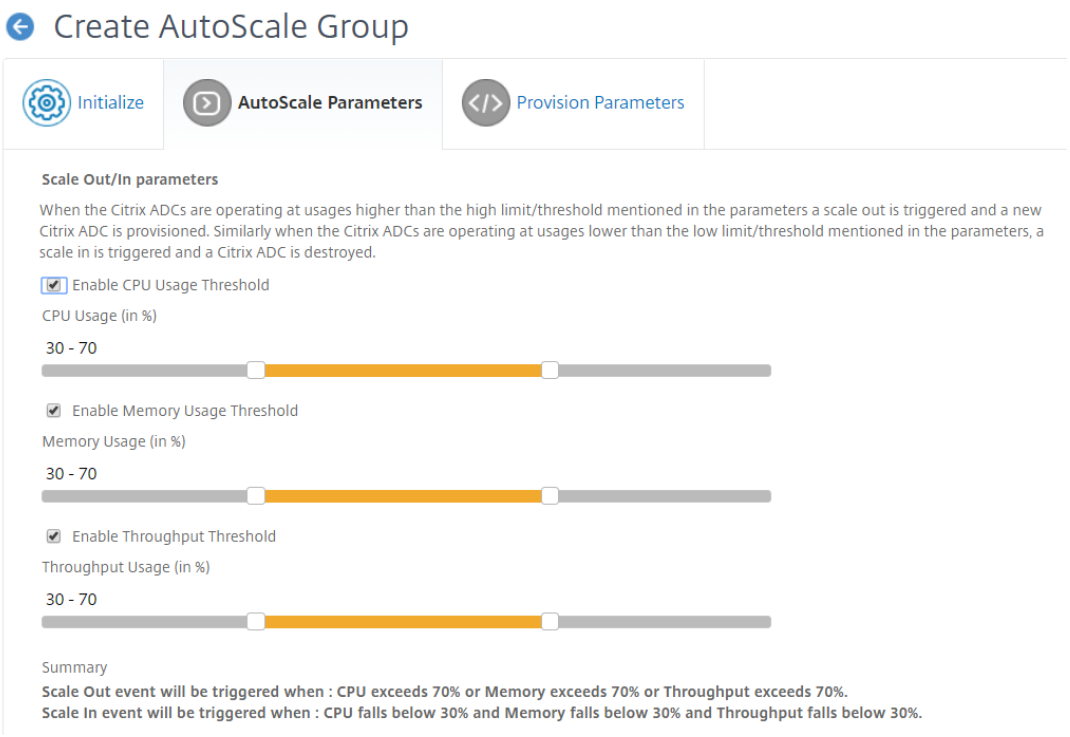
4. 单击下一步。

配置自动缩放参数

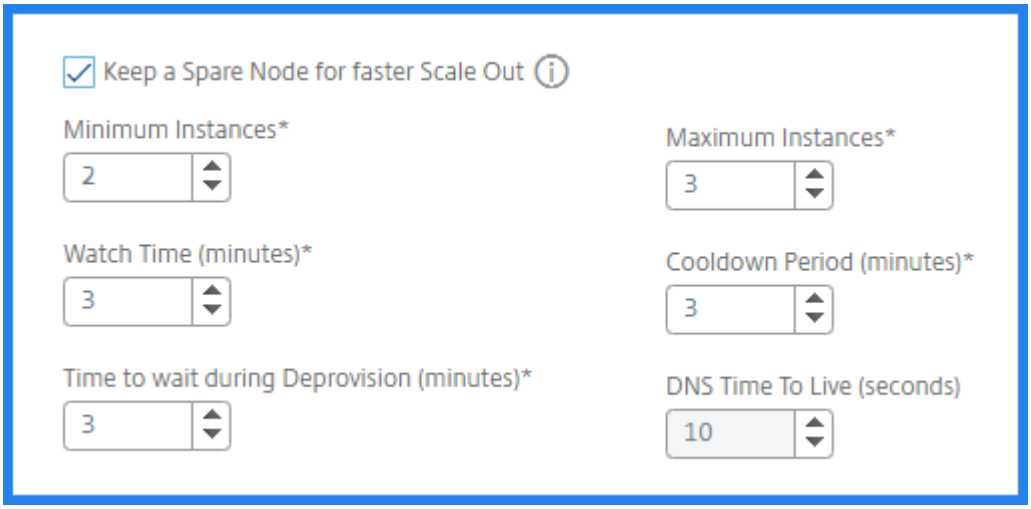


1. 在 自动缩放参数选项卡中，输入以下详细信息。
2. 选择以下一个或多个阈值参数，必须监视其值才能触发向外扩展或扩展。
   - 启用 **CPU** 使用率阈值：根据 CPU 使用率监控指标。
   - 启用内存使用阈值：根据内存使用情况监控指标。
   - 启用吞吐量阈值：根据吞吐量监控指标。

     注意
     - 默认最小阈值限制为 30，最大阈值限制为 70。但是，您更改修改限制。
     - 最小阈值限制必须等于或小于最大阈值限制的一半。
     - 可以选择多个阈值参数进行监视。在这种情况下，如果至少有一个阈值参数高于最大阈值，则会触发缩放。但是，只有当所有阈值参数都低于其正常阈值时，才会触发放入。



- 保留备用节点以加快向外扩展：此选项有助于实现更快的横向扩展。ADM 将备用节点置于非活动状态。当 ADM 触发横向扩展操作时，备用节点会立即变为活动状态。因此，它可以在横向扩展期间保存节点配置时间节点。
- 最小实例。选择必须为此自动扩展组预配置的最小实例数。
- 默认情况下，实例的最小数量等于选定的区域数。您可以按区域数的倍数增加最小实例。
- 例如，如果可用区数为 4，则默认情况下最小实例为 4。您可以将最小实例增加 8、12、16。
- 最大实例数。选择必须为此自动扩展组预配置的最大实例数。
- 最大实例数必须大于或等于最小实例值。可配置的最大实例数等于可用区数乘以 32 个。
- 最大实例数 = 可用区数 x 32
- 耗尽连接超时（分钟）。选择漏极连接超时周期。在扩展期间，一旦选择了要取消置备的实例，Citrix ADM 将从处理到 AutoScale 组的新连接中删除该实例，并等到指定的时间过期后才取消置备。此选项允许在取消置备前将与此实例的现有连接耗尽。
- 冷却时间（分钟）。选择冷却时间。在横向扩展期间，冷却时间是指在向外扩展发生后必须停止统计数据评估的时间。在作出下一个扩展决策之前，允许当前流量在当前实例集上稳定和平均值，从而确保 AutoScale 组的实例有机增长。
- **DNS** 生存时间（秒）。选择数据包在被路由器丢弃之前设置为网络内存在的时间（以秒为单位）。仅当流量分配模式为使用 AWS route53 的 DNS 时，此参数才适用。
- 观看时间（分钟）。选择监视时间持续时间。缩放参数的阈值必须保持超出以便进行缩放的时间。如果在此指定时间内收集的所有样本上超过阈值，则会进行缩放。



3. 单击下一步。

Provisioning 用于置备 **Citrix ADC** 实例的许可证

选择以下模式之一以许可属于 AutoScale 组的 Citrix ADC 实例：

- 使用 **Citrix ADM**：在 Provisioning Citrix ADC 实例时，自动扩展组会从 Citrix ADM 中签出许可证。
- 使用 **AWS** 云：从云分配选项使用 AWS 市场中提供的 Citrix 产品许可证。在 Provisioning Citrix ADC 实例时，自动扩展组使用市场中的许可证。

  如果您选择使用 AWS 市场的许可证，请在 云参数选项卡中指定产品或许可证。

有关详细信息，请参阅许可要求。

使用来自 **Citrix ADM** 的许可证

1. 在 许可证选项卡中，选择 从 **ADM** 分配。
2. 在 许可证类型”中，从列表中选择以下选项之一：
   - 带宽许可证：您可以从“带 宽许可证类型”列表中选择以下选项之一：
     - 池容量：指定要为自动扩展组中每个新实例分配的容量。

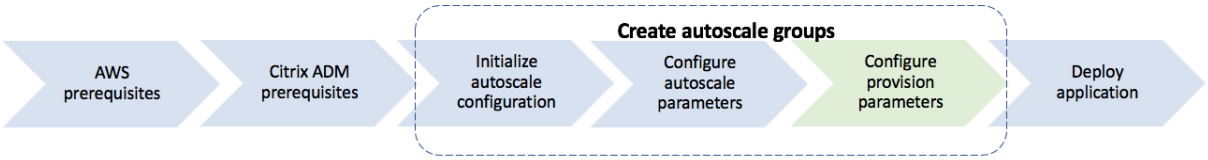
       在公共池中，Autoscale 组中的每个 ADC 实例签出一个实例许可证，并且只指定多大带宽。
     - **VPX** 许可证：预配 Citrix ADC VPX 实例时，实例将从 Citrix ADM 中签出许可证。
   - 虚拟 **CPU** 许可证：预配置的 Citrix ADC VPX 实例会根据自动扩展组中运行的活动 CPU 的数量签出许可证。

   > 注意：

> 删除或销毁预配置的实例后，应用的许可证将返回到 Citrix ADM 许可证池。在下一次 AutoScale 期间，这些许可证可以重复用于预配新实例。

3. 在 许可证版本中，选择许可证版本。自动扩展组使用指定版本来置备实例。
4. 单击下一步。

配置云参数



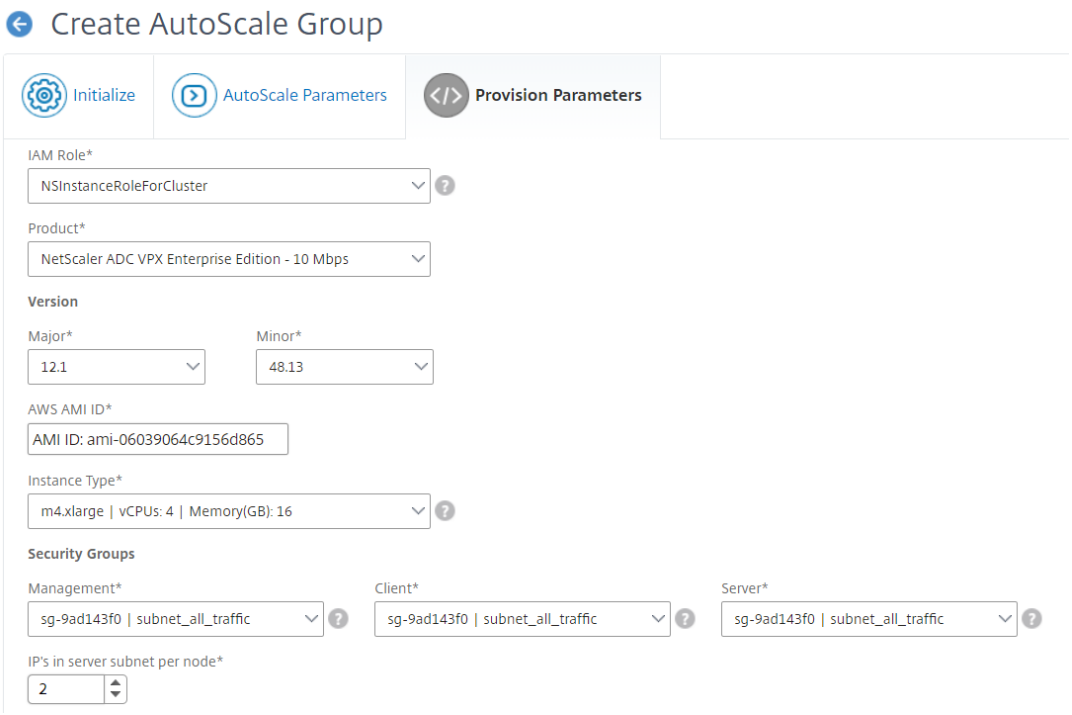
1. 在 “ 预配参数” 标签中，输入以下详细信息。
   - **IAM** 角色：选择您在 AWS 中创建的 IAM 角色。IAM 角色是一种 AWS 身份，其权限策略可确定身份在 AWS 中可以执行和不能执行的操作。
   - 产品：选择要置备的 Citrix ADC 产品版本。
   - 版本：选择 Citrix ADC 产品发行版本和内部版本号。发行版本和内部版本号将根据您选择的产品自动填充。
   - **AWS AMI ID**：输入特定于您所选区域的 AMI ID。
   - 实例类型：选择 EC2 实例类型。

     > 注意：
     >
     > 默认情况下，所选产品的推荐实例类型是自动填充的。

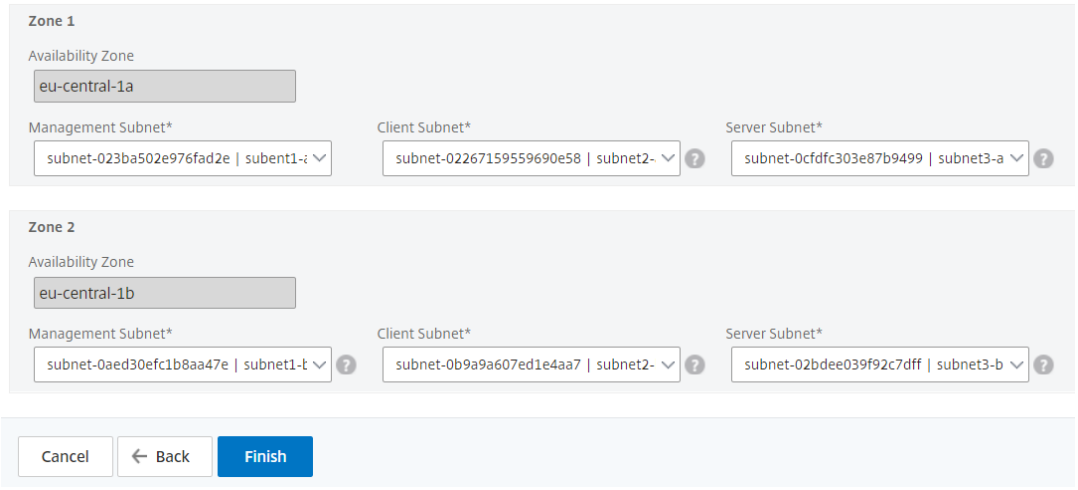
   - 安全组：安全组控制 Citrix ADC VPX 实例中的入站和出站流量。您可以为要控制的传入和传出流量创建规则。为以下子网选择适当的值：
   - 管理. 账户中专门用于管理 Citrix ADC VPX 实例的现有安全组。允许在以下 TCP 和 UDP 端口上使用入站规则。

     技术合作
     伙务：第六十七届、第二十二届、第四十三届、第四十三届、第四十三届、第六十一届、第五十三届、第五十三届、第四十五届、第四十五届、第二十三届、第四十五届、第四十五

     确保安全组允许 Citrix ADM 代理访问 VPX。
   - 客户端。您帐户中专门用于 Citrix ADC VPX 实例的客户端通信的现有安全组。通常，TCP 端口 80、22 和 443 上允许入站规则。
   - 服务器。您的帐户中的现有安全组专用于 Citrix ADC VPX 的服务器端通信。
   - 每个节点的服务器子网中的 IP：为安全组选择服务器子网中每个节点的 IP 地址数。

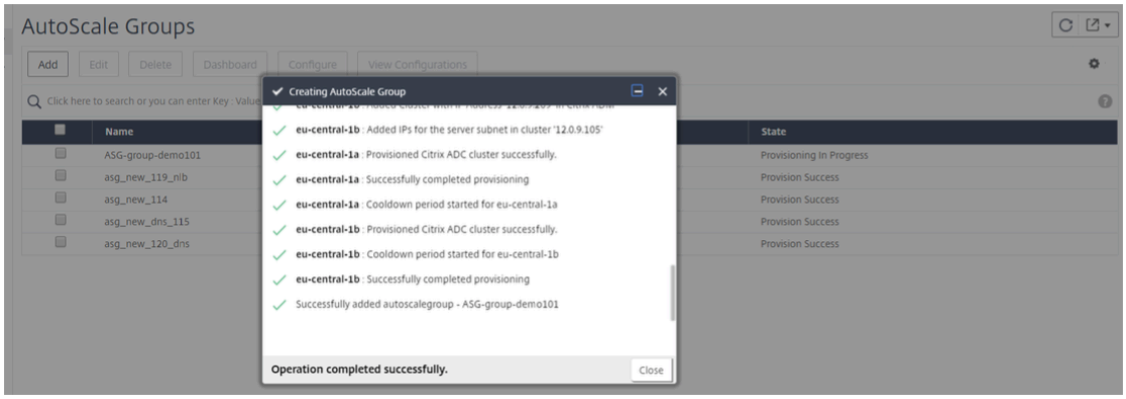


- 区域：填充的区域数等于您选择的可用区域数。对于每个区域，为以下子网选择适当的值：
- 管理. 虚拟私有云 (VPC) 中专门用于管理的现有子网。Citrix ADC 联系 AWS 服务，需要互联网访问。配置 NAT Gateway 并添加路由表条目以允许从此子网访问 Internet。
- 客户端。虚拟私有云 (VPC) 中专用于客户端的现有子网。通常情况下，Citrix ADC 从互联网通过公有子网接收应用程序的客户端流量。将客户端子网与具有通往 Internet Gateway 的路由表相关联。此子网允许 Citrix ADC 接收来自互联网的应用程序流量。
- 服务器。应用程序服务器在服务器子网中置备。您的所有应用程序服务器都位于此子网中，并通过此子网接收来自 Citrix ADC 的应用程序流量。



2. 单击完成。

此时将显示一个进度窗口，其中包含创建自动缩放组的状态。创建和配置 AutoScale 组可能需要几分钟的时间。



使用样书配置应用程序

1. 在 Citrix ADM 中，导航到 网络 > 自动缩放组。
2. 选择您创建的自动缩放组，然后单击 配置。
3. 在 配置应用程序中，指定以下详细信息：
   - 应用程序名称 -指定应用程序的名称。
   - 访问类型 -您可以将 ADM 自动扩缩解决方案用于外部和内部应用程序。选择所需的应用程序访问类型。
   - **FQDN** 类型 -选择分配域名和区域名称的模式。

     如果要手动指定，请选择 用户定义。要自动分配域名和区域名称，请选择 自动生成。
   - 域名 -指定应用程序的域名。仅当您选择用户定义的 FQDN 类型时，此选项才适用。
   - 域的区域 -从列表中选择应用程序的区域名称。仅当您选择用户定义的 FQDN 类型时，此选项才适用。

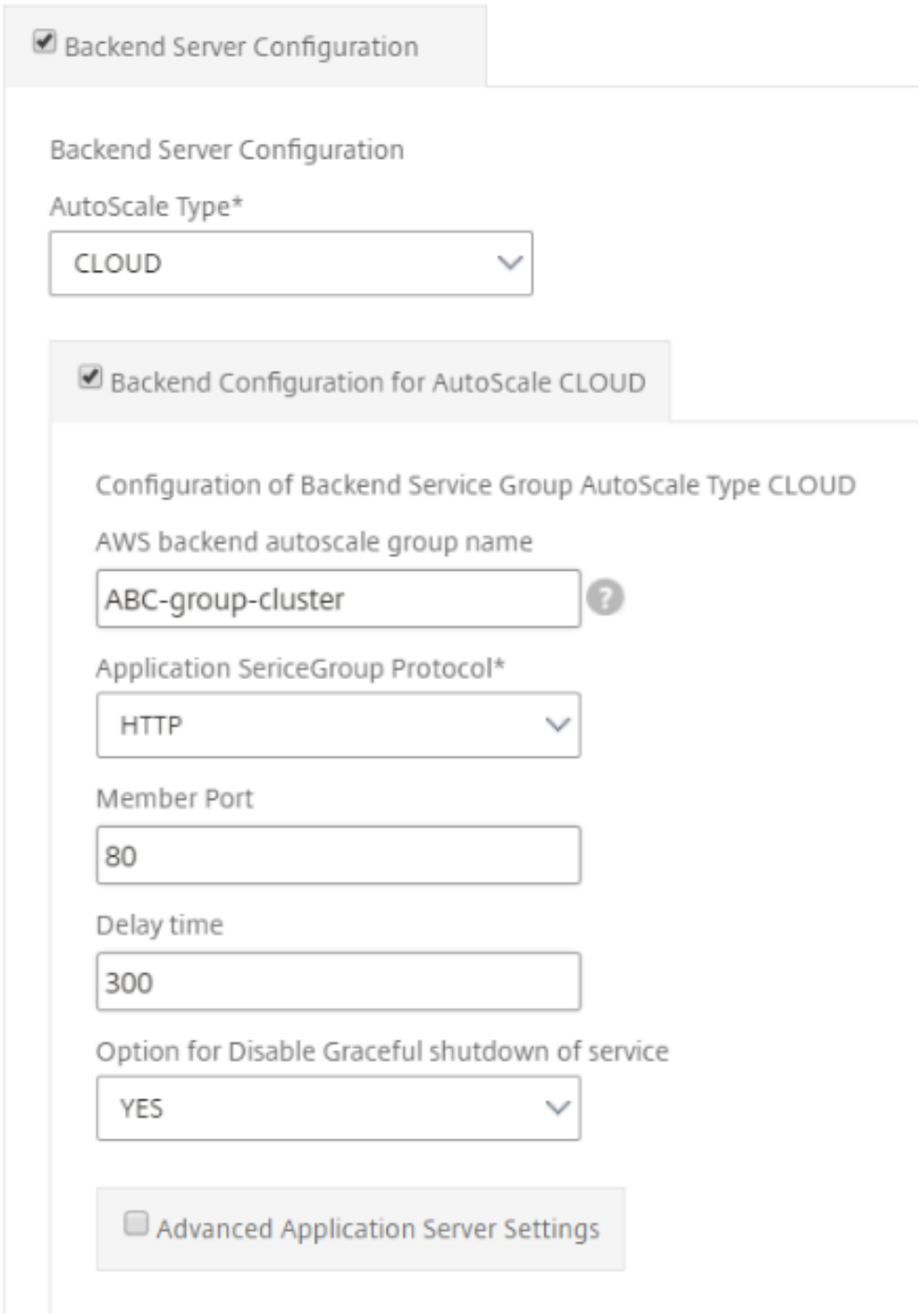
     此域名和区域名称将重定向到 AWS 中的虚拟服务器。例如，如果您在中托管应用程序 `app.example.com`，则 `app` 为域名和 `example.com` 区域名称。
   - 协议 -从列表中选择协议类型。配置的应用程序根据所选协议类型接收流量。
   - 端口 -指定端口值。指定的端口用于在应用程序和 AutoScale 组之间建立通信。

如果要使用样书配置应用程序，请在确认窗口中选择 是。

> 注意
>
> ：如果将来要修改以下详细信息，请更改应用程序的访问类型：

> - FQDN 类型
> - 域名
> - 域名的区域

4. “选择样书”页面显示了可用于在 AutoScale 集群中部署配置的所有样书。
   - 选择相应的样本。例如，您可以使用 **HTTP/SSL** 负载平衡样书。您还可以导入新的样本。
   - 单击样书以创建所需的配置。
     样本将以用户界面页面形式打开，您可以在此为此样本中定义的所有参数输入值。
   - 输入所有参数的值。
   - 如果要在 AWS 中创建后端服务器，请选择后 端服务器配置。进一步选择 **AWS EC2** 自动缩放 > 云，然后输入所有参数的值。



- 可能需要一些可选配置，具体取决于您选择的样本。例如，您可能必须创建监视器、提供 SSL 证书设置等。
- 单击 创建以在 Citrix ADC 群集上部署配置。

> 注意
>
> - 配置和部署应用程序或虚拟服务器的 FQDN 将无法修改。

> 使用 DNS 将应用程序的 FQDN 解析为 IP 地址。由于此 DNS 记录可能会跨不同的名称服务器缓存，因此更改 FQDN 可能会导致流量被黑化。
>
> - SSL 会话共享在可用区域内按预期工作，但跨可用区域，需要重新验证。
>
> SSL 会话在群集内同步。由于跨可用区域的 Autoscale 组在每个区域中都有单独的群集，因此无法跨区域同步 SSL 会话。
>
> - 共享限制（如最大客户端和溢出溢出）是根据可用区数静态设置的。手动计算之后设置此限制。限制 = `<Limit required>/<number of Zones>.`
>
> 共享限制在群集内的节点之间自动分配。由于跨可用区域的 Autoscale 组在每个区域中都有单独的集群，因此必须手动计算这些限制。

升级 **Citrix ADC** 群集

手动升级群集节点。首先升级现有节点的映像，然后从 Citrix ADM 更新 AMI。

> 重要信息：
>
> 确保在升级期间执行以下操作：
>
> - 不触发扩展或向外扩展。
> - 不得对自动缩放组中的群集执行任何配置更改。
> - 您保留以前版本的 `ns.conf` 文件的备份。如果升级失败，您可以回退到以前的版本。

执行以下步骤以升级 Citrix ADC 群集节点。

1. 禁用 MAS ASG 门户上的自动缩放组。
2. 选择自动缩放组中的一个群集进行升级。
3. 按照主题中记录的步骤操作 升级或降级 Citrix ADC 群集。

   > 注意
   >
   > - 升级群集中的一个节点。
   > - 监视应用程序流量是否有任何故障。
   > - 如果遇到任何问题或故障，请降级先前升级的节点。否则，继续升级所有节点。

4. 继续升级自动缩放组中所有群集中的节点。

   > 注意：
   >
   > 如果任何群集的升级失败，请将自动缩放组中的所有群集降级到以前的版本。按照主题中记录的步骤操作 升级或降级 Citrix ADC 群集。

5. 成功升级所有群集后，更新 MAS ASG 门户上的 AMI。AMI 必须与用于升级的映像的版本相同。
6. 编辑自动扩展组并键入与升级版本对应的 AMI。
7. 在 ADM 门户上启用自动缩放组。

修改自动扩展组配置

- 您可以修改自动缩放组配置或删除自动缩放组。您只能修改以下“自动缩放”组参数。
  - 流量分配模式
  - 阈值参数的最大和最小限制
  - 最小和最大实例值
  - 耗尽连接周期值
  - 冷却时间段值
  - 实现时间价值 — 如果流量分配模式为 DNS
  - 观看持续时间值
- 您也可以在创建自动缩放组后删除它们。

  删除自动缩放组时，所有域和 IP 地址都将从 DNS/NLB 取消注册，并取消配置群集节点。

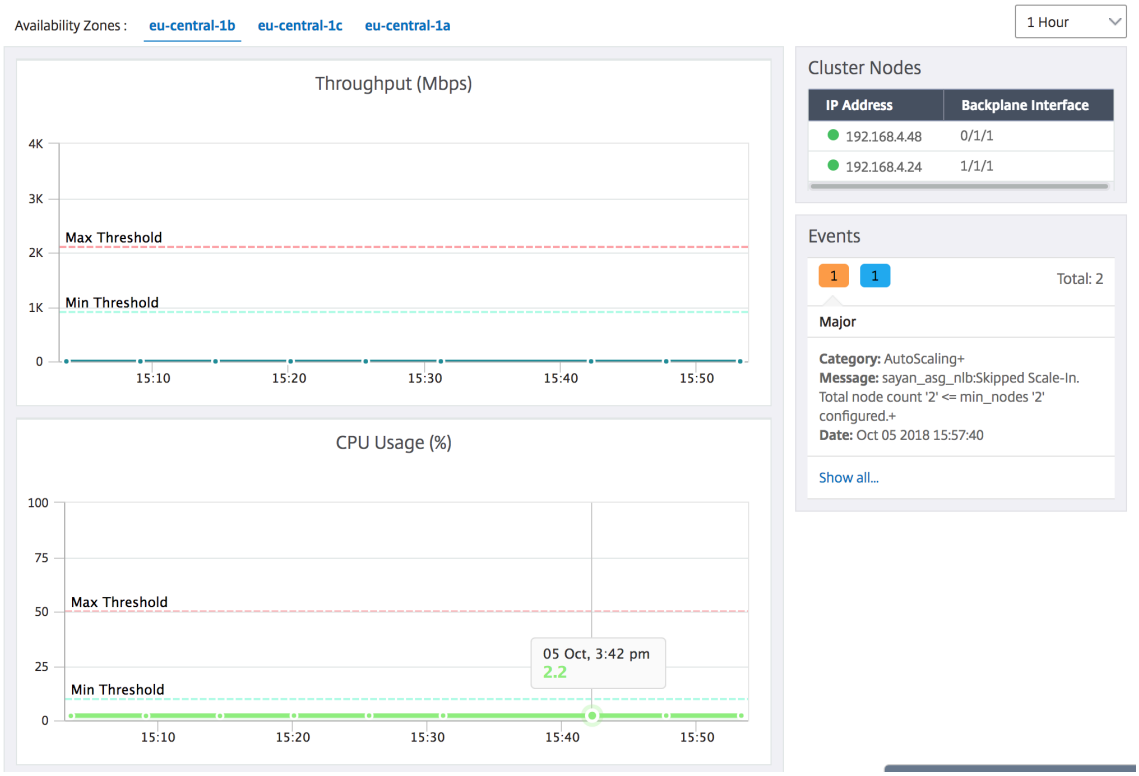
控制板

April 23, 2021

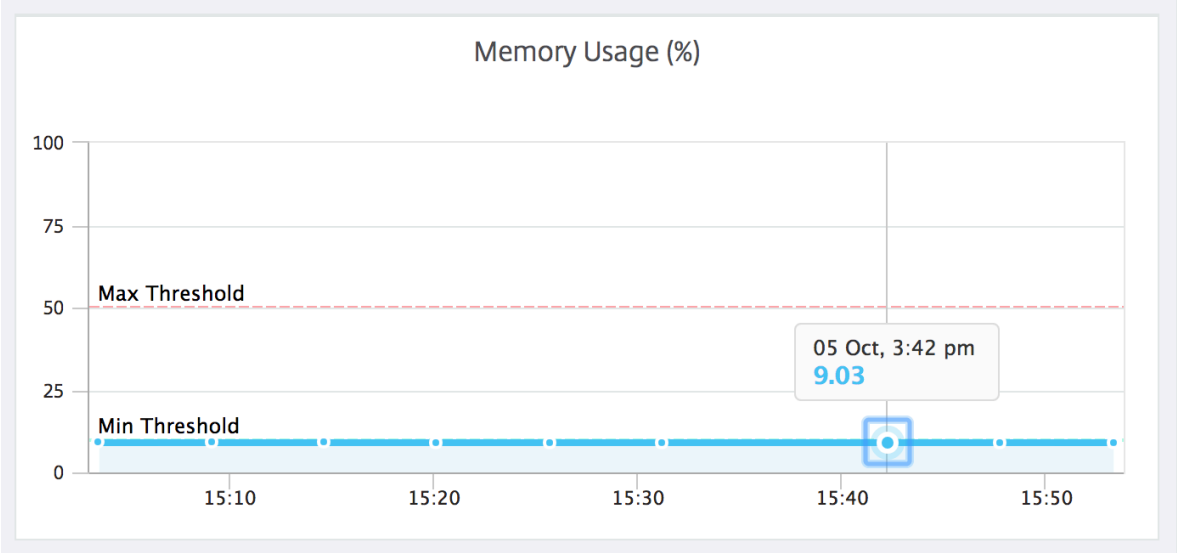
1. 在 Citrix ADM 中，导航到 **“网络” > “自动扩展组”**。
2. 选择自动缩放组，然后单击 仪表板。

   您可以查看所选监视参数的图形。右侧面板显示触发自动缩放的事件。左侧面板显示群集中每个区域的活动节点和事件。

   下图显示了示例控制板。



下图显示了自动缩放仪表板的一部分。



使用 **Citrix ADM** 在 **Microsoft Azure** 中自动缩放 **Citrix ADC VPX**

April 23, 2021

AutoScaling 是一种云计算方法，根据实际使用情况自动添加或删除资源。当您的站点或应用程序需要按需分配资源以

满足不断变化的客户端请求或处理作业时，AutoScaling 非常有用。

对 Web 应用程序或服务的需求可能会有很大差异。为不同的流量需求保持正确数量的 Citrix ADC 实例非常重要。您可以根据需求增加或减少 Microsoft Azure 上的网络资源。因此，它在不影响性能的情况下提供了成本优化。

Citrix Application Delivery Management (ADM) 自动缩放可保持 Citrix ADC 实例的确切数量，以应付不断波动的资源消耗。Citrix ADM 根据资源消耗波动来确定流量流，并决定在 Citrix ADC 实例中动态扩展或扩展。因此，它为您提供了维护正确数量的 Citrix ADC 实例的灵活性。

Citrix ADM 监视 Citrix ADC 实例的资源使用情况，并与配置的阈值匹配。如果其中一个已配置的资源超过指定的阈值，则会触发向外扩展操作。

只有当所有配置的资源的使用率低于正常阈值时，Citrix ADM 才会触发放大操作。

> 重要信息：
>
> 自动缩放支持所有 Citrix ADC 功能，但下列功能除外，这些功能需要群集节点上的配置：
>
> - GSLB
> - Citrix Gateway 及其功能
> - Telco 功能
>
> 有关斑点配置的详细信息，请参阅 带状、部分带状和斑点配置。

优势

应用程序的高可用性： AutoScaling 可确保您的应用程序始终拥有适当数量的 Citrix ADC VPX 实例来处理流量需求。它可以确保您的应用程序始终正常运行，而不考虑流量需求。

智能扩展决策和零接触配置：自动缩放持续监视您的应用程序，并根据需求动态添加或删除 Citrix ADC 实例。当需求在一段时间内增加时，系统会自动添加这些实例。当需求在一段时间内减少时，这些实例将自动移除。Citrix ADC 实例的添加和删除会自动执行，使其成为零接触手动配置。

自动 **DNS** 管理： Citrix ADM AutoScale 功能提供了自动 DNS 管理。每当添加新的 Citrix ADC 实例时，域名都会自动更新。

正常连接终止：在扩展过程中，Citrix ADC 实例会正常移除，避免客户端连接丢失。

更好的成本管理：自动扩展可根据需要动态增加或减少 Citrix ADC 实例。此方法使您能够优化所涉及的成本。仅在需要时启动实例并在不需要时终止它们可以降低运营成本。因此，您只需为使用的资源付费。

可观察性：可观察性是应用程序开发人员或 IT 人员监视应用程序运行状况的关键。Citrix ADM 的 AutoScale 仪表板使您能够可视化阈值参数值、自动缩放触发时间戳、事件和参与自动缩放的实例。

许可要求

为 Citrix AutoScale 组创建的 Citrix ADC 实例使用 Citrix ADC 高级或高级 ADC 许可证。Citrix ADC 群集功能包含在高级或高级 ADC 许可证中。

您可以选择以下方法之一来对 Citrix ADM 置备的 Citrix ADC 进行许可：

- 使用 **Citrix ADM** 中存在的 **ADC** 许可证：在创建 AutoScale 组时配置池容量、VPX 许可证或虚拟 CPU 许可证。因此，当为 AutoScale 组配置新实例时，已配置的许可证类型将自动应用于预配置的实例。
  - 池容量：将带宽分配给 Autoscale 组中的每个预配实例。确保您在 Citrix ADM 中具有预配新实例所需的可用带宽。有关详细信息，请参阅配置池容量。

    Autoscale 组中的每个 ADC 实例都会从池中签出一个实例许可证以及指定的带宽。
  - **VPX** 许可证：将 VPX 许可证应用于新预配置的实例。确保您在 Citrix ADM 中拥有必要数量的可用 VPX 许可证以置备新实例。

    预配置了 Citrix ADC VPX 实例后，该实例将从 Citrix ADM 中签出许可证。有关详细信息，请参阅Citrix ADC VPX 签入和签出许可。
  - 虚拟 **CPU** 许可证：将虚拟 CPU 许可证应用于新预配置的实例。此许可证指定授予 Citrix ADC VPX 实例的 CPU 数量。确保您在 Citrix ADM 中具有必要数量的虚拟 CPU 来置备新实例。

    预配置了 Citrix ADC VPX 实例后，该实例将从 Citrix ADM 中签出虚拟 CPU 许可证。有关详细信息，请参阅Citrix ADC 虚拟 CPU 许可。

  当预配置的实例被销毁或取消置备时，应用的许可证将自动返回到 Citrix ADM。

  要监视已使用的许可证，请导航到 网络 > 许可证页面。
- 使用 **Microsoft Azure** 订阅许可证：在创建自动缩放组时配置 Azure 市场中可用的 Citrix ADC 许可证。因此，当为 AutoScale 组配置新实例时，许可证将从 Azure 市场获取。

支持的用于自动缩放的 **Citrix ADC Azure** 虚拟机映像

使用至少支持三个网卡的 Azure 虚拟机映像。仅高级版和高级版支持自动扩缩 Citrix ADC VPX 实例。有关 Azure 虚拟机映像类型的详细信息，请参阅 Microsoft 文档中的 VM 类型和大小。

以下是用于自动扩展的推荐 VM 大小：

- Standard_DS3_v2
- Standard_B2ms
- Standard_DS4_v2

体系结构

Citrix ADM 使用 Azure DNS 或 Azure 负载平衡器 (ALB) 处理客户端流量分配。

使用 **Azure DNS** 进行流量分配

下图说明了如何使用 Azure 流量管理器作为流量分配器进行基于 DNS 的自动缩放：

在基于 DNS 的自动缩放中，DNS 充当分布层。Azure 流量管理器是 Microsoft Azure 中基于 DNS 的负载平衡器。流量管理器将客户端流量定向到 Citrix ADM 自动扩展组中可用的相应 Citrix ADC 实例。

Azure 流量管理器将 FQDN 解析为 Citrix ADC 实例的 VIP 地址。

> 注意：
>
> 在基于 DNS 的自动扩缩中，Citrix ADM AutoScale 组中的每个 Citrix ADC 实例都需要一个公有 IP 地址。

Citrix ADM 在群集级别触发向外扩展或扩展操作。当触发向外扩展时，将置备已注册的虚拟机并将其添加到群集中。同样，当触发扩展时，节点也会从 Citrix ADC VPX 群集中删除并取消置备。

使用 **Azure** 负载平衡器的流量分配

下图说明了如何使用 Azure 负载平衡器作为流量分发器进行自动缩放：

Azure 负载平衡器是群集节点的分发层。ALB 管理客户端流量并将其分发到 Citrix ADC VPX 群集。ALB 将客户端流量发送到 Citrix ADC VPX 群集节点，这些节点在 Citrix ADM 自动扩展组中可用。

> 注意
>
> 公有 IP 地址已分配给 Azure 负载平衡器。Citrix ADC VPX 实例不需要公有 IP 地址。

Citrix ADM 在群集级别触发向外扩展或扩展操作。当触发向外扩展时，注册的虚拟机将被置备并添加到群集中。同样，当触发扩展时，节点也会从 Citrix ADC VPX 群集中删除并取消置备。

Citrix ADM 自动缩放组

自动缩放组是一组 Citrix ADC 实例，它们将应用程序作为单个实体进行负载平衡，并根据配置的阈值参数值触发自动缩放。

资源组

资源组包含与 Citrix ADC 自动缩放相关的资源。此资源组可帮助您管理自动扩展所需的资源。有关详细信息，请参阅管理资源组。

Azure 后端虚拟机规模集

Azure 虚拟机规模是相同虚拟机实例的集合。VM 实例的数量可能会增加或减少，具体取决于客户端流量。此集为您的应用程序提供了高可用性。有关详细信息，请参阅虚拟机规模集。

可用区

可用区是 Azure 区域内的隔离位置。每个区域由多个可用区组成。每个可用区都属于一个区域。每个可用区都有一个 Citrix ADC VPX 群集。有关详细信息，请参阅Azure 中的可用区。

可用性集

可用性集是 Citrix ADC VPX 群集和应用程序服务器的逻辑分组。可用性集有助于跨群集中多个隔离硬件节点部署 ADC 实例。使用可用性集，您可以确保在 Azure 中出现硬件或软件故障时实现可靠的 ADM 自动缩放。有关详细信息，请参阅可用性集。

下图说明了可用性集中的自动扩展：

Azure 基础结构（ALB 或 Azure 流量管理器）将客户端流量发送到可用性集中的 Citrix ADM 自动缩放组。Citrix ADM 在群集级别触发向外扩展或扩展操作。

自动缩放的工作原理

下面的流程图说明了自动缩放工作流：

Citrix ADM 每分钟从 AutoScale 预配置的群集中收集统计信息（CPU、内存和吞吐量）。

将根据配置阈值评估统计信息。根据统计数据，将触发向外扩展或缩小。当统计数据超过最大阈值时，将触发向外扩展。当统计数据运行在最小阈值以下时触发缩放。

如果触发了横向扩展：

1. 已置备新节点。
2. 节点附加到群集，并且配置从群集同步到新节点。
3. 该节点已在 Citrix ADM 中注册。
4. 新节点 IP 地址将在 Azure 流量管理器中更新。

如果触发了缩放：

1. 已标识要删除的节点。
2. 停止与选定节点的新连接。
3. 等待指定的时间段以使连接耗尽。在 DNS 流量中，它还会等待指定的 TTL 周期。
4. 该节点将从群集中分离，从 Citrix ADM 取消注册，然后从 Microsoft Azure 中取消置备。

> 注意：部署应用程序
>
> 时，会在每个可用区域中的群集上创建一个 IP 集。然后，域和实例 IP 地址将注册到 Azure 流量管理器或 ALB。删除应用程序后，域和实例 IP 地址将从 Azure 流量管理器或 ALB 中取消注册。然后，IP 集被删除。

自动缩放方案示例

假设您已在具有以下配置的单个可用性区域中创建名为 asg_arn 的 Autoscale 组。

- 选定的阈值参数 — 内存使用情况。
- 设置为内存的阈值限制：
  - 最小限制：40
  - 最大限制：85
- 观看时间 — 2 分钟。
- 冷却时间 — 10 分钟。
- 取消置备期间的等待时间 — 10 分钟。
- DNS 生存时间 — 10 秒。

创建 AutoScale 组后，将从该组中收集统计信息。AutoScale 策略还会评估是否有任何 AutoScale 事件正在进行中。如果正在进行自动缩放，请等待该事件完成，然后再收集统计信息。

事件的顺序

1. 内存使用量超过 **T2** 的阈值限制。但是，横向扩展不会触发，因为它在指定的监视时间内没有违反。
2. 在连续超过最大阈值 2 分钟（观看时间）后，**T5** 触发向外扩展。
3. 由于节点 Provisioning 正在进行，因此未对 **T5-T10** 之间的违规执行任何操作。
4. 节点在 **T10** 上置备并添加到群集中。冷却时间开始。
5. 由于冷却时间，未对 **T10-T20** 之间的违规行为采取任何行动。此时间段确保了自动缩放组的实例的有机增长。在触发下一个扩展决策之前，它会等待当前流量稳定并平均出现当前实例集。
6. 内存使用率降至 **T23** 的最低阈值限制以下。但是，不会触发缩放，因为它在指定的监视时间内没有违反。
7. 在连续超过最小阈值 2 分钟（观看时间）后，**T26** 触发放量。群集中的节点被标识为取消置备。
8. 未对 **T26-T36** 之间的违规执行任何操作，因为 Citrix ADM 正在等待耗尽现有连接。对于基于 DNS 的自动缩放，TTL 生效。

   > 注意：
   >
   > 对于基于 DNS 的自动扩展，Citrix ADM 将等待指定的生存时间 (TTL) 期间。然后，它在启动节点取消置备之前等待现有连接耗尽。

9. 没有对 **T37-T39** 之间的违规执行任何操作，因为正在进行节点取消置备。
10. 节点将在 **T40** 从群集中删除并取消置备。

在启动节点取消置备之前，与选定节点的所有连接都已耗尽。因此，在节点取消置备后，将跳过冷却时间。

配置

April 23, 2021

Citrix ADM 管理 Microsoft Azure 中的所有 Citrix ADC VPX 群集。Citrix ADM 使用云访问配置文件访问 Azure 资源。

下面的流程图解释了创建和配置 AutoScale 组所涉及的步骤：

必备条件

本节介绍在配置自动扩缩 Citrix ADC VPX 实例之前，必须在 Microsoft Azure 和 Citrix ADM 中完成的先决条件。

本文档假定以下情况：

- 您拥有支持 Azure Resource Manager 部署模型的 Microsoft Azure 帐户。
- 您在 Microsoft Azure 中有一个资源组。

有关如何创建帐户和其他任务的详细信息，请参阅 Microsoft Azure 文档。

设置 **Microsoft Azure** 组件

在 Citrix ADM 中自动缩放 Citrix ADC VPX 实例之前，在 Azure 中执行以下任务。

1. 创建虚拟网络。
2. 创建安全组。
3. 创建子网。
4. 在 Microsoft Azure 中订阅 Citrix ADC VPX 许可证。
5. 创建和注册应用程序。
6. 设置 Citrix ADM 服务代理。

创建虚拟网络

1. 登录到您的 Microsoft Azure 门户。
2. 选择 创建资源。
3. 选择“网 络”，然后单击 虚拟网络。
4. 指定所需参数。
    - 在 资源组中，必须指定要在其中部署 Citrix ADC VPX 产品的资源组。
    - 在 位置”中，您必须指定支持可用区的位置，例如：

- 美国中部
- East US2
- 法國中部
- 北欧
- 东南亚
- 西欧
- West US2

> 注意：
>
> 应用程序服务器存在于此资源组中。

5. 单击创建。

有关详细信息，请参阅中的 Azure 虚拟网络 Microsoft 文档。

创建安全组

在虚拟网络 (VNet) 中创建三个安全组-管理、客户端和服务器连接各一个安全组。创建安全组以控制 Citrix ADC VPX 实例中的入站和出站流量。为要在 Citrix 自动缩放组中控制的传入流量创建规则。您可以根据需要添加多个规则。

- 管理：帐户中专门用于管理 Citrix ADC VPX 的安全组。Citrix ADC 必须与 Azure 服务联系，并需要互联网访问。允许在以下 TCP 和 UDP 端口上使用入站规则。
  - TCP：80、22、443、3008–3011、4001
  - UDP：67、123、161、500、3003、4500、7000

  > 注意
  >
  > 确保安全组允许 Citrix ADM 代理访问 VPX。

- 客户端：您帐户中专门用于 Citrix ADC VPX 实例的客户端通信的安全组。通常，TCP 端口 80、22 和 443 上允许入站规则。
- 服务器：您帐户中专门用于 Citrix ADC VPX 的服务器端通信的安全组。

有关如何在 Microsoft Azure 中创建安全组的详细信息，请参阅 创建、更改或删除网络安全组。

创建子网

在虚拟网络 (VNet) 中创建三个子网-管理、客户端和服务器连接各一个子网。指定 VNet 中为每个子网定义的地址范围。指定希望子网驻留的可用区。

- 管理：虚拟网络 (VNet) 中专门用于管理的子网。Citrix ADC 必须与 Azure 服务联系，并需要互联网访问。
- 客户端：虚拟网络 (VNet) 中专用于客户端的子网。通常情况下，Citrix ADC 从互联网通过公有子网接收应用程序的客户端流量。

- 服务器：设置应用程序服务器的子网。您的所有应用程序服务器都位于此子网中，并通过此子网接收来自 Citrix ADC 的应用程序流量。

> 注意
>
> 在创建子网时为子网指定适当的安全组。

有关如何在 Microsoft Azure 中创建子网的详细信息，请参阅 添加、更改或删除虚拟网络子网。

在 **Microsoft Azure** 中订阅 **Citrix ADC VPX** 许可证

1. 登录到您的 Microsoft Azure 门户。
2. 选择 创建资源。
3. 在 搜索商城栏中，搜索 `Citrix ADC` 并选择所需的商品版本。
4. 在 **"**选择软件计划列表中，选择以下许可证类型之一：
   - 携带您自己的许可证
   - Enterprise
   - Platinum

   > 注意
   >
   > - 如果选择 " 自带许可证 " 选项，则自动缩放组会在 Provisioning Citrix ADC 实例时从 Citrix ADM 中签出许可证。
   > - 在 Citrix ADM 中，**Advanced** 和 **Premium** 分别是 **Enterprise** 和 **Platinum** 的等效许可证类型。
5. 确保为选定的 Citrix ADC 产品启用了编程部署。
   a) 旁边 想要以编程方式部署**?** 中，单击开始**"**。
   b) 在 " 选 择订阅 " 中，选择 启用 " 以编程方式部署选定的 Citrix ADC VPX 版本。

   > 重要
   >
   > 在 Azure 中自动扩展 Citrix ADC VPX 实例需要启用编程部署。

   c) 单击保存。
   d) 关闭 配置程序化部署。
6. 单击创建。

创建和注册应用程序

Citrix ADM 使用此应用程序在 Azure 中自动缩放 Citrix ADC VPX 实例。

在 Azure 中创建和注册应用程序：

1. 在 Azure 门户中，选择 **Azure Active Directory**。
   此选项显示组织的目录。
2. 选择 应用注册：
   a) 在 名称” 中，指定应用程序的名称。
   b) 从列表中选择 应用程序类型。
   c) 在 登录 URL 中，指定用于访问应用程序的应用程序 URL。
3. 单击创建。

有关应用程序注册的更多信息，请参阅 Microsoft 文档。

Azure 会为应用程序分配应用程序 ID。以下是在 Microsoft Azure 中注册的应用程序示例：

在 Citrix ADM 中配置云访问配置文件时，复制以下 ID 并提供这些 ID。有关检索以下 ID 的步骤，请参阅 Microsoft 文档：

- 应用程序 ID
- 目录 ID
- 键
- 订阅 ID：从存储帐户复制订阅 ID。

为应用程序分配角色权限

Citrix ADM 使用应用程序即软件原则自动缩放 Microsoft Azure 中的 Citrix ADC 实例。此权限仅适用于选定的资源组。

若要为已注册的应用程序分配角色权限，您必须是 Microsoft Azure 订阅的所有者。

1. 在 Azure 门户中，选择 资源组。
2. 选择要为其分配角色权限的资源组。
3. 选择 访问控制 **(IAM)**。
4. 在 角色分配中，单击 添加。
5. 从 角色列表中选择 所有者。
6. 选择为自动扩展 Citrix ADC 实例注册的应用程序。
7. 单击保存。

设置 **Citrix ADM** 服务代理

在管理子网中安装 Citrix ADM 服务代理。此代理作为 Citrix Application Delivery Management (Citrix ADM) 和 Microsoft Azure 中的托管实例之间的中介工作。确保你已在 Azure 中安装了 Citrix ADM 代理。在 Azure ADM 代理中添加路由，以便 ADM 能够在建立第 3 层连接后访问该代理。

请按照以下步骤在 Azure 中安装的代理中添加路由：

1. 访问 Azure 上安装的 ADM 代理的控制台。
2. 在提示符下运行以下命令：

```
route add  -net <DMZ network> <gateway to ADM agent>

<!--NeedCopy-->
```

例如，`route add -net 10.x.x.0/24 21.1.1.10`

> 注意：
>
> 在代理重新启动后，路由将被删除。此行为特定于跳过网络设置的 Azure 代理映像。

有关如何在 Microsoft Azure 上安装 ADM 服务代理的详细信息，请参阅 ADM 服务文档 在 Microsoft Azure 云上安装 Citrix ADM 代理。

在 **Azure** 中创建路由表

添加路由表以建立从 Citrix ADC 实例到数据中心上部署的 Citrix ADM 的通信。

1. 登录 Azure 并创建路由表。
   a) 在 订阅中，选择 Azure 订阅。
   b) 选择要在其中部署 ADC 实例的资源组。请参阅创建路由表。
2. 在子网设置中，将管理子网与部署 ADC 实例的路由表相关联。将子网与路由表关联。
3. 在 “ 设置” 下，选择 “ 路由”，然后单击 “ **+** 添加”。

   确保指定以下详细信息：

   - 地址前缀：指定 Citrix ADM 网络。您可以指定 Citrix ADM IP 地址或 Citrix ADM 子网。
   - 下一跳类型：选择虚拟设备。
   - 下一跳地址：指定 Citrix SD-WAN 连接器通道 IP 地址。

   有关详细信息，请参阅添加路由。

设置 **Citrix ADM** 组件

在 Citrix ADM 中自动缩放 Citrix ADC VPX 实例之前，在 Azure 中执行以下任务：

1. 创建站点。
2. 将站点连接到 Citrix 服务代理。

创建站点

在 Citrix ADM 中创建站点，并添加与您的 Microsoft Azure 资源组关联的 VNet 详细信息。

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 站点”。
2. 单击添加。
3. 在 **“**选择云**”** 窗格中，
   a) 选择 数据中心作为 站点类型。
   b) 从 “ 类型” 列表中选择 **Azure** 。
   c) 选中 从 **Azure** 获取 **vNet** 复选框。

      此选项可帮助您从 Microsoft Azure 帐户中检索现有 VNet 信息。
   d) 单击下一步。
4. 在 **“**选择区域**”** 窗格中，
   a) 在 云访问配置文件中，选择为您的 Microsoft Azure 帐户创建的配置文件。如果没有配置文件，请创建配置文件。
   b) 要创建云访问配置文件，请单击 添加”。
   c) 在 名称” 中，指定用于在 Citrix ADM 中标识 Azure 帐户的名称。
   d) 在租户 **Active Directory ID/**租户 **ID** 中，指定 Microsoft Azure 中的租户或帐户的 Active Directory ID。
   e) 指定 订阅 **ID**。
   f) 指定应用程序 **ID/**客户端 **ID**。
   g) 指定 应用程序密钥密码**/**密码。
   h) 单击创建。

      有关详细信息，请参阅创建和注册应用程序和将云访问配置文件映射到 Azure 应用程序。
   i) 在 **VNet** 中，选择包含要管理的 Citrix ADC VPX 实例的虚拟网络。
   j) 指定 站点名称。
   k) 单击完成。

将云访问配置文件映射到 **Azure** 应用程序

Citrix ADM 期限	**Microsoft Azure** 术语
租户 Active Directory ID/租户 ID	目录 ID

Citrix ADM 期限	**Microsoft Azure** 术语
订阅 ID	订阅 ID
应用程序 ID/客户端 ID	应用程序 ID
应用程序密码/密码	密钥或证书或客户机密

将站点连接到 **Citrix ADM** 服务代理

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 代理”。
2. 选择要为其附加站点的代理。
3. 单击 “ 附加站点”。
4. 从要附加的列表中选择站点。
5. 单击保存。

步骤 **1**：初始化 **Citrix ADM** 中的自动扩展配置

1. 在 Citrix ADM 中，导航到 “ 网络” > “ 自动缩放组”。
2. 单击 添加以创建自动缩放组。

   此时将显示 “创建 自动缩放组” 页。
3. 选择 **Microsoft Azure** 并单击 下一步。
4. 在 基本参数中，输入以下详细信息：
   - 名称：键入自动扩展组的名称。
   - 站点：选择已创建用于在 Microsoft Azure 上自动扩展 Citrix ADC VPX 实例的站点。如果您尚未创建站点，请单击 添加以创建站点。
   - 代理：选择用于管理预配置实例的 Citrix ADM 代理。
   - 云访问配置文件：选择云访问配置文件。您还可以添加或编辑云访问配置文件。
   - 设备配置文件：从列表中选择设备配置文件。当需要登录到 Citrix ADC VPX 实例时，Citrix ADM 会使用设备配置文件。

     > 注意：
     >
     > 确保选定的设备配置文件符合 Microsoft Azure 密码规则。
   - 流量分配模式：使用 **Azure LB** 进行负载平衡选项作为默认流量分配模式。您还可以选择使用 **Azure DNS** 模式的 **DNS** 进行流量分配。

- 启用自动缩放组：启用或禁用 ASG 组的状态。默认情况下，此选项处于启用状态。如果禁用此选项，则不会触发自动缩放。
- 可用性集或可用区：选择要在其中创建自动扩展组的可用性集或可用区。根据您选择的云访问配置文件，可用区或可用性集将显示在列表中。
- 标签：键入自动缩放组标签的键值对。标签由区分大小写的键值对组成。这些标签使您能够轻松地组织和识别自动缩放组。这些标签同时应用于 Microsoft Azure 和 Citrix ADM。

5. 单击下一步。

步骤 **2**：配置自动缩放参数

1. 在 自动缩放参数选项卡中，输入以下详细信息。
2. 选择以下一个或多个阈值参数，必须监视其值才能触发向外扩展或扩展。
   - 启用 **CPU** 使用率阈值：根据 CPU 使用率监视衡量指标。
   - 启用内存使用阈值：根据内存使用情况监视衡量指标。
   - 启用吞吐量阈值：根据吞吐量监视指标。

     > 注意
     >
     > - 默认最小阈值限制为 30，最大阈值限制为 70。但是，您可以更改以修改限制。
     > - 最小阈值限制必须等于或小于最大阈值限制的一半。
     > - 您可以选择多个阈值参数进行监视。如果至少有一个阈值参数高于最大阈值，则会触发向外扩展。但是，只有当所有阈值参数都低于其正常阈值时，才会触发放入。

   - 保留备用节点以加快向外扩展：此选项有助于实现更快的横向扩展。ADM 将备用节点置于非活动状态。

     当 ADM 触发横向扩展操作时，备用节点会立即变为活动状态。因此，它可以在横向扩展期间保存节点配置时间节点。

   - 最小实例：选择必须为此 AutoScale 组配置的最小实例数。

     默认的最小实例数等于选定的区域数。您只能增加指定区域数量的倍数中的最小实例。

     例如，如果可用区数为 4，则默认情况下最少实例为 4。您可以将最小实例增加 8、12、16。

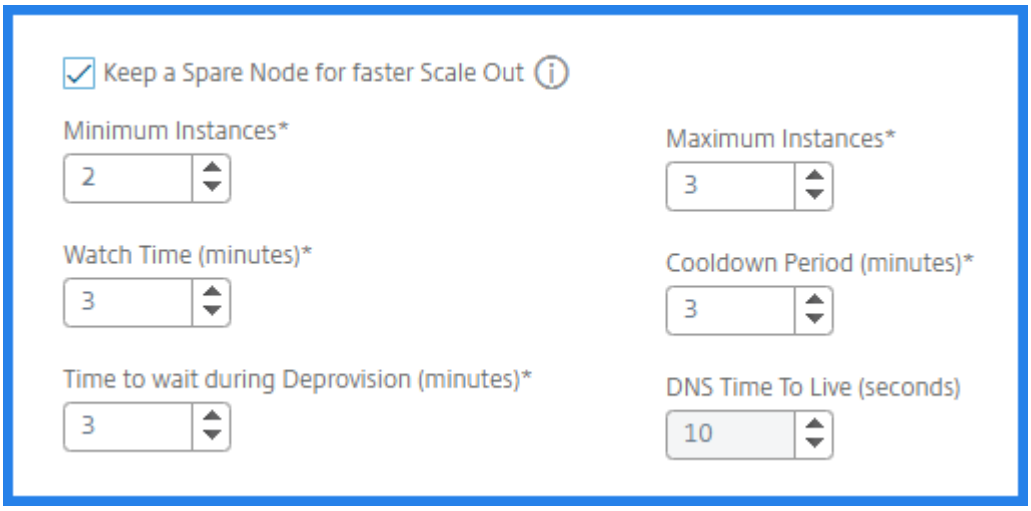
   - 最大实例数：选择必须为此 AutoScale 组预配的最大实例数。

     最大实例数必须大于或等于最小实例数。最大实例数不能超过可用区数乘以 32。

     最大实例数 = 可用区数 x 32

   - 观看时间（分钟）：选择观看时间持续时间。缩放参数阈值必须保持超出以便进行缩放的时间。如果在此指定时间内收集的所有样本上超过阈值，则会进行缩放。

- 冷却时间（分钟）：选择冷却时间。在横向扩展期间，冷却时间是指在向外扩展发生后必须停止统计数据评估的时间。此时间段确保了自动缩放组的实例的有机增长。在触发下一个扩展决策之前，它会等待当前流量稳定并平均出现当前实例集。
- 取消置备期间的等待时间（分钟）：选择耗尽连接超时周期。在扩展操作期间，将确定要取消置备的实例。Citrix ADM 限制已识别的实例处理新连接，直到指定的时间到期后才取消置备。在此期间，它允许在取消置备前将与此实例的现有连接耗尽。
- **DNS** 生存时间（秒）：选择时间（以秒为单位）。在此期间，在路由器丢弃数据包之前，数据包被设置为存在于网络中。此参数仅在使用 Microsoft Azure 流量管理器的流量分配模式为 DNS 时适用。



3. 单击下一步。

步骤 3：**Provisioning** 用于置备 **Citrix ADC** 实例的许可证

选择以下模式之一以许可属于 AutoScale 组的 Citrix ADC 实例：

- 使用 **Citrix ADM**：在 Provisioning Citrix ADC 实例时，自动扩展组会从 Citrix ADM 中签出许可证。
- 使用 **Microsoft Azure**：从云分配选项使用 Azure 市场中提供的 Citrix 产品许可证。在 Provisioning Citrix ADC 实例时，自动扩展组使用市场中的许可证。

  如果您选择使用 Azure 应用商店中的许可证，请在 云参数选项卡中指定产品或许可证。

有关详细信息，请参阅许可要求。

使用来自 **Citrix ADM** 的许可证

要使用此选项，请确保已使用 自带许可证软件计划在 Azure 中订阅 Citrix ADC 产品。请参阅在 Microsoft Azure 中订阅 Citrix ADC VPX 许可证。

1. 在 许可证选项卡中，选择 从 **ADM** 分配。
2. 在 许可证类型”中，从列表中选择以下选项之一：

- 带宽许可证：您可以从“带 宽许可证类型”列表中选择以下选项之一：
  - 池容量：指定要为自动扩展组中每个新实例分配的容量。

    在公共池中，Autoscale 组中的每个 ADC 实例签出一个实例许可证，并且只指定多大带宽。
  - **VPX** 许可证：预配 Citrix ADC VPX 实例时，实例将从 Citrix ADM 中签出许可证。
- 虚拟 **CPU** 许可证：预配置的 Citrix ADC VPX 实例会根据自动扩展组中运行的 CPU 数量签出许可证。

> 注意：
>
> 删除或销毁预配置的实例后，应用的许可证将返回到 Citrix ADM 许可证池。在下一次 AutoScale 期间，这些许可证可以重复用于预配新实例。

3. 在 许可证版本中，选择许可证版本。自动扩展组使用指定版本来置备实例。
4. 单击下一步。

步骤 **4**：配置云参数

1. 在 云参数选项卡中，输入以下详细信息：
   - 资源组：选择部署 Citrix ADC 实例的资源组。
   - 产品/许可证：选择要置备的 Citrix ADC 产品版本。确保为所选类型启用了编程访问。有关详细信息，请参阅在 Microsoft Azure 中订阅 Citrix ADC VPX 许可证。
   - **Azure** 虚拟机大小：从列表中选择所需的虚拟机大小。

     > 注意：
     >
     > 确保选定的 Azure 虚拟机大小至少具有三个网卡。有关详细信息，请参阅支持的 Azure 虚拟映像进行自动缩放。
   - **ADC** 的云访问配置文件： Citrix ADM 使用此配置文件登录到 Azure 帐户，以置备或取消置备 ADC 实例。它还配置 Azure 库或 Azure DNS。
   - 图像：选择所需的 Citrix ADC 版本映像。单击 添加新建以添加 Citrix ADC 映像。
   - 安全组：安全组控制 Citrix ADC VPX 实例中的入站和出站流量。为管理、客户端和服务器通信选择安全组。有关管理、客户端和服务器安全组的详细信息，请参阅安全组。
   - 子网：您必须拥有三个独立的子网（如管理、客户端和服务器子网）才能自动扩展 Citrix ADC 子网。子网包含自动缩放所需的实体。选择有关详细信息，请参阅子网。
2. 单击“ 完成”。

步骤 **5**：为自动缩放组配置应用程序

1. 在 Citrix ADM 中，导航到 网络 > 自动缩放组。

2. 选择您创建的自动缩放组，然后单击 配置。
3. 在 配置应用程序中，指定以下详细信息：
   - 应用程序名称 -指定应用程序的名称。
   - 访问类型 -您可以将 ADM 自动扩缩解决方案用于外部和内部应用程序。选择所需的应用程序访问类型。
   - **FQDN** 类型 -选择分配域名和区域名称的模式。

     如果要手动指定，请选择 用户定义。要自动分配域名和区域名称，请选择 自动生成。
   - 域名 -指定应用程序的域名。此选项仅在选择用户定义的 FQDN 类型时适用。
   - 域的区域 -从列表中选择应用程序的区域名称。此选项仅在选择用户定义的 FQDN 类型时适用。

     此域和区域名称将重定向到 Azure 中的虚拟服务器。例如，如果您在中托管应用程序 `app.example.com`，则 `app` 为域名和 `example.com` 区域名称。
   - 协议 -从列表中选择协议类型。配置的应用程序根据所选协议类型接收流量。
   - 端口 -指定端口值。指定的端口用于在应用程序和 AutoScale 组之间建立通信。

   如果要使用样书配置应用程序，请在确认窗口中选择 是。

   > 注意
   >
   > ：如果将来要修改以下详细信息，请更改应用程序的访问类型：
   >
   > - FQDN 类型
   > - 域名
   > - 域名的区域

4. 选择要为选定的自动缩放组部署配置的所需样书。

   如果要导入样本，请单击 导入新样本。
5. 指定所有参数的值。

   配置参数在所选样本中预先定义。
6. 选中 应用程序服务器组类型云复选框以指定虚拟机规模集中可用的应用程序服务器。
   a) 在 应用程序服务器队列名称中，指定虚拟机 规模集的自动缩放设置名称。
   b) 从列表中选择 应用程序服务器协议。
   c) 在 成员端口中，指定应用程序服务器的端口值。

   > 注意：
   >
   > 确保 “ 自动禁用正常关机” 选项设置为 “ 否”，并且 “ 自动禁用延迟” 字段为空。

   a) 如果要为应用程序服务器指定高级设置，请选中 高级应用程序服务器设置” 复选框。然后，指定在 高级应用程序服务器设置” 下列出的所需值。

7. 如果虚拟网络中有独立的应用程序服务器，请选中 应用程序服务器组类型静态复选框：
   a) 从列表中选择 应用程序服务器协议。
   b) 在 “ 服务器 **IP** 和端口” 中，单击 **+** 以添加应用程序服务器 IP 地址、端口和权重，然后单击 “ 创建”。
8. 单击创建。

修改自动缩放组配置

您可以修改自动缩放组配置或删除自动缩放组。只能修改以下 “自动缩放” 组参数：

- 阈值参数的最大和最小限制
- 最小和最大实例值
- 耗尽连接周期值
- 冷却时间段值
- 观看持续时间值

您也可以在创建自动缩放组后删除它们。

删除自动缩放组后，所有域和 IP 地址都将从 DNS 中取消注册，并取消配置群集节点。

控制板

April 23, 2021

1. 在 Citrix ADM 中，导航到 **“网络” > “自动扩展组”**。
2. 选择自动缩放组，然后单击 仪表板。

您可以查看所选监视参数的图形。右侧面板显示触发自动缩放的事件。左侧面板显示每个区域的群集中的活动节点、活动节点图形和事件。

下图显示了示例控制板。

下图显示了活动节点图形。时间戳下方的数字显示活动节点的数量。您可以在任何给定时间查看属于可用区域一部分的活动节点的数量。

事件

在 仪表板中，“ 事件” 选项卡显示所选自动缩放组的事件总数。它还会显示最新活动的简短消息。

要查看事件的详细信息，请单击 全部显示”。

Azure 术语

April 23, 2021

以下是 Citrix ADM 中所需的 Azure 术语列表：

术语	定义
Azure 负载平衡器	Azure 负载平衡器是一种资源，用于在网络中的 Citrix ADC VPX 实例之间分配传入流量。流量在负载平衡器集中定义的虚拟机之间分配。负载平衡器可以是外部或面向 Internet 的，也可以是内部的。
流量管理器	Azure 流量管理器是 Microsoft Azure 中基于 DNS 的负载平衡器。它将传入流量发送到网络中所需的 Citrix ADC VPX 实例。
Azure Resource Manager (ARM)	ARM 是 Azure 中服务的新管理框架。Azure 负载平衡器使用基于 ARM 的 API 和工具进行管理。
后端地址池	这些 IP 地址与负载分配到的虚拟机 NIC 相关联。
斑点	二进制大对象 — 可以存储在 Azure 存储中的任何二进制对象（如文件或图像）。
前端 IP 配置	Azure 负载均衡器可以包含一个或多个前端 IP 地址，也称为虚拟 IP (VIP)。这些 IP 地址用作流量的入口。
实例级公有 IP (ILPIP)	ILPIP 是可以直接分配给虚拟机或角色实例而不是云服务的公有 IP 地址。此 IP 不代替分配给您的云服务的 VIP（虚拟 IP）。相反，它是一个额外的 IP 地址，您可以使用它直接连接到虚拟机或角色实例。
入站 NAT 规则	这些规则将负载平衡器上的公有端口映射到后端地址池中特定虚拟机的端口。
IP 配置	它是与单个网卡关联的 IP 地址对（公共 IP 和私有 IP）。在 IP-Config 中，公用 IP 地址可以为空。每个网卡可以有多个与其关联的 IP 配置，最多可达 255 个。
负载平衡规则	将给定前端 IP 和端口组合映射到一组后端 IP 地址和端口组合的规则属性。使用负载平衡器资源的单个定义，您可以定义多个负载均衡规则。每个规则都反映了与虚拟机关联的前端 IP 和端口以及后端 IP 和端口的组合。
网络安全组 (NSG)	NSG 包含允许或拒绝向虚拟网络中虚拟机实例发送网络流量的访问控制列表 (ACL) 规则列表。可以将 NSG 与子网或该子网中的各个虚拟机实例相关联。

术语	定义
专用 IP 地址	此地址是用于 Azure 虚拟网络内通信的 IP 地址，当使用 VPN Gateway 将网络扩展到 Azure 时，您的本地网络。私有 IP 地址允许 Azure 资源与其他资源进行通信。虚拟网络或本地网络中的通信是通过 VPN Gateway 或 ExpressRoute 电路进行的。此通信不需要互联网可访问的 IP 地址。在 Azure Resource Manager 部署模型中，私有 IP 地址与 Azure 的虚拟机、内部负载平衡器 (ILB) 和应用程序网关关联。
探测器	运行状况探测器，用于检查后端地址池中虚拟机实例的可用性。
公有 IP 地址 (PIP)	PIP 用于与互联网的通信。它包括与虚拟机、内部负载平衡器 (ILB)、VPN 网关和 Azure 的应用程序网关关联的面向 Azure 公众的服务
地理区域	地理区域内不跨越国界，它包含一个或多个数据中心。定价、地区服务以及产品/服务类型在地区级别展现。一个区域通常与另一个区域配对，该区域与区域对的距离很大。区域配对也用作灾难恢复和高可用性方案的机制。也称为位置。
资源组	资源管理器中的容器保存应用程序的相关资源。资源组可以包括应用程序的所有资源，也可以仅包括逻辑分组的那些资源。
存储帐户	Azure 存储帐户允许您访问 Azure 存储中的 Azure blob、队列、表和文件服务。存储帐户为您的 Azure 存储数据对象提供唯一的命令空间。
虚拟机	运行操作系统的物理计算机的软件实现。多个虚拟机可以同时在同一硬件上运行。在 Azure 中，虚拟机有各种大小可用。
虚拟网络	Azure 虚拟网络是云中自己网络的表示形式。它在逻辑上是隔离的，专门用于 Azure 云中的订阅。您可以控制此网络中的 IP 地址块、DNS 设置、安全策略和路由表。

使用基础架构分析可视化问题

April 23, 2021

网络管理员的一个关键目标是监视 Citrix ADC 实例。ADC 实例提供了有趣的见解，了解通过它访问的应用程序和桌面的使用情况和性能。管理员必须监视 ADC 实例并分析每个 ADC 实例处理的应用程序流。他们可以修复配置、设置、连接、证书和其他可能影响应用程序使用或性能的任何可能的问题。例如，应用程序流量模式的突然变化可能是由于 SSL 配置的更改（如禁用 SSL 协议）造成的。管理员必须能够快速识别这些数据点之间的关联，以确保以下几点：

- 应用程序可用性处于最佳状态
- 没有资源消耗、硬件、容量或配置更改问题
- 没有未使用的库存
- 没有过期的证书

基础架构分析功能通过关联多个数据源并将其量化为可衡量的分数来定义实例运行状况，从而简化了数据分析过程。使用此功能，管理员可以获得单个接触点以了解是否存在问题、问题的根源以及他们可以执行的可能的修正。

基础架构分析

Citrix Application Delivery Management (ADM) 基础架构分析功能可对从 Citrix ADC 实例收集的所有数据进行整理，并将其量化为定义 实例运行状况的实例分数。实例分数通过表格视图或圆包可视化进行汇总。基础架构分析功能可帮助您可视化导致或可能导致实例问题的因素。此可视化还可帮助您确定为防止问题及其再次发生必须执行的操作。

实例分数

实例分数表示 ADC 实例的运行状况。分数为 100 意味着一个完美健康的实例没有任何问题。实例分数捕获实例上潜在问题的不同级别。它是一个可量化的实例健康度量，多个“健康指标”有助于分数。

运行状况指标是实例分数的构建块，其中分数是根据该时间窗口中检测到的所有指标定期计算的预定义“监视期”。目前，基础架构分析基于从实例收集的数据，每小时计算一次实例得分。
指标可以定义为属于实例上以下类别之一的任何活动（事件或问题）。

- 系统资源指标
- 关键事件指标
- SSL 配置指示器
- 配置偏差指示器

健康指标

- 系统资源指标

  以下是 Citrix ADC 实例上可能出现并由 Citrix ADM 监视的关键系统资源问题。

  - **CPU** 使用率高。CPU 使用率已超过 Citrix ADC 实例中的较高阈值。
  - 内存使用率高。在 Citrix ADC 实例中，内存使用量已超过较高的阈值。

- 磁盘使用率高。在 Citrix ADC 实例中，磁盘使用率已超过较高的阈值。
- 磁盘错误。安装 ADC 实例的 Hypervisor 上的硬盘 0 或硬盘 1 出现错误。
- 电源故障。电源出现故障或与 ADC 实例断开连接。
- **SSL** 卡故障。实例上安装的 SSL 卡失败。
- 闪存错误。在 Citrix ADC 实例上看到紧凑型闪存错误。
- 网卡丢弃。由 NIC 卡丢弃的数据包已超过 Citrix ADC 实例中的较高阈值。

有关这些系统资源错误的详细信息，请参阅 实例仪表板。

- 关键事件指标

  以下严重事件由 ADM 的事件管理功能下的事件标识，这些事件配置为严重严重性。

  - 高可用性同步失败。高可用性 ADC 实例之间的配置同步在辅助服务器上失败。
  - 高可用性无检测信号。一对高可用性 ADC 实例中的主服务器未从辅助服务器接收心跳。
  - 高可用性不良的辅助状态。一对高可用性 ADC 实例中的辅助服务器处于“关闭”、“未知”或“保持辅助”状态。
  - 高可用性版本不匹配。安装在一对高可用性 ADC 实例上的 ADC 软件映像版本不匹配。
  - 群集同步失败。群集模式下的 ADC 实例之间的配置同步失败。
  - 群集版本不匹配。在群集模式下安装在 ADC 实例上的 ADC 软件映像版本不匹配。
  - 群集传播失败。将配置传播到群集中的所有实例失败。

    > 注意：
    >
    > 您可以通过更改事件的严重性级别来获取关键 SNMP 事件列表。有关如何更改严重性级别的详细信息，请参阅 修改 Citrix ADC 实例上发生的事件的报告严重性。

  有关 Citrix ADM 中事件的详细信息，请参阅 事件。

- SSL 配置指示器
  - 不建议密钥强度。SSL 证书的关键强度不符合 Citrix 标准
  - 不推荐发行人。Citrix 不建议使用 SSL 证书的颁发者。
  - **SSL** 证书已过期。ADC 实例中安装的 SSL 证书已过期。
  - **SSL** 证书到期。ADC 实例中安装的 SSL 证书即将在下一周内过期。
  - 不推荐算法。ADC 实例中安装的 SSL 证书的签名算法不符合 Citrix 标准。

有关 SSL 证书的详细信息，请参阅 SSL 控制板。

- 配置偏差指示器
  - 配置漂移模板。您使用要在某些实例上审核的特定配置创建的审核模板中的配置存在偏移（未保存的更改）。

– 默认配置漂移。默认配置文件中的配置存在偏移（未保存的更改）。

有关配置偏差以及如何运行审计报告以检查配置偏差的详细信息，请参阅 查看审计报告。

查看 **ADC** 容量问题

当 ADC 实例消耗了其大部分可用容量时，处理客户端流量时可能会丢包。此问题会导致 ADC 实例中的性能低。通过了解此类 ADC 容量问题，您可以主动分配额外的许可证，以稳定 ADC 性能。

要查看 ADC 容量问题，请

1. 导航到 **“网络” > “基础架构分析”**。
2. 展开要查看其容量问题的实例。

ADM 每五分钟从 ADC 实例轮询一次这些事件，并显示数据包丢失或速率限制计数器增量（如果存在）。这些问题按以下容量参数进行分类：

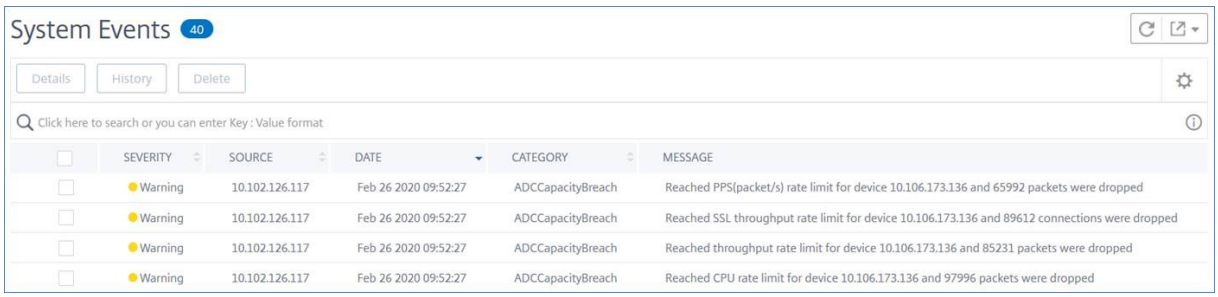
- 达到吞吐量限制 **—** 达到吞吐量限制后在实例中丢弃的数据包数。
- 已达到 **PE CPU** 限制**-**达到 PE CPU 限制后所有网卡上丢弃的数据包数。
- 已达到 **PPS** 限制 **—** 达到 PPS 限制后在实例中丢弃的数据包数。
- **SSL** 吞吐率限制 — 达到 SSL 吞吐量限制的次数。
- **SSL TPS** 费率限制 — 达到 SSL TPS 限制的次数。

ADM 根据定义的容量阈值计算实例得分。

- 低阈值 — 1 个数据包丢弃或速率限制计数器增量
- 高阈值 — 10000 个数据包丢弃或速率限制计数器增量

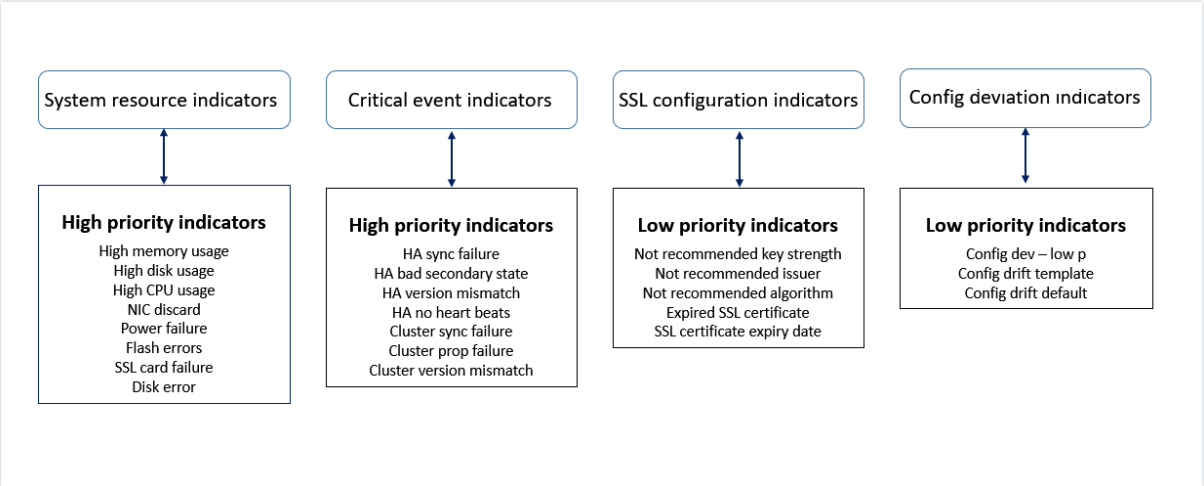
因此，当 ADC 实例超出容量阈值时，实例得分会受到影响。

当数据包丢弃或速率限制计数器递增时，将在 `ADCCapacityBreach` 类别下生成一个事件。要查看这些事件，请导航到 **“帐户” > “系统事件”**。



健康指标的价值

这些指标根据以下价值分为高优先指标和低优先指标：



同一组指标中的健康指标具有不同的权重。一个指标可能会比另一个指标对降低实例分数的贡献更大。例如，高内存使用率会降低实例分数超过高磁盘使用率、高 CPU 使用率和 NIC 丢弃。如果实例上检测到的指标数量较大，则实例得分越小。

指标的值是根据以下规则计算的。指标被认为是通过以下三种方式之一检测:

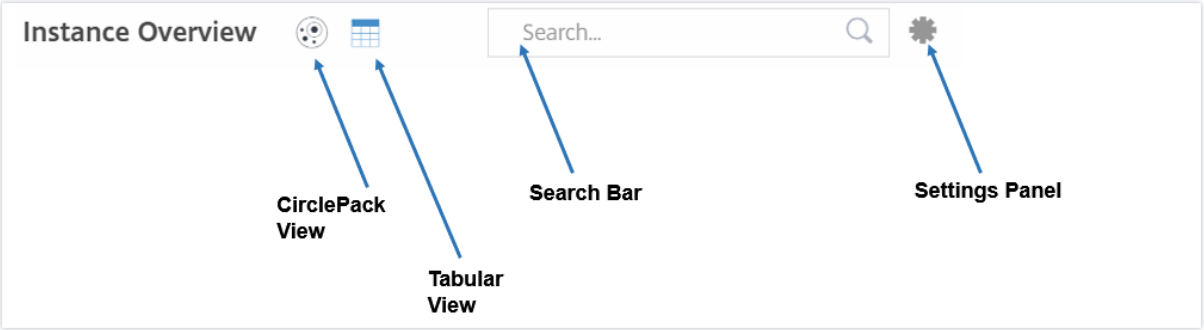
1. 基于活动。例如，只要实例出现电源故障，系统资源指示器就会触发，此指示器会降低实例得分的值。当指标被清除时，惩罚将被清除，并且实例得分增加。
2. 基于阈值违反。例如，当 NIC 卡丢弃数据包且超过阈值级别时，会触发系统资源指示器。
3. 基于低阈值和高阈值违反。在这里，指标可以通过两种方式触发：
    - 当指标值介于低阈值和高阈值之间时，在这种情况下，对实例分数征收部分罚款。
    - 当值超过高阈值时，在这种情况下，对实例得分征收全部罚款。
    - 如果该值低于低阈值，则不会对实例得分征收任何罚款。

例如，CPU 使用率是当使用率值超过低阈值时以及该值超过高阈值时触发的系统资源指示器。

基础设施分析控制板

导航到 网络 > 基础设施分析。

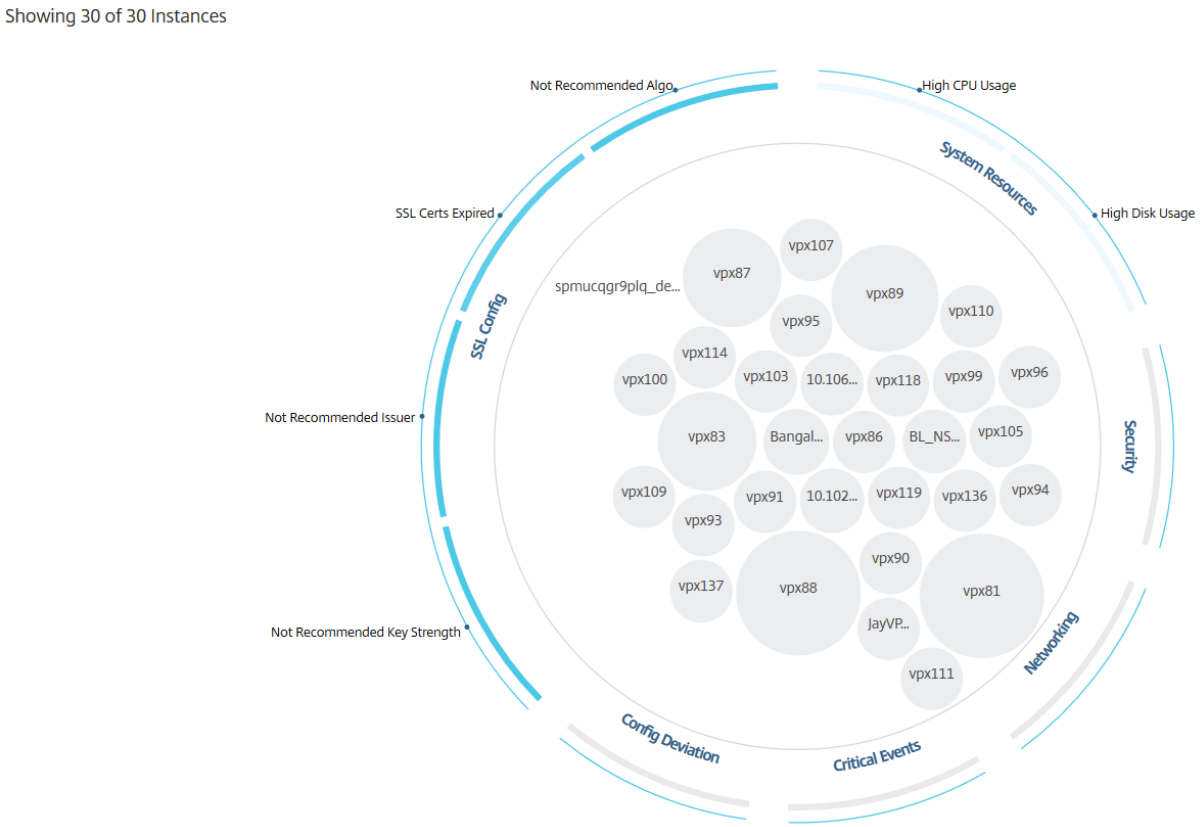
基础架构分析可以以 圆形包格式或 表格式查看。您可以在两种格式之间切换。



- 在“表格”视图中，您可以通过在搜索栏中键入主机名或 IP 地址来搜索实例。
- 默认情况下，“基础结构分析”页面将在页面右侧显示“摘要面板”。
- 单击设置图标以显示设置面板。
- 在这两种视图格式中，摘要面板都会显示网络中所有实例的详细信息。

圆包视图

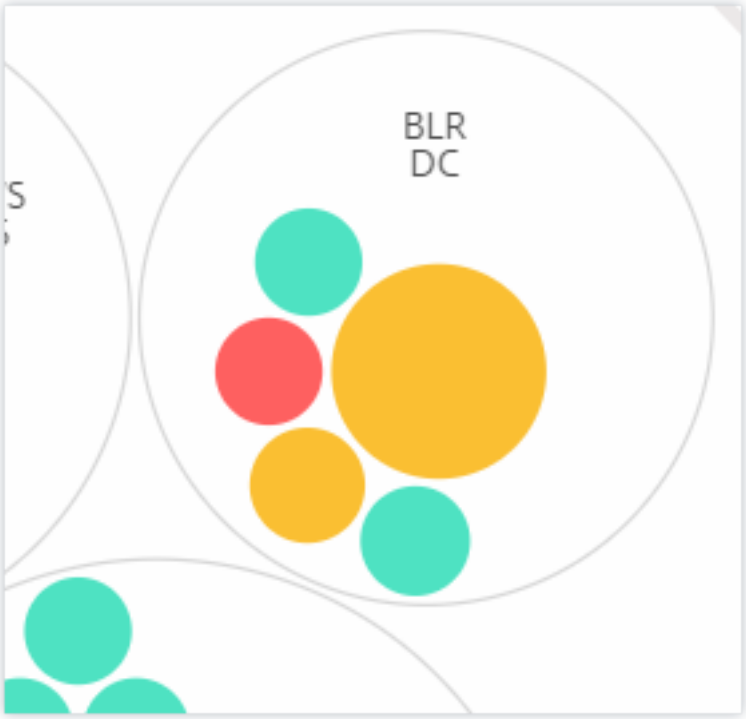
圆形包装图将实例组显示为紧密组织的圆形。它们通常显示层次结构，其中较小的实例组的颜色与同一类别中的其他实例组相似，或嵌套在较大的组中。圆包表示分层数据集，并显示层次结构中的不同级别以及它们之间的交互方式。



实例圆

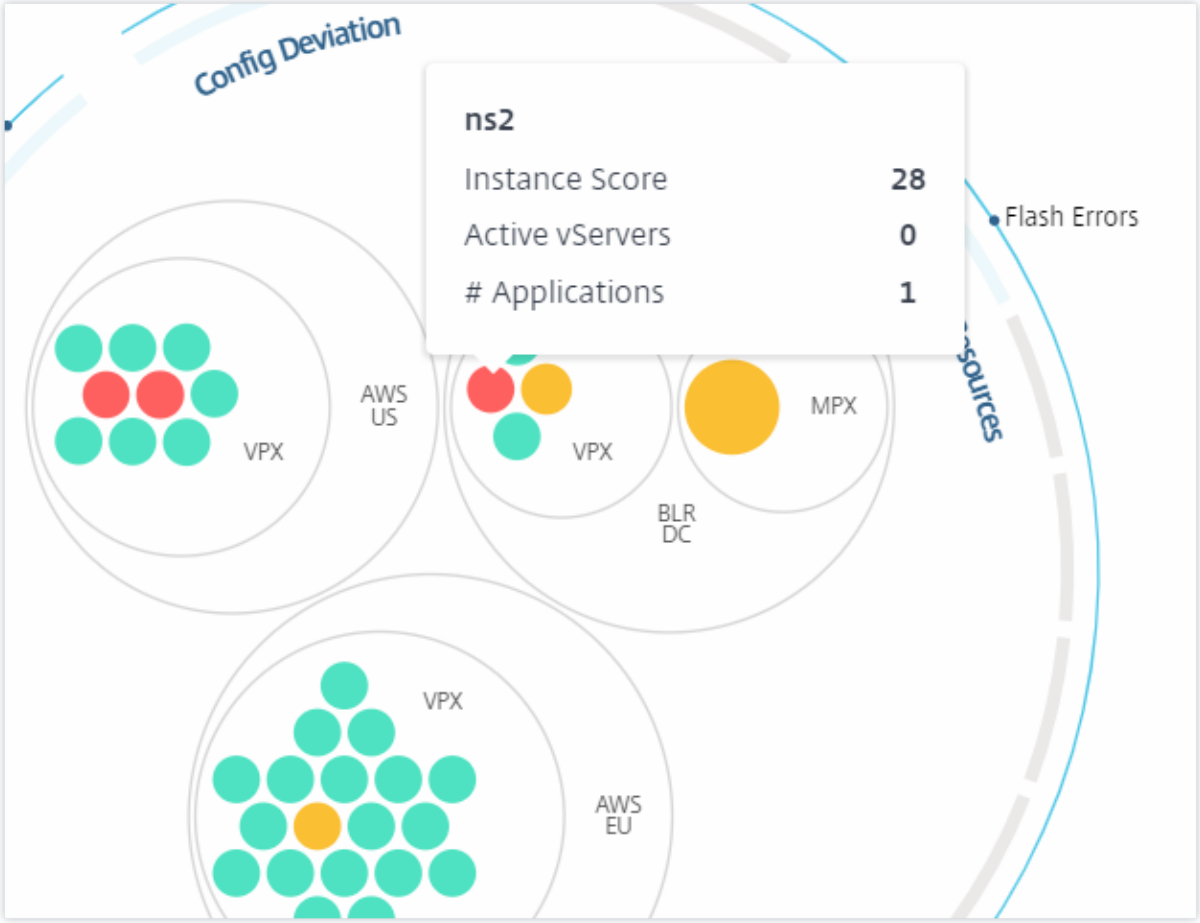
颜色。每个实例在圆形包中以彩色圆形表示。圆的颜色表示该实例的运行状况。

- 绿色 -实例得分介于 100 到 80 之间。实例运行状况良好。
- 黄色 -实例得分介于 80 到 50 之间；有些问题已被注意到，需要审核。
- 红色 -实例得分低于 50。实例处于关键阶段，因为在该实例上注意到多个问题。



尺寸。这些彩色圆圈的大小表示在该实例上配置的虚拟服务器的数量。圆圈越大表示虚拟服务器数量越多。

您可以将鼠标指针悬停在每个实例圆（彩色圆圈）上以查看摘要。悬停工具提示显示实例的主机名、活动虚拟服务器的数量以及在该实例上配置的应用程序的数量。

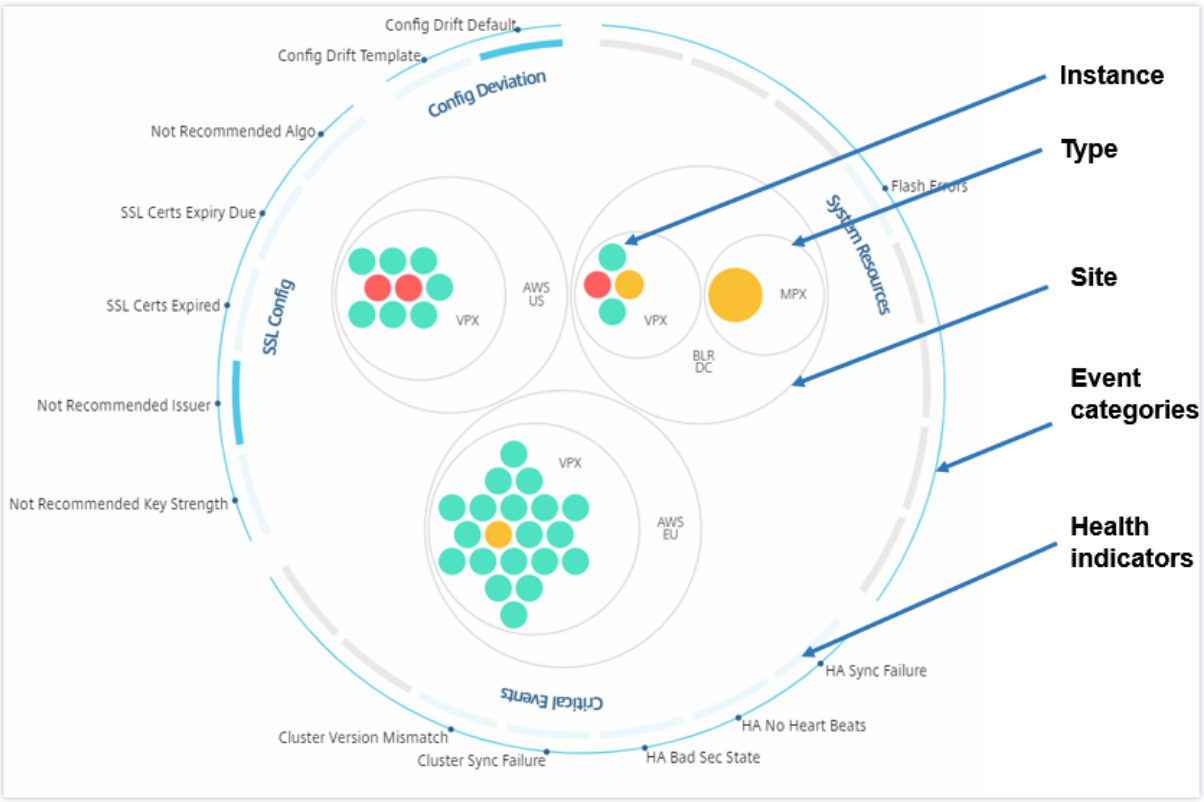


分组实例圆

Circle Pack 在开始时包含基于以下条件在另一个圆中分组、嵌套或打包的实例圆：

- 部署它们的站点
- 部署的实例类型-VPX、MPX、SDX 和 CPX
- ADC 实例的虚拟或物理模型
- 实例上安装的 ADC 映像版本

下图显示了 Circle Pack，其中实例首先按部署实例的站点或数据中心进行分组，然后根据实例的类型 VPX 和 MPX 进一步分组。

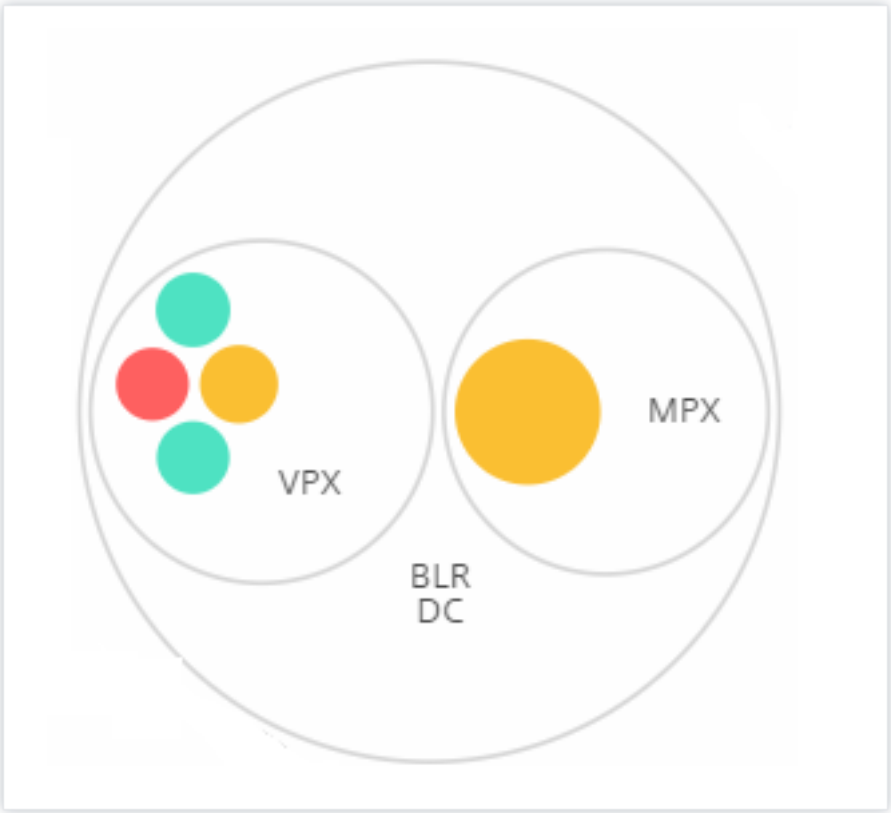


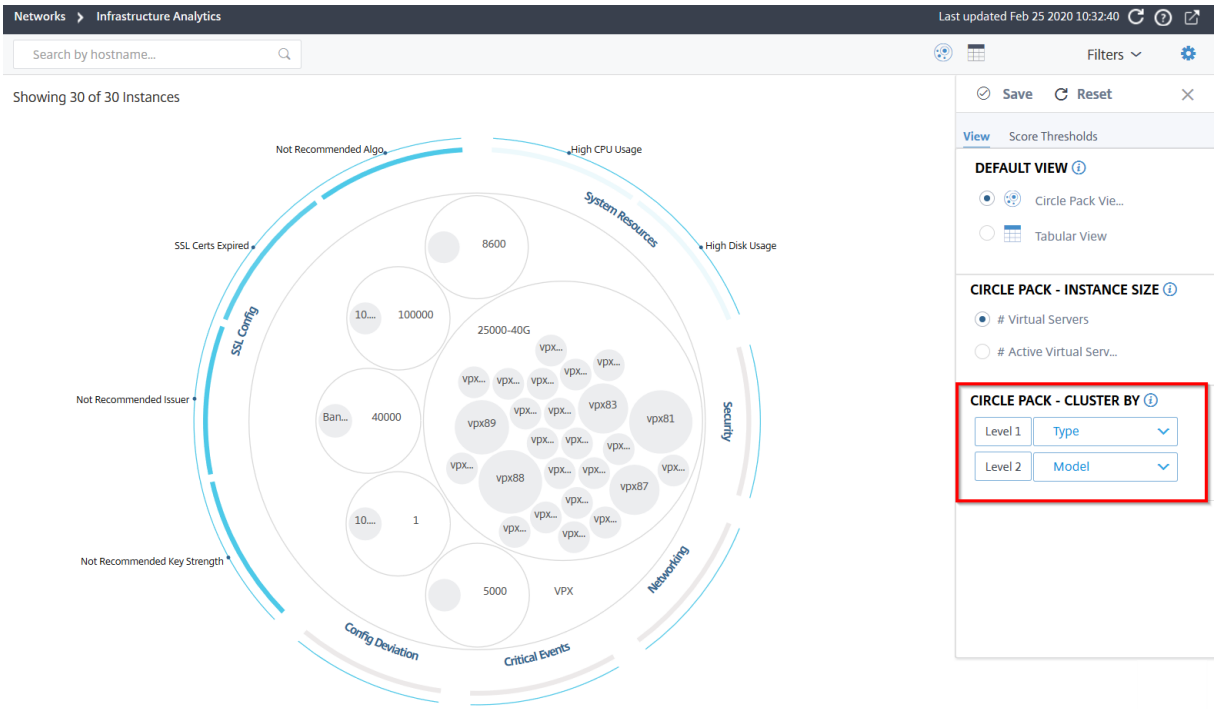
所有这些嵌套圆圈都由两个最外面的圆圈界限。外部两个圆表示 Citrix ADM 监视的四类事件（系统资源、关键事件、SSL 配置和配置偏差）和贡献的运行状况指标。

群集实例圆圈

Citrix ADM 监视许多实例。为了简化对这些实例的监视和维护，基础设施分析允许您将它们分为两个级别进行群集。也就是说，实例分组可以嵌套在另一个分组中。

例如，BLR 数据中心有两种类型的 ADC 实例-VPX 和 MPX，部署在其中。您可以首先按类型对 ADC 实例进行分组，然后按其分组的站点对所有实例进行分组。现在，您可以轻松识别在您管理的站点中部署了多少类型的实例。

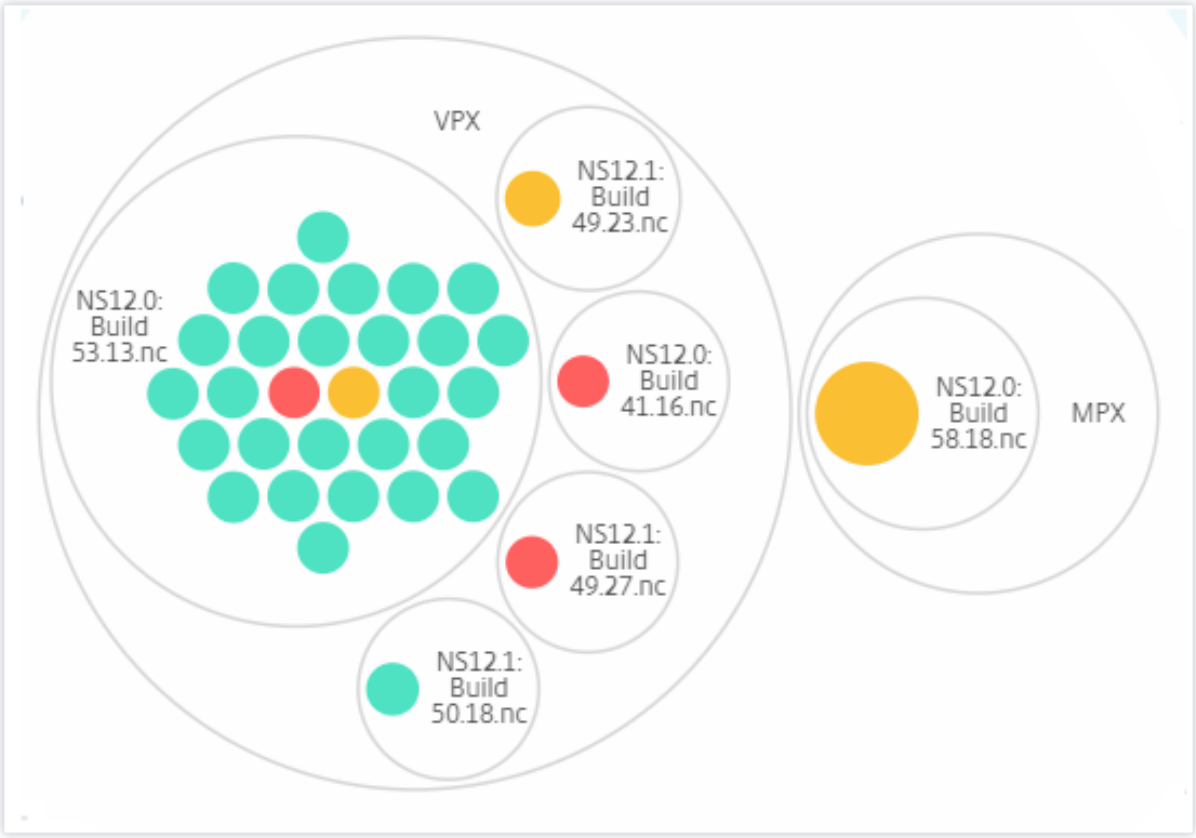




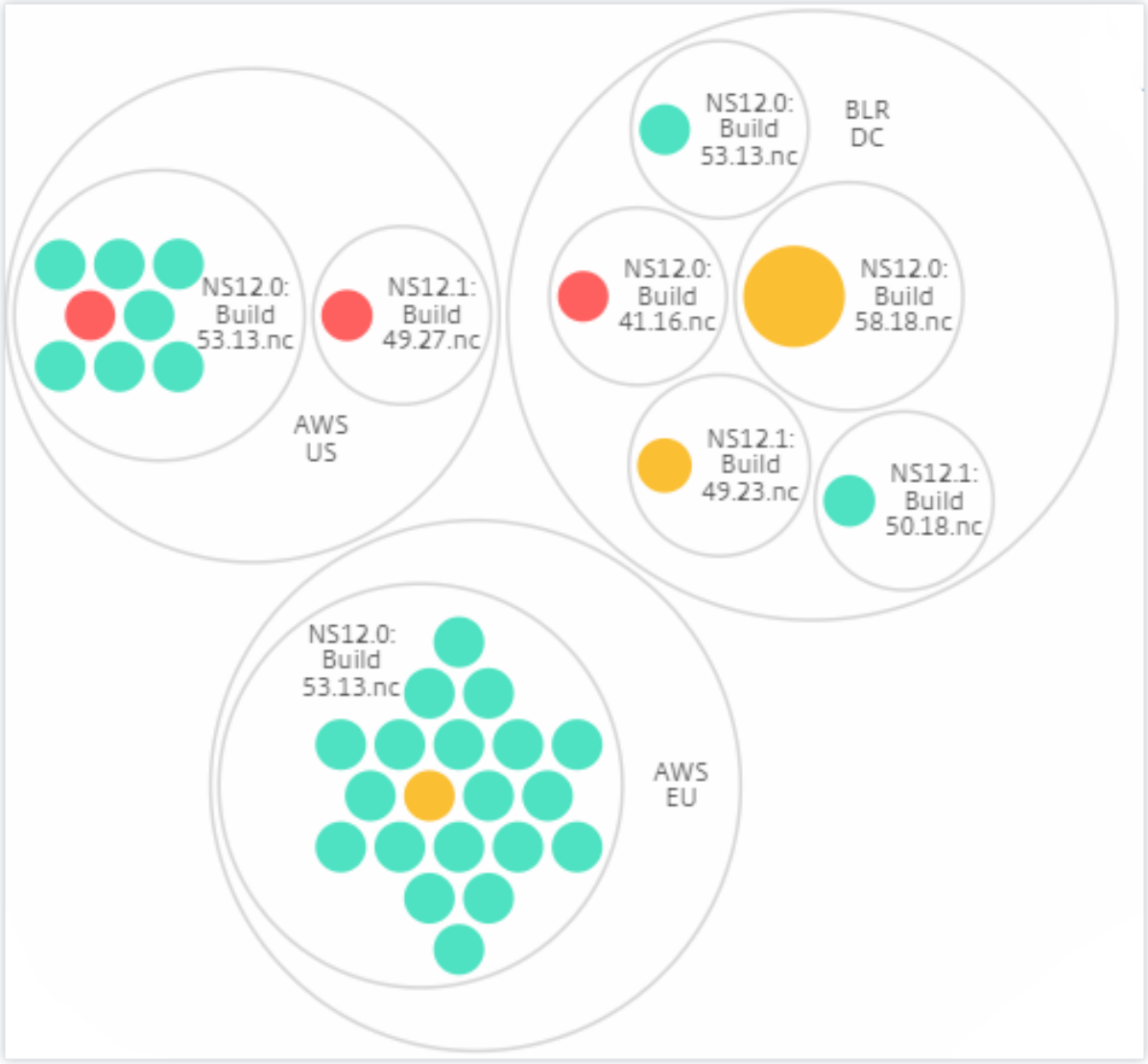
两级聚类的其他几个示例如下：

站点和型号：

类型和版本：

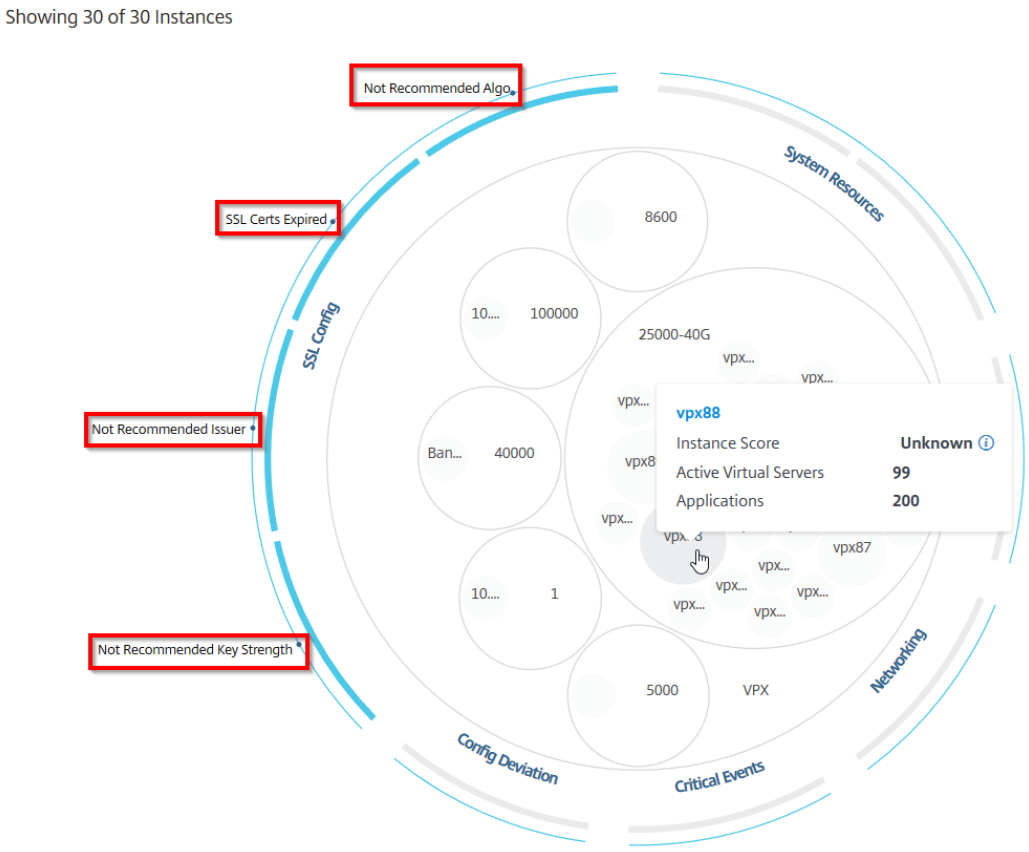


站点和版本：



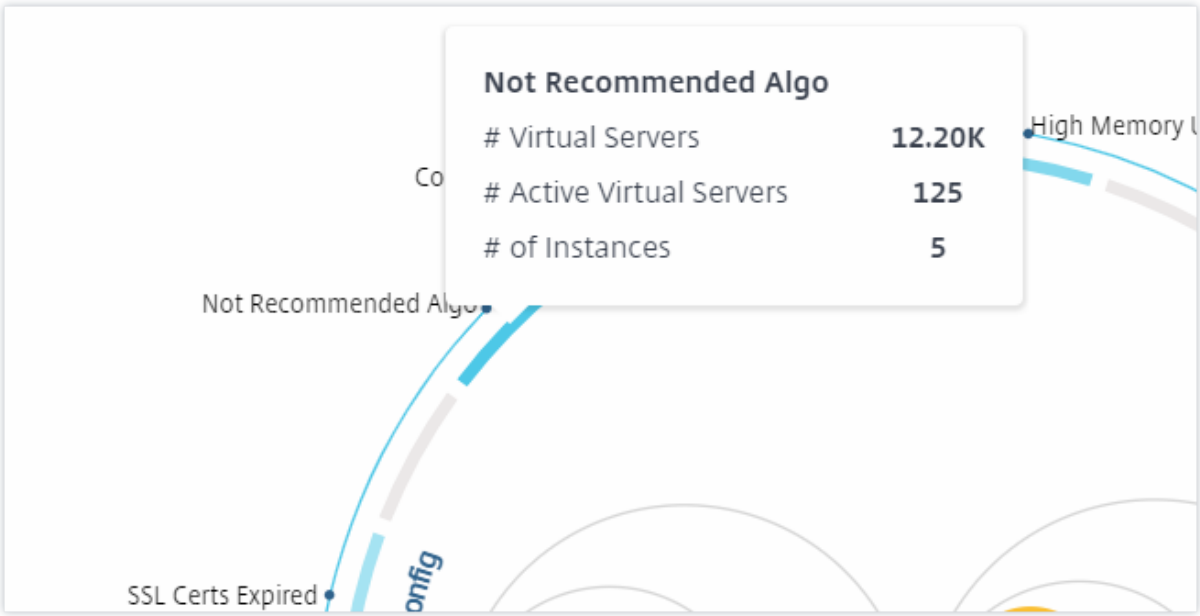
如何使用圆形包

单击每个彩色圆圈以突出显示该实例。



根据在这种情况下发生的事件，只有这些健康指标在外圈突出显示。例如，以下两个 Circle Pack 图像显示不同的风险指标集，尽管这两个实例都处于严重状态。

您还可以单击运行状况指标以获取有关报告该风险指标的实例数量的更多详细信息。例如，单击 `Not recommended Algo` 查看该风险指标的摘要报告。

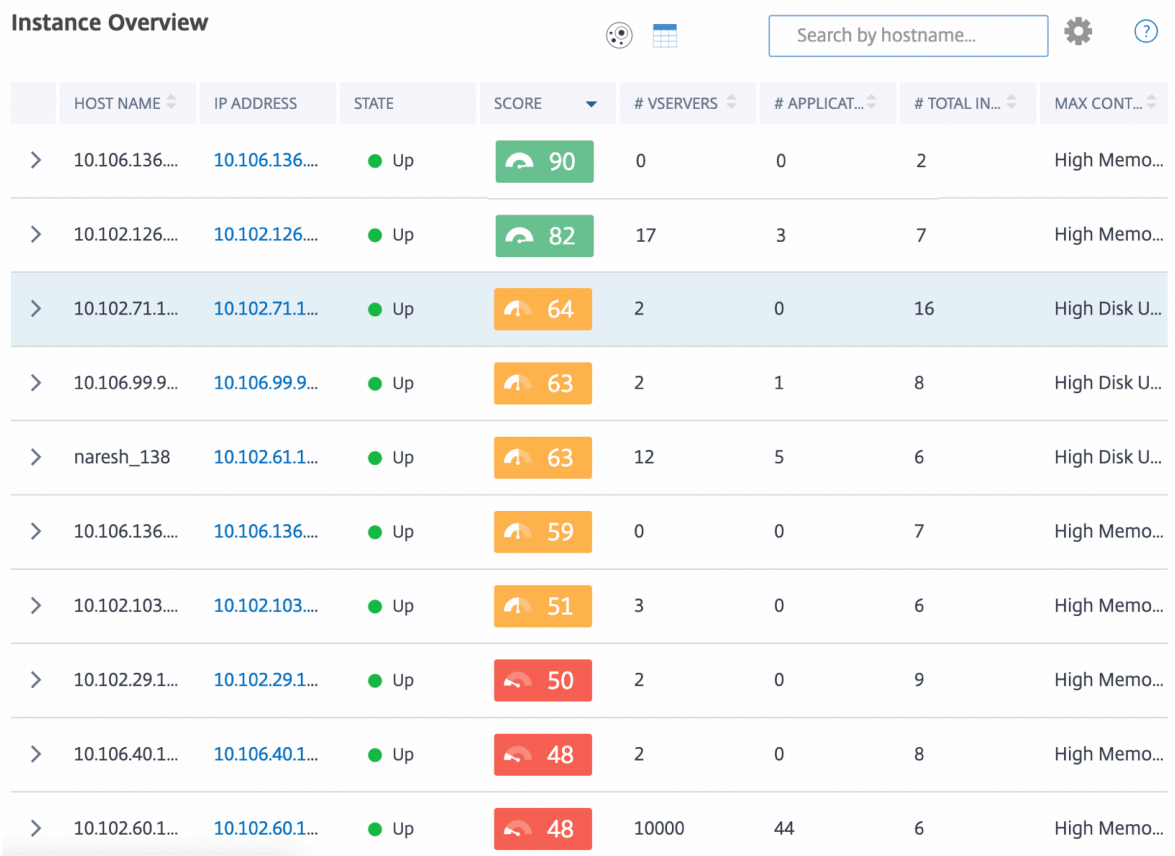


表格视图

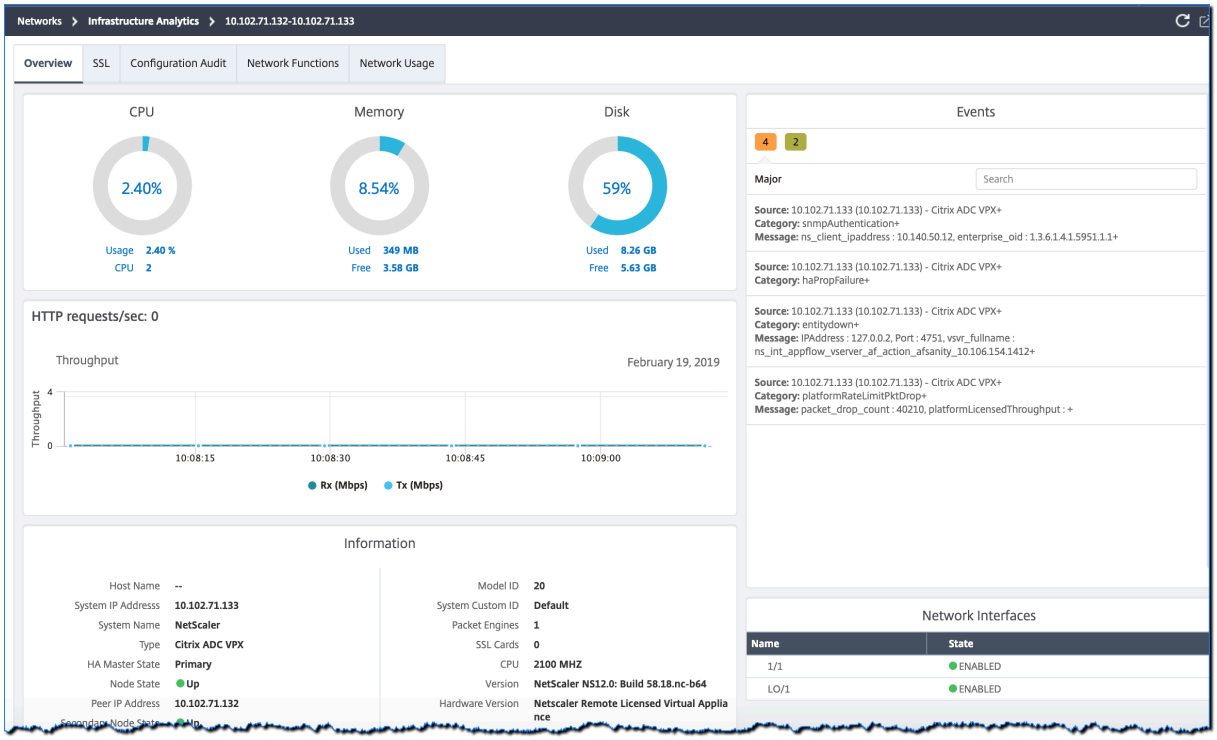
表格视图以表格格式显示实例和这些实例的详细信息。显示的详细信息如下所示：

- 实例的主机名
- 实例的 IP 地址
- 实例的状态
- 实例分数
- 在该实例上配置的虚拟服务器数量
- 在该实例上配置的应用程序数
- 风险指标总数
- 对降低实例得分作出更大贡献的事件

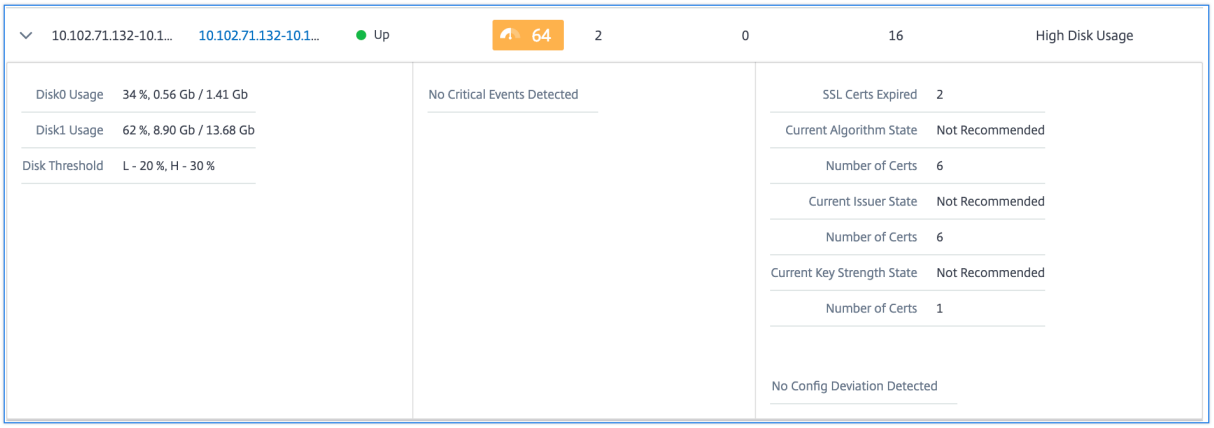
处于临界状态的实例位于表的顶部，其次是需要审核的实例，然后是更健康的实例。



单击表格视图中的实例 IP 地址，以显示控制板的形式查看该实例的更多详细信息。实例控制板显示了实例的概述，您可以在其中查看实例的 CPU、内存和磁盘使用情况。您还可以查看与 SSL 证书管理、配置审核、网络功能和显示实例详细网络使用情况的网络报告相关的详细信息。进一步向下滚动以查看在此实例上启用的功能和模式的列表。



您还可以单击每行开头的箭头以展开该行以了解更多详细信息。



展开的表格行显示所有类别的实例上发生的错误。在上面的示例中，您可以查看系统资源、SSL 配置和配置文件中存在错误。但实例没有报告任何关键事件。

如何使用摘要面板

摘要面板可帮助您高效、快速地专注于需要审核或关键状态的实例。该面板分为三个选项卡-概述、实例信息和流量配置文件。您在此面板中所做的更改会修改“圆形包装”和“表格”视图格式的显示。以下各节更详细地介绍了这些选项卡。以下各节中的示例可帮助您有效地使用不同的选择条件来分析实例报告的问题。

概述：

概览选项卡允许您根据实例中可能出现的硬件错误、使用情况、过期证书和类似指标来监视实例。您可以在这里监视的指标如下：

- CPU 使用率
- 内存使用率
- 磁盘使用情况
- 系统故障
- 关键事件
- SSL 证书到期

以下示例说明如何与概述面板进行交互以隔离报告错误的实例。

示例 **1**：查看处于审核状态的实例：

选中审核复选框可以仅查看未报告严重错误但仍需关注的实例。

概述面板中的“直方图”表示基于高 CPU 使用率、高内存使用率和高磁盘使用率事件的累计实例数。直方图分级为 10%、20%、30%、40%、50%、60%、70%、80%、90% 和 100%。将鼠标指针悬停在其中一个条形图上。图表底部的图例显示该范围内的使用范围和实例数。您也可以单击条形图以显示该范围内的所有实例。

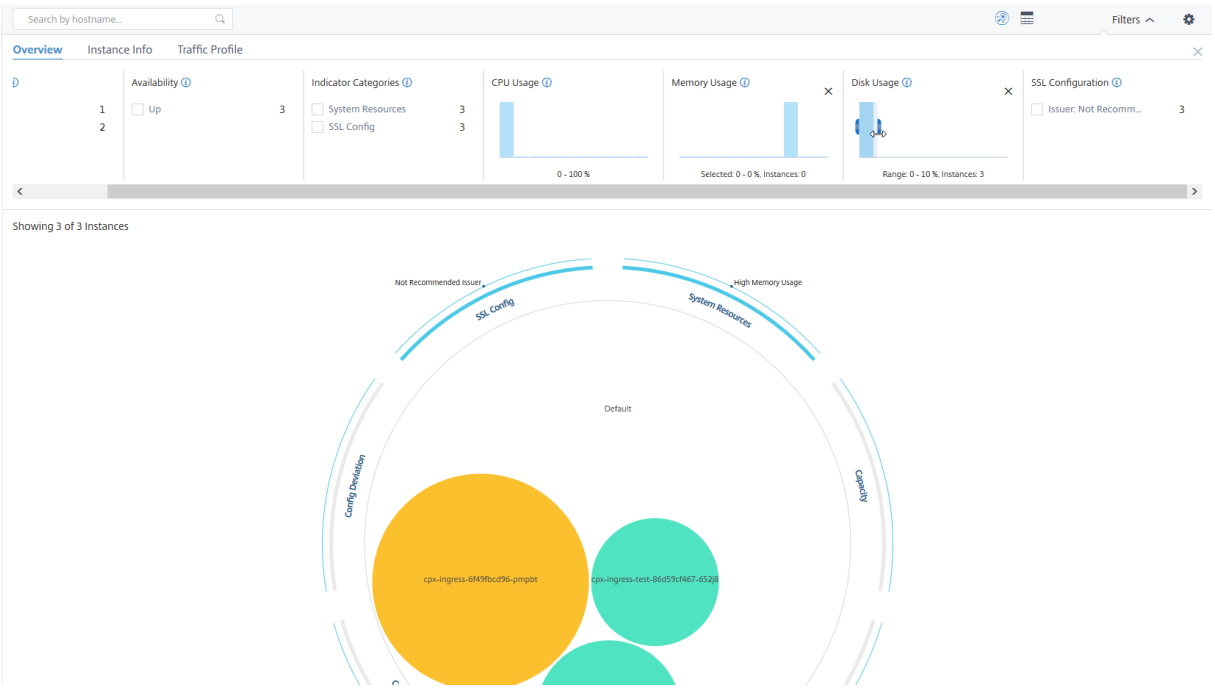
示例 **2**：查看占用分配内存的 **10%** 到 **20%** 之间的实例：

在内存使用情况部分，单击条形图。图例显示所选范围为 10 — 20%，并且有 29 个实例在该范围内运行。

您也可以在这些直方图中选择多个范围。

示例 **3**：查看在多个范围内消耗大磁盘空间的实例：

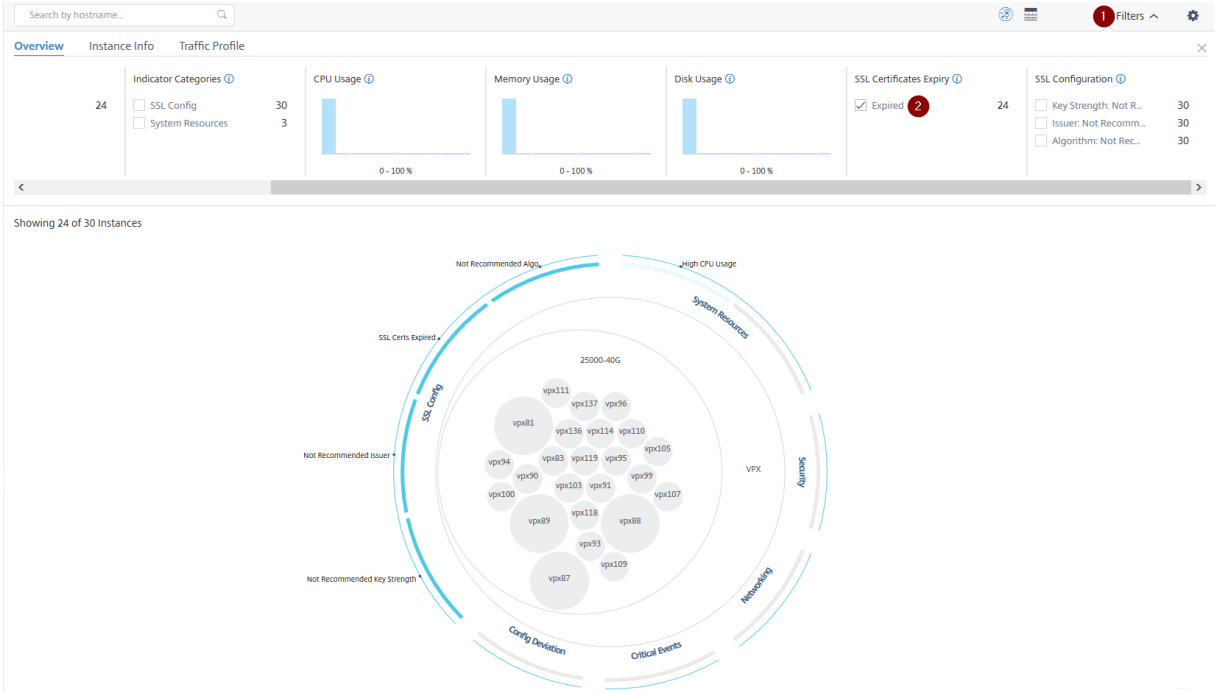
要查看已占用 0 到 10% 之间的磁盘空间的实例，请将鼠标指针拖动到这两个范围上。



> 注意
>
> 点击 “X” 删除选择内容。您也可以单击重置以删除多个选择。

概览面板中的水平条形图表示报告系统错误、严重事件和 SSL 证书到期状态的实例数。选中该复选框以查看这些实例。

示例 **4**：查看过期 **SSL** 证书的实例：



1 -单击 筛选器列表。

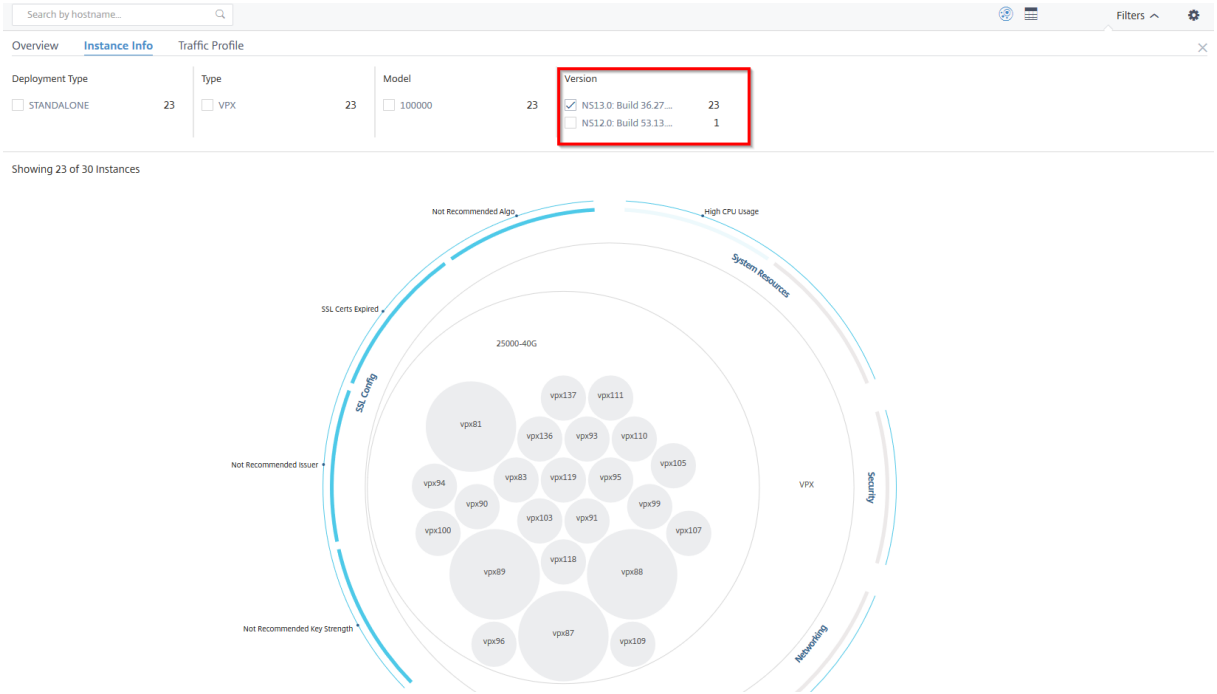
2 -在 **SSL** 证书到期部分，选中 过期复选框以查看实例。

实例信息

实例信息面板允许您根据部署类型、实例类型、型号和软件版本查看实例。您可以选中多个复选框来缩小选择范围。

示例 **5**：查看具有特定内部版本号的 **ADC VPX** 实例：

选择要查看的版本。

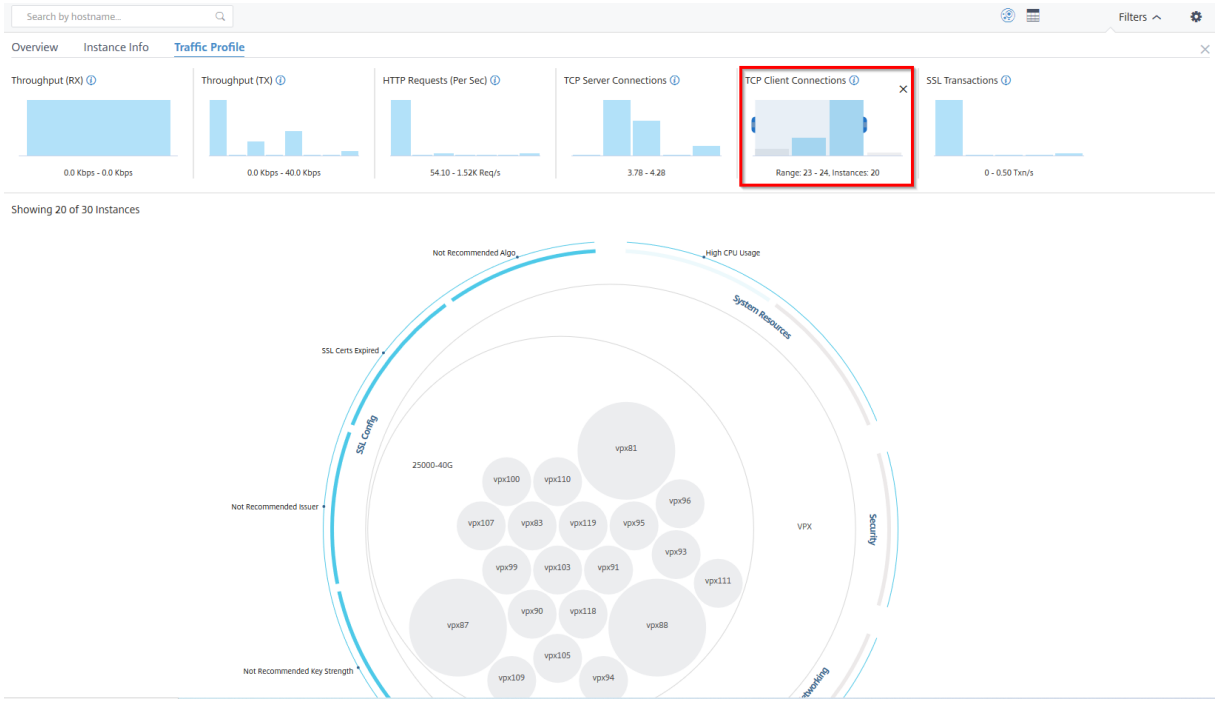


流量配置文件

流量配置文件面板中的“直方图”表示基于实例上的许可吞吐量、实例处理的请求数、连接数和事务数量的实例汇总数。选择条形图以查看该范围内的实例。

示例 **6**：查看支持 **TCP** 连接的实例：

下图显示了支持 TCP 连接的实例数。

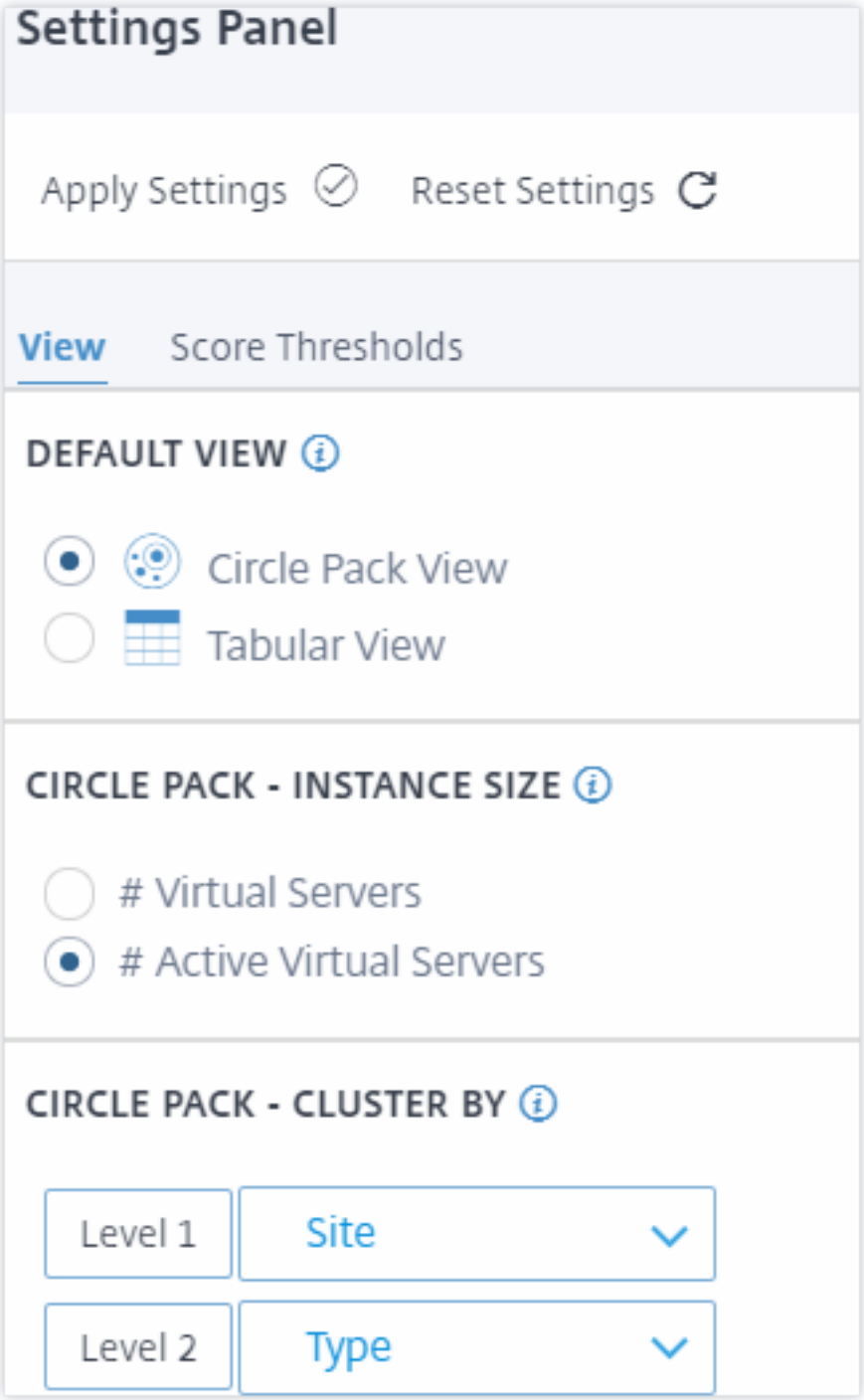


如何使用设置面板

设置面板允许您设置基础设施分析的默认视图。它还允许您为高 CPU 使用率、高磁盘使用率和高内存使用率设置低阈值和高阈值。“设置”面板分为两个选项卡-“查看”和“分数阈值”。

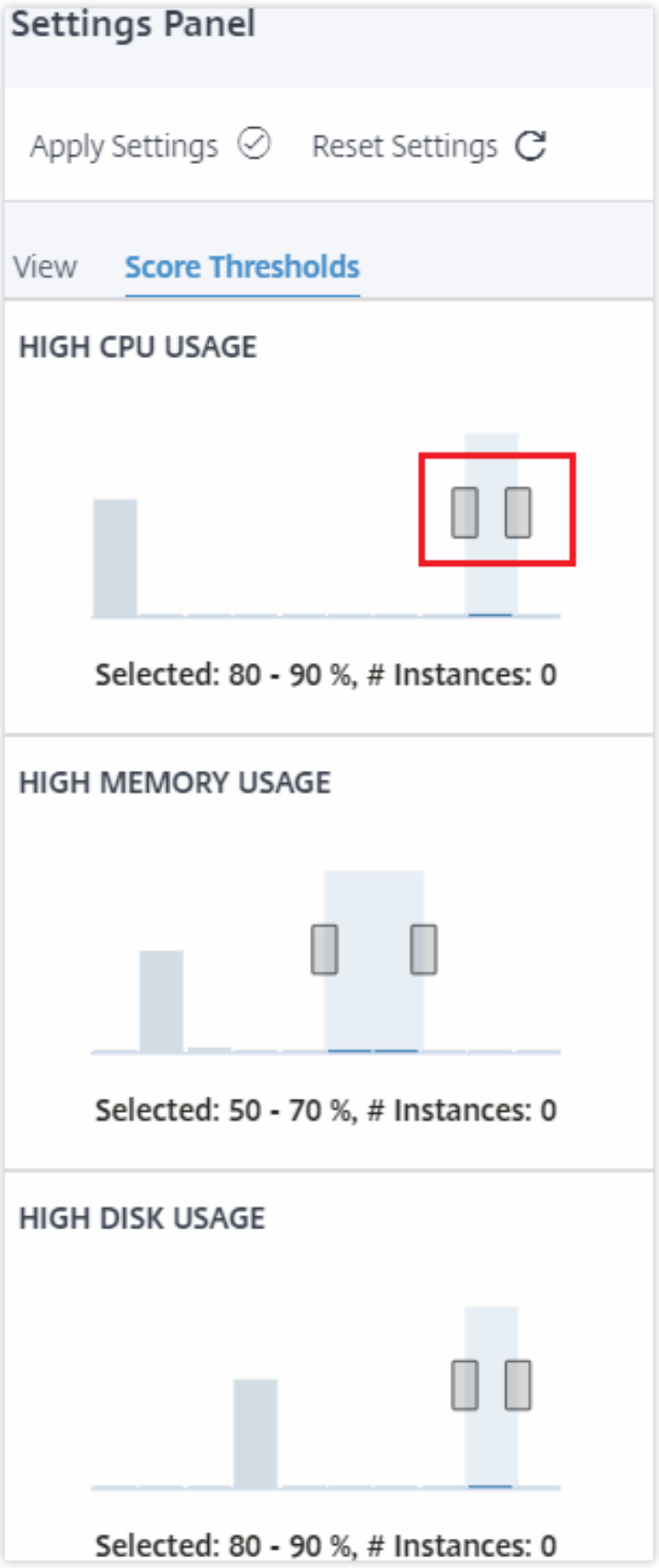
查看

- 默认视图。选择圆形包或表格格式作为分析页面上的默认视图。您选择的格式是在 Citrix ADM 中访问页面时看到的格式。
- 圆形包-实例大小。通过虚拟服务器数量或活动虚拟服务器数量，允许实例圆的大小。
- 圆包-群集通过. 确定实例圆的两级聚类。有关实例群集的详细信息，请参阅群集实例圈。



分数阈值

您可以根据组织中的流量要求修改高 CPU、内存和磁盘使用率的低阈值和高阈值。拖动每个选择直方图中的控制柄以设置值。



> 注意
>
> 单击应用设置以应用这些更改，或单击重置以删除所有更改。

如何在控制板上显示数据

使用基础架构分析，网络管理员现在可以在几秒钟内识别需要最多关注的实例。为了更详细地了解数据可视化，让我们考虑 Chris 的情况，Explecompany 的网络管理员。

克里斯在组织中维护了许多 Citrix ADC 实例。其中一些实例处理高流量，Chris 需要密切监控它们。Chris 注意到，一些高流量实例不再处理通过它们的完整流量。为了分析这种减少，早些时候，Chris 不得不读取来自各种来源的多个数据报告。Chris 不得不花更多的时间尝试手动关联数据，并确定哪些实例不处于最佳状态，需要关注。

Chris 使用基础架构分析功能以直观方式查看所有实例的运行状况。

以下两个示例说明了基础架构分析如何帮助 Chris 进行维护活动：

示例 **1-**要监视 **SSL** 流量，请执行以下操作：

Chris 在 Circle Pack 上注意到，一个实例的实例分数较低，并且该实例处于“严重”状态。Chris 单击该实例以查看问题是什么。实例摘要显示该实例上存在 SSL 卡故障，并且实例无法处理 SSL 流量（SSL 流量已减少）。Chris 提取这些信息，并向团队发送一份报告，以便立即调查问题。

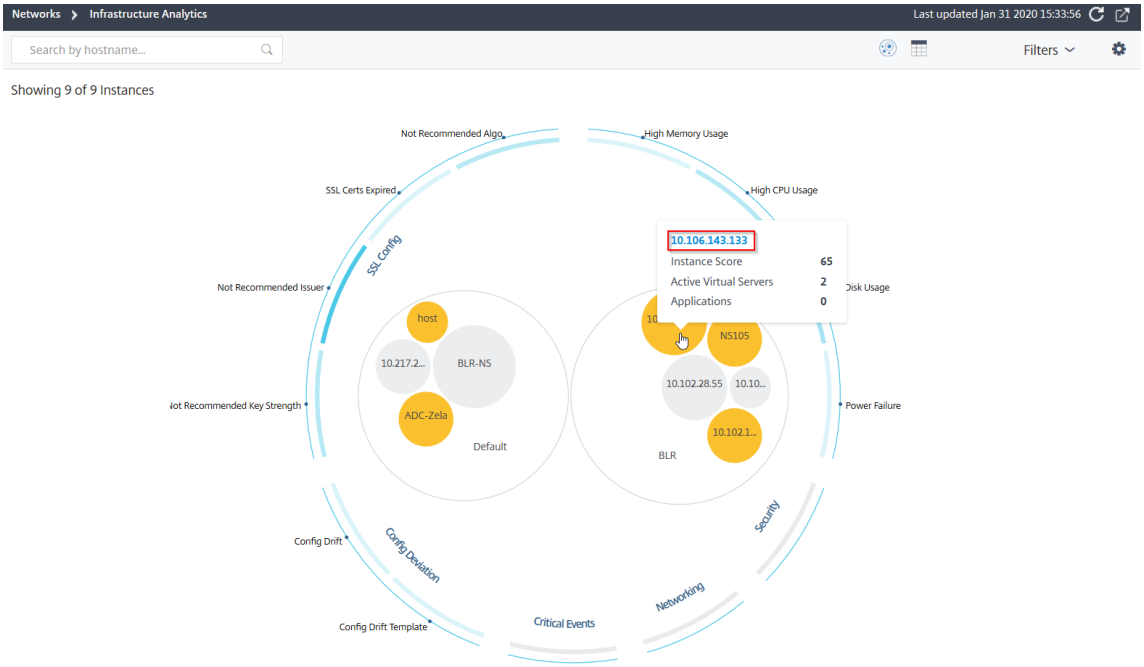
示例 **2-**要监视配置更改：

Chris 还注意到另一个实例处于“审查”状态，并且最近出现了配置偏差。当 Chris 单击配置偏差风险指示器时，Chris 注意到 RC4 密码、SSL v3、TLS 1.0 和 TLS 1.1 相关的配置更改可能是由于安全问题。Chris 还注意到此实例的 SSL 事务流量配置文件已关闭。Chris 导出此报告并将其发送给管理员进一步查询。

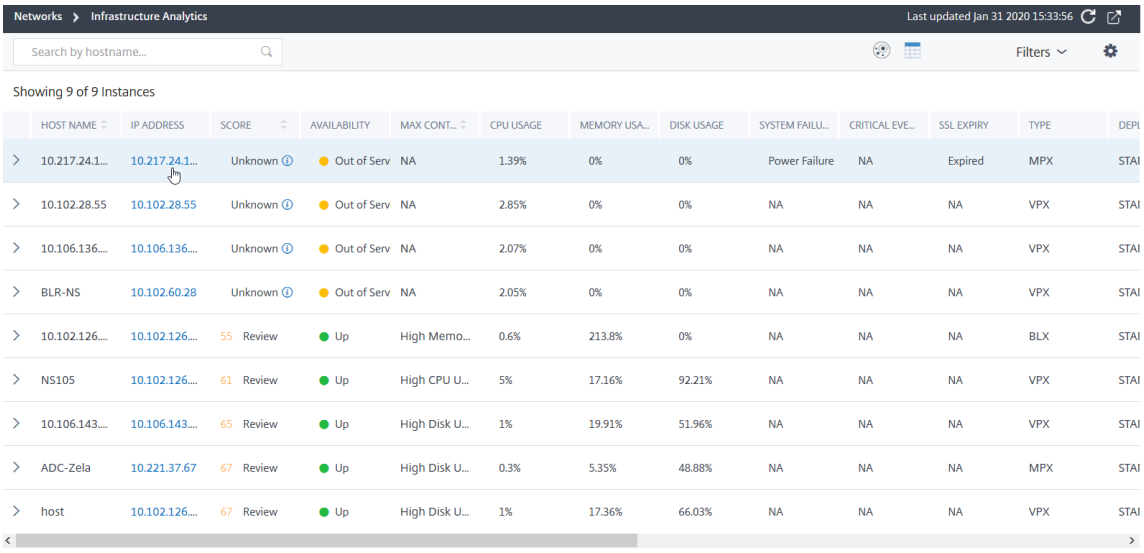
在基础架构分析中查看实例详细信息

April 23, 2021

1. 导航至“ 网络” > “ 基础架构分析”
2. 单击圆包视图并选择 IP 地址。



您也可以从表视图中单击 IP 地址。

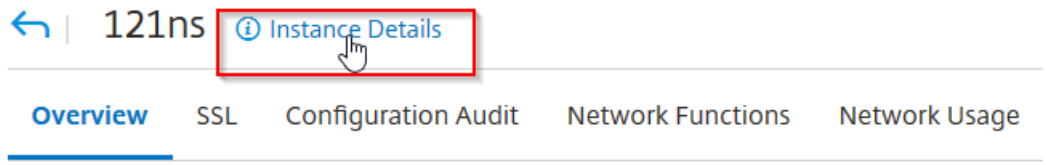


- 主机名 — 表示分配给 ADC 实例的主机名
- **IP** 地址 — 表示 ADC 实例的 IP 地址
- 分数 **—** 表示 ADC 实例得分和状态，如“严重”、“良好”和“公平”
- 可用性 — 表示 ADC 实例的状态，如“ 启动”、“关 闭”或“停 止服务”。
- 最大贡献 — 表示 ADC 实例具有最大错误计数的问题类别。
- **CPU** 使用率 — 表示实例使用的当前 CPU%
- 内存使用情况 — 表示实例使用的当前内存百分比

- 磁盘使用率 — 表示实例使用的当前磁盘百分比
- 系统故障 — 表示实例系统的错误总数
- 严重事件 — 表示 Citrix ADC 实例具有最大事件的事件类别
- **SSL** 过期 — 表示 ADC 实例上安装的 SSL 证书的状态
- 类型 — 表示 ADC 实例类型，如 VPX、SDX、MPX 或 CPX
- 部署 — 表示 ADC 实例是作为独立实例还是高可用性对部署
- 型号 — 表示 ADC 实例型号
- 版本 — 表示 ADC 实例版本和内部版本号
- 吞吐量 — 表示来自 ADC 实例的当前网络吞吐量
- **HTTPS** 请求/秒 — 表示 ADC 实例收到的当前 HTTPS 请求/秒
- **TCP** 连接 — 表示当前已建立的 TCP 连接
- **SSL** 事务 — 表示 ADC 实例处理的当前 SSL 事务
- 站点 — 表示部署 ADC 实例的站点的名称。

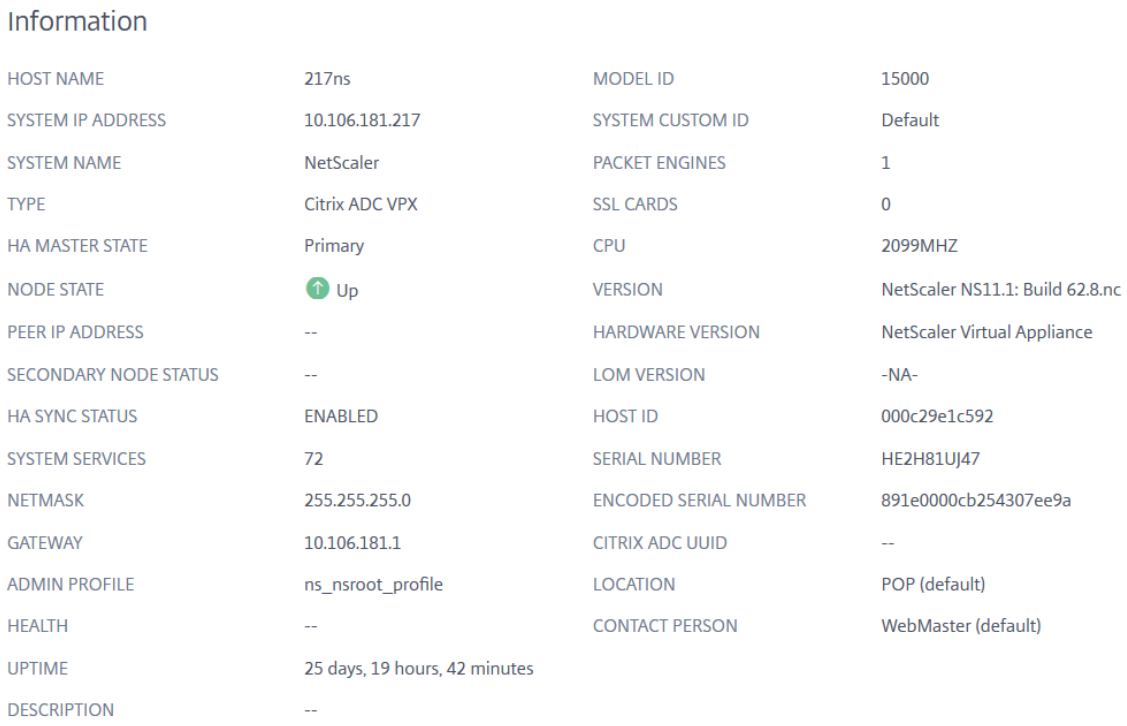
> 注意
>
> 每 5 分钟更新 CPU 使用率、内存使用率、磁盘使用率、吞吐量等当前值。

单击 “ 实例详细信息” 以查看详细信息。

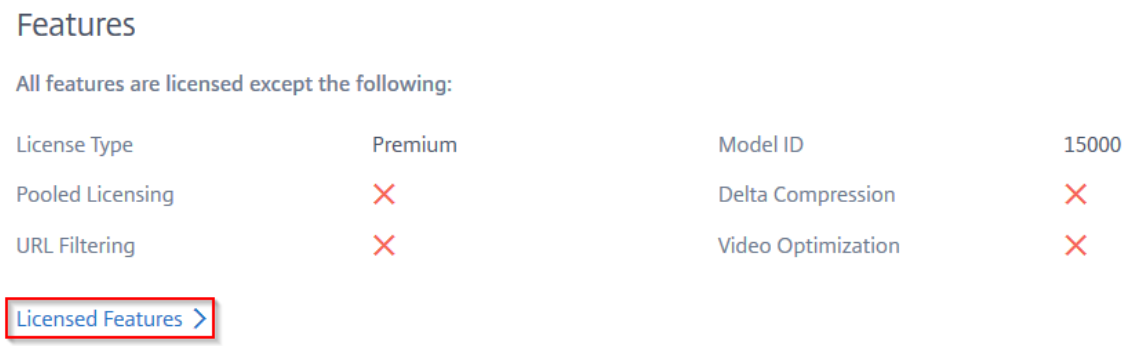


将显示以下详细信息：

- 信息 -实例详细信息，如实例类型、部署类型、版本、型号。



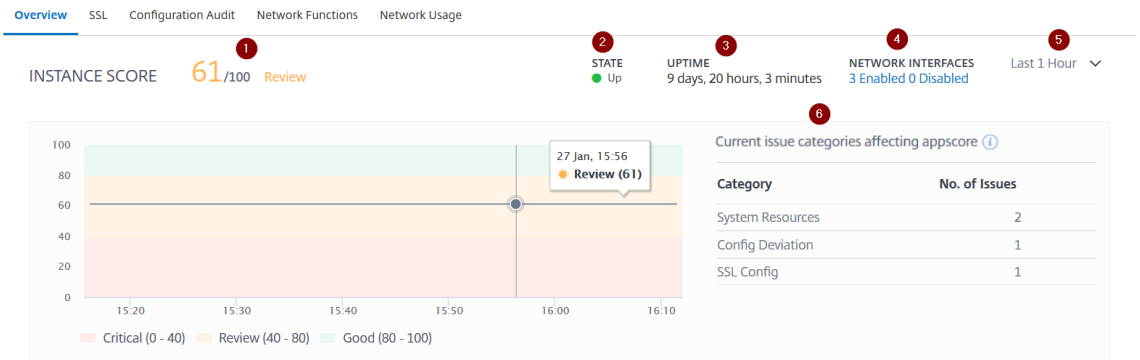
- 功能 — 默认情况下，显示未获许可的功能。单击 “ 许可功能” 以查看已许可的功能。



- 模式 — 默认情况下，将显示在实例上禁用的所有模式。单击 查看启用模式可查看实例上已启用的模式。

实例仪表板显示实例概述，您可以在其中查看以下详细信息：

- 实例分数

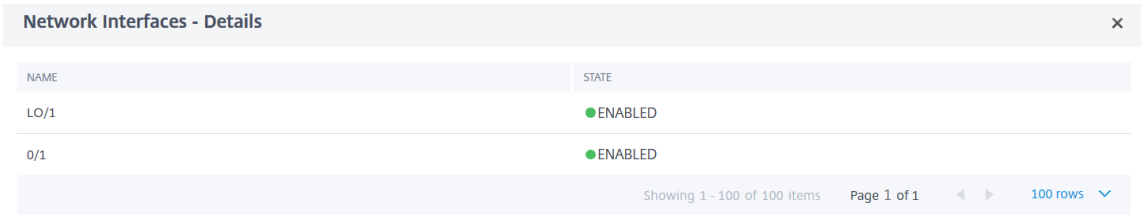


1 — 表示所选时间持续时间内的当前 Citrix ADC 实例得分。最终得分计算为 **100** 减去总处罚。图形显示选定时间持续时间的分数范围。

2 — 表示 Citrix ADC 实例的状态，例如 “ 启动”、“ 关闭” 和 “不服务”。

3 — 表示 Citrix ADC 实例启动并运行的持续时间。

4 — 表示为实例启用和禁用的网络接口总数。单击查看详细信息，如网络接口名称和状态（已启用或已禁用）。



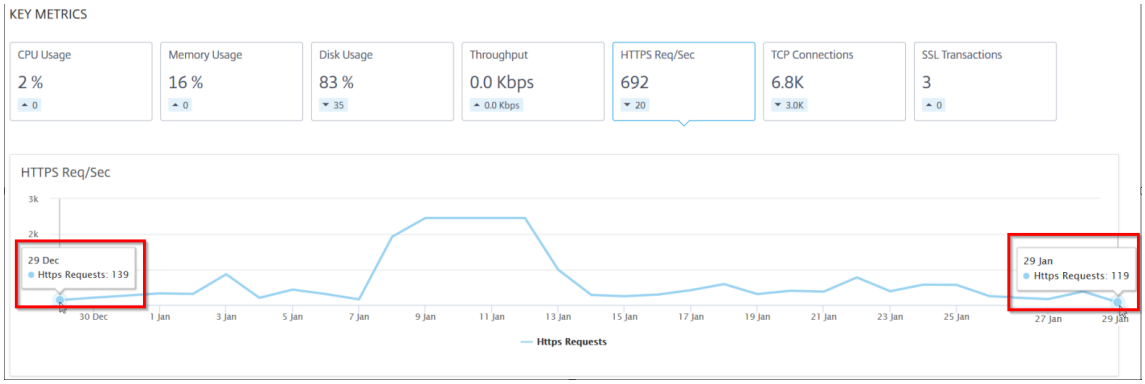
5 — 从列表中选择时间持续时间以查看实例详细信息。

6 — 显示 ADC 实例的总问题和问题类别。

- 关键指标

  单击每个选项卡以查看详细信息。在每个指标中，您可以查看所选时间的平均值和差值。

  下图是 HTTPS 请求/秒的示例，所选时间持续时间为 1 小时。值 **692** 是 1 个月持续时间内的平均 HTTPS 请求/秒，值 **20** 是差值。在图形中，第一个值为 **139** ，最后一个值为 **119**。差值为 **139-119 = 20**。



  您可以在所选时间持续时间内以图形格式查看以下实例指标：

  - **CPU** 使用率 — 在所选持续时间内实例的平均 CPU%（对于数据包 CPU 和管理 CPU 都显示）。
  - 内存使用率 — 在选定持续时间内实例的平均内存使用率%。
  - 磁盘使用率 — 选定持续时间内实例的平均磁盘空间%。
  - 吞吐量 — 实例在所选持续时间内处理的平均网络吞吐量。
  - **HTTPS** 请求/秒 — 实例在所选持续时间内收到的平均 HTTPS 请求。
  - **TCP** 连接 — 客户端和服务器在所选持续时间内建立的平均 TCP 连接。
  - **SSL** 事务 — 实例在所选持续时间内处理的平均 SSL 事务。

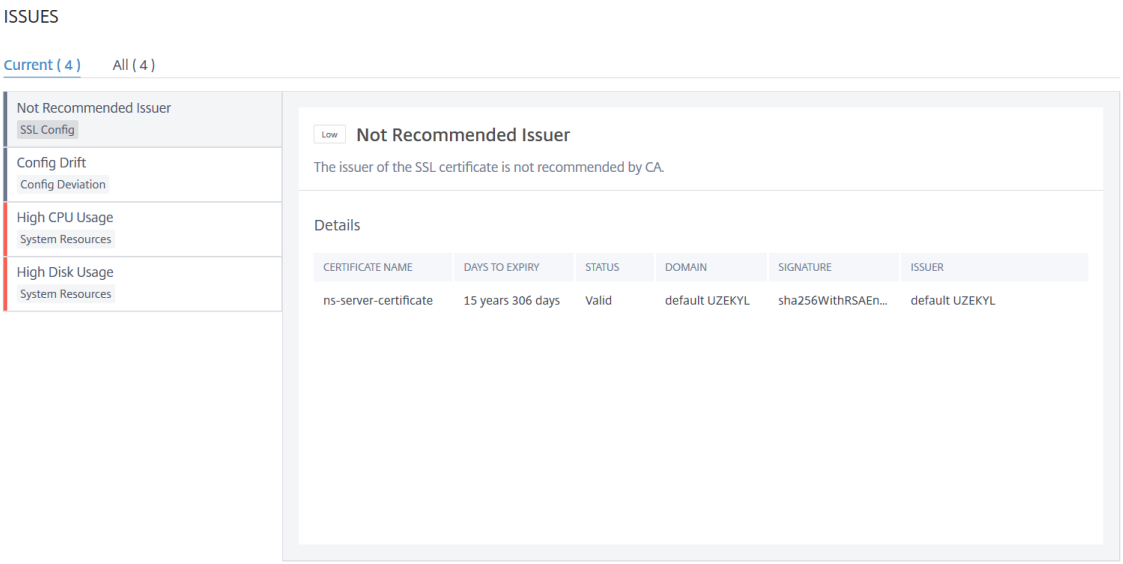
- 问题

  您可以查看 Citrix ADC 实例中出现的以下问题：

问题类别	说明	问题
系统资源	显示与 Citrix ADC 系统资源相关的所有问题，如 CPU、内存、磁盘使用情况。	- 高 CPU 使用率
		- 高内存使用率
		- 高磁盘使用率
		- SSL 卡故障
		- 电源故障
		- 磁盘错误

问题类别	说明	问题
		- 闪光错误
		- 网卡丢弃
SSL 配置	显示与 Citrix ADC 实例上的 SSL 配置相关的所有问题。	-SSL 证书已过期
		- 不推荐发行人
		- 不推荐算法
		- 不推荐密钥强度
配置偏差	显示与 Citrix ADC 实例中应用的配置作业相关的所有问题。	-配置漂移
		- 运行与模板
关键事件	显示与在 HA 对和群集中配置的 Citrix ADC 实例相关的所有关键事件。	- 群集道具失败
		- 群集同步失败
		- 群集版本不匹配
		- HA 坏坏的辅助状态
		- HA 无热节拍
		- HA 同步失败
		- HA 版本不匹配
网络连接	显示实例中出现的操作问题。	有关详细信息，请参阅使用新指标增强的基础架构分析。

单击每个选项卡以分析问题并进行故障排除。例如，假设某个实例在所选时间持续时间内存在以下错误：



- “当 前”选项卡显示当前影响实例分数的问题。
- “ 全部”选项卡显示在选定持续时间内检测到的所有问题。

查看 **ADC** 实例中的容量问题

April 23, 2021

当 ADC 实例消耗了其大部分可用容量时，处理客户端流量时可能会丢包。此问题会导致 ADC 实例中的性能低。通过了解此类 ADC 容量问题，您可以主动分配额外的许可证，以稳定 ADC 性能。

在 **Circle Pack View** 中，您可以查看 ADC 实例容量问题（如果存在）。

要查看 ADC 容量问题，请

1. 导航到 **“网络” > “基础架构分析”**。
2. 选择圆包视图。

下图表明选定实例中存在容量问题：

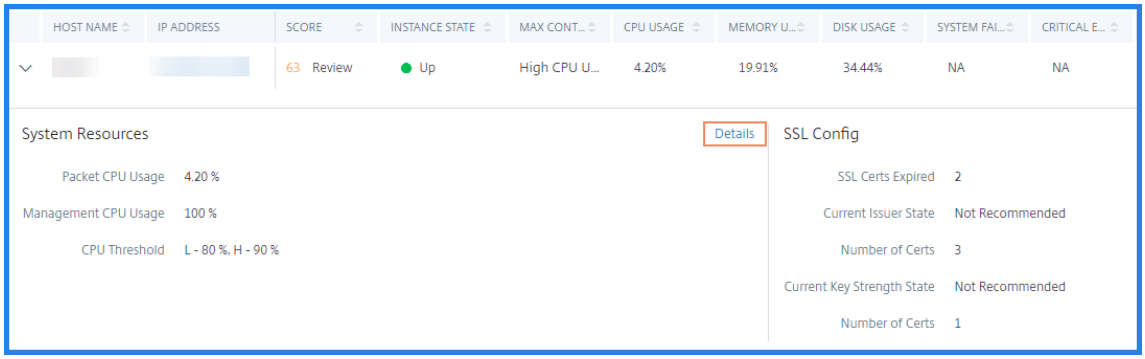
这些问题按以下容量参数进行分类：

- 达到吞吐量限制 — 达到吞吐量限制后在实例中丢弃的数据包数。
- 已达到 **PE CPU** 限制-达到 PE CPU 限制后所有网卡上丢弃的数据包数。
- 已达到 **PPS** 限制 — 达到 PPS 限制后在实例中丢弃的数据包数。
- **SSL** 吞吐率限制 — 达到 SSL 吞吐量限制的次数。
- **SSL TPS** 费率限制 — 达到 SSL TPS 限制的次数。

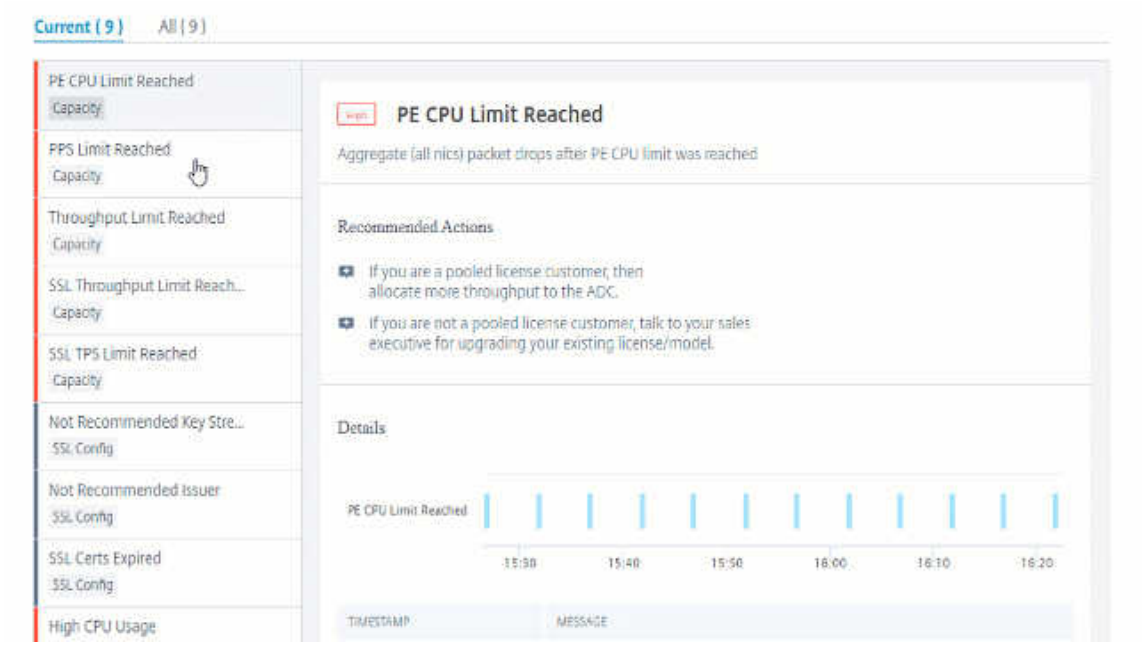
查看解决容量问题的建议操作

ADM 建议能够解决容量问题的操作。要查看建议的操作，请执行以下步骤：

1. 在 **“网络” > “**基础架构分析” 中，选择表格视图。
2. 选择存在容量问题的实例，然后单击 详细信息。



3. 在实例页面中，向下滚动到“问 题”部分。
4. 选择每个问题并查看建议的操作以解决容量问题。



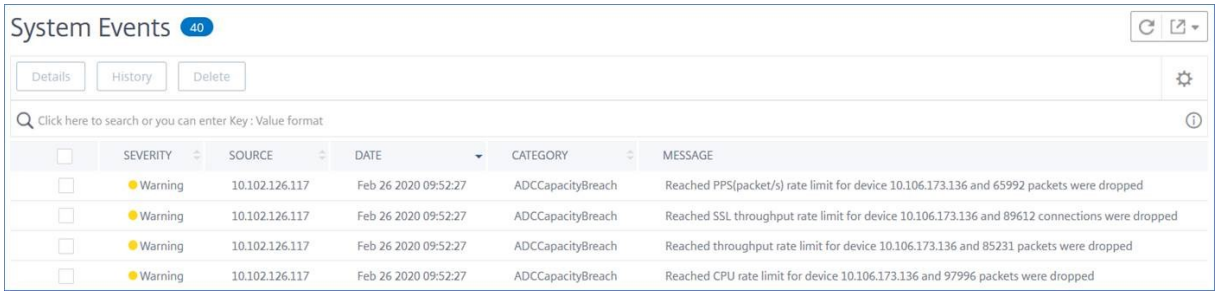
ADM 每五分钟从 ADC 实例轮询一次这些事件，并显示数据包丢失或速率限制计数器增量（如果存在）。

ADM 根据定义的容量阈值计算实例得分。

- 低阈值 — 1 个数据包丢弃或速率限制计数器增量
- 高阈值 — 10000 个数据包丢弃或速率限制计数器增量

因此，当 ADC 实例超过容量阈值时，实例得分会受到影响。

当数据包丢弃或速率限制计数器递增时，将在 `ADCCapacityBreach` 类别下生成一个事件。要查看这些事件，请导航到 **“帐户”>“系统事件”**。



使用新指标增强的基础架构分析

April 23, 2021

使用 Citrix ADM 基础架构分析，您可以执行以下操作：

- 查看 Citrix ADC 实例中出现的一组新操作问题。
- 查看错误消息并检查建议以解决问题。

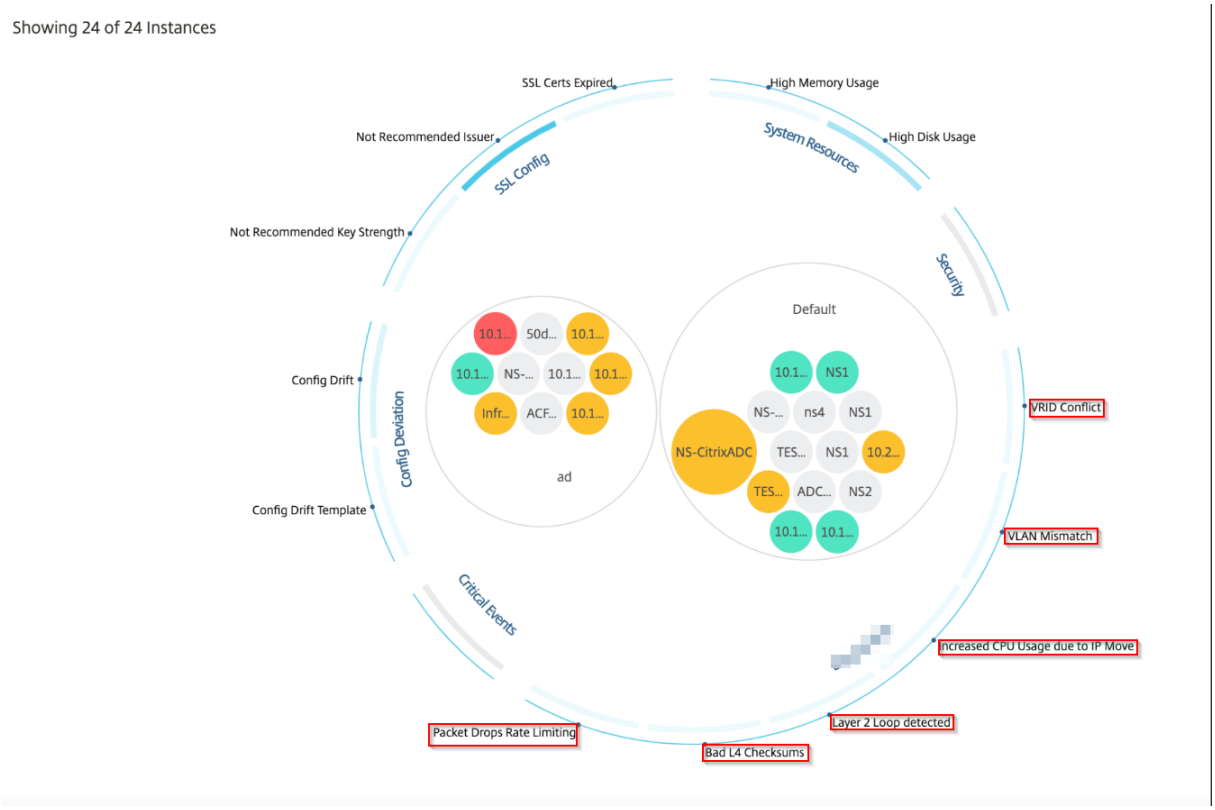
作为管理员，您可以快速识别问题的根本原因分析。

> 注意
>
> 不支持规则指示符：
>
> - 在群集模式下配置的 Citrix ADC 实例。
> - 使用管理分区配置的 Citrix ADC 实例。

在 Citrix ADM 中，导航到 网络 > 基础设施分析以查看以下指标：

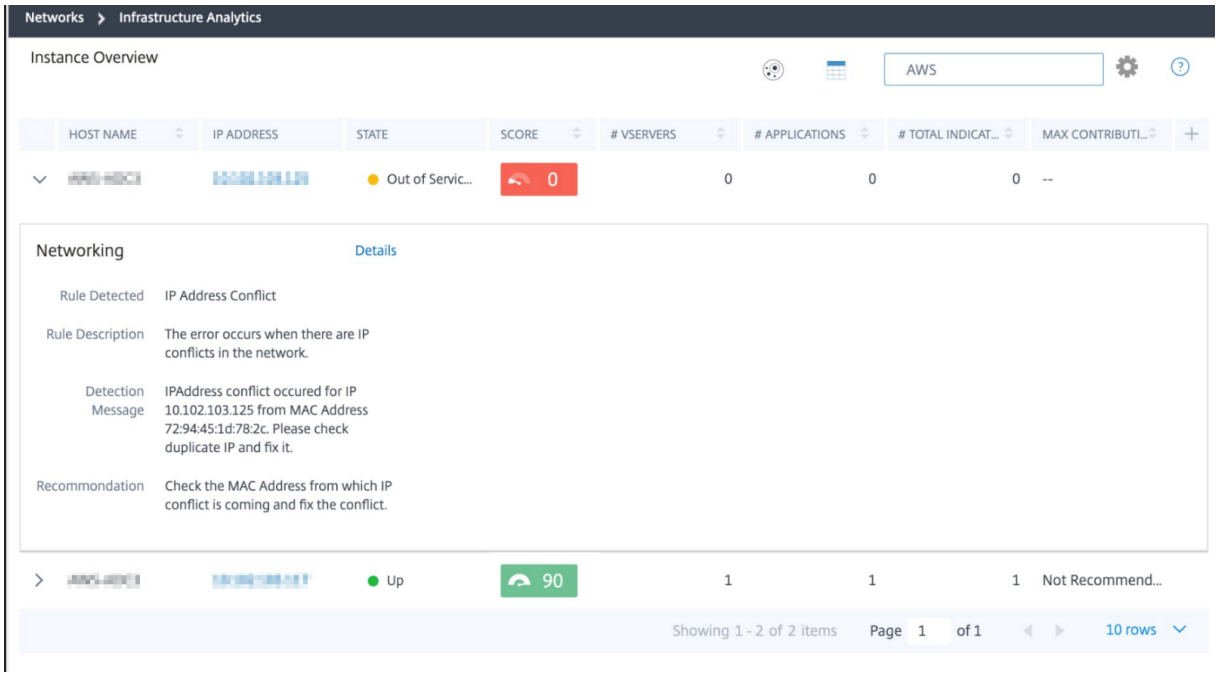
基础架构分析中的指标名称	说明
端口分配失败	检测 Citrix ADC 何时使用 SNIP 与新的服务器连接进行通信，并且该 SNIP 上的可用端口总数已耗尽。建议采取的操作是在同一子网中添加另一个 SNIP。
无默认路由配置	检测由于路由不可用而导致流量丢弃的时间。
IP 冲突	检测是否在网络中的两个或多个实例上配置或应用了相同的 IP 地址。
VRID 冲突	检测指定 VRID 何时出现间歇性访问问题。
VLAN 不匹配	检测绑定到 IP 子网的 VLAN 配置期间是否发生任何错误。
TCP 小窗口攻击	检测是否存在可能的小窗口攻击正在进行中。此警报仅供参考，因为 ADC 已经缓解了此攻击。

基础架构分析中的指标名称	说明
速率控制阈值	根据配置的速率控制阈值检测数据包何时丢弃。
持久性限制	检测何时对 Citrix ADC 内存施加最大命中值。
GSLB 站点名称不匹配	检测由于站点名称不匹配而导致 GSLB 配置同步失败的时间。
IP 标头格式不正确	检测 IPv4 数据包的完整性检查何时失败。
错误的 **L4** 校验和	检测 TCP 数据包的校验和验证何时失败。
由于 **IP** 移动而增加 **CPU** 使用率	检测是否需要更新大量的 Mac。
数据包转向过多	检测由于使用非对称 rss 密钥类型而导致的高级软件包转向。
第 **2** 层环路	检测网络中是否存在第 2 层环路。
标记 **VLAN** 不匹配	检测何时在未标记的接口上接收标记的 VLAN 数据包。



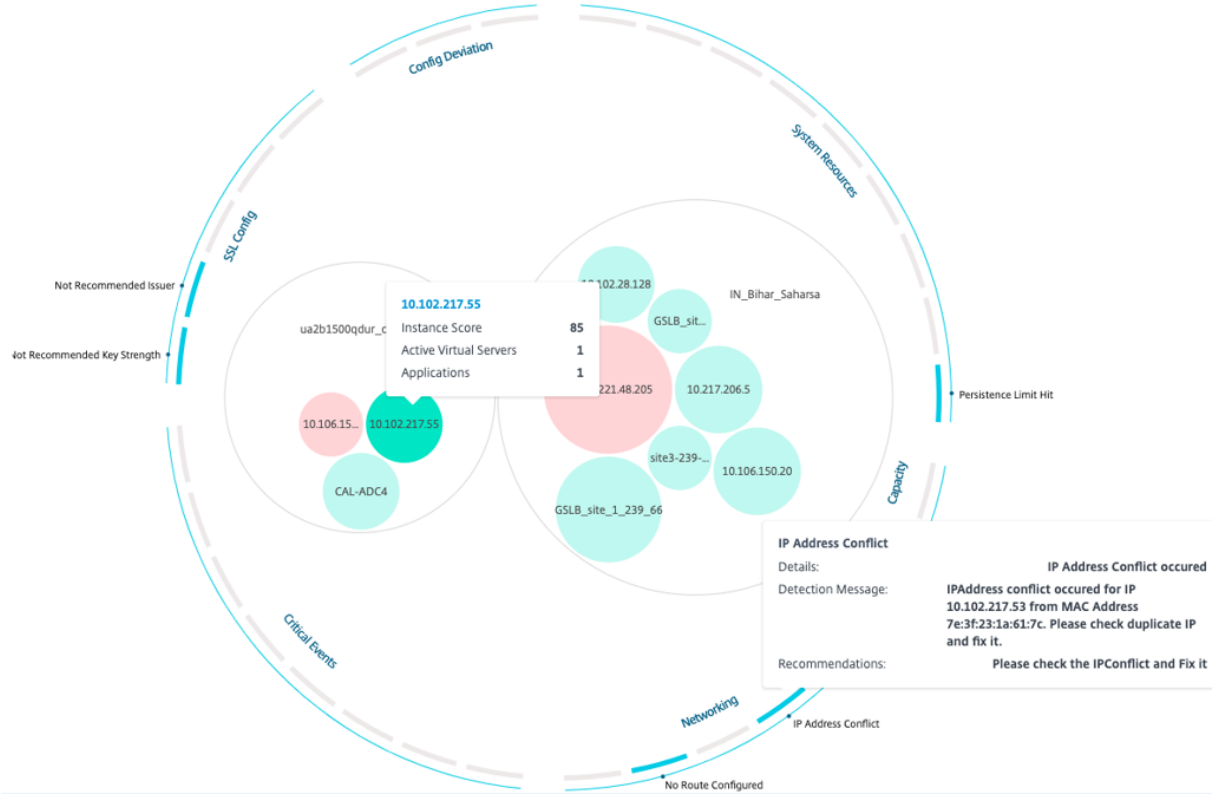
表格视图

您还可以使用 基础架构分析中的表格视图选项查看异常。导航到网络 > 基础设施分析，然后单击 以显示所有托管实例。单击 以展开以了解详细信息。



查看异常的详细信息

例如，如果要查看网络中的 **IP** 地址冲突的详细信息，请单击为 IP 地址冲突显示的异常以查看详细信息。



- 详细信息 -指示检测到的异常
- 检测消息 -指示 IP 地址发生冲突的 MAC 地址
- 建议 -指示解决此 IP 地址冲突的措施项

常见问题解答

April 23, 2021

本节提供有关以下 Citrix Application Delivery Management (Citrix ADM) 功能的常见问题解答。单击下表中的功能名称可查看该功能的常见问题列表。

分析	身份验证	配置管理
证书管理	部署	部署（灾难恢复）
事件管理	实例管理	样本
系统管理		

分析

是否需要在以单跳模式部署的 **Citrix Gateway** 实例上启用 **EUEM** 虚拟通道

EUEM 虚拟通道数据是 Citrix ADM 从网关实例接收到的 HDX Insight 能分析数据的一部分。EUEM 虚拟通道提供有关 ICA RTT 的数据。如果未启用 EUEM 虚拟通道，则其余 HDX Insight 数据仍会显示在 Citrix ADM 上。

EUEM 虚拟通道是 Citrix 虚拟桌面应用程序 (VDA) 上运行的默认服务。如果未运行，请在 VDA 服务中启动 “Citrix 最终用户体验监视” 过程。

如何使 **Citrix ADM** 能够监视 **Web** 应用程序和虚拟桌面流量**?**

1. 导航到 “ 基础架构” > “ 实例” > “ **Citrix ADC**”，然后选择要启用分析的 Citrix ADC 实例。
2. 从选择操作列表中，选择配置分析。
3. 在打开的 “ 配置分析” 页中，选择要在其上启用分析的所有虚拟服务器，然后单击 “ 启用 **AppFlow**”。有关更多详细信息，请参阅如何对实例启用分析。

> 注意
>
> 对于 11.0 版本、65.30 版本及更高版本的 Citrix ADC 实例，Citrix ADM 上没有显式启用安全智能分析的选项。确保在 Citrix ADC 实例上配置 AppFlow 参数，以便 Citrix ADM 开始接收安全智能分析通信以及 Web 智能分析通信。有关如何在 Citrix ADC 实例上设置 AppFlow 参数的详细信息，请参阅使用配置实用程序设置 AppFlow 参数的步骤。

添加 **Citrix ADC** 实例后，**Citrix ADM** 是否会自动开始收集分析信息**?**

不。对 Citrix ADM 管理的 Citrix ADC 实例中托管的虚拟服务器启用分析。有关更多详细信息，请参阅如何对实例启用分析。

是否需要访问各个 **Citrix ADC** 设备才能启用分析

否。所有配置都通过 Citrix ADM 用户界面完成，该界面列出了特定 Citrix ADC 实例上托管的虚拟服务器。有关更多详细信息，请参阅如何对实例启用分析。

可以在 **Citrix ADC** 实例上列出哪些虚拟服务器类型以启用分析**?**

当前，Citrix ADM 用户界面列出了以下用于启用分析的虚拟服务器：

- 负载平衡虚拟服务器
- 内容交换虚拟服务器
- VPN 虚拟服务器
- 缓存重定向虚拟服务器

如何将额外的磁盘附加到 **Citrix ADM**

要将额外的磁盘连接到 Citrix ADM，请执行以下操作：

1. 关闭 Citrix ADM 虚拟机。
2. 在虚拟机管理程序中，将所需磁盘大小的额外磁盘附加到 Citrix ADM 虚拟机。

   例如，让我们考虑您希望将磁盘空间增加到 200 GB, 在 Citrix ADM 虚拟机 120 GB. 在这种情况下，您必须附加 200 GB 而不是 80 GB 的磁盘空间。新附加的 200 GB 磁盘空间将用于存储数据库数据、Citrix ADM 日志文件。现有的 120 GB 磁盘空间用于存储核心文件、操作系统日志文件等。
3. 启动 Citrix ADM 虚拟机。

什么意思是收集器没有在 **Citrix ADC** 实例上配置**?**

收集器接收由 Citrix ADC 装置生成的 AppFlow 记录。

启用 AppFlow 功能后，Citrix ADM 从 Citrix ADC 实例接收安全智能分析和 Web 智能分析通信。在 Citrix ADC 实例上启用 AppFlow 功能时，必须至少指定一个将 AppFlow 记录发送到的收集器。如果未在 Citrix ADC 实例上配置收集器，则 Citrix ADM 不会接收来自这些实例的流量。

例如，将五个 Citrix ADC 实例添加到 Citrix ADM 中。如果未为两个实例指定收集器，则不会流向 Citrix ADM 的流量。自助诊断程序检测到问题，并将问题显示为“未在 2 个实例上配置收集器。“

有关如何配置 AppFlow 功能的详细信息，请参阅 配置 AppFlow 功能。

启用客户端测量有什么作用

启用客户端测量后，ADM 通过 HTML 注入捕获 HTML 页面的加载时间和渲染时间指标。使用这些指标，管理员可以识别 L7 延迟问题。

身份验证

什么是身份验证请求的负载均衡**?**

通过身份验证服务器负载平衡功能，Citrix ADM 可以对定向到外部身份验证服务器的身份验证请求进行负载平衡。对身份验证服务器执行负载平衡可确保在多个身份验证服务器之间分摊身份验证负载，从而避免某个身份验证服务器过载。可以创建身份验证服务以使用身份验证协议（例如，LDAP、RADIUS 或 TACACS）与现有外部身份验证服务器连接，并从其获取用户信息。

为什么我们需要级联外部认证服务器**?**

级联外部身份验证服务器提供不间断的身份验证处理，从而在某个身份验证服务器发生故障时允许对合法用户进行访问。可以级联的身份验证服务器的类型没有限制。可以全是 RADIUS 服务器或全是 LDAP 服务器，也可以是 RADIUS 服务器和 LDAP 服务器组合。

我可以级联多少个外部身份验证服务器**?**

您最多可以在 Citrix ADM 中级联 32 个外部身份验证服务器。

当外部身份验证失败时，我是否有其他选择**?**

可能会出现外部身份验证完全失败的情况，即使您已级联多台服务器也是如此。例如，外部服务器可能无法访问，或者可能没有在任何外部身份验证服务器中输入新用户的凭据。为了防止在此类情况下锁定用户，可以启用回退本地身份验证。有关更多详细信息，请参阅备用本地身份验证。

什么是回退本地身份验证**?**

回退本地身份验证是当外部身份验证失败时可以在本地对用户进行身份验证的一种方式。如果外部身份验证失败，Citrix ADM 将访问本地用户数据库以对用户进行身份验证。

在 Citrix ADM 中，导航到 “ 系统” > “ 身份验证” > “身 份验证配置”。在此页面上，可以将多个外部身份验证服务器添加到一个级联中，并可以选择 **Enable fallback local authentication**（启用回退本地身份验证）选项。

什么是外部用户组的提取

如果添加了用于验证用户的外部服务器，则可以将现有用户组导入（提取）到 Citrix ADM 中。必须导入一次用户组，并向用户组提供组权限，而不是导入各个用户并为其提供单独的权限。您不必在 Citrix ADM 上重新创建用户。

为什么我们需要分配组权限**?**

使用 Citrix ADC 的负载平衡功能时，可以将 Citrix ADM 与外部身份验证服务器集成，并从身份验证服务器导入用户组信息。登录 Citrix ADM 并在 Citrix ADM 中手动创建相同的组信息，然后将权限分配给这些组。用户和用户组权限在 Citrix ADM 中进行管理，而不是在外部服务器中进行管理。用户在外部服务器上有基于角色的不同访问权限。还为 Citrix ADM 中的用户配置相同的权限。不是为每个用户单独配置权限，而是可以配置组级别权限，以便用户组成员可以在负载平衡的虚拟服务器上访问特定服务。您可以分配的典型权限包括管理 Citrix ADC 实例、Citrix SDX 实例、虚拟服务器等的权限，以便该组的用户只能管理这些实例或虚拟服务器。可以在以后编辑指定给用户的组级别权限。您甚至可以删除一个或多个用户组；其他组用户仍可在 Citrix ADM 上运行。

配置管理

是否可以使用 **Citrix ADM** 同时跨多个 **Citrix ADC** 实例执行配置**?**

可以，您可以使用配置作业跨多个 Citrix ADC 实例执行配置。

什么是 **Citrix ADM** 上的配置作业**?**

作业是可以在一个或多个托管实例上创建并运行的一组配置命令。您可以使用 Citrix ADM GUI 创建作业以跨实例进行配置更改、在网络上的多个实例上复制配置以及录制和播放配置任务。还可以将录制的任务转换为 CLI 命令。

您可以使用 Citrix ADM 的配置作业功能创建配置作业、发送电子邮件通知以及检查所创建作业的执行日志。

是否可以使用 **Citrix ADM** 中的内置模板计划作业**?**

是的！可以使用内置模板选项计划作业。作业是可以在一个或多个托管实例上运行的一组配置命令。例如，可以使用内置模板选项计划作业来配置 syslog 服务器。您可以选择立即运行作业，也可以选择将作业安排在以后运行。

可以保存以前创建的一个作业的配置，在修改命令、参数、配置来源和目标实例后重新运行该作业。当必须在不同的实例上运行同一组命令或作业遇到错误并停止进一步执行时，这很有用。

证书管理

从 **Citrix ADM** 删除 **SSL** 证书是否会导致从 **Citrix ADC** 实例中删除证书

否

部署

什么是默认的用户名和密码**?**

- 完成初始网络配置后，您可以使用默认用户名和密码 (ns 恢复 /nsroot) 从 Hypervisor 或 SSH 控制台登录到 Citrix ADM。
- 要从 GUI 登录的默认用户名和密码是 *nsroot/nsroot*。

如何更改默认密码**?**

要更改密码，请执行以下操作：

1. 在 Citrix ADM 中，导航到 “ 系统” > “ 用户管理” > “用 户”。

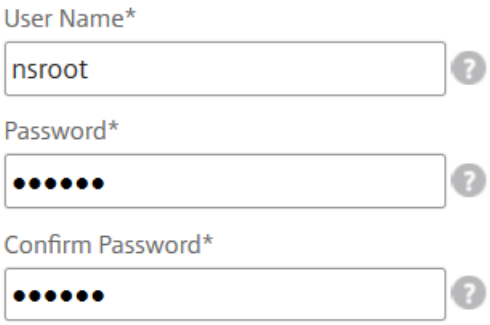
   此时将显示 “用户” 页。

2. 选择用户名 **nsroot** ，然后单击 编辑。

   此时将显示 “配置系统用户” 页。

3. 选择“ 更改密码”并创建您选择的密码。



4. 单击确定。

   现在，您可以使用新密码从 GUI 和 Hypervisor 或 SSH 控制台登录。

   > 注意
   >
   > 您不能修改用户名。

如何重置密码?

您可以看到它 文档 来重置密码。

在 HA 对中，如果在主节点中更改了密码，并且稍后选择了“中断 HA 对”选项，则行为是什么

您可以使用新密码登录到两个独立节点。

如果两个独立服务器具有不同的密码，那么在 HA 对中部署这两个服务器会产生什么影响?

当您将两个独立服务器部署到 HA 对时，建议两个服务器都使用默认密码。

HA 配置已完成，但主节点 GUI 无法访问。可能是什么原因?

配置需要几分钟时间才能生效。几分钟后，您可以尝试再次访问。

HA 配置已完成，但浮动 IP 地址 GUI 无法访问。可能是什么原因?

完成 HA 配置后，您需要首先访问主节点 GUI 并完成部署。有关详细信息，请参阅将主节点和辅助节点部署为高可用性对。部署完成后，服务器将重新启动并准备好进行高可用性部署。然后，您可以访问浮动 IP 地址 GUI。

Citrix ADM 独立和 Citrix ADM HA 支持哪个数据库?

独立的 Citrix ADM 和 Citrix ADM HA 均支持 PostgreSQL。

什么是辅助节点的潜在数据丢失**?**

辅助节点侦听主节点通过 Citrix ADM 数据库发送的检测信号消息。如果辅助节点未收到检测信号超过 180 秒，则辅助节点对主节点执行基于 SSH 的检查。如果检测信号和基于 SSU 的检查失败，则将认为主节点已关闭。

在这种情况下，辅助节点接管作为主节点，180 秒的时间范围可以被视为可能的数据丢失到辅助节点。

如果主节点关闭，会发生什么情况**?**

辅助节点接管并成为主节点。

如何重新安装失败的节点**?**

建议安装全新的虚拟机版本。要重新安装：

1. 打破 HA 对。导航至 “ 系统” > “ 部署”

   此时将显示部署页面。单击 中断 **HA**

2. 从 Hypervisor 中删除故障节点。
3. 将.XVA 映像文件导入 Hypervisor。
4. 在控制台选项卡中，使用初始网络配置配置 Citrix ADM。有关详细信息，请参阅注册和部署第一台服务器（主节点）和注册和部署第二个服务器（辅助节点）。
5. 重新部署 HA 对。

Citrix ADM 是否支持 **SAN** 存储**?**

思杰建议您在本地存储上托管 Citrix ADM VHD。当托管在 SAN 中的存储设备上时，Citrix ADM 可能无法按预期工作。

Citrix ADM 是否支持额外的磁盘

是。默认情况下，Citrix ADM HA 对的新安装会分配 120 GB 的存储空间。对于超过 120 GB 的存储空间，您可以添加一个额外的磁盘，最多可容纳 3 TB 的存储空间。不支持添加多个额外磁盘。

禁用 **HA** 对后，配置的浮动 **IP** 地址会发生什么情况**?**

浮动 IP 地址不再可访问，您需要重新部署高可用性对。

我可以在重新部署时提供不同的浮动 **IP** 地址吗**?**

是。您可以配置新的浮动 IP 地址。

为什么辅助节点 **GUI** 不可访问**?**

辅助节点只是只读副本服务器，只有在主节点因任何原因关闭时才能充当主节点。Citrix 建议访问主节点 GUI 或浮动 IP 地址 GUI。

如果主节点长时间关闭，可以使用浮动 **IP** 地址 **GUI** 来完成配置吗**?**

是。您仍然可以继续进行配置，并将配置保存在辅助节点中。主节点返回后，将同步所有配置。

如果将来需要更改主节点 **IP** 地址或辅助节点 **IP** 地址或浮动 **IP** 地址（例如，将其更改为 **IPv6**），建议遵循哪些解决方案**?**

在不破坏 HA 对的情况下，不支持更改 HA 对中的 IP 地址。

要更新主节点或辅助节点 IP 地址，请执行以下操作：

1. 打破 HA 对。导航到 “ 系统” > “ 部署”。

   此时将显示 “部署” 页。单击 中断 **HA**

   a) 使用 SSH 客户端或从 Hypervisor 登录到主节点。

   b) 用 `nsrecover` 作用户名并输入您设置的密码。

   c) 输入 网络配置。执行 步骤 **3** 中提供的过程 注册和部署第一台服务器（主节点）。

      在初始网络配置期间，您可以提供不同的 IP 地址。

   d) 对辅助节点执行相同的过程，并继续执行中的 步骤 **3** 中的过程 注册和部署第二个服务器（辅助节点）。

要更新浮动 IP 地址，请执行以下操作：

1. 导航到 “ 系统” > “ 部署”。

   此时将显示 “部署” 页。

   a) 单击 **HA** 设置。

   b) 单击 “ 配置浮动 **IP** 地址以实现高可用性模式”。

   c) 输入浮动 IP 地址，然后单击 “ 确定”。

ADM 是否支持 **AMD** 处理器

不。ADM 不支持 AMD 处理器。

部署（灾难恢复）

主站点和灾难恢复站点之间的复制频率如何**?**

主站点和灾难恢复站点之间的复制是实时的。

在 **DR** 站点启动备份脚本后，**DR** 站点是否会成为临时主站点，直到主站点恢复并完全运行**?**

否。灾难恢复站点现在将成为主站点。要将 HA 对恢复为主站点，请参阅 将配置还原到原始主站点

如果选择了 **"**中断 **HA** 对**"** 选项，则两个节点将作为独立服务器运行。由于 **DR** 支持不适用于独立服务器，因此如果选择了 **Break HA** 对，**DR** 站点会发生什么情况**?**

如果选择中断 HA 对选项，则终止主站点和 DR 站点之间的复制。您需要重新配置 DR 站点，作为重新部署 HA 对的一部分。

事件管理

如何使用 **Citrix ADM** 跟踪在我的托管 **Citrix ADC** 实例上生成的所有事件**?**

作为网络管理员，您可以查看 Citrix ADC 实例上的配置更改、登录条件、硬件故障、阈值违规和实体状态更改等详细信息，以及特定实例上的事件及其严重性。您可以使用 Citrix ADM 事件仪表板查看为所有 Citrix ADC 实例上的关键事件严重性详细信息生成的报告。

什么是活动规则**?**

使用 Citrix ADM，您可以配置规则来监视特定事件。通过事件规则，您可以更轻松地监控在 Citrix ADM 基础架构中生成的大量事件。

可以通过为规则配置特定条件及为规则分配操作来过滤一组事件。当生成的事件满足规则中的筛选条件时，将运行与该规则关联的操作。

您可以创建筛选器的条件包括严重性、Citrix ADC 实例、类别和故障对象。您可以分配给事件的操作包括：发送电子邮件通知、将受管 Citrix ADC 实例的 SNMP 陷阱转发到 Citrix ADM，以及发送 SMS 通知。

实例管理

使用 **Citrix ADC** 池容量许可时，如果 **ADC** 实例在带宽分配后无法连接到 **ADM**，会发生什么情况

如果 ADC 实例和 ADM 之间的心跳失败，则实例将进入 30 天的宽限期。重新建立通信后，集合容量许可开始运作。在宽限期内，ADC 功能不受影响。超过 30 天的宽限期后，ADC 实例将启动热重启并且处于未获许可状态。

Citrix ADM 中的数据中心是什么**?**

Citrix ADM 数据中心是特定地理位置中的 Citrix ADC 实例的逻辑分组。每台服务器都可以监视和管理数据中心内的多个 Citrix ADC 实例。您可以使用 Citrix ADM 服务器来管理来自托管实例的系统日志、应用程序流量和 SNMP 陷阱等数据。有关配置数据中心的详细信息，请参阅如何在 Citrix ADM 中为地理地图配置数据中心。

Citrix ADM 支持哪些不同的思杰设备**?**

实例是您希望从 Citrix ADM 中发现、管理和监视的 Citrix 设备或虚拟设备。您必须将这些实例添加到 Citrix ADM 服务器中。您可以将以下 Citrix 设备和虚拟设备添加到 Citrix ADM 中:

- Citrix MPX
- Citrix VPX
- Citrix SDX
- Citrix CPX
- Citrix Gateway
- Citrix SD-WAN O
- Citrix SD-WAN PE

您可以在首次设置 Citrix ADM 服务器时或以后添加实例。

什么是实例配置文件**?**

Citrix ADM 使用实例配置文件访问实例。

实例配置文件包含用于访问一个或多个实例的用户名和密码。每个实例类型都有一个默认配置文件。例如，ns-Rot 配置文件是 Citrix ADC 实例的默认配置文件。它包含默认的 Citrix ADC 管理员凭据。更改访问实例所需的凭据时，可以为那些实例定义自定义实例配置文件。

我们是否可以在 **Citrix ADM** 中添加无限制的 **SD-WAN** 实例**? Citrix ADM** 可以处理 **SD-WAN** 的所有标量和矢量计数器吗**?**

目前，可以添加到 Citrix ADM 的 SD-WAN 实例没有许可限制。Citrix ADM 具有一组内置报告，可在内部轮询标量计数器和矢量计数器。

是否可以重新发现 **Citrix ADM** 中的多个思杰 **VPX** 实例**?**

可以，您可以在 Citrix ADM 中重新发现多个 Citrix **VPX** 实例，以了解实例的最新状态和配置。

导航到 “ 网络” > “ 实例” > “ **Citrix ADC” > “VPX”**，选择要重新发现的实例，然后在 “ 操作” 列表中单击 “ 重新发现”。有关详细信息，请参阅如何重新发现多个 VPX 实例。

是否可以在 **Citrix SDX** 上安装 **Citrix ADM?**

否

是否可以使用公有 **IP** 地址在 **ADM** 软件上添加 **Citrix ADC** 实例**?**

可以，您可以使用网络地址转换 (NAT)。

- 添加单个实例：使用 ADC 实例公有 IP 地址的 NAT IP。
- 要添加 ADC HA 对，请按以下格式添加 HA 对的 NAT IP 地址：

  <NAT public IP of the primary instance>##<NAT public IP of the secondary instance>
- 添加 ADC 集群：添加集群中所有实例的所有 NAT 公有 IP 地址，每个地址都以逗号分隔，然后在括号或圆括号内添加集群 IP 的 NAT IP。一个示例格式：NAT1，NAT2，NAT3，(集群的国家标准)。

有关详细信息，请参阅以下主题：

- 将实例添加到 Citrix ADM
- 配置网络地址转换

如果 **DR** 节点凭据发生更改，如何注册灾难恢复节点**?**

nsrecover使用以下命令将灾难恢复 (DR) 节点凭据重置为 nsroot /：

```
./mps/change_freebsd_password.sh <username> <password>
<!--NeedCopy-->
```

要注册 DR 节点，请按照中的步骤操作 使用灾难恢复控制台部署和注册 Citrix ADM DR 节点。

样本

样书可以用于配置在不同版本的 **Citrix ADC** 软件上运行的不同 **Citrix ADC** 实例吗

是的，如果不同版本的命令之间没有差异，则可以使用样书来配置在不同版本上运行的不同 Citrix ADC 实例。

如果使用样书同时配置多个 **Citrix ADC** 实例，并且一个 **Citrix ADC** 实例的配置失败，会发生什么情况**?**

如果将配置应用于 Citrix ADC 实例失败，则该配置不再应用于任何实例，并且已应用的配置将回滚。

通过 **Citrix ADC** 进行的 **Citrix ADC** 备份是否包括通过样书应用的配置

是

系统管理

是否可以为我的 **Citrix ADM** 服务器分配主机名**?**

可以，您可以分配主机名来标识您的 Citrix ADM 服务器。要指定主机名，请导航至 **System**（系统）> **System Administration**（系统管理）> **System Settings**（系统设置），并单击 **Change Hostname**（更改主机名）。

主机名显示在 Citrix ADM 的通用许可证上。有关详细信息，请参阅 如何将主机名分配给 Citrix ADM 服务器。

是否可以备份和还原我的 **Citrix ADM** 配置**?**

是的，您可以备份配置文件（NTP 文件和 SSL 证书）、系统数据、基础架构和应用程序数据以及所有 **SNMP** 设置。如果您的 Citrix ADM 变得不稳定，您可以使用备份的文件将 Citrix ADM 恢复到稳定状态。

要备份和还原 Citrix ADM 配置，请导航到“系统”>“高级设置”>“备份文件”，然后根据情况单击备份或还原。有关详细信息，请参阅 如何在 Citrix ADM 上备份和还原配置。

Citrix 建议在执行升级之前或出于防范性措施的原因，使用此功能。

什么是 **Citrix ADM** 上的阈值和警报**?**

您可以设置阈值和警报，以监视 Citrix ADC 实例的状态并监视托管实例上的实体。

当计数器的值超过阈值时，Citrix ADM 会生成一个警报，指示性能相关问题。在计数器值回到阈值中指定的清除值时，事件将被清除。

是否可以为 **Citrix ADM** 生成技术支持文件**?**

是。Citrix 建议您在联系技术支持以调试问题之前生成 Citrix ADM 数据和统计信息的存档。存档是可以发送给技术支持团队的 TAR 文件。

您可以生成一个技术支持文件，其中包含调试日志、收集调试日志的持续时间以及 Citrix ADM 数据库中不同且不同的日志。

若要配置和发送技术支持文件，请导航到“系统”>“诊断”>“技术支持”，然后单击“生成技术支持文件”。有关详细信息，请参阅 如何为 Citrix ADM 生成技术支持文件。

什么是系统日志清除**?**

Syslog 是日志记录标准协议。通过 syslog 可以隔离生成信息的系统和存储信息的系统。可以合并日志记录信息，并基于收集的数据得出洞察信息。还可以配置 syslog 来记录不同类型的事件。

要限制数据库中存储的 syslog 数据量，可以指定希望清除 syslog 数据的时间间隔。您可以指定在天数之后将从 Citrix ADM 中删除所有通用系统日志数据、AppFirewall 数据和 CitCitrix Gateway 数据。

我可以在 **Citrix ADM** 上配置 **NTP** 服务器吗**?**

您可以在 Citrix ADM 中配置网络时间协议 (NTP) 服务器，以便将 Citrix ADM 时钟与 NTP 服务器同步。配置 NTP 服务器可确保 Citrix ADM 时钟具有与网络上其他服务器相同的日期和时间设置。

若要配置 NTP 服务器，请导航到“系统”>“**NTP** 服务器”，然后单击“添加”。有关详细信息，请参阅 如何在 Citrix ADM 上配置 NTP 服务器。

从哪个版本支持 **Citrix ADM** 主动-被动 **HA** 部署**?**

Citrix ADM 主动-被动高可用性部署模式受到 Citrix ADM 版本 12.0 版版本 51.24 的支持。

我有一个 **Citrix ADM** 主动-主动 **HA** 设置，并配置了一个带有负载平衡虚拟服务器的 **Citrix ADC** 设备以实现统一 **GUI** 访问。如何更新此配置**?**

将 Citrix ADM HA 对升级到主动-被动模式后，必须在 Citrix ADC 设备上运行以下命令以更新负载平衡配置：

添加 **lb** 监视器 MAS_ 监视器 **TCP-ECV-**发送 **“GET /mas_** 运行状况 **HTTP/1.1\ r\ n** 接受编码**:** 标识**\ r\ n** 用户代理**:** 网络扩展器监视器**\ r\ n** 连接**:** 关闭**\ r\ n\ r\ n\“”-recv “{\”** 状态代码**\”: 0}”-0”-LRTM** 已禁用

是否可以使用端口 **443** 在 **Citrix ADC** 实例上配置 **Citrix ADM HA** 对的负载均衡**?**

否，您不能使用端口 443 在 Citrix ADC 实例上配置 Citrix ADM HA 对的负载平衡。

在 Citrix ADC 上配置 `http-ecv` 和 `https-ecv` 监视器时，它无法正确监视 Citrix ADM HA 节点。

是否可以使用 **Citrix ADM** 服务器备份文件还原另一台 **Citrix ADM** 服务器的配置**?**

是

Citrix ADM 备份 **Citrix ADC** 实例后，是否可以使用该备份文件通过 **Citrix ADM** 还原另一个 **Citrix ADC** 实例的配置**?**

是。下载 Citrix ADM 备份文件，将其上载到另一个 Citrix ADC 实例的备份存储库中，然后还原该实例。确保网络信息和身份验证信息不冲突。例如，检查 IP 地址或端口冲突、密码配置文件不匹配。还要确保还原的 VPX 实例具有与备份的实例相同的 NSIP 地址和 Citrix ADC 许可证。

在恢复高可用性对中的实例之前，请确保备份文件中存储的 IP 地址和状态（主或辅助）与原始 HA 配置的 IP 地址和状态相匹配。还要验证新的主要和辅助服务是否具有相同类型的 Citrix ADC 许可证。

我们能否强制 **Citrix ADM** 使用 **SNIP** 地址与 **Citrix ADC** 实例进行通信，而不是使用 **Citrix ADM** 服务器的 **NSIP** 地址**?**

可以，您可以在 Citrix ADM 中添加 SNIP 地址（启用了管理功能），以便与 Citrix ADC 实例进行通信。

当我在 **Citrix ADM** 中备份 **Citrix ADC** 实例时，结果是完全备份还是基本备份**?**

Citrix ADM 对 Citrix ADC 实例的备份是完整备份。

是否有 **Citrix ADM** 的故障排除指南**?**

是。请参阅 https://support.citrix.com/article/CTX224502。

Citrix ADM HA 故障转移发生时，如何管理 **Citrix ADC** 实例**?**

如果检测信号和基于 SSH 的检查失败，则将认为主节点已关闭，辅助节点将作为主节点接管。默认情况下，所有 Citrix ADC 实例都会使用最新的主节点详细信息作为其 SNMP 陷阱目标进行更新。

新的主（活动）Citrix ADM 节点将检查以前的主动节点是否配置为 AppFlow 收集器还是 syslog 服务器。如果是，新的主节点会将 AppFlow 收集器或 syslog 服务器详细信息添加到发送到实例的信息中。

对于 syslog，它替换旧的服务器详细信息。

当出现故障的 **Citrix ADM HA** 节点恢复时，会发生什么情况**?**

返回服务后，Citrix ADM 节点将保持被动状态，除非主动节点故障转移

Citrix ADC 实例如何在 **Citrix ADM HA** 节点之间分布**?**

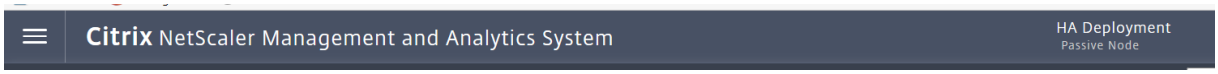
所有 Citrix ADC 实例都由主 Citrix ADM 节点进行管理。

如果存在 **Citrix ADM HA** 故障转移，如何管理虚拟服务器许可证**?**

如果应用虚拟服务器许可证的 Citrix ADM 主节点出现故障，则新的主节点将在 30 天的宽限期内管理虚拟服务器许可证。在宽限期结束之前，在新的主服务器上重新应用许可证。有关替代品，请联系 Citrix 支持部门。

Citrix ADM HA 设置是否必须使用负载均衡器**?**

否，但如果没有负载均衡器，则必须通过其自己的 IP 地址访问 Citrix ADM 节点。被动节点标记为 “被动”，Citrix 建议不要在被动节点上创建任何配置。



Citrix ADM 是否支持外部数据库**?**

否

是否可以将由 **Citrix ADM** 管理的 **Citrix ADC** 实例用作 **Citrix ADM HA** 的负载均衡器**?**

是

哪些数据在 **Citrix ADM HA** 节点之间进行同步**?**

已同步完整的 Citrix ADM 数据库，并同步以下文件夹：

- /var/mps/tenants/root/
- /var/mps/ns_images/
- /var/mps/sdx_images/
- /var/mps/xen_nsvpx_images/
- /var/mps/cbwanopt_images/
- /var/mps/sdwanvw_images/
- /var/mps/mps_images/
- /var/mps/ssl_certs/
- /var/mps/ssl_keys/
- /mpsconfig/ssl/
- /var/mps/backup/
- /var/mps/esx_nsvpx_images/
- /var/mps/locdb/

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States