NetScaler Application Delivery Management 13.1

Machine translated content

Disclaimer

Contents

发行说明

February 6, 2024

NetScaler Application Delivery Management (ADM) 13.1 发行说明描述了新功能、对现有功能的增强以及版本中的已知问题。13.1 版本的发行说明文档包括以下部分：

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

> 注意
>
> 这些发行说明未记录安全相关的修复。有关安全相关修复和建议的列表，请参阅安全公告。

NetScaler ADM 13.1-51.14 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1-51.14 的增强和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

已修复的问题

Build 13.1-51.14 中解决的问题。

基础结构

- 在网关 **> HDX Insight** 和网关 **> Gateway Insight** 中，图表的 X 轴显示日期而不是时间。

  [NSHELP-36043]

管理和监视

- 设置 **>** 备份文件 **>** 还原中的 NetScaler ADM 恢复操作间歇性地无法完成。

  [NSHELP-36527]

- NetScaler ADM 无法压缩某些核心文件，导致磁盘空间消耗增加。

  [NSHELP-36434]

- 在 NetScaler ADM HA 设置的主节点和辅助节点之间同步文件期间，库存子系统会间歇性地崩溃。

  [NSHELP-36357]

样书

- 当更新或删除参数中包含特殊字符的配置包时，尽管在 NetScaler 上执行的更新或删除操作未完成，但 NetScaler ADM 仍会显示成功消息。通过此修复，NetScaler ADM 现在可以准确显示由于配置包定义中的特殊字符而导致的任何不完整配置的错误。

  [NSADM-104423]

已知问题

版本 13.1-51.14 中存在的问题。

分析

- 定期修剪应用程序控制板数据并未按预期运行。因此，NetScaler ADM 消耗了更多的磁盘空间。

  [NSHELP-36184]

- 当 NetScaler ADM 丢失虚拟服务器许可证时，预计使用这些许可证的虚拟服务器的分析状态将被禁用。对于 VPN 虚拟服务器，这种情况不如预期的那样起作用。

  [NSHELP-36183]

基础结构

- 从 NetScaler ADM 中删除适用于 VMware ESXi 的许可后，“设置” **>** “许可和分析配置”中的许可数量 可能不会立即反映更新的数字。

  [NSADM-105851]

- 在 基础架构 **>** 事件 **>** 事件消息中，NetScaler ADM 不显示 NetScaler CPU 利用率陷阱是针对数据包 CPU 还是管理 CPU。

  [NSADM-103391]

- 在扩展部署中观察到 mas_service 子系统崩溃。

  如果您拥有 RBAC 权限，并且属于在“设置”**>**“用户和角色”**>**“组”**>**“授权设置”中具有以下配置的组，则会出现此问题：

  - 在“实例”中选择了特定的 实例
  - 在“应用程序”中选择“所有应用程序”

  [NSADM-99873]

- 修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

  [NSADM-94279]

管理和监视

- 如果您使用 VMware vMotion 在 ESXi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道将中断。因此，您无法访问 ADM GUI。

  [NSHELP-32647]

- 在网关 **> HDX Insight** 中，由于数据库损坏，数据不会显示。

  [NSHELP-30459]

- 在 ADM HA 对中，即使多次尝试使用 GUI 中的“同步数据库”选项，数据库状态仍处于关闭状态且未同步。

  [NSHELP-29626]

Provisioning

- 从 OpenStack 中删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1—50.23 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—50.23 的增强和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

已修复的问题

版本 13.1—50.23 中解决的问题。

分析

- 有时，NetScaler ADM 代理可能会崩溃并在升级后生成核心转储文件。

  [NSHELP-36428]

基础结构

- 由于心跳通信同步失败，NetScaler ADM HA 对无法从脑裂场景中恢复。

  [NSHELP-35934]

- 已为用户启用客户用户体验改善计划 (CUXIP) 功能，即使管理员在“设置”**>**“管理”**>**“**CUXIP** 设置”中禁用了 CUXIP，也会收集他们的使用数据。

  [NSADM-101771]

- 当您在分区上运行任何配置作业的命令时，会出现以下错误消息：“管理分区设备的命令已阻止”。

  在 NetScaler 13.1—42.47 及更高版本中会出现此问题。

  [NSADM-100416]

- 使用脚本同时创建多个 SNMP 用户时，向 ADM 发出的 SNMP 请求将失败。

  [NSADM-83924]

管理和监视

- 您无法在基础结构 **>** 网络功能中查看负载平衡和 **GSLB** 节点。

  如果您所在的组中没有为负载平衡和 **GSLB** 节点下的所有子节点分配权限，则会出现此问题。

  [NSHELP-36443]

- 在 NetScaler ADM 备份目录中创建的文件夹，在计划每 2 小时执行一次的备份删除操作期间不会被删除。

  [NSHELP-35911]

- 在 NetScaler ADM 中，使用外部 LDAP 进行身份验证会间歇性失败，只有通过重新启动 NetScaler ADM 才能解决。

  [NSHELP-35733]

- ADM mas_perf 子系统崩溃，在“设置”**>**“**ADM** 系统事件”中显示一条事件消息。

  [NSHELP-35711]

- 用户无法在“应用程序”**>**“应用程序控制面板”中查看其授权的应用程序。当用户属于多个组并且每个组都有许多应用程序时，就会出现此问题。

  [NSHELP-35165]

- 主站点（NetScaler ADM HA 对）一直在重试将数据与 NetScaler ADM 灾难恢复节点同步，但失败了。
  当主站点有大量数据 (>1 GB) 时，就会出现此问题。

  [NSHELP-32750]

- 当您在基础结构 **>** 实例 **> NetScaler > SDX >** 选择操作 **>** 预配 **VPX** 中在 SDX 上预置 VPX 实例时，不会出现“通过网络管理”选项。

  [NSHELP-36328]

- 如果 NetScaler 断开与许可证服务器的连接并在 10 分钟内重新连接，则 NetScaler 签出的许可证可能会在许可证服务器上出现两次。重新启动许可证服务器以释放此陈旧条目。

  [NSHELP-35420]

Provisioning

- 当您使用 ESXi 或 VMware vCenter 在云端配置 NetScaler VPX（基础架构 **>** 实例 **> NetScaler > VPX >** 预配）时，许可配置将被忽略。

  [NSHELP-35984]

- VMware vCenter 上的 NetScaler VPX 配置（基础架构 **>** 实例 **> NetScaler > VPX >** 预配）失败，因为之前删除的 VPX 实例中使用的名称相同。

  [NSHELP-35983]

样书

- 如果您根据具有身份验证虚拟服务器和内置缓存策略绑定的样书定义创建 configpack，然后删除了 configpack，则删除成功。但是，如果您尝试使用相同的参数再次创建 configpack，则会出现以下错误消息：

  资源已存在。

  [NSHELP-35646]

已知问题

版本 13.1—50.23 中存在的问题。

分析

- 定期修剪应用程序控制板数据并未按预期运行。因此，NetScaler ADM 消耗了更多的磁盘空间。

  [NSHELP-36184]

- 当 NetScaler ADM 丢失虚拟服务器许可证时，预计使用这些许可证的虚拟服务器的分析状态将被禁用。对于 VPN 虚拟服务器，这种情况不如预期的那样起作用。

  [NSHELP-36183]

基础结构

- 在扩展部署中观察到 mas_service 子系统崩溃。

  如果您拥有 RBAC 权限，并且属于在“设置”**>**“用户和角色”**>**“组”**>**“授权设置”中具有以下配置的组，则会出现此问题：

  - 在“实例”中选择了特定的 实例
  - 在“应用程序”中选择“所有应用程序”

  [NSADM-99873]

- 修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

  [NSADM-94279]

管理和监视

- 如果您使用 VMware vMotion 在 ESXi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道将中断。因此，您无法访问 ADM GUI。

  [NSHELP-32647]

- 在网关 **> HDX Insight** 中，由于数据库损坏，数据不会显示。

  [NSHELP-30459]

- 在 ADM HA 对中，即使多次尝试使用 GUI 中的“同步数据库”选项，数据库状态仍处于关闭状态且未同步。

  [NSHELP-29626]

Provisioning

- 从 OpenStack 删除虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1-49.13 版本的发行说明

February 6, 2024

本发行说明文档描述了 NetScaler ADM 版本 Build 13.1-49.13 中存在的增强功能和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

已修复的问题

在 Build 13.1-49.13 中解决的问题。

分析

- NetScaler ADM HA 对可能会间歇性地导致大脑分裂的情况。

  [NSHELP-35430]

- URL 中没有查询参数值的 HTTP Web 事务不会显示在 NetScaler ADM Web Insight 控制板（应用程序 **> Web Insight**）中。

  例如，如果 URL `https://www.google.com/search?q=abstract%20api` 没有查询参数值并且可用作 `https://www.google.com/search?q=`，则 HTTP 事务将被删除并且在控制面板上不可用。

  [NSADM-99448]

- 在 **Web Insight** 中，当您向下钻取任何指标以查看详细信息，然后进一步向下钻取任何指标时，图表仍保留在先前的视图中，但所有其他详细信息均按预期显示。

  因此，这就形成了一种假设，即进一步的向下钻取没有按预期进行。

  [NSADM-98995]

基础结构

- 基础架构 **> NetScaler** 清单 **> NetScaler** (MPX/VPX/CPX/BLX) 页面缺少 MPX 实例。

  [NSHELP-35593]

- 在“设置”**>**“部署”**>**“强制故障转移”中对 ADM HA 对执行故障转移后，在“设置”**>**“部署”页面中看不到辅助节点的详细信息。

  [NSADM-98674]

- 当您尝试在“设置”**>**“通知”**>**“**Slack**”**>**“添加”中添加 Slack 配置文件时，该配置文件未被添加，您会收到以下错误消息：

  `Please check internet connectivity`。

  [NSADM-98633]

管理和监视

- 当您备份或恢复 NetScaler 实例时，不会备份 `/var/metrics_conf` 目录。

  [NSHELP-35724]

- 当您从“基础架构”**>**“**SSL** 控制面板”**>**“**SSL** 证书”**>**“导出报告”中导出每周、30 天或 90 天的 SSL 到期报告并选择表格时，生成的报告会显示一个空的域列。

  [NSHELP-35592]

- 在 基础结构 **> SSL** 控制板 **> SSL** 证书中，NetScaler 高可用性对不显示主设备和辅助设备的“P”和“S”的上标。

  [NSHELP-35523]

- 即使在所有进程都已启动并运行之后，NetScaler ADM 状态也会间歇性地显示为“关闭”。

  [NSHELP-35408]

- 对于群集中的多个群集 IP 地址 (CLIP)，当您在基础架构 **>** 实例 **> NetScaler >** 添加中添加括号中的 CLIP 时，配置会失败，并且 CLIP 不会添加到 NetScaler ADM 中。

  [NSHELP-35323]

- 向其他 ADM 进程发送请求时，NetScaler ADM 清单进程间歇性地崩溃。

  [NSHELP-35048]

- 由于多个子系统崩溃，NetScaler ADM 没有响应。

  [NSHELP-34633]

已知问题

13.1-49.13 版本中存在的问题。

基础结构

- 当您在任何配置作业的分区上运行命令时，会出现以下错误消息：`Command Blocked for Admin Partition Device`。

  [NSADM-100416]

- 在扩展部署中观察到 mas_service 子系统崩溃。

  如果您拥有 RBAC 权限，并且属于在“设置”**>**“用户和角色”**>**“组”**>**“授权设置”中具有以下配置的组，则会出现此问题：

  - 在“实例”中选择了特定的 实例
  - 在“应用程序”中选择“所有应用程序”

  [NSADM-99873]

- 当您重命名包含 IP 地址和分区名的应用程序时，该应用程序将从“设置”**>**“用户和角色”**>**“修改系统组”**>**“授权设置”**>**“应用程序”页面中删除。

  解决办法：命名应用程序时不要包含 IP 地址和分区名称。

  [NSADM-98635]

- 当您使用 appAdminPolicy 或 appReadOnlyPolicy 角色登录时，您可能会看到在“设置”**>**“用户和角色”**>**“访问策略”中启用的其他功能，尽管您在 NetScaler ADM 控制面板中看不到这些功能。之所以显示“访问策略”页面中的这些附加功能，是因为应用程序和网络功能依赖于它们，但这并不意味着您拥有对这些附加功能的完全权限。

  [NSADM-98055]

- 修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

  [NSADM-94279]

管理和监视

- 如果您使用 VMware vMotion 在 ESXi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道将中断。因此，您无法访问 ADM GUI。

  [NSHELP-32647]

- 在网关 **> HDX Insight** 中，由于数据库损坏，数据不会显示。

  [NSHELP-30459]

- 在 ADM HA 对中，即使多次尝试使用 GUI 中的“同步数据库”选项，数据库状态仍处于关闭状态且未同步。

  [NSHELP-29626]

Provisioning

- 从 OpenStack 中删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1—48.47 版本的发行说明

February 6, 2024

本发行说明文档描述了 NetScaler ADM 版本 Build 13.1—48.47 中存在的增强和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关的修复和建议列表，请参阅 Citrix 安全公告。

新增功能

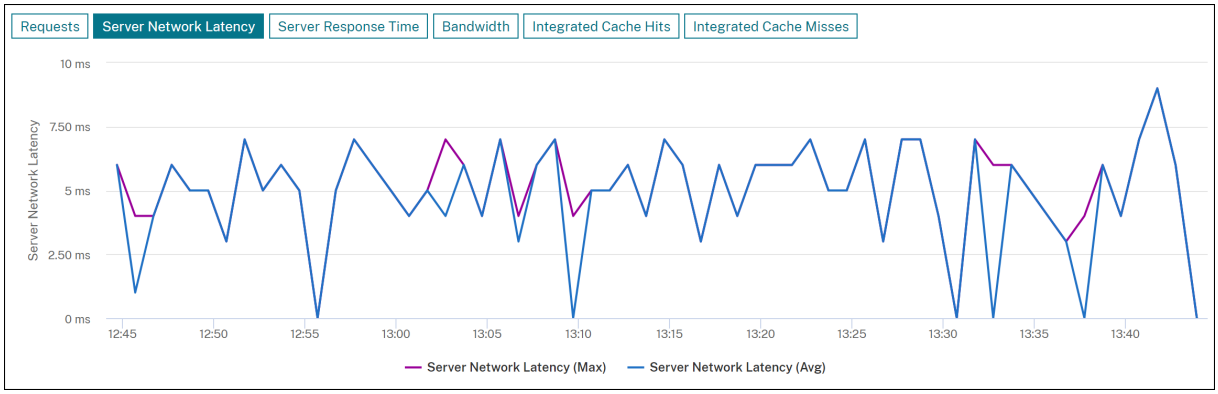
版本 13.1—48.47 中提供的增强和更改。

分析

Web Insight 的改进功能　在 **Web Insight** 中，您现在可以在服务器和客户端中查看最大网络延迟值。作为管理员，此增强功能使您能够确定以最大延迟运行的确切服务器或客户端。

早些时候，Web Insight 仅根据所有服务器和客户端的平均延迟值提供最大值。

除此支持外，当您深入查看服务器或客户端时，现在可以在摘要面板中查看平均值和最大值，也可以将鼠标指针悬停在服务器网络延迟、服务器响应时间和客户端网络延迟中的时间序列分析图上。

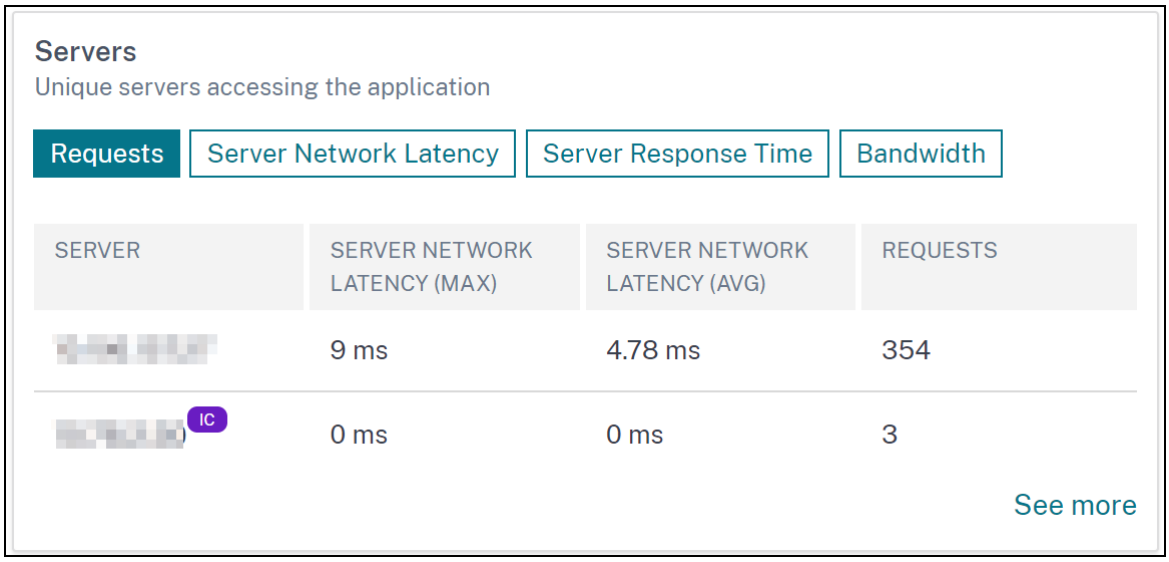


有关更多信息，请参阅 Web Insight。

[NSADM-91834]，[NSADM-93816]

Web Insight 中的集成缓存通知　在 NetScaler 实例中启用集成缓存后，无需往返原始服务器即可处理符合条件的请求。在 **Web Insight** 中，这些集成缓存请求当前显示在具有虚拟 服务器 IP 地址的服务器下方，而不是实际的服务器 IP 地址。

为了更好地了解这些集成缓存请求，您现在可以在“服务器”下的 ADC 虚拟服务器 IP 地址旁边查看 **IC** 通知。对于未使用集成缓存处理的请求，原始服务器 IP 地址是可见的。



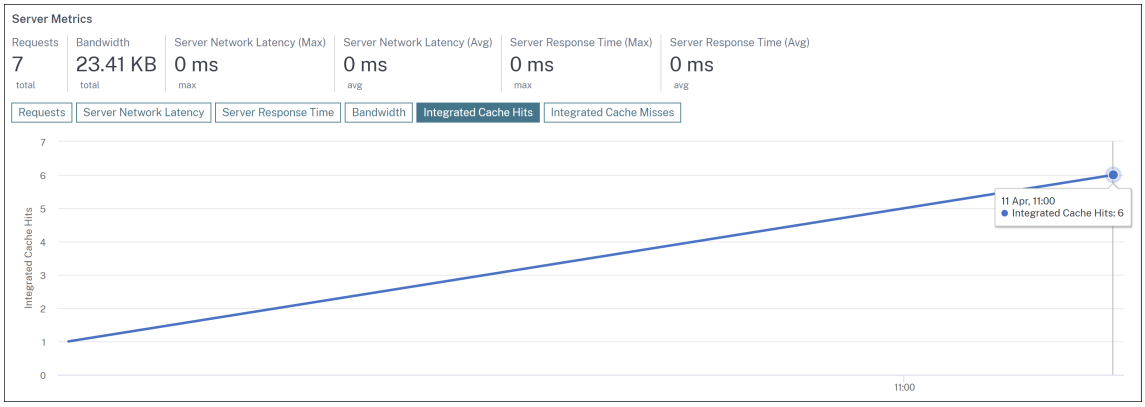
作为管理员，此通知使您能够快速识别 ADC 实例是否已处理集成缓存请求。

有关更多信息，请参阅 集成缓存请求。

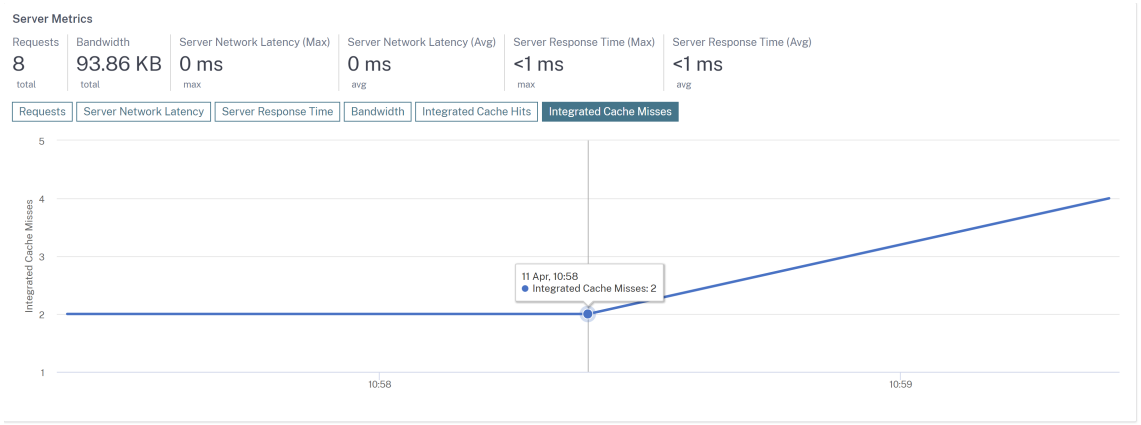
[NSADM-91864]

Web Insight 中的集成缓存命中率和未命中率图　在 **Web Insight** 中，当您深入查看服务器时，服务器指标 现在会显示“集成缓存命 中数”和“集成缓存未命中”选项卡。作为管理员，图表视图位于：

- 在集成缓存命中率选项卡中，您可以查看 NetScaler 设备从缓存中提供的响应总数。



- 在集成缓存未命中选项卡中，您可以查看 NetScaler 设备从源服务器提供的响应总数。



有关更多信息，请参阅 集成缓存请求。

[NSADM-93952]

在“任务”功能中添加了新建议　作为基于 NetScaler ADM 当前利用率的现有建议的一部分，现在添加了 设置任务页面，其中包含通知配置文件的新建议。作为管理员，如果您尚未在“设置”**>**“通知”中配置任何通知配置文件，则可以查看此建议。

有关更多信息，请参阅查看建议并高效管理您的 ADC 和应用程序。

[NSADM-93375]

将 **NetScaler ADM** 与 **Splunk** 和 **New Relic** 集成　您现在可以将 NetScaler ADM 与 Splunk 和 New Relic 集成，以查看以下方面的分析：

- WAF 违规行为
- 机器人违规行为
- SSL 证书见解

通过这种集成，您可以：

- 合并所有其他外部数据源。
- 集中提供更高的分析可见性。

NetScaler ADM 收集 Bot、WAF 和 SSL 证书事件，然后根据您的选择实时或定期发送给 Splunk 和 New Relic。作为管理员，您可以在 Splunk 和 New Relic 中创建控制板并查看事件。

有关更多信息，请参阅与 Splunk 集成和与 New Relic 集成。

[NSADM-92049]，[NSADM-92047]

基础结构

支持记录事件，无论事件时间长短　NetScaler ADM 现在允许您记录所有事件，无论您在事件规则中设置的事件年限如何。

要设置此选项，请导航到基础架构 **>** 规则 **>** 添加 **>** 配置事件年限，然后选中“无论事件持续时间长短都立即记录事件”复选框。

[NSHELP-19914]

支持在报告中查看 **NetScaler** 序列号　从 基础架构 **>** 实例 导出的报告不显示辅助节点的序列号。

现在，报告显示 NetScaler 实例的主节点和辅助节点的序列号。您还可以查看 基础结构 **>** **NetScaler** 清单中的报告。

[NSHELP-18816]

管理和监视

电子邮件通知在主题行中显示配置作业状态　当您在基础架构 **>** 配置 **>** 配置作业中创建作业时，配置作业电子邮件通知的主题行现在会显示作业状态。

[NSHELP-26985]

通知中提供实例主机名　实例主机名现在可以在从基础架构 **>** 网络报告收到的通知中找到。

[NSHELP-25622]

已修复的问题

版本 13.1—48.47 中解决的问题。

分析

- NetScaler ADM 会消耗更多的磁盘空间，因为 mps_counterd.log 文件未压缩。

  [NSHELP-35246]

- 在 Web Insight 中，当您使用快照选项导出数据时，报表中的图表显示为空白。

  [NSHELP-35147]

- HDX Insight 中显示的用户总数不正确。

  [NSHELP-34562]

- 在“设置”**>**“许可和分析配置”页面中，虚拟服务器许可证的数量会自动重置为默认值 2。出现此问题的原因是 NetScaler ADM 无法与许可服务器通信。

  [NSHELP-34299]

- 在网关 **> HDX Insight >** 实例中，当您选择一个实例并导出数据时，桌面用户的用户名信息不可用。应用此修复后，用户名信息也可以在报告中找到。

  [NSADM-96024]

基础结构

- 即使在所有进程都已启动并运行之后，NetScaler ADM 状态也会间歇性地显示为“关闭”。

  [NSHELP-35408]

- 在 应用程序 **>** 配置 **>** 配置包中，当您使用 属性 **>** 显示键的搜索条件输入搜索查询时，会显示搜索结果，但搜索栏会显示结果的索引号。

  修复后，搜索栏以文本而不是数字显示搜索查询。

  [NSADM-96859]

管理和监视

- 在 NetScaler ADC 版本 13.1 及更高版本中，在 NetScaler ADC 升级期间不执行 ISSU 命令。

  [NSHELP-35391]

- 当您在基础架构 **>** 实例 **> NetScaler > SDX** 中选择 SDX 实例配置 **SNMP** 时，会显示一条错误消息。如果将 SDX 配置文件配置为 SNMP v3 和 **NoAuthNoPriv** 作为安全级别，则会出现此问题。

  [NSHELP-35324]

- 在 ADM 审核日志（设置 **> ADM** 审核日志消息）中，密码在消息中可见。

  [NSHELP-35316]

- NetScaler ADM 会消耗更多的磁盘空间，因为 `mas_hb_monit.log` 文件未压缩。

  [NSHELP-35245]

- 如果重命名配置作业，则它不会在预定时间执行。

  [NSHELP-34990]

- 在基础结构 **>** 实例公告 **>** 升级建议中，版本 13.0 的维护结束 (EOM) 和生命周期结束 (EOL) 详细信息不正确。

  [NSHELP-34953]

- 将 ADM 升级到 13.1 37.38 版本后，拥有“只读”访问权限的用户无法在服务和服务组中搜索名称。显示错误消息“无权执行此操作”。

  [NSHELP-34808]

- NetScaler ADM 恢复操作间歇性挂起，登录页面被禁用。

  [NSHELP-3480]

- 在 基础架构 **>** 事件 **>** 系统日志消息中，当您在搜索查询中使用等号 (=) 符号搜索系统日志消息时，会显示“未找到行”消息。

  [NSHELP-34679]

- 在 ADM 用户界面中，SDX-Z 平台许可证的许可证到期时间错误地显示为 0。

  [NSHELP-35169]

- 尽管系统阈值尚未达到磁盘空间使用量的 80%，但由于存储空间问题，数据处理操作仍会中断。

  [NSHELP-35195]

- 使用 NetScaler ADM 执行灾难恢复后，不会在 NetScaler 中重新配置许可证服务器 IP 地址。

  [NSHELP-34015]

样书

- 即使超过文件大小限制，NetScaler ADM 样书日志文件也不会被压缩，因此会占用更多的磁盘空间。

  [NSHELP-35250]

已知问题

版本 13.1—48.47 中存在的问题。

分析

- 在 Web Insight 中，当您向下钻取任何指标以查看详细信息，然后进一步向下钻取任何指标时，图表仍保留在先前的视图中，但所有其他详细信息均按预期显示。

  因此，这就形成了一种假设，即进一步的向下钻取没有按预期进行。

  [NSADM-98995]

- 在 HDX Insight 中看不到分析。即使 NetScaler ADM 重新启动，分析也仅在短时间内可见，稍后变为不可见。

  [NSHELP-35128]

基础结构

- 在“设置”**>**“部署”**>**“强制故障转移”中对 ADM HA 对执行故障转移后，在“设置”**>**“部署”页面中看不到辅助节点的详细信息。

  [NSADM-98674]

- 当您重命名包含 IP 地址和分区名的应用程序时，该应用程序将从“设置”**>**“用户和角色”**>**“修改系统组”**>**“授权设置”**>**“应用程序”页面中删除。

  解决办法：命名应用程序时不要包含 IP 地址和分区名称。

  [NSADM-98635]

- 当您尝试在“设置”**>**“通知”**>**“**Slack**”**>**“添加”中添加 Slack 配置文件时，该配置文件未被添加，您会收到以下错误消息：

  ```
  Please check internet connectivity
  ```

  [NSADM-98633]

- 当您使用 appAdminPolicy 或 appReadOnlyPolicy 角色登录时，您可能会看到在“设置”**>**“用户和角色”**>**“访问策略”中启用的其他功能，尽管您在 NetScaler ADM 控制面板中看不到这些功能。之所以显示“访问策略”页面中的这些附加功能，是因为应用程序和网络功能依赖于它们，但这并不意味着您拥有对这些附加功能的完全权限。

  [NSADM-98055]

- 修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

  [NSADM-94279]

管理和监视

- 如果您使用 VMware vMotion 在 EXSi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道就会中断。因此，您无法访问 ADM GUI。

[NSHELP-32647]

- 在网关 **> HDX Insight** 中，由于数据库损坏，数据不会显示。

  [NSHELP-30459]

- 在 ADM HA 对中，即使多次尝试使用 GUI 中的“同步数据库”选项，数据库状态仍处于关闭状态且未同步。

  [NSHELP-29626]

Provisioning

- 从 OpenStack 删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1-45.61 版本的发行说明

February 6, 2024

本发行说明文档描述了 NetScaler ADM 版本 Build 13.1-45.61 中存在的增强和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

版本 13.1-45.61 中提供的增强和更改。

分析

使用“引导我”工作流程查看建议并将您的 **ADC** 和应用程序作为可操作的任务进行高效管理

在 NetScaler ADM GUI 中，引入了一个新的 任务 选项，您现在可以根据您的订阅和当前使用情况，查看有关许可、分析、事件、SSL 证书等的切实可行的建议。这些建议可确保您利用 NetScaler ADM 的所有功能，并启用产品推荐的产品发现和功能，以便有效地管理部署。

有关更多信息，请参阅 [查看推荐和高效管理您的 ADC]。(/en-us/netscaler-application-delivery-management-software/13-1/tasks-guide-me-workflow.html)

[NSADM-91872]

基础结构

支持 **NetScaler ADM** 代理的 **SNMP** 功能

在 基础架构 **>** 代理 **>** 管理 **SNMP** 中，您现在可以为代理创建 SNMP 管理器、SNMP 用户和 SNMP 视图。

有关更多信息，请参阅为 NetScaler ADM 代理创建 SNMP 管理器和用户。

[NSADM-91855]

添加新用户时查看用户名和密码标准

当您在“设置”**>**“用户与角色”**>**“添加”中添加新用户时，“用户名”和“密码”字段现在以红色文本显示以下条件：

- 允许的字符
- 最小和最大字符长度

如果您在字段中键入的字符符合条件，则红色文本将变为绿色。

[NSADM-91829]

支持在没有当前密码的情况下更改代理密码

作为超级管理员，您现在可以允许在不使用当前密码的情况下更改代理密码。

导航到“设置”**>**“管理”**>**“系统、时区、允许的 **URL** 和代理设置”**>**“基本设置”**>**“代理设置”，然后选中“删除更改代理密码的当前密码先决条件”复选框。更改代理密码页面将不再包含“当前密码”字段。

要再次显示“当前密码”字段，请清除“删除代理密码更改的当前密码必备条件”复选框。

[NSADM-91826]

在网络报告中为单个实体设置阈值

在基础结构 **>** 网络报告 **>** 阈值中，您现在可以在配置阈值时为特定实体设置阈值。

有关更多信息，请参阅 网络报告。

[NSADM-91727]

NetScaler 实例升级方面的改进功能

升级前验证选项卡中现在提供以下更改：

- 禁止升级的实例部分 - 此新部分列出了由于升级前验证错误而被阻止升级的实例。

- 快速清理按钮 - 此按钮在“磁盘空间详细信息”窗格中可用，可让您快速释放多个文件夹中的磁盘空间。

有关更多信息，请参阅 创建 ADC 升级作业。

[NSADM-91505]

VMware ESXi 上的 **NetScaler ADM** 代理的自动化

在 VMware ESXi 上部署 NetScaler ADM 代理现已自动部署。作为管理员，您现在可以自动执行以下操作：

- 配置代理。
- 注册代理并更改代理的默认密码。

有关更多信息，请参阅在 VMware ESXi 上自动部署 NetScaler ADM 代理。

[NSADM-87308]

已修复的问题

版本 13.1-45.61 中解决的问题。

分析

HDX Insight 和 **Gateway Insight** 中的带宽数据以每秒字节数而不是每秒位数显示不正确。

[NSHELP-34836]

在 HDX Insight 中看不到分析。即使重新启动 NetScaler ADM，分析也只能在最短的时间内可见，以后再也不可见。

[NSHELP-34561]

在 **Gateway > HDX Insights >** 用户的“已终止会话”下，缺少国家、地区和城市等位置信息。

通过此修复，此问题已得到解决。

[NSHELP-34130]

NetScaler ADM 磁盘空间会定期充满崩溃文件。结果，NetScaler ADM 停止了响应。

基础结构

在高可用性部署中，无法选择仅将构建映像文件上载到辅助节点。

作为修复的一部分，您现在可以从 基础结构 **>** 升级作业 **>** 创建任务选项卡 ****** 仅上载到辅助节点，将构建映像文件上载到辅助节点 ******。

[NSADM-96079]

管理和监视

在基础结构 **>** 实例 **>** 代理中，安装带有密码加密密钥的 SSL 证书后，端口 443 上与代理的连接将失败。

[NSHELP-33614]

Provisioning

重启后 NetScaler ADM GUI 无法加载。出现此问题是由于控制中心服务造成的。

通过此修复，控制中心服务功能已被禁用，此问题已得到解决。

[NSHELP-34543]

已知问题

版本 13.1-45.61 中存在的问题。

基础结构

修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

[NSADM-94279]

管理和监视

在 基础结构 **> SSL** 控制面板 **>** 管理证书存储中，当您单击“导入 **ADC** 证书”时，NetScaler ADM 无法导入 PFX 格式的 ADC 证书。

[NSHELP-34803]

如果您使用 VMware vMotion 在 EXSi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道就会中断。因此，您无法访问 ADM GUI。

[NSHELP-32647]

在网关 **> HDX Insight** 中，由于数据库损坏，数据不会显示。

[NSHELP-30459]

在 ADM HA 对中，即使在 GUI 中尝试多次使用同步数据库选项后，数据库状态仍处于关闭状态，并且未同步。

[NSHELP-29626]

Provisioning

从 OpenStack 删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

[NSADM-89919]

NetScaler ADM 13.1—42.47 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—42.47 中存在的增强功能和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

Build 13.1—42.47 中提供的增强功能和更改。

基础结构

NetScaler ADM 中显示的 **Z** 许可证到期信息　现在，您可以导航到基础结构 **>** 池许可 **>** 池容量 **> Z** 许可证，在 NetScaler ADM 中查看 MPX 和 SDX 实例的 Z 许可证到期信息。

[NSADM-80202]

管理和监视

支持在没有当前密码的情况下更改代理密码　作为超级管理员，您现在可以允许在不使用当前密码的情况下更改代理密码。

导航到“设置”**>**“管理”**>**“系统配置”**>**“代理设置”，然后选中“删除代理密码更改的当前密码必备条件”复选框。更改代理密码页面将不再包含“当前密码”字段。

要再次显示“当前密码”字段，请清除“删除代理密码更改的当前密码必备条件”复选框。

[NSADM-92585]

NetScaler ADM 中已停产的 **SD-WAN** 和 **HAProxy** 功能　NetScaler ADM 不再支持 SD-WAN 和 HAProxy 功能。因此，适用于 SD-WAN 和 HAProxy 的关联功能现在在 NetScaler ADM GUI 中不可用。

[NSADM-90549]

NetScaler Syslog 捕获 **NetScaler ADM** 服务完成的配置作业的用户信息　当用户在 NetScaler ADM 服务中运行配置作业时，作业中的命令将根据 NetScaler ADM 登录用户名进行记录，并存储在 NetScaler 系统日志文件中。

[NSADM-80418]

样书

表示子网值的新参数类型　现在，您可以在创建样书模板时指定 `type: ipnetwork` 的参数。这些参数允许将子网或 CIDR 值作为样书的输入提供。样书配置 GUI 显示此参数的以下任一字段：

- **IP** 地址和网络掩码长度
- **IP** 地址和网络掩码 **IP**

您可以通过开关选择使用网络掩码长度或网络掩码 IP：

- 启用输入网络掩码长度的开关
- 禁用输入网络掩码 IP 地址的切换

[NSADM-80696]

已修复的问题

版本 13.1—42.47 中解决的问题。

分析

在“安全”**>**“安全违规”**>**“所有违规”中，当您查看以下违规的详细信息时，可能会显示一条错误消息：

- HTTP 慢洛里斯
- DNS 慢洛里斯
- HTTP 慢速发布
- NXDOMAIN 淹没攻击
- HTTP 取消同步
- Bleichenbacher 攻击

- Segment Smack 攻击

[NSHELP-34006]

NetScaler ADM GUI 不显示标记为“WAF 其他”的违规行为。作为修复的一部分，这些违规行为现在出现在“安全” **>**“安全控制面板” **>**“应用程序安全调查器” **>**“**WAF** 其他”中。

[NSHELP-33757]

高可用性

在 NetScaler ADM 高可用性部署中，当您更改 NetScaler ADM 辅助节点的密码并重新启动系统时，NetScaler ADM 辅助节点将重置为旧密码。

[NSHELP-34016，NSHELP-34069]

对于 NetScaler ADM HA 部署，辅助节点的统计信息在设置 **>** 部署下不可见。

通过此修复，此问题现已解决。

[NSHELP-32746]

基础结构

当您通过导航到“设置” **>**“管理” **>**“配置 **SSL** 设置”并单击编辑设置下的密码套件来编辑 应用的密码套件时，会显示一条错误消息。

[NSADM-91382]

管理和监视

- 有时，在 NetScaler ADM HA 设置中，NetScaler ADM 辅助服务器上的文件同步会失败。

  [NSHELP-34070]

- 在基础架构 **>** 网络功能中，负载平衡页面需要很长时间才能加载。如果您属于具有正则表达式的组，则会出现此问题。

  作为管理员，您可以在“设置” **>**“用户和角色” **>**“创建系统组” **>**“授权设置” **>**“选择应用程序” **>**“为应用程序添加正则表达式”中添加正则表达式。

  [NSHELP-34035]

- 基础架构 **>** 网络报告 **>** 阈值中显示的条目数与每页 _ 项目数 _ 下拉菜单不匹配。

  [NSHELP-33895]

- 在“设置”**>**“网络功能”**>**“负载平衡”中，如果您按主机名或分区筛选虚拟服务器，则搜索结果会花费更多时间。如果您属于多个组，则会出现此问题。

  [NSHELP-33856]

- 在基础结构 **>** 升级作业中，当您选择已完成的作业，该作业的升级前或升级后脚本文件名带有特殊字符，然后从“选择操作”列表中下载输出脚本时，将显示“找不到文件”错误消息。

  [NSHELP-33854]

- 在 NetScaler ADM GUI 中，导航到升级作业 **>** 操作 **>** 下载升级后脚本输出或下载升级后故障转移后脚本输出时，您会看到“文件 **[**文件名**]** 不存在”错误消息。

  即使您执行了以下操作，仍会看到错误消息：

  1. 导航到升级 **NetScaler >** 自定义脚本
  2. 上载用于升级前的脚本文件。
  3. 选中故障转移前升级后和故障转移后升级后的使用与升级前相同的脚本复选框。

  [NSHELP-33836]

- 在基础架构 **>** 网络功能中，负载平衡页面显示所有虚拟服务器和实体。即使管理员通过选择所选实例的应用程序 **>** 所有应用程序来创建组，该组必须仅显示绑定到该实例的应用程序，也会发生这种情况。

  作为管理员，您可以在“设置”**>**“用户和角色”**>**“创建系统组”中创建组。

  [NSHELP-33809]

- 在 NetScaler ADM HA 对中，SNMP 陷阱在故障转移场景中不会生成。

  [NSHELP-33678]

- 被分配 appAdmin 或 appReadonly 角色的用户看不到 NetScaler ADM GUI 中应用程序下的所有功能。

  [NSHELP-33634]

- 将 NetScaler ADM 从 12.1 升级到 13.1 Build 33.50 后，ADC 事件修剪失败。因此，NetScaler ADM 在获取报告时停止响应。

  [NSHELP-33608]

- 从 NetScaler ADM 12.1 版本升级到 13.1 版本后，当您在基础架构 **>** 网络功能页面中启用或禁用虚拟服务器时，NetScaler ADM GUI 上会显示 `Not Authorized` 错误。

  [NSHELP-33592]

- 配置许可证页面（设置 **>** 许可和分析配置）显示所有虚拟服务器，而不仅仅是创建组时添加的虚拟服务器。

  作为管理员，您可以在“设置”**>**“用户和角色”**>**“创建系统组”**>**“授权设置”中添加虚拟服务器。

  [NSHELP-33584]

- 虚拟服务器页面（基础架构 **>** 网络功能 **>** 负载平衡）显示所有应用程序，而不仅仅是与特定组关联的应用程序。如果在“为应用程序添加正则表达式”字段（“设置” **>** “用户和角色” **>** “创建/修改系统组” **>** “授权设置” **>** “应用程序” **>** “特定应用程序”）中引入空字符串，则会出现此问题。

  [NSHELP-33556，NSHELP-33870]

- 从 NetScaler ADM 12.1 版本升级到 13.1 版本后，所有应用程序都显示在负载平衡页面（基础架构 **>** 网络功能）中，而不仅仅显示授权的应用程序。出现此问题的原因是未保存为应用程序配置的正则表达式。

  作为管理员，您可以在“设置” **>** “用户和角色” **>** “创建系统组” **>** “授权设置” **>** “创建应用程序” **>** “为应用程序添加正则表达式”中配置正则表达式。

  [NSHELP-3353]

- 即使在访问策略中定义了权限，也无法通过 NetScaler ADM 完成启用或禁用操作。权限通过 NetScaler ADM GUI 中的以下导航路径定义：设置 **>** 用户和角色 **>** 访问策略 **>** 基础架构 **>** 网络功能 **>** 负载平衡 **>** 虚拟服务器 **>** 启用-禁用。

  [NSHELP-33497]

- 在 NetScaler ADM GUI 中，当您从基础架构 **>** 实例控制板 **> NetScaler >** 选择操作 **>** 注释中为 NetScaler HA 对添加注释时，注释仅保存 NetScaler 主实例。HA 故障转移后，新的 NetScaler 主实例不显示注释。

  [NSHELP-33387]

- 即使启用了 TLS 1.2 SSL 协议，NetScaler ADM 和 SMTP 服务器之间的 SSL 加密也无法按预期运行。因此，SSL 跟踪中显示了错误的密码。

  [NSHELP-33363]

- “mas_inventory”子系统间歇性地崩溃。

  [NSHELP-33234]

- 如果服务或服务组未绑定到任何虚拟服务器，则在基础架构 **>** 网络功能 **>** 负载平衡中启用和禁用服务或服务组将失败。

  [NSHELP-32999]

- 当 NetScaler ADM 收到来自 NetScaler 的 URI 语法错误的系统日志消息时，基础结构 **>** 事件摘要中的系统日志消息页面显示为空白。

  [NSHELP-32912]

- 外部 TACACS 身份验证服务器的 NetScaler ADM 登录基于质询的身份验证失败。

  [NSHELP-33960]

- 在 NetScaler ADM GUI 中创建组会导致配置错误，因为 **API** 网关类别显示在“设置” **>** “用户和角色” **>** “组” **>** “添加” **>** “创建系统组” **>** “授权设置”页面中。作为修复的一部分，授权设置页面不显示 **API** 网关。

  [NSHELP-33524]

- NetScaler SDX 实例获得的许可不正确。因此，会为不由 NetScaler ADM 代理管理的 SDX 实例生成 SNMP 陷阱。

  [NSHELP-33415]

Provisioning

- 非对称加密单元 和 对称加密单元 现在是 NetScaler ADM GUI 中的可编辑字段。在配备了 Intel Coleto (COL) 芯片的 NetScaler SDX 设备上配置 NetScaler VPX 实例时，您可以输入 ASU 和 SCU 的数量。

  导航到 基础架构 **>** 实例 **> NetScaler**，然后在 SDX 选项卡上，选择要在其中配置 NetScaler VPX 实例的 SDX 实例。在“选择操作”中，选择“配置 **VPX**”，然后在显示的页面中，在“加密 分配”下输入加密容量

  [NSHELP-33297]

样书

- 使用在版本 13.0 或更早版本中创建的样书创建或更新配置包时，会显示错误消息“`unknown parameters received in payload`”。

  [NSHELP-33412]

用户界面

- 在 NetScaler VPX 实例进行 HA 故障转移后，不会在基础架构 **>** 网络功能 **>** 负载平衡中更新主节点和辅助节点状态。

  [NSHELP-33798]

- 在“设置”**>** “**ADM** 系统事件”**>** “消息”列中截断了消息，您必须选择该条目并单击“详细信息”才能了解有关该消息的更多信息。通过此修复，您可以在消息列中查看完整的消息。

  [NSHELP-33772]

已知问题

13.1—42.47 版本中存在的问题。

管理和监视

- 当分配了 `appAdmin` 或 `appReadonly` 角色的用户导航到基础架构 **>** 负载平衡 **>** 服务/服务组并使用名称键作为搜索筛选器时，会显示“未授权”错误。

  [NSHELP-34194]

- 如果您使用 VMware vMotion 在 ESXi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道将中断。因此，您无法访问 ADM GUI。

  [NSHELP-32647]

- 修改系统组页面（设置 **>** 用户和角色 **>** 组 **>** 编辑）需要很长时间才能加载。如果该组有两个或多个用户角色以及与之关联的正则表达式，则会出现此问题。

  [NSADM-94279]

调配

- 从 OpenStack 中删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1—37.38 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—37.38 中存在的增强功能和更改、已修复和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

版本 13.1—37.38 中提供的增强功能和更改。

基础结构

在 **NetScaler ADM** 上预览实例公告的详细信息　实例公告现已作为预览功能在 NetScaler ADM 中提供，其中包含安全和升级公告的详细信息。NetScaler ADM 对 ADC 执行版本扫描，以检查 CVE，并获取有关运行 EOM/EOL 版本的 ADC 的详细信息。

要获取有关最新 CVE、自定义扫描以及修复和升级工作流程的更新，您可以选择 ADC 实例并将其加载到 ADM 服务。有关更多信息，请参阅实例公告。

有关在 ADM 服务中加载 ADC 实例的信息，请查看实例公告页面上提供的 GIF 动画。

[NSADM-88911]

查看非托管 **CICO ADC** 实例的使用情况和许可证信息　现在，您可以导航到基础结构 **>** 池许可 **>** 带宽许可证 **> CICO**，查看 NetScaler ADM 上非托管 NetScaler 实例的使用情况和许可证信息。

[NSADM-85452]

样书

样书支持 **NetScaler BLX** 实例　在创建配置包时，您现在可以选择 NetScaler BLX 实例作为目标实例。早些时候，样书支持 NetScaler MPX、SDX、VPX 和 CPX 实例。

[NSADM-86253]

已修复的问题

版本 13.1—37.38 中已解决的问题。

分析

- 在与 NetScaler ADM 集成的 Citrix Director 上，当您导航到趋势 **>** 网络时，无法访问“网络”选项卡并显示一条错误消息。作为修复的一部分，您现在可以毫无问题地访问“网络”选项卡。

  [NSHELP-31776]

管理和监视

- 当 NetScaler ADM 收到来自 NetScaler 的 URI 语法错误的系统日志消息时，基础结构 **>** 事件摘要中的系统日志消息页面显示为空白。

  [NSHELP-32912]

- 有时，ADM 备份文件的临时文件夹不会从 /var/mps/backup 文件夹中删除。

  [NSHELP-32606]

- 在基础结构 **>** 实例 **> NetScaler** 中，当您选择 ADC 实例并尝试配置分析时，虚拟服务器的吞吐量显示为零。只有在搜索栏中添加任何过滤器时，才会出现此问题。

  [NSHELP-32390]

- NetScaler ADM 未记录 HA 强制故障转移命令的详细信息。通过此修复，ADM HA Force 故障切换详细信息将在运行命令之前记录在外部服务器中。

  [NSHELP-32366]

- 当您导航到基础结构 **>** 事件 **>** 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时，您无法选择和分配信息作为新的严重性级别。

  [NSHELP-32328]

- 在 ADM GUI 中，缺少一些 SDX SNMP 陷阱，因为 ADM 无法处理来自 SDX 设备的这些陷阱。

  [NSHELP-32326]

Provisioning

- 非对称加密单元 和 对称加密单元 现在是 NetScaler ADM GUI 中的可编辑字段。在配备了 Intel Coleto (COL) 芯片的 NetScaler SDX 设备上配置 NetScaler VPX 实例时，您可以输入 ASU 和 SCU 的数量。

  导航到 基础架构 > 实例 > **NetScaler**，然后在 SDX 选项卡上，选择要在其中配置 NetScaler VPX 实例的 SDX 实例。在“选择操作”中，选择“配置 **VPX**”，然后在显示的页面中，在“加密 分配”下输入加密容量

  [NSHELP-33297]

样书

- 当您使用在 13.0 或更早版本中创建的样本创建或更新配置包时，会显示一条错误消息“负载中收到未知参数”。

  [NSHELP-33478]

已知问题

版本 13.1—37.38 中存在的问题。

分析

- 在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

  [NSHELP-26545]

管理和监视

- 如果您使用 VMware vMotion 在 ESXi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道将中断。因此，您无法访问 ADM GUI。

  [NSHELP-32647]

- 配置第二个 NIC 以隔离对 NetScaler ADM 的管理访问时，第二个 NIC IP 地址被错误地分配了与主 NIC 相同的 IP 地址。

  [NSHELP-32567]

调配

- 从 OpenStack 中删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

  [NSADM-89919]

NetScaler ADM 13.1-33.50 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1-33.50 中存在的增强功能和更改、已修复问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

Build 13.1-33.50 中提供的增强功能和更改。

基础结构

支持 **ADM** 代理的双网卡

您可以在 ADM 代理上配置第二个 NIC 来管理对 NetScaler ADM 的访问权限。使用双 NIC 体系结构，ADM 代理现在能够：

- 在 ADM 代理和 ADC 实例之间建立通信
- 在 ADM 代理和 ADM 服务之间建立通信

有关更多信息，请参阅 NetScaler ADM 上的双网卡支持。

[NSADM-85781]

查看非托管 **CICO ADC** 实例的使用情况和许可证信息

现在，您可以导航到 基础结构 **>** 池化许可 **>** 带宽许可证 **> CICO** 以查看 ADM 服务上非托管 CICO ADC 实例的使用情况和许可证信息。

[NSADM-85452]

样书

样书支持 **NetScaler BLX** 实例

在创建配置包时，您现在可以选择 NetScaler BLX 实例作为目标实例。早些时候，样书支持 NetScaler MPX、SDX、VPX 和 CPX 实例。

[NSADM-86253]

已修复的问题

在 Build 13.1-33.50 中解决的问题。

样书

将 NetScaler ADM 从任何旧版本升级到任何版本（13.1.9.x 版本-13.1.30.x 版本）后，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

[NSHELP-33127]

分析

在与 NetScaler ADM 集成的 Desktop Director 上，当您导航到 趋势 **>** 网络时，网络选项卡无法访问并出现错误消息。作为修复的一部分，您现在可以毫无问题地访问“网络”选项卡。

[NSHELP-31776]

管理和监视

有时，ADM 备份文件的临时文件夹不会从 /var/mps/backup 文件夹中删除。

[NSHELP-32606]

配置第二个 NIC 以隔离对 NetScaler ADM 的管理访问时，第二个 NIC IP 地址被错误地分配了与主 NIC 相同的 IP 地址。

[NSHELP-32567]

在基础结构 **>** 实例 **> NetScaler** 中，当您选择 ADC 实例并尝试配置分析时，虚拟服务器的吞吐量显示为零。只有在搜索栏中添加任何过滤器时，才会出现此问题。

[NSHELP-32390]

当您导航到基础结构 **>** 事件 **>** 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时，您无法选择和分配信息作为新的严重性级别。

[NSHELP-32328]

在 ADM GUI 中，缺少一些 SDX SNMP 陷阱，因为 ADM 无法处理来自 SDX 设备的这些陷阱。

[NSHELP-32326]

将 NetScaler ADM 从版本 12.X 升级到版本 13.X 时，您无法访问 GUI。

[NSHELP-32224]

当您导航到“基础结构”**>**“**SSL** 控制面板”**>**“**SSL** 证书”页面时，单击“导出”图标并下载 CSV 格式的报告时，域信息不会导出，显示为空白。

[NSHELP-30767]

已知问题

版本 13.1-33.50 中存在的问题。

分析

在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

[NSHELP-26545]

管理和监视

如果您使用 VMware vMotion 在 EXSi 虚拟机管理程序上安排 ADM 服务器迁移，高可用性节点上的数据库流通道就会中断。因此，您无法访问 ADM GUI。

[NSHELP-32647]

调配

从 OpenStack 删除负载平衡虚拟服务器失败，因为 NetScaler ADM 不接受删除请求。即使删除绑定到负载平衡虚拟服务器的组件，此问题仍然存在。

[NSADM-89919]

NetScaler ADM 13.1.30.52 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1.30.52 中存在的增强和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

版本 13.1.30.52 中提供的增强功能和更改。

配置一个应用程序并将其与多个自定义应用程序关联

在 应用程序控制板中，您现在可以配置应用程序并将其与多个自定义应用程序关联。使用此功能，您可以对多个自定义应用程序重复使用同一个应用程序，而不必为每个自定义应用程序创建单独的应用程序。

有关更多信息，请参阅 配置应用程序并将其与多个自定义应用程序关联。

[NSADM-82040]

在 **Web** 事务分析中支持 **CSV** 格式和计划导出

在 Web 事务分析中，当您单击“导出”图标时，您现在可以查看以下增强功能：

- 在“立即导出”中，可以以 CSV 格式导出数据。
- 引入了“计划导出”选项，使您可以通过电子邮件和 Slack 计划并以 CSV 格式导出数据。

有关更多信息，请参阅 Web 事务分析。

[NSADM-43847]

配置升级作业的访问策略

作为超级管理员，您现在可以配置访问策略，设置升级作业的权限（查看/编辑），并将该策略应用于您的 NetScaler ADM 用户。在“设置”**>**“用户和角色”**>**“访问策略”中，单击“添加”，通过选择“权限”下的“基础结构”**>**“升级作业”来配置访问策略。

[NSADM-82494]

已修复的问题

版本 13.1.30.52 中解决的问题。

分析

- 启用分析或编辑从 HA 对配置的 NetScaler Gateway 虚拟服务器的分析后，高级设置（可选）下的 实例级别选项 将显示为禁用，即使启用了这些选项。

  [NSHELP-32188]

- 在“网关”**>**“**HDX Insight**”**>**“实例”中，当您单击某个国家/地区以深入了解更多详细信息时，不会显示“当前会话”下的数据。

  [NSHELP-32125]

基础结构

- 在 基础结构 **>** 网络功能中，在 具有最高客户端连接的前 **5** 个虚拟服务器下，将鼠标悬停在数据点上时，主机名或 ADC IP 地址将显示在方括号中。如果 ADC 实例具有分区，并且 ADC 主机名和分区名称相同，则很难区分数据属于 ADC 还是分区。

  通过此修复，主机名包含一个分区标签，用于区分 ADC 分区的数据。

  [NSHELP-32153]

- NetScaler ADM 未记录 HA 强制故障转移命令的详细信息。通过此修复，ADM HA Force 故障切换详细信息将在运行命令之前记录在外部服务器中。

  [NSHELP-32366]

- 在“配置客户身份”页面中，“服务和数据共享”选项将自动启用，即使手动禁用了这些选项也是如此。

  [NSHELP-32149]

- 如果配置了第二个 **NIC**，NetScaler ADM 控制台将显示一条错误消息。

  [NSHELP-29316]

- 使用脚本同时创建多个 SNMP 用户时，向 ADM 发出的 SNMP 请求将失败。

  [NSADM-83924]

- 在基础架构 **>** 实例 **> NetScaler > SDX** 中，当您配置为在没有任何用户定义配置的情况下在 SDX 上预置 NetScaler VPX 实例时，现有的配置模板选项会阻止配置。

  通过此修复，配置模板 不再是必需选项。

  [NSADM-88360]

- 升级到 13.1 27.62 版本后，当您在基础结构 **>** 池化许可 **>** 带宽许可证 **>** 池容量中访问控制面板时，会显示一条错误消息。

  [NSHELP-32583]

样书

- 在 NetScaler ADM 13.1 17.42 中，ADM GUI 不显示样书页面。

  [NSHELP-31468]

- 样本不支持对配置的 NS IP 地址进行操作，即使该地址位于托管 ADC 实例的域中。

  [NSHELP-31113]

已知问题

13.1.30.52 版中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.30.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

分析

- 在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

  [NSHELP-26545]

基础结构

当您在 SDX 上预置与之前删除的 VPX 实例同名的 VPX 实例时，会显示一条错误消息。

[NSADM-76468]

NetScaler ADM 13.1—27.62 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—27.62 中存在的增强和更改、已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

NetScaler BLX 实例的升级支持

在基础结构 **>** 升级作业中，您现在可以创建作业来升级 NetScaler BLX 实例。您必须选择适当的构建映像（适用于 Ubuntu 或 Red Hat）才能成功升级。有关更多信息，请参阅 升级作业。

已修复的问题

Build 13.1—27.62 中解决的问题。

管理和监视

- 请考虑分配到以下两个组的用户已登录到 NetScaler ADM：
  - 所有应用程序和所有实例的只读角色
  - 一些负载平衡虚拟服务器的读写权限

  在“基础结构”**>**“网络功能”**>**“负载平衡”中，仅对分配的读取和写入虚拟服务器具有权限的用户也可获得只读虚拟服务器的权限。

  [NSHELP-32110]

- 如果您的 NetScaler ADM 有 80 多个托管实例（包括管理分区），并且当您尝试在 基础结构 **>** 网络功能中对虚拟服务器使用立即轮询选项时，不会同时为所有 ADC 实例触发轮询。

  [NSHELP-32028]

- 删除 ADM 上的外部 Syslog 服务器时，会向外部 syslog 服务器发送一条日志消息，指示已启动删除操作。

  [NSHELP-32001]

- 在 **SSL** 控制面板中，不会显示 **SSL** 证书的颁发者信息。

  [NSHELP-31691]

- 在 基础结构 **>** 升级作业中，当您创建升级作业时，升级前验证检查 将失败。

  [NSHELP-31575]

- 导航到“基础结构”**>**“许可证设置”时，选择所有已过期的许可证，然后单击“删除”以删除所有已过期的池许可证，所有池许可证过期事件也会自动清除。

  [NSHELP-31622]

- 在 ADM 中具有只读访问权限且与 CVAD 关联的用户无法访问 ADM GUI。

  [NSHELP-31419]

- 在“基础结构”**>**“事件摘要”**>**“系统日志消息”中，仅显示过去 30 天的数据。通过此修复，数据最多可显示 180 天。

  [NSHELP-30961]

- NetScaler ADM 向外部服务器发送不完整的系统日志消息，因为系统日志消息的限制为 480 字节。

  [NSHELP-30924]

- 导航到 基础结构 **> SSL** 控制面板 **> SSL** 证书 页面，单击“导出”图标并下载 CSV 格式的报告时，域信息不会导出，而是显示为空白。

  [NSHELP-30767]

高可用性

ADM HA 主 IP 不响应 SNMP GET 请求。

[NSHELP-31510]

已知问题

版本 13.1—27.62 中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.27.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

分析

在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

[NSHELP-26545]

基础结构

使用脚本同时创建多个 SNMP 用户时，向 ADM 发出的 SNMP 请求将失败。

解决方法：

手动创建 SNMP 用户。

[NSADM-83924]

管理和监视

- 导航到“基础结构”**>**“许可证设置”时，选择所有已过期的许可证，然后单击“删除”按钮以删除所有已过期的池许可证，所有池许可证过期事件也会自动清除。

  [NSHELP-31622]

NetScaler ADM 13.1-24.38 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1-24.38 的增强功能和更改、已修复的问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

版本 13.1-24.38 中提供的增强功能和更改。

管理和监视

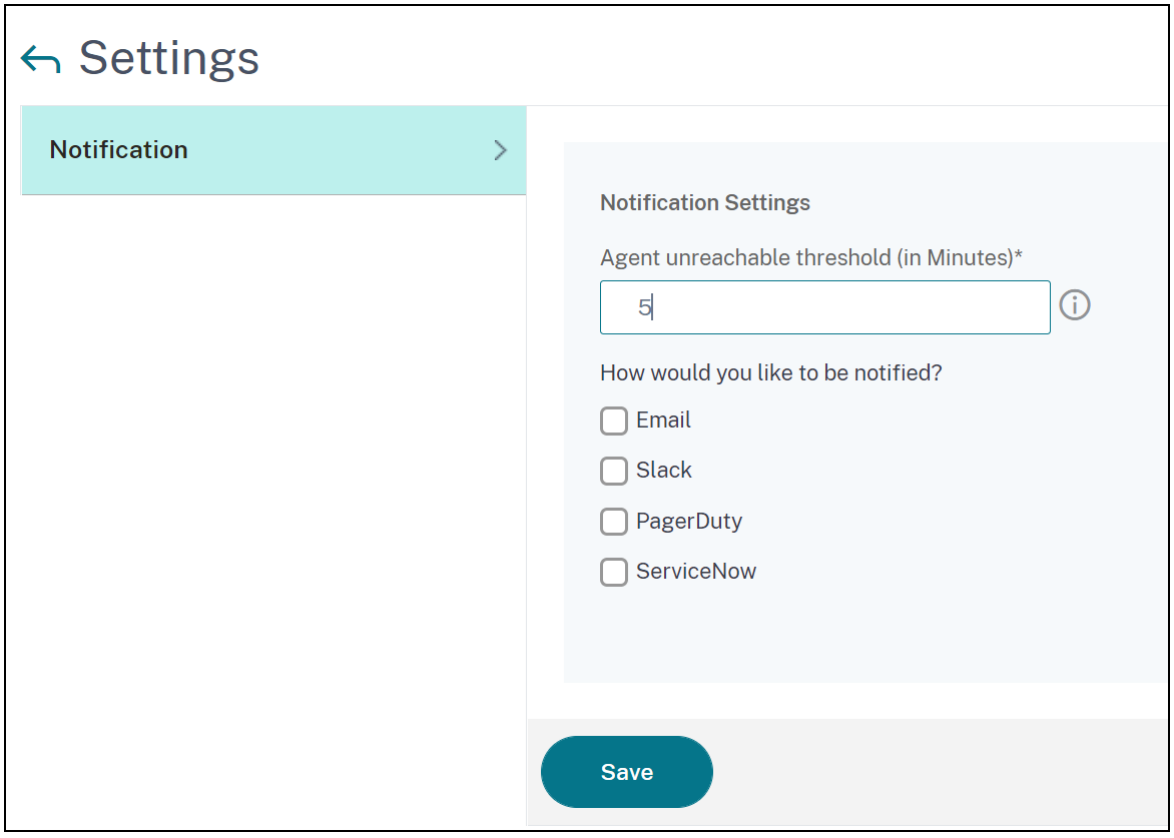
在应用程序控制板中保留筛选器　在“应用程序”**>**“控制板”中，当您通过搜索栏和关键量度应用筛选器时，筛选器现在会被保留。即使出现以下情况，您也可以查看相同的筛选器：

- 您可以从 ADM GUI 中的其他导航栏返回到“应用程序”**>**“控制板”。
- 关闭浏览器并从同一个浏览器中打开一个新会话。

> 注意
>
> 如果您使用其他浏览器或以隐身模式打开新会话，则不会保留过滤器。

[NSADM-82038]

配置 **ADM** 代理无法访问阈值和通知　在 基础结构 **>** 实例 **>** 代理 **>** 设置中，您现在可以配置阈值，并在 NetScaler ADM 代理在特定持续时间内无法访问 NetScaler ADM 代理时收到通知。



[NSADM-80415、NSADM-76845]

支持 **SSL** 控制板中的 **ECDSA** 算法　在 **SSL** 控制板 **>** 设置 **>** 企业策略中配置企业策略时，现在可以在 建议签名算法 中选择 **ECDSA**。

有关更多信息，请参阅 ECDSA 密码套件支持。

[NSADM-71321]

已修复的问题

Build 13.1-24.38 中解决的问题。

分析

- 当您在“网关”**>**“**HDX Insight**”**>**“用户”中选择要深入了解更多信息的用户时，当前会话下的会话类型 将显示 -1，而不是应用程序或桌面。

  [NSHELP-31178]

- NetScaler ADM 在处理分析数据时会消耗更多内存。

  [NSHELP-30895]

管理和监视

- 如果同一个域名绑定到具有 IPv4 和 IPv6 的 ADC 分区，则在 基础结构 **>** 网络功能 **> GSLB >** 虚拟服务器 中单击 立即轮询时会显示错误消息。通过此修复程序，NetScaler ADM 会将域名与虚拟服务器名称关联起来，以避免重复条目。

  [NSHELP-31513]

- 在 基础结构 **>** 实例 **> NetScaler** 中，当您更改管理员配置文件密码并在密码中包含% 时，将显示一条错误消息。

  [NSHELP-31392]

- 在“基础结构”**>**“池许可”中，当您尝试在非活动会话期间在“许可证文件”下下载许可证文件时，ADM 服务器会停止响应。

  [NSHELP-31323]

- 当 NetScaler SDX 设备在许可证宽限期内发送 SNMP 陷阱时，它们不会出现在 NetScaler ADM 上。

  [NSHELP-31286]

- 升级到 ADM 13.1 17.42 时，由于出现分裂的情况，该进程停止并显示错误消息。

  [NSHELP-31244]

- 在 SSL 控制面板中，使用的证书列表还会显示未绑定到任何虚拟服务器的 CRL 分布点 (CDP) 的 SSL 证书。

  通过此修复，SSL 控制板仅显示绑定到虚拟服务器的证书。

  [NSHELP-31137]
- 有时，基础结构 **>** 事件 > **syslog** 消息中的“syslog 消息”页面不显示数据，而是显示错误消息。

  [NSHELP-30888]
- 在“设置”**>**“通知”**>**“**ServiceNow**”中，当您单击 ServiceNow 票证时，详细信息在 ADM GUI 中不可见。

  [NSHELP-30751]
- 配置作业将通过 NetScaler ADM 本地代理持续对所有托管 ADC 实例执行。

  [NSHELP-30677]
- 将 NetScaler SDX 实例的备份文件副本传输到另一个系统时，它将失败。此问题已修复。

  [NSHELP-30650]
- 如果在重新启动 ADM 或强制执行 ADM 故障转移后 5 分钟内启动 ADM 升级任务，则升级将失败。

  [NSHELP-31715]
- 在 基础结构 **>** 实例 **> NetScaler** 中，当您尝试在云上预配 NetScaler VPX 时，未显示 CICO 许可文件。

  通过此修复，CICO 许可证文件受支持。

  [NSHELP-30186]

用户界面

在 NetScaler ADM 证书存储中，当您更新现有证书时，`Cert_Store_ID cannot be empty` 会显示一条错误消息。

[NSHELP-31136]

已知问题

13.1-24.38 版中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.24.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

基础结构

使用脚本同时创建多个 SNMP 用户时，向 ADM 发出的 SNMP 请求将失败。

解决方法：

手动创建 SNMP 用户。

[NSADM-83924]

管理和监视

- 如果配置了第二个 **NIC**，NetScaler ADM 控制台将显示一条错误消息。

  [NSHELP-29316]

- ADM HA 主 IP 不响应 SNMP GET 请求。

  [NSHELP-31510]

- 在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

  [NSHELP-26545]

NetScaler ADM 13.1—21.53 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—21.53 的增强功能和更改、已修复的问题和已知问题。

备注

- 本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。
- 内部版本 **13.0-21.53** 及更高版本解决了 https://support.citrix.com/article/CTX460016 中所述的安全漏洞。
- **Build 21.53** 取代了 **Build 21.50**。

新增功能

内部版本 13.1—21.53 中提供的增强功能和更改。

管理和监视

支持 **ShowConfiguration** 模板　在配置编辑器中，当您选择批处理配置时，现在可以使用 **ShowConfiguration** 模板。将 **ShowConfiguration** 模板拖到右窗格中，然后输入要在 NetScaler 实例上运行的 show 命令。

例如，您可以输入 **sh ns info**、**sh node**、**sh ns stats** 和 **sh interface, shell ls /var/tmp** 等命令并查看输出。

您可以将命令的输出作为文本文件下载。

[NSADM-66132、ADSS-4331]

ADM 中的新网络报告　以下新网络报告将添加为总计数器：

- 身份验证成功与失败
- **HTTP** 身份验证成功与失败
- 非 **HTTP** 身份验证成功与失败
- 身份验证、授权和审核会话
- 当前身份验证、授权和审核会话
- 当前 **ICAOnly** 会话
- 当前 **ICAOnly** 连接
- 当前的 **ICA (Smart Access)** 连接

您可以使用这些计数器来添加阈值和接收通知。有关更多信息，请参阅 网络报告。

[NSADM-62239]

已修复的问题

在版本 13.1—21.53 中解决的问题。

高可用性

在 ADM 高可用性对中，如果在主节点而不是辅助节点上运行复制脚本，则 ADM GUI 将无法访问，并且数据库流式传输通道在节点之间断开。应用此修复后，该脚本现在只能在辅助 ADM 节点上运行。

[NSHELP-30909]

管理和监视

- ADM GUI 不会显示托管在 SDX 设备（特别是 15XXX、26XXX）上的 VPX 实例的型号 ID。

  [NSHELP-28103]

- NetScaler ADM 向外部服务器发送不完整的系统日志消息，因为系统日志消息的限制为 480 字节。

  [NSHELP-30924]

用户界面

上载扩展名为.conf 的恶意配置建议文件时，NetScaler ADM 将无法检测和阻止此文件。应用此修复后，NetScaler ADM 可防止上载恶意文件。

[NSHELP-30171]

已知问题

13.1—21.53 版中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.21.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

基础结构

使用脚本同时创建多个 SNMP 用户时，向 ADM 发出的 SNMP 请求将失败。

解决方法：

手动创建 SNMP 用户。

[NSADM-83924]

管理和监视

- 在“基础结构”**>**“事件摘要”**>**“系统日志消息”中，仅显示过去 30 天的数据。通过此修复，数据最多可显示 180 天。

  [NSHELP-30961]

- 有时，基础结构 **>** 事件 > **syslog** 消息中的“syslog 消息”页面不显示数据，而是显示错误消息。

  [NSHELP-30888]

- 如果配置了第二个 **NIC**，NetScaler ADM 控制台将显示一条错误消息。

  [NSHELP-29316]

- 在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

  [NSHELP-26545]

NetScaler ADM 13.1-17.42 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM Build 13.1-17.42 中存在的增强功能和更改、已修复的问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

Build 13.1-17.42 中提供的增强功能和更改。

管理和监视

ADM 对 **BLX** 群集的支持　现在，您可以在 ADM 中添加 BLX 群集。在 ADM GUI 中，添加了群集 IP 地址 (CLIP)，现在可以在控制板中看到群集节点的计数。

[NSADM-78588]

改进了处理损坏的数据库流媒体渠道问题

在高可用性部署设置中，每当出现流式复制错误时，NetScaler ADM 都会自动检测到数据库流式传输通道已损坏，并在后台自动触发数据库同步。每 24 小时恢复一次损坏的数据库流通道。用户还可以使用“同步数据库”按钮从 GUI 手动 同步数据库。配置文件会自动从主节点同步到辅助节点，然后进行数据库的自我复制。通过单击“设置”**>**“部署”下的“查看日志”按钮，可以查看数据库同步的进度。

[NSADM-71053]

管理 **GSLB** 群集中的 **ADC** 实例

有时，在 GSLB 群集中，ADC 实例的配置对象会尝试互相覆盖。而且，它会导致竞争条件。要解决此类问题，您需要控制 GSLB 群集中的主节点选择。主节点中的配置将应用于其余的 ADC 实例。在 NetScaler ADM 中，您现在可以创建 GSLB 群集组并添加 ADC 实例。您还可以在 ADC 实例中选择一个主节点，并设置主节点选择的优先级顺序。

在 网络函数 > **GSLB** 下，用户现在只能查看主 ADC 节点中的实体。

[NSADM-61374]

安全性

机器人洞察中的 **IPv6** 支持　现在，当您在安全 **>** 安全违规 **>** 应用程序概述中的机器人下钻应用程序时，日志将显示客户端 **IP** 和机器人真客户端 **IP** 的 IPv6 地址。

[NSADM-77376]

查看绑定到负载平衡虚拟服务器的内容交换虚拟服务器的分析

现在，在“安全”**>**“安全违规”中，“应用程序概述”选项卡会显示与负载平衡虚拟服务器绑定的内容交换虚拟服务器的分析。
单击内容交换虚拟服务器，在“绑定负载平衡服务器”下，可以查看绑定到内容交换虚拟服务器的负载平衡服务器列表。

[NSADM-77369]

在虚拟服务器上启用分析的统一过程

除了启用分析的现有流程外，您现在还可以使用单窗格工作流在以下位置配置分析：

- 所有获得许可的现有虚拟服务器
- 随后获得许可的虚拟服务器

配置完成后，此功能消除了在现有和后续虚拟服务器上手动启用分析的必要性。

有关详细信息，请参阅 启用分析的统一流程。

[NSADM-74747]

安全违规**-JSON SQL** 注入语法

在 **WAF** 下的“安全”**>**“安全违规”中，您现在可以查看所选应用程序的 **JSON SQL** 注入语法 违规。有关详细信息，请参阅 https://docs.citrix.com/en-us/citrix-application-delivery-management-service/analytics/security/application-overview.html。

[NSADM-62909]

样书

样书支持嵌套参数条件　在样书定义中，您现在可以在参数条件中指定参数条件。这些条件称为嵌套参数条件，并使用 repeat 构造来定义这些条件。当您想要对列表参数的每个项目应用操作时，嵌套参数条件非常有用。示例：

```
parameters-conditions:
  -
    repeat: $parameters.lbvservers
    repeat-item: lbvserver
    parameters-conditions:
      -
        target: $lbvserver.port
        action: set-allowed-values
        condition: $lbvserver.protocol == "HTTPS"
        value: $parameters.ssl-ports
<!--NeedCopy-->
```

在此示例中，当用户为负载平衡虚拟服务器选择 HTTPS 协议时，将动态填充端口值。而且，它适用于列表中的每个负载平衡虚拟服务器。

[NSADM-62747]

已修复的问题

Build 13.1-17.42 中解决的问题。

分析

有时，ADM GUI 会将 SSL 密码名称显示为 NA。

[NSHELP-27624]

高可用性

在 NetScaler ADM 中，当您计划在特定时间升级 NetScaler 实例时，升级将立即触发。它不会在预定时间发生。

[NSHELP-30654]

管理和监视

对于 ADC 高可用性对，您无法通过 ADM GUI 创建辅助节点的备份。

[NSHELP-30637]

导航到“设置”**>**“部署”时会显示一条错误消息。当您执行以下操作时，将显示此错误消息：

- 导航到 基础结构 **>** 实例 **> NetScaler > SDX**，选择一个实例，然后单击 控制板 以查看详细信息。
- 返回 SDX 选项卡，选择同一个实例，然后在 选择操作 列表中单击 取消 管理。

[NSHELP-30635]

单击“查看日志”时，将显示“数据库同步日志”消息，您可以查看同步进度的实时详细信息。但是，如果数据库同步过程未启动，则会显示异常消息。

使用此修复后，不会出现异常消息，但它现在将显示相应的消息。

[NSHELP-30547]

重新启动 NetScaler ADM 后，NTP 同步可能会停止工作。

[NSHELP-30500]

有时，ConfigAuditOnTrapJob 会在所有 ADC 实例上触发配置审核，而不仅仅是针对所需的 ADC 实例。

[NSHELP-30440]

在 基础结构 **>** 配置 **>** 配置作业中，使用录制并播放的配置作业将显示一条错误消息。

[NSHELP-30349]

当 ADC 高可用性对中的同步失败时，从属服务器无法从其主服务器复制配置更改。因此，分区和关联的用户组配置将从 ADM 中删除。而且，分区计数显示为零。

[NSHELP-30179]

在 基础结构 **>** 事件 **>** 事件设置中，不会显示 NetScaler SDX 实例的磁盘故障事件。

[NSHELP-30049]

使用电子邮件选项配置计划导出时，附件将作为空报告接收。

[NSHELP-29146]

使用“计划导出”选项生成的报告可能无法按预期工作。

[NSHELP-28839]

如果源 ADC 配置有任何需要用户输入的命令，则复制配置将失败。
以下是一个示例命令：

```
set ssl parameter - defaultProfile ENABLED
```

[NSADM-74706]

系统

在 ADM GUI 中，使用 TAR 命令重新打包 SDX 时，即使出现故障，重新打包活动的状态也会显示为“正在进行中”。

[NSHELP-30579]

ADM 子系统不会在 ADM 高可用性故障切换后启动。出现此问题的原因是 ADM 数据库以只读模式启动。

[NSHELP-30482]

NetScaler ADM 13.1-12.x 版本仅支持两个免费的虚拟服务器许可证。有关详细信息，请参阅许可。
升级到 13.1-12.x 内部版本后，如果任何虚拟服务器（已启用分析）未获得许可，所有虚拟服务器页面（设置 **>** 许可和分析配置 **>** 配置分析）中的分析状态可能仍然将其显示为已启用，但分析数据未显示在 ADM 中。

[NSADM-79893]

样书

将 NetScaler ADM 升级到后 13.1.12.x，ADM GUI 不会加载 样书 页面。

[NSHELP-30636]

当您在 ADC 高可用性对的主节点上部署配置包并且该节点出现故障时，辅助服务器上的配置包不会更新。因此，配置不会按预期在目标实例上维护。

[NSHELP-28829]

已知问题

13.1-17.42 版本中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.17.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

分析

在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据将变为无效且在 ADM 报告中不可用。

[NSHELP-26545]

在 Azure 云上配置 NetScaler ADM 13.1 本地代理时，会显示一条错误消息。

解决方法：

您可以忽略此错误消息并继续配置。

[NSADM-81739]

调配

当您使用 ADM 调配在 OpenStack Lbaas 上创建成员时，OpenStack 上的成员创建会间歇性失败。当 ADM 向调配服务的代理请求在 30 秒后超时时，会出现此问题。通过此修复，调配 API 的请求超时时间已增加到 120 秒。

[NSHELP-21490]

如果您正在使用 OpenStack Queens for LBaas 工作流程，负载平衡虚拟服务器不会绑定到内容交换虚拟服务器。此问题会影响流量。

解决方法：

1. 使用负载平衡虚拟服务器创建池。
2. 使用池 ID 创建侦听器。
   如果您已有侦听器，请使用池 ID 更新该侦听器。

[NSADM-36631]

NetScaler ADM 13.1—12.50 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—12.50 中存在的增强功能和更改、已修复问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

内部版本 13.1—12.50 中提供的增强功能和更改。

管理和监视

查看数据库同步日志消息　在“设置”**>**“部署”中，您现在可以看到“查看日志”选项，通过该选项可以查看：

- 上次成功的数据库同步的详细信息。
- 在流式复制错误期间单击 **Sync Database** 时，当前数据库同步 进度。

[NSADM-71048]

许可

ADM 本地 **Express** 提供对 **2** 台虚拟服务器的更改　NetScaler ADM Express 版本已从 30 个免费虚拟服务器许可证更新为两个免费许可证。现在，您最多可以管理两个发现的应用程序或虚拟服务器并查看分析。要为两个以上的虚拟服务器应用许可证，必须购买新的 Advanced ADM 许可证。早些时候，ADM 支持 30 个虚拟服务器的免费许可证。

> 注意
>
> 如果您使用两个以上的虚拟服务器许可证，则在 30 天后，免费默认许可证仅适用于两个虚拟服务器。而且，您需要为剩余的虚拟服务器购买和应用新的许可证。

有关详细信息，请参阅许可。

[NSADM-76704]

样书

样书支持对数据类型进行隐式类型转换　当您将样书表达式用于不同的数据类型时，样书引擎现在会隐式地将输出类型转换为适当的数据类型。例如，如果在 `string` 和 `integer` 类型之间执行添加操作，样书引擎会将输出数据类型设置为 `string`。

[NSADM-77219]

已修复的问题

内部版本 13.1—12.50 中解决的问题。

分析

- mas_afdecoder 进程因内存损坏而失败。通过此修复，NetScaler ADM 会检查 mas_afdecoder 进程以避免内存损坏并减少调试的日志。

  [NSHELP-29237]

- 如果自定义应用程序具有停止服务的虚拟服务器，则向该应用程序添加新的虚拟服务器将失败。

  [NSHELP-29213]

- 当您监视许多虚拟服务器时，“网络功能”控制板需要更长的时间来加载，否则它将变得无响应。

  [NSHELP-29274]

管理和监视

- 在 GSLB 设置中，当多个 ADC 实例使用相同的域名时，实体轮询会错误地更新数据库。

  [NSHELP-29885]

- 在 NetScaler ADM 中，当您启用在 接收 **netScalerConfigChange** 事件时执行审核时，ADM 会轮询 ADC 实例以了解每次配置更改。但是，如果 ADC 配置同时发生了多次更改，则配置审核轮询将失败。有关启用配置审核轮询的更多信息，请参阅 设置配置审核通知。

  [NSHELP-29855]

- 将 NetScaler ADM 升级到 13.0.83.x 后，应用程序控制板 会在 ADC 实例中更改旧应用程序名称时显示该名称。

  [NSHELP-29518]

- 启用实例网络报告功能后，具有许多虚拟服务器、服务和服务组的 ADM 会导致更高的 CPU 消耗。

  [NSHELP-29436]

- 将 NetScaler ADM 升级到 13.1-4.43 版本后，ADM GUI 不会显示辅助 ADM 服务器的 CPU、内存和磁盘状态。

  [NSHELP-29344]

- 在 NetScaler ADM 中，如果添加两个具有相同 IP 地址的 ADC 实例，ADM GUI 将一个实例状态显示为启动，另一个实例状态显示为关闭。当您重新发现处于关闭状态的 ADC 实例时，ADM 无法获取 ADC 版本。

  [NSHELP-29227]

- 有时，配置审核无法按预期对 ADC 分区起作用。

  [NSHELP-29051]

- 使用 ADM 维护作业升级 ADC 实例时，实例重新启动后，NetScaler 实例页面下不会显示升级后的 ADC 映像版本。GUI 仍显示旧的映像版本。

  [NSADM-60824]

用户界面

当浏览器选项卡处于非活动状态时，ADM GUI 显示错误的 ADM 服务器时间。

[NSHELP-28278]

已知问题

13.1—12.50 版中存在的问题。

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.12.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

分析

- 在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据变为无效且在 ADM 报告中不可用。

  [NSHELP-26545]

- NetScaler ADM 13.1-12.x 版本仅支持两个免费的虚拟服务器许可证。有关详细信息，请参阅许可。

  升级到 13.1-12.x 版本后，如果任何虚拟服务器（已启用分析）未获得许可，则“所有虚拟服务器”页面（“设置”**>**“许可和分析配置”**>**“配置分析”）中的 **Analytics** 状态可能仍会将其显示为已启用，但分析数据未显示在 ADM 中。

  [NSADM-79893]

调配

- 当您使用 ADM 调配在 OpenStack Lbaas 上创建成员时，OpenStack 上的成员创建会间歇性失败。当 ADM 向调配服务的代理请求在 30 秒后超时时，会出现此问题。通过此修复，调配 API 的请求超时时间已增加到 120 秒。

  [NSHELP-21490]

- 如果您正在使用 OpenStack Queens for LBaas 工作流程，则负载平衡虚拟服务器不会绑定到内容交换虚拟服务器。此问题会影响流量。

解决方法：

1. 使用负载平衡虚拟服务器创建池。
2. 使用池 ID 创建侦听器。
   如果您已有侦听器，请使用池 ID 更新该侦听器。

[NSADM-36631]

管理和监视

- 在 Azure 云上配置 NetScaler ADM 13.1 本地代理时，会显示一条错误消息。

  解决办法：您可以忽略此错误消息并继续配置。

  [NSADM-81739]

NetScaler ADM 13.1-9.60 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1-9.60 中存在的增强功能和更改、已修复问题和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。

新增功能

Build 13.1-9.60 中提供的增强功能和更改。

管理和监视

查看用户对 **Gateway** 虚拟服务器的趋势

现在，在 ADM GUI 中的“基础结构”**>**“网络报告”（NetScaler Gateway 虚拟服务器）下，您可以查看以下趋势：

- 已建立的用户会话总数。
- 已连接的用户总数。

[NSADM-70811]

ADM 用户界面的变化

为了改善 NetScaler ADM 的用户体验，在 ADM 用户界面中添加了几项增强功能。这些增强功能可自动化并简化将 ADC 实例加载到 ADM 的过程。此外，新的更简单直观的界面使其更易于导航。以下是 GUI 更改的摘要：

ADM 登录页面：如果您在首次设置 ADM 服务时跳过了在 入门 工作流程中加入 ADC 实例的操作，则可以从 ADM GUI 控制板加载这些实例。如果尚未添加 ADC 实例，GUI 会提示您添加实例。
导航菜单**-**新的和更新的模块：

左侧的导航菜单已重新组织和分组。菜单中的新模块是“安全”、“网关”和“基础结构”。一些旧模块，网络、分析和调配，现在已合并到新模块中。如果尚未添加 ADC 实例，当您单击左侧导航栏上的任何模块时，右侧将显示该模块的功能和优势的表格预览。

[NSADM-68433]

分析

更改名称以获得 **Security Insight** 和机器人洞察

为虚拟服务器启用分析后，您现在可以查看以下名称更改，以获取 Security Insight 和机器人洞察：

- WAF 安全违规
- 机器人安全违规

[NSADM-72932]

WAF 和 **Bot** 分析仅支持高级许可证虚拟服务器

现在，您可以启用 WAF 安全违规和机器人安全违规，并仅查看高级许可虚拟服务器的 WAF/Bot 分析。对于标准和高级许可的虚拟服务器，这些选项处于禁用状态。

[NSADM-72931]

样书

在样本定义中指定参数条件

在样书定义中，参数定义样书用户为创建配置包而提供的输入。早些时候，每个参数都独立于其他参数。

有时，您可能想要修改参数的行为，如下所示：

- 仅在满足条件时向用户显示某些参数。
- 允许一个参数的值依赖于另一个参数。
- 仅在特定条件下将参数设置为必填参数。

在这些情况下，请使用 parameters-conditions 部分定义参数条件。参数条件具有以下属性：

- ‘target’： 指定要应用条件的参数。
- ‘action’： 指定在目标参数与条件匹配时要执行的操作。此功能支持许多操作。
- ‘条件’： 指定必须满足的条件。

例如，在样书中，您希望仅在协议参数设置为 SSL 时才显示证书参数。您可以指定一个参数条件，其中目标为证书参数。然后，条件在带有 action 的协议参数上 show。此条件可确保在没有证书文件的情况下不会创建任何配置包。

```
parameters-conditions:
-
 target: $parameters.certificates
 action: set-required
 condition: $parameters.lb-service-type == `SSL`
<!--NeedCopy-->
```

> 说明
>
> 目前无法对列表对象中的参数应用参数条件。

[NSADM-67721]

已修复的问题

版本 13.1-9.60 中解决的问题。

分析

显示内部部署 ADM 的所有托管实例的全局服务图会导致内存使用率过高。

[NSHELP-28044]

在 ADM 13.0 76.29 中，“分析” > “安全” > “安全违规” 中的 “网络” 选项卡下不会显示慢速 洛里斯 和慢速发布违规。

[NSHELP-27616]

启用 HDX Insight 后，mas_afdecoder 进程停止响应，生成 HDX 分析失败。

[NSHELP-26754]

管理和监视

在 ADM 代理进行故障转移后，如果 ADC 实例不足，NetScaler ADM 将重新平衡代理上的 ADC 实例。在此过程中，ADC 实例上的 SNMP 和 Appflw 将使用先前代理的 IP 地址而不是当前代理的 IP 地址进行配置。

[NSHELP-29160]

当您上载受密码保护的证书时 `Invalid PEM key: Incorrect password`，ADM 代理会显示一条错误消息。

[NSHELP-28983]

如果用户没有查看访问权限，当您重命名 ADC 实例上的虚拟服务器时，ADM GUI 会显示该用户的旧服务器名称。

[NSHELP-28849]

在以下情况下，ADM 代理不支持代理设置：

- 代理和 ADM 服务之间使用代理服务器。因此，ADC 备份失败。
- 代理中缺少代理服务器密码。因此，代理服务器配置失败。

[NSHELP-28216]

在某些 ADM 部署中，灾难恢复数据库的状态显示为空白。

[NSHELP-28025]

系统

在 13.0-76.x 和 13.0-79.x 版本中，`sync\\_adm\\_node.py` 脚本会失败。因此，灾难恢复和主站点之间的数据无法同步。

[NSHELP-27790]

分析

在 Web Insight 中，计划导出选项被暂时禁用，因为报告显示为空白。

[NSADM-77966]

已知问题

版本 13.1-9.60 中存在的问题

样书

当您将 NetScaler ADM 从任何旧版本升级到 13.1.9.x 版本时，NetScaler ADM 会将现有的 ConfigPack 回滚到其早期版本。

解决方法：升级到最新版本的 NetScaler ADM。

[NSHELP-33127]

分析

mas_afdecoder 进程因内存损坏而失败。通过此修复，NetScaler ADM 会检查 mas_afdecoder 进程以避免内存损坏并减少调试的日志。

[NSHELP-29237]

管理和监视

当您将 NetScaler ADM 从任何旧版本升级到 13.1.9.x 版本时，NetScaler ADM 会将现有样书 ConfigPack 回滚到早期版本。

解决方法：升级到最新版本的 NetScaler ADM

[NSHELP-33127]

有时，配置审核无法按预期对 ADC 分区起作用。

[NSHELP-29051]

分析

在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据变为无效且在 ADM 报告中不可用。

[NSHELP-26545]

调配

当您使用 ADM 调配在 OpenStack Lbaas 上创建成员时，OpenStack 上的成员创建会间歇性失败。当 ADM 向调配服务的代理请求在 30 秒后超时时，会出现此问题。通过此修复，调配 API 的请求超时时间已增加到 120 秒。

[NSHELP-21490]

如果您使用 OpenStack Queens 进行 LBaas 工作流程，则负载平衡虚拟服务器不会绑定到内容交换虚拟服务器。此问题会影响流量。

解决方法：

1. 使用负载平衡虚拟服务器创建池。
2. 使用池 ID 创建侦听器。
   如果您已有侦听器，请使用池 ID 更新该侦听器。

[NSADM-36631]

NetScaler ADM 13.1—4.43 版本的发行说明

February 6, 2024

本发行说明文档介绍了 NetScaler ADM 版本 Build 13.1—4.43 中存在的增强功能和更改以及已修复和已知问题。

备注

本发行说明文档不包括与安全相关的修补程序。有关安全相关修复和建议的列表，请参阅安全公告。
已修复的问题部分列出了 13.0-82.x 版之后的修复程序。

新增功能

内部版本 13.1—4.43 中提供的增强功能和更改。

管理和监视

ADM 在创建 **ADC** 升级作业之前检查经典策略

现在，在 ADM 中创建 ADC 升级作业时，ADM 会检查现有的经典策略，因为从 ADC 版本 13.1 开始，经典策略不再受支持。如果在实例中找到经典策略，则升级前验证报告将显示一条错误消息。在创建升级作业之前删除此类策略。

注意：将 ADC 实例升级到 13.1 之前，请删除经典策略或将其迁移到高级策略

[NSADM-75061]

分析

对 **RTT** 计算的改进

NetScaler 实例可能无法计算某些事务的 RTT 值。对于此类事务，ADM 中的 Web 事务分析和 Web Insight 会将 RTT 值显示为 < 1 毫秒。

此类事务的 RTT 计算得到改进，ADM 现在将以下 RTT 值显示为：

- NA 当 ADC 实例无法计算 RTT 时显示。
- <1 毫秒当 ADC 实例以 0 毫秒到 1 毫秒之间的小数位数计算 RTT 时显示。例如，0.22 毫秒。

[NSADM-65648]

样书

用于部署 **SNMP** 配置的新默认样书

用于在 ADC 实例上部署 SNMP 配置的新默认样书。在 ADM GUI 中，转到 应用程序 **>** 样书。通过键入名称 `snmp\\_configuration` 来搜索样书。

[NSADM-67723]

样书支持国际字符

您现在可以在样书中包含国际字符。

[NSADM-67719]

已修复的问题

内部版本 13.1—4.43 中解决的问题。

分析

在应用程序控制板中，当您向下钻取应用程序和 **Web Insight** 选项卡时，客户端 下的“查看更多”选项不起作用。在“应用程序” **>** “**Web Insight**”中也会观察到此问题。

[NSHELP-28153]

如果应用程序名称包含空格，则 Web Insight 数据将无法正确填充。

[NSHELP-27178]

在配置的数据持久性持续时间内保留的 ADM 分析报告数据。

[NSHELP-26208]

管理和监视

在备份已升级且正在 SDX 实例上运行的 ADC 实例时，即使 ADM 中已存在同一 XVA 映像，ADM 也会备份升级后的 ADC 映像。

[NSHELP-28303]

如果在 ADM 上注册了 ADC 实例，则处理服务状态更改的事件可能会导致 ADM 的内存使用量过高。

[NSHELP-27933]

ADM 错误地显示了 ADC 实例的配置审核以获取月度数据。

[NSHELP-27595]

在 SDX 管理服务 GUI 中，如果具有自定义`nsroot`用户凭据的非用户尝试将 ADM 添加为许可服务器，则会出现“未授权”错误。

[NSHELP-27327]

如果虚拟服务器名称太长，ADC 将为故障对象发送错误的值。通过此修复，以下 SNMP 陷阱会将虚拟服务器的服务名称更改为服务全名：

- `svcGrpMemberSynfloodRate`
- `svcGrpMemberRequestRate`
- `svcGrpMemberRxBytesRate`
- `svcGrpMemberMaxClients`

[NSADM-75809]

当您尝试使用 SDK 在部署为微服务的本地 ADM 上许可超过 30 台虚拟服务器时，ADM 不会显示 NITRO 异常。

[NSADM-67833]

分析

在 应用程序控制板中，应用程序详细信息页面将当天的数据显示为第二天的数据。当您选择的时间间隔大于一天时，会出现此问题。而且，它只能在“应用分数”和“问题”部分下显示。

[NSADM-73507]

用户界面

导出许可证使用情况报告时，表格数据无法正确导出。

[NSHELP-28423]

如果命令行号超过两位数，则配置模板不会显示这些编号。通过此修复，它最多支持六位数字。

[NSHELP-28330]

在 基础架构 **>** 配置作业中，当您将鼠标悬停在重命名的配置模板上时，它将显示旧名称。通过此修复，您可以向模板添加描述。现在，当您将鼠标悬停在模板上时，将显示此描述。

[NSHELP-28078]

已知问题

版本 13.1—4.43 中存在的问题。

管理和监视

使用 ADM 维护作业升级 ADC 实例时，实例重启后，不会显示升级后的 ADC 映像版本。GUI 仍在 NetScaler 实例页面 下显示旧映像版本。

[NSADM-60824]

分析

在虚拟服务器上启用分析时，ADC 和 ADM 之间可能会丢失一些必需的信息。因此，事务数据变为无效且在 ADM 报告中不可用。

[NSHELP-26545]

调配

当您使用 ADM 调配在 OpenStack 负载平衡器即服务 (LBaaS) 上创建成员时，OpenStack 上的成员创建会间歇性失败。当 ADM 向调配服务的代理请求在 30 秒后超时时，会出现此问题。通过此修复，调配 API 的请求超时时间已增加到 120 秒。

[NSHELP-21490]

如果您正在使用 OpenStack Queens for 负载平衡器即服务 (LBaaS) 工作流，则负载平衡虚拟服务器不会绑定到内容交换虚拟服务器。此问题会影响流量。

解决方法：

1. 使用负载平衡虚拟服务器创建池。
2. 使用池 ID 创建侦听器。

如果您已有侦听器，请使用池 ID 更新该侦听器。

[NSADM-36631]

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

February 6, 2024

您可以将本地 **NetScaler 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 获取客户端和机密 CSV 文件
- 验证 ADM 服务许可
- 使用脚本迁移

从本地 ADM 迁移到 ADM 服务后，如果要再次继续使用本地 ADM，则可以使用回滚脚本。有关详细信息，请参阅 回滚到内部部署 ADM。

配置 **ADM** 服务代理

要启用 NetScaler 实例和 NetScaler ADM 之间的通信，必须配置代理。默认情况下，NetScaler 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** 获取客户端和机密 **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 和密钥。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

您必须获取 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：
  - NetScaler SDX：13.0 74.11 或更高版本。
  - NetScaler 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

- 使用 ADM 82.x 版本，您可以选择该功能，然后进行迁移。
- 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 高可用性对，请登录主节点。

2. 键入 **shell** 并按 **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。

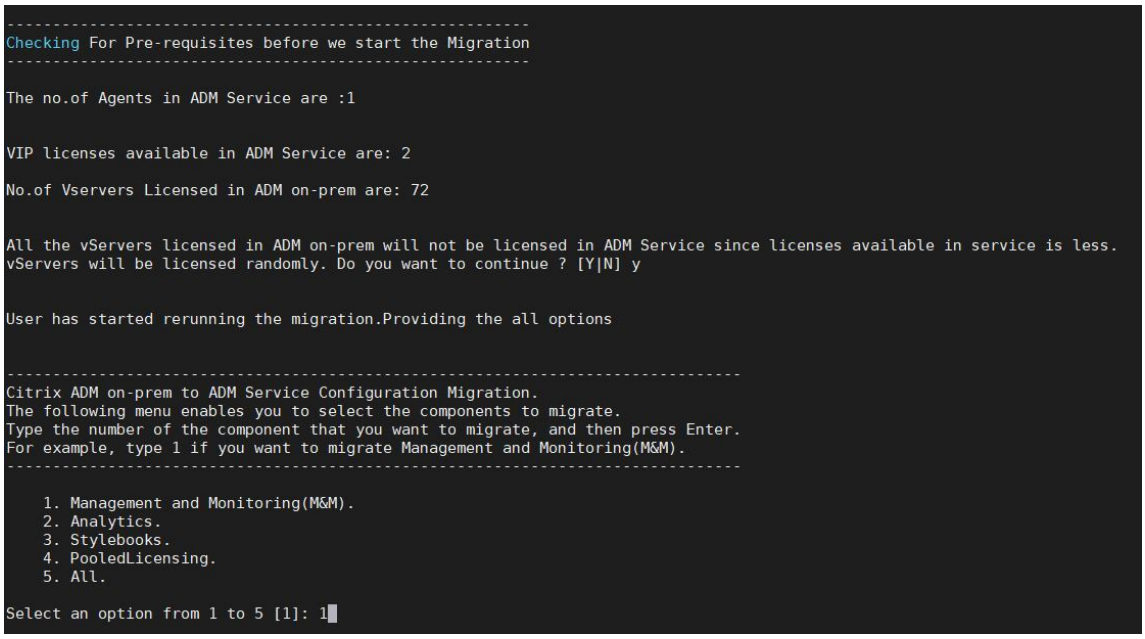
4. 对于 ADM **13.0 82.xx** 版本，请运行以下命令完成迁移：

   a) `cd /mps/scripts`

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

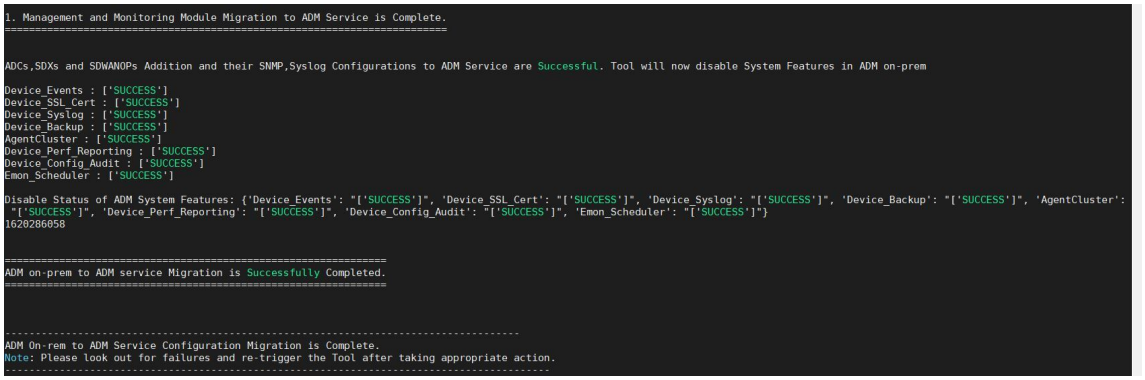
   例如，`python servicemigrationtool.py /var/secureclient.csv`

   运行迁移脚本后，该工具将显示以下选项：



   根据您提供的选择，只有该功能会迁移到 ADM 服务。

   在示例中，选择了选项 1。该工具完成管理和监视 (M&M) 迁移并显示以下消息：



   管理和监视 **(M&M)** 功能包括：

- ADC 实例、标签、实例组、配置文件、自定义应用、配置作业、SNMP、系统日志配置。
- 站点、IP 阻止、网络报告、分析阈值、通知设置、数据修剪设置。
- 配置审核模板、轮询间隔、事件规则和设置。
- RBAC 组、角色和策略

分析 功能包括：

- 来自 ADC 实例的每个虚拟服务器的 Appflow 配置。
- 每个 SDWAN 设备的 Appflow 配置。

> 注意：
>
> - 即使您选择任何其他功能（2、3 或 4），管理和监视 (M&M) 功能也会自动迁移。
> - 一次只能指定一个要素。
> - 完成任何要素的迁移后，如果要稍后迁移任何其他要素，则已迁移的要素不会显示在列表中。例如，如果您先完成了迁移 **Analytics**（分析）功能，下次运行迁移脚本时，只能看到 样书（样书）、**Pooled Licensing**（池许可）和 **All**（全部）选项。
> - 当您迁移池许可时，它会迁移包括虚拟服务器在内的所有类型。

5. 对于 ADM **13.0 76.xx** 版本，请运行以下命令完成迁移：

   a) `cd /mps/scripts`

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

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

6. 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=servicemigration.tgz`

   The downloaded file comprises two bundle scripts, `servicemigrationtool_27.py` and `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

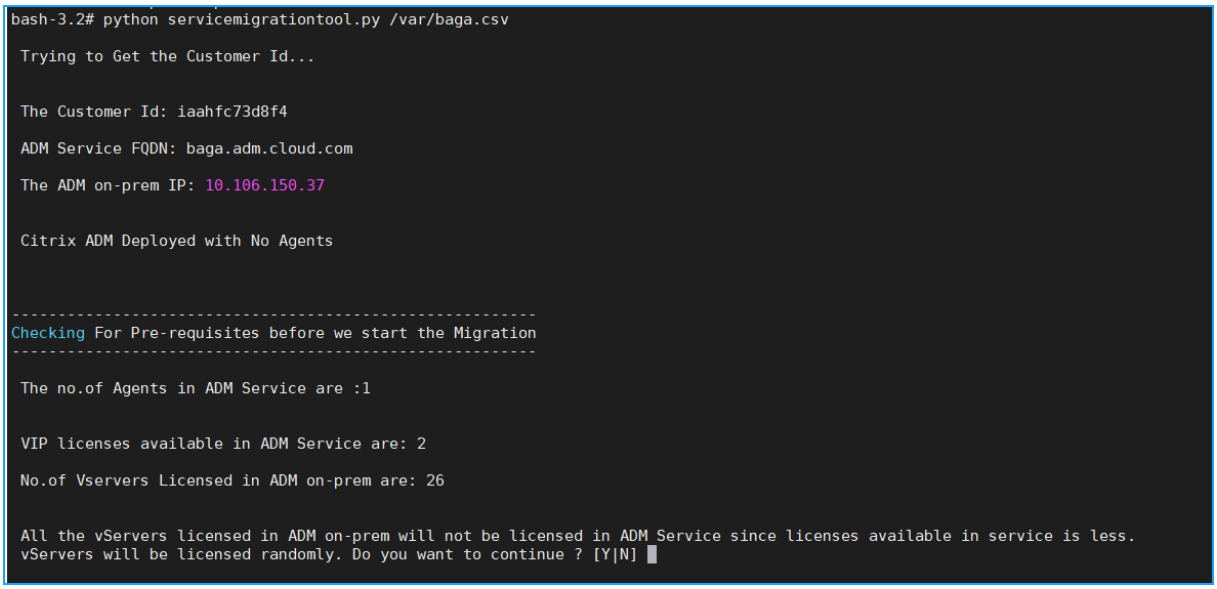
   c) 运行以下命令进行迁移：

      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，它会检查必备条件，然后继续进行迁移。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。



(本地许可证数量较少)

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。

如果您有池许可证服务器不支持的 ADC 实例版本，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，完成迁移的大概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 实例及其相应的配置成功移至 ADM 服务，迁移即告成功。成功迁移后，本地 NetScaler 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

回滚到内部部署 **ADM**

如果要回滚到本地 ADM，请确保满足先决条件。

必备条件

如果您的本地 ADM（在迁移到 ADM 服务之前）是：

- 用作池许可证服务器，请确保您在内部部署 ADM 中拥有所需的池许可证。
- 配置了本地 ADM 代理，确保代理处于“启动”状态。

使用回滚脚本

> 注意
>
> 回滚后，Analytics、SNMP、池许可中的相同配置（迁移前）将在本地 ADM 中再次可用。如果您在迁移后对这些配置进行了任何更改，则这些更改不会反映在本地 ADM 中。

- 对于 **ADM 82.xx** 或更高版本 的版本，回滚脚本作为构建的一部分提供，可从中访问 /mps/scripts。
- 对于 早于 **79.xx** 版本的 **ADM** ，您可以升级到 82.x 版本并使用回滚脚本，也可以下载回滚脚本并将脚本复制到本地 ADM 中。

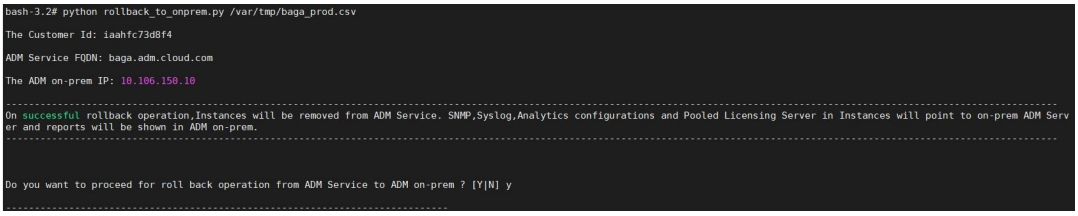
1. 使用 SSH 客户端登录本地 ADM。
2. 键入 shell 并按 Enter 键切换到 bash 模式。
3. 对于 ADM **13.0 82.xx** 构建，请运行以下命令以完成回滚：

   a) cd /mps/脚本

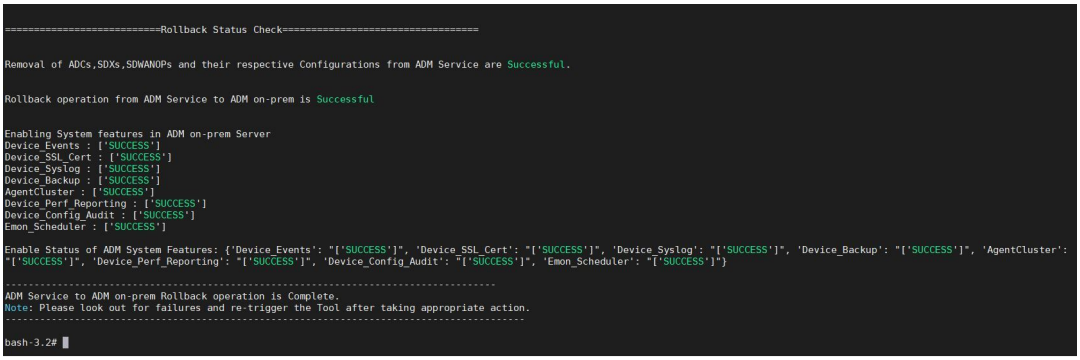
   b) python rollback_to_onprem.py <path of ClientID/Secret File in ADM on-prem VM>

   例如，python rollback_to_onprem.py /var/ secureclient.csv.csv

   该工具将启动回滚操作，并提示您是否要继续。键入 **Y** 继续。



   回滚完成后，您会看到以下消息。



4. 对于早于 82.xx 版本的 ADM：

   a) 从以下位置下载回滚脚本：

      `https://download.citrixnetworkapi.net/root/download/v1/public/software?product=admonprem&build=migrationtool&model=servicemigration.tgz`

   b) 对于 ADM 79.xx 和 76.xx 内部版本，请将脚本保存在中，`/mps/scripts` 然后运行以下命令进行回滚：

      i. `cd /mps/scripts`

      ii. `python rollback_to_onprem.py < path of client/secret csv file in ADM on-prem>`

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

   c) 对于早于 76.xx 版本的 ADM，请将脚本保存在本地 ADM 中。例如，将其保存在 `/var` 位置，然后运行以下命令进行回滚：

      i. `cd /var`

      ii. `python rollback_to_onprem_27.py < path of client/secret csv file in ADM on-prem>`

      例如，`python rollback_to_onprem_27.py /var/secureclient.csv`

   该工具将启动回滚操作，并提示您是否要继续。键入 **Y** 继续。

常见问题解答

February 6, 2024

ADM 服务

ADM 服务代理是否可选与本地 NetScaler 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 NetScaler 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 NetScaler 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://www.citrix.com/events/2022/whats-new-with-citrix-application-delivery-management.html

如果本地 NetScaler 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。您必须获取 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 **NetScaler 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，上载到本地 NetScaler ADM 的 SSL 证书/密钥不会迁移到 ADM 服务。

本地 **NetScaler 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 NetScaler 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

许可证服务器的更改仅适用于受支持的 NetScaler MPX、VPX 和 SDX 版本。

如果迁移脚本的有关 **ADC** 实例的配置失败，会发生什么

ADC 实例继续在本地 ADM 设置中运行。您可以根据建议的失败原因采取必要的措施，然后再次运行迁移脚本。

如果一些 **ADC** 实例无法迁移到 **ADM** 服务会发生什么。重新运行迁移脚本会有所帮助吗**?**

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 **NetScaler 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 **NetScaler 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”。

回滚脚本

如果在本地 **ADM HA** 对中使用回滚脚本，会发生什么情况

内部部署 ADM HA 对将使用迁移前可用的所有配置进行还原。

使用回滚脚本后，灾难恢复节点会发生什么情况

在迁移之前，灾难恢复节点还原为所有配置。

故障排除

February 6, 2024

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 NetScaler 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 **NetScaler** 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

```
==============Stylebook custom templates Import to ADM Service====================


neustar.citrix.adc.stylebooks_5.0_appfw-signature : FAILURE : There is an existing StyleBook with same namespace, version and name.

neustar.citrix.adc.stylebooks_5.0_customer-template : FAILURE : There is an existing StyleBook with same namespace, version and name.

 Custom stylebooks import status is:{'neustar.citrix.adc.stylebooks_5.0_appfw-signature': 'FAILURE', 'neustar.citrix.adc.stylebooks_5.0_customer-template': 'FAILURE'}
==============Stylebook repository Addition to ADM Service====================
```

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 NetScaler 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

```
===============Config Jobs Addition to ADM Service====================


config_job2_show_ns_ip : FAILURE : Express user can have maximum 2 config jobs

ConfigJob1_show_ha_node : FAILURE : Express user can have maximum 2 config jobs

 The config jobs status is :
{'config_job2_show_ns_ip': 'FAILURE', 'ConfigJob1_show_ha_node': 'FAILURE'}
```

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

```
====================IP Blocks Addition in ADM Service=======================

ipblock1 : FAILURE : IP Block Name ipblock1 already exists

ipblock3 : FAILURE : IP Block Name ipblock3 already exists

test : FAILURE : IP Block Name test already exists
```

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。

网络控制板报告添加状态

```
================Network Dashboard Reports Addition to ADM Service=================

new456 : FAILURE : Dashboard new456 already exists

new123 : FAILURE : Dashboard new123 already exists

 The network dashoard reports addition status is:
{'new456': "['FAILURE']", 'new123': "['FAILURE']"}
```

解决办法：删除在 ADM 服务中手动创建的控制板，然后重新运行迁移脚本。

所有操作方法文章

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM)“操作方法文章”是关于 NetScaler ADM 功能的简单、相关且易于实现的文章。这些文章包含有关一些常用 NetScaler ADM 功能的信息，例如实例管理、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	样书	证书管理	NetScaler ADM 系统
	配置管理	身份验证	分析	网络功能

实例管理

如何监视分布全球的站点

如何管理 NetScaler 实例的管理分区

如何向 NetScaler ADM 添加实例

如何在 NetScaler ADM 上创建实例组

如何在 NetScaler ADM 中为地理地图配置站点

如何使用 NetScaler ADM 强制故障转移到辅助 NetScaler 实例

如何使用 NetScaler ADM 强制备用 NetScaler 实例保持辅助状态

如何使用 NetScaler ADM 备份和恢复实例

如何使用 NetScaler ADM 控制板监视 HAProxy 实例

如何显示在 HAProxy 实例上配置的前端的详细信息

如何显示在 HAProxy 实例上配置的后端的详细信息

如何显示在 HAProxy 实例上配置的服务器的详细信息

如何从 NetScaler ADM 重启 HAProxy 实例

如何使用 NetScaler ADM 备份和恢复 HAProxy 实例

如何使用 NetScaler ADM 编辑 HAProxy 配置文件

如何重新发现多个 NetScaler VPX 实例

如何轮询 NetScaler ADM 中的 NetScaler 实例和实体

如何在 NetScaler ADM 上取消管理实例

如何追踪从 NetScaler ADM 到实例的路线

配置管理

如何在 NetScaler 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 NetScaler ADM 升级 NetScaler SDX 实例

如何在 NetScaler ADM 中使用内置模板安排创建的作业

如何重新安排使用 NetScaler 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 NetScaler ADM 升级 NetScaler 实例

如何在 NetScaler ADM 上的配置作业中使用变量

如何使用配置模板在 NetScaler ADM 上创建审核模板

如何在 NetScaler ADM 上使用更正命令创建配置作业

如何在 NetScaler ADM 中将正在运行和保存的配置命令从一个 NetScaler 实例复制到另一个实例

如何使用录制和播放来创建配置作业

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 NetScaler ADM 上使用主配置模板

如何对 NetScaler 实例进行轮询配置审核

如何在配置作业中重用配置审核模板

如何导入和导出配置模板

如何为 ConfigChange SNMP 陷阱生成配置审核差异

证书管理

如何在 NetScaler ADM 上配置企业策略

如何在 NetScaler ADM 的 NetScaler 实例上安装 SSL 证书

如何从 NetScaler ADM 更新已安装的证书

如何使用 NetScaler ADM 链接和取消链接 SSL 证书

如何使用 NetScaler ADM 创建证书签名请求 (CSR)

如何设置来自 NetScaler ADM 的 SSL 证书到期通知

如何在 NetScaler ADM 上使用 SSL 控制板

如何从 NetScaler 实例轮询 SSL 证书

样书

如何查看不同的样书组

如何创建自己的样书

如何在 NetScaler ADM 中使用用户定义的样书手册

如何使用 API 基于样书创建配置

如何对在样书中定义的虚拟服务器启用分析和配置警报

如何创建样书将文件上载到 NetScaler ADM

如何使用 API 创建配置以上载任何文件类型

如何创建样书以将 SSL 证书文件和证书密钥文件上载到 NetScaler ADM

如何使用 API 创建配置以上载证书和密钥文件

如何在企业中使用 Microsoft Skype for Business 样书

如何在企业中使用 Microsoft Exchange 样书

如何在企业中使用 Microsoft SharePoint 样书

分析

如何对实例启用分析

如何配置自适应阈值

如何配置 SLA 管理

如何配置用于分析的数据库汇总

如何使用 NetScaler ADM 创建阈值和警报

如何禁用 NetScaler ADM 进行分析的 URL 数据收集

如何查看您的网络中通过流技术推送的视频类型和使用的数据量

如何查看特定时间范围内的峰值数据速率

如何查看网络效率

事件管理

如何在 NetScaler ADM 上为事件设置事件存在时间

如何使用 NetScaler ADM 调度事件过滤器

如何为来自 NetScaler ADM 的事件设置重复的电子邮件通知

如何使用 NetScaler ADM 抑制事件

如何使用事件控制板来监视事件

如何在 NetScaler ADM 上创建事件规则

如何修改 NetScaler 实例上发生的事件的报告严重性

如何在 NetScaler ADM 中查看事件摘要

如何在 NetScaler ADM 上显示 SNMP 陷阱的事件严重性和偏差

如何使用 NetScaler ADM 导出系统日志消息

如何在 NetScaler ADM 中抑制系统日志消息

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 TACACS 身份验证服务器

如何在 NetScaler ADM 中提取身份验证服务器组

如何启用回退本地身份验证

NetScaler ADM 系统

如何升级 NetScaler ADM

如何重置 NetScaler ADM 的密码

如何为 NetScaler 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 NetScaler ADM 服务器

如何在 HA 对中备份和恢复 NetScaler ADM 配置

如何在 NetScaler ADM 中为非默认用户启用 shell 访问权限

如何在 NetScaler ADM 上配置 NTP 服务器

如何为 NetScaler ADM 配置 SSL 设置

如何配置 NetScaler ADM 的系统日志清除间隔

如何查看 NetScaler ADM 的审核信息

如何配置 NetScaler ADM 的系统通知设置

如何监视 NetScaler ADM 的 CPU、内存和磁盘使用情况

如何为 NetScaler ADM 配置密码组

如何在 NetScaler ADM 上创建 SNMP 陷阱、管理器和用户

如何为 NetScaler ADM 服务器分配主机名

如何为 NetScaler ADM 配置系统修剪设置

如何使用 NetScaler ADM 配置系统备份设置

如何在 NetScaler ADM 上配置和查看系统警报

网络功能

如何生成负载平衡实体的报告

如何导出或计划导出网络函数报告

概述

February 6, 2024

NetScaler Application Delivery Management (ADM) 是一种集中化管理解决方案，它通过为管理员提供企业范围的可见性并自动执行需要在多个实例上运行的管理任务来简化操作。您可以管理和监视 NetScaler 产品，包括 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler CPX 和 NetScaler Gateway。可以使用 ADM 从单个统一的控制台对整个全局应用程序交付基础结构进行管理、监视和故障排除。

ADM 是一种在 Citrix Hypervisor、VMware ESXi 和 Linux KVM 上运行的虚拟设备。ADM 通过收集以下有关 Web 应用程序和虚拟桌面流量的详细信息，解决了应用程序可见性难题：

- 用户会话级别信息
- Web 页面性能数据
- 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视客户问题。

功能和解决方案

February 6, 2024

NetScaler 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 控制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

Instances

使您能够管理 NetScaler 和 NetScaler Gateway 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

NetScaler 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 控制板及其功能，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

NetScaler 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

您可以通过监视 ADM 上的网络报告来优化资源使用情况。

分析

Web Insight

提供对企业 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视来监视 NetScaler 所服务的所有 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

为通过 NetScaler 的 ICA 流量提供端到端的可见性。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、实时和历史监视，监视 NetScaler 提供的所有安全 Web 应用程序。

TCP Insight

TCP Insight 提供了一种简单且可扩展的解决方案，用于监视 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 功能提供了一种简单且可扩展的解决方案，用于监视 NetScaler 实例使用的视频优化技术的指标，以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视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 NetScaler 产品与 OpenStack 云调配集成。NetScaler ADM 和 OpenStack 相互实现对方的 API，从而实现了 NetScaler 实例的负载平衡功能 (LBaaS) 与 OpenStack 云调配的集成。

Orchestration

NetScaler 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 Manager 和 Cisco Application Policy Infrastructure Controller (APIC)。

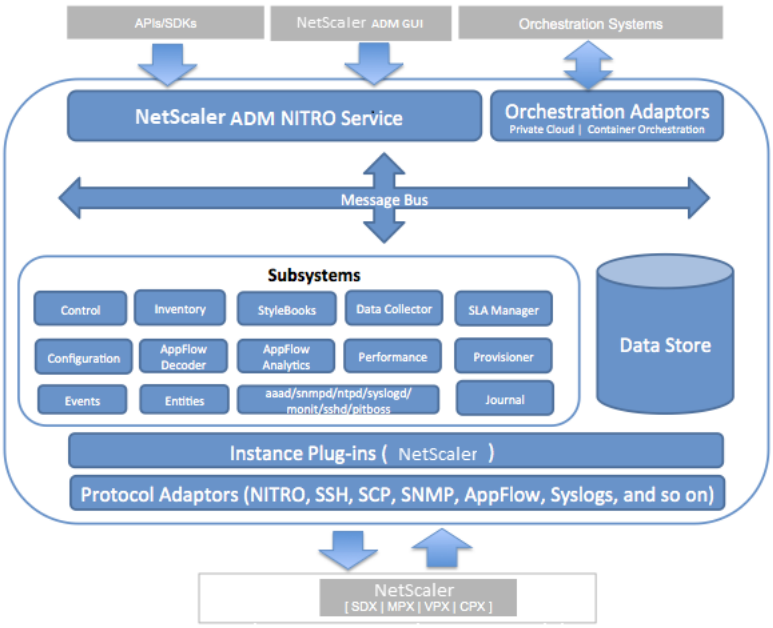
体系结构

February 6, 2024

NetScaler Application Delivery Management (ADM) 数据库与服务器集成，服务器管理所有关键进程，例如数据收集、NITRO 呼叫。服务器在其数据存储中存储实例详细信息清单，例如主机名、软件版本、运行和保存的配置、证书详细信息、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。

当前，ADM 支持两种类型的软件部署：单服务器部署和高可用性。

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。信息通过 NITRO 调用，或者通过 SNMP、Secure Shell (SSH) 或安全复制 (SCP) 协议在 ADM 和托管实例之间传输。然后对这些信息进行处理并存储在内部数据库（数据存储）中。

NetScaler ADM 如何发现实例

February 6, 2024

实例是您想要从 NetScaler Application Delivery Management (ADM) 发现、管理和监视的 NetScaler ADC 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 NetScaler ADM 服务器。您可以将以下 NetScaler ADC 设备和虚拟设备添加到 ADM：

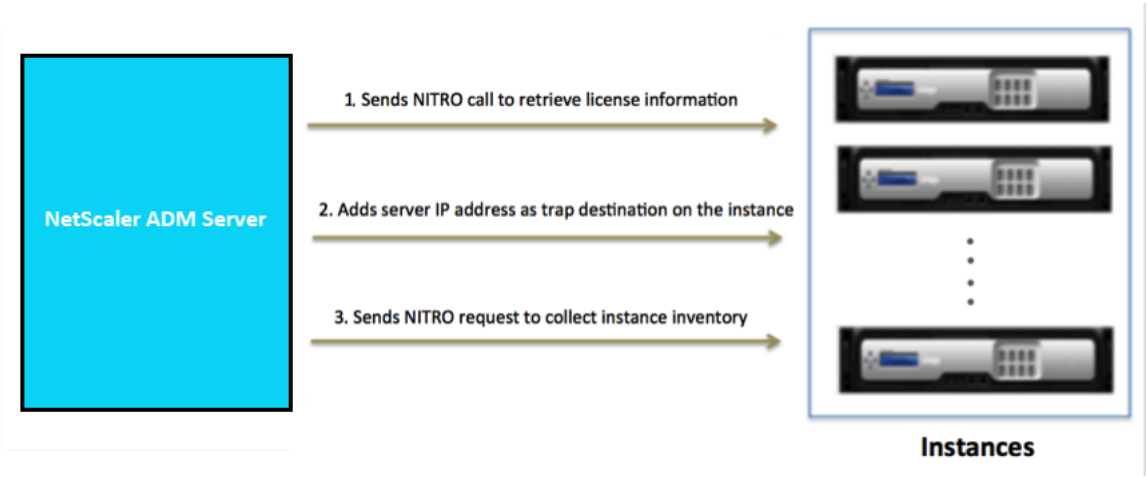
- NetScaler 实例
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
- NetScaler Gateway 实例

可以在第一次设置 NetScaler ADM 服务器时添加实例，也可在以后添加。

> 注意
>
> NetScaler ADM 使用 ADC 实例的 NetScaler 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。有关必须在 ADC 实例和 ADM 之间打开的端口的信息，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。

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，NetScaler ADM 隐式执行以下步骤。

1. NetScaler 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，它确定该实例是否是 ADC 实例以及 ADC 平台的类型（例如，NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX 或 NetScaler Gateway）。成功检测实例后，该实例将添加到 ADM 的数据库中。

   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 NetScaler MPX、NetScaler VPX、NetScaler SDX、NetScaler BLX 和 NetScaler Gateway 实例，如果许可证不适用于实例，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。

2. ADM 将其的 IP 地址添加到实例上的陷阱目的地列表中。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。

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

February 6, 2024

轮询是一个过程，在此过程中，NetScaler Application Delivery Management (ADM) 从 NetScaler 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 NetScaler 实例。要通过 NetScaler ADM 监视您的实例，

NetScaler ADM 必须从所有托管 ADC 实例收集某些信息，例如 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
- 配置审核投票
- SSL 证书轮询
- 实体轮询

NetScaler ADM 使用 NITRO 呼叫、安全外壳 (SSH) 和安全复制 (SCP) 等协议来轮询来自 NetScaler 实例的信息。

NetScaler ADM 如何轮询托管实例和实体

默认情况下，NetScaler ADM 会定期自动进行轮询。NetScaler ADM 还允许您为几种轮询类型配置轮询间隔，并允许您在需要时手动进行轮询。

下表描述了轮询类型、轮询间隔、使用的协议等的详细信息：

轮询类型	轮询间隔	民意调查信息	使用的协议	轮询间隔配置
实例轮询	每 5 分钟（默认）	统计信息，例如状态、每秒 HTTP 请求数、CPU 使用率、内存使用率和吞吐量。	NITRO call。	否
清单轮询	每 60 分钟（默认）	清单详细信息，如构建版本、系统信息、许可功能和模式。	NITRO 通话和 SSH	否
性能数据收集	每 5 分钟（默认）	网络报告信息	NITRO call	否
实例备份轮询	每 12 小时（默认情况下）	托管 ADC 实例当前状态的备份文件	NITRO 调用、SSH 和 SCP。	是。导航到基础结构 **>** 实例 **>** **NetScaler**。选择实例，然后从 选择操作”列表中单击“备份/还原。

轮询类型	轮询间隔	民意调查信息	使用的协议	轮询间隔配置
配置审核投票	每 10 小时（默认情况下）	ADC 实例上发生的配置更改（例如，正在运行的配置与保存的配置）	SSH、SCP 和 NITRO 通话	是。导航到基础架构 **>** 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，并将实例的所有配置审核立即添加到 NetScaler ADM。为此，请导航到 基础架构 **>** 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）	安装在 NetScaler 实例上的 SSL 证书。	NITRO 电话和 SCP	是。导航到 基础结构 **> SSL** 控制面板。在“SSL 控制面板”页上，单击设置以配置轮询间隔。 您可以手动轮询 SSL 证书，并将实例的所有证书立即添加到 NetScaler ADM。为此，请导航到 基础结构 **> SSL** 控制面板，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）	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。	可以，但不能设置为少于 10 分钟。要进行配置，请导航到 基础结构 **>** 网络功能。在“网络功能”页上，单击设置以配置轮询间隔。

轮询类型	轮询间隔	民意调查信息	使用的协议	轮询间隔配置
				您可以手动轮询实体，并将实例的所有实体立即添加到 NetScaler ADM。为此，请导航到 基础结构 **>** 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，NetScaler 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、数据库信息等将下载到 NetScaler 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 NetScaler 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 NetScaler ADM 在托管实例上执行的不同轮询方式：

- 对实例进行全局轮询
- 手动轮询实例
- 对实体进行人工投票

对实例进行全局轮询

NetScaler 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。尽管默认的轮询间隔是 30 分钟，但您可以通过导航到 基础架构 **>** 网络功能 ** 设置来根据需要设置 ** 间隔。

手动轮询实例

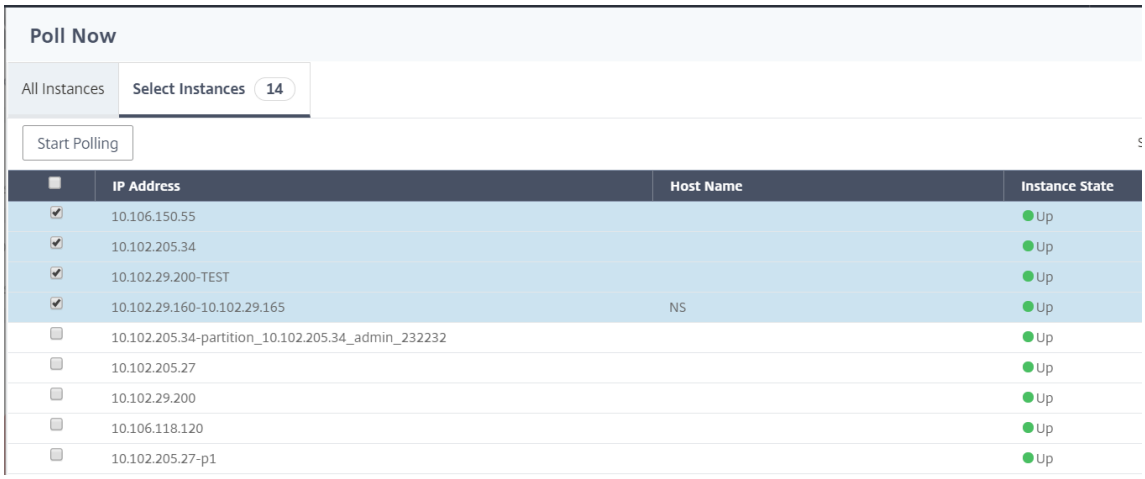
当 NetScaler ADM 管理多个实体时，轮询周期需要更长的时间才能生成报告，这可能会导致屏幕空白或系统可能仍显示较早的数据。

在 NetScaler ADM 中，如果不进行自动轮询，则有一个最短的轮询间隔周期。如果您添加新的 NetScaler 实例，或者更新了实体，则在下一次轮询之前，NetScaler ADM 无法识别新实例或对实体所做的更新。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。尽管您可以通过手动轮询来发现新添加的实例，但这会导致对整个 NetScaler 网络进行轮询，从而给网络带来沉重的负载。NetScaler 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。

NetScaler ADM 会自动轮询托管实例，以在一天中的设定时间收集信息。选定轮询减少了 NetScaler 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。

轮询 **NetScaler ADM** 中的特定实例：

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 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所有 NetScaler 实例或轮询选定实例的选项。
   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。



NetScaler ADM 启动手动轮询并添加所有实体。

对实体进行人工投票

NetScaler ADM 还允许您仅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，NetScaler ADM 仅轮询该实体并更新 NetScaler ADM GUI 中的状态。

以虚拟服务器处于 关闭状态的示例为例。在下一次自动轮询之前，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，可能需要只轮询该虚拟服务器，以便在 GUI 上立即显示正确的状态。

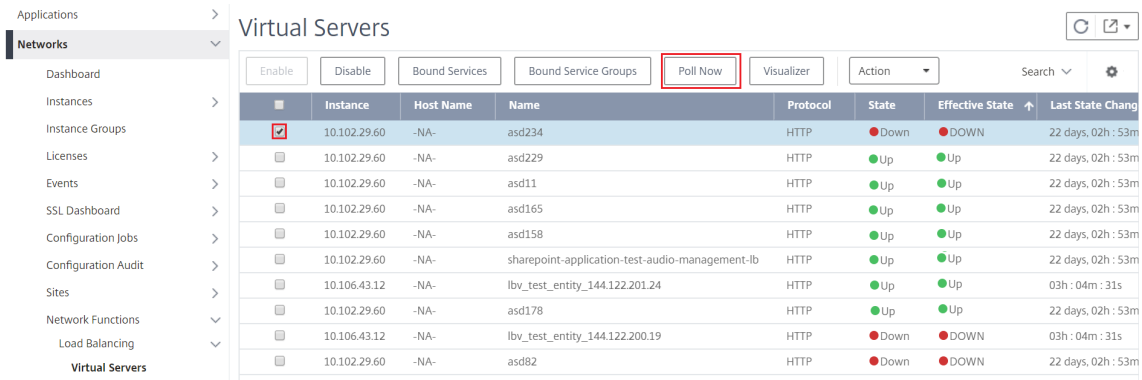
现在，您可以轮询以下实体以查看其状态的任何更新：服务、服务组、负载平衡虚拟服务器、缓存减少虚拟服务器、内容切换虚拟服务器、身份验证虚拟服务器、VPN 虚拟服务器、GSLB 虚拟服务器和应用程序服务器。

> 注意
>
> 如果您轮询虚拟服务器，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。如果您需要轮询所有关联实体，则必须手动轮询这些实体，或者必须轮询实例。

要轮询 **NetScaler ADM** 中的特定实体，请执行以下操作：

例如，此任务可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 NetScaler ADM 中，导航到基础架构 **>** 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。



数据治理

February 6, 2024

Citrix 收集有关您的 NetScaler 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。这些统计信息有助于 Citrix 主动排除 ADM 部署中的问题。

- **Create a customer identity on Citrix Cloud**（在 Citrix Cloud 上创建客户身份）- 将有关 ADM 运行状况、状态和其他指标的重要统计信息从 ADM 本地部署发送到 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。请参见 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 NetScaler 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

NetScaler Application Delivery Management (ADM) 要求您在开始访问信息之前在 ADM GUI 上对自己进行身份验证。必须先在 Citrix Cloud 服务上自行注册，才能在 ADM 上对自己进行身份验证。在 ADM GUI 上提供 Citrix Cloud 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 NetScaler 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。

工作流程 **1 -** 如果您是新用户

1. 在选定的 Hypervisor 上完成 NetScaler ADM 的安装。
2. 配置各种必需的 IP 地址。
3. 在 Web 浏览器中，键入 NetScaler 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 进行注册。
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 **I agree to share data for telemetry**（我同意共享遥测数据）旁边的复选框，然后单击 **Submit**（提交）。

工作流程 **2 -** 如果您是升级到最新 **ADM** 版本的现有用户

1. 将 NetScaler ADM 升级到最新版本后，在网络浏览器中键入 NetScaler 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 进行注册。
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 设置 **>** 系统管理，然后单击 身份验证。
- 单击 ADM GUI 右上角的云符号。
  成功进行身份验证后，X 会变成绿色的复选标记。

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

将您的数据上载到 NetScaler ADM 并使用 NetScaler 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 NetScaler 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 Citrix.com 隐私政策进行处理。

诊断和数据收集

NetScaler ADM 使用客户身份收集以下遥测数据：

- 在 **ADM** 中执行的操作：
  - 使用 NetScaler ADM UI/API 界面执行的操作。
  - 使用 NetScaler 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。
- **NetScaler ADM** 许可证信息：授权虚拟服务器的数量。
- **Key statistics**（关键统计数据）：
  - 事件规则的总计数。
  - 用户定义的样书总计数。
  - 托管应用程序和自定义应用程序的计数。
  - 注册的代理计数。
  - NetScaler (Rx+Tx) 的总吞吐量。
  - 托管实例计数。此计数还包括管理分区。
  - 使用 NetScaler ADM SaaS 的管理员人数。
- **NetScaler ADM** 的地理位置
- **Deployment information**（部署信息）：此信息包括部署类型，例如高可用性、灾难恢复和 ADM 代理。

为什么收集数据**?**

收集的遥测数据有助于：

- 推荐正确的 NetScaler ADM 规模和部署。
- 主动排除 ADM 本地部署中的问题。

谁可以使用这些数据**?**

Citrix 是所收集信息的唯一所有者。Citrix 有权访问/收集您自愿提供给我们的信息。我们不会将这些信息出售或出租给任何人。我们不会与我们组织以外的任何第三方共享您的信息，除非是为了满足您的请求所必需的。示例：配送订单或主动解决问题。

我们会将您的数据保留多长时间**?**

通常情况下，我们会存储个人/使用数据直到用户使用我们的服务。或者，我们还有另一个目的要这样做。之后，数据的存储时间不再超过法律要求或允许的范围，也不会超过内部报告和调配目的所必需的范围。

所有遥测数据的存储时间不超过 13 个月或 396 天。

使用维护脚本进行数据库优化

维护脚本用于解决 ADM 本地部署中与数据库相关的问题。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。客户用户体验改善计划 **(CUXIP)** 使用 Pendo 通过提供搜索文章、应用内指南等，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所有最近的公告。

通过 **CUXIP** 收集哪些使用情况数据**?**

使用情况数据完全是用户操作的。使用情况数据也称为事件级数据，包括用户在 Web 站点上访问的页面到特定功能的点击次数等所有内容。使用情况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。此数据可以优化我们的用户体验。

下面是我们收集的一些使用情况数据：

- 页面浏览量的详细信息、在每个页面上花费的时间。
- 访客 ID 是唯一的匿名标识符，用于帮助识别页面上唯一访客的数量。
- 问卷调查统计信息 - 分数、观看次数、提交数量等。

CUXIP 如何帮助您**?**

我们使用使用情况数据来改善您的 ADM 体验。下面是我们打算改善客户用户体验的一些方法：

- 应用内引导式工作流程和搜索相关文章的能力。
- 在应用程序内参与问卷调查，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 的工作原理是什么**?**

NetScaler ADM 设备可以位于内部网络中。浏览器必须具有 Internet 连接才能获得 CUXIP 指导式帮助的好处。

我怎样才能在我的 **ADM** 上禁用 **CUXIP?**

要禁用 CUXIP，请在 ADM GUI 中执行以下操作：

1. 导航到“设置”**>**“系统管理”。
2. 在 **CUXIP** 设置中，并禁用 CUXIP。

我们的隐私政策的变更

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这些更改。在变更生效之前，我们将通过电子邮件和/或我们服务的明确通知通知您，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 Citrix 隐私政策 页面上发布时生效。

引用

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

许可

February 6, 2024

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

NetScaler ADM 支持以下许可证版本。要购买 ADM 许可证，请联系您的 NetScaler 销售代表或合作伙伴。

Express 版—您可以使用 Express 版许可证管理和监视任意数量的实例。默认情况下，将应用 Express Edition 许可证。

Advanced Edition - 它允许管理发现的应用程序，并查看购买的虚拟服务器以及免费虚拟服务器的分析。

注意事项：

- 对于版本 **13.1-9.x** 或更早版本，您最多可以管理 30 个已发现的应用程序或虚拟服务器并查看分析。除了发现的 30 个应用程序或 30 个虚拟服务器之外，您还必须购买并应用高级许可证。例如，如果您购买了 100 个虚拟服务器许可证，则您有权使用最多 130 个虚拟服务器许可证。
- 对于版本 **13.1-12.x** 或更高版本，您最多可以管理两个发现的应用程序或虚拟服务器并查看分析。除了发现的两个应用程序或两个虚拟服务器之外，您还必须购买并应用 Advanced 许可证。例如，如果您购买了 100 个虚拟服务器许可证，则您有权使用最多 102 个虚拟服务器许可证。

升级后构建 **13.1-12.x**：

- 所有 Express 默认免费虚拟服务器将在 30 天内保持正常运行。您可以选择 2 个虚拟服务器并在 30 天宽限期内应用 2 个默认许可证。如果在升级 30 天后未执行用户操作，ADM 会随机将许可证应用于 2 台虚拟服务器，并取消其余虚拟服务器的许可。您必须购买并应用新的 Advanced 许可证才能启用这些虚拟服务器。
- 升级后，以下是 ADM 行为的变化：
  - ADM 强制执行 30 天的宽限期。
  - 在 30 天的宽限期内，将阻止为 30 个免费快速虚拟服务器分配新的虚拟服务器。
    - 例如，如果在升级到 12.x 之前的可用虚拟服务器许可证数量为 30，并且只使用了 20 个许可的虚拟服务器，则在 30 天宽限期内，您只能使用 20 个虚拟服务器，不允许许可剩余 10 个虚拟服务器。
  - 但是，在 30 天宽限期内，作为管理员，您仍然可以应用 Advanced ADM 许可证并分配新虚拟服务器。

功能	选项	Express Edition	Advance Edition	NetScaler 许可证
应用程序	应用程序控制板	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。	应用程序控制板上的 NetScaler Web App Firewall 相关信息需要使用应用程序防火墙许可证的高级版（或）高级版。
		Web Insight	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。
		服务图表	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。

功能	选项	Express Edition	Advance Edition	NetScaler 许可证
		“配置”>“样书”	无限制	无限制
安全	安全控制面板	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。	安全控制板上的 NetScaler Web App Firewall 相关信息需要使用应用程序防火墙许可证的高级版（或）高级版。
		安全违规	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。
		用户和终端	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。
网关	HDX Insight	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。	Advanced（报告 < 1 小时）Premium（报告 = 无限制）
		Gateway Insight	最多两台虚拟服务器。	有权获得所有购买的虚拟服务器许可证和另外两台虚拟服务器。
基础设施	基础设施分析	无限制	无限制	不适用
		实例	无限制	无限制
		SSL 控制板	无限制	无限制
		事件	无限制	无限制
		网络功能	无限制	无限制
		网络报告	无限制	无限制
		共用许可证	无限制	无限制
		“配置”>“配置作业”、“配置模板”和“配置建议”	无限制	无限制
		升级作业	无限制	无限制
		调配	无限制	无限制
		WAN Insight	无限制	无限制
设置	RBAC 和外部身份验证（实例级别）	无限制	无限制	不适用

功能	选项	Express Edition	Advance Edition	NetScaler 许可证
		RBAC 和外部身份验证	无限制	无限制

* 为了支持 Citrix Director 与 NetScaler ADM 集成 - Citrix Director 必须具有 Premium 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。您可以获得有效的许可证并通过 NetScaler ADM GUI 在 NetScaler ADM 服务器上添加许可证。

高可用性

NetScaler 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。

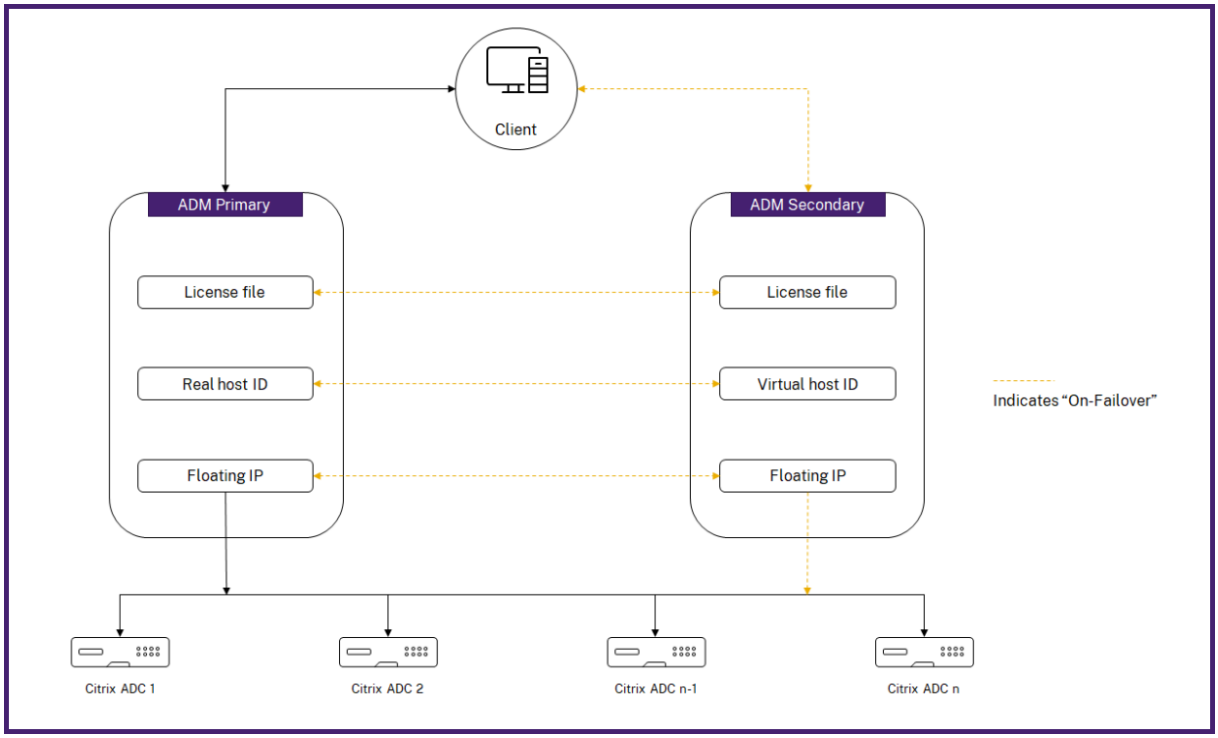
如果将 ADM 高可用性对配置为许可证服务器，则主服务器和辅助服务器必须具有相同的许可证文件。因此，在 ADM 高可用性部署中，NetScaler ADM 支持将相同的许可证文件分配给两台服务器。

> 注意
>
> - 如果您安装了 NetScaler ADM 12.1.49.x 或更早版本，则将有 30 天的宽限期来维持辅助节点的许可。宽限期过后，必须联系 Citrix 以重新托管原始许可证。
> - 对于 12.1.50.x 或更高版本，NetScaler 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。

- **Real Host ID**（真实主机 ID）- 此 ID 由 ADM 服务器的 MAC 地址生成。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. NetScaler 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 NetScaler ADM HA 中签出许可证，实例需要特定设备的 IP 地址。当您在负责许可的主服务器上申请许可证时，它会在该实例上应用所有未来的许可证。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 NetScaler ADM 上的许可，以监视和管理 NetScaler 设备上托管的更多虚拟服务器。

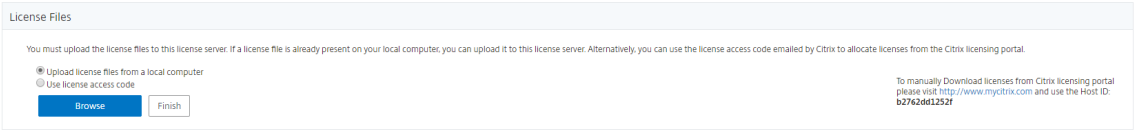
要升级您的设备许可证，请执行以下操作：

1. 使用管理员凭据登录到 NetScaler ADM。
2. 导航到 **Infrastructure**（基础结构）**> Pooled Licensing**（池许可）。

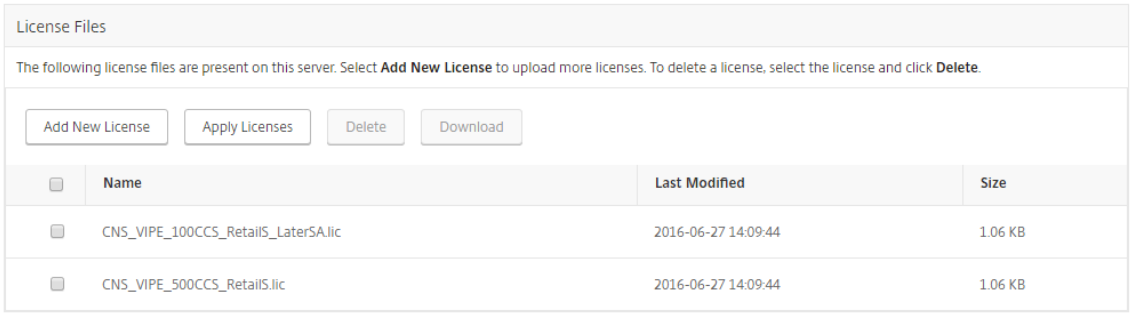
3. 转到 许可证文件，然后选择以下选项之一：

   - 从本地计算机上载许可证文件。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的许可证访问代码。在文本框中输入许可证访问代码，然后单击 **Get Licenses**（获取许可证）。

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

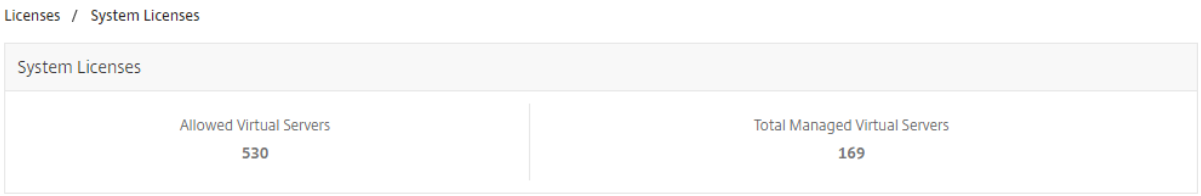


4. 您可以随时从“许可证设置”页面添加更多许可证。



验证

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



管理虚拟服务器

您可以选择要通过 NetScaler 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，NetScaler 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 NetScaler 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量，则默认情况下，NetScaler ADM 会为所有虚拟服务器提供许可证。

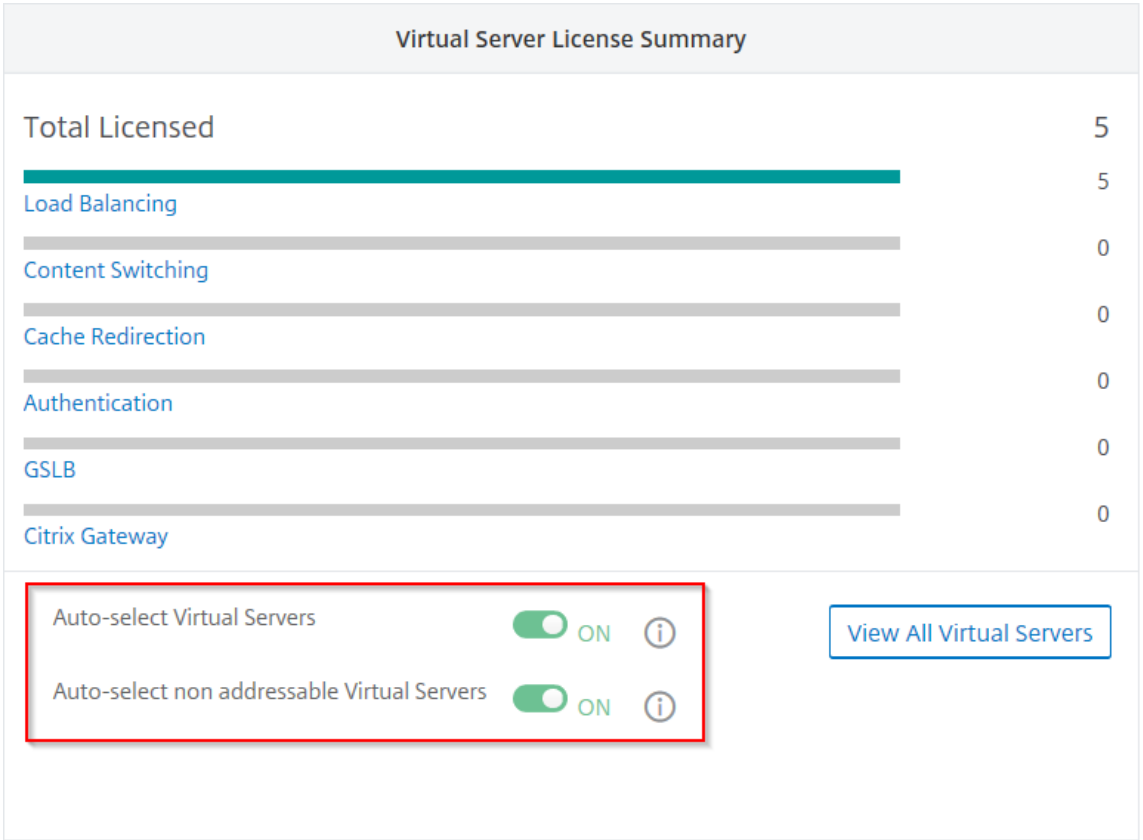
要手动选择虚拟服务器，或要仅对有限的虚拟服务器进行许可，您必须先禁用自动许可虚拟服务器，然后选择您要管理的虚拟服务器。

禁用自动许可虚拟服务器

1. 导航到 **Settings**（设置）**> Licensing & Analytics Configuration**（许可和分析配置）。

   控制板上将显示可用的虚拟服务器许可证、托管的虚拟服务器以及虚拟服务器类型和许可证过期信息。

2. 在 **Virtual Server License Allocation**（虚拟服务器许可证分配）中，禁用 **Auto Licensed Virtual Servers**（自动获得许可的虚拟服务器）和 **Auto-select non addressable Virtual Servers**（自动选择不可寻址的虚拟服务器）。

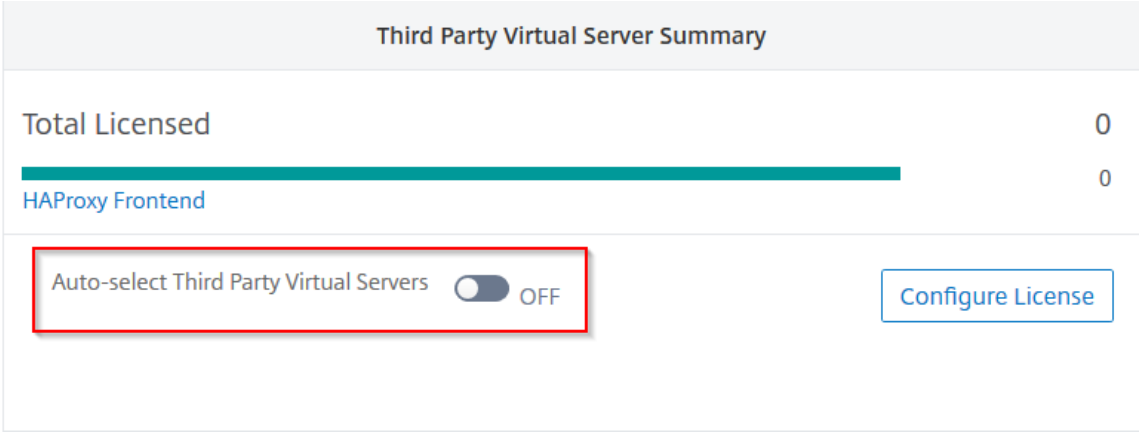


选择第三方虚拟服务器进行许可

1. 导航到 **Settings**（设置）**> Licensing & Analytics Configuration**（许可和分析配置）。

   控制板上将显示可用的虚拟服务器许可证、托管的虚拟服务器以及虚拟服务器类型和许可证过期信息。

2. 在 **Third Party Virtual Server Summary**（第三方虚拟服务器摘要）中，禁用 **Auto-select Third Party Virtual Servers**（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”。

   屏幕上将显示 **All Vitrual Servers**（所有虚拟服务器）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 **License**（许可证）。

配置基于策略的虚拟服务器许可

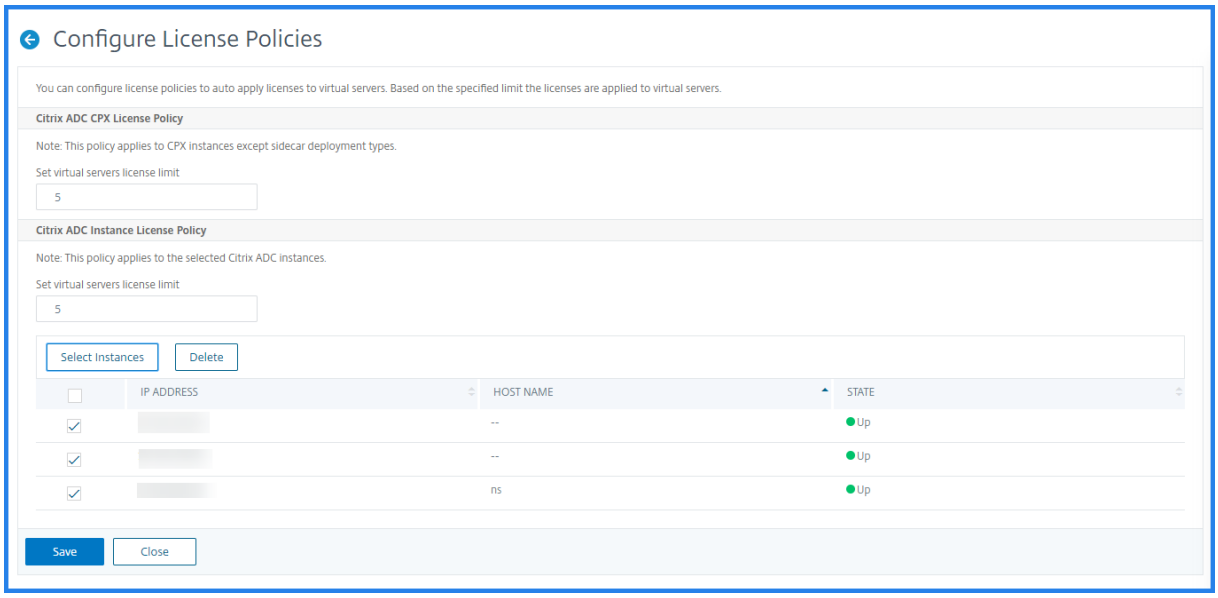
可以配置策略以将许可证应用到虚拟服务器。此策略控制您想要自动许可的虚拟服务器数量。它还将许可证仅应用到选定实例的虚拟服务器。

单击 **Edit Policies**（编辑策略），您可以指定以下内容：

- 单独设置 CPX 实例上的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
  >
  > 此限制适用于除 sidecar 部署类型之外的 CPX 实例。
  >
  > 要查看 sidecar 部署类型的 CPX 实例，请使用以下属性筛选虚拟服务器：`License Type: Freely Managed`。

- 在选定的 ADC 实例 (MPX/VPX/BLX) 上设置虚拟服务器限制以应用许可证。ADM 将许可证应用到 ADC 实例上的虚拟服务器，但不得超过指定的限制。
- 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，您可以查看已许可的虚拟服务器或第三方虚拟服务器。

1. 导航到 **Settings**（设置）**> Licensing & Analytics Configuration**（许可和分析配置）。
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。

为不可寻址的虚拟服务器配置自动许可支持

默认情况下，NetScaler ADM 不会自动将许可证应用于不可寻址的虚拟服务器。对于不可寻址的虚拟服务器的许可，必须禁用自动许可选项，然后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。

NetScaler ADM 在 NetScaler ADM 中的 **Virtual Server License Allocation**（虚拟服务器许可证分配）下提供了一个选项。如果启用“自动选择不可寻址的虚拟服务器”选项，则会自动应用许可证不可寻址的虚拟服务器。

> 注意
>
> - 默认情况下，NetScaler 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（应用程序控制板）是当前在许可的非寻址虚拟服务器上支持的唯一分析。

虚拟服务器许可证过期检查

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

查看许可证的状态：

1. 导航到 基础架构 **>** 池许可 **>** 系统许可证。
2. 在 **License Expiry Information**（许可证过期信息）部分中，可以看到要过期的许可证的详细信息：
    - **Feature**（功能）：要过期的许可证类型。
    - **Count**（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 基础架构 **>** 池化许可 **>** 设置。
2. 在 **Notification Settings**（通知设置）部分中，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 (Text Message)**（SMS (文本消息)）：用于在许可证达到阈值或要过期时发送通知的 SMS 配置文件或通讯组列表。
    - **Slack** -指定 Slack 配置文件详细信息。
    - **PagerDuty** 警报 - 指定 PagerDuty 配置文件。根据在 PagerDuty 门户中配置的通知设置，当证书即将过期时，系统会发送通知。
    - **Notify me**（通知我）：设置池许可证的百分比，以通过电子邮件或 SMS 通知管理员。
    - **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

February 6, 2024

在安装 NetScaler 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。

NetScaler ADM 的要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU 注意： Citrix 建议在 NetScaler ADM 部署中使用固态硬盘 (SSD) 技术。
存储空间	所需的默认存储空间为 120 GB。实际存储需求取决于 NetScaler ADM 大小估计。使用 NetScaler 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**NetScaler MAS** 版本 **12.1 >** 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 NetScaler ADM 存储需求超过 120 GB，则必须附加一个额外的磁盘。您只能再添加一个磁盘。 Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。 有关更多信息，请参阅 如何将其他磁盘附加到 NetScaler ADM。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

NetScaler 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

> 注意
>
> AMD 处理器在以下方面受支持：

- **NetScaler ADM 13.1 Build 4.43** 或更高版本。
- **NetScaler ADM** 代理 **13.1 Build 17.42** 或更高版本。

NetScaler ADM 功能所需的最低 **NetScaler** 版本

重要

NetScaler ADM 版本和内部版本应 等于或高 于您的 NetScaler 版本和内部版本。例如，如果您已安装 NetScaler ADM 12.1 Build 50.39，请确保已安装 NetScaler 12.1 Build 50.28/50.31 或更早版本。

NetScaler ADM 功能	NetScaler 软件版本
样书	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
备份/还原	对于 NetScaler，10.1 及更高版本
	适用于 NetScaler SDX、11.0 及更高版本
监视/报告和使用作业进行配置	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
WAF 安全违规	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

* 如果 NetScaler 实例运行的版本 11.0 Build 66.x，NetScaler ADM 中不支持集成缓存指标。

NetScaler ADM 分析的要求

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

NetScaler 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
>
> NetScaler Gateway 功能（在版本 9.3 和 10.x 中标记为接入网关企业版）必须在 NetScaler 实例上可用。NetScaler ADM 不支持独立 Access Gateway Standard 设备。

NetScaler ADM 可以为在 Citrix Virtual Apps 或 Citrix Virtual Desktops 上发布并通过 Citrix Workspace 访问的应用程序生成报告。但是，此功能取决于安装 Workspace 的操作系统。目前，NetScaler 不解析通过在 iOS 或 Android 操作系统上运行的 Citrix Workspace 访问的应用程序或桌面的 ICA 流量。

支持 **HDX Insight** 的瘦客户端

- 基于 Dell Wyse Windows 的瘦客户端
- 基于 Dell Wyse Linux 的瘦客户端
- 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 需要 **NetScaler** 实例许可证

NetScaler ADM 针对 HDX Insight 收集的数据取决于所监视的 NetScaler 实例的版本和许可证。HDX Insight 报告仅显示运行 10.5 及更高版本的 NetScaler 高级版和高级版设备。

NetScaler 许可证/持续时间	5 分钟	1 小时	1 天	1 周	1 个月
Standard	否	否	否	否	否
高级	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 NetScaler 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、6.7 和 7.0
Microsoft Hyper-V	2012 R2 和 2016
通用 KVM	RHEL 7.4、RHEL 8.0、Ubuntu 16.04 和 Ubuntu 18.04

支持的操作系统和 **Workspace** 版本

下表列出了 NetScaler ADM 支持的操作系统，以及每个系统目前支持的 Citrix Workspace 版本：

操作系统	Workspace 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

支持的浏览器

下表列出了 NetScaler ADM 支持的 Web 浏览器：

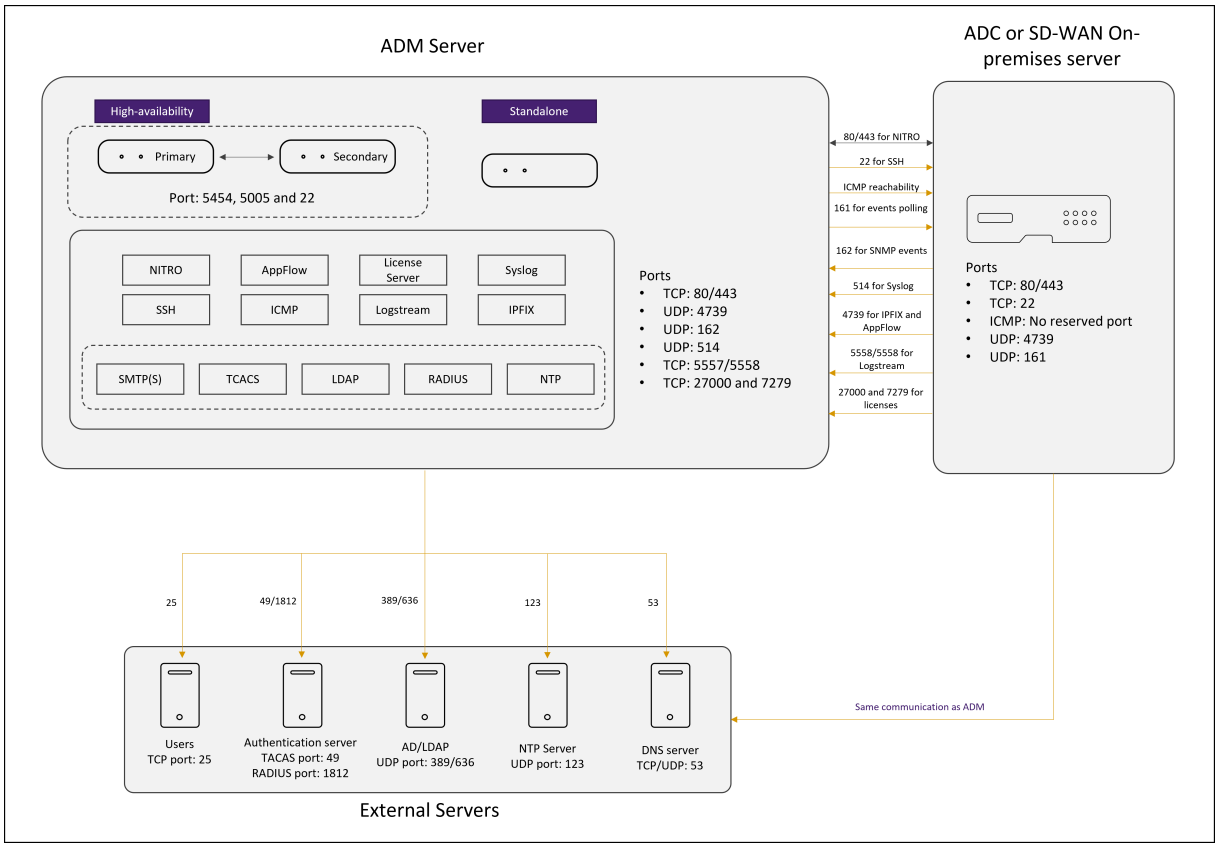
Web 浏览器	版本
Microsoft Edge	79 及更高版本
Google Chrome	51 及更高版本
Safari	10 及更高版本
Mozilla Firefox	52 及更高版本

支持的端口

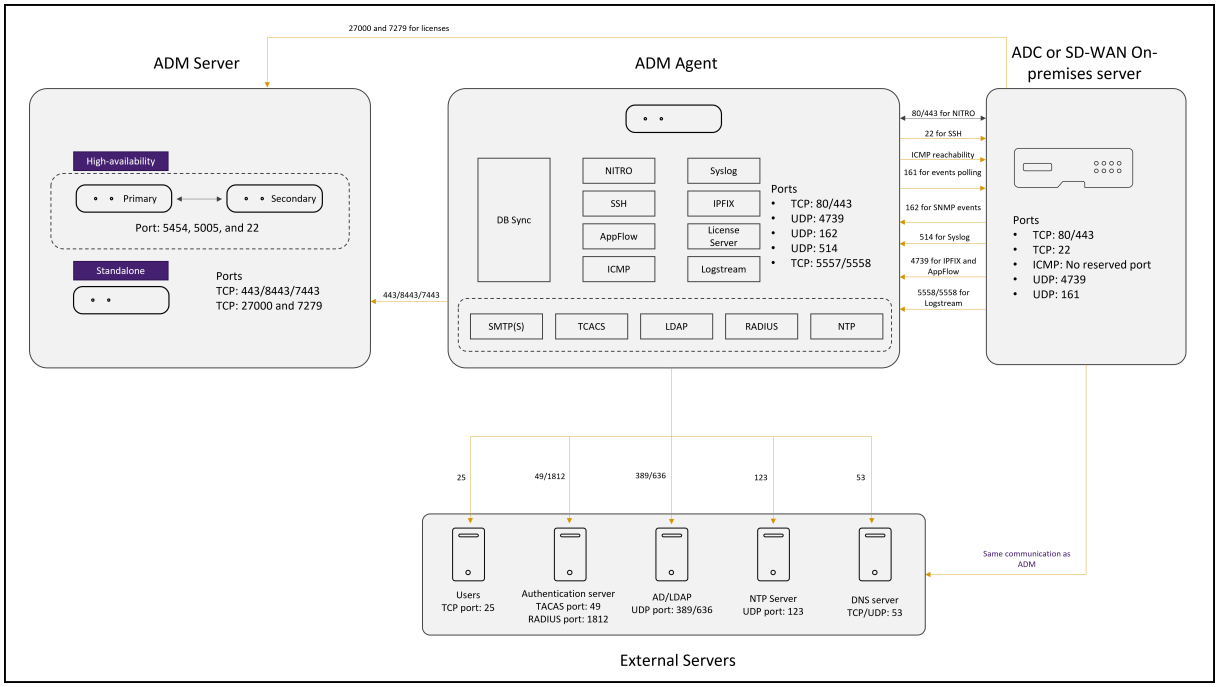
NetScaler ADM 使用 NetScaler IP（称为 NSIP）地址与 NetScaler 进行通信。您可以使用 ADM 代理作为 ADC 实例和 ADM 之间的中介。要与这些服务器建立通信，请打开所需的端口。

> 注意
>
> 如果您将 NetScaler 配置为高可用性模式，则 NetScaler ADM 使用 NSIP 与 NetScaler 通信，所需的端口保持不变。

无代理部署的网络端口示意图：



包含 **ADM** 代理的部署的网络端口示意图：



以下各节说明了所需的端口及其用途：

- ADM 服务器
- ADM 代理
- ADC 实例
- 外部服务器

ADM 服务器的端口

下表说明了必须在 ADM 服务器上打开的所需端口。

端口	类型	详细信息	通信方向
80/443/5454/22	TCP	在高可用性模式下，NetScaler ADM 节点之间用于通信和数据库同步的默认端口。	NetScaler ADM 主节点到 NetScaler ADM 辅助节点
443/8443/7443	TCP	NetScaler ADM 代理和 NetScaler ADM 之间的通信端口。	NetScaler ADM 代理启动与 NetScaler ADM 的通信。然后，NetScaler ADM 和代理相互交互。

端口	类型	详细信息	通信方向
27000 和 7279	TCP	NetScaler ADM 许可证服务器和 ADC 实例之间通信的许可证端口。这些端口也用于 ADC 池许可证。	NetScaler 到 NetScaler ADM
5005	UDP	在高可用性节点之间交换检测信号的端口。	NetScaler ADM 主节点到辅助节点。NetScaler ADM 辅助节点到主节点。

如果 ADM 和 ADC 实例未使用代理进行通信，请务必在 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 NetScaler ADM 到 NetScaler 实例的 NITRO 通信。	NetScaler ADM 代理到 NetScaler 以及 NetScaler 到 NetScaler ADM 代理
4739	UDP	用于从 NetScaler 实例到 NetScaler ADM 的 AppFlow 通信。	NetScaler 到 NetScaler ADM 代理
162	UDP	接收从 NetScaler 实例到 NetScaler ADM 的 SNMP 事件。	NetScaler 到 NetScaler ADM 代理
514	UDP	接收从 NetScaler 实例发送到 NetScaler ADM 的系统日志消息。	NetScaler 到 NetScaler ADM 代理
5557/5558	TCP	用于从 NetScaler 到 NetScaler ADM 的 Logstream 通信（针对 WAF 安全违规、Web Insight 察和 HDX Insight)。	NetScaler 到 NetScaler ADM
5563	TCP	接收从 NetScaler 实例到 NetScaler ADM 的 ADC 指标（计数器)、系统事件和审核日志消息	NetScaler 到 NetScaler 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 NetScaler ADM 到 NetScaler 实例的 NITRO 通信。	NetScaler ADM 代理到 NetScaler 以及 NetScaler 到 NetScaler ADM 代理
4739	UDP	用于从 NetScaler 实例到 NetScaler ADM 的 AppFlow 通信。	NetScaler 到 NetScaler ADM 代理
162	UDP	接收从 NetScaler 实例到 NetScaler ADM 的 SNMP 事件。	NetScaler 到 NetScaler ADM 代理
514	UDP	接收从 NetScaler 实例发送到 NetScaler ADM 的系统日志消息。	NetScaler 到 NetScaler ADM 代理
5557/5558	TCP	用于从 NetScaler 到 NetScaler ADM 的 Logstream 通信（针对 WAF 安全违规、Web Insight 察和 HDX Insight）。	NetScaler 到 NetScaler ADM

ADC 实例的端口

下表说明了必须在 NetScaler 实例上打开的所需端口。

端口	类型	详细信息	通信方向
80/443	TCP	用于从 NetScaler ADM 到 NetScaler 实例的 NITRO 通信。用于高可用性模式下 NetScaler ADM 服务器之间的 NITRO 通信。	NetScaler ADM 到 NetScaler 和从 NetScaler 到 NetScaler ADM

端口	类型	详细信息	通信方向
22	TCP	用于从 NetScaler ADM 到 NetScaler 实例的 SSH 通信。用于以高可用性模式部署的 NetScaler ADM 服务器之间的同步。而且，ADM 代理与 NetScaler 之间的 SSH 通信需要此端口。	NetScaler ADM 到 NetScaler。或者，将 NetScaler ADM 代理转到 NetScaler。
无保留的端口	ICMP	检测 NetScaler ADM 与 NetScaler 实例之间的网络可访问性，或者在高可用性模式下部署的辅助 NetScaler ADM 服务器之间的网络可访问性。	NetScaler ADM 到 NetScaler
161	UDP	轮询来自 ADC 实例的事件。	NetScaler ADM 到 NetScaler

ADC 内置代理的端口

下表说明了 NetScaler 内置代理必须打开的所需端口。

端口	类型	详细信息	通信方向
443	TCP	用于从 NetScaler ADM 到 NetScaler 内置代理的所有通信	NetScaler ADM 到 NetScaler 内置代理和 NetScaler 内置代理到 NetScaler ADM

> 注意：
>
> 在 ADM 高可用性部署中，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 NetScaler ADM 发送给用户。	面向用户的 NetScaler ADM。
389/636	TCP	用于身份验证协议的默认端口。用于 NetScaler ADM 和 LDAP 外部身份验证服务器之间的通信。	NetScaler ADM 到 LDAP 外部身份验证服务器
123	UDP	用于与多个时间源同步的默认 NTP 服务器端口。	NetScaler ADM 到 NTP 服务器
1812	RADIUS	用于身份验证协议的默认端口。用于 NetScaler ADM 和 RADIUS 外部身份验证服务器之间的通信。	NetScaler ADM 到 RADIUS 外部身份验证服务器
49	TACACS	用于身份验证协议的默认端口。用于 NetScaler ADM 和 TACACS 外部身份验证服务器之间的通信。	NetScaler ADM 到 TACACS 外部身份验证服务器

限制

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

1. 针对 NetScaler ADM GUI 的管理访问权限
2. NetScaler 的管理访问权限
3. 注册和库存
4. “网络”控制板
5. “SSL”控制板
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 NetScalers 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 接收的系统日志
3. ADC 上支持 IPv6 的样书
4. 分析
5. 池许可

快速入门

February 6, 2024

本文档引导您首次开始部署和设置 NetScaler Application Delivery Management (ADM)。本文档适用于管理 Citrix 网络设备（NetScaler 和 NetScaler Gateway）的网络和应用程序管理员。无论您计划使用 NetScaler ADM 管理的设备类型是什么，都请按照本文档中的步骤进行操作。

如果您是 NetScaler ADM 的现有用户，建议您在将服务器 升级到最新 版本的 NetScaler ADM 之前查看发行说明、系统要求 和 许可 详细信息。

步骤 **1-**检查系统要求

在开始在数据中心部署 NetScaler 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，在未应用许可证的情况下，只能管理 30 个发现的应用程序以及只能查看两个虚拟服务器的分析信息。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 NetScaler 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 NetScaler ADM 与 NetScaler 实例通信所需的端口处于打开状态。了解更多。
- **NetScaler** 实例要求。不同的 NetScaler 软件版本支持不同的 NetScaler ADM 功能。查看此信息，以确保您已将 NetScaler 实例升级到正确版本。了解更多。

步骤 **2-**部署 **NetScaler 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 NetScaler ADM。您可以将 NetScaler ADM 部署为单个服务器或高可用性模式。如果您使用的是 NetScaler Insight Center，则可以迁移到 NetScaler ADM，除分析功能外，还可以使用管理、监视、调配和应用程序管理功能。

- 单服务器部署。在 NetScaler 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 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 NetScaler ADM。请参阅：
  - Citrix Hypervisor 上的 NetScaler ADM
  - 搭载 Microsoft Hyper-V 的 NetScaler ADM
  - 搭载 VMware ESXi 的 NetScaler ADM
  - 搭载 Linux KVM 服务器的 NetScaler ADM
- 高可用性部署。两台 NetScaler 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，必须在主动-被动模式下部署两个 NetScaler ADM 节点，在同一子网中使用相同的软件版本和内部版本，并且必须具有相同的配置。通过高可用性部署，在 NetScaler ADM 主节点上配置浮动 IP 地址的功能消除了单独的 NetScaler 负载平衡器的需要。要了解更多信息，请参阅在高可用性部署中配置。

步骤 **3-**将实例添加到 **NetScaler ADM**

实例是您想要从 NetScaler ADM 发现、管理和监视的 NetScaler ADC 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 NetScaler ADM 服务器。您可以将以下实例添加到 NetScaler ADM 中：

- NetScaler
  - NetScaler MPX
  - NetScaler VPX
  - NetScaler SDX
  - NetScaler CPX
  - NetScaler BLX
  - NetScaler Gateway

将实例添加到 NetScaler ADM 服务器后，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 **NetScaler ADM** 上配置 **NTP** 服务器

您必须在 NetScaler ADM 中配置网络时间协议 (NTP) 服务器才能将其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler 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 **NetScaler ADM** 性能

在开始使用 NetScaler 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 NetScaler 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。
- 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 NetScaler 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 NetScaler ADM 服务器数据库中存储的报告数据量，可以指定希望 NetScaler 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 小时修剪一次（在 00.00 点）。
- 配置系统备份设置。NetScaler ADM 每天 00:30 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 NetScaler 实例的当前状态，则可以使用备份文件恢复稳定性，以防实例变得不稳定。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 NetScaler ADM 服务器数据库中存储的事件消息数据量，可以指定希望 NetScaler 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 **syslog** 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。您可以指定天数，在此天数之后将从 NetScaler ADM 中删除以下系统日志数据：
  - 通用系统日志数据
  - AppFirewall 数据
  - NetScaler Gateway 数据。

    了解更多

接下来做什么

部署和设置 NetScaler ADM 后，您可以开始管理和监视您的实例和应用程序。

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

部署

February 6, 2024

在使用 NetScaler ADM 管理和监视您的应用程序和网络基础设施之前，必须先将其安装在其中一个虚拟机管理程序或 Kubernetes 群集上。如果您在虚拟机管理程序上部署 NetScaler ADM，则可以将其部署为单个服务器或在高可用性模式下部署。高可用性模式不适用于 Kubernetes 群集。如果您使用的是 NetScaler Insight Center，则可以将其迁移到 NetScaler ADM，除分析功能外，还可以使用管理、监视、调配和应用程序管理功能。

- 单服务器部署：对于部署在虚拟机管理程序上的独立 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 Citrix Hypervisor、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 部署 NetScaler ADM。请参阅：
  - Citrix Hypervisor 上的 NetScaler ADM
  - Microsoft Hyper-V 上的 NetScaler ADM
  - NetScaler ADM 在 VMware ESXi 上
  - Linux KVM 服务器上的 NetScaler ADM
  - Kubernetes 群集上的 NetScaler ADM
- 高可用性 **(HA)** 部署：两台 NetScaler ADM 服务器的高可用性部署可提供不间断的操作。在 HA 设置中，两个 NetScaler 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 NetScaler ADM 主节点上配置浮动 IP 地址，无需使用单独的 NetScaler 负载平衡器。请参阅：在高可用性部署中配置。

> 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 **NetScaler ADM**：您可以将 NetScaler Insight Center 部署迁移至 NetScaler ADM，而不会丢失现有的配置、设置或数据。使用 NetScaler ADM，您不仅可以查看 NetScaler 生成的各种分析，还可以从单个统一控制台管理、监视整个全球应用程序交付基础架构并对其进行故障排除。请参阅：从 NetScaler Insight Center 迁移到 NetScaler ADM
- 将 **NetScaler ADM** 与 **Director** 集成：Director 与 NetScaler ADM 集成，用于网络分析和性能管理。请参阅：将 NetScaler ADM 与 Director集成

安装 NetScaler ADM 的必备条件

February 6, 2024

您可以下载适用于 Microsoft HyperV、
VMware ESXi、Linux KVM 和 Citrix Hypervisor 平台的 NetScaler Application Delivery Management (ADM) 作为虚拟设备进行安装。在安装
NetScaler 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 NetScaler ADM 的特定平台要求和详细步骤，请参阅以下主题：

- Citrix Hypervisor 上的 NetScaler ADM
- 采用 Microsoft HyperV 的 NetScaler ADM
- 搭载 VMware ESXi 的 NetScaler ADM
- 搭载 Linux KVM 服务器的 NetScaler ADM

NetScaler ADM 的一般要求

组件	要求
RAM	32 GB
虚拟 CPU	8 个 CPU
存储空间	Citrix 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。 所需的默认存储空间为 120 GB。实际存储需求取决于 NetScaler ADM 大小估计。使用 NetScaler 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**NetScaler MAS** 版本 **12.1 >** 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 NetScaler 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。 有关更多信息，请参阅 如何将其他磁盘附加到 NetScaler ADM。
虚拟网络接口	1

组件	要求
吞吐量	1 Gbps

> 注意：
>
> Citrix 建议您将 NetScaler ADM VHD 托管在本地存储上。当托管在 SAN 中的存储设备上时，NetScaler ADM 可能无法按预期工作。因此，不支持在 SAN 上部署 ADM。

Citrix Hypervisor 上的 NetScaler ADM

February 6, 2024

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

> 注意：
>
> NetScaler ADM 不支持 XenMotion。

必备条件

在安装 NetScaler 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 Citrix Hypervisor 上安装 NetScaler ADM。
- 您已经下载了 NetScaler ADM .XVA 镜像文件。

XenCenter 系统要求

XenCenter 是一款 Windows 客户端应用程序。它不能与 Citrix Hypervisor 主机在同一台计算机上运行。下表说明了最低系统要求。

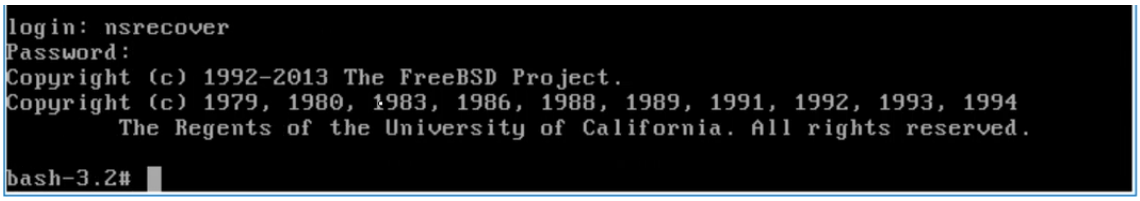
组件	要求
操作系统	Windows 7、Windows Server 2003 或 Windows 10
.NET Framework	2.0 版或更高版本

组件	要求
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 **NetScaler Application Delivery Management**

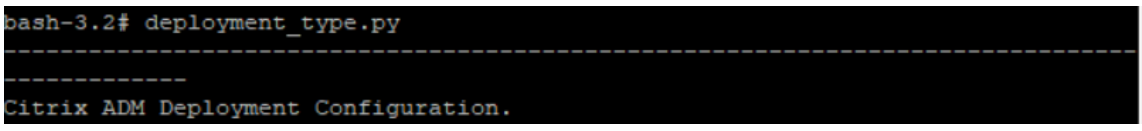
1. 将 XVA 映像文件导入 Citrix Hypervisor，然后从 控制台选项卡配置初始 网络配置选项。

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。

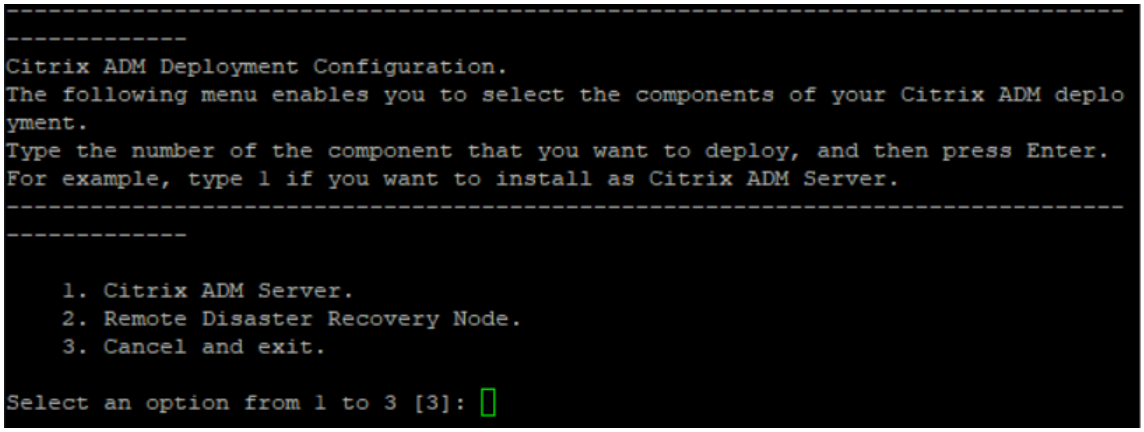


> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`、更新配置并保存配置。

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. 选择部署类型为 **NetScaler ADM** 服务器。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 NetScaler ADM 部署为独立部署。
7. 键入是以重新启动 NetScaler ADM 服务器。

> 注意
>
> 安装 NetScaler ADM 后，您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 NetScaler 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 NetScaler ADM 配置实用程序。

Microsoft Hyper-V 上的 NetScaler ADM

February 6, 2024

若要在 Microsoft Hyper-V 上安装 NetScaler ADM，您必须首先将 NetScaler 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 NetScaler 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。
- 您已经下载了 NetScaler ADM 镜像文件。

Microsoft 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。

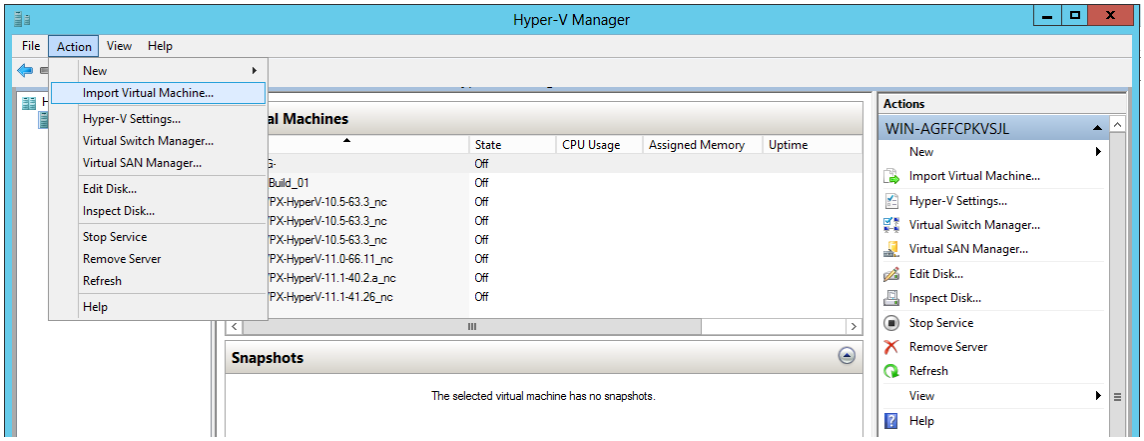
组件	要求
操作系统	Windows Server 2012 R2
.NET Framework	2.0 版或更高版本
CPU	750 MHz (MHz)，推荐：1 千兆赫兹（GHz）或更快
RAM	1 GB，建议：2 GB
NIC	100 Mbps 或速度更高的 NIC

安装 NetScaler Application Delivery Management

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

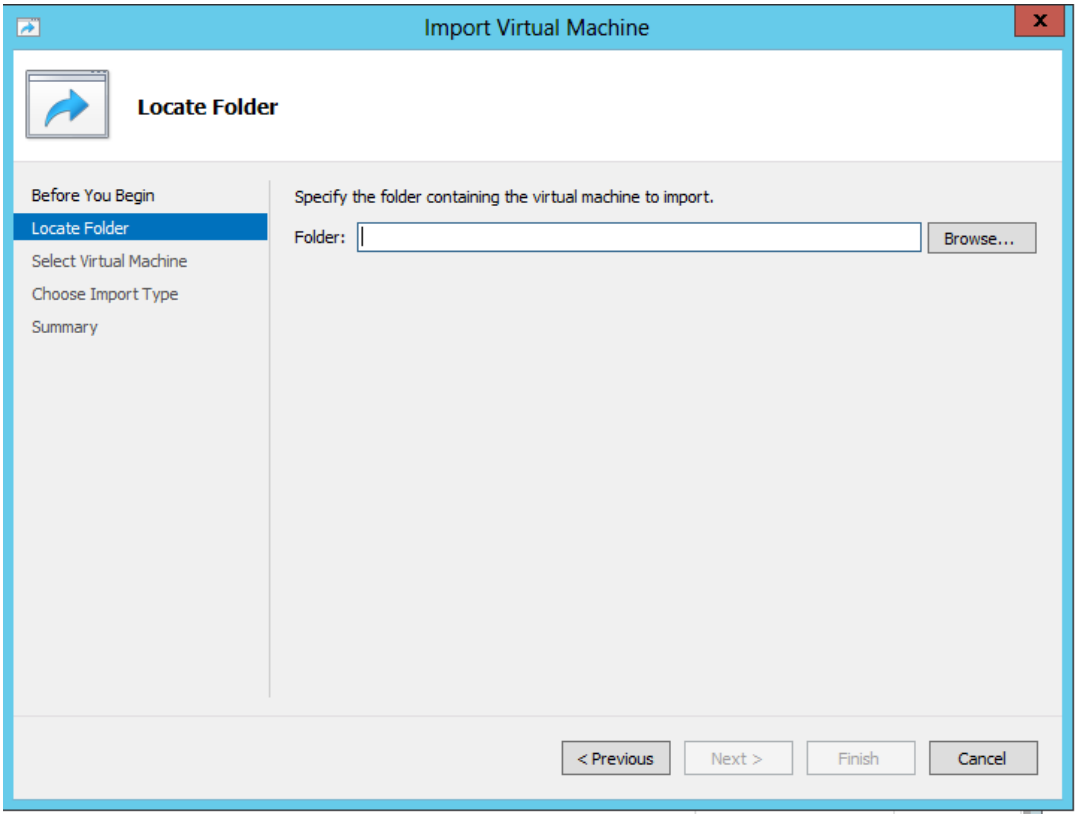
要安装 **NetScaler ADM**，请执行以下操作：

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）。



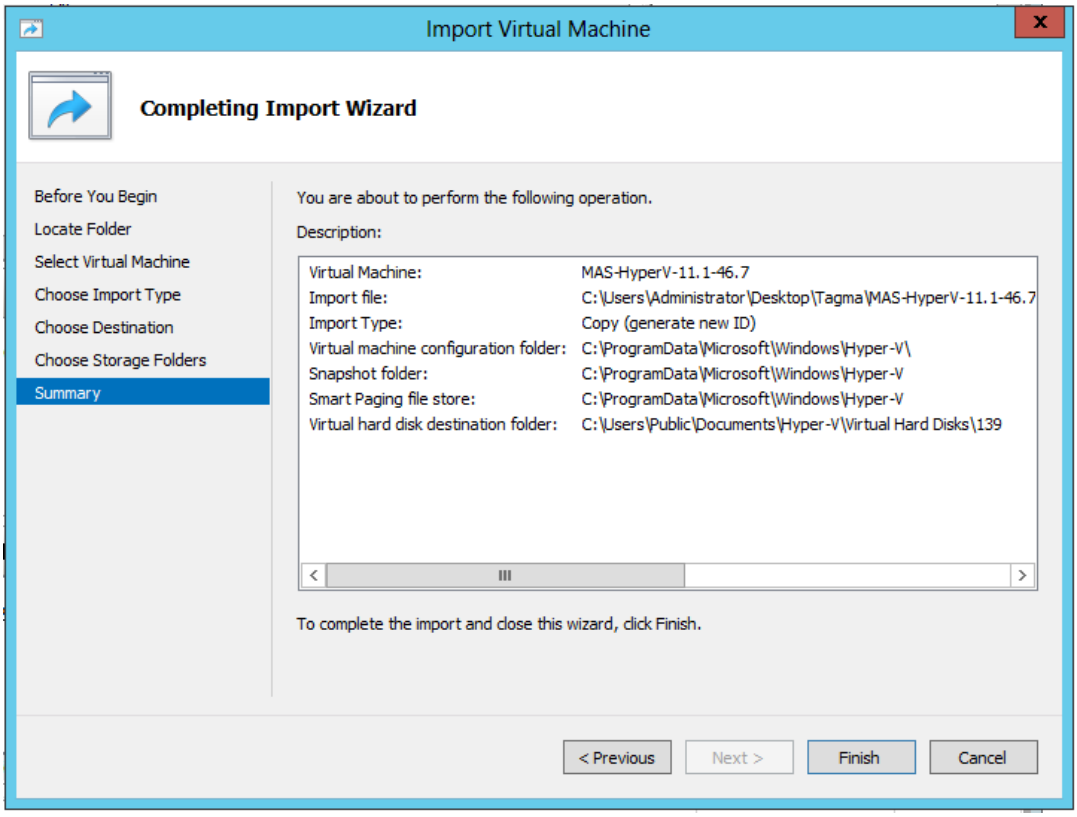
3. 导入 Hyper-V 映像，然后执行以下操作：
   a) 在“导入虚拟机”对话框的“查找文件夹”部分，浏览到保存 **NetScaler ADM Hyper-V** 映像的文件夹，选择该文件夹，然后单击下一步。
   b) 在“Select Virtual Machine”（选择虚拟机）部分，选择适当的虚拟机名称。
   c) 在 **Choose Import Type**（选择导入类型）部分，选择“Copy the virtual machine (create a new unique ID)”（复制虚拟机 (创建新的唯一 ID)）选项，并单击“Next”（下一步）。
   d)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



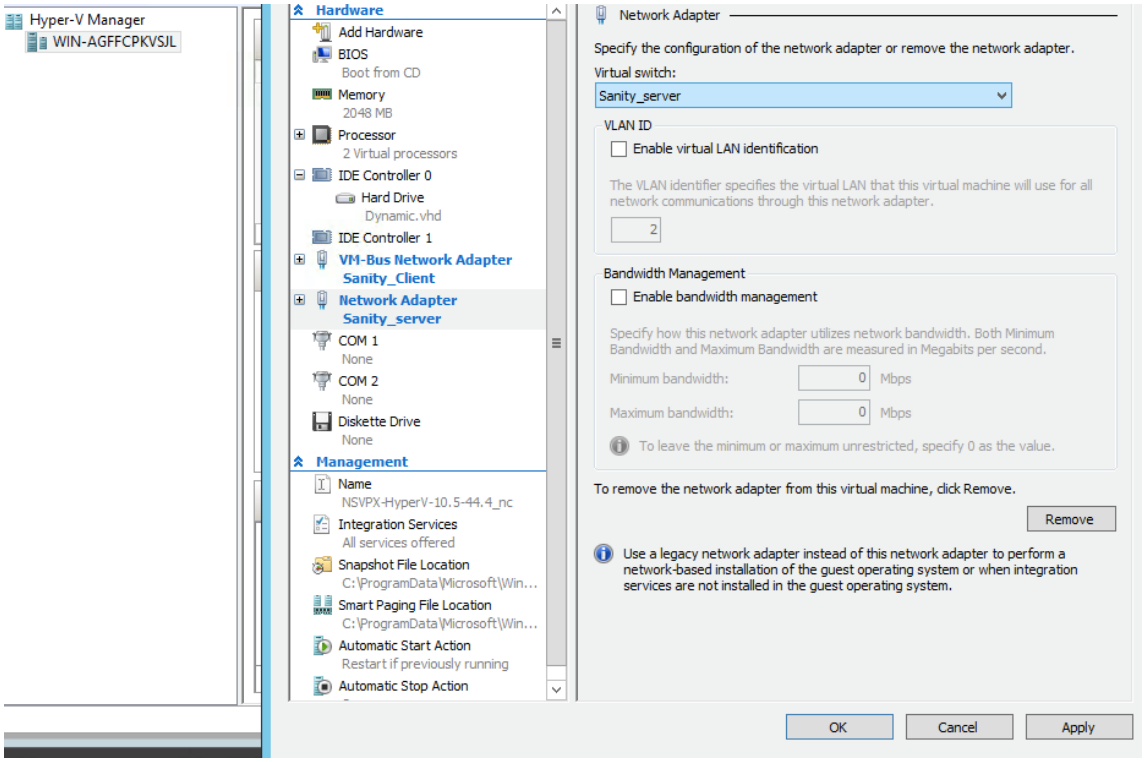
e) 在 **Choose Storage Folders**（选择存储文件夹）部分，可以选择要存储虚拟硬盘的位置，然后单击 **Next**（下一步）。

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



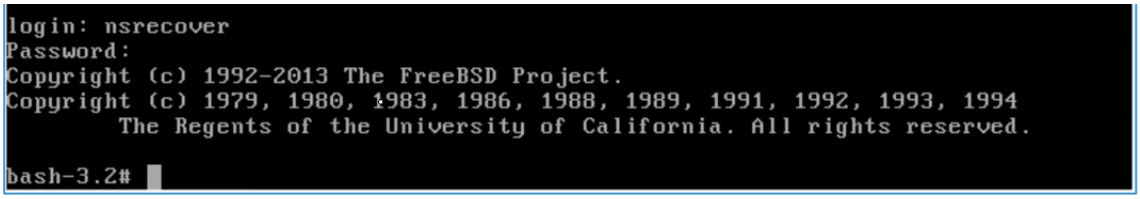
NetScaler ADM Hyper-V 图像显示在右侧窗格中。

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



6. 单击 **Apply**（应用），然后单击 **OK**（确定）。
7. 右键单击 **NetScaler ADM Hyper-V** 镜像，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. 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. 选择部署类型为 **NetScaler ADM** 服务器。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 NetScaler ADM 部署为独立部署。
15. 键入是以重新启动 NetScaler ADM 服务器。

> 注意
>
> 安装 NetScaler ADM 后，您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 NetScaler 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 NetScaler ADM 配置实用程序。

NetScaler ADM 在 VMware ESXi 上

February 6, 2024

本文档介绍了如何使用 VMware vSphere 客户端在 VMware ESXi 上安装 NetScaler ADM 虚拟设备。

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、6.7 和 7.0）。
- 在满足最低系统要求的管理工作站上安装 VMware 客户端。
- 下载 NetScaler ADM 安装文件。

> 注意
>
> - 只有 **NetScaler ADM 13.0** 版本 **47.22** 或更高版本支持 vMotion。您可以安排和自动执行部署在 ESXi 虚拟机管理程序上的 ADM 服务器的迁移，包括 vSphere 高可用性和 vSphere DRS 设置。
> - 适用于 NetScaler ADM 的 VMware Tools 作为软件版本的一部分提供，无法单独升级或修改。

安装 **NetScaler ADM**

请按照以下步骤在 VMware ESXi 上安装 ADM 虚拟设备。

> 注意
>
> 这些步骤和屏幕截图基于 VMware ESXi 6.0 版本。在其他 ESXi 版本中，GUI 可能有所不同。**NetScaler ADM 13.0 71.40** 或更高版本支持带有 VMXNET3 适配器的 VMware ESXi 7.0.1c 内部版本号 17325551。有关特定于版本的步骤，请参阅 VMware 文档。

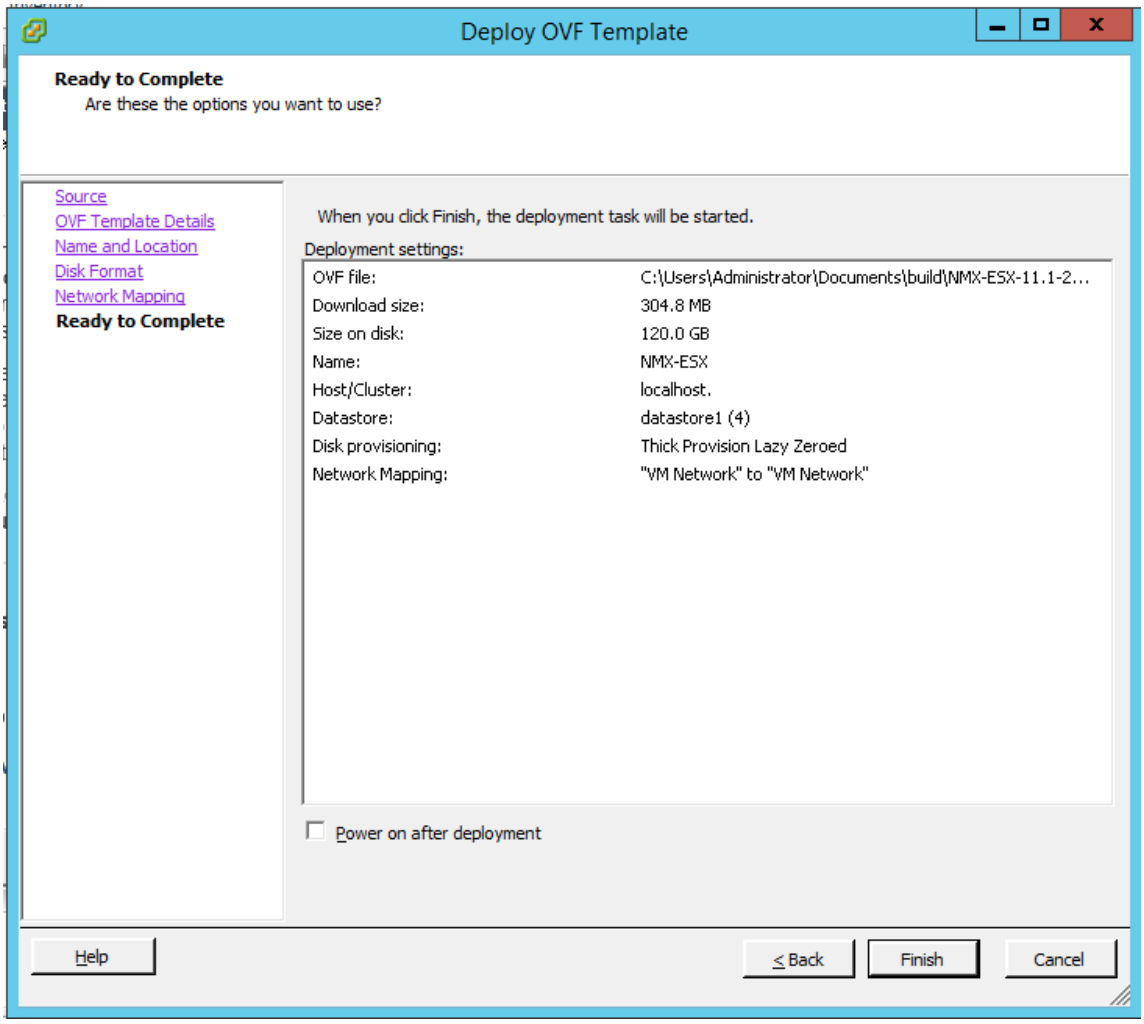
1. 在工作站上启动 VMware vSphere Client。
2. 在 **IP address / Name**（IP 地址/名称）文本框中，键入要连接到的 VMware ESXi 服务器的 IP 地址。
3. 在 **User Name**（用户名）和 **Password**（密码）文本框中，键入管理员凭据，然后单击 **Login**（登录）。
4. 在 **File**（文件）菜单中，单击 **Deploy OVF Template**（部署 OVF 模板）。
5. 在 **Deploy OVF Template**（部署 OVF 模板）对话框中，在 **Deploy from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

   > 注意
   >
   > 如果出现带有以下文本的警告消息：“所选主机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。

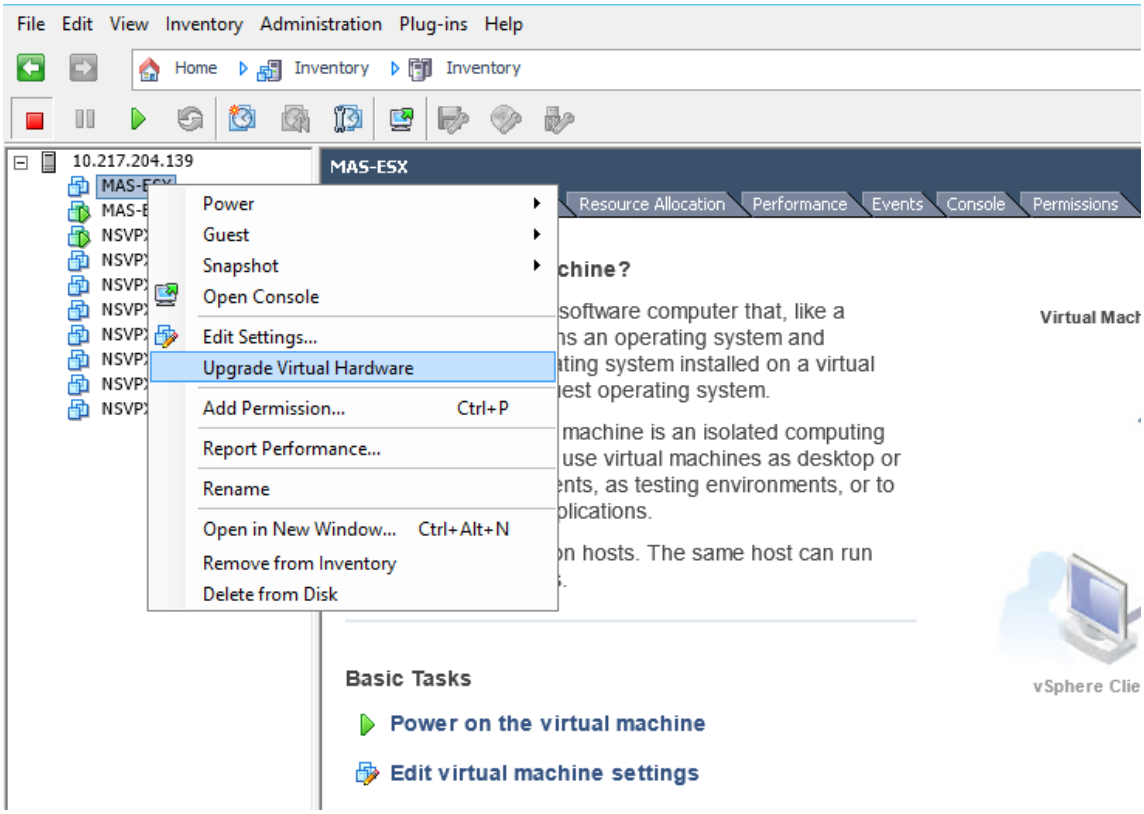
6. 在 **OVF Template Details**（OVF 模板详细信息）页面上，单击 **Next**（下一步）。
7. 键入 NetScaler ADM 虚拟设备的名称，然后单击 **Next**（下一步）。
8. 指定 “Disk Format”（磁盘格式）：选择” Thin provisioned format”（瘦置备格式）或 “Thick provisioned format”（密集置备格式）。

> 注意
>
> Citrix 建议选择 **Thick provisioned format**（密集置备格式）。

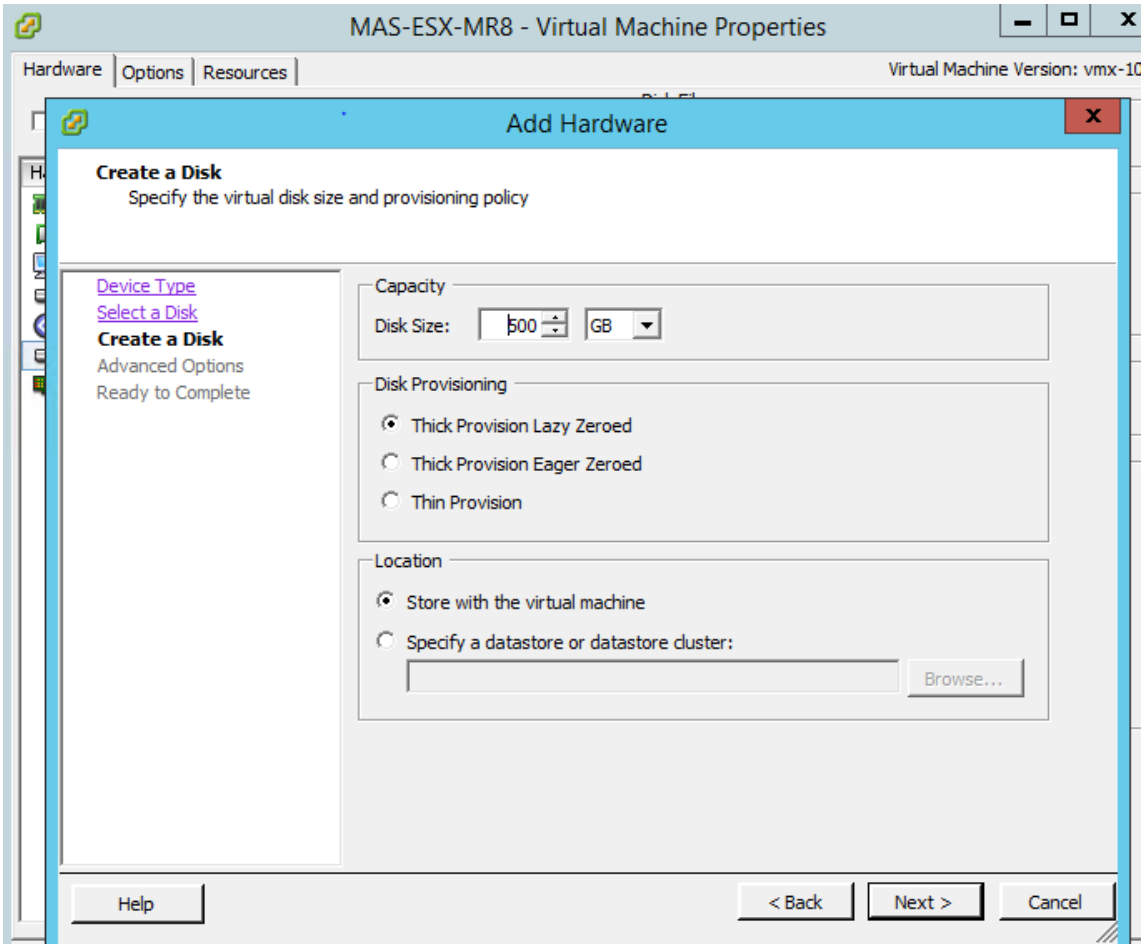
9. 单击 **Finish**（完成）开始安装过程。



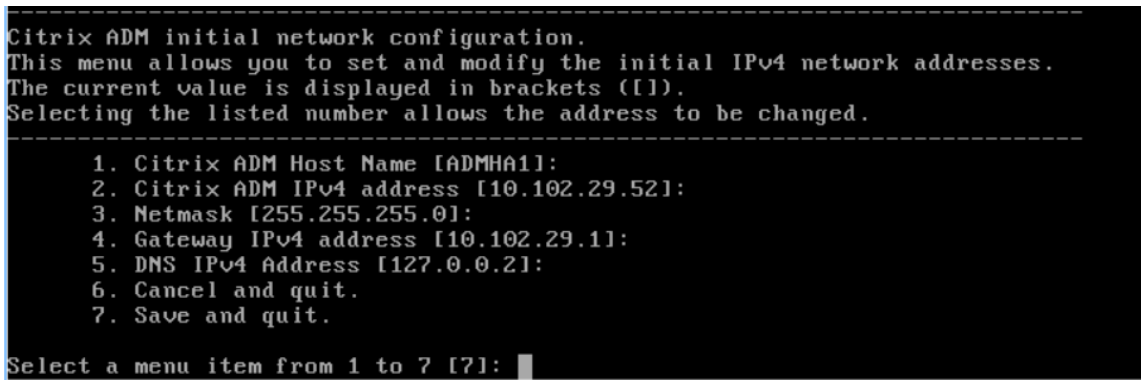
10. 此时您可以随时启动 NetScaler ADM 虚拟设备。
11. 在导航窗格中，选择您安装的虚拟设备。在清单菜单中，右键单击虚拟机，然后单击升级虚拟硬件。在 **Confirm Virtual Machine**（确认虚拟机）对话框中，单击 **Yes**（是）。



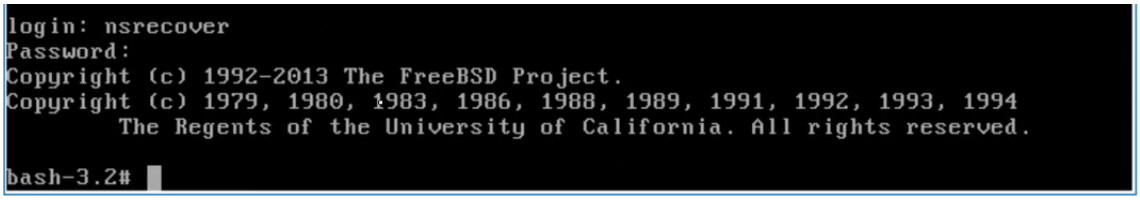
12. 在 **Inventory**（清单）菜单中，单击 **Virtual Machine**（虚拟机），然后选择 **Edit Settings**（编辑设置）。
13. 在 **Virtual Machine Properties**（虚拟机属性）对话框中的 **Hardware**（硬件）选项卡上，单击 **Memory**（内存），然后在右侧窗格中指定 **Memory Size**（内存大小）为 32 GB。
14. 单击 **CPUs**（CPU），然后在右侧窗格中指定 CPU 为 8。单击确定。
15. 根据您的要求添加额外的磁盘。



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，然后单击开机。
17. 单击控制台选项卡以显示 NetScaler ADM 初始网络配置选项。



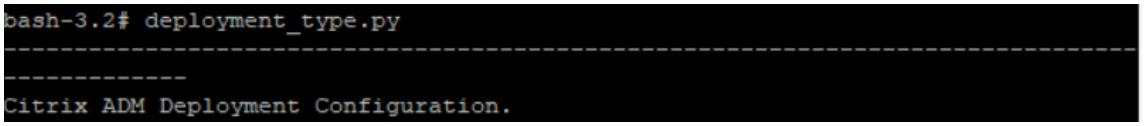
18. 指定所需的 IP 地址后，保存配置设置。
19. 出现提示时，使用 ns 恢复/nsroot 凭据登录。



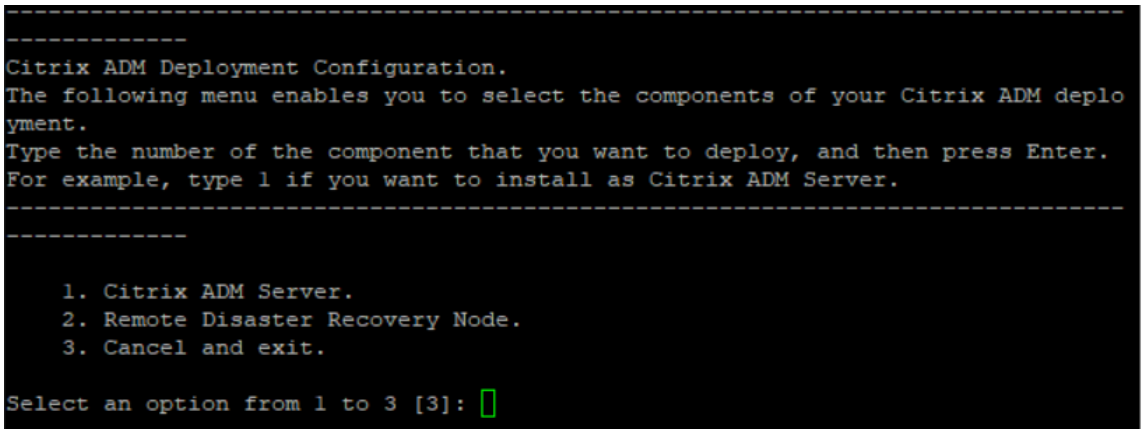
> 注意
>
> 登录后，如果要更新初始网络配置，请键入 `networkconfig`、更新配置并保存配置。

20. 在 shell 提示符下键入命令来运行部署脚本：

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



21. 选择部署类型为 **NetScaler ADM** 服务器。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 NetScaler ADM 部署为独立部署。
23. 键入是以重新启动 NetScaler ADM 服务器。

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

验证

安装服务器后，可以通过在浏览器中键入 NetScaler 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 NetScaler ADM 配置实用程序。

> 注意
>
> 在 VMware ESXi 上，典型的 ADM 安装时间约为 10 分钟，但在某些系统上可能需要更长的时间。

在 **VMware ESXi** 上自动部署 **NetScaler ADM** 代理

February 6, 2024

NetScaler ADM 允许您在 VMware ESXi 上自动部署 NetScaler ADM 代理。

作为管理员，您可以自动执行以下操作：

- 配置 NetScaler ADM 代理
- 注册 NetScaler ADM 代理并更改该代理的默认密码。

配置 **NetScaler ADM** 代理

要自动配置代理，请在.ovf 文件中添加以下参数的值：

1. IP 地址
2. 网络掩码
3. 网关
4. 域名服务器
5. 主机名

> 注意
>
> .ovf 文件在代理映像文件中可用。要下载 NetScaler ADM 代理文件，请转至。https://www.citrix.com/downloads/citrix-application-management/ 代理映像文件的命名模式如下所示，**MASAGENT-ESX-releasenumber-buildnumber.zip**

注册 **NetScaler ADM** 代理并更改默认密码

> 注意
>
> 在注册和更改默认密码之前，请确保已添加在 配置 NetScaler ADM 代理中指定的参数。

要自动注册 NetScaler ADM 代理和更改默认密码，请在同一个.ovf 文件中添加以下参数的值：

1. ADM 服务器 IP
2. ADM 用户名
3. ADM 密码
4. 代理新密码

必备条件

在开始安装虚拟设备之前，请确保：

- 在满足最低系统要求的管理工作站上安装 VMware vSphere 8.x。
- 下载 NetScaler ADM 安装文件。

如何配置和注册 **NetScaler ADM** 代理

1. 下载并编辑.OVF 文件
2. 在 VMware ESXi 上安装 NetScaler ADM 虚拟设备
3. 验证

下载并编辑**.OVF** 文件

1. 将文件从 MASAGENT-ESX-releasenumber-buildnumber.zip 解压缩到所需的位置。以下文件可用：
   - .ovf 文件
   - .vmdk 文件
   - .ova 文件
   - .mf 文件
2. 在任意编辑器中打开.ovf 文件，并在 </VirtualHardwareSection> 标签后添加以下 <ProductSection>..</ProductSection> 示例代码

```
<ProductSection>
    <Info>Information about the installed software</Info>
    <Product>Application Delivery management</Product>
    <Vendor>Citrix</Vendor>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.ip">
    <Label>IPAddress</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.netmask">
    <Label>Netmask</Label>
    </Property>

    <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
        string"
    ovf:key="eth0.gateway">
```



```
18      <Label>Gateway</Label>
19      </Property>
20
21      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
22      ovf:key="eth0.nameserver">
23      <Label>Nameserver</Label>
24      </Property>
25
26      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
27      ovf:key="eth0.hostname">
28      <Label>Hostname</Label>
29      </Property>
30
31      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
32      ovf:key="eth0.ServerIP">
33      <Label>ADM Server IP</Label>
34      </Property>
35
36      <Property ovf:userConfigurable="true" ovf:value="VALUE" ovf:type="
            string"
37      ovf:key="eth0.ServerUname">
38      <Label>ADM Username</Label>
39      </Property>
40
41      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
42      ovf:type="string" ovf:key="eth0.ServerPassword">
43      <Label>ADM Password</Label>
44      </Property>
45
46      <Property ovf:userConfigurable="true" ovf:password="true" ovf:value
            ="VALUE"
47      ovf:type="string" ovf:key="eth0.NewPassword">
48      <Label>Agent New Password</Label>
49      </Property>
50
51  </ProductSection>
52  <!--NeedCopy-->
```

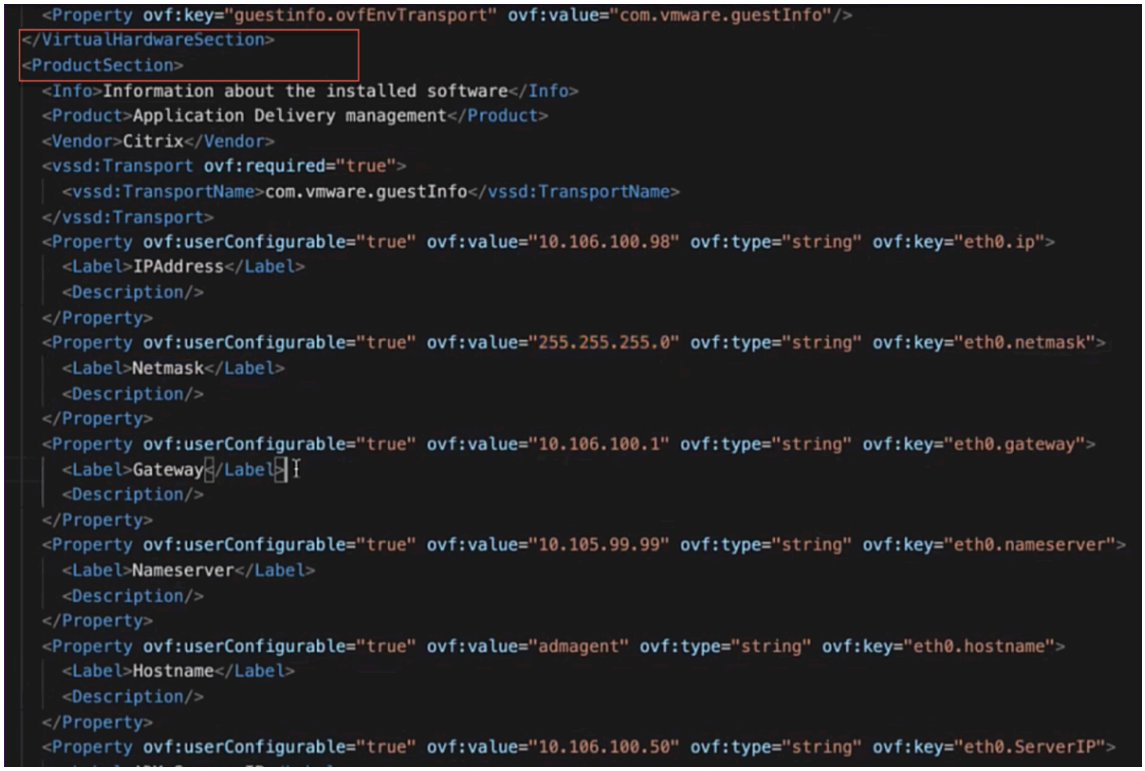
1. 对于要配置的参数，在 ovf:value=”VALUE”中添加其对应的值

   - 要配置 NetScaler ADM 代理，请将值添加到以下参数中：

     - IP 地址
     - 网络掩码
     - 网关
     - 域名服务器
     - 主机名

- 要注册和更改 NetScaler ADM 代理的默认密码，请将值添加到以下参数中：
  - ADM 服务器 IP
  - ADM 用户名
  - ADM 密码
  - 代理新密码

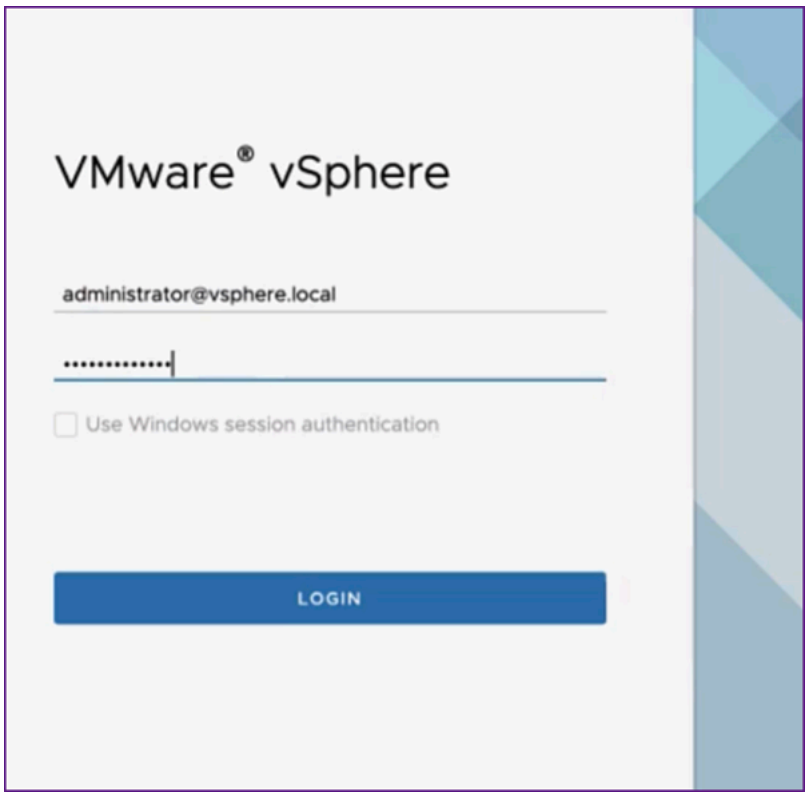
> 注意
>
> - 在注册和更改代理的默认密码之前，必须配置 NetScaler ADM 代理。
> - 如果您没有在.ovf 文件中注册和更改默认密码，则必须在部署 VM 后手动执行这些操作。



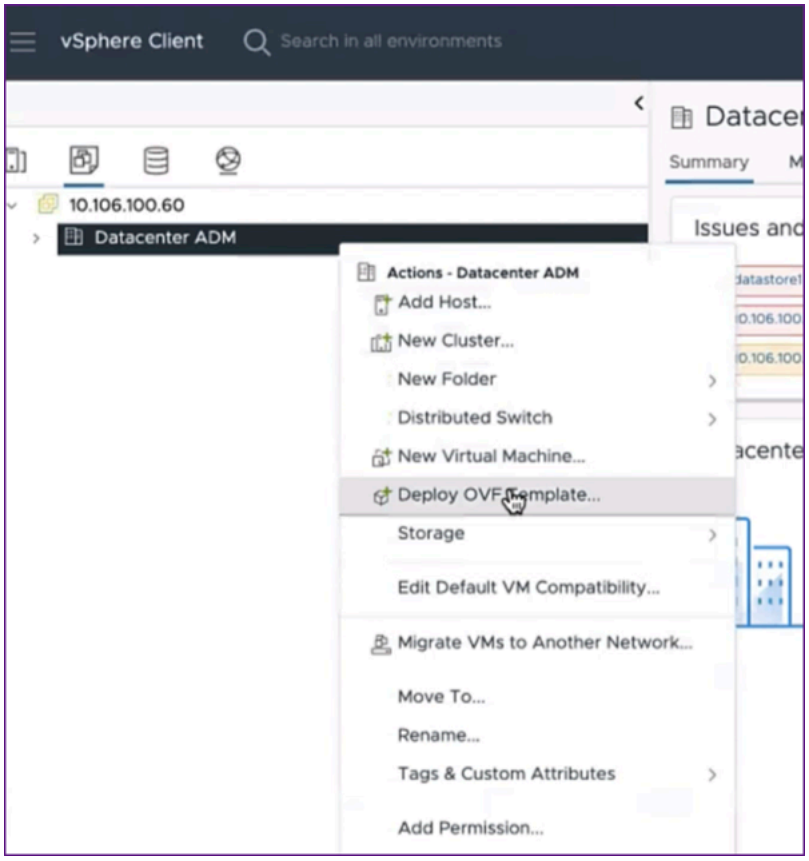
2. 添加参数及其值后，保存.ovf 文件。

在 **VMware ESXi** 上安装 **NetScaler ADM** 虚拟设备

1. 登录 **VMware vSphere** 客户端 并键入管理员凭据。单击“登录”。

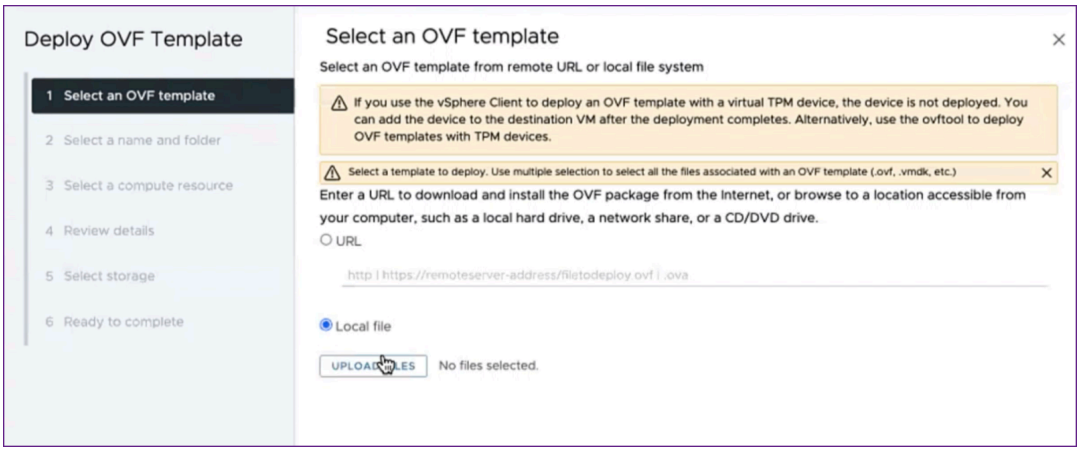


2. 选择您的 ESXi 服务器，然后右键单击选择“部署 **OVF** 模板”。

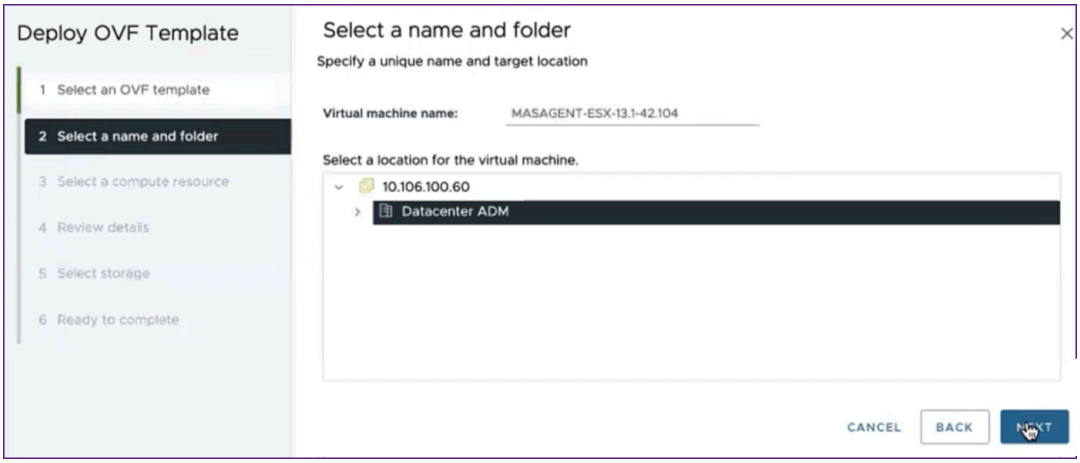


3. 在“部 署 **OVF** 模板”页面中：

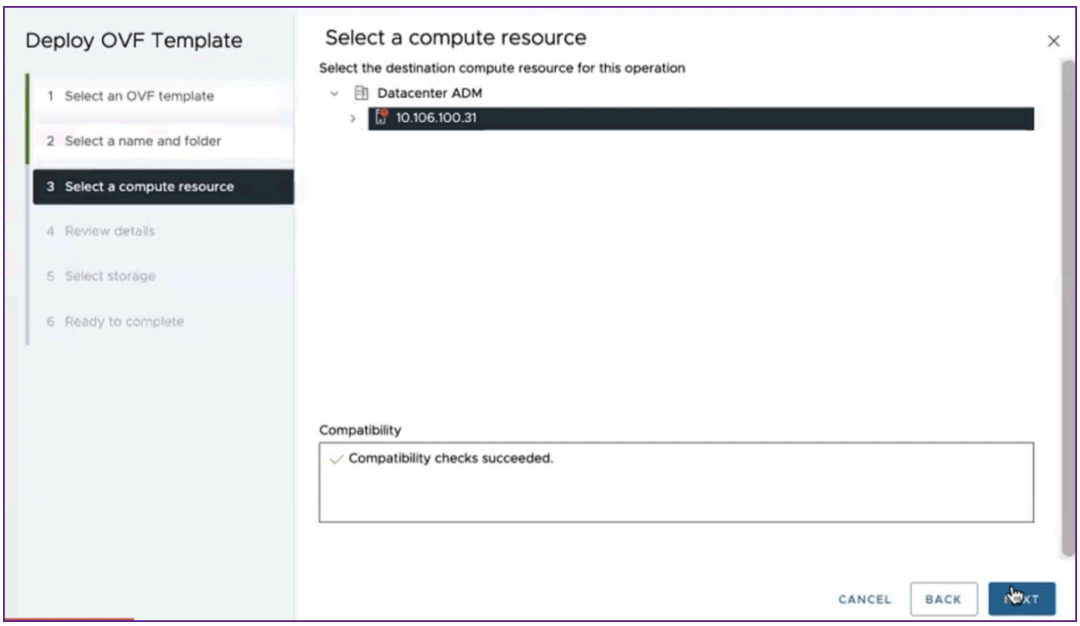
a) 选择 **OVF** 模板：选择 本地文件 并导航到您保存编辑过的.ovf 文件和.vmdk 文件的位置。选择文件并单击“打开”将其上载。单击下一步。



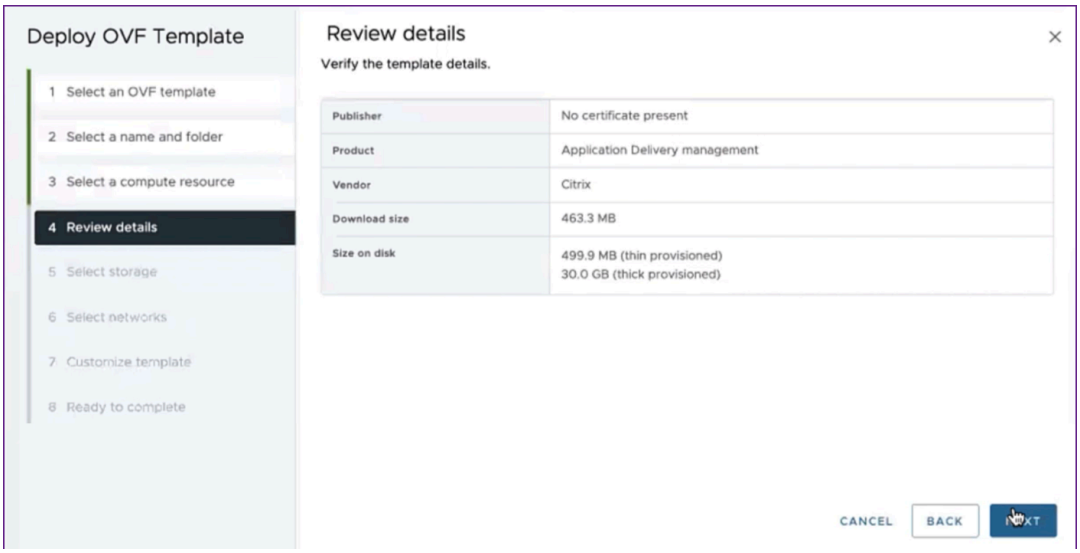
b) 选择名称和文件夹：为虚拟设备添加名称，然后在 ESXi 上选择要部署虚拟机的位置。单击下一步。



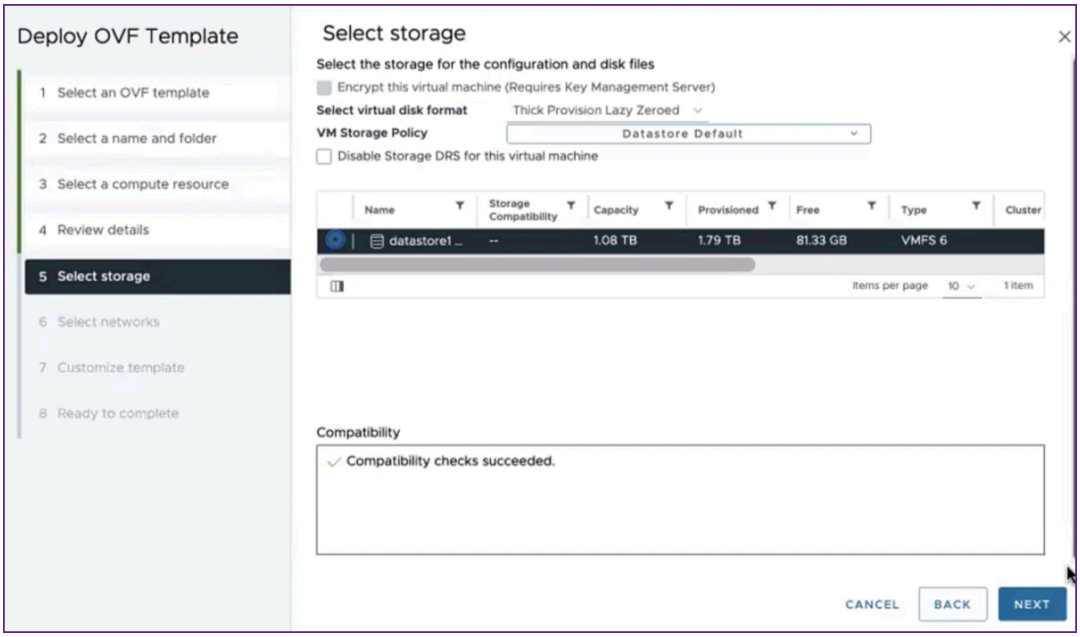
c) 选择计算资源：选择部署模板后要在其上运行的资源。单击下一步。



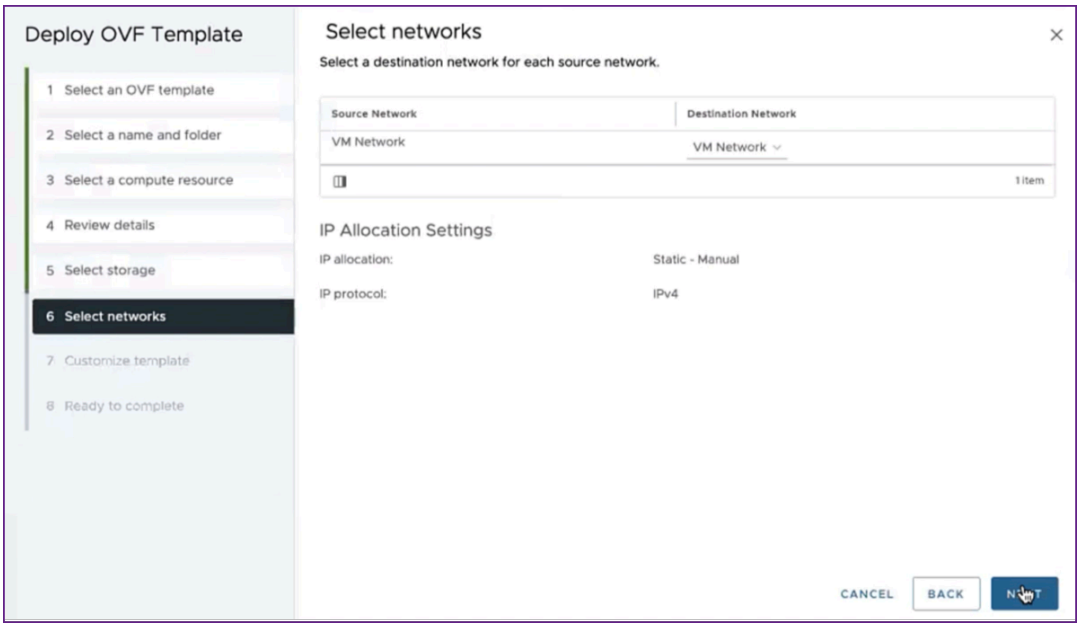
d) 查看详情：验证 OVF 模板的详细信息。单击下一步。



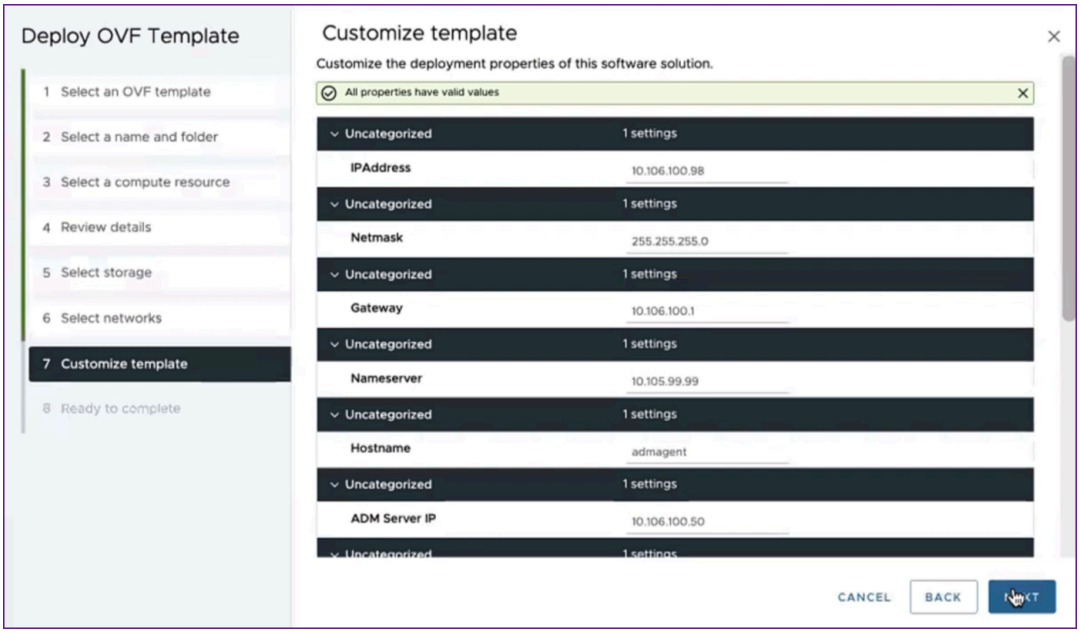
e) 选择存储：选择用于存储 OVF 模板的数据存储。单击下一步。



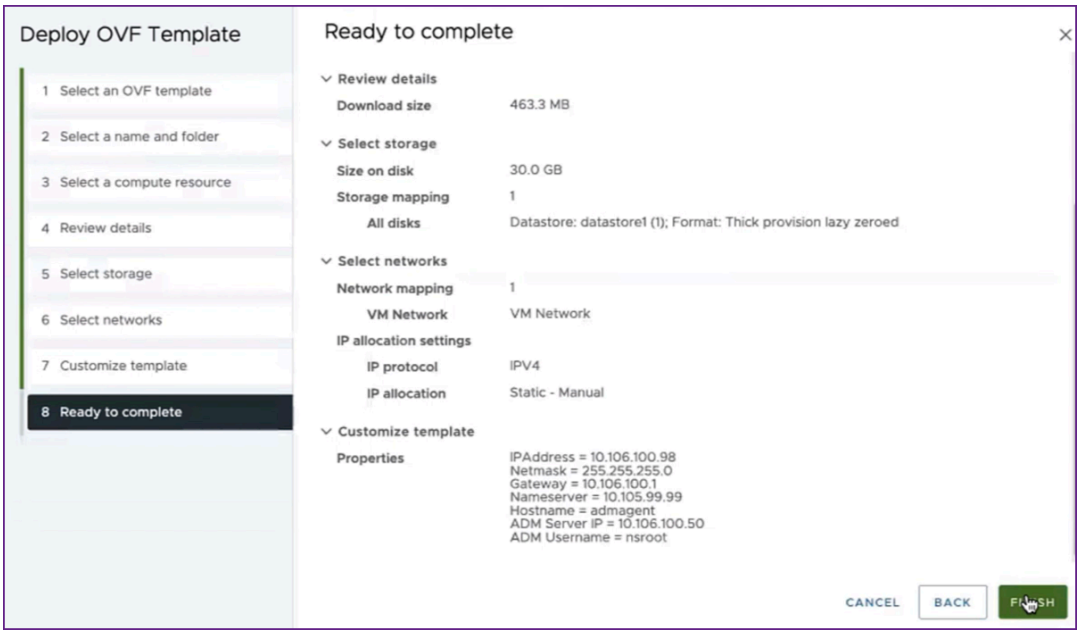
f) 选择网络：继续使用默认设置。单击下一步。



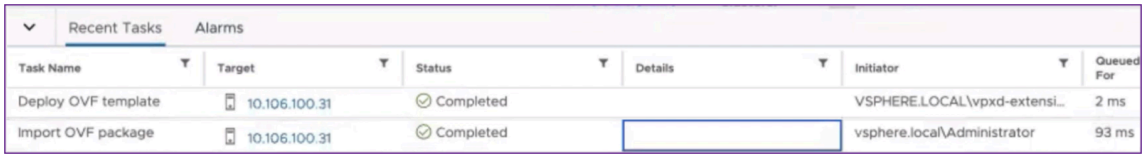
g) 自定义模板：查看 OVF 模板的所有属性。将显示您在 下载和编辑.OVF 文件部分的.ovf 文件中添加的所有参数和 值。



h) 准备完成：要保存设置并开始部署过程，请单击“完成”。

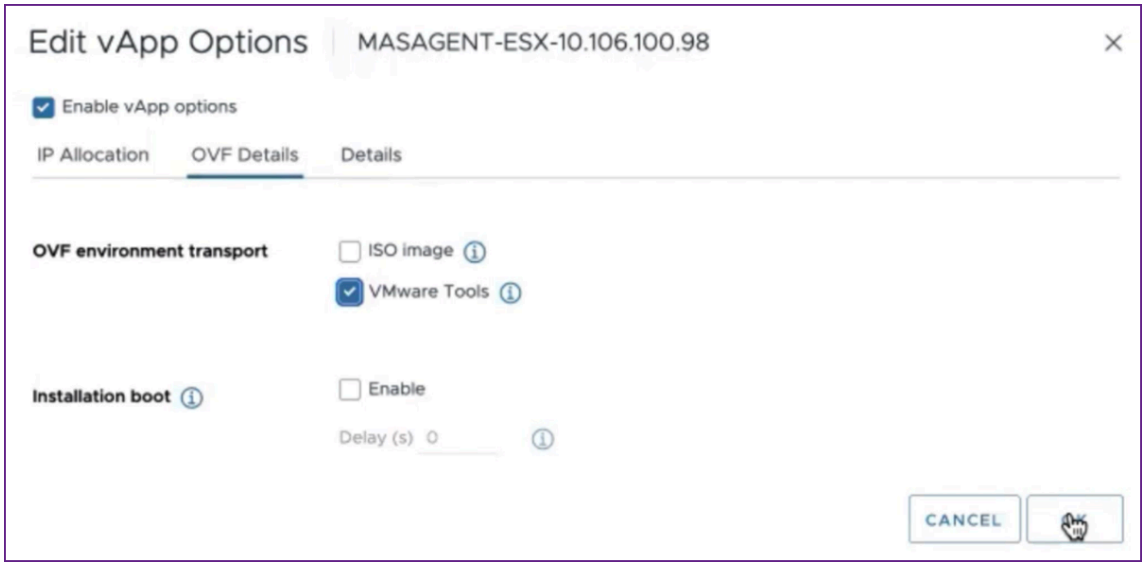


等待部署完成。部署 **OVF** 模板 操作的状态为 100% 完成后，您的代理即已部署。

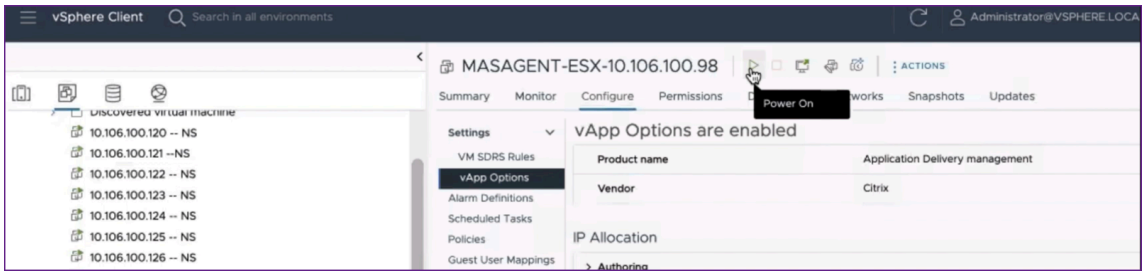


> 重要
>
> 在编辑设置之前，请勿打开虚拟设备的电源。

4. 单击您安装的新虚拟设备，然后导航到 配置 **>** 设置 **> vApp** 选项 **>** 编辑。
5. 在“编辑 **vApp** 选项”窗口中，导航到“在 **OVF** 详细信息”**>**“**OVF** 环境传输”中，然后选择 **VMware** 工具。单击确定。

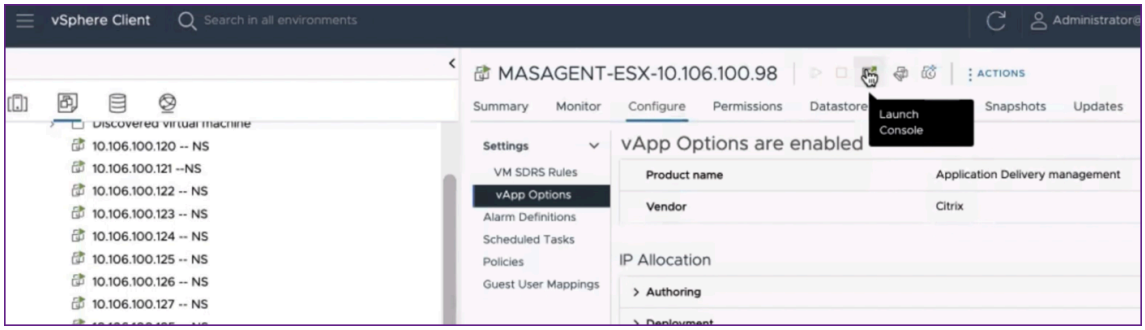


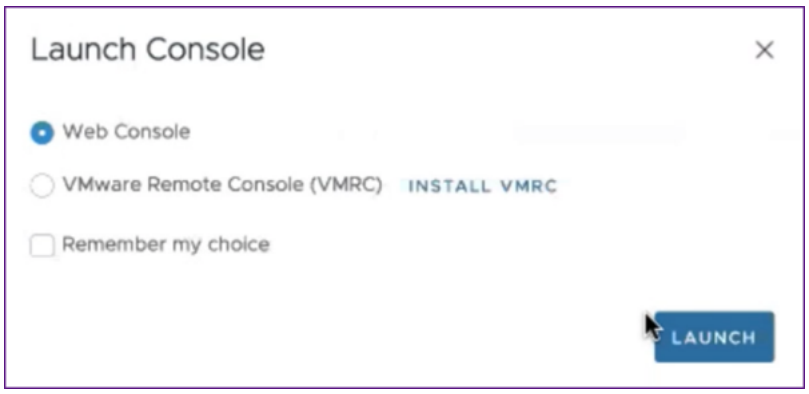
6. 右键单击虚拟机，然后单击“开机”。或者，您可以选择虚拟机的“摘要”选项卡，然后单击“开机”。



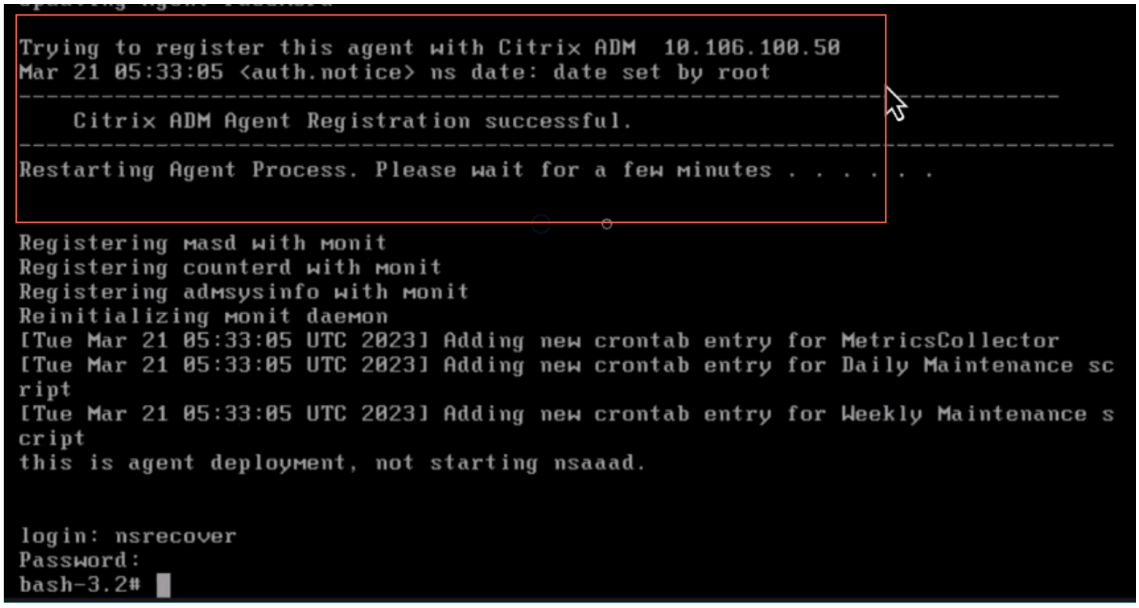
7. 在“摘要”选项卡中，选择“启动 **Web** 控制台”。

   在“启动控制台”窗口中，选择 **Web** 控制台。单击 **Launch**（启动）。





8. 在控制台中，将 NetScaler ADM 代理注册到 NetScaler ADM 服务器后，会显示一条成功的注册消息。要验证是否已部署 NetScaler ADM 代理以及默认密码是否已更改，请使用 NetScaler ADM 代理用户名和新密码登录。



验证

要验证是否已部署 NetScaler ADM 代理，请执行以下操作：

1. 部署 NetScaler ADM 代理后，通过在浏览器中键入 NetScaler ADM 服务器的 IP 地址来访问 NetScaler ADM GUI。
2. 使用您的凭据登录到服务器。
3. 导航到 基础结构 **>** 实例 **>** 代理。
   新部署的代理显示在 ESX 平台中。

Kubernetes 群集上的 NetScaler ADM

February 6, 2024

在 Kubernetes 群集上安装 NetScaler 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 群集必须是以下或更高版本：
  - 服务器版本 v1.20
  - 客户端版本 v1.20

  键入命令 `kubectl version` 以检查版本。
- 安装在群集上的 Helm 应用程序必须具有客户端版本 v3.4.0 或更高版本。

  使用 `helm version` 命令检查版本。
- Kubernetes 群集 CNI（容器网络接口）必须是印花语版本 v3.21.1 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 Ubuntu 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 股票

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 挂载。应用程序需要共享网络挂载中的两个文件夹：

- 一个用于存储文件，如证书、图像和其他文件
- 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。第一个文件夹的空间必须至少为 10 GB。第二个文件夹的大小取决于数据库中需要持久化的数据量。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。

NetScaler 设备

需要 NetScaler 设备作为入口设备。ADC 使所需的应用程序服务在 Kubernetes
群集之外可用。NetScaler 设备必须位于 Kubernetes 群集之外，并且必须可以从 ADC 访问工作节点。请执行以下步骤：

- 在 ADC 上配置一个 SNIP。ADC 使用这个 SNIP 来访问 Kubernetes 群集的工作节点。
- 确定一个可用的 IP 地址作为虚拟服务器 IP 地址，以便在 Kubernetes 群集之外提供所需的应用程序服务。

在库贝内特斯群集上安装 ADM

请按照以下步骤在 Kubernetes 群集上安装 ADM 设备：

1. 前往 NetScaler 网站 下载 Kubernetes 版 NetScaler ADM Helm Chart 的文件。
2. 将下载的 Helm Chart Tarball 提取到 Kubernetes 群集主节点的 /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 NetScaler 装置，以便将服务暴露于外部世界：
    - `ingressIP`：在 NetScaler 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 NetScaler 设备上的其余配置区分开来的唯一 ID。
    - `ingressADCIP`：NetScaler IP 地址 (NSIP)，用作 ADM 应用程序的入口。
    - `ingressADCUsername`：用于访问 NetScaler 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、20Gi。

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 版本不支持这个 helm 命令。

   此命令还会在群集中安装所需的 pod。命名空间参数是可选的。如果没有提供命名空间，Helm 会在默认命名空间中安装 ADM。为便于管理，请在单独的命名空间下安装 ADM。

9. 打开浏览器，然后使用 `nsroot`/`nsroot` 作为凭据键入 `http://< virtual server IP address >` 并登录 ADM。对于安全访问类型 `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 pod 的资源，该服务可能需要 5 到 15 分钟才能启动。

Linux KVM 服务器上的 NetScaler ADM

February 6, 2024

可以配置 NetScaler Application Delivery Management (ADM) 的虚拟化平台包括 Linux-KVM。

在 Linux-KVM 上安装 NetScaler 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 NetScaler 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 NetScaler ADM 并将其配置为您的网络。

必备条件

在安装 NetScaler ADM 虚拟设备之前，请验证 Linux-KVM 3.6.11-4 及更高版本是否安装在满足最低要求的硬件上。

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，NetScaler 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 NetScaler 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在运行，指定的内存和硬盘要求适用于在 OpenStack 平台上部署 NetScaler 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　NetScaler 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 NetScaler ADM 和 Linux-KVM 可以通信。

下载 **NetScaler ADM** 安装文件

要从以下地址下载 NetScaler ADM 安装文件，请执行以下操作：www.citrix.com

1. 打开 Web 浏览器并在地址栏中键入 www.citrix.com。
2. 将鼠标悬停在“登录”选项上，然后单击“我的帐户”，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 **NetScaler Application Delivery Management**。
5. 在 **NetScaler Application Delivery Management** 页面上，选择版本。例如，选择 版本 **13.0**。
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**Build 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 **NetScaler 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 命令解压 NetScaler Application Delivery Management 映像文件。解压缩的包中包含以下组件：

      i. 指定 NetScaler 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-->
```



```
root@ubuntu:~/mas-build#
root@ubuntu:~/mas-build# tar xvfz MAS-KVM-11.1-50.10.tgz
MAS-KVM.xml
checksum.txt
MAS-KVM-11.1-50.10.qcow2
root@ubuntu:~/mas-build#
```

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-->
```

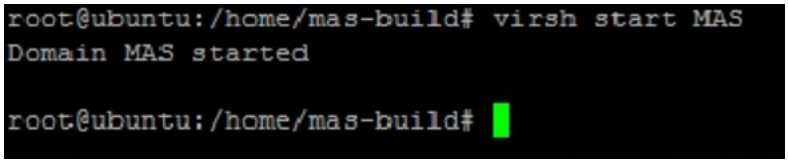
```
root@ubuntu:~/mas-build# virsh define MAS-KVM.xml
Domain MAS defined from MAS-KVM.xml

root@ubuntu:~/mas-build#
```

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

```
virsh start MAS
Domain MAS started
```

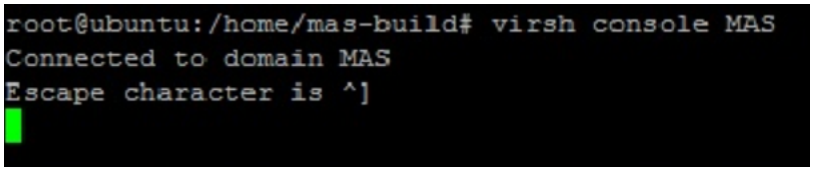


```
<!--NeedCopy-->
```



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

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



配置 NetScaler 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。当 NetScaler ADM 虚拟设备重启时，NetScaler ADM CLI 和 GUI 变得没有响应。有关详细信息，请参见https://bugs.launchpad.net/qemu/+bug/1329956
>
> 要避免 NetScaler ADM 虚拟设备重新启动时 NetScaler 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 NetScaler ADM 后，等待大约 10 分钟以使服务可用，然后登录 NetScaler 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 NetScaler ADM 用户界面更改密码。在 NetScaler ADM 主页上，导航到“设置”>“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 进入 NetScaler ADM 初始网络配置菜单。配置管理 IP 地址。
4. 要完成 NetScaler ADM 的初始网络配置，请按照提示进行操作。控制台显示 NetScaler ADM 的初始网络配置选项，用于为 NetScaler ADM 设置以下参数。默认情况下，已填充主机名。

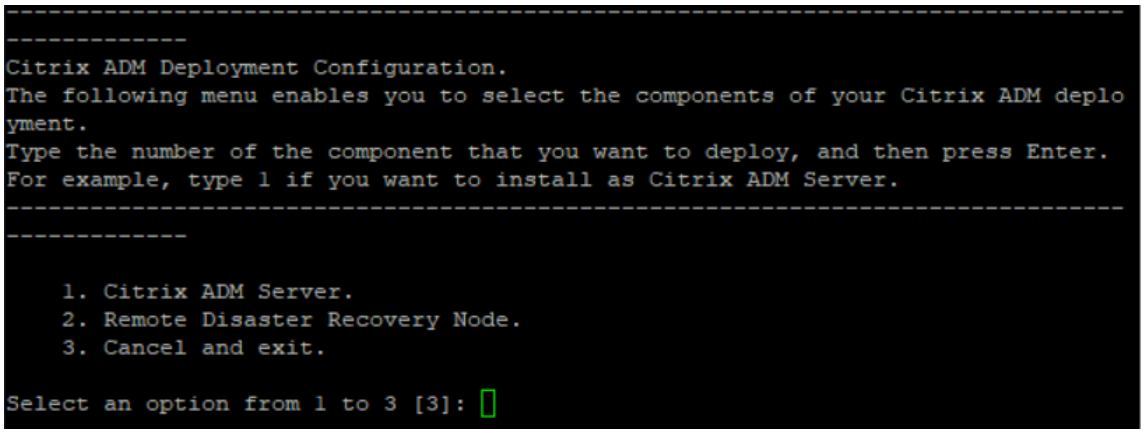
   a) 输入 **2** 更新 NetScaler ADM IPv4 地址——用于访问 NetScaler ADM 的管理 IP 地址

   b) 输入 **3** 更新网络掩码-与管理 IP 地址关联的子网掩码

   c) 输入 **4** 更新网关 IPv4 地址-NetScaler 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 **NetScaler ADM** 服务器的部署类型。



7. 键入“是”将 NetScaler ADM 部署为独立部署。
8. 键入“是”以重新启动 NetScaler ADM 服务器。

9. NetScaler ADM 服务器重启后，使用默认管理员凭据以 nsroot/nsroot 身份通过命令行或 GUI 登录 NetScaler ADM。

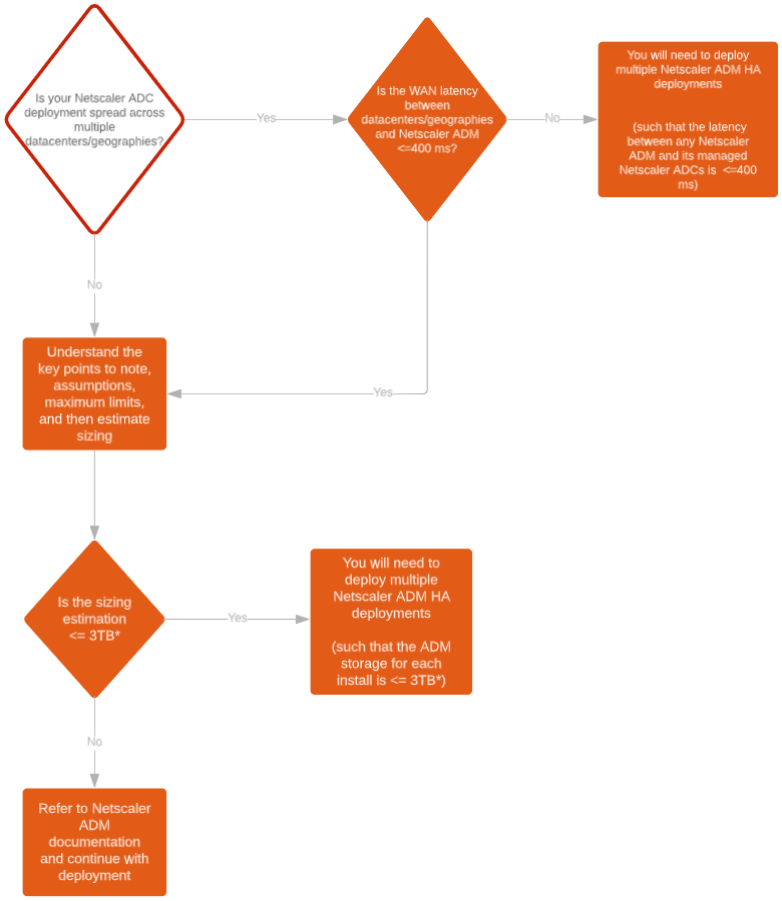
   稍后您可以通过在浏览器的地址栏中键入 NetScaler ADM 服务器的 IP 地址来访问 NetScaler ADM。登录服务器的默认管理员凭据是 *nsroot/nsroot*。

配置高可用性部署

February 6, 2024

高可用性 (HA) 是指在不中断服务的情况下始终可供用户使用的系统。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，是任何企业的关键要求。在主动-被动模式下以相同配置部署两个 NetScaler ADM 节点的高可用性可提供不间断的操作。

部署方案



> 注意
>
> 单个 NetScaler 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 **NetScaler ADM 12.1** 构建 **48.18** 或更高版本，请执行以下操作：
>
> 如果您已将 NetScaler 实例配置为在高可用性模式下对 NetScaler ADM 进行负载平衡，请先删除 NetScaler 实例。然后，配置浮动 IP 地址以在高可用性模式下访问 NetScaler ADM。

以下是在 NetScaler ADM 中部署高可用性的好处：

- 一种改进的监视主节点和辅助节点之间心跳的机制。
- 提供数据库的物理流式复制，而不是逻辑双向复制。
- 能够在主节点上配置浮动 IP 地址，无需单独的 NetScaler 负载平衡器。
- 使用浮动 IP 地址可轻松访问 NetScaler ADM 用户界面。
- 仅在主节点上提供 NetScaler 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，无需重新配置实例。
- 提供检测和处理脑分裂情况的内置能力。

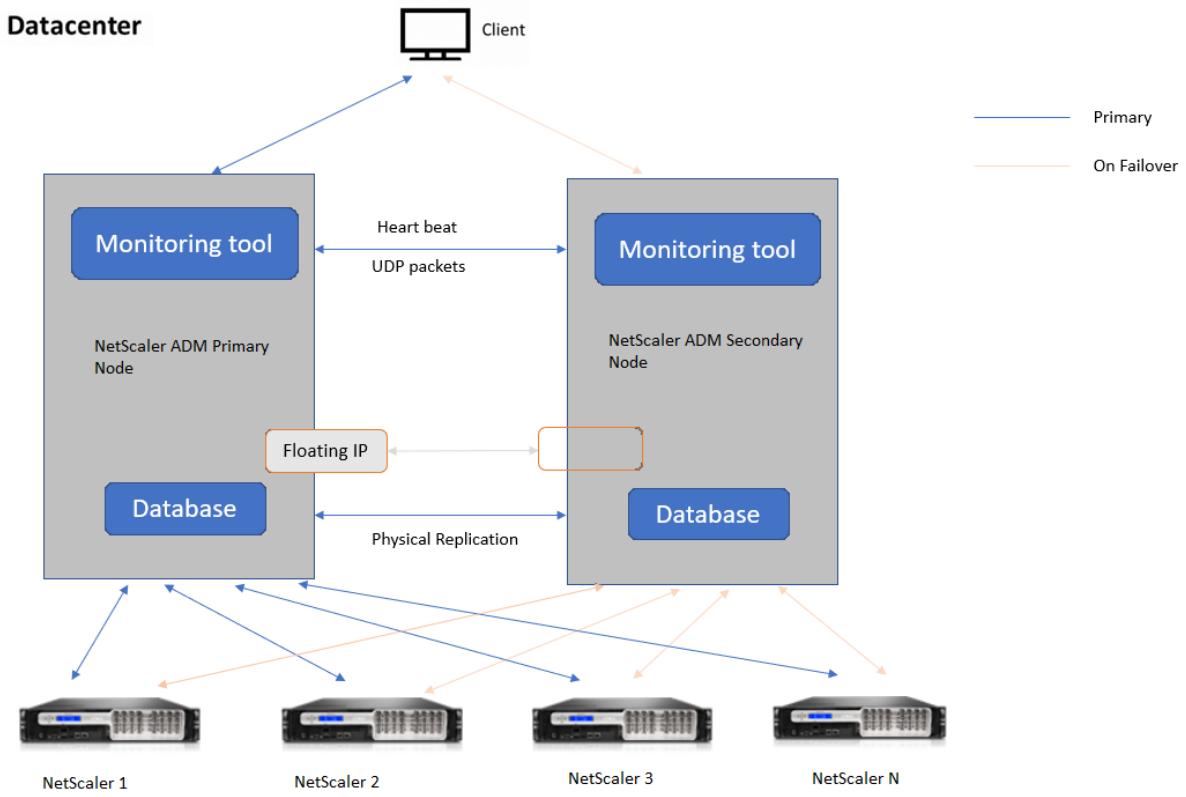
下表描述了高可用性部署中使用的术语。

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。
心跳	一种用于在高可用性设置中在主节点和辅助节点之间交换消息的机制。这些消息决定了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 是一种可以立即从同一子网中的一个节点移动到另一个节点的 IP 地址。在内部，它被设置为主节点网络接口上的别名。如果出现故障转移，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。

> 说明
>
> 有关端口和协议的详细信息，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 NetScaler ADM 节点的体系结构。



在高可用性部署中，一个 NetScaler 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。

监视工具

监视工具是一个内部进程，用于监视、发出警报和处理故障转移情况。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、决定是否存在故障转移是主节点还是辅助节点，等等。

主节点

主节点接受连接并管理实例。所有进程，例如 AppFlow、SNMP、LogStream、syslog 等，都由主节点管理。NetScaler ADM 用户界面可在主节点上访问。浮动 IP 地址是在主节点上配置的。

辅助节点

辅助节点监听从主节点发送的心跳消息。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 NetScaler ADM 用户界面。

物理流式复制

主节点和辅助节点通过心跳机制进行同步。通过数据库的物理流式复制，辅助节点以只读副本模式启动。辅助节点监听从主节点收到的心跳消息。如果辅助节点在 180 秒的时间段内未收到任何心跳信号，则认为主节点已关闭。然后，辅助节点接管主节点。

心跳消息

Heartbeat 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 NetScaler 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。如果出现故障转移或高可用性状态中断，则会将通知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。它是为主节点 IP 地址指定的别名，客户端可以使用它来连接主节点中的 NetScaler ADM。由于浮动 IP 地址是在主节点上配置的，因此在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 地址以访问新的主节点。

需要注意的要点

- 在高可用性设置中，两个 NetScaler ADM 节点均以主动-被动模式部署。它们必须位于相同的子网上，使用相同的软件版本和版本，并且具有相同的配置。
- 浮动 IP 地址：
  - 浮动 IP 地址是在主节点上配置的。
  - 如果存在故障转移，则无需重新配置实例。
  - 您可以使用主节点 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，所有配置文件会以一分钟的间隔自动从主节点同步到辅助节点。

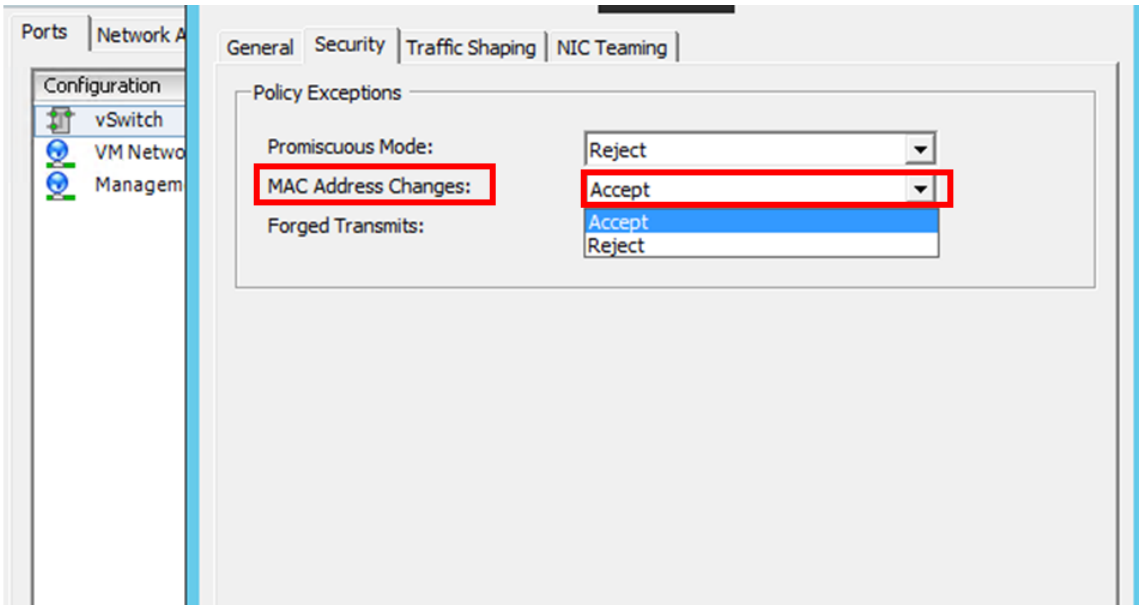
  - 数据库同步通过数据库的物理复制立即发生。
  - 辅助节点上的数据库处于只读副本模式。

- NetScaler ADM 升级：
  - 内部进程从早期版本隐式升级 NetScaler ADM。

    > 注意
    >
    > 升级成功后，必须配置浮动 IP 地址。

- UDP 默认端口 5005 在两个节点上都可用，用于发送心跳信号和接收消息。
- MAC 地址
  虚拟机管理程序中“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 上以高可用性部署 NetScaler 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
  >
  > 对于在 ESXI 版本 6.7 上部署的 NetScaler ADM，您也可以将 **MAC** 地址更改 选项设置为拒绝。故障转移后，无论 **MAC** 地址更改 设置如何，流量都会无缝流向新的主节点。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 NetScaler ADM，请确保将 **MAC** 地址更改 选项设置为仅 接受。



必备条件

在为 NetScaler ADM 节点设置高可用性之前，请注意以下先决条件：

- NetScaler ADM 版本 12.0 build 51.24 支持 NetScaler ADM 高可用性部署。
- 从 NetScaler 网站下载 NetScaler 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 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。默认值为 120 GB。实际存储需求取决于 NetScaler ADM 大小估计。如果您的 NetScaler ADM 存储要求超过 120 GB，则必须附加一块磁盘。注意 您只能添加一个额外的磁盘。Citrix 建议您在初始部署时估计存储量并附加额外的磁盘。有关更多信息，请参阅如何将其他磁盘连接到 NetScaler 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	Ubuntu 和 Fedora

在高可用性模式下设置 **NetScaler ADM**

1. 注册并部署第一台服务器（主节点）。
2. 注册并部署第二台服务器（辅助节点）。
3. 部署主节点和辅助节点以进行高可用性设置。

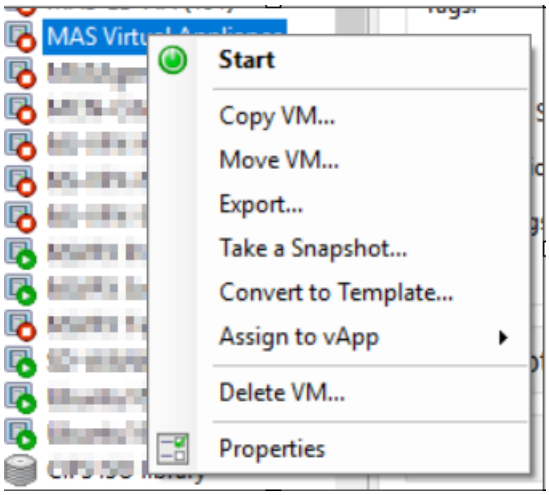
注册并部署第一台服务器（主节点）

要注册第一个节点，请执行以下操作：

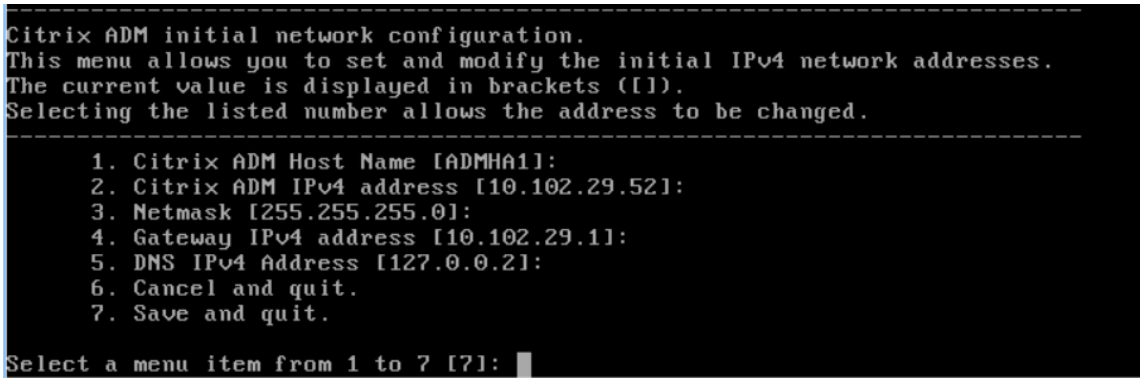
1. 使用从 NetScaler 站点下载的.xva 映像文件并将其导入到您的虚拟机管理程序。

> 注意
>
> .xva 图像文件可能需要几分钟才能导入并启动。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 NetScaler 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—*nsrecover/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 NetScaler ADM 部署配置菜单。


```
--------------------------------------------------------------------------------
------------
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]:
```

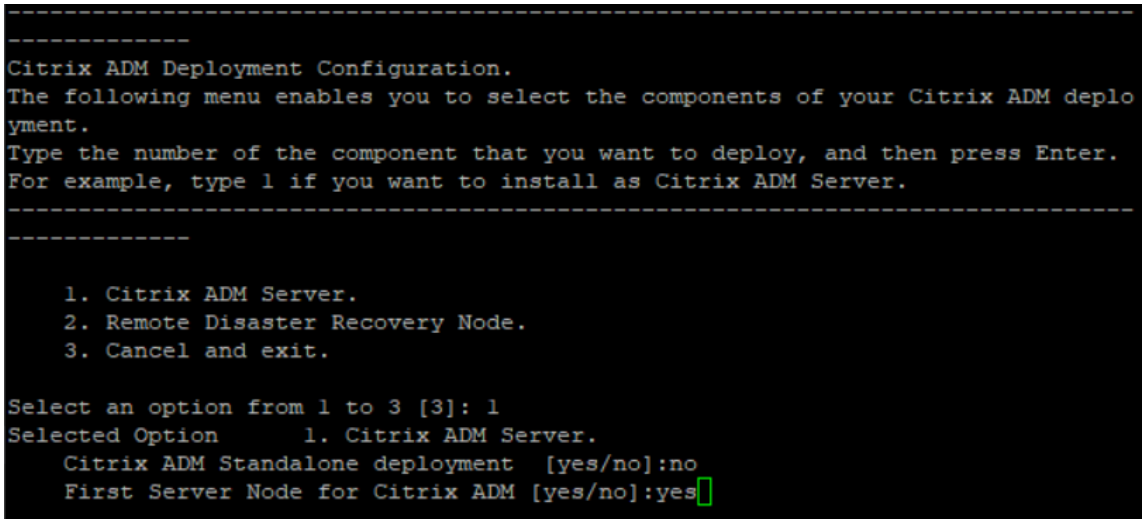
6. 选择 **1** 将 NetScaler ADM 服务器注册为主节点。

```
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]:
```

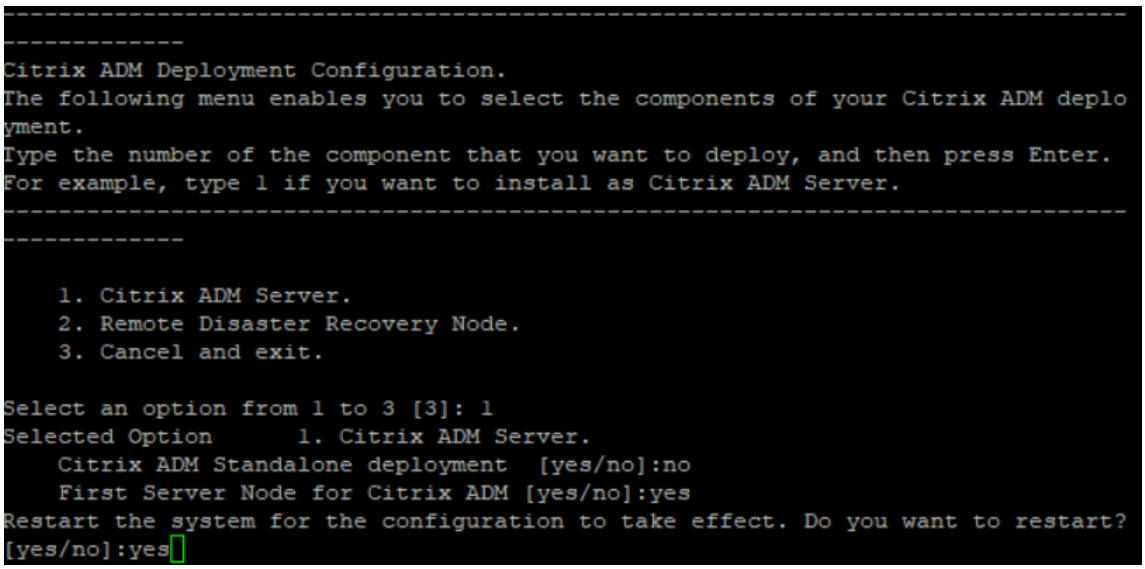
7. 控制台会提示您选择 NetScaler ADM 独立部署。输入否 以确认部署为高可用性。

```
--------------------------------------------------------------------------------
------------
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。



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 NetScaler ADM 用户界面中显示为主节点。

注册并部署第二台服务器（辅助节点）

1. 使用从 NetScaler 站点下载的 **.xva** 映像文件并将其导入到您的虚拟机管理程序。
2. 在 控制台 选项卡中，使用下图所示的初始网络配置配置 NetScaler ADM。
3. 完成初始网络配置后，系统会提示登录。使用以下凭据登录—*nsrecover/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 NetScaler ADM 部署配置菜单。

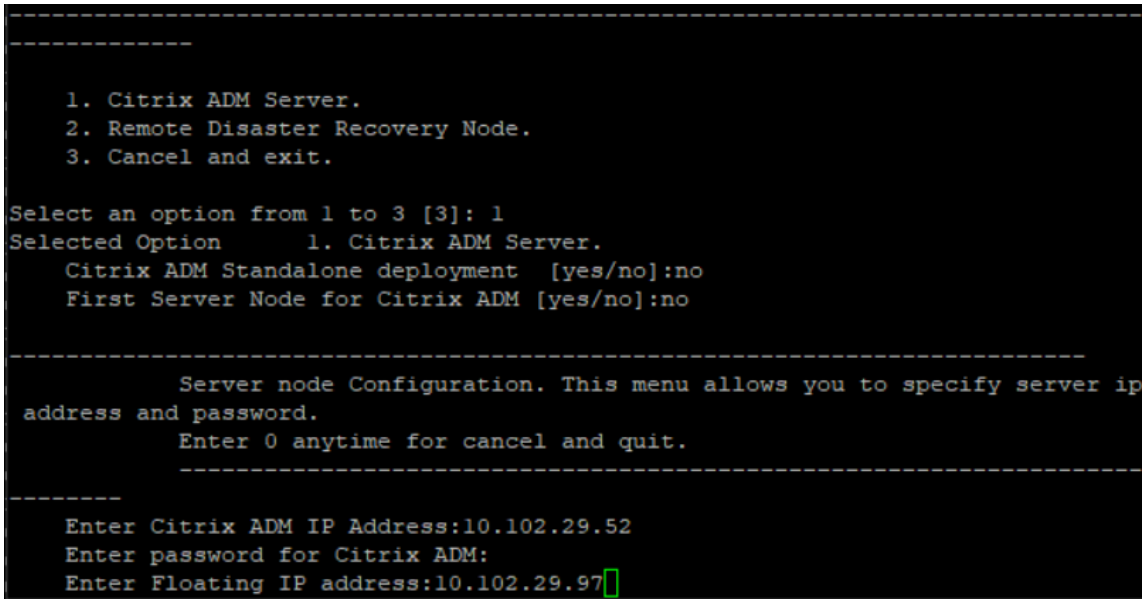
5. 选择 **1** 将 NetScaler ADM 服务器注册为辅助节点。
6. 控制台提示您选择 NetScaler ADM 作为独立部署。输入否 以确认部署为高可用性。
7. 控制台提示您选择第一个服务器节点。输入否 以确认节点为第二台服务器。

```
------------------------------------------------------------------------------
-------------
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
```

8. 控制台会提示您输入主节点的 IP 地址和密码。

```
------------------------------------------------------------------------------
-------------

    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

------------------------------------------------------------------------
            Server node Configuration. This menu allows you to specify server ip
 address and password.
            Enter 0 anytime for cancel and quit.
            ------------------------------------------------------------------
--------
    Enter Citrix ADM IP Address:10.102.29.52
    Enter password for Citrix ADM:
```

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 地址是节点高可用性部署的必备条件。
> - 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，需要几分钟才能使配置生效。

将主节点和辅助节点部署为高可用性对

注册后，主节点和辅助节点都显示在 NetScaler ADM 用户界面上。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之前，请确保在初始网络配置完成后重新启动辅助节点。
> - 高可用性部署完成后，使用浮动 IP 地址访问 NetScaler ADM 用户界面。

要将节点作为高可用性对部署，请执行以下操作：

1. 打开 Web 浏览器，输入第一个 NetScaler 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. 在主页中单击“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。

   NetScaler 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 NetScaler ADM，在主页中单击“入门”，然后根据需要完成以下操作：

   a) 添加 NetScaler 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“设置”**>**“部署”以验证部署。

   有关更多信息，请参阅 常见问题解答。

禁用高可用性功能

您可以在 NetScaler ADM 高可用性对上禁用高可用性并将节点转换为独立的 NetScaler 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. 在网络浏览器中，输入 NetScaler 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”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。有关更多详细信息，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

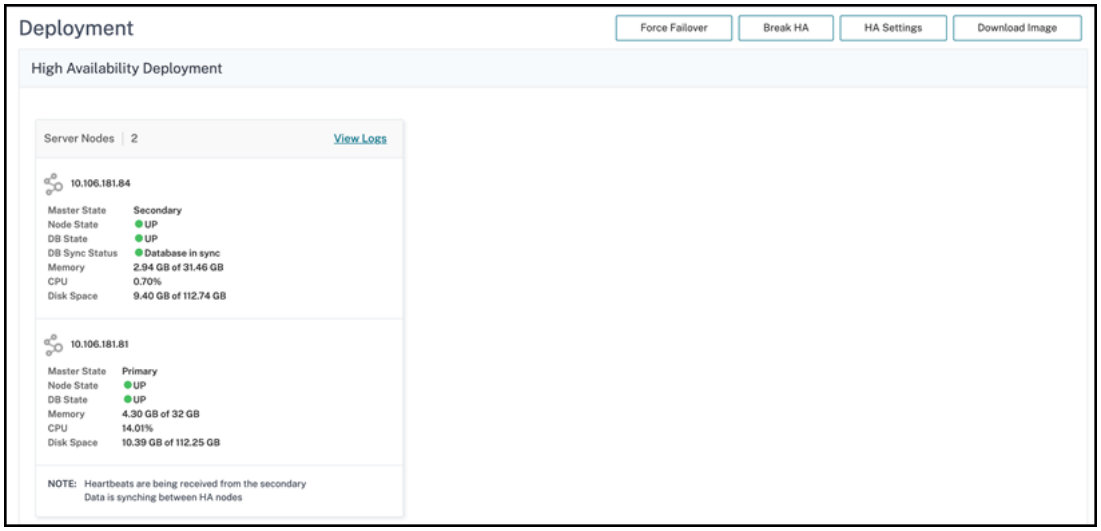
遇到下列情况之一时，会发生故障转移：

- 节点故障：主节点停机，180 秒内未检测到来自主节点的心跳。
- 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 NetScaler ADM 进程已关闭。

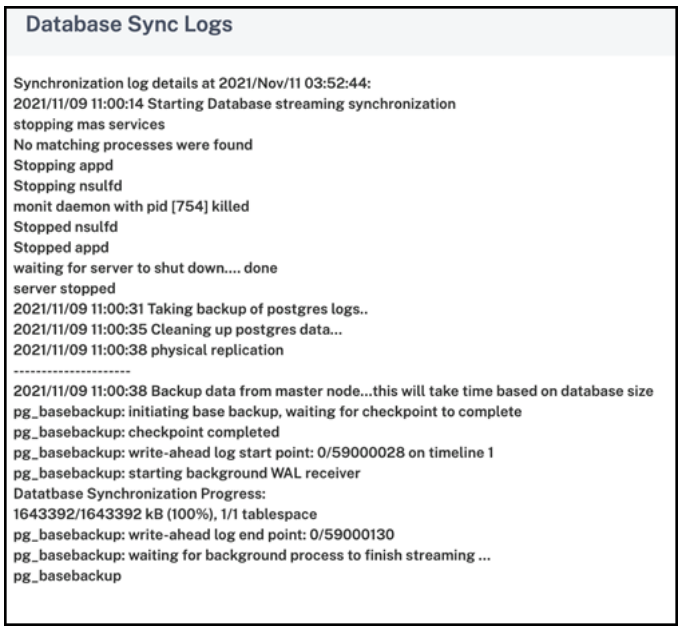
查看数据库同步日志消息

在 NetScaler ADM HA 对中，配置文件将自动从主节点同步到辅助节点，并进行数据库的物理流式复制。

但是，如果出现流式复制错误，则会显示“同步数据库”按钮。您可以单击 同步数据库 按钮以启动数据库同步过程。



要查看数据库同步的进度，请单击“查看日志”。此时将显示“数据库同步日志”消息，您可以实时查看同步进度的详细信息。



大脑分裂场景

当由于网络链路停机而导致两个节点之间没有通信时，那么：

- 主节点继续作为主节点运行
- 由于无法接收心跳，辅助节点取代主节点
- 这两个节点都将运行各自的数据库实例

例如，在企业中，已将两个 NetScaler ADM 节点部署为主节点和辅助节点。由于网络链路可能中断，两个 NetScaler ADM 节点之间的通信完全中断。由于在 180 秒内没有心跳交换，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。

从 NetScaler ADM 12.1 或更高版本开始，在网络链接和心跳恢复后，这种大脑分裂情况会得到妥善处理。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 split-brain 状态下，当新主节点以高可用性重新加入旧主节点时，在旧主节点上发生的更改将重置。分裂大脑期间在新主节点上发生的变化仍然完好无损。

配置灾难恢复以实现高可用性

February 6, 2024

灾害是由自然灾害或人为事件引起的业务功能突然中断。灾难会影响数据中心的运营，之后必须完全重建和恢复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。

NetScaler ADM 灾难恢复 (DR) 功能为在高可用性模式下部署的 NetScaler 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。

下表描述了在 NetScaler ADM 中配置灾难恢复时使用的术语。

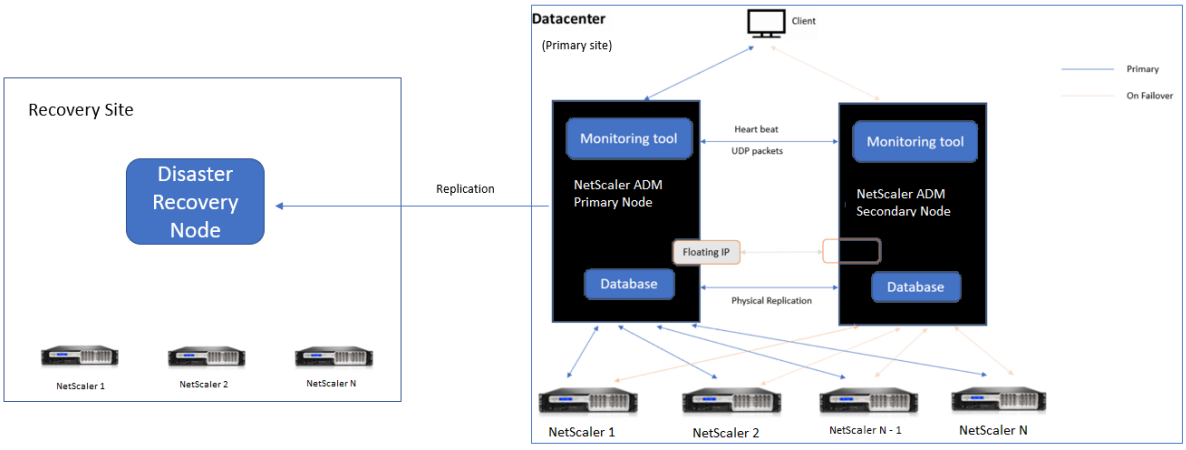
条款	说明
主站点（数据中心 A）	主站点以高可用性模式部署了 NetScaler ADM 节点。
恢复站点（数据中心 B）	恢复站点具有以独立模式部署的灾难恢复节点。此节点处于只读模式，在主站点关闭之前无法运行。
灾难恢复节点	恢复节点是部署在恢复站点中的独立节点。如果主站点发生灾难且该节点无法正常工作，则此节点将使该节点可以运行（对新的主节点）。

> 注意
>
> 主站点和灾难恢复站点通过端口 5454 和 22 相互通信，这些端口在默认情况下处于启用状态。
>
> 有关端口和协议的详细信息，请参阅 端口。

灾难恢复工作流程

下图显示了灾难恢复工作流程、灾难前的初始设置以及灾难发生后的工作流程。

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 NetScaler 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 NetScaler 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 NetScaler 实例，但它们没有任何流量流经它们。在备份过程中，所有数据、文件和配置都将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 NetScaler ADM 节点配置为高可用性模式。
- 在主站点上独立部署 NetScaler ADM 不支持灾难恢复功能。
- NetScaler ADM HA 对（在主站点中）和独立节点（在灾难恢复站点中）必须具有相同的软件版本、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 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。默认值为 120 GB。实际存储需求取决于 NetScaler ADM 大小估计。如果您的 NetScaler ADM 存储要求超过 120 GB，则必须额外附加磁盘。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。有关更多信息，请参阅 如何将其他磁盘附加到 NetScaler 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	Ubuntu 和 Fedora

首次灾难恢复设置

- 在高可用性模式下部署 NetScaler ADM
- 部署并注册 NetScaler 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 **NetScaler ADM**

要设置灾难恢复设置，请确保 NetScaler ADM 以高可用性模式部署。有关以高可用性方式部署 NetScaler ADM 的信息，请参阅高可用性部署

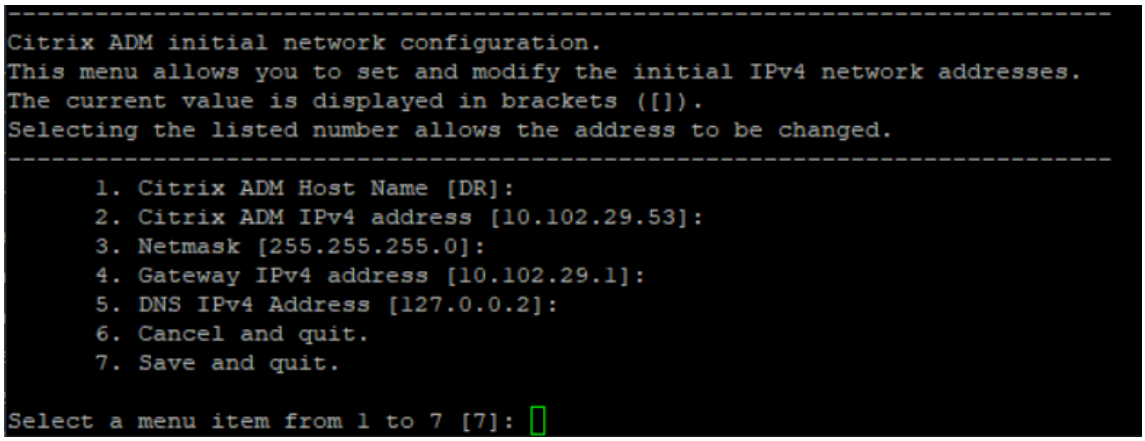
> 注意
>
> - 在高可用性模式下部署的 NetScaler ADM 必须升级到 NetScaler ADM 版本版本 13.1。
> - 向主节点注册灾难恢复节点时，必须使用浮动 **IP** 地址。

使用灾难恢复控制台部署和注册 **NetScaler ADM** 灾难恢复节点

要注册 NetScaler ADM 灾难恢复节点，请执行以下操作：

1. 从 NetScaler 站点下载 `.xva` 图像文件并将其导入到您的虚拟机管理程序中。
2. 在 控制台 选项卡中，使用初始网络配置配置 NetScaler 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
>
> 事项在注册期间不要更改 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 NetScaler 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。

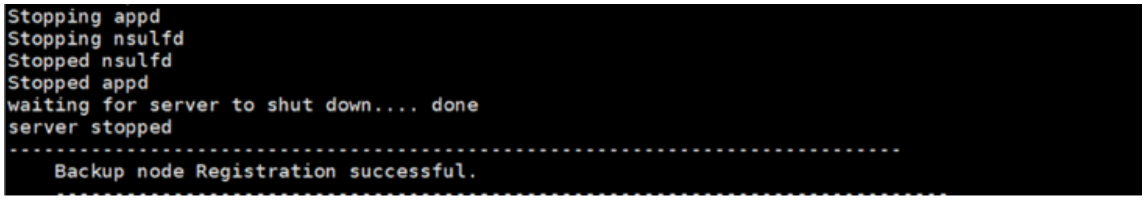
```
Citrix ADM Deployment Configuration.
The following menu enables you to select the components of your Citrix ADM deplo
yment.
Type the number of the component that you want to deploy, and then press Enter.
For example, type 1 if you want to install as Citrix ADM Server.
------------------------------------------------------------------------------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

    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。



> 注意
>
> - 灾难恢复节点没有 GUI。
> - 注册成功后，登录服务器的默认管理员凭据为 nsroot/nsroot。

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-->
```

示例：

```
/mps/change_freebsd_password.sh nsroot new_password
<!--NeedCopy-->
```

使用 **NetScaler ADM GUI** 部署灾难恢复节点

使用灾难恢复控制台成功注册灾难恢复节点后，从 NetScaler ADM GUI 部署灾难恢复节点。此步骤启用来自 NetScaler 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 页面上，选择 部署 **DR** 节点。
3. 将显示一个确认对话框。单击“是”继续。

> 注意
>
> 系统备份所花费的时间取决于数据大小和 WAN 链路速度。

在 NetScaler 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 部署中提供的过程配置 DR 节点，然后使用 DR 控制台注册 NetScaler ADM 灾难恢复节点。
3. 使用 NetScaler ADM GUI 部署灾难恢复节点。

有关更多信息，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

灾难发生后主站点出现故障时，必须按以下方式启动灾难恢复工作流程：

1. 管理员发现灾难袭击了主站点，该站点无法运行。
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：

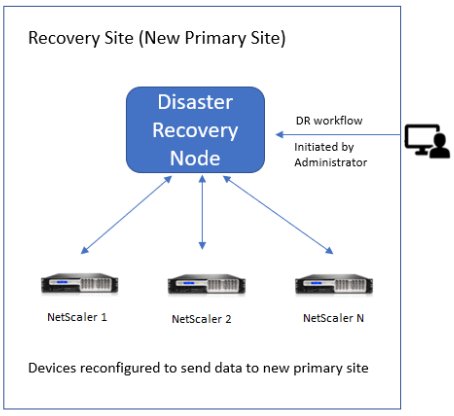
     ```
     /mps/scripts/pgsql/pgsql_restore_remote_backup.sh

     <!--NeedCopy-->
     ```

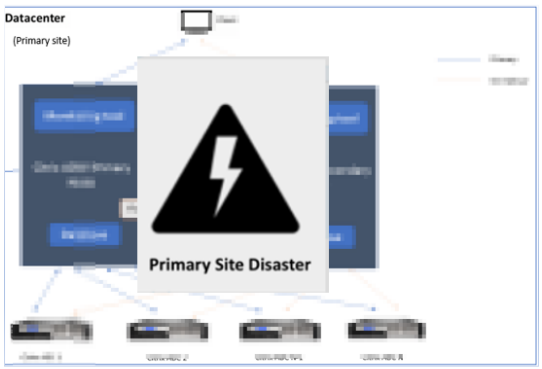
   - 还要将 DR 节点配置为许可证服务器：

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

     <!--NeedCopy-->
     ```

4. 在内部，NetScaler 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：
>
> 在灾难恢复站点启动脚本后，灾难恢复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

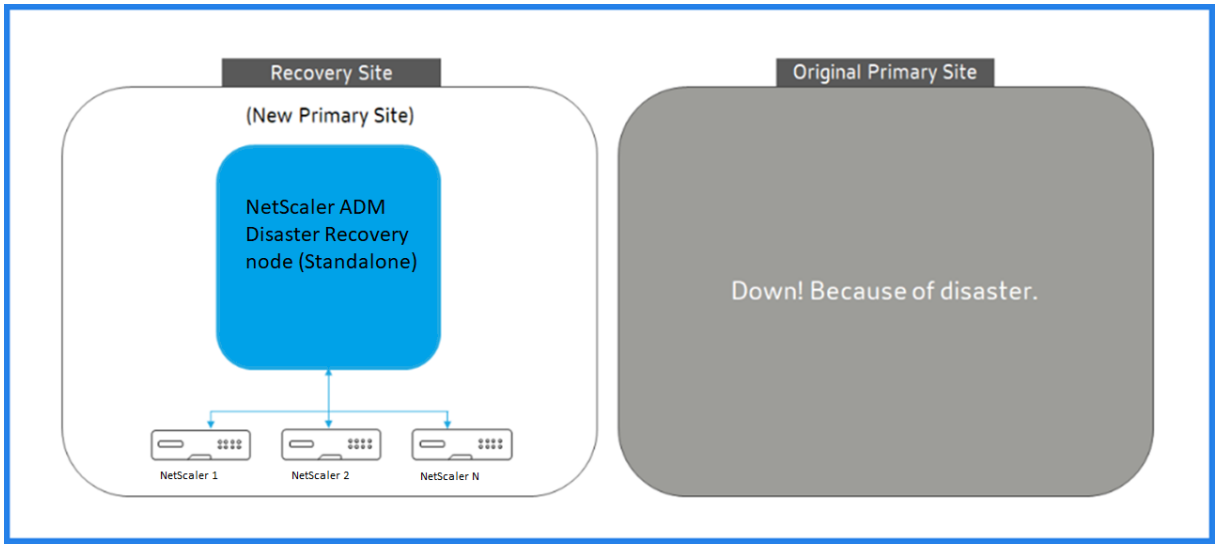
灾难发生并且管理员启动恢复脚本后，DR 站点现在成为新的主站点。

如果要稍后将配置还原为原始站点，请参阅 将配置还原为原始主站点。

> 重要
>
> - 如果您安装了 NetScaler ADM 12.1.49.x 或更早版本，则有 30 天的宽限期，可以联系 Citrix 在 NetScaler ADM（灾难恢复站点）上重新托管原始许可证。
> - 对于 12.1.50.x 或更高版本，NetScaler ADM 许可证会自动同步到灾难恢复站点（无需联系 Citrix 获取许可证）。
> - 如果您为实例申请了池化许可证，则版本为 **11.1 65.x** 或更高版本、**12.1 58.x** 或更高版本、**13.0 47.x** 或更高版本以及 NetScaler SDX **13.0 76.x** 或更高版本的 NetScaler 支持灾难恢复站点中的自动许可证服务器更新。所有其他版本，您必须手动将实例重新配置到灾难恢复站点。

将配置恢复到原始主站点

灾难发生后，配置的灾难恢复 (DR) 节点成为新的主站点，客户端流量流经此节点。



有关详细信息，请参阅 灾难发生后的工作流。

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。

开始之前，请确保主站点和灾难恢复站点都处于活动状态。

要将更改从灾难恢复站点恢复到原始主站点，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-->
```

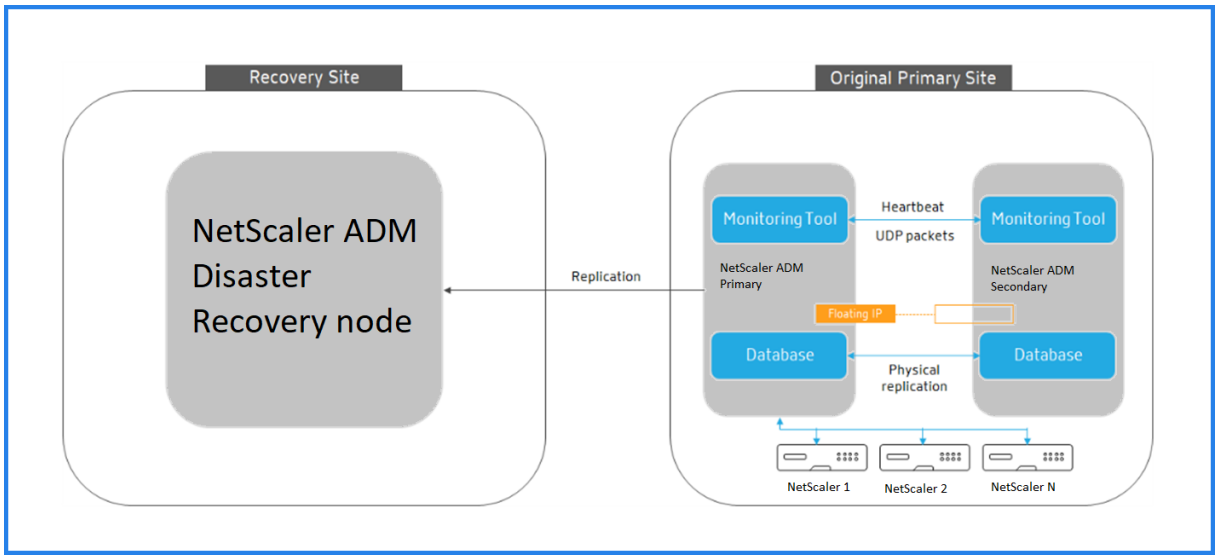
此命令仅为主站点配置 Syslog、SNMP 和分析。

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 NetScaler ADM 主节点进行流动。

为多站点部署配置本地代理

February 6, 2024

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

您可以将数据中心设在全球各地。代理在以下情形中起着至关重要的作用：

- 在远程数据中心安装代理，以减少 WAN 带宽消耗。
- 限制直接向主 NetScaler ADM 发送流量以进行数据处理的实例数量。

> 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 NetScaler 实例添加到主 NetScaler ADM。
> - 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，主站点与一个或多个远程数据中心之间的通信是通过浮动 IP 地址进行的。
> - NetScaler ADM 本地代理不支持共用许可。

在 NetScaler 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要 NetScaler ADM 进行通信。

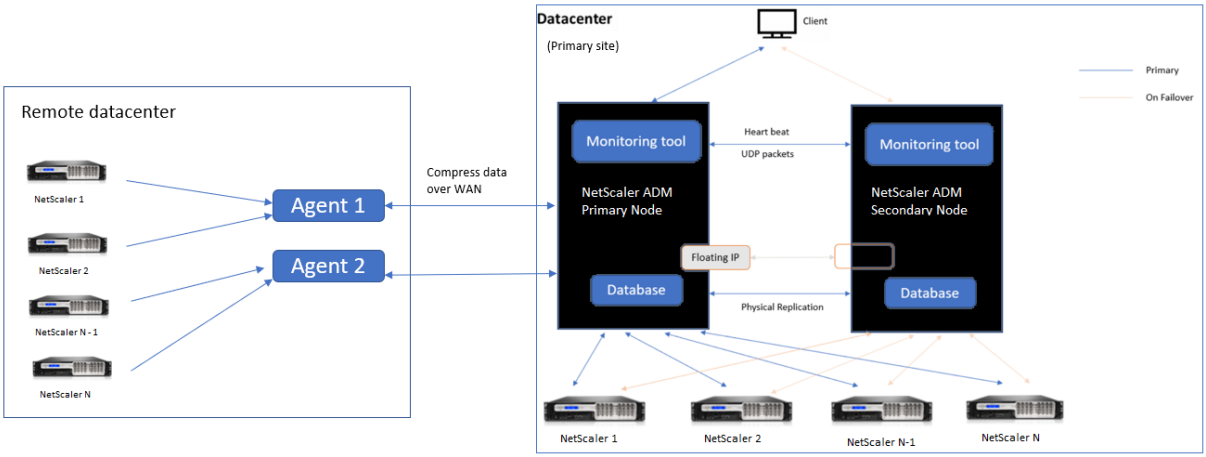
代理在不同数据中心的主 NetScaler ADM 和发现的实例之间起到中介作用。以下是安装代理的好处：

- 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 NetScaler ADM。代理执行第一级数据处理，然后将经过处理的数据以压缩格式发送到主 NetScaler 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 NetScaler 实例。当站点中的一个代理出现故障时，来自 NetScaler 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 NetScaler 实例以及使用基于多站点代理的体系结构的 NetScaler ADM 高可用性部署。



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

在辅助站点中，代理部署并向主站点中的 NetScaler 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连续的流量。辅助站点中的 NetScaler 实例通过位于该站点内的代理向主 NetScaler ADM 服务器注册。实例将数据直接发送到代理，而不是主 NetScaler 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 NetScaler ADM。代理通过安全通道与 NetScaler ADM 服务器通信，并压缩通过该通道发送的数据以提高带宽效率。

入门

- 在数据中心安装代理
  - 注册代理
  - 将代理附加到站点
- 添加 NetScaler 实例
  - 添加新实例
  - 更新现有实例

在数据中心安装代理

您可以安装和配置代理，以启用主 NetScaler ADM 与另一个数据中心中的托管 NetScaler 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
>
> 仅在 NetScaler ADM 高可用性部署中支持用于多站点部署的本地代理。

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 GB
虚拟网络接口	1
吞吐量	1 Gbps

端口

出于通信目的，代理和 NetScaler 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 NetScaler ADM 本地服务器之间的出站和入站通信。	NetScaler ADM 代理到 NetScaler ADM

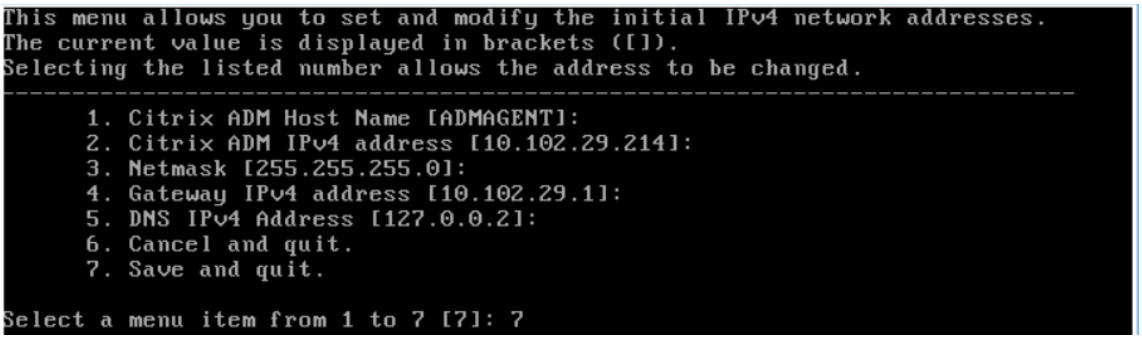
代理和 NetScaler 实例之间必须打开以下端口。

类型	端口	详细信息	通信方向
TCP	80	用于代理和 NetScaler 实例之间的 NITRO 通信。	NetScaler ADM 到 NetScaler 和从 NetScaler 到 NetScaler ADM
TCP	22	用于代理和 NetScaler 实例之间的 SSH 通信。用于以高可用性模式部署的 NetScaler ADM 服务器之间的同步。	NetScaler ADM 至 NetScaler，将 NetScaler ADM 代理转至 NetScaler
UDP	4739	用于代理和 NetScaler 实例之间的 AppFlow 通信。	NetScaler 到 NetScaler ADM

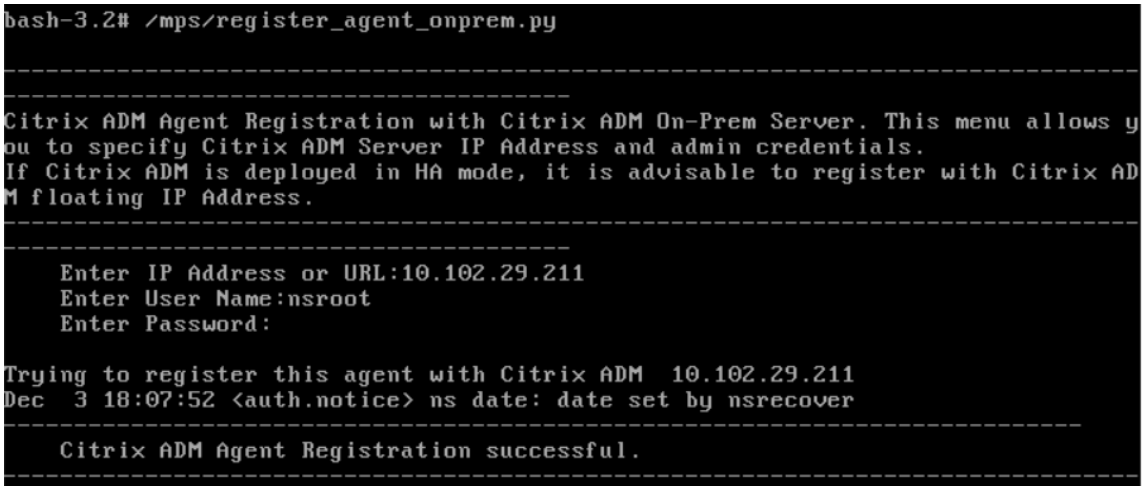
类型	端口	详细信息	通信方向
ICMP	无保留的端口	检测 NetScaler ADM 与 NetScaler 实例之间的网络可访问性，或者在高可用性模式下部署的辅助 NetScaler ADM 服务器之间的网络可访问性。	
UDP	161, 162	将 SNMP 事件从 NetScaler 实例接收到代理。	端口 161 -NetScaler ADM 到 NetScaler 端口 162 - NetScaler 到 NetScaler ADM
UDP	514	接收从 NetScaler 实例发送到代理的系统日志消息。	NetScaler 到 NetScaler ADM
TCP	5557	用于代理和 NetScaler 实例之间的 Logstream 通信。	NetScaler 到 NetScaler ADM

注册代理

1. 使用从 NetScaler 站点下载的代理映像文件并将其导入到您的虚拟机管理程序。代理映像文件的命名模式如下所示，即 **MASAGENT-<HYPERVISOR>-<Version.no>**。例如：**MASAGENT-XEN-13.0-xy.xva**
2. 在 控制台 选项卡中，使用初始网络配置配置 NetScaler ADM。
3. 输入 NetScaler ADM 主机名、IPv4 地址和网关 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**。将显示 NetScaler ADM 代理注册凭据，如下图所示。
6. 输入 NetScaler ADM 浮动 IP 地址和用户凭据。



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 NetScaler ADM GUI，从主菜单转到 基础架构 **>** 实例 **>** 代理 页面以验证代理的状态。新添加的代理将显示为“启动”状态。

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

将代理连接到站点

1. 选择代理，然后单击“连接站点”。
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将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 NetScaler 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 基础架构 **>** 客户端 **>** 选择操作下将各种操作应用于代理。

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您的安全要求，则可以添加一个。

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 NetScaler 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 技术支持部门进行调查和故障排除。

添加 **NetScaler** 实例

实例是您想要通过代理从 NetScaler ADM 发现、管理和监视的 NetScaler ADC 设备或虚拟设备。您可以将以下 NetScaler ADC 设备和虚拟设备添加到 NetScaler ADM 或代理中：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway
- Citrix SSL 转发代理

有关更多信息，请参阅 向 NetScaler ADM 添加实例。

将现有实例附加到代理

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

1. 导航到 基础架构 **>** 实例，然后选择实例类型。例如，NetScaler。
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 NetScaler ADM 中，导航到基础结构 **>** 实例。在“实例”下，选择要访问的实例类型（例如 NetScaler 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，代理被配置为实例上的陷阱目标。要进行确认，请登录实例的 GUI 并检查陷阱目的地。

> 重要
>
> 建议在远程数据中心为 NetScaler 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，请不要在添加实例时选择 代理。

NetScaler 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。当站点中的代理变为非活动状态（关闭状态）时，NetScaler ADM 会将非活动代理的 ADC 实例与其他活动代理重新分发。

> 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。

要在 ADM GUI 中将站点附加到代理，请参阅 将代理附加到站点。

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

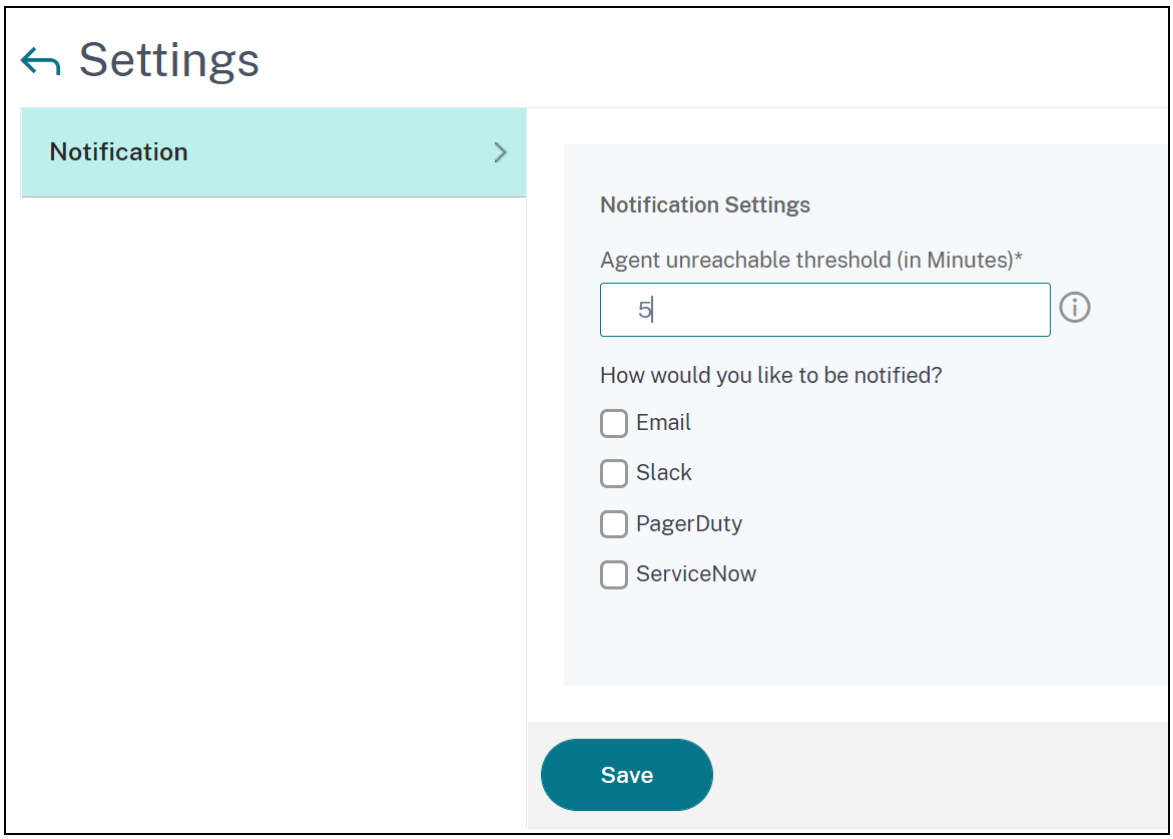
例如，两个代理 10.106.1xx.2x 和 10.106.1xx.3x 已连接并在班加罗尔站点中运行。如果一个代理处于非活动状态，NetScaler ADM 将检测到该代理并将状态显示为关闭。

当 NetScaler ADM 代理在站点中变为非活动状态（关闭状态）时，NetScaler ADM 将等待五分钟以使该代理变为活动状态（启动状态）。如果代理处于非活动状态，NetScaler 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。

NetScaler 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。

配置无法访问代理的阈值和通知

如果代理在一段时间内关闭或无法联系，您可以通过电子邮件、slack、PagerDuty 和 ServiceNow 获得有关座席状态的通知。在 基础架构 **>** 实例 **>** 代理中，单击 设置，指定 5 分钟到 60 分钟之间的持续时间，然后选择要接收通知的通知方法。



在 **Kubernetes** 群集上将 **ADM** 代理作为微服务安装

February 6, 2024

将 NetScaler ADM 代理部署为微服务对于管理 NetScaler CPX 非常有用。仅当 NetScaler 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 群集的微服务。

> 注意
>
> 您还可以配置 本地代理 ，并在托管 Kubernetes 群集的网络上注册代理。

入门

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 实例 **>** 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 群集中的代理定义服务并将此代理与同一群集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 **NetScaler ADM** 代理

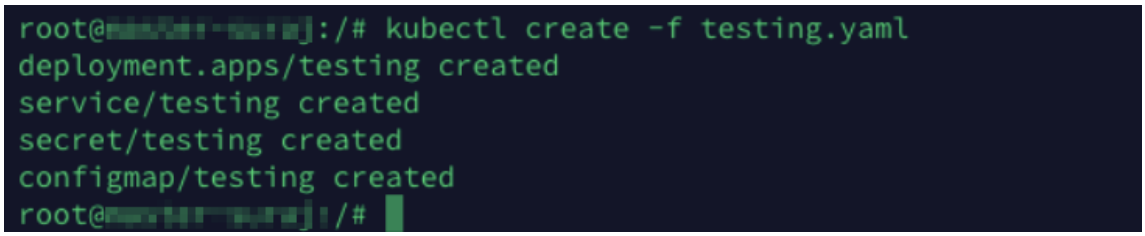
在 Kubernetes 主节点中：

1. 保存下载的 YAML 文件
2. 请运行以下命令：

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

   例如，`kubectl create -f testing.yaml`

   代理已成功创建。

在 NetScaler ADM 中，导航到 基础结构 **>** 实例 **>** 代理 以查看代理状态。

配置代理后，您可以添加 NetScaler CPX 实例并在服务图标中查看分析结果。有关详细信息，请参阅：

- 将 NetScaler CPX 实例添加到 NetScaler ADM 中。
- 设置服务图标。

将 **NetScaler ADM** 单服务器部署迁移到高可用性部署

February 6, 2024

您可以将 NetScaler ADM 单一服务器升级为由两台 NetScaler ADM 服务器组成的高可用性部署。一对高可用性 NetScaler ADM 服务器处于主动-被动模式，两台服务器的配置相同。在这种类型的主动-被动部署中，一台 NetScaler ADM 服务器被配置为主节点，另一台配置为辅助节点。如果出于任何原因主节点出现故障，则辅助节点接管。

要将 NetScaler ADM 单一服务器迁移到高可用性对，您需要预置一个新的 NetScaler ADM 服务器节点，将其配置为第二个 NetScaler ADM 单一服务器，并将两个 NetScaler ADM 服务器部署为高可用性对。

将 NetScaler ADM 单一服务器迁移到高可用性模式涉及以下步骤：

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

修改现有的 **NetScaler ADM** 服务器节点

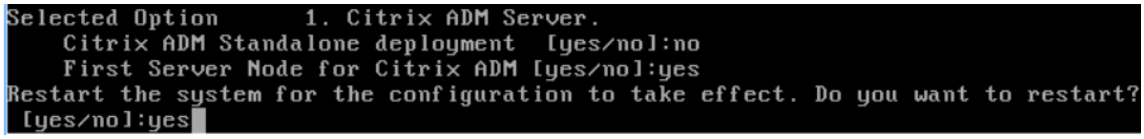
要将 NetScaler ADM 从单服务器迁移到高可用性模式，必须将服务器节点的初始部署类型更改为高可用性模式。

1. 在工作站或笔记本电脑上，打开现有 NetScaler 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 NetScaler ADM 部署为独立服务器。
2. 登录到 NetScaler ADM。默认凭据是 `nsroot` 和 `nsroot`。
3. 在 shell 提示符下，键入 `/mps/deployment_type.py`，然后按 **Enter** 键。
4. 将部署类型选择为 NetScaler ADM 服务器。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。

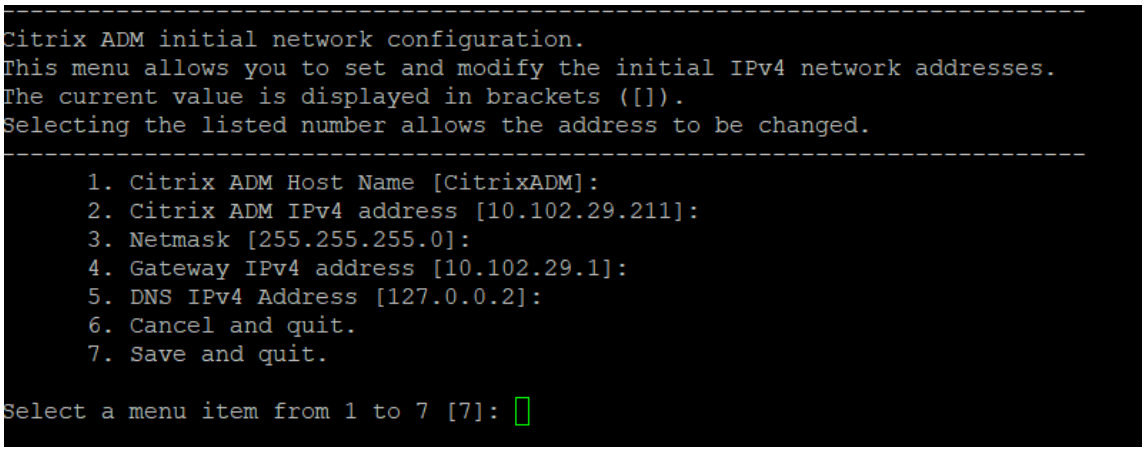
8. 键入 **Yes** 以重新启动。



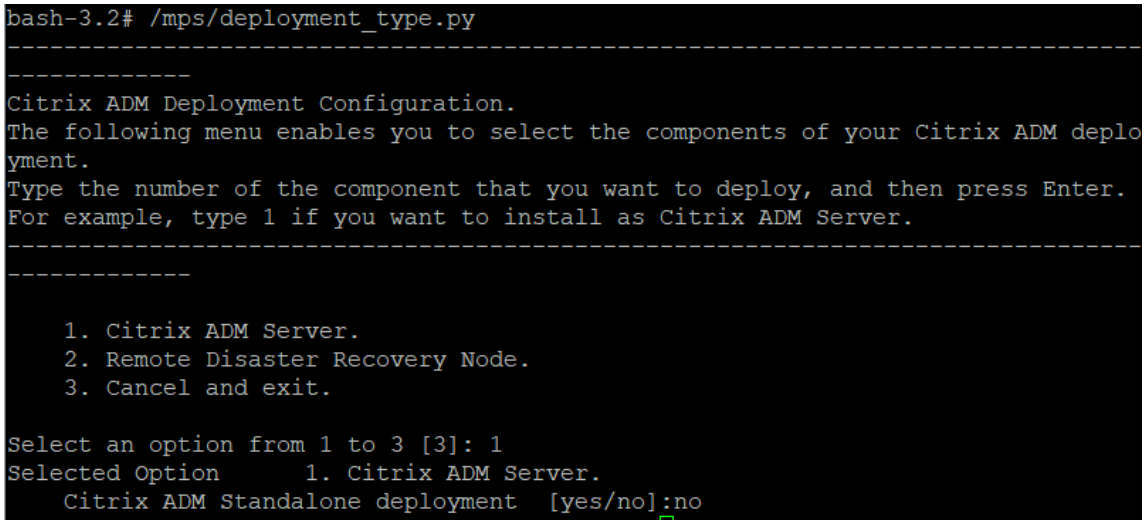
预配第二个服务器节点

必须在虚拟机管理程序上预配第二个服务器。使用与安装第一台服务器相同的映像文件，或从 NetScaler 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：

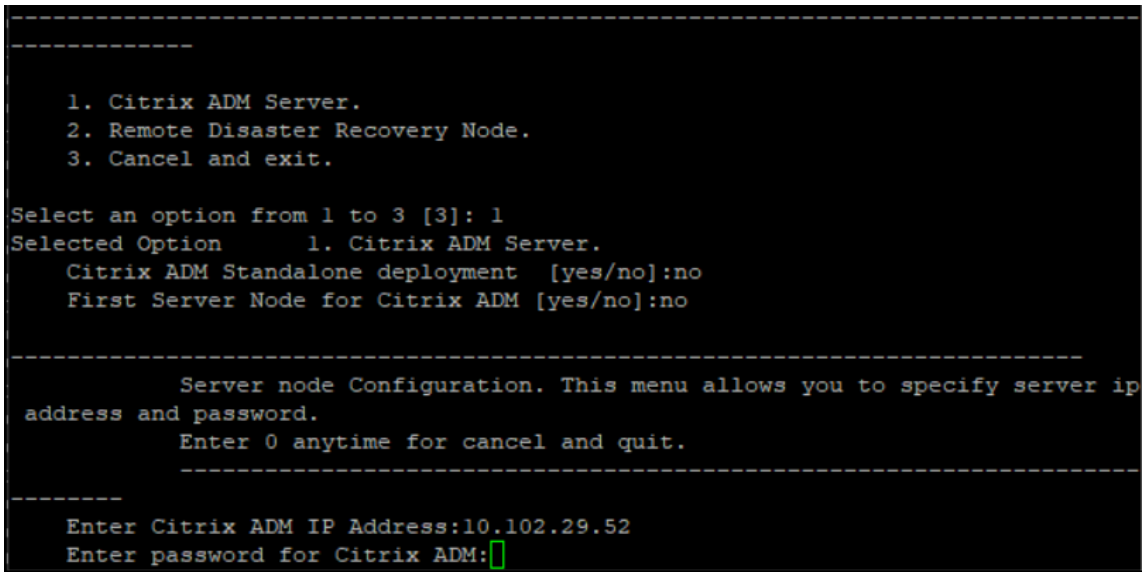


2. 指定所需的 IP 地址后，在 shell 提示符中键入 /mps/部署 _type.py，然后按 Enter 键。
3. 将部署类型选择为 **NetScaler ADM** 服务器。
4. 部署控制台提示您选择服务器部署（作为独立部署）。键入 **No** 以确认部署为高可用性对。

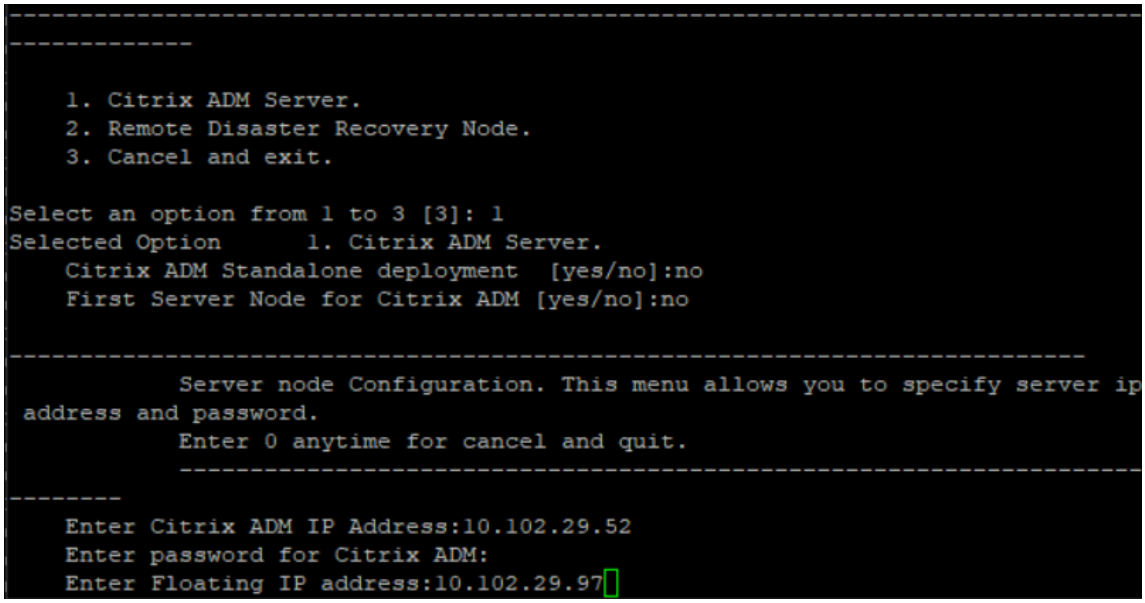


5. 控制台随后提示选择（第一个服务器节点）。键入 **No** 以确认该节点为第二个服务器节点。

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

要完成两个服务器节点作为高可用性对的安装过程，必须从先前存在的 NetScaler 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。

> 重要
>
> 信息：在部署高可用性节点之前，请确保更改默认密码。

1. 在 Web 浏览器中，键入先前存在的 NetScaler 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
   >
   > 在高可用性下部署 NetScaler 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. 尽管您在配置第二个服务器节点时输入了浮动 IP，但您可以在“系统”页面上选择更新 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 NetScaler ADM

February 6, 2024

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

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

必备条件

在将 NetScaler Insight Center 虚拟设备迁移到 NetScaler 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 NetScaler ADM 12.0 版本 57.24 .tgz 映像文件。

  > 注意：
  >
  > 您必须安装 NetScaler ADM 12.0 版本 57.24，然后升级到最新的 NetScaler ADM 13.1 版本。有关详细信息，请参阅升级。

- 您已下载了 NetScaler ADM 13.1 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 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps
虚拟机管理程序要求	

组件	要求
Citrix Hypervisor	6.2, 6.5
VMware ESX	5.5, 6.0
Microsoft Hyper-V	2012 R2
Linux - KVM	Ubuntu、Fedora

安装程序

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

1. 登录 NetScaler Insight Center 的 shell 提示符。
2. 将 NetScaler 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 NetScaler ADM 。**/**安装 **mas** 命令。

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

5. 安装 NetScaler ADM 12.0 build 57.24 后，您需要通过执行上述步骤升级到最新的 NetScaler ADM 13.1 内部版本。

迁移完成后，在 NetScaler Insight Center 清单中发现的所有 NetScaler 实例都将显示在 **NetScaler ADM** 的“基础架构”**>**“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
>
> 默认情况下，在 NetScaler ADM 中，管理和监视在发现的 NetScaler 实例中创建的两台虚拟服务器不产生许可成本。要监视和管理两个以上的虚拟服务器，请安装所需的 NetScaler ADM 许可证。有关更多详细信息，请参阅NetScaler ADM 许可。

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

February 6, 2024

Director 与 NetScaler ADM 集成，用于网络分析和性能管理。

- 网络分析从 NetScaler ADM 获取 HDX Insight 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 NetScaler ADM 与 Director 集成后，HDX Insight 报告会在 Director 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

从 **HDX Insight** 迁移到 **NetScaler ADM** 的硬件要求

组件	要求
RAM	32 GB
虚拟 CPU	8
存储空间	500 GB. Citrix 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。
虚拟网络接口	1
吞吐量	1 Gbps 或 100 Mbps

最低要求

在配置网络集成之前，请确保创建具有 HDX Insights 访问权限的 RBAC 用户。

软件要求

在迁移到 NetScaler 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 NetScaler ADM 支持 Citrix VDA 版本 7.0 及更高版本
- Citrix Virtual Apps and Desktops 7.0 版及更高版本支持 Citrix Workspace
- 确保适用于 Mac 的 MAC Citrix Workspace 版本 11.8 及更高版本和适用于 Windows 14.0 及更高版本的 Windows Citrix Workspace 可以显示准确的 ICA RTT 指标
- 安装了 NetScaler ADM 版本 11.0 及更高版本。有关如何安装 NetScaler ADM 的更多信息，请参阅 部署 NetScaler 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 会话往返时间 (RTT) 可以正确显示适用于 Windows 3.4 或更高版本的 Citrix Workspace 和适用于 Mac 11.8 或更高版本的 Citrix Workspace 的数据。对于这些工作区的早期版本，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 Director 的更多信息以及将 NetScaler ADM 与 Director 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 **NetScaler ADM**

February 6, 2024

NetScaler Application Delivery Management (ADM) 存储需求是根据您的 NetScaler ADM 规模估计值确定的。默认情况下，NetScaler 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 NetScaler ADM 时，估计存储需求并将额外的磁盘附加到服务器。

- 对于 NetScaler 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 NetScaler 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 建议使用固态硬盘 (SSD) 技术进行 NetScaler ADM 部署。

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

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

NetScaler ADM 磁盘分区工具

NetScaler ADM 现在提供了 **NetScaler 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

   - 不可能在不丢失数据的情况下调整现有磁盘的大小超过 2 TB。这是由于平台上的已知限制。
   - 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，您可以在磁盘上显式执行任何分区操作。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权。

> 注意：
>
> 您只能在已连接到 NetScaler ADM 服务器的其他磁盘上使用此工具。使用此工具无法在主（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（例如 PuTTY）打开与 NetScaler ADM 的 SSH 连接。
2. 使用 `nsrecover`/`nsroot` 凭据登录到 NetScaler ADM。
3. 切换到 shell 提示符并键入：

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

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

---------------------------------------
MAS/SVM Disk Partition Tool (DPT) 1.0
---------------------------------------
Welcome to MAS/SVM DPT! Type 'help' or '?' to view a list of commands.

(dpt):
```

> 注意
>
> 对于高可用性部署中的 NetScaler ADM，您必须在两个节点中启动该工具，然后在将磁盘附加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

每当添加新的辅助磁盘时，**create** 命令用于创建分区。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。在对磁盘进行分区时，会自动添加大小为 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
>
> - “调整大小”命令旨在在不丢失任何现有数据的情况下运行。但是 Citrix 建议您在尝试调整大小之前将此磁盘中的关键数据备份到外部存储。在调整大小操作期间磁盘数据可能损坏的情况下，数据备份非常有用。
> - 调整分区大小时，请确保以 100 GB 空间为增量增加磁盘空间。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 NetScaler ADM 子系统、PostgreSQL 数据库进程和 NetScaler ADM 监视器进程。进程停止后，将卸载磁盘，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全部可用空间，然后扩大文件系统来完成的。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。本文档的创建命令部分讨论了交换分区。

> 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，并注意不要在进程中中断该过程。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最多可以调整为 2 TB 的大小。这是由于分区存在已知限制。如果需要大于 2 TB 的磁盘，请使用磁盘分区工具连接新磁盘并对其进行分区。您还可以使用 remove 命令 删除 现有分区，然后创建一个分区。

> 注意：
>
> 移除现有分区将删除所有现有数据。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
>
> 移除分区后，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后，或者创建交换文件时，请重新启动虚拟机。这些更改只有在重新启动后才会生效。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
```

```
Rebooting VM now...

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

System going down IMMEDIATELY
```


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 NetScaler ADM 数据时应遵循的步骤。

> 注意：
>
> 创建备份文件需要磁盘空间。Citrix 建议您在运行备份命令之前确保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 /var/mps/mps_backup.tgz > /var/mps/mps_backup_checksum
<!--NeedCopy-->
```

6. 将 tarball 和校验和文件复制到远程服务器。
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 虚拟机中移除压缩包。

```
cd /var/mps/
rm mps_backup.tgz  mps_backup_checksum
<!--NeedCopy-->
```

其他命令

除了前面列出的命令外，您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。

```
(dpt): help

DPT Commands
------------
create  create_swapfile  exit  help  info  reboot  remove  resize

(dpt):
```

信息命令：

info 命令提供有关附加辅助磁盘的信息（如果该磁盘存在）。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的数量。该方案可以是 MBR 或 GPT。MBR 方案表示磁盘已使用早期版本的 NetScaler ADM 版本进行分区。基于 MBR/GPT 的分区可以调整大小，但不能超过 2 TB。GPT 分区方案意味着磁盘是使用 NetScaler ADM 12.1 或更高版本进行分区的。

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

```
(dpt): ?info
Provides information about attached disk (if found).
(dpt): info
--------------
Disk: da1
Scheme: MBR
Size: (150G)
Blocks: 314572737
--------------
(dpt):
```

创建交换文件命令：

NetScaler 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 NetScaler ADM 的默认内存配置（2 GB），此交换空间已足够。但是，使用更高内存配置运行 NetScaler ADM 时，需要在磁盘上分配更多的交换空间。

> 注意
>
> 交换分区通常是在操作系统安装过程中在硬盘驱动器 (HDD) 上创建的专用分区。这样的分区也称为交换空间。交换分区用于模拟额外主内存的虚拟内存。

默认情况下，在早期版本的 NetScaler 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 NetScaler ADM 版本创建的辅助磁盘。命令会检查以下内容：

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

“create_swapfile”命令仅在内存大于或等于 16 GB 时才有用，而在内存不足时不起作用。因此，此命令还会在继续创建交换文件之前检查内存。

```
(dpt): ?create_swapfile
Creates a 32GB swap file on the secondary disk. Pre-conditions are:
1. Secondary disk exists
2. Secondary disk is partitioned and mounted
3. Capacity of disk >= 500GB
4. Swap file is not already found
5. RAM size >= 16GB

Creating swapfile is a time consuming operation and can take ~5 minutes to complete. Once started the operation should n
ot be interrupted.
The VM will be automatically rebooted once the operation completes successfully for the changes to take effect.
```

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，请注意不要在创建过程中中断该过程。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。

```
CPU:  1.7% user,  0.0% nice,  0.8% system,  0.2% interrupt, 97.4% idle
Mem: 1847M Active, 506M Inact, 382M Wired, 4684K Cache, 199M Buf, 4473M Free
Swap: 4198M Total, 4198M Free
```

```
CPU: 42.0% user,  0.0% nice,  7.6% system,  5.0% interrupt, 45.3% idle
Mem: 1805M Active, 423M Inact, 393M Wired, 4792K Cache, 199M Buf, 4587M Free
Swap: 36G Total, 36G Free
```

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 **NetScaler ADM**

假设您在没有任何辅助磁盘的高可用性设置中配置了一对 NetScaler ADM 服务器。另外，请考虑您已添加 2 个或更多 NetScaler 实例，已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，您必须向两个节点添加其他磁盘，如以下任务中所述：

1. 关闭辅助节点。
2. 通过虚拟机管理程序添加额外的磁盘。

   > 注意
   >
   > 确保不要扩展辅助节点主磁盘。

3. 启动辅助节点。
4. 在辅助节点上运行分区工具。
5. 添加磁盘后，辅助节点将重新启动。
6. 在辅助节点重新启动后将其关闭。
7. 关闭主节点。
8. 通过虚拟机管理程序添加额外的磁盘。

   > 注意
   >
   > 确保不要扩展主节点主磁盘。

9. 启动主节点。
10. 在主节点上运行分区工具。
11. 添加磁盘后，主节点将重新启动。
12. 主节点启动并运行后，启动辅助节点。
13. 确保辅助节点已启动并正在运行，并且数据库已同步。
14. 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。不要重启节点。
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等地增加 RAM 大小。例如，如果将主节点上的 RAM 大小增加到 16 GB，也可以在辅助节点上执行相同的操作。

3. 重新启动 ADM_Primary。
4. 在 ADM_Primary 重新启动后，请检查它是否为主节点。

5. 现在启动 ADM_Secondary 节点。重新启动后，请确保它已作为辅助数据库启动，并且数据库同步工作正常。
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关闭一段时间。在规划此维护活动时，请考虑这种停机时间。

配置

February 6, 2024

只能使用 GUI 访问 NetScaler 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 NetScaler 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 **NetScaler ADM GUI**，请执行以下操作：

使用管理员凭据登录到 NetScaler ADM。

登录到 NetScaler ADM 后，您必须执行以下操作才能开始：

- 向NetScaler ADM 添加实例。如果要管理和监视这些实例，则必须将实例添加到 NetScaler 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NetScaler ADM 上配置 NTP 服务器。您必须在 NetScaler ADM 中配置网络时间协议 (NTP) 服务器才能将其时钟与 NTP 服务器同步。
- 配置系统设置以实现最佳 NetScaler ADM 性能。在开始使用 NetScaler 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 NetScaler ADM 服务器的最佳性能。

将实例添加到 **NetScaler ADM**

February 6, 2024

实例是您想要从 NetScaler ADM 发现、管理和监视的 NetScaler ADC 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 NetScaler ADM 服务器。您可以将以下 NetScaler ADC 设备和虚拟设备添加到 NetScaler ADM：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler BLX
- NetScaler Gateway

可以在第一次设置 NetScaler ADM 服务器时添加实例，也可在以后添加。然后，您必须指定 NetScaler ADM 可以用来访问该实例的实例配置文件。

> 注意
>
> - NetScaler ADM 使用 NetScaler 实例的 NetScaler IP (NSIP) 地址进行通信。有关 NetScaler 实例和 NetScaler ADM 之间必须打开的 端口的信息，请参阅端口。
> - 要了解 NetScaler ADM 如何发现实例，请参阅 发现实例。

如何创建 **NetScaler** 配置文件

NetScaler 配置文件包含要添加到 NetScaler 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 NetScaler 实例的默认配置文件。默认配置文件通过使用默认 NetScaler 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一个配置文件，然后重新发现实例。

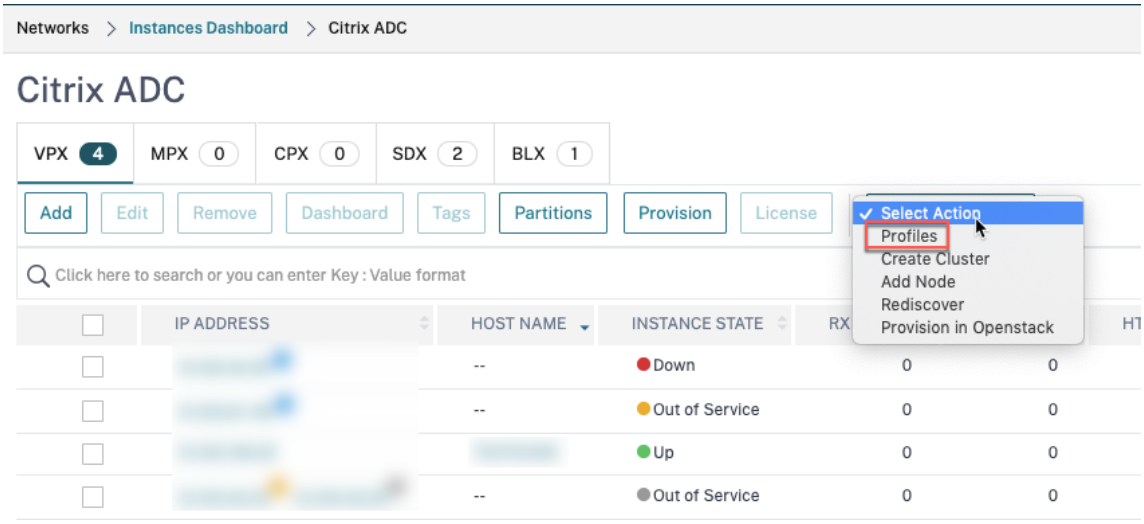
您可以从“实例”页面或在添加或更改实例 时创建 NetScaler 配置文件。

> 说明
>
> 请务必使用超级管理员帐户创建实例配置文件。

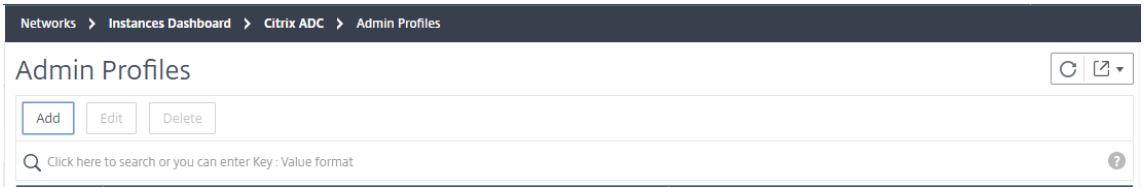
要从“实例”页创建 **NetScaler** 配置文件，请执行以下操作：

1. 导航到 **Infrastructure**（基础结构）**> Instances**（实例）。
2. 选择一个实例。例如，NetScaler。

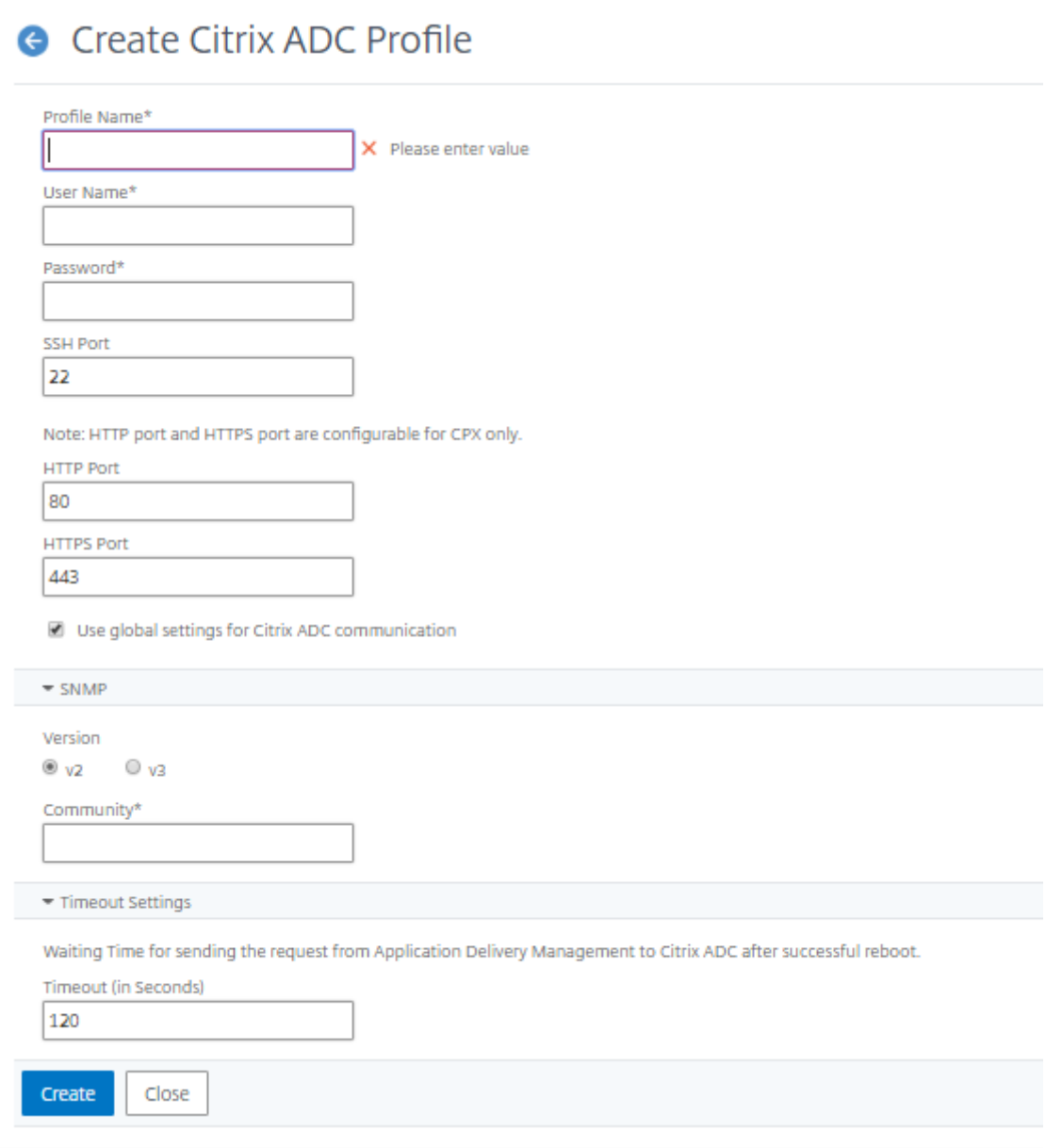
3. 在 NetScaler 页面上的 选择操作 下，选择 配置文件。



4. 在“管理员配置文件”页面上，选择“添加”。



5. 在创建 **NetScaler** 配置文件页面上，执行以下操作：



a) 配置文件名称：为 NetScaler 实例指定配置文件名称。

b) 用户名：指定登录到 NetScaler 实例的用户名。

c) 密码：指定登录到 NetScaler 实例的密码。

d) **SSH** 端口：指定 NetScaler ADM 与 NetScaler 实例之间的 SSH 通信端口。

e) **HTTP** 端口：指定 NetScaler ADM 与 NetScaler 实例之间的 HTTP 通信端口。

> 注意
>
> 默认 HTTP 端口是 80。您还可以指定可能在 NetScaler 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 NetScaler ADM 和 NetScaler CPX 之间的通信。

f) **HTTPS** 端口：指定 NetScaler ADM 与 NetScaler 实例之间的 HTTPS 通信端口。

> 注意
>
> 默认 HTTPS 端口是 443。您还可以指定可能在 NetScaler 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 NetScaler ADM 和 NetScaler CPX 之间的通信。

g) 使用 **NetScaler** 通信的全局设置：如果要使用系统设置进行 NetScaler ADM 和 NetScaler 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 NetScaler SDX，仅支持 **SNMPv2**。

i) 超时设置：指定 NetScaler ADM 在重新启动后向 NetScaler 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 **NetScaler ADM**

可以在第一次设置 NetScaler ADM 服务器时添加实例，也可在以后添加。

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

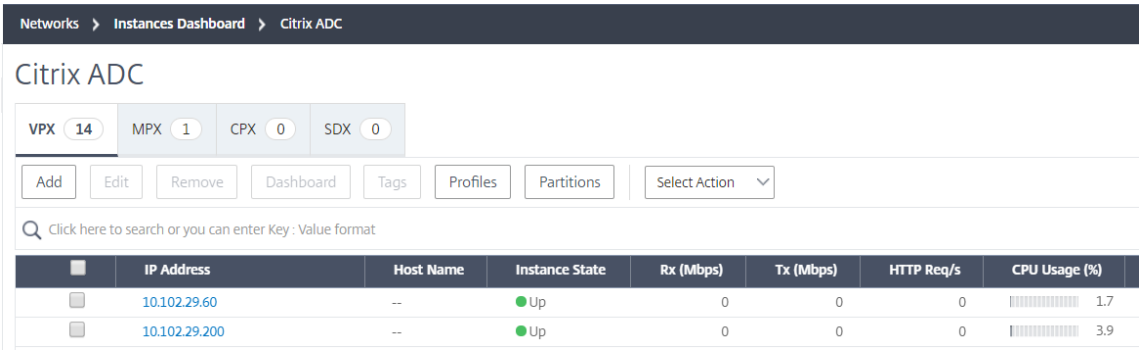
> 注意
>
> - 要添加在群集中配置的 NetScaler 实例，必须指定群集 IP 地址或群集设置中的任何一个单独节点。但是，在 NetScaler ADM 上，群集仅由群集 IP 地址表示。
> - 对于设置为 HA 对的 NetScaler 实例，添加一个实例时，将自动添加该对中的另一个实例。

如果将两台 NetScaler ADM 服务器设置为 高可用性模式，则在添加实例时，流量源将通过 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 **NetScaler ADM**，请执行以下操作：

1. 使用管理员凭据登录到 NetScaler ADM。
2. 导航到基础架构 **>** 实例 **> NetScaler**。选择要添加的实例类型（例如，NetScaler 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 NetScaler 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。并按以下格式指定 SNIP 地址：

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

     例如，`10.10.10.11#10.10.10.12`

   - **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 + 图标创建新的配置文件。
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”启动向 NetScaler ADM 添加实例的过程。

> 注意
>
> 如果要重新发现实例，请导航到 基础架构 **>** 实例 **> NetScaler**。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 **NetScaler CPX** 实例添加到 **NetScaler ADM**

NetScaler ADM 已得到增强，可为 CPX 功能中已完成的改进提供支持。NetScaler CPX 实例现已通过提供 CPX 的 IP 地址和设备配置文件添加到 NetScaler 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，NetScaler 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 基础架构 **>** 实例 **> NetScaler** ，然后单击 **CPX** 选项卡。
2. 单击 **Add**（添加）以在 NetScaler ADM 中添加新的 CPX 实例。
3. 此时将打开“添加 **NetScaler CPX**”页。为以下参数输入值：

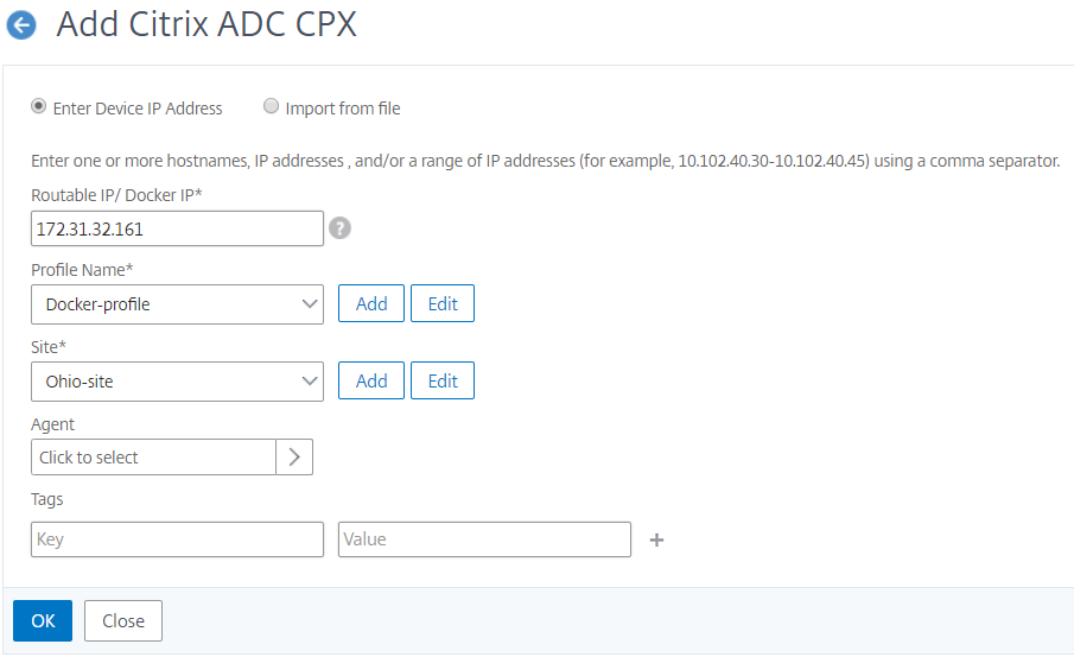
   a) 可以通过提供 CPX 实例的可访问 IP 地址或托管 CPX 实例的 Docker 容器的 IP 地址来添加 CPX 实例。

   b) 选择 CPX 实例的配置文件。

c) 选择要在其中部署实例的站点。

d) 选择代理。

e) 作为一种选择，您可以为实例输入键-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 NetScaler CPX 实例，在创建 CPX 实例配置文件时，必须指定主机的 **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 **NetScaler ADM** 中添加独立的 **NetScaler BLX** 实例

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

1. 导航到基础结构 **>** 实例 **> NetScaler**。
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 实例选择相应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
>
> ：确保在配置文件中指定了 Linux 服务器的正确主机用户名和密码。

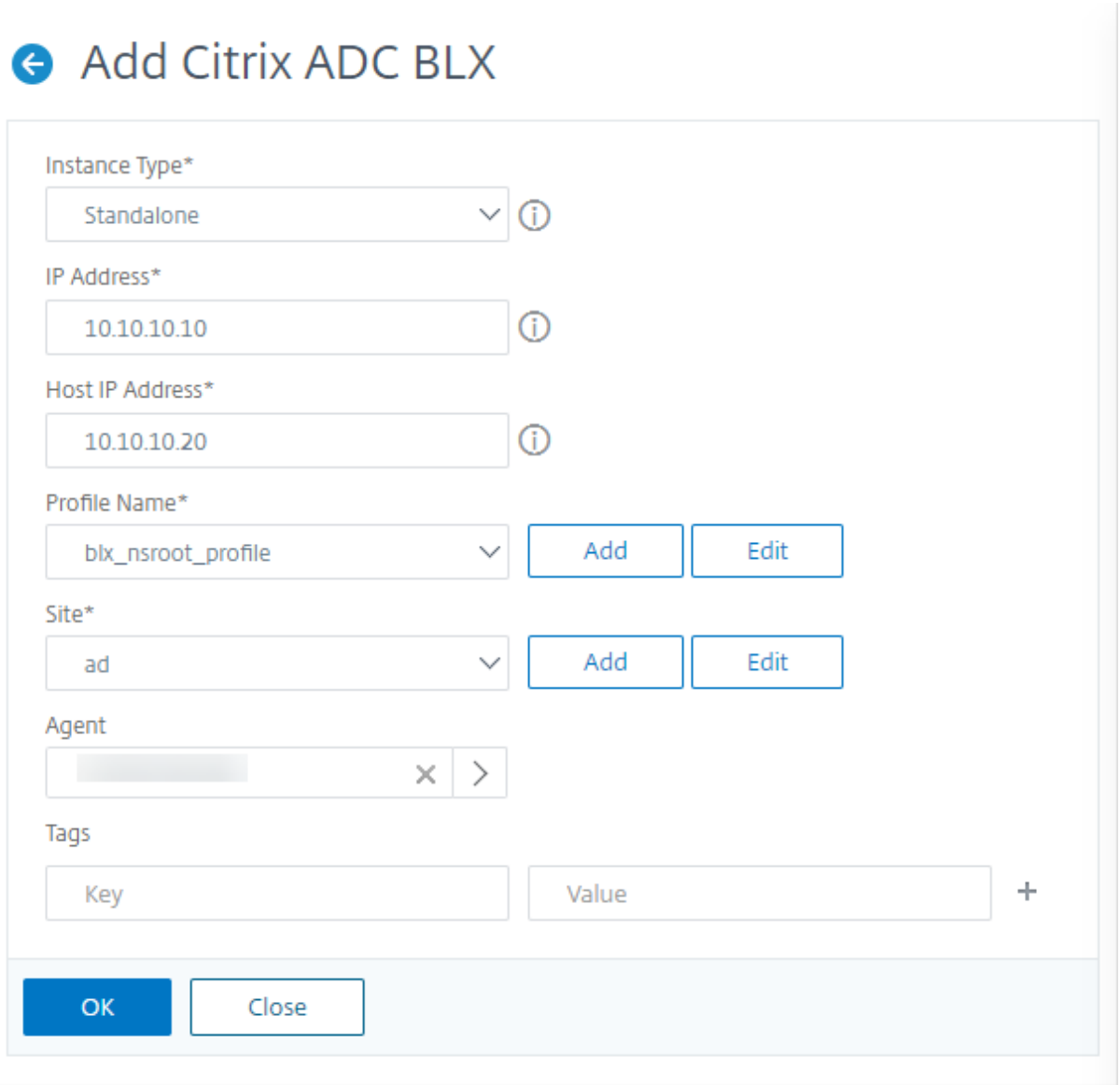
7. 在 站点 列表中，选择要添加实例的站点。

   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 NetScaler ADM 代理。

   如果在 NetScaler 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 **NetScaler ADM** 中添加高可用性 **NetScaler BLX** 实例

在不同主机 Linux 服务器上运行的高可用性 NetScaler BLX 实例。一台 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 实例选择相应的配置文件或创建配置文件。

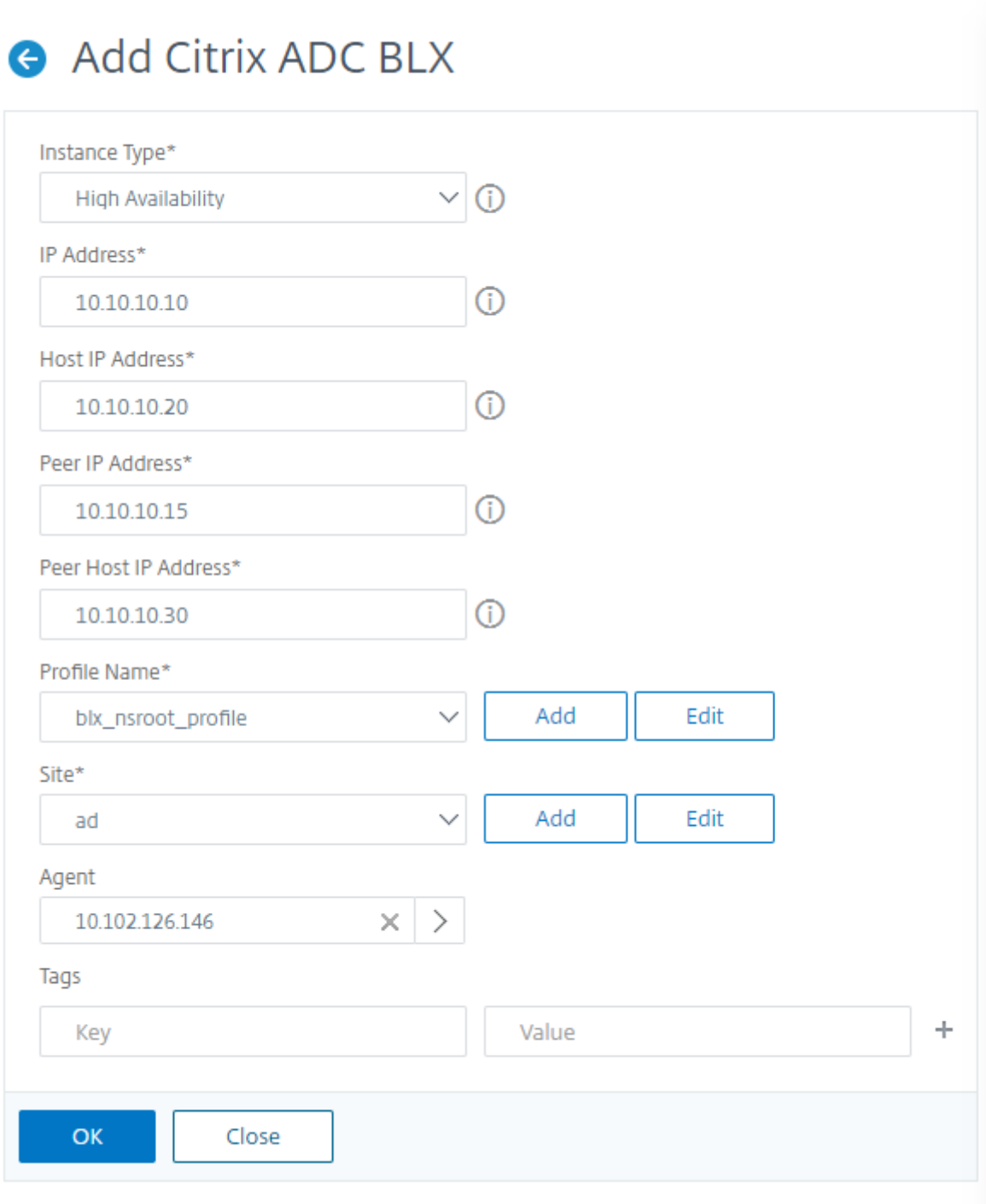
   要创建配置文件，请单击“添加”。

   > 重要
   >
   > ：确保在配置文件中指定了 Linux 服务器的正确主机用户名和密码。

8. 在 站点 列表中，选择要添加实例的站点。

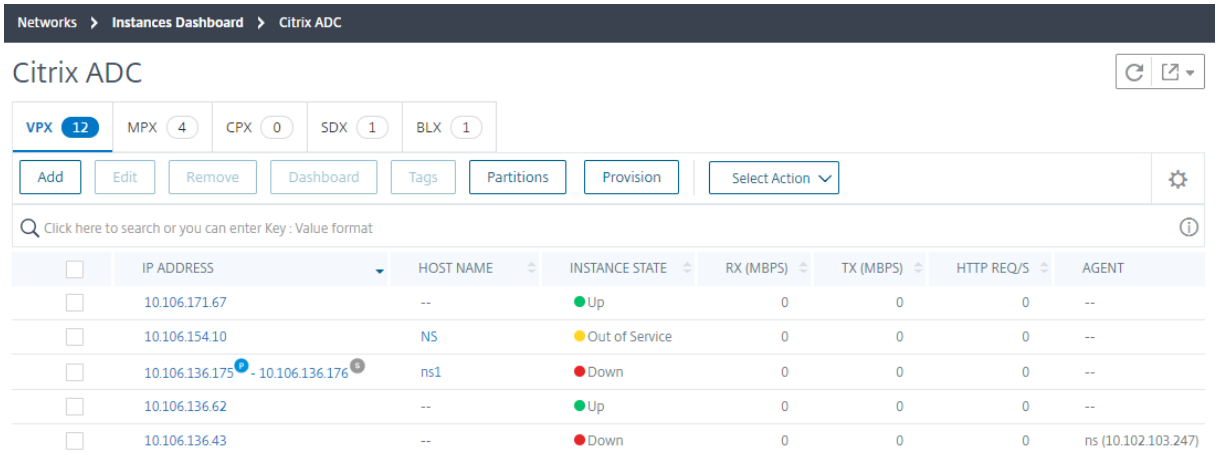
   如果要添加站点，请单击“添加”。
9. 在 代理 列表中，选择要与实例关联的 NetScaler ADM 代理。

   如果在 NetScaler 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 **NetScaler ADM** 访问实例图形用户界面

1. 导航到基础架构 **>** 实例 > **NetScaler**。
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 NetScaler IP 地址或主机名。



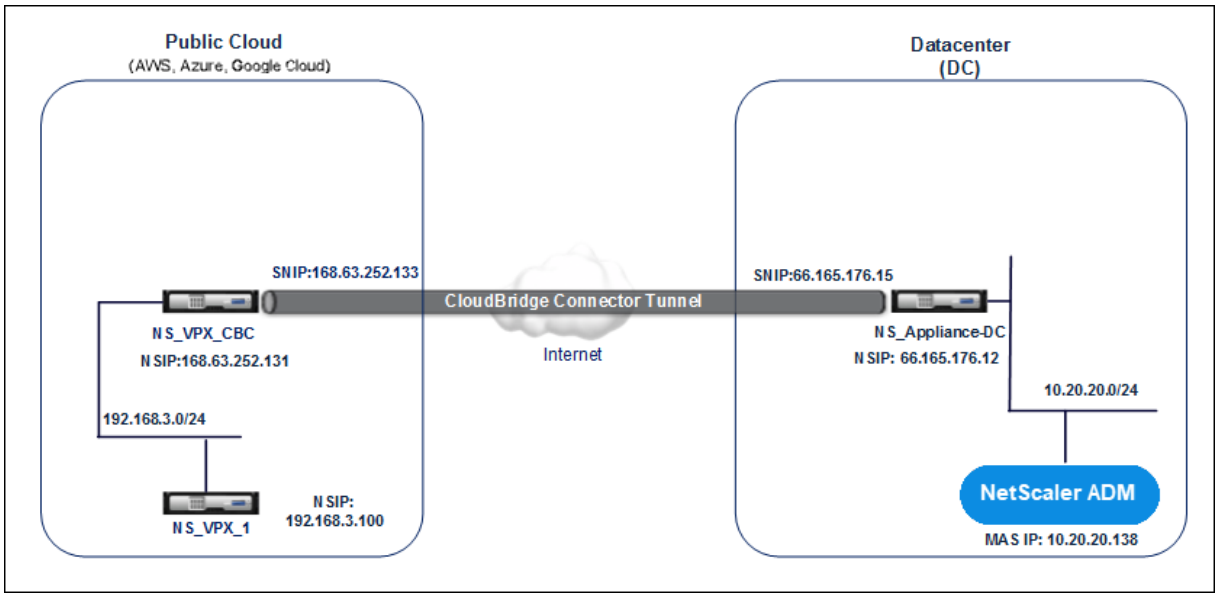
选定实例的 GUI 将显示在弹出窗口中。

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

February 6, 2024

您可以使用 NetScaler ADM 管理和监视部署在公有云（例如 Amazon Web Services (AWS)、Microsoft Azure 或 Google Cloud）上的 NetScaler VPX 实例。您需要在 NetScaler ADM 和部署在公有云上的 NetScaler VPX 实例之间建立第 3 层连接。要建立第 3 层连接，您可以使用直接连接到 AWS、Azure 中的 VPN 或 Equinix 等第三方连接器等解决方案。

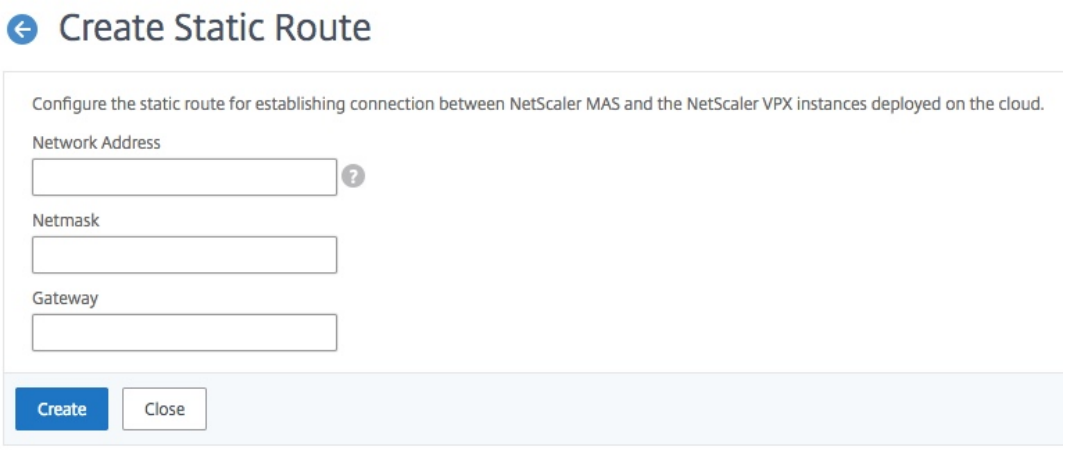
以下示例拓扑使用 Citrix CloudBridge Connector 在 NetScaler ADM 和云中部署的 NetScaler VPX 实例之间实现第 3 层连接。



Citrix CloudBridge 连接器隧道是在数据中心 DC 中的 NetScaler 设备 NS_Appliance-DC 和公有云中的 NetScaler 虚拟设备 (VPX) NS_VPX_CBC 之间建立的。NS_Appliance-DC 和 NS_VPX_CBC 可实现 NetScaler ADM 与部署在公有云中的 NetScaler VPX 实例 NS_VPX_1 之间的通信。建立通信后，您可以在 NetScaler 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 NetScaler VPX 实例。
   - 有关说明，请参阅在 AWS 上安装 NetScaler VPX。
   - 有关说明，请参阅在 Microsoft Azure 上安装 NetScaler VPX。
   - 有关说明，请参阅 在谷歌云上安装 NetScaler VPX。
2. 部署和配置 NetScaler 物理设备，或在数据中心的虚拟化平台上预配和配置 NetScaler 虚拟设备 (VPX)。
   - 有关说明，请参阅在 Citrix Hypervisor 上安装 NetScaler VPX 实例。
   - 有关说明，请参阅 在 VMware ESXi 上安装 Citrix 虚拟设备。
   - 有关说明，请参阅在 Microsoft Hyper-V 上安装 NetScaler 虚拟设备。
3. 在数据中心和公有云之间配置 Citrix CloudBridge Connector。有关说明，请参阅 配置 Citrix CloudBridge 连接器。
4. 配置用于在 NetScaler ADM 和部署在云中的 NetScaler VPX 实例之间建立连接的静态路由，如下所示：
   a) 登录到 NetScaler 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 NetScaler 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“网关”字段中，输入网关的地址。

5. 通过指定公有云中 NetScaler VPX 实例的 IP 地址范围，将 NetScaler VPX 云实例添加到 NetScaler ADM。有关详细说明，请参阅 将实例添加到 NetScaler ADM。

管理许可并在虚拟服务器上启用分析

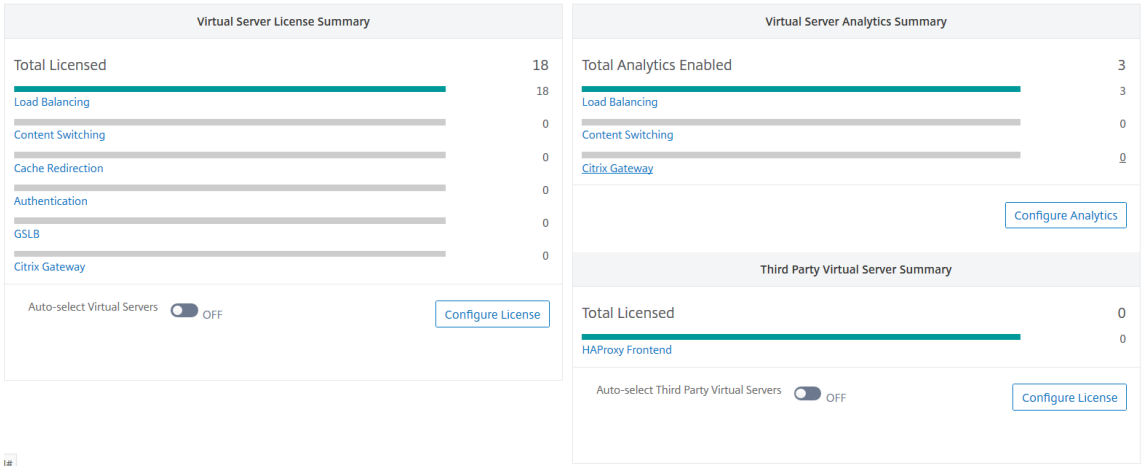
February 6, 2024

> 注意
>
> - 默认情况下，“自动许可的虚拟服务器”选项处于启用状态。您必须确保有足够的许可证来许可虚拟服务器。如果您的许可证有限，并且希望根据需要仅许可选择性虚拟服务器，请禁用“自动许可的虚拟服务器”选项。导航到 设置 > 许可和分析配置，然后禁用 虚拟服务器许可证分配下的自动许可虚拟服务器选项。

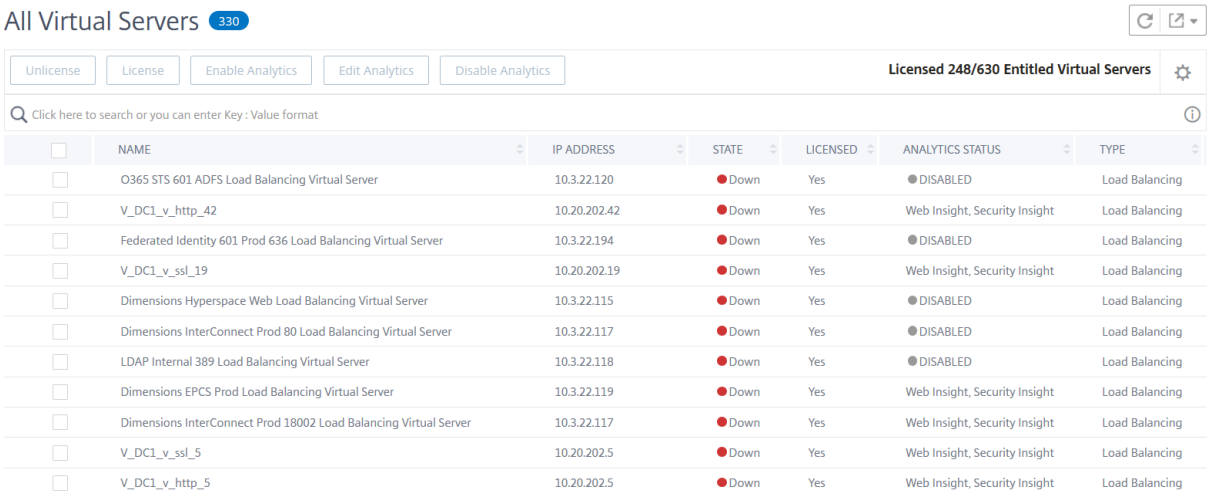
简化了启用分析的过程。您可以在单个工作流中许可虚拟服务器并启用分析。

导航到“设置”>“许可和分析配置”，以执行 以下操作：

- 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”页面。



在“所有虚拟服务器”页面上，您可以：

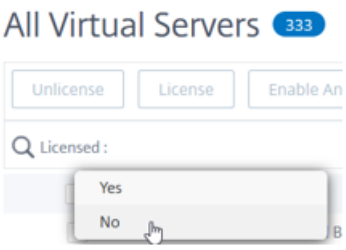
- 为未经许可的虚拟服务器申请许可证
- 移除获得许可的虚拟服务器的许可证
- 在许可的虚拟服务器上启用分析
- 编辑分析
- 禁用分析

> 注意
>
> 支持用于启用分析的虚拟服务器是负载平衡、内容切换和 NetScaler Gateway。

管理虚拟服务器上的许可

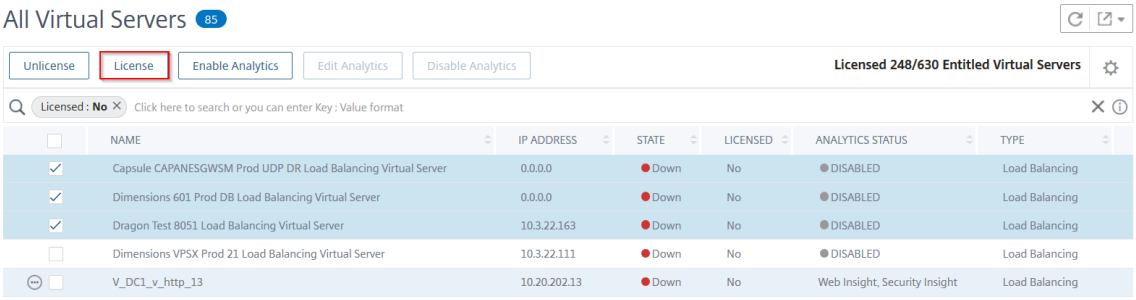
要许可虚拟服务器，请从“所有虚拟服务器”页面执行以下操作：

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，请在“所有虚拟服务器”页面中执行以下操作：

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”。

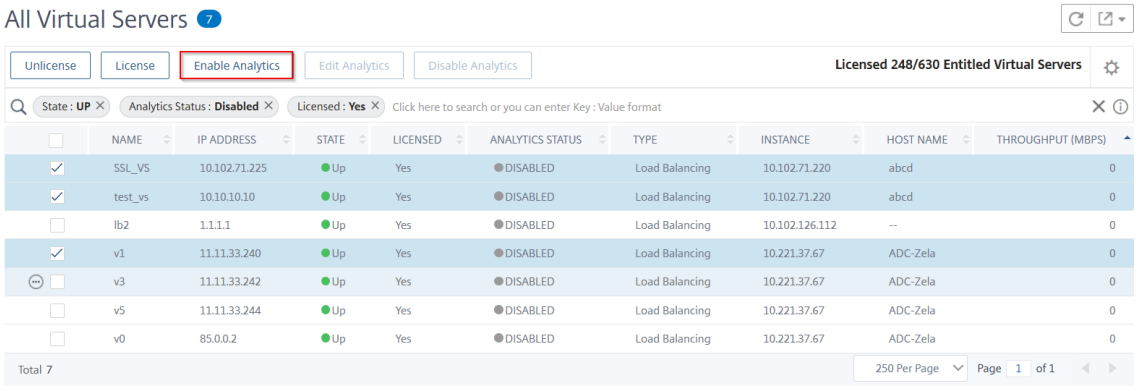
启用分析

以下是启用虚拟服务器分析的先决条件：

- 确保虚拟服务器已获得许可
- 确保分析状态为“已禁用”
- 确保虚拟服务器处于运行状态

您可以筛选结果以确定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“向上”。
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 **基础结构 > 实例 > NetScaler** ，然后选择实例类型。例如，VPX。
2
3. 选择实例，然后从“**选择操作”**列表中选择“**配置分析**”
4. 在“在虚拟服务器上配置分析”页面上，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) 选择数据分析类型（Web Insight 或 WAF 安全违规）

   b) 选择 **Logstream** 作为传输模式

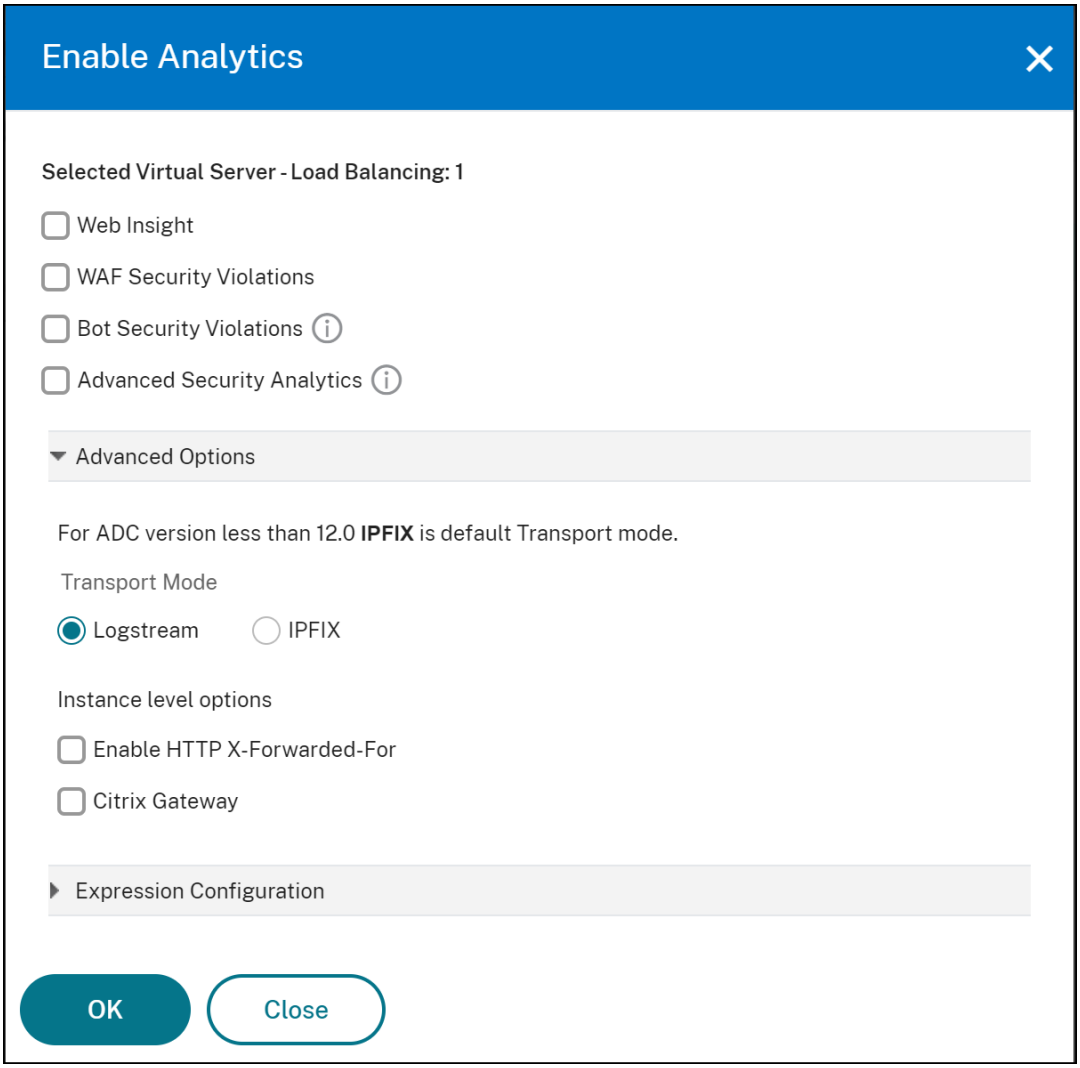
   > 注意
   >
   > 对于 NetScaler 12.0 或更低版本，**IPFIX** 是传输模式的默认选项。对于 NetScaler 12.0 或更高版本，您可以选择 **Logstream** 或 **IPFIX** 作为传输模式。
   >
   > 有关 IPFIX 和 Logstream 的更多信息，请参阅 Logstream 概述。

   c) 在 实例级别选项下：

   - 启用 **HTTP X-Forwarded-For** -选择此选项可标识客户端和应用程序之间通过 HTTP 代理或负载平衡器进行连接的 IP 地址。
   - **NetScaler Gateway** -选择此选项可查看 NetScaler Gateway 的分析。

   d) 默认情况下，表达式为 true

   e) 单击 **OK**（确定）



注意

- 如果您选择未获得许可的虚拟服务器，则 NetScaler ADM 将首先许可这些虚拟服务器，然后启用分析
- 对于管理分区，仅支持 **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，NetScaler ADM 将处理在所选虚拟服务器上启用分析。

注意

NetScaler ADM 使用 NetScaler SNIP 作为 Logstream，使用 NSIP 作为 IPFIX。如果在 NetScaler ADM 代理和 NetScaler 实例之间启用了防火墙，请确保打开以下端口，以允许 NetScaler ADM 收集 AppFlow 流量：

传输模式	源 IP	类型	端口
IPFIX	NSIP	UDP	4739
Logstream	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：

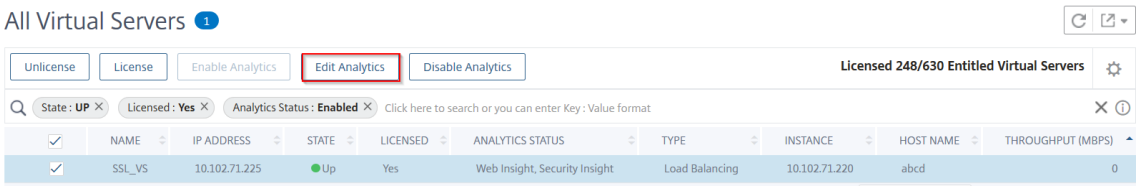
1. 选择虚拟服务器

   注意

   或者，您也可以编辑特定实例的分析：

   ```
   1. 导航到 **基础结构 > 实例 > NetScaler** ，然后选择实例类型。例如，VPX。
   2
   3. 选择该实例，然后单击“**编辑分析”**。
   ```

2. 单击 编辑分析

3. 在“编辑 分析配置”窗口中编辑 要应用的参数

4. 单击确定。

禁用分析

要在选定的虚拟服务器上禁用分析，请执行以下操作：

1. 选择虚拟服务器

2. 单击“禁用分析”

NetScaler ADM 禁用选定虚拟服务器上的分析

下表介绍了支持 IPFIX 和 Logstream 作为传输模式的 NetScaler ADM 的功能：

功能	IPFIX	Logstream
Web Insight	•	•
WAF 安全违规	•	•
Gateway Insight	•	•
HDX Insight	•	•
SSL Insight	不支持	•
CR Insight	•	•
IP 信誉	•	•
AppFirewall	•	•
客户端衡量标准	•	•
Syslog/Auditlog	•	•

在虚拟服务器上启用分析的统一过程

February 6, 2024

除了启用分析的现有流程外，您还可以使用单窗格工作流在以下位置配置分析：

- 所有获得许可的现有虚拟服务器
- 随后获得许可的虚拟服务器

配置完成后，此功能消除了在现有和后续虚拟服务器上手动启用分析的必要性。

注意事项：

在配置分析之前，必须了解 NetScaler ADM 的以下行为：

- 首次配置此功能时，必须确保满足本文档中提到的先决条件。
- 稍后修改分析设置。

  假设您已经通过选择 Web Insight、HDX Insight 和 Gateway Insight 首次配置了分析设置。如果您想稍后修改分析设置并取消选择 Gateway Insight，则所做的更改不会影响已启用分析功能的虚拟服务器。
- 已启用分析功能的虚拟服务器。

  假设您有 10 台获得许可的虚拟服务器，其中两台已经启用了分析功能。在这种情况下，此功能仅对剩余的八个虚拟服务器启用分析。

- 使用分析手动禁用的虚拟服务器。

  假设您有 10 台获得许可的虚拟服务器，并且手动禁用了两台虚拟服务器的分析。在这种情况下，此功能仅对剩余的八个虚拟服务器启用分析，并跳过通过分析手动禁用的虚拟服务器。

- 机器人安全违规和 **WAF** 安全违规选项仅在高级许可的虚拟服务器中受支持。如果虚拟服务器未获得高级许可，则不会启用机器人安全违规和 **WAF** 安全违规。

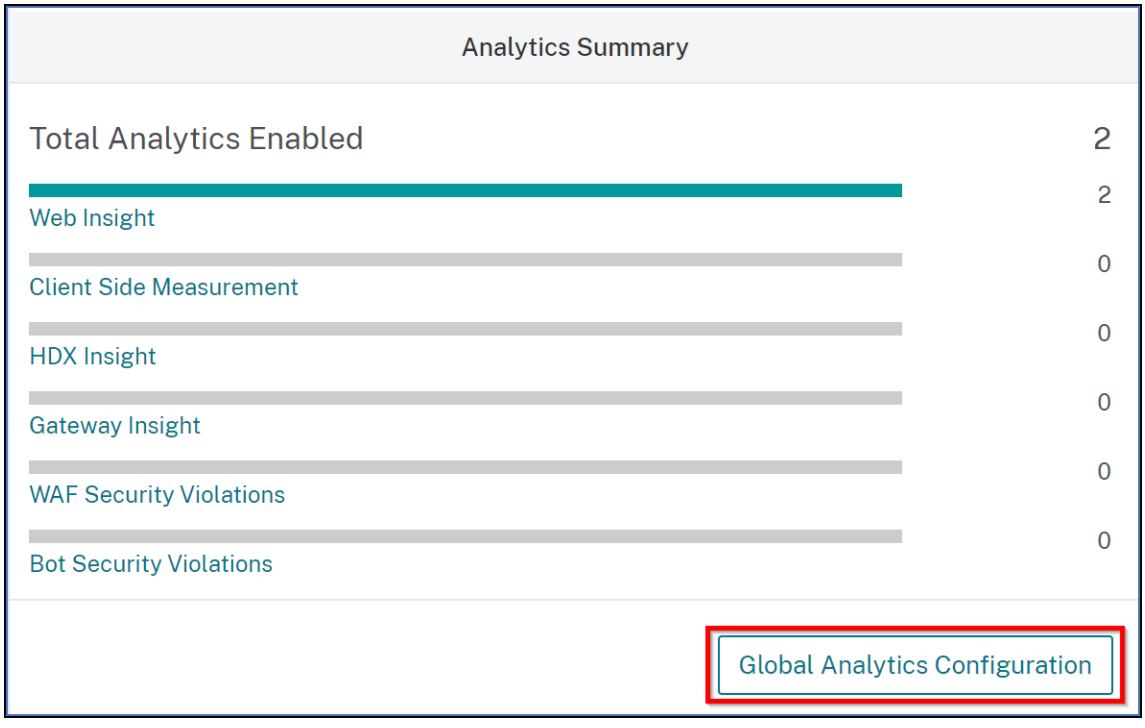
必备条件

请确保：

- 所有现有的虚拟服务器都已获得许可。
- 已启用自动许可选项以许可所有后续虚拟服务器。导航到设置 **>** 许可和分析配置，然后在虚拟服务器许可证分配下，打开自动许可的虚拟服务器选项。

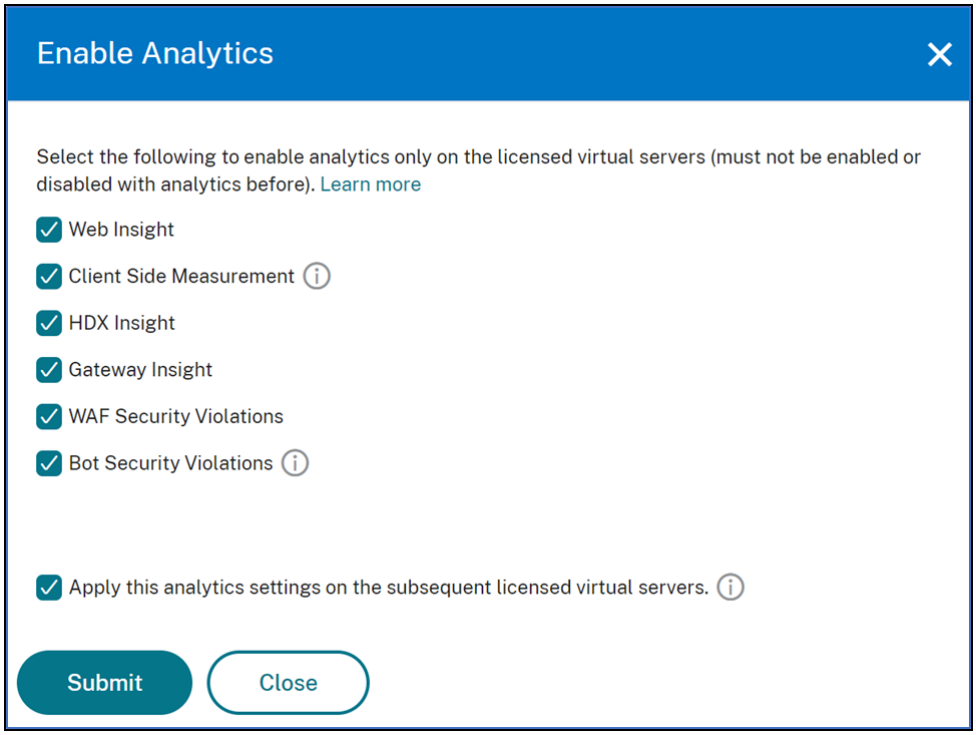
启用分析

1. 导航到设置 **>** 许可和分析配置。
2. 在分析摘要下，单击全局分析配置。



3. 选择要在虚拟服务器上启用分析的分析功能。
4. 要在后续虚拟服务器上启用分析，请选中在后续许可的虚拟服务器上应用此分析设置复选框。

5. 单击 **Submit**（提交）。



配置 NTP 服务器

February 6, 2024

您可以在 NetScaler ADM 中配置网络时间协议 (NTP) 服务器，使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler 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 **NetScaler ADM** 上配置 **NTP** 服务器，请执行以下操作：

1. 从 ADM GUI 中，导航到“设置”**>**“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 **NetScaler 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

February 6, 2024

在开始使用 NetScaler ADM 管理和监视您的实例和应用程序之前，建议您配置一些系统设置，确保 NetScaler 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。当某个警报类别（例如 memoryUsageHigh）的阈值超过阈值时，或者当发生与该警报类别相对应的事件（例如 LoginFailure）时，系统会记录一条消息，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“设置”**>**“**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. 要查看已超过阈值的警报或已发生事件的警报，请导航到 设置 **>** 审核，然后单击 系统日志消息。

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 NetScaler 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。设置通知可确保您收到任何系统级活动（如用户登录或系统重启）的通知。

要配置系统通知，请执行以下操作：

1. 导航到 **Settings**（设置）**> Administration**（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 NetScaler 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。

配置系统删除设置

要限制 NetScaler ADM 服务器数据库中存储的报告数据量，可以指定希望 NetScaler 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 小时修剪一次（在 00.00 点）。

要配置系统修剪设置，请执行以下操作：

1. 导航到“设置”**>**“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”页面中，指定保留数据的天数，然后单击“保存”。

配置实例 **syslog** 删除设置

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。您可以指定从 NetScaler ADM 中删除通用 syslog 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. 导航到“设置”**>**“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 **Syslog** 删除设置”页中，在“保留 **Syslog** 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 NetScaler ADM 服务器数据库中存储的事件消息数据量，可以指定希望 NetScaler 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 **Settings**（设置）**> Administration**（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”页面中，单击“实例事件”。
4. 在要保留的数据（天）字段中，输入要在 **NetScaler 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

NetScaler ADM 每天 00:30 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 **Settings**（设置）**> Administration**（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”页面上，指定所需的值。

配置实例备份设置

如果您备份 NetScaler 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 **Settings**（设置）**> Administration**（管理）。
2. 在“备份”下，单击“配置系统和实例备份”。
3. 单击“配置实例备份设置”下的“实例”，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“设置”**>**“管理”**>**“可配置功能”页面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，NetScaler 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 为多站点部署配置本地代理。
- 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，NetScaler 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 NetScaler 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。有关更多信息，请参阅 备份和还原 NetScaler 实例。

- 实例配置审核 -跨托管 NetScaler 实例监视配置更改，排除配置错误并恢复未保存的配置。有关详细信息，请参阅 创建审核模板。
- 实例事件 -事件表示在托管 NetScaler 实例上发生的事件或错误。在 NetScaler ADM 中收到的事件显示在“事件摘要”页面（基础架构 **>** 事件）上，所有活动事件显示在“事件消息”页面（基础架构 **>** 事件 **>** 事件消息）中。有关更多信息，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 -NetScaler ADM 提供了在所有托管 NetScaler 实例中安装的 SSL 证书的集中视图。有关详细信息，请参阅 SSL 控制面板。
- 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 NetScaler ADM，则可以监视在 NetScaler 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**。

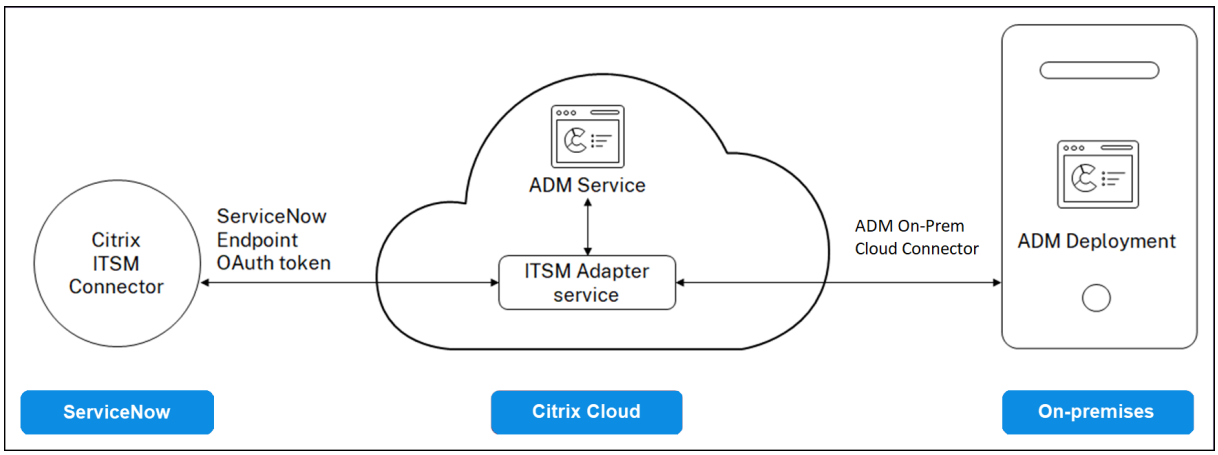
> 重要
>
> 信息如果某项功能被禁用，则用户无法执行与该功能相关的操作。

将 NetScaler ADM 与 ServiceNow 实例集成

February 6, 2024

如果要为 NetScaler 和 ADM 事件启用 ServiceNow 通知，请将 NetScaler ADM 与 ServiceNow 实例集成。此集成使用 Citrix ITSM 连接器 在 NetScaler ADM 和 ServiceNow 实例之间进行通信。

ServiceNow 与 ADM 的集成使用 ITSM Adapter 服务进行基于令牌的身份验证。为此，它会在 ServiceNow 中创建一个终端节点实例。有关更多信息，请参阅 ITSM 适配器的工作原理。



要将您的 ADM 本地部署与 ITSM 适配器连接，请确保配置客户身份。有关详细信息，请参阅 配置客户身份。

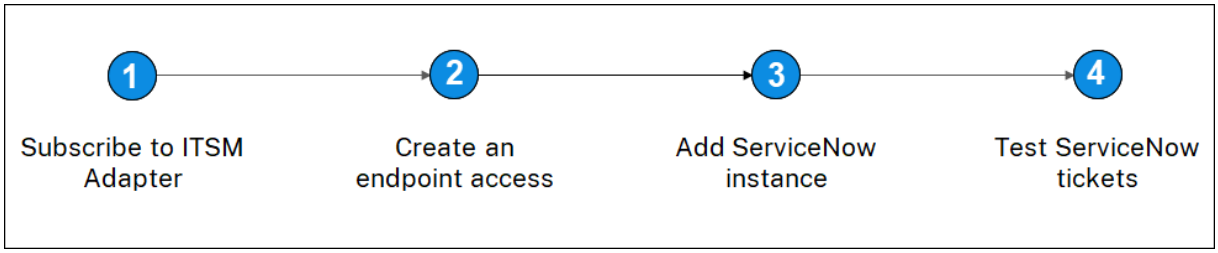
必备条件

在将 ADM 与 ServiceNow 集成之前，请确保满足以下条件：

1. 注册使用 Citrix Cloud。确保您有权管理 Citrix Cloud 管理员。有关更多信息，请参阅 管理 Citrix Cloud 管理员。

如何将 **ADM** 与 **ServiceNow** 集成

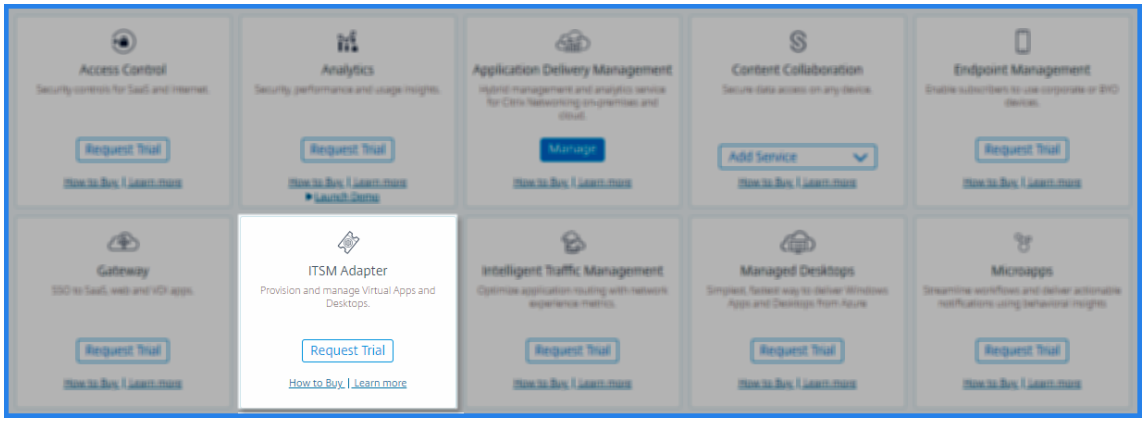
执行以下步骤，使用 ITSM 连接器将 NetScaler ADM 与 ServiceNow 集成：



1. 在 Citrix Cloud 中订阅 ITSM 适配器服务。
2. 在 ServiceNow 实例中创建终端节点访问权限。
3. 添加一个 ServiceNow 实例。
4. 在 ADM 中测试 ServiceNow 票证的自动生成。

步骤 **1-**在 **Citrix Cloud** 中订阅 **ITSM** 适配器服务

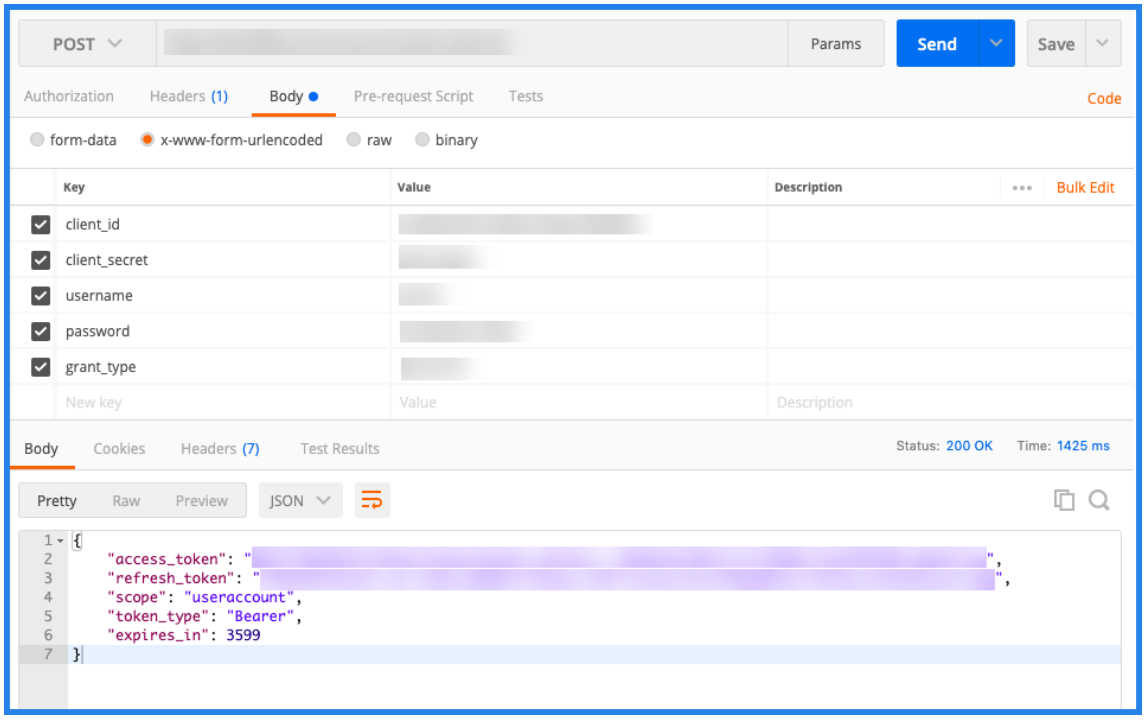
1. 在 **ITSM** 适配器 磁贴上，单击 请求试 用。



2. 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。

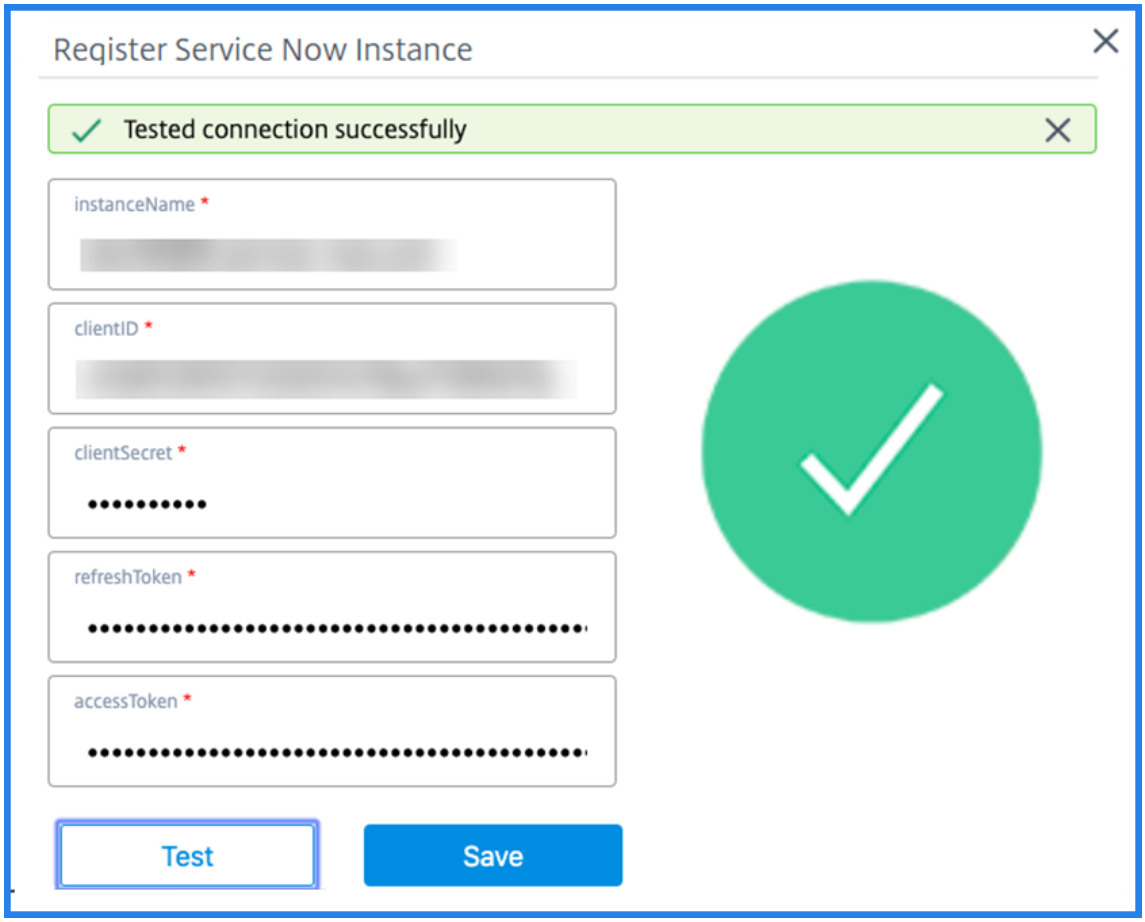
步骤 **2-**在 **ServiceNow** 实例中创建终端节点访问权限

1. 使用管理员凭据登录到您的 ServiceNow 实例。
2. 转到 ServiceNow 应用商店。下载并安装 **Citrix ITSM** 连接器。
3. 在 Citrix ITSM 连接器窗格上，选择主页，然后单击身份验证。键入您在 Citrix Cloud 中记下的客户端 ID 和密钥。
4. 测试连接。
5. 保存配置。出现来自 ServiceNow 的确认消息，表明连接处于活动状态。
6. 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。
7. 使用客户端 ID 和客户端密钥获取访问和刷新令牌。请参阅 OAuth 令牌。



步骤 **3-**添加 **ServiceNow** 实例

1. 在管理选项卡中，选择“添加 ServiceNow 实例”。
2. 指定 实例名称、客户端 **ID**、客户端密钥、刷新令牌和 访问令牌。
3. 单击“测试”。



ServiceNow 实例现已连接到 ITSM 适配器服务。

4. 成功测试连接后，单击保存以添加 ServiceNow 实例。

第 **4** 步-在 **ADM** 中测试 **ServiceNow** 票证的自动生成

1. 登录到 NetScaler ADM。
2. 导航到“帐户”**>**“通知”，然后选择 **ServiceNow**。
3. 从列表中选择 ServiceNow 配置文件。
4. 单击“测试”自动生成 ServiceNow 票证并验证配置。

   如果要在 NetScaler ADM GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。

在 **ADM** 中设置 **ServiceNow** 通知

在 ITSM 适配器上注册 ServiceNow 实例后，您可以在 NetScaler ADM GUI 中为以下事件设置 ServiceNow 通知：

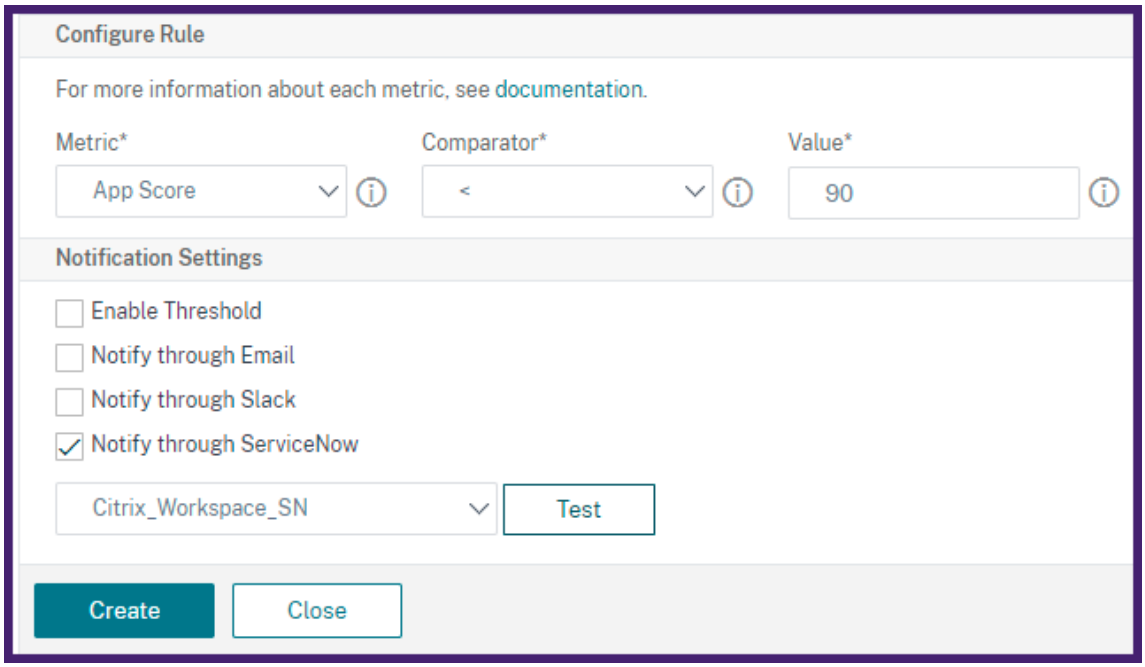
> 重要
>
> ServiceNow 云支持此功能。

- **NetScaler** 事件：NetScaler ADM 可以从选定托管 NetScaler 实例中为选定的一组 NetScaler 事件生成 ServiceNow 事件。

  要从托管实例发送 NetScaler 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。

  导航到 基础架构 **>** 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。

- 应用程序分析：NetScaler ADM 可以为超过指定阈值的应用程序生成 ServiceNow 事件。



  在此示例中，当应用程序的应用程序分数低于 90 时，将生成 ServiceNow 事件。

- **SSL** 证书和 **ADM** 许可证事件：NetScaler ADM 可以为 SSL 证书过期和 ADM 许可证过期事件生成 ServiceNow 事件。

  要发送有关 SSL 证书到期的 ServiceNow 通知，请参阅 SSL 证书到期时间。

  要发送有关 ADM 许可证到期的 ServiceNow 通知，请参阅 NetScaler ADM 许可证到期。

导出或计划导出报告

February 6, 2024

在 NetScaler ADM 中，您可以导出所选 NetScaler 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。

NetScaler 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 NetScaler 实例的导出报告，请导航到“网络”**>**“实例”**>**“**NetScaler**”，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。

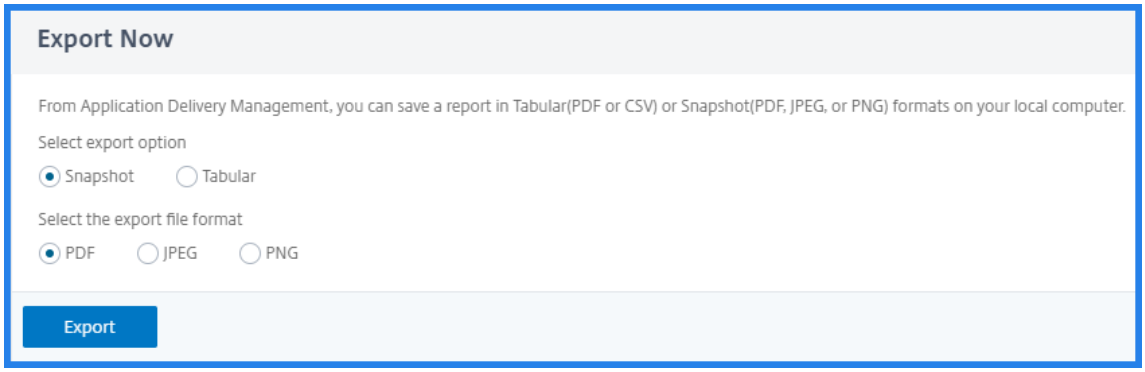
在“导出报告”中，您可以执行以下操作：

- 将报告导出到本地计算机
- 安排导出报告
- 查看、编辑或删除预定的导出报告

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。

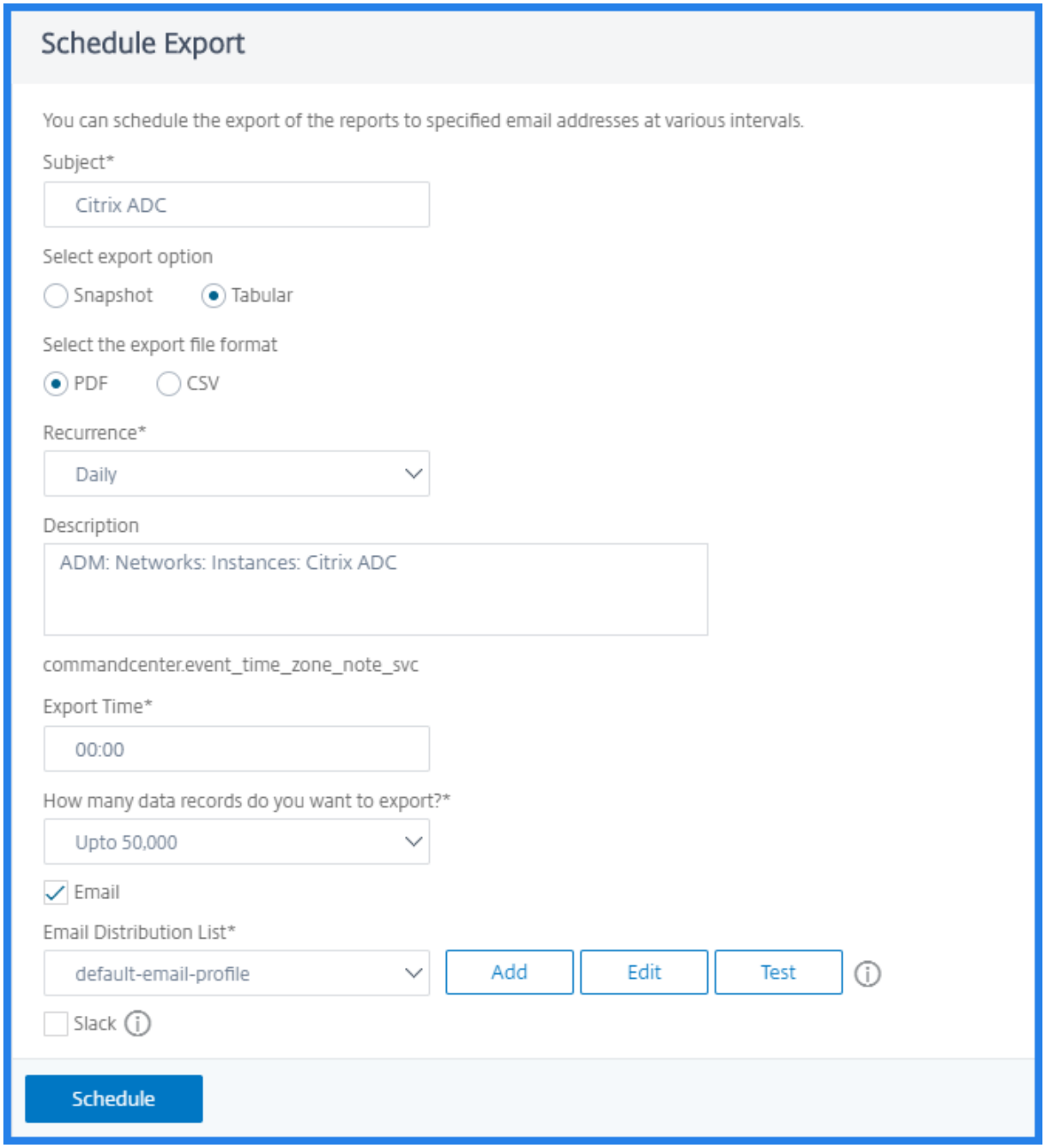
安排导出报告

要定期安排导出报告，请指定重复间隔。NetScaler ADM 将导出的报告发送到配置的电子邮件或 slack 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，此字段会自动填充选定的功能名称。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 -指定要导出报告的时间。
- 电子邮件 - 选中复选框并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** - 选中复选框并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 页面显示所有特定功能的导出报告。

2. 选择要编辑的报告，然后单击 编辑。

升级

February 6, 2024

每个 NetScaler 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 NetScaler ADM 升级到最新版本，以利用新功能和错误修复。增强功能、已知问题和缺陷修复的完整列表在每个版本发布时附带的发行说明中提供。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 NetScaler ADM 许可信息，请参阅许可。

升级路径信息也可在 Citrix 升级指南中找到。

升级准备

从 NetScaler ADM 的“Downloads”（下载）页面下载升级包，并按照本文中的说明将您的系统升级到最新的内部版本 13.1。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 NetScaler ADM 在升级完成之前不会处理任何数据。

> 重要
>
> NetScaler ADM 版本和内部版本应 等于或高 于您的 NetScaler 版本和内部版本。例如，如果您已安装 NetScaler ADM 12.1 Build 50.39，请确保已安装 NetScaler 12.1 Build 50.28/50.31 或更早版本。

升级到 **13.1** 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 13.1。
- 如果您从 12.0 版本 57.24 及更高版本升级，请先升级到 12.1，然后再升级到 13.1。
- 如果从 12.1 升级，则可以直接升级到 13.1。
- 如果从低于 13.0 64.xx 的版本升级，为了获得更好的用户体验，请先升级到 13.0 64.xx，然后再升级到 13.1。

升级到 **13.1 xx.xx** 及更高版本之前需要注意的重要事项

将 ADM 软件升级到版本 13.1 xx.xx 时，您的 ADM 数据库也会被迁移。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：

- 如果您要升级到 13.1 xx.xx 及更高版本，请拍下 NetScaler ADM 服务器的快照。
- 在升级之前，请备份 NetScaler ADM 服务器。
- 升级后，您可能需要在 NetScaler ADM 服务器与托管实例之间重新建立连接。如果继续，会有确认提示向您警告连接可能失败。
- 如果您升级到 13.1.9.x 和 13.1.30.x 之间的任何版本，NetScaler ADM 会将现有样书 ConfigPack 回滚到其早期版本。

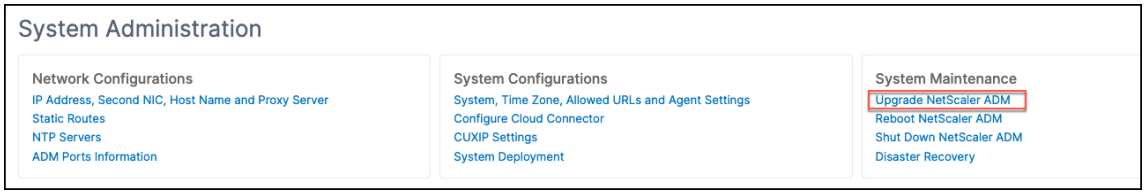
  要避免此问题，请升级到 13.1.33.50 版本。
- 对于高可用性设置中的 NetScaler ADM 服务器，升级时，请勿在其中任何一个节点上进行任何配置更改。

  > 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。

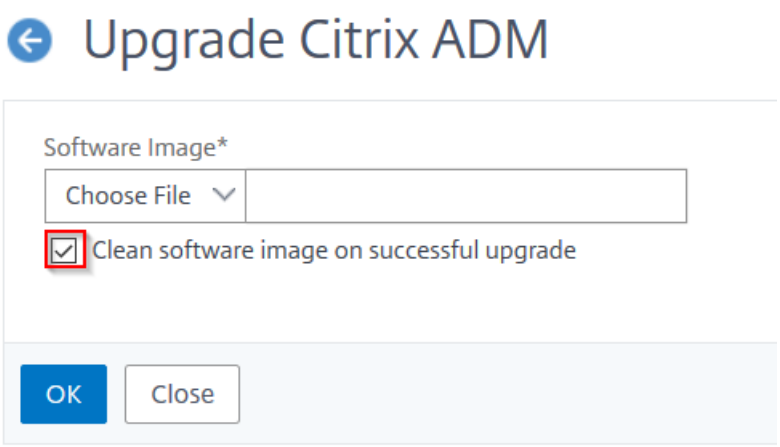
将单台 **NetScaler ADM** 服务器升级到 **13.1-12.x**

1. 使用管理员凭据登录到 NetScaler ADM。
2. 导航到 **Settings**（设置）**> Administration**（管理）。在“系统维护”下，单击“升级 **NetScaler ADM**”。

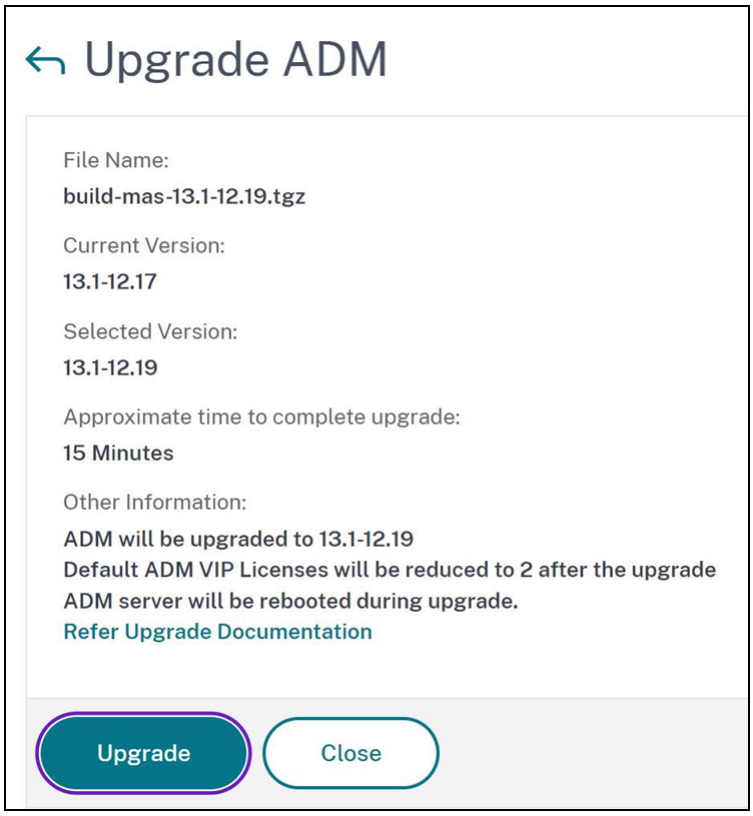


3. 在 升级 **NetScaler ADM** 页面 上，选中升级成功时清理软件映像 复选框以在升级后删除映像文件。选择此选项会在升级时自动删除 NetScaler ADM 映像文件。

   > 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。

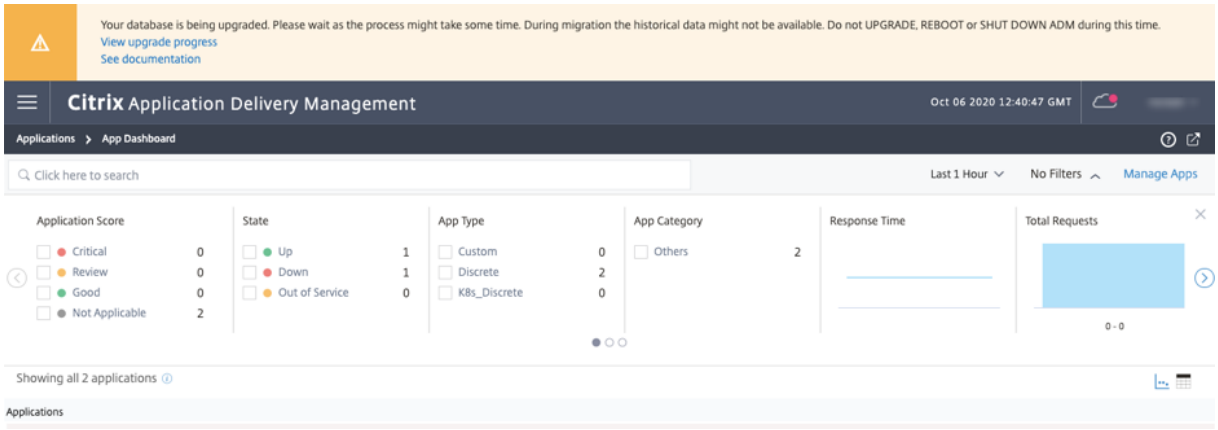


4. 然后，您可以通过选择“本地”（您的 本地 计算机）或“设备”来上载新的映像文件。构建文件必须存在于 NetScaler ADM 虚拟设备上。
5. 单击确定。
6. 升级 **ADM** 页面显示的详细信息很少，例如文件名、所选版本、预计完成时间。单击 **Upgrade**（升级）。



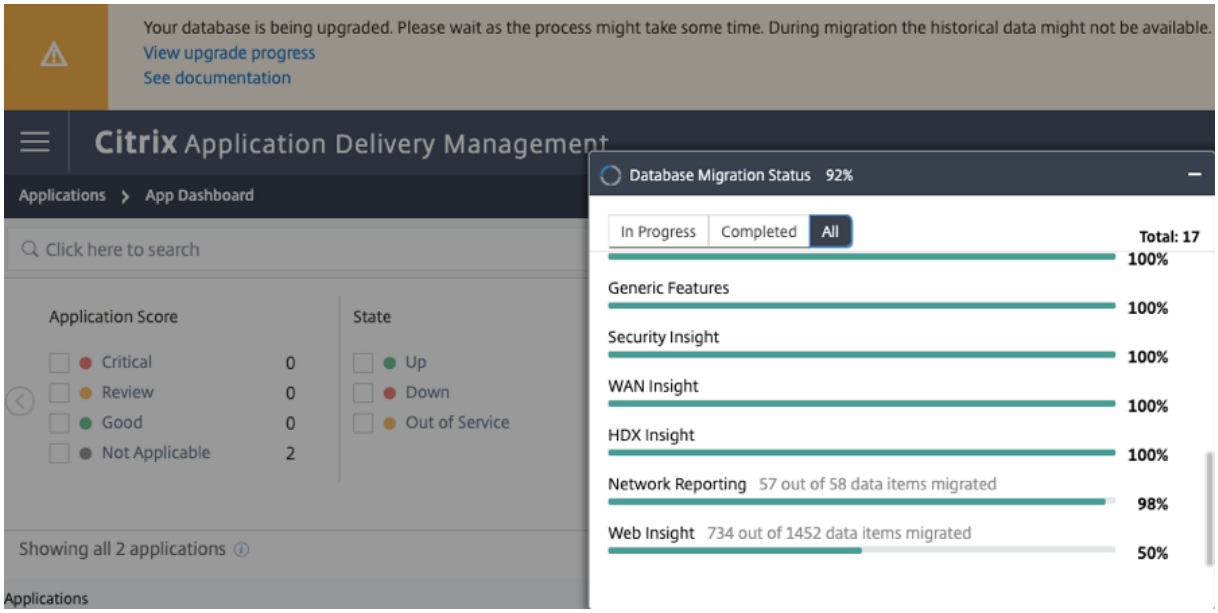
升级过程开始。

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。

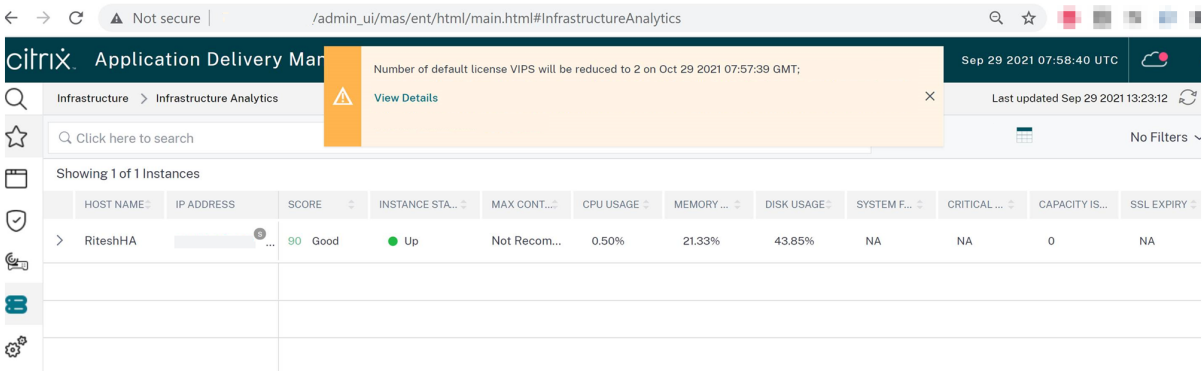


在历史数据迁移期间，某些旧数据可能不可用。迁移数据库所需的时间取决于数据的大小和表的数量。

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。

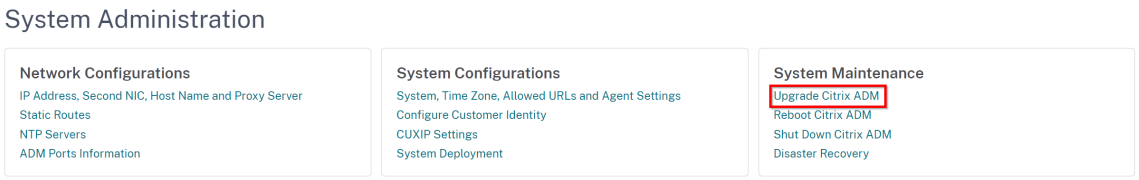


升级完成后，您可以查看默认免费许可证减少到两个的消息。单击 **View Details**（查看详细信息）了解更多信息。



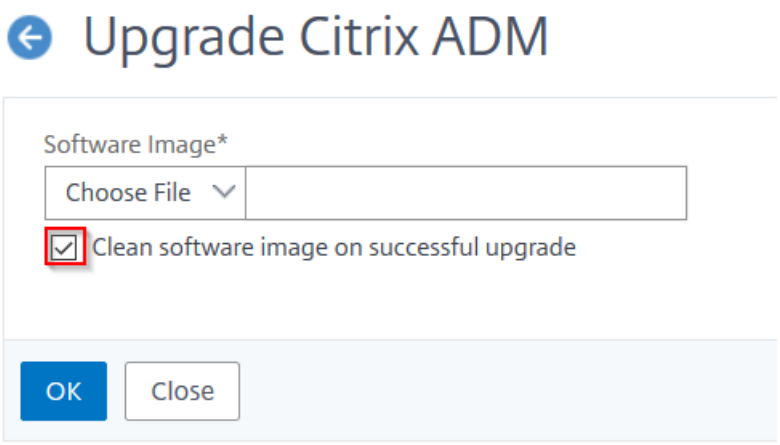
将单台 **NetScaler ADM** 服务器升级到 **13.1-4.x** 或 **13.1-9.x**

1. 使用管理员凭据登录到 NetScaler ADM。
2. 导航到 **System**（系统）> **System Administration**（系统管理）。在 系统管理 子标题下，单击 升级 **NetScaler ADM**。

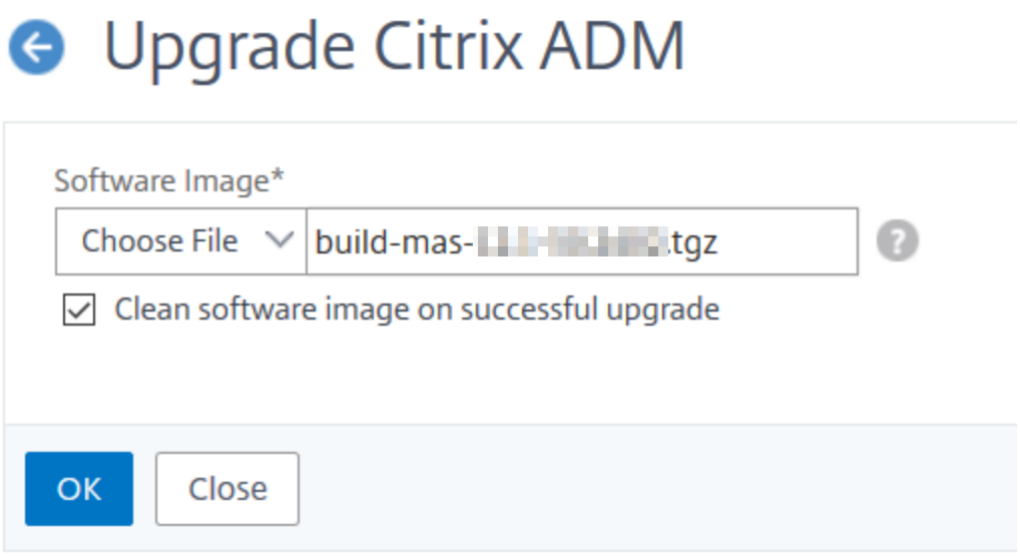


3. 在 升级 **NetScaler ADM** 页面 上，选中升级成功时清理软件映像 复选框以在升级后删除映像文件。选择此选项会在升级时自动删除 NetScaler ADM 映像文件。

> 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”（您的 本地 计算机）或“设备”来上载新的映像文件。构建文件必须存在于 NetScaler ADM 虚拟设备上。

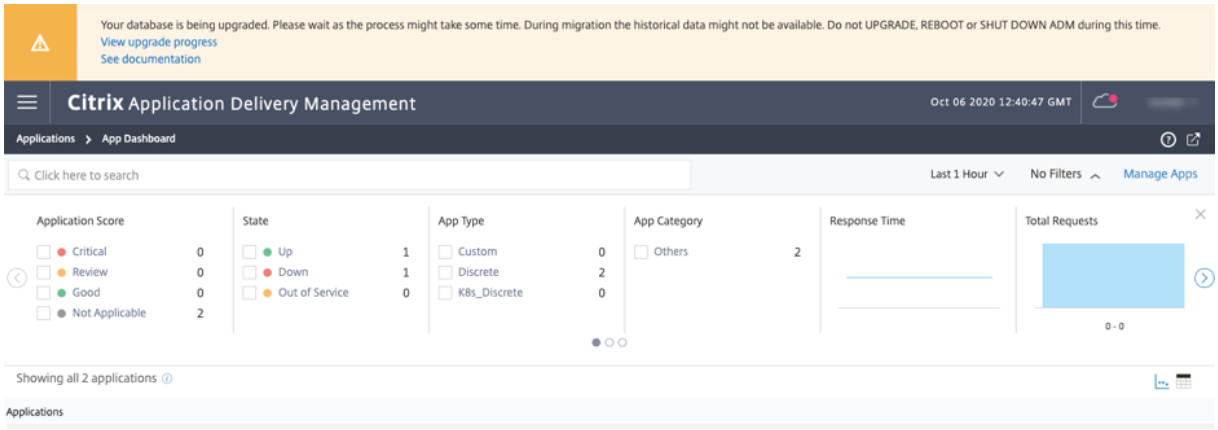


5. 单击确定。

   此时将显示“Confirm”（确认）对话框。单击是。

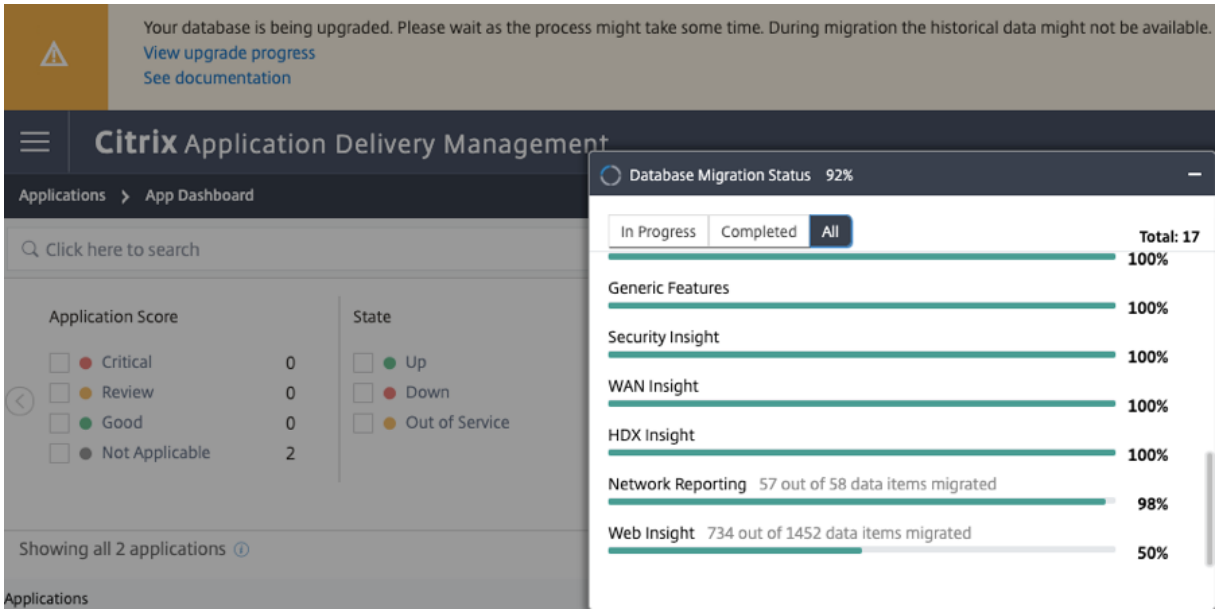
   升级过程开始。

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 13.1 xx.xx 及更高版本的过程中，Web Insight 历史数据的迁移有时可能会停滞不前。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** 版本升级到 **13.1** 版本

对于高可用性模式下的 NetScaler 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 NetScaler 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 NetScaler ADM 12.1 升级

升级 **NetScaler ADM** 灾难恢复部署

升级 NetScaler ADM 灾难恢复部署分为两个步骤：

- 升级主站点中在高可用性模式下配置的 NetScaler 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，请确保已升级以高可用性部署的 NetScaler ADM 服务器。

升级 **NetScaler ADM** 灾难恢复节点

1. 从 NetScaler 网站下载 NetScaler ADM 升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上载到灾难恢复节点。
3. 使用 `nsrecover` 凭据登录灾难恢复节点。
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：

   ./installmas

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

为多站点部署升级内部部署代理

升级 NetScaler ADM 代理部署分为三个步骤。
在升级本地代理之前，请确保已完成以下任务：

1. 升级在高可用性中部署的 NetScaler ADM 服务器。
2. 升级 NetScaler ADM 灾难恢复节点。

   有关详细信息，请参阅 升级 NetScaler ADM 灾难恢复部署。

升级本地代理

1. 从 NetScaler 网站下载 NetScaler ADM 代理升级映像文件。
2. 使用 `nsrecover` 凭据将此文件上载到代理节点。
3. 确保您下载了正确的代理升级映像。
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 **NetScaler ADM** 服务器添加额外的磁盘

如果 NetScaler 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。

从发行版 12.1–13.1Œ 升级 NetScaler ADM 时，您在早期版本中的其他磁盘上创建的分区将保持不变。分区不会被移除或调整大小。

在升级后的版本中，附加更多磁盘的过程保持不变。现在，您可以使用 NetScaler 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 NetScaler ADM。

使用样书在 **OpenStack** 中预配 **NetScaler** 实例

从 NetScaler ADM 12.1 版本 49.23 开始，OpenStack 调配工作流的体系结构已更新。该工作流程现在使用 NetScaler ADM 样书来配置 NetScaler 实例。如果从版本 12.0 或 12.1 版本 48.18 升级到 NetScaler ADM 13.1，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` 样书和迁移脚本的更多信息，请参阅 使用样书在 OpenStack 上预配 NetScaler VPX 实例

身份验证

February 6, 2024

用户可以通过 NetScaler 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进行身份验证，或者两者兼而有之。如果使用本地身份验证，则用户必须位于 NetScaler ADM 安全数据库中。如果在外部对用户进行身份验证，用户“外部名称”必须匹配向身份验证服务器注册的外部用户标识，具体取决于选定的身份验证协议。

NetScaler 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。NetScaler 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进行外部身份验证的 NetScaler ADM 实现时，请求的应用程序服务器会将用户名和密码发送到 RADIUS、LDAP 或 TACACS 服务器进行身份验证。如果身份验证成功，则授予用户访问 NetScaler ADM 的权限。

外部身份验证服务器

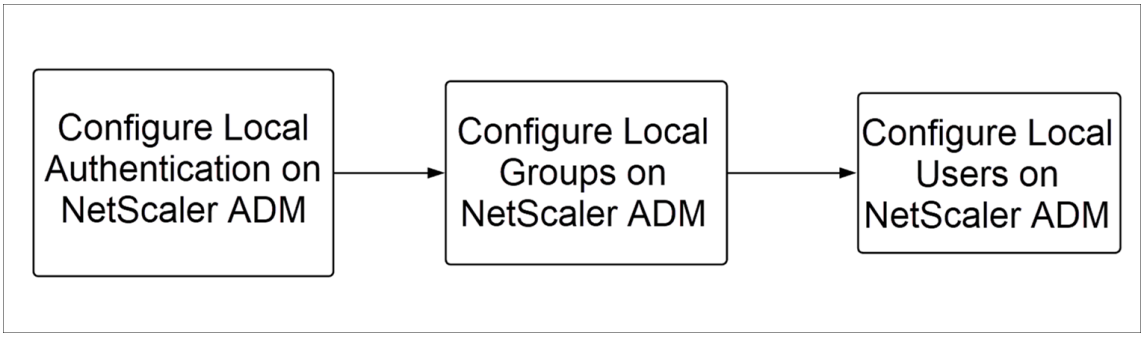
NetScaler ADM 将所有身份验证、授权和审核服务请求发送到远程 RADIUS、LDAP 或 TACACS 服务器。远程身份验证、授权和审核服务器接收请求、验证请求并向 NetScaler ADM 发送响应。当配置为使用远程 RADIUS、TACAS 或 LDAP 服务器进行身份验证时，NetScaler ADM 将成为 RADIUS、TACAS 或 LDAP 客户端。在其中任何配置中，身份验证记录都存储在远程主机服务器数据库中。帐户名称、分配的权限和时间记帐记录也存储在每个用户的身份验证、授权和审核服务器上。

此外，您可以使用 NetScaler 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。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。

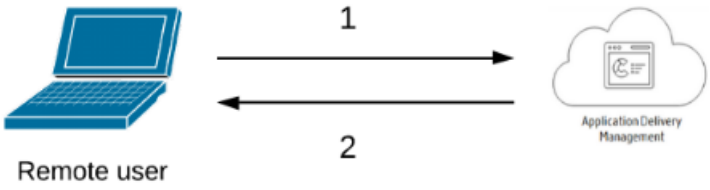
在 **NetScaler ADM** 中对用户进行身份验证

您可以通过两种方式在 NetScaler ADM 中对用户进行身份验证：

- 在 NetScaler ADM 中配置的本地用户



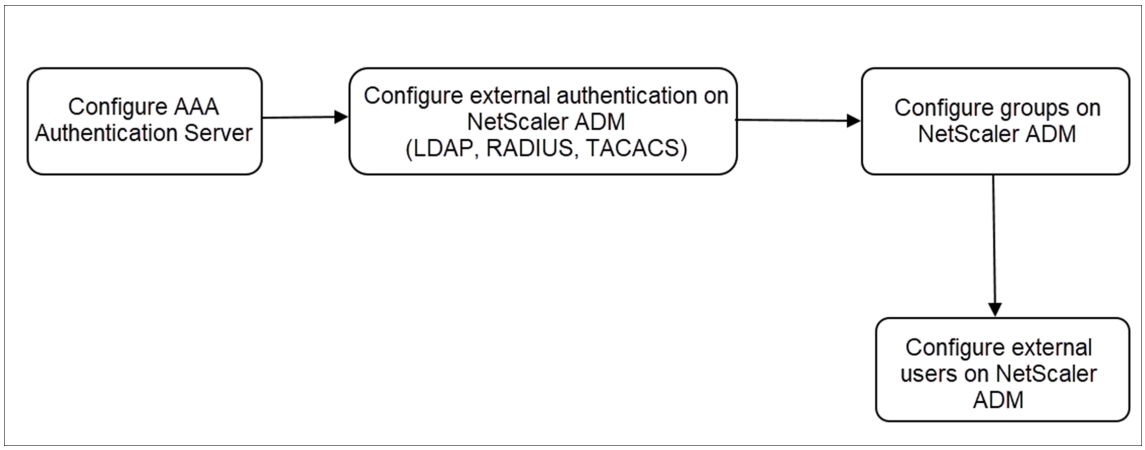
配置完成后，以下是在本地服务器中进行用户身份验证的工作流。



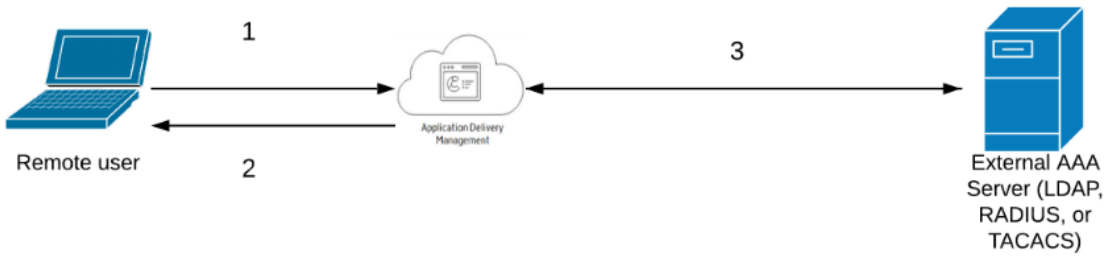
1 —用户登录 NetScaler ADM

2 —NetScaler ADM 提示用户提供身份验证凭据，并检查 ADM 数据库中的凭据是否匹配。

- 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 —用户连接到 NetScaler ADM

2 —NetScaler ADM 提示用户输入凭据

3 —NetScaler 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 **NetScaler ADM** 中配置外部身份验证服务器

February 6, 2024

配置 LDAP、RADIUS 或 TACAS 服务器后，可以在 NetScaler ADM 中添加这些服务器。

添加 **LDAP** 身份验证服务器

February 6, 2024

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“设置”**>**“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 页面上，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，则可以通过选择传输层安全 (TLS) 或 SSL 来选择加密通信

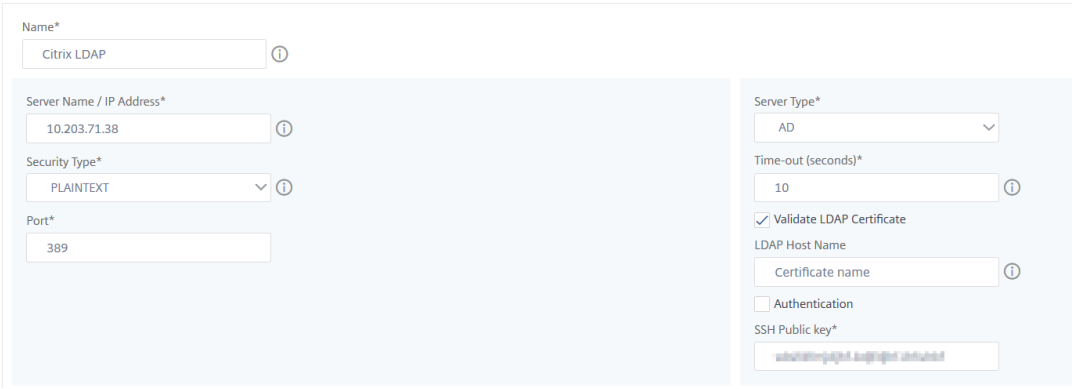
    d) 端口—默认情况下，端口 389 用于普通文本。您还可以为 SSL/TLS 指定端口 636

    e) 服务器类型—选择 Active Directory (AD) 或 Novell Directory Service (NDS) 作为 LDAP 服务器的类型

    f) 超时（秒）—NetScaler 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上输入的主机名

    清除“身份验证”选项并指定 SSH 公钥。使用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。

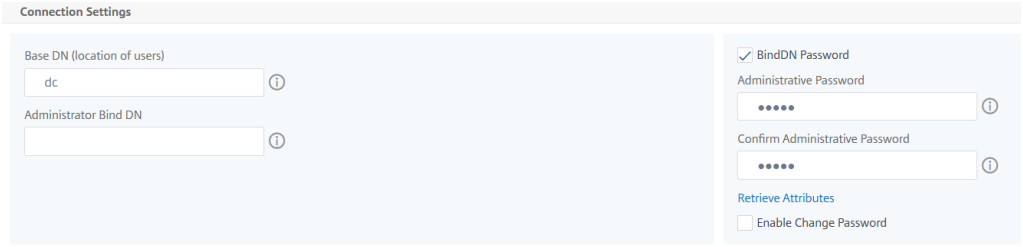
    在“连接设置”下，指定以下参数：

    i. 基本 **DN** —LDAP 服务器开始搜索的基本节点

    ii. 管理员绑定 **DN** —绑定到 LDAP 服务器的用户名。例如，admin@aaa.local。

iii. 绑定 **DN** 密码 -选择此选项可提供用于身份验证的密码

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 **samAccountname**。

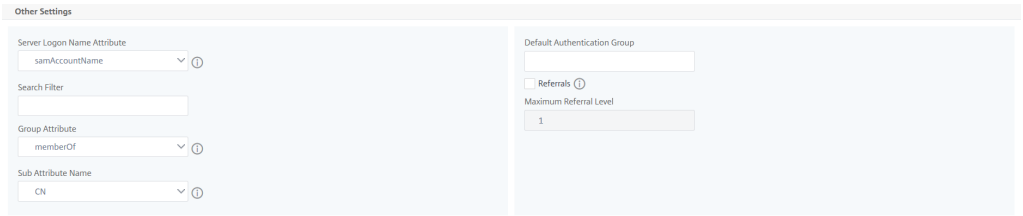
ii. 搜索筛选 器—根据 LDAP 服务器中配置的搜索筛选器配置外部用户进行双重身份验证。例如，vpnallowed=true 使用 ldaploginame `samaccount` 和用户提供的用户名 Bob 将产生一个 LDAP 搜索字符串: &(`vpnallowed`=**`true`**)(`samaccount`=`bob`)。

> 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—从 LDAP 服务器提取组的子属性名称。

v. 默认身份验证组 -除提取的组外，还可选择身份验证成功时的默认组。



4. 单击创建。

   LDAP 服务器现已配置完毕。

   > 注意：
   >
   > 如果用户是 Active Directory 组成员，则该组和 NetScaler ADM 上的用户名必须具有相同的 Active Directory 组成员的名称。

5. 启用外部身份验证服务器。

   有关启用外部身份验证服务器的详细信息，请参阅启用外部身份验证服务器和回退选项。

添加 **RADIUS** 身份验证服务器

February 6, 2024

1. 导航到“设置”**>**“身份验证”。
2. 选择 **RADIUS** 选项卡，然后单击 添加。

   在 创建 **RADIUS** 服务器 页面上，指定以下参数：

   a) 名称 -指定 RADIUS 服务器名称

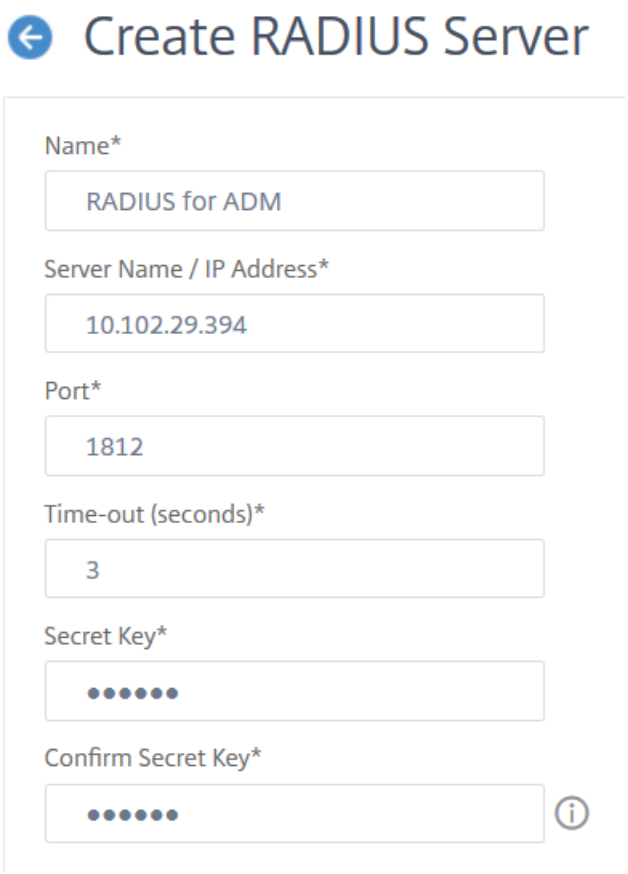
   b) 服务器名称**/ IP** 地址 -指定 RADIUS 服务器 IP 地址

   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）—NetScaler 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** —指定要将标识符发送到 RADIUS 服务器的 ID

ii. 组供应商标识符 -指定使用 RADIUS 组提取的供应商 ID

iii. 组前缀 -用于提取 RADIUS 组的 RADIUS 属性中组名称之前的字符串

iv. 组属性类型 -指定 RADIUS 组提取的属性类型

v. 组分隔符 -用于分隔 RADIUS 组提取的 RADIUS 属性内的组名的字符串

vi. **IP** 地址供应商标识符—RADIUS 中的供应商 ID 表示内联网 IP。值为 0 表示该属性未经过供应商编码

vii. 密码供应商标识符—RADIUS 响应中的供应商 ID 密码，用于提取用户密码

viii. **IP** 地址属性类型—RADIUS 响应的远程 IP 地址属性

ix. 密码属性类型 -RADIUS 响应的密码属性

x. 密码编码—从列表中选择 pap、chap、mschapv1 或 mschapv2。这表示在从系统传输到 RADIUS 服务器的 RADIUS 数据包中应如何对密码进行编码。

xi. 默认身份验证组 -除提取的组外，还可选择身份验证成功时的默认组

如果您希望设备在 RADIUS 服务器上记录审核信息，请选择“记账”。

3. 单击创建。

现在已配置 RADIUS 服务器。

4. 启用外部身份验证服务器。

有关启用外部身份验证服务器的详细信息，请参阅启用外部身份验证服务器和回退选项。

添加 **TACACS** 身份验证服务器

February 6, 2024

1. 导航到“设置”**>**“身份验证”。
2. 选择 **TACACS** 选项卡，然后单击添加。
3. 在创建 **TACACS** 页面上，指定以下参数：

a) 名称 -指定 TACACS 服务器名称

b) **IP** 地址—指定 TACACS 的 IP 地址

c) 端口 -指定托管 TACACS 服务器的端口号。默认端口为 49

d) 超时（秒）—NetScaler ADM 系统等待 LDAP 服务器响应的时间（以秒为单位）

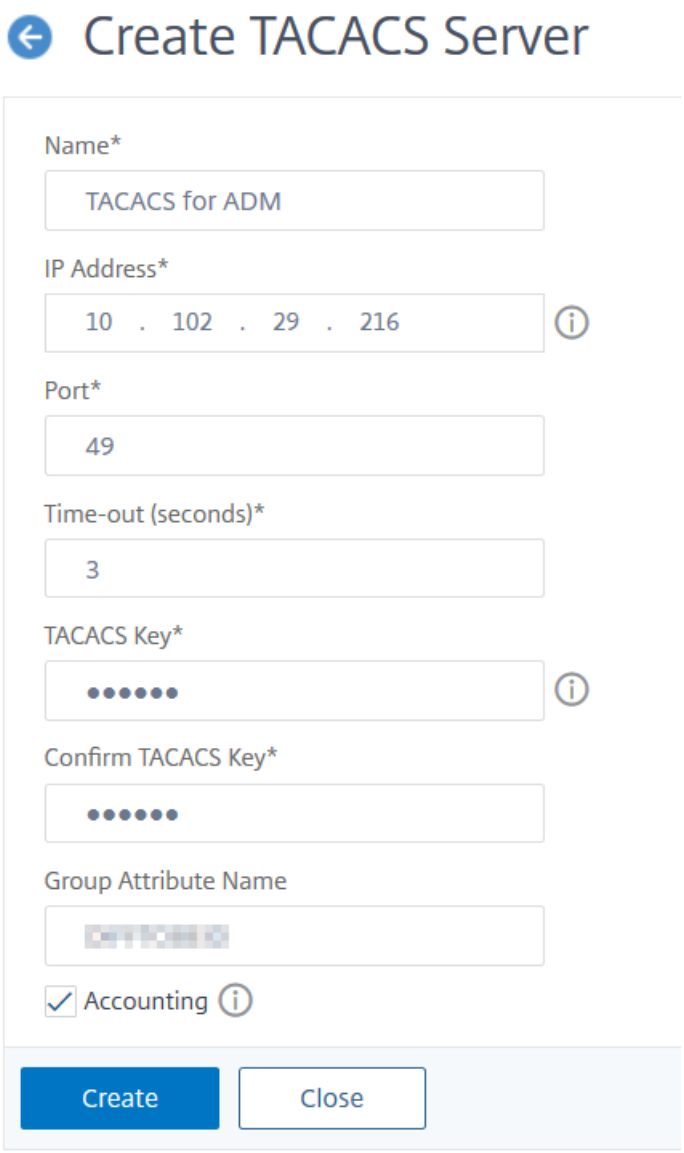
e) **TACACS** 密钥—指定 TACACS 密钥进行身份验证

f) 确认 **TACACS** 密钥—再次指定 TACACS 密钥进行确认

g) 组属性名称 -指定组名

如果您希望设备在 TACACS 服务器上记录审核信息，请选择“会计”。

4. 单击创建。



5. 启用外部身份验证服务器。

有关启用外部身份验证服务器的详细信息，请参阅启用外部身份验证服务器和回退选项。

NetScaler ADM 中的用户

February 6, 2024

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

有关配置用户的详细信息，请参阅 配置用户。

> 注意
>
> 如果用户在 Active Directory 上，请确保 NetScaler ADM 中的组名与外部服务器上 Active Directory 组的组名相同。

NetScaler ADM 中的用户组

NetScaler 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。一个组可以拥有“管理员”或“只读”权限，该组中的所有用户都将获得同等的权限。

在 NetScaler ADM 中：

- 组被定义为具有相似权限的用户的集合
- 一个组可以有一个或多个角色
- 用户被定义为可以根据分配的权限拥有访问权限的实体
- 一个用户可以属于一个或多个组

您可以在 NetScaler ADM 中创建本地组，并对组中的用户使用本地身份验证。如果您使用外部服务器进行身份验证，请在 NetScaler ADM 上配置组，使其与内部网络中身份验证服务器上配置的组相匹配。当用户登录并通过身份验证时，如果组名与身份验证服务器上的组匹配，则用户将继承 NetScaler ADM 上该组的设置。
如果您使用本地身份验证，请创建用户并将其添加到在 NetScaler 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

February 6, 2024

> 注意
>
> **NetScaler ADM 13.0** 支持 TACACS 服务器提取。

NetScaler ADM 使您能够：

- 在外部身份验证服务器上提取用户所属的组列表。
- 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 NetScaler ADM 中创建用户，因为这些用户在外部服务器上进行管理。
- NetScaler 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。

启用外部身份验证服务器和备用选项

February 6, 2024

Fallback 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 NetScaler ADM 和外部身份验证服务器上配置的用户可以登录 NetScaler ADM，即使配置的外部身份验证服务器已关闭或无法访问。要确保备用身份验证正常运行，请执行以下操作：

- 如果外部服务器已关闭或无法访问，非 nsroot 用户必须能够访问 NetScaler ADM
- 必须添加至少一台外部服务器

NetScaler ADM 还支持统一的身份验证、授权和记账系统 (AAA) 协议（LDAP、RADIUS 和 TACACS）以及本地身份验证。这种统一支持提供了一个通用接口，用于对访问系统的所有用户和外部 AAA 客户端进行身份验证和授权。

无论用户要与系统通信的实际协议如何，NetScaler 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，NetScaler 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 NetScaler 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，假设您要添加四台外部身份验证服务器并配置两台 RADIUS 服务器、一台 LDAP 服务器和一台 TACACS 服务器。NetScaler ADM 尝试根据配置向外部服务器进行身份验证。在此示例场景中，NetScaler ADM 尝试：

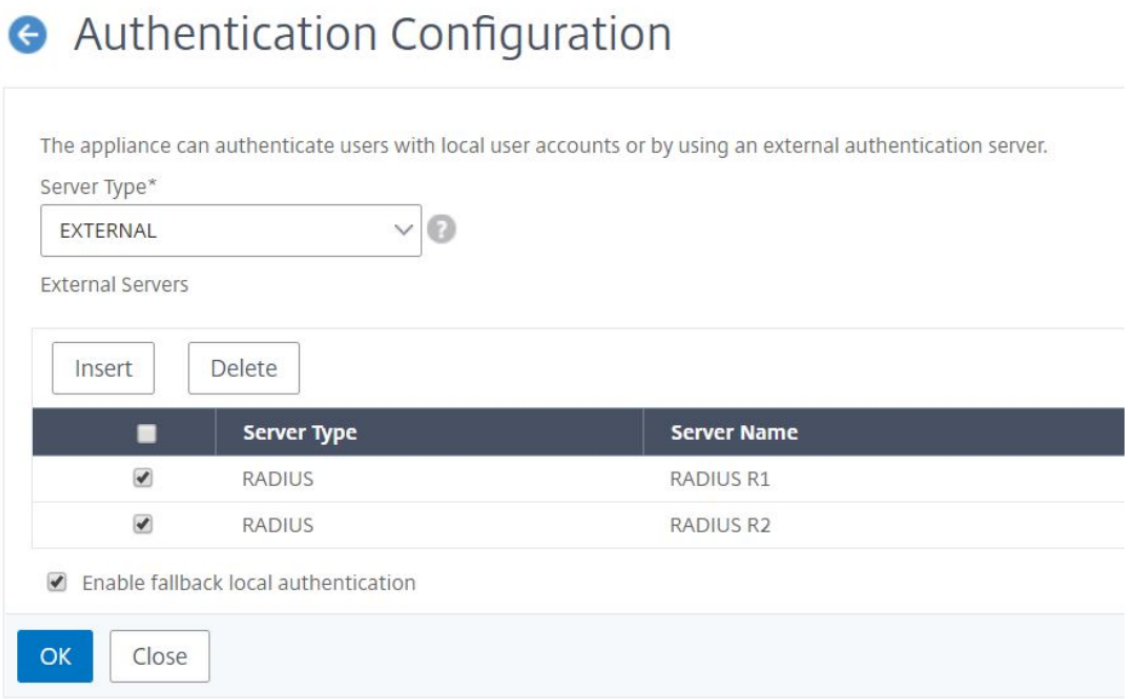
- 连接第一台 RADIUS 服务器
- 如果第一个 RADIUS 服务器的身份验证失败，请连接第二个 RADIUS 服务器
- 如果两台 RADIUS 服务器的身份验证均失败，请连接 LDAP 服务器
- 如果 RADIUS 服务器和 LDAP 服务器的身份验证均失败，请连接 TACACS 服务器。

> 注意
>
> 您可以在 NetScaler 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“设置”**>**“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”页面上，从“服务器类型”列表中选择 **EXTERNAL**（只能级联外部服务器）。
4. 单击“插入”，然后在“外部服务器”页面上，选择一个或多个要级联的身份验证服务器。
5. 如果您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. 如果要在系统审核 日志中捕获外部用户组信息，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

February 6, 2024

身份验证是验证某人是否属实的过程。为了执行身份验证，用户必须已在身份验证机制可以查询的系统中创建了帐户，或必须在首次身份验证过程中创建帐户。NetScaler 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。虽然本地用户需要在内部进行身份验证，但 NetScaler ADM 支持使用 RADIUS、LDAP 和 TACACS 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 NetScaler 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。经过身份验证后，将使用所需的协议在 NetScaler ADM 上识别用户。

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。NetScaler ADM 允许基于角色的精细访问控制 (RBAC)，管理员可以通过该控制根据企业内单个用户的角色向用户提供访问权限。NetScaler 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

February 6, 2024

NetScaler ADM 提供基于角色的精细访问控制 (RBAC)，您可以使用它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 NetScaler ADM 中，创建角色和策略特定于 NetScaler 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 NetScaler 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 证书管理和监视的完全访问权限，但对系统管理操作也具有只读访问权限。

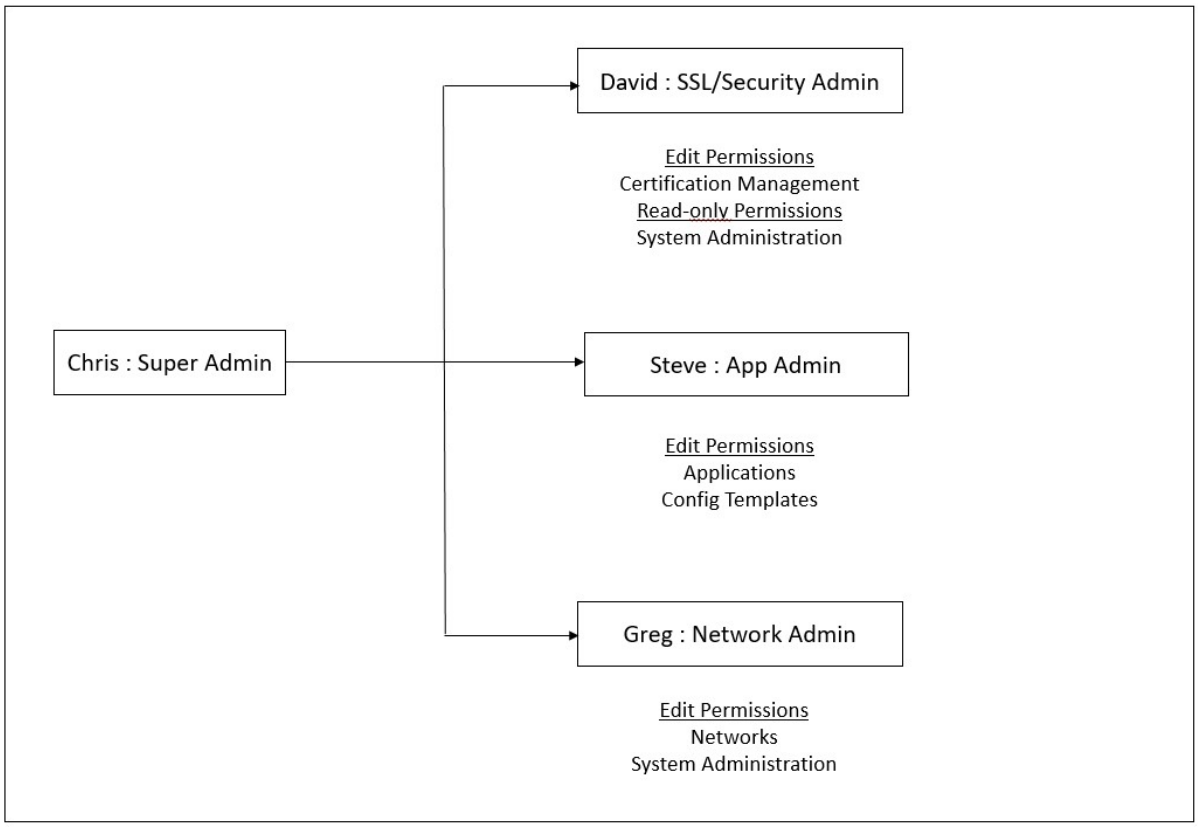
应用程序管理员 Steve 需要只对特定应用程序和特定配置模板拥有访问权限。

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。

NetScaler 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 NetScaler ADM 功能不完全支持 RBAC：

- 分析-分析 模块中不完全支持 RBAC。RBAC 支持仅限于实例级别，不适用于 Web Insight、SSL Insight、Gateway Insight、HDX Insight 和 WAF 安全违规分析模块中的应用程序级别。例如：

示例 **1**：基于实例的 RBAC（支持）

分配了几个实例的管理员只能在 **Web Insight** > 实例下看到这些实例，只能在 **Web Insight** > 应用程序下看到相应的虚拟服务器，因为实例级别支持 RBAC。

示例 **2**：基于应用程序的 RBAC（不支持）

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，因为应用程序级别不支持 RBAC。

- 样书—样书不完全支持 RBAC。
  - 在 NetScaler 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 NetScaler 实例上的配置，即使他们无权访问该实例。
- 调配 -调配不支持 RBAC。

配置访问策略

February 6, 2024

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。NetScaler Application Delivery Management (ADM) 提供四种预定义的访问策略：

1. 管理员政策。授予访问所有 NetScaler ADM 功能的权限。用户具有查看和编辑权限，可以查看所有 NetScaler 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. **readonlypolicy**。授予只读权限。用户可以查看 NetScaler ADM 上的所有内容，但无权执行任何操作。
3. **appAdminPolicy**。授予用于访问 NetScaler 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，内容切换、缓存重定向和 HAProxy 虚拟服务器。
4. **appReadOnlyPolicy**。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：
>
> 无法编辑预定义的策略。

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 NetScaler ADM 中，导航到“设置”**>**“用户和角色”**>**“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 NetScaler ADM 功能，其中包含指定只读、启用禁用或编辑访问权限的选项。

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：此选项允许用户在 NetScaler ADM 中查看该功能。
   - 启用-禁用：此选项仅适用于允许在 NetScaler 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。

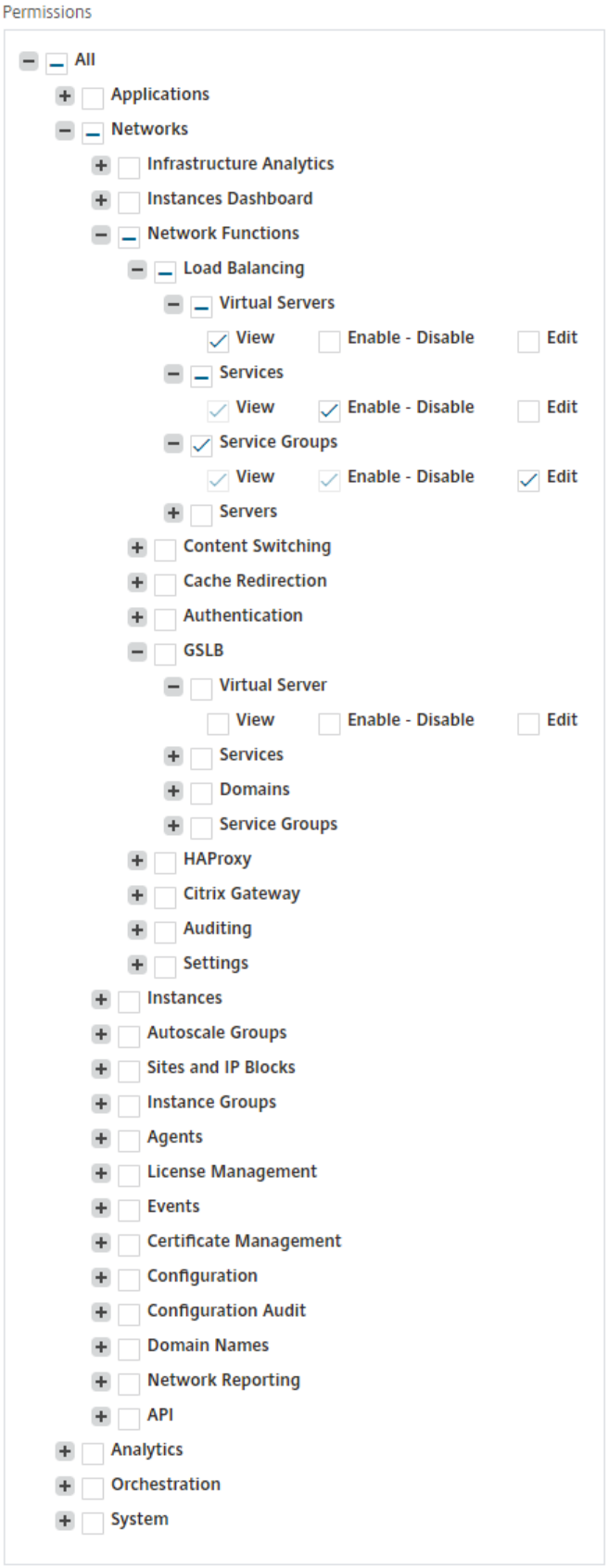
     向用户授予“启用-禁用”权限时，也会授予“查看”权限。您不能取消选择此选项。
   - 编辑：此选项向用户授予完全访问权限。用户可以修改该功能及其功能。

     如果您授予“编辑”权限，则会同时授予“查看”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，它将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 NetScaler 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 基础结构 **>** 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 基础结构 **>** 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，则在以下页面中限制对服务的启用或禁用操作：
>
> a) 导航到 基础结构 **>** 网络功能。
>
> b) 选择一个虚拟服务器，然后单击 配置。
>
> c) 选择负 载平衡虚拟服务器服务绑定 页面。
> 如果您选择“启 用”或“禁用”，则此页面会显示一条错误消息。

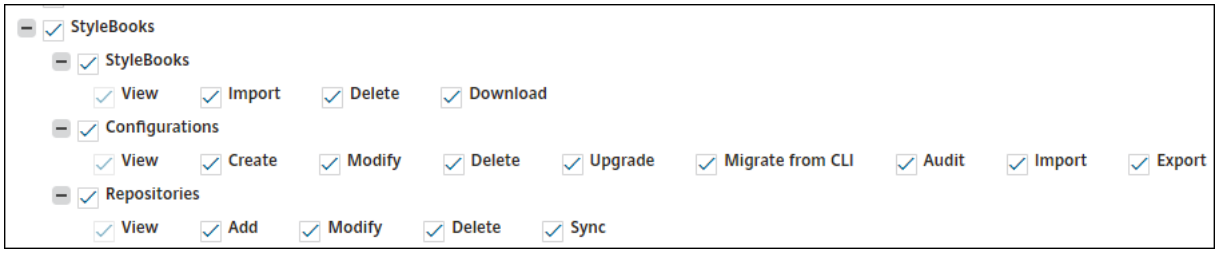
“编辑”权限被授予用户使用“服务组”功能。此权限授予完全访问权限，授予了“查看”和“启用-禁用”权限。用户可以修改绑定到负载平衡虚拟服务器的服务组。要编辑服务组，请导航到 基础结构 **>** 网络功能 **>** 负载平衡，然后选择 服务组 选项卡。

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，“查看”权限会自动启用。



配置组

February 6, 2024

在 NetScaler 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 NetScaler 实例；另一组用户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 NetScaler ADM 中分配相同的访问权限。

您可以在 NetScaler ADM 中管理网络功能实体的各个级别的用户访问权限。您可以在实体级别为用户或组动态分配特定权限。

NetScaler ADM 将虚拟服务器、服务、服务组和服务器视为网络功能实体。

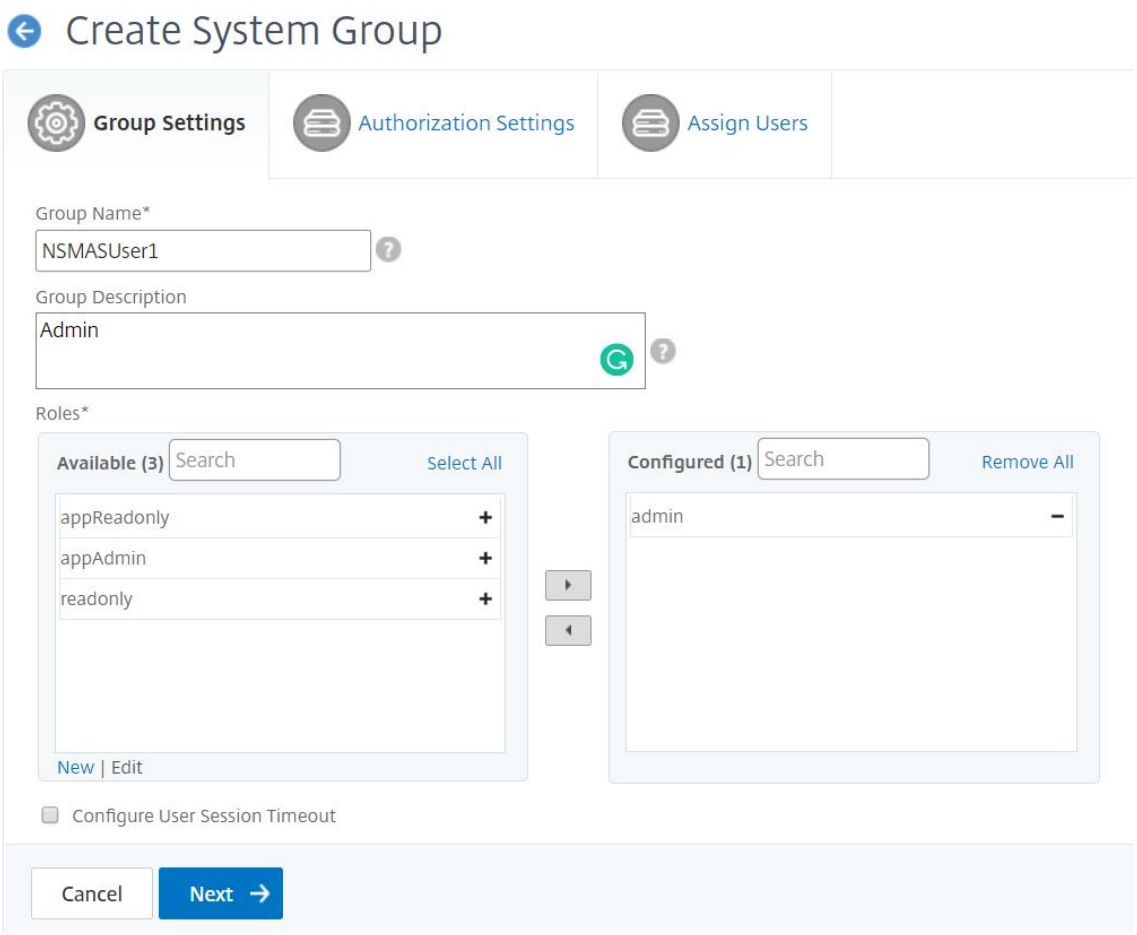
- 虚拟服务器（应用程序） - 负载平衡 (lb)、GSLB、上下文切换 (CS)、缓存重定向 (CR)、身份验证 (Auth) 和 NetScaler Gateway (VPN)
- 服务 -负载平衡和 GSLB 服务
- 服务组 -负载平衡和 GSLB 服务组
- 服务器 -负载平衡服务器

创建用户组

1. 在 NetScaler ADM 中，导航 到设置 **>** 用户和角色 **>** 组。
2. 单击添加。

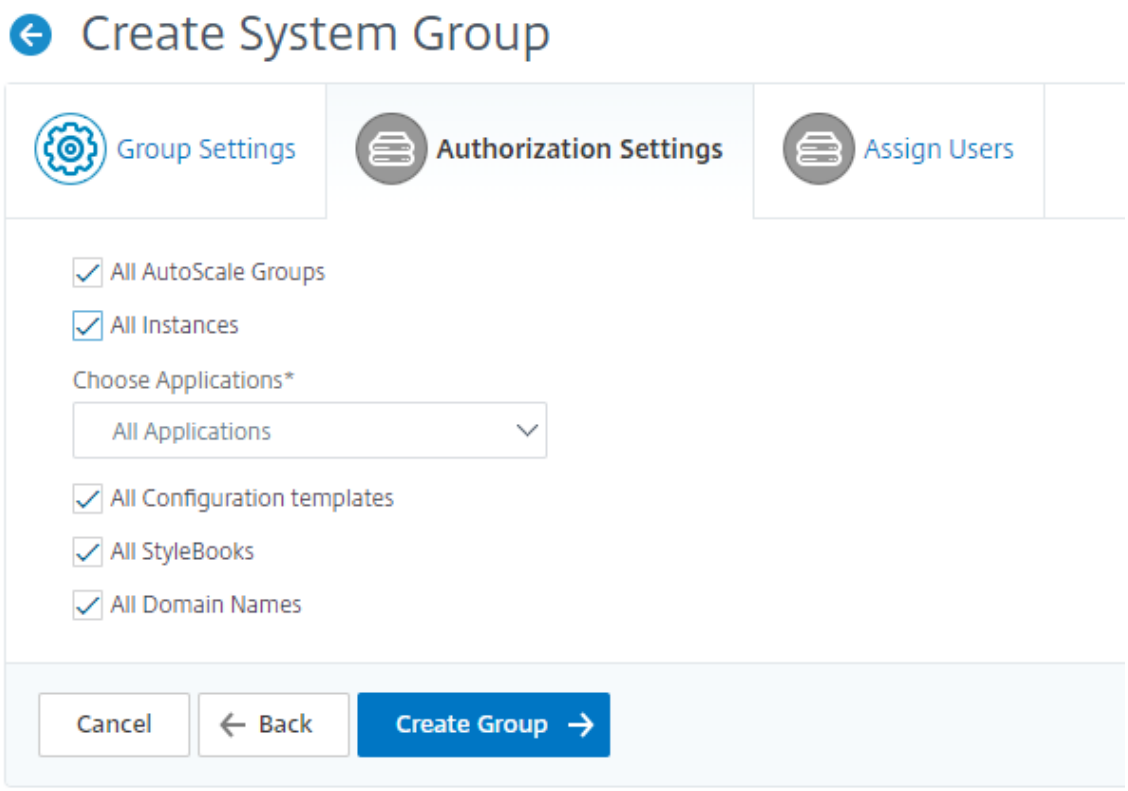
   屏幕上将显示“创建系统组”页面。
3. 在 组名称 字段中，输入组的名称。
4. 在“组描述”字段中，键入组的描述。对小组进行良好的描述有助于您在以后更好地了解该组的角色和职能。
5. 在“角色”部分中，将一个或多个角色添加或移动到“已配置”列表中。

   > 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“设置” **>** “用户和角色” **>** “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：

   - AutoScale 组
   - 实例
   - 应用程序
   - 配置模板
   - 样书
   - 配置包
   - 域名



您可能需要从用户可以访问的类别中选择特定资源。

AutoScale 组：

如果要选择用户可以查看或管理的特定 Autoscale 组，请执行以下步骤：

a) 清除“所有 **AutoScale** 组”复选框，然后单击“添加 **AutoScale** 组”。

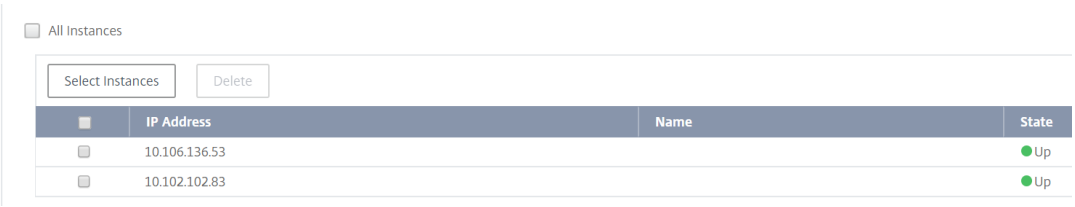
b) 从列表中选择所需的 AutoScale 组，然后单击“确定”。

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。

您可以向应用程序授予访问权限，而无需选择其实例。因为应用程序独立于其实例来授予用户访问权限。

当您向用户授予应用程序访问权限时，无论选择何种实例，该用户都有权仅访问该应用程序。

此列表为您提供了以下选项：

- 所有应用程序：默认情况下，此选项处于选中状态。它添加了 NetScaler ADM 中存在的所有应用程序。
- 选定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，此选项才会出现。它添加了选定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所需应用程序。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功能实体和相应的实体。

  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，如果您选择一个应用程序并选择“在绑定实体上应用”，则 NetScaler ADM 会对绑定到所选应用程序的所有实体进行授权。

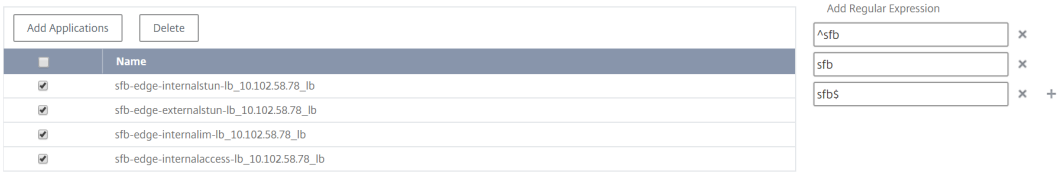
  > 注意：
  >
  > 如果要授权绑定实体，请确保只选择了一种实体类型。

您可以使用正则表达式搜索和添加符合组正则表达式条件的网络函数实体。指定的正则表达式保留在 NetScaler ADM 中。要添加正则表达式，请执行以下步骤：

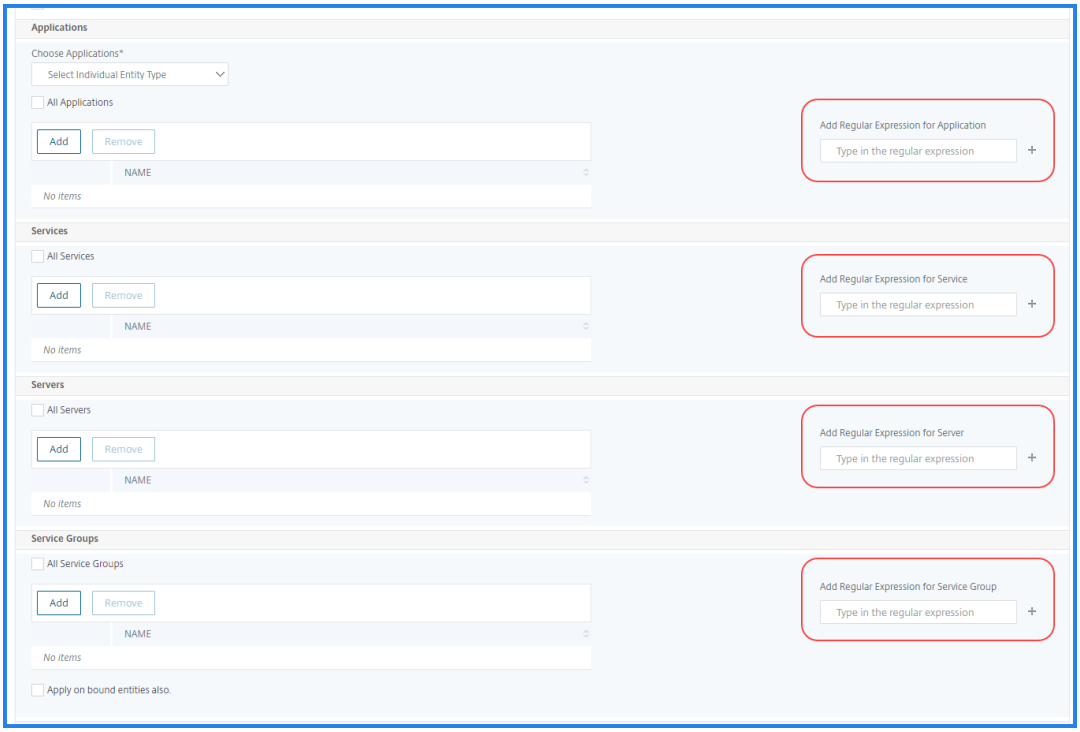
a) 单击“添加正则表达式”。

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。

如果您为已发现的 实体选择“同时应用于绑定 实体”选项，则用户可以自动访问绑定到已发现实体的实体。

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，NetScaler ADM 会将授权范围更新到新实体。

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”。

样书：

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 所有样书 复选框，然后单击 将样书添加到组。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”窗格中选择样书，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：

```
name=lb-mon|lb AND namespace=com.citrix.adc.stylebooks AND
    version=1.0
<!--NeedCopy-->
```

此查询列出了满足以下条件的样书：

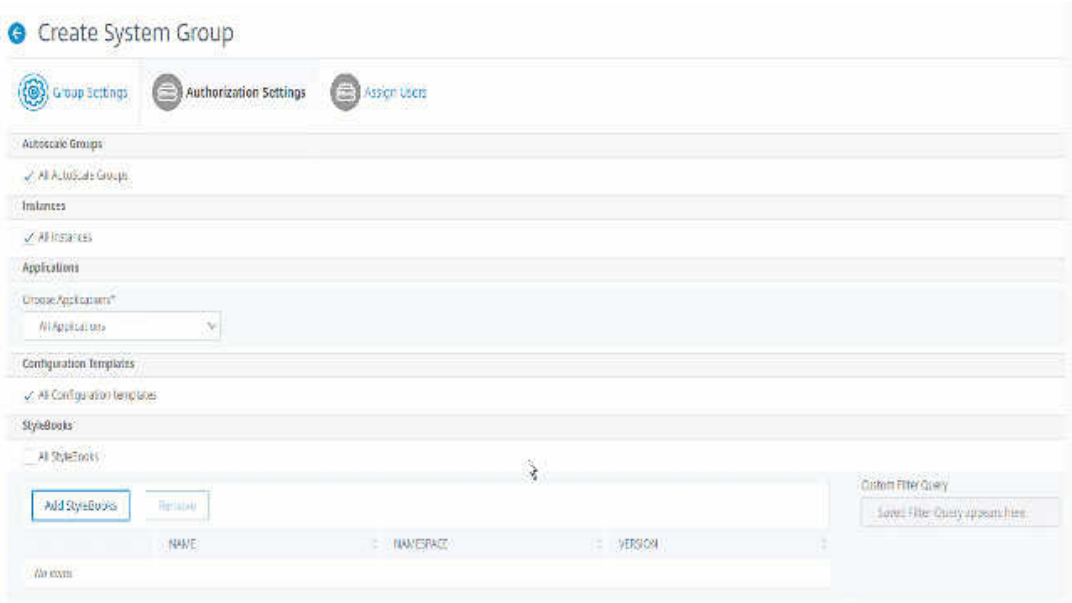
- 样书名称是 lb-mon 或 lb。
- 样书名称空间是 com.citrix.adc.stylebooks。
- 样书版本是 1.0。

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书，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书。当用户选择允许的样书时，也会选择所有相关样书。

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：

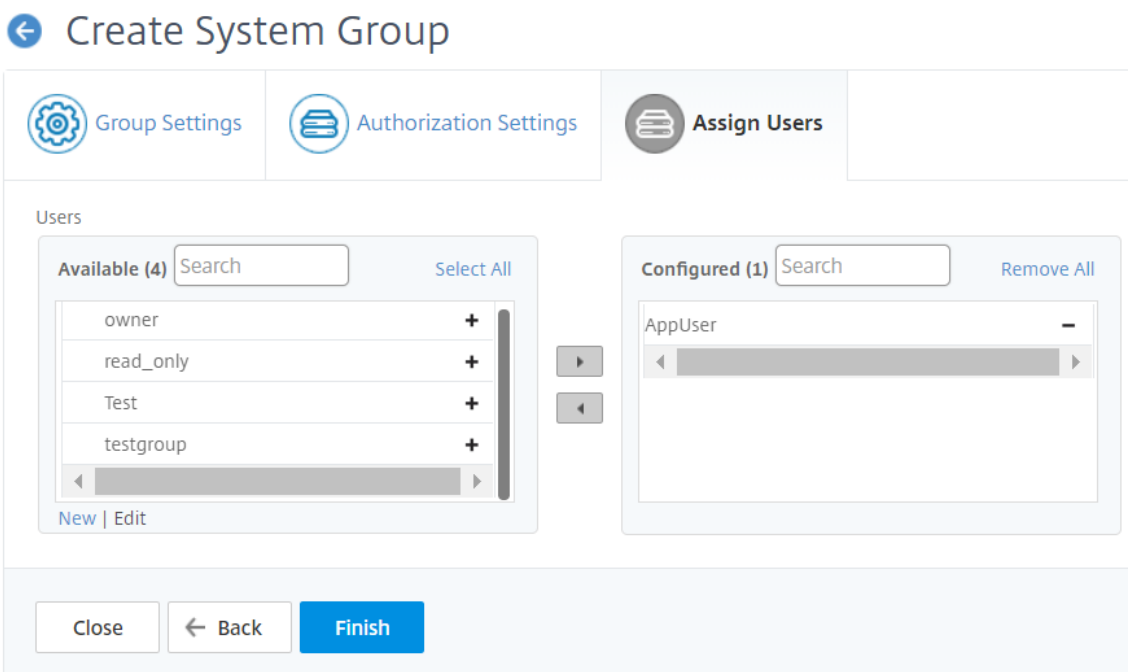
如果要选择用户可以查看或管理的特定域名，请执行以下步骤：

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”部分中，在“可用”列表中选择用户，然后将该用户添加到“已配置”列表中 **。

> 注意：
>
> 您也可以通过单击“新建”来添加用户。



9. 单击完成。

管理多个网络功能实体之间的用户访问权限

作为管理员，您可以在 NetScaler ADM 中管理网络功能实体的各个级别的用户访问权限。而且，您可以使用正则表达式筛选器在实体级别向用户或组动态分配特定权限。

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 NetScaler ADM 上配置组 。

使用方案：

假设一个或多个应用程序（虚拟服务器）托管在同一台服务器上的场景。超级管理员 (George) 只想向 Steve (应用程序管理员) 授予对 App1 的访问权限，而不想授予对托管服务器的访问权限。

下表说明了这种环境，其中 Server-A 托管应用程序 App-1 和 App-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
>
> NetScaler ADM 将虚拟服务器、服务、服务组和服务器视为网络功能实体。实体类型的虚拟服务器被称为应用程序。

为了向网络功能实体分配用户权限，George 将用户授权定义如下：

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 App-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，George 选择了 Steve 的用户个人资料。
7. 单击完成。

使用此授权设置，Steve 只能管理 App-1，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，NetScaler ADM 会授予绑定到 App-1 的所有网络功能实体的访问权限。因此，还授予对托管服务器的访问权限。

超级管理员可以为每种实体类型指定正则表达式（regex）。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，NetScaler 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 将应用程序实体类型添加 App* 为正则表达式，匹配正则表达式条件的应用程序出现在列表中。使用此授权设置，Steve 可以访问与正则 App* 表达式匹配的所有应用程序。但是，他的访问权限仅限于应用程序，不限于托管服务器。

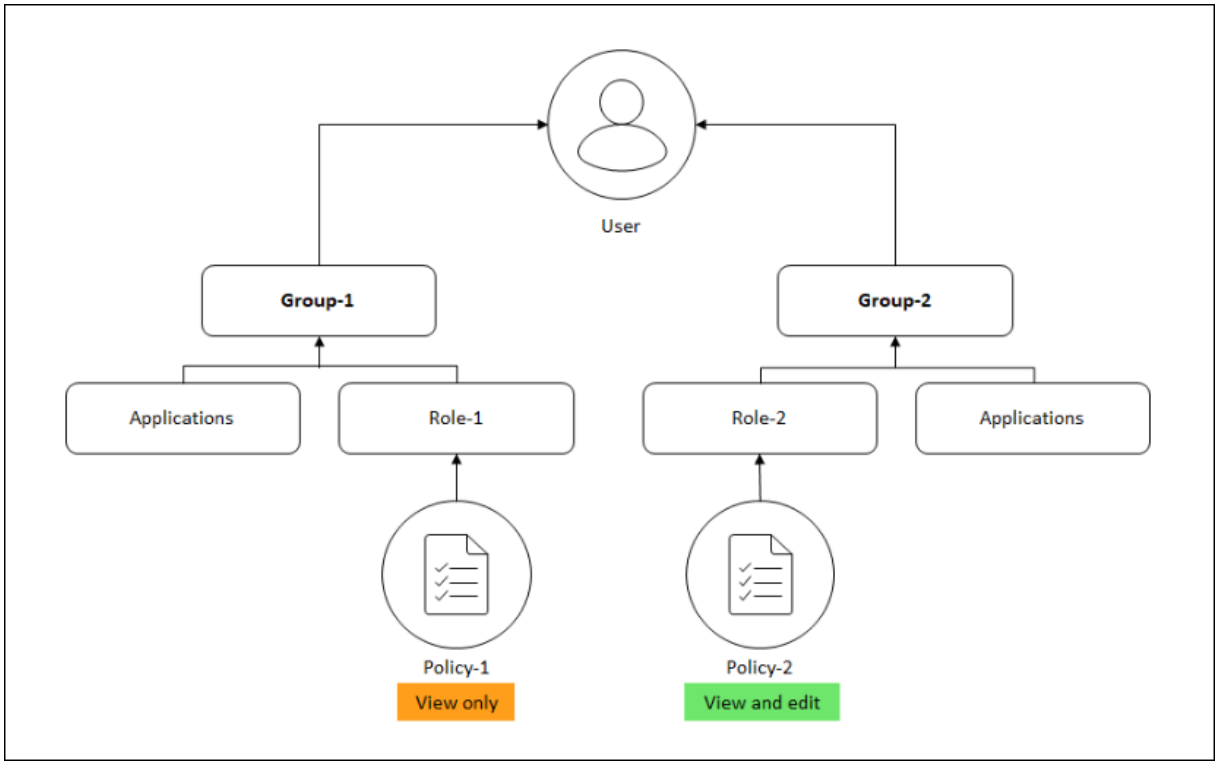
用户访问权限如何根据授权范围进行更改

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 根据特定的授权范围向用户授予应用程序访问权限。

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。
- **Policy-2** -查看和编辑应用程序的权限。



用户可以查看 Policy-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 **NetScaler ADM** 从 **12.0** 升级到更高版本时的 **RBAC** 映射

将 NetScaler ADM 从 12.0 升级到 13.1 时，您看不到在创建组时提供“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版本 13.1：

12.0	仅允许应用程序	13.1
admin read-write	False	`admin`

12.0	仅允许应用程序	13.1
admin read-write	True	`appAdmin`
admin read-only	False	`readonly`
admin read-only	True	`appReadonly`

配置角色

February 6, 2024

在 NetScaler 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 NetScaler ADM 中添加 NetScaler 实例的权限，另一个策略可能授予创建和部署样书以及配置 NetScaler 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。

NetScaler ADM 提供四个预定义角色：

- **admin**。可以访问所有 NetScaler ADM 功能。（此角色绑定到 adminpolicy。）
- **readonly**。拥有只读访问权限。（此角色绑定到 readonlypolicy。）
- **appAdmin**。仅对 NetScaler ADM 中的应用程序功能具有管理访问权限。（此角色绑定到 appAdminPolicy。）
- **appReadonly**。对应用程序功能拥有只读访问权限。（此角色绑定到 appReadOnlyPolicy。）

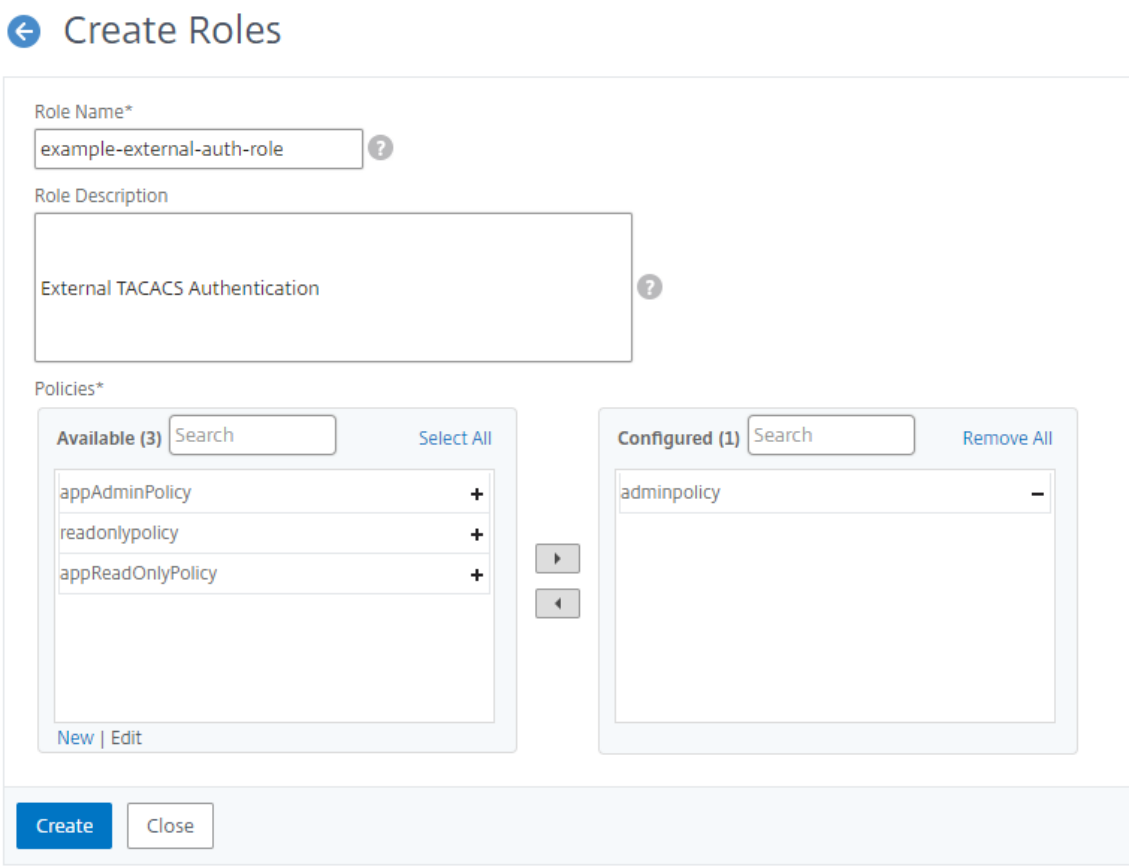
> 注意：
>
> 无法编辑预定义的角色。

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 NetScaler ADM 中，导航到“设置”**>**“用户和角色”。
2. 单击添加。
3. 在“角色名称”字段中，输入角色的名称，然后在“角色描述”字段中提供描述（可选）。

4. 在“策略”部分中，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

February 6, 2024

默认情况下，NetScaler Application Delivery Management (ADM) 只有一个用户：

nsroot - root 用户 (nsroot) 具有设备的完全管理权限。nsroot 用户是 NetScaler ADM 的超级管理员。

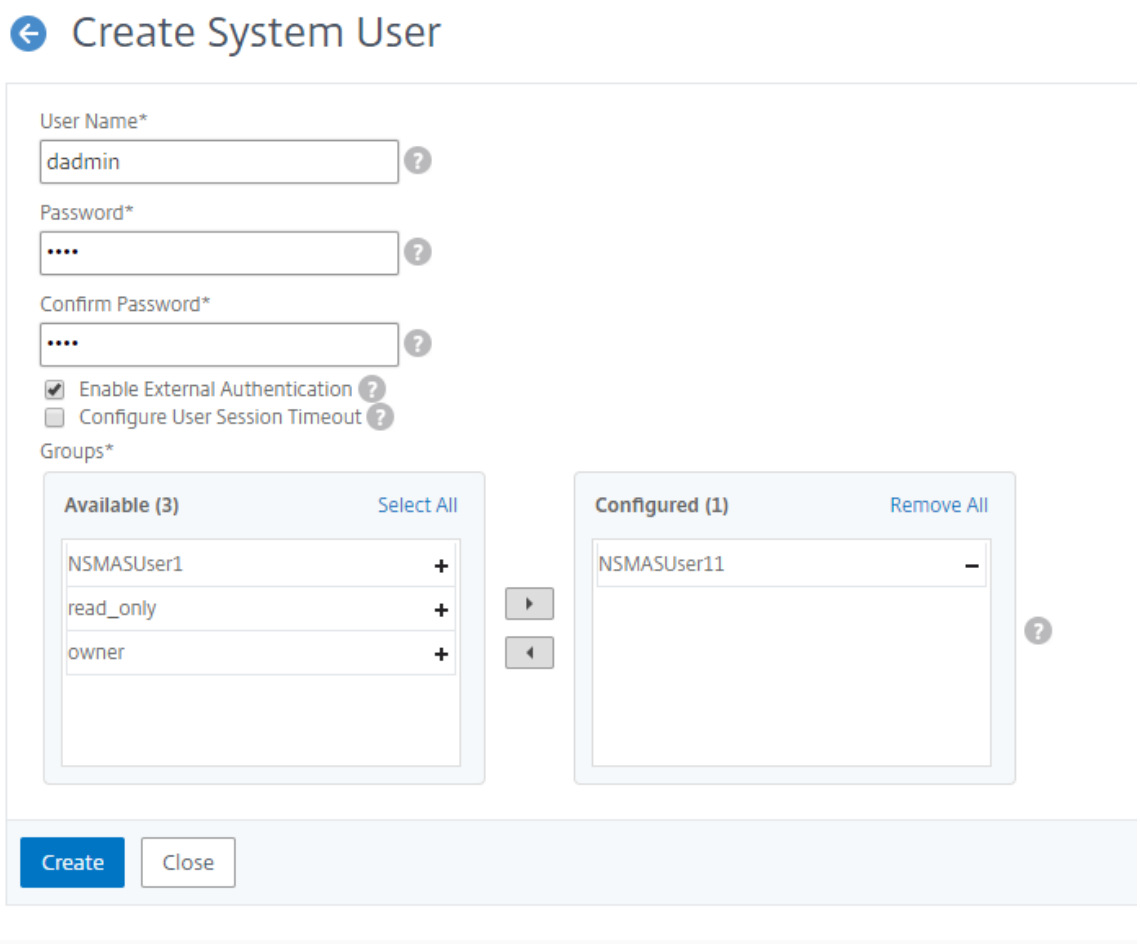
您可以创建其他用户，方法是为其配置帐户。将新用户添加到 NetScaler ADM 时，您可以通过分配相应的组、角色和策略来定义他们的权限。

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 **NetScaler ADM** 中配置用户，请执行以下操作：

1. 在 NetScaler ADM 中，导航到“设置”**>**“用户和角色”。

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 NetScaler ADM 时使用的密码
4. 或者，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. 如果您已创建组并想要将用户分配到组，请在“组”部分中，将一个或多个组从“可用”列表移至“已配置”列表。



6. 单击创建。

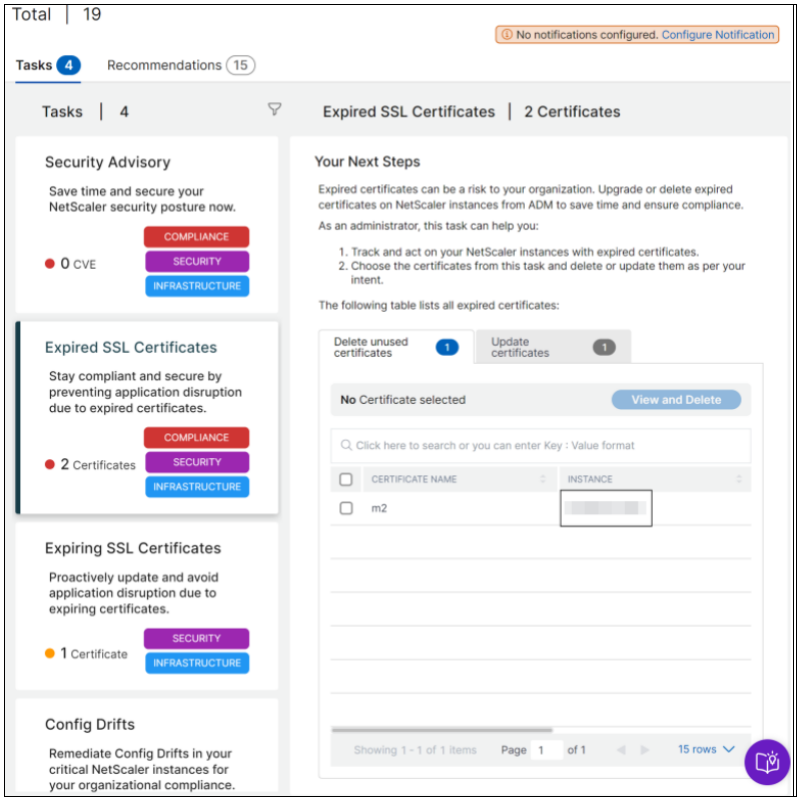
查看建议并高效管理您的 **ADC** 和应用程序

February 6, 2024

您可能发现了数百个 NetScaler 实例，并从每个 ADC 实例配置了多个虚拟服务器（应用程序）。作为管理员，您必须确保有效管理所有 NetScaler 实例和应用程序，以获得见解，从而更好地确定优先级和进行故障排除。

随着您进一步扩展基础架构，您可能还需要将注意力集中在需要立即关注的实例和应用程序上。NetScaler ADM 中的任务功能根据订阅和当前利用率提供建议，这些建议：

- 使用可操作的“引导我”工作流程，帮助管理员了解 NetScaler ADM 如何提供有效的部署。
- 通过完成任务或确认他们稍后完成，减少管理员的关键时间和精力。
- 确保管理员利用 NetScaler ADM 的所有功能，启用产品发现和产品推荐的功能，以有效管理部署。



在设置任务页面中，您可以查看以下选项卡：

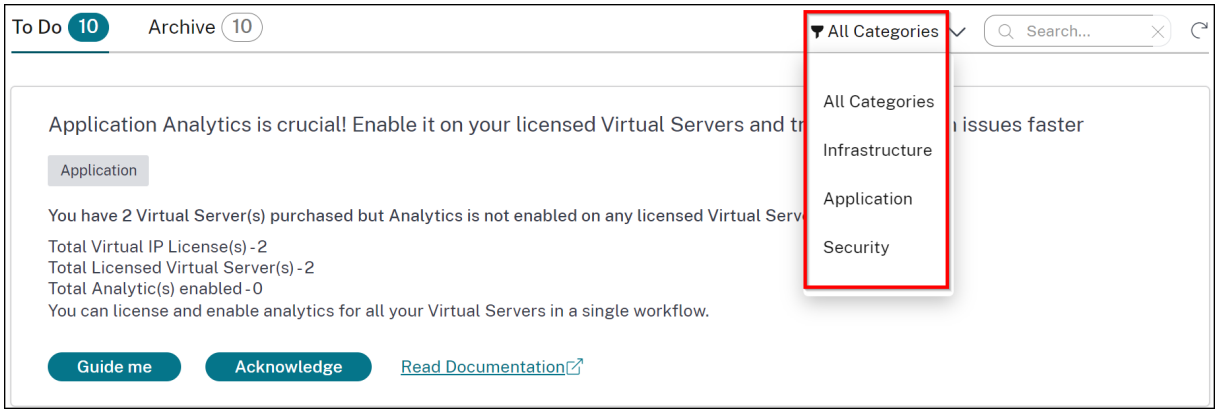
- 待办事项 - 使您能够查看建议列表。您可以查看并单击引导我完成任务，也可以单击“确认”跳过此任务。
- 存档 - 使您可以查看所有已完成或已确认任务的列表。您也可以使用“引导我”选项来完成经常性要求。

下表描述了您可以在 NetScaler ADM GUI 中查看的任务或建议：

建议名称	任务何时在 GUI 中可见？
添加 ADC 应用程序分析至关重要！在许可使用的虚拟服务器上将其启用，更快地对应用程序问题进行分类	在您加入 NetScaler ADM 之后，如果未发现 ADC 实例。 如果您有多个许可的虚拟服务器但未启用分析功能。

建议名称	任务何时在 GUI 中可见?
想要在您的 ADC 上重新分配带宽吗？很简单!	如果池许可证是在 ADC GUI 中分配的，并且在 NetScaler ADM 中发现了这些 ADC 实例，则可以使用 NetScaler ADM 进行重新分配。
从您的虚拟 IP 权利中获得更多价值！在发现的剩余虚拟服务器上启用更多虚拟 IP 许可证	如果您拥有所需的许可证，但未获得所有虚拟服务器的许可。
为您的关键企业用户启用基于精细角色的访问权限	如果尚未在 NetScaler ADM 中配置基于角色的访问控制 (RBAC)。
配置规则，切勿错过 ADC 实例上的任何关键事件	如果尚未配置自定义事件规则。
需要监视多个应用程序及其性能吗？只需创建一个自定义应用程序	如果尚未配置自定义应用程序。
避免应用程序中断，也不要错过应用程序中即将过期的 SSL 证书	如果没有为即将过期的 SSL 证书配置警报或通知
安全公告 - 使用 CVE 和缓解措施保持您的 ADC 处于最新状态	ADC 实例是否有任何 CVE 影响。
配置企业策略并监视是否存在任何偏差	如果 SSL 企业设置未更改或仍处于默认状态。
手动重复任务？创建配置作业并将其应用到多个 ADC	如果尚未配置作业任务。
通过选择您选择的自定义指标来管理和监视您的实例分数	如果未修改实例评分设置中的默认设置和阈值。
通过选择您选择的自定义指标来跟踪您的应用程序评分	如果默认使用应用程序控制板中的“应用程序评分”组件且未进行自定义。
添加专用 IP 块以在地理地图中可视化客户端请求	如果未配置 IP 块。您可以创建 IP 块，根据其专用 IP/范围在地理地图上映射和可视化客户端请求。
节省时间！使用样书简化应用程序部署和管理	如果尚未配置默认样式簿。
订阅您的 AppSec 违规行为并将其实时导出到 Splunk	如果尚未配置 NetScaler ADM 中的 Splunk 集成。
自定义默认阈值或为您的 Kubernetes 服务创建新的阈值	如果在服务图中仅使用默认阈值，并且不对服务应用任何单阈值或双阈值。
主动配置通知配置文件并在通信目的地接收通知	如果尚未配置通知配置文件。
安排定期导出并获取有关基础结构详细信息的通知	如果尚未在基础结构 **>** 实例中配置导出计划。
有 ServiceNow 并且想与 ADM 集成吗?	如果尚未配置 NetScaler ADM 中的 ServiceNow 集成。

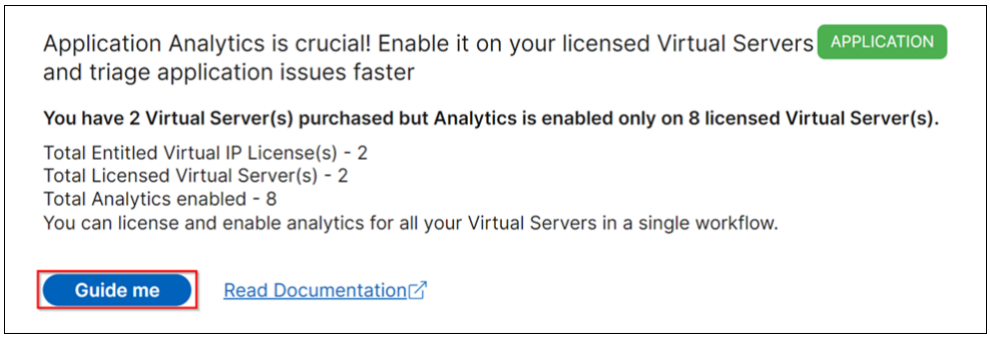
默认情况下，您可以查看前 5 个推荐。单击“显示全部”以查看所有推荐。您可以使用类别列表并选择一个类别，根据选择筛选特定推荐。



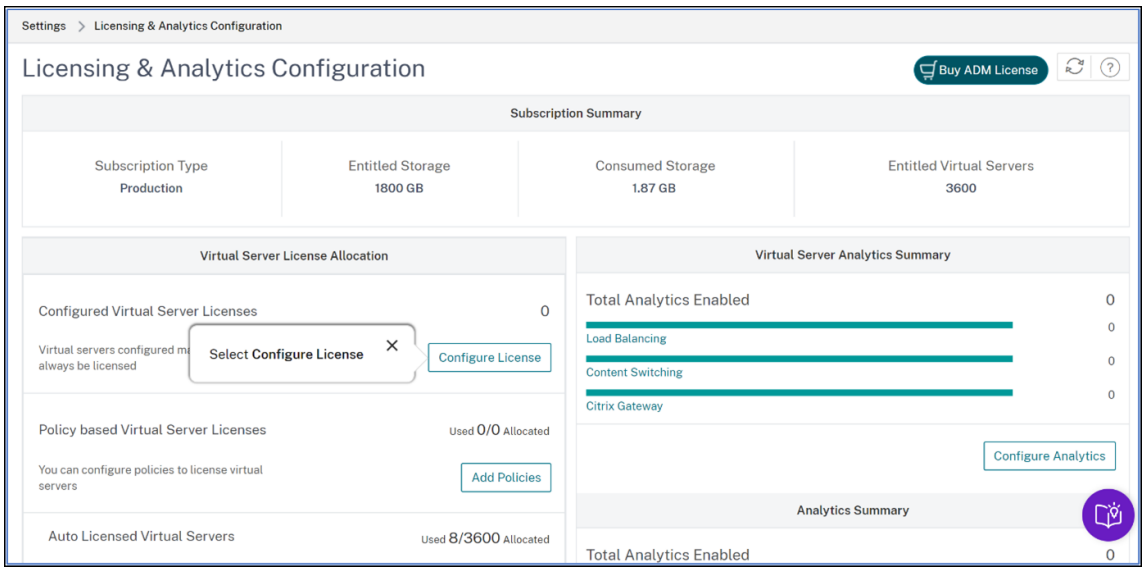
或者，您也可以使用 搜索 栏，键入前几个字符向下钻取任务。

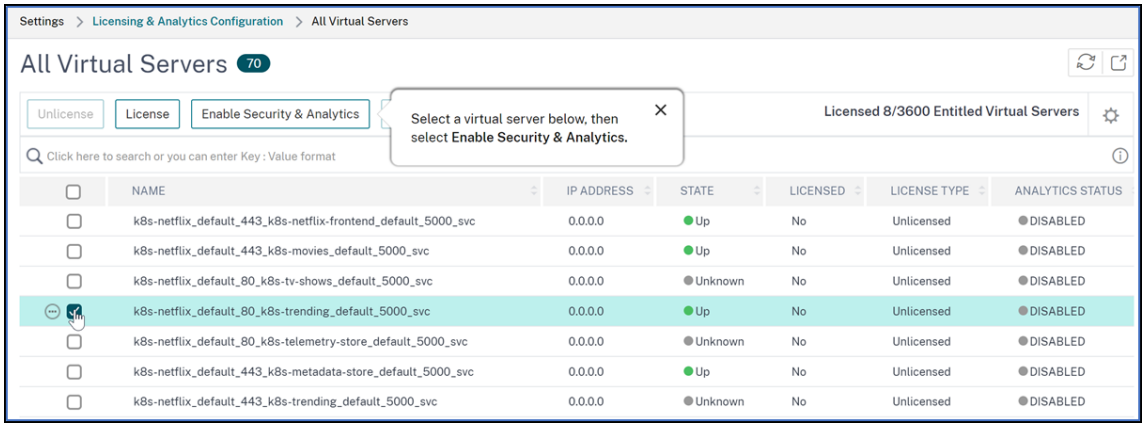
如何使用“引导我”工作流程并完成任务

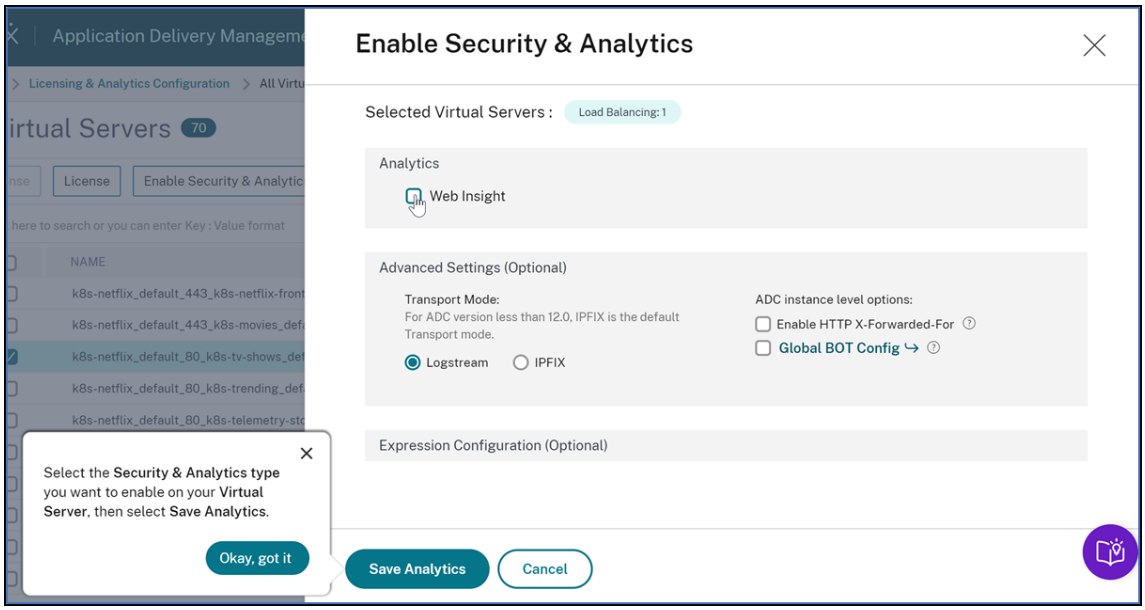
假设您想为所有许可的虚拟服务器启用分析。单击“引导我”执行以下任务：



该工作流程提供了完成任务所需的建议。在此示例中，单击引导我后，按照提供的工具提示建议进行操作：

1. 

2. 

3. 

选择分析类型并单击“保存分析”后，任务即告完成。此任务将移至“已存档”选项卡。

同样，您也可以使用相同的工作流程来满足“存档”选项卡中的重复需求。

在“热门功能”下，您可以查看 NetScaler ADM 的重要功能，它允许您通过单击功能来浏览这些功能。

常见问题解答

1. 引导我不显示工具提示，只显示界面重定向？我该怎么做才能解决这个问题？

   如果您的防火墙阻止 Pendo FQDN，则可能会发生此问题。请参阅为企业启用 Pendo 并确保在防火墙中允许 FQDN。允许 Pendo FQDN 可以让引导我显示工具提示。只有在 Pendo 可用时，您才能以最佳状态体验引导我工作流程。

2. 为什么管理员需要执行任务类型？

   目前，这些建议是专门针对部署的，可帮助管理员更多地了解配置和设置任务，从而提高部署效率。它还可以更好地发现产品，管理员可以在没有任何先验知识或不知道 ADM 中是否存在该功能的情况下知道任务的作用以及

它如何提供帮助。

3. 我可以将任务从“存档”带回待办事项吗?

   存档中的任何任务都只能根据特定条件返回“待办事项”。例如，如果所有事件规则都被删除或所有 ADC 都被移除，则存档的任务将再次移至管理员的待办事项任务中，以引起他们的注意。

4. 如果我确认，进度栏是否完成?

   是的！但是建议完成这些任务。但是，如果您想稍后再做，则可以确认自己知道产品建议，然后返回存档以完成该建议。

5. 如果我开始“引导我”工作流程，然后在进行过程中停止该流程，任务会转到“存档”吗?

   否，除非保存或完成操作，否则任务在“待办事项”中继续可用。

6. 我可以进行搜索或筛选吗?

   是的！您可以使用搜索栏或通过从列表中选择类别来缩小到特定任务。

7. 我会让任务对动态事件（例如 ADC 内存峰值、应用程序关闭、LB 虚拟服务器关闭等）采取操作吗?

   所有这些都是增强功能的一部分，计划在即将发布的版本中提供。

8. 这适用于本地 ADM 吗?

   此功能目前仅在 ADM 服务中可用。

9. 即使我没有在 NetScaler ADM 中添加 ADC，我的 20 多个任务都会显示吗?

   没有。NetScaler ADM 中必须有 ADC 实例和虚拟服务器都可用，才能显示所有这些任务。

10. 任务多久刷新一次?

```
When you click **Tasks** from the left navigation pane, they are
    refreshed and available at the latest status. The details for
    each task are fetched and updated. The tasks are automatically
    refreshed every 24 hours. For better administrative control,
    you can also do a manual refresh of tasks to get the latest
    status.
```

应用程序

February 6, 2024

NetScaler ADM 的应用程序分析和管理功能使您能够通过以应用程序为中心的方法监视应用程序。这种方法可以帮助您:

- 检查得分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 (NetScaler)。

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

- 确保您已经在 NetScaler ADM 中添加了 NetScaler 实例
- 确保您拥有适用于您的 NetScaler 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，您可以通过控制板管理和监视应用程序。您可以轻松监视归类为一个类别的特定应用程序。

例如，您可以为数据中心 1 创建一个类别并添加其 ADC 实例。为数据中心 1 定义类别并添加实例后，应用程序控制板将显示一个单独的类别，其中包括与您的数据中心 1 相关的所有应用程序。

需要注意的事项

- 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，NetScaler 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 群集中，NetScaler 为 NetScaler MPX（硬件）、NetScaler VPX（虚拟化）和 NetScaler CPX（容器化）提供 Ingress Controller。有关详细信息，请参阅 NetScaler Ingress Controller。

使用 NetScaler CPX 实例配置的离散应用程序称为微服务应用程序。

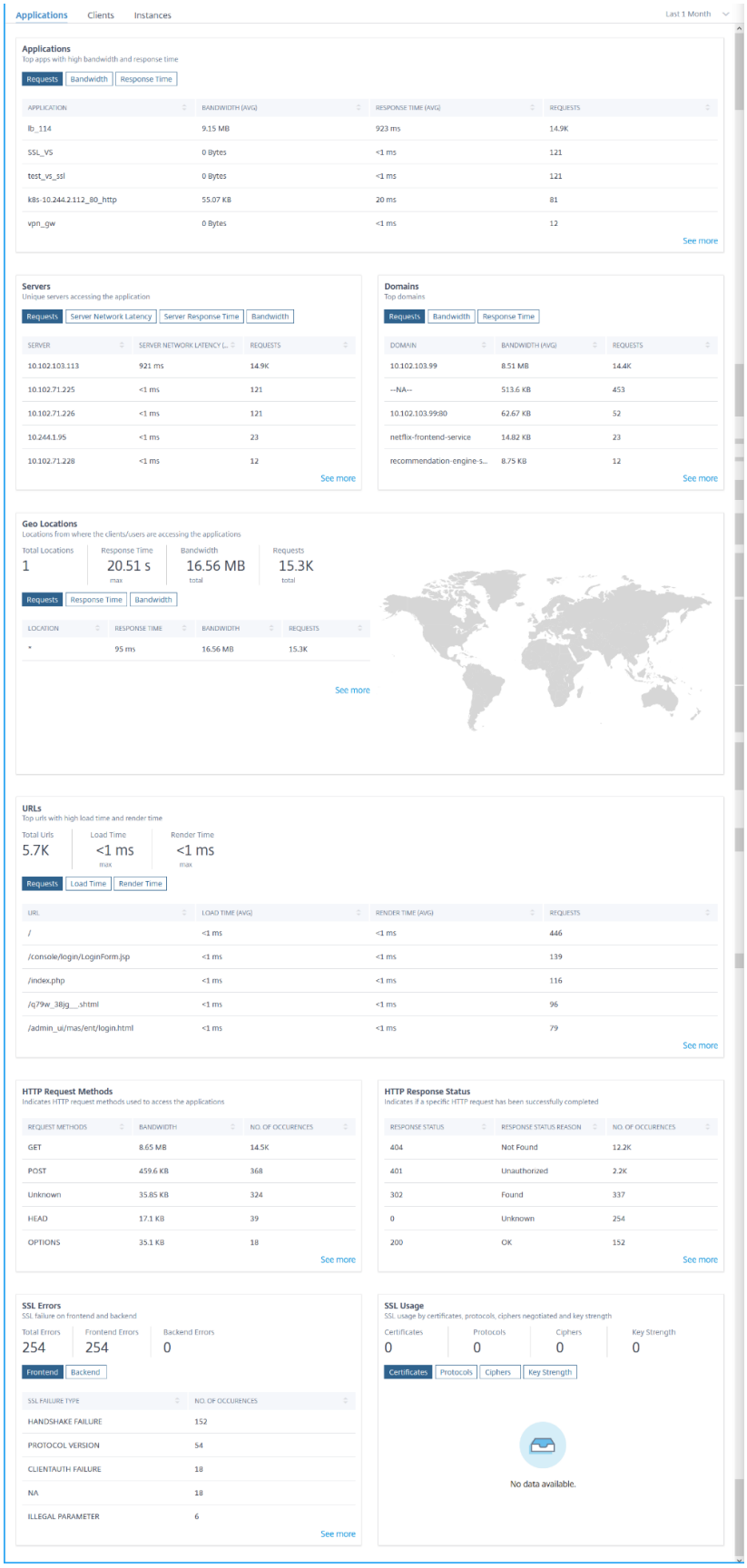
Web Insight 控制板

February 6, 2024

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 NetScaler 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 **>** 控制板，单击应用程序，然后选择 **Web Insight** 选项卡以查看详细指标。有关更多信息，请参阅 应用程序使用情况分析。
- 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	客户端	实例
应用程序	客户端	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
HTTP 响应状态	浏览器	客户端
SSL 错误	SSL 错误	服务器
SSL 使用情况	SSL 使用情况	操作系统
		浏览器

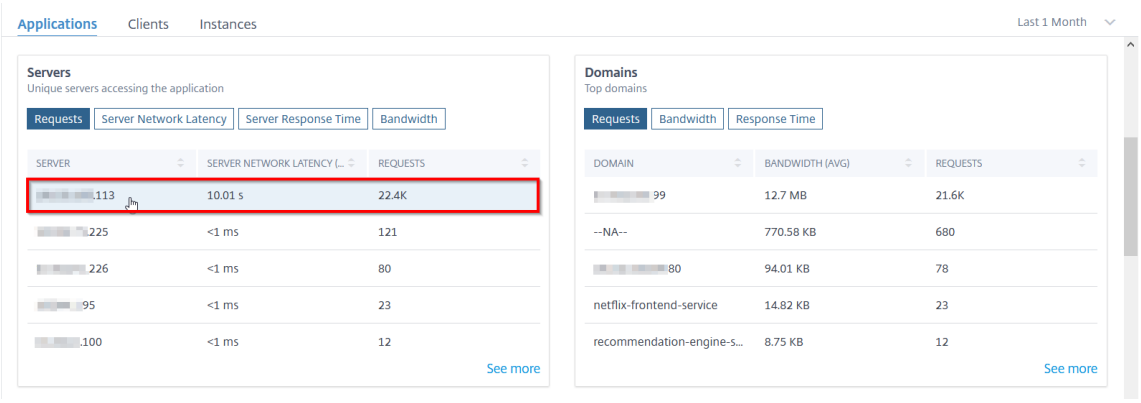


在每个指标中，您可以查看前 5 个结果。您可以单击进一步向下钻取以分析问题并更快地执行故障排除操作。

> 注意
>
> 在某些情况下，NetScaler 可能无法计算某些事务的 RTT 值。对于此类事务，NetScaler ADM 会将 RTT 值显示为
>
> - **NA** —当 ADC 实例无法计算 RTT 时显示。
> - **< 1ms** —当 ADC 实例以 0 毫秒到 1 毫秒之间的小数位数计算 RTT 时显示。例如，0.22 毫秒。

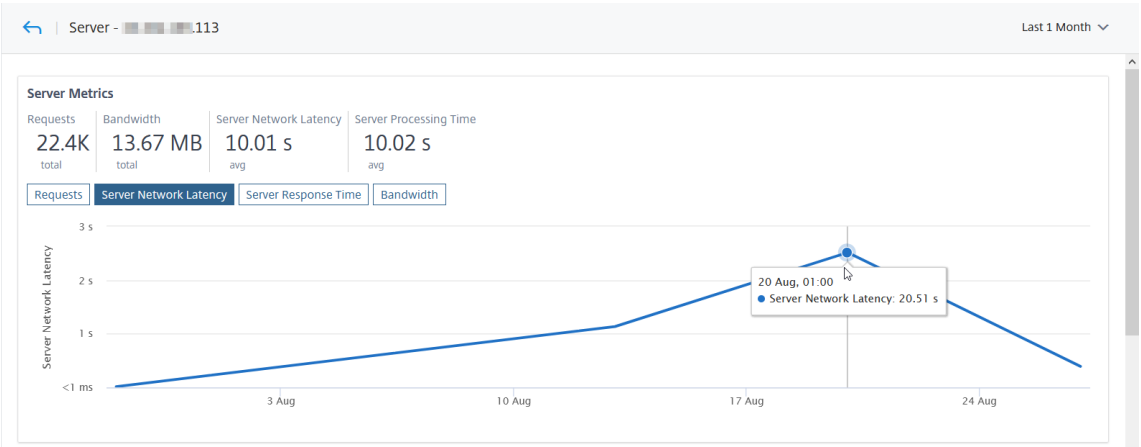
例如，考虑您想要分析服务器网络延迟 1 个月的持续时间，并决定是扩展还是缩小生产环境。要分析这个：

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。

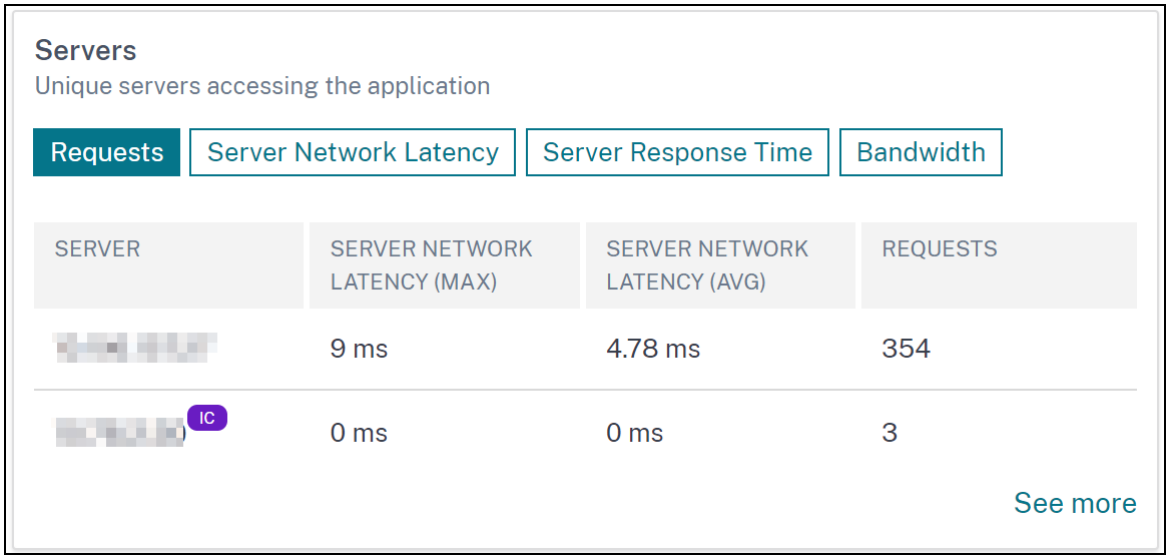


平均延迟表示 10.01 秒，从图表中，您可以分析过去 1 个月的服务器网络延迟似乎很高。作为管理员，您可以决定扩展生产环境。

集成缓存请求

集成缓存在 NetScaler 设备上提供内存存储，无需往返原始服务器即可向用户提供 Web 内容。

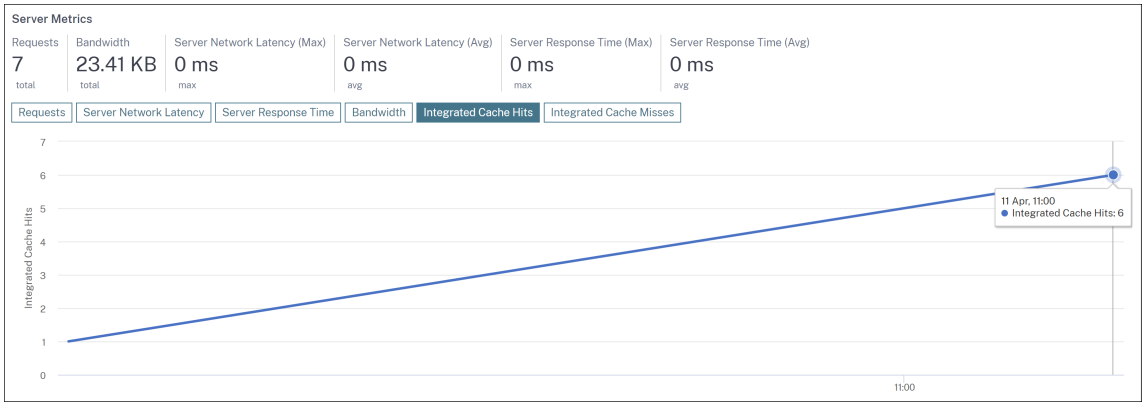
集成缓存请求目前在“服务器”下可见，ADC 虚拟服务器 IP 地址旁边会显示 IC 通知。使用源服务器 IP 地址，所有其他请求都可见。



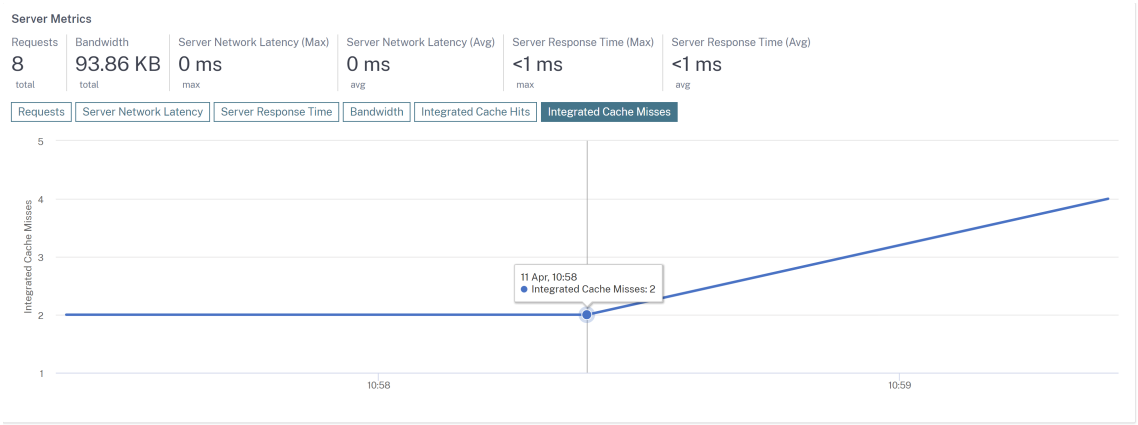
当您深入查看服务器以查看更多详细信息时，服务器指标会显示集成的缓存命中率和未命中率选项卡。

以下对象中的图表视图：

- 在集成缓存命中率选项卡中，您可以查看 NetScaler 设备从缓存中提供的响应总数。



- 在集成缓存未命中选项卡中，您可以查看 NetScaler 设备从源服务器提供的响应总数。



排除 **Web** 智能分析问题

有关详细信息，请参阅故障排除文档 Web Insight 问题故障排除。

服务图表

February 6, 2024

NetScaler 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 NetScaler 实例配置的应用程序
- Kubernetes 应用程序
- 3 层 Web 应用程序

跨所有 **NetScaler** 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结构（NetScaler 实例）视图
- 了解问题是来自客户端、基础结构还是应用程序
- 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 NetScaler 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
- NetScaler 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 NetScaler 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 服务中的应用程序的整体视图图。

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
- 识别因应用程序不同组件之间的相互依赖性而造成的瓶颈
- 收集对应用程序不同组件依赖关系的见解
- 监视 Kubernetes 群集中的服务
- 监视哪个服务有问题
- 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 NetScaler 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。要开始使用，请参阅 设置服务图。

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事务
- 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 NetScaler 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，例如“严重”、“审核”和“良好”。NetScaler ADM 根据服务响应时间和错误计数显示服务状态。
  - 严重（红色） -表示平均服务响应时间大于 200 毫秒且错误计数 > 0
  - 查看（橙色） -表示平均服务响应时间大于 200 毫秒或错误计数 > 0
  - 良好（绿色） -表示没有错误，平均服务响应时间小于 200 毫秒
- 客户端状态，例如“严重”、“审阅”和“良好”。NetScaler 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）-指示客户端网络平均延迟大于 200 毫秒且错误计数 > 0
  - 查看（橙色） -指示客户端网络平均延迟 > 200 毫秒或错误计数 > 0
  - 良好（绿色） -表示无错误且客户端网络平均延迟小于 200 毫秒
- 虚拟服务器的状态，例如“严重”、“审核”和“良好”。NetScaler ADM 根据应用程序得分显示虚拟服务器状态。
  - 严重（红色） -表示应用得分小于 40 时
  - 评价（橙色） -表示应用得分介于 40 和 75 之间的情况
  - 良好（绿色） -指示应用程序得分大于 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。

样书

February 6, 2024

样书简化了为应用程序管理复杂的 NetScaler 配置的任务。样书是可以用来创建和管理 NetScaler 配置的模板。可以创建用于配置 NetScaler 特定功能的样书，也可以设计样书为企业应用程序部署（例如 Microsoft Exchange 或 Lync）创建配置。

样书非常符合 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。样书具有以下优势：

- 声明式：样书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 NetScaler 实例上实现配置的分步说明。NetScaler Application Delivery Management (ADM) 计算 NetScaler 上的现有状态与您指定的所需状态之间的差异，并对基础架构进行必要的编辑。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，NetScaler 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：样书具有将其与系统中的任何其他样书唯一区分开的名称、命名空间和版本号。对样书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书的多个版本。
- 可组合：定义了样书后，可以将该样书用作构建其他样书的单元。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。由于样书是版本化的，因此，对现有样书进行更改会产生新的样书，从而确保绝不会意外破坏依赖样书。
- 以应用程序为中心：样书可用于定义完整应用程序的 NetScaler 配置。可以使用参数提取应用程序的配置。因此，基于样书创建配置的用户可以与一个简单界面交互，包括填写一些参数来创建复杂的 NetScaler 配置。基于样书创建的配置不绑定到基础结构。因此，可以在一个或多个 NetScaler 上部署单个配置，也可以在实例之间移动单个配置。
- 自动生成的 **UI**：NetScaler ADM 会自动生成 UI 表单，用于在使用 NetScaler ADM GUI 进行配置时填写样书的参数。样书作者无需了解新的 GUI 语言或单独创建 UI 页面和表单。
- **API** 驱动：使用 NetScaler ADM GUI 或 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，通过样书 API 还可以在运行时发现任何样书的架构（参数说明）。

可以使用一个样书创建多个配置。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书。可以创建包含用于负载平衡实体的值的配置，然后在 NetScaler 实例上执行该配置。此配置保存为一个配置包。可以使用同一样书创建包含不同值的另一个配置，然后在同一或不同的 NetScaler 实例上执行该配置。即为此配置创建一个新配置包。配置包既保存在 NetScaler ADM 上，也保存在执行配置的 NetScaler 实例上。

可以使用 NetScaler ADM 附带的默认样书为您的部署创建配置，也可以设计您自己的样书并将其导入 NetScaler ADM。您可以使用样书通过 NetScaler ADM GUI 或使用 API 来创建配置。

本文档包含以下信息：

应用程序安全控制板

February 6, 2024

应用程序安全 控制板提供了已发现/许可应用程序的安全度量概述。此控制面板显示已发现/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“**** 安全” **>** “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。

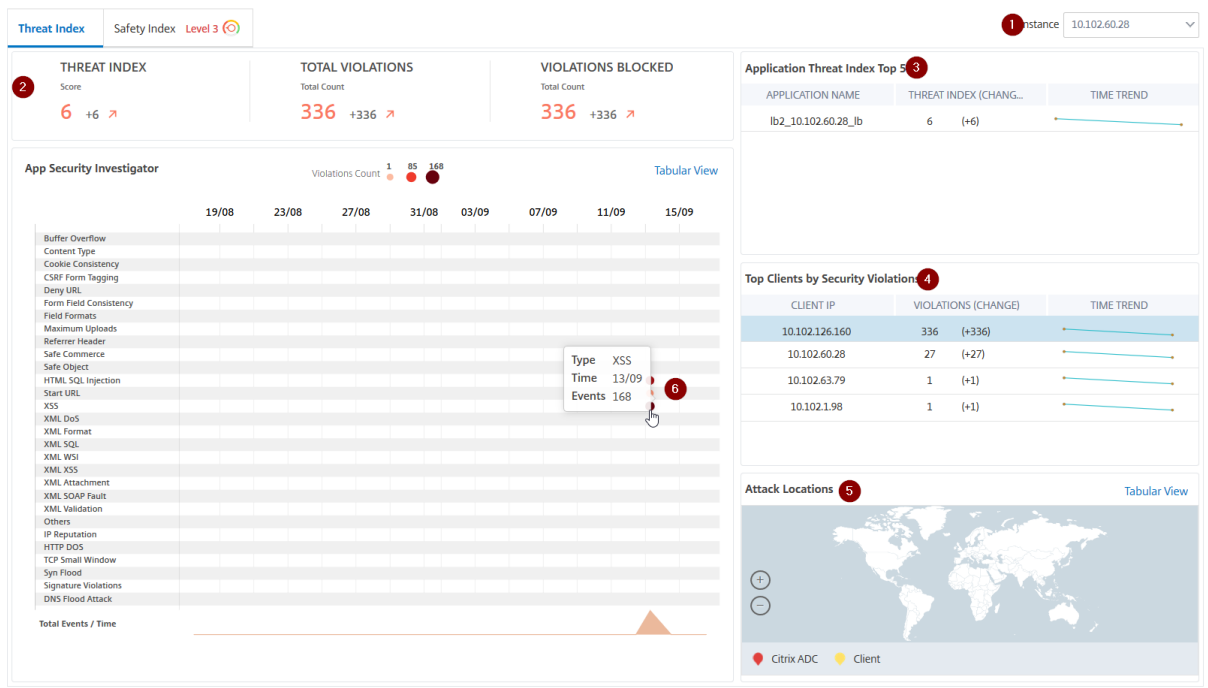
     威胁指数基于攻击信息。与攻击相关的信息，例如违规类型、攻击类别、位置和客户端详细信息，可以深入了解对应用程序的攻击。只有在发生违规或攻击时，才会向 NetScaler ADM 发送违规信息。大量违反和漏洞会导致较高的威胁指数值。

   - 安全指数。一个单位数评级系统，用于指示您配置 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 实例 IP 地址。

2 -显示威胁指数得分、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。

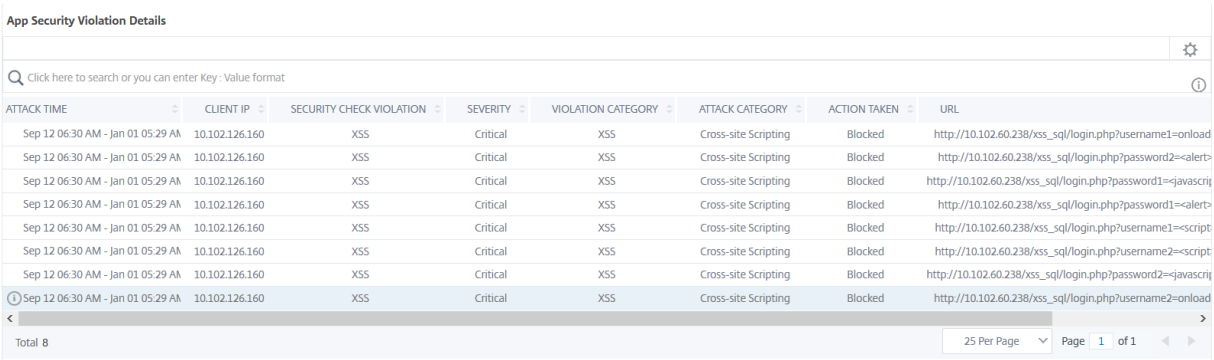
4 -显示基于客户端的安全违例。将显示每个客户端的“应用安全调查器”图形。您可以单击每个客户端 IP 以查看结果。

5 -在地图视图和表格视图中显示违规。

6 -显示违规详情。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。

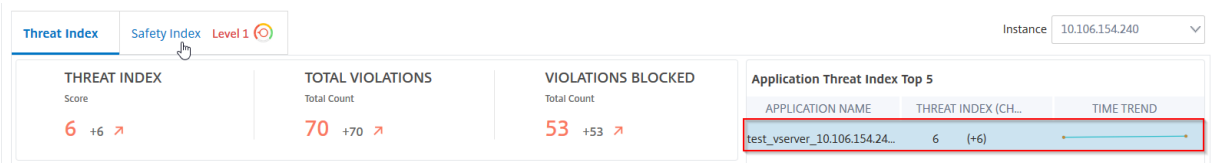
安全指数详细信息

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。

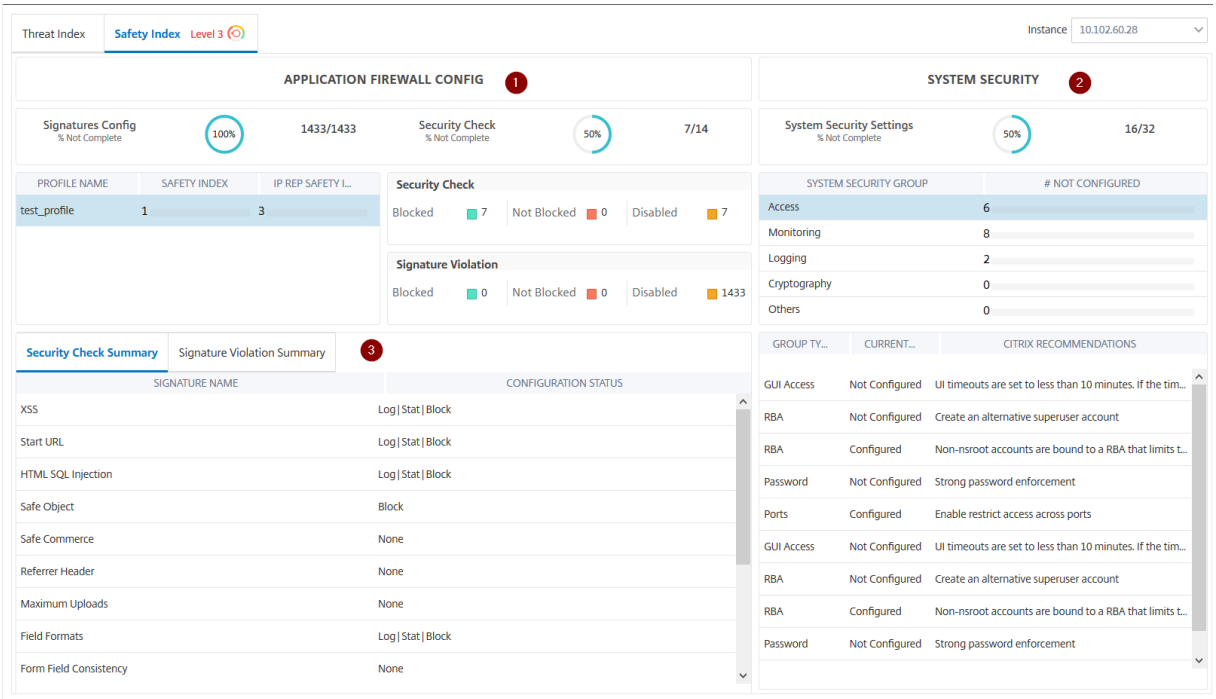
安全指数摘要为您提供有关以下安全配置的有效性：

- 应用程序防火墙配置。显示多少签名和安全实体未配置。
- **NetScaler ADM** 系统安全。显示多少系统安全设置未配置。

要查看安全指数详细信息，请选择虚拟服务器/应用程序，然后单击安全指数选项卡。



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。

** 您还可以通过为虚拟服务器启用 **WAF** 安全违规，然后导航到“安全” > “安全违规”来查看威胁环境的摘要。**

查看应用程序安全违规详细信息

February 6, 2024

暴露于 Internet 的 Web 应用程序已经变得容易受到严重攻击。NetScaler 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。导航至单窗格解决方案的“安全性”**>**“安全性违规”，以执行以下操作：

- 可视化应用程序，全面了解与 WAF 安全违规和机器人安全违规相关的威胁详细信息
- 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 和机器人违规总数、按国家/地区划分的违规等的应用程序的概述。有关更多信息，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

确保指标收集器是否已启用。默认情况下，在 NetScaler 实例上启用 度量收集器。有关更多信息，请参阅配置智能应用程序分析。

与 **Splunk** 集成

February 6, 2024

您现在可以将 NetScaler ADM 与 Splunk 集成，以查看以下方面的分析：

- WAF 违规行为
- 机器人违规行为
- SSL 证书见解

Splunk 插件使您能够：

- 合并所有其他外部数据源。
- 集中提供更高的分析可见性。

NetScaler ADM 收集 Bot、WAF、SSL 事件，然后定期发送给 Splunk。Splunk 通用信息模型 (CIM) 插件将事件转换为 CIM 兼容数据。作为管理员，您可以使用与 CIM 兼容的数据在 Splunk 控制板中查看事件。

要成功集成，您必须：

- 将 Splunk 配置为从 NetScaler ADM 接收数据
- 配置 NetScaler ADM 将数据导出到 Splunk
- 在 Splunk 中查看控制板

将 **Splunk** 配置为从 **NetScaler ADM** 接收数据

在 Splunk 中，您必须：

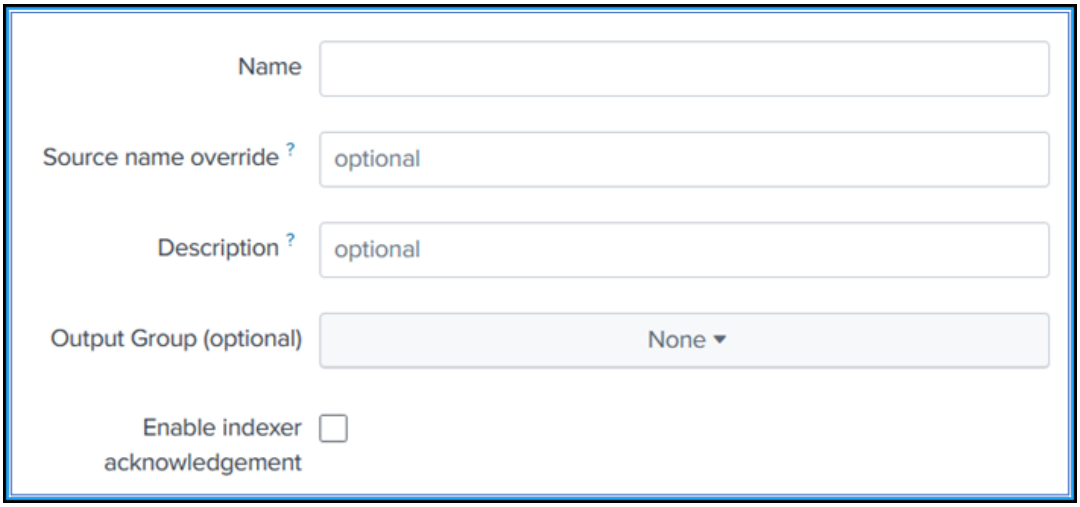
1. 设置 Splunk HTTP 事件收集器端点并生成令牌
2. 安装 Splunk 通用信息模型 (CIM) 插件
3. 在 Splunk 中准备一个示例控制板

设置 **Splunk HTTP** 事件收集器端点并生成令牌

您必须先在 Splunk 中设置 HTTP 事件收集器。此设置允许在 ADM 和 Splunk 之间进行集成以发送数据。接下来，您必须在 Splunk 中生成一个令牌以：

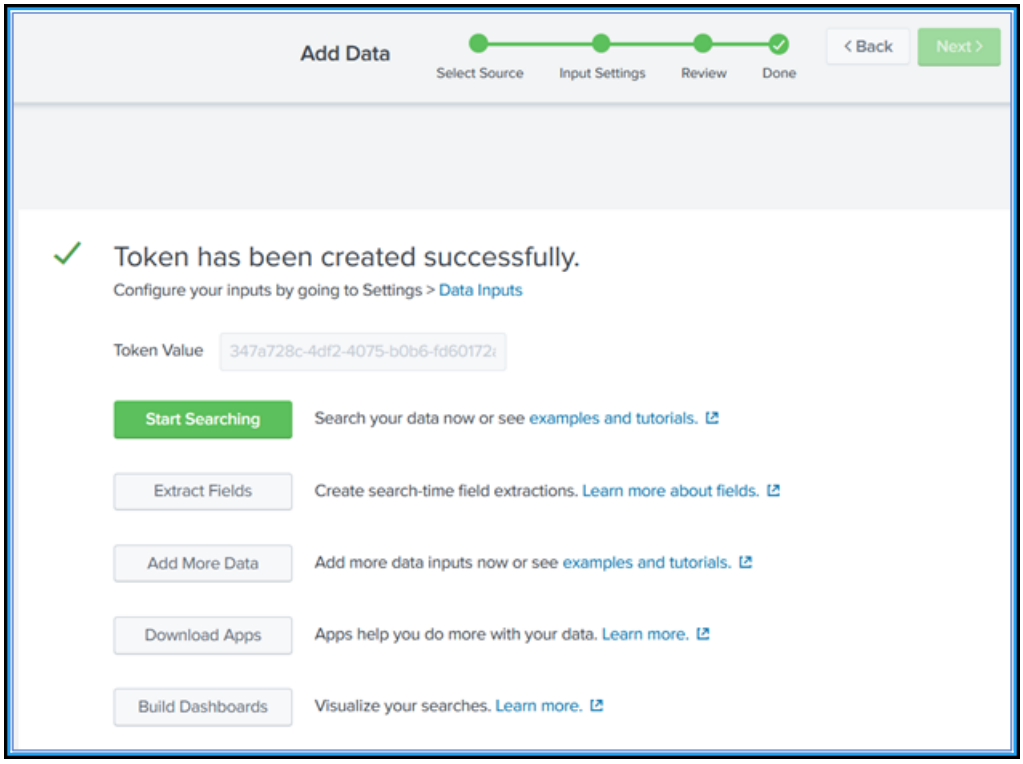
- 在 ADM 和 Splunk 之间启用身份验证。
- 通过事件收集器端点接收数据。

1. 登录 Splunk。
2. 导航到“设置”**>**“数据输入”**>**“**HTTP** 事件收集器”，然后单击“新增”。
3. 指定以下参数：
    a) 名称：指定您选择的名称。
    b) 源名称覆盖（可选）：如果设置一个值，它将覆盖 HTTP 事件收集器的源值。
    c) 描述（可选）：指定描述。
    d) 输出组（可选）：默认情况下，此选项被选为无。
    e) 启用索引器确认：默认情况下，未选择此选项。



4. 单击下一步。
5. 或者，您可以在“输入设置”页面中设置其他输入参数。
6. 单击“审阅”以验证参赛作品，然后单击“提交”。

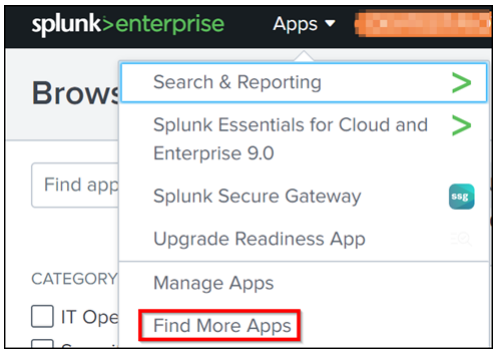
   生成令牌。在 NetScaler ADM 中添加详细信息时，必须使用此令牌。



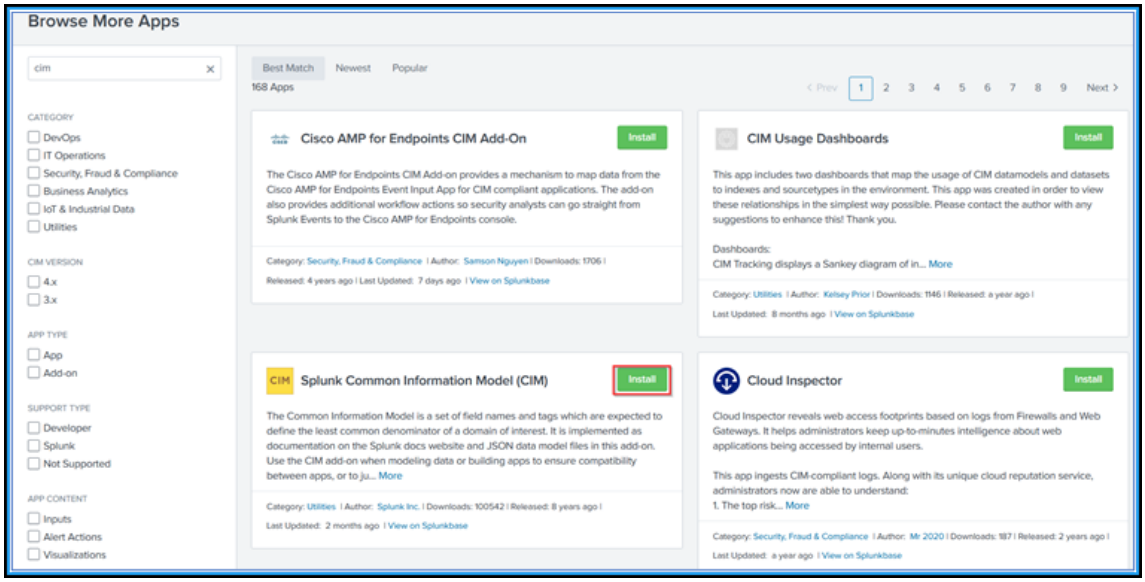
安装 **Splunk** 通用信息模型

在 Splunk 中，您必须安装 Splunk CIM 附加组件。此插件可确保从 NetScaler ADM 接收的数据对采集的数据进行标准化处理，并匹配使用相同字段名称和等效事件的事件标签的通用标准。

1. 登录 Splunk。
2. 导航到 应用程序 **>** 查找更多应用程序。



3. 在搜索栏中键入 **CIM** ，然后按 **Enter** 获取 **Splunk** 通用信息模型 **(CIM)** 插件，然后单击“安装”。



在 **Splunk** 中准备一个示例控制板

安装 Splunk CIM 后，必须使用 WAF 和 Bot 模板以及 SSL 证书见解准备示例控制板。您可以下载控制板模板 (`.tgz`) 文件，使用任何编辑器（例如，记事本）复制其内容，并通过在 Splunk 中粘贴数据来创建控制板。

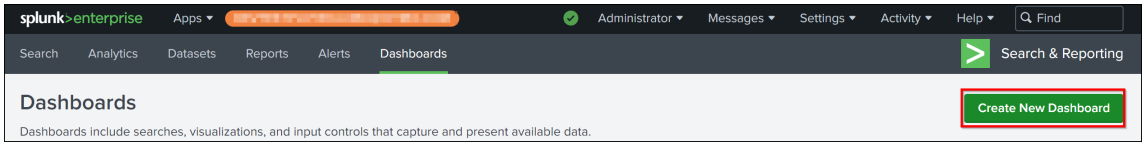
> 注意：
>
> 以下创建示例控制板的步骤适用于 WAF 和 Bot 以及 SSL 证书见解。必须使用所需的 `json` 文件。

1. 登录 Citrix 下载页面，下载可 观测性集成下提供的示例控制板。

2. 提取文件，使用任意编辑器打开 `json` 文件，然后从文件中复制数据。

   > 注意：
   >
   > 解压缩后，您会得到两个 `json` 文件。使用 `adm_splunk_security_violations.json` 创建 WAF 和 Bot 示例控制板，使用 `adm_splunk_ssl_certificate.json` 创建 SSL 证书洞察示例控制板。

3. 在 Splunk 门户中，导航到“搜索和报告” **>** “控制板”，然后单击“创建新控制板”。



4. 在“创建新控制板”页面中，指定以下参数：

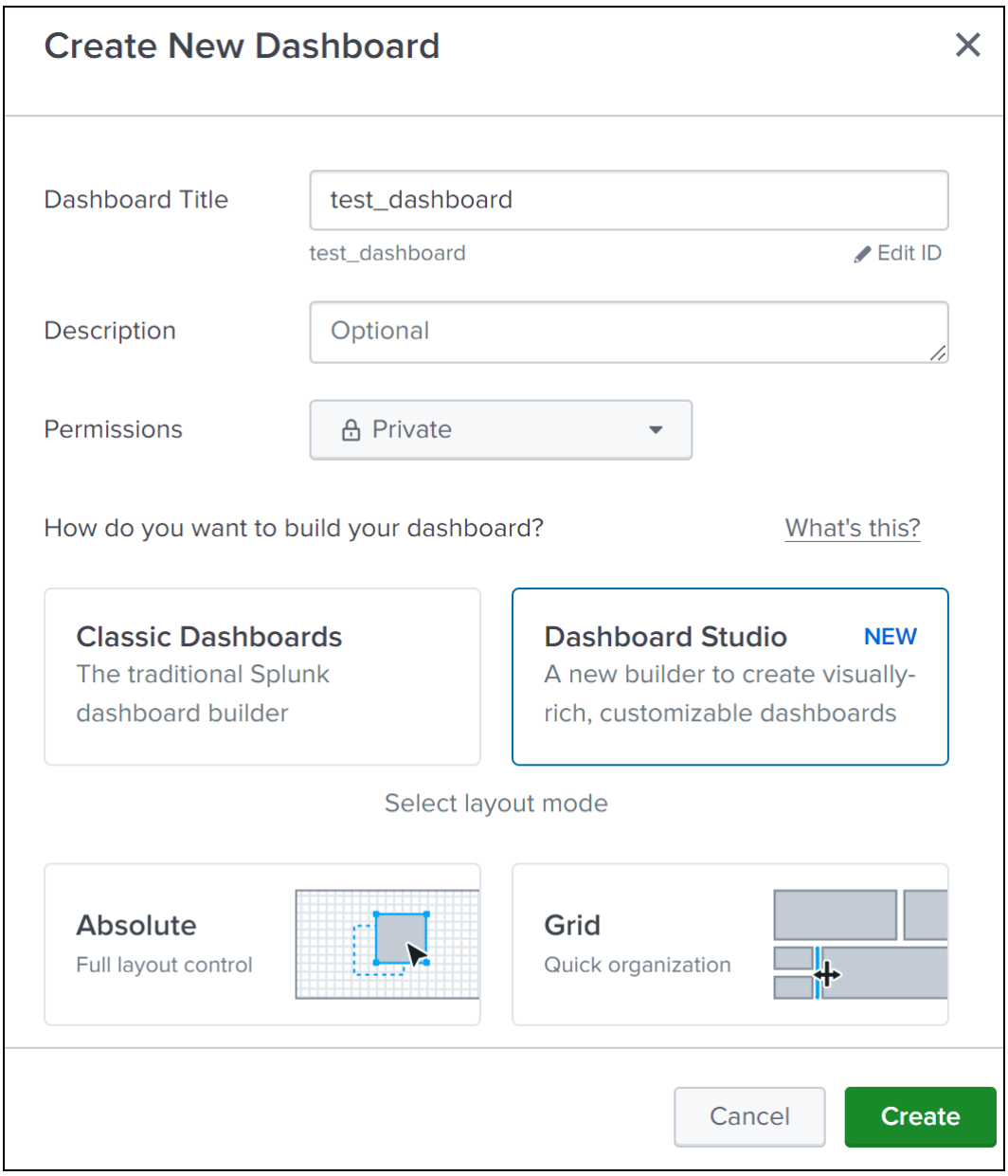
   a) 控制板标题 -提供您选择的标题。

   b) 说明 -（可选）您可以提供描述以供参考。

   c) 权限 -根据您的要求选择“专用”或“在应用程序中共享”。

   d) 选择“控制板 **Studio**”。

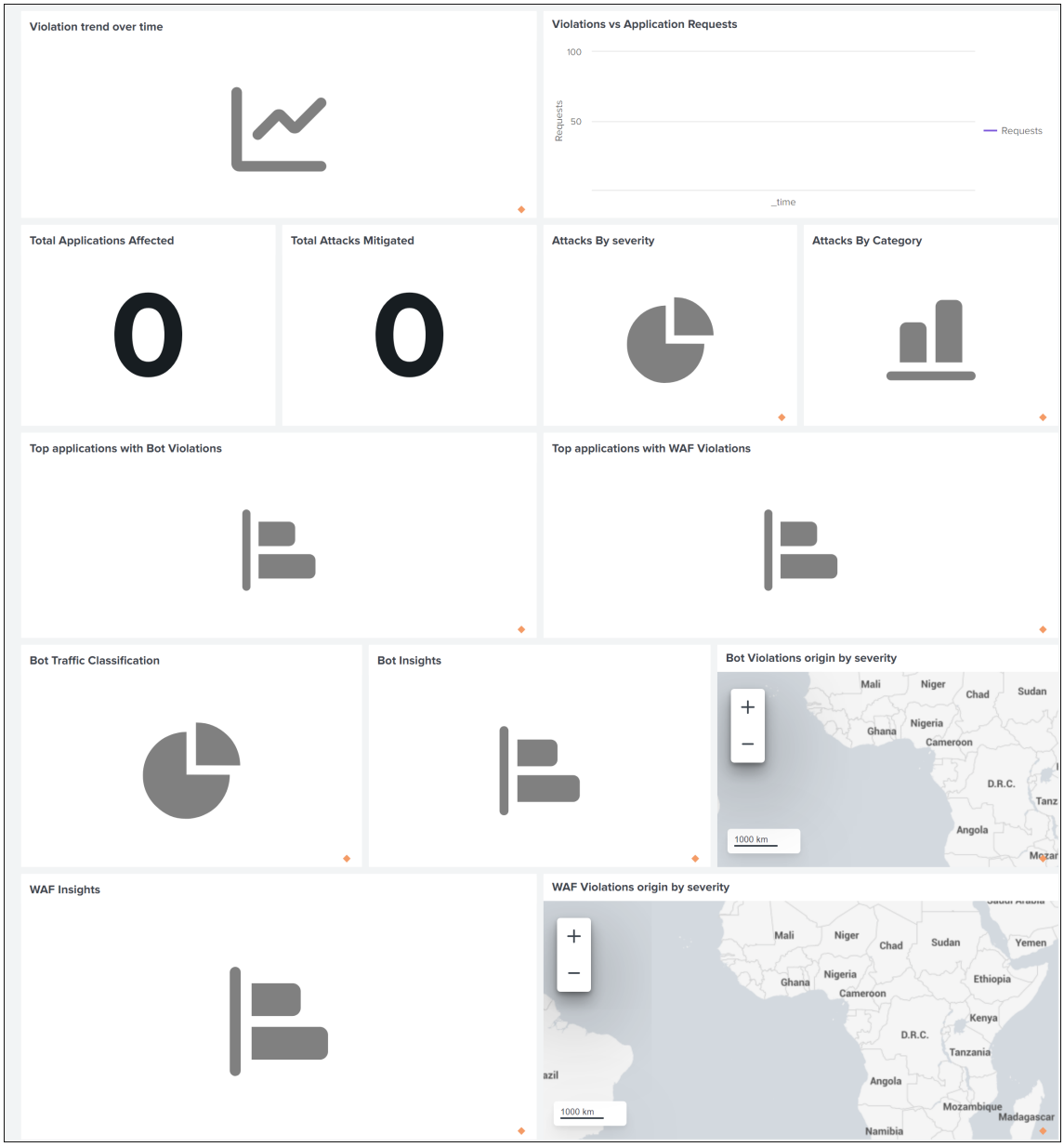
   e) 选择任意一种布局（绝对或网格），然后单击“创建”。



单击“创建”后，从布局中选择“源”图标。

5. 删除现有数据，粘贴您在步骤 2 中复制的数据，然后单击“返回”。
6. 单击保存。

   您可以在 Splunk 中查看以下示例控制板。



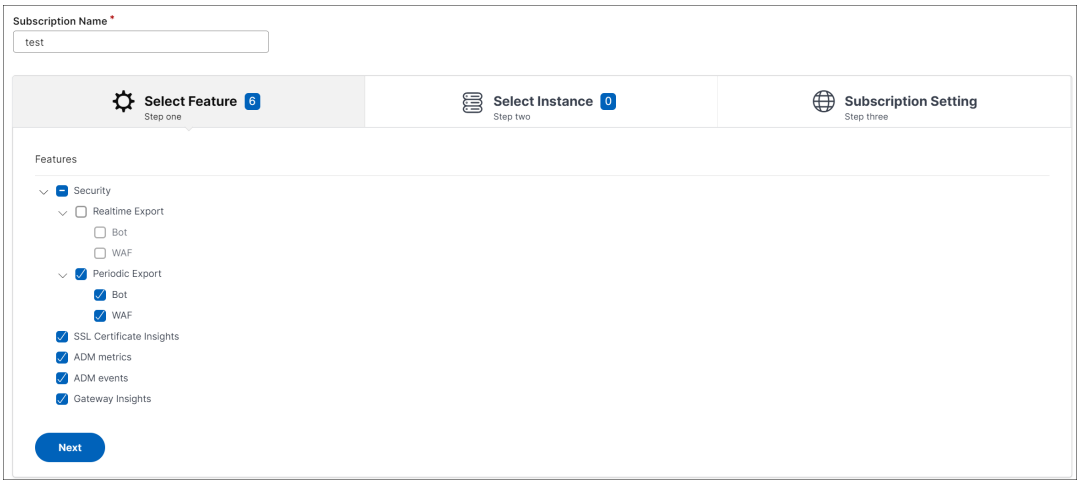
配置 **NetScaler ADM** 将数据导出到 **Splunk**

现在，您已经在 Splunk 中准备好一切了。最后一步是通过创建订阅并添加令牌来配置 NetScaler ADM。

完成以下步骤后，您可以在 Splunk 中查看 NetScaler ADM 中当前可用的更新控制板：

1. 登录到 NetScaler ADM。
2. 导航到 设置 **>** 生态系统集成。
3. 在“订阅”页面中，单击“添加”。
4. 在“选择要订阅的功能”选项卡中，选择要导出的功能，然后单击“下一步”。

- 实时导出 -选定的违规将立即导出到 Splunk。
- 定期导出 -根据您选择的持续时间，将选定的违规行为导出到 Splunk。



5. 在“指定导出配置”选项卡中：

   a) 端点类型 -从列表中选择 **Splunk** 。

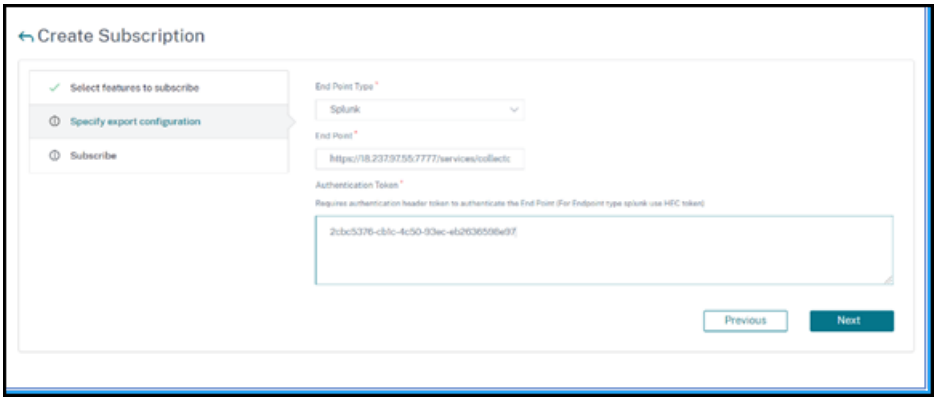
   b) 终点—指定 Splunk 端点的详细信息。终点必须采用以下 https://SPLUNK_PUBLIC_IP:SPLUNK_HEC_PORT/services/collector/event 格式。

   > 注意
   >
   > 出于安全考虑，建议使用 HTTPS。

   - **SPLUNK_PUBLIC_IP** —为 Splunk 配置的有效 IP 地址。
   - **SPLUNK_HEC_PORT** —表示您在 HTTP 事件端点配置期间指定的端口号。默认端口号为 8088。
   - 服务/收集器/事件—表示 HEC 应用程序的路径。

   c) 身份验证令牌 -从 Splunk 页面复制并粘贴身份验证令牌。

   d) 单击下一步。



6. 在“订 阅”页面中：

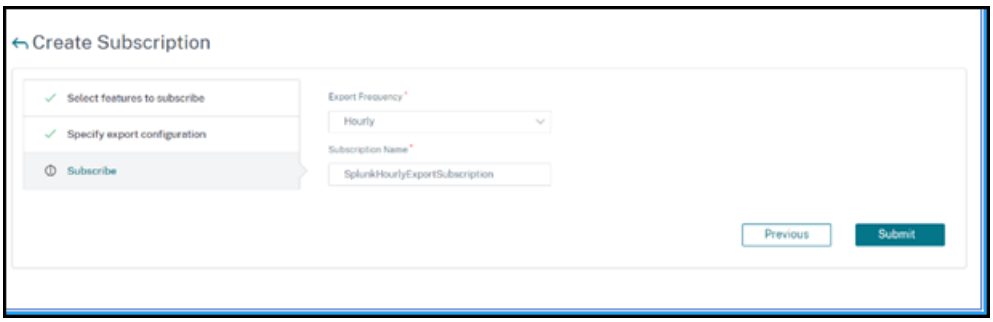
a) 导出频率 -从列表中选择“每天”或“每小时”。根据选择，NetScaler ADM 会将详细信息导出到 Splunk。

> 注意：
>
> 仅当您在“定期导出”中选择了违规行为时才适用。

b) 订阅名称—指定您选择的名称。

c) 选中“启用通知”复选框。

d) 单击 **Submit**（提交）。



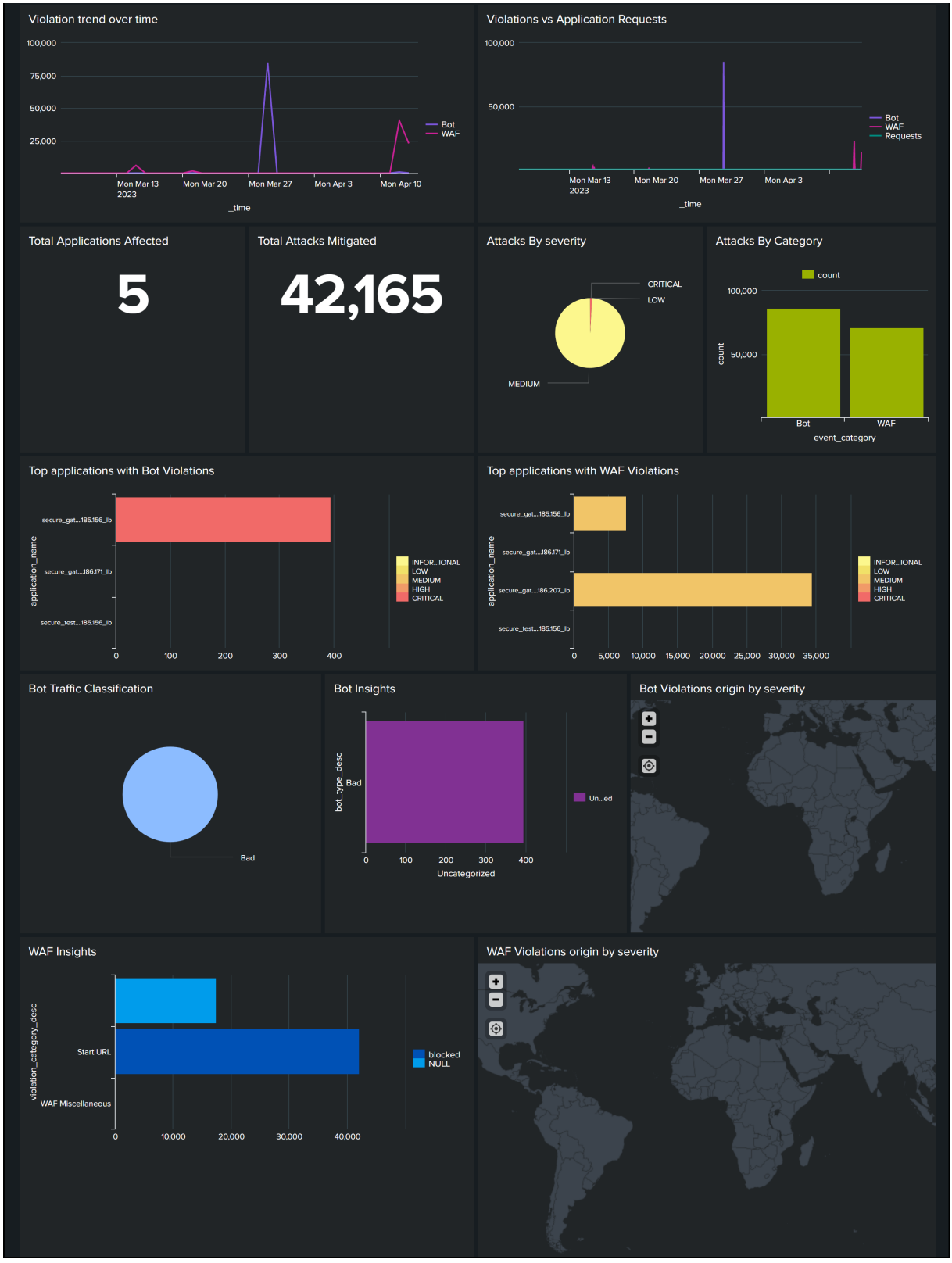
> 注意
>
> - 首次使用“定期导出”选项进行配置时，所选要素数据会立即推送到 Splunk。下一次导出频率取决于您的选择（每天或每小时）。
> - 首次配置“实时导出”选项时，在 NetScaler ADM 中检测到违规行为时，所选要素的数据会立即推送到 Splunk。

在 **Splunk** 中查看控制板

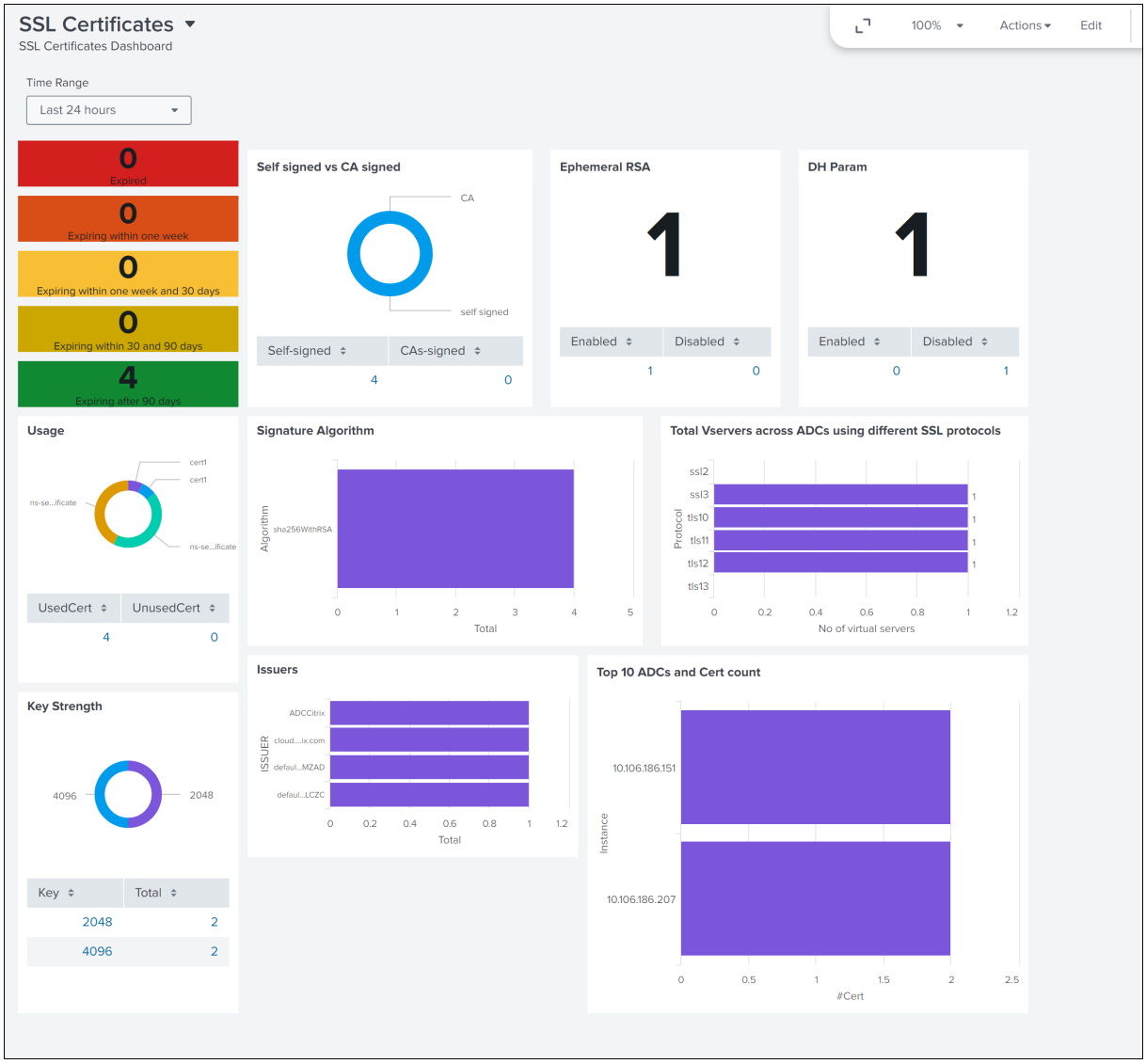
在 NetScaler ADM 中完成配置后，事件将出现在 Splunk 中。您无需任何其他步骤即可在 Splunk 中查看更新的控制板。

转到 Splunk 并单击您创建的控制板以查看更新的控制板。

以下是更新后的 WAF 和 Bot 控制板的示例：



以下控制板是更新后的 SSL 证书见解控制板的示例。



与 **New Relic** 集成

February 6, 2024

现在，您可以将 NetScaler ADM 与 New Relic 集成，以在 New Relic 控制板中查看 WAF 和机器人违规分析。通过这种集成，您可以：

- 在 New Relic 控制板中合并所有其他外部数据源。
- 集中查看分析情况。

NetScaler ADM 收集机器人和 WAF 事件，并根据您的选择实时或定期将其发送到 New Relic。作为管理员，您还可以在 New Relic 控制板中查看机器人和 WAF 事件。

必备条件

要成功集成，您必须：

- 使用以下格式获取 New Relic 事件终端节点：

  ```
  https://insights-collector.newrelic.com/v1/accounts/<account_id>/events
  ```

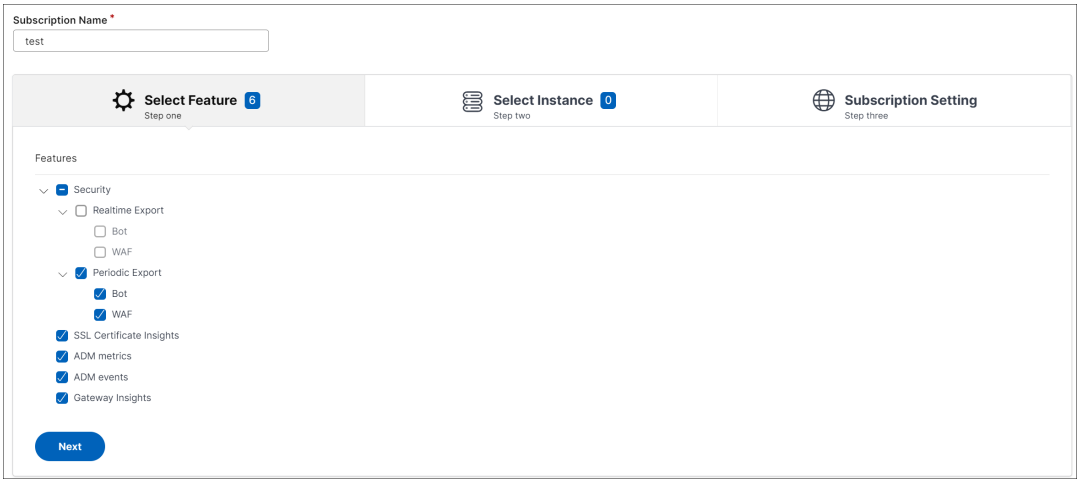
  有关配置事件端点的更多信息，请参阅 New Relic 文档。

  有关获取帐户 ID 的更多信息，请参阅 New Relic 文档。
- 获取 New Relic 密钥。有关更多信息，请参阅 New Relic 文档。
- 在 NetScaler ADM 中添加密钥详细信息

在 **NetScaler ADM** 中添加密钥详细信息

生成令牌后，必须在 NetScaler ADM 中添加详细信息才能与 New Relic 集成。

1. 登录到 NetScaler ADM。
2. 导航到 设置 **>** 生态系统集成。
3. 在“订阅”页面中，单击“添加”。
4. 在“选择要订阅的功能”选项卡中，选择要导出的功能，然后单击“下一步”。
   - 实时导出 -选定的违规行为会立即导出到 New Relic。
   - 定期导出 -选定的违规行为将根据您选择的持续时间导出到 New Relic。



5. 在“指定导出配置”选项卡中：

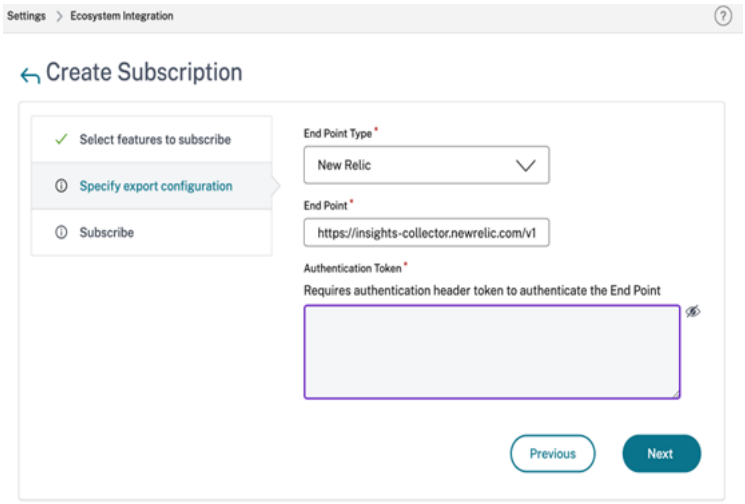
   a) 端点类型—从列表中选择 **New Relic**。

b) 终点—指定 New Relic 终点的详细信息。终点必须采用以下 `https://insights-collector.newrelic.com/v1/accounts/<account_id>/events` 格式。

> 注意
>
> 出于安全考虑，建议使用 HTTPS。

c) 身份验证令牌 -从 New Relic 页面复制并粘贴身份验证令牌。

d) 单击下一步。



6. 在“订 阅”页面中：

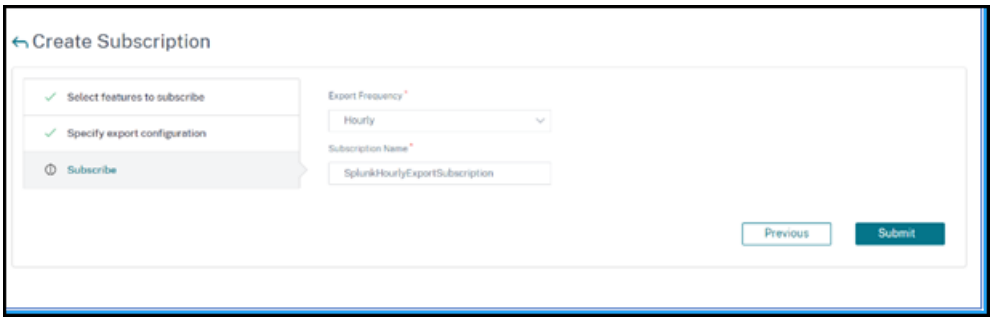
a) 导出频率 -从列表中选择“每天”或“每小时”。根据选择，NetScaler ADM 将详细信息导出到 New Relic。

> 注意
>
> 仅当您在“定期导出”中选择了违规行为时才适用。

b) 订阅名称—指定您选择的名称。

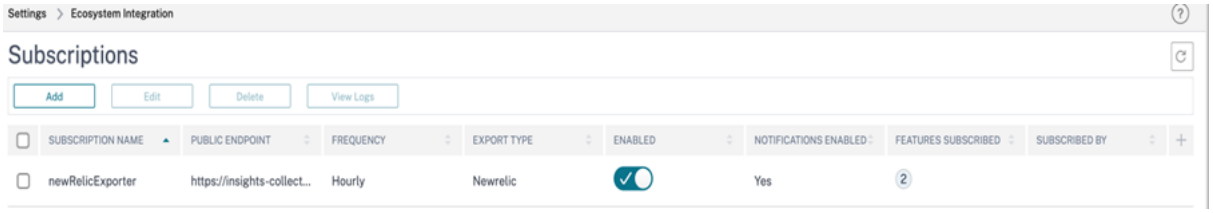
c) 选中“启用通知”复选框。

d) 单击 **Submit**（提交）。



> 注意
>
> - 首次使用“定期导出”选项进行配置时，所选要素数据会立即推送到 New Relic。下一次导出频率取决于您的选择（每天或每小时）。
> - 首次使用 实时导出 选项进行配置时，在 NetScaler ADM 中检测到违规行为后，所选功能数据会立即推送到 New Relic。

配置已完成。您可以在“订阅”页面中查看详细信息。

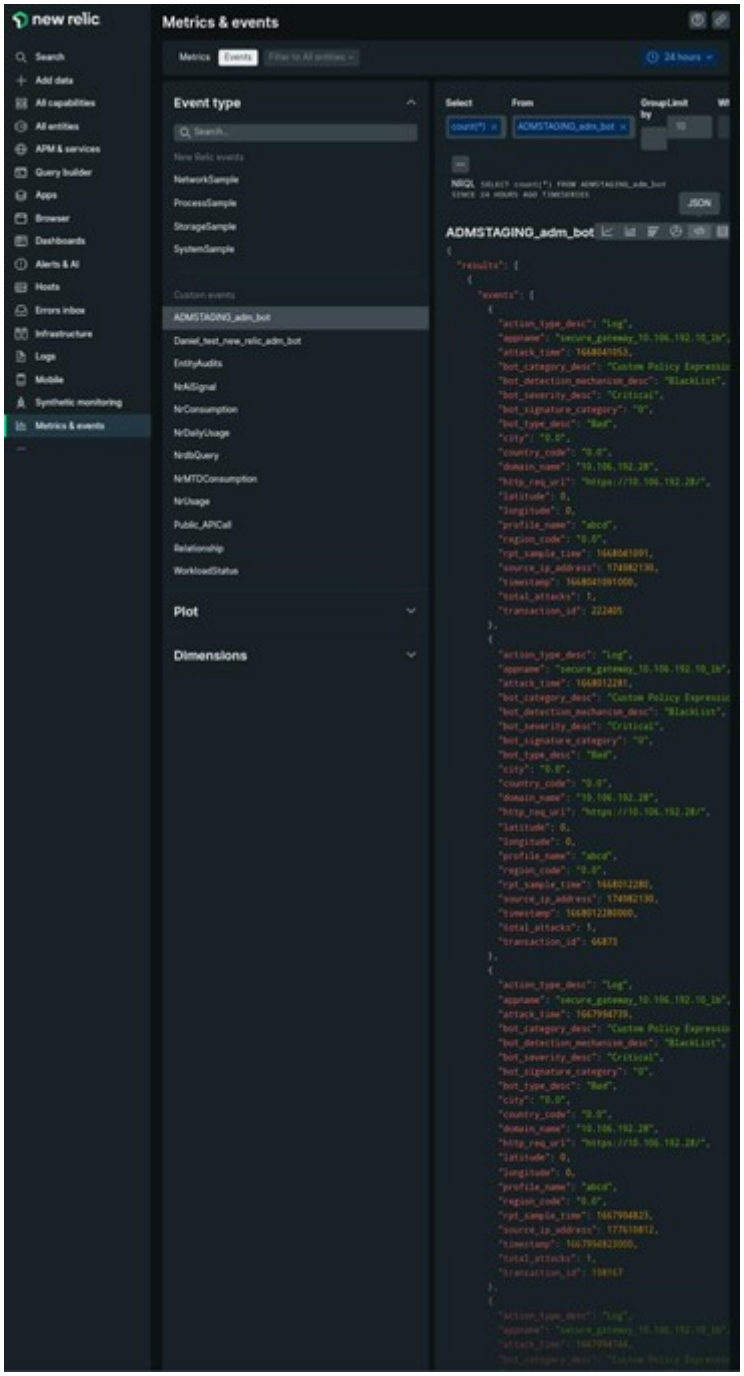


New Relic 控制板

在 New Relic 中导出事件后，您可以使用以下 JSON 格式在“指标和事件”下查看事件详细信息：

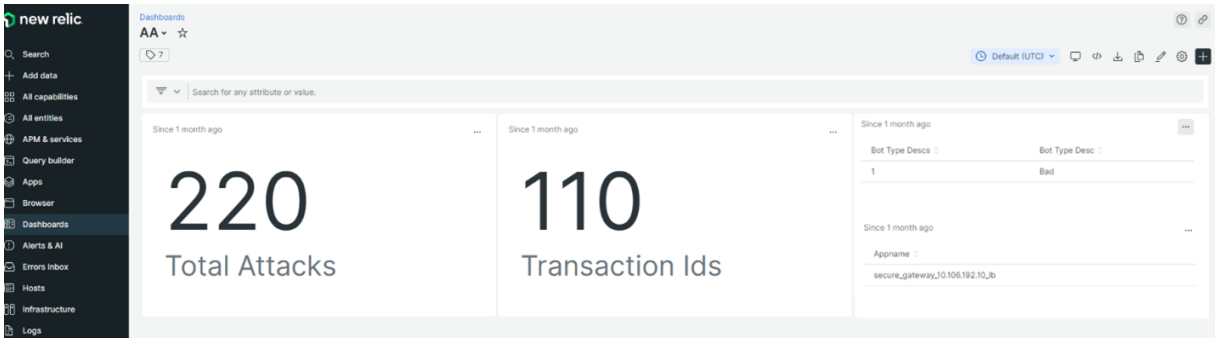
<subsription_name>_adm_<event name>，其中事件名称可以是机器人、WAF 等。

在以下示例中，ADMSTAGING 是 <subscription_name>，机器人是 <event_name>。



将 JSON 数据提取到 New Relic 控制板后，作为管理员，您可以使用 NRQL（New Relic Query Language），通过围绕提取的数据构建查询，根据您的选择创建包含分面和小部件的自定义控制板。有关详细信息，请参阅https://docs.newrelic.com/docs/query-your-data/nrql-new-relic-query-language/get-started/introduction-nrql-new-relics-query-language/。

以下是使用 NRQL 创建的控制板示例：



要创建此控制板，需要进行以下查询：

- 小组件 1：事件表中的传奇攻击总数

  ```
  SELECT count(total_attacks)from <event_name> since 30 days ago
  ```

- 小组件 2：事件表中的唯一事务 ID

  ```
  SELECT uniqueCount(transaction_id)from <event_name> since 30 days ago
  ```

- 小组件 3：独特机器人类型总数及其数量

  ```
  SELECT uniqueCount(bot_type_desc), uniques(bot_type_desc)from <event_name> since 30 days ago
  ```

- 小组件 4：看到机器人违规行为的唯一应用程序名称总数

  ```
  SELECT uniques(appname)from <event_name> since 30 days ago
  ```

Gateway Insight

February 6, 2024

在 NetScaler 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 NetScaler Gateway，您想知道用户活动和登录失败的原因。除非用户发送解决请求，否则此信息通常不可用。

通过 Gateway Insight 可以查看所有用户登录 NetScaler Gateway 时遇到的失败，而无论访问模式为何。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。您可以查看已启动的应用程序数、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。

您可以查看任何给定时间与 NetScaler Gateway 设备关联的所有网关使用的网关数量、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 NetScaler 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。

需要注意的事项

- 以下部署支持 Gateway Insight：
  - Access Gateway
  - Unified Gateway
- NetScaler ADM 的版本和版本必须与 NetScaler Gateway 设备的版本相同或更晚。
- 可以查看具有高级许可证的 NetScaler 实例的一小时 Gateway Insight 报告。高级许可证是必须查看超过一小时的 Gateway Insight 报告。

限制

- 当身份验证方法配置为基于证书的身份验证时，NetScaler Gateway 网关不支持 Gateway Insight。
- 对于 Gateway Insight 报告，NetScaler 设备不会提供地理位置信息。
- 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。
- 在双跃点模式下，无法查看第二个 DMZ 中 NetScaler Gateway 设备上的失败。
- 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 Gateway Insight。如果使用其他身份验证类型，您可能会在 Gateway Insight 中看到一些差异。
  - 本地
  - LDAP
  - RADIUS
  - TACACS
  - SAML
  - 本机 OTP

- OAuth-OpenID 连接

  对于 OAuth-OpenID Connect 身份验证，NetScaler 可以充当 OAuth-OpenID 连接信赖方 (RP) 或 OAuth-OpenID 连接身份提供商 (IdP)。身份验证成功后，将在“Gateway Insight”报表的“用户”选项卡下报告用户名。但是，您无法确定会话是在 IdP 还是 RP 创建的。

  注意： NetScaler ADM 13.1 版本 4.xx 及更高版本支持 OAuth-OpenID 连接身份验证。

启用 **Gateway Insight**

要为您的 NetScaler Gateway 设备启用 Gateway Insight，必须首先将 NetScaler Gateway 设备添加到 NetScaler ADM 中。然后必须为表示 VPN 应用程序的虚拟服务器启用 AppFlow。有关向 NetScaler ADM 添加设备的信息，请参阅添加设备。

> 注意
>
> 要在 NetScaler ADM 中查看端点分析 (EPA) 故障，必须在 NetScaler 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 NetScaler ADM 是 **13.0** 版本 **36.27**，则可以执行以下过程来启用 Gateway Insight：

1. 导航到 基础架构 **>** 实例，然后选择要为其启用 AppFlow 的实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。
3. 在“配置智能分析”页的“配置分析”下，选择 **NetScaler 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 **Logstream** 复选框。

   > 注意
   >
   > 您可以选择 **IPFIX** 或 **Logstream** 作为传输模式。
   >
   > 有关 **IPFIX** 和 **Logstream** 的更多信息，请参阅 **Logstream** 概述。

7. 单击确定。

对于 **NetScaler ADM** 版本 **13.0** 版本 **41.x** 或更高版本

1. 导航到 基础架构 **>** 实例，然后选择实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（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 **Logstream**

    b) 选择 **NetScaler Gateway**

5. 单击确定。

使用 **GUI** 在 **NetScaler 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”。

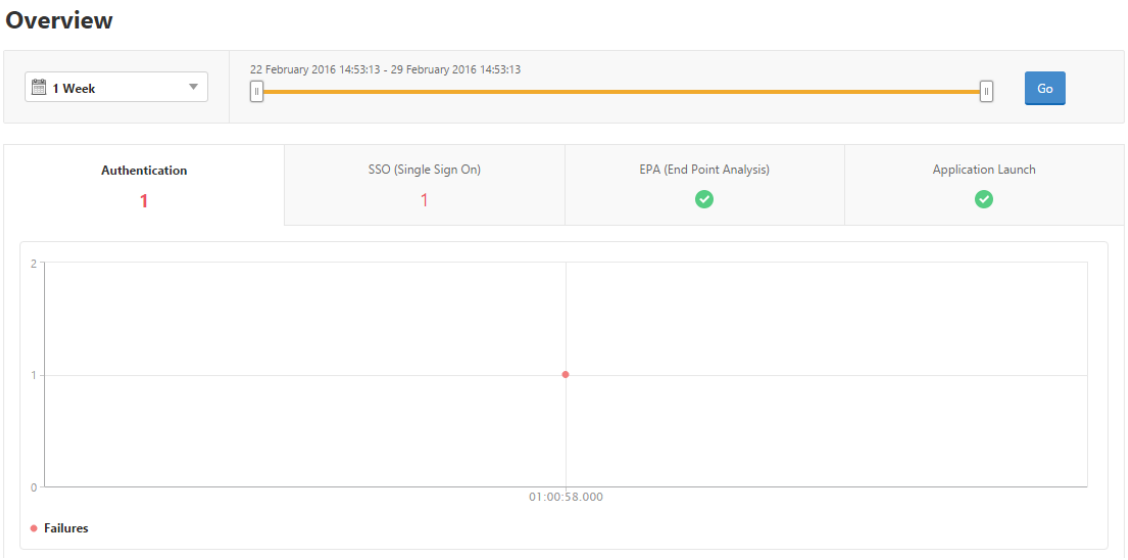
查看 **Gateway Insight** 报告

在 NetScaler ADM 中，您可以查看与 NetScaler 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。NetScaler 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。有关组和将用户分配到组的详细信息，请参阅 配置组。

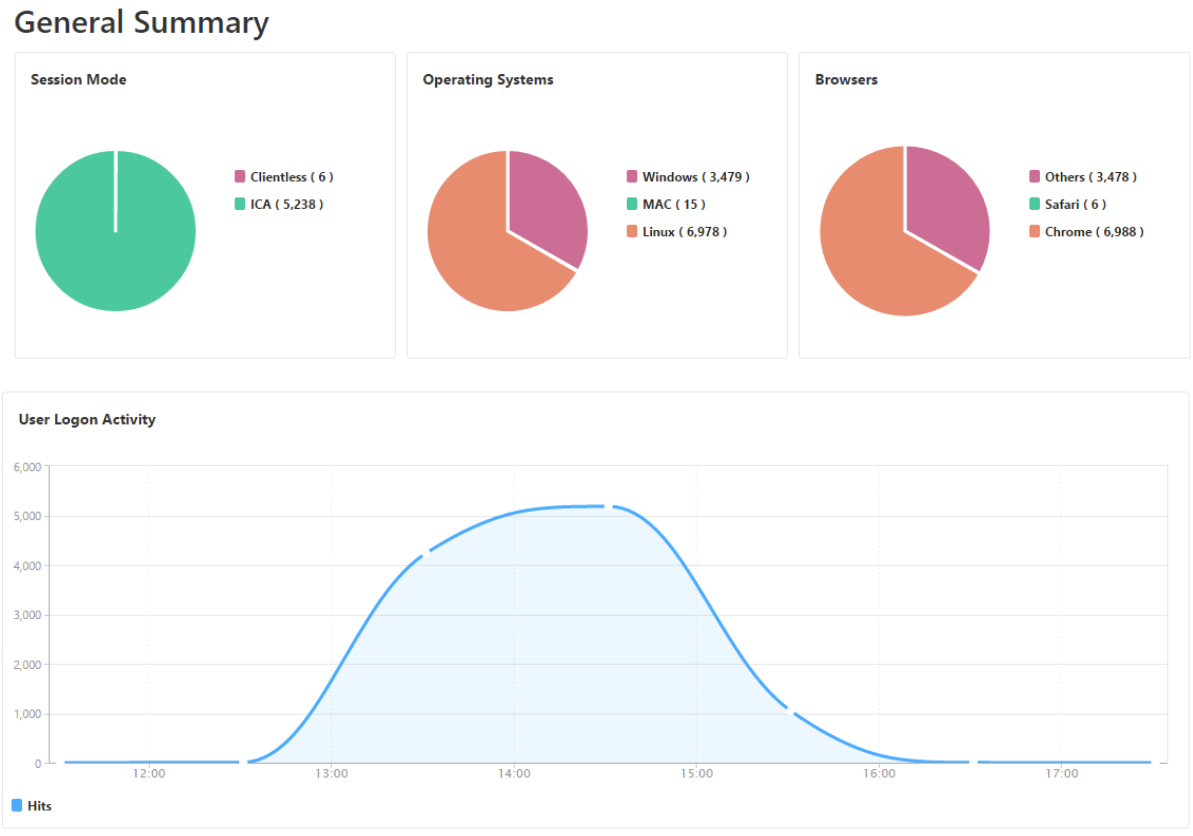
查看 **EPA**、**SSO**、身份验证、授权和应用程序启动失败

1. 在 NetScaler ADM 中，导航到 网关 **> 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 NetScaler ADM 中，导航到 网关 **> Gateway Insight**，向下滚动以查看报告。



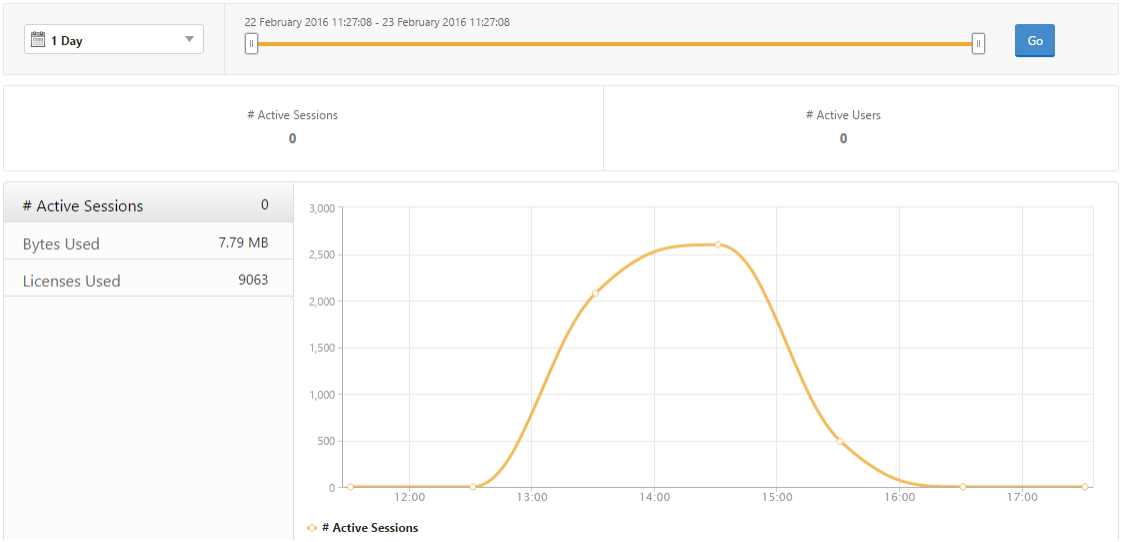
查看用户的 **Gateway Insight** 报告

您可以查看以下各项的报告：

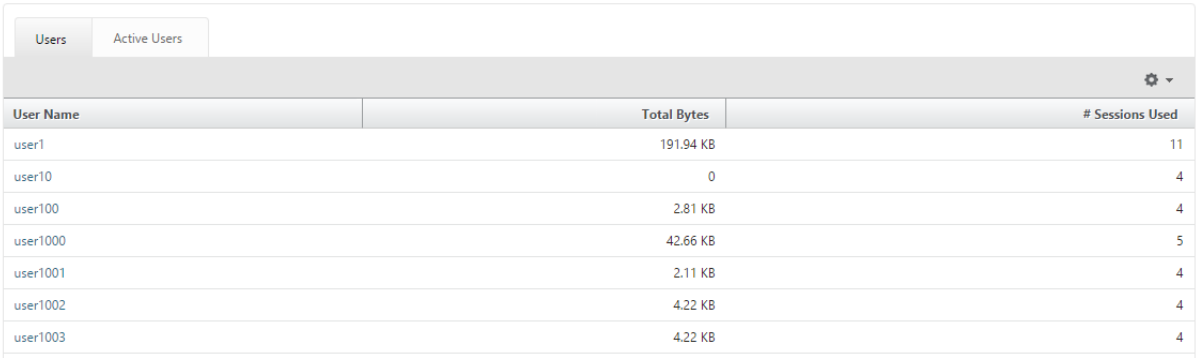
- 与 NetScaler Gateway 设备关联的所有用户。
- 用户的 EPA、身份验证、SSO 和应用程序启动失败。
- 用户的活动和已终止会话的详细信息。
- 会话模式的类型，如全通道、无客户端 VPN 和 ICA 代理。

查看用户详细信息

1. 在 NetScaler ADM 中，导航到网关 **> 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。



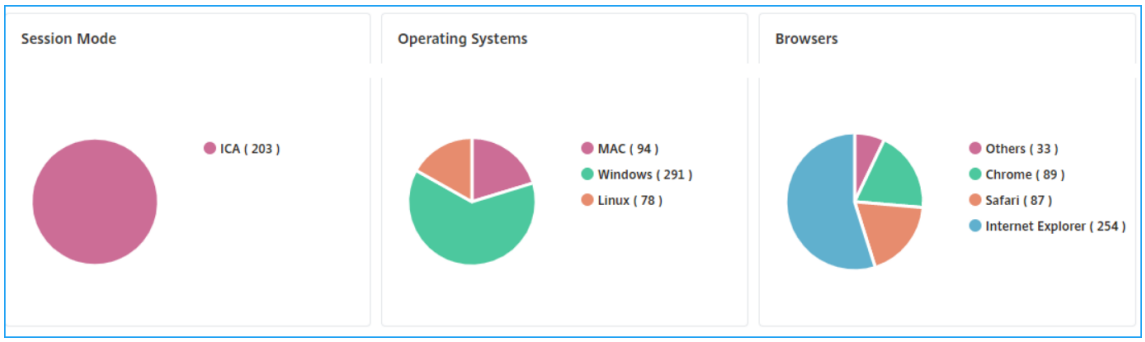
向下滚动可查看可用用户和活动用户列表。



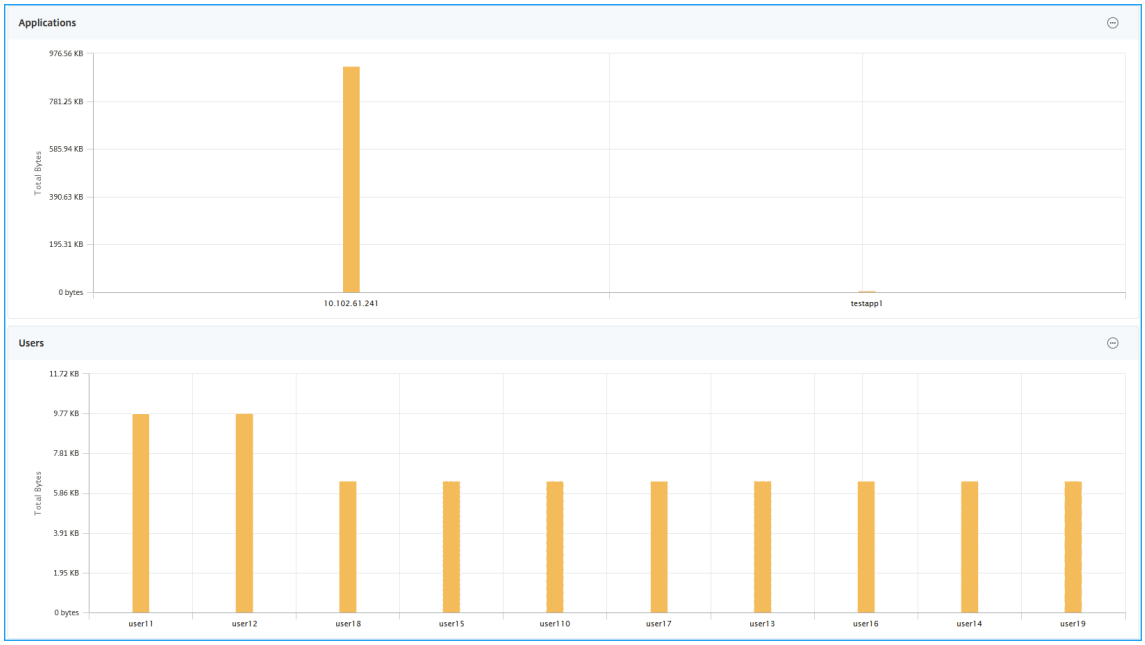
User Name	Total Bytes	# Sessions Used
user1	191.94 KB	11
user10	0	4
user100	2.81 KB	4
user1000	42.66 KB	5
user1001	2.11 KB	4
user1002	4.22 KB	4
user1003	4.22 KB	4

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：

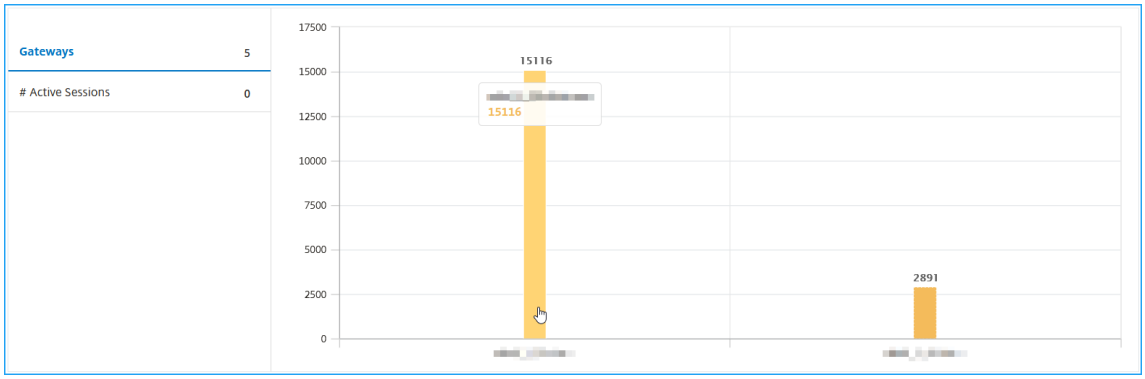
- 用户详细信息 -您可以查看与 ADC Gateway 设备关联的每个用户的见解。导航到网关 > **Gateway Insight** > 用户，然后单击用户以查看所选用户的见解，例如会话模式、操作系统和浏览器。



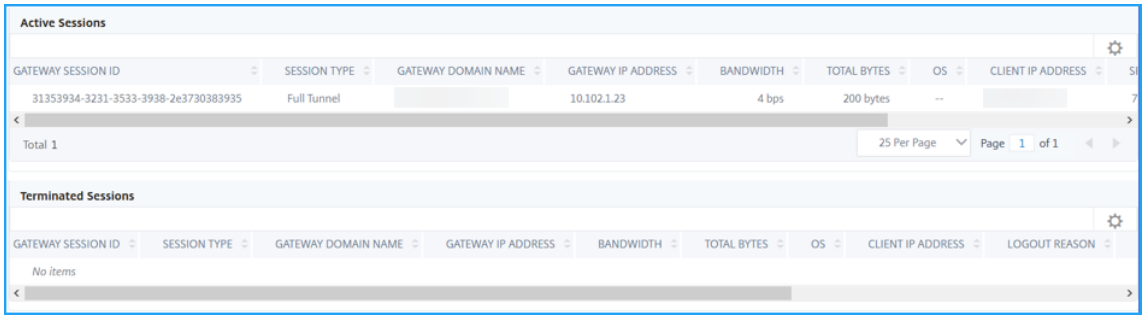
- 选定网关的用户和应用程序 - 导航到网关 > **Gateway Insight** > 网关，然后单击网关域名以查看与所选网关关联的前 10 个应用程序和前 10 个用户。



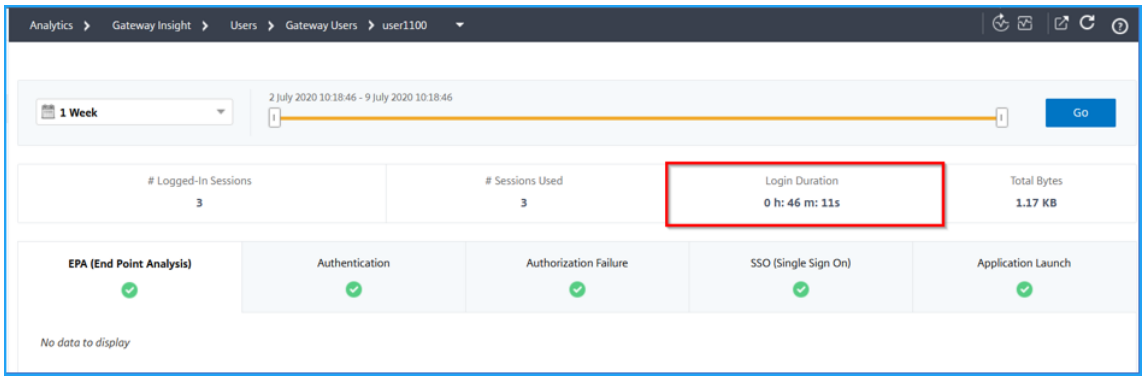
- 查看应用程序和用户的更多选项—对于 10 个以上的应用程序和用户，您可以单击应用程序和用户中的更多图标以查看与所选网关关联的所有用户和应用程序详细信息。
- 通过单击条形图查看详细信息—单击条形图时，可以查看相关详细信息。例如，导航到网关 **> Gateway Insight > 网关**，然后单击网关条形图以查看网关详细信息。



- 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

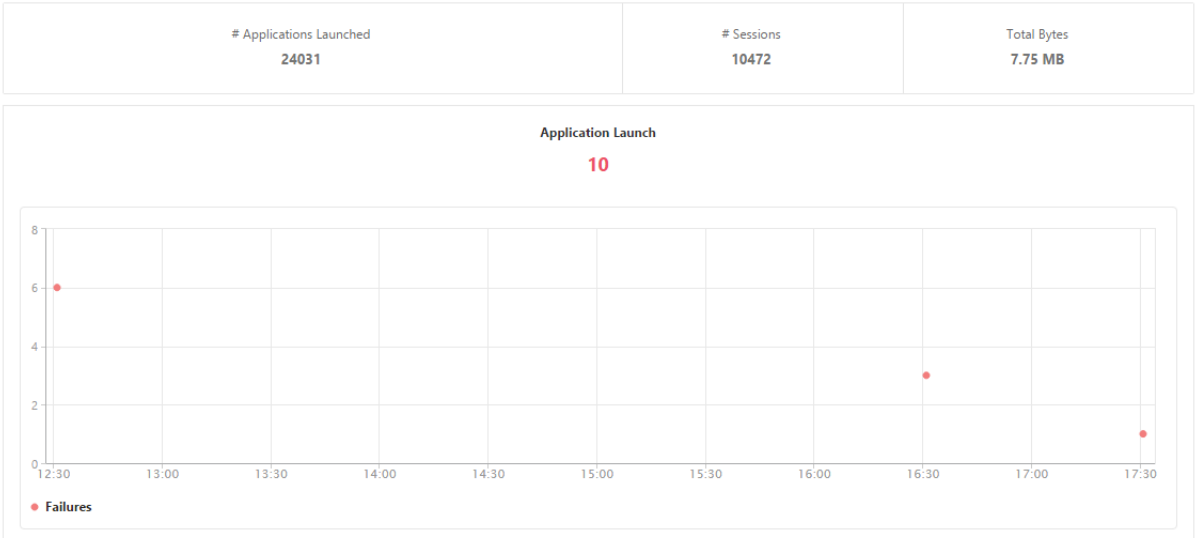
查看应用程序的 **Gateway Insight** 报告

您可以查看已启动的应用程序数量、总会话数和活动会话数、应用程序占用的总字节数和带宽。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 NetScaler ADM 中，导航到网关 **> 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，您可以查看已启动的应用程序数量、总会话数和活动会话数、应用程序占用的总字节数和带宽。



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。

查看网关的 **Gateway Insight** 报告

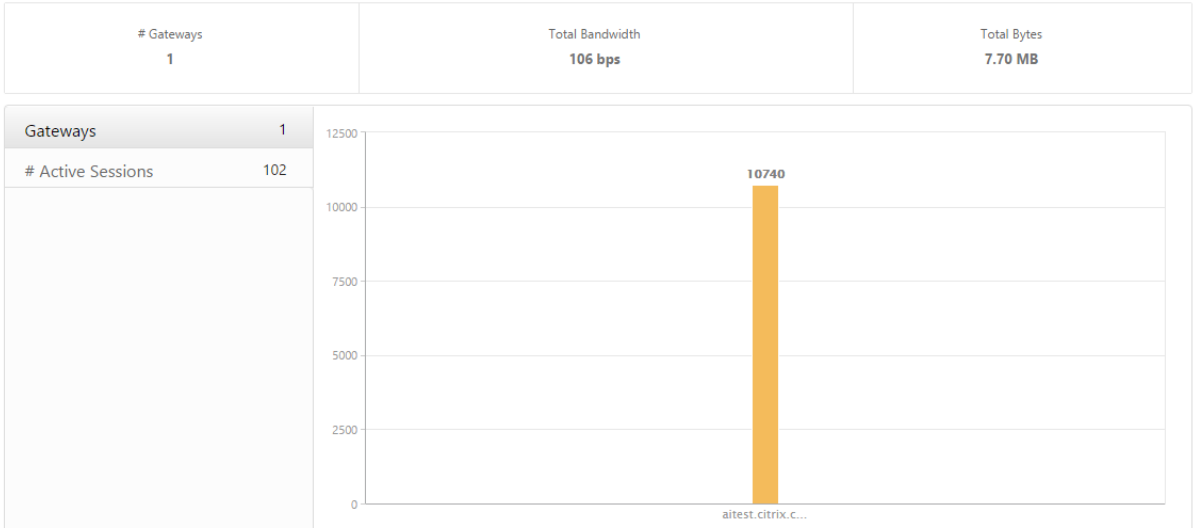
您可以查看任何给定时间与 NetScaler Gateway 设备关联的所有网关使用的网关数量、活动会话数、总字节数和带宽。可以查看某个网关的 EPA、身份验证、单点登录及应用程序启动失败。还可以查看与某个网关关联的所有用户及其

登录活动的详细信息。

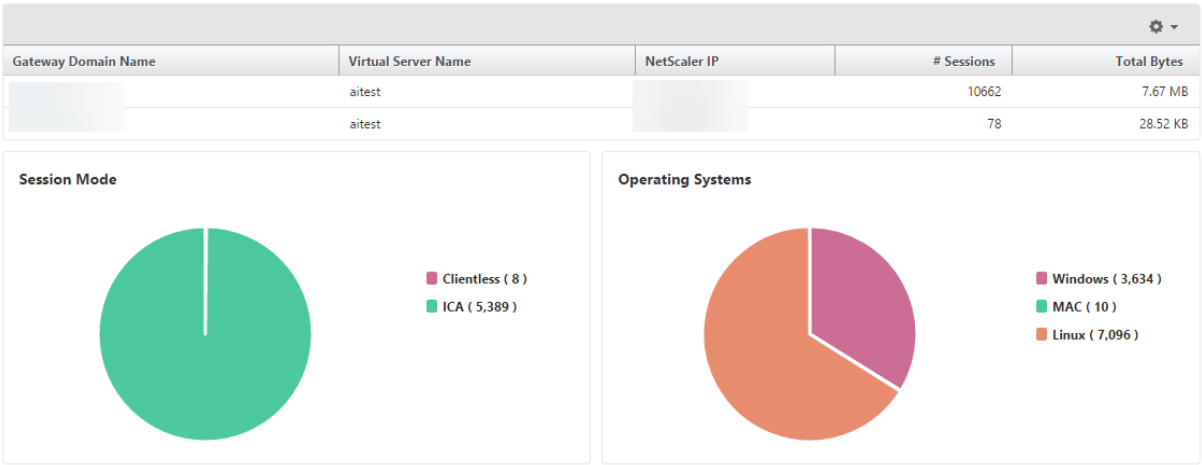
查看网关详细信息

1. 在 **NetScaler ADM** 中，导航到网关 **> Gateway Insight > Gateway Insight > Gateway**。
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 NetScaler 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 Gateway Insight 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 NetScaler ADM 具有 Internet 连接时，才会导出地理地图报告。

导出报告

1. 在“控制板”选项卡的右侧窗格中，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”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“计划导出”下，指定详细信息并单击“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“设置”**>**“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 **Gateway Insight** 控制板：

1. 在“控制板”选项卡的右侧窗格中，单击“导出”按钮。
2. 在“立即导出”下，选择 **PDF** 格式，然后单击“导出”。

Gateway Insight 使用案例

以下使用案例展示了如何使用 Gateway Insight 在 NetScaler Gateway 设备上查看用户的访问详细信息、应用程序和网关。

用户无法登录到 **NetScaler Gateway** 设备或内部 **Web** 服务器

您是 NetScaler Gateway 管理员，通过 NetScaler ADM 监视 NetScaler Gateway 设备，您想看看为什么用户无法登录，或者失败发生在登录过程的哪个阶段。

NetScaler ADM 使您能够在登录过程的以下阶段查看用户登录错误的详细信息：

- 身份验证
- 端点分析 (EPA)
- 单点登录

在 NetScaler 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：

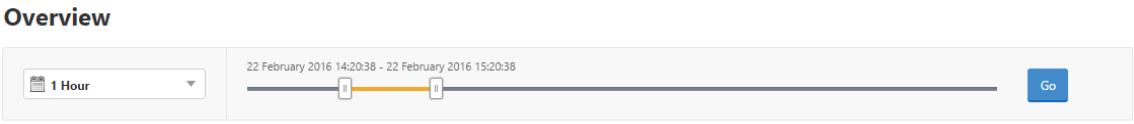
在 NetScaler ADM 中，导航到网关 **> Gateway Insight**，然后在搜索用户文本框中指定要搜索的用户。

身份验证失败

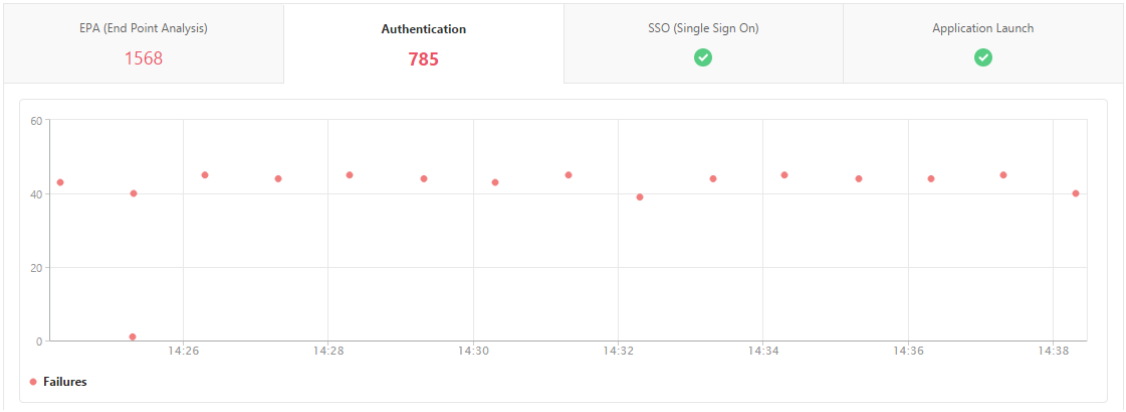
可以查看身份验证错误，例如，凭据错误或身份验证服务器没有响应。您还可以查看身份验证失败的因素。

要查看验证失败的详细信息，请执行以下操作：

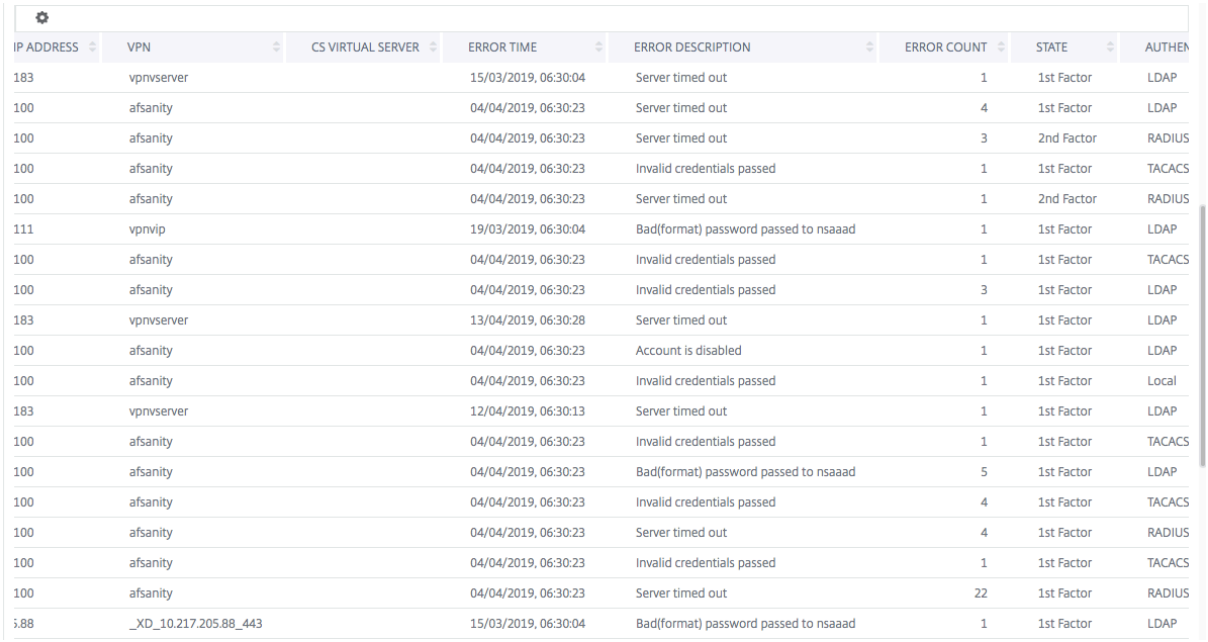
1. 在 NetScaler ADM 中，导航到 网关 **> Gateway Insight**。
2. 在概述部分中，选择要查看身份验证错误的时间段。可以使用时间滑块来进一步自定义所选时间段。单击转到。



3. 单击身份验证选项卡。您可以在故障图中查看任何给定时间的身份验证错误数量。



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 错误描述 列显示登录失败的原因，状态 列显示失败发生的第 n 个因素。



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。您可以使用设置图标自定义表格以添加或删除列。

> 重要：
>
> 如果 OAuth-OpenID 连接身份验证失败，则某些失败（例如“令牌验证失败”）的用户名会在 Gateway Insight 报告中显示为不适用。在此失败中，由于 OAuth-OpenID 连接信赖方的“令牌验证失败”，用户名无法用于身份验证失败。

USERNAME	CITRIX ADC IP ADDRESS	CLIENT IP ADDRESS	GATEWAY IP ADDRESS	VPN	CS VIRTUAL SERVER	ERROR DESCRIPTION
-NA-				gitest.citrix.com		Relying party: Token verification failed
-NA-				gitest.citrix.com		Relying party: Incoming URL query parameter from user agent is NULL in /nf/auth/doOAuth requ
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				gitest.citrix.com		Relying party: Action query parameter isn't present in the URL from user agent in /nf/auth/doOA
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token verification failed
-NA-				vpnvserver		Relying party: Token decryption failure

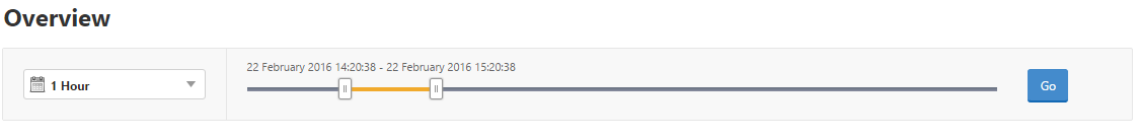
环保局失败

您可以在身份验证前或身份验证后阶段查看 EPA 失败。

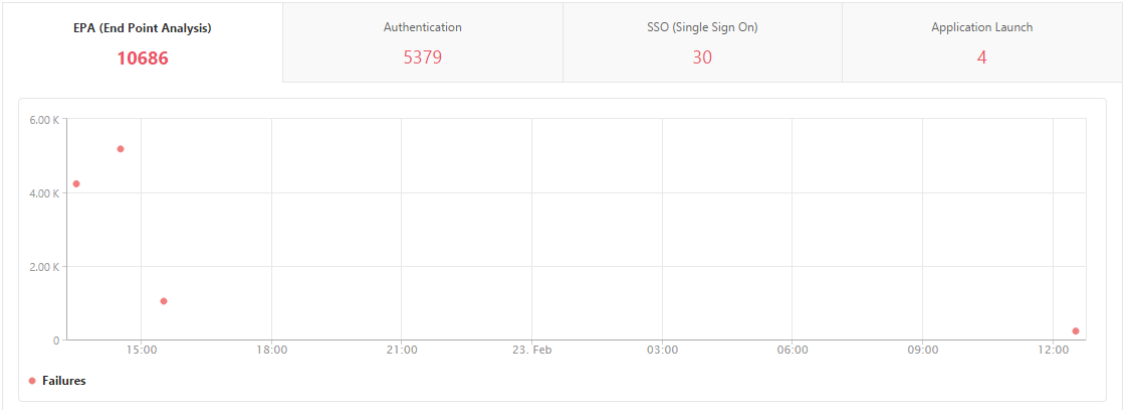
> 重要：
>
> - 仅当配置了经典表达式时，才会报告 EPA 失败。
> - 如果在身份验证前或身份验证后策略中配置了高级表达式，则不会报告 EPA 失败。
> - 如果将 EPA 配置为 nFactor 身份验证流程中的一个因素，则不会报告 EPA 失败。

要查看 **EPA** 失败详细信息，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 网关 **> Gateway Insight**。
2. 在“Overview”（概述）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。您可以使用向下箭头自定义表格以添加或删除列。

> 注意
>
> 将“clientSecurity”表达式配置为 VPN 会话策略规则时，NetScaler Gateway 不会报告 EPA 故障。

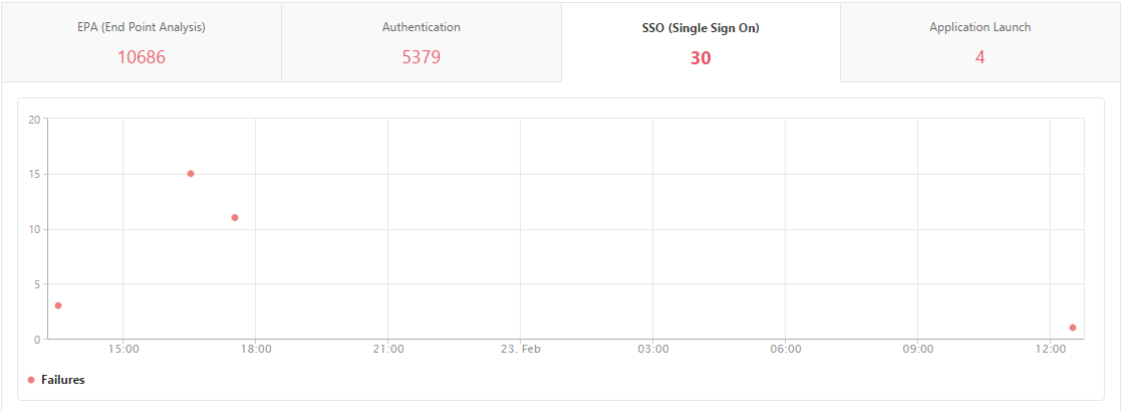
SSO 故障

可以查看通过 NetScaler Gateway 设备访问任何应用程序的用户在任何阶段的所有 SSO 失败。

要查看 **SSO** 故障详细信息，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 网关 **> 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

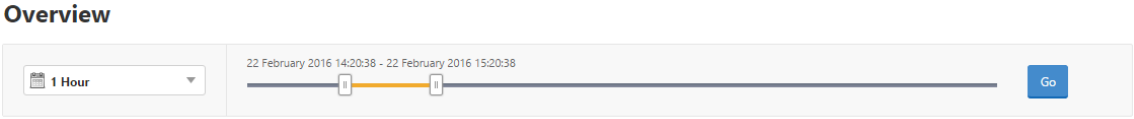
您可以单击“用户 名”列中的用户以显示该用户的 SSO 错误和其他详细信息。您可以使用向下箭头自定义表格以添加或删除列。

成功登录到 **NetScaler Gateway** 后，用户将无法启动任何虚拟应用程序

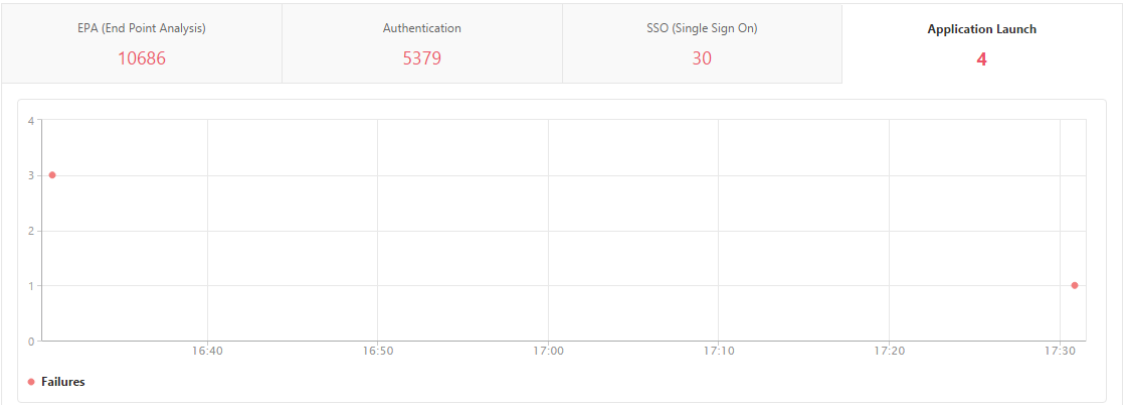
对于应用程序启动失败，您可以了解原因，例如无法访问的安全票证颁发机构 (STA) 或 Citrix 虚拟应用程序服务器或 STA 票证无效。可以查看错误发生的时间、错误的详细信息以及 STA 验证失败的资源。

查看应用程序启动失败的详细信息：

1. 在 NetScaler ADM 中，导航到 网关 **> Gateway Insight**。
2. 在概述部分中，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

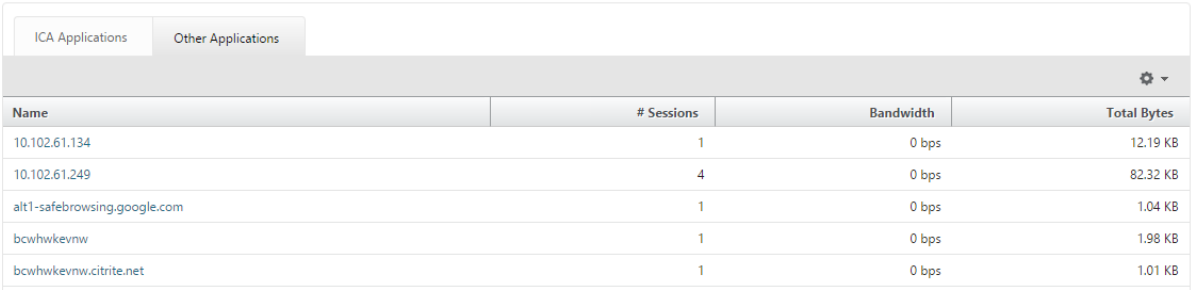
您可以单击“用户 名”列中的用户以显示该用户的应用程序启动错误和其他详细信息。您可以使用向下箭头自定义表格以添加或删除列。

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

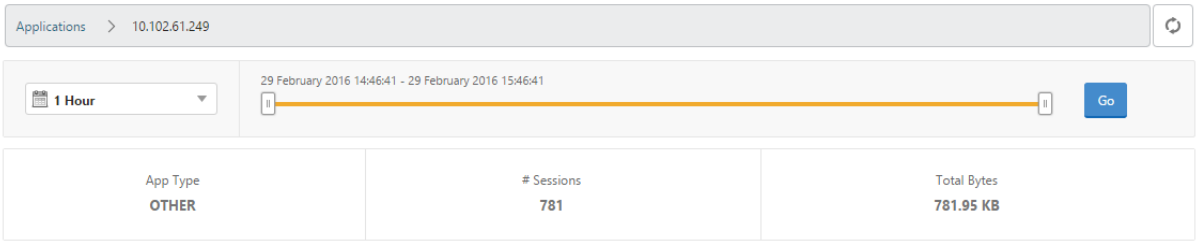
成功启动新应用程序后，可以在 NetScaler ADM 中查看该应用程序占用的总字节和带宽。

要查看应用程序消耗的总字节和带宽，请执行以下操作：

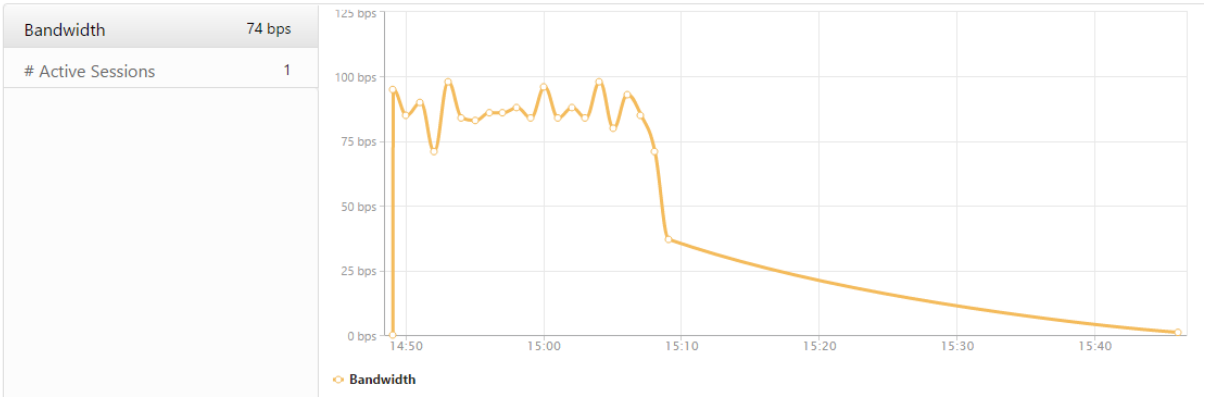
在 NetScaler ADM 中，导航到网关 **> Gateway Insight >** 应用程序，向下滚动，然后在其他应用程序选项卡上，单击要查看其详细信息的应用程序。



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。

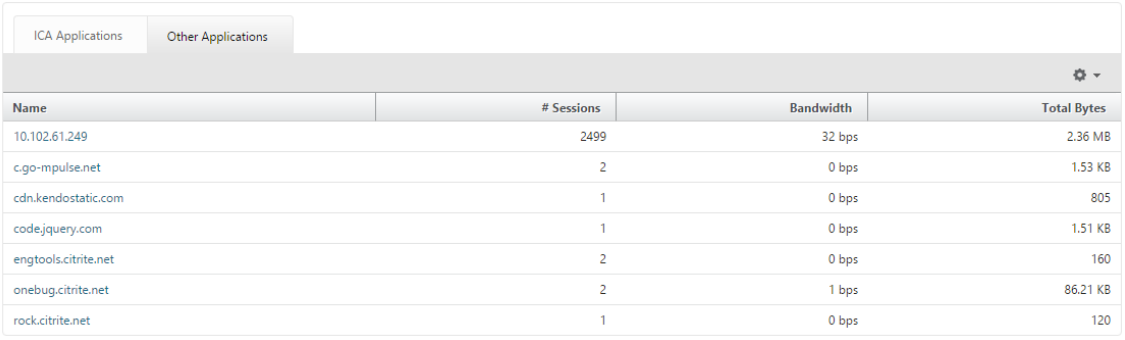


用户已成功登录到 **NetScaler Gateway**，但无法访问内部网络中的某些网络资源

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 NetScaler ADM 中，导航到 **Gateway > Gateway Insight >** 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

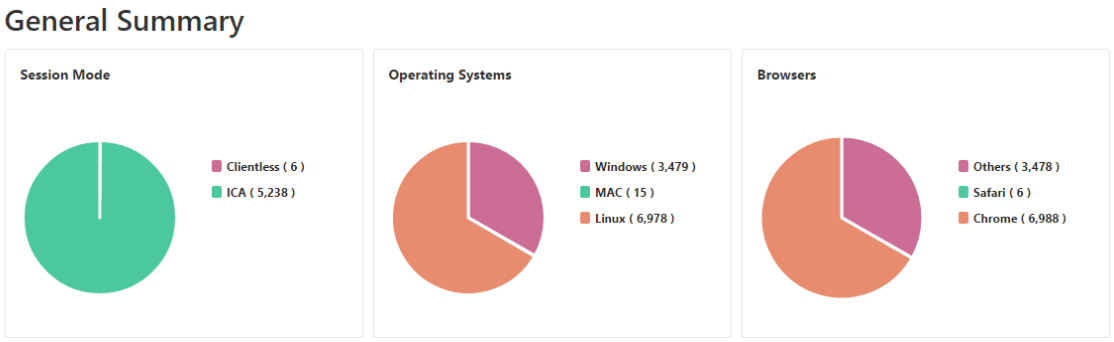
3. 向下滚动，在“用户”表中，将显示所有有权访问该应用程序的用户。

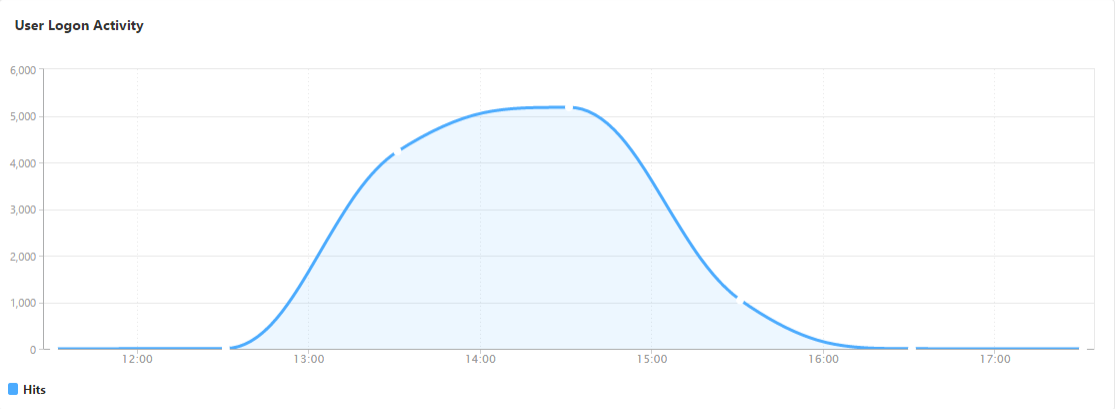
不同的用户可能正在使用不同的 **NetScaler Gateway** 部署，也可能通过不同的访问模式登录到 **NetScaler Gateway**。管理员必须能够查看有关部署类型和访问模式的详细信息

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经典 NetScaler 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 NetScaler ADM 中，导航到 网关 **> 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。





对 **Gateway Insight** 问题进行故障排除

February 6, 2024

如果 Gateway Insight 解决方案无法按预期运行，则问题可能出在以下任一方面。有关故障排除，请参阅相应部分中的清单。

- Gateway Insight 配置。
- NetScaler 和 NetScaler ADM 之间的连接问题。
- 在 NetScaler 中生成记录。
- 在 NetScaler ADM 中进行验证。

Gateway Insight 配置清单

- 确保 NetScaler 设备中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 NetScaler 运行配置中的 Gateway Insight 配置。

  运行 `show running | grep -i <appflow_policy>` 命令以检查 Gateway Insight 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 Gateway Insight 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 NetScaler Gateway/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。

NetScaler 与 NetScaler ADM 之间的连接检查表

- 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 NetScaler 和 AppFlow Collector 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“设置”**>**“**AppFlow**”**>**“策略”以查看 AppFlow 策略命中。
- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

NetScaler 核对清单中的记录生成

- 运行 `nsconmsg -d stats -g ai_tot` 命令并检查 NetScaler 中的统计数据增量。
- 捕获 `nstrace logs` 并检查 CFLOW 数据包以确认 NetScaler 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 NetScaler 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 NetScaler ADM 正在接收 AppFlow 记录。
- 确保 NetScaler 实例已添加到 NetScaler ADM。
- 确保 NetScaler Gateway/VPN 虚拟服务器已在 NetScaler ADM 中获得许可。

在 NetScaler ADM 中验证 Logstream 日志

可以使用以下方法验证 NetScaler ADM 接收的 Logstream 数据：

- 在 **NetScaler 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_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

NetScaler 日志中的 **AppFlow** 记录

从版本 13.0 版本开始，您可以检查 NetScaler 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

要快速解决问题，请确保在联系 Citrix 技术支持之前已掌握以下信息：

- 部署和网络拓扑的详细信息。
- NetScaler 和 NetScaler ADM 版本。
- 适用于 NetScaler 和 NetScaler ADM 的技术支持包。
- `nstrace` 在问题期间捕获。

已知问题

有关 Gateway Insight 的已知问题，请参阅 ADC 发行说明。

HDX Insight

February 6, 2024

HDX Insight 为通过 NetScaler 流向 Citrix Virtual Apps 和桌面的 HDX 流量提供端到端的可见性。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 NetScaler Application Delivery Management (ADM) 能够支持各种用例。

要显示任何数据，您需要在 NetScaler Gateway 虚拟服务器上启用 AppFlow。AppFlow 可以通过 IPFIX 协议或 Logstream 方法传递。

> 注意
>
> 要允许记录 ICA 往返时间计算，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获取带宽信息，例如音频、打印机映射和客户端驱动器映射。

> 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。NetScaler 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。

> 有关组和将用户分配到组的详细信息，请参阅 配置组。

您还可以导航到 网关 **> 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网关 **> HDX Insight >** 用户来查看所有已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 NetScaler 实例中配置的管理分区。

下列瘦客户端支持 HDX Insight：

- WYSE 基于 Windows 的瘦客户端
- WYSE 基于 Linux 的瘦客户端
- WYSE 基于 ThinOS 的瘦客户端
- 基于 10ZiG Ubuntu 的瘦客户端

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。

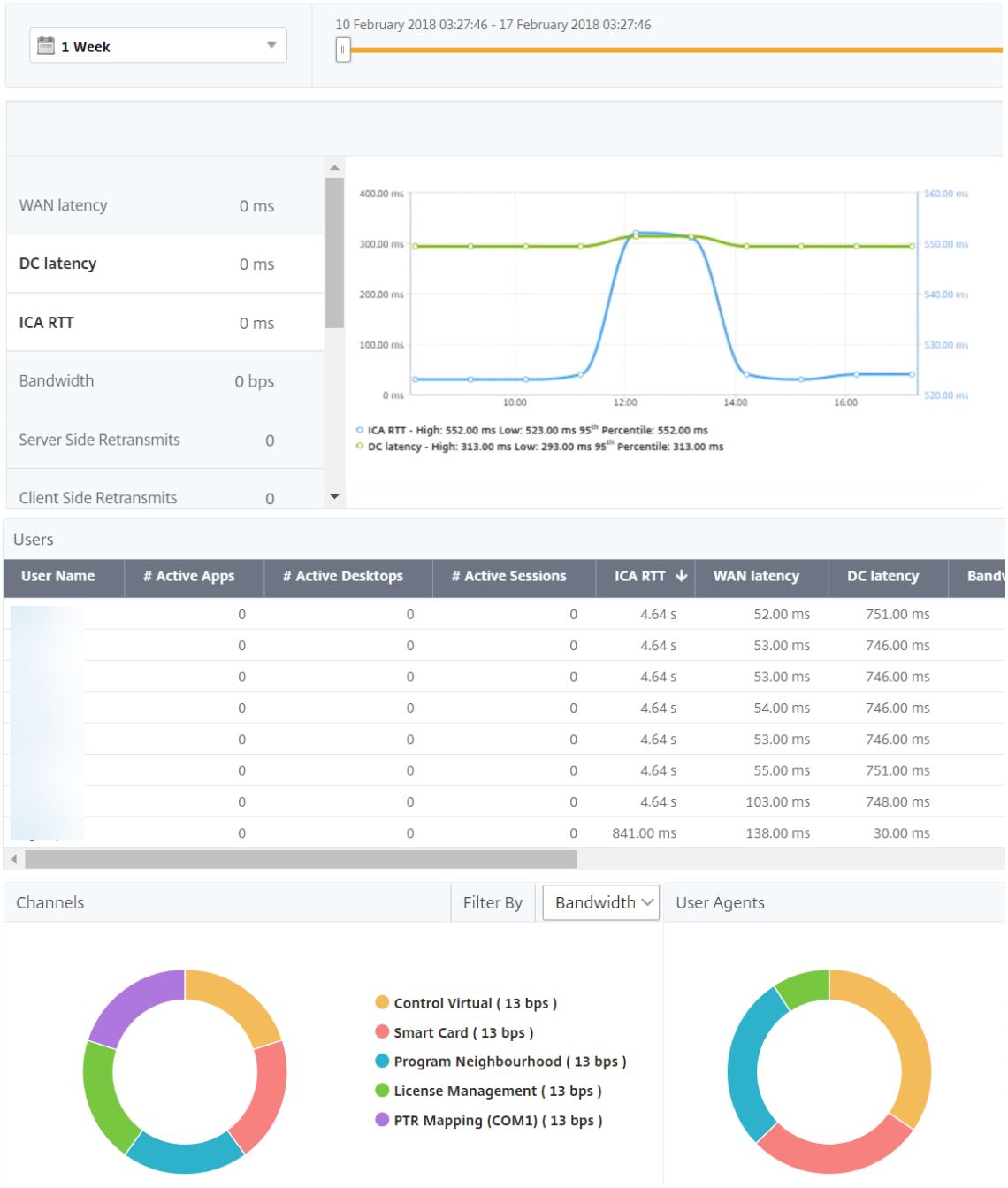
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟或客户端网络延迟造成。

为了找出问题的根本原因，请分析下列指标：

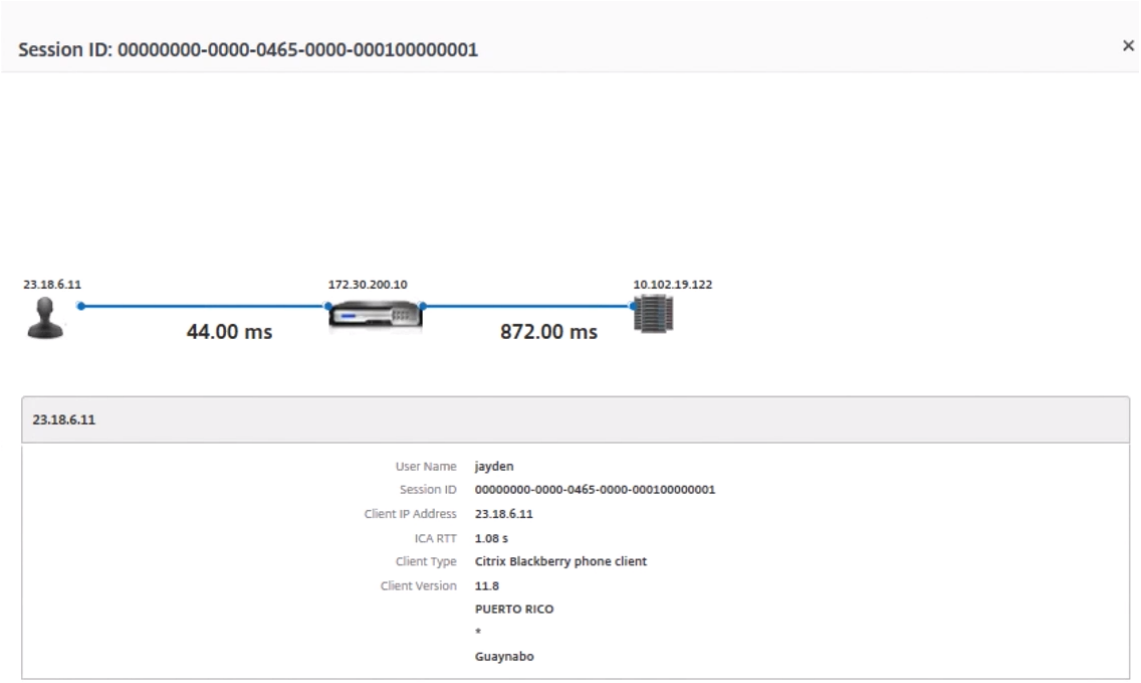
- WAN 延迟
- DC 延迟
- 主机延迟

要查看客户端度量，请执行以下操作：

1. 导航到 网关 **> HDX Insight >** 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。



总结　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

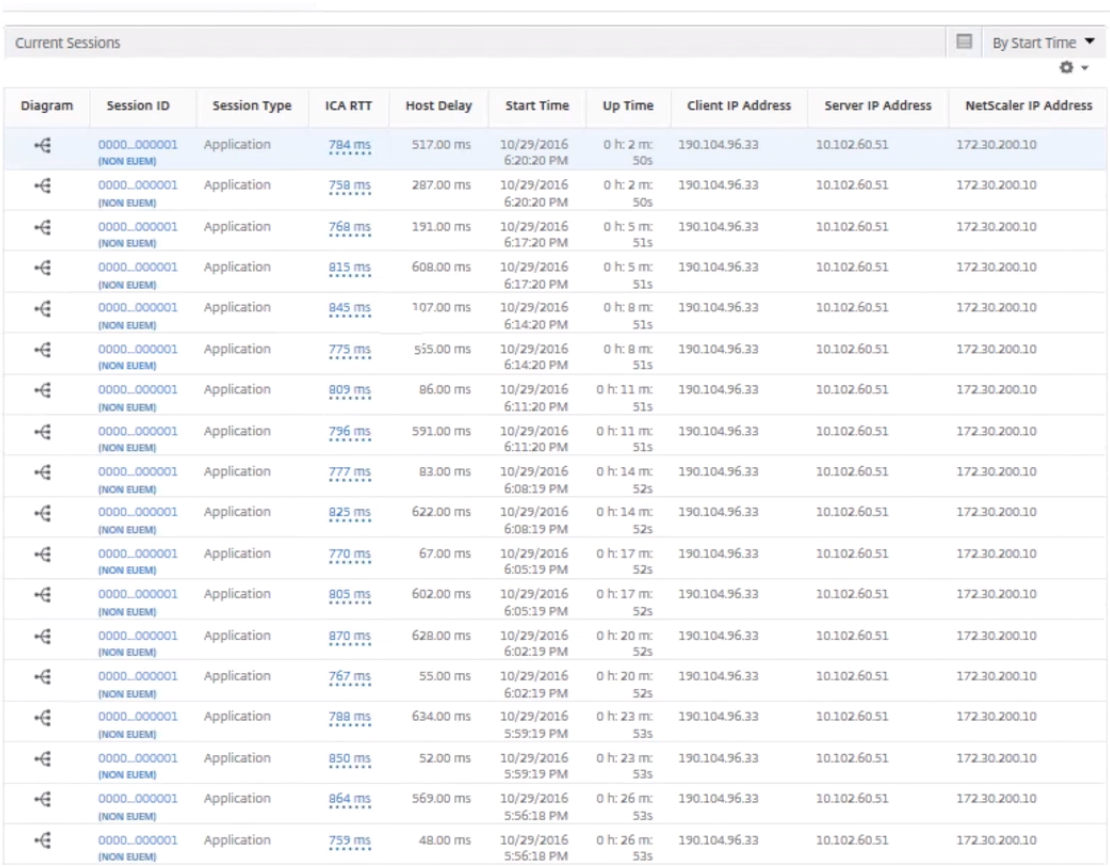
延迟可能是由于服务器网络延迟、服务器网络导致的 ICA 通信延迟、客户端网络延迟或应用程序启动所用时间造成。

为了找出问题的根本原因，请分析下列指标：

- WAN 延迟
- DC 延迟
- 主机延迟

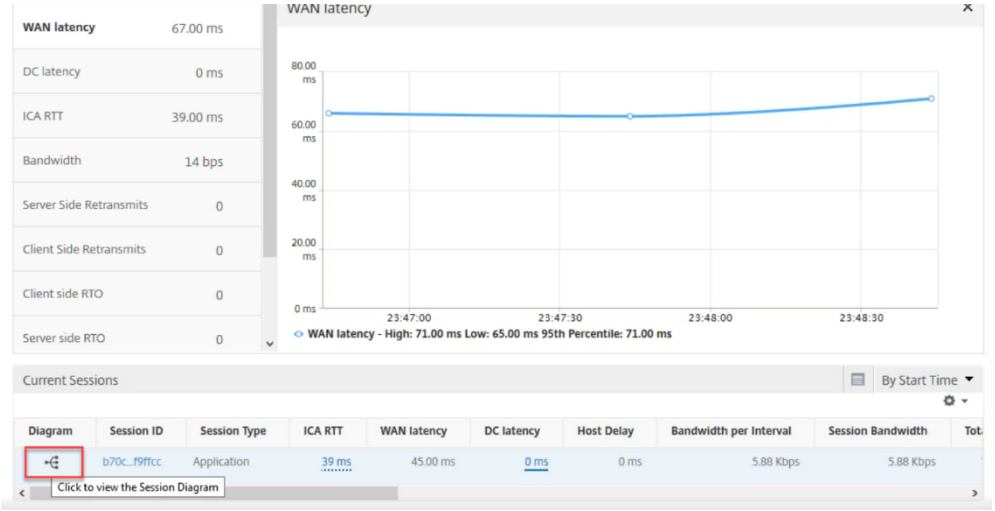
要查看用户指标，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 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。



总结　在此示例中，直流延迟为 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 NetScaler 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，请导航到网关 **> 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

NetScaler ADM 地理地图功能在地图上显示应用程序在不同地理位置的使用情况。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。

您可以通过指定特定地理位置或局域网的专用 IP 范围（起始和结束 IP 地址）来配置 NetScaler ADM 以显示该位置的地理地图。

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。导航到网关 **> HDX Insight**，然后在地图的 世界 部分中，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：

导航到 设置 **>** 分析设置 **> IP** 区块，为特定位置配置地理地图。

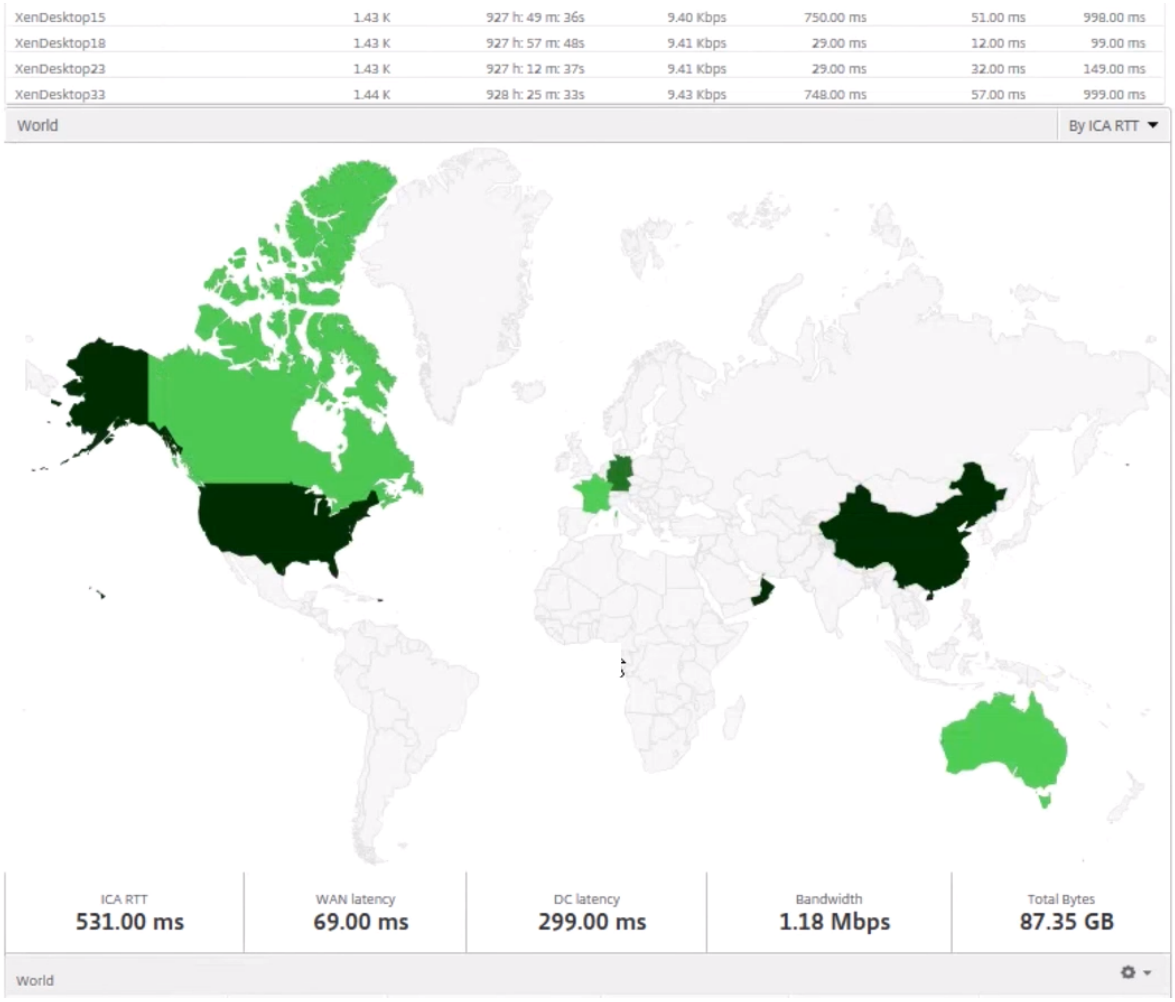
用例

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。

圣克拉拉的用户使用 NetScaler Gateway 设备连接到 SClara.x.com 来访问 VPN 流量。印度的用户使用 NetScaler Gateway 设备连接到 India.x.com 来访问 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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler Gateway，以便用户有两个本地 NetScaler Gateway 设备来访问 VPN。



限制

如果 NetScaler 实例具有高级许可证，则不会触发 NetScaler 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

February 6, 2024

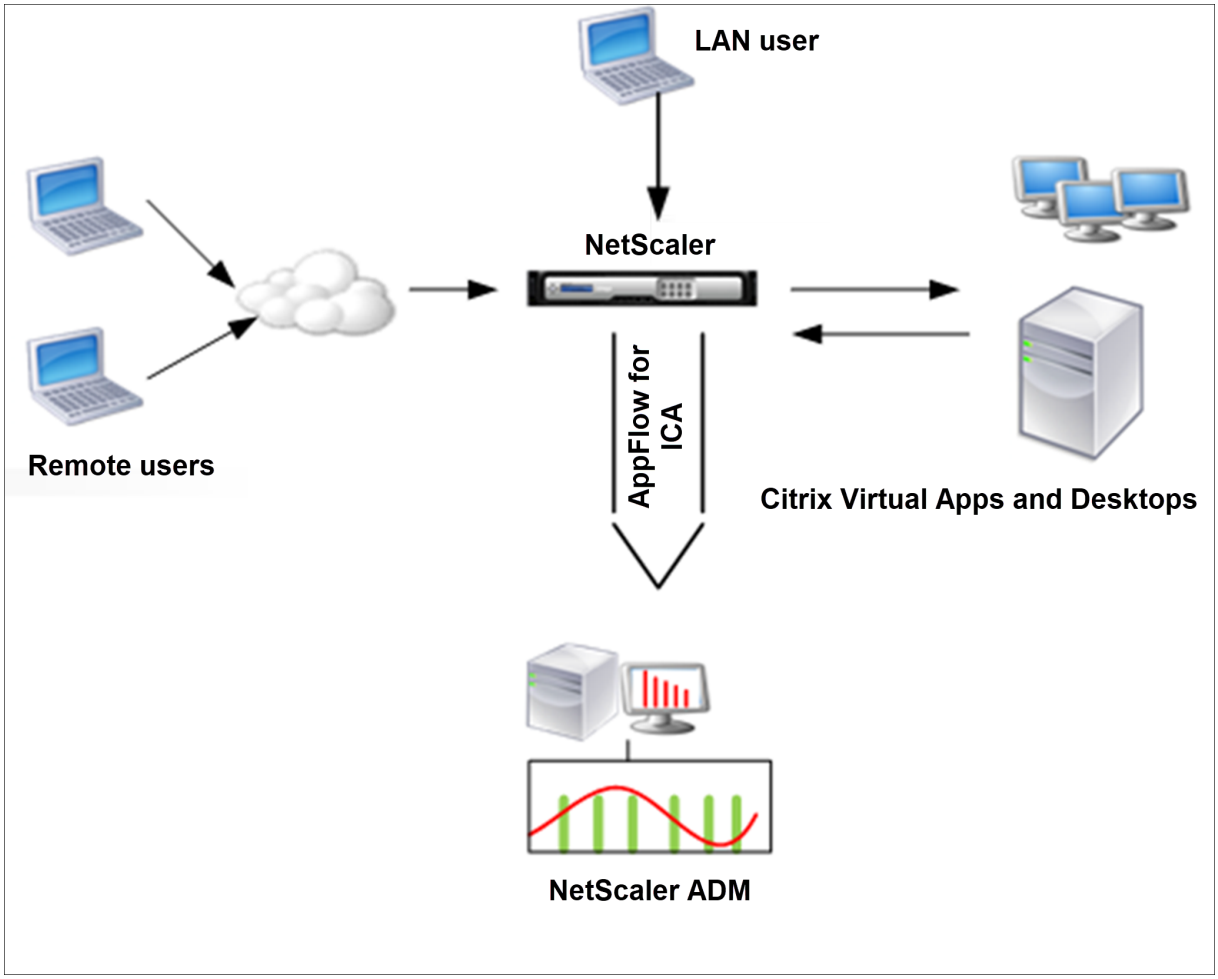
HDX Insight 是 NetScaler Application Delivery Management (ADM) 分析的一部分，为通过 NetScaler 实例的 ICA 流量提供前所未有的端到端可见性，使 IT 能够提供卓越的用户体验。HDX Insight 为网络、虚拟桌面、应用程序和应用程序结构提供引人注目且强大的商业智能和故障分析功能。HDX Insight 可以即时鉴别分类用户问题、收集有关虚拟桌面连接的数据、生成 AppFlow 记录并将其呈现为可视报告。

在 NetScaler 中启用数据收集的配置因设备在部署拓扑中的位置而异。

启用数据收集以监视在局域网用户模式下部署的 NetScaler

访问 Citrix Virtual Apps and Desktops 应用程序的外部用户必须在 NetScaler Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 NetScaler Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便请求重定向至 NetScaler 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 NetScaler Gateway 设备上的 SOCTS 代理）以 LAN 用户模式部署 NetScaler 设备。



> 注意 NetScaler ADM 和 NetScaler Gateway 设备位于同一子网中。

要监视在此模式下部署的 NetScaler 设备，请先将 NetScaler 设备添加到 NetScaler Insight 清单，启用 AppFlow，然后在控制板上查看报告。

将 NetScaler 装置添加到 NetScaler 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“设置”**>**“**AppFlow**”**>**“收集器”，以检查收集器（即 NetScaler ADM）

> 是否已启动。NetScaler 实例使用 NSIP 将 AppFlow 记录发送到 NetScaler ADM。但是该实例使用其 SNIP 来验证与 NetScaler ADM 的连接。因此，请确保在实例上配置 SNIP。
> - 无法使用 NetScaler ADM 配置实用程序在局域网用户模式下部署的 NetScaler 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 **NetScaler** 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 NetScaler Gateway 设备访问局域网网络，请添加与 VPN 流量匹配的策略要应用的操作。

```
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 NetScaler ADM 添加为 NetScaler 设备上的 AppFlow 收集器。

```
add appflow collector <name> -IPAddress <ip_addr>
<!--NeedCopy-->
```

Example:

‘‘‘

add appflow collector MyInsight -IPAddress 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_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`

为在单跃点模式下部署的 **NetScaler Gateway** 设备启用数据收集

在单跃点模式下部署 NetScaler Gateway 时，它位于网络的边缘。网关实例提供与桌面交付基础架构的代理 ICA 连接。单跃点是最简单、最常见的部署。如果外部用户尝试访问组织中的内部网络，单跃点模式可提供安全性。
在单跃点模式下，用户通过虚拟专用网络 (VPN) 访问 NetScaler 设备。

要开始收集报告，必须将 NetScaler Gateway 设备添加到 NetScaler Application Delivery Management (ADM) 清单中，然后在 ADM 上启用 AppFlow。

要从 **NetScaler ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 NetScaler 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. 导航到基础架构 **>** 实例，然后选择要启用分析的 NetScaler 实例。
4. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（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。

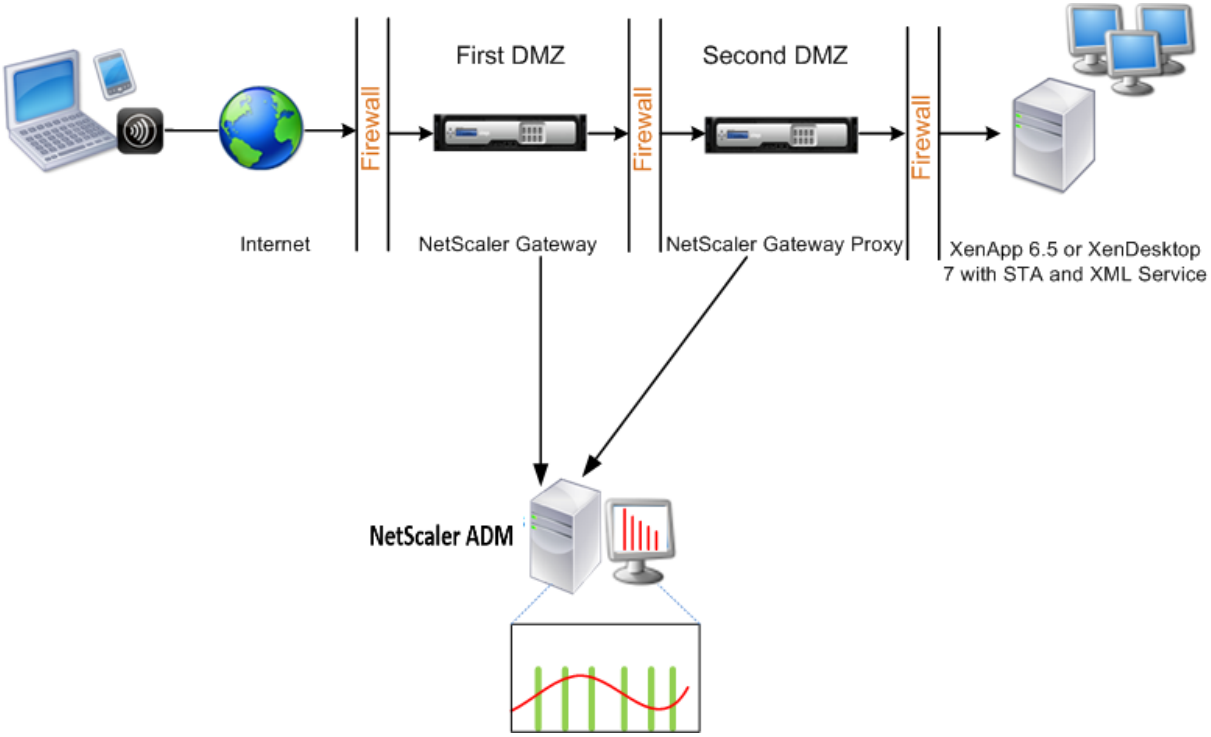
> 注意
>
> 在单跃点模式下启用 AppFlow 时，以下命令将在后台运行。此处显式指定这些命令是为了进行故障排除。

```
1  -  add appflow collector <name> -IPAddress <ip_addr>
2
3  -  add appflow action <name> -collectors <string>
4
5  -  set appflow param -flowRecordInterval <secs>
6
7  -  disable ns feature AppFlow
8
9  -  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 NetScaler 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 NetScaler ADM 上仍会显示剩余的 HDX Insight 数据。

为在双跃点模式下部署的 **NetScaler Gateway** 设备启用数据收集

NetScaler 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（NetScaler 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 NetScaler ADM，以便 NetScaler Gateway 设备报告这些生命统计数据。



第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 NetScaler Gateway 充当 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。

NetScaler ADM 可以部署在属于第一个 DMZ 中 NetScaler Gateway 设备的子网中，也可以部署在属于 NetScaler Gateway 设备的第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 NetScaler ADM 和 NetScaler Gateway 部署在同一个子网中。

在双跃点模式下，NetScaler ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 NetScaler Gateway 设备添加到 NetScaler ADM 清单并启用数据收集后，每个设备都会通过跟踪跳数和连接链 ID 来导出报告。

为了让 NetScaler 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。跃点数表示流量从客户端流向服务器的 NetScaler Gateway 设备的数量。连接链 ID 表示客户端与服务器之间的端到端连接。

NetScaler ADM 使用跳数和连接链 ID 来关联来自两个 NetScaler Gateway 设备的数据并生成报告。

要监视在此模式下部署的 NetScaler Gateway 装置，必须首先将 NetScaler Gateway 添加到 NetScaler ADM 清单中，启用 NetScaler ADM 上的 AppFlow，然后在 NetScaler ADM 控制板上查看报告。

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. 导航到基础架构 **>** 实例，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（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 6。

在 **NetScaler ADM** 上启用数据收集

如果启用 NetScaler 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。要克服这种情况，您必须在第一台 NetScaler Gateway 设备上启用 AppFlow for ICA，然后在第二台设备上启用 AppFlow for TCP。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 **NetScaler ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 在 Web 浏览器中，键入 NetScaler 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. 导航到基础架构 **>** 实例，然后选择要启用分析的 NetScaler 实例。
4. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（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**，然后分别为 **ICA** 流量或 **TCP** 流量选择 ICA 或 TCP 流量。

   > 注意
   >
   > 如果没有为 NetScaler 设备上的相应服务或服务组启用 AppFlow 日志记录，即使 Insight 列显示已启用，NetScaler ADM 控制板也不会显示记录。

7. 单击确定。

配置 **NetScaler Gateway** 设备以导出数据

安装 NetScaler Gateway 设备后，必须在 NetScaler Gateway 设备上配置以下设置，以便将报告导出到 NetScaler ADM：

- 在第一个和第二个 DMZ 中配置 NetScaler Gateway 设备的虚拟服务器以相互通信。

- 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。
- 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。
- 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。
- 允许其中一个 NetScaler Gateway 设备导出 ICA 记录
- 允许其他 NetScaler Gateway 设备导出 TCP 记录：
- 在两个 NetScaler Gateway 设备上启用连接链接。

使用命令行界面配置 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 虚拟服务器配置为与第二个 DMZ 中的 NetScaler 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 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。在第一个 DMZ 中的 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 NetScaler 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 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 配置为与第二个 DMZ 中的 NetScaler Gateway 进行通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。
   a) 在“配置”选项卡上，展开 **NetScaler 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) 单击下一个跃点服务器并将下一个跃点服务器绑定到第二台 NetScaler Gateway 设备。
2. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。
   a) 在“配置”选项卡上，展开 **NetScaler 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，选择双跃点，然后单击“确定”。
3. 在第二个 DMZ 中的 NetScaler Gateway 上禁用虚拟服务器上的身份验证。
   a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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 NetScaler Gateway 设备以导出 TCP 记录。
   a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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 NetScaler Gateway 设备以导出 ICA 记录：

   a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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）。

6. 在两个 NetScaler 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) 在右侧窗格的“设置”组中，双击“更改 **AppFlow** 设置”。

   c) 选择 **Connection Chaining**（连接链）并单击 **OK**（确定）。

7. 将第一个 DMZ 中的 NetScaler Gateway 配置为与第二个 DMZ 中的 NetScaler Gateway 进行通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。

   a) 在“配 置”选项卡上，展 开 **NetScaler 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台 NetScaler Gateway 设备。

8. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。

   a) 在“配 置”选项卡上，展 开 **NetScaler 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“双跃点”，然后单击“确定”。

9. 在第二个 DMZ 中的 NetScaler Gateway 上禁用虚拟服务器上的身份验证。

   a) 在“配置”选项卡上，展开 NetScaler 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”，然后清除“启用身份验证”。

10. 启用其中一个 NetScaler Gateway 设备以导出 TCP 记录。

    a) 在“配 置”选项卡上，展 开 **NetScaler 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，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. 允许其他 NetScaler Gateway 设备导出 ICA 记录。

a) 在“配 置”选项卡上，展 开 **NetScaler 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，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 NetScaler Gateway 设备上启用连接链接。

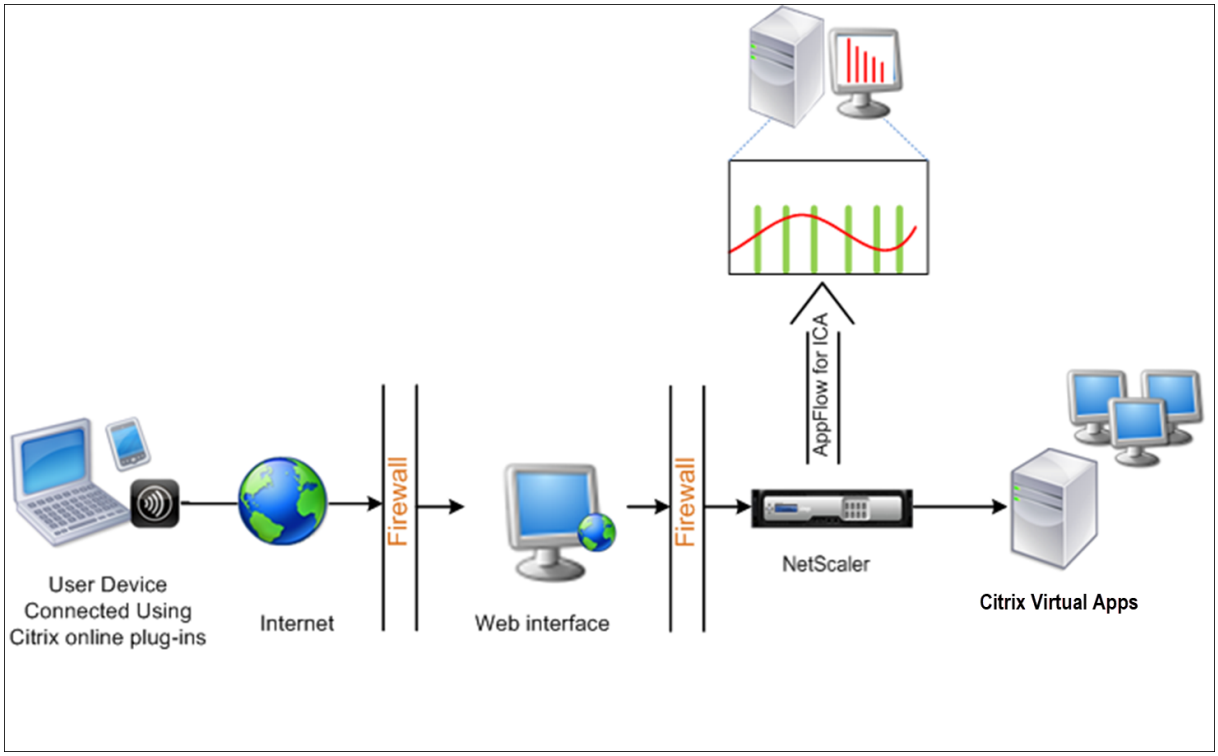
启用数据收集以监视在透明模式下部署的 **NetScaler**

当以透明模式部署 NetScaler 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 NetScaler 设备在 Citrix Virtual Apps and Desktops 环境中以透明模式部署，ICA 流量不会通过 VPN 传输。

将 NetScaler 添加到 NetScaler 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 NetScaler 设备上添加 NetScaler 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 NetScaler ADM 配置实用程序在透明模式下部署的 NetScaler 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。

下图显示了在透明模式下部署 NetScaler ADM NetScaler 时的网络部署情况：



要使用命令行界面在 **NetScaler** 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 NetScaler 设备侦听流量所用的 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 NetScaler 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 NetScaler 设备上配置的 AppFlow 收集器，请使用 **show appflow collector** 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：

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
>
> **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`

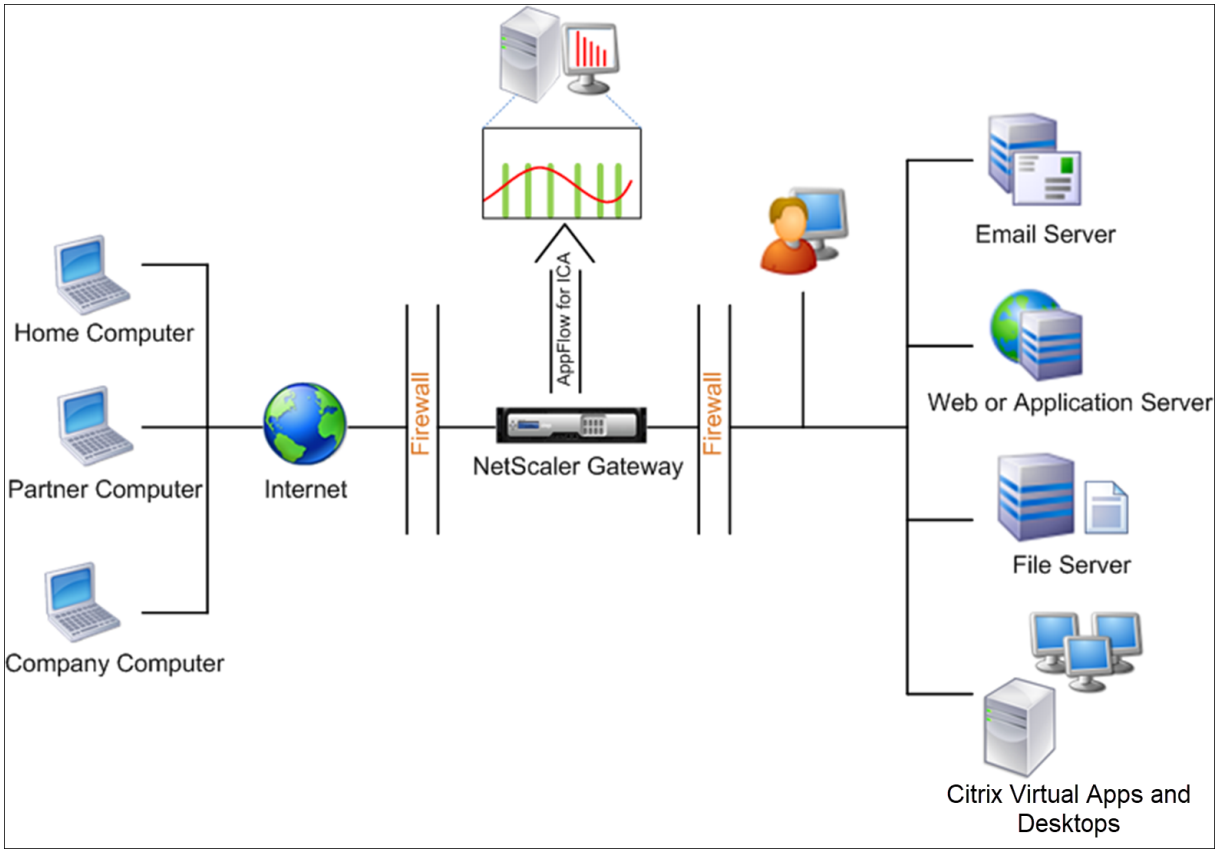
‘‘

为在单跃点模式下部署的 **NetScaler Gateway** 设备启用数据收集

February 6, 2024

在单跃点模式下部署 NetScaler Gateway 时，它位于网络的边缘。网关实例提供与桌面交付基础架构的代理 ICA 连接。单跃点是最简单、最常见的部署。如果外部用户尝试访问组织中的内部网络，单跃点模式可提供安全性。
在单跃点模式下，用户通过虚拟专用网络 (VPN) 访问 NetScaler 设备。

要开始收集报告，必须将 NetScaler Gateway 设备添加到 NetScaler Application Delivery Management (ADM) 清单中，然后在 ADM 上启用 AppFlow。



要从 **ADM** 启用 **AppFlow** 功能，请执行以下操作：

1. 导航到基础架构 > 实例，然后选择要启用分析的 NetScaler 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
>
> 在单跃点模式下启用 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 NetScaler 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 NetScaler 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 NetScaler

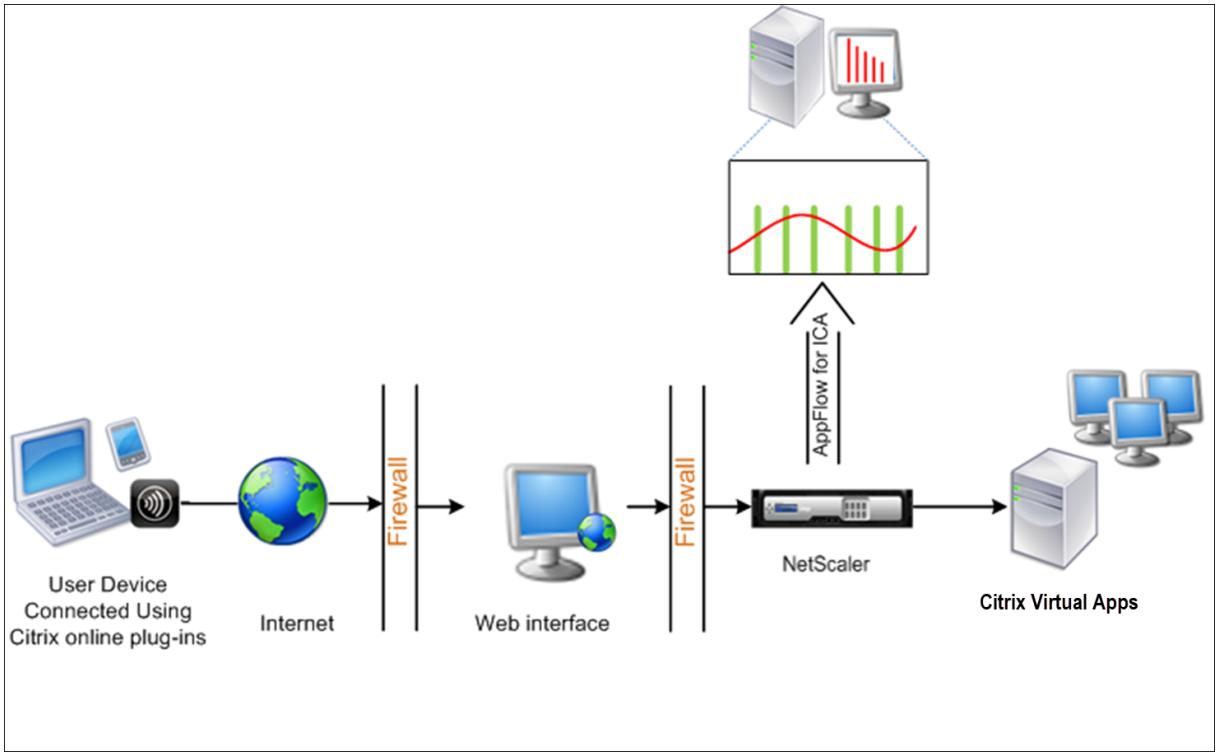
February 6, 2024

当以透明模式部署 NetScaler 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 NetScaler，则 ICA 流量不会通过 VPN 传输。

将 NetScaler 添加到 NetScaler 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 NetScaler 实例上将 NetScaler ADM 添加为 AppFlow 收集器，并且必须配置 AppFlow 策略来收集流经该设备的所有或特定 ICA 流量。

> 注意
>
> - 无法使用 NetScaler ADM 配置实用程序在透明模式下部署的 NetScaler 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。

下图显示了在透明模式下部署 NetScaler ADM NetScaler 时的网络部署情况：



要使用命令行界面在 **NetScaler** 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 NetScaler 设备侦听流量所用的 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 NetScaler 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 NetScaler 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。

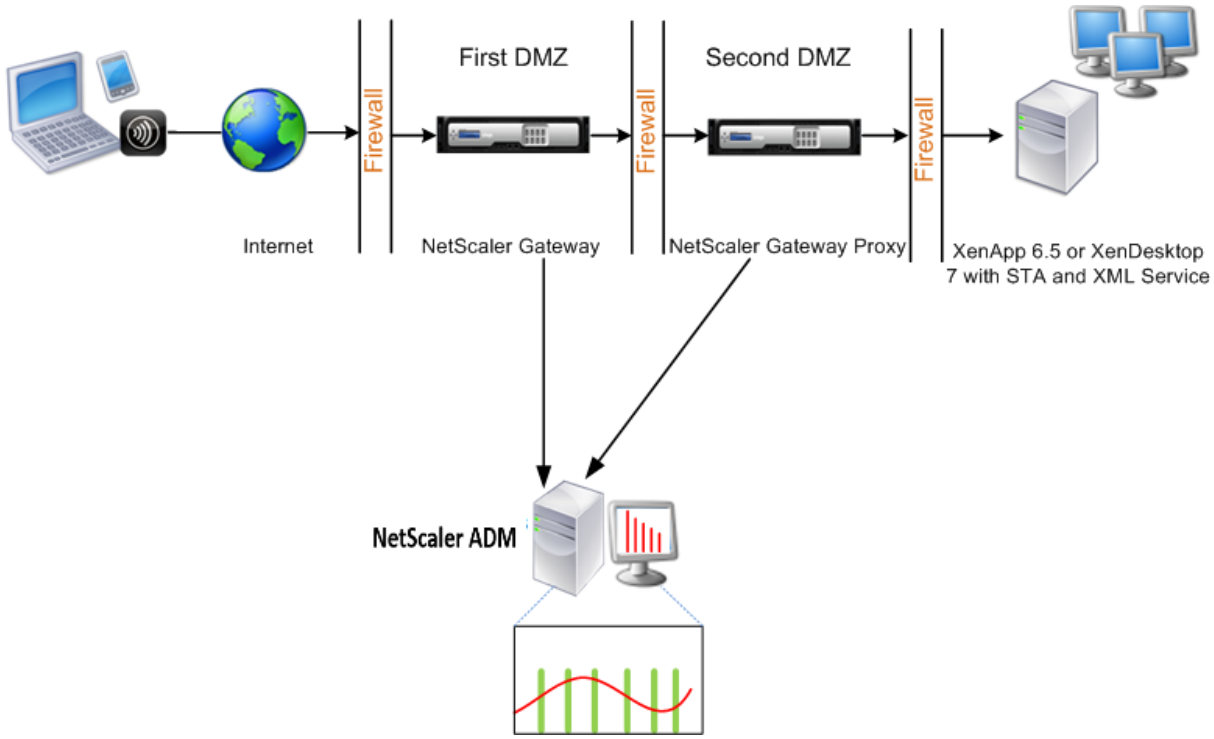
```
save ns config
<!--NeedCopy-->
```


为部署在双跃点模式下的 **NetScaler Gateway** 设备启用数据收集

February 6, 2024

NetScaler 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（NetScaler 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 NetScaler ADM，以便 NetScaler Gateway 装置报告这些生命统计数据。

图 3. NetScaler ADM 在双跃点模式下部署



第一个 DMZ 中的 NetScaler Gateway 处理用户连接并执行 SSL VPN 的安全功能。此 NetScaler Gateway 对用户连接进行加密，确定如何对用户进行身份验证，并控制对内部网络中服务器的访问。

第二个 DMZ 中的 NetScaler Gateway 充当 NetScaler Gateway 代理设备。此 NetScaler Gateway 使 ICA 流量能够遍历第二个 DMZ，从而完成用户与服务器场的连接。

NetScaler ADM 可以部署在属于第一个 DMZ 中 NetScaler Gateway 设备的子网中，也可以部署在属于 NetScaler Gateway 设备的第二个 DMZ 的子网中。在上图中，第一个 DMZ 中的 NetScaler ADM 和 NetScaler Gateway 部署在同一个子网中。

在双跃点模式下，NetScaler ADM 从一台装置收集 TCP 记录，从另一台装置收集 ICA 记录。将 NetScaler Gateway 设备添加到 NetScaler 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 NetScaler 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。跃点数表示流量从客户端流向服务器的 NetScaler Gateway 设备的数量。连接链 ID 表示客户端与服务器之间的端到端

连接。

NetScaler ADM 使用跳数和连接链 ID 来关联来自两个 NetScaler Gateway 设备的数据并生成报告。

要监视在此模式下部署的 NetScaler Gateway 装置，必须首先将 NetScaler Gateway 添加到 NetScaler ADM 清单中，启用 NetScaler ADM 上的 AppFlow，然后在 NetScaler ADM 控制板上查看报告。

在 **NetScaler ADM** 上启用数据收集

如果启用 NetScaler 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。要克服这种情况，必须在第一批 NetScaler Gateway 设备之一上启用适用于 TCP 的 AppFlow，然后在第二台设备上启用适用于 ICA 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 **NetScaler 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 NetScaler 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 NetScaler 设备上的服务或服务组启用 AppFlow 日志记录，NetScaler ADM 控制板不会显示记录，即使 Insight 列显示已启用。

5. 单击确定。

配置 **NetScaler Gateway** 设备以导出数据

安装 NetScaler Gateway 设备后，必须在 NetScaler Gateway 设备上配置以下设置，以便将报告导出到 NetScaler ADM：

- 在第一个和第二个 DMZ 中配置 NetScaler Gateway 设备的虚拟服务器以相互通信。
- 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。
- 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。
- 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。
- 允许其中一个 NetScaler Gateway 设备导出 ICA 记录
- 允许其他 NetScaler Gateway 设备导出 TCP 记录：

- 在两个 NetScaler Gateway 设备上启用连接链接。

使用命令行界面配置 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 虚拟服务器配置为与第二个 DMZ 中的 NetScaler Gateway 虚拟服务器进行通信。

---

add vpn nextHopServer [**-secure**(ON OFF)] [**-imgGifToPng**] …

```
add vpn nextHopServer nh1 10.102.2.33 8443 -secure ON
<!--NeedCopy-->
```

2. 将第二个 DMZ 中的 NetScaler Gateway 虚拟服务器绑定到第一个 DMZ 中的 NetScaler Gateway 虚拟服务器。在第一个 DMZ 中的 NetScaler Gateway 上运行以下命令：

   bind vpn vserver <name> **-nextHopServer** <name>

```
bind vpn vserver vs1 -nextHopServer nh1
<!--NeedCopy-->
```

3. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点和 AppFlow。

---

set vpn DISABLED)] [**- appflowLog** (DISABLED)]
vserver [**- doubleHop** (ENABLED
ENABLED

```
set vpn vserver vpnhop2 -doubleHop ENABLED -appFlowLog ENABLED
<!--NeedCopy-->
```

4. 在第二个 DMZ 中的 NetScaler Gateway 虚拟服务器上禁用身份验证。

---

set vpn vserver [**-authentication** (ON OFF)]

```
set vpn vserver vs -authentication OFF
<!--NeedCopy-->
```

5. 启用其中一个 NetScaler 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 NetScaler 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 NetScaler Gateway 设备上启用连接链接：

set appFlow DISABLED)]
param [**-connectionChaining** (ENABLED

```
set appflow param -connectionChaining ENABLED
<!--NeedCopy-->
```

使用配置实用程序配置 **NetScaler Gateway**：

1. 将第一个 DMZ 中的 NetScaler Gateway 配置为与第二个 DMZ 中的 NetScaler Gateway 进行通信，并将第二个 DMZ 中的 NetScaler Gateway 绑定到第一个 DMZ 中的 NetScaler Gateway。
   a) 在“配置”选项卡上，展开 **NetScaler 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) 单击下一个跃点服务器并将下一个跃点服务器绑定到第二台 NetScaler Gateway 设备。
2. 在第二个 DMZ 中的 NetScaler Gateway 上启用双跃点。
   a) 在“配置”选项卡上，展开 **NetScaler 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 中的 NetScaler Gateway 上禁用虚拟服务器上的身份验证。
   a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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 NetScaler Gateway 设备以导出 TCP 记录。
   a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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 NetScaler Gateway 设备以导出 ICA 记录：

a) 在 **Configuration**（配置）选项卡上，展开 **NetScaler Gateway**，并单击 **Virtual Servers**（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 NetScaler Gateway 设备上启用连接链接。

a) 在“配置”选项卡上，导航到“设置”**>** “**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）。

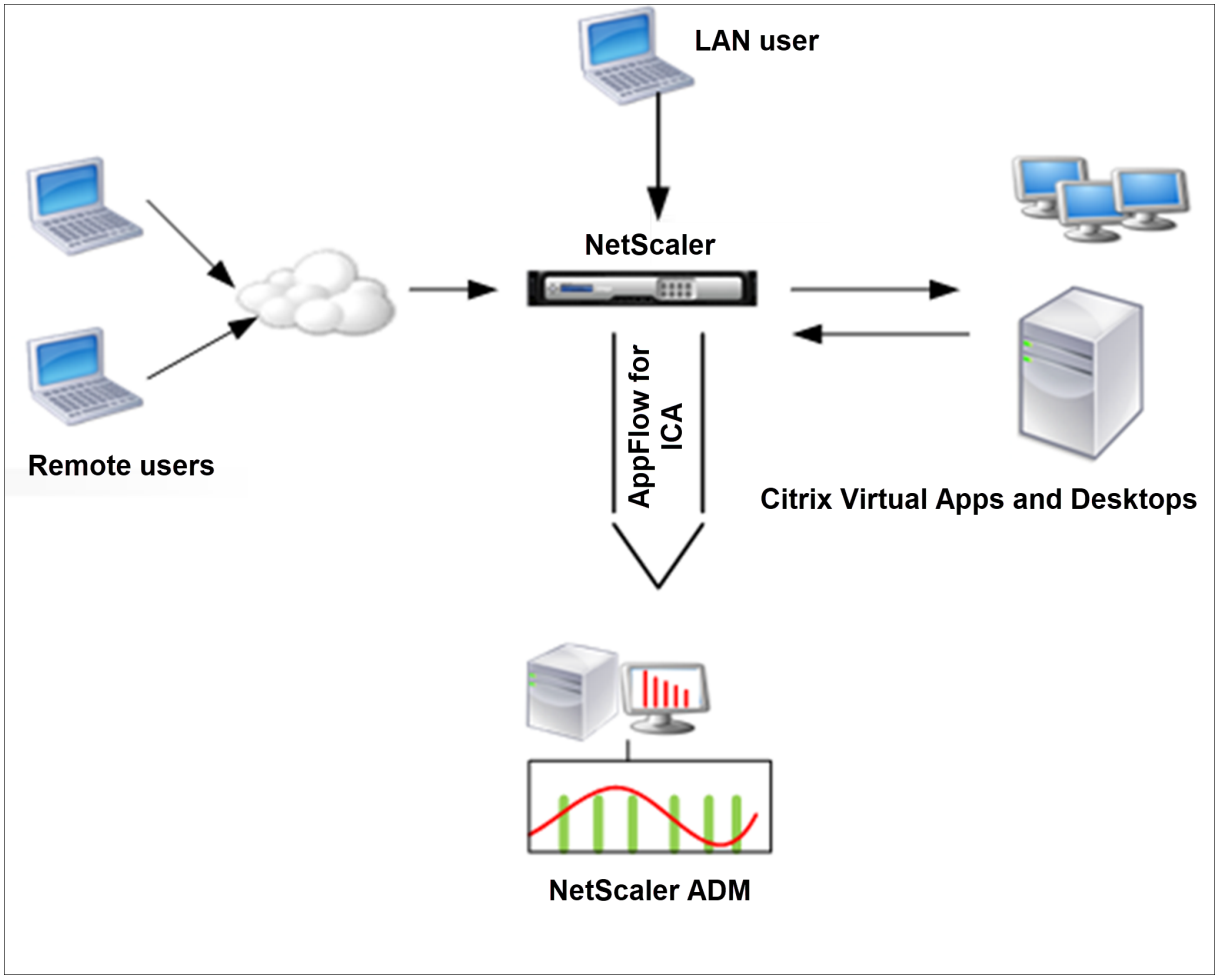
启用数据收集以监视在局域网用户模式下部署的 **NetScaler**

February 6, 2024

访问 Citrix 虚拟应用程序或桌面应用程序的外部用户必须在 NetScaler Gateway 上进行身份验证。但是，内部用户可能不需要重定向到 NetScaler Gateway。此外，在透明模式部署中，管理员必须手动应用路由策略，以便请求重定向至 NetScaler 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 NetScaler Gateway 设备上的 SOCTS 代理）以 LAN 用户模式部署 NetScaler 设备。

图 4. 在局域网用户模式下部署的 NetScaler ADM



注意： NetScaler ADM 和 NetScaler Gateway 设备位于同一子网中。

要监视在此模式下部署的 NetScaler 设备，请先将 NetScaler 设备添加到 NetScaler Insight 清单，启用 AppFlow，然后在控制板上查看报告。

将 NetScaler 装置添加到 NetScaler ADM 清单后，必须为数据收集启用 AppFlow。

> 注意
>
> - 无法使用 NetScaler ADM 配置实用程序在局域网用户模式下部署的 NetScaler 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 **NetScaler** 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 NetScaler 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 NetScaler ADM 添加为 NetScaler 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_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-->
```

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

February 6, 2024

NetScaler Application Delivery Management (ADM) 上的 HDX Insight 允许您监视通过 NetScaler 实例的 HDX 流量。NetScaler 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 NetScaler 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。

NetScaler ADM 中的 HDX Insight 阈值管理允许您在突破设置的阈值时主动创建规则和配置警报。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。阈值规则组由从用户、应用程序和桌面等实体中选择的指标的一个或多个用户定义的阈值规则组成。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 NetScaler ADM 上生成警报。例如，您可以根据会话启动总数监视应用程序，也可以将应用程序启动计数作为一个阈值组进行监视。只有在违反两条规则时才会生成警报。这允许您在实体上设置更真实的阈值。

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，然后选择会话启动总计数或应用程序启动计数。您可以为实体和指标的每种组合创建一条规则。使用提供的比较器（>、<、>= 和 <=），键入每个指标的阈值。

> 注意
>
> 如果您不想监视单个组中的多个实体，则必须为每个实体创建一个单独的阈值规则组。

当计数器的值超过阈值时，NetScaler ADM 会生成一个事件以表示违反阈值，并为每个事件创建警报。

您必须配置接收警报的方式。您可以允许在 NetScaler ADM 上显示警报和/或在移动设备上以电子邮件或 SMS 的形式接收警报。对于最后两个操作，您必须在 NetScaler 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特定地理监视。

示例用例

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 NetScaler Gateway 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，数据中心附近位置的 ICA RTT 可能为 5-10 毫秒，而远程位置的 ICA RTT 可能在 100 毫秒左右。

借助 HDX Insight 的阈值规则组管理，Eric 可以为每个位置设置特定地理位置的阈值规则组，并通过电子邮件或短信收到每个区域的违规警报。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 **NetScaler 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 NetScaler ADM 中，导航到“设置”**>**“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：

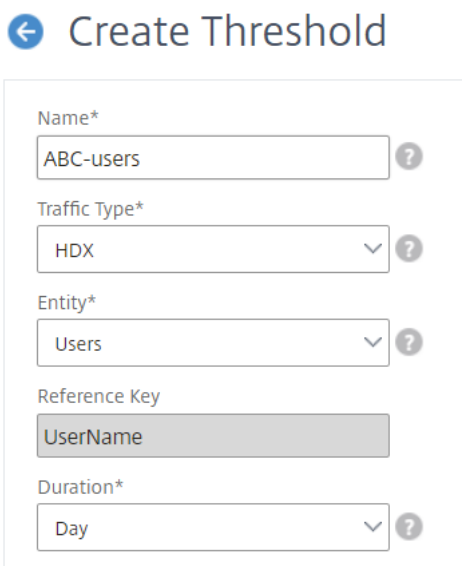
   a) 名称。键入用于创建 NetScaler ADM 生成警报的事件的名称。

   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。

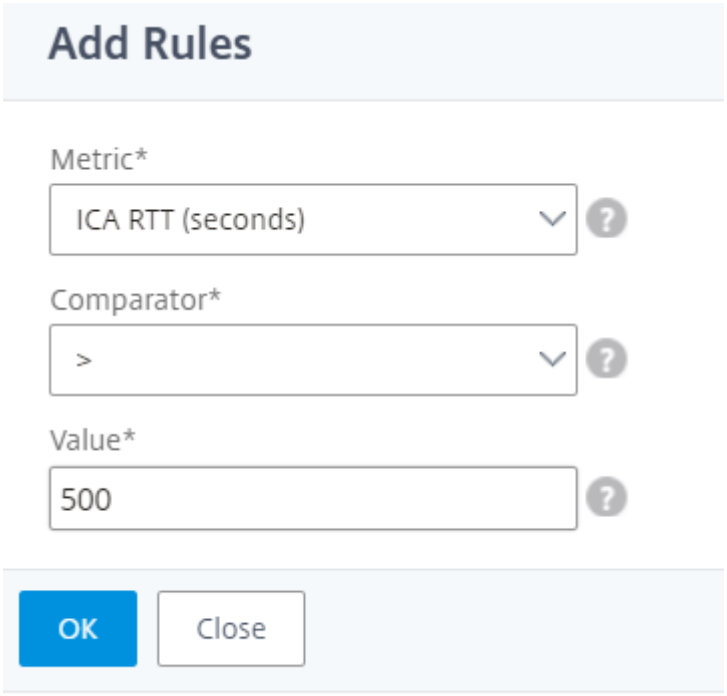
   d) 参考键。参考密钥是根据您选择的流量类型和实体自动生成的。

   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。

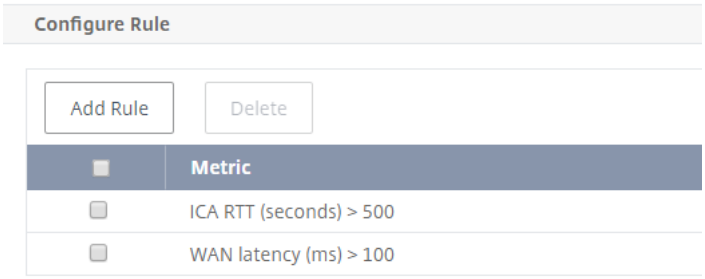


3. 为所有实体创建阈值规则组：

   对于 HDX 流量，必须通过单击“添加规则”来创建规则。在打开的“添加规则”弹出窗口中输入值。

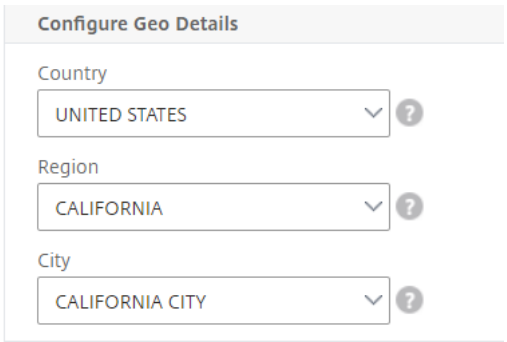


您可以创建多个规则来监视每个实体。在一个组中创建多个规则允许您将实体作为一组阈值规则而不是单个规则进行监视。单击确定关闭窗口。



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”部分中为用户实体创建基于位置的警报。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 NetScaler 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

February 6, 2024

HDX Insight 提供与 NetScaler 实例上的 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：

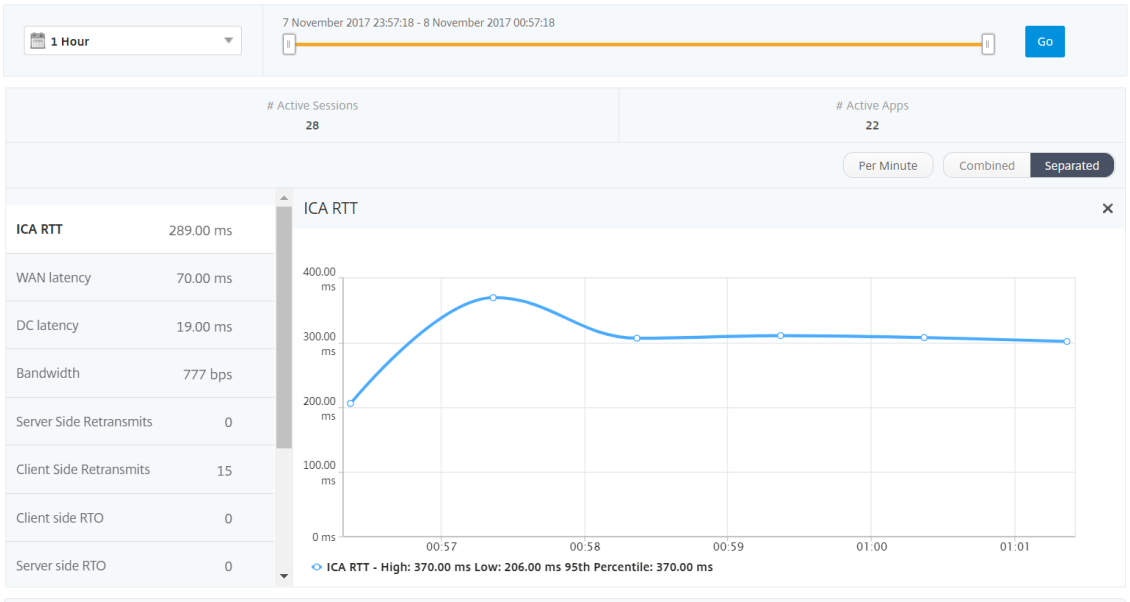
- 用户：显示在选定时间间隔内访问 Citrix 虚拟应用程序或桌面的所有用户的报告。
- 应用程序：显示应用程序总数的报告以及所有相关信息，例如在指定时间间隔内启动应用程序的总次数。
- 实例：显示用作传入流量网关的 NetScaler 实例的报告。
- 桌面：显示在选定时间范围内使用的桌面的报告。
- 许可证：显示指定时段内使用的 SSL VPN 许可证总数的报告。

“**User**”（用户）视图报告和指标

此视图中的报告和衡量指标按照 Citrix Virtual Apps and Desktops 用户显示。

要导航到用户视图，请执行以下操作：

1. 导航到网关 **> 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/报告都将显示选定时段内与其对应的值。

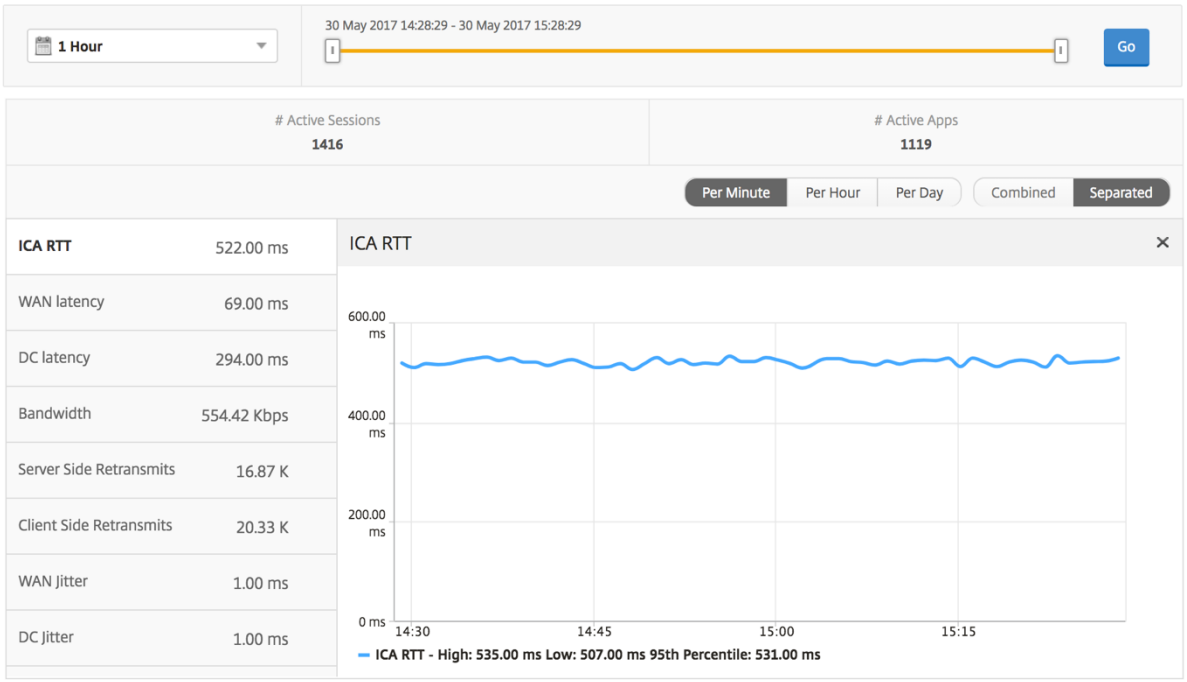
要更改选定时间段，请执行以下操作：

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
Active Sessions（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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接发生重新传输超时的次数。

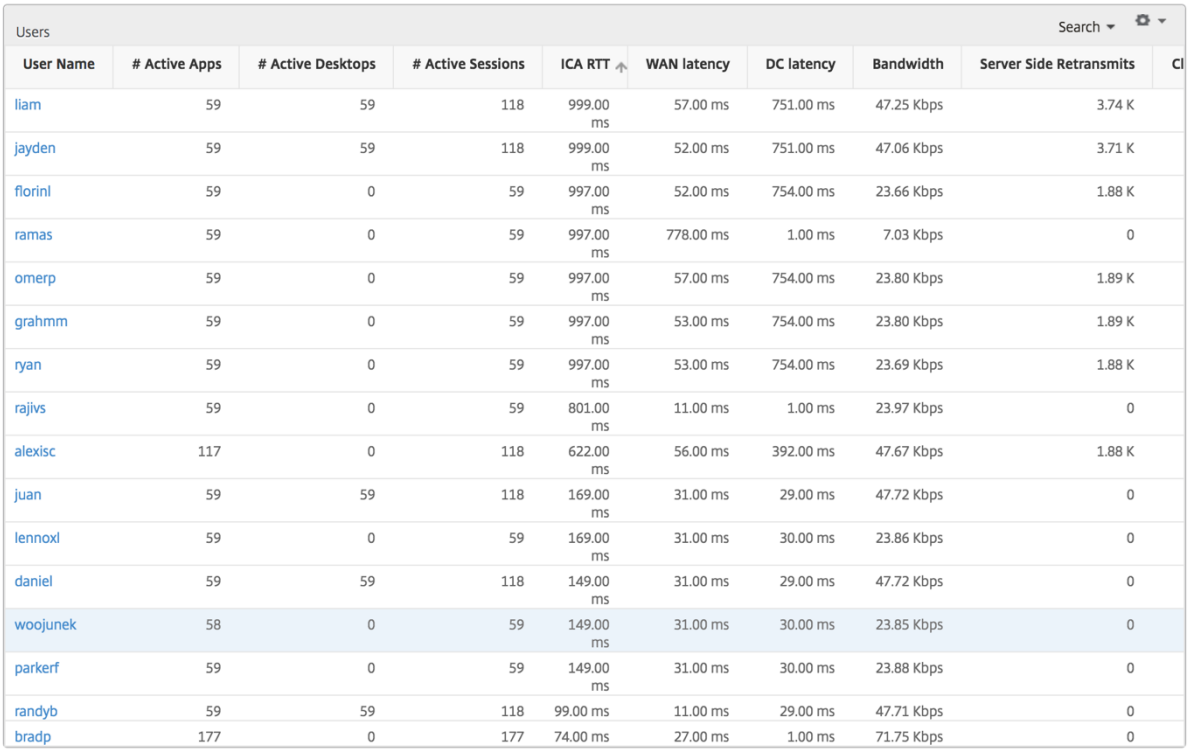
指标	说明
Client side Zero Window size event（客户端零窗口大小事件）	此计数器指示客户端播发零 TCP 窗口的次数。
Server side Zero Window size event（服务器端零窗口大小事件）	此计数器指示服务器播发零 TCP 窗口的次数。



用户摘要报告　下面是与此报告特定相关的指标。

指标	说明
Active Sessions（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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。

指标	说明
Server Side Retransmits（服务器端重新传输数）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

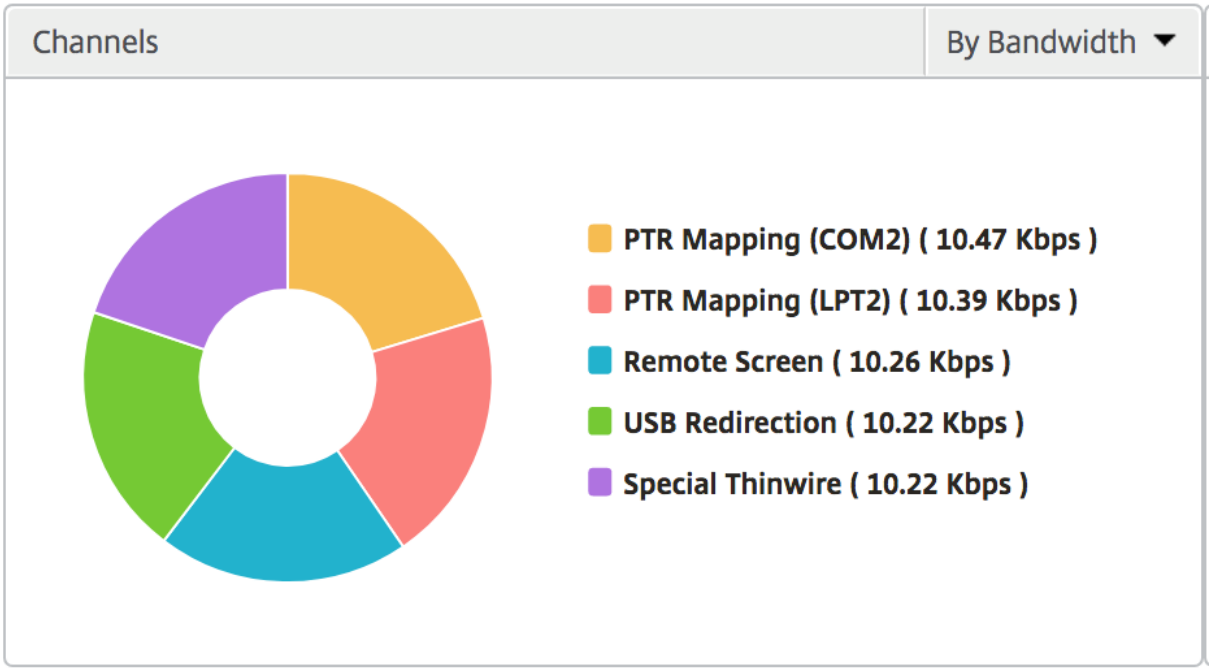


Users

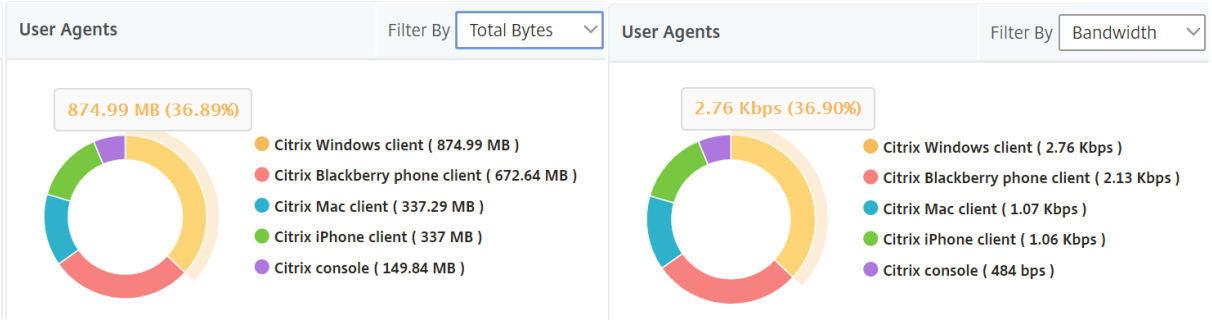
Search

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	

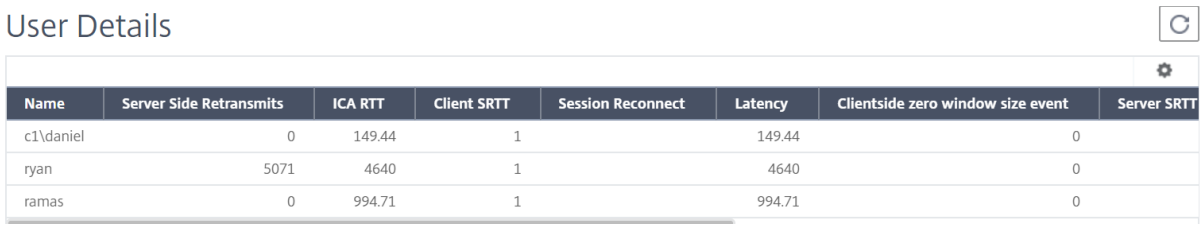
Channels（通道） “Channels”（通道）以环形图的形式表示每个 ICA 虚拟通道占用的总带宽或总字节数。您还可以按带宽或总字节数对指标排序。



用户代理　用户代理以圆环图的形式表示每个 Workspace 客户端消耗的总带宽/总字节数。图表中的每个彩色段代表一个 Workspace 客户端。分段的长度取决于在该工作区客户端上启动应用程序的用户数量。您还可以按带宽或总字节对指标进行排序。



单击每个区段可查看使用该 Workspace 客户端的用户的详细信息。



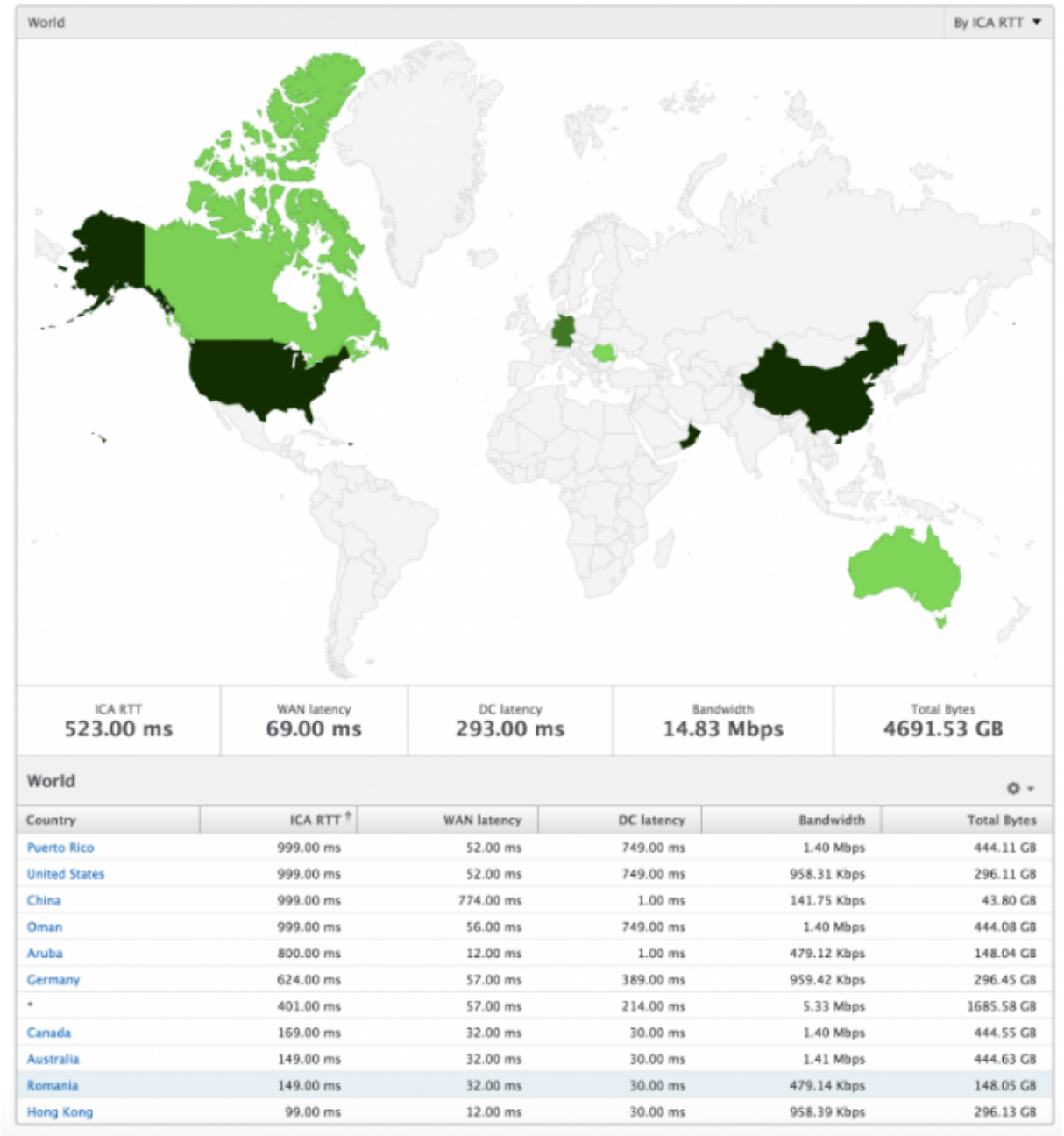
Name	Server Side Retransmits	ICA RTT	Client SRTT	Session Reconnect	Latency	Clientside zero window size event	Server SRTT
c1\daniel	0	149.44	1		149.44	0	
ryan	5071	4640	1		4640	0	
ramas	0	994.71	1		994.71	0	

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 NetScaler 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 Insight 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 NetScaler ADM。
2. 导航到网关 **> 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/已终止会话报告　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。

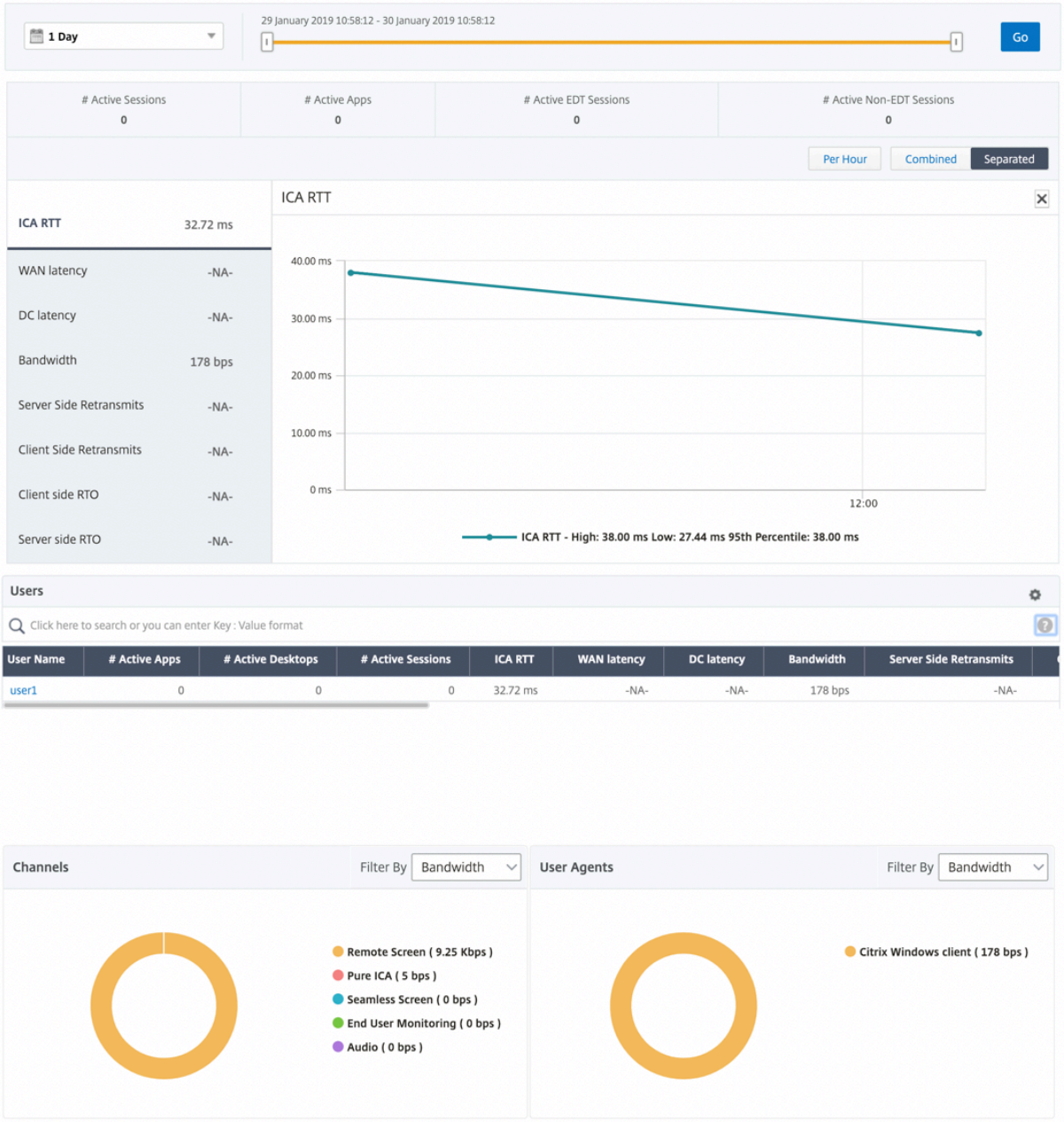
指标	说明
会话 ID	ICA 会话的唯一标识。
会话类型	应用程序/桌面。
状态	绿色/红色分别表示活动/非活动会话。
主机延迟	服务器网络造成的 ICA 流量通过 NetScalers 的平均延迟。
Bandwidth per Interval（每个间隔内的带宽）	在特定时间间隔内会话占用的带宽。
Session Bandwidth（会话带宽）	会话占用的带宽，与时间间隔无关。
Bytes per Interval（每个间隔内的字节数）	在特定时间间隔内会话占用的字节数。
Start Time（开始时间）	会话开始时间。
Up Time（运行时间）	会话持续时间。
客户端 IP 地址	最终用户 IP。
服务器 IP 地址	后端/Citrix Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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，NetScaler 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 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 和后端服务器之间的连接发生重新传输超时的次数。

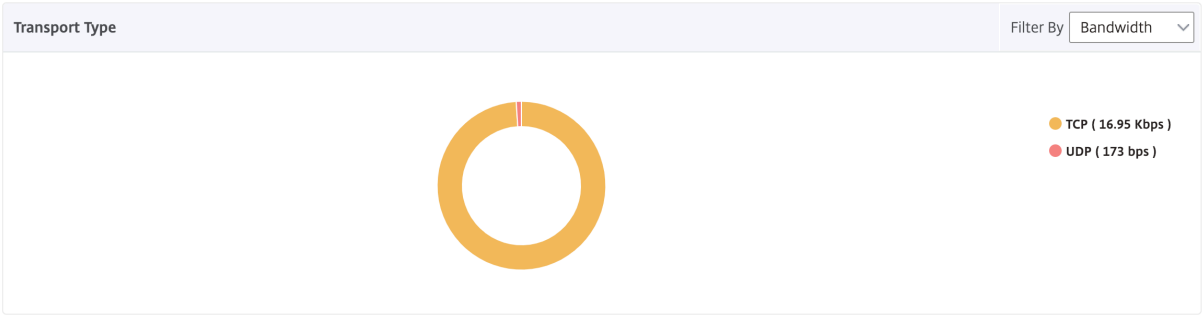
支持 **HDX Insight** 中的 **EDT**

NetScaler Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示 HDX Insight 的分析结果。也就是说, ADM 现在同时支持 UDP 和 TCP 协议。对 NetScaler Gateway 的 EDT 支持确保运行 Citrix Workspace 的用户在会话中获得虚拟桌面的高清晰度用户体验

HDX Insight 现在在活动会话报告中显示 EDT 会话和非 EDT 会话的数量。“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”。



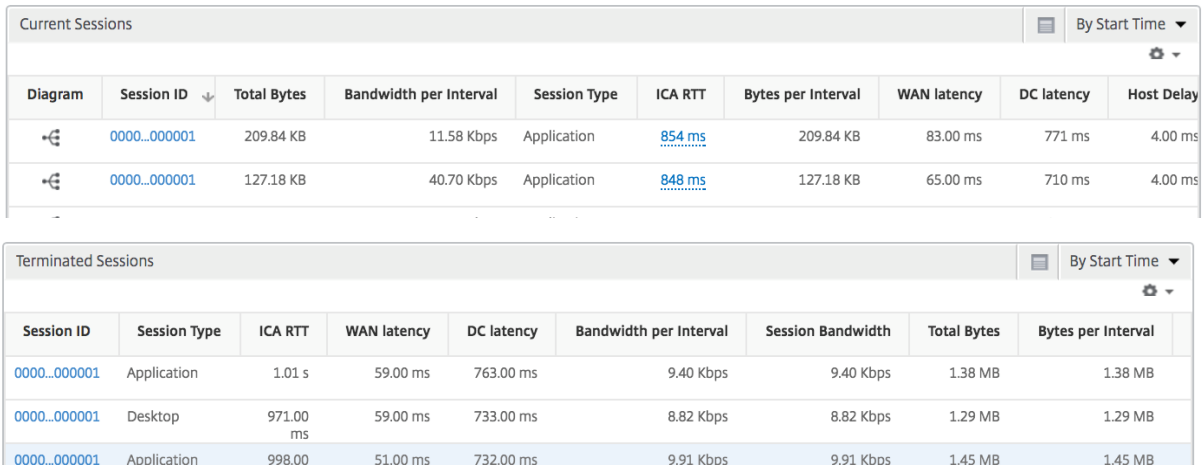
引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。



> 注意：从版本 12.1 版本 50.28 开始的 NetScaler 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。

NetScaler ADM 12.0 及更高版本中提供的 **HDX Insight** 分析指标：

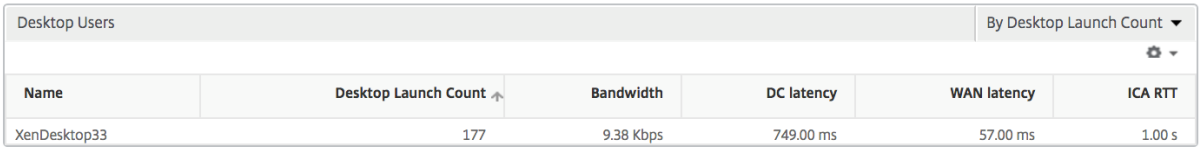
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 NetScaler 实例之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
L7 Server-side Latency（L7 服务器端延迟）	NetScaler 设备与 Citrix 虚拟应用程序之间观察到的平均 L7 延迟。如果交付路径中存在非 Citrix 设备，此衡量指标非常有用。
Maximum Breach Latency（最大违反延迟）	在设置的时间间隔内违反定义的阈值时，L7 延迟的最高值。
Average Breach Latency（平均违反延迟）	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。



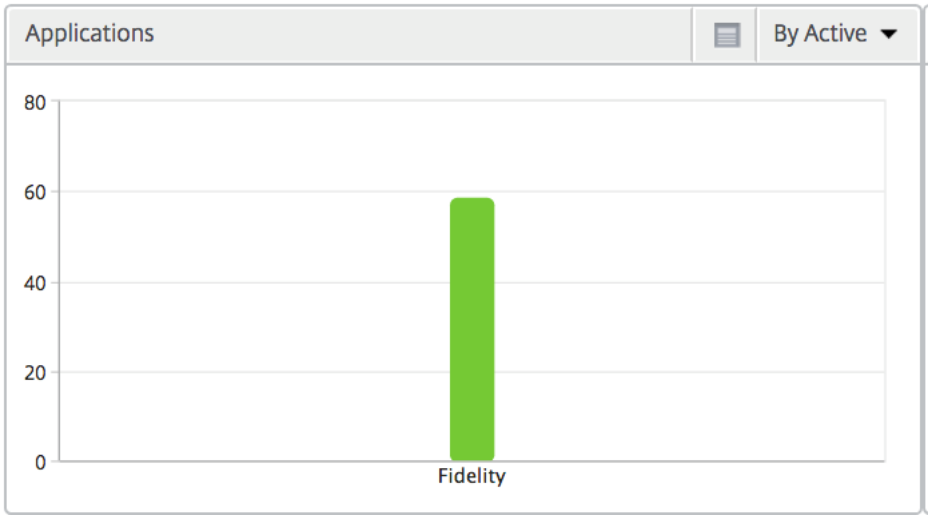
桌面用户　此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	NetScaler Gateway 和 VDI、CVAD 或 StoreFront 服务器之间的网络服务器端造成的延迟。

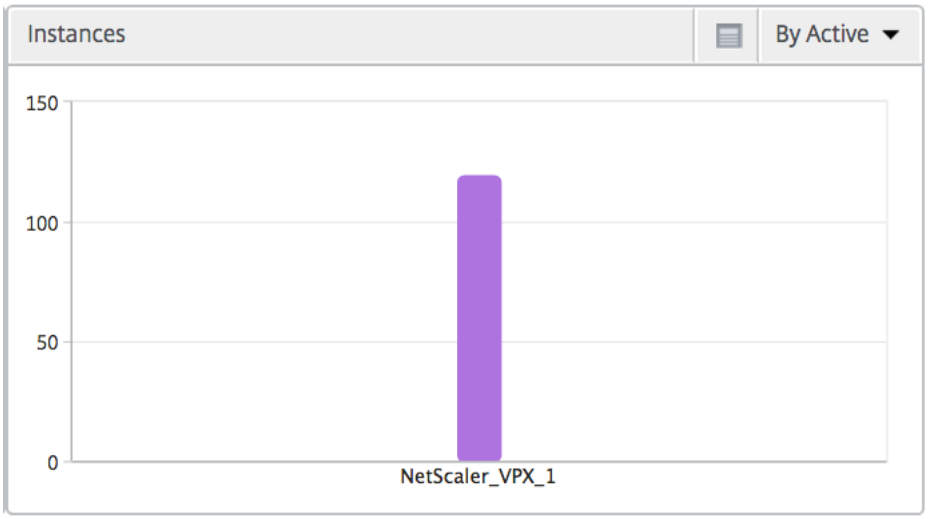
指标	说明
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序或桌面上托管的应用程序或桌面进行交互时遇到的屏幕滞后。



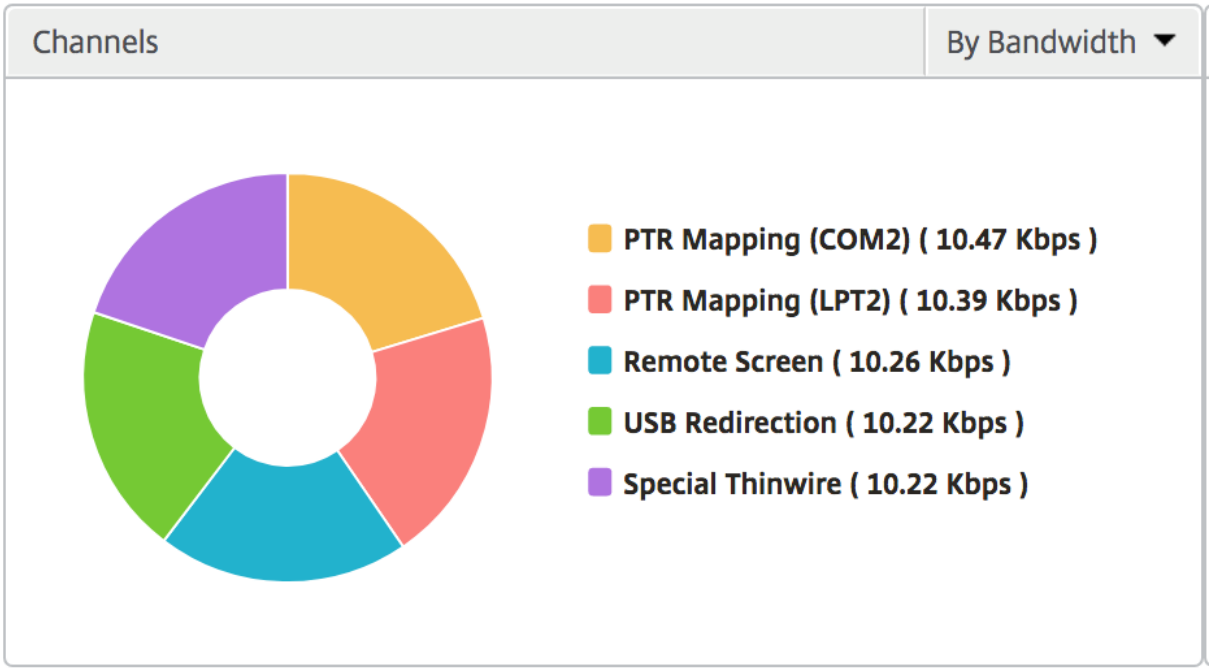
应用程序　一个条形图，表示按活动状态、总会话启动次数、总应用程序启动次数和启动持续时间排序的应用程序。



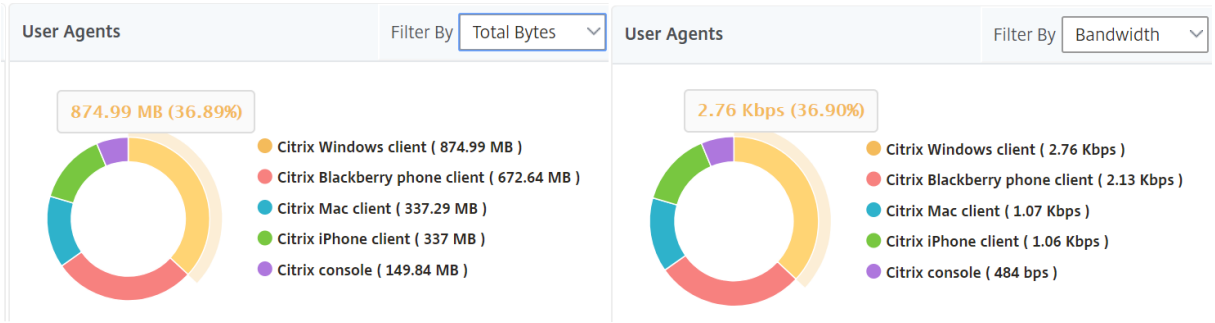
实例　表示按活动应用程序和总应用程序排序的 NetScaler 实例的条形图



Channels（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。

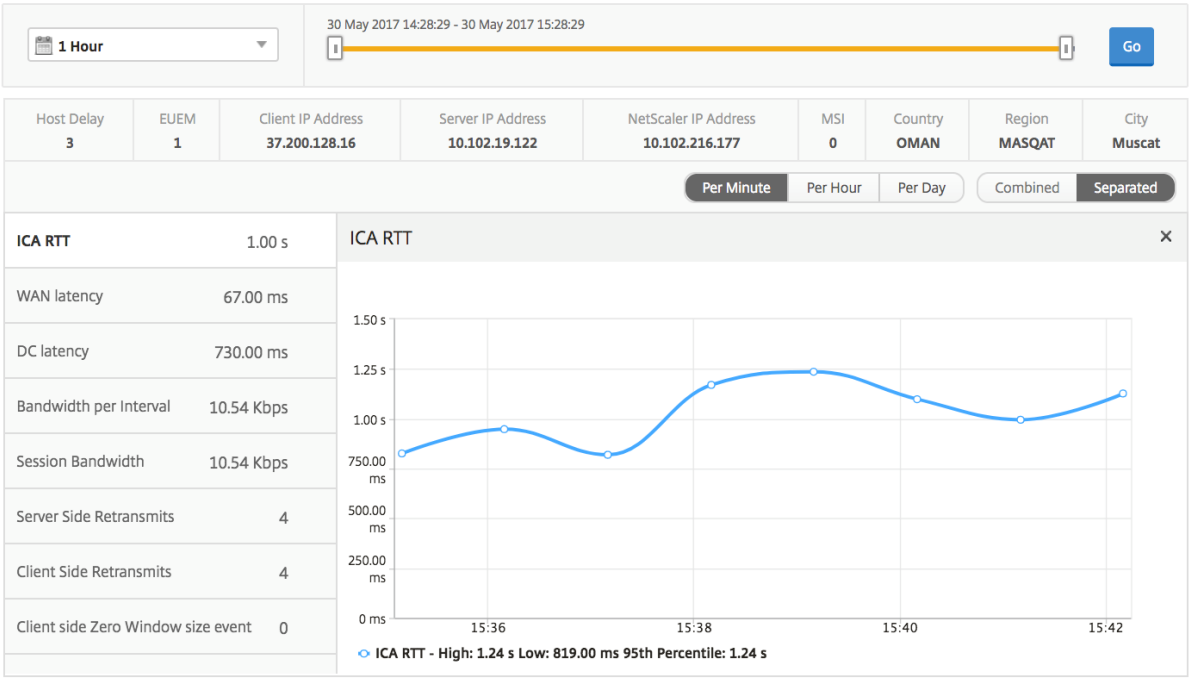
要查看选定用户会话的度量，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或已终止的会话列中选择一个会话。

时间线图

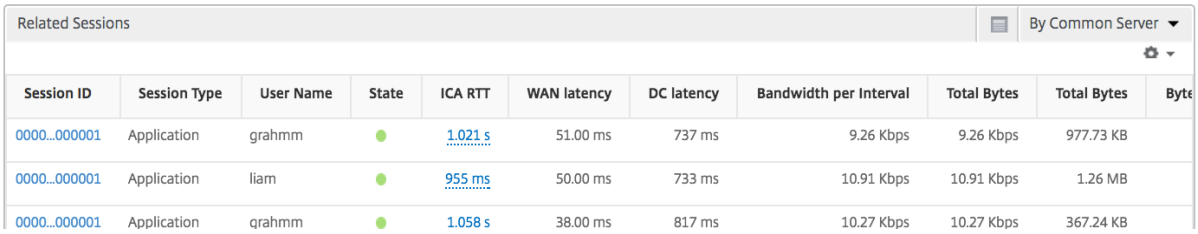
指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix Virtual Apps 或 Citrix Virtual Desktops 上托管的应用程序或桌面进行交互时遇到的屏幕延迟。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	NetScaler Gateway 和 VDI、CVAD 或 StoreFront 服务器之间的网络服务器端造成的延迟。
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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

相关会话　“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 NetScaler。



“**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。

要导航到“应用程序”视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 应用程序。

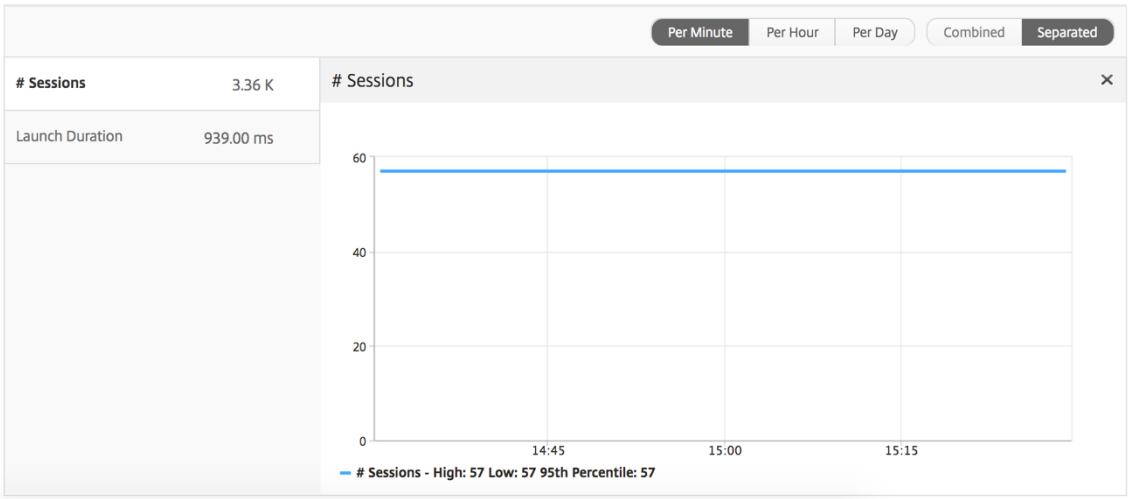
Summary View（摘要视图）

“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。

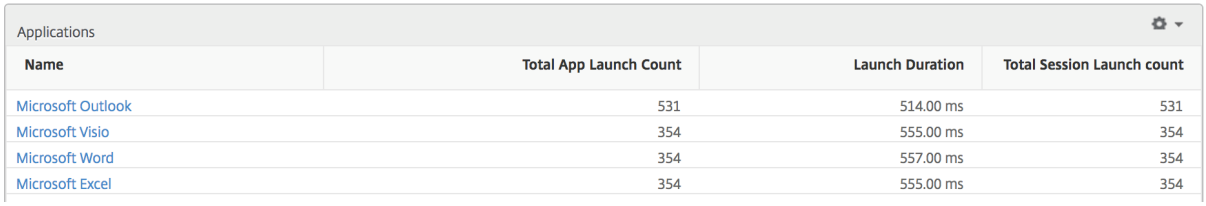
折线图

指标	说明
Sessions（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

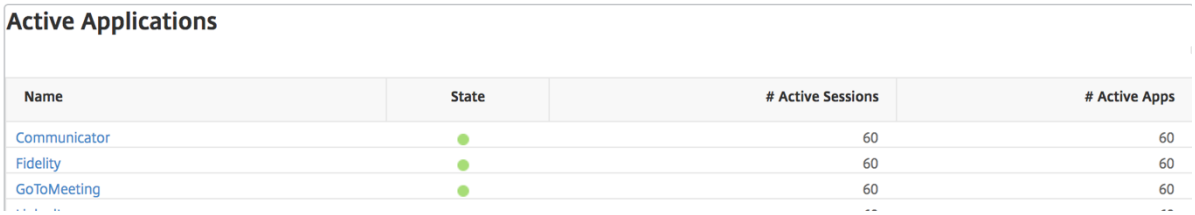
指标	说明
名称	Citrix Virtual Apps 的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix Virtual Apps 应用程序总数。
Launch Duration（启动持续时间）	启动 Citrix 虚拟应用程序所需的平均时间。



活动应用程序报告

指标	说明
名称	Citrix Virtual Apps 的名称。
状态	显示应用程序的状态：绿色 - 活动、红色 - 不活动
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。

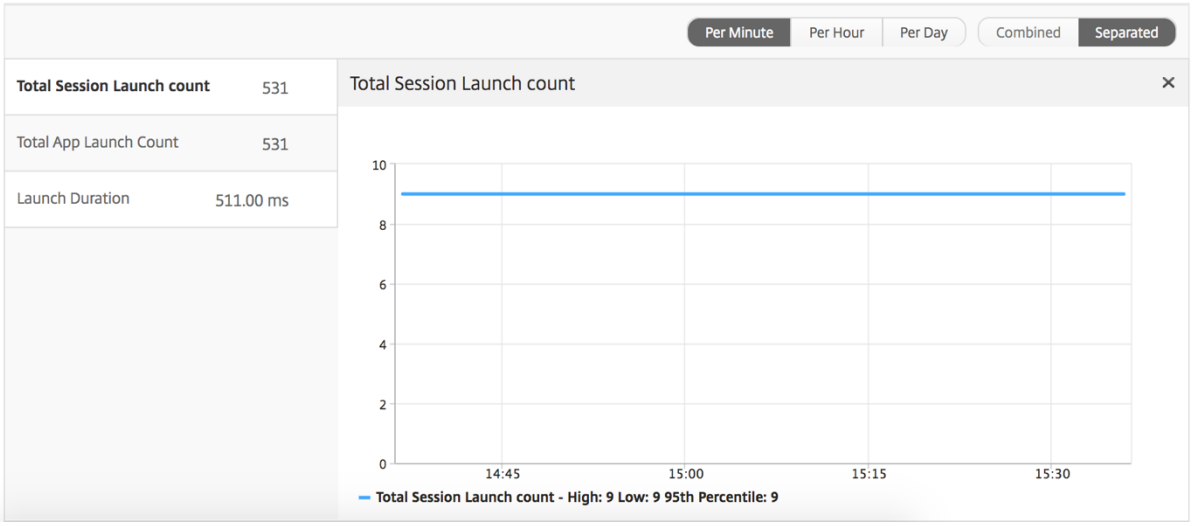
指标	说明
Active Apps（活动应用程序数）	此应用程序的活动会话数。



阈值报告　阈值报告表示在选定时间段内将 实体 选为应用程序时突破的阈值计数。有关详细信息，请参阅 如何创建阈值。

折线图

指标	说明
Active Sessions（活动会话数）	此数字表示活动 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。

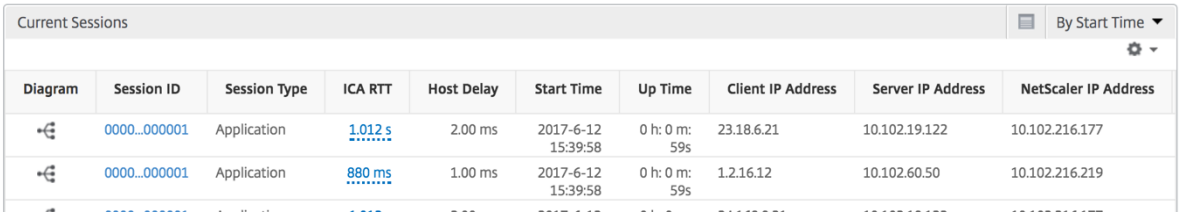


当前会话报告

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	服务器网络造成的 ICA 流量通过 NetScalers 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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，NetScaler 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。

指标	说明
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 Virtual Apps 或 Citrix Virtual Desktops 上托管的应用程序或桌面进行交互时遇到的屏幕延迟。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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 Virtual Apps 的用户的用户名。
会话 ID	Citrix Virtual Apps 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，红色表示不活动。
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。
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 NetScaler 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。

指标	说明
L7 Server-side Latency（L7 服务器端延迟）	NetScaler 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。

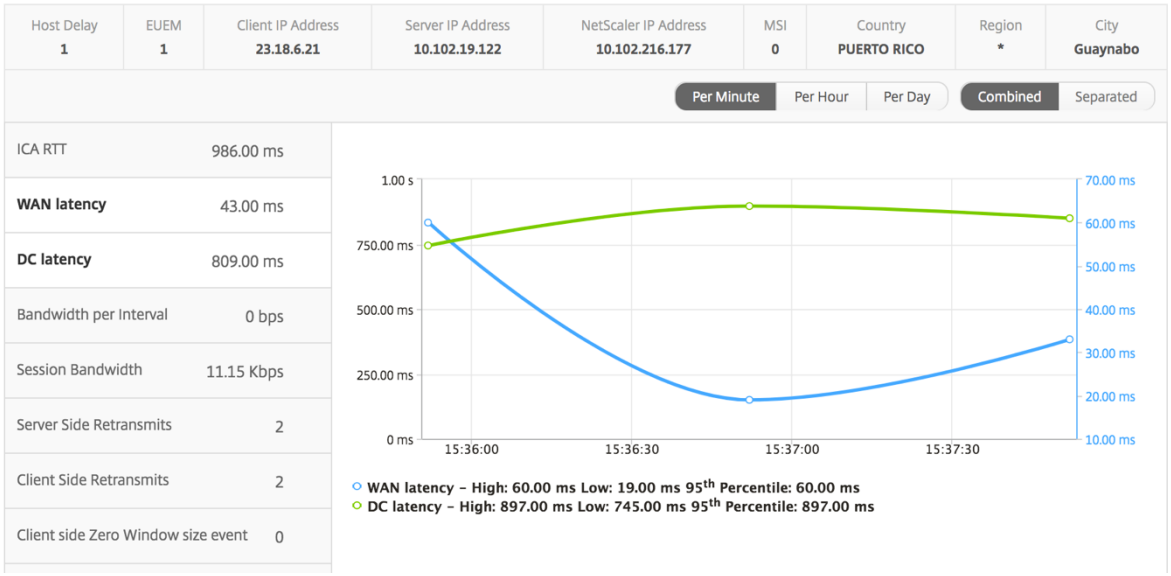
要查看会话报告，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 NetScaler ADM。
2. 导航到网关 **> 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。

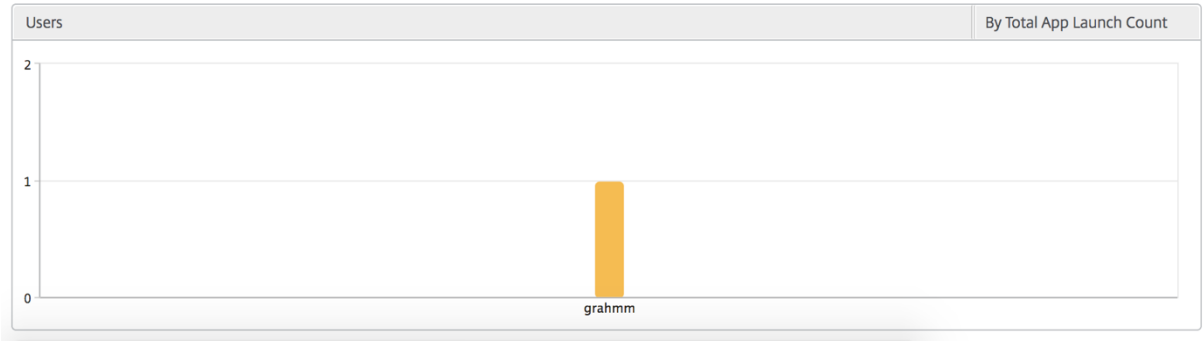
折线图

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 NetScaler 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 NetScaler 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。

指标	说明
Server Side Retransmits（服务器端重新传输数）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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集中在 Citrix Virtual Desktops 上。

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 NetScaler ADM。
2. 导航到网关 **> HDX Insight >** 桌面。

Summary View（摘要视图）

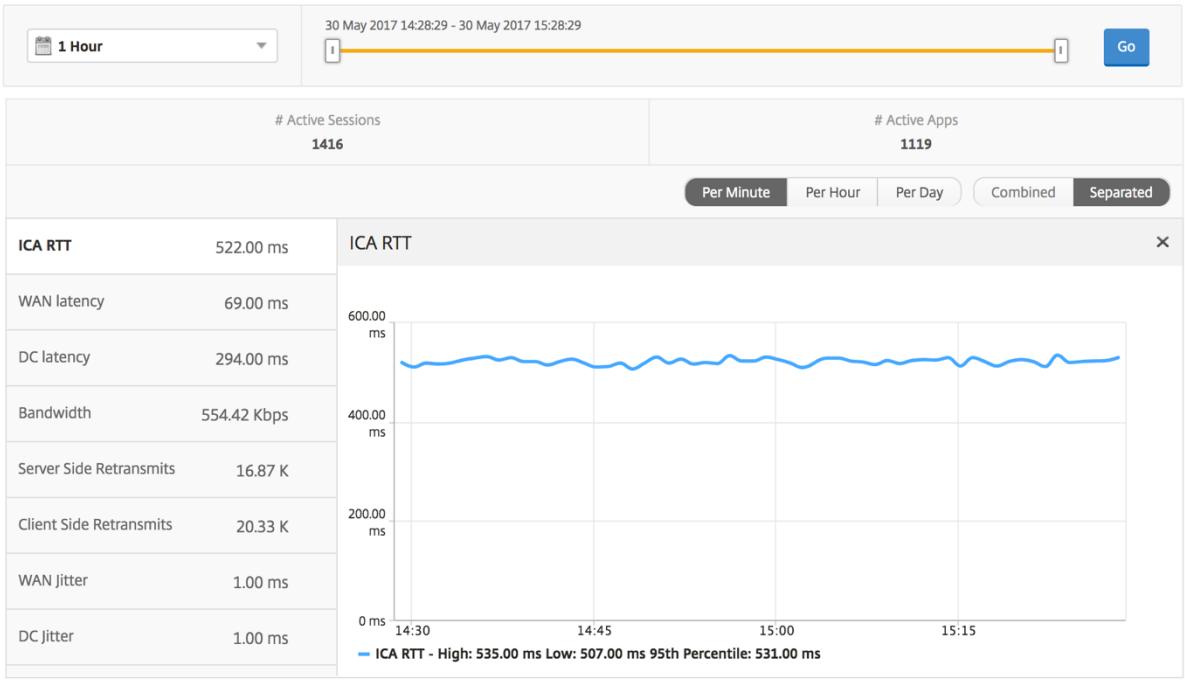
摘要视图显示在选定时间轴内登录的所有 Citrix Virtual Desktops 的报告。

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
Active Sessions（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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。

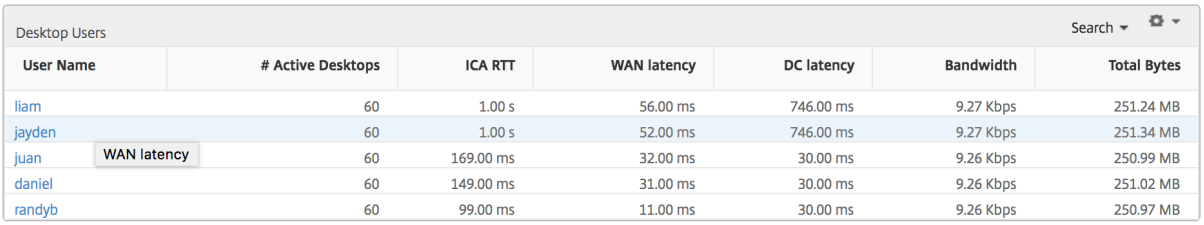
指标	说明
Server Side Retransmits（服务器端重新传输数）	NetScaler 和后端服务器之间的连接上重新传输的数据包数。
Client Side Retransmits（客户端重新传输数）	NetScaler 与最终用户之间的连接上重新传输的数据包数。此指标值较高并不意味着用户体验将是无缝的，而是指示由于重新传输，带宽利用率较高。
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 和后端服务器之间的连接发生重新传输超时的次数。
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	在给定时间间隔内活动 Citrix Virtual Desktops 会话的总数。
Active Desktops（活动桌面数）	指定时间间隔内活动的 Citrix Virtual Desktops 总数。

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。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
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。

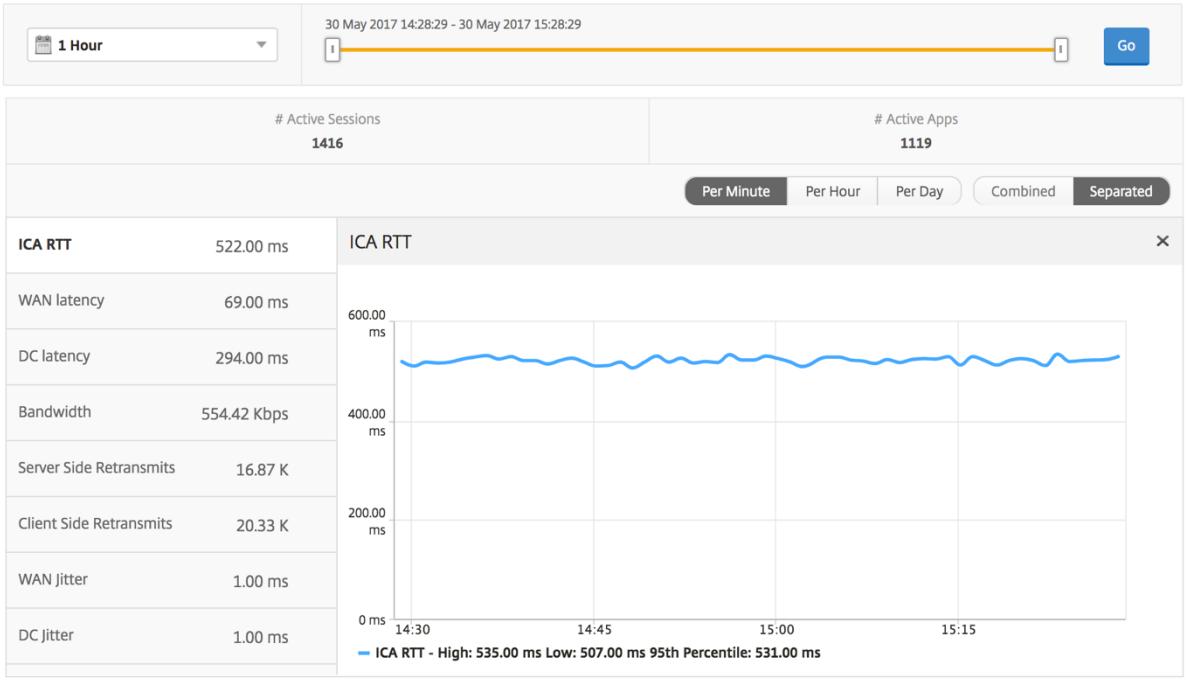
要导航到特定的桌面视图，请执行以下操作：

1. 使用支持的 Web 浏览器登录到您的 NetScaler 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

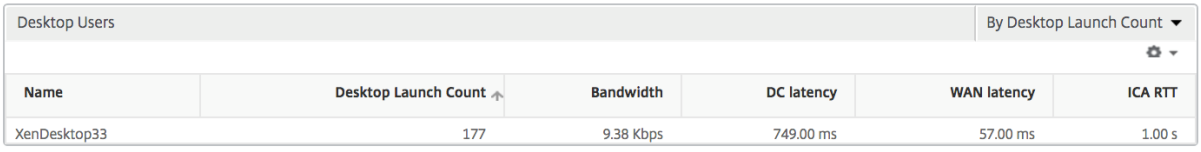
指标	说明
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual Apps and Desktops 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 会话的计数。

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。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
Server Side Retransmits（服务器端重新传输数）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

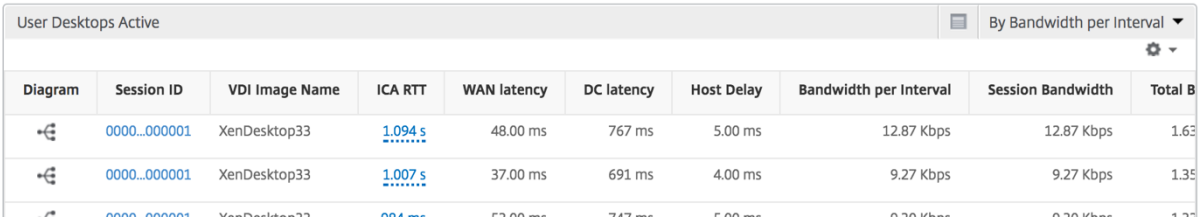
指标	说明
名称	Citrix Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
ICA RTT	ICA RTT 是用户在与分别托管在 Citrix Virtual Apps and Desktops 上的应用程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	服务器网络造成的 ICA 流量通过 NetScalers 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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，NetScaler 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。

指标	说明
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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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 NetScaler 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。

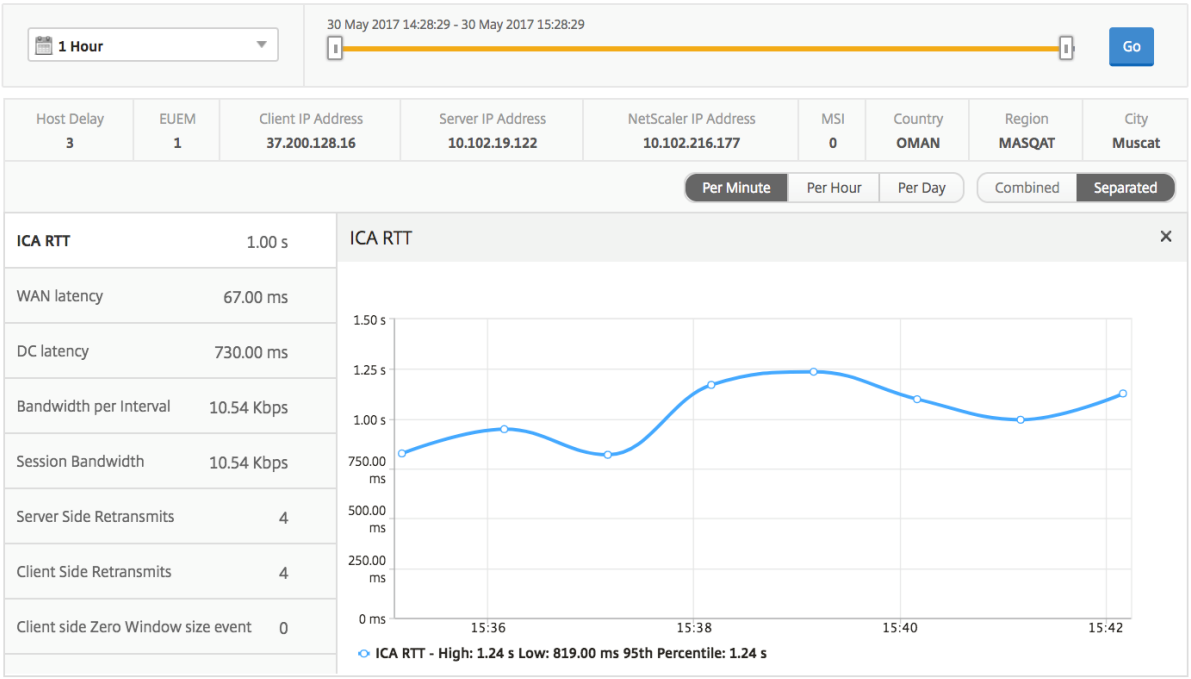
时间线图 “Per User Session View”（每个用户会话视图）提供特定的选定用户的会话的报告。

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 NetScaler ADM。
2. 导航到网关 **> HDX Insight >** 用户。
3. 从用户摘要报告部分选择特定用户。
4. 从当前会话或已终止的会话列中选择一个会话。

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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

指标	说明
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。

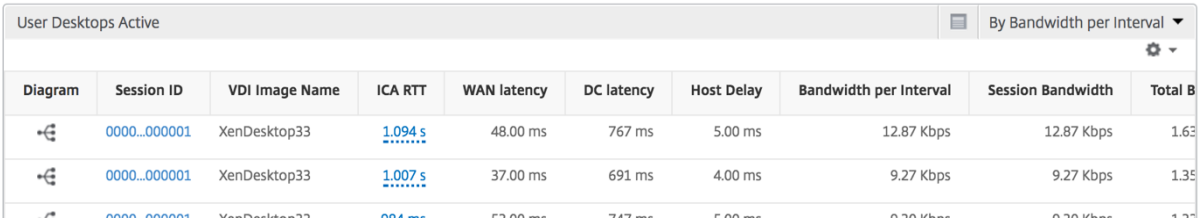


相关桌面会话报告　以下指标可以按每个间隔内的带宽、会话重新连接数和 ACR 计数排序。

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	服务器网络造成的 ICA 流量通过 NetScalers 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。
Start Time（开始时间）	会话开始时间。

指标	说明
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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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，NetScaler 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。
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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
Total Bytes（总字节数）	在选定的时间段内用户占用的总字节数。

指标	说明
Server Side Retransmits（服务器端重新传输数）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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集中在 NetScaler 实例上。

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 NetScaler 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）

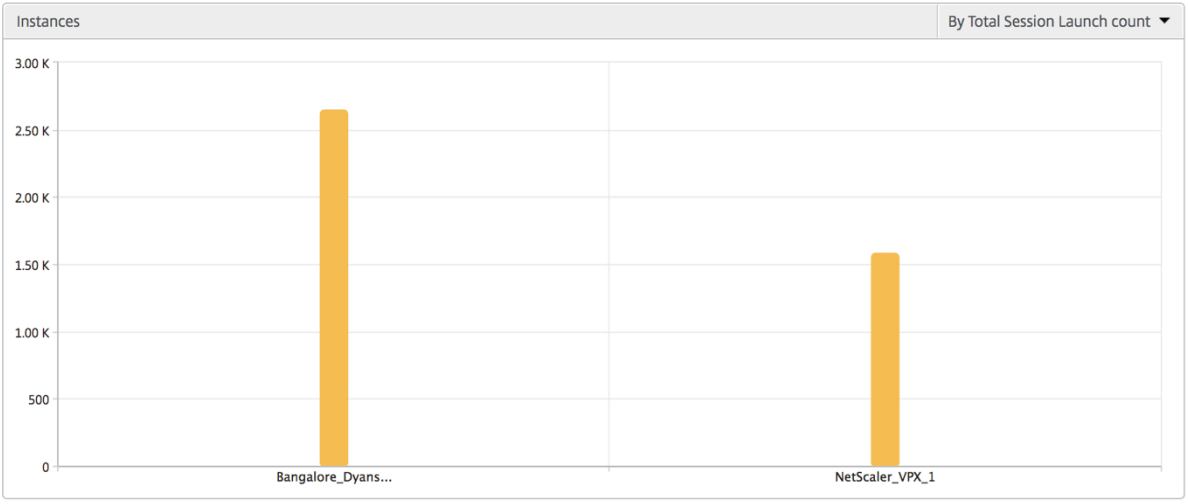
实例摘要视图

此视图称为摘要视图，因为它显示了添加到 NetScaler ADM 的所有 NetScaler 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。

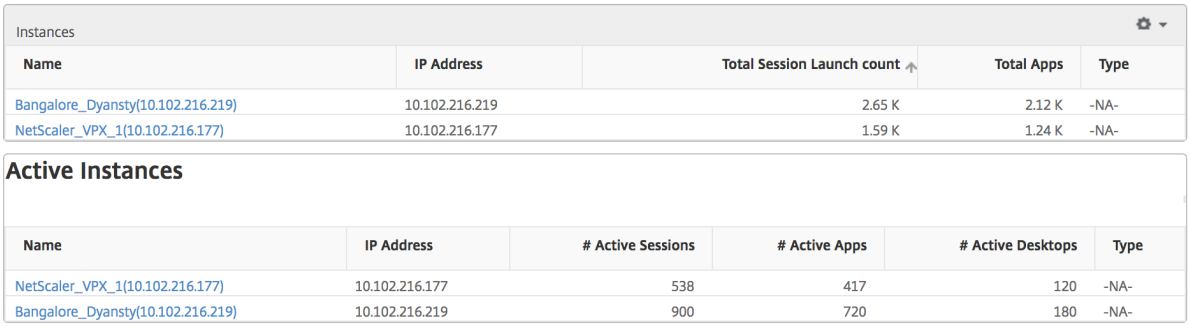
实例条形图

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	NetScaler 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



Instances

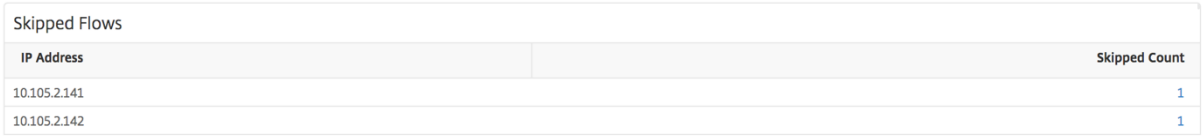
Name	IP Address	Total Session Launch count	Total Apps	Type
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	2.65 K	2.12 K	-NA-
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	1.59 K	1.24 K	-NA-

Active Instances

Name	IP Address	# Active Sessions	# Active Apps	# Active Desktops	Type
NetScaler_VPX_1(10.102.216.177)	10.102.216.177	538	417	120	-NA-
Bangalore_Dyansty(10.102.216.219)	10.102.216.219	900	720	180	-NA-

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 and Desktops 版本、不支持的 Workspace 版本或工作区类型等。此表显示了 IP 地址和跳过的流量计数。这些工作区可能不属于列入白名单的工作区。因此，这些会话将从监视中跳过。



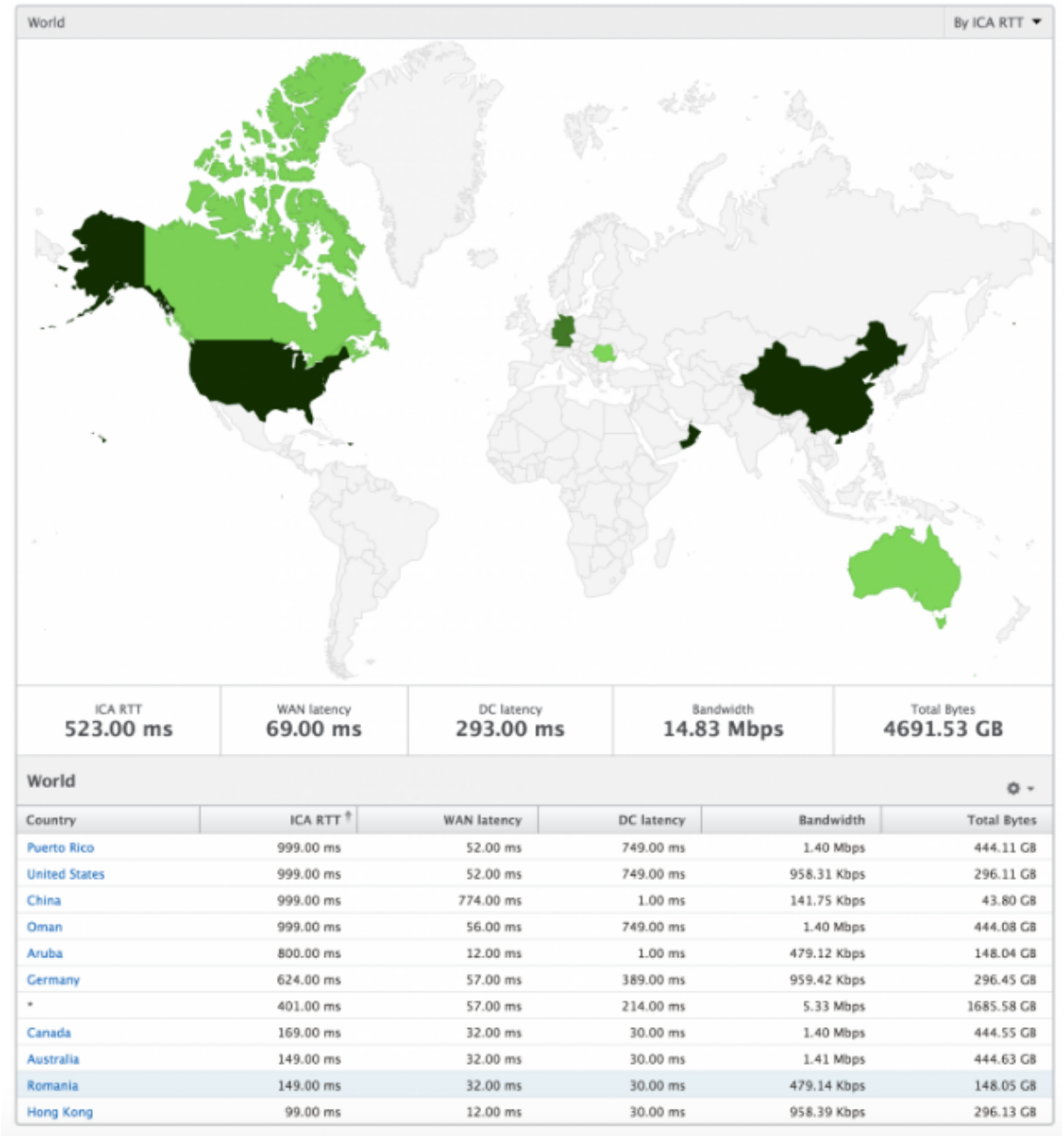
Skipped Flows

IP Address	Skipped Count
10.105.2.141	1
10.105.2.142	1

“**World**”（世界）视图　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 NetScaler 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 Insight 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

每个实例视图

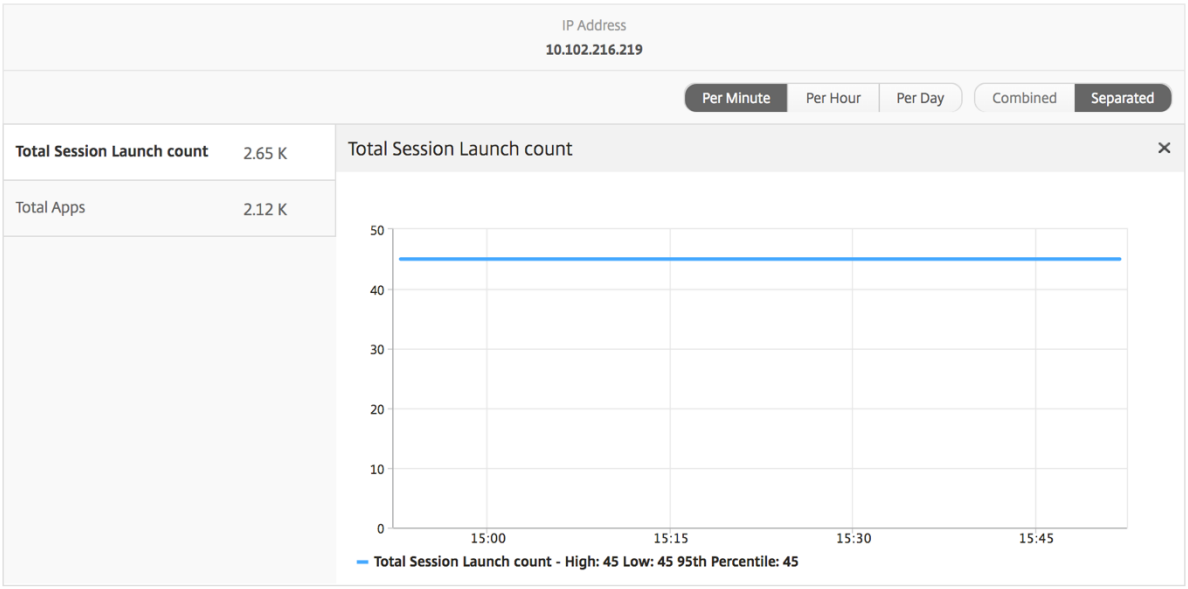
每个实例视图为特定选定的 NetScaler 实例提供详细的最终用户体验报告。

要导航到实例视图，请执行以下操作：

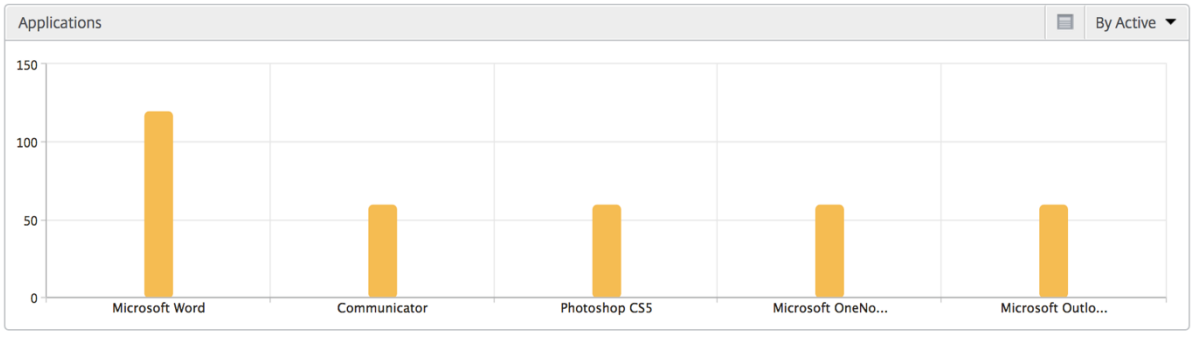
1. 使用支持的 Web 浏览器登录到您的 NetScaler ADM。
2. 导航到“分析”**>**“**HDX Insight**”**>**“实例”。
3. 从“实例 摘要报告”中选择特定实例。

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）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
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。



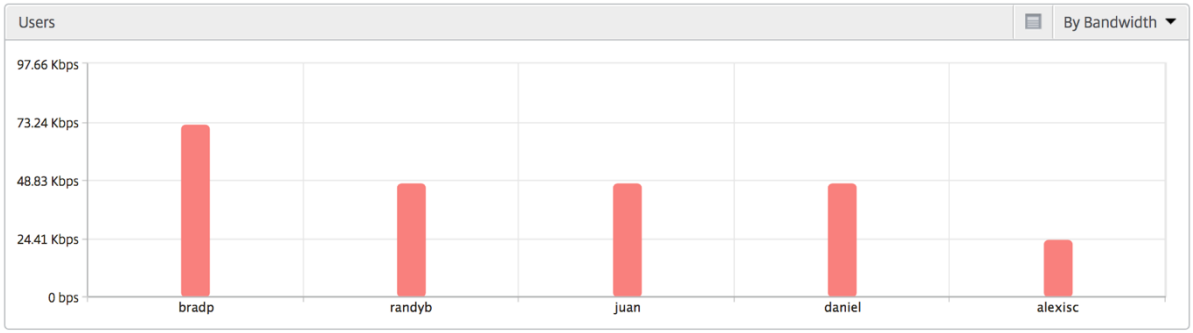
“**Applications**”（应用程序）条形图　根据以下条件显示前 5 个应用程序-按活动应用程序、总会话启动次数、总应用程序启动次数或启动持续时间。



“**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

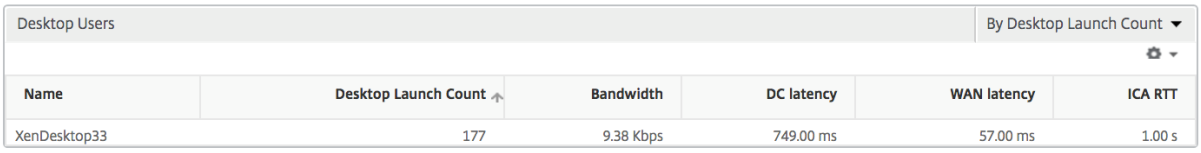
- Bandwidth（带宽）
- WAN 延迟

- 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 Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。
Bandwidth（带宽）	在所选时间间隔内，端到端通信所占用的每秒总字节数。
DC 延迟	网络的服务器端导致的延迟。也就是说，在 NetScaler Gateway 和 VDI 或 CVAD 或 StoreFront 服务器之间。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 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。

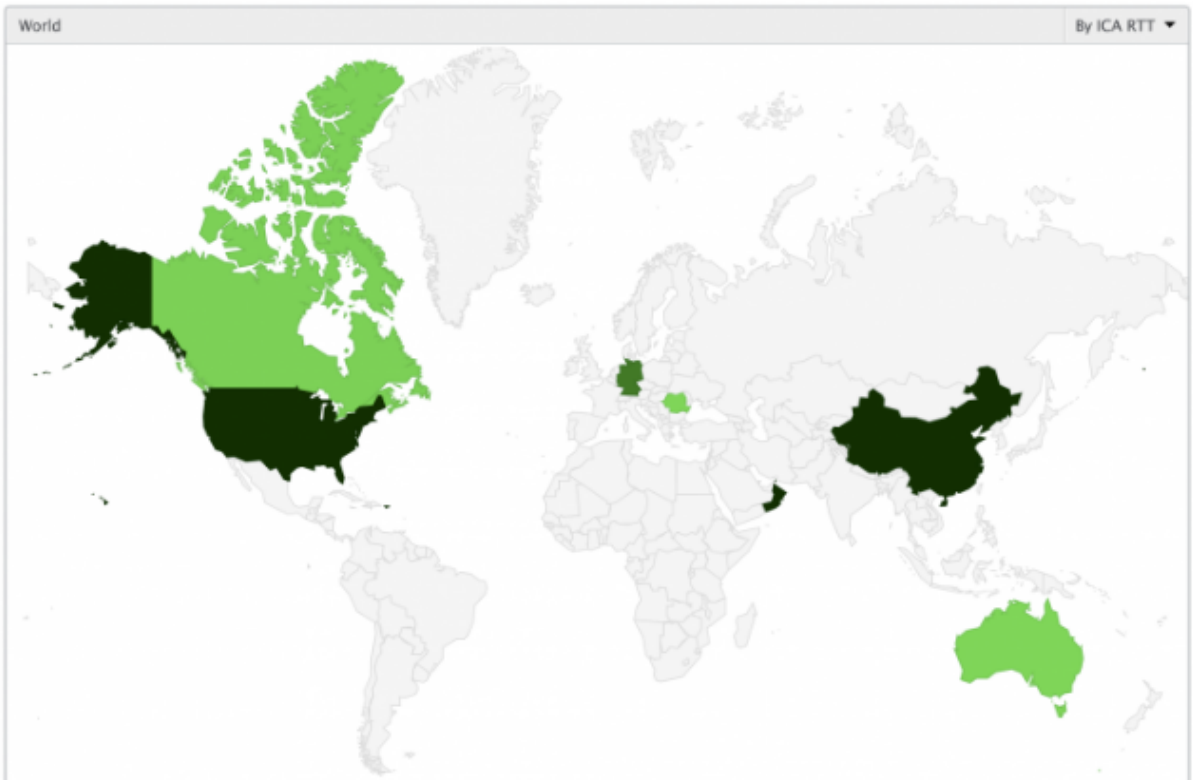


“**World**”（世界）视图　通过 HDX Insight 中的世界地图视图，管理员可以从地理视角查看历史和活动用户详细信息。管理员可以拥有系统的“世界”视图，向下钻取到特定国家/地区，并进一步查看城市以及通过单击区域。管理员可以按城市和省/自治区进一步深入查看信息。从 NetScaler ADM 12.0 版及更高版本中，您可以深入到从地理位置连接的用户。

以下详细信息可以在 HDX Insight 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

许可证查看报告和指标

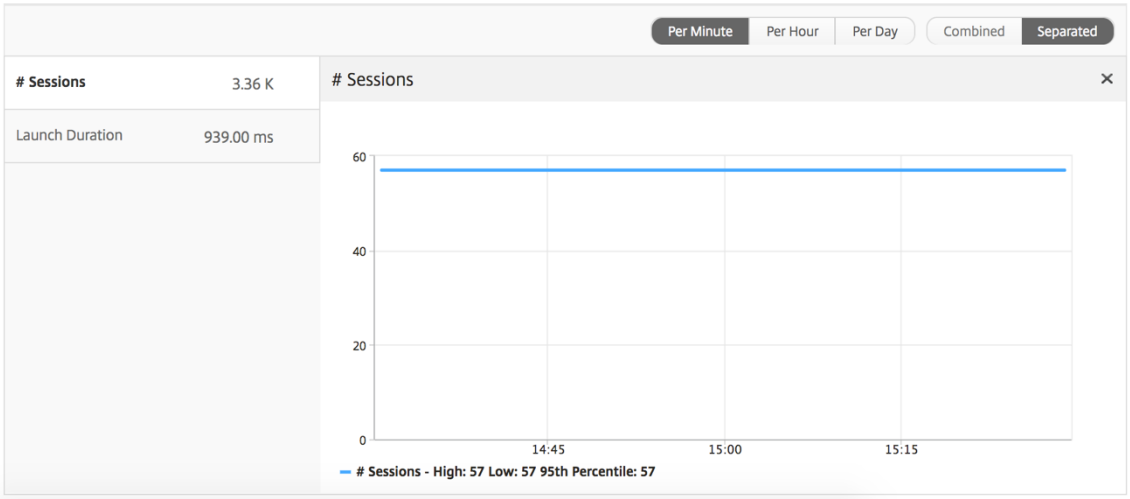
许可证视图提供了有关 NetScaler Gateway 许可证信息的详细信息。

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 NetScaler 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	在选定的时间轴内使用的 NetScaler 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 NetScaler 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

February 6, 2024

此视图中的报告和衡量指标侧重于 Citrix Virtual Apps。

要导航到“应用程序”视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 应用程序。

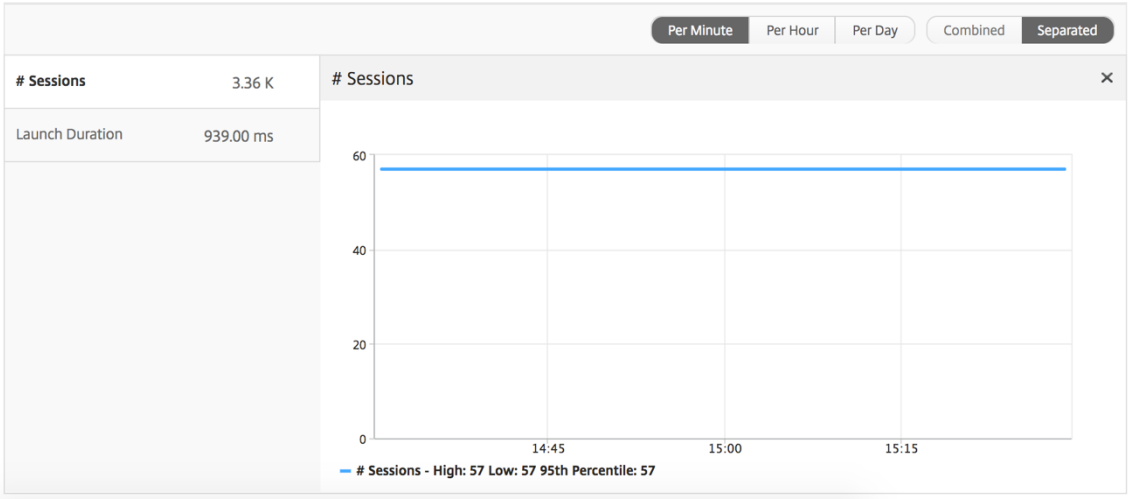
Summary View（摘要视图）

“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。

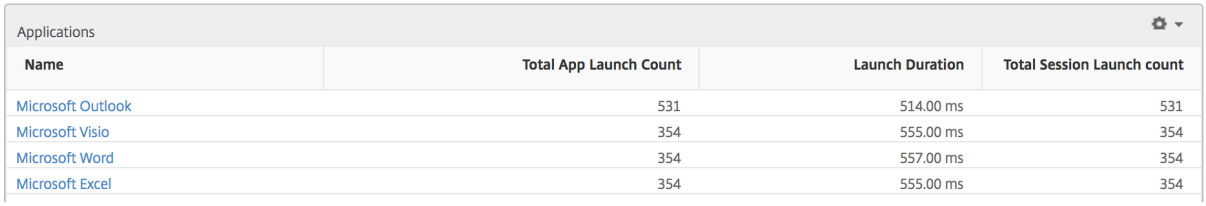
折线图

指标	说明
Sessions（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 Virtual Apps 的名称。
Total Session Launch Count（会话启动总数）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
Total App Launch Count（应用程序启动总数）	在给定时间间隔内启动的 Citrix Virtual Apps 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。

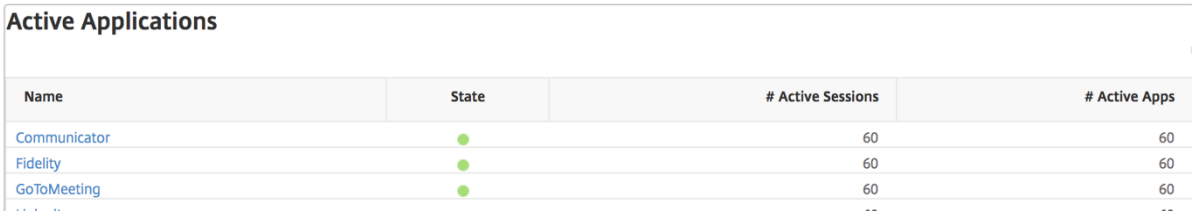


Applications

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 Virtual Apps 的名称。
状态	显示应用程序的状态：绿色 - 活动、红色 - 不活动
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。



Active Applications

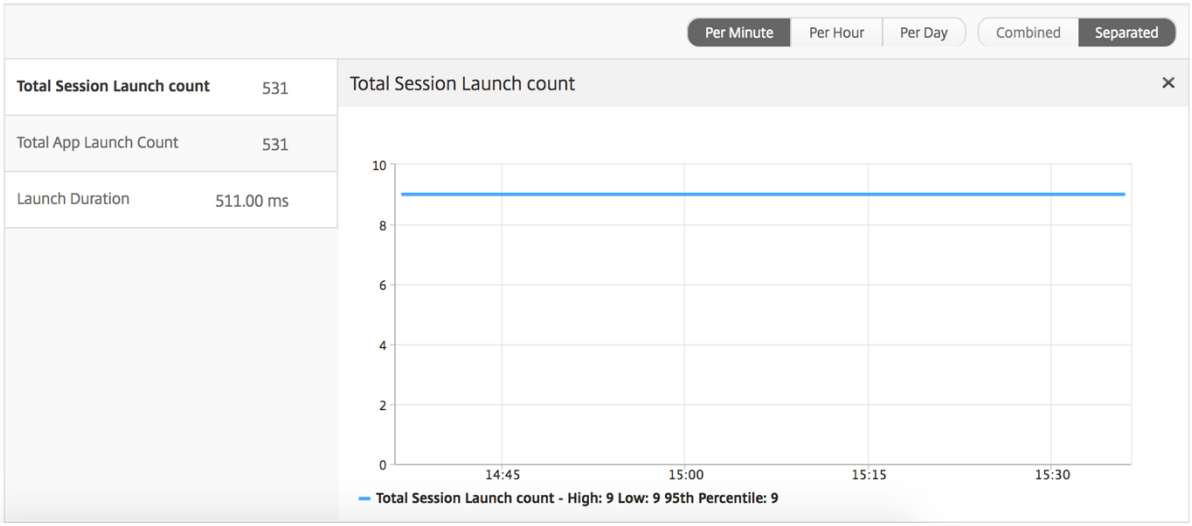
Name	State	# Active Sessions	# Active Apps
Communicator		60	60
Fidelity		60	60
GoToMeeting		60	60

阈值报告

阈值报告表示在选定时间段内将 实体 选为应用程序时突破的阈值计数。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
Active Sessions（活动会话数）	此数字表示活动 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。

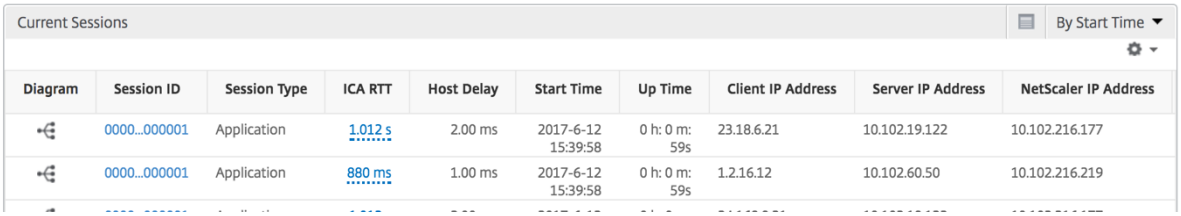


当前会话报告

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	服务器网络造成的 ICA 流量通过 NetScalers 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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。

指标	说明
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，NetScaler 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。
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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 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 Virtual Apps 的用户的用户名。
会话 ID	Citrix Virtual Apps 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，红色表示不活动。
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。
L7 Client-side Latency（L7 客户端延迟）	ICA 客户端和 NetScaler 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）	NetScaler 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

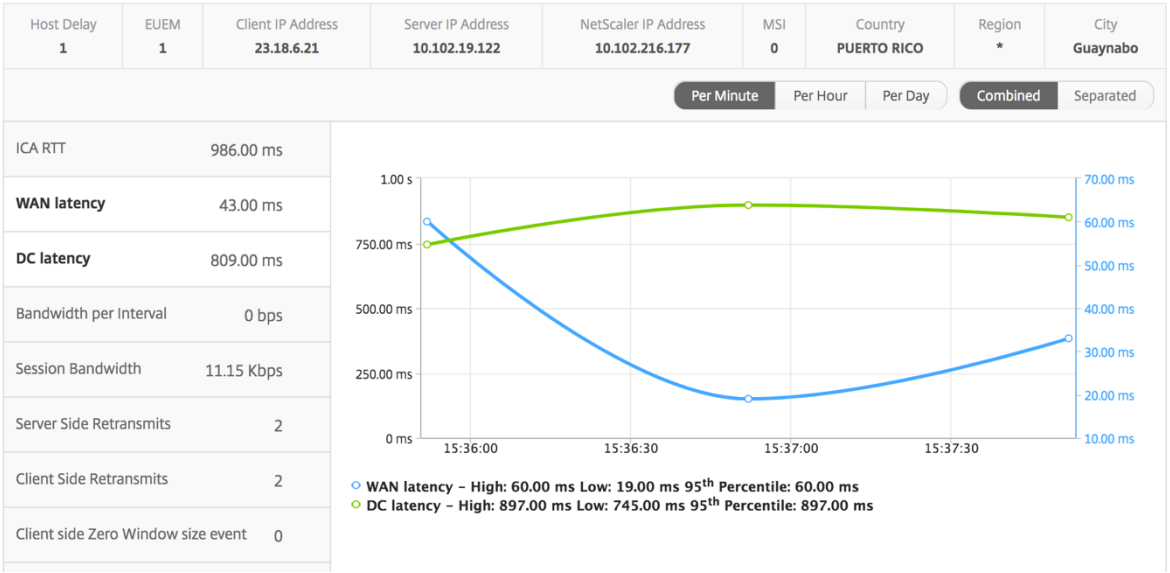
“Per Application Session View”（每个应用程序会话视图）显示特定的选定应用程序会话的报告。

要查看会话报告，请执行以下操作：

1. 导航到网关 **> 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。

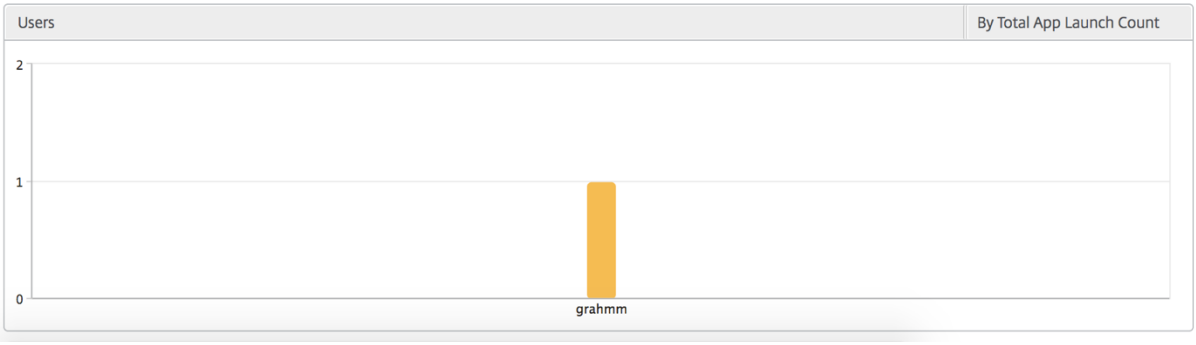
折线图

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。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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

February 6, 2024

此视图中的报告和衡量指标集中在 Citrix Virtual Desktops 上。

要导航到桌面视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 桌面。

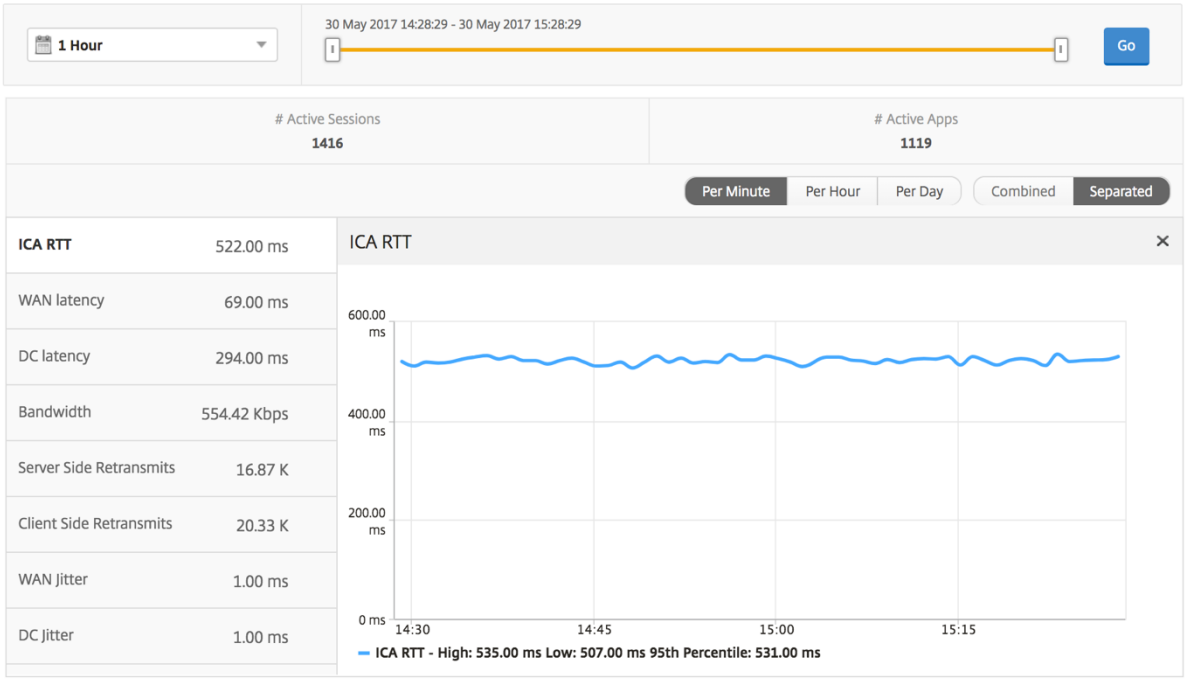
Summary View（摘要视图）

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。

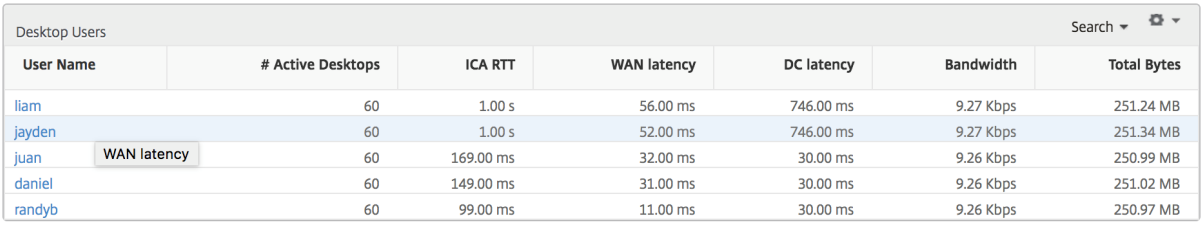
折线图

指标	说明
Active Sessions（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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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	在给定时间间隔内活动 Citrix Virtual Desktops 会话的总数。
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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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。

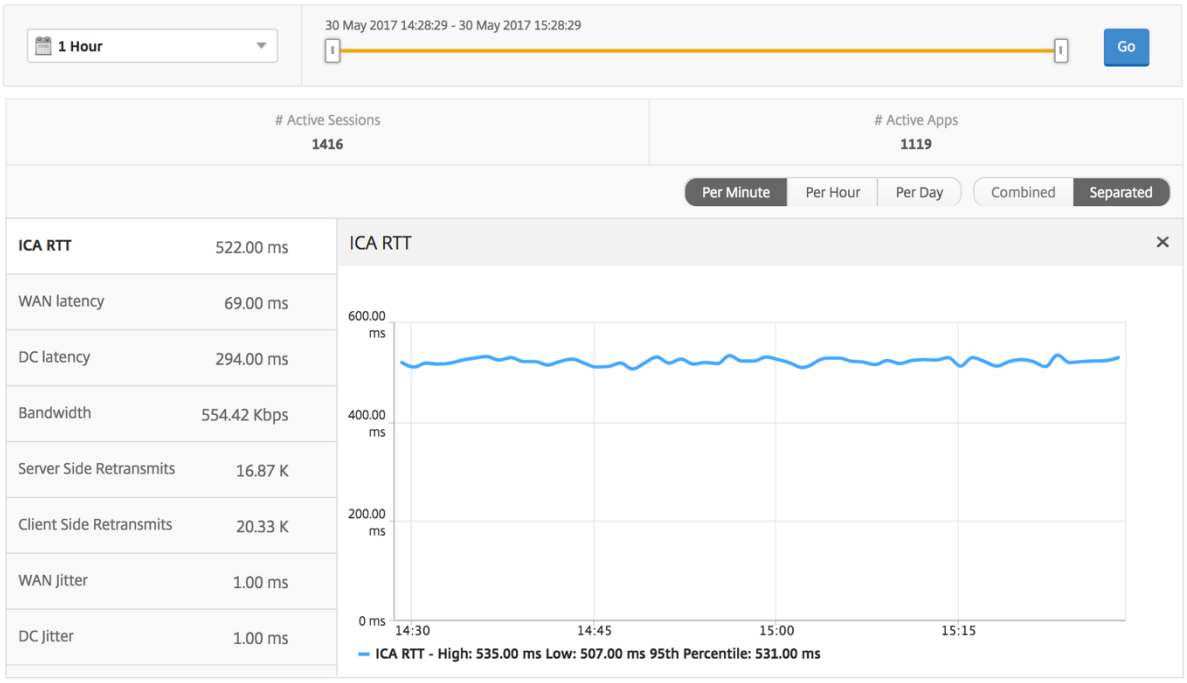
要导航到特定的桌面视图，请执行以下操作：

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
Active Sessions（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 Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

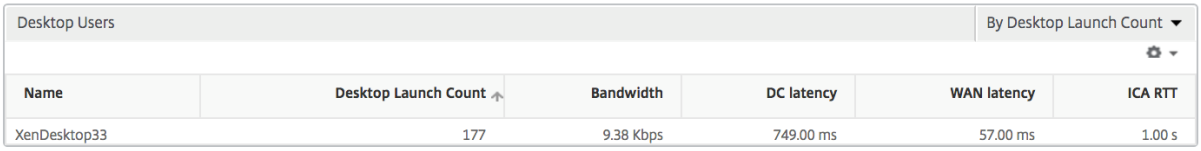


“**Desktop Users**”（桌面用户）报告

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 Virtual Desktops 的名称。
Desktop Launch Count（桌面启动计数）	桌面启动次数。

指标	说明
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 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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。



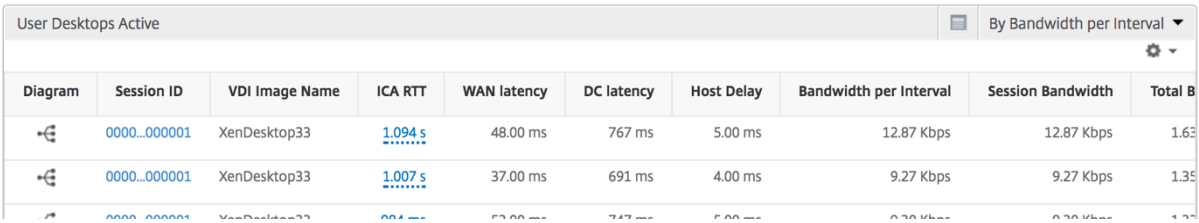
用户桌面活动/非活动报告

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	服务器网络导致的通过 NetScaler 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等

指标	说明
客户端版本	Workspace 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，NetScaler 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。
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 Virtual Apps 或 Citrix Virtual Desktops 上托管的应用程序或桌面进行交互时遇到的屏幕延迟。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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。

指标	说明
Client side fast RTO（客户端快速 RTO）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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. 导航到网关 **> 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。

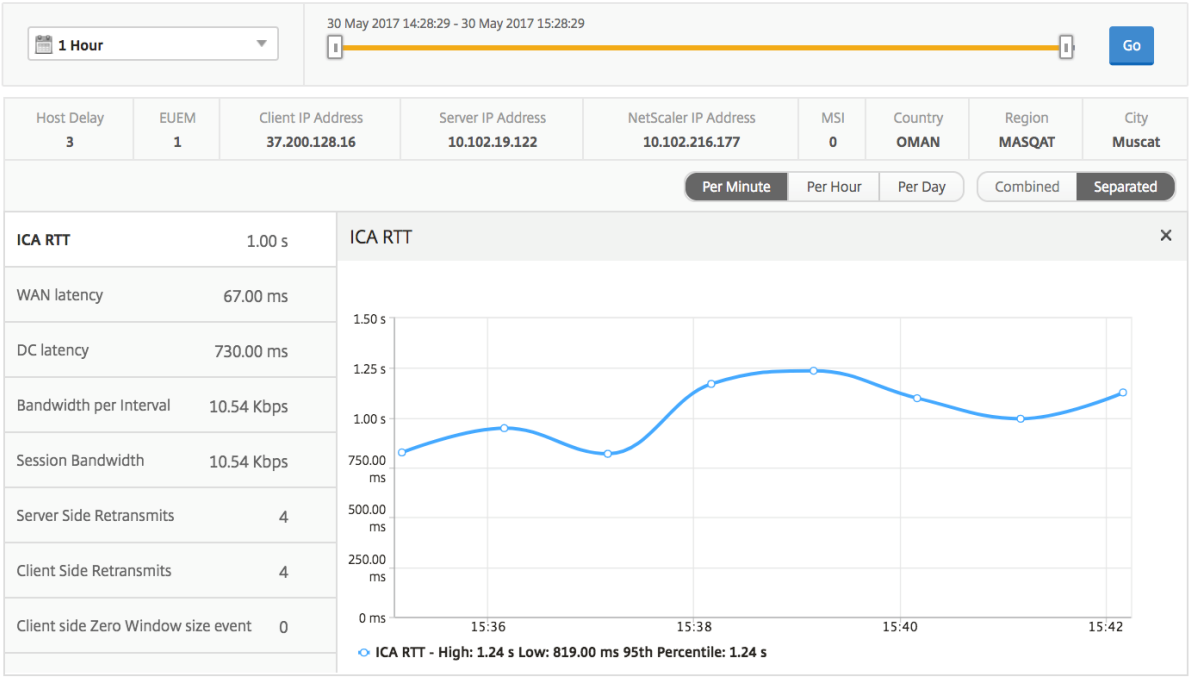
时间线图

“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. 导航到网关 **> HDX Insight >** 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或已终止的会话列中选择一个会话。

指标	说明
Session Reconnects（会话重新连接数）	此数字表示活动 Citrix Virtual App and Desktop 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 会话的计数。
ICA RTT	ICA RTT 是用户在与 Citrix 虚拟应用程序和桌面上分别托管的应用程序或桌面进行交互时遇到的屏幕延迟。
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。



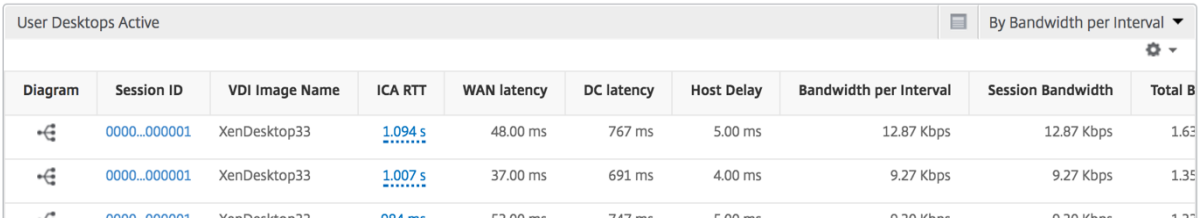
相关桌面会话报告

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	服务器网络造成的 ICA 流量通过 NetScalers 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。

指标	说明
客户端类型	Receiver 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，NetScaler 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。
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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	NetScaler 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）	NetScaler 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 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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



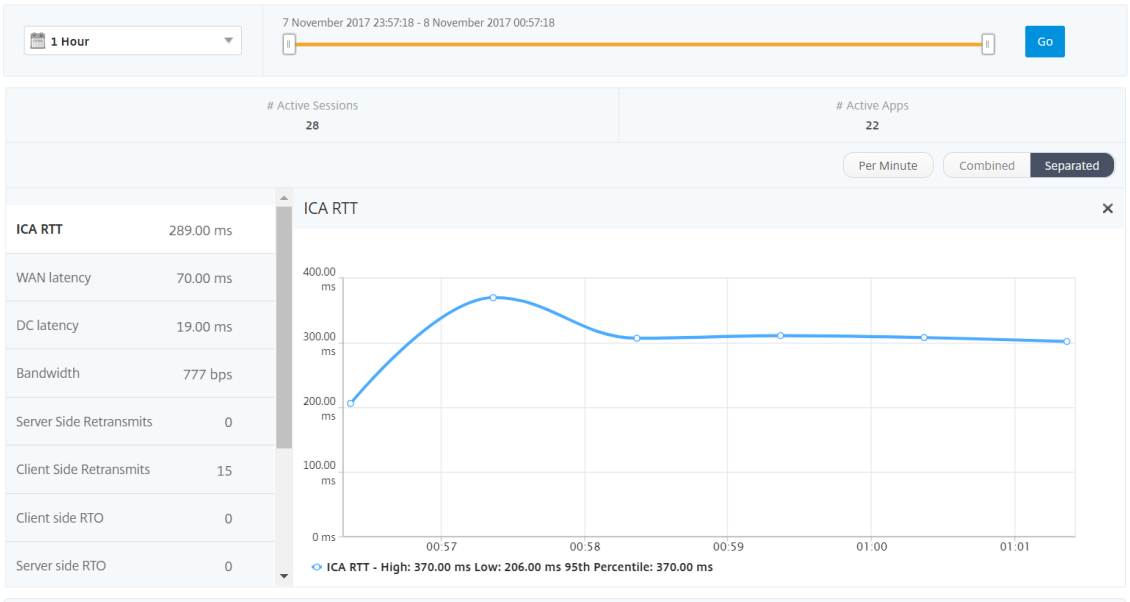
“**User**”（用户）视图报告和指标

February 6, 2024

此视图中的报告和衡量指标按 Citrix Virtual Apps and Desktops 用户显示。

要导航到“用户”视图，请执行以下操作：

1. 导航到网关 **> 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/报告都将显示选定时段内与其对应的值。

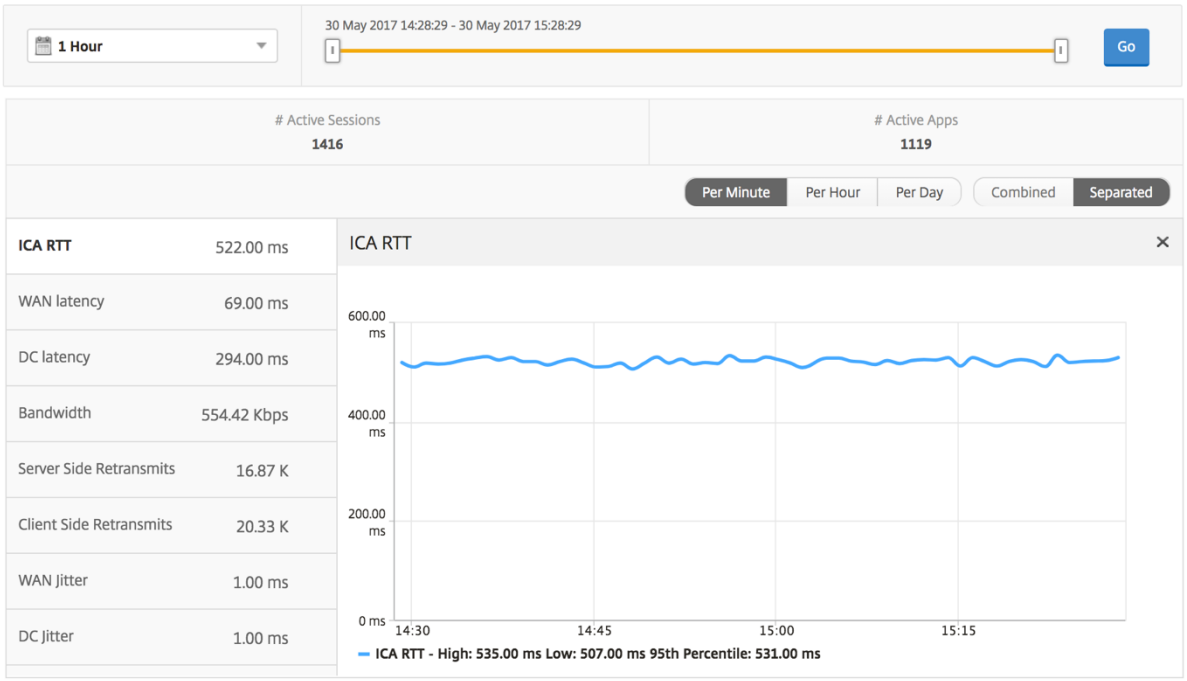
要更改选定时间段，请执行以下操作：

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
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual App and Desktop 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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）	在 NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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
Active Sessions（活动会话数）	此数字表示活动 Citrix Virtual App and Desktop 会话的计数。
Active 应用程序	此数字表示活动 Citrix Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

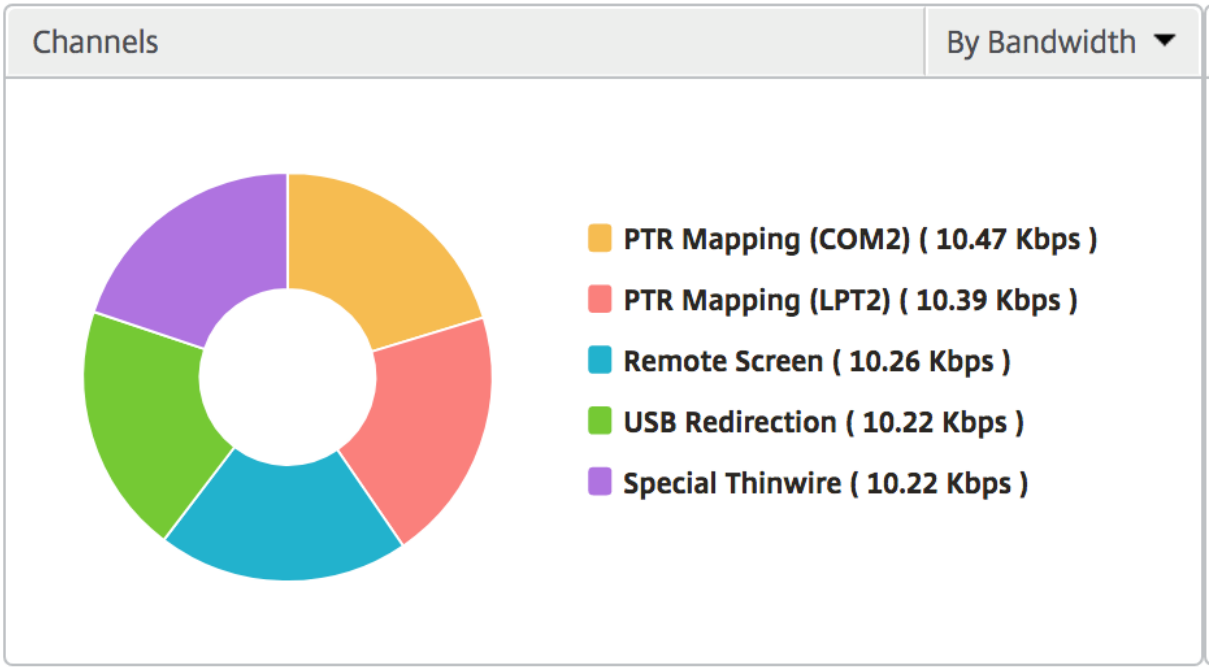
Users

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	

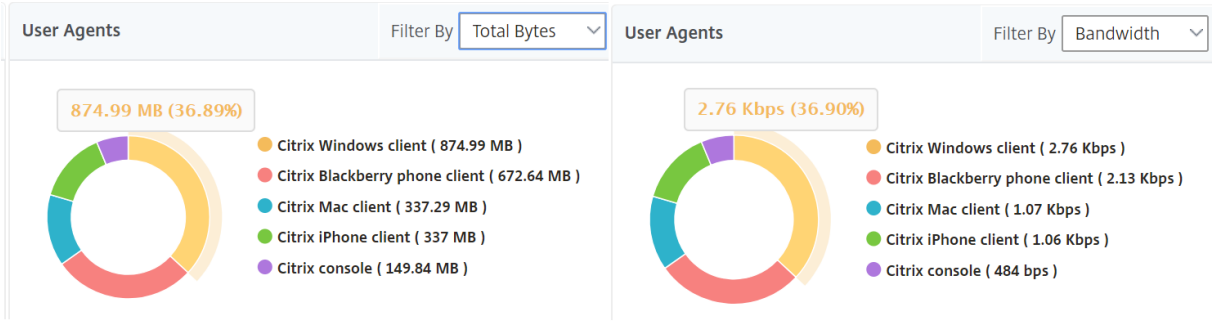
Channels（通道）

“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

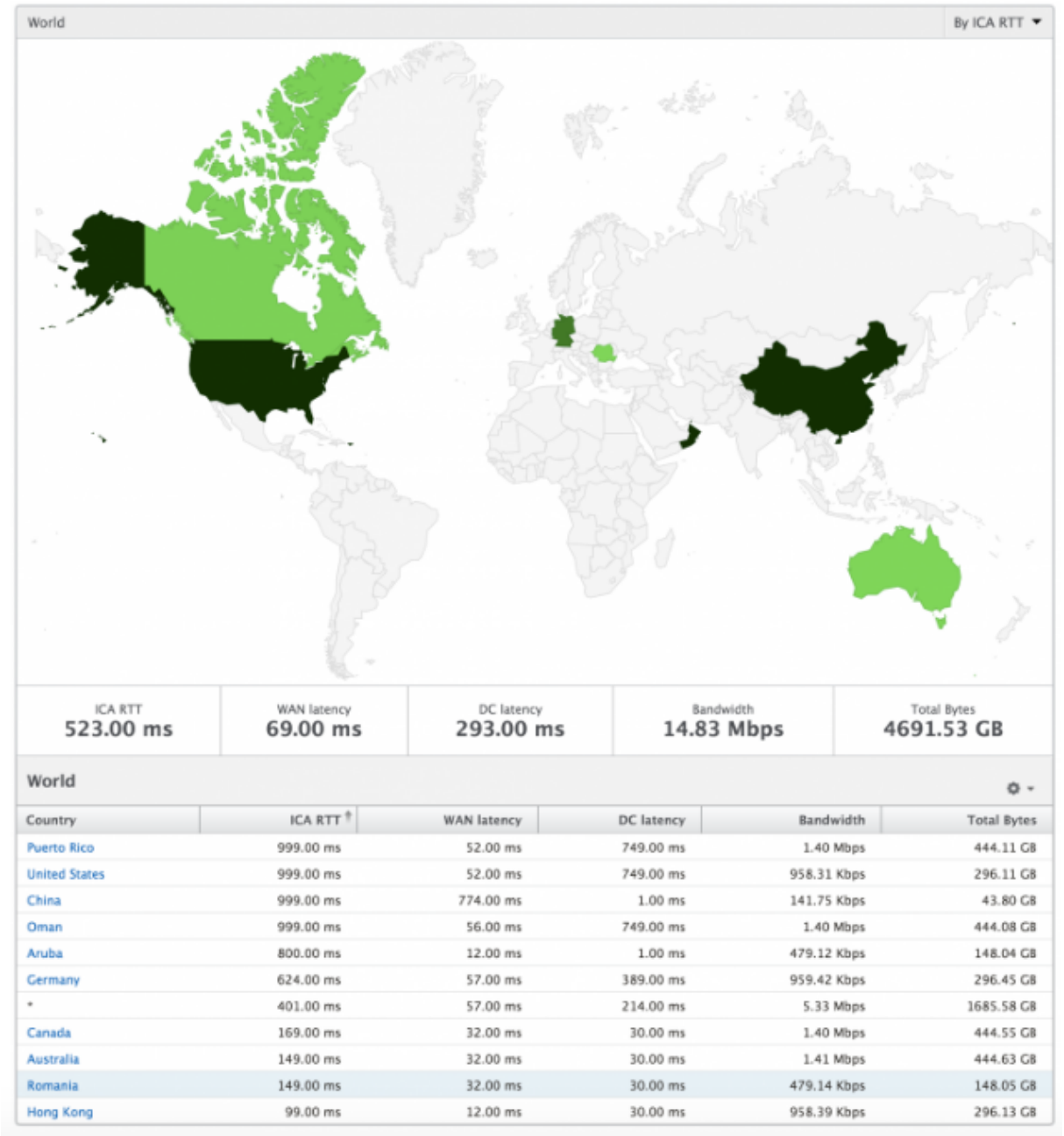
阈值违反计数指标表示在选定时间段内违反的阈值计数。有关更多信息，请参阅 如何创建阈值和警报。

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/自治区进一步深入查看信息。从 NetScaler 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 Insight 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. 导航到网关 **> 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/已终止会话报告

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	服务器网络导致的通过 NetScaler 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。
Start Time（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 Virtual Apps 服务器 IP。
NetScaler IP Address（NetScaler IP 地址）	NetScaler 管理 IP (NSIP)。
客户端类型	工作区类型 - Citrix Windows 客户端等等
客户端版本	Workspace 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，NetScaler 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。

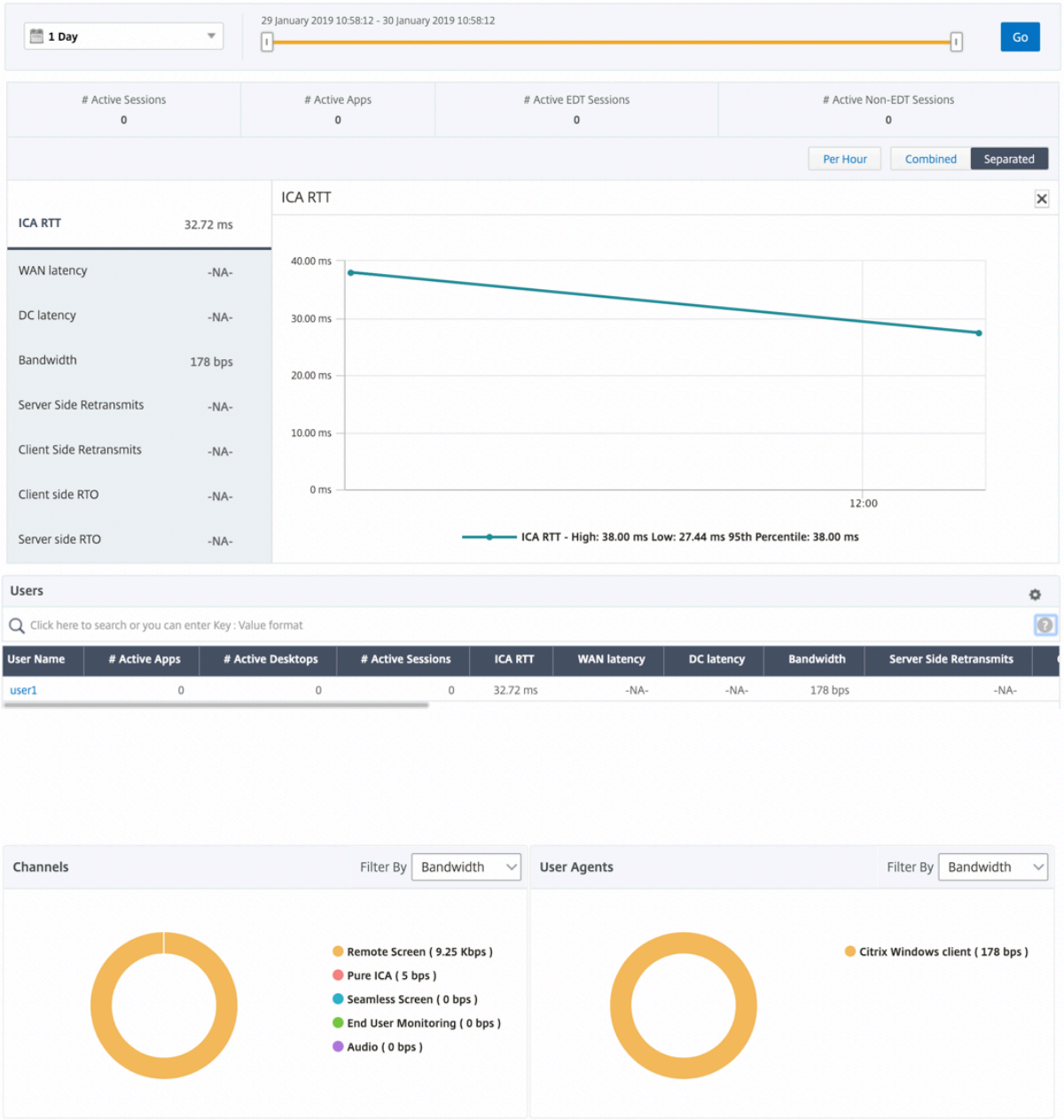
指标	说明
Number of USB Instances Accepted（接受的 USB 实例数）	接受的 USB 实例计数。
Number of USB Instances Rejected（拒绝的 USB 实例数）	拒绝的 USB 实例计数。
Number of USB Instances Stopped（停止的 USB 实例数）	停止的 USB 实例计数。
Client Host Name（客户端主机名）	客户端的主机名。
HA Failover Count（HA 故障转移计数）	发生的 HA 故障转移次数。
Reason for termination（终止原因）	显示会话终止的原因。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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。
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）	NetScaler 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 Insight** 中的 **EDT**

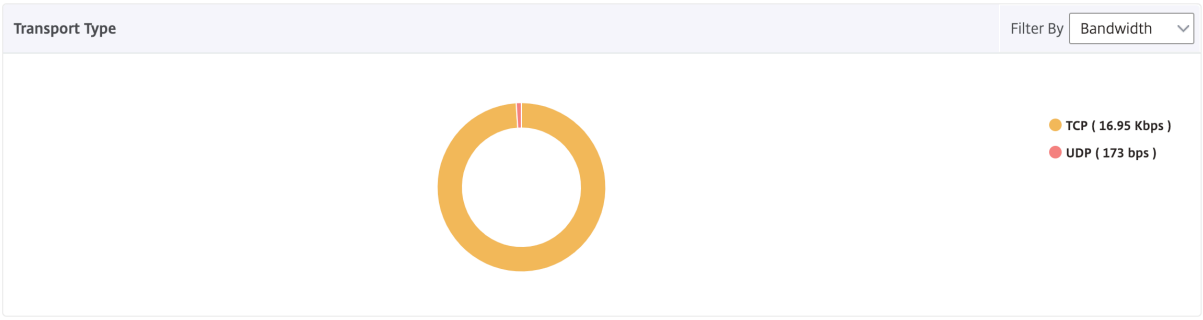
NetScaler Application Delivery Management (ADM) 现在支持开明的数据传输 (EDT)，用于显示 HDX Insight 的分析结果。也就是说, ADM 现在同时支持 UDP 和 TCP 协议。对 NetScaler Gateway 的 EDT 支持确保运行 Citrix Workspace 的用户在会话中获得虚拟桌面的高清晰度用户体验

HDX Insight 现在在活动会话报告中显示 EDT 会话和非 EDT 会话的数量。“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。其中一些指标不适用于拥有 EDT 会话的用户，因为这些指标是根据当前 TCP 堆栈计算得出的。因此，它们显示为“NA”。

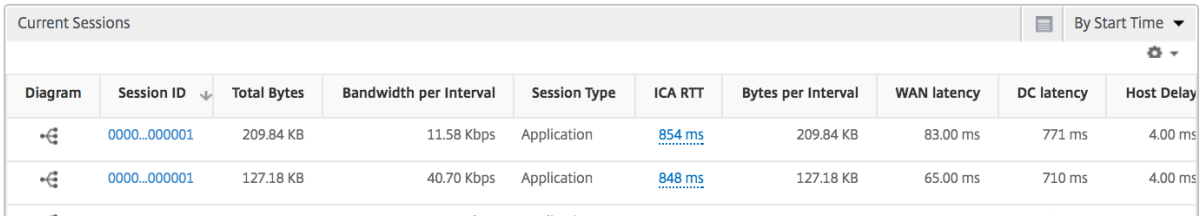


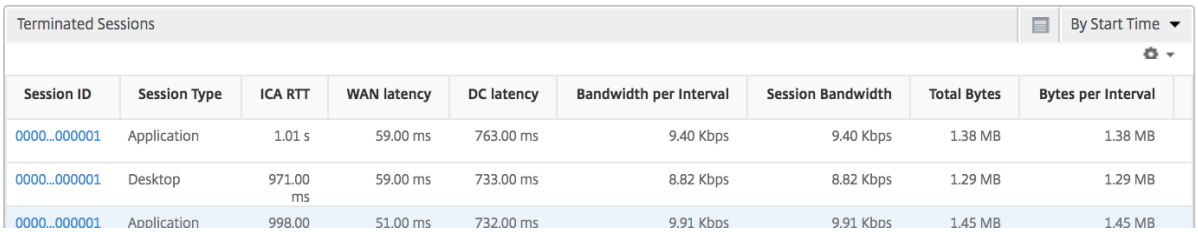
引入了一个新的圆环图，允许您查看用户消耗的带宽以及基于用户使用的协议类型的总字节数。



NetScaler 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 NetScaler 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）	NetScaler 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。

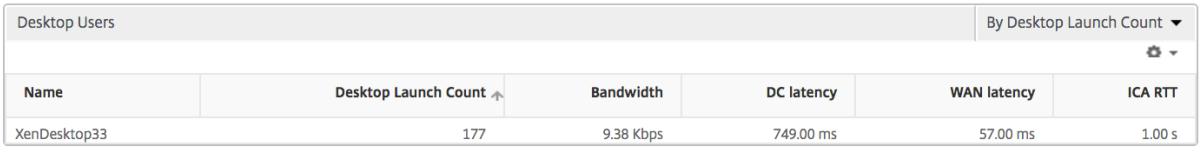




Desktop Users（桌面用户）

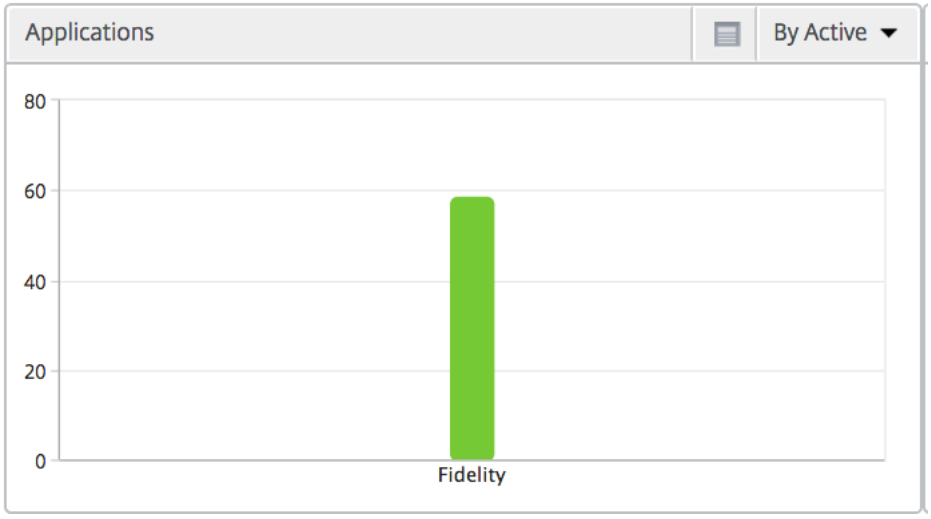
此表可深入了解特定用户的 Citrix 虚拟桌面会话。这些指标可以按桌面启动计数和带宽排序。

指标	说明
名称	Citrix Virtual Desktops 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 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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。



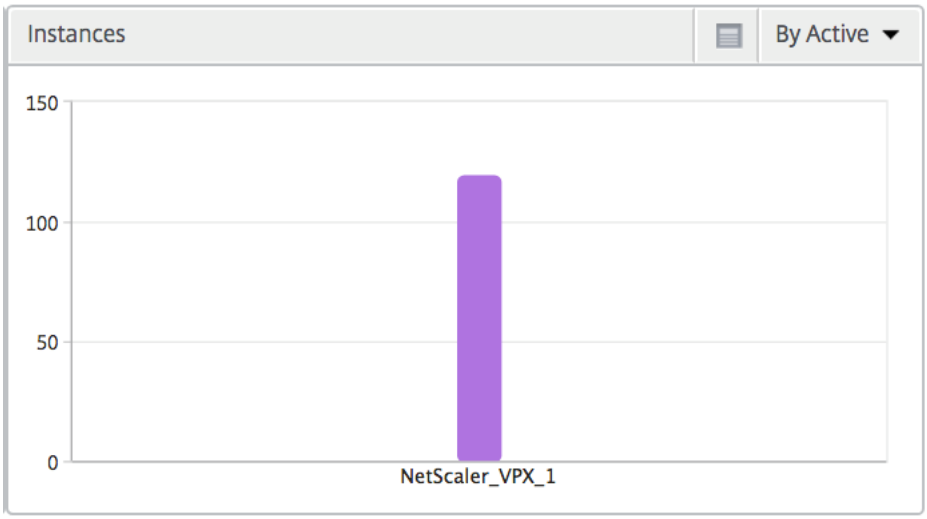
应用程序

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。



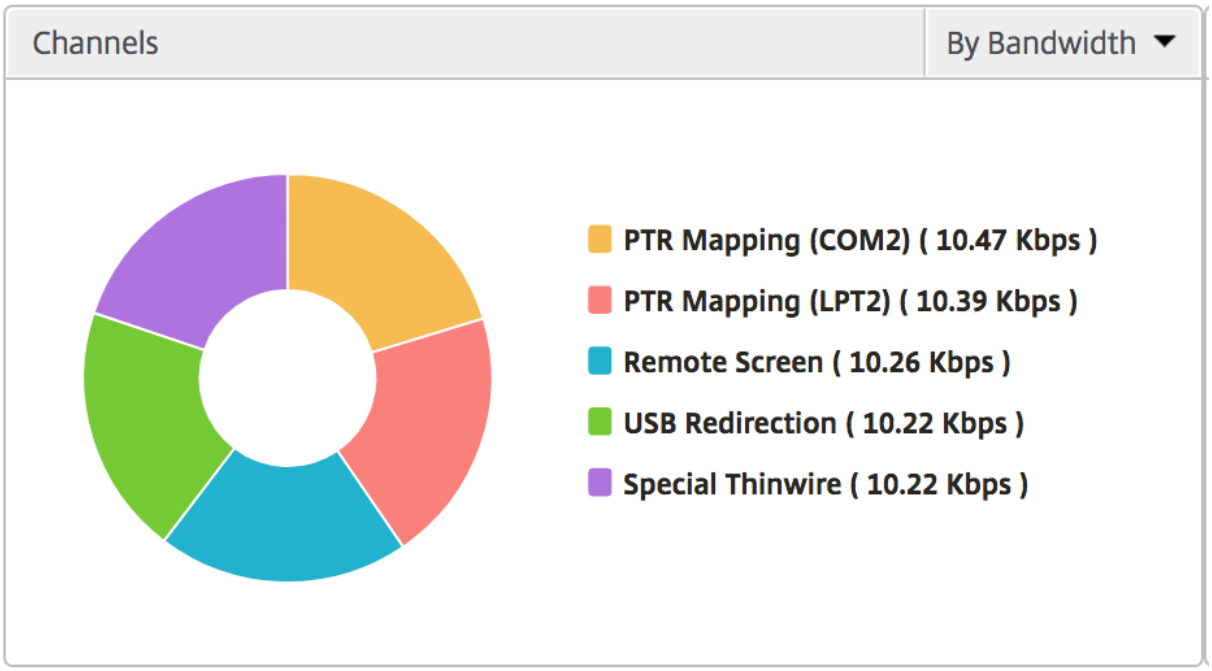
实例

表示按活动应用程序和总应用程序排序的 NetScaler 实例的条形图



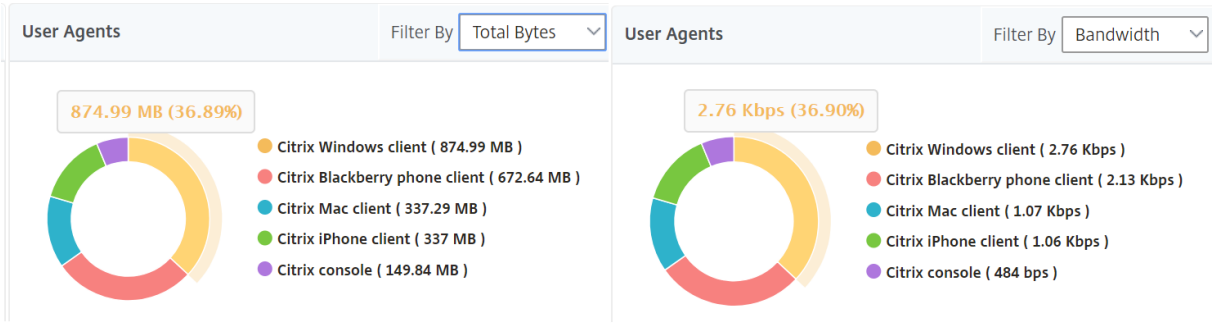
Channels（通道）

“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。

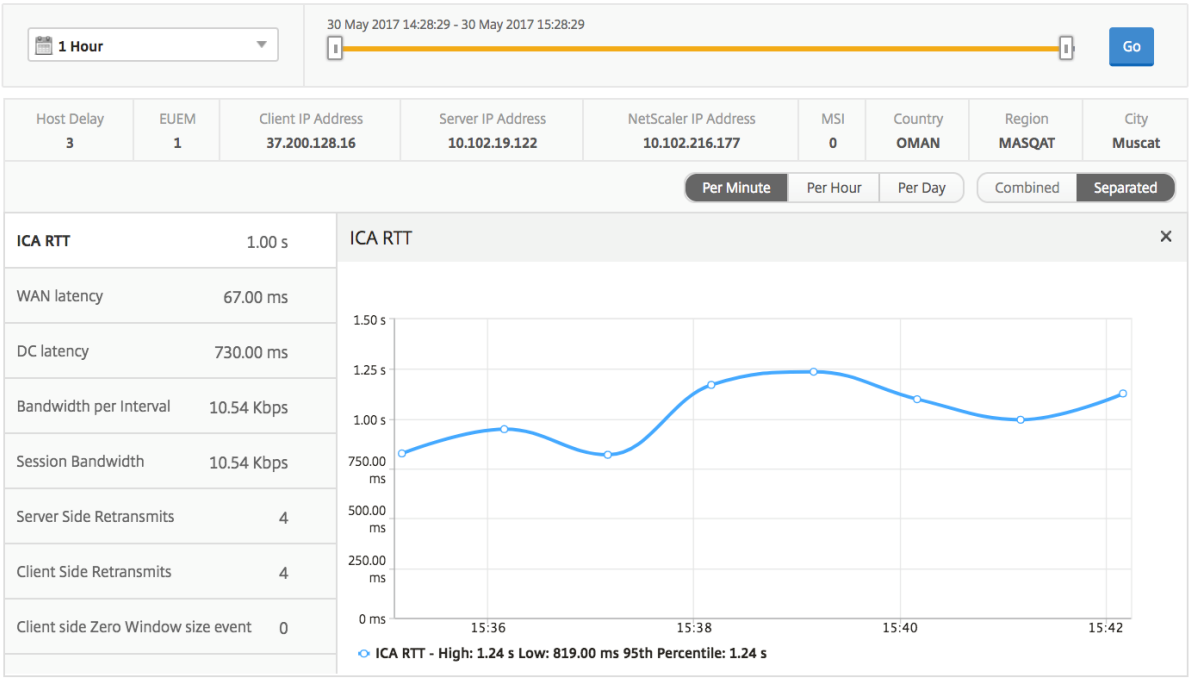
要查看选定用户会话的度量，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 用户。
2. 从用户摘要报告部分选择特定用户。
3. 从当前会话或已终止的会话列中选择一个会话。

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 App and Desktop 会话的计数。
ACR Counts（ACR 计数）	此数字表示活动 Citrix Virtual Apps 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 NetScaler 到最终用户。
DC 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 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 NetScaler 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）	NetScaler 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）	NetScaler 与最终用户之间的连接发生重传超时的次数。

指标	说明
Server side fast RTO（服务器端快速 RTO）	NetScaler 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。

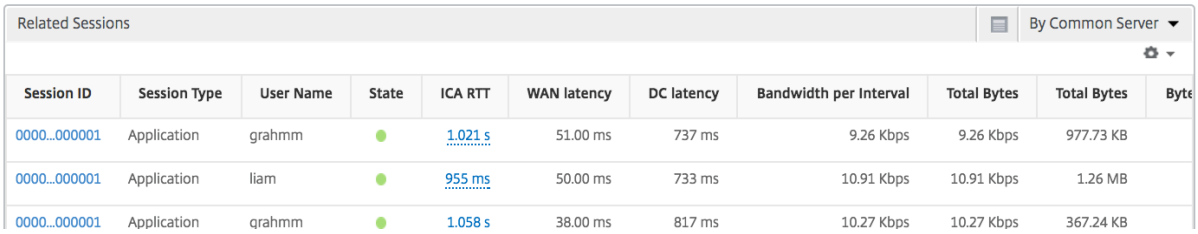


活动应用程序

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。

相关会话

“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 NetScaler。



“Instance”（实例）视图报告和指标

February 6, 2024

实例视图中的报告和指标集中在 NetScaler 实例上。

要导航到实例视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 实例。

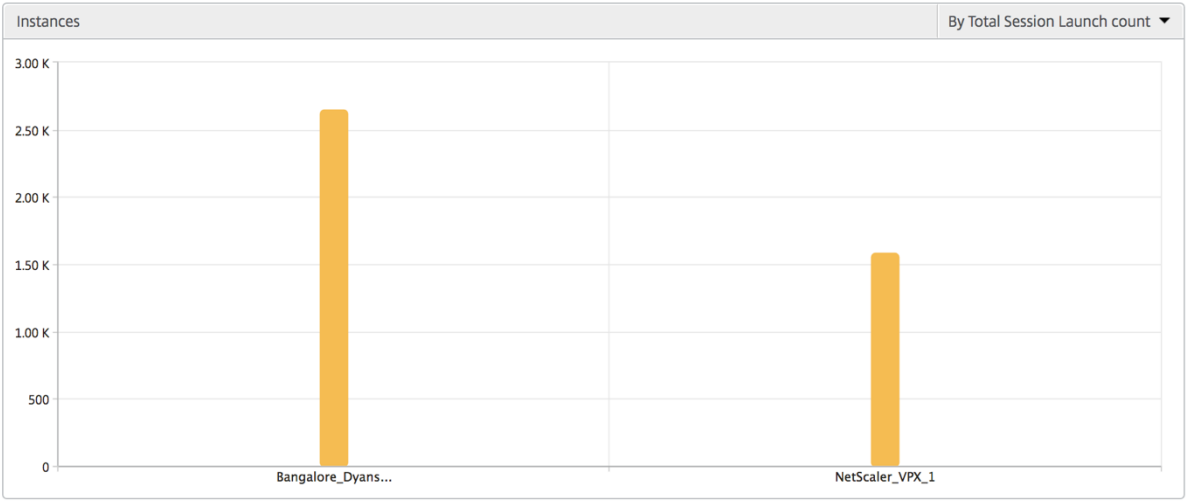
实例摘要视图

此视图称为摘要视图，因为它显示了添加到 NetScaler ADM 的所有 NetScaler 实例的报告。

除非明确提及，否则所有指标/报告在所选时间段内都将具有与之对应的值。

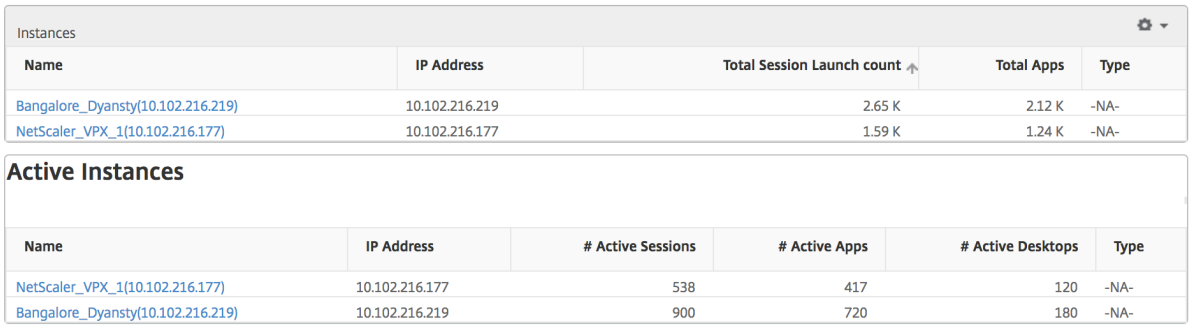
实例条形图

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	NetScaler 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



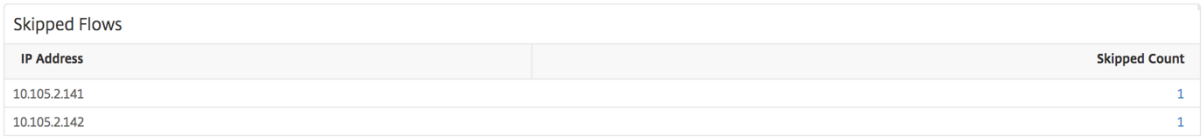
阈值报告

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。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 and Desktops 版本、不支持的 Workspace 版本或工作区类型等。此表显示 IP 地址和跳过的流计数。这些工作区可能不属于列入白名单的工作区。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。



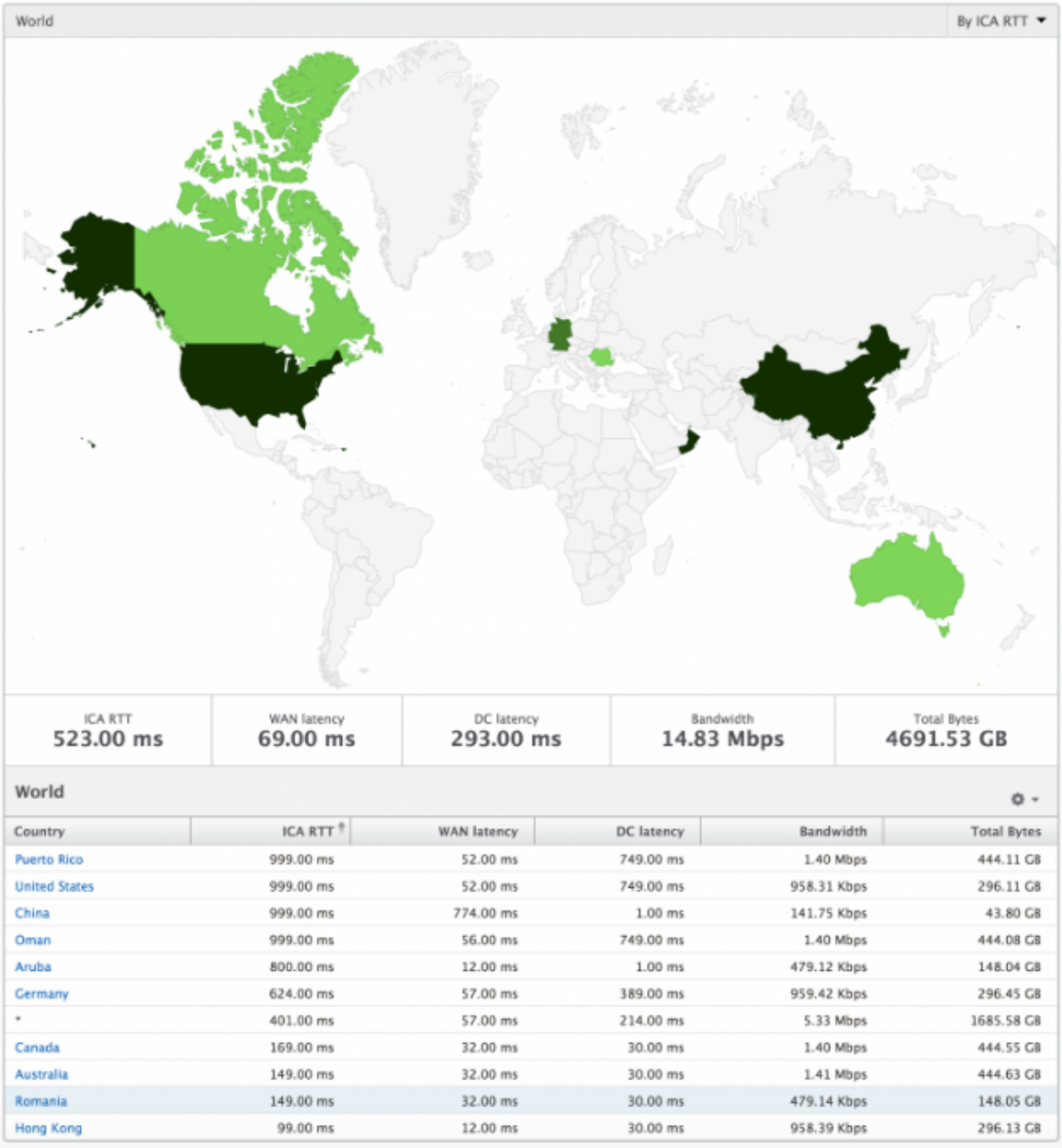
“**World**”（世界）视图

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。管理员可以进一步向下钻取以按城市

和州查看信息。从 NetScaler 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 Insight 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

每个实例视图

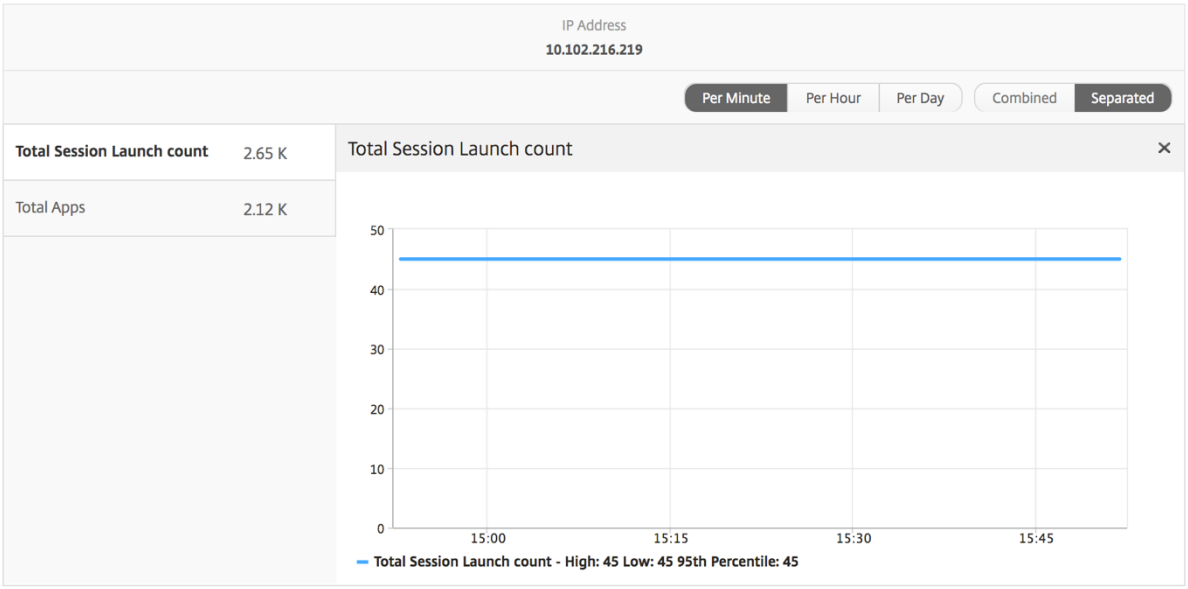
每个实例视图为特定选定的 NetScaler 实例提供详细的最终用户体验报告。

要导航到实例视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 实例。
2. 从“实例 摘要报告”中选择特定实例。

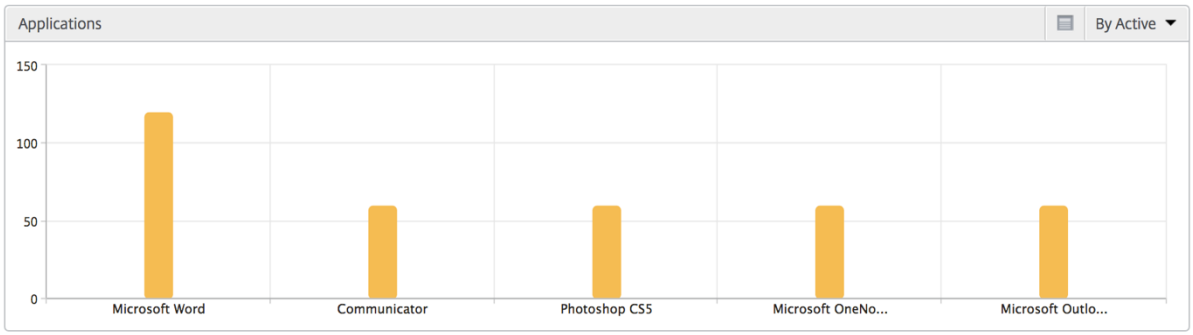
折线图

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）	在给定时间间隔内活动 Citrix Virtual Apps 会话的总数。
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

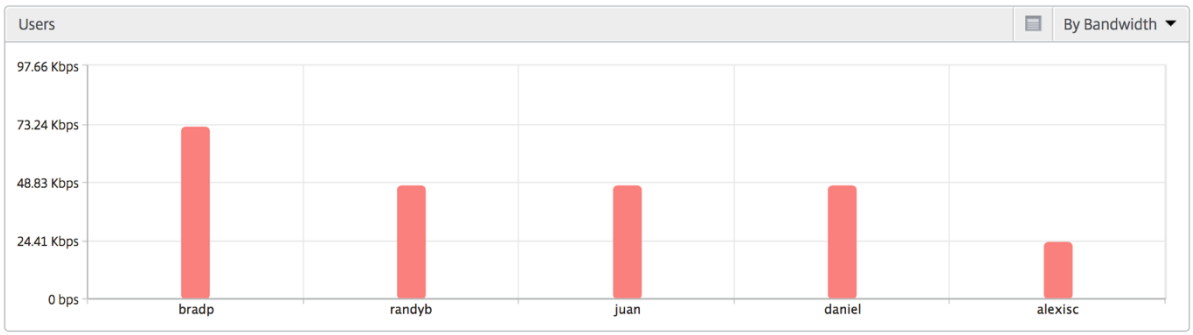
根据以下条件显示前 5 个应用程序-按活动应用程序、总会话启动次数、总应用程序启动次数或启动持续时间。



“**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

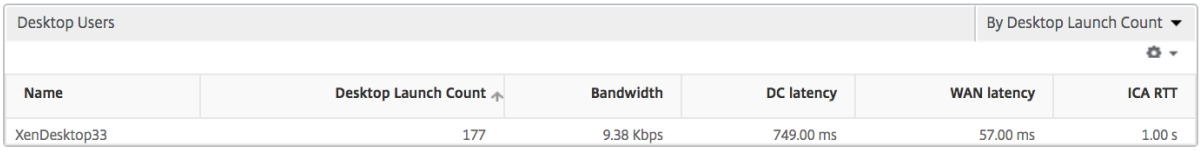


“**Desktop Users**”（桌面用户）报告

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 Virtual Desktops 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 延迟	网络的服务器端导致的延迟。也就是说，从 NetScaler 到后端服务器。

指标	说明
WAN 延迟	网络的客户端导致的延迟。也就是说，从 NetScaler 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。

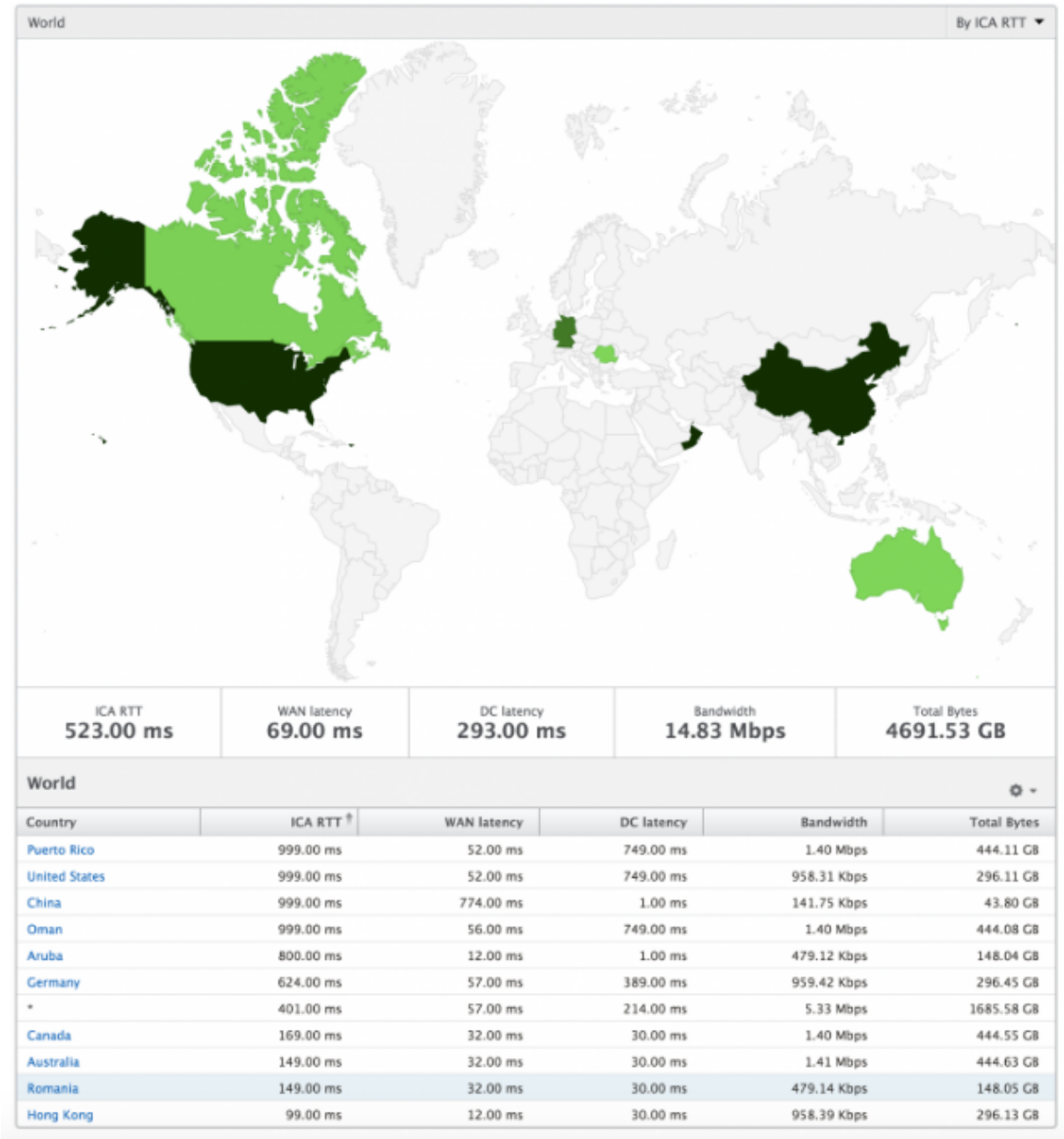


“**World**”（世界）视图

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 NetScaler 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 Insight 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

February 6, 2024

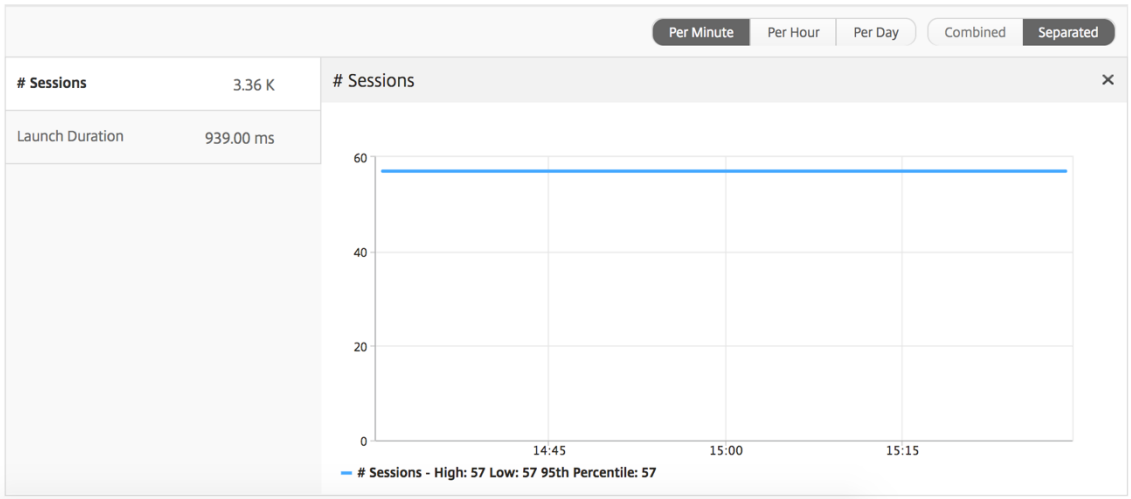
许可证视图提供了有关 NetScaler Gateway 许可证信息的详细信息。

要导航到许可证视图，请执行以下操作：

1. 导航到网关 **> HDX Insight >** 许可证。

折线图

指标	说明
正在使用的许可证	在选定的时间轴内使用的 NetScaler 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 NetScaler 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

February 6, 2024

如果 HDX Insight 解决方案未按预期运行，则问题可能出在以下情况之一。有关故障排除，请参阅相应部分中的清单。

- HDX Insight 配置。
- NetScaler 和 NetScaler ADM 之间的连接。

- 在 NetScaler 中生成 HDX/ICA 流量的记录。
- NetScaler ADM 中的记录总量。

HDX Insight 配置清单

- 确保在 NetScaler 中启用了 AppFlow 功能。有关详细信息，请参阅 启用 AppFlow。
- 检查 NetScaler 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 ICA_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
  ```

- 对于单跃点/Access Gateway 或双跃点部署，请确保 HDX Insight AppFlow 策略绑定到 VPN 虚拟服务器，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 或双跃点部署启用 NetScaler 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。
- 选中双跃点 NetScaler 中已启用“连接链接”。有关详细信息，请参阅 配置 NetScaler 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“enableSRonHAFailover”是否已启用。有关详细信息，请参阅 NetScaler 高可用性对上的会话可靠性。

NetScaler 与 NetScaler ADM 之间的连接检查表

- 检查 NetScaler 中的 AppFlow 收集器状态。有关详细信息，请参阅 如何检查 NetScaler 和 AppFlow Collector 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“设置”**>**“**AppFlow**”**>**“策略”以查看 AppFlow 策略命中。

- 验证任何阻止 AppFlow 端口 4739 或 5557 的防火墙。

在 **NetScaler** 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：跳过解析 **ICA** 连接 **-** 此主机不支持 **HDX Insight**

  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 流量时出现问题

  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：无效过渡：**NS_ICA_ST_FLOW_INIT/NS_ICA_EVT_INVALID -> NS_ICA_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 **EUEM ICA RTT**

  原因：无法解析最终用户体验监视通道数据

  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。确保您使用的是受支持的 Citrix Workspace 应用程序版本。

- 日志：通道标头无效

  原因：无法识别通道头

  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

  如果您看到以下任何跳过代码值，则会跳过解析 Insight 详细信息。

  > 跳过代码 0 表示记录已成功从 NetScaler 导出。

跳过代码	错误消息	错误原因
100	NS_ICA_ERR_NULL_FRAG	处理 ICA 碎片时出错，可能是内存状况造成的

跳过代码	错误消息	错误原因
101	NS_ICA_ERR_INVALID_HS_CMD	收到的握手命令无效
102	NS_ICA_ERR_REDUC_PARAM_CNT	为 V3 扩展器初始化指定的参数无效
103	NS_ICA_ERR_REDUC_INIT	无法正确初始化 V3 扩展器
104	NS_ICA_ERR_REDUC_PARAM_BYTES	字节不足，无法将编码器分配给通道
105	NS_ICA_ERR_INVALID_CHANNEL	ICA 通道号无效
106	NS_ICA_ERR_INVALID_DECODER	为通道指定的解码器无效
107	NS_ICA_ERR_INVALID_TW_PARAM	在 Thinwire 通道上指定的参数计数无效
108	NS_ICA_ERR_INVALID_TW_DECODER	Thinwire 通道的解码器无效
109	NS_ICA_ERR_REDUC_NO_DECODER	没有为通道定义解码器
110	NS_ICA_ERR_REDUC_V3_EXPAND_ER	无法扩展通道数据
111	NS_ICA_ERR_REDUC_BYTES_V3_OOR	扩展器错误：消耗的字节多于可用字节
112	NS_ICA_ERR_REDUC_BYTES_OOR	错误：未压缩的数据溢出
113	NS_ICA_ERR_REDUC_INVALID_CMD	未定义的扩展器命令
114	NS_ICA_ERR_CGP_FILL_HOLE	处理拆分 CGP 帧时出错
115	NS_ICA_ERR_MEM_NSB_ALLOC	NSB 分配错误—由于内存不足
116	NS_ICA_ERR_MEM_REDUC_CTX_ALLOC	扩展器上下文的内存分配错误
117	NS_ICA_ERR_ICA_OLD_SERVER	旧服务器，不支持功能块
118	NS_ICA_ERR_PIR_MANY_FRAG	数据包初始化请求被分段，无法处理
119	NS_ICA_ERR_INIT_ICA_CAPS	ICA 功能初始化错误
120	NS_ICA_ERR_NO_MSI_SUPPORT	主机不支持 MSI 功能。表示低于 6.5 的 XenApp 版本或低于 5.0 的 XenDesktop 版本
121	NS_ICA_ERR_CGP_INVALID_CMD	遇到无效的 CGP 命令
122	NS_ICA_ERR_INSUFFICENT_CHANNEL_BYTES	通道上的字节数不足
123	NS_ICA_ERR_CHANNEL_DATA	EUEM、CONTROL 或 SEAMLESS 通道上的数据不正确
124	NS_ICA_ERR_INVALID_PURE_CMD	处理 PURE ICA 通道数据时收到无效命令
125	NS_ICA_ERR_INVALID_PURE_LENGTH	处理 PURE ICA 通道数据时遇到无效长度

跳过代码	错误消息	错误原因
126	NS_ICA_ERR_INVALID_PURE_LEN	处理 PURE ICA 通道数据时遇到无效长度
127	NS_ICA_ERR_INVALID_CLNT_DATA	从客户端接收到的数据长度无效
128	NS_ICA_ERR_MSI_GUID_SZ	MSI GUID 大小错误
129	NS_ICA_ERR_INVALID_CHANNEL_HEADER	检测到无效的通道头
130	NS_ICA_ERR_CGP_PARSE_RECONNECT	从客户端重新连接的会话失败
131	NS_ICA_ERR_DISABLE_SR_NON_NSPROTOCOL	禁用 SR，非 NSPROTOCONNECT
132	NS_ICA_ERR_REDUC_NOT_V3	不支持的 ICA Reducer 版本
133	NS_ICA_ERR_HS_COMPRESSION_DISABLED	已禁用压缩，主机不支持压缩
134	NS_ICA_ERR_IDENT_PROTO	无法识别 ICA 或 CGP 协议，工作区不正确
135	NS_ICA_ERR_INVALID_SIGNATURE	ICA 签名或幻字符串不正确
136	NS_ICA_ERR_PARSE_RAW	解析 ICA 握手数据包时出错
137	NS_ICA_ERR_INCOMPLETE_PKT	握手时收到的数据包不完整
138	NS_ICA_ERR_ICAFRAME_TOO_LARGE	ICA 帧太大，超过 1460 字节
139	NS_ICA_ERR_FORWARD	转发 ICA 数据时出错
140	NS_ICA_ERR_MAX_HOLES	无法处理 CGP 命令，因为它被拆分超出了支持的限制
141	NS_ICA_ERR_ASSEMBLE_FRAME	无法正确重组 ICA 框架
142	NS_ICA_ERR_UNSUPPORTED_RECEIVER_VERSION	已跳过此工作站（客户端）的 ICA 解析，因为它不在允许列表中
143	NS_ICA_ERR_LOOKUP_RECONNECT_ID	无法检测客户端重新连接 Cookie 的解析状态
144	NS_ICA_ERR_SYNCUP_RECONNECT_ID	客户端重新连接后检测到的重新连接 Cookie 长度无效
145	NS_ICA_ERR_INVALID_RECONNECT_ID	客户端重新连接 cookie 错过了所需的约束
146	NS_ICA_ERR_INVALID_CLIENT_VERSION	从客户端收到的 Workspace 版本字符串无效
147	NS_ICA_ERR_UNKNOWN_CLIENT_PRODUCT_ID	从客户端收到的产品编码无效
148	NS_ICA_ERR_V3_HDR_CORRUPT_LEN	重组后的通道长度无效
149	NS_ICA_ERR_SPECIAL_THINWIRE	解压缩错误

跳过代码	错误消息	错误原因
150	NS_ICA_ERR_SEAMLESS_INSUFFBYTE	遇到无法执行无缝命令的字节不足的问题
151	NS_ICA_ERR_EUEM_INSUFFBYTE	遇到 EUEM 命令的字节不足
152	NS_ICA_ERR_SEAMLESS_INVALID_EVENT	无缝通道解析的事件无效
153	NS_ICA_ERR_CTRL_INVALID_EVENT	CTRL 通道解析的事件无效
154	NS_ICA_ERR_EUEM_INVALID_EVENT	EUEM 通道解析的事件无效
155	NS_ICA_ERR_USB_INVALID_EVENT	USB 通道解析的事件无效
156	NS_ICA_ERR_PURE_INVALID_EVENT	PT 通道解析的事件无效
157	NS_ICA_ERR_VCP_INVALID_EVENT	虚拟通道解析的事件无效
158	NS_ICA_ERR_ICAP_INVALID_EVENT	ICA 数据解析的事件无效
159	NS_ICA_ERR_CGPP_INVALID_EVENT	CGP 数据解析的事件无效
160	NS_ICA_ERR_BASICCRYPT_INVALIDSTATE	基本加密中 crypt 命令的状态无效
161	NS_ICA_ERR_BASICCRYPT_INVALIDCRYPTCMD	基本加密中的 crypt 命令无效
162	NS_ICA_ERR_ADVCRYPT_INVALIDSTATE	RC5 加密中 crypt 命令的状态无效
163	NS_ICA_ERR_ADVCRYPT_INVALIDCRYPTCMD	RC5 加密中的 crypt 命令无效
164	NS_ICA_ERR_ADVCRYPT_ENC	RC5 加密/解密时出错
165	NS_ICA_ERR_ADVCRYPT_DEC	RC5 加密/解密时出错
166	NS_ICA_ERR_SERVER_NOT_REDUCER_V3	VDA 不支持 Reducer 版本 3
167	NS_ICA_ERR_CLIENT_NOT_REDUCER_V3	Workspace 不支持 Reducer 版本 3
168	NS_ICA_ERR_ICAP_INSUFFBYTE	ICA 握手中出现意外的字节数
169	NS_ICA_ERR_HIGHER_RECONSEQ	对等发布重新连接的 CGP 恢复序列号较高
170	NS_ICA_ERR_DESCSRINFO_ABSENT	重新连接后无法恢复 ICA 解析状态
171	NS_ICA_ERR_NSAP_PARSING	解析 Insight 通道数据时出错
172	NS_ICA_ERR_NSAP_APP	从 Insight 渠道数据解析应用详细信息时出错
173	NS_ICA_ERR_NSAP_ACR	解析 Insight 通道数据中的 ACR 详细信息时出错
174	NS_ICA_ERR_NSAP_SESSION_END	从 Insight 通道数据解析会话结束详细信息时出错

跳过代码	错误消息	错误原因
175	NS_ICA_ERR_NON_NSAP_SN	由于缺少 Insight 渠道支持，跳过了服务节点上的 ICA 解析
176	NS_ICA_ERR_NON_NSAP_CLIENT	客户端不支持 NSAP
177	NS_ICA_ERR_NON_NSAP_SERVER	VDA 不支持 NSAP
178	NS_ICA_ERR_NSAP_NEG_FAIL	NSAP 数据协商时出错
179	NS_ICA_ERR_SN_RECONNECT_TKT	获取服务节点中的票证时出错重新连接服务节点
180	NS_ICA_ERR_SN_HIGHER_RECONNSEQ	从服务节点中接收更高的重新连接序列号时出错
181	NS_ICA_ERR_DISABLE_HDXINSIGHT_NONSAP	对非 NSAP 连接禁用 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 [0
x8820220228], 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 [0
x8820220008], Track Flags [0x1600010c040], Skip Code [171]"
```

错误计数器

ICA 解析时会捕获各种计数器。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/错误/诊断）
hdx_tot_ica_conn	指示 NS 检测到的纯 ICA 连接的总数。每当检测到基于客户端 PCB 上的 ICA 签名的 ICA 连接时，就会递增。	统计信息
hdx_tot_cgp_conn	指示 NS 检测到的 CGP 连接总数（会话可靠性开启）。每当检测到基于客户端 PCB 上的 CGP 签名的 CGP 连接时，就会递增。	统计信息
hdx_dbg_tot_udt_conn	表示 NS 检测到的 UDP ICA 连接总数	统计信息
hdx_dbg_tot_nsap_conn	表示 NS 检测到的支持 NSAP 的连接总数	统计信息
hdx_tot_skip_conn	表示由于 ICA 或 CGP 签名无效，解析器跳过了多少个 ICA 连接。	统计信息
hdx_dbg_active_conn	此时处于活动状态的 EDT/CGP/ICA 连接总数。	统计信息
hdx_dbg_active_nsap_conn	当时活跃的 EDT/CGP/ICA NSAP 连接总数。	统计信息
hdx_dbg_skip_appflow_disabled	由于禁用 AppFlow 而将 AppFlow 从会话中分离的实例总数	统计/诊断
hdx_dbg_transparent_user	透明用户访问的总数	统计/诊断
hdx_dbg_ag_user	Access Gateway 用户访问总数	统计/诊断
hdx_dbg_lan_user	局域网用户模式访问总数	统计/诊断
hdx_basic_enc	指示使用基本加密的 ICA 连接数	统计/诊断
hdx_advanced_enc	表示使用基于 RC5 的高级加密的 ICA 连接数	统计/诊断
hdx_dbg_reconnected_session	来自客户端的未出现任何 NetScaler 错误的重新连接请求总数	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
hdx_euem_available	指示具有“最终用户体验监视”通道可用的连接数。需要最终用户体验监视通道来收集 ICA RTT 等统计信息。	统计/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
hdx_err_skip_no_msi	XA/XD 服务器缺少 MSI 功能。这表示服务器版本较旧，而 HDX Insight 会跳过此连接。	错误

HDX 计数器名称	用途	类别（统计/错误/诊断）
hdx_err_skip_old_server	不支持的旧服务器版本	错误
高清错误白名单	客户端工作区不在允许列表中，HDX Insight 跳过此连接	错误
hdx_sm_ica_cam_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CAM_CHANNEL 总数	诊断
hdx_sm_ica_usb_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_USB_CHANNEL 总数	诊断
hdx_sm_ica_clip_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CLIP_CHANNEL 总数	诊断
hdx_sm_ica_ccm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CCM_CHANNEL 总数	诊断
hdx_sm_ica_cdm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CDM_CHANNEL 总数	诊断
hdx_sm_ica_com1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM1_CHANNEL 总数	诊断
hdx_sm_ica_com2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_COM2_CHANNEL 总数	诊断
hdx_sm_ica_cpm_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_CPM_CHANNEL 总数	诊断
hdx_sm_ica_lpt1_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT1_CHANNEL 总数	诊断
hdx_sm_ica_lpt2_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_LPT2_CHANNEL 总数	诊断
dx_dbg_sm_ica_msi_disabled	通过 SmartAccess 策略禁用 MSI 的案例总数	诊断
hdx_sm_ica_file_channel_disabled	通过 SmartAccess 策略禁用的 NS_ICA_FILE_CHANNEL 总数	诊断
hdx_dbg_usb_accept_device	接受的 USB 设备总数	诊断
hdx_dbg_usb_reject_device	拒绝的 USB 设备总数	诊断
hdx_dbg_usb_reset_endpoint	重置的 USB 端点总数	诊断
hdx_dbg_usb_reset_device	重置的 USB 设备总数	诊断
hdx_dbg_usb_stop_device	已停止的 USB 设备总数	诊断
hdx_dbg_usb_stop_device_response	来自已停止的 USB 设备的响应总数	诊断
hdx_dbg_usb_device_gone	消失的 USB 设备总数	诊断

hdx_dbg_usb_device_stopped	已停止的 USB 设备总数	诊断

nstrace validation

检查 CFLOW 协议以查看 NetScaler 中的所有 AppFlow 记录。

NetScaler 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 NetScaler ADM 正在接收 AppFlow 记录。
- 确认已将 NetScaler 实例添加到 NetScaler ADM 中。
- 验证 NetScaler Gateway/VPN 虚拟服务器是否已在 NetScaler ADM 中获得许可。
- 确保为双跃点启用了多跳参数设置。
- 确保 NetScaler Gateway 在双跃点部署中已获得第二跃点许可。

在联系 Citrix 技术支持之前

要快速解决问题，请确保在联系 Citrix 技术支持之前已掌握以下信息：

- 部署和网络拓扑的详细信息。
- NetScaler 和 NetScaler ADM 版本。
- Citrix Virtual Apps and Desktops 服务器版本。
- 客户端 Workspace 版本。
- 发生问题时的活动 ICA 会话数。
- 通过在 NetScaler `show techsupport` 命令提示符下运行命令捕获的技术支持包。
- 为 NetScaler ADM 捕获的技术支持包。
- 在所有 NetScaler 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 上的已知问题，请参阅 ADC 发行说明。

基础结构分析

February 6, 2024

网络管理员的一个关键目标是监视 NetScaler 实例。ADC 实例提供了有关通过它访问的应用程序和桌面的使用情况和性能的有趣见解。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
- 不存在资源消耗、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

基础设施分析功能通过关联多个数据源并将其量化为定义实例运行状况的可测量分数来简化数据分析过程。借助此功能，管理员只需一个接触点即可了解是否存在问题、问题的根源以及他们可以采取的可能的补救措施。

基础架构分析

NetScaler Application Delivery Management (ADM) 基础架构分析功能整理从 NetScaler 实例收集的所有数据，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形式汇总。基础结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。此可视化还可以帮助您确定为防止问题及其再次出现而必须执行的操作。

实例得分

实例得分表示 ADC 实例的运行状况。得分为 100 表示实例运行状况良好，没有任何问题。实例得分可捕捉实例上不同级别的潜在问题。它是实例运行状况的可量化衡量标准，多个“运行状况指标”为得分做出了贡献。

运行状况指标 是实例得分的基石，在实例得分中，根据在该时间窗口内检测到的所有指标，定期计算预定义的“监视周期”的得分。目前，基础设施分析根据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）。

- 系统资源指示器
- 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 NetScaler 实例上可能出现并由 NetScaler ADM 监视的关键系统资源问题。

  - **CPU** 使用率高。在 NetScaler 实例中，CPU 使用率已超过较高的阈值。
  - 内存使用率高。在 NetScaler 实例中，内存使用量已超过较高的阈值。
  - 磁盘使用率高。在 NetScaler 实例中，磁盘使用量已超过较高的阈值。
  - 磁盘错误。安装了 ADC 实例的虚拟机管理程序上的硬盘 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** 卡出现故障。安装在实例上的 SSL 卡出现故障。
  - 闪存错误。在 NetScaler 实例上看到紧凑型闪存错误。
  - 网卡丢弃。NIC 卡丢弃的数据包已跨越 NetScaler 实例中较高的阈值。

有关这些系统资源错误的更多信息，请参阅 实例控制面板。

- 关键事件指标

  以下严重事件由 ADM 事件管理功能下配置为严重性的事件识别。

  - **HA** 同步失败。在辅助服务器上，处于高可用性状态的 ADC 实例之间的配置同步失败。
  - 哈哈没有心跳。一对处于高可用性的 ADC 实例中的主服务器无法接收来自辅助服务器的心跳。
  - **HA** 次要状态不正确。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”。
  - **HA** 版本不匹配。安装在一对 ADC 实例上的高可用性的 ADC 软件映像版本不匹配。
  - 群集同步失败。群集模式下 ADC 实例之间的配置同步失败。
  - 群集版本不匹配。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。向群集中的所有实例传播配置已失败。

    > 注意
    >
    > 您可以通过更改事件的严重性级别来获得关键 SNMP 事件的列表。有关如何更改严重性级别的更多信息，请参阅 修改 NetScaler 实例上发生的事件的报告严重性。

  有关 NetScaler ADM 中事件的更多信息，请参阅事件。

- SSL 配置指示器

  - 不建议密钥强度。SSL 证书的密钥强度不符合 NetScaler 标准
  - 不建议发行人。Citrix 不建议使用 SSL 证书的颁发者。

  - **SSL** 证书已过期。安装在 ADC 实例中的 SSL 证书已过期。
  - **SSL** 证书到期。安装在 ADC 实例中的 SSL 证书将在接下来的一周内到期。
  - 不建议算法。安装在 ADC 实例中的 SSL 证书的签名算法不符合 NetScaler 标准。

有关 SSL 证书的更多信息，请参阅 SSL 控制板。

- 配置偏差指示器
  - 配置漂移模板。您使用要对某些实例进行审核的特定配置创建的审核模板存在配置偏差（未保存的更改）。
  - 配置偏移默认。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核报告以检查配置偏差的更多信息，请参阅 查看审核报告。

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。通过了解这些 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 基础结构 **>** 基础结构分析。
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分类：

- 达到吞吐量限制**-**达到 吞吐量限制后实例中丢弃的数据包数量。
- 已达到 **PE CPU** 限制**-**达到 PE CPU 限制后在所有 NIC 上丢弃的数据包数量。
- 已达到 **PPS** 限制**-**达到 PPS 限制后实例中丢弃的数据包数量。
- **SSL** 吞吐量速率限制 -达到 SSL 吞吐量限制的次数。
- **SSL TPS** 速率限制—达到 SSL TPS 限制的次数。

ADM 根据定义的容量阈值计算实例分数。

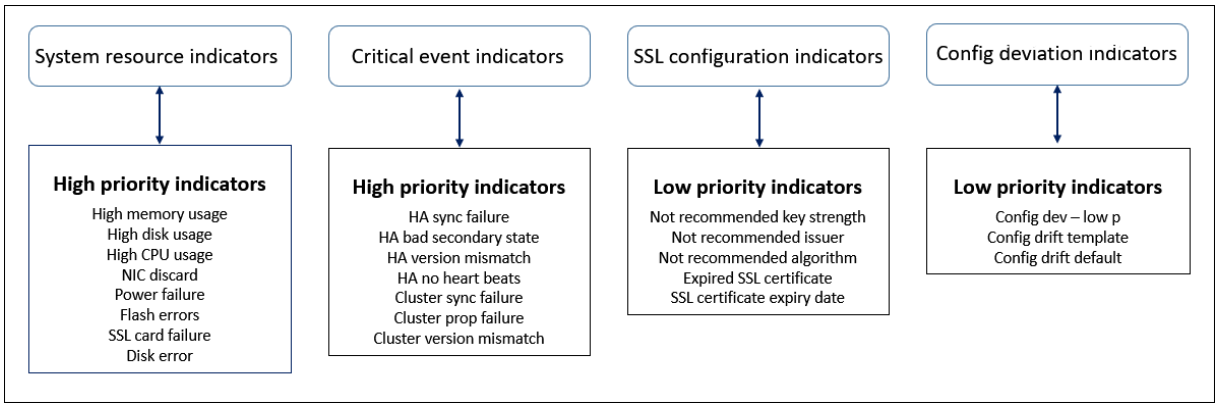
- 低阈值—1 个数据包丢弃或速率限制计数器增量
- 高阈值—10000 个数据包丢弃或速率限制计数器增量

因此，当 ADC 实例突破容量阈值时，实例分数会受到影响。

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。

运行状况指标的价值

这些指标根据以下价值分为高优先指标和低优先指标：



同一组指标中的运行状况指标具有不同的权重。一个指标可能比另一个指标更能降低实例得分。例如，高内存使用率比高磁盘使用率、高 CPU 使用率和 NIC 丢弃更能降低实例得分。如果在实例上检测到的指标数量较多，则实例得分越低。

指标的值是根据以下规则计算的。据说该指标可以通过以下三种方式之一进行检测：

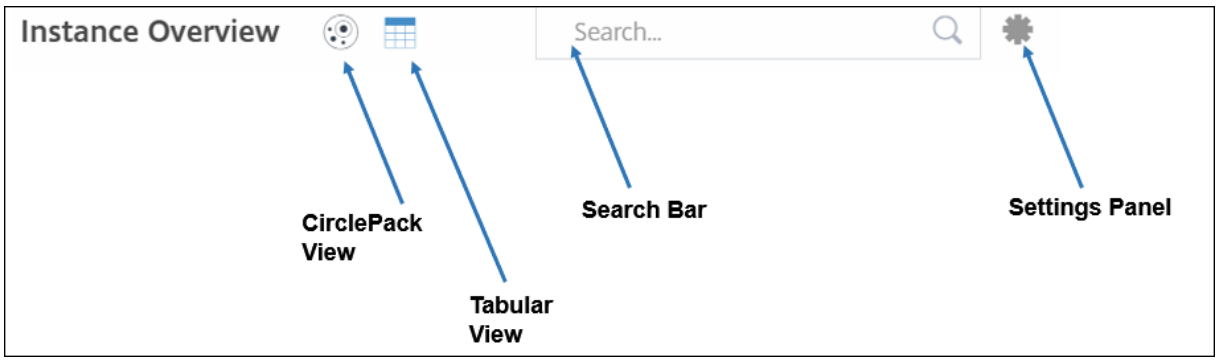
1. 基于某项活动。例如，每当实例出现电源故障时，系统资源指示器就会触发，该指示器会降低实例得分的值。当指标被清除时，惩罚被清除，实例得分增加。
2. 根据阈值突破情况而定。例如，当 NIC 卡丢弃数据包并且超过阈值级别时，会触发系统资源指示器。
3. 基于低阈值和高阈值突破情况。在这里，可以通过两种方式触发指标：
    - 当指标的值介于低阈值和高阈值之间时，将对实例得分征收部分罚款。
    - 当该值超过上限阈值时，将对实例得分征收全额罚款。
    - 如果该值降至低阈值以下，则不会对实例得分征收任何罚款。

例如，CPU 使用率是当使用率值超过低阈值时触发的系统资源指示器，也是在该值超过高阈值时触发的系统资源指标。

基础设施分析控制板

导航到 基础结构 **>** 基础结构分析。

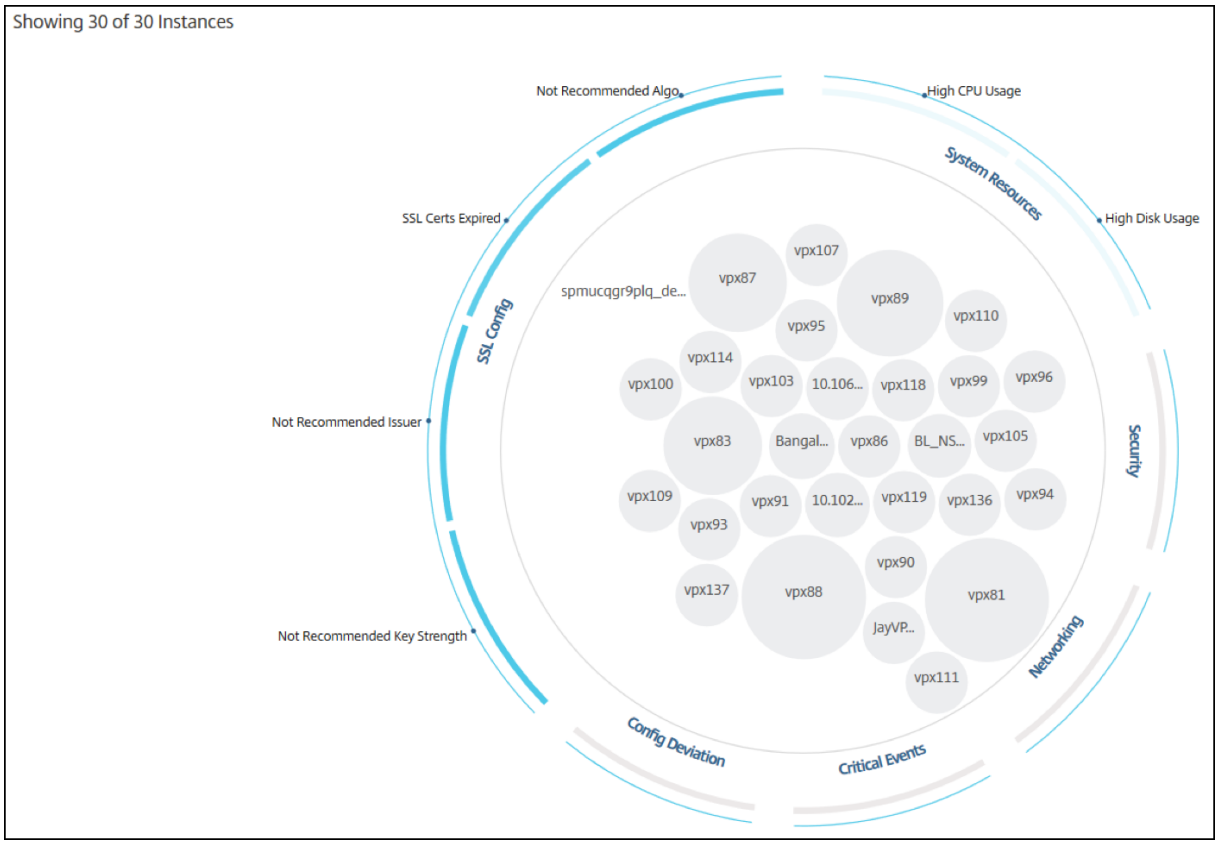
基础设施分析可以通过 圆形包 格式或 表格格 式查看。您可以在两种格式之间切换。



- 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，基础设施分析页面在页面的右侧显示摘要面板。
- 单击“设置”图标以显示“设置”面板。
- 在这两种视图格式中，摘要面板显示网络中所有实例的详细信息。

圆形包装视图

圆形包装图将实例组显示为组织严密的圆圈。它们通常显示层次结构，其中较小的实例组要么颜色与同一类别中的其他实例组相似，要么嵌套在较大的组中。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。



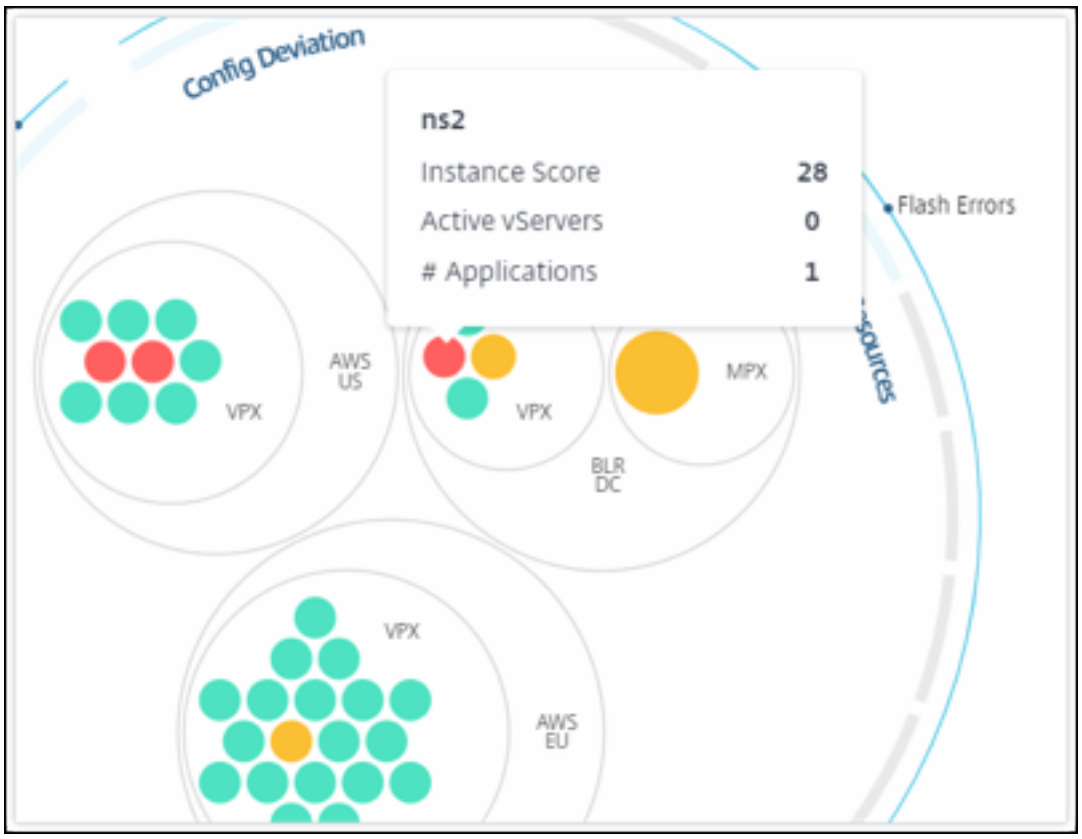
实例圆

颜色。每个实例在 Circle Pack 中都表示为彩色圆圈。圆圈的颜色表示该实例的运行状况。

- 绿色 -实例得分介于 100 和 80 之间。该实例运行正常。
- 黄色 -实例分数介于 80 到 50 之间；已注意到一些问题，需要审查。
- 红色 -实例得分低于 50。该实例处于关键阶段，因为在该实例上发现了多个问题。

大小。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，表示虚拟服务器的数量越多。

您可以将鼠标指针悬停在每个实例圆圈（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和在该实例上配置的应用程序数量。

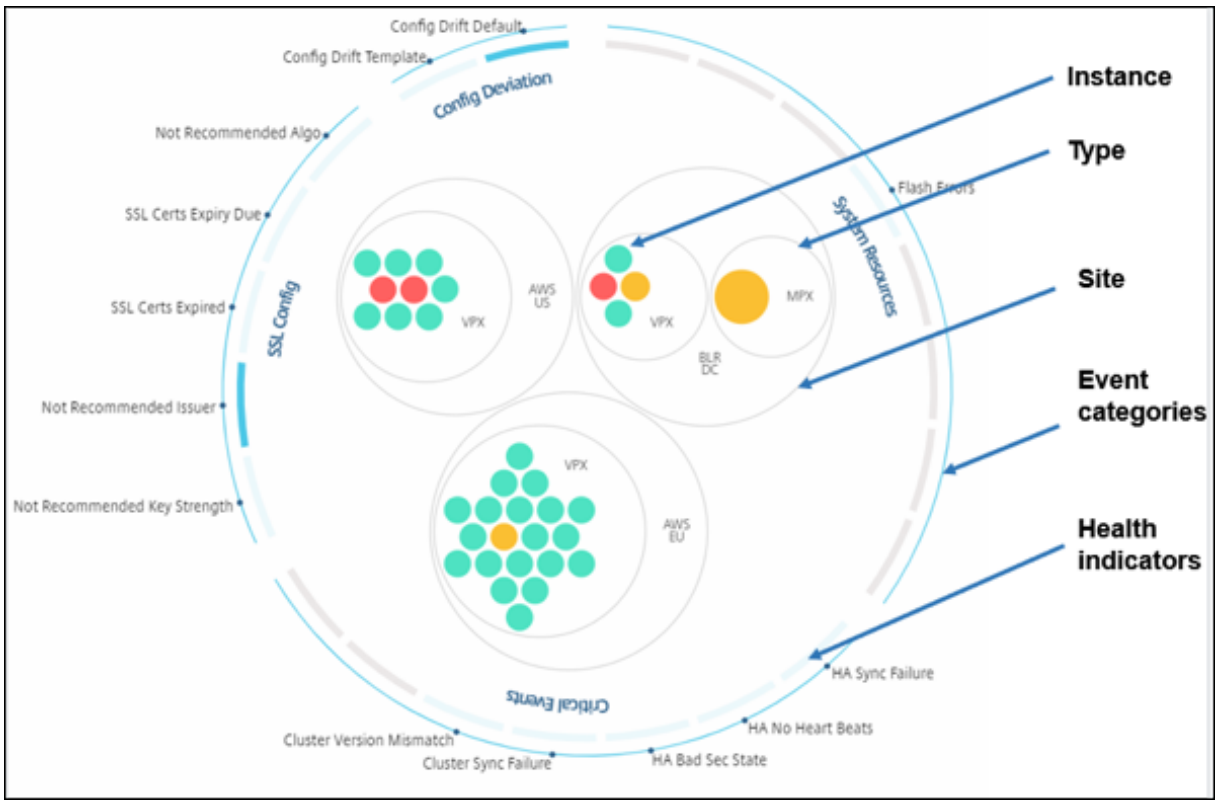


分组实例圆

Circle Pack 从一开始就由实例圈组成，这些圈子根据以下标准分组、嵌套或打包在另一个圈子中：

- 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
- 安装在实例上的 ADC 镜像版本

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。

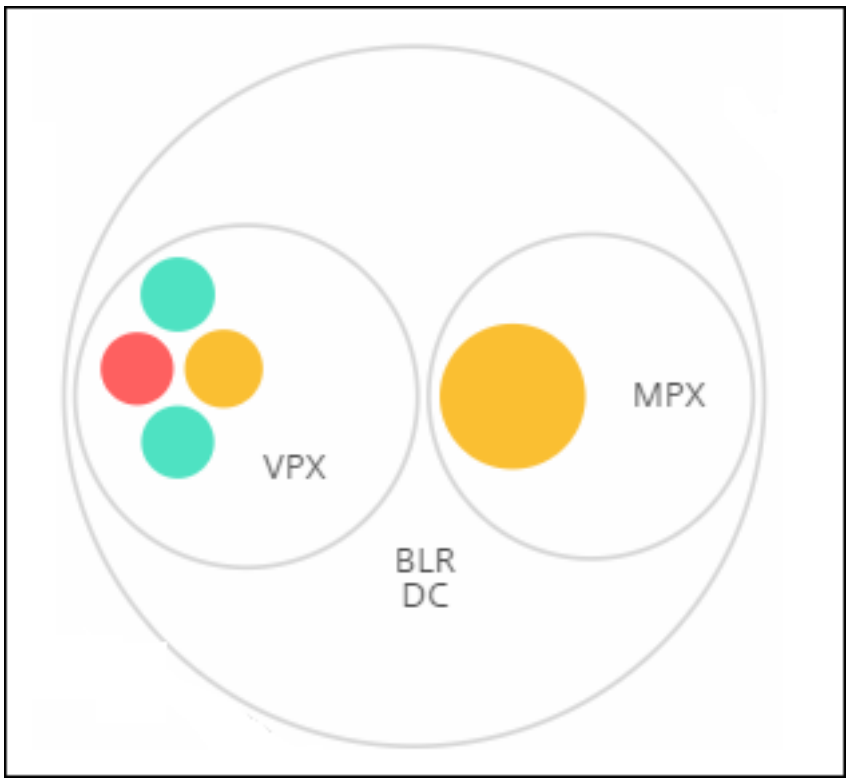


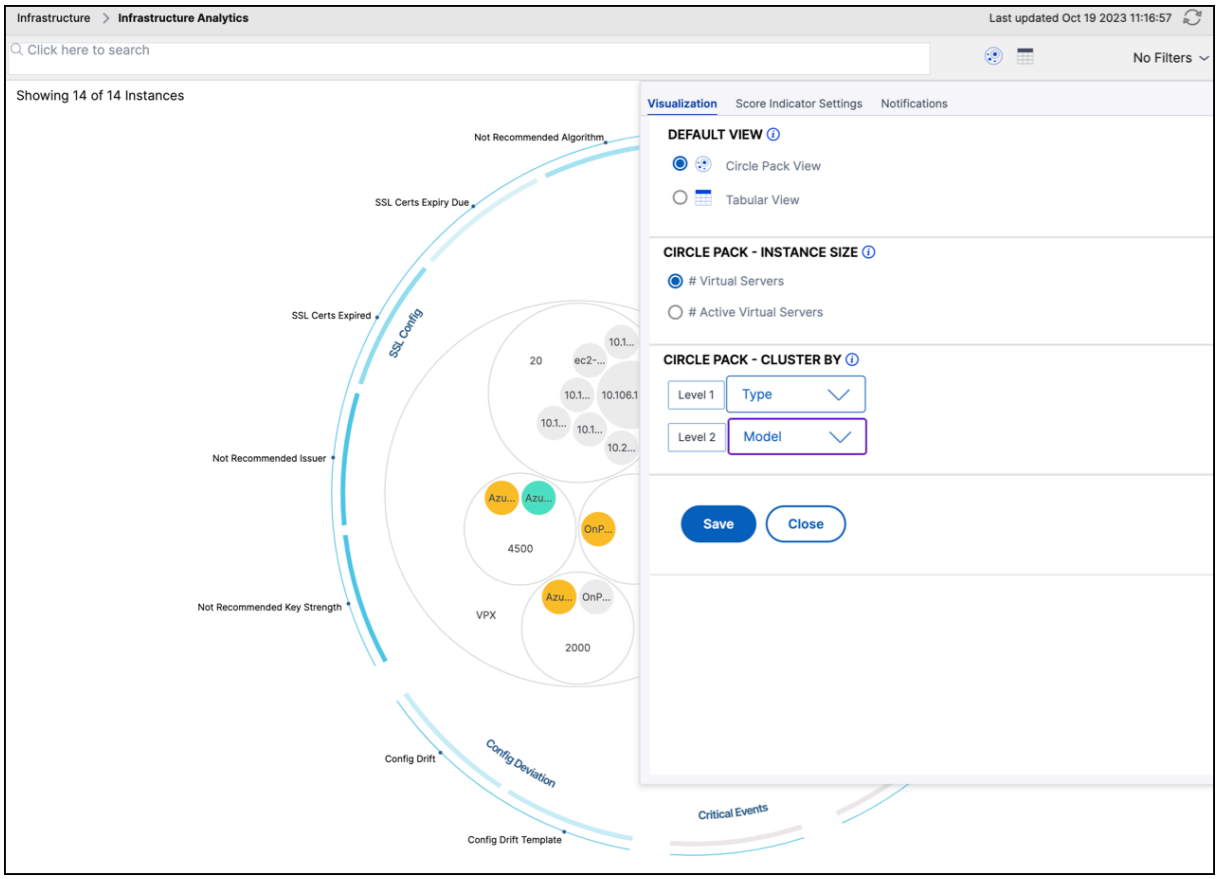
所有这些嵌套圆圈都由两个最外面的圆圈界限。外面的两个圆圈表示 NetScaler ADM 监视的四类事件（系统资源、关键事件、SSL 配置和配置偏差）以及相关的运行状况指标。

群集实例圈

NetScaler 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。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。您可以先按类型对 ADC 实例进行分组，然后按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。

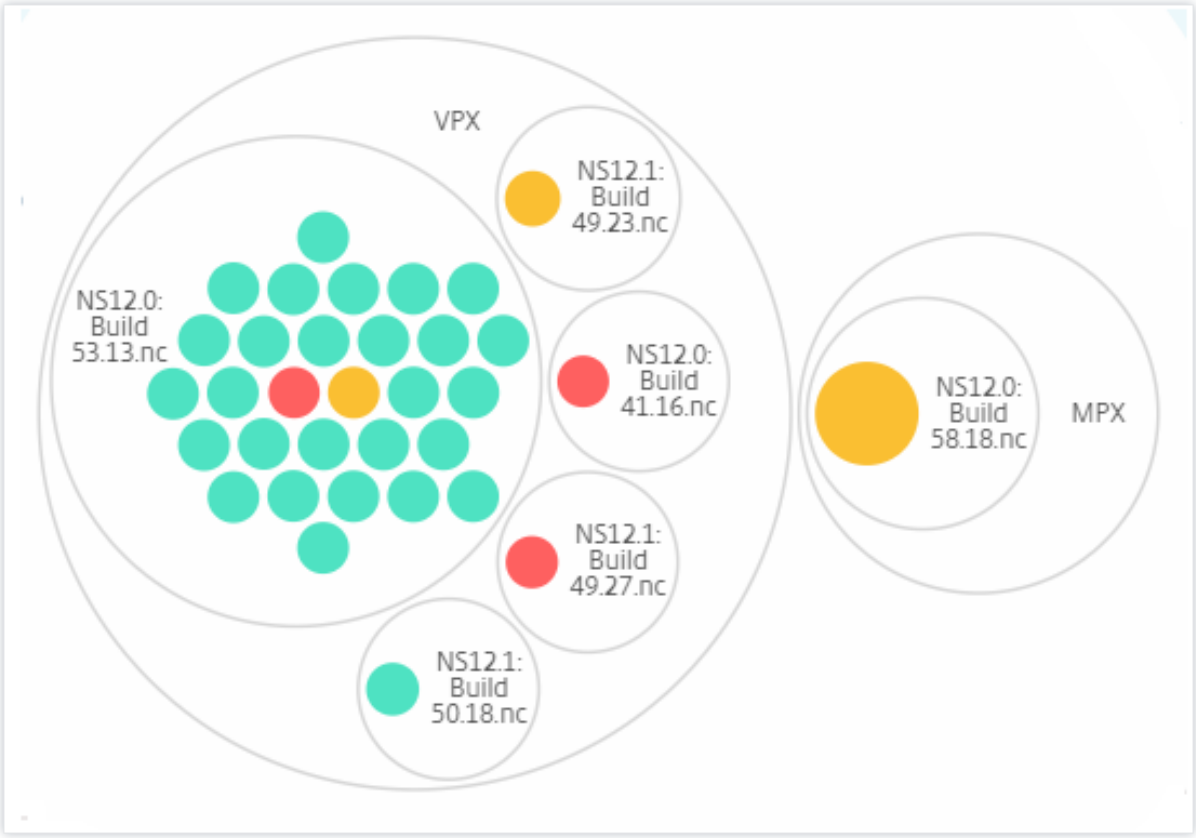




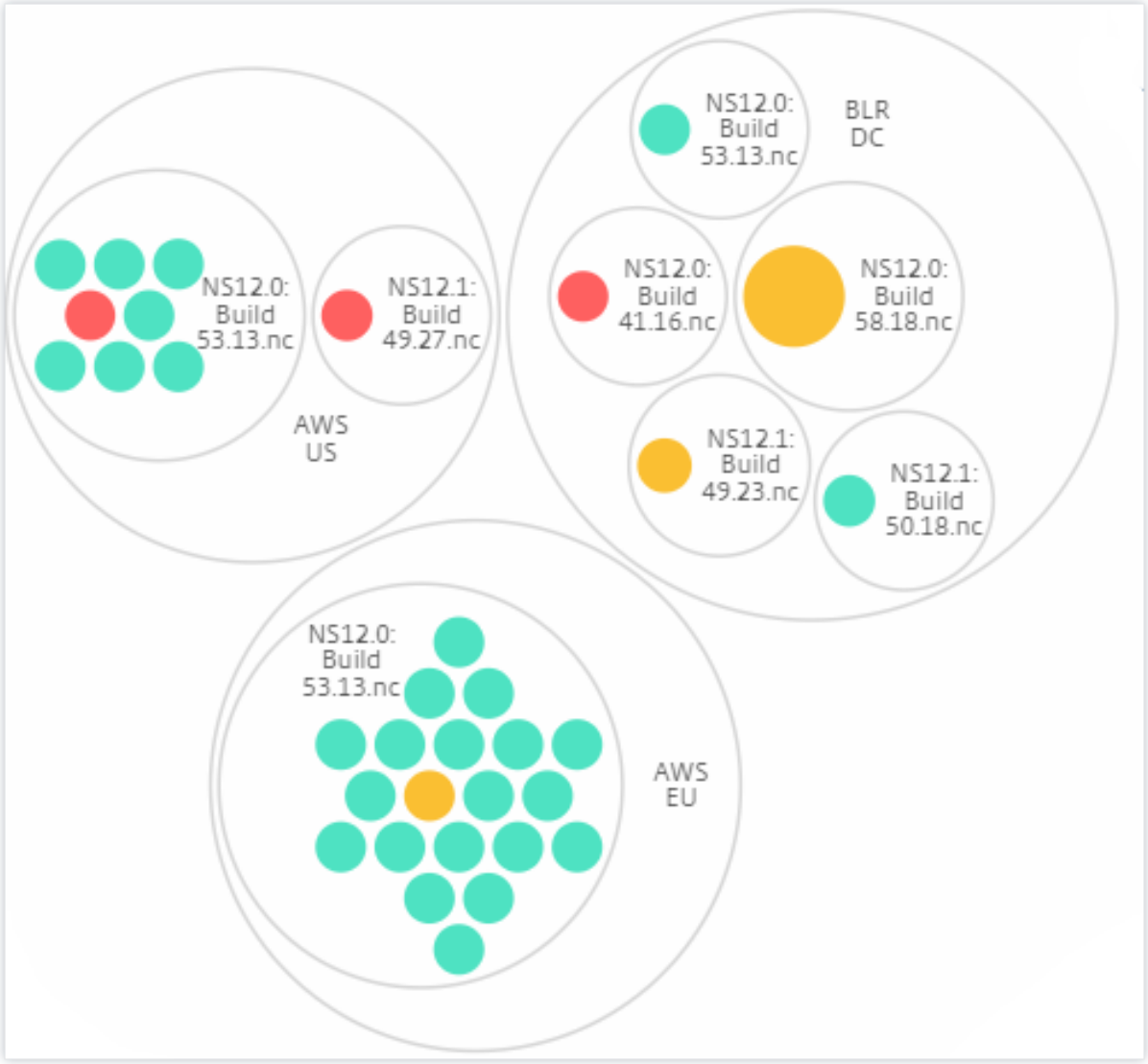
两级聚类的其他几个示例如下：

地点和型号：

类型和版本：

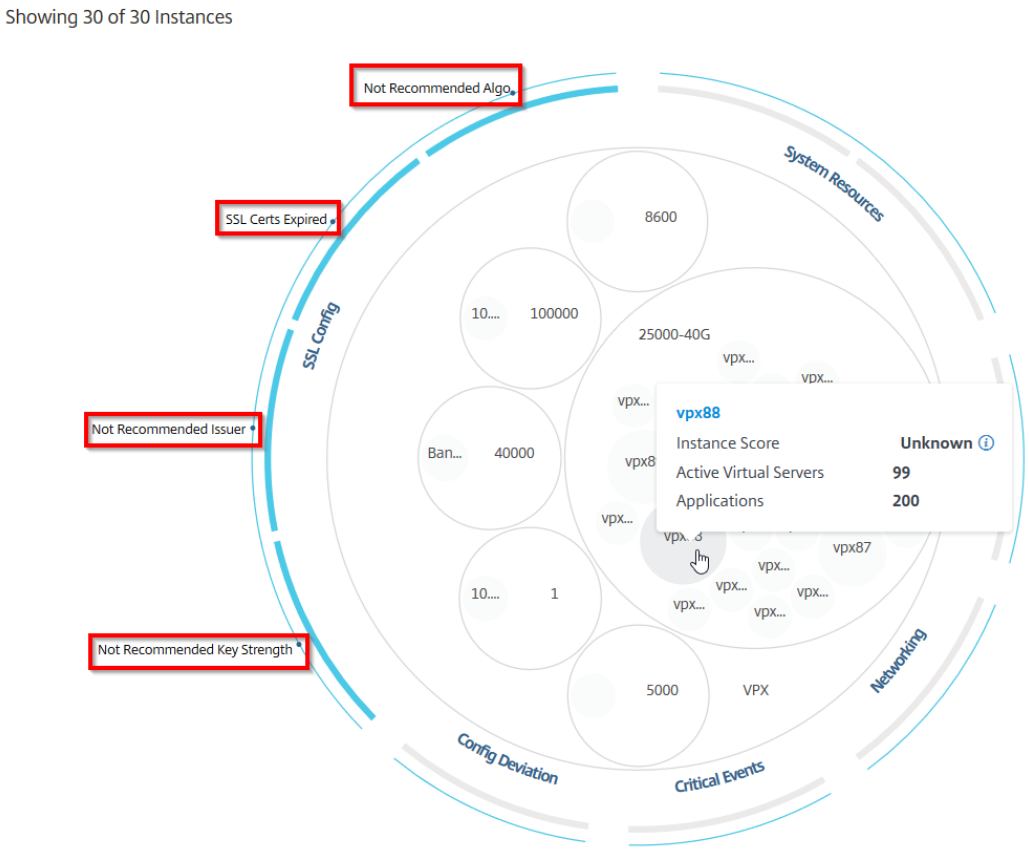


站点和版本：



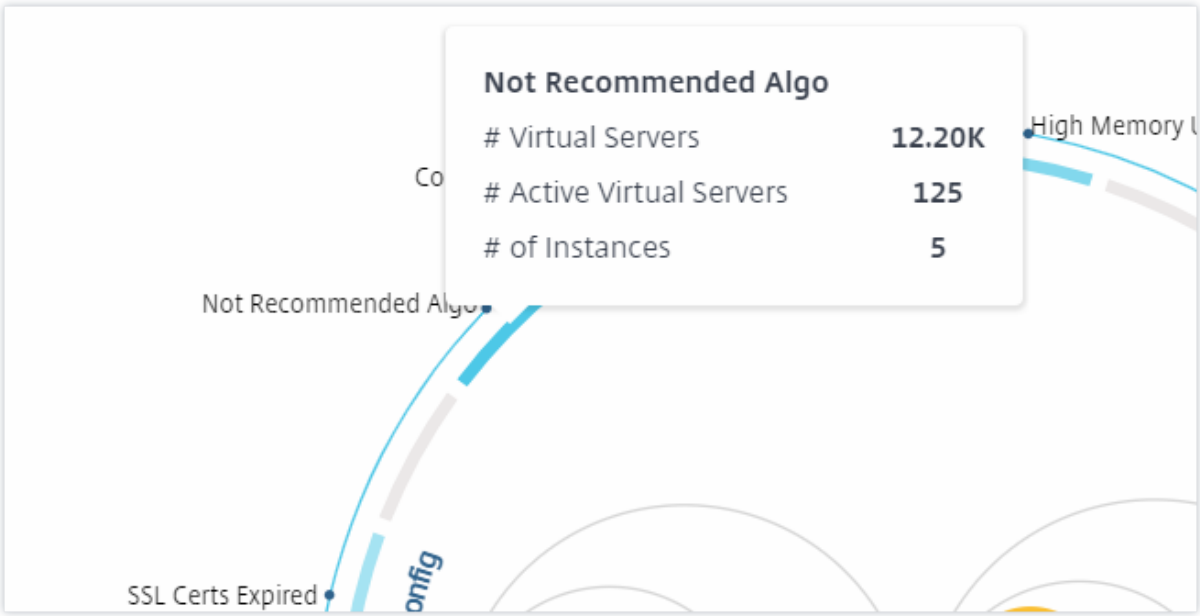
如何使用 **Circle Pack**

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，只有这些运行状况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。

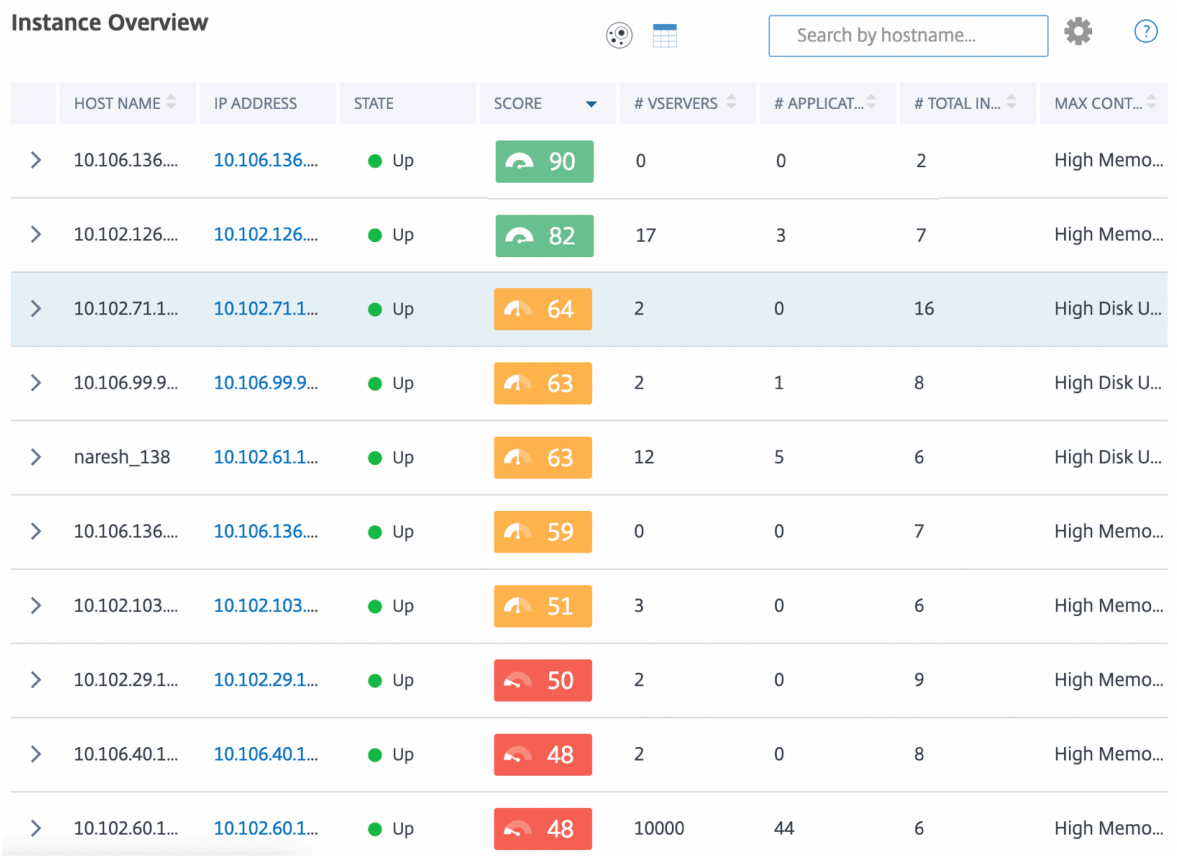


表格视图

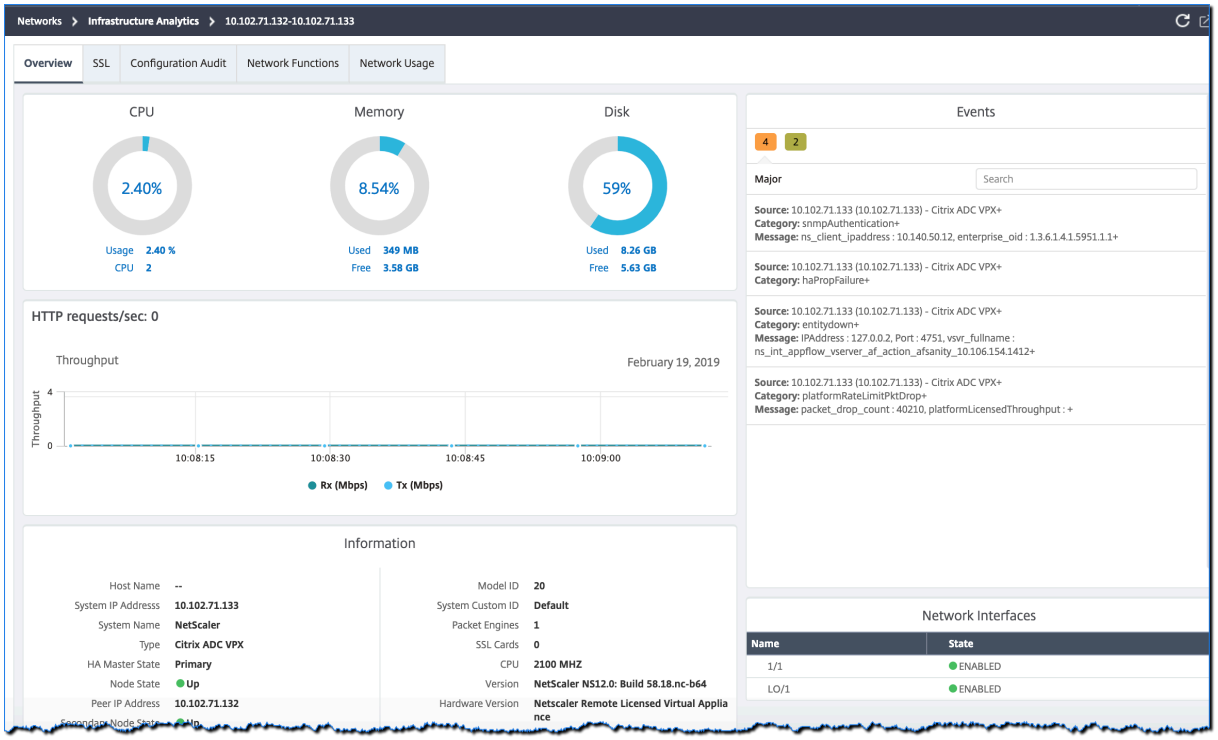
表格视图以表格格式显示实例和这些实例的详细信息。显示的详细信息如下所示：

- 实例的主机名
- 实例的 IP 地址
- 实例的状态
- 实例得分
- 在该实例上配置的虚拟服务器的数量
- 在该实例上配置的应用程序数量
- 风险指标总数
- 对降低实例分数有更大贡献的赛事

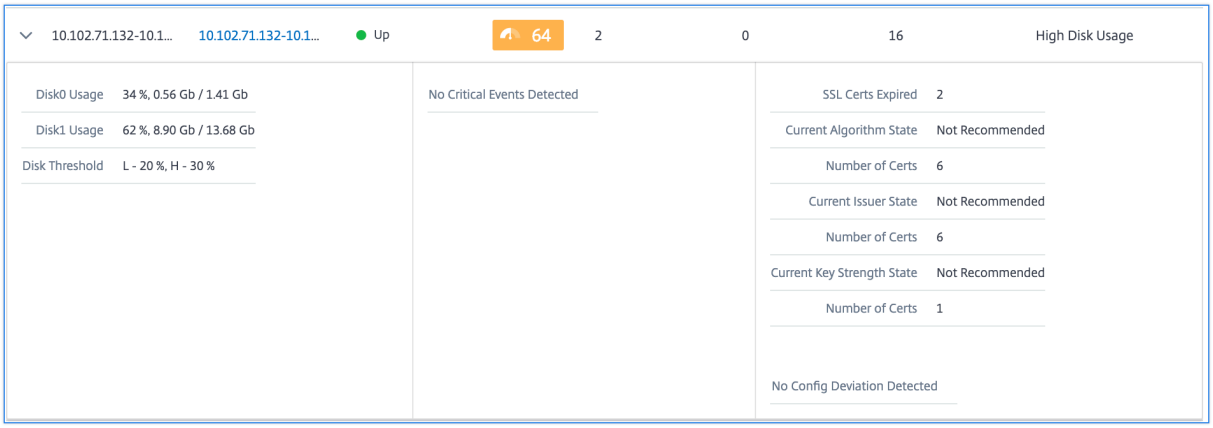
处于危急状态的实例排在表的顶部，其次是需要审查的实例，然后是更健康的实例。



在表格视图中单击实例 IP 地址，在控制板显示屏中查看该实例的更多详细信息。实例控制面板概述了实例，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，查看此实例上启用的功能和模式列表。



您也可以单击每行开头的箭头以展开该行以获取更多详细信息。



扩展后的表格行显示了实例上发生的所有类别的错误。在上面的示例中，您可以看到系统资源、SSL 配置和配置文件中存在偏差。但是该实例没有报告任何严重事件。

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、实例信息和流量概况。您在此面板中所做的更改会修改圆形包和表格视图格式的显示。以下各节更详细地描述了这些选项卡。以下部分中的示例可帮助您有效地使用不同的选择标准来分析实例报告的问题。

概述：

概述 选项卡允许您根据硬件错误、使用情况、过期证书和实例中可能出现的类似指标来监视实例。您可以在此处监视的指标如下：

- 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

以下示例说明了如何与概述面板交互以隔离那些报告错误的实例。

示例 **1**：查看处于审阅状态的实例：

选中“查 看”复选框以仅查看那些未报告严重错误但仍需要注意的实例。

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实例聚合数。直方图的分级分别为 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使用范围和该范围内的实例数。您也可以单击条形图以显示该范围内的所有实例。

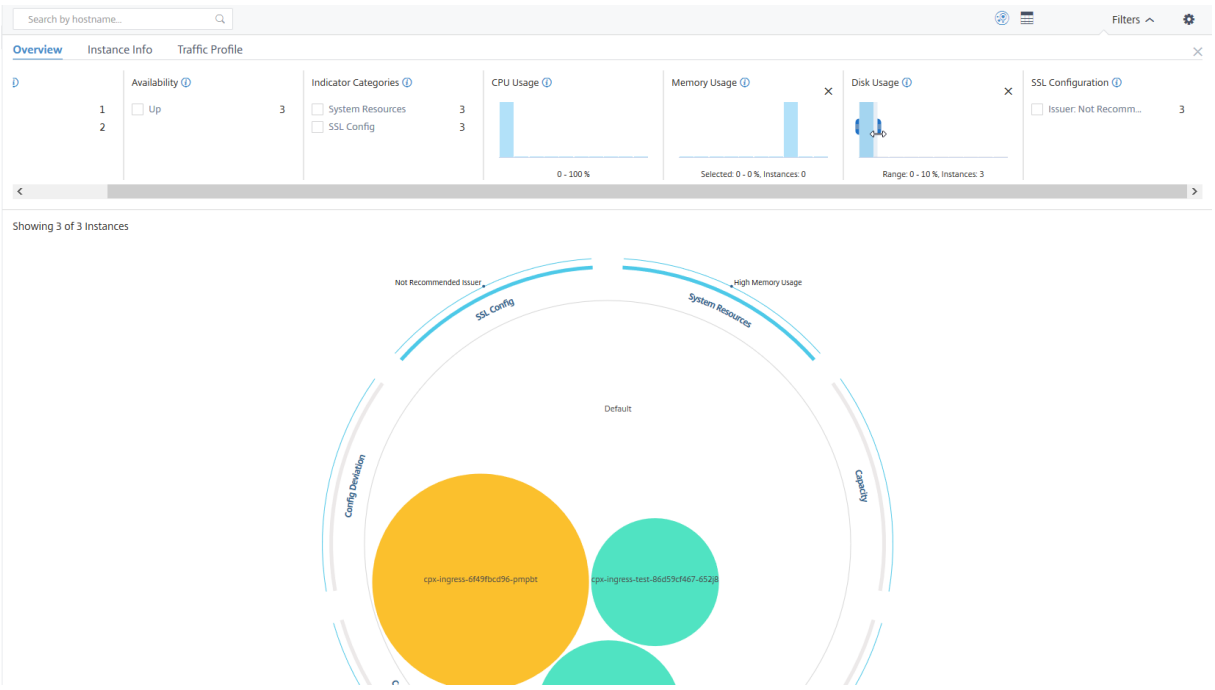
示例 **2**：查看消耗分配内存的 **10%** 到 **20%** 的实例：

在内存使用情况部分中，单击条形图。图例显示所选范围为 10-20%，该范围内有 29 个实例在运行。

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量磁盘空间的实例：

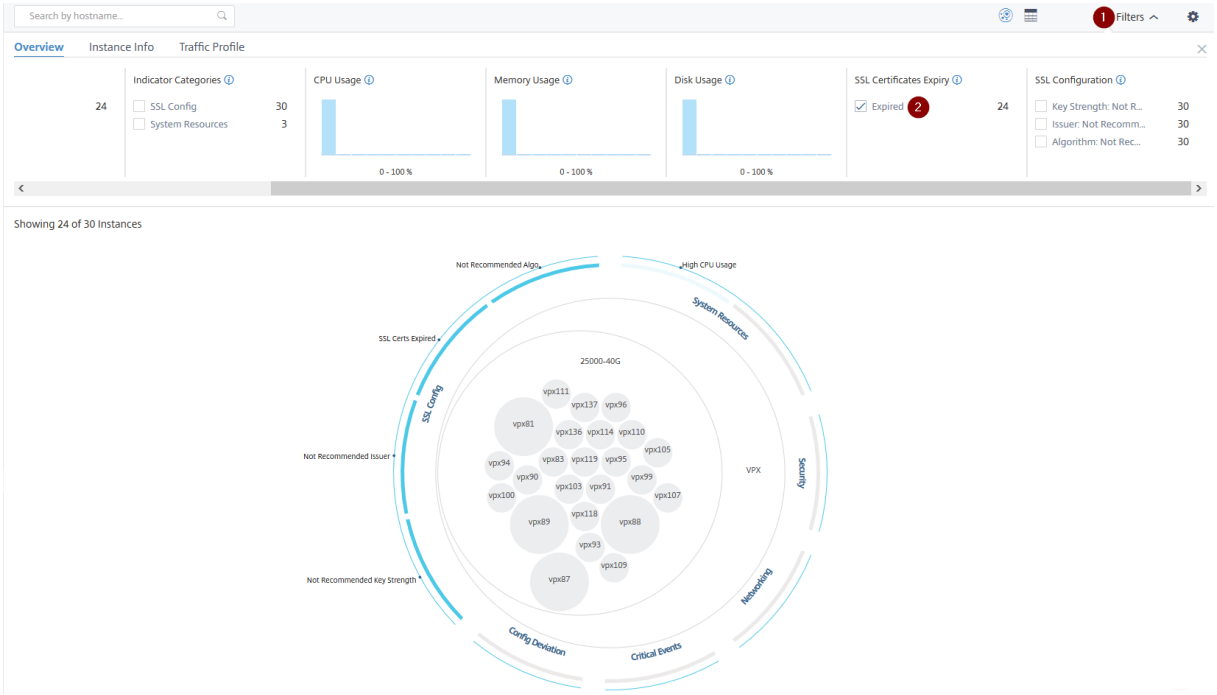
要查看占用磁盘空间介于 0 到 10% 之间的实例，请将鼠标指针拖动到这两个范围上。



> 注意
>
> 单击“X”可删除选择。您也可以单击“重置”以删除多个选择。

概述 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量。选中该复选框可查看这些实例。

示例 **4**：查看过期 **SSL** 证书的实例：



1 -单击 筛选器 列表。

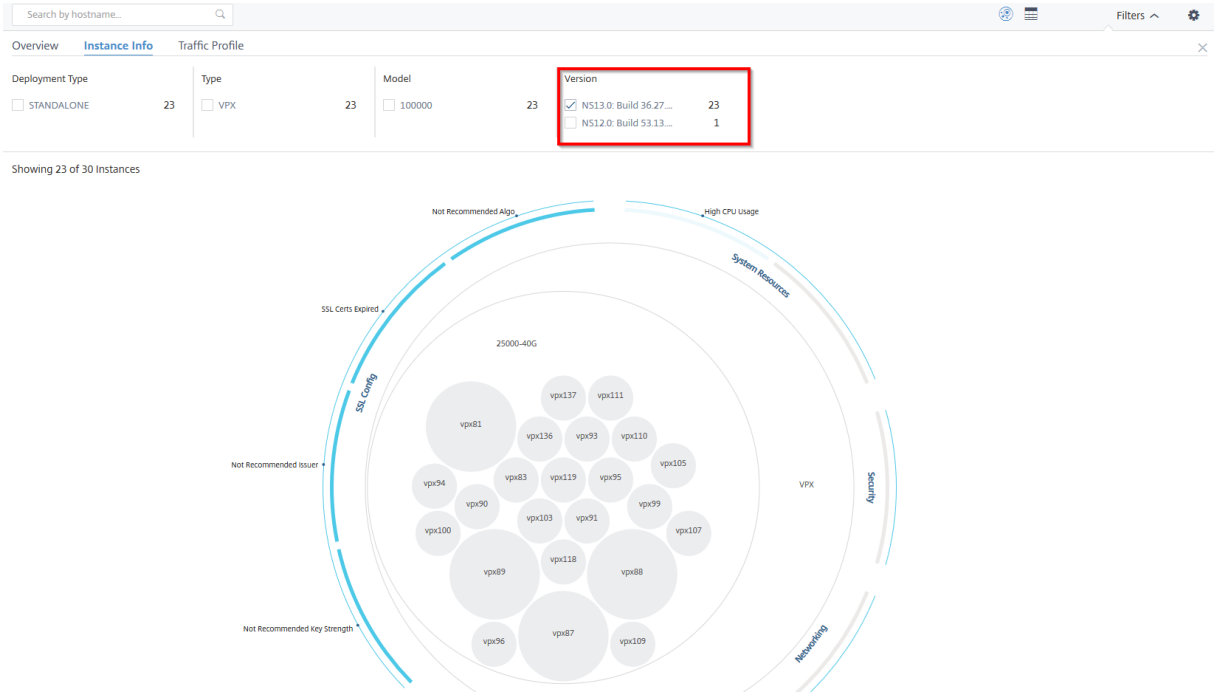
2 -在 **SSL** 证书到期 部分，选中“已过期”复选框以查看实例。

实例信息

实例信息 面板允许您根据部署类型、实例类型、模型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 **NetScaler VPX** 实例：

选择要查看的版本。

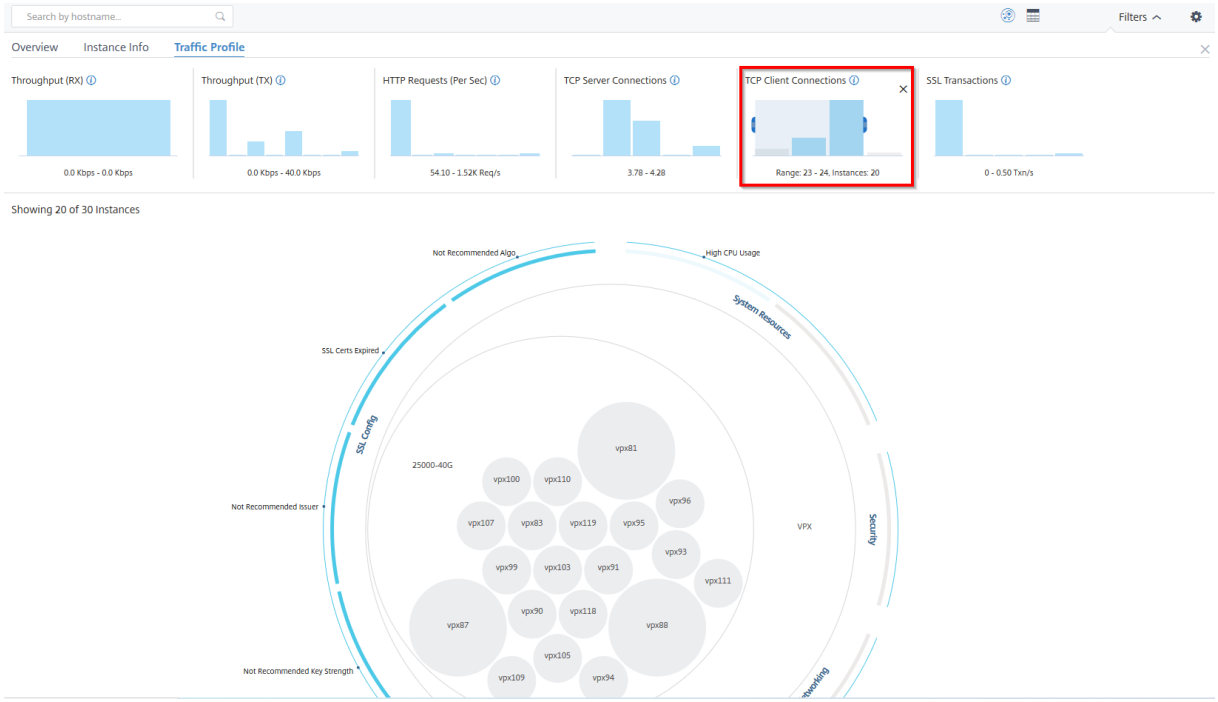


流量配置文件

Traffic p **ro** file 面板中的直方图表示基于实例的许可吞吐量、请求数量、连接数和实例处理的事务的实例聚合数。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 连接的实例数量。

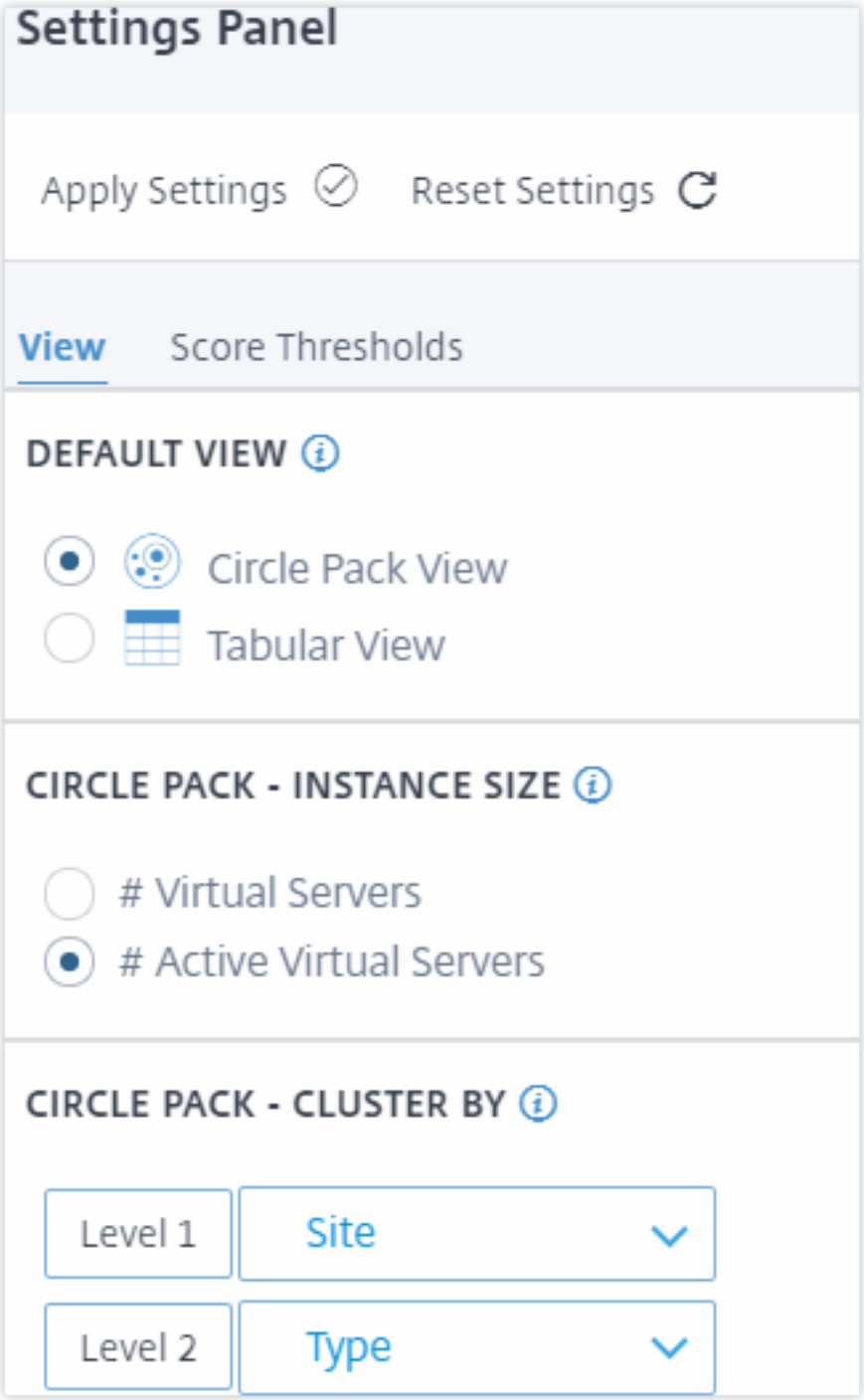


如何使用设置面板

设置 面板允许您设置基础架构分析的默认视图。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”。

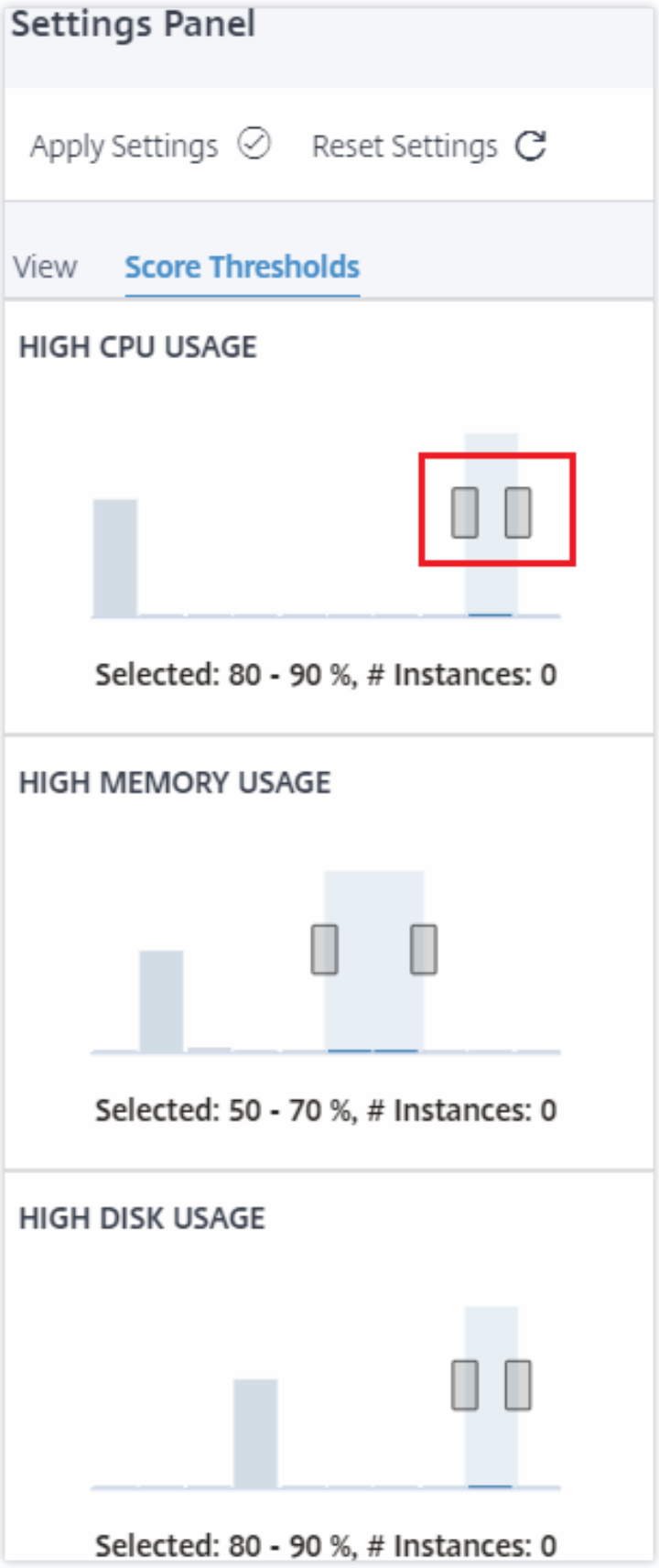
查看

- 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。您选择的格式就是您在 NetScaler ADM 中访问页面时看到的格式。
- 圆形包装-实例大小。允许实例圈的大小乘以虚拟服务器的数量或活动虚拟服务器的数量。
- **Circle Pack**-聚类依据。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。



得分阈值

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。

如何在控制板上可视化数据

使用基础结构分析，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，让我们来看看 ExampleCompany 的网络管理员 Chris 的案例。

克里斯在组织中维护着许多 NetScaler 实例。其中一些实例处理高流量，Chris 需要密切监视它们。Chris 注意到一些高流量实例不再处理通过它们的全部流量。早些时候，为了分析这种减少情况，克里斯必须阅读来自不同来源的多份数据报告。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 使用基础设施分析功能直观地查看所有实例的运行状况。

以下两个示例说明了基础结构分析如何帮助 Chris 进行维护活动：

示例 **1-**监视 **SSL** 流量：

Chris 在 Circle Pack 上注意到，一个实例的实例得分较低，并且该实例处于“严重”状态。Chris 点击该实例查看问题所在。实例摘要显示该实例上出现 SSL 卡故障，并且该实例无法处理 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。

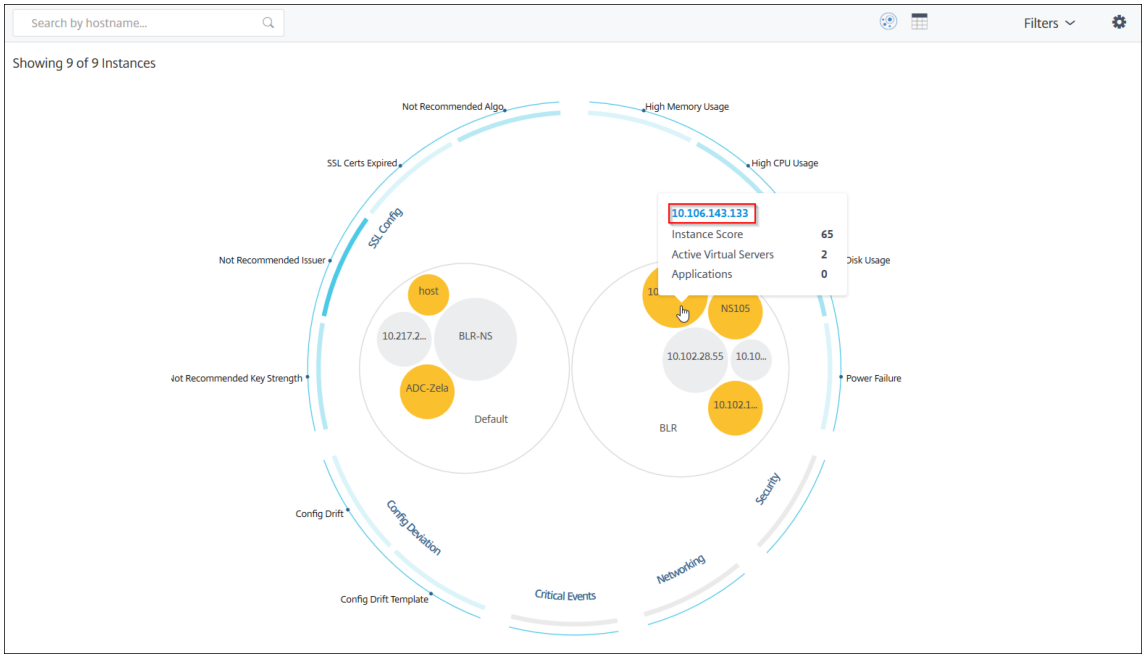
示例 **2-**监视配置更改：

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 点击配置偏差风险指标时，Chris 注意到已对 RC4 Cipher、SSL v3、TLS 1.0 和 TLS 1.1 相关的配置进行了更改，这可能是出于安全考虑。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。

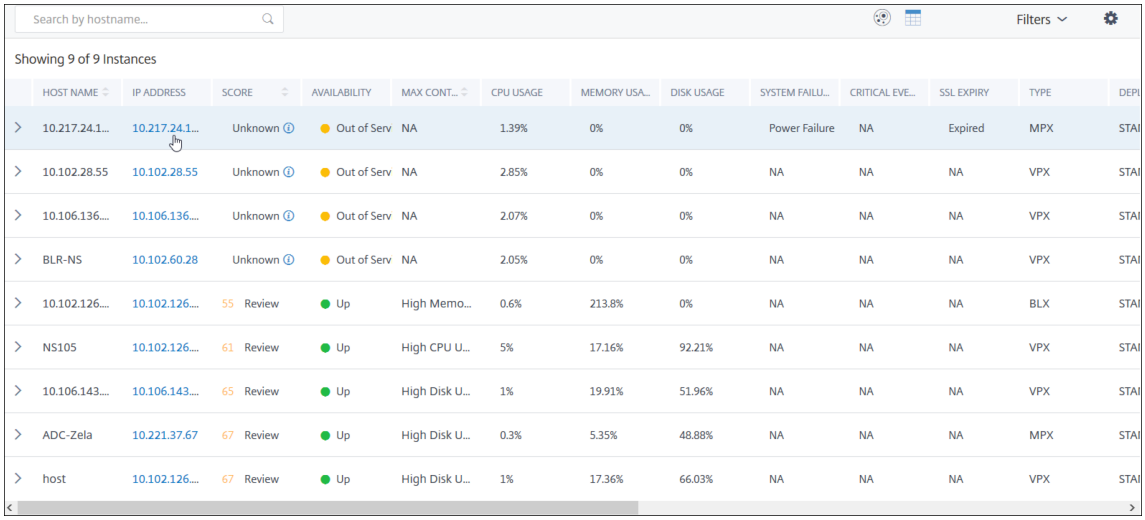
在基础结构分析中查看实例详细信息

February 6, 2024

1. 导航到 基础架构 **>** 基础架构分析
2. 单击圆包视图并选择 IP 地址。



您也可以单击表格视图中的 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
- 得分—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，例如“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—表示实例当前使用的 CPU 百分比
- 内存使用率—表示实例当前使用的内存百分比
- 磁盘使用率—表示实例当前使用的磁盘百分比

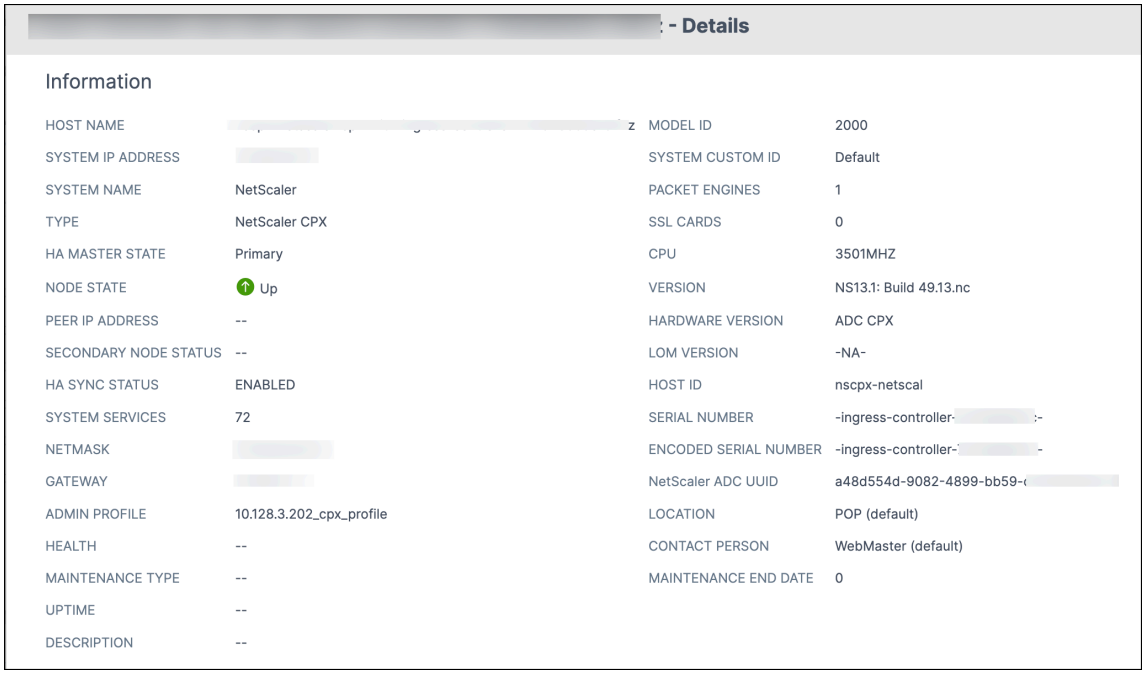
- 系统故障—表示实例系统的错误总数
- 严重事件—表示 NetScaler 实例具有最大事件的事件类别
- **SSL** 到期—表示 ADC 实例上安装的 SSL 证书的状态
- 类型—表示 ADC 实例类型，如 VPX、SDX、MPX 或 CPX
- 部署 -表示 ADC 实例是作为独立实例还是作为高可用性对部署
- 型号—表示 ADC 实例型号
- 版本—表示 ADC 实例版本和版本号
- 吞吐量—表示 ADC 实例的当前网络吞吐量
- **HTTPS** 请求/秒—表示 ADC 实例收到的当前 HTTPS 请求/秒
- **TCP** 连接 -表示当前建立的 TCP 连接
- **SSL** 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 分钟更新一次 CPU 使用率、内存使用率、磁盘使用率、吞吐量等的当前值。

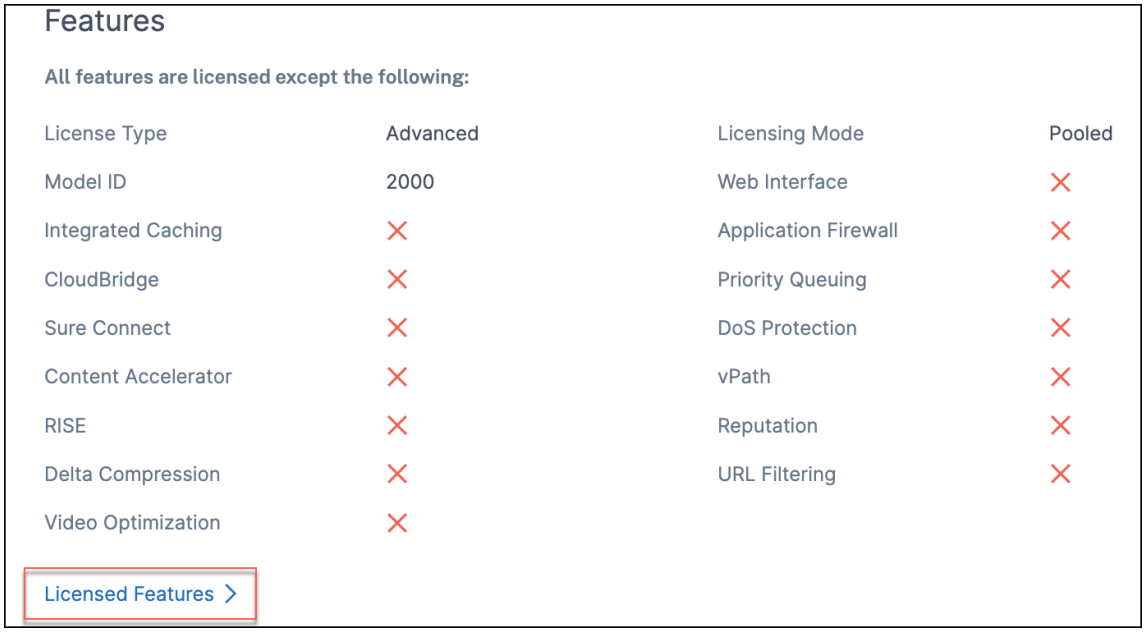
单击“实例详细信息”以查看详细信息。

将显示以下详细信息：

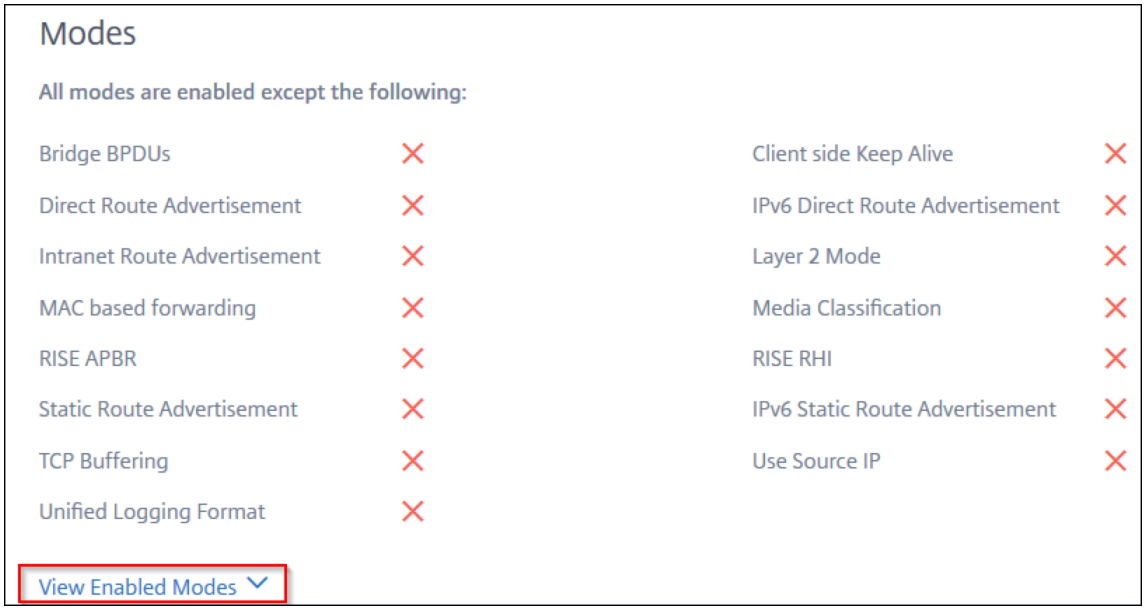
- 信息 -实例详细信息，例如实例类型、部署类型、版本、型号。



- 功能 -默认情况下，显示未获得许可的功能。单击“许可功能”查看已许可的功能。

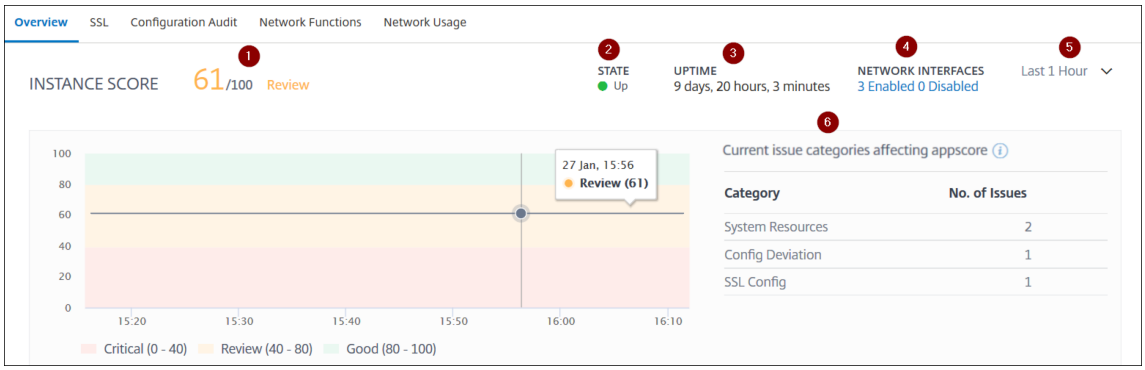


- 模式 -默认情况下，显示在实例上禁用的所有模式。单击“查看启用模式”以查看实例上的启用模式。



实例控制板显示实例概述，您可以在其中查看以下详细信息：

- 实例得分



1 —表示选定持续时间内的当前 NetScaler 实例得分。最终得分以 **100** 减去总点球计算。图形显示选定时间持续时间的得分范围。

2 —表示 NetScaler 实例的状态，例如“启动”、“关闭”和“停止 服务”。

3 —表示 NetScaler 实例启动并运行的持续时间。

4 —表示实例启用和禁用的网络接口总数。单击可查看网络接口名称和状态（启用或禁用）等详细信息。

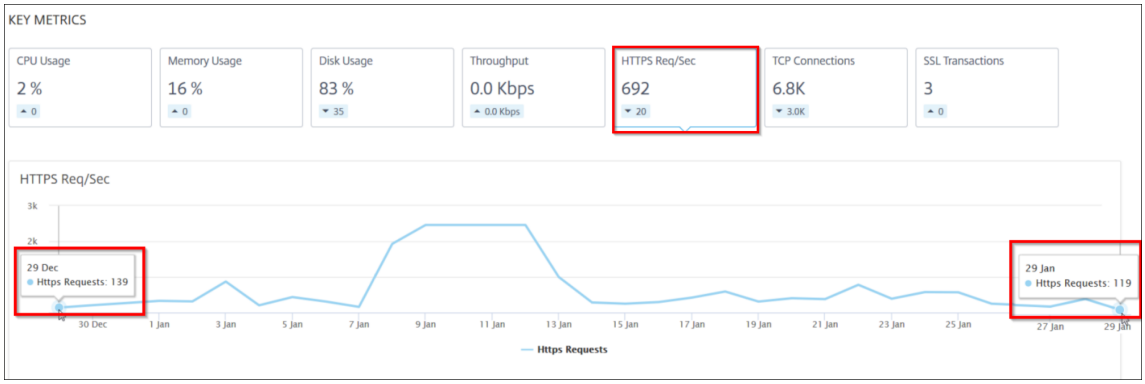
5 —从列表中选择持续时间以查看实例详细信息。

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，所选持续时间为 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 -选定持续时间内实例的平均 CPU 百分比（显示数据包 CPU 和管理 CPU）。
- 内存使用率—选定持续时间内实例的平均内存使用百分比。
- 磁盘使用率—选定持续时间内实例的平均磁盘空间百分比。
- 吞吐量—实例在选定持续时间内处理的平均网络吞吐量。
- **HTTPS** 请求/秒—实例在所选时长内收到的平均 HTTPS 请求数。
- **TCP** 连接 -客户端和服务器在选定持续时间内建立的平均 TCP 连接。
- **SSL** 事务—实例在选定持续时间内处理的平均 SSL 事务。

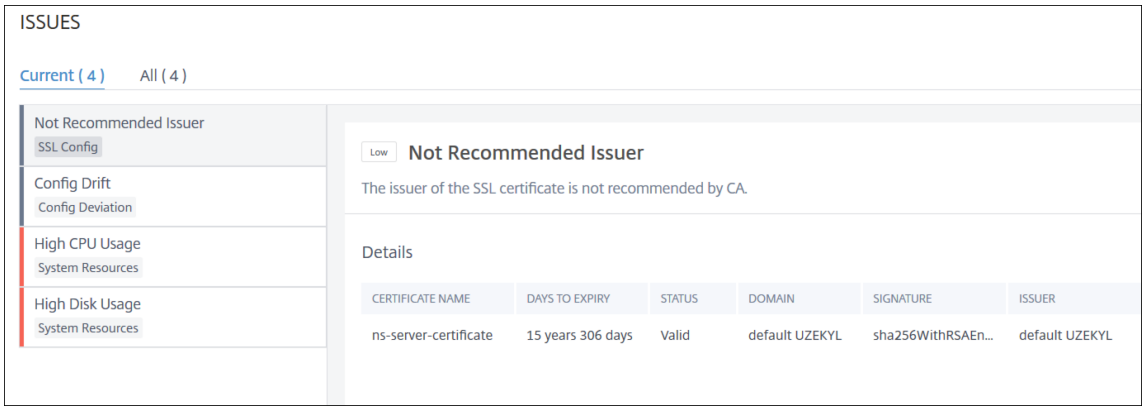
- 问题

  您可以查看 NetScaler 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 NetScaler 系统资源相关的所有问题，例如 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 - 闪存错误 - 网卡丢弃
SSL 配置	显示与 NetScaler 实例上的 SSL 配置相关的所有问题。	-SSL 证书已过期

问题类别	说明	问题
		– 不建议发行人 – 不推荐的算法 – 不建议密钥强度
配置偏差	显示与 NetScaler 实例中应用的配置作业相关的所有问题。	-配置偏移 – 运行与模板
关键事件	显示与在 HA 对和群集中配置的 NetScaler 实例相关的所有关键事件。	– 群集道具故障 – 群集同步失败 – 群集版本不匹配 – HA 辅助状态不正确 – 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。	有关更多信息，请参阅 使用新指标增强的基础设施分析。

单击每个选项卡以分析问题并进行故障排除。例如，假设一个实例在选定的持续时间内存在以下错误：



– “当前”选项卡显示当前影响实例得分的问题。

– “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

February 6, 2024

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 基础结构 **>** 基础结构分析。
2. 选择圆包视图。

> 注意
>
> 在 基础结构分析中，圆形视图和表格视图显示过去一小时内发生的事件和问题。

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分类：

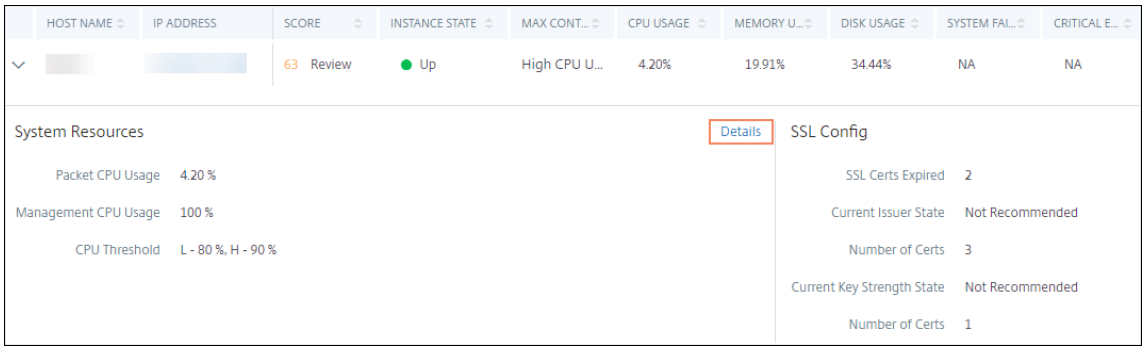
- 达到吞吐量限制**-**达到 吞吐量限制后实例中丢弃的数据包数量。
- 已达到 **PE CPU** 限制**-**达到 PE CPU 限制后在所有 NIC 上丢弃的数据包数量。

- 已达到 **PPS** 限制—达到 PPS 限制后在实例中丢弃的数据包数量。
- **SSL** 吞吐量速率限制 -达到 SSL 吞吐量限制的次数。
- **SSL TPS** 速率限制—达到 SSL TPS 限制的次数。

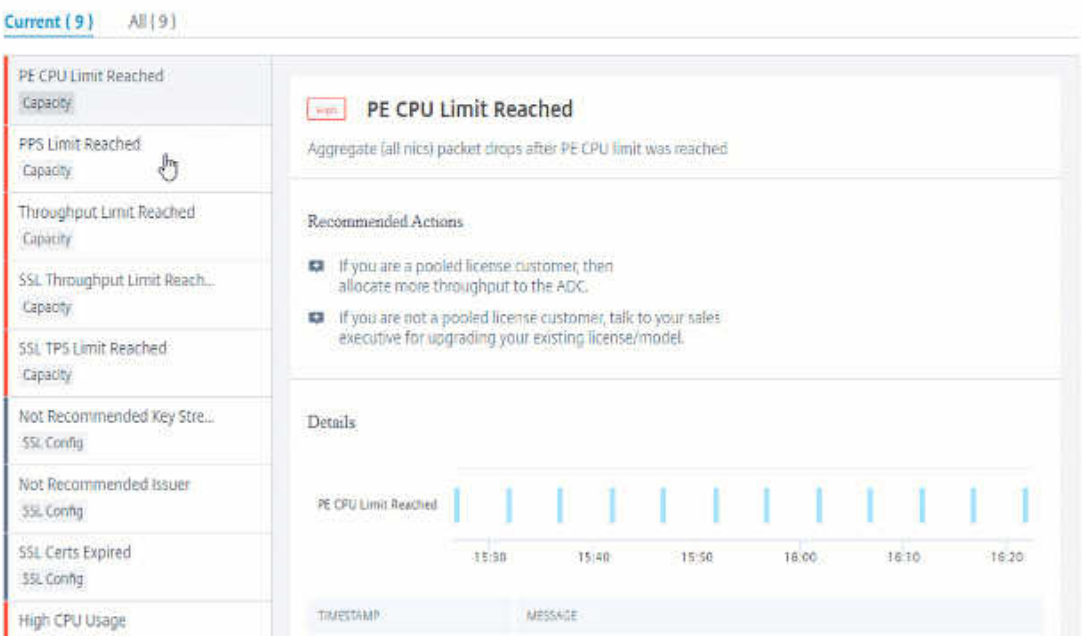
查看解决容量问题的建议措施

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 基础结构 **>** 基础结构分析中，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解决容量问题的建议措施。



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分数。

- 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。

利用新指标增强的基础结构分析

February 6, 2024

使用 NetScaler ADM 基础设施分析，您可以：

- 查看 NetScaler 实例中出现的一系列新的操作问题。
- 查看错误消息并查看建议以解决问题。

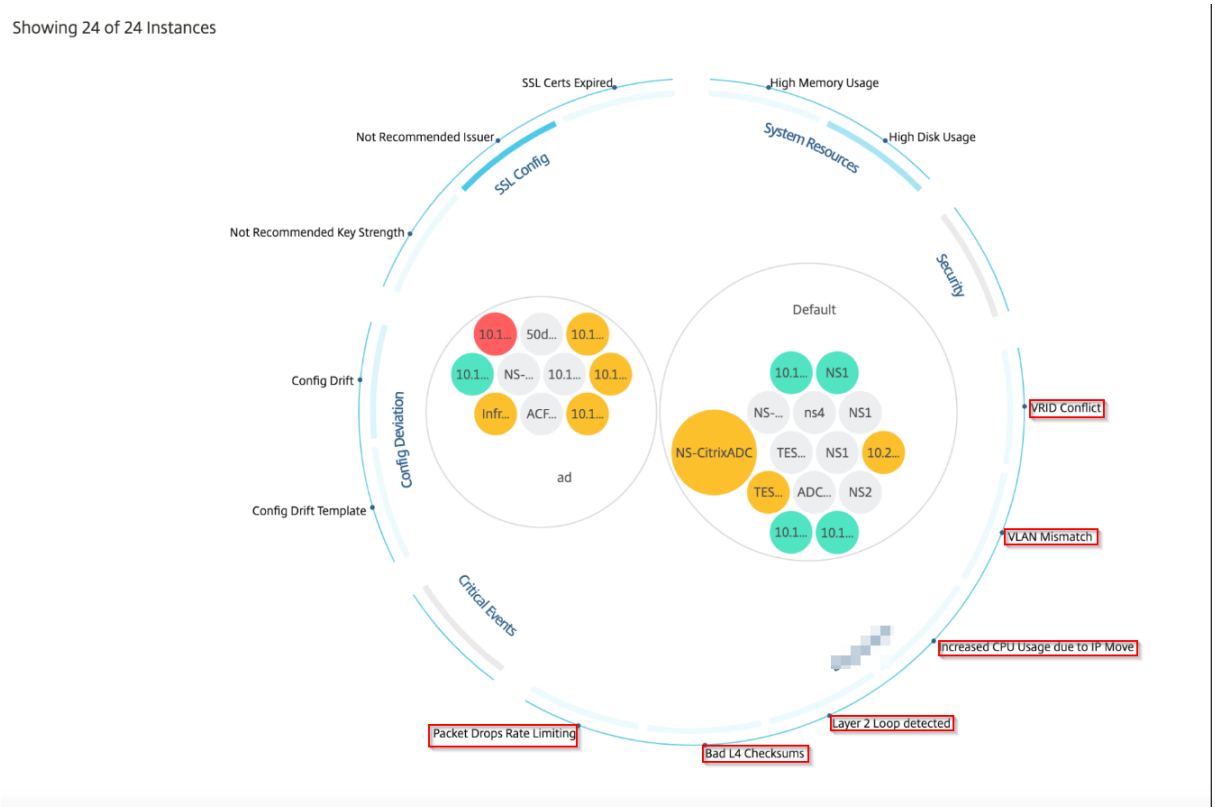
作为管理员，您可以快速确定问题的根本原因分析。

> 注意
>
> 规则指示器不支持以下用途：
>
> - 在群集模式下配置的 NetScaler 实例。
> - 配置了管理分区的 NetScaler 实例。

在 NetScaler ADM 中，导航到 基础架构 **>** 基础架构分析 以查看以下各项的指标：

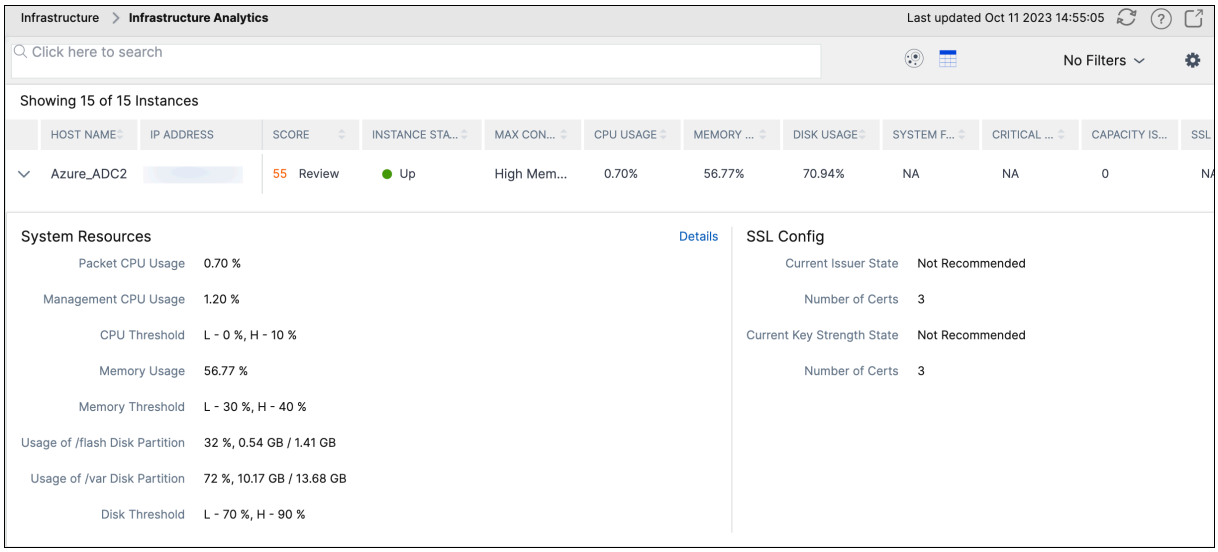
基础结构分析中的指标名称	说明
端口分配失败	检测 NetScaler 何时使用 SNIP 与新的服务器连接进行通信，并且该 SNIP 上的可用端口总数已耗尽。建议采取的操作是在同一子网中添加另一个 SNIP。
无默认路由配置	检测何时由于路由不可用而导致流量丢失。
IP 冲突	检测是否在网络中的两个或多个实例上配置或应用了相同的 IP 地址。
VRID 冲突	检测指定 VRID 何时出现间歇性访问问题。
VLAN 不匹配	检测在绑定到 IP 子网的 VLAN 配置期间是否出现任何错误。
TCP 小窗口攻击	检测何时可能存在小窗口攻击。此警报仅供参考，因为 ADC 已经缓解了此攻击。

基础结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被丢弃。
持久性限制	检测何时对 NetScaler 内存施加最大命中率。
GSLB 站点名称不匹配	检测何时由于站点名称不匹配而发生 GSLB 配置同步故障。
IP 标头格式不正确	检测 IPv4 数据包的健全性检查何时失败。
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 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水平软件数据包转向。
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	检测何时在无标记接口上接收到带标记的 VLAN 数据包。



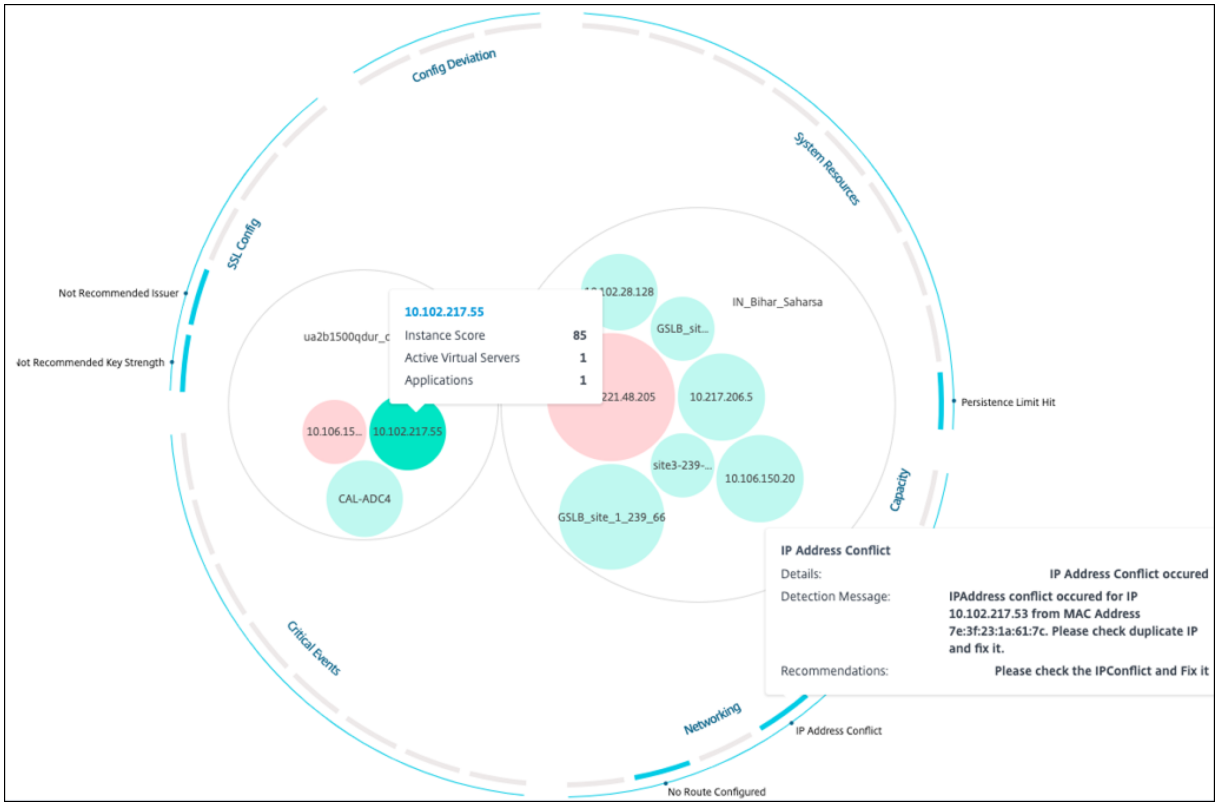
表格视图

您还可以使用 基础结构分析中的表格视图选项查看异常情况。导航到 基础架构 **>** 基础架构分析，然后单击 t 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 **IP** 地址冲突 的详细信息，请单击显示的 IP 地址冲突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

实例管理

February 6, 2024

实例是 Citrix Application Delivery Controller (ADC) 设备，您可以使用 NetScaler Application Delivery Management (ADM) 对其进行管理、监视和故障排除。您必须将实例添加到 NetScaler ADM 才能对其进行监视。可以在设置 NetScaler ADM 或更高版本时添加实例。将实例添加到 NetScaler 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专用 IP 块。当您想要运行特定任务（例如配置作业等）时，静态实例组可能很有用。专用 IP 块根据实例的地理位置对实例进行分组。

添加实例

可以在第一次设置 NetScaler ADM 服务器时添加实例，也可在以后添加。要添加实例，您必须指定每个 NetScaler 实例的主机名或 IP 地址，或指定 IP 地址范围。

要了解如何向 NetScaler ADM 添加实例，请参阅 向 NetScaler ADM 添加实例。

将实例添加到 NetScaler 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 NetScaler ADM 如何发现实例。

添加实例后，您可以通过导航到 基础架构 **>** 实例，然后单击所有实例来删除该实例。在“实例”页面上，选择要删除的实例，然后单击删除”。

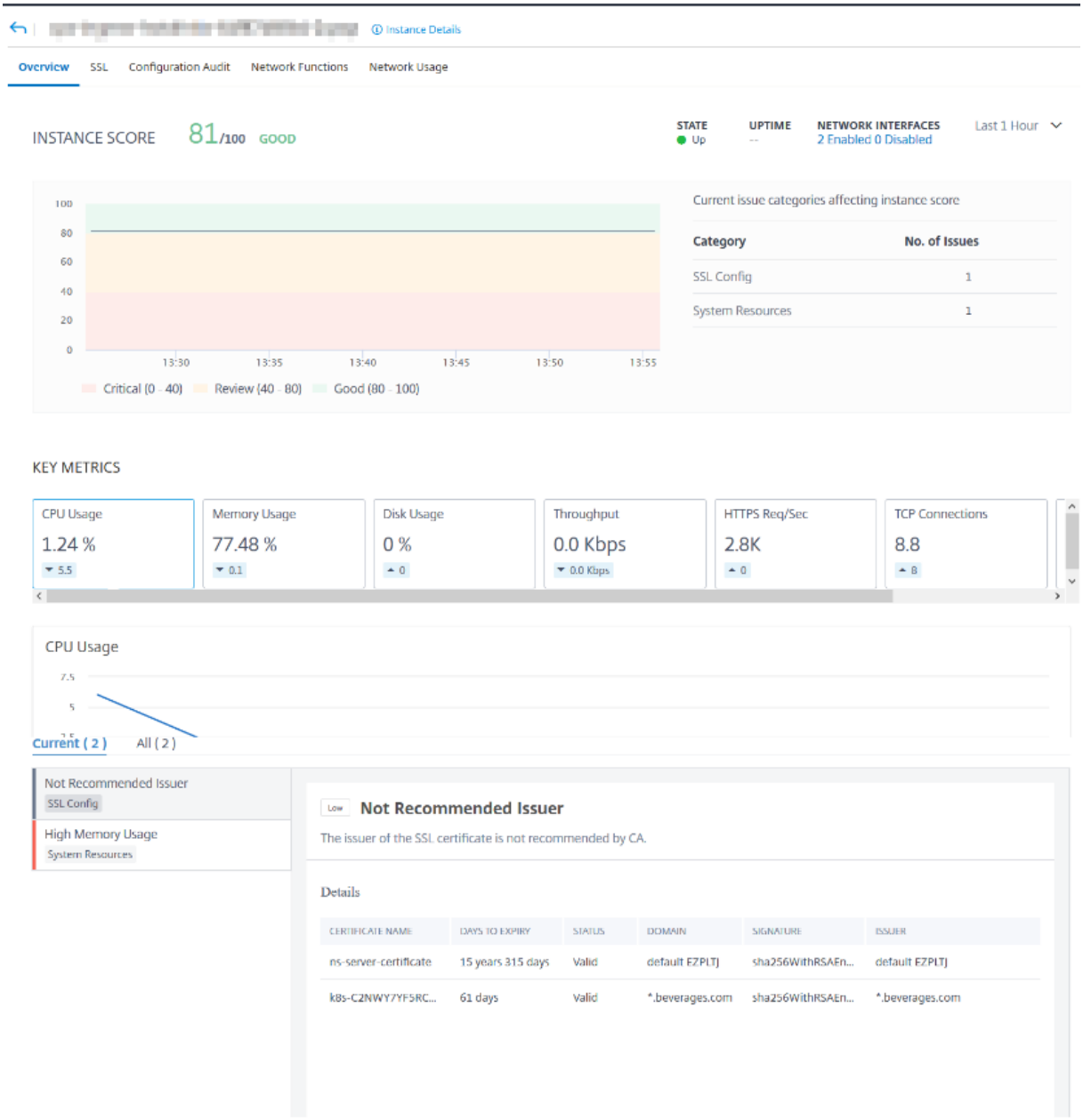
如何使用实例控制面板

NetScaler ADM 中的每实例控制板以表格和图形格式显示选定实例的数据。在轮询过程中从您的实例收集的数据显示在控制面板上。

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。

要查看特定实例的控制板，请导航到 基础架构 **>** 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 控制板。

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。

  有关更多信息，请参阅 实例详情。

- **SSL** 控制板。您可以使用每个实例控制面板上的 SSL 选项卡来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。您可以单击图表中的“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。控制面板上的 **NetScaler** 配置保存状态 和 **NetScaler** 配置偏移图表显示了有关已保存配置更改的高级详细信息，这些更改针对未保存的配置进行了保存。

- 网络功能。使用网络功能控制板，您可以监视在所选 NetScaler 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表。
- 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。

监视分布全球的站点

February 6, 2024

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。

NetScaler Application Delivery Management (ADM) 中的 Geomaps 为您提供站点的图形化表示，并按地理位置细分您的网络监视体验。通过 Geomap，您可以按位置呈现网络实例分布，并监视网络问题。

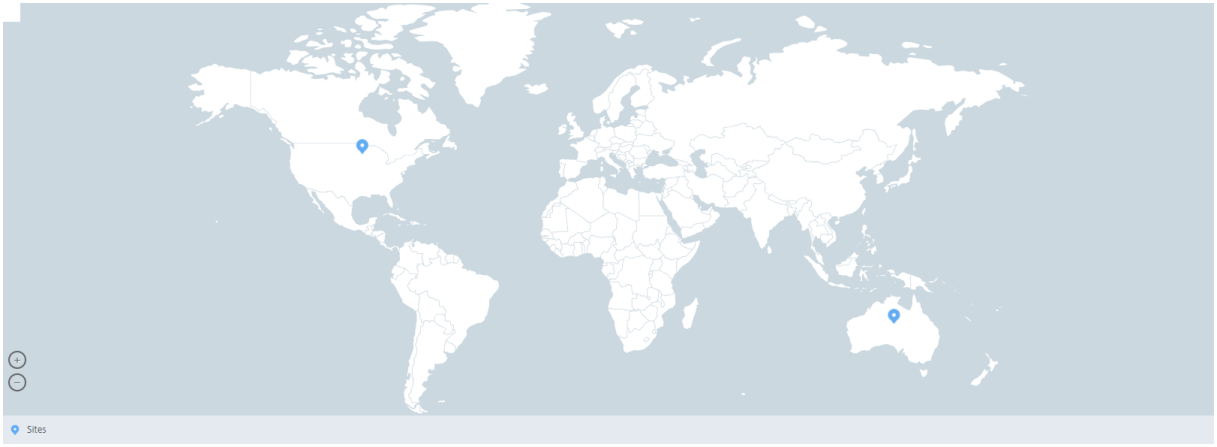
以下部分介绍如何监视 NetScaler ADM 中的数据中心。

NetScaler ADM 站点是特定地理位置中的 Citrix Application 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™。还有另一个网站托管在租户的场所内。NetScaler ADM 管理和监视连接到所有站点的所有 NetScaler 实例。您可以使用 NetScaler 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。

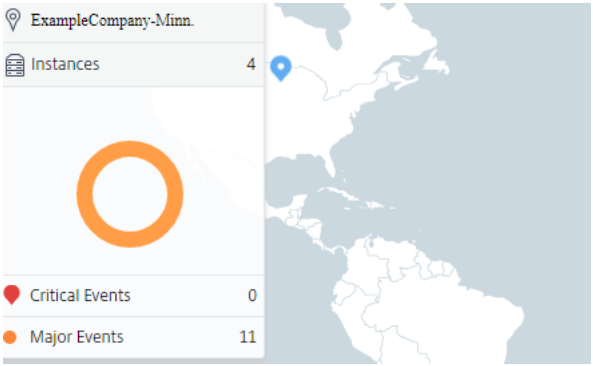
NetScaler ADM 中的地理地图为您提供站点的图形表示。Geomaps 还会按地理位置细分您的网络监视体验。通过地理图，您可以按位置可视化您的网络实例分布并监视所有网络问题。您可以导航到 基础架构 **>** 实例 页面，查看在世界地图上创建的站点的直观表示。

用例

一家领先的移动运营商公司 ExampleCompany 依靠私有服务提供商来托管其资源和应用程序。该公司已经有两个基地——一个位于美国的明尼阿波利斯，另一个在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。

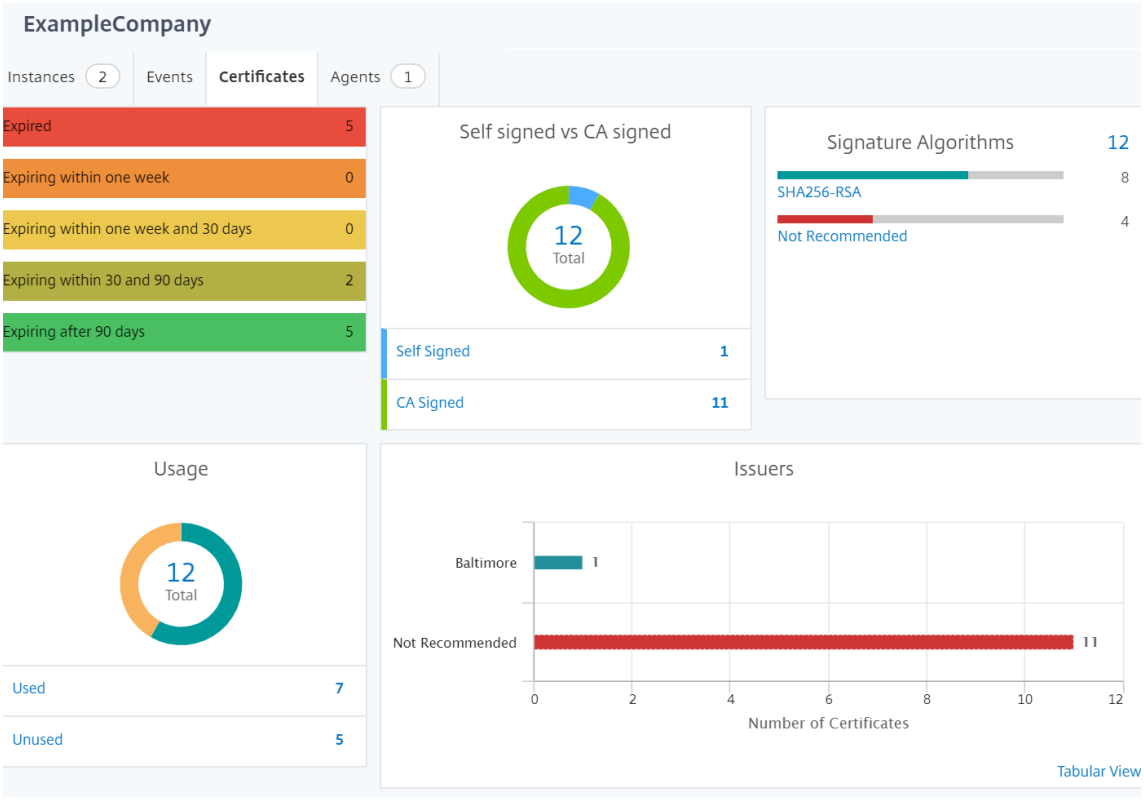


标记还会显示一个数字，显示每个站点中的应用程序数。您可以单击这些标记以了解有关每个站点的详细信息。



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
  - 他们身上的关键事件数量
  - 在 NetScaler 实例上引发的重大事件和所有事件。
- “事件”选项卡：查看实例上引发的关键和重要事件列表。
- “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
  - 重要信息以及许多正在使用的证书中排名前 10 位的实例。
- 代理选项卡：查看绑定实例的代理列表。



配置地理地图

ExampleCompany 决定在印度班加罗尔创建第三个站点。该公司希望通过将一些不太重要的内部 IT 应用程序转移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，您必须先创建一个站点，然后在 NetScaler ADM 中添加 NetScaler 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，NetScaler ADM 会识别 NetScaler 实例和代理所属的站点。

有关添加 NetScaler 实例的更多信息，请参阅 添加实例。

要创建站点：

在 NetScaler ADM 中添加实例之前，请先创建站点。通过提供位置信息，您可以精确地定位站点。

导航到基础架构 **>** 实例 **>** 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
   >
   > 该站点可以用作主数据中心或分支机构。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。

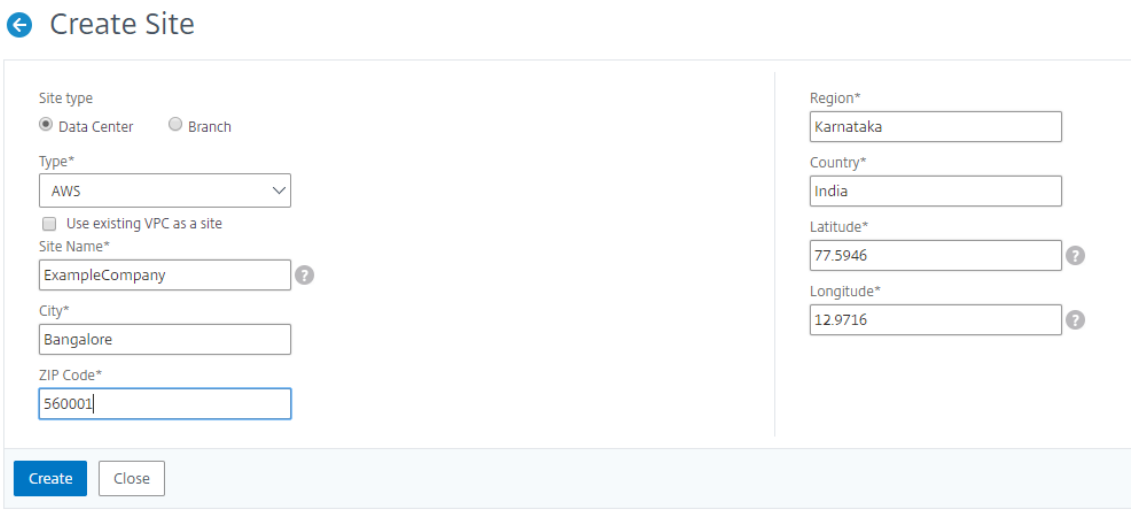
f) 区域：键入区域。

g) 国家：键入国家

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。

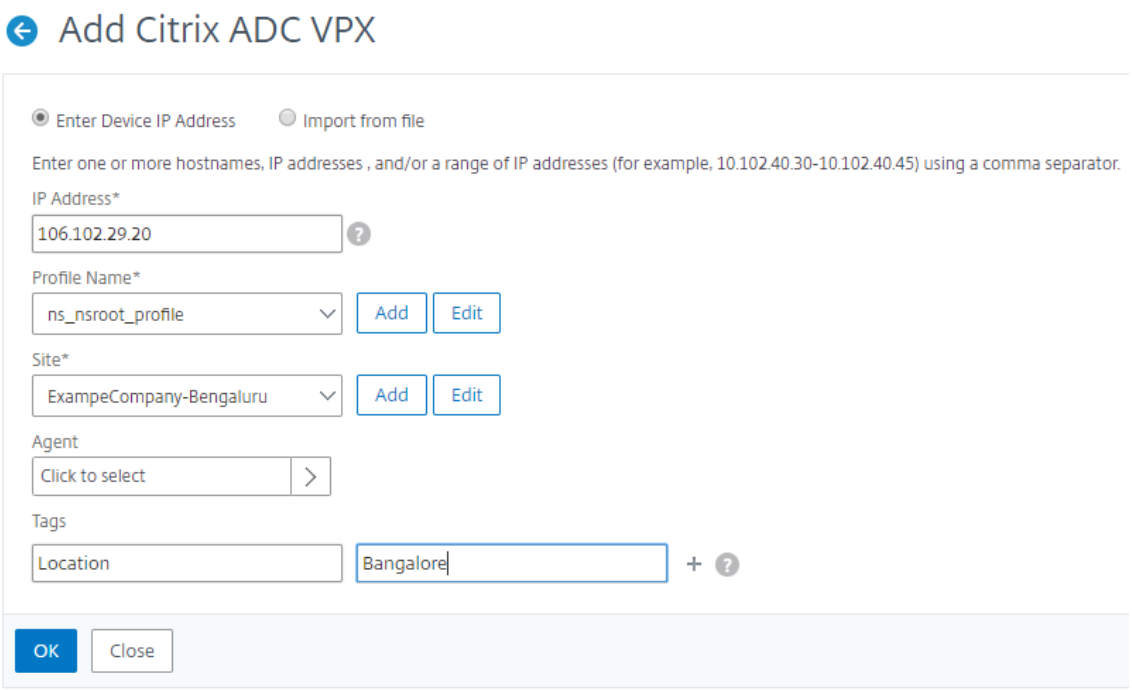


要添加实例并选择站点，请执行以下操作：

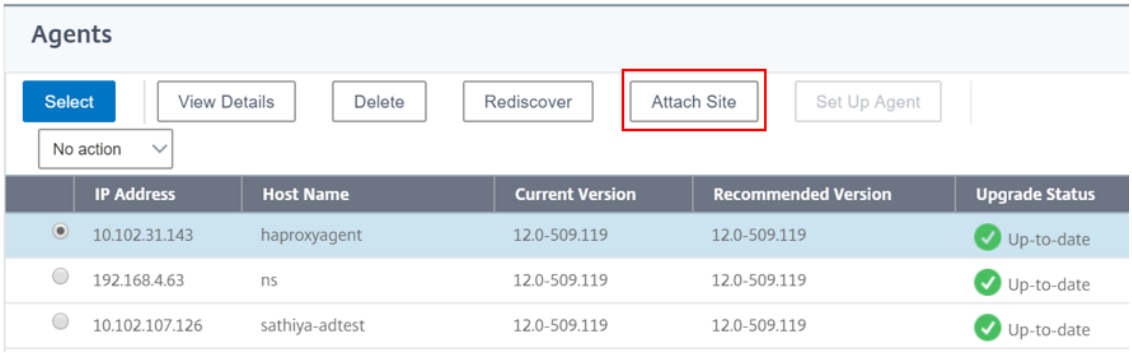
创建站点后，必须在 NetScaler ADM 中添加实例。您可以选择先前创建的站点，也可以创建站点并关联实例。

创建站点后，必须在 NetScaler 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 NetScaler ADM 中，导航到基础架构 > 实例。
2. 选择要创建的实例类型，然后单击 添加。
3. 在 添加 **NetScaler 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，也可以单击“编辑”图标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。选择代理并单击 附加站点。



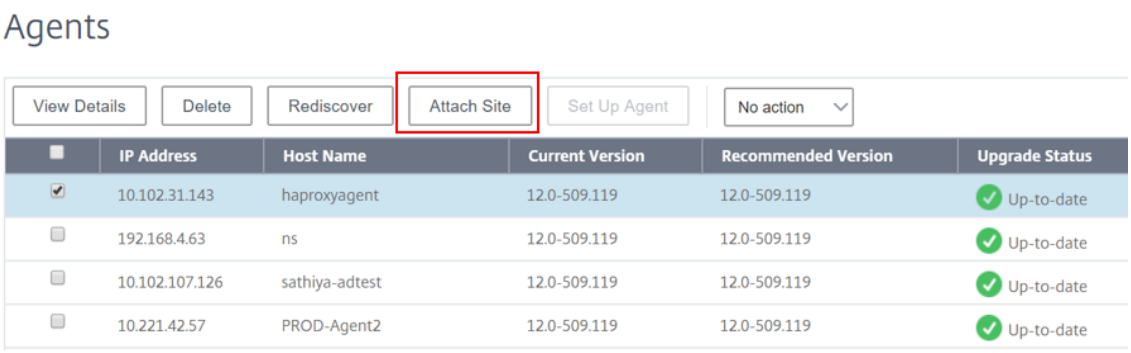
1. 从列表中选择站点，然后单击 保存”。

1. 单击确定。

您还可以通过导航到 基础结构 **>** 实例 **>** 代理将代理附加到站点。

要将 **NetScaler ADM** 代理与站点关联，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 实例 **>** 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”。

NetScaler ADM 开始监视在班加罗尔站点添加的 NetScaler 实例以及其他两个站点的实例。

如何创建标记并分配给实例

February 6, 2024

NetScaler Application Delivery Management (ADM) 现在允许您将您的 Citrix Application 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。可以将标签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视实例。

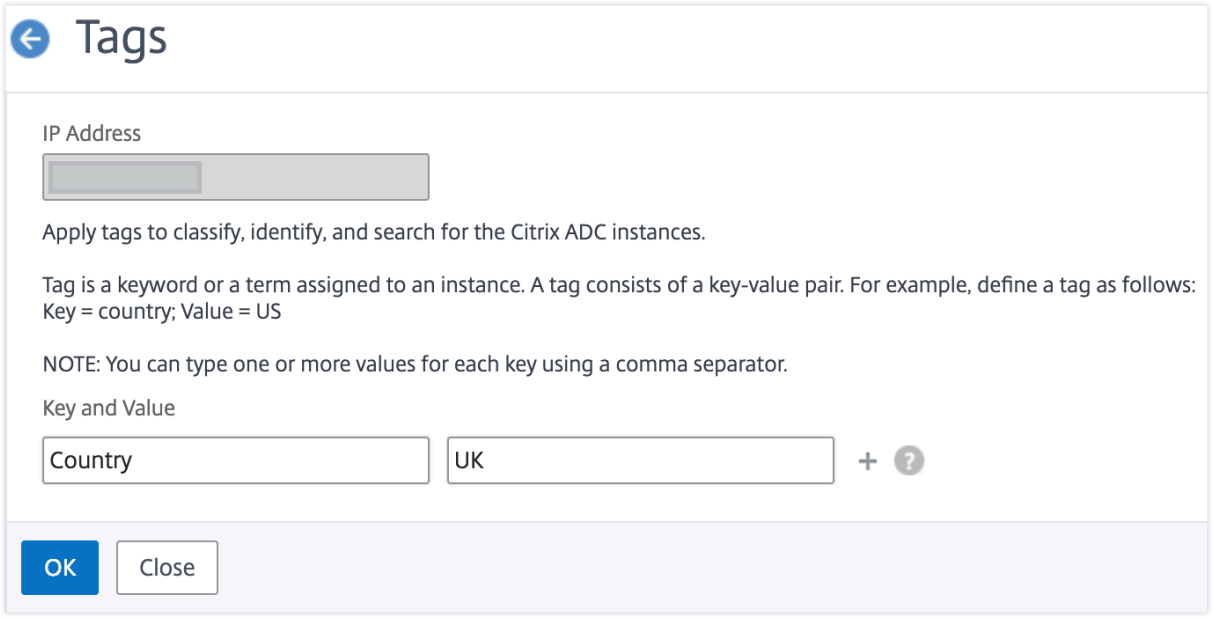
- 使用案例 **1**：您可以创建标签来标识英国的所有实例。在这里，您可以创建一个标签，密钥为“国家/地区”，值为“UK”。此标签可以帮助您搜索和监视英国境内的所有这些实例。
- 使用案例 **2**：您要搜索处于临时环境中的实例。在这里，您可以创建一个标签，其中密钥为“目的”，值为“Staging_NS”。此标记可帮助您将正在暂存环境中使用的所有实例与运行客户端请求的实例隔离开来。
- 使用案例 **3**：考虑一种情况，您想要查找位于英国“Swindon”区域并由您（David T）拥有的 NetScaler 实例列表。您可以为所有这些要求创建标签，然后将其分配给满足这些条件的所有实例。

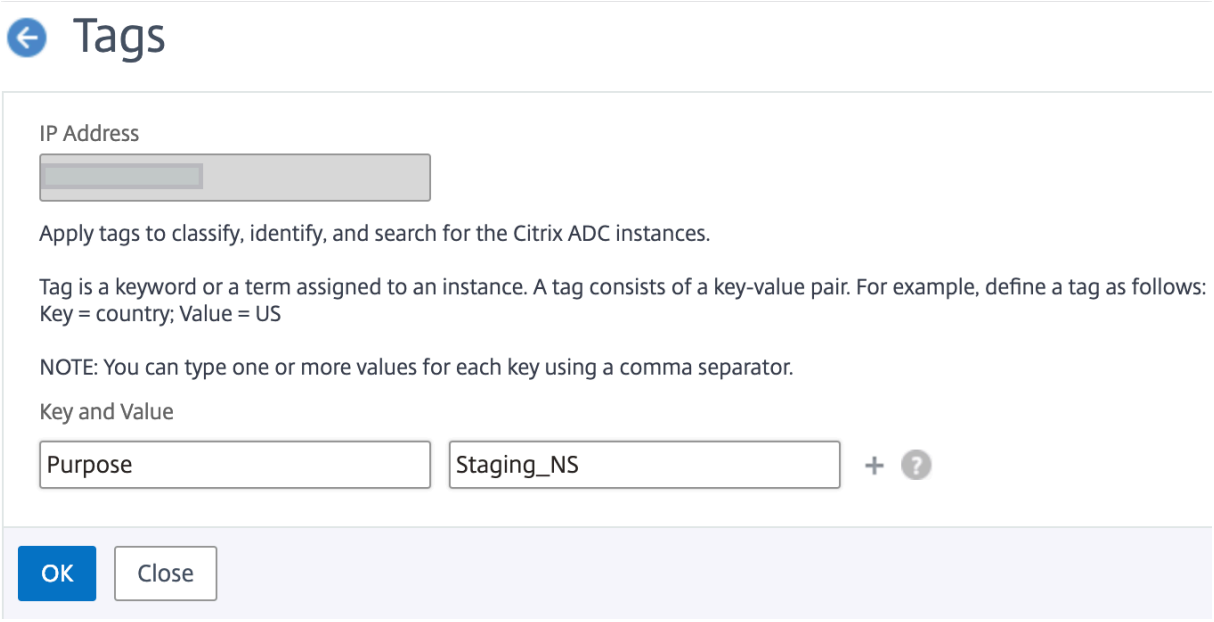
要为 **NetScaler VPX** 实例分配标签，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 实例 **> NetScaler**。
2. 选择 **NetScaler VPX** 选项卡。
3. 选择所需的 NetScaler VPX。
4. 单击“标签”。
5. 创建标签并单击“确定”。

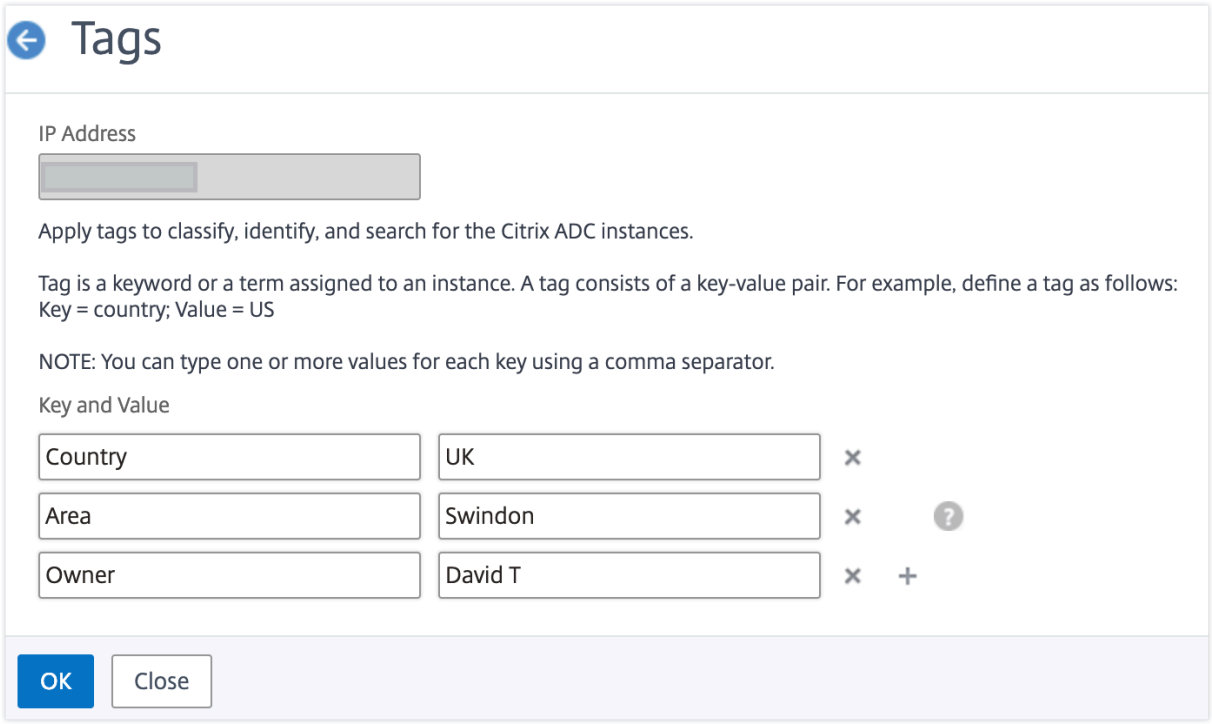
出现的“标签”窗口允许您通过为创建的每个关键字分配值来创建自己的“键值”对。

例如，下图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。



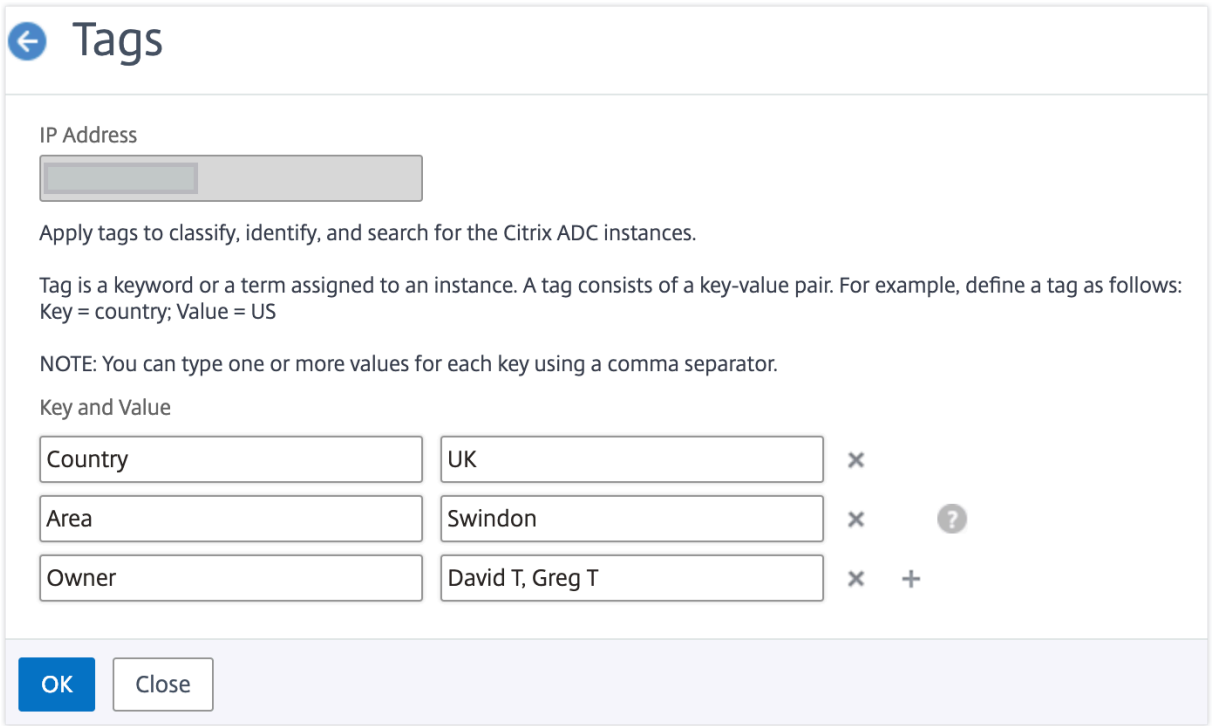


您也可以通过点击“+”添加多个标签。通过添加多个有意义的标签，您可以高效地搜索实例。



您可以通过用逗号分隔来向关键字添加多个值。

例如，您正在为另一位同事 Greg T 分配管理员角色。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。NetScaler ADM 将逗号分隔的值识别为两个不同的值。



要详细了解如何根据标签搜索实例，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。

如何使用标记和属性的值搜索实例

February 6, 2024

可能会出现这样的情况：NetScaler Application Delivery Management (ADM) 正在管理许多 NetScaler 实例。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。NetScaler ADM 现在提供了改进的搜索功能，可以根据您在搜索字段中定义的参数搜索 NetScaler 实例的子集。您可以根据两个标准（标签和属性）搜索实例。

- 标签。标签是可以分配给 NetScaler 实例的术语或关键字，以添加有关 NetScaler 实例的一些其他说明。现在，您可以将您的 NetScaler 实例与标签相关联。这些标签可用于更好地识别和搜索 NetScaler 实例。
- 属性。在 NetScaler ADM 中添加的每个 NetScaler 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，假设您想要找出版本为 12.0 且处于 UP 状态的 NetScaler 实例列表。在这里，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。

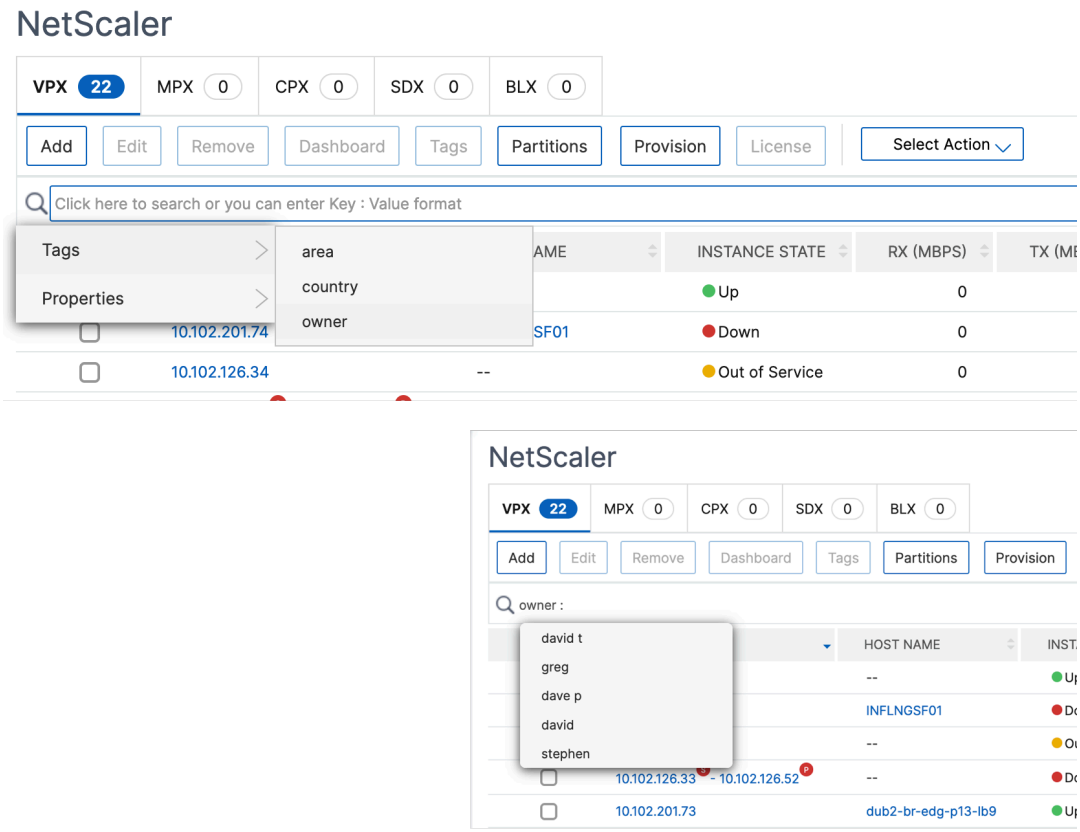
您可以使用标签和属性的组合来创建自己的搜索条件。

搜索 **NetScaler VPX** 实例

1. 在 NetScaler ADM 中，导航到 基础架构 **>** 实例 **> NetScaler** > **VPX** 选项卡。
2. 单击搜索字段。您可以使用标签或属性或将两者结合起来来创建搜索表达式。

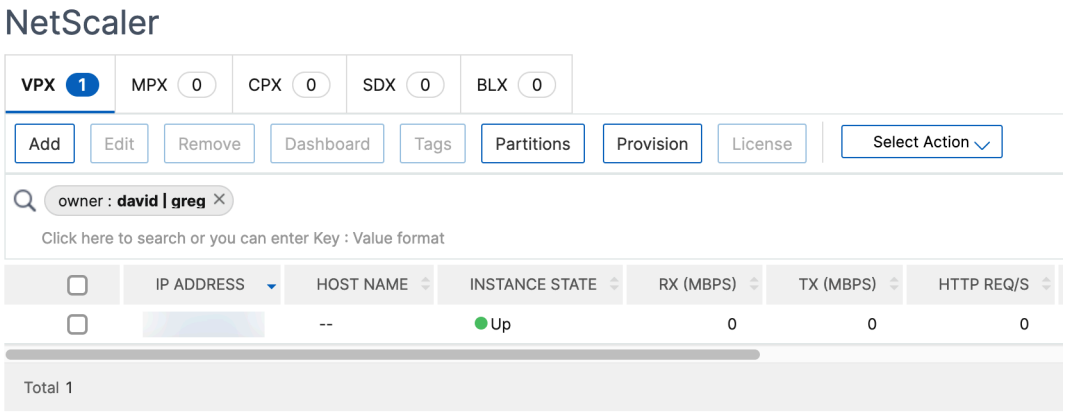
   以下示例显示如何有效地使用搜索表达式来搜索实例。

   a) 选择“标签”选项，然后选择“所有者”。选择“大卫 T.”

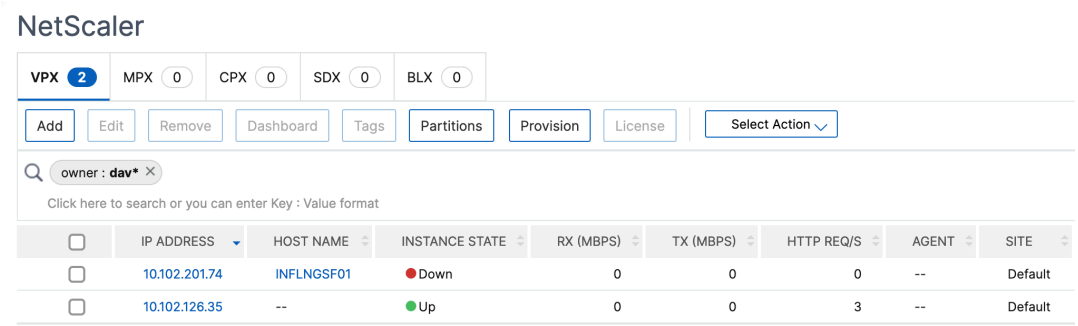


NetScaler ADM 支持搜索表达式中的正则表达式和通配符。

b) 您可以使用正则表达式来进一步扩展搜索条件。例如，您要搜索由 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以及如何使用它们的详细信息，请单击搜索栏中的“信息”图标。

管理 **NetScaler** 实例的管理分区

February 6, 2024

您可以在 Citrix Application Delivery Controller (ADC) 实例上配置管理分区，以便在同一 NetScaler 实例上为组织中的不同组分配不同的分区。可以指定网络管理员管理多个 NetScaler 实例上的多个分区。

NetScaler Application Delivery Management (ADM) 提供了一种从单一控制台无缝管理管理员拥有的所有分区的方法。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组中的分区。每个管理分区都被视为 NetScaler ADM 中的一个实例。当您发现 NetScaler 实例时，在该 NetScaler 实例上配置的管理分区会自动添加到系统中。

假设您有两个 NetScaler VPX 实例，一个实例上配置两个分区，另一个实例上配置三个分区。例如，NetScaler 实例 10.102.216.49 具有分区 1、分区 2 和分区 3，而 NetScaler 实例 10.102.29.120 具有 p1 和 p2，如下图所示。

要查看分区，请导航到基础架构 **>** 实例 **> NetScaler > 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，您可以指定 user-p2 来管理分区 10.102.29.80-p2、102.216.49-Partition_2 和 10.102.216.49-Partition_3。

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。

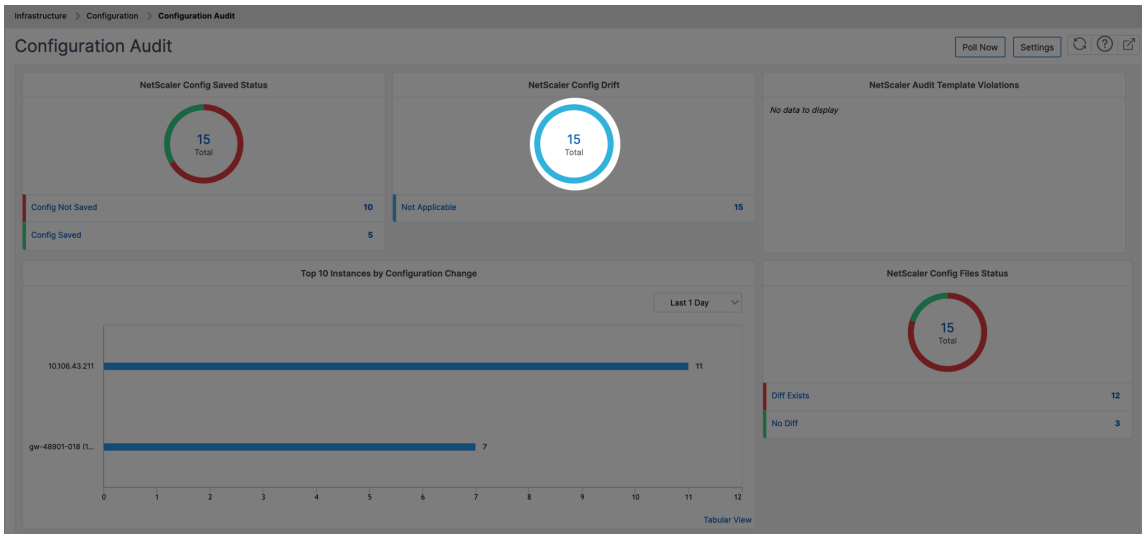
首先，您必须创建两个具有适当权限的组（例如：管理员权限），并在每个组中包含所需的管理员分区实例。例如，创建系统组 partition1-admin 并将 NetScaler 管理分区 10.102.29.120-p1 和 10.102.216.49-Partition_1 添加到此组。此外，还创建系统组 partition2-admin 并将 NetScaler 管理分区 10.102.29.120-p2、10.102.216.49-Partition_2 和 10.102.216.49-Partition_3 添加到此组。

创建管理分区后，您还可以使用修订历史差异功能和管理员分区审核模板功能进行审核

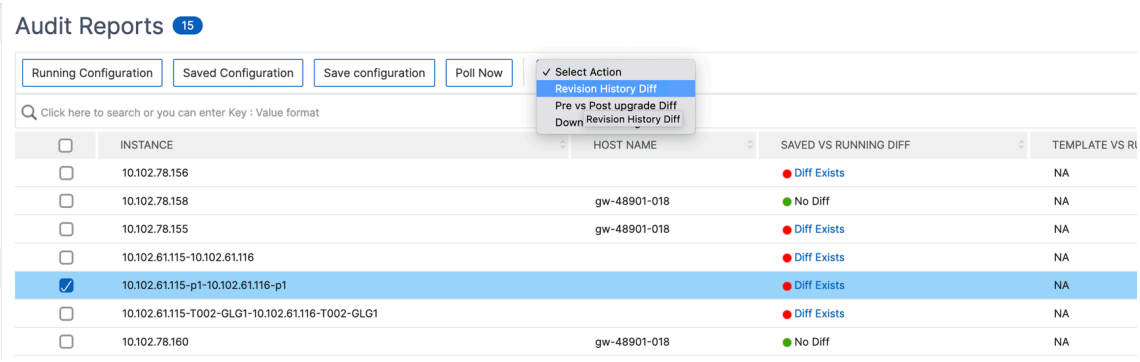
管理员分区的修订历史差异 允许您查看分区的 NetScaler 实例的五个最新配置文件之间的差异。您可以将配置文件相互比较（例如配置修订版-1 和配置修订版 -2），也可以将配置文件与当前正在运行/保存的配置与配置修订版进行比较。除了配置的差异外，还显示了校正配置。您可以将所有更正命令导出到本地文件夹并更正配置。

要查看修订历史记录差异，请执行以下操作：

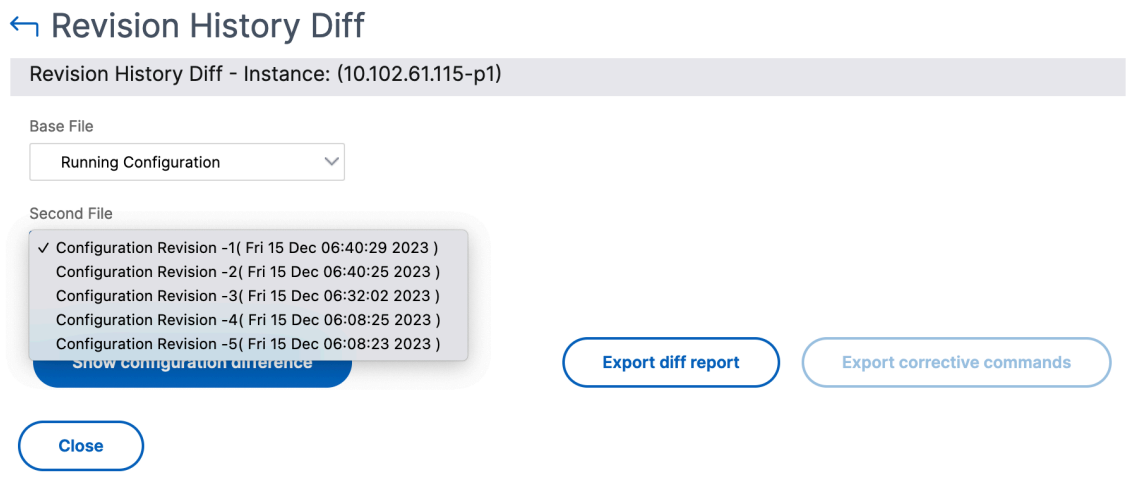
1. 导航到 基础架构 **>** 配置审核。在表示实例配置状态的圆环图中单击。在打开的“审核报告”页中，单击已分区的 NetScaler 实例。



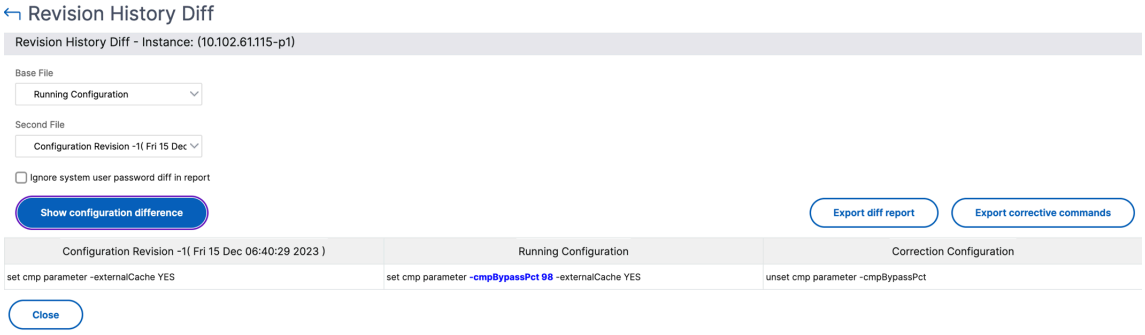
2. 在“操 作”菜单中，单击“修订历史记录比较”。



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。



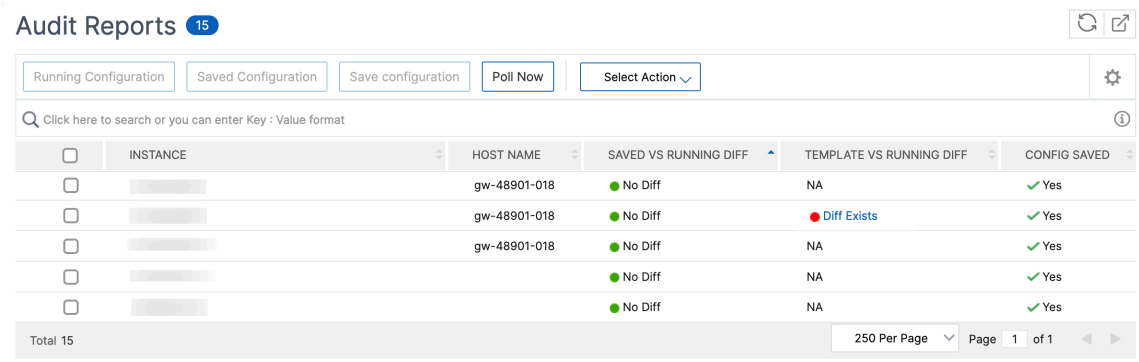
4. 然后，您可以查看所选分区 NetScaler 实例的五个最新配置文件之间的差异，如下所示。您还可以查看更正配置命令并将这些更正命令导出到本地文件夹。这些纠正命令是需要在基础文件上运行的命令，以使配置到所需状态（用于比较的配置文件）。



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。审核报告页面的模板与运行差异列显示在 审核报告页面的 模板与运行差异 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：

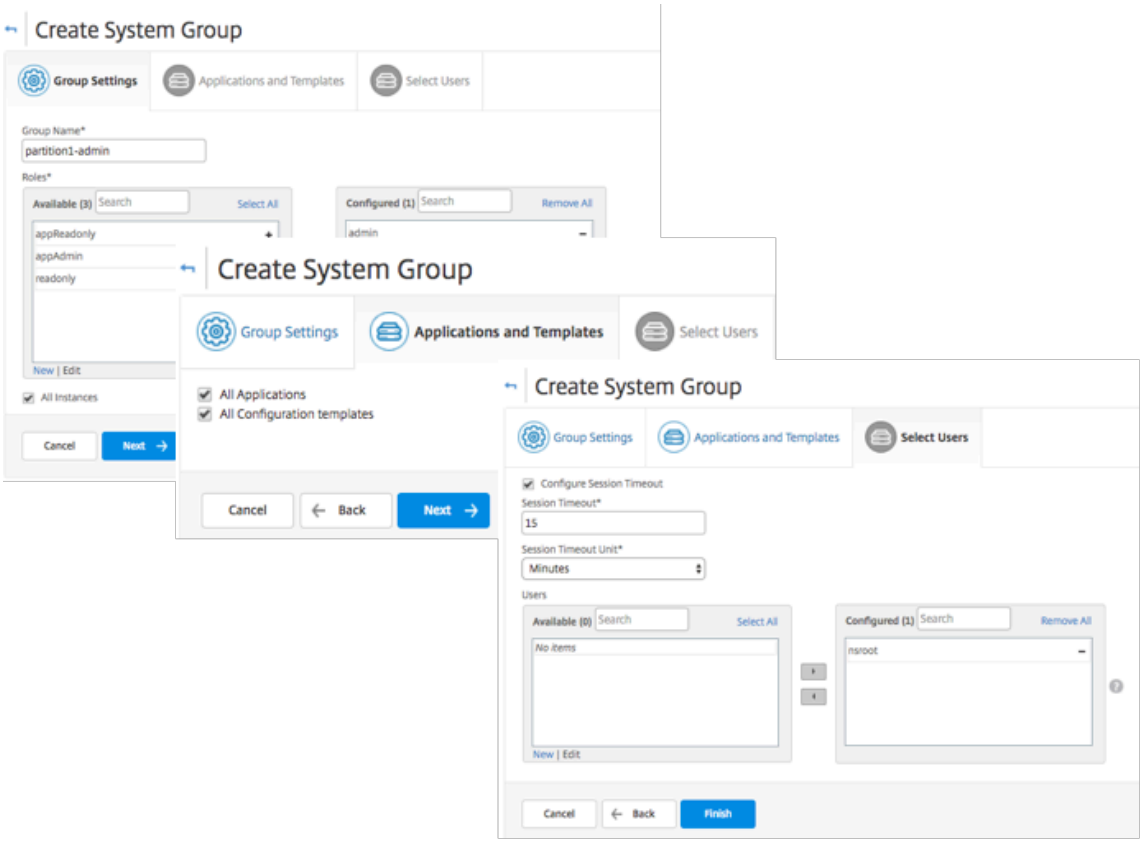
1. 在 审核报告 页面中，单击已分区的 NetScaler 实例。



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“设置”**>**“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“设置”**>**“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 **NetScaler** 高可用性对

January 29, 2024

NetScaler 高可用性 (HA) 组合可以在停机或网络故障期间提供不间断的操作。您可以使用 NetScaler ADM 创建一对高可用性 ADC 实例。有关更多信息，请参阅 NetScaler 高可用性。

要在 NetScaler ADM 中创建一对高可用性 ADC 实例，请执行以下步骤：

1. 导航到基础结构 **>** 实例 **> NetScaler**。

2. 从列表中选择要用来创建 HA 对的 ADC 实例。

   所选实例成为 HA 对中的主实例。

3. 单击“选择 操作”**>**“创建 **HA** 对”。

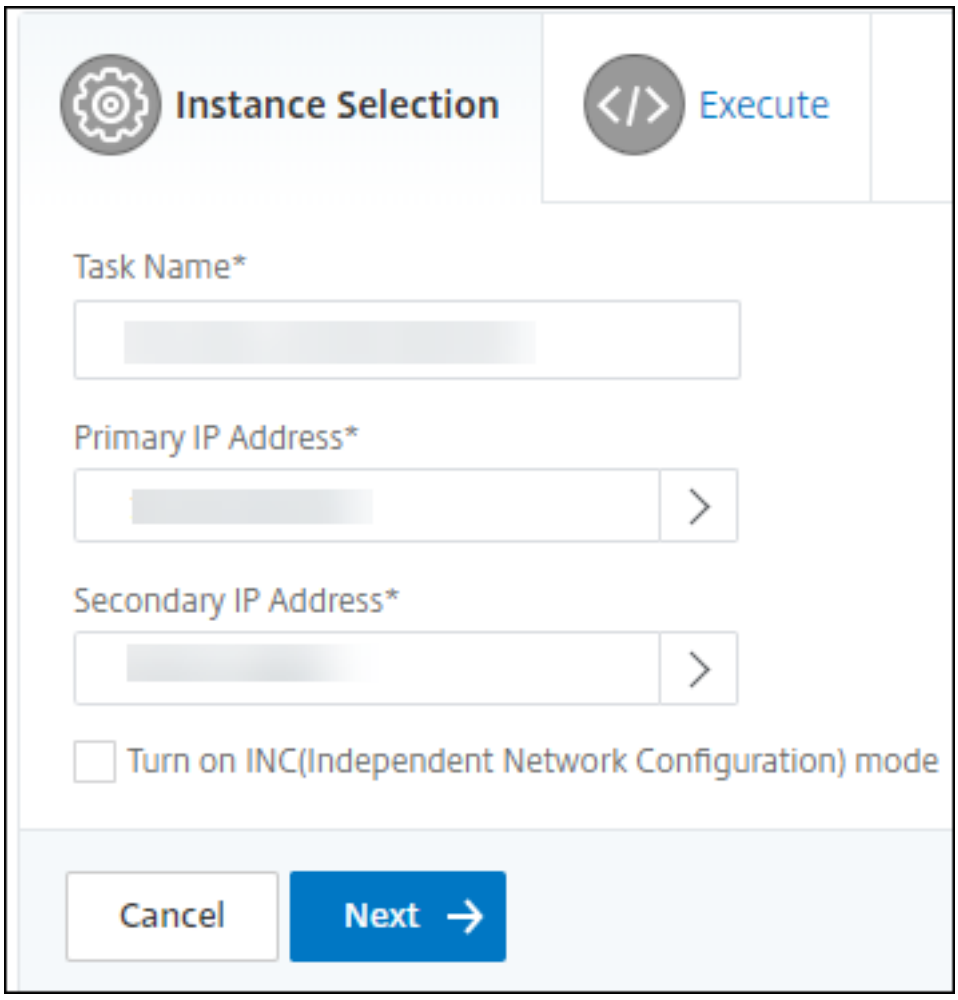
4. 在 实例选择中，执行以下步骤：

   a) 在 辅助 **IP** 地址中，单击选择辅助实例。

   b) 在 HA 对中选择要配置为辅助实例的 ADC 实例。

   c) 可选，如果您 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。



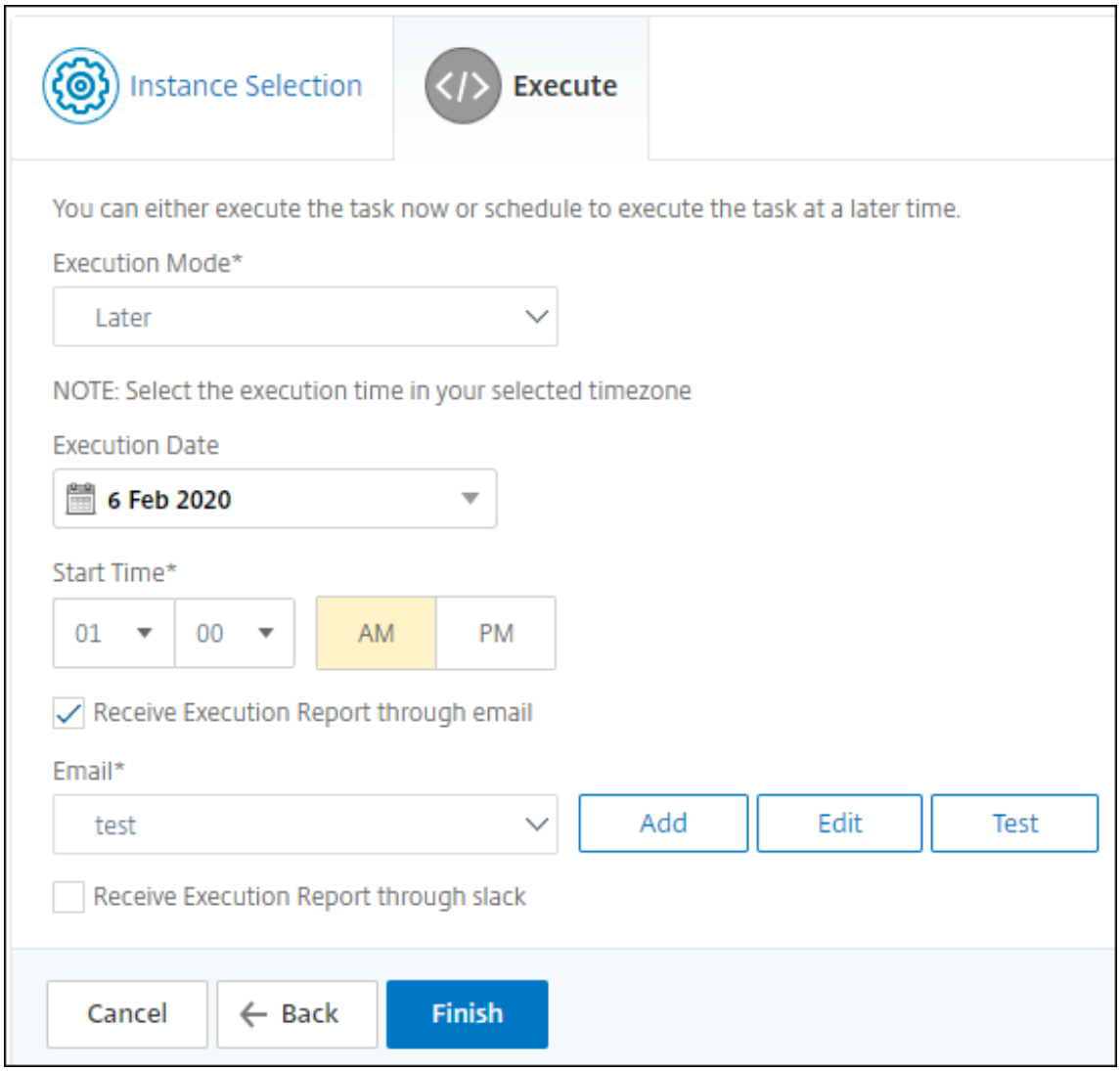
5. 在 **Execute** 中，您可以决定立即或稍后创建 HA 对。

   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。

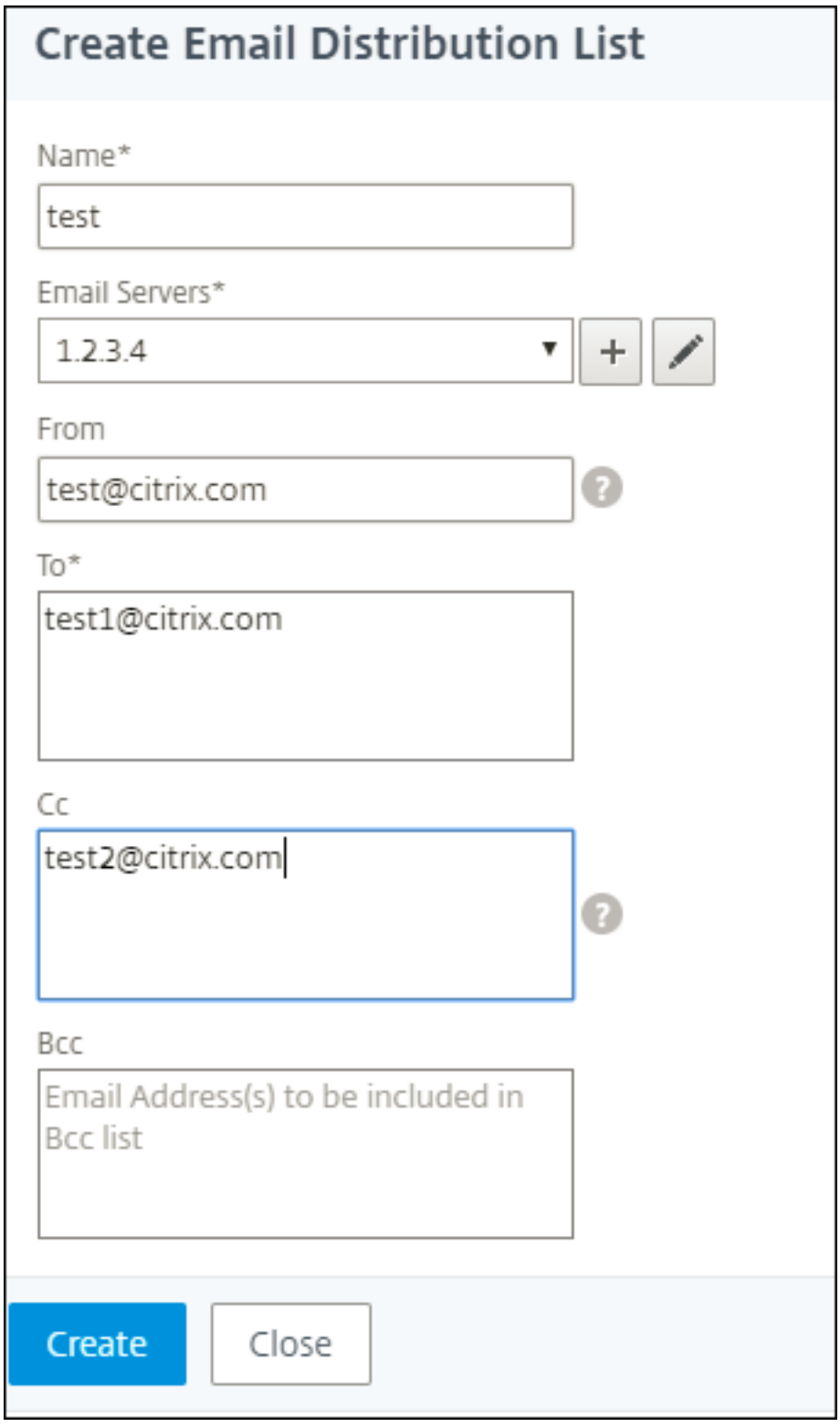
> ** 注
>
> 意：** 执行时间显示在 NetScaler ADM 中设置的时区中。



您可以通过以下方式接收此任务的执行报告：

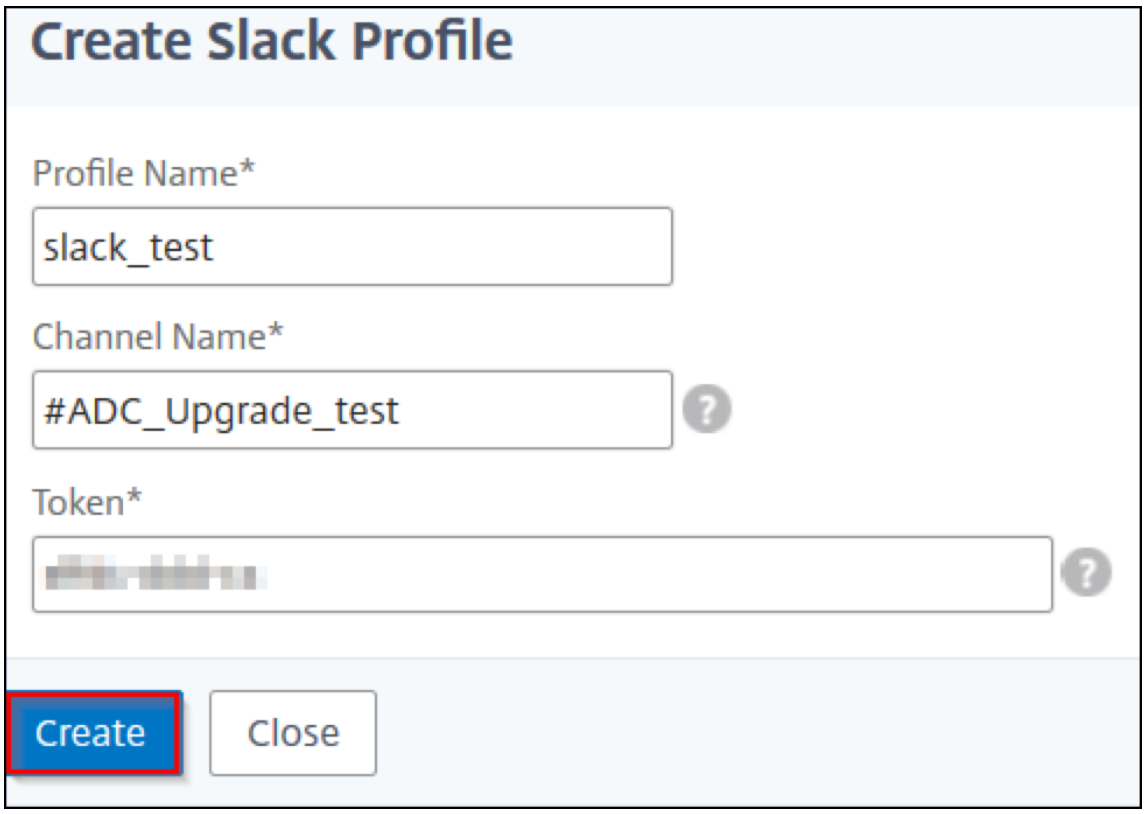
- 电子邮件 -从列表中选择电子邮件分发。

  要添加分发列表，请单击“添加”。指定添加分发列表所需的参数，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 配置文件名称、频道名称和 令牌，然后单击“创建”。



备份和还原 **NetScaler** 实例

February 6, 2024

您可以备份 NetScaler 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，请务必对其进行备份。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 NetScaler 实例上执行备份和恢复。您可以使用 GUI 和 CLI 手动备份和恢复 NetScaler 配置。您也可以使用 NetScaler ADM 执行自动备份和手动恢复。

NetScaler ADM 使用 NITRO 调用和安全外壳 (SSH) 和安全复制 (SCP) 协议复制托管 NetScaler 实例的当前状态。

NetScaler ADM 创建完整备份并恢复以下 NetScaler 实例类型：

- NetScaler SDX
- NetScaler VPX
- NetScaler MPX
- NetScaler BLX

有关更多信息，请参阅备份和还原 ADC 实例。

> 注意
>
> - 确保 NetScaler ADM 配置文件具有备份和恢复 ADC 实例的管理员访问权限。
> - 在 NetScaler ADM 中，您无法在 NetScaler 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导致的问题，您最多可以在此目录中为每个 ADC 实例保存 50 个备份文件。

要备份和还原 NetScaler 实例，必须首先在 NetScaler ADM 上配预配份设置。配置设置后，您可以选择单个 NetScaler 实例或多个实例，然后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文件恢复 NetScaler 实例。

配置实例备份设置

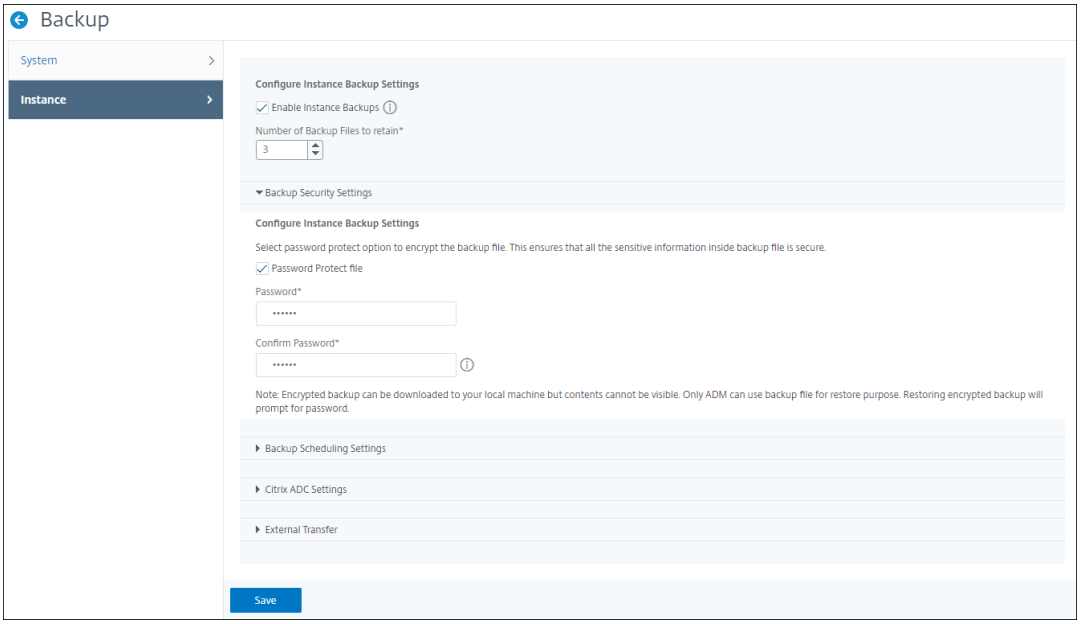
使用“实例备份设置”页可以配置 NetScaler ADM 上的设置，以备份选定的 NetScaler 实例或多个实例：

1. 在 NetScaler ADM 中，导航到“设置”>“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，NetScaler ADM 处于启用状态，以备份 NetScaler 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）选择密码保护选项对备份文件进行加密。加密备份文件可确保备份文件内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 NetScaler ADM GUI 或任何文本编辑器打开该文件。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 NetScaler ADM 中保留的备份文件数。每个 ADC 实例最多可以保留 50 个备份文件。默认是三个备份文件。

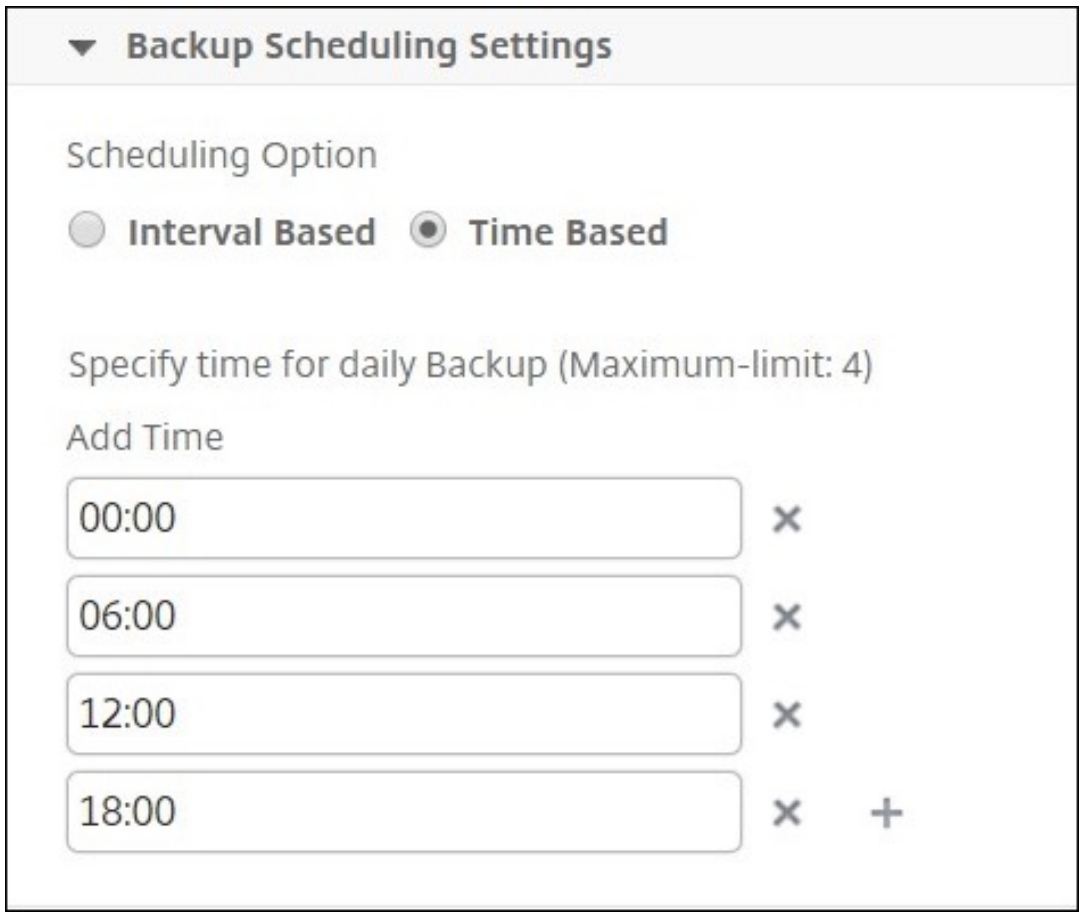
      > 注意
      >
      > 每个备份文件都涉及一定的存储需求。Citrix 建议您根据您的要求在 NetScaler ADM 上存储最佳数量的 NetScaler 备份文件。



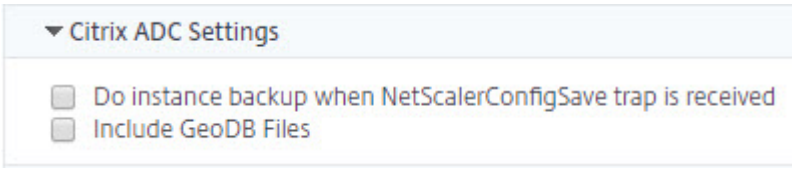
- 备份计划设置：（可选）有两个选项可用于创建备份文件，但一次只能使用一个选项：

  a) 默认的备份计划选项是“基于间隔”。经过指定的间隔后，将在 NetScaler ADM 中创建备份文件。默认备份时间间隔是 12 小时。

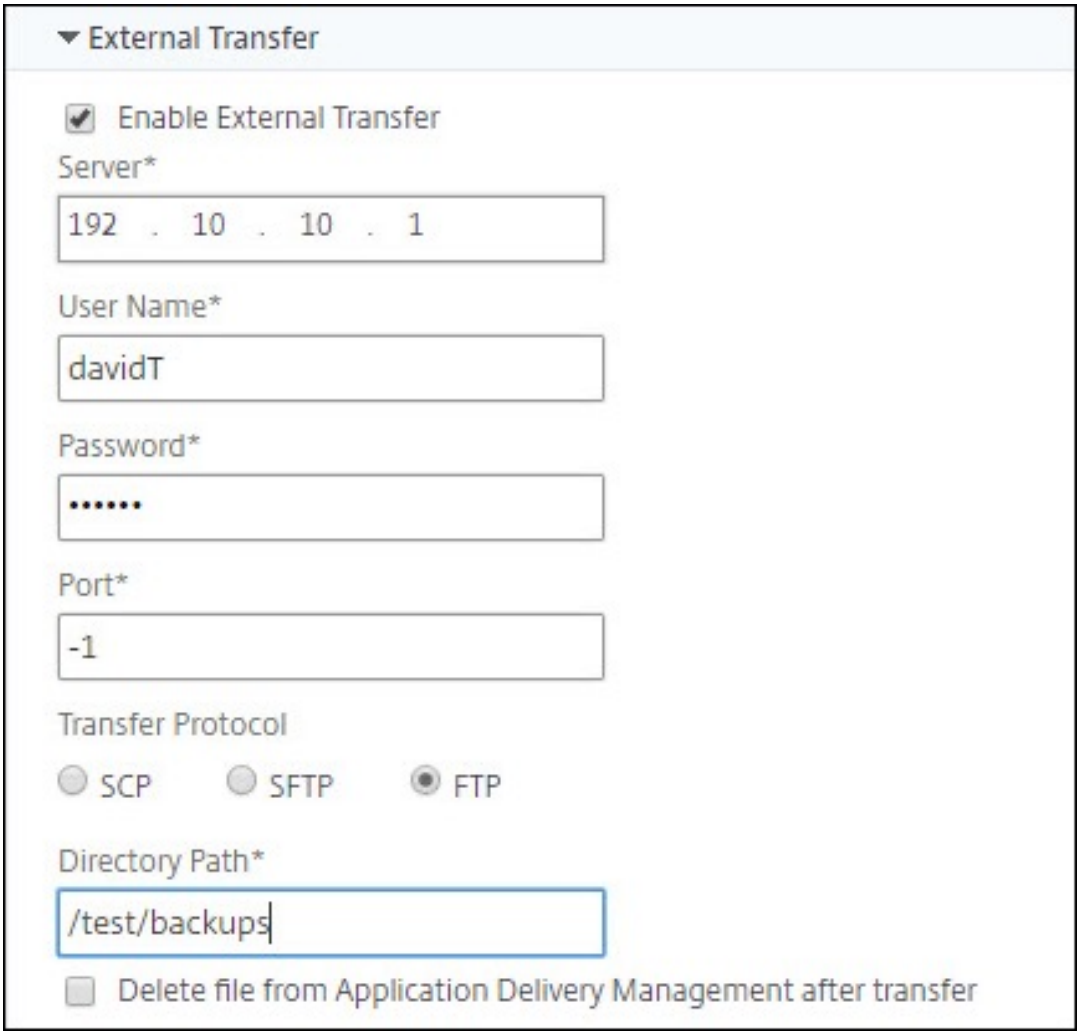
  b) 您还可以将定时备份的类型更改为“基于时间”。在此选项中，以 `hours:minutes` 格式指定在指定时间备份实例的时间。NetScaler ADM 允许在实例上进行最多四次每日备份。



- **NetScaler** 设置：（可选）默认情况下，NetScaler ADM 在收到“NetScalerConfigSave”陷阱时不会创建备份文件。但是，每当 NetScaler 实例向 NetScaler ADM 发送“NetScalerConfigSave”陷阱时，您可以启用创建备份文件的选项。每次保存 NetScaler 实例上的配置时，该实例都会发生“NetScalerConfigSave”。
- 地理数据库文件：（可选）默认情况下，NetScaler 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）NetScaler ADM 允许您将 NetScaler 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，您还可以在将备份文件传输到外部服务器后将其从 NetScaler ADM 中删除。



> 注意
>
> 当任何选定的 NetScaler 实例出现备份失败时，NetScaler ADM 会向自己发送 SNMP 陷阱或 Syslog 通知。

使用 **NetScaler ADM** 为选定的 **NetScaler** 实例创建备份

如果要备份选定的 NetScaler 实例或多个实例，请执行以下任务：

1. 在 NetScaler ADM 中，导航到基础架构 > 实例。在“实例”下，选择要在屏幕上显示的实例类型（例如 NetScaler VPX）。
2. 选择要备份的实例。
   - 对于 MPX、VPX 和 BLX 实例，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”。

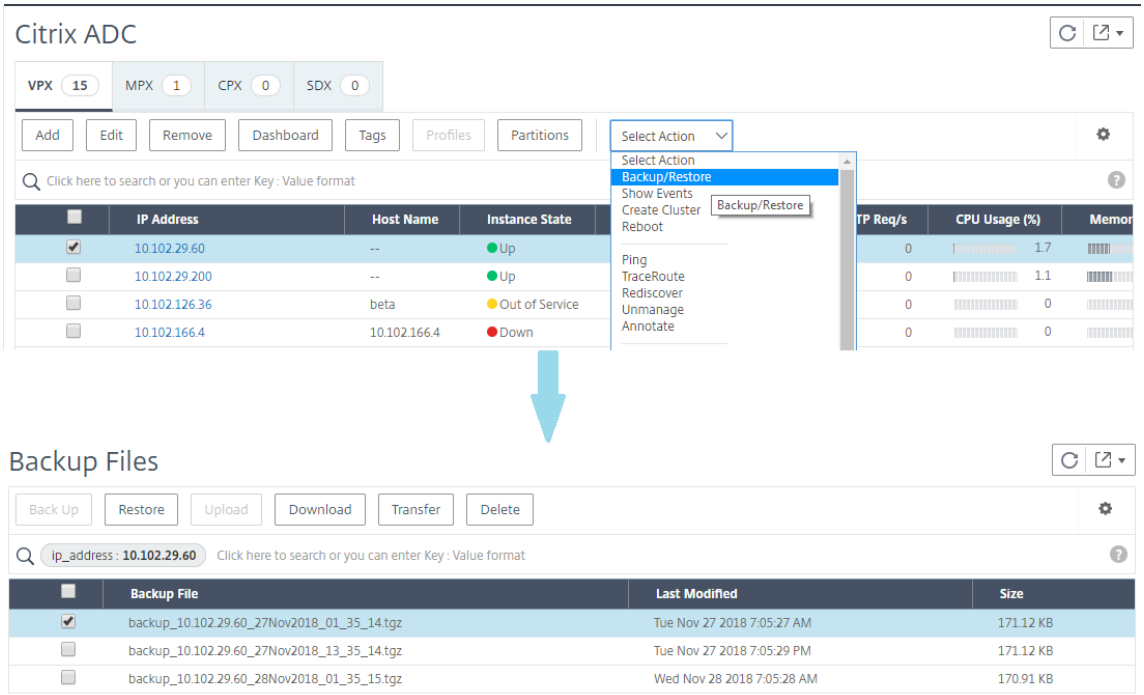
4. 您可以指定是否加密备份文件以提高安全性。您可以输入密码，也可以使用之前在 实例备份设置页面上指定的全局密码。
5. 单击 继续。

使用 **NetScaler ADM** 还原 **NetScaler** 实例

> 注意：
>
> 如果您在 HA 对中有 NetScaler 实例，则需要注意以下几点：
>
> - 恢复创建备份文件的同一个实例。例如，让我们考虑一下从 HA 对的主实例中获取备份的情况。在还原过程中，确保您恢复的是同一个实例，即使它不再是主实例。
> - 当您在主 ADC 实例上启动还原过程时，您无法访问主实例，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** 更改为 **ENABLED** 模式，并再次成为 HA 对的一部分。在还原过程完成之前，您可以预期主实例可能会停机。

执行以下任务，使用您之前创建的备份文件恢复 NetScaler 实例：

1. 导航到基础架构 **>** 实例，选择要恢复的实例，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 **NetScaler ADM** 恢复 **NetScaler SDX** 装置

在 NetScaler ADM 中，NetScaler SDX 设备的备份包括以下内容：

- 设备上托管的 NetScaler 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）
- SVM 数据库文件
- SDX 上存在的设备的 NetScaler 配置文件
- NetScaler 构建映像
- NetScaler XVA 图像，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（如果已预配）

将您的 NetScaler SDX 设备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。

如果您要使用其他 NetScaler SDX 设备的备份来恢复 NetScaler SDX 设备，请确保在开始还原过程之前添加许可证并配置新设备的管理服务网络设置，使其与备份文件中的设置相匹配。也就是说，新设备必须获得许可并满足备份文件的最低许可要求。例如，如果备份有五个 VPX 实例，总容量为 5 GB，则新设备还必须能够支持这些要求。或者，如果备份设备有白金许可证，则新设备必须具有相同或更高的许可证。必须在新设备上正确配置 IP 地址、网络掩码、网关、XenServer IP 地址和 DNS 服务器等网络设置。

在恢复 SDX 设备之前，请确保备份的 SDX 设备平台变体与设备相同。不能从另一个平台变体还原。

> 注意
>
> 在恢复 SDX RMA 设备之前，请确保备份的版本等于或高于 RMA 版本。

要从备份文件中恢复 SDX 装置，请执行以下操作：

1. 在 NetScaler ADM GUI 中，导航到 基础结构 **>** 实例 **> NetScaler**。
2. 点击 备份**/**还原。
3. 选择要恢复的同一个实例的备份文件。
4. 单击“重新打包备份”。

   备份 SDX 设备时，XVA 文件和图像将分开存储，以节省网络带宽和磁盘空间。因此，在恢复 SDX 设备之前，必须重新打包备份的文件。

   当您重新打包备份文件时，它会将所有备份文件包含在一起以恢复 SDX 设备。重新打包的备份文件可确保成功恢复 SDX 设备。
5. 选择重新打包的备份文件，然后单击“恢复”。

强制故障转移到辅助 **NetScaler** 实例

February 6, 2024

例如，如果您需要更换或升级主 Citrix Application Delivery Controller (ADC) 实例，则可能需要强制进行故障转移。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：

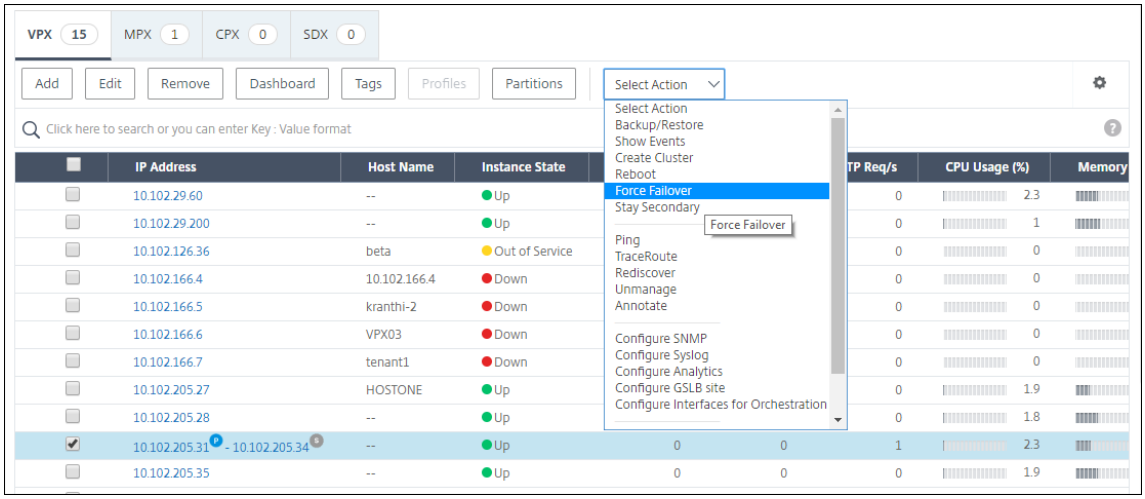
- 在独立的系统上强制执行故障转移。
- 辅助实例处于禁用或非活动状态。如果辅助实例处于非活动状态，必须等待其状态变为“UP”（运行）时才能强制执行故障转移。
- 辅助实例配置为保持辅助状态。

如果 NetScaler 实例在您运行强制故障转移命令时检测到潜在问题，则会显示一条警告消息。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 **NetScaler ADM** 强制故障切换到辅助 **NetScaler** 实例，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **>** 实例 **> NetScaler > 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“强制故障转移”。
4. 单击 **Yes**（是）确认强制执行故障转移操作。



强制辅助 **NetScaler** 实例保持辅助状态

February 6, 2024

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。

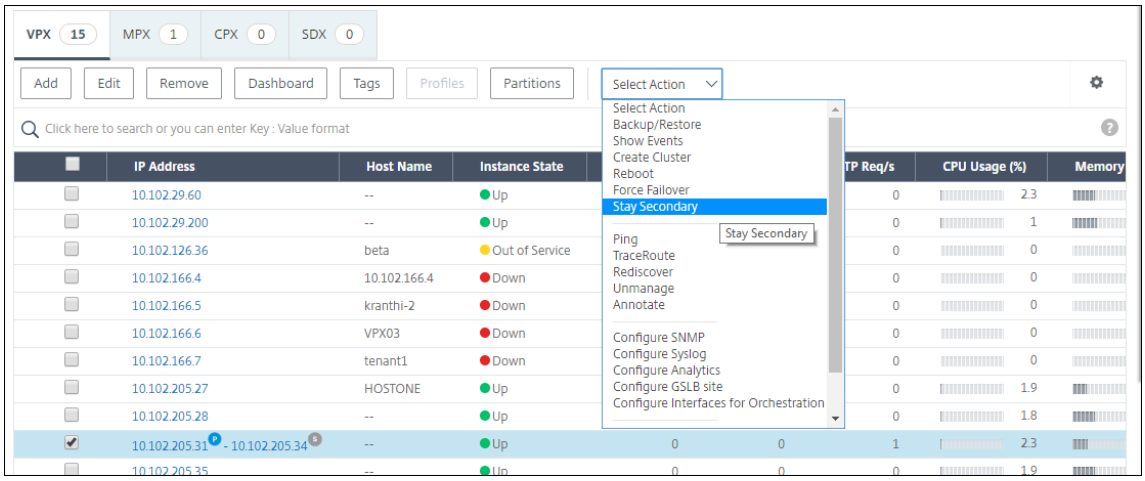
例如，假定主节点需要升级，该过程需要数秒。升级期间，主节点可能会关闭几秒钟，但您不希望辅助节点接管。即使在主节点中检测到故障，您也希望它仍然是辅助节点。

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 **NetScaler ADM** 配置辅助 **NetScaler** 实例保持辅助实例，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **>** 实例 > **NetScaler** > **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“保持辅助状态”。
4. 单击 **Yes**（是）确认执行“Stay Secondary”（保持辅助状态）操作。



创建实例组

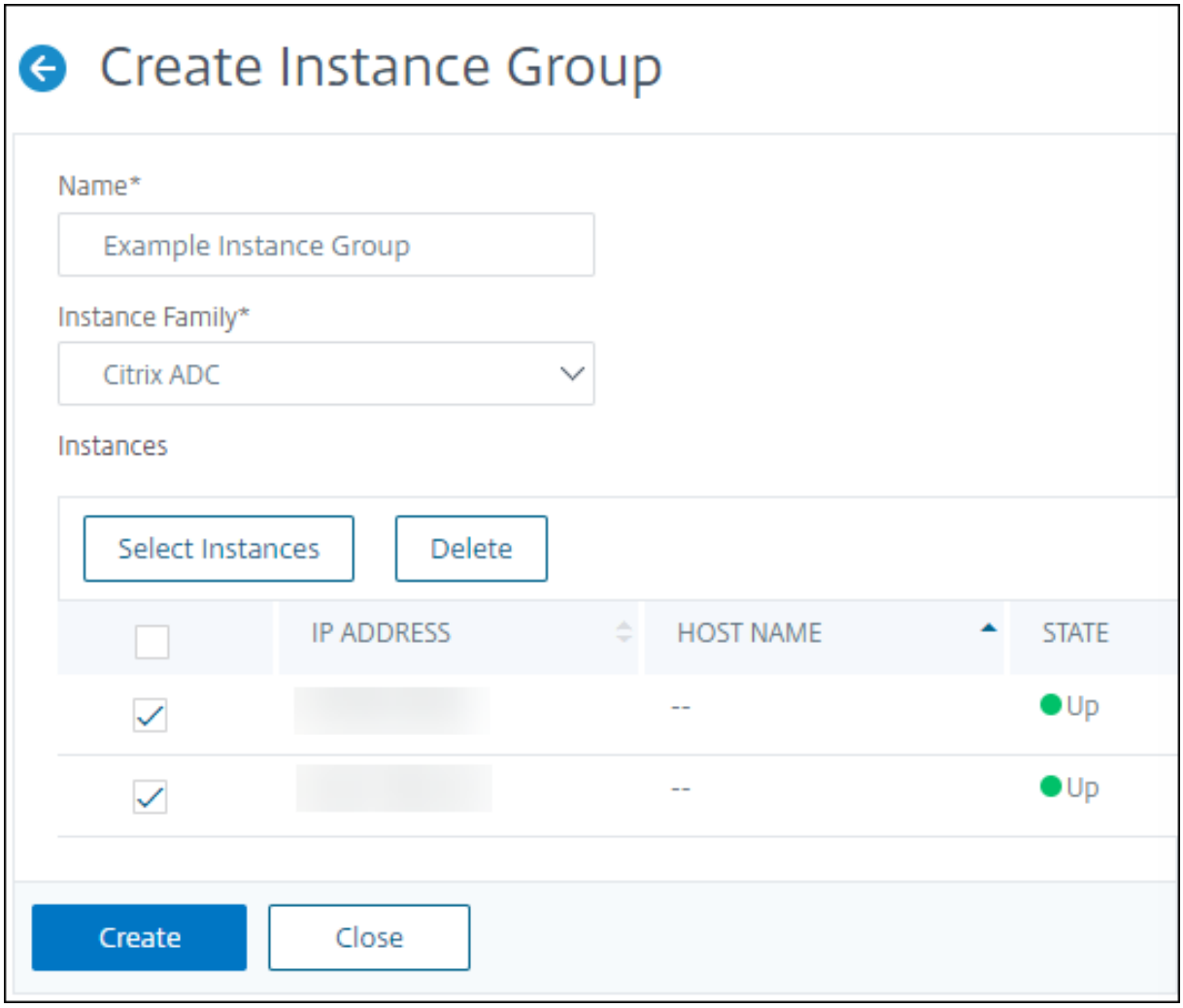
February 6, 2024

要创建实例组，必须先将所有 NetScaler 实例添加到 NetScaler ADM 中。成功添加实例后，根据实例系列创建实例组。创建一组实例可帮助您一次性对分组实例进行升级、备份或恢复。

使用 **NetScaler ADM** 创建实例组

1. 在 NetScaler ADM 中，导航到 基础架构 **>** 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 **NetScaler** 。
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。如果要从组中移除任何实例，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** 上配置 **NetScaler VPX** 实例

February 6, 2024

您可以使用 NetScaler ADM 在 SDX 设备上预置一个或多个 NetScaler 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 将限制您预配更多 NetScaler 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：

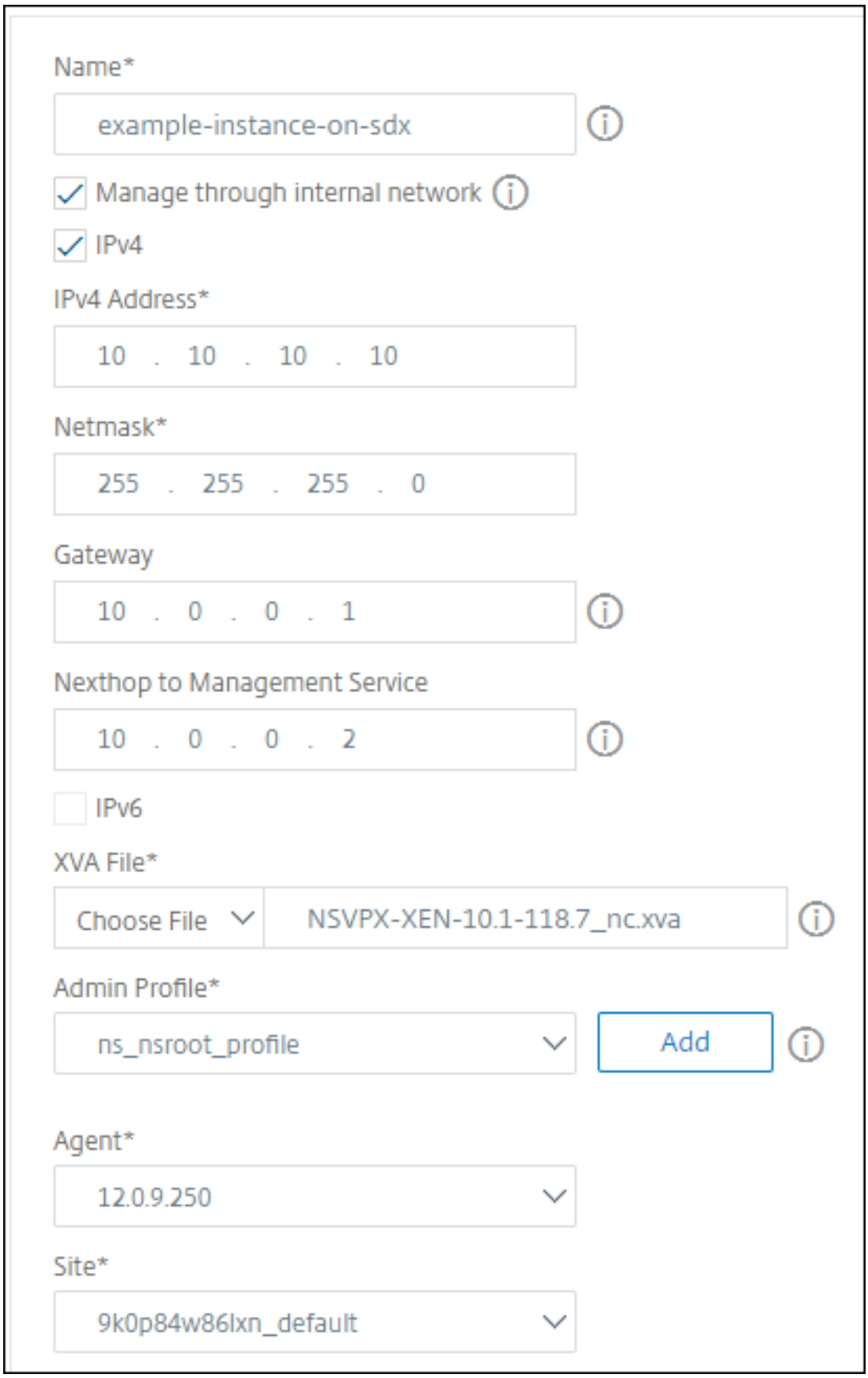
1. 导航到基础结构 **>** 实例 **> NetScaler**。
2. 在 **SDX** 选项卡中，选择要预配 VPX 实例的 SDX 实例。
3. 在 选择操作中，选择 预配 **VPX**。

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** 地址或同时选择两者来管理 NetScaler VPX 实例。VPX 实例只能有一个管理 IP（也称为 NetScaler IP）。您无法删除 NetScaler 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

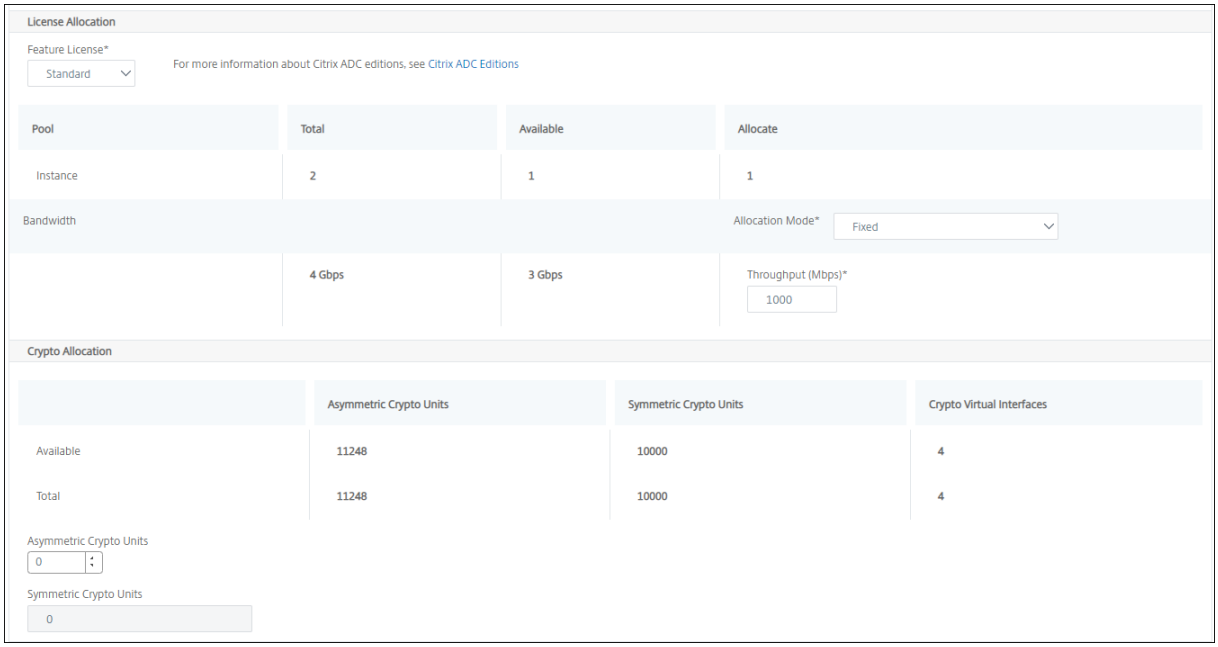
在“许可证分配”部分 中，指定 VPX 许可证。您可以使用标准、高级和高级许可证。

- 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 (用于安全 Web Gateway 的 SDX 2 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。有关更多信息，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。

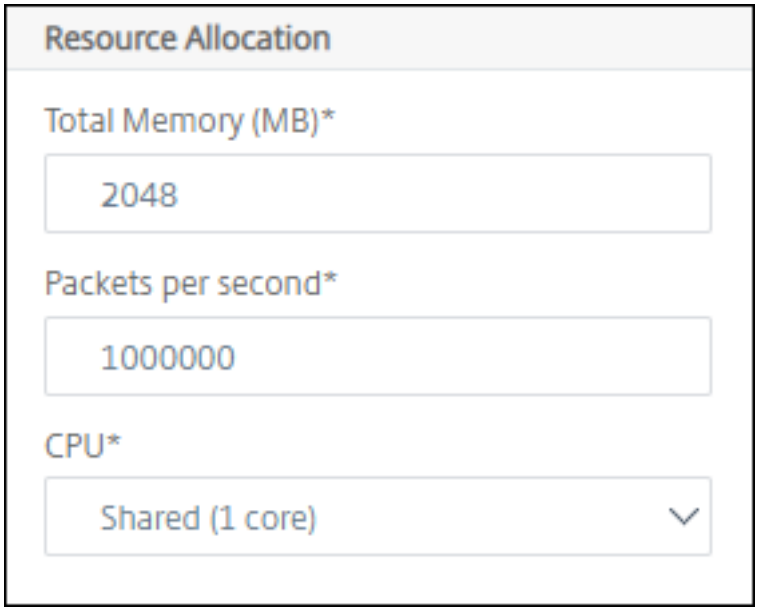
- 总内存 **(MB)** -为实例分配总内存。最小值为 2048 MB。
- 每秒数据包 数-指定每秒要传输的数据包数。
- **CPU** -指定实例的 CPU 内核数。您可以使用共享或专用 CPU 内核。

  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 预配的内核总数	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

平台名称	核心总数	可用于 VPX 预配的内核总数	可分配给单个实例的最大核心数
SDX 17550、SDX 19550、SDX 20550 和 SDX 21550	12	10	5
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
15000-50G	16	14	7

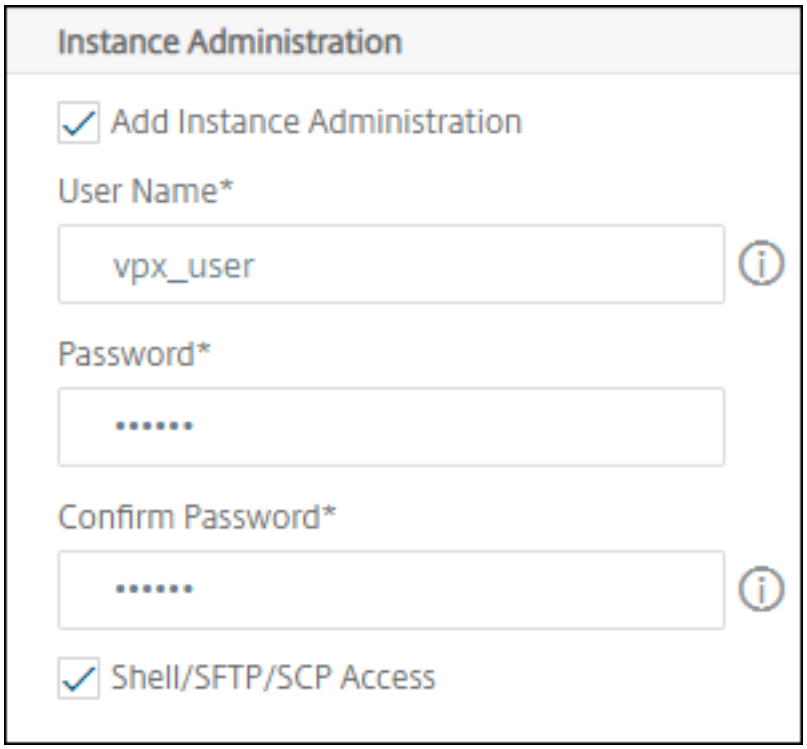
> 注意
>
> 在 SDX 26xxx 平台上，最多可以为 VPX 实例分配 26 个 CPU 内核。如果为实例分配了加密单元，则核心的最大数量取决于加密单元和数据接口的数量。
>
> 例如，如果您为实例分配 24000 个加密单位，则可以为实例分配 24 个 CPU 核心和最多两个数据接口。SDX 设备将数据接口和加密单元视为 PCI 设备。对于 26000 个加密单元，VPX 实例配置失败，因为没有添加数据接口的空间。

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：NetScaler 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。
- **Shell/Sftp/Scp** 访问权限：允许给 NetScaler 实例管理员的访问权限。此选项默认处于选中状态。



步骤 **5-**指定网络设置

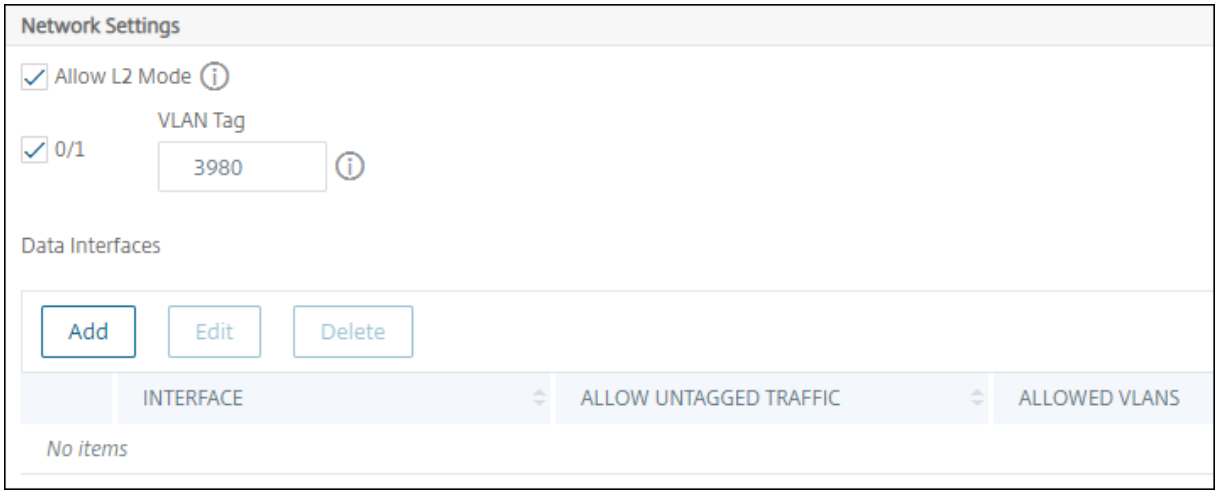
为实例选择所需的网络设置：

- 在网络设置下允许 **L2** 模式 -您可以在 NetScaler 实例上允许 L2 模式。选择“网络设置”下的“允许 L2 模式”。在登录实例并启用 L2 模式之前。有关更多信息，请参阅在 NetScaler 实例上允许 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 NetScaler 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。



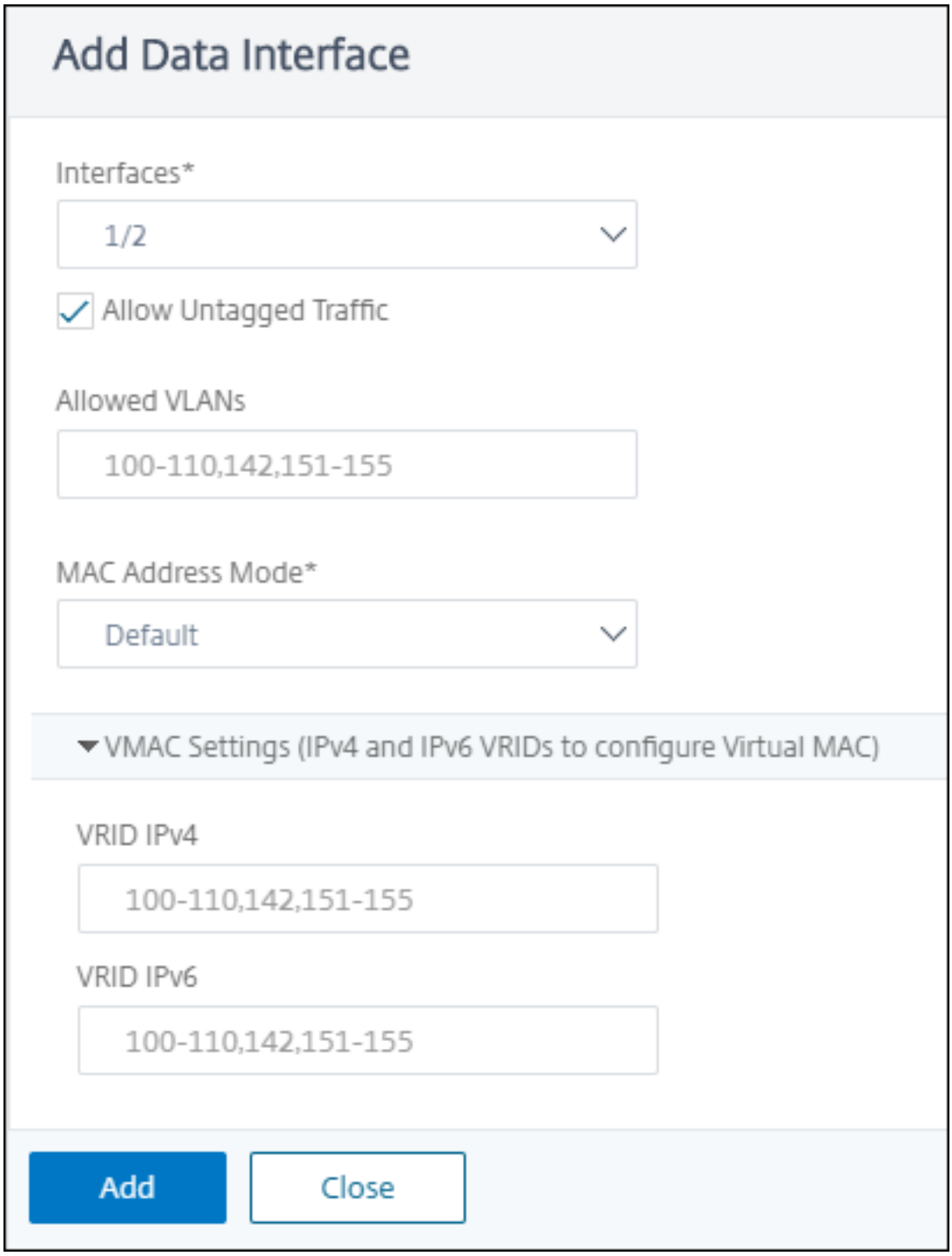
在 数据接口中，单击 添加 以添加数据接口并指定以下内容：

- 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 ID 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 NetScaler 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。
- 虚拟 **MAC** 设置（用于配置虚拟 **MAC** 的 **IPv4** 和 **IPv6** 虚拟视频识别）

- **VRID IPV4** -标识 VMAC 的 IPv4 VRID。可能的值：1—255。有关更多信息，请参阅在接口上配置 VMAC。
- VRID IPv6 - 标识 VMAC 的 IPv6 VRID。可能的值：1—255。有关更多信息，请参阅在接口上配置 VMAC。



单击添加。

步骤 6-指定管理 VLAN 设置

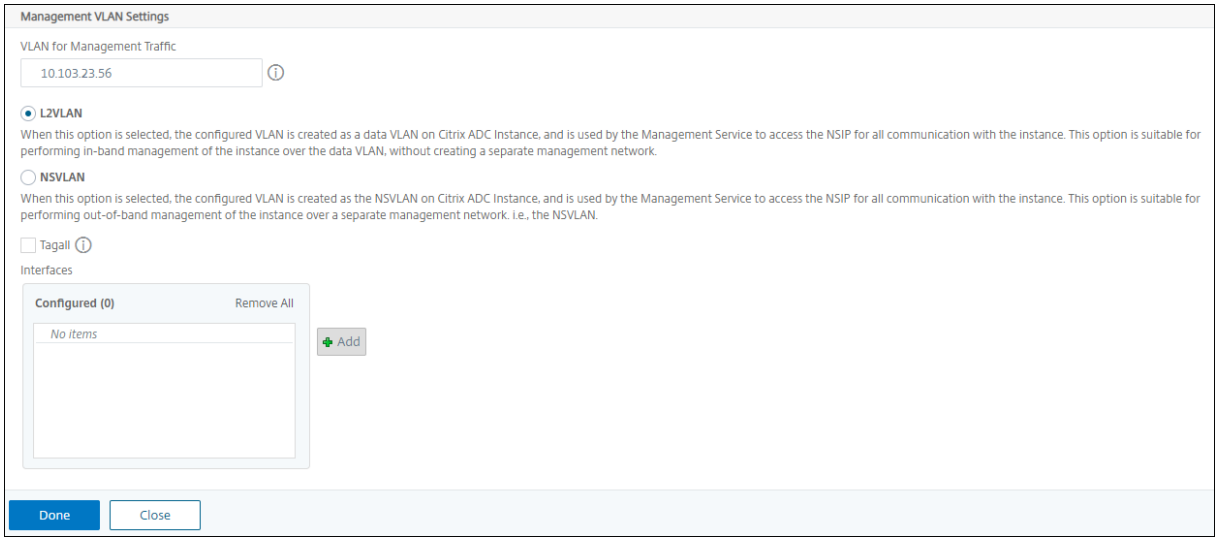
VPX 实例的管理服务和管理地址 (NSIP) 位于同一子网中，通信通过管理接口进行。

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
>
> - 预配 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。

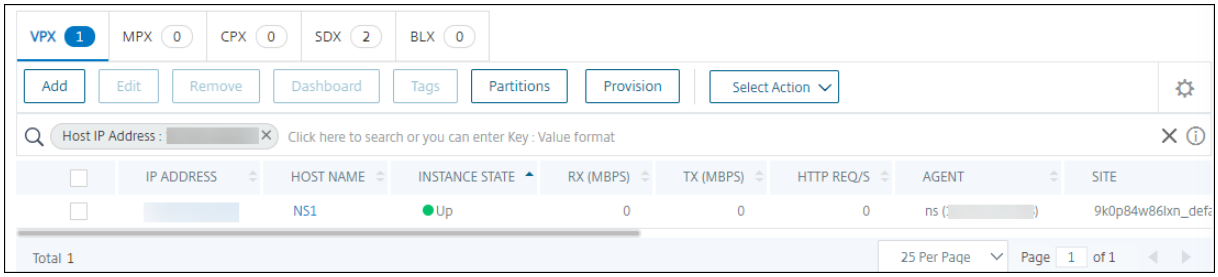


单击“完成”以配置 VPX 实例。

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. 导航到基础结构 **>** 实例 **> NetScaler**。
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 **NetScaler VPX** 实例

February 6, 2024

您可以在 NetScaler Application Delivery Management (ADM) 设置中重新发现多个 NetScaler VPX 实例。此外，当您想要查看多个 NetScaler VPX 实例的最新状态和配置时，可以重新发现这些实例。NetScaler ADM 服务器重新发现所有 NetScaler VPX 实例，并检查 Citrix Application Delivery Controller (ADC) 实例是否可访问。

要重新发现多个 **NetScaler VPX** 实例，请：

1. 在网络浏览器中，键入 NetScaler 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 基础架构 **>** 实例 **> NetScaler> 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”。

   屏幕会报告重新发现每个 NetScaler VPX 实例的进度。

取消托管实例

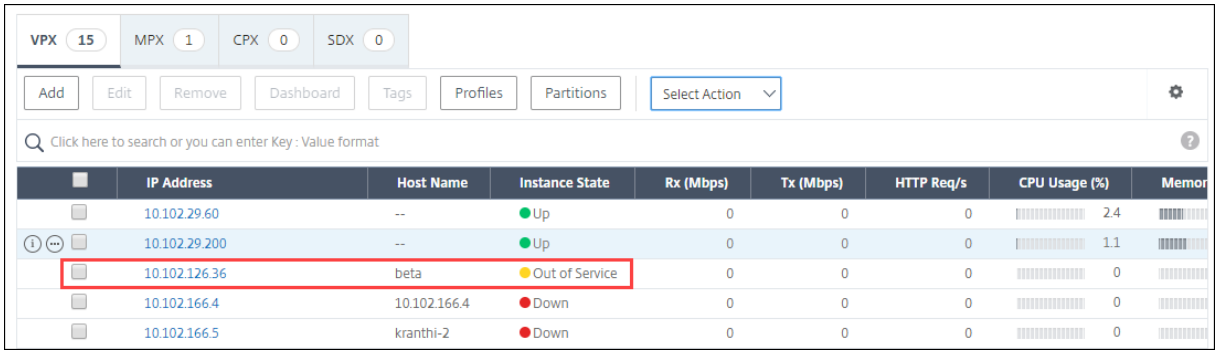
February 6, 2024

如果您想停止 NetScaler Application Delivery Management (ADM) 与网络中的实例之间的信息交换，则可以取消对实例的管理。

要取消管理实例，请执行以下操作：

导航到 基础架构 **>** 实例 **> NetScaler** > **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。



该实例不再由 NetScaler ADM 管理，也不再与 NetScaler ADM 交换数据。

跟踪到实例的路由

February 6, 2024

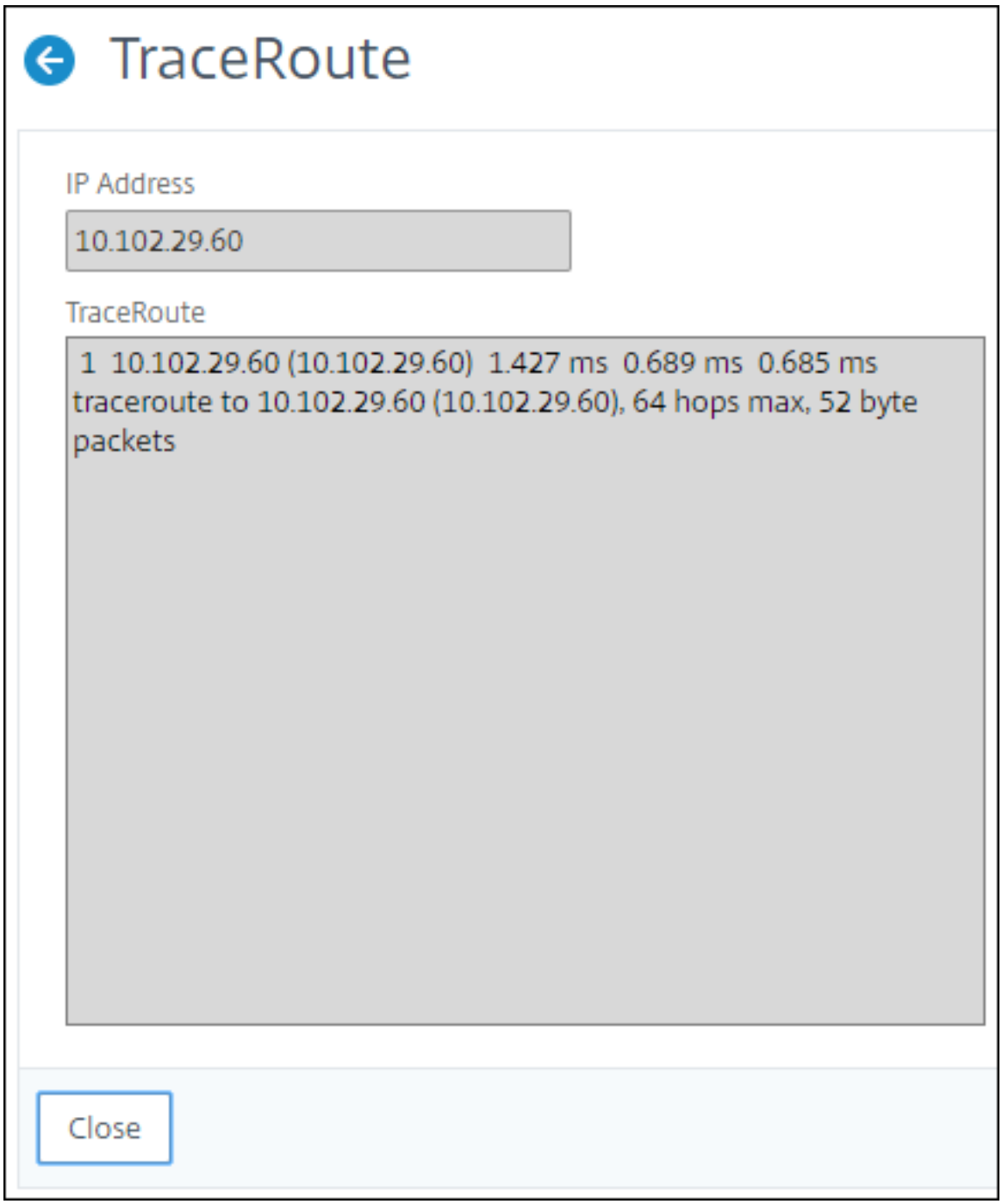
通过跟踪数据包从 NetScaler Application Delivery Management (ADM) 到实例的路径，您可以找到到达该实例所需的跳数等信息。Traceroute 会跟踪数据包从源到目标的路径。它显示网络跃点列表以及路由中每个实体的主机名和 IP 地址。

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，路由跟踪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 NetScaler ADM 中，导航到 基础架构 **>** 实例 **> NetScaler** > **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径以及每跳所消耗的时间量（以毫秒为单位）。



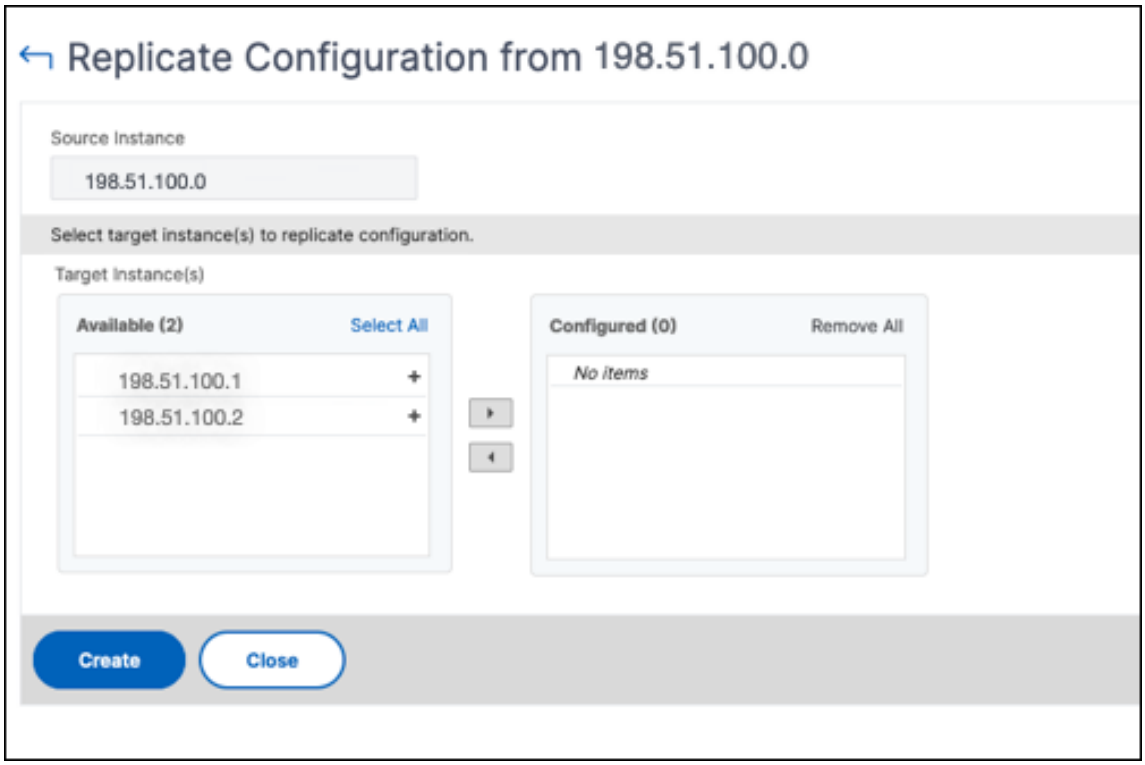
将配置从一个 **NetScaler** 实例复制到另一个实例

February 6, 2024

您可以使用 NetScaler ADM 的复制配置功能从 NetScaler 实例复制配置，然后将其复制到单个或多个实例上。

将配置从一个实例复制到其他 **NetScaler** 实例

1. 导航到基础结构 **>** 实例 **> NetScaler**。选择要在其他实例上复制其配置的源实例，然后从“选择操作”列表中单击“复制配置”。
2. 在 复制配置中，选择要应用源实例配置的目标实例。您可以将配置从单个源实例复制到单个实例或多个目标实例。



3. 单击创建。

复制的配置将添加到 NetScaler 实例列表中。要查看已复制实例的状态，请单击刷新图标。

> 注意：
>
> 在复制过程中，源实例的所有网络 IP 都将复制到目标实例。如果目标实例与源实例位于不同的网络中，则可能无法访问目标实例中的 IP。当无法访问 IP 时，目标实例中实体的状态显示为“关闭”。
>
> 要查看在托管 NetScaler 实例上配置的实体的状态，请导航到基础架构 **>** 网络功能。

SSL 证书管理

February 6, 2024

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 事务的一部分，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 Application Delivery Controller (ADC) 设备上，用于完成非对称密钥（或公钥）加密和解密。

NetScaler Application Delivery Management (ADM) 为您提供统一控制台，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。NetScaler 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：

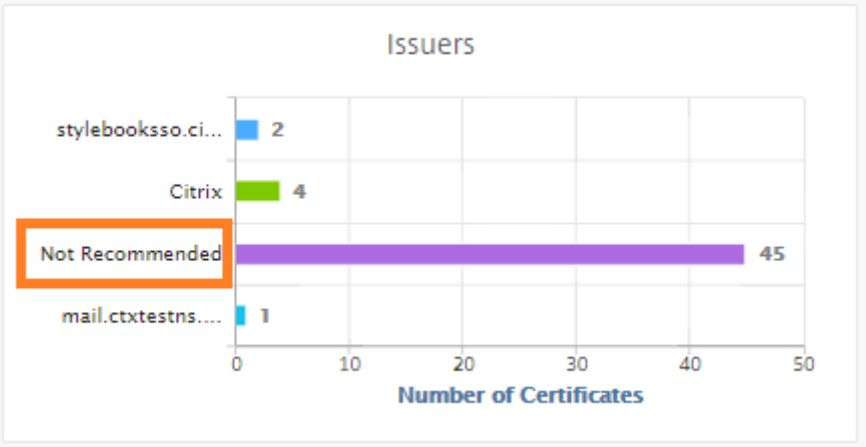
- 来自授权证书颁发机构 (CA)，例如威瑞信
- 通过在 NetScaler 设备上生成新的 SSL 证书和密钥

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，NetScaler 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。

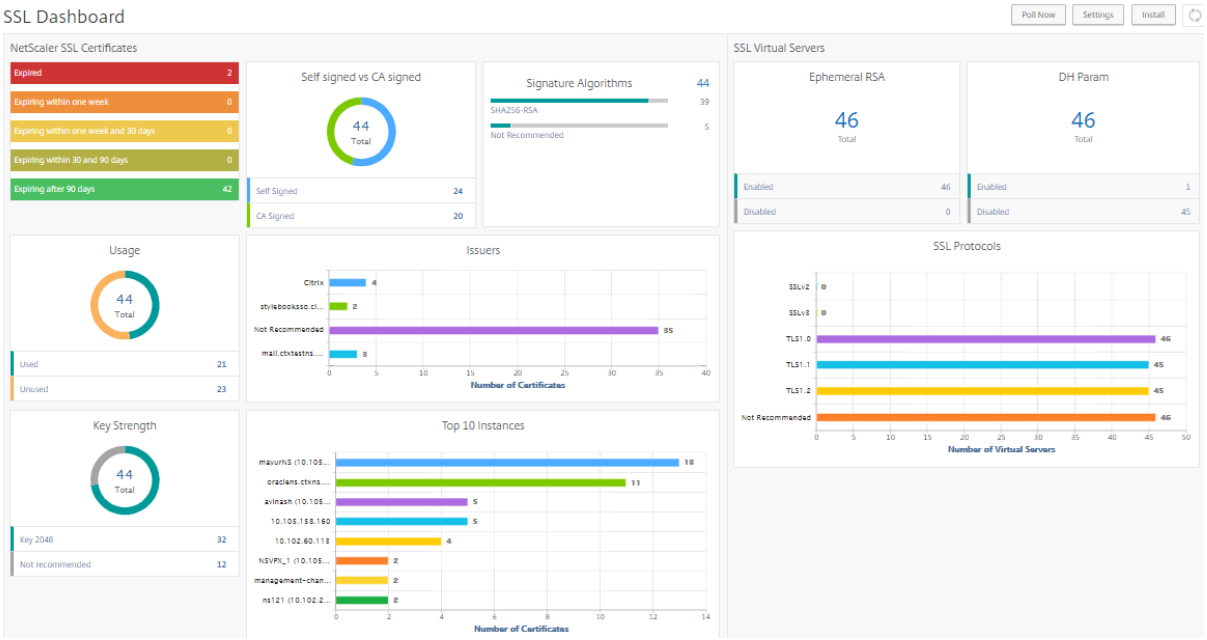


> 注意
>
> “不推荐”证书根据不同的参数进行分类，您可以在相关组件中查看它们。

NetScaler ADM 证书的工作原理

SSL 控制板为您提供了在不同 NetScaler 实例上安装的所有 SSL 证书的直观演示。SSL 控制板包括 NetScaler 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 NetScaler 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 NetScaler 实例管理和监视证书。

安装 **SSL** 证书

想象一下，您有一个 NetScaler 实例队列，您必须在其上部署所需的 SSL 证书。NetScaler ADM 为您提供了一个统一的控制台，用于一次尝试在多个 NetScaler 实例之间部署 SSL 证书。

例如，您可能希望在一个或多个 NetScaler 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 NetScaler 实例上安装 SSL 证书的手动干预。您可以跨一个或多个 NetScaler 实例批量安装 SSL 证书。

要获取 SSL 证书的摘要，请登录 **NetScaler ADM**，然后导航到 基础架构 **> SSL** 控制面板。

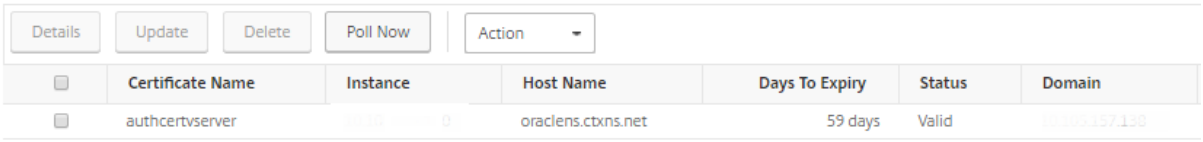
证书到期的通知设置

在此使用案例中，您可能跨多个 NetScaler 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 NetScaler 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 NetScaler 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：

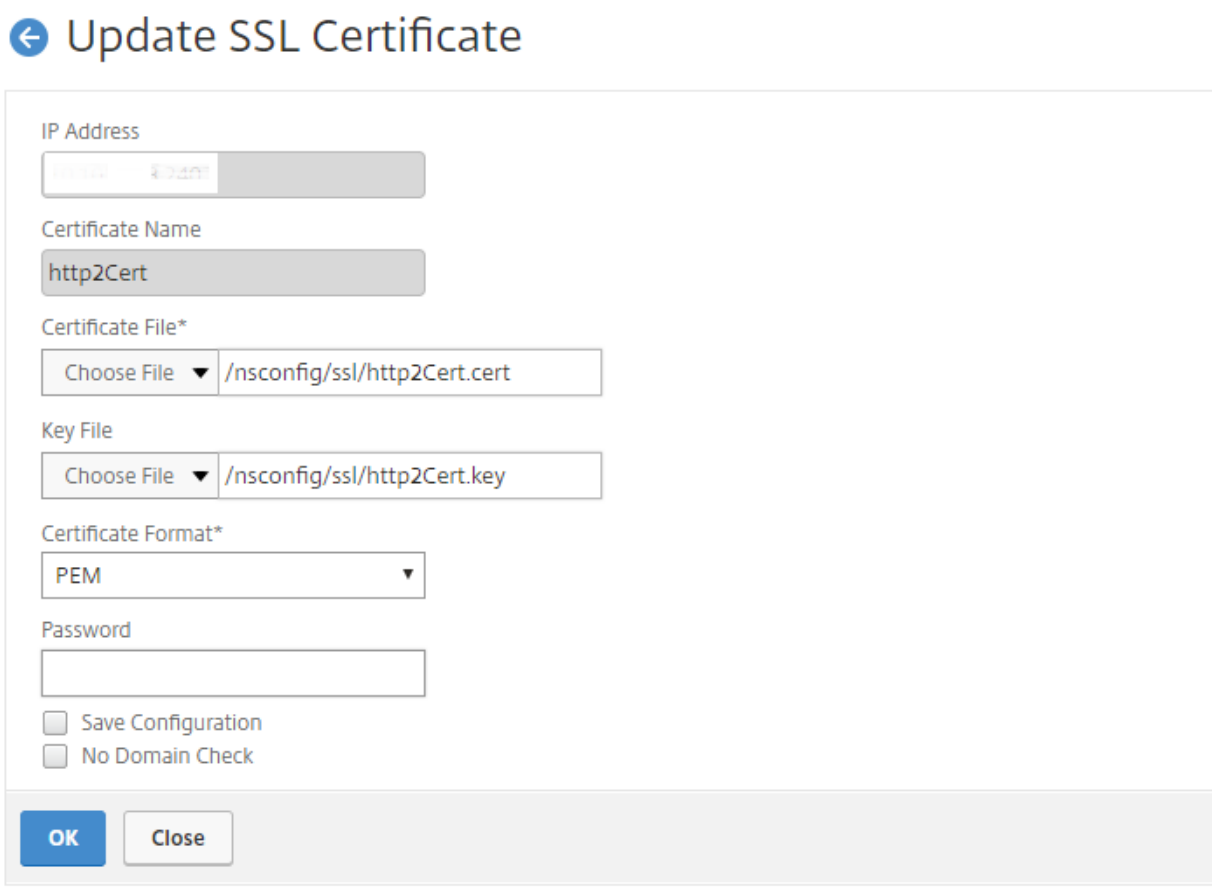
更新现有证书　在此使用案例中，您必须在收到证书颁发机构 (CA) 的续订证书后更新现有证书。现在，您可以从 NetScaler ADM 更新现有证书，而无需登录 NetScaler 实例。

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 NetScaler ADM 更新 SSL 证书，而不是转到 NetScaler 设备。

要更新任何证书，请登录 NetScaler ADM，然后导航到 基础架构 **> SSL** 控制面板。

选择要更新的证书，然后单击 更新。

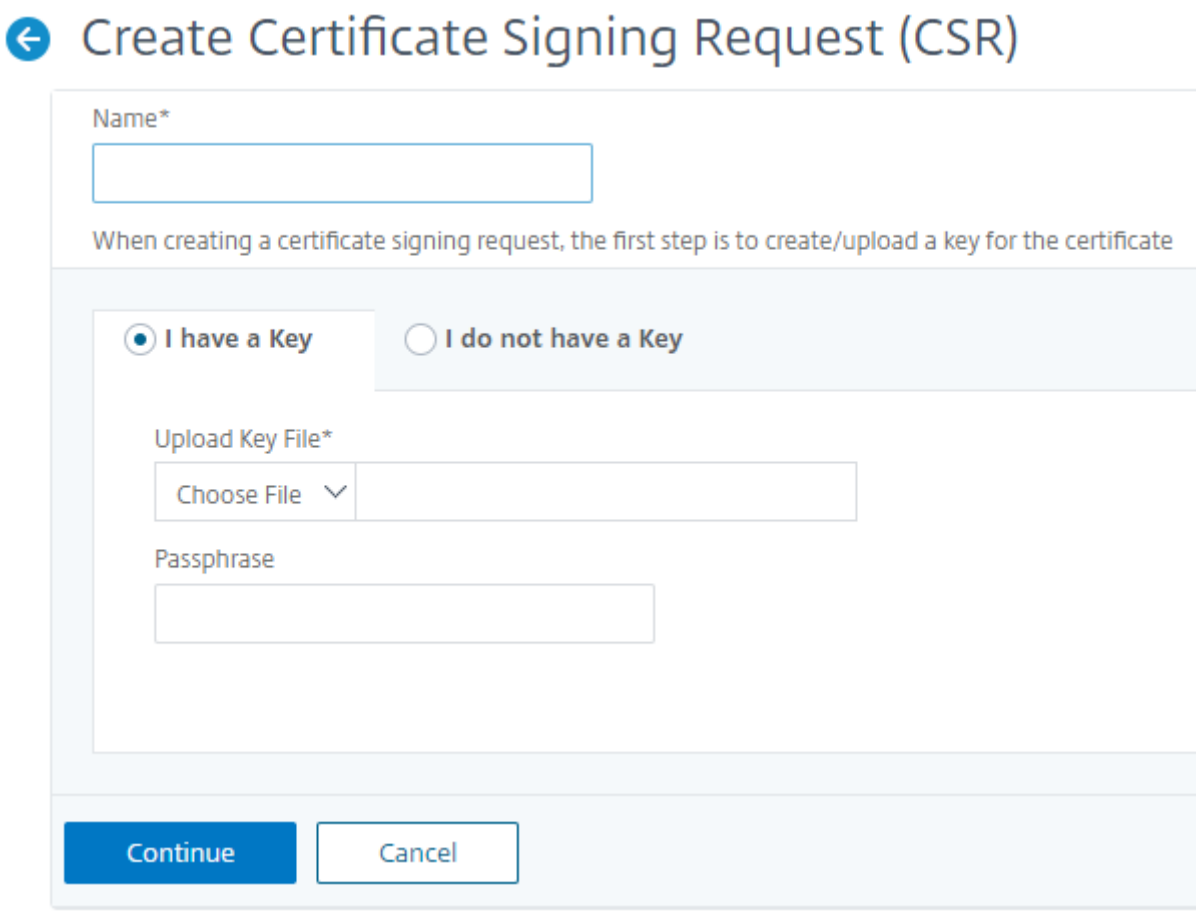
您可以选择更新 NetScaler ADM 所选证书的相关字段。



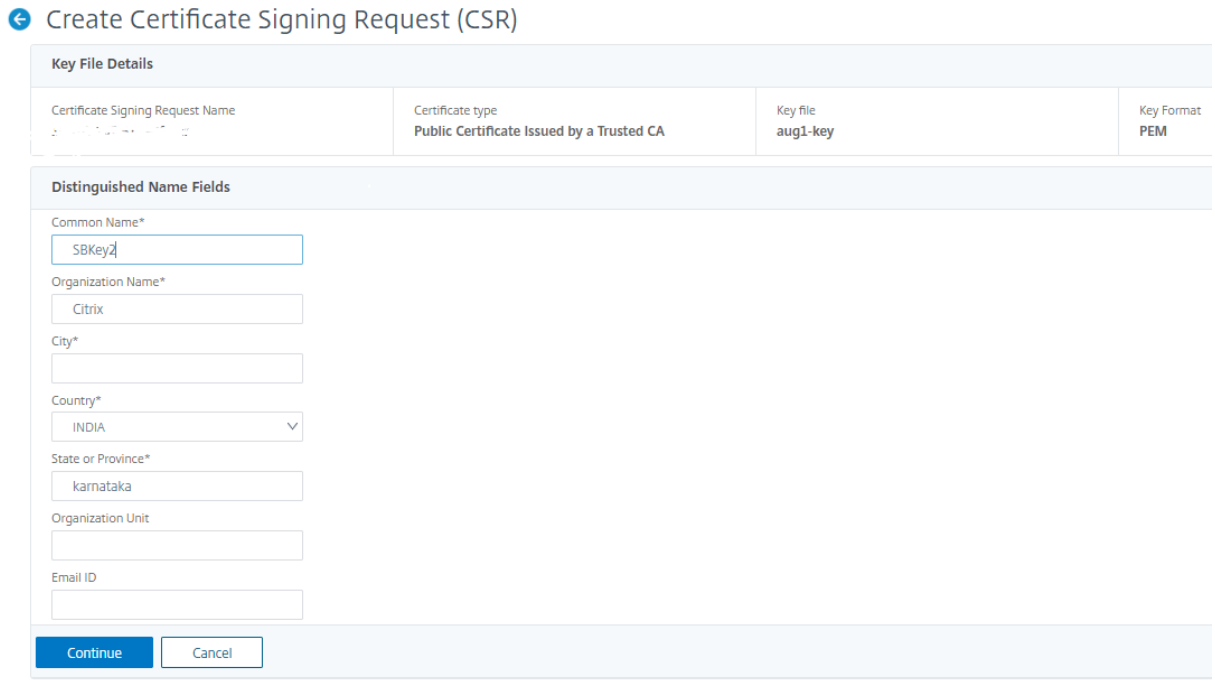
创建证书签名请求　想象一下，其中一个 SSL 证书不符合组织策略的使用案例。您想从证书颁发机构获得新证书。您现在可以从 NetScaler ADM 生成证书签名请求 (CSR)。可以将 CSR 和公钥发送到 CA 以获取 SSL 证书。

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。要上载密钥，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。

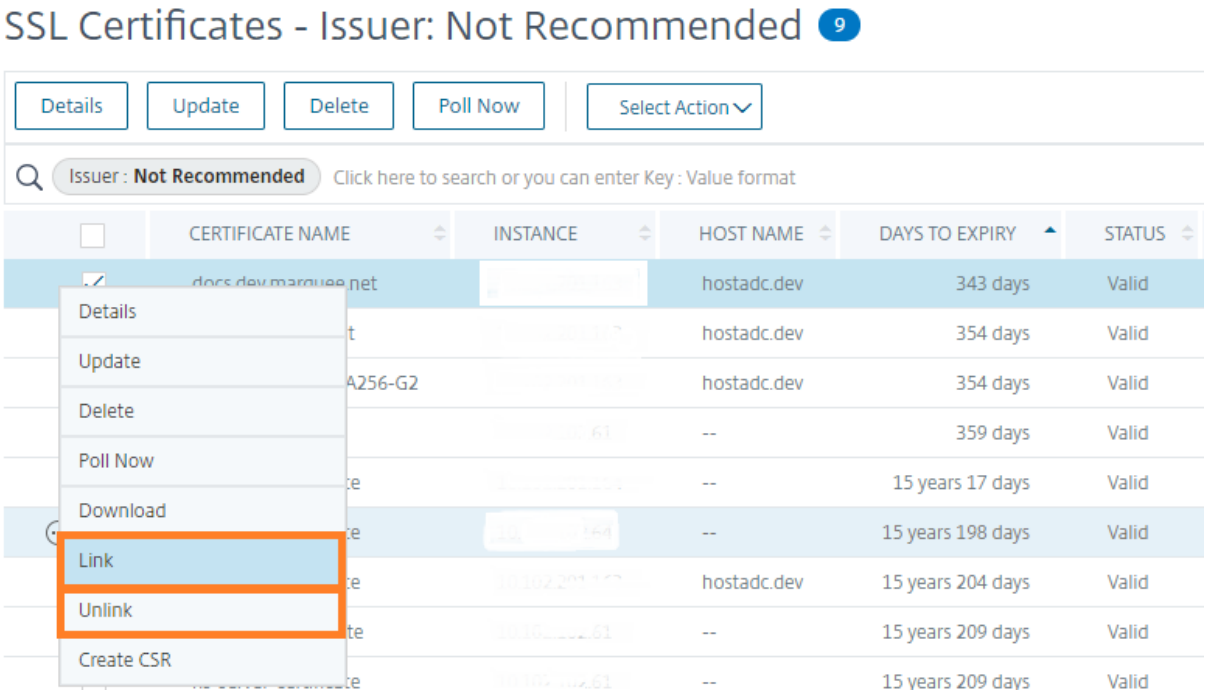


提供所选密钥（如公用名称、组织名称、城市、国家/地区、州、组织单位和电子邮件 ID）的更多详细信息，以创建 CSR。



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。

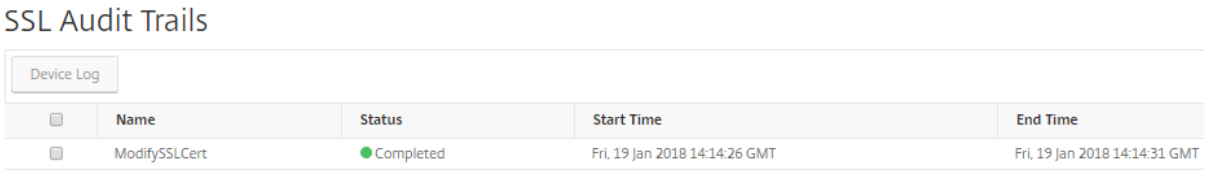


审核日志

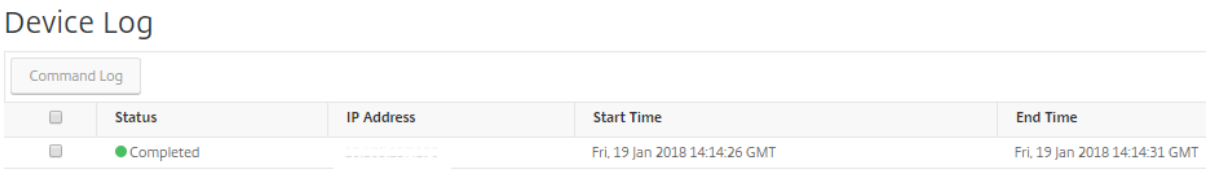
审核日志是 NetScaler ADM 生成的文本日志文件的集合。它显示了通过将 NetScaler ADM 添加、修改和更改的 SSL 证书的历史记录到特定 NetScaler 设备。审核日志还显示 NetScaler 设备的 IP 地址、状态、开始时间和特定操作的结束时间。

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。

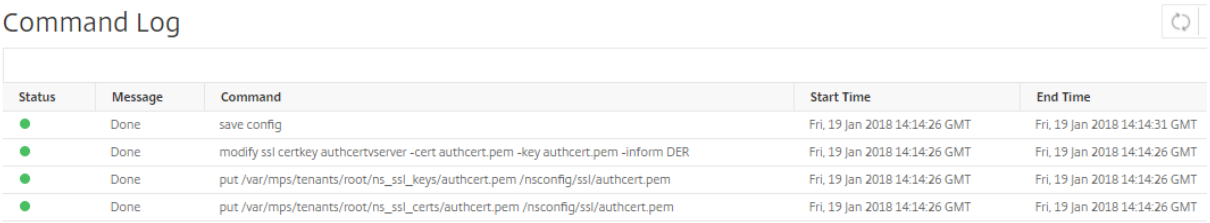
要确定 SSL 证书的信息，请在 **SSL** 控制面板上单击 审核日志。应用程序摘要包括启动时间和结束时间的 SSL 证书状态。



要确定特定 SSL 证书的 NetScaler 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** 控制板

February 6, 2024

您可以使用 NetScaler Application Delivery Management (ADM) 中的 SSL 证书控制面板来查看可帮助您跟踪证书颁发者、关键优势和签名算法的图表。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

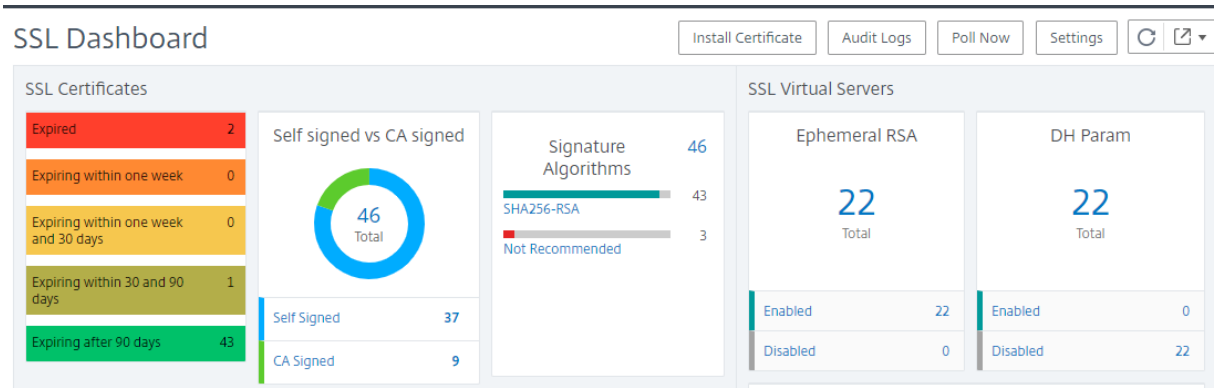
- 颁发者数
- 签名算法
- SSL 协议
- 按使用的证书数排在前 10 位的实例

监视 **SSL** 证书

如果您的公司有 SSL 策略，您定义了某些 SSL 证书要求，例如所有证书的最低密钥强度必须为 2048 位，并且必须由可信的 CA 机构授权，则可以使用 NetScaler ADM 上的 SSL 控制面板来监视您的证书。

在另一个示例中，您可能上载了新证书，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 NetScaler ADM 中监视 SSL 证书，请导航到基础架构 **> SSL** 控制面板。



NetScaler ADM 允许您轮询 SSL 证书，并立即将实例的所有 SSL 证书添加到 NetScaler ADM 中。为此，

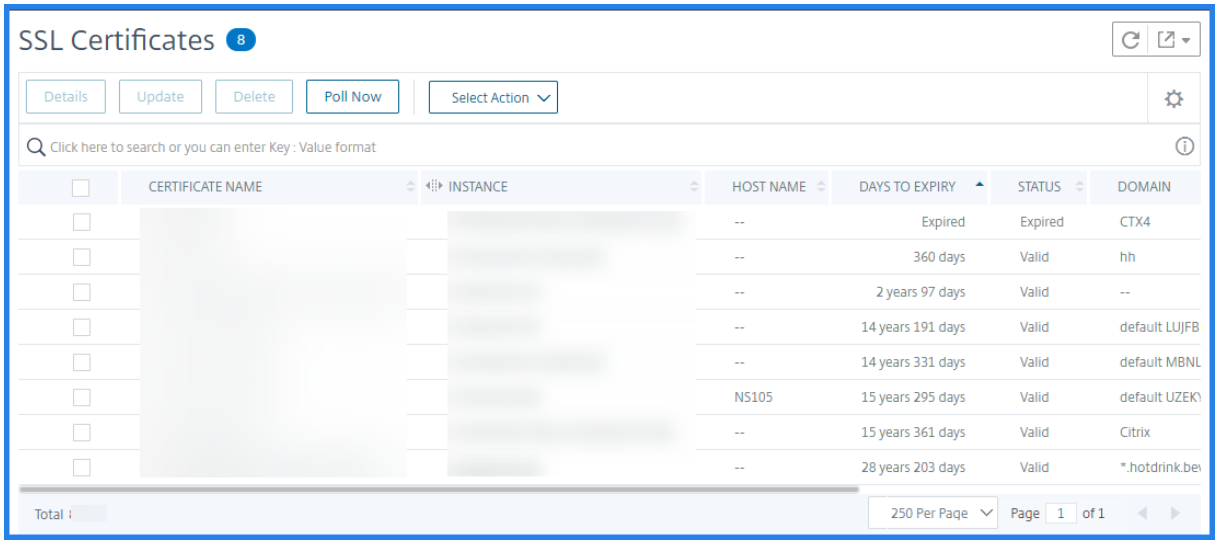
1. 导航到 基础架构 **> SSL** 控制面板。
2. 单击 立即轮询。

   在“立即轮询”页面上，您可以轮询所有托管 ADC 实例或选择特定实例。
3. 单击 开始轮询。

在 **SSL** 控制面板中，您可以监视 ADC SSL 证书、SSL 虚拟服务器和 SSL 协议。

您可以单击控制板上的指标来查看与 SSL 证书、SSL 虚拟服务器或 SSL 协议相关的详细信息。

例如，当您单击控制板上 自签名与 **CA** 签名 下的数字时，ADM GUI 将显示 NetScaler 实例上的所有 SSL 证书。



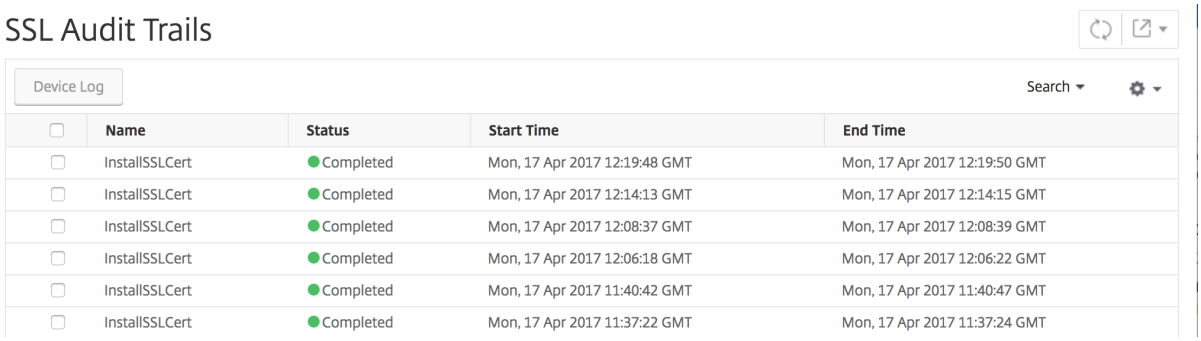
NetScaler ADM SSL 控制板还显示了虚拟服务器上运行的 SSL 协议的分布情况。作为管理员，您可以指定要通过 SSL 策略监视的协议，有关详细信息，请参阅 配置 SSL 策略。支持的协议包括 SSLv2、SSLv3、TLS 1.0、TLS 1.1、TLS 1.2 和 TLS 1.3。虚拟服务器上使用的 SSL 协议以条形图格式显示。单击特定协议会显示使用该协议的虚拟服务器列表。

在 SSL 控制板上启用或禁用 Diffie-Hellman (DH) 或 Ephemeral RSA 密钥后，将显示圆环图。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。

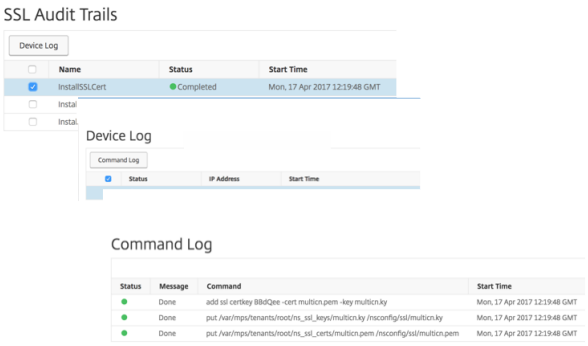
查看 **SSL** 证书的审核追踪

您现在可以在 NetScaler ADM 上查看 SSL 证书的日志详细信息。日志详细信息显示在 NetScaler 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 NetScaler ADM 上执行的特定操作的审核日志，请导航到 基础架构 **> SSL** 控制板 >，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。

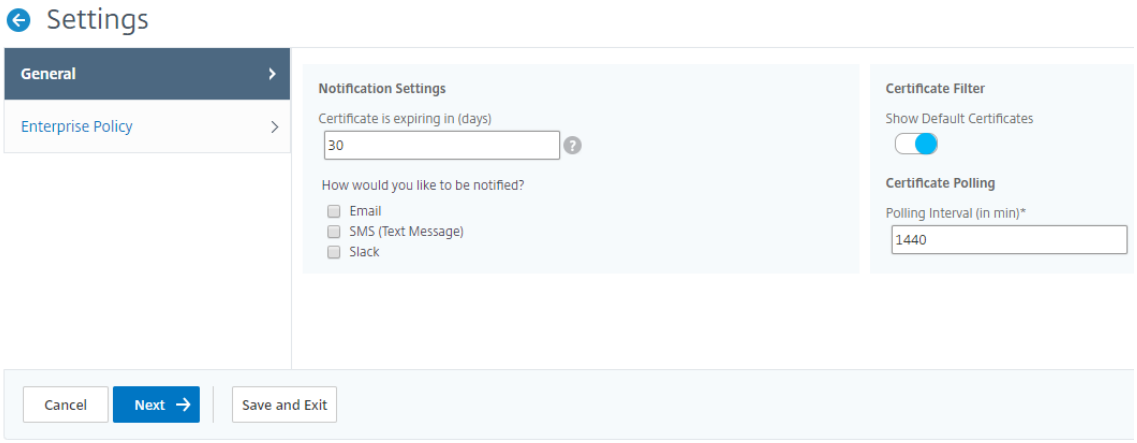


排除 **SSL** 控制板上的默认 **NetScaler** 证书

NetScaler ADM 允许您根据自己的喜好显示或隐藏 SSL 控制面板图表上显示的默认 NetScaler 证书。默认情况下，所有证书（包括默身份验证书）都显示在 SSL 控制面板上。

要在 SSL 控制板上显示或隐藏默身份验证书，请执行以下操作：

1. 导航到 NetScaler ADM GUI 中的 基础结构 **> SSL** 控制板。
2. 在“**SSL** 控制板”页面上，单击“设置”。
3. 在 设置 页面上，选择 常规。
4. 键入证书到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“显示默身份验证书”复选框，然后单击“保存并退出”。



查看、上载和下载 **SSL** 文件

要在 NetScaler ADM 上查看 SSL 文件，请导航到基础架构 **> SSL** 控制板 **> Citrix ADM** 上的 **SSL** 文件。

在此页中，您可以在 NetScaler ADM 上查看、上载和下载以下文件：

- SSL 证书
- SSL 密钥
- SSL CSR

要在 NetScaler 实例上查看和下载 SSL 文件，请导航到 NetScaler 上的基础架构 **> SSL** 控制板 **> SSL** 文件。

只有在手动或通过定时备份过程备份 NetScaler 实例之后，您才能访问 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 证书过期通知

February 6, 2024

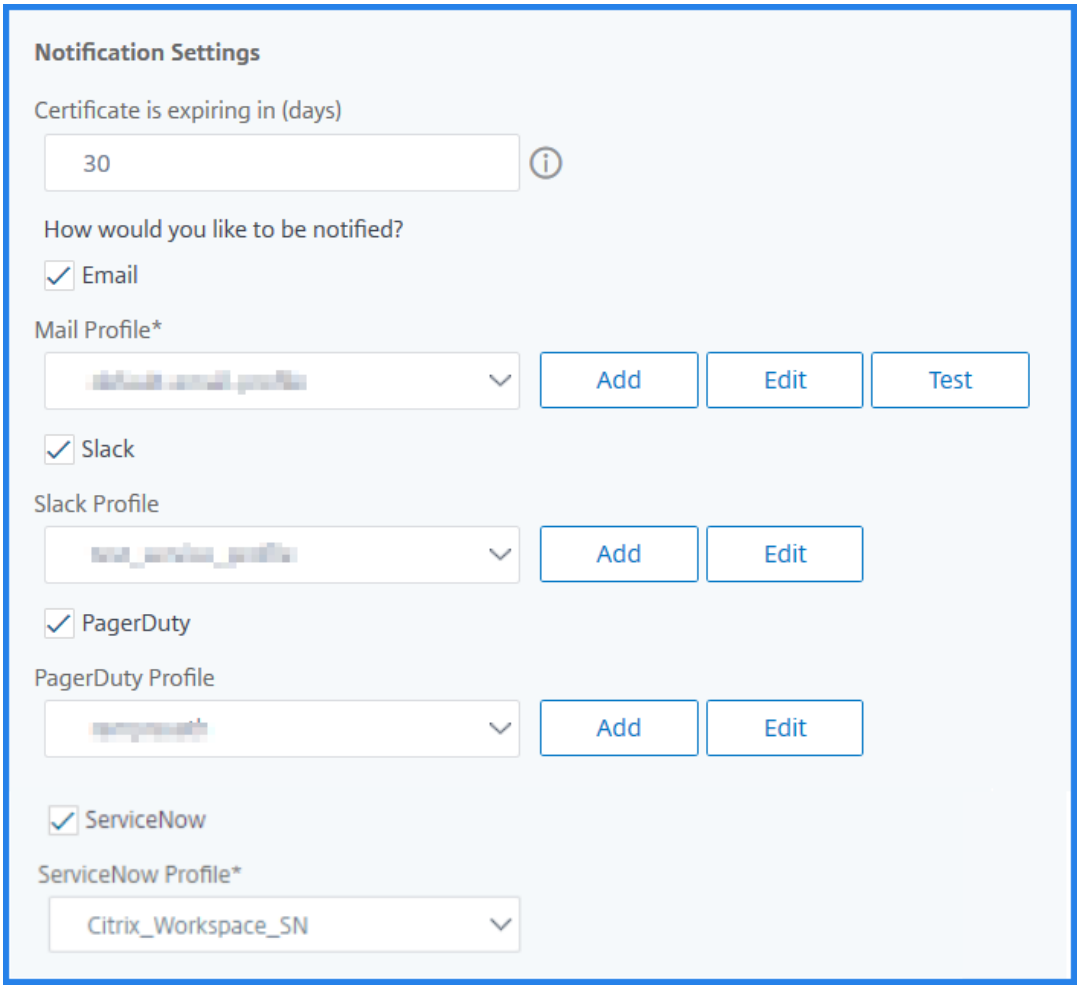
作为安全管理员，您可以设置通知，在证书即将到期时通知您，并包含有关哪个 Citrix Application Delivery Controller (ADC) 实例使用这些证书的信息。通过启用通知，您可以及时续订您的 SSL 证书。

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 **NetScaler ADM** 的通知，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **> SSL** 控制面板。
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。
    - **PagerDuty** 警报 - 指定 PagerDuty 配置文件。根据在 PagerDuty 门户中配置的通知设置，当证书即将过期时，系统会发送通知。
    - **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
      >
      > 确保 Citrix Cloud ITSM 适配器已配置为 ServiceNow 并与 NetScaler ADM 集成。有关更多信息，请参阅 将 NetScaler ADM 与 ServiceNow 实例集成。



6. 点击 保存并退出。

现在，当您的 SSL 证书到期时，NetScaler 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，NetScaler ADM 会发送陷阱：

- 您已在 SSL 控制面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“设置”**>**“**SNMP**”**>**“陷阱目的地”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”（不带引号）作为社区字符串。

更新已安装的证书

February 6, 2024

从证书颁发机构 (CA) 收到续订的证书后，您可以更新来自 NetScaler Application Delivery Management (ADM) 的现有证书，无需登录单个 Citrix Application Delivery Controller (ADC) 实例。

要从 **NetScaler ADM** 更新 **SSL** 证书、密钥或两者，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **> 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 证书以查看其详细信息，然后单击 **SSL** 证书 页面右上角的 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 **NetScaler** 实例上安装 **SSL** 证书

February 6, 2024

在 Citrix Application Delivery Controller (ADC) 实例上安装 SSL 证书之前，请确保证书由可信 CA 颁发。此外，请确保证书密钥的密钥强度为 2048 位或更高，并且密钥使用安全签名算法进行签名。

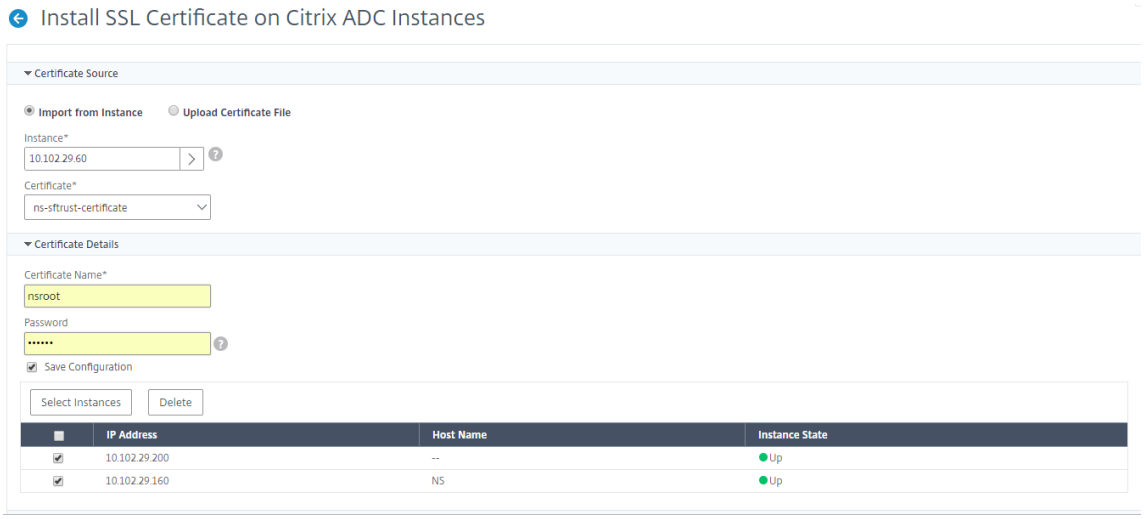
要从另一个 **NetScaler** 实例安装 **SSL** 证书，请执行以下操作：

您也可以从选定的 NetScaler 实例导入证书，然后从 NetScaler Application Delivery Management (ADM) GUI 将其应用到其他目标 NetScaler 实例。

1. 导航到 基础结构 **> SSL** 控制面板。
2. 在 SSL 控制板的右上角，单击 安装。
3. 在 **NetScaler** 实例上安装 **SSL** 证书页面上，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。

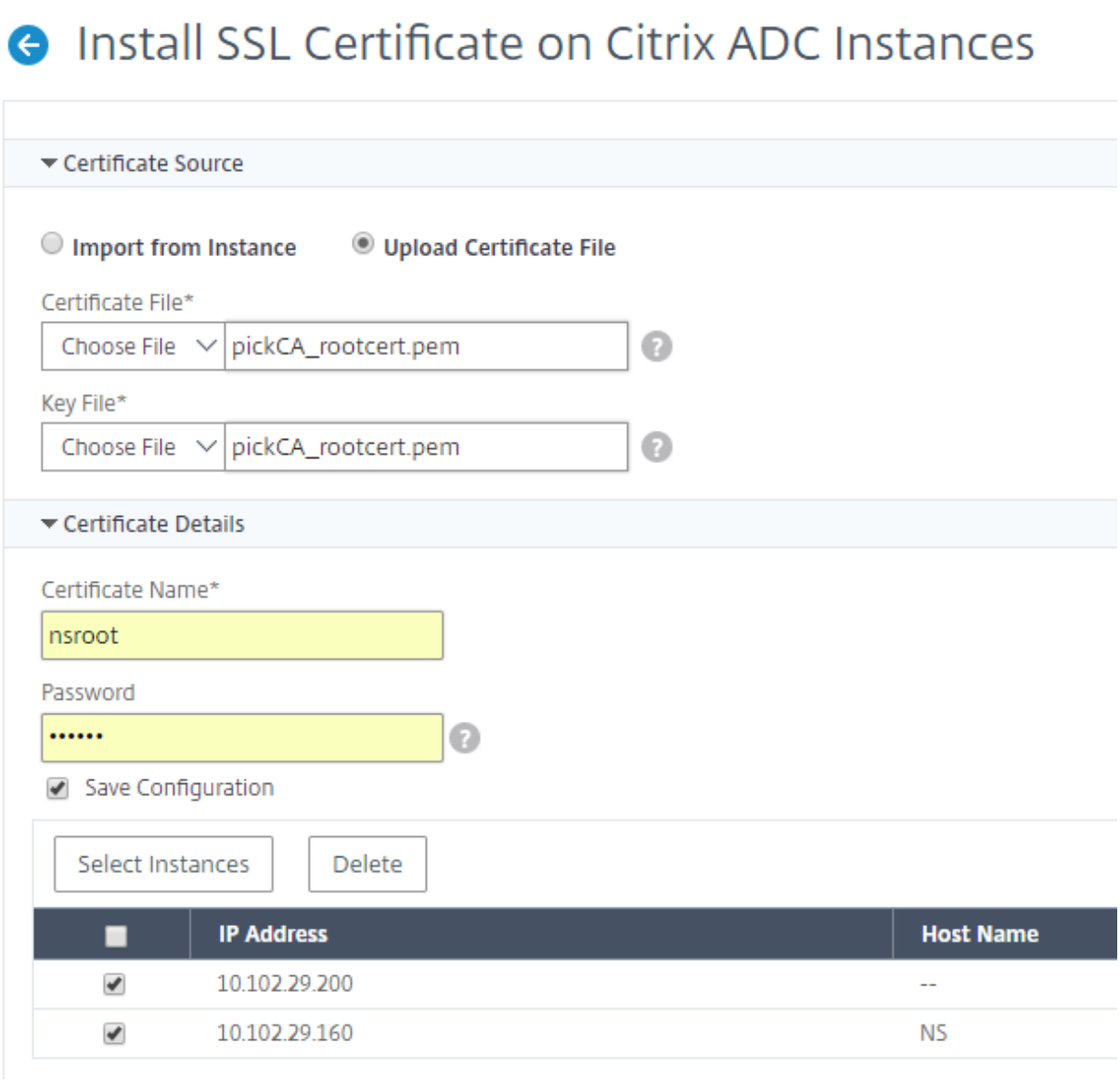
   b) 证书详细信息
      - 证书名称。指定证书密钥的名称。
      - 密码。用于加密私钥的密码。可以使用此选项上载加密的私钥。
4. 单击“选择实例”以选择要安装证书的 NetScaler 实例。

5. 单击确定。



要从 **NetScaler ADM** 安装 **SSL** 证书，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **> SSL** 控制板。
2. 在控制板的右上角，单击 **Install**（安装）。
3. 在“在 **NetScaler** 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 NetScaler ADM 虚拟实例上）来上载 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 NetScaler ADM 实例。
4. 要保存配置以备将来使用，请选中“保存配置”复选框。
5. 单击确定。



创建证书签名请求 (CSR)

February 6, 2024

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 **NetScaler ADM** 创建 **CSR**，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **> SSL** 控制面板。
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。要上载密钥文件，请选择本 地（您的本地计算机）或 设备（密钥文件必须存在于 NetScaler 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。

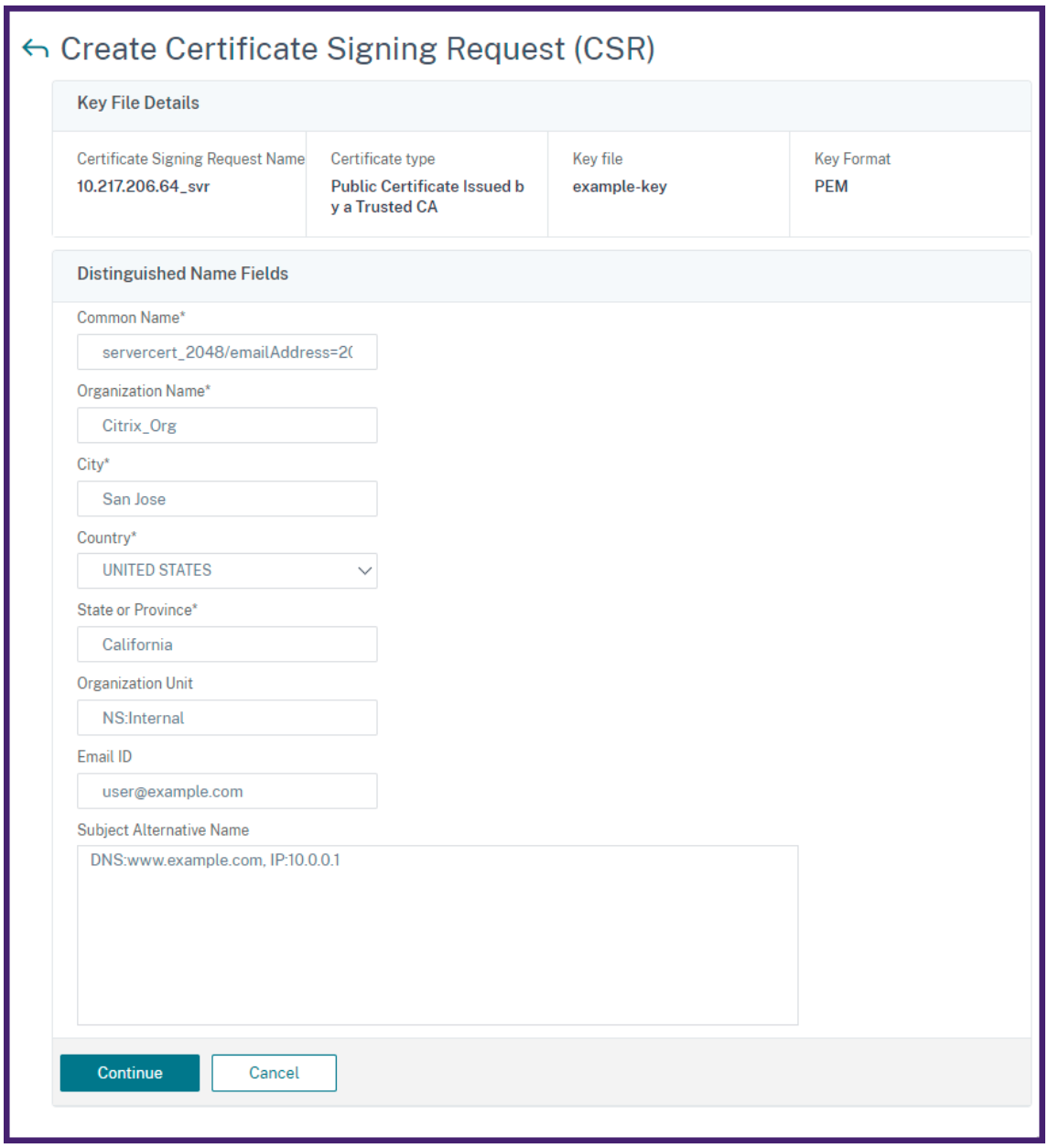
5. 单击继续。
6. 在下一页中，提供更多详细信息。

   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

February 6, 2024

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 **NetScaler ADM** 将一个 **SSL** 证书链接到另一个证书，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **> SSL** 控制面板。
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 **NetScaler ADM** 取消 **SSL** 证书的链接，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **> 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

February 6, 2024

您可以在 NetScaler Application Delivery Management (ADM) 中配置企业策略并添加所有可信 CA、安全签名算法，并为您的证书密钥选择推荐的密钥强度。如果 Citrix Application 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 证书控制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推荐的密钥强度不匹配，SSL 证书控制板会将这些密钥的强度显示为“不推荐”。

要在 **NetScaler ADM** 上配置企业策略，请执行以下操作：

1. 在 **NetScaler ADM** 中，导航到基础架构 **>**SSL 控制面板，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、安全签名算法，然后为您的证书和密钥选择推荐的密钥强度。
3. 单击 **Save**（保存）以保存企业策略。

> 注意
>
> SSL 控制板仅显示通过“设置”选项选择的“签名算法”，其他则显示为“不推荐”。

轮询 **NetScaler** 实例中的 **SSL** 证书

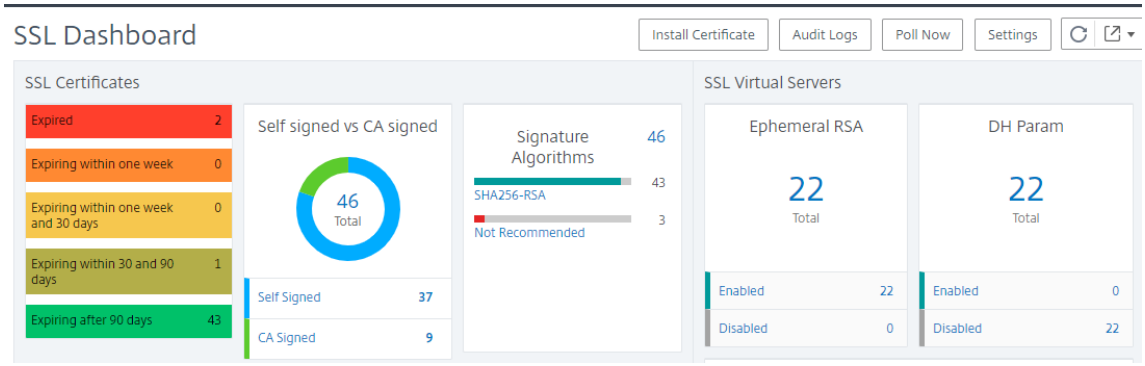
February 6, 2024

NetScaler Application Delivery Management (ADM) 使用 NITRO 呼叫和安全复制 (SCP) 协议，每 24 小时自动轮询一次 SSL 证书。您也可以手动轮询 SSL 证书，在 Citrix Application Delivery Controller (ADC) 实例上发现新添加的 SSL 证书。轮询所有 NetScaler 实例 SSL 证书会给网络带来沉重负载。

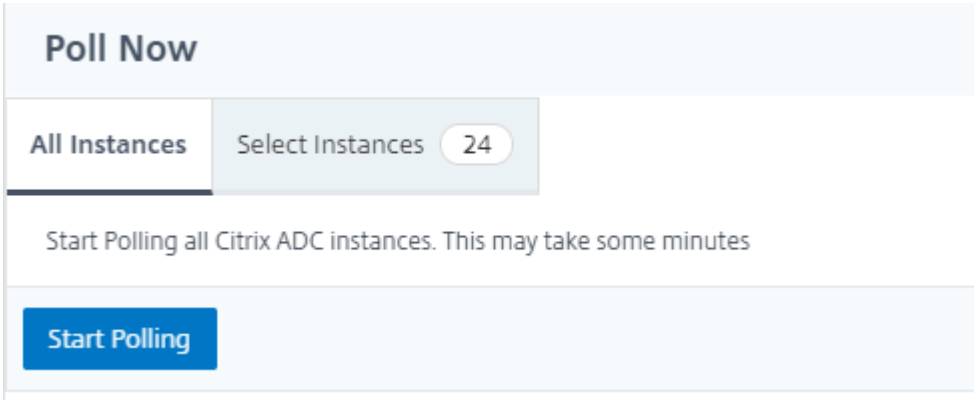
您可以仅手动轮询一个或多个选定实例的 SSL 证书，而不是轮询所有 NetScaler 实例 SSL 证书。

要在 **NetScaler** 实例上轮询 **SSL** 证书，请执行以下操作：

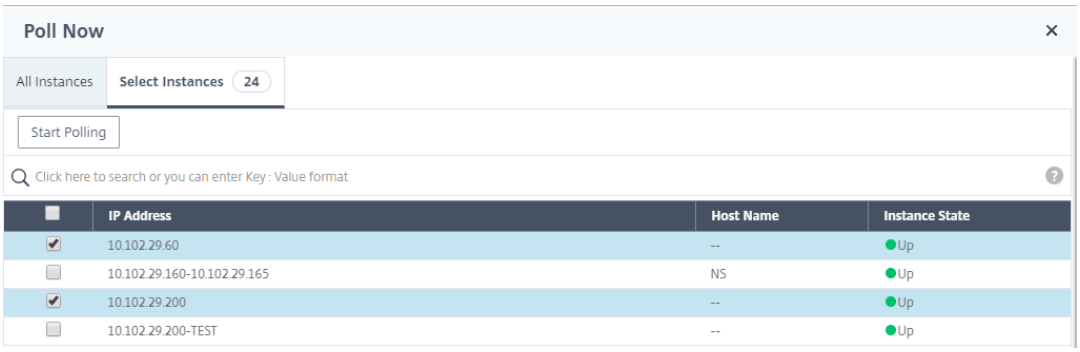
1. 在 NetScaler ADM 中，导航到 基础结构 **> SSL** 控制板。
2. 在 **SSL** 控制板 页面的右上角，单击 立即轮询。



3. 将弹出“立即轮询”页面，您可以选择轮询网络中的所有 NetScaler 实例或轮询所选实例。
   a) 要轮询所有 NetScaler 实例的 SSL 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。



事件

February 6, 2024

将 Citrix Application Delivery Controller (ADC) 实例的 IP 地址添加到 NetScaler Application Delivery Management (ADM) 时，NetScaler ADM 会发送 NITRO 调用，并隐式将自己添加为陷阱目的地，以便实例接收其陷阱或事件。

事件表示托管 NetScaler 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 NetScaler ADM 服务器上生成并记录事件。在 NetScaler ADM 中收到的事件显示在“事件摘要”页面（基础架构 **>** 事件）上，所有活动事件显示在“事件消息”页面（基础架构 **>** 事件 **>** 事件消息）中。

NetScaler 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。规则使监视跨 NetScaler 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、NetScaler 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，然后上载附件。

使用事件控制板

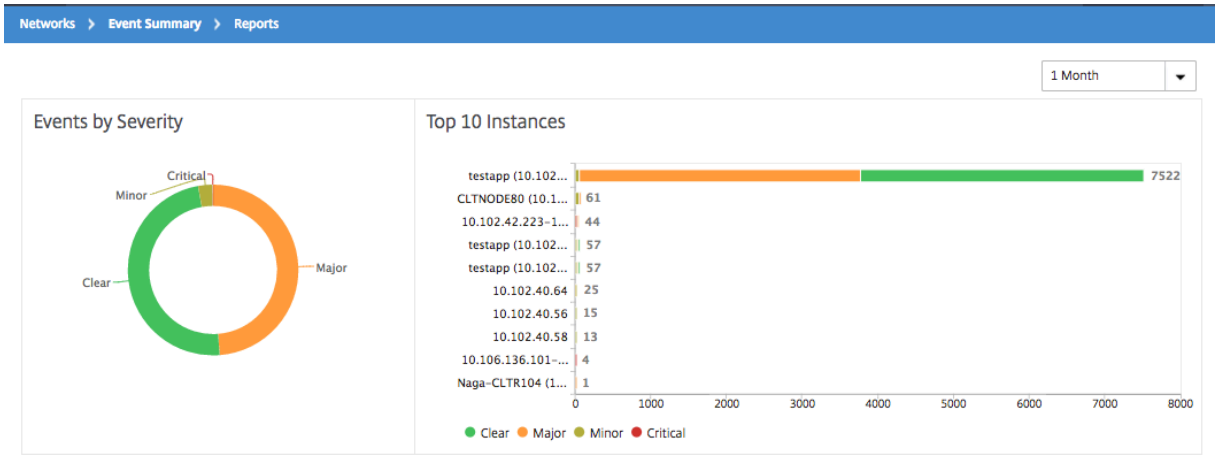
February 6, 2024

作为网络管理员，您可以查看 Citrix Application 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 NetScaler Application Delivery Management (ADM) 的事件控制面板来查看为所有 NetScaler 实例的关键事件严重性详细信息而生成的报告。

要查看事件控制板上的详细信息：

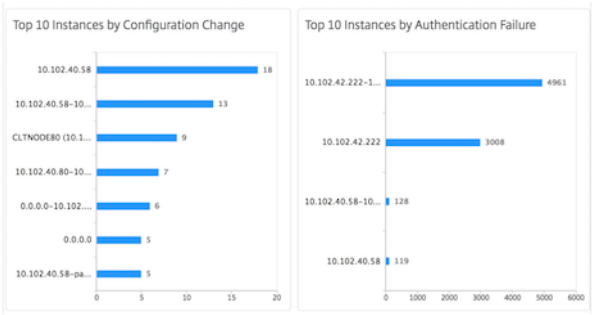
导航到 基础架构 **>** 事件 **>** 报告。

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。

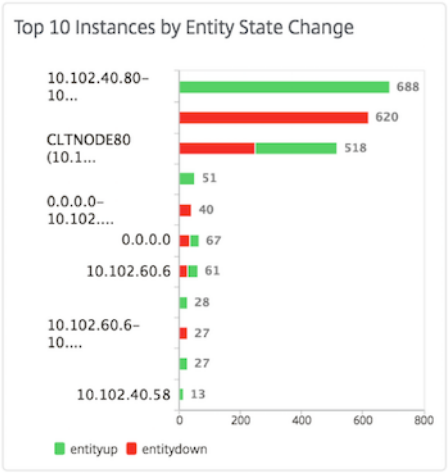


您可以通过导航到 NetScaler 实例类型（基础架构 **>** 事件 **>** 报告 > **NetScaler/NetScaler SDX**）查看以下内容来查看更多详细信息：

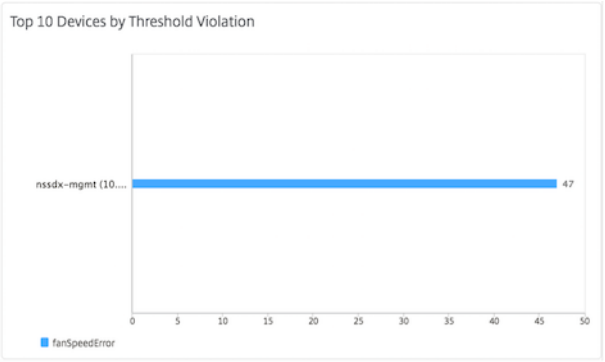
- Top 10 devices by hardware failure（按硬件故障排在前 10 位的设备）
- Top 10 devices by configuration change（按配置变更排在前 10 位的设备）
- Top 10 devices by authentication failure（按身份验证失败排在前 10 位的设备）



- 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）



设置事件的事件期限

February 6, 2024

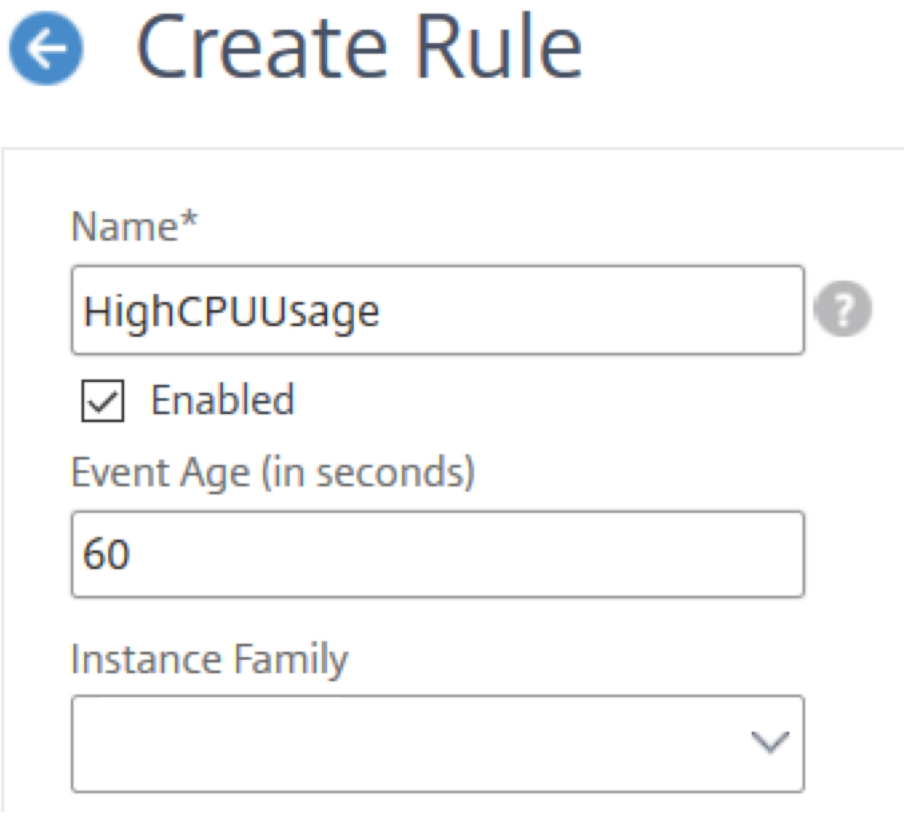
您可以设置事件时间选项来指定时间间隔（以秒为单位）。NetScaler ADM 会监视设备直到设置的持续时间，并且只有在事件持续时间超过设定的持续时间时才生成事件。

> 注意：
>
> 事件持续时间的最小值为 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，假设您想要管理各种 ADC 设备，并在任何虚拟服务器停机 60 秒或更长时间时通过电子邮件收到通知。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 **NetScaler ADM** 中设置事件期限，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础架构 **>** 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。

安排事件过滤器

February 6, 2024

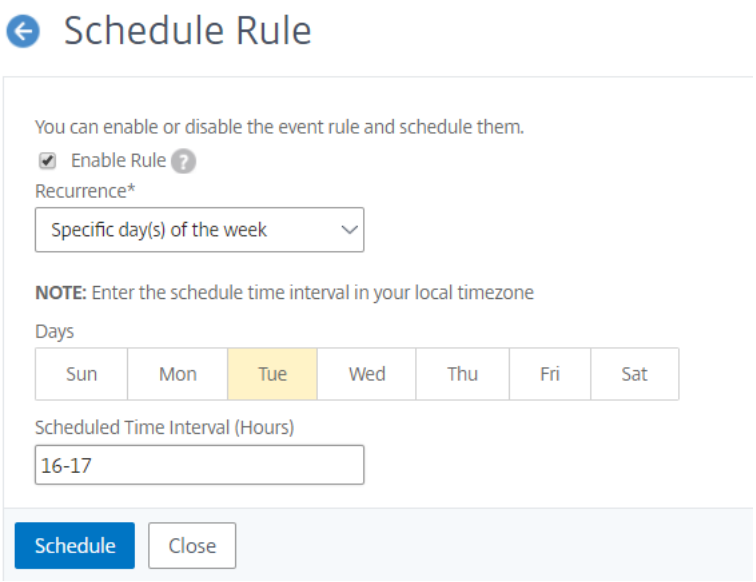
为您的规则创建筛选器后，如果您不希望 NetScaler Application Delivery Management (ADM) 服务器在每次生成的事件满足筛选条件时发送通知，则可以将筛选器设置为仅在特定的时间间隔（例如每天、每周或每月）触发。

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过滤器并为这些过滤器启用了电子邮件通知，则当 NetScaler 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 **NetScaler ADM** 计划筛选器，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础架构 **>** 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：选择一周中的哪一天来运行规则。您可以选择多天。
   - 日期：输入日期。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）。



为事件设置重复的电子邮件通知

February 6, 2024

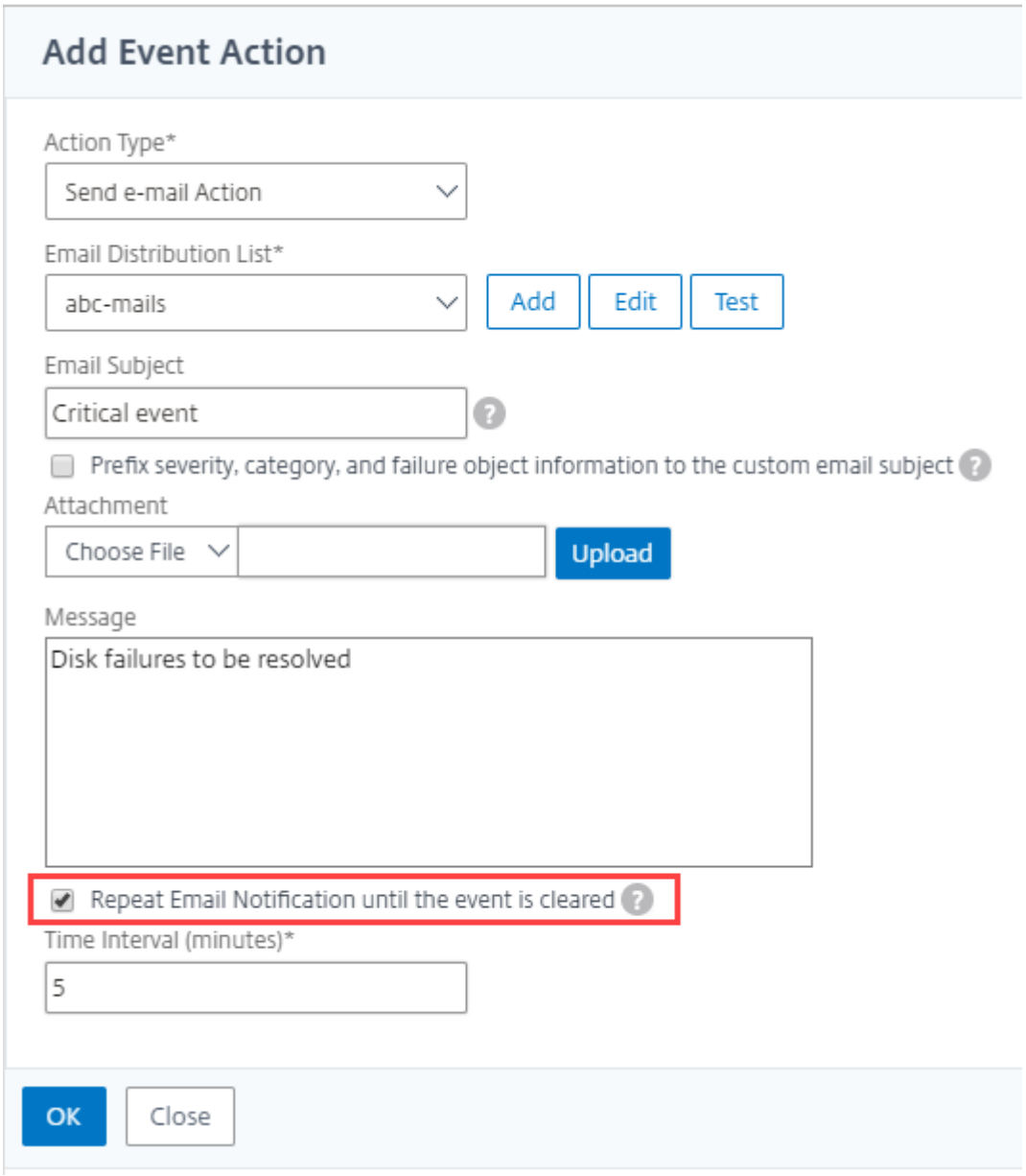
为了确保所有严重事件都被解决且没有重要电子邮件通知丢失，可以选择为满足所选择条件的事件规则发送重复的电子邮件通知。例如，如果为涉及磁盘故障的实例创建了事件规则，并希望在问题解决之前一直收到通知，可以选择接收有关那些事件的重复电子邮件通知。

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
>
> 只有在设置了等效的“清除”陷阱并从您的 Citrix Application 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 基础架构 **>** 事件 **>** 事件摘要，选择一个 类别，然后在类别中选择一个事件，然后单击 清除。
> - 或者，导航到 基础结构 **>** 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 **NetScaler ADM** 的重复电子邮件通知，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **>** 事件 **>** 规则，然后单击添加创建规则。
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”，然后选择电子邮件分发列表。
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。



禁止显示事件

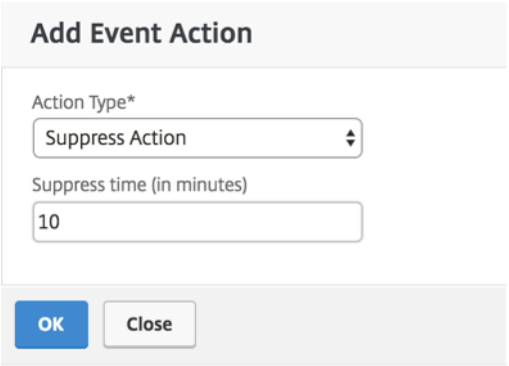
February 6, 2024

选择“抑制操作”事件操作时，可以配置一个时间段（以分钟为单位），在此时间段内抑制或删除事件。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，NetScaler ADM 将隐藏时间视为零，并且永远不会过期。

要通过使用 **NetScaler ADM** 隐藏事件，请执行以下操作：

1. 在 NetScaler Application Delivery Management (ADM) 中，导航到基础架构 **>** 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

February 6, 2024

可以配置规则以监视特定事件。规则可以更轻松地监视整个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 (NetScaler) 实例、类别、故障对象、配置命令和消息。

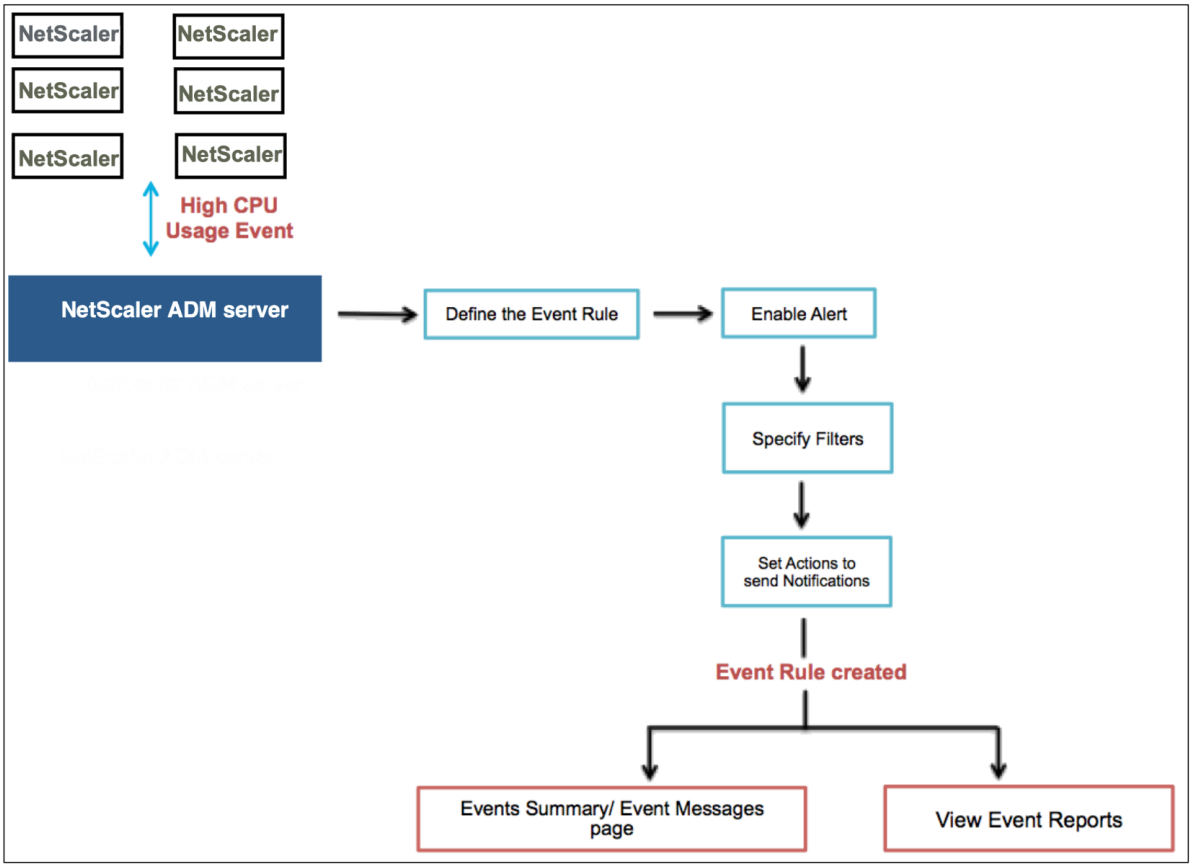
可以为事件分配以下操作：

- 发送电子邮件操作：针对符合筛选条件的事件发送电子邮件。
- 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：在配置的 Slack 频道上发送符合筛选条件的事件的通知。
- 发送 **PagerDuty** 通知：根据符合筛选条件的事件的 PagerDuty 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 NetScaler 实例的“高 CPU 使用率”事件可能会导致 NetScaler 实例中断，则您可能希望监视这些事件。您可以：

- 创建规则以监视实例，并指定在发生“高 CPU 使用率”类别的事件时向您发送电子邮件通知的操作。
- 将规则安排在特定时间（例如上午 11 点到晚上 11 点之间）运行，这样就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 NetScaler 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

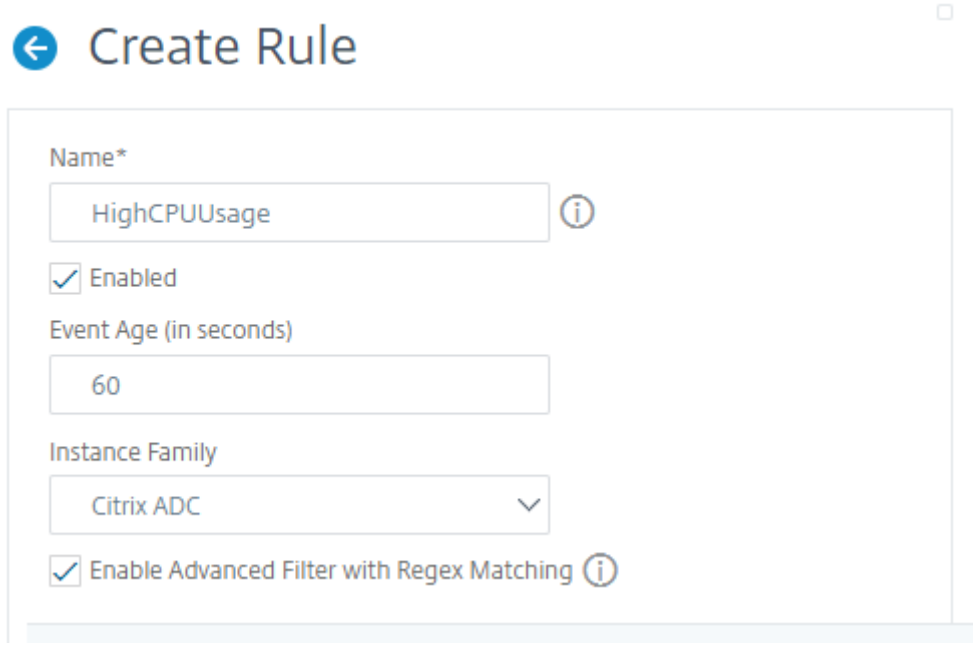
步骤 **1-**定义事件规则

导航到 基础架构 **>** 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“事件时限”选项来指定 NetScaler ADM 刷新事件规则的时间间隔（以秒为单位）。

> 注意：
>
> 事件持续时间的最小值为 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。

根据上面的示例，每当 NetScaler 实例发生 60 秒或更长时间的“高 CPU 使用率”事件时，您可能希望收到电子邮件通知。您可以将事件时间设置为 60 秒，这样，每当 NetScaler 实例发生“高 CPU 使用率”事件持续 60 秒或更长时间时，您都会收到一封包含该事件详细信息的电子邮件通知。



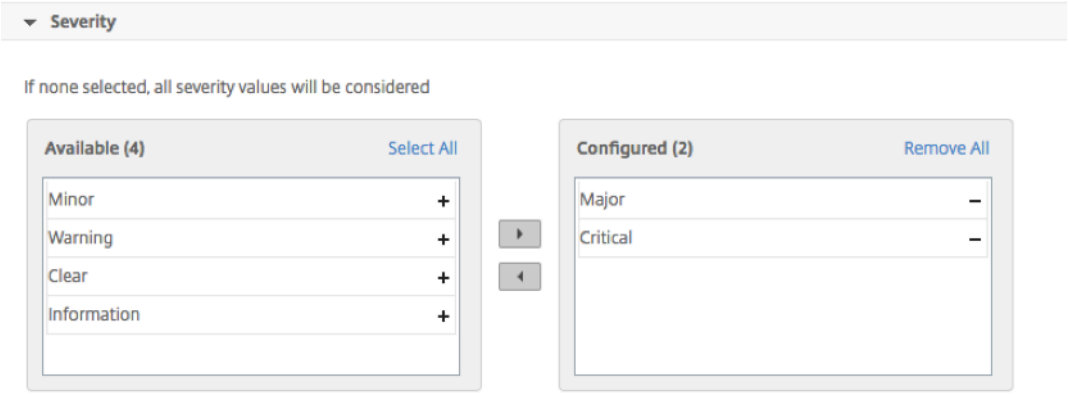
您还可以按 实例系列 筛选事件规则，以跟踪 NetScaler ADM 从中接收事件的 NetScaler 实例。

如果要包含星号 (*) 模式匹配以外的正则表达式，请选择“使用正则表达式匹配启用高级筛选器”。

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）。

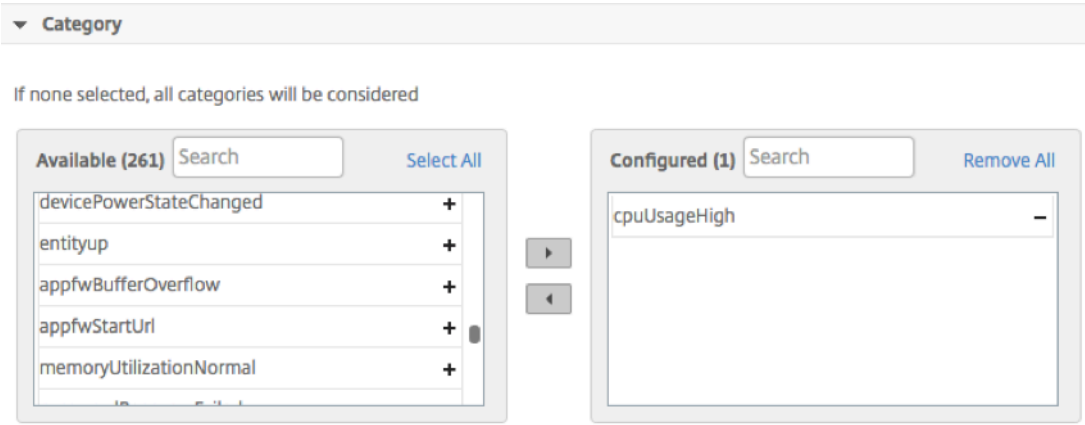


> 注意
>
> 您可以为通用事件和高级特定事件配置严重性。要修改在 NetScaler ADM 上管理的 NetScaler 实例的事件严重性，请导航到 基础架构 **>** 事件 **>** 事件设置。选择要为其配置事件严重性的 类别，然后单击 配置严重性。分配新的严重性级别，然后单击 确定”。

步骤 **3-**指定事件类别

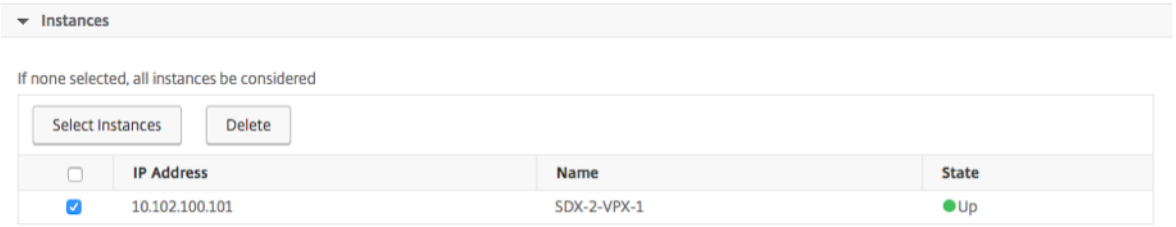
您可以指定 NetScaler 实例生成的事件的类别或类别。所有类别都在 NetScaler 实例上创建。然后使用可用于定义事件规则的 NetScaler ADM 映射这些类别。选择要考虑的类别，然后将其从 可用 表移动到 已配置 表。

在上面的示例中，您必须从显示的表格中选择“cpuUsageHigh”作为事件类别。



步骤 **4-**指定 **NetScaler** 实例

选择要为其定义事件规则的 NetScaler 实例的 IP 地址。在“实 例”部分中，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。



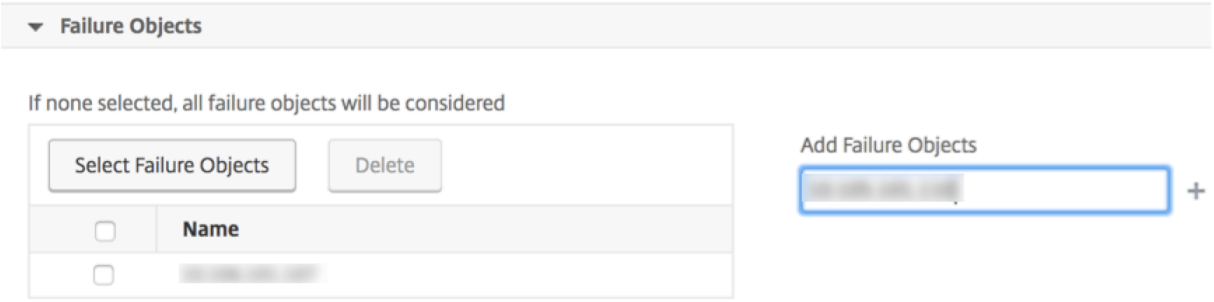
步骤 **5-**选择失败对象

您可以从提供的列表中选择失败对象，也可以添加已生成事件的失败对象。您也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 步骤 1 中选择 使用正则表达式匹配启用高级筛选器。

故障对象会影响事件的处理方式，并确保它反映了所通知的确切问题。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。

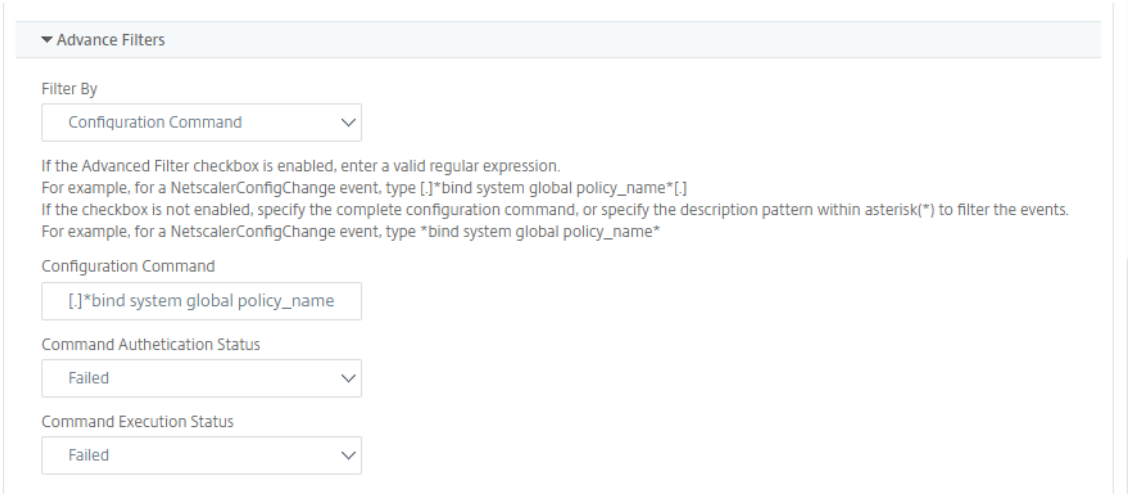


步骤 **6-**指定高级筛选器

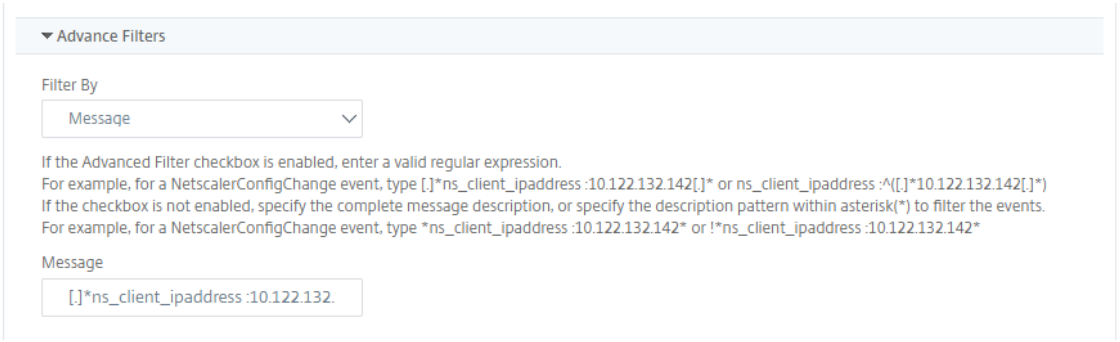
您可以按以下内容进一步过滤事件规则：

- 配置命令 -您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`，请键入 `[.]*bind system global policy_name[.]*`。



- 消息 -您可以指定完整的消息描述，也可以指定正则表达式来筛选事件。
  例如，对于 `NetscalerConfigChange` 事件，请键入 `[.]*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 PagerDuty 通知

- 发送 ServiceNow 通知

设置电子邮件事件规则操作

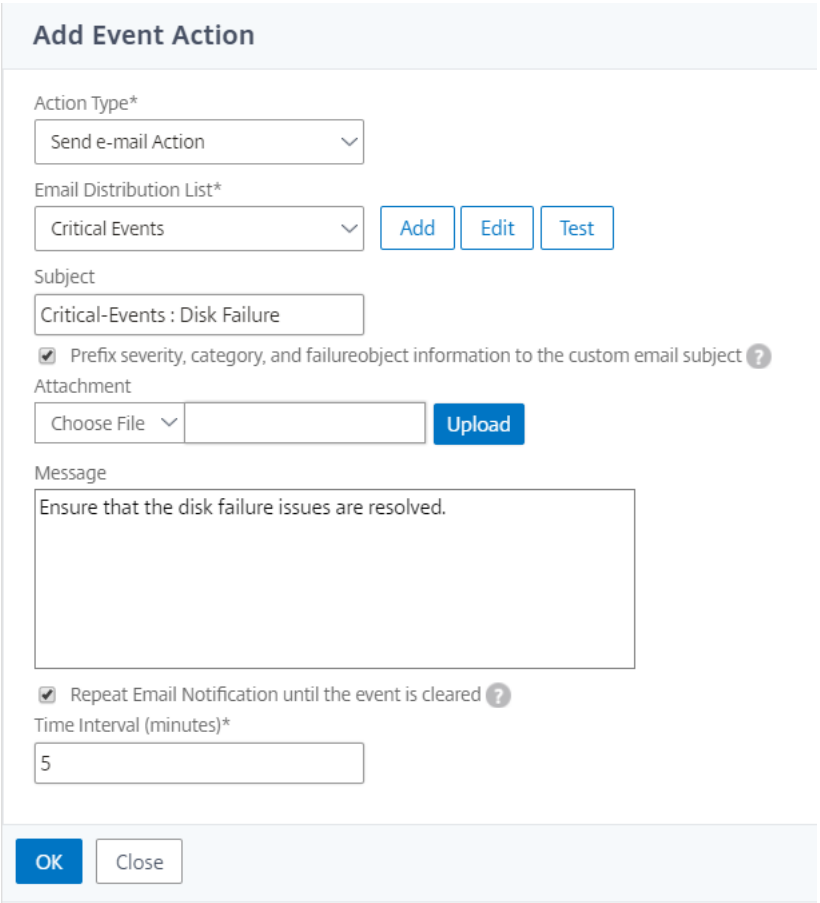
当您选择“发送电子邮件操作”事件操作类型时，当事件满足定义的筛选条件时，将触发电子邮件。您必须通过提供邮件服务器或邮件配置文件详细信息来创建电子邮件分发列表，也可以选择以前创建的电子邮件分发列表。

由于 NetScaler 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。这些电子邮件有一个默认的主题行，提供有关事件严重性、事件类别和失败对象的信息。但是主题行没有包含有关这些事件源自的虚拟服务器名称的任何信息。现在，您可以选择添加一些其他信息，例如受影响实体的名称、故障对象的名称。

您还可以添加自定义的主题行和用户消息，并在传入事件与配置的规则匹配时将附件上载到您的电子邮件中。

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。现在，“测试”按钮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。

您还可以选中“在事件被清除之前重复发送电子邮件通知”复选框，针对符合所选条件的事件规则重复发送电子邮件通知，从而确保所有关键事件都得到解决，不会错过任何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。通过定义陷阱分布列表（或陷阱目的地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的陷阱侦听器。

设置运行命令操作

选择“运行命令操作”事件操作 时，可以创建可在 NetScaler ADM 上针对匹配特定筛选条件的事件运行的命令或脚本。

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	故障对象会影响事件的处理方式，并确保故障对象反映所通知的确切问题。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”时设置运行命令操作。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一种快速的解决方法。在 NetScaler ADM 中，您可以：

- 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 NetScaler ADM 代理上的任何永久位置。例如，/var。
- 在 NetScaler 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 en **titydown**
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”，然后从“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”。

   屏幕上将显示“创建命令分发列表”页面。

   a) 在 配置文件名称中，指定您选择的名称

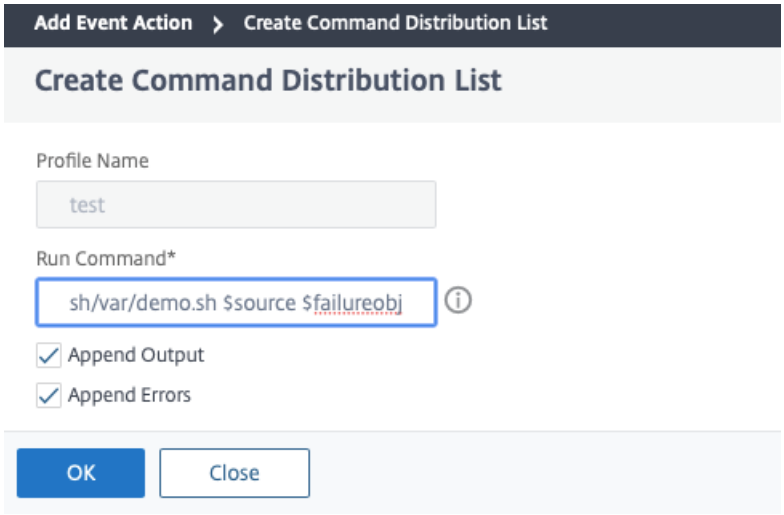
   b) 在 运行命令中，指定必须在其中运行脚本的 NetScaler ADM 代理位置。例如：/sh/var/demo.sh $source $failureobj。

   c) 选择“追加输出”和“追加错误”

   > 注意
   >
   > 如果要在 **NetScaler 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，NetScaler 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。

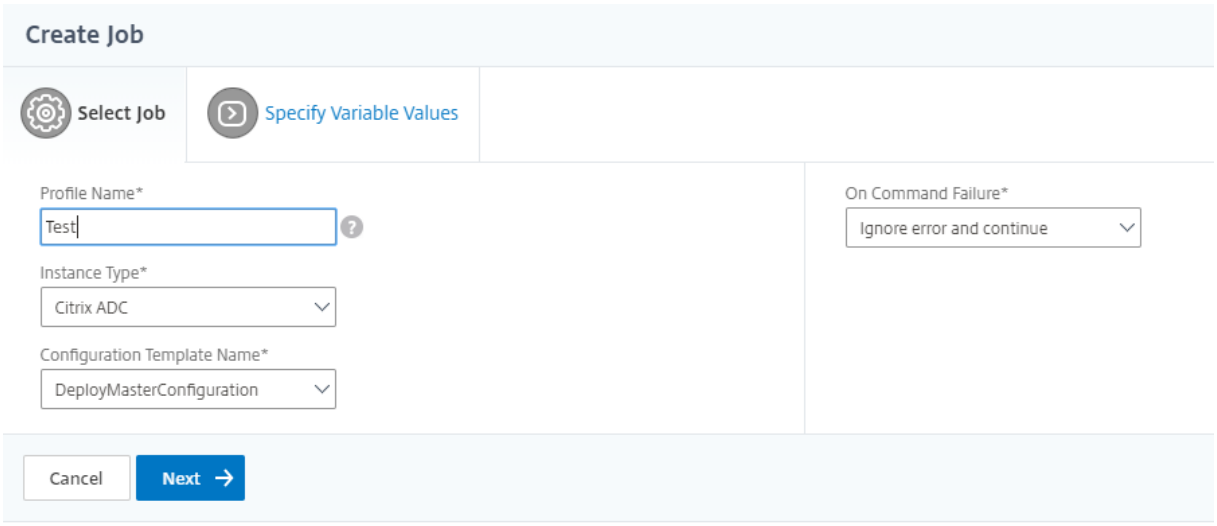


> 注意
>
> 如果要在 **NetScaler ADM** 服务器日志文件中运行命令脚本时存储输出和生成的错误（如果有），则可以启用追加输出”和“追加错误”选项。如果不启用这些选项，NetScaler ADM 会丢弃运行命令脚本时生成的所有输出和错误。

设置 **Execute** 作业操作

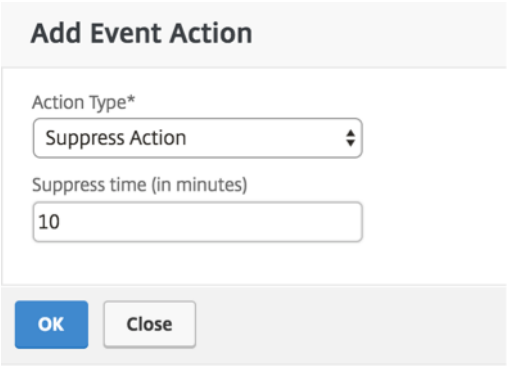
通过创建包含配置作业的配置文件，作业将作为 NetScaler 和 NetScaler SDX 实例的内置作业或自定义作业运行，以处理与您指定的筛选条件相匹配的事件和警报。

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. 创建配置文件，其中包含要在事件满足定义的筛选条件时运行的作业。
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 **NetScaler ADM** 的 **Slack** 通知

通过在 NetScaler ADM GUI 中提供配置文件名称和 webhook URL 来配置所需的 Slack 频道。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 NetScaler ADM 中，导航到 **Infrastructure >** 事件 **>** 规则，然后单击添加以创建规则。
2. 在 创建规则页面上，设置规则参数，例如严重性和类别。选择必须监视的实例和故障对象。
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”字段旁边的“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 NetScaler 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**。键入您之前输入的通道的 Webhook URL。传入的 Webhook 是将来自外部来源的消息发布到 Slack 的简单方法。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 的一个例子如下：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：
>
> 您也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 **NetScaler ADM** 的 **PagerDuty** 通知

您可以在 NetScaler 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 使您能够通过电子邮件、短信、推送通知和拨打注册号码的电话来配置通知。

在 NetScaler 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。有关更多信息，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 NetScaler 实例生成的事件列表。
- 许可证—当前处于活动状态、即将到期等的许可证列表。
- **SSL** 证书—添加到 NetScaler 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 NetScaler ADM。
2. 导航到“设置”**>**“通知”**>**“**PagerDuty** 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。

      您可以从您的 PagerDuty 门户获取集成密钥。

   c) 单击创建。

   使用案例：

   考虑一个场景，您：

   - 想要向您的 PagerDuty 配置文件发送通知。
   - 已在 PagerDuty 中将电话配置为接收通知的选项。
   - 想要获取 NetScaler 事件的电话提醒。

   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”。

      屏幕上 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 NetScaler 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
- 上报给其他团队成员

从 **NetScaler ADM** 自动生成 **ServiceNow** 事件

通过在 NetScaler ADM GUI 上选择 ServiceNow 配置文件，您可以为 NetScaler ADM 事件自动生成 ServiceNow 事件。您必须在 NetScaler 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 NetScaler 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”。

   屏幕上 将显示“添加事件操作”页面。

   a) 在 操作类型中，选择 发送 **ServiceNow** 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。

修改报告的 **NetScaler** 实例上发生的事件的严重性

February 6, 2024

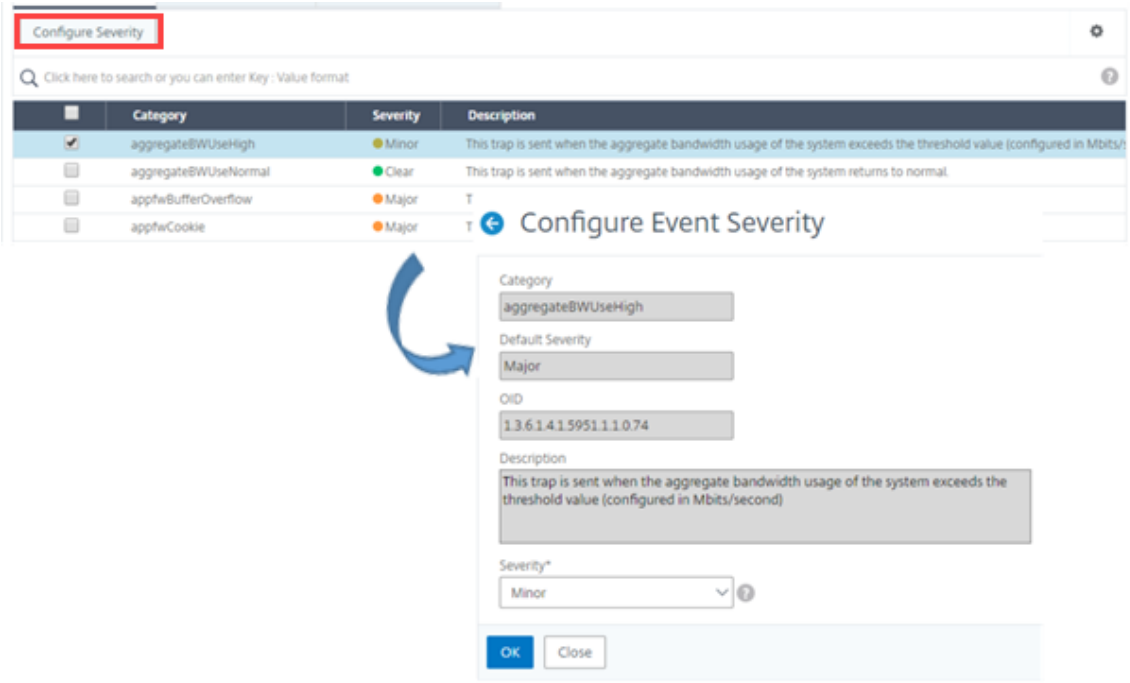
您可以管理您的所有设备上生成的事件的报告，以便可以查看有关特定实例上特定事件的事件详细信息，以及根据事件严重性查看报告。可以创建使用默认严重性设置的事件规则，并可以更改严重性设置。可以为一般事件和企业特定的事件配置严重性。

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 基础结构 **>** 事件 **>** 事件设置。

2. 单击要修改的 Citrix Application 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。

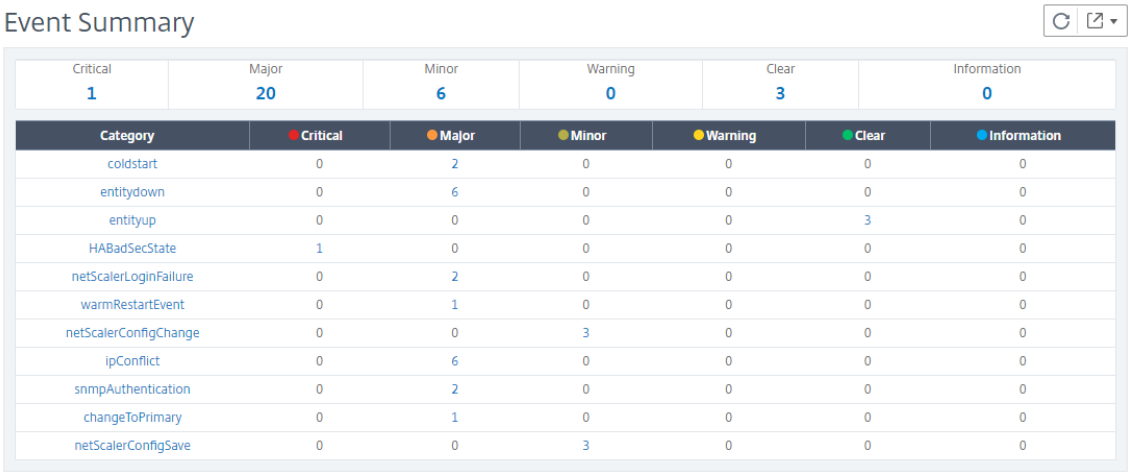


查看事件摘要

February 6, 2024

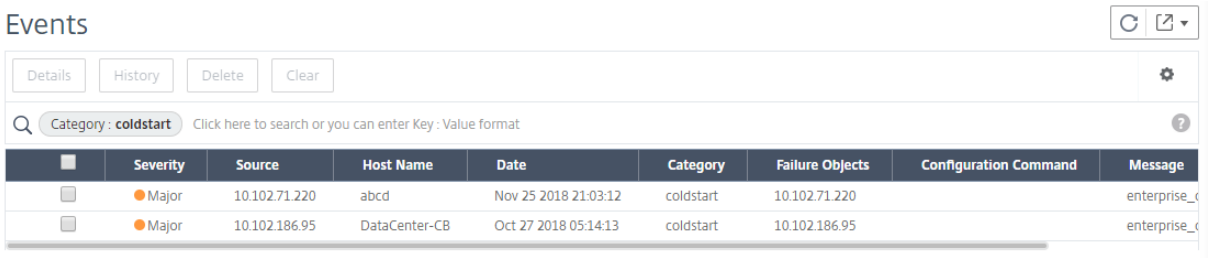
现在，您可以查看“事件摘要”页面，以监视 NetScaler Application Delivery Management (ADM) 服务器上收到的事件和陷阱。导航到基础架构 **>** 事件。“Events Summary”（事件摘要）页面以表格形式显示以下信息：

- **NetScaler 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 Application Delivery Controller (ADC) 实例关闭并停止向 NetScaler 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 NetScaler 实例发送到 NetScaler 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 NetScaler 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 NetScaler 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

February 6, 2024

当您在 NetScaler Application Delivery Management (ADM) 中创建事件及其设置时，可以立即在“事件摘要”页面上查看该事件。同样，您可以在基础架构控制板上详细查看和监视添加到 NetScaler ADM 服务器的所有 Citrix Application Delivery Controller (ADC) 实例的运行状况、运行时间、型号和版本。

在基础结构控制板上，您现在可以屏蔽不相关的值，以便更轻松地查看和监视按严重性划分的事件、运行状况、正常运行时间、型号和 NetScaler 实例版本等信息。

例如，严重级别为“严 重”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。

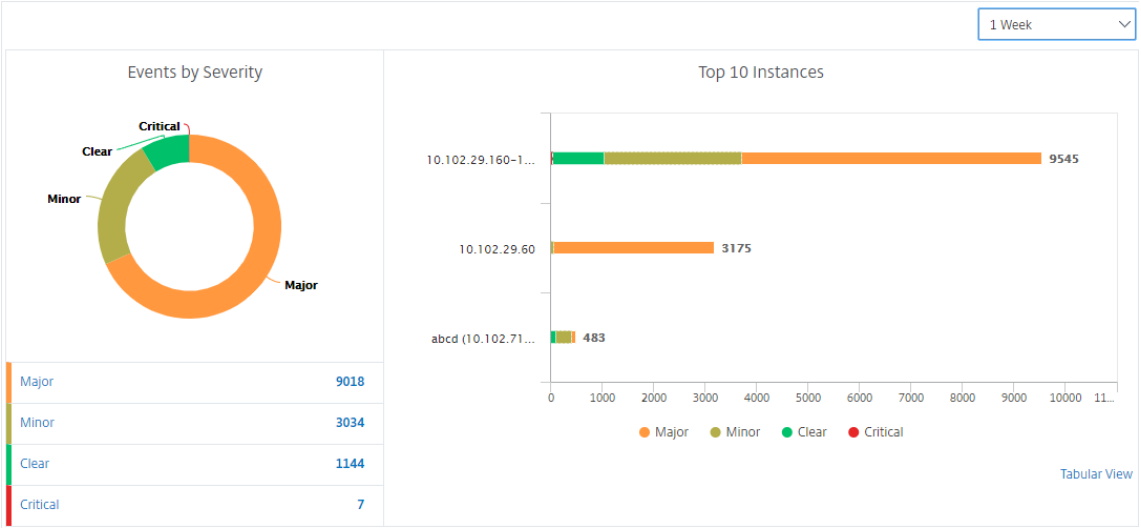
同样，可以在控制板上查看 NetScaler VPX 实例的运行状况。您可以屏蔽实例已启动并运行的时间段，只显示实例停止工作的时间段。通过单击图表，您将进入该实例的页面，其中已应用 了不服务 筛选器，并查看详细信息，如主机名、每秒接收的 HTTP 请求数、CPU 使用率等。您还可以选择实例并查看特定 Citrix 实例的控制板以了解更多详细信息。

要在 **NetScaler 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 NetScaler ADM。
2. 导航到 基础架构 **>** 控制板。

   或者，

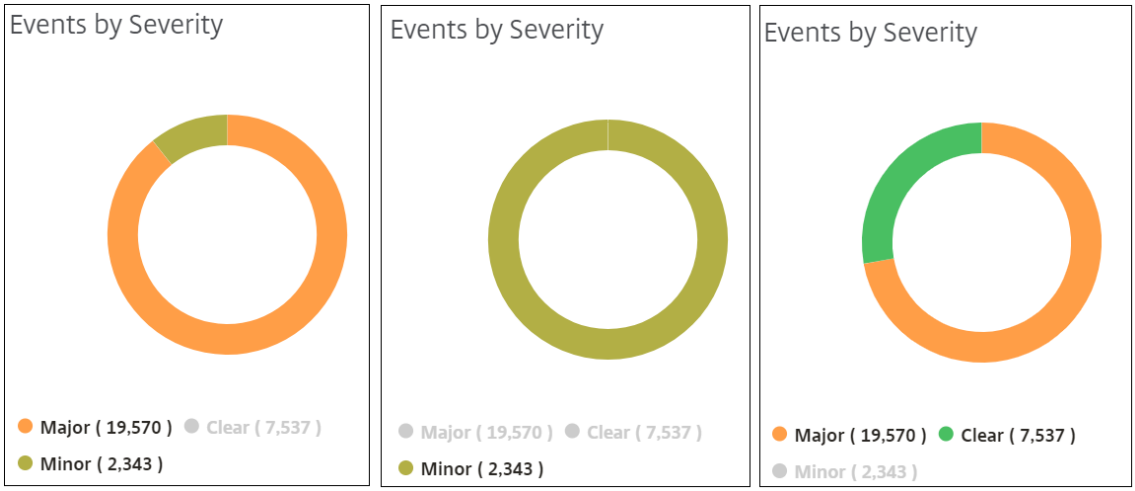
   导航到 基础结构 **>** 事件 **>** 报告。
3. 从页面右上角的菜单中，选择要按严重程度查看事件的持续时间。



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
   - 由 NetScaler 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 **NetScaler ADM** 上的 **NetScaler 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 NetScaler ADM 服务器上的托管 NetScaler 实例收到的每个 SNMP 陷阱的详细信息。导航到基础架构 **>** 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，陷阱类别为 **monresptimeoutBelowThresh** 的事件，该陷阱的描述显示为“当监视探测器的响应超时恢复正常，小于设定的阈值时，就会发送此陷阱。”

查看和导出 **NetScaler syslog** 消息

February 6, 2024

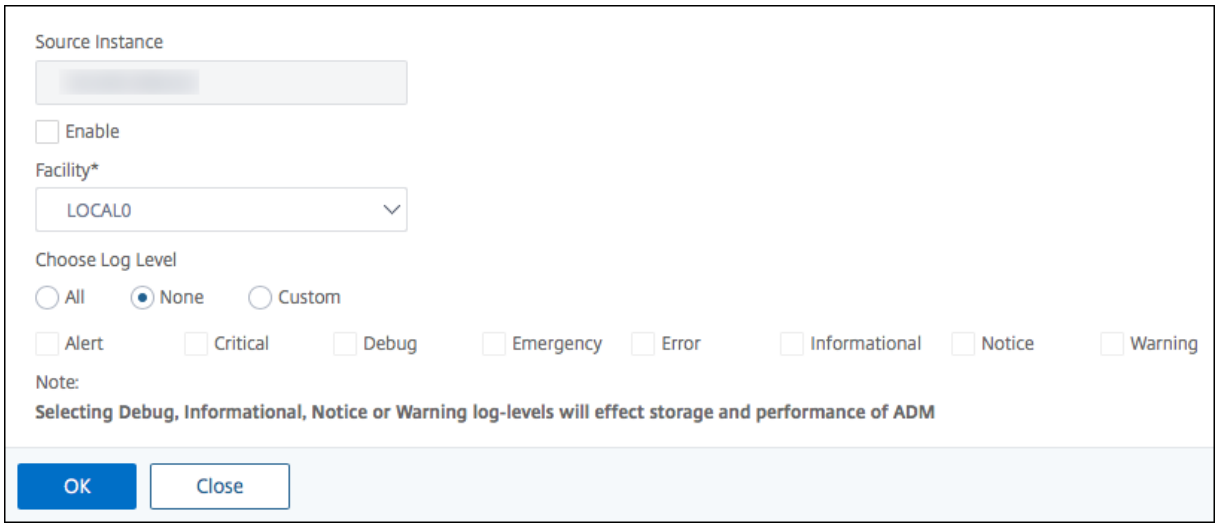
通过 ADM 软件，您可以监视在 Citrix Application Delivery Controller (ADC) 实例上生成的 syslog 事件。为此，您必须将 ADM 配置为 NetScaler 实例的 syslog 服务器。配置 ADM 后，所有系统日志消息都将从 ADC 实例重定向到 ADM。

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. 从 ADM GUI 中，导航到 基础架构 **>** 实例。
2. 选择要从中收集 syslog 消息并在 NetScaler ADM 中显示的 NetScaler 实例。

3. 在 **Select Action**（选择操作）列表中，选择 **Configure Syslog**（配置 Syslog）。
4. Click **Enable**。
5. 在 **Facility**（设施）下拉列表中，选择本地或用户级别的设施。
6. 为 syslog 消息选择所需的日志级别。
7. 单击确定。

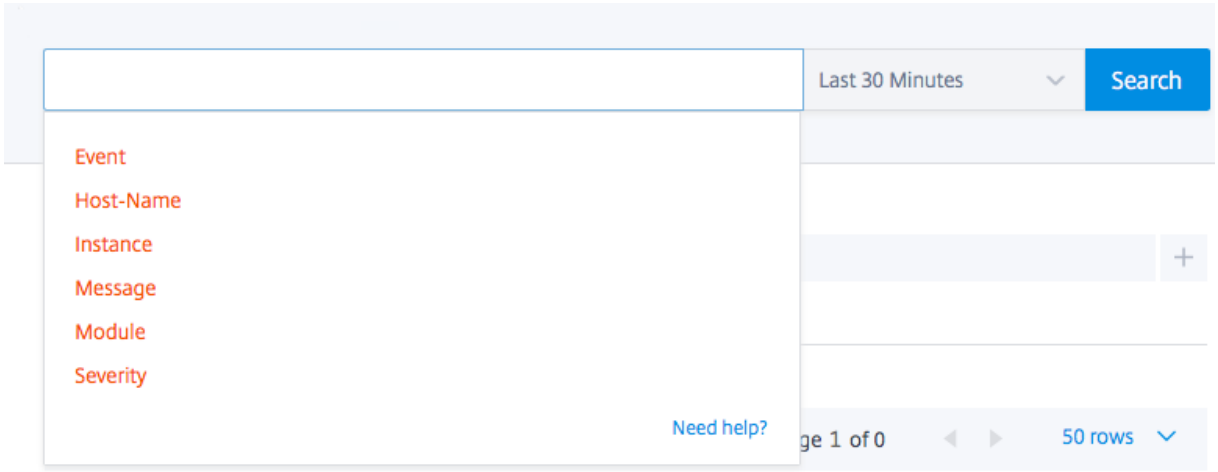


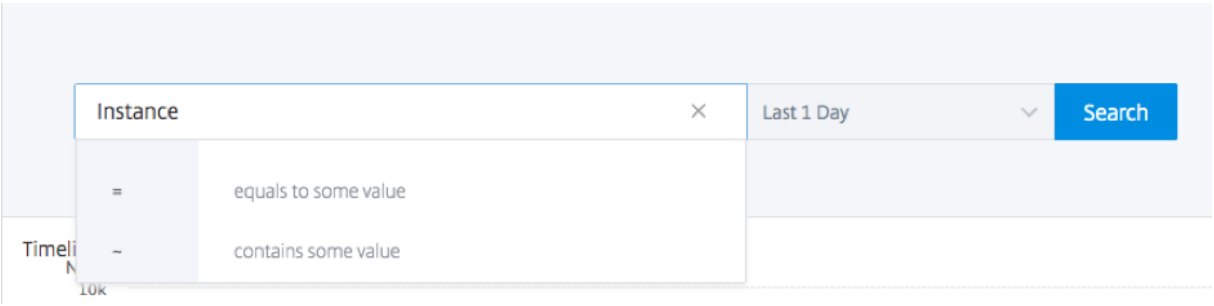
这些步骤将配置 NetScaler 实例中的所有 syslog 命令，然后 NetScaler ADM 开始接收 syslog 消息。

查看和搜索 **syslog** 消息

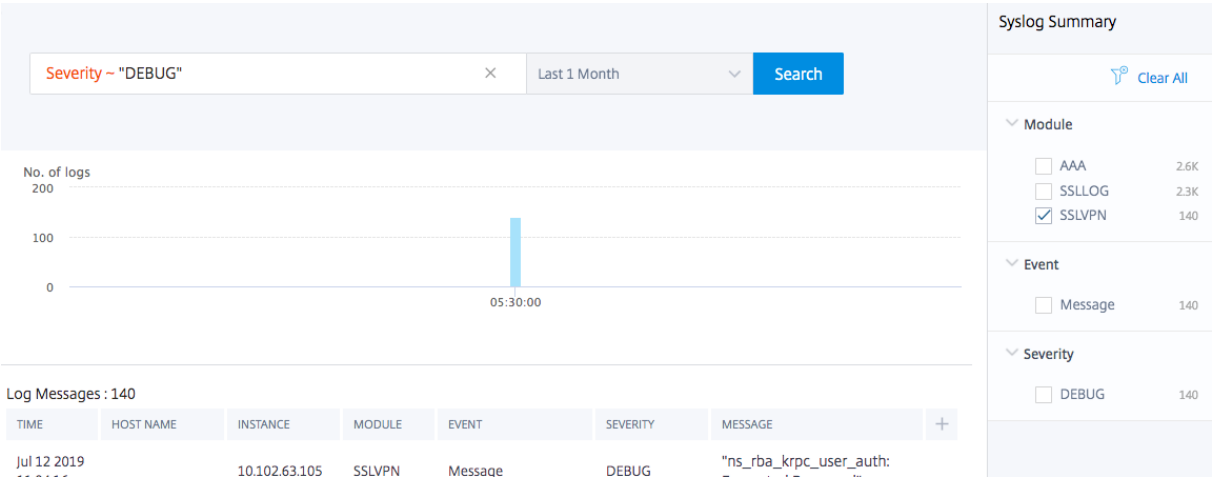
您可以查看在托管 NetScaler 实例上生成的所有 syslog 消息。系统日志消息集中存储在数据库中，可在 基础架构 **>** 事件 **> Syslog** 消息 下用于审核。您可以合并这些日志记录信息，然后从收集的数据中派生报告以进行分析。

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 **Need Help?**（需要帮助?）打开内置的搜索帮助。





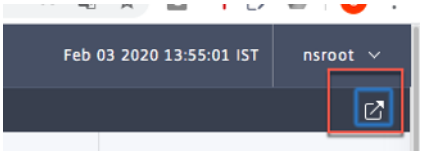
接下来，添加搜索词。对于某些类别，会显示预先填充的搜索词列表。默认情况下，搜索时间为 1 天。您可以通过单击向下箭头更改时间和日期范围。您可以通过从“系统日志摘要”窗格中选择选项来进一步缩小搜索范围。



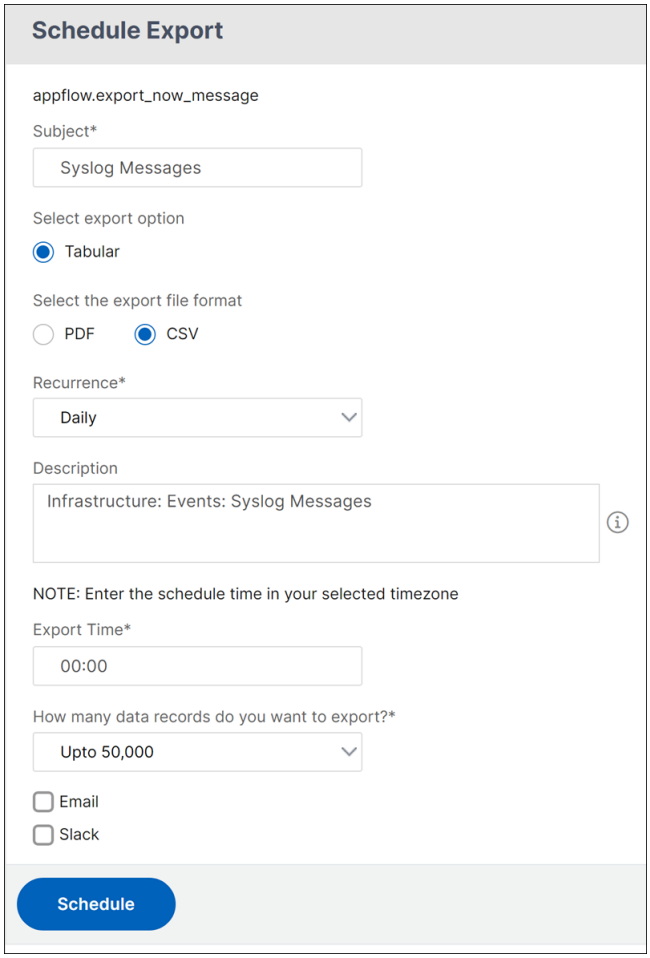
导出和安排 **syslog** 消息

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。



禁止显示 **syslog** 消息

February 6, 2024

配置为系统日志服务器时，NetScaler Application Delivery Management (ADM) 将接收由配置的 Citrix Application Delivery Controller (ADC) 实例发送给它的所有系统日志消息。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过滤器来抑制进入 NetScaler ADM 的某些系统日志消息。NetScaler ADM 会删除所有符合条件的消息。这些删除的消息不会显示在 NetScaler ADM GUI 上，这些消息也不会存储在客户的 NetScaler ADM 数据库中。

您可以通过设置一些过滤器来抑制某些已记录的 syslog 消息进入 NetScaler ADM。用于阻止 syslog 消息的两个过滤器是严重性和设施。您还可以隐藏来自特定 NetScaler 实例或多个实例的消息。您还可以为 NetScaler ADM 提供用于搜索和禁止消息的文本模式。NetScaler ADM 会删除所有符合条件的消息。这些删除的消息不会显示在 NetScaler 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

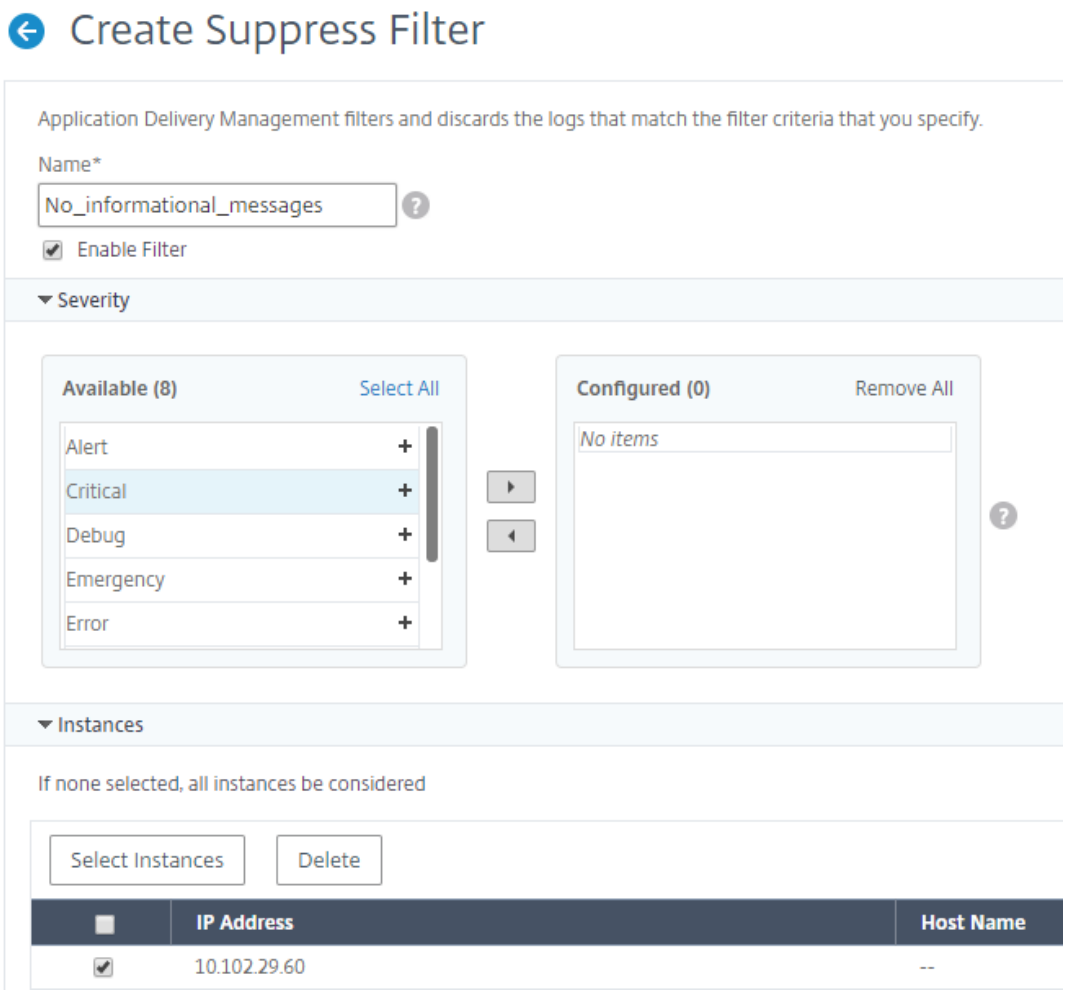
1. 在 NetScaler ADM 中，导航到 基础架构 **>** 事件 **>** 系统日志消息 > 禁止过滤器。
2. 在“创建隐藏过滤器”页上，更新以下信息：

   a) 名称 -键入筛选器的名称。

   > 注意
   >
   > 如果不同的用户对多个 NetScaler 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筛选器。

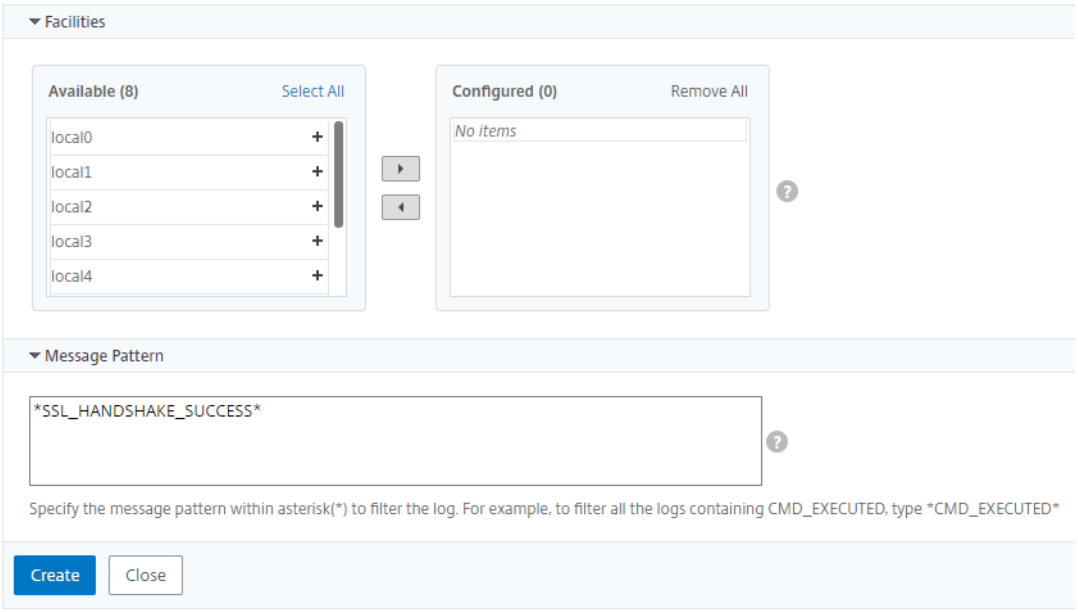
   b) 严重性 -选择并添加必须隐藏消息的日志级别。例如，如果您不想查看传入的任何信息消息，则可以选择“Informational”（信息）以阻止这些消息。

   c) 实例 -选择已配置 syslog 消息的 NetScaler 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 -您也可以键入用星号 (*) 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 NetScaler ADM 上查看消息，必须禁用筛选器。

1. 导航到 基础架构 **>** 事件 **>** **Syslog** 消息 > 禁止过滤器，然后在 禁止过滤器 页面上，选择过滤器并单击 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。

配置实例事件的删除设置

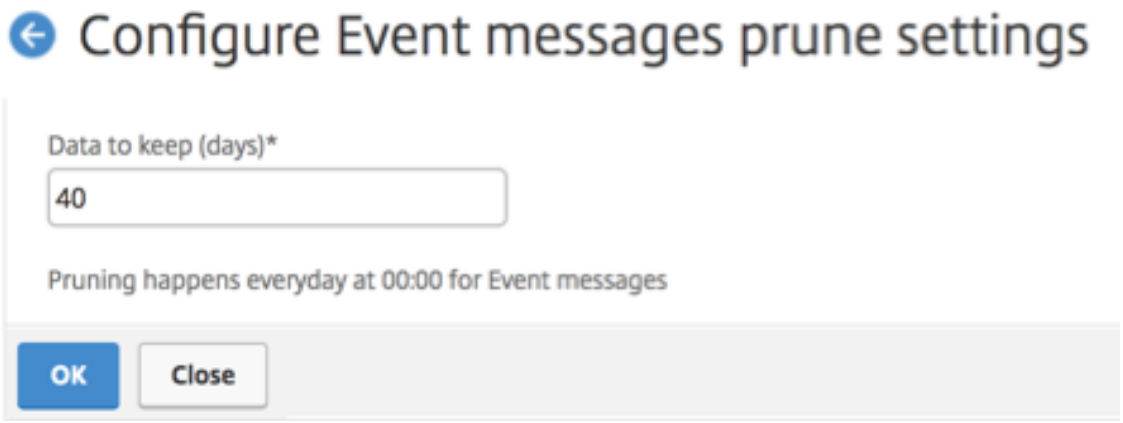
February 6, 2024

由 NetScaler Application Delivery Management (ADM) 服务器管理的 Citrix Application Delivery Controller (ADC) 实例持续发送事件消息数据，存储在 NetScaler ADM 上。您可以指定希望 NetScaler 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 小时修剪一次（在 00.00 点）。

> 注意
>
> 您可以指定的值不能超过 40 天或小于 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 NetScaler 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”。



网络功能

February 6, 2024

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

生成负载平衡实体的报告

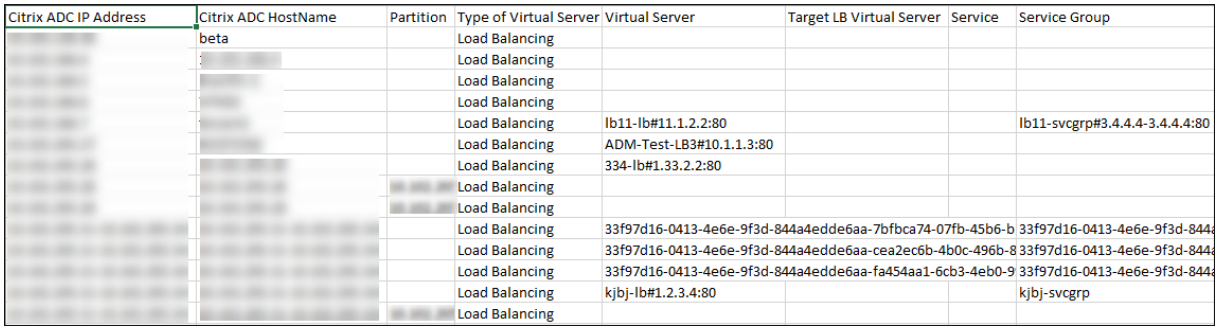
February 6, 2024

NetScaler Application Delivery Management (ADM) 允许您查看各个级别的 Citrix Application Delivery Controller (ADC) 实例实体的报告。您可以在 NetScaler ADM > 网络 函数中下载两种类型的报告：合并报告和单个报告。

合并报告：您可以下载和查看在 NetScaler 实例上管理的所有实体的合并报告或汇总报告。

此报告允许您大致了解 NetScaler 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]	beta		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#3.4.4.4-3.4.4.4:80
[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-b			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-cea2ec6b-4b0c-496b-8			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	33f97d16-0413-4e6e-9f3d-844a4edde6aa-fa454aa1-6cb3-4eb0-9			33f97d16-0413-4e6e-9f3d-844
[redacted]	[redacted]		Load Balancing	kjbj-lb#1.2.3.4:80			kjbj-svcgrp
[redacted]	[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：NetScaler 实例的 IP 地址显示在报告中
- **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 :port_number
- 服务：<name_of_the_service>#service-IP_address:port_number
- 服务组:<name_of_service_group>#server_member1_IP_address:port,server_member2_IP_address:port,se ……..,server_membern_IP_address:port

> 注意
>
> - 如果没有主机名，则显示对应的 IP 地址。
> - 空列表示未为该 NetScaler 实例配置相应的实体。

个人报告：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。

NetScaler 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 NetScaler ADM 中，导航到 基础架构 **>** 网络功能 **>** 负载平衡。
2. 在“负载平衡”页面上，  。
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。

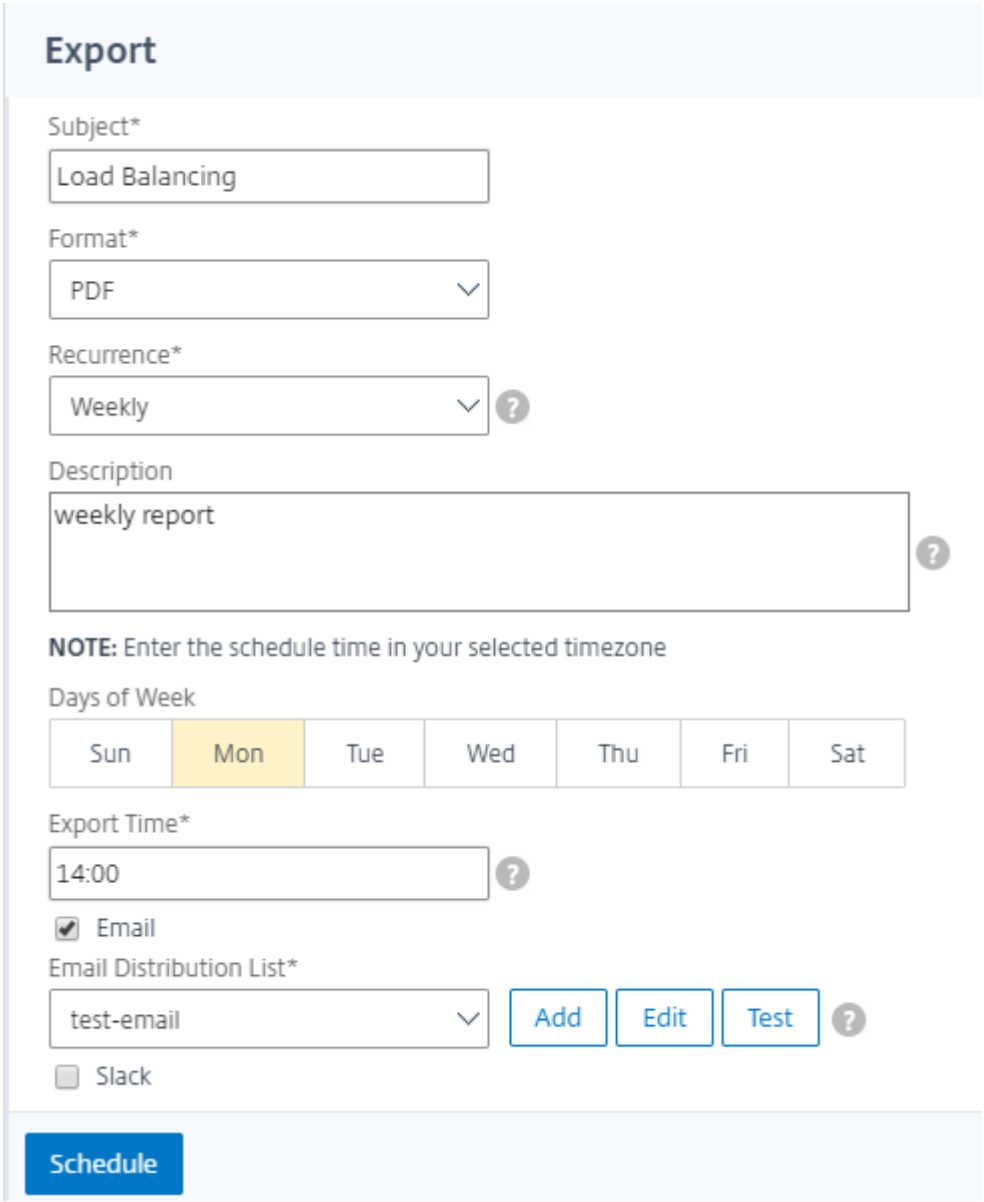
   b) 选择“计划报告”选项卡，计划定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

      i. 重复 -从下拉列表框中选择“每日”、“每周”或“每 月”。

      ii. 重复时间**-**以 24 小时格式将时间输入为 Hour: minute。

      iii. 电子邮件配置文件 -从下拉列表框中选择一个配置文件，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。

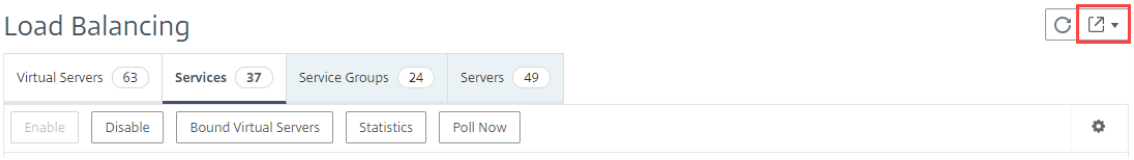


> 注意
>
> 如果选择 每月 重复，请确保输入希望报告以逗号分隔的所有日期。

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 NetScaler ADM 中，导航到 基础架构 **>** 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 NetScaler ADM GUI 上查看报告。

导出或计划网络功能报告的导出

February 6, 2024

您可以在 NetScaler Application Delivery Management (ADM) 中为选定的网络功能（例如负载平衡、内容切换、缓存重定向、全局服务器负载平衡 (GSLB)、身份验证和 NetScaler Gateway）生成综合报告。此报告允许您从高级视图了解 NetScaler 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

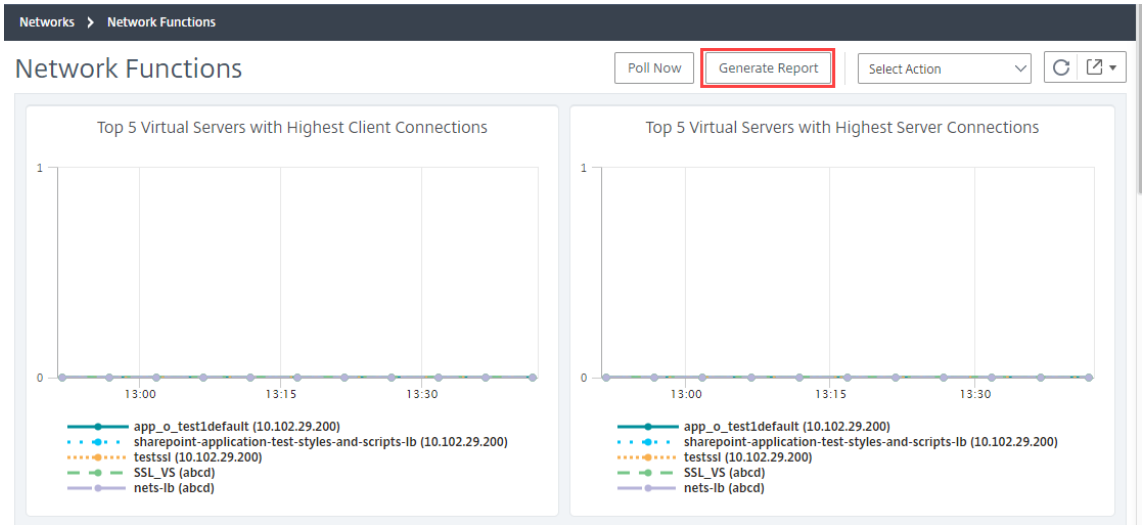
> 注意：
>
> 对于内容交换和缓存重定向虚拟服务器，Target LB 虚拟服务器列列出了所有 LB 服务器，即默认服务器和基于策略的服务器。
>
> - 服务名称
> - 服务组名称

您可以计划按不同的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 虚拟服务器和关联服务。
> - 对于内容切换和缓存重定向虚拟服务器，报告仅显示与关联负载平衡服务器的绑定。
> - 此报告中未列出 SSL 虚拟服务器，因为 NetScaler ADM 上未维护单独的 SSL 虚拟服务器列表。
> - 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。

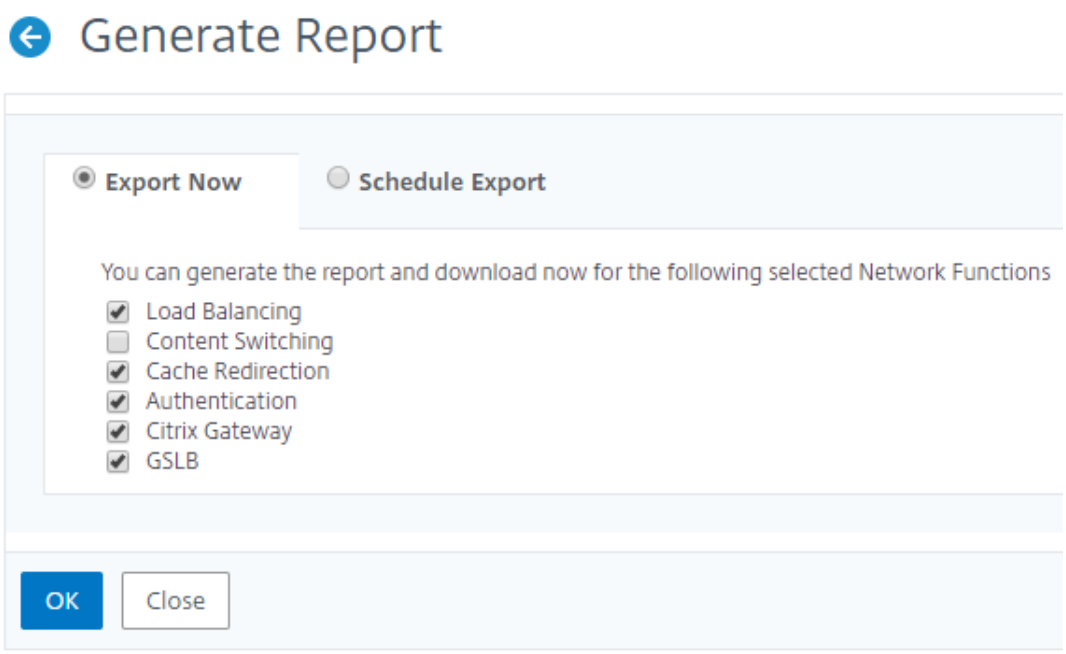
要导出和计划网络函数报告，请执行以下操作：

1. 导航到基础架构 **>** 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。

NetScaler ADC IP Address	NetScaler ADC HostName	Partition	Type of Virtual Server	Virtual Server	Target LB Virtual Server	Service	Service Group
10.	10.		Load Balancing	lb_test_1#10.10.10.10:80		adm_metric_collector_svc_10.106.171.41#10.10	
10.	10.		Load Balancing	lbvs_511#51.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	lbvs_521#52.1.1.1:80		test_1#10.102.61.105:80	
10.	10.		Load Balancing	SG_HS_DNS_MON#1.2.22.2:80			sc1
10.	10.		Load Balancing	SG_HS_DNS_MONgdvfffs#1.3.4.5:80			
10.	10.		Load Balancing	atest94#1.1.1.11:80			
10.	10.		Load Balancing	lbvs1_101#1.10.1.1:80			
10.	10.		Load Balancing	lbvs1_1010#1.10.1.10:80			
10.	10.		Load Balancing	lbvs1_10100#1.10.1.100:80			
10.	10.		Load Balancing	lbvs1_10101#1.10.1.101:80			
10.	10.		Load Balancing	lbvs1_10102#1.10.1.102:80			
10.	10.		Load Balancing	lbvs1_10103#1.10.1.103:80			

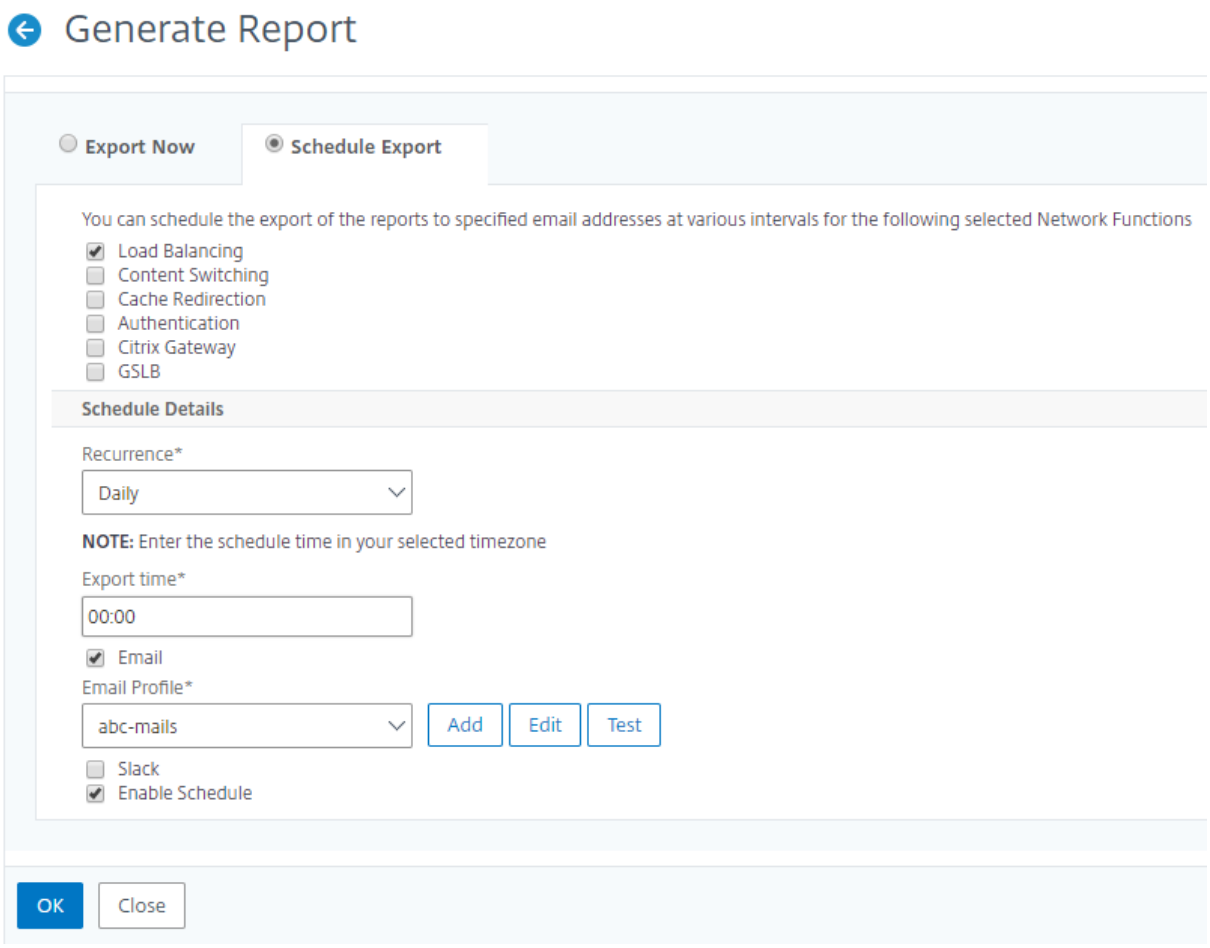
b) 选择“计划报告”选项卡，以计划定期生成和导出报告。指定报告生成定期循环设置，并创建报告导出到的电子邮件配置文件。

   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一个配置文件，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

February 6, 2024

您可以通过在 NetScaler Application Delivery Management (NetScaler ADM) 上监视您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。为确保应用程序获得最佳性能，您还部署了多个 Citrix Application Delivery Controller (NetScaler) 实例来实现负载平衡、内容切换或压缩流量。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，您必须定期监视网络性能，并确保所有资源都得到最佳使用。

现在，NetScaler 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。实例系列包括 NetScaler 实例。您可以为其生成报告的虚拟服务器如下所示：

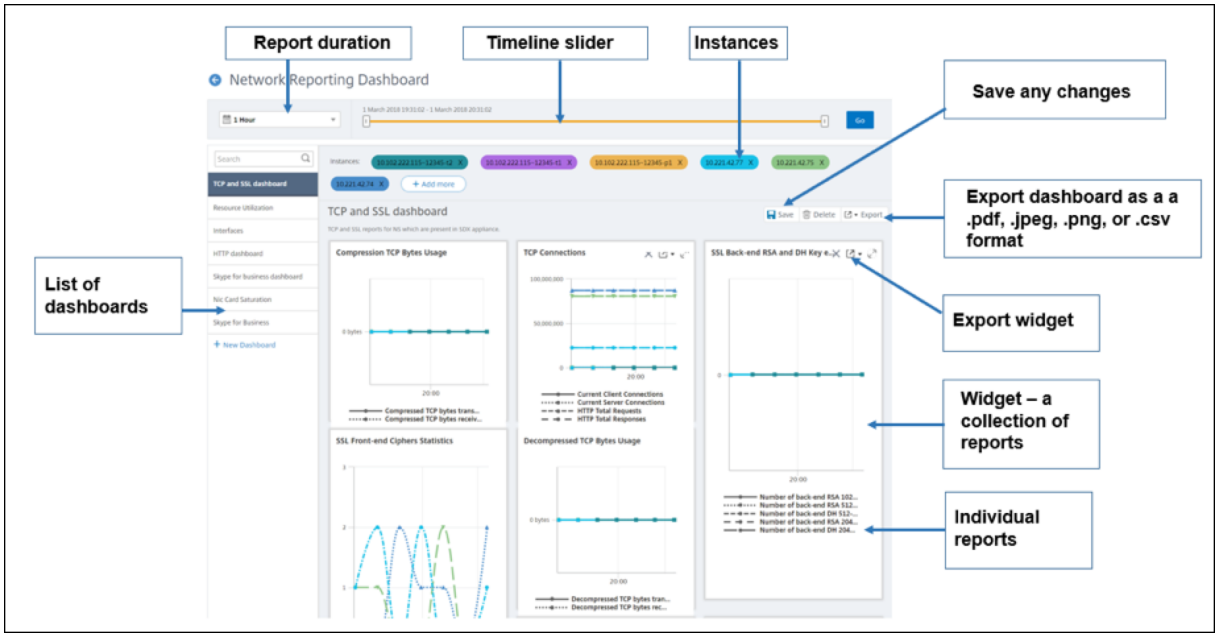
- 负载平衡服务器、服务和服务组
- 内容交换服务器
- 缓存重定向服务器
- 全局服务负载平衡 (GSLB)

- 身份验证
- NetScaler Gateway

NetScaler ADM 中的网络报告控制板是高度可定制的。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：

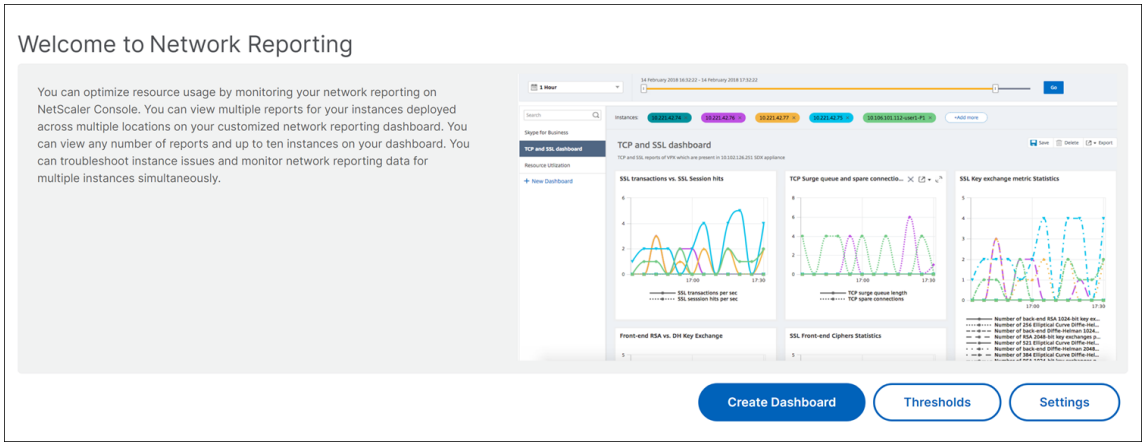


- 左侧面板列出了在 NetScaler ADM 中创建的所有自定义控制板。您可以单击其中一个以查看控制面板所组成的各种报告。例如，TCP 和 SSL 控制板包含与 TCP 和 SSL 协议相关的各种报告。
- 您可以使用多个微件自定义每个控制板以显示各种报告。小组件表示控制板上的报表，即更多相关报表的集合。例如，压缩 TCP 字节使用情况报告包含每秒传输和接收的压缩 TCP 字节的报告。
- 您可以显示一小时、一天、一周或一个月的报告。此外，您现在可以使用时间轴滑块选项来自定义 NetScaler ADM 上生成报告的持续时间。
- 您可以通过单击“X”删除报告。您也可以将报告导出为.pdf、.jpeg、.png 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 NetScaler 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。

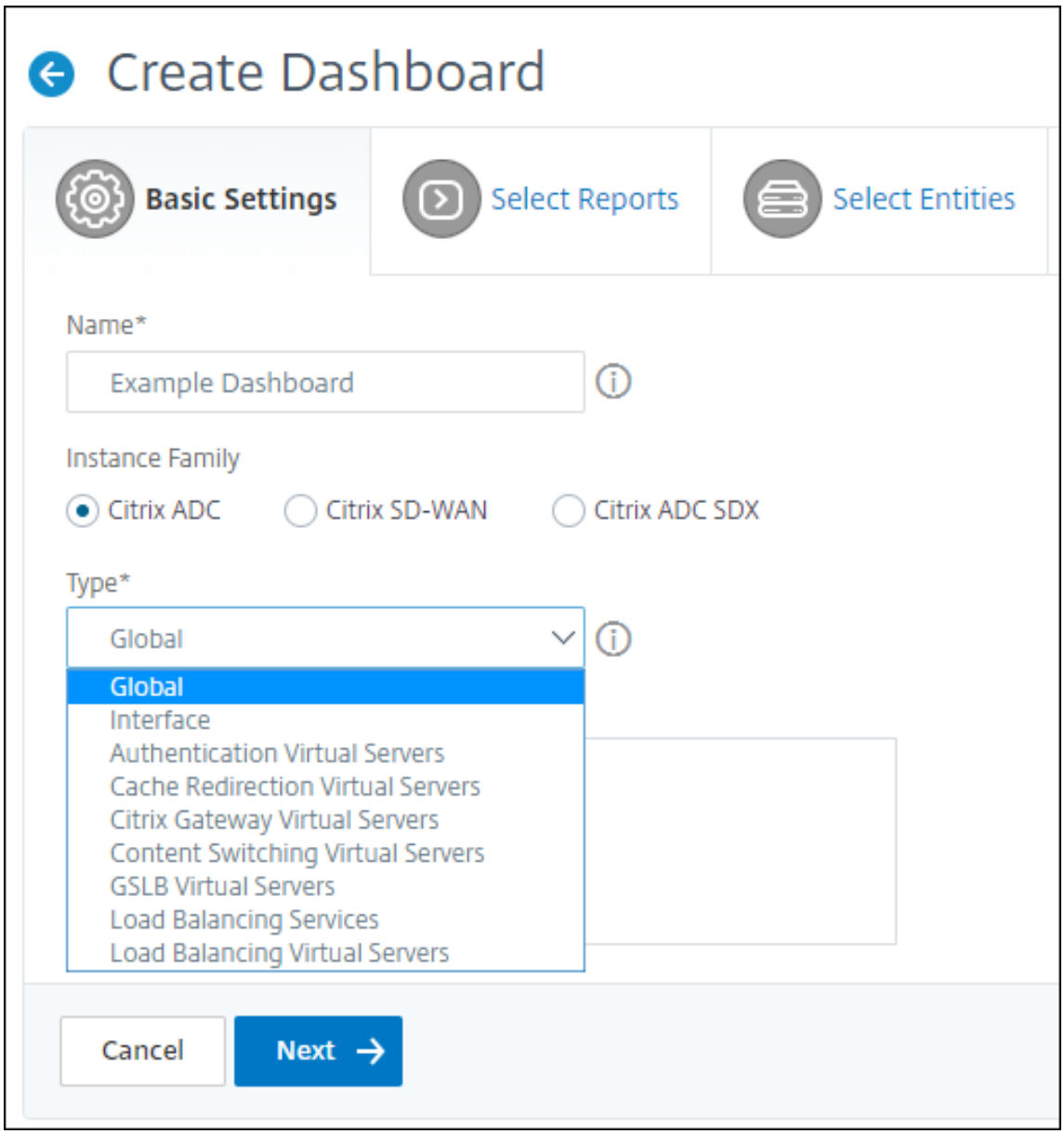
要查看或创建控制板，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 > 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“新建控制板”。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。

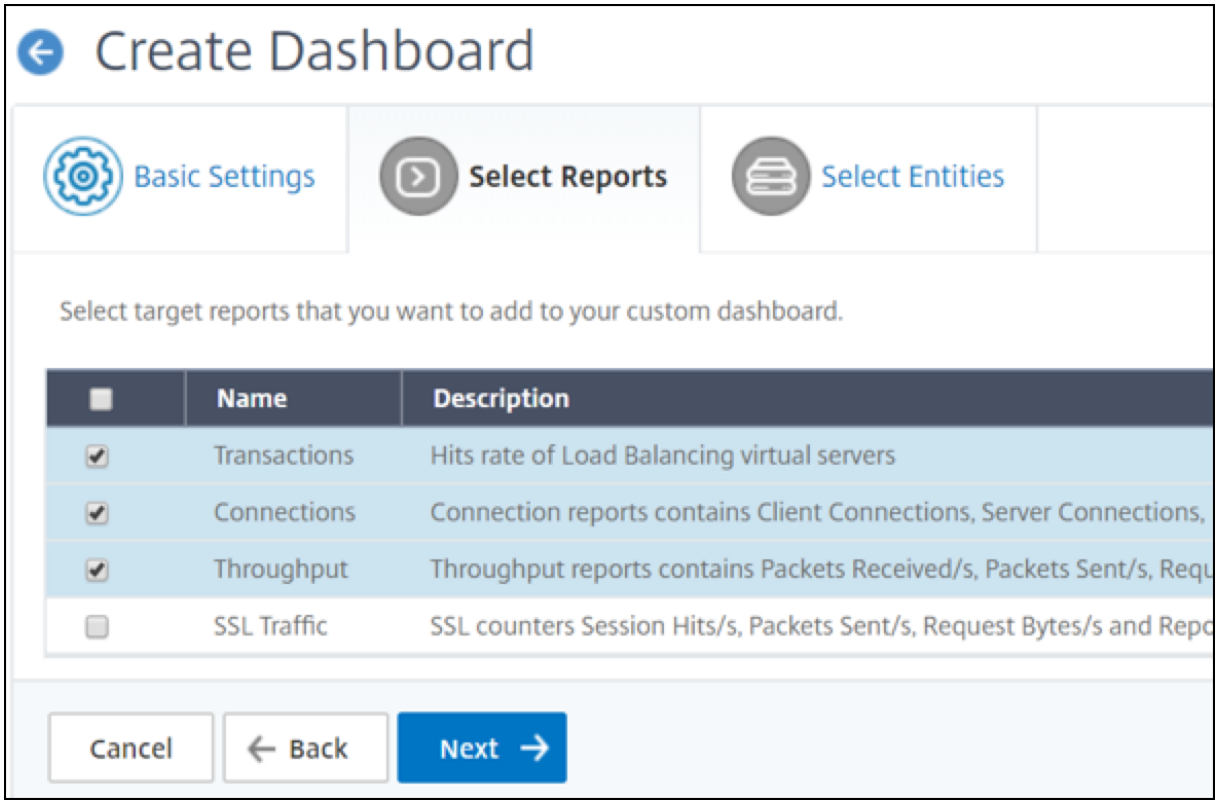
   b) 实例系列。选择实例类型——NetScaler 或 NetScaler SDX。

   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。为控制板键入有意义的描述。

5. 单击下一步。此时将显示实例和特定实体的所有受支持报告。

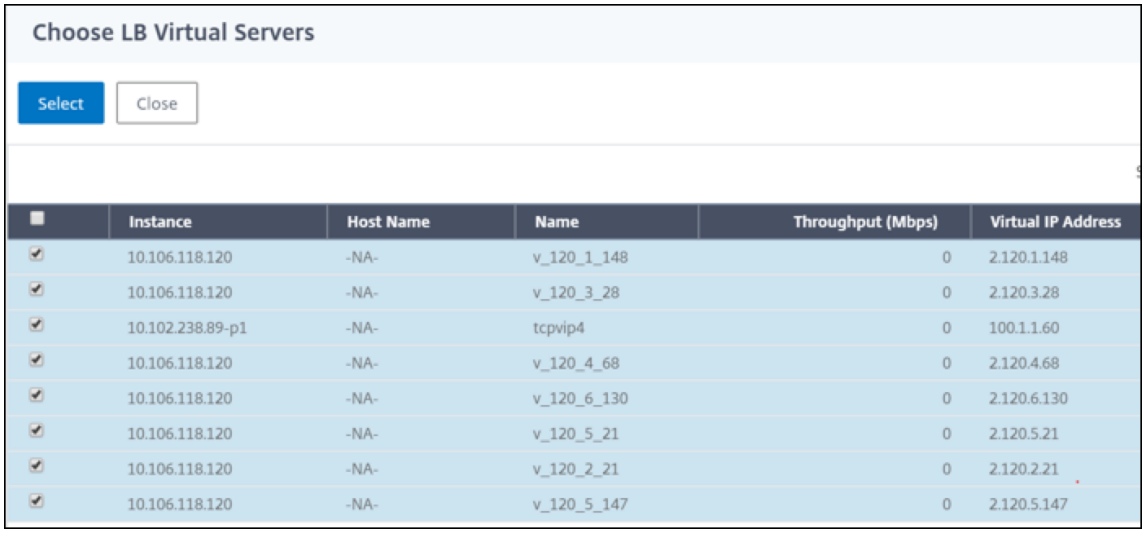
6. 在 选择报告 选项卡中，选择所需的报告。在此示例中，您可以选择事务、连接和吞吐量。单击下一步。



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，出现“选择 **LB** 虚拟服务器”窗口。

2. 选择要监视的实体。



3. 单击创建。

控制板已创建并显示您选择的所有报告。

> 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 NetScaler ADM 中导出报告。您需要编辑权限才能在 NetScaler ADM 中创建文件并导出该文件。

要导出控制板报告，请执行以下操作：

1. 导航到 基础结构 **>** 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. 点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”控制板页面。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，该报告每周生成一次，显示控制板的状态。该报告将覆盖时间和日期戳（如果由用户设置）。

> 注意
>
> - 如果选择“每周重复”，请确保选择要在哪个工作日安排报告。
> - 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。

在计划网络报告时，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。

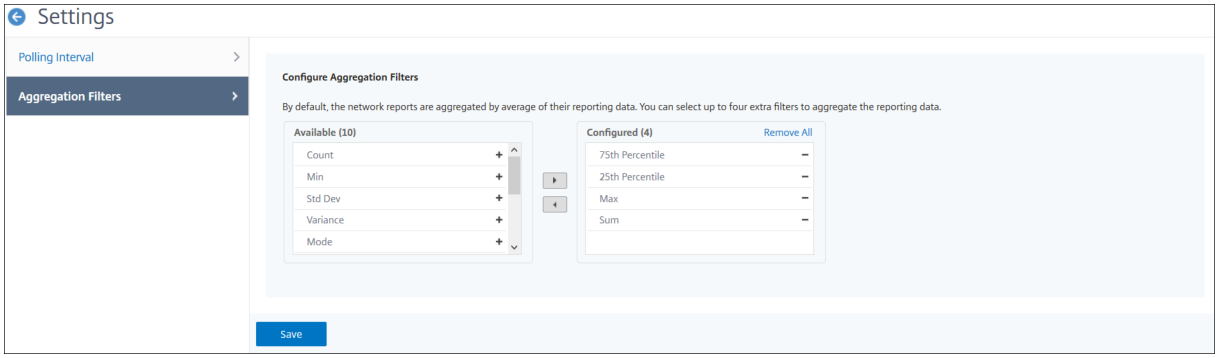
例如，对于来自特定虚拟服务器的网络报告，可以键入主题为“身份验证报告-10.106.118.120”，其中 10.106.118.120 是被监视虚拟服务器的 IP 地址。

> 注意
>
> 当前，此选项仅在您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，并在控制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，您可以分析并确保所有资源是否都得到最佳利用。导航到“网络”**>**“网络报告”，然后选择“持续时间 1 天或更晚”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，控制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。



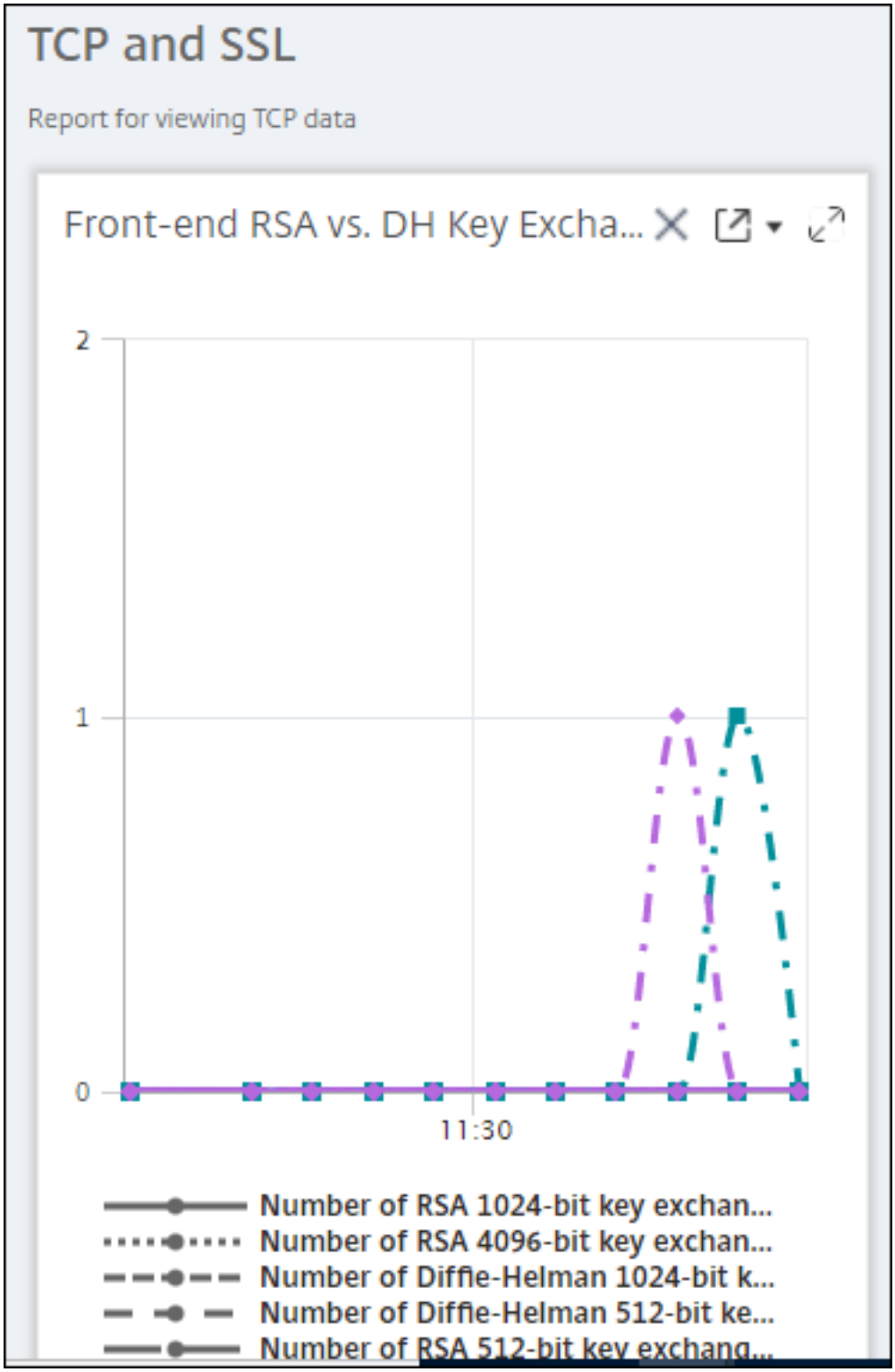
以下是您可以添加的聚合：

- 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

您最多可以向控制板添加 4 个聚合选项。添加聚合选项后，NetScaler 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 基础结构 **>** 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 **NetScaler ADM** 上管理网络报告的阈值

要监视 NetScaler 实例的状态，可以在计数器上设置阈值并在超过阈值时接收通知。在 NetScaler ADM 上，您可以配置阈值并查看、编辑和删除它们。

例如，当内容交换虚拟服务器的连接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（由规则指定）阈值时，将生成具有指定严重性的事件以表示存在性能相关问题。计数器值恢复到您认为正常的值时，将清除事件。可以通过导航到 基础架构 **>** 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。

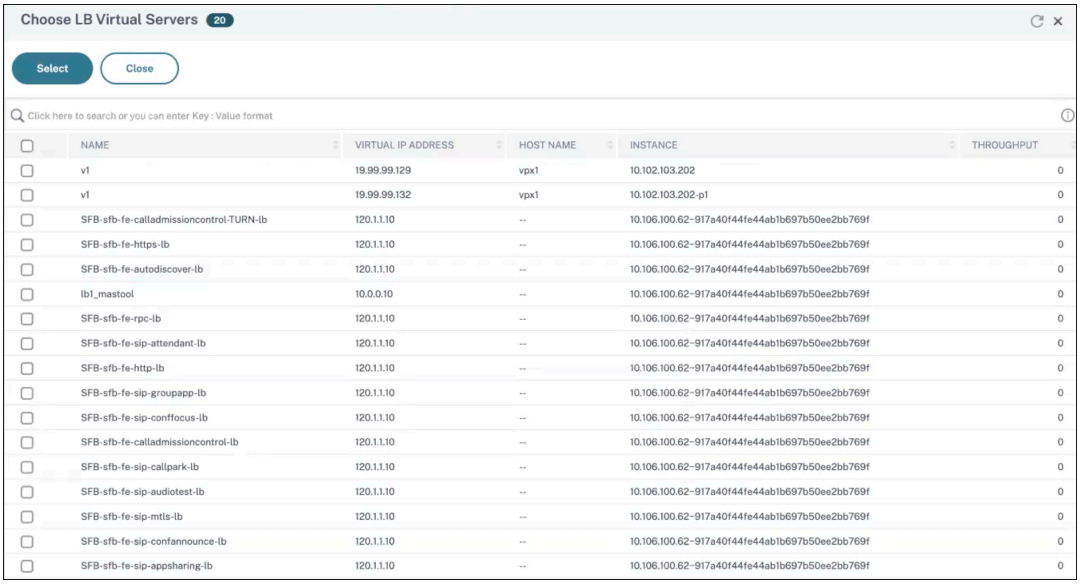
您还可以将操作与阈值关联，例如在超过阈值时发送电子邮件或 SMS 消息。

要创建阈值，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 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 NetScaler。
   - 报告名称。提供有关此阈值的信息的性能报告的名称。
3. 您还可以设置规则来指定何时生成或清除事件。您可以在“配置规则”部分下指定以下详细信息：
   - 指标。选择要为其设置阈值的指标。
   - 比较器。选择比较器以检查监视值是否大于或等于或小于或等于阈值。
   - 阈值。键入用于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 基础架构 **>** 事件 **>** 报告来查看“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. 您可以选择使用阈值设置的实例和实体。在实例部分中，选择以下选项之一：
   - 所有实例。为所有实例设置了阈值。
   - 特定实例。阈值是为特定实例设置的。使用右箭头将实例从“可用”列表移至“已配置”列表。阈值是为已配置列表中的实例设置的。
   - 特定实体。阈值是为特定实体设置的。

     单击“添加”以选择实体。

     将出现一个窗口，其中包含实体列表，具体取决于报告名称字段中选定的报告类型。在此示例中，将显示“选择 **LB** 虚拟服务器”窗口。



选择要为其设置阈值的实体。单击 **Select**（选择）。所选实体显示在“实例”部分中。

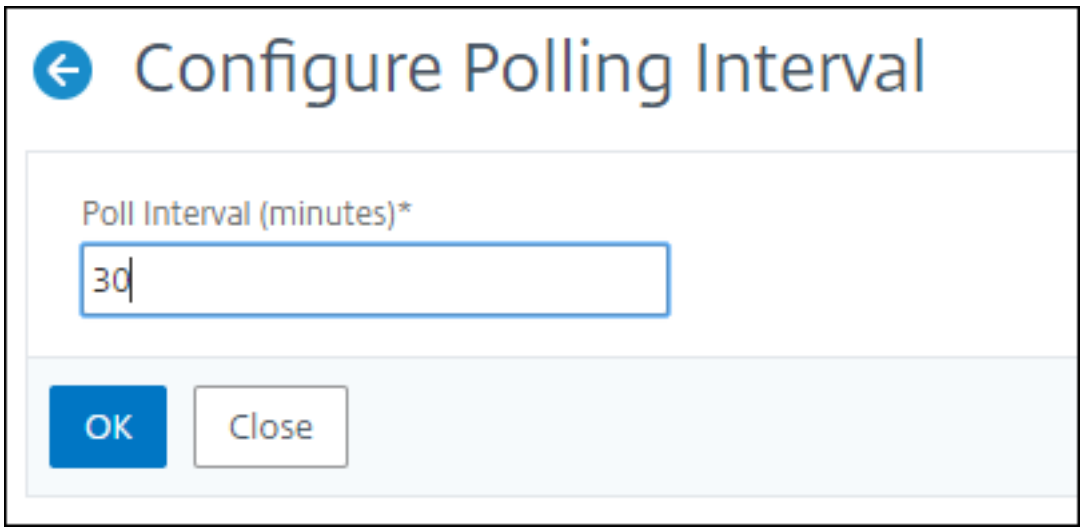
> 注意：
>
> 只有在报表 名称 中选择基于虚拟服务器的报表时，才会出现“特定实体”选项。例如，如果您选择 **LB** 服务统计信息

5. 您还可以添加事件消息。键入您希望在达到阈值时显示的消息。NetScaler ADM 将监视值和阈值附加到此消息中。
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 **Infrasturcture >** 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 NetScaler ADM 中配置网络报告数据的清除间隔。此设置限制存储在 NetScaler ADM 服务器数据库中的网络报告数据量。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 30 天或少于 1 天。

配置作业

February 6, 2024

NetScaler Application Delivery Management (NetScaler ADM) 配置管理流程可确保在网络中的多个 Citrix Application 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。

NetScaler 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 NetScaler 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 NetScaler 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
> 默认配置模板的 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，将配置保存为模板，然后使用它来配置作业。

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 NetScaler 11.0 版及更高版本的 NetScaler SDX 实例执行单捆绑升级。要执行单捆绑升级，请使用 NetScaler 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 NetScaler 实例上运行命令来升级 NetScaler 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 NetScaler 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 NetScaler 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
- 如何使用更正命令创建配置作业
- 如何使用配置模板创建审核模板
- 如何使用录制和播放来创建配置作业
- 如何在 NetScaler ADM 上使用主配置模板

创建配置作业

February 6, 2024

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 NetScaler Application Delivery Management (ADM) GUI 创建作业以跨实例更改配置、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，然后将其转换为 CLI 命令。

可以使用 NetScaler 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。

要在 **NetScaler ADM** 上创建配置作业，请执行以下操作：

1. 导航到 基础架构 **>** 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，指定任务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。

    - 您可以输入命令或从保存的配置模板中导入现有命令。
    - 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在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。要指定您的自定义命令，请启用自定义回滚选项。

> 重要
>
> 事项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 NetScaler 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 NetScaler ADM 服务器。

   b) 输入您为所有实例定义的变量的通用值

   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。

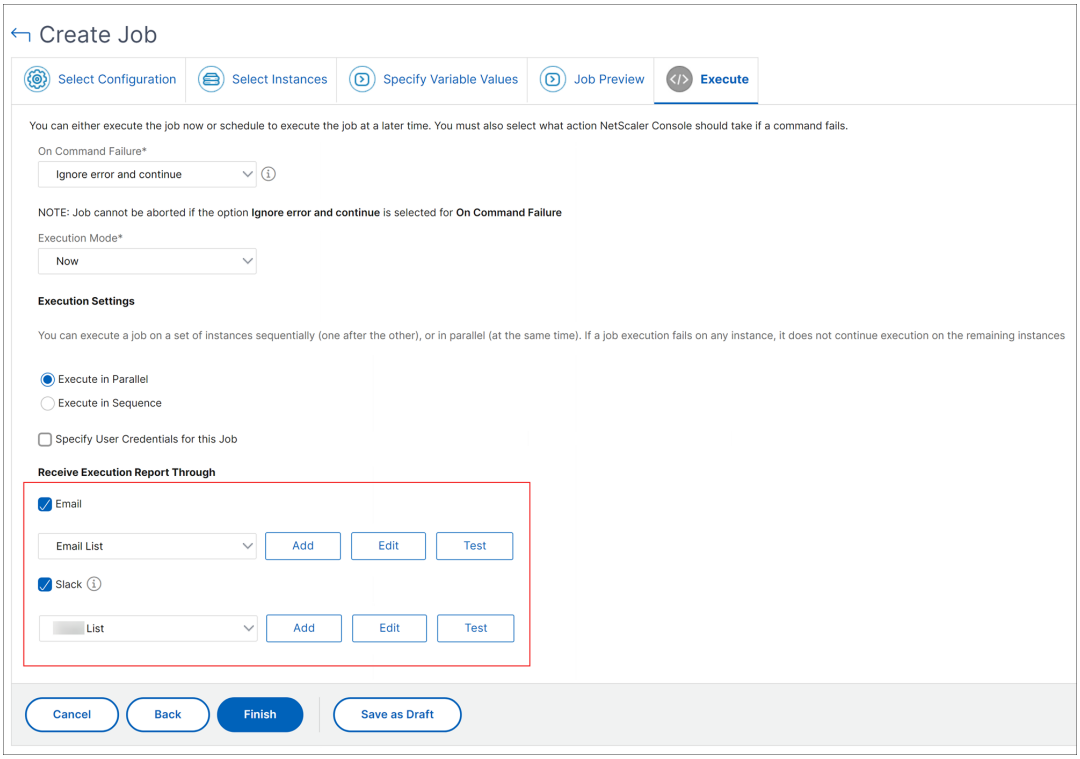
1. 导航到 基础架构 **>** 配置作业。
2. 选择要启用电子邮件和 Slack 通知的作业，然后单击 编辑。
3. 在“执行”选项卡中，转到“通过以下方式接收执行报告”窗格：

   - 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分发列表。

     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的详细信息。

   - 选中 **Slac** k 复选框，然后选择要向其发送执行报告的 Slack 频道。

     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 基础架构 **>** 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“通过以下方式接收执行报告”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分发列表。

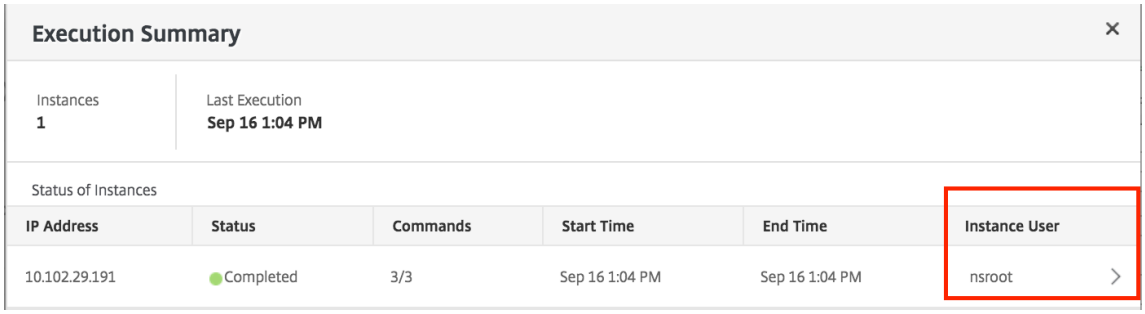
     如果要添加电子邮件通讯组列表，请单击“添加”并指定电子邮件服务器的详细信息。
   - 选中 **Slac** k 复选框，然后选择要向其发送执行报告的 Slack 频道。

     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 基础架构 **>** 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



配置审核

February 6, 2024

本文档包括：

- 创建审核模板
- 查看审核报告
- 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 NetScaler 实例的配置审核

升级作业

February 6, 2024

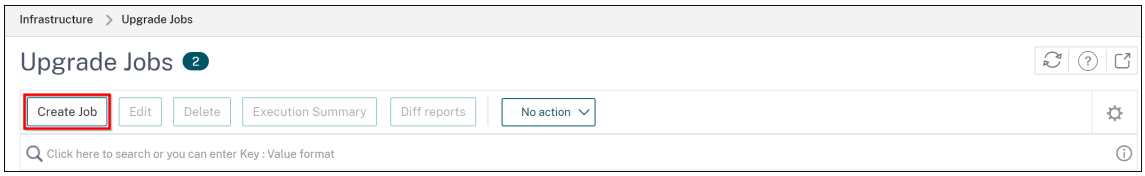
您可以使用 NetScaler ADM 创建以下维护任务。然后，您可以将维护任务安排在特定的日期和时间。

- 升级 NetScaler 实例
- 升级 NetScaler SDX 实例
- 升级 NetScaler BLX 实例

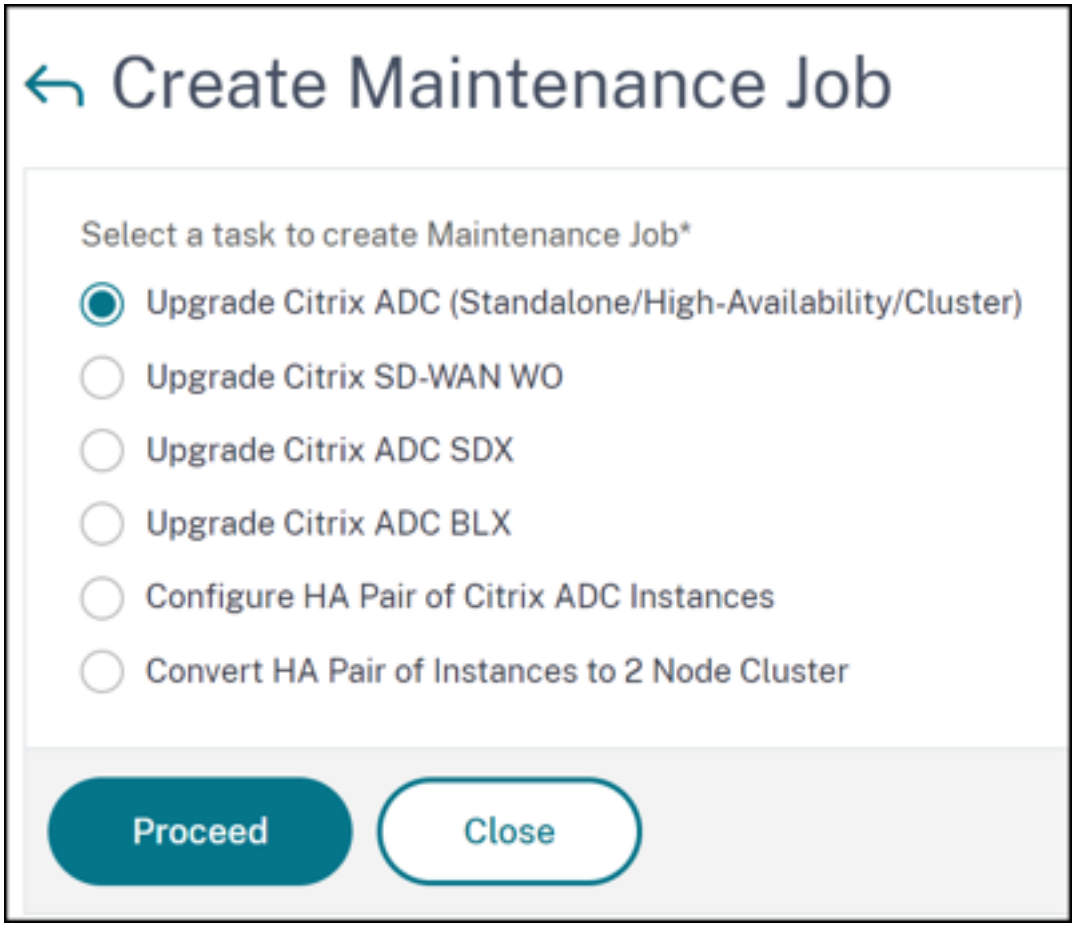
- 升级 AutoScale 组中的 NetScaler 实例
- 配置 NetScaler 实例的高可用性对
- 将 HA 实例对转换为群集

计划升级 **NetScaler** 实例

1. 导航到基础结构 **>** 升级作业。单击 创建作业。

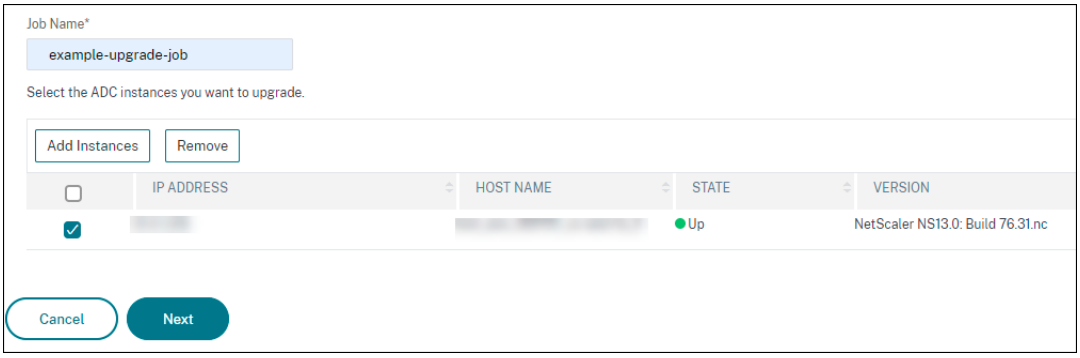


2. 在 创建维护作业中，选择 升级 **NetScaler**（独立/高可用性/群集），然后单击 继续。



3. 在选择实例中，为作业名称键入您选择的名称。
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”以选择图像。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。
   - 设备 - 从 NetScaler ADM 文件浏览器中选择实例升级文件。NetScaler ADM GUI 显示 `/var/mps/mps_images` 中存在的实例文件。
     - 如果所选映像已可用，请跳过将映像上载到 **ADC** - 如果映像已存在于 NetScaler 实例中，请选择此选项。
     - 成功升级时从 **NetScaler** 清除软件映像-选择此选项可在实例升 级后清除 ADC 实例中上载的映像。

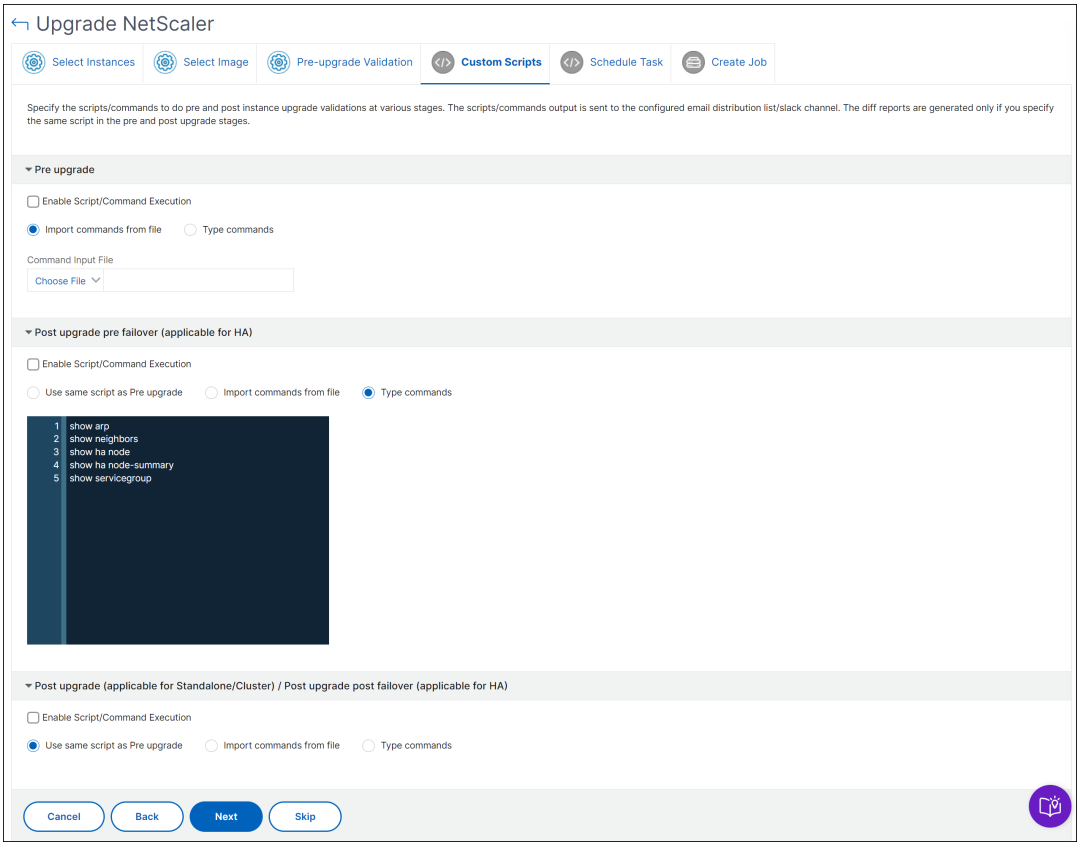
6. 单击 下一步 开始对所选实例进行升级前验证。

   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
   >
   > 如果指定群集 IP 地址，NetScaler ADM 将仅在指定的实例上执行升级前验证，而不会在其他群集节点上执行升级前验证。

7. 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。



可以使用自定义脚本在实例升级前后检查更改。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。

8. 单击下一步。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，请选择对高可用性 中的节点执行两阶段升级。

     如果要升级高可用性对中的其他实例，请指定执行日期和开始时间。

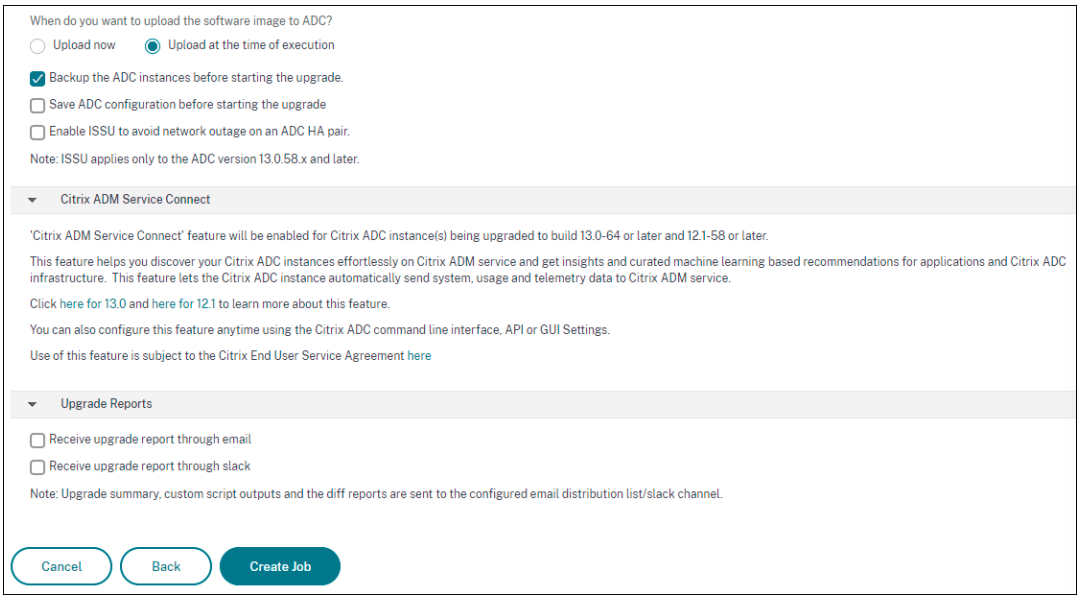
9. 单击下一步。在 创建作业中，指定以下详细信息：

   a) 指定您希望何时将映像上载到实例：

      - 立即上载 -选择此选项可立即上载图片。但是，升级作业将在计划的时间运行。
      - 执行时上载 -选择此选项可在升级作业执行时上载映像。

- 在开始升级之前备份 **ADC** 实例。-创建所选 ADC 实例的备份。
- 在开始升级之前保存 **ADC** 配置 - 保存升级前在实例上配置的配置作业。
- 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。

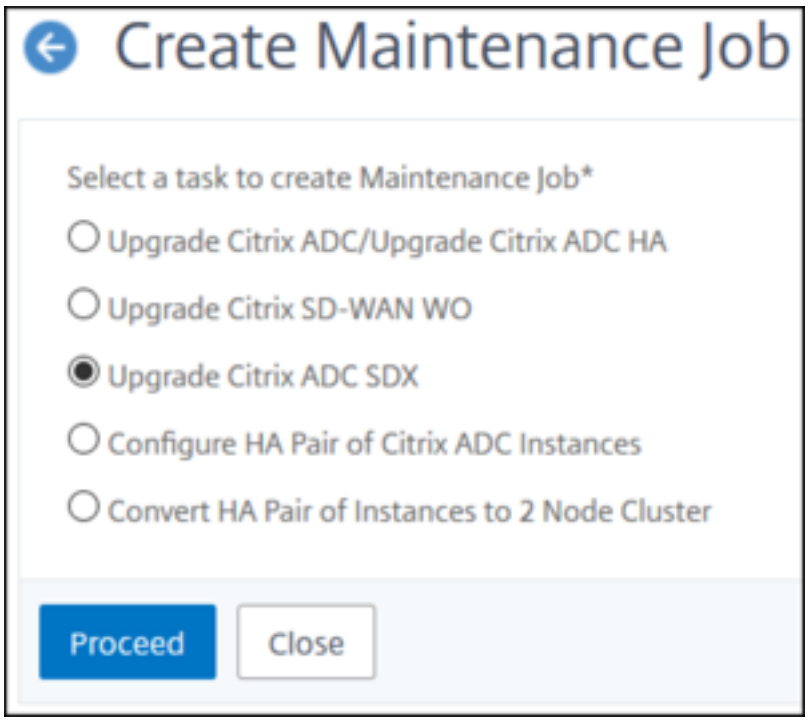
- **NetScaler ADM Service Connect** - 如果要升级到版本 **13.0-64** 或更高版本以及 **12.1-58** 或更高版本，NetScaler ADM Service Connect 将自动启用。有关详细信息，请参阅使用 NetScaler ADM Service Connect 对 NetScaler 实例进行低接触式加载。
- 通过电子邮件接收执行报告 -通过电子邮件发送执行报告。要添加电子邮件通讯组列表，请参阅 创建电子邮件通讯组列表。
- 通过松弛接收执行报告 -以松弛方式发送执行报告。要添加 Slack 配置文件，请参阅 创建 Slack 配置文件。



10. 单击 创建作业。

计划升级 **NetScaler SDX** 实例

1. 导航到基础结构 **>** 升级作业。单击 创建作业。
2. 选择 升级 **NetScaler SDX** ，然后单击 继续。

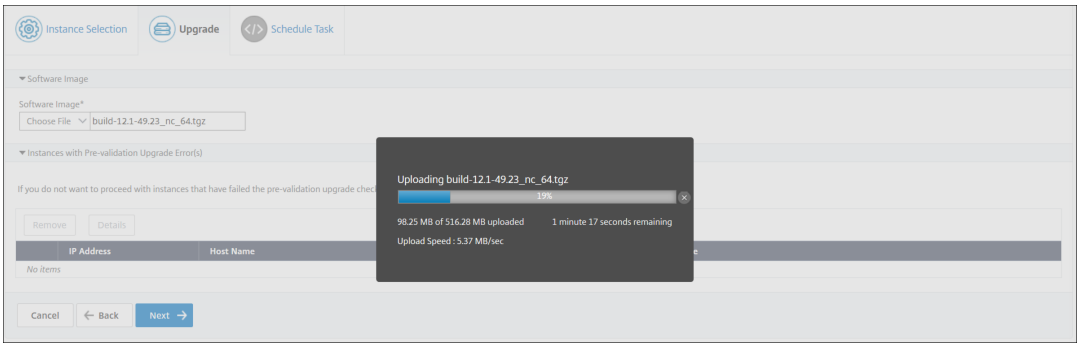


3. 在 升级 **NetScaler SDX** 页面的 实例选择”选 项卡中：

   a) 添加任务名称。

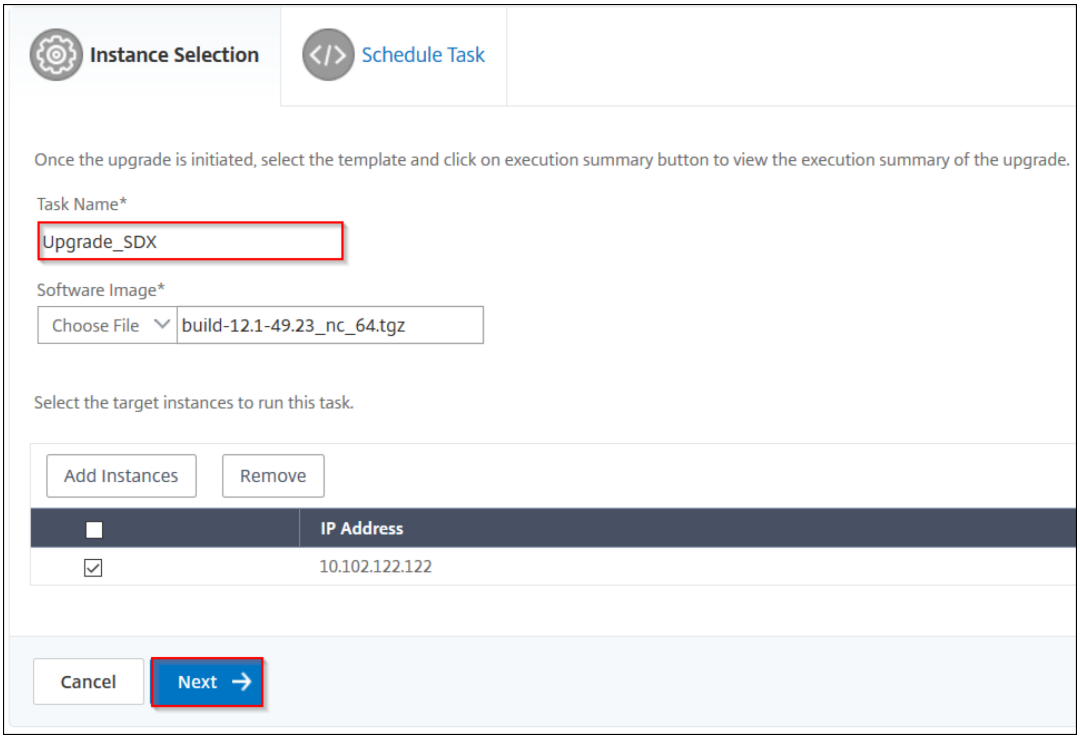
   b) 从软件映像列表中，选择本地（您的本地计算机）或设备（构建文件必须存在于 NetScaler ADM 虚拟设备上）。

   上载过程开始。

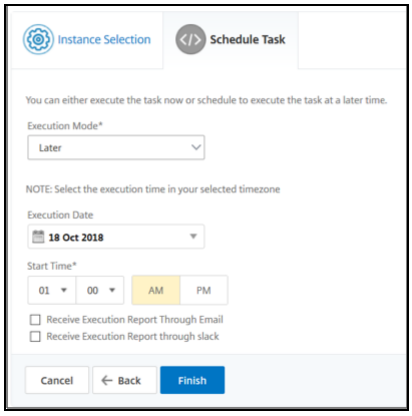


   c) 添加要在其上运行升级过程的 NetScaler SDX 实例。

   d) 单击下一步。



4. 在“计划任务”选项卡上，从“执行模式”列表中选择“立即 升级 NetScaler SDX 实例”，然后单击完成。
5. 要稍后升级 NetScaler SDX 实例，请从 执行模式 列表中选择以 后。然后，您可以选择升级 NetScaler 实例的执行日期和开始时间，然后单击 完成

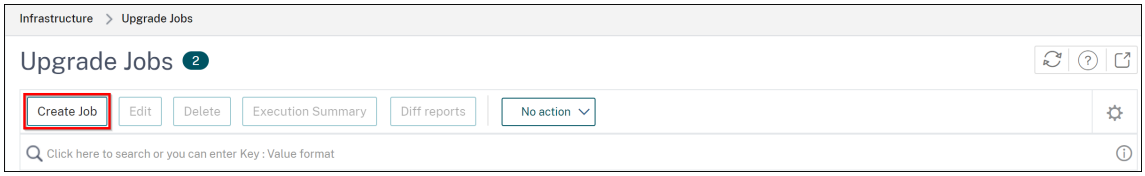


6. 您还可以启用电子邮件和 slack 通知以接收升级 NetScaler SDX 实例的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

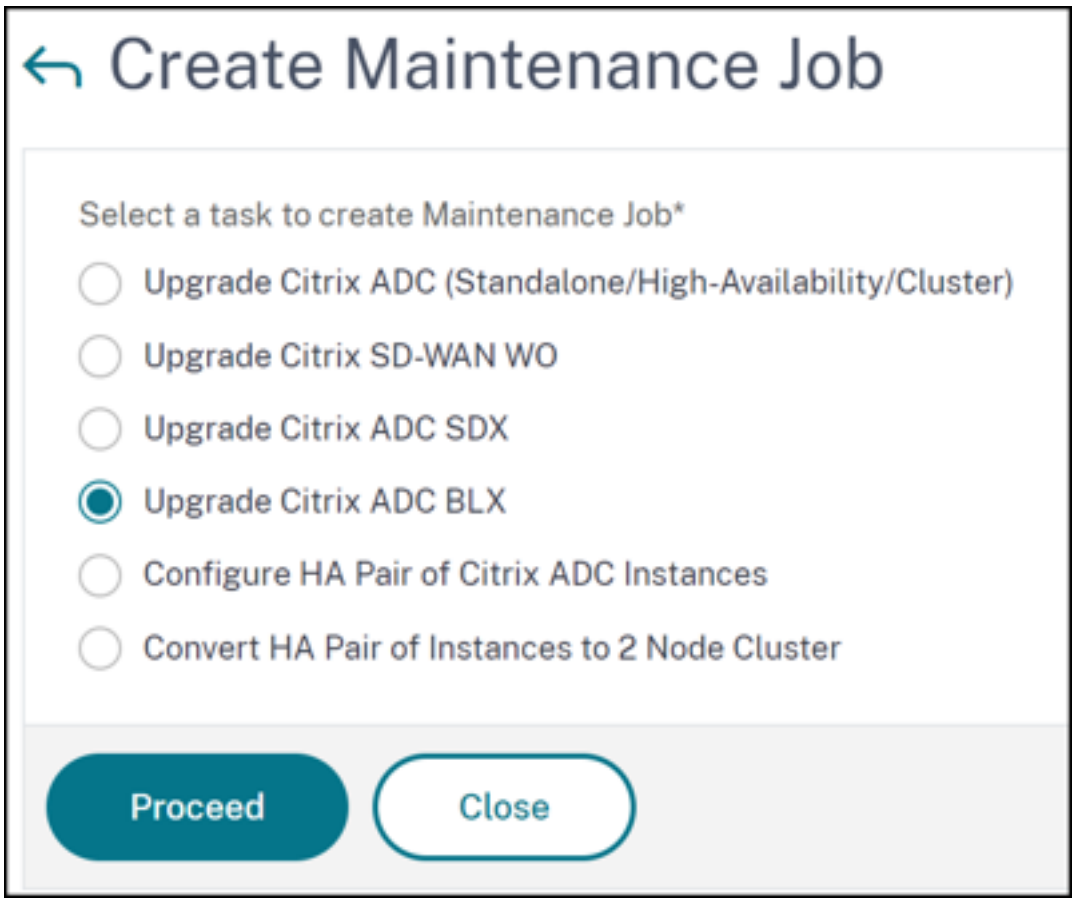
   有关配置电子邮件通讯组列表和 Slack 通道的详细信息，请参阅 NetScaler 实例的计划升级中的步骤 **8**

计划升级 **NetScaler BLX** 实例

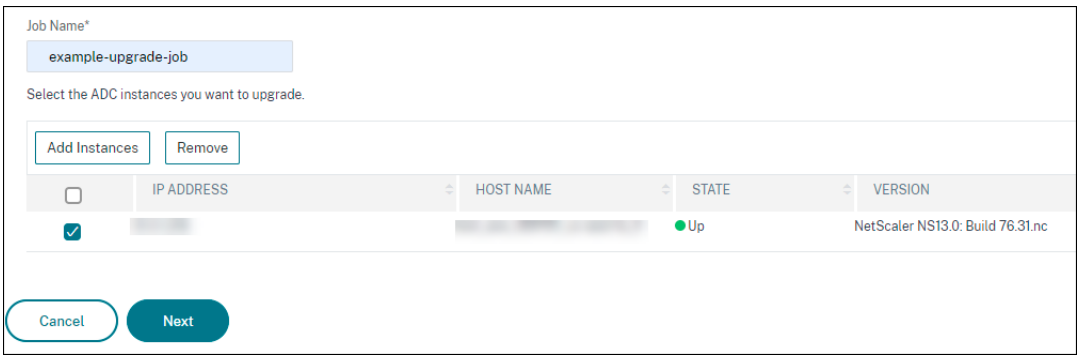
1. 导航到基础结构 **>** 升级作业。单击 创建作业。



2. 在 创建维护作业中，选择 升级 **NetScaler BLX** ，然后单击 继续。

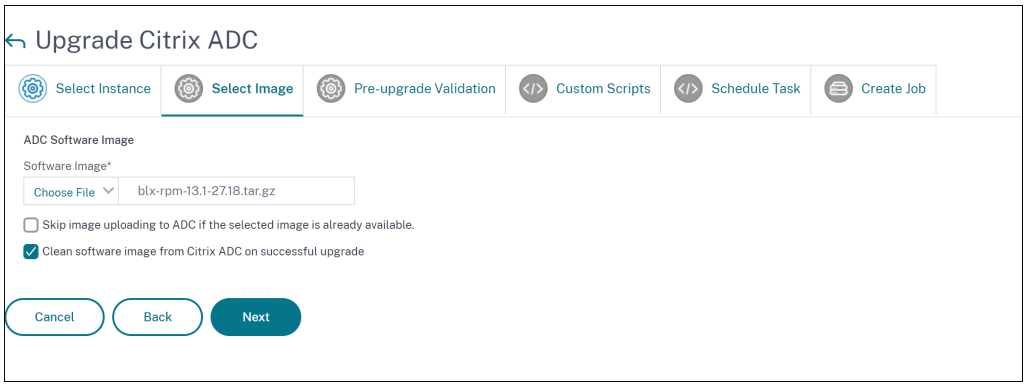


3. 在选择实例中，为作业名称键入您选择的名称。
4. 单击 添加实例 以添加要升级的 BLX 实例。
    - 要升级 HA 对，请指定主节点或辅助节点的 IP 地址。但是，建议使用主实例升级 HA 对。
    - 要升级群集，请指定群集 IP 地址。



5. 单击“下一步”选择映像。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。
   - 设备 - 从 NetScaler ADM 文件浏览器中选择实例升级文件。NetScaler ADM GUI 显示 `/var/mps/mps_images` 中存在的实例文件。
     - 如果所选映像已可用，请跳过将映像上载到 **ADC** - 如果映像已存在于 NetScaler 实例中，请选择此选项。
     - 成功升级时从 **NetScaler** 清除软件映像-选择此选项可在实例升 级后清除 ADC 实例中上载的映像。



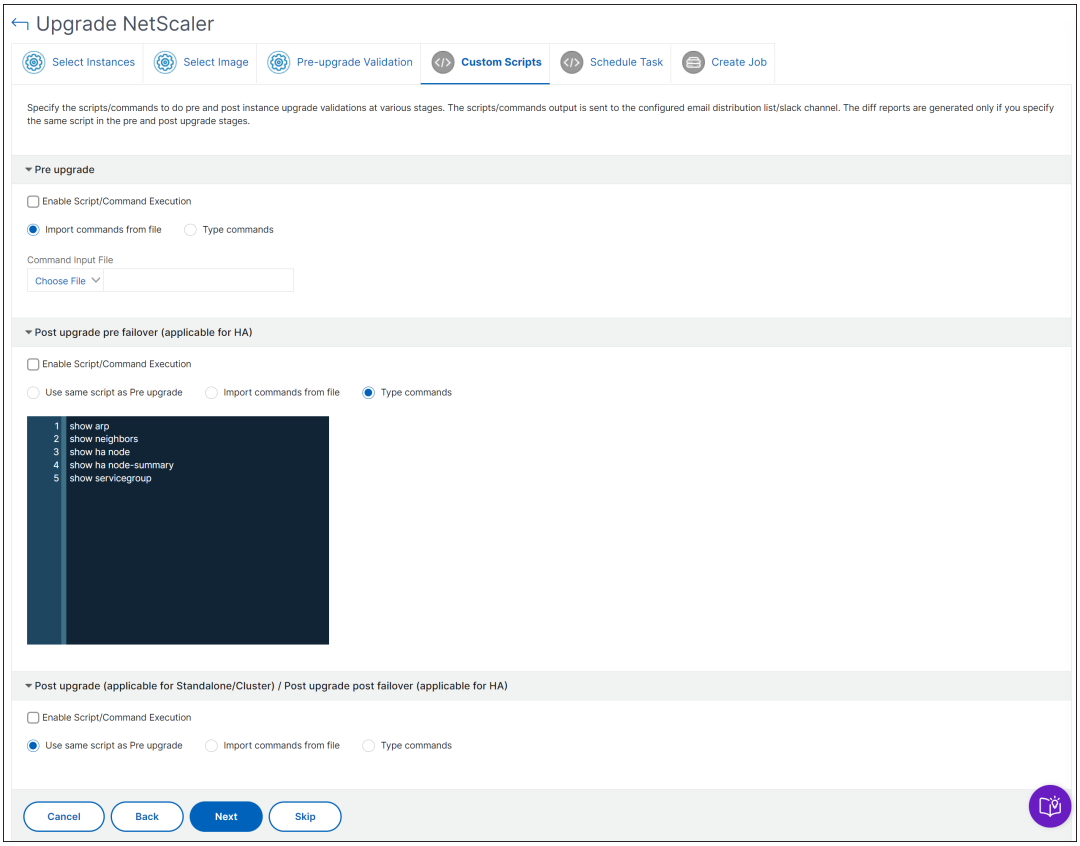
6. 单击 下一步 开始对所选实例进行升级前验证。

   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
   >
   > 如果指定群集 IP 地址，NetScaler ADM 将仅在指定的实例上执行升级前验证，而不会在其他群集节点上执行升级前验证。

7. 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。



可以使用自定义脚本在实例升级前后检查更改。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。

8. 单击下一步。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 HA 对，请选择对高 可用性中的节点执行两阶段升级。

     如果要升级高可用性对中的其他实例，请指定执行日期和开始时间。

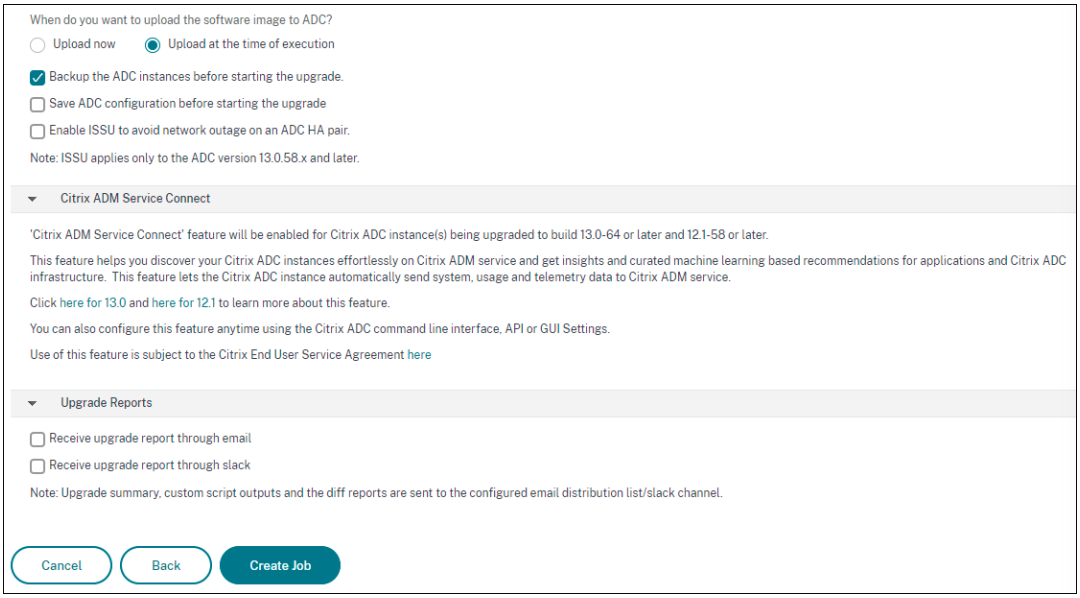
9. 单击下一步。在 创建作业中，指定以下详细信息：

   a) 指定您希望何时将映像上载到实例：

      - 立即上载 -选择此选项可立即上载图片。但是，升级作业将在计划的时间运行。
      - 执行时上载 -选择此选项可在升级作业执行时上载映像。

- 在开始升级之前备份 **ADC** 实例 -创建所选 ADC 实例的备份。
- 在开始升级之前保存 **ADC** 配置 - 保存升级前在实例上配置的配置作业。
- 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。

- **NetScaler ADM Service Connect** - 如果要升级到版本 **13.0-64** 或更高版本以及 **12.1-58** 或更高版本，NetScaler ADM Service Connect 将自动启用。有关详细信息，请参阅使用 NetScaler ADM Service Connect 对 NetScaler 实例进行低接触式加载。
- 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。



10. 单击 创建作业。

计划升级自动扩展组

执行以下步骤以升级属于 AutoScale 组的云服务中的所有实例：

1. 导航到基础结构 **>** 升级作业。单击 创建作业。
2. 选择升级 **AutoScale** 组，然后单击继续。
3. 在 升级设置 选项卡中：
   a) 选择要升级的 **AutoScale** 组。
   b) 在映像中，选择 NetScaler 版本。此映像是 AutoScale 组中 NetScaler 实例的现有版本。

c) 在 **NetScaler** 映像中，浏览要升级到的 NetScaler 版本文件。

如果选中“平滑升级”，则升级任务将等到指定的耗尽连接期限到期。

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：要启动 NetScaler 实例，请立即升级。
- 稍后：稍后启动 NetScaler 实例升级。

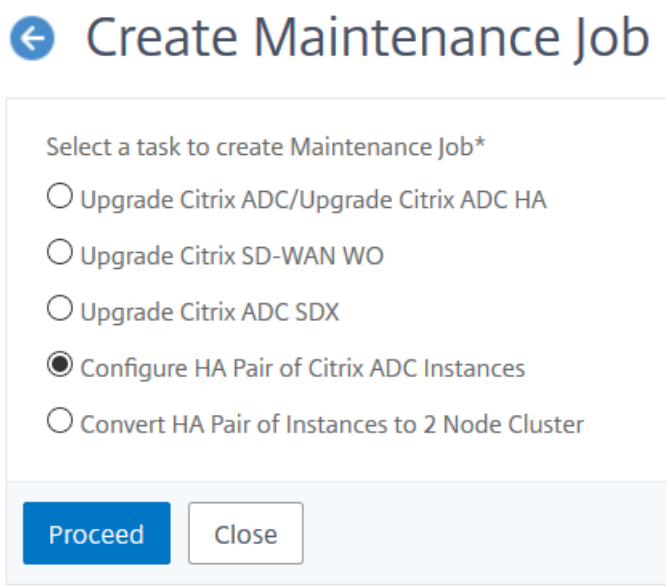
b) 如果选择“以 后 选项，请在要启动升级任务时选择“执行日期”和“开始时间”。

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。

安排配置 **NetScaler** 实例的高可用性对

1. 导航到基础结构 **>** 升级作业。单击 创建作业。
2. 选择 配置 **NetScaler** 实例的 **HA** 对，然后单击 继续。



3. 在 **NetScaler HA** 对 页面的 实例选择”选 项卡中：

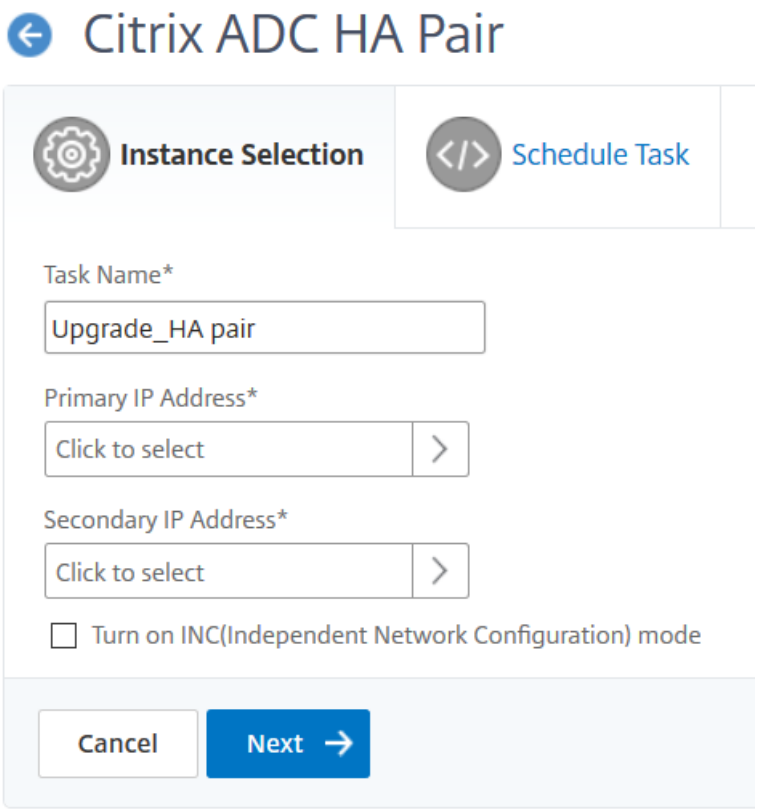
a) 添加任务名称。

b) 输入主 IP 地址。

c) 输入辅助 IP 地址。

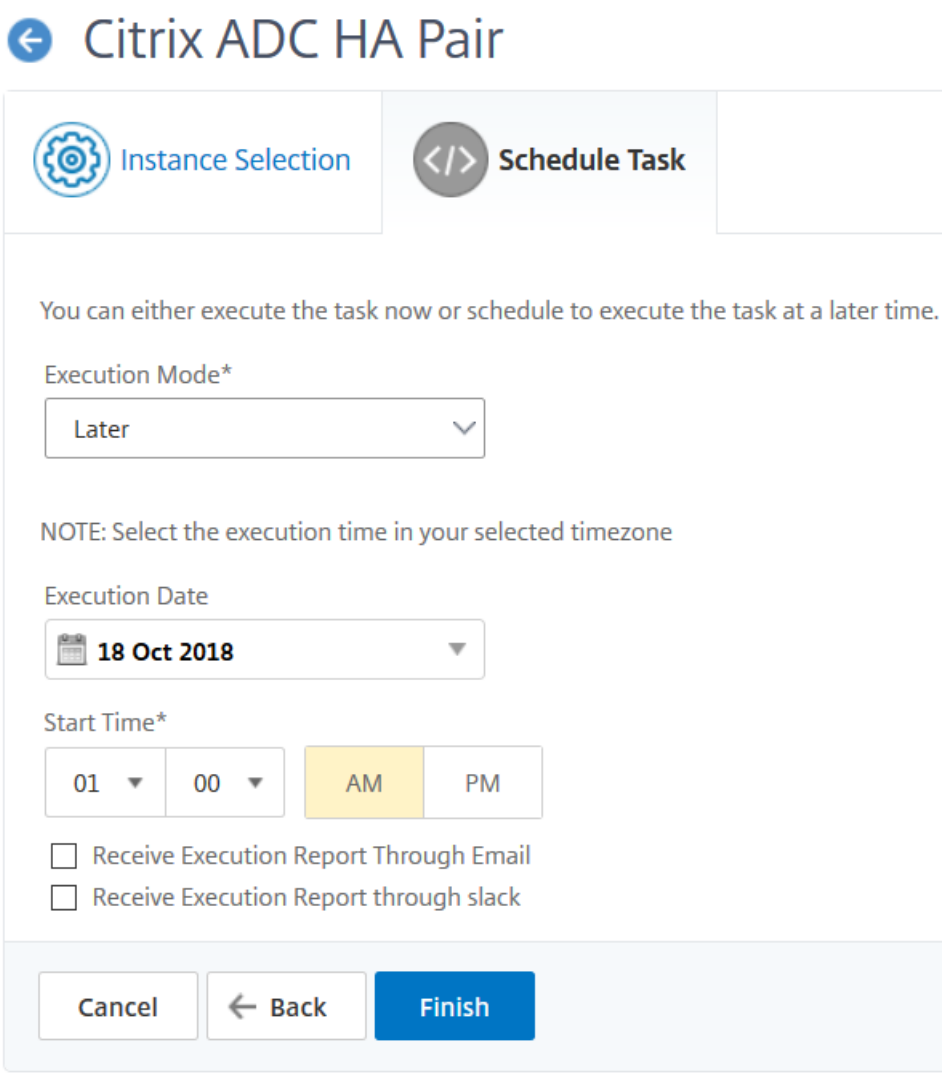
d) 单击下一步。

e) 如果您在两个子 网中有 **HA** 对实例，请单击以启用打开 **INC**（独立网络配置）模式。



4. 在计划任务选项卡上，从执行模式列表中选择立即立即升级 NetScaler 实例，然后单击完成。

5. 要稍后升级 NetScaler HA 对，请从 执行模式 列表中选择以 后。然后，您可以选择升级 NetScaler 实例的执行日期和开始时间，然后单击 完成。

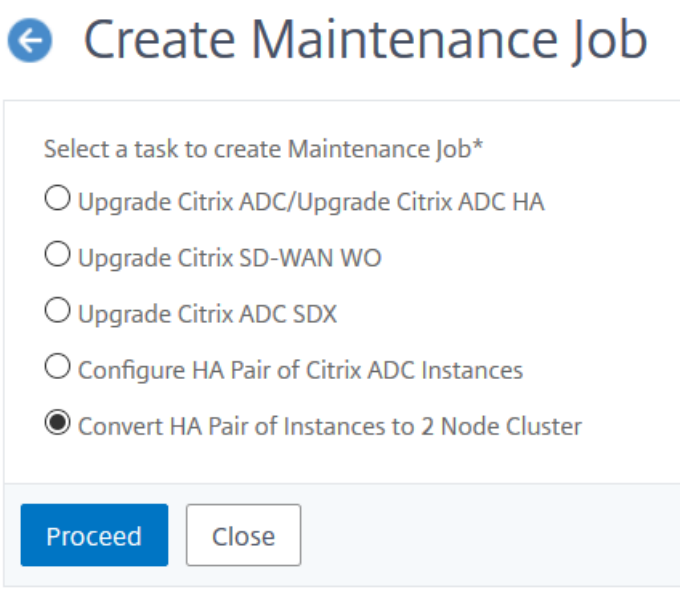


6. 您还可以启用电子邮件和 slack 通知以接收创建 ADC HA 对的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

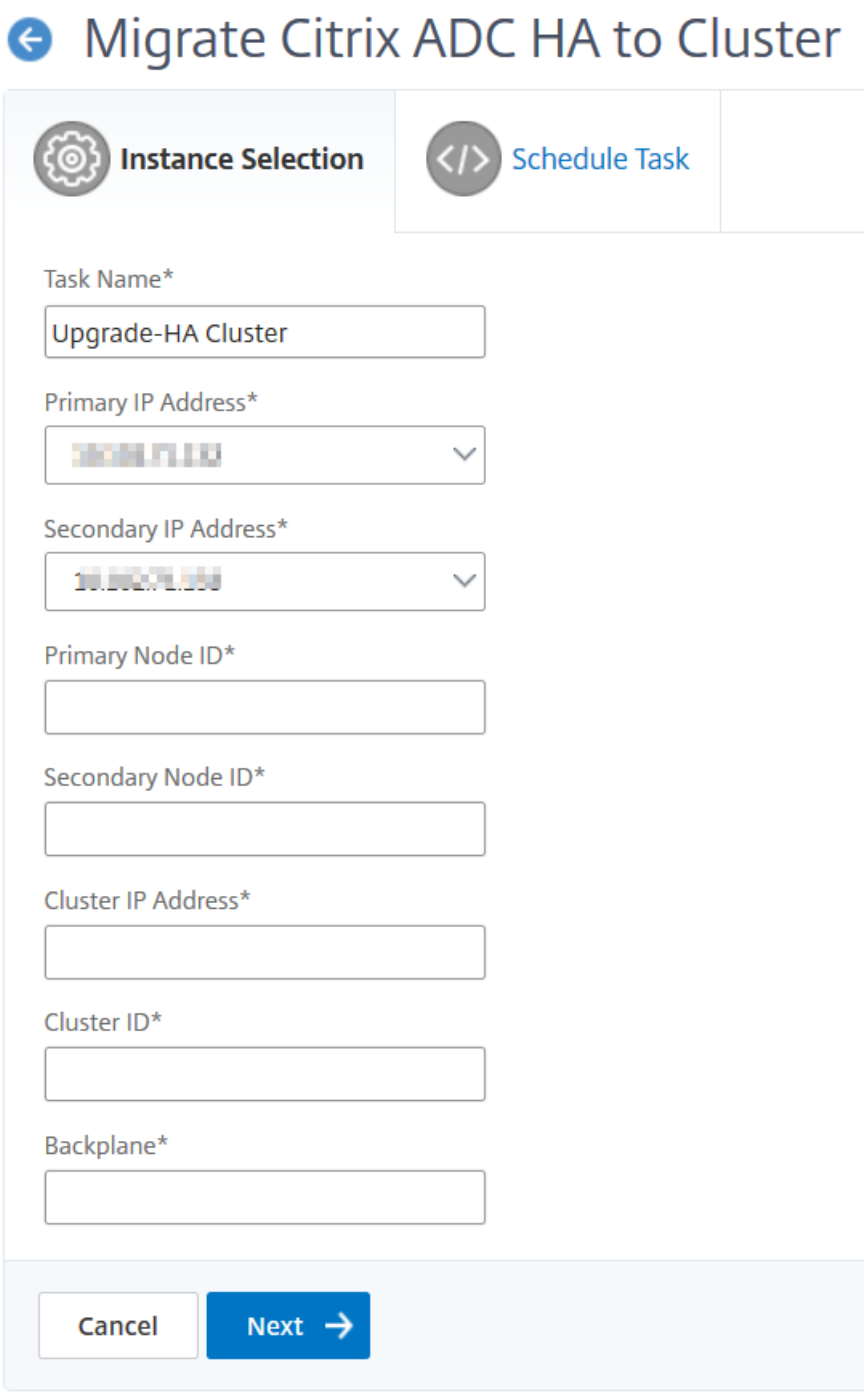
   有关配置电子邮件通讯组列表和 Slack 通道的详细信息，请参阅 NetScaler 实例的计划升级中的步骤 **8**

计划将 **HA** 实例对转换为群集

1. 导航到基础结构 **>** 升级作业。单击 创建作业。
2. 选择 将 **HA** 实例对转换为 **2** 节点群集，然后单击 继续。



3. 在 将 **NetScaler HA** 迁移到群集 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 IP 地址、主节点 ID、辅助节点 ID、群集 IP 地址、群集 ID 和背板，然后单击 下一步。



4. 在计划任务选项卡上，从执行模式列表中选择立即立即升级 NetScaler 实例，然后单击完成。
5. 要稍后升级，请从“执行模式”列表中选择以 后。然后，您可以选择升级 NetScaler HA 对实例的 执行日期 和开始时间，然后单击 完成。
6. 您还可以启用电子邮件和 slack 通知以接收升级 NetScaler SDX 实例的执行报告。单击“通 过电子邮件接收执行报告 复选框和“通 过松弛接收执行报告 复选框以启用通知。

   有关配置电子邮件通讯组列表和 Slack 通道的详细信息，请参阅 NetScaler 实例的计划升级中的步骤 **8**

升级公告（预览版）

February 6, 2024

作为网络管理员，您可以在 NetScaler ADM 中管理许多在不同 ADC 版本上运行的 ADC 实例。监视每个 ADC 实例的生命周期可能是一项繁琐的任务。您必须访问 NetScaler 产品矩阵，确定即将或已经达到生命周期终止 (EOL) 或维护终止 (EOM) 的 ADC 实例。然后，计划他们的升级。

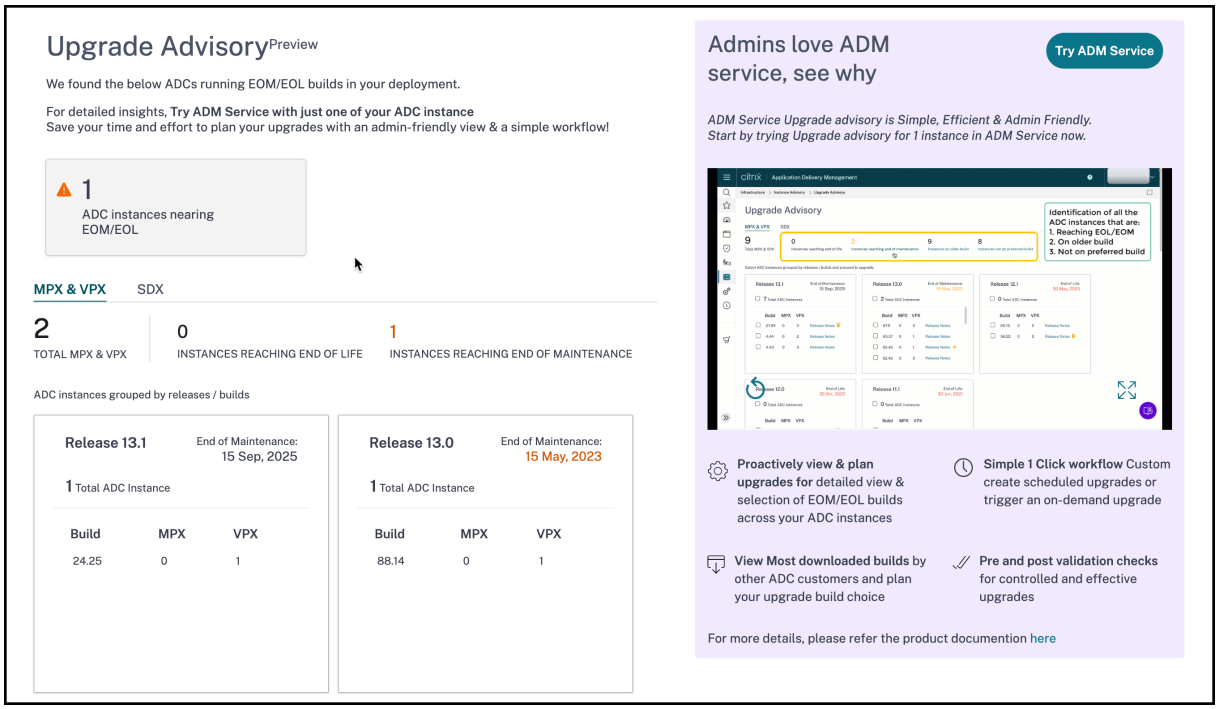
NetScaler ADM 本地升级建议对 ADC 执行版本扫描，并提供您的 ADC 实例上的 EOM/EOL 内部版本视图。

> 重要
>
> 有关详细见解和升级 ADC 实例的工作流程，请试用 **NetScaler ADM** 服务。

查看升级公告

导航到基础结构 **>** 实例公告 **>** 升级公告，然后查看以下信息：

- ADC 实例的总计数。
- 实例即将结束。
- 维护即将结束的实例。



升级公告页面按 ADC 实例的版本对其进行分组。

NetScaler ADM 本地升级公告还允许您选择其中一个 ADC 实例，然后将 ADC 实例加载到 ADM 服务。单击“试用 **ADM** 服务”，将 ADC 实例加载到 ADM 服务。ADM 服务升级公告为您提供了按所选 ADC 实例进行升级的工作流程。

有关 ADM 服务升级公告的详细信息，请查看升级公告页面上的 gif 动画。

安全公告（预览版）

February 6, 2024

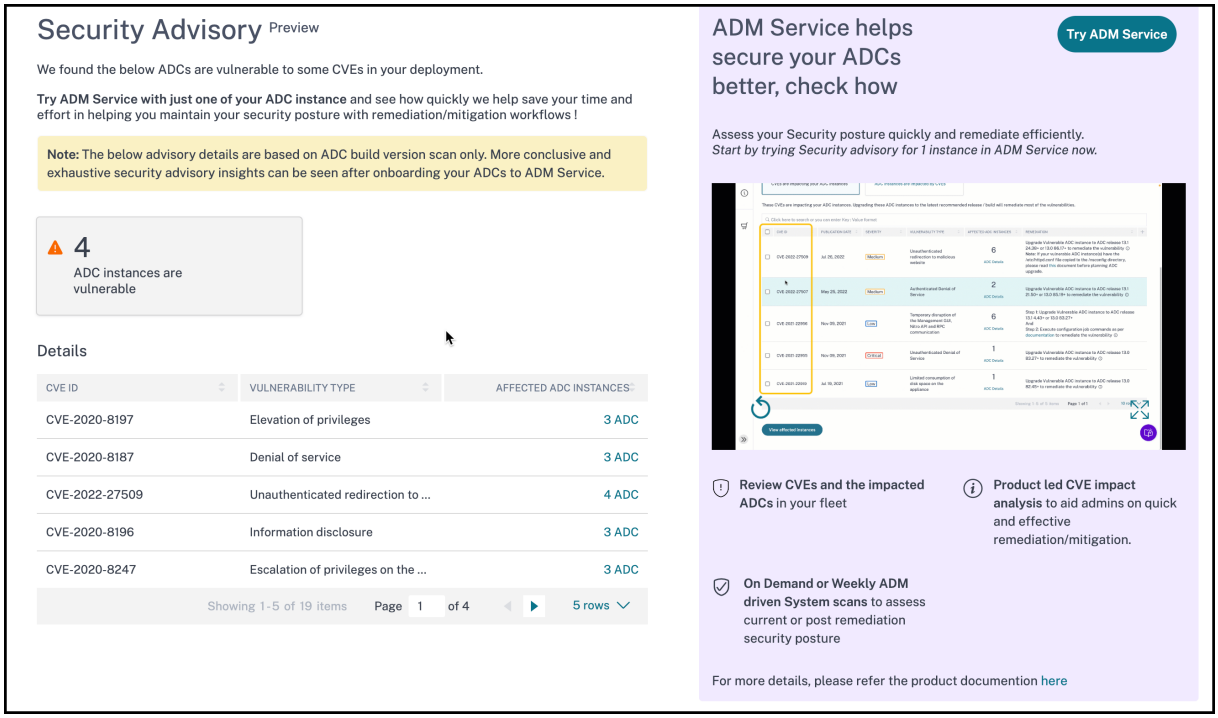
安全、可靠且具有弹性的基础设施是任何组织的生命线。组织必须跟踪新的常见漏洞和暴露 (CVE)，并评估 CVE 对其基础结构的影响。他们还必须了解并计划缓解和补救措施以解决漏洞。

NetScaler ADM 本地安全公告仅重点介绍存在风险的 NetScaler CVE 和 ADC 实例。

> 重要
>
> 要详细分析 CVE 影响、有关自定义扫描/系统扫描、修复和缓解工作流程的确凿信息，请试用 **NetScaler ADM** 服务。

查看安全公告

要访问安全公告，请导航到基础结构 **>** 实例公告 **>** 安全公告。您可以查看通过 NetScaler ADM 管理的所有 ADC 实例的漏洞状态。



NetScaler ADM 本地安全公告仅执行 ADC 版本扫描来检查 CVE，并显示以下信息。

- **CVE ID**：影响实例的 CVE 的 ID。

- 漏洞类型：此 CVE 的漏洞类型。
- 受影响的 **ADC** 实例：CVE ID 正在影响的实例数量。

NetScaler ADM 本地安全公告还允许您选择其中一个 ADC 实例，然后将 ADC 实例加载到 ADM 服务。单击“试用 **ADM** 服务”，将 ADC 实例加载到 ADM 服务。ADM 服务安全公告允许您检查特定 CVE 的漏洞类型，并获取有关缓解和补救措施的信息，以解决漏洞。

有关 ADM 服务安全公告的更多信息，请查看安全公告页面上的 gif 动画。

调配

February 6, 2024

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

NetScaler Application Delivery Management (ADM) 通过集成不同供应商的 SDN 控制器来支持企业网络中的 SDN。NetScaler ADM 同时支持 VMware NSX Manager 和 Cisco Application Policy Infrastructure Controller (APIC)。

VMware NSX Manager

NetScaler ADM 与 VMware 网络虚拟化平台集成，可自动部署、配置和管理 NetScaler 服务。此集成消除了与物理网络拓扑关联的传统复杂性，从而让 vSphere/vCenter 管理员能够以程序化方式更快地部署 NetScaler 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。

NetScaler ADM 的云调配功能支持将 NetScaler 产品与 VMware NSX 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 NetScaler 的高级功能（如 SSL 和 CS）以及基本负载平衡。
- 能够在服务删除过程中从特定 Edge 网关取消分配 VPX，并为另一个 Edge 网关重新分配同一 VPX。
- 能够从 vCenter 控制台快速部署 NetScaler 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使用模型，同时为云管理员提供单一控制点
- 更轻松地与 NetScaler ADM API 集成，这有助于支持意外的未来使用。

有关如何在 NetScaler ADM 上配置 VMware NSX Manager 的更多信息，请参阅 将 NetScaler 设备与 VMware NSX Manager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设施控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委托给 NetScaler ADM，后者在 APIC 中充当设备管理器。

混合模式设备包和 NetScaler ADM 支持 NetScaler 混合模式解决方案。需要在 APIC 中上载混合模式设备包。有关更多信息，请参阅在 Cisco ACI 的混合模式下使用 Citrix NetScaler M 进行 NetScaler ADM 自动化。

开放式堆栈：集成 **NetScaler** 实例

February 6, 2024

NetScaler Application Delivery Management (ADM) 的云调配功能支持将 NetScaler 产品与 OpenStack 平台集成。通过将此功能与 OpenStack 平台结合使用，OpenStack 用户可以使用 NetScaler 的负载平衡功能 (LBaaS)。此后，OpenStack 用户可以在 NetScaler 实例中从 OpenStack 部署其负载平衡器配置。

以下各节简要描述了 NetScaler ADM 和 OpenStack 集成工作流程中的功能。

NetScaler 驱动器用于开放式堆栈中子 **LBA**

OpenStack Neutron LBAS 插件包括 NetScaler 驱动程序，该驱动程序使 OpenStack 能够与 NetScaler ADM 进行通信。OpenStack 使用此驱动程序将通过 LBaaS API 完成的任何负载平衡配置转发到 NetScaler ADM，

NetScaler ADM 将在所需的 NetScaler 实例上创建负载平衡器配置。OpenStack 还使用该驱动程序定期调用 NetScaler ADM，以检索来自 NetScalers 的所有负载平衡配置的不同实体（例如 VIP 和池）的状态。适用于 OpenStack 平台的 NetScaler 驱动程序软件与 NetScaler ADM 捆绑在一起。要下载并安装驱动程序，必须首先安装 NetScaler ADM 并启动应用程序。

相互注册 **NetScaler ADM** 和 **OpenStack**

您必须首先在 NetScaler ADM 上注册 OpenStack 信息。指定 OpenStack 控制器 IP 地址和云管理用户凭据，以及 OpenStack NetScaler 驱动程序用户凭据。稍后您可以在 Neutron 配置文件 (neutron.conf) 的 NetScaler_driver 部分中指定相同的登录凭据，这样 OpenStack 中的 NetScaler 驱动程序就能够在 LB 配置期间连接到 NetScaler ADM。

在 OpenStack 和 NetScaler ADM 相互注册后，两者就可以相互通信。此外，OpenStack 用户可以使用他们在 OpenStack 中的现有凭据登录 NetScaler ADM 用户界面，查看他们的 LB 配置在 NetScalers 中的表现。

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

放置策略提供了对用户创建的每个负载平衡器配置中使用的 NetScaler 实例进行决定的灵活性。或者，NetScaler ADM 还提供了基于 OpenStack 租户分配 NetScaler 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 NetScaler 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

以下用例场景解释了 NetScaler 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 NetScaler 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 NetScaler 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。

Steve 必须向 NetScaler ADM 注册 OpenStack 的详细信息，然后在 OpenStack 网络组件 Neutron 中配置 NetScaler LBaaS 驱动程序。注册完成后，NetScaler ADM 会显示 OpenStack 中所有租户的详细信息。Steve 可以从列表中选择想要 NetScaler LBaaS 功能的 example-SportsOnline，然后配置 Tom 在 NetScaler ADM 中为他的负载平衡器配置分配专用 NetScaler。

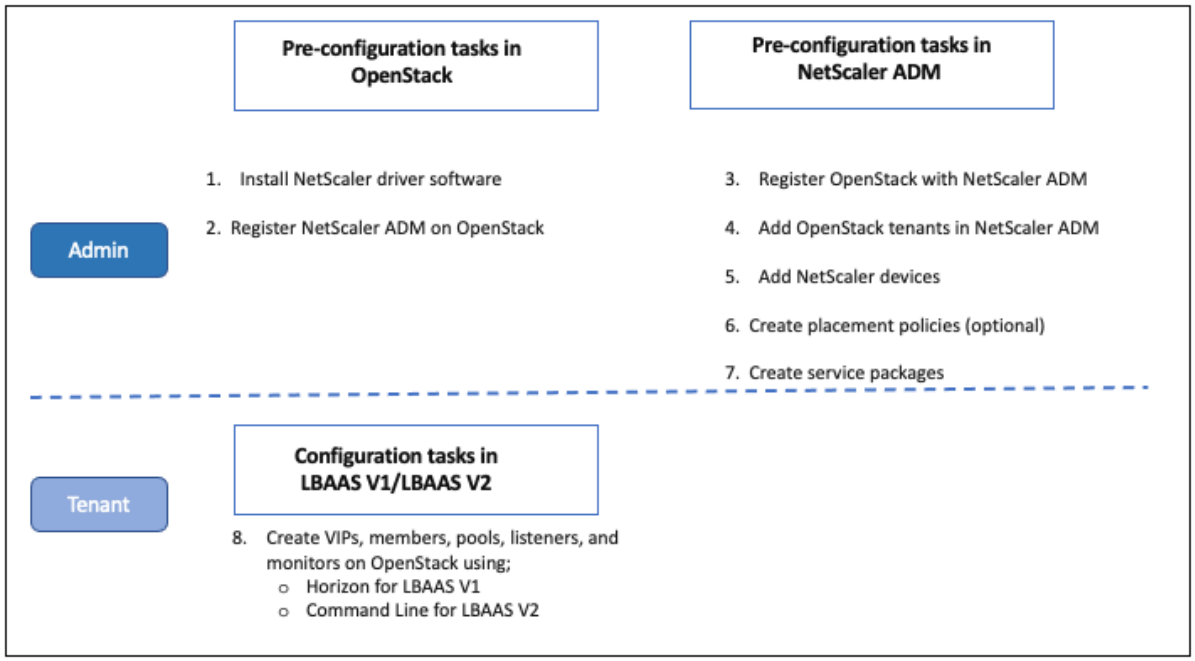
为此，Steve 可以使用 NetScaler ADM 用户界面在 OpenStack 的计算层 (Nova) 上预置 NetScaler VPX 实例，也可以让 MAS 在 Tom 在 OpenStack 中进行 LB 配置时按需自动配置 NetScaler VPX 实例。无论哪种情况，NetScaler ADM 都会管理 VPX 实例。为了实现这一目标，Steve 在 NetScaler ADM 中创建了一个服务包，并在服务包中定义了与 Tom 达成的服务包中的条件。例如，Steve 选择“专用”隔离策略来提供专用实例用于为 Tom 提供负载平衡器配置。即，Steve 在服务包中为 Tom 选择非共享实例。之后他为服务包分配许多 NetScaler VPX 实例，并与在服务包中要求专用 NetScaler 的其他租户一起关联 Example-SportsOnline。因此，当 Tom 执行他的第一个负载平衡器配置时，NetScaler ADM 将服务包中的一个 NetScaler VPX 实例分配给 Example-SportsOnline，并将他的配置部署到那个 NetScaler 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 部署为 NetScaler 实例上的服务组和虚拟服务器。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给在任何时间点都处于“UP”（运行）状态且可从 NetScaler 访问的那些服务器。

在 OpenStack 中创建的负载平衡配置现在实施在 NetScaler 实例上。完全配置后，NetScaler 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。

NetScaler ADM 与 **OpenStack** 工作流程集成

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。



NSX 管理器：手动 Provisioning NetScaler 实例

February 6, 2024

NetScaler Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动部署、配置和管理 NetScaler 服务。此集成消除了与物理网络拓扑关联的传统复杂性，从而让 vSphere/vCenter 管理员能够以程序化方式更快地部署 NetScaler 服务。

本文为您提供了必须在 VMware NSX Manager 和 NetScaler ADM 上执行的任务列表。

> 注意
>
> 确保已安装和配置适用于 vSphere 6.2 及更高版本的 VMware NSX，并且已经创建了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 NetScaler ADM。

有关在任何受支持的虚拟机管理程序上安装 NetScaler ADM build 13.1 的任务，请参阅 部署 NetScaler ADM。

VMware ESXi 硬件要求

下表列出了在 VMware ESXi 服务器上安装 NetScaler 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：
>
> 考虑到主机上没有其他虚拟机在运行，上面指定的内存和硬盘要求适用于在 VMware ESXi 服务器上部署 NetScaler ADM。对 VMware ESXi 服务器的硬件要求取决于在其中运行的虚拟机数。

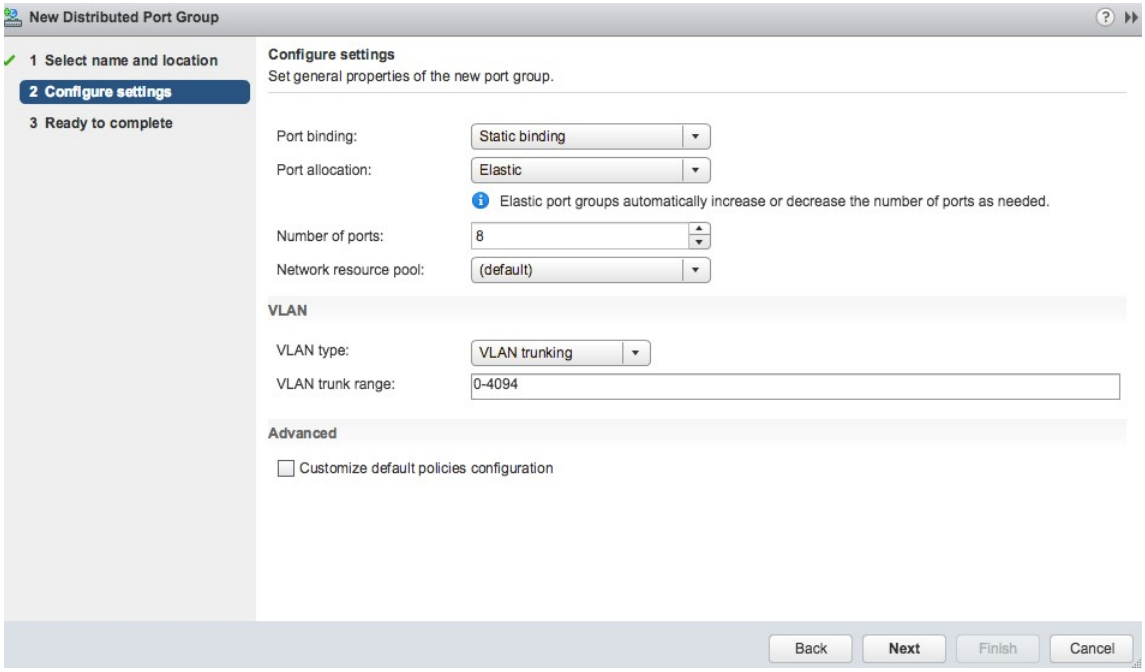
配置 VMware NSX

- 创建包含不同容量的 NetScaler VPX 实例的池，这些实例添加到不同的服务包。

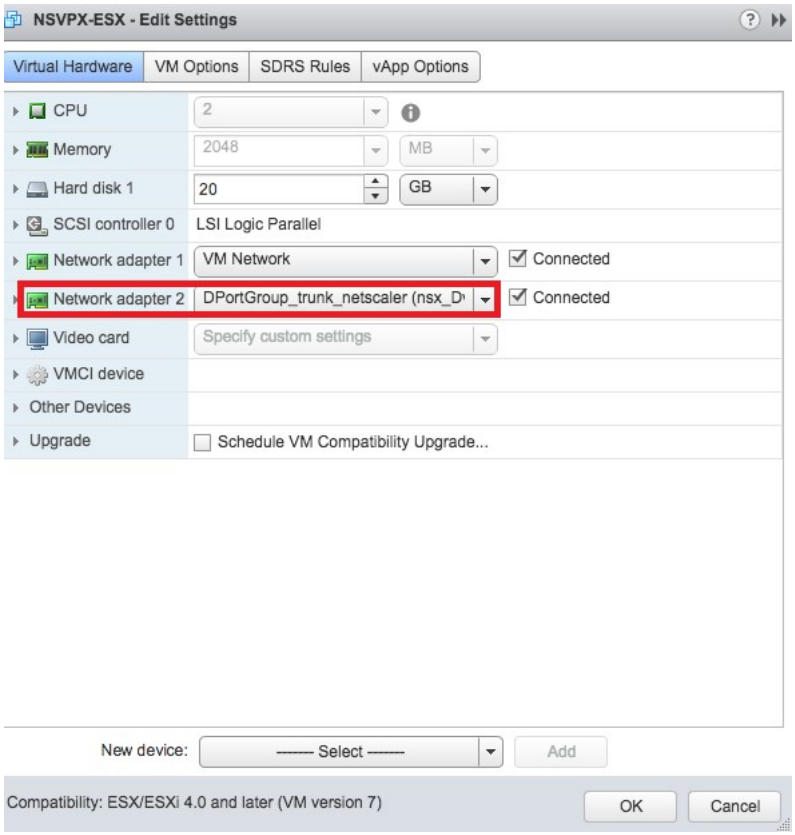
例如：

- 创建 VPX1000 (1 Gbps) 的五个 NetScaler VPX 实例。这些实例添加到金牌级服务包。
- 创建 VPX10 (10 Mbps) 的五个 NetScaler 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）。



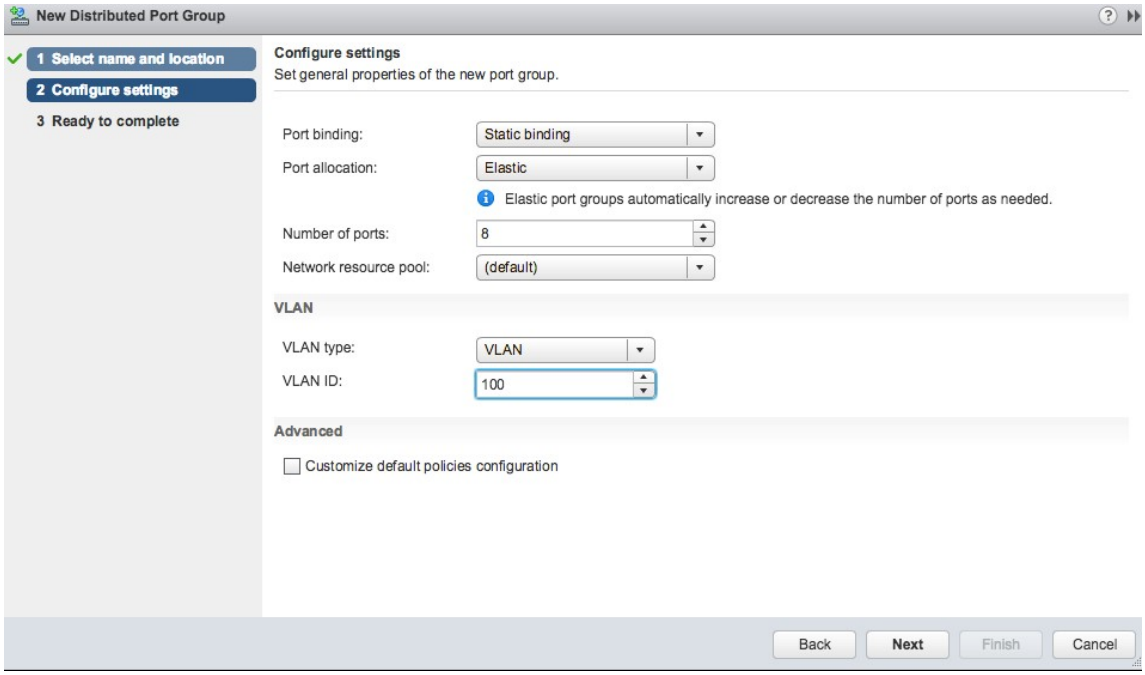
2. 为每个 NetScaler VPX 实例创建一个新接口，并将其连接到上面创建的 VLAN 范围中继端口组。



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

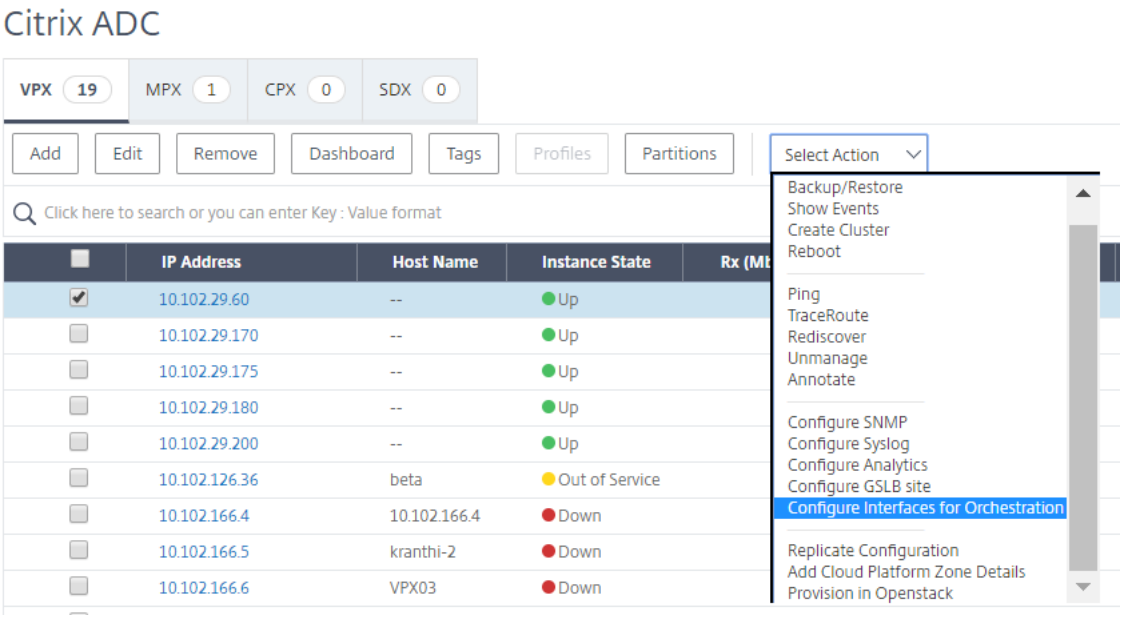
口组），即虚拟 LAN 101 一个端口组，虚拟 LAN 102 另一个端口组，依次类推，直至虚拟 LAN 105。



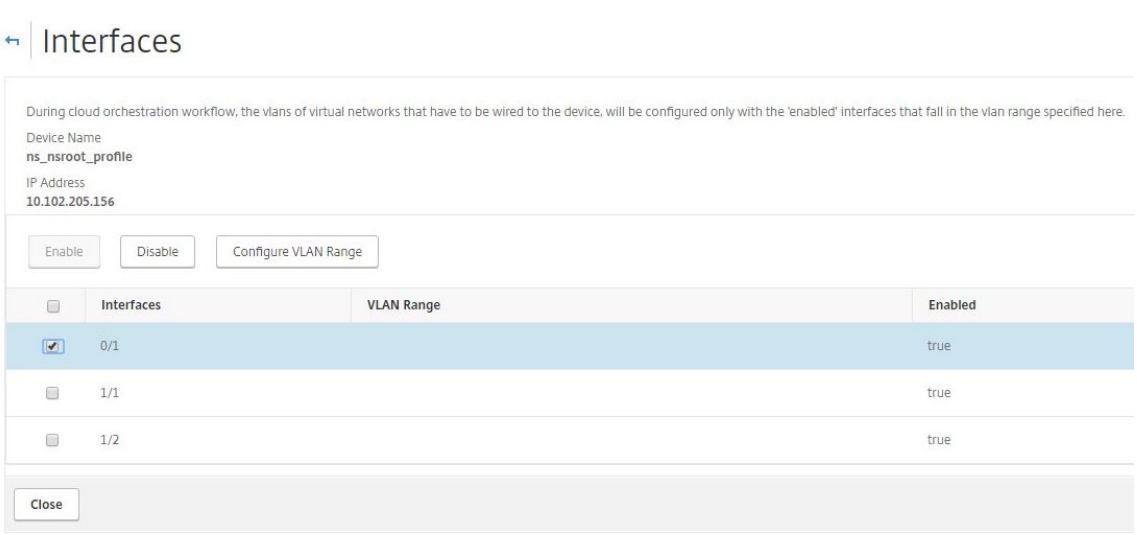
在 **NetScaler ADM** 中添加 **NetScaler VPX** 实例

在 NetScaler ADM 中添加 NetScaler VPX 实例，并为每台设备指定中继组的 VLAN 范围。

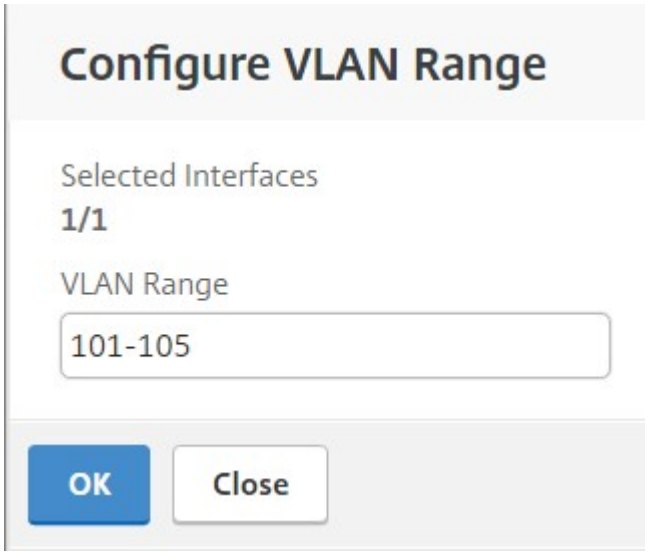
1. 在 NetScaler ADM 中，导航到基础架构 > 实例 > **NetScaler VPX**，然后单击添加。
2. 在添加 **NetScaler VPX** 页面上，指定实例的主机名、每个实例的 IP 地址或 IP 地址范围，然后从配置文件名称列表中选择一个实例配置文件。还可以单击 + 图标创建新实例配置文件。
3. 单击确定。
4. 从 NetScaler VPX 页面的列表中选择新添加的 **NetScaler VPX** 实例，然后单击“操作”字段中的向下箭头按钮。选择 **Configure Interfaces for Orchestration**（为调配配置接口）。



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。



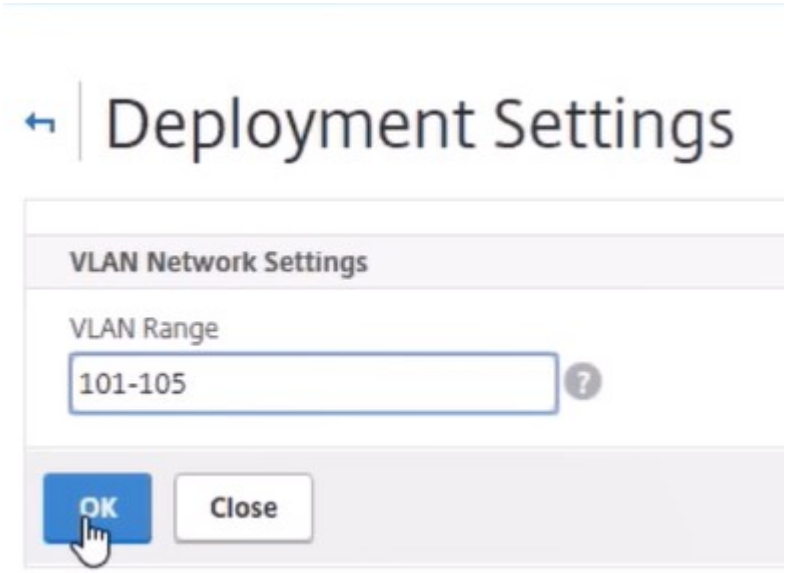
6. 在“接口”页面上，选择所需的接口，然后单击“配置 **VLAN** 范围”。
7. 输入 NSX Manager 中配置的 VLAN 范围，单 击确定，然后单击 关闭。



在 **NetScaler ADM** 中注册 **VMware NSX** 管理器

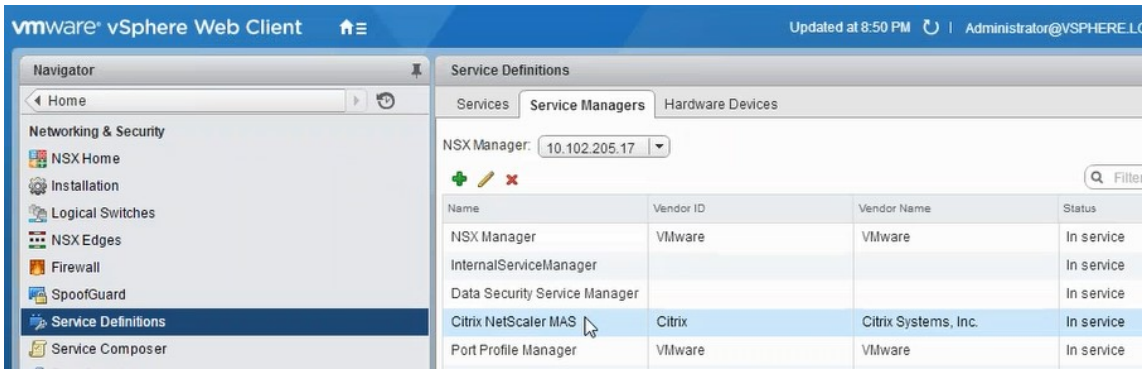
在 NetScaler ADM 中注册 VMware NSX 管理器，在它们之间创建通信渠道。

1. 在 NetScaler ADM 中，从下拉列表中导航到调配 > **SDN** 调配 > **VMware NSX Manager**，然后单击配置 **NSX Manager** 设置。
2. 在 配置 **NSX Manager** 设置 页面上，设置以下参数：
   a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
   b) NSX Manager 用户名-NSX Manager 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 **NetScaler ADM** 帐户部分中，为 **NSX Manager** 设置 NetScaler 驱动程序用户名和密码。NetScaler ADM 使用这些登录凭据对来自 NSX 管理器的负载平衡器配置请求进行身份验证。
4. 单击确定。
5. 导航到“调配”>“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 NetScaler ADM 视为服务管理器之一。这表示注册成功，并在 NSX 管理器和 NetScaler ADM 之间建立了通信通道。



在 **NetScaler ADM** 中创建服务包

1. 在 NetScaler ADM 中，导航到 **Orchestrat** ion >**SDN Orchestrat**ion >**VMware NSX Manager**> 服务包，然后单击 添加以添加 新的服务包。
2. 在“服务包”页面的“基本设置”部分中，设置以下参数：

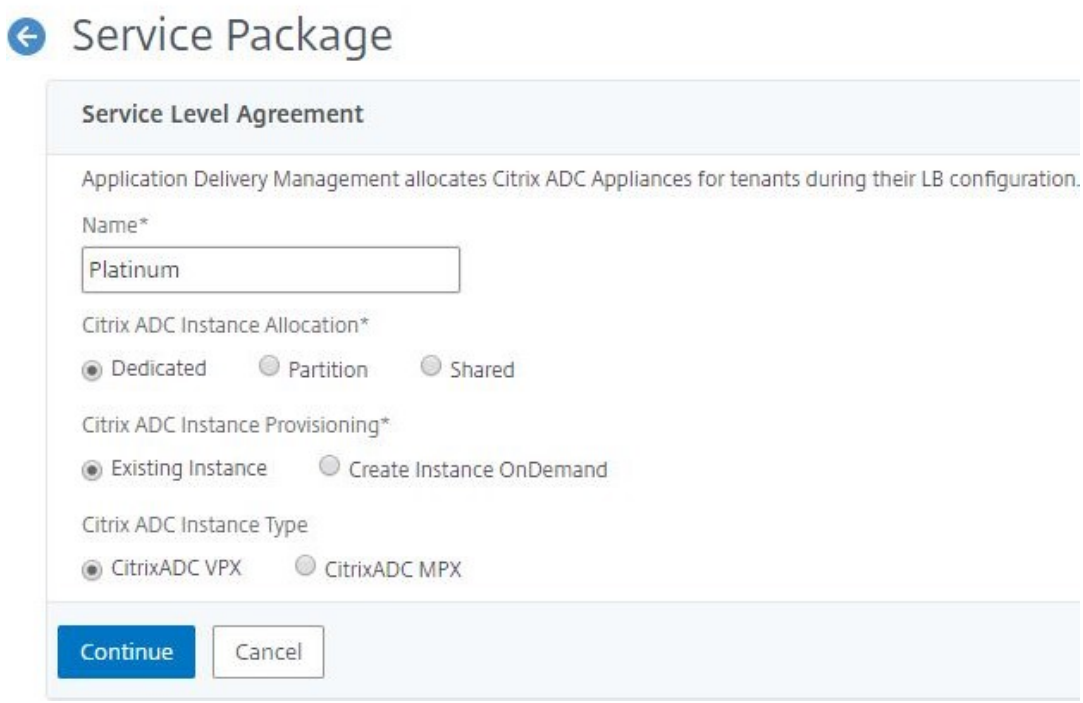
   a) Name（名称）- 键入服务包的名称

   b) Isolation Policy（隔离策略）- 默认情况下，隔离策略设置为“Dedicated”（专用）

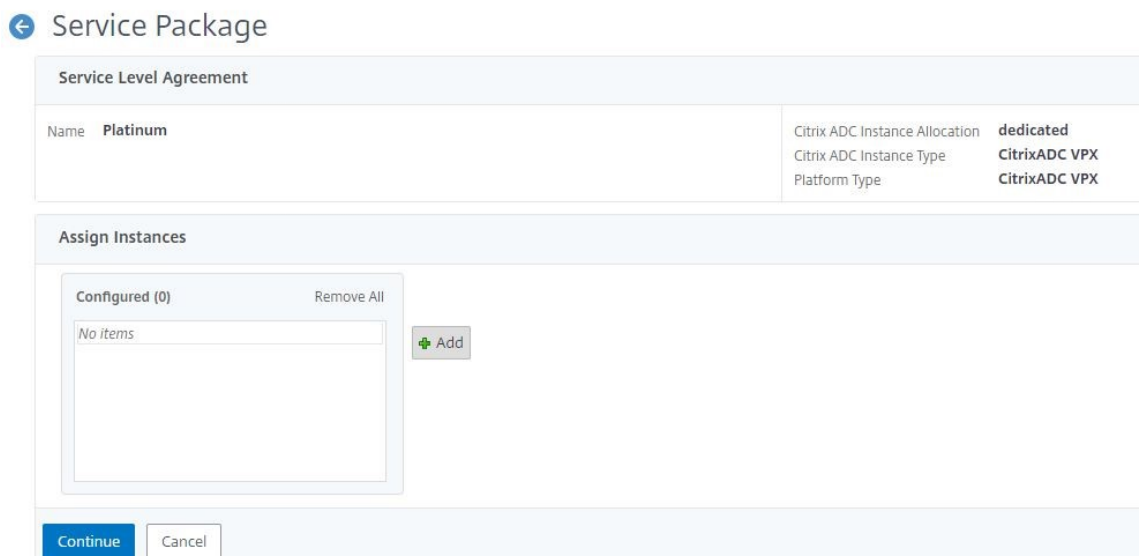
   c) Device Type（设备类型）- 默认情况下，设备类型设置为 NetScaler VPX

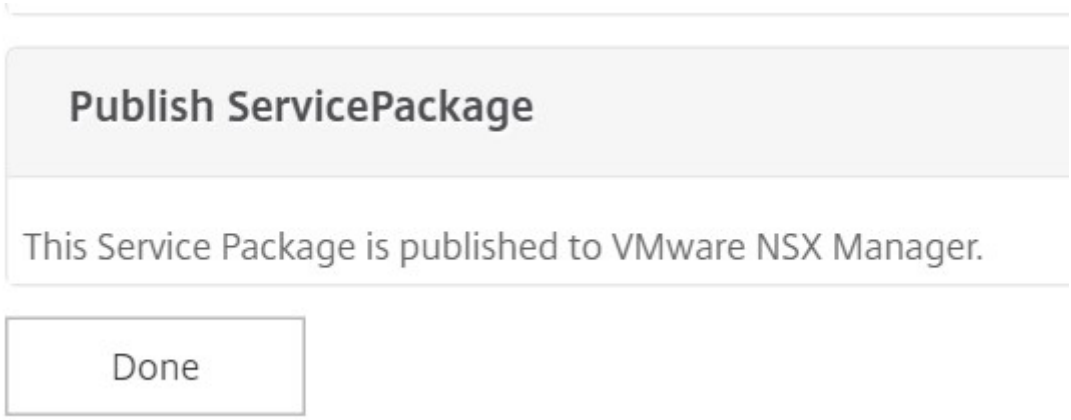
> 注意
>
> 这些值在此版本中是默认设置的，您无法对其进行修改。

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。一项服务可以添加多个设备，多个边缘可以使用相同的服务包将 NetScaler VPX 实例卸载到 NetScaler ADM。

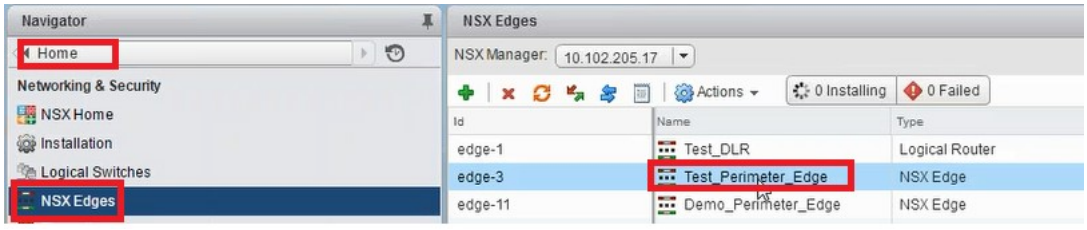
5. 登录 vSphere Web Client 上的 NSX Manager，然后导航到服务定义 > 服务。

   您可以看到 NetScaler ADM 服务包已注册。

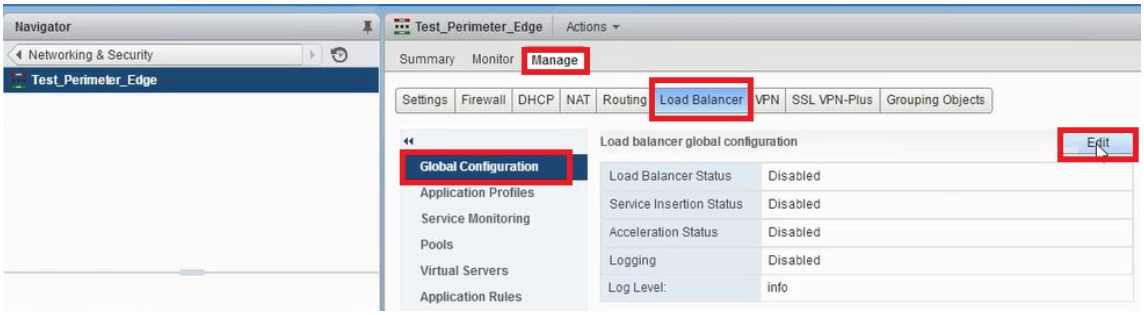
为边界执行负载平衡器服务插入

对之前创建的 NSX Edge 网关执行负载平衡器服务插入（将负载平衡功能从 NSX LB 卸载到 NetScaler）。

1. 在 NSX Manager 中，导航到“主页”>“**NSX** 边缘”，然后选择已配置的边缘 Gateway。

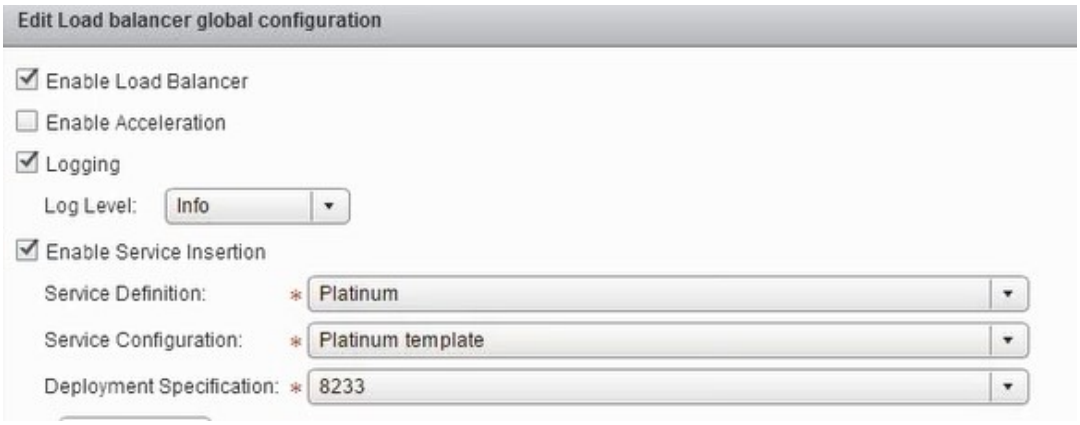


2. 单击 管理，然后在 负载平衡器 选项卡上，选择 全局配置，然后单击 编辑。

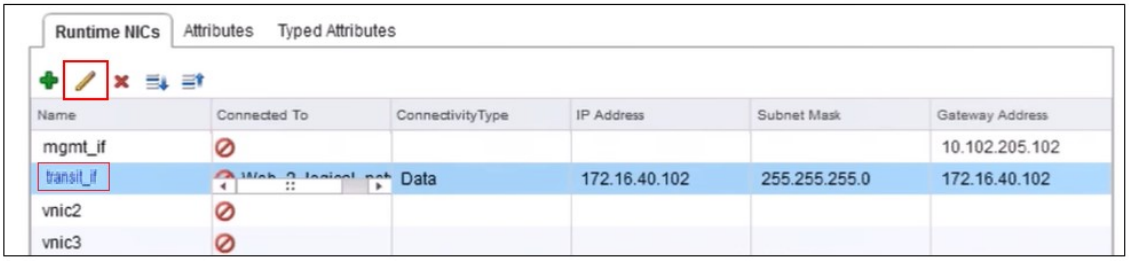


3. 选择 启用负载平衡器、日志记录、启用服务插入 以启用它们。

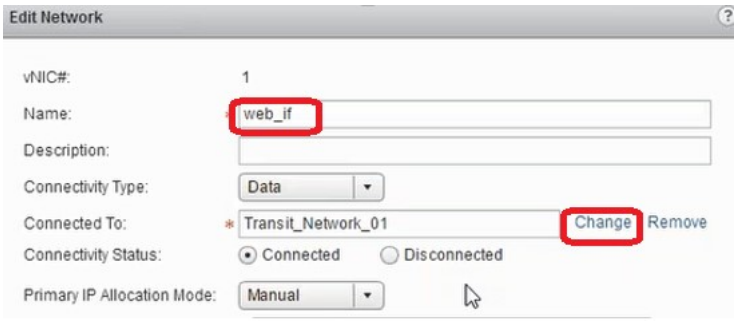
   a) 在 服务定义中，选择在 NetScaler ADM 中创建并发布到 NSX 管理器的服务包。



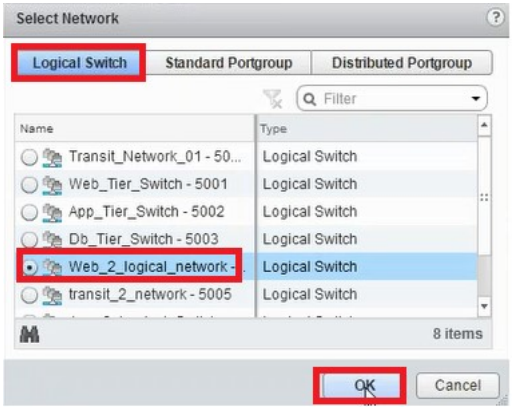
4. 选择现有的运行时网卡，然后单击“编辑”图标以编辑在分配 NetScaler VPX 时必须连接的运行时 NIC。



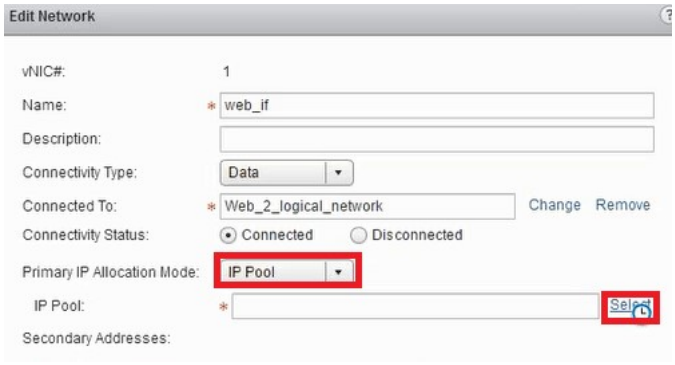
5. 编辑 NIC 的名称，将连接类型指定为 数据，然后单击 更改。



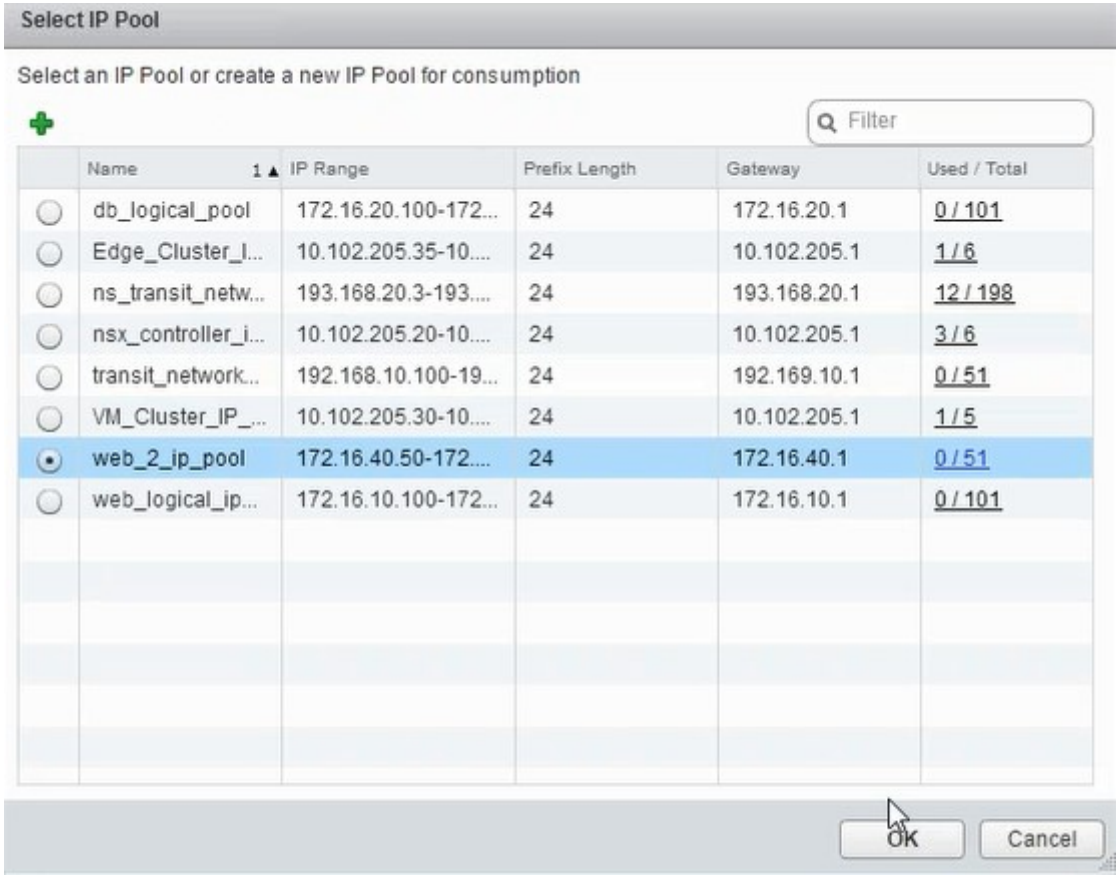
6. 选择适当的 Web 逻辑交换机。



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。



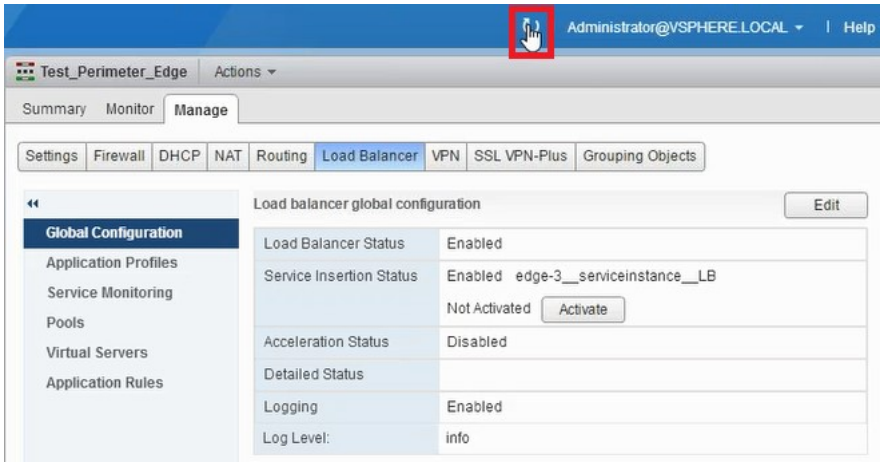
8. 在“选 择 **IP** 池”窗口中，选择相应的 IP 池，然后单击“确定”。

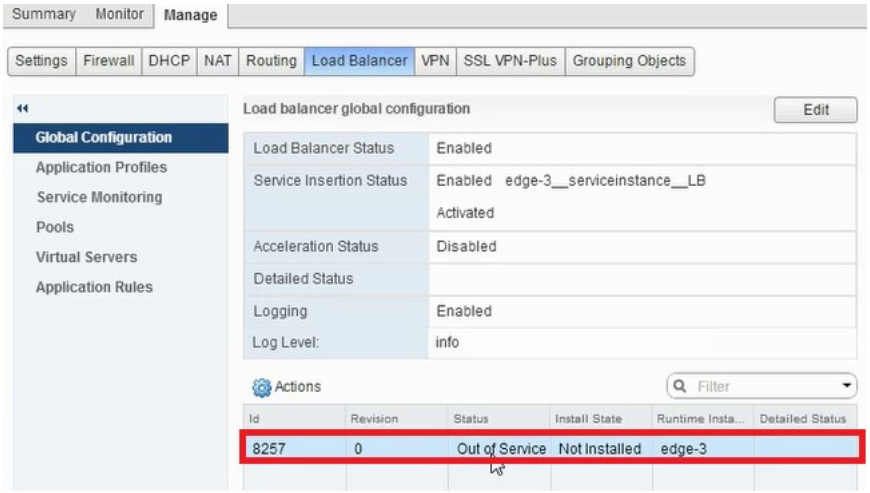


在 NetScaler VPX 装置中获取 IP 地址并将其设置为源净 IP 地址。在 NSX Manager 中创建一个 L2 网关以将 VXLAN 映射到虚拟 LAN。

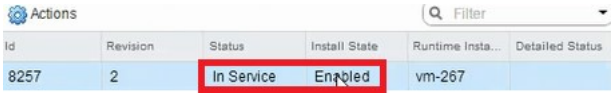
> 注意：
>
> 所有数据接口都作为运行时 NIC 连接，它们是 DLR 接口的一部分。

9. 刷新视图以查看运行时间的创建。





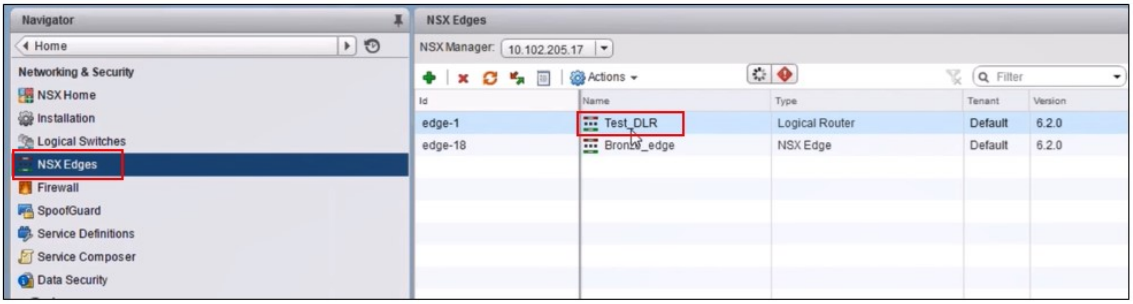
10. VM 启动后，“状态”的值将更改为“正 在服务”，“安装状态”的值更改为“已启用”。



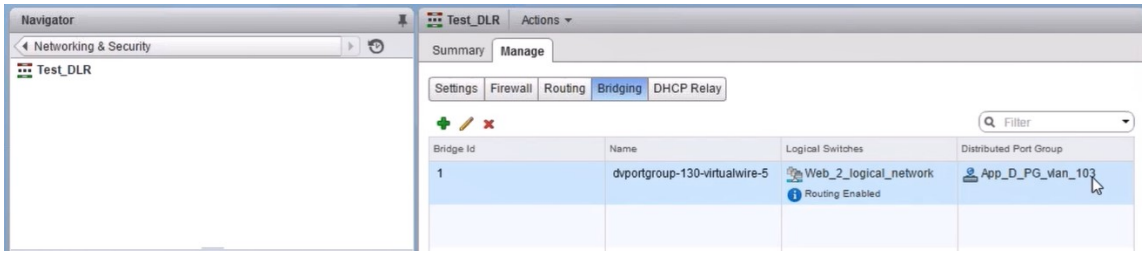
> 注意：
>
> 在 NetScaler ADM 中，导航到“业务 流程”>“请求”以查看 LB 服务插入完成的进度详细信息。

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。



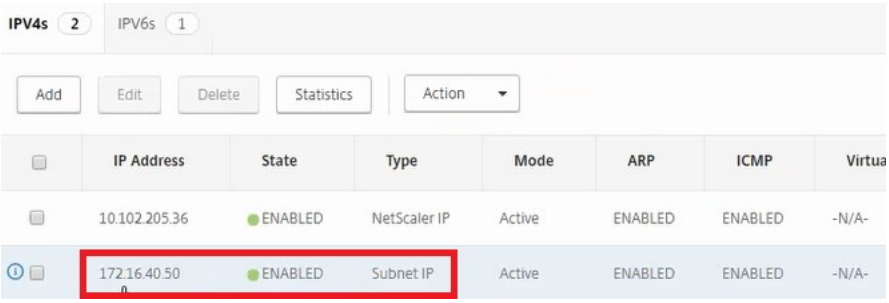
> 注意为每个数据接口创建
>
> 一个 L2 Gateway。

查看分配的 **NetScaler**

1. 使用 NetScaler ADM 中显示的 IP 地址登录 NetScaler 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 **NetScaler VPX** 实例

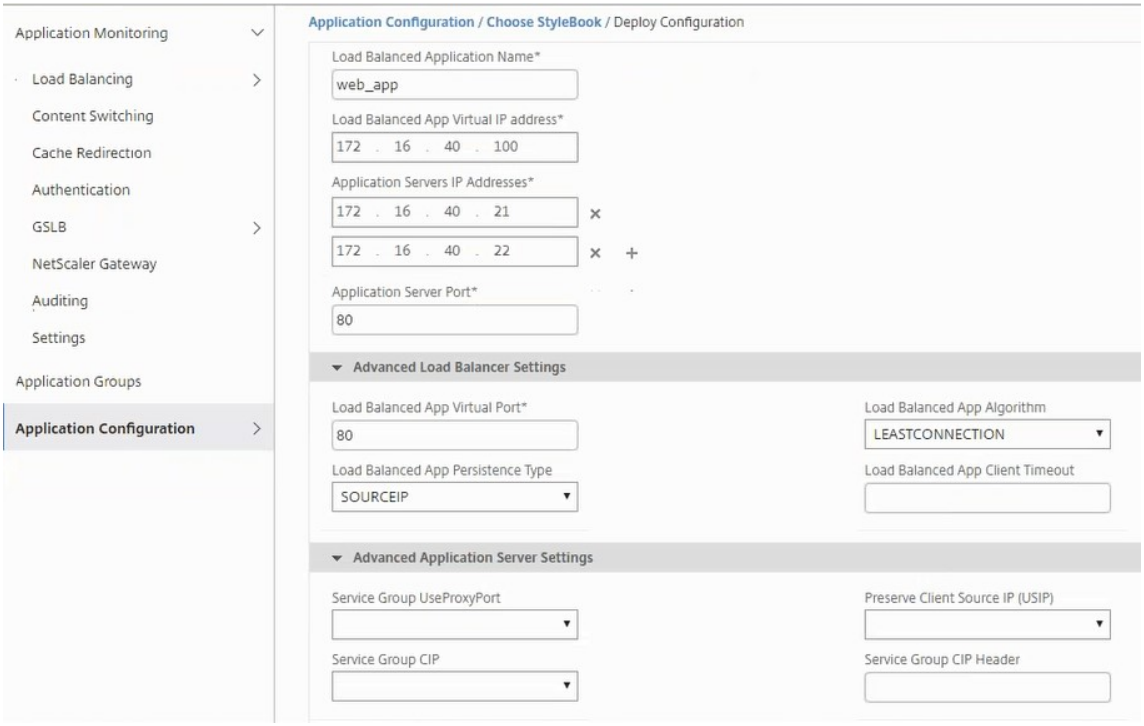
1. 在 NetScaler ADM 中，导航到“调配”>“**SDN** 调配”>“配置 **NSX** 管理器”>“边缘网关”。

   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 NetScaler 实例 IP。

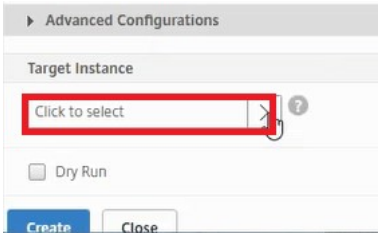
2. 创建一本新的样书。导航到 应用程序 > 配置，导入样书，然后从列表中选择样书。

   要创建新样书，请参阅 创建您自己的样书。

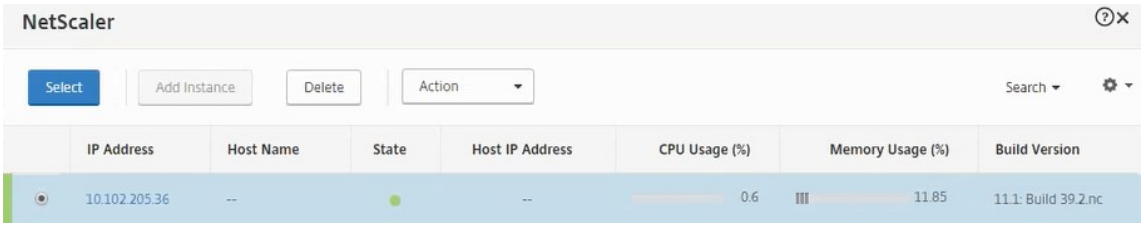
3. 为所有所需参数指定值。



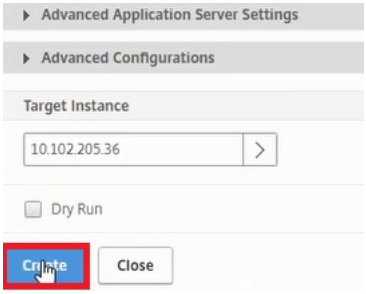
4. 指定要在其上运行这些配置设置的 NetScaler VPX 实例。



5. 选择前面说明的 IP 实例，然后单击“选择”。

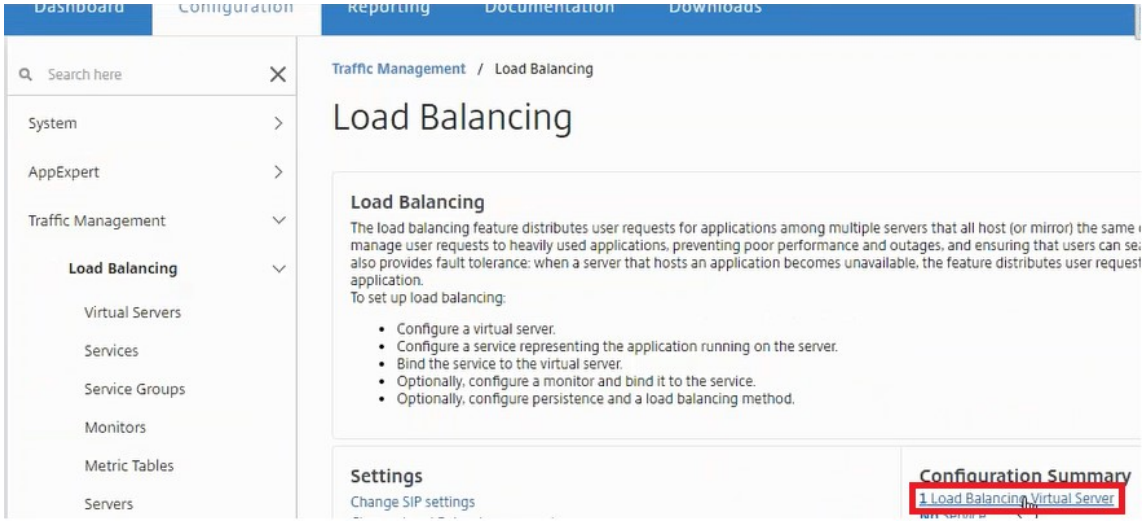


6. 单击 创建 可在选定的设备上应用配置。

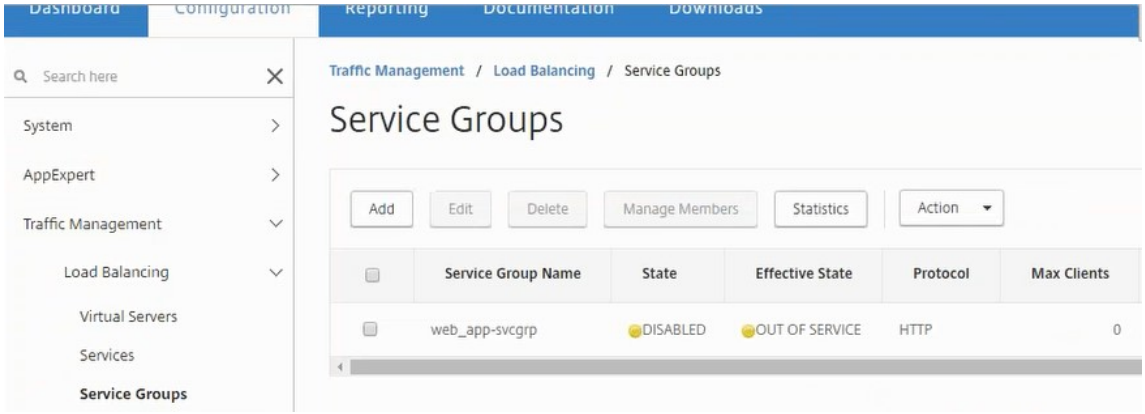


查看负载平衡器配置

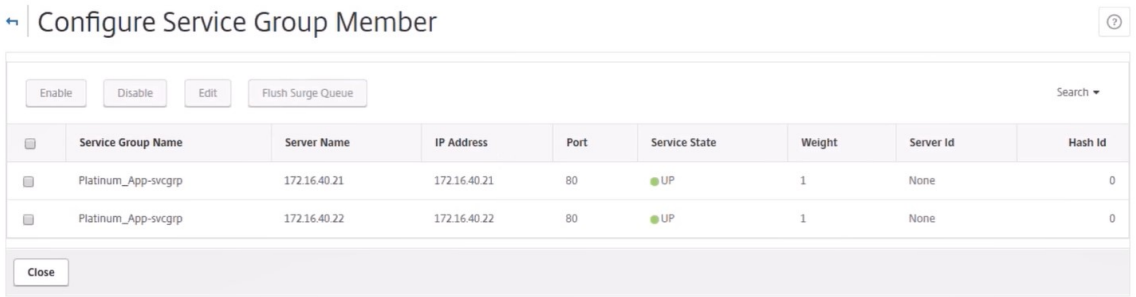
1. 登录到 NetScaler VPX 实例，导航到“配置”>“流量管理”>“负载平衡”以查看创建的负载平衡虚拟服务器。



还可以查看创建的服务组。



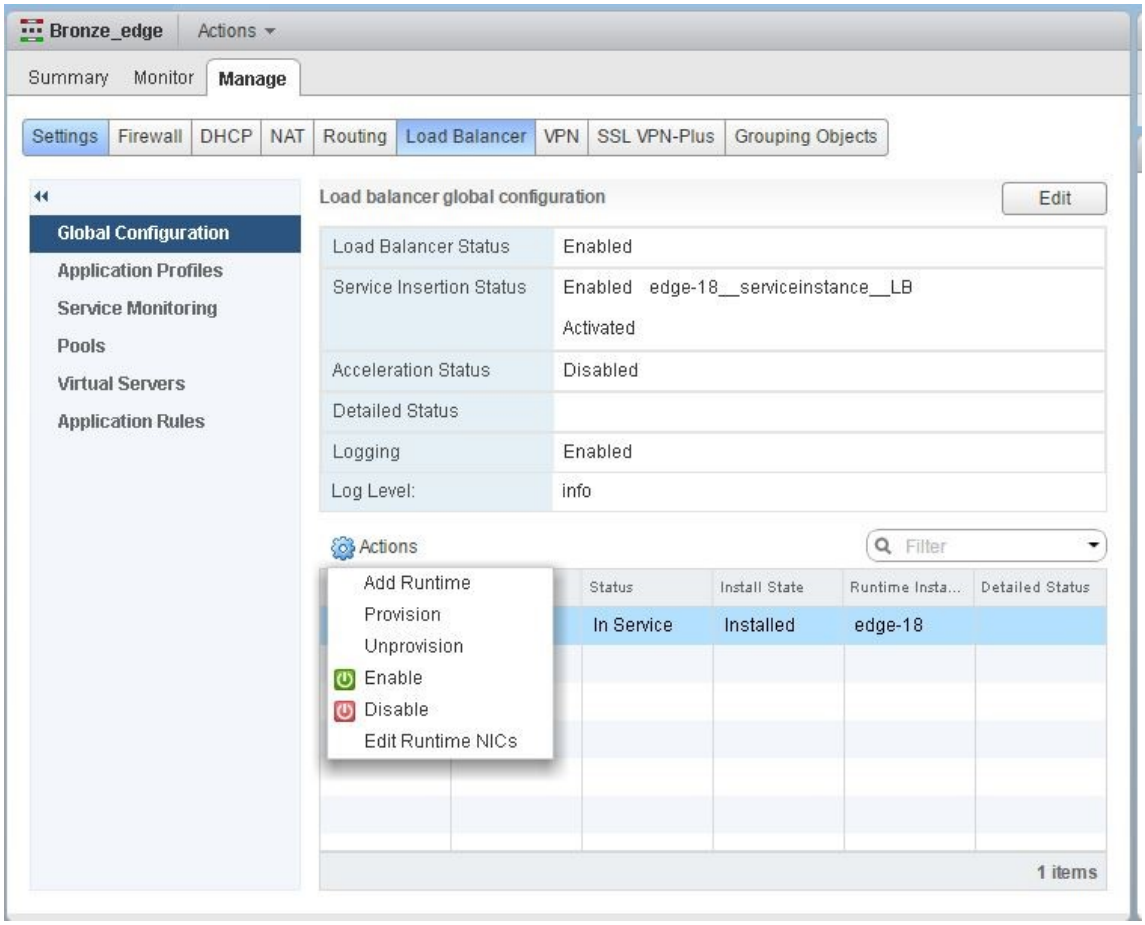
2. 选择服务组，然后单击 管理成员。**Configure Service Group Member**（配置服务组成员）页面显示与服务组关联的成员。



删除负载平衡器服务

1. 在 NetScaler ADM 中，导航到 应用程序 > 配置，然后单击 **X** 图标删除应用程序配置。
2. 在 vSphere Web Client 上登录 NSX Manager，然后导航到 NetScaler VPX 实例所连接的边缘网关。
3. 导航到“管 理”>“负载平衡器”>“全局配置”，右键单击运行时条目，然后单击“取消置备”。

   > 注意：
   >
   > NetScaler ADM 中的 Edge 网关对应于 NSX Manager 中的运行时条目。



   NetScaler VPX 实例已停止服务。

4. 在 NetScaler ADM 中，导航到“调配”>“**SDN** 调配”>“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 NetScaler** 实例

February 6, 2024

概述

NetScaler Application Delivery Management (ADM) 与 VMware 网络虚拟化平台集成，可自动部署、配置和管理 NetScaler 服务。此集成消除了与物理网络拓扑关联的传统复杂性，从而让 vSphere/vCenter 管理员能够以程序化方式更快地部署 NetScaler 服务。

在 VMware NSX Manager 上插入和删除负载平衡服务期间，NetScaler ADM 会动态配置和销毁 NetScaler 实例。这种动态配置要求在 NetScaler ADM 中自动分配 NetScaler VPX 许可证。当 NetScaler 许可证上载到 NetScaler ADM 时，NetScaler ADM 将扮演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。

- NetScaler ADM，版本 13.0 设置为高可用性并安装在 ESX 上。
- NetScaler VPX，版本 13.0
- 适用于 NetScaler VPX 实例 13.0 版的 NetScaler VPX 许可证
- 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）。

NetScaler ADM 和 **NetScaler** 实例的高可用性部署

要配置 NetScaler ADM HA 设置，请安装从 NetScaler 网站下载的 NetScaler ADM 映像文件。有关如何配置 NetScaler ADM HA 设置的详细信息，请参阅 在高可用性中部署 NetScaler ADM。

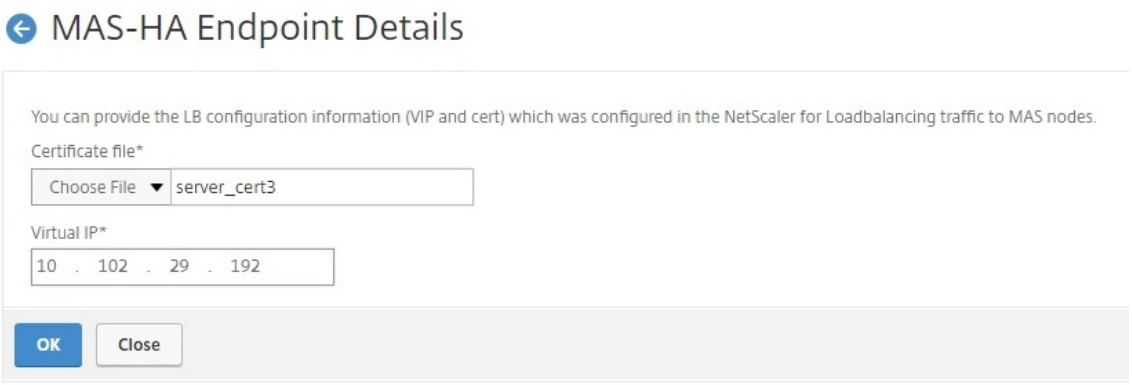
设置 **NetScaler ADM HA** 端点详细信息

要将 VMware NSX 管理器与在 HA 模式下部署的 NetScaler ADM 集成，必须先输入负载平衡 NetScaler 实例的虚拟 IP 地址。您还必须将 NetScaler 负载平衡虚拟服务器上存在的证书文件上载到 NetScaler ADM 文件系统。

要在 **NetScaler ADM** 中提供负载平衡配置信息，请执行以下操作：

1. 在 NetScaler 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 NetScaler 实例上已存在的相同证书。
4. 输入负载平衡 NetScaler 实例的虚拟 IP 地址，然后单 击确定。



在 **NetScaler ADM** 中注册 **VMware NSX** 管理器

当您将两个 NetScaler ADM 服务器设置为高可用性时，这两个服务器节点处于主动-被动模式。登录 NetScaler ADM 服务器主节点，在 HA 中向 NetScaler ADM 注册 VMware NSX manager，在它们之间创建通信信道。

要在 **HA** 中向 **NetScaler ADM** 注册 **VMware NSX** 管理器，请执行以下操作：

1. 在主 NetScaler ADM 服务器节点中，导航到调配 > **SDN** 调配 > **VMware NSX Manager**。
2. 单击“配置 **NSX** 管理器设置”。
3. 在 配置 **NSX Manager** 设置 页面上，设置以下参数：
   a) NSX Manager IP Address（NSX Manager IP 地址）- NSX Manager 的 IP 地址。
   b) NSX Manager 用户名-NSX Manager 的管理用户名。
   c) Password（密码）- NSX Manager 的管理用户的密码。
4. 在 NSX Manager 使用的 NetScaler ADM 帐户部分中，设置 NSX Manager 的 NetScaler 驱动程序密码。
5. 单击确定。

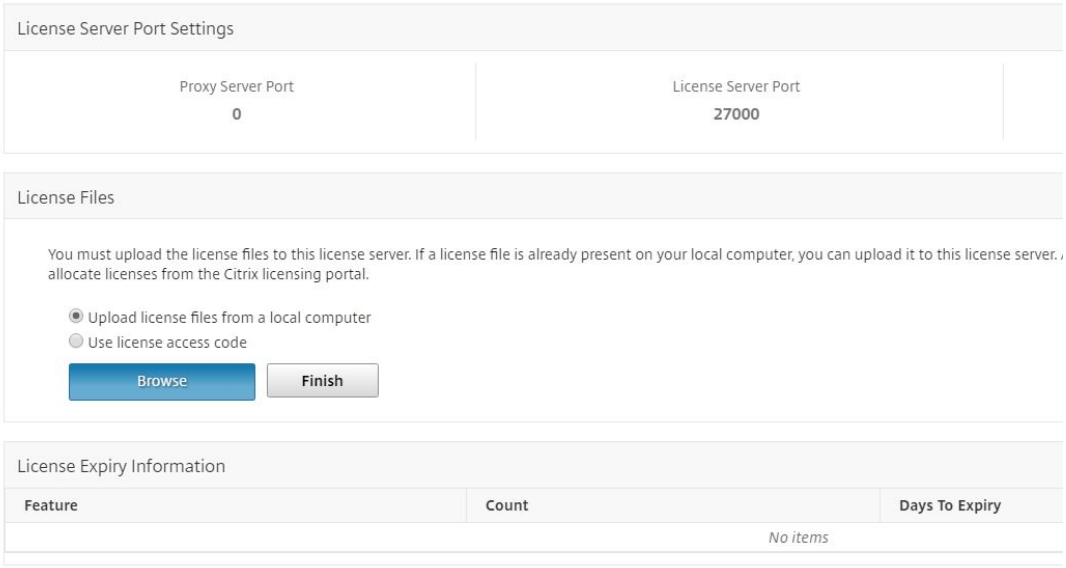
在 **NetScaler ADM** 中上载许可证

将 NetScaler VPX 许可证上载到 NetScaler ADM，以便 NetScaler ADM 可以在与 NSX 进行调配期间自动向实例分配许可证。

要在 **NetScaler ADM** 上安装许可证文件，请执行以下操作：

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 池许可。
2. 在“许可证文件”部分，选择以下选项之一：
   a) 从本地计算机上载许可证文件-如果您的本地计算机 上已经存在许可证文件，则可以将其上载到 NetScaler 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”。
   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 NetScaler ADM 添加更多许可证。



在 **NetScaler ADM** 中上载 **NetScaler VPX** 映像

将 NetScaler 映像添加到 NetScaler ADM 中，以便 NetScaler ADM 使用服务包中定义的这些映像。

要在 **NetScaler ADM** 中上载 **NetScaler VPX** 图像，请执行以下操作：

1. 在 NetScaler ADM 中，导航到“调配”>“**SDN** 调配”>“**VMware NSX** 管理器”>“**ESX NSVPX** 映像”。
2. 单击“上载”，然后从本地存储文件夹中选择 NetScaler VPX zip 包。

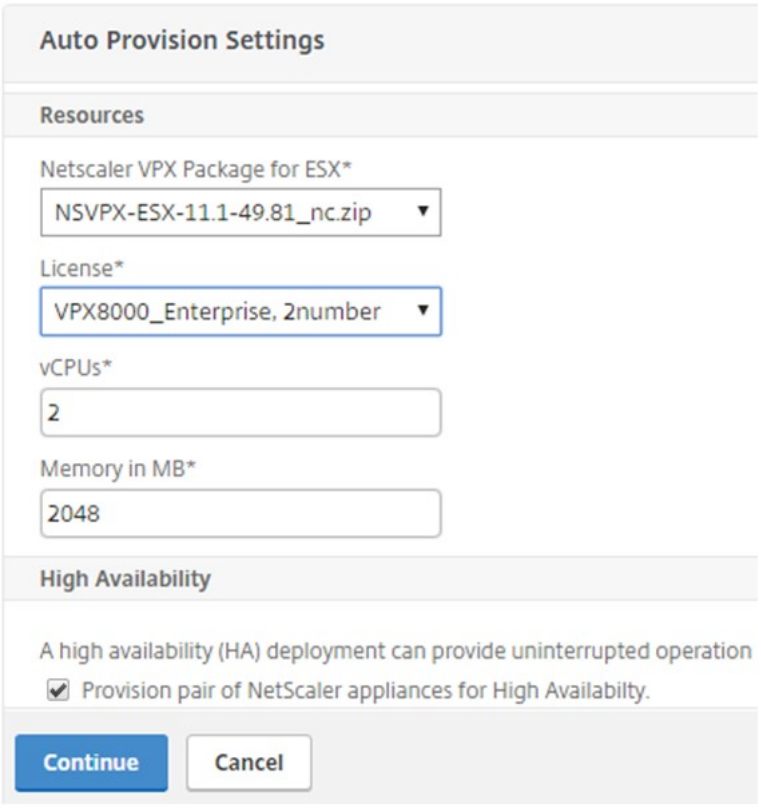
在 **NetScaler ADM** 中创建服务包

在 NetScaler ADM 中创建服务包以定义 SLA 集，该集指示如何分配 NetScaler 资源。

要在 **NetScaler ADM** 中创建服务包，请执行以下操作：

1. 在 NetScaler ADM 中，导航到调配 > **SDN** 调配 > **VMware NSX Manager** > 服务包，然后单击添加以添加新的服务包。
2. 在“服务包”页面的“基本设置”部分中，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) NetScaler 实例 Provisioning-选择按需 创建实例
   d) 自动配置平台——选择 **CitrixNetScaler SDX**
   e) 单击继续
3. 在“自动配置设置”部分中，选择最近上载的 **NetScaler VPX** 压缩包以将其部署在 **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 NetScaler 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 NetScaler VPX 实例
> - 8000 - 可占用的带宽为 8 GB
> - 高级-NetScaler 提供三种类型的许可证-标准、高级和高级
> - 2 个数字-使用此许可证可以部署两个 NetScaler 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. 该服务包已发布到 NSX Manager。在 NSX Manager 中，导航到“服务定义”>“服务管理器”。您可以将 NetScaler ADM 视为服务管理器之一。这表示注册成功并且 NSX 管理器与 NetScaler ADM 之间建立了双向通信。

> 注意
>
> 对于高可用性部署中的 NetScaler ADM，许可证仅在 NetScaler ADM 许可证服务器节点上载。NetScaler 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 负载平衡器卸载到 NetScaler。

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 E**dges，然后双击选择已配置的 Edge 网关。
2. 单击 管理，然后在 负载平衡器 选项卡上，选择 全局配置，然后单击 编辑。
3. 选择“启用负载平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。NetScaler ADM 不支持手动或 DHCP 分配 IP 地址。

6. 单击“刷新”图标查看运行时的创建情况。

> 注意
>
> 由于您要在 HA 部署中部署两个 NetScaler VPX 实例，因此在 NSX 管理器中创建了两个运行时。

> 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. 当两台虚拟机启动时，状态的值更改为“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变化。

9. 在 NetScaler ADM 中，导航到调配 > 请求以查看服务插入完成的进度详细信息。您可以看到，创建和更新运行时间的请求已发送到 NetScaler ADM。更新运行时间后，选择请求并单击“任务”按钮，查看 NetScaler ADM 是否已添加到 NSX Manager 中。

   对于 HA，将有两个请求在 NetScaler ADM 中创建和更新两个运行时间。两个运行时间均已更新后，选择两个请求并单击“任务”按钮，查看是否已在 NSX Manager 中添加了两个 NetScaler ADM HA 节点。

10. 在 NetScaler ADM 中，导航到调配 > **SDN** 调配 > **VMware NSX Manager** > **Edge** 网关。在右侧面板中，可以看到 NetScaler VPX 已添加到 NSX Edge 网关。

    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 NetScaler VPX 实例。

11. 在 NetScaler ADM 中，导航到 基础架构 **>** 池许可 **> VPX** 许可证。选择 NetScaler VPX 许可证和您已安装的版本。

    处于 HA 模式的 NetScaler 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 NetScaler 实例：

- 使用 VMware NSX Manager GUI 在 NetScaler VPX 上配置负载平衡服务
- 在 NetScaler ADM GUI 中在 NetScaler VPX 上配置负载平衡服务

使用 **VMware NSX Manager GUI** 在 **NetScaler 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 E**dges，然后双击选择已配置的 Edge 网关。

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“负载平衡器”选项卡上选择“池”，然后单击“**+**”图标添加新池，然后设置以下参数：
   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“负载平衡器”选项卡上，选择“虚拟服务器”，然后单击“**+**”图标添加虚拟服务器，然后设置以下参数：

   a) 应用程序配置文件-默认情况下，将显示您在 NetScaler ADM 中创建的服务配置文件。

   b) Name（名称）- 虚拟服务器的名称。

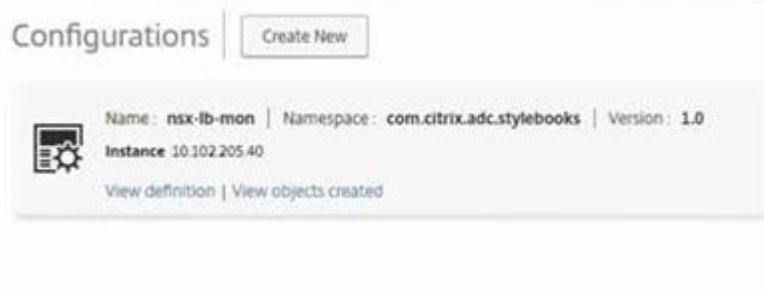
   c) IP Address（IP 地址）- 单击“Select”（选择）以选择现有的 IP 地址池或创建新的 IP 地址池。

   d) Default pool（默认池）- 从下拉列表中选择默认池。

2. 单击确定。

3. 在 NetScaler ADM 中，导航到“业务 流 程”>“请求”，以查看在一个或多个选定 NetScaler 实例上完成服务创建的进度详细信息。

4. 在 NetScaler 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 **NetScaler ADM GUI** 中在 **NetScaler VPX** 上配置负载平衡服务

使用 NetScaler ADM 样书在 NetScaler 实例上部署负载平衡器配置。对于 HA，配置部署在 HA 中的两个 NetScaler 实例上。

要通过样书创建配置包，请执行以下操作：

1. 在 NetScaler ADM 中，导航到“应用程序”>“配置”>“新建”，然后从列表中选择 **HTTP/SSL** 负载平衡（带显示器）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 环境中配置的目标 NetScaler VPX 实例，然后单击“创建”将配置应用到所选设备上。对于 HA 部署，请选择处于 HA 模式的实例。

验证在 **NetScaler VPX** 实例中创建虚拟服务器和服务组

您可以查看服务组和虚拟服务器是通过登录 NetScaler VPX 实例创建的。

要查看服务组和虚拟服务器，请执行以下操作：

1. 登录 NetScaler VPX 实例对于 HA 部署，您必须登录处于 HA 模式的的两个 NetScaler 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 并查看虚拟服务器的详细信息。
4. 接下来，导航到 服务组 并查看服务组的详细信息。
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 NetScaler 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，请执行以下操作：

1. 在 NetScaler 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 Manager 中，导航到 NetScaler VPX 实例连接到的 Edge 网关。导航到 管理 > 负载平衡器 > G 全局配置，右键单击运行时条目，然后单击“取消配置”。将是虚拟机停止工作。
3. 在 NetScaler ADM 中，导航到“调配”>“云调配”>“边缘网关”。确保没有将 Edge 网关与已删除的实例相应映射。

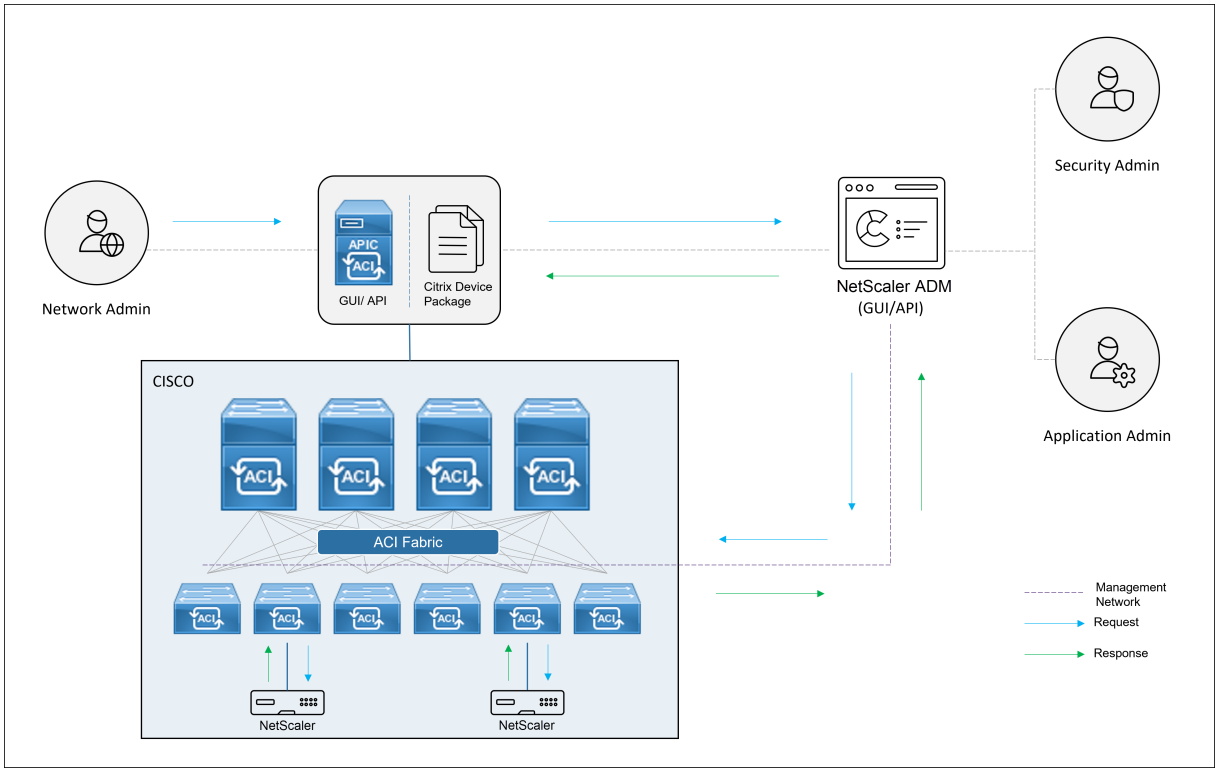
在 **Cisco ACI** 混合模式下使用 **NetScaler** 实现的 **NetScaler ADM** 自动化

February 6, 2024

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设施控制器 (APIC) 执行网络自动化，同时将 L4-L7 配置委托给 NetScaler Application Delivery Management (ADM)，后者在 APIC 中充当设备管理器。

混合模式设备包和 NetScaler ADM 支持 NetScaler 混合模式解决方案。需要在 APIC 中上载混合模式设备包。此包提供 NetScaler 中的所有网络 L2-L3 可配置实体。样书 将应用程序奇偶校验从 NetScaler 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。必须在从 APIC 为 NetScaler 配置网络实体时提供样书名称。

下图概述了混合模式解决方案中的 NetScaler：

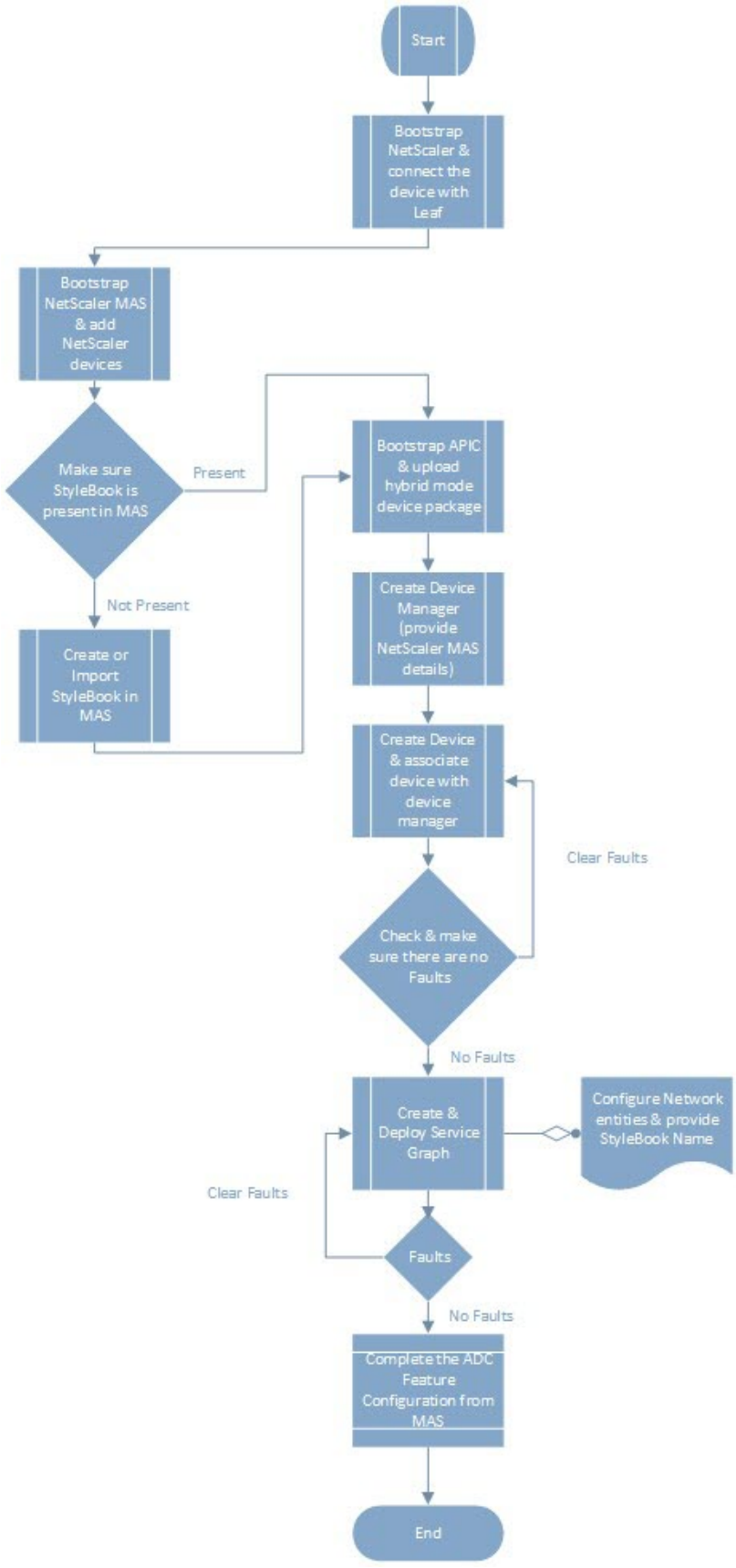


在混合模式下，NetScaler 配置分两个阶段执行：

1. 从 Cisco APIC 进行网络交换
2. 配置是从 NetScaler ADM 完成的

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，这些配置详细信息通过设备包推送到 NetScaler ADM，然后 NetScaler ADM 在内部处理这些详细信息并配置 NetScaler。应用程序管理员在 NetScaler ADM 中使用样书创建应用程序的 ADC 相关配置，然后将这些配置从 NetScaler ADM 推送到 NetScaler。Cisco APIC 和 NetScaler ADM 通过管理网络与 ADC 通信。

下图显示了混合解决方案中的 NetScaler 工作流：



NetScaler 设备封装，采用 **Cisco ACI** 云调配器模式

February 6, 2024

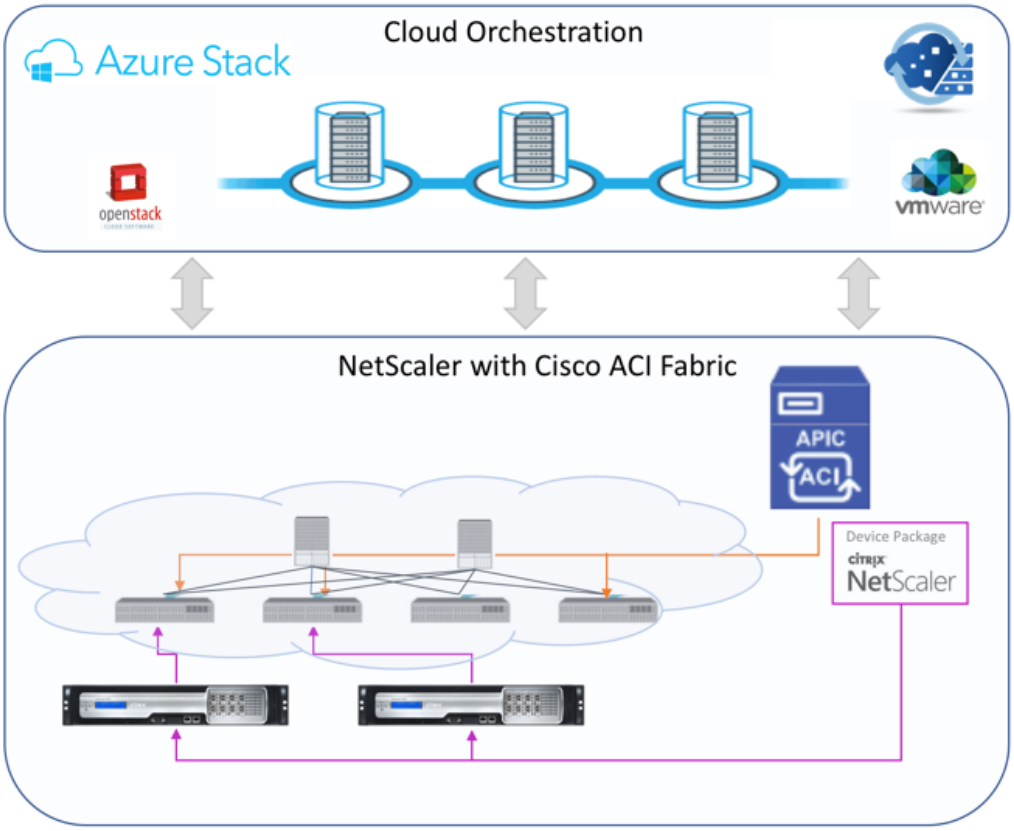
借助 Application Policy Infrastructure Controller (APIC) 3.1 版，Citrix NetScaler 和 Cisco ACI 扩展了联合集成产品组合，以提供满足客户需求的新解决方案。新的集成模式 ACI 云调配程序模式 ** 通过标准化参数抽象配置复杂性，简化了 L4-L7 的集成。该解决方案无缝协作以使 L4-L7 服务自动化，从而实现敏捷应用程序部署、运营灵活性和简便性的目标。

使用 NetScaler 解决方案的 Cisco ACI 云调配程序模式具有以下优势：

- 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 Web 应用程序、虚拟机和 SQL 等应用程序的性能。
- 跨物理和虚拟网络组件全面集成对应用程序（例如 Web 应用程序、虚拟机和 SQL）的运行状况的可见性。

ACI 云调配程序模式现在为您提供了更多选择，可以直接使用新的简化的 APIC GUI，或者根据自己的喜好选择任何云调配程序，例如 Cisco Cloud Center、Windows Azure Pack、OpenStack、vRealize 或任何其他云调配程序这一新变化是通过将一组 ADC 属性公开为 ADC 架构来实现的。这些属性映射到设备包函数配置文件中。您可以在云调配程序（Cisco Cloud Center 或无线应用协议 (WAP)）配置 ADC 服务时为这些属性提供值。

下图概述了云调配解决方案中的 NetScaler：

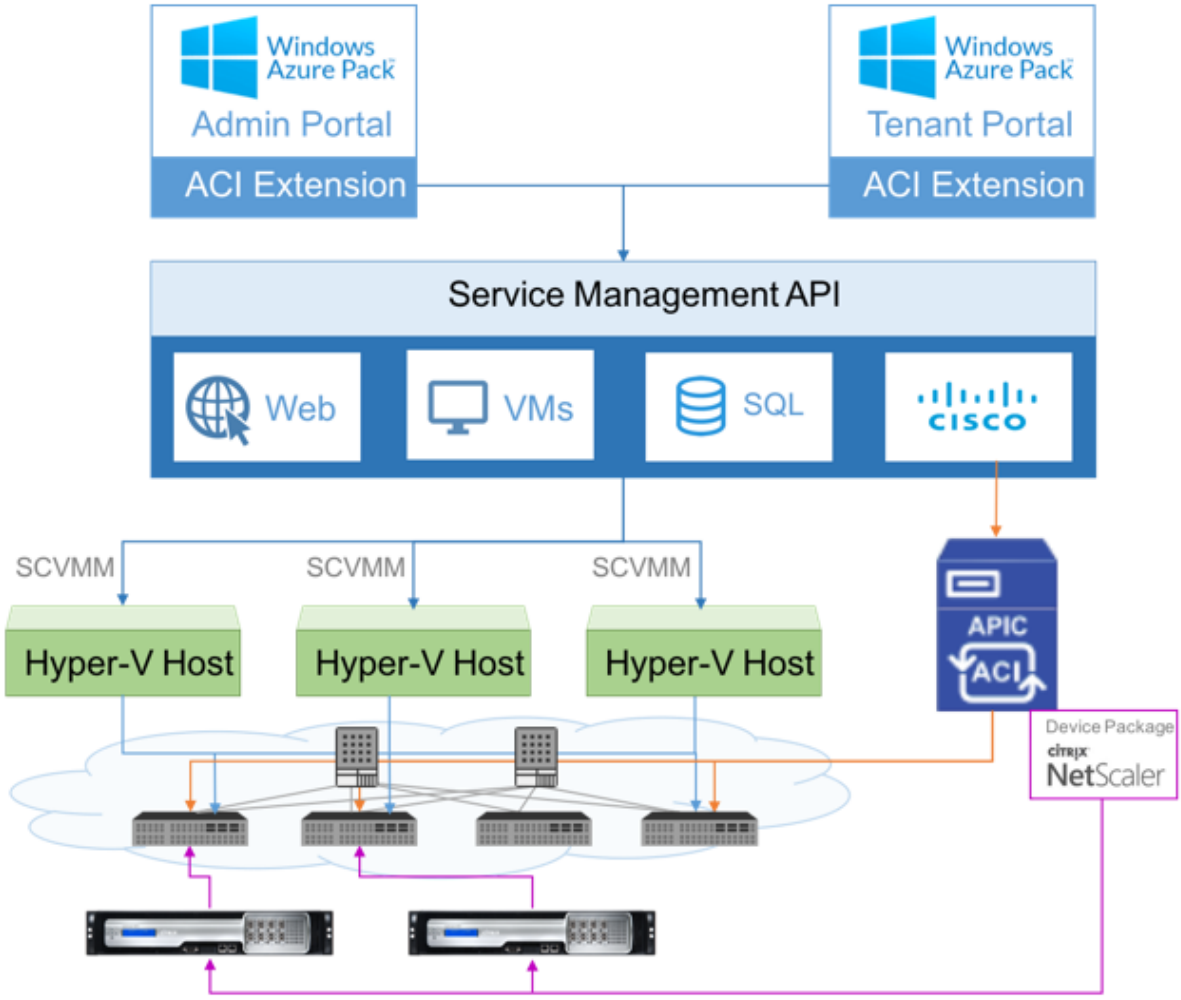


使用 Microsoft Azure 包的云调配程序模式解决方案涉及许多集成点，例如 Azure 包到 Cisco APIC、Cisco APIC 到系统中心虚拟机管理器 (SCVMM)，Cisco APIC 到 NetScaler。作为私有云中的租户，您可以启用 NAT、配置网络服务以及添加负载平衡器。

Azure Pack 支持租户和管理员门户，每个门户都有自己的一组可执行的操作。

- 作为管理员，您可以执行管理任务，例如 ACI 注册、VIP 范围、NetScaler 设备与虚拟机云的关联以及租户用户帐户创建。
- 作为租户，您可以执行诸如登录 Azure Pack 租户门户和配置网络、桥接域和虚拟路由和转发 (VRF) 等任务，还可以使用 NetScaler 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

- 云管理员可以协助使用 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，您就可以配置和部署 NetScaler，使其与受支持的功能集相同。
- 租户可以为同一网络部署具有不同端口的多个 VIP 地址。必须确保 IP 和端口组合是唯一的。
- NetScaler 设备包仅支持单上下文部署。每个租户都将获得一个专用的 NetScaler 实例。
- 无线应用程序协议 (WAP) 支持 NetScaler MPX 设备和 NetScaler VPX 设备（包括部署在 NetScaler SDX 平台上的 NetScaler VPX 实例）。

云调配程序模式设备包同时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、内容交换、SSL 卸载和其他配置文件。这些功能配置文件涵盖了 NetScaler 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单臂和双臂配置以及使用 APIC 部署 NetScaler。NetScaler Application Delivery Management (ADM) 充当 APIC 的服务管理器，您可以使用 NetScaler ADM 配置 NetScaler L4-L7 参数。

> 注意
>
> 在服务管理器模式（混合模式）下，您无法重复使用或重新分配相同的服务器 IP 地址，该地址已存在于 NetScaler 设备中。

云调配程序模式功能配置文件有一组映射到 APIC ADC 架构的参数，并且调配程序将使用这些参数。云调配程序提供 ADC 参数的值（VIP，同时通过 APIC 预配 NetScaler）。调配程序与 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进行传递。在内部，APIC 提取值并将其传递给在内部配置 NetScaler 的设备包。

有关 Cisco APIC 支持的 ADC 架构的完整列表的详细信息，请参阅 Cisco APIC 第 4 层至第 7 层服务部署指南，版本 3.x 及更高版本）。

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

NetScaler 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。如果功能配置文件中存在 Cisco ACI 不支持的属性，则必须克隆云调配程序模式功能配置文件，并由 APIC 为所有不受支持的属性提供值，并且必须保存这些属性。稍后，调配程序可以使用新克隆的功能配置文件。

Citrix Cloud 模式设备包支持 NetScaler 12.0，服务管理器模式也使用 NetScaler ADM 12.0。设备包已将模型版本从 1.0 更改为 2.0，可以用作新安装。云调配模式模式设备包无法从以前的设备包版本升级，因为模型版本已更改。

云调配程序模式设备包也可以在常规部署中使用。该包不强制用户通过任何云调配程序预配 NetScaler。该设备包仅与 APIC 兼容，而 APIC 与云调配程序兼容。

管理 **NetScaler ADM** 中的库伯内特斯入口配置

February 6, 2024

Kubernetes (K8s) 是一个开源容器调配平台，可自动部署、扩展和管理云原生应用。

Kubernetes 提供了 Ingress 功能，该功能允许群集外部的客户端流量访问在 Kubernetes 群集中运行的应用程序的微服务。ADC 实例可以充当 Kubernetes 群集中运行的应用程序的入口。ADC 实例可以负载平衡，并将南北向流量从客户端路由到 Kubernetes 群集内的任何微服务。

> 注意
>
> - NetScaler ADM 在具有 Kubernetes 版本 1.14—1.21 的群集上支持 Ingress 功能。

> - NetScaler ADM 支持 NetScaler VPX 和 MPX 装置作为入口设备。
> - 在 Kubernetes 环境中，NetScaler 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 Ingress 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 Ingress 配置。您还可以从 NetScaler ADM 配置和部署入口。

您可以在 ADM 中指定 Kubernetes 集成的以下几个方面：

- 群集—您可以注册或取消注册 ADM 可以为其部署 Ingress 配置的 Kubernetes 群集。在 NetScaler ADM 中注册群集时，请指定 Kubernetes API 服务器信息。然后，选择一个可以访问 Kubernetes 群集的 ADM 代理并部署 Ingress 配置。
- 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 Ingress 配置。在添加策略时指定群集、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。还可以使用 Kubernetes 密钥资源指定 SSL/TLS 证书（用于卸载 ADC 实例上的 SSL 处理）。

NetScaler 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 Ingress 配置，NetScaler ADM 都会生成一个样书 ConfigPack。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 ConfigPack，请导航到“应用程序” **>** “样书” **>** “配置”。

开始之前的准备工作

要在 Kubernetes 群集上将 NetScaler 实例用作 Ingress 设备，请确保您具备以下条件：

- 库贝内特斯群集到位。
- 在 NetScaler ADM 中注册的库贝内特斯群集。

使用秘密令牌配置 **NetScaler ADM** 以管理 **Kubernetes** 群集

为了使 NetScaler ADM 能够接收来自 Kubernetes 的事件，您需要在库贝内特斯中为 NetScaler 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 NetScaler 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 NetScaler ADM 服务帐户。此绑定将 `ClusterRole` 整个群集中的授予服务帐户。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 NetScaler 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` 创建 `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. 运行以下命令获取令牌的密钥字符串：

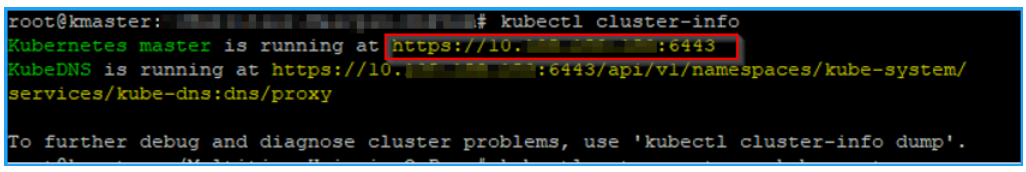
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

在 **NetScaler ADM** 中添加 **Kubernetes** 群集

配置 NetScaler ADM 代理并配置静态路由后，必须在 NetScaler 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 NetScaler ADM。
2. 导航到调配 > **Kubernetes** > 群集。
   屏幕上将显示“群集”页面。
3. 单击添加。
4. 在“添加群集”页中，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 配置 NetScaler ADM 以管理 Kubernetes 群集时获得的身份验证令牌字符串。验证 Kubernetes 群集和 NetScaler 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：

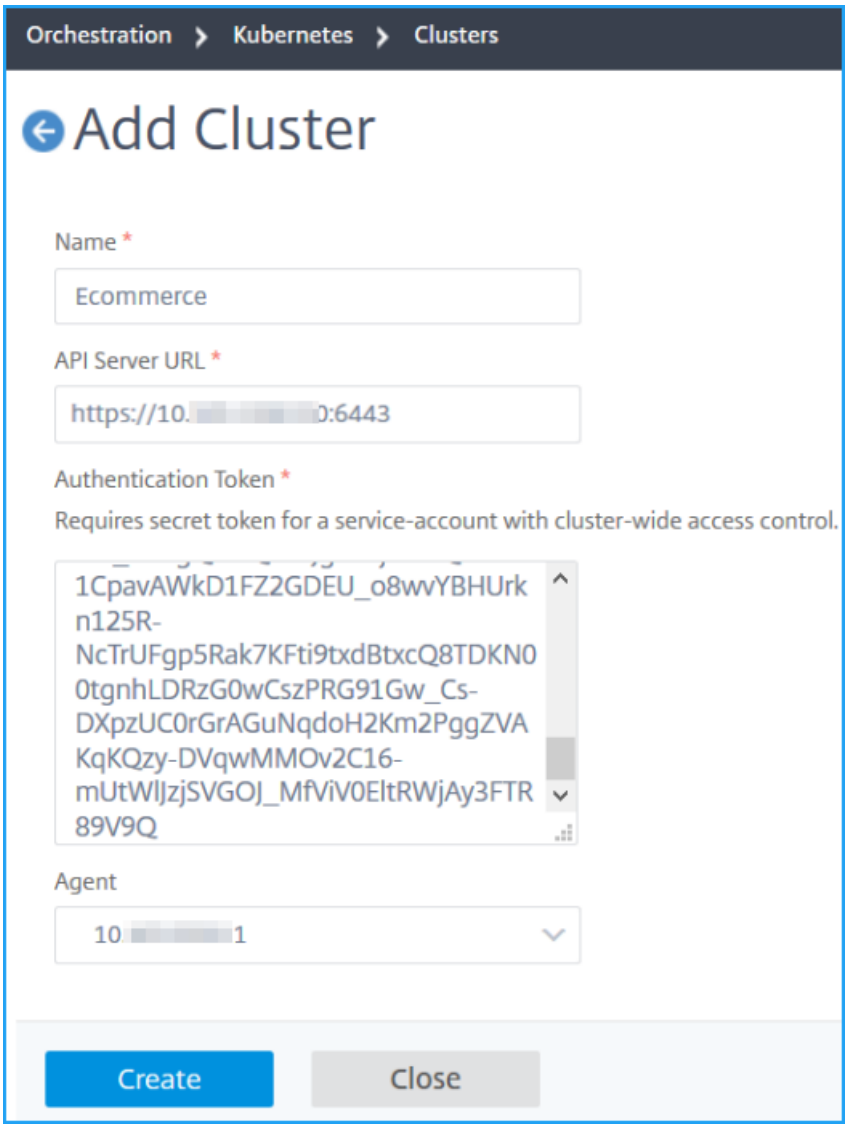
```
kubectl describe secret <token-name>
<!--NeedCopy-->
```

ii. 复制生成的令牌并将其粘贴为身份验证令牌

有关更多信息，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来决定使用哪个 NetScaler 来部署入口配置。

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 条件 以在 Kubernetes 群集上部署 Ingress 配置。这些条件通常基于 Ingress 群集和命名空间。
   c) 在“基础架构”面板中，
      - 站点 -从列表中选择一个站点。
      - 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。

      这些列表显示了与使用 Kubernetes 群集配置的 NetScaler ADM 代理关联的站点或实例。
   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。

      此列表显示了在 基础架构 **> IPAM** 中创建的网络。
   e) 单击创建。

部署入口配置

您可以使用 `kubectl`Kubernetes API 或其他工具从 Kubernetes 部署入口配置。您还可以直接从 NetScaler ADM 部署 Ingress 配置。

1. 导航到 调配 **> Kubernetes >** 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 Ingress 的 Kubernetes 群集。
   c) 从列表中选择 群集命名空间。此字段列出了指定 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** 密钥。

      这个密钥嵌入了嵌入 HTTPS 证书和私钥的 Kubernetes 密钥资源。

      HTTPS 入口需要在 Kubernetes 群集上配置一个基于 TLS 的密钥。指定 `tls.crt` 和 `tls.key` 字段以分别包含服务器证书和证书密钥。
   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。
- 负载平衡方法 - 为选定的 Kubernetes 服务选择首选的负载平衡方法。

  选定的方法会使用相应的注释来更新 Ingress 规范。例如，如果选择 **ROUNDROBIN** 方法，Citrix 注释将显示如下：

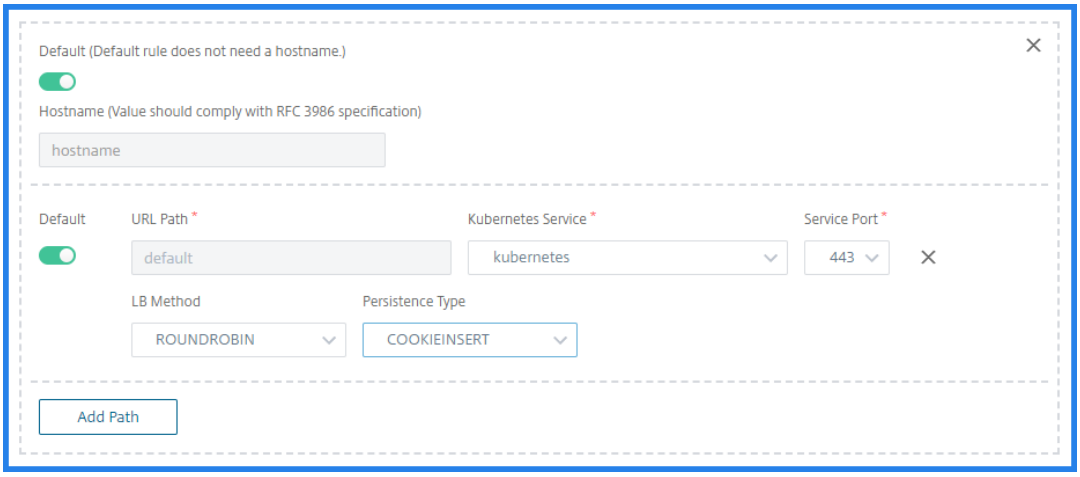
```
"lbmethod":"ROUNDROBIN"
<!--NeedCopy-->
```

- 持久性类型 -选择所选 Kubernetes 服务的首选负载平衡持久性类型。

  选定的持久性类型会使用相应的注解来更新 Ingress 规范。例如，如果选择 **COOKIEINSERT**，Citrix 注释将显示如下：

```
"persistenceType":"COOKIEINSERT"
<!--NeedCopy-->
```

单击“添加”将更多 URL 路径和端口添加到 Ingress 配置中。



部署后，Ingress 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
>
> 入口配置中使用的 Kubernetes 服务应该是 NodePort 类型。

g) 可选，指定 入口描述。

h) 单击部署。

如果要在部署前查看配置，请单击 生成 **Ingress** 规范。指定的 Ingress 配置将以 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 Ingress 配置创建的虚拟服务器。要应用许可证，请执行以下步骤：
>
> 1. 前往“设置”>“许可和分析配置”。
> 2. 在“虚拟服务器许可证摘要”下，启用 自动选择虚拟服务器。

Video Insight

February 6, 2024

Video Insight 功能提供了一种简单且可扩展的解决方案，用于监视 NetScaler 设备使用的视频优化技术的指标，以改善客户体验和运营效率，其优点包括：

- 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，NetScaler 设备使用特殊机制来动态调节视频比特率，并采用随机采样技术来估计优化技术节省的成本。有关 NetScaler 视频优化功能的详细信息，请参阅 视频优化。当您将 NetScaler 设备与 NetScaler Application Delivery Management (ADM) 集成时，它会从流经 NetScaler 设备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
>
> NetScaler ADM 中提供的未优化会话的统计信息与您在 NetScaler 设备中选择的随机采样会话相对应。有关随机采样的更多信息，请参阅视频优化。

NetScaler ADM 中的 Video Insight 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 NetScaler 高级许可证的 NetScaler 实例支持 Video Insight。NetScaler 高级许可证受到 NetScaler 电信平台（VPX T1000 和 VPX-T）的支持。

要在 NetScaler 实例上配置 Video Insight，请先启用 AppFlow 功能、配置 AppFlow 收集器、操作和策略以及全局绑定策略。配置收集器时，必须指定要监视报告的 NetScaler ADM 服务器的 IP 地址。

要在 NetScaler 实例上配置 Video Insight，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

set appflow param -**videoInsight** ENABLED

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-->
```

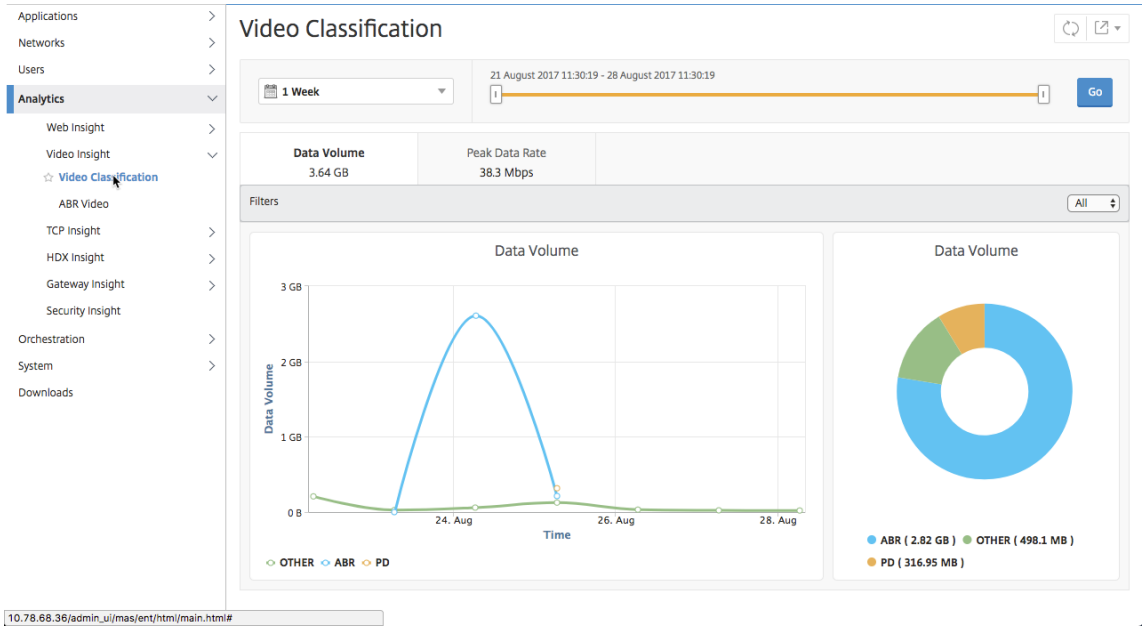
在 **NetScaler ADM** 中查看 **Video Insight** 指标

在 NetScaler ADM 中启用 Video Insight 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 **NetScaler ADM** 中查看 **Video Insight** 指标，请执行以下操作：

1. 在网络浏览器中，键入 NetScaler 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
>
> 图表中图例 **OTHER** 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过滤器：
>
> - 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

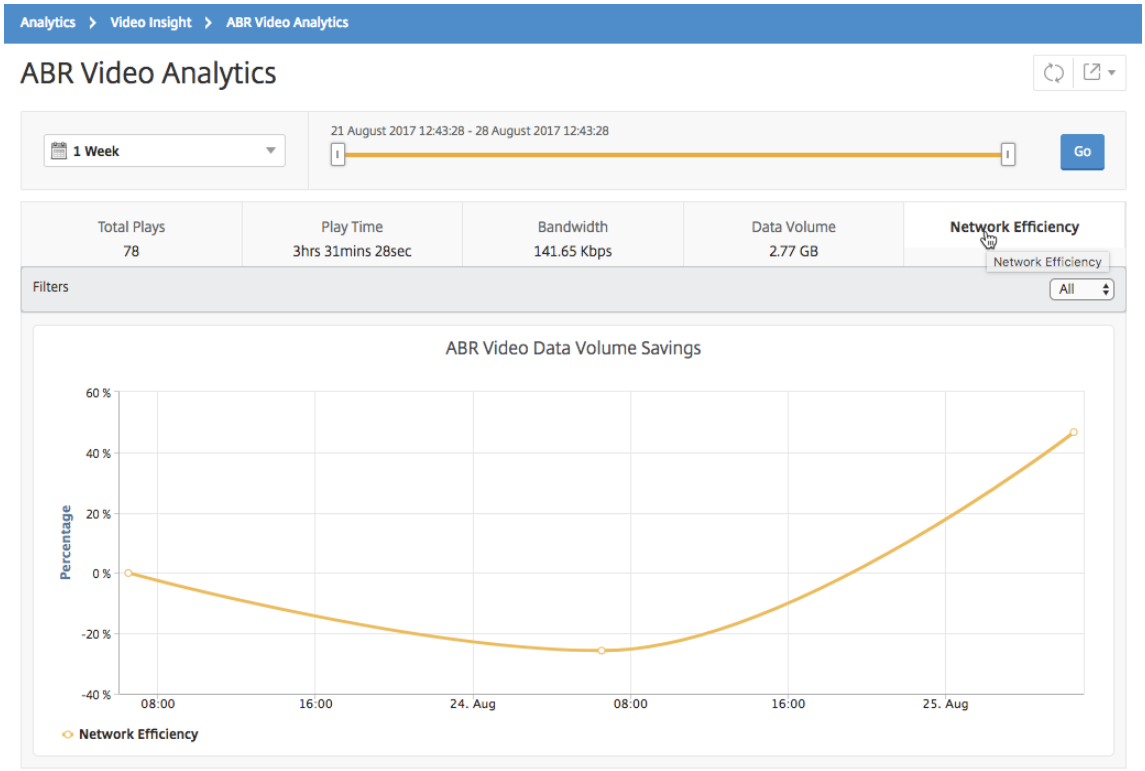
February 6, 2024

在给定的时间范围内，NetScaler Application Delivery Management (ADM) 提供了一张图表，显示了该时间范围内优化和未优化的视频会话的比率。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。

要查看通过优化节省的带宽百分比，请执行以下操作：

1. 导航到“分析”**>** “**Video Insight**”，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。



比较优化和未优化的 **ABR** 视频使用的数据量

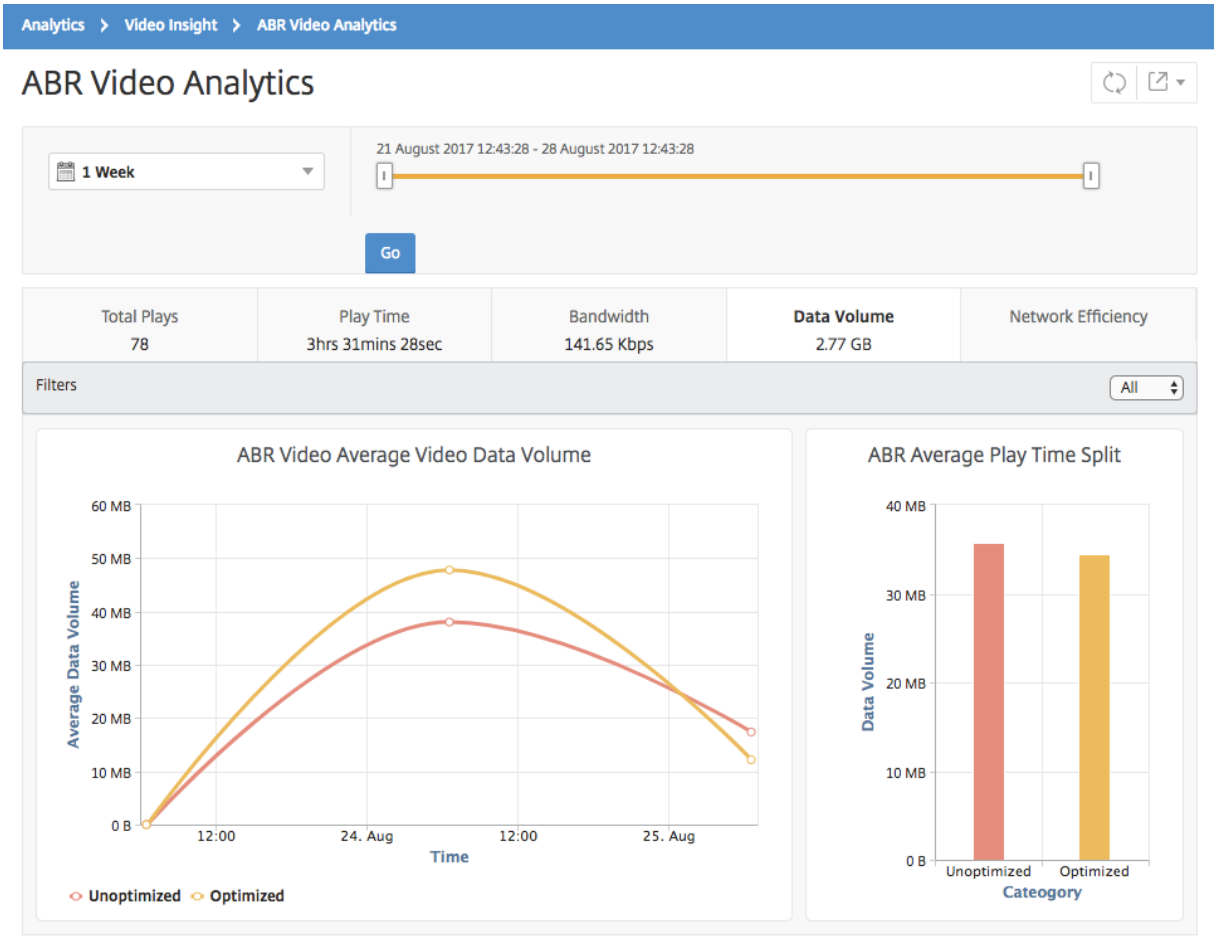
February 6, 2024

在给定的时间范围内，NetScaler Application Delivery Management (ADM) 显示优化和未优化的 ABR 视频使用的数据量，以便您可以比较这两个数据量。

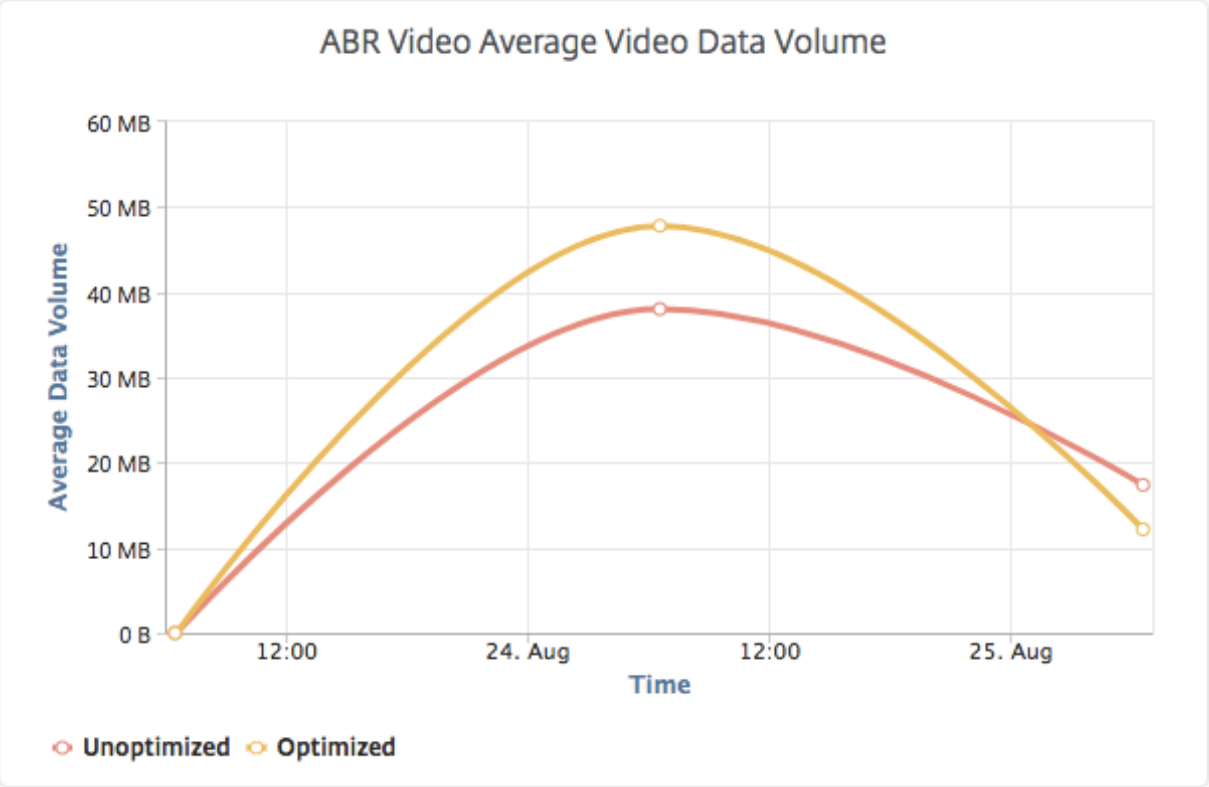
要查看 ABR 视频使用的数据量，请执行以下操作：

1. 导航到“分析”**>** “**Video Insight**”，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：



查看您的网络中通过流技术推送的视频类型和使用的数据量

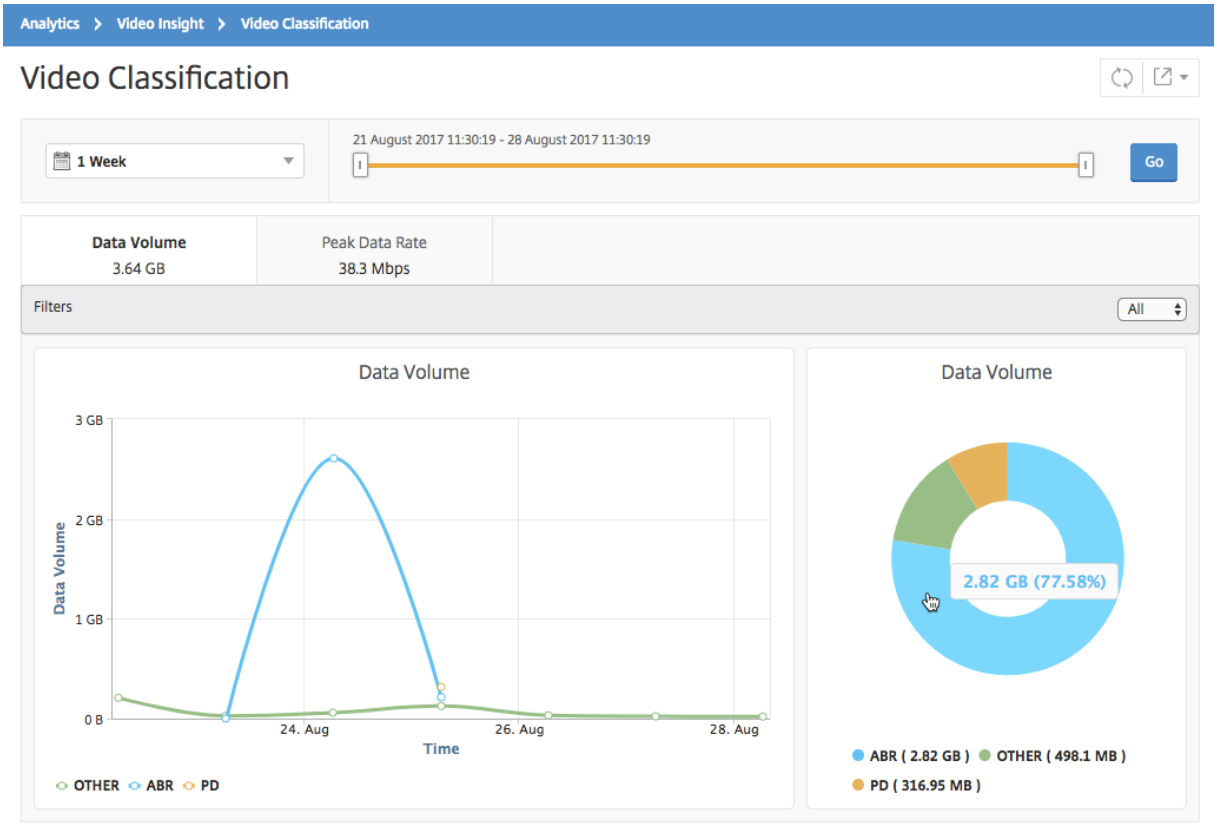
February 6, 2024

NetScaler 设备可检测您的网络中的加密或未加密视频流量以及视频流的类型 (PD 或 ABR)。NetScaler Application Delivery Management (ADM) 显示这些指标以及在定义的时间范围内视频流量消耗的数据量。

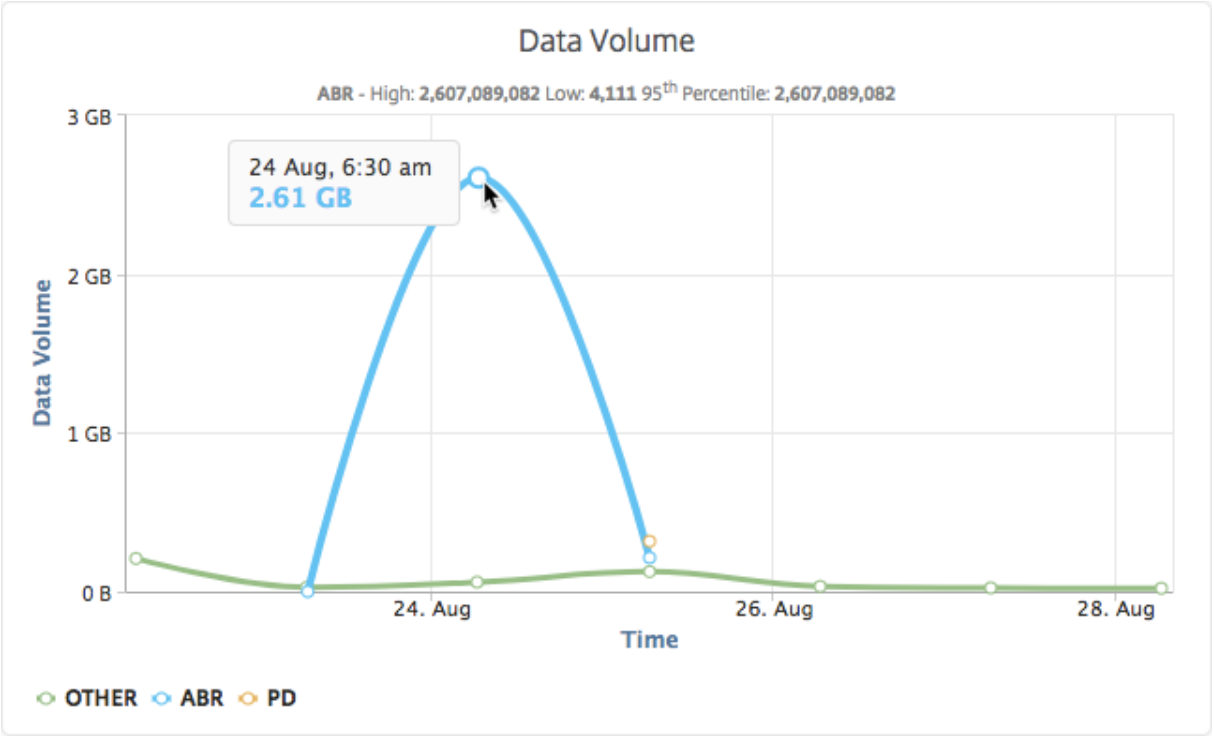
要查看视频类型和消耗的数据量，请执行以下操作：

1. 导航到“分析”**>** “**Video Insight**”，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。

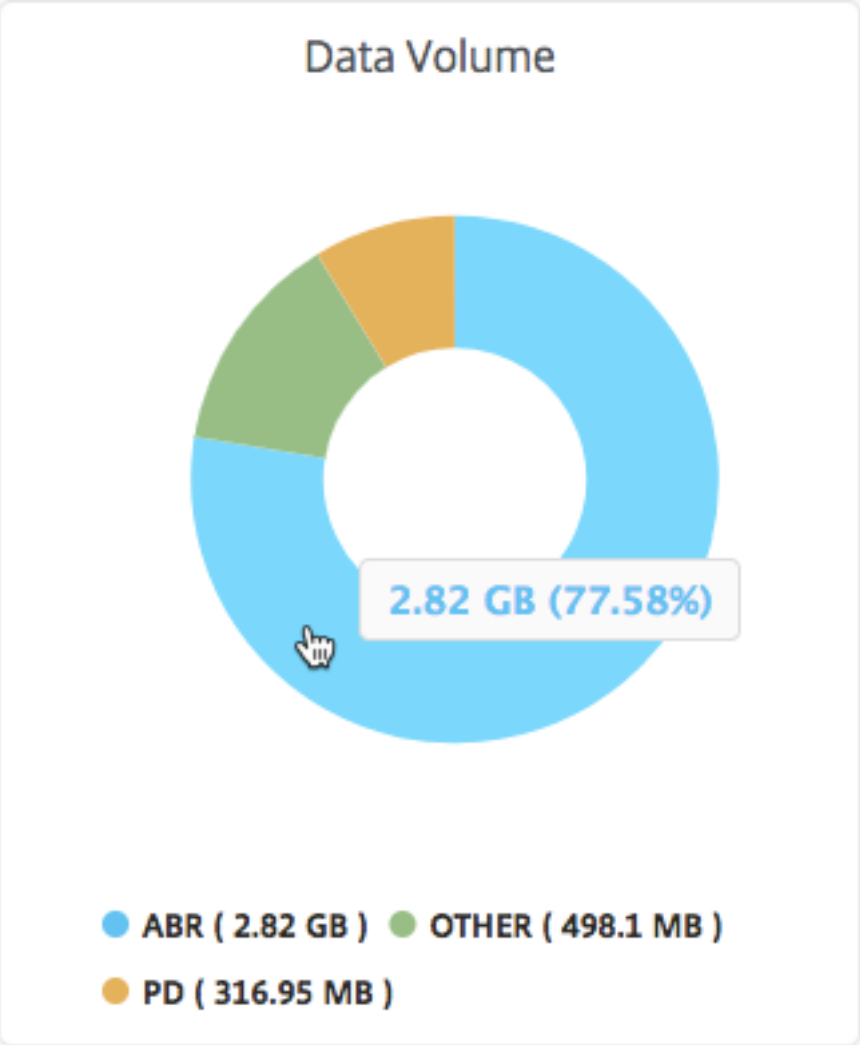
您可以使用 筛选器 列表选择 HTTP、HTTPS 或 QUIC 流量。



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的播放时间

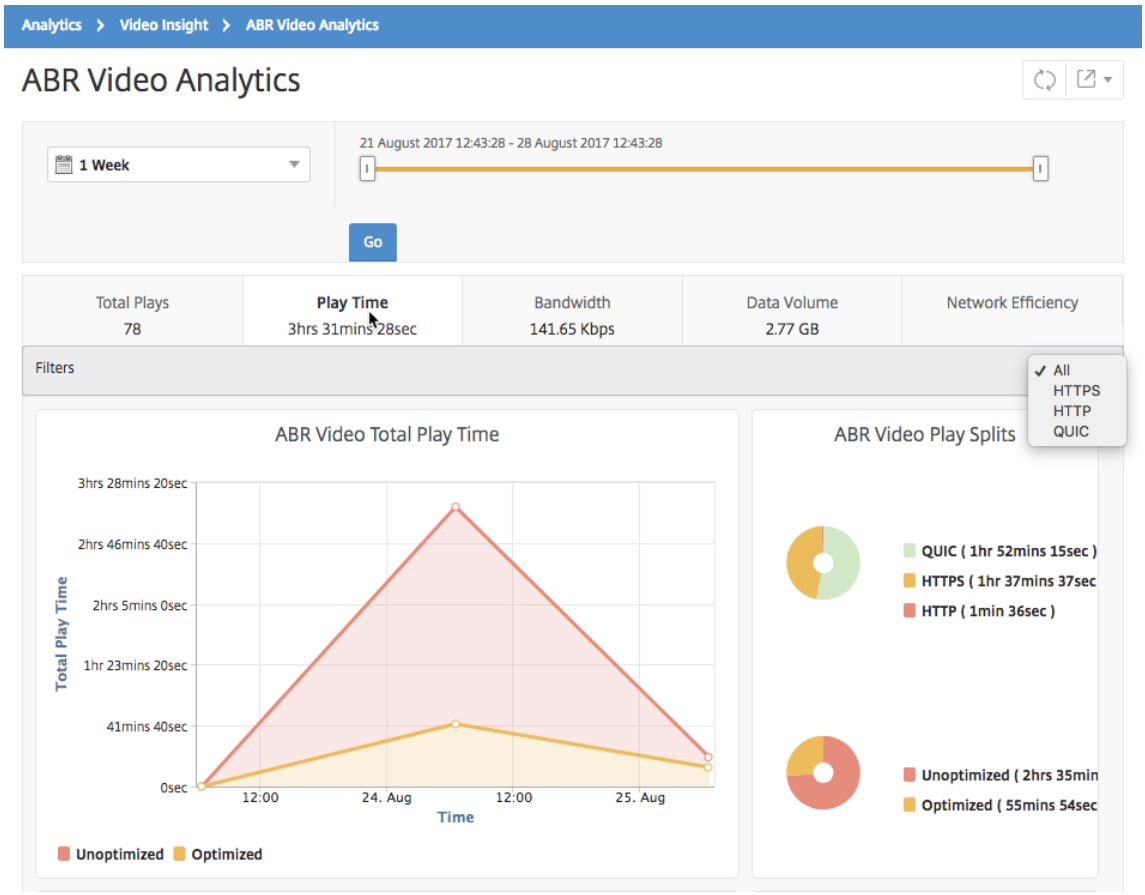
February 6, 2024

在给定的时间范围内，NetScaler Application Delivery Management (ADM) 提供 ABR 视频的播放时间，还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：

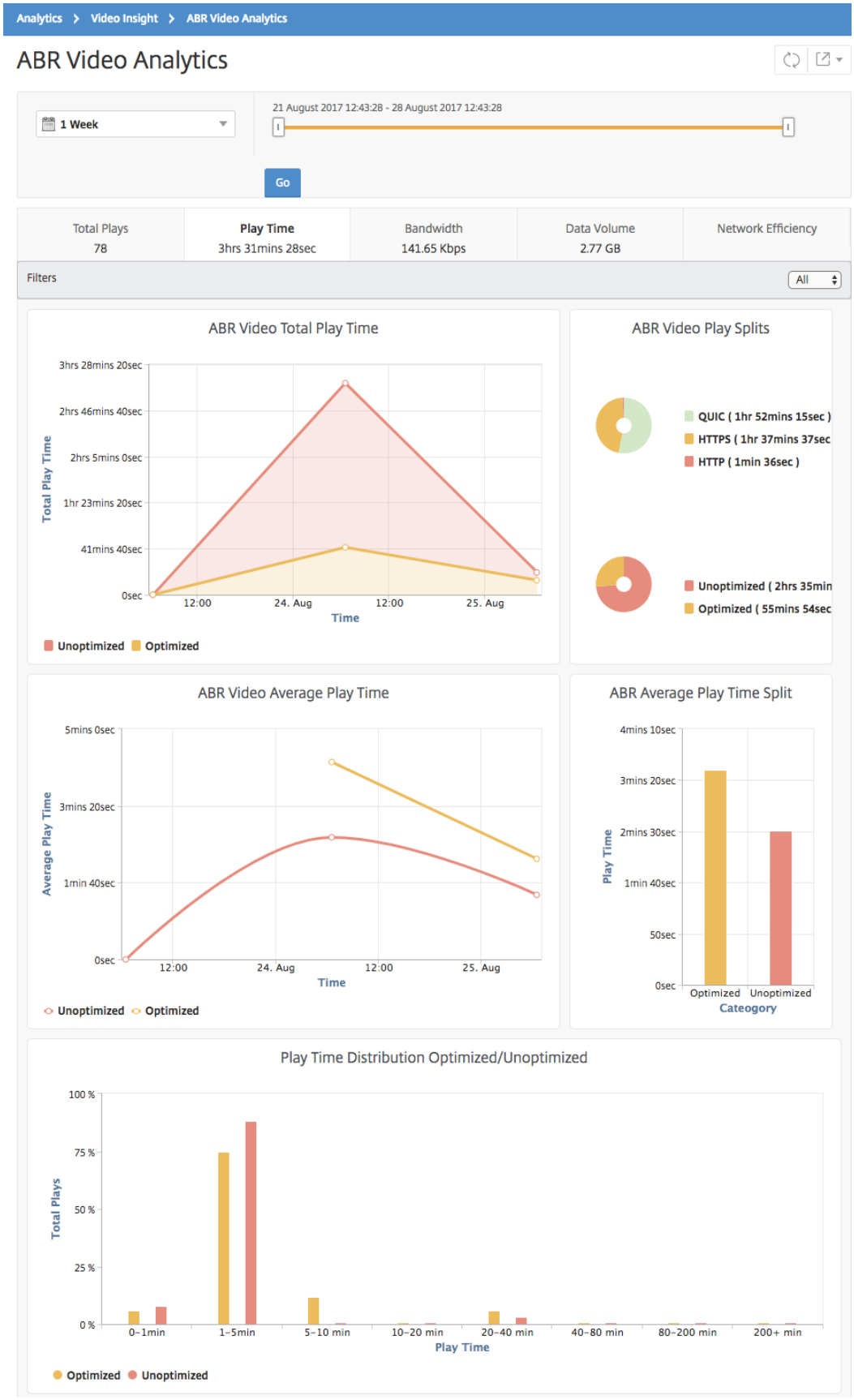
1. 导航到“分析”**>** “**Video Insight**”，然后单击“**ABR** 视频”。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（转到），并选择 **Play Time**（播放时间）选项卡。

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
- 在选定时间范围内播放来自您的网络的 ABR 视频的优化和未优化播放的总播放时间
- 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



比较优化和未优化的 **ABR** 视频的带宽占用量

February 6, 2024

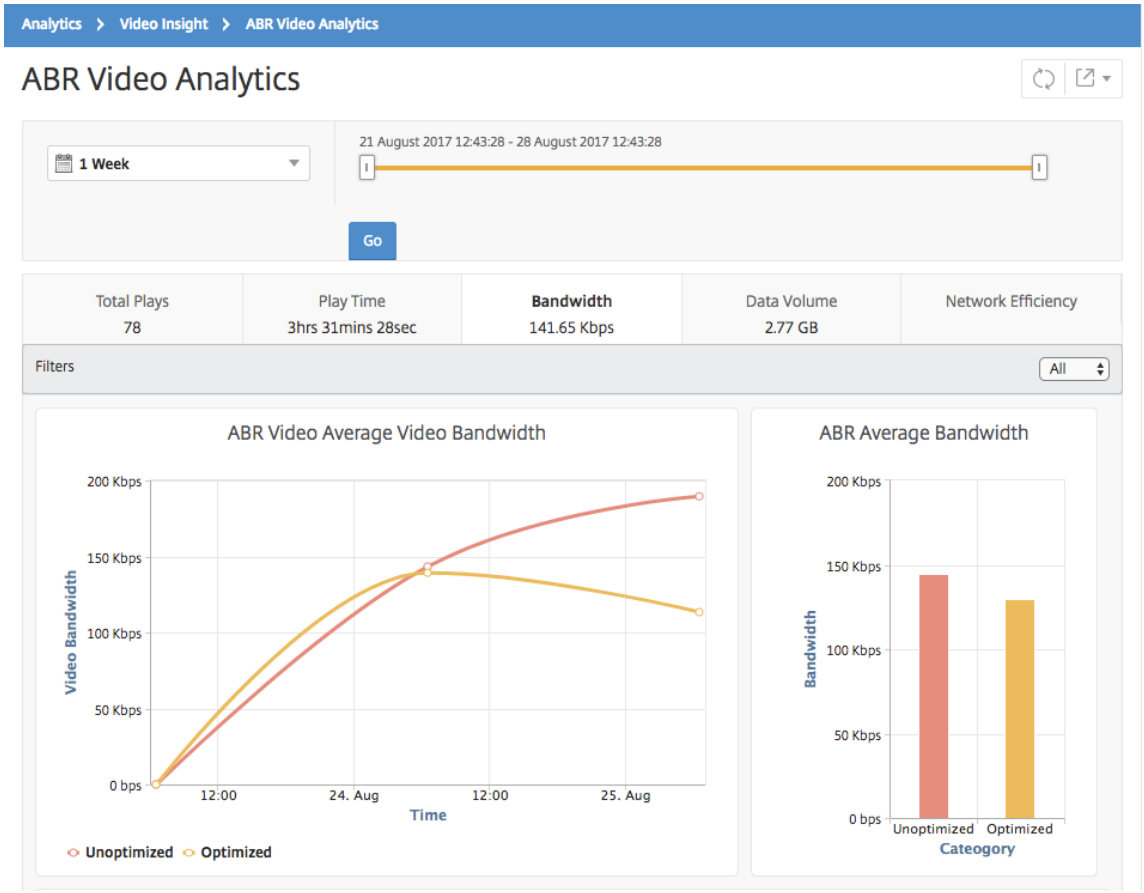
在给定的时间范围内，NetScaler Application Delivery Management (ADM) 提供优化和未优化 ABR 视频所消耗的带宽，还使您能够根据以下条件比较网络中优化和未优化的 ABR 视频消耗的带宽：

- Play Time（播放时间）
- Data Volume（数据量）

要查看带宽消耗，请执行以下操作：

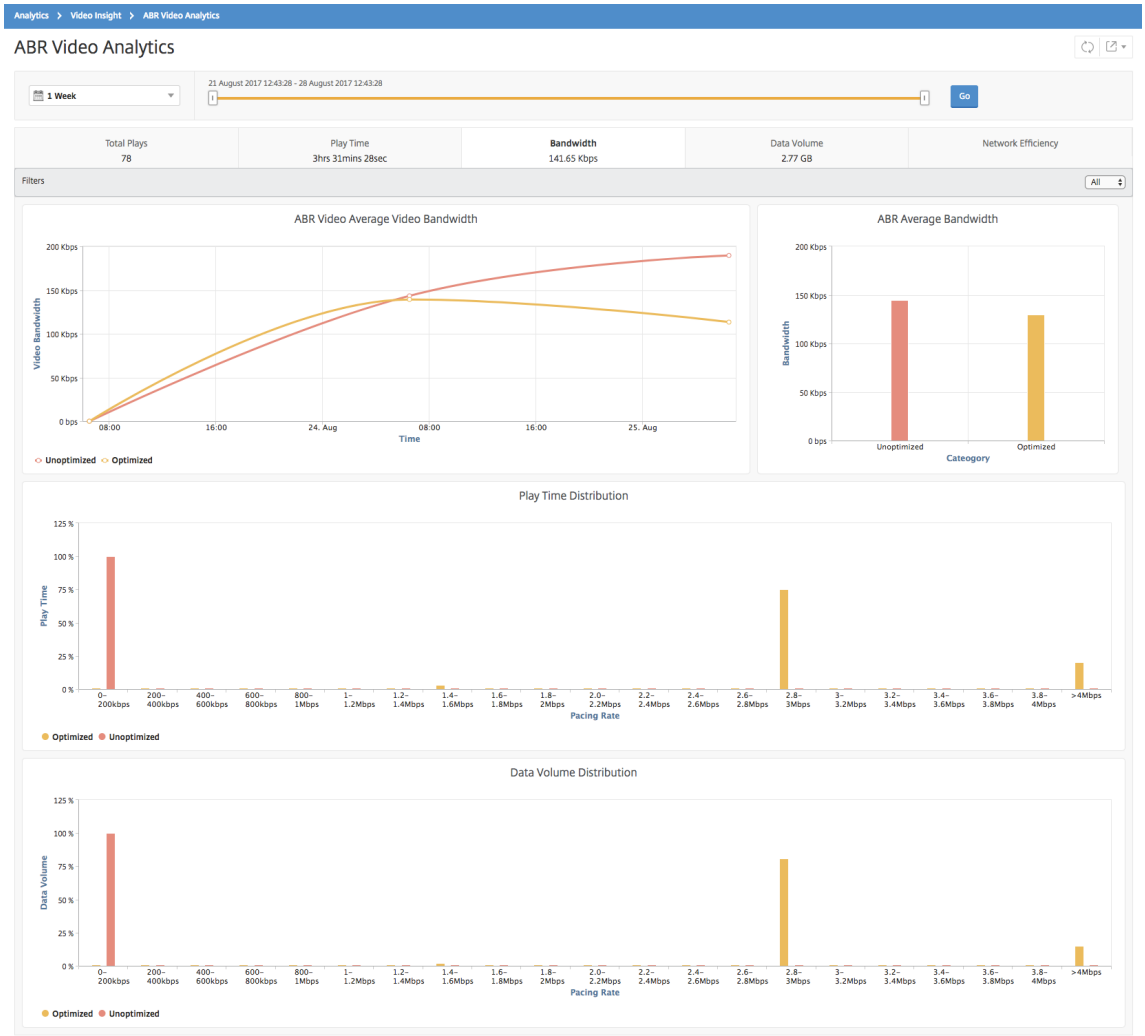
1. 导航到 分析 **> Video Insight** ，然后单击 **ABR** 视频分析。
2. 在右窗格中，从列表中选择一个时间范围。可以使用时间范围滑块进一步自定义时间范围。
3. 单击 **Go**（转到），并选择 **Bandwidth**（带宽）选项卡。

   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 **ABR** 视频的优化和未优化的播放数

February 6, 2024

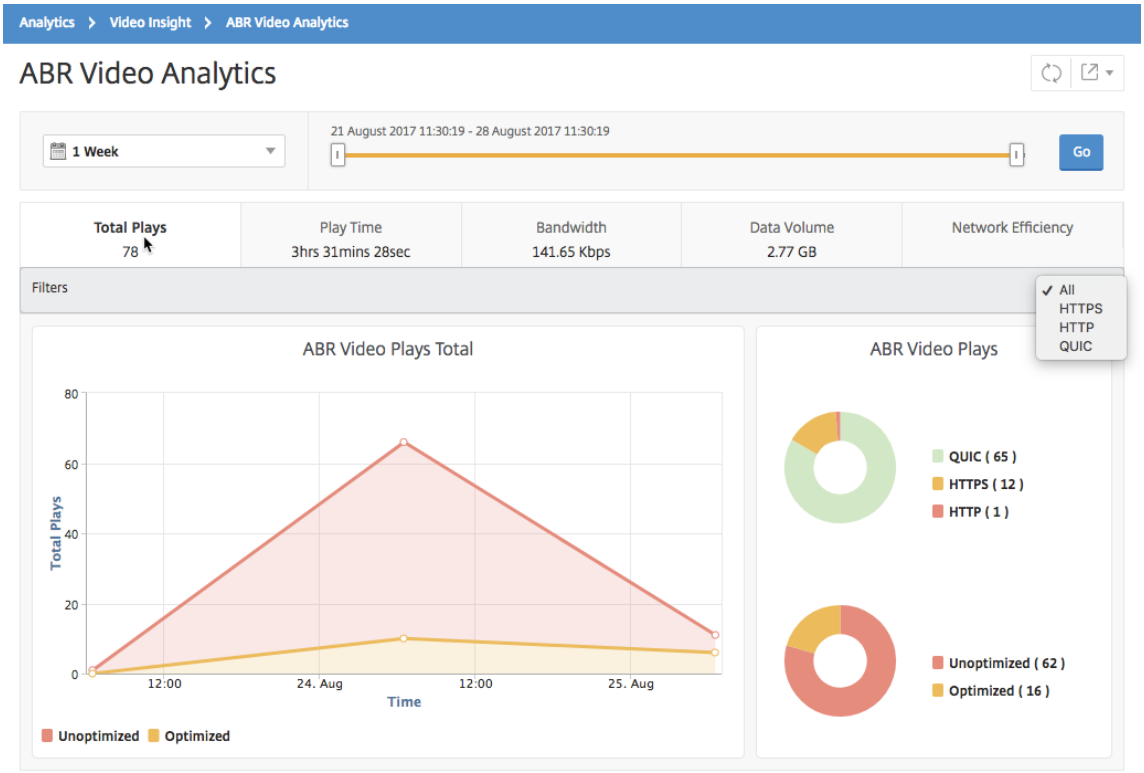
在给定的时间范围内，NetScaler Application Delivery Management (ADM) 显示 ABR 视频的播放次数，使您能够比较网络中优化和未优化的播放次数。

要查看播放次数，请执行以下操作：

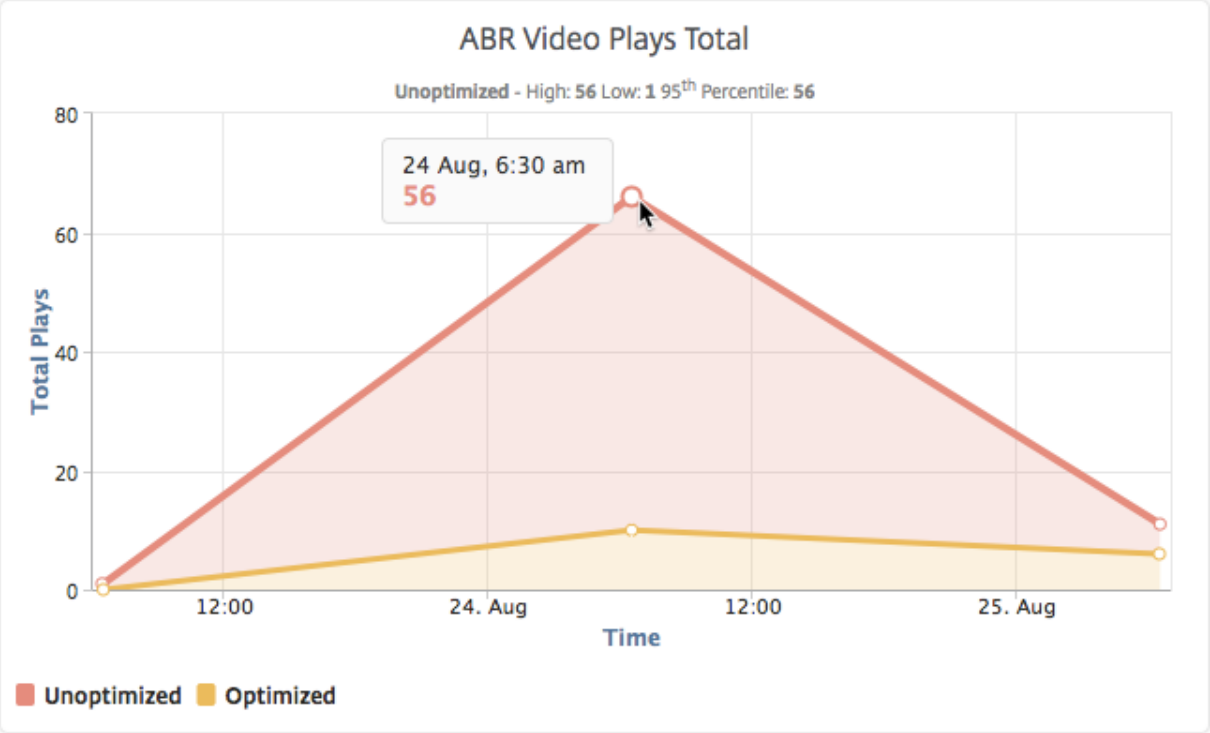
1. 导航到“分析”**>**“**Video Insight**”，然后单击 **ABR** 视频分析。

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。

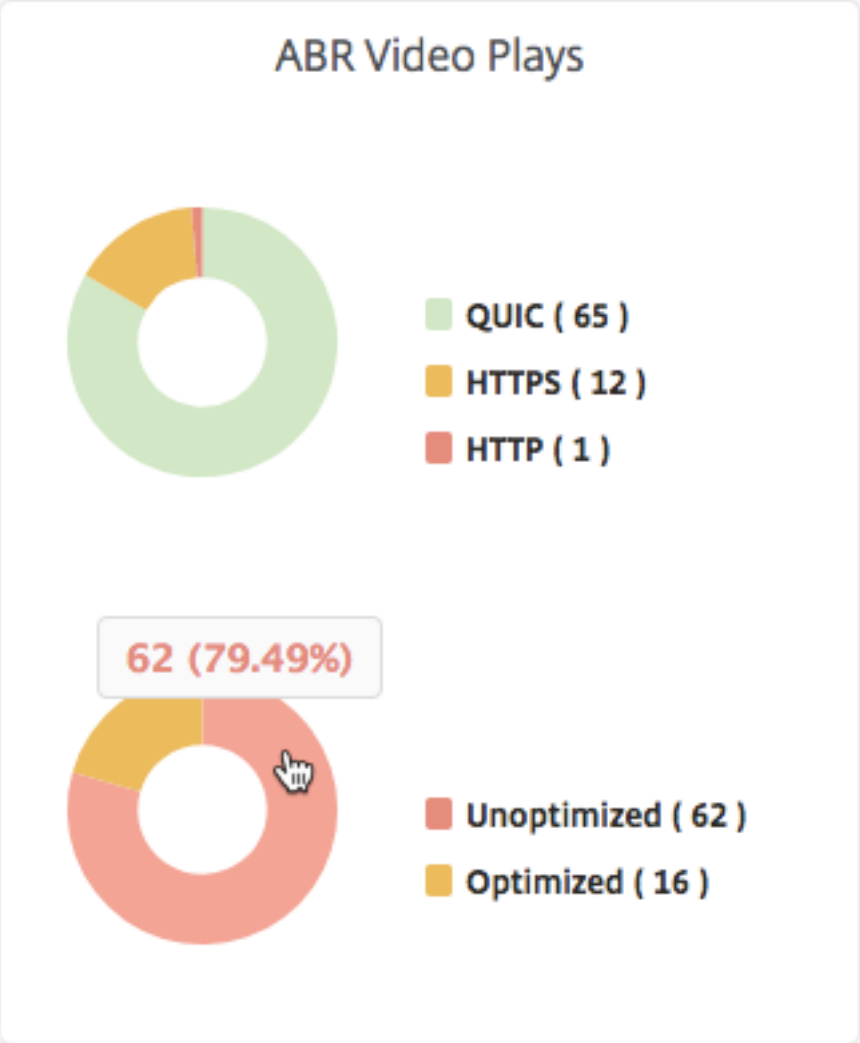
   您可以使用 **Filters**（过滤器）列表选择 HTTP、HTTPS 或 QUIC ABR 视频。



# 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

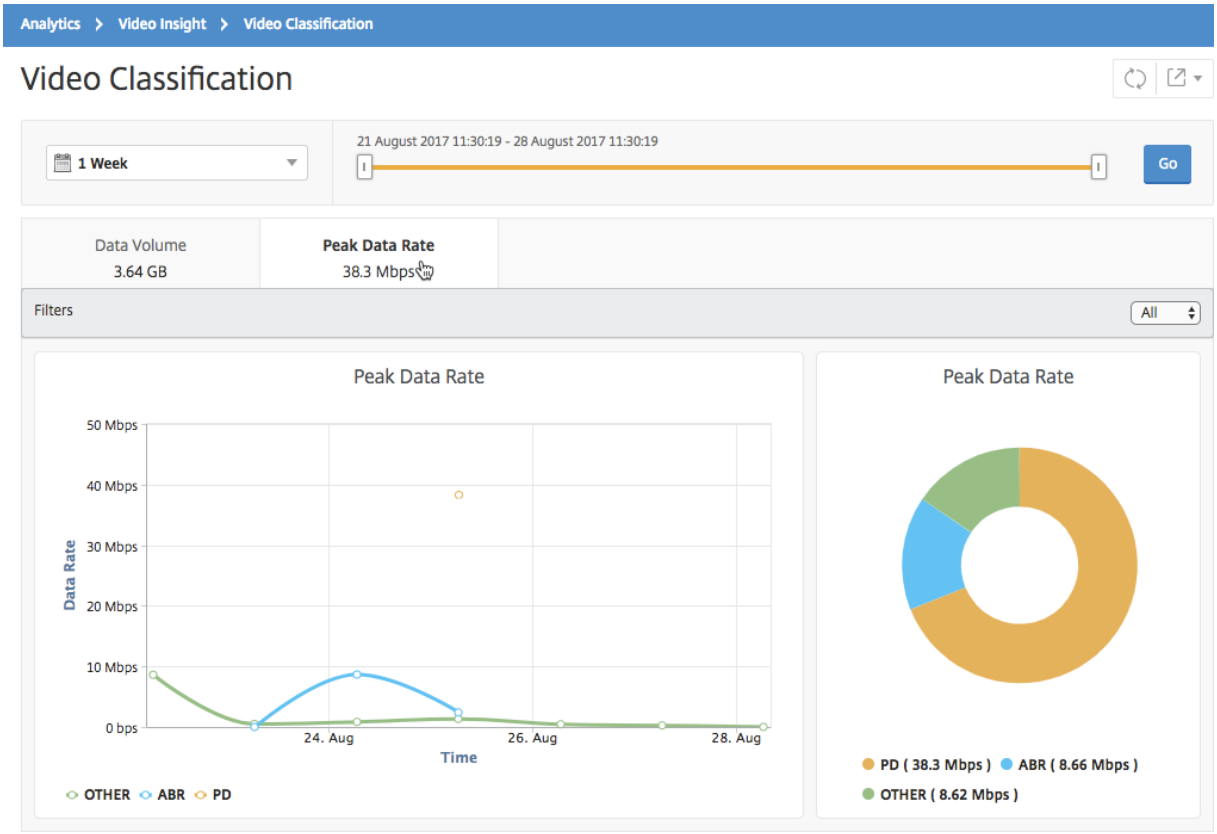
February 6, 2024

NetScaler Application Delivery Management (ADM) 向您显示网络中视频流量的峰值吞吐量或数据速率。

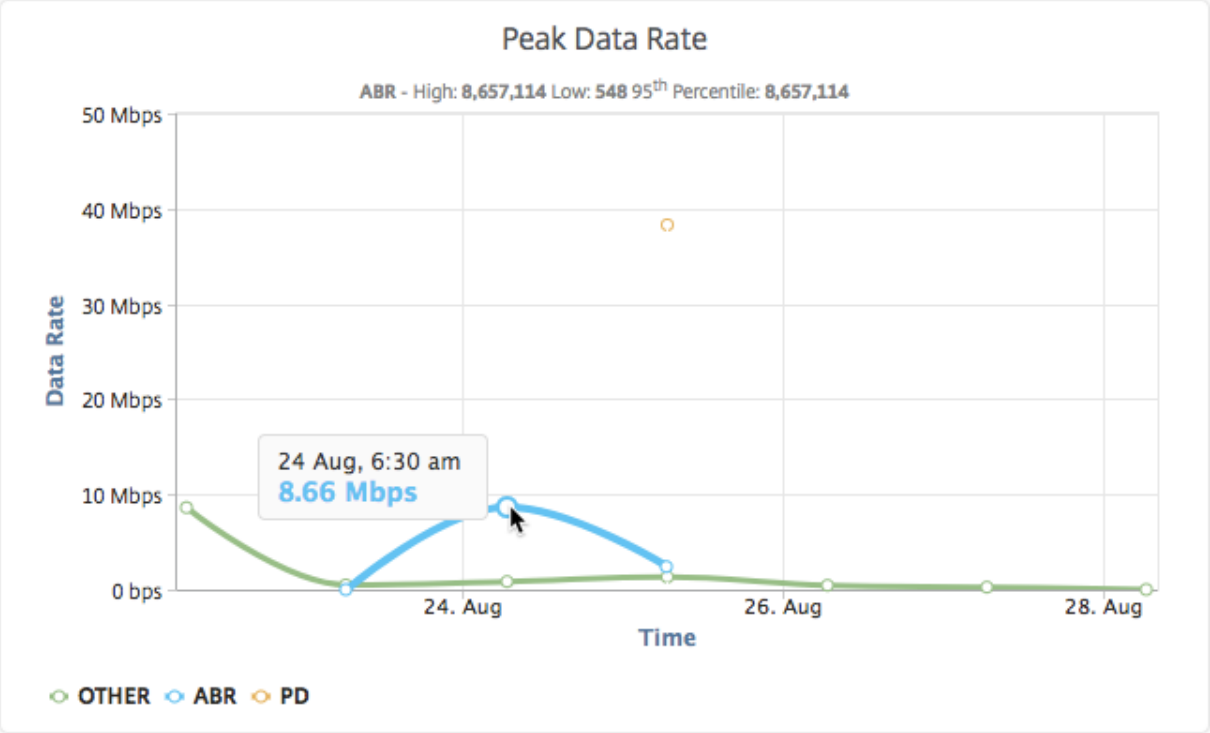
要查看视频流量的峰值数据速率，请执行以下操作：

1. 导航到“分析”**>**“**Video Insight**”，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。

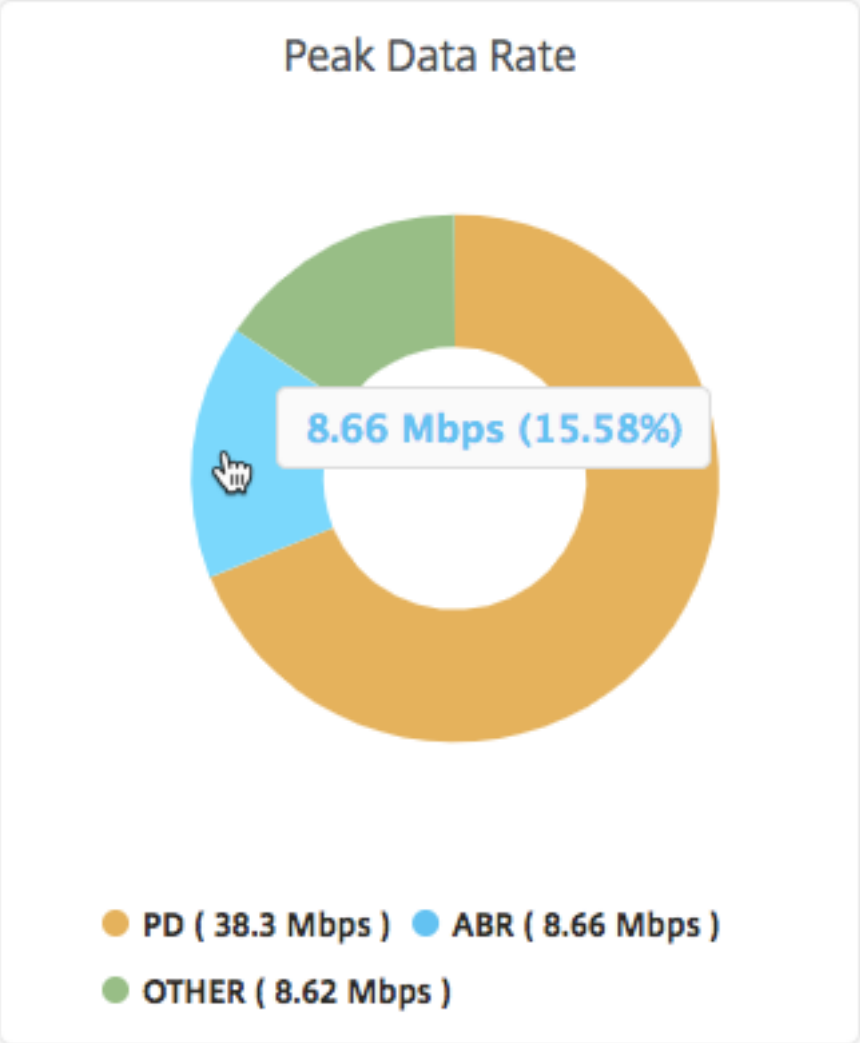
您可以使用 筛选器 列表选择 HTTP、HTTPS 或 QUIC 流量。



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。



配置 **IP** 地址管理 **(IPAM)**

February 6, 2024

ADM IPAM 使您能够在 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 提供商定义的网络或 IP 范围中分配 IP 地址：

- ADM 内置 IPAM 提供商。
- 信息布鲁 IPAM 解决方案。有关更多信息，请参阅 Infoblox DDI。

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 分配给虚拟服务器。
- **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** 地址提供商

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 基础架构 **> 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 提供商：
    - 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 -指定登录到 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 基础架构 **> IPAM**。
2. 在 网络中，单击 添加。
3. 指定以下详细信息：
    - 网络名称 -指定网络名称以在 ADM 中标识网络。
    - 提供商 -从列表中选择提供商。

      此列表显示了在 ADM 中添加的提供商。
    - 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 基础架构 **> IPAM**。
2. 在 网络 选项卡中，单击 查看所有已分配的 **IP**。

   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**。

使用 **ADM** 审核日志管理和监视您的基础架构

February 6, 2024

您可以使用 NetScaler ADM 服务来跟踪 ADM 上的所有事件以及在 ADM 管理的 ADC 实例上生成的 syslog 事件。这些消息可以帮助您管理和监视基础结构。但是，只有在您查看日志消息时，日志消息才是很好的信息来源，而且 ADM 简化了查看日志消息的方式。

可以使用过滤器搜索 ADM syslog 和审核日志消息。过滤器有助于缩小结果范围，并实时准确找到您要查找的内容。内置的“Search Help”（搜索帮助）将指导您筛选日志。查看日志消息的另一种方法是将其导出为 PDF、CSV、PNG 和 JPEG 格式。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。

可以从 ADM GUI 中查看以下类型的日志消息：

- 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

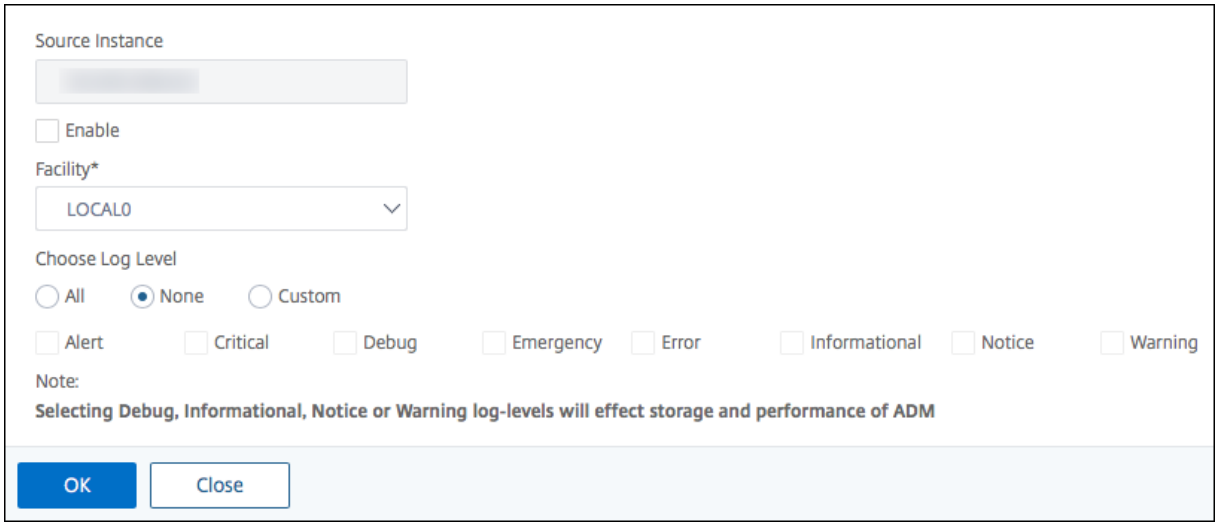
ADC 实例相关的审核日志

在查看来自 ADM 的 ADC 实例相关系统日志消息之前，请将 NetScaler ADM 服务配置为 NetScaler 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。

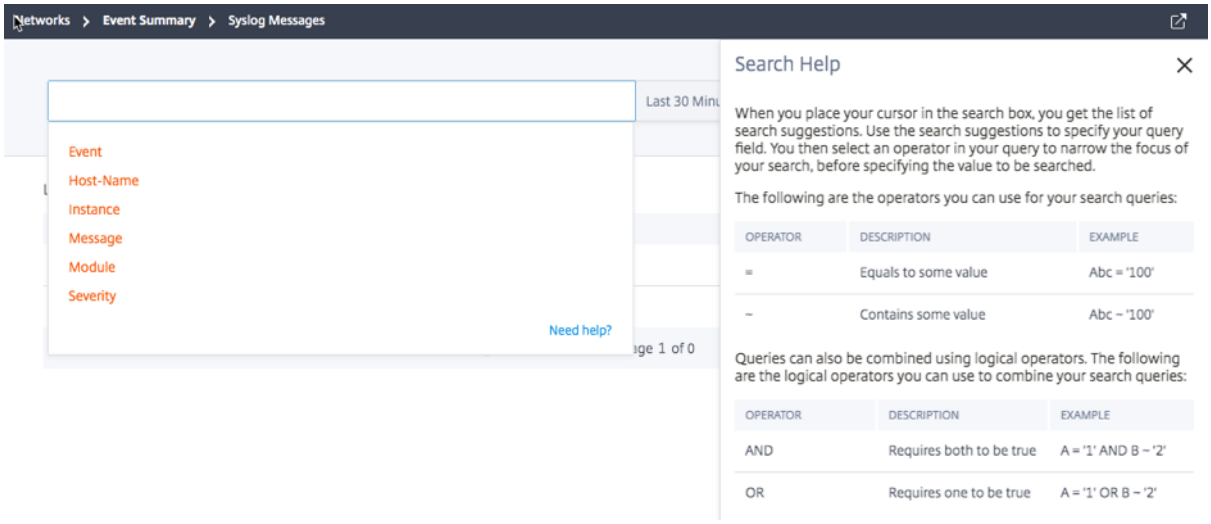
将 **ADM** 服务配置为 **syslog** 服务器

请按照以下步骤将 ADM 配置为 syslog 服务器：

1. 从 ADM GUI 中，导航到 基础架构 **>** 实例。
2. 选择要从中收集 syslog 消息并在 NetScaler ADM 中显示的 NetScaler 实例。
3. 在 **Select Action**（选择操作）列表中，选择 **Configure Syslog**（配置 Syslog）。
4. Click **Enable**。
5. 在 **Facility**（设施）下拉列表中，选择本地或用户级别的设施。
6. 为 syslog 消息选择所需的日志级别。
7. 单击确定。



这些步骤将配置 NetScaler 实例中的所有 syslog 命令，然后 NetScaler ADM 开始接收 syslog 消息。您可以通过导航到 **Infrastructure**（基础结构）**> Events**（事件）**> Syslog Messages**（**syslog** 消息）来查看消息。单击 **Need Help?**（需要帮助?）打开内置的搜索帮助。有关详细信息，请参阅 查看和导出 syslog 消息。



要导出日志消息，请单击右上角的箭头图标。

下一步，单击 **Export Now**（立即导出）或 **Schedule Export**（计划导出）。有关详细信息，请参阅 查看和导出 syslog 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，从而帮助您监视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“设置”**>** “**ADM** 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 基础架构 **>** 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，请导航到 应用程序 **>** 控制板，单击虚拟服务器，然后选择 审核日志。

NetScaler 池容量

February 6, 2024

NetScaler 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。将此池容量用于位于数据中心或公有云中的实例。当实例不再需要资源时，它会将分配的容量重新检查到公用池中。将释放的容量重用于需要资源的其他 ADC 实例。

您可以使用池化许可，通过确保为实例分配必要的带宽而不是超出其需要的带宽来最大限度地提高带宽利用率。在不影响流量的情况下，增加或减少在运行时分配给实例的带宽。使用池容量许可证，您可以自动执行实例 Provisioning。

NetScaler 池容量许可的工作原理

NetScaler 池容量包含以下组件：

- NetScaler 实例，可以分为以下几类：
  - 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 NetScaler ADM

零容量硬件

当通过 NetScaler 池容量进行管理时，MPX 和 SDX 实例被称为“零容量硬件”，因为这些实例在将资源从带宽和实例池中检出之前无法运行。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。

> 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。
> - 零容量许可证的安装与其他 NetScaler 本地许可证的工作方式相同。有关如何获取和安装零容量许可证的更多信息，请参阅 NetScaler 许可指南。

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，它将锁定到硬件，无法按需在 NetScaler 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 NetScaler 硬件实例。

运行 ADC 软件版本 11.1 build 54.14 或更高版本的 NetScaler MPX 实例和运行 11.1 build 58.13 或更高版本的 NetScaler SDX 实例支持 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 **NetScaler VPX** 实例

在以下虚拟机管理程序上运行 NetScaler 软件版本 11.1 Build 54.14 及更高版本的 NetScaler VPX 实例支持池容量：

- 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 NetScaler 软件版本 12.0 Build 51.24 及更高版本的 NetScaler VPX 实例支持池容量：

- Microsoft Hyper-V
- AWS
- Microsoft Azure
- Google Cloud

在以下虚拟机管理程序和云平台上运行 NetScaler 软件版本 13.0 和 13.1（所有版本）的 NetScaler VPX 实例支持池容量：

- VMware ESX 6.0
- Citrix Hypervisor
- Linux KVM
- Microsoft Hyper-V

- AWS
- Microsoft Azure
- Google Cloud

> 注意
>
> 要启用 NetScaler 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 NetScaler VPX 实例添加到 NetScaler 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。

独立的 **NetScaler CPX** 实例

部署在 Docker 主机上的 NetScaler 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 **NetScaler BLX** 实例

NetScaler BLX 实例支持池容量许可证。NetScaler BLX 实例不需要平台许可证。要处理流量，NetScaler 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 NetScaler 实例（物理和虚拟）可共享的总带宽。每个软件版本（标准、高级和高级）的带宽池由单独的池组成。给定的 NetScaler 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 NetScaler 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。

从池中签出后，许可证将解锁 MPX-Z、SDX-Z、VPX、CPX 和 BLX 实例的资源，包括 CPU/PE、SSL 内核、每秒数据包数和带宽。

> 注意
>
> SDX-Z 的管理服务不使用实例。

NetScaler ADM 许可证服务器

NetScaler 池容量使用配置为许可证服务器的 NetScaler 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 NetScaler ADM 软件在没有 ADM 许可证的情况下管理池容量许可证。

从带宽和实例池中签出许可证时，零容量硬件上的 NetScaler 外形规格和硬件型号决定

- NetScaler 实例在正常运行之前必须签出的最小带宽和实例数。
- NetScaler 可以签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 NetScaler 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 NetScaler 的最小带宽单位为 1 Gbps，则可以检出 1000 Gbps，但不能检出 200 Mbps 或 150.5 Gbps。最小带宽单位不同于最低带宽要求。NetScaler 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 NetScaler 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 NetScaler 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)	最小实例数	最大实例数	最低带宽单位
MPX 5900Z	10	1	不适用	不适用	1 Gbps
MPX 8900Z	30	5	不适用	不适用	1 Gbps
MPX 9100Z	30	10	不适用	不适用	1 Gbps
MPX 8900Z FIPS	33	5	不适用	不适用	1 Gbps
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

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
MPX 15000Z FIPS 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 16000Z 系列	200	30	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 8900Z	30	10	2	7	1 Gbps
SDX 9100Z	95	20	4	7	1 Gbps
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	20	10	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

产品系列	最大带宽 (Gbps)	最小带宽 (Gbps)	最小实例数	最大实例数	最低带宽单位
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 16000Z 系列	200	15	10	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)	最小实例数	最大实例数	最低带宽单位
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)	最小实例数	最大实例数	最低带宽单位
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
Google Cloud	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)	最小实例数	最大实例数	最低带宽单位
BLX	100	10	1	1	10 Mbps

表 **5.** 不同外形规格的许可证要求

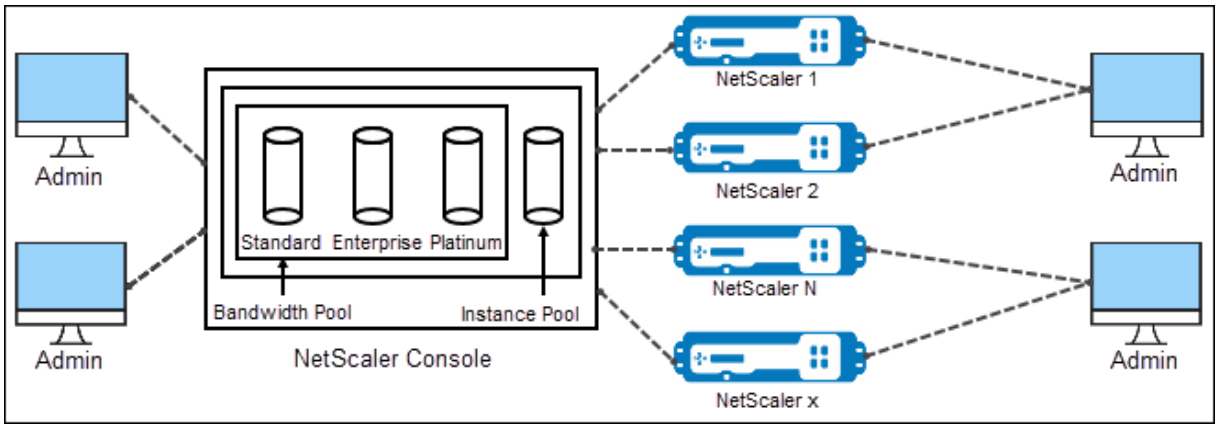
产品系列	零容量硬件购买	带宽和版本订阅	实例订阅
MPX	需要许可证	需要许可证	-
SDX	需要许可证	需要许可证	需要许可证
VPX	-	需要许可证	需要许可证
CPX	-	-	需要许可证
BLX	-	需要许可证	需要许可证

配置 NetScaler 池容量

February 6, 2024

要使用 ADC 池容量，请将 NetScaler 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）上载到许可证服务器。
- 根据需要将许可证池中的许可证分配给 NetScaler 实例。
- 根据实例的最小和最大容量查看 NetScaler 实例（MPX-Z /SDX-Z/VPX/CPX/BLX）的许可证。
- 为 NetScaler 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 NetScaler 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。配置了池化容量的 ADC 实例将显示以下状态之一：

- 最佳：实例以适当的许可证容量运行。
- 容量不匹配：实例的运行容量小于用户配置的容量。
- 宽限：实例正在使用宽限许可证运行。
- 宽限期和不匹配：实例在宽限期运行，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 ADM 与实例的 NITRO 通信无法正常工作。
- 未分配：未在实例中分配许可证。

步骤 **1-**在 **ADM** 中应用许可证

1. 在 NetScaler ADM 中，导航到 基础结构 **>** 池许可。
2. 在“许可证文件”部分中，选择“添加许可证文件”，然后选择以下选项之一：
   - 从本地计算机上载许可证文件。如果本地计算机上已存在许可证文件，则可以将其上载到 ADM。
   - **Use license access code**（使用许可证访问代码）。为您从 Citrix 购买的许可证指定许可证访问代码。然后，选择 获取许可证。然后选择完成。

   > 注意：
   >
   > 您可以随时通过许可证设置向 ADM 添加更多许可证。

3. 单击完成。

   许可证文件将添加到 ADM 中。许可证过期信息选项卡列出了 ADM 中存在的许可证以及剩余的到期天数。
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。

   有关如何向 NetScaler ADM 应用共享许可证的更多信息，请在此处观看相关视频。

步骤 **2-**将 **NetScaler ADM** 注册为许可证服务器

要将 ADM 注册为 NetScaler 实例的许可证服务器，请按照以下步骤之一进行操作：

- 使用图形用户界面
- 使用 CLI

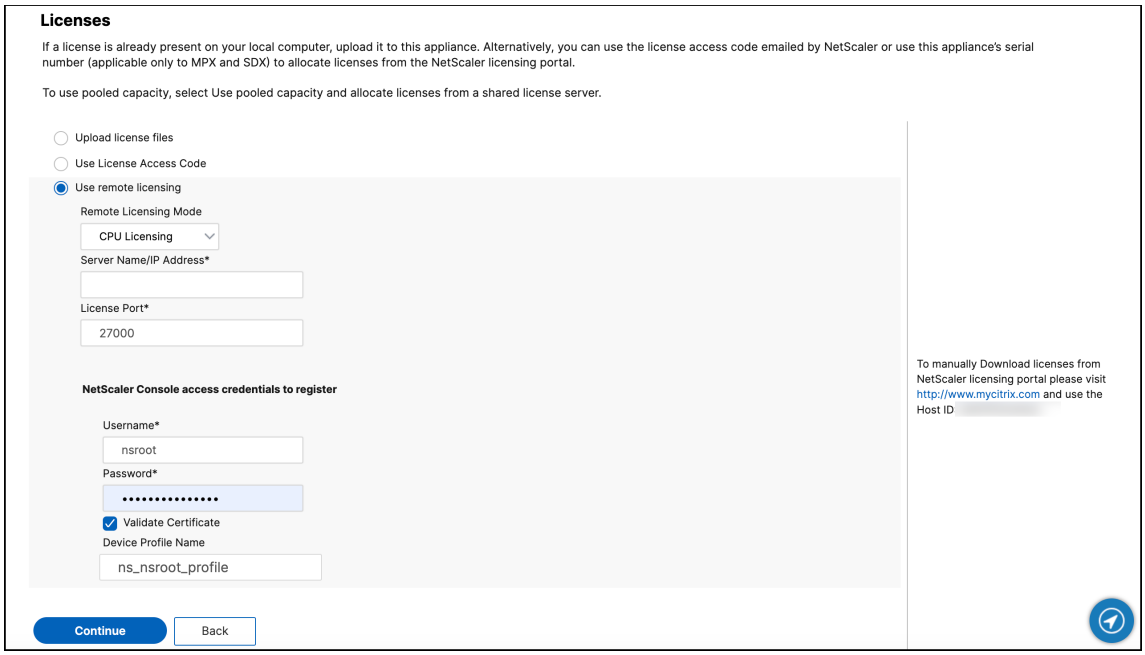
使用 **GUI** 将 **ADM** 注册为许可证服务器

在 ADC GUI 中，将 ADM 服务器注册为许可证服务器。

1. 登录到 NetScaler 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。

   > 对于 HA 部署，请使用浮动 IP。有关配置的更多信息，请参阅配置高可用性部署。
   >
   > 有关使用独立 ADM 或代理的部署，请参阅许可概述

6. 选择“向 **NetScaler ADM** 注册”。
7. 输入您的 ADM 凭据以向 NetScaler 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 NetScaler 中分配许可证。您可以稍后从 ADM GUI 更改或释放许可证分配。

   a) 单击 **Get Licenses**（获取许可证）。

> 重要：
>
> 如果您更改了许可证版本，请热重启实例。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 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> -licensemode <license-mode>
2 <!--NeedCopy-->
```

   有关更多信息，请参阅 许可概述。

3. 查看许可证服务器中可用的许可证带宽。

```
1 > sh ns licenseserverpool
2 <!--NeedCopy-->
```


此命令在添加许可证服务器时根据指定的许可证模式列出许可证。

示例 **1**：

如果指定的许可证模式为 CICO，则输出仅包含 CICO 许可证。

```
> add licenseserver [redacted] -licensemode CICO
 Done
> sh licenseserverpool
        VPX8000P Total                  : 1
        VPX8000P Available              : 1
```

示例 **2**：

如果指定的许可证模式为 Pooled，则输出仅包含池容量许可证。

```
> add licenseserver [redacted] -licensemode Pooled
 Done
> sh licenseserverpool
        Instance Total                  : 40
        Instance Available              : 38
        Standard Bandwidth Total        : 210.00 Gbps
        Standard Bandwidth Available    : 210.00 Gbps
        Enterprise Bandwidth Total      : 50.00 Gbps
        Enterprise Bandwidth Available  : 50.00 Gbps
        Platinum Bandwidth Total        : 210.00 Gbps
        Platinum Bandwidth Available    : 205.00 Gbps
```

示例 **3**：

如果指定的许可证模式为 vCPU，则输出仅包含虚拟 CPU 许可证。

```
> add licenseserver [redacted] -licensemode vCPU
 Done
> sh licenseserverpool
        Standard CPU Total              : 100
        Standard CPU Available          : 100
        Enterprise CPU Total            : 100
        Enterprise CPU Available        : 100
        Platinum CPU Total              : 25
        Platinum CPU Available          : 20
```

要同时查看所有许可证，请运行以下命令：

```
1 > sh ns licenseserverpool -getallLicenses
2 <!--NeedCopy-->
```

输出示例：


```
> sh licenseserverpool -getallLicenses
        Instance Total                      : 40
        Instance Available                  : 33
        Standard Bandwidth Total            : 210.00 Gbps
        Standard Bandwidth Available        : 210.00 Gbps
        Enterprise Bandwidth Total          : 50.00 Gbps
        Enterprise Bandwidth Available      : 50.00 Gbps
        Platinum Bandwidth Total            : 210.00 Gbps
        Platinum Bandwidth Available        : 205.00 Gbps
        VPX8000P Total                      : 1
        VPX8000P Available                  : 1
        Standard CPU Total                  : 100
        Standard CPU Available              : 100
        Enterprise CPU Total                : 100
        Enterprise CPU Available            : 100
        Platinum CPU Total                  : 25
        Platinum CPU Available              : 20
```

4. 从所需的许可证版本中分配许可证带宽：

```
> set ns capacity -unit <specify-mbps-or-gbps> -bandwidth <specify
    -amount-license-bandwidth> -edition <specify-license-edition>
<!--NeedCopy-->
```

许可证版本可以是 **Standard**、**Enterprise** 或 **Platinum**。

> 重要信息：如果您更改许可证版本，则“
>
> 热”重新启动实例。
>
> ```
> reboot -w
> ```
>
> 配置更改在您重新启动实例后才会生效。

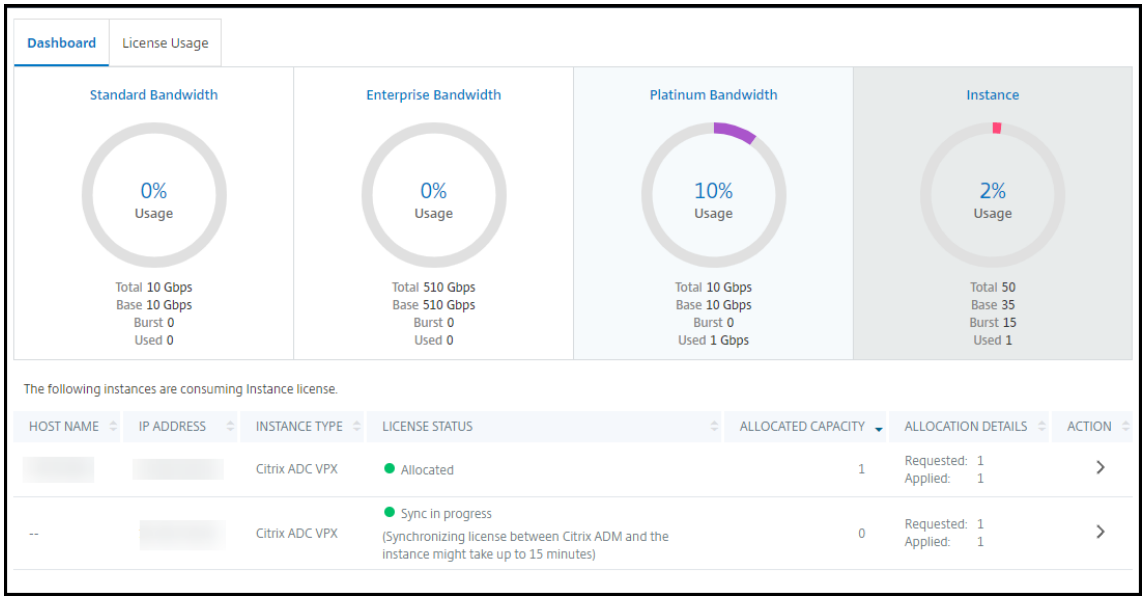
步骤 **3-**将池许可证分配给 **ADC** 实例

要从 ADM GUI 分配池容量许可证，请执行以下操作：

1. 登录到 NetScaler ADM。
2. 导航到 基础架构 **>** 许可证 **>** 带宽许可证 **>** 池容量。

   仅当您将 FIPS 实例许可证上载到 ADM 时，才会显示 FIPS 实例容量。
3. 单击要管理的许可证池。

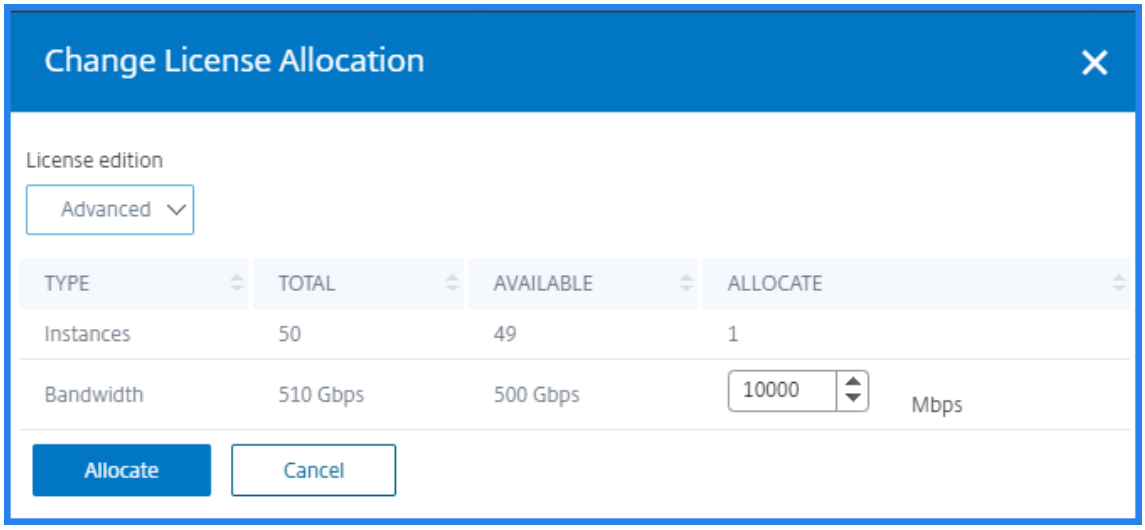
   > 注意：
   >
   > “分配的容量”字段不会立即反映更改的带宽。带宽更改在 ADC 热重启后生效。
   >
   > 在 分配详细信息中，当您更改实例的带宽分配时，会更新 请求 和已 应用 字段。
4. 单击 **>** 按钮，从可用实例列表中选择一个 ADC 实例。



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 NetScaler 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. 将出现一个弹出窗口，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。做出选择后，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分配的许可证版本。



> 注意
>
> 如果您更改了许可版本，请热重启实例。

有关如何更改带宽分配的更多信息，请在此处观看相关视频。

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：

- NetScaler 实例
- NetScaler VPX 实例
- NetScaler 高可用性对

NetScaler MPX 实例

MPX-Z 是支持共用容量的 NetScaler MPX 设备。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：

- 从本地计算机上载许可证文件。
- 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，则会禁用池容量功能。实例许可证将释放到许可证服务器。

您可以在不重新启动的情况下动态修改 MPX-Z 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 当您重启实例时，它会自动检查其配置容量所需的池化许可证。

NetScaler VPX 实例

启用了池容量的 NetScaler VPX 实例可以从带宽池（高级版/高级版/标准版）中签出许可证。您可以使用 ADC GUI 从许可证服务器签出许可证。

您可以在不重新启动的情况下动态修改 VPX 实例的带宽。仅当您要更改许可证版本时才需要重新启动。

> 注意：
>
> 重启实例时，配置的池容量许可证将自动从 ADM 服务器签出。

NetScaler 高可用性对

在开始之前，请确保将 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。

对于在高可用性模式下配置的 ADC 实例，您必须在高可用性对的每个节点上配置池容量。对于主节点和辅助节点，都需要分配相同容量的许可证。例如，如果您希望高可用性对中的每个实例提供 1 Gbps 的容量，则需要公用池的两倍容量 (2 Gbps)。然后，您可以为每个节点分配 1 Gbps 的容量。

要将池许可证分配给对中的每个节点，请按照 将池许可证分配给 ADC 实例中给出的步骤进行操作。首先将许可证分配给第一个节点，然后重复相同的步骤将许可证分配给第二个节点。

仅将 **ADM** 服务器配置为池许可证服务器

February 6, 2024

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、监视和分析功能。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。

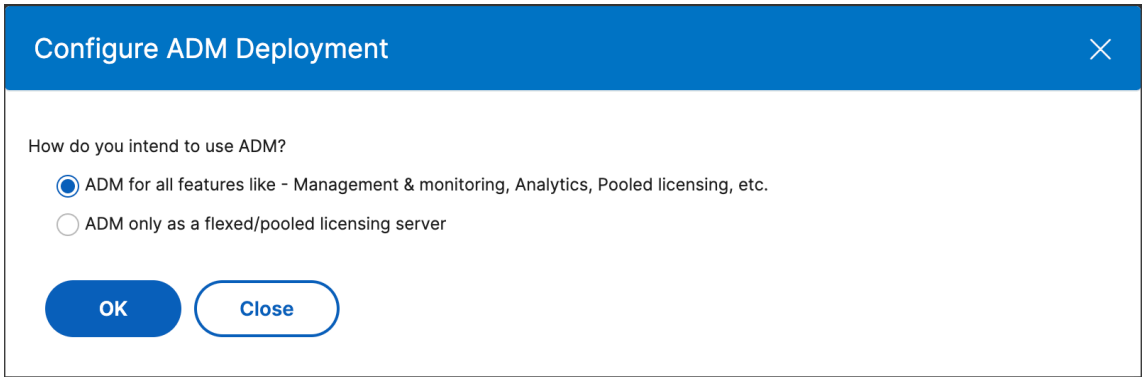
本文档介绍如何仅将 ADM 服务器配置为池许可证服务器。

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 **Settings**（设置）**> Administration**（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 基础架构 > 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 NetScaler ADM 上配置访问策略。

将 **NetScaler VPX** 中的永久许可证升级到 **NetScaler** 池容量

February 6, 2024

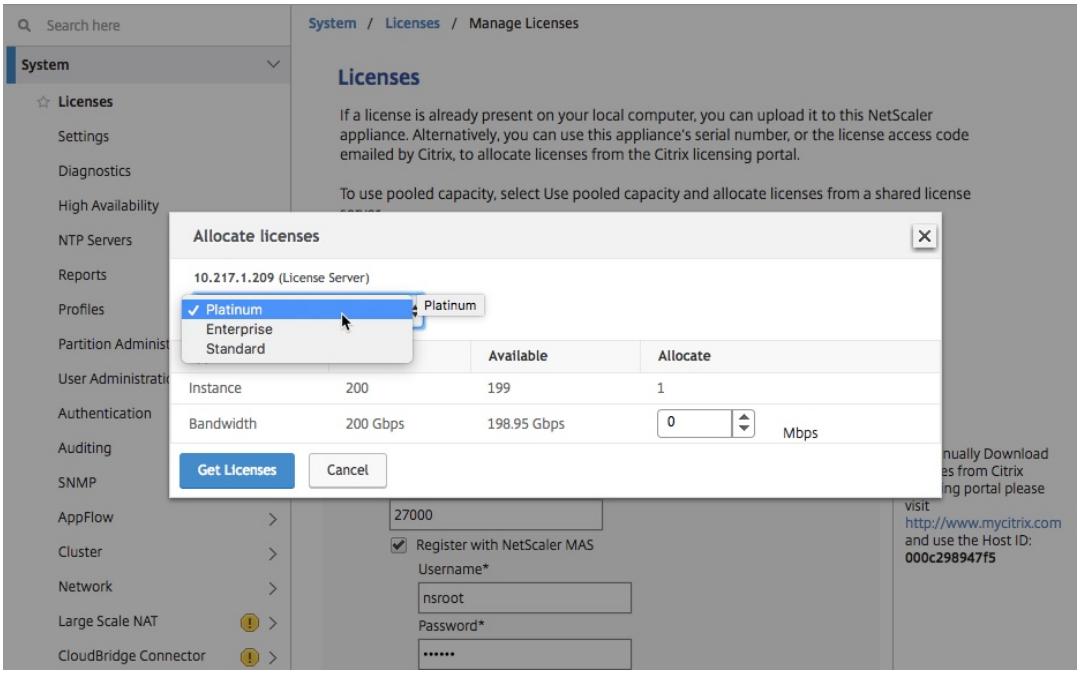
具有永久许可证的 NetScaler VPX 实例可以升级到 ADC 池容量许可证。升级到池容量许可证后，您可以按需将许可证池中的许可证分配给 VPX 实例。您还可以为在高可用性模式下配置的 ADC 实例配置池容量许可证。要为处于高可用性模式的 VPX 实例配置池容量许可证，请参阅将 NetScaler VPX 高可用性对中的永久许可证升级为 NetScaler 池容量。

必备条件

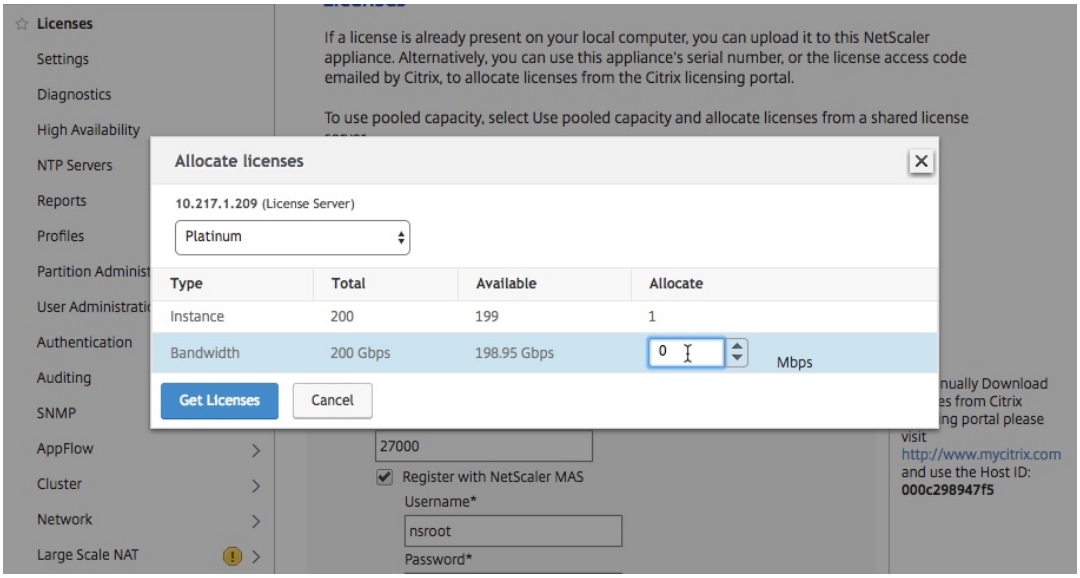
确保将 VPX 实例升级到版本 12.0.56.x。

要升级到 **NetScaler** 池容量，请执行以下操作：

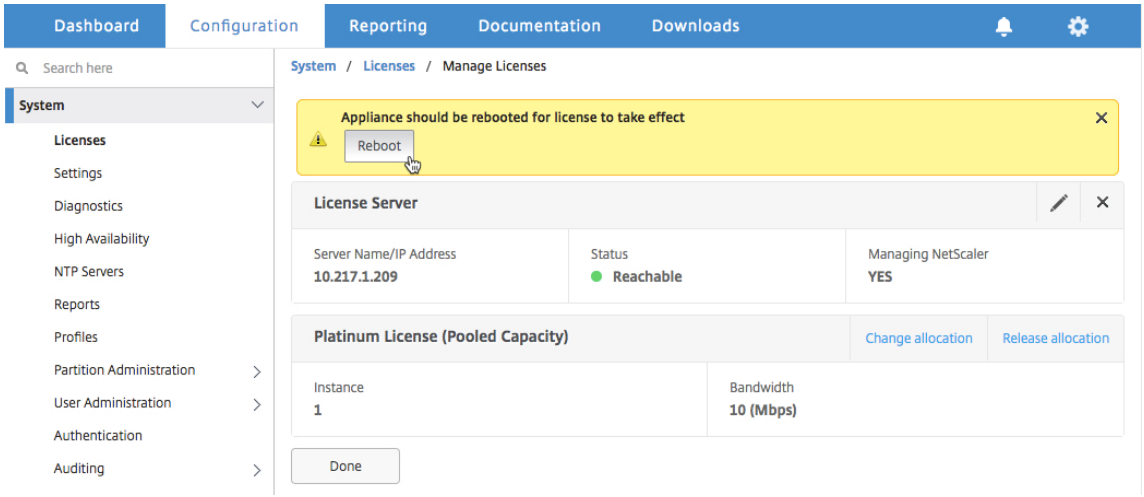
1. 在 Web 浏览器中，键入 VPX 实例的 IP 地址，如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 在“配置”选项卡上，导航到“系统”**>**“许可证”，然后单击“管理许可证”。
5. 在“许可证”页面上，单击“添加新许可证”。
6. 在“许可证”页面上，选择“使用远程许 可”，然后执行以下操作：
    a) 在 远程授权模式 下拉列表中，选择 池授权。
    b) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器的详细信息。
    c) 如果要通过 **ADM** 管理实例的池许可证，请确保选中向 **NetScaler ADM** 注册 复选框并输入 NetScaler ADM 凭据。
    d) 单击继续。
7. 在分配许可证中，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 NetScaler 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. VPX 实例重启后，登录该实例。在“欢迎 使用”页面上，单击“继续”。

    许可 证页面显示在 NetScaler 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 **NetScaler VPX** 高可用性对中的永久许可证升级到 **NetScaler** 池容量

对于配置为高可用性模式的 VPX 实例，您必须在 HA 对中的主实例和辅助实例上配置池容量。对于主实例和辅助实例，您需要分配容量相同的许可证。例如，如果您希望高可用性对中的每个实例提供 1 Gbps 的容量，则需要公用池的两倍容量 (2 Gbps)。然后，您可以为高可用性对中的主实例和辅助实例各分配 1 Gbps 的容量。

要将现有的 **NetScaler VPX HA** 设置升级到 **NetScaler** 池容量，请执行以下操作：

1. 登录辅助 VPX（节点 2）实例。在 Web 浏览器中，键入 NetScaler 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. 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. 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。

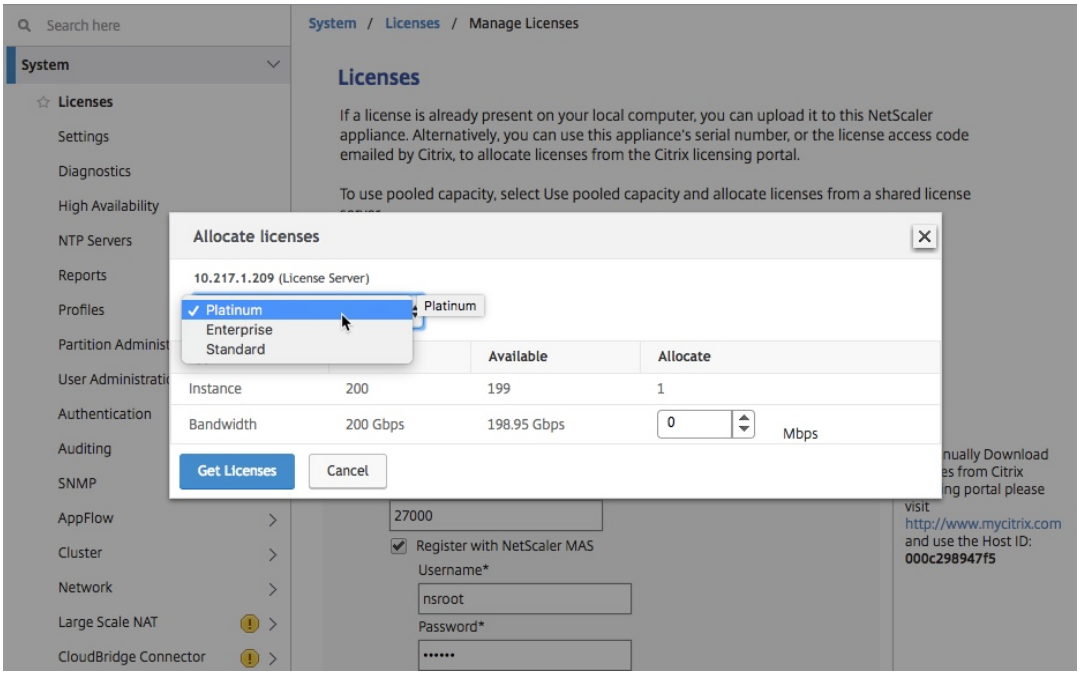
    b) 在“服务器名称 **/IP** 地址”字段中，输入许可证服务器的详细信息。

c) 如果要通过 **NetScaler ADM** 管理实例的池许可证，请确保选中向 **NetScaler ADM** 注册 复选框并输入 ADM 凭据。

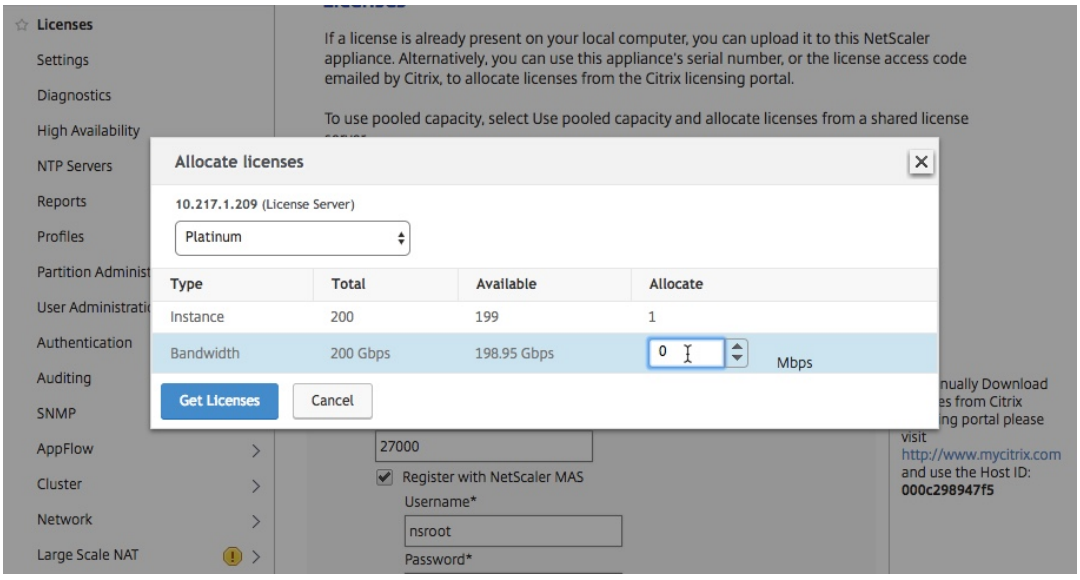
d) 单击继续。

7. 在分配许可证中，执行以下操作：

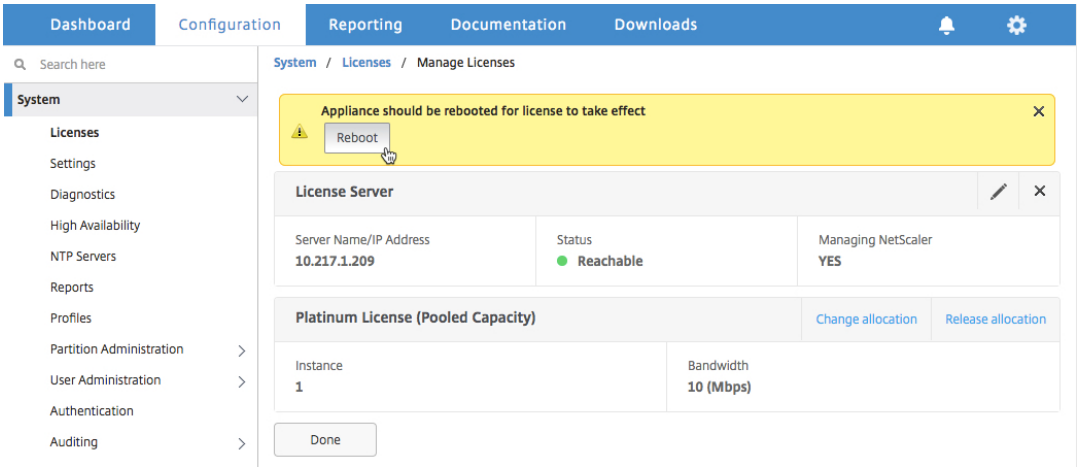
a) 从下拉列表中选择许可证版本。



b) 从“分配”菜单将带宽分配 给 NetScaler 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启实例。



8. 在“确认”对话框中，单击“是”。

   VPX 实例将重新启动。

   出现提示时，单击“重新启动”以重新启动设备。使用新许可证启动并运行设备后，键入 `force ha failover` 强制进行故障转移。此故障切换可确保 HA 对处于良好状态。

9. 故障转移后，登录到新的辅助 VPX 实例（节点 1），然后重复相同的过程，将新的辅助 VPX 实例添加到池中。

   如果要将 HA 对中的主实例和辅助实例更改为原始 HA 对配置，请强制进行故障转移。在 HA 对中的任何实例上运行以下命令：

   ```
   1   > force ha failover
   2 <!--NeedCopy-->
   ```

10. 要验证 VPX 实例是否已升级到池容量许可证，请登录主实例和辅助实例并完成以下步骤。

    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 **NetScaler MPX** 中的永久许可证升级到 **NetScaler** 池容量

February 6, 2024

具有永久许可证的 NetScaler MPX 装置可升级到 NetScaler 池容量许可证。升级到 NetScaler 池容量许可证允许您按需将许可证池中的许可证分配给 NetScaler 设备。您还可以为在高可用性模式下配置的 NetScaler 实例配置 NetScaler 池容量许可证。要在高可用性模式下为 NetScaler MPX 实例配置 NetScaler 池容量 许可证，请参阅将 NetScaler MPX 高可用性对中的永久许可证升级为 NetScaler 池容量。

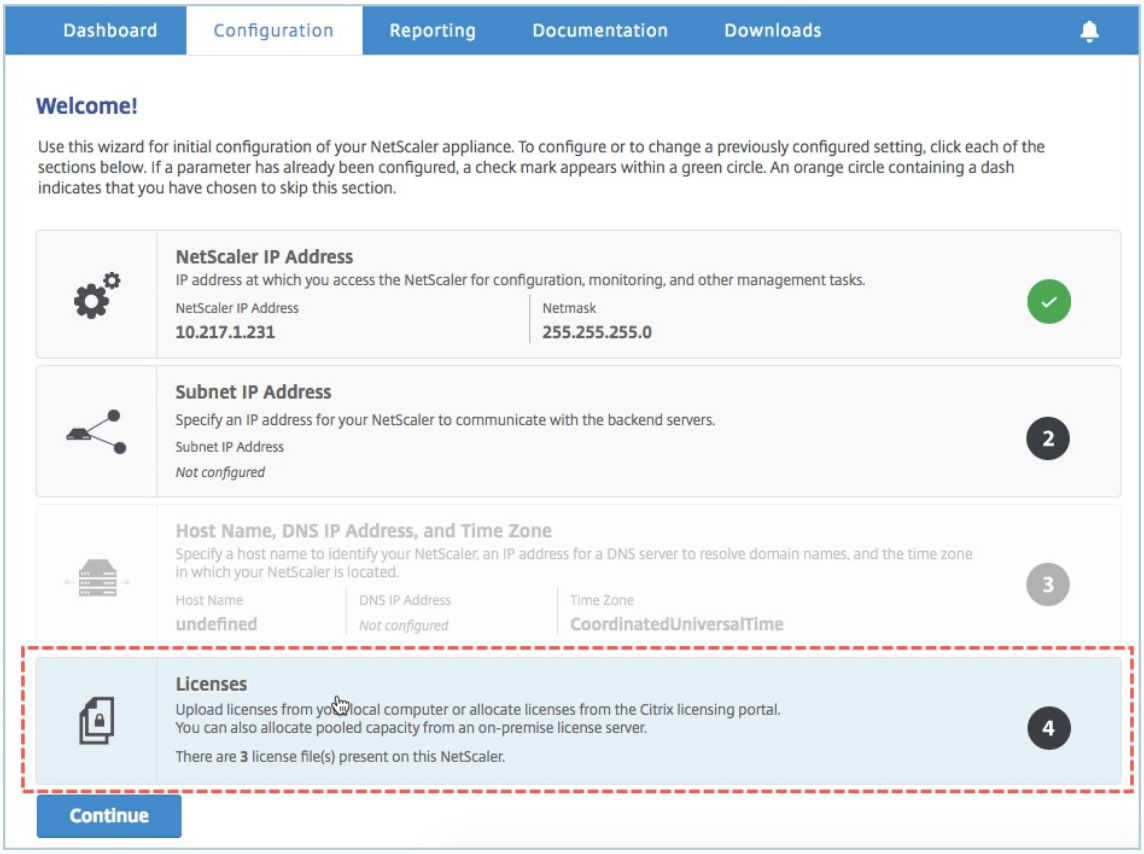
> 注意
>
> 从永久许可证转换为池容量许可证是许可证授权的单向过程。您无法将池容量许可证恢复为永久许可证。
> 重要
>
> 要将 NetScaler MPX 设备升级到 NetScaler 池容量许可证，您需要将 MPX-Z 许可证上载到该设备。

要升级到 **NetScaler** 池容量，请执行以下操作：

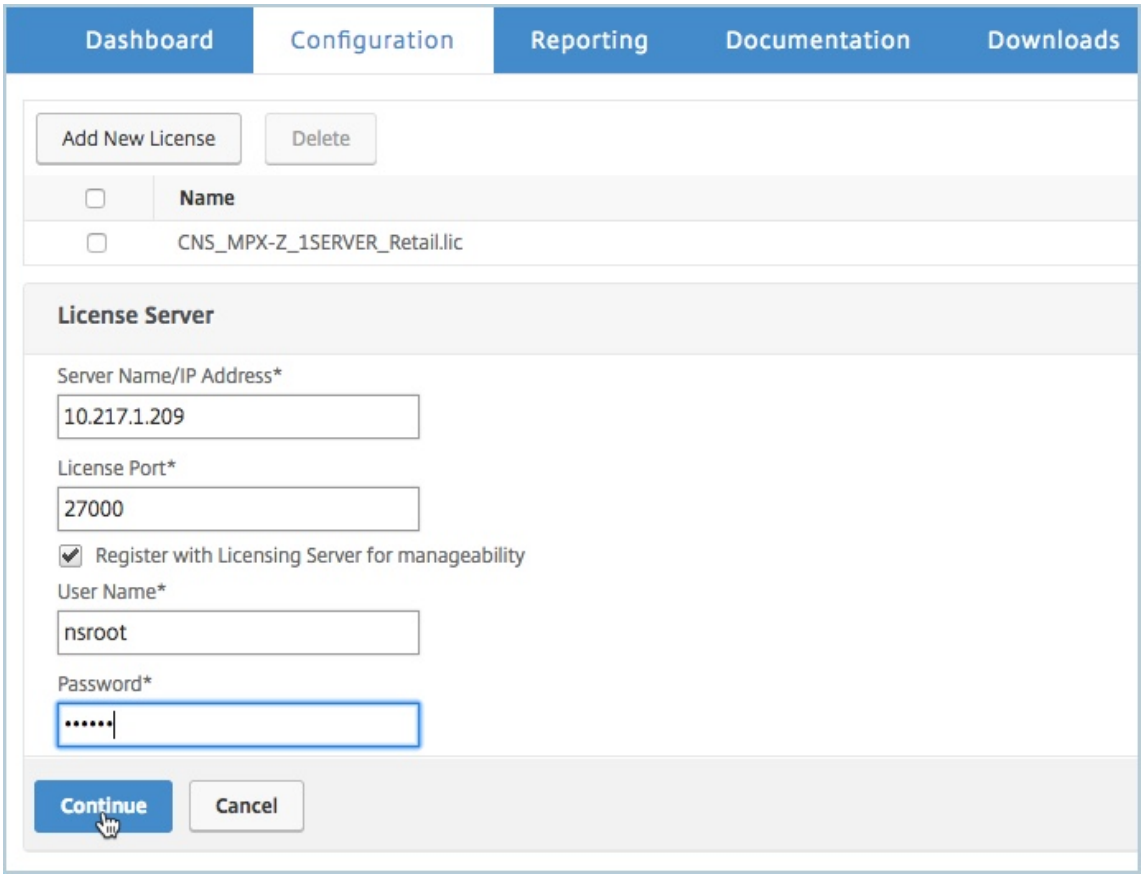
1. 在 Web 浏览器中，键入 NetScaler 设备的 IP 地址，例如 http://192.168.100.1。
2. 在“用户名”和“密码”字段中，键入管理员凭据。
3. 在“欢迎 使用”页面上，单击“继续”。
4. 上载零容量许可证（MPX-Z 许可证）。在配置选项卡上，导航到 系统 > 许可证。
5. 在详细信息窗格中，单击“管理许可证”，单击“添加 新许可证”。
6. 在“许可证”页面中，选择“上载许可证文件”，然后单击“浏览”以从本地计算机中选择零容量许可证。
7. 上载许可证后，单击 重新启动 以重新启动设备。

   > 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。
   >
   > 如果在升级之前在设备上启用了“仅限安全访问”选项，则无法使用 HTTPS 通过 NetScaler ADM GUI 连接到设备。

8. 在“确 认”页面上，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。

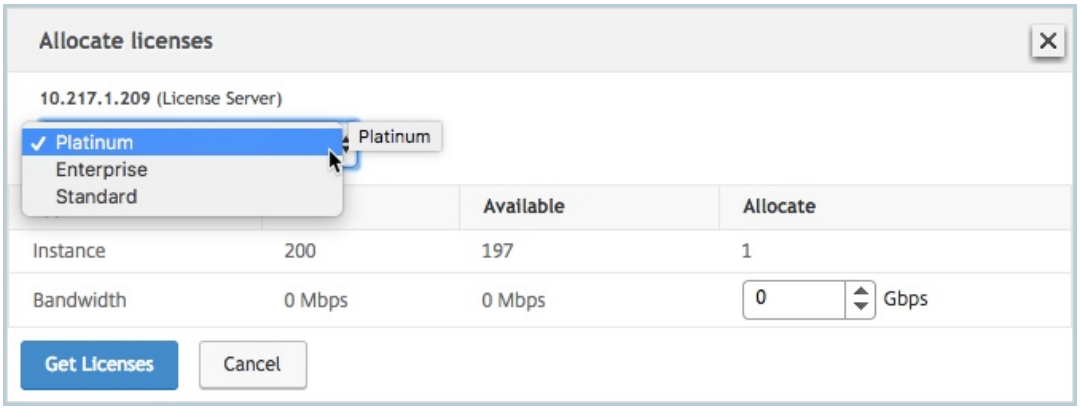
b) 在 许可证端口 字段中，输入许可证服务器端口。默认值：27000。

c) 如果要通过 NetScaler ADM 管理实例的池许可证，请选中向 许可服务器注册以实现可管理性 复选框，然后输入 ADM 凭据。

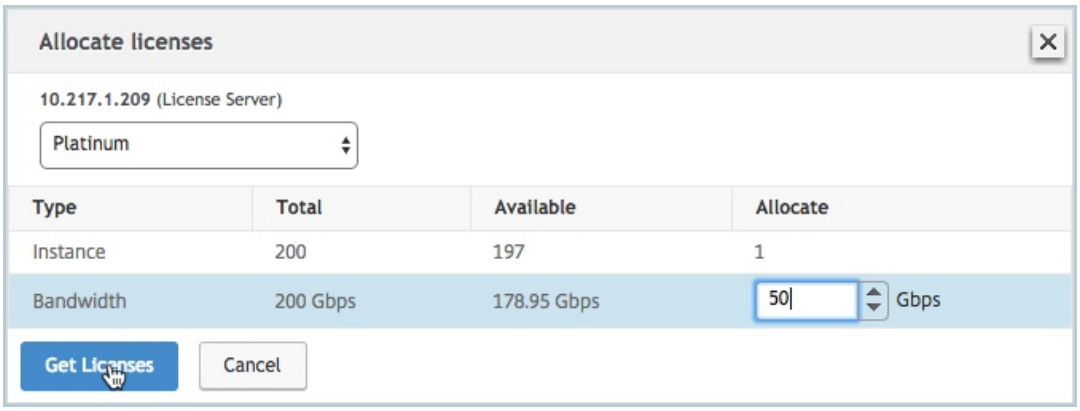
d) 单击继续。

12. 在分配许可证中，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 NetScaler 装置，然后单击“获取许可证”。



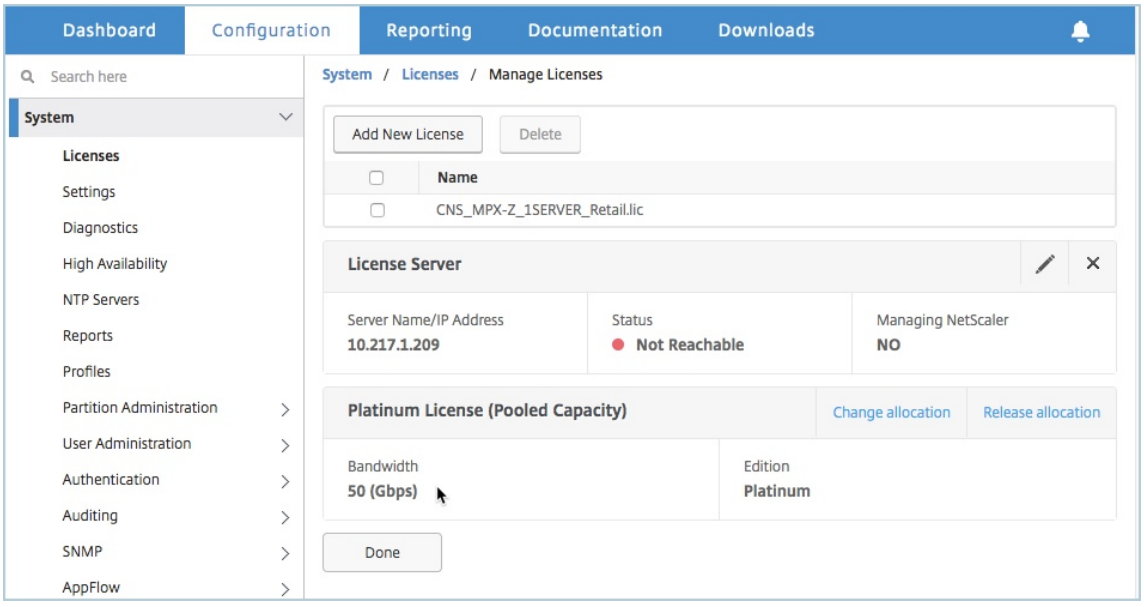
c) 出现提示时，单击 重新启动 以重新启动装置。

13. NetScaler MPX 设备重新启动后，登录 NetScaler MPX 设备。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 **NetScaler MPX** 高可用性对中的永久许可证升级到 **NetScaler** 池容量

对于在高可用性模式下配置的 MPX 设备，您必须在 HA 对中的主 ADC 实例和辅助 ADC 实例上配置池容量。向 HA 对中的主 NetScaler 实例和辅助 NetScaler 实例分配相同容量的许可证。例如，如果您希望高可用性对中的每个实例提供 1 Gbps 的容量，则需要从公用池中分配 2 Gbps 的容量。借助 2 Gbps 的容量，您可以为高可用性对中的主要 NetScaler 实例和辅助 NetScaler 实例各分配 1 Gbps。

> 重要
>
> 要升级 NetScaler MPX 设备以使用 NetScaler 池容量许可证，您需要将 MPX-Z 上载到该设备。

必备条件

确保将 MPX-Z 许可证上载到 HA 对中的主实例和辅助实例。

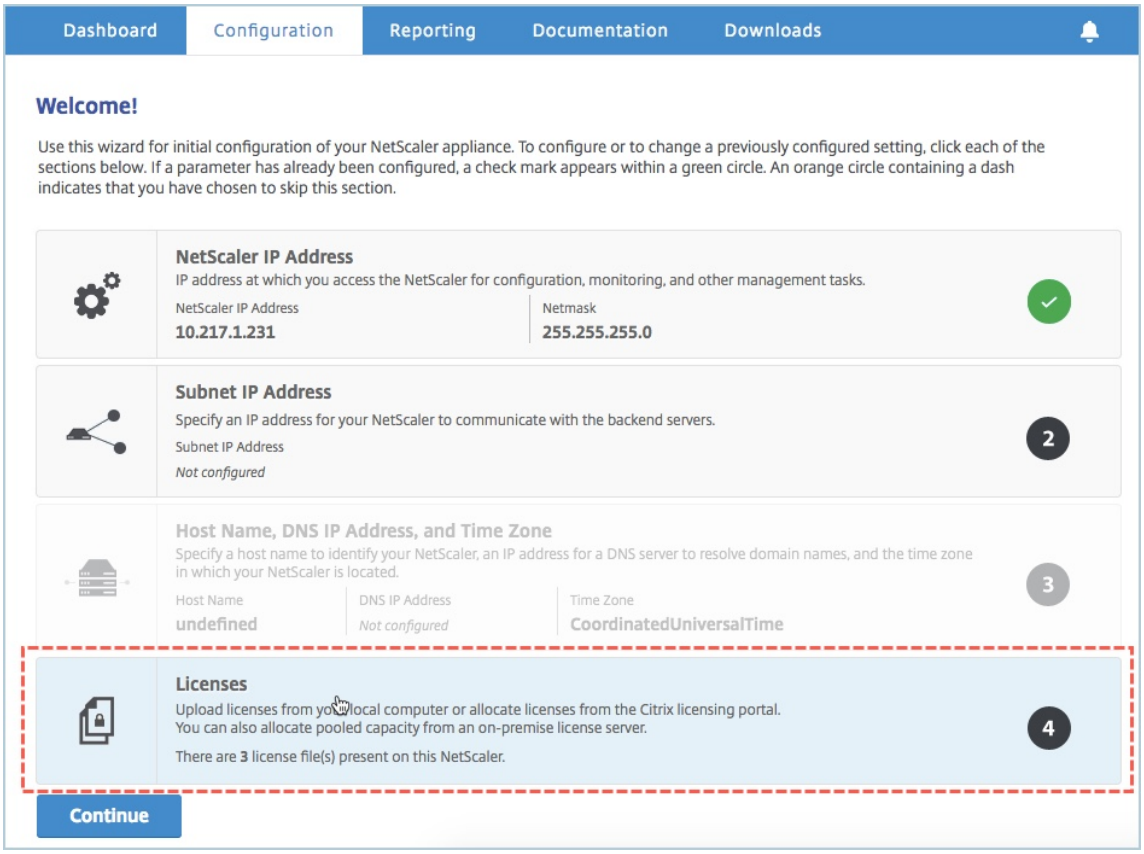
要将 **MPX-Z** 许可证上载到 **HA** 对中的 **NetScaler MPX** 实例，请执行以下操作：

1. 在 Web 浏览器中，键入设备的 IP 地址，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. 上载零容量许可证（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“上载许可证文件”，然后单击“浏览”以从本地计算机中选择零容量许可证。

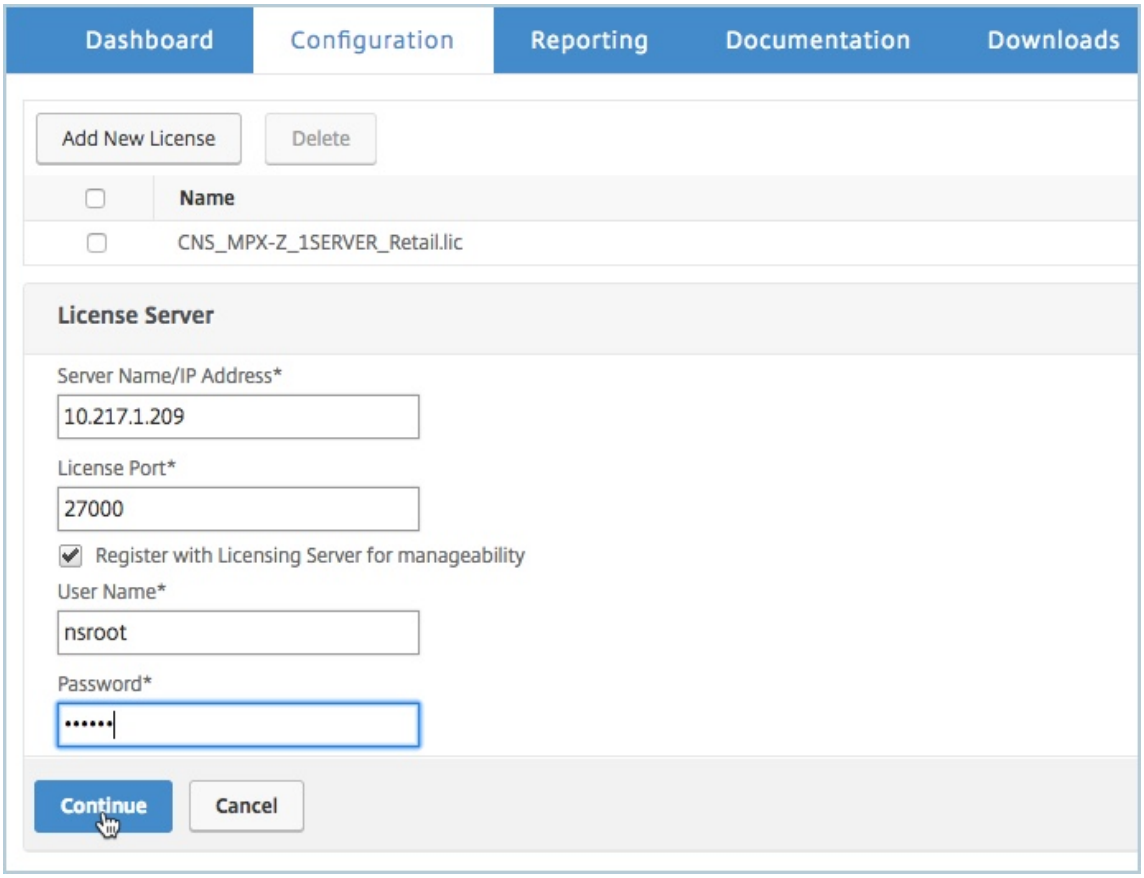
   上载许可证后，系统会提示您重新启动设备。
7. 单击“重新启 动”以重新启动装置。
8. 在“确 认”页面上，单击“是”。

要将现有的 **HA** 设置升级到 **NetScaler** 池容量，请执行以下操作：

1. 登录到辅助 NetScaler MPX 实例。在 Web 浏览器中，键入 NetScaler 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”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。

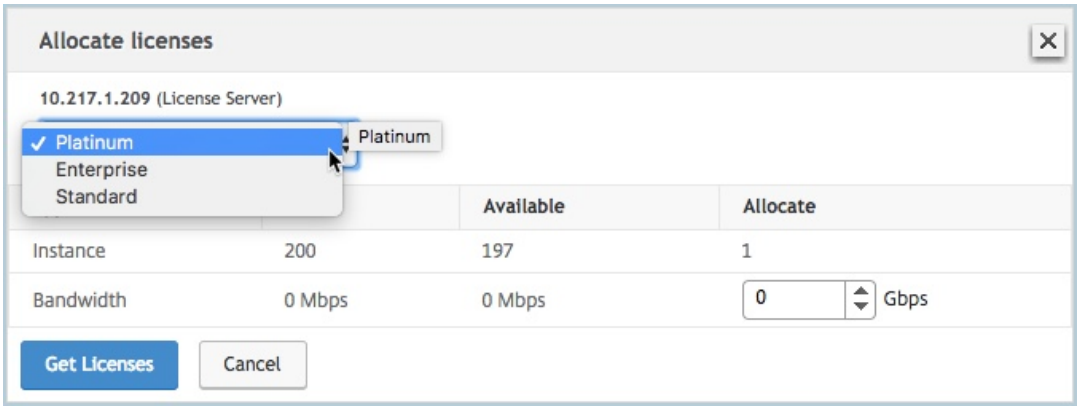
b) 在 许可证端口 字段中，输入许可证服务器端口。默认值：27000。

c) 如果您想通过 NetScaler ADM 管理实例的池许可证，请选中“注册许可服务器以获得可管理性”复选框并输入 **ADM** 凭 据。

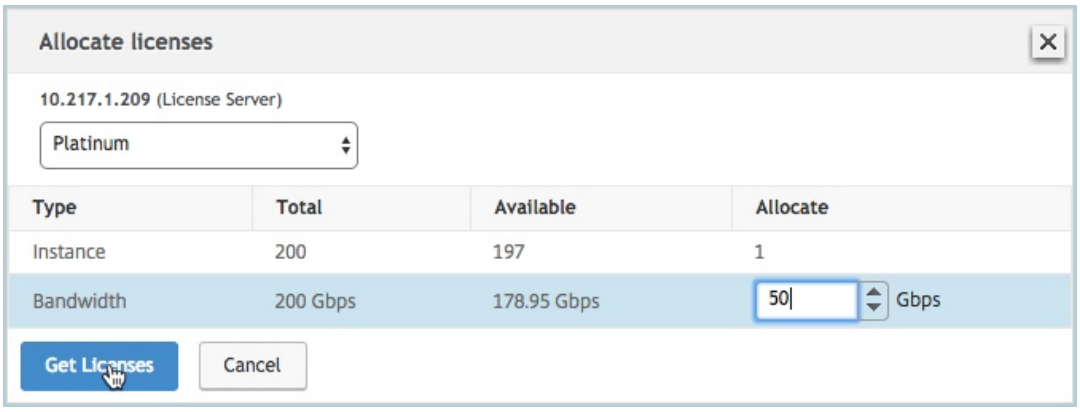
d) 单击继续。

5. 在分配许可证中，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 NetScaler 装置，然后单击“获取许可证”。



c) 出现提示时，单击“重新启动”以重新启动设备。使用新许可证启动并运行设备后，键入 `force ha failover` 强制进行故障转移。此故障切换可确保 HA 对处于良好状态。

6. 登录现有主 NetScaler 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 NetScaler 设备的 IP 地址，例如 http://192.168.100.1。

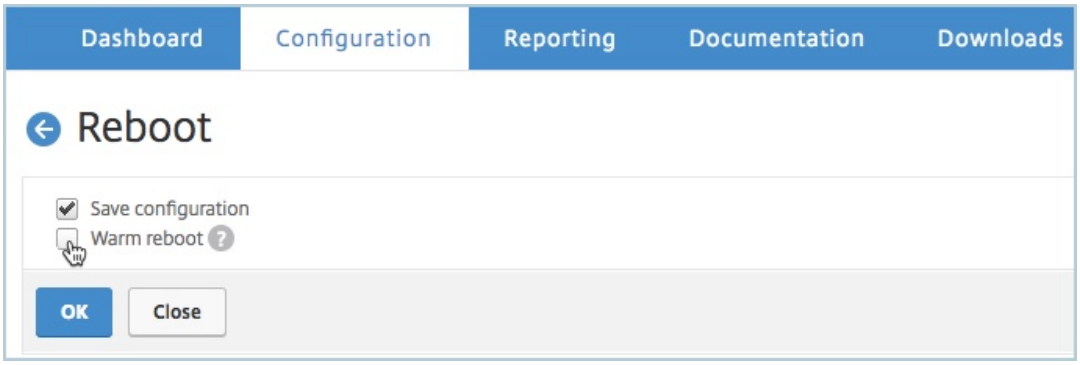
b) 在“用户名”和“密码”字段中，键入管理员凭据。

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 NetScaler MPX 装置重新启动后，它将成为 HA 对中的辅助 NetScaler MPX 装置。如果要将 HA 对中的主实例和辅助实例更改为原始 HA 对配置，请强制进行故障转移。在 HA 对中的任何实例上运行以下命令：

```
1 > force ha failover
2 <!--NeedCopy-->
```


将 NetScaler SDX 中的永久许可证升级到 NetScaler 池容量

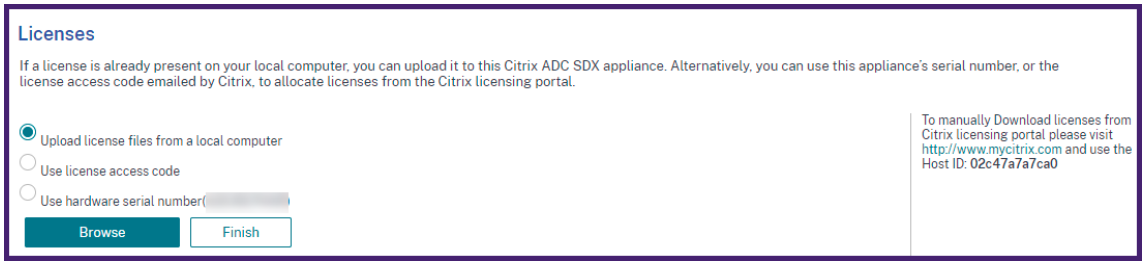
February 6, 2024

具有永久许可证的 NetScaler SDX 设备可以升级到 NetScaler 池容量许可证。升级到 NetScaler 池容量许可证允许您按需将许可证池中的许可证分配给 NetScaler 设备。您还可以为在高可用性模式下配置的 NetScaler 实例配置 ADC 池容量许可证。

> 重要
>
> 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。
>
> - 要将 SDX 设备升级到 NetScaler 池容量许可证，必须将 SDX-Z 许可证上载到设备。
> - 确保您有权在 ADM 中添加 ADC 实例。
> - 为确保不影响当前许可证，客户必须分配与永久许可证中可用相同数量的实例和带宽。

要升级到 **NetScaler** 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. 上载零容量许可证。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“从本地计算机上上载许可证文件”，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。

> 注意
>
> 要删除旧的许可证文件，您不必重新启动 SDX 设备，这样就不会出现停机时间。如需更多帮助，请联系 NetScaler 支持团队。

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。

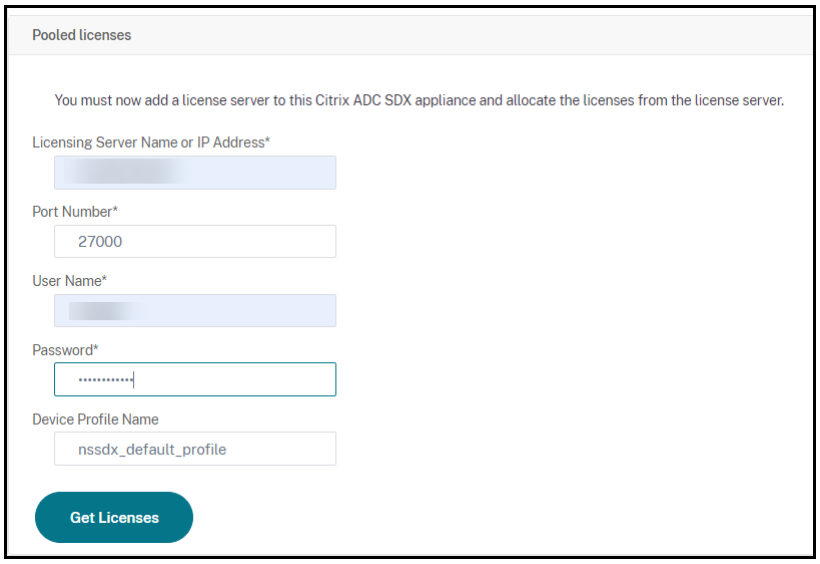
- 如果要将 ADM 服务器配置为许可证服务器，请指定 ADM 服务器的 IP 地址。
- 如果使用代理与 ADM 服务器通信，请指定 ADM 代理的 IP 地址。

b) 在 端口号 字段中，输入许可证服务器端口。默认值：27000。

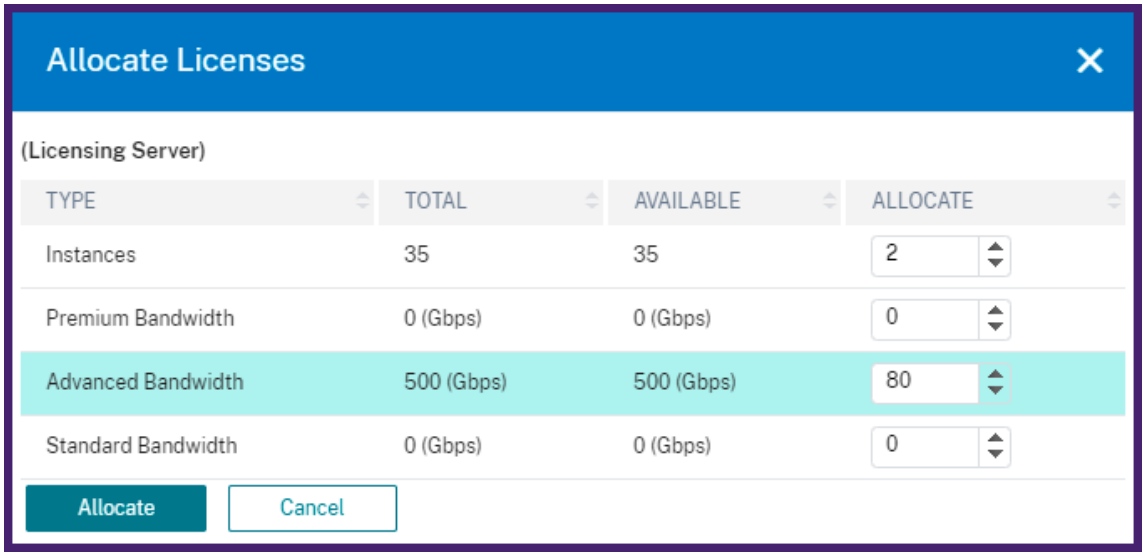
c) 指定许可服务器的 用户名 和 密码。

- 对于 ADM 服务器，输入管理员凭据。
- 对于 ADM 代理，输入代理凭据。

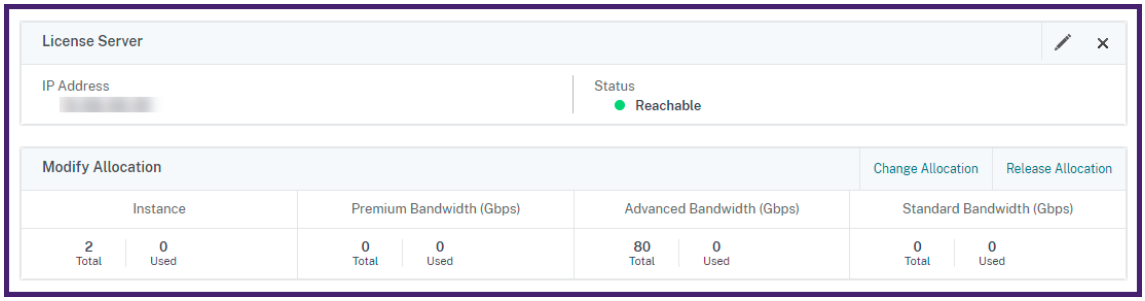
d) 单击 **Get Licenses**（获取许可证）。



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。

NetScaler 群集模式下的 NetScaler 池容量

February 6, 2024

您可以在配置为群集的 NetScaler 实例上配置 NetScaler 池容量。以下是在群集模式下在 NetScaler 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群集。
- 所有实例必须以相同的带宽运行。
- 所有实例都检查了来自同一 NetScaler Application Delivery Management (ADM) 的池化容量。
- 除非新实例的容量和 NetScaler ADM 配置与群集中现有实例的容量和 NetScaler ADM 配置相同，否则无法将新实例添加到现有 NetScaler 群集中。

来自 NetScaler 群集的任何容量检出都会为所有群集节点分配相同的容量，签出带宽 = 提供的带宽 x 节点数量。

例如，如果从 NetScaler 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，则群集将继续使用剩余实例的容量处理流量。

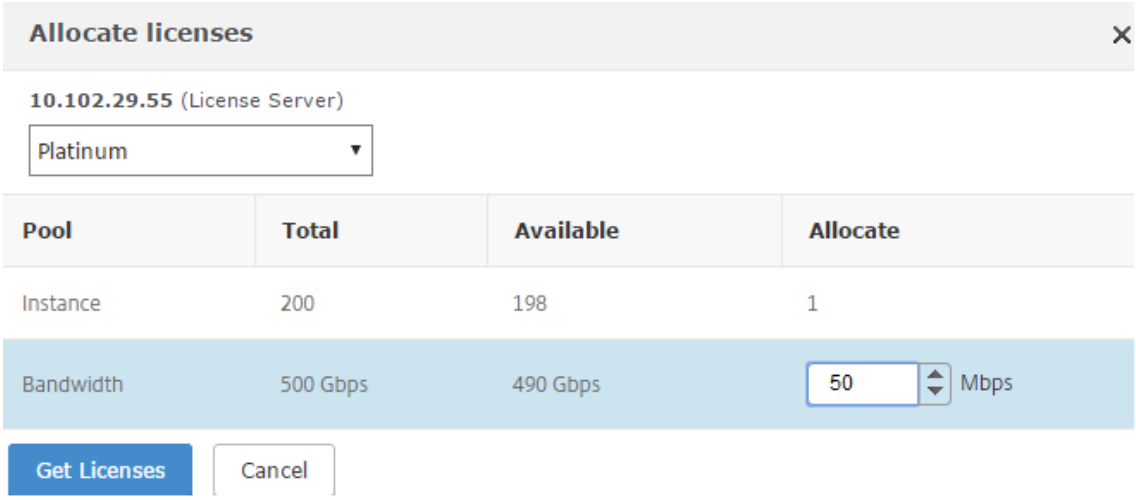
为 ADC 群集分配 ADC 池容量

分别为每个群集节点分配许可证。因为在群集节点之间传播和同步许可证的命令已禁用。

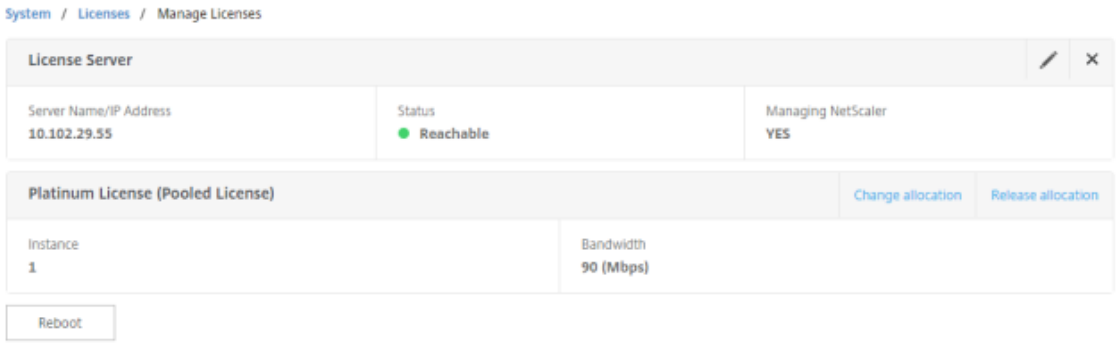
在每个群集节点上重复以下步骤：

1. 在网络浏览器中，键入 NetScaler 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“使用池化许可”。
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. 如果您想通过 NetScaler ADM 管理实例的池许可证，请选中“向 NetScaler ADM 注册以获得可管理性”复选框并输入 **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。

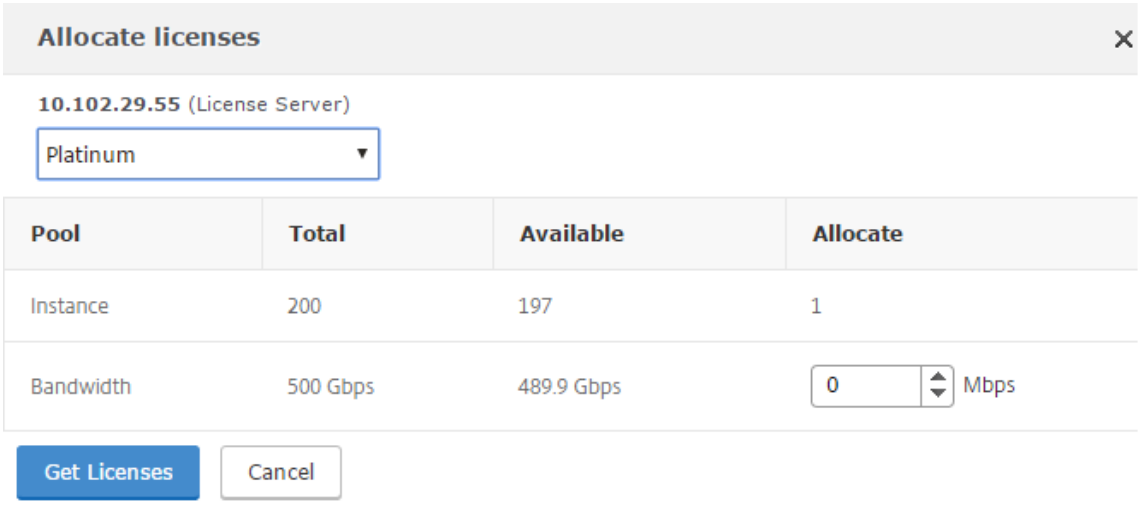


7. 您可以通过选择“更改分配”或“发布分配”来 更改 或 释放许可证分配。



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 NetScaler 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** 为 **ADC** 群集分配 **ADC** 池容量

分别为每个群集节点分配许可证。因为在群集节点之间传播和同步许可证的命令已禁用。

在每个群集节点上重复以下步骤：

1. 在 SSH 客户端中，输入 NetScaler 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 NetScaler 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

February 6, 2024

许可证服务器会持续监视启用了 NetScaler 池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。

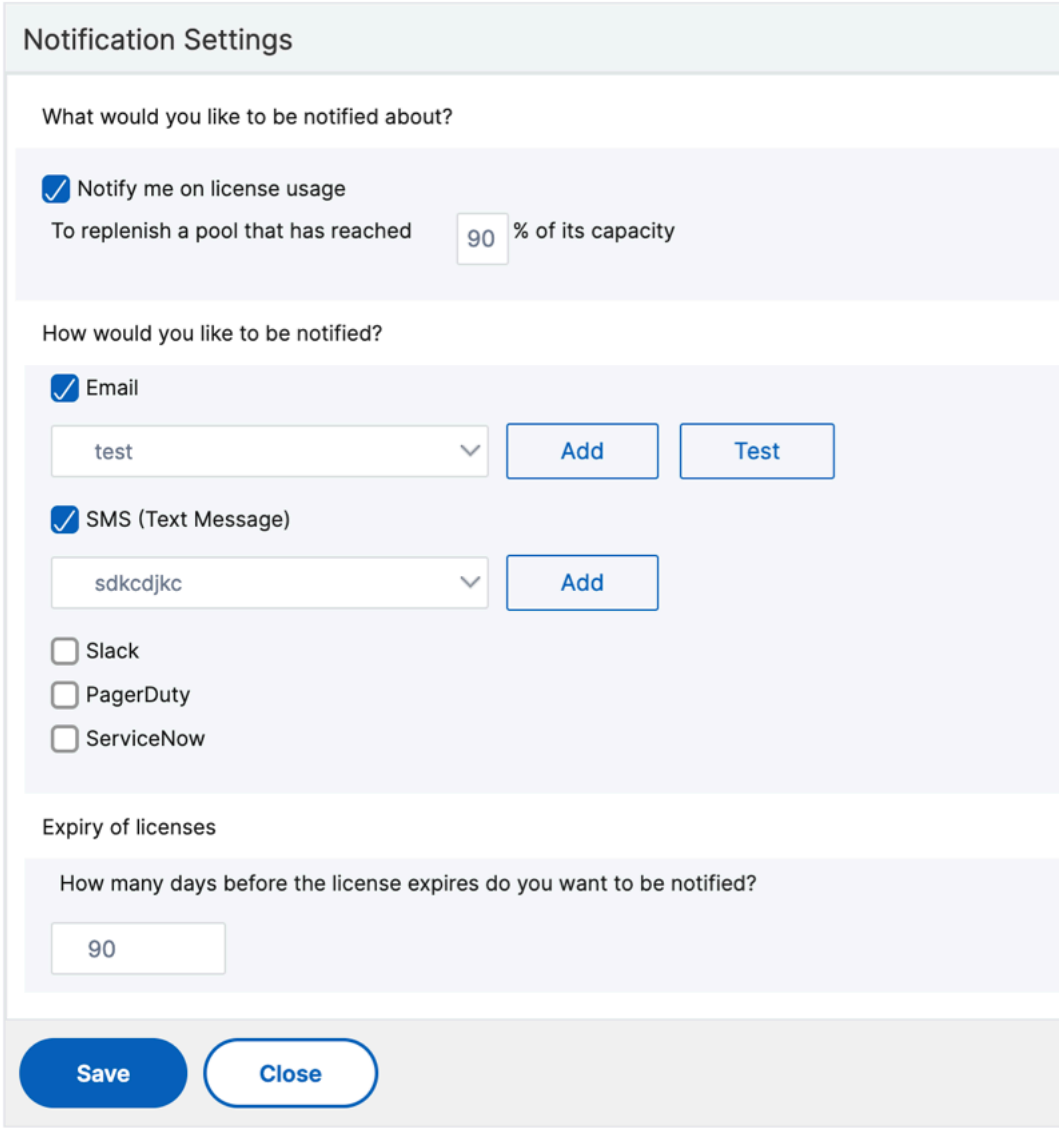
您可以创建自定义通知以补充默认的警报。

宽限期

启用了 NetScaler 池容量的实例处于正常状态且许可证服务器停止响应时，实例会继续使用当前容量运行 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

可以从 NetScaler Application Delivery Management (ADM) 为在实例上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：要为补充已耗尽一定百分比容量的池配置警报，请导航到 基础架构 **>** 池化许可，然后在“通知设置”下，单击“编辑”图标。



发生问题时的预期行为

February 6, 2024

下面是许可证服务器和 NetScaler 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。NetScaler 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，NetScaler 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，NetScaler 实例将进入宽限期，直到连接恢复为止。

启用了 **NetScaler** 池容量的实例停止响应

如果启用了 NetScaler 池容量的实例停止响应且许可证服务器处于正常状态，则许可证服务器在 10 分钟后签入 NetScaler 实例的所有许可证。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 **NetScaler** 集容量的实例都停止响应

如果许可证服务器和启用 NetScaler 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 NetScaler 池容量启用的实例会在重启完成后自动签出许可证。

启用 **NetScaler** 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 NetScaler 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。

如果系统重新启动并且由于池中没有可用容量而导致签出失败，NetScaler 将检查 NetScaler Application Delivery Management (ADM) 池许可证的清单并检查所有可用容量。如果 NetScaler 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）
>
> 许可证服务器未响应。

如果许可证服务器和启用 NetScaler 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 NetScaler 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过期检查

February 6, 2024

现在，您可以为 NetScaler 池容量许可证配置许可证到期阈值。通过设置阈值，NetScaler Application Delivery Management (ADM) 在许可证即将到期时通过电子邮件或 SMS 发送通知。当 NetScaler 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 NetScaler 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. 导航到基础架构 **>** 池化许可。
2. 在“许可证设置”页面的“许可证到期信息”部分下，您可以找到即将到期的许可证的详细信息：
    - 功能：即将过期的许可证类型。
    - 数量：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来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：指定短信服务 (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，NetScaler 实例将在其现有许可证到期时使用新许可证。

签入并签出 **NetScaler VPX** 和 **BLX** 许可证

February 6, 2024

您可以按需从 NetScaler Application Delivery Management (ADM) 向 NetScaler 实例分配 VPX 和 BLX 许可证。ADM 软件存储和管理许可证，许可证具有许可框架，可提供可扩展和自动化的许可证配置。预配实例后，可以从 NetScaler ADM 中检出许可证。当实例被删除或销毁时，实例将其许可证重新检回到 NetScaler ADM 软件。

必备条件

请务必满足以下必备条件：

- 您使用的是运行 12.0 软件版本的 NetScaler VPX 映像。
  例如：NSVPX-ESX-12.0-xx.xx_nc.zip
- 您已经安装了运行版本 12.0 的 NetScaler ADM。
  例如：MAS-ESX-12.0-xx.xx.zip

> 注意
>
> 要管理 NetScaler ADM 提供的现有 VPX 许可证，您需要将许可证重新托管到 NetScaler ADM。

在 **NetScaler 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 NetScaler ADM 虚拟设备。

要在 **NetScaler 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 NetScaler 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 **Infrastructure**（基础结构）**> Pooled Licensing** （池许可）。
4. 在“许可证文件”部分中，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 上已经存在许可证文件，则可以将其上载到 NetScaler 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”页面向 NetScaler ADM 添加更多许可证。

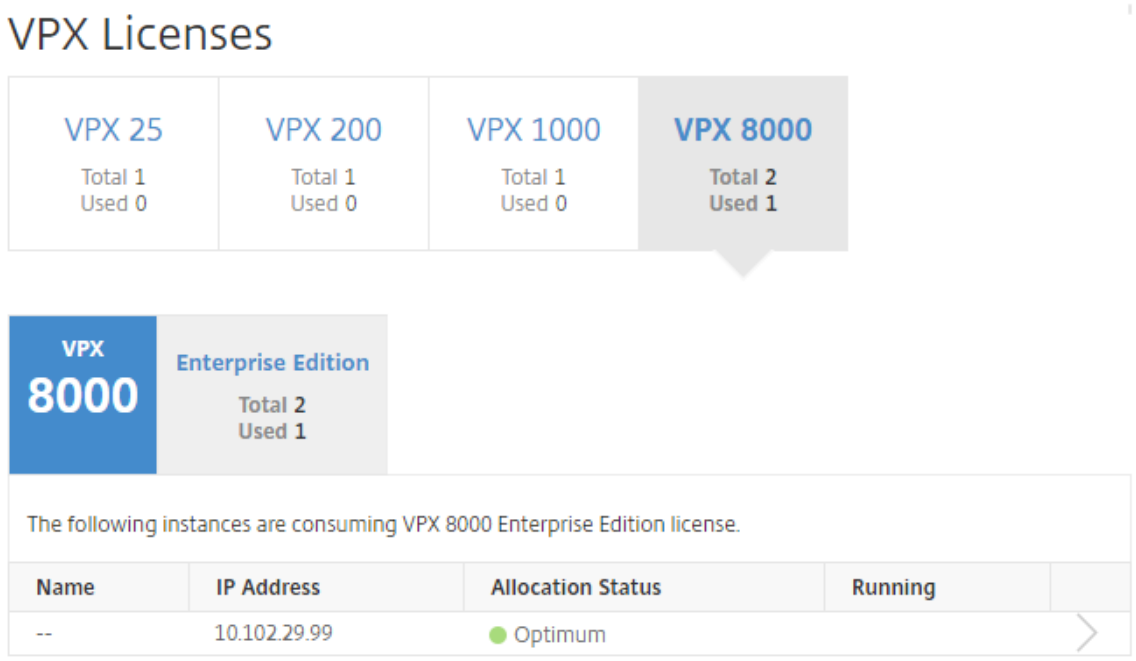
验证

您可以在 NetScaler 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 NetScaler 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。

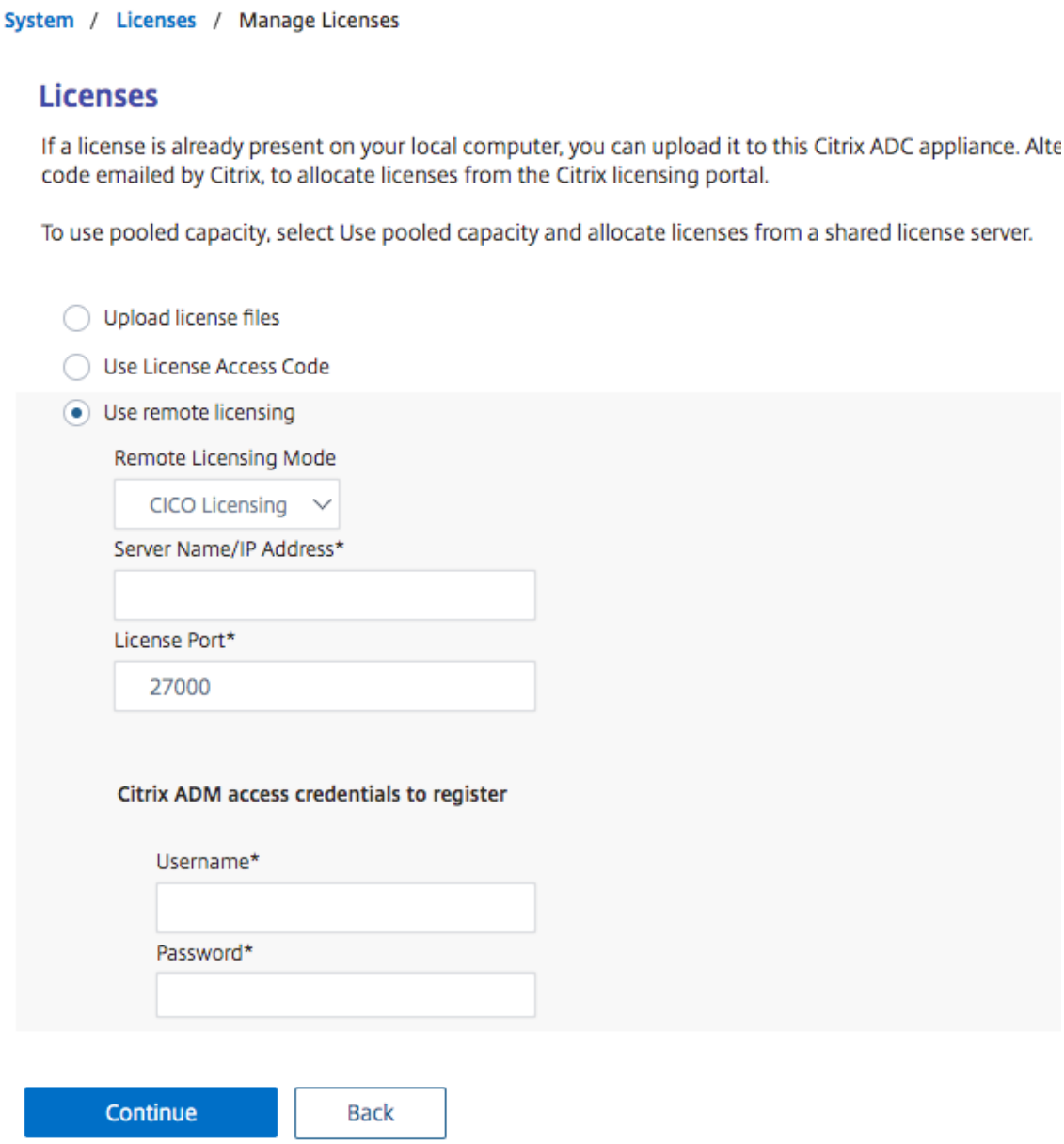
3. 在配置选项卡上，导航到 基础架构 **>** 池许可 **> VPX** 许可证。



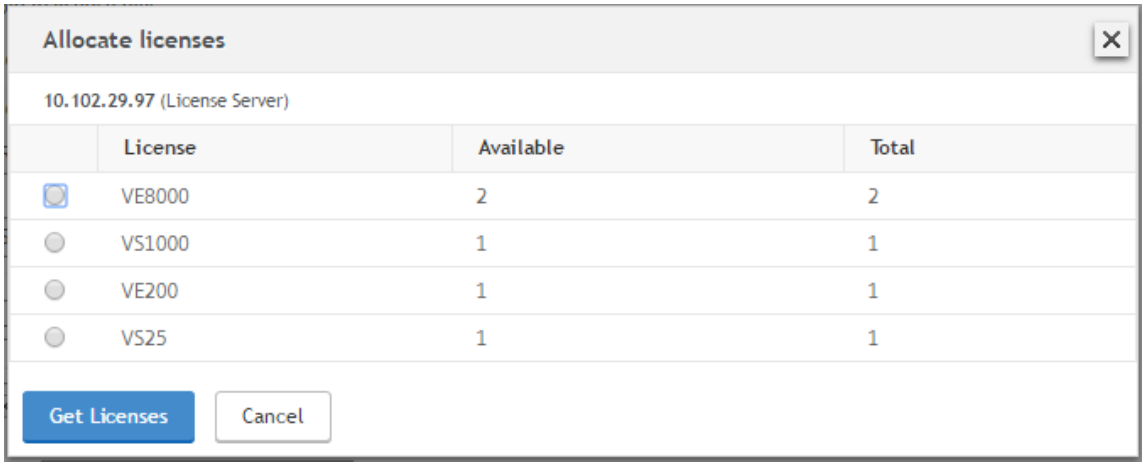
4. 您可以在可用许可证部分下的表中查看分配的许可证。

使用 **NetScaler GUI** 将 **VPX** 和 **BLX** 许可证分配给 **ADC** 实例

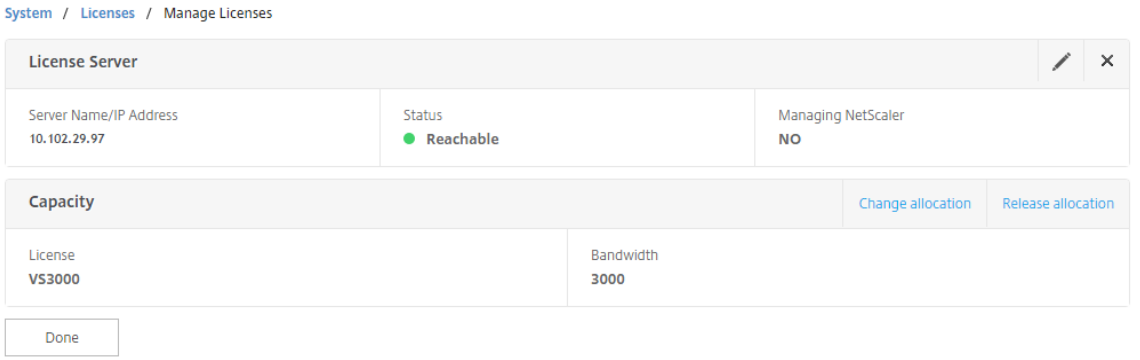
1. 在 Web 浏览器中，键入 NetScaler 实例的 IP 地址（例如，http://192.168.100.1）。
2. 在 **User Name**（用户名）和 **Password**（密码）字段中，输入管理员凭据。
3. 在“配置”选项卡上，导航到“设置” **>** “许可证” **>** “管理许可证”，单击“添加新许可证”，然后选择“使用远程许可” **>** “**CICO** 许可”。
4. 在“服务器 名称**/IP** 地址”字段中输入许可证服务器的详细信息。
5. 在上面屏幕的用户名和密码字段中，输入 NetScaler ADM 凭据，然后单击“继续”。



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 重启，您的 NetScaler 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 **NetScaler CLI** 将 **VPX** 和 **BLX** 许可证分配给 **ADC** 实例

1. 在 SSH 客户端中，输入 NetScaler 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. 要向 NetScaler 设备分配许可证，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
```

使用 **API** 将 **VPX** 和 **BLX** 许可证分配给 **ADC** 实例

在 Web 浏览器或 API 客户端中，使用管理员凭据登录 NetScaler 实例。

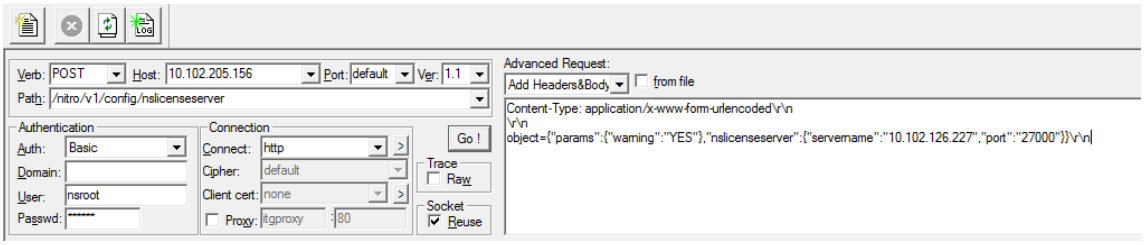
要添加许可服务器，请执行以下操作：

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” :” <NetScaler ADM IP>” ,  “port” :” 27000”  }
  }
 \r\n
<!--NeedCopy-->
```

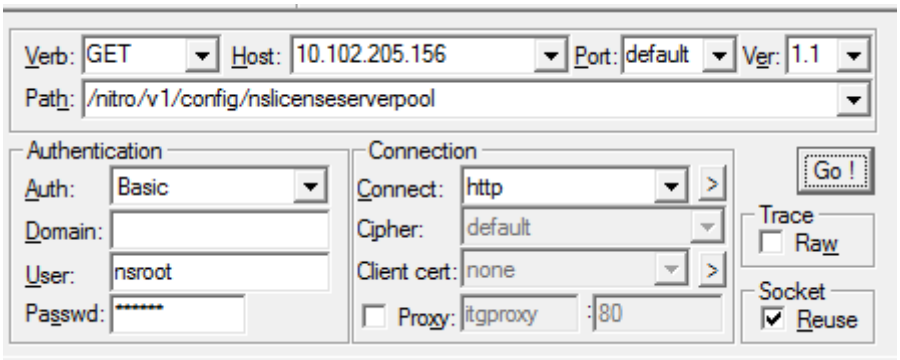


NetScaler ADM 响应请求。以下示例响应显示成功。

```
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 **Get**。
2. 将路径设置为 /nitro/v1/config/nslicenseserverpool



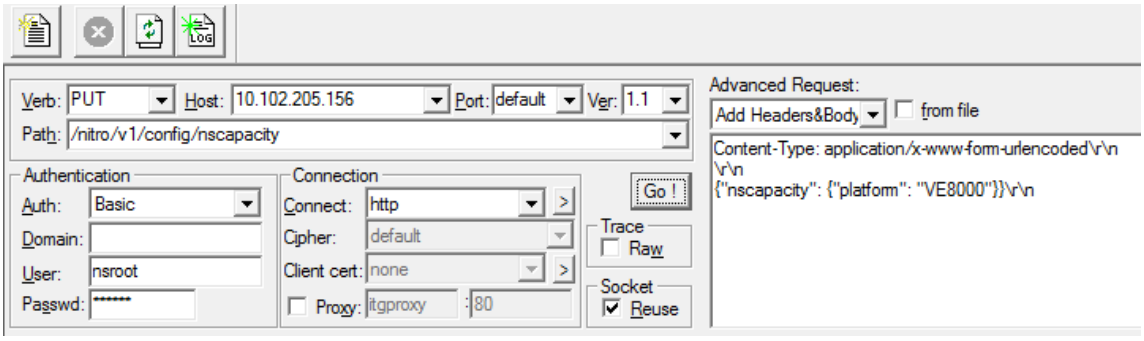
NetScaler ADM 响应请求。以下示例响应显示成功，以及许可证服务器上的可用许可证列表。

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.

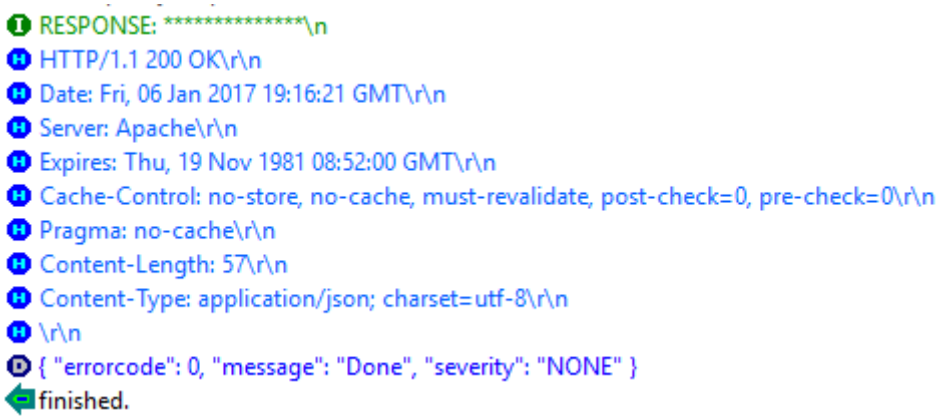
要向 **NetScaler** 设备分配许可证，请执行以下操作：

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-->
```



NetScaler 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 和 BLX 实例中的许可服务器 IP 地址，而不会对实例分配的许可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。有关更多信息，请参阅 使用 NetScaler GUI 将 VPX 和 BLX 许可证分配给 ADC 实例。

为 **NetScaler VPX** 和 **BLX** 签入和签出许可证配置到期检查

现在，您可以为 NetScaler VPX 和 BLX 许可证配置许可证到期阈值。通过设置阈值，NetScaler ADM 在许可证即将到期时通过电子邮件或 SMS 发送通知。当 NetScaler ADM 上的许可证到期时，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 NetScaler 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. 导航到基础架构 **>** 池化许可。
2. 在“许可证设 置”页面的 “许可证到期 信息”部分下，您可以找到即将到期的许可证的详细信息：
   - 功能：即将过期的许可证类型。
   - 数量：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来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：指定短信服务 (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。

NetScaler 虚拟 CPU 许可

February 6, 2024

像您这样的数据中心管理员正在转向更新的技术，这些技术可以简化网络功能，同时提供更低的成本和更大的可扩展性。较新的数据中心架构必须至少包含以下功能：

- 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

这样的变革还需要软件要求动态、灵活和敏捷，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。

NetScaler VPX 的虚拟 CPU 许可

早些时候，NetScaler VPX 许可证是根据实例的带宽消耗分配的。NetScaler VPX 仅限使用基于其绑定许可证版本的特定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，带宽要求可能较低，但对其他 L7 性能（例如 SSL TPS、压缩吞吐量等）的要求更高。在这种情况下，升级 NetScaler VPX 许可证可能不合适。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。NetScaler ADM 现在支持根据虚拟 CPU 要求向 NetScaler 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 NetScaler VPX 有权使用的 CPU 数量。因此，NetScaler 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。NetScaler VPX 会根据系统中运行的 CPU 数量签出许可证。NetScaler VPX 在签出许可证时不考虑空闲 CPU。

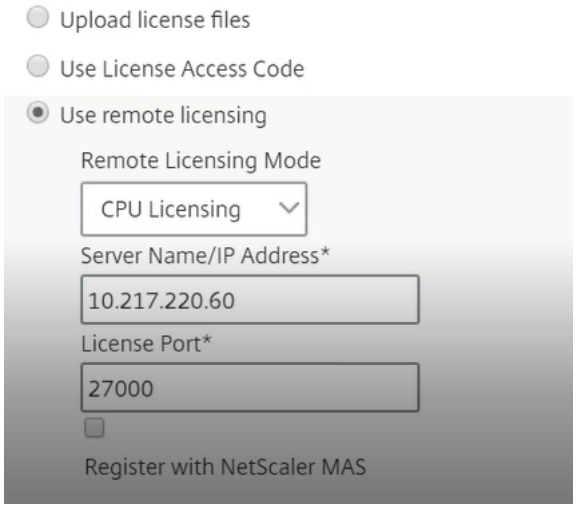
与池许可证容量和 CICO 许可证功能类似，NetScaler ADM 许可证服务器管理一组单独的虚拟 CPU 许可证。此外，为虚拟 CPU 许可证管理的三个版本是标准版、高级版和高级版。这些版本解锁了与带宽许可证版本解锁的功能集相同。

虚拟 CPU 的数量可能会发生变化，或者许可证版本有变化时。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 NetScaler VPX。

要使用 **GUI** 在 **NetScaler VPX** 中配置许可服务器，请执行以下操作：

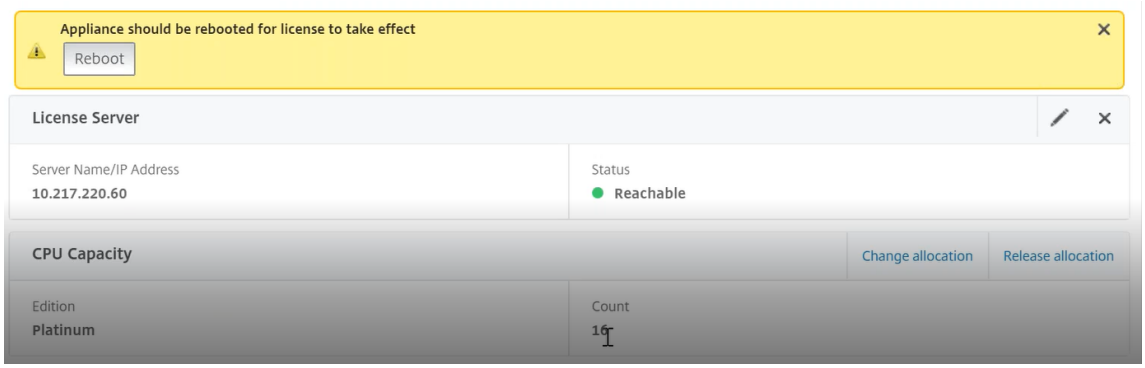
1. 在 NetScaler VPX 中，导航到“系统”“许可证”，然后单击“管理许可”。

2. 在“许可证”页面上，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
>
> 您必须始终在 NetScaler ADM 中注册 NetScaler VPX 实例。如果尚未完成，请启用 NetScaler ADM 注册并键入 **NetScaler ADM** 登录凭 据。

7. 在“分配许可证”窗口中，选择许可证类型。该窗口显示总数和可用的虚拟 CPU 以及可以分配的 CPU。单击 **Get Licenses**（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 **NetScaler VPX** 许可证中配置许可服务器

在 NetScaler 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 NetScaler VPX，请执行以下操作：

```
add licenseserver <IP address of the license server>
<!--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，而不会对实例上分配的许可证带宽产生任何影响，也不会丢失数据。要更新许可服务器 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。

在 **NetScaler ADM** 上管理虚拟 **CPU** 许可证

1. 在 NetScaler ADM 中，导航到 基础架构 **>** 池化许可 **>** 池化 **vCPU**。
2. 此页面显示为每种类型的许可证版本分配的许可证。
3. 单击每个圆环中的数字以查看使用此许可证的 NetScaler 实例。

适用于 **NetScaler CPX** 的虚拟 **CPU** 许可

在配置 NetScaler CPX 实例时，您可以将 NetScaler CPX 实例配置为根据实例的 CPU 使用情况从许可证服务器签出许可证。

NetScaler CPX 依靠在 NetScaler ADM 上运行的许可证服务器来管理许可证。NetScaler CPX 在启动时从许可证服务器签出许可证。当 NetScaler CPX 关闭时，许可证将签回许可证服务器。

您可以使用“docker pull”命令从 Quay 容器注册表下载 NetScaler CPX 映像，然后将其部署在您的环境中。

CPX 许可证有三种许可证类型：

1. CPX 和 VPX 支持虚拟 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 **NetScaler CPX** 实例的同时 **Provisioning vCPU** 订阅许可证，请执行以下操作：

指定 NetScaler CPX 实例使用的 vCPU 许可证数量。

- 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-->
```

在配置 NetScaler CPX 实例时，在 **docker run** 命令中将 NetScaler 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_ADDRESS>* 是 NetScaler 许可服务器的 IP 地址。
- *<LS_PORT>* 是 NetScaler 许可服务器的端口。默认情况下，端口为 27000。

> 注意
>
> 默认情况下，NetScaler CPX 实例会从 vCPU 订阅池中签出许可证。如果 CPX 实例使用“n”个 CPU 运行，则 CPX 实例会检出“n”个许可证。

要在预配 **NetScaler CPX** 实例时 **Provisioning NetScaler** 池容量或 **CP1000** 许可证，请执行以下操作：

如果您想使用池化许可（基于带宽）或 CPX 私有池（CP1000 或基于专用池）查看 CPX 实例的许可证，则必须相应地提供环境变量。

例如，

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

CP1000. 此命令触发从 CP1000 池（CPX 专用池）检出。然后，NetScaler CPX 实例检索为 CPX_CORES 指定的“n”个内核数量的“n”个实例。最常见的用例是为单个实例的检出指定 n = 1。多核 CPX 用例查看“n”个 vCPU（其中“n”介于 1 到 7 之间）。

```
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，消耗高级带宽池中的 1000 Mbps 带宽，但允许 CPX 运行高达 2000 Mbps。在池许可中，不收费前 1000 Mbps 的费用。

> 注意
>
> 从带宽池中取出时，为所需目标带宽指定相应的 vCPU 数量，如下表所示：

内核数量 (vCPU)	最大带宽
1	1000 Mbps
2	2000 Mbps
3	3500 Mbps
4	5000 Mbps
5	6500 Mbps
6	8000 Mbps
7	9300 Mbps

管理系统设置

February 6, 2024

下表介绍了“设置”**>**“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 NetScaler ADM 的 NetScaler ADM 网络配置 IP 地址详细信息
	第二个 NIC	使您可以配置第二个网卡以隔离 NetScaler ADM 管理访问。有关详细信息，请参阅 配置双网卡以访问 NetScaler ADM
	主机名	使您能够为 NetScaler ADM 分配主机名。有关详细信息，请参阅 为 NetScaler 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 NetScaler ADM
静态路由		使您能够配置静态路由，在 NetScaler ADM 和 NetScaler VPX 实例之间建立连接
NTP 服务器		确保 NetScaler 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 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 和当天的消息	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	使您能够修改要在 NetScaler ADM 中使用的时区。默认时区为 UTC

系统配置	选项	说明
	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 NetScaler ADM 中创建欢迎消息。您可以使用此功能为自己或登录到 NetScaler ADM 的用户设置提醒消息。单击 **Enable Message**（启用消息），在消息框中键入消息，然后单击 **Save**（保存）
查看 ADM 指纹		使您能够复制唯一的 NetScaler ADM 指纹 ID 以开始使用服务图
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，则将只为了改进 GUI 来收集使用情况统计信息。收到的数据仅由 Citrix 工程师使用，不会与任何人共享

系统维护

系统维护	说明
升级 NetScaler ADM	使您能够通过 GUI 升级 NetScaler ADM。有关详细信息，请参阅 升级
重新启动 NetScaler ADM	允许您重启 NetScaler ADM
关闭 NetScaler ADM	使您能够关闭 NetScaler ADM
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 NetScaler 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	使您能够限制存储在 NetScaler ADM 中的事件消息报告数据
	实例 syslog	使您可以限制存储在数据库中的 syslog 数据量。有关更多信息，请参阅 配置实例 syslog 修剪设置
	网络报告	使您能够限制存储在 NetScaler 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 NetScaler ADM 上配置设置，以备份选定的 NetScaler 实例或多个实例。有关更多信息，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	可以发送通知来为多种系统相关的功能选择用户组。这些系统功能按事件类别（例如 SystemReboot、StatusPoll、SystemState 等）划分。您可以将 NetScaler Application Delivery Management (ADM) 配置为通过电子邮件、短信或 Slack 向您发送通知。这样可以确保您收到任何系统级别活动的通知，例如超出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合并报告

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 证书的详细信息
配置 SSL 设置	有关详细信息，请参阅 配置 SSL 设置
SSL Certificates（SSL 证书）	使您能够上载、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

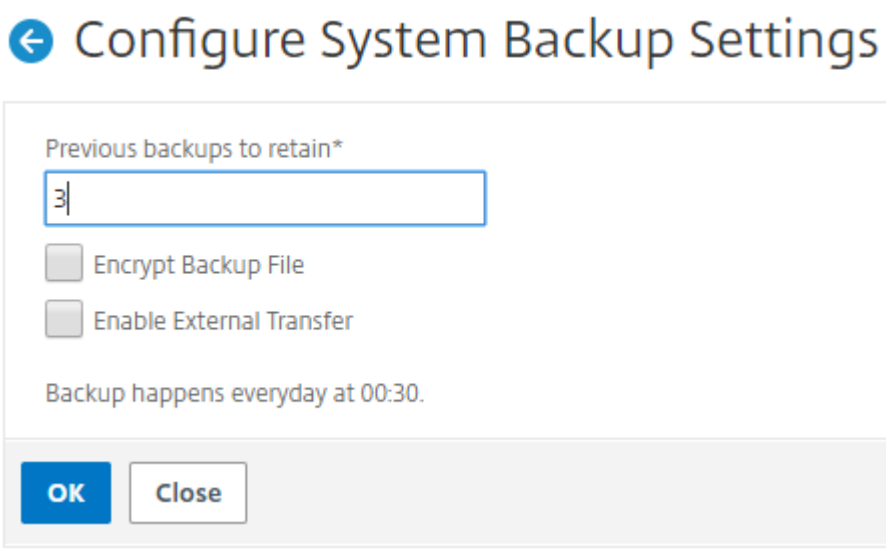
配置功能	说明
禁用或启用功能	您可以在 NetScaler ADM 中启用或禁用功能。有关详细信息，请参阅 启用或禁用 ADM 功能

配置系统备份设置

February 6, 2024

在需要备份和恢复 NetScaler Application Delivery Management (ADM) 系统之前，请先设置初始系统备份设置。

1. 导航到“设置”**>**“管理”。在“备份”下，单击“配置系统和实例备份”。
2. 在备份 **>** 系统页面上，指定以下内容：
   - 要保留以前的备份。您最多只能保留 10 个备份。
   - 选择“加密备份文件”以加密备份文件。
   - 选择“启用外部传输”将备份文件的副本传输到另一个系统。要恢复配置时，必须先将文件上载到 NetScaler 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NetScaler ADM 备份文件传输到外部系统。
3. 单击确定。



配置 **NTP** 服务器

February 6, 2024

您可以在 NetScaler Application Delivery Management (ADM) 中配置网络时间协议 (NTP) 服务器，使其时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler 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 **NetScaler ADM** 上配置 **NTP** 服务器，请执行以下操作：

1. 导航到“设置”**>**“**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 **NetScaler ADM** 上启用 **NTP** 同步，请执行以下操作：

1. 导航到 设置 **> 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 NetScaler Application Delivery Management (ADM)

February 6, 2024

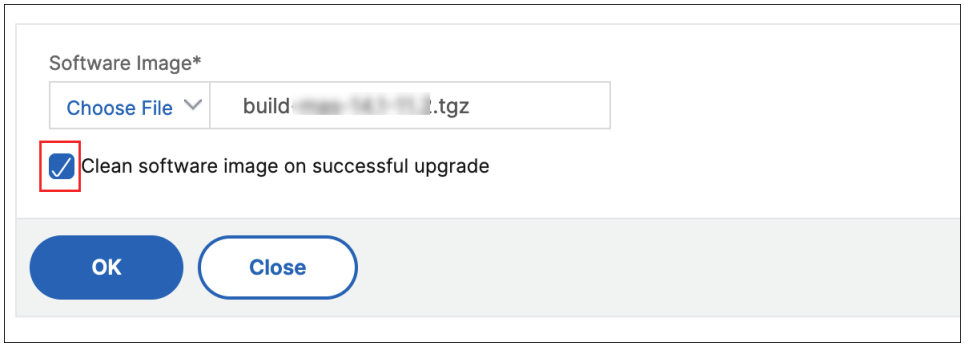
每个 NetScaler ADM 版本都提供了新的和更新的功能，并增强了功能。增强功能的完整列表在版本发布时附带的发行说明中提供。升级软件前，请花一些时间阅读发行说明。在开始升级软件前了解许可框架及许可证类型，这很重要。

要升级 **NetScaler ADM**，请执行以下操作：

1. 导航到 **Settings**（设置）**> Administration**（管理）。在“系统维护”下，单击“升级 **NetScaler ADM**”。
2. 在升级 NetScaler ADM 页面上，通过选择 本地（您的本地 计算机）或 设备来上载新的映像文件。

   > 注意
   >
   > 选择“设备”时，请确保升级映像在 NetScaler ADM 中的 /var/mps/mps_images 下提供。

   默认情况下，软件映像在成功升级后被清理。
3. 单击确定。



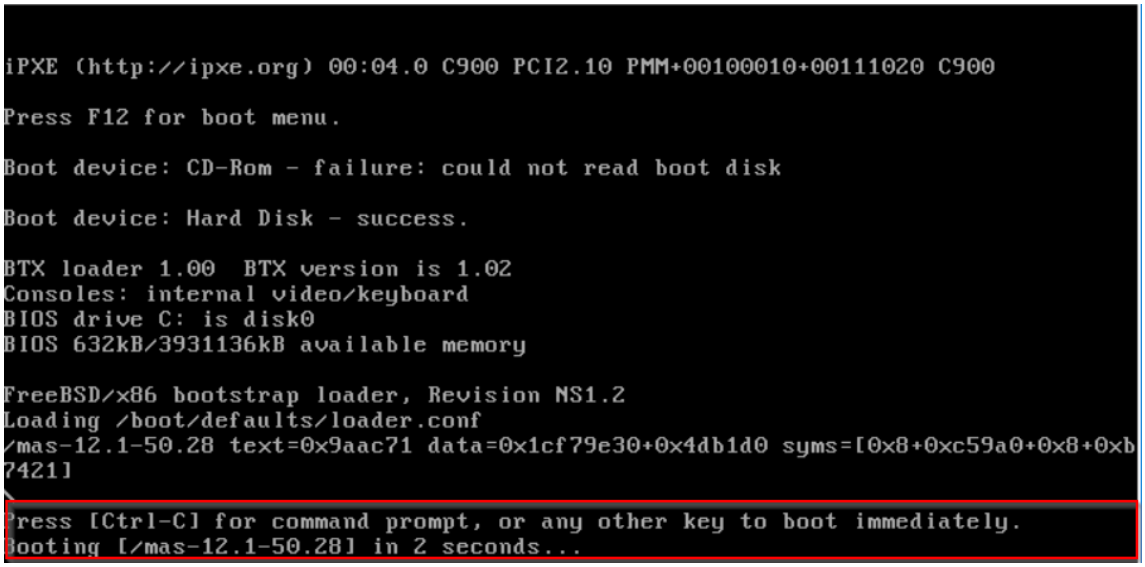
如何重置 NetScaler ADM 的密码

February 6, 2024

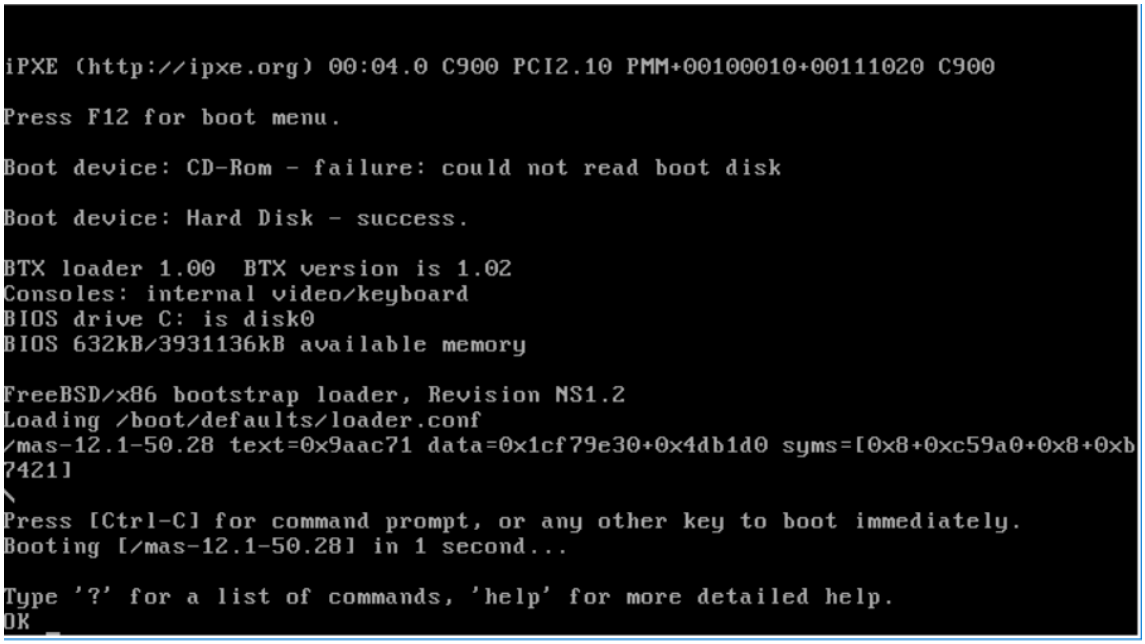
在托管 NetScaler ADM 的虚拟机管理程序上，重置 NetScaler ADM 密码的过程可能有所不同。如果您已更改默认密码并想要重置为默认密码，则可以通过重新启动 NetScaler ADM 节点来重置密码。

使用 **XenCenter** 的 **Citrix Hypervisor**：

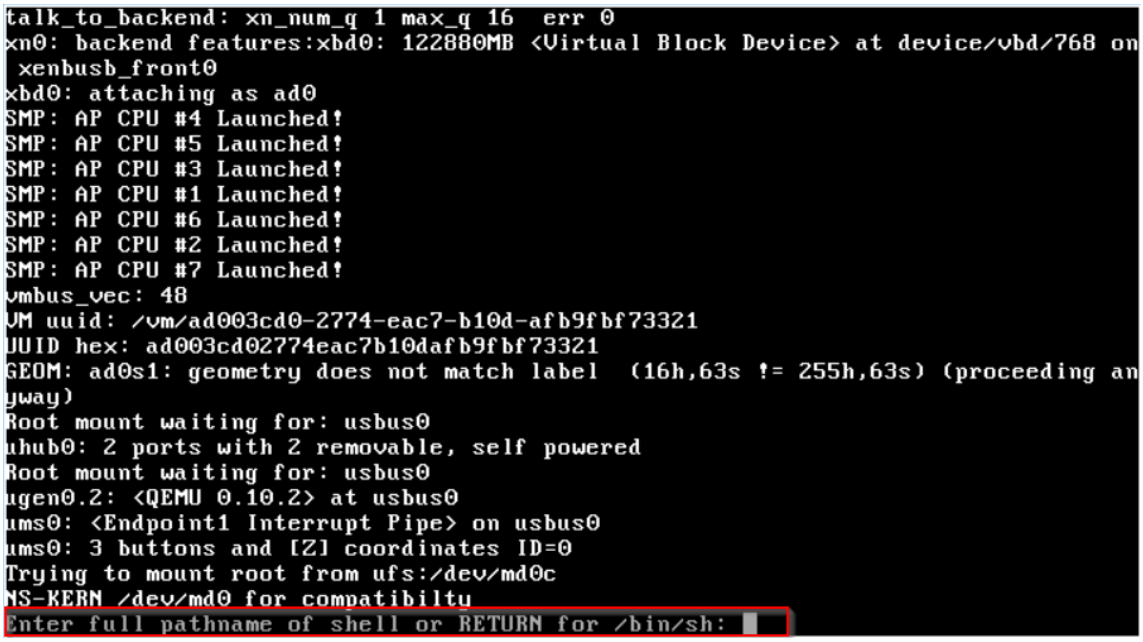
1. 使用 XenCenter 登录 Citrix Hypervisor。
2. 选择 NetScaler ADM 节点，右键单击，然后选择 重新启动。
3. 在 控制台 选项卡上，按 **CTL + C** 中断启动顺序。



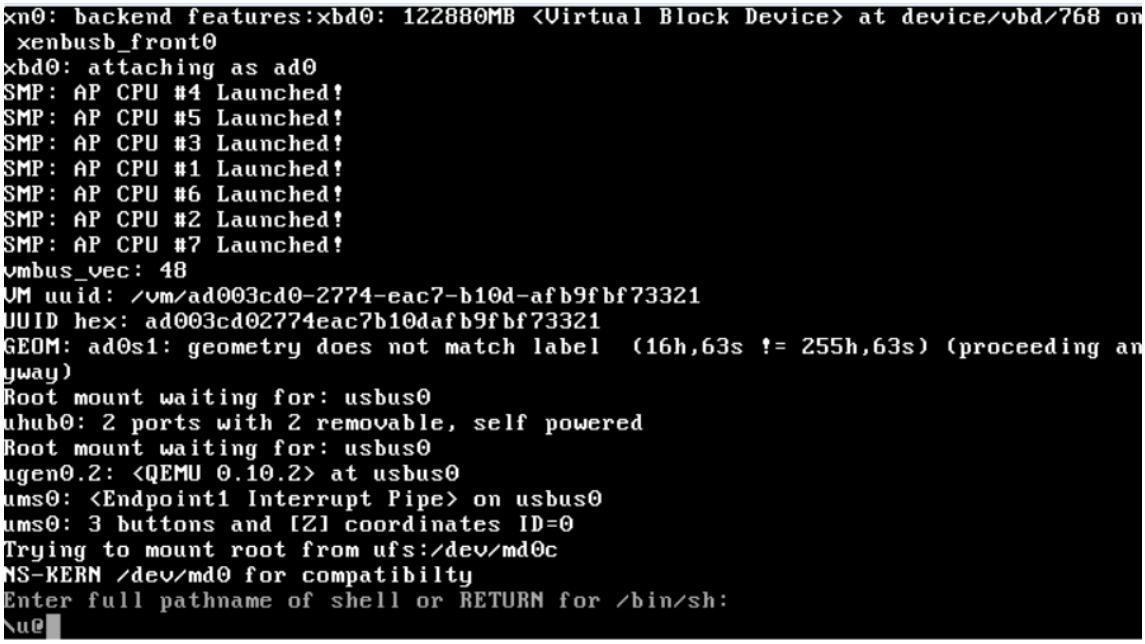
4. 在 OK 提示符下运行 **boot-s** 命令。



NetScaler ADM 重新启动并显示以下消息：

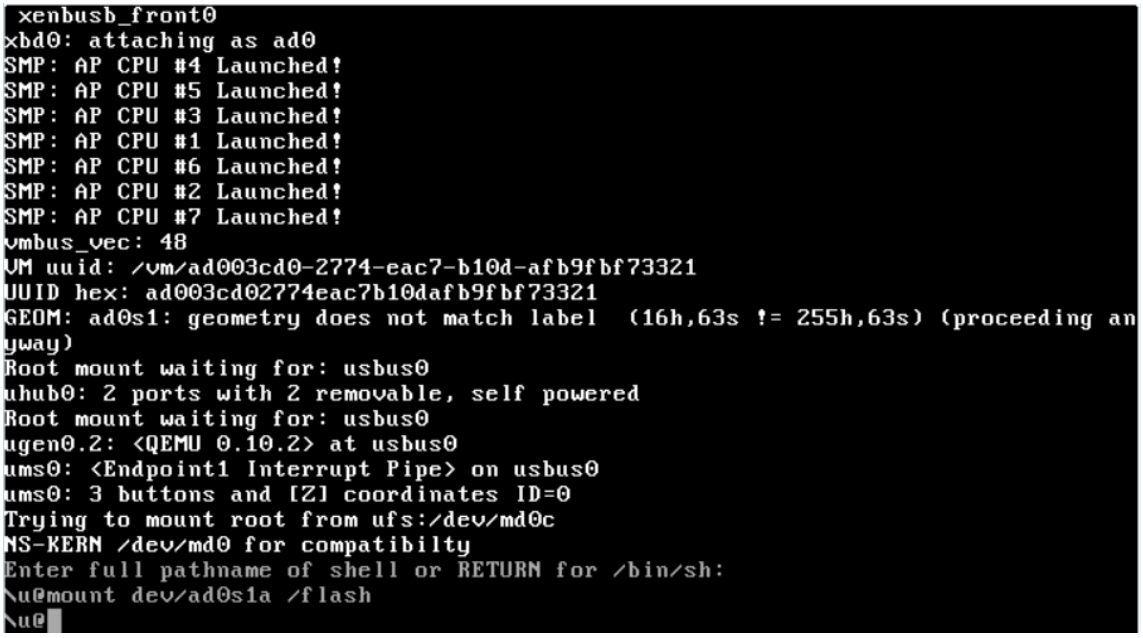


5. 按 **Enter** 获取 /u @ 提示符。



6. 使用以下命令装载闪存分区：

```
mount /dev/da0s1a /flash
```

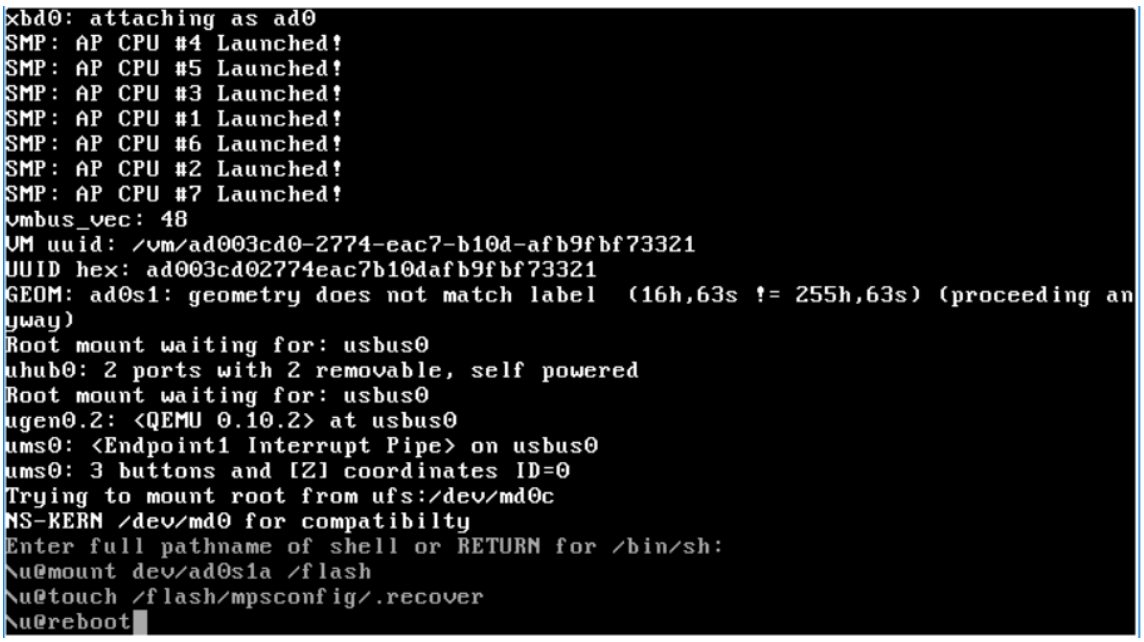



7. 使用以下命令创建文件：

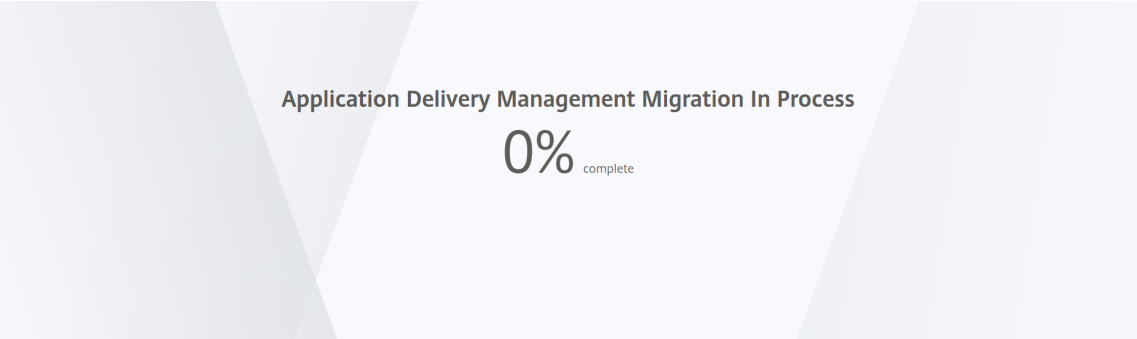
   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

8. 运行 重启 命令以重新启动 NetScaler ADM。



9. 访问 NetScaler ADM GUI，然后等待重新启动完成。

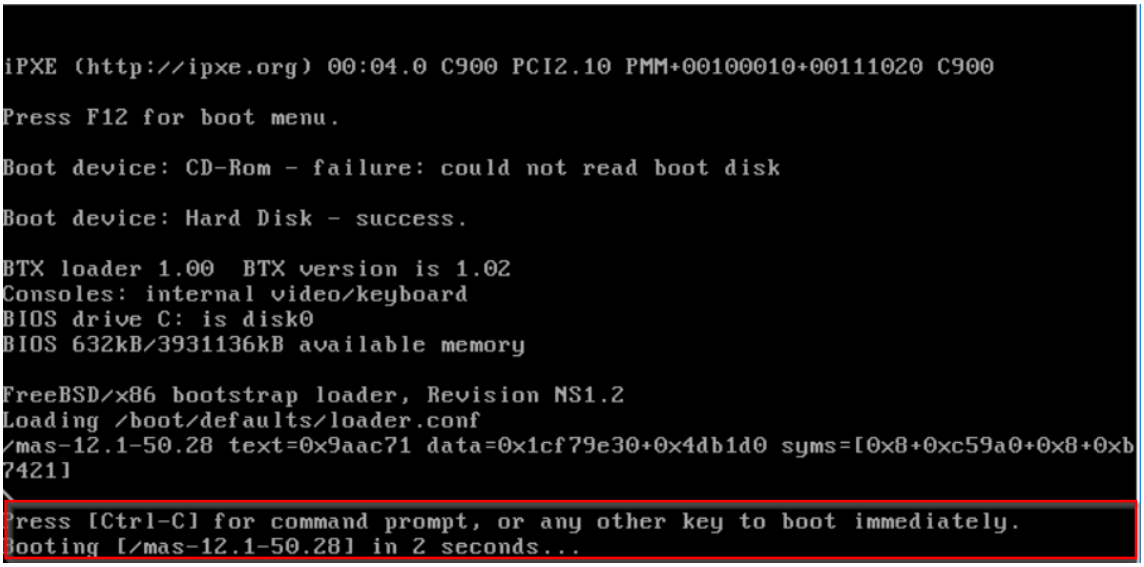


现在，您可以使用 *nsroot/nsroot* 凭据从 GUI 登录，并使用 *nsroot/nsroot* 从 Hypervisor 登录。

> 注意
>
> 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler ADM：
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm -rf /etc/passwd`

使用 **vSphere** 的 **ESX**：

1. 使用 vSphere 登录 ESX。
2. 选择 NetScaler 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** 中断启动顺序。



4. 在 OK 提示符下运行 **boot-s** 命令。

   NetScaler ADM 将重新启动。

5. 按 **Enter** 获取 /u @ 提示符。

6. 使用以下命令装载闪存分区：

   ```
   mount dev/da0s1a /flash
   ```

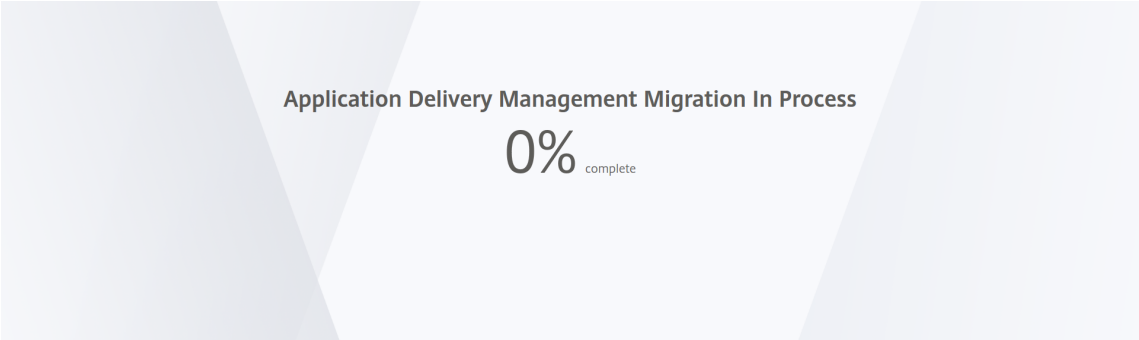
7. 使用以下命令创建文件：

   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

8. 运行 重启 命令以重新启动 NetScaler ADM。

9. 访问 NetScaler ADM GUI，然后等待重新启动完成。

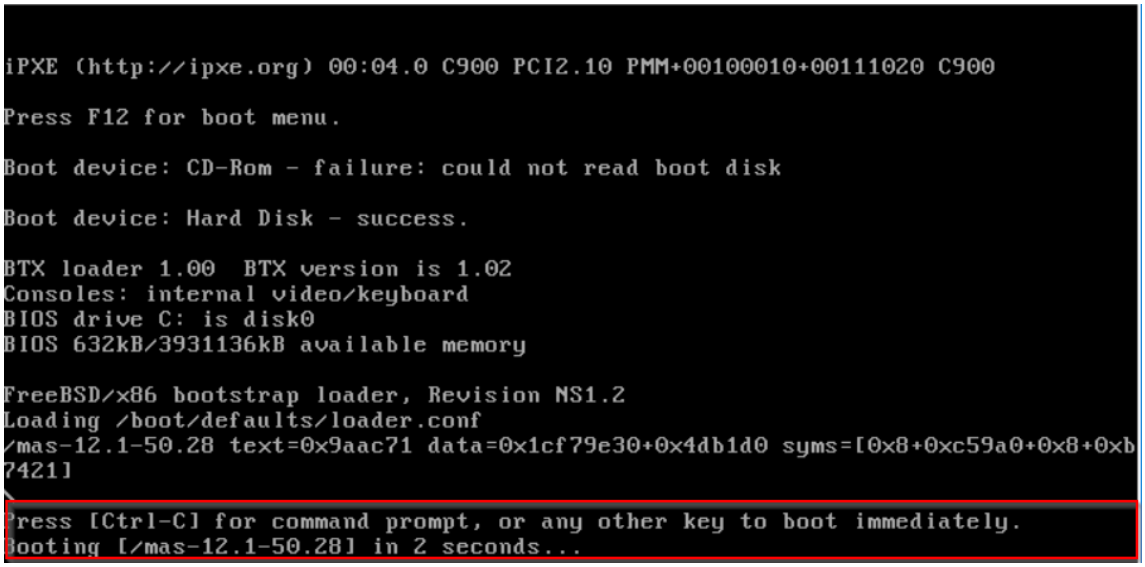


   您现在可以使用 nsroot/nsroot 凭据从图形用户界面登录，从 *ESX* 服务器登录。

   > 注意
   >
   > 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler ADM：
   >
   > - `rm /flash/mpsconfig/master.passwd`
   > - `rm -rf /etc/passwd`

使用 **Hyper-V** 管理器的 **Hyper-V**：

1. 使用 Hyper-v 管理器登录 hyper-v。
2. 选择 NetScaler 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** 中断启动顺序。



4. 在 OK 提示符下运行 **boot-s** 命令。

   NetScaler ADM 将重新启动。

5. 按 **Enter** 获取 /u @ 提示符。

6. 使用以下命令装载闪存分区：

   ```
   mount dev/ad0s1a /flash
   ```

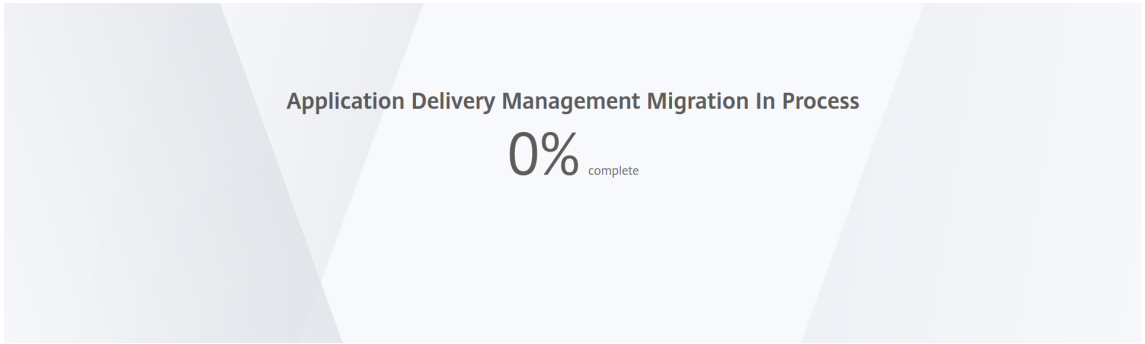
7. 使用以下命令创建文件：

   ```
   touch /flash/mpsconfig/.recover
   ```

   密码现在重置为默认密码。

8. 运行 重启 命令以重新启动 NetScaler ADM。

9. 访问 NetScaler ADM GUI，然后等待重新启动完成。



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。

> 注意
>
> 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并

> 重新启动 NetScaler ADM：
>
> - `rm /flash/mpsconfig/master.passwd`
> - `rm -rf /etc/passwd`

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 NetScaler ADM 到 KVM 服务器。
2. 重启 NetScaler 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'
   ```

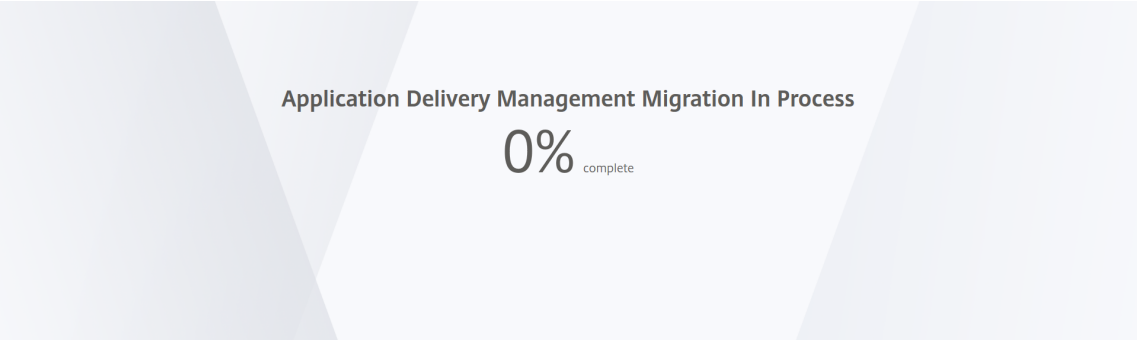
5. 运行 引导**-s** 命令以重新启动 NetScaler ADM。
6. 显示输入 **shell** 的完整路径或 **/bin/sh** 的 **RETURN** 消息后，按 **Enter** 获取 /u@ 提示符。
7. 使用以下命令装载闪存分区：

   ```
   mount dev/vtbd0s1a /flash
   ```

8. 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。
9. 运行 重启 命令以重新启动 NetScaler ADM。
10. 访问 NetScaler ADM GUI，然后等待重新启动完成。



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。

> 注意
>
> 重新启动后，如果密码未重置为默认密码，请重复相同的步骤（步骤 1 到步骤 7）。然后，运行以下命令并重新启动 NetScaler ADM：
>
> - `rm /flash/mpsconfig/master.passwd`


```
• rm -rf /etc/passwd
```

配置辅助网卡以访问 **NetScaler ADM**

February 6, 2024

您可以配置第二个 NIC 以隔离对 NetScaler ADM 的管理访问权限。使用第二个 NIC 功能，根据您的要求，您可以选择如何隔离通过 NetScaler ADM 接收和发送的流量。

假设您要将流量隔离到以下场景：

- 将 NetScaler ADM 与其托管的 NetScaler 实例之间的所有通信置于一个网络中。
- 拥有对其他网络中的 NetScaler ADM 的管理访问权限。

在这种情况下，作为管理员，您可以：

- 为 NetScaler ADM 与其托管的 NetScaler 实例之间的流量配置一个 IP 地址。
- 配置另一个用于管理 NetScaler ADM 软件的 IP 地址，以执行软件中的所有管理任务。

> 注意
>
> 如果 NetScaler 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。

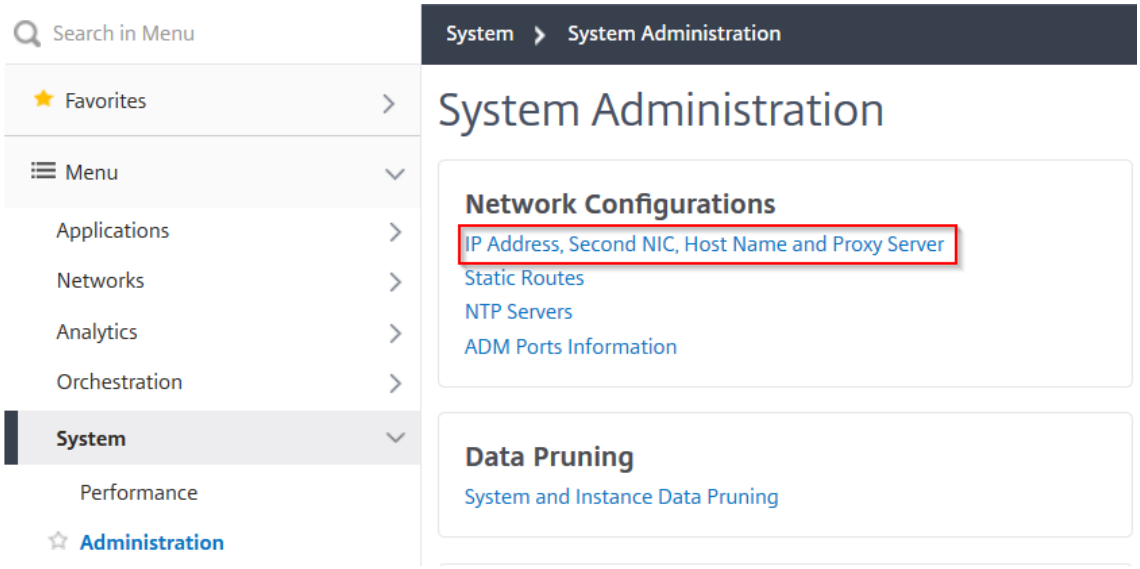
必备条件

- 确保已在 Hypervisor（**Citrix Hypervisor**、**Microsoft Hyper-V**、**Linux KVM** 或 **VMware ESXi**）上部署并配置了 **NetScaler ADM 13.0** 版本 **47.x** 版本或更 高版本。
- 确保已在 Hypervisor（Citrix Hypervisor、Microsoft Hyper-V、Linux KVM 或 VMware ESXi）上添加了第二个网卡。

要为 Citrix Hypervisor 上的 NIC 分配 IP 地址并创建辅助接口，请参阅 为 NIC 分配 IP 地址。

在 **NetScaler ADM** 中配置第二个网卡

1. 登录到 ADM 图形用户界面。
2. 导航到 **Settings**（设置）**> Administration**（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”。



屏幕上将显示“网络配置”页面。

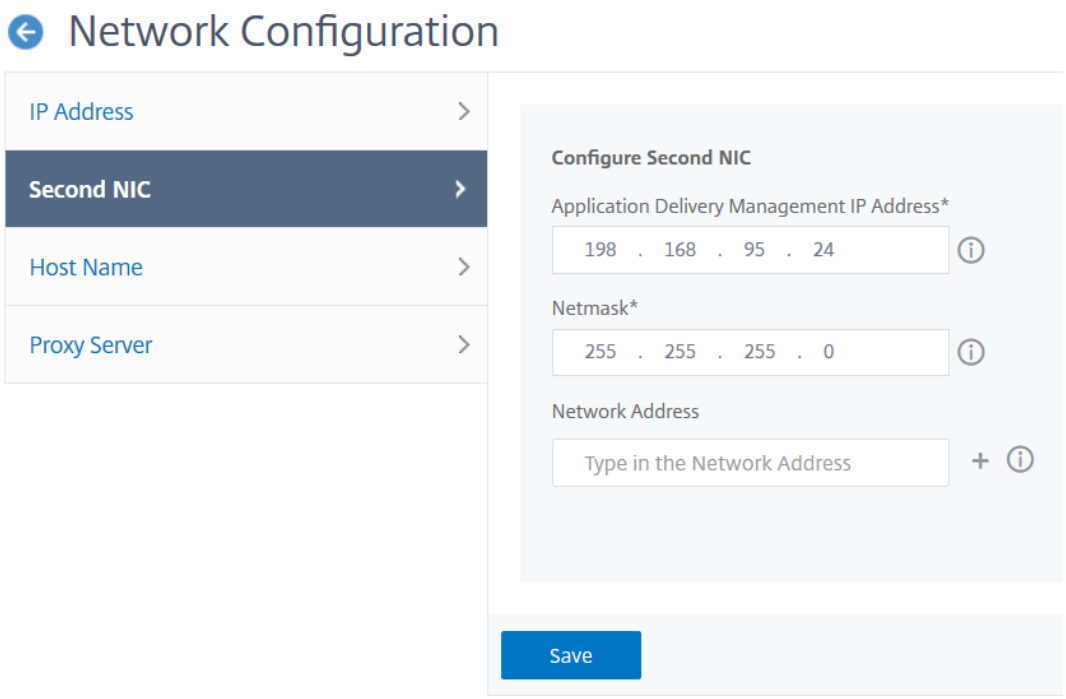
4. 单击第二个 NIC 选项卡并配置以下参数：

   a) **Application Delivery Management IP** 地址—输入有效的 IP 地址以访问 NetScaler ADM。除了现有的管理 IP 地址外，您还可以使用此 IP 地址访问 NetScaler 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 255.255.255.0。

   c) 网络地址—输入 IP 地址以为 NetScaler ADM 添加路由条目。单击 **+** 添加更多 IP 地址。此字段为可选字段。

   d) 单击保存。



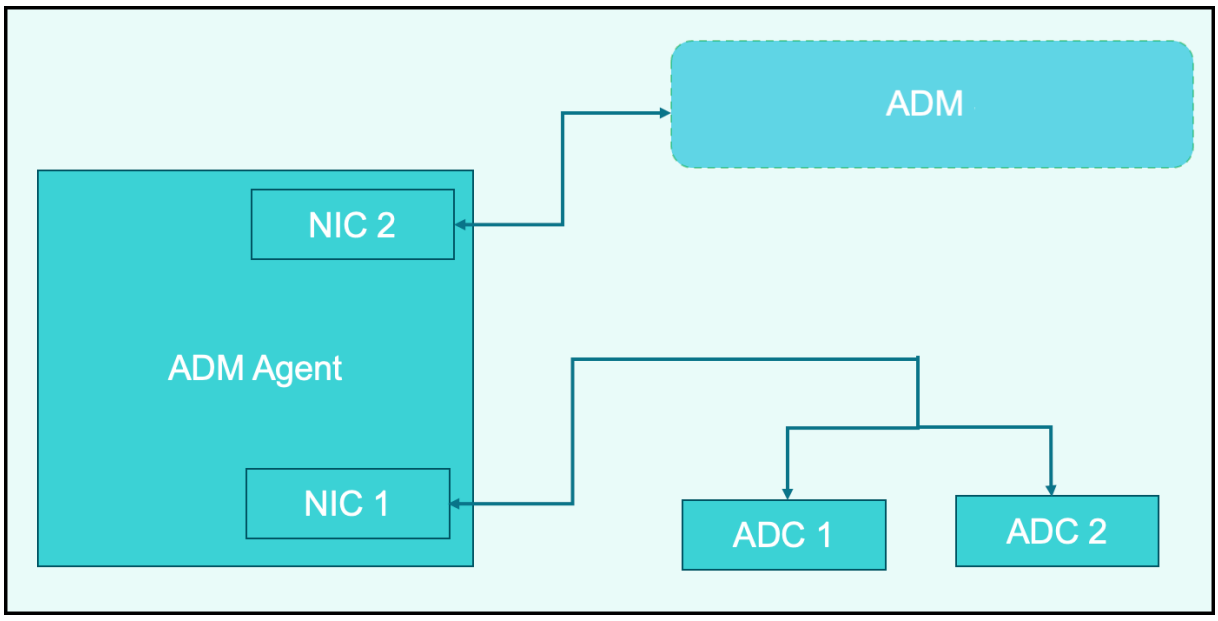
配置辅助网卡以访问 **ADM** 代理

February 6, 2024

您可以在 ADM 代理上配置两个 NIC。使用双 NIC 架构，ADM 代理将能够：

- 在 ADM 代理和 ADC 实例之间建立通信——您可以使用第一个 NIC 隔离通过 NetScaler ADM 接收和发送的流量，也可以在 NetScaler ADM 与其在另一个网络中的托管 NetScaler 实例之间进行通信。
- 在 ADM 代理和 NetScaler ADM 之间建立通信-您可以使用第二个 NIC 来管理网络上的 NetScaler ADM 并执行管理任务

> 注意
>
> 您无法交换两个 NIC 的功能和配置。



在这种情况下，作为管理员，您可以：

- 为 NetScaler ADM 与其托管的 NetScaler 实例之间的流量配置 IP 地址。
- 配置 IP 地址以管理 NetScaler ADM 软件以执行软件中的所有管理任务。

> 注意
>
> 为 ADM 代理配置双网卡不是强制性的。它是可选的，仅在需要分离 ADM 代理、NetScaler ADM 和 ADC 之间的流量时才是必需的。

使用 **CLI** 修改 **IPV4** 网卡网络地址

1. 使用 SSH 客户端（例如 PuTTY）打开连接到 NetScaler ADM 代理控制台的 SSHconnection。
2. 使用 nsrec **over/nsroot** 凭据登录并切换到 shell 提示符。
3. 运行 **ifconfig** 命令。您可以看到已配置的两个 NIC 的详细信息-
    - NIC 1 —用于 ADM 代理与 ADC 通信之间的通信
    - NIC 2 —用于 ADM 代理与 NetScaler ADM 之间的通信


```
bash-3.2# ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 1500
        options=680003<RXCSUM,TXCSUM,LINKSTATE,RXCSUM_IPV6,TXCSUM_IPV6>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        groups: lo
pflog0: flags=0<> metric 0 mtu 33152
        groups: pflog
1/1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether a2:56:cd:d2:f8:8c
        hwaddr a2:56:cd:d2:f8:8c
        inet6 fe80::a056:cdff:fed2:f88c%1/1 prefixlen 64 scopeid 0x3
        inet 10.102.103.247 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
1/2: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
        ether 32:89:fe:8c:8f:45
        hwaddr 32:89:fe:8c:8f:45
        inet6 fe80::3089:feff:fe8c:8f45%1/2 prefixlen 64 scopeid 0x4
        inet 10.102.103.250 netmask 0xffffff00 broadcast 10.102.103.255
        nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
        media: Ethernet manual
        status: active
```

4. 运行 n **etworkconfig** 命令。出现一个菜单，允许您设置或修改 IPV4 网络地址。

```
bash-3.2# /mps/networkconfig

--------------------------------------------------------------------------------
Citrix ADM Agent 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 Agent Host Name [ns]:
     2. Citrix ADM Agent IPv4 address [10.102.103.247]:
     3. Netmask [255.255.255.0]:
     4. Gateway IPv4 address [10.102.103.1]:
     5. DNS IPv4 Address [10.102.166.70]:
     6. Second NIC IPv4 address [10.102.103.250]:
     7. Second NIC Netmask [255.255.255.0]:
     8. Second NIC Network address [10.102.103.251,10.102.103.252,10.102.103.252]:
     9. Second NIC Gateway IPv4 address [10.102.103.2]:
    10. Cancel and quit.
    11. Save and quit.
```

> 注意
>
> 第二个 NIC 网络地址可以采用多个 IP 值。

5. 选择要修改的菜单项。保存并退出设置。

配置 **syslog** 删除时间间隔

February 6, 2024

Syslog 是日志记录标准协议。它有两个组件：在 Citrix Application Delivery Controller (ADC) 实例上运行的 Syslog 审核模块和 Syslog 服务器，它可以在 NetScaler 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。

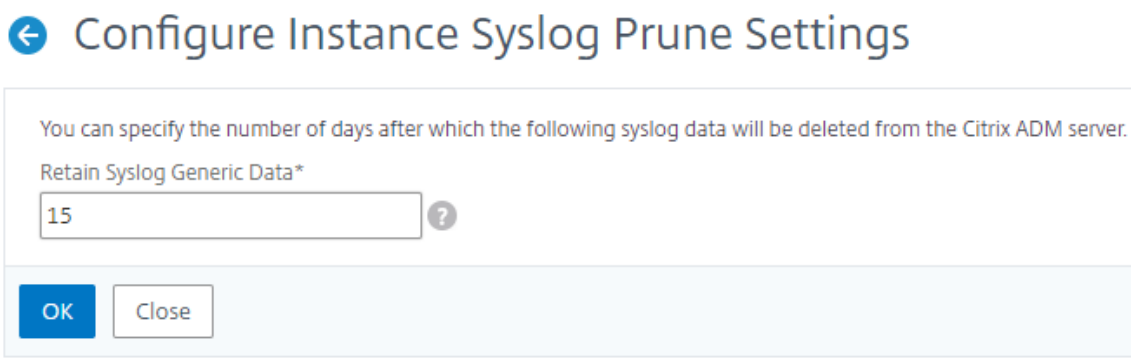
要限制存储在数据库中的 syslog 数据量，可以指定要修剪 syslog 数据的时间间隔。您可以指定天数，在此天数之后将从 NetScaler Application Delivery Management (ADM) 中删除以下 syslog 数据：

- 一般 Syslog 数据
- AppFirewall 数据
- NetScaler Gateway 数据

您也可以按系统日志类型配置 NetScaler Gateway 的删除间隔。此修剪间隔优先于为保留 NetScaler Gateway 数据而配置的符文间隔。

要为 **NetScaler ADM** 配置系统日志修剪间隔设置，请执行以下操作：

1. 导航到 **Settings**（设置）**> Administration**（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 **Syslog** 删除设置 页面中，指定 保留 **Syslog** 通用数据（天）。键入 NetScaler 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

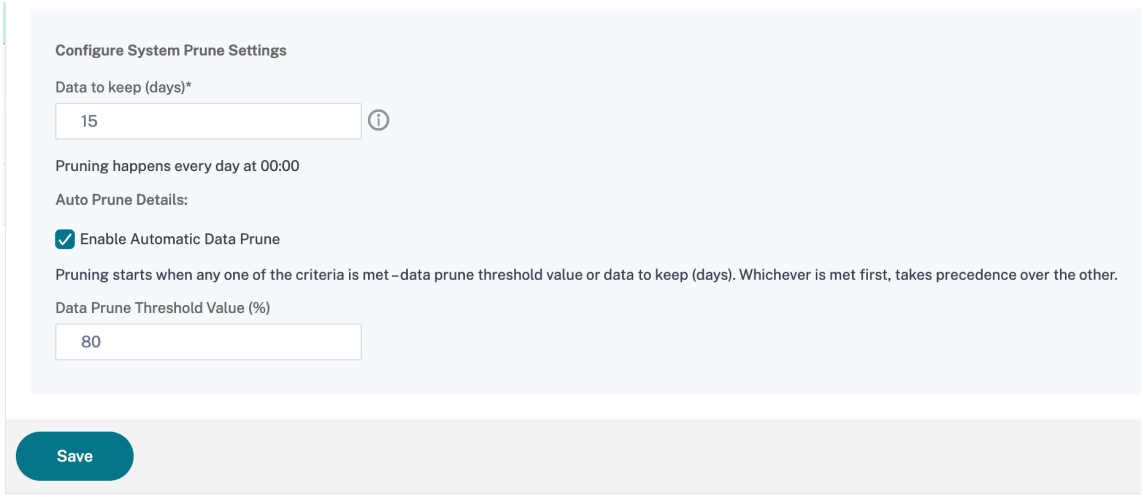
February 6, 2024

要限制存储在 NetScaler 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 NetScaler 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 小时修剪一次（在 00.00 点）。

> 注意
>
> 您指定的值不能超过 30 天或小于 15 天。

要为性能报告配置系统删除设置，请执行以下操作：

1. 导航到 “设置” > “管理”。在“数据修剪”下，单击“系统和实例数据修剪”。
2. 在“配置系统删除设置”页中，指定以下内容：
   - 保留数据的天数
   - 磁盘空间百分比（修剪阈值）
3. 单击确定。



您可以通过选中“启用自动数据修剪”复选框来启用自动修剪。当磁盘使用量超过配置的数据删除阈值时，将触发警报并发送电子邮件。

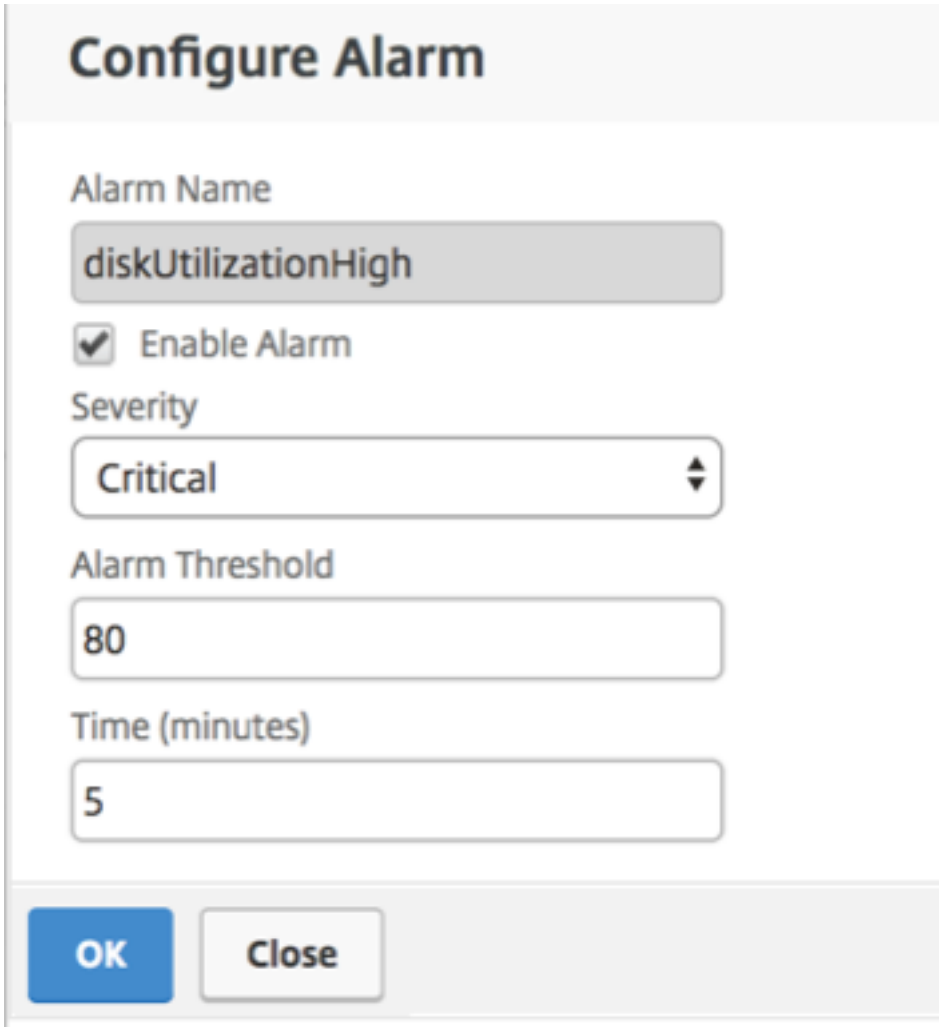
> 注意
>
> 当满足任一条件（数据删除阈值或要保留的数据（天数）时，即开始修剪。以先满足者为准，优先于另一个。

要配置和启用警报设置，请执行以下操作：

1. 导航到设置 > **SNMP**。单击右上角的“警报”。
2. 选择要配置的警报（例如 diskUtilizationHigh），然后单击“编辑”。
3. 在“配置警报”页面中，指定以下内容：

- 严重性—选择严重性级别。
- 警报阈值-键入用于计算事件严重性的值。

- 时间—键入要触发警报的时间（以分钟为单位）。



使用 **NetScaler ADM** 配置事件修剪设置

要限制存储在 NetScaler ADM 数据库中的事件消息数据量，可以指定希望 NetScaler 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 小时修剪一次（在 00.00 点）。

1. 导航到 设置 **>** 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。
2. 输入要在 NetScaler ADM 服务器上保存数据的时间间隔（以天为单位），然后单击“保存”。

为非默认用户启用 **shell** 访问权限

February 6, 2024

您可以在 NetScaler Application Delivery Management (ADM) 中为非默认用户启用 shell 访问权限。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 **NetScaler ADM** 中为非默认用户启用 **shell** 访问权限，请执行以下操作：

1. 在 NetScaler 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 -为 NetScaler ADM 启用安全访问。
    - **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 NetScaler 下载证书。
    - 为非 **nsroot** 用户启用 **Shell** 访问权限 - 在 NetScaler ADM 中为非默认用户启用 shell 访问权限。
    - 提示用户凭据进行实例登录 -允许用户在从 NetScaler ADM 登录实例时输入其用户凭据。
4. 单击确定。

恢复无法访问的 **NetScaler ADM** 服务器

February 6, 2024

NetScaler Application Delivery Management (ADM) 现在提供数据库维护工具，用于清理系统数据库。现在，您可以启动 NetScaler ADM 实用工具来连接到文件系统、删除一些组件并使数据库可访问。NetScaler 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。该工具可帮助您按连续步骤浏览数据库表和文件，并显示相应项目在文件系统上占用的当前空间。选择要删除的数据库表和文件后，该工具将在确认后从文件系统中删除这些表和文件。

如何使用 **NetScaler ADM** 数据库恢复脚本进行 **NetScaler ADM** 独立部署

在单个服务器 NetScaler 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 NetScaler 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 NetScaler 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。

```
--------------------------------------------------------------------------------
*************************** Citrix ADM Cleanup Utility ***************************
--------------------------------------------------------------------------------

        This utility helps you gain disk space by performing cleanup.


                    Checking whether DB is accessible...

                              DB is accessible.

            Please wait. Gathering data. This will take some time.



                                <----------->
```

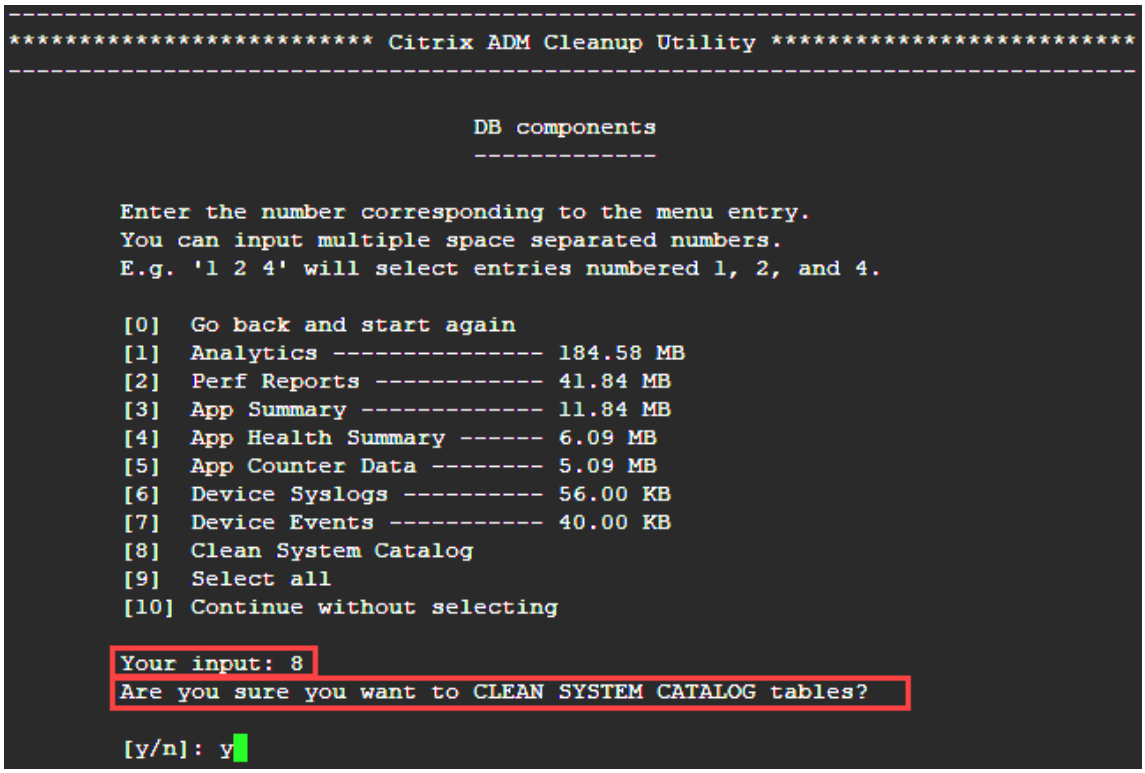
3. 屏幕显示数据库中的文件列表。键入“y”，然后按 Enter 键开始清理过程。

```
--------------------------------  SUMMARY  ---------------------------------

                  DB component                Current size
                  ------------                ------------

                  Analytics  ------------------  184.58 MB
                  Perf Reports  ----------------  43.73 MB
                  App Summary  -----------------  12.03 MB
                  App Health Summary  -----------  6.33 MB
                  App Counter Data  -------------  5.30 MB
                  Device Syslogs  --------------  56.00 KB
                  Device Events  ---------------  40.00 KB

                  Filesystem component        Current size
                  --------------------        ------------

                  Citrix ADM Images  -----------  15.51 GB
                  Core Files  -----------------  718.37 MB
                  Citrix ADC Images  ----------  453.32 MB
                  Techsupport Bundles  --------  439.35 MB
                  Device Backup  --------------  131.79 MB
                  Citrix ADM Backup  -----------  35.21 KB
                Citrix ADC VPX ESXi Images  -------  0.00 B
                  Citrix ADC SDX Images  ---------  0.00 B
                  Citrix ADC CPX images  ---------  0.00 B

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

        Do you wish to proceed with cleanup?
        [y/n]:
```

4. 您可以选择需要清理的特定数据库组件，然后键入相应的数字。按下 回车 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。

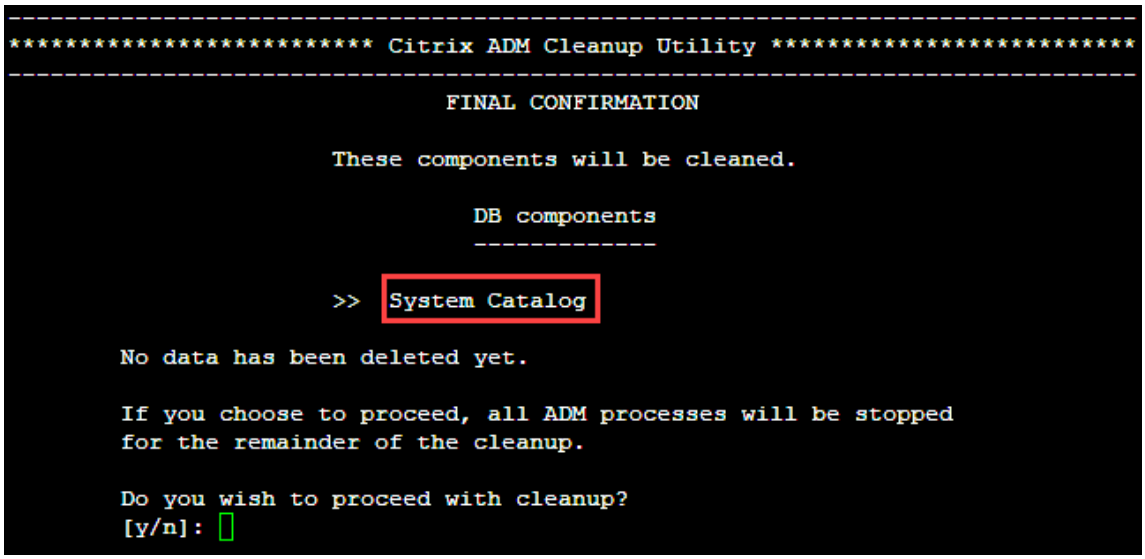
> 注意
>
> NetScaler ADM 包括被称为系统目录的用户表。系统目录是 NetScaler ADM 数据库中的一个位置，关系数据库管理系统在该位置存储架构元数据，例如有关表和列的信息以及内部记录。系统目录中的表就像常规表一样，随着时间的推移，它们会累积膨胀行和死行，因此需要定期清理以获得最佳性能。定期维护这些表是一种很好的做法。该活动不仅释放了磁盘空间，还提高了数据库的整体性能，从而提高了 NetScaler ADM 的整体性能。



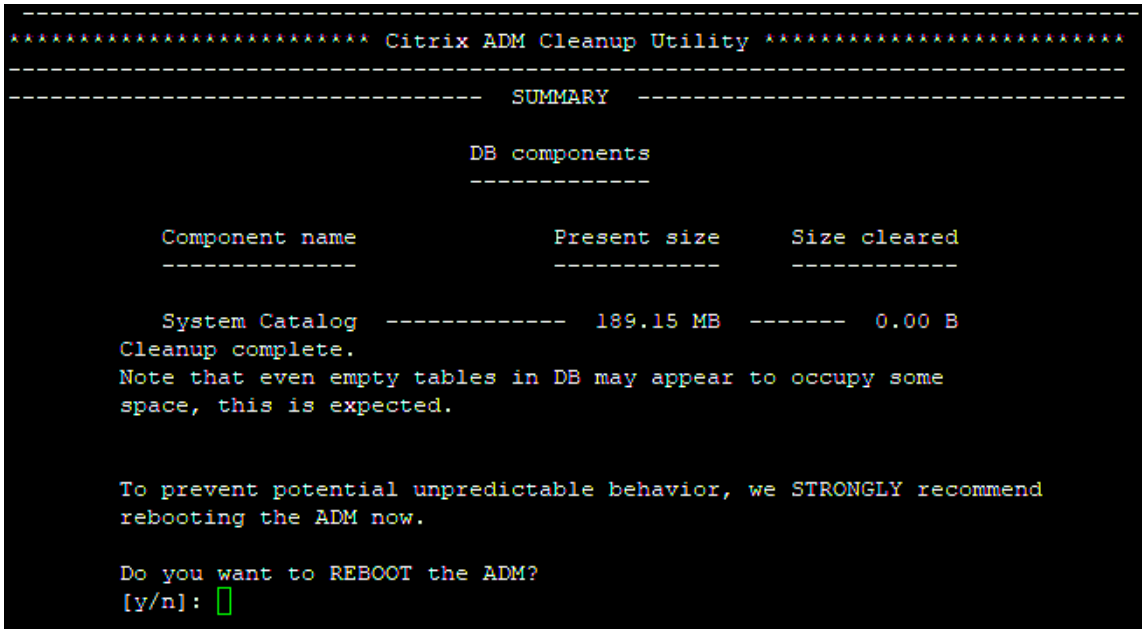
清理实用程序为您提供了清理数据库组件和文件组件的选项。您可以通过键入 “1” 和 “9” 之间的数字来选择任何文件组件，或者键入 “11” 并按 Enter 键清理数据库组件。

> 注意
>
> 数字 “11” 表示您尚未选择任何要清理的文件组件，正在清理先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**”，然后在最终确认屏幕中再次按下 **Enter** 键。



系统目录已清理，这可能需要一些时间，具体取决于系统目录中表格的大小。该过程完成后，将显示摘要屏幕。



6. 键入 “**y**”，然后按 **Enter** 键重新启动 **NetScaler ADM**。

   确保在系统清理后重新启动 NetScaler ADM。在 NetScaler 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 NetScaler 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 NetScaler ADM 启动并运行时，它应该可以按预期工作。

   > ** 注
   >
   > 意：** 清理后，系统目录表的当前大小永远不会等于零。这是因为只有空行会从表中删除，即使清理了表中也可能有一些有效的条目。

如何使用 **NetScaler ADM** 数据库恢复脚本进行 **NetScaler ADM** 高可用性部署

高可用性部署中 NetScaler ADM 服务器的数据库系统处于持续同步模式。在使用新的数据库恢复工具时，您无需在两台 NetScaler 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. 请运行以下命令：

   ```
   /mps/mas_recovery/mas_recovery.py
   ```

3. 按照适用于 NetScaler ADM 独立部署恢复脚本的步骤 2 中的过程进行操作

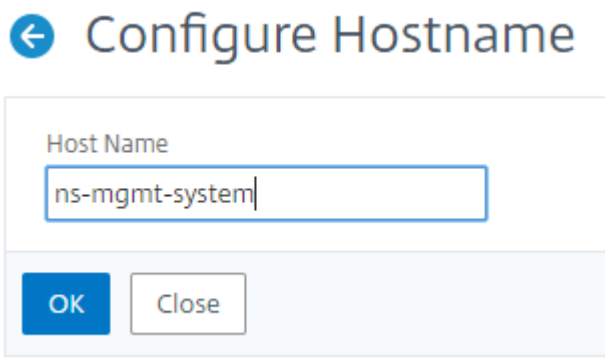
为 **NetScaler ADM** 服务器分配主机名

February 6, 2024

要识别 NetScaler Application Delivery Management (ADM) 服务器，可以为该服务器分配主机名。主机名将显示在 NetScaler ADM 的通用许可证上。

要为 **NetScaler ADM** 服务器分配主机名，请执行以下操作：

1. 在 NetScaler 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”。



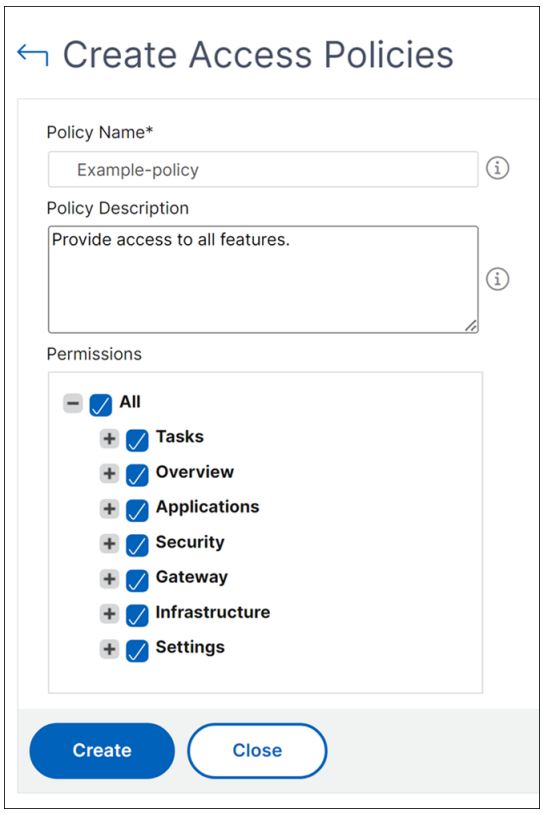
> 注意
>
> 您也可以在虚拟机管理程序中使用 `networkconfig` 命令并更改主机名。

备份和还原您的 **NetScaler ADM** 服务器

February 6, 2024

您可以定期备份您的 NetScaler ADM 服务器。您可以备份和还原配置文件、实例详细信息、系统数据等。

> 重要
>
> 信息 Citrix 建议您使用相同版本的备份还原 ADM 服务器。例如，如果 ADM 版本为 13.0，则使用 13.0 ADM 备份来还原服务器。
>
> 用户对备份和还原 ADM 服务器的访问权限受到限制。“设置”>“备份文件”页面仅对有权访问所有 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。



有关详细信息，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：

- NetScaler 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
- NetScaler ADM 服务器管理的 NetScaler 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 NetScaler 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。

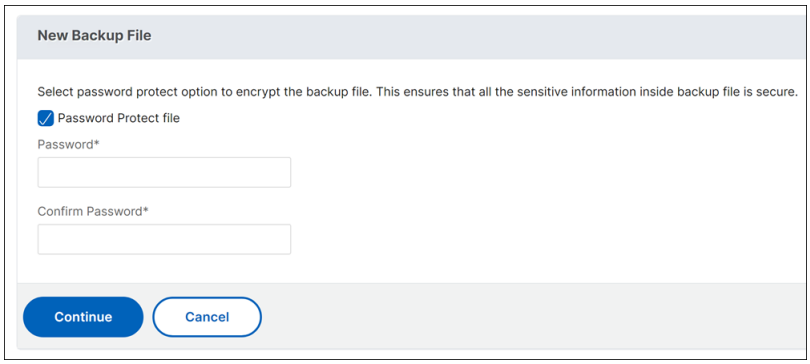
备份 **NetScaler ADM** 配置

默认情况下，NetScaler ADM 服务器每 24 小时（00.30 小时）备份一次配置。您也可以安排和选择备份时间。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 NetScaler ADM 服务器上存储 10 个备份文件。但是，作为预防措施，Citrix 建议您在服务器上存储备份文件的一些副本或 将文件传输到另一个系统 。

要备份 **NetScaler ADM** 配置，请执行以下操作：

1. 导航到“设置” **>** “备份文件”，然后单击“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。

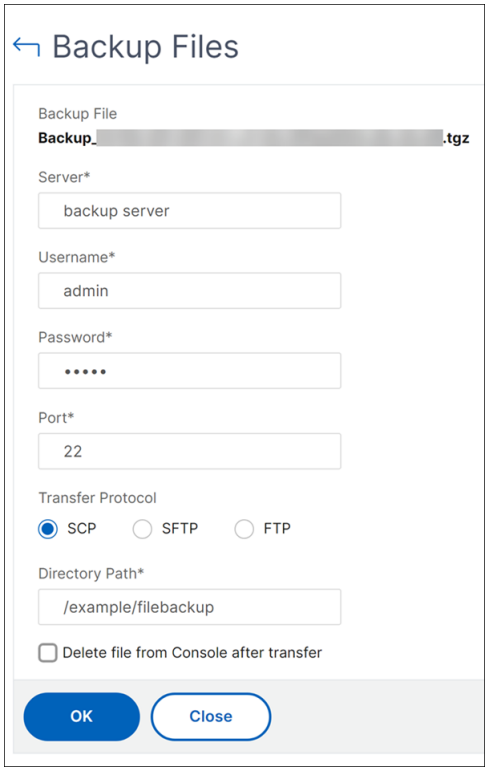


将 **NetScaler ADM** 备份文件传输到外部系统

可以将备份文件副本传输到另一个系统上作为预防措施。要还原配置时，请先将文件上载到 NetScaler ADM 服务器，然后执行 还原操作。

要传输 **NetScaler ADM** 备份文件，请执行以下操作：

1. 导航到“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”页面上，指定以下参数：
   - 服务器 -您要传输备份文件的系统的 IP 地址。
   - 用户名和密码 -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。
4. 通过选中“传输后从 **Application Delivery Management** 中删除文件”复选框，可以在传输后从 NetScaler 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“设置”**>**“备份文件”，选择要复制的文件，然后单击“下载”。

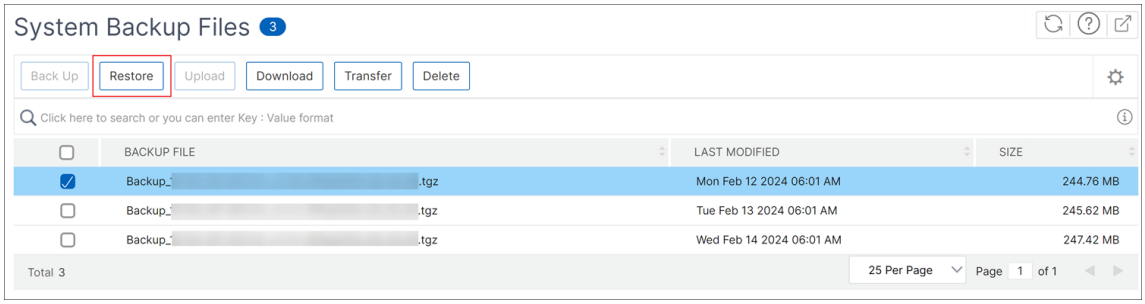
从备份文件还原 **NetScaler ADM** 配置

当您从先前备份的文件恢复 NetScaler ADM 配置时，还原操作会解压缩备份文件，然后还原配置。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了备份文件内容，则还原操作将失败。

要从备份文件还原 **NetScaler ADM** 配置，请执行以下操作：

1. 导航到“设置” **>** “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载到 ADM 服务器。要上载文件，请导航到“设置” **>** “备份文件”，然后单击“上载”。

高可用性部署中 **NetScaler ADM** 的 **VM** 快照

February 6, 2024

在开始升级之前，您可以在 HA 部署中拍摄 NetScaler ADM 服务器的快照。快照会捕获您拍摄虚拟机时的整个状态。

拍下 **NetScaler ADM** 服务器的快照

按照以下顺序拍摄 NetScaler ADM 服务器的快照：

1. NetScaler ADM 辅助服务器
2. NetScaler ADM 主服务器

要拍摄 **NetScaler ADM** 服务器的快照，请执行以下操作：

1. 在虚拟机管理程序上，从虚拟机列表中选择 NetScaler ADM 辅助服务器。
2. 创建 VM 快照。
3. 为快照命名一个有意义的名称，并在需要时输入描述。

   快照存储在默认 VM 目录中。
4. 对主服务器重复相同的步骤。

> 注意：
>
> 拍摄快照时不必关闭虚拟机的电源。

恢复 **NetScaler ADM** 服务器的快照

还原快照时，可以将虚拟机的内存、设置和虚拟机磁盘的状态恢复到拍摄快照时的状态。

使用以下顺序恢复 NetScaler ADM 服务器的快照：

1. NetScaler ADM 主服务器
2. NetScaler ADM 辅助服务器

要恢复 **NetScaler ADM** 服务器的快照，请执行以下操作：

1. 在虚拟机管理程序上，从虚拟机列表中选择 NetScaler ADM 主服务器。
2. 右键单击 VM 并恢复快照。

   虚拟机将恢复到最新的快照。
3. 对 NetScaler ADM 辅助服务器重复相同的步骤。

查看审核信息

January 29, 2024

Syslog 是日志记录标准协议。它有两个组件：在 Citrix Application Delivery Controller (ADC) 实例上运行的 Syslog 审核模块和 Syslog 服务器，它可以在 NetScaler 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。

如果您将 NetScaler 设备配置为将 syslog 消息重定向到 NetScaler Application Delivery Management (ADM)，则可以监视 NetScaler 设备生成的 syslog 消息。您可以使用 NetScaler ADM 中的内置模板功能安排作业来创建生成不同类型 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 **NetScaler ADM** 上配置 **syslog** 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 **Syslog** 服务器。或者您可以导航到“系统”>“审核”>“**syslog** 服务器”。
2. 在 **Syslog** 服务器 页面中，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 **NetScaler ADM** 上配置 **syslog** 日期和时间格式，请执行以下操作：

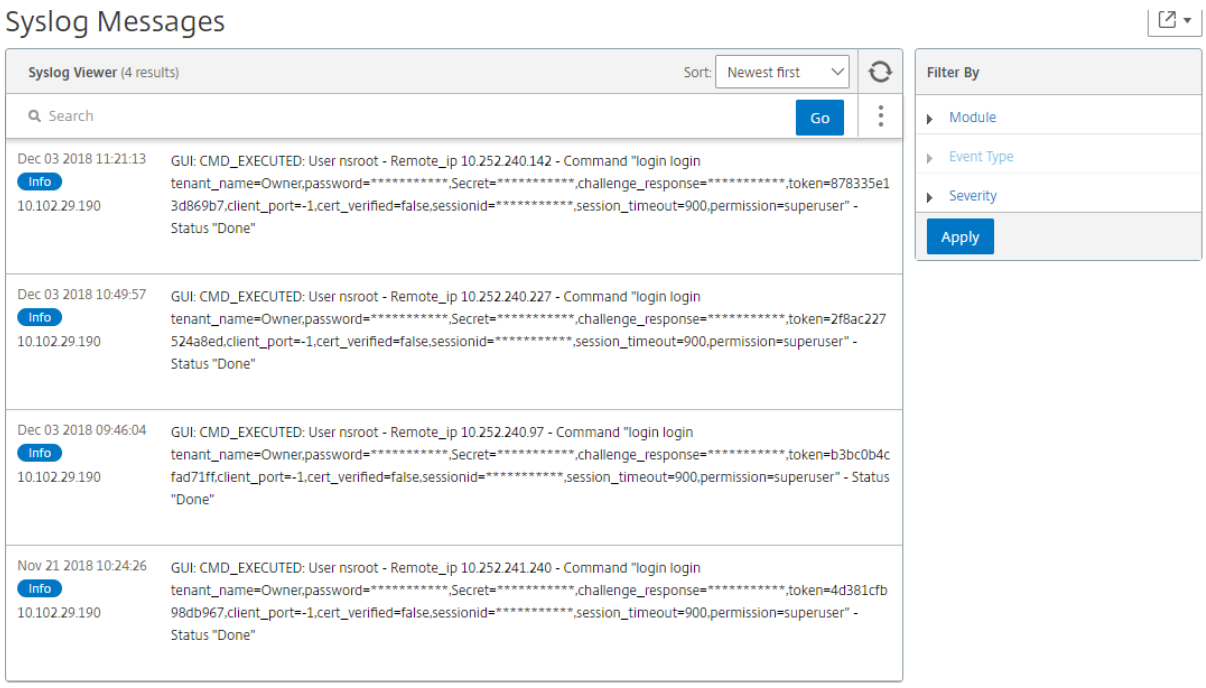
1. 导航到“系统”>“审核”。在“配置摘要”下，选择 **Syslog** 服务器。
2. 在 **Syslog** 服务器页面中，选择一个 syslog 服务器，然后单击 S**yslog** 参数。
3. 在 **Configure Syslog Parameters**（配置 Syslog 参数）页面上，指定日期和时间格式。
4. 单击确定。

要在 **NetScaler ADM** 上查看 **syslog** 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 NetScaler ADM 服务器，则现在可以查看在托管 NetScaler 实例上生成的所有 syslog 消息。syslog 消息集中存储在 NetScaler ADM 服务器的数据库中，并将在 Syslog Viewer 上用于审核目的。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 **Syslog** 查看器，请导航到“系统”>“审核”。在“审核”页面的“审核消息”下，选择 **Syslog** 消息。选择合适的过滤器以查看您的 syslog 消息。



配置 **SSL** 设置

February 6, 2024

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 NetScaler 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 **NetScaler 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，查看当前的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“**确定”，然后单击“关闭**”。

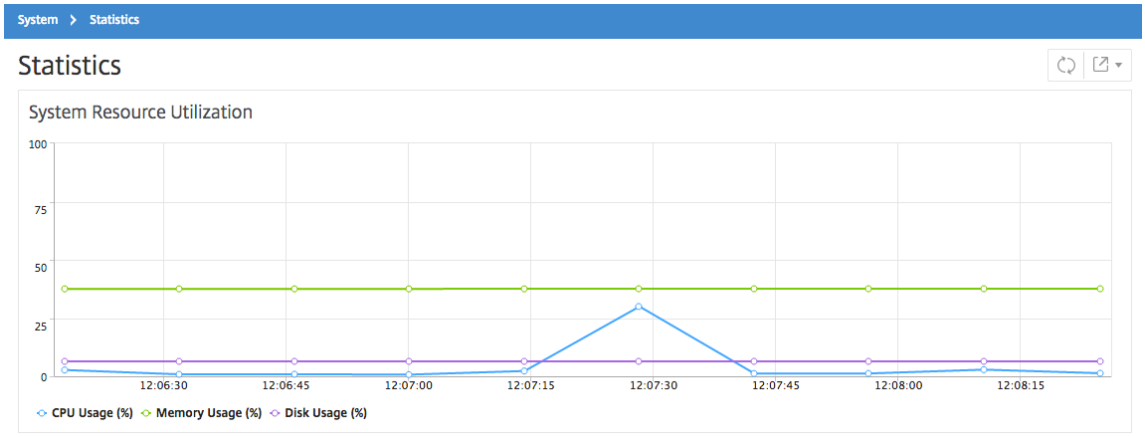
监视 **CPU**、内存和磁盘使用情况

January 29, 2024

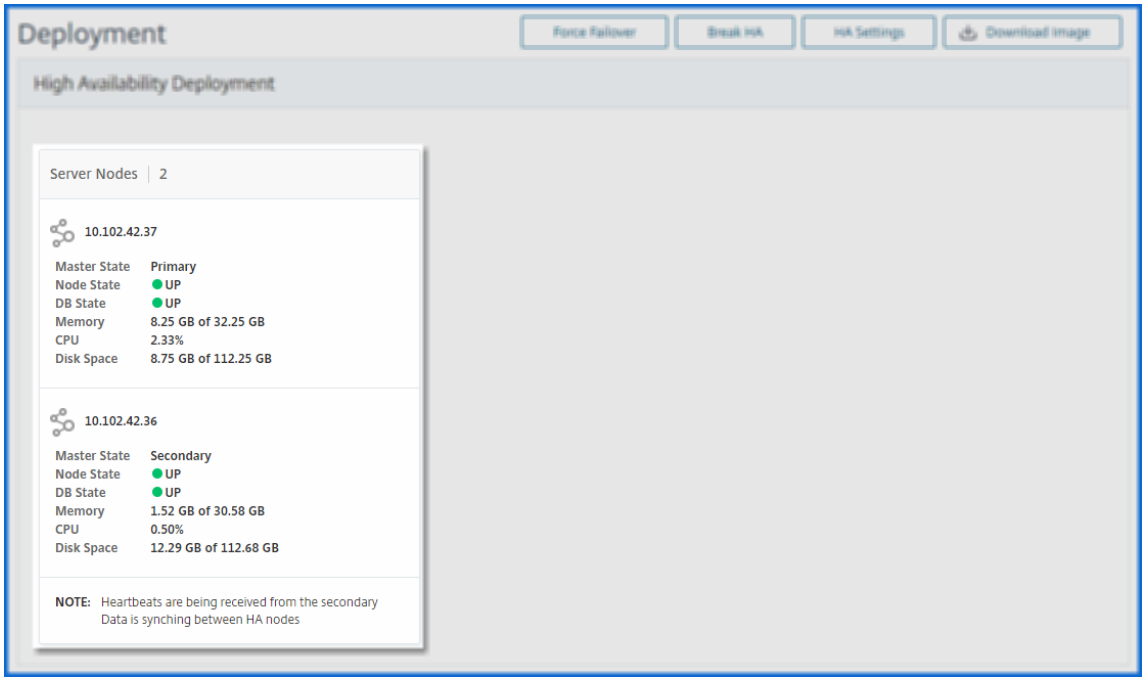
您可以使用日志和统计信息中保存的信息。此信息还显示在帮助您配置和维护 NetScaler Application Delivery Management (ADM) 的报告中。

要监视 CPU、内存和磁盘使用情况，

- 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“设置”**>**“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

January 29, 2024

您可以选择通知类型来接收以下功能的通知：

- 事件—为 NetScaler 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、即将到期等的许可证列表。有关详细信息，请参阅 NetScaler ADM 许可证到期。
- **SSL** 证书—添加到 NetScaler 实例的 SSL 证书列表。有关详细信息，请参阅 SSL 证书过期

ADM 支持以下通知类型：

- 电子邮件
- SMS
- Slack
- PagerDuty
- ServiceNow

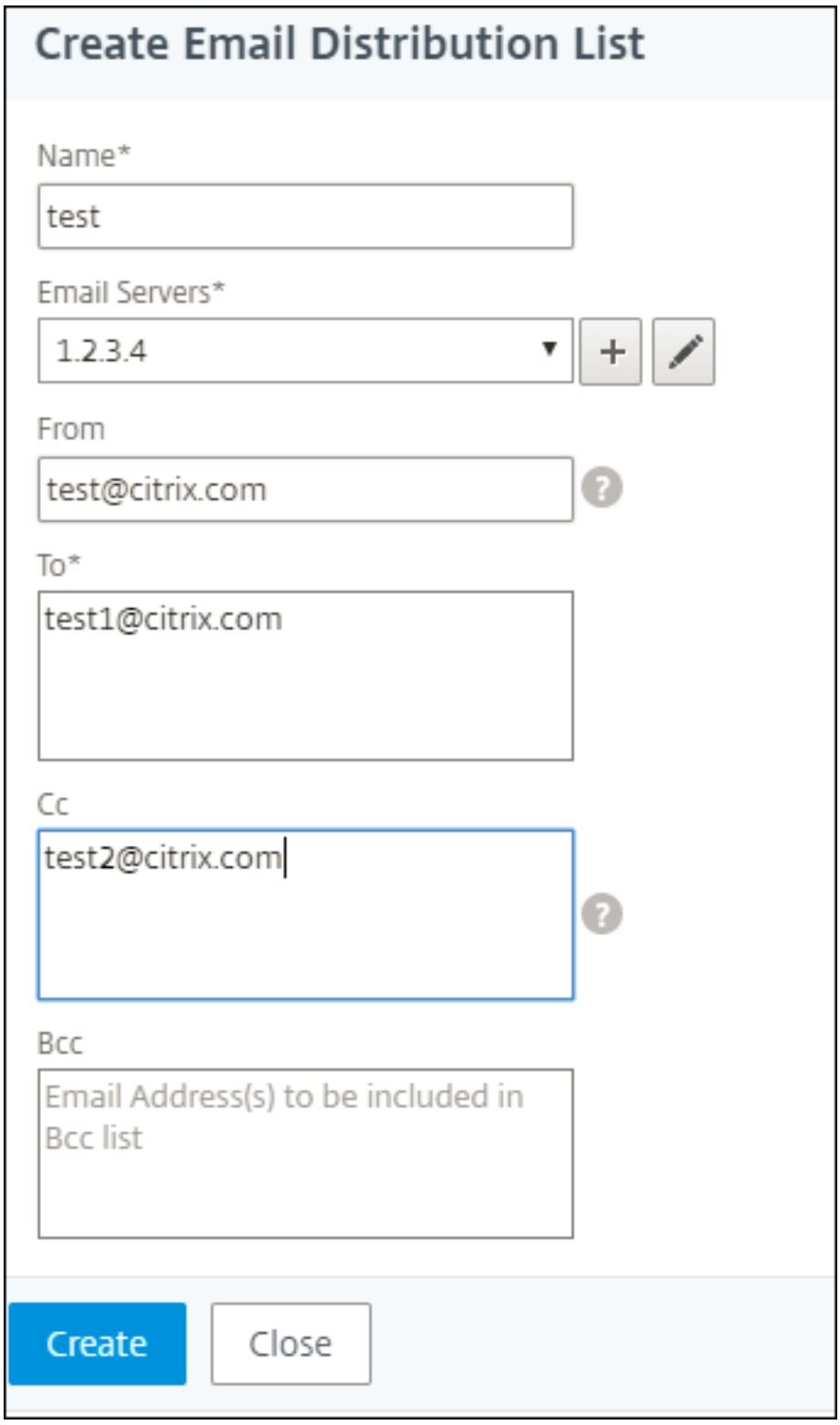
对于每种通知类型，ADM GUI 会显示已配置的分发列表或配置文件。ADM 向选定的分发列表或个人资料发送通知。

创建电子邮件通讯组列表

要接收有关 ADM 功能的电子邮件通知，必须添加电子邮件服务器和分发列表。

执行以下步骤创建电子邮件通讯组列表：

1. 导航到“设置”**>**“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。
    - **Cc** -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 在不显示地址的情况下必须将邮件副本发送到的电子邮件地址。



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分发列表。

创建 **SMS** 分发列表

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“设置”**>**“通知”。
2. 在 **SMS** 中，单击 添加。
3. 在“创建 **SMS** 分发列表”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。

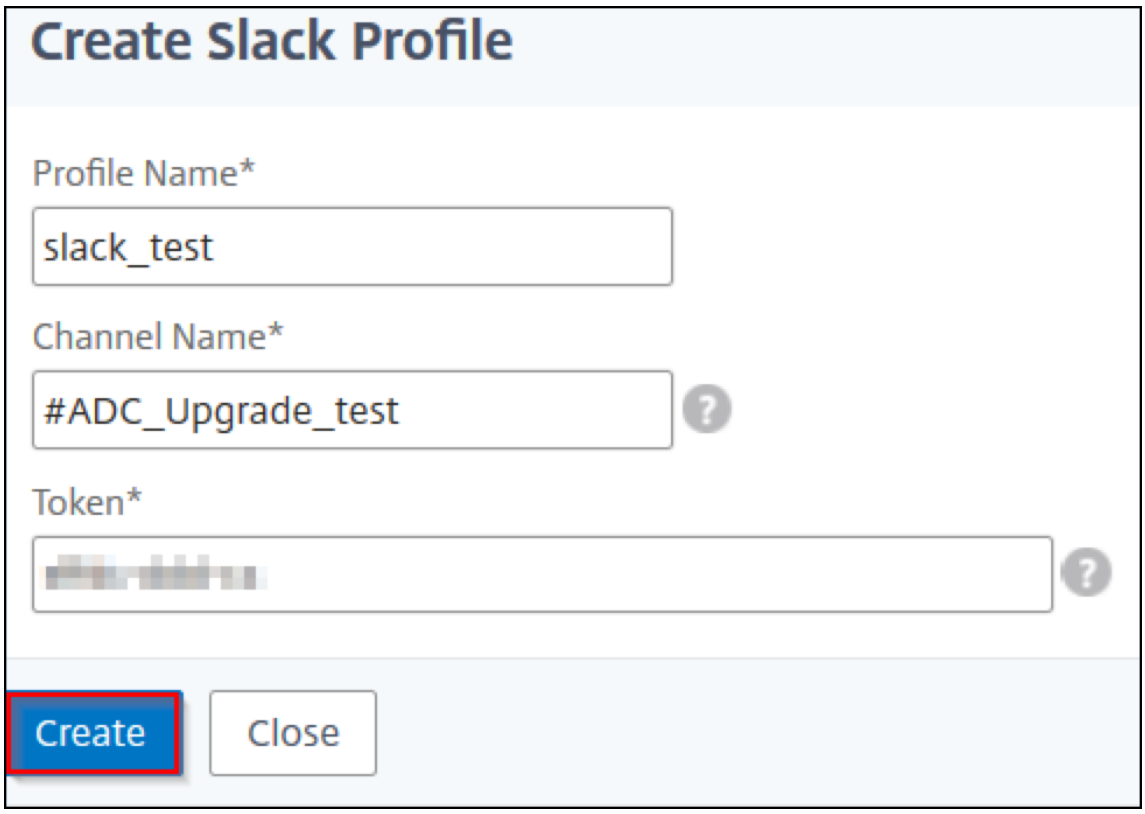
重复此步骤创建多个 SMS 通讯组列表。**SMS** 选项卡显示 ADM 中存在的所有 SMS 分发列表。

创建 **Slack** 配置文件

要接收 ADM 功能的 Slack 通知，必须创建 slack 配置文件。

执行以下步骤来创建“Slack”配置文件：

1. 导航到“设置”**>**“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。
    - 频道名称 -指定 ADM 必须向其发送通知的 Slack 频道名称。
    - **Webhook URL** -指定该频道的 Webhook URL。传入的 Webhook 是将来自外部来源的消息发布到 Slack 的简单方法。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。下面是 webhook 的示例：https://hooks.slack.com/services/T0******E/B9X55DUMQ/c4tewWAiGVTT51Fl6oEOVirK



4. 单击创建。

重复此过程创建多个 Slack 配置文件。**Slack** 选项卡显示了 ADM 中存在的所有 Slack 配置文件。

创建 **PagerDuty** 配置文件

您可以添加 PagerDuty 配置文件来监视基于 PagerDuty 配置的事件通知。使用 PagerDuty，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 NetScaler 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 PagerDuty，请参阅 PagerDuty 文档。

请执行以下步骤来创建 PagerDuty 配置文件：

1. 导航到“设置”**>**“通知”。
2. 在“**PagerDuty**”中，单击“添加”。
3. 在 创建 **PagerDuty** 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 PagerDuty 门户网站获取此密钥。
4. 单击创建。

有关更多信息，请参阅 PagerDuty 文档中的 服务和集成 。

重复此过程以创建多个 PagerDuty 配置文件。**PagerDuty** 选项卡显示了 ADM 中存在的所有 PagerDuty 配置文件。

查看 **ServiceNow** 配置文件

如果要为 NetScaler 事件和 ADM 事件启用 ServiceNow 通知，则必须使用 ITSM 连接器将 NetScaler ADM 与 ServiceNow 集成。有关更多信息，请参阅 将 NetScaler 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“设置”**>**“通知”。
2. 在“**ServiceNow**”中，从列表中选择 **Citrix_Workspace_SN** 配置文件。
3. 单击“测试”自动生成 ServiceNow 票证并验证配置。

   如果要在 NetScaler ADM GUI 中查看 ServiceNow 票证，请选择 **ServiceNow** 票证。

生成技术支持文件

February 6, 2024

Citrix 建议您在联系技术支持部门调试问题之前，生成 NetScaler Application Delivery Management (ADM) 数据和统计数据存档。存档是可以发送给技术支持团队的 TAR 文件。

> 注意
>
> 对于处于高可用性模式的 NetScaler 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。

要配置和发送来自 **NetScaler ADM** 的技术支持文件，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。

```
The archive file is created as a TAR file.

```



```
3   For example, the archive file that is created might be named as
       follows:   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，然后使用 Web 浏览器上载到 Citrix Insight Services (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载到 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/collector_upload.pl

下面给出了完整的命令，其中包含您需要提供的属性：

```
1  /mps/collector_upload.pl [-proxy [<proxy_user>:<proxy_password>@]<
      proxy_host>:<proxy_port>] [-user <user>] [-password <password>] [-sr
       <sr>] [-description <description>] [-debug] <file>
2  <!--NeedCopy-->
```

运行 Perl 脚本的好处是您不必将技术支持文件从 ADM 下载到本地系统，然后将其上载到 CIS。作为一种选择，您可以使用来自 ADM 控制台的代理将文件直接上载到 CIS。

确保您在 CIS 上有一个帐户。您可以使用您的 Citrix 帐户凭据将文件上载到 CIS。

如果您没有代理服务器怎么办？或者，如果您在使用 SSL 转发代理时遇到了一些问题怎么办？（如果 Perl 脚本不信任代理服务器的根证书，就会发生这种情况。）
您仍然可以将文件直接从 ADM 外壳上载到 CIS。

> 注意
>
> 在 ADM 无法从控制台将文件上载到 CIS 的情况下，您仍然可以下载文件并通过电子邮件将其发送给 Citrix 技术支持团队。或者，您可以将文件从 ADM 下载到本地存储，然后使用 Web 浏览器上载到 CIS。

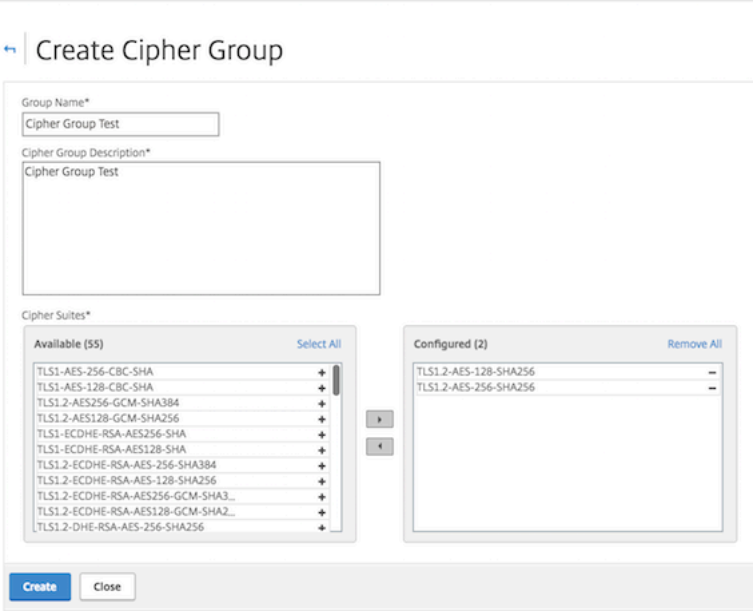
配置密码组

January 29, 2024

密码组是绑定到 Citrix Application 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 **NetScaler ADM** 上添加密码组，请执行以下操作：

1. 导航到“设置”**>**“管理”
2. 在“**SSL** 设置”下，单击“密码组”
3. 单击 **Add**（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

February 6, 2024

每当 NetScaler ADM 上出现异常情况时，就会生成 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。在这里，NetScaler ADM 被配置为陷阱目的地。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 **NetScaler ADM** 上创建 **SNMP** 陷阱目的地，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”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。陷阱目的地的名称或 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
>
> 如果您正在创建 SNMP v3 陷阱目的地，请指定要将陷阱绑定到的 SNMP 用户凭据。要添加 SNMP 用户凭据，请单击“插入”，然后从可用 SNMP 用户列表中添加用户。

要创建 **SNMP** 管理员社区，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”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。指定向陷阱侦听器发送陷阱时要使用的社区字符串。
3. 或者，您可以选中“启用管理网络”复选框来指定网络 掩码，即 SNMP 管理器网络的子网掩码。
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

February 6, 2024

您可以启用和配置一组警报来监视 NetScaler 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。

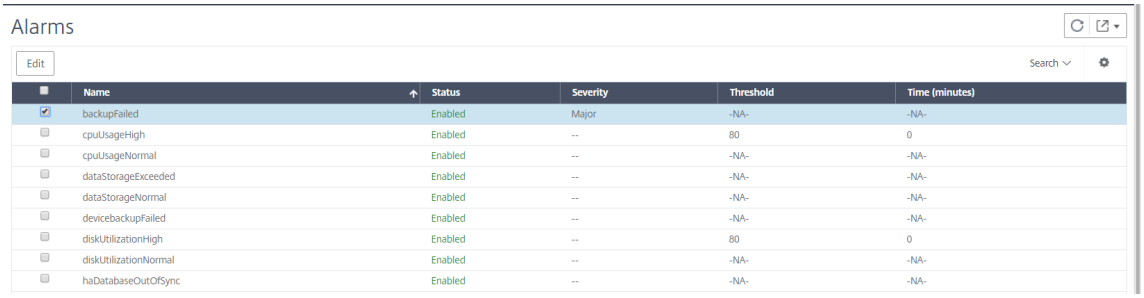
可以分配或修改警报的严重性。您可以分配的严重性级别为“严重”、“严重”、“次要”、“警告”和“信息”。

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 NetScaler 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 NetScaler 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，必须选择 BackupFailed 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 **NetScaler ADM** 配置和查看系统警报，请执行以下操作：

1. 导航到“设置”**>**“**SNMP**”。单击右上角的“警报”。

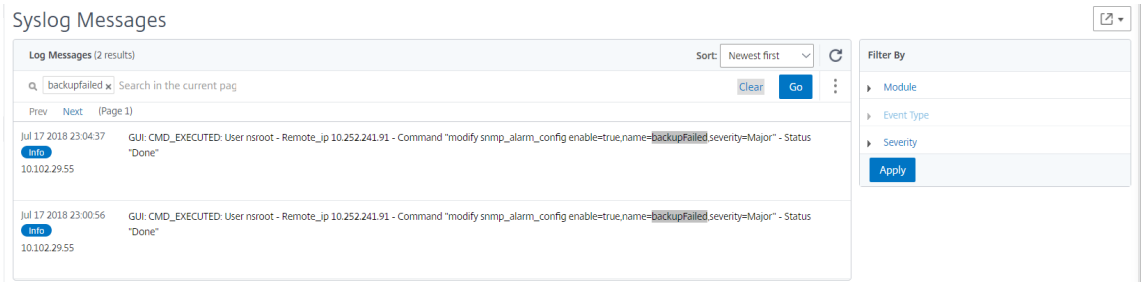


2. 选择要配置的警报（例如，备份失败），然后单击“编辑”修改其设置。
3. 默认情况下，启用警报。分配严重性级别（例如：主要），然后单击“确定”。

> 注意
>
> 对于少数警报，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 **NetScaler ADM** 查看 **BackupFailed** 警报生成的事件，请执行以下操作：

1. 导航到“系统”>“审核”。
2. 在“审核”页面的“审核消息”下，选择 **Syslog** 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 NetScaler ADM 的系统通知设置。

为 **NetScaler ADM** 代理创建 **SNMP** 管理器和用户

January 29, 2024

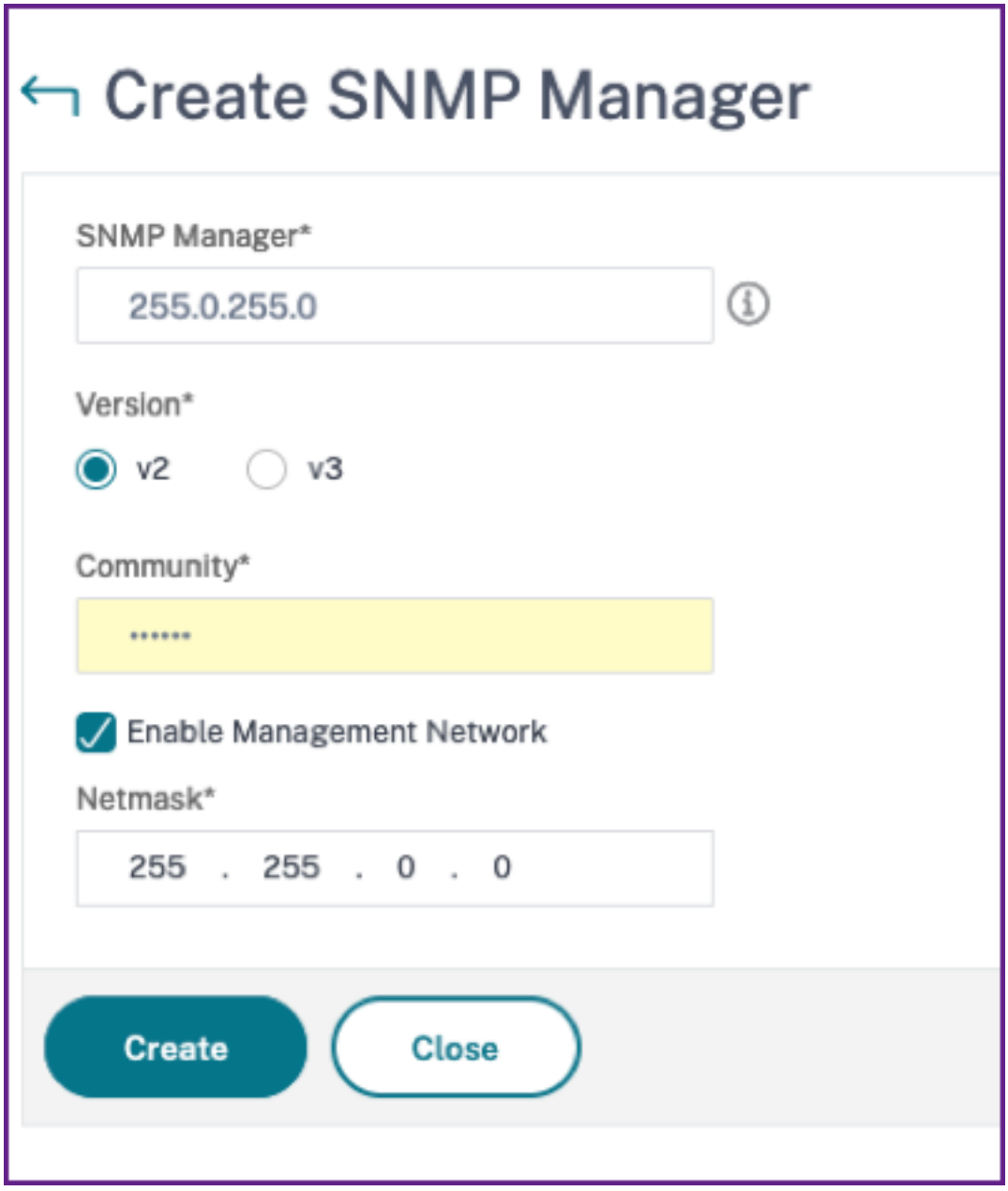
您可以从名为 SNMP 管理器的远程设备向 S NMP 代理查询系统特定信息。该代理随后会在管理信息库 (MIB) 搜索请求的数据，并将其发送到 SNMP 管理器。

您可以添加 SNMP 管理器来查询 NetScaler ADM 代理。管理器符合 SNMP V2 和 V3 的要求。如果您指定一个或多个 SNMP 管理器，则 NetScaler ADM 代理不接受来自除指定的 SNMP 管理器之外的任何主机的 SNMP 查询。

添加 **SNMP v2** 管理器

要为 NetScaler ADM 代理添加 SNMP v2 管理器，请执行以下操作：

1. 导航到 基础架构 **>** 代理，选择 NetScaler ADM 代理，然后单击 选择操作 > 管理 SNMP。
2. 在 **SNMP> SNMP** 管理器选项卡中，单击“添加”。
3. 在“创建 **SNMP** 管理器”页面中，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。
   - 版本。选择 v2。
   - 社区。输入社区名称。SNMP 社区配置对来自 SNMP 管理器的 SNMP 查询进行身份验证。
   - 启用管理网络：选中此复选框可指定 SNMP 管理器网络的网络掩码。
   - 网络掩码：输入与 IP 地址关联的子网掩码。
4. 单击创建。



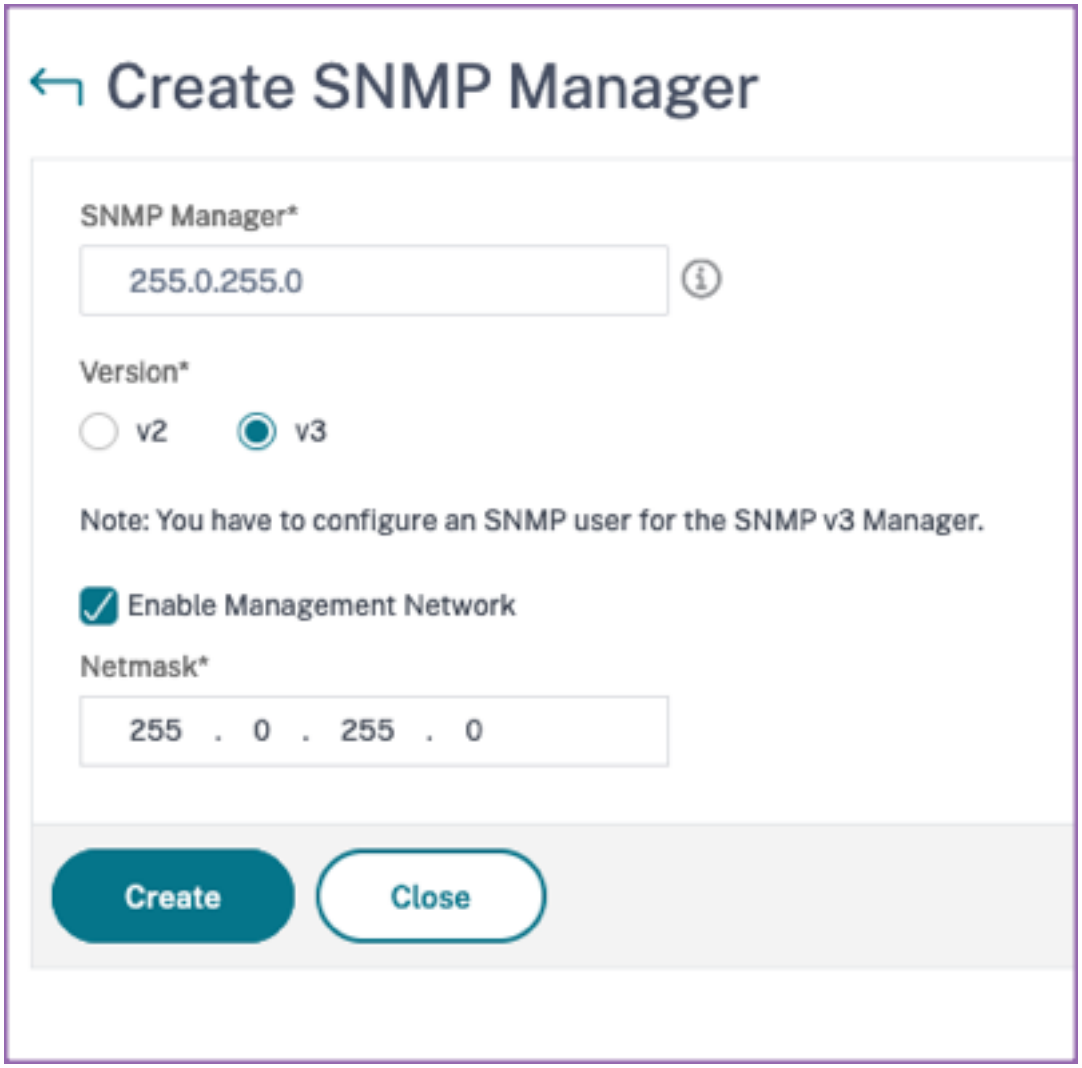
添加 **SNMP v3** 管理器

要为 NetScaler ADM 代理添加 SNMP v3 管理器，请执行以下操作：

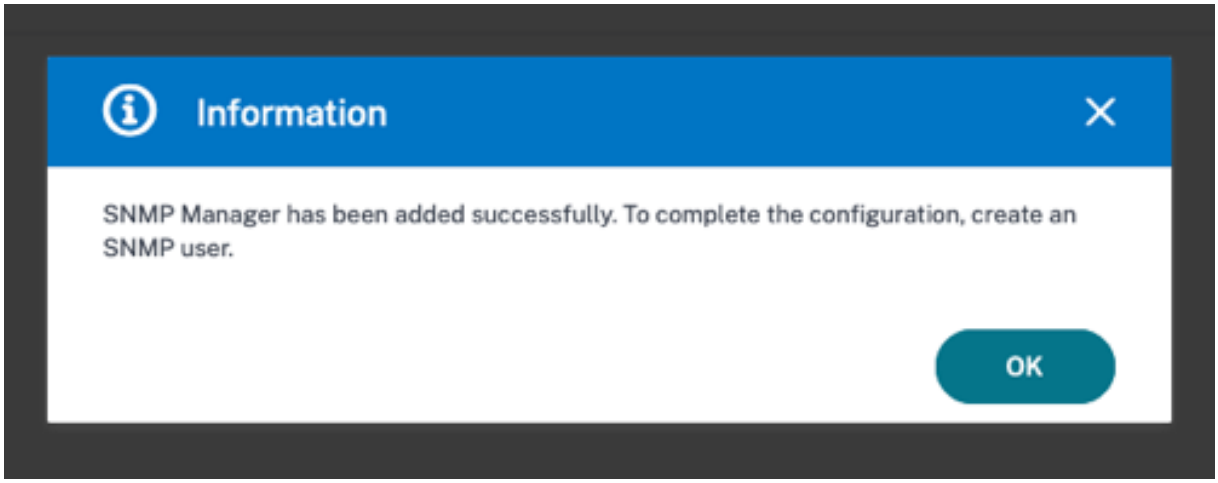
1. 导航到 基础架构 **>** 代理，选择 NetScaler ADM 代理，然后单击 选择操作 > 管理 SNMP。
2. 在 **SNMP> SNMP** 管理器选项卡中，单击“添加”。
3. 在“创建 **SNMP** 管理器”页面中，指定以下详细信息：
    - **SNMP** 管理器。输入 SNMP 管理器的名称或 IP 地址。

- 版本。选择 v3。
- 启用管理网络：选中此复选框可指定 SNMP 管理器网络的网络掩码。
- 网络掩码：输入与 IP 地址关联的子网掩码。

4. 单击创建。



出现一个对话框，确认已创建 SNMP 管理器并提示您配置 SNMP 用户。



> 注意
>
> 必须为 SNMP v3 管理器配置 SNMP 用户。要配置 SNMP 用户，请转到 **SNMP > SNMP** 用户。

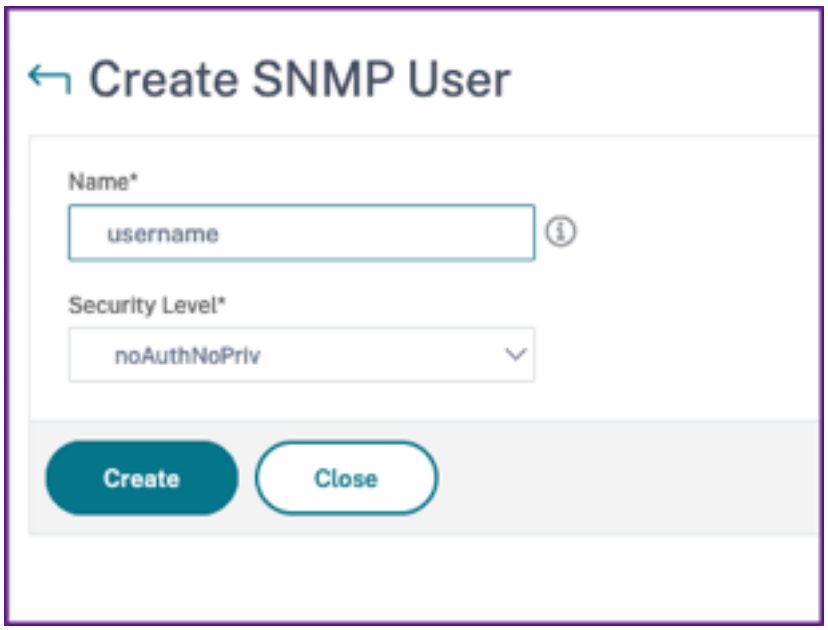
添加 **SNMP** 用户

添加一个 SNMP 用户来回应来自 SNMP 管理器的 SNMP v3 查询。

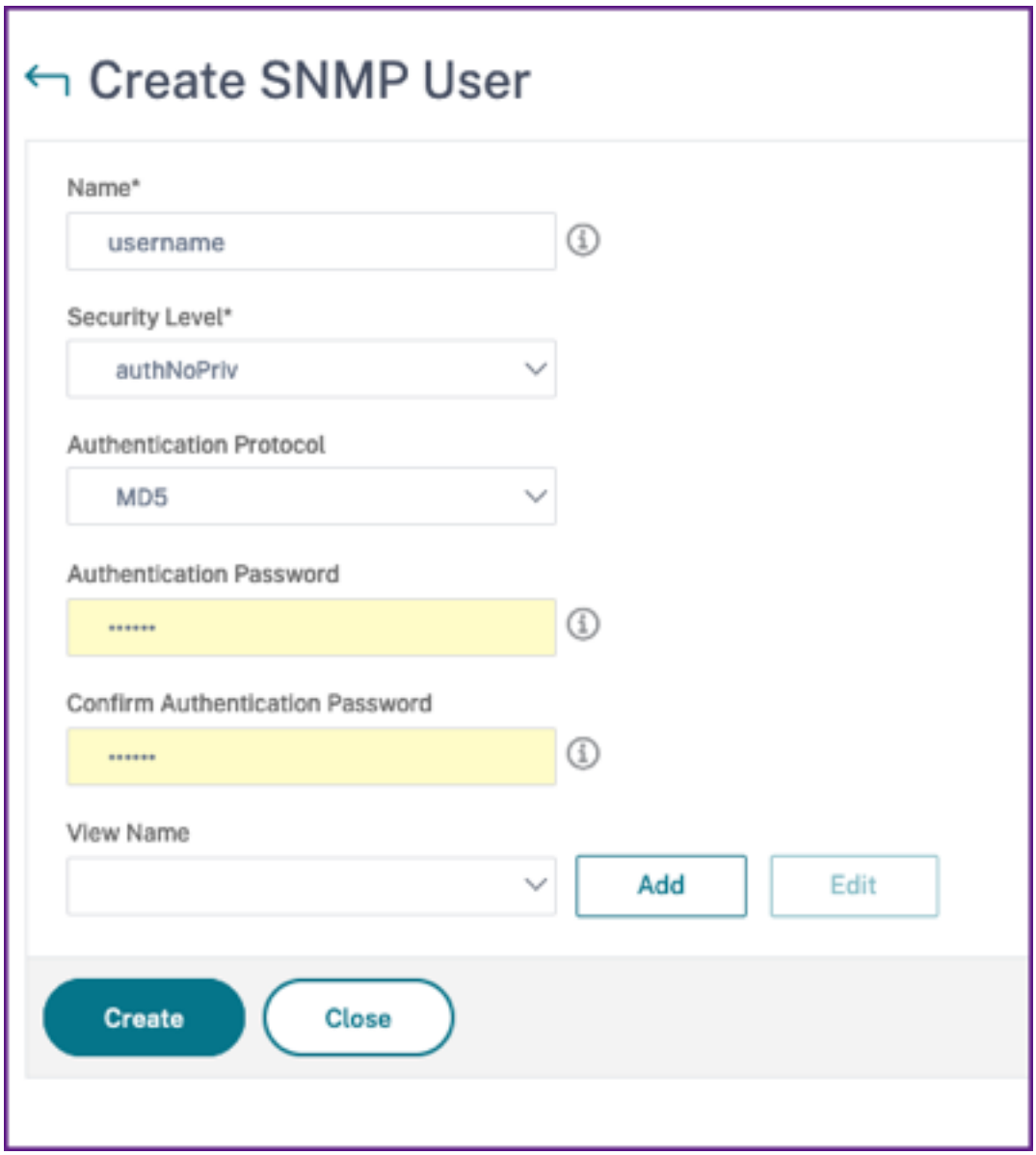
要为 NetScaler ADM 代理添加 SNMP 用户，请执行以下操作：

1. 导航到 基础架构 **>** 代理，选择 NetScaler ADM 代理，然后单击 选择操作 > 管理 SNMP。
2. 在 **SNMP > SNMP** 用户选项卡中，单击“添加”。
3. 在 创建 **SNMP** 用户 页面中，添加以下详细信息：
    - 名称。输入用户名。
    - 安全级别。NetScaler ADM 代理与 SNMP 管理器之间的通信所需的安全级别。

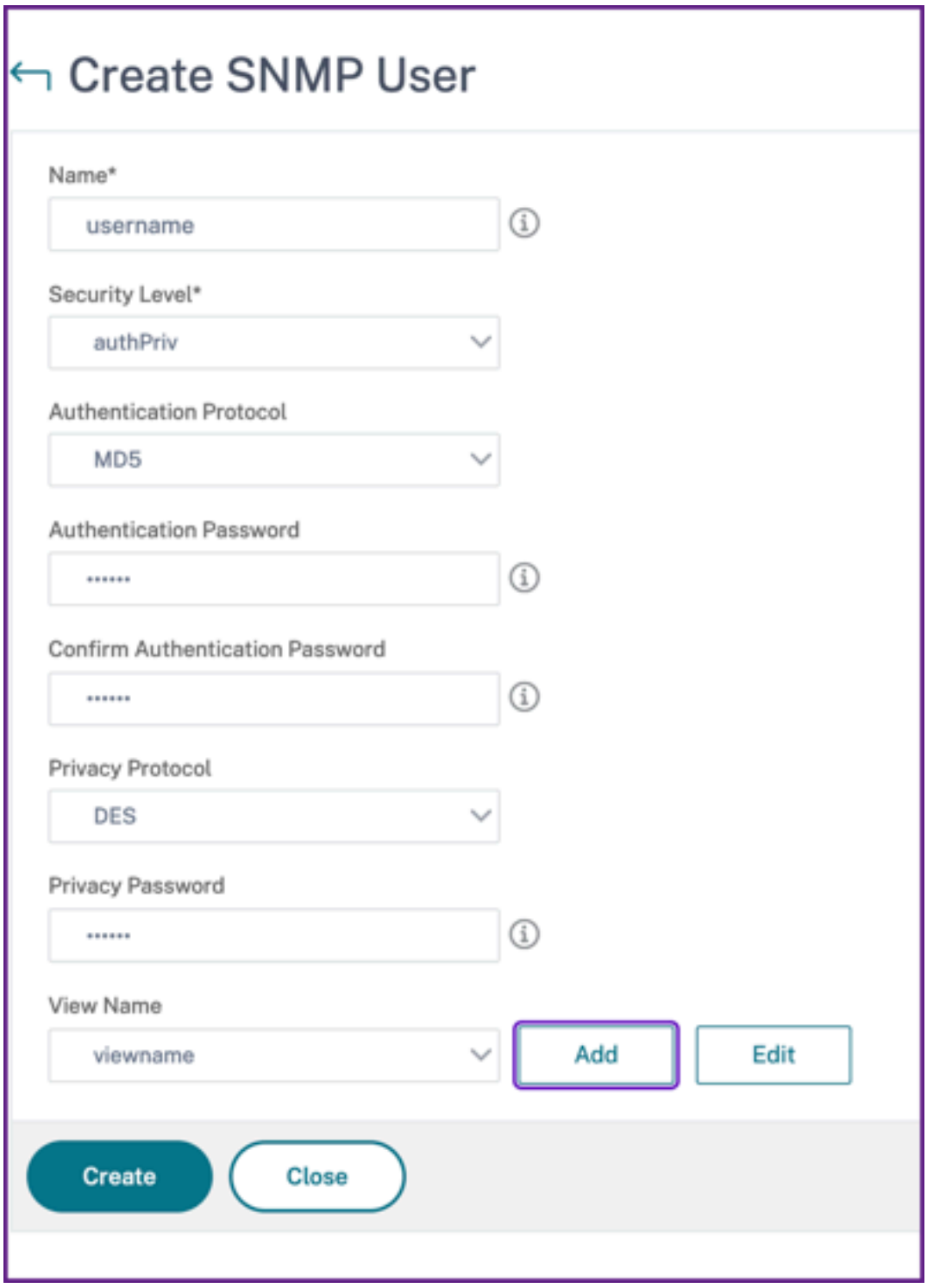
      选择以下安全级别之一：
    - **noAuthNoPriv**. 既不需要身份验证，也不需要加密。



- **authNoPriv**. 需要身份验证但不需要加密。



- **authPriv**。需要身份验证和加密。



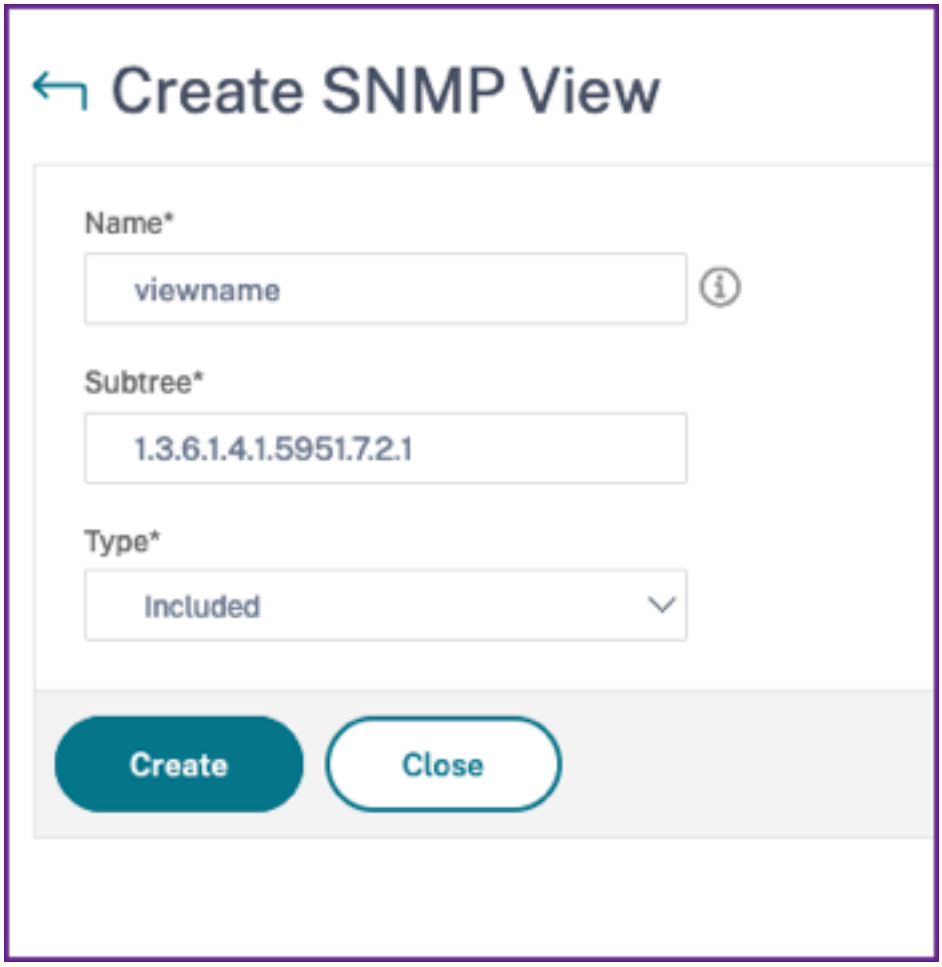
根据您分配给用户的安全级别，提供额外的身份验证协议，如身份验证协议、隐私密码和分配 SNMP 视图。

管理 **SNMP** 视图

SNMP 视图用于实现 SNMP 用户的访问控制。SNMP 视图限制用户访问 MIB 的特定部分。

要允许或限制 NetScaler ADM 代理的 SNMP OID，请执行以下操作：

1. 导航到 基础架构 **>** 代理 **>** 管理 **SNMP** ，然后在 **SNMP** 视图选项卡中单击添加。
2. 在 创建 **SNMP** 视图中，输入以下详细信息：
   - 视图名称：SNMP 视图的名称。一个实例可以有许多同名的 SNMP 视图，这些视图因素树参数设置而有所区别。
   - 子树：要与此 SNMP 视图关联的 MIB 树的特定分支（子树）。必须将子树指定为 SNMP OID。
   - 类型：此字段允许您在视图中包含或排除子树。
3. 单击创建。



配置代理设置

February 6, 2024

您可以修改 NetScaler ADM 代理的保持连接间隔和密码更改要求。

设置座席的保持活动时间间隔

NetScaler ADM 服务器和代理在指定的保持活动时间间隔内维护相同的 TCP 连接。代理使用此连接将托管实例数据发送到 NetScaler ADM 服务器。

1. 导航到 **Settings**（设置）**> Administration**（管理）。
2. 在“系统配置”下选择“系统”、“时区”、“允许的 **URL**”和“代理设置”。
3. 在 基本设置 **>** 代理设置中，指定 30—120 秒之间的保持连接间隔。
4. 单击保存。

在不使用当前密码的情况下更改代理的密码

您可以允许在不使用当前密码的情况下更改代理密码。

1. 导航到 **Settings**（设置）**> Administration**（管理）。
2. 在“系统配置”下选择“系统”、“时区”、“允许的 **URL**”和“代理设置”。
3. 在“基本设置”**>**“代理设置”**>**“删除更改代理密码的当前密码先决条件”复选框中，您可以执行以下操作：
   - 选中该复选框可删除“更改代理密码”页面中的“当前密码”字段。
   - 清除该复选框可保留“更改代理密码”页面中的“当前密码”字段。
4. 单击保存。

> 注意
>
> 要查看“更改代理密码”页面，请导航到 基础架构 **>** 实例代理，选择代理，然后单击 选择操作 **>** 更改密码。

作为 **API** 代理服务器的 **NetScaler ADM**

February 6, 2024

除了能够接收有关其自身管理和分析功能的 NITRO REST API 请求外，NetScaler Application Delivery Management (NetScaler ADM) 还可以充当其托管实例的 REST API 代理服务器。REST API 客户端可以向 NetScaler ADM 发送 API 请求，而不是直接向托管实例发送 API 请求。NetScaler ADM 可以区分它必须响应的 API 请求和必须原封不动地转发到托管实例的 API 请求。

作为 API 代理服务器，NetScaler ADM 为您提供以下好处：

- 验证 **API** 请求。NetScaler ADM 根据已配置的安全和基于角色的访问控制 (RBAC) 策略对所有 API 请求进行验证。NetScaler ADM 还具有租户感知能力，可确保 API 活动不会跨越租户边界。

- 集中审核。NetScaler 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。NetScaler ADM 使 API 客户端不必维护与托管实例的会话的任务。

NetScaler ADM 如何作为 **API** 代理服务器工作

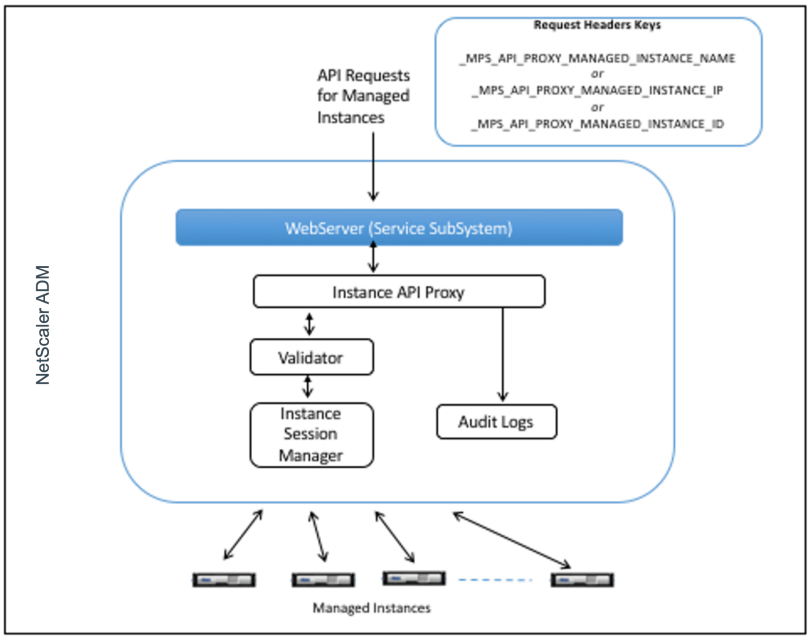
如果希望 NetScaler ADM 将请求转发到托管实例，则可以将 API 客户端配置为在 API 请求中包含以下任何一个 HTTP 标头：

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_SESSID	访问托管实例的会话 ID。

> 注意
>
> 在“设置”**>**“管理”**>**“系统配置”**>**“基本设置”中，如果选择了 提示实例登录凭据，请确保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 NetScaler ADM 将 API 请求识别为它必须转发给托管实例的 API 请求。标头的值有助于 NetScaler ADM 识别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，NetScaler ADM 按如下方式处理请求：

1. 在不修改请求的情况下，NetScaler 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，NetScaler 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。请执行以下操作：
>
> 1. 导航到 **Settings**（设置）**> Administration**（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 **NetScaler ADM** 用作 **API** 代理服务器

以下示例显示了 API 客户端向 IP 地址为 192.0.2.5 的 NetScaler ADM 服务器发送的 REST API 请求。需要 NetScaler ADM 将未更改的请求转发到 IP 地址为 192.0.2.10 的托管实例。所有示例都使用 _MPS_API_PROXY_MANAGED_INSTANCE_IP 标头。

在发送 NetScaler ADM API 请求之前，API 客户端必须：

- 登录 NetScaler ADM

- 获取会话 ID
- 在后续的 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-->
```

NetScaler ADM 使用包含会话 ID 的响应来响应登录请求。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",

      "session_timeout": "36000",

      "challenge_token": "",

      "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 NetScaler 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 NetScaler 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
```



```
    {

         "lbvserver":{

             "name":"sample_lbvserver",
             "servicetype":"HTTP",
             "ipv46":"10.102.1.11",
             "port":"80"
          }

     }

<!--NeedCopy-->
```

示例 **3**：修改负载平衡虚拟服务器

客户端必须向 NetScaler ADM 发送以下形式的 API 请求：

```
    PUT /nitro/v1/config/lbvserver
    Content-type: application/json
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

    {

       "lbvserver":{

            "name":"sample_lbvserver",
            "appflowlog":"DISABLED"
         }

     }

<!--NeedCopy-->
```

示例 **4**：删除负载平衡虚拟服务器

客户端必须向 NetScaler ADM 发送以下形式的 API 请求：

```
    DELETE /nitro/v1/config/lbvserver/sample_lbvserver
    Accept-type: application/json
    _MPS_API_PROXY_MANAGED_INSTANCE_IP: 192.0.2.10
    SESSID: ##
       D2BF9C5F40E5B2E884A9C45C89F0ADE24DA8A8169BE6358D39F5D471B73D

<!--NeedCopy-->
```


示例 **5**：在 **ADC** 上下载 **CLI** 运行配置

客户端必须向 NetScaler 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-->
```

常见问题解答

February 6, 2024

本节提供有关以下 NetScaler Application Delivery Management (NetScaler ADM) 功能的常见问题解答。单击下表中的功能名称可以查看该功能的常见问题解答列表。

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	样书
系统管理		

分析

是否需要在以单跳模式部署的 **NetScaler Gateway** 实例上启用 **EUEM** 虚拟通道

EUEM 虚拟通道数据是 NetScaler 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 NetScaler 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。

如何启用 **NetScaler ADM** 监视网络应用程序和虚拟桌面流量

1. 导航到基础架构 > 实例 > **NetScaler**，然后选择要启用分析的 NetScaler 实例。
2. 从 **Select Action**（选择操作）列表中，选择 **Configure Analytics**（配置分析）。

3. 在 配置分析 页面中，选择要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，请参阅如何在实例上启用分析。

> 注意
>
> 对于 11.0 版本、65.30 版本及更高版本的 NetScaler 实例，NetScaler ADM 上没有显式启用安全智能分析的选项。确保在 NetScaler 实例上配置 AppFlow 参数，以便 NetScaler 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 NetScaler 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。

添加 **NetScaler** 实例后，**NetScaler ADM** 是否会自动开始收集分析信息**?**

不。对 NetScaler ADM 管理的 NetScaler 实例中托管的虚拟服务器启用分析。有关更多详细信息，请参阅如何在实例上启用分析。

是否需要访问各个 **NetScaler** 设备才能启用分析

不是。所有配置均通过 NetScaler ADM 用户界面完成，该界面列出了特定 NetScaler 实例上托管的虚拟服务器。有关更多详细信息，请参阅如何在实例上启用分析。

可以在 **NetScaler** 实例上列出哪些虚拟服务器类型以启用分析**?**

当前，NetScaler 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 **NetScaler ADM**

要将额外的磁盘连接到 NetScaler ADM，请执行以下操作：

1. 关闭 NetScaler 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 NetScaler 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 NetScaler ADM 虚拟机 120 GB. 在这种情况下，必须连接 200 GB 而非 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、NetScaler 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 NetScaler ADM 虚拟机。

您所说的未在 **NetScaler** 实例上配置收集器是什么意思

收集器接收由 NetScaler 设备生成的 AppFlow 记录。

启用 AppFlow 功能后，NetScaler ADM 会接收来自 NetScaler 实例 Security Insight 察和 Web Insight 流量。在 NetScaler 实例上启用 AppFlow 功能时，必须至少指定一个 AppFlow 记录要发送到的收集器。如果未在 NetScaler 实例上配置收集器，则 NetScaler ADM 不会接收来自实例的流量。

例如，将五个 NetScaler 实例添加到 NetScaler ADM 中。如果未为两个实例指定收集器，则不会有流量流向 NetScaler ADM。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 功能的更多信息，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

身份验证请求的负载平衡是什么

身份验证服务器负载平衡功能使 NetScaler ADM 能够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。

是否需要级联外部身份验证服务器

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。

可以级联多少个外部身份验证服务器

您可以在 NetScaler ADM 中级联多达 32 个外部身份验证服务器。

外部身份验证失败时，是否有备用方法

可能会出现即使级联了几台服务器，外部身份验证仍彻底失败的情况。例如，外部服务器可能会变得不可访问，或者可能没有在其中任何一个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 回退本地身份验证。

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，NetScaler ADM 将访问本地用户数据库以对用户进行身份验证。

在 NetScaler ADM 中，导航到“设置”**>**“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 NetScaler 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 NetScaler ADM 上重新创建用户。

为什么需要指定组权限

使用 NetScaler 的负载平衡功能时，可以将 NetScaler 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 NetScaler ADM 并在 NetScaler 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 NetScaler 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。还要在 NetScaler ADM 中为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。可以分配的典型权限是管理 NetScaler 实例、NetScaler SDX 实例、虚拟服务器等权限，以便该组的用户只能管理那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。您甚至可以移除一个或多个用户组；其他组用户仍可在 NetScaler ADM 上运行。

配置管理

我能否使用 **NetScaler ADM** 同时在多个 **NetScaler** 实例上进行配置

是，可以使用配置作业在多个 NetScaler 实例之间执行配置。

NetScaler ADM 上的配置任务是什么

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。您可以创建任务以跨实例进行配置更改，在网络上的多个实例上复制配置，以及使用 NetScaler ADM GUI 录制和播放配置任务。还可以将录制的任务转换为 CLI 命令。

可以使用 NetScaler 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。

我能否在 **NetScaler ADM** 中使用内置模板安排作业

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 **NetScaler ADM** 删除 **SSL** 证书是否会导致从 **NetScaler** 实例中删除证书

否

部署

默认用户名和密码是什么**?**

- 完成初始网络配置后，您可以使用默认用户名和密码 (nsrecover/nsroot) 从虚拟机管理程序或 SSH 控制台登录 NetScaler ADM。
- 用于从 GUI 登录的默认用户名和密码为 *nsroot/nsroot*。

如何更改默认密码**?**

要更改密码，请执行以下操作：

1. 在 NetScaler ADM 中，导航到“设置”**>**“用户管理”**>**“用户”。

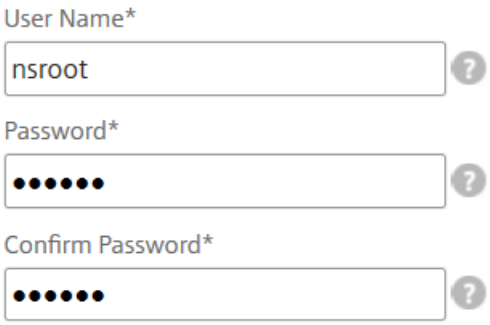
   此时将显示“用户”页面。

2. 选择用户名 **nsroot** ，然后单击 编辑。

   屏幕上 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、虚拟机管理程序或 SSH 控制台登录。

> 注意
>
> 不能修改用户名。

如何重置密码**?**

您可以查看此 文档 来重置密码。

在高可用性对中，如果在主节点中更改了密码，并且稍后选择了“**Break HA pair**”（中断高可用性对）选项，则会出现什么行为**?**

您可以使用新密码登录到两个独立节点。

如果两台独立服务器的密码不同，在高可用性对中部署这两台服务器会有什么影响**?**

当您将两台独立服务器部署到高可用性对时，建议两台服务器都使用默认密码。

高可用性配置已完成，但无法访问主节点 **GUI**。可能的原因是什么**?**

配置需要几分钟时间才能生效。您可以在几分钟后再次尝试访问。

高可用性配置已完成，但无法访问浮动 **IP** 地址 **GUI**。可能的原因是什么**?**

完成 HA 配置后，您需要首先访问主节点 GUI 并完成部署。有关更多信息，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。

NetScaler ADM 独立版和 **NetScaler ADM HA** 支持什么数据库

NetScaler ADM 独立版和 NetScaler ADM HA 都支持 PostgreSQL。

辅助节点可能会丢失哪些数据**?**

辅助节点监听主节点通过 NetScaler ADM 数据库发送的心跳消息。如果辅助节点未收到检测信号的时间超过 180 秒，辅助节点将在主节点上执行基于 SSH 的检查。如果检测信号和基于 SSH 的检查失败，则认为主节点已关闭。

在这种情况下，辅助节点将接管成为主节点，180 秒的时间范围可以被视为辅助节点可能丢失的数据。

如果主节点关闭，会发生什么情况**?**

辅助节点将接管并成为主节点。

如何重新安装出现故障的节点**?**

建议安装全新的 VM 版本。要重新安装，请执行以下操作：

1. 打破 HA 对。导航到 设置 **>** 部署

   此时将显示部署页面。单击 **Break HA**（中断高可用性）
2. 从 Hypervisor 中删除故障节点。
3. 将.XVA 映像文件导入到虚拟机管理程序中。
4. 在 控制台 选项卡中，使用初始网络配置配置 NetScaler ADM。有关详细信息，请参阅 注册并部署第一台服务器（主节点） 和 注册并部署第二台服务器（辅助节点）。
5. 重新部署 HA 对。

NetScaler ADM 是否支持 **SAN** 存储**?**

Citrix 建议您在本地存储上托管 NetScaler ADM VHD。当托管在 SAN 中的存储设备上时，NetScaler ADM 可能无法按预期工作。因此，不支持在 SAN 上部署 ADM。

NetScaler ADM 是否支持额外的磁盘

是。默认情况下，NetScaler 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，您可以额外添加一个磁盘，以获得最多 3 TB 的存储空间。不支持添加多个额外磁盘。

禁用高可用性对后，配置的浮动 **IP** 地址会发生什么**?**

浮动 IP 地址不再可访问，您需要重新部署高可用性对。

我是否可以在重新部署时提供不同的浮动 **IP** 地址**?**

是。可以配置新的浮动 IP 地址。

为什么辅助节点 **GUI** 无法访问**?**

辅助节点只是一个只读副本服务器，并且仅在主节点因任何原因关闭时才充当主节点。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，是否仍然可以使用浮动 **IP** 地址 **GUI** 完成配置**?**

是。您仍然可以继续进行配置，并且配置将保存在辅助节点中。主节点恢复后，将同步所有配置。

如果将来有必要更改主节点 **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**），建议执行哪些解决方案**?**

如果不中断高可用性对，则不支持更改高可用性对中的 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“设置”**>**“部署”。

   此时将显示“部署”页。单击 **Break HA**（中断高可用性）

   a) 使用 SSH 客户端或从虚拟机管理程序登录到主节点。

   b) 使用 `nsrecover` 作为用户名并输入您设置的密码。

   c) 输入 网络配置。执行 Regi ster 中提供的 步骤 **3** 中的步骤，然后部署第一台服务器（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，然后继续执行 注册和部署第二台服务器（辅助节点）中提供的 步骤 **3** 中的过程。

要更新浮动 IP 地址，请执行以下操作：

1. 导航到“设置”**>**“部署”。

   此时将显示“部署”页。

   a) 单击 **HA Settings**（高可用性设置）。

b) 单击 **Configure Floating IP Address for High Availability Mode**（为高可用性模式配置浮动 IP 地址）。

c) 输入浮动 IP 地址，然后单击“确定”。

ADM 是否支持 **AMD** 处理器**?**

AMD 处理器在以下方面受支持：

- **NetScaler ADM 13.1 Build 4.43** 或更高版本。
- **NetScaler ADM** 代理 **13.1 Build 17.42** 或更高版本。

部署（灾难恢复）

主站点与灾难恢复站点之间的复制频率有多高**?**

主站点与灾难恢复站点之间的复制是实时的。

在灾难恢复站点启动备份脚本后，在主站点恢复并完全运行之前，灾难恢复站点是否会成为临时主站点**?**

否。灾难恢复站点现在将成为主站点。要将 HA 对还原为主站点，请参阅 将配置还原为原始主站点

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，如果选择“**Break HA pair**”（断开高可用性对），灾难恢复站点会发生什么情况**?**

如果选择“Break HA pair”（断开高可用性对）选项，主站点与灾难恢复站点之间的复制将终止。作为重新部署高可用性对的一部分，您需要重新配置 DR 站点。

事件管理

如何使用 **NetScaler ADM** 跟踪在我的托管 **NetScaler** 实例上生成的所有事件

作为网络管理员，您可以查看一些详细信息，例如，您的 NetScaler 实例上的配置更改、登录情况、硬件故障、阈值违反和实体状态变化，以及特定实例上的事件及其严重性。您可以使用 NetScaler ADM 事件控制面板来查看为所有 NetScaler 实例的关键事件严重性详细信息而生成的报告。

什么是事件规则

使用 NetScaler ADM，您可以配置规则来监视特定事件。通过事件规则，您可以更轻松地监视 NetScaler ADM 基础架构中生成的许多事件。

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、NetScaler 实例、类别和故障对象。您可以为事件分配的操作包括发送电子邮件通知、将 SNMP 陷阱从托管 NetScaler 实例转发到 NetScaler ADM，以及发送短信通知。

实例管理

使用 **NetScaler** 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，池容量许可开始工作。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。

NetScaler ADM 中的数据中心是什么**?**

NetScaler ADM 数据中心是特定地理位置的 NetScaler 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 NetScaler 实例。您可以使用 NetScaler ADM 服务器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更多详细信息，请参阅 NetScaler ADM 中的如何为地理地图配置数据中心。

NetScaler ADM 支持哪些不同的 **NetScaler ADC** 设备

实例是您想要从 NetScaler ADM 发现、管理和监视的 NetScaler ADC 设备或虚拟设备。您必须将这些实例添加到 NetScaler ADM 服务器。您可以将以下 NetScaler ADC 设备和虚拟设备添加到 NetScaler ADM：

- NetScaler MPX
- NetScaler VPX
- NetScaler SDX
- NetScaler CPX
- NetScaler Gateway

可以在第一次设置 NetScaler ADM 服务器时添加实例，也可在以后添加。

什么是实例配置文件**?**

NetScaler ADM 使用实例配置文件来访问实例。

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-root-profile 是 NetScaler 实例的默认配置文件。它包含默认的 NetScaler 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。

我能否在 **NetScaler ADM** 中重新发现多个 **NetScaler VPX** 实例

可以，您可以在 NetScaler 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 基础架构 **>** 实例 **> NetScaler > 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。有关更多信息，请参阅 如何重新发现多个 VPX 实例。

NetScaler ADM 可以安装在 **NetScaler SDX** 上吗

否

我能否使用公用 **IP** 地址在 **ADM** 软件上添加 **NetScaler** 实例

是，您可以使用网络地址转换 (NAT)。

- 添加单个实例：使用 ADC 实例的公用 IP 地址的 NAT IP。
- 要添加 ADC 高可用性对，请按以下格式添加高可用性对的 NAT IP 地址：

  <NAT **public** IP of the primary instance>#<NAT **public** IP of the secondary instance>

- 添加 ADC 群集：添加群集中所有实例的所有 NAT 公用 IP 地址，每个地址用逗号分隔，然后在括号或圆括号内添加群集 IP 的 NAT IP。示例格式：NAT1、NAT2、NAT3、(CLUSTERIP 的 NATIP)。

有关详细信息，请参阅以下主题：

- 将实例添加到 NetScaler ADM
- 配置网络地址转换

如果 **DR** 节点凭据发生变化，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-->
```

要注册灾难恢复节点，请按照 部署中的步骤操作，然后使用灾难恢复控制台注册 NetScaler ADM DR 节点。

样书

样书可以用于配置在不同版本的 **NetScaler** 软件上运行的不同 **NetScaler** 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 NetScaler 实例。

如果使用样书同时配置多个 **NetScaler** 实例，并且一个 **NetScaler** 实例的配置失败，会发生什么情况**?**

如果将配置应用于 NetScaler 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 **NetScaler** 进行的 **NetScaler** 备份是否包括通过样书应用的配置

是

系统管理

我可以为我的 **NetScaler ADM** 服务器分配主机名吗

可以，您可以分配主机名来标识您的 NetScaler ADM 服务器。要指定主机名，请导航到 **System**（系统）> **System Administration**（系统管理）> **System Settings**（系统设置），然后单击 **Change Hostname**（更改主机名）。

主机名将显示在 NetScaler 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 NetScaler ADM 服务器。

是否可以备份和还原我的 **NetScaler 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 NetScaler ADM 变得不稳定，您可以使用备份的文件将 NetScaler ADM 恢复到稳定状态。

要备份和还原 **NetScaler 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 NetScaler 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。

NetScaler ADM 上的阈值和警报是什么

可以设置阈值和警报来监视 NetScaler 实例的状态及监视托管实例上的实体。

当计数器的值超过阈值时，NetScaler ADM 会生成警报以表示存在与性能相关的问题。在计数器值回到阈值中指定的清除值时，事件将被清除。

我可以为 **NetScaler ADM** 生成技术支持文件吗

是。Citrix 建议您在联系技术支持部门调试问题之前生成 NetScaler ADM 数据和统计数据存档。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 NetScaler ADM 数据库中不同且不同的日志。

要配置和发送技术支持文件，请导航到 **System**（系统）> **Diagnostics**（诊断）> **Technical Support**（技术支持），然后单击 **Generate Technical Support File**（生成技术支持文件）。有关详细信息，请参阅如何为 NetScaler ADM 生成技术支持文件。

什么是 **syslog** 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。您可以指定将从 NetScaler ADM 中删除所有通用 Syslog 数据、AppFirewall 数据和 NetScaler Gateway 数据的天数。

我可以在 **NetScaler ADM** 上配置 **NTP** 服务器吗**?**

您可以在 NetScaler ADM 中配置网络时间协议 (NTP) 服务器，使 NetScaler ADM 时钟与 NTP 服务器同步。配置 NTP 服务器可确保 NetScaler 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 NetScaler ADM 上配置 NTP 服务器。

从哪个版本支持 **NetScaler ADM** 主动-被动 **HA** 部署**?**

NetScaler ADM 版本 12.0 build 51.24 支持 NetScaler ADM 主动-被动 HA 部署模式。

我设置了 **NetScaler ADM active-active HA**，并在其上配置了带有负载平衡虚拟服务器的 **NetScaler** 设备，用于统一 **GUI** 访问。如何更新此配置

将 NetScaler ADM HA 对升级到主动-被动模式后，必须在 NetScaler 设备上运行以下命令来更新负载平衡配置：

add lb monitor MAS_Monitor **TCP-ECV -send** “**GET /mas_health HTTP/1.1\r\nAccept-Encoding: identity\r\nUser-Agent: NetScaler-Monitor\r\nConnection: close\r\n\r\n\”-recv “{\“statuscode\ “:0, \ “is_passive\ “:0}” -LRTM DISABLED**

我能否使用端口 **443** 在 **NetScaler** 实例上配置 **NetScaler ADM HA** 对的负载平衡

否，您不能使用端口 443 在 NetScaler 实例上配置 NetScaler ADM HA 对的负载平衡。

在 NetScaler 上配置 `http-ecv` 和 `https-ecv` 监视器时，它无法正确监视 NetScaler ADM HA 节点。

是否可以使用 **NetScaler ADM** 服务器备份文件还原另一台 **NetScaler ADM** 服务器的配置**?**

是

在 **NetScaler ADM** 备份 **NetScaler** 实例之后，能否使用该备份文件通过 **NetScaler ADM** 恢复另一个 **NetScaler** 实例的配置

是。下载 NetScaler ADM 备份文件，将其上载到另一个 NetScaler 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、不匹配的密码配置文件。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 NetScaler 许可证。

在还原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 NetScaler 许可证。

我们能否强制 **NetScaler ADM** 使用 **SNIP** 地址与 **NetScaler** 实例通信，而不是使用 **NetScaler ADM** 服务器的 **NSIP** 地址

可以，您可以在 NetScaler ADM 中添加 SNIP 地址（启用了管理功能），以便与 NetScaler 实例进行通信。

当我在 **NetScaler ADM** 中备份 **NetScaler** 实例时，结果是完整备份还是基本备份

NetScaler ADM 对 NetScaler 实例的备份是完整备份。

有 **NetScaler ADM** 的故障排除指南吗

是。请参阅 https://support.citrix.com/article/CTX224502。

发生 **NetScaler ADM HA** 故障转移时，如何管理 **NetScaler** 实例

如果检测信号和基于 SSH 的检查失败，则认为主节点关闭，辅助节点将作为主节点接管工作。默认情况下，所有 NetScaler 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）NetScaler 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 **NetScaler ADM HA** 节点恢复运行时会发生什么

恢复服务后，除非主动节点发生故障转移，否则 NetScaler ADM 节点将保持被动状态

NetScaler 实例如何分布在 **NetScaler ADM HA** 节点上

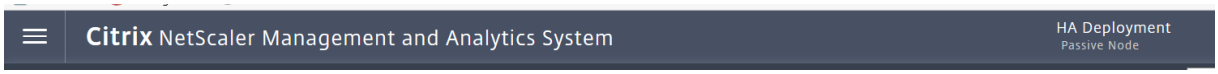
所有 NetScaler 实例都由主 NetScaler ADM 节点进行管理。

如果存在 **NetScaler 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 NetScaler 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。如需替代方案，请联系 NetScaler 支持人员。

NetScaler ADM HA 设置是否必须使用负载平衡器

否，但如果没有负载平衡器，则必须通过其自己的 IP 地址访问 NetScaler 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。



NetScaler ADM 是否支持外部数据库**?**

否

由 **NetScaler ADM** 管理的 **NetScaler** 实例能否用作 **NetScaler ADM HA** 的负载平衡器

是

NetScaler ADM HA 节点之间同步了哪些数据

完整的 NetScaler ADM 数据库已同步，以下文件夹已同步：

- /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/