最新功能

Citrix 的目标是在新功能和产品更新可用时，立即将其交付给 Citrix Analytics 客户。新版本提供更多价值，因此没有理由延迟更新。

对于您，即客户而言，此过程是透明的。初始更新仅应用于 Citrix 内部站点，然后逐步应用于客户环境。分阶段增量交付更新有助于确保产品质量并最大限度地提高可用性。

Citrix Analytics 具有以下产品或服务。请参阅针对每项服务发布的最新功能文章，以了解新功能和产品更新。

- Citrix 安全分析
- Citrix 性能分析

本发行说明重点介绍了 Citrix Analytics 平台特有的新功能和产品更新。

September 21, 2023

使用 PowerShell 脚本简化 StoreFront™ 载入

已引入一个新的 **PowerShell** 脚本，可自动执行检查先决条件、安装和配置 StoreFront 的过程。客户必须在 StoreFront 上以管理员模式运行此脚本，才能进行载入、取消载入、执行自检、故障排除以及验证是否成功载入 Citrix Analytics Service GUI。

有关详细信息，请参阅 连接到 StoreFront 部署。

August 28, 2023

Microapps 服务（生命周期结束）

Citrix Microapps 服务已达到其生命周期结束，不再向用户提供。

August 01, 2023

Citrix Analytics - 使用情况 (停止服务)

Citrix 使用情况分析已停止服务，不再向用户提供。

February 23, 2023

已修复的问题

在 Citrix Virtual Apps and Desktops™ 2112 发布之前，Citrix Analytics 无法发现从 Citrix Director 连接且最近在 Citrix Cloud 上注册的本地站点。因此，您在 **Virtual Apps and Desktops- Monitoring** 站点卡上看不到这些已连接的站点。此问题现已修复。

September 28, 2022

用于警报通知的 Webhook

您可以使用 Webhook 将 Citrix Analytics 警报通知发送到已配置传入 Webhook URL 的任何第三方应用程序。Webhook 是一种 HTTP 回调，可在服务提供商应用程序和使用者应用程序之间实现实时消息传递。由于警报通知是实时发送的，因此您会在事件发生时收到通知。有关详细信息，请参阅 用于警报通知的 Webhook。

September 08, 2022

CSV 导出中的导出限制已增加

使用 **导出为 CSV 格式** 功能可导出的行数限制已从 1 万行增加到 10 万行。有关详细信息，请参阅 将事件导出到 CSV 文件。

August 18, 2022

已修复的问题

- 在 Apps and Desktops 的自助服务搜索中，下载的 CSV 文件中，Workspace 应用程序版本值显示为 **NA**（不可用），而页面视图中则可用。此问题现已修复。

August 10, 2022

StoreFront 无站点聚合的入门

StoreFront 的站点聚合依赖项已从“**应用程序和桌面 - Workspace 应用程序**”站点卡中移除。即使您没有将任何站点添加到站点聚合中，您也可以在工作区应用程序上看到“**连接 StoreFront 部署**”选项。有关更多详细信息，请参阅 Citrix Virtual Apps and Desktops 数据源。

April 05, 2022

安全工作区访问 已更名为 安全私有访问

在 Analytics 控制板和报告中，所有 **Secure Workspace Access** 标签现已更新为 **Secure Private Access**，以与更名的产品名称保持一致。

例如，在“**数据源**”页面和“**自助搜索页面**”上，**Secure Workspace Access** 标签已更名为 **Secure Private Access**。

March 21, 2022

已修复问题

- 在“**搜索**”页面中，如果搜索查询的先前条件包含由空格分隔的维度值，则维度和运算符的自动建议不起作用。

  例如，在以下查询中，在您将城市选择为 `San Jose` 后，自动建议将停止工作。此问题现已修复。



February 10, 2022

新增功能

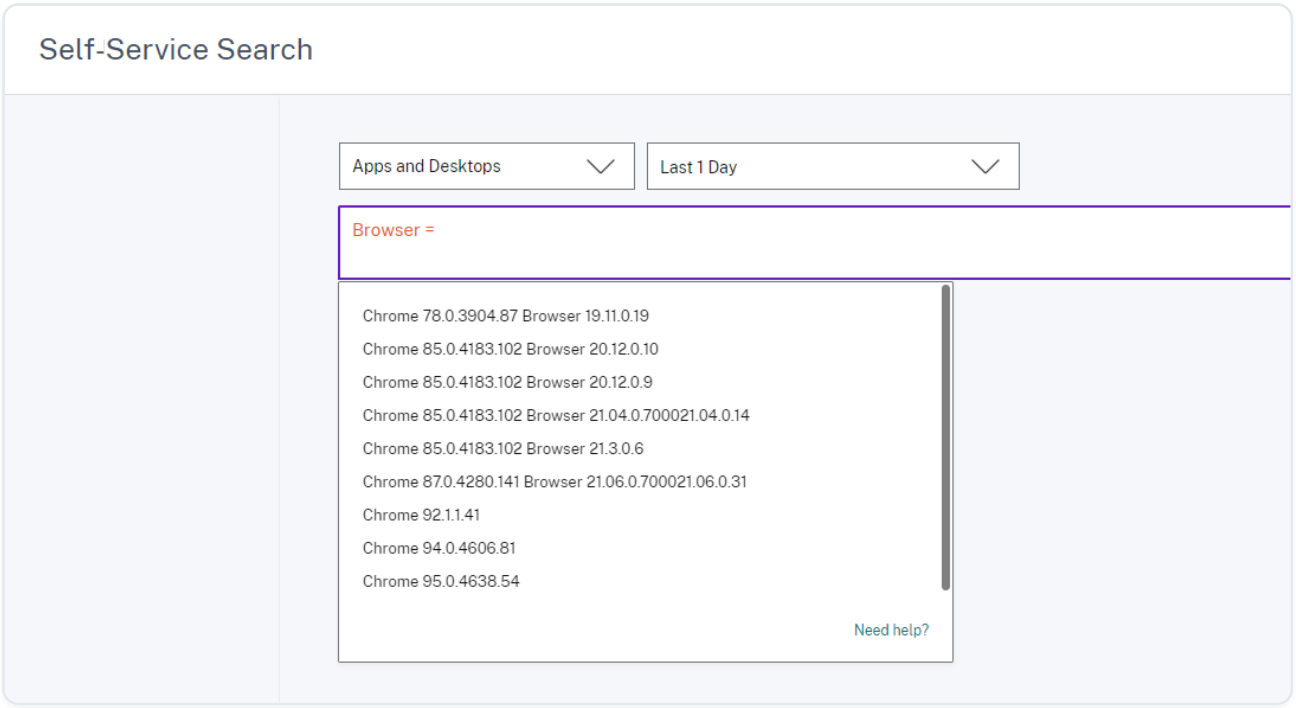
自助搜索框中维度的自动建议值

在自助搜索页面中，当您在搜索框中选择维度和有效运算符时，将自动显示维度的值。从自动建议列表中选择一个值，或根据您的用例手动输入一个值。当您键入值时，记录中可用的匹配值将自动建议。

维度建议的值列表可以是数据库中预定义的（已知值），也可以是基于历史事件的。

例如，当您选择维度 `Browser` 和赋值运算符时，已知值将自动建议。您可以根据需要选择一个值。

有关详细信息，请参阅自助搜索。



December 20, 2021

新增功能

访问控制已重命名为安全工作区访问

在 Analytics 控制板和报告中，所有 **Access Control** 标签现在都已更新为 **Secure Workspace Access**，以与更名后的产品名称保持一致。

例如，在**数据源**页面和**自助搜索**页面上，**Access Control** 标签已重命名为 **Secure Workspace Access**。

December 06, 2021

新增功能

Citrix Analytics 现已支持亚太南部区域

- 现在，在将组织载入 Citrix Cloud 并使用 Citrix Analytics 服务时，您可以选择亚太南部作为主区域。有关详细信息，请参阅地理注意事项。
- 当您选择亚太南部作为主区域时，Citrix Analytics 现在会将您组织的用户事件和元数据存储在该区域。有关详细信息，请参阅数据治理。
- 有关亚太南部区域的网络要求信息，请参阅技术安全概述。
- 有关亚太南部区域支持的数据源信息，请参阅数据源。

August 19, 2021

新增功能

支持 IS EMPTY 运算符

在自助搜索中，您现在可以在条件中使用 **IS EMPTY** 运算符来检查空值或空维度。

> **注意**
>
> 此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。
>
> 有关详细信息，请参阅自助搜索。

July 14, 2021

新增功能

支持 IS NOT EMPTY 运算符

在自助搜索中，您现在可以在查询中使用 **IS NOT EMPTY** 运算符来检查维度是否不为空（非空白）。

> **注意**
>
> 此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。
>
> 有关详细信息，请参阅自助搜索。

June 07, 2021

已弃用的功能

已移除 Citrix Analytics 演示环境

安全分析和性能分析的 **试用演示** 链接已从 Analytics 概述页面中移除。您无法再访问每个产品的演示环境。有关如何访问 Citrix Analytics 产品的更多信息，请参阅入门。

May 18, 2021

新增功能

支持 * 运算符与 != 运算符结合使用

在搜索查询中，您现在可以将 * 运算符与 `!=` 运算符结合使用来查找用户事件。例如：

- 要查找所有不以名称“John”开头的用户事件，请使用查询：User-Name != John*
- 要查找所有不以名称“Smith”结尾的用户事件，请使用查询：User-Name != *Smith

> **注意**
>
> 搜索结果区分大小写。

> 有关更多信息，请参阅自助搜索。

自助搜索页面中增强的搜索栏体验

- 当搜索栏扩展到多行时，它现在可以更好地显示您的查询。使用滚动条滚动您的多行查询。以前，很难查看多行查询。

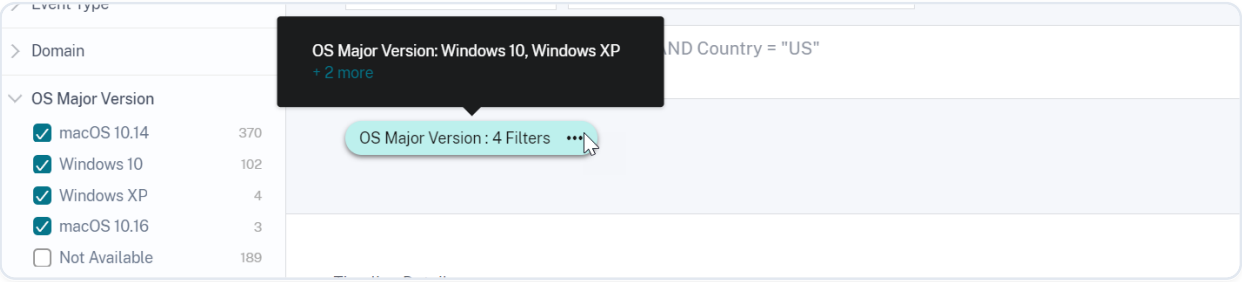


- 在 Safari 浏览器中观察到的光标跳动问题现已修复。

有关详细信息，请参阅 自助搜索。

自助搜索中重新设计的芯片视图

- 重新设计的芯片现在可以更好地显示您已选择的多个方面。



- 单击芯片可根据您的要求选择或取消选择方面。

已修复问题

- 在 Citrix Director 上，**转到分析**链接不起作用。对于已在 Citrix Cloud 的欧盟区域加入其组织的客户，会观察到此问题。

March 31, 2021

支持 Apps and Desktops 搜索查询的 IN 和 NOT IN 运算符

借助 Apps and Desktops 维度 - `Device ID`、`Domain`、`Event-Type` 和 `User-Name`，您现在可以使用以下运算符：

- **IN**：为维度分配多个值，以获取与一个或多个值相关的事件。
- **NOT IN**：为维度分配多个值，并查找不包含指定值的事件。

> **注意**

> 这些运算符仅适用于字符串值。

> 有关运算符的更多信息，请参阅自助搜索。

March 18, 2021

新增功能

支持 NOT LIKE (!~) 运算符

对于自助搜索查询，您现在可以使用 NOT LIKE (!~) 运算符。该运算符检查用户事件中是否存在您指定的匹配模式。它返回事件字符串中不包含指定模式的事件。

例如，查询 `User-Name !~ “John”` 显示除 John、John Smith 或任何包含匹配名称“John”的用户之外的用户的事件。

有关详细信息，请参阅自助搜索。

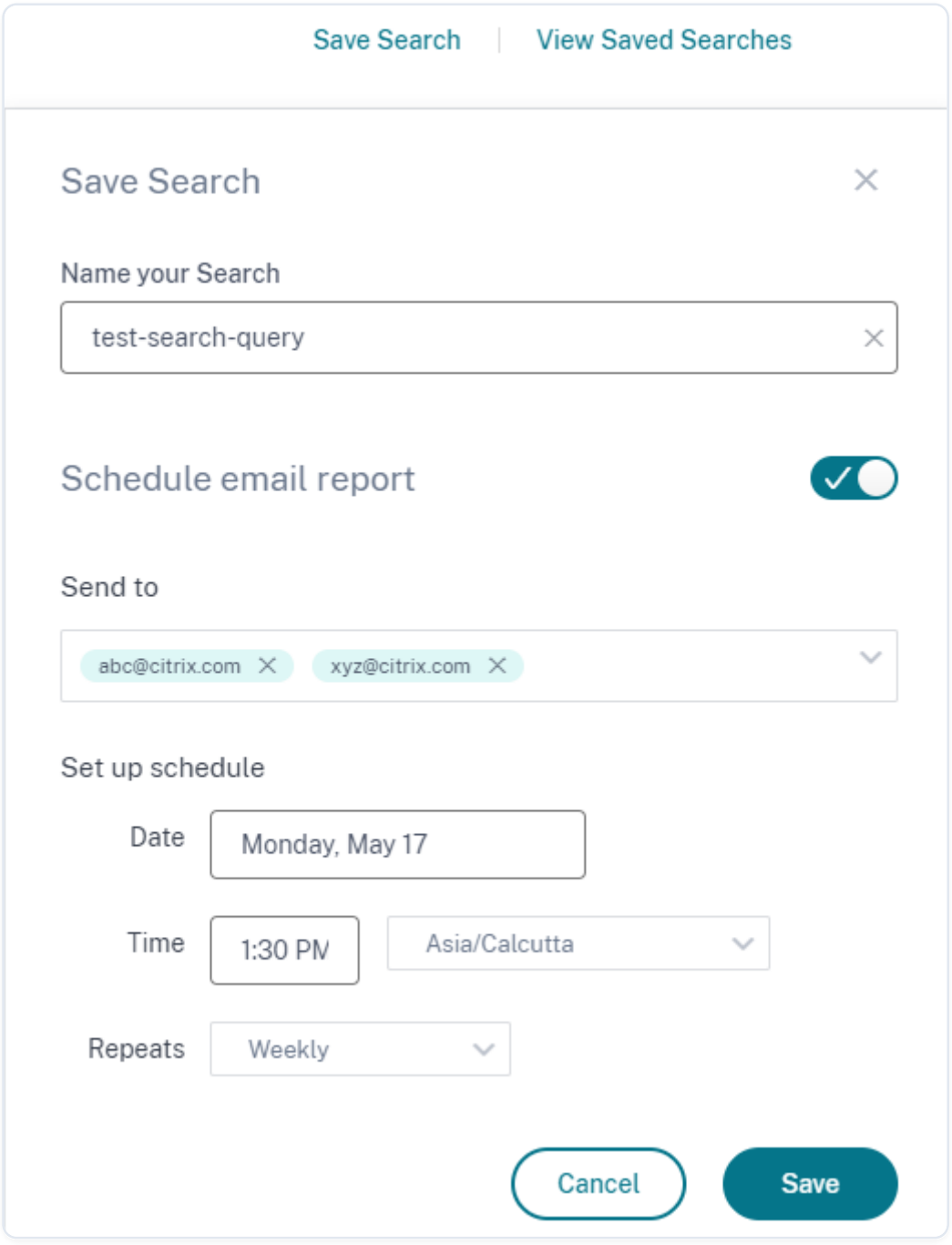
February 23, 2021

新增功能

为搜索查询安排电子邮件发送

在自助搜索页面上，保存搜索查询时，您还可以安排电子邮件发送，将保存的搜索查询和相应的可视化摘要报告副本发送给自己和其他用户。设置日期、时间和频率（每日、每周或每月）以开始发送电子邮件。您还可以安排发送以前保存的搜索查询的电子邮件。

有关详细信息，请参阅自助搜索。



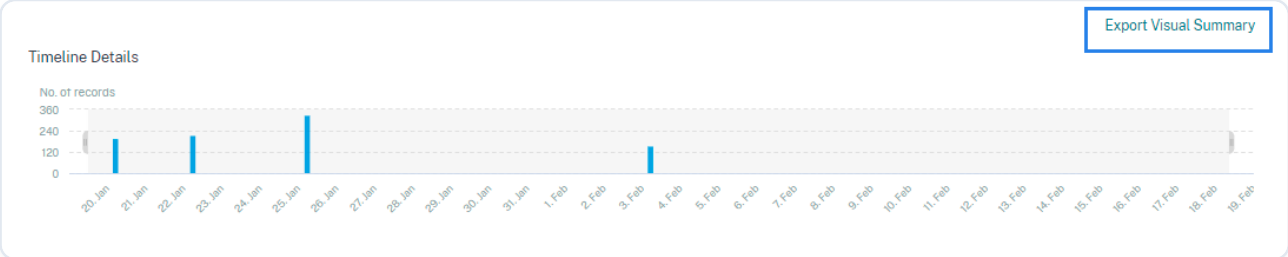
下载搜索查询的可视化摘要

在自助服务页面上，您现在可以下载选定时间段内搜索查询的可视化摘要报告，并与其他用户共享副本。单击“**导出可视化摘要**”以下载 PDF 格式的可视化摘要报告。

报告包含以下信息：

- 您为事件指定的搜索查询。
- 您应用于事件的分面（筛选器）。
- 搜索事件的可视化摘要，例如时间线图表、条形图或图形。

有关详细信息，请参阅自助服务搜索。



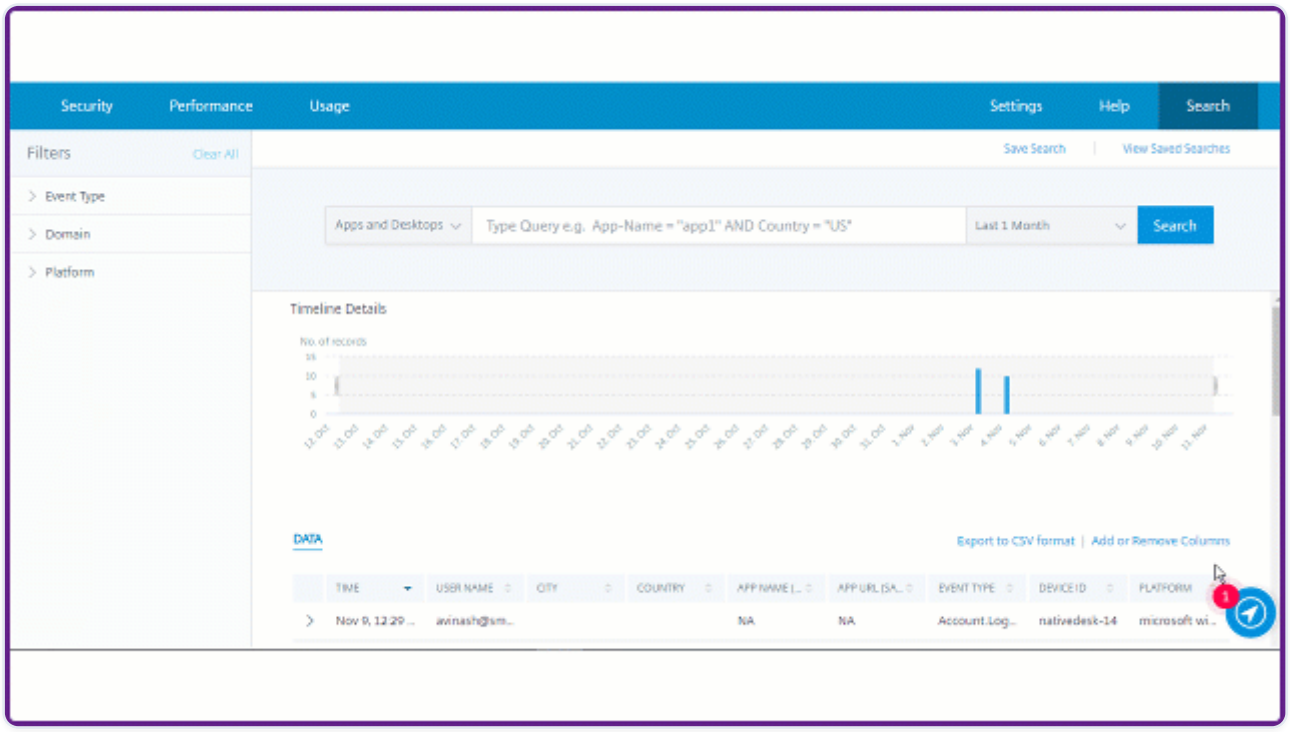
November 12, 2020

新功能

保存自助服务查询

创建自助服务查询后，您可以将其保存以供以后使用。以下选项将随查询一起保存：

- 已应用的搜索筛选器
- 选定的数据源和持续时间



有关详细信息，请参阅如何保存自助服务搜索。

October 20, 2020

新增功能

支持欧盟地区的 Citrix Gateway

Citrix Analytics 现在支持欧盟地区的 Citrix Gateway。有关详细信息，请参阅 Citrix Gateway 数据源。

July 09, 2020

已弃用的支持

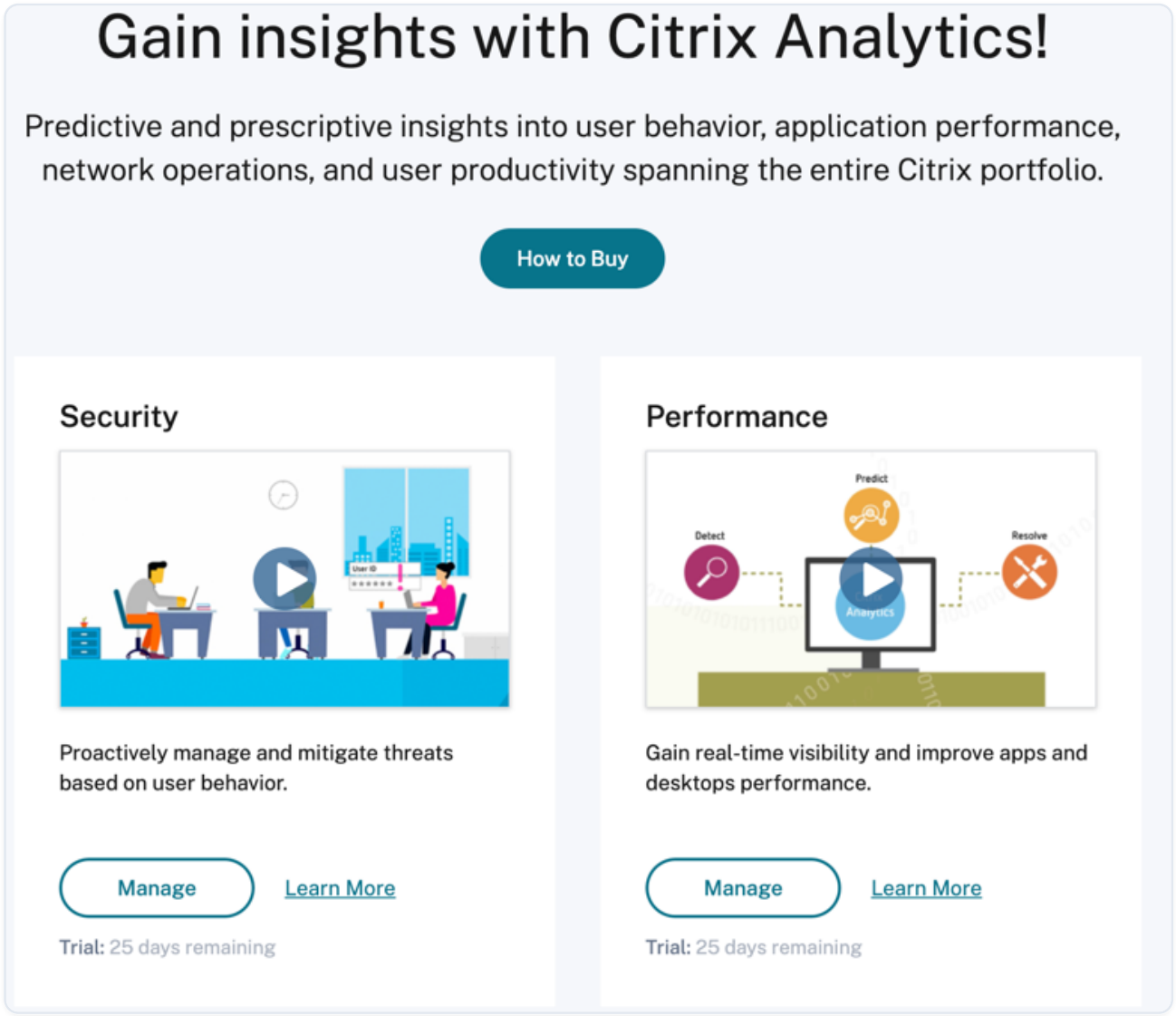
Microsoft Internet Explorer 11 已从支持的浏览器列表中删除。此弃用是由于在该浏览器中观察到的安全漏洞。有关支持的浏览器列表，请参阅 系统要求。

June 02, 2020

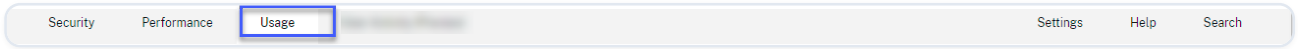
新增功能

重新设计的 Analytics 概览页面和顶部栏

Analytics 概览页面显示了 **Usage**（使用情况）磁贴，它取代了之前存在的 **Operations**（操作）磁贴。此外，**Productivity**（生产力）磁贴已从此页面中移除。要查看概览页面，请选择 **Help**（帮助）> **Overview**（概览）。



同样，在顶部栏中，**Usage**（使用情况）选项卡取代了 **Operations**（操作）选项卡。



February 20, 2020

新功能

Citrix Analytics 订阅产品

为用户提供灵活的购买选项，Citrix 现提供三种基于订阅的独立 Citrix Analytics 产品。Citrix Analytics 根据您订阅的产品提供独特的安全性或性能（或两者兼有）见解。

您可以购买以下 Citrix Analytics 订阅产品：

- Citrix 安全分析
- Citrix 性能分析
- Citrix 安全分析™ 和 性能分析（捆绑包）

数据治理日志更新

为以下数据源添加了新日志：

- Citrix 身份提供程序
- Citrix 网关
- 安全浏览器
- 微软 Graph 安全
- Microsoft 活动目录

有关更多信息，请参阅 数据治理。

已修复的问题

- 自助搜索在 Internet Explorer 11 上无法准确运行。因此，您无法输入搜索查询并执行搜索操作。

January 09, 2020

已修复的问题

- 对于欧盟主区域的用户，Citrix Analytics 演练功能无法正常工作。

December 18, 2019

已修复的问题

在 **Citrix Cloud** 页面上，**Analytics** 磁贴显示“**查看服务**”按钮。为了提供更好的用户体验，此按钮现已更改为“**管理**”。

December 12, 2019

新增功能

支持亚太南部地区的 Microapps 服务事件

Citrix Analytics 平台现在处理来自亚太南部地区 Microapps 服务的通知。但是，衡量性能、 稳定性、使用情况、安全性和支持的记录会在美国进行汇总和存储。有关详细信息，请参阅数据治理。

> **注意**
>
> Microapps 服务作为 Citrix Workspace 的一部分提供。有关详细信息，请参阅 Microapps 文档。

December 04, 2019

已修复问题

亚太南部地区的一些用户无法登录 Citrix Analytics，尽管他们通过选择“**美国**”作为主区域已加入 Citrix Cloud。

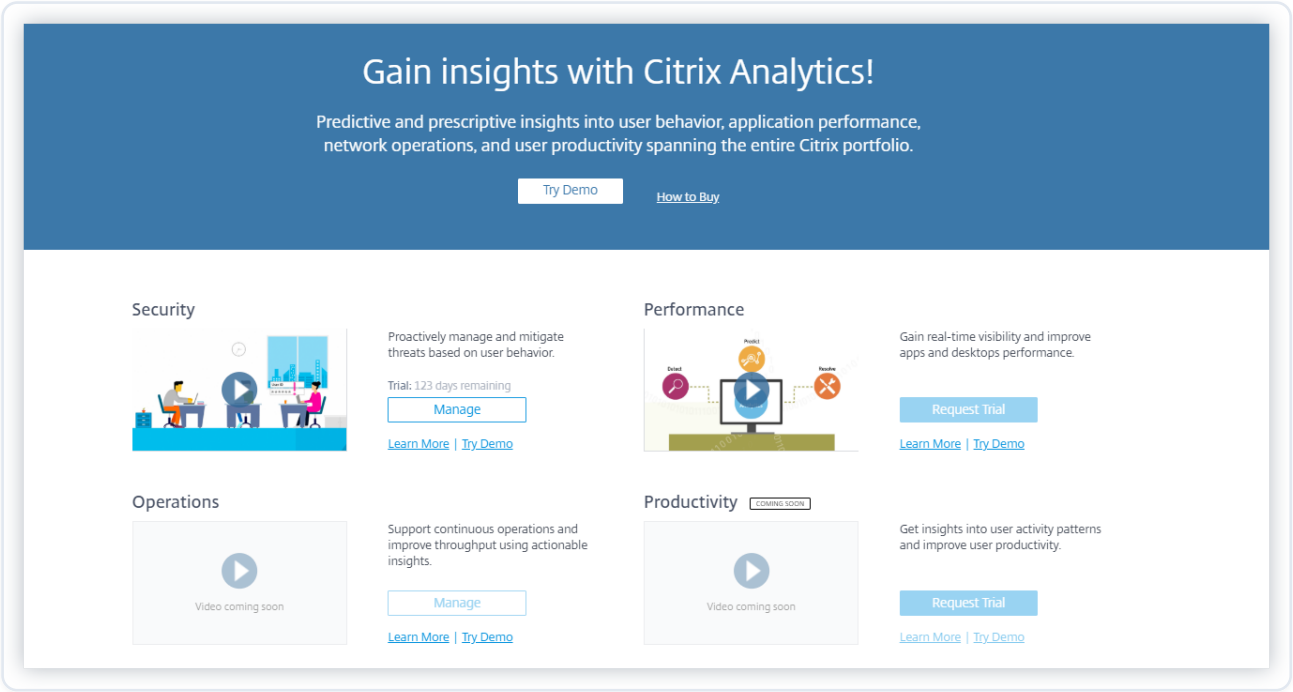
November 22, 2019

新增功能

重新设计的 Analytics 概览页面

Analytics 概览页面经过重新设计，允许从此页面访问所有 Analytics 产品。您可以申请试用、尝试演示或管理您的 Analytics 产品。目前，只有 Security Analytics 和 Operations Analytics 已正式发布，因此在此页面上处于活动状态。

要查看概览页面，请选择“**帮助**”>“**概览**”。



October 21, 2019

新增功能

技术安全概览

技术安全概览 让您了解与 Citrix Analytics 相关的安全最佳实践。本文档介绍了使用 Citrix Analytics 时需要考虑的数据流、数据保护、网络要求和安全职责。

September 11, 2019

已修复问题

- Citrix Cloud 无法将用户重定向到特定区域的 Citrix Analytics 页面。

August 20, 2019

已修复的问题

- Citrix Analytics 演练功能无法在 Microsoft Edge 和 Safari 浏览器上准确加载。

July 31, 2019

新增功能

支持欧盟地区

Citrix Analytics 现已支持欧盟地区。在将您的组织载入 Citrix Cloud 并使用 Citrix Analytics 服务时，您可以选择**欧盟**作为主区域。Citrix Analytics 将您组织的用户事件和元数据存储在欧盟地区。有关 Citrix Cloud 区域的更多信息，请参阅地理注意事项。

June 26, 2019

已修复的问题

- Citrix Analytics 无法在 Internet Explorer 11 上准确加载。

June 19, 2019

已修复的问题

- Citrix Analytics 无法在 Microsoft Edge 上准确加载。

November 16, 2018

已修复的问题

- 如果您使用 Internet Explorer 11.0 版访问 Citrix Analytics，则 **Citrix Cloud** 导航栏将无法加载，并限制您访问汉堡菜单。

October 10, 2018

架构和平台增强功能

此版本进行了多项架构和平台改进，以增强性能、可伸缩性、监控、可支持性、安全性和用户体验。

August 23, 2018

Citrix Analytics 是通过 Citrix Cloud 提供的云服务。它收集 Citrix 产品组合中的数据并提供可操作的见解，使管理员能够主动处理安全威胁、提高应用程序性能并支持持续运营。目前，Citrix Analytics 提供以下分析产品：

- **安全分析**：整理并提供用户和实体行为的可见性。有关更多信息，请参阅 安全分析。
- **运营分析**：整理并呈现用户活动信息，例如访问的网站和使用的带宽。有关更多信息，请参阅 运营分析。

新产品名称

Citrix Analytics 支持的 Citrix 产品现已作为 Citrix 统一产品组合的一部分进行了重命名。

您可能会在我们的产品和产品文档中注意到新名称。此次品牌重塑是 Citrix 产品组合和云战略扩展的结果。有关 Citrix 统一产品组合的更多详细信息，请参阅 Citrix 产品指南。 在我们的产品及其文档中实施此过渡是一个持续进行的过程。

- 产品内内容和文档可能仍包含旧名称。例如，您可能会在控制台文本、消息、目录/文件名、屏幕截图和图表中看到旧名称的实例。
- 某些项目（例如命令）可能会继续保留其旧名称，以防止破坏现有客户脚本。
- 从本产品文档链接的相关产品文档和其他资源（例如视频和博客文章）可能仍包含旧名称。

已知问题

本文重点介绍适用于 Citrix Analytics 产品（性能分析和安全分析）的已知问题。

有关每个产品特有的问题，请参阅相应的已知问题文章：安全分析 和 性能分析。

- 当用户首次登录并通过 Gateway 访问服务或应用程序时，会触发**Gateway - 首次从新 IP 访问指示器**。

数据源

数据源是向 Citrix Analytics 发送数据的云服务和本地产品。

Citrix Analytics 从以下数据源收集数据：

- **Citrix 数据源**。向 Citrix Analytics 发送数据的 Citrix Cloud™ 服务和本地产品。Citrix Analytics 会自动发现与您的 Citrix Cloud 帐户关联的 Citrix Cloud 服务，例如 Content Collaboration 和 Endpoint Management。

  对于 Citrix Gateway 和 Citrix Virtual Apps and Desktops 等本地产品，您必须执行一系列配置才能连接到 Citrix Analytics。例如，必须将本地 Gateway 实例添加到 Application Delivery Management。并且必须将本地 Virtual Apps and Desktops 站点添加到 Workspace 或配置 StoreFront 服务器。
- **外部数据源**。可以与 Citrix Analytics 集成的第三方应用程序，例如 Microsoft Graph Security、Microsoft Active Directory。成功集成后，Citrix Analytics 会从这些外部数据源收集数据。

支持的数据源

根据您使用的 Citrix Analytics 产品，数据源会有所不同。请参阅以下文章以查看每个产品支持的数据源：

- Citrix Analytics for Security 支持的数据源
- Citrix Analytics for Performance 支持的数据源

Citrix Gateway、Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 Citrix Virtual Apps and Desktops 数据源受 Citrix Analytics for Security 和 Citrix Analytics for Performance 这两种产品支持。有关适用于这两种产品的入门步骤的信息，请参阅以下文章：

- Citrix Gateway 数据源
- 思杰虚拟应用和桌面数据源

Citrix Gateway 数据源

Gateway 数据源表示您环境中的本地 Citrix Gateway 实例。Citrix Analytics 会自动发现 Citrix Application Delivery Management (ADM) 代理以及添加到 Citrix ADM 服务中的 Gateway 实例。

当用户通过 Gateway 访问任何服务或应用程序时，Citrix Analytics 会实时接收用户访问事件。用户事件会经过处理以检测任何安全威胁。

本文介绍了将 Citrix Gateway 添加到 Citrix Analytics 的步骤。这些步骤适用于两种产品：Citrix Analytics for Performance™ 和 Citrix Analytics for Security。

先决条件

- 订阅 Citrix Cloud 上提供的 Citrix ADM。要了解如何开始使用 Citrix ADM，请参阅入门。
- 已验证的 Citrix ADM 许可证。要了解有关 Citrix ADM 许可的更多信息，请参阅许可证。
- 查看系统要求并确保满足这些要求。

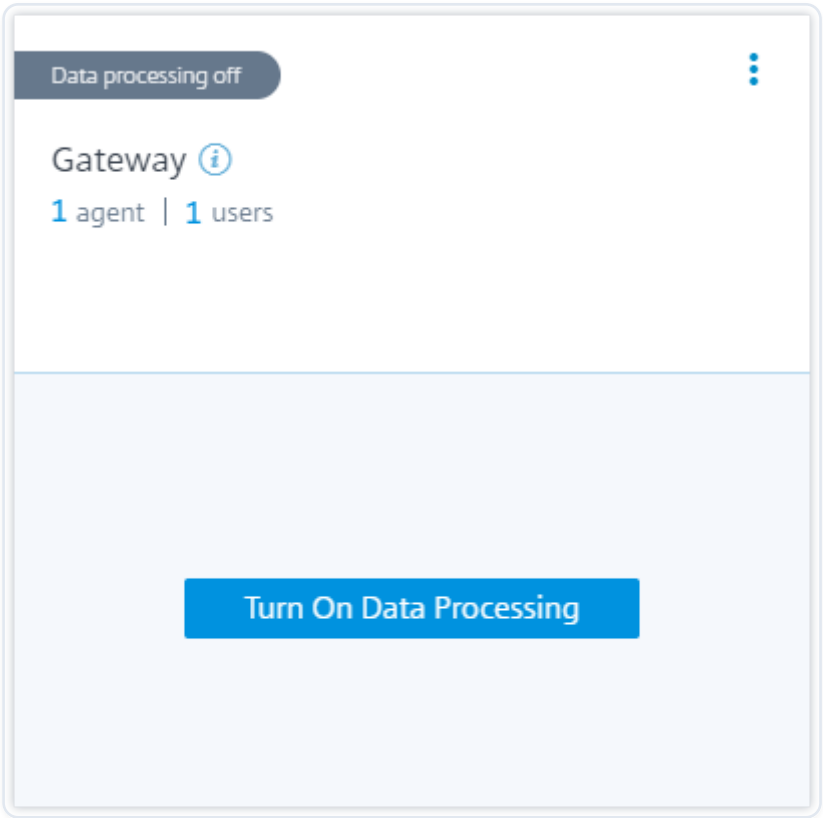
已添加到 Citrix ADM 的 Gateway 数据源

Citrix Analytics 会自动发现已添加到 Citrix ADM 服务中的 Citrix ADM 代理和 Citrix Gateway 实例。

要查看数据源：

在顶部栏中，单击**设置** > **数据源**。根据您的产品，选择**安全**或**性能**以查看 Gateway 站点卡。

发现的代理和用户显示在 Gateway 站点卡上。单击**开启数据处理**以允许 Citrix Analytics 开始处理此数据源的数据。

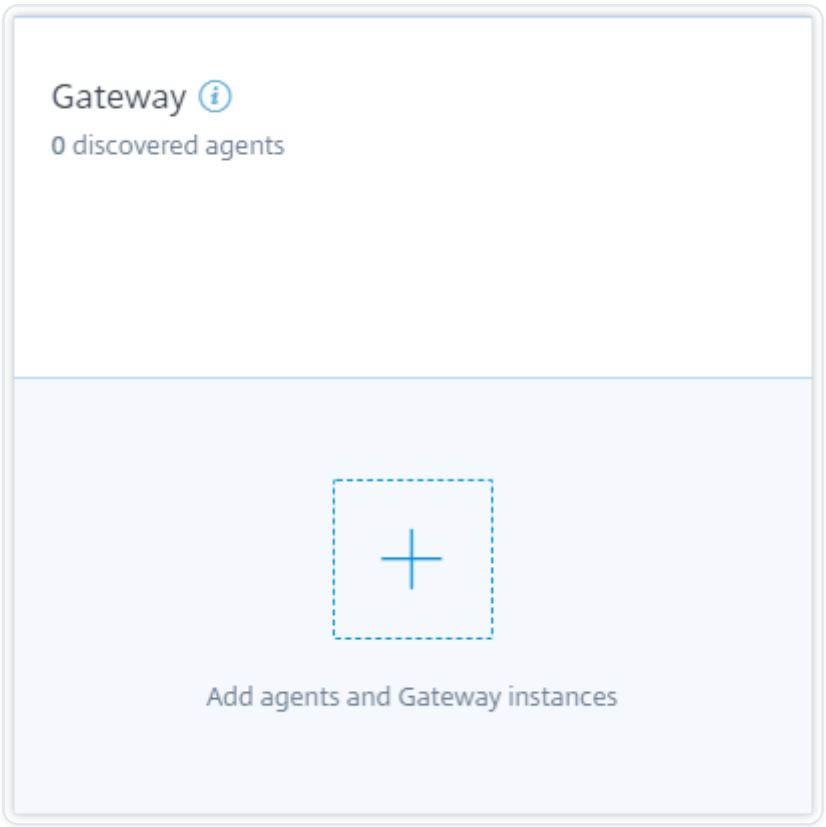


您可以查看收到的事件。

如果尚未在 Citrix ADM 服务上启用 Citrix Analytics，请参阅 (/zh-cn/citrix-application-delivery-management-service/setting-up/unified-analytics-workflow.html) 以启用 Citrix Analytics。

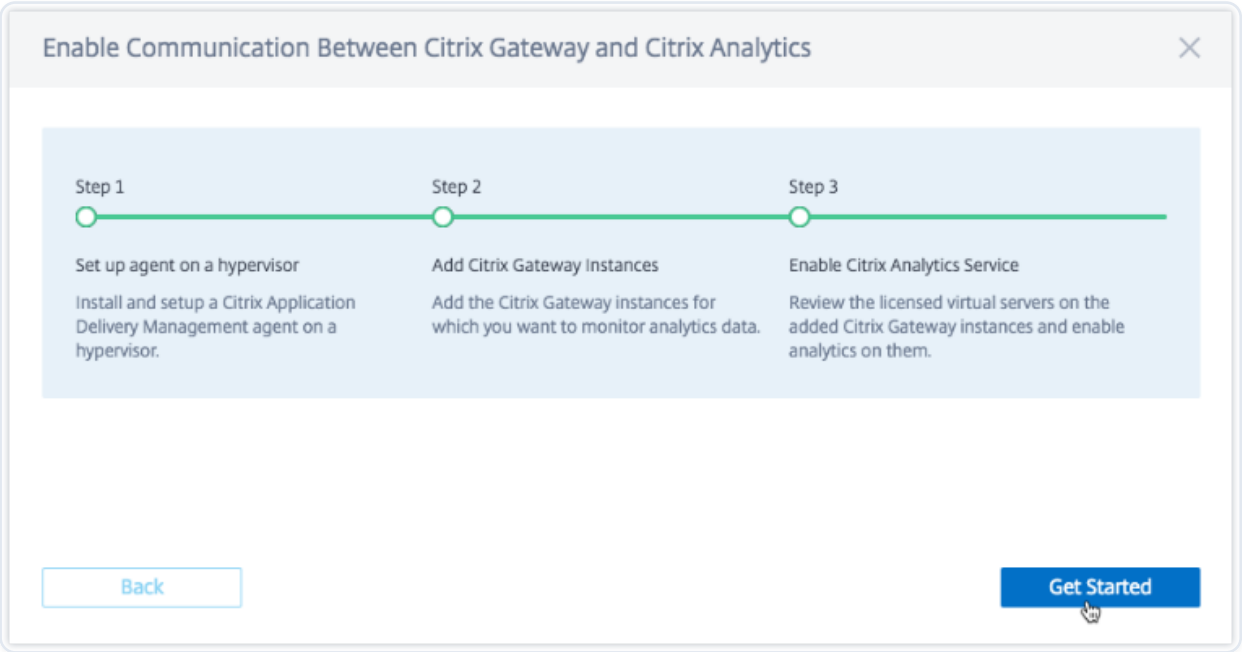
未添加到 Citrix ADM 的 Gateway 数据源

当 Citrix ADM 代理和 Citrix Gateway 实例未添加到 Citrix ADM 服务时，Gateway 站点卡会显示 **0 个已发现代理**。



要发现代理和 Gateway 实例，请执行以下操作：

1. 如果您已有 Citrix ADM 服务订阅，请单击站点卡上的 **+** 以添加代理和 Gateway 实例。
2. 如果您没有 Citrix ADM 服务订阅，则必须订阅。转到您的 Citrix Cloud™ 帐户并执行以下操作：
    a. 在 **可用服务** 下，单击 **Application Delivery Management** 磁贴上的 **管理**。
    b. 按照屏幕上的说明为 Citrix ADM 创建 Express 帐户。有关详细信息，请参阅 Citrix ADM 文档中的 (/zh-cn/citrix-application-delivery-management-service/getting-started.html#step-2-manage-citrix-adm-with-an-express-account)。
    c. 创建 Express 帐户后，重新登录 Analytics 并单击 **设置 > 数据源 > 安全**。
    d. 在 Gateway 站点卡上，单击 **+** 以添加代理和 Gateway 实例。
3. 在下一页上，单击 **开始使用**。



4. 执行以下任务：

   - 安装 Citrix ADM 代理
   - 添加您的 Gateway 实例
   - 在虚拟服务器上启用 Analytics

先决条件

- **Citrix ADM 代理安装要求**：在您的数据中心，您可以在 Citrix Hypervisor™、VMware ESXi、Microsoft Hyper-V 和 Linux KVM 服务器上安装代理。

  下表列出了管理程序必须为代理提供的虚拟计算资源。

组件	要求
RAM	8 GB（建议 32 GB 以获得更好的性能。）
虚拟 CPU	4 个（建议 8 个虚拟 CPU 以获得更好的性能）
存储空间	120 GB
虚拟网络接口	1
吞吐量	1 吉比特每秒

- **端口要求**：确保以下端口已打开，以便 Citrix ADM 代理与 Citrix Gateway 实例通信。

类型	端口	描述
TCP	80/443	用于代理与 Citrix Gateway 实例之间的 NITRO 通信
TCP	22	用于代理与 Citrix Gateway 实例之间的 SSH 通信。
UDP	4739	用于 Citrix Gateway 与代理之间的 AppFlow® 通信
ICMP	无预留端口	用于检测代理到 Citrix Gateway 实例的网络可达性。
SNMP	161, 162	用于从 Citrix Gateway 实例接收 SNMP 事件到代理。
系统日志	514	用于从 Citrix Gateway 实例接收 syslog 消息到代理。
TCP	5557	用于从 Citrix Gateway 实例到代理的日志流通信。

为了实现 Citrix ADM 代理与 Citrix Analytics 之间的通信，请确保以下端口已打开：

类型	端口	描述
TCP	443	用于代理与 Citrix Application Delivery Management 服务之间的 NITRO 通信。

为了实现 Citrix ADM 代理与 Citrix Analytics 之间的通信，请确保以下端点已列入白名单：

端点	美国区域	欧盟区域	亚太南区域
事件中心	`https://cas-eh-ns-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`	`https://cas-eh-ns-aps-alias.servicebus.windows.net/`

安装并设置代理

在您的网络环境中安装并配置 Citrix ADM 服务代理，以实现 Analytics 与数据中心中的 Gateway 实例之间的通信。

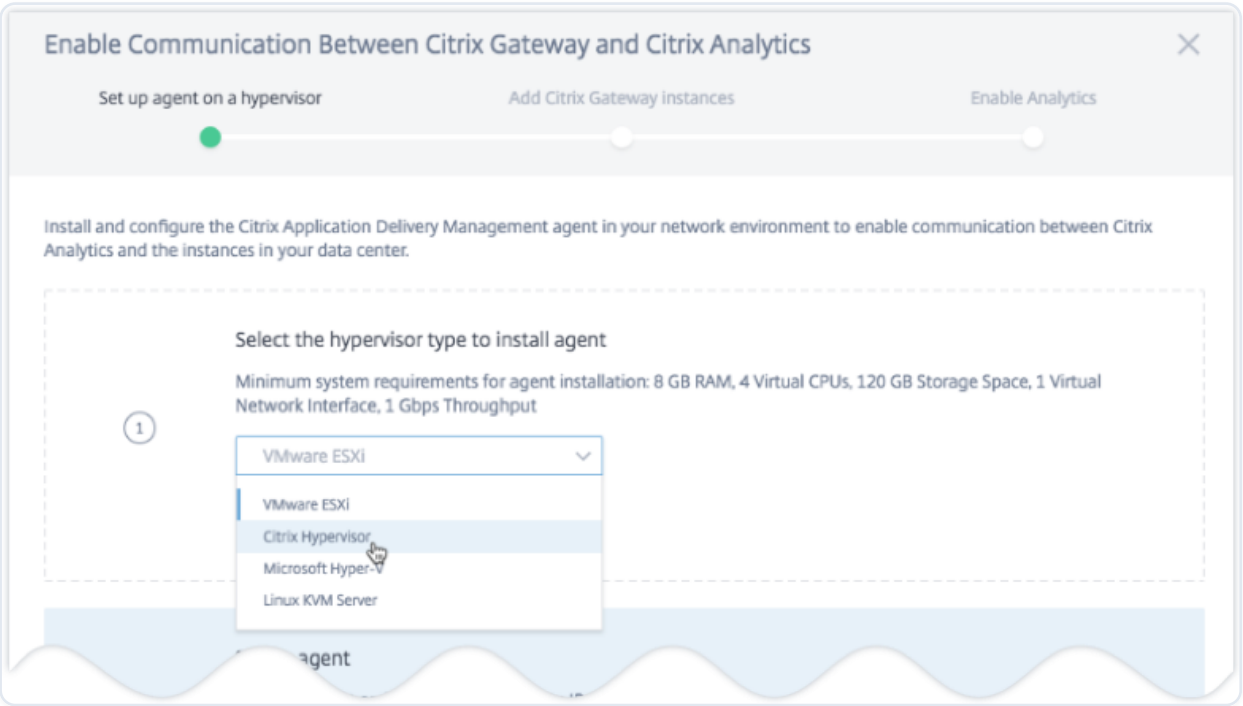
您可以在企业数据中心中的以下虚拟机管理程序上安装代理：

- 思杰虚拟机监控程序
- 威睿 ESXi
- 微软 Hyper-V
- Linux KVM 服务器

要安装和设置代理，请执行以下操作：

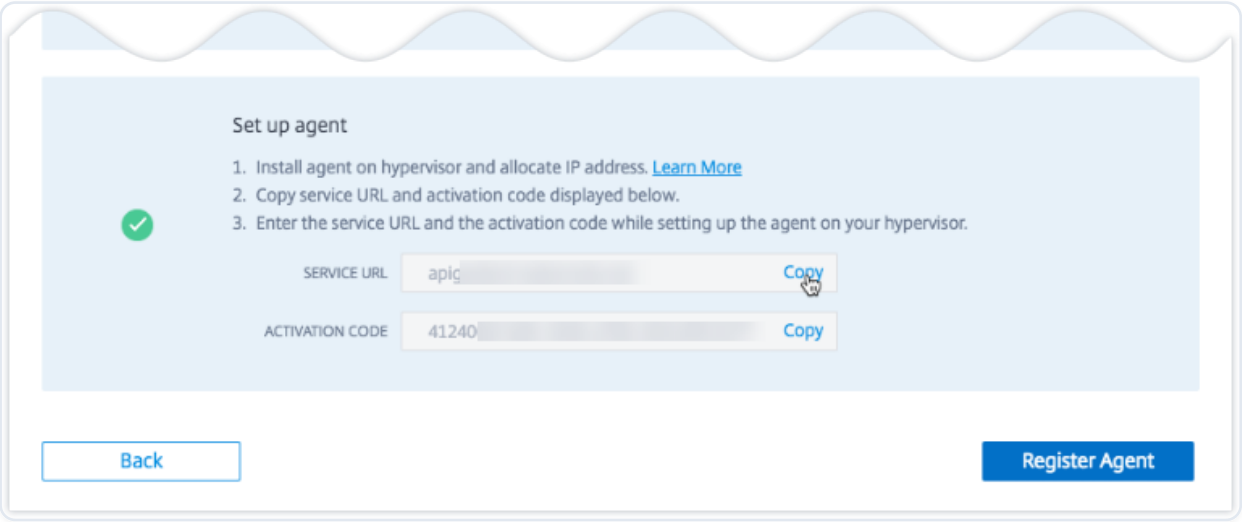
1. 下载代理映像。

   在“**在虚拟机管理程序上设置代理**”页面上，选择虚拟机管理程序，然后单击“**下载映像**”将代理映像下载到本地系统。



2. 复制服务 URL 和激活码。

   将生成服务 URL 和激活码，并显示在 UI 上，如以下图像所示。（此过程可能需要几秒钟。）代理使用服务 URL 定位服务，并使用激活码向服务注册。在虚拟机管理程序上安装代理时，输入服务 URL 和激活码。

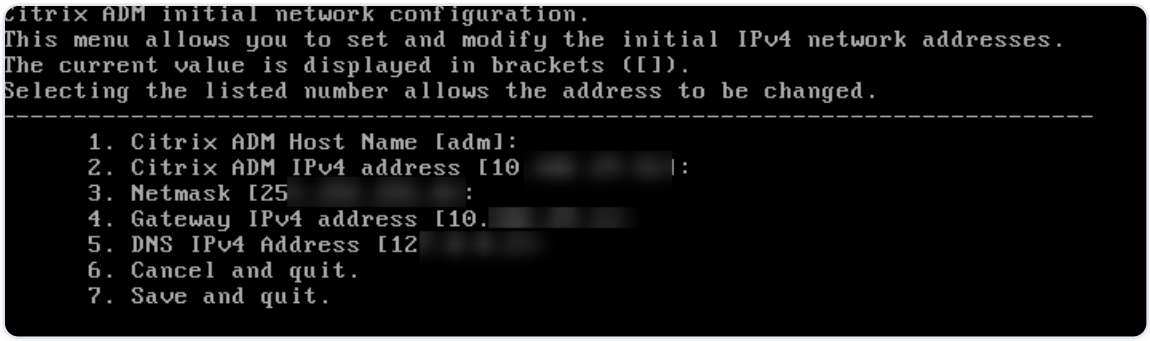


3. 在虚拟机管理程序上安装代理。

> **注意**
>
> 在开始安装代理之前，请确保：
>
> - 您拥有管理程序必须为每个代理提供的所需虚拟计算资源：RAM：8 GB，vCPU：4，存储空间：120 GB，虚拟网络接口：1，吞吐量：1 Gbps
> - 您配置 DNS 以允许您的代理访问互联网。

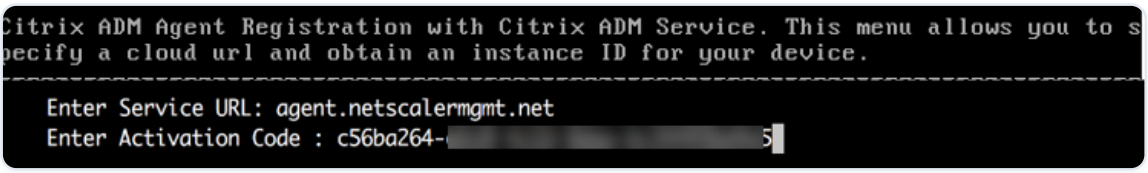
- 在 Citrix Hypervisor 上，执行以下操作：

  a. 将代理映像文件导入到您的管理程序。从“**控制台**”选项卡配置初始网络配置选项，如以下示例所示。



  如果您输入了不正确的值或想要更改任何值，请使用默认凭据 `nsrecover` / `nsroot` 登录到 shell 提示符。然后运行命令 `networkconfig`。

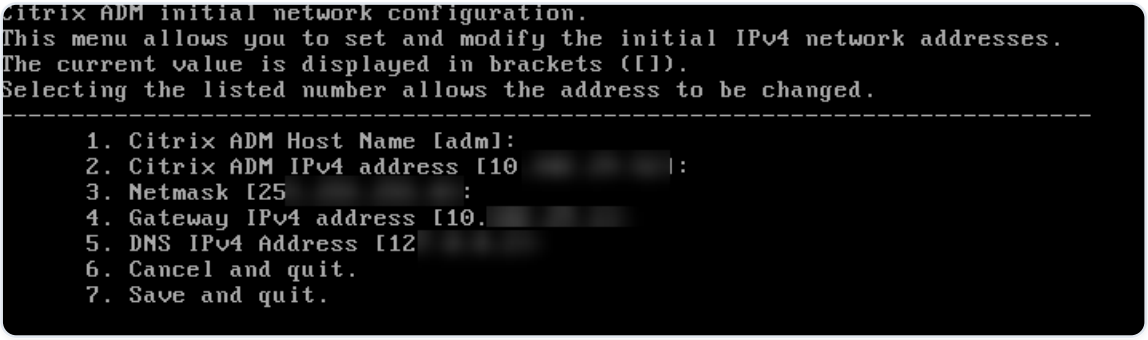
  b. 输入您在下载代理映像时保存的“**服务 URL**”和“**激活码**”。



如果您输入的服务 URL 或激活码不正确，请登录到代理的 shell 提示符，然后运行脚本：`deployment_type.py`。此脚本允许您重新输入服务 URL 和激活码。

- 在 VMware ESXi 管理程序上，执行以下操作：

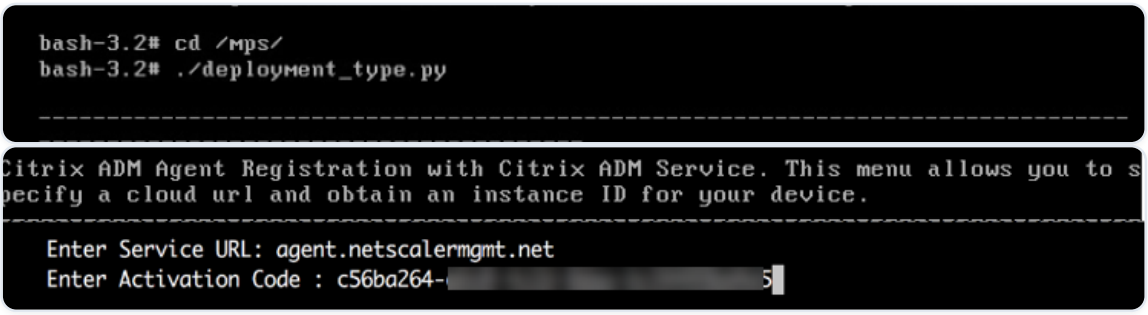
  a. 将代理映像文件导入到您的管理程序。从“**控制台**”选项卡配置初始网络配置选项，如以下示例所示。



  b. 配置网络后，在出现提示时，使用默认凭据 `nsrecover` / `nsroot` 登录到代理的 shell 提示符。



  c. 导航到 **/mps** 目录，运行脚本，然后输入您在下载代理映像时保存的“**服务 URL**”和“**激活码**”。

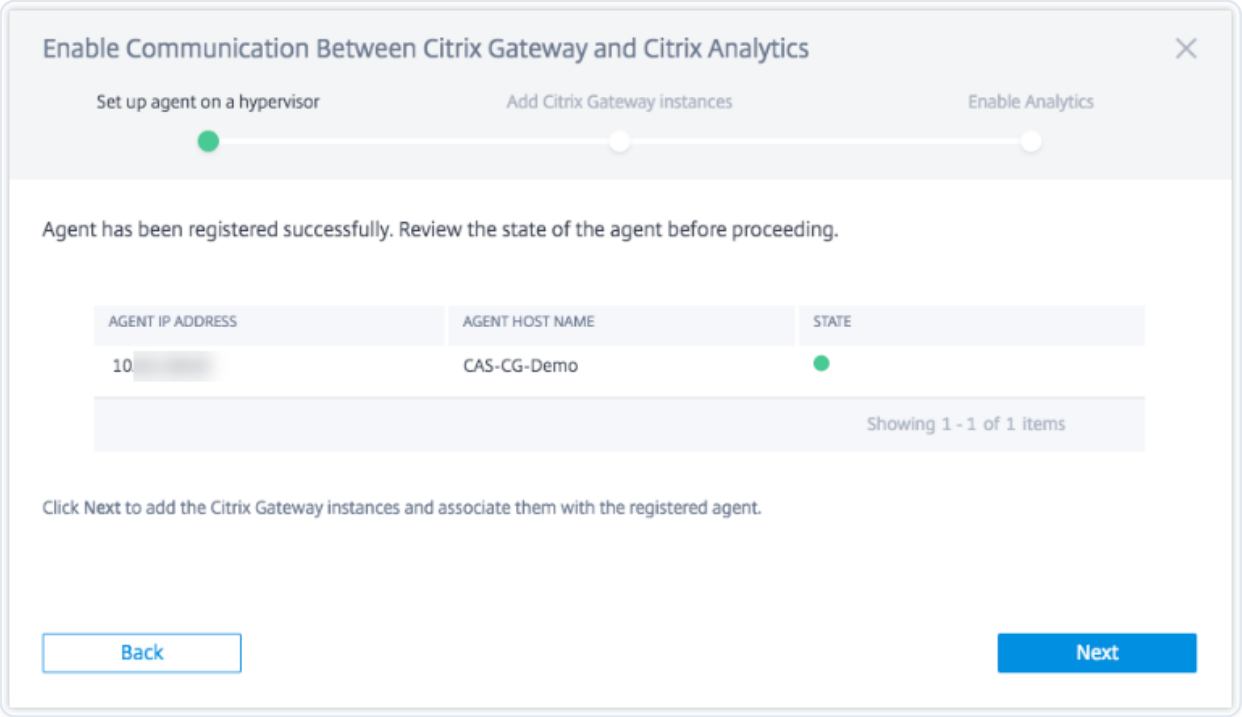


> **注意**

> 您可以使用相同的映像文件安装多个代理。但是，您不能在多个代理上使用相同的激活码。要生成新的激活码，请访问 Citrix Analytics，然后在“在虚拟机管理程序上设置代理”步骤中，再次单击 **下载映像**。将生成一个新的激活码。

4. 注册代理。

   代理注册成功后，代理将重新启动以完成安装过程。代理重新启动后，访问 Citrix Analytics 并单击 **注册代理**，然后验证代理的状态。

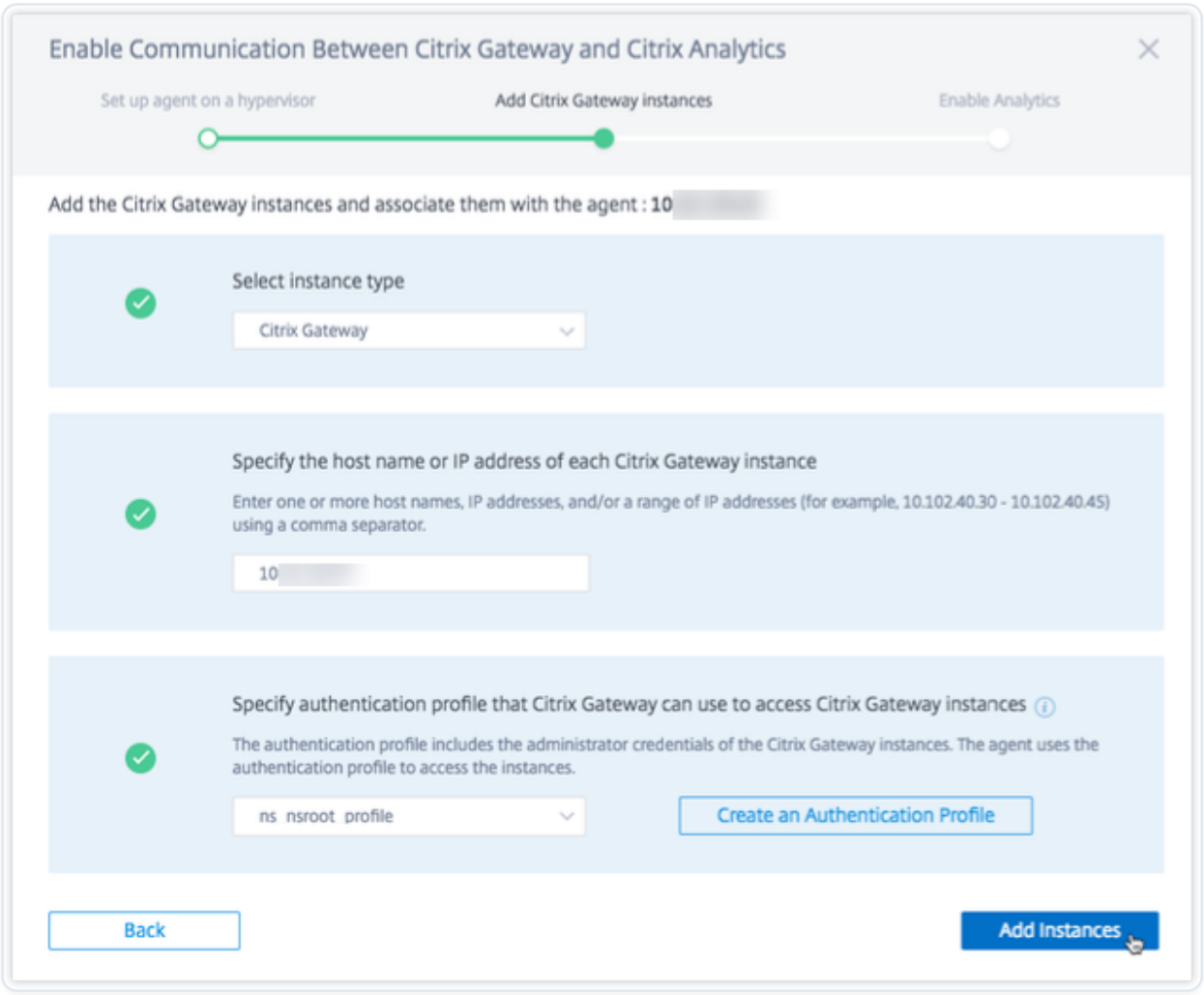


   当代理状态为 UP（旁边有一个绿点表示）时，单击 **下一步** 开始向服务添加实例。

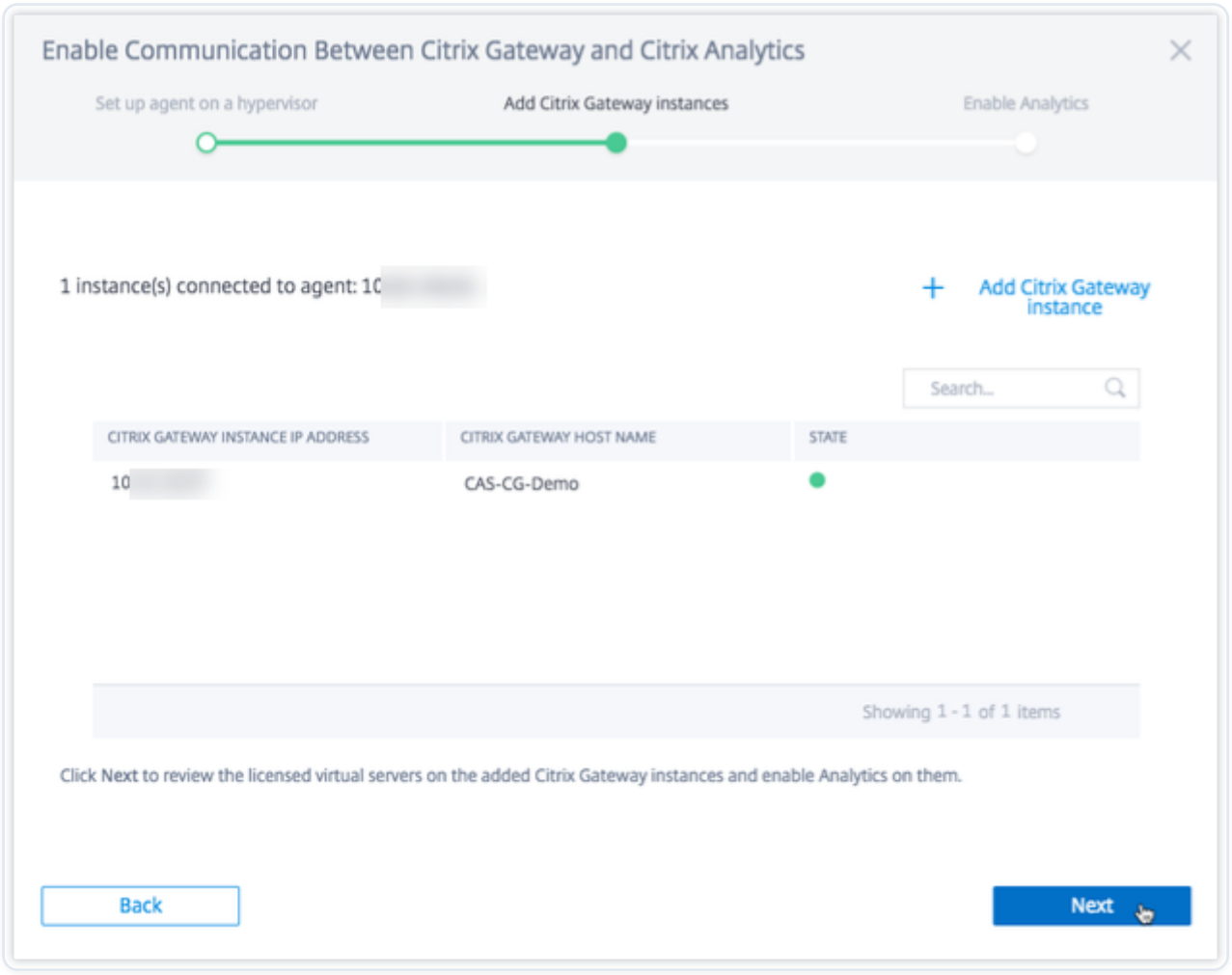
添加 Citrix Gateway 实例

实例是 Citrix Gateway 设备或虚拟设备，它们是 Citrix Analytics 的数据源。

1. 在 **添加 Citrix Gateway 实例** 页面上，选择实例类型并指定要发现的 Gateway 实例的主机名、IP 地址或 IP 地址范围。
2. 创建代理可用于访问 Gateway 实例的身份验证配置文件。此配置文件是 Gateway 实例的管理员凭据。然后，单击 **添加实例**。



添加实例后，您可以查看已成功发现的实例数量。要添加更多实例，请单击 **添加 Citrix Gateway 实例**。



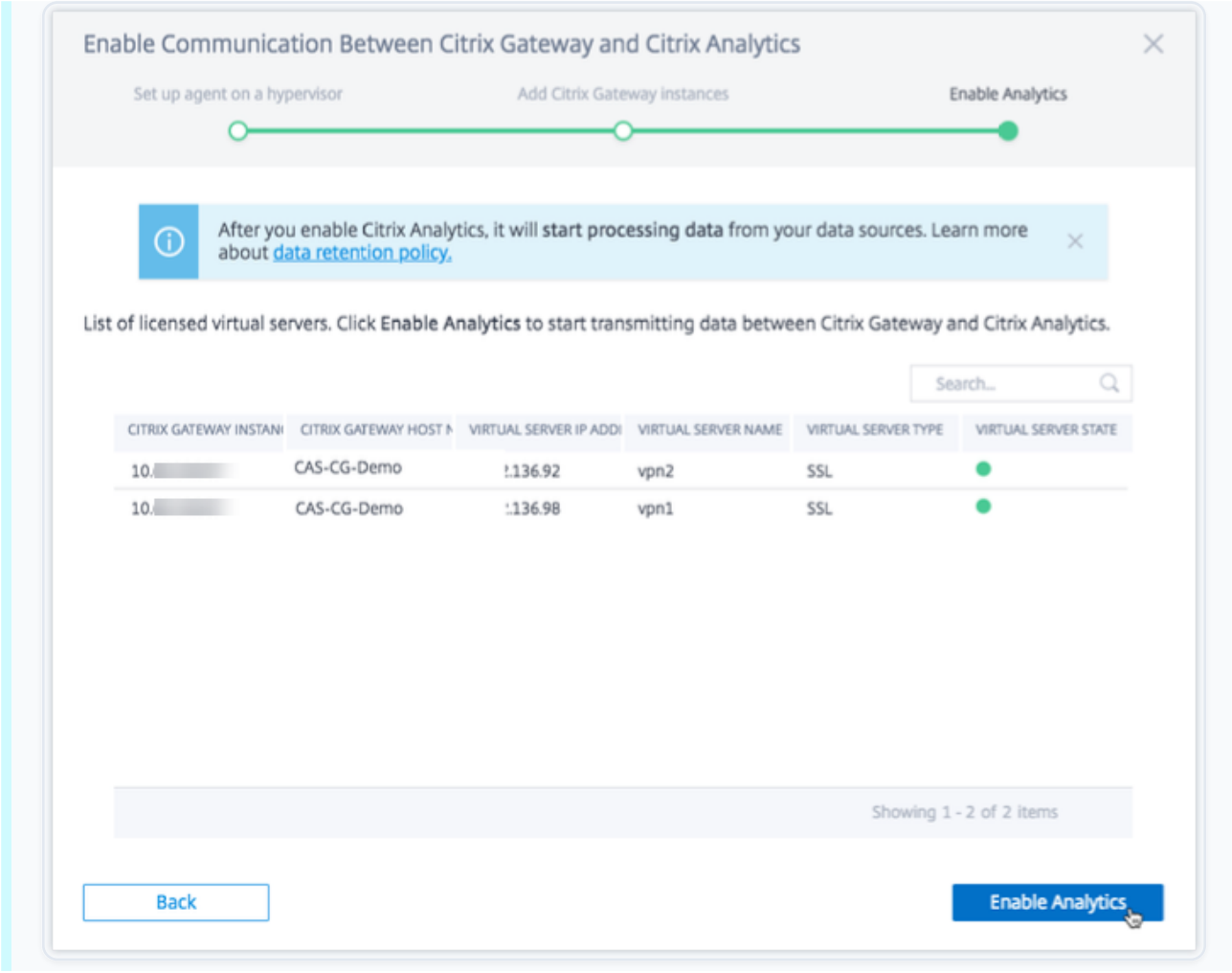
单击“**下一步**”以启用分析。

启用分析

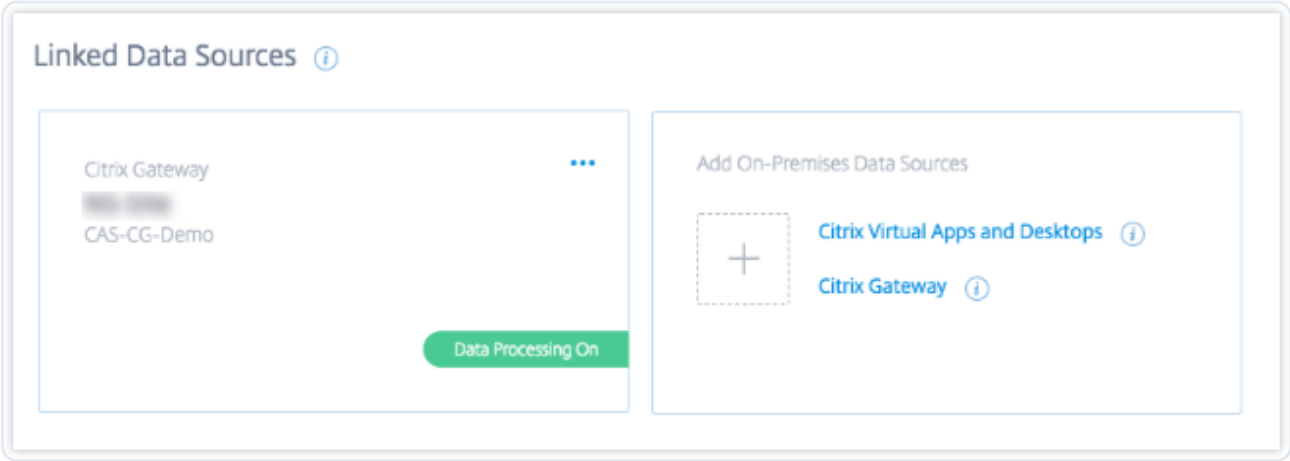
Citrix Analytics 会自动发现已添加的 Citrix Gateway 实例上的许可虚拟服务器。在所有发现的虚拟服务器上启用分析。

在“**启用分析**”页面上，默认情况下会显示 Gateway 实例中的所有许可虚拟服务器。查看许可虚拟服务器列表，然后单击“**启用分析**”以在虚拟服务器上启用分析。

> **注意**
>
> 虚拟服务器可能需要大约 10 分钟才能显示在页面上。



站点卡的状体更改为“**数据处理已开启**”。您可以查看收到的事件。



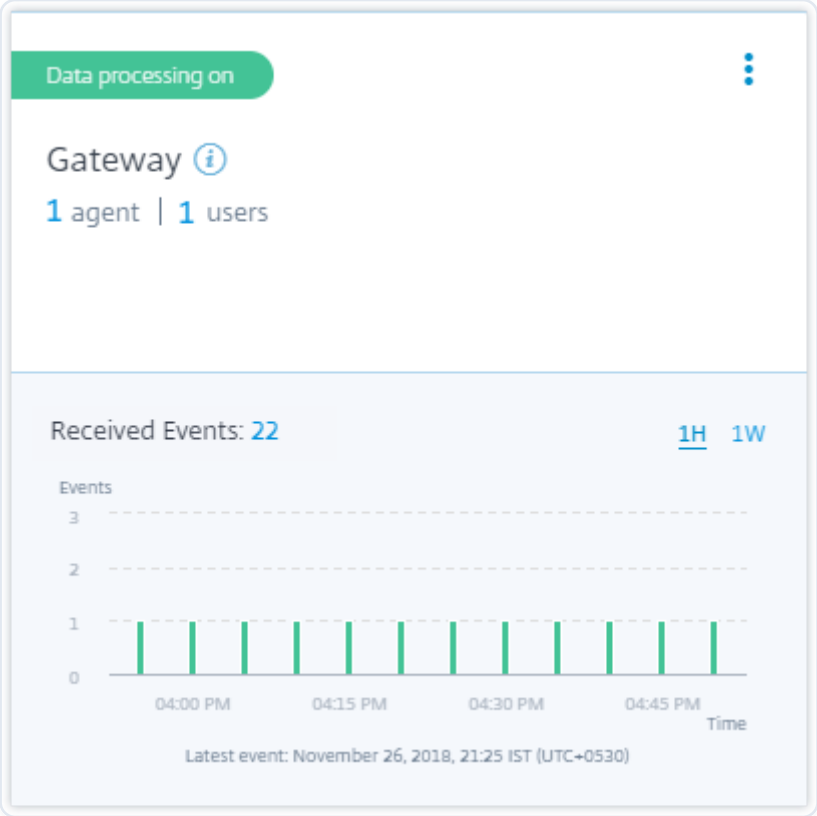
观看入门视频

以下视频显示了载入 Gateway 实例的步骤：

<iframe src="https://www.youtube.com/embed/Bw_CXAUHINk" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

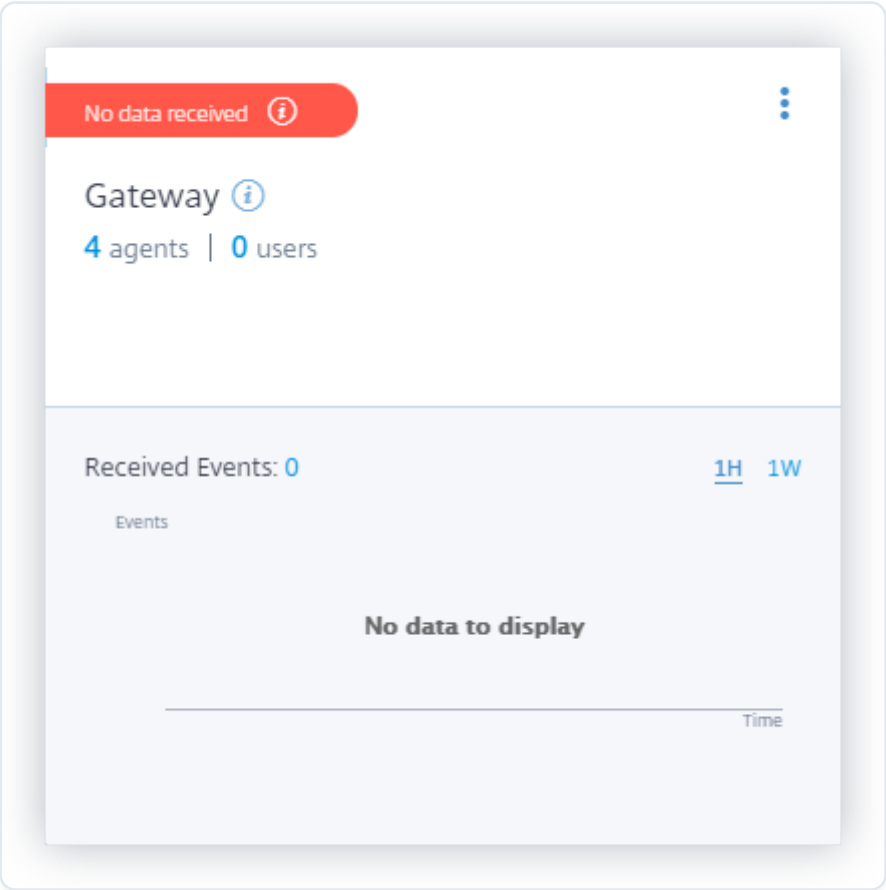
查看收到的事件、用户和代理

站点卡显示 Gateway 用户数、Citrix ADM 代理数以及过去一小时（默认时间选择）从数据源收到的事件。您还可以选择 1 周 (**1W**) 并查看数据。单击用户数可在“**用户**”页面上查看。单击代理数可查看 Citrix Gateway 实例和代理。



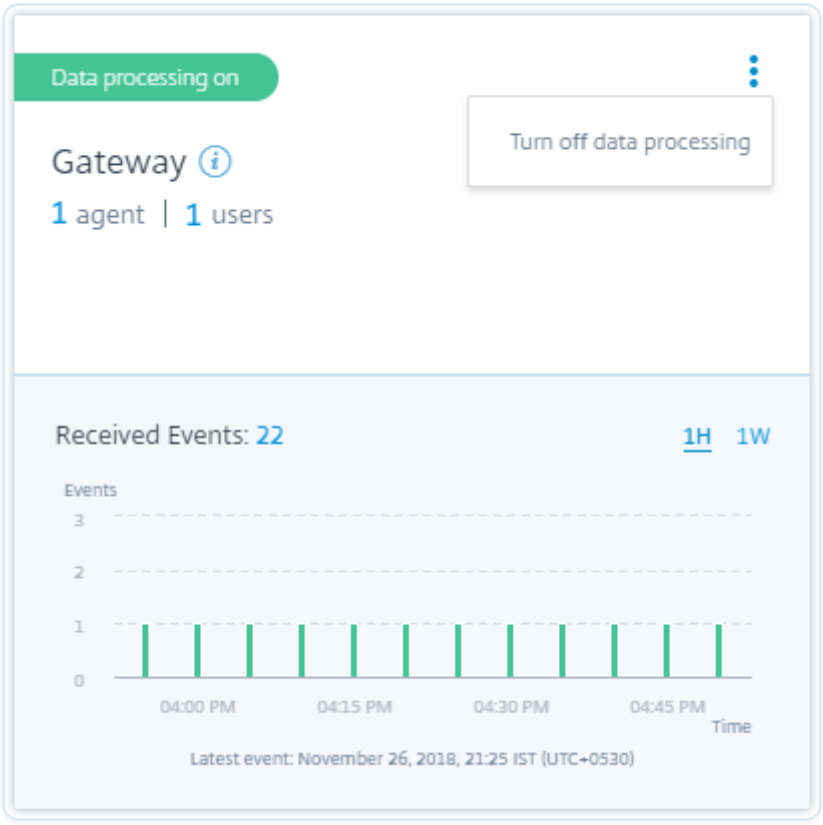
启用数据处理后，站点卡片可能会显示“**未收到数据**”状态。此状态出现的原因有两个：

1. 如果您是首次开启数据处理，事件需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件后，状态将变为“**数据处理已开启**”。如果一段时间后状态未更改，请刷新“**数据源**”页面。
2. 在过去一小时内，Analytics 未从数据源收到任何事件。

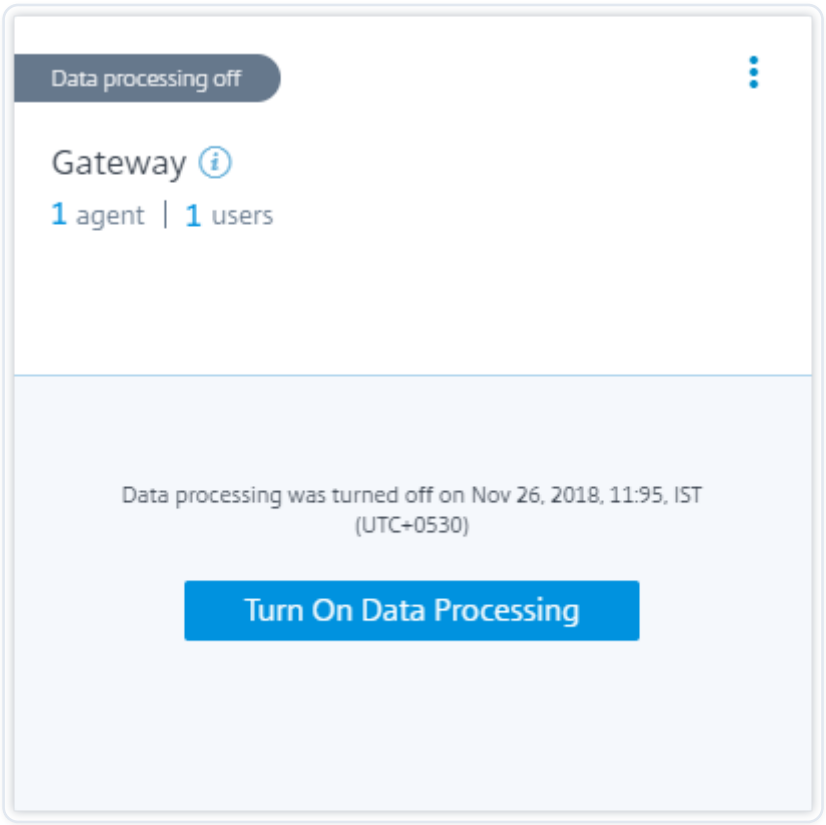


开启或关闭数据处理

要停止数据处理，请单击站点卡片上的垂直省略号 (⋮)，然后单击“**关闭数据处理**”。Citrix Analytics 将停止处理此数据源的数据。

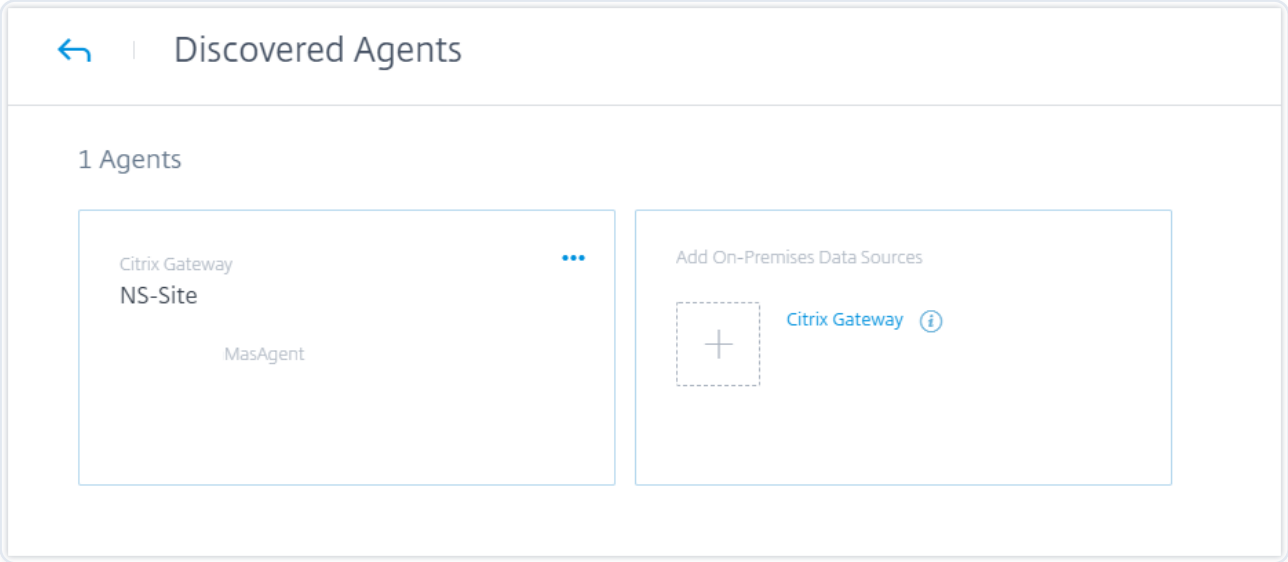


要再次启用数据处理，请单击“**开启数据处理**”。



添加更多 Gateway 实例

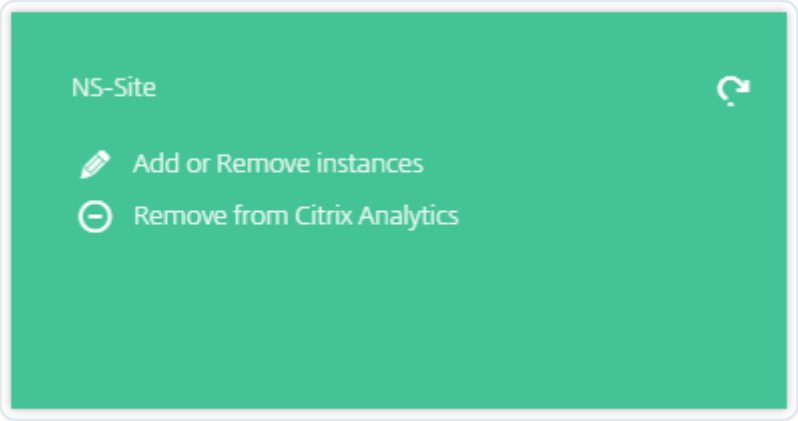
如果要添加更多 Gateway 实例，请单击 Gateway 站点卡片上的代理数量以查看“**已发现代理**”页面。在“**添加本地数据源**”磁贴中，单击“**Citrix Gateway**”。



管理数据源

您还可以向代理添加更多实例或删除与代理关联的实例。您还可以从 Citrix Analytics 中删除代理及其关联的实例。

翻转代理站点卡片并执行以下操作之一：



- **添加或删除实例**。您可以向代理添加更多 Gateway 实例，并在这些实例上配置的虚拟服务器上启用 Analytics。您还可以删除已添加到代理的实例。当您将实例与代理解除关联时，Citrix Analytics 无法与该实例通信。
- **从 Citrix Analytics 中删除**。删除代理站点后，Citrix Analytics 将停止从与该代理关联的实例收集数据。但所有先前处理的数据在保留期内仍然可用。

Citrix 虚拟应用和桌面™ 数据源

本文介绍了使用 StoreFront 将本地 Citrix Virtual Apps and Desktops 站点连接到 Citrix Analytics 的步骤。本文中提到的载入步骤适用于以下两种产品：Citrix Analytics for Performance（性能分析）和 Citrix Analytics for Security（安全分析）。

有关每种产品特定的载入步骤，请参阅以下文章：

- 使用 Citrix 性能分析 配置本地 Citrix 虚拟应用和桌面 站点
- 为 Citrix 安全分析 配置 Citrix 虚拟应用和桌面 和 Citrix DaaS 数据源

使用 StoreFront 载入 Citrix Virtual Apps and Desktops 本地站点

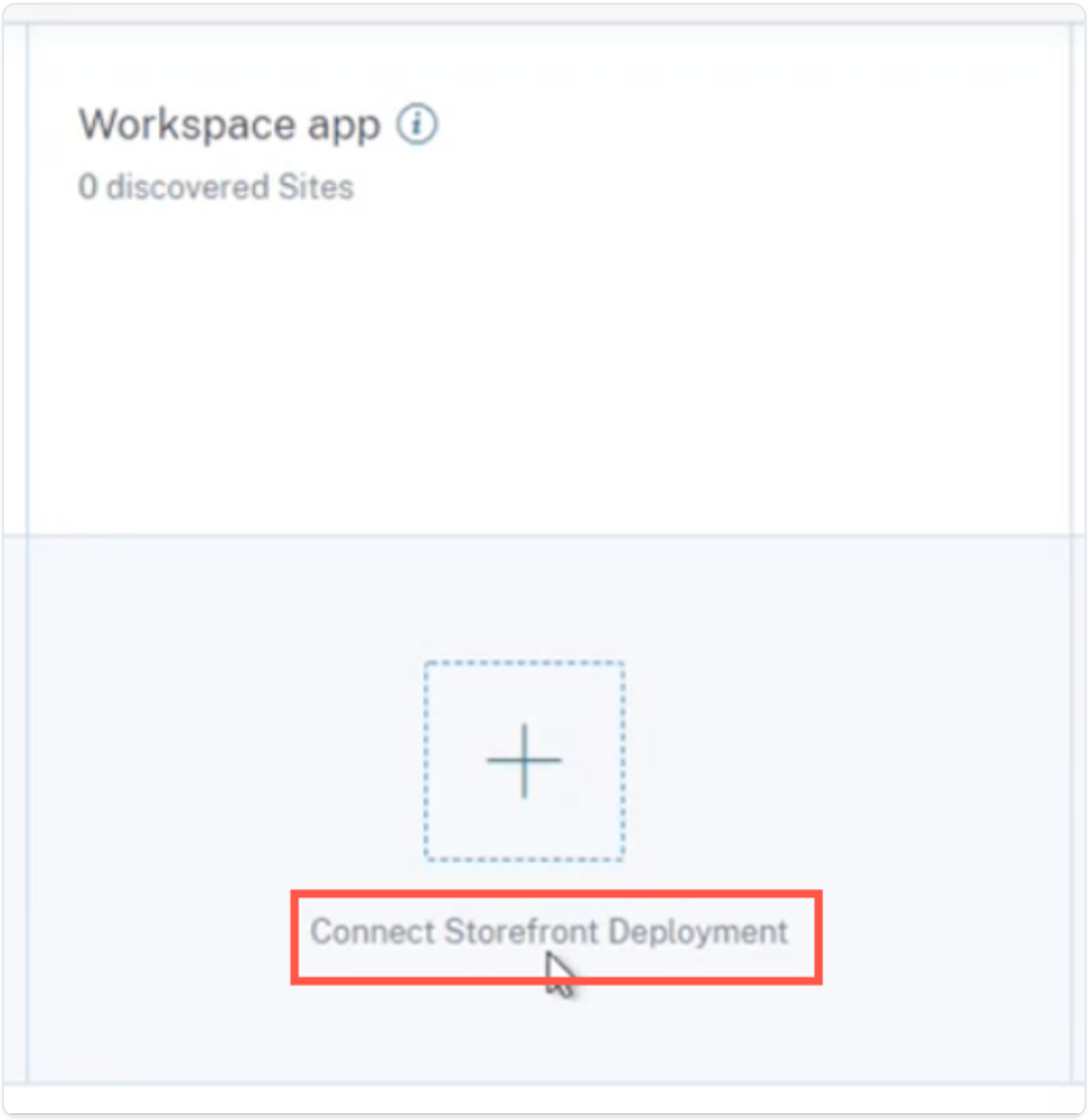
如果您的组织使用本地 StoreFront™ 部署，则必须配置 StoreFront 服务器，以使 Citrix Workspace™ 应用程序能够将事件发送到 Citrix Analytics。Citrix Analytics 处理事件，以提供有关 Citrix IT 基础架构性能和用户行为的可操作见解。

有关如何为 Citrix Analytics 配置 StoreFront 部署的更多信息，请参阅 StoreFront 文档中的Citrix Analytics 服务文章。

以前，使用 Citrix Apps and Desktops 本地站点的客户必须使用站点聚合来载入 Citrix Analytics for Security™ 和 Performance 的本地站点。

您现在可以载入 Citrix Apps and Desktops 本地站点，而无需依赖站点聚合。

即使您没有将任何站点添加到站点聚合中，您也可以在工作区应用程序上看到“**连接 Storefront 部署**”选项。



先决条件

开始之前，请确保满足以下条件：

- 您的 StoreFront 版本必须是 1906 或更高版本。
- StoreFront 部署必须能够连接到以下地址：
  - `<https://*.cloud.com>`
  - `<https://api.analytics.cloud.com>`
- StoreFront 部署必须打开端口 443 以进行出站 Internet 连接。网络上的任何代理服务器都必须允许此通信与 Citrix Analytics 进行。

- 如果 StoreFront 部署托管在使用 Web 代理连接到 Internet 的 Web 服务器上，则必须手动配置每个商店的代理以允许出站流量。StoreFront 不会自动使用主机 Web 服务器的代理设置。有关更多信息，请参阅 配置托管在使用 HTTP 代理的 StoreFront 部署。
- 必须使用以下客户端之一访问 StoreFront 部署：
  - 兼容 HTML5 的浏览器中的 Citrix Receiver™ for websites。

    > **注意**
    >
    > 如果您是 HTML5 用户，当在 StoreFront 上启用某些配置时，Citrix Virtual Apps and Desktops 可以启动事件。有关配置步骤的信息，请参阅 Citrix Workspace app for HTML5 文档中的 安装 文章。对于与打印相关的事件，必须在 StoreFront 上配置额外的策略。有关更多信息，请参阅 Citrix Workspace app for HTML5 文档中的 PDF 打印 文章。

  - 适用于 Windows 1907 或更高版本的 Citrix Workspace app。
  - 适用于 Linux 2006 或更高版本的 Citrix Workspace app。
  - 适用于 Mac 2006 或更高版本的 Citrix Workspace app
- 如果您使用的是 Citrix Virtual Apps and Desktops 7 1912 LTSR，则支持的 StoreFront 版本为 1912。

连接到 StoreFront 部署

您可以通过以下方式连接到 StoreFront 部署 –

- 使用**应用程序和桌面 - Workspace 应用程序**站点卡和**应用程序和桌面 - 监控**站点卡
- 使用**建议**面板

使用应用程序和桌面 - Workspace 应用程序站点卡和应用程序和桌面 - 监控站点卡进行连接

1. 导航到**设置 > 数据源 > 安全**。在**应用程序和桌面 - Workspace 应用程序**站点卡上，单击垂直省略号 (⋮)，然后选择**连接 StoreFront 部署**。

   连接商店安全性(/en-us/citrix-analytics/media/store-front-site-card-1.png)
2. 导航到**设置 > 数据源 > 性能**。在**应用程序和桌面 - 监控**站点卡上，单击垂直省略号 (⋮)，然后选择**连接 StoreFront 部署**。

连接商店性能(/en-us/citrix-analytics/media/cvad-performance-sf-connect.png)

StoreFront 入门向导或**连接 StoreFront 部署**弹出窗口出现。

3. 单击**下载程序包**。

StoreFront 入门向导(/en-us/citrix-analytics/media/sf-onboarding-wizard.png)

> **注意**
>
> 该文件包含敏感信息。请将文件保存在安全的位置。

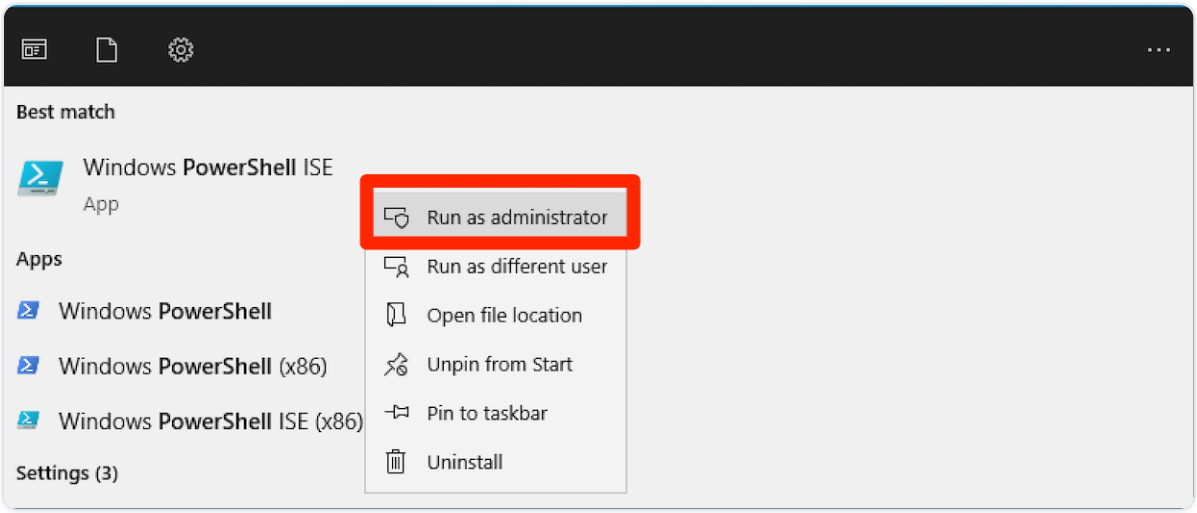
4. 要配置 StoreFront 部署，

   a. 将安装程序包复制到 StoreFront 服务器。

   b. 解压缩复制的文件，并导航到该文件夹（在 PowerShell 中）。

   c. 您必须以管理员身份运行以下命令才能载入 StoreFront：

      .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront

      有关更多选项或参数，请参阅PowerShell 脚本 部分。

   d. 打开 StoreFront 服务器并执行 PowerShell 脚本。

   e. 如果在运行 OnboardStorefront 后 StoreFront 站点仍未显示在 Citrix Analytics Service GUI 中，请运行 iisreset 命令。

   f. 登录到 Citrix Analytics Service GUI，并验证群集 ID 是否与脚本在控制台中记录的 ID 匹配。

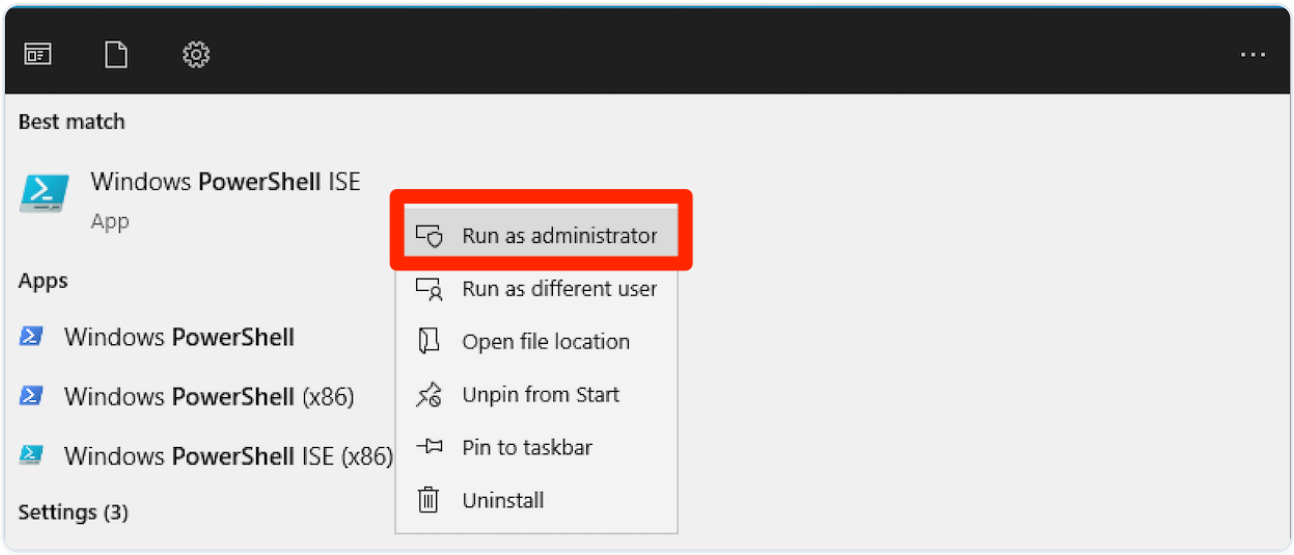
   g. 配置完成后，登录到 Citrix Analytics 以查看已连接的 StoreFront 部署。

5. 配置成功后，单击 **完成**。

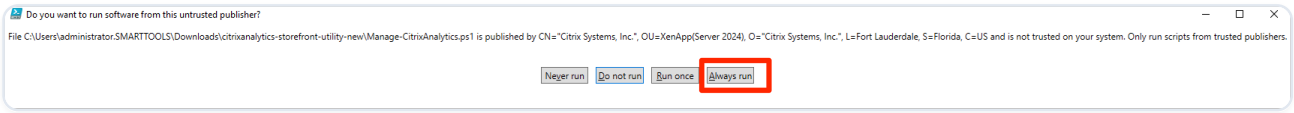
6. 单击 **启用数据处理** 以允许 Citrix Analytics 处理数据。

PowerShell 脚本

已引入新的 PowerShell 脚本，以简化 StoreFront 载入 Citrix Analytics Service 的过程。此 PowerShell 脚本可自动执行先决条件检查、安装和配置 StoreFront 的过程。PowerShell 脚本需要以管理员模式运行。



客户可以在 StoreFront 上执行此 PowerShell 脚本，以载入、卸载、执行自检、故障排除以及验证载入 Citrix Analytics Service GUI 是否成功。当客户首次执行脚本时，会出现安全警告消息以确认发布者。如果发布者受信任，请选择“始终运行”选项。



PowerShell 脚本可在“**连接 StoreFront 部署**”页面上找到，它位于一个 zip 文件中，其中包含 StoreFrontConfiguration.json 文件、一些 CCAuth 和 dll 文件。PowerShell 脚本日志保存在“**下载**”文件夹下的 cas-logs 文件中。

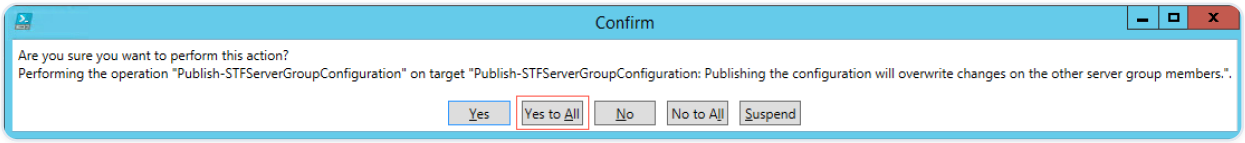
PowerShell 脚本支持以下参数：

- **SelfCheck**：**SelfCheck** 参数用于验证是否满足 StoreFront 载入的先决条件。它会检查 StoreFront 安装、所需版本、出站连接、cURL Analytics 服务器网络连接、互联网连接、服务器组配置以及任何现有的 Citrix Analytics Service 配置。使用以下命令运行 **selfcheck**：

  ```
  .\Manage-CitrixAnalytics.ps1 –param SelfCheck
  ```

- **OnboardStorefront**：**OnboardStoreFront** 参数会快速执行自检，以验证 Citrix Analytics Service 配置的设置就绪情况。如果设置已就绪，它会导入 Citrix Analytics Service 配置，并将更改发布到服务器组中的其他服务器。对于服务器组，PublishConfiguration 命令会自动从脚本

运行，以将 StoreFront 配置发布到该 StoreFront 中的所有服务器。您会看到一个弹出窗口，用于确认 `PublishConfiguration` 操作。选择“**全部是**”按钮。



配置发布成功完成后，脚本会调用 Citrix Analytics Service API，以检查 StoreFront 是否已载入到 Citrix Analytics Service GUI。要调用此 API，需要私钥进行身份验证。要生成此私钥，您需要 CCAuth 和 dll 文件以及下载的 JSON 文件中提供的凭据。

> **注意**
>
> StoreFront 载入过程完成后，StoreFront 可能需要两到五分钟才能显示在 Citrix Analytics Service GUI 中。如果 StoreFront 站点未显示在 Citrix Analytics Service GUI 中，您必须执行 IISRESET 以重置 Internet 信息服务。

使用以下命令运行 **OnboardStoreFront**：

```
.\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
```

- **IsOnboarded**：**IsOnboarded** 参数用于验证 StoreFront 是否已载入到 Citrix Analytics Service GUI。脚本在退出前会等待一分钟，但是，StoreFront 在成功载入后可能需要长达五分钟才能显示在 GUI 中。您必须运行此命令进行验证。此命令还依赖于 CCAuth 和 dll 文件。使用以下命令运行 **IsOnboarded**：

  ```
  .\Manage-CitrixAnalytics.ps1 –param IsOnboarded
  ```

- **Troubleshoot**：等待五分钟后，如果 StoreFront 站点未显示在 Citrix Analytics Service GUI 中，您必须执行 IISRESET 以重置 Internet 信息服务。如果 StoreFront 站点仍然未显示在 GUI 中，请使用 **Troubleshoot** 参数。它可帮助您排查任何连接问题并收集日志。使用以下命令运行 **Troubleshoot**：

  ```
  .\Manage-CitrixAnalytics.ps1 –param TroubleShoot
  ```

  故障排除参数适用于以下两种用例：

  - **用例 1**：作为自检的一部分，如果 curlAnalytics 失败，则会创建防火墙规则。此防火墙规则会打开 443 端口并验证其与 Analytics 的连接。如果无法连接，则表示 Analytics 服务器不可达，脚本将在此处退出。在与 Citrix Analytics Service 的连接恢复后，重新运行脚本。

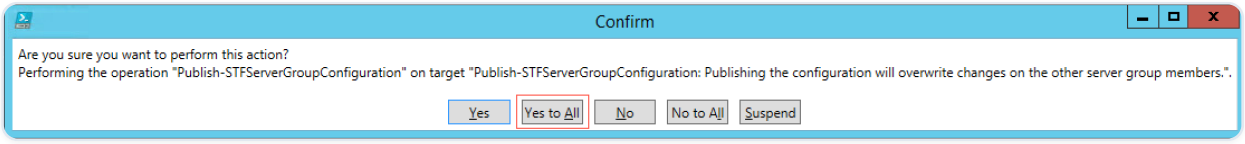
- **用例 2**：如果 cURL 运行正常，但 StoreFront 站点未在 GUI 中显示，则管理员必须从 下载 DebugView 下载 DebugView 工具 zip 文件，解压缩并将其放置在 **Downloads** 文件夹下。PowerShell 脚本首先卸载已配置的 Citrix Analytics Service。它会启用详细日志记录。然后，它会启动 DebugView 工具并重新安装 Citrix Analytics Service。最后，它会停止 DebugView 并禁用详细日志记录。

可以捕获调试视图日志并与 Citrix 支持部门共享。Citrix 管理员会进一步调试并尝试找出问题并解决。日志会生成并保存为 DebugView 文件夹中的日志文件。

您需要与 Citrix 管理员共享以下三个日志文件：

- DebugView 日志文件 (Downloads\DebugView\log)
- StoreFront 日志文件 (C:\Program Files\Citrix\Receiver StoreFront\Admin\trace)
- CAS 日志文件。这些日志是脚本执行的一部分，并保存在 **Downloads > cas-logs** 文件夹下。

对于服务器组，当脚本尝试取消或加入 StoreFront 时，`PublishConfiguration` 命令会自动运行。PublishConfiguration 命令有助于将 StoreFront 配置发布到该 StoreFront 中的所有服务器。您会看到一个弹出窗口以确认此操作。选择“**全部是**”按钮。

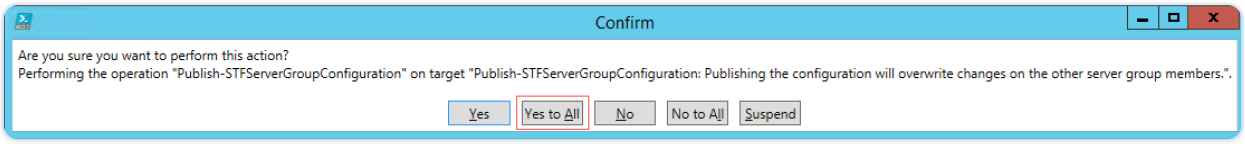


- **DeboardStoreFront**：DeboardStoreFront 参数用于从 Citrix Analytics Service 取消 StoreFront 服务器。使用以下命令运行 DeboardStoreFront：

```
.\Manage-CitrixAnalytics.ps1 –param DeboardStoreFront
```

PowerShell 脚本首先从 StoreFront 中删除所有 Citrix Analytics Service 配置，并验证删除是否成功。然后，它会检查 ServerGroup 是否存在，如果存在，则发布配置，以便将已删除的配置发布到所有 StoreFront。最后，它会调用 DeleteSiteOnboarded。如果站点未从 Citrix Analytics Service GUI 中删除，则需要手动删除 StoreFront 部署中的 StoreFront 站点以及 StoreFront 部署下的 Workspace Application 站点卡中的站点。

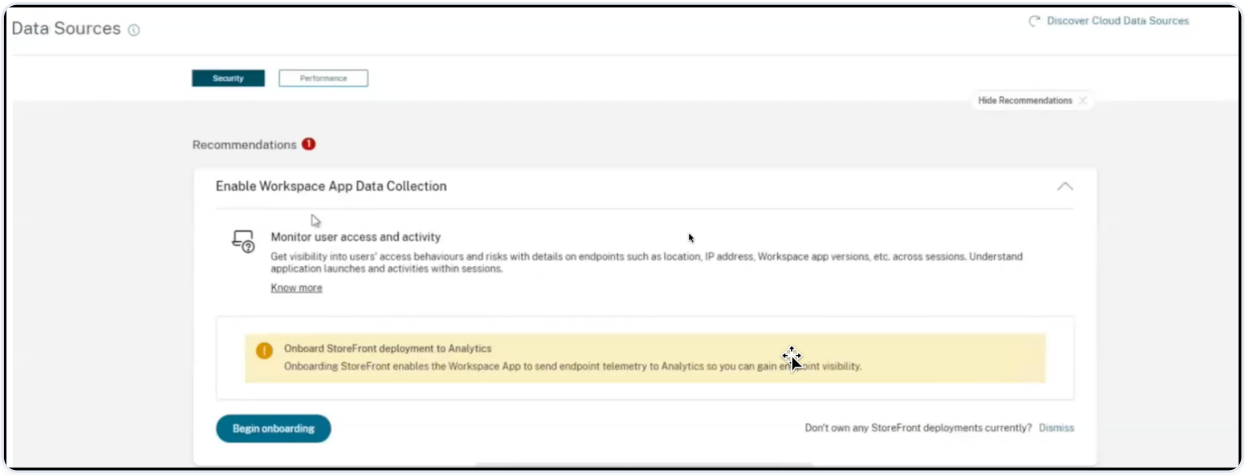
对于服务器组，PublishConfiguration 命令会自动从脚本运行，以将 StoreFront 配置发布到该 StoreFront 中的所有服务器。您会看到一个弹出窗口以确认此操作。选择“**全部是**”按钮。



使用推荐面板连接

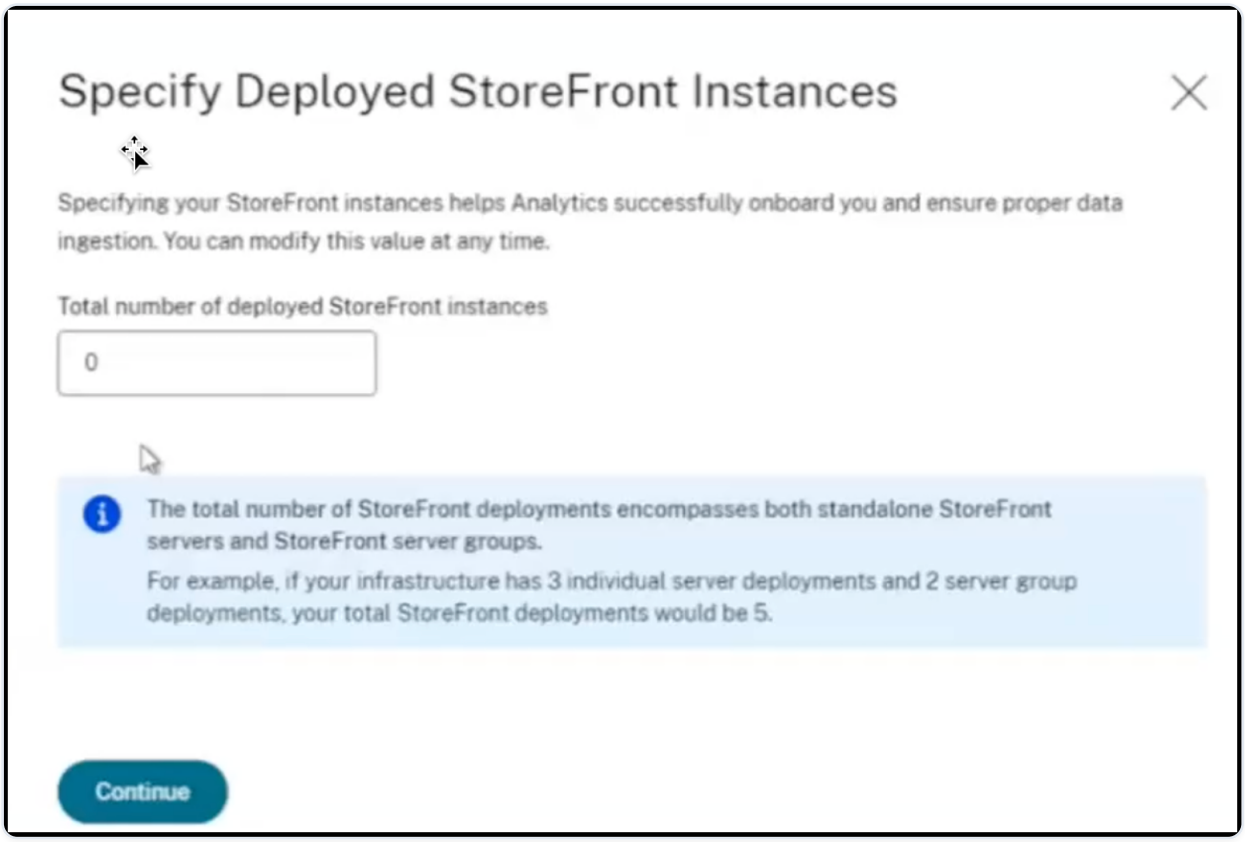
数据源页面上的**推荐**面板向用户介绍了载入数据源的重要性。它帮助用户轻松载入数据源，并提供了一个选项，让用户可以查看并确保已载入所有可用的数据源。

1. 如果您正在使用安全分析产品，请选择**设置 > 数据源 > 安全**。
2. 如果您正在使用性能分析产品，请导航到**设置 > 数据源 > 性能**。
3. 在**数据源**页面上，查看**推荐**面板上的信息和建议，以载入 Storefront 部署。



> **注意**
>
> 载入 StoreFront 数据源使 Workspace 应用程序能够将有关端点可见性的遥测数据发送到 Analytics。

4. 单击**开始载入**。将显示**指定已部署的 Storefront 实例**页面。



5. 为确保 Analytics 成功载入数据源，请指定**已部署的 StoreFront 实例总数**。

> **注意：**
>
> **已部署的 StoreFront 实例总数**是 StoreFront 组的总数，而不是单个 StoreFront 服务器的数量。

6. 单击**继续**。将显示 StoreFront 载入向导或**连接 StoreFront 部署**弹出窗口。
7. 在**连接 StoreFront 部署**页面上，单击“下载包”以下载安装包。

StoreFront 入门向导(/en-us/citrix-analytics/media/sf-onboarding-wizard.png)

> **注意**
>
> 该文件包含敏感信息。请将文件保存在安全可靠的位置。
>
> 您只能下载一个软件包并使用它来加入一个 StoreFront 组。如果您有多个 StoreFront 组，则必须为每个 StoreFront 组单独下载软件包。使用一个软件包完成一个 StoreFront 组的加入后，请再次下载该软件包并继续加入下一个 StoreFront 组。

> 如果由于某种问题，StoreFront 入门未能在两天内使用一个软件包正确完成，则必须在两天后重新下载一个新软件包。因为如果未能在两天内成功加入，软件包中的密钥将过期。

8. 要配置 StoreFront 部署，
   a. 将安装包复制到 StoreFront 服务器。
   b. 解压缩复制的文件，并在 PowerShell 中导航到该文件夹。
   c. 运行以下命令以加入 StoreFront：

      ```
      .\Manage-CitrixAnalytics.ps1 –param OnboardStorefront
      ```

   d. 打开 StoreFront 服务器并执行 PowerShell 脚本。
   e. 如果 StoreFront 站点未显示在 Citrix Analytics Service GUI 中，请运行以下命令：

      ```
      Execute iisreset
      ```

   f. 记录并验证 PowerShell 脚本中可用的群集 ID。
   g. 配置完成后，登录 Citrix Analytics 以查看连接的 StoreFront 部署。
9. 配置成功后，点击 **完成**。

如果您通过“**建议**”面板进行载入，系统会获取您已载入到 Citrix Analytics 服务的 StoreFront 部署数量。“**建议**”面板会显示，您可以查看已载入的 StoreFront 部署。您可以查看“**建议**”面板中的消息，然后点击“**标记为完成**”。

> **注意**

> 只有当所有声明的 StoreFront 部署都已载入时，“**建议**”面板和消息才会消失。

1. 点击“**开启数据处理**”以允许 Citrix Analytics 处理数据。

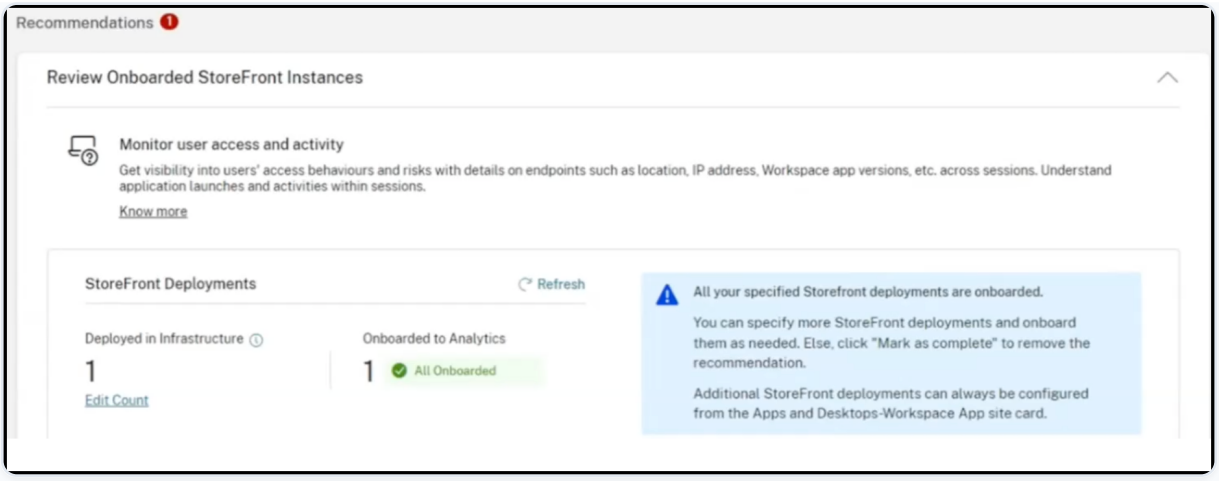
查看“建议”面板

您可以在“**建议**”面板中比较声明的 StoreFront 部署数量与已载入的 StoreFront 部署数量。

如果声明的 StoreFront 部署数量与已载入的 StoreFront 部署数量相同，则会显示“**全部已载入**”消息，表明所有 StoreFront 部署均已载入。您可以查看“**建议**”面板中的消息，然后点击“**标记为完成**”。

> **注意**

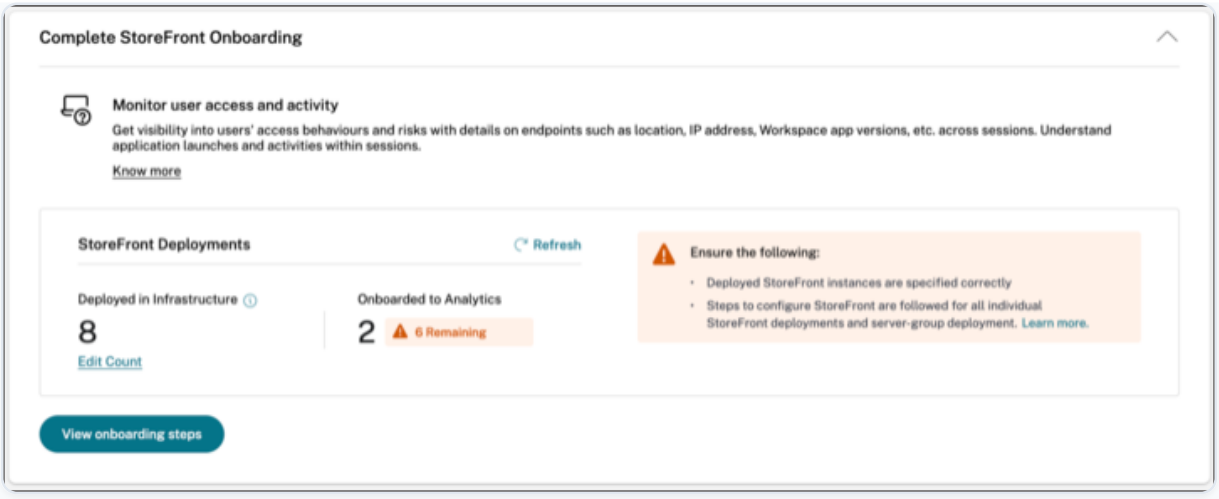
如果您想载入更多 StoreFront 部署，请点击“**查看载入步骤**”，StoreFront 载入向导或“**连接 StoreFront 部署**”弹出窗口将再次出现。



如果声明的 StoreFront 部署数量少于已载入的 StoreFront 部署数量，请点击“**编辑计数**”，然后会显示“**指定已部署的 StoreFront 实例**”页面。然后您可以输入“**已部署的 StoreFront 实例总数**”，并点击“**继续**”。StoreFront 载入向导或“**连接 StoreFront 部署**”弹出窗口将再次出现。按照步骤载入更多 StoreFront 部署。

注意：

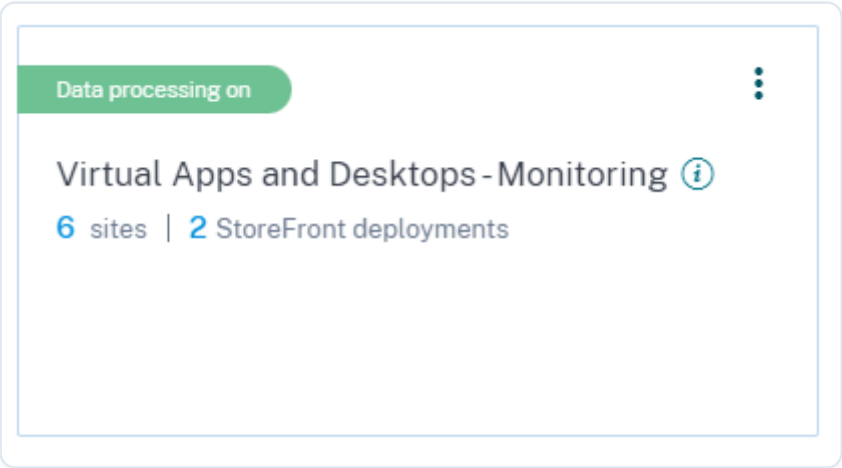
“**已部署的 StoreFront 实例总数**”是 StoreFront 组的总数，而不是单个 StoreFront 服务器的数量。



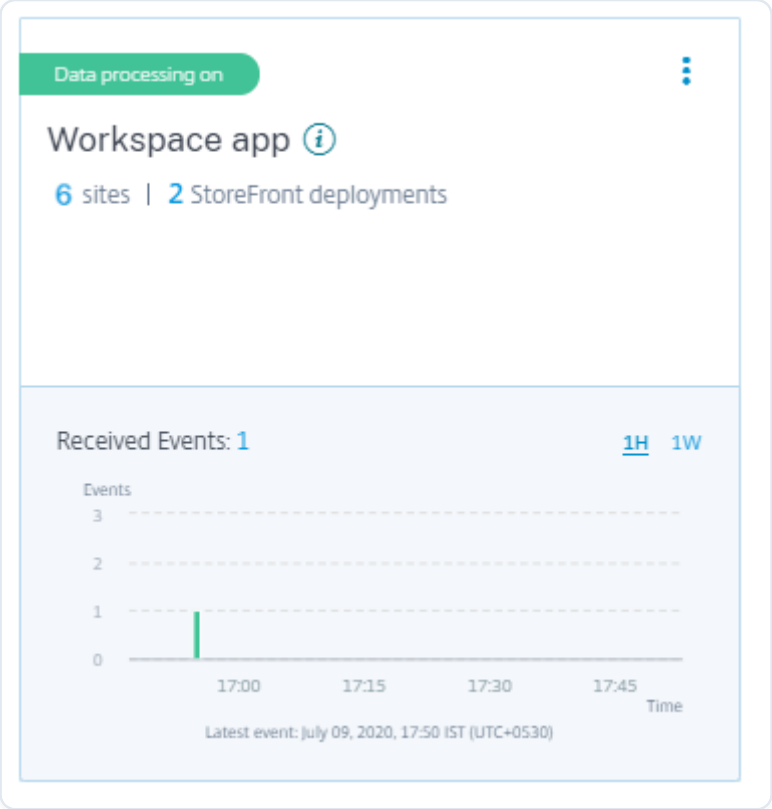
查看已连接的 StoreFront 部署

StoreFront 部署仅在配置成功后才会显示在站点卡上。站点卡显示有多少 StoreFront 部署已与 Citrix Analytics 建立连接。

- 如果您使用的是 Performance Analytics 产品，您将在 **Apps and Desktops- Monitoring** 站点卡上看到以下信息：

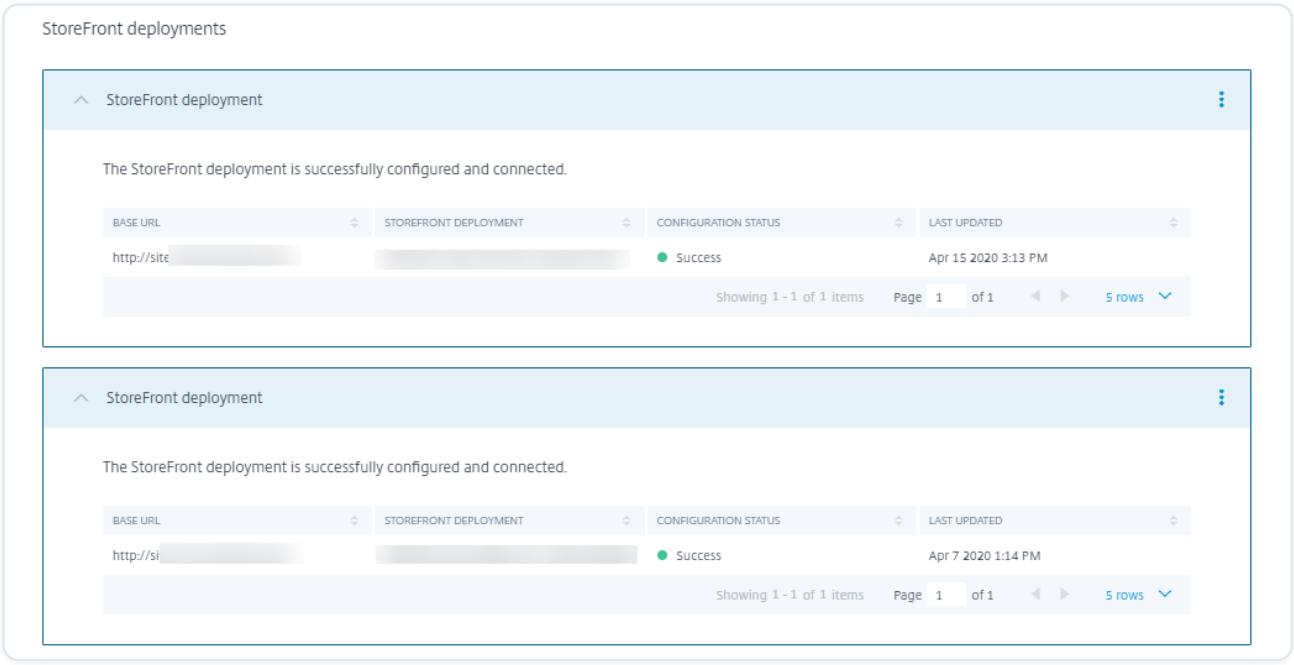


- 如果您使用的是 Security Analytics 产品，您将在 **Workspace app** 站点卡上看到以下信息：



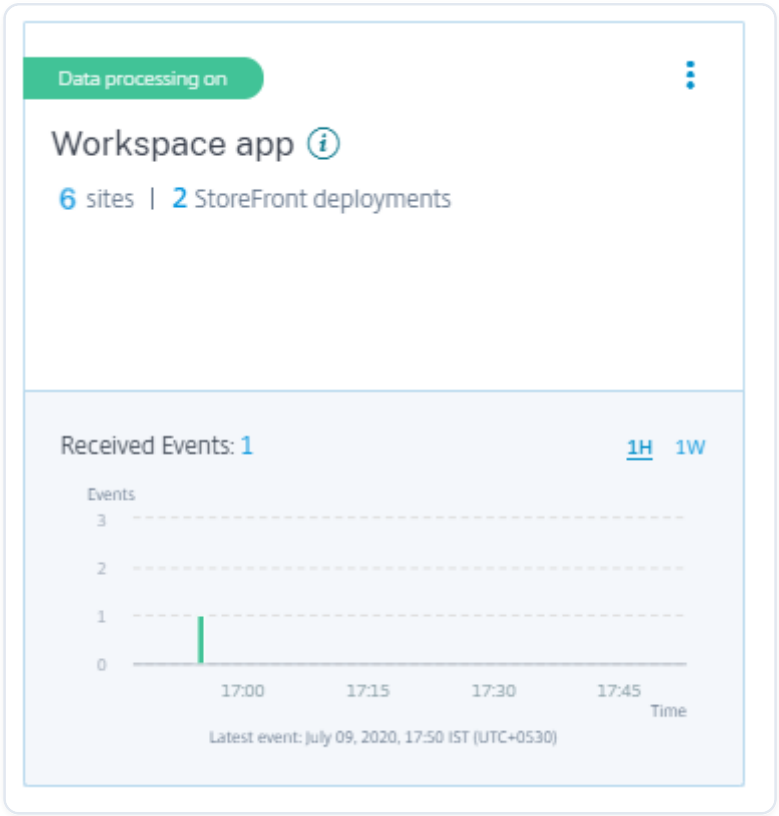
单击站点卡上的 StoreFront 部署数量以查看服务器组。

每个 StoreFront 部署都由一个基本 URL 和一个 ServerGroupID 表示。



如果您使用的是 Security Analytics 产品，站点卡还会显示有关接收到的事件的以下信息：

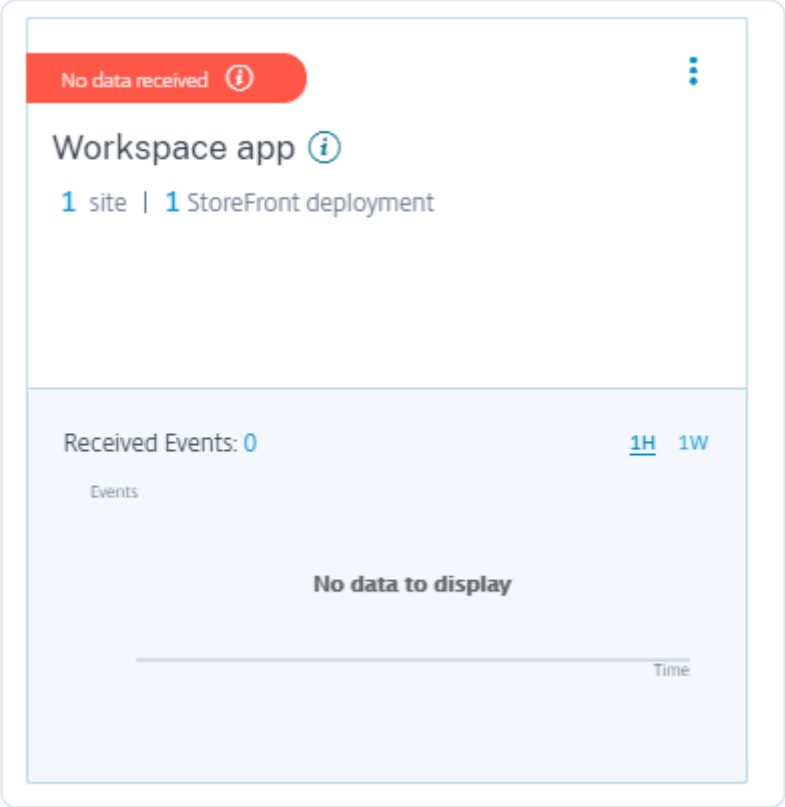
- 在过去一小时内从 StoreFront 部署接收到的事件，这是默认时间选择。您还可以选择 1 周 (1 W) 并查看数据。单击接收到的事件数量以在 自助搜索 页面上查看事件。



- 启用数据处理后，站点卡可能会显示“**未接收到数据**”状态。此状态出现的原因有两个：

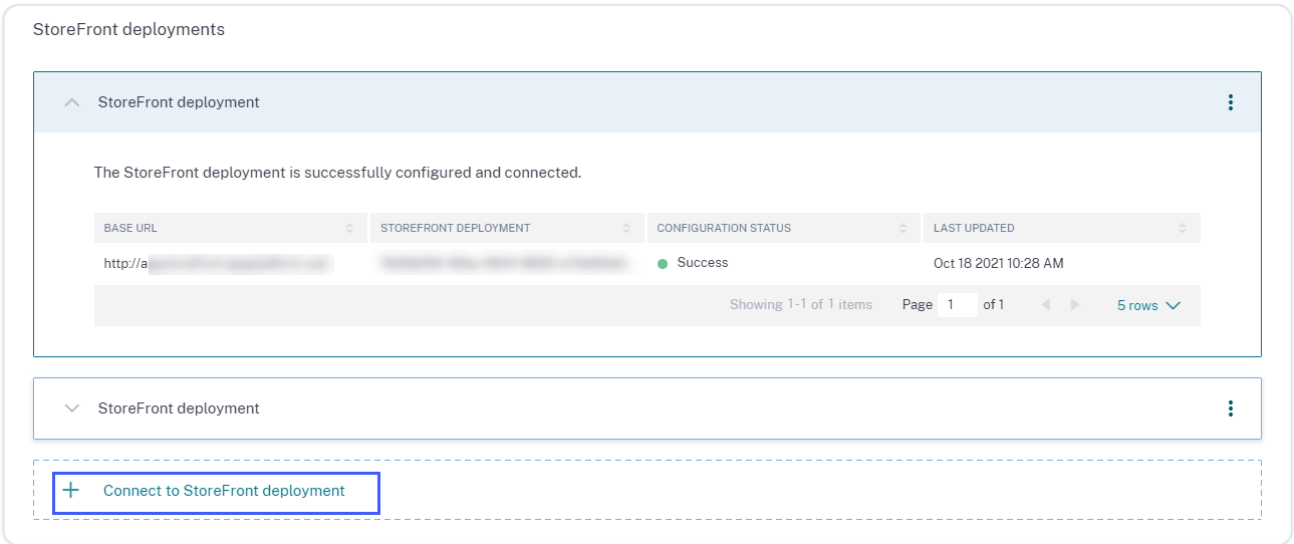
  a. 如果您是首次开启数据处理，事件需要一些时间才能到达 Citrix Analytics 中的事件中心。当 Citrix Analytics 收到事件时，状态将变为“**数据处理已开启**”。如果一段时间后状态未更改，请刷新“**数据源**”页面。

b. Citrix Analytics 在过去一小时内未从数据源接收到任何事件。



添加或删除 StoreFront 部署

要添加 StoreFront 部署，请在“**StoreFront 部署**”部分中单击“**连接到 StoreFront 部署**”。下载配置文件并按照步骤配置 StoreFront 部署。



要停止从已配置的 StoreFront 部署传输事件并将其从 Citrix Analytics 中删除，请执行以下操作：

1. 转到要从 Citrix Analytics 中删除的 StoreFront 部署。运行以下命令以从 StoreFront 服务器中删除配置设置：

```
Remove-STFCasConfiguration
```

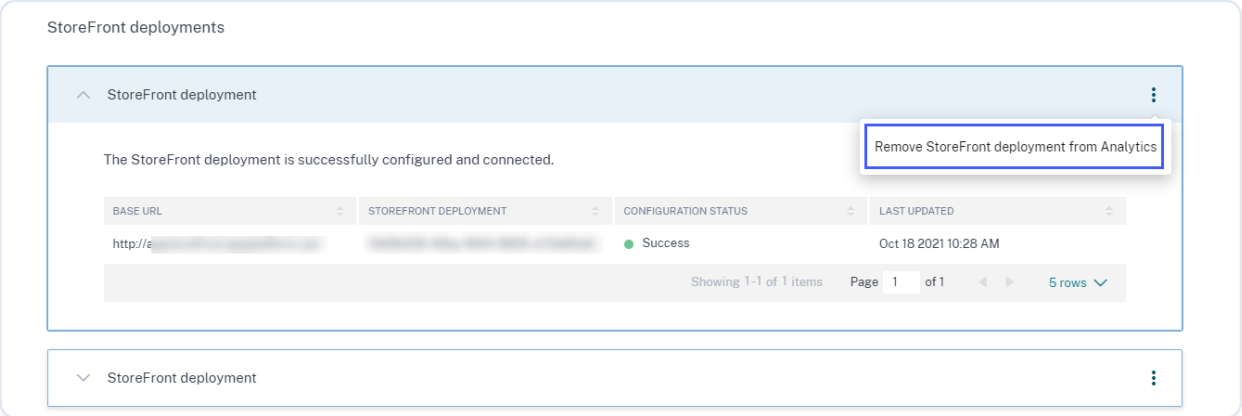
2. 如果您使用的是多服务器部署，请运行以下命令以传播更改并从 StoreFront 服务器组中的所有服务器中删除配置设置：

```
Publish-STFServerGroupConfiguration
```

3. 运行以下命令以验证配置设置是否已成功删除。如果设置已成功删除，则该命令不返回任何内容。

```
Get-STFCasConfiguration
```

4. 重新登录 Citrix Analytics，然后在“**StoreFront 部署**”部分中选择 StoreFront 部署。单击垂直省略号 (⋮) 并选择“**从 Analytics 中删除 StoreFront 部署**”。



注意

在从 Citrix Analytics 中删除 StoreFront 部署之前，请在该部署上运行指定的命令。如果您未能运行这些命令，Citrix Analytics 将继续接收事件，并且 StoreFront 部署将在下一个事件池化周期再次添加。

配置托管在使用 HTTP 代理的 Web 服务器上的 StoreFront 部署

如果 StoreFront 托管在使用 Web 代理连接到 Internet 的 Web 服务器上，则必须手动配置应用商店才能向 Citrix Analytics 注册。此配置要求您将 `<system.net>` 部分添加到应用商店的 web.config 文件中。您必须配置 StoreFront 部署上向 Citrix Analytics 发送事件的每个应用商店。

您可以通过两种方法将 `<system.net>` 部分添加到应用商店的 web.config 文件中：

- 通过 PowerShell 为一个或多个应用商店设置应用商店代理配置（推荐方法）。
- 手动将 `<system.net>` 部分添加到应用商店的 web.config 文件中。

有关这些方法的更多信息，请参阅 StoreFront 文档中的 配置 StoreFront 以使用 Web 代理联系 Citrix Cloud 并向 Citrix Analytics 注册 文章。

数据治理

技术安全概述

Citrix Cloud™ 中托管的 Analytics 服务收集 Citrix 产品组合和第三方产品的数据。这些产品称为数据源。Citrix Analytics 支持云数据源和本地数据源。本文档中的信息适用于 Citrix Analytics 及其数据源。

数据流

Citrix Analytics 自动发现客户订阅的 Citrix Cloud 数据源。但是，本地数据源需要额外的配置才能与 Citrix Analytics 集成。例如，您必须将 Citrix Virtual Apps and Desktops 站点添加到 Citrix Workspace，然后 Citrix Analytics 才能发现这些站点。同样，本地 Citrix Gateway 要求您配置 Citrix ADM 代理。有关在数据源上启用 Citrix Analytics 的更多信息，请参阅在 Citrix 数据源上启用 Analytics。

您可以将 Microsoft Graph Security 和 Microsoft Active Directory 等一些第三方产品与 Citrix Analytics 集成。有关详细信息，请参阅以下主题：

- 在 微软图形安全 上启用分析功能
- 将分析功能与 微软活动目录 集成

Citrix Analytics 还可以将风险情报信息发送到客户拥有的 Splunk 环境。此集成需要在 Splunk 环境中部署和配置 **Citrix Analytics Add-on for Spunk**。有关详细信息，请参阅 Splunk 集成。

未经客户同意，Citrix Analytics 不会处理从数据源收到的任何事件。要处理来自数据源的事件，Analytics 管理员必须启用数据处理。有关 Analytics 的数据收集、存储和保留的更多信息，请参阅数据治理。

网络要求

- **Citrix Cloud 服务要求**：要使用 Citrix Cloud 服务，您必须能够通过 HTTPS 端口 443 连接到所需的 Citrix 地址。有关详细信息，请参阅 Internet 连接要求。
- **Citrix Analytics 要求**：在使用 Citrix Analytics 之前，请查看 系统要求。除了 Citrix Cloud 要求之外，以下端点地址必须可通过 HTTPS 端口 443 访问才能使用 Citrix Analytics 服务。

端点	美国区域	欧盟区域	亚太南部地区
管理用户界面	`https://analytics.cloud.com/`	`https://analytics-eu.cloud.com/`	`https://analytics-aps.cloud.com/`
管理用户界面 (CDN)	`https://cas-api-cdn-ep-h9apa4bsccg0gfe7.a02.azurefd.net/`	`https://cas-api-cdn-ep-eu-g5d6bhadh5gvd0fh.a02.azurefd.net/`	`https://cas-api-cdn-ep-aps-a0fwd8c3d7bbfxdt.a02.azurefd.net/`
API 服务	`https://api.analytics.cloud.com/`	`https://api.analytics-eu.cloud.com/`	`https://api.analytics-aps.cloud.com/`
API 服务（性能分析）	`https://api-a.was.cloud.com/`	`https://api-eu-a.was.cloud.com/`	`https://api-ap-s-a.was.cloud.com/`
	`https://api-b.was.cloud.com/`	`https://api-eu-b.was.cloud.com/`	`https://api-ap-s-b.was.cloud.com/`
获取公共 IP	`https://locus.analytics.cloud.com/`	`https://locus.analytics.cloud.com/`	`https://locus.analytics.cloud.com/`
事件中心（不适用于 Citrix ADM 代理）	`https://citrixanalyticseh-alias.servicebus.windows.net/`	`https://citrixanalyticseheu-alias.servicebus.windows.net/`	`https://citrixanalyticsehaps-alias.servicebus.windows.net/`
	`https://citrixanalyticseh2-alias.servicebus.windows.net/`	`https://citrixanalyticseh2eu-alias.servicebus.windows.net/`	
	`https://citrixanalyticseh3-`		

CITRIX ANALYTICS

端点	美国区域	欧盟区域	亚太南部地区
	`alias.servicebus.windows.net/`		
Event Hub (适用于 Citrix ADM 代理)	`https://cas-eh-ns-alias.servicebus.windows.net/` 和 `https://cas-eh-ns2-alias.servicebus.windows.net/`	`https://cas-eh-ns-eu-alias.servicebus.windows.net/`	`https://cas-eh-ns-aps-alias.servicebus.windows.net/`
批量上传	`https://casstoragebulk.blob.core.windows.net/`	`https://casstorebulkeu.blob.core.windows.net/`	`https://casstorebulkaps.blob.core.windows.net/`

注意

Citrix Analytics 已停止支持大多数上述端点的 TLS 1.0 和 TLS 1.1。

- **Citrix Cloud Connector 安装**：某些数据源（例如 Citrix Endpoint Management、Citrix Virtual Apps and Desktops 和 Microsoft Active Directory）要求您在资源位置安装 Citrix Cloud Connector。Citrix Cloud Connector 是 Citrix Cloud 与您的资源位置之间的通信通道。安装 Citrix Cloud Connector 后，您必须配置 Web 代理设置。有关更多信息，请参阅Cloud Connector 代理和防火墙配置。
- **用于 SIEM 集成的 Citrix Analytics 端点**：要将 Citrix Analytics 与您的安全信息和事件管理 (SIEM) 集成，请确保以下端点在您的网络允许列表中：

端点	美国区域	欧盟地区	亚太南部地区
Kafka 代理	`casnb-0.citrix.com:9094`	`casnb-eu-0.citrix.com:9094`	`casnb-aps-0.citrix.com:9094`

端点	美国区域	欧盟地区	亚太南部地区
	`casnb-1.citrix.com:9094`	`casnb-eu-1.citrix.com:9094`	`casnb-aps-1.citrix.com:9094`
	`casnb-2.citrix.com:9094`	`casnb-eu-2.citrix.com:9094`	`casnb-aps-2.citrix.com:9094`
	`casnb-3.citrix.com:9094`		

身份和访问管理

- 要访问 Citrix Analytics，您必须使用您的 Citrix Cloud 帐户。默认情况下，Citrix Cloud 使用 Citrix 身份提供程序来管理 Citrix Cloud 帐户中所有用户的身份信息。您还可以使用 身份和访问管理 中提到的其他身份提供程序。
- Citrix Analytics 支持委派管理员权限。您可以为用户分配只读管理员权限，以在企业中管理 Analytics。有关详细信息，请参阅管理管理员角色。

数据驻留

Citrix Cloud 管理 Citrix Analytics 的控制平面。从数据源接收的数据存储在多个 Microsoft Azure 环境中。这些环境位于美国、欧盟和亚太南部地区。存储位置取决于 Citrix Cloud 管理员在将其组织加入 Citrix Cloud 时选择的“主区域”。有关详细信息，请参阅以下主题：

- 地理考量
- 数据治理

数据保护

Citrix Analytics 从订阅的 Citrix Cloud 数据源、本地数据源和第三方产品接收数据。仅当客户拥有 Citrix Cloud 授权且 Analytics 管理员已明确为每个订阅的数据源启用数据处理时，才会处理接收到的数据。

Citrix Analytics 使用以下安全措施保护客户数据：

- 适用于 Analytics 用户的 Citrix Cloud 身份验证。有关信息，请参阅身份和访问管理。
- 由数据服务和数据访问层强制执行的基于租户的数据访问控制。

- 数据湖和数据仓库中所有数据存储中每个客户或租户的强大数据隔离。
- 各种微服务和数据存储之间采用 TLS 加密的数据传输，适用于平台的公共端点（APT/输入/输出）以及平台内部。
- TLS 端点的高标准。TLS 1.0 和 TLS 1.1 已禁用。
- 使用存储在相应密钥保管库中的加密密钥和机密进行加密数据存储。
- 强大的用户管理访问控制，用于服务操作和支持，同时保护客户日志。
- 漏洞扫描、入侵检测、反恶意软件、Rootkit 扫描与 Azure 安全中心结合使用。

与所有 Citrix Cloud 服务一样，数据收集严格遵守最终用户服务协议 (EUSA)。有关更多信息，请参阅以下协议：

- 用户协议
- Citrix 隐私策略
- Citrix 数据处理协议
- Citrix 服务安全附录
- Citrix Cloud 服务：客户内容和日志处理
- Citrix 隐私和合规性信息

安全责任

Citrix 责任

Citrix 负责保护托管 Citrix Analytics 的 Citrix 管理云环境中的所有基础设施和数据。Citrix 负责在云环境中应用定期软件更新和补丁，以解决安全漏洞。

客户责任

Citrix 客户负责保护其数据源、策略实施点以及与 Citrix Analytics 集成的安全信息和事件管理 (SIEM) 系统，其中包括：

- 客户拥有和管理的本地数据源：
  - **本地数据源**：Citrix 网关、Citrix 虚拟应用和桌面、Microsoft 活动目录
  - **SIEM**：Splunk 以及任何其他使用 Kafka 代理从 Citrix Analytics 读取事件的第三方产品。
- 客户提供的用于管理 Citrix Cloud 服务（包括 Citrix Analytics）的管理员凭据。
- 接收来自 Citrix Cloud 服务的电子邮件或通知的客户拥有的管理员帐户。

- 客户提供的用于部署和集成代理（例如 Citrix ADM 代理）的管理员凭据。必须限制对这些代理的访问，因为它们在本地存储密钥以与 Citrix Analytics 通信。
- Citrix Analytics 生成的用于配置**适用于 Splunk 的 Citrix Analytics 附加组件**的凭据。
- 运行在 Windows、Mac、Android、iOS 上的最终用户设备，用于连接到 Citrix Cloud 或 Citrix Workspace™ 并与数据源集成。

有关安全条款的更多信息，请参阅以下文档：

- Citrix Cloud 平台安全部署指南
- 思杰工作区文档
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）技术安全概述
- Citrix Virtual Apps and Desktops 的安全注意事项
- 保护您的 StoreFront 部署文档
- Citrix Endpoint Management 技术安全概述
- 思杰安全私有访问服务文档
- Citrix ADC 安全部署指南
- Citrix ADM 系统要求

系统要求

在使用 Citrix Analytics 之前，您必须查看许可信息、软件要求和浏览器要求。

思杰分析订阅

您必须拥有有效的订阅才能使用以下 Analytics 产品：

- Citrix Analytics 安全版
- Citrix Analytics 性能版

有关更多信息，请参阅 Citrix Cloud services。

数据源要求

数据源是将事件发送到 Citrix Analytics 的产品。根据您使用的 Citrix Analytics 产品，数据源会有所不同。请参阅以下文章以查看每个产品支持的数据源：

- Citrix Analytics for Security 支持的数据源
- Citrix Analytics for Performance 支持的数据源

支持的浏览器

要访问 Citrix Analytics，您的工作站必须安装以下受支持的 Web 浏览器：

- 最新版 Google Chrome
- 最新版 Mozilla Firefox
- 最新版本的 Microsoft Edge
- 最新版本的 Apple Safari

管理 Citrix Analytics 的管理员角色

> **注意：**
>
> 自 2023 年 7 月起，Microsoft 已将 Azure Active Directory (Azure AD) 更名为 Microsoft Entra ID。在本文件中，任何提及 Azure Active Directory、Azure AD 或 AAD 的地方现在均指 Microsoft Entra ID。

> 默认情况下，Citrix Cloud™ 管理员对其 Citrix Cloud 帐户上的所有订阅服务拥有完全访问权限。通过完全访问权限，管理员可以使用订阅服务的所有特性和功能。

作为具有完全访问权限的 Citrix Cloud 管理员，您可以邀请其他管理员加入您的 Citrix Cloud 帐户，以管理您组织的订阅服务。然后，您可以定义他们的访问权限，并允许他们管理订阅服务中的特定功能。

可以通过两种方式添加新管理员：

1. 作为来自 Citrix Identity 和 Azure AD/Active Directory 的用户单独添加。有关更多信息，请参阅管理 Citrix Cloud 管理员。
2. 使用 Azure Active Directory 中的组。有关更多信息，请参阅 管理管理员组。

管理员可以使用其 Citrix Cloud、Active Directory 或 Azure Active Directory 帐户登录 Citrix Cloud，并根据其角色访问特定功能和执行任务。

对于 Citrix Analytics，您可以为管理员分配以下自定义角色：

角色	权限
性能分析 - 完全管理员	为性能分析的 Citrix Cloud 管理员分配完全访问权限。
性能分析 - 只读管理员	将只读访问权限分配给 Performance Analytics 的 Citrix Cloud 管理员。

角色	权限
安全与性能分析 - 只读管理员	将只读访问权限分配给安全分析和性能分析的 Citrix Cloud 管理员。
安全分析 - 完全管理员	将完全访问权限分配给安全分析的 Citrix Cloud 管理员。
安全分析 - 只读管理员	将只读访问权限分配给安全分析的 Citrix Cloud 管理员。

分析管理员角色(/en-us/citrix-analytics/media/analytics-rbac.png)

注意

- 如果您为管理员选择多个角色，则具有更高访问权限的角色将生效。
- 如果用户直接作为用户以及通过 Azure Active Directory 组获得访问权限，则单独授予用户的访问权限将生效。
- Azure Active Directory 组只能添加为自定义管理员。完全访问管理员角色不适用于组。
- 之前可用的具有 **只读管理员** 角色的管理员已重命名为 **安全与性能 - 只读管理员**。
- 具有 **安全与性能分析 - 只读管理员** 角色和 **性能分析 - 只读管理员** 角色的管理员不会收到来自 Citrix Analytics 的任何电子邮件通知。

有关产品特定角色的更多信息，请参阅以下文章：

- 管理性能分析的管理员角色
- 管理安全分析的管理员角色

入门

本文档介绍了如何首次开始使用 Citrix Analytics。

步骤 1：登录 Citrix Cloud™

要使用 Citrix Analytics，您必须拥有一个 Citrix Cloud 帐户。转到 https://citrix.cloud.com 并使用您现有的 Citrix Cloud 帐户登录。

如果您没有 Citrix Cloud 帐户，则必须首先创建一个 Citrix Cloud 帐户，或者加入组织中其他人创建的现有帐户。有关如何操作的详细流程和说明，请参阅 注册 Citrix Cloud。

步骤 2：获取 Analytics 访问权限

您可以通过以下方式之一访问 Analytics：

- **请求 Citrix Analytics 试用版**。登录 Citrix Cloud 后，在**可用服务**部分中，在**Analytics**磁贴上，单击**管理**以查看 Analytics 概述页面。

  概述页面显示 Analytics 产品 - **安全**和**性能**。

  - 对于安全分析和性能分析，单击**请求试用**以使用该产品的试用版。当您的请求获得批准且试用版可用时，您将收到一封电子邮件。您最多可以使用试用版 60 天。有关服务试用的更多信息，请参阅 Citrix Cloud 服务试用版。

  在 Citrix Cloud 页面上，**Analytics**磁贴将移至**我的服务**部分。

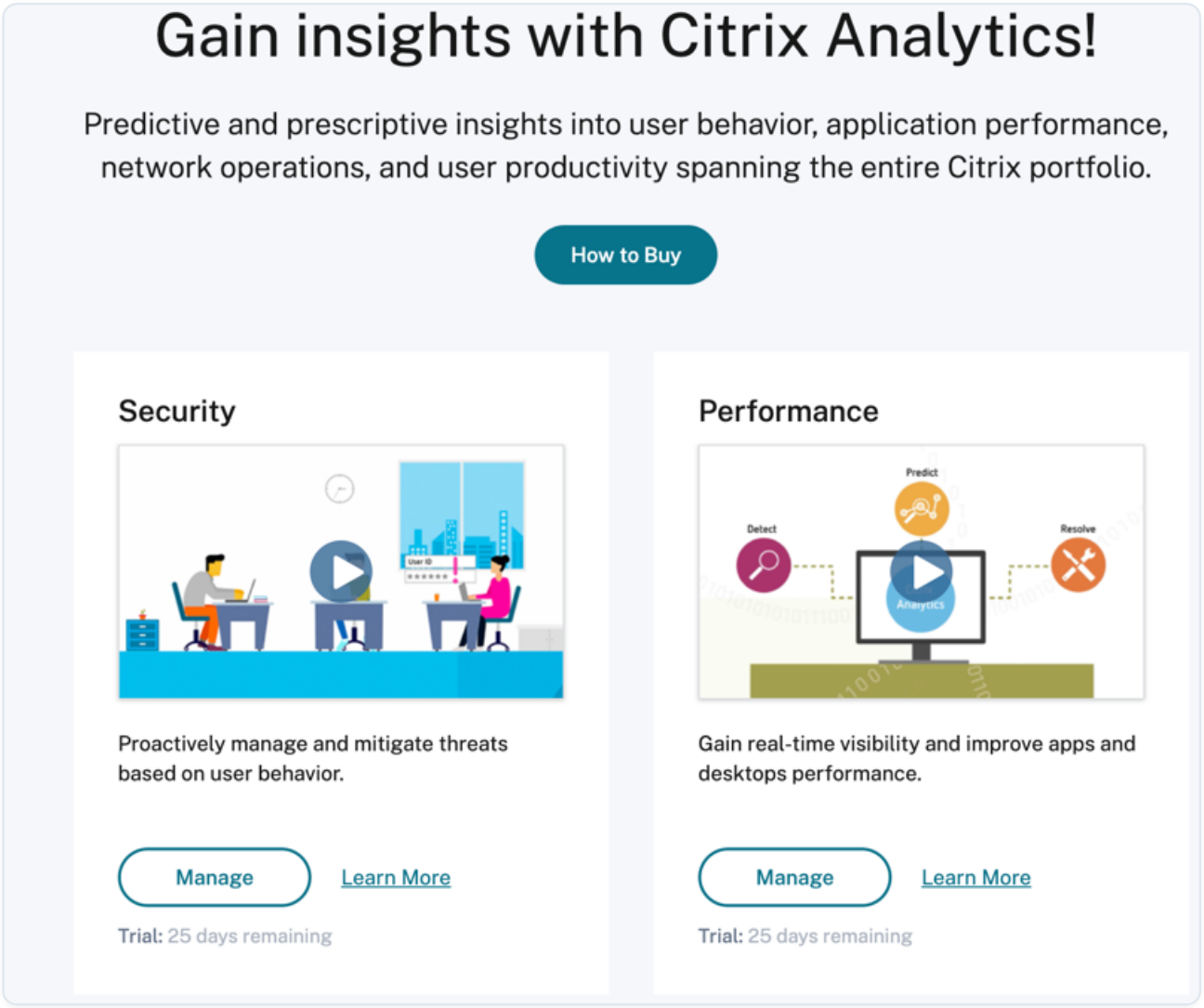
- **订阅 Citrix Analytics**。您可以购买以下 Citrix Analytics 订阅：

  - Citrix 安全分析™
  - Citrix 性能分析™
  - Citrix 安全和性能分析

  Citrix 安全分析和 Citrix 性能分析作为附加服务，随 Citrix Workspace 套件（包括 Workspace 标准版、Workspace 高级版和 Workspace 高级增强版）提供。有关更多信息，请参阅 Citrix Cloud 服务。

步骤 3：管理 Analytics

对于 Security Analytics 和 Performance Analytics，在您拥有必要的订阅或获得试用授权后，在 Analytics 概览页面上，该产品的“**请求试用**”按钮会变为“**管理**”。单击“**管理**”可查看与每个产品对应的用户仪表板。



Analytics 会自动发现与您的 Citrix Cloud 帐户关联的 Citrix Cloud 服务（数据源）。要查看您发现的数据源，请单击“**设置 > 数据源**”，然后单击所需的选项卡 - “**安全**”或“**性能**”。

有关每个 Analytics 产品的更多信息，请参阅

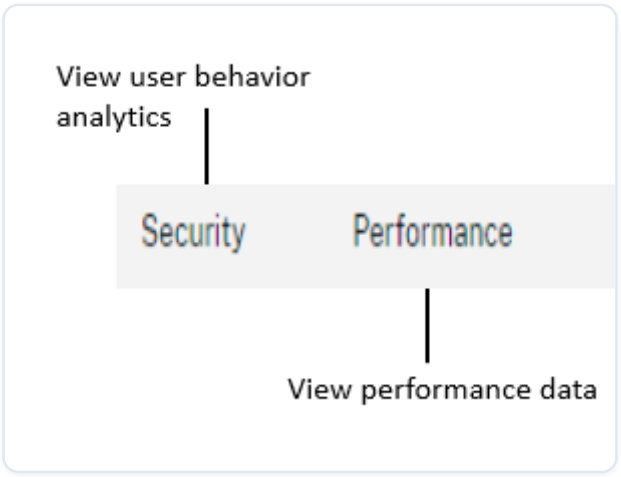
- Citrix 安全分析
- Citrix 性能分析

了解界面

熟悉 Analytics 用户界面上的主要控件。

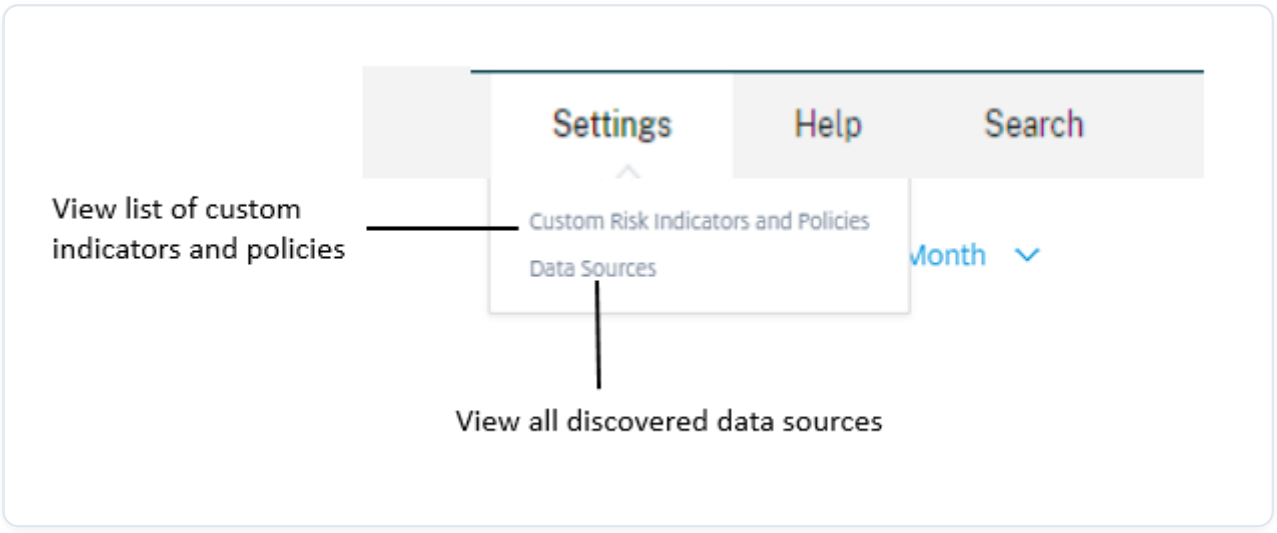
顶部栏

从顶部栏导航到各种 Analytics 产品。

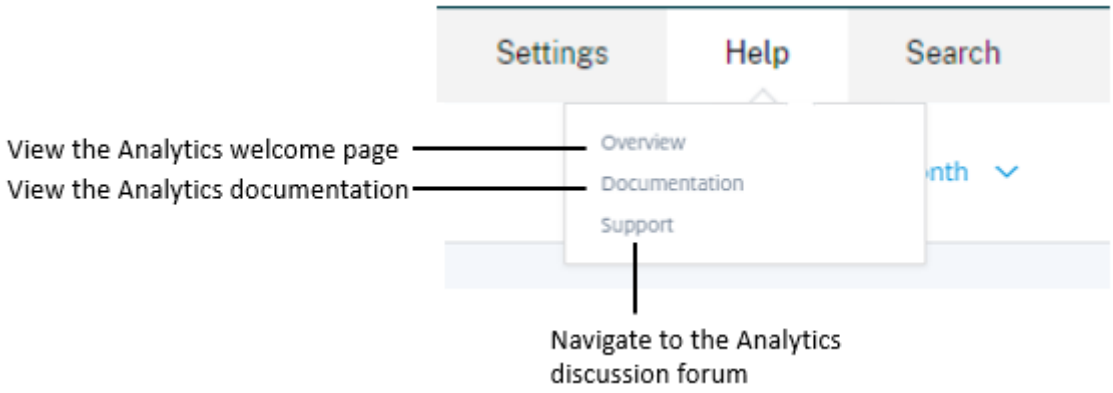


设置菜单

从**设置**菜单，导航到指标和策略页面或数据源页面。

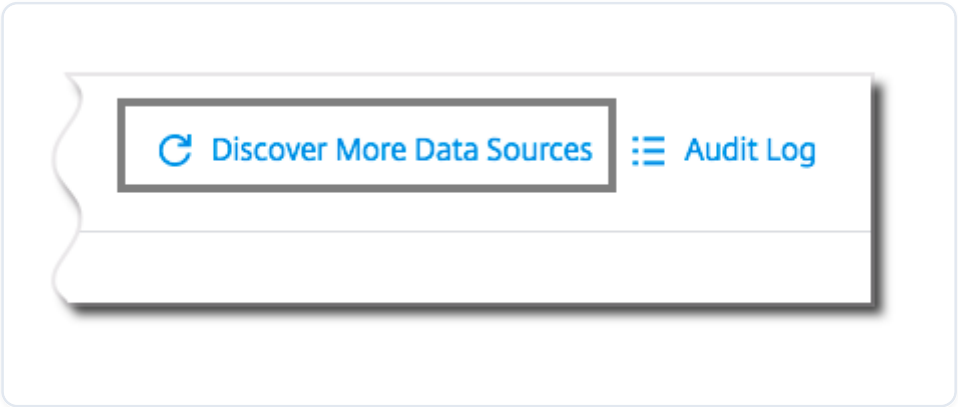


帮助菜单



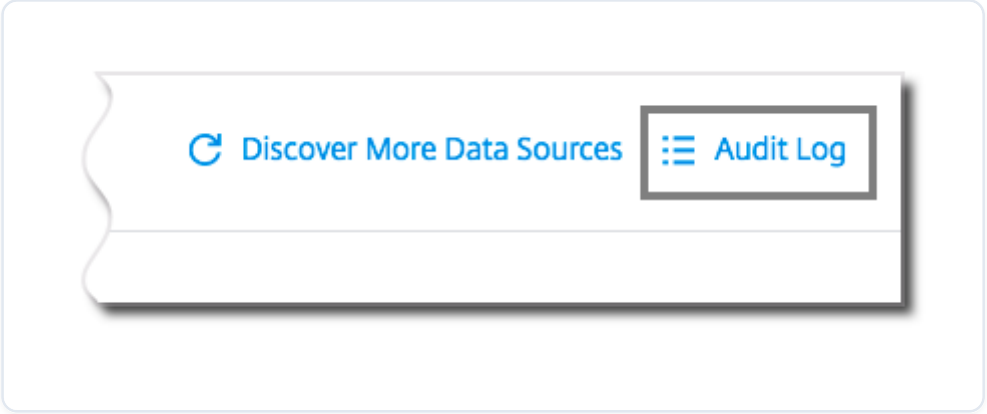
发现更多数据源

发现新添加的数据源或以前删除的数据源。



审计日志

导航到审计日志页面，该页面列出了 Analytics 上生成的所有事件。



自助搜索

警报设置

Citrix Analytics 根据警报策略条件生成警报。您可以配置通过电子邮件和 Webhook 接收来自 Citrix Analytics for Security™ 和 Performance 的警报通知。

- 电子邮件分发列表(/zh-cn/citrix-analytics/alert-settings/email-distribution-lists.html)
- 警报通知的 Webhook(/zh-cn/citrix-analytics/alert-settings/webhook-for-alerts.html)

您可以设置来自 Citrix Analytics for Security 的警报电子邮件通知的格式。

- 最终用户电子邮件设置(/zh-cn/security-analytics/email-settings.html)

电子邮件分发列表

当您手动或通过创建策略应用“**通知管理员**”操作时，系统会向选定的管理员发送有关风险指标的通知。

> **重要**
>
> 您可以从 Citrix Cloud™ 域和组织中的其他非 Citrix Cloud 域中选择管理员。
>
> 要将通知发送给适当的管理员组，请使用他们的电子邮件地址创建分发列表。

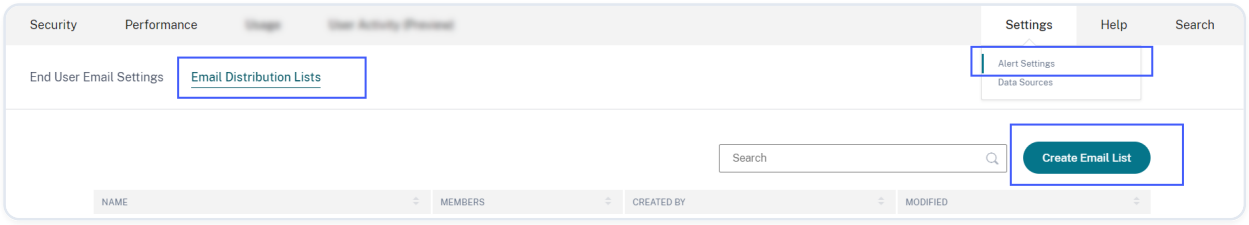
使用电子邮件分发列表，您可以执行以下操作：

- 创建一个通用电子邮件分发列表，其中包含来自组织中不同域的成员。
- 一次性通知所有成员。
- 节省您从不同域中选择管理员的时间和精力。
- 根据您的要求管理和维护电子邮件分发列表，例如添加新成员或删除现有成员。

创建电子邮件分发列表

要创建电子邮件分发列表：

1. 单击“**设置 > 警报设置 > 电子邮件分发列表 > 创建电子邮件列表**”。



或者，您也可以从策略创建电子邮件分发列表。修改现有策略或创建策略，然后选择“**通知管理员**”操作。单击“**创建电子邮件列表**”链接。

从策略创建电子邮件列表(/en-us/citrix-analytics/media/create-email-list-policy.png)

2. 输入电子邮件分发列表的名称和描述，以明确其用途。
3. 使用以下选项将成员添加到电子邮件分发列表：
   - **从域添加用户**。此选项要求您的域已连接到 Citrix Cloud。
   - **通过电子邮件地址添加用户**。如果要添加所选域之外的用户，请使用此选项。
4. 要从域添加用户，请选择一个域并搜索用户或用户组。

> **注意**
>
> 您还可以通过逐个选择域来添加来自多个域的用户和用户组。对于每个域，搜索并添加用户或用户组。

5. 单击用户或用户组旁边的“**添加**”图标。

从域添加成员(/en-us/citrix-analytics/media/add-domain-users.png)

6. 要添加所选域中不可用的用户，请输入用户的电子邮件地址或电子邮件分发列表。

> **注意**
>
> 在输入电子邮件分发列表之前，请确保您可以从组织网络外部访问该电子邮件分发列表。如果您添加了组织内部的电子邮件分发列表，则该列表的成员将无法收到来自 Citrix Analytics 的任何通知。

通过电子邮件添加成员(/en-us/citrix-analytics/media/add-members-emails.png)

7. 单击“**创建电子邮件列表**”。

查看电子邮件分发列表

要查看您的电子邮件分发列表，请单击“**设置 > 警报设置 > 电子邮件分发列表**”。

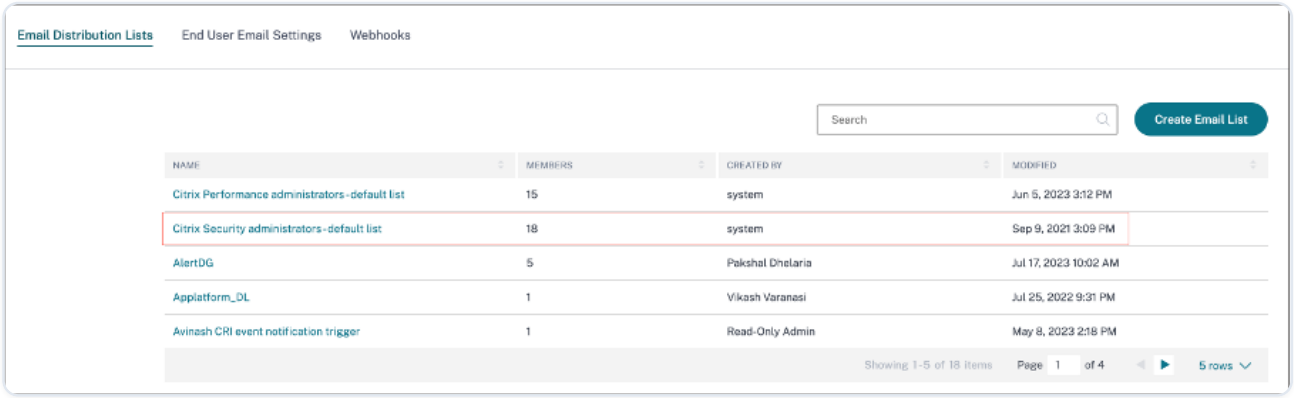
该页面显示您帐户中创建的所有电子邮件分发列表。选择一个电子邮件分发列表以查看成员或修改列表。

您会看到帐户中默认创建的电子邮件分发列表。它包含在其 Citrix Cloud 帐户中启用了“**电子邮件通知**”选项的 Citrix Cloud 管理员。您无法删除或修改默认列表。

> **注意**
>
> 对于默认电子邮件分发列表，Citrix Analytics 会缓存已启用电子邮件通知的管理员信息。缓存每 24 小时刷新一次。因此，如果任何管理员更改了电子邮件通知首选项，此更改将在 24 小时后在 Citrix Analytics 中更新。

> 例如，如果 Citrix Cloud 管理员启用其电子邮件通知，他们将在 24 小时后（而非立即）开始接收通知。同样，如果 Citrix Cloud 管理员禁用其电子邮件通知，他们将在 24 小时后停止接收通知。

> 安全管理员的默认分发列表现在包括在其 Citrix Cloud 帐户中启用了“**电子邮件通知**”选项的完全管理员和自定义管理员。



修改电子邮件分发列表

要修改电子邮件分发列表，请执行以下操作：

1. 单击“**设置 > 警报设置 > 电子邮件分发列表**”。
2. 单击要修改的电子邮件分发列表。
3. 在电子邮件分发列表中，更新所需详细信息，例如名称、描述，以及添加或删除成员。

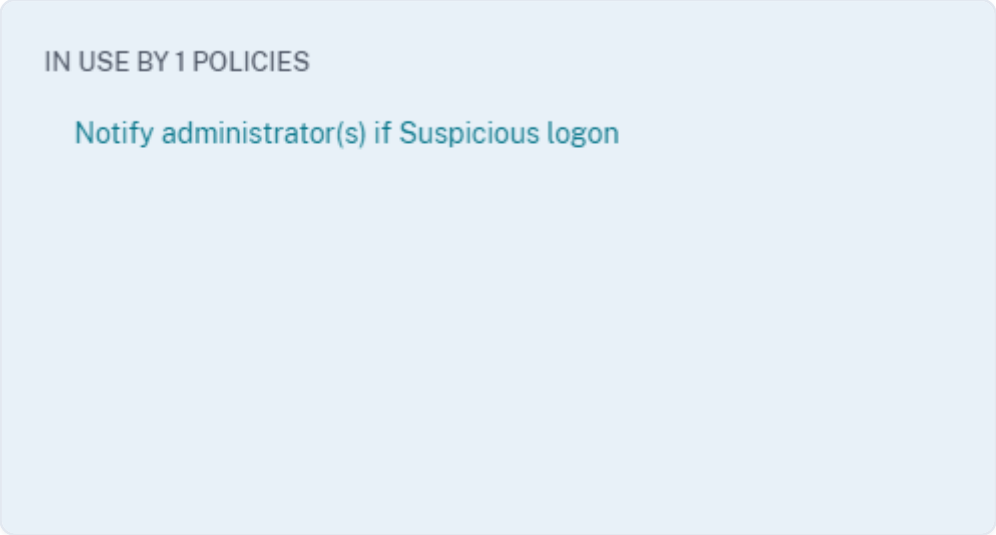
4. 单击“**保存更改**”。

删除电子邮件通讯组列表

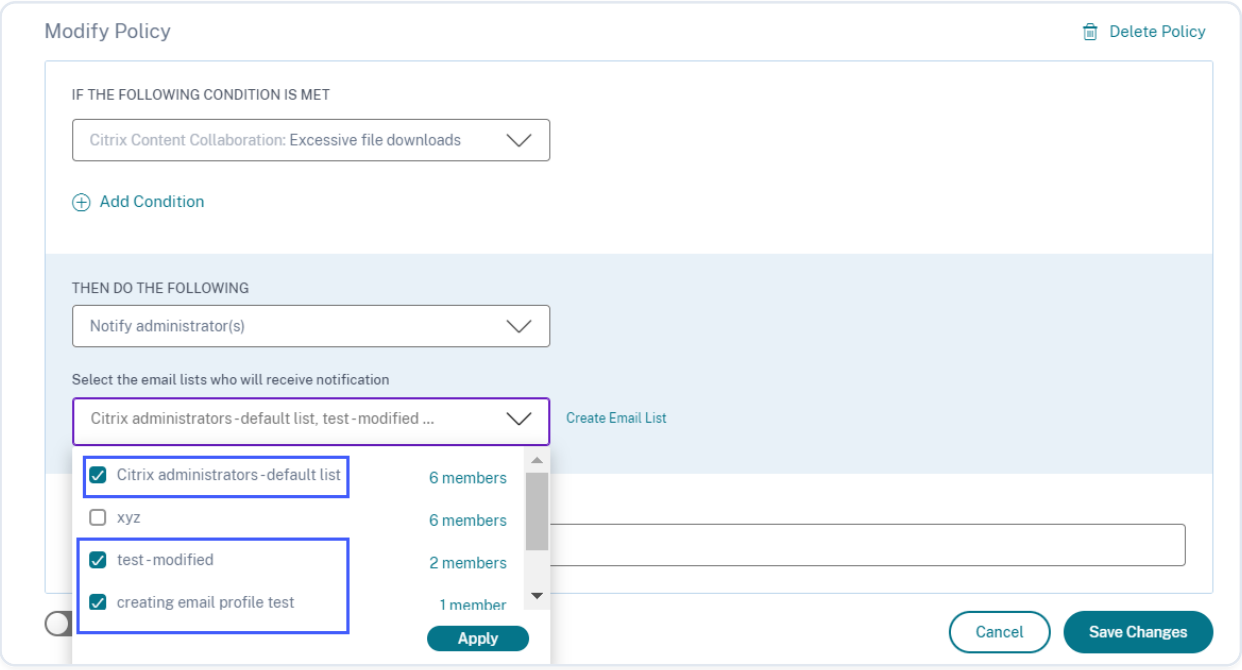
仅当电子邮件通讯组列表未与任何策略关联时，您才能将其删除。如果它与某些策略关联，则需要首先从关联的策略中删除该电子邮件通讯组列表。

要删除电子邮件通讯组列表：

1. 单击 **设置 > 警报设置 > 电子邮件通讯组列表**。
2. 单击要删除的电子邮件通讯组列表。
3. 在电子邮件通讯组列表上，查看关联的策略。



4. 单击策略以将其打开并删除电子邮件通讯组列表。如果需要，您也可以删除该策略。



5. 单击 **保存更改** 并返回电子邮件通讯组列表。
6. 打开电子邮件通讯组列表，然后单击 **删除** 图标。

警报通知的 Webhook

您可以使用 Webhook 将 Citrix Analytics 警报通知发送到任何配置了传入 Webhook URL 的第三方应用程序。Webhook 是 HTTP 回调，可在服务提供商应用程序和消费者应用程序之间实现实时消息传递。由于警报通知是实时发送的，因此您会在事件发生时收到通知。

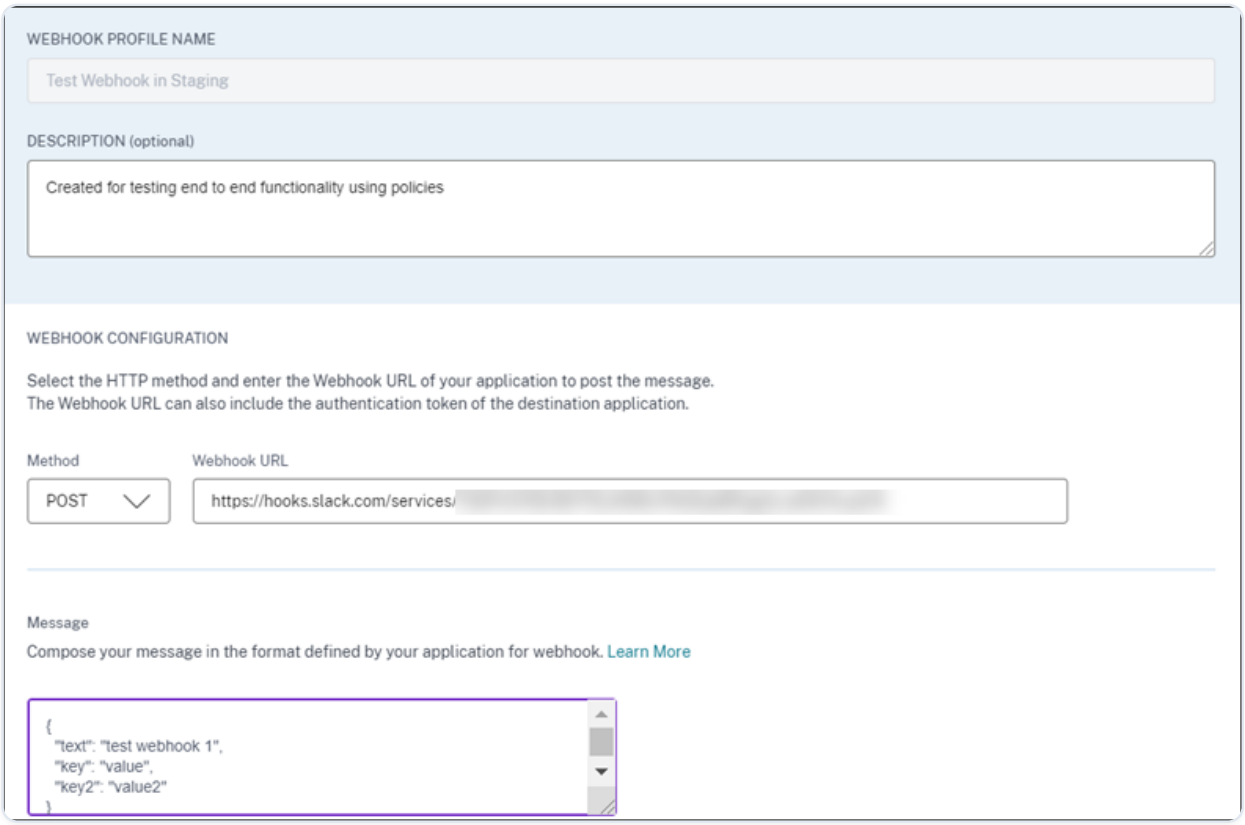
当 Citrix Analytics 触发警报时，关联的 Webhook 会将警报消息发送到目标应用程序的 URL。警报通过 HTTP POST 或 PUT 请求以 JSON 有效负载的形式发送。例如，当用户触发风险指示器或 VDI 计算机性能下降时，您可以设置 Webhook 将警报通知发送到您的 Slack 频道。 为警报管理设置 Webhook 有助于您在应用程序中获取实时通知。您可以及时采取措施来降低安全风险或提高 Citrix Virtual Apps and Desktops™ 部署的性能。

创建 Webhook 配置文件

要在 Citrix Analytics 上创建 Webhook 配置文件，请执行以下操作：

1. 登录到 Citrix Analytics。
2. 根据您订阅的产品，单击 **管理** 以访问安全分析或性能分析。
3. 从顶部栏中，单击 **设置 > 警报设置 > Webhook**。

4. 选择 **创建 Webhook**。



5. 输入配置文件名称和 Webhook 的描述，以识别其用途。
6. 选择 HTTP 方法和应用程序的 Webhook URL 以发送警报消息。
7. 输入您要发送到 Webhook URL 的警报消息。消息必须按照目标应用程序的定义，以 JSON 或 XML 等格式进行结构化。有关详细信息，请参阅 Webhook 示例。
8. (可选) 输入消息的标头键和值。标头可以包含身份验证令牌或其他自定义键值对，以安全地将有效负载发送到您的应用程序。
9. 要验证 Webhook 配置，请单击 **测试**。 该测试会验证出站 Webhook URL、有效负载结构和标头键。如果您的配置中未发现任何问题，您将收到“测试成功”消息。

Webhook 配置示例

本节提供了配置 Webhook 以将警报发送到第三方应用程序（例如 Slack 和 Microsoft Teams）的示例。

将警报消息发送到 Slack

在 Slack 上，发送警报之前请确保已完成以下任务：

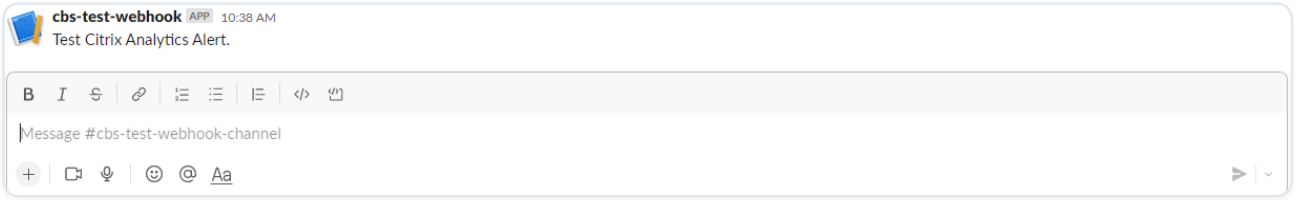
1. 如果您还没有，请为 Citrix Analytics 创建一个 Slack 应用程序。

2. 对于该应用程序，启用“传入 Webhook”功能并创建一个传入 Webhook。
3. 选择应用程序发布消息的频道。
4. 授权应用程序后，您将获得用于发送消息的 Webhook URL。 有关信息，请参阅传入 Webhook 入门。

消息格式示例

```
curl --location --request POST 'WEBHOOK URL' --header 'Content-Type:
application/json' --data-raw '{"text": "Test Citrix Analytics Alert."}
```

输出



将警报消息发送到 Microsoft Teams

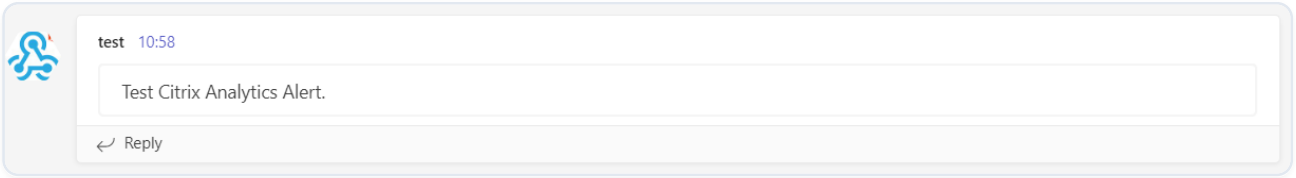
在 Microsoft Teams 上，发送警报之前请确保已完成以下任务：

1. 如果您还没有，请在 Teams 中创建一个 Teams 组。
2. 创建一个 Webhook 连接器。请参阅 创建和发送消息 文章中描述的步骤。
3. 获取 Webhook 的 URL。

消息格式示例

```
curl --location --request POST 'WEBHOOK URL' --header 'Content-Type:
application/json' --data-raw '{"text": "Test Citrix Analytics Alert."}
```

输出



思杰安全分析™ (安全分析)

借助随时随地、使用任何设备在任何网络上工作的优势，敏感的企业数据比用户仅在隔离的企业办公室工作时更容易暴露。恶意用户有很大的攻击面可供利用。IT 团队的任务是在不损害安全性的前提下提供出色的用户体验。Citrix Analytics for Security 专注于用户安全，可以帮助弥合这一差距。

什么是安全分析?

Citrix Analytics for Security 持续评估 Citrix Virtual Apps and Desktops™ 用户、Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops service）用户和 Citrix Workspace™ 用户的行为。它会采取措施来保护敏感的企业信息。跨网络、虚拟化应用程序和桌面工具的数据聚合和关联能够生成有价值的见解和更集中的操作，以应对用户安全威胁。此外，机器学习支持高度预测性的方法来识别恶意用户行为。

功能

- 来自 Citrix 产品和合作伙伴集成的简化见解。有关详细信息，请参阅自助搜索。
- 易于使用的控制板提供用户行为的完整视图。有关详细信息，请参阅用户控制板。
- 使用机器学习和自定义策略以及自动化操作来检测和缓解恶意用户行为。有关详细信息，请参阅策略和操作。
- 在首次对企业网络进行身份验证后，持续监控用户行为，以平衡全面的安全性和出色的用户体验。有关详细信息，请参阅持续风险评估。



控制板

您可以在以下安全控制板上查看有关用户或实体行为的详细信息：

- 用户：提供对整个组织用户行为模式的可见性。
- 访问保障位置：汇总 Citrix Virtual Apps and Desktops 用户和 Citrix DaaS 用户的访问详细信息和登录详细信息。
- 报告：根据已载入数据源中可用的维度和指标创建自定义报告。

下一步

- 系统要求：开始之前必须满足的最低要求。
- 数据源：了解 Analytics 支持的产品。
- 数据治理：了解 Analytics 如何收集、存储和保留日志。
- 开始使用：如何在您的组织中开始使用 Analytics。

Citrix Analytics for Performance™（思杰性能分析）

什么是性能分析

性能分析是 Citrix Analytics 提供的一项服务，可让您跟踪、聚合和可视化您的应用程序和桌面环境的关键性能指标。

- 性能分析将站点性能指标聚合到易于查看的用户体验和基础架构控制板中。这些控制板可帮助您分析用户体验并优化应用程序和桌面站点的使用。
- 性能分析支持多站点聚合和报告。它聚合了您的云和本地设置中的性能指标。因此，您可以在单个控制台上查看环境中所有站点的数据。
- 性能分析量化用户性能因素并根据这些因素对用户进行分类。它提供可操作的洞察，以排查故障、屏幕延迟、会话登录延迟和其他性能指标。
- 性能分析允许您查找和筛选指标，以缩小范围到面临性能问题的特定用户或会话。

如何使用性能分析

用户体验控制板

用户体验控制板显示了站点性能，涉及会话响应能力、会话登录持续时间、会话故障和会话重新连接等共同定义用户体验的因素。

如果您在组织中支持虚拟应用程序和桌面的多个用户，并且他们偶尔在启动应用程序或桌面时遇到延迟，则登录持续时间指标可以为您提供有关该问题的见解。深入分析可以帮助您识别导致这些问题的因素。

基础架构控制板

基础架构控制板显示您站点中计算机的状态和运行状况。当用户和基础架构控制板一起使用时，可以帮助您主动检查资源的可用性并识别站点上的性能瓶颈。

- 如果用户或会话趋势显示下降，表明登录到站点的用户或会话数量减少，请使用此指标检查管理程序是否已重新启动或计算机数量是否不足。

- 如果您看到多个会话启动失败的案例，请深入分析以确定失败的原因。这可能是许可证数量不足或计算机与交付控制器连接存在问题。

> **注意：**
>
> **基础架构分析仪表板**目前处于预览阶段。

> 使用 Performance Analytics，您可以快速分析问题、进行故障排除并解决问题，并保持应用程序和桌面的最佳服务水平。

入门

先决条件

1. 检查您的工作站是否具有 支持的浏览器 文章中列出的受支持的 Web 浏览器。有关系统要求的信息，请参阅 Citrix Analytics 系统要求 文章。
2. 您必须拥有 Citrix Cloud 帐户才能使用 Analytics 服务。有关如何创建 Citrix Cloud 帐户的详细说明，请参阅 注册 Citrix Cloud。转到 https://citrix.cloud.com 并使用您的 Citrix Cloud 帐户登录。
3. Citrix Analytics for Performance 可作为基于订阅的产品提供，既可作为独立产品，也可与 Citrix Analytics for Security 捆绑提供。要订阅 Citrix Analytics for Performance，请参阅 `https://www.citrix.com/products/citrix-analytics-performance.html)`。
4. 数据源的受支持版本可在 数据源 文章中找到。
5. Citrix Profile Management 必须安装在所有计算机上。
6. 最终用户体验监控 (EUEM) 服务必须正在运行，并且必须在所有计算机上配置相应的策略。有关更多详细信息，请参阅 最终用户监控策略设置。
7. 必须在计算机上将**用于 Performance Analytics 的 VDA 数据收集**策略设置为**允许**，以使监控服务能够收集与计算机相关的性能指标，例如带宽和延迟统计信息。有关更多信息，请参阅 用于收集 Performance Analytics 数据的策略。
8. 从 Citrix Studio 启用进程监控策略，以在**计算机统计信息 > 进程**选项卡中查看高资源消耗进程。有关更多信息，请参阅 启用进程监控。
9. 确保可以从所有端点（如果已配置代理）访问以下 URL：

端点	美国区域	欧盟区域	亚太南部区域
Citrix 密钥注册	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`	`https://trust.citrixnetworkapi.net`
思杰云	`https://trust.citrixworkspacesapi.net`	`https://trust-eu.citrixworkspacesapi.net`	`https://trust-aps.citrixworkspacesapi.net`
思杰分析	`https://api.was.cloud.com`	`https://api-eu.was.cloud.com`	`https://api-aps.was.cloud.com`
批量上传	`https://citrixanalyticseh-alias.servicebus.windows.net/`	`https://citrixanalyticseheu-alias.servicebus.windows.net/`	`https://citrixanalyticsehaps-alias.servicebus.windows.net/`
批量上传	`https://citrixanalyticseh2-alias.servicebus.windows.net/`	`https://citrixanalyticseh2eu-alias.servicebus.windows.net/`	
批量上传	`https://citrixanalyticseh3-alias.servicebus.windows.net/`		

访问

1. 登录到 Citrix Cloud。找到 Analytics 服务磁贴并单击**管理**。概述页面显示了 Analytics 产品组合中可用的产品。
2. 在**性能**产品中，要使用该产品的试用版，请单击**请求试用**。如果您已购买 Citrix Analytics for Performance 产品，请改为单击**管理**链接。

(/en-us/citrix-analytics/media/pa-ftu.png)。

1. Citrix Analytics for Performance 将打开，显示用户体验和基础架构性能分析仪表板。 (/en-us/citrix-analytics/media/pa-user-analytics-dashboard1.png)

从亚太南部区域访问

Citrix Analytics for Performance 现已为亚太南部 (APS) 区域的试用客户和订阅客户自动启用。有关 Citrix Cloud 支持的区域的更多信息，请参阅 地理注意事项。

要从 APS 区域访问 Performance Analytics，请在将租户载入 Citrix Cloud 时选择亚太南部区域。登录 Citrix Cloud，并在 Citrix Cloud 的 APS 区域中选择您的租户。使用 `https://analytics-aps.cloud.com` URL 访问您的 Citrix Analytics Cloud Service。

- 当您选择亚太南部区域作为您的主区域时，Citrix Analytics for Performance 现在会将您组织的用户事件和元数据存储在该区域。有关更多信息，请参阅 数据治理。
- 有关亚太南部区域的网络要求信息，请参阅 技术安全概述。

配置数据源

您可以使用 Performance Analytics 监控本地站点或云站点。无论您是纯本地客户、云客户，还是混合了本地和云站点的混合客户，都可以使用此产品。

Performance Analytics 会自动检测您的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops™ 服务）。 如果您是本地客户，

- 首先将您的 Citrix Virtual Apps and Desktops 站点载入 Performance Analytics。
- 要获取 Performance Analytics 上的网络相关信息，您还必须载入您的本地 Citrix Gateway。

按照 数据源 文章中的说明配置所需的数据源。

> **注意：**

> - Citrix Analytics for Performance 收集并存储 Citrix Analytics for Performance 收集的日志中列出的数据点的日志。
> - Citrix Analytics for Performance 服务的建议限制列在 限制 文章中。

服务连续性

如果服务中断，Citrix Analytics for Performance 将在有限容量下运行。

管理员可以选择**保持**并查看当前屏幕上的可用数据，或以降级模式**转到仪表板**。

读取弹性对话框(/en-us/citrix-analytics/media/pa-read-resiliency-dialog.png)

在降级模式下，用户将切换到包含过去一天所有站点数据的仪表板。 所有筛选器和下钻功能都将禁用，直到服务在任何一种情况下恢复正常运行。

读取弹性(/en-us/citrix-analytics/media/pa-read-resiliency.png)

此更新提高了产品弹性，并有助于符合服务级别协议。

Citrix Analytics for Security and Performance 故障排除

将匿名用户验证为合法用户

排除来自数据源的事件传输问题

触发 Virtual Apps and Desktops 事件、SaaS 事件并验证事件传输

配置的 Session Recording 服务器无法连接

适用于 Splunk 的 Citrix Analytics 附加组件的配置问题

无法将 StoreFront™ 服务器与 Citrix Analytics 连接

常见问题

术语表

Citrix Analytics 文档历史

下表介绍了 Citrix Analytics 平台文档的重要更改。要接收有关这些更新的通知，请订阅 RSS 源。

日期	更改	说明
07 Jun 2021	更新了“新增功能”	从 Analytics 概述页面删除了试用演示链接了解详情.
07 Jun 2021	已更新入门	从 Analytics 概述页面删除了试用演示链接了解详情.
18 May 2021	更新了“新增功能”	添加了增强功能和修复的问题-CAS-50224。了解详情.
18 May 2021	更新了自助搜索	添加了对 * 操作员的支持!= 运算符。更新了新的搜索栏。了解详情.
31 Mar 2021	更新了“新增功能”	添加了功能。了解详情.
31 Mar 2021	更新了自助搜索	添加了 **IN** 和 **NOT IN** 运算符。了解详情.
18 Mar 2021	更新了“新增功能”	添加了功能。了解详情.
18 Mar 2021	更新了自助搜索	添加了对 NOT LIKE (!~) 运算符的支持。了解详情.
23 Feb 2021	更新了“新增功能”	添加了功能。了解详情.
23 Feb 2021	更新了自助搜索	添加了电子邮件发送计划和导出视觉摘要了解详情.
03 Dec 2020	更新了主题 - 技术安全性概述	添加了获取公共 IP 终端节点和更新了 Kafka 经纪商终端节点。了解详情.
12 Nov 2020	更新了主题 - 新增功能	添加了功能。了解详情.

日期	更改	说明
20 Oct 2020	更新了主题 - 新增功能	添加了功能。了解详情.
09 Jul 2020	更新了主题 - 新增功能	添加了已弃用的支持。了解详情.
09 Jul 2020	更新了主题 - 系统要求	已从支持的浏览器列表中删除 Internet Explorer 11。了解详情.
09 Jul 2020	更新的主题 - 找到自己的方法	删除了警报功能。了解详情.
02 Jul 2020	更新了主题 - Citrix Analytics 概述页面	添加了有关如何购买 Citrix Analytics 的信息。了解详情.
02 Jun 2020	更新了主题 - 新增功能	重新设计了“分析”概述页面，并将顶栏上的“**操作**”选项卡重命名为“**使用情况**”。了解详情.
14 May 2020	更新了主题 - 系统要求	更新了系统要求。了解详情.
11 May 2020	更新了主题 - 技术安全性概述	更正了“**网络要求**”部分中的终端 URL。了解详情.
02 Apr 2020	更新主题 - Citrix Analytics 故障排除	已更新有关 StoreFront 载入的信息。了解详情.
23 Mar 2020	更新了主题-概述	在分析产品列表中添加了 Citrix Analytics - Fundamentals。了解详情.
20 Feb 2020	更新了主题 - 新增功能	更新了已修复的问题 CAS-18657。了解详情.
20 Feb 2020	更新主题 - 数据管理	更新了数据管理日志。了解详情.
09 Jan 2020	更新了主题 - 新增功能	添加了已修复的问题 CAS-26297。了解详情.
18 Dec 2019	更新了主题 - 新增功能	添加了已修复的问题 CAS-27922。了解详情.

日期	更改	说明
12 Dec 2019	更新主题 - 数据管理	分析支持来自亚太南部微应用服务的活动。了解详情.
12 Dec 2019	更新了主题 - 新增功能	添加了功能。了解详情.
04 Dec 2019	更新了主题 - 新增功能	添加了已修复的问题 CAS-27368。了解详情.
22 Nov 2019	更新主题 - 入门	重新设计的 Analytics 概述页面，方便访问每个产品。了解详情.
22 Nov 2019	更新了主题 - 新增功能	添加了功能。了解详情.
21 Oct 2019	新增主题 - 技术安全性概述	了解使用 Analytics 时的安全最佳实践、数据流、网络要求和安全责任。了解详情.
21 Oct 2019	更新了主题 - 新增功能	添加了功能。了解详情.
11 Sep 2019	更新了主题 - 新增功能	添加了已修复的问题 CAS-20559。了解详情.
20 Aug 2019	更新了主题 - 新增功能	添加了已修复的问题 CAS-20906。了解详情.
31 Jul 2019	更新了主题 - 新增功能	增加了对欧盟地区的支持。了解详情.
26 Jun 2019	更新了主题 - 新增功能	添加了已修复的问题 CAS-19867。了解详情.
19 Jun 2019	更新了主题 - 新增功能	增加了已修复的问题 CAS-19930.了解详情.