Citrix Analytics

Machine translated content

Disclaimer

Contents

新增功能

September 25, 2023

Citrix 的目标是在 Citrix Analytics 客户可用时向其提供新增功能和产品更新。新版本会带来更多的价值，应立即将更新告知客户。

对您（即客户）来说，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。以分阶段的递增方式提供更新有助于确保产品质量并最大程度地保证可用性。

Citrix Analytics 提供以下产品或产品。有关新功能和产品更新的信息，请参阅每个产品的特定新文章。

- Citrix Analytics for Security
- Citrix Analytics for Performance

本发行说明重点介绍了特定于 Citrix Analytics 平台的新功能和产品更新。

2023 年 **9** 月 **21** 日

使用 **PowerShell** 脚本简化 **StoreFront** 登录流程

引入了一个新的 **PowerShell** 脚本，该脚本可以自动执行检查必备条件、安装和配置 StoreFront 的过程。客户必须在 StoreFront 的管理员模式下运行此脚本，才能加载、登机、执行自检、故障排除以及验证是否成功登录 Citrix Analytics Service GUI。

有关更多信息，请参阅连接到 StoreFront 部署。

2023 年 **8** 月 **28** 日

微应用程序服务（生命周期终止）

Citrix 微应用服务已接近使用寿命，不再向用户提供。

2023 年 **8** 月 **1** 日

Citrix Analytics - 使用情况（生命周期已结束）

Citrix 使用情况分析已接近使用寿命，不再向用户提供。

2023 年 2 月 23 日

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** 监视站点卡上看不到这些已连接的站点。此问题现已修复。[CAS-63132]

2022 年 9 月 28 日

用于警报通知的 **Webhook**

您可以使用 Webhook 将 Citrix Analytics 警报通知发送给配置了传入 Webhook URL 的任何第三方应用程序。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。有关详细信息，请参阅警报通知的 Webhook。

2022 年 9 月 8 日

CSV 导出中的导出限制增加

现在，使用导出为 **CSV** 格式功能可以导出的行数限制已从 1 万行增加到 100K 行。有关更多信息，请参阅将事件导出到 CSV 文件。

2022 年 8 月 18 日

已修复的问题

- 在应用程序和桌面的自助搜索中，Workspace 应用程序版本值在下载的 CSV 文件中填充为 **NA**（不可用），而该值在页面视图中可用。此问题现已修复。[CAS-70361]

2022 年 8 月 10 日

无需网站聚合即可上线 **StoreFront**

StoreFront 的网站聚合依赖项已从应用程序和桌面**-Workspace** 应用程序站点卡片中删除。即使您没有将任何站点添加到站点集合中，您也可以在工作区应用程序上查看连接 **Storefront** 部署选项。有关更多详细信息，请参阅 Citrix Virtual Apps and Desktops 数据源。

2022 年 4 月 5 日

Secure Workspace Access 已重命名为 Secure Private Access

在 Analytics 控制板和报告中，所有 **Secure Workspace Access** 标签现在都更新为 **Secure Private Access**，以便与重新命名的产品名称保持一致。

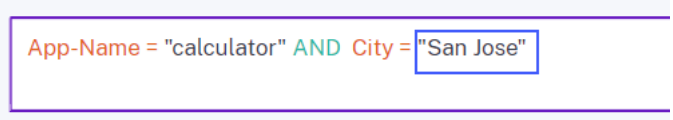
例如，在数据源页面和自助搜索页面上，**Secure Workspace Access** 标签被重命名为 **Secure Private Access**。

2022 年 3 月 21 日

已修复的问题

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

  例如，在以下查询中，将城市选择为 `San Jose` 后，自动建议将停止运行。此问题现已修复。[CAS-64126]



2022 年 2 月 10 日

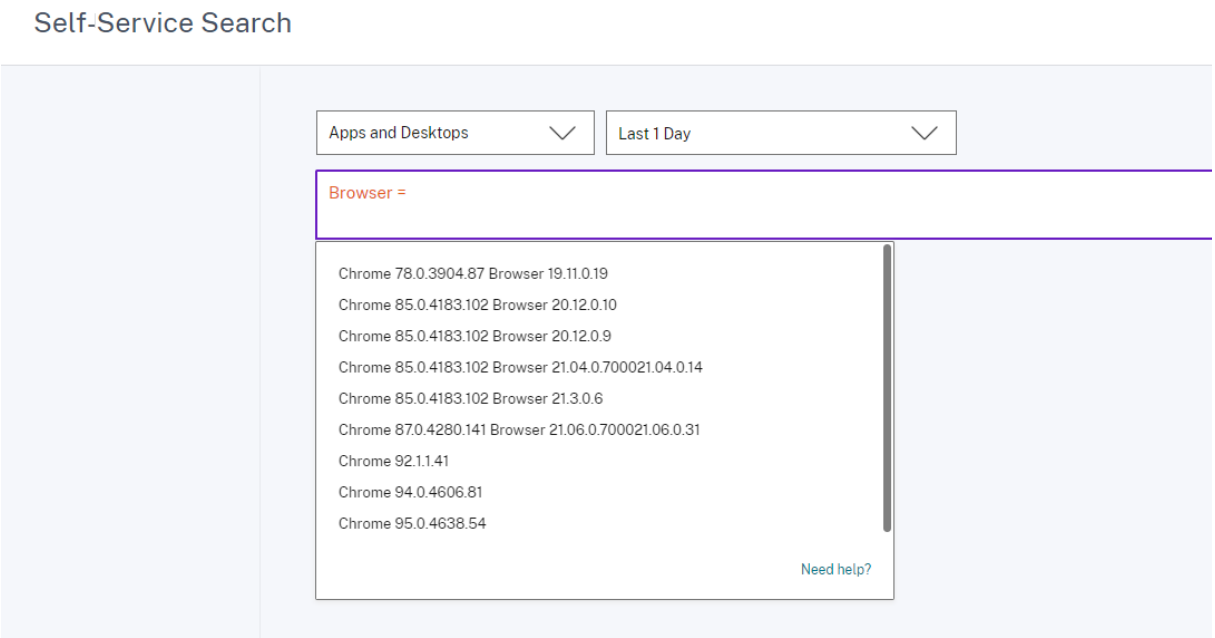
新增功能

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，将自动显示该维度的值。从自动建议列表中选择一个值，或者根据您的用例手动输入值。键入值时，系统会自动建议记录中可用的匹配值。

为维度建议的值列表要么是数据库中预定义的（已知值），要么基于历史事件。

例如，当您选择维度 `Browser` 和赋值运算符时，系统会自动建议已知值。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。



2021 年 12 月 20 日

新增功能

访问控制已重命名为 **Secure Workspace Access**　在 Analytics 控制板和报表中，所有访问控制标签现在都更新为 **Secure Workspace Access**，以便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，“访问控制”标签被重命名为“**Secure Workspace Access**”。

2021 年 12 月 6 日

新增功能

亚太南部区域现已支持 **Citrix Analytics**

- 现在，您可以在组织加入 Citrix Cloud 并使用 Citrix Analytics 服务时，选择亚太地区南部作为主区域。有关详细信息，请参阅地理方面的注意事项。
- 现在，当您选择亚太南部区域作为主区域时，Citrix Analytics 会将组织的用户事件和元数据存储在亚太南部区域。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的信息，请参阅技术安全概述。
- 有关亚太南部区域支持的数据源的信息，请参阅 数据源。

2021 年 8 月 19 日

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** 运算符来检查空维或空维。

> 注意
>
> 该运算符仅适用于字符串类型的维度，例如应用程序名称、浏览器和国家/地区。

有关详细信息，请参阅 自助搜索。

2021 年 7 月 14 日

新增功能

支持 **IS NOT EMPTY** 运算符　在自助服务搜索中，您现在可以在查询中使用 **IS NOT EMPTY** 运算符来检查维度是否为空（不是空白）。

> 注意
>
> 该运算符仅适用于字符串类型的维度，例如应用程序名称、浏览器和国家/地区。

有关详细信息，请参阅 自助搜索。

2021 年 6 月 7 日

已弃用的功能

删除 **Citrix Analytics** 演示环境　Security Analytics 和 Performance Analytics 的试用演示版链接现已从 Analytics 概述页面中删除。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。

2021 年 5 月 18 日

新增功能

支持 ***** 操作员使用**!=** 操作员　在搜索查询中，您现在可以将 * 运算符与 ！= 运算符一起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。

有关详细信息，请参阅 自助搜索。

增强自助搜索页面中的搜索栏体验

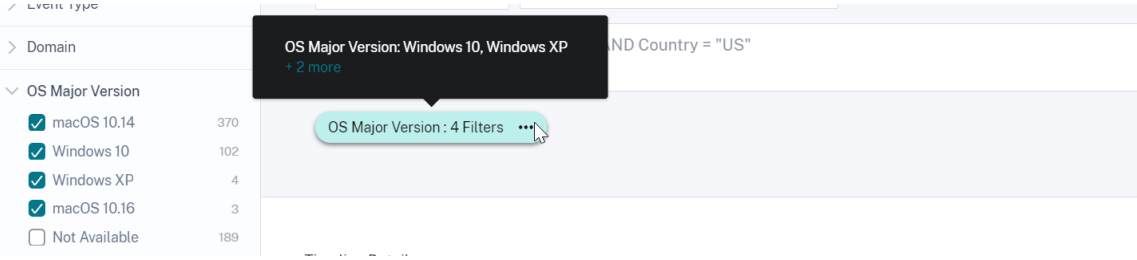
- 现在，当搜索栏扩展到多行时，可以更好地查询。使用滚动条滚动多行查询。以前，很难查看多行查询。

- 在 Safari 浏览器中观察到的光标跳跃问题现已修复。

有关详细信息，请参阅 自助搜索。

自助搜索中重新设计的筹码视图

- 重新设计的芯片现在可以让你更好地了解你选择的多个方面。



- 单击芯片可根据您的要求选择或取消选择小平面。

已修复的问题

- 在 Citrix Director 上，转到 **Analytics** 链接不起作用。对于已在 Citrix Cloud 的欧盟区域加入其组织的用户，可以观察到此问题。[CAS-50224]

2021 年 **3** 月 **31** 日

支持应用和桌面的 **IN** 和 **NOT IN** 运算符搜索查询

使用应用程序和桌面维度 - `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。

有关运算符的详细信息，请参阅 自助搜索。

2021 年 3 月 18 日

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。运算符会检查用户事件是否符合您指定的匹配模式。它返回事件字符串中任意位置不包含指定模式的事件。

例如，查询 `User-Name !~ “John”` 显示除了 John、John Smith 或包含匹配名称“约翰”的任何此类用户以外的用户的事件。

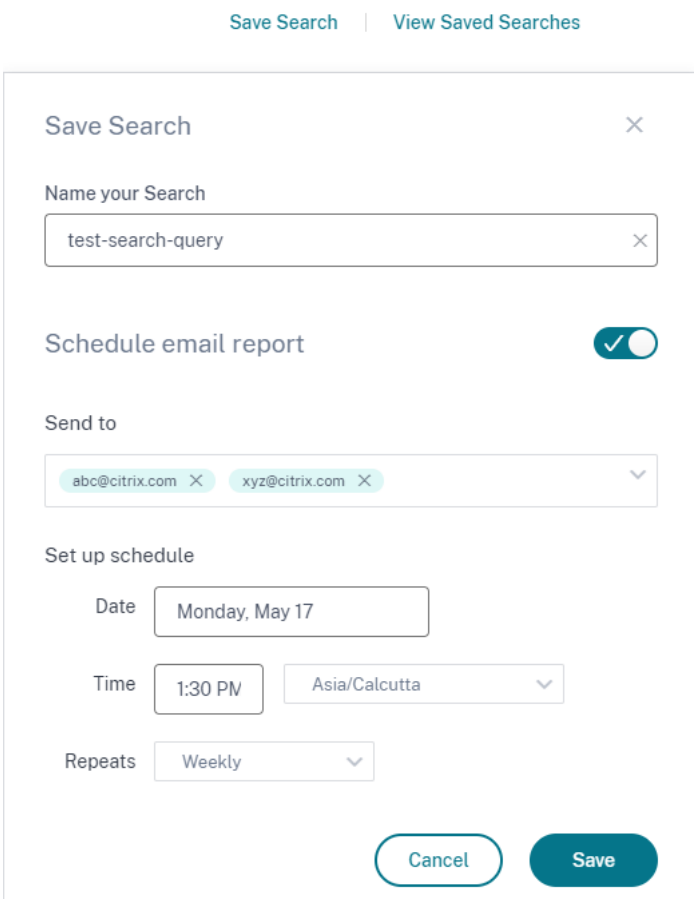
有关详细信息，请参阅 自助搜索。

2021 年 2 月 23 日

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，在保存搜索查询的同时，您还可以安排电子邮件传递，以便将保存的搜索查询和相应的可视化摘要报告的副本发送给您自己和其他用户。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。您还可以安排先前保存的搜索查询的电子邮件发送。

有关详细信息，请参阅 自助搜索。

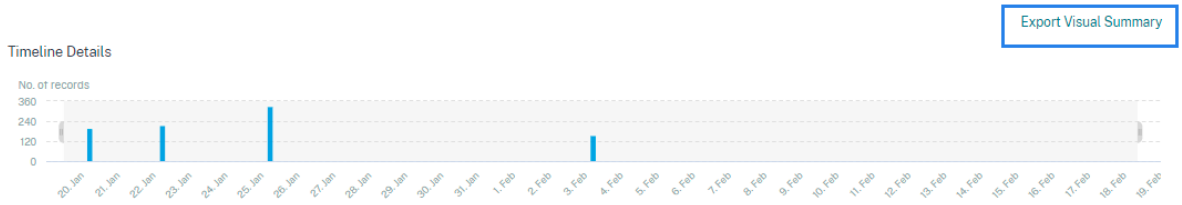


下载搜索查询的可视摘要　在自助服务页面上，您现在可以下载所选时间段内搜索查询的可视摘要报告，并与其他用户共享副本。单击 导出可视摘要 以 PDF 格式下载视觉摘要报告。

该报告包含以下信息：

- 您为事件指定的搜索查询。
- 您在事件上应用的方面（过滤器）。
- 视觉摘要，例如时间线图、条形图或搜索事件的图表。

有关详细信息，请参阅 自助搜索。

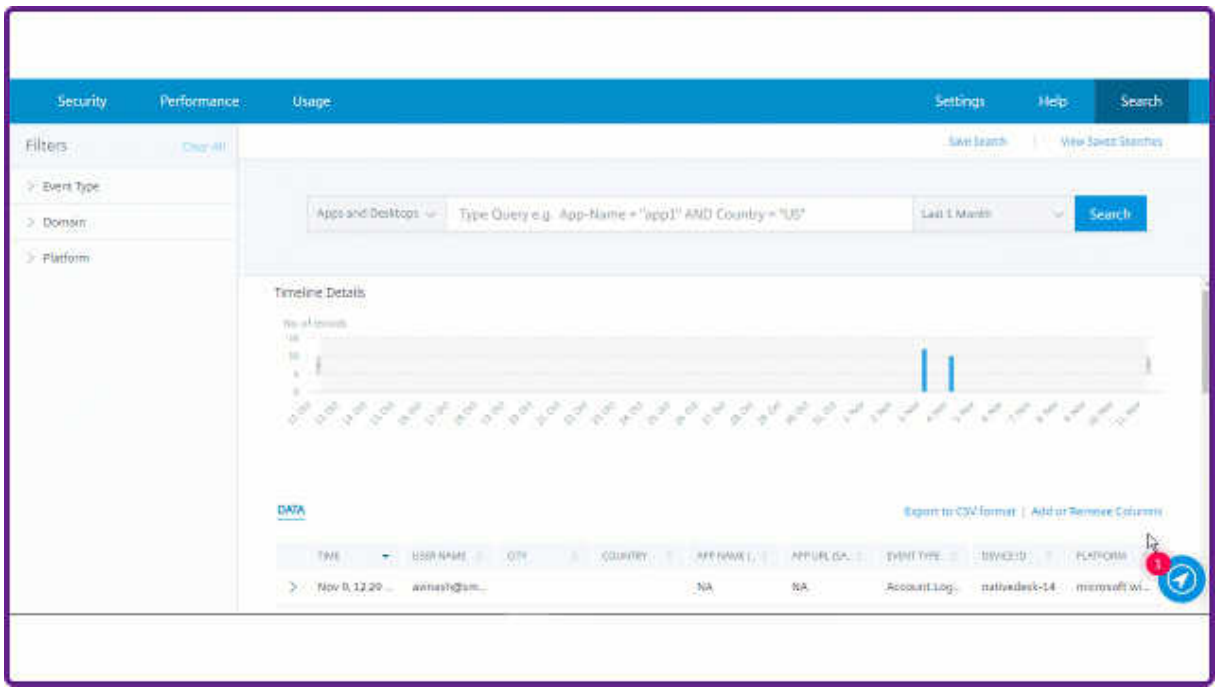


2020 年 11 月 12 日

新功能

保存自助服务查询　创建自助查询后，可以将其保存以备以后使用。以下选项随查询一起保存：

- 应用的搜索筛选
- 选定的数据源和持续时间



有关详细信息，请参阅 如何保存自助搜索。

2020 年 10 月 20 日

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。

2020 年 7 月 9 日

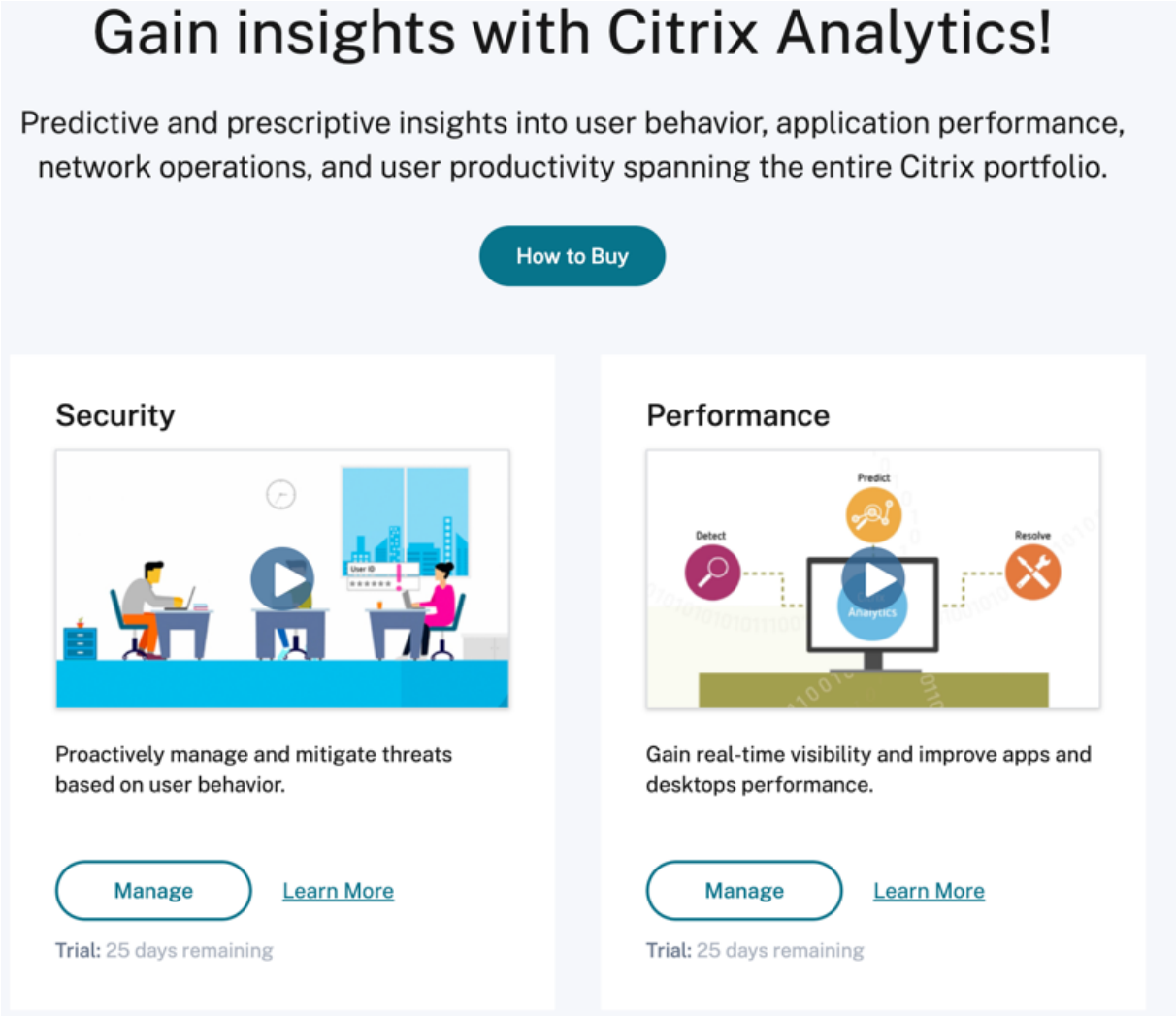
已弃用的支持

Microsoft Internet Explorer 11 现已从支持的浏览器列表中删除。这种弃用是因为在浏览器中观察到安全漏洞。有关支持的浏览器的列表，请参阅 系统要求。

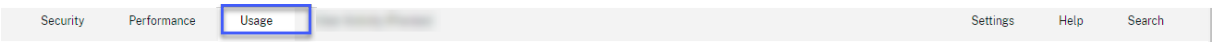
2020 年 **6** 月 **2** 日

新增功能

重新设计了 **Analytics** 中的概述页面和顶栏　Analytics 概述页面显示 用量 磁贴，该磁贴替换了之前存在的 操作 磁贴。此外，生产力 磁贴也会从此页面中移除。要查看概述页面，请选择“帮助”>“概述”。



同样，在顶部栏中，“使用情况”选项卡取代了“操 作”选项卡。



2020 年 **2** 月 **20** 日

新增功能

Citrix Analytics 订阅产品　Citrix 现在提供三种基于单独订阅的 Citrix Analytics 产品，为用户提供灵活的购买选项。Citrix Analytics 根据您订阅的产品提供独特的安全性或性能（或两者兼而有之）见解。

您可以购买以下 Citrix Analytics 订阅产品：

- Citrix Analytics for Security
- Citrix Analytics for Performance
- Citrix Analytics for Security and Performance（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 Gateway
- Secure Browser
- Microsoft Graph 安全性
- Microsoft Active Directory

有关详细信息，请参阅数据治理。

已修复的问题

- 自助搜索在 Internet Explorer 11 上无法正常工作。因此，您无法键入搜索查询并执行搜索操作。[CAS-18657]

2020 年 **1** 月 **9** 日

已修复的问题

- Citrix Analytics 演练功能不适用于欧盟主区域的用户。[CAS-26297]

2019 年 **12** 月 **18** 日

已修复的问题

Citrix Cloud 页面上的 分析 磁贴显示了“查 看服务”按钮。此按钮现已更改为 **Manage** ，以获得更好的用户体验。[CAS-27922]

2019 年 **12** 月 **12** 日

新增功能

支持亚太南部地区的微应用服务活动　Citrix Analytics 平台现在处理来自亚太南部地区微应用服务的通知。但是，衡量性能、
稳定性、使用情况、安全性和支持的记录会汇总并存储在美国。有关详细信息，请参阅数据治理。

> 注意
>
> 微应用服务作为 Citrix Workspace 的一部分提供。有关更多信息，请参阅 微应用 文档。

2019 年 12 月 4 日

已修复的问题

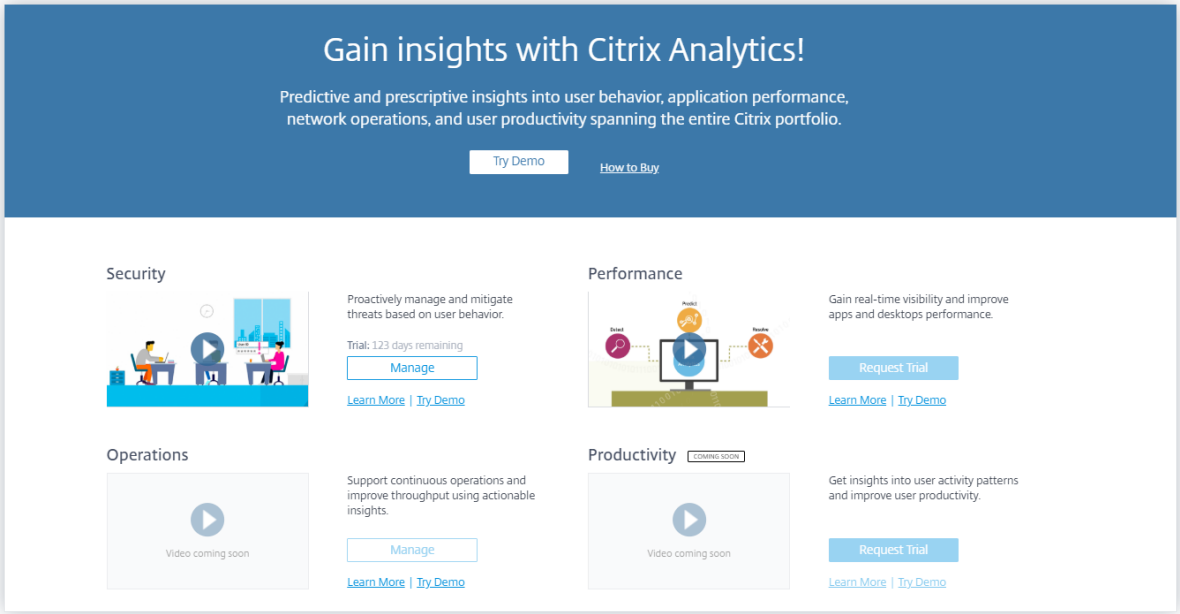
亚太地区南部地区的某些用户无法登录 Citrix Analytics，尽管他们已通过选择 美国 作为本地区域加入 Citrix Cloud。[CAS-27368]

2019 年 11 月 22 日

新增功能

重新设计了 **Analytics** 的概述页面　Analytics 概述页面经过重新设计，允许访问此页面上的所有 Analytics 产品。您可以申请试用、试用演示或管理您的 Analytics 产品。目前，只有 Security Analytics 和 Operations Analytics 提供一般可用版本，因此在此页面上处于活动状态。

要查看概述页面，请选择“帮助”>“概述”。



2019 年 10 月 21 日

新增功能

技术安全性概述　通过 技术安全概述，您可以了解与 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、网络要求以及安全责任。

2019 年 9 月 11 日

已修复的问题

- Citrix Cloud 无法将用户重定向到特定于区域的 Citrix Analytics 页面。[CAS-20559]

2019 年 8 月 20 日

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。[CAS-20906]

2019 年 7 月 31 日

新增功能

对欧盟地区的支持　Citrix Analytics 现在支持欧盟地区。在将组织加入 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。

2019 年 6 月 26 日

已修复的问题

- Citrix Analytics 无法在 Internet Explorer 11 上准确加载。[CAS-19867]

2019 年 6 月 19 日

已修复的问题

- Citrix Analytics 无法在 Microsoft Edge 上准确加载。[CAS-19930]

2018 年 11 月 16 日

已修复的问题

- 如果使用版本 11.0 的 Internet Explorer 访问 Citrix Analytics，**Citrix Cloud** 导航栏将无法加载并限制您访问汉堡包菜单。

2018 年 10 月 10 日

架构和平台增强功能

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

2018 年 8 月 23 日

Citrix Analytics 是一项通过 Citrix Cloud 提供的云服务。它收集 Citrix 产品组合中的数据并提供切实可行的见解，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：

- **Security Analytics**：整理并提供对用户和实体行为的可见性。有关更多信息，请参阅 Security Analytics。
- **Operations Analytics**：整理并显示有关用户活动的信息，例如访问的网站和花费的带宽。有关更多信息，请参阅 Operations Analytics。

新产品名

Citrix Analytics 支持的 Citrix 产品现已重命名为 Citrix 统一产品组合的一部分。

您可能会注意到我们的产品和产品文档中的新名称。这次品牌重塑是 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现此转换是一个正在进行的过程。

- 产品内容和文档可能仍包含以前的名称。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早期名称的实例。
- 有些项目（如命令）可能会继续保留其以前的名称，以防止破坏现有的客户脚本。
- 相关产品文档以及从此产品的文档链接的其他资源（例如视频和博客文章）可能仍包含以前的名称。

已知问题

September 25, 2023

本文重点介绍了适用于 Citrix Analytics 产品的已知问题（Performance 和 Security）。

有关每种产品的特定问题，请参阅相应的“已知问题”文章：Security 和 Performance。

- 首次登录时通过网关访问服务或应用程序的用户将触发“网关首次从新 **IP** 访问”指示器。[CAS-57963]

数据源

September 25, 2023

数据源是将数据发送到 Citrix Analytics 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。

  对于本地产品，例如 Citrix Gateway 和 Citrix Virtual Apps and Desktops Virtual Apps and Desktops，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 实例添加到应用程序交付管理中。并且必须将本地 Virtual Apps and Desktops 站点添加到 Workspace 中，否则必须配置 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，查看每种产品支持的数据源：

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

两种产品都支持 Citrix Gateway、Citrix DaaS（前身为 Citrix Virtual Apps and Desktops 服务）和 Citrix Virtual Apps and Desktops 数据源：Citrix Analytics for Security 和 Citrix Analytics for Performancee。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
- Citrix Virtual Apps and Desktops 数据源

Citrix Gateway 数据源

April 12, 2024

网关数据源表示环境中的本地 Citrix Gateway 实例。Citrix Analytics 会自动发现 Citrix Application Delivery Management (ADM) 代理和添加到 Citrix ADM 服务的网关实例。

当用户通过网关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 。处理用户事件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。这些步骤适用于以下两种产品：Citrix Analytics for Performance 和 Citrix Analytics for Security。

必备条件

- 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 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 并确保满足要求。

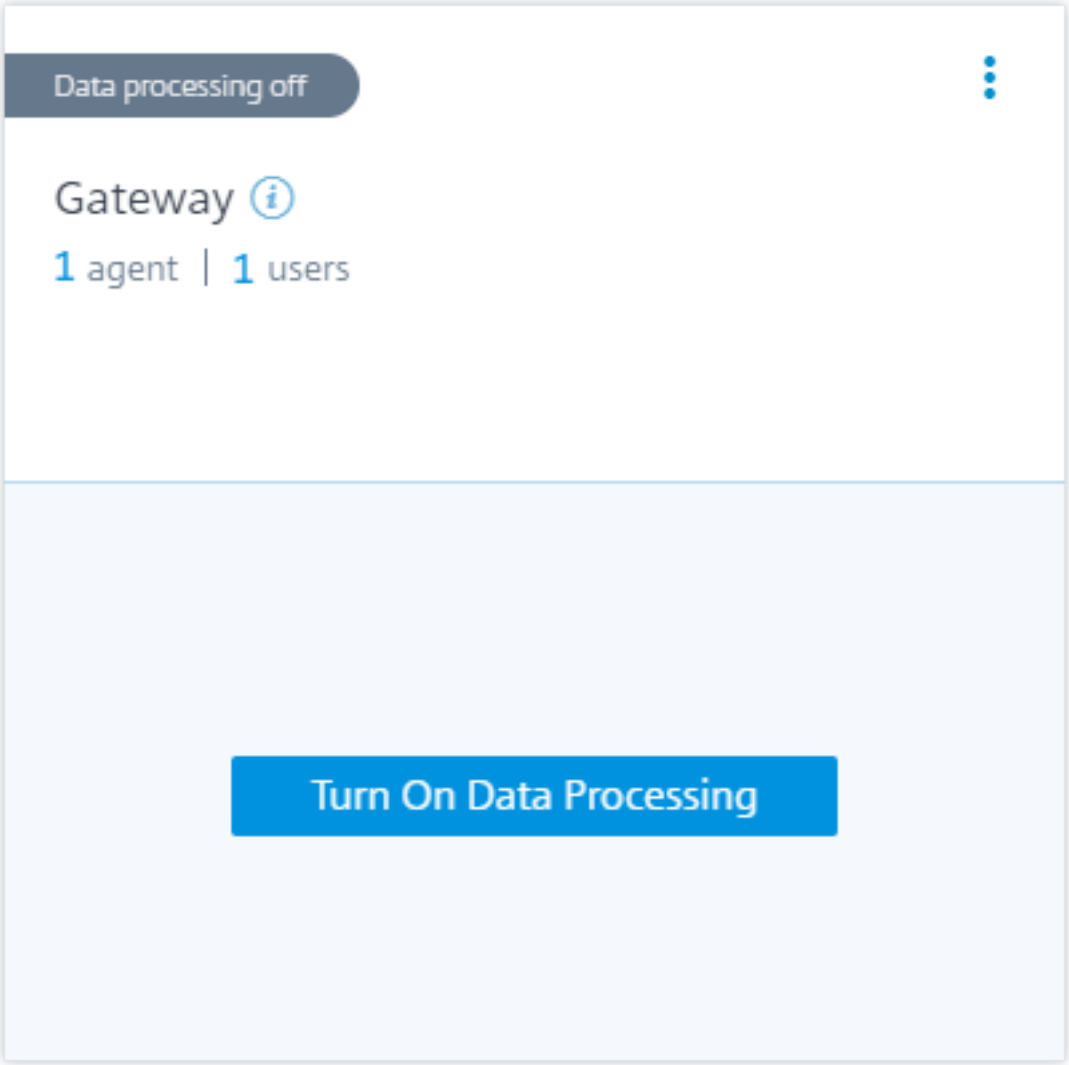
已添加到 **Citrix ADM** 的网关数据源

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，请执行以下操作：

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

发现的代理和用户将显示在网关站点卡上。单 击打开数据处理 以允许 Citrix Analytics 开始处理此数据源的数据。

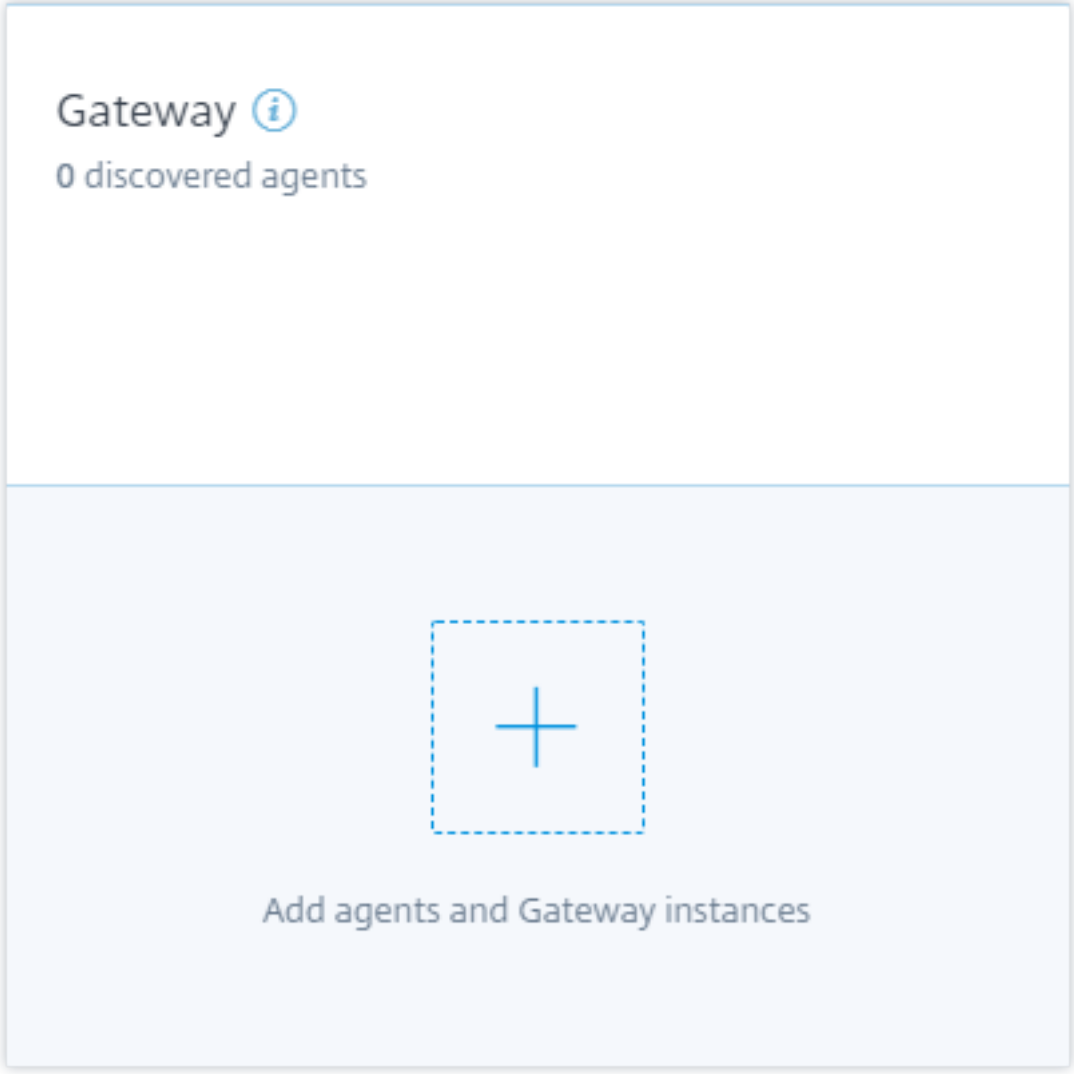


您可以查看 收到的事件。

如果尚未在 Citrix ADM 服务上启用 Citrix Analytics，请参阅在虚拟服务器上启用分析的统一流程，以启用 Citrix Analytics。

网关数据源未添加到 **Citrix ADM**

如果 Citrix ADM 代理和 Citrix Gateway 实例未添加到 Citrix ADM 服务中，网关站点卡会显示 **0** 个已发现的代理。



要发现代理和网关实例，请执行以下操作：

1. 如果您已经有 Citrix ADM 服务订阅，请单击站点卡上的 **+** 以添加代理和网关实例。
2. 如果您没有 Citrix ADM 服务订阅，则必须订阅它。转到您的 Citrix Cloud 帐户并执行以下操作：
    a) 在可用服务下，单击应用程序交付管理磁贴上的管理。
    b) 按照屏幕上的说明为 Citrix ADM 创建 Express 帐户。有关更多信息，请参阅 Citrix ADM 文档中的入门。
    c) 创建 Express 帐户后，请重新登录到 Analytics，然后单击 设置 **>** 数据源 **>** 安全性。
    d) 在网关站点卡片上，单击 **+** 以添加代理和网关实例。
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
   - 添加您的网关实例
   - 在虚拟服务器上启用分析

必备条件

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

  下表列出了虚拟机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（建议使用 32 GB 以获得更好的性能。）
虚拟 CPU	4（建议使用 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 Gbps

- 端口要求：确保以下端口处于打开状态，以便 Citrix ADM 代理与 Citrix Gateway 实例进行通信。

类型	Port（端口）	说明
TCP	80/443	用于从代理到 Citrix Gateway 实例的 NITRO 通信
TCP	22	用于从代理到 Citrix Gateway 实例的 SSH 通信。
UDP	4739	用于从 Citrix Gateway 到代理的 AppFlow 通信
ICMP	无保留的端口	检测从代理到 Citrix Gateway 实例的网络可访问性。
SNMP	161, 162	将 SNMP 事件从 Citrix Gateway 实例接收到代理。
Syslog	514	在代理中从 Citrix Gateway 实例接收系统日志消息。
TCP	5557	用于从 Citrix Gateway 实例到代理的日志流通信。

对于 Citrix ADM 代理与 Citrix Analytics 之间的通信，请确保以下端口处于打开状态：

类型	Port（端口）	说明
TCP	443	用于代理与 Citrix Application Delivery Management 服务之间的 NITRO 通信。

对于 Citrix ADM 代理与 Citrix Analytics 之间的通信，请确保将以下终端节点列入白名单：

端点	美国地区	欧盟地区
事件中心	https://cas-eh-ns-alias.servicebus.windows.net/	https://cas-eh-ns-eu-alias.servicebus.windows.net/

安装和设置代理

在网络环境中安装和配置 Citrix ADM 服务代理，以启用 Analytics 与数据中心中的网关实例之间的通信。

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：

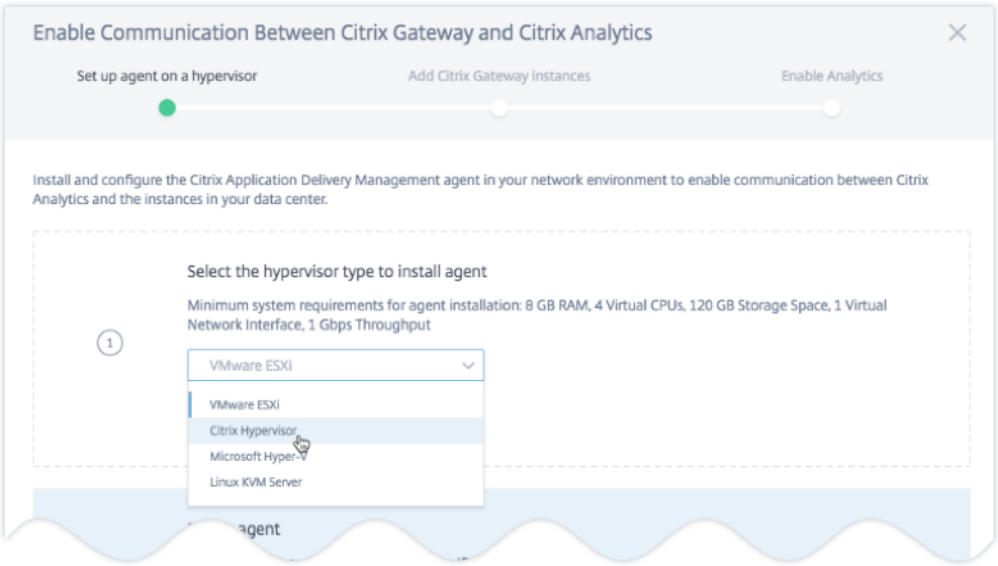
- Citrix Hypervisor

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

要安装和设置代理，请执行以下操作：

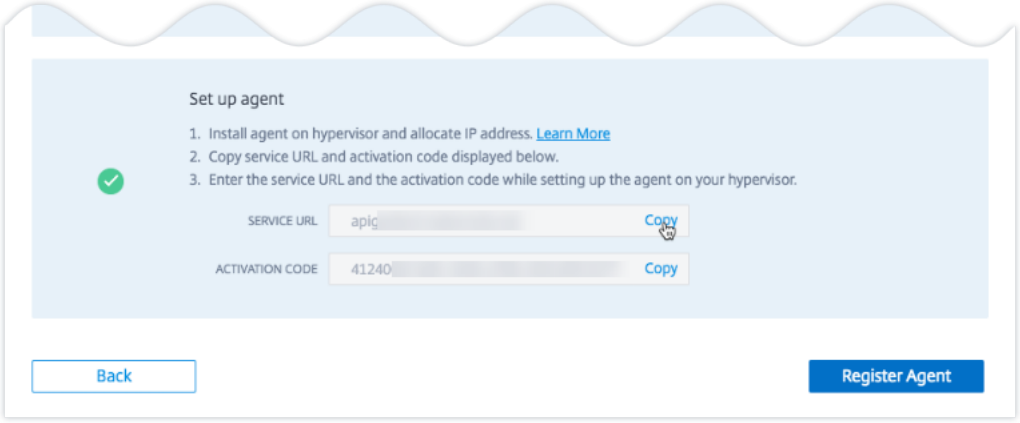
1. 下载代理映像。

   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，并将其显示在 UI 上，如下图所示。（此过程可能需要几秒钟。）代理使用服务 URL 查找服务，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。

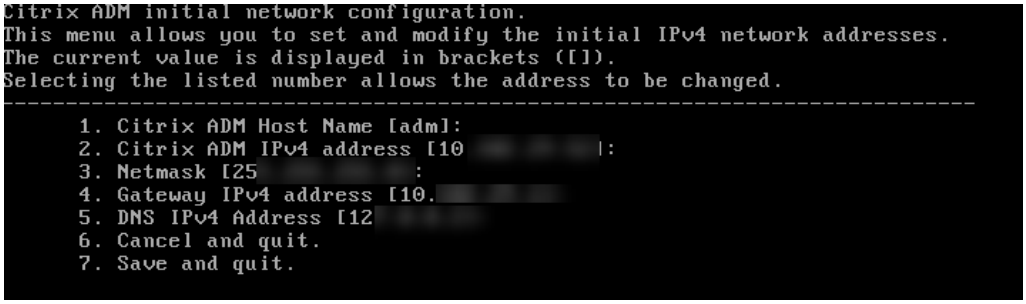


3. 在虚拟机管理程序上安装代理。

> 注意
>
> ：在开始安装代理之前，请确保：
>
> - 您拥有虚拟机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
> - 您可以将 DNS 配置为允许代理访问互联网。

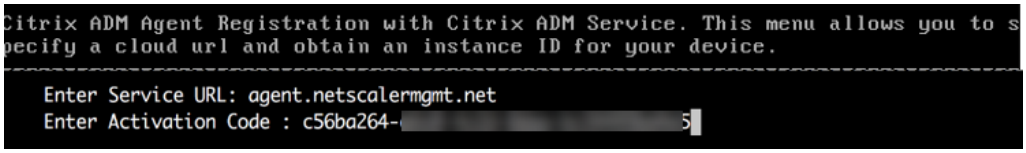
- 在 Citrix Hypervisor 上，执行以下操作：

  a) 将代理映像文件导入虚拟机管理程序。从 控制台 选项卡配置初始网络配置选项，如以下示例所示。

  如果输入的值不正确或想要更改任何值，请使用默认凭据 `nsrecover`/`nsroot` 登录 shell 提示符。然后运行命令 `networkconfig`。

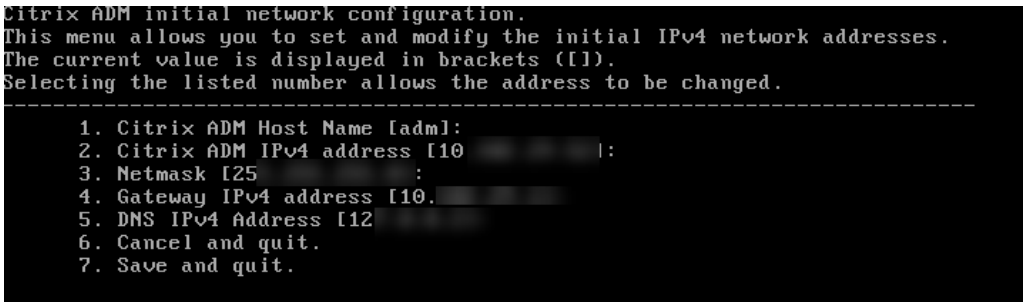
  b) 输入下载代理映像时保存的 服务 **URL** 和 激活码。

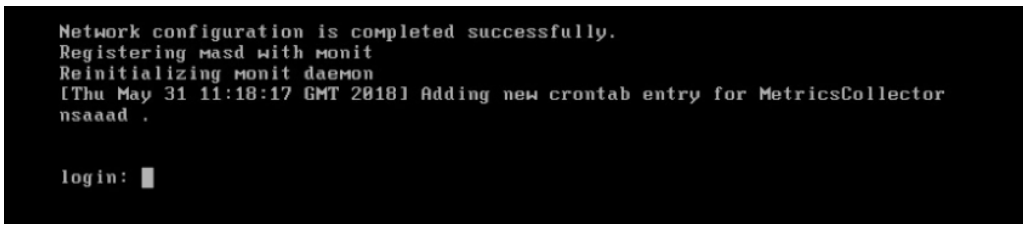
  如果输入的服务 URL 或激活码不正确，请登录到代理的 shell 提示符，然后运行脚本：`deployment_type.py`。此脚本允许您重新输入服务 URL 和激活码。

- 在 VMware ESXi 虚拟机管理程序上，执行以下操作：

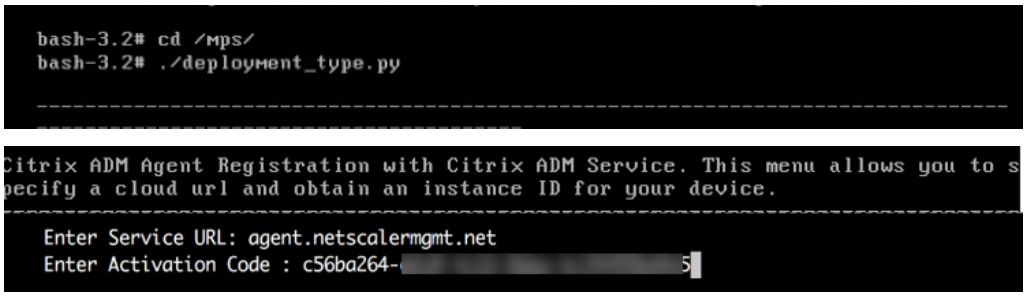
  a) 将代理映像文件导入虚拟机管理程序。从 控制台 选项卡配置初始网络配置选项，如以下示例所示。

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



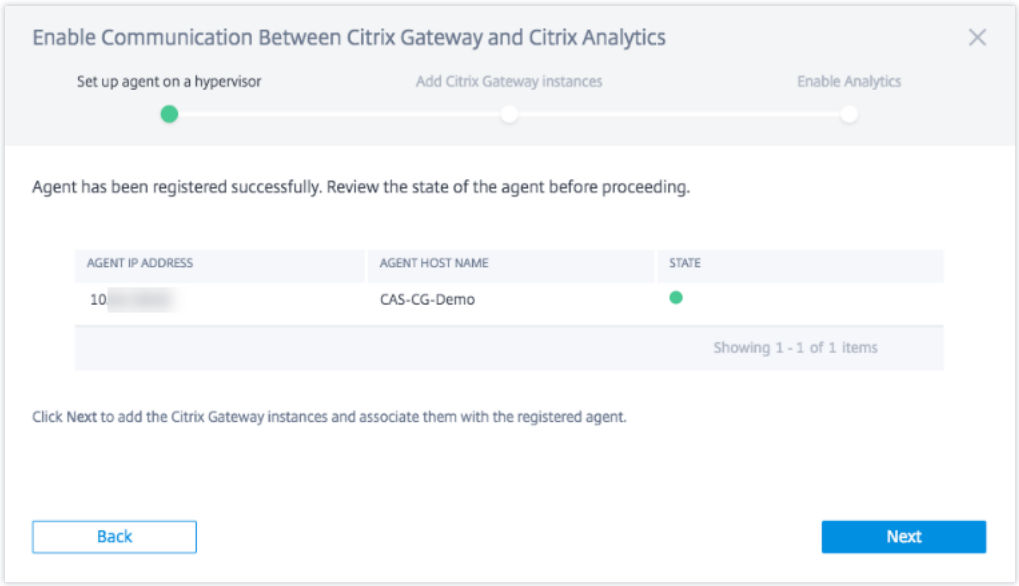
c) 导航到 **/mps** 目录，运行脚本，然后输入下载代理映像时保存的 服务 **URL** 和 激活码。



> 注意：
>
> 您可以使用同一个映像文件来安装多个代理。但是，您不能在多个代理上使用相同的激活码。要生成新的激活代码，请访问 Citrix Analytics，然后在虚拟机管理程序步骤上的安装代理上，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，代理程序将重新启动以完成安装过程。代理重新启动后，访问 Citrix Analytics，然后单击 注册代理，然后验证代理的状态。

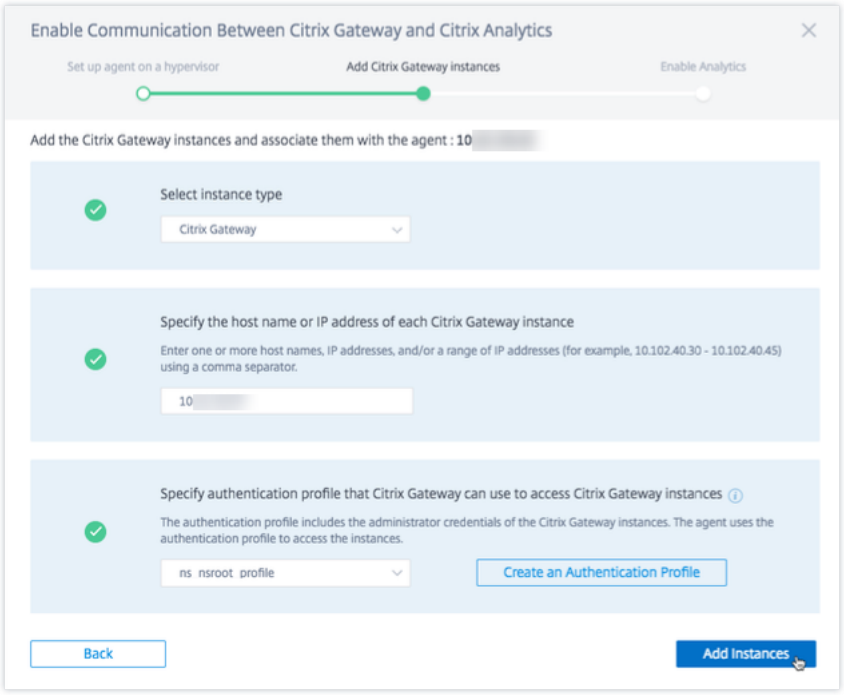


当代理状态处于运行状态，由旁边的绿色圆点表示时，单击 **Next**（下一步）开始向服务添加实例。

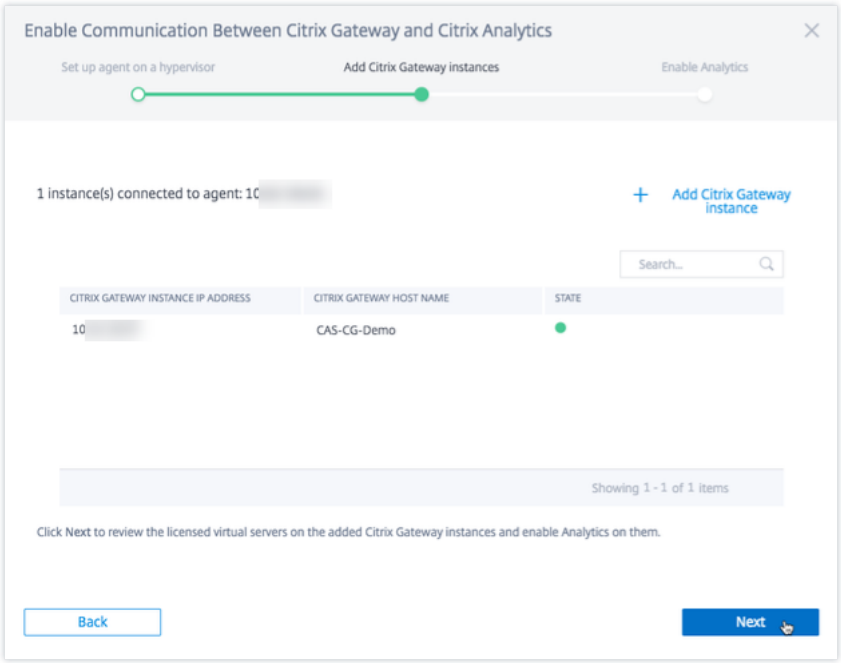
添加 **Citrix Gateway** 实例

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，然后指定要发现的网关实例的主机名或 IP 地址或 IP 地址范围。
2. 创建代理可用于访问网关实例的身份验证配置文件。此配置文件是网关实例的管理员凭证。然后，单击 添加实例。



添加实例后，您可以查看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。



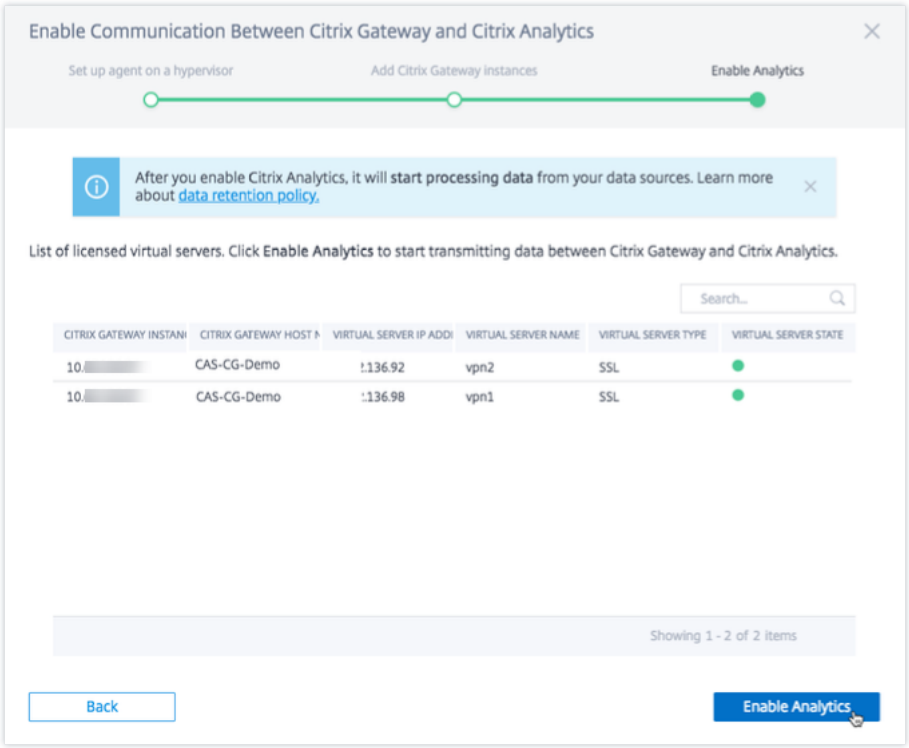
单击 下一步 启用分析。

启用分析

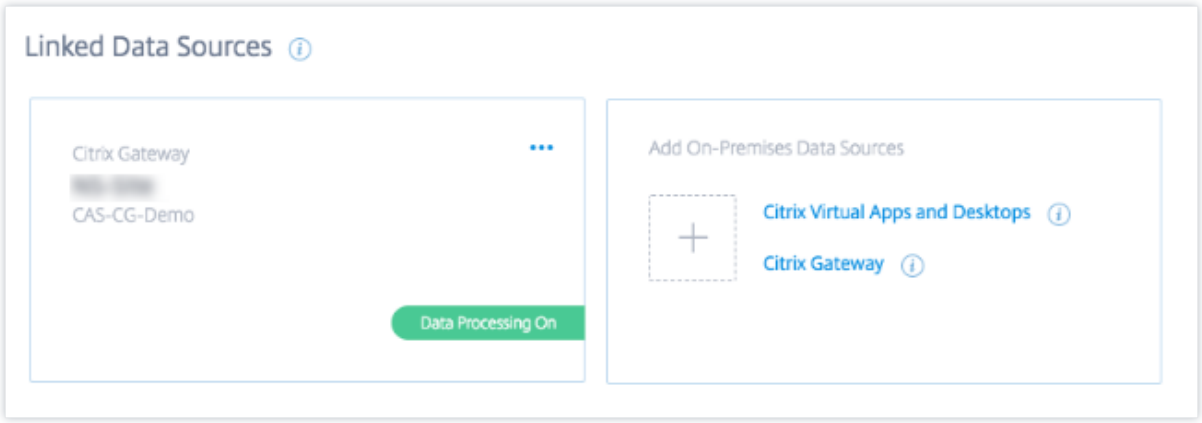
Citrix Analytics 会自动在添加的 Citrix Gateway 实例上发现许可的虚拟服务器。在所有发现的虚拟服务器上启用分析。

默认情况下，在 启用分析 页面上，将显示来自 Gateway 实例的所有许可虚拟服务器。查看许可的虚拟服务器列表，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一些时间（大约 10 分钟）才能显示在页面上。



站点卡的状态更改为“数据处理开”。您可以查看 收到的事件。



观看载入视频

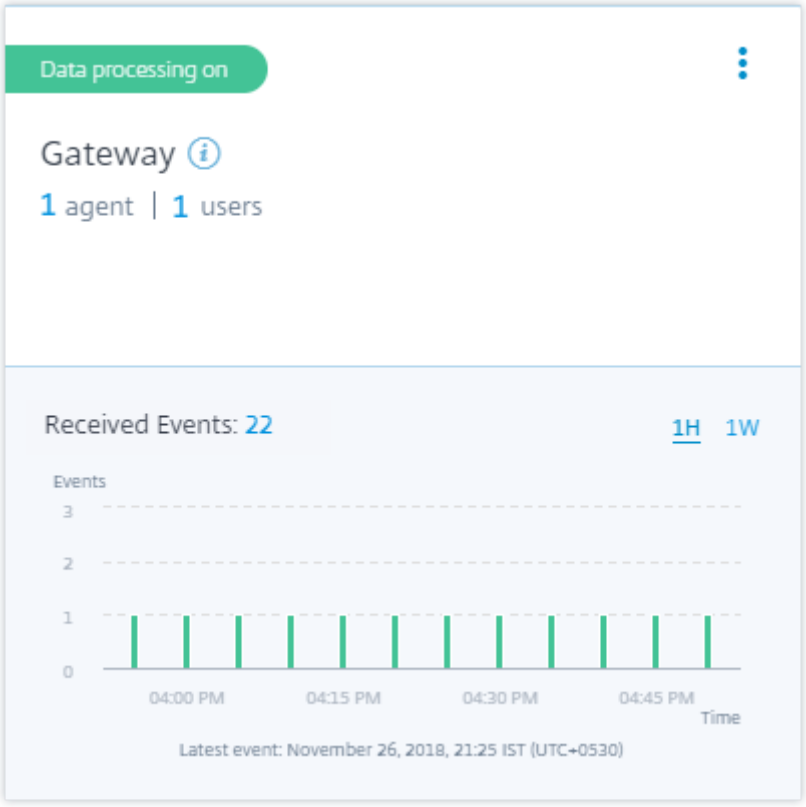
以下视频显示了载入 Gateway 实例的步骤：

这是一个嵌入式视频。单击链接观看视频

查看收到的事件、用户和代理

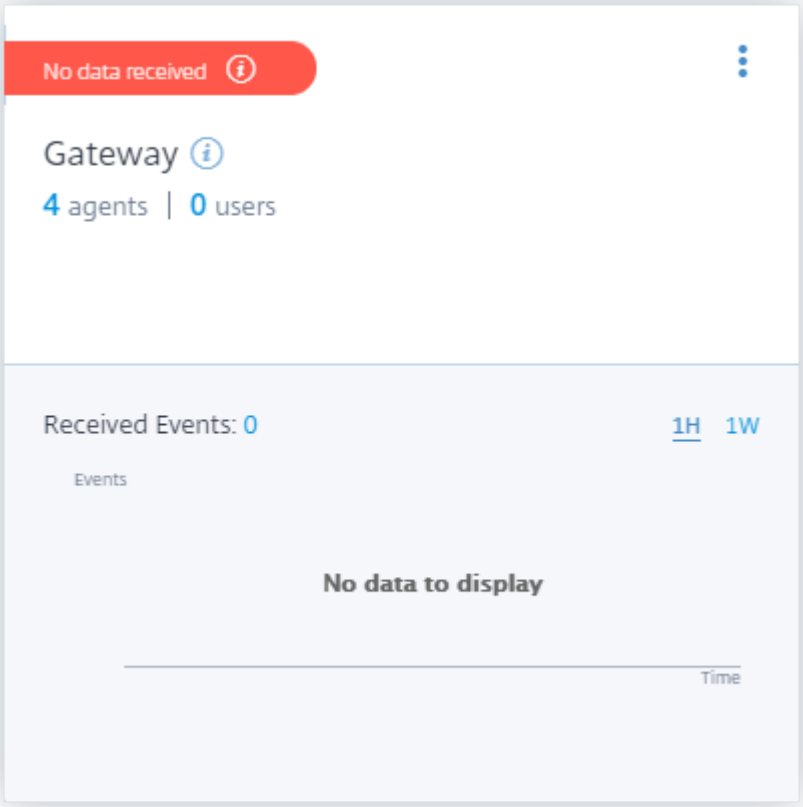
站点卡片显示过去一小时内 Gateway 用户、Citrix ADM 代理以及从数据源接收的事件的数量，这是默认时间选择。您还可以选择 1 周（**1W**）并查看数据。在“用户”页面上单击要查看的 用户 数。单击代理数量以查看 Citrix Gateway

实例和代理。



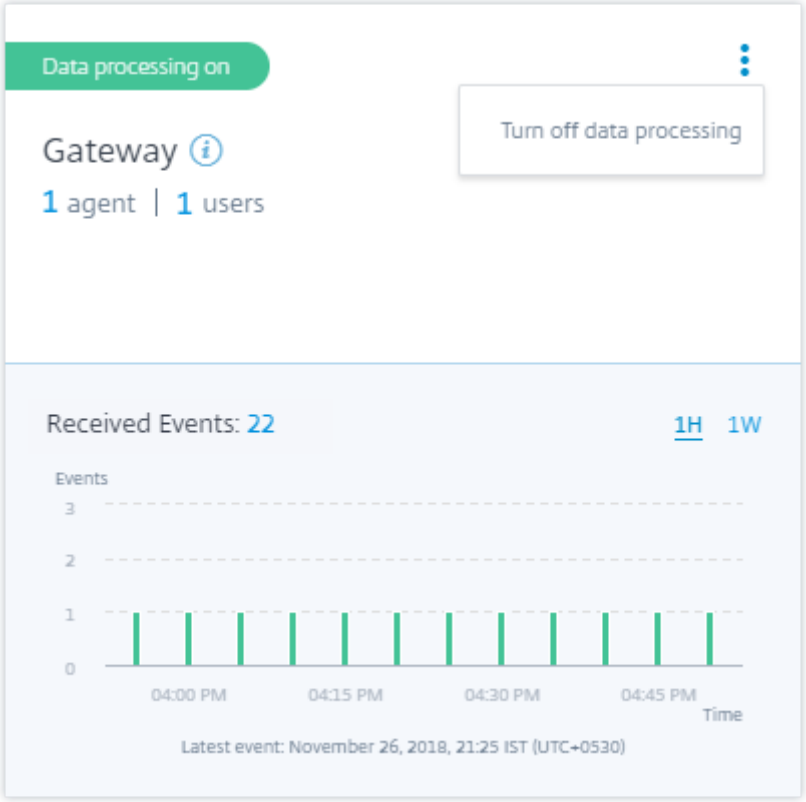
启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将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，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未更改，请刷新数据源页面。
2. Analytics 在过去一小时内未收到来自数据源的任何事件。

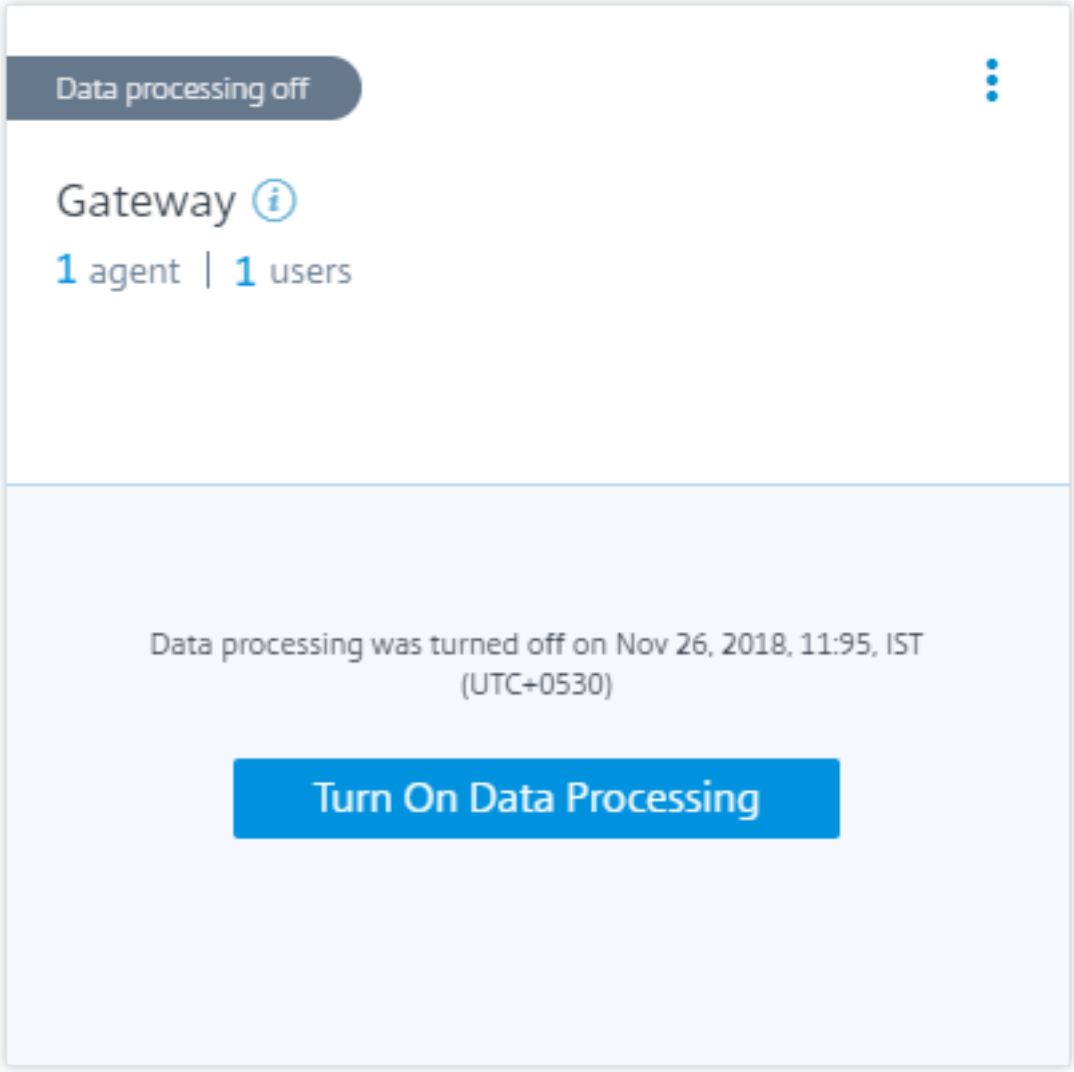


打开或关闭数据处理

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 停止处理此数据源的数据。

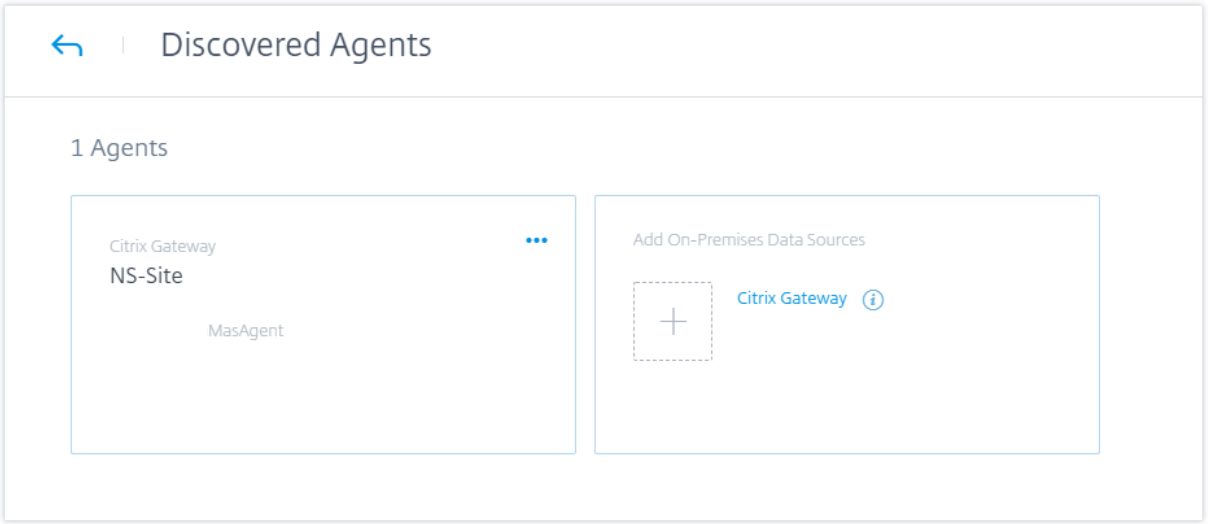


要再次启用数据处理，请单击“打开数据处理”。



添加更多网关实例

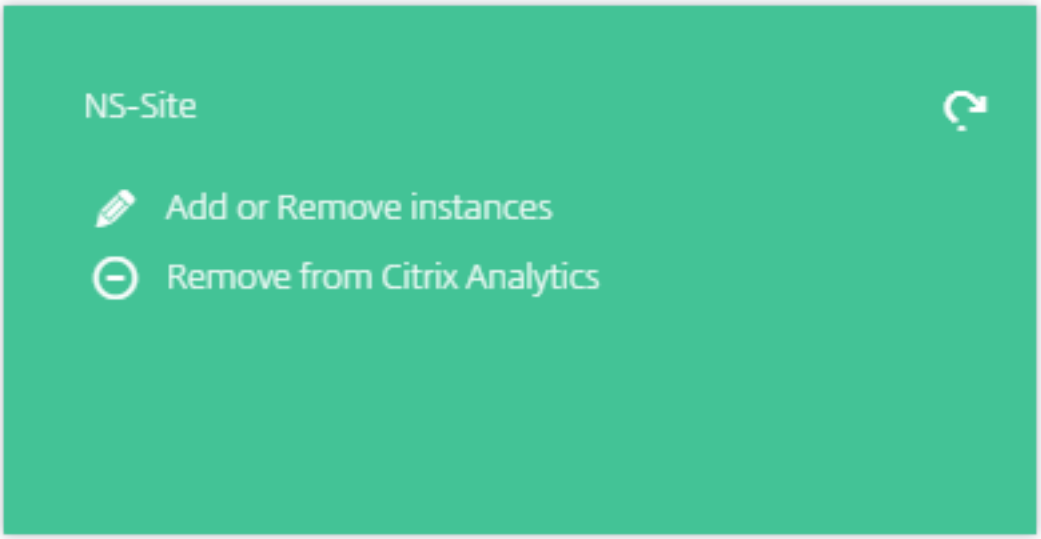
如果要添加更多网关实例，请单击网关站点卡上的代理数量以查看 发现的代理 页面。在添加本地数据源磁贴中，单击 **Citrix Gateway**。



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。

翻转座席站点卡片，然后执行以下操作之一：



- 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。您还可以移除添加到代理的实例。当您将实例与代理解除关联时，Citrix Analytics 无法与该实例进行通信。
- 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中收集数据。但是，之前处理过的所有数据在保留期内都可用。

Citrix Virtual Apps and Desktops 数据源

April 12, 2024

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。本文中提到的入门步骤适用于以下两种产品：Citrix Analytics for Performance (Performance Analytics) 和 Citrix Analytics for Security (Security Analytics)。

有关特定于每个产品的入门步骤，请参阅以下文章：

- 使用 Citrix Analytics for Performance 配置本地 Citrix Virtual Apps and Desktops 站点
- 为 Citrix Analytics for Security 配置 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源

使用 **StoreFront** 载入 **Citrix Virtual Apps and Desktops** 本地站点

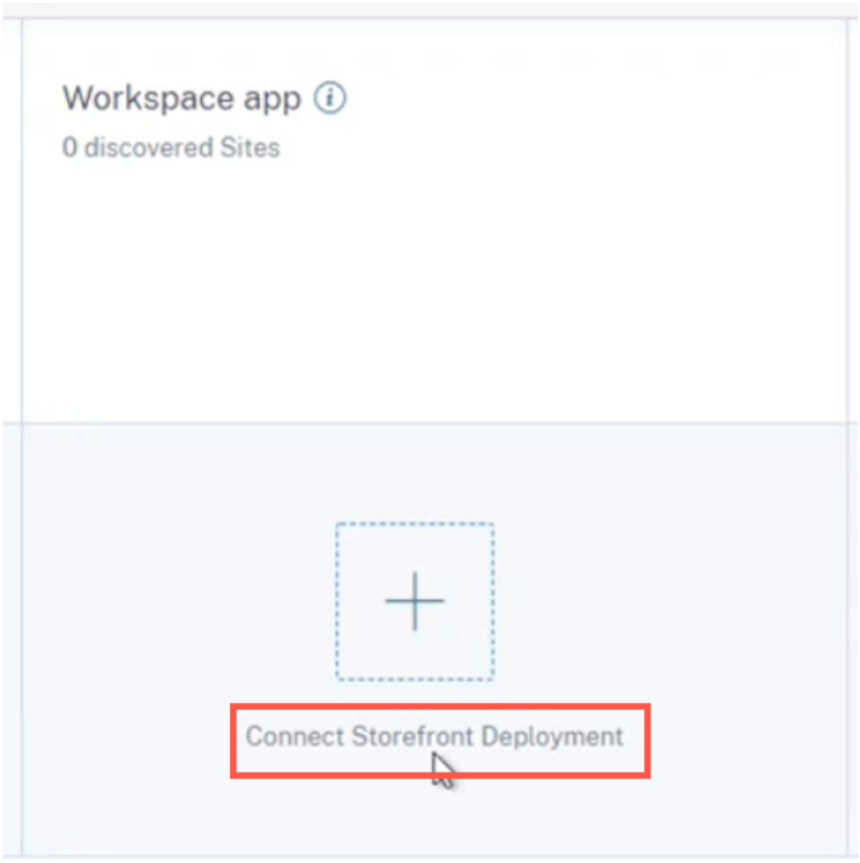
如果您的组织使用本地 StoreFront 部署，则必须将 StoreFront 服务器配置为使 Citrix Workspace 应用程序能够向 Citrix Analytics 发送事件。Citrix Analytics 处理事件，为您的 Citrix IT 基础设施的性能和用户行为提供切实可行的见解。

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 Service 一文。

此前，使用 Citrix Apps and Desktops 本地站点的客户被迫使用站点聚合在本地站点上加载 Citrix Analytics for Security 和 Citrix Analytics for Performance。

您现在可以加入 Citrix 应用程序和桌面本地站点，而无需依赖站点聚合。

即使您没有将任何站点添加到站点集合中，您也可以在 Workspace 应用程序上查看连接 **Storefront** 部署选项。



必备条件

在开始之前，请确保执行以下操作：

- 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 部署必须为出站互联网连接开放端口 443。网络上的任何代理服务器都必须允许与 Citrix Analytics 进行此通信。
- 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 Web 服务器上的 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 Web 站点。

> 注意
>
> 如果您是 HTML5 用户，则在 StoreFront 上启用某些配置后，Citrix Virtual Apps and Desktops 可以启动事件。有关配置步骤的信息，请参阅适用于 HTML5 的 Citrix Workspace 应用程序文档中的 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，请参阅适用于 HTML5 的 Citrix Workspace 应用程序文档中的 PDF 打印 文章。

  - 适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本。
  - 适用于 Linux 的 Citrix Workspace 应用程序 2006 或更高版本。
  - 适用于 Mac 的 Citrix Workspace 应用程序 2006 或更高版本

- 如果您使用的是 Citrix Virtual Apps and Desktops 7 1912 LTSR，则支持的 StoreFront 版本为 1912。

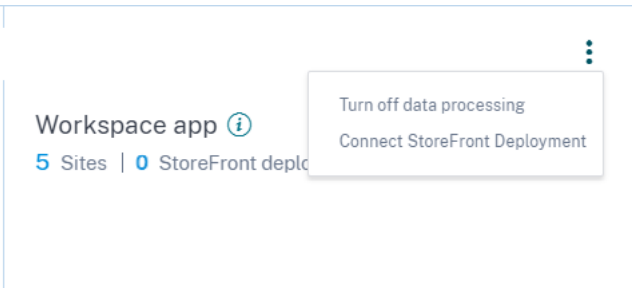
连接到 **StoreFront** 部署

您可以通过以下方式连接到 StoreFront 部署：

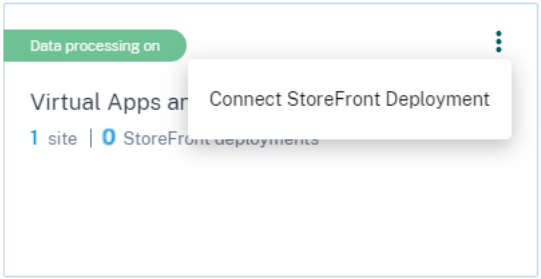
- 使用 **Apps and Desktops - Workspace** 应用程序站点卡和 **Apps and Desktops -** 监视站点卡
- 使用“推荐”面板

使用“**Apps and Desktops - Workspace** 应用程序”站点卡和“**Apps and Desktops -** 监视”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。

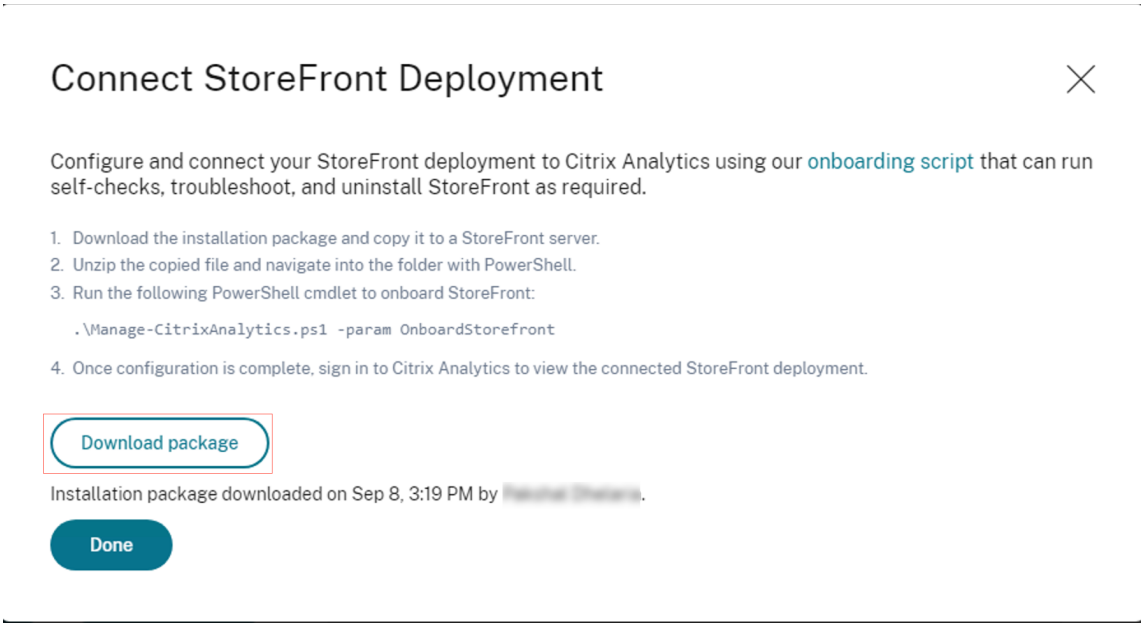


2. 导航到设置 **>** 数据源 **>** 性能。在应用程序和桌面 **-** 监视站点卡片上，单击垂直省略号 (⋮)，然后选择连接 **StoreFront** 部署。



此时将出现 StoreFront 入门向导或连接 **StoreFront** 部署弹出窗口。

3. 单击“下载软件包”。



> 注意
>
> 该文件包含敏感信息。请将该文件保存在安全的位置。

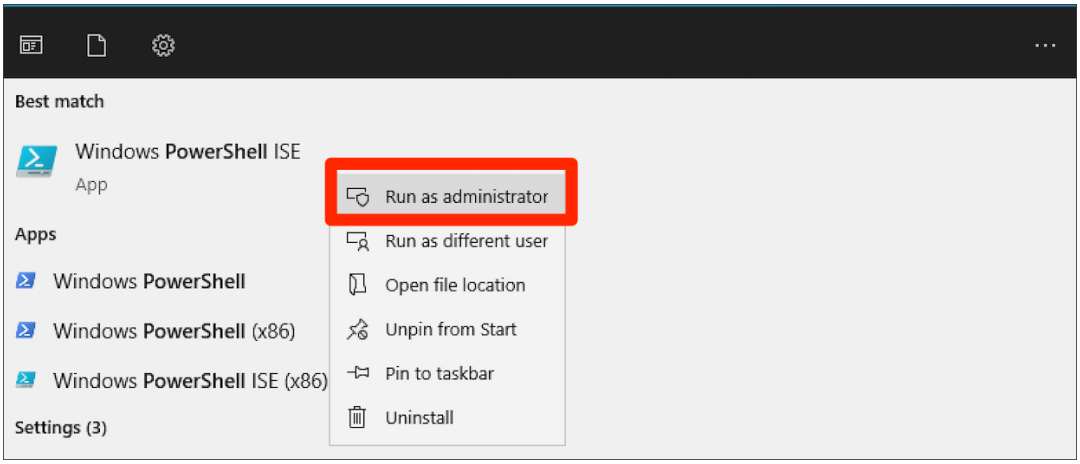
4. 要配置 StoreFront 部署，请

   a) 将安装包复制到 StoreFront 服务器。

   b) 解压缩复制的文件，然后在 PowerShell 中导航到该文件夹。

   c) 您必须以管理员身份运行以下命令才能加载 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) 如果即使在运行 OnboardStorefront 之后，StoreFront 站点仍未出现在 Citrix Analytics 服务 GUI 中，请运行 iisreset 命令。

f) 登录 Citrix Analytics Service GUI 并验证群集 ID 是否与脚本在控制台中登录的群集 ID 相匹配。

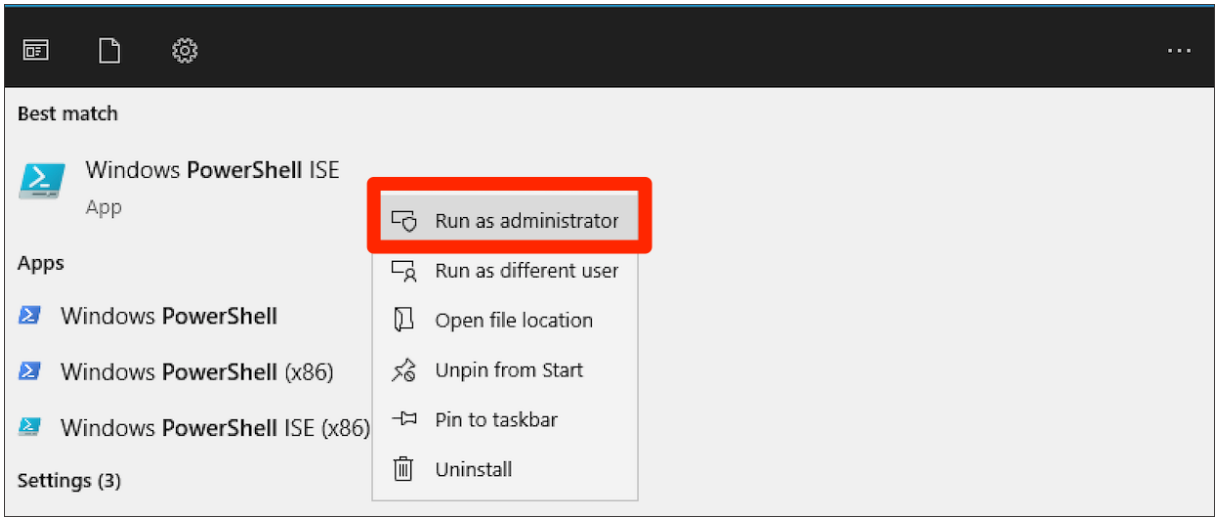
g) 配置完成后，登录 Citrix Analytics 以查看连接的 StoreFront 部署。

5. 配置成功后，单击“完成”。

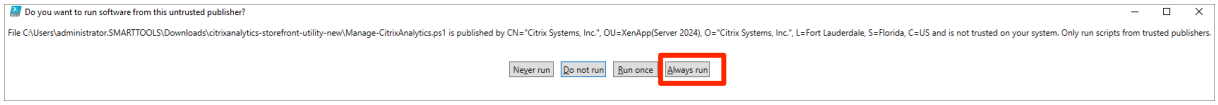
6. 单击打开数据处理以允许 Citrix Analytics 处理数据。

PowerShell 脚本

引入了新的 PowerShell 脚本，以简化 Citrix Analytics Service 的 StoreFront 登录流程。此 PowerShell 脚本可自动执行必备条件检查、安装和配置 StoreFront 的过程。PowerShell 脚本需要在管理员模式下运行。



客户可以在 StoreFront 上执行此 PowerShell 脚本来加载、登机、执行自检、故障排除以及验证 Citrix Analytics Service GUI 的入门操作是否成功。当客户首次执行脚本时，发布者上会显示一条安全警告消息，以进行确认。如果发布者受到信任，请选择“始终运行”选项。



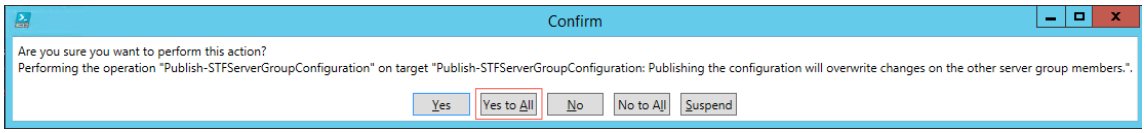
PowerShell 脚本可在连接 **StoreFront** 部署页面的 zip 文件中找到，还有 StoreFrontConfiguration.json 文件、一些 CCAuth 和 dll 文件。PowerShell 脚本日志保存在下载文件夹下的 cas-logs 文件中。

PowerShell 脚本支持以下参数：

- **SelfCheck**：**SelfCheck** 参数用于验证是否已满足 StoreFront 登录的必备条件。它会检查 StoreFront 安装、所需版本、出站连接、cURL Analytics 服务器网络连接、Internet 连接、服务器组配置以及任何现有的 Citrix Analytics 服务配置。使用以下命令运行 自检：

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

- **OnboardStorefront**：**OnboardStoreFront** 参数可快速执行自检，以验证 Citrix Analytics 服务配置的设置准备就绪。如果设置准备就绪，它将导入 Citrix Analytics 服务配置，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，将 StoreFront 配置发布到该 StoreFront 中的所有服务器。您可以看到一个弹出窗口来确认 `PublishConfiguration` 操作。选择“全是”按钮。

  成功完成配置发布后，该脚本会调用 Citrix Analytics 服务 API，以检查 StoreFront 是否已加入 Citrix Analytics 服务 GUI。要调用此 API，需要使用私钥进行身份验证。要生成此私钥，您需要 CCAuth 和 dll 文件，以及下载的 JSON 文件中可用的凭据。

  > 注意
  >
  > StoreFront 登录流程完成后，StoreFront 可能需要两到五分钟才能显示在 Citrix Analytics Service GUI 中。如果 StoreFront 网站未出现在 Citrix Analytics 服务 GUI 中，则必须执行 IISRESET 才能重置互联网信息服务。

  使用以下命令运行 **OnboardStoreFront**：

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

- **IsOnboarded**：**IsOnboarded** 参数用于验证 StoreFront 是否已加入 Citrix Analytics Service GUI。脚本会等待一分钟才退出，但是，成功启动后，StoreFront 最多可能需要五分钟才能显示在 GUI 中。您必须运行此命令才能对其进行验证。此命令还具有 CCAuth 和 dll 文件依赖关系。使用以下命令运行 **IsOnboarded**：

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


- 故障排除：等待五分钟后，如果 StoreFront 网站未出现在 Citrix Analytics Service GUI 中，则必须执行 IISRESET 才能重置互联网信息服务。如果 StoreFront 网站仍未显示在 GUI 中，请使用 故障排除 参数。它可以帮助您解决任何连接问题并收集日志。使用以下命令运行“故障排除”：

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

  故障排除参数对以下两个用例很有用：

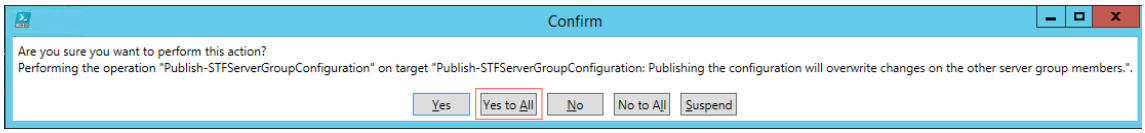
  - 用例 **1**：作为自检的一部分，如果 curlAnalytics 失败，则会创建防火墙规则。此防火墙规则打开 443 端口并验证其与 Analytics 的连接。如果不是，则意味着无法访问 Analytics 服务器，脚本将从此处退出。恢复与 Citrix Analytics 服务的连接后，重新运行脚本。
  - 用例 **2**：如果 cURL 运行良好，但是 StoreFront 网站没有反映在 GUI 中，则管理员必须从“下载 DebugView”中下载 DebugView 工具 zip 文件，解压缩，然后将其放在“下载”文件夹下。如果已经配置了 Citrix Analytics 服务，PowerShell 脚本会首先将其卸载。它启用详细日志。然后，它启动 DebugView 工具并重新安装 Citrix Analytics 服务。最后，它会停止 DebugView 并禁用 Verbose 日志记录。

  可以捕获调试视图日志，并与 Citrix 支持部门共享。Citrix 管理员进一步调试并尝试找出问题并加以解决。生成日志并将其作为日志文件保存在 DebugView 文件夹中。

  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。这些日志是在脚本执行过程中生成的，并保存在“下载”**>**“**cas-logs**”文件夹下。

  对于服务器组，当脚本尝试退出或加载 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 内的所有服务器。您可以看到一个弹出窗口来确认此操作。选择“全是”按钮。

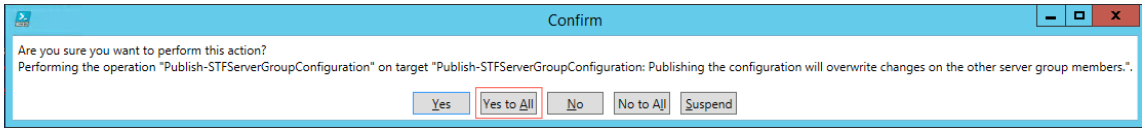
  

- **DeboardStoreFront**：DeboardStoreFront 参数用于从 Citrix Analytics Service 中删除 StoreFront 服务器。使用以下命令运行 DeboardStoreFront：

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

  PowerShell 脚本首先从 StoreFront 中删除所有 Citrix Analytics 服务配置，然后验证删除是否成功。然后，它会检查 ServerGroup 是否存在，然后发布配置，以便将删除的配置发布到所有 StoreFront。最后，它会调用 DeleteSiteOnboarded。如果网站未从 Citrix Analytics Service GUI 中删除，则需要使用 StoreFront 部署和 StoreFront 部署下的 Workspace 应用程序网站卡手动删除 StoreFront 站点。

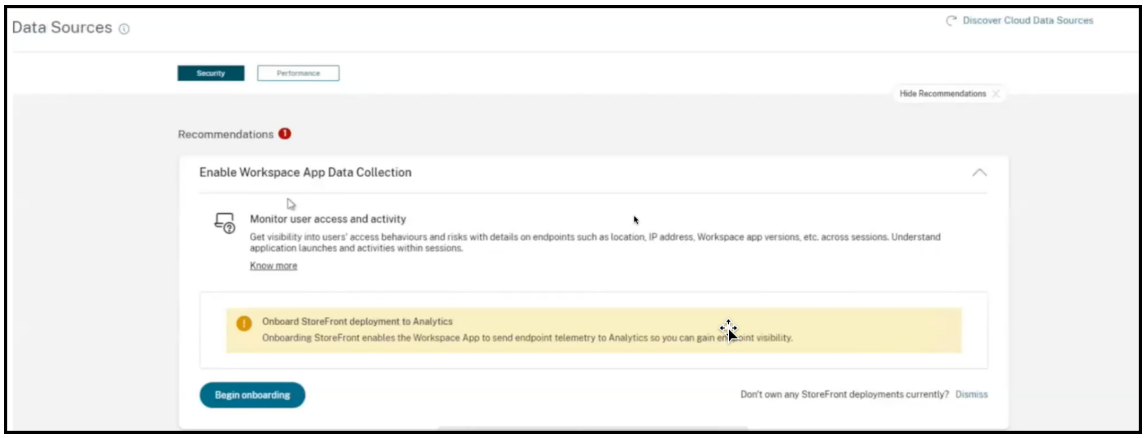
  对于服务器组，PublishConfiguration 命令会自动从脚本运行，将 StoreFront 配置发布到该 StoreFront 中的所有服务器。您可以看到一个弹出窗口来确认此操作。选择“全是”按钮。



使用“推荐”面板进行连接

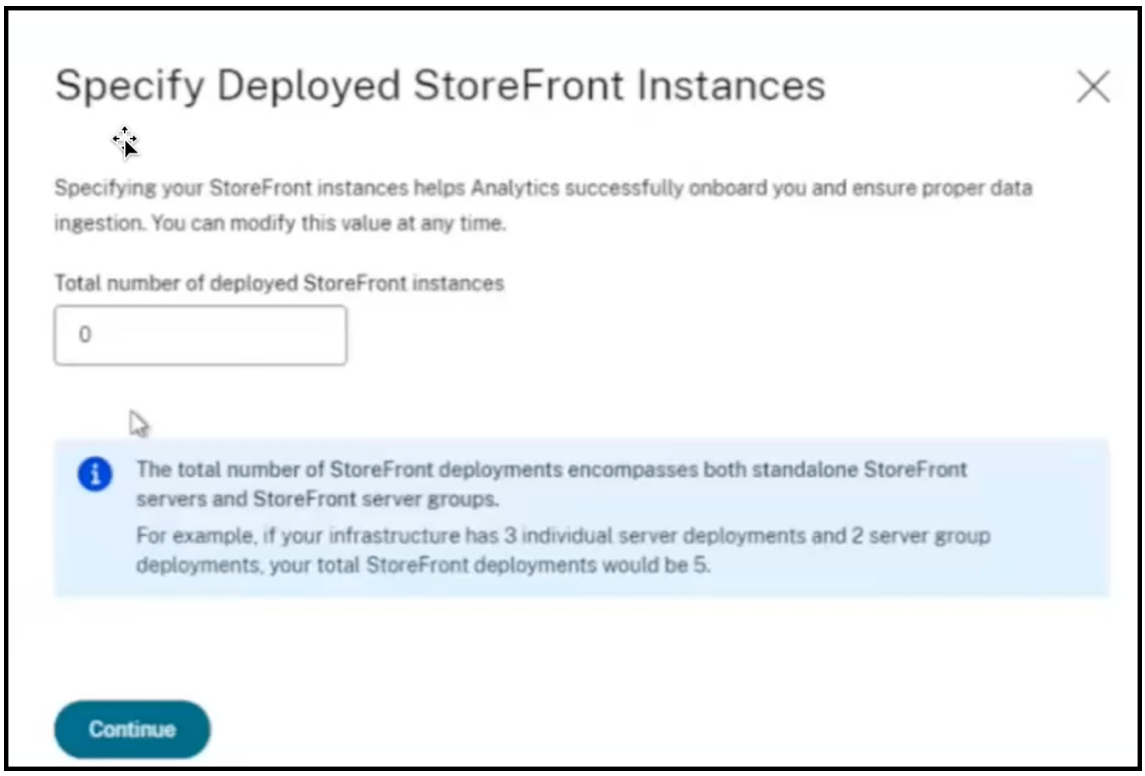
“数据源”页面上的“建议”面板向用户介绍登录数据源的重要性。它可以帮助用户轻松加载数据源，还为用户提供了查看和确保他已载入所有可用数据源的选项。

1. 如果您使用的是 Security Analytics 产品，请选择“设置”**>**“数据源”**>**“安全性”。
2. 如果您使用的是性能分析产品，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，以加入 Storefront 部署。



> 注意
>
> 通过加入 StoreFront 数据源，Workspace 应用程序可以将有关端点可见性的遥测数据发送到 Analytics。

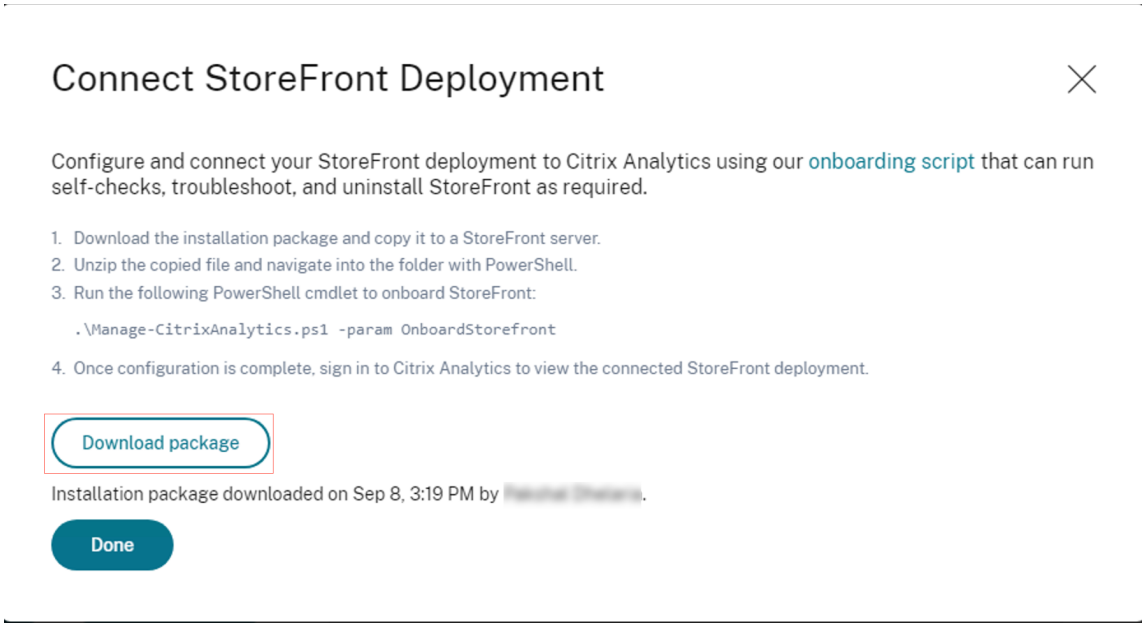
4. 单击“开始入门”。此时将出现“指定已部署的 **StoreFront** 实例”页面。



5. 为确保 Analytics 成功加载数据源，请指定已部署的 **StoreFront** 实例总数。

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

6. 单击继续。此时将出现 StoreFront 入门向导或连接 **StoreFront** 部署弹出窗口。
7. 在“连接 **StoreFront** 部署”页面上，单击“下载软件包”以下载安装包。



> 备注
>
> 该文件包含敏感信息。请将该文件保存在安全的位置。
>
> 您可以下载一个套餐并仅用于加入一个 StoreFront 组。如果您有多个 StoreFront 组，则必须为每个 StoreFront 组分别下载套餐。使用一个套餐完成一个 StoreFront 组入职后，再次下载该套餐并继续为下一个 StoreFront 组加入。
>
> 如果由于某些问题，StoreFront 入门服务未在两天内使用一个套餐正确完成，则必须在两天后重新下载新套餐。因为如果在两天内未成功登录，套餐中的密钥将过期。

8. 要配置 StoreFront 部署，请

   a) 将安装包复制到 StoreFront 服务器。

   b) 解压缩复制的文件，然后在 PowerShell 中导航到该文件夹。

   c) 运行以下命令以登录 StoreFront：

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

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

   e) 如果 StoreFront 网站未出现在 Citrix Analytics 服务 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，单击“完成”。

如果您通过“推荐”面板进行入门，则系统会获取您已加载到 Citrix Analytics 服务的 StoreFront 部署数量。将出现“建议”面板，您可以查看已加入的 StoreFront 部署。您可以在“推荐”面板中查看消息，然后单击“标记为完成”。

> 注意
>
> 只有当所有已声明的 Storefront 部署都已加入时，推荐面板和消息才会消失。

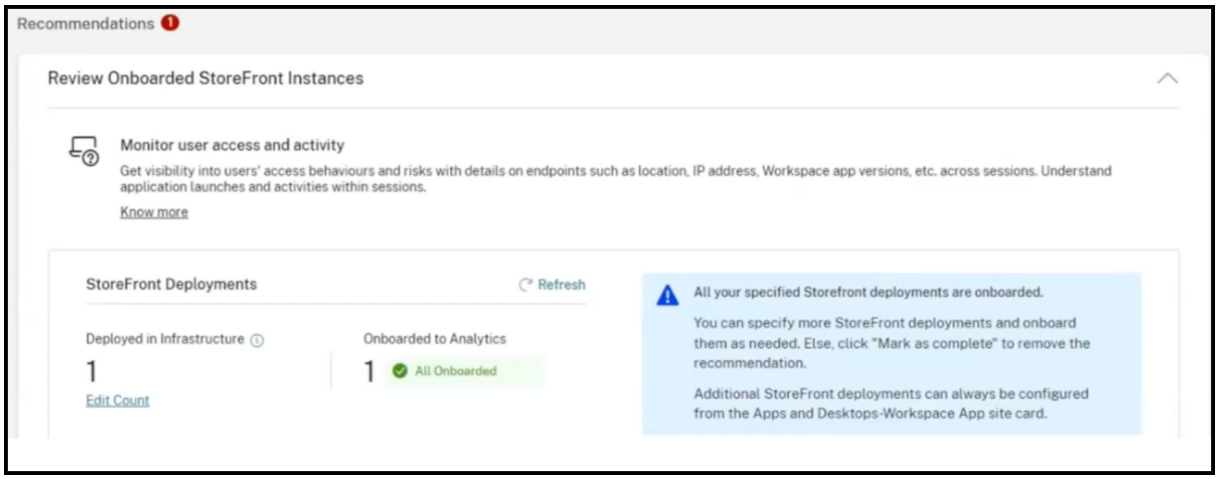
1. 单击打开数据处理以允许 Citrix Analytics 处理数据。

查看“建议”面板

您可以将在“建议”面板中声明的 StoreFront 部署数量与已加入的 StoreFront 部署数量进行比较。

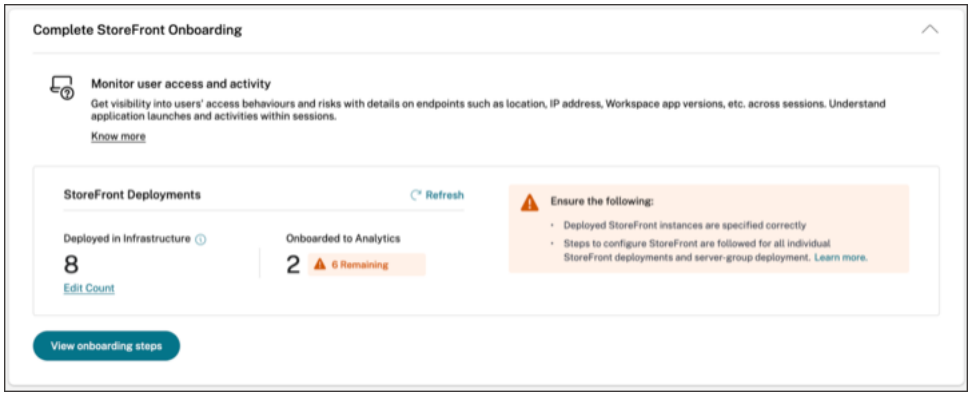
如果声明的 StoreFront 部署数量与已载入的 StoreFront 部署数量相同，则会显示一条全部已载入消息，指示所有 StoreFront 部署均已加载。您可以在“推荐”面板中查看消息，然后单击“标记为完成”。

> 注意
>
> 如果您想加入更多 StoreFront 部署，请单击“查看入门步骤”，StoreFront 入门向导或连接 **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，请单击“编辑数量”，然后显示“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，然后单击继续。StoreFront 入门向导或连接 **StoreFront** 部署弹出窗口再次出现。按照步骤启动更多 StoreFront 部署。

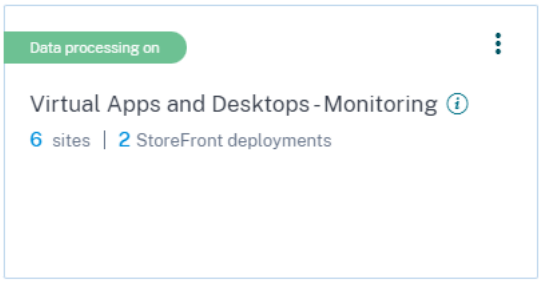
> 注意：
>
> 部署的 **StoreFront** 实例总数是 StoreFront 组的总数，它不是单个 StoreFront 服务器的数量。



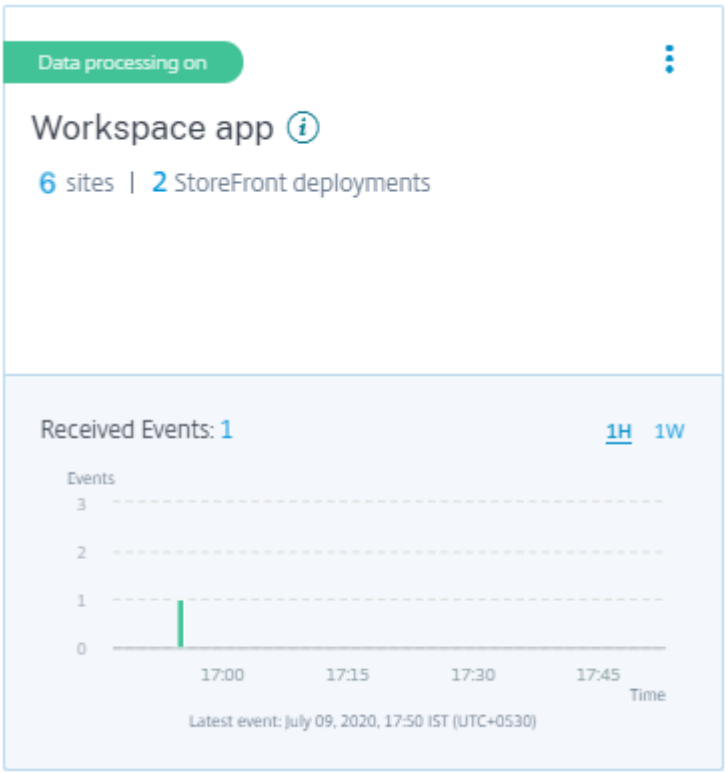
查看已连接的 **StoreFront**

仅当配置成功时，StoreFront 部署才会显示在站点卡上。站点卡片显示有多少 StoreFront 部署已与 Citrix Analytics 建立了连接。

- 如果您使用的是 Performance Analytics 产品，则可以在应用程序和桌面监视站点卡片上看到以下信息：

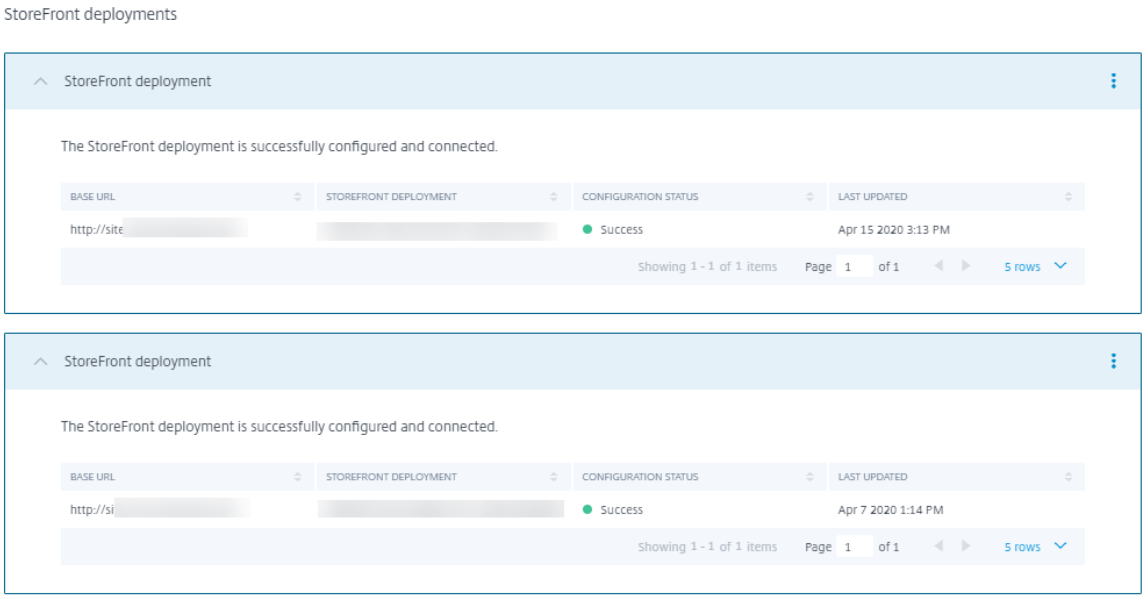


- 如果您使用的是 Security Analytics 产品，则可以在 **Workspace** 应用程序站点卡片上看到以下信息：



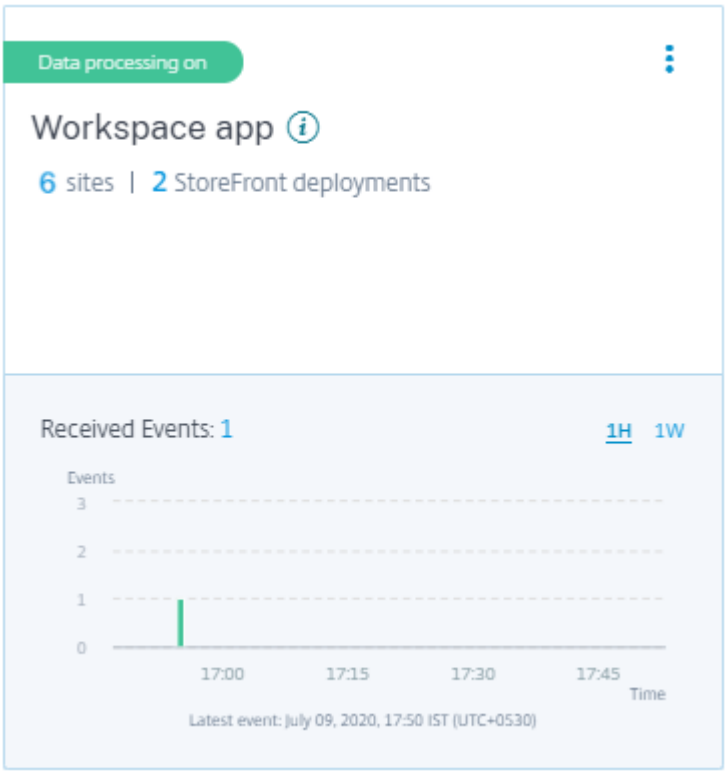
单击站点卡片上的 StoreFront 部署数以查看服务器组。

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



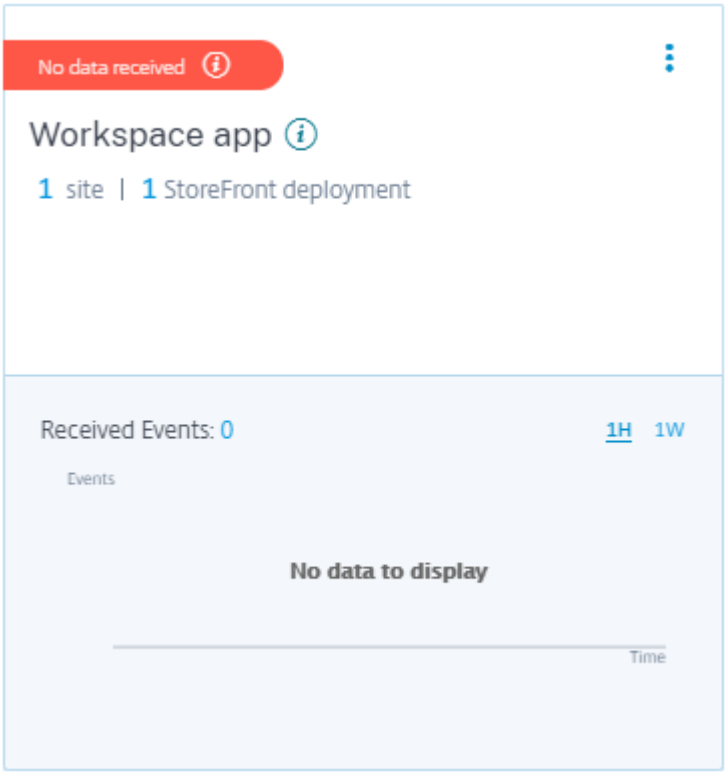
如果您使用的是 Security Analytics 产品，站点卡还会显示有关接收到的事件的以下信息：

- 过去一小时（默认时间选择）内从 StoreFront 部署接收的事件。还可以选择 1 周 (1 W) 并查看数据。单击接收的事件数可在 自助搜索 页面上查看事件。



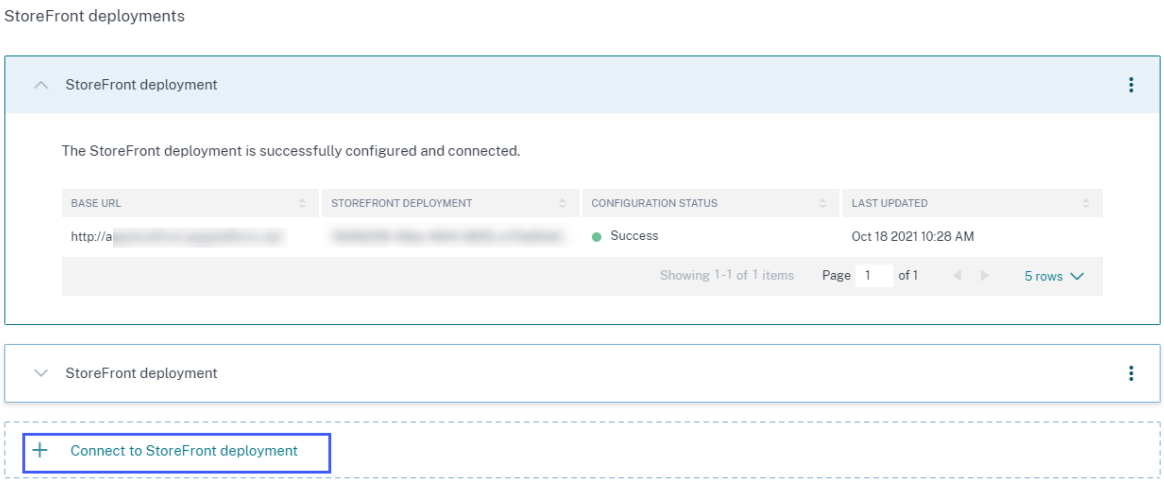
- 启用数据处理后，站点卡片可能会显示“未收到数据”状态。出现此状态有两种原因：

1. 如果您是首次打开数据处理，事件将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，状态将更改为 **Data processing on**（数据处理已启用）。如果状态在一段时间后仍未更改，请刷新数据源页面。
2. Citrix Analytics 在过去一小时内未收到来自数据源的任何事件。



添加或删除 **StoreFront** 部署

要添加 StoreFront 部署，请单击 **StoreFront** 部署部分上的连接到 **StoreFront** 部署。下载配置文件，然后按照步骤配置 StoreFront 部署。



要停止从已配置的 StoreFront 部署中传输事件并将其从 Citrix Analytics 中删除，请执行

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

```
Remove-STFCasConfiguration
```

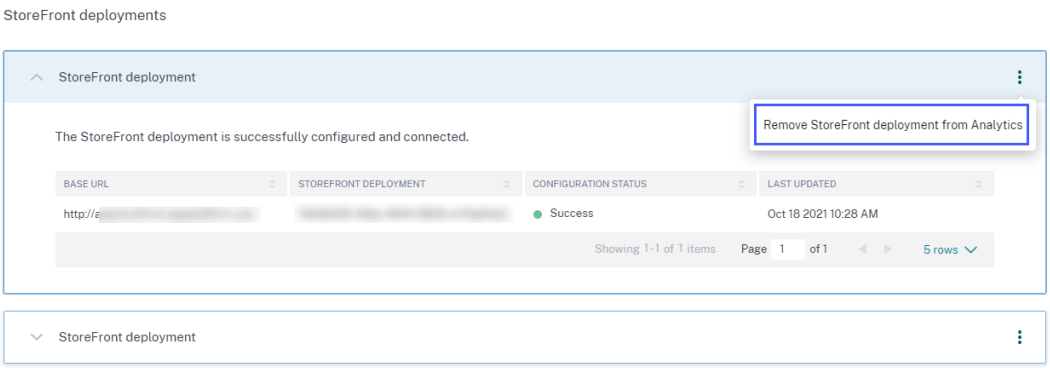
2. 如果您使用的是多服务器部署，请运行以下命令来传播更改，并从 StoreFront 服务器组中的所有服务器中删除配置设置：

```
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，该命令将不返回任何内容。

```
Get-STFCasConfiguration
```

4. 重新登录到 Citrix Analytics，然后在 StoreFront 部署部分选择 **StoreFront** 部署。单击垂直省略号 (⋮)，然后选择从 **Analytics** 中移除 **StoreFront** 部署。



> 注意
>
> 在将其从 Citrix Analytics 中删除之前，在 StoreFront 部署上运行指定的命令。如果无法运行命令，Citrix Analytics 将继续接收事件，并在下一个事件池周期再次添加 StoreFront 部署。

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

如果 StoreFront 托管在使用网络代理连接互联网的网络服务器上，则必须手动将商店配置为向 Citrix Analytics 注册。此配置要求您在商店 web.config 文件中添加一个 <system.net> 部分。您必须在 StoreFront 部署上配置向 Citrix Analytics 发送事件的每个应用商店。

有两种方法可以将 <system.net> 部分添加到 store 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）。
- 在商店 web.config 文件中手动添加一个 <system.net> 部分。

有关这些方法的详细信息，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 注册一 文。

数据治理

April 12, 2024

本节提供有关 Citrix Analytics 服务收集、存储和保留日志的信息。未在“定 义”部分中定义 的任何大写术语均具有 Citrix 最终用户服务协议中指定的含义。

Citrix Analytics 旨在让客户深入了解其 Citrix 计算环境中的事件。Citrix Analytics 使安全管理员能够选择他们想要监视的日志，并根据记录的事件采取定向措施。这些见解可帮助安全管理员管理对其计算环境的访问，并在客户的计算环境中保护客户内容。

数据驻留

Citrix Analytics 日志与数据源分开维护，并聚合到位于美国、欧盟和亚太南部地区的多个 Microsoft Azure 云环境中。日志的存储取决于 Citrix Cloud 管理员在将组织加入 Citrix Cloud 时选择的主区域。例如，如果您在将组织加入 Citrix Cloud 时选择了欧洲区域，则 Citrix Analytics 日志将存储在欧盟的 Microsoft Azure 环境中。

有关更多信息，请参阅 Citrix Cloud Services 客户内容和日志处理 以及 地理注意事项。

数据收集

Citrix Cloud 服务经过精心设计，可将日志传输到 Citrix Analytics。日志是从以下数据源收集的：

- Citrix ADC（本地）以及 Citrix Application Delivery Management 的订阅
- Citrix Endpoint Management
- Citrix Gateway（本地）

- Citrix 身份提供程序
- Citrix Secure Browser
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
- Microsoft Active Directory
- Microsoft Graph 安全性

数据传输

Citrix Cloud 日志安全传输到 Citrix Analytics。当客户环境的管理员明确启用 Citrix Analytics 时，这些日志将被分析并存储在客户数据库中。这同样适用于配置了 Citrix Workspace 的 Citrix Virtual Apps and Desktops 数据源。

对于 Citrix ADC 数据源，只有当管理员为特定数据源明确启用 Citrix Analytics 时，才会启动日志传输。

数据控制

管理员可以随时打开或关闭发送到 Citrix Analytics 的日志。

当 Citrix ADC 本地数据源关闭时，特定 ADC 数据源与 Citrix Analytics 之间的通信将停止。

如果对其他数据源全部关闭，则不再分析特定数据源的日志并将其存储在 Citrix Analytics 中。

数据保留

Citrix Analytics 日志以可识别的形式保留最长 13 个月或 396 天。所有日志和相关的分析数据（如用户风险概况、用户风险评分详细信息、用户风险事件详细信息、用户观察列表、用户操作和用户配置文件）将在此期间保留。

例如，如果您已于 2021 年 1 月 1 日在数据源上启用了分析，则默认情况下，2021 年 1 月 1 日收集的数据将保留在 Citrix Analytics 中，直到 2022 年 1 月 31 日。同样，2021 年 1 月 15 日收集的数据将保留到 2022 年 2 月 15 日，依此类推。

即使在关闭数据源的数据处理或从 Citrix Analytics 中删除数据源之后，此数据仍会在默认数据保留期内存储。

Citrix Analytics 将在订阅期或试用期到期后 90 天内删除所有客户内容。

数据导出

本节介绍从 Citrix Analytics for Security 和 Citrix Analytics for Performance 中导出的数据。

Citrix Analytics for Performance 从数据源收集和分析性能指标。

您可以将自助搜索页面中的数据下载为 CSV 文件。

Citrix Analytics for Security 从各种产品（数据源）收集用户事件。对这些事件进行处理，以提供对用户风险和异常行为的可见性。您可以将这些与用户风险洞察和用户事件相关的已处理数据导出到系统信息和事件管理 (SIEM) 服务。

目前，可以通过两种方式从 Citrix Analytics for Security 中导出数据：

- 将 Citrix Analytics for Security 与您的 SIEM 服务集成
- 将自助搜索页面中的数据作为 CSV 文件下载。

将 Citrix Analytics for Security 与 SIEM 服务集成时，数据将通过使用北向的 Kafka 主题或基于 Logstash 的数据连接器发送到您的 SIEM 服务。

目前，您可以与以下 SIEM 服务集成：

- Splunk（通过 Citrix Analytics 附加组件进行连接）
- 任何支持 Kafka 主题或基于 Logstash 的数据连接器的 SIEM 服务，例如 Elasticsearch 和 Microsoft Azure Sentinel

您还可以使用 CSV 文件将数据导出到 SIEM 服务。在自助搜索页面中，您可以查看数据源的数据（用户事件）并将这些数据下载为 CSV 文件。有关 CSV 文件的详细信息，请参阅 自助搜索。

> 重要提示
>
> 将数据导出到 SIEM 服务后，Citrix 不负责安全性、存储、管理和导出数据在 SIEM 环境中的使用。

您可以打开或关闭从 Citrix Analytics for Security 到 SIEM 服务的数据传输。

有关处理过的数据和 SIEM 集成的信息，请参阅安全信息和事件管理 (SIEM) 集成和适用于 SIEM 的 Citrix Analytics 数据格式。

Citrix Services Security Exhibit

有关应用于 Citrix Analytics 的安全控制的详细信息，包括访问和身份验证、安全计划管理、业务连续性和事件管理，都包含在 Citrix Services 安全展览中。

定义

客户内容 是指上载到客户帐户以供存储的任何数据，或客户环境中允许 Citrix 执行服务的数据。

日志是指与服务相关的事件记录，包括衡量性能、稳定性、使用率、安全性和支持的记录。

服务 是指上述为 Citrix Analytics 目的概述的 Citrix Cloud 服务。

数据收集协议

将数据上传到 Citrix Analytics 并使用 Citrix Analytics 的功能，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 Citrix 产品和服务的技术、用户或相关信息。

Citrix 始终根据 Citrix 隐私政策处理收到的信息。

附录：收集的日志

- Citrix Analytics for Security 日志
- Citrix Analytics for Performance 日志

Citrix Analytics for Security 日志

常规日志

通常，Citrix Analytics 日志包含以下标头标识数据点：

- 标题键
- 设备识别
- 标识
- IP 地址
- 组织
- 产品
- 产品版本
- 系统时间
- 租户身份
- 类型
- 用户：电子邮件、ID、SAM 帐户名、域、UPN
- 版本

Citrix Endpoint Management 服务日志

Citrix Endpoint Management 服务日志包含以下数据点：

- 合规性
- 企业拥有
- 设备 ID
- 设备型号
- 设备类型
- 地理纬度
- 地理经度
- 主机名
- IMEI
- IP 地址
- 越狱
- 上次事件
- 管理模式
- 操作系统
- 操作系统版本
- 平台信息
- 原因
- 序列号
- 受监督

Citrix Secure Private Access 日志

- AAA 用户名
- 身份验证策略操作名称
- 身份验证会话 ID
- 请求 URL
- URL 类别策略名称
- VPN 会话 ID

- 虚拟服务器 IP
- AAA 用户电子邮件 ID
- 实际模板代码
- 应用程序 FQDN
- 应用程序名称
- 应用名称虚拟服务器 LS
- 应用标志
- 身份验证类型
- 认证阶段
- 身份验证状态码
- 后端服务器 Dst IPv4 地址
- 后端服务器 IPv4 地址
- 后端服务器 IPv6 地址
- 类别域名
- 类别域名来源
- 客户端 IP
- 客户端 MSS
- 客户端快速 Rex 计数
- 客户端 TCP 抖动
- 重新传输的客户端 TCP 数据包
- 客户端 TCP RTO 计数
- 客户端 TCP 零窗口计数
- 客户端流标志 Rx
- 客户端流标志 Tx
- 客户端 TCP 标志 Rx
- 客户端 TCP 标志 Tx
- 连接链跳数
- 连接链 ID
- 出口接口

- 导出进程 ID
- 流量标志 Rx
- 流量标志 Tx
- HTTP 内容类型
- HTTP 域名
- HTTP 请求授权
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP 请求主机
- HTTP 请求方法
- HTTP Rq Rcv FB
- HTTP Req Rcv LB
- HTTP Req 引用
- HTTP 请求 URL
- HTTP Req XForwarded For
- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP 资产位置
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp 状态
- HTTP 事务结束时间
- HTTP 事务 ID
- IC Cont Gp 名称
- IC 标志
- IC 没有商店标志

- IC 策略名称
- 入口接口客户端
- NetScaler Gateway Service 应用程序 ID
- NetScaler Gateway Service 应用程序名称
- NetScaler Gateway Service 应用程序类型
- NetScaler 分区 ID
- 观察域 ID
- 观察点 ID
- 起源资源状态
- 原产地 Rsp Len
- 协议标识符
- 速率限制标识符名称
- 记录类型
- 响应程序操作类型
- 响应媒体类型
- Srv Flow 标志 Rx
- Srv Flow 标志 Tx
- srvr 快速 Rex 计数
- 服务器 TCP 抖动
- 服务器 TCP 数据包已重新传输
- 服务器 TCP 恢复计数
- 服务器 TCP 零窗口计数
- SSL 密码值 BE
- SSL 密码值 FE
- SSL 客户端证书大小 BE
- SSL 客户端证书大小 FE
- SSL 客户端证书签名哈希 BE
- SSL Cnt 证书签名哈希 FE
- SSL Err 应用程序名称

- SSL 错误标志
- SSL 标志 BE
- SSL 标志 FE
- SSL 握手错误消息
- SSL 服务器证书大小 BE
- SSL 服务器证书大小 FE
- SSL 会话 ID BE
- SSL 会话 ID FE
- SSL Sig 哈希算法 BE
- SSL Sig 哈希算法 FE
- SSL 服务器证书签名哈希 BE
- SSL 服务器证书签名哈希 FE
- SSL iDomain 类别
- SSL iDomain 类别组
- SSL iDomain 名称
- SSL iDomain 声誉
- SSL iExecuted 操作
- SSL iPolicy 操作
- SSL iReason 采取行动
- SSL iURL 集已匹配
- SSL iURL 设置为私有
- 订户标识符
- Svr Tcp 标志 Rx
- Svr Tcp 标志 Tx
- 租户姓名
- 跟踪请求父跨度 ID
- 跟踪请求跨度 ID
- 跟踪跟踪 ID
- Trans Ct Dst IPv4 地址

- 事务客户端目标 IPv6 地址
- 事务客户端目标端口
- Trans Ct Flow 最终使用 Rx
- Trans Clt Flow End Usec Tx
- Trans Ct Flow 开始使用 Rx
- Trans Clt Flow Start Usec Tx
- Trans Clr IPv4 地址
- Trans Clr IPv6 地址
- Trans Ct 数据包 Tt Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- 事务客户端 RTT
- Trans Clr Ssc 端口
- Trans Ct Tt Rx Oct Cnt
- Trans Ct Tt Tx Oct Cnt
- Trans Info
- Trans Srv Dst 端口
- Trans srv 数据包 Tt Cnt Rx
- Trans Srv 数据包 Tt Cnt Tx
- Trans Srv Src 端口
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- 事务服务器 RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- 事务 ID
- URL 类别
- URL 类别组

- URL 类别声誉
- URL 类别操作原因
- URL 集已匹配
- URL 设置为私人
- URL 对象 ID
- VLAN 编号

Citrix Virtual Apps and Desktops 和 **Citrix DaaS** 日志

Citrix Virtual Apps and Desktops 和 Citrix DaaS 日志包含以下数据点：

- 应用程序名称
- 浏览器
- 客户 ID
- 详细信息：格式大小、格式类型、启动器、结果
- 设备 ID
- 设备类型
- 反馈
- 反馈 ID
- 文件名
- 文件路径
- 文件大小
- 就像
- 越狱
- 作业详细信息：文件名、格式、大小
- 位置：估计、纬度、经度

  > 注意
  >
  > 位置信息是在城市和国家/地区级别提供的，并不代表精确的地理位置。

- 长 CMD 线
- 模块文件路径
- 操作

- 操作系统
- 平台额外信息
- 打印机名称
- 问题
- 问题 ID
- SaaS 应用程序名称
- 会话域
- 会话服务器名称
- 会话用户名
- 会话 GUID
- 时间戳
- 时区：Bias、DST、名称
- 打印的总份数
- 打印的总页数
- 类型
- URL
- 用户代理

Citrix ADC 日志

Citrix ADC 日志包含以下数据点：

- 集装箱
- 文件
- 格式
- 类型

Citrix DaaS Standard for Azure 日志

适用于 Azure 的 Citrix DaaS 标准日志包含以下数据点：

- 应用程序名称
- 浏览器

- 详细信息：格式大小、格式类型、启动器、结果
- 设备 ID
- 设备类型
- 文件名
- 文件路径
- 文件大小
- 越狱
- 作业详细信息：文件名、格式、大小
- 位置：估计、纬度、经度

  > 注意
  >
  > 位置信息是在城市和国家/地区级别提供的，并不代表精确的地理位置。

- 长 CMD 线
- 模块文件路径
- 操作
- 操作系统
- 平台额外信息
- 打印机名称
- SaaS 应用程序名称
- 会话域
- 会话服务器名称
- 会话用户名
- 会话 GUID
- 时间戳
- 时区：Bias、DST、名称
- 类型
- URL
- 用户代理

Citrix 身份提供程序日志

- 用户登录：
  - Authentication Domains: Name, Product, IdP Type, IdP Display Name
    - IdP Properties: App, Auth Type, Customer Id, Client Id, Directory, Issuer, Logo, Resources, TID
    - 扩展程序：
      - Workspace: Background Color, Header Logo, Logon Logo, Link Color, Text Color, StoreFront Domains
      - ShareFile: Customer Id, Customer Geo
      - Long Lived Token: Enabled, Expiry Type, Absolute Expiry Seconds, Sliding Expiry Seconds
  - Authentication Result: User Name, Error Message
  - Sign-in Message: Client Id, Client Name
  - User Claim: AMR, Access Token Hash, Aud, Auth Time, CIP Cred, Auth Alias, Auth Domains, Groups, Product, System Aliases, Email, Email Verified, Exp, Family Name, Given Name, IAT, IdP, ISS, Locale, Name, NBF, SID, Sub
    - Auth Alias Claims: Name, Value
    - Directory Context: Domain, Forrest, Identity Provider, Tenant Id
    - User: Customers, Email, OID, SID, UPN
    - IdP Extra Fields: Azure AD OID, Azure AD TID
- User Logoff: Client Id, Client Name, Nonce, Sub
- Client Update: Action, Client Id, Client Name

Citrix Gateway 日志

- 交易事件：
  - ICA App: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module

Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App

- ICA Event: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
- ICA Update: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes
- AppFlow Config: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5

- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID
- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert

Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- 指标事件：
  - VServer LB: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
  - CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
  - Server Service Group: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot

Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions

- Server SVC CFG: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

- Memory Pool: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Monitoring Service Binding: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes
- Interface: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets
- VServer CS: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

安全浏览器日志

- 申请帖子：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- 应用程序删除：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- 应用程序更新：
  - Logs before the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Logs after the published application: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- 权利创建：
  - Logs before the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
  - Logs after the entitlement creation: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type
- 权利更新：
  - Logs before the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

  - Logs after the entitlement update: Approved, Customer Id, Data Retention Days, End Date, Grace Period Days, Session Id, Product SKU, Quantity, Serial Numbers, Start Date, State, Type

- Session Access Host: Accept Host, Client IP, Date Time, Host, Session, User Name
- 会话连接：
  - Logs before the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session connection: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- 会话启动:
  - Logs before the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session launch: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- 会话勾号：
  - Logs before the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Logs after the session tick: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

Microsoft Graph 安全性日志

- 租户 ID
- 用户 ID
- 指标 ID
- 指标 UUID
- 事件时间
- 创建时间
- 警报类别
- 登录位置
- 登录 IP
- 登录类型

- 用户帐户类型
- 供应商信息
- 厂商提供商信息
- 漏洞状态
- 漏洞严重性

Microsoft Active Directory 日志

- 租户 ID
- 收集时间
- 类型
- 目录上下文
- 组
- 身份
- 用户类型
- 帐户名称
- 密码计数错误
- 城市
- 普通名
- 公司
- 国家/地区
- 密码到期前的天数
- 部门
- 说明
- 显示名称
- 唯一判别名
- 电子邮件
- 传真号码
- 名字
- 组类别

- 组范围
- 家庭电话
- 首字母缩写
- IP 电话
- 帐户是否已启用
- 帐户被锁定了
- 是安全组
- 姓氏
- 经理
- 的成员
- 移动电话
- 寻呼机
- 密码永不过期
- 实物配送办公室名称
- 邮局信箱
- 邮政编码
- 主要组 ID
- 状态
- 街道地址
- 标题
- 用户帐户控制
- 用户组列表
- 用户主体名称
- 工作电话

Citrix Analytics for Performance 日志

- actionid
- actionreason
- actiontype

- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath
- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent

- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress
- clientname
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted

- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason
- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype

- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate
- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate

- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress
- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent

- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex
- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocol
- provisioningschemeid
- provisioningtype

- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure
- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username

- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate
- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

技术安全性概述

April 12, 2024

Citrix Cloud 中托管的分析服务可收集 Citrix 产品组合产品和第三方产品中的数据。这些产品称为数据源。Citrix Analytics 同时支持云和本地数据源。本文档中的信息适用于 Citrix Analytics 及其数据源。

数据流

Citrix Analytics 会自动发现订阅给客户的 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，在 Citrix Analytics 发现站点之前，您必须将您的 Citrix Virtual Apps and Desktops 站点添加到 Citrix Workspace。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 的详细信息，请参阅 在 Citrix 数据源上启用分析。

您可以将一些第三方产品（例如 Microsoft Graph Security 和 Microsoft Active Directory）与 Citrix Analytics 集成在一起。有关详细信息，请参阅以下主题：

- 在 Microsoft Graph 安全上启用分析
- 将 Analytics 与 Microsoft Active Directory 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 环境中部署和配置适用于 **Spunk** 的 **Citrix Analytics** 加载项。有关更多信息，请参阅 Splunk 集成。

未经客户同意，Citrix Analytics 不会处理从数据源接收的任何事件。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 收集、存储和保留数据的更多信息，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 互联网连接要求。
- **Citrix Analytics** 要求：在使用 Citrix Analytics 之前，请检查系统要求。除了 Citrix Cloud 要求外，还必须通过 HTTPS 端口 443 访问以下终端节点地址才能使用 Citrix Analytics 服务。

端点	美国地区	欧盟区域	亚太南部地区
管理员 UI	https://analytics.cloud.com/	https://analytics-eu.cloud.com/	https://analytics-aps.cloud.com/
管理员用户界面 (CDN)	https://cas-api-cdn-ep.azureedge.net/	https://cas-api-cdn-ep-eu.azureedge.net/	https://cas-api-cdn-ep-aps.azureedge.net/
API 服务	https://api.analytics.cloud.com/	https://api.analytics-eu.cloud.com/	https://api.analytics-aps.cloud.com/
API 服务 (Performance Analytics)	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/		

端点	美国地区	欧盟区域	亚太南部地区
事件中心（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/
批量上载	https://casstoragebulk.blob.core.windows.net/	https://casstorebulkeu.blob.core.windows.net/	https://casstorebulkaps.blob.core.windows.net/

> 注意
>
> Citrix Analytics 已停止对上述大多数终端节点的 TLS 1.0 和 TLS 1.1 的支持。

- **Citrix Cloud Connector** 安装：某些数据源，例如 Citrix Endpoint Management、Citrix Virtual Apps and Desktops 以及 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，必须配置 Web 代理设置。有关详细信息，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 与安全信息和事件管理 (SIEM) 集成，请确保以下端点位于网络的允许列表中：

端点	美国地区	欧盟区域	亚太南部地区
Kafka 代理	casnb-0.citrix.com:9094 casnb-1.citrix.com:9094 casnb-2.citrix.com:9094 casnb-3.citrix.com:9094	casnb-eu-0.citrix.com:9094 casnb-eu-1.citrix.com:9094 casnb-eu-2.citrix.com:9094	casnb-aps-0.citrix.com:9094 casnb-aps-1.citrix.com:9094 casnb-aps-2.citrix.com:9094

身份识别和访问管理

- 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您的 Citrix Cloud 帐户中的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商。
- 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，以便在企业中管理 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、欧盟和亚太南部区域。存储位置取决于 Citrix Cloud 管理员在将其组织载入到 Citrix Cloud 时选择的主区域。有关详细信息，请参阅以下主题：

- 地理方面的注意事项
- 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 授权并且 Analytics 管理员已为每个订阅的数据源明确启用数据处理时，才会处理收到的数据。

Citrix Analytics 使用以下安全措施保护客户的数据：

- 面向分析用户的 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实施的基于租户的数据访问控制。
- 在数据湖和数据仓库中的所有数据存储中，每个客户或租户都能实现强大的数据隔离。
- 在各种微服务和数据存储之间进行 TLS 加密的数据传输，适用于平台和平台内的公共端点（APT/输入/输出）。
- TLS 端点的高标准。TLS 1.0 和 TLS 1.1 被禁用。
- 使用存储在相应密钥保管库中的加密密钥和密钥进行加密的数据存储。
- 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。
- 与 Azure 安全中心一起使用的漏洞扫描、入侵检测、反恶意软件、rootkit 扫描。

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)。有关详细信息，请参阅以下协议：

- 用户协议
- Citrix 隐私政策
- Citrix 数据处理协议

- Citrix Services Security Exhibit
- 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 负责保护驻留在托管 Citrix Analytics 的 Citrix 管理的云环境中的所有基础架构和数据的安全。Citrix 负责在云环境中定期应用软件更新和修补程序，以解决安全漏洞。

客户责任

Citrix 客户负责保护其数据源、策略执行点以及与 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 Gateway、Citrix Virtual Apps and Desktops、Microsoft Active Directory
  - **SIEM**：Splunk 和任何其他使用 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。
- 客户提供的管理员凭据，用于部署和集成代理，例如 Citrix ADM 代理。必须限制对这些代理的访问，因为它们会在本地存储密钥以与 Citrix Analytics 进行通信。
- Citrix Analytics 生成的用于配置适用于 **Splunk** 的 **Citrix Analytics** 的凭据。
- 在 Windows、Mac、Android、iOS 上运行的最终用户设备可以连接到 Citrix Cloud 或 Citrix Workspace 并与数据源集成。

有关安全规定的更多信息，请参阅以下文档：

- 适用于 Citrix Cloud 平台的安全部署指南
- Citrix Workspace 文档
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的技术安全概述
- Citrix Virtual Apps and Desktops 安全注意事项
- 保护您的 StoreFront 部署文档
- Citrix Endpoint Management 的技术安全概述

- Citrix Secure Private Access 服务文档
- Citrix ADC 的安全部署指南
- Citrix ADM 系统要求

系统要求

September 25, 2023

在开始使用 Citrix Analytics 之前，必须查看许可证信息、软件要求和浏览器要求。

Citrix Analytics 订阅

您必须拥有有效的订阅才能使用以下 Analytics 产品：

- Citrix Analytics for Security
- Citrix Analytics for Performance

有关详细信息，请参阅 Citrix Cloud 服务。

数据源要求

数据源是向 Citrix Analytics 发送事件的产品。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，查看每种产品支持的数据源：

- 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，您的工作站必须具有以下受支持的网络浏览器：

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

管理 **Citrix Analytics** 的管理员角色

May 8, 2023

默认情况下，Citrix Cloud 管理员对其 Citrix Cloud 帐户上的所有订阅服务具有完全访问权限。通过完全访问权限，管理员可以使用已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使用您的 Citrix Cloud 帐户来管理组织的订阅服务。然后，您可以定义其访问权限，并允许他们管理已订阅服务中的特定功能。

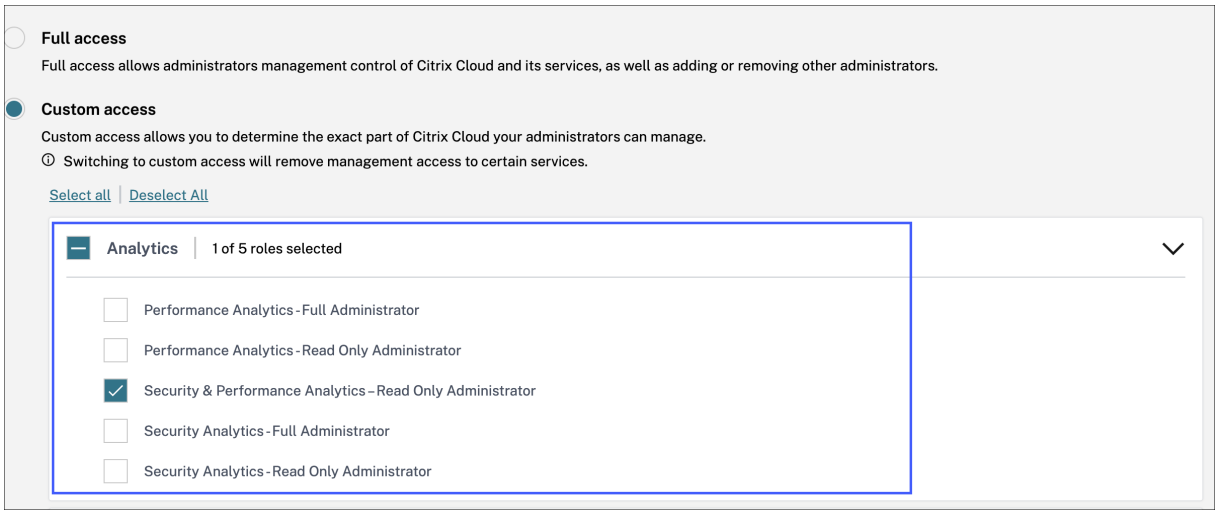
可以通过两种方式添加新管理员：

1. 分别作为来自 Citrix Identity 和 Azure AD/Active Directory 的用户。有关更多信息，请参阅 管理 Citrix Cloud 管理员。
2. 在 Azure Active Directory 中使用组。有关详细信息，请参阅管理管理员组。

管理员可以使用他们的 Citrix Cloud、Active Directory 或 Azure Active Directory 帐户登录 Citrix Cloud，并根据自己的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-完全权限管理员	向性能分析的 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性能分析的 Citrix Cloud 管理员。
安全与性能分析-只读管理员	为安全分析和性能分析的 Citrix Cloud 管理员分配只读访问权限。
安全分析-完全权限管理员	向安全分析的 Citrix Cloud 管理员分配完全访问权限。
Security Analytics - 只读管理员	向安全分析的 Citrix Cloud 管理员分配只读访问权限。



> 备注
>
> - 如果为管理员选择了多个角色，则具有较高访问权限的角色将生效。
> - 如果用户直接以用户身份通过 Azure Active Directory 组获得访问权限，则单独授予该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。
> - 具有先前可用的“只读管理员”角色的管理员 将重命名为“安全与性能-只读管理员”。
> - 具有安全和性能分析 - 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/服务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 Security Analytics 的管理员角色

快速入门

April 12, 2024

本文档介绍了如何首次开始使用 Citrix Analytics。

步骤 **1**：登录到 **Citrix Cloud**

要使用 Citrix Analytics，您必须拥有 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 Citrix Cloud 帐户或加入组织中其他人创建的现有帐户。有关如何继续的详细过程和说明，请参阅 注册 Citrix Cloud。

步骤 **2**：获取对分析的访问权限

您可以通过以下方式之一访问 Analytics：

- 申请 **Citrix Analytics** 产品试用。登录 Citrix Cloud 后，在“可用服务”部分的“分析”磁贴上，单击“管理”以查看“分析”概述页面。

  概述页面显示 Analytics 产品 - **Security** 和 **Performance**。

  - 对于安全分析和性能分析，请单击“申请试用”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，您会收到一封电子邮件。您最多可以使用 60 天的试用期。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，“分析”磁贴将移至“我的服务”部分。

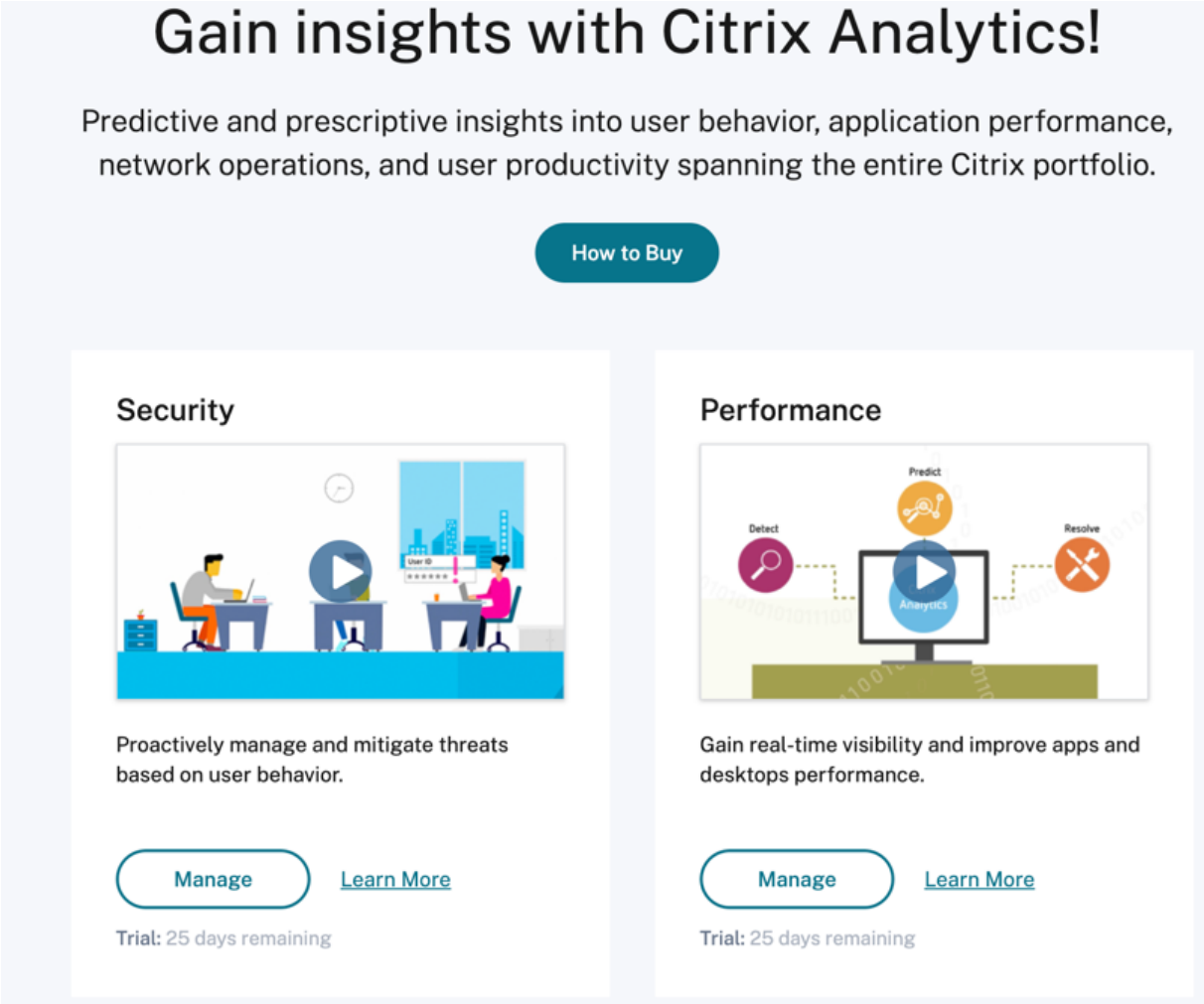
- 订阅 **Citrix Analytics**。您可以购买以下 Citrix Analytics 订阅：

  - Citrix Analytics for Security
  - Citrix Analytics for Performance
  - Citrix Analytics for Security 和 Citrix Analytics for Performance

  Citrix Analytics for Security 和 Citrix Analytics for Performance 作为附加服务提供，包括 Citrix Workspace Standard、Workspace Premium 和 Workspace Premium Plus。有关详细信息，请参阅 Citrix Cloud 服务。

步骤 **3**：管理 **Analytics**

对于安全分析和性能分析，在您获得必要的订阅或授权访问试用版后，在 Analytics 概述页面上，该产品的“申请试用”按钮将更改为“管理”。单击“管理”可查看与每个产品对应的用户控制面板。



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-**Security** 或 **Performance**.。

有关每个 Analytics 产品的更多信息，请参阅

- Citrix Analytics for Security
- Citrix Analytics for Performance

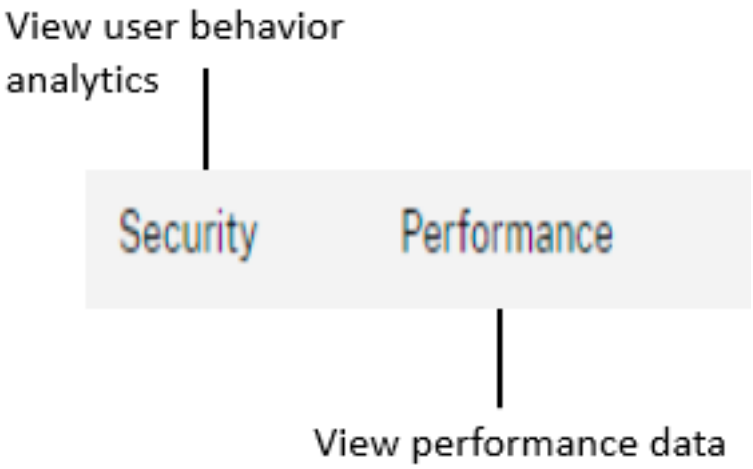
探索方法

May 7, 2022

熟悉 Analytics 用户界面上的主要控件。

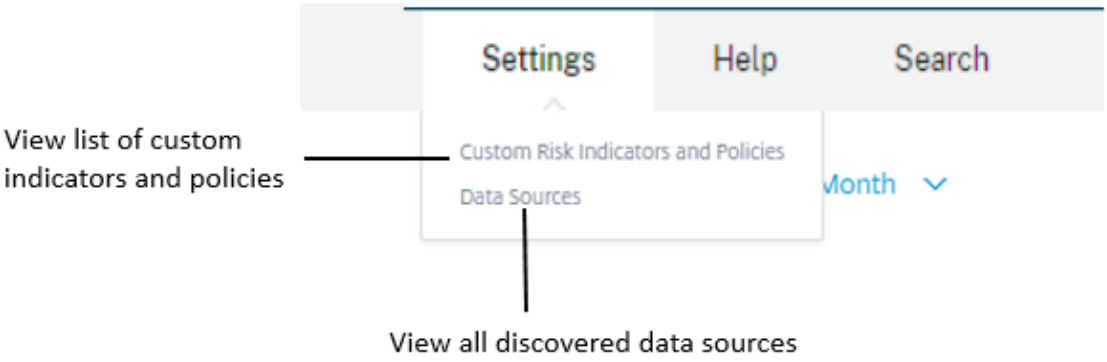
顶栏

从顶部栏导航到各种 Analytics 产品。

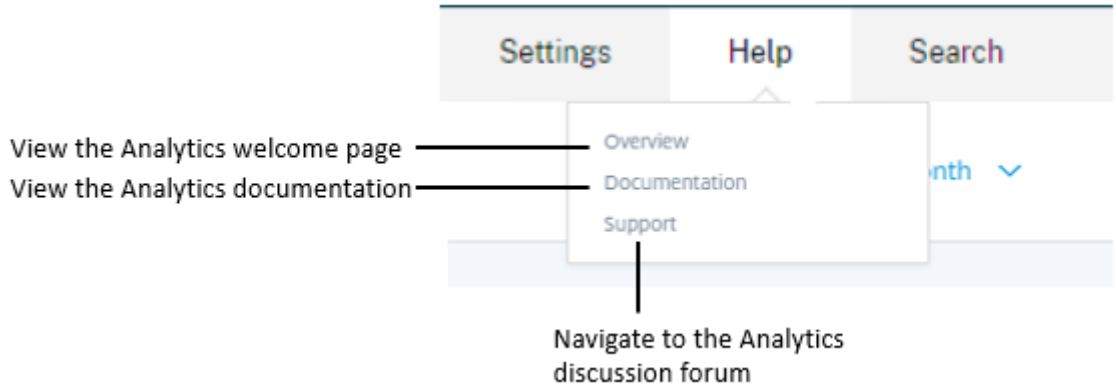


设置菜单

从“设置”菜单中，导航到“指标和策略”页面或“数据源”页面。

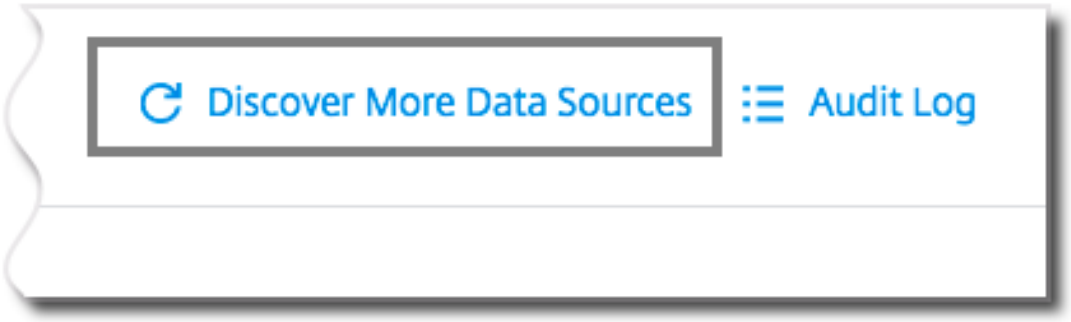


“帮助”菜单



了解更多信息数据源

发现新添加的数据源或以前删除的数据源。



审核日志

导航到“审核日志”页面，其中列出了在 Analytics 上生成的所有事件。

自助搜索

December 7, 2023

什么是自助搜索

自助搜索功能使您能够查找和筛选从数据源接收的用户事件。您可以探索底层用户事件及其属性。这些事件可帮助您识别任何数据问题并进行故障排除。搜索页面显示数据源的各个方面（维度）和量度。您可以定义搜索查询并应用筛选器来查看符合定义条件的事件。默认情况下，自助搜索页面显示最近一天的用户事件。

目前，自助搜索功能可用于以下数据源：

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- 应用程序和桌面
- 性能用户、计算机和会话

此外，您还可以对符合定义策略的事件执行自助搜索。有关详细信息，请参阅面向策略的自助搜索。

如何访问自助搜索

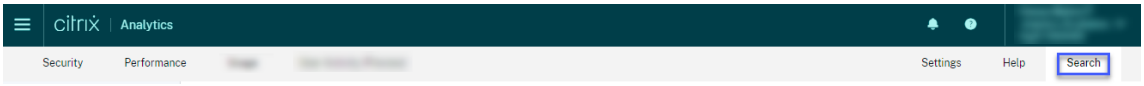
您可以使用以下选项访问自助搜索：

- 顶栏：单击顶栏中的 搜索 可查看所选数据源的所有用户事件。
- 用户个人资料页面上的风险时间表：单击 事件搜索 可查看相应用户的事件。

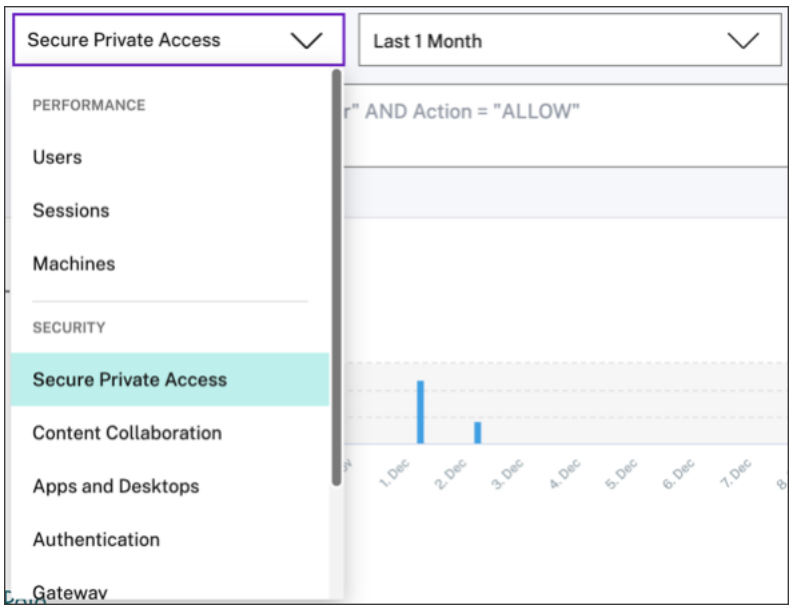
从顶部栏进行自助搜索

使用此选项可从用户界面中的任何位置转到自助搜索页面。

1. 单击 搜索 以查看自助服务页面。



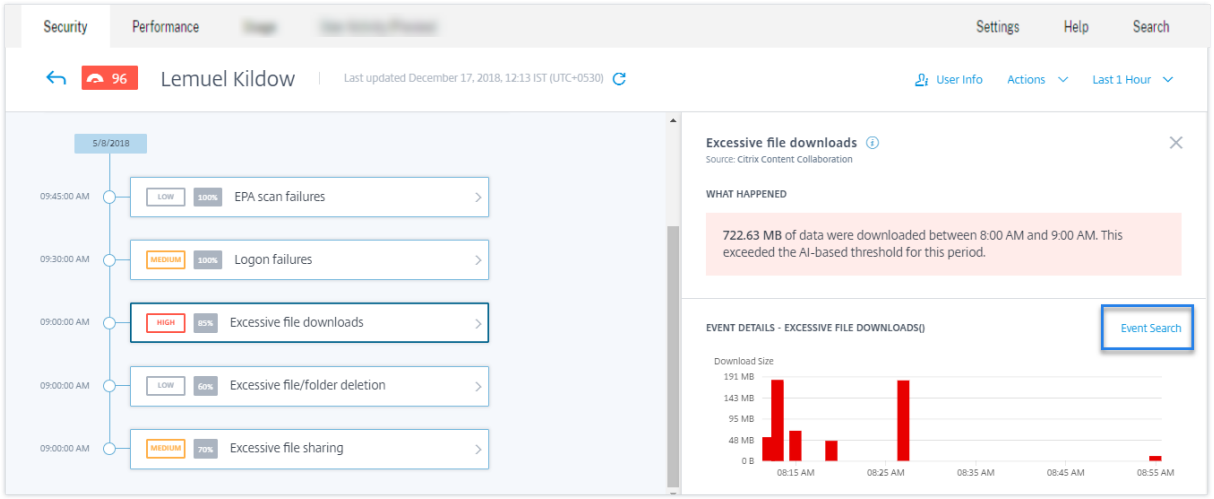
2. 选择数据源和时间段以查看相应的事件。



从用户的风险时间表进行自助搜索

如果要查看与风险指示器关联的用户事件，请使用此选项。

当您从用户的时间轴中选择风险指示器时，风险指示器信息部分将显示在右侧窗格中。单击 事件搜索 可在自助搜索页面上浏览与用户和数据源关联的事件（为其触发风险指示器）。



有关用户风险时间表的更多信息，请参阅 风险时间表。

如何使用自助搜索

使用自助搜索页面上的以下功能：

- 用于过滤事件的 Facets 。
- 用于输入查询和筛选事件的搜 索框。
- 用于选择时间 段的时间选择器。
- 查看事件图表的时间轴详细信息 。
- 用于查看事件的事件数据 。
- 导出为 CSV 格式 ，将搜索事件下载为 CSV 文件。
- 导出可视摘要 以下载搜索查询的可视摘要报告。
- 多列排序 ，按多列对事件进行排序。

使用 **Facets** 过滤事件

Facets 是构成事件的数据点的摘要。Facet 因数据源而异。例如，Secure Private Access 数据源的方面是信誉、操作、位置和类别组。而应用程序和桌面的方面是事件类型、域和平台。

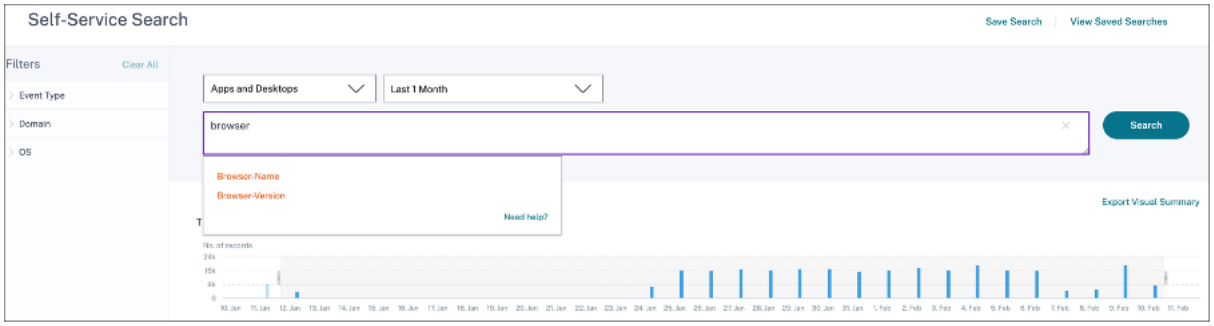
选择要过滤搜索结果的平面。选定的小平面显示为筹码。

有关与每个数据源相对应的方面的详细信息，请参阅本文前面提到的数据源的自助搜索文章。

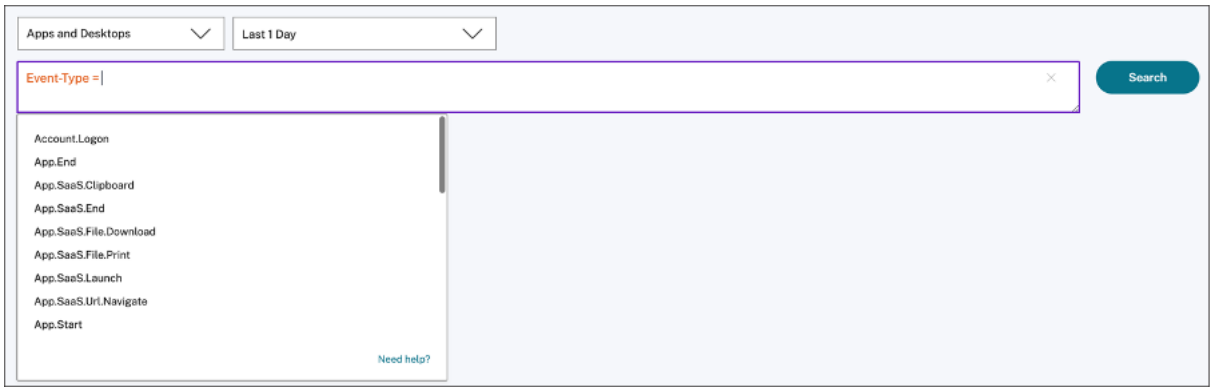
使用搜索框中的搜索查询过滤事件

将光标置于搜索框中时，搜索框会根据用户事件显示维度列表。这些维度因数据源而异。使用维度和有效 运算符 定义搜索条件并搜索所需的事件。

例如，在应用程序和桌面的自助搜索中，您将获得维度 `Browser` 的以下值。使用维度键入查询，选择时间段，然后单击 搜索。



当选择某些维度（例如 `Event-Type` 和 `Clipboard-Operation` 以及有效的运算符）时，维度的值会自动显示。您可以从建议的选项中选择一个值，也可以根据需要输入一个新值。



搜索查询中支持的运算符　在搜索查询中使用以下运算符来优化搜索结果。

操作员	说明	示例	输出
	为搜索维度分配一个值。	用户名：John	显示用户 John 的事件。
=	为搜索维度分配一个值。	用户名 = John	显示用户 John 的事件。
~	搜索具有相似值的事件。	用户名 ~ test	显示具有相似用户名的事件。
" "	用空格分隔的值括起来。	User-Name = “John Smith”	显示用户约翰·史密斯的事件。
< >	搜索关系价值。	数据量 > 100	显示数据量大于 100 GB 的事件。

操作员	说明	示例	输出
AND	搜索指定条件为真的事件。	User-Name : John AND Data Volume > 100	显示用户 John 的事件，其中数据量大于 100 GB。
! ~	检查事件中指定的匹配模式。此 NOT LIKE 运算符返回事件字符串中任意位置不包含匹配模式的事件。	User-Name !~ John	显示除 John、John Smith 或包含匹配名称“John”的任何此类用户以外的用户的事件。
! =	检查事件是否确切指定的字符串。此 NOT EQUAL 运算符返回事件字符串中任意位置不包含确切字符串的事件。	Country != USA	显示除美国以外国家/地区的事件。
*	搜索与指定字符串匹配的事件。目前，只有以下运算符：、= 和 != 才支持 * 运算符。搜索结果区分大小写。	User-Name = John*	显示以 John 开头的所有用户名的事件。
		User-Name = *John*	显示包含 John 的所有用户名的事件。
		User-Name = *Smith	显示以 Smith 结尾的所有用户名的事件。
		用户名：John*	显示以 John 开头的所有用户名的事件。
		用户名：*John*	显示包含 John 的所有用户名的事件。
		用户名：*Smith	显示以 Smith 结尾的所有用户名的事件。
		User-Name != John*	显示不以 John 开头的所有用户名的事件。
		User-Name != *Smith	显示不以 Smith 结尾的所有用户名的事件。

操作员	说明	示例	输出
IN	为搜索维度分配多个值以获取与一个或多个值相关的事件。注意：目前，您可以将此运算符用于应用程序和桌面的以下维度：Device ID、Domain、Event-Type 和 User-Name。此运算符仅适用于字符串值。	User-Name IN (John, Kevin)	查找与约翰或凯文相关的所有事件。
NOT IN	为搜索维度分配多个值，然后查找不包含指定值的事件。注意：目前，您可以将此运算符用于应用程序和桌面的以下维度：Device ID、Domain、Event-Type 和 User-Name。此运算符仅适用于字符串值。	User-Name NOT IN (John, Kevin)	查找除 John 和 Kevin 之外的所有用户的事件。
IS EMPTY	检查维度的空值或空值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS EMPTY	查找国家名称不可用或为空（未指定）的事件。

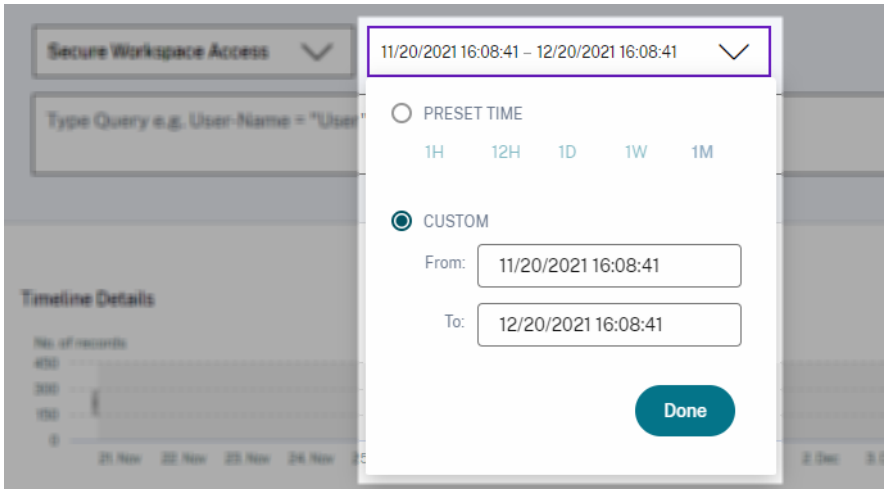
操作员	说明	示例	输出
IS NOT EMPTY	检查维度的非空值或特定值。此运算符仅适用于字符串类型的维度，例如 App-Name、Browser 和 Country。它不适用于非字符串（数字）类型的维度，例如 Upload-File-Size、Download-File-Size 和 Client-IP。	国家/地区 IS NOT EMPTY	查找可用或指定了国家/地区名称的事件。
OR	搜索其中一个或两个条件均为 true 时的值。	(User-Name = John* OR User-Name = *Smith) AND Event-Type = “Session.Logon”	显示所有以 John 开头或以 Smith 结尾的用户名的 Session.Logon 事件。

> 注意
>
> 对于 **NOT EQUAL** 运算符，在为查询中的维度输入值时，请使用自助搜索页面上提供的数据源的精确值。尺寸值区分大小写。

有关如何为数据源指定搜索查询的详细信息，请参阅本文前面提到的有关数据源的自助搜索文章。

选择查看活动的时间

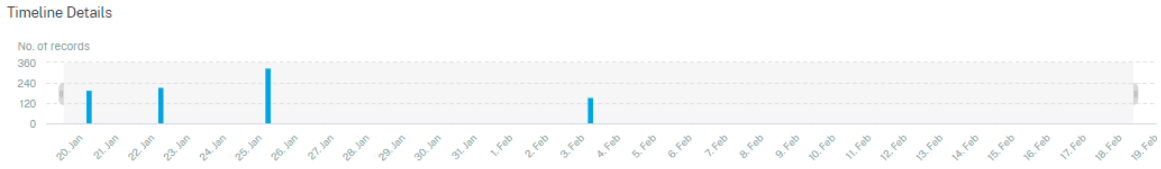
选择预设时间或输入自定义时间范围，然后单击 搜索 以查看事件。



查看时间轴详细信息

时间轴提供所选时间段内用户事件的图形表示。移动选择器栏以选择时间范围并查看与所选时间范围对应的事件。

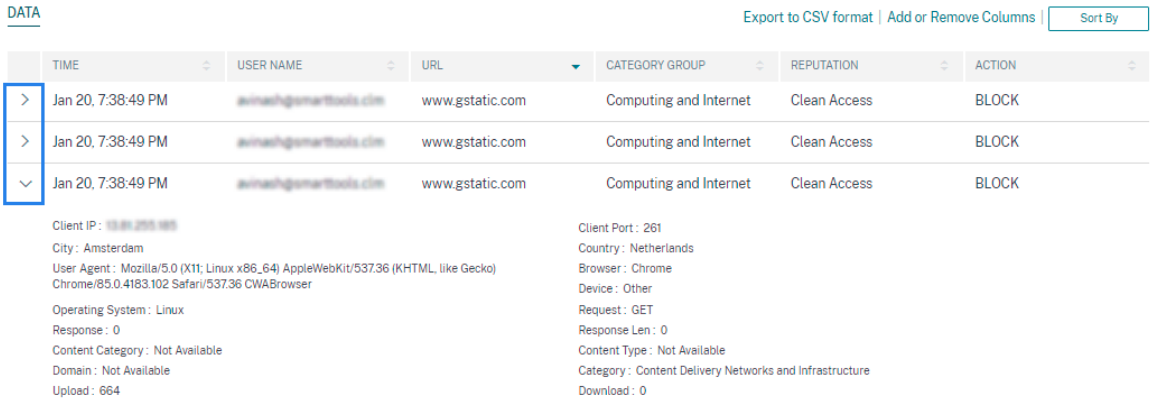
图中显示了访问数据的时间轴详细信息。



查看活动

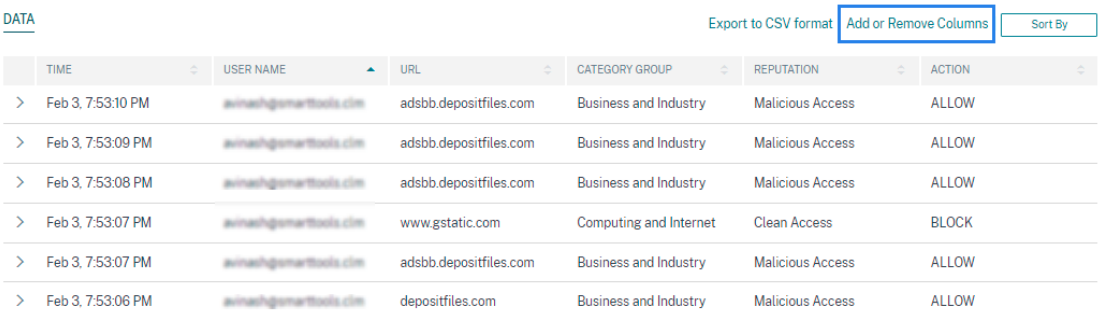
您可以查看有关用户事件的详细信息。在 **DATA** 表中，单击每列的箭头以查看用户事件详细信息。

图中显示了有关用户访问数据的详细信息。

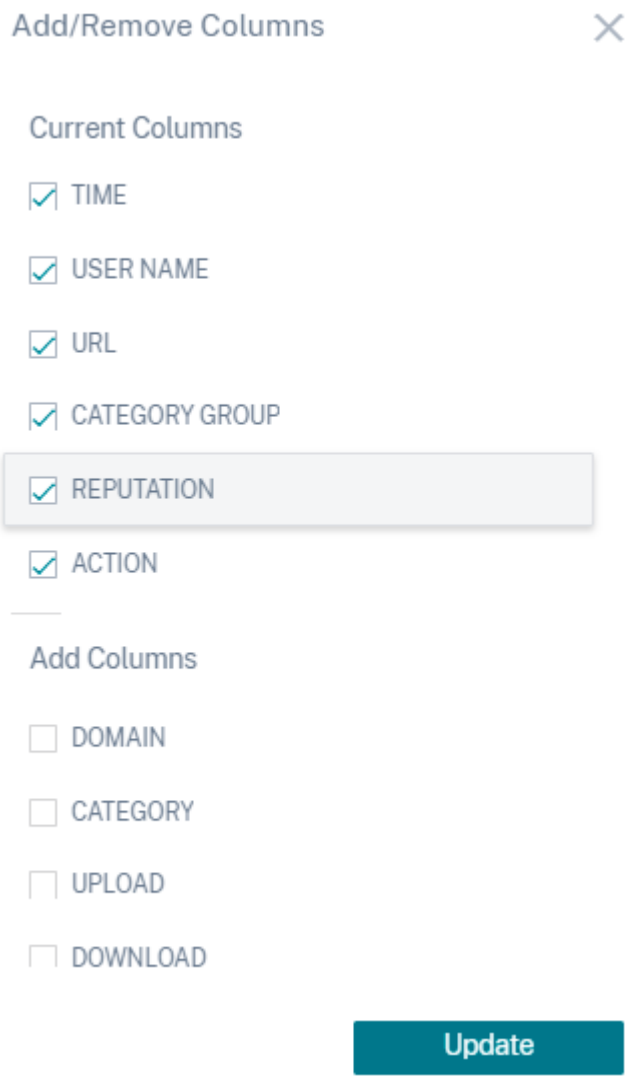


添加或删除列　您可以在事件表中添加或删除列以显示或隐藏相应的数据点。请执行以下操作：

1. 单击 添加或删除列。

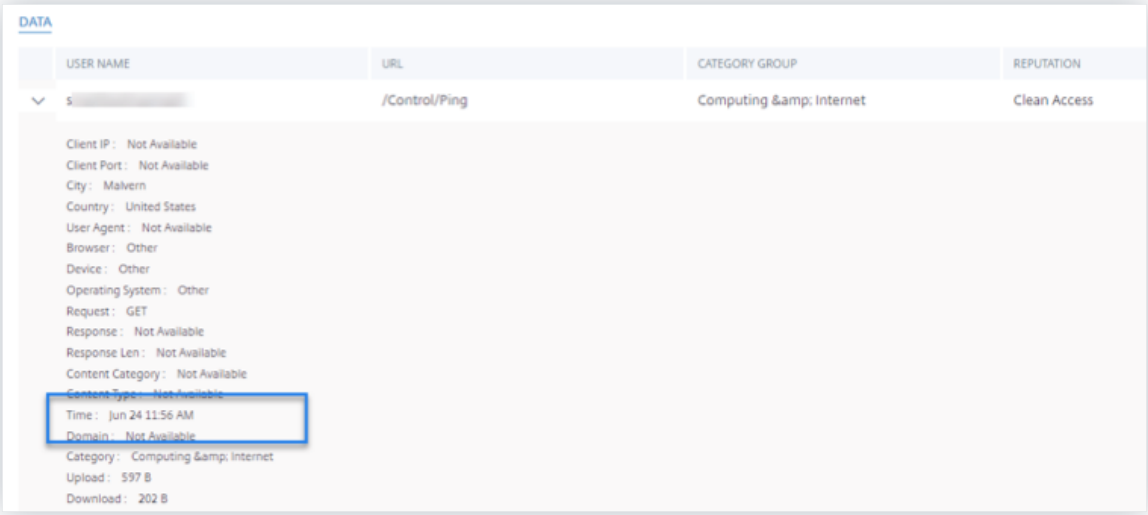


2. 从列表中选择或取消选择数据元素，然后单击“更新”。



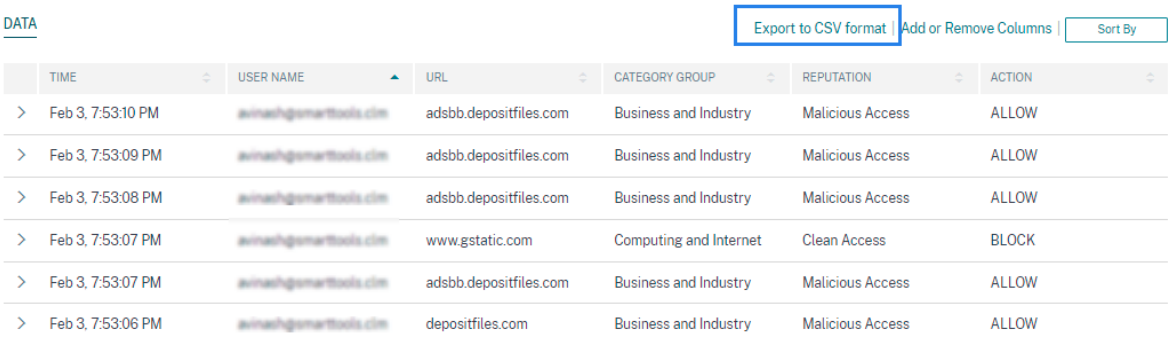
如果从列表中取消选择一个数据点，则会从事件表中删除相应的列。但是，您可以通过展开用户的事件行来查看该数据

点。例如，当您从列表中取消选择 **TIME** 数据点时，**TIME** 列将从事件表中移除。要查看时间记录，请展开用户的事件行。



将事件导出到 **CSV** 文件

将搜索结果导出为 CSV 文件并保存以供参考。单击 导出为 **CSV** 格式 以导出事件并下载生成的 CSV 文件。您可以使用导出为 **CSV** 格式功能导出 100K 行。



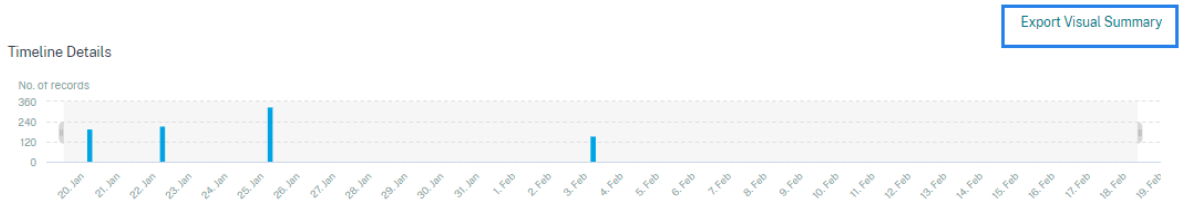
导出视觉摘要

您可以下载搜索查询的可视摘要报告，并与其他用户、管理员或管理团队共享副本。

单击 导出可视摘要 以 PDF 格式下载视觉摘要报告。该报告包含以下信息：

- 您为选定时间段内的事件指定的搜索查询。
- 在所选时间段内，您在事件上应用的方面（过滤器）。
- 可视摘要，例如时间轴图、条形图或选定时间段内搜索事件的图形。

对于数据源，只有在以条形图、时间线详细信息等视觉格式显示数据时，才能下载可视摘要报告。否则，此选项不可用。例如，您可以下载数据源的可视化摘要报表，例如应用程序和桌面、会话，您可以在其中查看时间轴详细信息和条形图的数据。对于用户和计算机等数据源，您只能看到表格格式的数据。因此，您无法下载任何视觉摘要报告。

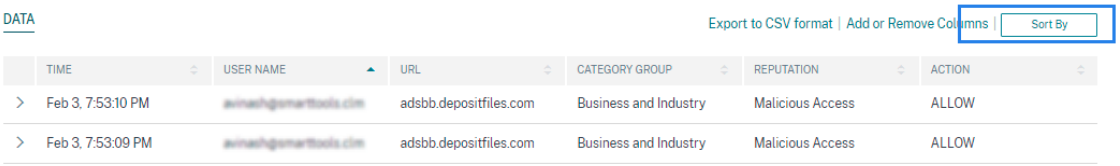


多列排序

排序有助于组织数据并提供更好的可见性。在自助搜索页面上，您可以按一列或多列对用户事件进行排序。这些列表示各种数据元素的值，例如用户名、日期和时间以及 URL。这些数据元素因选定的数据源而异。

要执行多列排序，请执行以下操作：

1. 单击“排序方式”。

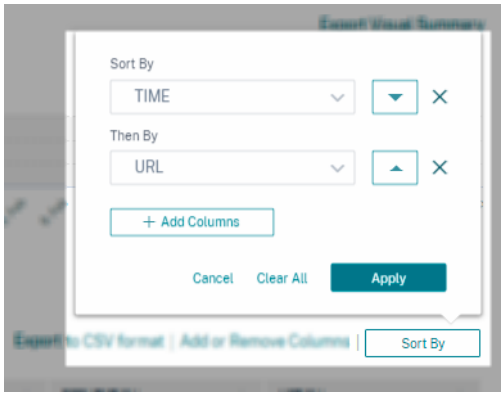


2. 从“排序方式”列表中选择一列。
3. 选择排序顺序-升序（向上箭头）或降序（向下箭头）以对列中的事件进行排序。
4. 单击 **+** 添加列。
5. 从“然后依 据”列表中选择另一列。
6. 选择排序顺序-升序（向上箭头）或降序（向下错误）以对列中的事件进行排序。

> 注意
>
> 您最多可以添加六列来执行排序。

7. 单击应用。
8. 如果不想应用上述设置，请单击“取消”。要删除所选列的值，请单击“全部清除”。

以下示例显示了对 Secure Private Access 事件的多列排序。事件按时间排序（从最新到最早的顺序），然后按 URL（按字母顺序）排序。



或者，您可以使用 **Shift** 键执行多列排序。按住 **Shift** 键并单击列标题以对用户事件进行排序。

如何保存自助搜索

作为管理员，您可以保存自助查询。此功能可节省重写经常用于分析或故障排除的查询的时间和精力。以下选项随查询一起保存：

- 应用的搜索筛选
- 选定的数据源和持续时间

执行以下操作以保存自助服务查询：

1. 选择所需的数据源和持续时间。
2. 在搜索栏中键入查询。
3. 应用所需的过滤器。
4. 单击“保存搜索”。
5. 指定用于保存自定义查询的名称。

   > 注意请
   >
   > 确保查询名称是唯一的。否则，查询不会保存。

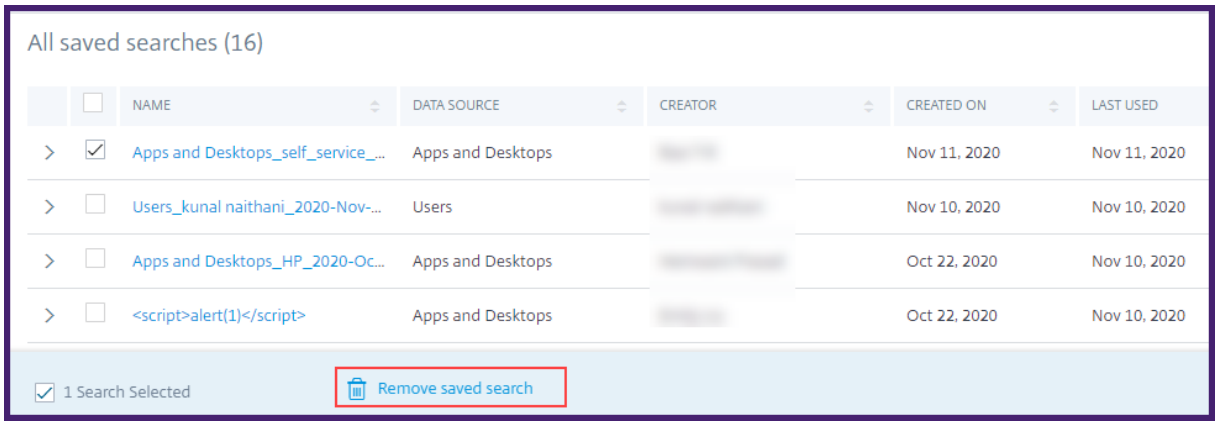
6. 如果要定期向自己和其他用户发送搜索查询报告的副本，请启用“计划电 子邮件报告”按钮。有关详细信息，请参阅为搜索查询安排电子邮件。
7. 单击保存。

要查看保存的搜索：

1. 单击查看保存的搜索。
2. 单击搜索查询的名称。

要删除已保存的搜索：

1. 单击查看保存的搜索。
2. 选择已保存的搜索查询。
3. 单击 删除保存的搜索。



要修改已保存的搜索：

1. 单击查看保存的搜索。
2. 单击已保存的搜索查询的名称。
3. 根据您的要求修改搜索查询或小平面选择。
4. 单击 更新搜索 **>** 保存 以更新和保存使用相同的搜索查询名称保存修改后的搜索。
5. 如果要使用新名称保存修改后的搜索，请单击向下箭头，然后单击 另存为新搜索 **>** 另存为。

如果用新名称替换搜索，则搜索将另存为新条目。如果在替换时保留现有搜索名称，则修改后的搜索数据将覆盖现有的搜索数据。

> 注意
>
> - 只有查询所有者可以修改或删除其保存的搜索。
> - 您可以复制保存的搜索链接地址以与其他用户共享。

为搜索查询安排电子邮件

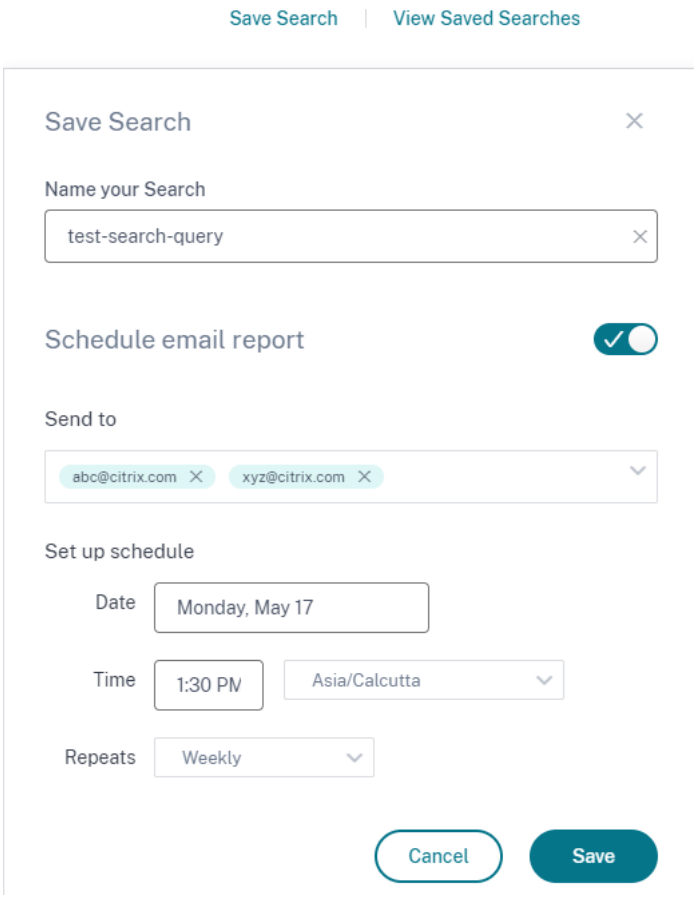
通过设置电子邮件发送计划，您可以定期向自己和其他用户发送搜索查询报告的副本。

仅当搜索查询报告包含条形图、时间线详细信息等视觉格式的数据时，此选项才可用。否则，您无法安排电子邮件发送。例如，您可以为数据源（例如应用程序和桌面、会话）安排电子邮件，在这些数据源中，您可以将数据视为时间轴详细信息和条形图。对于用户和计算机等数据源，您只能看到表格格式的数据。因此，您无法安排电子邮件。

在保存搜索查询的同时安排电子邮件

保存搜索查询时，请按如下方式设置电子邮件发送计划：

1. 在“保存搜索”对话框中，启用“计划电子邮件报告”按钮。



2. 输入或粘贴收件人的电子邮件地址。

> 注意
>
> 不支持电子邮件组。

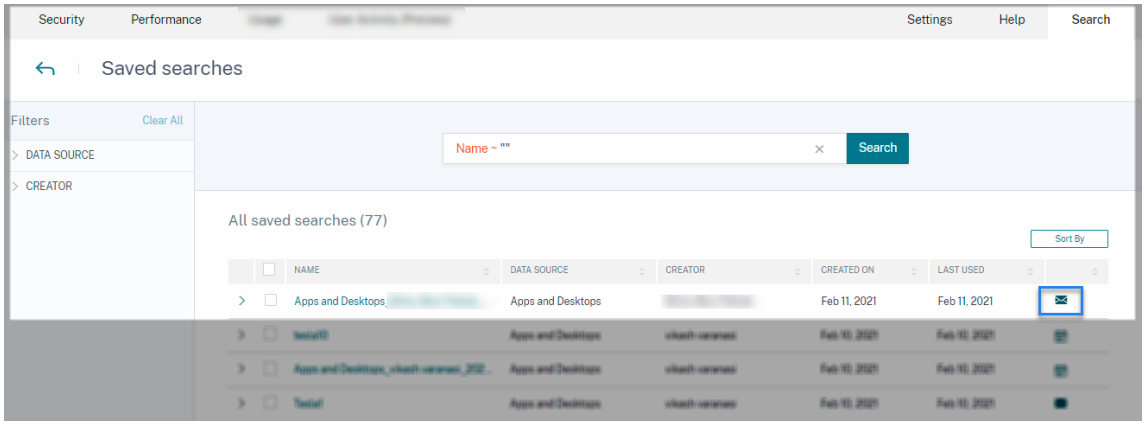
3. 设置电子邮件发送的日期和时间。
4. 选择配送频率-每天、每周或每月。
5. 单击保存。

为已保存的搜索查询安排电子邮件

如果要为之前保存的搜索查询设置电子邮件发送计划，请执行以下操作：

1. 单击查看保存的搜索。
2. 转到您创建的搜索查询。单击 电子邮件此查询 图标。

> 注意
>
> 只有查询所有者可以安排其保存的搜索查询的电子邮件发送。



3. 启用计 划电子邮件报告 按钮。
4. 输入或粘贴收件人的电子邮件地址。

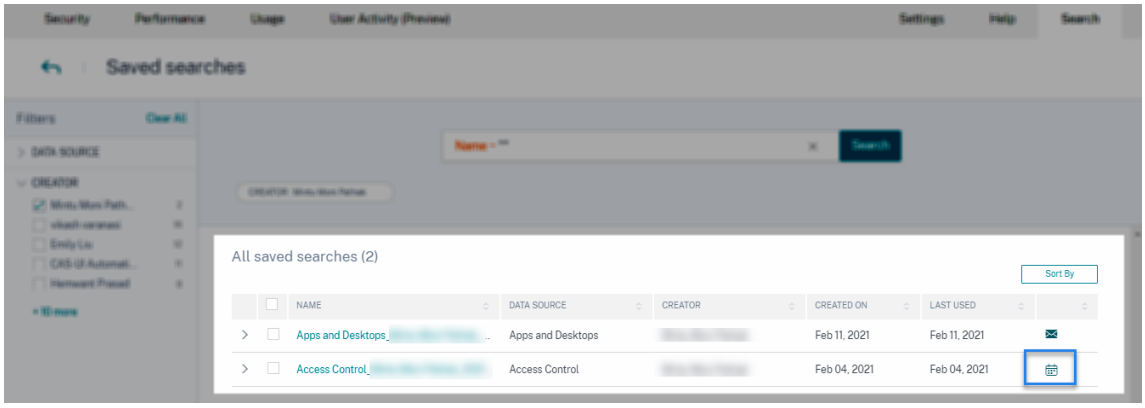
> 注意
>
> 不支持电子邮件组。

5. 设置电子邮件发送的日期和时间。
6. 选择配送频率-每天、每周或每月。
7. 单击保存。

停止搜索查询的电子邮件发送计划

1. 单击查看保存的搜索。
2. 转到您创建的搜索查询。单击查 看电子邮件发送计划 图标。

> 注意
>
> 只有查询所有者可以停止其保存的搜索查询的电子邮件计划。



3. 禁用计 划电子邮件报告 按钮。
4. 单击保存。

邮件内容

收件人会收到来自“Citrix Cloud - 通知 donotreplynotifications@citrix.com”的有关搜索查询报告的电子邮件。该报告作为 PDF 文档附件。电子邮件将按您在 计划电子邮件报告 设置中定义的定期间隔发送。

搜索查询报告包含以下信息：

- 您为选定时段内的事件指定的搜索查询。
- 您在事件上应用的方面（过滤器）。
- 视觉摘要，例如时间线图、条形图或搜索事件的图表。

完全访问权限和只读访问权限管理员的权限

- 如果您是具有完全访问权限的 Citrix Cloud 管理员，则可以使用 搜索 页面上的所有可用功能。
- 如果您是具有只读访问权限的 Citrix Cloud 管理员，则只能在 搜索 页面上执行以下活动：
  - 通过选择数据源和时间段来查看搜索结果。
  - 输入搜索查询并查看搜索结果。
  - 查看其他管理员保存的搜索结果。
  - 导出可视摘要并将搜索结果下载为 CSV 文件。

有关管理员角色的信息，请参阅 管理 Citrix Analytics 的管理员角色。

警报设置

December 7, 2023

Citrix Analytics 根据警报策略标准生成警报。您可以配置为通过电子邮件和 Webhook 接收来自 Citrix Analytics for Security and Performance 的警报通知。

- 邮件通讯组列表
- 用于警报通知的 Webhook

您可以格式化来自 Citrix Analytics for Security 的警报的电子邮件通知。

- 最终用户电子邮件设

电子邮件分发名单

December 7, 2023

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

> 重要
>
> 您可以从组织中的 Citrix Cloud 域和其他非 Citrix Cloud 域中选择管理员。

要向适当的管理员组发送通知，请使用他们的电子邮件地址创建通讯组列表。

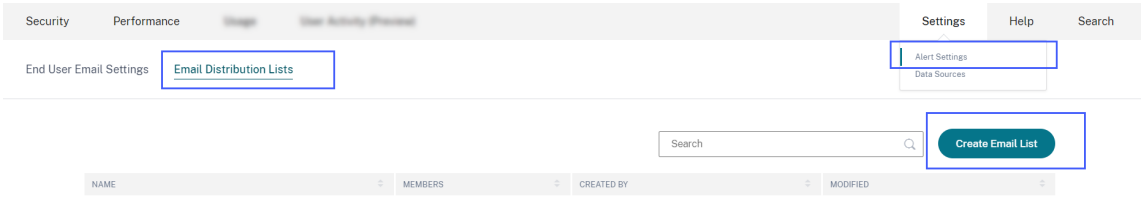
使用电子邮件通讯组列表，您可以执行以下操作：

- 创建一个包含组织中不同域的成员的通用电子邮件通讯组列表。
- 一次通知所有成员。
- 节省从不同域中选择管理员的时间和精力。
- 根据您的要求（例如添加新成员或删除现有成员）管理和维护电子邮件通讯组列表。

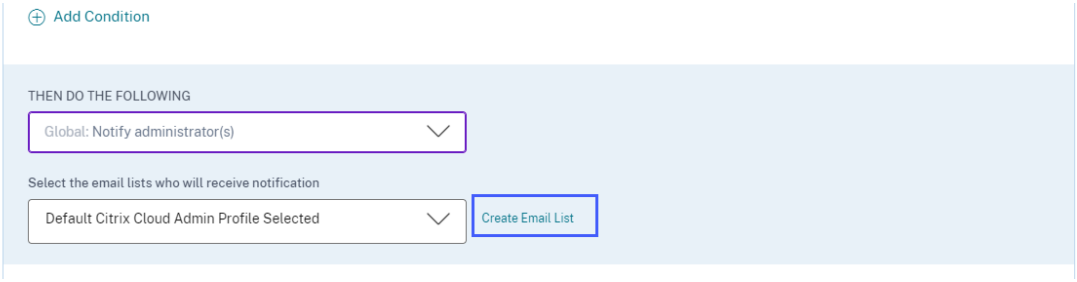
创建邮件通讯组列表

要创建电子邮件通讯组列表：

1. 单击 设置 **>** 警报设置 **>** 电子邮件分发名单 **>** 创建电子邮件列表。



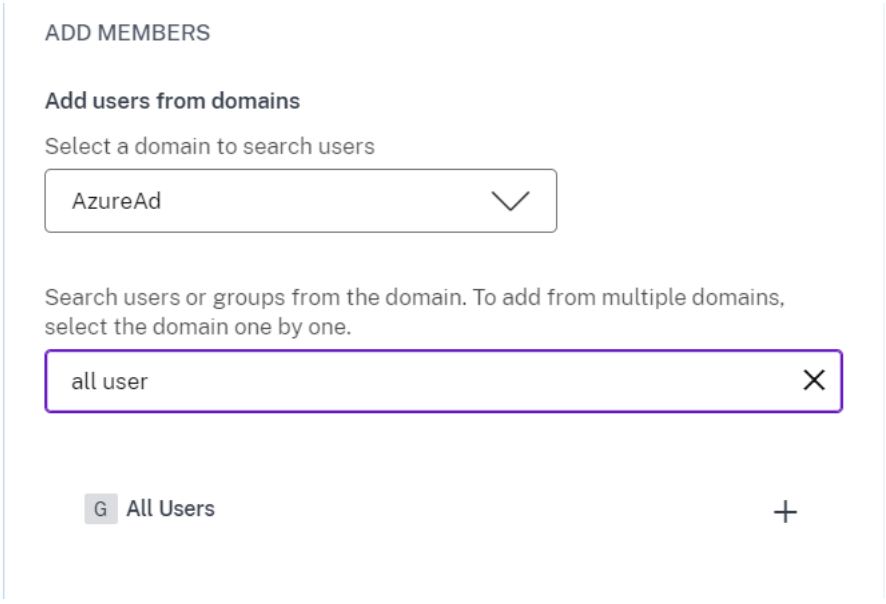
或者，您也可以根据策略创建电子邮件分发列表。修改现有策略或创建策略，然后选择 通知管理员 操作。单击创建电子邮件列表 链接。



2. 输入电子邮件通讯组列表的名称和说明以标识其用途。
3. 使用以下选项将成员添加到电子邮件通讯组列表：
   - 从域添加用户。此选项要求您的域与 Citrix Cloud 连接。
   - 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，然后搜索用户或用户组。

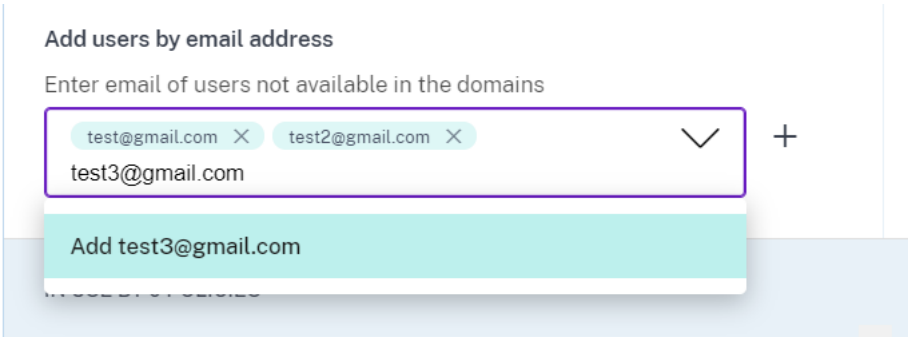
   > 注意
   >
   > 您还可以通过逐个选择域来添加来自多个域的用户和用户组。对于每个域，搜索并添加用户或用户组。

5. 单击用户或用户组旁边的 添加 图标。



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通讯组列表。

> 注意
>
> 在输入电子邮件通讯组列表之前，请确保您可以从组织的网络外部访问电子邮件通讯组列表。如果添加组织内部的电子邮件通讯组列表，则该列表的成员将无法收到来自 Citrix Analytics 的任何通知。



7. 单击 创建电子邮件列表。

查看邮件通讯组列表

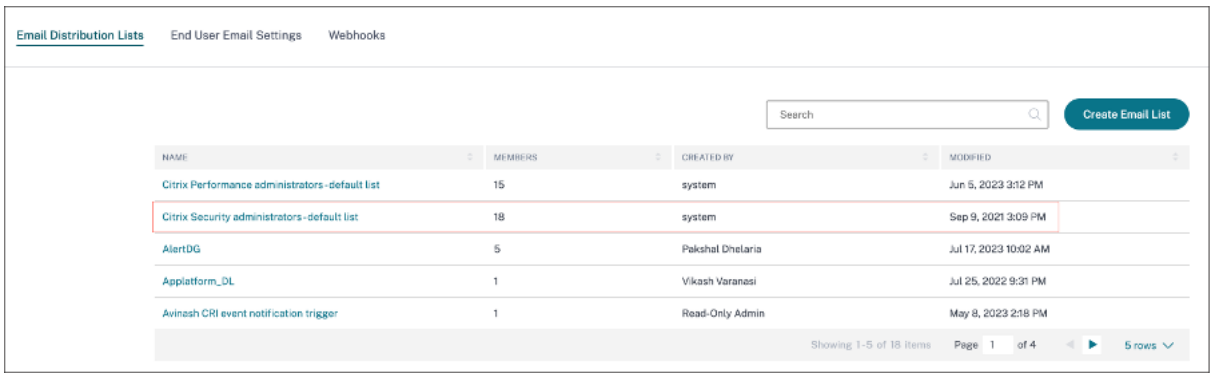
要查看电子邮件通讯组列表，请单击 设置 **>** 警报设置 **>** 电子邮件分发名单。

该页面显示在您的帐户中创建的所有电子邮件通讯组列表。选择电子邮件通讯组列表以查看成员或修改列表。

您会在帐户中看到默认创建的电子邮件通讯组列表。它包含 Citrix Cloud 管理员的 电子邮件通知 选项已在其 Citrix Cloud 帐户中启用。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 会缓存有关启用了电子邮件通知的管理员的信息。缓存每 24 小时刷新一次。因此，如果任何管理员更改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 管理员启用了电子邮件通知，他们将在 24 小时后开始接收通知，而不是立即收到通知。同样，如果 Citrix Cloud 管理员禁用电子邮件通知，他们将在 24 小时后停止接收通知。

现在，安全管理员的默认通讯组列表包括在 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。



修改电子邮件通讯组列表

要修改电子邮件通讯组列表：

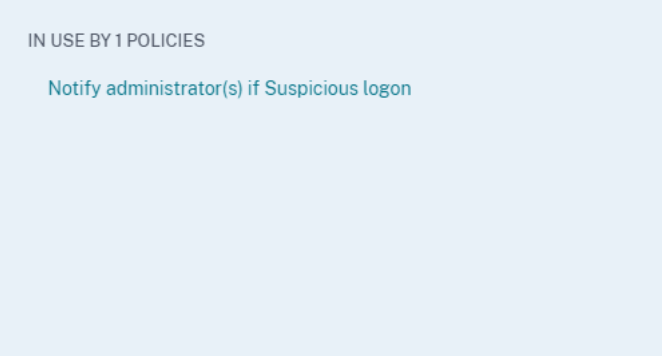
1. 单击 设置 **>** 警报设置 **>** 电子邮件通讯组列表。
2. 单击要修改的电子邮件通讯组列表。
3. 在电子邮件通讯组列表中，更新所需的详细信息，例如姓名、描述以及添加或删除成员。
4. 单击保存更改。

删除电子邮件通讯组列表

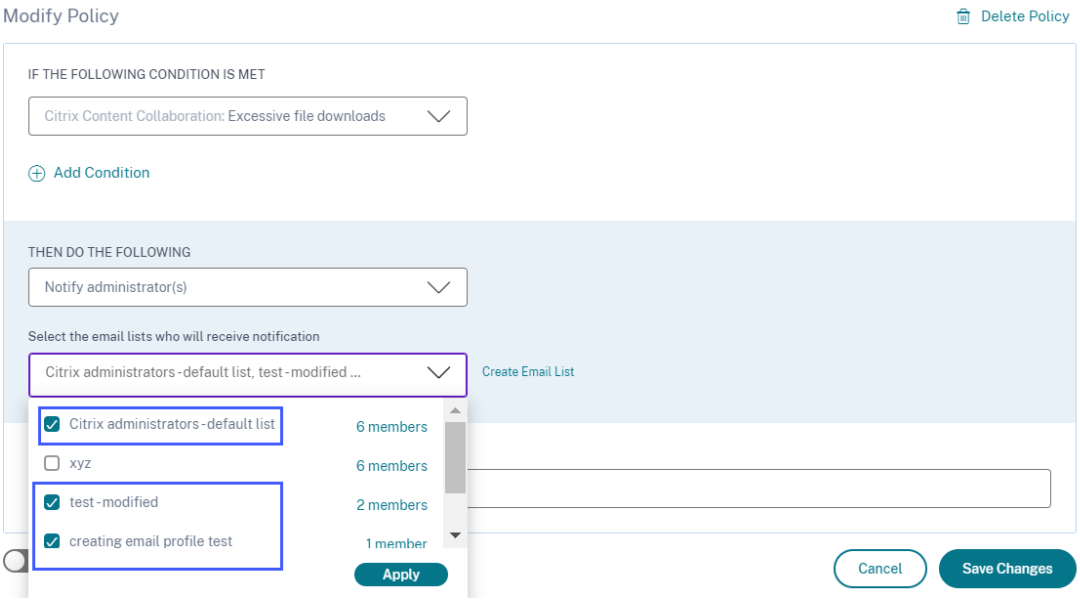
只有在未与任何策略关联的电子邮件通讯组列表时，才能删除该列表。如果它与某些策略相关联，则需要首先从关联的策略中删除电子邮件通讯组列表。

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中，查看关联的策略。



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



5. 单击“保存更改”，然后返回到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。

用于警报通知的 **Webhook**

June 26, 2023

您可以使用 Webhook 将 Citrix Analytics 警报通知发送给配置了传入 Webhook URL 的任何第三方应用程序。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。

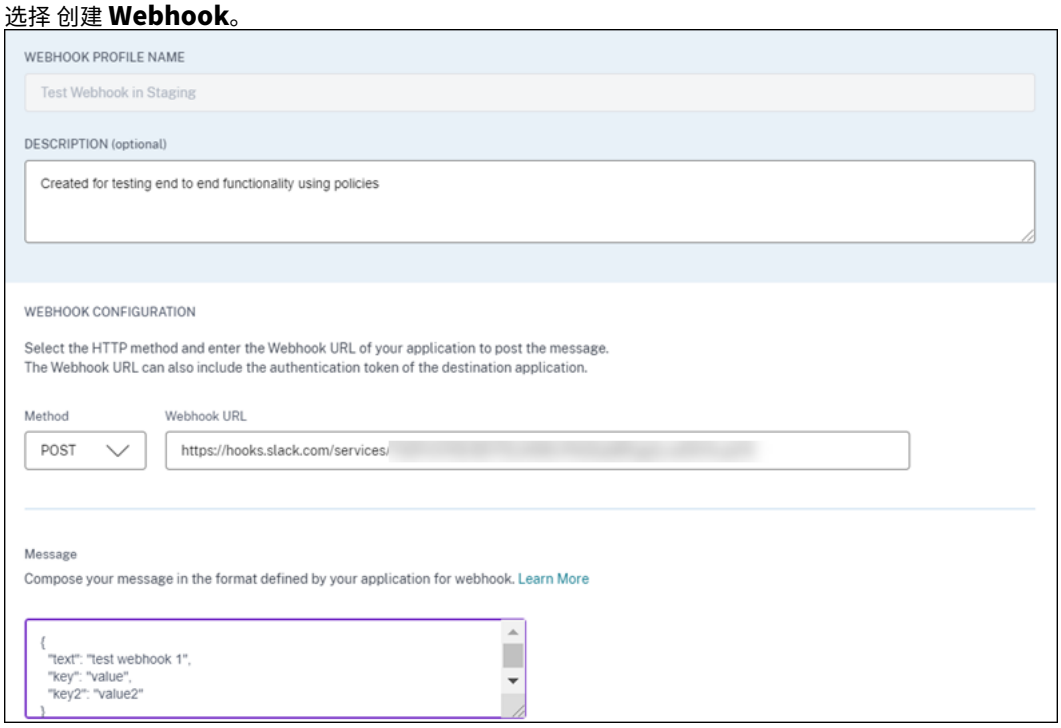
当 Citrix Analytics 触发警报时，关联的 Webhook 会将警报消息发送到目标应用程序的 URL。警报以 JSON 负载的形式通过 HTTP POST 或 PUT 请求发送。例如，当用户触发风险指示器或 VDI 计算机的性能下降时，您可以设置 Webhook 将警报通知发送到您的 Slack 频道。
为警报管理设置 Webhook 可帮助您在应用程序中获取实时通知。您可以及时采取措施来降低安全风险或提高 Citrix Virtual Apps and Desktops 部署的性能。

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 Citrix Analytics。
2. 根据您订阅的产品，单击“管理”以访问 Security Analytics 或 Performance Analytics。

3. 在顶栏中，单击“设置”**>**“警报设置”**>**“**Webhook**”。
4. 选择 创建 **Webhook**。



5. 输入 Webhook 的配置文件名称和描述以确定其用途。
6. 选择应用程序的 HTTP 方法和 Webhook URL 来发送警报消息。

> 注意：
> 传出的 Webhook 通常是通过 HTTP POST 请求发送的。您还可以在应用程序的 Webhook URL 中包含身份验证令牌。

7. 输入有关您要发送到 Webhook URL 的警报的消息。消息的结构必须采用目标应用程序定义的 JSON 或 XML 等格式。有关更多信息，请参阅 Webhook 示例。
8. （可选）输入消息的标题键和值。标头可以包含身份验证令牌或其他自定义键值对，以将负载安全地发送到您的应用程序。
9. 要验证 Webhook 配置，请单击“测试”。
   该测试会验证传出的 Webhook URL、负载结构和标头密钥。如果在配置中未发现任何问题，则会收到“测试成功”消息。

Webhook 配置示例

本节提供了配置 Webhook 以向 Slack 和 Microsoft Teams 等第三方应用程序发送警报的示例。

> 注意：
> 有关如何获取 Webhook URL 和 Webhook 所需的配置，请参阅第三方应用程序的产品文档。

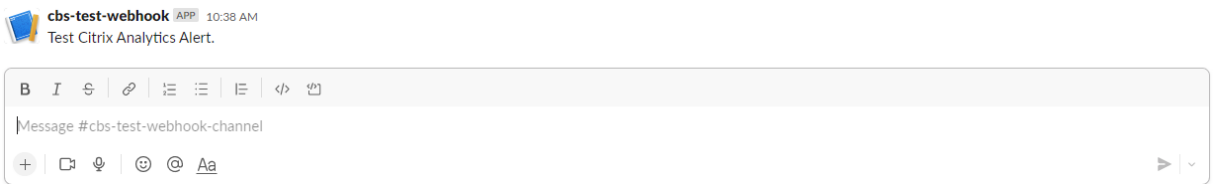
向 **Slack** 发送警报消息

在 Slack 上，请确保在发送警报之前已完成以下任务：

1. 如果您还没有 Slack 应用程序，请为 Citrix Analytics 创建一个 Slack 应用程序。
2. 对于应用程序，启用传入 Webhook 功能并创建传入 Webhook。
3. 选择应用程序向其发布消息的频道。
4. 当您授权应用程序时，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。

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

输出



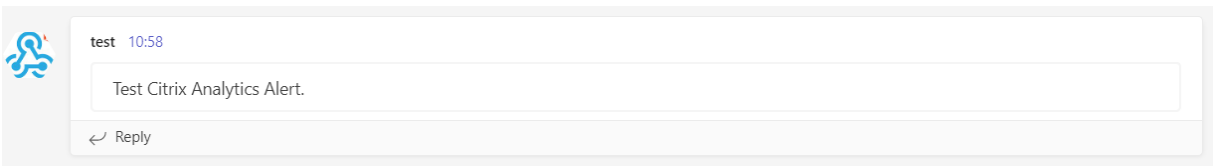
向 **Microsoft Teams** 发送警报消息

在 Microsoft Teams 上，请确保在发送警报之前已完成以下任务：

1. 如果您还没有 Teams 组，请在 Teams 中创建一个 Teams 组。
2. 创建 Webhook 连接器。请参阅“创建和发送消息”一文中描述的步骤。
3. 获取 Webhook 的 URL。

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

输出



Citrix Analytics for Security (Security Analytics)

February 14, 2024

凭借在任何地点、任何时间、任何网络上的任何设备上工作的优势，与用户仅在孤立的公司办公室工作时相比，敏感的公司数据暴露得更多。恶意用户的攻击面很大。IT 团队负责在不影响安全性的情况下提供出色的用户体验。针对安全的 Citrix Analytics 可以通过关注用户安全来帮助弥合这一差距。

Citrix Analytics 是什么

Citrix Analytics for Security 会持续评估 Citrix Virtual Apps and Desktops 用户、Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）用户和 Citrix Workspace 用户的行为。它采取措施来保护敏感的公司信息。通过网络、虚拟化应用程序和桌面工具聚合和关联数据，可以生成有价值的见解，并采取更有针对性的行动来应对用户安全威胁。此外，机器学习还支持高度预测性的方法来识别恶意用户行为。

功能

- 简化了来自 Citrix 产品和合作伙伴集成的见解。有关详细信息，请参阅 自助搜索。
- 易于使用的控制板提供了用户行为的完整视图。有关详细信息，请参阅 用户控制板。
- 使用机器学习和自动化操作的自定义策略来检测和缓解恶意用户行为。有关更多信息，请参阅 策略和操作。
- 在对企业网络进行初始身份验证后，对用户行为的持续监视可以平衡彻底的安全性和有关更多信息，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：提供对整个组织中用户行为模式的可见性。
- 用户访问权限：汇总网络中用户访问的风险域的数量以及用户上载和下载的数据量。
- 应用程序访问：汇总网络中用户访问的域、URL 和应用程序的详细信息。
- 访问保证位置：汇总 Citrix Virtual Apps and Desktops 用户以及 Citrix DaaS 用户的访问详细信息和登录详细信息。
- 报告：根据载入数据源中提供的维度和指标创建自定义报告。

接下来做什么

- 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 对日志的收集、存储和保留。
- 开始使用：如何开始在组织中使用 Analytics。

Citrix Analytics for Performance (Performance Analytics)

September 25, 2023

什么是 **Performance Analytics**

性能分析是 Citrix Analytics 的一项产品，使您能够跟踪、汇总和可视化应用程序和桌面环境的关键性能指标。

- Performance Analytics 将站点性能指标汇总到易于查看的用户体验和基础架构控制板中。控制板可帮助您分析用户体验并优化应用程序和桌面网站的使用情况。
- Performance Analytics 支持多站点聚合和报告。它汇总了整个云和本地设置的性能指标。因此，您可以在单个控制台上查看环境中所有站点的数据。
- Performance Analytics 可以量化用户性能因素，并根据这些因素对用户进行分类。它提供了可操作的见解，以解决故障、屏幕滞后、延迟会话登录和其他性能指标。
- 通过 Performance Analytics，您可以查找和筛选指标，以缩小到面临性能问题的特定用户或会话。

如何使用 **Performance Analytics**

用户体验控制板

用户体验控制板显示与会话响应能力、会话登录持续时间、会话失败和会话重新连接等因素有关的站点性能，这些因素共同定义了用户体验。

如果您支持组织中虚拟应用程序和桌面的多个用户，并且他们在启动应用程序或桌面时偶尔会遇到延迟，则登录持续时间指标可帮助您深入了解问题。向下钻取可以帮助您确定导致问题的因素。

基础结构控制板

基础架构控制板显示站点中计算机的状态和运行状况。当一起使用时，“用户”和“基础架构”控制板可以帮助您主动检查资源的可用性并确定站点上的性能瓶颈。

- 如果用户或会话趋势显示下降，表示登录到站点的用户或会话数量减少，请使用此指示器检查虚拟机管理程序是否已重新启动或计算机数量不足。
- 如果您看到多个会话无法启动的情况，请深入查看以确定失败的原因。可能是许可证数量不足或计算机连接到 Delivery Controller 的问题。

> 注意：
>
> 基础架构分析控制板 目前处于预览版

使用 Performance Analytics，您可以快速分析问题、进行故障排除和解决，并保持应用程序和桌面的最佳服务级别。

快速入门

必备条件

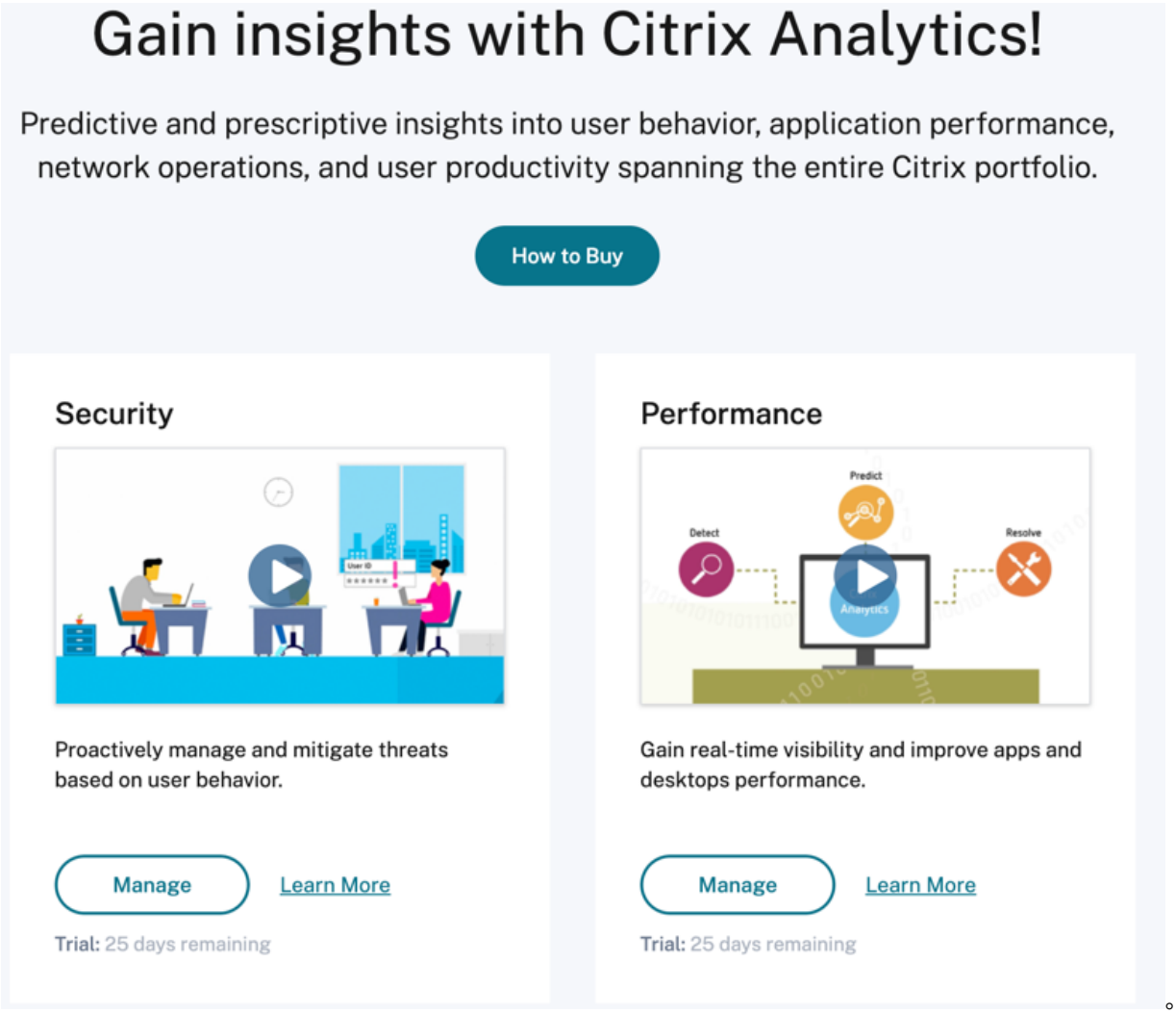
1. 检查您的工作站是否有支持的浏览器一文中列出的 受支持的 Web 浏览器 。有关系统要求的信息，请参阅 Citrix Analytics 系统要求 一文。
2. 您必须拥有 Citrix Cloud 帐户才能使用分析服务。有关如何创建 Citrix Cloud 帐户的详细说明，请参阅注册 Citrix Cloud。转到 https://citrix.cloud.com 并使用您的 Citrix Cloud 帐户登录。
3. Citrix Analytics for Performance 可作为基于订阅的产品提供，既可以作为独立产的品，也可以与 Citrix Analytics for Security 捆绑在一起。要订阅 Citrix Analytics for Performance，请参阅 `https://www.citrix.com/products/citrix-analytics-performance.html)`。
4. 数据源一文中提供了受支持 的数据源 版本。
5. 必须在所有计算机上安装 Citrix Profile Management。

6. 最终用户体验监视 (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。有关详细信息，请参阅 最终用户监视策略设置。
7. 必须将用于 **Performance Analytics** 的 **VDA** 数据收集策略设置为允许在计算机上使用，以使监视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 为 Performance Analytics 收集数据的策略。
8. 启用 Citrix Studio 的进程监视策略，以在“计算机统计”**>**“进程”选项卡中查看高资源消耗进程。
   有关更多信息，请参阅、启用进程监视。
9. 确保从所有端点（或代理，如果已配置）访问以下 URL：

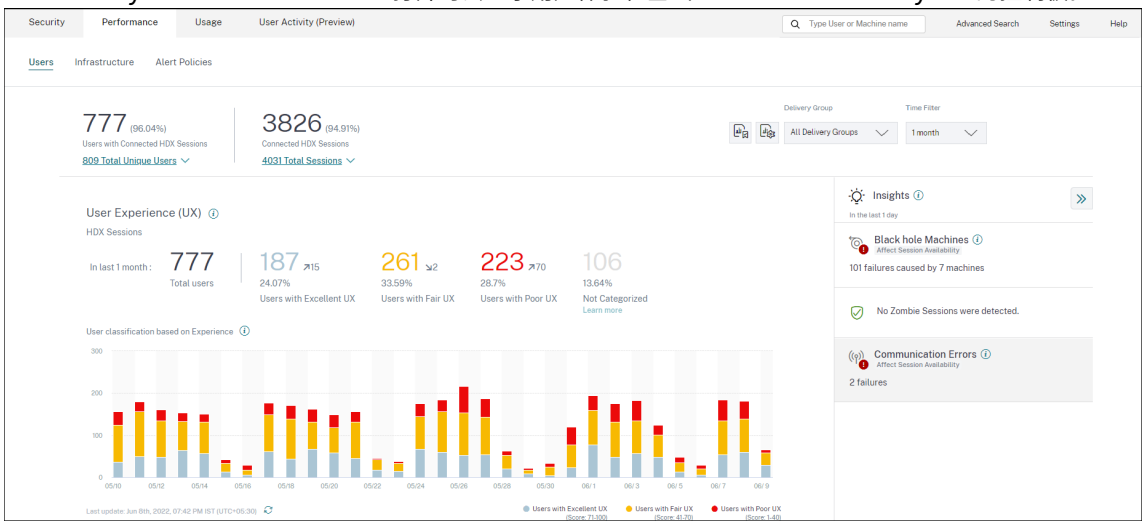
端点	美国地区	欧盟区域	亚太南部地区
Citrix 密钥注册	https://trust.citrixnetworkapi.net	https://trust.citrixnetworkapi.net	https://trust.citrixnetworkapi.net
Citrix Cloud	https://trust.citrixworkspacesapi.net	https://trust-eu.citrixworkspacesapi.net	https://trust-aps.citrixworkspacesapi.net
Citrix Analytics	https://api.was.cloud.com	https://api-eu.was.cloud.com	https://api-aps.was.cloud.com
批量上传	https://citrixanalyticseh-alias.servicebus.windows.net/	https://citrixanalyticsehe-alias.servicebus.windows.net/	https://citrixanalyticsehaps-alias.servicebus.windows.net/

访问

1. 登录 Citrix Cloud。查找 Analytics 服务磁贴，然后单击 管理。概述页面显示 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，请单击申请试用。如果您已购买 Citrix Analytics for Performance 产品，请改为单击管理链接。



1. Citrix Analytics for Performance 打开时会显示用户体验和基础 Performance Analytics 的控制板。



从亚太南部地区访问　面向亚太南部 (APS) 区域的试用客户和订阅型客户现已自动加入 Citrix Analytics for Performance。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，请在租户加入 Citrix Cloud 时选择亚太南部区域。登录 Citrix Cloud，然后在 Citrix Cloud 的 APS 区域中选择租户。使用 `https://analytics-aps.cloud.com` URL 访问您的 Citrix Analytics 云服务。

- 现在，当您选择亚太南部区域作为主区域时，Citrix Analytics for Performance 会将组织的用户事件和元数据存储在亚太南部区域。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的信息，请参阅技术安全概述。

配置数据源

您可以使用 Performance Analytics 来监视本地或云站点。无论您是纯本地客户、云客户还是混合使用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 Citrix Virtual Apps and Desktops 站点加入 Performance Analytics。
- 要在 Performance Analytics 上获取与网络相关的信息，您还必须加载本地 Citrix Gateway。

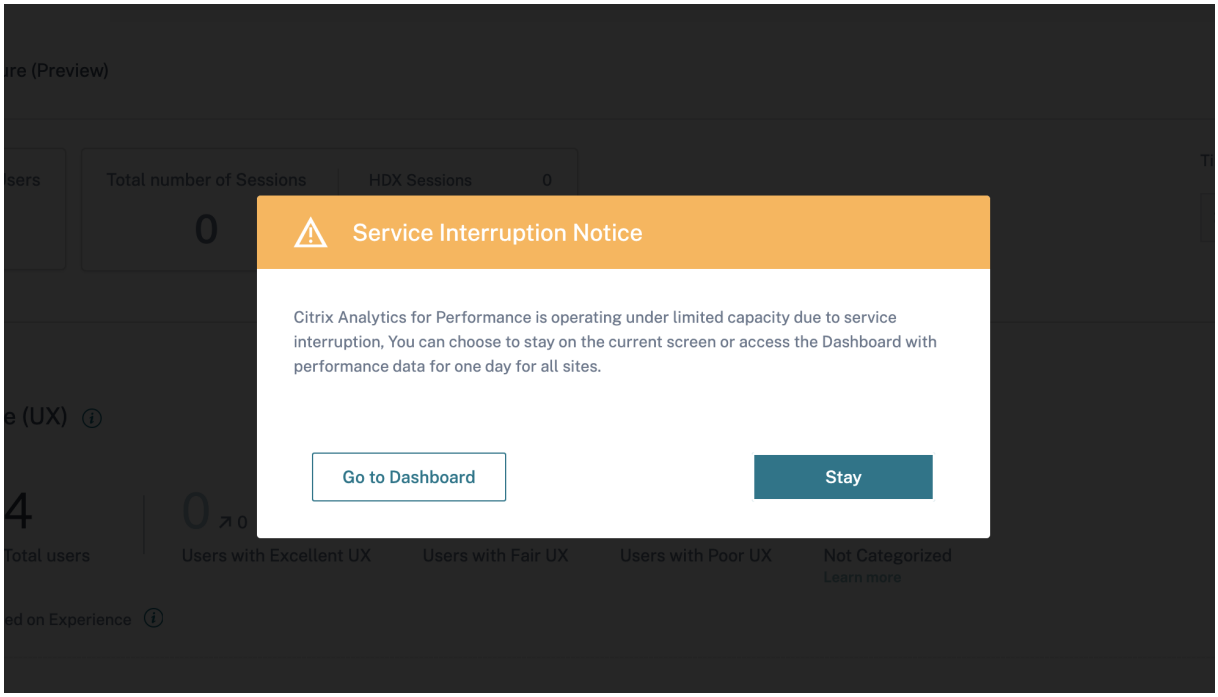
按照数据源一文中的说明配置所需的 数据源 。

> 注意：
>
> - Citrix Analytics for Performance 收集和存储为 Citrix Analytics for Performance 而收集的日志中列出的数据点的日志。
> - 限制一文中列出了针对 Citrix Analytics for Performance 服务的建议限制。

服务连续性

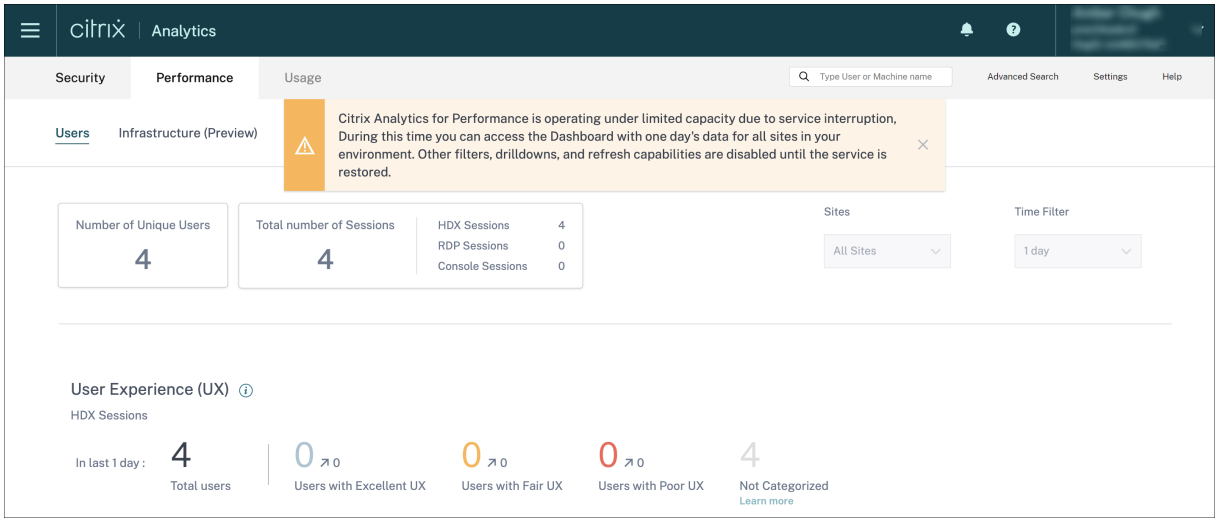
如果服务中断，Citrix Analytics for Performance 将以有限的容量运行。

管理员可以选择保 留 并查看当前屏幕上的可用数据，或者在降级模式下 转到控制板。



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控制板。

无论哪种情况，在服务恢复正常运行之前，所有筛选器和向下钻取都将被禁用。



此更新提高了产品弹性，有助于与 服务级别协议保持一致。

Citrix Analytics for Security 和 Citrix Analytics for Performance 故障排除

December 7, 2023

本节介绍了如何解决在使用 Citrix Analytics for Security 时可能遇到的以下问题。

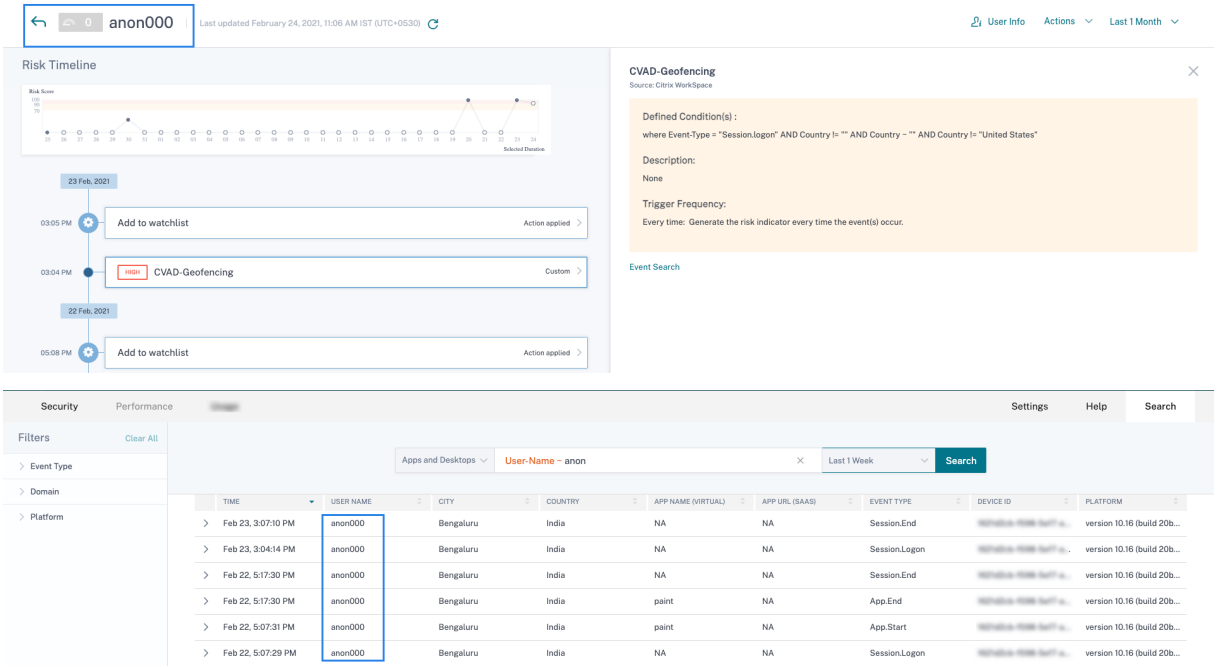
- 将匿名用户验证为合法用户。
- 排查来自数据源的事件传输问题。
- 触发 Virtual Apps and Desktops 事件、SaaS 事件，并验证事件传输到 Citrix Analytics for Security。
- Session Recording 服务器无法连接。
- 适用于 Splunk 的 Citrix Analytics 加载项存在配置问题

验证匿名用户为合法用户

July 12, 2022

作为管理员，您可能会注意到某些 Citrix Virtual Apps and Desktops
用户和 Citrix DaaS（以前是 Citrix Virtual Apps and Desktops 服务）用户在 Citrix Analytics for Security 上显示为匿名用户。这些用户被标识为已发现的用户。但是他们的用户名在以下页面上显示为 anonXYZ（其中“XYZ”表示三位数字）：

- 用户
- 用户的时间表
- 有风险的用户
- 自助搜索 Apps and Desktops 数据源



当你看到这样的用户时，你可能想知道：

- 这些用户是谁?
- 这些用户本质上是合法还是恶意的?
- 如何验证它们?
- 我必须为这些用户申请哪些操作?

在以下情况下，您可以在 Citrix IT 环境中看到匿名用户：

- 当用户使用已发布的安全浏览器应用程序时
- 当用户使用未经身份验证的商店时

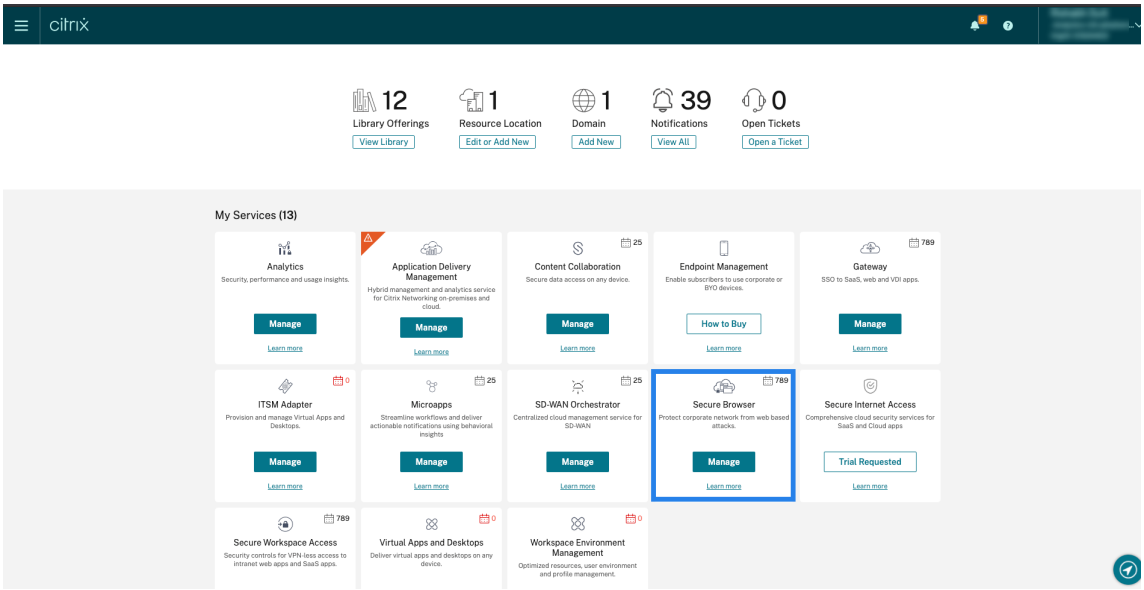
使用已发布的安全浏览器应用

安全浏览器应用程序是使用 Citrix Secure Browser 服务发布的 Web 应用程序。这些应用程序隔离您的 Web 浏览事件，保护您的公司网络免受基于浏览器的攻击。有关详细信息，请参阅 安全浏览器服务。

安全浏览器应用程序使用 Citrix DaaS 的匿名会话功能。

要验证 Citrix Cloud 帐户是否配置了安全浏览器，请执行以下操作：

1. 登录 Citrix Cloud。
2. 在 安全浏览器 卡上，单击 管理。



3. 在 管 理页面上，检查已发布的安全浏览器应用程序。

如果用户使用 Web 浏览器通过 Citrix Receiver for Web 站点访问 StoreFront 应用商店并使用已发布的安全浏览器应用程序，则该用户的身份将隐藏。因此，Citrix Analytics 会将用户显示为匿名。

如果用户通过安装在其设备上的 Citrix Receiver 或 Citrix Workspace 应用程序访问 StoreFront 应用商店并使用已发布的安全浏览器应用程序，Citrix Analytics 将该用户显示为 StoreFront 中指定的用户名。

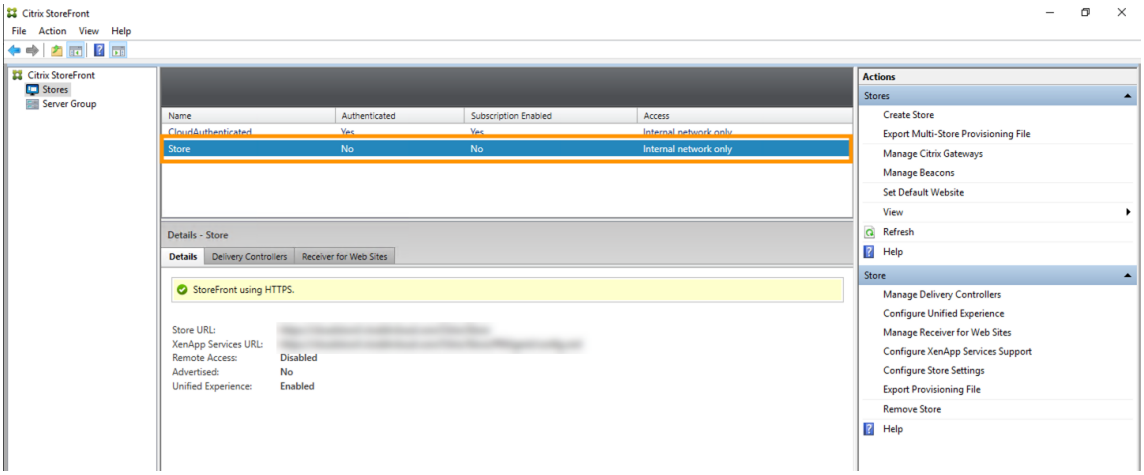
因此，您可以将该用户视为组织的合法用户。如果没有与用户相关的危险行为，则无需应用任何操作。

用户使用未经身份验证的商店

未经身份验证的应用商店是 Citrix StoreFront 的一项功能，适用于客户管理的商店。此功能支持未经身份验证（匿名）用户的访问权限。

要验证组织是否有未经身份验证的商店，请执行以

1. 启动 Citrix Studio。
2. 点击 商店。
3. 对于您的商店，请在已验证列中检查身份验证状态。



如果商店未经过身份验证且用户正在访问该未经身份验证的应用商店，则用户身份将保持匿名。因此，Citrix Analytics 会将用户显示为匿名。您可以将此用户视为组织的合法用户。如果没有与用户相关的危险行为，则无需应用任何操作。

解决数据源的事件传输问题

April 12, 2024

本节帮助您解决 Citrix Analytics for Security 中的数据传输问题。当数据源无法准确传输用户事件时，您可能会遇到未发现用户和风险指示器等问题。

清单

序列	检查
1	您是否拥有使用 Security Analytics 的正确权利?
2	您所在的区域是否支持该数据源?
3	您的环境是否满足所有系统要求?
4	是否在 Analytics 上发现了所有数据源并启用了数据处理?
5	数据源上的用户活动是否将事件准确地传输到 Analytics?
6	虚拟应用程序和桌面事件是否会传输到 Analytics?
7	用户事件是否显示在 Analytics 的自助搜索页面上?
8	用户是否被 Analytics 发现?

检查 **1 -** 您是否拥有使用 **Security Analytics** 的正确权利

Citrix Analytics for Security 是一项基于订阅的产品。有关更多信息，请参阅 入门。

检查 **2-**您的本地区域是否支持数据源

以下主区域支持 Citrix Analytics for Security：

- 美国 (US)
- 欧洲联盟（EU）
- 亚太南部 (APS)

根据组织所在的位置，您可以在其中一个主区域加入 Citrix Cloud。

但是，并非所有主区域都支持某些数据源。[数据源](/en-us/security-analytics/data-sources.html)）是 Citrix Analytics for Security 从中接收用户事件的产品。

如果您的组织在不支持数据源的主区域中加入了 Citrix Cloud，则不会从数据源获取用户事件。

使用下表查看数据源及其受支持的区域。

数据源	在美国地区受支持	在欧盟地区受支持	APS 区域支持
Citrix Endpoint Management	是	是	是
Citrix Gateway（本地）	是	是	是
Citrix 身份提供程序	是	是	是
Citrix Secure Browser	是	是	是
Citrix Secure Private Access	是	否	否
Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	是	是	是
Citrix Virtual Apps and Desktops 本地	是	是	是
Microsoft Active Directory	是	是	是
Microsoft Graph 安全性	是	是	是

检查 **3-**您的环境是否满足所有系统要求

Citrix Analytics 可能需要几分钟时间才能从数据源接收用户事件。如果在数据源站点卡上看不到任何用户事件，请确保您的环境满足必备条件和 系统要求。

必备条件

1. 您的所有 Citrix Cloud 订阅都必须处于活动状态。在 Citrix Cloud 页面上，确保所有 Citrix Cloud 服务均处于活动状态。
2. 如果使用本地部署 Citrix Virtual Apps and Desktops，则必须将站点添加到 Citrix Workspace 并配置站点聚合。Citrix Analytics 会自动发现添加到 Citrix Workspace 的站点。有关更多信息，请参阅 聚合工作区中的本地虚拟应用程序和桌面。
3. 如果要为站点使用 StoreFront 部署，请将 StoreFront 服务器配置为使 Citrix Workspace 应用程序能够向 Citrix Analytics 发送用户事件。确保 StoreFront 版本为 1906 或更高版本。如果不配置 StoreFront 服务器，Citrix Analytics 将无法从本地 Citrix Virtual Apps and Desktops 接收用户事件。要配置 StoreFront 部署，请参阅 StoreFront 文档中的 Citrix Analytics Service 一文。

4. Citrix Virtual Apps and Desktops 用户和 Citrix DaaS 用户必须在其端点使用指定版本的 Citrix Workspace 应用程序或 Citrix Receiver。否则，Analytics 不会从用户端点接收用户事件。Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源中提供了受支持的 Citrix Workspace 应用程序或 Citrix Receiver 版本列表。
5. 要从已发布的安全浏览器会话中接收用户的事件，请在安全浏览器中启用 主机名跟踪 设置。默认情况下，禁用此设置。有关更多信息，请参阅管理已发布的安全浏览器。
6. 如以下文章所述，载入数据源：
    - Citrix Endpoint Management 数据源
    - Citrix Gateway 数据源
    - Citrix Secure Private Access 数据源
    - Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源
    - Microsoft Active Directory 集成
    - Microsoft Graph 安全性集成

检查 **4-Analytics** 上是否发现了所有数据源并启用了数据处理

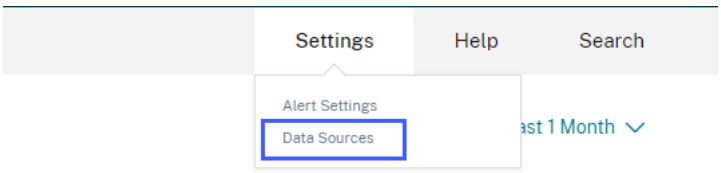
确保已发现所有数据源，并且已为它们启用了数据处理。如果不为数据源启用数据处理，则不会发现使用该数据源的用户。这种情况可能会造成潜在的安全风险。

启用数据处理可确保 Citrix Analytics 正在处理您的用户事件。只有在用户主动使用数据源时，才会将事件发送到 Citrix Analytics。

> 注意
>
> Citrix Analytics 不会主动从您的环境中提取数据。

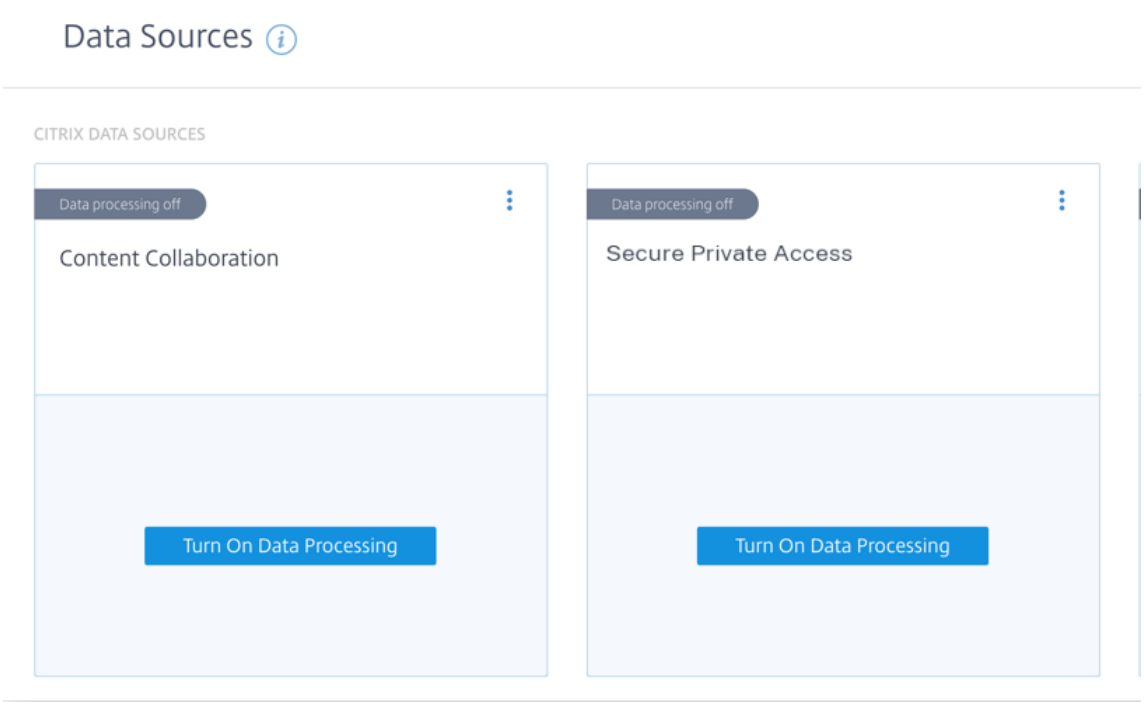
要发现数据源并启用分析，请执行以下操作：

1. 单击“设置”>“数据源”>“安全”以查看发现的数据源。Citrix Analytics 会自动发现您已订阅 Citrix Cloud 账户的数据源。

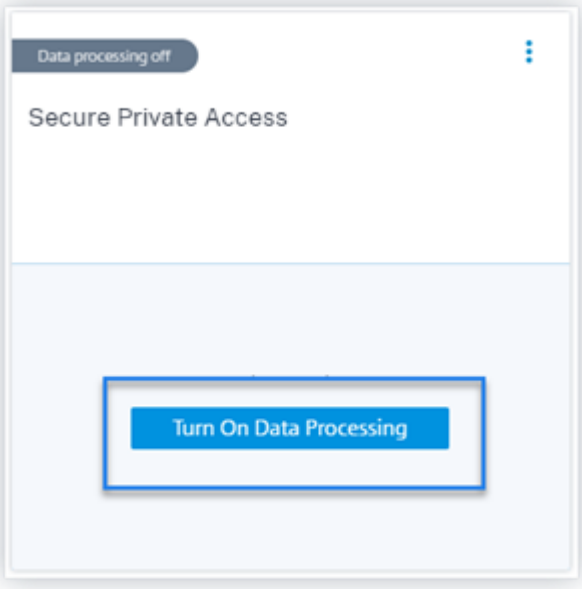


2. 在“数据源”页面上，发现的数据源将显示为站点卡。默认情况下，数据处理处于关闭状态。

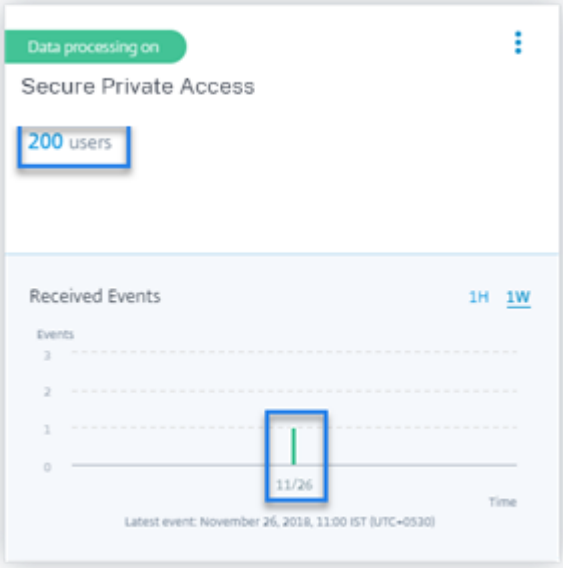
> 重要提示
>
> Citrix Analytics 会在您同意后处理您的数据。



3. 在希望 **Citrix Analytics** 为其处理事件的站点卡片上，单击打开数据 处理。例如，在 Citrix Secure Private Access 站点卡片上，单击“打开数据处理”。



4. 打开数据处理功能后，Citrix Analytics 将处理数据源的事件。网站卡的状态更改为数据处理。您可以根据所选时间段查看用户数量和接收的事件。



5. 对于所有发现的数据源，请按照 入门 中指定的步骤启用分析。

检查 **5-**数据源上的用户活动是否将事件准确地传输到 **Analytics**

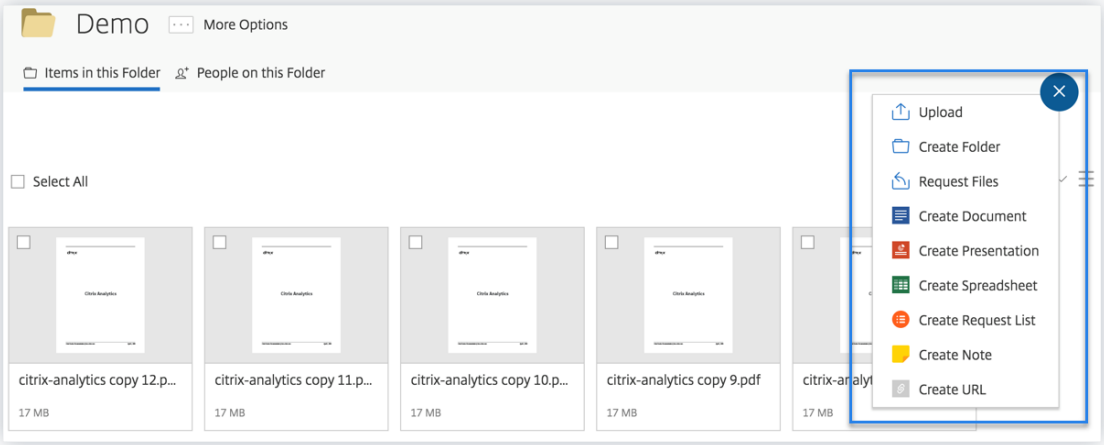
当用户主动使用数据源时，Citrix Analytics 会从数据源接收用户事件。用户必须在数据源上执行某些活动才能生成事件。例如，要接收来自应用程序和桌面数据源的事件，应用程序和桌面用户必须共享、上传或下载某些文件。

> 注意
>
> Citrix Analytics 不会主动从您的环境中提取数据。

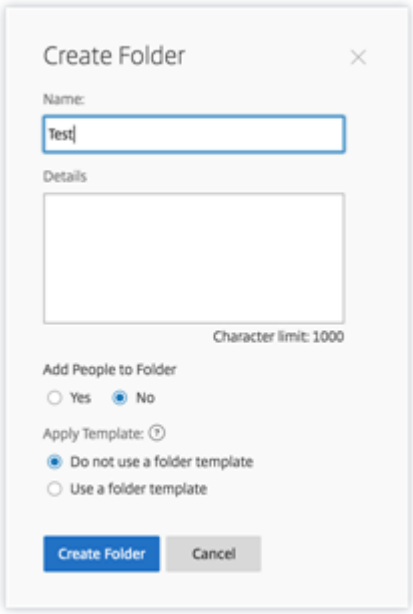
如果您在 Citrix Analytics 中看不到数据源的任何用户事件，则用户很有可能此时未处于活动状态。

要验证 Citrix Analytics 是否准确地接收了用户事件，请执行以下活动。此活动使用 Citrix 应用程序和桌面数据源。您可以根据您的订阅使用其他 Citrix 产品（数据源）执行类似的活动。

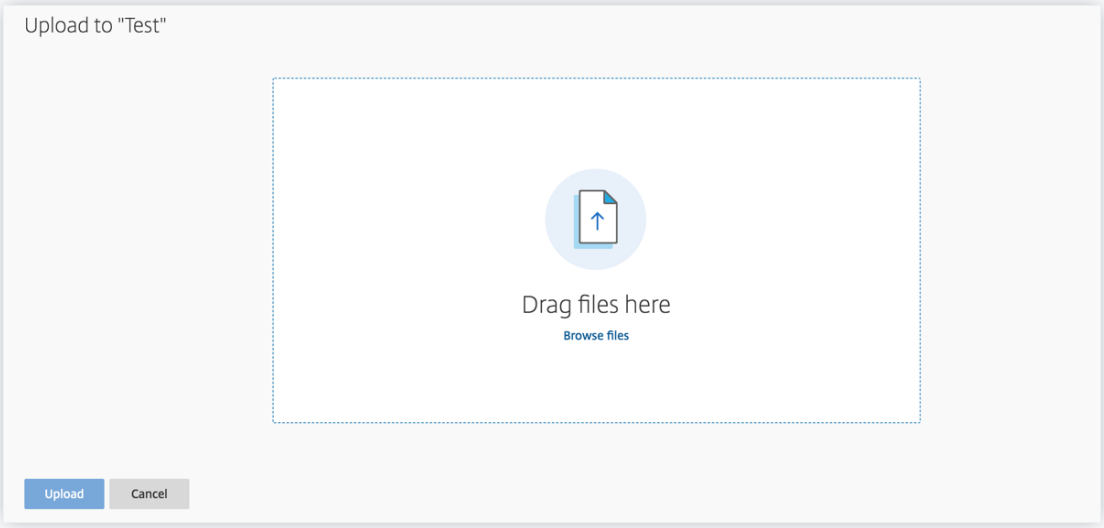
1. 登录 Citrix 应用程序和桌面服务。
2. 执行一些常见的用户活动，例如创建文件夹、下载文件、上传文件或删除文件。



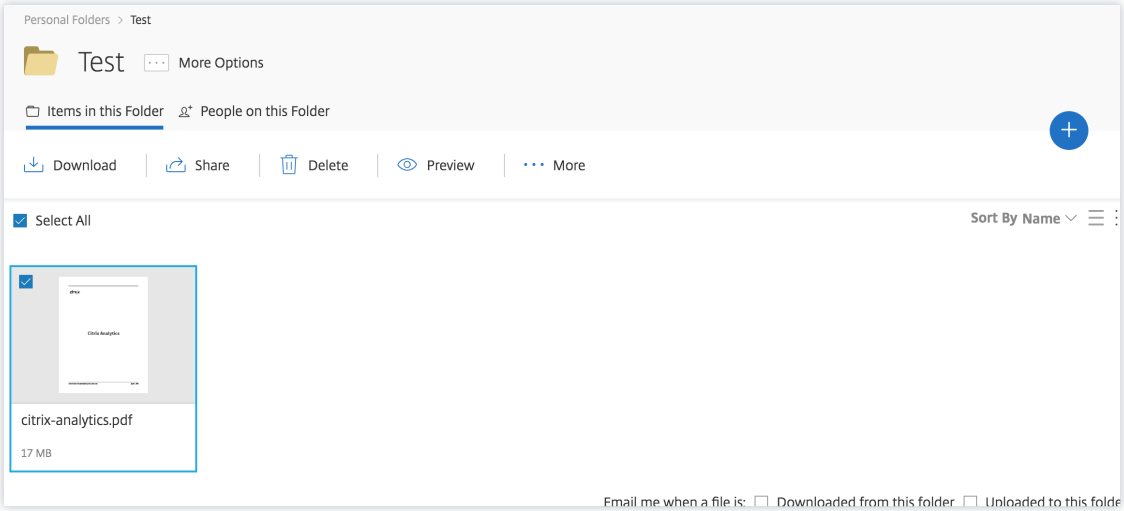
3. 例如，创建一个 Test 文件夹。



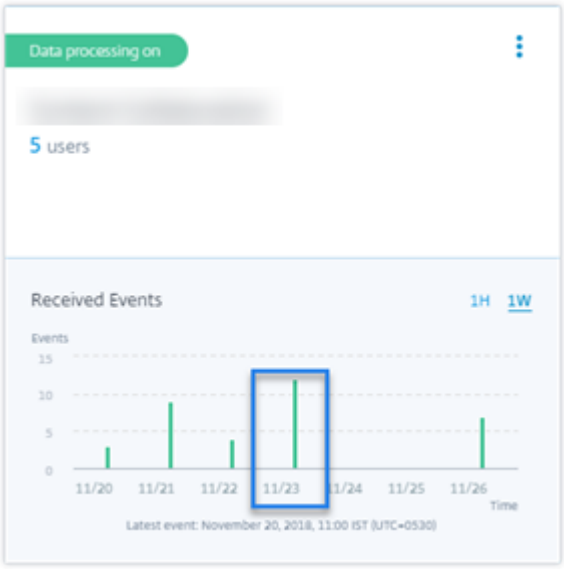
4. 上载一些本地文件。



5. 删除文件夹中的一些文件。



6. 返回 Citrix Analytics，在“数据源”页面上查看“应用程序和桌面”侧卡。Citrix Analytics 接收来自应用程序和桌面数据源的用户事件，并将其显示在网站卡上。



检查 **6**：虚拟应用程序和桌面事件是否传输到 **Analytics**

某些版本的 Citrix Workspace 应用程序或 Citrix Receiver 客户端无法向 Citrix Analytics 发送用户事件。当用户通过这些客户端启动虚拟应用程序和桌面时，Citrix Analytics 无法发现用户，直到他们执行受支持的事件。

例如，适用于 Linux 2006 或更高版本的 Citrix Workspace 应用程序不会将 ***SaaS*** 应用程序启动 和 ***SaaS*** 应用程序结束 事件发送到 Citrix Analytics。Citrix Analytics 上未发现使用适用于 Linux 的 Citrix Workspace 应用程序启动 SaaS 应用程序的用户。

支持的事件

请参阅下表以查看每个客户端版本支持的用户事件。

- 是-事件由客户端发送给 Citrix Analytics。
- 否-客户端不会将事件发送给 Citrix Analytics。
- 不适用-该事件不适用于客户端。

事件	适用于 Windows 的 Workspace 应用程序 1907 或更高版本	适用于 Mac 的 Workspace 应用程序 1910.2 或更高版本	适用于 Linux 的 Workspace 2006 或更高版本	适用于 Android 的 Workspace 应用程序 - Google Play 中提供的最新版本	适用于 iOS 的 Workspace 应用程序 - Apple App Store 中提供的最新版本	适用于 Chrome 的 Workspace 应用程序 - Chrome 网上应用店中提供的最新版本	适用于 HTML5 的 Workspace 2007 或更高版本
帐户登录	是	是	是	是	是	否	否
会话登录	是	是	是	是	是	是	是
会话启动	是	是	是	是	是	是	是
会话结束	是	是	是	是	是	是	是
应用程序启动	是	是	是	否	是	是	是
应用程序结束	是	是	是	否	是	是	是
文件下载	是	是	是	否	否	是	是
打印	否	是	是	否	否	是	是
SaaS 应用程序启动	是	是	否	否	否	否	否
SaaS 应用程序结束	是	是	否	否	否	否	否
SaaS 应用程序 URL 导航	是	是	否	否	否	否	否
SaaS 应用剪贴板访问	是	是	否	否	否	否	否
SaaS 应用程序文件下载	是	是	否	否	否	否	否
SaaS 应用程序文件打印	是	是	否	否	否	否	否

根据事件传输状态，您可能会遇到以下问题：

- 当用户使用其客户端连接到 Citrix Virtual Apps and Desktops 或 Citrix DaaS 时，在执行受支持的事件（活

动）之前，用户可能不会在 Citrix Analytics 中被发现。例如，考虑两个用户事件-应用程序启动和 SaaS 应用程序启动。使用适用于 iOS 的 Citrix Workspace 应用程序的用户，Citrix Analytics 会收到应用程序启动事件，但不接收 SaaS 应用程序启动事件。因此，当用户启动任何虚拟应用程序时，应用程序启动事件都会传输到 Citrix Analytics，然后发现该用户。但是，如果用户启动 SaaS 应用程序，Citrix Analytics 将不会收到 SaaS 应用程序启动事件，也不会发现该用户。有关已发现用户的信息，请参阅 发现的用户。

- 表格上标记为“否”的事件不会显示在自助搜索页面上。有关如何使用自助服务页面的信息，请参阅 关于自助搜索。

建议

为了获得分析的最大优势，Citrix 建议采取以下措施：

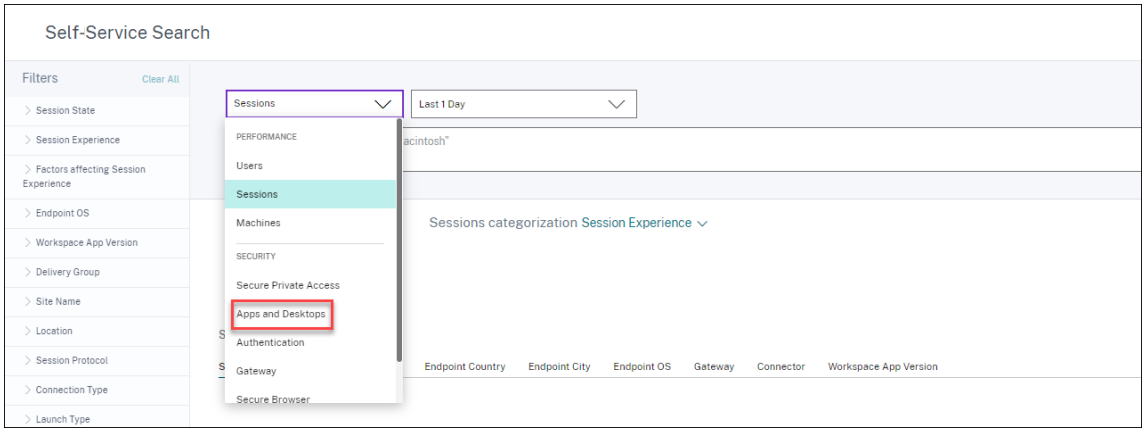
- **Windows** 用户：使用适用于 Windows 的 Citrix Workspace 应用程序 1907 或更高版本连接到您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS。
- **Mac** 用户：Citrix Virtual Apps and Desktops 和 Citrix DaaS 使用适用于 Mac 1910.2 或更高版本的 Citrix Workspace 应用程序连接到你的。

检查 **7-**用户事件是否显示在 **Analytics**（分析）的自助搜索页面上

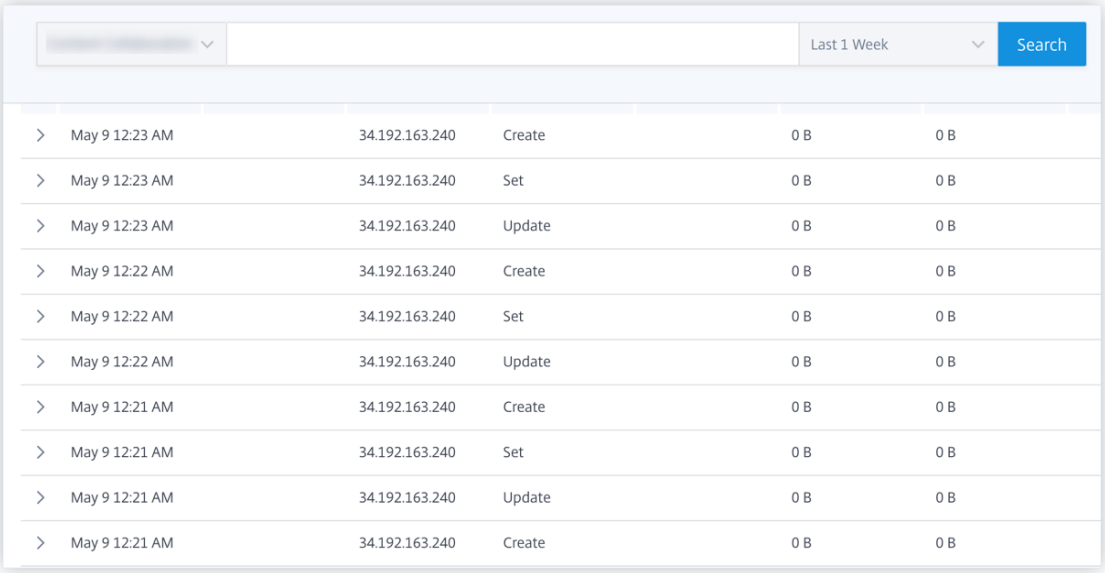
执行最后一次检查以确保事件准确地传输到 Citrix Analytics。

1. 在顶部栏上，单击“高级搜索”以转到自助服务搜索页面。

2. 选择数据源以查看相应的搜索页面和事件。



3. 要查看与应用程序和桌面事件相关的数据，请从列表中选择 应用程序和桌面，选择时间段，然后单击 搜索。

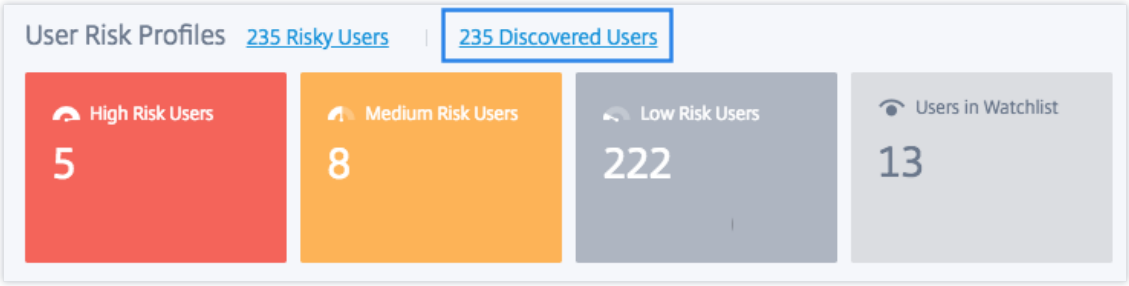


有关详细信息，请参阅 自助搜索。

检查 8-分析是否发现了用户

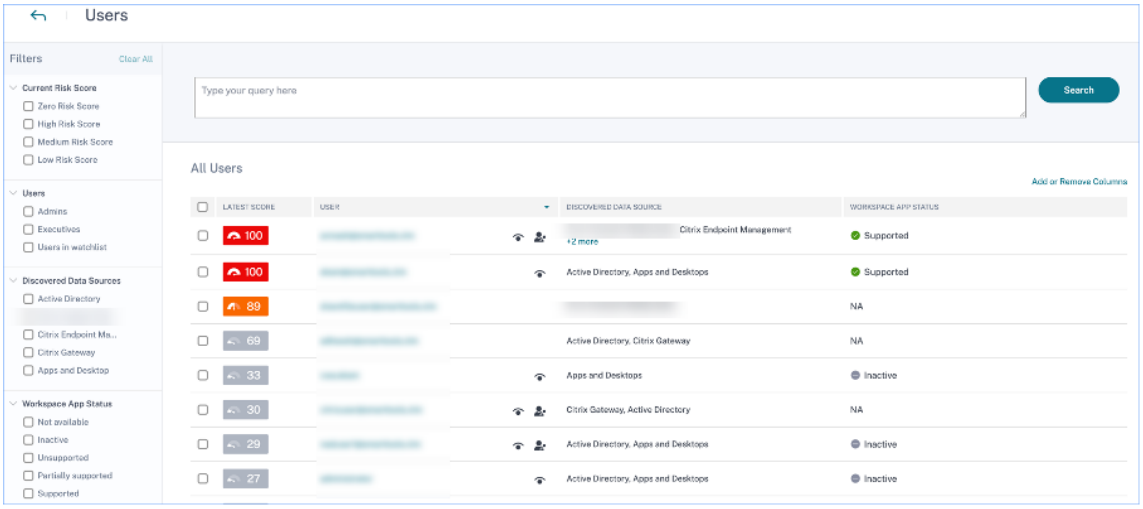
当事件开始流向 Citrix Analytics 时，系统会发现生成事件的用户并将其显示在用户控制板上。此过程通常需要大约几分钟时间，然后您才能在控制板上查看它们。

1. 单击“用户”控制板上的“已发现用户”链接，以查看 Citrix Analytics 发现的用户的完整列表。



2. “用户”页面显示过去 31 天内发现的所有用户的列表。选择时间段以查看风险指示器发生次数。

> 注意
>
> 如果您尝试设置的值大于 31 天，系统会显示一条错误消息，指出 - 日期范围无效。开始日期和结束日期之间的最大允许范围为 **31** 天。



如果事件成功传输，则表明您的 Citrix Analytics 环境将按预期执行。当发现异常时，会生成风险指示器。

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

April 12, 2024

本节介绍触发应用程序和桌面事件、SaaS 事件以及验证 Citrix Analytics for Security 是否正在主动接收这些用户事件的过程。

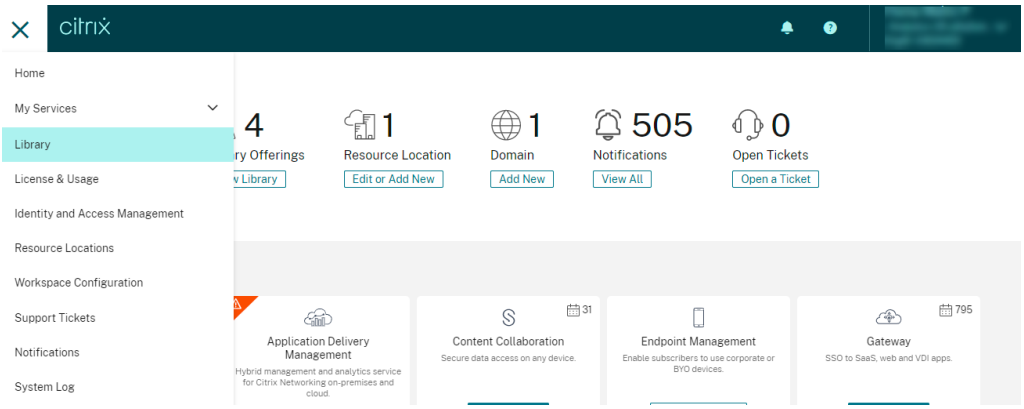
必备条件

- 如果您使用本地 Citrix Virtual Apps and Desktops，请将本地站点加载到 Citrix Analytics，然后从站点卡启用数据处理。如果您使用的是 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务），请直接从站点卡启用数据处理。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。
- 在用户的终端设备中使用正确版本的 Citrix Workspace 应用程序或 Citrix Receiver，以便将事件准确发送到 Citrix Analytics。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 和 Citrix DaaS 数据源。
- 在从虚拟桌面触发打印事件之前，请确保在应用程序和桌面环境中配置和配置了打印机。有关管理打印机的详细信息，请参阅 打印。
- 要触发 SaaS 应用程序启动、SaaS 应用程序 URL 导航、SaaS 应用程序文件下载等 SaaS 事件，必须使用 Workspace 中已配置的 SaaS 应用程序。常用的 SaaS 应用程序包括 Salesforce、Workday、Concur、GoToMeeting。
  - 如果没有已配置 SaaS 应用程序，则必须配置和发布 SaaS 应用程序。有关详细信息，请参阅 对软件即服务应用程序的支持。配置 SaaS 应用程序时，请确保禁用以下安全选项：
    - 限制剪贴板访问

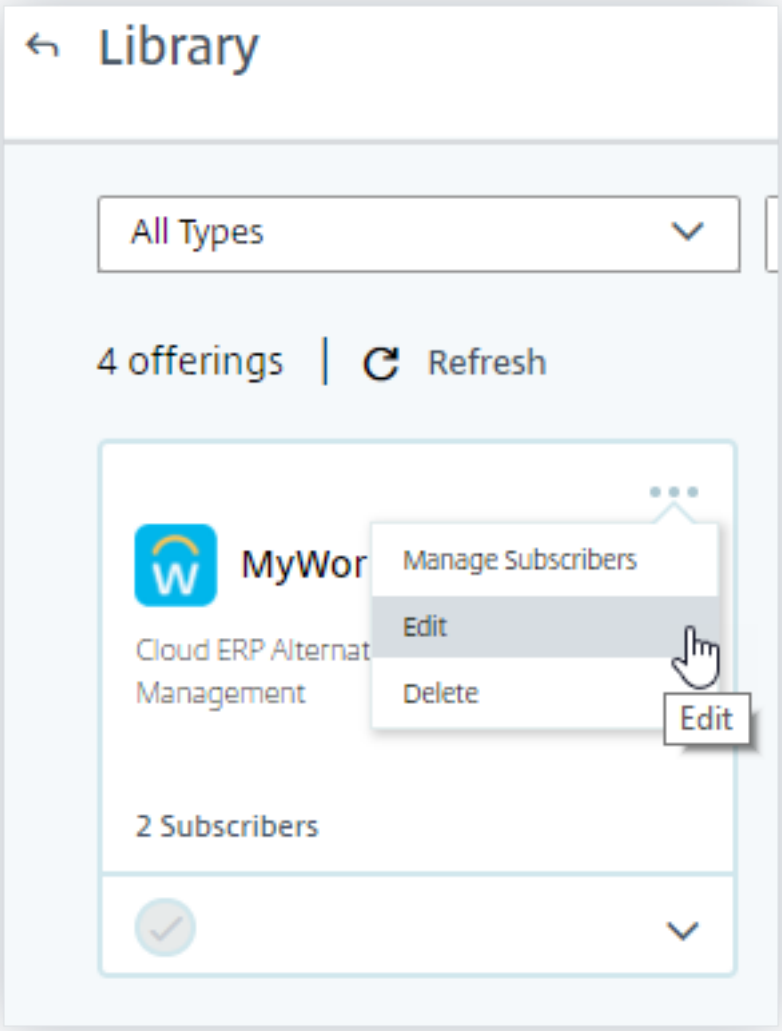
* 限制打印
* 限制导航
* 限制下载

– 如果要使用 Workspace 中已配置的 SaaS 应用来触发事件，请确保为 SaaS 应用程序禁用指定的增强安全选项：

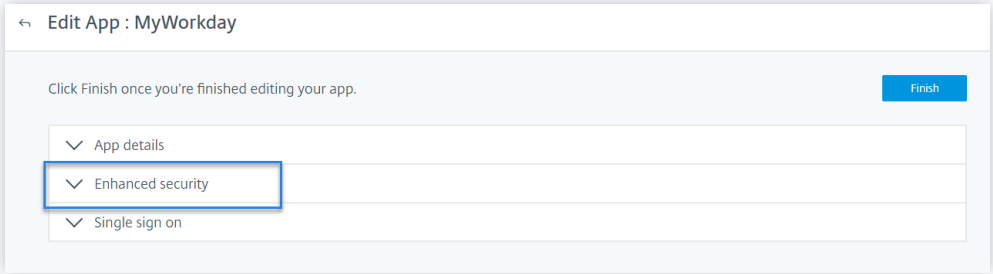
1. 转到您的 Citrix Cloud 帐户，然后选择 库。



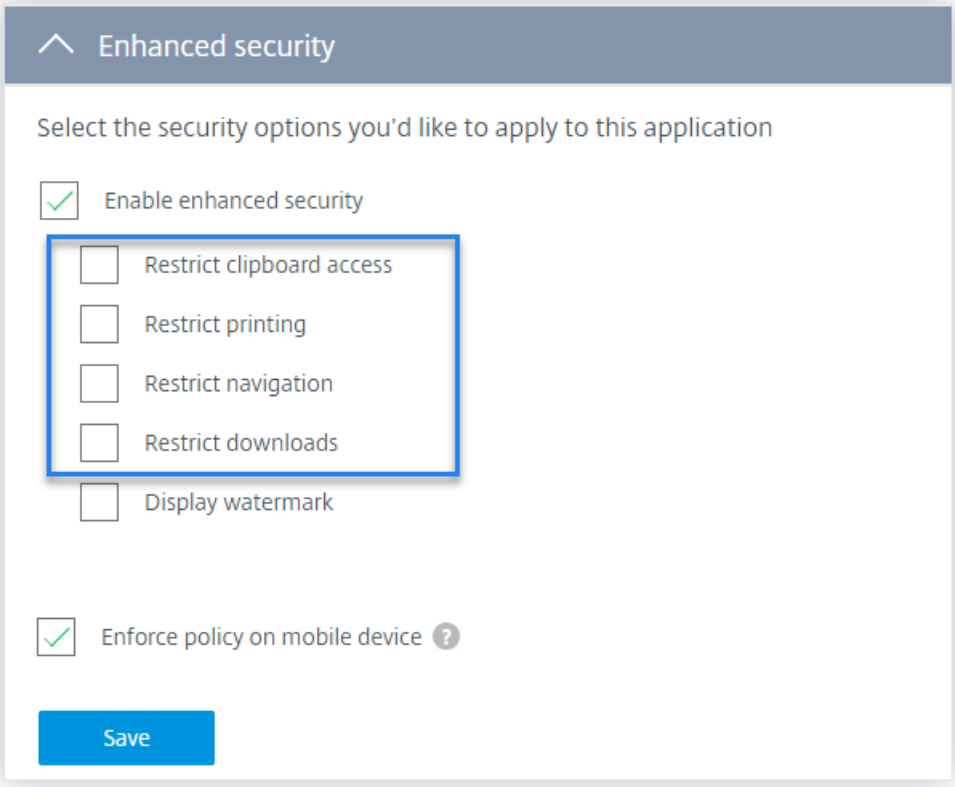
2. 在 资源库 页面上，确定要用于验证事件的 SaaS 应用程序。例如，Workday。
3. 单击省略号，然后选择 编辑。



4. 在 编辑应用程序 页面上，单击增强安全性的向下箭头。



5. 确保未选择以下安全选项。



已知问题

很少有版本的 Citrix Workspace 应用程序和 Citrix Receiver 无法将某些事件发送给 Citrix Analytics 因此，Citrix Analytics 无法为这些事件提供见解并生成风险指示器。有关此问题及其解决方法的更多信息，请参阅已知问题-CAS-16151。

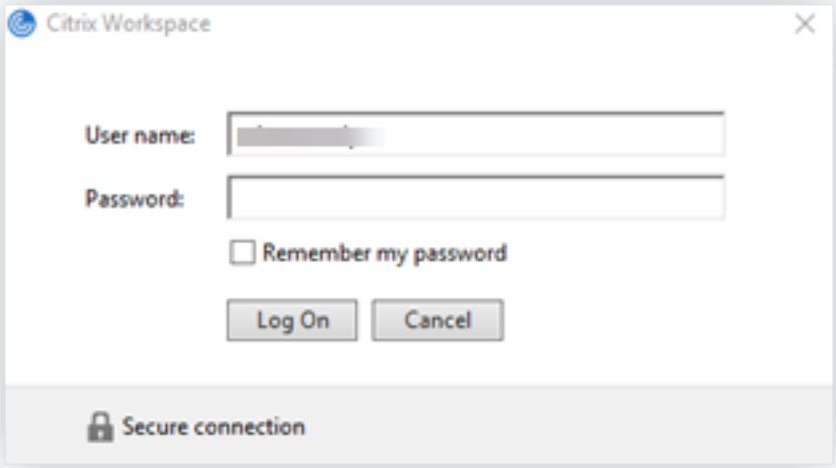
过程

按顺序执行以下步骤以触发应用程序和桌面环境中的事件，并验证 Citrix Analytics for Security 是否正在主动接收这些事件。

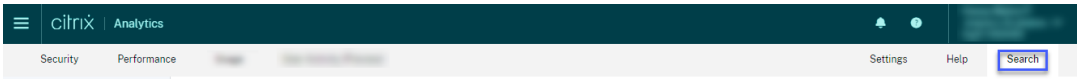
> 注意
>
> - 这些活动可能需要一些时间才能到达 Citrix Analytics。如果看不到触发的事件，请刷新 Citrix Analytics 页面。
> - 为了触发 SaaS 事件，此过程以 Workday 应用程序为例。您可以使用工作区中任何已配置的 SaaS 应用程序来触发 SaaS 事件。

- 帐户登录

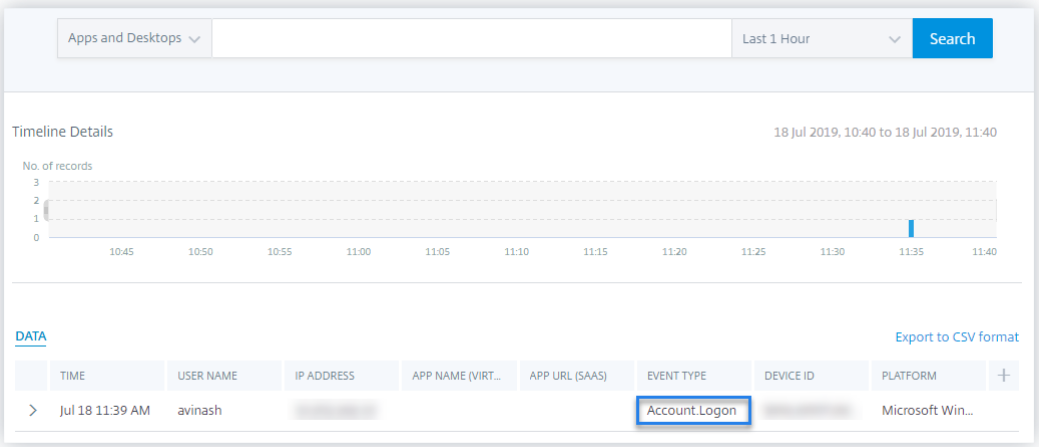
1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 输入您的凭据以登录 Citrix Workspace 应用程序或 Citrix Receiver。



3. 转到 Citrix Analytics。
4. 单击 搜索，然后从列表中选择 应用程序和桌面。



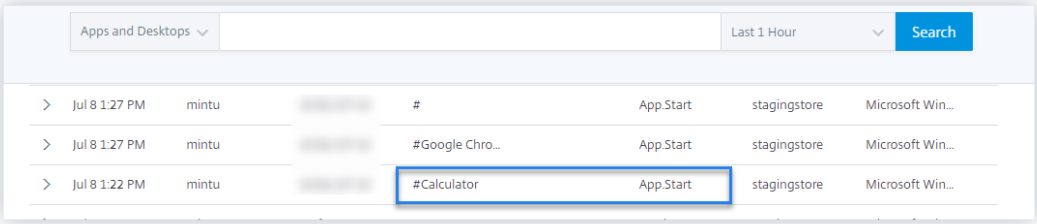
5. 在搜索页面中，查看 **Account.Logon** 事件的数据。展开该行以查看事件详细信息。



- 应用程序启动

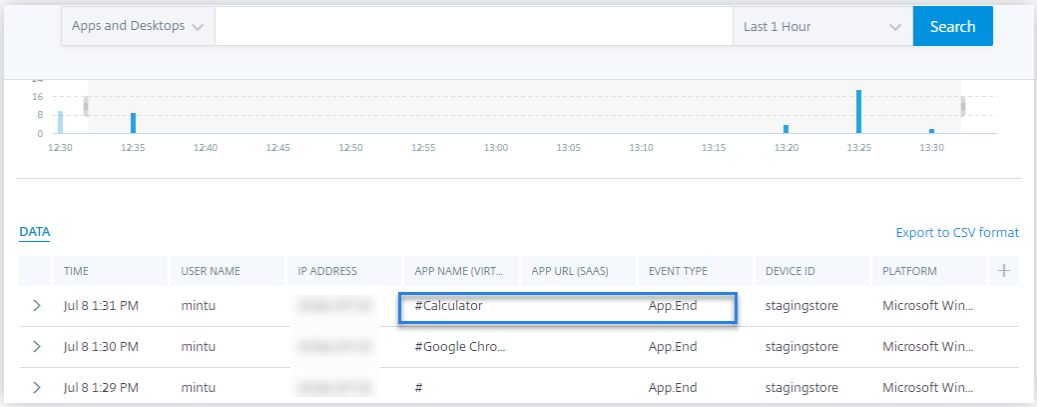
1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 启动计算器之类的应用程序。
3. 转到 Citrix Analytics。

4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 **App.Start** 事件数据的数据。展开该行以查看事件详细信息。



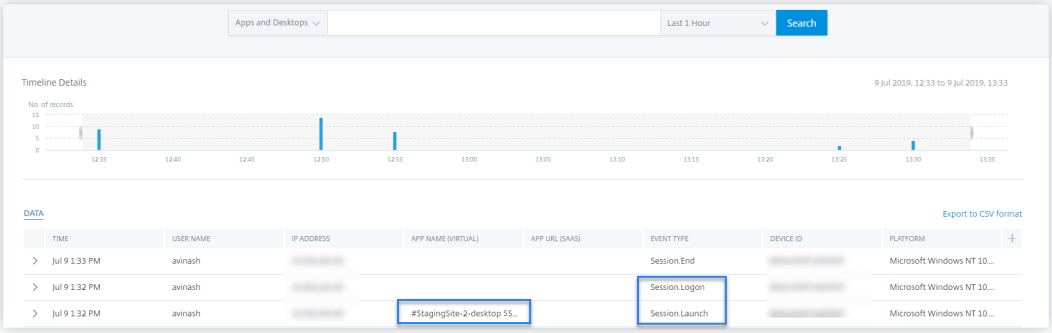
- 应用程序结束

1. 关闭已在工作区或 StoreFront 中启动的计算器。
2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.End** 事件数据的数据。展开该行以查看事件详细信息。



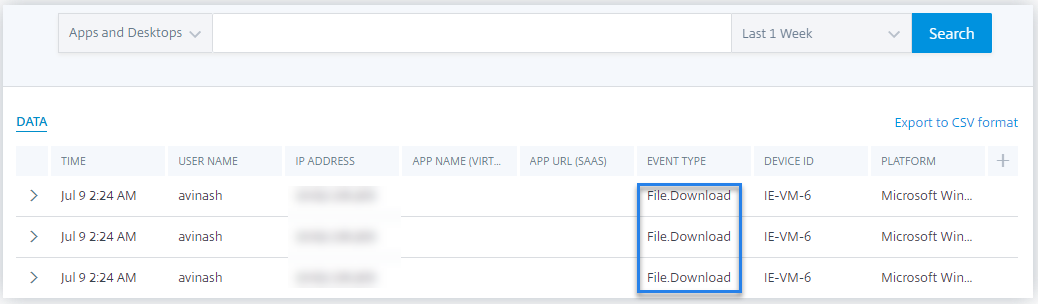
- 会话登录和会话启动

1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
2. 启动虚拟桌面。
3. 转到 Citrix Analytics。
4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 Session.L **ogon** 和 **Session.Launch** 事件的数据。展开该行以查看事件详细信息。



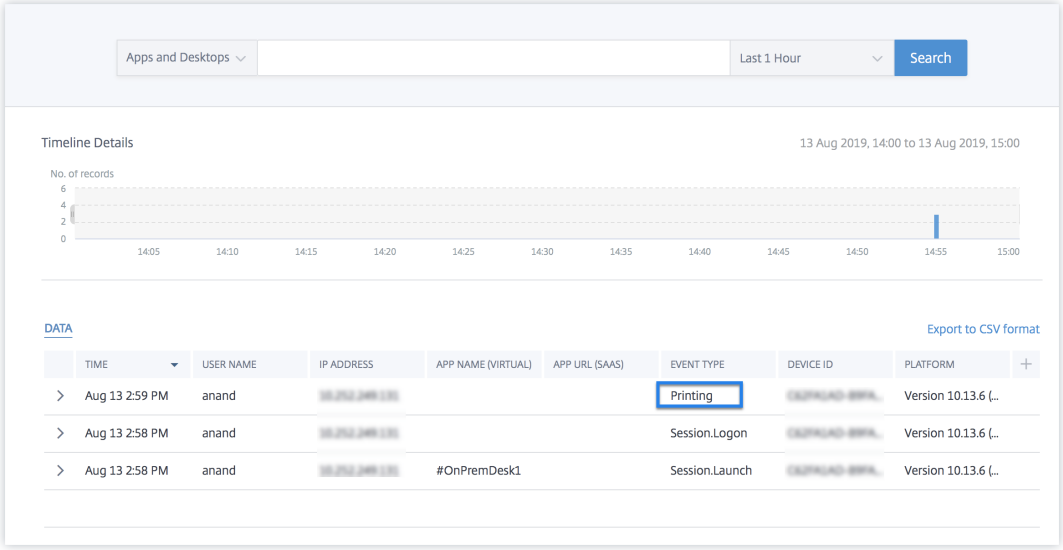
- 文件下载

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront
  2. 启动虚拟桌面。
  3. 将文件从虚拟桌面复制到本地计算机。
  4. 转到 Citrix Analytics。
  5. 单击“搜索”，然后选择“应用程序和桌面”。
  6. 在搜索页面中，查看 **File.Download** 事件的数据。展开该行以查看事件详细信息。



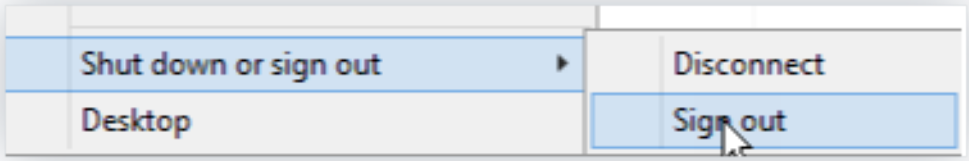
- 打印

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver
  2. 启动虚拟桌面。
  3. 使用配置有虚拟桌面的打印机打印文档。
  4. 转到 Citrix Analytics。
  5. 单击“搜索”，然后选择“应用程序和桌面”。
  6. 在“搜索”页面中，查看“打印”事件的数据。展开该行以查看事件详细信息。

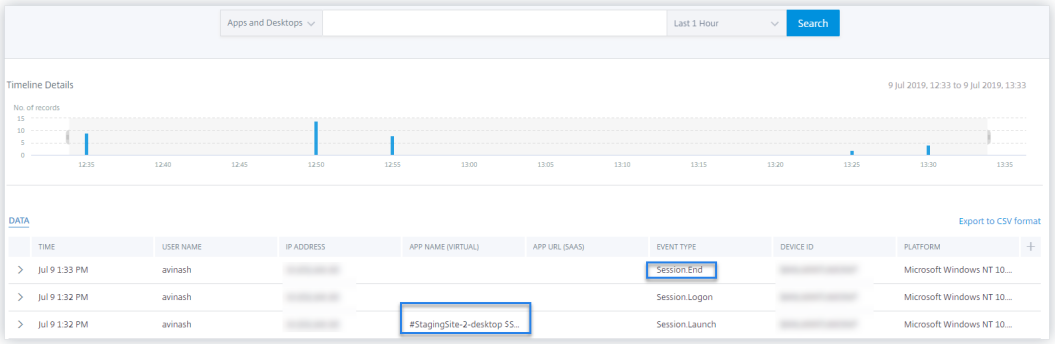


- 会话结束

  1. 从虚拟桌面注销。例如，如果您使用的是 Windows 虚拟桌面，请选择“注销”选项。



  2. 转到 Citrix Analytics。
  3. 单击“搜索”，然后选择“应用程序和桌面”。
  4. 在搜索页面中，查看 S **ession.End** 事件的数据。展开该行以查看事件详细信息。



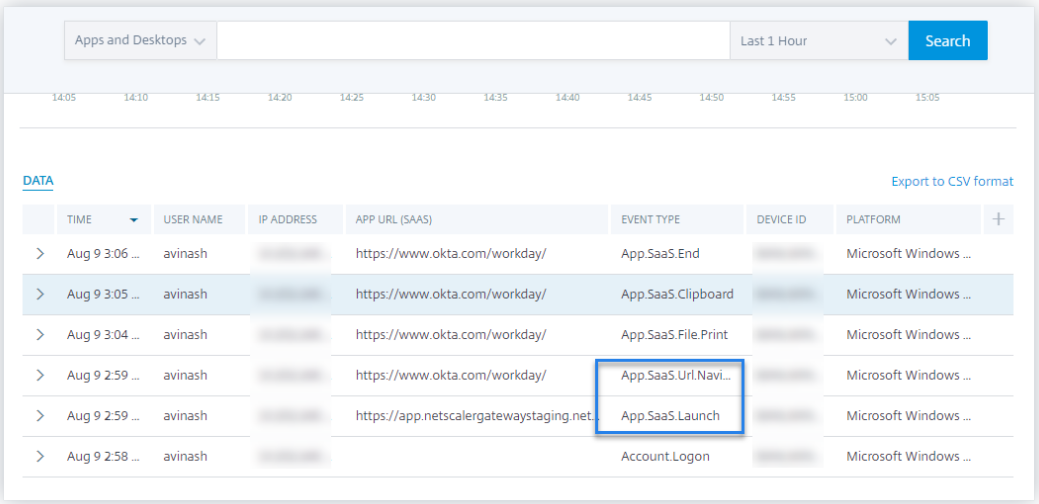
- **SaaS** 应用程序启动和 **SaaS** 应用程序 **URL** 导航

  1. 启动 Citrix Workspace 应用程序或 Citrix Receiver 以访问您的 Workspace 或 StoreFront

2. 启动诸如 Workday 之类的 SaaS 应用程序，然后等待 Workday 页面加载完毕。在 Workday 中浏览网页。

   > 注意
   >
   > 确保在“增强的安全性”部分中禁用了 限制导航 选项。有关更多信息，请参阅 先决条件。

3. 转到 Citrix Analytics。
4. 单击“搜索”，然后选择“应用程序和桌面”。
5. 在搜索页面中，查看 **App.SaaS.Launch** 和 **App.SaaS.URL.Navigation** 事件的数据。展开该行以查看事件详细信息。

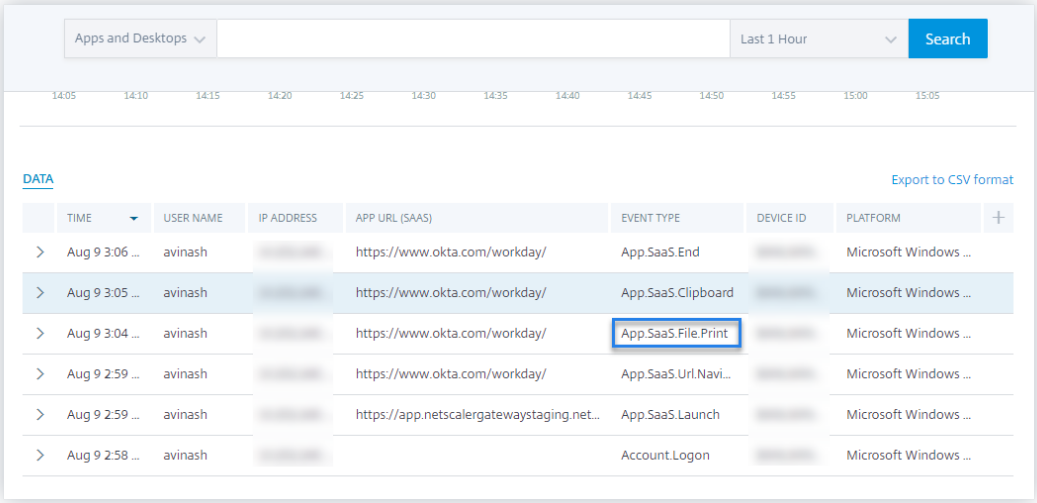


- **SaaS** 应用程序文件打印

1. 打印当前正在查看的 Workday 页面。

   > 注意
   >
   > 确保在增强的安全性部分禁用了 限制打印 选项。有关详细信息，请参阅必备条件。

2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.File.Print** 事件的数据。展开该行以查看事件详细信息。

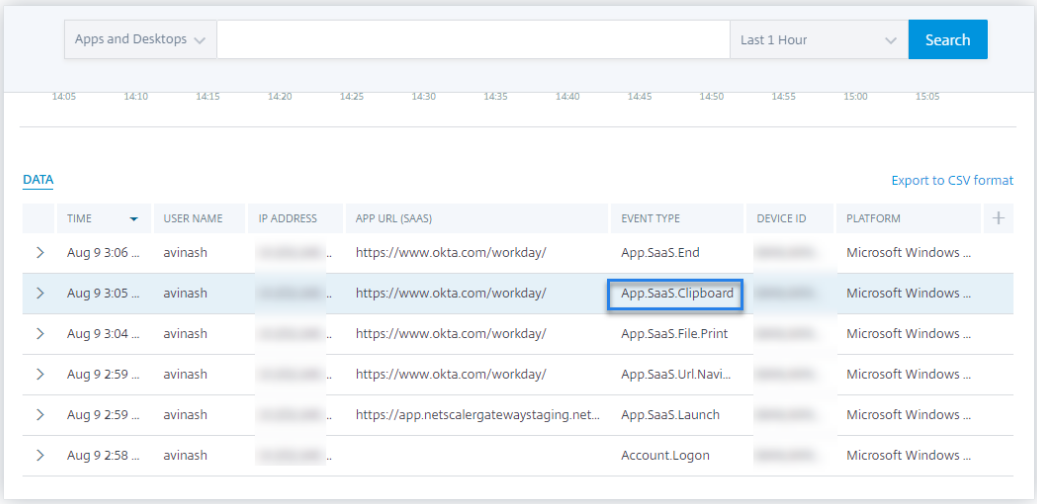


- **SaaS** 应用剪贴板访问

  1. 在 Workday 页面上，将一些文本复制到系统剪贴板。

     > 注意
     >
     > 确保在增强的安全性部分中禁用了 限制剪贴板访问 选项。有关详细信息，请参阅必备条件。

  2. 转到 Citrix Analytics。
  3. 单击“搜索”，然后选择“应用程序和桌面”。
  4. 在搜索页面中，查看 **App.SaaS.Clipboard** 事件的数据。展开该行以查看事件详细信息。

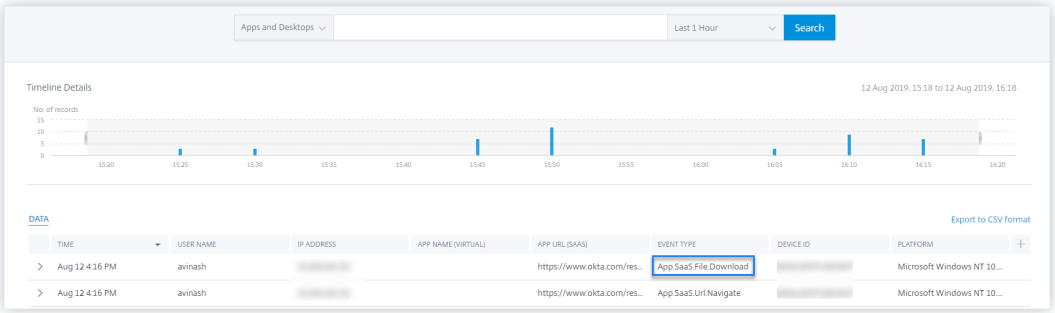


- **SaaS** 应用程序文件下载

  1. 在 Workday 页面上，搜索诸如白皮书之类的公开文档，然后下载该文档。

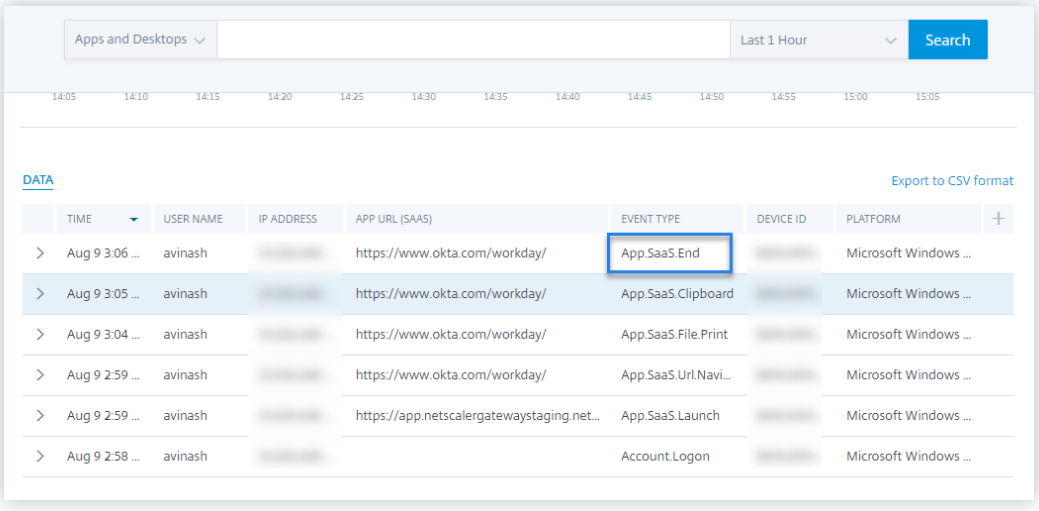
> 注意
>
> 确保在增强的安全性部分禁用了 限制下载 选项。有关详细信息，请参阅必备条件。

2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.File.Download** 事件的数据。展开该行以查看事件详细信息。



- **SaaS** 应用程序结束

1. 关闭“工作日”页面。
2. 转到 Citrix Analytics。
3. 单击“搜索”，然后选择“应用程序和桌面”。
4. 在搜索页面中，查看 **App.SaaS.End** 事件的数据。展开该行以查看事件详细信息。



- **VDA.Print**

  必备条件

  在触发打印事件之前，请参阅为 Citrix DaaS 启用打印遥测。

要触发打印事件，请执行以下操作：

1. 使用记事本或任何其他允许打印的应用程序打开文本文档。
2. 单击“文件”**>**“打印”或按 **Ctrl + P**。
3. 在“选择打印机”中，选择您的打印机，然后单击“应用”，然后打印。

- **VDA.Clipboard**

  必备条件

  在触发打印事件之前，请参阅为 Citrix DaaS 启用剪贴板遥测。

  要触发剪贴板事件，请执行以下操作：

  1. 使用记事本或任何文本编辑器打开文本文档。
  2. 选择要复制的内容。
  3. 右键单击“复制”或按 Ctrl+c。

配置的 **Session Recording Server** 无法连接

July 12, 2022

配置后，Session Recording Server 无法连接到 Citrix Analytics。因此，在 **Session Recording** 站点卡片上看不到已配置的服务器。

要解决此问题，请执行以下操作：

1. 在配置的会话录制服务器上，运行以下 PowerShell 命令以检查客户端计算机标识 (CMID)。

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. 如果 CMID 为空，请在指定的路径中添加以下注册表文件。

注册表名称	注册表路径	注册表项类型	值
AuditorUniqueID	Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\	字符串	输入您的 UUID。

注册表名称	注册表路径	注册表项类型	值
EnableCASUseAuditorComputerID	HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/	REG_DWORD	1

3. 重新启动以下服务：
    - Citrix Session Recording Analytics Service
    - Citrix Session Recording Storage Manager

适用于 **Splunk** 的 **Citrix Analytics** 加载项存在配置问题

July 12, 2022

Citrix Analytics 加载项设置不可用

在您的 Splunk Forwarder 或 Splunk 独立环境中安装适用于 Splunk 的 Citrix Analytics 加载项后，您不会在“设置”**>**“数据输入”下看到 Citrix Analytics 加载项设置。

原因

在不受支持的 Splunk 环境中安装适用于 Splunk 的 Citrix Analytics 加载项时，会出现此问题。

修复

在受支持的 Splunk 环境中安装适用于 Splunk 的 Citrix Analytics 加载项。有关受支持版本的信息，请参阅 Splunk 集成。

Splunk 控制板上没有可用的数据

在 Splunk Forwarder 或 Splunk Standalone 环境中安装和配置适用于 Splunk 的 Citrix Analytics 加载项后，您在 Splunk 控制板中看不到来自 Citrix Analytics 的任何数据。

检查

要解决此问题，请在您的 Splunk 转发器或 Splunk 独立环境中验证以下各项：

1. 确保满足 Splunk 集成的 必备条件 。
2. 转到 设置 **>** 数据输入 **> Citrix Analytics** 加载项。确保 Citrix Analytics 配置详细信息 可用。
3. 如果配置详细信息可用，请运行以下查询以检查日志中是否存在与适用于 Splunk 的 Citrix Analytics 加载项相关的任何错误：

```
index=_internal sourcetype=splunkd log_level=ERROR component=
    ExecProcessor cas_siem_consumer
```

4. 如果您没有发现任何错误，适用于 Splunk 的 Citrix Analytics 加载项将按预期工作。如果在日志中发现任何错误，可能是由于以下原因之一：

   - 无法在您的 Splunk 环境与 Citrix Analytics Kafka 端点之间建立连接。此问题可能是由于防火墙设置造成的。

     修复：请咨询网络管理员以解决此问题。

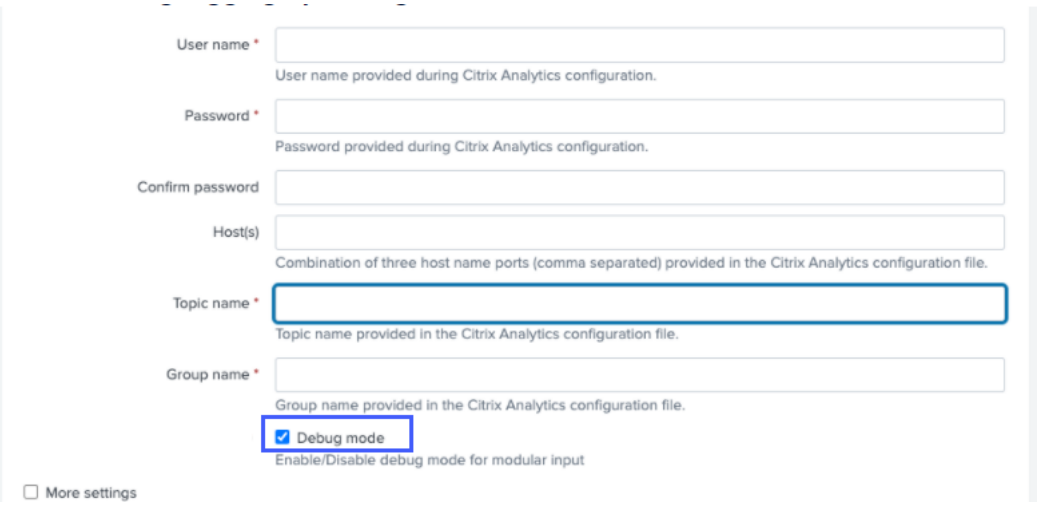
   - 设置 **>** 数据输入 **> Citrix Analytics** 加载项中的配置详细信息不正确。

     修复：确保按照 Citrix Analytics 配置文件正确输入了 Citrix Analytics 配置详细信息，例如用户名、密码、主机端点、主题和使用者组。有关更多信息，请参阅 为 Splunk 配置 Citrix Analytics 加载项。

5. 如果您无法从上述日志中找到问题的原因并希望进一步调查：

   a) 在 设置 **>** 数据输入 **> Citrix Analytics** 加载项 中启用 调试模式。

   > 注意
   >
   > 默认情况下，调试模式处于 禁用状态。启用此模式会生成太多日志。因此，请仅在需要时使用此选项，并在完成调试任务后将其禁用。



b) 在以下位置找到生成的调试日志，并检查是否有任何错误：

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c)（可选）使用适用于 Splunk 的 Citrix Analytics 加载项提供的调试脚本 `splunk cmd python cas_siem_consumer_debug.py`。此脚本生成一个日志文件，其中包含您的 Splunk 环境和连接检查的详细信息。您可以使用详细信息来调试问题。使用以下命令运行脚本：

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

错误消息

在与适用于 Splunk 的 Citrix Analytics 加载项相关的日志中，您可能会看到以下错误：

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

此错误是由于网络连接问题或身份验证问题造成的。

要调试问题，请执行以下操作：

1. 在您的 Splunk 转发器或 Splunk 独立环境中，启用调试模式以获取调试日志。请参考前面的步骤 5.a。
2. 运行以下查询以查找调试日志中的任何身份验证问题：

```
index=_internal source="*
    splunk_citrix_analytics_add_on_debug_connection.log*" "
    Authentication failure"
```

3. 如果在调试日志中未发现任何身份验证问题，则该错误是由于网络连接问题造成的。
4. 使用 telnet 或前面的步骤 5.c 中提到的调试脚本查找并解决问题。

从低于 **2.0.0** 的版本升级加载项失败

在您的 Splunk 转发器或 Splunk 独立环境中，当您将适用于 Splunk 的 Citrix Analytics 加载项从 2.0.0 之前的版本升级到 最新 版本时，升级将失败。

修复

1. 删除适用于 Splunk 的 Citrix Analytics 加载项安装文件夹的 `/bin` 文件夹的以下文件和文件夹：
   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
   - `rm -rf splunklib`

- `rm -rf mac`
- `rm -rf linux_x64`
- `rm CARoot.pem`
- `rm certificate.pem`

2. 重启您的 Splunk 转发器或 Splunk 独立版环境。

无法将 **StoreFront** 服务器与 **Citrix Analytics** 连接

January 5, 2023

将配置设置从 Citrix Analytics 导入到 StoreFront 服务器后，StoreFront 服务器无法连接到 Citrix Analytics。

有关如何将配置设置导入到 StoreFront 服务器的信息，请参阅 使用 StoreFront 的登录 Virtual Apps and Desktops 站点。

CAS 登录助手可帮助检查和解决本文中描述的问题。有关更多信息，请参阅 Citrix Analytics Service (CAS) 登录助手。

要解决此问题，请执行以下操作：

1. 在 StoreFront 服务器上，ping Citrix Analytics 的 特定于区域的端点 以测试 StoreFront 服务器与 Citrix Analytics 服务器之间的连接。此外，请确保 满足必备条件 。

   > 注意
   >
   > 在 StoreFront 服务器上，您可以通过直接 ping 区域特定的终端节点或打开 Web 浏览器并访问特定于区域的终端节点来测试连通性。

2. 在 StoreFront 服务器中启用详细日志记录以跟踪日志。有关详细日志记录的详细信息，请参阅文章-CTX139592。
3. 打开互联网信息服务 (IIS) 管理器并检查以下内容：
   - 如果 StoreFront 站点位于 IIS 默认站点下，则 IIS 会重新启动 StoreFront 站点。
   - 如果 StoreFront 站点位于其他驱动程序中或不在默认站点下，请打开命令窗口并键入 `iisreset`。
4. 运行以下命令以导入 Citrix Analytics 设置：

```
Import-STFCasConfiguration -Path "configuration file path"
```

5. 运行以下命令验证导入的设置：

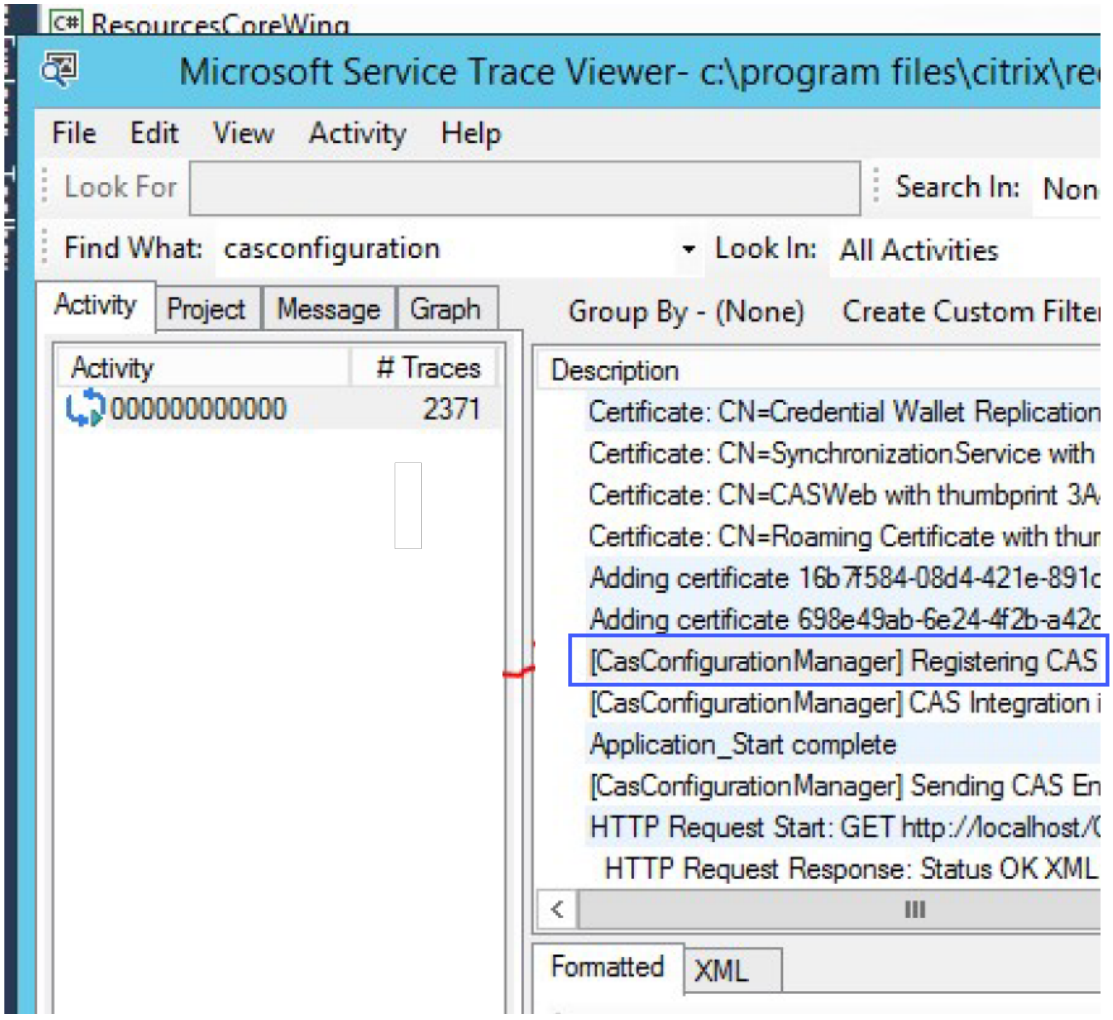
```
Get-STFCasConfiguration
```


6. 如果 StoreFront 站点位于其他驱动程序中或不在默认站点下，请打开命令窗口。键入 `iisreset` 以让 StoreFront 站点读取 Citrix Analytics
7. 从以下位置获取 StoreFront 详细日志文件：

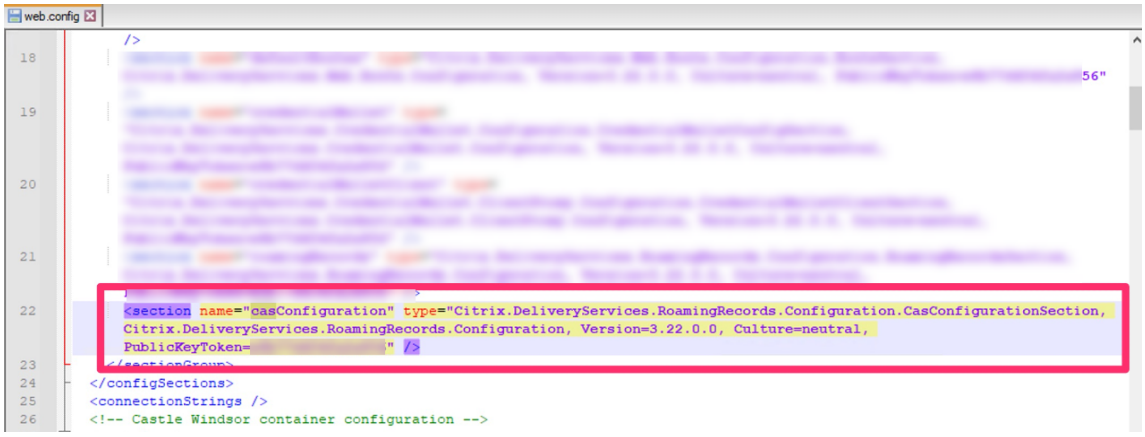
```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   在上述位置下，您可以找到多个 svclog 文件，这些文件可以在事件查看器中打开。

8. 使用 Microsoft 服务跟踪查看器打开以下日志：
   - StoreFront 日志
   - 漫游站点详细日志
9. 在日志中，确保 **casConfigurationManager** 部分和 Citrix Analytics 服务器信息可用。



10. 如果 casConfigurationManager 部分不可用，请打开在 `roaming site\folder` 中找到的漫游站点的 web.config 文件。
11. 在 `web.config` 文件中，找到 **casConfiguration** 部分，并确保 Citrix Analytics 服务器信息可用。



12. 在安装了 StoreFront 服务器的 Windows Server 计算机上，请确保满足以下条件：

    - TLS 1.2 客户端已启用。
    - 至少启用了以下密码套件之一：
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
        - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

    有关如何配置 TLS 密码套件顺序的信息，请参阅 Microsoft 文档。

13. 如果您使用的是 Windows Server 2012 计算机，请确保已启用 Diffie-Hellman Exchange (ECDHE/DHE)。

14. 确保安装了 StoreFront 服务器的 Windows Server 计算机必须包含 Microsoft 文档中提到的注册表设置。

    > 重要
    >
    > 说明使用组策略更新 TLS/SSL 密码套件。请勿手动修改 TLS/SSL 密码套件。有关如何使用组策略的更多信息，请参阅 Microsoft 文档。

    例如，以下注册表设置必须在 Windows Server 计算机中可用：

    TLS 1.2 客户端：

    ```
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
       SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
    "Enabled"=dword:00000001
    [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
       SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
    "DisabledByDefault"=dword:00000000

    <!--NeedCopy-->
    ```

    Diffie-Hellman KEA:


```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
    ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

AES-128/AES-256 密码：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

SHA256/SHA384 哈希：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff

<!--NeedCopy-->
```

常见问题解答

November 26, 2023

数据源

什么是数据源

数据源是向 Citrix Analytics 发送数据的 Citrix 服务和产品。

了解更多：数据源

如何添加数据源

登录 Citrix Analytics 后，在 欢迎屏幕上，选择入门以将数据源添加到 Citrix Analytics 中。或者，您也可以通过导航设置 **>** 数据源来添加数据源。

Citrix ADM 代理

在本地虚拟机管理程序上安装代理的最低资源要求是多少

8 GB RAM、4 个虚拟 CPU、120 GB 存储空间、1 个虚拟网络接口、1 Gbps 吞吐量

预配时是否需要向 **Citrix ADM** 代理分配额外的磁盘

不需要，您不必再添加磁盘。该代理仅用作 Citrix Analytics 与企业数据中心中的实例之间的中介。它不存储需要额外磁盘的库存或分析数据。

登录代理的默认凭据是什么

登录到代理的默认凭据是 `nsrecover`/`nsroot`。这会将您登录到代理的 shell 提示符。

如果我输入的值不正确，如何更改代理的网络设置

登录到虚拟机管理程序上的代理控制台，使用凭据 `nsrecover`/`nsroot` 访问 shell 提示符，然后运行命令 `networkconfig`。

为什么我需要服务 **URL** 和激活码

代理使用服务 URL 查找服务，使用激活码向服务注册代理。

如果我在代理控制台中输入的服务 **URL** 不正确，如何才能重新输入服务 **URL**

使用凭据 `nsrecover`/`nsroot` 登录到代理的 shell 提示符，然后键入 `deployment_type.py`。此脚本允许您重新输入服务 URL 和激活码。

如何获得新的激活码

您可以从 Citrix ADM 服务获取新的激活码。登录 Citrix ADM 服务并导航到网络 **>** 代理。在代理页上的选择操作列表中，选择生成激活码。

我可以使用多个代理重复使用激活码吗**?**

不，您不能。

我需要安装多少 **Citrix ADM** 代理

代理的数量取决于数据中心中托管实例的数量和总吞吐量。Citrix 建议您为每个数据中心至少安装一个代理。

如何安装多个 **Citrix ADM** 代理

在“数据源”页面上，单击 Citrix Gateway 旁边的加号 (+)，然后按照说明安装其他代理。

或者，您可以访问 Citrix ADM GUI 并导航到“网络”>“代理”，然后单击安装代理以安装多个代理。

我能否在高可用性设置中安装两个代理

不，您不能。

如果我的代理注册失败，我该怎么办**?**

- 确保您的代理可以访问互联网（配置 DNS）。
- 确保您已正确复制激活码。
- 确保您已正确输入服务 URL。
- 确保您已打开所需的端口。

注册成功，但如何知道代理是否正常运行呢

您可以执行以下操作来检查代理是否运行正常：

- 成功注册代理后，访问 Citrix ADM 并导航到网络 **>** 代理。您可以在此页面上查看发现的代理。如果代理运行正常，则状态由绿色图标表示。如果它未运行，则状态由红色图标表示。
- 登录到代理的 shell 提示符并运行以下命令：`ps -ax | grep mas` 和 `ps -ax | grep ulfd`。确保以下进程正在运行。

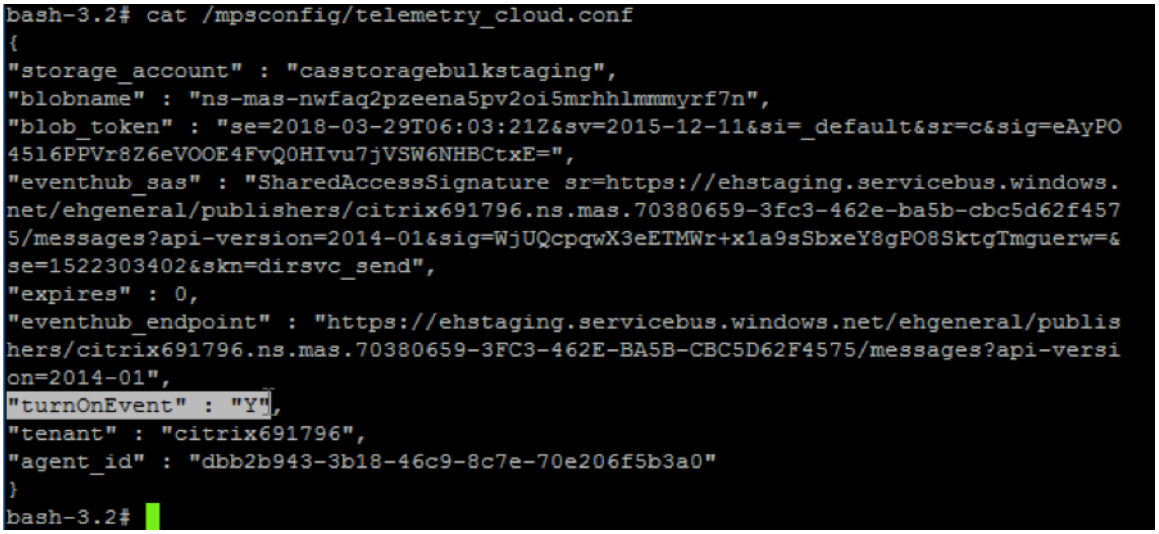
- 如果有任何进程未运行，请运行命令 **masd restart**。启动所有守护程序可能需要一些时间（1 分钟左右）。
- 成功注册代理后，确保在 /mpsconfig 中创建 agent.conf。

管理 Citrix Gateway 实例

Citrix Gateway 实例已添加到 **Citrix Analytics** 中，但我如何知道代理程序上是否启用了分析

您可以使用代理的 shell 提示符验证是否在代理上启用了分析。如果在代理上成功启用分析，则 /mpsconfig/telemetry_cloud.conf 文件中的 turnOnEvent 参数将设置为 Y。

登录到代理的 shell 提示符并运行以下命令：cat /mpsconfig/telemetry_cloud.conf 并验证 turnOnEvent 参数的值。



我不小心关闭了 **Citrix Gateway** 入门向导。我必须从头开始配置吗

不是。Citrix Analytics 会保存进度，并将未完成的配置显示为 数据源 **>** 设置 页面中的磁贴。单击继续设置以完成配置。

Virtual Apps and Desktops 入门网站

如何关闭数据处理

如果要暂时禁用从站点到 Citrix Analytics 的数据处理，只需单击 站点 卡，然后单击 关闭数据处理即可。

将站点添加到 **Workspace** 并单击“测试 **STA**”时，测试失败。我该怎么做

您的 Citrix Gateway 和 Cloud Connector 之间可能存在连接问题。要进行故障排除，请参阅 Citrix 支持知识中心中的 CTX232517 。

我在哪里可以获得有关 **Citrix Analytics** 的帮助

您可以在 Citrix Analytics 讨论论坛（网址为 https://discussions.citrix.com/forum/1710-citrix-analytics/）上提问并与 Citrix Analytics 专家联系。

要参与论坛，您必须使用您的 Citrix ID 登录。

访问保障-地理定位

Analytics 是如何推导出地理位置详细信息的

Citrix Analytics 使用从其启动 Workspace 客户端的设备的 IP 地址。Citrix Analytics 利用第三方 IP 地理位置数据提供商从用户的 IP 地址中获取用户的位置。当您执行会话登录时，它会将您的位置（IPv4 地址）解析为国家或城市，并且映射会定期更新。组织可以使用这些由国家/地区定义的地点来监视他们不开展业务的地方的访问模式。

推导用户位置的准确度是多少

Citrix Analytics 利用第三方 IP 地理位置数据提供商从用户的 IP 地址中获取用户的位置。大多数情况下，GeoIP 服务都能够解析到正确的城市或位置，但 GeoIP 查找从来都不是完全准确的。有时，为用户显示的位置可能与其访问的确切位置不同。

根据 IP GeoPoint 文档，覆盖级别约为全球分配的 IP 地址（IPv4 可路由 IP 地址）的 99.99%。就位置精度而言，它在每个基本位置字段（国家、州、城市、邮政编码）中都附有置信因子。

在哪些情况下，位置的确定不准确

地理位置数据的准确性取决于设备连接到互联网的方式。设备可以通过以下方式连接到互联网：

- 移动网关

- VPN 或托管设施
- 区域或国际代理/匿名服务器

在这种情况下，无论使用 IP 地理位置提供商软件如何，地理位置数据都不准确。

支持的 **Citrix Workspace** 应用程序版本是什么

将 **IP** 地址属性发送到 Citrix Analytics for Security 时，操作系统对 Citrix Workspace 应用程序的最低版本有要求。有关更多详细信息，请参阅 矩阵表 或 标识为不可用的位置 。

在哪些情况下，我们不会收到地质详细信息

要查看地理位置详细信息，请参阅 标识为不可用的位置 部分以了解详细信息。

Citrix Analytics 使用哪种地理位置服务来报告用户的位置？如何报告错误的 **IP** 位置

Citrix Analytics 使用 基于 Neustar 文件的地理定位服务 为传入访问提供地理位置数据。它有一个面向公众的 IP 更正页面，可用于自行提交更正请求。提交更正请求后，Neustar 将审核该请求的准确性并进行处理。

GeoIP 提供程序有助于显示尽可能准确的信息。遗憾的是，在某些情况下，由于 GeoIP 的固有特性，GeoIP 数据可能不准确。

术语表

April 12, 2024

- 操作：对可疑事件的闭环响应。应用操作以防止将来发生异常事件。了解更多。
- **Cloud Access** 安全代理 **(CASB)**：位于云服务使用者和云服务提供商之间的本地或基于云的安全策略执行点。在访问基于云的资源时，CASB 会合并和插入企业安全策略。它们还可以帮助组织将其内部基础设施的安全控制扩展到云中。
- **Citrix ADC**（应用程序 **Delivery Controller**）：位于数据中心的网络设备，战略性地位于防火墙与一台或多台应用程序服务器之间。处理服务器之间的负载平衡，并优化企业应用程序的最终用户性能和安全性。了解更多。
- **Citrix ADM**（应用程序交付管理）：集中式网络管理、分析和编排解决方案。管理员可以在单个平台上查看、自动化和管理横向扩展应用程序架构的网络服务。了解更多。
- **Citrix ADM** 代理：支持 Citrix ADM 与数据中心中的托管实例之间进行通信的代理。了解更多。
- **Citrix Analytics**：跨服务和产品（本地和云）收集数据并生成切实可行的见解的云服务，使管理员能够主动处理用户和应用程序安全威胁，提高应用性能并支持持续运营。了解更多。

- **Citrix Cloud**：通过任何云或基础架构（本地、公有云、私有云或混合云）上的 Citrix Cloud Connector 连接到资源的平台。了解更多。
- **Citrix Gateway**：整合了远程访问基础架构的整合远程访问解决方案，以提供跨所有应用程序的单点登录，无论是在数据中心、云中还是作为 SaaS 交付。了解更多.
- **Citrix Hypervisor**：针对应用程序、桌面和服务器虚拟化基础架构进行了优化的虚拟化管理平台。了解更多。
- **Citrix Workspace** 应用程序（以前称为 Citrix Receiver）：客户端软件，可通过任何设备（包括智能手机、平板电脑、个人电脑和 Mac）无缝、安全地访问应用程序、桌面和数据。了解更多。
- **DLP**（数据丢失防护）：描述一组技术和检查技术的解决方案，用于对对象（如文件、电子邮件、数据包、应用程序或数据存储）中包含的信息进行分类。此外，对象还可以在存储中、使用中或通过网络存储。DLP 工具可以动态应用日志、报告、分类、重新定位、标记和加密等策略。DLP 工具还可以应用企业数据权限管理保护。了解更多。
- **DNS**（域名系统）：用于查找互联网域名并将其转换为互联网协议（IP）地址的网络服务。DNS 将用户提供的网站名称映射到机器提供的相应的 IP 地址，以定位网站，而不管实体的物理位置如何。
- 数据处理：将数据源中的数据处理到 Citrix Analytics 的方法。了解更多。
- 数据源：向 Citrix Analytics 发送数据的产品或服务。数据源可以是内部数据源，也可以是外部数据源。[了解更多] /zh-cn/citrix-analytics/data-sources.html)。
- 数据导出：从 Citrix Analytics 接收数据并提供见解的产品或服务。了解更多。
- 发现的用户：组织中使用数据源的用户总数。了解更多。
- **FQDN**（完全限定域名）：用于内部 (StoreFront) 和外部 (Citrix ADC) 访问的完整域名。
- 机器学习：一种数据分析技术，无需明确编程即可提取知识。来自各种潜在来源（例如应用程序、传感器、网络、设备和设备）的数据被输入到机器学习系统中。系统使用数据并应用算法来构建自己的逻辑来解决问题、获得见解或做出预测。
- **Microsoft Graph** 安全性：连接客户安全和组织数据的网关。在必须采取措施时提供易于查看的警报和补救选项。了解更多。
- 性能分析：提供组织内用户会话详细信息可见性的服务。了解更多。
- 策略：对用户的风险配置文件应用操作所要满足的一组条件。了解更多。
- 风险指示器：提供有关组织在给定时间面临的业务风险程度的信息的指标。了解更多。
- 风险评分：动态值，表示用户或实体在预先确定的监视期内对 IT 基础架构构成的总体风险水平。了解更多。
- 风险时间表：记录用户或实体的风险行为，允许管理员调查风险概况并了解数据使用情况、设备使用情况、应用程序使用情况和位置使用情况。了解更多。
- 有风险的用户：以危险方式行事或表现出危险行为的用户。了解更多。
- 安全分析：对数据进行高级分析，用于实现令人信服的安全成果，例如安全监视和威胁追踪。了解更多。
- **Secure Private Access**：该服务将单点登录、远程访问和内容检查集成到单个解决方案中，以实现端到端访问控制。了解更多。

- **Splunk**：SIEM（安全信息和事件管理）软件，用于接收来自 Citrix Analytics 的智能数据，并提供有关潜在业务风险的见解。了解更多。
- **UBA**（用户行为分析）：将用户活动和行为与对等组分析相结合的基准化过程，以检测潜在的入侵和恶意活动。
- 监视列表：管理员希望监视可疑活动的用户或实体的列表。了解更多。