Citrix Cloud

Contents

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud

July 1, 2024

> 注意：
>
> Citrix Virtual Apps Essentials 和 Citrix Virtual Desktops Essentials 已达到销售终止和生命周期结束状态。有关详细信息，请参阅 CTX583004。

Citrix Cloud 是一个托管和管理 Citrix 云服务的平台。它通过您选择的任何云或基础架构（本地、公共云、私有云或混合云）上的 连接器 连接到您的资源。在 Citrix Cloud 中，您可以从单个控制台为最终用户创建、管理和部署包含应用程序和数据的工作区。

新增功能

访问 Citrix Cloud 更新，及时了解 Citrix Cloud 中的新增功能和即将推出的功能以及以下服务：

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

试用 **Citrix Cloud**

在一项或多项 Citrix Cloud 服务的概念证明中体验完整的生产环境。注册 Citrix Cloud后，您可以直接在控制台中请求服务试用。试用结束时，可以转换为生产环境，以便保留所有配置。有关详细信息，请参阅 Citrix Cloud 服务试用版。

Citrix Cloud 服务文档

正在寻找有关设置或管理 Citrix Cloud 服务的信息？前往 Citrix Cloud 服务，查找指向所有云服务的产品文档的链接。

架构和部署资源

Citrix Tech Zone 包含大量信息，可帮助您了解有关 Citrix Cloud 和其他 Citrix 产品的更多信息。在这里，您可以找到参考架构、图表和技术论文，这些文件为设计、构建和部署 Citrix 技术提供了见解。

要了解有关 Citrix Cloud 中关键服务组件的更多信息，请参阅以下资源：

- Citrix Workspace 概念图：提供关键领域的概述，例如身份、工作区智能和单点登录。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 参考体系结构：为规划 Citrix Workspace 实施提供全面的指南，包括使用案例、建议和相关资源。
- Citrix DaaS 参考体系结构：提供有关使用相关服务部署 Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）的深入指导。

教育资源

C itrix 云学习系列门户 提供教育模块，帮助您开始使用 Citrix Cloud 及其服务。您可以按顺序查看所有模块，从概览到规划和建筑服务。通过以下课程开始您的云之旅：

- Citrix Cloud 基础知识
- Citrix 身份和身份验证简介
- 从 StoreFront 迁移到工作区

Citrix Education 视频库 提供在线视频课程，引导您完成关键的部署任务以及对 Citrix Cloud 服务使用的组件进行故障排除。详细了解安装 Cloud Connector 和注册 VDA 以及对这些组件进行故障排除等任务。

服务级别协议

July 1, 2024

生效日期：2020 年 10 月 30 日

Citrix Cloud 采用行业最佳实践进行设计，以实现高度的服务可用性。

本服务等级协议 (SLA) 描述了 Citrix 对 Citrix Cloud 服务可用性的承诺。本 SLA 是 Cloud Software Group 针对涵盖的服务（下称“本服务”）的最终用户协议 (EULA) 的一部分。

Citrix 的服务承诺（下称“服务承诺”）是将服务的每月正常运行时间保持至少 99.9%（“每月正常运行时间”）。每月正常运行时间的计算方法是从 100% 中减去服务实例处于“不可用”状态的整整一个月内的分钟百分比。下表列出了服务和每种服务的可用性衡量标准。每月正常运行时间百分比测量不包括以下原因导致的停机时间：

- 定期安排维护窗口。
- 客户未能遵守 https://docs.citrix.com 上记录的服务配置要求，或者滥用行为或错误输入。
- 在 Citrix 建议客户修改服务使用情况后，如果客户未修改使用服务，则客户对服务的使用。
- 由非 Citrix 管理的任何组件引起，包括但不限于客户控制的物理机和虚拟机、客户安装和维护的操作系统、客户安装和控制的软件、网络设备或其他硬件；客户定义和控制的安全设置、组策略和其他配置策略；公共云提供商故障、Internet 服务提供商故障；或 Citrix 控制之外的其他客户支持因素。
- 客户的员工、代理人、承包商或供应商，或任何通过客户的密码或设备获得访问权限的人，或者由于客户未能遵守适当的安全措施而导致的其他访问权限的人。
- 客户尝试执行超出服务权限的操作。
- 不可抗力导致的服务中断，包括但不限于自然灾害、战争或恐怖行为或政府行为。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

任何 Citrix 试用版、技术预览版、Labs 或 Beta 服务均不提供服务承诺。

Citrix 向客户提供以下服务承诺：

- 已使用基于期限的订阅（最短订阅期限为 1 年）购买服务。
- 在声明期内，根据适用于服务的许可证模式，至少订阅 100 个单位（Citrix Service Provider 的最低订阅量为 1000 个）。

Citrix Service Provider (CSP) 将于 2018 年 10 月 1 日获得资格。

每项服务的可用性衡量标准

服务	衡量每月正常运行时间
Citrix Analytics for Performance	用户可以访问应用程序和桌面并提高其性能的时间。
Citrix Analytics for Security	用户可以检测和缓解用户访问和活动风险的时间。
NetScaler 控制台服务	服务在所有 POP 上可用的平均时间。
Citrix Endpoint Management	用户可以通过该服务访问其 Citrix 交付的移动应用程序和注册设备的时间。
适用于 HDX 代理的 Citrix Gateway 服务	用户可以通过该服务访问其应用程序或桌面会话的时间。
NetScaler Intelligent Traffic Management	时间用户可以通过 DNS 查询或 HTTP API 调用访问流量管理功能。
NetScaler SD-WAN Orchestrator	Time 用户可以通过该服务访问他们的 SD-WAN Orchestrator 帐户并管理他们的 SD-WAN 网络。
Citrix Secure Private Access	时间用户可以通过该服务访问其 SaaS 或内部 Web 应用程序。
Citrix DaaS	用户可以通过该服务访问其应用程序或桌面会话的时间。
Citrix Workspace	与上述组件服务相同，但包括每种服务的可用性。如果索赔涉及的部分少于所有部分，则可以按比例分配积分。

> 注意：
>
> Citrix DaaS 是 Citrix Virtual Apps 服务、Citrix Virtual Desktops 服务以及 Citrix Virtual Apps and Desktops 服务的新名称。

服务承诺和补救措施

如果 Citrix 在 SLA 生效之日当天或之后的任意 5 个月中至少有 3 个月未能兑现服务承诺，则唯一的补救措施是，对于 Citrix 未能履行服务承诺的月份，按月发放 10% 的服务抵免额，适用于客户在即时续订期内的下一次年度服务延期，适用于受影响的相同服务和相同数量的单位的下一次年度服务延期。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 每月正常运行时间百分比：> 99.9%
- 服务积分：适用月份可享受 10%的折扣（作为优惠券提供给客户）

要获得上述补救措施，客户必须遵守 EULA，并且客户必须在连续五个月提出信用索赔的最后一个月结束后的三十 (30) 天内报告故障。有关报告可能违反本 SLA 的说明，请参阅 CTX237141。

请求必须标识服务，定义不可用的日期、时间和持续时间，以及证实不可用的支持日志或记录，并确定受影响的用户及其位置，以及请求的任何技术支持或实施的补救措施。在适用的月数内，每项服务只能发放一个服务积分，延期的所有月份最多可获得 10% 的服务积分。客户在购买延期时必须出示优惠券。

如果您通过经销商购买扩展，您将通过经销商获得积分。我们为直接购买申请的积分，或转给您的经销商进行间接购买的积分，将基于相同数量商品的延期按比例分配的混合建议零售价。Citrix 不控制转售定价或转售积分。积分不包括应付给 Citrix 或经销商的款项的抵消权。Citrix 偶尔会更新这些条款。更新时，Citrix 还将修改服务级别协议顶部的发布日期。任何更改仅适用于您在当前发布日期当天或之后购买的新服务或服务扩展。

第三方声明

November 8, 2023

- Citrix Cloud 第三方通知 (PDF)
- Citrix Analytics 服务第三方通知 (PDF)
- Citrix DaaS 第三方通知 (PDF)
- Citrix DaaS Standard for Azure 第三方通知 (PDF)
- Remote Browser Isolation（以前称为 Secure Browser） (PDF)
- Citrix Endpoint Management 第三方通知 (PDF)
- Citrix Cloud Linux VDA Image Service 第三方通知 (PDF)
- 适用于云服务的 Connector Appliance 第三方声明 (PDF)
- Citrix Gateway 服务第三方通知 (PDF)
- Citrix 设备状态服务第三方声明 (PDF)

> 注意：
>
> Citrix DaaS 以前称为 Citrix Virtual Apps and Desktops 服务。适用于 Azure 的 Citrix DaaS Standard 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard。

如何获得帮助和支持

July 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本文介绍在创建帐户或登录 Citrix Cloud 或其他 Citrix 网站时遇到问题时如何进行故障排除和获得帮助。本文还包括其他自助资源和指导支持选项。

> 重要：
>
> 如果您在登录 Citrix 网站或注册多重身份验证 (MFA) 时遇到问题，请先查看本文以获取故障排除资源。如果这些资源不能帮助您解决问题，请通过 https://www.citrix.com/contact/customer-service.html 联系 Citrix Customer Service。

创建帐户

需要 Citrix 帐户才能访问 Citrix 网站上的某些资源，例如 Citrix 讨论论坛、培训课程、某些产品下载和 Citrix 技术支持。

要为您的公司创建新的 Citrix 帐户，请使用以下方法之一与 Citrix 联系：

- 请联系 Citrix Customer Service。
- 联系您所在地区的 Citrix Partner 或 Citrix Sales 办事处。

如果您已经拥有 Citrix 帐户，则可以创建 Citrix Cloud 帐户，然后完成创建 Citrix Cloud 帐户中描述的任务，完成载入流程。

如果您在注册 Citrix Cloud 时遇到问题，请联系 Citrix Customer Service。

登录 **Citrix** 网站和 **Citrix Cloud**

如果您在使用 Citrix 帐户登录 Citrix 网站时遇到问题，请使用以下资源进行故障排除：

- CTX228792：解决 Citrix 网站上的登录问题
- CTX283814：设置 Citrix 帐户后出现登录问题

登录我的 **Citrix** 帐户时，我无法设置 **MFA** 或者无法使用 **MFA** 进行身份验证

有关故障排除信息，请参阅以下文章：

- CTX461297: How to Enroll into Multi Factor Authentication (MFA)（CTX461297：如何注册多重身份验证 (MFA)）
- CIX463758: How to recover access to your account（CIX463758：如何恢复对您帐户的访问权限）

如果您仍然无法使用 MFA 登录，请通过 https://www.citrix.com/contact/customer-service.html 与 Citrix Customer Service 部门联系。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如何找到我的 **Citrix** 帐户用户名或重置我的 **Citrix** 密码

使用以下步骤验证您的 Citrix 帐户用户名并重置密码。

1. 访问 https://www.citrix.com/welcome/request-password.html。
2. 要验证您的 Citrix 帐户用户名，请执行以下操作：
   a) 在“查找我的帐户依据”下，选择“电子邮件”。
   b) 输入与您的 Citrix 帐户关联的电子邮件地址。
3. 要重置您的 Citrix 帐户密码，请执行以下操作：
   a) 在“查找我的帐户依据”下，选择 用户名。
   b) 输入您的 Citrix 帐户用户名。
4. 单击“查找我的帐户”。

如果 Citrix 使用您的电子邮件地址找到了您的帐户，Citrix 会向您发送一封电子邮件，其中包含与您的电子邮件地址关联的用户名和公司名称。如果 Citrix 发现您的帐户使用您的 Citrix 用户名，Citrix 会向您发送一封电子邮件，其中包含有关重置密码的说明。

如果您在几分钟后仍未收到电子邮件，请参阅本文中我的电子邮件收件箱中未显示 Citrix 电子邮件。

我无法登录 **Citrix Cloud**

- 请确保使用正确的帐户凭据登录。要验证您的帐户用户名，请访问 https://citrix.cloud.com/，选择忘记了用户名**?**，然后输入您的电子邮件地址。Citrix 会向您发送一封包含您的帐户用户名的电子邮件。
- 您可能需要重置密码。如果您最近未登录或密码不够强大，Citrix Cloud 会提示您更改密码。有关更多信息，请参阅本文中的 更改密码 。
- 您可能需要使用自定义登录 URL 登录。如果您的 Citrix Cloud 帐户使用 Azure AD、Google Cloud Identity 或 SAML 对管理员进行身份验证，请选择使用我的公司凭据登录，然后输入贵公司的登录 URL。然后可以输入您的公司凭据以访问贵公司的 Citrix Cloud 帐户。如果您不知道贵公司的登录 URL，请联系贵公司的管理员以获得帮助。

如果您仍然无法登录 Citrix Cloud，请联系 Citrix Customer Service。

Citrix 电子邮件未出现在我的电子邮件收件箱中

当 Citrix 向您发送电子邮件以验证您的 MFA 身份时、查找您的 Citrix 帐户或更改密码时，电子邮件通常会在几分钟内送达。如果您没有收到这些电子邮件：

- 检查为您的 Citrix 帐户注册的电子邮件地址，并验证其是否正确。如果您最近更改了电子邮件地址，则验证电子邮件可能会发送到您的旧地址。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 该电子邮件可能被意外过滤了。检查电子邮件客户端中的垃圾邮件和垃圾文件夹。您也可以在电子邮件帐户中搜索来自 donotreplynotifications@citrix.com 或 cloud@citrix.com 的电子邮件。
- 您的防火墙可能已阻止该电子邮件。确保将以下地址列为可信发件人：
  - donotreplynotifications@citrix.com
  - cloud@citrix.com
  - CustomerService@citrix.com

如果几分钟后仍未收到电子邮件，或者在登录时遇到其他问题，请联系 Citrix Customer Service。

Citrix 和 Citrix Cloud 帐户的多因素身份验证

Citrix 客户必须使用 MFA 登录他们的 Citrix 帐户和 Citrix Cloud。以下情况下会在 MFA 中注册：

- 一位新客户首次登录他们的 Citrix 帐户。
- 一位 Citrix 客户注册了一个新的 Citrix Cloud 帐户，但尚未在 MFA 中注册。
- 新管理员加入了现有的 Citrix Cloud 帐户。

如果在登录 Citrix 帐户或 Citrix Cloud 时系统提示您在 MFA 中注册，请按照 CTX461297: How to Enroll into Multi Factor Authentication (MFA)（CTX461297：如何注册多重身份验证 (MFA)）中的步骤进行操作。

有关 Citrix 帐户的 MFA 的更多信息，请参阅 CTX463482：在 Citrix 属性上设置多因素身份验证 (MFA) 时的常见问题。

帐户恢复

如果您在恢复 Citrix 帐户凭据时需要帮助，请参阅本文中的如何找到我的 Citrix 帐户用户名或重置我的 Citrix 密码?。

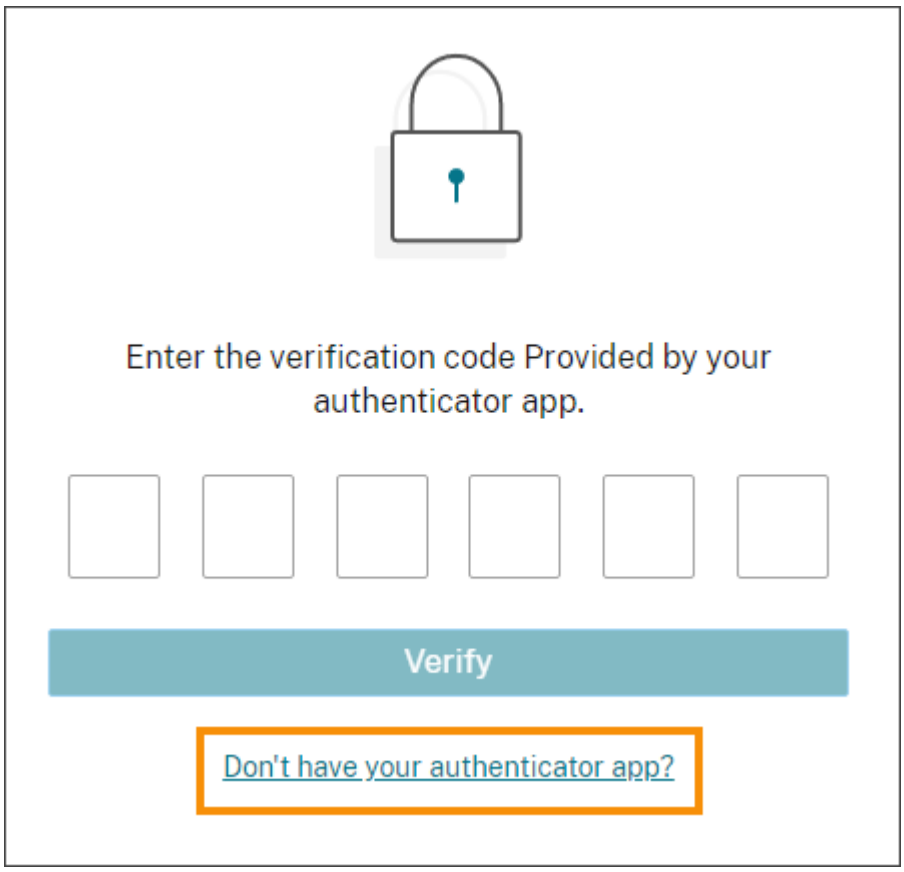
如果您需要帮助恢复对您的 Citrix Cloud 帐户的访问权限，则可以使用您在 MFA 中注册时配置的恢复方法。这些恢复方法包括：

- Citrix 发送到您的辅助邮箱地址的一次性代码。
- 您在 MFA 中注册期间生成的列表中的备用代码。
- Citrix 支持人员拨打您的辅助电话号码，以验证您的身份并帮助您访问您的帐户。注册 MFA 期间需要设置辅助电话号码。

要使用恢复方法登录，请执行以下操作：

1. 在 Citrix 帐户 或 Citrix Cloud 登录页面上，输入您的用户名和密码，然后选择 登录。
2. 当系统提示您输入主要 MFA 方法中的代码时，请选择使用恢复方法。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 选择要使用的恢复方法（如果适用）。如果您只配置了另一种恢复方法，除了恢复电话号码外，Citrix 会提示您自动使用该方法。
4. 如果使用您的辅助电子邮件地址，请输入 Citrix 发送的一次性代码，然后选择 验证。如果您在一段时间内没有收到验证码，请选择 重新发送电子邮件。验证后，Citrix Cloud 将为您登录。
5. 如果使用备用代码，请在出现提示时输入验证码，然后选择“验证并继续”。Citrix Cloud 登录并向您发送一封电子邮件，通知您已使用备份代码以及剩余有效备份代码的数量。记下或删除已使用的备用代码，以确保您不会再次使用它。
6. 如果您无法使用辅助电子邮件或备用代码：
   a) 选择 联系 **Citrix** 支持。
   b) 填写表格并详细说明您的问题。Citrix 支持代表使用您的辅助电话号码与您联系以验证您的身份。之后，代表会向您发送一个恢复码，您可以使用该代码登录。
   c) 返回 Citrix Cloud 登录页面并使用您的 Citrix Cloud 凭据登录。
   d) 当系统提示输入代码时，输入从 Citrix 支持部门收到的恢复代码，然后选择 验证。

登录后，请务必更新您的帐户恢复方法，以避免将来的登录延迟。

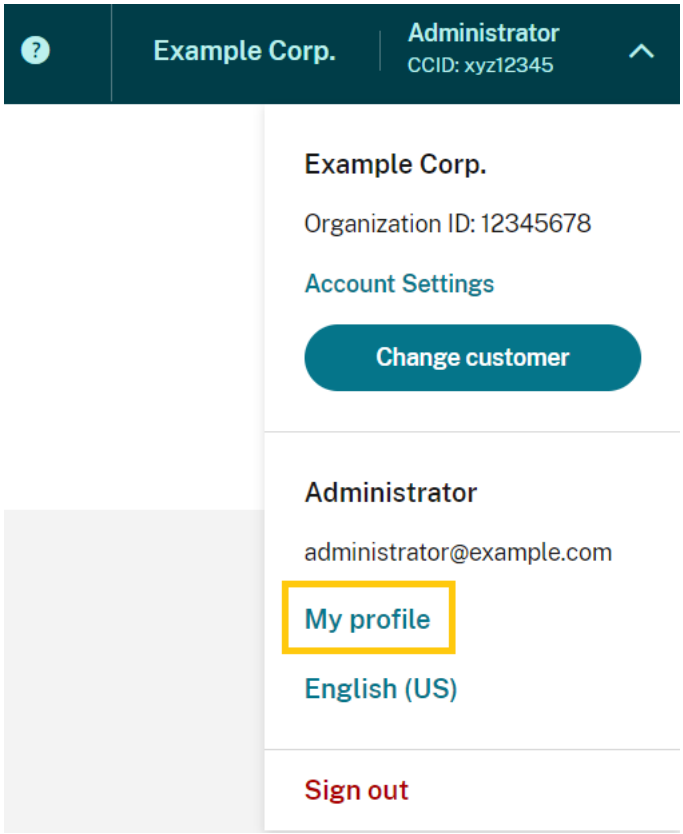
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更新您的 **MFA** 设置

您可以通过“我的设置”页面更新您的 MFA 访问和恢复设置。您可以通过您的 Citrix 帐户或 Citrix Cloud 访问此页面。

要访问您的我的设置页面，请执行以下操作：

1. 登录您的 Citrix 帐户或 Citrix Cloud。
2. 从您的 Citrix 帐户访问 https://accounts.cloud.com/core/profile。
3. 在 Citrix Cloud 中，从右上角的菜单中选择“我的设置”。



要更改您的 MFA 设置，请参阅以下章节：

- 管理您的主要 MFA 方法
- 管理您的 MFA 恢复方法

修改您的密码

如果您忘记了帐户密码，请选择 忘记密码？并在出现提示时输入您的帐户用户名。Citrix 向您帐户中的电子邮件地址发送一封电子邮件，其中包含用于设置新密码的链接。如果几分钟后仍未收到此电子邮件，或者需要更多帮助，请联系 Citrix Customer Service。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

当您尝试登录时，Citrix Cloud 可能会提示您重置密码。在以下情况下会出现此提示：

- 您的密码不符合 Citrix Cloud 的复杂性要求。
- 您的密码包含字典中的单词。
- 您的密码列在已知的泄露密码数据库中。
- 您在过去 60 天内没有登录 Citrix Cloud。

密码长度必须介于 8 到 128 个字符之间，并且包括：

- 至少有一个数字
- 至少包含一个大写字母
- 至少有一个符号：！@ # $ % ^ * ? + = -

出现提示时，选择“重置密码”为您的帐户创建一个新的强密码。

云服务运行状况

Citrix Cloud Health 控制面板 (https://status.cloud.com) 概述了 Citrix Cloud 平台和服务在每个地理区域的实时可用性。如果您在使用 Citrix Cloud 时遇到任何问题，请查看云运行状况控制面板，以验证 Citrix Cloud 或特定服务是否正常运行。

有关 Cloud Health 控制面板的更多信息，请参阅 服务运行状况。

Citrix Cloud 支持论坛

在 Citrix Cloud 支持论坛 上，您可以获得帮助、提供反馈和改进建议、查看其他用户的对话或开始自己的话题。

Citrix 技术支持部门的员工将跟踪这些论坛并随时准备回答您提出的问题。其他 Citrix Cloud 社区成员也可以提供帮助或加入讨论。

您无需登录即可阅读论坛主题。但是，您必须登录才能发布或回复主题。要登录，请使用现有的 Citrix 帐户凭据，或使用您在创建 Citrix Cloud 帐户时提供的电子邮件地址和密码。

支持文章和文档

Citrix 提供了大量的产品和支持内容，可帮助您充分利用 Citrix Cloud 并解决您在使用 Citrix 产品时可能遇到的问题。

Citrix 支持知识中心

知识中心 提供所有 Citrix 产品的故障排除内容以及安全公告和软件更新通知。只需输入搜索字符串即可查找相关内容。您可以根据产品和文章类型筛选结果。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Tech Zone

Citrix Tech Zone 包含可帮助您了解有关 Citrix Cloud 和其他 Citrix 产品的更多信息。在这里，您可以找到参考架构、图表、视频和技术论文，为设计、构建和部署 Citrix 技术提供见解。

用户帮助中心

C itrix 用户帮助中心 仅为组织中的最终用户提供 Citrix 产品文档。用户帮助中心以易于阅读的格式为面向最终用户的产品（例如 Citrix Workspace 应用程序和 Citrix SSO）提供说明。有关 ShareFile 的最终用户文档，请参阅 ShareFile 产品文档 Web 站点上的 Citrix Files 应用程序。

技术支持

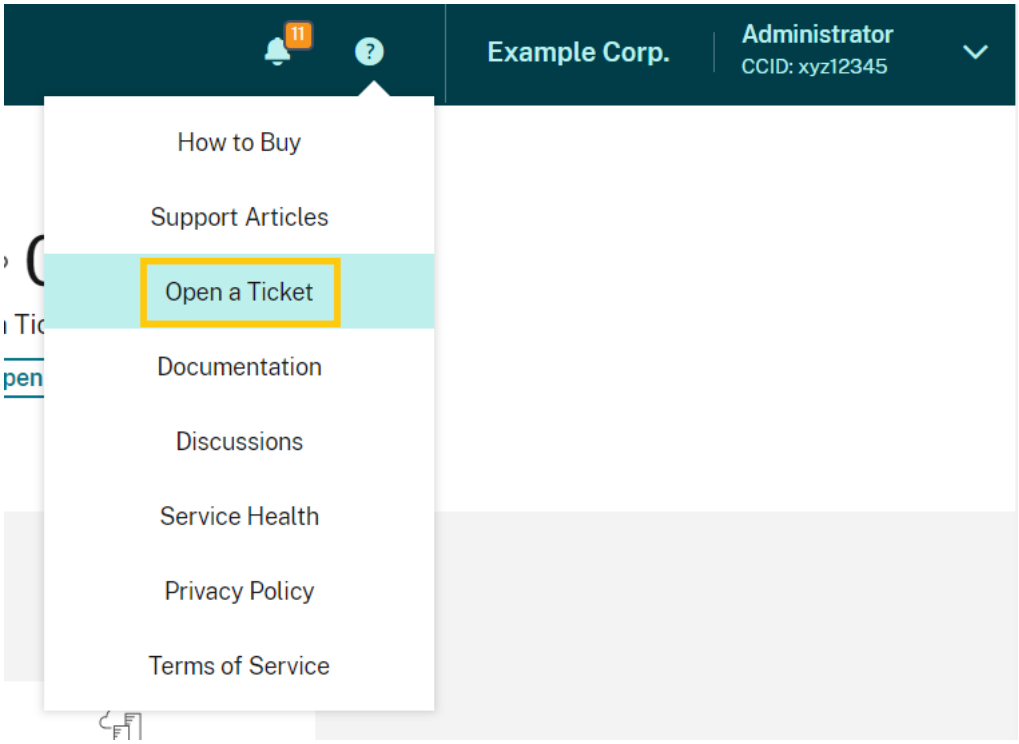
如果您遇到需要技术帮助的问题，可以访问“我的支持”门户以打开支持案例或与 Citrix 技术支持代表交谈。

要访问“我的支持”门户，请访问 https://support.citrix.com/case/manage。

要从 Citrix Cloud 访问门户，您必须拥有支持票据权限。有关管理员权限的更多信息，请参阅修改管理员权限。

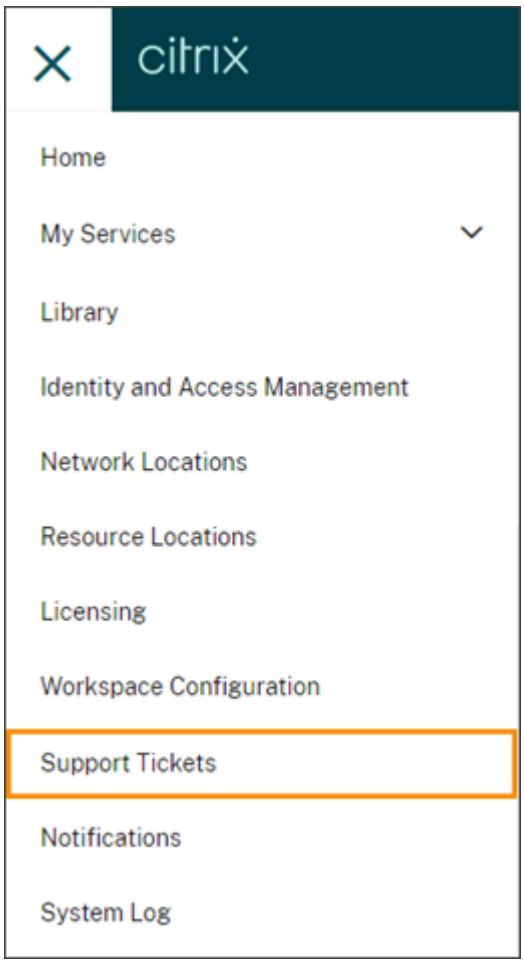
在 Citrix Cloud 管理控制台中，您可以使用以下方法访问“我的支持”：

- 在屏幕右上角附近的“帮助”图标中，选择“打开票据”。



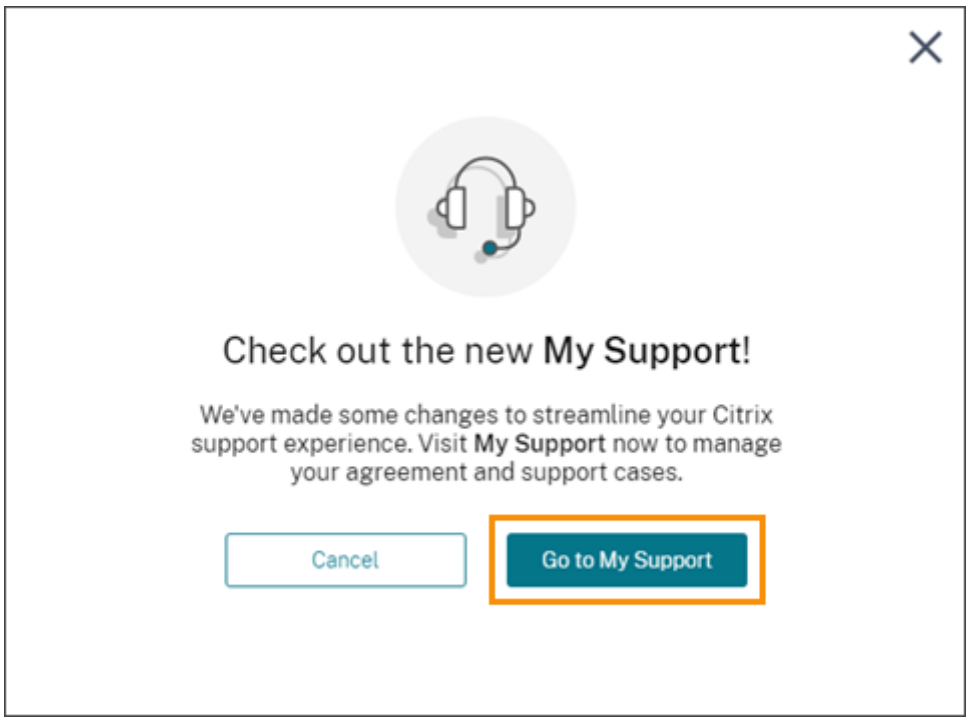
- 从屏幕左上角的 Citrix Cloud 菜单中，选择支持票据。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



选择其中任一选项后，选择转至“我的支持”，然后使用您的 Citrix 帐户凭据登录。

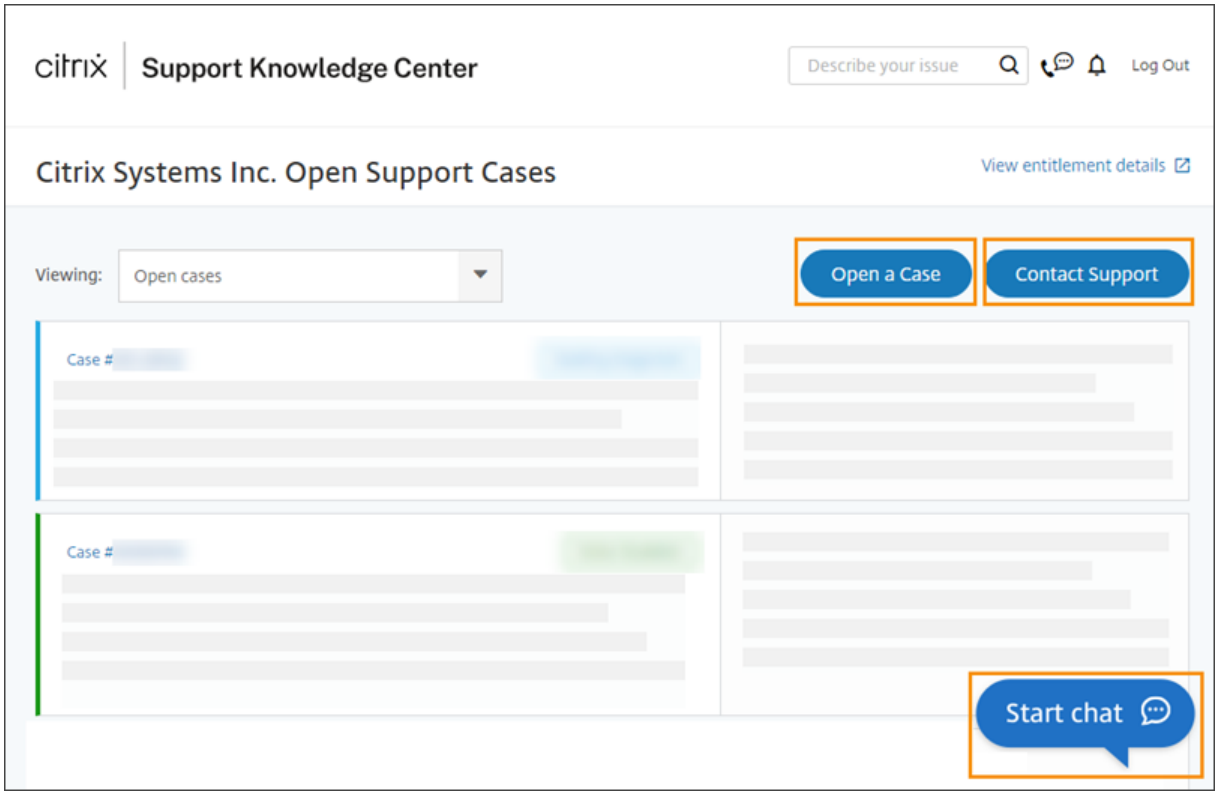
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



登录后，使用以下方法之一联系 Citrix 技术支持：

- 启动支持案例：选择 打开案例，然后提供您遇到的问题的详细信息。
- 通过电话：选择 联系支持 以查看可用于拨打 Citrix 技术支持的本地电话号码列表。
- 实时聊天：选择页面右下角的 开始聊天，与 Citrix 技术支持代表交谈。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

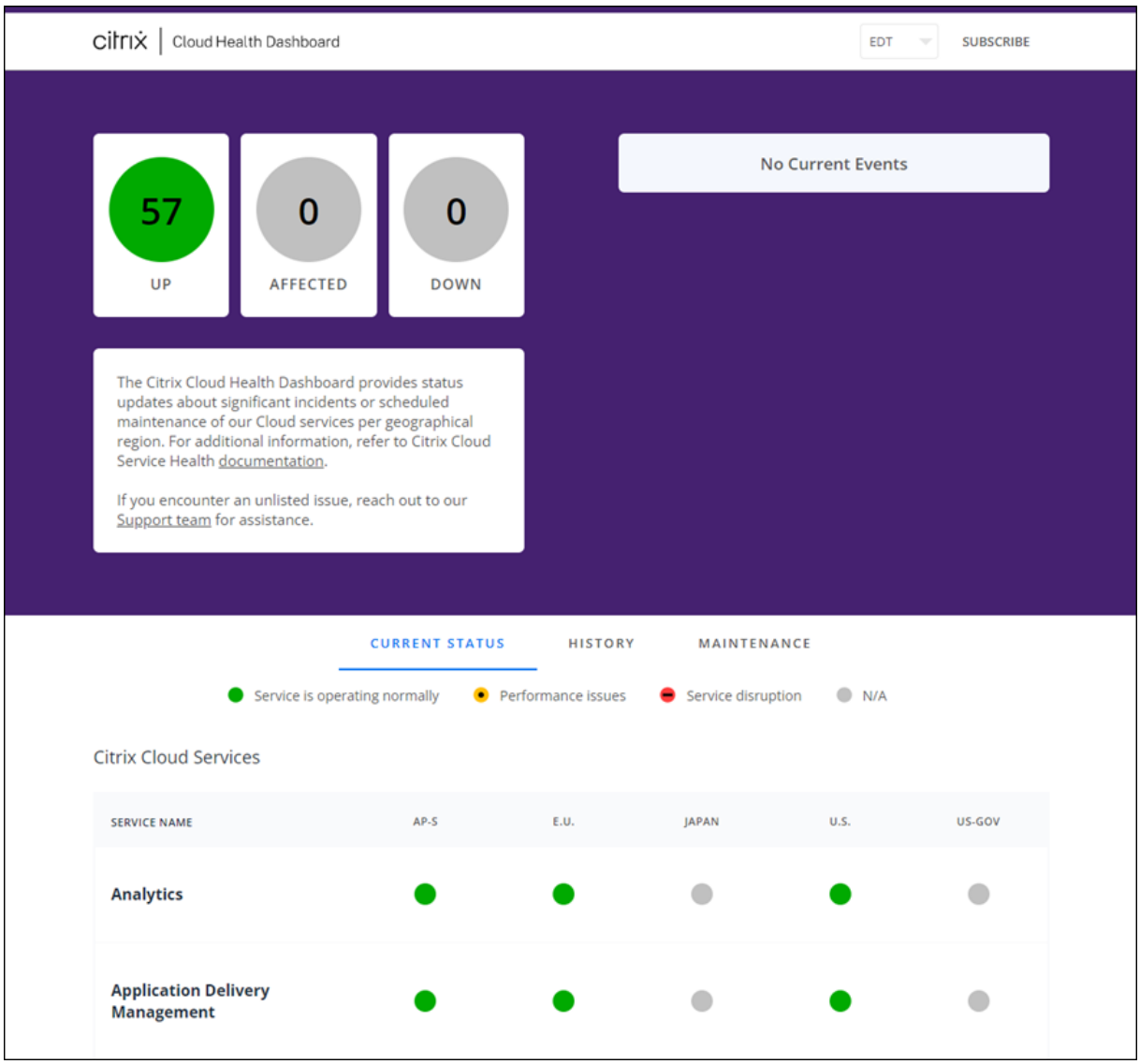


Citrix Cloud 服务运行状况

November 30, 2023

Citrix Cloud Health 控制面板概述了每个地理区域 Citrix Cloud 平台和服务的实时可用性。如果您在使用 Citrix Cloud 时遇到任何问题，请查看云运行状况控制面板，以验证 Citrix Cloud 或特定服务是否正常运行。

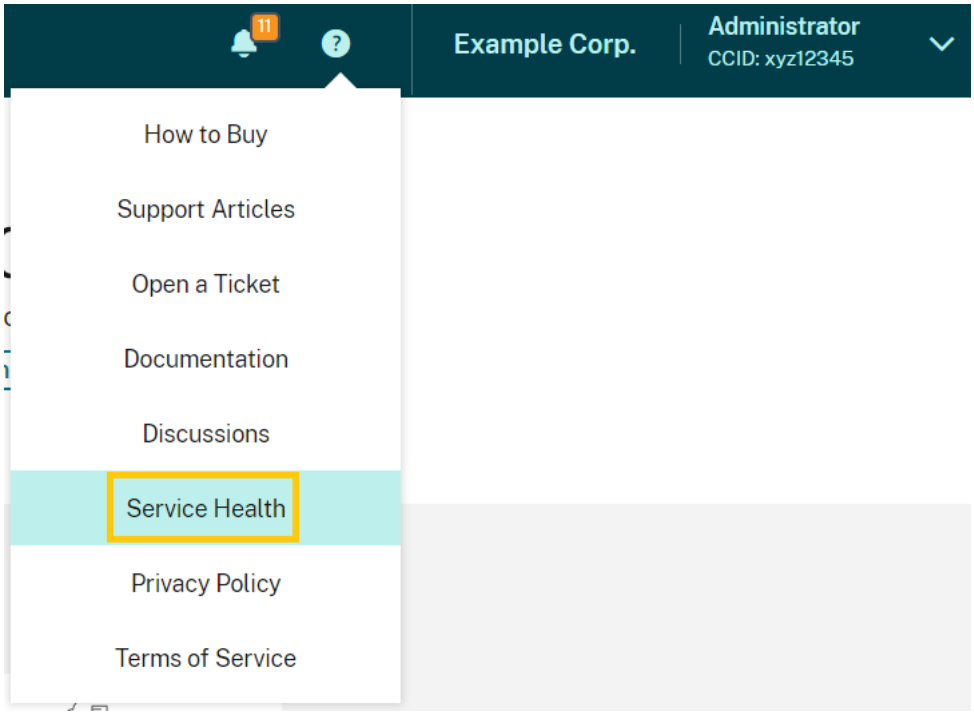
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



您可以使用以下方法访问 Cloud Health 控制板：

- 通过 Web 浏览器导航到 https://status.cloud.com。
- 从 Citrix Cloud 的“帮助”菜单中选择“服务运行状况”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



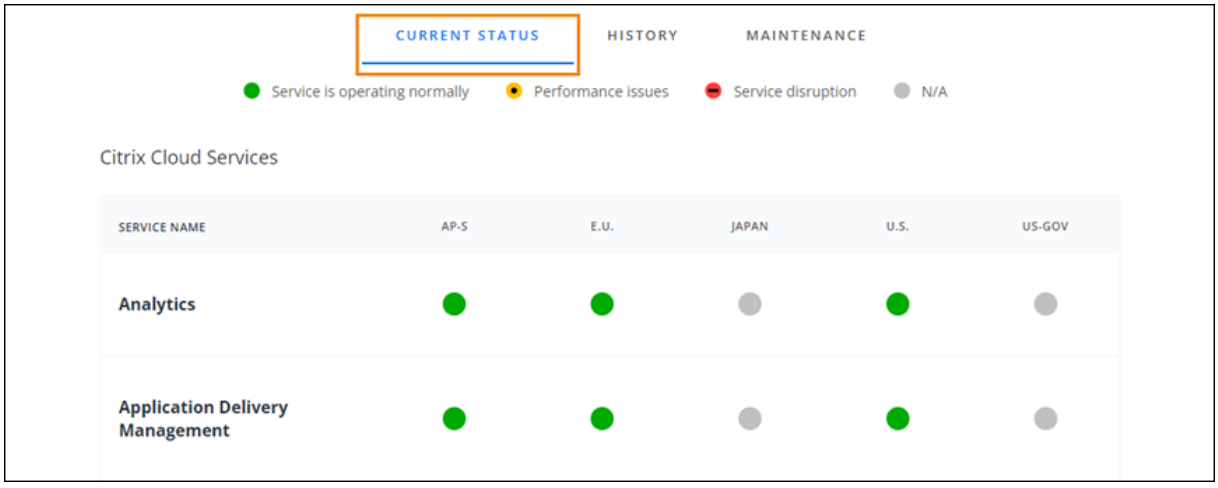
使用控制面板了解有关以下条件的更多信息：

- 所有 Citrix Cloud 服务的当前运行状况，按地理区域分组
- 过去七天内每项服务的运行状况历史记录
- 特定服务的维护窗口

您还可以订阅有关维护时段和服务事件等事件的通知。

查看运行状况和维护状态

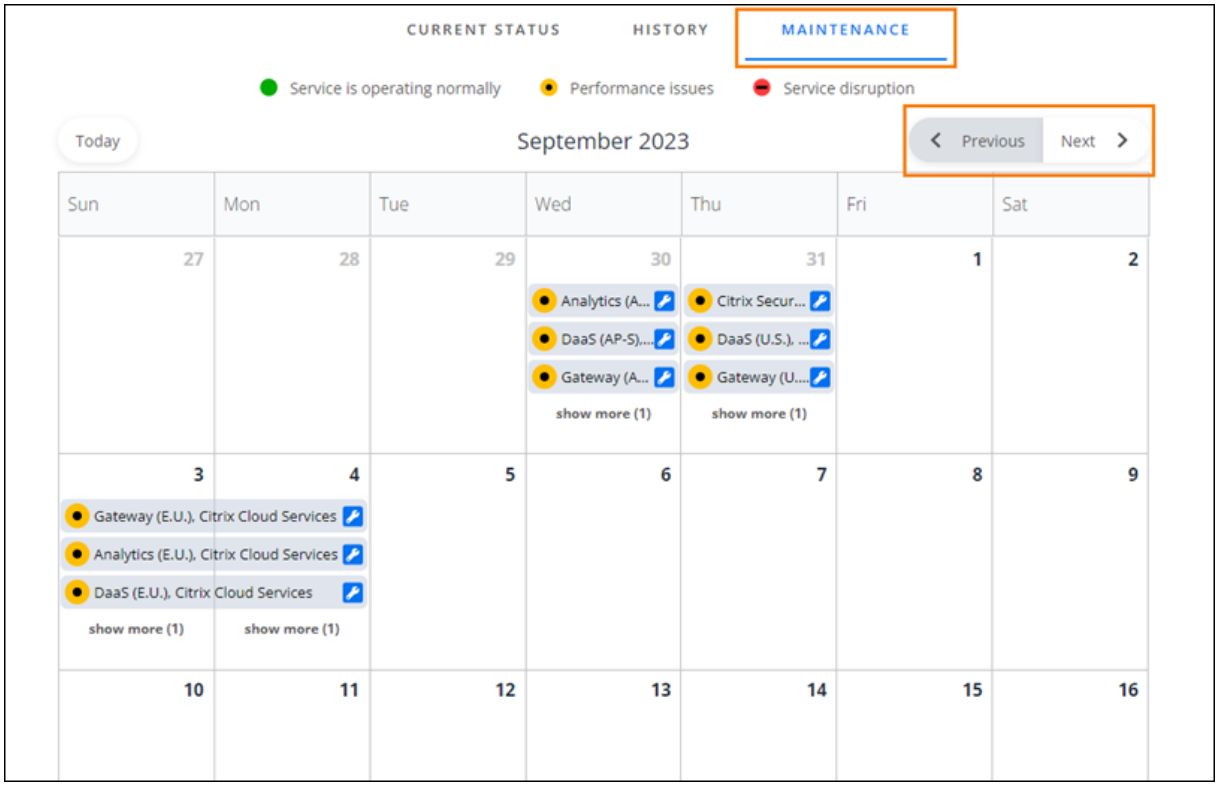
选择 当前状态 以显示每个地理区域中所有 Citrix Cloud 服务和平台组件的当前运行状况。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择“历史记录”以显示过去七天内所有 Citrix Cloud 服务和平台组件的运行状况。选择“仅显示受影响”以仅显示在过去七天内发生过维护或运行状况事件的服务。

选择“维护”以显示服务维护窗口的日历视图。选择“下一步”查看计划在未来几个月举行的维护活动。选择“上一页”可返回当前月份的活动。

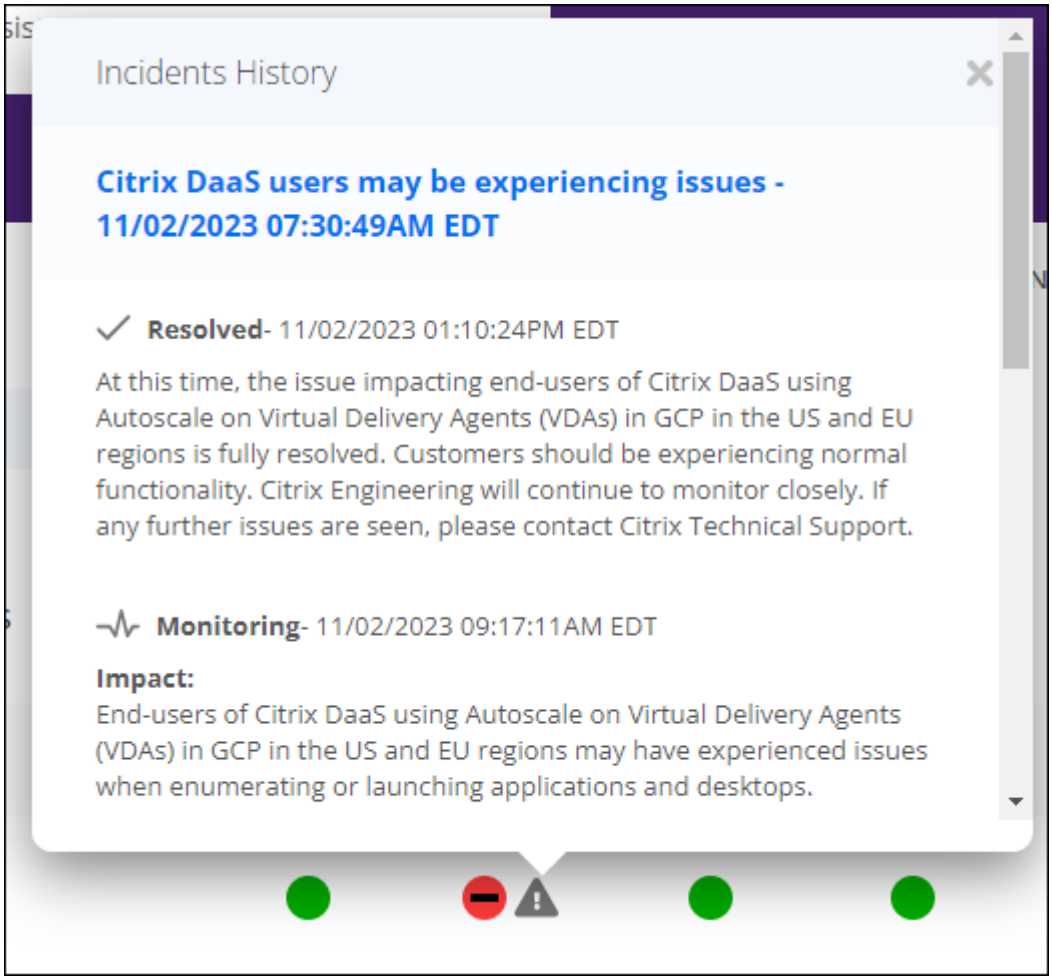


查看服务事件详情

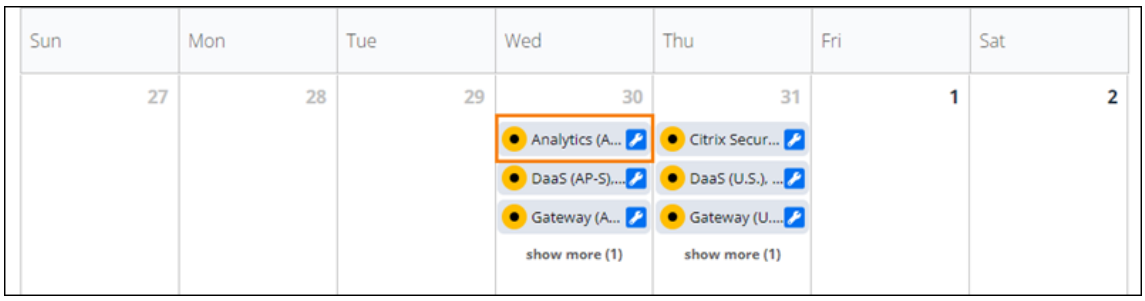
要查看有关受影响服务的服务运行状况事件的更多详细信息，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在“历史记录”视图中，单击服务指示器旁边的图标以查看有关服务运行状况事件的更多详细信息。



- 在“维护”视图中，单击服务条目以查看计划维护时段的状态页面。



事件通知频率

如果发生服务运行状况事件，Citrix 在发布到 status.cloud.com 时会考虑以下特征：

- 影响持续时间
- 影响频率

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在事件得到解决时，Citrix 会将以下类型的通知发布到云运行状况控制板：

- 调查：此通知表明 Citrix 已将问题确定为紧急问题并正在调查该问题。
- 监视：此通知表明 Citrix 已确定根本原因并正在缓解问题。
- 已解决：此通知表明 Citrix 已解决问题，服务已恢复到正常状态。

在调查和监视事件时，Citrix 每隔 60 到 120 分钟发布最新消息。这些更新可能包含以下信息：

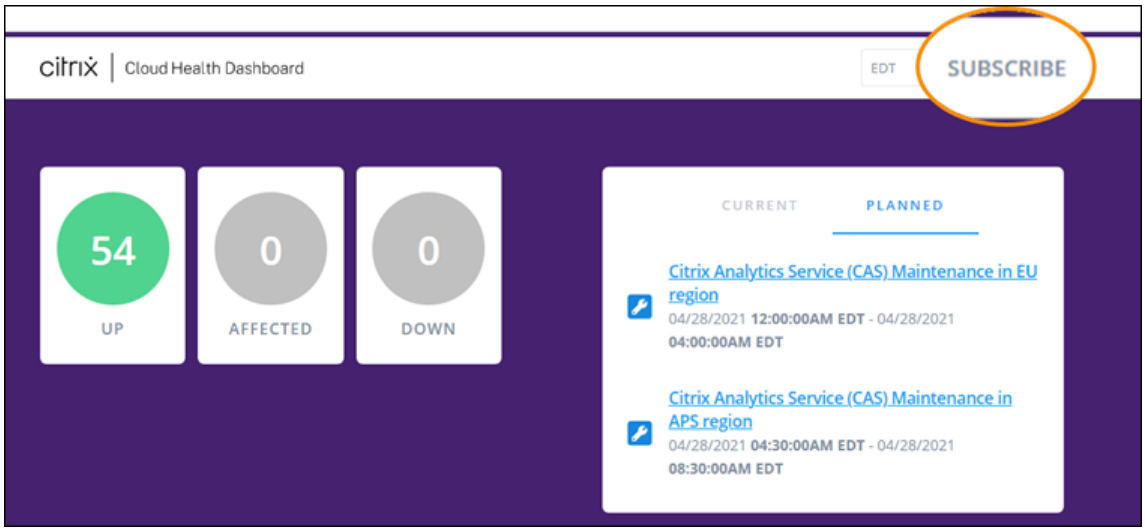
- 有关该事件的更多细节。
- 描述 Citrix 为解决该事件而采取的行动。
- 这表明自上次更新以来没有发生任何新变化。

事件得到解决后，Citrix 会发布最终更新。此更新可能表明该事件已得到解决，服务已恢复到正常状态。

订阅通知

您可以使用以下方法接收有关服务运行状况事件的通知：

- 选择控制面板右上角的“订阅”，然后选择要使用的通知方法。您可以从多种方法中进行选择，包括电子邮件和电话（作为短信）。



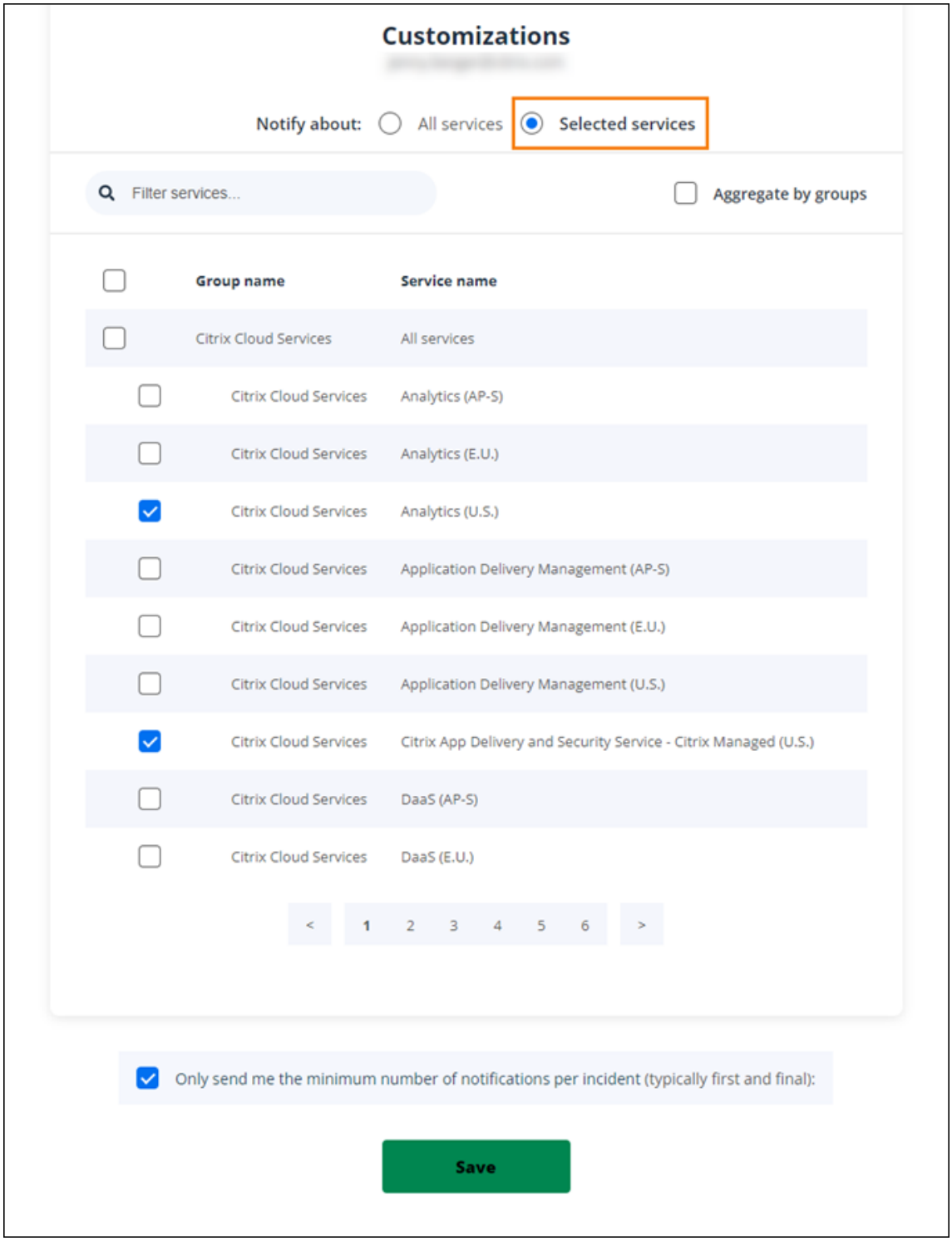
- 在 RSS 阅读器中输入以下 URL 以订阅 Citrix Cloud Health RSS 源：
  - 要在单个 Feed 中接收服务事件和维护通知，请订阅 `https://status.cloud.com/?format=atom`。
  - 要仅接收服务事件通知，请订阅 `https://status.cloud.com/atom/incidents`。
  - 要仅接收维护通知，请订阅 `https://status.cloud.com/atom/maintenances`。

订阅某个地区的特定服务

1. 选择控制面板右上角的“订阅”，然后选择要使用的通知方法。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 输入所选订阅方法的联系方式或 URL，然后选择“我接受条款和服务”。选择下一步。将出现“自定义”页面，其中默认选择了所选服务。
3. 在“自定义”页面上，从多页列表中选择所需区域中的服务。



4. 要仅接收每个事件的第一个和最后一个通知，请选择“仅向我发送每个事件的最小通知数”。

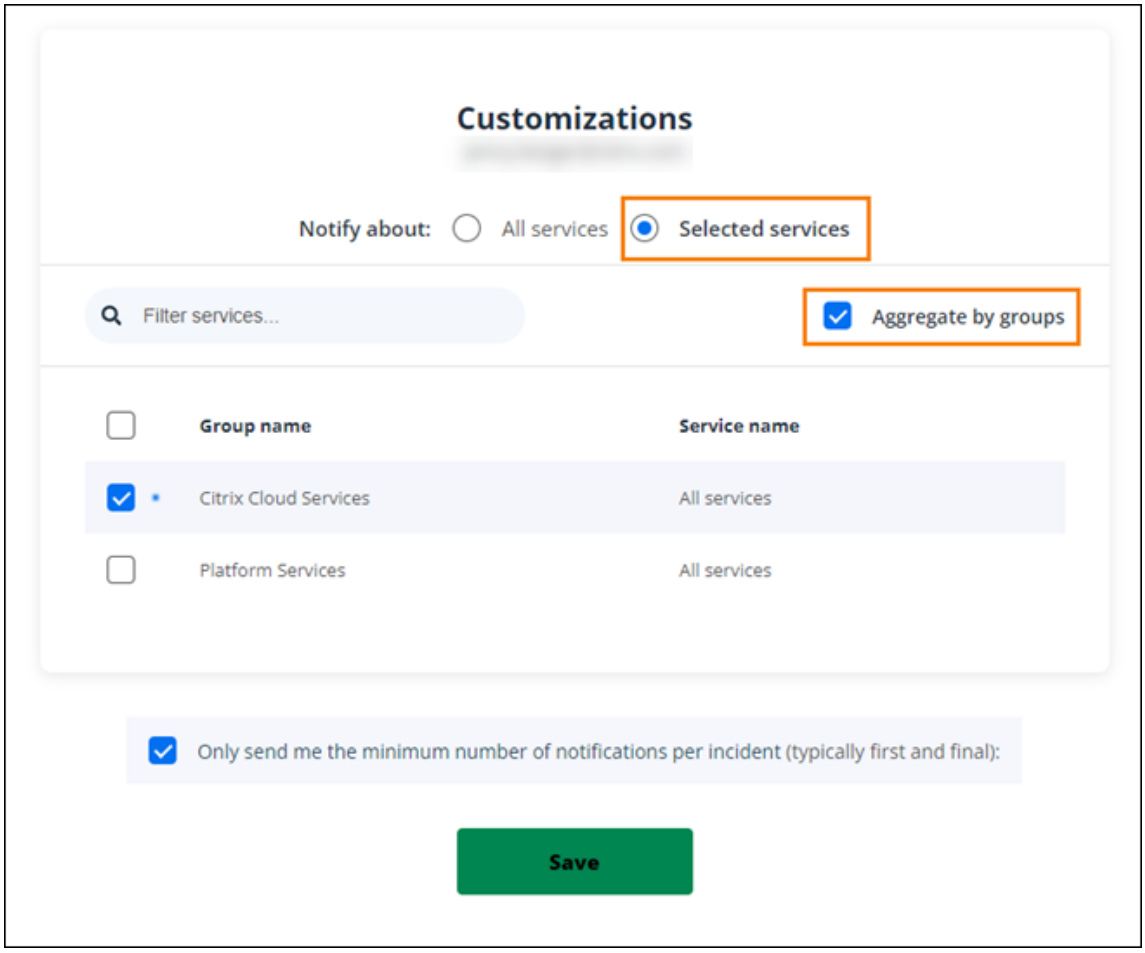
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. 单击保存。

订阅特定的服务组

您可以订阅所有区域的所有云服务（例如，分析和 DaaS）或所有平台服务（例如控制平面和云 API）的通知。

1. 选择控制面板右上角的“订阅”，然后选择要使用的通知方法。
2. 输入所选订阅方法的联系方式或 URL，然后选择“我接受条款和服务”。选择下一步。将出现“自定义”页面，其中默认选择了所选服务。
3. 在自定义页面上，选择按组聚合。
4. 选择 **Citrix Cloud** 服务或平台服务。



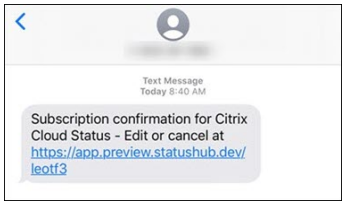
5. 要仅接收每个事件的第一个和最后一个通知，请选择“仅向我发送每个事件的最小通知数”。
6. 单击保存。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

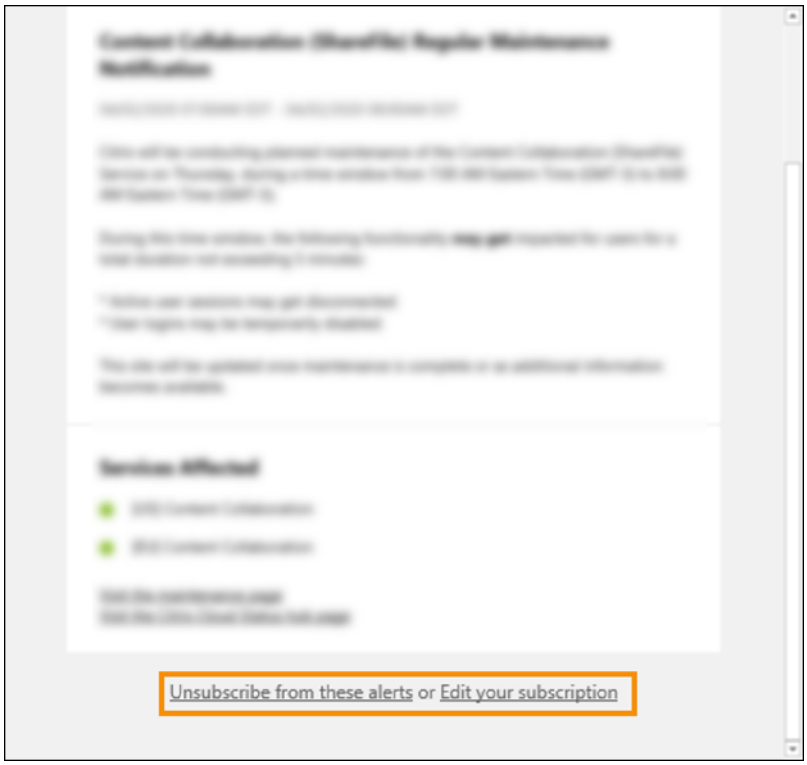
取消订阅通知

根据订阅方式，取消订阅或更改订阅的链接会包含在您收到的确认消息（例如，订阅电话通知时）或每条通知消息（例如，当您订阅电子邮件通知时）中。例如：

- 带有订阅选项的电话通知：



- 带有订阅选项的通知电子邮件



要取消订阅所有通知并移除所有订阅方式，请执行以下操作：

1. 找到您的订阅确认消息或现有通知，然后选择要取消订阅的链接。某些订阅方法可能会提供用于编辑或取消订阅的单个链接。
2. 根据您的订阅方式，使用“编辑订阅”页面上的以下选项之一：
    - 选择“删除所有订阅”。
    - 选择 取消订阅。在“取消订阅方法”页面中，选择“删除所有订阅”。

要取消订阅特定订阅方式的所有通知，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 找到您的订阅确认消息或现有通知，然后选择要取消订阅的链接。某些订阅方法可能会提供用于编辑或取消订阅的单个链接。
2. 根据您的订阅方式，使用“编辑订阅”页面上的以下选项之一：
   - 选择要移除的订阅方式。您的订阅将立即移除。
   - 选择 取消订阅。在“取消订阅方法”页面中，选择要移除的订阅方式。您的订阅将立即移除。

更改服务通知

1. 找到您的订阅确认消息或现有通知，然后选择链接以编辑您的订阅。某些订阅方法可能会提供用于编辑或取消订阅的单个链接。
2. 在“编辑订阅”页面中，选择要管理的订阅方式。
3. 在“自定义”页面上，选择要接收通知的服务，或者根据需要清除不再需要通知的服务。
4. 选择保存。

系统和连接要求

July 1, 2024

Citrix Cloud 提供管理功能（通过 Web 浏览器）和操作请求（来自其他已安装的组件），用于连接到部署中的资源。本文介绍了系统要求、所需的可联系 Internet 地址以及在资源与 Citrix Cloud 之间建立连接的注意事项。

系统要求

Citrix Cloud 要求下列最低配置：

- Active Directory 域
- 用于 Citrix Cloud Connector 的两台物理机或虚拟机已加入您的域。有关更多信息，请参阅 Citrix Cloud Connector 技术详细信息。
- 加入到您的域的物理机或虚拟机，用于托管工作负载和 StoreFront 等其他组件。有关特定服务的系统要求的详细信息，请参阅每项服务的 Citrix 文档。

有关规模和大小要求的信息，请参阅 Cloud Connector 的缩放和大小注意事项。

支持的 **Web** 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

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

传输层安全要求

对于组件之间基于 TCP 的连接，Citrix Cloud 支持传输层安全性 (TLS) 1.2。Citrix Cloud 不允许通过 TLS 1.0 或 TLS 1.1 进行通信。

要访问 Citrix Cloud，必须使用支持 TLS 1.2 且已配置接受密码套件的浏览器。有关更多信息，请参阅 加密和密钥管理。

Citrix Cloud 管理控制台

Citrix Cloud 管理控制台是一个基于 Web 的控制台，您可以 通过 https://citrix.cloud.com登录后访问该控制台。组成控制台的 Web 页面在登录时或者以后执行特定操作时需要使用 Internet 上的其他资源。

代理配置

如果您通过代理服务器进行连接，则管理控制台使用与您的 Web 浏览器相同的配置运行。控制台在用户环境中运行，因此，需要用户身份验证的代理服务器的任何配置都应按预期运行。

防火墙配置

对于要运行的管理控制台，必须打开端口 443 以便建立出站连接。可以通过在控制台内部导航来测试常规连接。有关所需端口的更多信息，请参阅 入站和出站端口配置。

控制台通知

管理控制台使用 Pendo 显示关键警报、有关新功能的通知以及某些功能和服务的产品内指南。为确保您可以在管理控制台中查看 Pendo 内容，Citrix 建议可以联系 `https://citrix-cloud-content.customer.pendo.io/` 该地址。

显示 Pendo 内容的服务包括：

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

Pendo 是 Citrix 用来向 Citrix 客户提供云和支持服务的第三方子处理器。有关这些子处理者的完整列表，请参阅 Citrix Cloud 和支持服务子处理者以及 Citrix 附属机构。

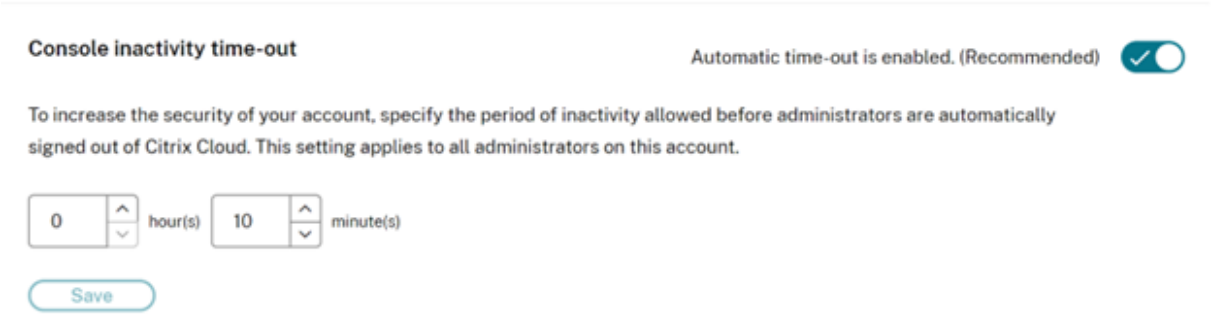
会话超时

管理员登录 Citrix Cloud 后，管理控制台会话在 72 小时后超时。无论控制台活动如何，都会出现这种超时。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

控制台可配置的非活动超时

作为完全访问权限的管理员，您可以在管理员自动注销之前在 Citrix Cloud 控制台上配置不活动的时间。配置完成后，指定的超时时间将应用于 Citrix Cloud 帐户的所有管理员。



启用该功能后，管理员将在配置的非活动时间段后注销，并且会话超时将在每次后续登录时重置。

禁用该功能后，没有非活动计时器，只有在达到 72 小时会话限制时，管理员才会被注销。

> 注意：
>
> - 默认情况下，此功能处于禁用状态。
> - 可配置的非活动超时时间为 10 分钟到 12 小时。
> - 默认的非活动超时为 60 分钟。

在 **Citrix Cloud** 注册许可证服务器

如果您要向 Citrix Cloud 注册本地 Citrix 许可证服务器以监视本地部署的使用情况，请确保以下地址可联系：

- `https://trust.citrixnetworkapi.net` （用于检索代码）
- `https://trust.citrixworkspacesapi.net/` （用于确认许可证服务器已注册）
- `https://cis.citrix.com` （用于数据上载）
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

如果您将代理服务器与 Citrix 许可证服务器一起使用，请确保按照许可产品文档中的配置代理服务器中所述配置代理服务器进行配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud Connector

Citrix Cloud Connector 是一个软件包，用于部署在 Microsoft Windows 服务器上运行的一组服务。托管 Cloud Connector 的计算机位于您在 Citrix Cloud 上使用的资源所在的网络中。Cloud Connector 连接到 Citrix Cloud，允许您根据需要操作和管理资源。

有关安装 Cloud Connector 要求，请参阅 系统要求。Cloud Connector 要求在端口 443 上建立出站连接，以便进行操作。安装后，Cloud Connector 可能会有其他访问要求，具体取决于与其配合使用的 Citrix Cloud 服务。

托管 Cloud Connector 器的计算机必须与 Citrix Cloud 具有稳定的网络连接。网络组件必须支持 HTTPS 和长期安全 Web 套接字。如果在网络组件中配置了超时，则它必须大于 2 分钟。

有关对 Cloud Connector 和 Citrix Cloud 之间的连接进行故障排除的帮助，请使用 Cloud Connector 连接检查实用程序。此实用程序在 Cloud Connector 计算机上运行一系列检查，以验证其是否可以访问 Citrix Cloud 和相关服务。如果您在环境中使用代理服务器，则所有连接检查都将通过代理服务器进行隧道传输。要下载该实用程序，请参阅 Citrix 支持知识中心中的 CTX260337 。

Cloud Connector 公共服务连接要求

从您的数据中心连接到 Internet 需要打开端口 443 以便建立出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中进行操作，可能需要进一步进行配置。有关详细信息，请参阅 Cloud Connector 代理和防火墙配置。

本文中每项服务的地址必须是可联系的，才能正确操作和使用该服务。以下列表包括大多数 Citrix Cloud 服务通用的地址：

- `https://*.citrixworkspacesapi.net`（提供对服务使用的 Citrix Cloud API 的访问权限）
- `https://*.cloud.com`（提供对 Citrix Cloud 登录界面的访问权限）
- `https://*.blob.core.windows.net`（提供对 Azure Blob 存储的访问权限，该存储用于存储 Citrix Cloud Connector 更新）
- `https://*.servicebus.windows.net`（提供对用于日志记录的 Azure 服务总线和 Active Directory 代理的访问权限）

这些地址仅作为域名提供，因为 Citrix Cloud 服务是动态的，其 IP 地址会受到例行更改的影响。

最佳做法是使用组策略来配置和管理这些地址。此外，仅配置适用于您和您的最终用户正在使用的服务的地址。

如果您使用 Citrix Cloud 和 Citrix 许可证服务器来注册本地产品，请参阅本文中的 Citrix Cloud 许可证服务器注册，了解其他所需的可联系地址。

Cloud Connector 允许的 FQDN

为了帮助您确保允许所有必需的完全限定域名 (FQDN) 通过您的防火墙，Citrix 提供了以下资源：

- allowlist.json

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- CTX270584：Citrix Gateway 服务—接入点 (PoP)

配置防火墙时，请查阅这两个资源，以验证您的服务部署所需的 FQDN 是否被允许。

本地主机缓存（高可用性服务） 在连接器中使用本地主机缓存 (LHC) 时，请确保连接器可以到达资源位置中所有其他连接器的选举端点。选举端点位于端口 80 上，可以通过以下 URL 进行访问：`http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`。

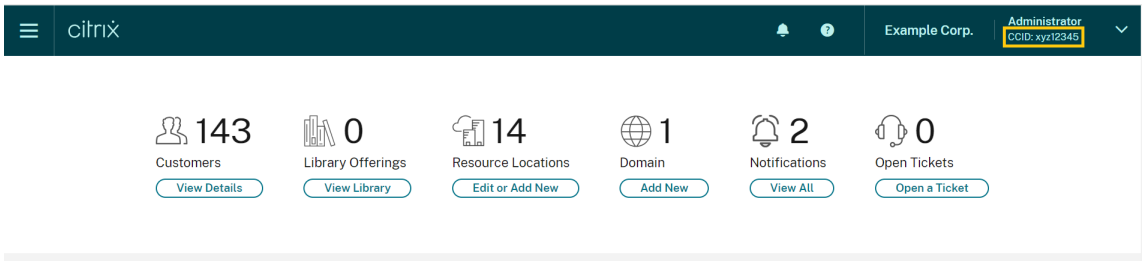
如果连接器无法在此地址进行通信，则在 LHC 事件期间会选择多个代理，这可能会导致虚拟应用程序和桌面间歇性启动失败。有关更多信息，请参阅具有多个 Cloud Connector 的资源位置。

自适应身份验证 使用 Cloud Connector 连接到自适应身份验证服务时，必须允许您的 Citrix Cloud Connector 访问您为自适应身份验证实例保留的域名或 URL。例如，允许 `https://aauth.xyz.com`。有关更多信息，请参阅自适应身份验证。

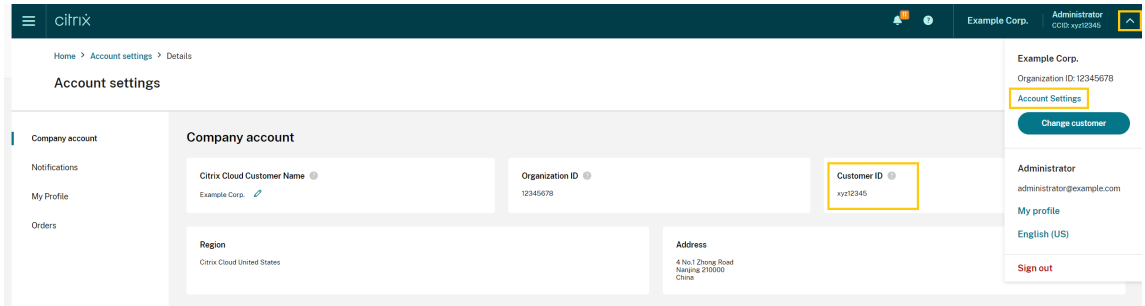
Allowlist.json allowlist.json 文件位于 https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json，列出了 Cloud Connector 访问的 FQDN。此列表按产品分组，包括每组 FQDN 的更改日志。

其中一些 FQDN 是特定于客户的，并在尖括号中包含模板部分。在使用之前，必须将这些模板化部分替换为实际值。例如，对于 `<CUSTOMER_ID>.xendesktop.net`，将 `<CUSTOMER_ID>` 替换为您的 Citrix Cloud 帐户的实际客户 ID。您可以在以下控制台位置找到客户 ID：

- 位于屏幕右上角的 Citrix Cloud 帐户的客户名称下方。

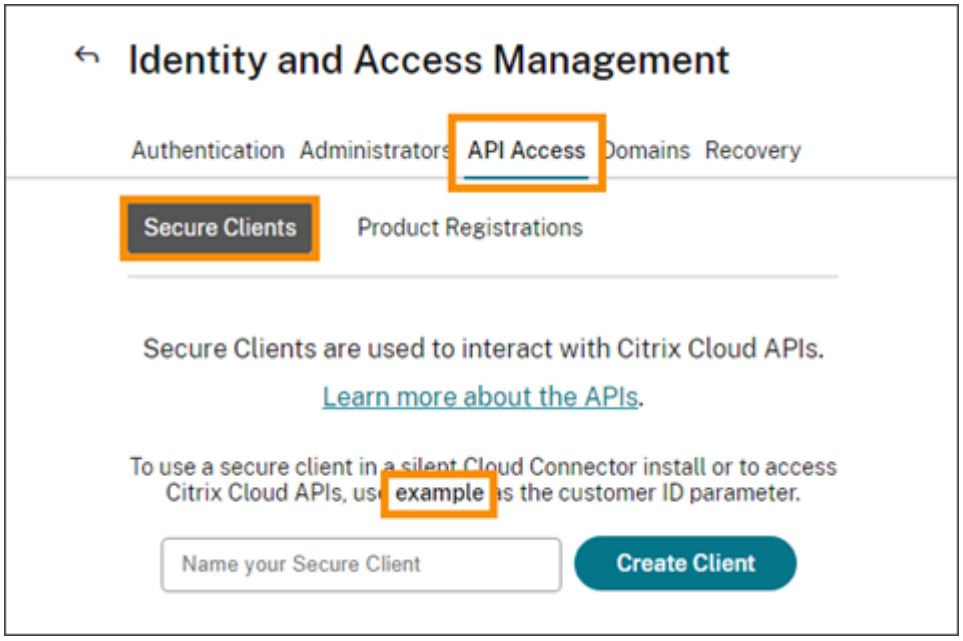


- 在“帐户设置”页面上的 **Citrix Cloud** 客户 **ID (CCID)** 下。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在“安全客户端”选项卡上，“身份和访问管理”**>**“**API** 访问”**>**“安全客户端”。



网关服务接入点　allowlist.json 文件中包含的一些 FQDN 也包含在 CTX270584：Citrix Gateway 服务 - 接入点 (PoP) 中。但是，CTX270584 还包括客户端访问的 FQDN，例如：

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

证书验证

Cloud Connector 联系的 Cloud Connector 二进制文件和端点受 X.509 证书的保护，这些证书在安装软件时经过验证。要验证这些证书，每台 Cloud Connector 计算机都必须满足特定要求。有关这些要求的完整列表，请参阅 证书验证要求。

SSL 解密

在某些代理上启用 SSL 解密可能会阻止 Cloud Connector 成功连接到 Citrix Cloud。有关解决此问题的更多信息，请参阅 CTX221535。

适用于云服务的 **Citrix Connector Appliance**

Connector Appliance 是可以在虚拟机管理程序中部署的设备。托管 Connector Appliance 的虚拟机管理程序位于您在 Citrix Cloud 上使用的资源所在的网络中。Connector Appliance 连接到 Citrix Cloud，允许其根据需要操作和管理您的资源。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关安装 Connector Appliance 的要求，请参阅系统要求。

要运行，Connector Appliance 需要端口 443 上的出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中进行操作，可能需要进一步进行配置。

要正确操作和使用 Citrix Cloud 服务，必须联系以下地址：

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`

  无法启用所有子域的客户可以使用以下地址来代替

  ```
  - https://*.g.nssvc.net
  - https://*.c.nssvc.net
  ```

- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

网络要求

确保您的 Connector Appliance 环境具有以下配置：

- 网络允许 Connector Appliance 使用 DHCP 获取 DNS 和 NTP 服务器、IP 地址、主机名和域名，或者您可以在 Connector Appliance 控制台中手动设置网络设置。
- 网络未配置为使用 Connector Appliance 内部使用的链路本地 IP 范围 169.254.0.1/24、169.254.64.0/18 或 169.254.192.0/18。
- 虚拟机管理程序时钟设置为协调世界时 (UTC) 并与时间服务器同步，或者 DHCP 向 Connector Appliance 提供 NTP 服务器信息。
- 如果将代理与 Connector Appliance 配合使用，则该代理必须未经身份验证或使用基本身份验证。

Citrix Analytics 服务连接

- 对于包括新功能和关键通信在内的产品内消息：`https://citrix-cloud-content.customer.pendo.io/`
- 其他要求：前提条件

有关将数据源载入服务的详细信息，请参阅 支持的数据源。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

控制台服务连接

有关完整的 Internet 连接要求，请参阅 NetScaler 产品文档中的支持的端口。

Citrix DaaS 服务连接

Citrix Cloud 资源位置/Cloud Connector：

- Cloud Connector 公共服务连接要求
- `https://[customerid].xendesktop.net`，其中 `[customerid]` 是 Citrix Cloud 管理控制台的“安全客户端”选项卡（身份和访问管理 **> API** 访问 **>** 安全客户端）上显示的客户 ID 参数。
  - 使用 Citrix Virtual Apps Essentials 的客户需要 `https://*.xendesktop.net` 改为使用。
- 使用 Quick D eploy 安装 Citrix DaaS 的客户需要联系以下额外地址：
  - `https://*.apps.cloud.com`
  - `AzureCloud` 服务标签
- `https://*.*.nssvc.net`
  - 无法启用所有子域名的客户可以使用以下地址：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

有关 Cloud Connector 如何与服务通信的概述，请参阅 Citrix Tech Zone Web 站点上的 Citrix DaaS 示意图。

管理控制台：

- `https://*.citrixworkspacesapi.net`（Rendezvous 协议不需要）
- `https://*.citrixnetworkapi.net`（Rendezvous 协议不需要）
- `https://*.cloud.com`（Rendezvous 协议不需要）
- `https://[customerid].xendesktop.net`，其中 `[customerid]` 是 Citrix Cloud 管理控制台的“安全客户端”选项卡（身份和访问管理 **> API** 访问 **>** 安全客户端）上显示的客户 ID 参数。
  - 使用 Citrix Virtual Apps Essentials 的客户需要 `https://*.xendesktop.net` 改为使用。
- `https://*.*.nssvc.net`（Citrix DaaS Standard for Azure 不需要）
  - 无法启用所有子域名的客户可以使用以下地址：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- 对于包括新功能和关键通信在内的产品内消息：`https://citrix-cloud-content.customer.pendo.io/`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Rendezvous 协议

使用 Citrix Gateway 服务时，Rendezvous 协议允许 VDA 绕过 Citrix Cloud Connector，以直接安全地连接到 Citrix Cloud 控制平面。

除非另有说明，否则无论您使用哪种协议版本，VDA 都必须能够联系上面列出的管理控制台的地址。有关 Rendezvous 协议要求的完整列表，请参阅 Citrix DaaS 产品文档的以下部分：

- Rendezvous V1
- Rendezvous V2

本地主机缓存要求

如果您的防火墙执行数据包检查并且您想要使用本地主机缓存功能，请确保您的防火墙接受 XML 和 SOAP 流量。此功能要求能够下载 MDF 文件，当 Cloud Connector 将配置数据与 Citrix Cloud 同步时，就会出现这种情况。这些文件通过 XML 和 SOAP 流量传送到 Cloud Connector。如果防火墙阻止此流量，则 Cloud Connector 和 Citrix Cloud 之间的同步将失败。如果发生中断，用户将无法继续工作，因为驻留在 Cloud Connector 上的配置数据已过期。

有关此功能的更多信息，请参阅 Citrix DaaS 产品文档中的 本地主机缓存 。

VDA 升级要求

使用 Citrix DaaS 的完整配置界面，可以在每个目录或每台计算机的基础上升级 VDA。您可以立即或在预定时间升级它们。有关 VDA 升级功能的更多信息，请参阅使用完整配置界面升级 VDA。

使用该功能时，请确保满足以下连接要求：

- 以下 Azure CDN URL 已添加到允许列表中。该功能从 Azure CDN 端点下载 VDA 安装程序。
  - 生产 - 美国 (US)：`https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 欧盟 (EU)：`https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 亚太南部 (APS)：`https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - 生产 - 日本 (JP)：`https://prod-jp-vus-storage-endpoint.azureedge.net/*`
- 该功能验证 VDA 安装程序是否由有效证书签名。确保已将以下 URL 添加到允许列表中，以进行证书有效性和吊销检查：
  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - http://ocsp.digicert.com/*
  - http://cacerts.digicert.com/*

- 该功能需要 VDA 升级代理才能运行。在 VDA 上运行的 VDA 升级代理与 Citrix DaaS 通信。确保以下 URL 已添加到允许列表中：
  - https://[customerId].xendesktop.net/citrix/VdaUpdateService/*，其中 [customerid] 是 Citrix Cloud 管理控制台的“安全客户端”选项卡（身份和访问管理 **> API** 访问 **>** 安全客户端）上显示的客户 ID 参数。
  - http://xendesktop.net/citrix/VdaUpdateService/*

Endpoint Management 服务连接

Citrix Cloud 资源位置/Cloud Connector：

- Cloud Connector 公共服务连接要求
- 其他要求：/en-us/citrix-endpoint-management/endpoint-management.html

管理控制台：

- https://*.citrix.com
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- 其他要求：/en-us/citrix-endpoint-management/endpoint-management.html

Citrix Gateway 服务连接

- Cloud Connector 公共服务连接要求
- https://*.*.nssvc.net
  - 无法启用所有子域名的客户可以使用以下地址：
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net

> 重要：
>
> 无法对 Citrix Gateway 地址执行 SSL 拦截。在某些代理上启用 SSL 拦截可能会阻止 Cloud Connector 成功连接到 Citrix Cloud。

NetScaler Intelligent Traffic Management 服务连接

- https://*.cedexis-test.com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- https://*.citm-test.com
- https://cedexis.com
- https://cedexis-radar.net

SD-WAN Orchestrator 服务连接

有关完整的 Internet 连接要求，请参阅使用 Citrix SD-WAN Orchestrator 服务的必备条件。

Remote Browser Isolation（以前称为 Secure Browser）服务连接

Citrix Cloud 资源位置/Cloud Connector：

Cloud Connector 公共服务连接要求

管理控制台：

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://browser-release-a.azureedge.net
- https://browser-release-b.azureedge.net

Citrix Secure Private Access 服务连接

- https://*.netscalergateway.net
- https://*.*.nssvc.net
  - 无法启用所有子域名的客户可以使用以下地址：
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net

Citrix Workspace 服务连接

- https://*.cloud.com
- https://*.citrixdata.com
- 对于包括新功能和关键通信在内的产品内消息：https://citrix-cloud-content.customer.pendo.io/

Global App Configuration Service 连接

https://discovery.cem.cloud.us

有关此服务的详细信息，请参阅以下资源：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 自定义 Workspace 应用程序设置 - Citrix Workspace 产品文档
- Global App Configuration Service - Citrix Developer 文档

Citrix Workspace 应用程序连接

将以下 URL 添加到您的允许列表中：

- https://*.cloud.com
- 身份提供商地址。请参阅相应身份提供商文档中的说明。
- https://*.wsp.cloud.com

对于特定 URL，允许访问以下地址：

- <yourcustomer>.cloud.com

Citrix Secure Private Access

- ngspolicy.netscalergateway.net
- config.netscalergateway.net
- app.netscalergateway.net
- http://tunnel.netscalergateway.net/

Global App Configuration Service

请参阅本文中的 Global App Configuration Service 连接。

身份验证

- accounts.cloud.com
- accounts-dsauthweb.cloud.com

确保您的身份提供商 URL 也可以从您的最终用户设备访问。

Citrix Analytics 服务

- locus.analytics.cloud.com

根据您的位置，启用对以下列表中相应 URL 的访问权限：

- 美国：citrixanalyticseh.servicebus.windows.net
- 欧盟：citrixanalyticseheu.servicebus.windows.net
- 亚太南部：citrixanalyticsehaps.servicebus.windows.net

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workspace 图形界面资产

- ctx-ws-assets.cloud.com

个性化、通知和功能推出

- customer-**interface**-personalization.us.wsp.cloud.com
- user-personalization.us.wsp.cloud.com
- admin-notification.us.wsp.cloud.com
- customer-**interface**-personalization.eu.wsp.cloud.com
- user-personalization.eu.wsp.cloud.com
- admin-notification.eu.wsp.cloud.com
- customer-**interface**-personalization.ap-s.wsp.cloud.com
- user-personalization.ap-s.wsp.cloud.com
- admin-notification.ap-s.wsp.cloud.com
- feature-rollout.us.wsp.cloud.com
- feature-rollout.eu.wsp.cloud.com
- feature-rollout.ap-s.wsp.cloud.com

设备注册服务

- device-registration.us.wsp.cloud.com
- device-registration.eu.wsp.cloud.com
- device-registration.ap-s.wsp.cloud.com

推送通知服务

- push-events-signalr.us.wsp.cloud.com
- push-events-signalr.eu.wsp.cloud.com
- push-events-signalr.ap-s.wsp.cloud.com

Citrix Gateway 服务

- https://*.g.nssvc.net

使用 **Citrix** 联合身份验证服务 **(FAS)** 进行 **Workspace** 单点登录

控制台和 FAS 服务分别使用用户帐户和网络服务帐户访问以下地址。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- FAS 管理控制台，在用户的帐户下：
  - https://*.cloud.com
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/
  - 第三方身份提供程序所需的地址（如果您的环境中使用了第三方身份提供程序）
- FAS 服务，在网络服务帐户下：
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/

如果您的环境包含代理服务器，请使用 FAS 管理控制台的地址配置用户代理。此外，请确保将网络服务帐户的地址配置为适合您的环境。

如果您使用 Active Directory 或 Active Directory 和基于时间的一次性密码 (TOTP) 作为 Citrix Workspace 应用程序的身份提供商，则还必须将其列入白名单 `login.cloud.com`。如果您使用其他身份提供商，请单独允许身份提供商 URL。

CAS 事件中心的 URL 也是特定于地理区域的。citrixanalyticseh-alias.servicebus.windows.net

Workspace Environment Management 服务连接

Citrix 资源位置/Cloud Connector/代理：

`https://*.wem.cloud.com`

有关完整要求，请参阅 Workspace Environment Management 服务文档中的连接必备条件。

规划部署

July 1, 2024

要了解客户旅程视角，请转到 Citrix Success Center。成功中心为 Citrix 之旅的五个关键阶段提供指导：规划、构建、推出、管理和优化。成功中心文章和指南是本文档的配套内容，提供了基于解决方案的广泛视角。

服务试用和订阅

Citrix Cloud 为大多数云服务提供试用版。试用版具有与付费服务相同的特性和功能，因此它们适用于概念验证或试点部署。有关详细信息，请参阅 Citrix Cloud 服务试用版。

通常，付费服务权利可以有按月、按年或定期的期限。在授权即将到期时，Citrix Cloud 会发送提醒并提供宽限期，这样您就可以在不造成不当服务中断的情况下续订您的权利。有关续订您的权利的更多信息，请参阅 延长 Citrix Cloud 服务订阅。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

区域和服务状态

Citrix Cloud 在三个地区提供服务：美国、欧盟和亚太南部。注册 Citrix Cloud 时，必须选择最适合您的性能和业务需求的区域。

要了解有关选择区域和每个区域提供的服务的更多信息，请参阅 地理注意事项。

部署资源

- Citrix Cloud 弹性
- Tech Zone 概念验证指南
- Tech Zone 参考架构
- Cloud Connector 的扩展和大小注意事项
- 本地主机缓存的扩展和大小注意事项
- Citrix DaaS 的本地 StoreFront 身份验证参考架构

迁移资源

- 概念证明：自动配置工具
- 将本地的 Citrix Virtual Apps and Desktops 迁移到 Citrix Cloud
- 在 Microsoft Azure 上将 Citrix Virtual Apps and Desktops 从 VMware vSphere 迁移到 Citrix DaaS
- 使用 Citrix Endpoint Management 从 Android 设备管理员迁移到 Android Enterprise

更多信息

- Citrix Discussions：Citrix Cloud：Citrix Cloud 和 Citrix Cloud 服务的社区支持论坛
- Citrix 培训：
  - Citrix Cloud 基础知识
  - Citrix 身份和身份验证简介

Citrix Cloud 服务试用版

July 1, 2024

单个 Citrix Cloud 服务的试用版通过 Citrix Cloud 管理控制台提供。服务试用版中的功能与购买的服务相同，因此适用于概念验证 (POC) 或试点部署。

当您准备购买 Citrix Cloud 服务时，您的试用版将转换为生产服务。无需重新配置任何内容或创建单独的生产帐户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务试用概述

本节中的信息适用于大多数 Citrix Cloud 服务试用版。试用期不同的服务将在单独的章节中进行介绍。

		Citrix Cloud 试用版
	允许的订阅者数量	25
	试用的最大时长	60 个日历天
	宽限期	试用期满 14 天后
	数据保留期	试用期过期后 90 个日历日
	可用性	受限可用性
	资源位置	客户提供并配置
	用户会话长度	无限制
	本地 Microsoft Active Directory 集成	是
	资源位置的选择	是
	部署到本地	是
	Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）	完整功能集
	Endpoint Management	完整功能集
	可自定义	是

申请服务试用

Citrix Cloud 试用访问权限是基于每项服务进行管理的。对于某些服务，您可以按照本文中的 请求服务试用中所述请求试用 。对于其他服务，您必须在获得试用访问权限之前申请演示，如本文中的 请求服务演示 中所述。

服务试用期

对于大多数服务，试用申请获得批准后，您有 60 天的时间试用该服务。您只能为一项服务申请一次试用。

购买服务订阅

在试用期间或数据保留期内，您可以随时购买服务订阅。有关更多信息，请参阅 购买 Citrix Cloud 服务。

购买订阅后，您的试用版将转换为生产服务。管理员和用户可以访问该服务，并且您在试用期间添加的任何数据都将保持不变。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix DaaS Standard for Azure

本节介绍 Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）的以下试用类型：

- 自动批准的试用版：通过 Citrix Cloud 管理控制台 请求 试用版后，试用版将自动获得批准并可供使用。
- 经销售批准的试用版：联系 Citrix 销售代表请求试用后，销售代表将批准试用版。批准后，该试用版即可使用。

		自动批准的试用版	销售批准的试用版
	试用的最大时长	7 个日历天	14 个日历天
	宽限期	试用期满后 1 个日历日	试用期满后 14 个日历日
	数据保留期	试用期满后 30 个日历日	试用期过期后 90 个日历日

根据试用类型，您可以在 7 天或 14 天内使用该服务。只能申请试用服务一次。

试用包括试用期到期后访问服务的宽限期。此宽限期允许您购买该服务的订阅或删除您添加的任何数据。宽限期结束后，Citrix 将阻止管理员和用户访问该服务。

根据试用类型，Citrix 会在试用期到期后 30 天或 90 天内保留您添加到服务中的任何数据。如果您在此保留期内购买了该服务的订阅，则管理员和用户可以在您的数据完好无损的情况下访问该服务。

您可以通过 Azure 市场 或 联系您的 Citrix 销售代表购买该服务的订阅。

申请服务演示

对于某些服务，必须先向 Citrix 销售代表申请演示，然后才能试用该服务。通过申请演示，您可以与 Citrix 销售代表讨论贵组织的云服务需求。此外，销售代表还确保您拥有成功使用该服务所需的所有信息。

1. 登录到您的 Citrix Cloud 帐户。
2. 在管理控制台中，为所需的服务选择“请求演示”。此时将显示该服务的演示请求页面。
3. 填写并提交表单。Citrix 销售代表与您联系以提供更多信息，并指导您使用该服务。

申请服务试用版

1. 登录到您的 Citrix Cloud 帐户。
2. 在管理控制台中，为要试用的服务选择请求试用。

试用版获得批准并准备使用后，Citrix 会向您发送电子邮件通知。

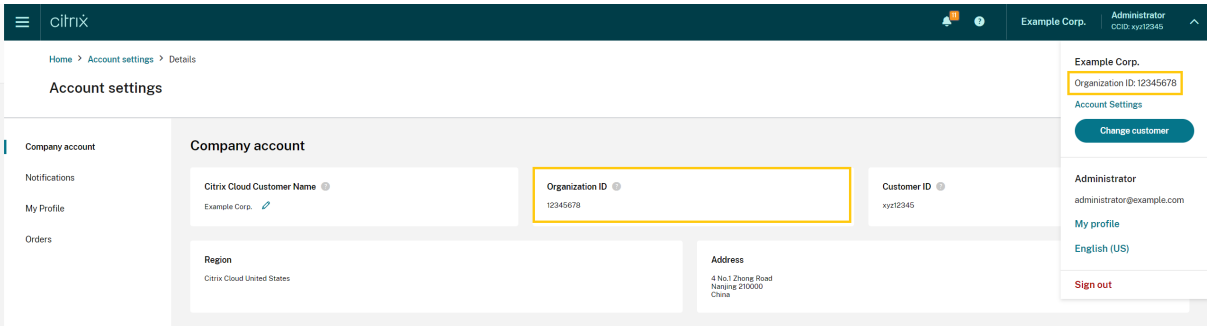
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 为了提供最佳的客户体验，Citrix 保留在任何给定时间为有限数量的参与者批准试用的权利。

购买 **Citrix Cloud** 服务

当您准备好将试用版转换为生产服务时，请访问 https://www.citrix.com/buy/ 寻找当地 Citrix 合作伙伴。

要购买该服务，您需要您的组织 ID (OrgID)。您的 OrgID 将显示在 Citrix Cloud 管理控制台右上角的客户菜单中。您的 OrgID 也会显示在“帐户设置”页面上。



更多信息

- Citrix Cloud 服务的服务条款
- Citrix Cloud 基础知识 课程包括一个简短的视频，指导您申请试用。完整课程还涵盖了 Citrix Cloud 平台及其服务的组件。

延长 **Citrix Cloud** 服务订阅

July 1, 2024

本文介绍购买的 Citrix Cloud 服务订阅的过期时间以及如何延长订阅。

在本文中，月度订阅 是指按月购买的服务。年度订阅 是指按年购买的服务。多年期订阅 是指以多年为基础购买的服务。

> 注意：
>
> Citrix Service Provider (CSP) 可以通过向其 CSP 分销商提交零美元采购订单来延长订阅期限。有关 CSP 产品续订和许可的详细信息，请参阅 面向 *Citrix Cloud* 的 *Citrix Service Provider* 许可指南，该指南可通过 Citrix Partner Central Web 站点获得。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

到期前

对于月度订阅，Citrix Cloud 不会在到期前发送通知。

对于年度和多年期订阅，Citrix Cloud 会在现有订阅即将到期时按特定时间间隔通知您。这些通知将提醒您延长订阅期限，避免服务中断。Citrix Cloud 管理控制台中将显示以下通知：

- 到期前 90 天：出现黄色横幅，显示需要延期的服务及其到期日期。此通知每七天在控制台中显示一次，或者直到服务延长为止。
- 到期前七天：将出现一个红色横幅，显示需要延期的服务及其到期日期。此通知将一直显示在控制台中，直到服务延长或 30 天过期宽限期结束。

当这些通知出现时，您可以将其关闭；但是，它们将在七天后重新显示。

Citrix 还会向您发送电子邮件通知，其中包含需要延期的服务及其到期日期的列表。Citrix 按以下时间间隔发送此通知：

- 到期前 90 天
- 到期前 60 天
- 到期前 30 天
- 到期前七天
- 到期前一天

过期后：服务块和数据保留

如果在宽限期内未延长服务订阅，Citrix 将按以下方式阻止对服务的访问：

- 对于过期的月度订阅，管理员和用户在过期日期过后五天后将被禁止访问。
- 对于过期的年度和多年期订阅，管理员和用户将在过期日期后 30 天后被阻止访问。

Citrix 会在服务过期日期后将您添加到服务的所有数据保留 90 天。如果您在 90 天保留期结束之前延长订阅，则管理员和用户可以在数据完好无损的情况下访问该服务。您的延期订阅开始时间如下：

- 对于月度订阅，第一个月订阅的开始日期是您购买扩展的日期。之后，您的订阅将在随后每个月的第一天自动续订。
- 对于年度和多年订阅，延期订阅的开始日期是到期日期后的第二天。例如，如果您的订阅在 9 月 30 日到期，而您在 10 月 23 日延长订阅，则延期订阅的开始日期为 10 月 1 日。

如果您未在 90 天保留期结束之前延长订阅，Citrix 会重置服务并删除您添加的所有数据。如果您同意允许 Citrix 管理您的云部署（例如，使用 Citrix Essentials 服务或 Citrix DaaS 中的 Azure 快速部署选项时），Citrix 将在 90 天保留期结束后执行以下操作：

- 从 Citrix 数据库中删除所有与客户相关的数据。
- 删除 Citrix 在云环境中预配的与 Citrix Cloud 服务相关的所有资源，包括 Citrix 托管的 VM。有关特定 Citrix Cloud 服务中包含的 Citrix 托管组件的说明，请参阅该服务的文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

客户管理的 **Azure** 订阅

如果您将自己的 Azure 订阅与 Citrix Cloud 服务配合使用，则当您将 Azure 订阅连接到该服务时，该服务将安装应用程序。如果您不延长 Citrix Cloud 服务订阅，Citrix 不会在 90 天保留期结束后从您的 Azure 订阅中删除此应用程序。必须删除此应用程序才能从 Azure 订阅中完全删除该服务。您可以使用以下方法之一删除应用程序：

- 如果尚未阻止管理员访问该服务，请从服务中删除此应用程序。
- 如果管理员被阻止访问该服务，请从 Azure 门户中删除此应用程序。

购买服务延期

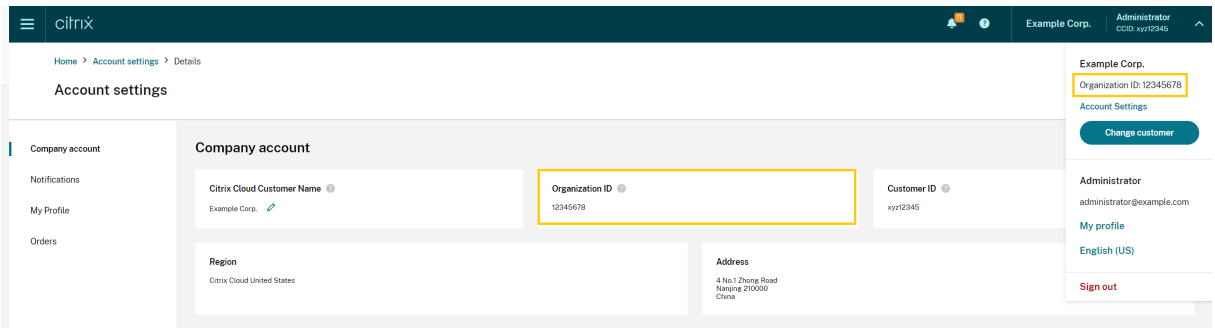
要延长 Citrix Cloud 服务的订阅，请联系您的 Citrix 销售代表。要找到您的销售代表，请使用以下步骤：

1. 登录到您的 Citrix 帐户。
2. 选择 报价 **(DOTI)**，然后选择 交易。您的销售代表及其电子邮件地址显示在此视图顶部附近。

或者，访问 Citrix 客户服务 页面以获取您所在地理区域的联系信息。

要完成购买，您的销售代表需要您的 Citrix Cloud 帐户的组织 ID。要查找您的组织 ID，请登录您的 Citrix Cloud 帐户。您的组织 ID 显示在以下位置：

- 在 Citrix Cloud 控制台右上角的客户菜单中。
- 在“帐户设置”页面上。



地理方面的注意事项

July 1, 2024

本文讨论了 Citrix Cloud 使用的商业区域以及每个区域中是否存在 Citrix Cloud 商业服务。

有关 Citrix 公共部门和专用云平台的地理区域和服务状况的更多信息，请参阅 Citrix 提供的其他云平台。

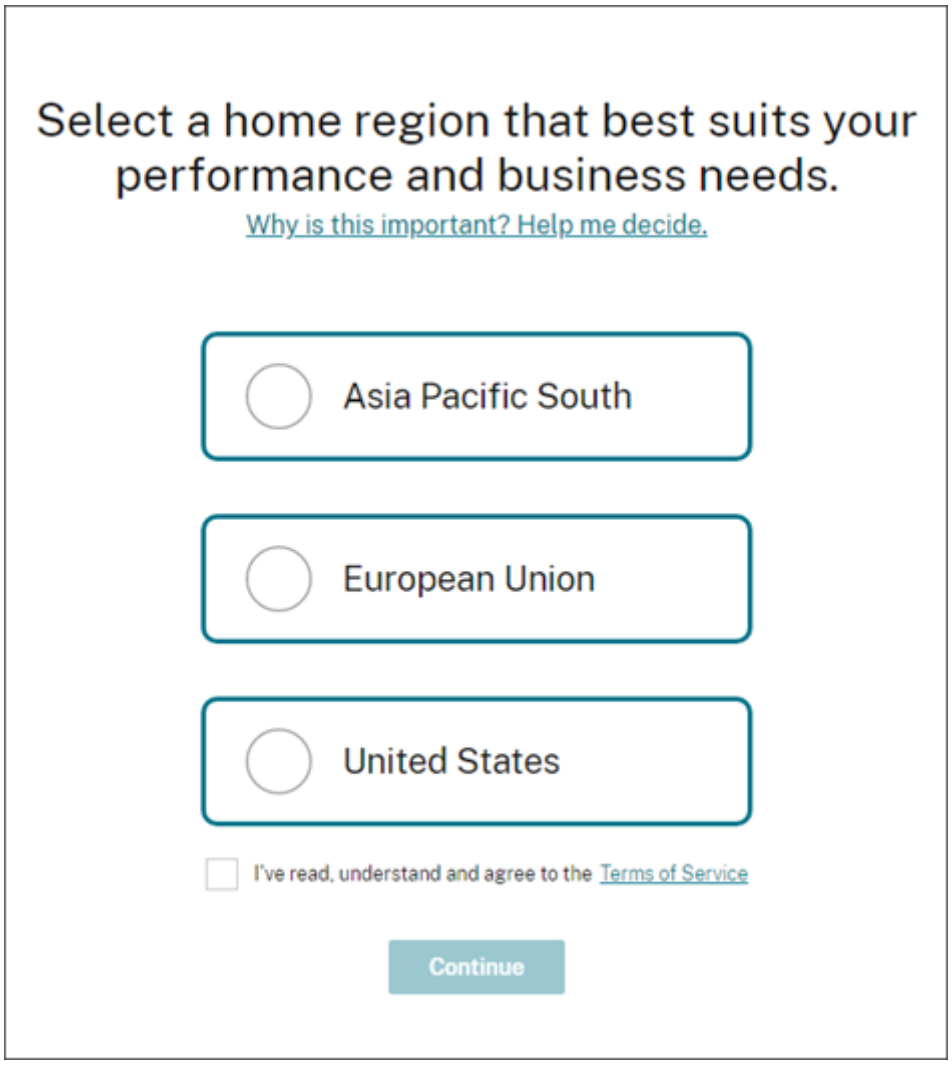
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择一个地区

当您的组织加入到 Citrix Cloud 并且您首次登录时，系统会要求您选择以下区域之一：

- 美国
- 欧洲联盟
- 亚太南部

当您选择区域时，该地理区域中托管的服务将尽可能用于与组织相关的操作。选择一个映射到大多数用户和资源所在的区域。



> 重要注意事项：
>
> - 当您的组织加入时，您只能选择一次区域。以后将无法更改您的区域。
> - 如果您位于一个区域，而在另一个地区使用服务，则对性能的影响将微乎其微。Citrix Cloud 服务旨在在

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 全球范围内使用。例如，在澳大利亚拥有用户和连接器的美国客户将看到延迟的影响最小。
> - 如果您所在的地区不支持 Citrix Cloud，请选择一个距离您的大部分用户和资源所在地最近的区域。

每个地区的服务存在

大部分 Citrix Cloud 服务都是在全球范围内复制的。您选择的区域表示必须在何处建立连接的首选项。但是，仍可能与其他地理区域建立联系。当一项服务进行全局复制时，该服务的所有数据都存储在所有区域。

同样，Citrix 关联公司或子处理方可能会在全球范围内处理您的数据，以执行服务。

某些服务有专用的区域实例。某些服务仅有美国的实例。在这些情况下，连接和数据包含在地理区域内。

如果某项服务在您为组织选择的区域不可用，则某些信息（例如身份验证数据）可能会根据需要在区域之间传输。

服务	美国	欧盟	亚太南部	备注
Citrix Cloud 控制平面	是	是	是	
Citrix Analytics for Security	是	是	是	
Citrix Analytics for Performance	是	是	是	
NetScaler 控制台（前身为应用程序交付管理）	是	是	是	请参阅本文中的使用 Console Advisory Connect 对 NetScaler 实例进行低接触式加载。有关控制台本地遥测程序，请参阅此处。
Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）	是	是	是	服务使用 Citrix Cloud 区域。
Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Virtual Apps and Desktops Standard）	是	是	是	服务使用 Citrix Cloud 区域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务	美国	欧盟	亚太南部	备注
适用于 Google Cloud 的 Citrix DaaS Standard（以前称为适用于 Google Cloud 的 Virtual Apps and Desktops Standard）	是	否（使用美国地区）	否（使用美国地区）	
Citrix DaaS Premium for Google Cloud（以前称为 Virtual Apps and Desktops Premium for Google Cloud）	是	否（使用美国地区）	否（使用美国地区）	
Citrix Endpoint Management	是	是	是	从多个区域的多个位置中进行选择。请参阅本文中的 Endpoint Management 服务位置 。
Remote Browser Isolation 服务	是	是	是	服务使用 Citrix Cloud 区域。
SD-WAN Orchestrator	是	是	是	
Citrix Secure Internet Access 节点/POP	多个全球范围内的节点；流量根据需要路由，以确保最佳体验全球复制	多个全球范围内的节点；流量根据需要路由，以确保最佳体验全球复制	多个全球范围内的节点；流量根据需要路由，以确保最佳体验全球复制	请参阅本文中的安全 Internet 访问服务位置。
Citrix Secure Private Access				请参阅本文中的 Secure Private Access 接入点。
Session Recording 服务	是	是	是	
Citrix Virtual Apps Essentials	是	是	是	服务使用 Citrix Cloud 区域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务	美国	欧盟	亚太南部	备注
Citrix Virtual Desktops Essentials	是	是	是	服务使用 Citrix Cloud 区域。
Web App Firewall	是	是	否（使用美国地区）	
Workspace Environment Management; Citrix Optimization Pack	是	是	是	
联网服务	是	否（使用美国地区）	否（使用美国地区）	
License Usage Insights（仅限 CSP）	全球复制	全球复制	全球复制	
Citrix Gateway 服务访问节点/POP	多个全球范围内的节点；流量根据需要路由，以确保最佳体验	多个全球范围内的节点；流量根据需要路由，以确保最佳体验	多个全球范围内的节点；流量根据需要路由，以确保最佳体验	您可以配置资源位置以启用将用户流量路由到特定区域。有关更多信息，请参阅地理位置路由 - 预览版

> 注意：
>
> 某些区域服务可能附带上表其他地方列出的非区域组件服务的权利，并可由客户选择使用。
>
> Citrix Cloud Services 使用客户的指定区域来存储客户内容和日志，但由 Citrix 子处理器收集的部分日志或需要非区域存储才能执行服务（包括支持或故障排除、监视性能、安全、审核）以及允许跨区域身份验证（例如，当欧盟的支持工程师需要访问美国环境时）除外。如有必要，可以在全球范围内访问客户内容和日志，以执行服务。

有关各个服务存储的数据的详细信息，请参阅每项服务的 技术安全概述 。

使用 **Console Advisory Connect** 以低接触方式加载 **NetScaler** 控制台实例

作为基于 Console Advisory Connect 的控制台实例低接触入门的一部分：

- 如果您是 Citrix Cloud 的现有客户，则在创建 Citrix Cloud 帐户时选择的地理区域中创建控制台服务租户。
- 如果您不是 Citrix Cloud 的现有客户，则会引用 Citrix.com 门户中为该客户提及的地址。占位控制台服务租户是在与该推荐地址的区域相对应的地理区域中创建的。如果您将来选择加入 Citrix Cloud，则将在创建 Citrix Cloud 帐户时选择的相同区域创建新的控制台服务租户。此外，数据将从占位控制台服务租户迁移到新的控制台服务租户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Endpoint Management 服务位置

您可以从您的本地区域中选择以下 Endpoint Management 服务位置之一：

- 美国东部
- 美国西部
- 欧盟西部
- 东南亚
- 悉尼

安全的互联网接入服务地点

流量根据可用性和最终用户接近程度路由到以下安全互联网接入服务位置，以确保获得最佳体验。

北美

- 美国弗吉尼亚州斯特林
- 加拿大多伦多
- 美国加利福尼亚州洛杉矶
- 美国加利福尼亚州欧文
- 美国华盛顿州西雅图
- 美国科罗拉多州丹佛
- 美国北卡罗来纳州夏洛特
- 美国德克萨斯州达拉斯
- 美国德克萨斯州艾伦
- 美国佛罗里达州迈阿密
- 美国伊利诺伊州芝加哥
- 美国纽约州纽约
- 美国麻萨诸塞州波士顿
- 加拿大温哥华

南美洲

- 墨西哥克雷塔罗
- 巴西圣保罗
- 阿根廷布宜诺斯艾利斯
- 哥伦比亚波哥大

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

亚太地区

- 澳大利亚珀斯
- 澳大利亚悉尼
- 日本东京
- 新加坡、新加坡
- 印度孟买
- 印度德里

非洲

南非约翰内斯堡

中东

- 阿拉伯联合酋长国迪拜
- 土耳其伊斯坦布尔

西欧

- 英国伦敦
- 英国曼彻斯特
- 德国法兰克福
- 德国杜塞尔多夫
- 德国曼海姆
- 法国巴黎

欧洲

- 芬兰赫尔辛基
- 荷兰阿姆斯特丹
- 瑞典斯德哥尔摩
- 波兰华沙
- 西班牙马德里
- 保加利亚索菲亚
- 瑞士苏黎世
- 意大利米兰

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Secure Private Access 接入点

有关 Secure Private Access 用来确保为客户提供服务的连续性和质量的接入点 (PoP) 列表，请参阅 Secure Private Access 服务文档中的 Secure Private Access 的所有接入点 (PoP) 位于哪里？ 。

Citrix 提供的其他云平台

除了 Citrix Cloud 之外，Citrix 还提供其他与 Citrix 云隔离和分离的云。

Citrix Cloud Government

Citrix Cloud Government 允许美国政府机构和美国的其他公共部门客户根据法规和合规性要求使用 Citrix 云服务。Citrix Cloud Government 是 Citrix 运营、存储和复制服务和数据以交付 Citrix Cloud Government 服务的地理边界。Citrix 可能会使用位于美国一个或多个州的多个公共云或私有云来提供服务。

Citrix Cloud Government 和提供的服务仅在美国地区提供。

有关详细信息，请参阅 Citrix Cloud Government 产品文档。

Citrix Cloud Japan

Citrix Cloud Japan 允许日本客户在 Citrix 管理的专用环境中使用某些 Citrix 云服务。Citrix Cloud Japan 和所提供的服务仅在日本提供。

有关更多信息，请参阅 Citrix Cloud Japan 产品文档。

适用于 **Citrix Cloud** 平台的安全部署指南

July 1, 2024

《适用于 Citrix Cloud 的安全部署指南》概述了使用 Citrix Cloud 时的安全性最佳做法并介绍了 Citrix Cloud 收集和管理的信息。

服务的技术安全概述

有关 Citrix Cloud Services 中数据安全的更多信息，请参阅以下文章：

- 分析技术安全概述
- Endpoint Management 技术安全概述
- Remote Browser Isolation 技术安全概述

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix DaaS 技术安全概述
- Citrix DaaS Standard for Azure 技术安全概述

管理员指南

- 使用强密码并定期更改您的密码。
- 客户帐户内的所有管理员都可以添加和删除其他管理员。确保只有受信任的管理员有权访问 Citrix Cloud。
- 客户的管理员默认对所有服务具有完全访问权限。某些服务提供限制管理员的访问权限的功能。有关详细信息，请参阅每项服务的文档。
- Citrix Cloud 管理员的双重身份验证是使用默认 Citrix 身份提供商实现的。当管理员注册 Citrix Cloud 或受邀加入 Citrix Cloud 帐户时，他们需要注册多因素身份验证 (MFA)。如果客户使用 Microsoft Azure 对 Citrix Cloud 管理员进行身份验证，则可以按照 Microsoft Web 站点上配置 Azure AD 多重身份验证设置中的说明配置多因素身份验证。
- 默认情况下，无论控制台活动如何，Citrix Cloud 都会在 24 小时后自动终止管理员会话。此超时无法更改。
- 管理员帐户最多可以与 100 个客户帐户关联。如果管理员需要管理 100 多个客户帐户，则他们必须使用不同的电子邮件地址创建一个单独的管理员帐户来管理其他客户帐户。或者，可以将他们作为管理员从不再需要管理的客户帐户中删除。

密码合规性

如果存在以下情况之一，Citrix Cloud 会提示管理员更改密码：

- 当前密码已超过 60 天未用于登录。
- 当前密码已在已知的泄露密码数据库中列出。

新密码必须满足以下所有条件：

- 长度至少为 8 个字符（最多 128 个字符）
- 至少包含一个大写和小写字母
- 至少包含一个数字
- 包含至少一个特殊字符:!@ # $% ^ *? + =-

更改密码的规则：

- 当前密码不能用作新密码。
- 之前的 5 个密码无法重复使用。
- 新密码不能与帐户用户名相似。
- 新密码不得在已知的泄露密码数据库中列出。Citrix Cloud 使用 https://haveibeenpwned.com/ 提供的列表来确定新密码是否违反此条件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

加密和密钥管理

Citrix Cloud 控制平面不存储敏感的客户信息。相反，Citrix Cloud 会按需检索管理员密码等信息（通过明确提示管理员）。

对于静态数据，Citrix Cloud 存储使用 AES-256 位或更高的密钥进行加密。这些密钥由 Citrix 管理。

对于动态数据，Citrix 使用行业标准 TLS 1.2 以及最强的密码套件。客户无法控制正在使用的 TLS 证书，因为 Citrix Cloud 托管在 Citrix 拥有的 cloud.com 域中。要访问 Citrix Cloud，客户必须使用支持 TLS 1.2 的浏览器，并且必须配置接受的密码套件。

- 如果从 Windows Server 2016、Windows Server 2019 或 Windows Server 2022 访问 Citrix Cloud 控制平面，建议使用以下强密码：TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- 如果从 Windows Server 2012 R2 访问 Citrix Cloud 控制平面，则强密码不可用，因此必须使用以下密码：TLS_DHE_RSA_WITH_AES_256_GCM_SHA384、TLS_DHE_RSA_WITH_AES_128_GCM_SHA256、TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384、TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

有关如何保护 Citrix Cloud 服务数据的更多信息，请参阅 Citrix Web 站点上的 Citrix Cloud Services 数据保护概述。

有关每个云服务中的加密和密钥管理的更多信息，请参阅该服务的文档。

有关 TLS 1.2 配置的更多信息，请参阅以下文章：

- 在客户端计算机上强制使用 TLS 1.2：CTX245765，查询 Monitoring Service 的 OData 端点时出现错误：“底层连接已关闭：发送时出现意外错误。”
- Microsoft Docs Web 站点上的更新和配置.NET Framework 以支持 TLS 1.2。

数据主权

Citrix Cloud 控制平面托管在美国、欧盟和澳大利亚。客户无法对此进行控制。

客户拥有和管理与 Citrix Cloud 结合使用的资源位置。可以在客户要求的任何数据中心、云、位置或地理区域中创建资源位置。所有关键的业务数据（例如，文档、电子表格等）都存储在资源位置中，由客户控制。

其他服务可能具有在不同的地区存储数据的选项。有关每项服务，请查阅 地理注意事项 主题或 技术安全概述 （在本文开头列出）。

安全问题见解

status.cloud.com 网站提供对持续影响客户的安全问题的透明度。站点日志状态和运行时信息。存在一个用于订阅平台或各项服务的更新的选项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud Connector

安装 Cloud Connector

出于安全和性能原因，Citrix 建议客户不要在域控制器上安装 Cloud Connector 软件。

此外，Citrix 强烈建议安装了 Cloud Connector 软件的计算机位于客户的专用网络内，而不是位于 DMZ 中。有关网络和系统要求以及安装 Cloud Connector 的说明，请参阅 Citrix Cloud Connector。

配置 Cloud Connector

客户负责通过安装 Windows 安全更新来保持安装了 Cloud Connector 的计算机处于最新状态。

客户可以与 Cloud Connector 一起使用防病毒软件。Citrix 测试了 McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8。Citrix 为使用其他行业标准音视产品的客户提供支持。

在客户的 Active Directory (AD) 中，Citrix 强烈建议将 Cloud Connector 的计算机帐户限制为只读访问权限。这是 Active Directory 中的默认配置。此外，客户还可以在 Cloud Connector 的计算机帐户上启用 AD 日志记录和审核，以监视任何 AD 访问活动。

登录托管 Cloud Connector 的计算机

Cloud Connector 允许将敏感的安全信息传递到 Citrix Cloud 服务中的其他平台组件，但也存储以下敏感信息：

- 用于与 Citrix Cloud 通信的服务密钥
- Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）中用于电源管理的 Hypervisor 服务凭据

这些敏感信息在托管 Cloud Connector 的 Windows 服务器上使用数据保护 API (DPAPI) 进行加密。Citrix 强烈建议只允许权限最高的管理员登录 Cloud Connector 计算机（例如，执行维护操作）。一般而言，管理员不需要登录这些计算机即可管理任何 Citrix 产品。Cloud Connector 在管理方面执行自助管理。

请勿允许最终用户登录托管 Cloud Connector 的计算机。

在 Cloud Connector 计算机上安装其他软件

客户可以在安装了 Cloud Connector 的计算机上安装防病毒软件和虚拟机管理程序工具（如果已在虚拟机上安装）。但是，Citrix 建议客户不要在这些计算机上安装任何其他软件。其他软件可能会产生安全攻击媒介，并可能降低整个 Citrix Cloud 解决方案的安全性。

入站和出站端口配置

Cloud Connector 要求打开对 Internet 具有访问权限的出站端口 443。Citrix 强烈建议 Cloud Connector 没有可从互联网访问的入站端口。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

客户可以在用于监视其出站 Internet 通信的 Web 代理后面找到 Cloud Connector。但是，Web 代理必须支持 SSL/TLS 加密通信。

Cloud Connector 可能有其他可以访问互联网的出站端口。如果有其他端口可用，Cloud Connector 可通过各种端口进行协商，以优化网络带宽和性能。

Cloud Connector 必须具有在内部网络中打开的范围广泛的入站和出站端口。下表列出了所需的基本开放端口集。

客户端口	服务器端口	服务
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	RPC 终结点映射程序
49152 -65535/TCP	464/TCP/UDP	Kerberos 密码更改
49152 -65535/TCP	49152-65535/TCP	RPC（适用于 LSA）、SAM、Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

Cloud Connector 使用 LDAP 签名和密封来保护与域控制器的连接。这意味着不需要基于 SSL 的 LDAP (LDAPS)。有关 LDAP 签名的更多信息，请参阅如何在 Windows Server 中启用 LDAP 签名和 Microsoft 启用 LDAP 通道绑定和 LDAP 签名的指南。

Citrix Cloud 中使用的每项服务都扩展了所需的开放端口列表。有关详细信息，请参阅以下资源：

- 每项服务的技术安全概述（在本文开头列出）
- Citrix Cloud 服务的 Internet 连接要求
- 控制台服务端口要求
- Endpoint Management 端口要求

监视出站通信

Cloud Connector 在端口 443 上与 Internet 进行出站通信，将通信同时传输至 Citrix Cloud 服务器和 Microsoft Azure 服务总线服务器。

Cloud Connector 与本地网络中托管 Cloud Connector 的计算机所在的 Active Directory 林中的域控制器进行通信。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在正常操作期间，Cloud Connector 仅与 Citrix Cloud 用户界面的“身份和访问管理”页面上未禁用的域中的域控制器进行通信。

Citrix Cloud 中的每项服务都会扩展 Cloud Connector 在正常操作期间可能联系的服务器和内部资源的列表。此外，客户无法控制 Cloud Connector 发送到 Citrix 的数据。有关服务向 Citrix 发送的内部资源和数据的详细信息，请参阅以下资源：

- 每项服务的技术安全概述（在本文开头列出）
- Citrix Cloud 服务的 Internet 连接要求

查看 **Cloud Connector** 日志

与管理员有关的或者管理员可操作的任何信息都在 Cloud Connector 计算机上的 Windows 事件日志中提供。

请查看以下目录中的 Cloud Connector 的安装日志：

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Cloud Connector 向云发送的信息的日志位于%ProgramData%\Citrix\WorkspaceCloud\Logs 中。

超出指定的大小阈值时，将删除 WorkspaceCloud\Logs 目录中的日志。管理员可以通过调整 HKEY_LOCAL_MACHINE\SOFTWAR 的注册表项值来控制此大小阈值。

SSL/TLS 配置

托管 Cloud Connector 的 Windows Server 必须启用 加密和密钥管理 中详细介绍的密码。

Cloud Connector 必须信任 Citrix Cloud SSL/TLS 证书和 Microsoft Azure 服务总线 SSL/TLS 证书使用的证书颁发机构 (CA)。Citrix 和 Microsoft 将来可能会更改证书和 CA，但始终使用属于标准 Windows 可信发布者列表一部分的 CA。

Citrix Cloud 中的每项服务可能有不同的 SSL 配置要求。有关更多信息，请参阅每项服务的 技术安全概述 （在本文开头列出）。

安全合规性

为确保安全合规性，Cloud Connector 可自行管理。请勿禁用重新启动，或者对 Cloud Connector 设置其他限制。这些操作将阻止 Cloud Connector 在有关键更新时进行自助更新。

客户不需要采取任何其他操作来对安全问题做出反应。Cloud Connector 将自动应用所有安全修复。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

适用于云服务的 **Citrix Connector Appliance**

安装 **Connector Appliance**

Connector Appliance 托管在虚拟机管理程序上。此虚拟机管理程序必须位于您的专用网络内部，而不在 DMZ 中。

确保 Connector Appliance 位于默认情况下阻止访问的防火墙内。使用允许列表仅允许来自 Connector Appliance 的预期流量。

确保托管 Connector Appliance 的虚拟机管理程序安装了最新的安全更新。

有关网络和系统要求以及安装 Connector Appliance 的说明，请参阅适用于云服务的 Connector Appliance。

登录到托管 **Connector Appliance** 的虚拟机管理程序

Connector Appliance 包含用于与 Citrix Cloud 通信的服务密钥。仅允许特权最高的管理员登录托管 Connector Appliance 的虚拟机管理程序（例如，执行维护操作）。通常，管理员无需登录这些虚拟机管理程序即可管理任何 Citrix 产品。Connector Appliance 是自我管理的。

入站和出站端口配置

Connector Appliance 需要打开出站端口 443 才能访问 Internet。Citrix 强烈建议 Connector Appliance 没有可从 Internet 访问的入站端口。

您可以在 Web 代理后面找到 Connector Appliance 以监视其出站 Internet 通信。但是，Web 代理必须支持 SSL/TLS 加密通信。

Connector Appliance 可能有其他可以访问 Internet 的出站端口。如果有其他端口可用，Connector Appliance 会跨各种端口进行协商，以优化网络带宽和性能。

Connector Appliance 必须在内部网络中打开大量的入站和出站端口。下表列出了所需的基本开放端口集。

连接方向	Connector Appliance 端口	外部端口	服务
入库	443/TCP	任意	本地 Web 用户界面
出站	49152-65535/UDP	123/UDP	NTP
出站	53、49152-65535/TCP/UDP	53/TCP/UDP	DNS
出站	67/UDP	68/UDP	DHCP 和广播
出站	49152 -65535/UDP	123/UDP	W32Time
出站	49152 -65535/TCP	464/TCP/UDP	Kerberos 密码更改

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

连接方向	Connector Appliance 端口	外部端口	服务
出站	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
出站	49152 -65535/TCP	3268/TCP	LDAP GC
出站	49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
出站	49152 -65535/TCP/UDP	445/TCP	SMB
出站	137/UDP	137/UDP	NetBIOS 名称服务
出站	138/UDP	138/UDP	NetBIOS 数据报
出站	139/TCP	139/TCP	NetBIOS 会话

Citrix Cloud 中使用的每项服务都扩展了所需的开放端口列表。有关详细信息，请参阅以下资源：

- 每项服务的技术安全概述（在本文开头列出）
- Citrix Cloud 服务的系统和连接要求

监视出站通信

Connector Appliance 通过端口 443 与 Citrix Cloud 服务器进行出站通信。

Citrix Cloud 中的每项服务都会扩展 Connector Appliance 在正常操作期间可能联系的服务器和内部资源的列表。此外，客户无法控制 Connector Appliance 发送到 Citrix 的数据。有关服务向 Citrix 发送的内部资源和数据的详细信息，请参阅以下资源：

- 每项服务的技术安全概述（在本文开头列出）
- Citrix Cloud 服务的系统和连接要求

查看 **Connector Appliance** 日志

您可以下载包含各种日志文件的 Connector Appliance 的诊断报告。有关获取此报告的更多信息，请参阅适用于云服务的 Connector Appliance。

SSL/TLS 配置

Connector Appliance 不需要任何特殊的 SSL/TLS 配置。

Connector Appliance 信任 Citrix Cloud SSL/TLS 证书使用的证书颁发机构 (CA)。Citrix 将来可能会更改证书和 CA，但始终使用 Connector Appliance 信任的 CA。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 中的每项服务可能有不同的 SSL 配置要求。有关更多信息，请参阅每项服务的 技术安全概述 （在本文开头列出）。

安全合规性

为确保安全合规，Connector Appliance 自行管理，您无法通过控制台登录。

您无需采取任何其他措施来应对连接器安全问题。Connector Appliance 会自动应用所有安全修复程序。

确保托管 Connector Appliance 的虚拟机管理程序安装了最新的安全更新。

在 Active Directory (AD) 中，我们建议将 Connector Appliance 计算机帐户限制为只读访问权限。这是 Active Directory 中的默认配置。此外，客户还可以在 Connector Appliance 计算机帐户上启用 AD 日志记录和审核，以监视任何 AD 访问活动。

处理受到威胁的帐户的指南

- 审核 Citrix Cloud 中的管理员列表并删除任何不受信任的管理员。
- 禁用贵公司 Active Directory 中所有被盗用的帐户。
- 联系 Citrix 并要求轮转为客户的所有 Cloud Connector 存储的授权机密。根据破坏的严重程度执行以下操作：
  - 低风险： Citrix 可以随着时间的推移轮换密钥。Cloud Connector 继续正常运行。旧的授权密钥将在 2-4 周后失效。请在此时间内监视 Cloud Connector，以确保不执行任何非预期操作。
  - 持续存在的高风险： Citrix 可以撤销所有旧密钥。现有的 Cloud Connector 将不再运行。要继续正常运行，客户必须在所有适用的计算机上卸载并重新安装 Cloud Connector。

创建 **Citrix Cloud** 帐户

December 14, 2023

本文将引导您完成创建 Citrix Cloud 帐户以及完成成功注册帐户所需任务的过程。

与 Citrix 有合作关系且刚接触 Citrix Cloud Services 的客户可以使用本文中的任务来完成载入流程。

Citrix 新客户的注册流程

如果您不熟悉 Citrix 和 Citrix Cloud，则必须联系 Citrix 为您的公司创建一个新的 Citrix 帐户。使用以下联系方式之一：

- 请联系 Citrix Customer Service。
- 联系您所在地区的 Citrix Partner 或 Citrix Sales 办事处。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

当您联系 Citrix 时，您可以与 Citrix 代表讨论您的业务需求。该代表将帮助您完成注册过程并为您提供您的 Citrix 登录凭据。

收到 Citrix 帐户凭据后，您可以使用本文中的任务登录并开始使用 Citrix Cloud。

什么是 **Citrix** 帐户

Citrix 帐户（也称为 Citrix.com 帐户或 My Citrix 帐户）使您能够管理对已购买许可证的访问权限。您的 Citrix 帐户使用组织 ID (OrgID) 作为唯一标识符。您可以使用用户名（也称为网络登录）或您的电子邮件地址（如果已关联到您的帐户）登录 https://www.citrix.com 来访问您的 Citrix 帐户。

> 重要：
>
> 用户名映射到一个唯一的 Citrix 帐户，但一个电子邮件地址可以映射到多个 Citrix 帐户。

什么是 **OrgID**

OrgID 是分配给您的 Citrix 帐户的唯一标识符。您的 OrgID 与实际站点地址相关联，通常是您公司的公司地址。公司通常只有一个 OrgID。但是，在某些情况下，例如拥有不同的分支机构或由不同的部门分别管理其资产，Citrix 可能允许单个公司拥有多个 OrgID。

Citrix 会定期清理某些 OrgID，在某些情况下合并重复项。如果贵公司有 OrgID 要与有效且活跃的 OrgID 合并，则可以联系 Citrix 客户支持部门提供要合并的 OrgID。

> 注意：
>
> 各公司已经根据自己想要的资产管理方式设置了 OrgID，因此，如果您不知道需要使用哪个 OrgID 或拥有多少 OrgID，请联系公司的 IT 部门或 Citrix 管理员。如果您需要帮助，请通过 https://www.citrix.com/support/ 与 Citrix Customer Service 部门联系，找到您的 OrgID。

什么是 **Citrix Cloud** 帐户

Citrix Cloud 帐户使您能够使用一个或多个 Citrix Cloud Services 来安全地交付应用程序和数据。Citrix Cloud 帐户由客户 ID 标识，并与 OrgID 关联。一个 OrgID 可以与多个 Citrix Cloud 客户 ID 关联，但一个客户 ID 只能与一个 OrgID 相关联。

请务必根据贵组织设置 OrgID 的方式使用正确的 Citrix Cloud 帐户，这样您的购买和管理员访问权限才能继续使用相同的 OrgID。例如，如果一家使用 OrgID 1234 的公司的设计部门一直在本地使用虚拟应用程序和桌面，并想试用 Citrix Cloud，那么 OrgID 1234 的一位管理员可以使用其 Citrix 帐户登录凭据或与该 OrgID 关联的电子邮件地址在该 OrgID 上注册 Citrix Cloud。当公司决定购买 Citrix DaaS 订阅时，可以在 OrgID 1234 上正确下订单。

> 重要：
>
> 有权访问特定 Citrix 帐户的用户不会自动访问与该 Citrix 帐户的 OrgID 关联的 Citrix Cloud 帐户。由于 Citrix

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> Cloud 访问允许用户对服务产生潜在影响，因此控制谁访问 Citrix Cloud 帐户非常重要。

多因素身份验证

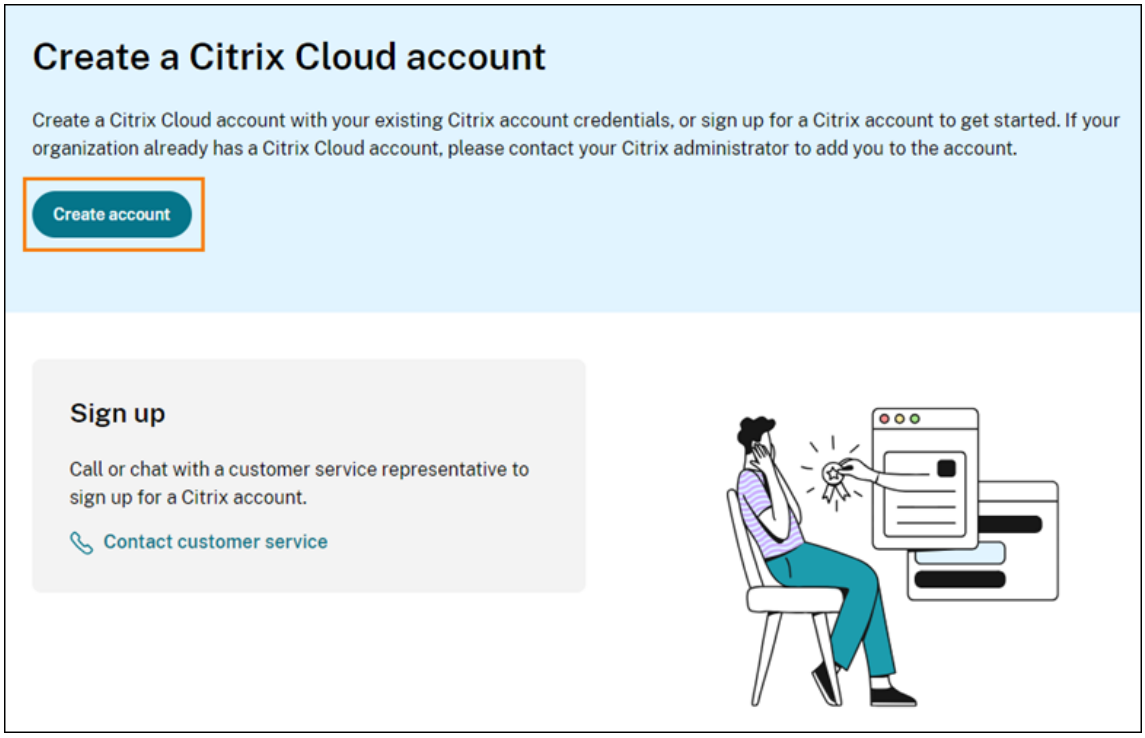
为了确保您的 Citrix Cloud 帐户安全，Citrix 要求所有客户注册多重身份验证 (MFA)。要注册，您只需要一台设备（例如计算机或移动设备），并安装身份验证器应用程序，例如 Citrix SSO。如果无法使用带有身份验证器应用程序的设备，则可以改用电子邮件地址。

如果您尚未注册 MFA，则当您使用 Citrix 帐户凭据登录时，Citrix 会提示您进行注册。有关要求和说明，请参阅本文中的步骤 2：设置多重身份验证。

第 **1** 步：访问 **Citrix Cloud Web** 站点

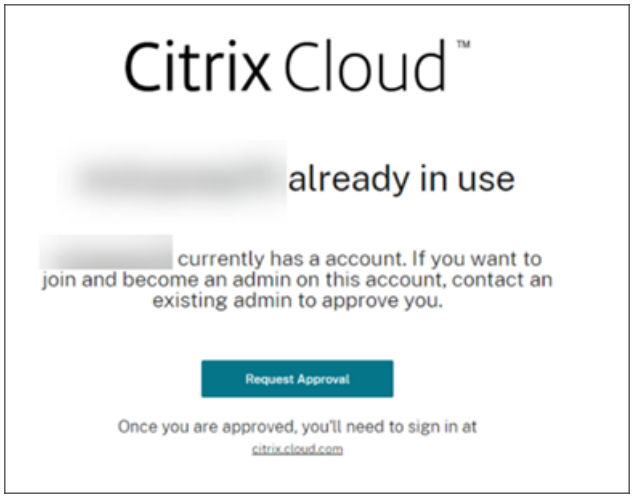
1. 使用网络浏览器访问 https://onboarding.cloud.com。
2. 选择 创建帐户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 输入您的用户名和密码或与您的 Citrix.com 帐户关联的电子邮件地址和密码。

如果帐户已经在使用中会发生什么



如果您看到一条消息，表明贵组织的 Citrix Cloud 帐户已在使用中，则表示您的 Citrix 帐户中的另一位管理员已经创建了 Citrix Cloud 帐户。即使您已经是 Citrix 帐户的成员，现有管理员也需要邀请您成为管理员，然后才能访问该帐户。

由于 Citrix Cloud 帐户允许管理员更好地控制服务，因此我们希望创建 Citrix Cloud 帐户的第一个管理员必须明确授予其他管理员访问权限，即使其他管理员已经是 Citrix 帐户的成员。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要请求加入 Citrix Cloud 帐户的邀请，请选择请求批准。该帐户的所有现有管理员都会收到一封电子邮件，通知他们您的请求。如果现有管理员已不在您的组织中，请联系 Citrix 支持部门。

当管理员收到您的批准请求时，他们会邀请您成为管理员，如邀请个人管理员中所述。

收到邀请电子邮件后，单击“登录”链接接受邀请。浏览器打开时，Citrix Cloud 会提示您创建密码并登录 Citrix Cloud 帐户。

步骤 **2**：设置多重身份验证

如果您尚未在 MFA 中注册，Citrix Cloud 会在登录前提示您进行注册。您可以选择使用身份验证器应用程序（推荐）或您的电子邮件地址在 MFA 中注册。

> 备注：
>
> - 只有 Citrix 身份提供商下的管理员才能通过 Citrix Cloud 设置 MFA。如果您使用 Azure AD 来管理 Citrix Cloud 管理员，您可以使用 Azure 门户配置 MFA。有关详细信息，请参阅 Microsoft 网站上的“配置 Azure 多重身份验证”设置 。
> - 完成设置过程后，MFA 将用于您在 Citrix Cloud 中属于的所有客户组织。完成设置过程后，您无法禁用 MFA。
> - 您只能注册一台设备。如果您稍后注册其他设备，Citrix Cloud 将删除当前设备注册并将其替换为新设备。有关更多信息，请参阅管理您的主要 MFA 方法。

电子邮件作为身份验证方法

如果您无法使用身份验证器应用程序访问 Citrix Cloud，则使用电子邮件 MFA 是一种便捷的选择。但是，Citrix 强烈建议您采取预防措施，确保安全访问您的电子邮件地址。

MFA 要求

要使用身份验证器应用程序设置 MFA，您必须在您的设备（例如智能手机或台式计算机）上安装遵循 基于时间的一次性密码 标准的应用程序。根据您注册的设备，该应用程序可能需要访问设备的摄像头才能扫描 QR 码。如果您的设备没有摄像头，则可以输入 Citrix Cloud 提供的密钥。

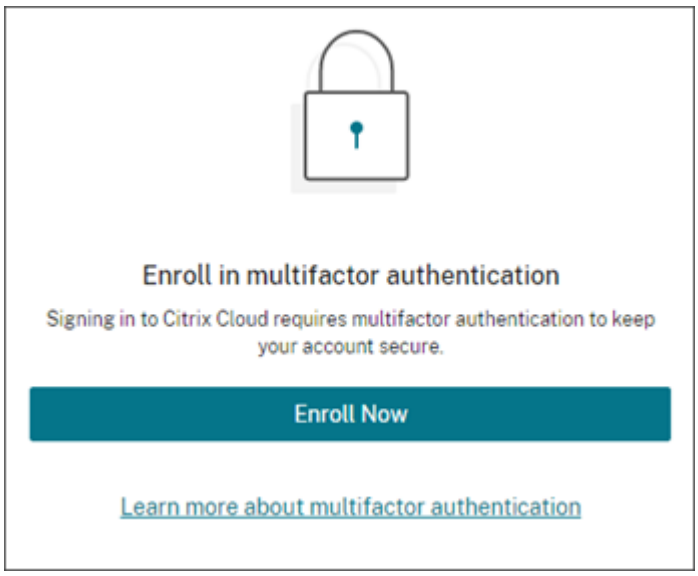
要使用电子邮件地址设置 MFA，必须使用符合以下要求的电子邮件地址：

- 该电子邮件地址与您在 Citrix 帐户中使用的电子邮件地址不同。
- 该电子邮件地址是您可以访问该地址来接收来自 Citrix 的验证电子邮件。

注册多重身份验证

1. 当系统提示您注册 MFA 时，请选择 立即注册。

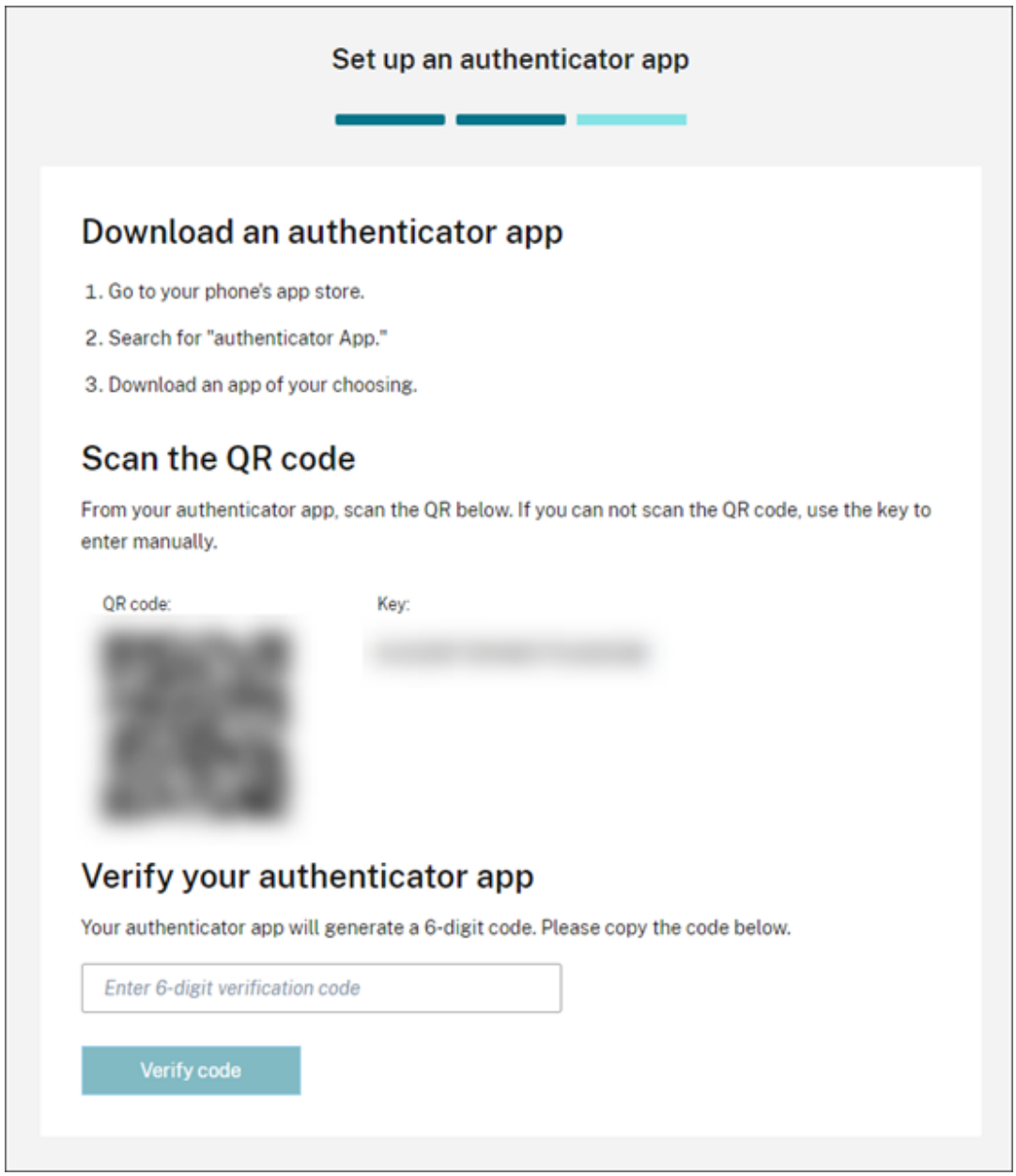
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. 出现提示时，输入您的电子邮件地址并选择发送电子邮件。Citrix Cloud 会向您发送一封包含验证码的电子邮件。
3. 输入电子邮件中的验证码和您的 Citrix 帐户密码。单击“验证”并继续。
4. 选择要使用的身份验证方法，即身份验证器应用程序或电子邮件。
5. 如果您选择了身份验证器应用程序，请执行以下操作：

    a) 在身份验证器应用程序中，扫描 QR 码或手动输入密钥。您的身份验证器应用程序显示 Citrix Cloud 的条目并生成一个 6 位数的代码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) 在“验证您的身份验证器应用程序”下，输入来自身份验证器应用程序的验证码，然后选择“验证码”。

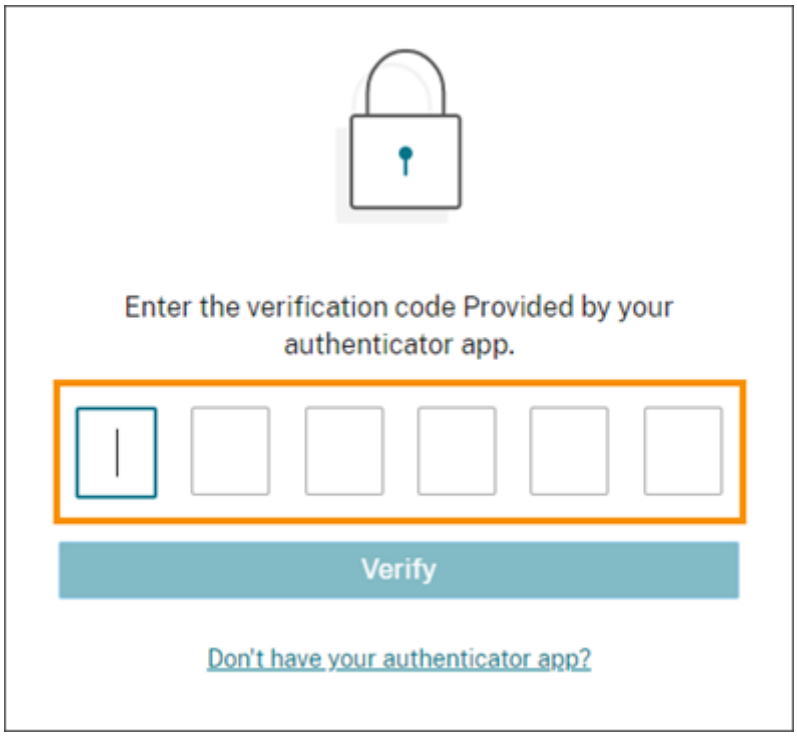
6. 单击“下一步：恢复方法”。
7. 选择“添加辅助电话”，然后输入辅助电话号码，Citrix 支持人员可以用该号码给您打电话并验证您的身份。Citrix 建议使用固定电话号码。完成后，单击“保存辅助电话号码”。
8. 选择下一步。
9. 选择“添加辅助电子邮件”，然后输入可以访问的电子邮件地址，该地址与您在 Citrix Cloud 上使用的电子邮件地址不同。Citrix 使用此地址向您发送验证码以验证您的身份。

   如果您没有其他电子邮件地址，请选择“没有辅助电子邮件**?**”改为生成备用代码列表。不建议使用备份代码，因为它们很容易丢失。如果您选择此选项，请下载代码并将其保存在需要时可以访问的位置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

10. 选择“完成”完成注册。

下次您使用 Citrix Cloud 管理员凭据登录时，Citrix Cloud 会提示您输入所选 MFA 方法中的验证码。



管理您的 **MFA** 注册

要更改您的设备、切换到其他 MFA 方法或更新恢复方法，请参阅以下文章：

- 管理您的主要 MFA 方法
- 管理您的 MFA 恢复方法

第 **3** 步：验证您的 **OrgID**

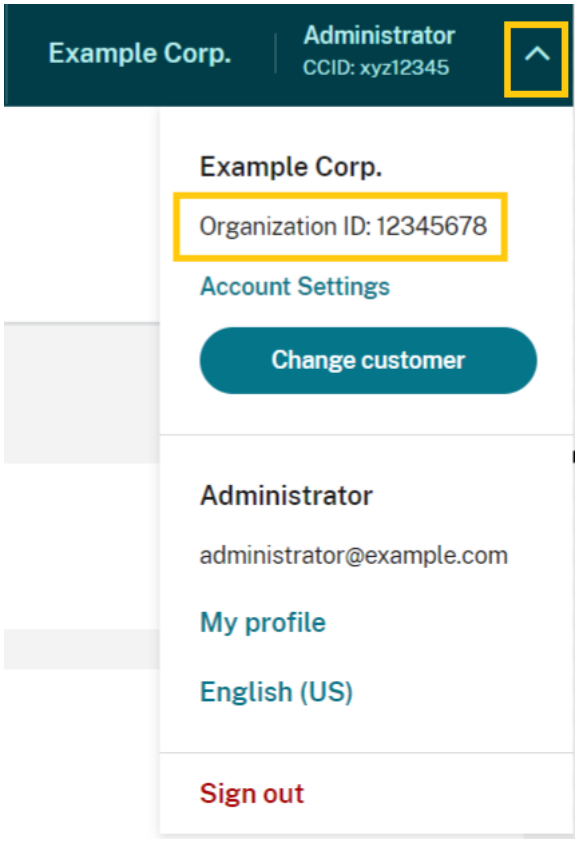
在开始使用 Citrix Cloud 之前，请花点时间验证您的 OrgID。

确保您的帐户 OrgID 与您用于下单的 OrgID 相匹配。Citrix Cloud 的好处之一是，如果您尝试某项服务并决定购买该服务，则您在试用版中进行的所有配置都将保留在购买的服务中，因为购买是在同一个帐户中进行的。因此，当您决定购买时，确保在正确的 OrgID 中开始试用可以节省精力。

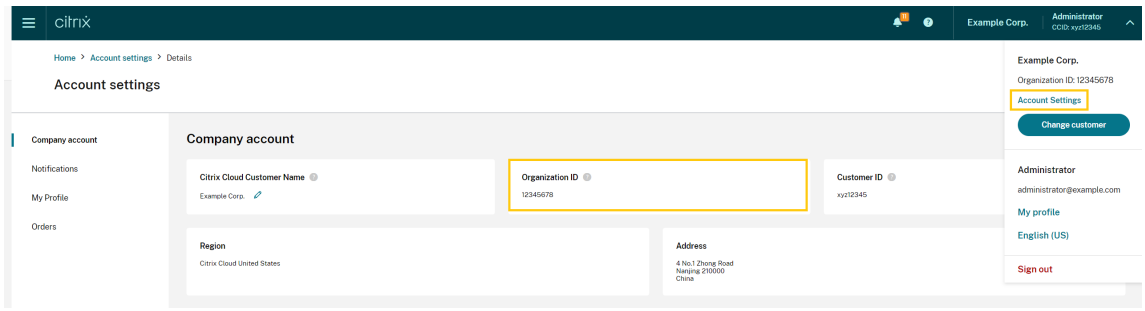
您的 OrgID 显示在管理控制台的以下位置：

- 在客户名称下方的菜单中。点击右上角的客户名称以显示菜单。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 在“帐户设置”页面上。从客户菜单中选择 帐户设置。



后续步骤

载入后，您可以继续执行以下任务：

- 添加身份提供者以对管理员或 Workspace 用户进行身份验证。
- 将管理员添加到您的 Citrix Cloud 帐户。即使您的其他管理员可以访问您在 Citrix.com 上的 Citrix 帐户，您仍然需要将其添加到您的 Citrix Cloud 帐户中。
- 申请云服务试用。试用版旨在通过您选择的本地基础架构或公有云、应用程序和 Microsoft Active Directory 进行测试。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更多信息

- Citrix 培训：Citrix Cloud 基础知识
- YouTube 上的 Citrix 频道：Citrix Cloud 大师班

为 **Citrix Cloud** 验证您的电子邮件

October 26, 2023

Citrix 有时可能会要求您验证自己的 Citrix Cloud 帐户。可能会要求您验证自己的电子邮件的部分原因如下：

- 您在一段时间内未登录 Citrix Cloud。
- 您更改了自己的电子邮件地址。
- 您向自己的 Citrix Cloud 帐户中添加了一个新管理员。
- 由于 Citrix Cloud 的安全系统更新，您需要重新验证您的 Citrix Cloud 帐户。

常见问题解答

多久会要求我验证一次

验证您的帐户属于一次性事件。Citrix Cloud 不会在您每次登录时或您的帐户中的某些设置发生变化时要求您进行验证。如果频繁要求您进行验证，请联系 Citrix 技术支持。

我的帐户发生了什么事情吗

否，要求您验证帐户并不表示您的帐户或您的任何 Citrix Cloud 服务出现了任何故障。这只是 Citrix 保持您的信息安全无恙的措施的一部分。

我还没有收到验证电子邮件。我该怎么做

请执行以下步骤：

1. 在收件箱中搜索来自“Citrix”的验证电子邮件。验证电子邮件将在 24 小时后过期。要触发新的验证电子邮件，请再次登录 Citrix Cloud。这是每次 Web 登录的一次性流程。
2. 如果不在您的收件箱中，请检查您的文件夹。如果垃圾邮件过滤器或电子邮件规则移动了电子邮件，则该电子邮件可能位于您的垃圾邮件或垃圾邮件文件夹中。检查所有防火墙。
3. 确保您检查的电子邮件帐户正确。Citrix 向您的帐户的当前存档的电子邮件地址发送验证电子邮件。通常情况下，此电子邮件地址是您最初注册 Citrix Cloud 时使用的电子邮件地址，或者邀请您加入 Citrix Cloud 帐户时使用的电子邮件地址。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 登录您的 Citrix 帐户，确认记录在案的电子邮件地址是否有效，网址为 {https://www.citrix.com/account%7D(https://www.citrix.com/account)。如果电子邮件无效，请更新您的电子邮件地址并再次登录 Citrix Cloud 以触发新的验证电子邮件。有关详细信息，请参阅 Citrix 支持知识中心中的 CTX126336 或 CTX130452。
5. 如果您仍未收到验证电子邮件，请联系 Citrix 支持 部门提交支持案例。对于教育网站（参见“合作伙伴服务交付” **>** “电子学习” **>** “**Citrix** 培训”），请向教育团队提起案例以进行进一步调查。要打开案例，请在“联系我们”页面上申请 一般支持。

如果您已成功验证电子邮件但仍无法登录 Citrix Cloud，请参阅 Citrix 网站登录问题故障排除。

联系 **Citrix** 技术支持

如果您遇到此处未涵盖的问题，请联系 Citrix 支持 部门提交支持案例。

连接到 **Citrix Cloud**

April 5, 2024

将资源连接到 Citrix Cloud 需要在环境中部署连接器和创建 资源位置。

资源位置包含向您的订阅者提供云服务所需的资源。您可以从 Citrix Cloud 控制台管理这些资源。资源位置中包含不同的资源（具体取决于您正在使用的 Citrix Cloud 服务）以及要向您的订阅者提供的服务。

要创建资源位置，请在域中至少安装两个连接器。根据您使用的云服务，需要使用 Cloud Connector 或连接器设备才能启用 Citrix Cloud 与您的资源之间的通信。有关部署连接器的更多信息，请参阅以下文章：

- Cloud Connector 技术详细信息
- 适用于云服务的连接器设备

资源类型

资源位置中包含不同的资源（具体取决于您正在使用的 Citrix Cloud 服务）以及要向您的订阅者提供的服务。不同的资源使用不同类型的连接器。大多数服务使用 Citrix Cloud Connector，但某些特定服务需要连接器设备。

使用 **Citrix Cloud Connector** 服务

- **Citrix DaaS**（以前称为 Citrix Virtual Apps and Desktops 服务）需要 Cloud Connector 来发布应用程序和桌面以及置备资源位置中的计算机目录。有关 Cloud Connector 如何与此服务通信的概述，请参阅 Citrix Tech Zone 中的 Citrix DaaS 示意图。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 适用于 **Azure** 的 **Citrix DaaS Standard**（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）要求 Cloud Connector 从多会话计算机交付 Citrix 托管的 Azure 虚拟桌面和应用程序。
- **Endpoint Management** 需要 Cloud Connector 来管理应用程序和设备策略以及向用户交付应用程序。

使用连接器设备的服务

- 图像可移植服务 简化了跨平台图像的管理。此功能对于管理本地资源位置和公有云中的资源位置之间的映像非常有用。Citrix Virtual Apps and Desktops REST API 可用于自动管理 Citrix Virtual Apps and Desktops 站点中的资源。

  映像可移植性工作流在使用 Citrix Cloud 启动映像从本地位置迁移到公有云订阅时开始。准备好映像后，Image Portability Service 可帮助您将映像转移到公有云订阅并准备运行。最后，Citrix Provisioning 或 Machine Creation Services 会在公有云订阅中预配映像。

  有关更多信息，请参阅 图像可移植性服务。

- **Citrix Secure Private Access** 使管理员能够提供紧密的体验，将单点登录、远程访问和内容检查集成到用于端到端访问控制的单一解决方案中。有关详细信息，请参阅在连接器设备中配置 Secure Private Access。

预览版中可能还有其他服务也依赖于连接器设备。

资源的位置

资源位置是指您的资源所在的位置，而无论该位置是公有云、私有云、分支机构还是数据中心。如果您自己的云或数据中心中已有资源，这些资源将保留在原位置。不需要将其移动到其他位置，即可在 Citrix Cloud 中使用。

位置的选择可能受以下因素影响：

- 与订阅者的临近程度
- 与数据的临近程度
- 规模要求
- 安全属性

资源位置部署示例

- 根据需要接近数据的用户和应用程序，在数据中心为总部建立 第一个资源位置。
- 在公有云中为您的全局用户添加第二个资源位置。或者，在分支机构构建单独的资源位置，以提供能够提供最佳服务的靠近分支机构工作人员的应用程序。
- 在单独的网络中添加另一个提供受限制的应用程序的资源位置。这将提供对其他资源和订阅者的受限可见性，而不需要调整其他资源位置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

资源位置限制

您的 Citrix Cloud 帐户中最多可以有 50 个资源位置。

命名限制

分配给资源位置的名称必须符合以下限制：

- 最大长度：64 个字符
- 不允许使用的字符：
  - #, $, %, ^, &, ?, +
  - 大括号: [ ], { }
  - 管道 (|)
  - 小于符号 (<) 和大于符号 (>)
  - 向前和向后斜杠 (/ , \ )
- 不得与 Citrix Cloud 帐户中的任何其他资源位置名称（不区分大小写）匹配

主资源位置

主资源位置是您指定为“首选”的资源位置，用于您的域与 Citrix Cloud 之间的某些通信。主资源位置中的 Cloud Connector 用于用户登录和配置操作。选择作为“主要”的资源位置应包含具有最佳性能并且连接到您的域的 Cloud Connector。这使您的用户能够快速登录 Citrix Cloud。

有关更多信息，请参阅 选择主要资源位置。

Citrix Cloud Connector

April 5, 2024

Citrix Cloud Connector 是 Citrix 的一个组件，用作 Citrix Cloud 与您的资源位置之间的通信通道，此组件不需要任何复杂的网络连接或基础结构配置即可进行云管理。这摆脱了管理交付基础结构的所有麻烦。通过此组件，您可以管理并专注于能够向您的用户提供价值的资源。

> 注意：
>
> 请勿在 Citrix Cloud Connector 计算机上安装远程 PowerShell SDK。它可以安装在同一资源位置内的任何加入域的计算机上。
>
> Citrix 建议您不要在 Cloud Connector 上运行此 SDK 的 cmdlet。SDK 的操作不涉及 Cloud Connector。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

需要 **Cloud Connector** 的服务

Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）需要使用 Cloud Connector。有关 Cloud Connector 如何与服务通信的概述，请参阅 Citrix Citrix Tech Zone 中的 Citrix DaaS 图表 。

Citrix Endpoint Management 需要 Cloud Connector 才能连接到 Endpoint Management 服务。Remote Browser Isolation 服务需要 Cloud Connector 才能使用经过身份验证的外部 Web 应用程序。

Cloud Connector 功能

- **Active Directory (AD)**：启用 AD 管理，允许在资源位置内使用 AD 林和域。它不需要再添加任何附加的 AD 信任。
- 虚拟应用程序和桌面发布：启用从资源位置中的资源发布 Citrix DaaS。
- **Endpoint Management**：启用移动设备管理 (MDM) 和移动应用程序管理 (MAM) 环境，用于管理设备和应用程序策略以及向用户交付应用程序。
- 计算机目录置备：允许将计算机直接置备到您的资源位置。

> 注意：
>
> 尽管可以运行，但在与 Citrix Cloud 的连接不可用期间，功能可能会减少。可以从 Citrix Cloud 控制台监视 Cloud Connector 的运行状况。

Cloud Connector 通信

Cloud Connector 进行身份验证并加密 Citrix Cloud 与您的资源位置之间的所有通信。安装后，Cloud Connector 将通过出站连接启动与 Citrix Cloud 的通信。所有连接都是从 Cloud Connector 到云使用标准 HTTPS 端口 (443) 和 TCP 协议建立的。不接受任何传入连接。

Cloud Connector 可用性和负载管理

为了实现持续可用性和管理负载，请在每个资源位置安装多个 Cloud Connector。为确保与 Citrix Cloud 的高可用性连接，每个资源位置至少需要两个 Cloud Connector。如果一个 Cloud Connector 在任何时段内都不可用，其他 Cloud Connector 可以维持连接。由于每个 Cloud Connector 都无状态，因此可以跨所有可用的 Cloud Connector 分发负载。不需要配置此负载平衡功能。此过程完全自动执行。

只要有一个 Cloud Connector 可用，与 Citrix Cloud 之间的通信将不会断开。最终用户与资源位置中的资源的连接尽可能不依赖与 Citrix Cloud 的连接。这使资源位置能够向用户提供对其资源的访问权限，而无论连接是否对 Citrix Cloud 可用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

获取 **Cloud Connector** 的位置

可以在 Citrix Cloud 内部下载 Cloud Connector 软件。

1. 登录 Citrix Cloud。
2. 从屏幕左上角的菜单中，选择 资源位置。
3. 如果您没有现有的资源位置，请单击资源位置页面上的 下载。出现提示时，保存 **cwcconnector.exe** 文件。
4. 如果您有资源位置但未安装 Cloud Connector，请单击“Cloud Connector”栏，然后单击下载。出现提示时，保存 **cwcconnector.exe** 文件。

我需要多少个 **Cloud Connector**

要在 Citrix Cloud 和您的资源位置之间创建高可用性连接，至少需要两 (2) 个 Cloud Connector。根据您的环境和所支持的工作负载，您可能需要更多的 Cloud Connector 来确保为用户提供最佳体验。

作为最佳实践，Citrix 建议在确定需要部署的 Cloud Connector 数量时使用 N+1 冗余模型。根据您的环境、工作负载、Active Directory 配置和服务，确定资源位置所需的 Cloud Connector 数量。除此数字外，至少再添加一个 Cloud Connector 以提供弹性。例如，如果您确定需要五个 Cloud Connector，则在此总数中再添加一个，然后在资源位置安装六个 Cloud Connector。

有关其他缩放和大小调整指南，请参阅 Cloud Connector 的缩放和大小注意事项。

Cloud Connector 的安装位置

查看支持的平台、操作系统和版本的系统 要求 。

在运行 Windows Server 2016、Windows Server 2019 或 Windows Server 2022 的专用计算机上安装 Cloud Connector。此计算机必须加入到您的域中，并且能够与您要从 Citrix Cloud 管理的资源进行通信。

> 重要：
>
> - 请勿在 Active Directory 域控制器上安装 Cloud Connector 器或任何其他 Citrix 组件。
> - 请勿在属于其他 Citrix 部署的计算机（例如，本地 Virtual Apps and Desktops 部署中的交付控制器）上安装 Cloud Connector。

有关部署的更多信息，请参阅以下文章：

- Active Directory 中 Cloud Connector 的部署方案
- Cloud Connector 安装

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud Connector 技术详细信息

July 1, 2024

Citrix Cloud Connector 是一个组件，用于在 Citrix Cloud 和您的资源位置之间建立连接。本文介绍部署要求和方案、Active Directory 和 FIPS 支持以及故障排除选项。

系统要求

托管 Cloud Connector 计算机必须满足以下要求。为确保高可用性，每个资源位置至少需要两个 Cloud Connector。作为最佳实践，Citrix 建议在部署 Cloud Connector 时使用 N+1 冗余模型，以保持与 Citrix Cloud 的高可用连接。

硬件要求

每个 Cloud Connector 至少需要：

- 2 vCPU
- 4 GB 内存
- 20 GB 磁盘空间

更大的 vCPU 内存使 Cloud Connector 能够针对更大的站点进行扩展。有关推荐配置，请参阅 Cloud Connector 的规模和大小注意事项。

操作系统

支持以下操作系统：

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

Cloud Connector 不支持与 Windows Server 核心配合使用。

.NET 要求

需要 Microsoft .NET Framework 4.7.2 或更高版本。从 Microsoft Web 站点下载最新版本。

> 注意：
>
> 不要将 Microsoft .NET Core 与 Cloud Connector 一起使用。如果您使用.NET Core 而不是.NET Frame-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> work，则安装 Cloud Connector 可能会失败。仅将.NET 框架与 Cloud Connector 一起使用。

服务器要求

如果您将 Cloud Connector 与 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）配合使用，请参阅 Cloud Connector 的扩展和大小注意事项以获取计算机配置指南。

以下要求适用于安装了 Cloud Connector 的所有计算机：

- 使用专用计算机托管 Cloud Connector。请勿在这些计算机上安装任何其他组件。
- 计算机 未 配置为 Active Directory 域控制器。不支持在域控制器上安装 Cloud Connector 器。
- 服务器时钟设置为正确的 UTC 时间。
- 如果您使用的是图形安装程序，则必须安装浏览器并设置默认系统浏览器。

Windows 更新指南

Citrix 强烈建议在托管 Citrix Cloud Connector 的所有计算机上启用 Windows 更新。Citrix Cloud Connector 每五分钟定期检查是否有待重启，这可能由包括 Windows 更新在内的各种因素触发。无论资源位置上设置的首选日程安排如何，检测到的任何重启都会立即执行。这种主动方法可确保 Citrix Cloud Connector 不会长时间处于待定更新状态，从而保持系统稳定。

Citrix Cloud 平台管理重启以保持可用性，一次只允许一个 Citrix Cloud Connector 重启。设置 Windows 更新时，请确保 Windows 设置为在非工作时间自动下载和安装更新。但是，至少在四小时内不允许自动重启，以便让 Citrix Cloud Connector 有足够的时间来管理重启过程。此外，对于更新后必须重新启动计算机的情况，您可以使用组策略或系统管理工具建立备用重启机制。有关更多信息，请参阅管理更新后的设备重启。

> 注意：
>
> - 如果客户不打算在工作时间内重启 Citrix Cloud Connector，我们建议客户在工作时间之外相应地安排 Windows 更新。
> - 每个 Citrix Cloud Connector 需要大约 10 分钟才能重启，其中包括与 Citrix Cloud 平台同步所需的时间，以确保在任何给定时间点只有一个 Citrix Cloud Connector 重启。因此，如前所述，自动重启的最短延迟时间为四小时，可以根据租户中 Citrix Cloud Connector 的数量相应地调整为更短或更长的时间。

证书验证要求

Cloud Connector 联系的 Cloud Connector 二进制文件和端点受广受尊敬的企业证书颁发机构 (CA) 颁发的 X.509 证书的保护。公钥基础设施 (PKI) 中的证书验证包括证书吊销列表 (CRL)。当客户端收到证书时，客户端会检查它是否信任颁发证书的 CA，以及证书是否在 CRL 上。如果证书位于 CRL 上，则该证书将被吊销且不可信任，即使它看起来是有效的。

CRL 服务器在端口 80 上使用 HTTP, 而在端口 443 上使用 HTTPS。Cloud Connector 组件本身不通过外部端口 80 进行通信。对外部端口 80 的需求是操作系统执行的证书验证过程的副产品。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

X.509 证书将在 Cloud Connector 安装期间进行验证。因此，必须将所有 Cloud Connector 计算机配置为信任这些证书，以确保可以成功安装 Cloud Connector 软件。

Citrix Cloud 端点受到 DigiCert 颁发的证书或 Azure 使用的根证书颁发机构之一的保护。有关 Azure 使用的根 CA 的更多信息，请参阅 https://docs.microsoft.com/en-us/azure/security/fundamentals/tls-certificate-changes。

要验证证书，每台 Cloud Connector 计算机都必须满足以下要求：

- HTTP 端口 80 对以下地址开放。此端口在 Cloud Connector 安装期间和定期 CRL 检查期间使用。有关如何测试 CRL 和 OCSP 连接的更多信息，请参阅 DigiCert 网站上的 https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm 。
  - http://cacerts.digicert.com/
  - http://dl.cacerts.digicert.com/
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://www.d-trust.net
  - http://root-c3-ca2-2009.ocsp.d-trust.net
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
  - http://ocsp.msocsp.com
- 已启用与以下地址的通信：
  - https://*.digicert.com
- 安装了以下根证书：
  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/DigiCertTrustedRootG4.crt
  - https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
  - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt
- 安装了以下中间证书：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
- https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384
  .crt
- https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA
  .crt
```

如果缺少任何证书，Cloud Connector 安装程序将从 `http://cacerts.digicert.com` 中下载证书。

有关下载和安装证书的完整说明，请参阅 CTX223828。

Citrix DaaS 使用 Cloud Connector 连接到 DaaS 资源需要安装额外的证书并授予对扩展 PKI 基础结构的访问权限。每台 Cloud Connector 计算机都必须满足以下要求：

- HTTP 端口 80 对以下地址开放：

```
- crl.*.amazontrust.com
- ocsp.*.amazontrust.com
- *.ss2.us
```

- 已启用与以下地址的通信

```
- https://*.amazontrust.com
- https://*.ss2.us
```

- 安装了以下根证书：

```
- https://www.amazontrust.com/repository/AmazonRootCA1.cer
- https://www.amazontrust.com/repository/AmazonRootCA2.cer
- https://www.amazontrust.com/repository/AmazonRootCA3.cer
- https://www.amazontrust.com/repository/AmazonRootCA4.cer
- https://www.amazontrust.com/repository/SFSRootCAG2.cer
```

- 安装了以下中间证书：

```
- https://www.amazontrust.com/repository/G2-RootCA4.orig.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.
  cer
- https://www.amazontrust.com/repository/G2-RootCA1.orig.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.cer
- https://www.amazontrust.com/repository/G2-RootCA3.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA2.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA4.cer
- https://www.amazontrust.com/repository/R2-ServerCA2A.cer
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
- https://www.amazontrust.com/repository/R4-ServerCA4A.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA1.cer
- https://www.amazontrust.com/repository/G2-RootCA2.cer
- https://www.amazontrust.com/repository/G2-RootCA3.orig.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer
- https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.
  cer
```

如果缺少任何证书，Cloud Connector 将从 https://www.amazontrust.com 中下载该证书

有关下载和安装证书的完整说明，请参阅 CTX223828。

Active Directory 要求

- 已加入一个 Active Directory 域，该域包含用于为用户创建产品/服务的资源和用户。对于多域环境，请参阅本文中的 Active Directory 中 Cloud Connector 的部署方案。
- 您计划在 Citrix Cloud 上使用的每个 Active Directory 林必须始终可以通过两个 Cloud Connector 进行访问。
- Cloud Connector 必须能够访问林根域和您打算与 Citrix Cloud 配合使用的域中的域控制器。有关详细信息，请参阅以下 Microsoft 支持文章：
  - 如何配置域和信任
  - 服务 概述和 Windows 网络端口要求中的“系统服务端口”部分
- 使用通用安全组而不是全局安全组。此配置确保可以从林中的任何域控制器获取用户组成员资格。

网络要求

- 已连接到可以联系您在资源位置使用的资源的网络。有关详细信息，请参阅 Cloud Connector 代理和防火墙配置。
- 已连接到 Internet。有关更多信息，请参阅“系统和连接要求”中的以下章节：
  - Cloud Connector 公共服务连接要求
  - Cloud Connector 允许的 FQDN

支持的 **Active Directory** 功能级别

Citrix Cloud Connector 支持 Active Directory 中的以下林和域功能级别。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

林功能级别	域功能级别	支持的域控制器
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012、Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2、Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016、Windows Server 2019、Windows Server 2022

联邦信息处理标准 **(FIPS)** 支持

Cloud Connector 目前支持在启用 FIPS 的计算机上使用的经过 FIPS 验证的加密算法。只有 Citrix Cloud 中提供的最新版本的 Cloud Connector 软件包含此支持。如果您的环境中有现有 Cloud Connector 计算机（在 2018 年 11 月之前安装），并且希望在这些计算机上启用 FIPS 模式，请执行以下操作：

1. 在资源位置的每台计算机上卸载 Cloud Connector 软件。
2. 在每台计算机上启用 FIPS 模式。
3. 在每台启用 FIPS 的计算机上安装最新版本的 Cloud Connector。

> 重要：
>
> - 请勿尝试将现有的 Cloud Connector 安装升级到最新版本。务必先卸载旧的 Cloud Connector，然后安装较新的。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - 请勿在托管较早版本的 Cloud Connector 计算机上启用 FIPS 模式。早于 5.102 版本的 Cloud Connector 不支持 FIPS 模式。在安装了较旧的 Cloud Connector 的计算机上启用 FIPS 模式会阻止 Citrix Cloud 对 Cloud Connector 执行定期维护更新。

有关下载最新版本的 Cloud Connector 说明，请参阅 从何处获取 Cloud Connector。

Cloud Connector 安装的服务

本节介绍使用 Cloud Connector 安装的服务及其系统权限。

在安装过程中，Citrix Cloud Connector 可执行文件将安装所需的服务配置并将其设置为运行所需的默认设置。如果手动更改默认配置，则 Cloud Connector 可能无法按预期运行。在这种情况下，配置将在下一次 Cloud Connector 更新时重置为默认状态，前提是处理更新过程的服务仍然可以运行。

Citrix Cloud Agent System 简化了其他 Cloud Connector 服务正常运行所需的所有提升调用，并且不会直接在网络上进行通信。当 Cloud Connector 上的服务需要执行需要本地系统权限的操作时，它会通过 Citrix Cloud Agent 系统可以执行的一组预定义的操作来执行此操作。

服务名称	说明	运行方式
Citrix Cloud 代理系统	处理本地代理所需的系统调用。包括安装、重启和注册表访问。只能由 Citrix Cloud 服务代理监视程序调用。	本地系统
Citrix Cloud 服务代理监视程序	监视和升级本地代理（常绿）。	网络服务
Citrix Cloud 服务代理日志记录器	为 Citrix Cloud Connector 服务提供支持日志记录框架。	网络服务
Citrix Cloud Services AD 提供商	使 Citrix Cloud 能够简化与安装它的 Active Directory 域帐户关联的资源的管理。	网络服务
Citrix Cloud 服务代理发现	使 Citrix Cloud 能够简化对 XenApp 和 XenDesktop 旧版本地 Citrix 产品的管理。	网络服务
Citrix Cloud 服务凭据提供商	处理加密数据的存储和检索。	网络服务
Citrix Cloud Services WebRelay 提供商	允许将从 WebRelay 云服务接收的 HTTP 请求转发到本地 Web 服务器。	网络服务
Citrix CDF 捕获服务	从所有配置的产品和组件中捕获 CDF 轨迹。	网络服务
Citrix Config Synchronizer Service	在本地复制代理配置以实现高可用性模式。	网络服务

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务名称	说明	运行方式
Citrix 连接租赁交换服务	允许在 Workspace 应用程序和 Cloud Connector 之间交换连接租用文件以实现 Workspace 的服务连续性	网络服务
Citrix High Availability Service	在中心站点停机期间提供服务的连续性。	网络服务
Citrix ITSM 适配器提供商	自动配置和管理虚拟应用程序和桌面。	网络服务
Citrix NetScaler CloudGateway	提供与本地桌面和应用程序的 Internet 连接，而无需打开入站防火墙规则或在 DMZ 中部署组件。	网络服务
Citrix 远程代理提供商	允许从本地 VDA 和 StoreFront 服务器与远程代理服务进行通信。	网络服务
Citrix 远程 HCL 服务器	代理 Delivery Controller 与虚拟机管理程序之间的通信。	网络服务
Citrix WEM 云身份验证服务	为 Citrix WEM 代理提供身份验证服务，以连接到云基础架构服务器。	网络服务
Citrix WEM 云消息传递服务	为 Citrix WEM 云服务提供服务，以便从云基础架构服务器接收消息。	网络服务

Active Directory 中 **Cloud Connector** 的部署方案

您可以同时使用 Cloud Connector 和 Connector Appliance 连接到 Active Directory 控制器。要使用的连接器类型取决于您的部署。

有关在 Active Directory 中使用 Connector Appliance 的更多信息，请参阅 Active Directory 中 Connector Appliance 的部署

在安全的内部网络中安装 Cloud Connector。

如果您在单个林中有单个域，则只需在该域中安装 Cloud Connectors 即可建立资源位置。如果您的环境中有多个域，则必须考虑在何处安装 Cloud Connector，以便您的用户可以访问您提供的资源。

如果域之间的信任不是父域/子域，则可能需要为每个单独的域或林安装 Cloud Connector。使用安全组分配资源或注册任一域中的 VDA 时，可能需要此配置来处理资源枚举。

> 注意：
>
> 以下资源位置构成了一个蓝图，您可能需要在其他物理位置重复该蓝图，具体取决于您的资源托管位置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用一组 **Cloud Connector** 的单个林中的单个域

在这种情况下，单个域包含所有资源和用户对象 (forest1.local)。一组 Cloud Connector 部署在单个资源位置内，并加入了 forest1.local 域。

- 信任关系：无-单域
- 身份识别和访问管理中列出的域：forest1.local
- 用户登录到 Citrix Workspace：支持所有用户
- 用户登录到本地 StoreFront：支持所有用户

> 注意：
>
> 如果您在单独的域中有一个虚拟机管理程序实例，那么只要虚拟机管理程序实例和 Cloud Connector 可以通过同一个网络访问，您仍然可以部署一组 Cloud Connector。Citrix Cloud 使用托管连接和可用网络与虚拟机管理程序建立通信。因此，即使虚拟机管理程序位于不同的域中，您也无需在该域中部署另一组 Cloud Connector 来确保 Citrix Cloud 可以与虚拟机管理程序通信。

使用一组 **Cloud Connector** 的单个林中的父域和子域

在这种情况下，父域 (forest1.local) 及其子域 (user.forest1.local) 驻留在单个林中。父域充当资源域，子域是用户域。一组 Cloud Connector 部署在单个资源位置内，并加入了 forest1.local 域。

- 信任关系：父/子域信任
- 身份识别和访问管理中列出的域：forest1.local、user.forest1.local
- 用户登录到 Citrix Workspace：支持所有用户
- 用户登录到本地 StoreFront：支持所有用户

> 注意：
>
> 您可能需要重新启动 Cloud Connector 以确保 Citrix Cloud 注册子域。

使用一组 **Cloud Connector** 将用户和资源置于独立林中（具有信任）

在这种情况下，一个林 (forest1.local) 包含您的资源域，一个林 (forest2.local) 包含您的用户域。存在单向信任，其中包含资源域的林信任包含用户域的林。一组 Cloud Connector 部署在单个资源位置并加入 forest1.local 域。

- 信任关系：单向林信任
- 身份识别和访问管理中列出的域：forest1.local
- 用户登录到 Citrix Workspace：仅支持 forest1.local 用户
- 用户登录到本地 StoreFront：支持所有用户

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 两个林之间的信任关系需要允许用户林中的用户能够登录到资源林中的计算机。

由于 Cloud Connector 无法遍历林级信任，因此 forest2.local 域不会显示在 Citrix Cloud 控制台的身份识别和访问管理页面上，并且任何云端功能都无法使用 forest2.local 域。这有以下限制：

- 资源只能发布给位于 Citrix Cloud 中 forest1.local 中的用户和组。但是，如果您使用的是 StoreFront 应用商店，则可以将 forest2.local 用户嵌套到 forest1.local 安全组中以缓解此问题。
- Citrix Workspace 无法对来自 forest2.local 域的用户进行身份验证。
- Citrix DaaS 中的 Monitor 控制台无法枚举来自 forest2.local 域的用户。

要解决这些限制，请按照 用户和资源中的说明在单独的林中部署 Cloud Connector（信任），并在每个林中使用一组 Cloud Connector。

单独林中的用户和资源（受信任），每个林中都有一组 **Cloud Connector**

在这种情况下，一个林 (forest1.local) 包含您的资源域，一个林 (forest2.local) 包含您的用户域。存在单向信任，其中包含资源域的林信任包含用户域的林。一组 Cloud Connector 部署在 forest1.local 域中，第二组部署在 forest2.local 域中。

- 信任关系：单向林信任
- 身份识别和访问管理中列出的域：forest1.local、forest2.local
- 用户登录到 Citrix Workspace：支持所有用户
- 用户登录到本地 StoreFront：支持所有用户

在这种情况下，可以使用 Connector Appliance 代替用户林中的 Cloud Connector，而无需资源来降低成本和管理开支，尤其是在有多个用户林的情况下。有关更多信息，请参阅使用适用于所有林的单组 Connector Appliance（具有信任）中的用户和资源

查看 **Cloud Connector** 的运行状况

Citrix Cloud 中的“Resource Locations”（资源位置）页面显示您的资源位置中的所有 Cloud Connector 的运行状态。您还可以查看每个 Cloud Connector 的高级运行状况检查数据。有关更多信息，请参阅 Cloud Connector 高级运行状况检查。

事件消息

Cloud Connector 会生成某些事件消息，您可以通过 Windows 事件查看器查看这些消息。如果要启用首选监视软件来查找这些邮件，可以将它们下载为 ZIP 存档。ZIP 下载将这些消息包含在以下 XML 文件中：

- Citrix.CloudServices.Agent.Core.dll.xml（连接器代理提供商）

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Connector AgentWatchDog Provider)

下载 Cloud Connector 事件消息。

事件日志

默认情况下，事件日志位于托管 Cloud Connector 的计算机的 C:\ProgramData\Citrix\WorkspaceCloud\Logs 目录中。

故障排除

对 Cloud Connector 出现的任何问题进行故障排除的第一个步骤是检查事件消息和事件日志。如果您未在资源位置中看到 Cloud Connector 列出，或者“未联系”，则事件日志会提供一些初始信息。

Cloud Connector 连接

如果 Cloud Connector“已断开连接”，则 Cloud Connector 检查实用程序可以帮助您验证 Cloud Connector 是否可以访问 Citrix Cloud 及其相关服务。

Cloud Connector 连接检查实用程序在托管 Cloud Connector 的计算机上运行。如果您在环境中使用代理服务器，则该实用程序可以通过隧道进行所有连接检查来帮助您验证通过代理服务器的连通性。如果需要，该实用程序还可以将任何缺失的 Citrix 受信任站点添加到 Internet Explorer 中的“受信任站点”区域。

有关下载和使用此实用程序的更多信息，请参阅 Citrix 支持知识中心中的 CTX260337 。

安装

如果 Cloud Connector 处于“错误”状态，托管 Cloud Connector 时可能出现问题。请在新计算机上安装 Cloud Connector。如果问题仍然存在，请联系 Citrix 技术支持。要对安装或使用 Cloud Connector 常见问题进行故障排除，请参阅 CTX221535。

将 **Cloud Connector** 部署为 **Secure Ticket Authority** 服务器

如果在 NetScaler Console 中使用多个 Cloud Connector 作为 Secure Ticket Authority (STA) 服务器，则在 NetScaler 控制台管理以及应用程序和桌面启动的 ICA 文件中，每台 STA 服务器的 ID 都可能显示为 **CWSSTA**。因此，STA 票证路由不正确，启动会话失败。如果 Cloud Connector 部署在具有不同客户 ID 的不同 Citrix Cloud 帐户下，则可能会出现此问题。在这种情况下，单个帐户之间会出现票证不匹配，从而导致无法创建会话。

要解决此问题，请确保作为 STA 服务器绑定的 Cloud Connector 属于具有相同客户 ID 的 Citrix Cloud 帐户。如果您需要在同一 NetScaler 控制台部署中支持多个客户帐户，请为每个帐户创建一个网关虚拟服务器。有关更多信息，请参阅以下文章：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 创建网关虚拟服务器：创建虚拟服务器
- 在 Citrix Gateway 上配置 Secure Ticket Authority
- 部署指南：将 Citrix Virtual Apps and Desktops 从本地迁移到 Citrix Cloud
- CTX232640：如何将 Citrix Gateway 配置为使用 Cloud Connector 作为 STA

Cloud Connector 代理和防火墙配置

April 6, 2024

Cloud Connector 支持通过未经身份验证的 Web 代理服务器连接到互联网。安装程序及其安装的服务都需要连接到 Citrix Cloud。
这两个点都需要提供互联网接入。

连接要求

将端口 443 用于 HTTP 流量，仅限出口。有关所需联系地址的列表，请参阅以下资源：

- 系统和连接要求
- Cloud Connector 公共服务连接要求

Citrix Cloud 所需的可联系地址指定为域名，而不是 IP 地址。由于 IP 地址可能会更改，因此允许使用域名可确保与 Citrix Cloud 的连接保持稳定。

有关所需端口的列表，请参阅 入站和出站端口配置。

> 重要：
>
> - 在某些代理上启用 SSL 拦截可能会阻止 Cloud Connector 成功连接到 Citrix Cloud。
> - 无法对 Citrix Gateway 地址执行 SSL 拦截。有关详细信息，请参阅 Citrix Gateway 服务连接要求。
> - SSL 拦截不得影响网络连接或稳定性。有关详细信息，请参阅 Citrix Cloud Connector
> - 如果您使用代理，建议以下流量绕过代理：
>
> - 连接器之间的通信（例如，在 LHC 事件期间）。
> - 连接器与 VDA 之间的通信（WCF 连接）。
> - 连接器和域控制器之间的通信（AD 请求）。

此外，需要注意的是，连接器使用了 WinHTTP 代理设置。有关配置设置，请参阅 CTX222727。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

检查 **Cloud Connector** 连接

Cloud Connector 连接检查实用程序通过一系列连接检查帮助您验证 Cloud Connector 与 Citrix Cloud 之间的连接。如果您在环境中使用代理服务器，则该实用程序可以帮助您在 Cloud Connector 上配置代理设置并测试通过代理服务器的连接。配置代理服务器后，连接测试将通过代理服务器进行隧道传输。

> 注意：
>
> Cloud Connector 连接检查实用程序仅适用于商业 Citrix Cloud 帐户。请勿将其用于 Citrix Cloud Government 或 Citrix Cloud Japan。

有关下载和使用 Cloud Connector 连接检查实用程序的更多信息，请参阅 CTX260337。

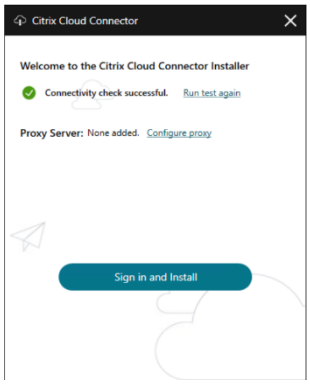
安装程序

安装程序使用为 Internet 连接配置的设置。如果可以从计算机浏览 Internet，安装程序也应能够运行。

运行时服务

运行时服务在本地服务环境中运行。它不使用为用户定义的设置（如上所述）。

您可以在安装过程中配置代理设置。



安装程序启动后，在登录 Citrix Cloud 之前，请单击 配置代理。系统会提示您添加代理信息和地址以绕过代理。指定跳过地址时，支持完全限定域名 (FQDN) 和通配符地址。

> 注意：
>
> 如果您使用代理服务器，则必须使用手动代理设置。不支持通过自动检测或 PAC/设置脚本自动设置代理。

Cloud Connector 安装

July 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可以以 交互方式 或使用 命令行安装 Cloud Connector 软件。

安装以开始安装的用户的权限进行。Cloud Connector 需要访问云才能执行以下操作：

- 对执行安装的用户进行身份验证
- 验证安装程序的权限
- 下载并配置 Cloud Connector 服务

安装之前要查看的信息

- 系统要求：为托管 Cloud Connector 器的计算机做好准备。
- 端点安全和防病毒最佳实践 Tech Zone 文章的“防病毒排除”部分：提供指导方针，帮助您确定环境中 Cloud Connector 的安全性和性能之间的适当平衡。Citrix 强烈建议您与组织的防病毒和安全团队一起查看这些准则，并在将这些准则应用到生产环境之前执行严格的基于实验室的测试。
- 系统和连接要求：确保托管 Cloud Connector 的所有计算机都能与 Citrix Cloud 进行通信。
- Cloud Connector 代理和防火墙配置：如果您要在具有 Web 代理或严格防火墙规则的环境中安装 Cloud Connector。
- Cloud Connector 的规模和大小注意事项：提供已测试的最大容量的详细信息以及配置计算机以托管 Cloud Connector 的最佳实践建议。

安装注意事项和指导

- 不要在 Active Directory 域控制器或对资源位置基础设施至关重要的任何其他计算机上安装 Cloud Connector。Cloud Connector 上的定期维护会执行导致这些额外资源中断的计算机操作。
- 请勿在托管 Cloud Connector 计算机上下载或安装其他 Citrix 产品。
- 不要单独升级 Cloud Connector 的各个组件。
- 请勿在属于其他 Citrix 产品部署（例如，本地 Citrix Virtual Apps and Desktops 部署中的交付控制器）的计算机上下载或安装 Cloud Connector。
- 不要将以前安装的 Cloud Connector 升级为较新的版本。相反，请先卸载旧 Cloud Connector，然后安装新版本。
- Cloud Connector 安装程序从 Citrix Cloud 中下载。因此，您的浏览器必须允许下载可执行文件。
- 如果您使用的是图形安装程序，则必须安装浏览器并设置默认系统浏览器。

部署后指导

安装后，保持所有 Cloud Connector 持续开机，以确保与 Citrix Cloud 的连接始终处于开启状态。

重命名计算机

安装后，不要重命名托管 Cloud Connector 的计算机。如果您稍后需要更改服务器名称，请执行以下任务：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 从资源位置移除计算机：
    a) 从 Citrix Cloud 菜单中，选择资源位置。
    b) 找到要管理的资源位置，然后选择 **Cloud Connector** 磁贴。
    c) 找到要管理的计算机，然后单击省略号菜单。选择“移除连接器”。
2. 卸载 Cloud Connector 软件。
3. 重命名 计算机。
4. 请按照本文所述安装最新版本的 Cloud Connector 软件。

将计算机移至其他域

安装后，不要将托管 Cloud Connector 的计算机移到其他域中。如果您稍后需要将计算机加入其他域，请执行以下任务：

1. 将计算机从资源位置移除。
2. 卸载 Cloud Connector 软件。
3. 将计算机从其当前域中取消加入，然后将计算机重新加入新域。
4. 请按照本文所述安装最新版本的 Cloud Connector 软件。

克隆的计算机的注意事项

托管 Cloud Connector 的每个计算机必须具有唯一的 SID 和 Connector ID，以便 Citrix Cloud 能够与您的资源位置中的计算机可靠地通信。如果要在您的资源位置中的多个计算机上托管 Cloud Connector，并且要使用克隆的计算机，请执行以下步骤：

1. 根据您的环境要求准备计算机模板。
2. 配置要用作 Cloud Connector 的计算机数量。
3. 手动或使用无提示安装模式在每个计算机上安装 Cloud Connector。

不支持在计算机模板上安装 Cloud Connector（在克隆之前）。如果克隆安装了 Cloud Connector 器的计算机，则 Cloud Connector 服务将无法运行，并且计算机无法连接到 Citrix Cloud。

服务注意事项

本文中的安装步骤描述了部署 Cloud Connector 的过程，无论它们用于何种服务。

为 Citrix DaaS 部署 Cloud Connector 时，请验证连接器所在的 AD 域是否处于活动状态，并且在 Citrix Cloud 控制台中未显示为“未使用”。如果您在 Citrix DaaS 中设置计算机目录期间指定了未使用的域，则可能会出现错误。有关详细信息，请参阅 Citrix DaaS 产品文档中的在 Citrix Cloud 中添加资源类型或激活未使用的域。

有关其他服务的其他注意事项，请参阅该服务的文档。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

默认资源位置

如果您的 Citrix Cloud 帐户中没有资源位置，并且您在域中安装了 Cloud Connector，则 Citrix Cloud 创建的资源位置将成为默认资源位置。您的帐户中只能有一个默认资源位置。如果需要，可以在 Citrix Cloud 中 创建其他资源位置 ，然后在其他域中安装 Cloud Connector 时选择所需的资源位置。

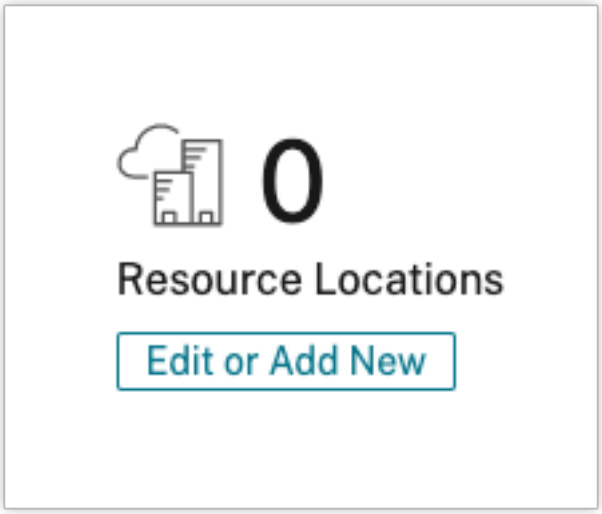
或者，您可以先在控制台中创建所需的资源位置，然后再在域中安装 Cloud Connector。Cloud Connector 安装程序会提示您在安装过程中选择所需的资源位置。

交互式安装

您可以使用图形安装程序界面下载和安装 Cloud Connector。在执行此操作之前，必须在 Citrix Cloud 管理控制台中创建一个或多个资源位置，以便在其上部署 Cloud Connector。有关资源位置的更多信息，请参阅 资源位置。

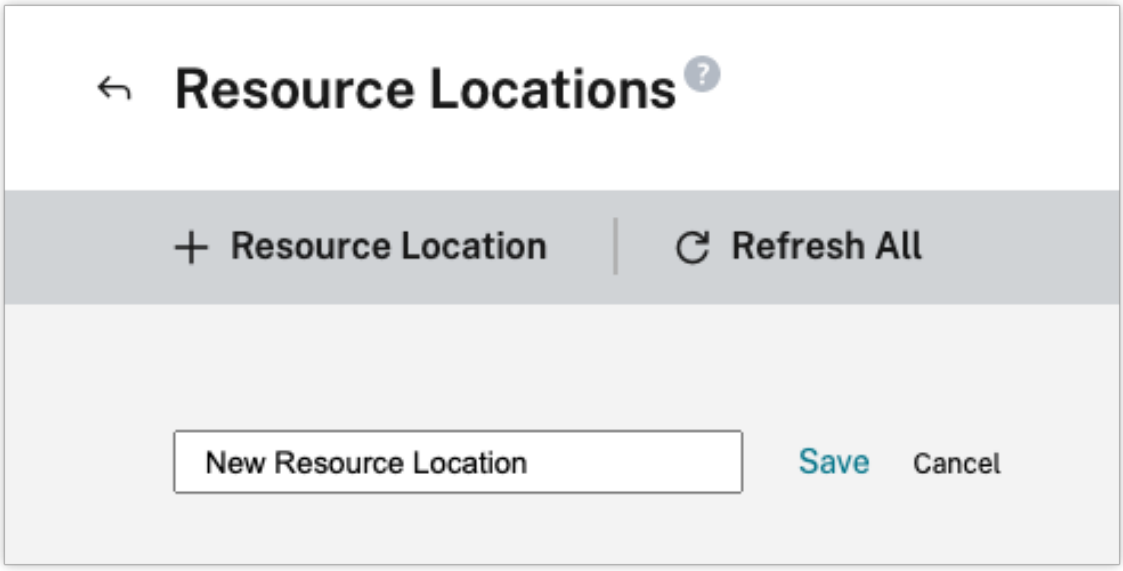
创建资源位置

1. 以 Windows 管理员身份登录到要安装 Citrix Cloud Connectors 的计算机。
2. 访问 https://citrix.cloud.com 并登录您的管理员帐户。
3. 在 Citrix Cloud 控制台中，从主菜单导航到资源位置，或者在页面顶部的资源位置下选择编辑或新增。



4. 在资源位置中，选择页面顶部的 **+** 资源位置，然后为其保存一个有意义的新名称。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

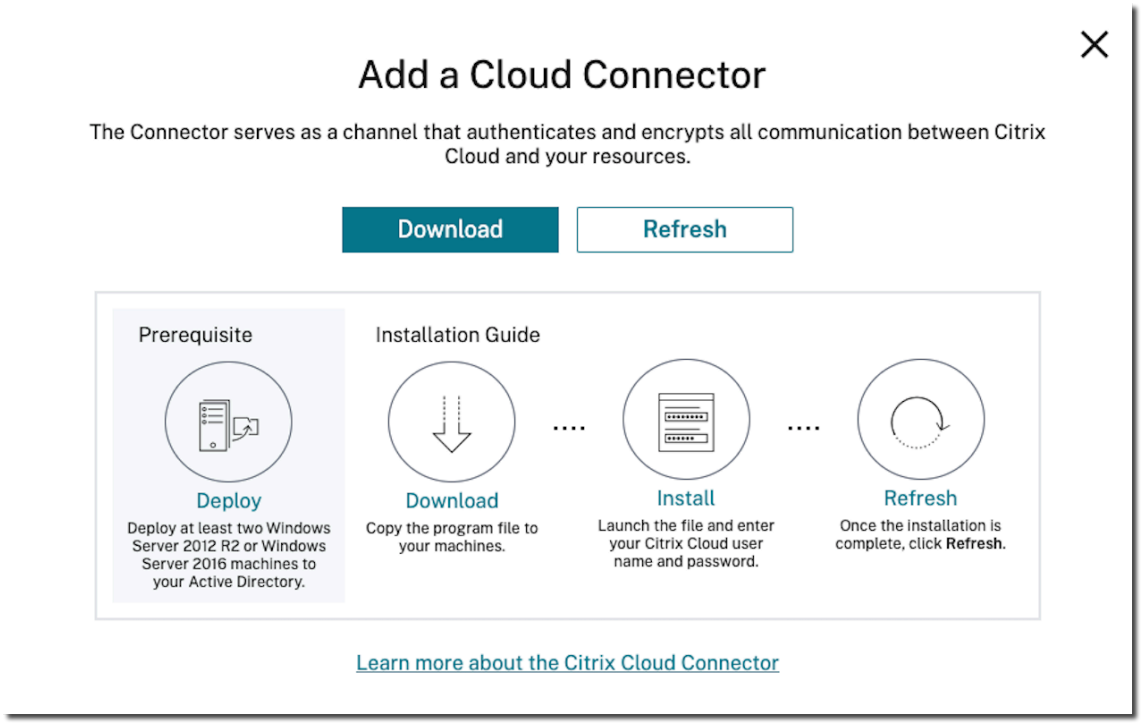


下载 **Citrix Cloud Connector** 软件

1. 找到要管理的资源位置，然后选择 **+ Cloud Connector**。

2. 在打开的窗口中选择“下载”。将 **cwcconnector.exe** 文件保存到连接器计算机上的本地文件位置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



安装 **Citrix Cloud Connector** 软件

1. 右键单击 **cwcconnector.exe** 安装程序文件，然后选择 以管理员身份运行。安装程序将执行初始连接检查，以确保您可以连接到 Citrix Cloud。
2. （可选）如果需要，请单击 配置代理 以添加代理服务器。系统会提示您添加代理信息和地址以绕过代理。指定跳过地址时，支持完全限定域名 (FQDN) 和通配符地址。
3. 单击“登录并安装”以登录 Citrix Cloud。
4. 要安装和配置 Cloud Connector，请按照向导说明进行操作。安装完成后，安装程序将执行最终连接检查，以验证 Cloud Connector 和 Citrix Cloud 之间的通信。
5. 在要用作 Citrix Cloud 连接器的其他计算机上重复这些步骤。为了获得高可用性，Citrix 建议您为每个资源位置安装至少两个 Cloud Connector。

Citrix Cloud 会在资源位置的连接器页面上显示新安装的 Cloud Connector。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

安装后，Citrix Cloud 还会在 身份和访问管理 **>** 域中注册您的域。有关详细信息，请参阅身份识别和访问管理。

激活未使用的域

如果您正在为 Citrix DaaS 创建资源位置和部署 Cloud Connector，请验证您在 Citrix DaaS A 中使用的 AD 域是否处于活动状态且未被视为未使用。如果在 Citrix DaaS 中设置计算机目录时指定未使用的域，则可能会出现错误。

有关详细信息，请参阅 Citrix DaaS 产品文档中的在 Citrix Cloud 中添加资源类型或激活未使用的域。

创建其他资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮，然后选择 资源位置。
2. 单击 **+** 资源位置，然后输入一个有意义的名称。
3. 单击保存。Citrix Cloud 将显示新资源位置的磁贴。
4. 单击“**Cloud Connector**”，然后单击“下载”以获取 Cloud Connector 软件。
5. 在每台准备好的计算机上，使用安装向导或 命令行安装安装 Cloud Connector 软件。Citrix Cloud 会提示您选择要与 Cloud Connector 关联的资源位置。

包含多个客户和现有资源位置的安装

如果您是多个客户帐户的管理员，Citrix Cloud 将提示您选择要与 Cloud Connector 关联的客户帐户。

如果您的客户帐户已有多个资源位置，Citrix Cloud 将提示您选择要与 Cloud Connector 关联的资源位置。

命令行安装

支持无提示或自动安装。但是，不建议使用相同的安装程序进行重复安装。在 Citrix Cloud 控制台中从“Resource Locations”（资源位置）页面下载新的 Cloud Connector。

要求

要在 Citrix Cloud 中使用命令行安装，您需要提供以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 要为其安装 Cloud Connector 的 Citrix Cloud 帐户的客户 ID。此 ID 显示在“身份识别和访问管理”中“**API** 访问”选项卡的顶部。
- 您要用来安装 Cloud Connector 的安全 API 客户端的客户端 ID 和密钥。要获取这些值，必须先创建一个安全客户端。客户端 ID 和密钥可确保您对 Citrix Cloud API 的访问得到适当的保护。创建安全客户端时，该客户端将使用与您拥有的相同级别的管理员权限进行操作。要安装 Cloud Connector，必须使用由 Full Access 管理员创建的安全客户端，这意味着也具有完全访问权限的安全客户端。
- 要与 Cloud Connector 关联的资源位置的资源位置 ID。要检索此值，请在“资源位置”页面上选择资源位置名称下方的 **ID** 按钮。如果不提供此值，Citrix Cloud 将使用默认资源位置的 ID。

创建安全的客户端

创建安全客户端时，Citrix Cloud 会生成唯一的客户端 ID 和密钥。通过命令行调用 API 时，必须提供这些值。

1. 从 Citrix Cloud 菜单中，选择 身份和访问管理，然后选择 **API** 访问。
2. 在“安全客户端”选项卡中，输入客户端的名称，然后选择“创建客户端”。Citrix Cloud 会生成并显示安全客户端的客户端 ID 和密钥。
3. 选择 下载 将客户端 ID 和密钥下载为 CSV 文件，并将其存储在安全的位置。或者，选择“复制”以手动获取每个值。完成后，选择 关闭 以返回控制台。

支持的参数

为确保安全客户端详细信息的安全，必须向安装程序提供 JSON 配置文件。安装完成后，必须删除此文件。配置文件支持的值有：

- **customerName** 必需。在 Citrix Cloud 控制台（在“Identity and Access Management”（身份识别和访问管理））中的“API Access”（API 访问）页面上显示的客户 ID。
- **clientId** 必需。管理员可以创建的安全客户端 ID，位于“API Access”（API 访问）页面上。
- **clientSecret** 必需。可以在创建安全客户端后下载的安全客户端机密。位于“API Access”（API 访问）页面上。
- **resourceLocationId** 推荐。现有资源位置的唯一标识符。在 Citrix Cloud 控制台的“资源位置”页面上选择 ID 按钮以检索资源位置 ID。如果未指定任何值，Citrix Cloud 将使用帐户中的第一个资源位置的 ID。
- **acceptTermsOfService** 必需。必须设置为 **true**。

示例配置文件

```
{

"customerName": "*CustomerID*",
"clientId": "*ClientID*",
"clientSecret": "*ClientSecret*",
"resourceLocationId": "*ResourceLocationId*",
"acceptTermsOfService": "true"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
 }

<!--NeedCopy-->
```

命令示例

以下命令使用 JSON 配置文件静默安装 Cloud Connector 软件：

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
    json
<!--NeedCopy-->
```

使用 /q 可指定静默安装。

使用 **Start /Wait CWCConnector.exe /ParametersFilePath: Val** ue 检查出现故障时可能出现的错误代码。安装完成后，您可以使用运行 **echo %ErrorLevel%** 的标准机制。

> 注意：
>
> 不再支持使用参数传递客户端 ID 和客户端密钥，必须使用配置文件进行自动安装。

后续步骤

1. 设置 Citrix Cloud Connector 更新时间表。有关 Citrix Cloud Connector 更新和管理更新计划的信息，请访问 连接器更新
2. 设置身份提供商来验证您的工作区订阅者。您可以在身份 和访问管理控制台中将默认 **Citrix** 身份提供程序更改为您的 **Active Directory** 或其他身份 提供商。有关更多信息，请访问 要将 Active Directory 连接到 Citrix Cloud。

安装问题故障排除

本节详细介绍一些诊断和修复安装过程中可能遇到的问题的方法。有关安装问题故障排除的更多指导，请参阅 Citrix Cloud Connector 故障排除指南。

安装日志

您可以先查阅可用的日志文件来解决安装过程中遇到的问题。

安装期间发生的事件可在 **Windows** 事件查看器中查看。您也可以查看 Cloud Connector 安装日志，这些日志位于 **%LOCALAPPDATA%\ Temp\ CitrixLogs\ CloudServicesSetup**。
安装后，日志也会添加到 **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** 中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

退出代码

根据安装过程的成功与否，可能会返回以下退出代码：

- 1603-发生了意外错误
- 2 - 必备项检查失败
- 0-安装成功完成

安装错误

如果通过双击安装程序安装 Citrix Cloud Connector 软件，则可能会收到以下错误消息：

```
Can't reach this page.
```

即使您以管理员身份登录计算机以安装 Citrix Cloud Connector，也可能发生此错误。要避免此错误，请以管理员身份运行 Citrix Cloud Connector 软件，方法是右键单击安装程序并选择以管理员身份运行。

连接故障

为确保 Cloud Connector 可以与 Citrix Cloud 通信，请确认以下 Citrix 服务处于已启动状态：

- Citrix Cloud AD 提供商
- Citrix Cloud 代理日志记录器
- Citrix Cloud 代理系统
- Citrix Cloud 代理看门狗
- Citrix Cloud 凭据提供商
- Citrix Config Synchronizer Service
- Citrix High Availability Service
- Citrix NetScaler CloudGateway
- Citrix 远程代理提供商
- Citrix 远程 HCL 服务器
- Citrix 会话管理器代理

有关这些服务的更多信息，请参阅 已安装的服务。

如果继续遇到连接故障，请使用 Citrix 支持知识中心提供的 Cloud Connector 连接检查实用程序。有关更多信息，请参阅知识中心网站上的 CTX260337 。

该工具可用于执行以下任务：

- 测试 Citrix Cloud 及其相关服务是否可访问。
- 检查常见的错误配置设置。
- 在 Citrix Cloud Connector 上配置代理设置。

有关如何解决连接检查失败的更多信息，请参阅 CTX224133：Cloud Connector 连接检查失败。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Cloud Connector 高级运行状况检查

December 14, 2023

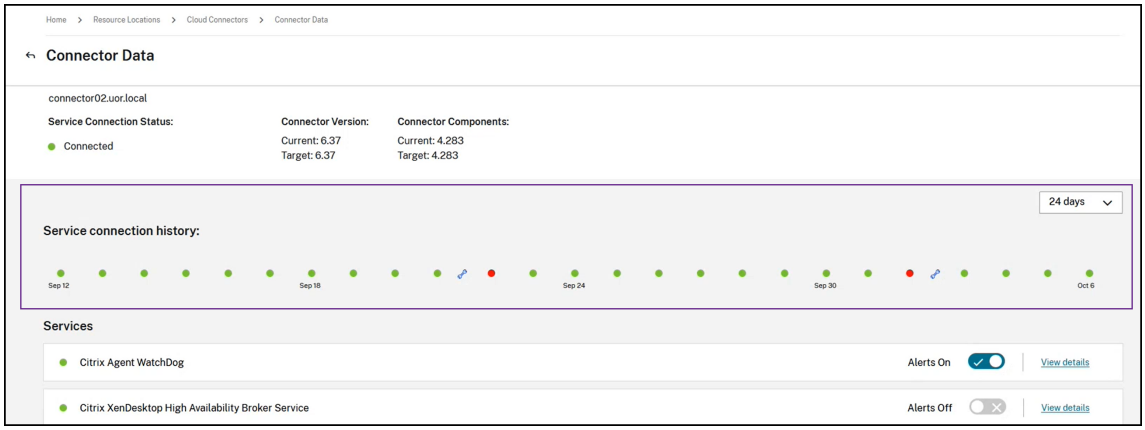
在更新之前和更新之后，Cloud Connector 都会执行运行状况检查，以确保更新不会给提供商造成不必要的停机。您可以在 Connector 上查看连接器以及每个服务或提供商的连接和运行状况。

查看连接器运行状况检查数据

1. 从 Citrix Cloud 菜单中，选择资源位置。
2. 选择要查看其运行状况检查数据的连接器。
3. 在连接器页面上，转到连接器旁边的省略号菜单，然后选择查看连接器数据。

此时将出现“连接器数据”页面，其中显示以下信息。

- 服务连接状态。连接器数据页面的此区域显示：
  - 您的连接器是否已连接到云端
  - 对于连接器及其组件，当前安装的版本和将在下次更新中安装的目标版本
- 服务连接历史记录。24 个状态指示器显示连接器在一段时间内的运行状况。默认情况下，服务连接历史记录以一小时为间隔显示过去 24 小时的状态。要查看更多历史记录，请从下拉菜单中选择 **24** 天。该视图以一天为间隔显示过去 24 天的状态。
  - 绿点表示时间间隔内的健康状态。
  - 红点表示在时间间隔内出现故障或异常状态。将鼠标悬停在圆点上可了解更多信息。
  - 扳手图标表示在时间间隔内进行了更新。将鼠标悬停在扳手图标上可了解更多信息。
  - 灰点表示在时间间隔内未收到任何运行状况信息。



- 服务。此区域列出了连接器上运行的每项服务。
  - 每项服务旁边的点表示该服务的当前状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

  - 使用“警报开启”和“警报关闭”来控制您是否收到来自该服务的警报的通知。如果警报设置为“开”，则服务失败会导致连接器的整体连接状态出现故障。
  - 选择 查看详细信息 可查看一段时间内服务运行状况的详细信息。

- 连接器指标。此区域显示连接器在过去 24 小时或 24 天内内存使用情况、CPU、网络数据和磁盘空间的使用情况。使用 服务连接历史记录 区域中的下拉菜单控制显示的时间段。

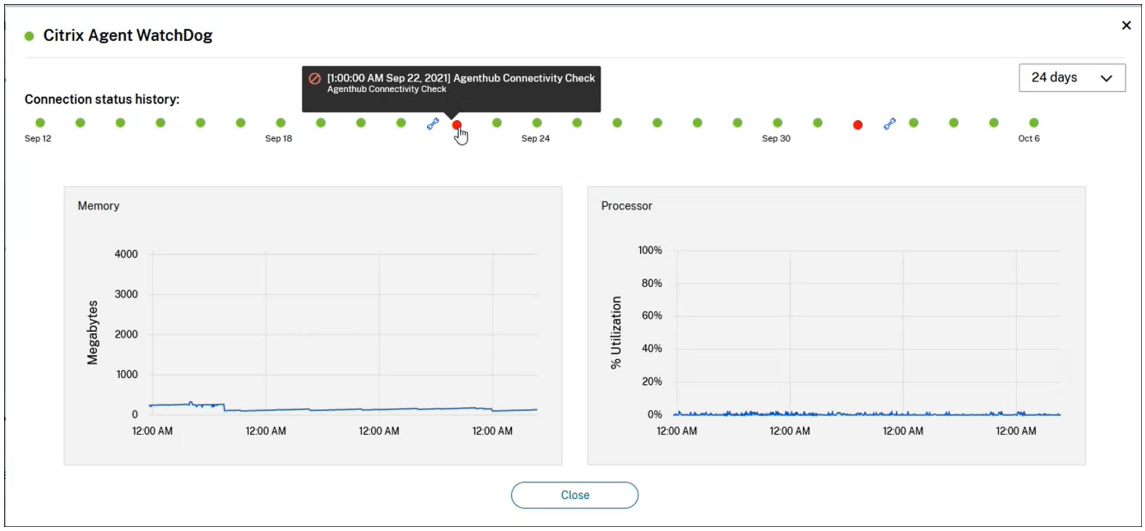
查看服务详细信息

要查看每项服务的连接状态历史记录和度量，请执行以下操作：

1. 使用 服务连接历史记录 部分中的下拉菜单选择时间段。您可以以一小时为间隔查看过去 24 小时或以一天为间隔查看过去 24 天。
2. 在“连接器数据”页面上，选择服务旁边的“查看详细信息”。

出现的页面显示：

- 24 个状态指示器，显示服务在一段时间内的运行状况。
  - 绿点表示时间间隔内的健康状态。
  - 红点表示在时间间隔内出现故障或异常状态。将鼠标悬停在圆点上可了解更多信息。
  - 扳手图标表示在时间间隔内进行了更新。将鼠标悬停在扳手图标上可了解更多信息。
  - 灰点表示在时间间隔内未收到任何运行状况信息。
- 显示指定时段内服务的内存和处理器使用情况的图表。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

连接器通知

November 2, 2022

您的连接器会在出现警告或错误情况后的 2 小时内生成通知。您可以在 Citrix Cloud 标题中的铃状图标上看到新的通知。

单击此图标查看通知，或从控制台菜单中选择“通知”。

有关更多信息，请参阅 通知。

Cloud Connector

下表列出了 Cloud Connector 可以发出的通知：

警报消息	警报类型	详细信息	解决方案
连接器 *CONNECTOR_NAME* 因未能执行定期维护而处于脱机状态且已过期。过时的连接器会影响服务可用性并妨碍维护。	错误	如果连接器处于脱机状态很长时间后又重新联机，则可能是无法更新到最新版本的旧版本。过时的连接器无法进行维护，可能会影响环境中其他连接器的维护过程。	如何更新过时的 Cloud Connector
连接器 *CONNECTOR_NAME* 与 UTC 时间不同步。处于这种状态的连接器可能会影响服务可用性、功能或性能。	错误		我如何同步 Cloud Connector 时间
连接器 *CONNECTOR_NAME* 的维护失败。此连接器的维护失败将阻止对环境中其他连接器的维护。维护失败的连接器可能会影响服务的可用性、功能或性能。	错误	此连接器上的连接器升级或其他维护操作失败。	我如何解决 Cloud Connector 维护失败的问题

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

警报消息	警报类型	详细信息	解决方案
连接器 *CONNECTOR_NAME* 已脱机数小时或更长时间。脱机连接器将影响服务可用性并妨碍维护。	警告	如果连接器在一定小时内无法接触，则将其视为脱机。	我如何将脱机 Cloud Connector 恢复到在线状态
连接器 *CONNECTOR_NAME* 未通过最近的连接检查。连接检查失败可能会影响服务可用性或功能。	警告	连接检查失败，错误代码为 *HEALTH_CHECK_CODE*。此连接器无法联系通知消息中列出的某些 Web 或 IP 地址。	Cloud Connector 连接检查失败
连接器 *CONNECTOR_NAME* 的 CPU 使用率很高。在资源有限的情况下运行的连接器可能会影响服务可用性、功能或性能。	警告	在一小时的采样周期内，此连接器的 CPU 利用率已超过 80%。	我如何解决 Cloud Connector 资源可用性警报
连接器 *CONNECTOR_NAME* 的可用磁盘空间不足。在有限的磁盘空间下运行的连接器将影响服务性能和维护。	警告	此连接器的可用磁盘空间少于 2 GB。	我如何解决 Cloud Connector 资源可用性警报
连接器 *CONNECTOR_NAME* 已检测到关键进程或服务已停止运行。此状态可能会影响服务可用性、功能或性能。	警告		

Citrix Cloud Connector 日志收集

October 5, 2023

CDF 日志用于 Citrix 产品中的故障排除目的。Citrix 支持使用 CDF 跟踪来识别应用程序和桌面代理、用户身份验证、Virtual Delivery Agent (VDA) 注册方面的问题。本文讨论了如何捕获 Cloud Connector 数据，这些数据可用于对环境中可能遇到的问题进行故障排除和解决。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要注意事项：
>
> - 在资源位置的所有 Cloud Connector 计算机上启用日志记录。
> - 为确保捕获全部数据，Citrix 建议使用驻留在 VDA 上的 CDFControl 捕获工具。有关更多信息，请参阅 Citrix 支持知识中心中的 CTX111961 。有关 Citrix Workspace 应用程序日志收集的更多信息，请 访问 CTX141751。
> - 要向 Citrix 提交 CDF 跟踪，您必须有一个未结的 Citrix 支持案例。Citrix 支持技术人员无法查看未附加到现有支持案例的 CDF 跟踪。

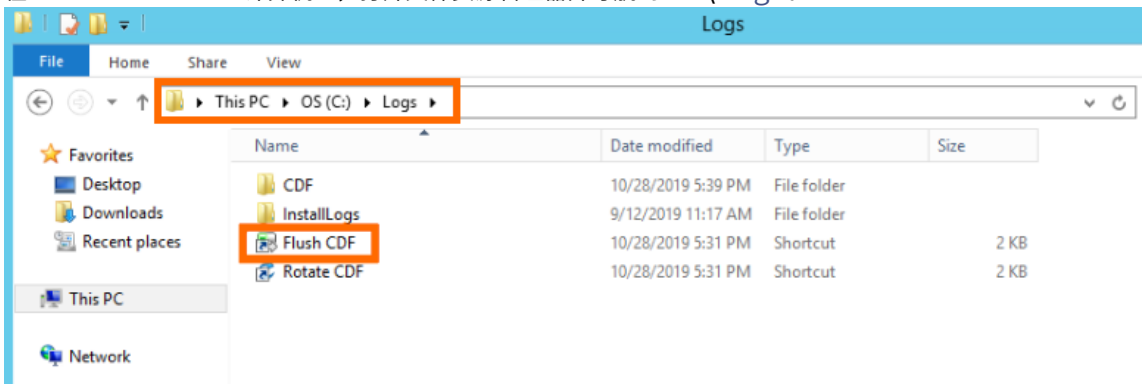
第 **1** 步：重现问题

在此步骤中，重现您在环境中遇到的问题。如果问题与应用程序启动或代理有关，请重现启动失败。如果问题与 VDA 注册有关，请在 VDA 计算机上手动重新启动 Citrix 桌面服务，重新创建 VDA 注册尝试。

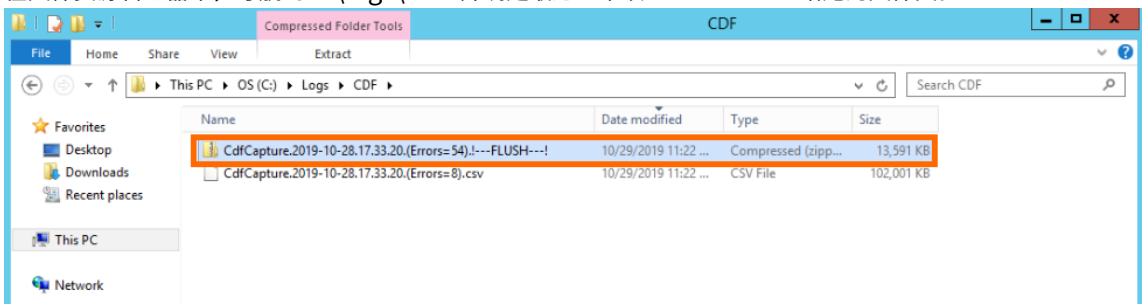
步骤 **2**：收集 **CDF** 轨迹

在此步骤中，您将从资源位置的每个 Cloud Connector 中收集 CDF 刷新跟踪记录。

1. 通过使用域管理员或本地管理员帐户启动 RDP 连接来访问 Cloud Connector 计算机。
2. 在 Cloud Connector 计算机上，打开文件资源管理器并导航到 `C:\logs`。



3. 运行 刷新 **CDF**。Cloud Connector 计算机的任务栏上会短暂出现一个图标，然后消失。
4. 在文件资源管理器中，导航到 C:\logs\CDF 并确定最近一个以 **!-FLUSH-!**. 结尾的文件夹。



5. 在资源位置的每台 Cloud Connector 计算机上执行步骤 1-5，并将所有 Cloud Connector 刷新跟踪合并到单个 ZIP 存档中。如果您没有创建来自所有 Cloud Connector 计算机的刷新跟踪的 ZIP 存档，则需要一次向

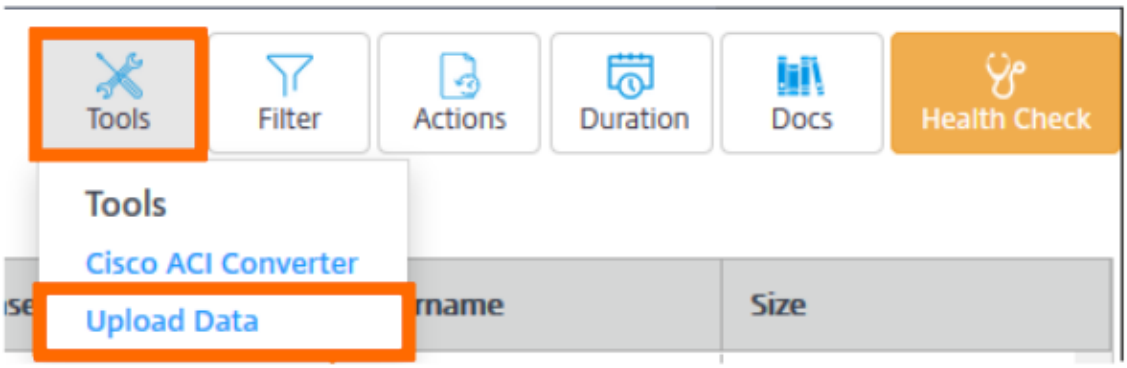
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 提交一个刷新跟踪记录。

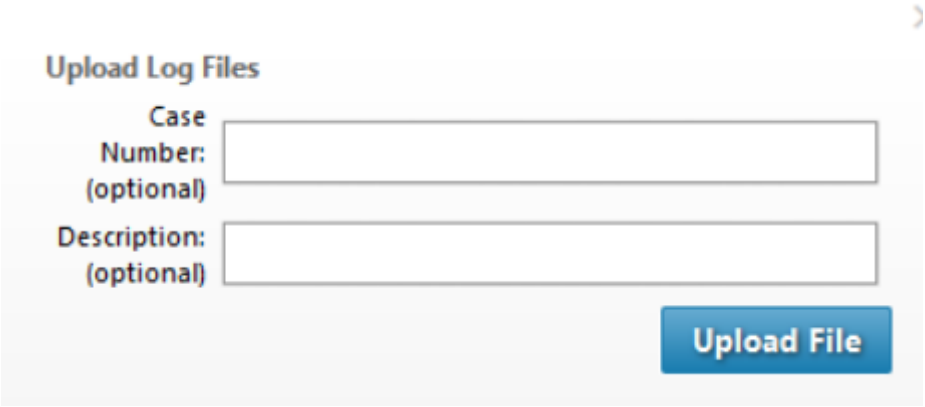
步骤 3：向 Citrix 提交数据

在此步骤中，您将跟踪信息附加到您的 Citrix 支持案例并提交以供审核。

1. 访问 https://cis.citrix.com/ 并使用你的 Citrix.com 凭据登录。
2. 选择“诊断”。
3. 选择 工具，然后选择 上载数据。



4. 在 案例编号中，输入现有支持案例的 Citrix 支持案例编号。如果数据上传没有附加案例编号，Citrix 支持技术人员将无法正确查看 CDF 跟踪。



5. 在 说明（可选）中，您可以输入简要说明或将此字段留空。
6. 选择“上载文件”，然后选择您之前创建的 ZIP 存档。如果您没有创建来自所有 Cloud Connector 计算机的刷新跟踪的 ZIP 存档，请重复步骤 3-6 以附加要提交的每个刷新跟踪记录。

提交刷新跟踪后，Citrix Insight Services 会处理这些跟踪并将其附加到您指定的支持案例中。此过程可能需要长达 24 小时，具体取决于文件的大小。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择主要资源位置

October 5, 2023

如果您的域中有多个资源位置，可以选择一个作为 Citrix Cloud 的“主要”位置或“最优先选择”的位置。主要资源位置在 Citrix Cloud 与您的域之间提供最佳性能和连接，使用户能够快速登录。

选择主资源位置时，该资源位置中的 Cloud Connector 将在可能的情况下用于用户登录和置备操作。如果主要资源位置中的 Cloud Connector 不可用，则将使用域中的另一个 Cloud Connector 执行这些操作。使用用户主体名称 (UPN) 的登录可能不包含域名，也可能不使用主资源位置。

> 注意：
>
> 为确保 Cloud Connector 在任何资源位置始终可用，请在每个资源位置至少安装两个 Cloud Connector。

决定要将哪个资源位置用作主要资源位置时，请注意以下事项：

- 该资源位置是否与您的域具有最佳连接？
- 该资源位置是否最靠近您在其中使用 Citrix Cloud 管理控制台的地理区域？例如，如果您的 Citrix Cloud 控制台位于 https://us.cloud.com，则您选择的资源位置将是离美国区域最近的资源位置。

选择主要资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮，然后选择 身份和访问管理。
2. 单击“域”，然后展开包含要使用的资源位置的域。
3. 单击“设置主要资源位置”，然后选择要指定为主要资源位置的资源位置。
4. 单击保存。Citrix Cloud 将在您选择的资源位置旁边显示“Primary”（主要）。

> 注意：
>
> 在扩展其他域之前，请务必将您的选择保存在一个域中。展开一个域，然后再展开另一个域时，以前展开的域将折叠并放弃未保存的所有选择。

选择另一个主要资源位置

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮，然后选择 身份和访问管理。
2. 单击“域”，然后展开包含要更改的主要资源位置的域。
3. 单击“更改主要资源位置”，然后选择要使用的资源位置。
4. 单击保存。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

重置主要资源位置

重置主要资源位置将允许您从某个资源位置中删除“Primary”（主要）标志，而不需要选择另一个资源位置。删除“Primary”（主要）标志时，域中的所有 Cloud Connector 都可以处理用户登录操作。因此，某些用户可能会遇到登录较为缓慢的情况。

1. 在 Citrix Cloud 管理控制台中，单击菜单按钮，然后选择 身份和访问管理。
2. 选择“域”，然后展开包含要更改的主要资源位置的域。
3. 选择“更改主要资源位置”，然后选择“重置”。此时将显示一条通知，警告您登录性能可能会受到影响。
4. 选择“我了解对订阅者的潜在影响”，然后单击“确认重置”。

适用于云服务的 **Connector Appliance**

April 5, 2024

Connector Appliance 是虚拟机管理程序中托管的 Citrix 组件。它充当 Citrix Cloud 与您的资源位置之间的通信渠道，无需任何复杂的网络或基础架构配置即可实现云管理。Connector Appliance 使您能够管理和专注于为用户提供价值的资源。

Connector Appliance 提供以下功能：

- 将 **Active Directory** 连接到 **Citrix Cloud** 可启用 AD 管理，允许在资源位置内使用 AD 林和域。它不需要再添加任何附加的 AD 信任。有关详细信息，请参阅带 Connector Appliance 的 Active Directory。
- **Image Portability Service** 简化了跨平台映像的管理。此功能对于管理本地资源位置和公有云中的资源位置之间的映像非常有用。Citrix Virtual Apps and Desktops REST API 可用于自动管理 Citrix Virtual Apps and Desktops 站点中的资源。

  映像可移植性工作流在使用 Citrix Cloud 启动映像从本地位置迁移到公有云订阅时开始。准备好映像后，Image Portability Service 可帮助您将映像传输到公有云订阅并准备运行。最后，Citrix Provisioning 或 Machine Creation Services 会在公有云订阅中预配映像。

  有关更多信息，请参阅 Image Portability Service。
- **Citrix Secure Private Access** 使管理员能够提供紧密的体验，将单点登录、远程访问和内容检查集成到用于端到端访问控制的单一解决方案中。有关详细信息，请参阅在 Connector Appliance 中配置 Secure Private Access。

预览版中可能还有其他服务也依赖于 Connector Appliance。

Connector Appliance 平台是 Citrix Cloud 平台和 Citrix 身份平台的一部分，可以处理数据，包括以下信息：

- IP 地址或 FQDN
- 设备、用户和资源位置标识符

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 时间戳
- 赛事数据
- 来自 Active Directory 的用户和组详细信息（例如，用于验证和搜索用户和组）

Citrix Cloud Services 数据保护概述中的 _Citrix Cloud 平台收集的数据 _ 表中提供了 Connector Appliance 处理的特定信息的详细信息。

Connector Appliance 可用性和负载管理

为了实现持续可用性和管理负载，请在每个资源位置安装多台 Connector Appliance。Citrix 建议在每个资源位置至少安装两个 Connector Appliance。如果一个 Connector Appliance 在任何时候都不可用，其他 Connector Appliance 可以保持连接。由于每个 Connector Appliance 都是无状态的，因此可以在所有可用的 Connector Appliance 之间分配负载。不需要配置此负载平衡功能。它是自动化的。如果至少有一个 Connector Appliance 可用，则与 Citrix Cloud 的通信不会中断。

如果只为资源位置配置了一个连接器，Citrix Cloud 会在 资源位置 和 连接器 页面上显示警告。

Connector Appliance 更新

Connector Appliance 会自动更新。您无需采取任何操作来更新连接器。

您可以将资源位置配置为在更新可用时立即应用更新，也可以在特定的维护时段内应用更新。

有关配置更新的更多信息，请参阅连接器更新

作为更新的一部分，Connector Appliance 暂时不可用。一次只能将更新应用于资源位置中的一个 Connector Appliance。因此，请在每个资源位置至少注册两个 Connector Appliance，以确保至少有一个 Connector Appliance 始终可用。

Connector Appliance 通信

Connector Appliance 对 Citrix Cloud 与您的资源位置之间的所有通信进行身份验证和加密。安装后，Connector Appliance 将通过出站连接启动与 Citrix Cloud 的通信。从 Connector Appliance 到云的所有连接均使用标准 HTTPS 端口 (443) 和 TCP 协议建立。不允许传入连接。

下表列出了 Connector Appliance 需要访问的端口：

服务	端口	支持的域协议	配置详细信息
DNS	53	TCP/UDP	此端口必须对本地设置开放
NTP	123	UDP	此端口必须对本地设置开放

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务	端口	支持的域协议	配置详细信息
HTTPS	443	TCP	Connector Appliance 需要出站访问此端口

要配置 Connector Appliance，IT 管理员必须能够访问 Connector Appliance 端口 443 (HTTPS) 上的管理界面。

> 注意：
>
> 必须在 IP 地址的开头加上 `https://`。

Connector Appliance 可以与资源位置中的本地系统和外部系统进行通信。如果在 Connector Appliance 注册期间定义了一个或多个 Web 代理，则只有从 Connector Appliance 到外部系统的流量才会通过此 Web 代理路由。如果您的本地系统位于专用地址空间中，则从 Connector Appliance 到此系统的流量不会通过 Web 代理路由。

Connector Appliance 将专用地址空间定义为以下 IPv4 地址范围：

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 —192.168.255.255

Internet 连接要求

从您的数据中心连接到 Internet 需要打开端口 443 以便建立出站连接。但是，要在包含 Internet 代理服务器或防火墙限制的环境中进行操作，可能需要进一步进行配置。

要正确操作和使用 Citrix Cloud 服务，必须能够通过未经修改的 HTTPS 连接联系以下地址：

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.nssvc.net`
  - 无法启用所有子域名的客户可以使用以下地址：
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

网络要求

确保您的环境具有以下配置：

- 网络允许 Connector Appliance 使用 DHCP 获取 DNS 和 NTP 服务器、IP 地址、主机名和域名，或者您可以在 Connector Appliance 控制台中手动设置网络设置。
- 网络未配置为使用 Connector Appliance 内部使用的链路本地 IP 范围 169.254.0.1/24、169.254.64.0/18 或 169.254.192.0/18。
- 虚拟机管理程序时钟设置为协调世界时 (UTC) 并与时间服务器同步，或者 DHCP 向 Connector Appliance 提供 NTP 服务器信息。
- 如果将代理与 Connector Appliance 配合使用，则该代理必须未经身份验证或使用基本身份验证。

系统要求

以下虚拟机管理程序支持 Connector Appliance：

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi 第 7 版更新 2
- Windows Server 2016、Windows Server 2019 或 Windows Server 2022 上的 Hyper-V。
- Nutanix AHV
- Microsoft Azure
- AWS
- Google 云端平台

您的虚拟机管理程序必须提供以下最低功能：

- 20 GB 根磁盘
- 2 个 vCPU
- 4 GB 内存
- 一个 IPv4 网络

您可以在同一个虚拟机管理程序主机上托管多个 Connector Appliance。同一主机上的 Connector Appliance 的数量仅受虚拟机管理程序和硬件限制的限制。

> 注意：
>
> 不支持克隆、暂停和拍摄 Connector Appliance VM 的快照。

获取 **Connector Appliance**

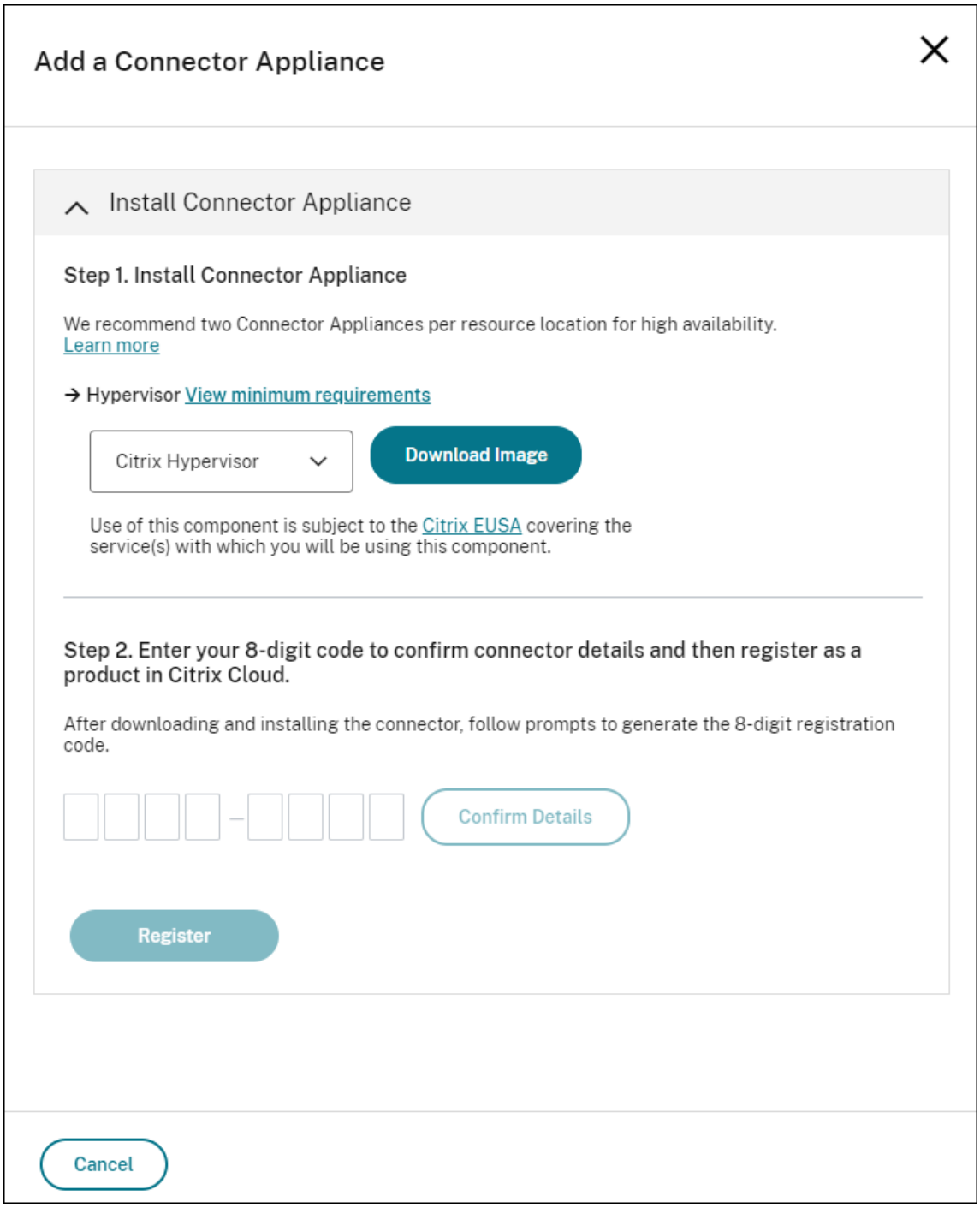
从 Citrix Cloud 中下载 Connector Appliance 软件。

1. 登录 Citrix Cloud。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 从屏幕左上角的菜单中，选择 资源位置。
3. 如果您还没有资源位置，请单击加号图标 (+) 或选择 添加资源位置。
4. 在要注册 Connector Appliance 的资源位置中，单击连接器 设备 加号图标 (+)。

   “添加 **Connector Appliance**” 任务打开。



5. 从步骤 **1** 的虚拟机管理程序列表中，选择用于托管 Connector Appliance 的虚拟机管理程序或云提供商的类

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

型。

- 对于本地虚拟机管理程序和云环境，您可以在 Citrix Cloud 中下载 Connector Appliance：

  a) 单击下载映像。

  b) 查看 Citrix 最终用户服务协议，如果您同意，请选择 同意并继续。

  c) 出现提示时，保存提供的 Connector Appliance 文件。

  Connector Appliance 文件的文件扩展名取决于您选择的虚拟机管理程序。

- 对于某些云环境，您可以从市场上购买 Connector Appliance：
  - AWS
  - Microsoft Azure
  - Google Cloud

6. 保持安装 **Connector Appliance** 任务处于打开状态。安装 Connector Appliance 后，在 步骤 **2** 中输入注册码。

您也可以从连接器页面转到安装 **Connector Appliance** 任务。选择加号图标 (+) 以添加连接器，然后选择添加连接器装置。

在虚拟机管理程序上安装 **Connector Appliance**

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google 云端平台
- AWS

Citrix Hypervisor

本节介绍如何使用 XenCenter 将 Connector Appliance 导入到 Citrix Hypervisor 服务器。

1. 在有权访问下载的 Connector Appliance XVA 文件的系统上使用 XenCenter 连接到您的 Citrix Hypervisor 服务器或池。
2. 选择“文件”>“导入”。
3. 指定或浏览至 Connector Appliance XVA 文件所在的路径。单击下一步。
4. 选择要在其中托管 Connector Appliance 的 Citrix Hypervisor 服务器。或者，您可以选择要在其中托管 Connector Appliance 的池，然后 Citrix Hypervisor 会选择合适的可用服务器。单击下一步。
5. 指定要用于 Connector Appliance 的存储库。单击导入。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

6. 单击添加以添加虚拟网络接口。从网络列表中，选择 Connector Appliance 要使用的网络。单击下一步。
7. 查看用于部署 Connector Appliance 的选项。如有任何不正确，请使用上一步更改这些选项。
8. 确保选 中导入完成后立即启动新 **VM** 。单击完成。

部署 Connector Appliance 并成功启动后，其控制台将显示包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。如果 DHCP 在您的环境中不可用，则必须先在 Connector Appliance 控制台上设置网络配置，然后才能访问 Connector Appliance 管理控制台。有关更多信息，请参阅 使用 Connector Appliance 控制台设置网络配置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

VMware ESXi

本节介绍如何使用 VMware vSphere 客户端在 VMware ESXi 主机上部署 Connector Appliance 。

1. 在有权访问下载的 Connector Appliance OVA 文件的系统上使用 vSphere Client 连接到您的 ESXi 主机。
2. 选择“文件”>“部署 **OVF** 模板…”。
3. 指定或浏览至 Connector Appliance OVA 文件所在的路径。单击下一步。
4. 查看模板详情。单击下一步。
5. 您可以为 Connector Appliance 实例指定一个唯一的名称。默认情况下，名称设置为 “**Connector Appliance**”。确保您选择的名称将 Connector Appliance 的此实例与此 ESXi 主机上托管的其他实例区分开来。单击下一步。
6. 指定 Connector Appliance 的目标存储器。单击下一步。
7. 选择存储虚拟磁盘的格式。单击下一步。
8. 查看用于部署 Connector Appliance 的选项。如果有任何不正确，请使用“返回”更改这些选项。
9. 选择 部署后开机。单击完成。

部署 Connector Appliance 并成功启动后，其控制台将显示包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。如果 DHCP 在您的环境中不可用，则必须先在 Connector Appliance 控制台上设置网络配置，然后才能访问 Connector Appliance UI。有关更多信息，请参阅使用 Connector Appliance 控制台设置网络配置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

Hyper-V

本节介绍如何在 Hyper-V 主机上部署 Connector Appliance 。您可以使用 Hyper-V 管理器或使用随附的 PowerShell 脚本来部署虚拟机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **Hyper-V** 管理器部署 **Connector Appliance**

1. 连接到您的 Hyper-V 主机。
2. 将 Connector Appliance ZIP 文件复制或下载到 Hyper-V 主机。
3. 提取 ZIP 文件的内容。ZIP 文件包含 PowerShell 脚本和 connector-appliance.vhdx 文件。
4. 将 VHDX 文件复制到要保存 VM 磁盘的位置。例如，`C:\ConnectorApplianceVMs`。
5. 打开 Hyper-V 管理器。
6. 右键单击您的服务器名称，然后选择 新建 **>** 虚拟机。
7. 在“新建虚拟机向导”的“指定名称和位置”面板上，输入一个唯一的名称来标识您的 Connector Appliance。单击下一步。
8. 在“指定层代”面板上，选择“第 **1** 代”。单击下一步。
9. 在“分配内存”面板上，配置以下设置，然后单击“下一步”：
   a) 分配 4 GB 的内存。
   b) 禁用动态内存。
10. 在“配置网络”面板上，从列表中选择一台交换机（例如，默认交换机）。单击下一步。
11. 在“连接虚拟硬盘”面板上，选择“使用现有虚拟硬盘”。
12. 浏览到 connector-appliance.vhdx 文件所在的位置并将其选中。单击下一步。
13. 在 摘要 面板上，查看您选择的值，然后单击 完成 以创建 VM。
14. 在 虚拟机 面板上，右键单击 Connector Appliance VM，然后选择 设置。
15. 在“设置”窗口中，选择“硬件”**>**“处理器”，然后执行以下操作：
    a) 在虚拟处理器数量中，将值更改为 **2**。
    b) 单击应用。
    c) 单击“确定”。
16. 在 虚拟机 面板上，右键单击 Connector Appliance VM，然后选择 启动。
17. 右键单击 Connector Appliance VM，然后选择 连接 以打开控制台。

部署 Connector Appliance 并成功启动后，使用 Hyper-V 管理器连接到控制台。控制台将显示一个登录页面，其中包含 Connector Appliance IP 地址。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。如果 DHCP 在您的环境中不可用，则必须先在 Connector Appliance 控制台上设置网络配置，然后才能访问 Connector Appliance UI。有关更多信息，请参阅使用 Connector Appliance 控制台设置网络配置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **PowerShell** 脚本部署 **Connector Appliance**　connector-appliance.zip 文件包含用于创建和启动新虚拟机的 PowerShell 脚本。

> 注意：
>
> 要运行此未签名的 PowerShell 脚本，您可能需要更改 Hyper-V 系统上的执行策略。有关详细信息，请参阅 https://go.microsoft.com/fwlink/?LinkID=135170。或者，您可以使用提供的脚本作为创建或修改自己的本地脚本的基础。

1. 连接到您的 Hyper-V 主机。
2. 将 Connector Appliance ZIP 文件复制或下载到 Hyper-V 主机。
3. 提取 ZIP 文件的内容：PowerShell 脚本和 VHDX 文件。
4. 在 PowerShell 控制台中，将当前目录更改为 ZIP 文件内容所在的位置，然后运行以下命令：

```
.\connector-appliance-install.ps1
<!--NeedCopy-->
```

5. 出现提示时，键入虚拟机的名称或选择 **Enter** 以接受 **Connector Appliance** 的默认值。
6. 出现提示时，键入根磁盘的目标位置或按 Enter 键使用 VHD 的系统默认目录。
7. 出现提示时，键入根磁盘的文件名或选择 **Enter** 接受 connector-appliance.vhdx 的默认值。
8. 出现提示时，选择要使用的交换机。选择“**Enter**”。
9. 查看 VM 导入信息的摘要。如果信息正确，请选择 **Enter** 继续。该脚本将创建并启动 Connector Appliance VM。

部署 Connector Appliance 并成功启动后，其控制台将显示包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 并完成注册过程。

下一步：向 Citrix Cloud 注册 Connector Appliance。

Nutanix AHV

本节介绍如何使用 Nutanix Prism Web 控制台将 Connector Appliance 从 `connector-appliance.vhdx` 文件部署到 Nutanix AHV 主机上。

1. 在 Nutanix Prism Web 控制台的主菜单上，选择 存储 视图。
2. 单击 **+** 存储容器创建存储容器来存放 Connector Appliance 映像文件。或者，您可以使用现有的存储容器。
3. 将 `connector-appliance.vhdx` 文件上载到您的存储容器。
    a) 在 Web 控制台的主菜单上，选择 设置。
    b) 选择“图片配置”选项卡，然后单击 **+** 上载图片
    c) 在 创建图像中，为您的图像指定一个 名称。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

d) 在 映像类型 列表中，选择 磁盘。
e) 从 存储容器 列表中，选择您创建的存储容器。
f) 选择 上载文件。
g) 单击“选择文件”，然后导航到本地系统上的 `connector-appliance.vhdx` 文件。
h) 单击保存。

4. 等待镜像创建完成，其状态在映像配置页面中显示为活动。
5. 选择“网络配置”选项卡。
6. 单击 **+** 创建网络以创建供 Connector Appliance 使用的网络。
7. 在“创建网络”页中，指定以下信息：

   - 网络名称。
   - 网络 VLAN ID。

8. 在 Web 控制台的主菜单上，选择 **VM** 视图。
9. 单击 **+** 创建虚拟机以创建 Connector Appliance 实例。
10. 在 创建 **VM** 中，指定以下信息：

    - 虚拟机名称
    - vCPU 的数量
    - 以 GiB 为单位的内存量

11. 选择使用传统 **BIOS**。
12. 单击 **+** 添加新磁盘 将磁盘添加到 VM。
13. 在“添加磁盘”中，填写以下信息：

    a) 对于“类型”，选择“磁盘”。
    b) 在“操作”中，选择“从镜像服务克隆”。
    c) 对于 总线类型，选择 **SCSI**
    d) 对于映像，请选择您在上载 Connector Appliance 文件时创建的映像。

14. 单击“添加”完成添加磁盘。
15. 在“创建虚拟机”中，单击 **+** 添加新 **NIC**。
16. 在 创建 **NIC** 中，选择要将 VM 添加到的网络。
17. 对于“网络连接状态”，选择“已连接”。
18. 单击“添加”完成 NIC 的添加。
19. 单击 保存 以创建 VM。

    默认情况下，新 VM 处于关闭状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

20. 在 **VM** 视图中，选择虚拟机，然后单击“开机”。
21. 等待 VM 启动。此过程可能需要几分钟。

部署 Connector Appliance 并成功启动后，可以在以下位置之一找到 Connector Appliance IP 地址：

- 在 Nutanix Prism 网络控制台的 虚拟机 视图中。
- 在 Connector Appliance 控制台中。

使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：向 Citrix Cloud 注册 Connector Appliance。

Microsoft Azure

本节介绍如何在 Microsoft Azure 中部署 Connector Appliance 。您可以使用随附的 PowerShell 脚本从 Azure 市场或下载的磁盘映像部署 Connector Appliance 。

从 **Azure** 市场部署 **Connector Appliance**　要从 Azure 市场部署 Connector Appliance ，请完成以下步骤：

1. 前往 Azure 市场中的 Connector Appliance 。（Azure 市场）

   或者，您可以在市场搜索中搜索“适用于云服务的 Connector Appliance ”。

2. 单击“立即获取”，然后单击“创建”。
3. 在为云服务创建 **Citrix Connector Appliance** 页面上，填写以下信息：

   - 选择要使用的 订阅。
   - 选择要使用的 资源组。
   - 选择要在其中定位 Connector Appliance 的 区域。
   - 指定 **VM** 名称。
   - 选择要将 Connector Appliance 添加到的 虚拟网络。此网络用于访问 Citrix Cloud、本地资源和 Connector Appliance 管理页面。以后无法更改此网络。
   - 为“子网”指定一个值。

   单击下一步**:** 标记 **>**。

4. 在标记选项卡上，根据需要添加所需的标记。

   单击 **Next: Review + create >**（下一步: 检查 + 创建 >）。

5. 查看部署详细信息后，单击创建。

部署 Connector Appliance 并成功启动后，其控制台将显示包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：向 Citrix Cloud 注册 Connector Appliance。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **PowerShell** 脚本部署 **Connector Appliance** 虚拟机　`connector-appliance-azure.zip` 文件包含用于创建和启动新虚拟机的 PowerShell 脚本。您可以使用提供的脚本作为创建或修改自己的本地脚本的基础。

在运行该脚本之前，请确保您具备以下先决条件：

- 将 Az PowerShell 模块安装到您的本地 PowerShell 环境中。
- 在 VHD 文件所在的目录中运行 PowerShell 脚本。

完成以下步骤：

1. 将 Connector Appliance ZIP 文件复制或下载到您的 Windows 系统。
2. 提取 ZIP 文件的内容：PowerShell 脚本和 VHD 文件。
3. 以管理员身份打开 PowerShell 控制台。
4. 将当前目录更改为 ZIP 文件内容所在的位置，然后运行以下命令：

```
.\connector-appliance-upload-Azure.ps1
```

5. 此时会出现一个对话框，提示您登录 Microsoft Azure。输入您的凭据。
6. 当 PowerShell 脚本提示时，请选择要使用的订阅。按 Enter 键。
7. 按照脚本中的提示进行操作，该脚本将指导您上载映像和创建虚拟机。
8. 创建第一个 VM 后，脚本会询问您是否要从上载的映像创建另一个 VM。
    - 键入 `y` 以创建另一个 VM。
    - 键 `n` 入退出脚本。

部署 Connector Appliance 并成功启动后，其控制台将显示包含 Connector Appliance IP 地址的登录页面。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。

下一步：向 Citrix Cloud 注册 Connector Appliance。

AWS

本节介绍如何在 AWS 中部署 Connector Appliance 。Connector Appliance 在 AWS 市场中作为 AMI 提供，我们建议您从 AMI 安装 Connector Appliance 。或者，您可以使用 AWS 用户界面或使用随附的 PowerShell 脚本部署下载的磁盘映像。

联网前提条件　要在 AWS 上部署 Connector Appliance ，请确保您可以从创建 Connector Appliance 的子网访问 Citrix Cloud。

我们建议为设备使用私有 IP 地址，这需要进行特定配置才能提供对 Citrix Cloud 的访问权限。要实现此配置，请在 **AWS** 管理控制台中完成以下步骤：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 创建 NAT 网关。

   a) 在顶部导航栏中，选择 服务 **> VPC > NAT** 网关。

   b) 点击右上角的 创建 **NAT** 网关。输入以下信息：

      - 输入 名称。
      - 从列表中选择 子网。
      - 将 连接类型 设置为 公共。
      - 从列表中选择 弹性 **IP** 分配 **ID** 。如果没有可用的弹性 IP，请单击 分配弹性 **IP** ，然后按照说明创建一个。

   c) 点击 创建 **NAT** 网关。

2. 创建包含 NAT 网关的路由表条目。

   a) 在顶部导航栏中，选择 服务 **> VPC >** 路由表。

   b) 点击右上角的 创建路由表。输入以下信息：

      - 输入 名称。
      - 从列表中选择包含您在创建 NAT 网关时选择的子网的 VPC。

   c) 点击 创建路由表。

   d) 在您创建的 路由 表的路径选项卡中，单击 编辑路由 **>** 添加路由。

   e) 输入新路径条 目的目的地 和 目标。

      - 将目标设置为 0.0.0.0/0。
      - 对于目标，从列表中选择您创建的 **NAT** 网关。

   f) 点击 保存更改。

3. 将用于 Connector Appliance 的子网附加到此路由表。

   a) 在顶部导航栏中，选择服务 **> VPC >** 路由表。
   b) 选择包含 NAT 网关的路由表。
   c) 在显示页面中，转到“子网关联”选项卡。
   d) 点击 编辑子网关联。
   e) 选择要附加到路由表的一个或多个子网。
   f) 单击保存关联。

从 **AWS Marketplace** 部署 **Connector Appliance**　开始之前，请确保满足以下先决条件：

- 您有权操作 EC2 资源。
- 您已完成 网络先决条件中的配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- （可选）您可以创建一个安全组，以限制允许哪些 IP 地址访问您的 Connector Appliance 。

完成以下步骤：

1. 登录 **AWS** 管理控制台。
2. 在 AWS 市场中找到 Connector Appliance AMI。可以使用以下任一方法执行此操作：
   - 点击 Citrix Cloud 中提供的市场链接。（AWS Marketplace）
   - 在 AWS 管理控制台中搜索 AMI：
     a) 转到 服务 **>** 计算 **> EC2 > AMI**
     b) 确保您位于美国东部（俄亥俄）区域。
     c) 在 公共图片中，搜索“Citrix Connector Appliance”或 AMI ID“ami-026eaf9b3b232577f”。
3. 检查 AMI ID（ami-026eaf9b3b232577f）和所有者 ID（414337923189），验证您的 AMI 是否正确。
4. 将 AMI 复制到您的订阅中：
   a) 转到 操作 **>** 复制 **AMI**。
   b) 在 复制 **AMI** 对话框中，您可以选择所需的 目标区域。
   c) 点击 复制 **AMI**
5. 在复制的 AMI 摘要页面中，单击 从 **AMI** 启动实例。
6. 在 启动实例 对话框中，完成以下步骤：
   a) 选择要创建的实例数。为了实现弹性，我们建议您在每个资源位置安装两个或更多的 Connector Appliance 。
   b) 指定实例的名称。
   c) 对于 实例类型，选择 **t2.medium**。实例类型必须至少有 4 GB 和 2 个 CPU。
   d) 对于 密钥对（登录），选择在没有 密钥对的情况下继续。不允许 SSH 登录 Connector Appliance ，因此不需要密钥对。
   e) 对于 网络设置，在 防火墙（安全组）部分中，配置以下设置：
      i. 选择是 创建安全组 还是 选择现有安全组。
      ii. 取消选择“允许来自 **Internet** 的 **SSH** 流量”
      iii. 选择允许来自 **Internet** 的 **HTTPS** 流量
      iv. 选择 允许来自 **Internet** 的 **HTTP** 流量

   点击 启动实例。
7. 创建实例后，在“成功”部分中，单击“实例 ID”链接以查看您的 Connector Appliance 实例。

   或者，您可以单击此页面上的 查看所有实例 按钮或转到 AWS 管理控制台中的 服务 **> EC2 >** 实例 以查看您的实例列表。
8. 当您的实例状态更改为正在运行时，进入实例详细信息并使用专用 **IPv4** 地址连接到 Connector Appliance 管理页面并完成注册过程。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可能需要使用堡垒主机从浏览器进入内部 IP 地址处的 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅 Connector Appliance 管理页面上的配置网络设置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

使用 **AWS UI** 部署 **Connector Appliance**　开始之前，请确保满足以下先决条件：

- 您有权操作 S3 和 EC2 资源。
- 您已创建具有虚拟机导入访问权限的服务角色和策略。有关详细信息，请参阅 https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role。

  > 注意：
  >
  > 要创建服务角色，您必须创建 S3 存储桶。创建策略时，请将您创建的 S3 存储桶设置为具有虚拟机导入访问权限。

- 您可以访问 AWS CloudShell。它仅在某些地区可用。有关支持 AWS CloudShell 的区域列表，请参阅 https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html。
- 您已完成 网络先决条件中的配置。

完成以下步骤：

1. 在本地系统上，提取的内容 `connector-appliance-aws.zip`。
2. 登录 **AWS** 管理控制台。
3. 通过完成以下步骤来创建存储分区。（或者，您可以跳过这些步骤并使用现有的存储分区。）
   a) 在顶部导航栏中，选择 服务 > **S3** > 创建存储桶。
   b) 为您的存储桶输入一个唯一的名称。有关 Amazon S3 中存储桶的命名约定，请参阅 https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html。
   c) 为您的存储桶选择区域。请确保选择与您的 AWS 区域相同的区域，因为如果这些区域不同，则无法使用存储桶中的文件。
   d) 将剩余设置保持为默认设置，然后点击 创建存储桶。
4. 点击您创建的存储段的名称。单击“上载”>“添加文件”，然后选择 `connector-appliance.vhd` 文件。将剩余设置保持为默认值，然后点击 上载。
5. 点击您上载的文件。单击“复制 **S3 URI**”。
6. 单击顶部导航栏中的 **AWS CloudShell** 图标 并运行以下命令：
   a) 创建任务以将 VHD 文件转换为快照：

```
aws ec2 import-snapshot --disk-container Format=VHD,Url="<S3_URI>"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将占位符值替换为您从上一步复制的 S3 URI。例如，`aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`。

当以下命令返回包含的 JSON 字符串时，此命令即完成 `"Status": "completed"`。记下 JSON 输出中的 `ImportTaskId` 值。

b) 请运行以下命令：

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <ImportTaskId>
```

将占位符值替换为从上一步 `ImportTaskId` 复制的值。例如，`aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`。

7. 在 **AWS** 管理控制台的顶部导航栏中，选择 服务 > **EC2**。
8. 在屏幕左侧的菜单中，单击“快照”。
9. 右键单击您创建的快照，然后单击“创建映像”。
10. 在打开的窗格中，完成以下步骤：

    a) 输入您的 AMI 的名称。
    b) 选择 硬件辅助虚拟化。

    单击 **Create**（创建）。

11. 在屏幕左侧的菜单中，单击 **AMI**。
12. 右键单击您创建的 AMI，然后单击 **Launch**。
13. 在打开的窗格中，完成以下步骤：

    a) 选择实例类型。
    b)（可选）在 配置实例 选项卡上自定义网络。
    c)（可选）在“添加存储”选项卡上附加另一个卷。
    d) 在 配置安全组选项卡上设置安全组 规则。

    查看实例启动后，单击 查看并启动。

部署 Connector Appliance 并成功启动后，转到 服务 > **EC2** > 实例，然后选择您创建的实例。使用专用 **IPv4** 地址连接到 Connector Appliance 管理页面并完成注册过程。您可能需要使用堡垒主机从浏览器的内部 IP 地址转到 Connector Appliance 管理页面，以继续安装过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅 Connector Appliance 管理页面上的配置网络设置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **PowerShell** 脚本部署 **Connector Appliance** `connector-appliance-aws.zip` 文件包含用于创建和启动新虚拟机的 PowerShell 脚本。在运行该脚本之前，请确保您具备以下先决条件：

- 您的系统上安装了 AWS.Tools、AWSPowerShell.NetCore 或 AWSPowerShell。有关详细信息，请参阅 https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html。
- 您已创建具有虚拟机导入访问权限的服务角色和策略。必须同时命名 `vmimport` 服务角色和策略，此 PowerShell 脚本才能正常工作。有关详细信息，请参阅 https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role。

  > 注意：
  >
  > 要创建服务角色，您必须创建 S3 存储桶。创建策略时，请将您创建的 S3 存储桶设置为具有虚拟机导入访问权限。

- 您已创建了 Amazon EC2 安全组。
- 您拥有 S3 权限和 API 访问权限。
- 您已完成 网络先决条件中的配置。

完成以下步骤：

1. 在本地系统上，将的内容解压 `connector-appliance-aws.zip` 到文件夹。
2. 在 PowerShell 中，运行以下命令：

   a) 要能够在本地环境中运行 AWS cmdlet，请运行以下命令将新配置文件添加到 AWS SDK 存储中：

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   将占位符值替换为您的访问密钥和私有密钥。提供唯一的配置文件名称。在我们提供的示例中，它是 `MyProfile`。

   b) 将配置文件设置为默认值：

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) 将当前目录更改为解压文件所在的文件夹，然后运行以下命令：

   ```
   .\connector-appliance-upload-aws.ps1
   ```

3. 按照脚本中的提示进行操作，该脚本将指导您选择 Connector Appliance 部署的区域、将映像上载到所选存储桶以及输入 VM 的名称。

   - 您必须使用之前创建的具有 VM 导入访问权限的存储桶。
   - 当系统要求您选择要使用的 VPC 时，请选择配置 NAT 网关和路由表的 VPC。
   - 当系统要求您选择要使用的子网时，请选择附加到包含 NAT 网关的路由表的子网。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关更多信息，请参阅 网络先决条件。

部署 Connector Appliance 并成功启动后，脚本将显示 Connector Appliance 的专用 IP 地址。您可能需要使用堡垒主机从浏览器进入内部 IP 地址处的 Connector Appliance 管理页面并完成注册过程。

默认情况下，Connector Appliance 使用 DHCP 来设置其网络配置。您可以使用 Connector Appliance Web 界面编辑此网络配置。有关详细信息，请参阅 Connector Appliance 管理页面上的配置网络设置。

下一步：向 Citrix Cloud 注册 Connector Appliance。

Google 云端平台

本节介绍如何在 Google 云端平台上部署 Connector Appliance 。您可以从 Google Cloud 市场安装 Connector Appliance 。或者，您可以使用 Google Cloud Platform 控制台或使用随附的 PowerShell 脚本来部署下载的磁盘映像。

文件 `connector-appliance-gcp.zip` 包含：

- `connector-appliance.tar.gz`，它是 Connector Appliance 磁盘映像
- `connector-appliance-upload-gcp.ps1`，这是一个 PowerShell 脚本，可用于自动部署 Connector Appliance

从 **Google Cloud** 市场部署 **Connector Appliance**

1. 登录到您的 Google 帐户。
2. 点击 Citrix Cloud 中提供的市场链接。（Google Cloud 市场）

   或者，您可以在市场搜索中搜索“适用于云服务的 Connector Appliance ”。
3. 单击 **Launch**（启动）。
4. 在适用于云服务的新 **Citrix Connector Appliance** 部署页面上，填写以下信息：

   - 为部署任务指定部署名称。
   - 选择要在其中找到 Connector Appliance 的区域。
   - 选择要使用的计算机系列、序列和计算机类型。
   - 选择要使用的 启动磁盘类型 和 启动磁盘大小（以 **GB** 为单位）。
   - 在网络部分中，指定 Connector Appliance 要使用的网络接口。如果您希望能够从公共网络连接到管理页面，请指定 外部 **IP**。

   单击部署。您将被定向到“部署管理器”页面。

   > 注意：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 部署 Connector Appliance 并成功启动后，您会收到一封电子邮件，确认 Connector Appliance 已部署在 Google 云端平台上。

5. 在 部署管理器 页面上，单击实例名称。或者，可以搜索您在计算引擎中创建的 Connector Appliance 实例。
6. 如果您之前在为 Connector Appliance 设置网络接口时指定了外部 **IP**，请在“详细信息”选项卡的“网络接口”部分中复制外部 **IP** 地址。使用此 IP 地址连接到 Connector Appliance 管理页面并完成注册过程。或者，您可以使用主内部 **IP** 地址从与 Connector Appliance 位于同一子网的另一台计算机上访问 Connector Appliance 管理页面。

下一步：向 Citrix Cloud 注册 Connector Appliance。

使用 **Google** 云端平台控制台部署 **Connector Appliance**

1. 在本地系统上，提取的内容 `connector-appliance-gcp.zip`。
2. 在您的 Google Cloud Platform 项目中，创建存储分区。（或者，您可以使用现有的存储分区。）
   a) 从主菜单中选择 云存储。
   b) 在主窗格中，选择 创建存储桶。
   c) 为您的存储桶指定一个名称。
   d) 配置所需的数据存储和访问设置。您可以将这些设置保留为默认设置。
   e) 单击 **Create**（创建）。
3. 在存储分区中，选择 上载文件 并选择文件 `connector-appliance.tar.gz`。等待文件上载。
4. 选择上载的文件以查看其详细信息。将 **gsutil URI** 的值复制到剪贴板。
5. 单击标题栏中的 激活云外壳 图标以打开云外壳。
6. 在 Cloud Shell 中，运行以下命令来创建映像：

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. 从主菜单中，选择 计算引擎 > 虚拟机实例。
8. 选择 创建实例。在打开的窗格中，指定以下信息：
   a) 在“名称”字段中，指定 Connector Appliance 实例的名称。
   b) 选择要在其中定位 Connector Appliance 的区域。
   c) 选择计算机配置。
   d) 在“启动盘”部分中，单击“更改”。
   e) 在打开的部分中，转到 自定义图像 选项卡。
   f) 从 图像 列表中选择您创建的图像。
   g) 单击 **Select**（选择）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

h) 在“防火墙”部分中，启用 HTTPS 通信以允许访问 Connector Appliance 管理页面。
i) 指定所需的任何其他配置。例如，您可能不想使用默认网络配置。

单击 **Create**（创建）。

9. 在 虚拟机实例 部分中，选择新创建的 VM 以查看其详细信息。

部署 Connector Appliance 并成功启动后，“虚拟机实例”部分将显示 Connector Appliance IP 地址。

如果 Connector Appliance 有外部 IP 地址，则可以使用此 IP 地址从浏览器转到 Connector Appliance 管理页面并完成注册过程。

如果 Connector Appliance 只有一个内部 IP 地址，请使用堡垒主机从浏览器转到 Connector Appliance 管理页面并完成注册过程。有关详细信息，请参阅 https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host。

下一步：向 Citrix Cloud 注册 Connector Appliance。

使用 **PowerShell** 脚本部署 **Connector Appliance**　要使用提供的 PowerShell 脚本部署 Connector Appliance，必须在系统上安装 Google Cloud SDK。

1. 在本地系统上，将的内容解压 `connector-appliance-gcp.zip` 到文件夹。
2. 在 PowerShell 中，将目录更改为解压文件所在的文件夹。
3. 运行命令 `.\connector-appliance-upload-GCP.ps1`。
4. 在打开的浏览器窗口中，使用有权访问要将 Connector Appliance 部署到的项目的帐号通过 Google Cloud SDK 进行身份验证。
5. 在适用于 PowerShell 的 Google Cloud 工具中，当 PowerShell 脚本提示时，选择要使用的项目。按 Enter 键。
6. 按照脚本中的提示操作，该脚本将指导您完成上载磁盘、创建映像和创建虚拟机的过程。
7. 创建第一个 VM 后，脚本会询问您是否要从上载的映像创建另一个 VM。
   - 键入 `y` 以创建另一个 VM。
   - 键 `n` 入退出脚本。

部署 Connector Appliance 并成功启动后，脚本将显示 Connector Appliance 的内部 IP 地址。或者，您可以转到 Google 云端平台控制台查找 Connector Appliance 的内部 IP 地址。计算引擎 > 虚拟机实例 部分显示 Connector Appliance IP 地址。

使用堡垒主机从浏览器进入内部 IP 地址处的 Connector Appliance 管理页面，然后完成注册过程。有关详细信息，请参阅 https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host。

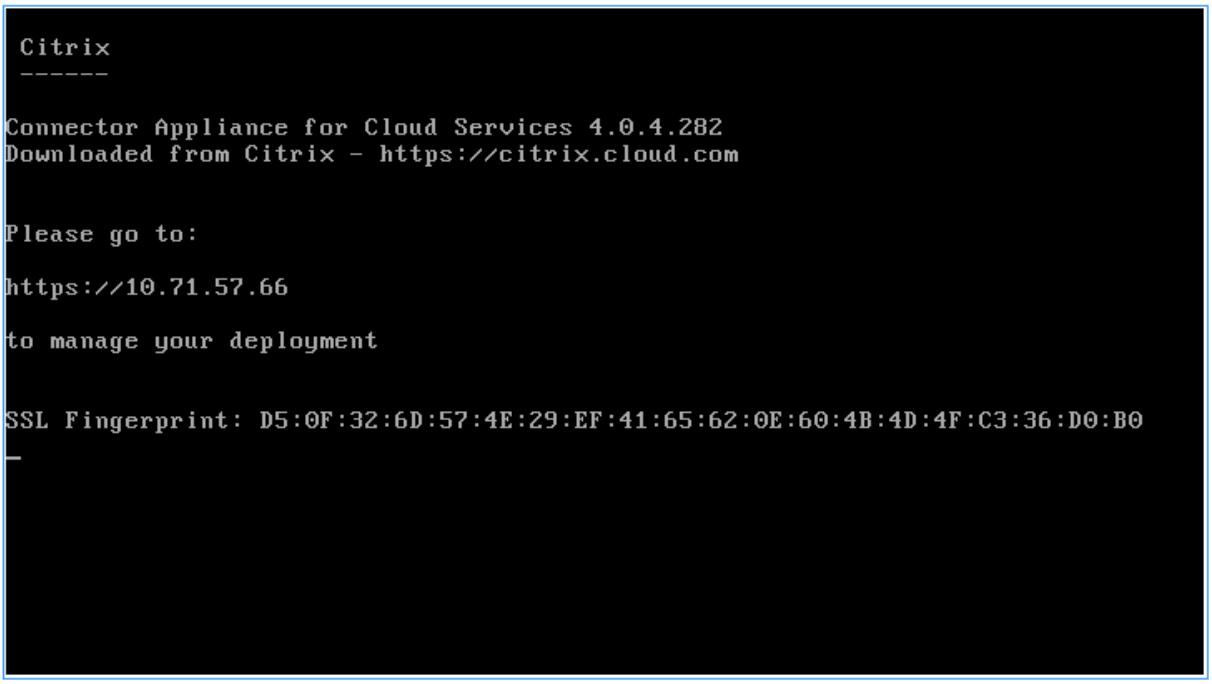
下一步：向 Citrix Cloud 注册 Connector Appliance。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

向 **Citrix Cloud** 注册您的 **Connector Appliance**

向 Citrix Cloud 注册 Connector Appliance，以便为 Citrix Cloud 与您的资源位置之间的通信提供渠道。

在虚拟机管理程序上安装并启动 Connector Appliance 后，控制台将显示 Connector Appliance 的 IP 地址。控制台还会显示 SSL 指纹，您可以使用该指纹验证与 Connector Appliance UI 的连接。



1. 将 Connector Appliance IP 地址复制到浏览器地址栏。

   > 注意：
   >
   > 您可能必须 `https://` 在 IP 地址的开头加上。

   Connector Appliance 用户界面使用自签名证书，有效期为五年。因此，您可能会看到一条关于连接不安全的消息。要验证与 Connector Appliance 的连接，可以将控制台中的 SSL 指纹与浏览器从 Web 页面接收的指纹进行比较。

   例如，在 Google Chrome 浏览器中，完成以下步骤：

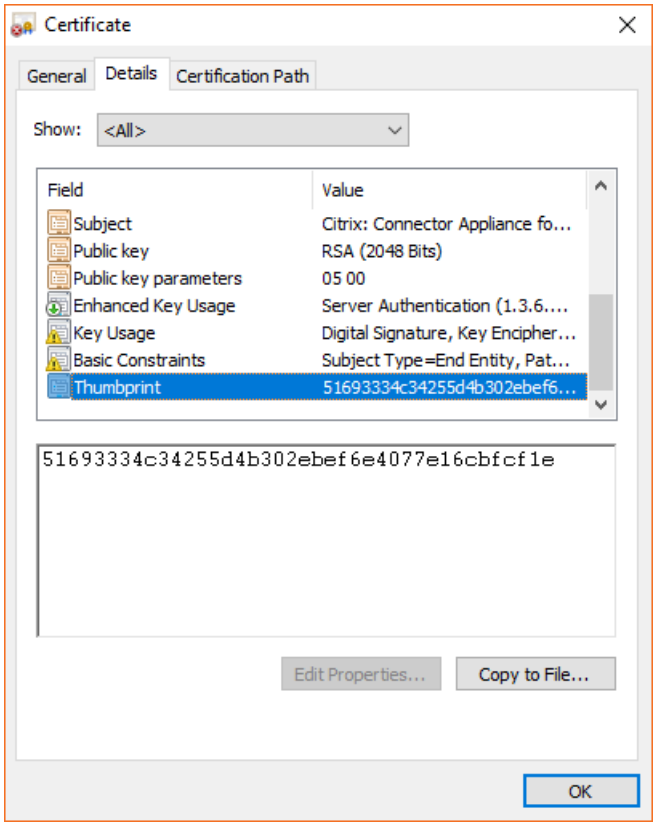
   a) 单击地址栏旁边的不安全标记。

   b) 选择证书。此时将打开证书窗口。

   c) 转到详细信息选项卡并找到指纹字段。

      如果指纹字段的值与控制台中提供的 SSL 指纹匹配，则可以确认您的浏览器直接连接到 Connector Appliance UI。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



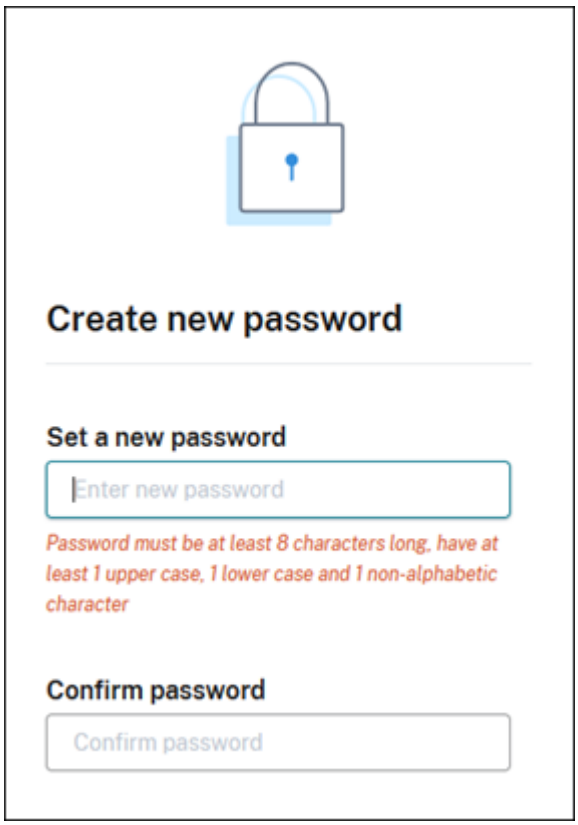
您可以将此自签名证书替换为自己的证书，该证书由您的组织签名或使用组织的信任链生成。有关更多信息，请参阅 管理证书。

2. 如果您的浏览器需要执行额外步骤来确认您要继续访问相应站点，请立即完成此步骤。

   此时将打开创建新密码 Web 页面。

3. 为您的 Connector Appliance UI 创建密码，然后单击 设置密码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



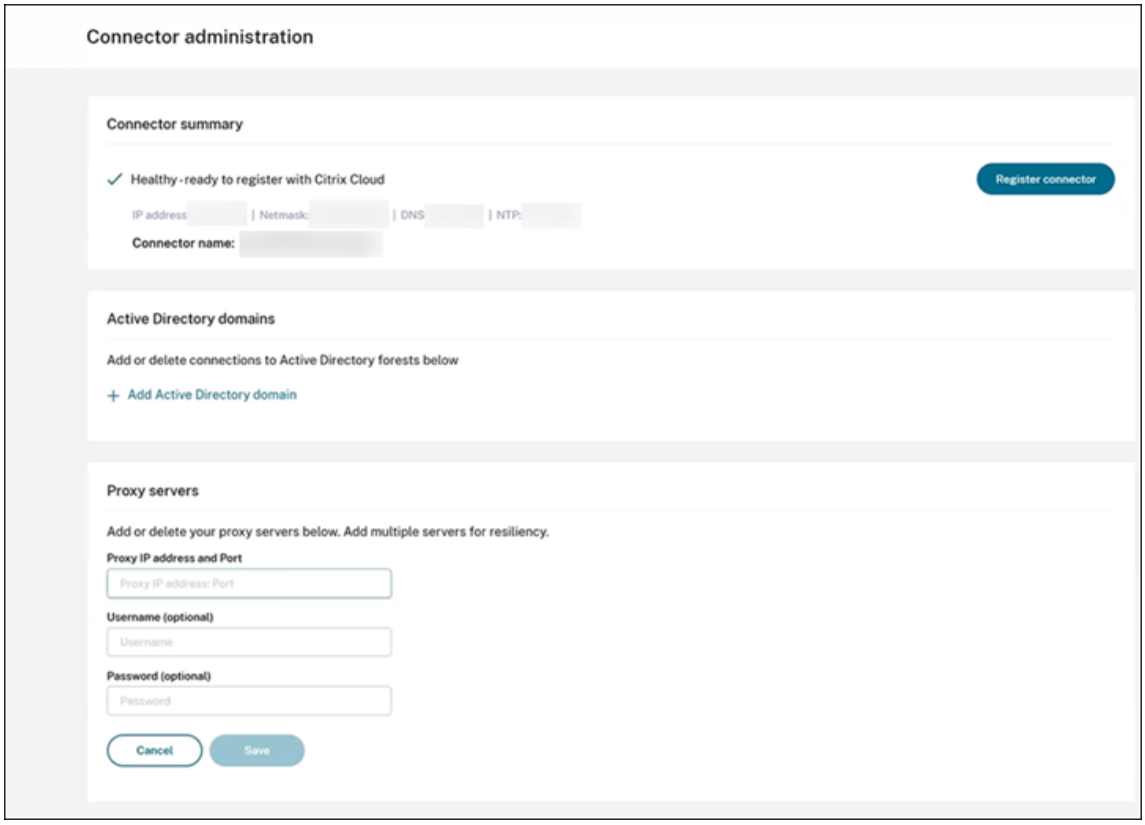
您设置的密码必须满足以下要求：

- 8 个或更多字符长
- 包含大写和小写字母
- 至少包含一个非字母字符

务必将此密码存储在安全的位置，以供将来使用。

4. 使用您设置的密码登录。连接器管理页面打开。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. （可选）如果您使用一个或多个 Web 代理，则可以在代理服务器部分添加代理地址。支持未经身份验证的代理和经过身份验证的代理。要添加未经身份验证的代理，请提供有效的 代理 **IP** 地址和端口。要添加经过身份验证的代理，请同时提供有效的 用户名 和 密码。

   > 注意：
   >
   > 仅支持基本代理身份验证。不支持其他形式的身份验证。

   只有流向外部系统的流量才会通过 Web 代理进行路由。有关更多信息，请参阅 Connector Appliance 通信。

6. （可选）如果您的网络使用 TLS 拦截 Web 代理来访问互联网，则可能需要连接器信任其根证书颁发机构才能成功与云通信。

   a) 在“根证书颁发机构”下，选择“添加证书”。

   b) 以 PEM 格式复制证书的内容：

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   <!--NeedCopy-->
   ```

   c) 在 完整证书详细信息中，粘贴证书内容。

   d) 选择“添加证书”。

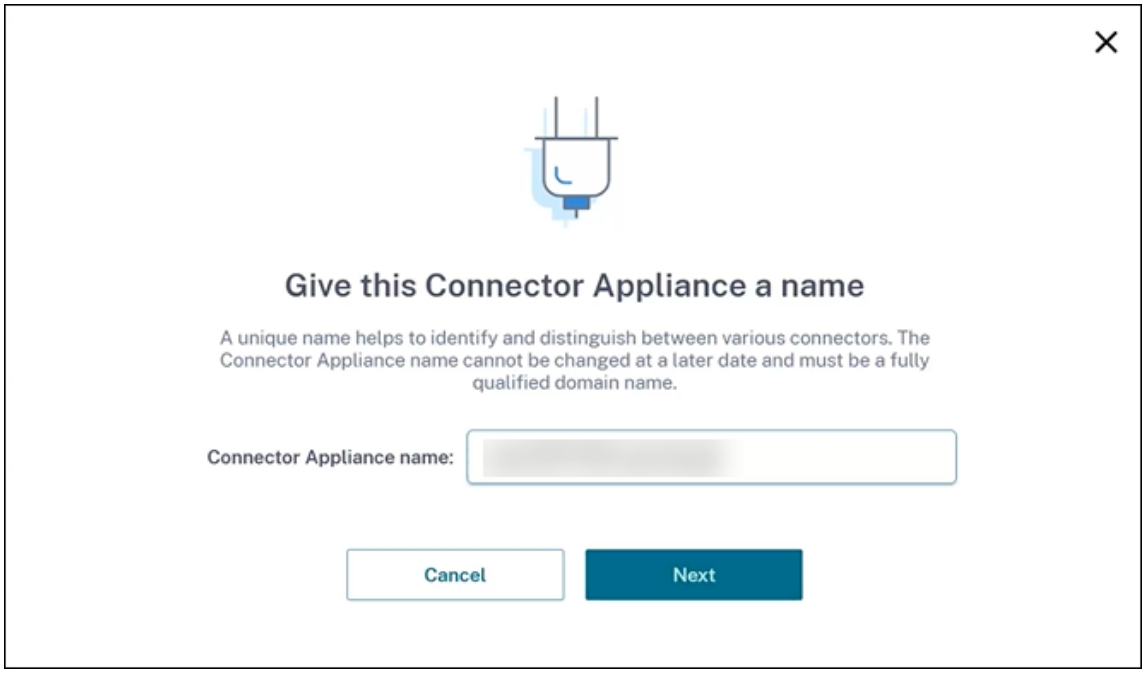
   要使用 Connector Appliance API 添加 RootCA，请参阅 Citrix Developer 文档中的管理根证书颁发机构 。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 已过期或将在未来 30 天内过期的证书将显示警告。

7. 单击注册连接器以打开注册任务。
8. 为您的 Connector Appliance 选择名称。此名称可帮助您区分资源位置中存在的各种 Connector Appliance 。注册 Connector Appliance 后，无法更改名称。

   在“**Connector Appliance** 名称”字段中输入名称，然后单击“下一步”。

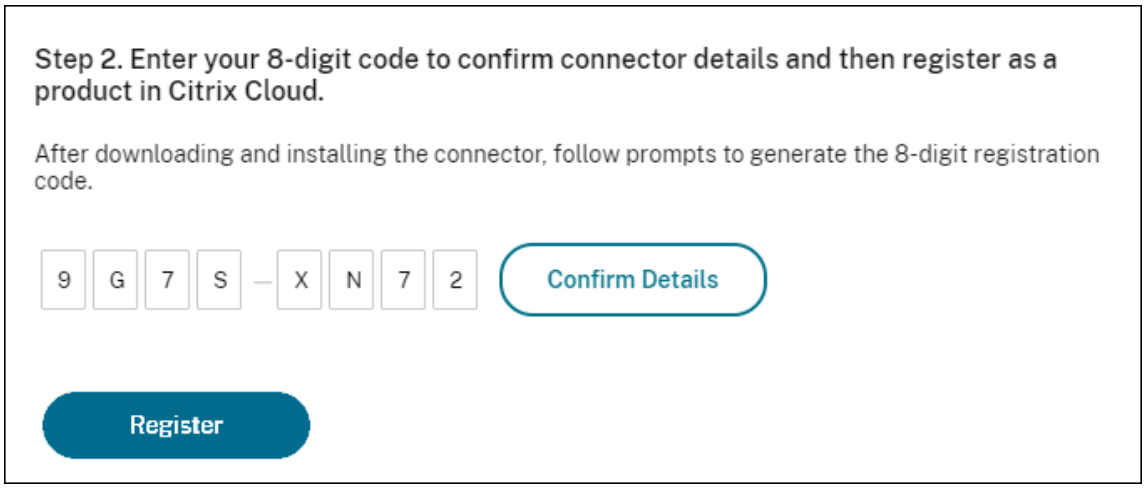


   该网页提供了用于向 Citrix Cloud 注册的代码。此代码将在 15 分钟后过期。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. 使用复制按钮将代码复制到剪贴板。
10. 返回 资源位置 网页。
11. 将代码粘贴到安装 **Connector Appliance** 任务的步骤 **2** 中。点击 确认详情。

    Citrix Cloud 会验证 Connector Appliance 是否存在且可以联系。如果注册码已过期，系统会提示您生成新代码。



12. 单击注册。

    该页面显示注册是否成功。如果注册失败，系统会提示您重试。

13. 单击关闭。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Connector Appliance 管理页面 还允许您下载 Connector Appliance 的诊断报告。有关更多信息，请参阅 生成诊断报告。

注册 **Connector Appliance** 后

对于每个资源位置，我们建议您安装并注册两个或更多的 Connector Appliance 。此配置可确保持续可用性，并使连接器能够平衡负载。

您无法直接管理 Connector Appliance 。

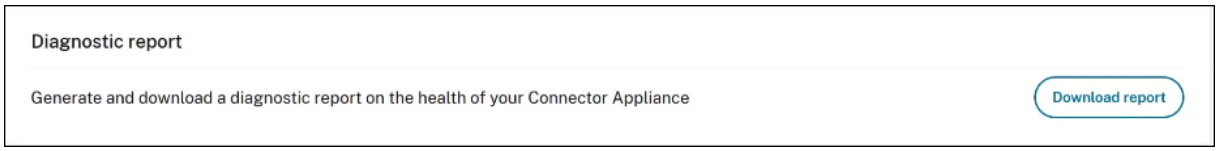
Connector Appliance 会自动更新。您无需采取任何操作来更新连接器。您可以指定希望在资源位置中应用 Connector Appliance 更新的时间和日期。有关更多信息，请参阅 连接器更新。

请勿克隆、暂停或拍摄 Connector Appliance VM 的快照。不支持这些操作。

只有在您第一次连接到 Connector Appliance 用户界面时，才会出现“创建新密码”页面。务必将此密码存储在安全的位置，以供将来使用。此密码无法重置。如果您忘记了密码，则必须重新安装 Connector Appliance 。在随后连接到 UI 时，系统会要求您输入注册 Connector Appliance 时设置的密码。

生成诊断报告

您可以从 **Connector Appliance** 管理页面生成和下载诊断报告。



1. 从虚拟机管理程序的 Connector Appliance 控制台中，将 IP 地址复制到浏览器地址栏。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 输入您在注册 Connector Appliance 时设置的密码。
3. 在页面的“诊断报告”部分，单击“下载报告”。

诊断报告以 `.zip` 文件形式提供。

验证您的网络连接

您可以使用 **TCP** 捕获诊断检查从 **Connector Appliance** 管理页面检查网络连接。

1. 在 **Connector Appliance** 管理页面上，在标题栏中单击您的帐户名，然后选择“网络诊断”。
2. （可选）在“**TCP** 捕获”部分中，输入目标 IP 地址、主机名或端口以限制 TCP 捕获。
3. 从“跟踪持续时间”菜单中，选择要运行跟踪的持续时间。
4. （可选）启用 数据包跟踪 以捕获数据包的内容。

   禁用数据包跟踪时，TCP 捕获功能会尽力捕获标头以进行诊断。这种尽力方法捕获每个数据包的前 94 个字节。但是，由于标头不是固定大小，因此此方法可能无法捕获所有标头。
5. 单击“开始跟踪”。
6. 等到追踪完成。跟踪完成后，您可以下载跟踪报告或开始新的追踪。

   - 单击“下载”以下载追踪报告。跟踪报告以 `.pcap` 文件形式提供。
   - 单击“开始新跟踪”以开始另一条跟踪。

将 **Active Directory** 连接到 **Citrix Cloud**

您可以使用 Connector Appliance 将资源位置连接到不包含 Citrix Virtual Apps and Desktops 资源的林。例如，对于某些林仅用于用户身份验证的 Citrix Secure Private Access 客户或 Citrix Virtual Apps and Desktops 客户。

有关详细信息，请参阅带 Connector Appliance 的 Active Directory。

验证您的 **Kerberos** 配置

如果您使用 Kerberos 进行单点登录，则可以从 **Connector Appliance** 管理页面验证 Active Directory 控制器上的配置是否正确。**Kerberos** 验证功能使您能够验证 Kerberos 仅限领域模式配置或 Kerberos 约束委派 (KCD) 模式配置。

验证 **Kerberos** 仅限领域的配置：

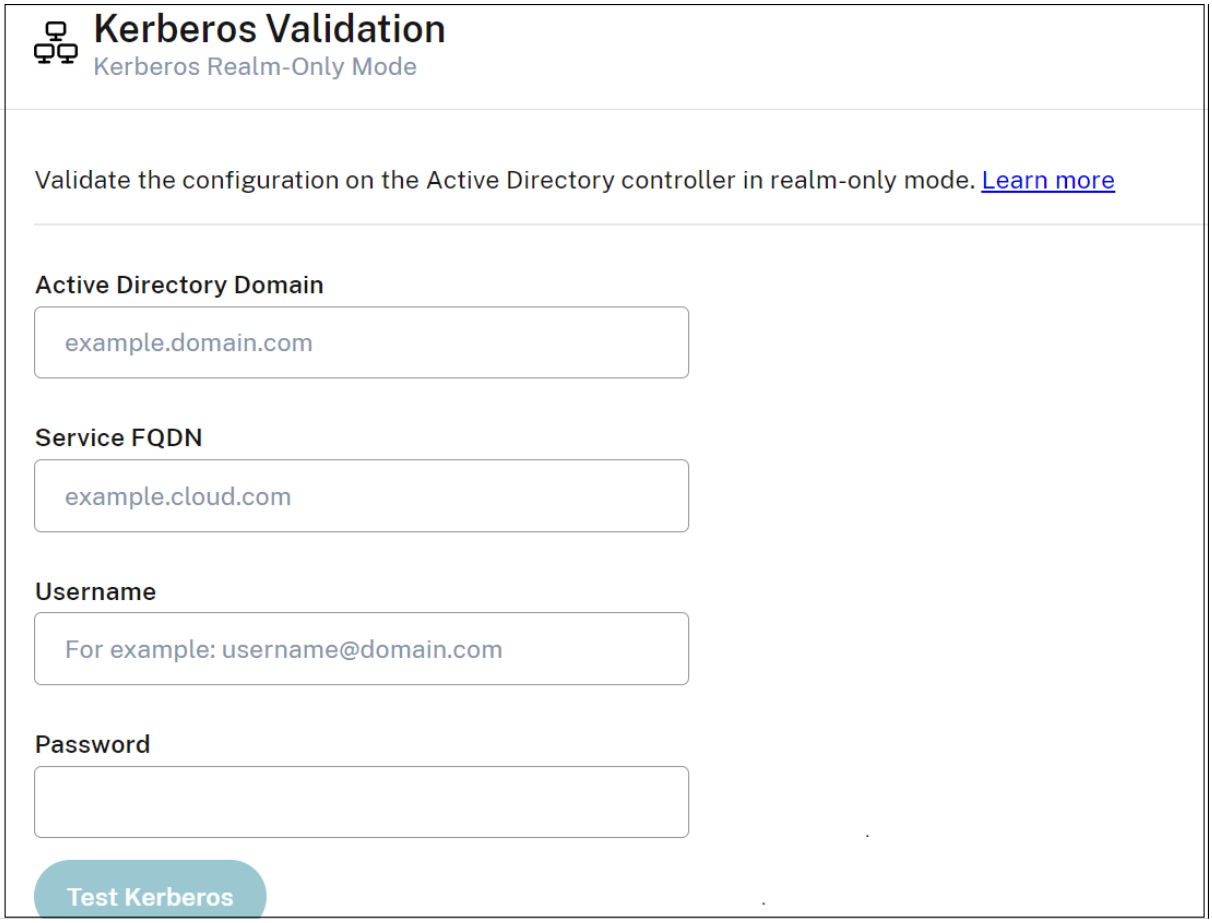
1. 转到 **Connector Appliance** 管理页面。
2. 从虚拟机管理程序的 Connector Appliance 控制台中，将 IP 地址复制到浏览器地址栏。
3. 输入您在注册 Connector Appliance 时设置的密码。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 要验证您的仅限域的 Kerberos 配置，请在 **Active Directory** 域部分中选择仅限 **Kerberos** 验证领驭。
5. 指定 **Active Directory** 域。

    - 如果您正在验证 Kerberos 仅限领域的模式配置，您可以指定任何 Active Directory 域。此模式不依赖于是否加入该域。

6. 指定 服务 **FQDN**。假定默认服务名称为“https”。如果指定“computer.example.com”，则此值被视为与“https://computer.example.com”相同。
7. 指定用户 名。
8. 指定密码。
9. 单击“测试 **Kerberos**”。



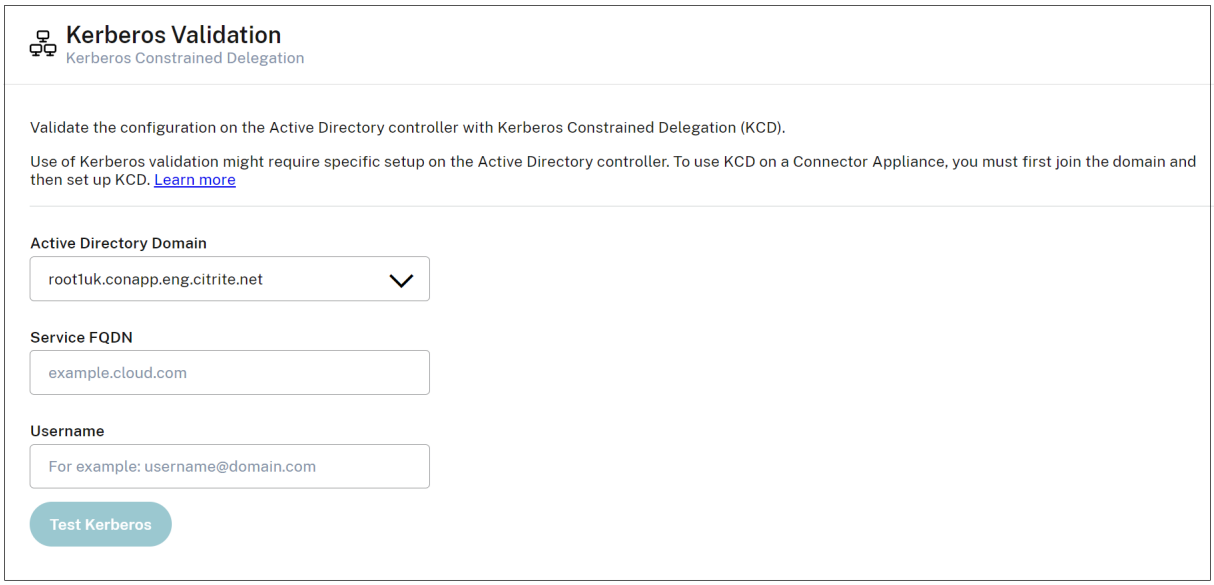
验证 **Kerberos** 限制委托 **(KCD)** 配置：

1. 转到 **Connector Appliance** 管理页面。
2. 要验证已加入 Connector Appliance 的域的 **Kerberos** 约束委派 **(KCD)** 模式，请从相关域的省略号菜单 (…) 中选择 **Kerberos** 验证。
3. 指定 **Active Directory** 域。

    - 如果您正在验证 Kerberos 约束委派配置，则必须从加入的域列表中进行选择。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 指定 服务 **FQDN**。假定默认服务名称为“https”。例如，指定“computer.example.com”，该值被视为与“https://computer.example.com%E2%80%9D”相同。
5. 指定用户 名。
    - 对于 Kerberos 约束委派模式，您还可以通过选择“服务帐户”选项卡，使用服务帐户验证 kerberos 设置。
6. 单击“测试 **Kerberos**”。



如果 Kerberos 配置正确，则会看到消息“已成功验证 Kerberos 设置”。如果 Kerberos 配置不正确，您会看到一条错误消息，其中提供了有关验证失败原因的信息。

有关 Kerberos 的更多信息，请参阅 Microsoft 文档。

Connector Appliance 的网络设置

默认情况下，Connector Appliance 的 IP 地址和网络设置是使用 DHCP 自动分配的。

使用 DHCP 注册 Connector Appliance 后，可以在 **Connector Appliance** 管理页面中编辑其网络设置。

但是，如果 DHCP 在您的环境中不可用，或者您无权访问 **Connector Appliance** 管理页面，则可以直接在 Connector Appliance 控制台上设置网络配置。

在 **Connector Appliance** 管理页面上配置网络设置

使用 DHCP 注册 Connector Appliance 后，可以在 **Connector Appliance** 管理页面中编辑其网络设置。

要手动配置网络设置，请执行以下操作：

1. 在连接器摘要部分中，选择编辑网络设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 在“网络设置”对话框中，选择“配置您自己的网络设置”。
3. 输入 **IP** 地址、子网掩码和 默认网关。
4. 添加一个或多个 **DNS** 服务器。
5. 添加一个或多个 **NTP** 服务器。
6. 单击保存。

保存对网络设置的更改后，Connector Appliance 将重新启动。在重新启动期间，Connector Appliance 暂时不可用。您已从 **Connector Appliance** 管理页面注销，并且此页面的 URL 发生更改。您可以在 Connector Appliance 控制台中找到新的 URL，也可以通过查看虚拟机管理程序中的网络信息来找到新的 URL。

要将网络配置更改为使用自动分配的值，请执行以下操作：

1. 在连接器摘要部分中，选择编辑网络设置。
2. 在“网络设置”对话框中，选择“自动获取 **IP** 地址”。
3. 单击保存。

保存对网络设置的更改后，Connector Appliance 将重新启动。在重新启动期间，Connector Appliance 暂时不可用。您已从 **Connector Appliance** 管理页面注销，并且此页面的 URL 发生更改。您可以在 Connector Appliance 控制台中找到新的 URL，也可以通过查看虚拟机管理程序中的网络信息来找到新的 URL。

使用 **Connector Appliance** 控制台设置网络配置

默认情况下，Connector Appliance 的 IP 地址和网络设置是使用 DHCP 自动分配的。但是，如果 DHCP 在您的环境中不可用，或者您无权访问 **Connector Appliance** 管理页面，则可以直接在 Connector Appliance 控制台上设置网络配置。

要设置网络配置，请执行以下操作：

1. 在虚拟机管理程序中，重新启动 Connector Appliance。
2. 当 Connector Appliance 启动时，请注意控制台上的消息 `Welcome to GRUB!`。
3. 当您看到此消息时，按 **Esc** 键进入 GRUB 菜单。
4. 要编辑引导参数，请按 **e**。

   您会看到如下图所示的视图：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. 编辑以开头的行 `linux` ，以包括所需的网络配置。

   - 要指定 DHCP 网络连接，`network=dhcp` 请在行末追加。
   - 要指定静态网络，请将以下参数附加到该行的末尾：

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     <!--NeedCopy-->
     ```

     将占位符值替换为您的配置的值。

6. 按 **Ctrl+X** 以使用新配置启动 Connector Appliance 。

更改 **Connector Appliance** 的管理员用户密码

1. 在控制台右上角的用户菜单中，选择更改密码。

   屏幕上将显示更改密码页面。

2. 输入您的当前密码，然后输入并确认新密码。您设置的新密码必须满足以下要求：

   - 8 个或更多字符长
   - 包含大写和小写字母
   - 至少包含一个非字母字符
   - 不得与当前密码相同

3. 选择“更改密码”以保存您的更改。

Citrix Cloud 会自动将您注销并将您重定向到登录页面。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

带 Connector Appliance 的 Active Directory

April 5, 2024

您可以使用 Connector Appliance 将资源位置连接到不包含 Citrix Virtual Apps and Desktops 资源的林。例如，对于某些林仅用于用户身份验证的 Citrix Secure Private Access 客户或 Citrix Virtual Apps and Desktops 客户。

将多域 Active Directory 与 Connector Appliance 配合使用时，以下限制适用：

- 在包含 VDA 的林中，无法使用 Connector Appliance 代替 Cloud Connector。

要求

Active Directory 要求

- 已加入一个 Active Directory 域，该域包含用于为用户创建产品/服务的资源和用户。有关详细信息，请参阅本文中的 Active Directory 中 Connector Appliance 的部署方案 。
- 您计划在 Citrix Cloud 上使用的每个 Active Directory 林必须始终可以通过两台 Connector Appliance 进行访问。
- Connector Appliance 必须能够访问林根域和您打算用于 Citrix Cloud 的域中的域控制器。有关详细信息，请参阅以下 Microsoft 支持文章：
  - 如何配置域和信任
  - 服务 概述和 Windows 网络端口要求中的“系统服务端口”部分
- 使用通用安全组而不是全局安全组。此配置确保可以从林中的任何域控制器获取用户组成员资格。

网络要求

- 已连接到可以联系您在资源位置使用的资源的网络。
- 已连接到 Internet。有关详细信息，请参阅系统和连接要求。

除了 Connector Appliance 通信中列出的端口外，Connector Appliance 还需要通过以下端口出站连接到 Active Directory 域：

服务	端口	支持的域协议
Kerberos	88	TCP/UDP
端点映射器（DCE/RPC 定位器服务）	135	TCP
NetBIOS 名称服务	137	UDP

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

服务	端口	支持的域协议
NetBIOS 数据报	138	UDP
NetBIOS 会话	139	TCP
LDAP	389	TCP/UDP
TCP 上的 SMB	445	TCP
Kerberos kpasswd	464	TCP/UDP
全局目录	3268	TCP
动态 RPC 端口	49152–65535	TCP

Connector Appliance 使用 LDAP 签名来保护与域控制器的连接。这意味着不需要基于 SSL 的 LDAP (LDAPS)。有关 LDAP 签名的更多信息，请参阅如何在 Windows Server 中启用 LDAP 签名和 Microsoft 启用 LDAP 通道绑定和 LDAP 签名的指南。

支持的 **Active Directory** 功能级别

Connector Appliance 已经过测试，在 Active Directory 中受以下林和域功能级别的支持。

林功能级别	域功能级别	支持的域控制器
Windows Server 2016	Windows Server 2016	Windows Server 2019

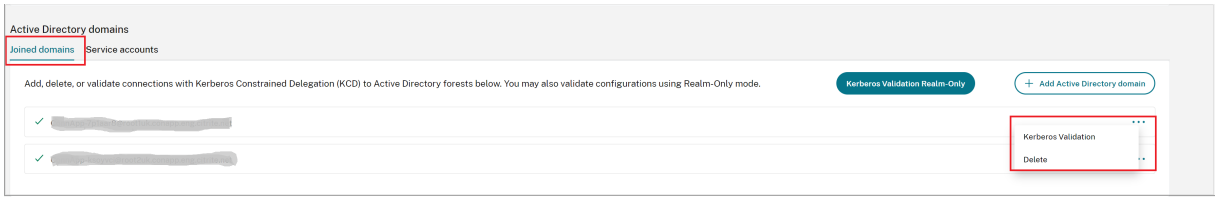
尚未使用 Connector Appliance 测试域控制器、林功能级别和域功能级别的其他组合。但是，这些组合应该起作用并且也受支持。

使用 **Connector Appliance** 将 **Active Directory** 域连接到 **Citrix Cloud**

当您连接到 Connector Appliance 管理网页时，Active Directory 域部分会显示两个选项卡。

- 加入域 -用于通过在域中为设备创建计算机帐户将 Connector Appliance 加入到 AD 域。可以通过单击已加入域右侧的省略号菜单来验证 Kerberos。需要在域中存在计算机帐户。
- 服务帐户 -用作 Secure Private Access (SPA) 解决方案的一部分，使用服务帐户而不是加入域时创建的计算机帐户来实现 Kerberos SSO。可以通过单击服务帐户右侧的省略号菜单来验证 Kerberos。拥有与计算机关联的特定域并不是强制性的。但是，即使 Connector Appliance 未连接到域，它仍然可以连接到域控制器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要将 Active Directory 配置为通过 Connector Appliance 连接到 Citrix Cloud，请完成以下步骤。

1. 在您的资源位置安装 Connector Appliance。

   您可以按照 Connector Appliance 产品文档中的信息进行操作。

2. 使用 Connector Appliance 控制台中提供的 IP 地址连接到浏览器中的 Connector Appliance 管理 Web 页面。

3. 在 **Active Directory** 域名 部分中，导航到 已加入的域名 选项卡。

4. 单击 **+** 添加 **Active Directory** 域名，将显示一个新的弹出窗口，用于输入域名。

   Connector Appliance 会检查域。如果检查成功，则会打开“加入 **Active Directory**”对话框。这个新窗口允许您输入用户名和密码以加入该域。

5. 单击添加。

6. 提供具有该域加入权限的 Active Directory 用户的用户名和密码。

7. Connector Appliance 会建议计算机名称。您可以选择覆盖建议的名称，并自行提供长度不超过 15 个字符的计算机名称。

   此计算机名称是在 Connector Appliance 加入时在 Active Directory 域中创建的。

8. 单击“加入”。

   该域现在列在 Connector Appliance UI 的 **Active Directory** 域 部分中。

9. 要添加更多 **Active Directory** 域，请选择 **+** 添加 **Active Directory** 域 并重复上述步骤。

10. 前往 **Citrix Cloud** 控制台中的域名页面，然后选择 **Connector Appliance** 为您的域提供服务。

11. 如果您尚未注册 Connector Appliance，请按照向 Citrix Cloud 注册 Connector Appliance 中所述继续执行步骤。

如果您在加入域时收到错误，请验证您的环境是否满足 Active Directory 要求和网络要求。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

接下来做什么

- 您可以向此 Connector Appliance 添加更多域。

  > 注意：
  >
  > Connector Appliance 在多达 10 个林中进行了测试。

- 为了恢复能力，请将每个域添加到每个资源位置中的多个 Connector Appliance 中。

查看您的 **Active Directory** 配置

您可以在资源位置的以下位置查看 Active Directory 域和 Connector Appliance 的配置：

- 在 Citrix Cloud 中：
  1. 在菜单中，转到 身份和访问管理 页面。
  2. 转到“域”选项卡。

     列出了您的 Active Directory 域名以及它们所属的资源位置。
- 在 Connector Appliance Web 页面中：
  1. 使用 Connector Appliance 控制台中提供的 IP 地址连接到 Connector Appliance 网页。
  2. 使用您首次注册时创建的密码登录。
  3. 在该页的 **Active Directory** 域 部分中，您可以看到此 Connector Appliance 加入的 Active Directory 域的列表。

从 **Connector Appliance** 中删除 **Active Directory** 域

要退出 Active Directory 域，请完成以下步骤：

1. 使用 Connector Appliance 控制台中提供的 IP 地址连接到 Connector Appliance 网页。
2. 使用您首次注册时创建的密码登录。
3. 在该页的 **Active Directory** 域 部分中，在已加入的 Active Directory 域列表中找到要保留的域。
4. 记下 Connector Appliance 创建的计算机帐户的名称。
5. 单击域旁边的删除图标（垃圾桶）。将显示确认对话框。
6. 单击“继续”以确认操作。
7. 转到您的 Active Directory 控制器。
8. 从控制器中删除 Connector Appliance 创建的计算机帐户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将 **Connector Appliance** 与 **Active Directory** 配合使用的部署方案

您可以同时使用 Cloud Connector 和 Connector Appliance 连接到 Active Directory 控制器。要使用的连接器类型取决于您的部署。

有关将 Cloud Connector 与 Active Directory 结合使用的详细信息，请参阅 Active Directory 中 Cloud Connector 的部署方案

在以下情况下，使用 Connector Appliance 将您的资源位置连接到 Active Directory 林：

- 您正在设置 Secure Private Access。有关详细信息，请参阅在 Connector Appliance 中配置 Secure Private Access。
- 您有一个或多个仅用于用户身份验证的林
- 您希望减少支持多个林所需的连接器数量
- 您需要 Connector Appliance 用于其他用例

仅限一个或多个林中的用户对所有林使用一套 **Connector Appliance**

此方案适用于 Workspace Standard 客户或使用适用于 Secure Private Access 的 Connector Appliance 的客户。

在这种情况下，有几个林仅包含用户对象 (`forest1.local`、`forest2.local`)。这些森林不包含资源。一组 Connector Appliance 部署在资源位置中，并加入到每个林的域中。

- 信任关系：无
- 身份和访问管理中列出的域：`forest1.local`、`forest2.local`
- 用户登录到 Citrix Workspace：支持所有用户
- 用户登录到本地 StoreFront：支持所有用户

单独林中的用户和资源（受信任），使用一套适用于所有林的 **Connector Appliance**

此方案适用于具有多个林的 Citrix Virtual Apps and Desktops 客户。

在这种情况下，有些林 (`resourceforest1.local`, `resourceforest2.local`) 包含您的资源（例如 VDA），而一些林（`userforest1.local`、`userforest2.local`）仅包含您的用户。这些林之间存在信任，允许用户登录到资源。

`resourceforest1.local` 林中部署了一组 Cloud Connector。在 `resourceforest2.local` 林中部署了一组单独的 Cloud Connector。

一组 Connector Appliance 部署在 `userforest1.local` 林中，同一组 Connector Appliance 部署在 `userforest2.local` 林中。

- 信任关系：双向林信任，或从资源林到用户林的单向信任

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 身份和访问管理中列出的域：resourceforest1.local、resourceforest2.local、userforest1.local、userforest2.local
- 用户登录到 Citrix Workspace：支持所有用户
- 用户登录到本地 StoreFront：支持所有用户

Connector 更新

August 7, 2023

Citrix 会定期发布更新，以提高 Cloud Connector 或连接器设备的性能、安全性和可靠性。默认情况下，Citrix Cloud 会在每个连接器上安装更新（一次一个），只要这些更新可用。为确保及时安装更新而不会对用户的 Citrix Cloud 体验造成不当影响，您可以按如下方式控制连接器更新：

- 为一天中的首选时间和一周中的首选日期安排更新。
- 执行一次性延迟，这样您指定的连接器就会比计划晚两周更新。
- 如果由于主机上的问题而导致更新失败，请在问题得到解决后重新启动更新。

此外，您可以通过将资源位置中的当前连接器版本与 Citrix Cloud 中的目标版本进行比较来验证连接器是否为最新版本。

> 注意：
>
> 本文介绍如何使用 Citrix Cloud 管理控制台安排连接器更新。有关使用 Citrix Cloud API 安排连接器更新的信息，请参阅 Citrix Developer 文档中的 Citrix Cloud-维护计划 。

一天中的首选时间

指定一天中的首选时间后，Citrix Cloud 会在更新可用后 24 小时内按照您的首选时间进行安装。例如，如果一天中的首选时间是美国太平洋时间凌晨 2:00，并且星期二有更新可用，则 Citrix Cloud 将等待 24 小时，然后在第二天凌晨 2:00 安装更新。

一周中的首选日期

指定一周中的首选日期时，Citrix Cloud 将等待 7 天，然后在首选日期安装更新。这七天的等待期使您有足够的时间来选择是按需安装更新，还是等待 Citrix Cloud 在首选日期安装更新。根据您选择的星期几和可用的更新日期，Citrix Cloud 可能会等待最多 13 天才能安装更新。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8 天等待期示例

在星期一，您可以将星期二下午 6:00 配置为首选的更新日期。当天晚些时候，Citrix Cloud 会通知您有可用的更新，并显示 更新 按钮。如果您不启动更新，Citrix Cloud 将等待 7 天，然后在第二天（星期二下午 6:00）安装更新。

等待 **13** 天的示例

您已将星期一下午 6:00 配置为一天中进行更新的首选时间。星期二，Citrix Cloud 会通知您有可用的更新，并显示 更新 按钮。如果您不启动更新，Citrix Cloud 将等待 7 天，然后在六天后的星期一下午 6:00 安装更新。

更新通知和按需更新

当更新可用时，Citrix Cloud 会在通知中通过警报 通知您。此外，每个连接器还会显示安装更新的日期和时间。

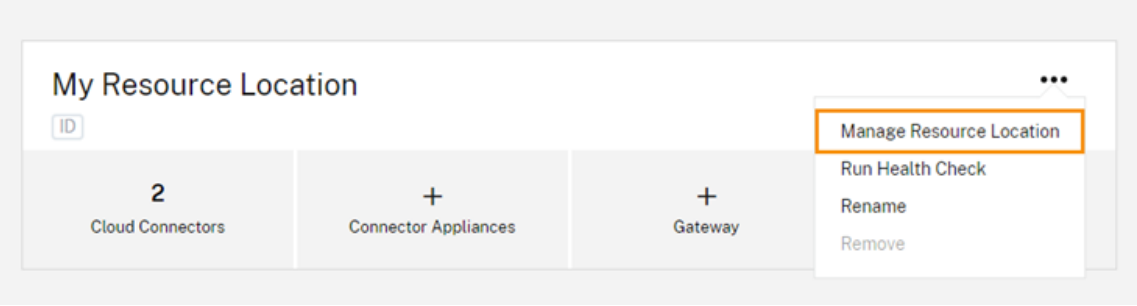
在 Citrix Cloud 通知您有可用更新后，每个连接器都会显示一个 更新 按钮，以便您可以在首选时间或日期之前安装更新。为每个连接器选择“更新”后，Citrix Cloud 会将更新排入队列并逐一安装。启动更新后，您无法取消更新。

更新完成后，Citrix Cloud 将显示上次更新的日期。如果某些更新无法完成，则会发送通知您。

选择更新计划

使用本节中的步骤通过 Citrix Cloud 管理控制台安排连接器更新。有关使用 Citrix Cloud API 安排更新的信息，请参阅 Citrix Developer 文档中的 Citrix Cloud-维护计划 。

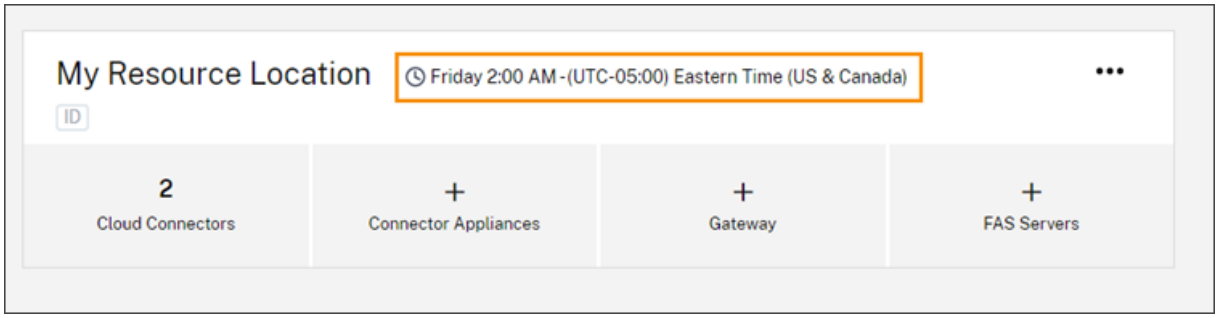
1. 从 Citrix Cloud 菜单中，选择资源位置。
2. 找到要修改的资源位置，然后从省略号菜单中选择 管理资源位置。



3. 在“选择更新方法”下，选择“设置维护开始时间”，然后选择安装更新的首选日期、时间和时区。
   - 要仅指定一天中的首选时间，请选择要安装更新的时间和时区。Citrix Cloud 会在更新可用后 24 小时内按照您的首选时间安装更新。
   - 要指定一周中的首选日期，请选择小时、星期和时区。Citrix Cloud 在更新可用后等待 7 天，然后在首选日期进行安装。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置更新计划后，Citrix Cloud 会在资源位置名称旁边显示该计划。



您选择的开始时间将应用于所有连接器，无论它们位于哪个时区。如果您的连接器位于不同的时区，Citrix Cloud 会在您选择的时间和时区安装更新。例如，如果您计划在美国太平洋时区凌晨 2:00 进行更新，而伦敦有连接器，Citrix Cloud 将在美国太平洋时间凌晨 2:00 开始在这些连接器上安装更新。

重新启动更新

如果连接器在更新安装过程中遇到问题，安装将暂停，直到问题得到解决。由于更新一次安装在每个连接器上，因此在一个连接器上暂停更新可能会阻止 Citrix Cloud 帐户中所有剩余的 Cloud Connector 的更新。问题解决后，您可以重新启动更新。

1. 从 Citrix Cloud 菜单中，选择资源位置。
2. 找到要管理的资源位置，然后选择“**Cloud Connector**”或“**Connector Appliance**”磁贴。
3. 找到要管理的连接器，然后选择“重新启动更新”。

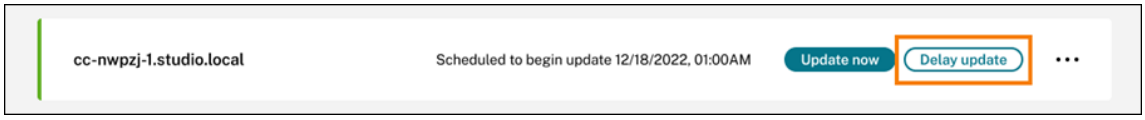
延迟更新

您可以延迟预设更新，以便在两周后对您指定的连接器进行更新。您只能将预设更新延迟一次。延迟更新一次后，就无法再延迟更新。此外，您无法更改默认的两周周期。

1. 从 Citrix Cloud 菜单中，选择资源位置。
2. 找到要管理的资源位置，然后选择“**Cloud Connector**”或“**Connector Appliance**”磁贴。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 找到要管理的连接器，然后选择“延迟更新”。



预定日期更改为比原定日期晚两周的日期。

计划外更新

即使您将更新安排在以后的日期和时间，Citrix Cloud 仍可能在更新发布后尽快安装更新。在以下情况下会发生计划外更新：

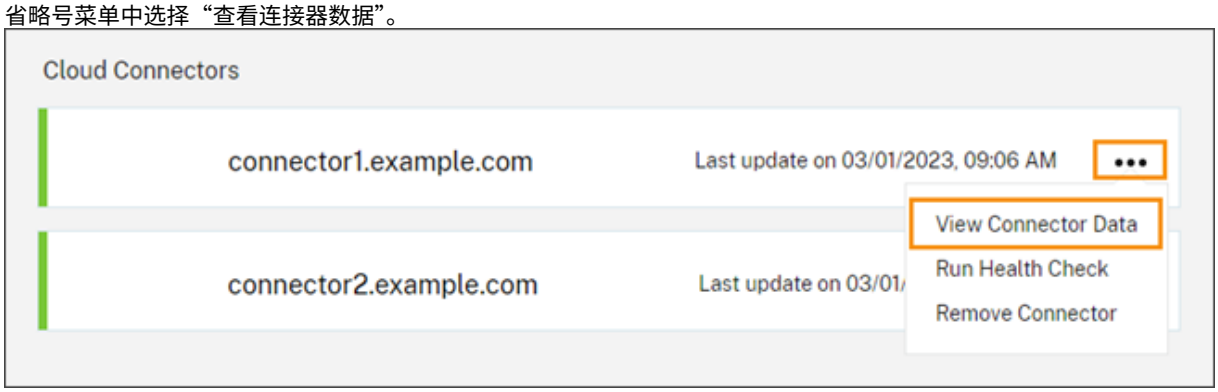
- 更新无法在可用后的 48 小时内按首选时间安装。例如，如果您的首选时间是凌晨 2:00，并且连接器在更新发布后三天内处于脱机状态，Citrix Cloud 会在连接器重新联机时立即安装更新。
- 此更新包含针对严重安全或功能问题的修复程序。

比较 **Cloud Connector** 版本

您可以查看资源位置中运行的是哪个版本的 Cloud Connector，以及它是否为最新版本。此信息可帮助您验证 Cloud Connector 是否已成功更新。

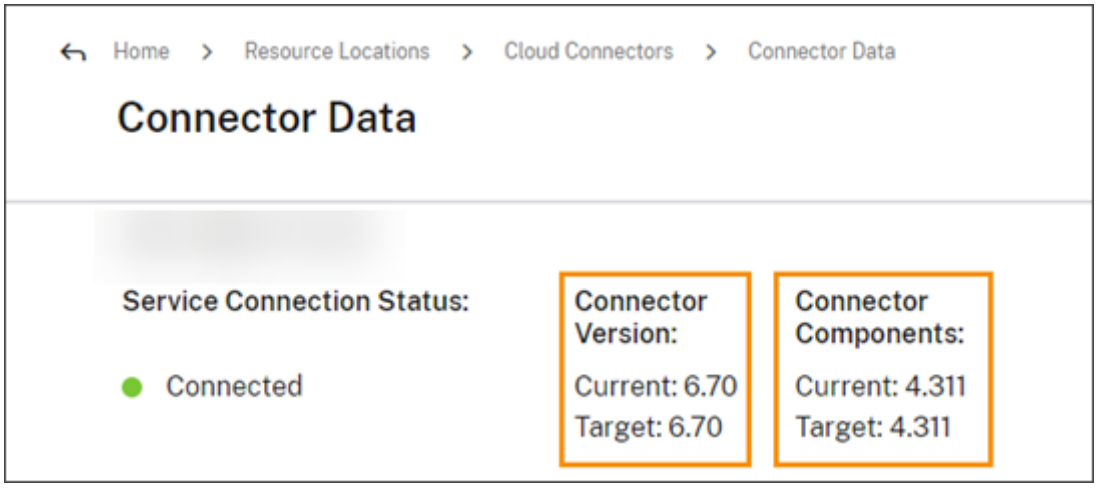
> 注意：
>
> 此信息不适用于连接器设备。

在资源位置页面中，选择要管理的资源位置的 **Cloud Connector** 磁贴。找到要检查的 Cloud Connector，然后从省略号菜单中选择“查看连接器数据”。



当前版本号是当前 在 Cloud Connector 计算机上运行的 Cloud Connector 软件的版本。目标 版本号是 Citrix 发布的 Cloud Connector 软件的最新版本。如果计算机更新成功，则当前版本号和目标版本号匹配。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



更新失败疑难解答

Cloud Connector 计算机上安装的软件冲突或维护期间出现意外错误可能会导致 Cloud Connector 无法更新和服务中断。有关如何处理 Cloud Connector 维护后失败更新的信息，请访问 解决 Cloud Connector 维护失败的问题。

如果 Cloud Connector 更新不成功，您可以通过验证以下条件开始对问题进行故障排除：

- Cloud Connector 已打开电源并使用 Cloud Connector 连接检查实用程序连接到 Citrix Cloud。
- 代理和防火墙配置正确。
- 所需的 Windows 服务处于“已启动”状态。
- 已在 Cloud Connector 上启用高级日志记录。

有关对 Cloud Connector 更新失败进行故障排除的说明，请参阅 Citrix 支持知识中心中的 CTX270718 。

要获得故障排除帮助，您可以 Citrix Cloud Connector 日志发送到 Citrix。有关信息，请参阅 Citrix Cloud Connector 日志收集。

身份识别和访问管理

July 1, 2024

身份识别和访问管理定义了用于 Citrix Cloud 管理员和 Workspace 订阅者的身份提供商和帐户。

身份提供商

Citrix Cloud 支持的身份提供程序可用于对 Citrix Cloud 管理员、Workspace 订阅者或两者进行身份验证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

身份提供商	管理员身份验证	订阅者身份验证
Citrix 身份提供程序	是	否
本地 Active Directory	否	是
Active Directory 加令牌	否	是
Azure Active Directory	是	是
Citrix Gateway	否	是
Google Cloud Identity	是	是
Okta	否	是
SAML 2.0	是（仅限 AD 组）	是

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。Citrix 身份提供程序仅对 Citrix Cloud 管理员进行身份验证。

Citrix 身份提供程序

Citrix Cloud 包括内置的 Citrix 身份提供商，用于在管理员登录时对其进行身份验证。在 Citrix Cloud 控制台中，Citrix 身份提供商被标记为 Citrix Identity。
如果您使用其他身份提供商进行管理员身份验证，Citrix 建议在 **Citrix** 身份提供者下至少有一个完全访问权限管理员。此条件可确保：

- 如果您的主要身份提供商不可用，您的 Citrix Cloud 帐户不会被锁定。
- 您可以访问自己的 Citrix Cloud 帐户来执行某些在使用其他身份提供商（例如 Azure AD）登录时无法完成的操作。例如，如果 Azure AD 是您选择的身份提供商，并且您需要重新启动 Azure AD 和 Citrix Cloud 之间的连接，则可以在使用 Citrix 身份提供商登录后执行此任务。

删除 **Citrix** 身份提供商

对于所有新的 Citrix Cloud 帐户，Citrix 身份提供商默认处于连接状态。如果您选择不使用 Citrix 身份提供商，则可以在需要时删除连接。例如，您可以选择删除此连接，以符合贵组织的安全和管理员管理政策。

删除此连接会禁用 Citrix 身份提供商，因此无法使用它对 Citrix Cloud 管理员进行身份验证。

在删除 Citrix 身份提供商连接之前，必须在 Citrix Cloud 中配置另一个身份提供商。如果没有其他已配置的身份提供商，Citrix Cloud 不允许您删除此连接。

> 重要
>
> 如果您无法访问所选身份提供商，则必须联系 Citrix 支持部门以恢复您的 Citrix Cloud 帐户。此过程可能需要几

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 天才能完成。

要删除 Citrix 身份提供商连接，请执行以下操作：

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
2. 在身份验证选项卡上，找到 Citrix 身份提供商。
3. 单击省略号菜单，然后选择删除身份提供商。

4. 当系统提示确认删除时，选择“我知道删除此身份提供者也会删除 **Citrix Cloud** 中该身份提供者的配置数据”。
5. 单击“删除身份提供商”。

Citrix 联合身份验证服务

Citrix Cloud 还支持使用 Citrix 联合身份验证服务为 Workspace 订阅者提供单点登录访问权限。有关更多信息，请参阅以下文章：

- 将 FAS 连接到 Citrix Cloud：使用 Citrix 联合身份验证服务为 Workspace 启用单点登录
- Citrix Tech Zone：
  - 参考体系结构：联合身份验证服务
  - 技术洞察：联合身份验证服务

管理员

管理员使用其身份来访问 Citrix Cloud，执行管理活动和安装 Citrix Cloud Connector。

Citrix 身份机制提供使用电子邮件地址和密码对管理员进行身份验证的方法。管理员还可以使用其 My Citrix 凭据登录 Citrix Cloud。

多重身份验证

Citrix Cloud 为管理员和 Workspace 订阅者提供多重身份验证方法。

对于管理员来说，登录 Citrix Cloud 时需要进行多重身份验证。管理员可以在加入 Citrix Cloud 帐户时或在接受其他管理员的邀请后注册其设备。有关详细信息，请参阅以下文章：

- 设置多重身份验证

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 管理您的主要 MFA 方法
- 管理您的 MFA 恢复方法

对于 Workspace 订阅者，当管理员配置 Active Directory plus 令牌身份验证方法时，将启用多重身份验证。Active Directory 加令牌是 Citrix Workspace 的默认身份提供程序。配置完成后，订阅者注册其设备进行多重身份验证。有关详细信息，请参阅以下文章：

- 启用 Active Directory 加令牌身份验证
- 注册设备进行双重身份验证
- 重新注册设备

或者，您可以对 Citrix Cloud 管理员和 Workspace 订阅者使用 Azure AD 多重身份验证。有关部署方法的更多信息，请参阅 Microsoft Azure MFA 部署方法。

添加新管理员

帐户加入过程中，将创建一个初始管理员。作为初始管理员，您可以将其他管理员添加到您的 Citrix Cloud 帐户。这些新管理员可以使用自己现有的 Citrix 帐户凭据或者根据需要设置一个新帐户。您还可以微调您添加的管理员的访问权限。通过设置这些权限，您可以使访问级别与组织中的管理员角色保持一致。

有关添加管理员和设置访问权限的更多信息，请参阅 管理管理员访问权限。

重置您的密码

如果您忘记或想要重置密码，请单击“忘记用户名或密码?”在 Citrix Cloud 登录页面上。输入电子邮件地址或用户名以查找您的帐户之后，Citrix 将向您发送一封电子邮件，其中包含一个用于重置密码的链接。

Citrix 要求您在特定条件下重置密码，以帮助您保护帐户密码的安全。有关这些条件的更多信息，请参阅 更改密码。

> 注意：
>
> 将 **customerservice@citrix.com** 添加到允许的电子邮件地址列表中，以确保 Citrix Cloud 电子邮件不会进入您的垃圾邮件或垃圾文件夹。

删除管理员

您可以在“管理员”选项卡上从 Citrix Cloud 帐户中移除 管理员。移除管理员后，他们将无法再登录 Citrix Cloud。

如果管理员在您删除帐户时已登录，则该管理员最多保持活动状态一分钟。之后，对 Citrix Cloud 的访问将被拒绝。

> 注意：
>
> - 如果帐户中只有一个管理员，则无法删除该管理员。Citrix Cloud 要求每个客户帐户至少有一个管理员。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> - Citrix Cloud Connector 不链接到管理员帐户。因此，即使您移除了安装 Cloud Connector 的管理员，Cloud Connector 仍能继续运行。

订阅者

订阅者的身份定义其在 Citrix Cloud 中具有访问权限的服务。此身份来自从资源位置中的域提供的 Active Directory 域帐户。将某个订阅者分配给某个库服务会授权该订阅者访问该服务。

管理员可以在“域”选项卡上控制使用哪些 域 来提供这些身份。如果您计划使用来自多个林的域，请在每个林中至少安装两个 Citrix Cloud Connector。Citrix 建议至少使用两个 Citrix Cloud Connector 来维护高可用性环境。有关在 Active Directory 中部署 Cloud Connector 的更多信息，请参阅 Active Directory 中 Cloud Connector 的部署方案。

> 注意：
>
> - 禁用域将仅阻止选择新身份。不阻止订阅者使用已分配的身份。
> - 每个 Citrix Cloud Connector 都可以枚举和使用安装它的单个林中的所有域。

管理订阅者使用情况

可以使用单个帐户或 Active Directory 组向服务中添加订阅者。使用 Active Directory 组不要求在您将组分配给服务后通过 Citrix Cloud 进行管理。

管理员从服务中删除了一个订阅者或一组订阅者时，这些订阅者将无法再访问该服务。有关从特定服务中删除订阅者的详细信息，请参阅 Citrix 产品文档网站上的服务文档 。

主资源位置

主资源位置是指您为自己的域与 Citrix Cloud 之间的通信指定为“最优先选择”的资源位置。对于您的主资源位置，请选择具有 Citrix Cloud Connector 的资源位置，该连接器具有最佳性能和与域的连接。将此资源位置设为主资源位置可让您的用户快速登录到 Citrix Cloud。

有关更多信息，请参阅选择主要资源位置。

更多信息

- 通过 Citrix Training Web 站点上的 Citrix 身份和身份验证简介教育课程，了解有关支持的身份提供商的更多信息。
- Citrix Tech Zone：
  - 技术简报：Workspace 身份
  - 技术简报：Workspace 单点登录

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 技术洞察：移动 SSO

管理管理员对 **Citrix Cloud** 的访问权限

April 5, 2024

管理员是在 Citrix Cloud 控制台中进行管理的。根据用于对管理员进行身份验证的身份提供商，您可以单独添加管理员或使用组添加管理员。

登录 Citrix Cloud 时，所有管理员都必须使用令牌作为身份验证的第二个因素。添加管理员后，他们可以使用任何遵循基于时间的一次性密码 标准的应用程序（例如 Citrix SSO）在多重身份验证中注册其设备并生成令牌。

添加新管理员

Citrix Cloud 支持以下身份提供商对管理员进行身份验证：

- Citrix 身份提供商：Citrix Cloud 中的默认身份提供商。仅支持添加个人管理员。
- Azure AD：支持单独或通过 AAD 组添加管理员。AAD 组中的管理员仅限于自定义访问角色。有关详细信息，请参阅管理管理员组。
- SAML 2.0：仅支持通过 AD 组添加管理员。有关更多信息，请参阅 将 SAML 作为身份提供商连接到 Citrix Cloud

添加新管理员将使用以下工作流：

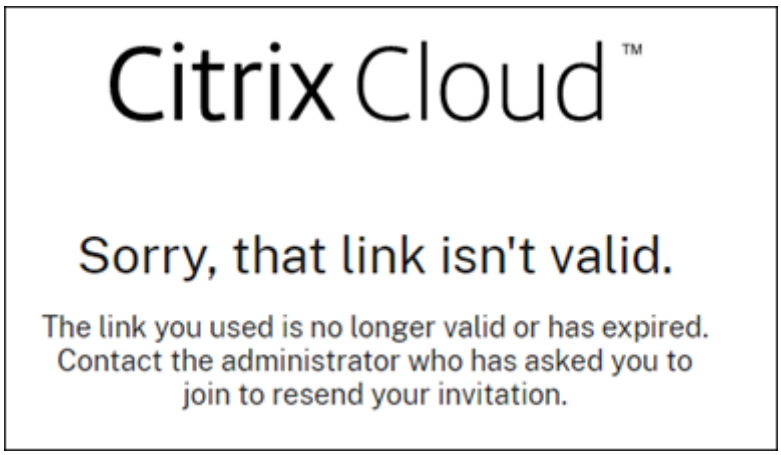
1. 选择要用于对管理员进行身份验证的身份提供商。
2. 根据身份提供商的不同，邀请单个管理员或选择管理员所属的组。
3. 指定与组织中管理员角色一致的访问权限。有关详细信息，请参阅本文中的 修改管理员权限 。

邀请个人管理员

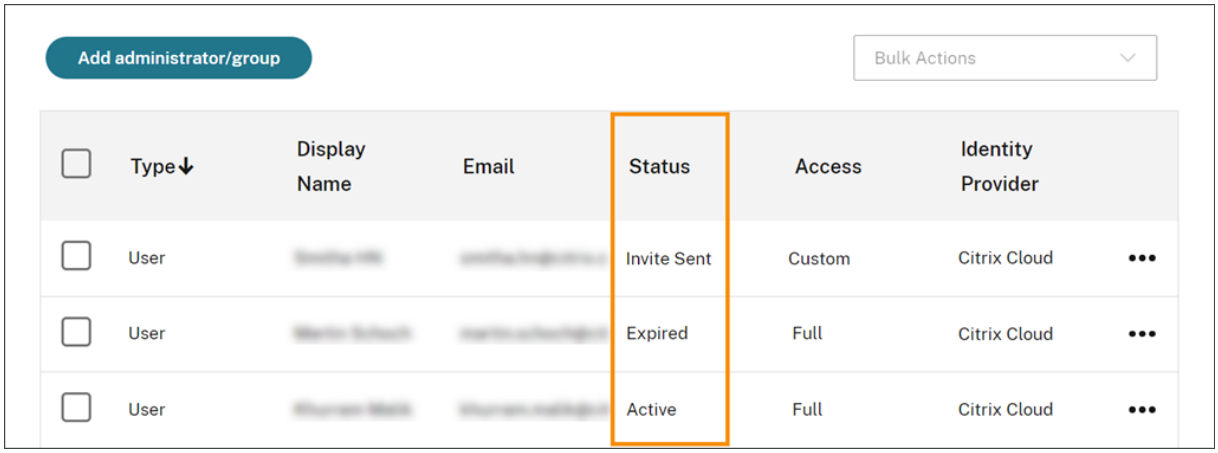
添加个人管理员需要邀请他们加入您的 Citrix Cloud 帐户。添加管理员时，Citrix 会向他们发送邀请电子邮件。管理员必须先接受邀请，然后才能登录。您通过组添加的管理员不会收到邀请，可以在添加邀请后立即登录。

邀请电子邮件从 `cloud@citrix.com` 发送，其中说明了如何访问该帐户。该邀请自您发送之日起连续五天内有效。五天过后，邀请链接将过期。如果受邀管理员使用已过期的链接，Citrix Cloud 将显示一条消息，指示该链接无效。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



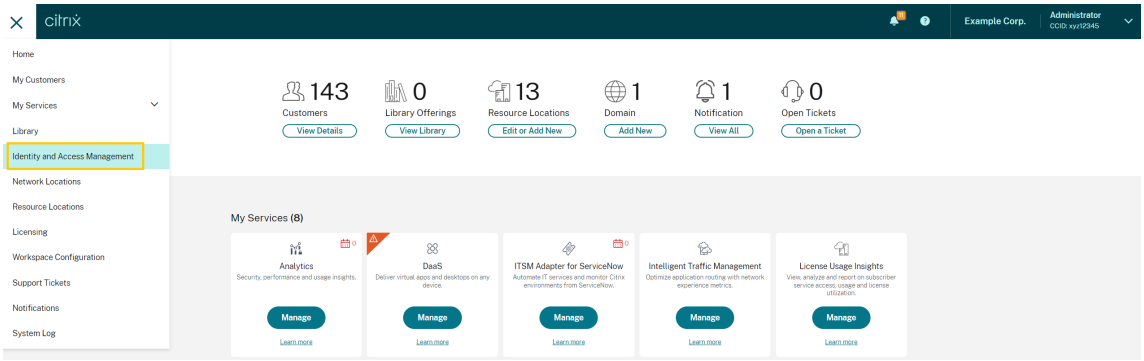
Citrix Cloud 还会显示邀请的状态，以便您可以查看管理员是否接受邀请并登录到 Citrix Cloud。



> 注意
>
> 管理员帐户可以与最多 100 个客户帐户关联。如果管理员需要管理 100 多个客户帐户，则他们必须使用不同的电子邮件地址创建一个单独的管理员帐户来管理其他客户。或者，您可以将管理员从不再需要管理的客户帐户中删除。

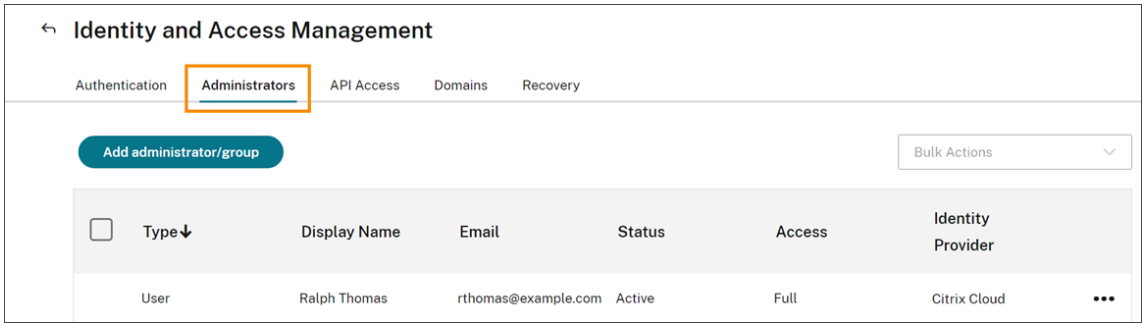
邀请管理员

1. 登录 Citrix Cloud，然后从菜单中选择身份识别和访问管理。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

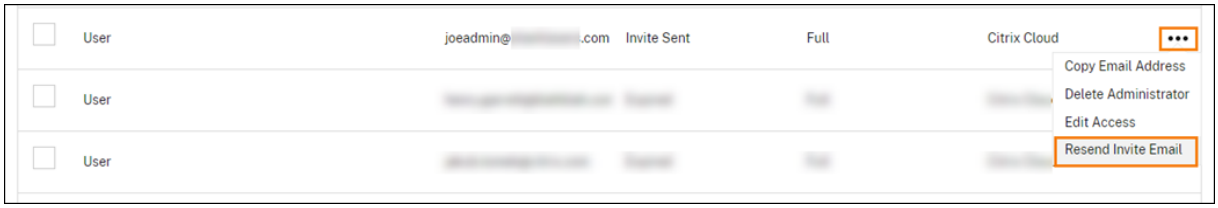
2. 在 **Identity and Access Management**（身份识别和访问管理）页面上，选择 **Administrators**（管理员）。控制台将显示帐户中当前的所有管理员。



3. 选择 添加管理员/组。
4. 在 管理员详细信息中，选择要使用的身份提供商。如果使用 Azure AD，Citrix Cloud 可能会提示您先登录。
5. 如果选择了 **Citrix Identity**，请输入用户的电子邮件地址，然后选择 下一步。
6. 如果选择了 **Azure Active Directory**，请键入要添加的用户的名称，然后单击下一步。不支持邀请 AAD 来宾用户。
7. 在 设置访问权限中，为管理员配置相应的权限。完全访问权限（默认情况下处于选中状态）允许控制所有 Citrix Cloud 功能和订阅的服务。自定义访问权限 允许控制您选择的功能和服务。
8. 查看管理员详情。选择返回进行任何更改。
9. 选择 发送邀请。Citrix Cloud 会向您指定的用户发送邀请，并将管理员添加到列表中。

重新发送邀请

要重新发送邀请，请从控制台最右侧的省略号菜单中选择重新发送邀请电子邮件。重新发送邀请不会影响邀请到期前的五天时限。



使用新的登录链接重新发送邀请

如果原始邀请电子邮件过期，您可以向管理员发送新的邀请电子邮件。请执行以下步骤：

1. 从 Citrix Cloud 中删除管理员：在管理员页面上，在列表中找到管理员，然后从省略号菜单中选择删除管理员。
2. 等待几分钟，确保 Citrix Cloud 完成删除。在某些情况下，删除后立即再次邀请管理员可能会导致发送带有错误登录链接的邀请。
3. 按照邀请管理员中所述再次邀请管理员。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

接受管理员邀请

如果您受邀加入 Citrix Cloud 帐户，Citrix 会向您发送一封电子邮件，其中包含该帐户的组织 ID 和客户名称。

要接受邀请，请单击登录。之后，将打开一个浏览器窗口。如果您还没有 Citrix Cloud 帐户，浏览器将显示一个页面，您可以在其中创建密码。如果您已有帐户，Citrix Cloud 会提示您使用现有密码登录。

登录期间，系统可能会提示您注册多重身份验证。有关注册说明，请参阅设置多重身份验证。

添加管理员组

您可以使用 AD 组（用于 SAML 身份验证）或 Azure AD 组（用于 Azure AD 身份验证）添加管理员。有关详细信息，请参阅管理管理员组。

批准加入 **Citrix Cloud** 的请求

您可能会不时收到 Citrix Cloud 代表组织中想要以管理员身份加入您的 Citrix Cloud 帐户的某人发出的批准请求。

要批准这些请求，您可以邀请请求访问权限的人员成为管理员，如本文中的邀请个人管理员中所述。您 必须使用批准请求电子邮件中显示的相同电子邮件地址。

收到邀请后，请求访问权限的人员单击“登录”链接接受邀请。然后，该人可以为 Citrix Cloud 创建密码并登录到您的帐户。

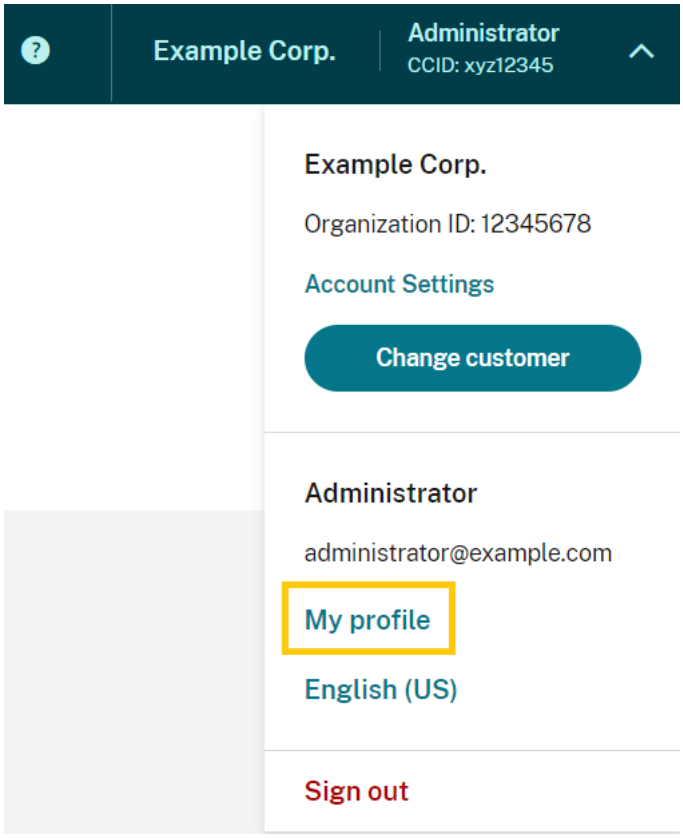
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关如何生成批准请求的更多信息，请参阅如果帐户已经在使用中会发生什么？。

更改您的电子邮件地址

您可以在 Citrix Cloud 中更改自己的电子邮件地址。您的新地址必须与多重身份验证 (MFA) 的辅助电子邮件地址不同。更改您的电子邮件地址时，Citrix Cloud 会向您发送一封验证电子邮件到新地址。验证后，Citrix Cloud 会将您注销，以便完成更改。几分钟后，您可以使用新的电子邮件地址再次登录。

1. 从右上角的菜单中选择“我的设置”。



2. 在“电子邮件地址”中，选择“更改电子邮件”。
3. 输入新的电子邮件地址，然后选择“发送验证电子邮件”。
4. 输入电子邮件中的 6 位数验证码，然后选择“验证并完成”。
5. 选择“是，更改我的电子邮件地址”以确认更改。

确认您的更改后，Citrix Cloud 会将您注销。几分钟后，您可以使用新的电子邮件地址再次登录。

修改管理员权限

将管理员添加到 Citrix Cloud 帐户时，您需要定义适合其在组织中的角色的管理员权限。默认情况下，为新管理员分配对所有 Citrix Cloud 帐户功能和可用服务的 完全访问权限。如果要限制对管理控制台的某些区域或特定服务的访问权

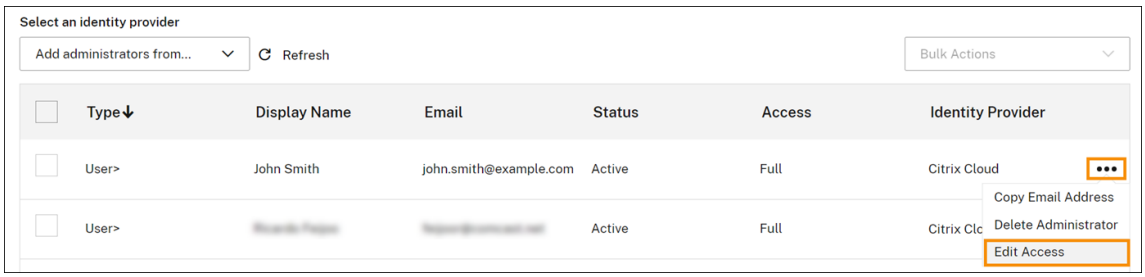
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

限，则可以定义 自定义访问权限。

只有具有完全访问权限的 Citrix Cloud 管理员才能为其他管理员定义权限。

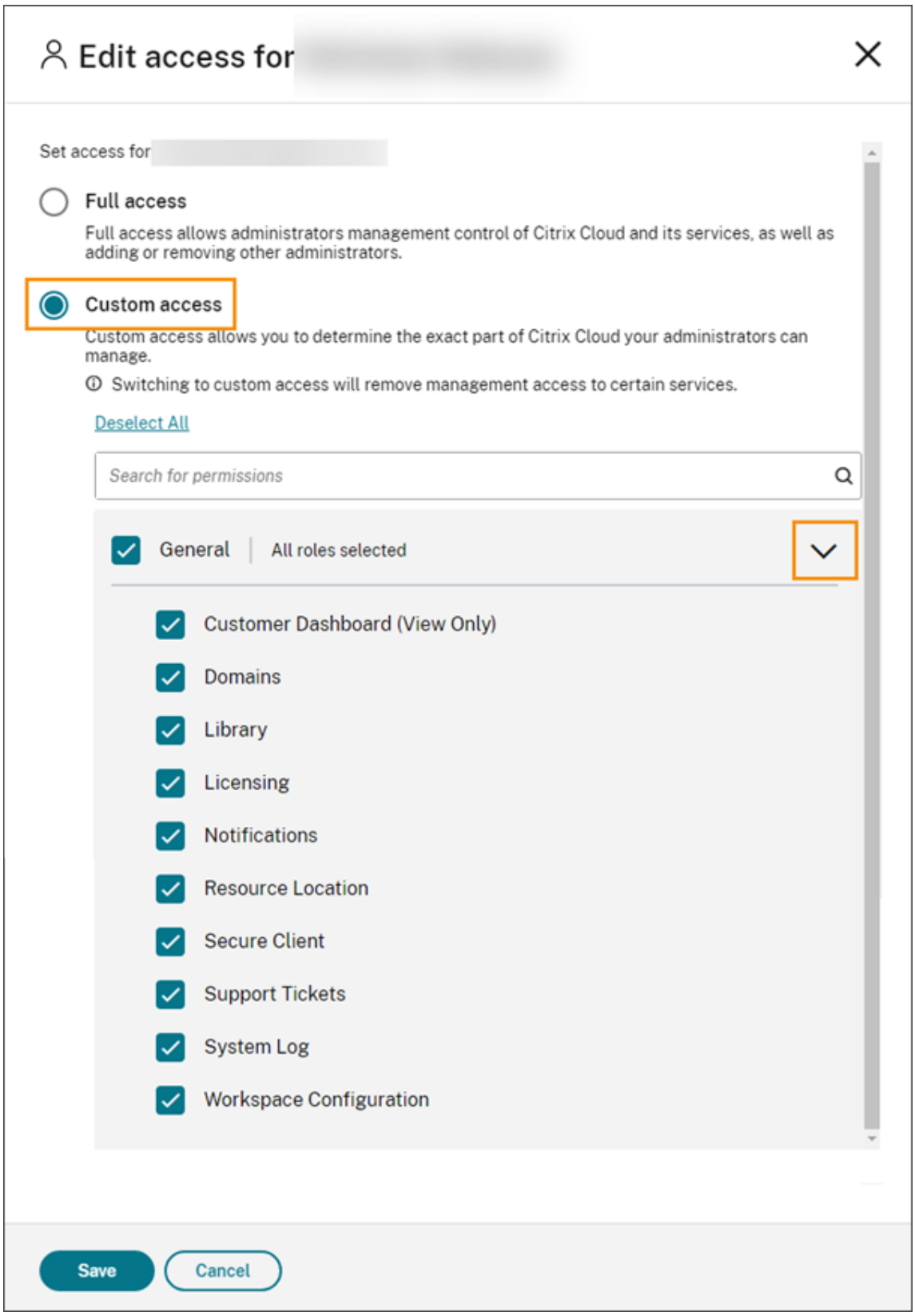
要更改现有的管理员权限，请执行以下操作：

1. 通过 https://citrix.cloud.com登录 Citrix Cloud。
2. 在 Citrix Cloud 菜单中，选择身份和访问管理，然后选择管理员。
3. 选择要管理的身份提供商：Citrix Identity（默认）、Active Directory（如果使用 SAML 作为身份提供程序）或 Azure AD（如果已连接）。
4. 找到要管理的管理员或组，单击省略号按钮，然后选择 编辑访问权限。



5. 要允许或禁止特定权限，请选择 自定义访问权限。要允许访问所有 Citrix Cloud 功能，请选择 完全访问权限。
6. 要快速找到服务权限，请开始在搜索框中键入。Citrix Cloud 会在您键入时显示匹配的权限。例如，如果您开始键入“只读”，则会显示标题中包含“只读”的权限。搜索权限不区分大小写。
7. 要定义 Citrix Cloud 管理控制台的自定义访问权限，请展开常规。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



8. 要为特定服务定义自定义访问权限，请展开该服务。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

9. 对于每种权限，请根据需要选中或取消选中复选框。
10. 选择保存。

控制台权限

本节介绍可用于 Citrix Cloud 管理控制台的自定义访问权限。有关特定服务的自定义访问权限的更多信息，请查阅该服务的文档。

- 客户控制面板（仅限查看）：仅适用于 Citrix Service Provider (CSP)。授予 客户控制面板的视图访问权限。
- 域：授予对 身份识别和访问管理 **>** 域选项卡的访问权限。管理员可以通过从此选项卡下载 Citrix Cloud Connector 软件并将其安装在域中的服务器上来添加 Active Directory 域。
- 库：授予对 库 控制台页面的访问权限。根据管理员有权访问的服务，管理员可以将 Citrix DaaS 交付组分配给用户，从 Endpoint Management 添加 Intune 托管应用程序，或者允许只读管理员查看 Secure Private Access 的应用程序详细信息。
- 许可：授予对许可控制台页面的云服务和许可部署选项卡的访问权限。
- 通知：授予对 通知 控制台页面的访问权限。管理员可以查看和关闭 Citrix Cloud 通知。
- 资源位置：授予对 资源位置 控制台页面的访问权限。管理员可以 为 Citrix Workspace 单点登录添加新的资源位置和添加 FAS 服务器。他们还可以管理连接器更新。
- 安全客户端：授予对 身份识别和访问管理 **> API** 访问 **>** 安全客户端 选项卡的访问权限。管理员可以创建和管理自己的安全客户端，以便与 Citrix Cloud API配合使用。此权限不包括对 身份识别和访问管理 **> API** 访问 **>** 产品注册选项卡的访问权限。只有完全访问权限的管理员才能访问产品注册选项卡。
- 支持票据：授予访问支持票据控制台菜单选项和打开票据帮助菜单选项的访问权限。选择这两个选项中的任何一个都会将管理员发送到“我的支持”门户。有关更多信息，请参阅技术支持。
- 系统日志：授予访问系统日志控制台页面的权限。管理员可以 查看系统日志事件 并将事件导出到 CSV 文件。
- **Workspace** 配置：授予对 **Workspace** 配置控制台页面的访问权限。管理员可以更改身份验证方法、自定义 Workspace 外观和行为、启用和禁用服务以及配置站点聚合。有关更多信息，请参阅 Citrix Workspace 产品文档。
- **Workspace OAuth** 客户端（预览版）：授予对身份和访问管理 **> API** 访问权限 **> Workspace API** 选项卡的访问权限。管理员可以创建和管理自己的 OAuth 客户端，以便与 Citrix Workspace 平台 API 进行交互。OAuth 客户端仅用于 Workspace API，包括创建自动过期的专用客户端的选项。

> 注意：
>
> 建议谨慎分配 **Workspace OAuth** 客户端自定义角色。与此角色相关的访问权限可能使管理员能够在 Workspace 平台上访问最终用户的资源（VDA 或应用程序）。还需要注意的是，具有完全访问权限的管理员将自动获得等同于拥有 **Workspace OAuth** 客户端权限的管理员的访问权限。

管理您的主要 **MFA** 方法

要使用多重身份验证 (MFA) 登录 Citrix Cloud，您可以使用身份验证器应用程序，也可以使用您的电子邮件地址。本节介绍如何更改 MFA 的设备注册或切换到其他 MFA 方法。

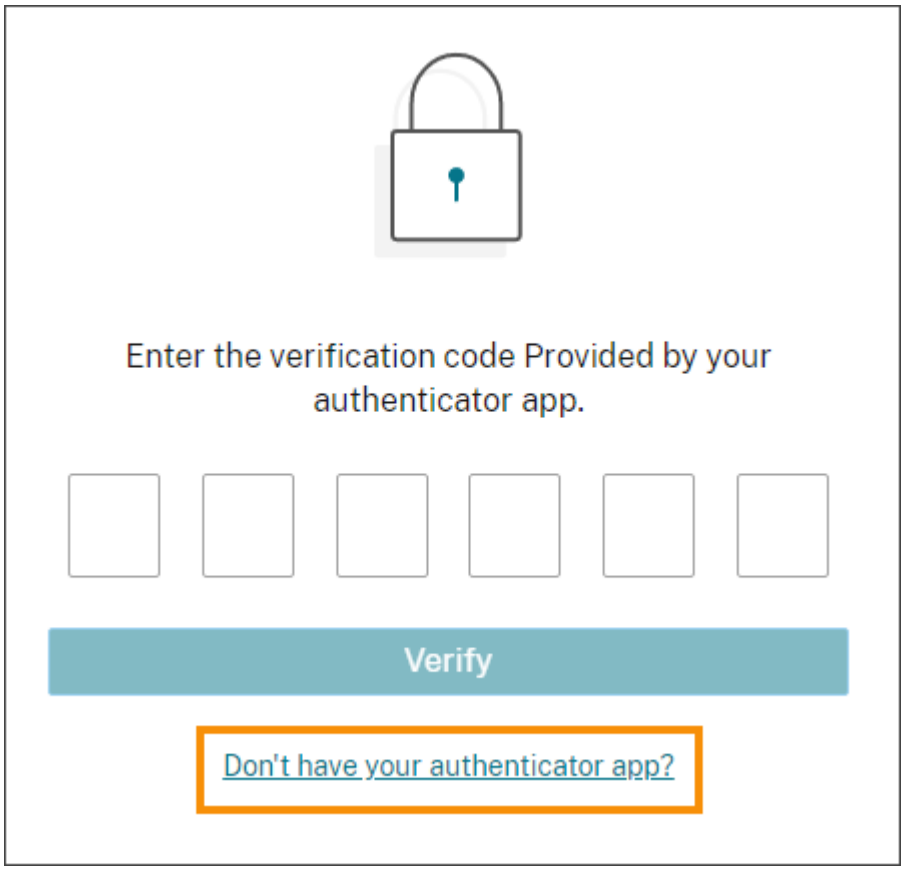
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将您的设备更改为 **MFA**

如果您丢失了已注册的设备、想要在 Citrix Cloud 上使用其他设备或重置身份验证器应用程序，则可以在 Citrix Cloud MFA 中重新注册。

> 备注
>
> - 更改设备会删除当前设备注册并生成新的身份验证器应用程序密钥。
> - 如果您要使用与原始注册相同的身份验证器应用程序重新注册，请在重新注册之前从身份验证器应用程序中删除 Citrix Cloud 条目。完成重新注册后，此条目中显示的代码将不再起作用。如果您未在重新注册之前或之后删除此条目，则身份验证器应用程序会显示两个 Citrix Cloud 条目，代码不同，这可能会在登录 Citrix Cloud 时造成混淆。
> - 如果您要使用新设备重新注册，但没有身份验证器应用程序，请从设备的应用商店下载并安装一个。为了获得更流畅的体验，Citrix 建议在重新注册设备之前安装身份验证器应用程序。

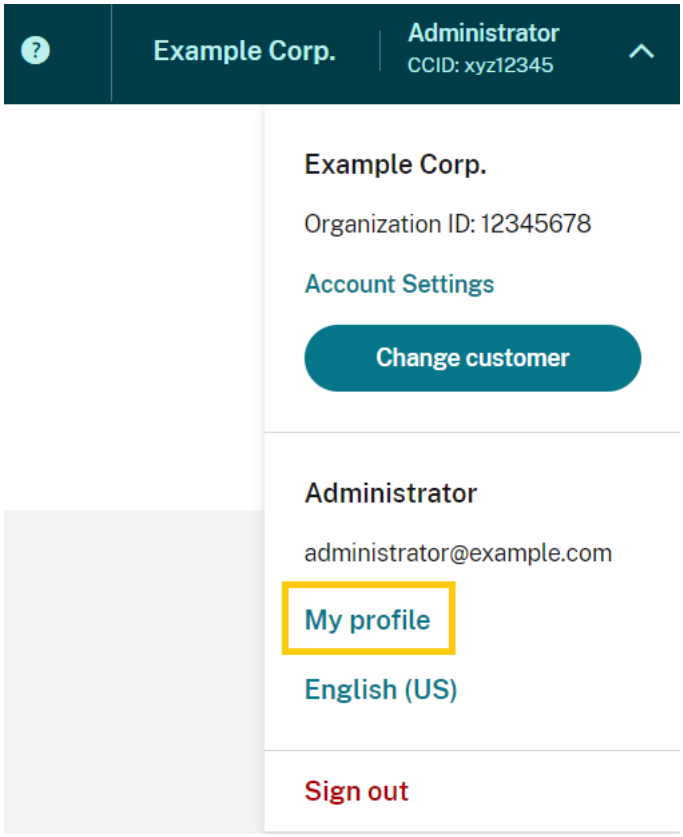
1. 登录 Citrix Cloud 并输入身份验证器应用程序中的代码。



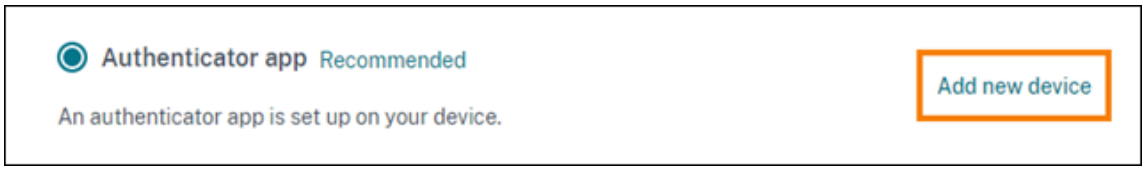
   如果您没有身份验证器应用程序，请点击 没有身份验证器应用程序？并选择一种恢复方法来帮助您登录。根据选择的恢复方法，输入您收到的恢复代码或未使用的备份代码，然后选择 验证。

2. 如果您是多个客户组织的管理员，请选择任何客户组织。
3. 从右上角的菜单中选择“我的设置”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 在 身份验证器应用程序中，选择 添加新设备。



5. 当系统提示您确认更改设备时，选择“是，更改我的设备”。
6. 通过输入身份验证器应用程序中的验证码来验证您的身份。如果您没有身份验证器应用程序，请选择 使用恢复方法 使用您选择的恢复方法来验证您的身份。根据您选择的恢复方法，输入您收到的验证码或恢复码或未使用的备用代码。选择验证并继续。
7. 如果您使用的是最初注册的设备和原始身份验证器应用程序，请从身份验证器应用程序中删除现有 Citrix Cloud 条目。
8. 如果您正在注册新设备，但没有身份验证器应用程序，请从设备的应用商店下载一个。
9. 在身份验证器应用程序中，使用设备扫描 QR 代码或手动输入密钥。
10. 从您的身份验证器应用程序中输入 6 位数的验证码，然后选择 验证码。

更换设备后，Citrix 强烈建议您检查“我的个人资料”页面中的验证方法是否为最新。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更改您的 **MFA** 方法

如果您使用身份验证器应用程序注册了 MFA 并想切换到使用您的电子邮件地址，请注意，更改身份验证方法会删除您的设备注册。如果您想重新使用身份验证器应用程序进行 MFA，则需要重新注册您的设备。

1. 从 Citrix Cloud 控制台的右上角菜单中，选择我的设置。
2. 在 多重身份验证 **(MFA)** 下，选择要切换到的身份验证方法。
3. 如果切换到电子邮件 MFA：

    a) 选择“是，更改为电子邮件”以确认您要更改 MFA 方法。
    b) 输入身份验证器应用程序中的验证码或使用恢复方法确认您的身份。
    c) 选择验证并继续完成更改。

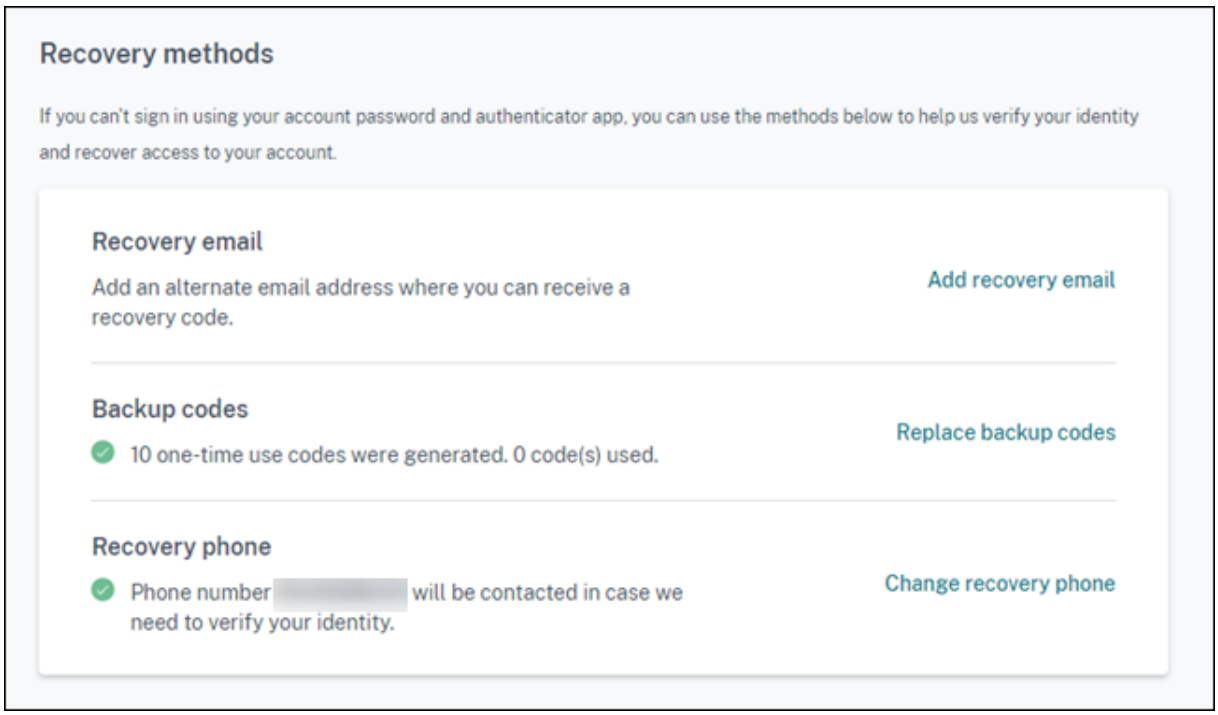
4. 如果切换到身份验证器应用程序：

    a) 出现提示时，输入 Citrix Cloud 发送到您的电子邮件地址的验证码，然后选择验证并继续。或者，使用恢复方法确认您的身份。
    b) 使用身份验证器应用程序，使用设备的摄像头扫描 QR 代码或输入字母数字密钥。
    c) 在“验证您的身份验证器应用程序”下，输入身份验证器应用程序中的 6 位数代码。
    d) 单击“验证码”以完成设备注册。

管理您的 **MFA** 恢复方法

> 重要：
>
> 为确保您的 Citrix Cloud 帐户保持安全，请使用准确的信息使您的验证方法保持最新。如果您无法访问身份验证器应用程序或 MFA 电子邮件地址，则这些验证方法是恢复帐户访问权限的唯一方法。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



添加或更改您的辅助邮箱

1. 从右上角的菜单中选择“我的设置”。
2. 如果您尚未添加辅助电子邮件地址，请在恢复方法下的恢复电子邮件中，选择添加辅助电子邮件。如果您已添加辅助电子邮件地址，请选择更改辅助邮箱。
3. 出现提示时，输入身份验证器应用程序中的验证码或发送到您的电子邮件地址的验证码。
4. 输入您要使用的新电子邮件地址，然后选择 发送验证电子邮件。此电子邮件地址必须与您用于 Citrix Cloud 帐户的电子邮件地址不同。Citrix Cloud 向您输入的电子邮件地址发送一封验证电子邮件。
5. 输入验证电子邮件中的代码，然后单击“验证码并完成”。

生成新的备用码

您可以随时生成一组新的备用代码。使用备份代码时，Citrix Cloud 会记录已在“我的个人资料”页面中使用的号码。

生成新的备用代码后，请务必将它们存储在安全的地方。

1. 从右上角的菜单中选择“我的设置”。
2. 如果您之前没有生成过备份代码，请在恢复方法下的备份代码中选择生成新的备份代码。如果您之前生成了备用代码，请选择“替换备用代码”。
3. 当系统提示您替换备用代码时，选择“是，替换我的密码”。
4. 通过输入身份验证器应用程序中的验证码或发送到您的电子邮件地址的验证码来验证您的身份。
5. 选择验证并继续。Citrix Cloud 生成并显示一组新的备份代码。
6. 选择 下载代码 将新代码下载为文本文件。然后，选择“我已存储我的备用代码”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. 选择“我已存储我的备用代码”以完成替换您的备用代码。

更改您的辅助电话号码

1. 从右上角的菜单中选择“我的设置”。
2. 在“恢复方法”下的“恢复电话”中，选择“更改辅助电话”。
3. 输入身份验证器应用程序中的验证码或发送到您的电子邮件地址的验证码。选择验证并继续。
4. 输入您要使用的新电话号码。然后，重新输入电话号码进行确认。
5. 选择“保存备用电话号码”。

> 注意：
>
> 只有在 Citrix Endpoint Management (CEM) 管理员接受管理员邀请并单击 CEM 磁贴上的 管理 后，才能修改管理员的权限。与所有 Citrix Cloud 管理员一样，默认情况下，CEM 管理员具有完全访问权限。

管理管理员组

February 16, 2024

您可以使用 Active Directory、Azure Active Directory (AD) 或 Google Cloud Identity 中的组将管理员添加到 Citrix Cloud 帐户。然后，您可以管理组中所有管理员的服务访问权限。

AD 必备条件

Citrix Cloud 支持通过 SAML 2.0 进行 AD 组身份验证。在将 AD 管理员组的成员添加到 Citrix Cloud 之前，您需要配置 Citrix Cloud 和 SAML 提供商之间的连接。有关更多信息，请参阅 将 SAML 作为身份提供程序连接到 Citrix Cloud。

如果您在 Citrix Cloud 中已有 SAML 连接，则在添加 AD 管理员组之前，必须将 SAML 提供程序重新连接到 Citrix Cloud。如果不重新连接 SAML，添加 AD 管理员组可能会失败。有关更多信息，请参阅 使用现有 SAML 连接进行管理员身份验证。

Azure AD 必备

使用 Azure AD 组身份验证需要最新版本的 Azure AD 应用程序才能将 Azure AD 连接到 Citrix Cloud。Citrix Cloud 在您首次连接 Azure AD 时获得了此应用程序。如果您在 2019 年 5 月之前将 Azure AD 连接到 Citrix Cloud，则 Citrix Cloud 可能没有使用最新的应用程序与 Azure AD 进行连接。如果您的帐户未使用最新的应用程序，Citrix Cloud 将无法显示您的 Azure AD 组。

在 Citrix Cloud 中使用 Azure AD 组之前，请执行以下任务：

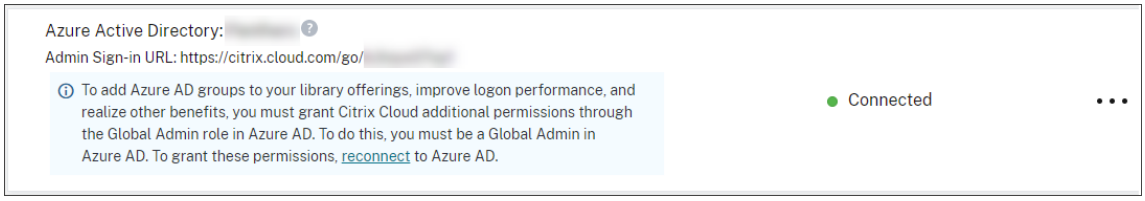
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 验证您使用的是最新的 Azure AD 连接应用程序。如果您未使用最新的应用程序，Citrix Cloud 将显示一条通知。
2. 如果必须更新应用程序，请将您的 Azure AD 重新连接到 Citrix Cloud。通过重新连接到 Azure AD，可以向 Citrix Cloud 授予应用程序级只读权限，并允许 Citrix Cloud 代表您重新连接到您的 Azure AD。在重新连接期间，将显示这些权限的列表供您查看。有关 Citrix Cloud 请求的权限的更多信息，请参阅适用于 Citrix Cloud 的 Azure Active Directory 权限。

   > 重要提示：
   >
   > 要完成此任务，您必须是 Azure AD 中的全局管理员。此外，您必须使用 Citrix 身份提供商下的完全访问管理员帐户登录 Citrix Cloud。如果使用 Azure AD 凭据登录，重新连接将失败。如果您没有任何管理员在使用 Citrix 身份提供程序，则可以临时添加一个管理员来执行此任务，然后再将其删除。

验证您与 **Azure AD** 的连接

1. 使用 Citrix 身份提供商下的完全访问管理员帐户登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 身份识别和访问管理，然后选择 身份验证。
3. 找到 **Azure Active Directory**。如果 Citrix Cloud 必须为您的 Azure AD 连接更新应用程序，则会显示一条通知。

   如果 Citrix Cloud 已在使用最新的应用程序，则不会显示任何通知。

重新连接到 **Azure AD**

1. 在 Citrix Cloud 控制台中的 Azure AD 通知中，单击 重新连接 链接。此时将显示所请求的 Azure 权限的列表。
2. 查看权限，然后选择 接受。

Google Cloud Identity

Citrix Cloud 支持通过 Google Cloud Identity 验证管理员组。在将管理员组添加到 Citrix Cloud 之前，必须配置 Citrix Cloud 和 Google Cloud Identity 之间的连接。有关更多信息，请参阅将 Google Cloud Identity 作为身份提供商连接到 Citrix Cloud。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

支持的服务

以下服务支持管理员组的自定义访问权限：

- Citrix Analytics
- NetScaler 控制台
- Citrix DaaS
- Workspace Environment Management 服务
- 许可证使用情况见解

支持的权限

您只能为 Citrix Cloud 平台的支持服务和某些功能分配自定义访问权限。不支持完全访问权限。

对于 Citrix Cloud 平台功能，支持以下自定义访问权限：

- 域
- 许可
- 资源位置
- 支持票据
- 系统日志
- Workspace 配置

有关这些权限的更多信息，请参阅控制台权限。

管理员组无权访问任何其他服务。他们只能管理他们有权访问的受支持服务。

已登录的管理员组成员的权限更改只有在注销并再次登录后才会生效。

拥有 **Citrix**、**AD**、**Azure AD** 和 **Google Cloud** 身份的管理员的相应权限

管理员登录 Citrix Cloud 时，如果管理员同时拥有 Citrix 身份（Citrix Cloud 中的默认身份提供商）和通过 AD、Azure AD 或 Google Cloud Identity 拥有单用户或基于组的身份，则只有某些权限才可用。本节中的表格描述了这些身份的每种组合可用的权限。

_ 单用户身份 _ 是指通过个人帐户授予管理员的 AD、Azure AD 或 Google Cloud Identity 权限。_ 基于组的身份 _ 是指作为组成员授予的 AD、Azure AD 或 Google Cloud Identity 权限。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 身份	单用户 AD 或 Azure AD 标识	基于组的 AD 或 Azure AD 标识	基于单用户或组的 Google Cloud Identity	身份验证后可用的权限
X	X			成功使用 Citrix 身份、AD 身份或 Azure AD 身份进行身份验证后，管理员拥有两个身份的累积权限。
X		X		每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是 Azure AD 身份进行身份验证。
X			X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是使用 Google Cloud 身份进行身份验证。
	X	X		使用 AD 或 Azure AD 向 Citrix Cloud 进行身份验证时，管理员拥有两个身份的累积权限。
	X		X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是使用 Google Cloud 身份进行身份验证。
		X	X	每个身份都被视为一个独立的实体。可用权限取决于管理员是使用 Citrix 身份还是使用 Google Cloud 身份进行身份验证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

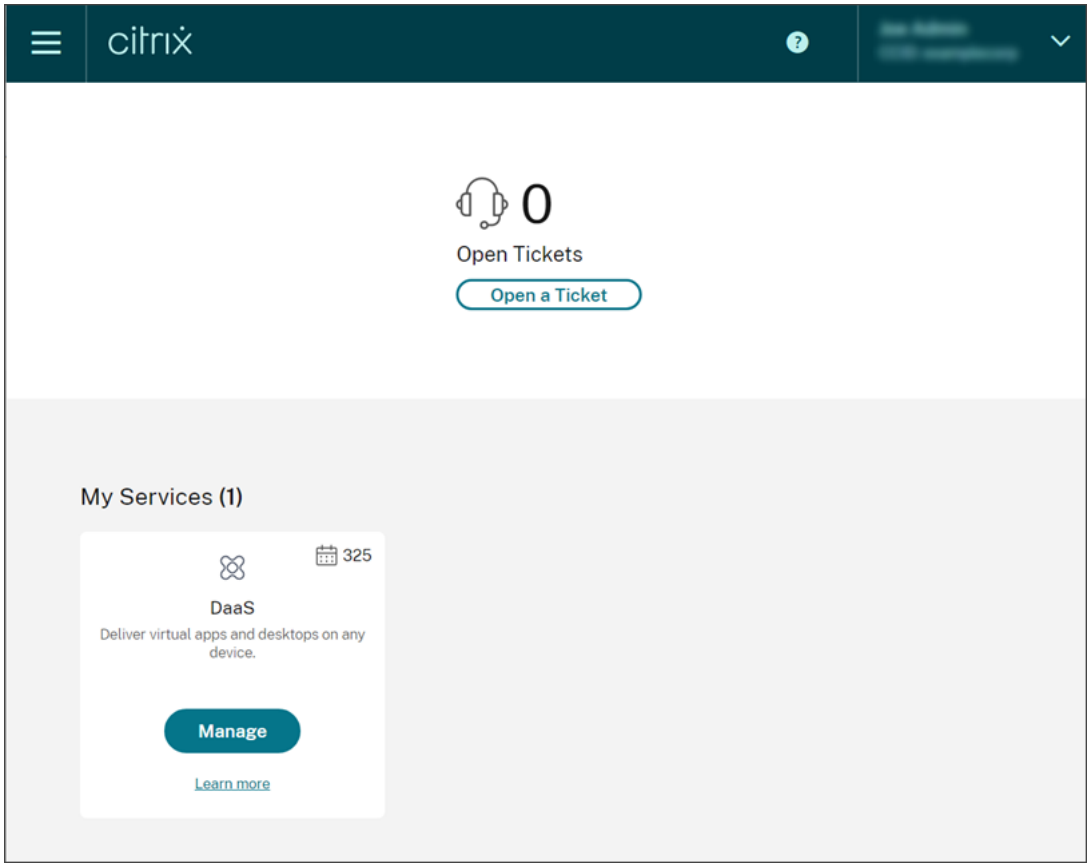
Citrix 身份	单用户 AD 或 Azure AD 标识	基于组的 AD 或 Azure AD 标识	基于单用户或组的 Google Cloud Identity	身份验证后可用的权限
X	X	X		使用其 Citrix 身份进行身份验证时，管理员拥有 Citrix 身份和单用户 Azure AD 身份的累积权限。使用 Azure AD 进行身份验证时，管理员拥有所有三个身份的累积权限。

管理员的登录体验

将组添加到 Citrix Cloud 并定义服务权限后，组中的管理员只需在 Citrix Cloud 登录页面上选择“使用我的公司凭据登录”，然后输入帐户的登录 URL（例如 `https://citrix.cloud.com/go/mycompany`）即可登录。与添加个人管理员不同，组中的管理员不会被明确邀请，因此他们不会收到任何接受成为 Citrix Cloud 管理员邀请的电子邮件。

登录后，管理员从服务磁贴中选择 管理 以访问服务的管理控制台。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



仅作为组成员被授予权限的管理员可以使用 Citrix Cloud 帐户的登录 URL 访问 Citrix Cloud 帐户。

通过个人帐户授予权限并作为组成员的管理员可以选择他们要访问的 Citrix Cloud 帐户。如果管理员是多个 Citrix Cloud 帐户的成员，则可以在成功进行身份验证后从客户选取器中选择一个 Citrix Cloud 帐户。

限制

访问平台和服务功能

管理员组成员不可使用以下 Citrix Cloud 平台功能的自定义访问权限：

- 图书馆
- 通知
- 安全客户端

有关可用权限的更多信息，请参阅本文中的支持的权限。

依赖于 Citrix Cloud 平台功能的 Citrix DaaS 功能（例如快速部署用户分配）不可用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

多个组对应用程序性能的影响

Citrix 建议单个管理员所属的组不超过 20 个，这些组已添加到 Citrix Cloud 中。如果组数量较多，则可能导致应用程序性能降低。

多个组对身份验证的影响

如果将基于组的管理员分配给 AD 或 Azure AD 中的多个组，则身份验证可能会失败，因为组的数量太大。出现此问题的原因是 Citrix Cloud 与 AD 和 Azure AD 的集成存在限制。当管理员尝试登录时，Citrix Cloud 会尝试压缩检索的组数。如果 Citrix Cloud 无法成功应用压缩，则无法检索所有组，并且身份验证将失败。

此问题还可能影响通过 AD 或 Azure AD 向 Citrix Workspace 进行身份验证的用户。如果用户属于多个组，则身份验证可能会失败，因为组的数量太大。

要解决此问题，请查看管理员或用户帐户，并验证他们是否仅属于其在组织中的角色所必需的组。

由于分配的角色/作用域对过多，添加组失败

添加具有多个角色/作用域对的组时，可能会出现错误，指示无法创建该组。出现此错误的原因是分配给该组的角色/作用域对的数量过大。要解决此错误，请在两个或多个组之间划分角色/作用域对，然后将管理员分配到这些组。

向 **Citrix Cloud** 添加管理员组

1. 在 Citrix Cloud 菜单中，选择身份和访问管理，然后选择管理员。
2. 选择 添加管理员/组。
3. 在 管理员详细信息中，选择要使用的身份提供商。如果选择了 Azure AD，请根据需要登录到您的 Azure。选择下一步。
4. 如果需要，请选择要使用的域。
5. 搜索要添加的组，然后选择该组。
6. 在 设置访问权限中，选择要分配给组的角色。必须至少选择一个角色。
7. 完成后，选择“保存”。

修改管理员组的服务权限

1. 在 Citrix Cloud 菜单中，选择身份和访问管理，然后选择管理员。
2. 找到要管理的管理员组，然后从省略号菜单中选择 编辑访问权限。

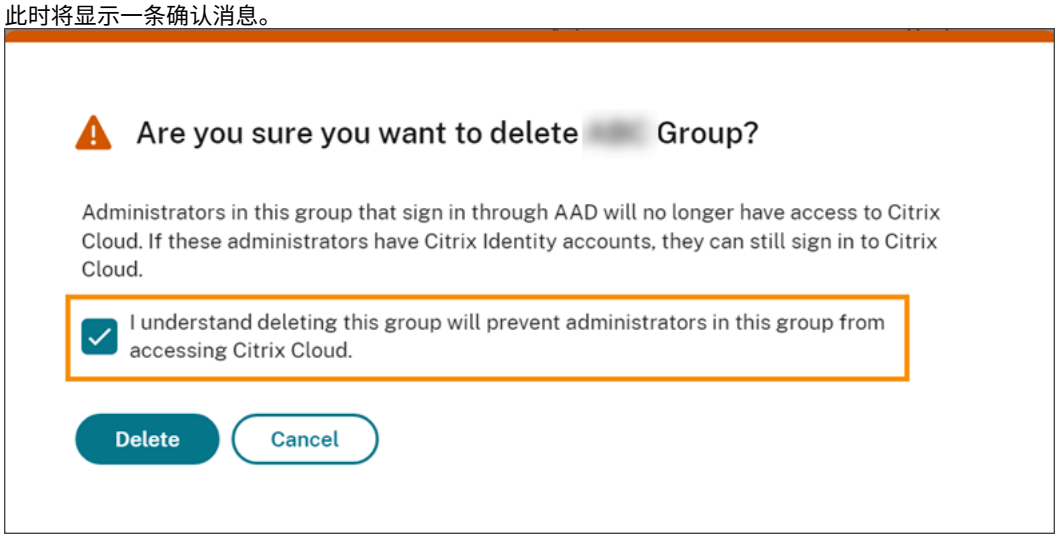
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 根据需要选择或清除一个或多个角色和作用域对旁边的复选标记。
4. 完成后，选择“保存”。

删除管理员组

1. 在 Citrix Cloud 菜单中，选择身份和访问管理，然后选择管理员。
2. 找到要管理的管理员组，然后从省略号菜单中选择 删除组。

此时将显示一条确认消息。



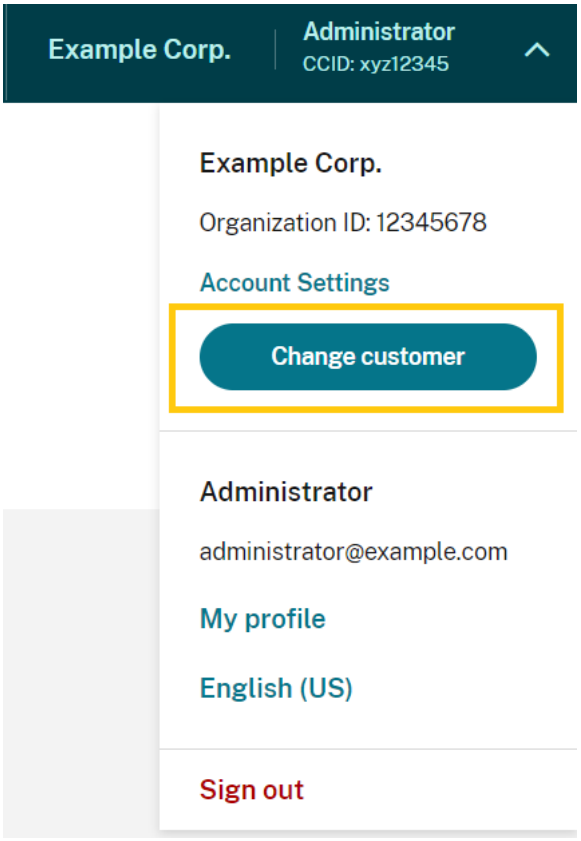
3. 选择 我明白删除此组将阻止该组中的管理员访问 **Citrix Cloud**。以确认您已意识到删除该组的后果。
4. 选择删除。

在多个 **Citrix Cloud** 帐户之间切换

> 注意：
>
> 本节介绍仅影响 Azure AD 管理员组成员的方案。

默认情况下，Azure AD 管理员组的成员无法在他们可以访问的其他 Citrix Cloud 帐户之间切换。对于这些管理员，下图所示的“更改客户”选项不会显示在 Citrix Cloud 用户菜单中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

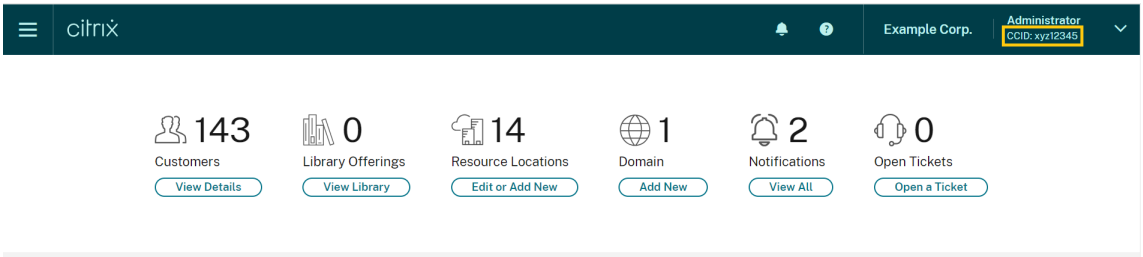


要启用此菜单选项并允许 Azure AD 组成员在其他 Citrix Cloud 帐户之间切换，必须关联要在其中进行更改的帐户。

关联 Citrix Cloud 帐户涉及一种中心辐射式方法。在关联帐户之前，请确定哪个 Citrix Cloud 帐户将用作访问其他帐户的帐户（“中心”），以及要在客户选取器中列出哪些帐户（“分支”）。

在关联帐户之前，请确保您满足以下要求：

- 您在 Citrix Cloud 中拥有完全访问权限。
- 您可以访问 Windows PowerShell 集成脚本环境 (ISE)。
- 您拥有要关联的 Citrix Cloud 帐户的客户 ID。客户 ID 显示在每个帐户的管理控制台右上角。



- 您拥有要作为中心帐户关联的 Citrix Cloud 帐户的 Citrix CWSAuth 不记名令牌。要检索此不记名令牌，请按照 CTX330675中的说明进行操作。在关联 Citrix Cloud 帐户时，您需要提供此信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

关联 **Citrix Cloud** 帐户

1. 打开 PowerShell ISE 并将以下脚本粘贴到工作窗格中：

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
20 <!--NeedCopy-->
```

2. 在第 4 行中，将 `CWSAuth bearer=XXXXXXX` 替换为您的 CWSAuth 值（例如 `CWSAuth bearer=AbCdef123Ghik…`）。此值是一个类似于证书密钥的长散列。
3. 在第 6 行，`HubCustomerID` 替换为 Hub 帐户的客户 ID。
4. 在第 9 行，`SpokeCustomerID` 替换为分支帐户的客户 ID。
5. 运行脚本。
6. 重复步骤 3-5，将其他帐户关联为分支帐户。

取消关联 **Citrix Cloud** 帐户

1. 打开 PowerShell ISE。如果 PowerShell ISE 已经打开，请清除工作窗格。
2. 将以下脚本粘贴到工作窗格中：

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
     SpokeCustomerID"
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
12 <!--NeedCopy-->
```

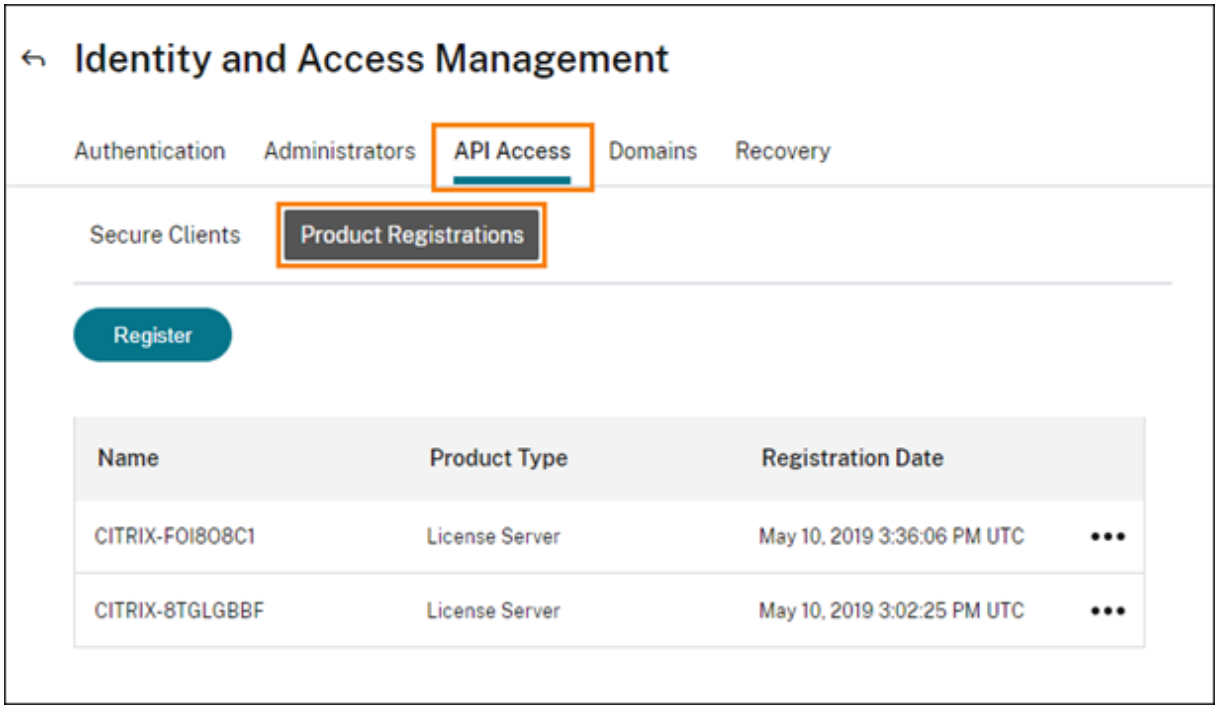
3. 在第 4 行中，将 `CWSAuth bearer=xxxxxxx1` 替换为您的 CWSAuth 值（例如 `CWSAuth bearer=AbCdef123Ghik…`）。此值是一个类似于证书密钥的长散列。
4. 在第 6 行，`HubCustomerID` 替换为 Hub 帐户的客户 ID。
5. 在第 6 行，`SpokeCustomerID` 替换为分支帐户的客户 ID。
6. 运行脚本。
7. 重复步骤 4-6 以解除其他帐户的关联。

在 **Citrix Cloud** 中注册本地产品

October 5, 2023

您可以通过 Citrix Cloud 使用短码激活轻松注册本地 Citrix 产品。这个 8 位代码可能会在产品安装过程中或运行产品的管理控制台时生成，具体取决于您的产品。当产品提示您注册时，产品会从 Citrix Cloud 请求代码并显示该代码。然后，您可以复制并粘贴此代码，或者在 Citrix Cloud 中手动输入该代码。

注册后，产品注册页面（身份和访问管理 **> API** 访问 **>** 产品注册）将显示注册产品所在的服务器。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

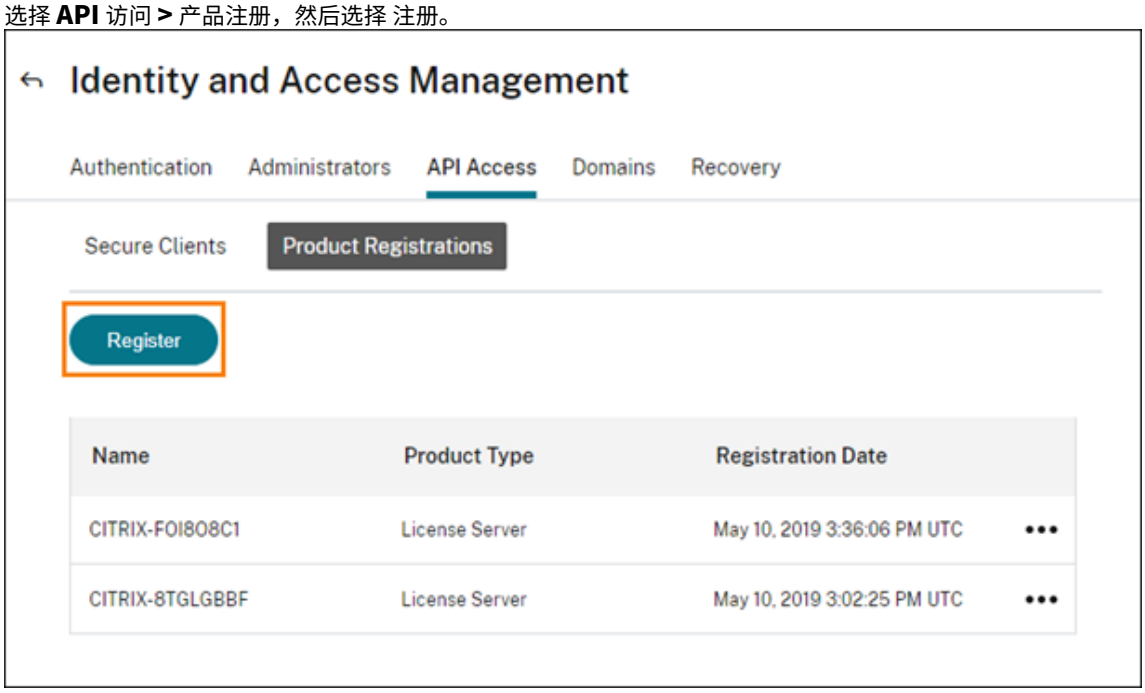
您可以在 Citrix Cloud 注册的本地产品包括：

- 适用于云服务的 Citrix 连接器设备
- Citrix 联合身份验证服务
- Citrix 许可证服务器
- Citrix Virtual Apps and Desktops，向 Citrix Analytics for Performance 注册站点时

> 注意：
>
> 本文介绍了向 Citrix Cloud 注册本地产品的步骤。有关产品的特定要求，请参阅该产品的文档。

注册产品

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份识别和访问管理）。
2. 选择 **API** 访问 **>** 产品注册，然后选择 注册。



3. 输入 Citrix 产品的 8 个字符的字母数字代码，然后单击“继续”。
4. 查看注册详细信息，然后单击注册。

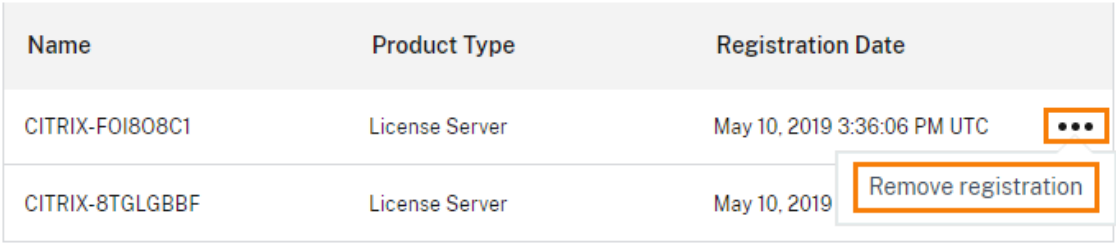
移除产品注册

如果从环境中移除运行已注册 Citrix 产品的服务器，“产品注册”页面仍会显示这些服务器。使用以下步骤从 Citrix Cloud 中删除服务器。如果需要，您可以稍后再次注册该产品，以便在“产品注册”页面上显示服务器。

1. 在“产品注册”页面中，找到要移除的服务器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 单击省略号按钮，然后选择 移除注册。



3. 出现提示时，选择移除。

将 **Active Directory** 连接到 **Citrix Cloud**

July 1, 2024

Citrix Cloud 支持使用本地 Active Directory (AD) 对工作区订阅者进行身份验证。此外，某些工作区身份验证方法需要在 AD 和 Citrix Cloud 之间建立连接。有关更多信息，请参阅 选择或更改身份验证方法。

Citrix Cloud 还支持使用令牌作为第二个身份验证因素，供订阅者通过 Active Directory 登录其工作区。Workspace 订阅者可以使用任何遵循 基于时间的一次性密码 标准的应用程序（例如 Citrix SSO）生成令牌。

有关使用 Active Directory 加令牌对工作空间订阅者进行身份验证的更多信息，请参阅 Active Directory 加令牌。

> 提示：
>
> 通过 Citrix 身份和身份验证简介教育课程，详细了解受支持的身份 提供商。“规划 Citrix 身份和访问管理”模块包括一些简短的视频，这些视频将引导您完成将此身份提供商连接到 Citrix Cloud 以及为 Citrix Workspace 启用身份验证的过程。

连接 **Active Directory**

将 Active Directory 连接到 Citrix Cloud 需要在域中安装连接器。您可以选择使用 Cloud Connector 或连接器设备作为 Active Directory 的连接器。要为您的环境选择要使用的连接器类型，请参阅以下文章：

- Active Directory 中 Cloud Connector 的部署方案
- Active Directory 中连接器设备的部署方案

通过连接器设备连接 **Active Directory**

您可以使用连接器设备将资源位置连接到不包含 Citrix Virtual Apps and Desktops 资源的林。例如，对于某些林仅用于用户身份验证的 Citrix Secure Private Access 客户或 Citrix Virtual Apps and Desktops 客户。

有关详细信息，请参阅 带连接器设备的 Active Directory

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

通过 **Cloud Connector** 连接 **Active Directory**

至少需要两个 Cloud Connector 才能确保与 Citrix Cloud 的高可用性连接。有关详细信息，请参阅以下文章：

- Cloud Connector 技术详情：有关系统要求和部署建议。
- Cloud Connector 安装：有关使用图形界面或命令行的安装说明。

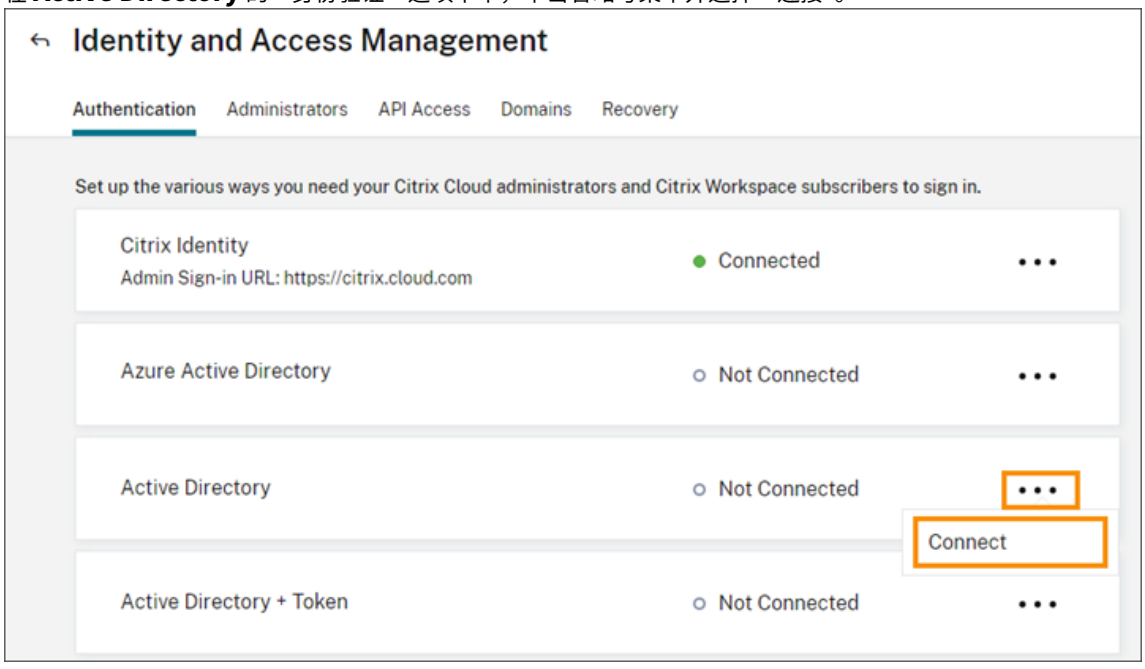
将 Active Directory 连接到 Citrix Cloud 涉及以下任务：

1. 在您的域中安装 Cloud Connector。Citrix 建议安装两个 Cloud Connector 以实现高可用性。
2. 如果适用，请为用户设备启用令牌。订阅者一次只能注册一台设备。

> 重要：
>
> 如果您正在部署 Cloud Connector 以用于 Citrix DaaS，则可能需要采取其他步骤来确保您的 AD 域在部署 Cloud Connector 后注册并处于活动状态。在 Citrix Cloud 中验证您的 AD 域是否处于活动状态可确保计算机目录设置顺利进行。有关 Citrix DaaS 部署后步骤的更多信息，请参阅 Citrix DaaS 产品文档中的在 Citrix Cloud 中添加资源类型或激活未使用的域。

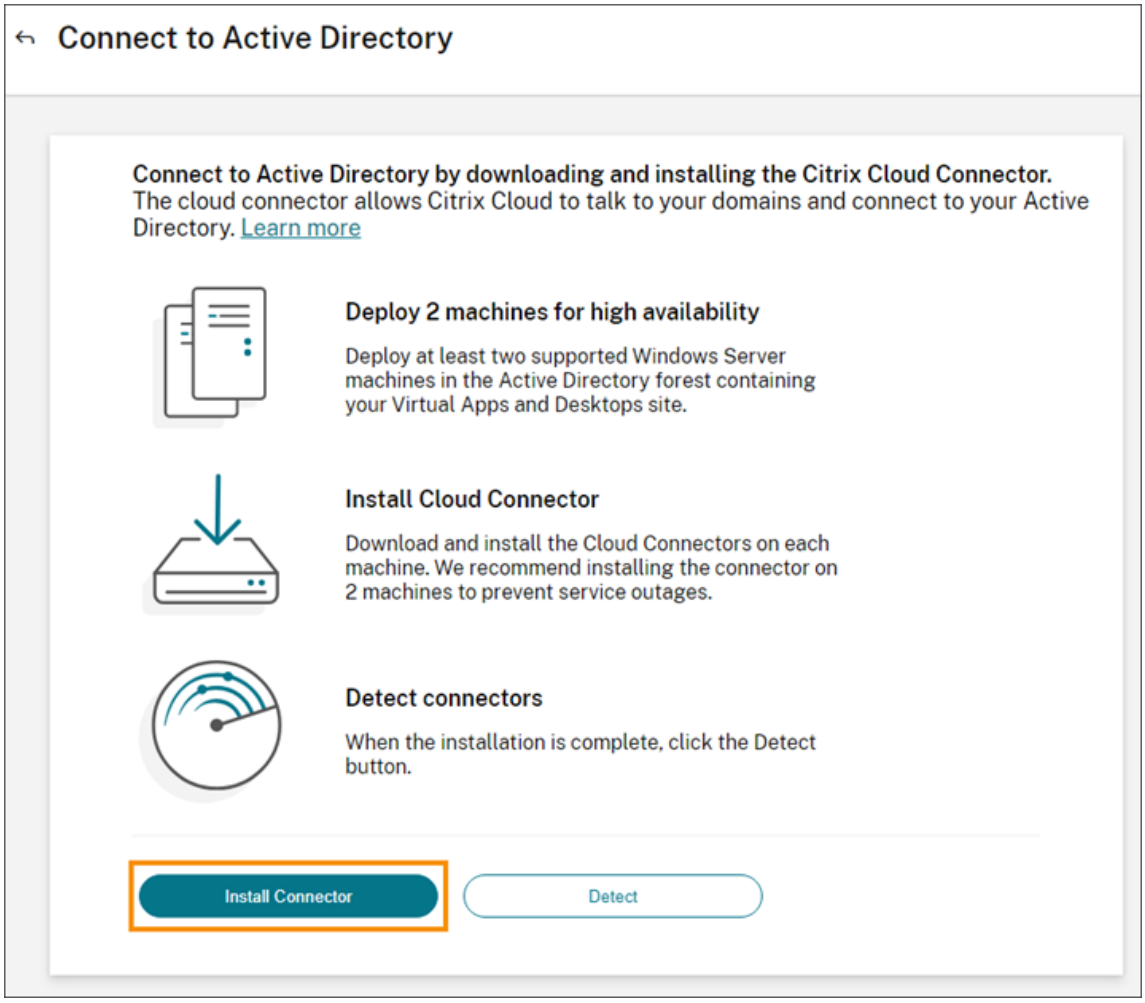
将 **Active Directory** 连接到 **Citrix Cloud**

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份识别和访问管理）。
2. 在 **Active Directory** 的“身份验证”选项卡中，单击省略号菜单并选择“连接”。



3. 单击“安装 **Cloud Connector**”以下载 Cloud Connector 软件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



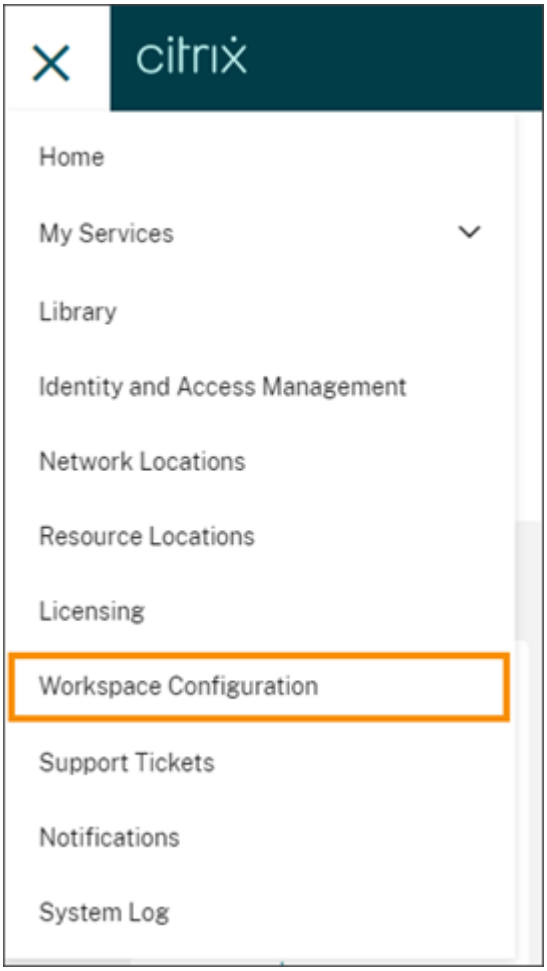
4. 启动 Cloud Connector 安装程序并按照安装向导进行操作。
5. 在“连接到 **Active Directory**”页面中，单击“检测”。验证后，Citrix Cloud 将显示一条消息，表明您的 Active Directory 已连接。
6. 单击“返回身份验证”。**Active Directory** 条目在“身份验证”选项卡上标记为“启用”。

启用 **Active Directory** 加令牌身份验证

1. 使用连接器设备或 Cloud Connector 将 Active Directory 连接到 Citrix Cloud。
2. 在 Citrix Cloud 身份和访问管理 部分的身份 验证 选项卡上，检查 A **ctive Directory** 条目是否标记为 已启用。
3. 单击下一步。将出现“配置令牌”页面，默认情况下选择“单个设备”选项。
4. 单击“保存并完成”以完成配置。在 身份验证 选项卡上，**Active Directory +** 令牌 条目被标记为 已启用。
5. 为工作区启用令牌身份验证：

    a) 在 Citrix Cloud 菜单中，选择 **Workspace** 配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) 在“身份验证”选项卡中，选择“**Active Directory +** 令牌”。

启用 Active Directory plus 令牌身份验证后，Workspace 订阅者可以注册其设备并使用身份验证器应用程序生成令牌。订阅者一次只能注册一台设备。有关注册用户设备的说明，请参阅 双重身份验证（可选）。

有关重新注册订阅者设备的选项，请参阅 重新注册设备。

更多信息

Citrix Tech Zone:

- 技术洞察：身份验证-TOTP
- 技术洞察：身份验证-推送

将 **Azure Active Directory** 连接到 **Citrix Cloud**

June 2, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 支持使用 Azure Active Directory (AD) 对 Citrix Cloud 管理员和工作区订阅者进行身份验证。

在 Citrix Cloud 中使用 Azure AD 时，可以执行以下操作：

- 利用自己的 Active Directory，以便能够控制审核和密码策略，以及在需要时轻松禁用帐户。
- 配置多因素身份验证以提高安全级别，防止出现被盗登录凭据的可能性。
- 使用带标志的登录页面，以便您的用户知晓自己正在正确的位置登录。
- 使用您选择的身份提供程序的联合，其中包括 ADFS、Okta 和 Ping。

Azure AD 应用程序和权限

Citrix Cloud 包含一个 Azure AD 应用程序，该应用程序允许 Citrix Cloud 无需登录活动的 Azure AD 会话即可与 Azure AD 进行连接。自此应用程序推出以来，Citrix 发布了可提高性能并支持新功能和权限的更新。

如果您有与 Citrix Cloud 的现有 Azure AD 连接，并且想要使用最新更新的应用程序，则需要在 Citrix Cloud 中更新您的 Azure AD 连接。有关详细信息，请参阅本文中的 已更新应用程序的重新连接到 Azure AD 。如果您选择不更新应用程序，则现有连接将继续正常运行。

有关 Citrix Cloud 用于连接您的 Azure AD 的 Azure AD 应用程序和权限的详细信息，请参阅适用于 Citrix Cloud 的 Azure Active Directory 权限。

> 提示：
>
> 通过 Citrix 身份和身份验证简介教育课程，详细了解受支持的身份 提供商。“规划 Citrix 身份和访问管理”模块包括一些简短的视频，这些视频将引导您完成将此身份提供商连接到 Citrix Cloud 以及为 Citrix Workspace 启用身份验证的过程。

使用多个 **Citrix Cloud** 帐户进行身份验证

本文介绍如何将作为身份提供者的 Azure AD 连接到单个 Citrix Cloud 帐户。如果您有多个 Citrix Cloud 帐户，则可以将每个帐户连接到同一 Azure AD 租户。请执行以下任务：

1. 登录您的 Citrix Cloud 帐户，然后从客户选择器中选择相应的客户 ID。
2. 如果所选客户是您第一个连接到 Azure AD 的客户，请按照本文中的所有步骤同步您的 AD 和 Azure AD、将客户连接到 Citrix Cloud 以及添加管理员。
3. 要连接其他客户，请单击 Citrix Cloud 控制台右上角的用户菜单，选择更改客户，然后选择要连接的下一个客户 ID。
4. 按照本文将 Citrix Cloud 连接到 Azure AD 中所述，将客户连接到您的 Azure AD。
5. 对每个客户 ID 重复步骤 3 和 4。

准备您的 **Active Directory** 和 **Azure AD**

请务必满足以下要求，以便能够使用 Azure AD：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 您有一个 Microsoft Azure 帐户。每个 Azure 帐户都随附免费的 Azure AD。如果您没有 Azure 帐户，请 通过 https://azure.microsoft.com/en-us/free/?v=17.36注册。
- 您在 Azure AD 中拥有全局管理员角色。要允许 Citrix Cloud 连接 Azure AD，必须使用此角色。
- 管理员帐户具有在 Azure AD 中配置的“mail”属性。为此，您可以使用 Microsoft 的 Azure AD Connect 工具将帐户从本地 Active Directory 同步到 Azure AD 中。或者，可以通过 Office 365 电子邮件配置未同步的 Azure AD 帐户。

通过 **Azure AD Connect** 同步帐户

1. 确保 Active Directory 帐户配置了电子邮件用户属性：
   a) 打开 Active Directory 用户和计算机。
   b) 在 用户 文件夹中，找到要检查的帐户，右键单击并选择 属性。在“常规”选项卡上，验证“电子邮件”字段的条目有效。Citrix Cloud 要求从 Azure AD 添加的管理员具有的电子邮件地址与使用 Citrix 托管的身份登录的管理员的电子邮件地址不同。
2. 安装并配置 Azure AD Connect。有关完整说明，请参阅 Microsoft Azure 网站上使用快速设置开始使用 Azure AD Connect。

将 **Citrix Cloud** 连接到 **Azure AD**

将 Citrix Cloud 帐户连接到您的 Azure AD 时，Citrix Cloud 除了需要访问您的 Azure AD 中用户的基本配置文件外，还需要访问您的用户配置文件（或登录用户的配置文件）的权限。Citrix 申请此权限，以便能够获取您的姓名和电子邮件地址（以用户身份）并使您能够浏览其他用户并在以后将其添加为管理员。有关 Citrix Cloud 请求的应用程序权限的更多信息，请参阅适用于 Citrix Cloud 的 Azure Active Directory 权限。

> 重要：
>
> 在登录 Citrix Cloud 之前，您必须是 Azure AD 的全局管理员才能完成此任务，或者要求任何全局管理员执行必备条件。

1. 单击页面左上角的“菜单”，然后选择“身份识别和访问管理”。
2. 找到 Azure Active Directory 并从省略号菜单中选择“连接”。
3. 出现提示时，为贵公司输入一个简短的 URL 友好型标识符，然后单击“连接”。所选标识符必须在 Citrix Cloud 中具有全局唯一性。
4. 系统提示时，登录要用于建立连接的 Azure 帐户。Azure 向您显示 Citrix Cloud 访问帐户以及获取连接所需的信息需要的权限。这些权限中的大多数都是只读的，允许 Citrix Cloud 从您的 Microsoft Graph 中收集基本信息，例如组和用户配置文件。如果您 Citrix Endpoint Management 或 XenMobile Server 与 Microsoft Intune 集成在一起，则必须授予与 Microsoft Intune 相关的读写权限。有关详细信息，请参阅适用于 Citrix Cloud 的 Azure Active Directory 权限。
5. 单击 **Accept**（接受）接受权限申请。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

备用连接方法

您可以将连接流分为以下两个阶段：

1. 在 Azure 中创建 Azure AD (Entra ID) 应用程序。
2. Citrix Cloud 连接到 Citrix Cloud 中的 Azure AD (Entra ID) 应用程序。

首先，您需要构造一个 URL，全局管理员可以使用该 URL 将企业应用程序添加到租户中。有关详细信息，请参阅构造用于授予租户范围管理员同意的 URL。

下面是对构造的 URL 的解释。

```
https://login.microsoftonline.com/<tenant url>/adminconsent?client_id
=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.
azure.com
```

其中：

`tenant url` 是您的租户 URL 或 ID。

`f9c0e999-22e7-409f-bb5e-956986abdf02` 是 Citrix Cloud 的客户端 ID。

从 **Azure AD** 将管理员添加到 **Citrix Cloud**

Citrix Cloud 支持单独添加管理员或作为 Azure AD 组添加管理员。

要从 Azure AD 添加个人管理员，请参阅 管理管理员访问权限。

要将 Azure AD 管理员组添加到 Citrix Cloud，请参阅 管理管理员组。

使用 **Azure AD** 登录 **Citrix Cloud**

连接 Azure AD 用户帐户后，用户可以使用以下方法之一登录 Citrix Cloud：

- 导航到您在最初连接贵公司的 Azure AD 身份提供程序时配置的管理员登录 URL。示例：`https://citrix.cloud.com/go/mycompany`
- 在 Citrix Cloud 登录页面 中，单击“使用我的公司凭据登录”，键入最初连接 Azure AD 时创建的标识符（例如“mycompany”），然后单击“继续”。

为工作区启用 **Azure AD** 身份验证

将 Azure AD 连接到 Citrix Cloud 后，您可以允许订阅者通过 Azure AD 向其工作区进行身份验证。

> 重要：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 在启用 Azure AD 工作区身份验证之前，请查看 Azure Active Directory 部分，了解将 Azure AD 与工作区结合使用的注意事项。

1. 在 Citrix Cloud 中，单击左上角的菜单按钮，然后选择 **Workspace** 配置。
2. 从“身份验证”选项卡中，选择“**Azure Active Directory**”。
3. 单击“确认”接受启用 Azure AD 身份验证时将发生的工作区体验更改。

启用高级 **Azure AD** 功能

Azure AD 提供高级多重身份验证、世界一流的安全功能、与 20 个不同身份提供商的联合、自助服务密码更改和重置以及许多其他功能。为您的 Azure AD 用户打开这些功能将使 Citrix Cloud 能够自动使用这些功能。

要比较 Azure AD 服务级别功能和定价，请参阅 https://azure.microsoft.com/en-us/pricing/details/active-directory/。

重新连接到 **Azure AD** 以获取更新的应用程序

Citrix Cloud 包含一个 Azure AD 应用程序，该应用程序允许 Citrix Cloud 无需登录活动的 Azure AD 会话即可与 Azure AD 进行连接。自推出此应用程序以来，Citrix 已对应用程序进行了如下更新：

- 2018 年 8 月，该应用程序进行了更新，以提高性能，并允许您为将来的版本做好准备。
- 2019 年 5 月，该应用程序进行了更新，支持将 Azure AD 管理员组添加到 Citrix Cloud。
- 2022 年 4 月，该应用程序进行了更新，使用了 GroupMember.read.all 权限，该权限取代了 Group.Read.All 权限。

如果您在发布这些更新之前将 Azure AD 连接到 Citrix Cloud，并且想要使用最新更新的应用程序，则需要断开您的 Azure AD 与 Citrix Cloud 的连接，然后重新连接它。使用最新的应用程序是可选的。如果您选择不更新应用程序，则现有连接仍能正常运行。

要求

在重新连接 Azure AD 之前，请验证是否满足以下要求：

- 您必须是默认 Citrix 身份提供程序下具有完全访问权限的管理员。如果您使用 Azure AD 凭据登录到 Citrix Cloud，则重新连接将失败。如果您的帐户中没有任何管理员在使用 Citrix 身份提供程序，则可以在重新连接 Azure AD 后暂时添加一个管理员并将其删除。有关说明，请参阅 邀请个人管理员。
- 如果使用 Azure AD 对工作区订阅者进行身份验证，请暂时选择其他身份提供程序。如果 Azure AD 也用作 Citrix Workspace 的身份验证方法，则 Citrix Cloud 不允许您断开连接 Azure AD 的连接。有关详细信息，请参阅 Citrix Workspace 文档中的 选择或更改身份验证方法 。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

重新连接 **Azure AD**

1. 以 Citrix 身份提供商下具有完全访问权限的管理员身份登录 Citrix Cloud。
2. 从 Citrix Cloud 菜单中，选择 身份识别和访问管理，然后选择 身份验证。
3. 找到 **Azure Active Directory**，然后从页面最右侧的省略号菜单中选择“断开连接”。
4. 从省略号菜单中，选择 连接。

> 注意：
>
> 如果您如步骤 3 中所述断开 Azure Active Directory 的连接，Citrix Cloud 会要求管理员删除该身份提供商下的所有管理配置文件。
> 要绕过这项工作，管理员可以按照以下步骤重新连接 Azure AD 身份提供商。
>
> 1. 作为全局管理员，导航到 Azure 并删除应用程序。
> 2. 登录 Citrix Cloud 并导航到“身份识别和访问管理”，然后单击“身份验证”。在“身份验证”选项卡中，您可以注意到 Azure AD 仍处于连接状态。
> 3. 在适用于 Azure AD 的 Citrix Cloud 中添加新管理员。
>
> 这将在不删除管理员的情况下触发应用程序的重新创建和重新连接。

Citrix Cloud 的 **Azure Active Directory** 权限

December 14, 2023

本文介绍了 Citrix Cloud 在连接和使用 Azure Active Directory (AD) 时请求的权限。根据在 Citrix Cloud 帐户中使用 Azure AD 的方式，可能会在目标 Azure AD 租户中创建一个或多个企业应用程序。您可以将多个 Citrix Cloud 帐户连接到一个 Azure AD 租户并使用相同的企业应用程序，而无需为每个帐户创建一组应用程序。

> 注意：
>
> 截至 2022 年 4 月，Citrix Cloud 用于连接 Azure AD 的 Azure AD 应用程序已更新为使用 GroupMember.Read.All 权限而不是 Group.Read.All 权限。如果你有现有 Azure AD 连接（2022 年 4 月之前），并且你希望应用程序使用新权限，则必须断开连接然后将你的 Azure AD 重新连接到 Citrix Cloud。此操作可确保你的帐户使用的是 Citrix Cloud 中最新的 Azure AD 应用程序。有关详细信息，请参阅 为升级后的应用程序重新连接到 Azure AD。
>
> 如果您选择不更新应用程序，则现有连接仍能正常运行。

企业应用程序

下表列出了 Citrix Cloud 在连接和使用 Azure AD 时使用的 Azure AD 企业应用程序以及每个应用程序的用途。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

名称	应用程序 ID	使用情况
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Workspace 订阅者登录
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Azure AD 和 Citrix Cloud 之间的默认连接
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	管理员邀请和登录
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Azure AD 与使用 Citrix Endpoint Management 的 Citrix Cloud 之间的默认连接
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Azure AD 与使用 Citrix Endpoint Management 的 Citrix Cloud 之间的传统连接

权限

Citrix Cloud 企业应用程序中的权限允许 Citrix Cloud 访问你的 Azure AD 租户中的某些数据。Citrix Cloud 使用这些数据执行特定功能，例如连接到你的 Azure AD 租户、允许管理员使用专用的登录 URL 登录 Citrix Cloud 以及将 Azure AD 租户与 Endpoint Management 连接起来。Citrix Cloud 只有在您同意的情况下才能访问这些数据。这些权限表示 Citrix Cloud 使用你的 Azure AD 所需的最低权限量。有关 Azure AD 权限和同意的更多信息，请参阅 Microsoft Azure 文档网站上的 Microsoft 身份平台中的权限和同意。

在本文中，每组 Azure AD 应用程序权限都包含以下信息：

- **API** 名称： Citrix Cloud 从中请求权限的资源应用程序。这些应用程序是 Microsoft Graph 和 Windows Azure Active Directory。Citrix Cloud 向这两个资源应用程序请求相同的权限。
- 类型： Citrix Cloud 为给定权限请求的访问级别。给定企业应用程序中的权限可以具有以下访问级别之一：
  - 委派权限 用于代表登录用户执行操作，例如在查询用户的配置文件时。
  - 当应用程序在用户不在场的情况下执行某项操作（例如查询特定群中的用户）时，将使用应用程序权限。此权限类型需要 Azure AD 中全局管理员的同意。
- 声明值： Azure AD 分配给给定权限的信息字符串。给定企业应用程序中的权限可以具有以下声明值之一：
  - **User.Read**：允许 Citrix Cloud 管理员将连接的 Azure AD 中的用户添加为 Citrix Cloud 帐户的管理员。
  - **User.ReadBasic.All**：从用户的个人资料中收集基本信息。它是 User.Read.All 的一个子集，但为了向后兼容，权限本身仍然存在。
  - **User.Read.All**： Citrix Cloud 调用 Microsoft Graph 中的 列出用户 ，以允许浏览和选择客户连接的 Azure AD 中的用户。例如，可以向来自 Azure AD 的用户授予使用 Workspace 访问 Citrix DaaS 资源

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

的权限。Citrix Cloud 无法使用，`User.ReadBasic.All` 因为 Citrix Cloud 需要访问基本配置文件之外的属性，例如 `onPremisesSecurityIdentifier`。

- **GroupMember.read.all**： Citrix Cloud 在 Microsoft Graph 中调用 列表 组，允许从客户连接的 Azure AD 中浏览和选择组。例如，也可以授予来自 Azure AD 的组访问 Citrix DaaS 应用程序的权限。
- **Directory.Read.All**： Citrix Cloud 调用 Microsoft Graph 中的 List memberOf 来获取用户的组成员资格，因为 `Groups.Read.All` 权限不足。
- **DeviceManagementApps.ReadWrite.All**：允许 Citrix Cloud 读写由 Microsoft Intune 管理的属性、组分配、应用程序状态、应用程序配置和 App Protection 策略。
- **Directory.AccessAsUser.All**：允许 Citrix Cloud 拥有与登录用户相同的目录中信息的访问权限。

> 注意：
>
> Direct **ory.Read.All** 仅适用于 **Azure AD** 和带有 **Endpoint Management** 的 **Citrix Cloud** 之间的默认连接。

Workspace 订阅者登录

此 Citrix Cloud 应用程序（ID：e95c4605-aeab-48d9-9c36-1a262ef8048e）使用以下权限：

API 名称	索赔价值	权限名称	类型
Microsoft Graph	User.Read	登录并阅读用户个人资料	已委派

Azure AD 和 **Citrix Cloud** 之间的默认连接

此 Citrix Cloud 应用程序（ID：f9c0e999-22e7-409f-bb5e-956986abdf02）使用以下权限：

API 名称	索赔价值	权限	类型
Microsoft Graph	GroupMember.Read.All	阅读所有组	已委派
Microsoft Graph	User.ReadBasic.All	阅读所有用户的基本配置文件	已委派
Microsoft Graph	User.Read.All	阅读所有用户的完整档案	已委派
Microsoft Graph	User.Read	登录并阅读用户个人资料	已委派
Microsoft Graph	GroupMember.Read.All	阅读所有组	应用程序
Microsoft Graph	User.Read.All	阅读所有用户的完整档案	应用程序
Microsoft Graph	User.Read	登录并阅读用户个人资料	应用程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

管理员邀请和登录

此 Citrix Cloud 应用程序（ID：1b32f261-b20c-4399-8368-c8f0092b4470）使用以下权限：

API 名称	索赔价值	权限名称	类型
Microsoft Graph	User.Read	登录并阅读用户个人资料	已委派
Microsoft Graph	User.ReadBasic.All	阅读所有用户的基本配置文件	已委派

Azure AD 和 **Citrix Cloud** 之间的默认连接以及 **Endpoint Management**

此 Citrix Cloud 应用程序（ID：5c913119-2257-4316-9994-5e8f3832265b）使用以下权限：

API 名称	索赔价值	权限名称	类型
Microsoft Graph	GroupMember.Read.All	阅读所有组	已委派
Microsoft Graph	User.ReadBasic.All	阅读所有用户的基本配置文件	已委派
Microsoft Graph	User.Read	登录并阅读用户个人资料	已委派
Microsoft Graph	Directory.Read.All	读取目录数据	应用程序
Microsoft Graph	Directory.Read.All	读取目录数据	已委派
Microsoft Graph	DeviceManagementApps.ReadWrite.All	读写 Microsoft Intune 应用程序	已委派
Microsoft Graph	Directory.AccessAsUser.All	以登录用户身份访问目录	已委派

Azure AD 和 **Citrix Cloud** 之间的传统连接以及 **Endpoint Management**

此 Citrix Cloud 应用程序（ID：e067934c-b52d-4e92-b1ca-70700bd1124e）使用以下权限：

API 名称	索赔价值	权限名称	类型
Microsoft Graph	GroupMember.Read.All	阅读所有组	已委派
Microsoft Graph	User.ReadBasic.All	阅读所有用户的基本配置文件	已委派
Microsoft Graph	User.Read	登录并阅读用户个人资料	已委派
Microsoft Graph	DeviceManagementApps.ReadWrite.All	读写 Microsoft Intune 应用程序	已委派

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

API 名称	索赔价值	权限名称	类型
Microsoft Graph	Directory.AccessAsUser.All	以登录用户身份访问目录	已委派

将本地 **Citrix Gateway** 作为身份提供程序连接到 **Citrix Cloud**

July 1, 2024

Citrix Cloud 支持使用本地 Citrix Gateway 作为身份提供程序对登录到其工作区的订阅者进行身份验证。

通过使用 Citrix Gateway 身份验证，您可以：

- 继续通过现有 Citrix Gateway 对用户进行身份验证，以便其能够通过 Citrix Workspace 访问本地 Virtual Apps and Desktops 部署中的资源。
- 在 Citrix Workspace 中使用 Citrix Gateway 身份验证、授权和审核 (AAA) 功能 。
- 使用直通身份验证、智能卡、安全令牌、条件访问策略、联合身份验证等功能，同时为用户提供通过 Citrix Workspace 访问所需资源的权限。

> 提示：
>
> 通过 Citrix 身份和身份验证简介教育课程，详细了解受支持的身份 提供商。“规划 Citrix 身份和访问管理”模块包括一些简短的视频，这些视频将引导您完成将此身份提供商连接到 Citrix Cloud 以及为 Citrix Workspace 启用身份验证的过程。

支持的版本

以下本地产品版本支持 Citrix Gateway 身份验证：

- Citrix Gateway 12.1 54.13 Advanced Edition 或更高版本
- Citrix Gateway 13.0 41.20 Advanced Edition 或更高版本

必备条件

Cloud Connector

您至少需要两 (2) 台服务器才能安装 Citrix Cloud Connector 软件。这些服务器必须满足以下要求：

- 符合 Cloud Connector 技术详情中描述的系统要求。
- 未安装任何其他 Citrix 组件，不是 Active Directory 域控制器，也不是对您的资源位置基础结构至关重要的计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 已加入您的网站所在的域。如果用户在多个域中访问您站点的应用程序，则必须在每个域中至少安装两个 Cloud Connector。
- 已连接到可以联系您网站的网络。
- 已连接到 Internet。有关详细信息，请参阅系统和连接要求。
- 至少需要两个 Cloud Connector 才能确保与 Citrix Cloud 的高可用连接。安装后，Cloud Connector 允许 Citrix Cloud 找到您的站点并与之通信。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。

Active Directory

在启用 Citrix Gateway 身份验证之前，请执行以下任务：

- 验证您的工作区订阅者在 Active Directory (AD) 中是否有用户帐户。没有 AD 帐户的订阅者无法成功登录其工作区。
- 确保已填充订阅者 AD 帐户中的用户属性。Citrix Cloud 需要这些属性才能在订阅者登录时建立用户上下文。如果未填充这些属性，订阅者将无法登录其工作区。这些属性包括：
  - 电子邮件地址
  - 显示名称
  - 常见的名字
  - SAM 帐户名
  - 用户主体名称
  - OID
  - SID
- 将您的 Active Directory (AD) 连接到您的 Citrix Cloud 帐户。在本任务中，您将在准备好的服务器上安装 Cloud Connector 软件，如 Cloud Connector 部分所述。Cloud Connector 使 Citrix Cloud 能够与您的本地环境通信。有关说明，请参阅 将 Active Directory 连接到 Citrix Cloud。
- 如果要使用 Citrix Gateway 身份验证执行联合，请将 AD 用户同步到联合身份验证提供程序。Citrix Cloud 要求您的工作空间订阅者具有 AD 用户属性，以便他们能够成功登录。

要求

Citrix Gateway 高级策略

由于已弃用经典策略，Citrix Gateway 身份验证需要在本地网关上使用高级策略。高级策略支持 Citrix Cloud 的多重身份验证 (MFA)，包括身份提供商链接等选项。如果您当前使用经典策略，则必须创建新的高级策略才能在 Citrix Cloud 中使用 Citrix Gateway 身份验证。创建高级策略时，您可以重复使用经典策略的“操作”部分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

签名证书

配置网关以对 Citrix Workspace 的订阅者进行身份验证时，网关充当 OpenID Connect 提供商。Citrix Cloud 与 Gateway 之间的消息符合 OIDC 协议，该协议涉及对令牌进行数字签名。因此，您必须配置证书以对这些令牌进行签名。此证书必须由公共证书颁发机构 (CA) 颁发。不支持使用私有 CA 颁发的证书，因为无法向 Citrix Cloud 提供私有根 CA 证书。因此，无法建立证书信任链。如果您为签名配置了多个证书，则会为每条消息轮换这些密钥。

密钥必须绑定到 **vpn** 全局。如果没有这些密钥，订阅者在登录后将无法成功访问其工作区。

时钟同步

由于 OIDC 中的数字签名消息带有时间戳，因此必须将网关同步到 NTP 时间。如果时钟未同步，Citrix Cloud 会在检查令牌的有效性时假定令牌已过时。

任务概述

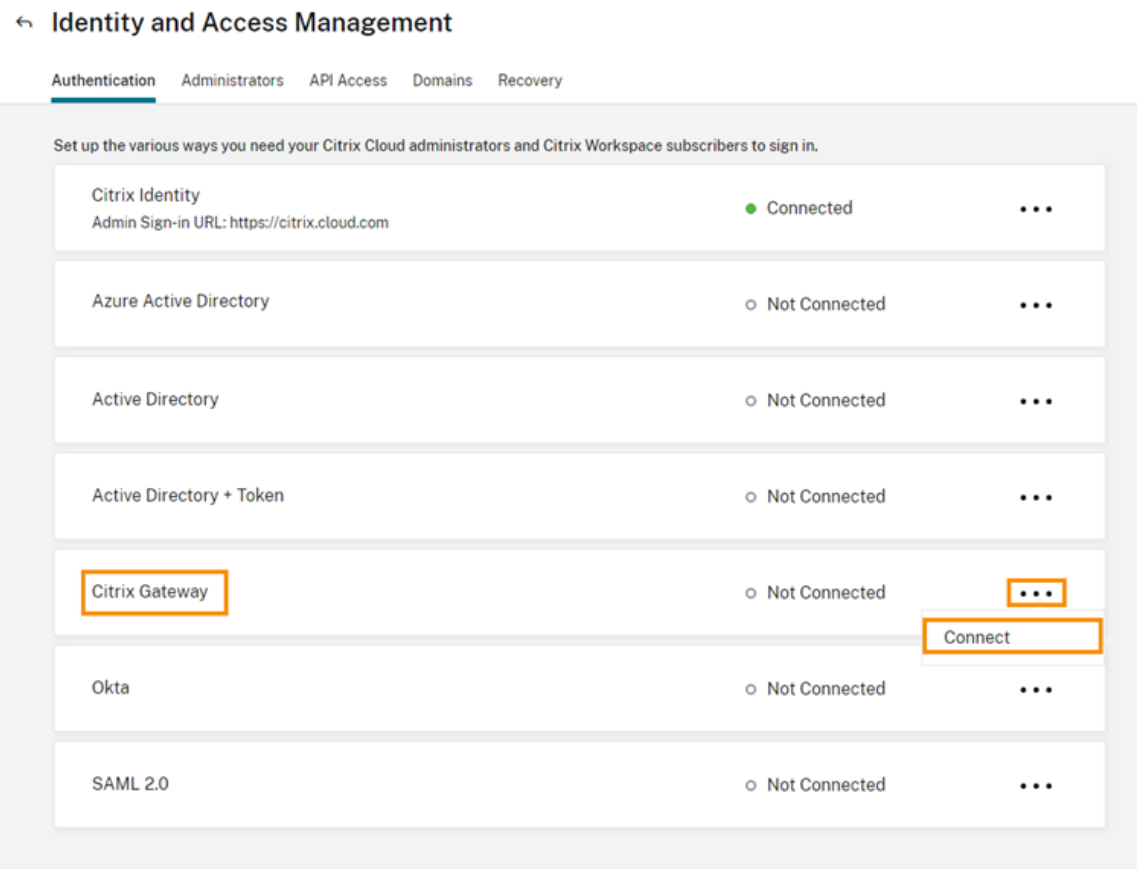
要设置 Citrix Gateway 身份验证，请执行以下任务：

1. 在 身份和访问管理中，开始配置与网关的连接。在此步骤中，您将生成网关的客户端 ID、密钥和重定向 URL。
2. 在网关上，使用从 Citrix Cloud 生成的信息创建 OAuth IdP 高级策略。这使 Citrix Cloud 能够与您的本地网关进行连接。有关说明，请参阅以下文章：
   - Citrix Gateway 12.1：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商
   - Citrix Gateway 13.0：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商
3. 在 **Workspace** 配置中，为订阅者启用 Citrix Gateway 身份验证。

为工作区订阅者启用 **Citrix Gateway** 身份验证

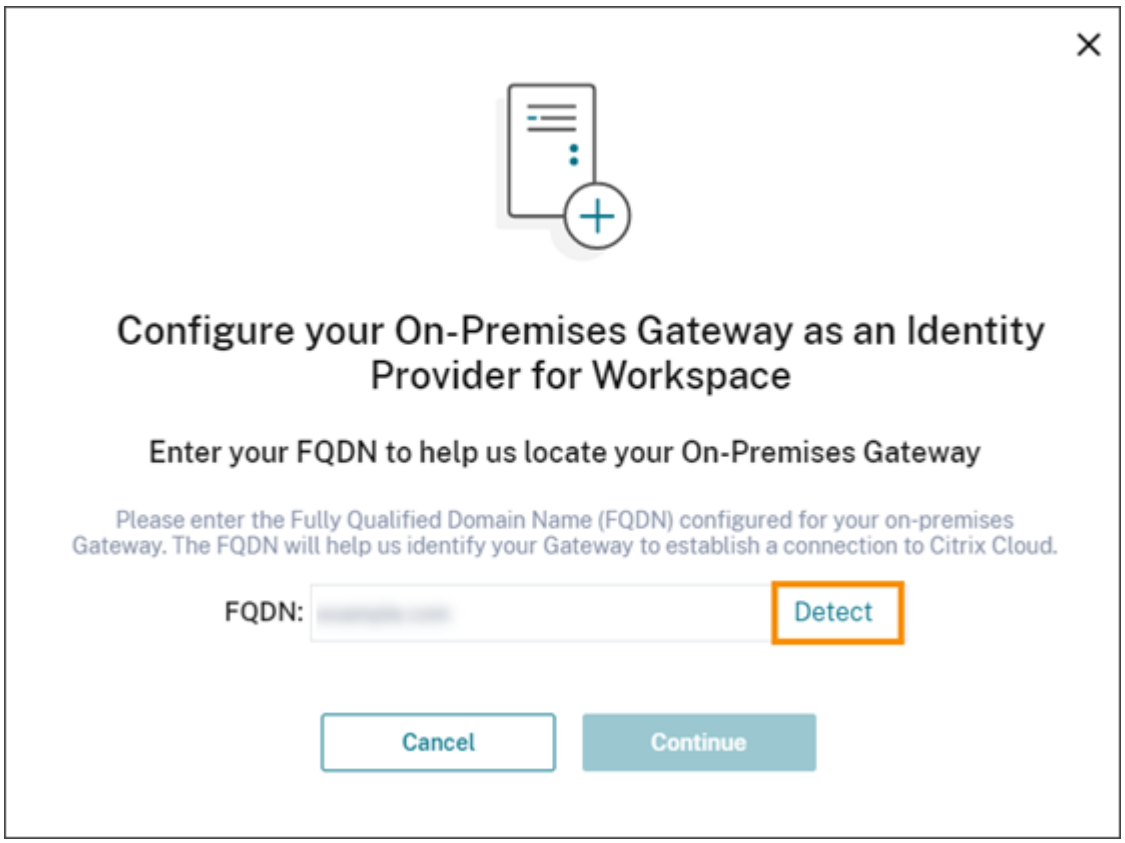
1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份识别和访问管理）。
2. 在 **Citrix Gateway** 的“身份验证”选项卡中，单击省略号菜单并选择“连接”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 输入本地网关的 FQDN，然后单击 检测。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

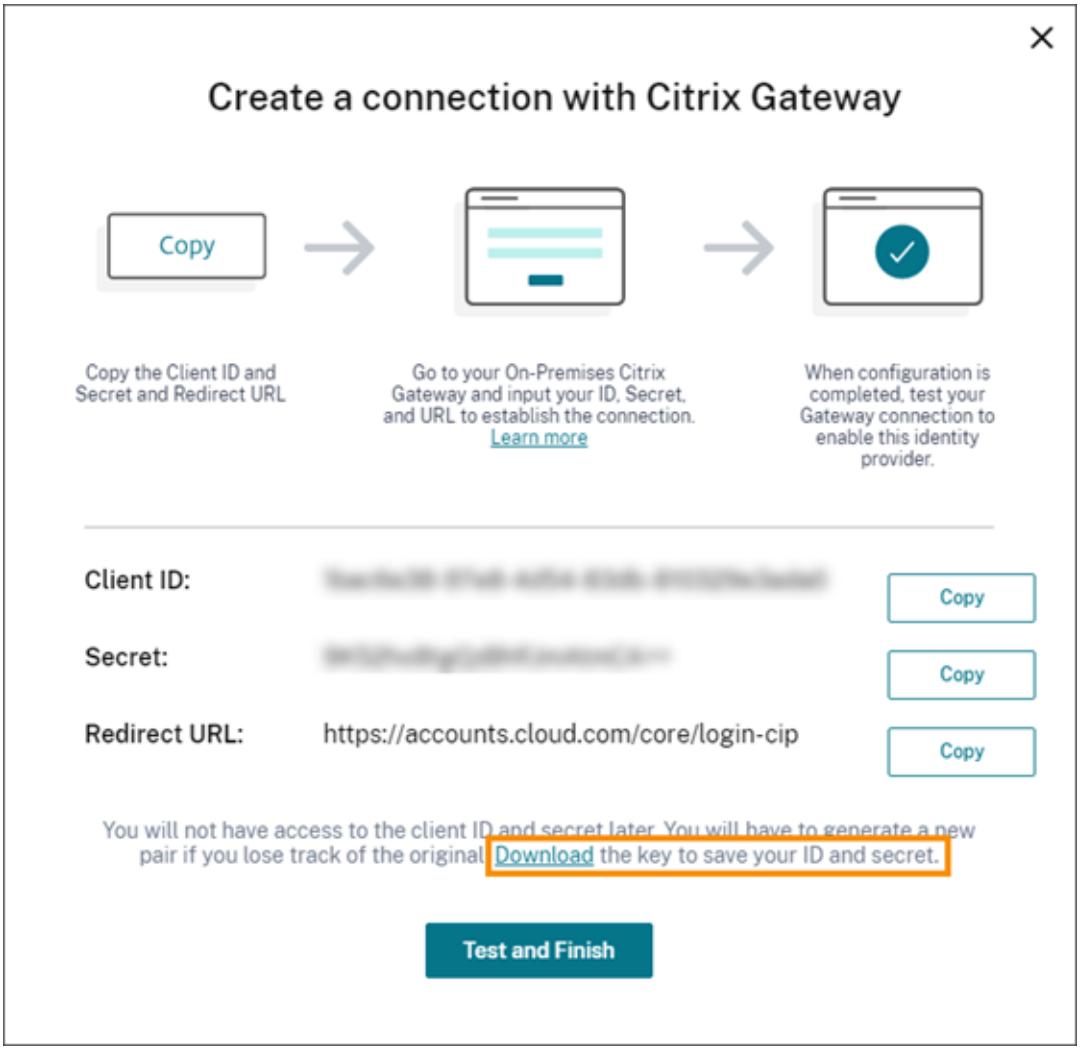


在 Citrix Cloud 成功检测到该对话框后，单击 继续。

4. 创建与本地网关的连接：

   a) 复制 Citrix Cloud 显示的客户端 ID、密钥和重定向 URL。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



另外，下载此信息的副本并将其安全地脱机保存以供参考。此信息生成后在 Citrix Cloud 中不可用。

b) 在网关上，使用来自 Citrix Cloud 的客户端 ID、密钥和重定向 URL 创建 OAuth IdP 高级策略。有关说明，请参阅以下文章：

- 对于 Citrix Gateway 12.1：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商
- 对于 Citrix Gateway 13.0：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商

c) 单击 **Test and Finish**（测试并完成）。Citrix Cloud 会验证您的网关是否可访问且配置正确。

5. 为工作区启用 Citrix Gateway 身份验证：

a) 在 Citrix Cloud 菜单中，选择 **Workspace** 配置。
b) 在“身份验证”选项卡中，选择 **Citrix Gateway**。
c) 选择“我了解对订阅者体验的影响”，然后单击“保存”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除

作为第一步，请查看本文中的 先决条件 和 要求 部分。确认您的本地环境中有所有必需的组件，并且已完成所有必需的配置。如果这些项目中的任何一项丢失或配置错误，则使用 Citrix Gateway 进行工作区身份验证将不起作用。

如果您在 Citrix Cloud 和本地网关之间建立连接时遇到问题，请验证以下各项：

- 网关 FQDN 可从互联网访问。
- 您已在 Citrix Cloud 中正确输入网关 FQDN。
- 您已在 OAuth IdP 策略的 `-issuer` 参数中正确输入了网关 URL。示例：`-issuer https://GatewayFQDN.com`。`issuer` 参数区分大小写。
- 在 OAuth IdP 策略的客户端 ID、客户端密钥、重定向 URL 和受众字段中正确输入来自 Citrix Cloud 的客户端 ID、密钥和重定向 URL 值。确认在策略的“受众”字段中输入了正确的客户 ID。
- OAuth IdP 身份验证策略配置正确。有关说明，请参阅以下文章：
  - Citrix Gateway 12.1：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商
  - Citrix Gateway 13.0：使用本地 Citrix Gateway 作为 Citrix Cloud 的身份提供商
- 验证策略是否已正确绑定到 AAA 身份验证服务器，如 绑定身份验证策略中所述。

全局编录服务器

除了检索用户帐户详细信息外，网关还会检索用户的域名、AD NETBIOS 名称和根 AD 域名。要检索 AD NETBIOS 名称，Gateway 会搜索用户帐户所在的 AD。NETBIOS 名称不会在全局编录服务器上复制。

如果您在 AD 环境中使用全局编录服务器，则在这些服务器上配置的 LDAP 操作不适用于 Citrix Cloud。相反，您必须在 LDAP 操作中配置单个 AD。如果您有多个域或林，则可以配置多个 LDAP 策略。

使用 **Kerberos** 或 **IdP** 链接对单点登录进行 **AD** 搜索

如果您使用 Kerberos 或使用 SAML 或 OIDC 协议进行订阅者登录的外部身份提供商，请验证是否配置了 AD 查找。Gateway 需要 AD 查找来检索订阅者的 AD 用户属性和广告配置属性。

确保已配置 LDAP 策略，即使身份验证是由第三方服务器处理的。要配置这些策略，可通过执行以下任务向现有登录架构配置文件添加第二个身份验证因素：

1. 创建一个仅从 Active Directory 中提取属性和组的 LDAP 身份验证服务器。
2. 创建 LDAP 高级身份验证策略。
3. 创建身份验证策略标签。
4. 将身份验证策略标签定义为主身份提供者之后的下一个因素。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

添加 **LDAP** 作为第二个身份验证因素

1. 创建 LDAP 身份验证服务器：

   a) 选择 系统 **>** 身份验证 **>** 基本策略 **> LDAP >** 服务器 **>** 添加。
   b) 在“创建身份验证 **LDAP** 服务器”页面上，输入以下信息：

      - 在 选择服务器类型中，选择 **LDAP**。
      - 在 名称中，输入服务器的友好名称。
      - 选择 服务器 **IP** ，然后输入 LDAP 服务器的 IP 地址。
      - 在 安全类型中，选择所需的 LDAP 安全类型。
      - 在“服务器类型”中，选择 **AD**。
      - 在“身份验证”中，不要选中该复选框。必须清除此复选框，因为此身份验证服务器仅用于从 Active Directory 中提取用户属性和组，而不是身份验证。

   c) 在“其他设置”下，输入以下信息：

      - 在 服务器登录名属性中，输入 **UserPrincipalName**。
      - 在 组属性中，选择 **memberOf**。
      - 在 子属性名称中，选择 **cn**。

2. 创建 LDAP 高级身份验证策略：

   a) 选择 安全 **> AAA-**应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 策略 **>** 添加。
   b) 在“创建身份验证策略”页面上，输入以下信息：

      - 在 名称中，输入策略的友好名称。
      - 在 操作类型中，选择 **LDAP**。
      - 在“操作”中，选择您之前创建的 LDAP 身份验证服务器。
      - 在 表达式中，输入 **TRUE**。

   c) 单击“创建”保存配置。

3. 创建身份验证策略标签：

   a) 选择安全 **> AAA** —应用程序流量 **>** 策略 **>** 身份验证 **>** 高级策略 **>** 策略标签 **>** 添加。
   b) 在 名称中，输入身份验证策略标签的友好名称。
   c) 在登录架构中，选择 **LSCHEMA_INT**。
   d) 在 策略绑定下的 选择策略中，选择您之前创建的 LDAP 高级身份验证策略。
   e) 在 **GoTo** 表达式中，选择 **END**。
   f) 单击“绑定”完成配置。

4. 将 LDAP 身份验证策略标签定义为主身份提供程序之后的下一个因素：

   a) 选择 系统 **>** 安全 **> AAA-**应用程序流量 **>** 虚拟服务器。
   b) 选择包含主身份提供商绑定的虚拟服务器，然后选择 编辑。
   c) 在“高级身份验证策略”下，选择现有的身份验证策略绑定。
   d) 选择主身份提供商的绑定，然后选择 编辑绑定。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) 在“策略绑定”页面的 选择下一个因素中，选择您之前创建的 LDAP 身份验证策略标签。
f) 单击“绑定”保存配置。

多因素身份验证的默认密码

如果您对工作空间订阅者使用多因素身份验证 (MFA)，网关会使用最后一个因素的密码作为单点登录的默认密码。订阅者登录其工作区时，此密码将发送到 Citrix Cloud。如果环境中的 LDAP 身份验证后面有其他因素，则必须将 LDAP 密码配置为发送到 Citrix Cloud 的默认密码。在与 LDAP 因素对应的登录架构上启用 **SSOCredentials**。

更多信息

Citrix Tech Zone：技术见解：身份验证 - 网关

将作为身份提供商的 **Google Cloud Identity** 连接到 **Citrix Cloud**

October 5, 2023

Citrix Cloud 支持使用 Google Cloud Identity 作为身份提供商对登录其工作区的订阅者进行身份验证。通过将组织的 Google 帐户关联到 Citrix Cloud，您可以为访问 Citrix Workspace 和 Google 资源提供统一的登录体验。

加入域和未加入域配置的要求

可以使用已加入域或未加入域的计算机在 Citrix Cloud 中将 Google Cloud Identity 配置为身份提供商。

- 加入域意味着计算机加入到本地 Active Directory (AD) 中的域，身份验证使用存储在该域中的用户配置文件。
- 未加入域意味着计算机未加入到 AD 域，并且身份验证使用存储在您的 Google Workspace 目录中的用户配置文件（也称为 Google 本地用户）。

下表列出了每种配置类型的要求。

要求	已加入域	未加入域	更多信息
本地 AD	是	否	请参阅本文中的 准备 Active Directory 和 Citrix Cloud 连接器 。
在您的资源位置部署了 Citrix Cloud 连接器	是	否；无需 Cloud Connector 即可访问未加入域的计算机。	在本文中 @@ 准备 Active Directory 和 Citrix Cloud 连接器 。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要求	已加入域	未加入域	更多信息
AD 与 Google Cloud 同步	仅在使用 Gateway 服务且不使用其他服务时才可选。否则，此任务是必需的。	否	请参阅本文中的将 Active Directory 与 Google Cloud Identity 同步。
具有 Google Cloud Platform 控制台访问权限的开发者帐号。用于创建服务帐号和密钥，以及启用管理员 SDK API。	是	是	请参阅本文中的 创建服务帐号、创建服务帐号密钥和配置域范围委 派。
具有 Google Workspace 管理员控制台访问权限的管理员帐号。用于配置域范围的委派和只读 API 用户帐户。	是	是	请参阅本文中的 配置域范围委派 和 添加只读 API 用户帐户 。

使用多个 **Citrix Cloud** 帐户进行身份验证

本文介绍如何将作为身份提供商的 Google Cloud Identity 连接到单个 Citrix Cloud 帐户。如果您有多个 Citrix Cloud 帐户，则可以使用相同的服务帐户和只读 API 用户帐户将每个帐户连接到同一 Google Cloud 帐户。只需登录 Citrix Cloud 并从客户选取器中选择相应的客户 ID 即可。

准备 **Active Directory** 和 **Citrix Cloud** 连接器

如果您使用的是加入了域的带 Google Cloud Identity 的计算机，请使用此部分来准备您的本地 AD。如果您使用的是未加入域的计算机，请跳过此任务并继续本文中的 创建服务帐户 。

您的 Active Directory 域中至少需要两 (2) 台服务器才能安装 Citrix Cloud Connector 软件。要启用 Citrix Cloud 与您的 资源位置之间的通信，需要使用 Cloud Connector。至少需要两个 Cloud Connector 才能确保与 Citrix Cloud 的高可用连接。这些服务器必须满足以下要求：

- 符合 Cloud Connector 技术详情中描述的要求。
- 未安装任何其他 Citrix 组件，不是 Active Directory 域控制器，也不是对您的资源位置基础结构至关重要的计算机。
- 已加入您的 Active Directory (AD) 域。如果您的工作空间资源和用户位于多个域中，则必须在每个域中至少安装两个 Cloud Connector。有关更多信息，请参阅 Active Directory 中 Cloud Connector 的部署方案。
- 已连接到可以联系用户通过 Citrix Workspace 访问的资源的网络。
- 已连接到 Internet。有关详细信息，请参阅系统和连接要求。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

将 **Active Directory** 与 **Google Cloud Identity** 同步

如果您使用的是加入了域的带 Google Cloud Identity 的计算机，请使用此部分来准备您的本地 AD。如果您使用的是未加入域的计算机，请跳过此任务并继续本文中的 创建服务帐户 。

如果您仅使用 Citrix Gateway 服务，而未启用其他服务，则可以选择将 AD 与 Google Cloud Identity 同步。仅针对这些服务，您可以使用 Google 本地用户，而无需与 AD 同步。

如果您使用的是其他 Citrix Cloud 服务，则需要将您的 AD 与 Google Cloud Identity 同步。Google Cloud 必须将以下 AD 用户属性传递给 Citrix Cloud：

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

将您的 **AD** 与 **Google Cloud** 同步

1. 从谷歌网站下载并安装 谷歌云目录同步实用程序 。有关此实用程序的 更多信息，请参阅 Google 网站上的 Google Cloud 目录同步 文档。
2. 安装该实用程序后，启动 Configuration Manager（开始 **> Configuration Manager**）。
3. 指定 Google 域名设置和 LDAP 设置，如实用程序文档中的设置与 Configuration Manager 的同步中所述。
4. 在 常规设置中，选择 自定义架构。保持默认选择不变。
5. 配置自定义架构以应用于所有用户帐户。使用本节中指定的精确大小写和拼写输入所需信息。

    a) 选择“自定义架构”选项卡，然后选择“添加架构”。
    b) 选择 使用“用户帐户”中定义的规则。
    c) 在 架构名称中，输入 **citrix-schema**。
    d) 选择添加字段，然后输入以下信息：
        - 在架构字段模板下的架构字段中，选择 **userPrincipalName**。
        - 在 **Google** 字段详细信息下的 字段名称中，输入 **UPN**。
    e) 重复步骤 4 以创建以下字段：
        - objectGUID：在架构字段模板下，选择 **objectGUID**。在 **Google** 字段详细信息下，输入 **objectGUID**。
        - SID：在 架构字段模板下，选择 自定义。在 **Google** 字段详细信息下，输入 **SID**。
        - objectSID：在架构字段模板下，选择自定义。在 **Google** 字段详细信息下，输入 **objectSID**。
    f) 选择“确定”保存您输入的内容。

6. 按照实用程序文档的“设置与 Configuration Manager 的同步”中所述完成组织的所有剩余设置配置并验证同步设置。
7. 选择“同步并应用更改”，将您的 Active Directory 与您的 Google 帐户同步。

同步完成后，Google Cloud 中的用户信息部分会显示用户的 Active Directory 信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

创建一个服务帐户

要完成此任务，您需要一个 Google Cloud Platform 开发者帐户。

1. 登录 https://console.cloud.google.com。
2. 从控制面板侧边栏中，选择 **IAM** 和管理员，然后选择 服务帐户。
3. 选择创建服务帐户。
4. 在 服务帐户详细信息下，输入服务帐户名称和服务帐户 ID。
5. 选择完成。

创建服务帐户密钥

1. 在“服务帐户”页面上，选择您刚刚创建的服务帐户。
2. 选择密钥选项卡，然后选择添加密钥 **>** 创建新密钥。
3. 将默认 JSON 密钥类型选项保留为选中状态。
4. 选择创建。将密钥保存到稍后可以访问的安全位置。当您以身份提供商的身份连接 Google Cloud Identity 时，可以在 Citrix Cloud 控制台中输入私钥。

配置域范围的委派

1. 启用管理员 SDK API：
    a) 从 Google Cloud Platform 菜单中选择 **API** 和服务 **>** 已启用 **API** 和服务。
    b) 选择控制台顶部附近的 启用 **API** 和服务。此时将显示 API 库主页。
    c) 搜索 管理员 **SDK API** ，然后从结果列表中选择它。
    d) 选择“启用”。
2. 为服务帐户创建 API 客户端：
    a) 从 Google Cloud Platform 菜单中选择 **IAM** 和管理员 **>** 服务帐户，然后选择您之前创建的服务帐户。
    b) 在服务帐户的 详细信息 选项卡中，展开 高级设置。
    c) 在“全域委派”下，复制客户端 ID，然后选择“查看 **Google Workspace** 管理员控制台”。
    d) 如果适用，请选择要使用的 Google Workspace 管理员帐户。此时将显示 Google 管理控制台。
    e) 在 Google 管理员侧栏中，选择 安全 **>** 访问和数据控制 **> API** 控制。
    f) 在“域范围委派”下，单击“管理全域委派”。
    g) 选择“新增”。
    h) 在客户端 **ID** 中，粘贴您在步骤 C 中复制的服务帐户的客户端 ID。
    i) 在 **OAuth** 作用域中，在以逗号分隔的单行中输入以下范围：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

```
https://www.googleapis.com/auth/admin.directory.user.readonly,
    https://www.googleapis.com/auth/admin.directory.group.
    readonly,https://www.googleapis.com/auth/admin.directory.
    domain.readonly
<!--NeedCopy-->
```

j) 选择 授权。

添加只读 **API** 用户帐户

在此任务中，您将创建一个具有 Citrix Cloud 只读 API 访问权限的 Google Workspace 用户帐户。此帐户不用于任何其他目的，也没有其他权限。

1. 从 Google 管理员菜单中，选择 目录 **>** 用户。
2. 选择 添加新用户 并输入相应的用户信息。
3. 选择 添加新用户 以保存帐户信息。
4. 为只读用户帐户创建自定义角色：
   a) 在 Google 管理员菜单中，选择 帐户 **>** 管理员角色。
   b) 选择 创建新角色。
   c) 输入新角色的名称。示例：API-ReadOnly
   d) 选择继续。
   e) 在 管理员 **API** 权限下，选择以下权限：
      - 用户 > 读取
      - 组 > 读取
      - 域管理
   f) 选择 继续，然后选择 创建角色。
5. 将自定义角色分配给您之前创建的只读用户帐户：
   a) 在自定义角色详细信息页面的 管理员 窗格中，选择 分配用户。
   b) 开始键入只读用户帐户的名称，然后从用户列表中选择它。
   c) 选择 分配角色。
   d) 要验证角色分配，请返回用户页面（目录 **>** 用户），然后选择只读用户帐户。自定义角色分配显示在 管理员角色和权限下。

将 **Google Cloud Identity** 连接到 **Citrix Cloud**

1. 通过 https://citrix.cloud.com登录 Citrix Cloud。
2. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份识别和访问管理）。
3. 找到 **Google Cloud Identity**，然后从省略号菜单中选择“连接”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

4. 出现提示时，为贵公司输入一个简短的 URL 友好标识符，然后选择“保存并继续”。所选标识符必须在 Citrix Cloud 中具有全局唯一性。
5. 选择 导入文件，然后选择您在 为服务帐户创建密钥时保存的 JSON 文件。此操作会导入您的私钥和您创建的 Google Cloud 服务帐户的电子邮件地址。
6. 在 模拟用户中，输入只读 API 用户帐户的名称。
7. 选择下一步。Citrix Cloud 会验证您的 Google 帐户详细信息并测试连接。
8. 查看列出的关联域。如果正确，请选择确认以保存您的配置。

向 **Citrix Cloud** 添加管理员

您可以通过 Google Cloud 添加单个 Citrix Cloud 管理员和管理员组。有关详细信息，请参阅以下文章：

- 对于个人管理员：管理管理员对 Citrix Cloud 的访问权限
- 对于管理员组：管理管理员组

将管理员添加到 Citrix Cloud 后，他们可以使用以下方法之一登录：

- 导航到您在最初将 Google Cloud 配置为身份提供商时配置的管理员登录网址。示例：`https://citrix.cloud.com/go/mycompany`
- 在 Citrix Cloud 登录页面上，选择使用我的公司凭据登录，输入贵公司的唯一标识符（例如“mycompany”），然后单击继续。

启用 **Google Cloud Identity** 进行工作区身份验证

1. 在 Citrix Cloud 菜单中，选择 **Workspace** 配置 **>** 身份验证。
2. 选择 **Google Cloud Identity**。出现提示时，选择“我了解对订阅者体验的影响”，然后单击“保存”。

将 **Okta** 作为身份提供程序连接到 **Citrix Cloud**

July 1, 2024

Citrix Cloud 支持使用 Okta 作为身份提供程序来对登录其 Workspace 的订阅者进行身份验证。通过将您的 Okta 组织连接到 Citrix Cloud，您可以为订阅者提供通用的登录体验，以访问 Citrix Workspace 中的资源。

在 Workspace 配置中启用 Okta 身份验证后，订阅者将获得不同的登录体验。选择 Okta 身份验证提供联合登录，而不是单点登录。订阅者从 Okta 登录页面登录 Workspace，但在从 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）打开应用程序或桌面时，他们可能需要再次进行身份验证。要启用单点登录并防止出现第二次登录提示，您需要将 Citrix 联合身份验证服务与 Citrix Cloud 结合使用。有关详细信息，请参阅将 Citrix 联合身份验证服务连接到 Citrix Cloud。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

必备条件

Cloud Connector 或 Connector Appliance

要启用 Citrix Cloud 与您的资源位置之间的通信，需要使用 Cloud Connector 或 Connector Appliance。至少需要两个 Cloud Connector 或 Connector Appliance 才能确保与 Citrix Cloud 的高可用连接。您需要至少两个连接器加入您的 Active Directory 域。它们可以是 Cloud Connector 或 Connector Appliance。

连接器必须满足以下要求：

- 满足各自文档中描述的要求
- 已加入您的 Active Directory (AD) 域。如果您的 Workspace 用户位于多个域中，则可以使用 Connector Appliance 多域功能加入多个域。
- 已连接到可以联系用户通过 Citrix Workspace 访问的资源的网络。
- 已连接到 Internet。有关详细信息，请参阅系统和连接要求。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。
有关安装 Connector Appliance 的详细信息，请参阅 Connector Appliance 安装。

Okta 域

将 Okta 连接到 Citrix Cloud 时，必须为组织提供 Okta 域。Citrix 支持以下 Okta 域：

- okta.com
- okta-eu.com
- oktapreview.com

您还可以将 Okta 自定义域与 Citrix Cloud 配合使用。在 Okta Web 站点上的“自定义 Okta URL 域”中查看使用自定义域的重要注意事项。

有关为您的组织查找自定义域的更多信息，请参阅在 Okta 网站上查找您的 Okta 域 。

Okta OIDC Web 应用程序

要使用 Okta 作为身份提供商，必须首先使用可与 Citrix Cloud 配合使用的客户端凭据创建 Okta OIDC Web 应用程序。创建并配置应用程序后，请记下客户端 ID 和客户端密钥。在连接 Okta 组织时，您可以向 Citrix Cloud 提供这些值。

要创建和配置此应用程序，请参阅本文中的以下部分：

- 创建 Okta OIDC Web 应用程序集成
- 配置 Okta OIDC Web 应用程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workspace URL

创建 Okta 应用程序时，必须提供来自 Citrix Cloud 的 Workspace URL。要找到 Workspace URL，请从 Citrix Cloud 菜单中选择 **Workspace** 配置。Workspace URL 显示在访问选项卡上。

> 重要：
>
> 如果稍后修改 Workspace URL，则必须使用新的 URL 更新 Okta 应用程序配置。否则，您的订阅者可能会遇到从其 Workspace 注销的问题。

Okta API 令牌

使用 Okta 作为 Citrix Cloud 的身份提供商需要为您的 Okta 组织提供 API 令牌。使用您的 Okta 组织中的只读管理员帐户创建此令牌。此令牌必须能够读取 Okta 组织中的用户和组。

要创建 API 令牌，请参阅本文中的 创建 Okta API 令牌 。有关 API 令牌的更多信息，请参阅 Okta 网站上的 创建 API 令牌 。

> 重要：
>
> 创建 API 令牌时，请记下令牌值（例如，将该值临时复制到纯文本文档中）。Okta 仅显示一次此值，因此您可以在执行 将 Citrix Cloud 连接到 Okta 组织中的步骤之前创建令牌。

与 Okta AD 代理同步帐户

要使用 Okta 作为身份提供商，您必须先将本地 AD 与 Okta 集成。为此，您需要在域中安装 Okta AD 代理，然后将您的 AD 添加到您的 Okta 组织。有关部署 Okta AD 代理的指导，请参阅 Okta Web 站点上的 Active Directory 集成入门。

之后，将您的 AD 用户和组导入 Okta。导入时，请包括以下与您的 AD 帐户关联的值：

- 电子邮件
- SID
- UPN
- OID

> 注意：
>
> 如果您将 Citrix Gateway 服务与 Workspace 配合使用，则无需将 AD 帐户与 Okta 组织同步。

要将 AD 用户和组与 Okta 组织同步，请执行以下操作：

1. 安装和配置 Okta AD 代理。有关完整说明，请参阅 Okta 网站上的以下文章：
   - 安装 Okta Active Directory 代理
   - 配置 Active Directory 导入和帐户设置

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 配置 Active Directory 置备设置

2. 通过执行手动导入或自动导入，将您的 AD 用户和组添加到 Okta。有关 Okta 导入方法和说明的详细信息，请参阅 Okta 网站上的 管理 Active Directory 用户和组 。

创建 **Okta OIDC Web** 应用程序集成

1. 在 Okta 管理控制台的 应用程序下，选择 应用程序。
2. 选择 创建应用程序集成。
3. 在登录方法中，选择 **OIDC - OpenID Connect**。
4. 在应用程序类型中，选择 **Web** 应用程序。选择下一步。
5. 在应用程序集成名称中，输入应用程序集成的友好名称。
6. 在授权类型中，选择授权码（默认选中）。
7. 在 登录重定向 **URI** 中，输入 `https://accounts.cloud.com/core/login-okta`。
8. 在 注销重定向 **URI** 中，输入来自 Citrix Cloud 的 Workspace URL。
9. 在“分配”下的“受控访问权限”中，选择是将应用程序集成分配给组织中的所有人，仅向您指定的组分配应用程序集成，还是稍后分配访问权限。
10. 选择保存。保存应用程序集成后，控制台将显示应用程序配置页面。
11. 在“客户端凭证”部分中，复制客户端 **ID** 和客户端密钥值。将 Citrix Cloud 连接到 Okta 组织时，您可以使用这些值。

配置 **Okta OIDC Web** 应用程序

在此步骤中，您将使用 Citrix Cloud 所需的设置配置 Okta OIDC Web 应用程序。Citrix Cloud 要求这些设置在订阅者登录其 Workspace 时通过 Okta 对他们进行身份验证。

1. （可选）更新隐式授权类型的客户端权限。如果您希望允许此授权类型的最小权限，则可以选择执行此步骤。
   a) 在 Okta 应用程序配置页面的“常规”选项卡上，滚动到“常规设置”部分，然后选择“编辑”。
   b) 在“应用程序”部分的“授权类型”中，在“代表用户操作的客户端”下，清除“允许使用隐式授予类型访问令牌”设置。
   c) 选择保存。
2. 添加应用程序属性。这些属性区分大小写。
   a) 从 Okta 控制台菜单中，选择 目录 **>** 配置文件编辑器。
   b) 选择 Okta 用户 **(**默认**)** 配置文件。Okta 显示用户配置文件页面。
   c) 在 属性下，选择添加属性。
   d) 输入以下信息：
      - 显示名称：cip_email
      - 变量名称：cip_email
      - 说明：AD 用户电子邮件

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 属性长度：选择“大于”，然后输入 **1**。
- 必需属性：是

e) 选择保存并添加另一个。

f) 输入以下信息：

- 显示名称：cip_sid
- 变量名：cip_sid
- 描述：AD 用户安全标识符
- 属性长度：选择“大于”，然后输入 **1**。
- 必需属性：是

g) 选择保存并添加另一个。

h) 输入以下信息：

- 显示名称：cip_upn
- 变量名称：cip_upn
- 描述：AD 用户主体名称
- 属性长度：选择“大于”，然后输入 **1**。
- 必需属性：是

i) 选择保存并添加另一个。

j) 输入以下信息：

- 显示名称：cip_oid
- 变量名称：cip_oid
- 描述：AD 用户 GUID
- 属性长度：选择“大于”，然后输入 **1**。
- 必需属性：是

k) 选择保存。

3. 编辑应用程序的属性映射：

a) 在 Okta 控制台中，选择目录 **>** 配置文件编辑器。

b) 找到您的 AD 的 **active_directory** 配置文件。此配置文件可能使用 `myDomain User` 格式进行标记，其中 `myDomain` 是您的集成 AD 域的名称。

c) 选择“映射”。将显示您的 AD 域的“用户个人资料映射”页面，并选中用于将 AD 映射到 Okta 用户的选项卡。

d) 在 **Okta** 用户用户配置文件列中，找到您在步骤 2 中创建的属性并按如下所示进行映射：

- 对于 `cip_email`，请从您的域名的“用户配置文件”列中选择 `email`。选中后，映射将显示为 `appuser.email`。
- 对于 `cip_sid`，请从您的域名的“用户配置文件”列中选择 `objectSid`。选中后，映射将显示为 `appuser.objectSid`。
- 对于 `cip_upn`，请从您的域名的“用户配置文件”列中选择 `userName`。选中后，映射将显示为 `appuser.userName`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 对于 `cip_oid`，请从您的域名的“用户配置文件”列中选择 `externalId`。选中后，映射将显示为 `appuser.externalId`。

e) 选择“保存映射”。
f) 选择“立即应用更新”。Okta 启动一项应用映射的作业。
g) 将 Okta 与您的 AD 同步。
   i. 在 Okta 控制台中，选择 目录 **>** 目录集成。
   ii. 选择您的集成 AD。
   iii. 选择“预配”选项卡。
   iv. 在“设置”下，选择“到 **Okta**”。
   v. 滚动到 **Okta** 属性映射部分，然后选择强制同步。

创建 **Okta API** 令牌

1. 使用只读管理员帐户登录 Okta 控制台。
2. 从 Okta 控制台菜单中，选择 安全 **> API**。
3. 选择令 牌 选项卡，然后选择 创建令牌。
4. 输入令牌的名称。
5. 选择 创建令牌。
6. 复制令牌值。将 Okta 组织连接到 Citrix Cloud 时，需要提供此值。

将 **Citrix Cloud** 连接到您的 **Okta** 组织

1. 通过 https://citrix.cloud.com登录 Citrix Cloud。
2. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
3. 找到 **Okta** ，然后从省略号菜单中选择连接。
4. 在 **Okta URL** 中，输入您的 Okta 域。
5. 在 **Okta API Token**（Okta API 令牌）中，输入您的 Okta 组织的 API 令牌。
6. 在 **Client ID**（客户端 ID）和 **Client Secret**（客户端密码）中，输入您之前创建的 OIDC Web 应用程序集成中的客户端 ID 和密码。要从 Okta 控制台复制这些值，请选择 **Applications**（应用程序）并找到您的 Okta 应用程序。在 **Client Credentials**（客户端凭据）下，对每个值使用 **Copy to Clipboard**（复制到剪贴板）按钮。
7. 单击 **Test and Finish**（测试并完成）。Citrix Cloud 会验证您的 Okta 详细信息并测试连接。

成功验证连接后，可以为 Workspace 订阅者启用 Okta 身份验证。

为 **Workspace** 启用 **Okta** 身份验证

1. 在 Citrix Cloud 菜单中，选择 **Workspace** 配置 **>** 身份验证。
2. 选择 **Okta**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 出现提示时，请选择 **I understand the impact on the subscriber experience**（我了解对订阅者体验产生的影响）。
4. 选择保存。

切换到 Okta 身份验证后，Citrix Cloud 会暂时禁用 Workspace 几分钟。重新启用 Workspace 后，您的订阅者可以使用 Okta 登录。

更多信息

- Citrix Tech Zone：
  - 技术洞察：身份验证-Okta
  - 技术简报：Workspace 身份
  - 技术简报：Workspace SSO

将 **SAML** 作为身份提供商连接到 **Citrix Cloud**

July 1, 2024

Citrix Cloud 支持使用 SAML（安全断言标记语言）作为身份提供程序来对登录其 Workspace 的 Citrix Cloud 管理员和订阅者进行身份验证。您可以将自己选择的 SAML 2.0 提供程序与本地 Active Directory (AD) 配合使用。

关于这篇文章

本文介绍了在 Citrix Cloud 和您的 SAML 提供商之间配置连接所需的步骤。其中一些步骤描述了您在 SAML 提供商的管理控制台中执行的操作。您用于执行这些操作的特定命令可能与本文中描述的命令有所不同，具体取决于您选择的 SAML 提供商。这些 SAML 提供程序命令仅作为示例提供。有关适用于 SAML 提供商的相应命令的更多信息，请参阅 SAML 提供商的文档。

SAML 提供商配置

Citrix 提供了以下配置指南，以确保您的 SAML 提供商与 Citrix Cloud 顺畅交互：

- 使用 Active Directory 联合服务 (ADFS) 的 SAML：请参阅使用 ADFS 在 Citrix Cloud 中配置 SAML 身份验证。
- 具有 Azure Active Directory 身份的 SAML：参见使用 Azure Active Directory 身份使用 SAML 登录 Workspace。
- 适用于 Azure AD 的 Citrix Cloud SAML SSO 应用程序：参见 Microsoft Azure AD 应用程序文档网站上的教程：Azure Active Directory 单点登录 (SSO) 与 Citrix Cloud SAML SSO 集成 。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 使用 Citrix Workspace 自定义域的 SAML：请参阅使用自定义域通过 SAML 登录 Workspace
- 使用 Okta 的 SAML：请参阅将 Okta 配置为 SAML 提供商以进行 Workspace 身份验证

支持的 **SAML** 提供商

支持官方 SAML 2.0 规范的 SAML 提供商可与 Citrix Cloud 配合使用。

Citrix 已经测试了以下 SAML 提供商，用于对 Citrix Cloud 管理员进行身份验证，以及使用单点登录 (SSO) 和单点注销 (SLO) 对 Citrix Workspace 订阅者进行身份验证。还支持未出现在此列表中的 SAML 提供商。

- Microsoft ADFS
- Microsoft Azure AD
- Duo
- Okta
- OneLogin
- PingOne SSO
- PingFederate

在测试这些提供程序时，Citrix 使用以下设置在 Citrix Cloud 控制台中配置 SAML 连接：

- 绑定机制：HTTP Post
- SAML 响应：对响应或断言进行签名
- 身份验证上下文：未指定、精确

这些设置的值是在您在 Citrix Cloud 中配置 SAML 连接时默认配置的。Citrix 建议在配置与所选 SAML 提供商的连接时使用这些设置。

有关这些设置的更多信息，请参阅本文中的将 SAML 提供程序元数据添加到 Citrix Cloud。

支持限定范围内的实体 **ID**

本文介绍如何使用单个 SAML 应用程序和 Citrix Cloud 的默认通用实体 ID 配置 SAML 身份验证。

如果您的 SAML 身份验证要求包括需要在单个 SAML 提供程序中使用多个 SAML 应用程序，请参阅在 Citrix Cloud 中使用限定范围内的实体 ID 配置 SAML 应用程序。

必备条件

在 Citrix Cloud 中使用 SAML 身份验证有以下要求：

- 支持 SAML 2.0 的 SAML 提供商。
- 本地 AD 域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 两个 Cloud Connector 部署到资源位置并加入到您的本地 AD 域。Cloud Connector 用于确保 Citrix Cloud 可以与您的资源位置进行通信。
- 与您的 SAML 提供商的 AD 集成。

Cloud Connector

您至少需要两 (2) 台服务器才能安装 Citrix Cloud Connector 软件。Citrix 建议至少使用两台服务器以 Cloud Connector 高可用性。这些服务器必须满足以下要求：

- 符合 Cloud Connector 技术详情中描述的系统要求。
- 未安装任何其他 Citrix 组件，不是 AD 域控制器，也不是对资源位置基础架构至关重要的计算机。
- 已加入您的资源所在的域。如果用户访问多个域中的资源，则需要在每个域中至少安装两个 Cloud Connector。
- 已连接到可以联系订阅者通过 Citrix Workspace 访问的资源的网络。
- 已连接到 Internet。有关详细信息，请参阅系统和连接要求。

有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。

Active Directory

在配置 SAML 身份验证之前，请执行以下任务：

- 验证您的 Workspace 订阅者在您的 AD 中是否有用户帐户。配置 SAML 身份验证后，没有 AD 帐户的订阅者无法成功登录其 Workspace。
- 通过在本地 AD 中部署 Cloud Connector，将 AD 连接到 Citrix Cloud 帐户。
- 将您的 AD 用户与 SAML 提供商同步。Citrix Cloud 要求您的 Workspace 订阅者具有 AD 用户属性，以便他们能够成功登录。

AD 用户属性　以下属性是所有 Active Directory 用户对象的必填属性，并且必须填充：

- 常见的名字
- SAM 帐户名
- User Principal Name (UPN)（用户主体名称 (UPN)）
- 对象 GUID
- SID

订阅者登录 Citrix Workspace 时，Citrix Cloud 使用您的 AD 中的对象 GUID 和 SID 属性来建立用户上下文。如果其中任何一个属性均未填充，则订阅者将无法登录。

在 Citrix Cloud 上使用 SAML 身份验证不需要以下属性，但 Citrix 建议填充这些属性以确保最佳的用户体验：

- 电子邮件地址
- 显示名称

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 使用“显示名称”属性在 Citrix Workspace 中正确显示订阅者的姓名。如果未填充此属性，订阅者仍然可以登录，但他们的姓名可能无法按预期显示。

SAML 与 **Active Directory** 集成

在启用 SAML 身份验证之前，您必须将本地 AD 与 SAML 提供商集成。此集成允许 SAML 提供商在 SAML 断言中将以下必需的 AD 用户属性传递给 Citrix Cloud：

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- 邮件（电子邮件）
- 显示名称 (displayName)

您可以配置这些属性的子集，前提是 SAML 断言中包含 SID 或 UPN 属性。Citrix Cloud 会根据需要从您的 AD 中检索其他属性。

> 注意：
>
> 为确保最佳性能，Citrix 建议配置本节中提到的所有属性。

尽管精确的集成步骤因 SAML 提供商而异，但集成过程通常包括以下任务：

1. 在 AD 域中安装同步代理，以便在域和 SAML 提供商之间建立连接。如果您使用 ADFS 作为 SAML 提供商，则无需执行此步骤。
2. 创建自定义属性并将其映射到本节前面提到的必需 AD 用户属性。本文中的 创建和映射自定义 SAML 属性 中介绍了此任务的一般步骤，以供参考。
3. 将您的 AD 用户与 SAML 提供商同步。

有关将 AD 与 SAML 提供商集成的更多信息，请查阅 SAML 提供商的产品文档。

使用 **SAML 2.0** 进行管理员身份验证

Citrix Cloud 支持使用 SAML 2.0 对 AD 中管理员组的成员进行身份验证。有关向 Citrix Cloud 添加管理员组的更多信息，请参阅 管理管理员组。

使用现有 **SAML** 连接进行管理员身份验证

如果您已在 Citrix Cloud 中拥有 SAML 2.0 连接并希望使用它对管理员进行身份验证，则必须先在 身份和访问管理 中断开 SAML 2.0 连接，然后重新配置连接。如果您使用 SAML 连接对 Citrix Workspace 订阅者进行身份验证，则还必须在 **Workspace** 配置中禁用 SAML 身份验证方法。重新配置 SAML 连接后，您可以将管理员组添加到 Citrix Cloud。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您在未先断开连接并重新连接 SAML 2.0 的情况下尝试添加管理员组，则不会显示将管理员组添加到 Citrix Cloud 中描述的 **Active Directory** 身份选项。

设置新 **SAML** 连接的任务概述

要在 Citrix Cloud 中设置新的 SAML 2.0 连接，请执行以下任务：

1. 在 身份和访问管理中，按照将 Active Directory 连接到 Citrix Cloud 中所述，将本地 AD 连接到 Citrix Cloud。
2. 按照本文中的 SAML 与 Active Directory 集成中所述，将 SAML 提供商与本地 AD 集成。
3. 配置管理员可用于登录 Citrix Cloud 的登录 URL 。
4. 在 身份和访问管理中，在 Citrix Cloud 中 配置 SAML 身份验证 。此任务包括使用来自 Citrix Cloud 的 SAML 元数据配置 SAML 提供商，然后使用来自 SAML 提供商的元数据配置 Citrix Cloud 以创建 SAML 连接。

Citrix Cloud 管理员使用现有 **SAML** 连接的任务概述

如果您在 Citrix Cloud 中已有 SAML 2.0 连接，并且想要将其用于管理员身份验证，请执行以下任务：

1. 如果适用，请禁用 SAML 2.0 Workspace 身份验证：在 **Workspace** 配置 **>** 身份验证中，选择其他身份验证方法，然后在出现提示时选择 确认。
2. 断开现有的 SAML 2.0 连接：在 身份和访问管理 **>** 身份验证中，找到 SAML 连接。从最右侧的省略号菜单中，选择 断开连接。选择 是，断开连接 以确认操作。
3. 重新连接 SAML 2.0 并配置连接：在 **SAML 2.0** 的省略号菜单中，选择 连接。
4. 出现提示时，输入管理员用于 登录的登录 URL 的唯一标识符。
5. 按照本文中的 配置 SAML 提供程序元数据中所述配置 SAML 连接。

配置 SAML 连接后，您可以将 AD 管理员组添加到 Citrix Cloud，如 管理管理员组中所述。您还可以 为 Workspace 订阅者重新启用 SAML ，如本文所述。

创建和映射自定义 **SAML** 属性

如果您已经在 SAML 提供商中配置了 SID、UPN、OID、电子邮件和 displayName 属性的自定义属性，则无需执行此任务。继续执行 创建 SAML 连接器应用程序 并使用步骤 5 中的现有自定义 SAML 属性。

> 注意：
>
> 本节中的步骤描述了您在 SAML 提供商的管理控制台中执行的操作。用于执行这些操作的特定命令可能与本部分中描述的命令有所不同，具体取决于您选择的 SAML 提供商。本节中的 SAML 提供程序命令仅作为示例提供。有关适用于 SAML 提供商的相应命令的更多信息，请参阅 SAML 提供商的文档。

1. 登录 SAML 提供商的管理控制台，然后选择用于创建自定义用户属性的选项。例如，根据您的 SAML 提供商的控制台，您可以选择用户 **>** 自定义用户字段 **>** 新建用户字段。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 为以下 AD 属性添加属性。使用显示的默认值命名属性。

AD 属性	必需或可选	默认值
userPrincipalName	如果未为 SID 添加属性，则为必填项（推荐）。	`cip_upn`
objectSID	如果不为 UPN 添加属性，则为必填项。	`cip_sid`
objectGUID	对身份验证而言是可选项	`cip_oid`
mail	对身份验证而言是可选项	`cip_email`
displayName	Workspace 用户界面所必需	`displayName`
givenName	Workspace 用户界面所必需	`firstName`
sn	Workspace 用户界面所必需	`lastName`
AD 林	对身份验证而言是可选项	`cip_forest`
AD 域	对身份验证而言是可选项	`cip_domain`

3. 选择您与 Citrix Cloud 连接的 AD。例如，根据您的 SAML 提供商的控制台，您可以选择用户 **>** 目录。
4. 选择用于添加目录属性的选项。例如，根据您的 SAML 提供商的控制台，您可以选择 目录属性。
5. 选择用于添加属性的选项，并将以下 AD 属性映射到您在步骤 2 中创建的自定义用户属性：
   - 如果您在步骤 2 中添加了 SID 的属性（例如 `cip_sid`），请选择 **objectSid** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了 UPN 的属性（例如 `cip_upn`），请选择 **userPrincipalName** 并映射到您创建的属性。
   - 如果您在步骤 2 中为 ObjectGUID 添加了属性（例如 `cip_oid`），请选择 **ObjectGUID** 并映射到您创建的属性。
   - 如果您在步骤 2 中添加了“邮件”的属性（例如 `cip_email`），请选择 “**mail**” 并映射到您创建的属性。
   - 如果您在步骤 2 中为“显示名称”添加了属性（例如，`displayName`），请选择 **displayName** 并映射到您创建的属性。

配置管理员登录 **URL**

1. 通过 https://citrix.cloud.com登录 Citrix Cloud。
2. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
3. 找到 **SAML 2.0** ，然后从省略号菜单中选择连接。
4. 出现提示时，为贵公司输入一个简短的 URL 友好型标识符，然后选择 保存并继续。此时 将显示配置 **SAML** 页面。
5. 继续下一部分以配置与 Citrix Cloud 的 SAML 连接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置 **SAML** 提供程序元数据

在此任务中，您将使用来自 Citrix Cloud 的 SAML 元数据创建连接器应用程序。配置 SAML 应用程序后，您可以使用连接器应用程序中的 SAML 元数据来配置与 Citrix Cloud 的 SAML 连接。

> 注意：
>
> 本节中的一些步骤描述了您在 SAML 提供商的管理控制台中执行的操作。用于执行这些操作的特定命令可能与本部分中描述的命令有所不同，具体取决于您选择的 SAML 提供商。本节中的 SAML 提供程序命令仅作为示例提供。有关适用于 SAML 提供商的相应命令的更多信息，请参阅 SAML 提供商的文档。

创建 **SAML** 连接器应用程序

1. 从 SAML 提供商的管理控制台中，为身份提供商添加具有属性和签名响应的应用程序。例如，根据提供商的控制台，您可以选择应用程序 **>** 应用程序 **>** 添加应用程序，然后选择 **SAML** 测试连接器（带符号响应的 **IdP w/attr**）。
2. 如果适用，请输入显示名称并保存应用程序。
3. 在 Citrix Cloud 的 配置 **SAML** 屏幕中，在 **SAML** 元数据中，选择 下载。元数据 XML 文件将显示在另一个浏览器选项卡中。

   > 注意：
   >
   > 如果需要，也可以从下载此文件 `https://saml.cloud.com/saml/metadata.xml`。在导入和监视 SAML 提供商元数据时，此端点可能对某些身份提供商更友好。

4. 输入连接器应用程序的以下详细信息：
   - 在“受 众”字段中，输入 `https://saml.cloud.com`。
   - 在“收 件人”字段中，输入 `https://saml.cloud.com/saml/acs`。
   - 在 ACS URL 验证器的字段中，输入 `https://saml.cloud.com/saml/acs`。
   - 在 ACS URL 的字段中，输入 `https://saml.cloud.com/saml/acs`。
5. 在应用程序中添加自定义 SAML 属性作为参数值：

创建此字段	分配此自定义属性
cip_sid	您为 SID 创建的自定义属性。示例：cip_sid
cip_upn	您为 UPN 创建的自定义属性。示例：cip_upn
cip_oid	您为 ObjectGUID 创建的自定义属性。示例：cip_oid
cip_email	您为邮件创建的自定义属性。示例：cip_email
displayName	您为“显示名称”创建的自定义属性。示例：displayName

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

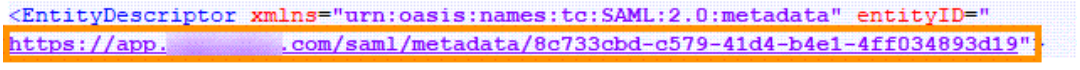
6. 将您的 Workspace 订阅者添加为用户，以允许他们访问应用程序。

将 **SAML** 提供商元数据添加到 **Citrix Cloud**

1. 从 SAML 提供商处获取 SAML 元数据。下图是此文件外观的示例：

2. 在 Citrix Cloud 的 配置 **SAML** 屏幕中，从 SAML 提供商的元数据文件中输入以下值：

   - 在身份提供者实体 **ID** 中，输入元数据中 **EntityDescriptor** 元素中的 **entityID** 值。

   - 在 签名身份验证请求中，选择 是 以允许 Citrix Cloud 对身份验证请求进行签名，证明这些请求来自 Citrix Cloud 而不是恶意行为者。如果您希望将 Citrix ACS URL 添加到 SAML 提供商用于安全发布 SAML 响应的允许列表中，请选择“否”。

   - 在 **SSO** 服务 **URL** 中，输入要使用的绑定机制的 URL。您可以使用 HTTP-POST 或 HTTP 重定向绑定。在元数据文件中，找到绑定值为 **HTTP-POST** 或 **HTTP** 重定向的 **SingleSignOnService** 元素。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在 绑定机制中，选择与从元数据文件中选择的 SSO 服务 URL 的绑定匹配的机制。默认情况下，“**HTTP Post**”处于选中状态。
- 在 **SAML** 响应中，选择您的 SAML 提供商用于 SAML 响应和 SAML 断言的签名方法。默认情况下，选择“签名响应或断言”。Citrix Cloud 会拒绝任何未按此字段中指定的方式签名的响应。

3. 在 SAML 提供商的管理控制台中，执行以下操作：
   - 选择 **SHA-256** 作为 SAML 签名算法。
   - 将 X.509 证书下载为 Base64 编码的 PEM、CRT 或 CER 文件。
4. 在 Citrix Cloud 的“配置 **SAML**”页面上，在 **X.509** 证书中，选择“上载文件”，然后选择您在上一步中下载的证书文件。
5. 选择继续以完成上载。
6. 在 身份验证上下文中，选择要使用的上下文以及希望 Citrix Cloud 强制执行此上下文的严格程度。选择最小可在所选上下文中请求身份验证，而不在该上下文中强制执行身份验证。选择“精确”可在选定的上下文中请求身份验证，并仅在该上下文中强制执行身份验证。如果您的 SAML 提供程序不支持身份验证上下文，或者您选择不使用它们，请选择未指定和最小值。默认情况下，选择“未指定”和“精确”。
7. 对于注销 **URL** （可选），请决定是否希望退出 Citrix Workspace 或 Citrix Cloud 的用户同时退出他们之前通过 SAML 提供商登录的所有网络应用程序。
   - 如果您希望用户在退出 Citrix Workspace 或 Citrix Cloud 后保持其网络应用程序的登录状态，请将注销 **URL** 字段留空。
   - 如果您希望用户在退出 Citrix Workspace 或 Citrix Cloud 后退出所有 Web 应用程序，请输入您的 SAML 提供商提供的 SingleLogout (SLO) 端点。如果您使用 Microsoft ADFS 或 Azure Active Directory Active Directory 作为 SAML 提供者，则 SLO 端点与单点登录 (SSO) 端点相同。

8. 验证 Citrix Cloud 中的以下默认属性值是否与 SAML 提供商中配置的相应属性值相匹配。为了让 Citrix Cloud 在 SAML 断言中找到这些属性，此处输入的值必须与您的 SAML 提供商中的值相匹配。如果您没有在 SAML 提供商中配置特定属性，则可以在 Citrix Cloud 中使用默认值或将该字段留空，除非另有说明。
   - 用户显示名称的属性名称：默认值为 `displayName`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 用户给定名称的属性名称：默认值为 `firstName`。
- 用户姓氏的属性名称：默认值为 `lastName`。
- 安全标识符 **(SID)** 的属性名称：如果您没有为 UPN 创建属性，则必须输入 SAML 提供商提供的此属性名称。默认值为 `cip_sid`。
- 用户主体名称 **(UPN)** 的属性名称：如果您没有为 SID 创建属性，则必须输入 SAML 提供商提供的此属性名称。默认值为 `cip_upn`。
- 电子邮件的属性名称：默认值为 `cip_email`。
- **AD** 对象标识符 **(OID)** 的属性名称：默认值为 `cip_oid`。
- **AD** 林的属性名称：默认值为 `cip_forest`。
- **AD** 域的属性名称：默认值为 `cip_domain`。

9. 选择 测试和完成 以验证是否已成功配置连接。

从 **AD** 向 **Citrix Cloud** 添加管理员

有关在 Citrix Cloud 中添加和管理 AD 组的说明，请参阅 管理管理员组。

为 **Workspace** 启用 **SAML** 身份验证

1. 在 Citrix Cloud 菜单中，选择 **Workspace** 配置。
2. 选择“身份验证”选项卡
3. 选择 **SAML 2.0**。

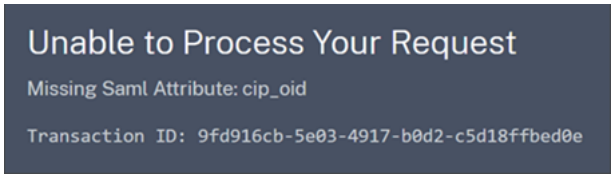
故障排除

属性错误

在以下任何一种情况下，都可能出现属性错误：

- 您的 SAML 配置中的必填属性编码不正确。
- SAML 断言中缺少 `cip_sid` 和 `cip_upn` 属性。
- SAML 断言中缺少 `cip_sid` 或 `cip_oid` 属性，由于连接问题，Citrix Cloud 无法从 Active Directory 中检索它们。

发生属性错误时，Citrix Cloud 会显示一条包含错误属性的错误消息。



要解决此类错误，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 确保您的 SAML 提供商使用正确的编码发送所需的属性，如下表所示。至少必须包含 SID 或 UPN 属性。

属性	编码	必需
cip_email	必须为字符串格式 (`user@domain`)	
cip_oid	必须为 Base64 或字符串格式	
cip_sid	必须为 Base64 或字符串格式	是，如果不使用 `cip_upn`
cip_upn	必须为字符串格式 (`user@domain`)	是，如果不使用 `cip_sid`

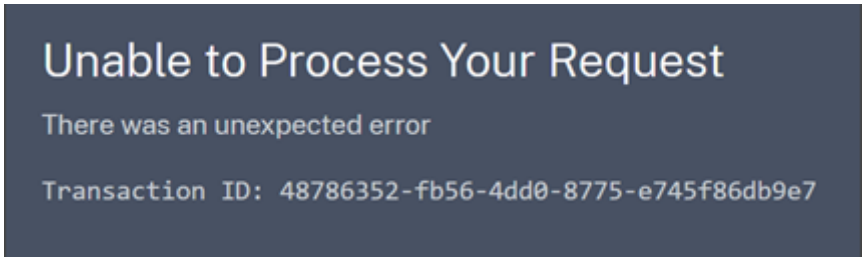
2. 验证 Cloud Connector 是否在线且运行正常，以便 Citrix Cloud 可以检索所需的任何缺失属性。有关更多信息，请参阅 Cloud Connector 高级运行状况检查。

意外错误

在以下情况下，Citrix Cloud 可能会遇到意外错误：

- 用户使用 IDP 发起的流程发起 SAML 请求。例如，请求是通过身份提供商的应用程序门户选择磁贴，而不是直接导航到 Workspace URL (`customer.cloud.com`) 来发出的。
- SAML 证书无效或已过期。
- 身份验证上下文无效。
- SAML 断言和响应签名不匹配。

发生此错误时，Citrix Cloud 将显示一条一般错误消息。



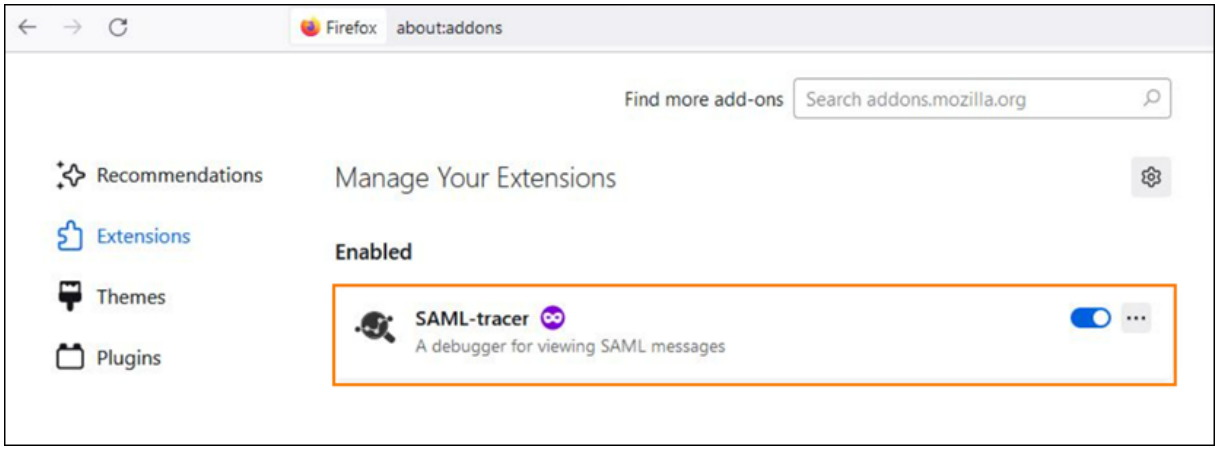
如果通过身份提供商的应用程序门户导航到 Citrix Cloud 导致此错误，则可以使用以下解决方法：

1. 在身份提供商的应用程序门户中创建引用您的 Workspace URL 的书签应用程序（例如，`https://customer.cloud.com`）。
2. 将用户分配给 SAML 应用程序和书签应用程序。
3. 更改 SAML 应用程序和书签应用程序的可见性设置，以便在应用程序门户中显示书签应用程序并隐藏 SAML 应用程序。
4. 禁用 Workspace 配置中的联合身份提供商会话设置以删除其他密码提示。有关说明，请参阅 Citrix Workspace 产品文档中的联邦身份提供商会话。

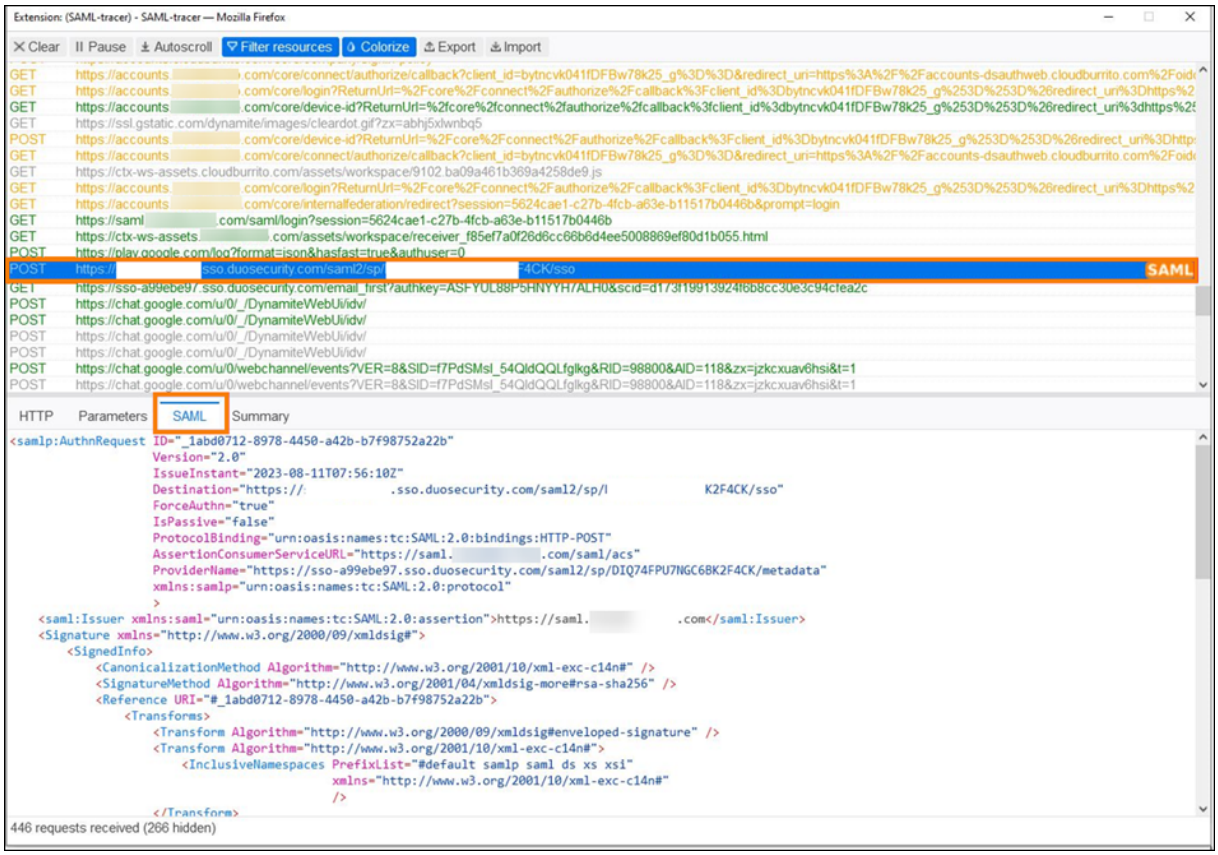
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

调试建议

Citrix 建议在所有 SAML 调试中使用 SAML-Tracer 浏览器扩展程序。此扩展程序适用于大多数常见的网络浏览器。该扩展程序将 Base64 编码的请求和响应解码为 SAML XML，这样它们便于人类阅读。



作为管理员，此工具允许您检查发送给用户的 SAML 属性的值，并查找 SAML 请求和响应中是否存在签名。如果您在 SAML 相关问题上需要帮助，Citrix 支持部门会请求 SAML-Tracer 文件以了解问题并解决您的支持案例。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更多信息

- Microsoft 文档：教程：Azure Active Directory 单点登录 (SSO) 与 Citrix Cloud SAML SSO 集成
- 使用 Active Directory 联合身份验证服务 (ADFS) 的 SAML：使用 ADFS 在 Citrix Cloud 中配置 SAML 身份验证
- Citrix Tech Zone：技术见解：身份验证 - SAML

在 **Citrix Cloud** 中使用限定范围内的实体 **ID** 配置 **SAML** 应用程序

December 14, 2023

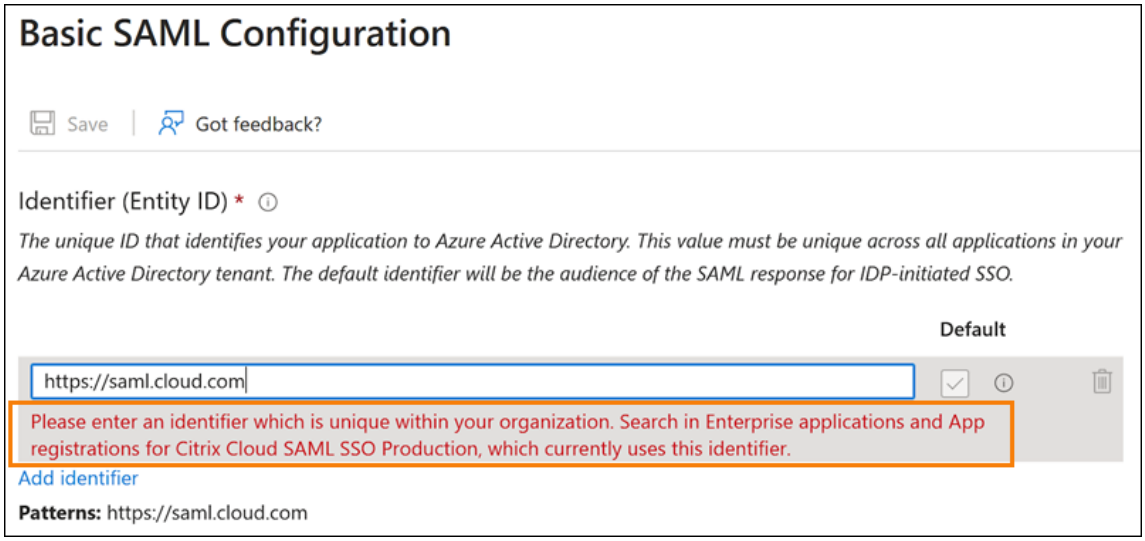
Author:
Mark Dear

本文介绍如何在同一 SAML 提供程序中配置多个 SAML 应用程序。

某些 SAML 提供商，例如 Azure Active Directory (AD)、Active Directory 联合服务 (ADFS)、PingFederate 和 PingSSO，禁止在多个 SAML 应用程序中重复使用相同的服务提供商 (SP) 实体 ID。因此，在同一 SAML 提供程序中创建两个或更多不同的 SAML 应用程序的管理员无法将它们链接到相同或不同的 Citrix Cloud 租户。尝试使用相同的 SP 实体 ID 创建第二个 SAML 应用程序，例如 `https:\\saml.cloud.com`，当现有的 SAML 应用程序已经在使用它时，会在 SAML 提供程序上触发错误，表明该实体 ID 已在使用中。

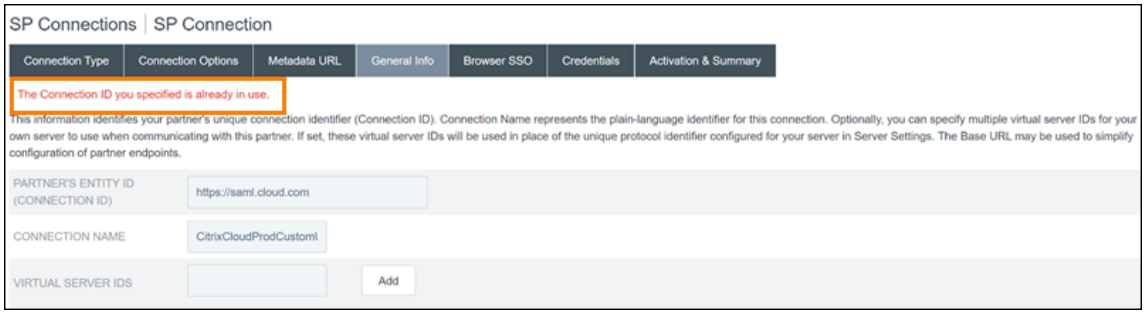
下图说明了此错误：

- 在 Azure Active Directory 中



- 在 PingFederate 中：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix Cloud 中限定范围内的实体 ID 功能解决了这一限制，因此您可以在 SAML 提供程序（例如 Azure AD 租户）中创建多个 SAML 应用程序，并将其链接到单个 Citrix Cloud 租户。

什么是实体 **ID**

SAML 实体 ID 是一个唯一标识符，用于在 SAML 身份验证和授权协议中标识特定实体。通常，实体 ID 是分配给实体并用于 SAML 消息和元数据的 URL 或 URI。您在 SAML 提供商中创建的每个 SAML 应用程序都被视为一个独特的实体。

例如，在 Citrix Cloud 和 Azure AD 之间的 SAML 连接中，Citrix Cloud 是服务提供商 (SP)，Azure AD 是 SAML 提供商。两者都有一个实体 ID，必须在 SAML 连接的另一端进行配置。这意味着必须在 Azure AD 中配置 Citrix Cloud 的实体 ID，并且 Azure AD 的实体 ID 必须在 Citrix Cloud 中配置。

以下实体 ID 是 Citrix Cloud 中通用实体 ID 和限定范围内的实体 ID 的示例：

- 通用：`https://saml.cloud.com`
- 限定范围：`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

按地区划分的通用和限定范围内的 **SP** 实体 **ID**

Citrix Cloud 中的现有 SAML 连接（在 2023 年 11 月之前创建）对每个 SAML 连接和 Citrix Cloud 租户使用相同的通用实体 ID。只有新的 Citrix Cloud SAML 连接才提供使用限定范围内的实体 ID 的选项。

如果您选择将限定范围内的实体 ID 用于新连接，则任何现有的 SAML 连接将继续使用其原始通用实体 ID 运行。

下表列出了每个 Citrix Cloud 区域的通用和限定范围内的 SP 实体 ID：

Citrix Cloud 区域	通用 SP 实体 ID	限定范围内的实体 ID
美国、欧盟、亚太南部	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 区域	通用 SP 实体 ID	限定范围内的实体 ID
日本	https://saml.citrixcloud.jp	https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29
政府	https://saml.cloud.us	https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820

为新的和现有的 **SAML** 连接生成唯一的 **SP** 实体 **ID**

当您创建新的 SAML 连接时，Citrix Cloud 会生成一个唯一 ID (GUID)。要生成限定范围内的实体 ID，请在创建新连接时启用配置限定范围内的 **SAML** 实体 **ID** 设置。

如果要更新现有 SAML 连接以使用限定范围内的实体 ID，则必须断开 SAML 提供程序与 Citrix Cloud 中的身份和访问管理 **>** 身份验证页面的连接，然后将其重新连接。Citrix Cloud 不允许您直接编辑现有 SAML 连接。但是，您可以克隆配置并修改克隆。

> 重要：
>
> 在完成 SAML 连接过程之前将其关闭，会丢弃 Citrix Cloud 自动生成的实体 ID。当您重启 SAML 连接过程时，Citrix Cloud 会生成一个新的限定范围内的实体 ID GUID。配置 SAML 提供程序时，请使用这个新的限定范围内的实体 ID。如果您要更新现有 SAML 连接以使用限定范围内的实体 ID，则必须使用 Citrix Cloud 生成的限定范围内的 ID 更新该连接的 SAML 应用程序。

有关限定范围内的实体 **ID** 的常见问题

我能否在同一 **Azure AD** 租户中创建多个 **Azure AD SAML** 应用程序并将其链接到一个或多个 **Citrix Cloud** 租户

Citrix Cloud 的限定范围内的实体 ID 功能解决了某些 SAML 提供商施加的防止重复实体 ID 的限制。使用此功能，您可以在 Azure AD 租户中预置多个 SAML 应用程序，并使用来自单个 Citrix Cloud 租户的限定范围内的实体 ID 配置每个应用程序。

我还能将相同的 **Azure AD SAML** 应用程序链接到多个 **Citrix Cloud** 租户吗

这种情况在 Citrix Cloud 客户中很常见，Citrix 将继续支持这种情况。要实现此方案，您必须满足以下要求：

- 使用通用实体 ID，例如 https://saml.cloud.com。
- 不要为你的 SAML 连接启用限定范围内的实体 ID。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如何决定是否在我的 **SAML** 提供商中使用限定范围内的实体 **ID**

Citrix Cloud 中的限定范围内的实体 ID 允许您根据要求灵活使用通用或限定范围内的实体 ID。考虑您需要的 SAML 应用程序的数量以及您拥有的 Citrix Cloud 租户的数量。此外，请考虑每个租户是否可以共享现有的 SAML 应用程序或需要自己的限定范围内的 SAML 应用程序。

> 重要：
>
> 如果您的 SAML 提供商已经允许您使用相同的实体 ID 创建多个 SAML 应用程序（例如 `https://saml.cloud.com`），则无需启用限定范围内的实体 ID 或对现有 SAML 配置进行任何更改。您无需在 Citrix Cloud 或 SAML 应用程序中更新任何设置。

受影响的 **SAML** 提供商

下表列出了允许或限制使用重复实体 ID 的 SAML 提供商。

SAML 提供商	支持重复的实体 ID
Azure AD（云端）	否
ADFS（本地）	否
PingFederate（本地）	否
PingOneSSO（云端）	否
Okta（云端）	是
Duo（云端）	是
OneLogin（云端）	是

受影响的用例

下表根据您的用例所需的 SAML 应用程序，说明是否支持通用或限定范围内的实体 ID，以及您的 SAML 提供商是否支持重复的实体 ID。

用例要求	SAML 提供商支持重复的实体 ID?	支持的配置
只有一个 SAML 应用程序	是	通用或限定范围内的实体 ID
只有一个 SAML 应用程序	否	通用或限定范围内的实体 ID
两个或多个 SAML 应用程序	是	通用或限定范围内的实体 ID
两个或多个 SAML 应用程序	否	限定范围内的实体 ID

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用例要求	SAML 提供商支持重复的实体 ID?	支持的配置
Workspace 自定义 URL 和 SAML 应用程序对	是	通用或限定范围内的实体 ID
Workspace 自定义 URL 和 SAML 应用程序对	否	限定范围内的实体 ID
将同一 SAML 应用程序关联到多个 Citrix Cloud 租户	是	通用实体 ID
将同一 SAML 应用程序关联到多个 Citrix Cloud 租户	否	通用实体 ID

使用限定范围内的实体 **ID** 配置主 **SAML** 连接

在此任务中，您将使用主 SAML 应用程序（SAML 应用程序 1）的限定范围内的实体 ID 在 Citrix Cloud 中创建 SAML 连接。

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
2. 在“身份验证”选项卡上，找到 **SAML 2.0**，然后从省略号菜单中选择“连接”。
3. 当系统提示您创建唯一的登录 URL 时，输入贵公司的简短 URL 友好标识符（例如 `https://citrix.cloud.com/go/mycompany`），然后选择“保存并继续”。此标识符在 Citrix Cloud 中必须是唯一的。
4. 在“配置 **SAML** 身份提供商”下，选择 配置限定范围内的 **SAML** 实体 **ID**。Citrix Cloud 会自动生成限定范围内的实体 ID，并填充实体 ID、断言使用者服务和注销 URL 的字段。
5. 在配置与 **Citrix Cloud** 的 **SAML** 连接下，输入您的 SAML 提供商提供的连接详情。
6. 接受默认 SAML 属性映射。
7. 选择“测试并完成”。

使用通用实体 **ID** 配置主 **SAML** 连接

在此任务中，您将使用主 SAML 应用程序（SAML 应用程序 1）的默认通用实体 ID 在 Citrix Cloud 中创建 SAML 连接。

1. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
2. 在“身份验证”选项卡上，找到 **SAML 2.0**，然后从省略号菜单中选择“连接”。
3. 当系统提示您创建唯一的登录 URL 时，输入贵公司的简短 URL 友好标识符（例如 `https://citrix.cloud.com/go/mycompany`），然后选择“保存并继续”。此标识符在 Citrix Cloud 中必须是唯一的。
4. 在“配置 **SAML** 身份提供商”下，验证配置限定范围内的 **SAML** 实体 **ID** 是否已禁用。
5. 在配置与 **Citrix Cloud** 的 **SAML** 连接下，输入您的 SAML 提供商提供的连接详情。
6. 如果需要，在 服务提供商 **SAML** 元数据中，单击“下载”以获取通用 SAML 元数据的副本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

7. 接受默认 SAML 属性映射。
8. 选择“测试并完成”。

使用 **Citrix Workspace** 定制域配置 **SAML** 连接

本部分包括使用限定范围内的或通用实体 ID 的自定义 Workspace URL 配置 SAML 连接。

本节中的任务仅在您拥有用于 SAML 的现有自定义 Workspace URL 时适用。如果您没有使用带有 SAML 身份验证的自定义 Workspace URL，则可以跳过本节中的任务。

有关更多信息，请参阅以下文章：

- 配置自定义域
- 使用自定义域通过 SAML 登录 Workspace

使用 **Workspace** 自定义 **URL** 和通用实体 **ID** 配置 **SAML** 连接

在此任务中，“配置限定范围内的实体 **ID** 设置被禁用。

1. 从 Citrix Cloud 菜单中，选择 **Workspace** 身份验证。
2. 在“自定义 **Workspace URL**”中，从省略号菜单中选择“编辑”。
3. 选择同时使用 **[customerName] .cloud.com URL** 和自定义域 **URL**。
4. 输入 SAML 应用程序 2 的通用实体 ID、SSO URL 和可选 SLO URL，然后上载您之前从 SAML 提供商处下载的签名证书。
5. 如果需要，在自定义域的服务提供商 **SAML** 元数据中，单击下载以获取 Workspace 自定义 URL SAML 应用程序的通用 SAML 元数据的副本。
6. 单击保存。

使用 **Workspace** 自定义 **URL** 和限定范围内的实体 **ID** 配置 **SAML** 连接

在此任务中，启用了配置限定范围内的实体 **ID** 设置。

1. 从 Citrix Cloud 菜单中，选择 **Workspace** 身份验证。
2. 在“自定义 **Workspace URL**”中，从省略号菜单中选择“编辑”。
3. 选择同时使用 **[customerName] .cloud.com URL** 和自定义域 **URL**。
4. 输入 SAML 应用程序 2 的限定范围内的实体 ID、SSO URL 和可选 SLO URL，然后上载您之前从 SAML 提供商处下载的 SAML 签名证书。
5. 单击保存。

保存配置后，Citrix Cloud 会生成包含正确 GUID 的限定范围内的 SAML 元数据。如果需要，您可以获取 Workspace 自定义 URL SAML 应用程序的限定范围内的元数据的副本。

1. 在“身份和访问管理”页面上，找到 SAML 连接，然后从省略号菜单中选择“查看”。

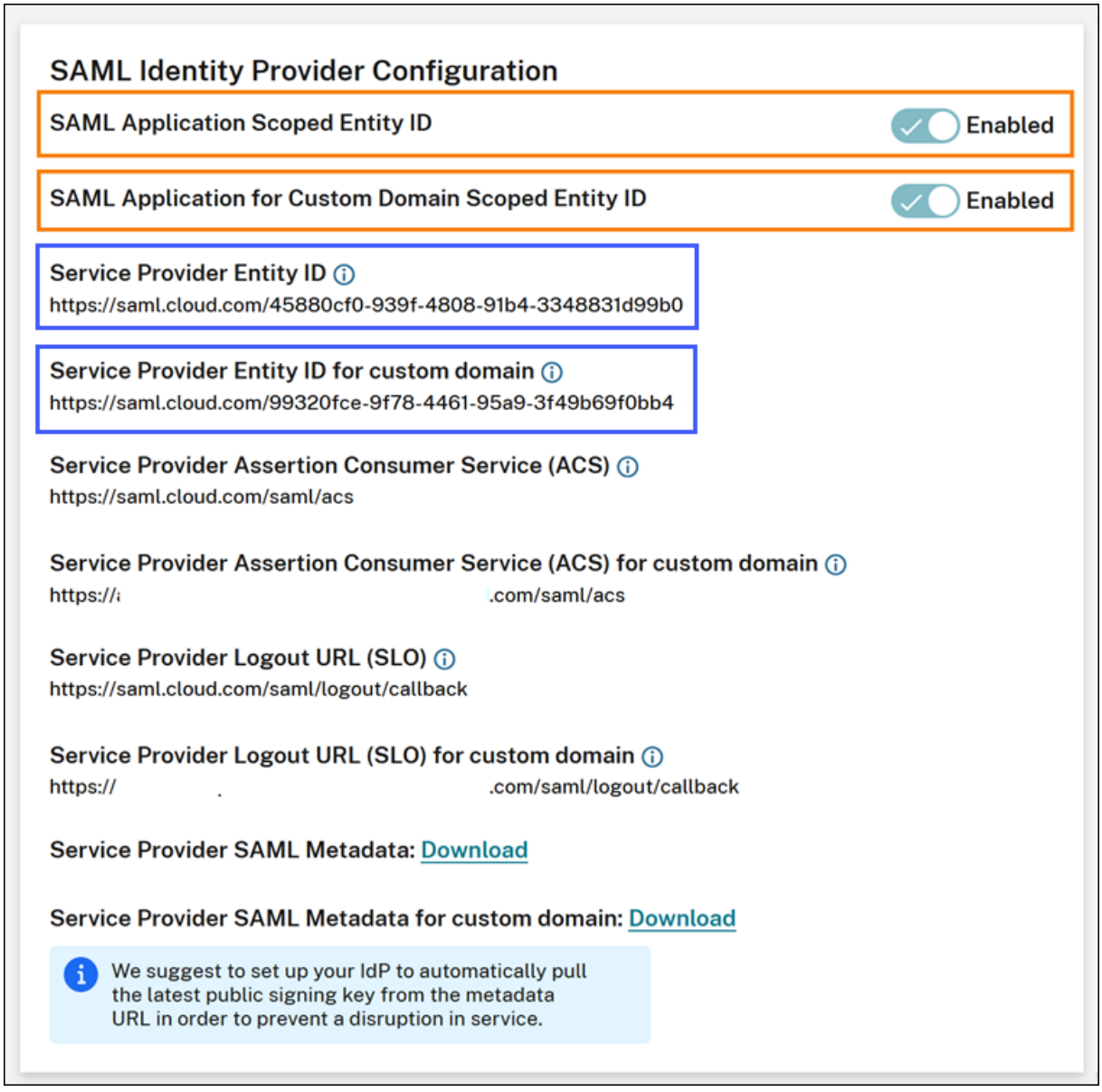
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

2. 在 自定义域的服务提供商 **SAML** 元数据中，单击 下载。

查看主 **Workspace URL** 和自定义 **Workspace URL SAML** 应用程序的 **SAML** 配置

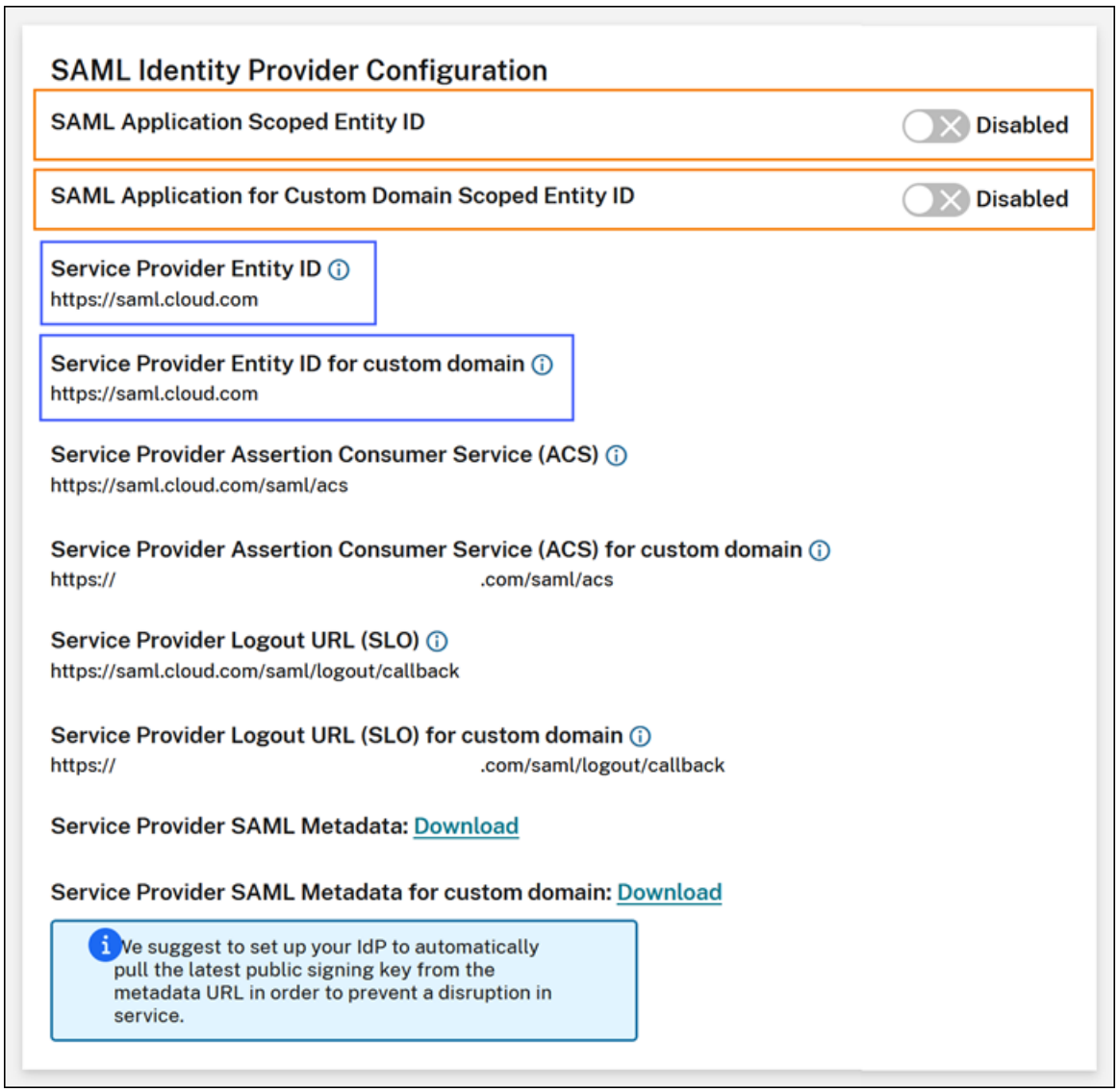
查看您的限定范围内的 SAML 连接的配置详细信息时，Citrix Cloud 会显示主 SAML 应用程序和 Workspace 自定义域 SAML 应用程序的限定范围内的实体 ID 设置。

例如，启用限定范围内的实体 ID 时，自定义域字段的服务提供商实体 **ID** 和服务提供商实体 **ID** 包含 Citrix Cloud 生成的限定范围内的实体 ID。



禁用限定范围内的实体 ID 时，自定义域字段的服务提供商实体 **ID** 和服务提供商实体 **ID** 包含通用实体 ID。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



您可以通过将限定范围内的实体 ID 附加到现有实体 ID 值来更新 SAML 提供商中的现有 SAML 应用程序。

限定范围内的实体 **ID** 的 **SAML** 提供商配置

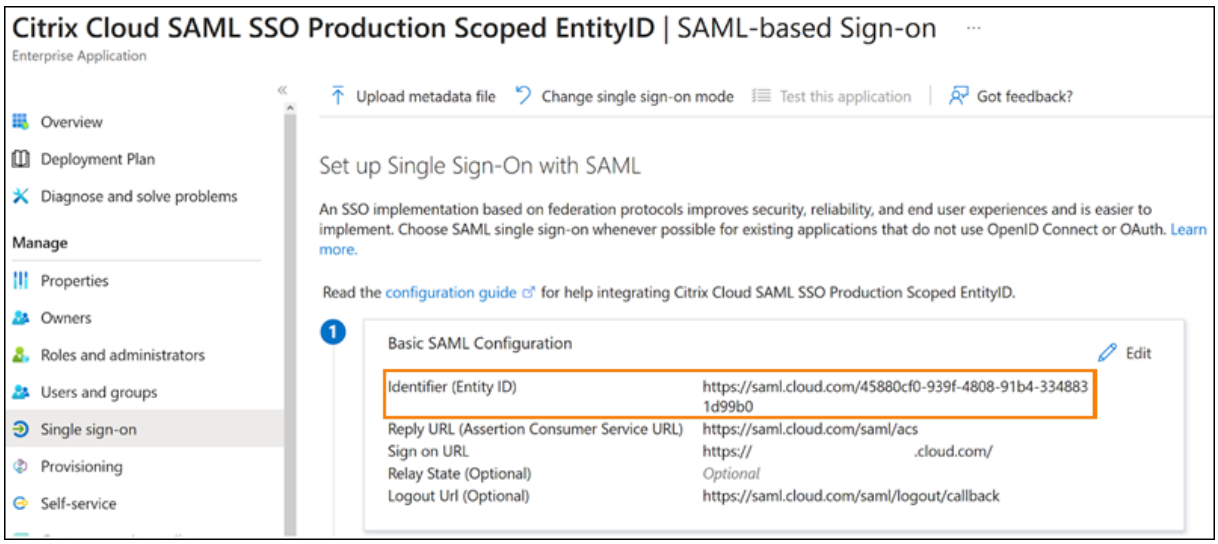
在 Citrix Cloud 中使用限定范围内的实体 ID 配置 SAML 连接后，您可以将限定范围内的实体 ID 添加到您的 SAML 提供程序。

本节包括来自 Azure AD 和 PingFederate 的配置示例。

限定范围内的实体 **ID** 的 **Azure AD SAML** 配置

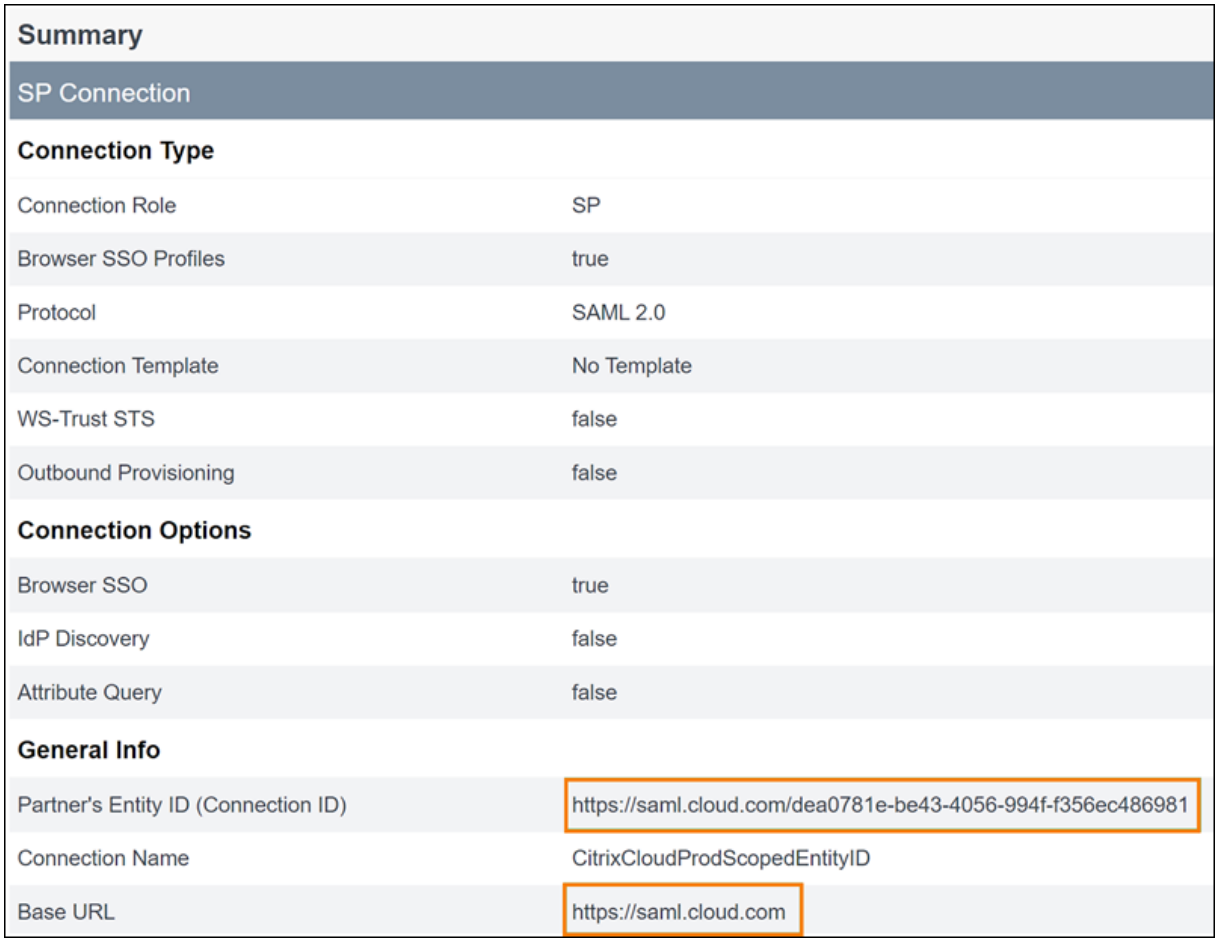
在此示例中，在 Azure AD 的标识符字段中输入来自 Citrix Cloud 的限定范围内的实体 ID。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



带限定范围内的实体 **ID** 的 **PingFederate SAML** 配置

在此示例中，在“合作伙伴的实体 **ID**”字段和“基本 **URL**”字段中分别填充了 Citrix Cloud 中指定限定范围内的实体 ID 和通用实体 ID。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

故障排除

Citrix 建议使用 SAML-tracer 浏览器扩展来解决 SAML 配置中的任何问题。此扩展程序将 Base64 编码的请求和响应解码为 SAML XML，从而使信息呈现人类可读性。您可以使用 SAML-tracer 扩展来检查 Citrix Cloud（服务提供商）生成并发送给您的 SAML 提供商（身份提供商）的 SSO 和 SLO SAML 请求。扩展可以显示两个请求中是否都包含实体 ID 范围 (GUID)。

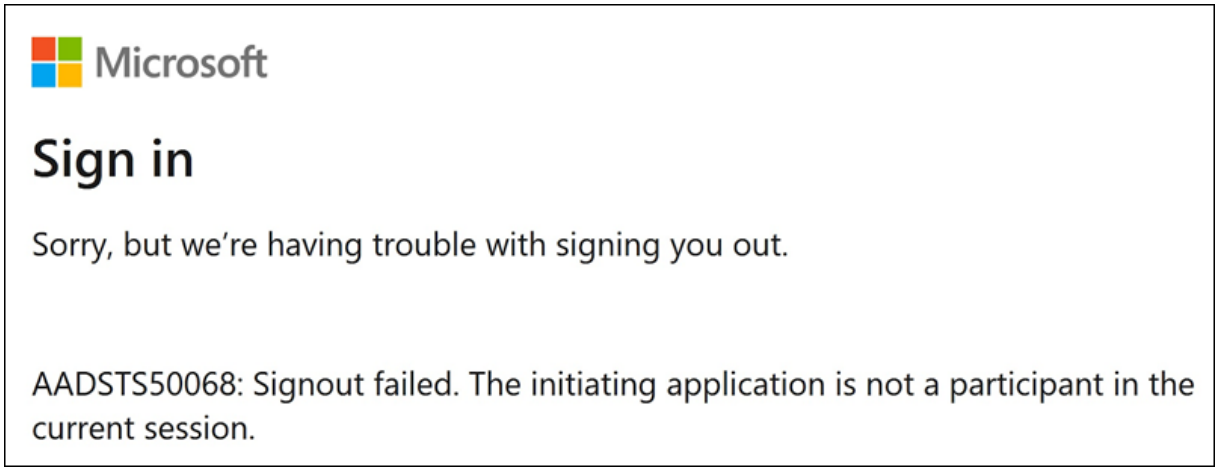
1. 在 Web 浏览器的扩展面板中，安装并启用 SAML-tracer 扩展程序。
2. 执行 SAML 登录和注销操作，并使用 SAML-tracer 扩展程序捕获整个流程。
3. 在 SAML SSO 请求或 SLO 请求中找到以下行。

```
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
   https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
   saml:Issuer>
<!--NeedCopy-->
```

4. 验证实体 ID 是否与您的 SAML 提供商应用程序中配置的实体 ID 相匹配。
5. 验证“颁发者”字段中是否存在限定范围内的实体 ID，并验证它在 SAML 提供商中的配置是否正确。
6. 导出并保存 SAML-tracer JSON 输出。如果您正在与 Citrix 支持部门合作解决问题，请将输出上载到您的 Citrix 支持案例。

Azure AD 故障排除

问题：配置 SLO 后，注销 Azure AD 失败。Azure AD 向用户显示以下错误：



如果在 Citrix Cloud 中为 SAML 连接启用了限定范围内的实体 ID，则必须在 SSO 和 SLO 请求中发送限定范围内的实体 ID。

原因：已配置限定范围内的实体，但 SLO 请求中缺少实体 ID。验证限定范围内的实体 ID 是否存在于 SAML-tracer 输出中的 SLO 请求中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本地 **PingFederate** 故障排除

问题：启用限定范围内的实体 ID 设置后，登录或注销 PingFederate 失败。

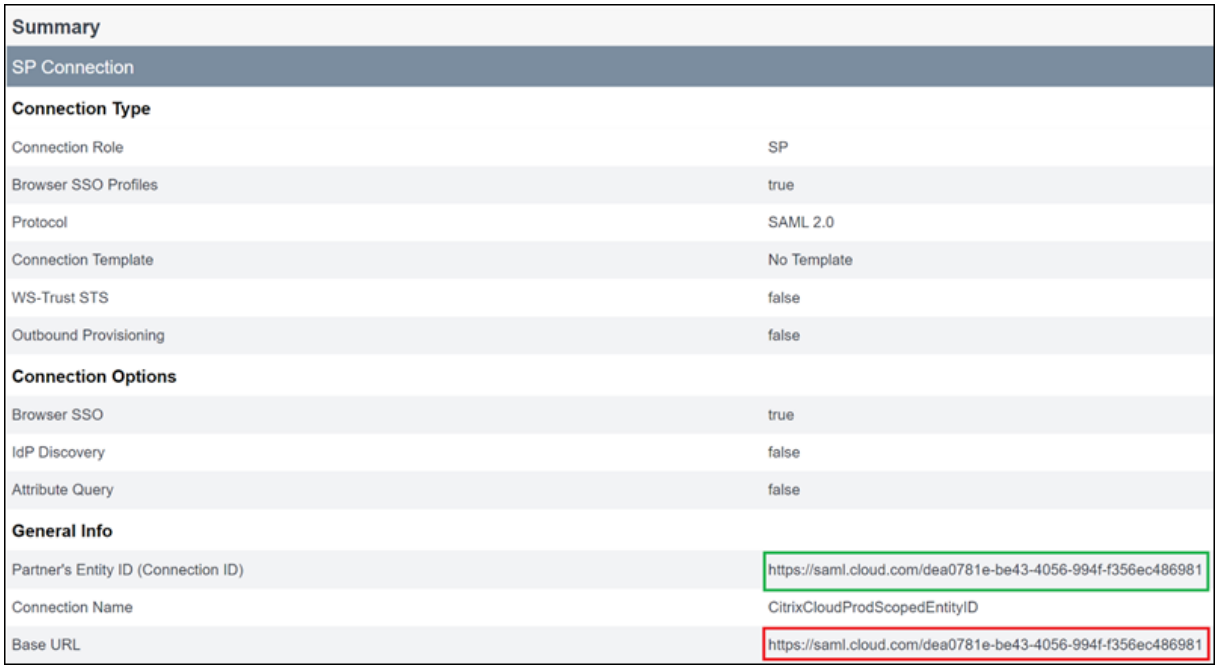
原因： PingFederate 管理员将限定范围内的实体 ID 添加到 SP 连接基础 URL 中。

要更正此问题，请仅将限定范围内的实体 ID 添加到合作伙伴的实体 **ID** 字段中。将限定范围内的实体 ID 添加到基本 URL 会导致 SAML 端点格式不正确。如果 Citrix Cloud 基本 URL 更新不正确，则从基本 URL 派生的所有其他 SAML 端点相关 URL 都会导致登录失败。

以下端点是 SAML-tracer 输出中可能出现格式错误的 Citrix Cloud SAML 端点的示例：

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

下图显示了一个配置错误的 PingFederate SAML 应用程序。正确配置的字段显示为绿色。配置错误的字段显示为红色。



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

SAML 使用 **Azure AD** 和 **AAD** 身份进行工作区身份验证

March 11, 2024

Author:
Mark Dear

本文介绍如何使用 Azure Active Directory (AD) 身份而不是 AD 身份为工作区身份验证配置 SAML。如果您的 Azure AD 用户在使用默认 SAML 行为登录 Citrix Workspace 后无法枚举 Windows 365 云电脑或已加入 Azure AD 域的

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

VDA，请使用此配置。完成配置后，您的用户可以使用 SAML 身份验证登录 Citrix Workspace，通过 Citrix DaaS 同时访问 HDX 应用程序和桌面，通过 Azure 访问 Windows 365 云电脑。

Citrix Cloud 和 Citrix Workspace 的 SAML 身份验证的默认行为是根据 AD 用户身份进行断言。对于本文中描述的配置，需要使用 Azure AD Connect 将您的 AD 身份导入 Azure AD。AD 身份包含用户的 SID，Citrix Workspace 可以将其发送到 Citrix DaaS，并允许枚举和启动 HDX 资源。由于使用了 Azure AD 版本的用户身份，因此用户还可以从 Citrix Workspace 中枚举和启动 Azure 资源，例如 Windows 365 云电脑。

> 重要提示：
>
> 枚举是指用户登录 Citrix Workspace 后看到的资源列表。允许给定用户访问的资源取决于他们的用户身份以及在 Citrix DaaS 中与该身份关联的资源。有一篇相关文章提供了有关使用 Azure AD 和 AD 身份作为 SAML 提供程序在 Workspace 中进行身份验证的说明。您可以在 SAML 中找到使用 Azure AD 和 AD 身份进行 Workspace 身份验证的详细说明

功能范围

本文适用于使用以下 Citrix Cloud 和 Azure 功能组合的用户：

- 用于工作区身份验证的 SAML
- 使用加入了 AD 域的 VDA 发布的 Citrix DaaS 和 HDX 资源枚举
- Azure AD 加入域的 VDA 资源枚举
- Azure 混合域加入的 VDA 资源枚举
- W365 Cloud PC 枚举和启动

> 重要提示：
>
> 请勿使用此 AAD SAML 流程进行 SAML 登录到 Citrix Cloud，因为这要求 Citrix Cloud 管理员用户是 AD 组的成员，因此应使用 AD 用户身份。您可以在 SAML 中找到使用 Azure AD 和 AD 身份进行 Workspace 身份验证的详细说明

哪个最好：**AD** 身份还是 **Azure AD** 身份

要确定您的工作区用户应该使用 SAML AD 还是 SAML Azure AD 身份进行身份验证，请执行以下操作：

1. 决定您打算在 Citrix Workspace 中向用户提供哪种资源组合。
2. 使用下表来确定哪种类型的用户身份适合每种资源类型。

资源类型 (VDA)	登录 Citrix Workspace 时的用户身份	需要使用 Azure AD 的 SAML 身份吗?	FAS 提供对 VDA 的单点登录 (SSO) 吗?
已加入 AD	AD，从 AD 导入的 Azure AD（包含 SID）	否。使用默认 SAML。	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

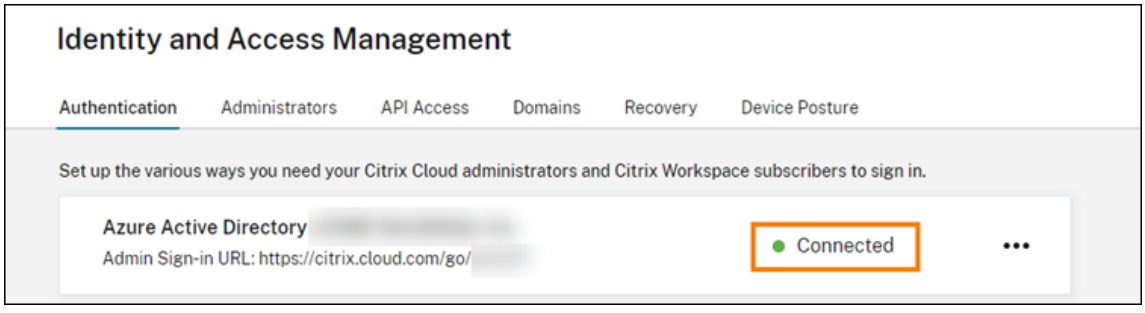
资源类型 (VDA)	登录 Citrix Workspace 时的用户身份	需要使用 Azure AD 的 SAML 身份吗?	FAS 提供对 VDA 的单点登录 (SSO) 吗?
混合加入	AD，从 AD 导入的 Azure AD（包含 SID）	否。使用默认 SAML。	是的，对于 AD 作为身份提供商。如果为 VDA 选择了 Azure AD，则不需要 FAS。
已加入 Azure AD	Azure AD 本机用户，从 AD 导入的 Azure AD（包含 SID）	是，通过 Azure AD 使用 SAML。	SSO 可与 Azure AD 新式验证配合使用。不需要 FAS。
Windows 365 云电脑	Azure AD 本机用户，从 AD 导入的 Azure AD（包含 SID）	是，通过 Azure AD 使用 SAML。	SSO 可与 Azure AD 新式验证配合使用。不需要 FAS。
已加入 AD，已加入 Azure AD，Windows 365 云电脑	从 AD 导入的 Azure AD（包含 SID）	是，通过 Azure AD 使用 SAML。	是的，对于 AD 已加入。不是，适用于已加入 Azure AD 和 Windows 365 云电脑。

更多信息

- Citrix DaaS 文档：
  - 计算机标识
  - 适用于 Windows 365 的 Citrix HDX
- Citrix FAS 文档：安装和配置
- Microsoft Azure 文档：Azure AD Connect 是什么?

要求

- 您的 Azure AD 租户必须连接到您的 Citrix Cloud 租户。在 Citrix Cloud 控制台中，您可以通过选择“身份和访问管理”**>**“身份验证”来找到您的 Azure AD 连接。



- 工作区身份验证方法必须设置为 **SAML 2.0**。请勿使用 Azure AD 作为身份验证方法。要更改 Workspace 身份验证方法，请转到 Citrix Cloud 控制台中的 **Workspace** 配置 **>** 身份验证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 必须将 UPN 后缀 `@yourdomain.com` 作为自定义域名导入并在 Azure AD 中进行验证。在 Azure 门户中，它位于 **Azure Active Directory >**“自定义域名”下。
- Azure AD 用户身份必须使用 Microsoft Azure AD Connect 从 AD 导入。这样可以确保正确导入用户身份并具有正确的 UPN 后缀。不支持带有 `@yourtenant.onmicrosoft.com` UPN 后缀的 Azure AD 用户。
- 必须部署 Citrix FAS 并将其连接到 Citrix Cloud 租户和资源位置。FAS 为从 Citrix Workspace 启动的 HDX 桌面和应用程序提供单点登录。您不必配置 AD 影子帐户，因为 AD 和 Azure AD 用户身份的 UPN `user@customerdomain` 必须匹配。FAS 使用正确的 UPN 生成必要的用户证书，并在启动 HDX 资源时执行智能卡登录。

配置自定义 **Azure AD Enterprise SAML** 应用程序

默认情况下，SAML 登录工作区的行为是根据 AD 用户身份进行断言。**cip_directory** SAML 属性是一个硬编码的字符串值，对于所有订阅者来说都是一样的，可以用作开关。Citrix Cloud 和 Citrix Workspace 在登录期间会检测到此属性，并触发 SAML 对用户身份的 Azure AD 版本进行断言。使用带有此属性的 **azuread** 参数会覆盖默认 SAML 行为，从而触发在 Azure AD 中使用 SAML。

尽管本节中的步骤适用于 Azure AD，但只要您执行相同的任务，您可以使用不同的 SAML 2.0 提供程序（例如 ADFS、Duo、Okta、OneLogin、PingOneSSO 等）创建类似的 SAML 应用程序。您的 SAML 提供商必须允许您在 SAML 应用程序中配置硬编码的 SAML 属性（cip_directory = azuread）。只需按照本节所述创建相同的 SAML 属性映射即可。

1. 登录 Azure 门户。
2. 从门户菜单中选择 **Azure Active Directory**。
3. 在左侧窗格的“管理”下，选择“企业应用程序”。
4. 在工作窗格的命令栏中，选择“新建应用程序”。
5. 在命令栏中，选择“创建自己的应用程序”。不要使用 Citrix Cloud SAML SSO 企业应用程序模板。该模板不允许您修改声明列表和 SAML 属性。
6. 输入应用程序的名称，然后选择“整合您在图库中找不到的任何其他应用程序（非图库）”。单击创建。将出现应用程序概述页面。
7. 在左侧窗格中，选择 单点登录。在工作窗格中，选择 **SAML**。
8. 在“基本 **SAML** 配置”部分中，选择 编辑 并配置以下设置：

    a) 在 标识符（实体 **ID**）部分，选择 添加标识符，然后输入与您的 Citrix Cloud 租户所在区域关联的值：
    - 对于欧盟、美国和亚太南部地区，请输入 `https://saml.cloud.com`。
    - 对于日本区域，请输入 `https://saml.citrixcloud.jp`。
    - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) 在“回复 **URL**（断言消费者服务 **URL**）”部分，选择“添加回复 **URL**”，然后输入与 Citrix Cloud 租户所在区域关联的值：

- 对于欧盟、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
- 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/acs`。
- 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

c) 在注销 **URL**（可选）部分，输入与您的 Citrix Cloud 租户所在区域关联的值：

- 对于欧盟、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/logout/callback`。
- 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
- 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/logout/callback`。

d) 在命令栏中，选择“保存”。

9. 在“属性和声明”部分，选择“编辑”以配置以下声明。这些声明出现在 SAML 响应中的 SAML 断言中。

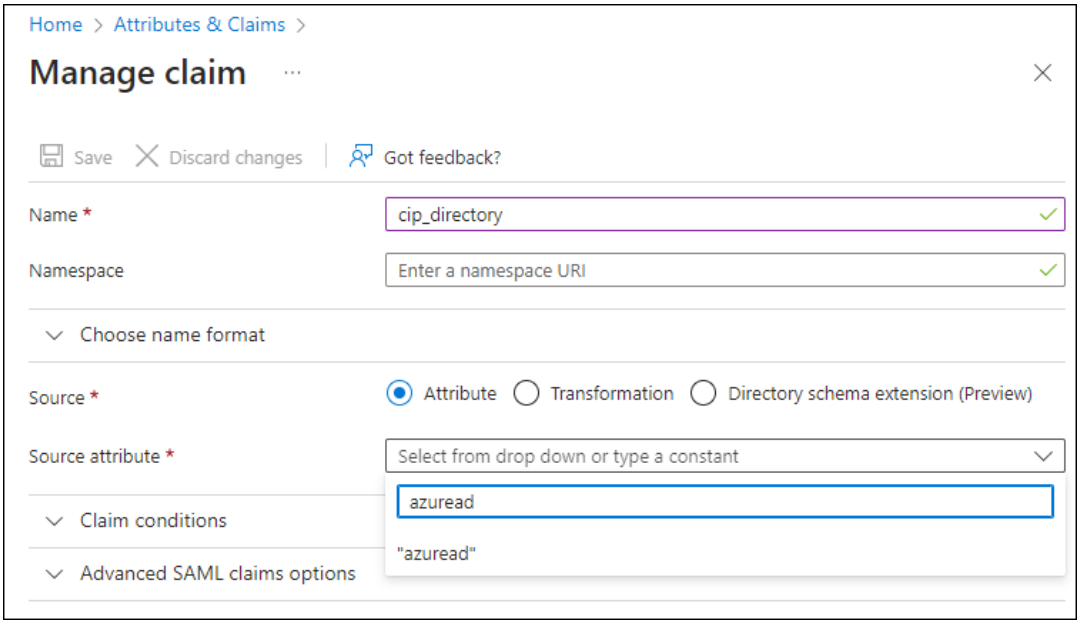
a) 对于 唯一用户标识符（姓名 **ID**）声明，请保留默认值 `user.userprincipalname`。

b) 在命令栏中，选择“添加新声明”。

c) 在 名称中输入 **cip_directory**。

d) 在 源中，保持选中 属性。

e) 在 来源属性中，输入 **azuread**。输入该值后，该值将以引号形式出现。

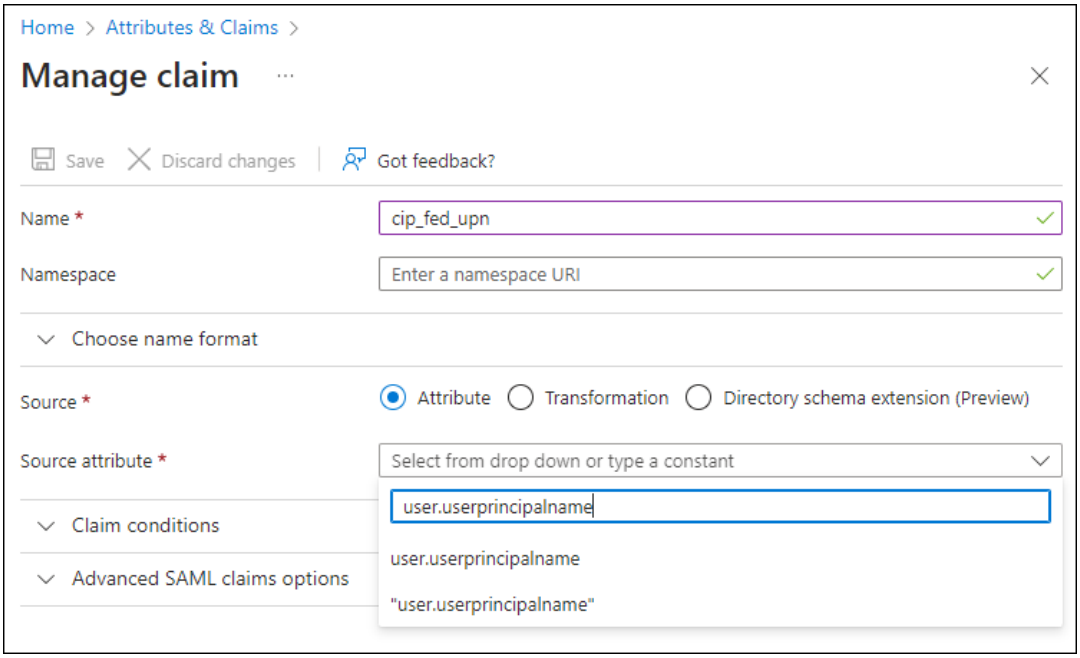


f) 在命令栏中，选择“保存”。

g) 在“名称”和“来源”属性 字段中使用以下值创建其他声明：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

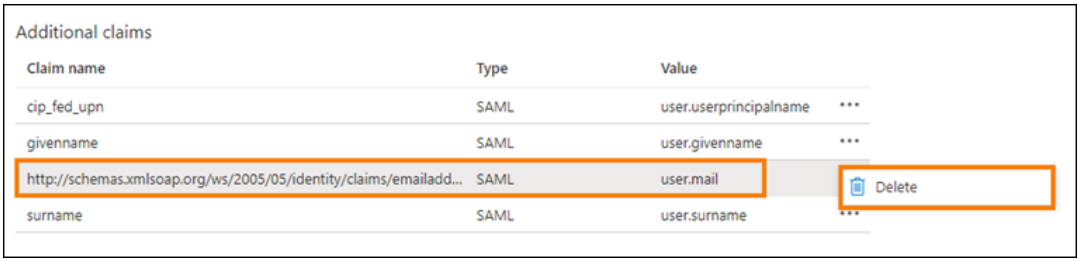
名称	来源属性
cip_fed_upn	user.userprincipalname
displayName	user.displayname
firstName	user.givenname
lastName	user.surname



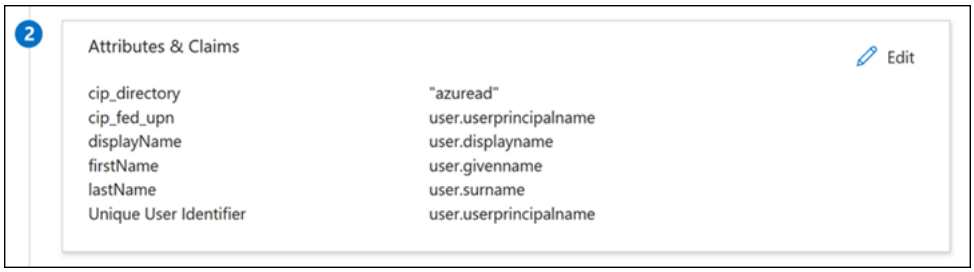
> 重要提示：
>
> 您可以通过对每个声明重复步骤 b-f 或修改其他声明部分中已具有上表中列出的来源属性的默认声明来创建这些其他声明。默认声明包括命名空间 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`。
>
> 如果您修改了默认声明，则必须从每个声明中删除命名空间。如果您创建新的声明，则必须删除包含命名空间的声明。如果使用此命名空间的声明包含在生成的 SAML 断言中，则该断言将无效，并且会包含错误的 SAML 属性名称。

h) 在“其他声明”部分中，对于 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的所有剩余声明，请单击省略号 (…) 按钮，然后单击“删除”。

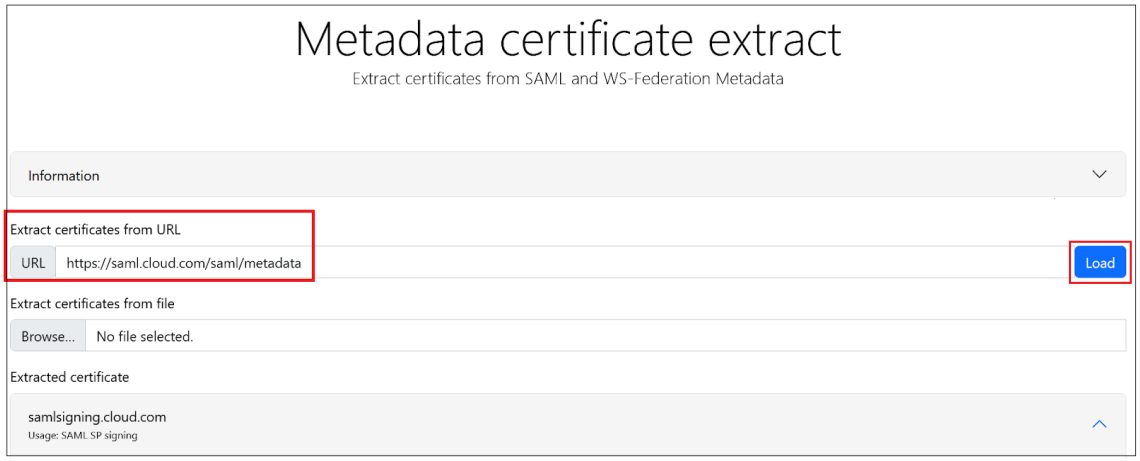
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



完成后，“属性和声明”部分将显示如下所示：

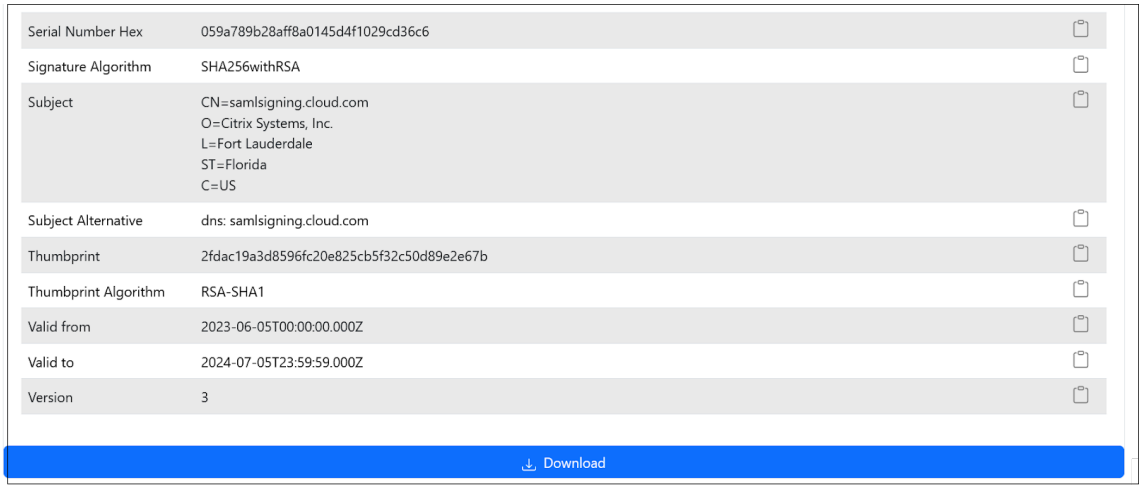


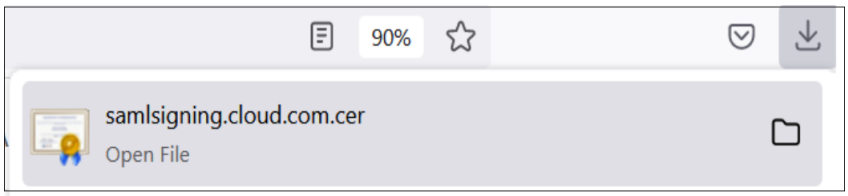
10. 使用此第三方在线工具获取 Citrix Cloud SAML 签名证书的副本。
11. 在 URL 字段中输入 https://saml.cloud.com/saml/metadata，然后单击“加载”。



12. 滚动到页面底部，然后单击“下载”。

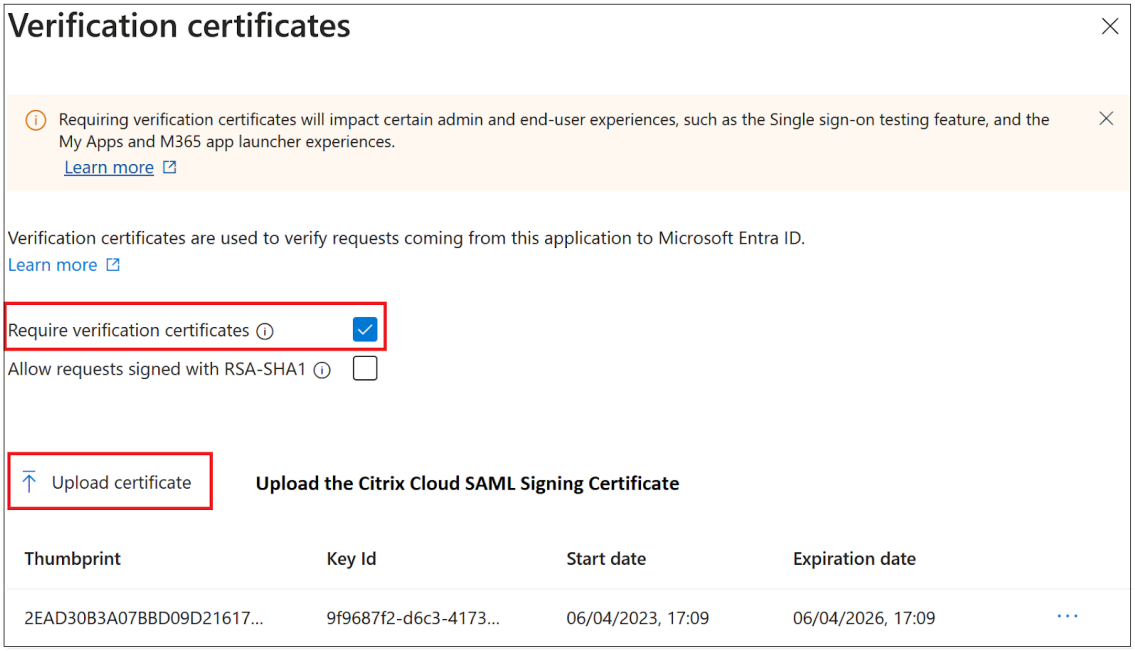
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



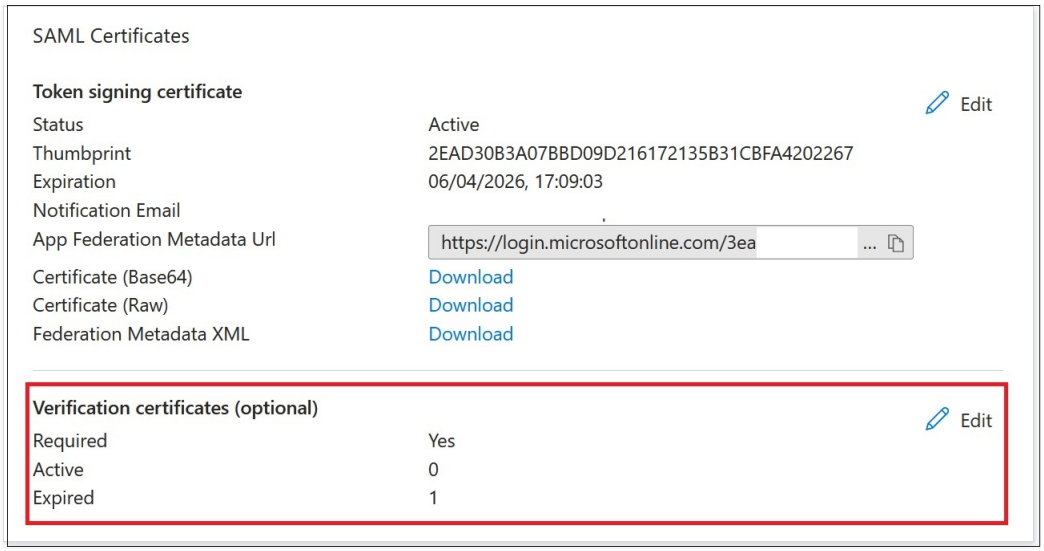


13. 配置 Azure Active Directory SAML 应用程序签名设置。
14. 在 Azure Active Directory SAML 应用程序中上载在步骤 10 中获得的生产 SAML 签名证书。

    - 启用“需要验证证书”。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.



故障排除

1. 使用 SAML 网络工具（例如 SAML-tracer browser extension）验证您的 SAML 断言包含正确的用户属性。
2. 找到黄色显示的 SAML 响应并与以下示例进行比较：

3. 单击底部窗格中的 **SAML** 选项卡，解码 SAML 响应并以 XML 格式查看。
4. 滚动到响应底部，验证 SAML 断言是否包含正确的 SAML 属性和用户值。

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>3ea                              98498</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>0813                             3462d</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/3ea                                  98498/</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>       @      .com</AttributeValue>
    </Attribute>
    <Attribute Name="cip_email">
        <AttributeValue>       @      .com</AttributeValue>
    </Attribute>
    <Attribute Name="cip_sid">
        <AttributeValue>S-1-5-21-17                                  282</AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>       </AttributeValue>
    </Attribute>
    <Attribute Name="cip_oid">
        <AttributeValue>0813                             462d</AttributeValue>
    </Attribute>
</AttributeStatement>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您的订阅者仍然无法登录其工作区，请联系 Citrix 支持并提供以下信息：

- SAML-tracer capture
- 登录 Citrix Workspace 失败的日期和时间
- 受影响的用户名
- 您用于登录 Citrix Workspace 的客户端计算机的主叫方 IP 地址。您可以使用像 https://whatismyip.com 这样的工具来获取这个 IP 地址。

SAML 使用 Azure AD 和 AD 身份进行 Workspace 身份验证

June 2, 2024

Author:
Mark Dear

本文介绍如何使用 Active Directory (AD) 身份为工作区身份验证配置 SAML。无论使用哪个 SAML 提供商，Citrix Cloud 和 SAML 向 Citrix Workspace 或 Citrix Cloud 进行身份验证的默认行为都是断言 AD 用户身份。对于本文中描述的配置，需要使用 Azure AD Connect 将您的 AD 身份导入 Azure AD。

> 重要：
>
> 为 Workspace 最终用户确定适当的 SAML 流程至关重要，因为这会直接影响他们的登录流程和资源可见性。所选身份会影响 Workspace 最终用户可访问的资源类型。
> 有一篇相关文章提供了有关使用 Azure AD 作为 SAML 提供者使用 AAD 身份在 Workspace 中进行身份验证的说明。您可以在 SAML 中找到使用 Azure AD 和 AAD 身份进行工作区身份验证的详细说明。
> 通常，Workspace 最终用户通常需要打开加入 AD 域的 VDA 提供的应用程序和桌面。在决定最适合贵组织的 SAML 流程之前，必须仔细阅读两篇文章中概述的用例。如果不确定，Citrix 建议使用 **AD SAML** 流程并按照本文中的说明进行操作，因为它符合最常见的 DaaS 方案。

功能范围

本文适用于使用以下 Citrix Cloud 和 Azure 功能组合的用户：

- 使用 AD 身份进行工作区身份验证的 SAML
- 使用 AD 身份登录 Citrix Cloud 管理员时使用 SAML
- 使用加入了 AD 域的 VDA 发布的 Citrix DaaS 和 HDX 资源枚举
- 加入 AD 域的 VDA 资源枚举

哪个最好：AD 身份还是 Azure AD 身份

要确定您的工作区用户应该使用 SAML AD 还是 SAML Azure AD 身份进行身份验证，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

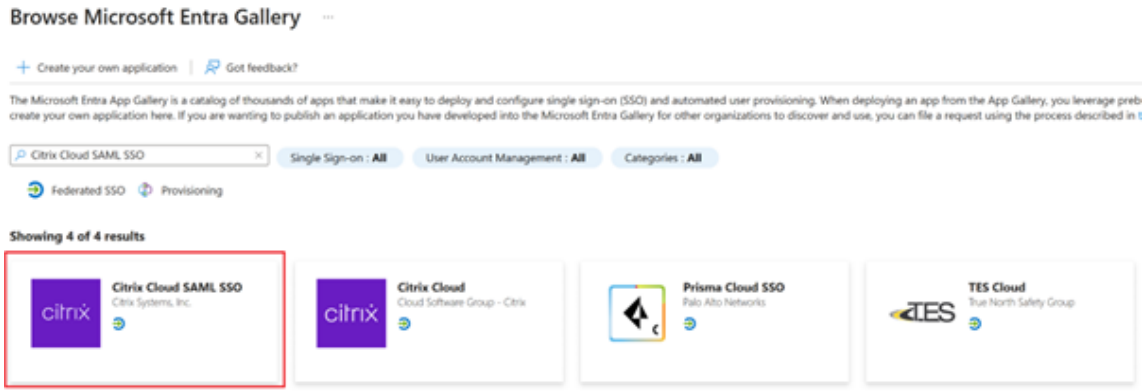
1. 决定您打算在 Citrix Workspace 中向用户提供哪种资源组合。
2. 使用下表来确定哪种类型的用户身份适合每种资源类型。

资源类型 (VDA)	登录 Citrix Workspace 时的用户身份	需要使用 Azure AD 的 SAML 身份吗?	FAS 提供对 VDA 的单点登录 (SSO) 吗?
已加入 AD	AD，从 AD 导入的 Azure AD（包含 SID）	否。使用默认 SAML。	是

配置自定义 **Azure AD Enterprise SAML** 应用程序

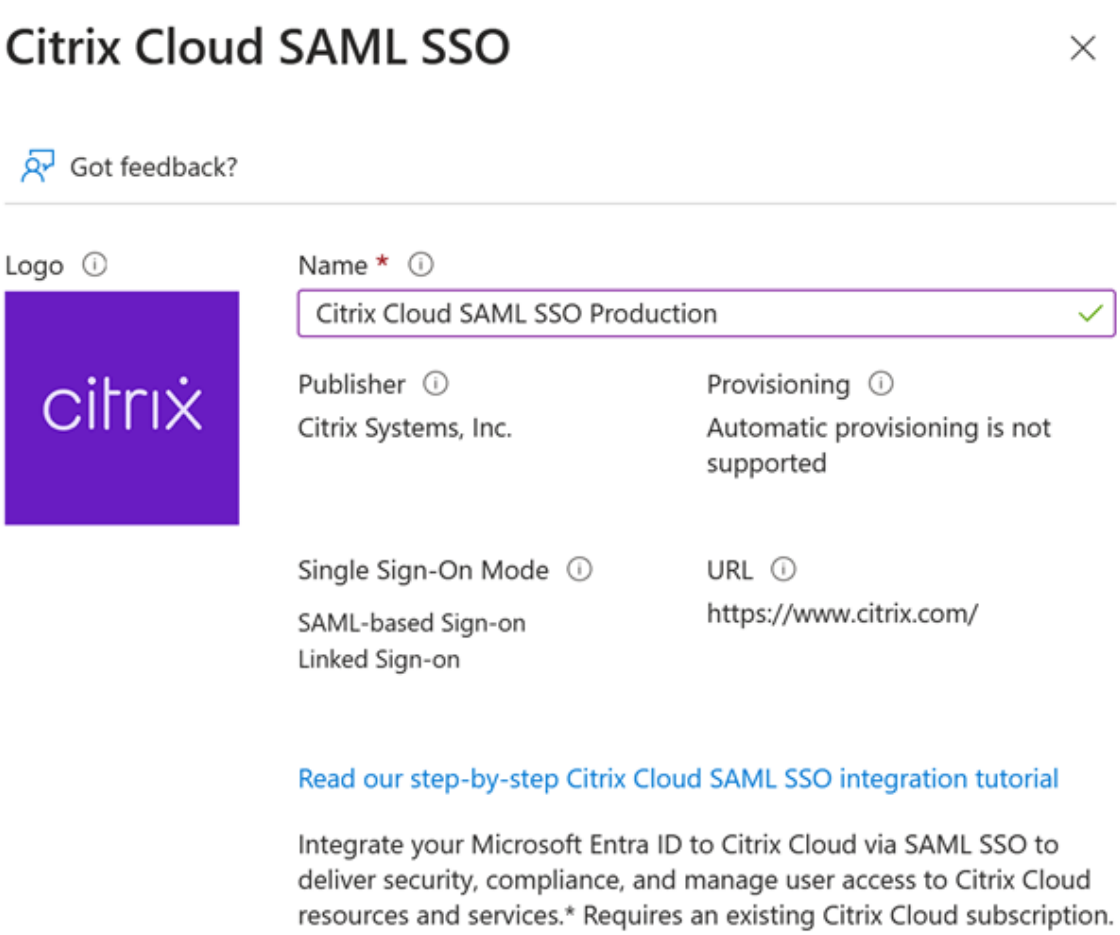
默认情况下，SAML 登录工作区的行为是根据 AD 用户身份进行断言。

1. 登录 Azure 门户。
2. 从门户菜单中选择 **Azure Active Directory**。
3. 在左侧窗格的“管理”下，选择“企业应用程序”。
4. 在搜索框中，输入 `Citrix Cloud SAML SSO` 以找到 Citrix SAML 应用程序模板。



5. 为 SAML 应用程序输入合适的名称，例如 `Citrix Cloud SAML SSO Production`

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. 在左侧导航窗格中，选择单点登录，然后在工作窗格中单击 **SAML**。
7. 在“基本 **SAML** 配置”部分中，单击“编辑”并配置以下设置：
   a) 在 标识符（实体 **ID**）部分，选择 添加标识符，然后输入与您的 Citrix Cloud 租户所在区域关联的值：
      - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com`。
      - 对于日本区域，请输入 `https://saml.citrixcloud.jp`。
      - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

   b) 在“回复 **URL**（断言消费者服务 **URL**）”部分，选择“添加回复 **URL**”，然后输入与 Citrix Cloud 租户所在区域关联的值：
      - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
      - 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/acs`。
      - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

   c) 在“登录 **URL**”部分，输入您的 Workspace URL。
   d) 在注销 **URL**（可选）部分，输入与您的 Citrix Cloud 租户所在区域关联的值：
      - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/logout/callback`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

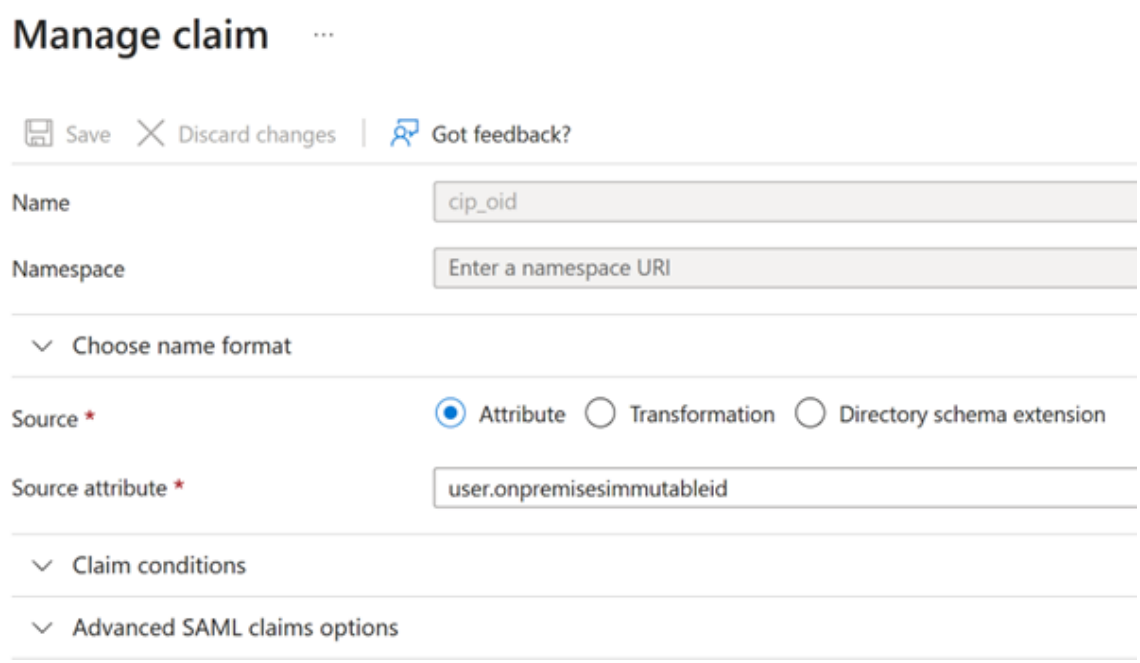
- 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
- 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/logout/callback`。

e) 在命令栏上，单击“保存”。“基本 **SAML** 配置”部分显示如下：

8. 在“属性和声明”部分，单击“编辑”以配置以下声明。这些声明出现在 SAML 响应中的 SAML 断言中。创建 SAML 应用程序后，配置以下属性。

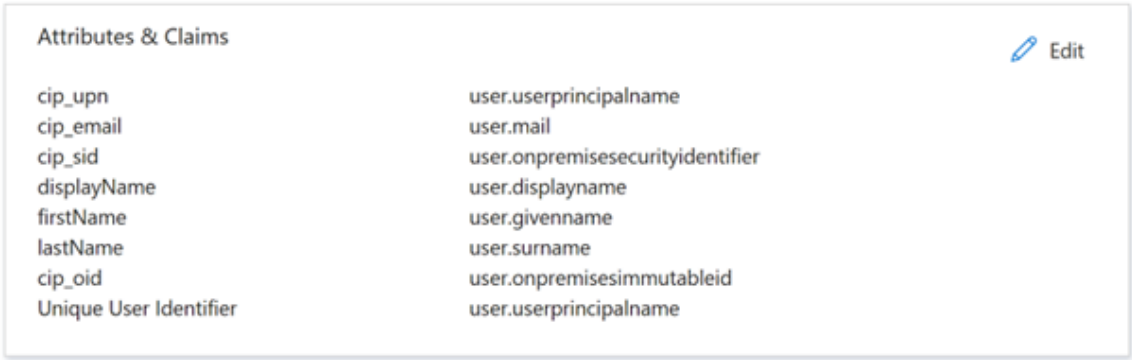
a) 对于唯一用户标识符（姓名 **ID**）声明，请保留默认值 `user.userprincipalname`。
b) 对于 **cip_upn** 声明，请保留 `user.userprincipalname` 的默认值。
c) 对于 **cip_email** 声明，请保留 `user.mail` 的默认值。
d) 对于 **cip_sid** 声明，请保留 `user.onpremisesecurityidentitier` 的默认值。
e) 对于 **cip_oid** 声明，请编辑现有声明并选择来源属性。搜索字符串 `object` 并选择 `user.onpremisesimmutableid`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



a) 对于 **displayName**，请保留 `user.displayname` 的默认值。

b) 在“其他声明”部分中，对于 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的所有剩余声明，请单击省略号 (…) 按钮，然后单击“删除”。无需包含这些声明，因为它们是上述用户属性的重复。



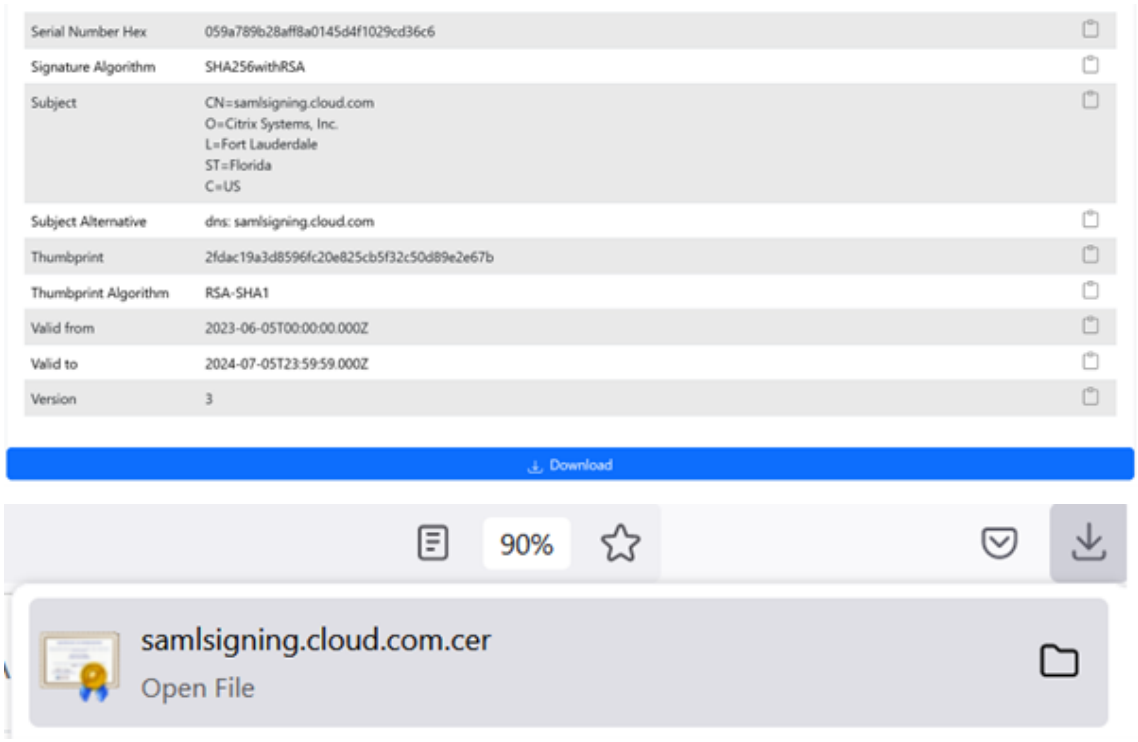
完成后，“属性和声明”部分将显示如下所示：

a) 使用此第三方在线工具获取 Citrix Cloud SAML 签名证书的副本。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

b) 在 URL 字段中输入 `https://saml.cloud.com/saml/metadata` 并单击“加载”。

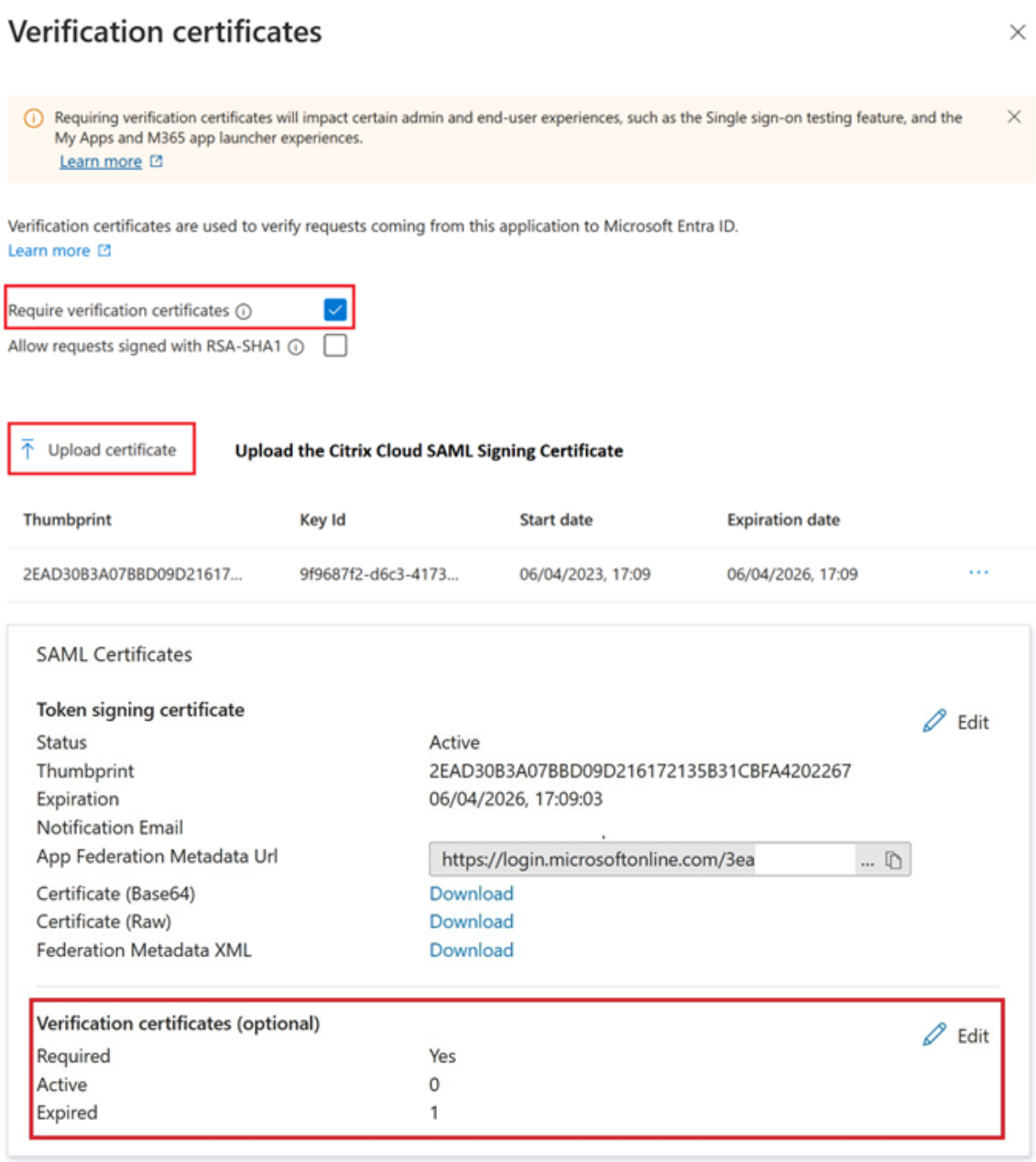
9. 滚动到页面底部，然后单击“下载”。



10. 配置 Azure Active Directory SAML 应用程序签名设置。
11. 在 Azure Active Directory SAML 应用程序中上载步骤 10 中获得的生产 SAML 签名证书

    a) 启用“需要验证证书”。

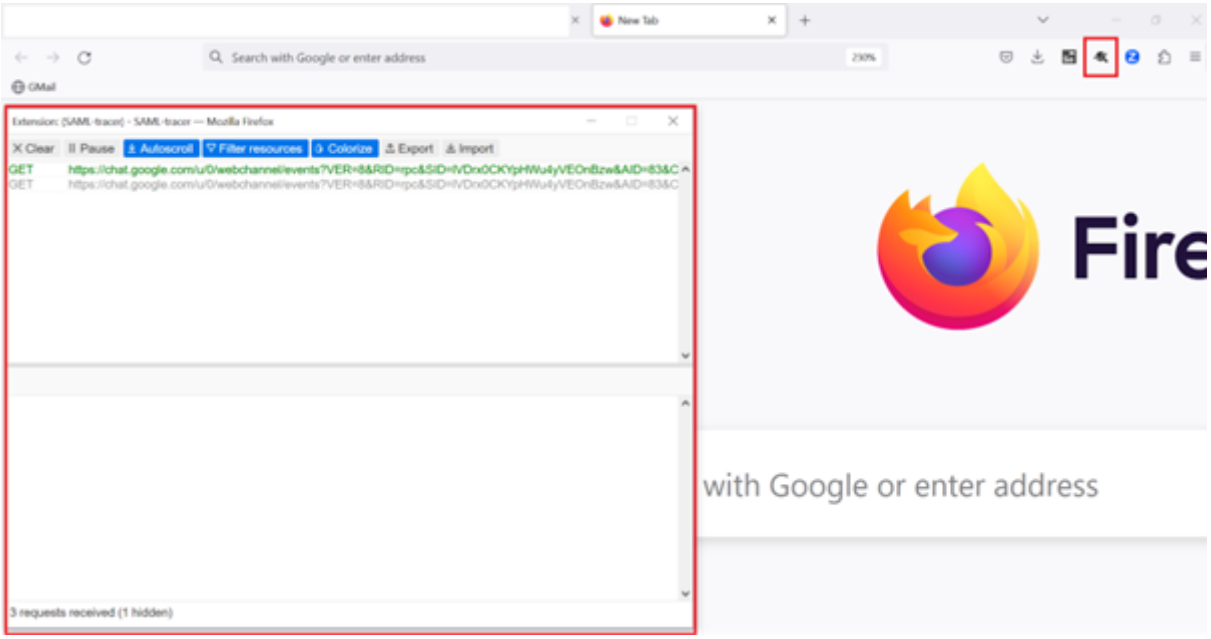
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



故障排除

1. 使用 SAML 网络工具（例如 SAML-tracer browser extension）验证您的 SAML 断言包含正确的用户属性。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



1. 找到黄色显示的 SAML 响应并与以下示例进行比较：

2. 单击底部窗格中的 **SAML** 选项卡，解码 SAML 响应并以 XML 格式查看。

3. 滚动到响应底部，验证 SAML 断言是否包含正确的 SAML 属性和用户值。

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>3ea                              98498</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>0813                             3462d</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/3ea                                98498/</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password</AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>       @      .com</AttributeValue>
    </Attribute>
    <Attribute Name="cip_email">
        <AttributeValue>       @      .com</AttributeValue>
    </Attribute>
    <Attribute Name="cip_sid">
        <AttributeValue>S-1-5-21-17                                    282</AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>       </AttributeValue>
    </Attribute>
    <Attribute Name="cip_oid">
        <AttributeValue>0813                             462d</AttributeValue>
    </Attribute>
</AttributeStatement>
```

如果您的订阅者仍然无法登录其工作区或无法看到适用于 Windows 365 桌面的 Citrix HDX Plus，请联系 Citrix 支持部门并提供以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- SAML-tracer 捕获
- 登录 Citrix Workspace 失败的日期和时间
- 受影响的用户名
- 您用于登录 Citrix Workspace 的客户端计算机的主叫方 IP 地址。您可以使用像 https://whatismyip.com 这样的工具来获取这个 IP 地址。

配置简化的 **SAML** 以供本地和来宾 **SAML** 用户使用

July 1, 2024

Author:
Mark Dear, Javier Lopez Santacruz

在阅读本文之前，必须了解“简化的 SAML”是否适合您的身份验证用例。在决定实施这个特定的特殊情况 SAML 解决方案之前，请仔细阅读用例描述和常见问题解答。在继续操作之前，请确保您完全了解简化的 SAML 的适用场景以及需要使用哪些类型的身份。大多数 SAML 用例可以通过关注其他 SAML 文章并发送所有四个 cip_* 属性进行身份验证来实现。

> 注意：
>
> 使用“简化的 SAML”会增加 Citrix Cloud Connector 的负载，因为他们必须为每个 Workspace 最终用户登录查询用户邮箱、SID 和 OID，而不是 SAML 断言提供这些值。如果实际上并不需要简化的 SAML，则从 Citrix Cloud Connector 性能的角度来看，最好在 SAML 断言中发送所有四个 cip_* 属性。

必备条件

- 专门配置为与简化的 SAML 一起使用的 SAML 应用程序，它仅在 SAML 断言中发送 **cip_upn** 进行身份验证。
- 您的 SAML 提供商中的前端用户。
- 包含两个 Citrix Cloud Connector 的资源位置，这些连接器加入了 AD 林和创建 AD 影子帐户的域。
- 备用 UPN 后缀添加到创建 AD 影子帐户的后端 AD 林中。
- 具有匹配的 UPN 的后端 AD 影子帐户。
- 映射到 AD 影子帐户用户的 DaaS 或 CVAD 资源。
- 一个或多个 FAS 服务器链接到同一个资源位置。

常见问题解答

我为什么要使用简化的 **SAML**

大型组织邀请承包商和临时员工加入他们的身份平台是很常见的。目标是授予承包商使用用户的现有身份（例如承包商电子邮件地址或组织外部的电子邮件地址）临时访问 Citrix Workspace 的权限。简化的 SAML 允许使用在发布 DaaS

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

资源的 AD 域中不存在的本机或来宾前端身份。

什么是简化的 **SAML**

通常，登录 Citrix Workspace 时，使用四个 SAML 属性 cip_* 及其相应的 AD 用户属性对最终用户进行身份验证。这四个 SAML 属性预计将出现在 SAML 断言中，并使用 AD 用户属性进行填充。简化的 SAML 是指仅需要 cip_upn SAML 属性即可成功进行身份验证的事实。

AD 属性	SAML 断言中的默认属性名称
userPrincipalName	cip_upn
邮件	cip_email
objectSID	cip_sid
objectGUID	cip_oid

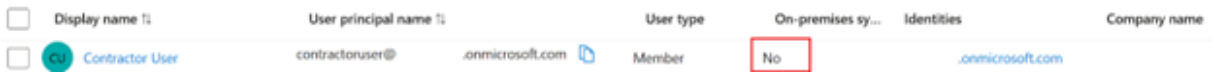
身份验证所需的其他三个 AD 用户属性 objectSID、objectGUID 和 mail 是使用加入到 AD 影子帐户所在的 AD 域的 Citrix Cloud Connector 获取的。在 Workspace 或 Citrix Cloud 的 SAML 登录流程中，不再需要将它们包含在 SAML 断言中。

AD 属性	SAML 断言中的默认属性名称
userPrincipalName	cip_upn

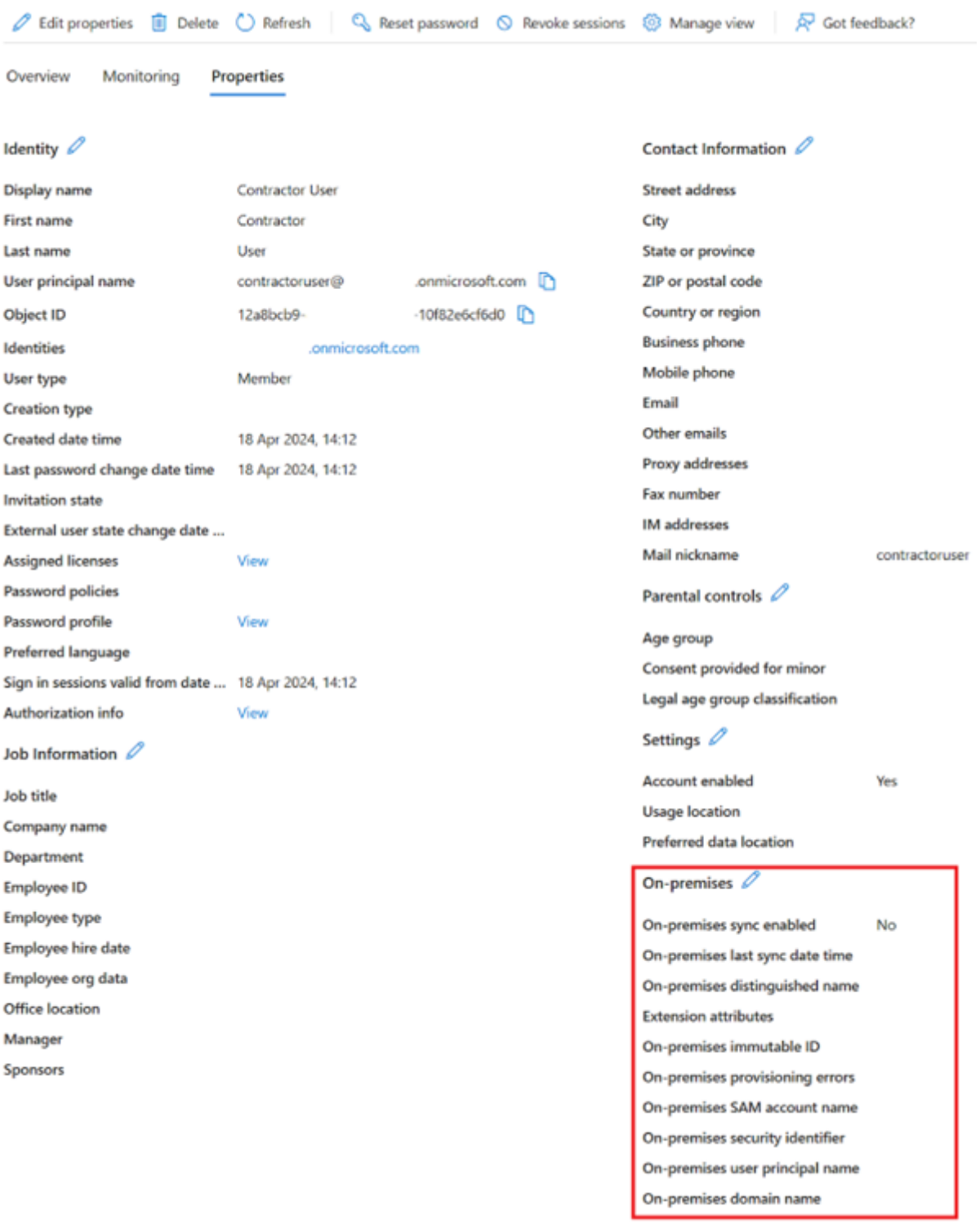
> 重要：
>
> 仍然需要为包括简化的 SAML 在内的所有 SAML 流程发送 **displayName**。Workspace 用户界面要求 **displayName** 才能正确显示 Workspace 用户的全名。

什么是本机 **SAML** 用户身份

本机 SAML 用户是仅存在于您的 SAML 提供商目录中的用户身份，例如 Entra ID 或 Okta。这些身份不包含本地用户属性，因为它们不是通过 Entra ID connect 等 AD 同步工具创建的。它们需要匹配的 AD 后端影子帐户才能枚举和启动 DaaS 资源，本机 SAML 用户必须映射到 Active Directory 中的相应帐户。



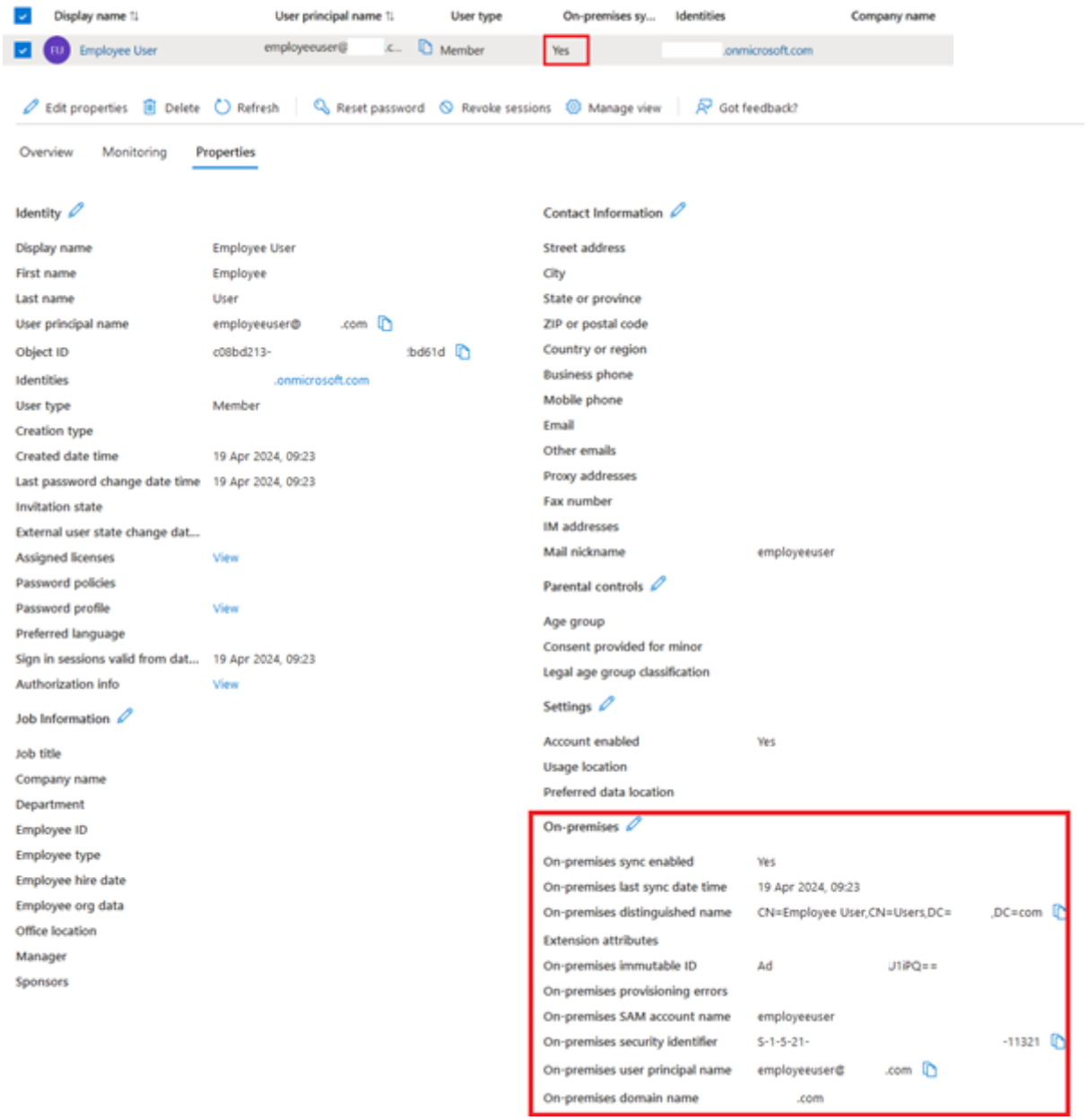
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

什么是 **AD** 支持的 **SAML** 用户身份

AD 支持的 SAML 用户是存在于您的 SAML 提供商目录（如 Entra ID 或 Okta）中的用户身份，也存在于您的本地 AD 林中。这些身份包含本地用户属性，因为它们是通过 Entra ID connect 等 AD 同步工具创建的。这些用户不需要 AD 后端影子帐户，因为它们包含本地 SID 和 OID，因此可以枚举和启动 DaaS 资源。



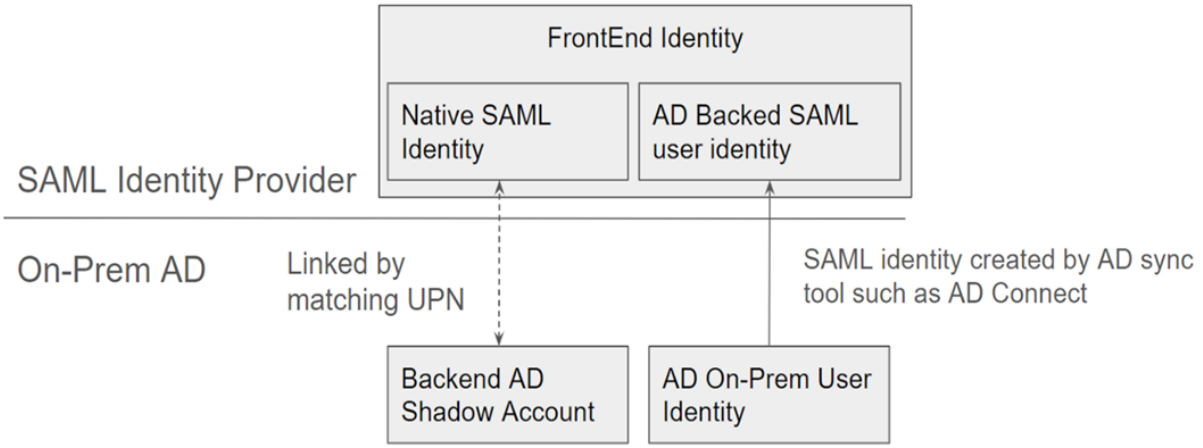
什么是前端身份

前端身份是用于登录 SAML 提供商和 Workspace 的身份。前端身份具有不同的用户属性，具体取决于它们是如何在 SAML 提供商中创建的。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 本机 SAML 用户身份
2. AD 支持的 SAML 用户身份

您的 SAML 提供商可能混合使用这两种类型的身份。例如，如果您的身份平台内既有承包商又有长期员工，则简化的 SAML 适用于两种类型的前端身份，但仅当您的某些帐户类型为本机 SAML 用户身份时才是强制性的。



什么是后端 **AD** 影子帐户

后端 AD 影子帐户是 DaaS 使用的 AD 帐户，它映射到您的 SAML 提供商中相应的前端身份。

为什么需要后端 **AD** 影子帐户

为了枚举使用 AD 域加入的 VDA 发布的 DaaS 或 CVAD 资源，需要加入 VDA 的 Active Directory 林中的 AD 帐户。将您的 DaaS 交付组中的资源映射到影子帐户用户，以及包含您加入 VDA 的 AD 域中的影子帐户的 AD 组。

> 重要：
>
> 只有没有 AD 域属性的本地 SAML 用户才需要匹配的 AD 影子帐户。如果您的前端身份是从 Active Directory 导入的，那么您不需要使用简化的 SAML，也不需要创建后端 AD 影子帐户。

我们如何将前端身份关联到相应的后端 **AD** 影子帐户

用于关联前端身份和后端身份的方法是使用匹配的 UPN。这两个关联的身份应具有相同的 UPN，这样 Workspace 就可以知道它们代表的是需要登录 Workspace、枚举和启动 DaaS 资源的同一个最终用户。

简化的 **SAML** 是否需要 **Citrix FAS**

是。当使用任何联合身份验证方法登录 Workspace 时，SSON 在 VDA 启动期间都需要 FAS。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

什么是“**SID** 不匹配问题”？何时会发生

当 SAML 断言包含前端用户的 SID 与 AD 影子帐户用户的 SID 不匹配时，就会出现“SID 不匹配问题”。当登录到您的 SAML 提供商的帐户具有本地 SID（与影子帐户用户的 SID 不同）时，就会发生这种情况。只有当前端身份由 Entra ID connect 等 AD 同步工具进行配置，并且来自与创建影子帐户时不同的 AD 林时，才会发生这种情况。

简化的 SAML 可防止“SID 不匹配问题”的发生。始终通过加入后端 AD 域的 Citrix Cloud Connector 为影子帐户用户获取正确的 SID。使用前端用户的 UPN 执行影子帐户用户查询，然后将其与相应的后端影子帐户用户进行匹配。

SID 不匹配问题示例：
前端用户由 Entra ID connect 创建，并从 **AD** 林 **1** 同步。
`S-1-5-21-000000000-0000000000-0000000001-0001`

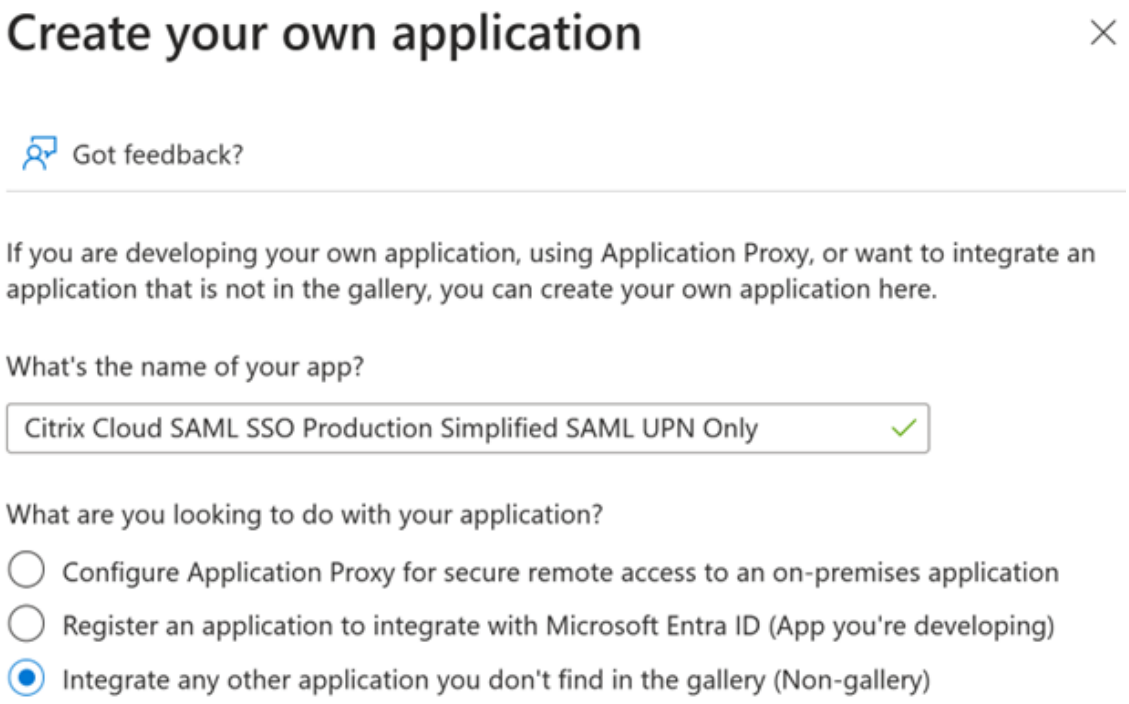
后端影子帐户用户是在 **AD** 森林 **2** 中创建的，并映射到 DaaS 资源
`S-1-5-21-000000000-0000000000-0000000002-0002`

SAML 断言包含所有四个 cip_* 属性，**cip_sid** 包含值 `S-1-5-21-000000000-0000000000-0000000001-0001`，该值与影子帐户的 SID 不匹配并会触发错误。

使用 **Entra ID** 为外部来宾帐户配置简化的 **SAML**

1. 登录 Azure 门户。
2. 在门户菜单中，选择 **Entra ID**。
3. 在左侧窗格的“管理”下，选择“企业应用程序”。
4. 选择“创建自己的应用程序”。
5. 为 SAML 应用程序输入合适的名称，例如 `Citrix Cloud SAML SSO Production Simplified SAML`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. 在左侧导航窗格中，选择单点登录，然后在工作窗格中单击 **SAML**。
7. 在“基本 **SAML** 配置”部分中，单击“编辑”并配置以下设置：

   a) 在 标识符（实体 **ID**）部分，选择 添加标识符，然后输入与您的 Citrix Cloud 租户所在区域关联的值：

   - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com`。
   - 对于日本区域，请输入 `https://saml.citrixcloud.jp`。
   - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

   b) 在“回复 **URL**（断言消费者服务 **URL**）”部分，选择“添加回复 **URL**”，然后输入与 Citrix Cloud 租户所在区域关联的值：

   - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
   - 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/acs`。
   - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

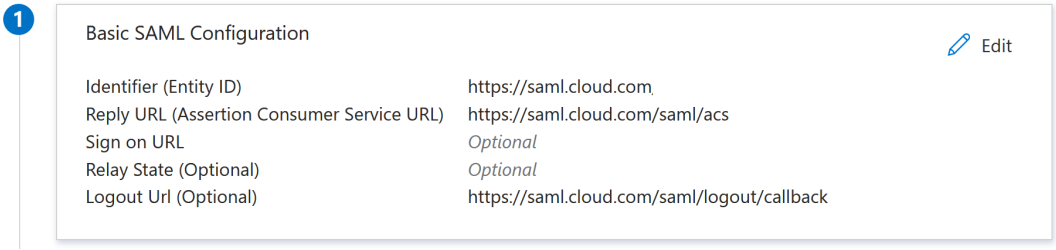
   c) 在“登录 **URL**”部分，输入您的 Workspace URL。

   d) 在注销 **URL**（可选）部分，输入与您的 Citrix Cloud 租户所在区域关联的值：

   - 对于欧洲、美国和亚太南部地区，请输入 `https://saml.cloud.com/saml/logout/callback`。
   - 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/logout/callback`。
   - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/logout/callback`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

e) 在命令栏上，单击“保存”。“基本 **SAML** 配置”部分显示如下：



8. 在“属性和声明”部分，单击“编辑”以配置以下声明。这些声明出现在 SAML 响应中的 SAML 断言中。创建 SAML 应用程序后，配置以下属性。

a) 对于 唯一用户标识符（姓名 **ID**）声明，请保留默认值 `user.userprincipalname`。

b) 对于 **cip_upn** 声明，请保留 `user.userprincipalname` 的默认值。

c) 对于 **displayName**，请保留 `user.displayname` 的默认值。

d) 在“其他声明”部分中，对于 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` 命名空间的所有剩余声明，请单击省略号 (…) 按钮，然后单击“删除”。无需包含这些声明，因为它们是上述用户属性的重复。

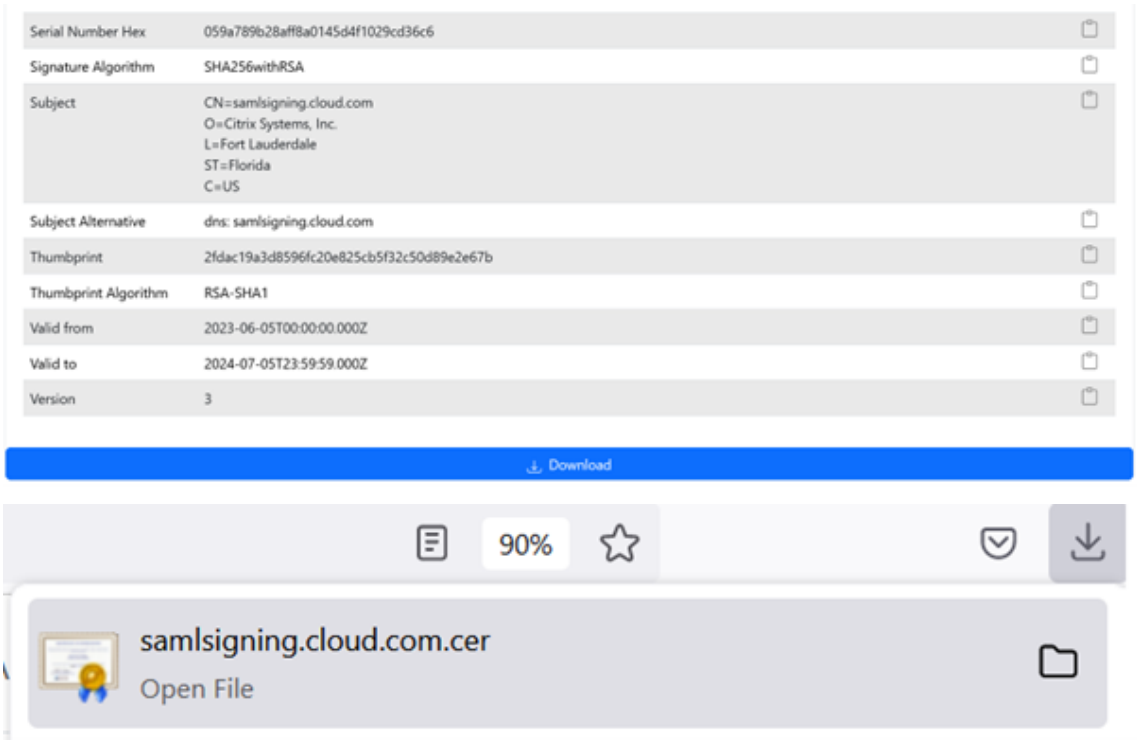
完成后，“属性和声明”部分将显示如下所示：

e) 使用此第三方在线工具获取 Citrix Cloud SAML 签名证书的副本。

f) 在 URL 字段中输入 `https://saml.cloud.com/saml/metadata` 并单击“加载”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

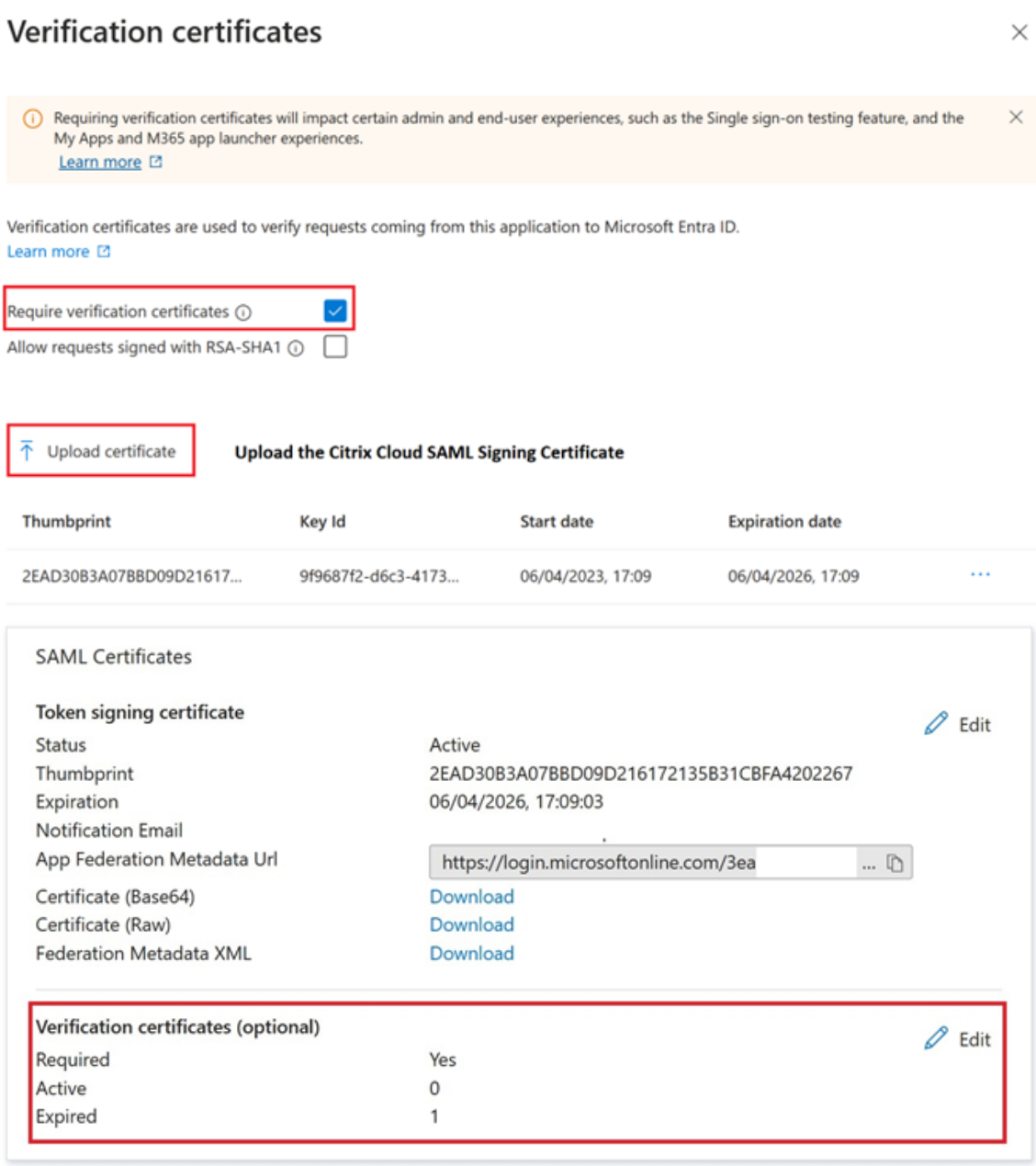
9. 滚动到页面底部，然后单击“下载”。



10. 配置 Azure Active Directory SAML 应用程序签名设置。
11. 在 Azure Active Directory SAML 应用程序中上载步骤 10 中获得的生产 SAML 签名证书

    a) 启用“需要验证证书”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



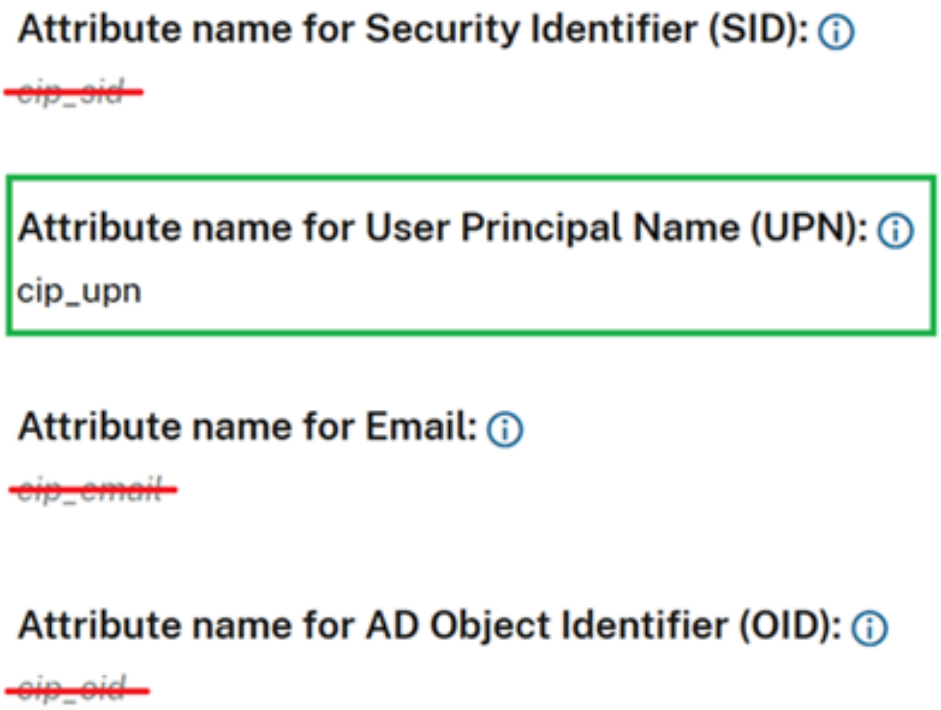
配置 **Citrix Cloud** 简化的 **SAML** 连接

默认情况下，Citrix Cloud 预计在 SAML 断言中会出现 cip_upn、cip_email、cip_sid 和 cip_oid，如果不发送这些属性，SAML 登录将失败。为防止出现这种情况，请在创建新的 SAML 连接时取消对这些属性的检查。

1. 使用默认设置创建新的 SAML 连接。
2. 导航到底部的“**SAML** 属性映射配置”部分，在保存新的 SAML 配置之前进行更改。
3. 从每个 **cip_email**、**cip_sid** 和 **cip_oid** 字段中删除 SAML 属性名称。
4. 不要从其字段中删除 **cip_upn**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. 不要从各自的字段中移除任何其他属性。Workspace 用户界面仍然需要 **displayName**，不应进行更改。



配置您的 **AD** 影子帐户资源位置和连接器

后端影子帐户 AD 林中的资源位置和连接器对是必需的。当 SAML 断言中直接提供 cip_upn 时，Citrix Cloud 要求此 AD 林中的连接器查找影子帐户用户的身份和属性，例如 cip_email、cip_sid 和 cip_oid。

1. 创建一个新的资源位置，其中将包含加入后端影子帐户 AD 林的 Citrix Cloud Connector。

2. 命名资源位置以匹配 AD 林，其中包含您要使用的后端 AD 影子帐户。
3. 在新创建的资源位置内配置一对 Citrix Cloud Connector。

举个例子

```
ccconnector1.shadowaccountforest.com
ccconnector2.shadowaccountforest.com
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在后端 **AD** 林中配置 **FAS**

承包商前端用户肯定需要 FAS。在 DaaS 启动期间，承包商用户将无法手动输入 Windows 凭据来完成启动，因为他们可能不知道 AD 影子帐户的密码。

1. 在创建影子帐户的后端 AD 林中配置一个或多个 FAS 服务器。
2. 将 FAS 服务器链接到包含两个 Citrix Cloud Connector 的同一个资源位置，这些连接器已连接到创建影子帐户的后端 AD 林。

在 **AD** 域中配置备用 **UPN** 后缀

> 重要：
>
> UPN 与用户的电子邮件地址不同。在许多情况下，为了便于使用，它们具有相同的值，但是 UPN 和电子邮件具有不同的内部用途，并且定义在不同的 active Directory 属性中。

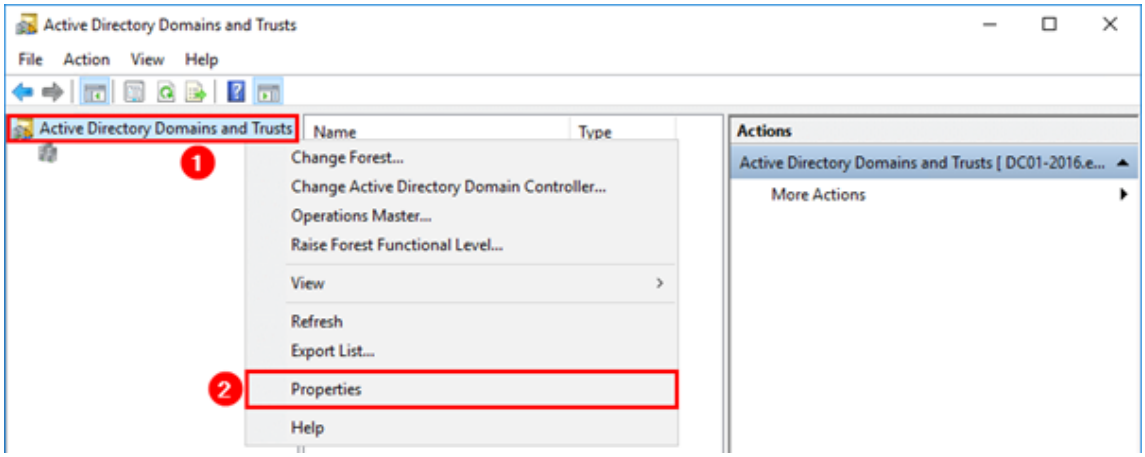
用户主体名称 (UPN) 后缀是 AD 中登录名称的一部分。当您创建新帐户时，它会默认使用您的 AD 林的隐式 UPN 后缀，例如 yourforest.com。您需要为您希望邀请加入 Okta 或 Azure AD 租户的每位外部前端用户添加匹配的备用 UPN 后缀。

例如，如果您邀请外部用户 `contractoruser@hotmail.co.uk` 并希望将其与后端 AD 影子帐户 `contractoruser@yourforest.com` 关联起来，则在您的 AD 林中添加 `yourforest.com` 作为 ALT UPN 后缀。

使用 **Active Directory** 域和信任 **UI** 在 **Active Directory** 中添加备用 **UPN** 后缀

1. 登录您的后端 AD 林中的域控制器。
2. 打开“运行”对话框，键入 `domain.msc`，然后单击“确定”。
3. 在 Active Directory 域和信任窗口中，右键单击 **Active Directory** 域和信任，然后选择“属性”。
4. 在 **UPN** 后缀选项卡上的“备用 UPN 后缀”框中，添加备用 UPN 后缀，然后选择“添加”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. 单击确定。

使用 **PowerShell** 管理您的后端 **AD** 林的 **UPN** 后缀

您可能需要向后端 AD 林中添加大量新的 UPN 后缀，才能创建必要的影子帐户 UPN。您需要向后端 AD 林中添加备用 UPN 后缀的数量将取决于您选择邀请多少不同的外部用户加入 SAML 提供商租户。

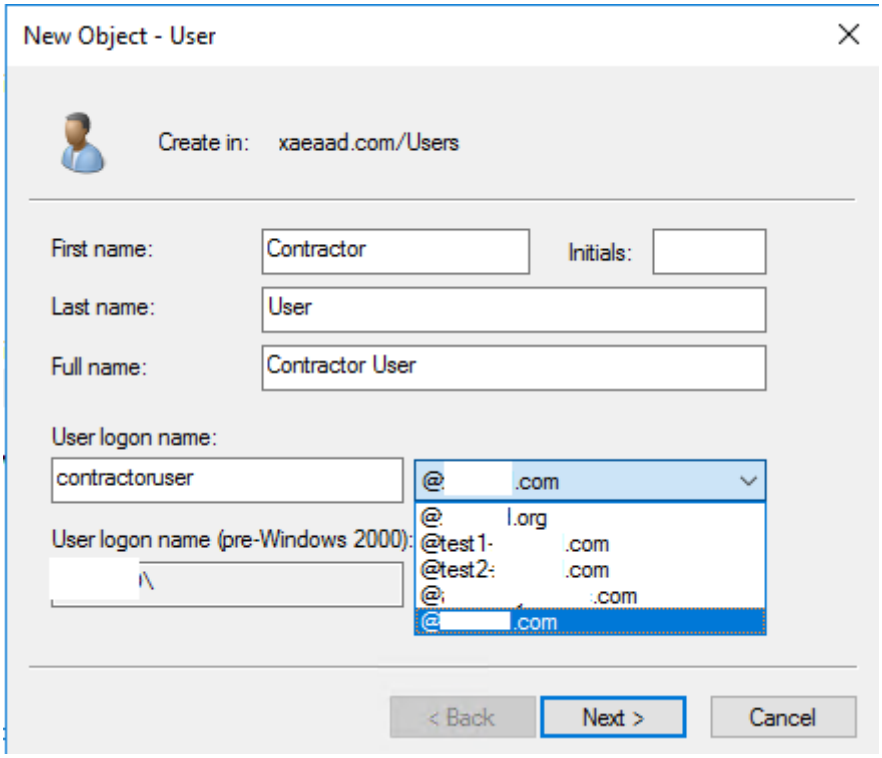
如果需要创建大量新的备用 UPN 后缀，以下是一些可以实现此目的的 PowerShell。

```
# Get the list of existing ALT UPN suffixes within your AD Forest
(Get-ADForest).UPNSuffixes

# Add or remove ALT UPN Suffixes
$NewUPNSuffixes = @("yourforest.com","externalusers.com")

# Set action to "add" or "remove" depending on the operation you wish
   to perform.
$Action = "add"
foreach($NewUPNSuffix in $NewUPNSuffixes)
{

    Get-ADForest | Set-ADForest -UPNSuffixes @{
 $Action=$NewUPNSuffix }

 }

<!--NeedCopy-->
```

在您的后端 **AD** 林中配置 **AD** 影子帐户

1. 创建新的 AD 影子帐户用户。
2. 默认情况下，新的 AD 用户会选择 AD 林隐式 UPN，例如 `yourforest.local`。选择您之前创建的相应备用 UPN 后缀。例如，选择 `yourforest.com` 作为影子帐户用户的 UPN 后缀。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



影子帐户用户的 UPN 也可以通过 PowerShell 更新。

```
Set-ADUser "contractoruser" -UserPrincipalName "
   contractoruser@yourforest.com"
<!--NeedCopy-->
```

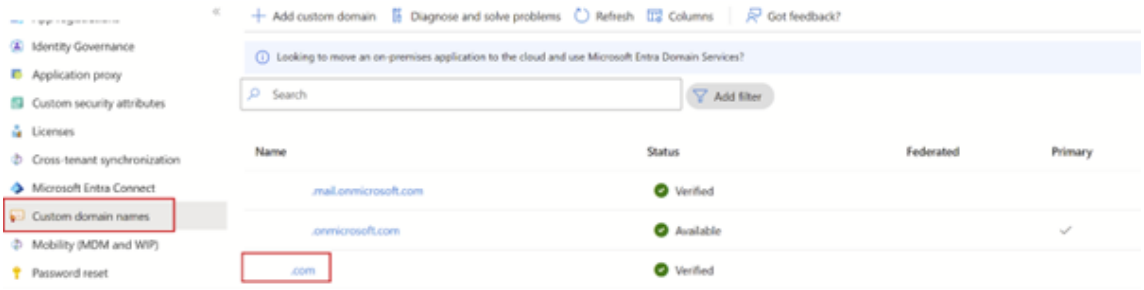
3. 影子帐户用户的 UPN 应与外部前端身份用户的 UPN 完全匹配。
4. 测试前端用户登录 Workspace 的情况。
5. 验证登录成功后，在 Workspace 中枚举了所有预期的资源。映射到 AD 影子帐户的资源应显示出来。

配置来宾输入 **ID** 用户 **UPN** 以匹配 **AD** 影子帐户 **UPN**

当邀请外部来宾用户加入 Entra ID 租户时，会创建一个自动生成的 UPN，表明该用户是外部用户。将自动为外部 Entra ID 用户分配 @Entra IDtenant.onmicrosoft.com UPN 后缀，该后缀不适合与简化的 SAML 一起使用，也与您的 AD 影子帐户不匹配。需要对其进行更新，以匹配 Entra ID 中导入的 DNS 域以及您在 AD 林中创建的备用 UPN 后缀。

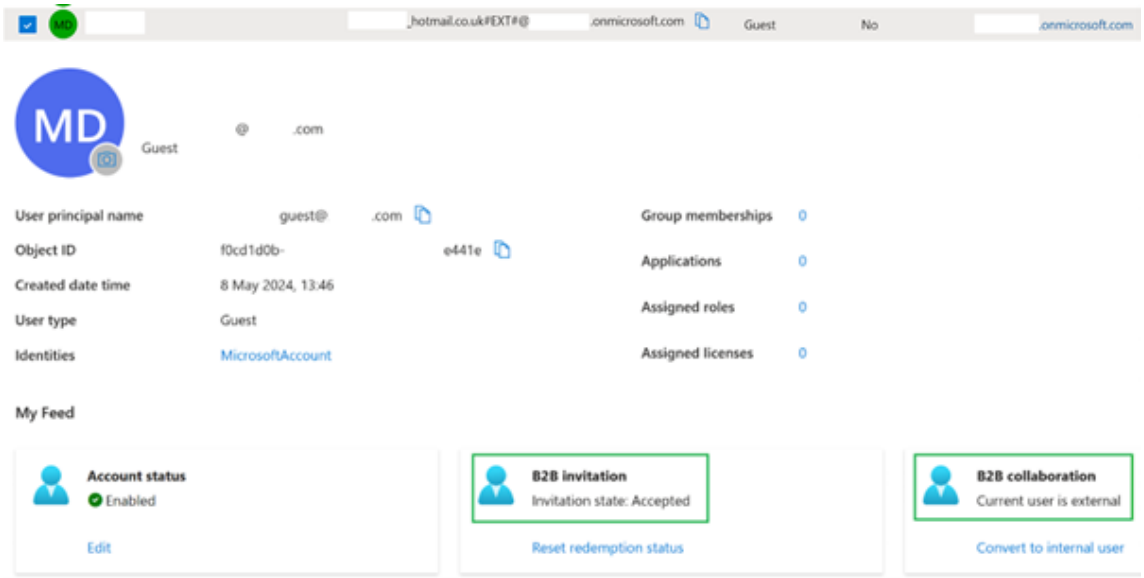
1. 将与您添加到 AD 林中的备用 UPN 后缀相匹配的自定义域名导入 Entra ID。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. 邀请来宾用户（例如 `contractoruser@hotmail.co.uk`）并确保受邀来宾用户接受 Entra ID 租户的 Microsoft 邀请。

   Microsoft 生成的外部来宾用户 UPN 格式示例。
   `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



> 重要：
>
> Citrix Cloud 和 Workspace 不能使用包含 # 字符的 UPN 进行 SAML 身份验证。

3. 安装必要的 Azure PowerShell Graph 模块以允许您管理 Entra ID 用户。

```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
<!--NeedCopy-->
```

4. 使用全局管理员帐户和 `Directory.AccessAsUser.All` 作用域登录到您的 Entra ID 租户。

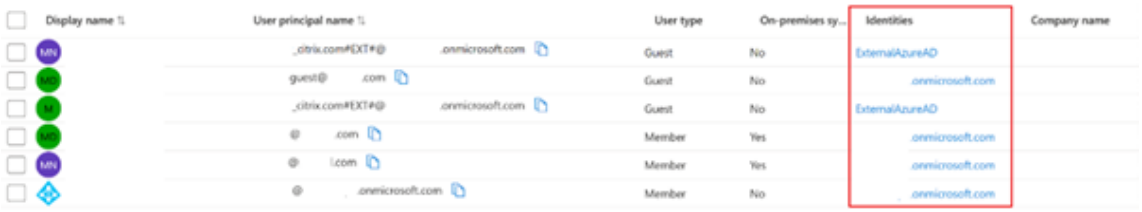
> 重要：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 如果您使用权限较低的帐户或未指定 `Directory.AccessAsUser.All` 作用域，则将无法完成步骤 4 和更新来宾用户的 UPN。

```
$EntraTenantID = "<yourEntraTenantID>"
Connect-MgGraph -Tenant $EntraTenantID -Scopes "Directory.
    AccessAsUser.All"
<!--NeedCopy-->
```

5. 获取 Entra ID 租户中外部来宾用户的完整列表（可选）。




```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
<!--NeedCopy-->
```

6. 获取需要更新 UPN 的来宾用户身份，然后更新其 UPN 后缀。

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourEntra IDtenant.onmicrosoft.com").Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

7. 检查来宾用户身份可以使用其最新更新的 UPN 找到。

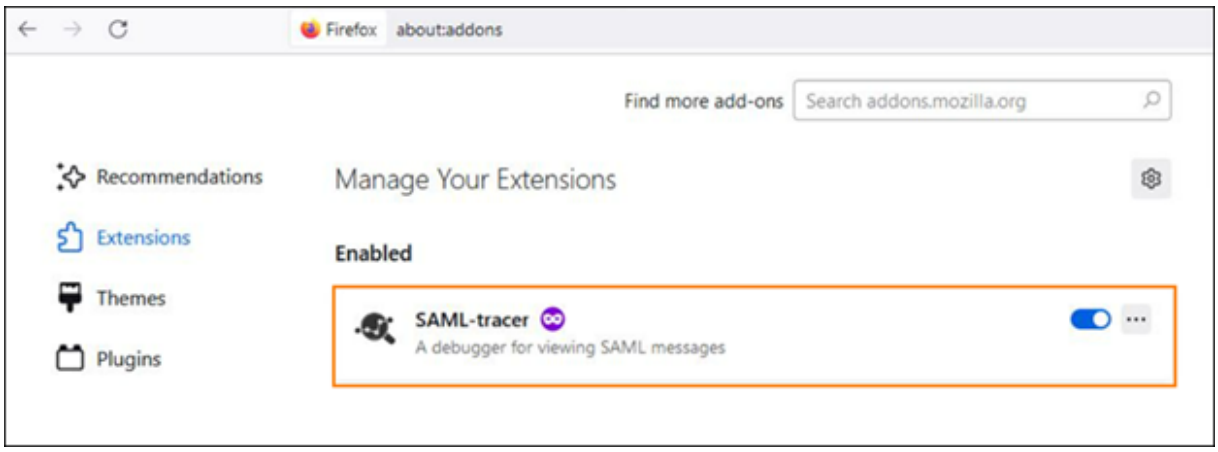
```
Get-MgUser -UserId "contractoruser@yourforest.com"
<!--NeedCopy-->
```

测试简化的 **SAML** 解决方案

在 AD、Citrix Cloud 和您的 SAML 提供商中完成所有记录的步骤后，您需要测试登录并验证在 Workspace 中为来宾用户显示的资源列表是否正确。

Citrix 建议在所有 SAML 调试中使用 SAML-Tracer 浏览器扩展程序。此扩展程序适用于大多数常见的网络浏览器。该扩展程序将 Base64 编码的请求和响应解码为 SAML XML，这样它们便于人类阅读。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



使用 SAML tracer 捕获的仅使用 cip_upn 进行身份验证的简化的 SAML 断言示例。

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>        </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. 将正确的 DaaS 资源映射到由 AD 支持的和影子帐户用户或包含这些资源的组。
2. 启动 SAML tracer 浏览器扩展程序并捕获整个登录和注销流程。
3. 使用表中为要测试的前端用户类型指定的属性登录到 Workspace。

   来宾 **Entra ID** 用户登录：您作为来宾用户邀请加入 Entra ID 租户的承包商用户拥有该电子邮件地址 contractoruser@hotmail.co.uk。

   Entra ID 提示时，输入来宾用户的电子邮件地址。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

或

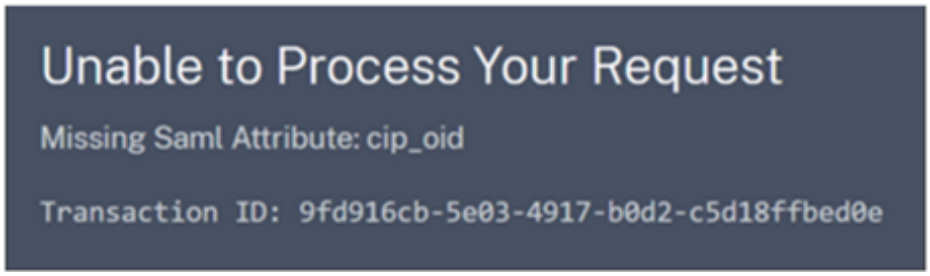
AD 支持的 **EntraID** 用户/本地 **EntraID** 用户登录：这些 Entra ID 用户将拥有格式为 `adbackeduser@yourforest.com` 或 `nativeuser@yourforest.com` 的 UPN。

当出现 Entra ID 提示时，输入用户的 **UPN**。

4. 检查断言仅包含用于身份验证的 **cip_upn** 属性，并且它还包含 Workspace 用户界面要求的 **displayName** 属性。
5. 检查用户能否在用户界面中看到所需的 DaaS 资源。

对简化的 **SAML** 解决方案进行故障排除

缺少 **cip_*** 属性错误



原因 1：SAML 断言中不存在 SAML 属性，但是 Citrix Cloud 配置为期望接收该属性。您未能在 SAML 属性部分中从 Citrix Cloud SAML 连接中删除不必要的 cip_* 属性。断开连接并重新连接 SAML 以删除对不必要的 cip_* 属性的引用。

原因 2：如果 Citrix Cloud Connector 在您的后端 AD 林中没有相应的 AD 影子帐户可供查找，也可能发生此错误。您可能已正确配置了前端身份，但带有匹配的 UPN 的后端 AD 影子帐户身份不存在或找不到。

登录成功，但在用户登录 **Workspace** 后不显示 **DaaS** 资源

原因：这很可能是由不正确的前端到后端身份 UPN 映射造成的。

确保前端和后端身份的 2 个 UPN 完全匹配并代表登录到 Workspace 的同一最终用户。检查 DaaS 交付组是否包含指向正确 AD 影子帐户用户或包含这些用户的 AD 组的映射。

在启动 **DaaS** 资源期间，加入了 **AD** 域的 **FAS SSON** 出现故障

尝试启动 DaaS 资源时，系统会提示 Workspace 最终用户在 GINA 中输入其 Windows 凭据。此外，事件 ID 103 出现在您的 FAS 服务器的 Windows 事件日志中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

[S103] Server [CC:FASServer] requested UPN [frontenduser@yourforest.com] SID S-1-5-21-000000000-00
, but lookup returned SID S-1-5-21-000000000-0000000000-0000000001-0002.
[correlation: cc#967472c8-4342-489b-9589-044a24ca57d1]

原因：您的简化的 SAML 部署出现“SID 不匹配问题”。您的前端身份包含来自 AD 林的 SID，该林与后端影子帐户 AD 林不同。
不要在 SAML 断言中发送 **cip_sid**。

当多个连接的 **AD** 林中存在相同的 **UPN** 后缀时，支持 **AD** 的用户登录失败

Citrix Cloud 有多个资源位置和连接器连接到不同的 AD 林。当 AD 支持的用户从与影子 accountAD 林不同的 AD 林导入 Entra ID 时，登录失败。

AD 林 1 与 Entra ID 同步，使用 UPN 创建前端用户，例如 frontenduser@yourforest.com。

AD 林 2 包含带有 UPN 的后端影子帐户，例如 frontenduser@yourforest.com。

原因：您的简化的 SAML 部署遇到“UPN 歧义问题”。Citrix Cloud 无法确定使用哪些连接器来查找用户的后端身份。

不要在 SAML 断言中发送 **cip_sid**。
您的用户的 UPN 存在于连接到 Citrix Cloud 的多个 AD 林中。

将本地 **PingFederate** 服务器配置为工作区和 **Citrix Cloud** 的 **SAML** 提供商

April 26, 2024

Author:
Mark Dear

本文由 Citrix 和 Ping 的两位工程师合作撰写，经过双方审查，以确保撰写本文时技术准确无误。有关如何预置、配置和许可本地 PingFederate 服务器用作 SAML 提供商的说明，请参阅 Ping 文档，因为这超出了本文的范围。

本文档使用 PingFederate 版本 11.3 和 12 撰写。

必备条件

本文专门介绍了 SAML 配置，并确保满足以下条件。

- 您已经在组织内部配置了本地 PingFederate 服务器并获得了必要的许可证。有关更多信息，请参阅 PingFederate 安装。
- 您需要在 PingFederate 服务器上安装支持的 Java 版本。有关支持的 Java 版本，请参阅 Ping 身份文档。有关更多信息，请参阅 Java PingFederate 要求。

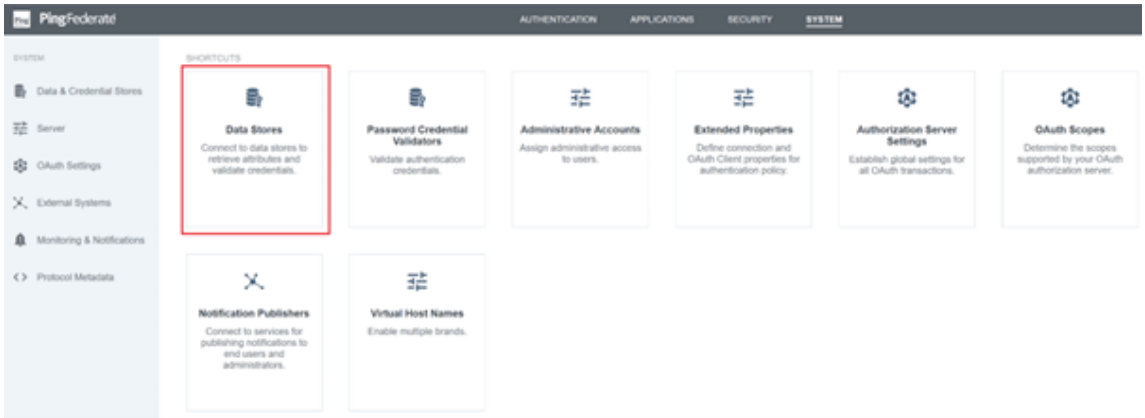
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 您已经配置了所需的网络和防火墙规则，以允许 Citrix Cloud 和 Workspace 在 Workspace/Citrix Cloud 管理控制台 SAML 登录过程中重定向到本地 PingFederate 服务器。有关更多信息，请参阅 PingFederate 网络要求。
- 您已经将公开签名的 x509 证书导入到您的 PingFederate 服务器上，该证书可以用作 PingFederate 服务器的服务器证书。
- 您已将公开签名的 x509 证书导入到您的 PingFederate 服务器上，该证书可以用作 IdP 的 SAML 签名证书。在 SAML 连接过程中，必须将此证书上载到 Citrix Cloud。
- 您已将本地 Active Directory 连接到 PingFederate。有关更多信息，请参阅 PingFederate LDAP 数据存储

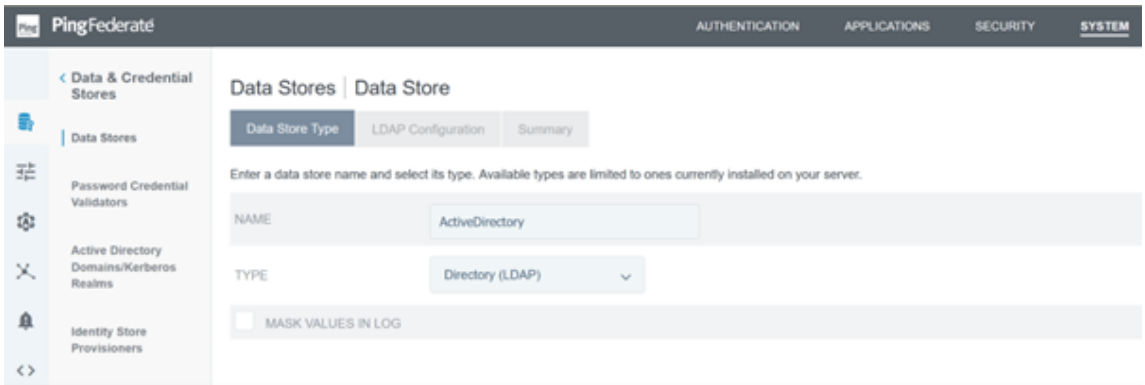
> 注意：
>
> 在配置 PingFederate 以与 Citrix Cloud 和 Workspace 配合使用时，请参阅 PingFederate 文档，了解各个 SAML 设置的作用并帮助补充此处提供的说明。

使用 **PingFederate** 中的数据存储配置与您的 **AD** 域的 **Active Directory** 连接

1. 在数据存储中配置 Active Directory 连接。

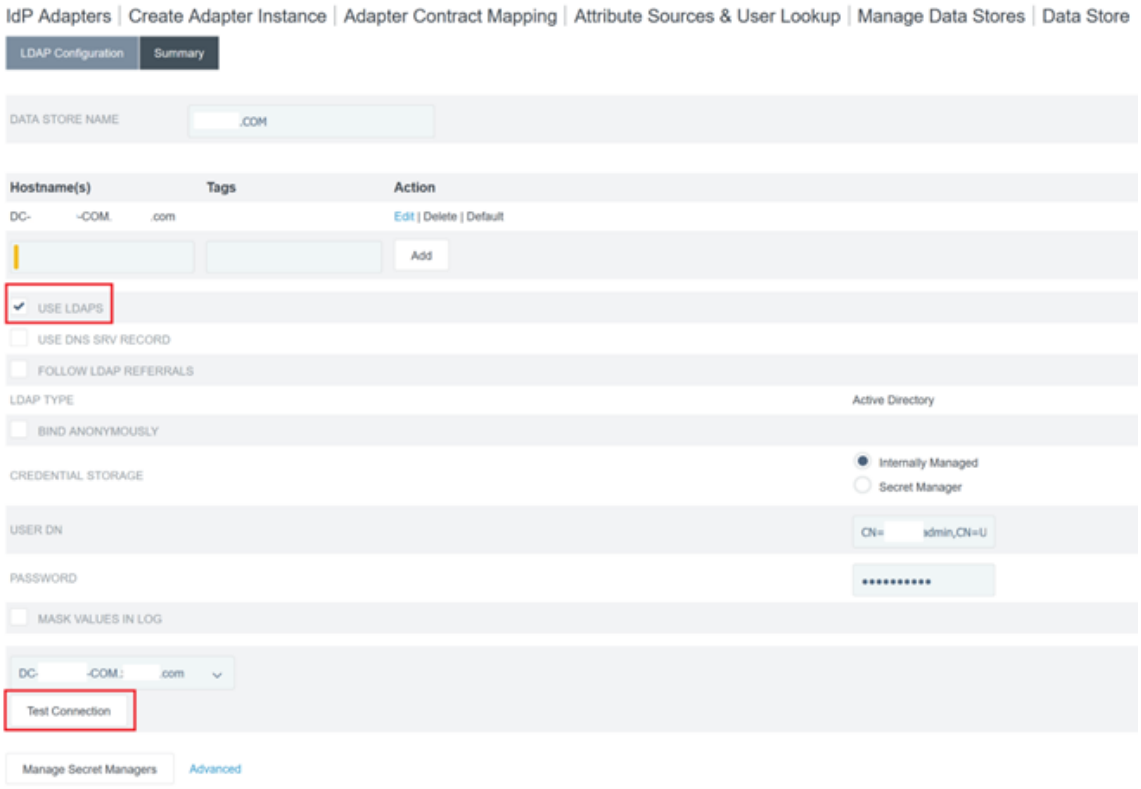


2. 选择“键入为目录 **(LDAP)**”。

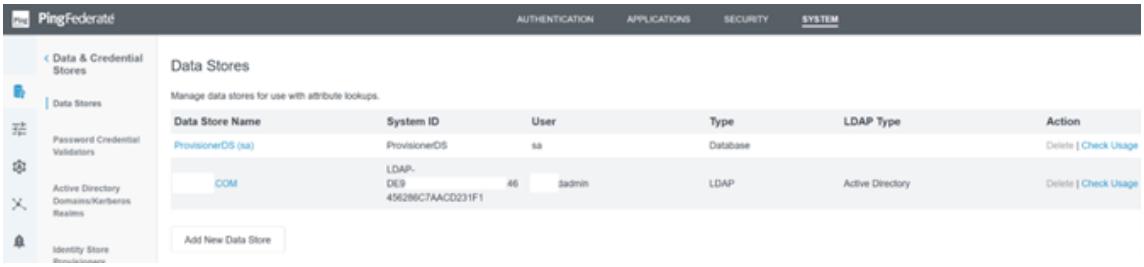


3. 为 LDAPS 连接配置域控制器，并在主机名字段中添加域控制器 FQDN 列表。然后单击“测试连接”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

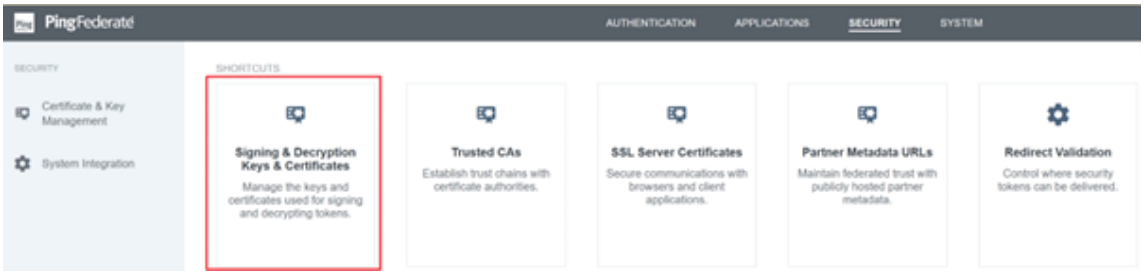


4. 配置完成后，Active Directory 连接应与以下示例类似：



上载 **Citrix Cloud SAML** 签名证书

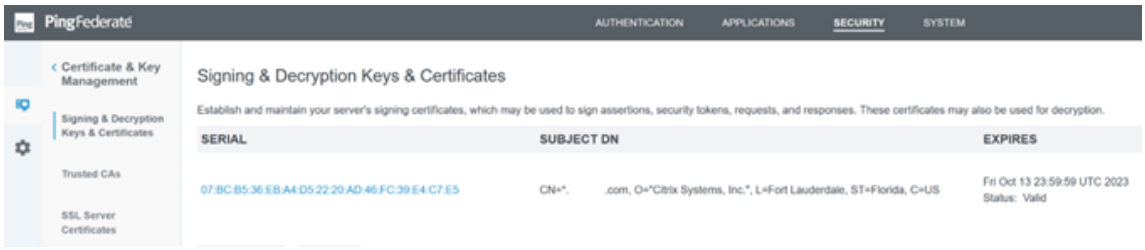
1. 单击“安全”选项卡
2. 在签名和解密密钥和证书中上载您希望 PingFederate 使用的 SAML 签名证书。



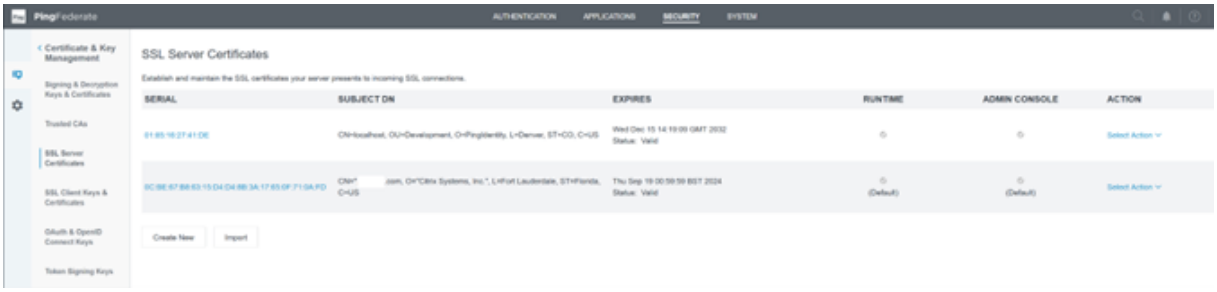
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 在本示例中，使用的证书是公开签名的 Digicert `pingfederateserver.domain.com` 证书。

3. 上载用于签署您的 PingFederate 服务器 SAML 签名证书的所有 CA 证书。



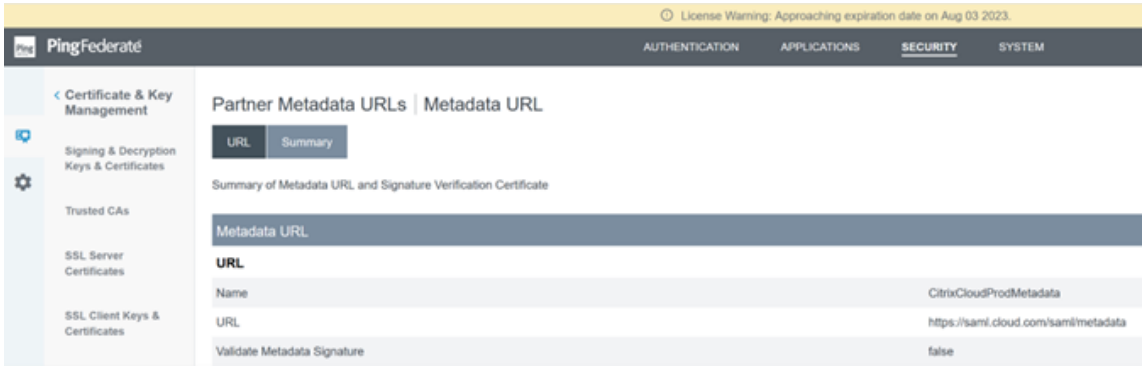
> 注意：
>
> PingFederate 服务器证书和 SAML 签名证书可以是相同的 SSL 证书，也可以使用不同的 SSL 证书。配置 SAML 连接时，需要向 Citrix Cloud 提供 SAML 签名证书的副本。



上载 **Citrix Cloud** 元数据

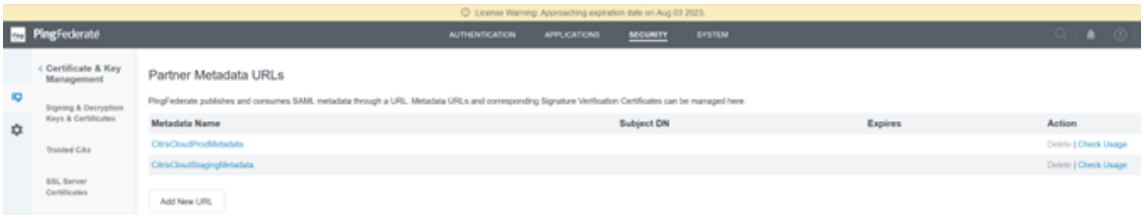
1. 提供 Citrix Cloud 元数据的名称，然后输入与您的 Citrix Cloud 租户所在的 Citrix Cloud 区域相对应的元数据 URL。

   - https://saml.cloud.com/saml/metadata - 商用，欧盟、美国和亚太地区
   - https://saml.citrixcloud.jp/saml/metadata - 日本
   - https://saml.cloud.us/saml/metadata -政府



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

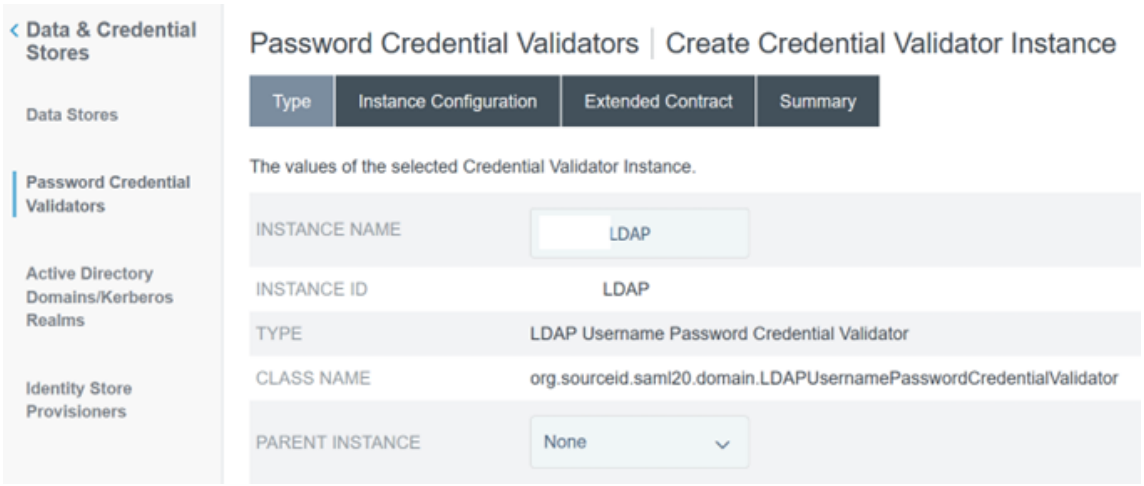
2. 配置完成后，Citrix Cloud 元数据配置应与以下示例类似。



在 **PingFederate** 中配置密码凭据验证器

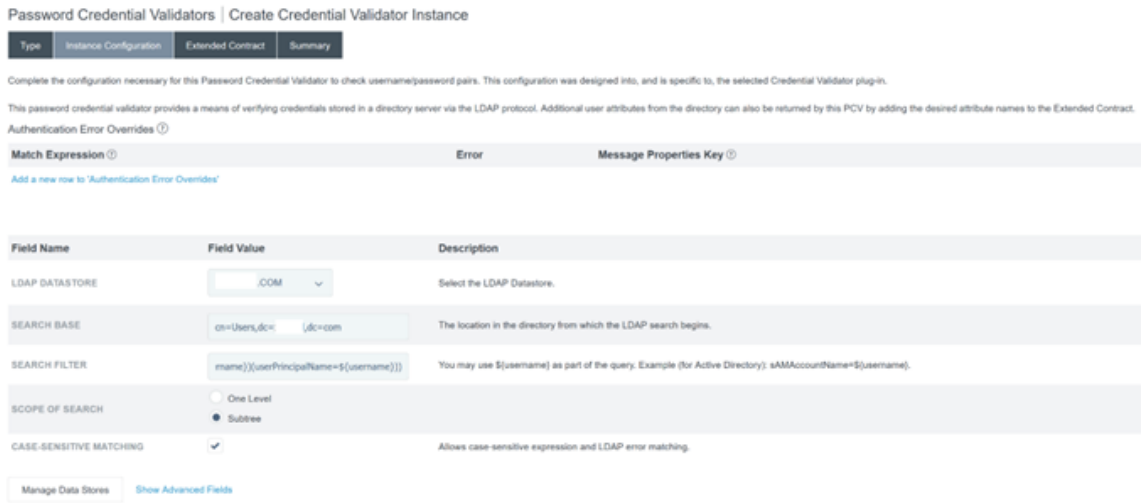
有关更多信息，请参阅 PingFederate 密码凭据验证器

1. 将密码凭据验证器类型配置为 LDAP 用户名和密码。



2. 配置实例配置。选择您在使用 PingFederate 中的数据存储配置与您的 AD 域的 Active Directory 连接之前配置的 AD 域连接和数据存储。输入合适的 LDAP 过滤器，如示例所示。

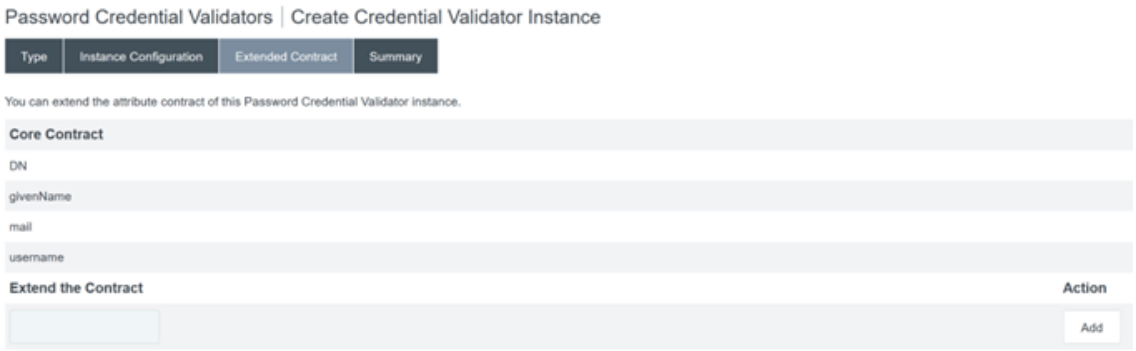
```
(((sAMAccountName=${ username } )(userPrincipalName=${ username } ))
```



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

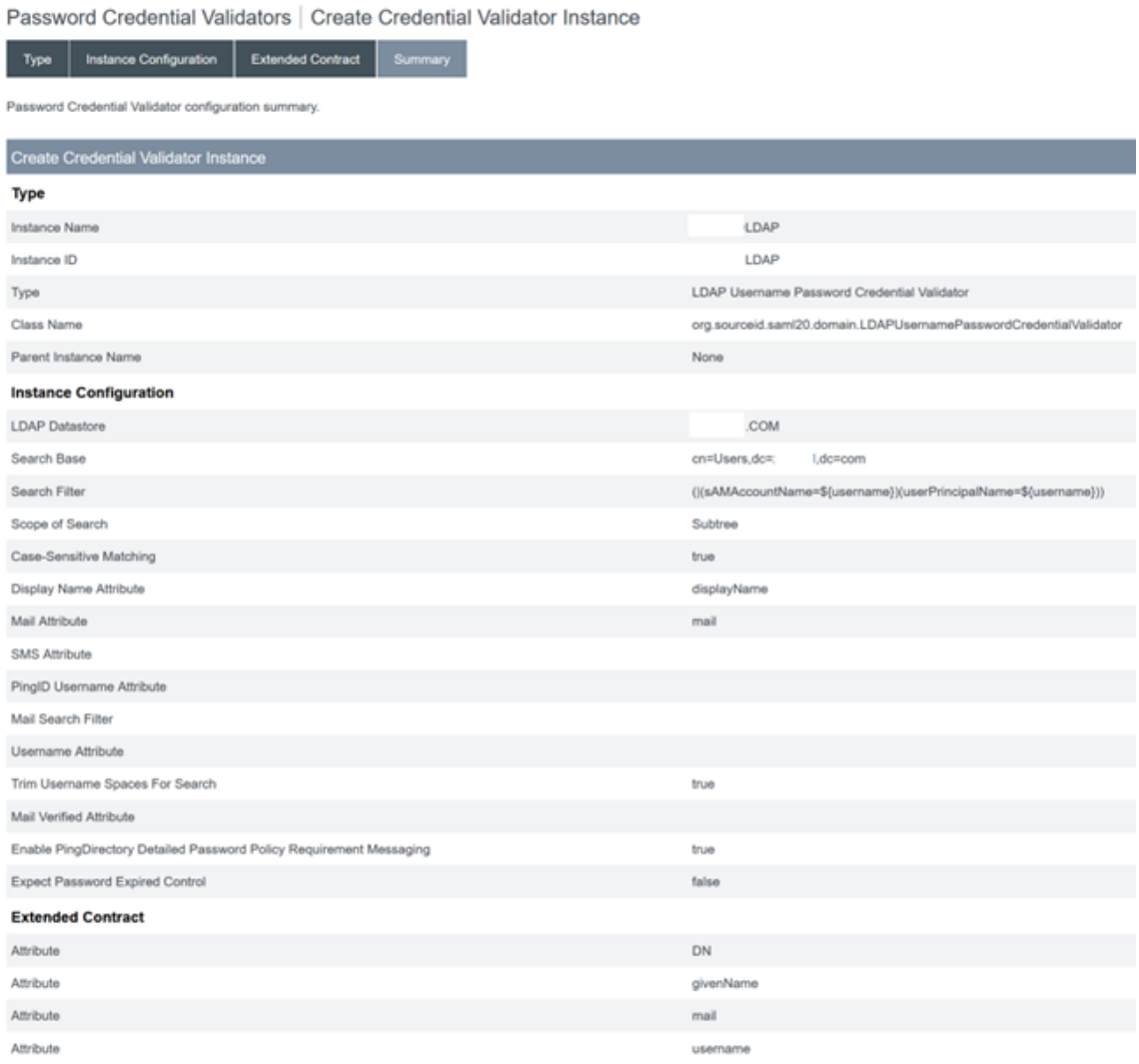
> 注意：示例筛选器匹配 sAMAccountName 和 userPrincipalName AD 用户名格式，使最终用户能够使用这两种格式登录 Workspace 或 Citrix Cloud。示例筛选器支持 sAMAccountName 和 userPrincipalName AD 用户名格式，使最终用户能够使用这两种格式登录 Workspace 或 Citrix Cloud。

3. 配置延期合约。



4. 密码凭据验证器摘要应类似于此示例。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

Password Credential Validator configuration summary.

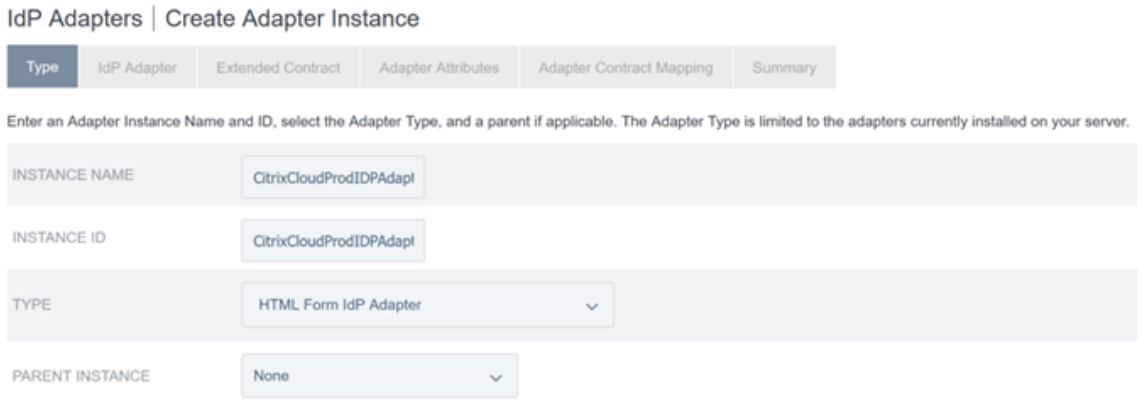
Create Credential Validator Instance	
Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

在 **PingFederate** 中配置 **IDP** 适配器

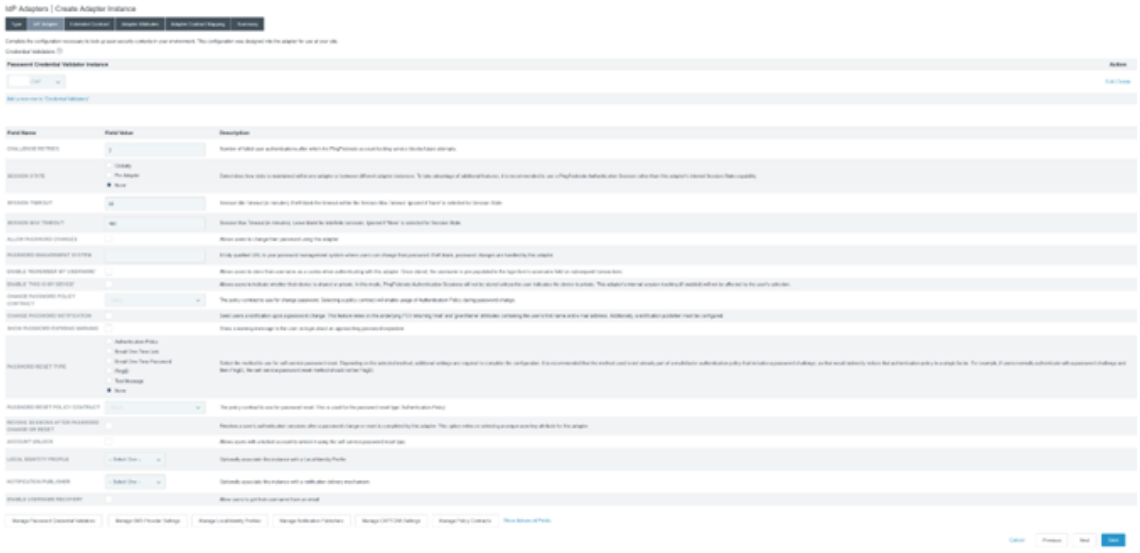
有关更多信息，请参阅 PingFederate HTML 表单适配器

1. 创建类型为 HTML 表单 IdP 适配器的新 IDP 适配器。

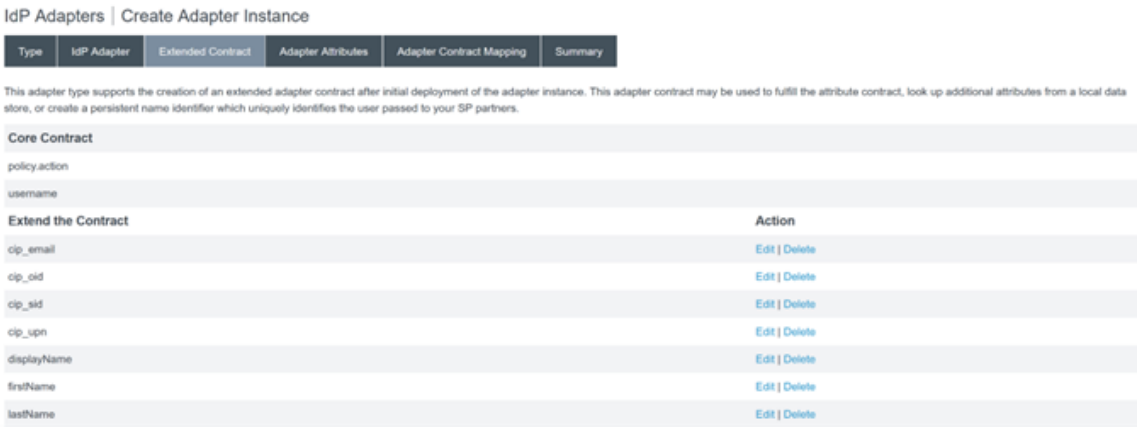
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. 选择您之前配置的现有密码凭据验证器并配置 IDP 适配器。有关更多信息，请参阅在 PingFederate 中配置密码凭据验证器。

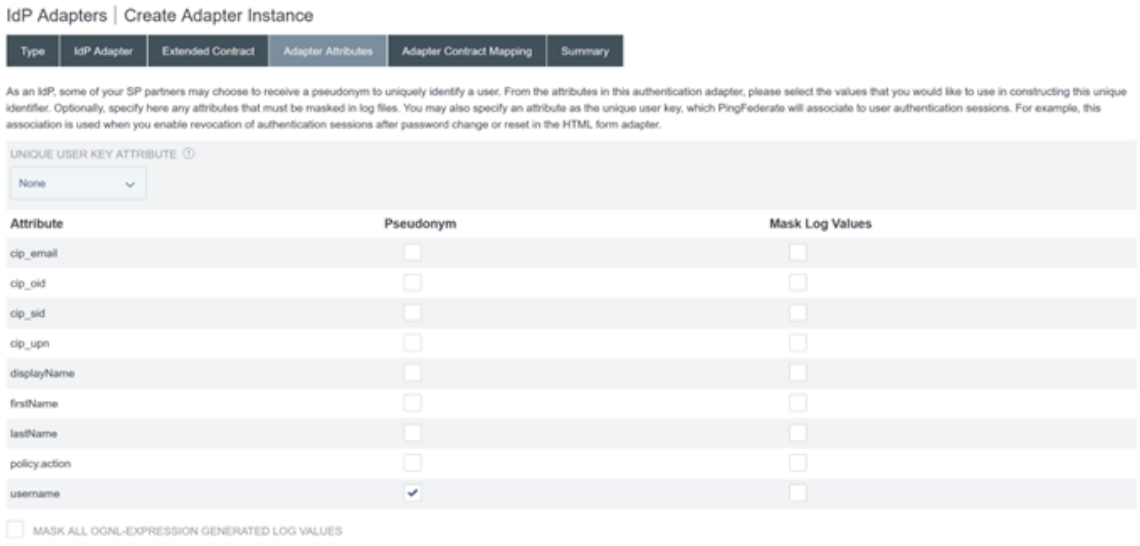


3. 使用在 SAML 登录期间传递给 Citrix Cloud 或 Workspaces 的 SAML 属性配置延期合约。



4. 配置适配器属性。

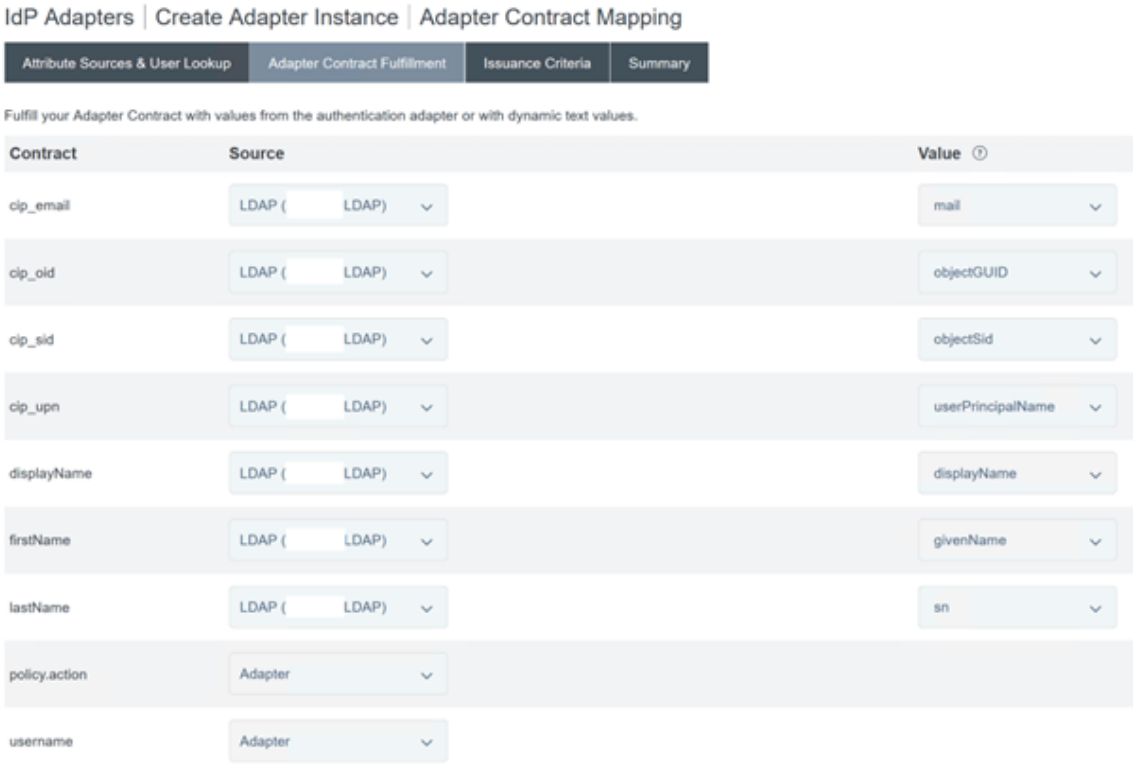
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. 配置适配器合约映射，其中 SAML 属性映射到来自 AD 身份的 LDAP 用户属性。单击“配置适配器合约”。
6. 配置属性来源和用户查询。

7. 配置适配器合约履行。选择 **LDAP** 和 Active Directory 数据存储的名称作为用户属性数据的来源。值是用户的 Active Directory 属性，例如 `objectGUID` 或 `objectSid`。

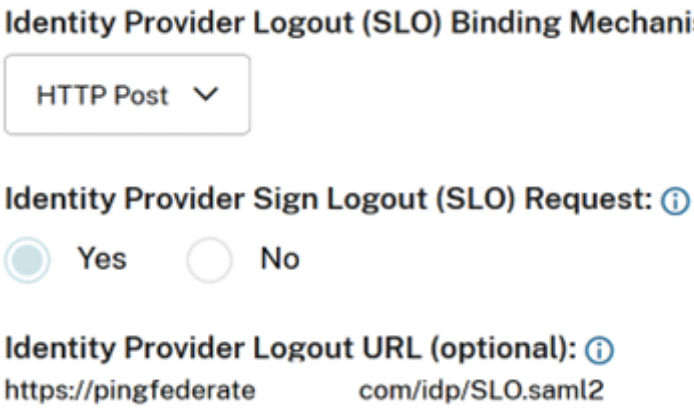
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



为 **Citrix Cloud** 或 **Workspaces** 配置服务提供商连接（**SAML** 应用程序）

下面提供的示例 PingFederate 配置假设您的组织内满足以下 SAML 身份验证要求。

- 从 Workspace/Citrix Cloud 管理员控制台发送的 SAML 身份验证请求必须经过签名。
- SAML HTTP POST 绑定将用于 SSO 和 SLO 请求。
- 单点注销 (SLO) 是组织内部的一项要求。当最终用户退出 Workspace 或 Citrix Cloud 管理控制台时，Citrix Cloud 会向 SAML 提供商 (IdP) 发送 SAML SLO 请求，要求该用户注销。
- PingFederate 需要签名的 HTTP POST 请求才能启动注销。SAML 提供商需要签名的 SLO 请求。

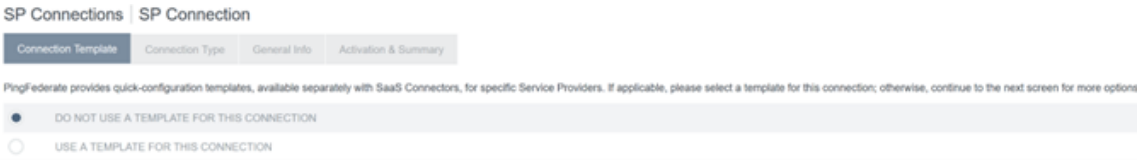


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

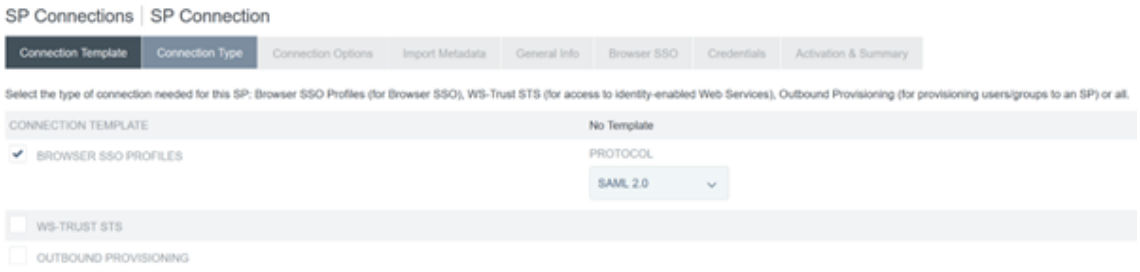
有关更多信息，请参阅 PingFederate SP 管理

过程

1. 配置连接模板。

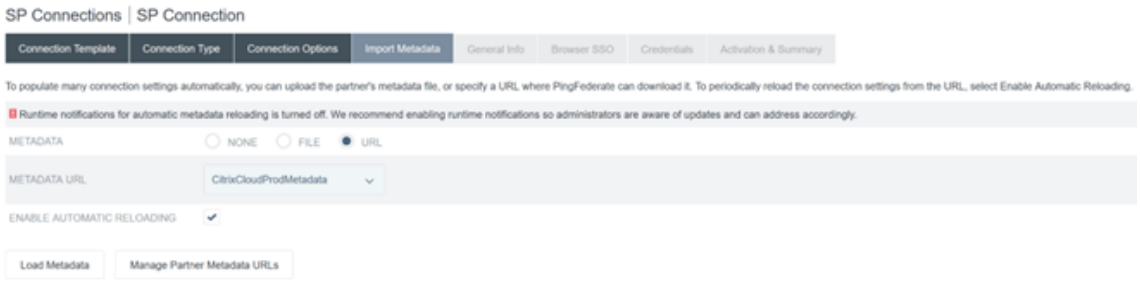


2. 配置连接类型并选择浏览器 **SSO** 配置文件和 **SAML 2.0**。



3. 配置连接选项。

4. 导入 Citrix Cloud 元数据。选择 URL 和您之前创建的 `CitrixCloudProdMetadata` URL，然后单击“加载元数据”

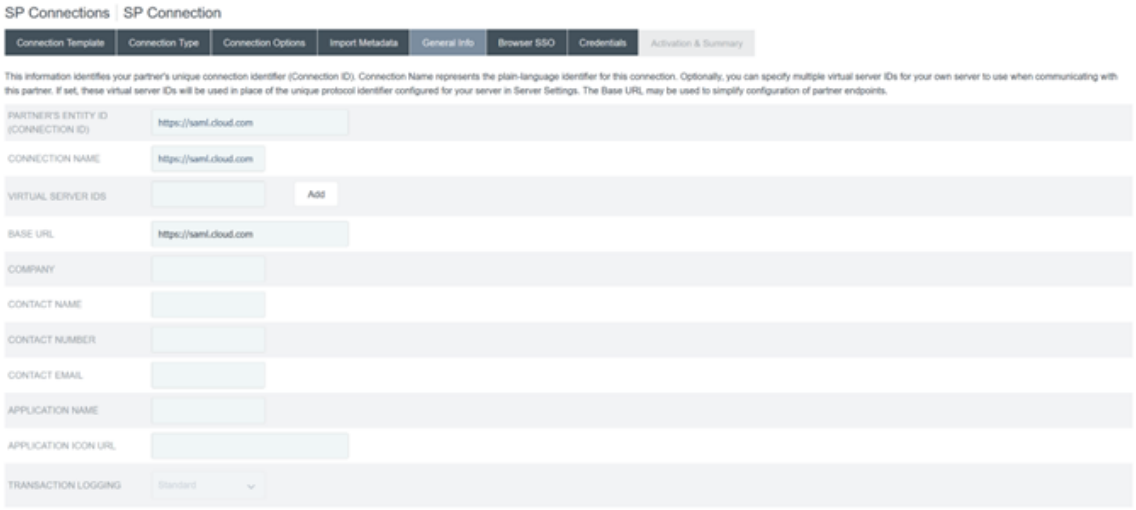


5. 配置常规信息。将服务提供商连接实体 ID、基本 URL 和连接名称设置为 Citrix Cloud 客户区域的 Citrix Cloud SAML 端点。

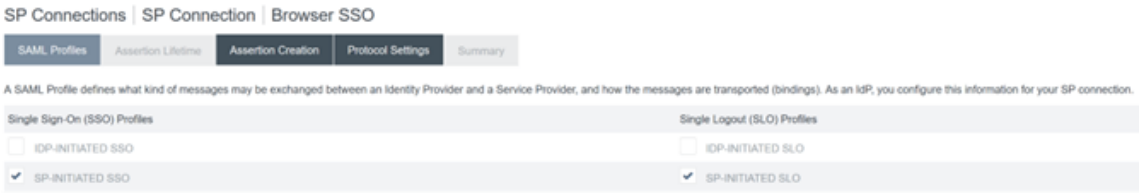
   - https://saml.cloud.com - 商用，欧盟、美国和亚太地区
   - https://saml.citrixcloud.jp - 日本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- https://saml.cloud.us - 政府



6. 配置协议设置。

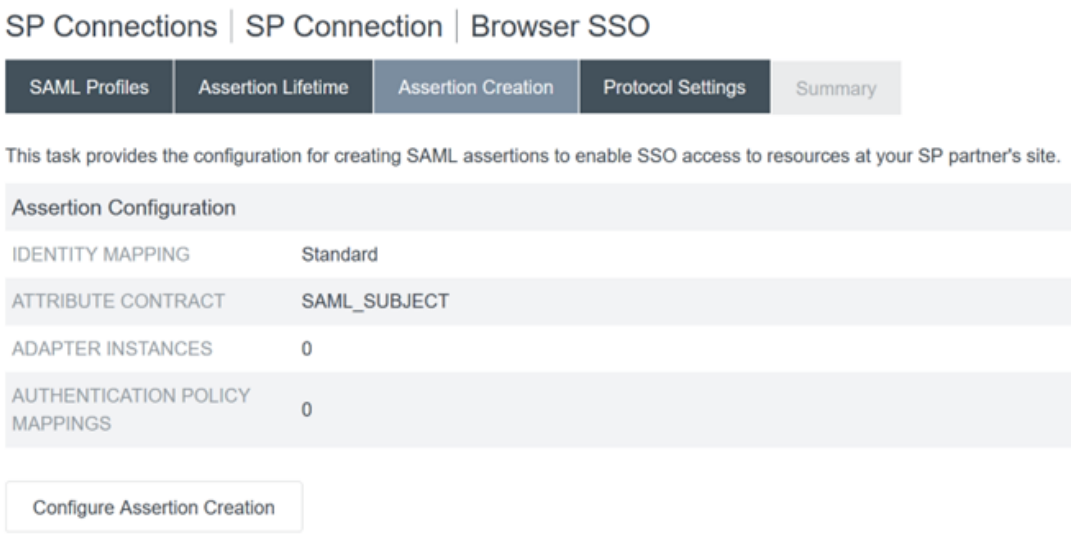


7. 使用默认的断言生命周期设置。

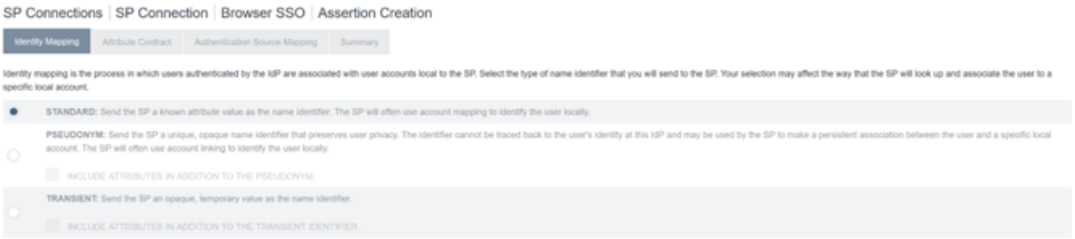
8. 配置 SAML 断言创建。

   a) 单击“配置断言创建”

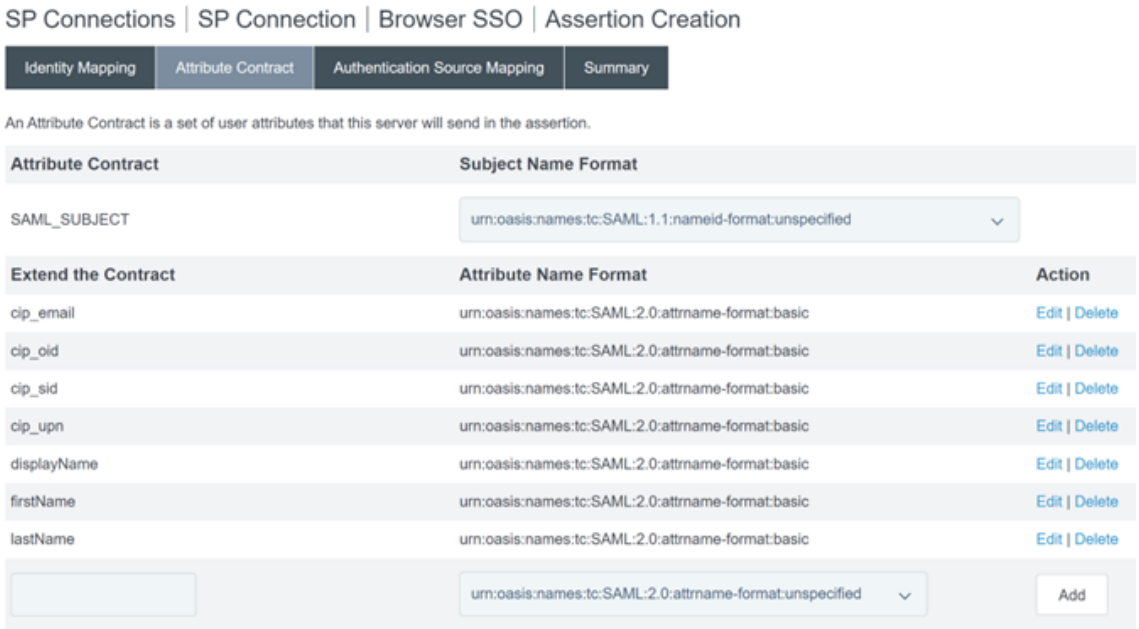
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



b) 选择“标准”。



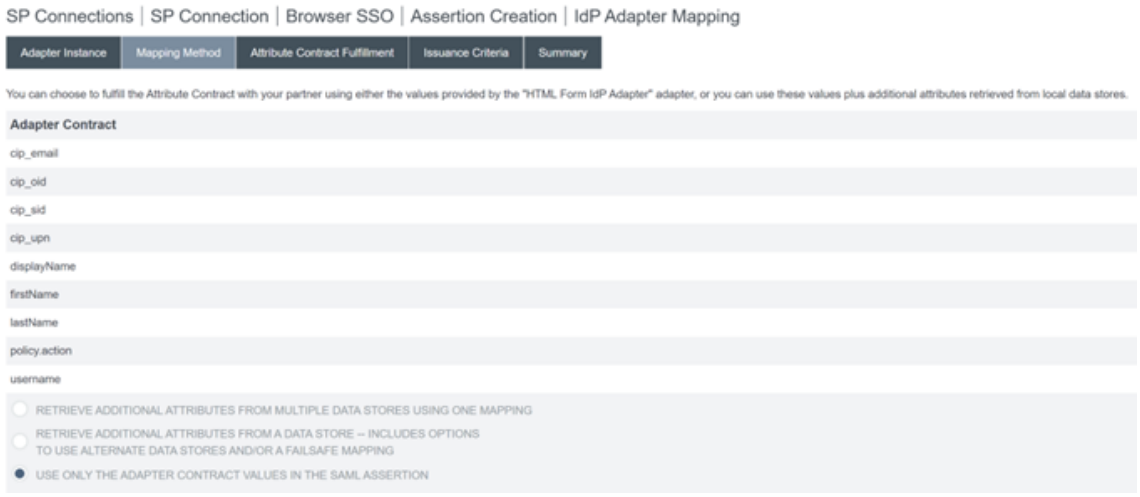
9. 配置属性合约。



10. 配置适配器实例。

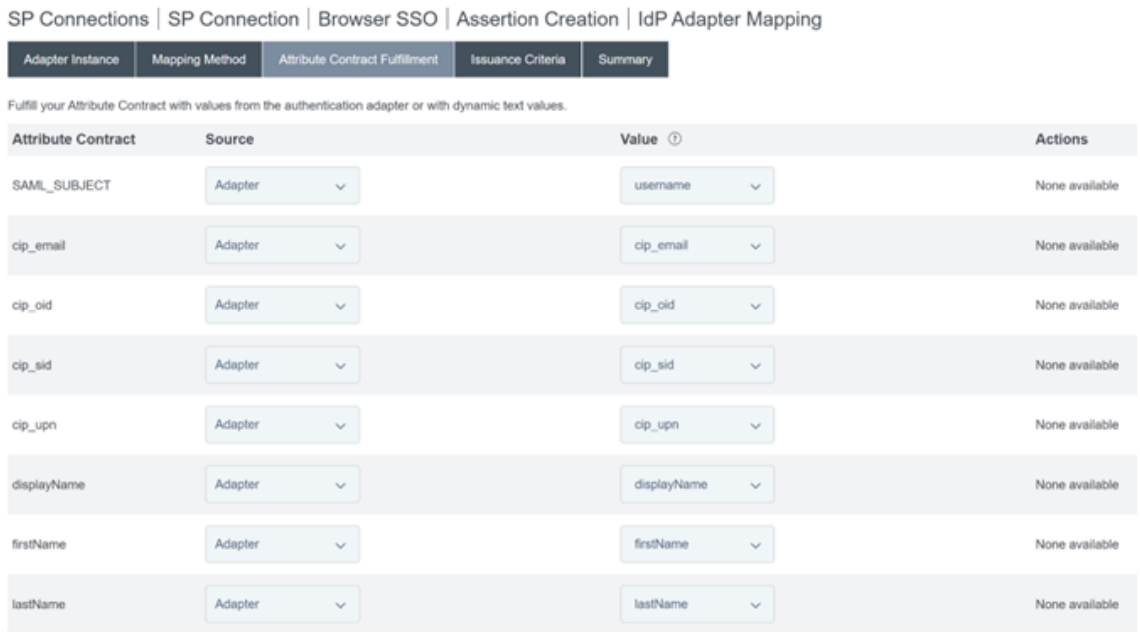
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

11. 配置映射方法。



12. 配置属性合约履行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

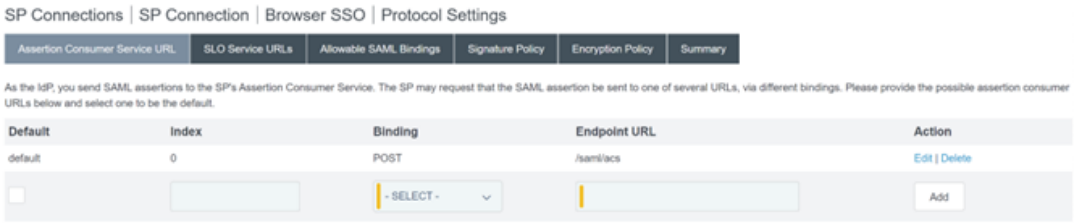


13. 将颁发标准配置为默认值，不带任何条件。

14. 完成的 **IDP** 适配器映射如下所示：

15. 配置协议设置。Citrix Cloud 所需的 SAML 路径将附加到您的 PingFederate 服务器基本 URL 中。可以通过在端点 URL 字段中输入完整路径来覆盖基本 URL，但这通常是不必要和不可取的。
    基本 URL - https://youpingfederateserver.domain.com

    a) 配置将 SAML 路径附加到 PingFederate 服务器基本 URL 的声明使用者服务 URL。EndpointURL - `/saml/acs`

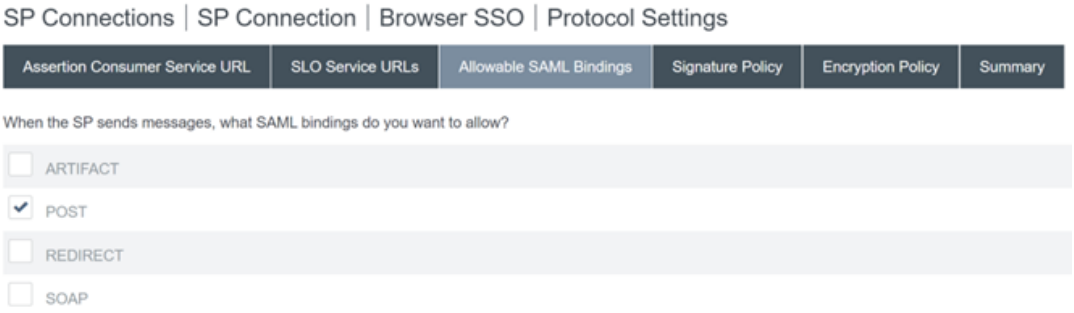


    b) 配置 **SLO** 服务 **URL**。EndpointURL - `/saml/logout/callback`

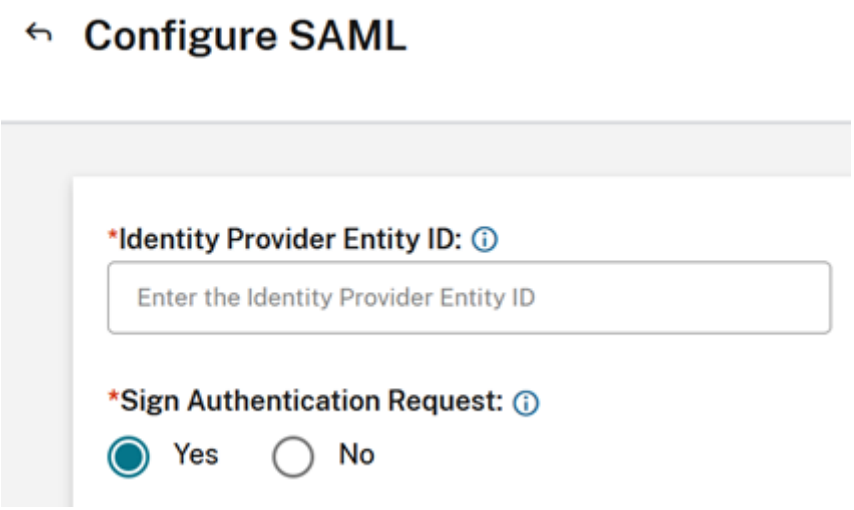
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 如果您希望在退出 Workspace 或 Citrix Cloud 时执行 SLO，Citrix Cloud SAML 连接需要将 PingFederate 注销 URL 配置为与此相匹配。未能在 SAML 连接中配置注销 URL 将导致最终用户只注销 Workspace 而不是 PingFederate。

a) 配置允许的 **SAML** 绑定。



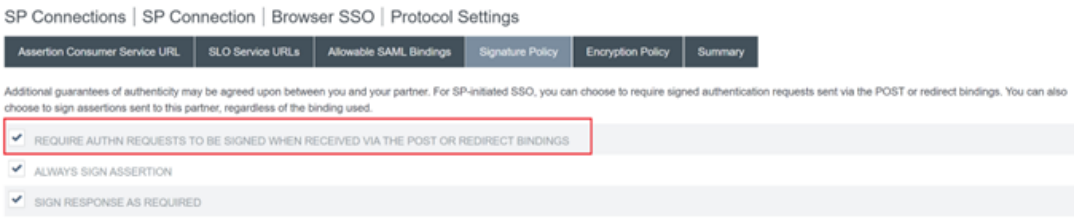
b) 配置签名策略。



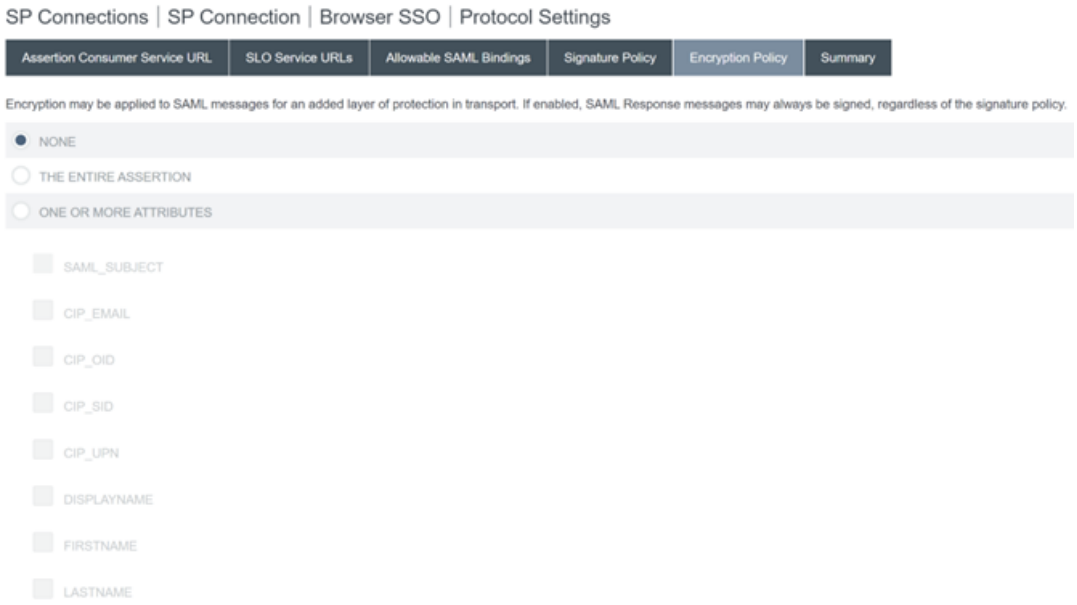
> 重要：
>
> 必须在 SAML 连接的两端统一配置 SAML 签名设置。必须将 Workspace 或 Citrix Cloud (SP) 配置为发送签名的 SSO 和 SLO 请求。

a) 必须将 PingFederate (IDP) 配置为使用 Citrix Cloud SAML 签名验证证书强制执行签名请求。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



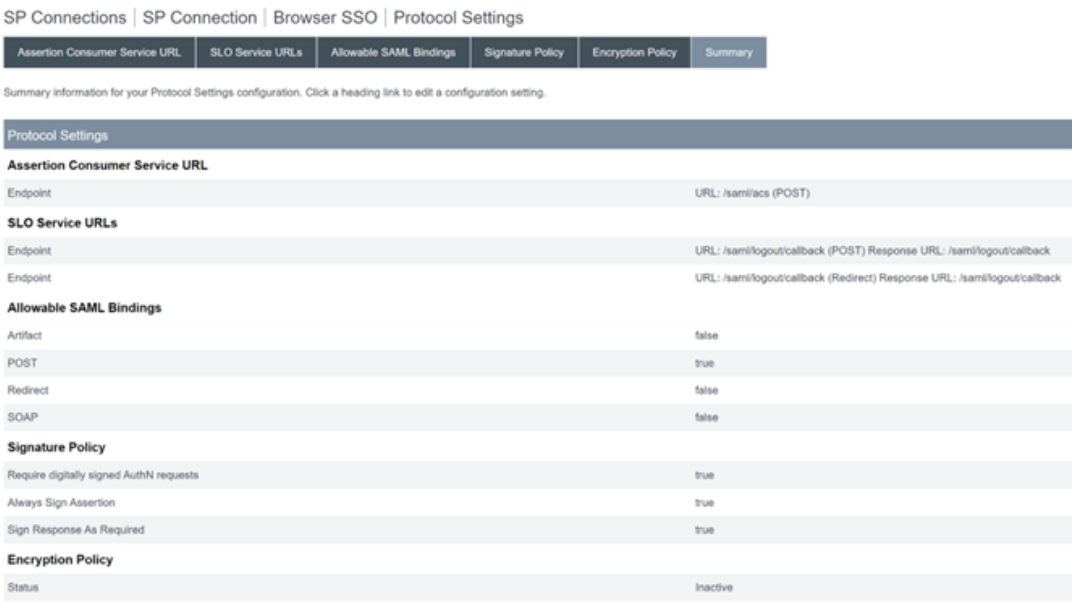
b) 配置加密策略。



> 注意：
>
> 建议在初始设置和测试期间将“加密”设置为“无”，这样您就可以调试断言中缺少 SAML 属性或不正确的任何问题。如果您需要加密断言，建议您在证明成功登录到 Workspace 或 Citrix Cloud 且所有资源均已成功枚举并可以启动后启用加密。如果您无法查看 SAML 断言的纯文本内容，则无法在启用加密的情况下调试 SAML 问题。

c) 查看“摘要”选项卡。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



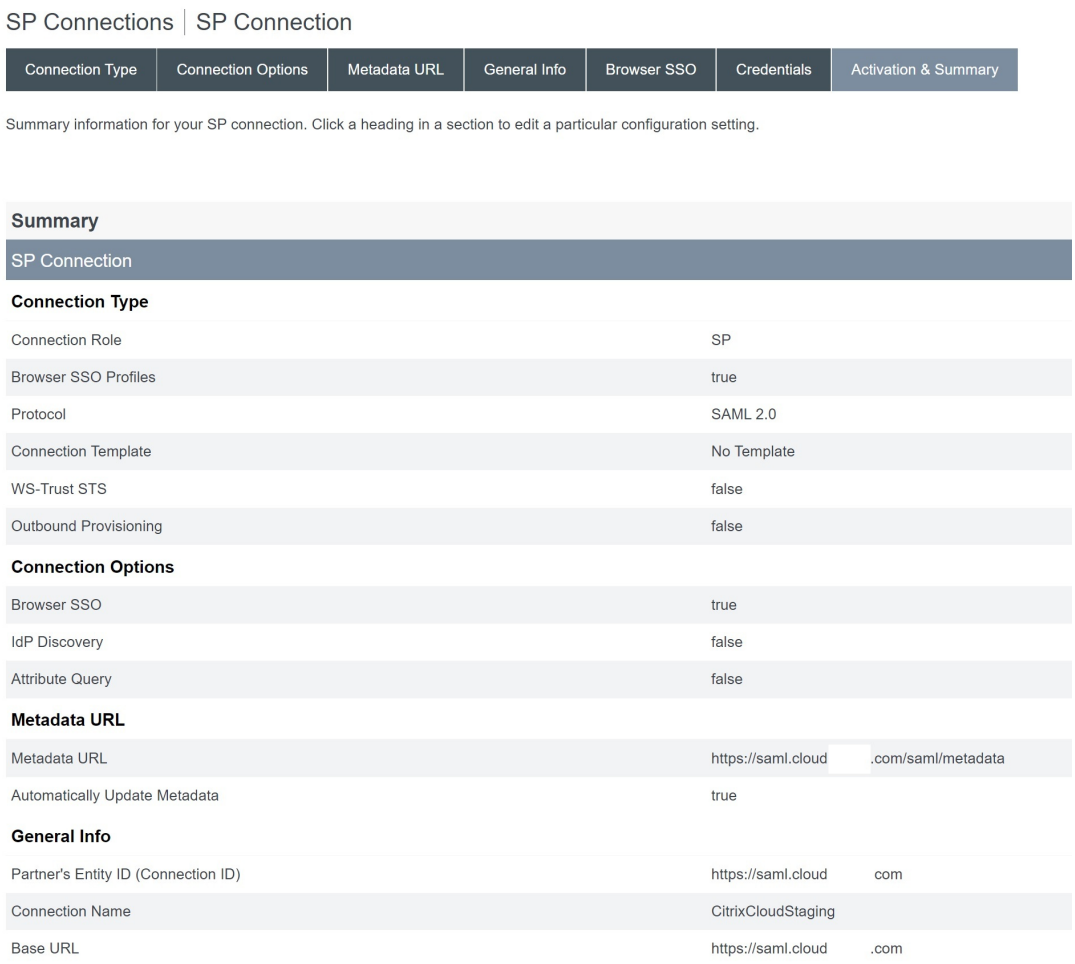
SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

d) 查看 **Citrix Cloud** 服务提供商 **(SP)** 连接。配置 **Citrix Cloud SP** 连接后，应如下所示：



SP Connections | SP Connection

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

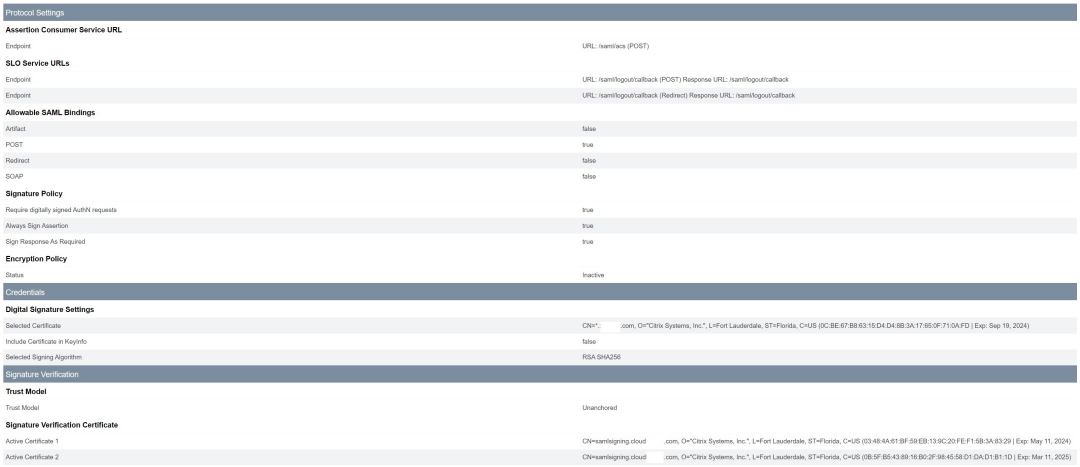
Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
Metadata URL	
Metadata URL	https://saml.cloud .com/saml/metadata
Automatically Update Metadata	true
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud com
Connection Name	CitrixCloudStaging
Base URL	https://saml.cloud .com

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_email
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_oid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_sid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	firstName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	lastName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_email	cip_email (Adapter)
cip_oid	cip_oid (Adapter)
cip_sid	cip_sid (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
firstName	firstName (Adapter)
lastName	lastName (Adapter)
Issuance Criteria	
Criterion	(None)

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive
Credentials	
Digital Signature Settings	
Selected Certificate	CN=*; .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256
Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> 有用的提示：
>
> 使用 SP 连接激活和摘要页面查看您的 SAML 应用程序并用于调试，因为它允许快速轻松地进行配置更改。SP 连接激活和摘要页面允许您通过单击任何 SAML 配置子部分的标题来导航到该部分的标题。点击任何以红色突出显示的标题来更新这些设置。

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. 完成的 **Citrix Cloud SP** 连接应如下所示出现在列表中。

17. 可以以 XML 文件的形式导出 SP 连接。Citrix 建议在使用 Citrix Cloud 和 Workspace 测试后，对 SP 连接进行备份。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更新身份提供商 **SAML** 签名证书

June 2, 2024

Author:
Mark Dear

使用签名请求和响应的 SAML 连接取决于两种不同的 SAML 签名证书。SAML 连接的每一端都有一个。

SAML 提供商签名证书

此证书由您的 SAML 提供商提供，并在配置 SAML 连接时上载到 Citrix Cloud。

SAML 签名证书需要在过期日期之前进行轮换，以便让 Citrix Cloud 管理员有时间为部署做准备。服务提供商和身份提供商都需要轮换证书，以确保一致性并防止停机。

常见问题解答

SAML 提供商证书的用途是什么

SAML 提供商证书用于验证身份验证过程中从 SAML 提供者发送到 Citrix Cloud 的 SAML 响应的签名。

在哪里可以获得最新的身份提供商 **(IdP)** 签名证书的副本

此证书由您的 SAML 提供商提供，例如 Azure AD、Okta、PingFederate 或 ADFS。Citrix 不控制此证书的轮换和更新。此证书将在您最初创建 SAML 连接时上载到 Citrix Cloud。**IDP** 签名证书的过期日期通常很长。他们可能需要每隔几年更换一次，而且更换频率要低于 **SP** 签名证书

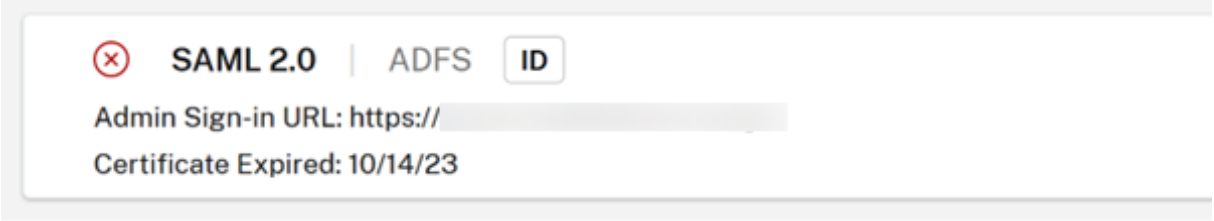
如何知道我的 **SAML** 提供商签名证书是否即将过期并影响我的 **Citrix Cloud SAML** 连接

Citrix Cloud 将在您的 SAML 提供商签名证书到期日临近 30 天前显示警告。

```
Certificate Expiring Soon: <certExpirationDate>
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

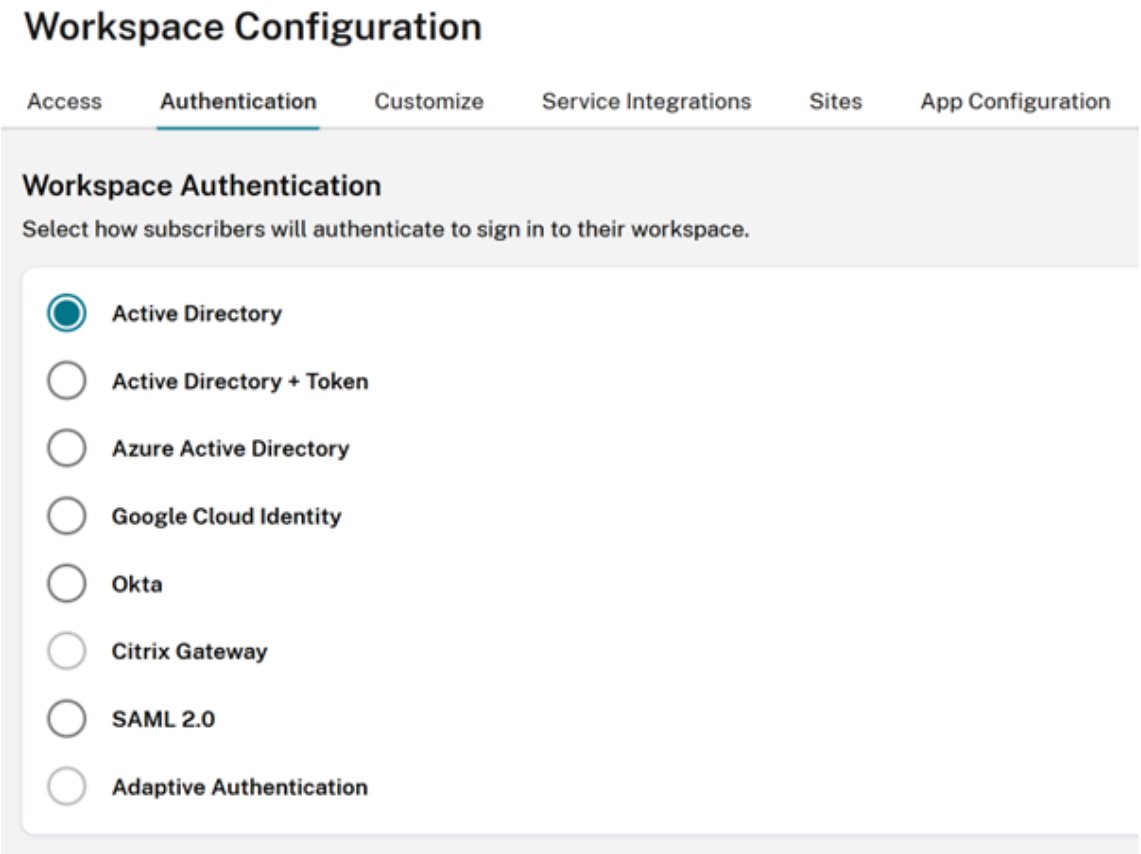
证书实际到期后，它还会显示错误，如下所示。



我是否可以在不停机的情况下在使用 **SAML** 连接的同时更新 **SAML** 提供商证书

否。必须在预定的维护时段内执行 SAML 断开连接并重新连接。
更新身份提供商 (IdP) 签名证书

1. 在 **Workspace** 配置中选择备用 IdP，在执行 SAML 断开/重新连接操作（例如 Active Directory）时选择身份验证。



2. 将您的现有 GO URL（例如用于 SAML 登录的 `https://citrix.cloud.com/go/<yourgourl>`）备份到 Citrix Cloud。
3. 备份您的现有 SAML 端点。这些可以从 Citrix Cloud 控制台复制。从现有 SAML 连接中备份以下 SAML 端点。
    - 身份提供商实体 ID

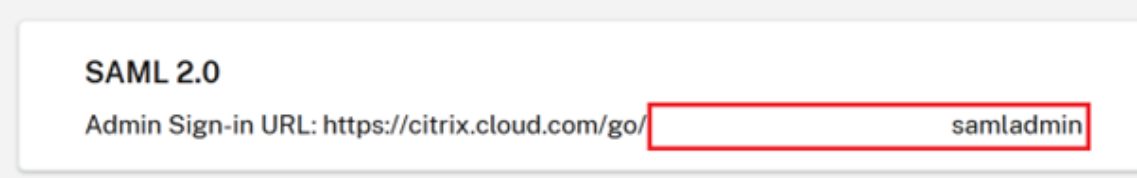
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

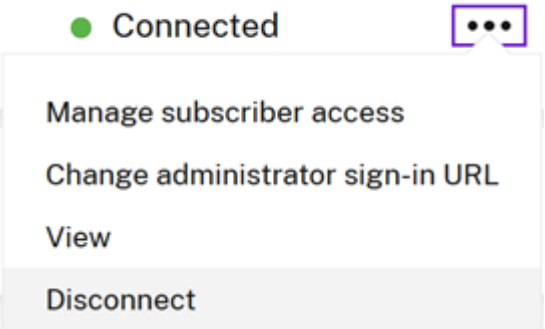
- 身份提供商 SSO 服务 URL
- 身份提供商注销 URL

备份 EntityID、SSO URL 和注销 URL。

> 重要：
>
> 在执行断开连接之前，请确保您有现有和替换的 IDP 签名证书的副本。这样，如果新的 SAML 提供商证书无效并导致任何登录问题，您就可以回滚到旧证书。在执行断开连接之前，您将无法从 Citrix Cloud 用户界面获取旧证书的副本。您需要从您的 SAML 应用程序中获取它。

1. 在身份识别和访问管理中断开 SAML，导航到身份验证，选择 SAML 连接，单击椭圆并选择断开连接
2. 在“身份识别和访问管理”中重新连接 SAML，然后单击“身份验证”





3. 接受所有默认 SAML 连接设置。
4. 重新输入您之前备份的所有 SAML 应用程序端点，或者在 SAML 提供商用户界面中再次为您的 SAML 应用程序获取这些端点。

- 身份提供商实体 ID
- 身份提供商 SSO 服务 URL
- 身份提供商注销 URL

> 重要：
>
> 如果您使用的是 Scoped EntityID 功能，则在执行 SAML 断开/重新连接后，还需要使用新的作用域 ID 更新 SAML 应用程序。有关 Scoped EntityID 功能的更多信息，请参阅在 Citrix Cloud 中使用作用域实体 ID 配置 SAML 应用程序。从 Citrix Cloud SAML UI 复制新生成的作用域 ID，并使用替换作用域 ID 更新您的 SAML 应用程序实体 ID。
> EntityID 应更新为 `https://saml.cloud.com/<new scope ID after reconnect>`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

更新服务提供商 **SAML** 签名证书

June 2, 2024

Author:
Mark Dear

使用签名请求和响应的 SAML 连接取决于两种不同的 SAML 签名证书。SAML 连接的每一端都有一个。

服务提供商签名证书

此证书由 Citrix 定期提供并上载到您的 SAML 应用程序中或通过 Citrix Cloud SAML 元数据获取。

SAML 签名证书需要在过期日期之前进行轮换，以便让 Citrix Cloud 管理员有时间为部署做准备。服务提供商和身份提供商都要求轮换证书，以确保一致性并防止任何停机。

如果选定的 SAML 提供商不支持 SP SAML 签名证书的自动轮换，则必须在 SAML 提供商内手动轮换 SAML 签名证书以替换即将到期的证书。

> 重要：
>
> 此 SAML eDoc 部分中的所有现有指南都包含有关如何在 SAML 连接两端配置签名的详细信息。Citrix 只推荐签名的 SAML 配置，因为这些配置更安全，而且某些 SAML 提供商要求这些配置才能成功注销 (SLO)。

常见问题解答

什么是 **SAML** 签名

SAML 签名证书是 X.509 证书，用于验证服务提供商 (SP) 和 SAML 提供商 (IdP) 之间发送的数据。您的 SAML 提供商 (IdP) 使用 Citrix Cloud SAML 签名证书来验证 Citrix Cloud 在其 SAML 身份验证请求中发送的签名。Citrix Cloud 使用 SAML 提供商签名证书来验证 SAML 响应来自可信且互连的 IdP。

什么是 **SAML** 签名请求的执行

仅仅因为 Citrix Cloud 配置为发送签名请求，这并不能保证 SAML 提供商将强制使用签名并拒绝任何未签名的传入 SAML 请求。大多数 SAML 提供商都可以选择强制执行签名请求，这意味着如果收到未签名的登录 SAML 提供商的请求，则登录将失败。检查 IdP 配置的状态是 SAML 提供商管理员的责任。Citrix 支持部门无法控制也无法查看是否在您的 SAML 应用程序中强制执行签名请求。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 多久轮换一次其服务提供商 **SAML** 签名证书

为了允许有效的服务提供商签名证书和新颁发的签名证书之间有足够的重叠之处，Citrix 大约每 11 个月轮换一次服务提供商签名证书。这是为了确保在现有证书到期前 30 天向 Citrix Cloud 客户提供有效证书。

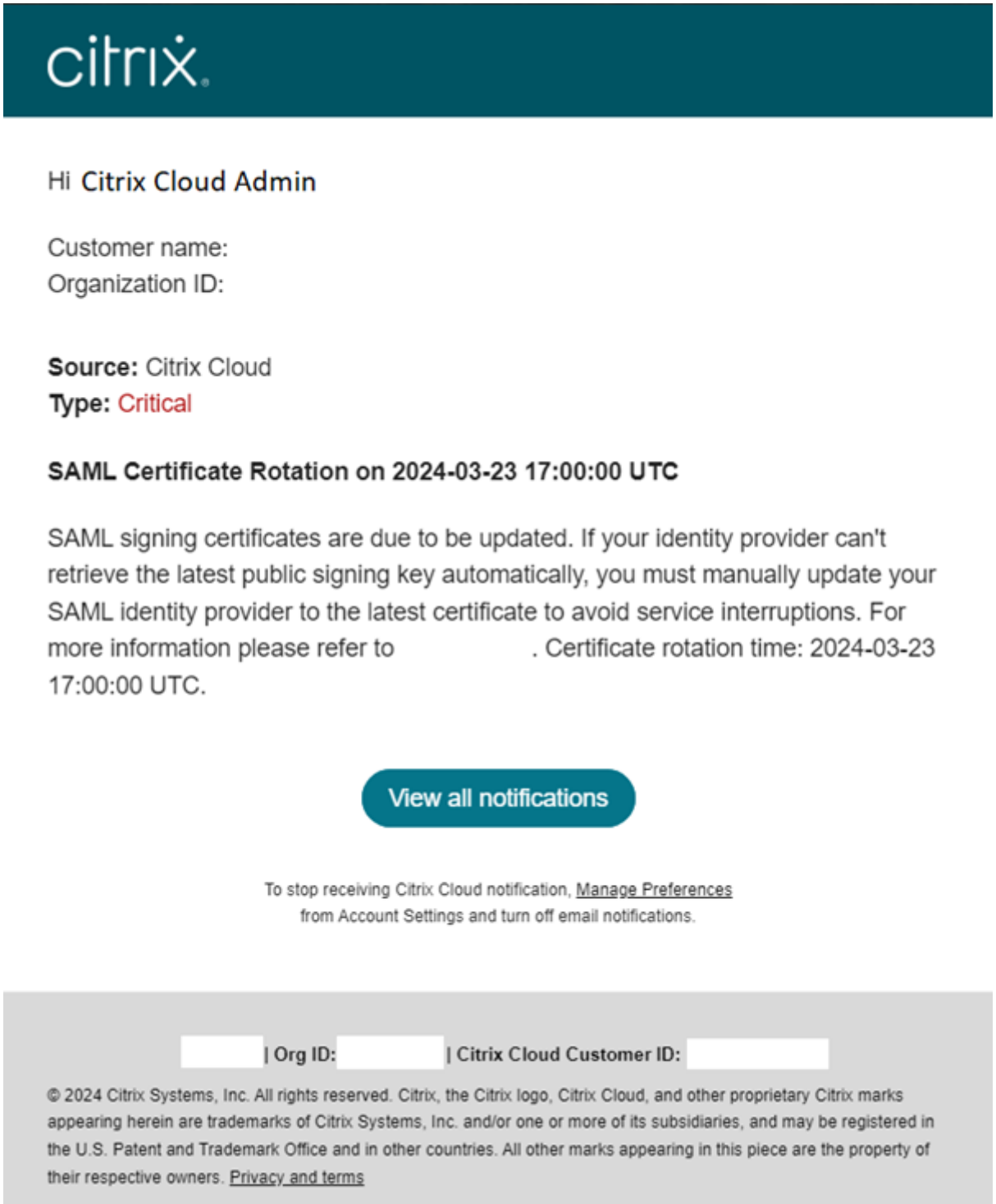
什么是服务提供商 **SAML** 签名证书广告阶段

在广告阶段，当前和替换的 SAML 签名证书将出现在 Citrix Cloud 元数据中。在轮换日期和时间之前，只有有效的证书可以用于 SAML 请求验证。

为什么我通过电子邮件和 **Citrix Cloud** 管理控制台收到通知，表明当前 **Citrix Cloud SAML** 签名证书即将到期，必须更换

SAML 提供商 (IdP) 需要有效且有效的证书来验证来自 Workspace 和 Citrix Cloud 管理员控制台等服务提供商的传入 SAML 请求的签名。将联系使用 SAML for Workspace 或 Citrix Cloud 管理控制台登录的 Citrix Cloud 客户，告知他们即将轮换 SAML 签名证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



citrix.

Hi **Citrix Cloud Admin**

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

SAML Certificate Rotation on 2024-03-23 17:00:00 UTC

SAML signing certificates are due to be updated. If your identity provider can't retrieve the latest public signing key automatically, you must manually update your SAML identity provider to the latest certificate to avoid service interruptions. For more information please refer to . Certificate rotation time: 2024-03-23 17:00:00 UTC.

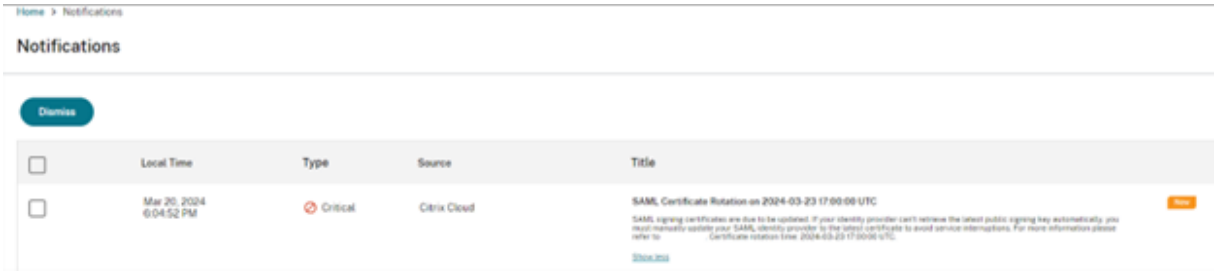
View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

| Org ID: | Citrix Cloud Customer ID:

© 2024 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



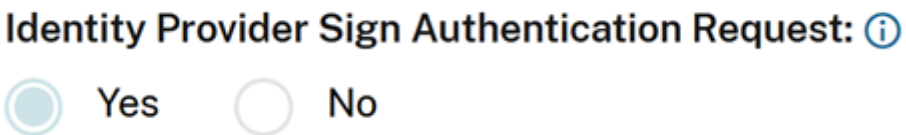
如何知道我的 **Citrix Cloud** 客户是否受到 **Citrix Cloud SAML** 签名证书轮换的影响

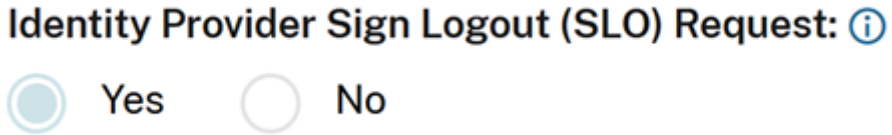
这将影响使用以下 SAML 配置的 Citrix Cloud 客户。

- 您在 Citrix Cloud 中的 SAML 连接配置为使用签名身份验证请求 **=** 是
- 您已将 Azure Active Directory、ADFS 或 Okta 等 SAML 提供商配置为拒绝未签名的 SAML 请求（强制执行签名请求）。
- 您在 Citrix Cloud SAML 连接和 SAML 提供商中配置了单点注销 (SLO)。您的 SAML 提供商可能要求签署 SLO 请求，例如 Okta 和 PingFederate 的请求。

如何检查我的 **Citrix Cloud SAML** 连接的签名配置

导航到身份识别和访问管理 > **SAML 2.0** > 查看，检查您是否在 Citrix Cloud SAML 连接中启用了签名身份验证请求。对于登录 (SSO) 和注销 (SLO)，Citrix Cloud 中所有新的 SAML 连接都将默认为身份提供商签名身份验证/注销请求 **=** 是。





如何检查我的 **SAML** 应用程序中是否配置了强制签名

这因您使用的 SAML 提供商而异。有些人甚至可能不提供此选项。AzureAD、ADFS、Okta 和 PingFederate 都支持强制签名。SAML 管理员必须了解您的 SAML 提供商的功能及其当前配置。Citrix 支持人员无法控制或查看这一点。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

在哪里可以获得最新的服务提供商 **(SP)** 签名证书的副本

该证书由 Citrix 通过 Citrix Cloud SAML 元数据提供，并在 SP 签名证书轮换的广告阶段定期更新。这种情况每个日历年至少发生一次。

美国、欧盟和亚太南部：https://saml.cloud.com/saml/metadata

JP：https://saml.citrixcloud.jp/saml/

GOV：https://saml.cloud.us/saml/metadata

如果我的 **SAML** 应用程序支持多个验证证书，何时可以安全地删除旧的 **Citrix Cloud SAML** 签名证书

只有在电子邮件和 Citrix Cloud 管理控制台通知中给出的证书轮换日期和时间之后才删除旧的 Citrix Cloud 签名证书。

使用元数据交换使用最新的 **Citrix Cloud SP SAML** 签名证书自动更新 **SAML** 提供商

使用 SAML 元数据交换，SAML 提供商通过监视元数据 URL 来自动使用 Citrix Cloud SAML 元数据，例如 https://saml.cloud.com/saml/metadata。如果您的 SAML 提供商支持 SAML 元数据交换，则 SP 签名证书可能已经自动更新。
确认您的 SAML 提供商支持元数据交换。之后，您可以验证更新是否在当前 SAML 签名证书到期之前发生。

> 重要
>
> 每个第三方 SAML 提供商支持的 SAML 功能存在很大差异。Citrix Cloud 管理员有责任了解和了解您正在使用的 SAML 提供商的功能和要求。这是确保 Citrix Cloud SAML 连接配置 (SP) 和 SAML 提供商 (IdP) 配置匹配所必需的。请参阅您的 SAML 提供商的文档，以确定其是否支持签名验证以及是否需要对 SAML 请求和响应进行签名。

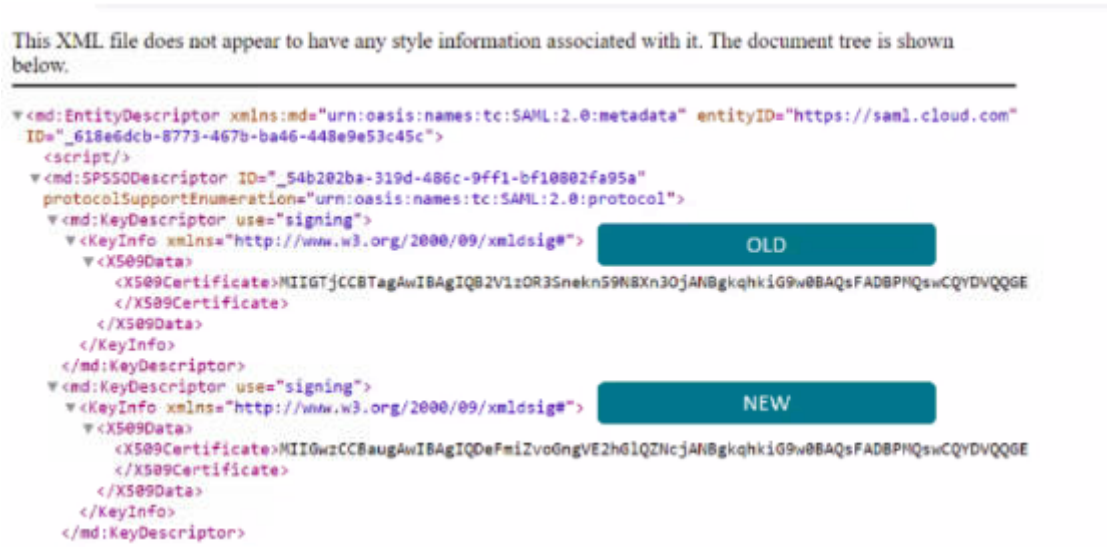
使用最新的 **Citrix Cloud SP SAML** 签名证书手动更新 **SAML** 提供商

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要
>
> 每次从 Citrix Cloud 发布新证书时都必须轮换 SP 证书，否则 SAML 登录将受到影响，您将面临停机。

1. 在身份识别和访问管理中查看当前 SAML 连接，从 Citrix Cloud 获取最新的 SAML 元数据，单击“身份验证”，选择“**SAML** 连接”，然后单击“查看”。
   下图是该文件在 Citrix Cloud 地区（例如美国、欧盟和亚太南部）的外观示例：

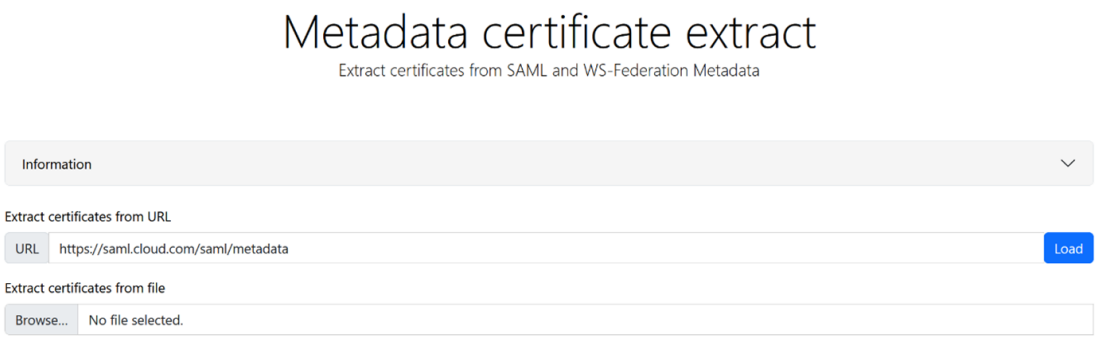
   https://saml.cloud.com/saml/metadata



   在此元数据 XML 文件示例中，有两个 x509 Citrix Cloud SAML 签名证书。

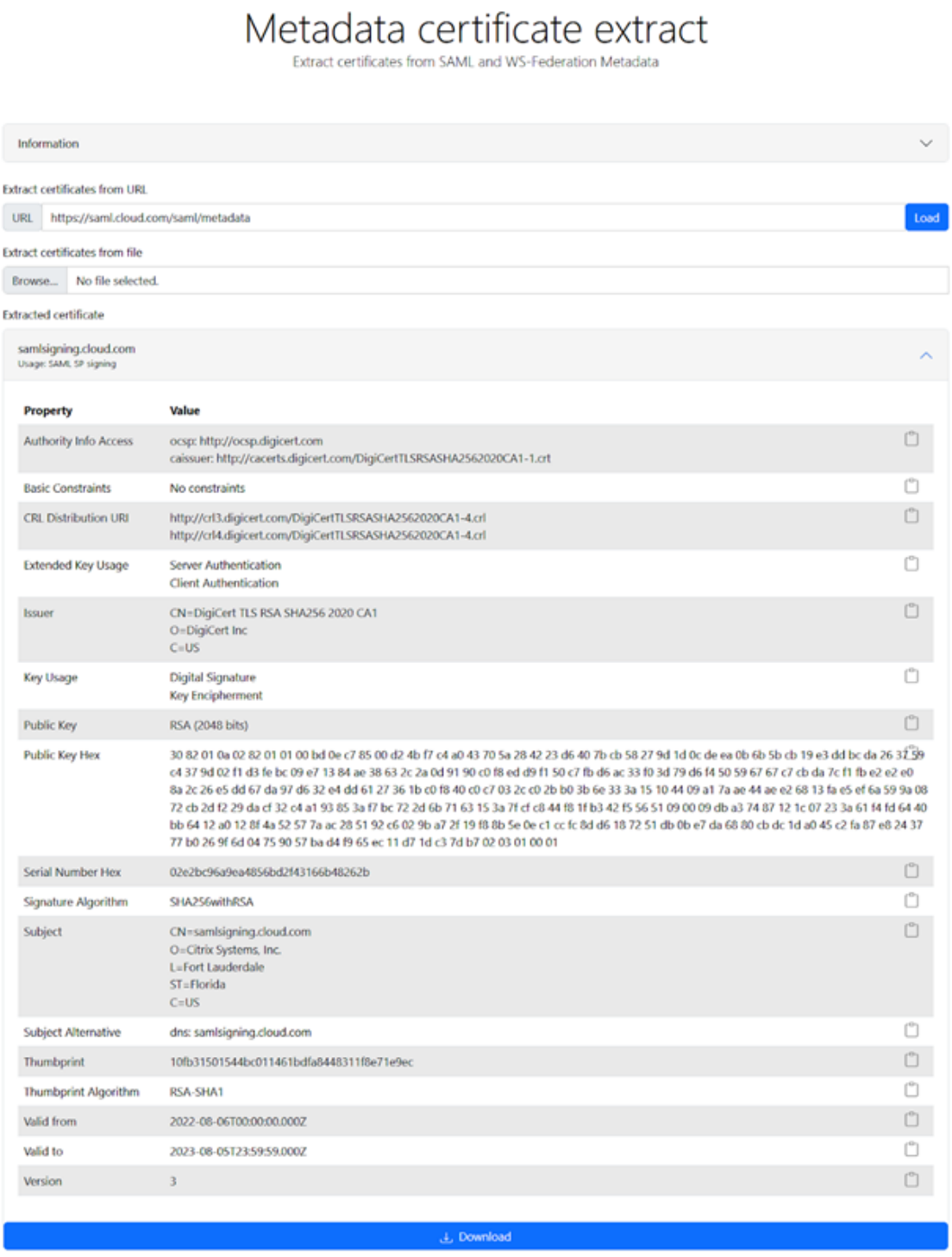
2. 通过将 XML 文件上载到第三方工具或提供元数据 URL，可以从元数据中提取 x509 证书。
3. 导航到 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract
4. 输入与您的 Citrix Cloud 客户区域相对应的 SAML 元数据 URL：

   - 美国、欧盟和亚太南部：https://saml.cloud.com/saml/metadata
   - JP：https://saml.citrixcloud.jp/saml/metadata
   - GOV：https://saml.cloud.us/saml/metadata



   从 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract 下载 SAML 签名证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



5. 将新提取的 Citrix Cloud SP SAML 证书上载到您的 SAML 提供商。对于每个 SAML 提供商，此过程将有所不同。使用特定的 SAML 提供商文档，验证正确的 SP 签名证书轮换程序。

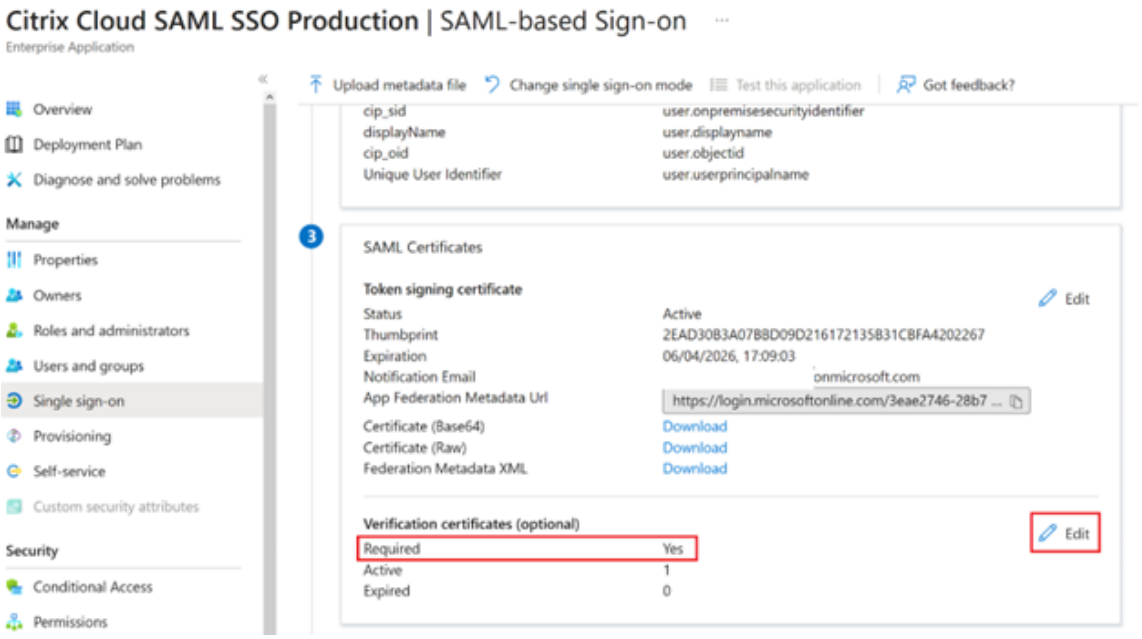
   视您的 SAML 提供商而定，可能需要用新的 SAML 签名证书替换现有的 SAML 签名证书。在某些情况下，SAML 提供商可能同时支持多个 SP 签名证书，因此仅上载新的 SP 签名证书就足够了。建议您在旧证书过期后将其删除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

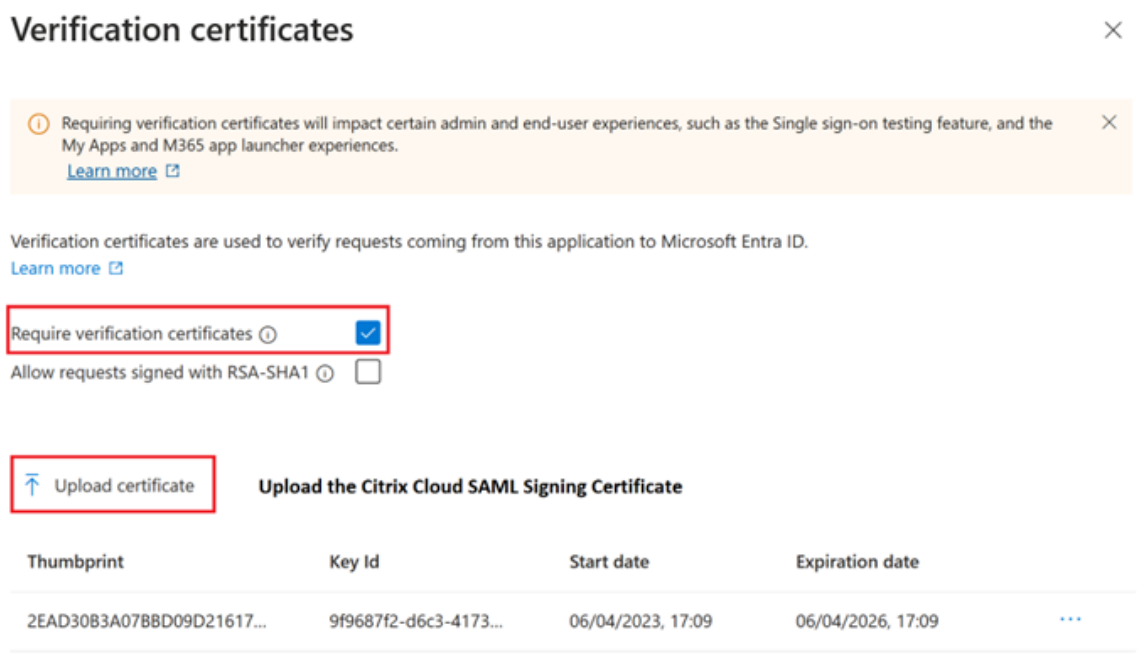
将替换的 **Citrix Cloud SAML** 签名证书上载到您的 **Azure Active Directory SAML** 应用程序

在配置 Azure Active Directory SAML 应用程序之前，请参阅 SAML 请求签名验证以了解更多信息。

1. 导航到 **Azure Active Directory**，选择“企业应用程序”，然后单击“您的 SAML 应用程序”。
2. 在 SAML 应用程序中找到 SAML 证书部分。

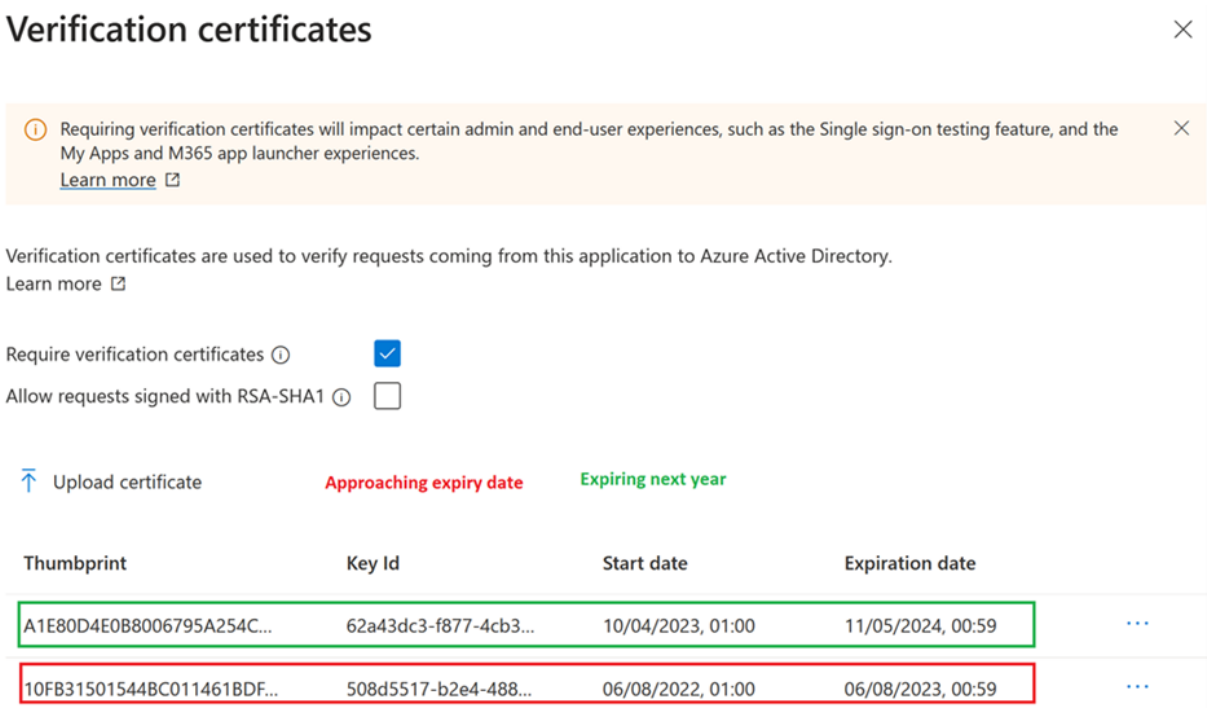


3. 选择上载证书，然后上载从 SAML 元数据中获得的替换 Citrix Cloud SAML 签名证书。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> Azure Active Directory SAML 应用程序可以配置多个签名验证证书，因此可以在当前证书到期之前很久就上载替换证书。以下屏幕截图显示了两个有效的证书。其中一份证书将在不久的将来过期。只要上载的证书中至少有一个有效且尚未过期，将继续通过 SAML 登录 Citrix Workspace 和 Citrix Cloud，并且不会出现中断的情况。



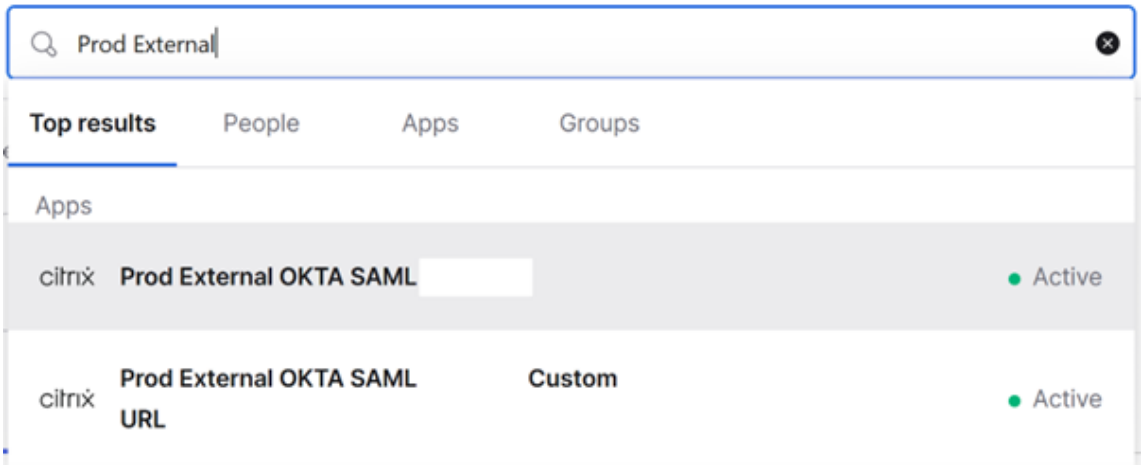
> 重要：
>
> 在电子邮件和 Citrix Cloud 管理控制台通知中提供的 SAML 轮换日期和时间结束之前，不要删除现有验证证书。新的 Citrix Cloud 证书仅在这两份通知中给出的日期和时间生效。

将替换的 **Citrix Cloud SAML** 签名证书上载到您的 **Okta SAML** 应用程序

Okta 不支持同时支持多个 SP SAML 签名证书。您别无选择，只能用新证书覆盖您目前正在使用的现有 Citrix Cloud SP 签名证书。建议您在定期维护时段内执行此操作。

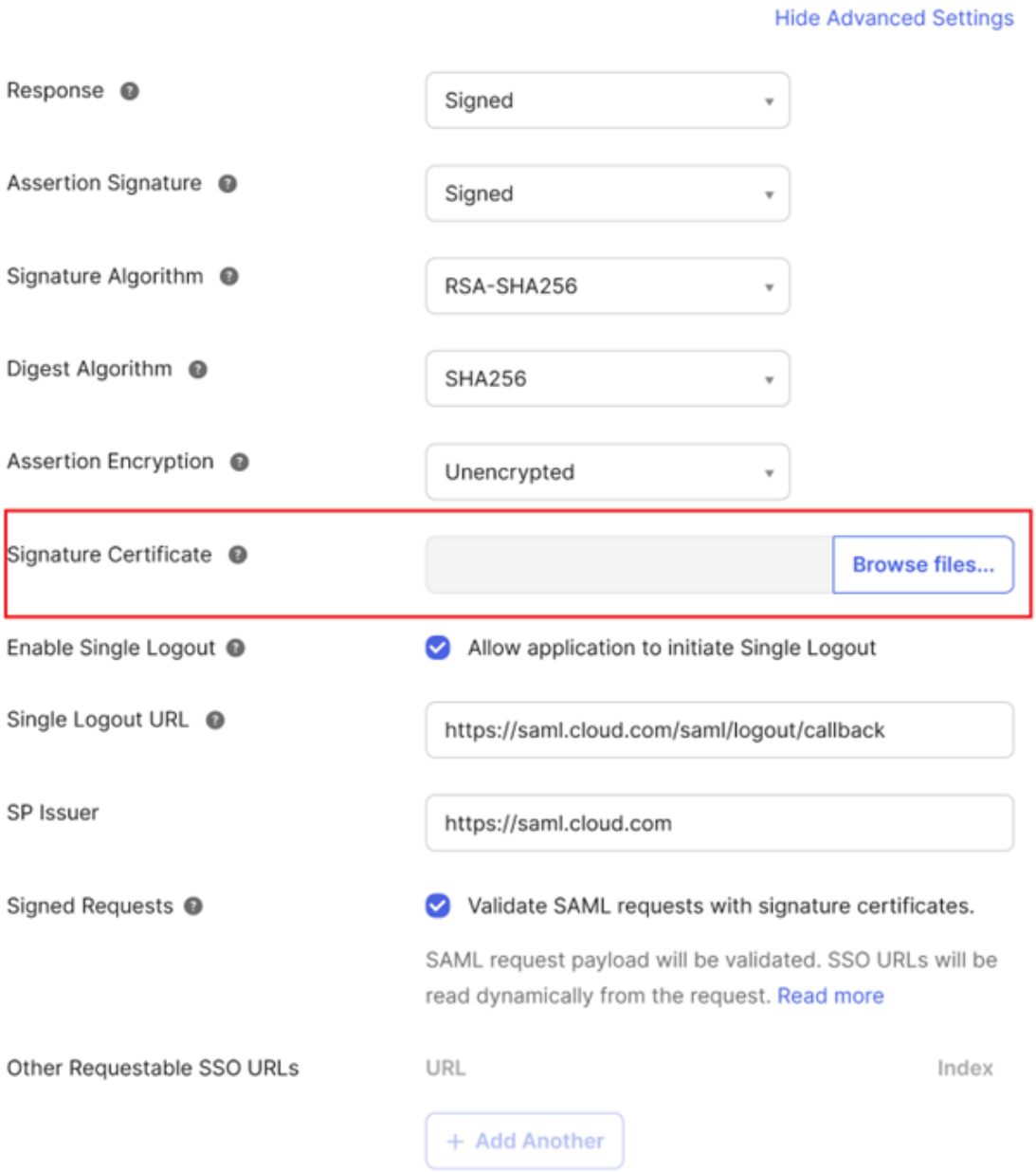
1. 导航到“应用程序”，选择“应用程序”，然后搜索您的 Okta SAML 应用程序

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



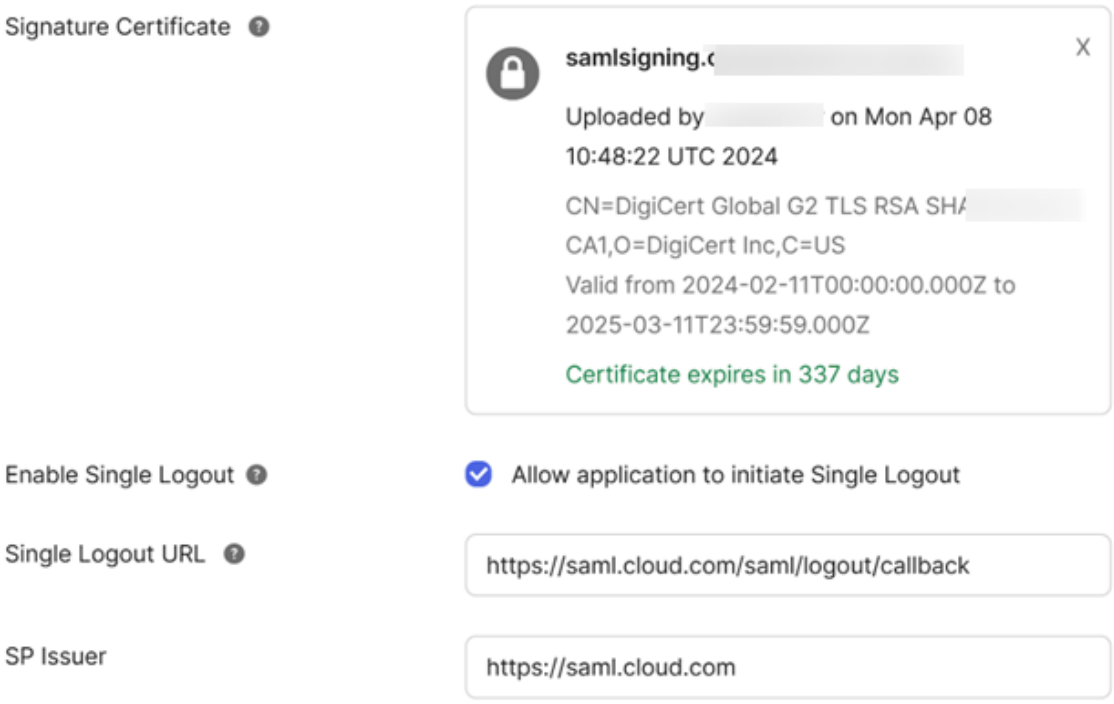
2. 在“常规”中，导航到“**SAML** 设置”，单击“编辑”，选择“配置 **SAML**”，选择“显示高级设置”，然后单击“签名证书”以上载替代证书。Okta 不在上载用户界面中显示当前 Citrix Cloud SAML 签名证书。它只会在上载后显示替换证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 选择签名证书，单击“浏览文件”，然后上载从 Citrix Cloud SAML 元数据中获得的替换 Citrix Cloud SAML 签名证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



> 重要
>
> 在电子邮件和 Citrix Cloud 管理控制台通知中提供的 SAML 轮换日期和时间之前，不要覆盖现有验证证书。新的 Citrix Cloud 证书仅在这两份通知中给出的日期和时间生效。

将 **ADFS** 配置为区身份验证的 **SAML** 提供商

July 1, 2024

Author:
Mark Dear

本文介绍如何配置 Citrix Cloud 使用 SAML 登录 Citrix Workspace 或 Citrix Cloud 所需的信赖方信任。

完成本文中的步骤后，您可以在 ADFS 服务器和 Citrix Cloud 之间配置 SAML 连接，如 Connect SAML 作为 Citrix Cloud 中的身份提供商中所述。有关为 SAML 连接输入正确 ADFS 值的指导，请参阅本文中的 Citrix Cloud 中的 SAML 配置。

必备条件

本文中的说明假设您的环境中部署了 Citrix FAS 的 ADFS 服务器。在会话启动期间，Citrix FAS 必须提供 VDA 的单点登录。

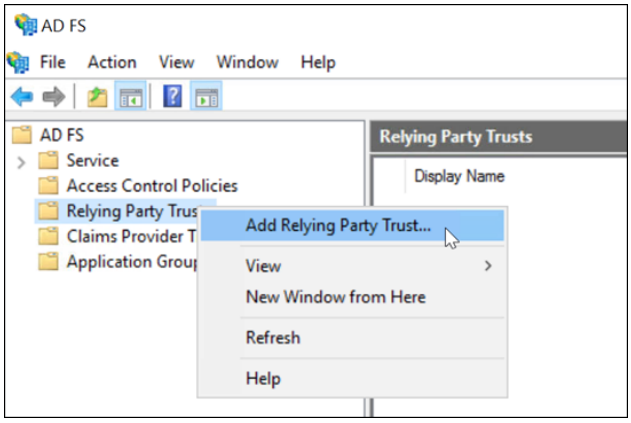
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关更多信息，请参阅以下文章：

- Citrix FAS 文档：
  - 安装和配置
  - ADFS 部署
- Citrix Tech Zone：参考体系结构：联合身份验证服务

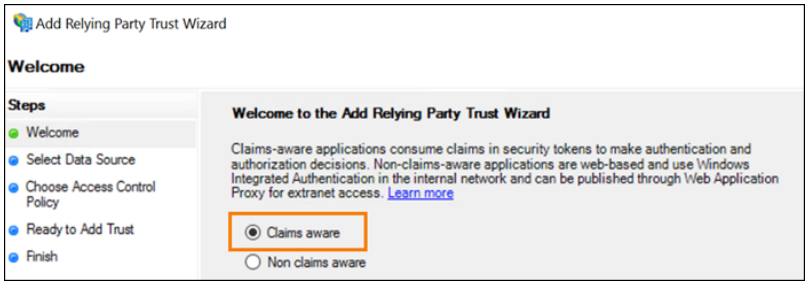
为 **Citrix Cloud** 配置信赖方信任

1. 在 AD FS 管理控制台中，展开左侧窗格中的 **AD FS** 节点。
2. 右键单击“信赖方信任”，然后选择“添加信赖方信任”。

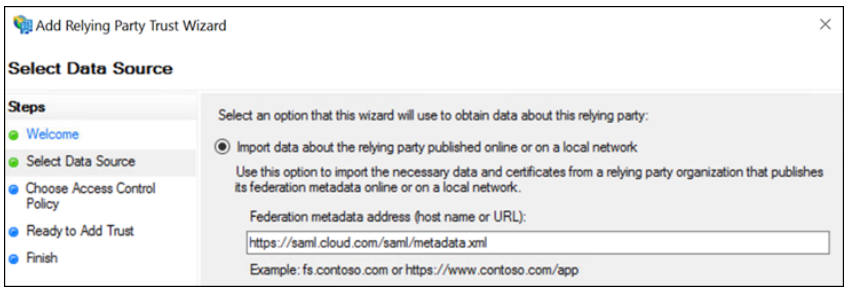


将出现“添加信赖方信任”向导。

3. 选择“声明感知”，然后选择“下一步”。

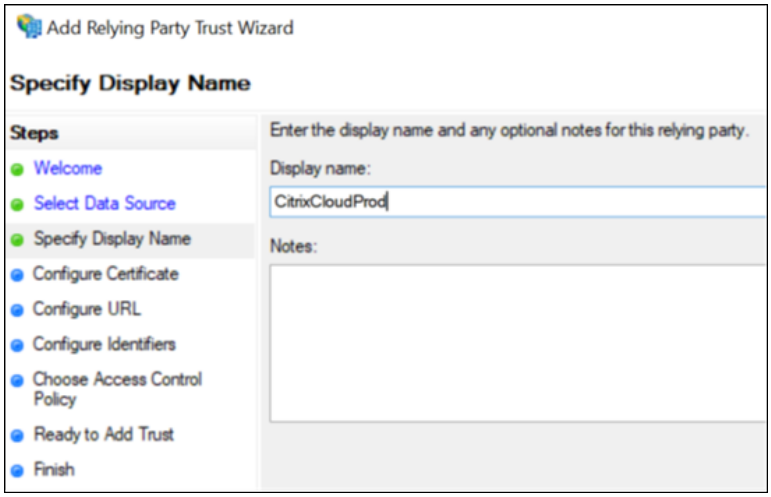


4. 在联邦元数据地址中，输入 `https://saml.cloud.com/saml/metadata.xml`。选择下一步。

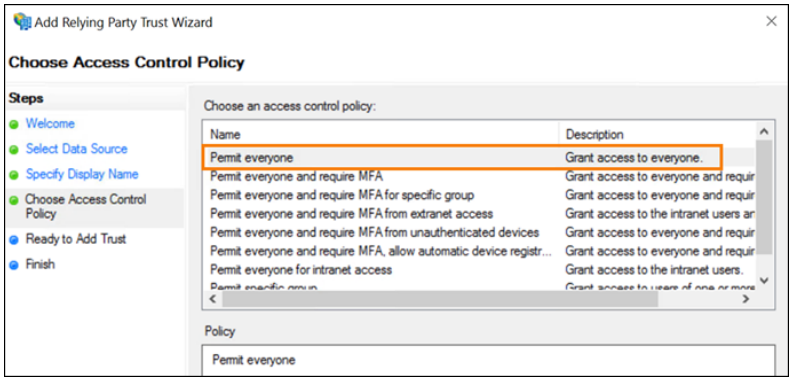


© 1999–2024 Cloud Software Group, Inc. All rights reserved.

5. 对于显示名称，请输入 `CitrixCloudProd`。选择下一步。

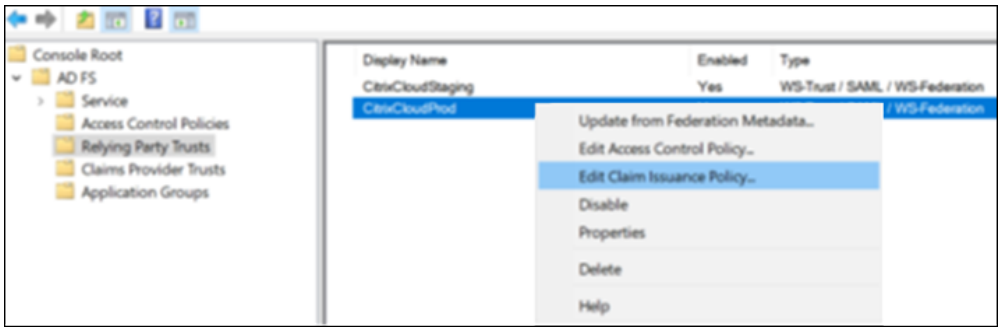


6. 对于访问控制策略，选择“允许所有人”。选择下一步。



7. 在“准备添加信任”屏幕上，选择“下一步”。

8. 在“完成”屏幕上，选择“为此应用程序配置声明颁发策略”。选择下一步。



9. 右键单击新创建的中继方信任，然后选择“编辑声明颁发策略”。

10. 单击“添加规则”，然后选择“将 **LDAP** 属性作为声明发送”。选择下一步。

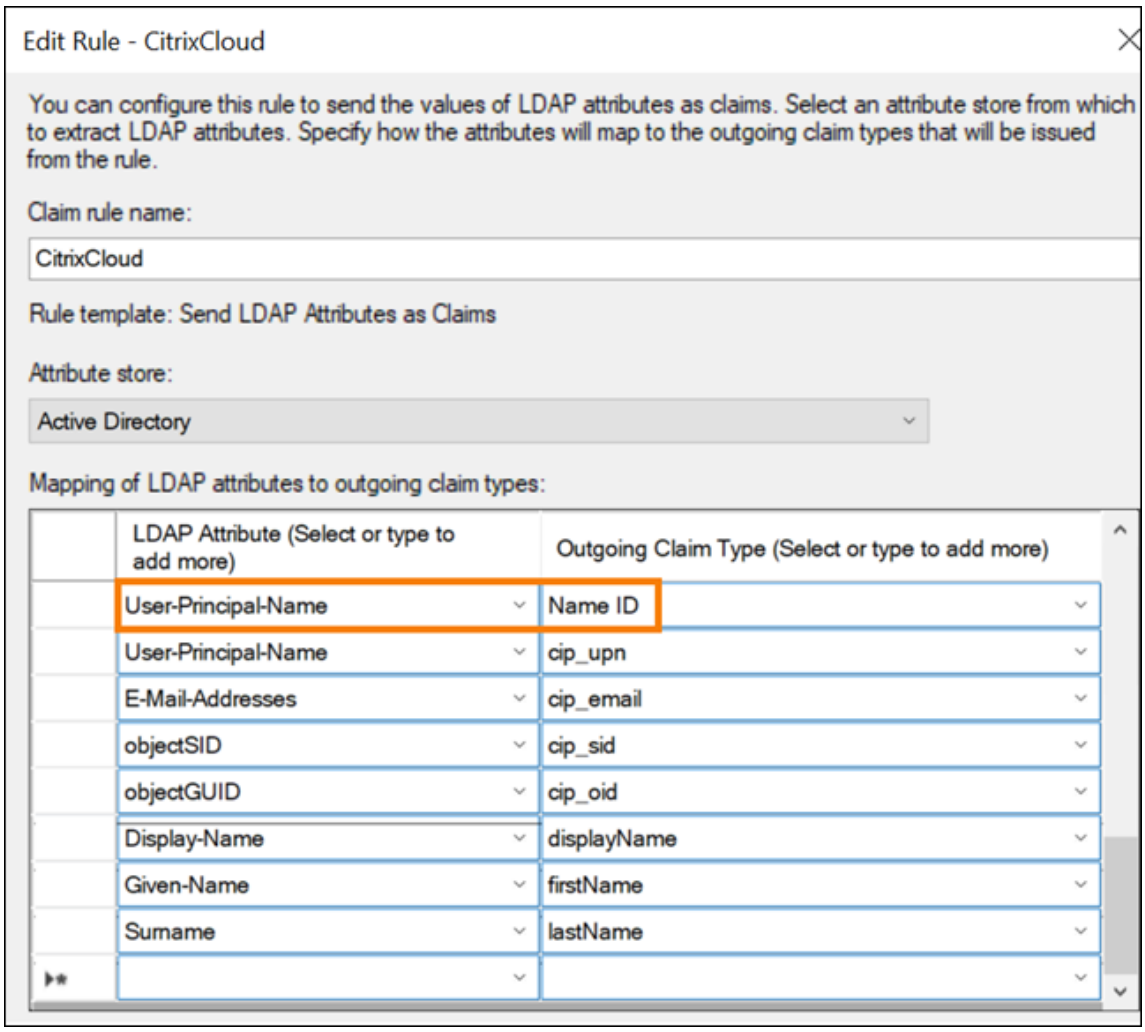
11. 在声明规则名称中，输入 `CitrixCloud`。

12. 在属性存储中，选择 **Active Directory**。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

13. 在“将 **LDAP** 属性映射到传出声明类型”下，添加以下 LDAP 属性，如下所示：

LDAP 属性	发出的声明类型
用户主要名称	名称 ID
用户主要名称	cip_upn
E-Mail-Addresses	cip_email
objectSID	cip_sid
objectGUID	cip_oid
Display-Name	displayName
Given-Name	firstName
姓氏	lastName



14. 选择完成。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 **PowerShell** 修改 **Citrix Cloud** 信赖方信任

如果您已使用默认的“开箱即用”配置您的 ADFS 服务器，则可以通过本节中的步骤对其进行更新，使其符合 Citrix 推荐的配置。如果 `nameidentifier` 属性未包含在声明规则集中，或者不是声明规则集中的第一个 SAML 属性，则从 Citrix Cloud 或 Citrix Workspace 的 SAML 单一注销会失败，则需要执行此任务。

> 注意：
>
> 如果您使用本文中为 Citrix Cloud 配置信赖方信任中的步骤创建了声明规则集，则无需执行此任务。

要完成此任务，请使用 PowerShell 将现有规则集替换为新的声明规则集。ADFS 管理控制台不支持此类操作。

1. 在 ADFS 服务器上，找到 PowerShell ISE。右键单击并选择“以管理员身份运行”。
2. 将现有的 ADFS 声明规则备份到文本文件中：

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudStaging" | Select-
    Object -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
<!--NeedCopy-->
```

3. 下载 Citrix 提供的 claimrules.txt 文件，网址为 https://github.com/citrix/sample-scripts/tree/master/citrix-cloud。
4. 将 claimrules.txt 文件复制到您的桌面。
5. 使用 claimrules.txt 文件导入所需的声明规则：

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -MetadataUrl "https://saml.cloud.com/saml/
                         metadata" `
                      -AutoUpdateEnabled $True `
                      -IssuanceTransformRulesFile "$env:
                         USERPROFILE\desktop\claimrules.txt" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
                          `
                      -Enabled $True
<!--NeedCopy-->
```

使用 **PowerShell** 更新信赖方信任的 **SAML** 签名设置

默认情况下，ADFS 信赖方信任具有以下设置：

- EncryptClaims: True
- SignedSamlRequestsRequired: False
- SamlResponseSignature: AssertionOnly

为了提高安全性，Citrix 建议对单点登录 (SSO) 和单点注销都使用已签名的 SAML 请求。本节介绍如何使用 PowerShell 更新现有信赖方信任的签名设置，使其符合 Citrix 推荐的配置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 在 ADFS 服务器上获取当前 RelyingPartyTrust 配置。

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
<!--NeedCopy-->
```

2. 更新 **CitrixCloudProd** 信赖方信任设置。

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                          -SignedSamlRequestsRequired $True `
                          -SamlResponseSignature "MessageAndAssertion"
<!--NeedCopy-->
```

3. 联系 Citrix 支持部门，申请激活 Citrix Cloud 客户的 **EnableSamlLogoutSigningAndPost** 身份验证功能。这会导致 Citrix Cloud 在用户注销 Citrix Workspace 或 Citrix Cloud 时以已签名的 POST 请求而不是未签名的重定向请求发送 SAML 单点注销请求。如果 SAML 提供商要求单点注销的签名请求并拒绝未签名的重定向，则需要发送已签名的 POST 请求。

Citrix Cloud 中的 SAML 配置

在 Citrix Cloud 中配置 SAML 连接时（如将 SAML 提供商元数据添加到 Citrix Cloud 中所述），您需要按如下方式输入 ADFS 的值：

在 Citrix Cloud 的这个字段中	输入此值
实体 ID	`https://adfs.YourDomain.com/adfs/services/trust`，其中 `YourDomain.com` 为您的 ADFS 服务器域。
签署身份验证请求	是
SSO 服务 URL	`https://adfs.YourDomain.com/adfs/ls`，其中 `YourDomain.com` 为您的 ADFS 服务器域。
绑定机制	HTTP 发布
SAML 响应	在回应或断言上签名
身份验证上下文	未指定，精确
注销 URL	`https://adfs.YourDomain.com/adfs/ls`，其中 `YourDomain.com` 为您的 ADFS 服务器域。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用自定义域通过 **SAML** 登录工作区

November 30, 2023

Author:
Mark Dear

如果您已在 Citrix Workspace 中配置了自定义域（例如 `https://workspaces.yourdomain.com`），则可能需要在 Citrix Cloud 和您的 SAML 提供程序中进行额外配置，具体取决于您希望在 Citrix Cloud 中支持的 SAML 登录场景。

您可能需要两个 SAML 应用程序才能进行此配置。Citrix Cloud 需要不同的 SAML 服务提供商 (SP) 端点，具体取决于 SAML 应用程序是使用 cloud.com 还是 workspaces.yourdomain.com URL 来执行登录操作。

有关在 Citrix Workspace 中配置自定义域的更多信息，请参阅 Citrix Workspace 产品文档中的配置自定义域。

部署一两个 **SAML** 应用程序的注意事项

要确定您需要部署单还是双 SAML 应用程序解决方案，请确定您需要您的 SAML 提供商支持哪种 SAML 登录场景组合。

默认情况下，以下登录场景共享相同的 SAML 应用程序（SAML 应用程序 1）：

- Citrix Workspace 的 SAML 身份验证，其中在您的 SAML 提供商中将您所在区域（cloud.com、citrixcloud.jp、cloud.us）的 Workspace 登录 URL 配置为 SP 实体 ID。
- 使用您的唯一登录 URL（例如 `https://citrix.cloud.com/go/mycompany`）对 Citrix Cloud 进行 SAML 身份验证。在这种情况下，根据管理员的 Active Directory (AD) 组成员资格，使用 SAML 向 Citrix Cloud 进行身份验证。

通过您在 Workspace 配置中配置的自定义域（例如 `https://workspaces.mycompany.com`）为用户添加 SAML 身份验证需要第二个 SAML 应用程序（SAML 应用程序 2）。

下表列出了 SAML 登录场景和所需的 SAML 应用程序的支持组合。

使用 Workspace URL 登录 Workspace	使用自定义域 URL 登录 Workspace	使用 SAML 登录 URL 登录 Citrix Cloud	需要 SAML 应用程序 1?	需要 SAML 应用程序 2?
是	否	否	是 - 使用 cloud.com SAML 端点	否
否	是	否	是 - 使用自定义域 SAML 端点	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用 Workspace URL 登录 Workspace	使用自定义域 URL 登录 Workspace	使用 SAML 登录 URL 登录 Citrix Cloud	需要 SAML 应用程序 1?	需要 SAML 应用程序 2?
否	否	是	是 - 使用 cloud.com SAML 端点	否
是	否	是	是 - 使用 cloud.com SAML 端点	否
否	否	是	是 - 使用 cloud.com SAML 端点	是 - 使用自定义域 SAML 端点
是	是	是	是 - 使用 cloud.com SAML 端点	是 - 使用自定义域 SAML 端点

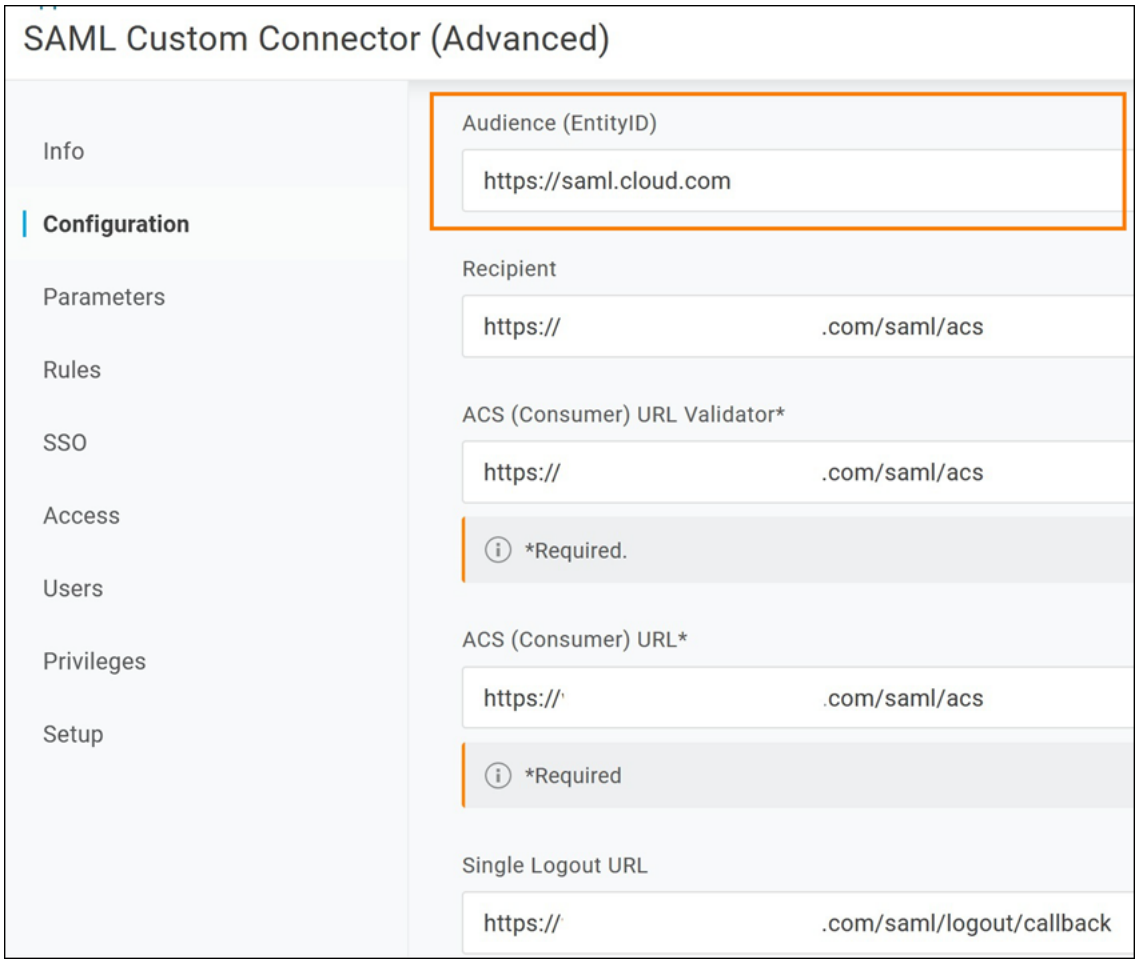
单个 **SAML** 应用程序配置

1. 在 Citrix Cloud 中，转到 **Workspace** 配置 **>** 访问并配置自定义域。有关更多信息，请参阅配置自定义域。
2. 在您的 SAML 提供商的管理控制台中，使用自定义域作为 SP 端点配置单个 SAML 应用程序。
3. 下载 SAML 应用程序的 SAML 签名证书。在稍后的步骤中，您将此证书上载到 Citrix Cloud。
4. 对于实体 ID，请确保已输入 `https://saml.cloud.com`。根据您的 SAML 提供商的不同，此设置可能会被标记为“受众”。对于所有其他端点，请将 `https://saml.cloud.com` 替换为您在步骤 1 中配置的 Workspace 自定义域。

   以下示例说明了 Okta 的端点配置，其中受众限制包含实体 ID 值：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

以下示例说明了 OneLogin 的端点配置，其中受众包含实体 ID 值：



5. 在 Citrix Cloud 中，转到身份和访问管理 **>** 身份验证并配置 SAML 连接。
6. 转到 **Workspace** 配置 **>** 身份验证，然后选择 **SAML 2.0**。
7. 转到 **Workspace** 配置 **>** 自定义 **Workspace URL >** 编辑，然后选择仅使用自定义域。
8. 选择“保存”以保存您的更改。
9. 要测试配置，请使用您的自定义 Workspace URL (`https://workspaces.mycompany.com`) 登录 Citrix Workspace。

双 **SAML** 应用程序配置

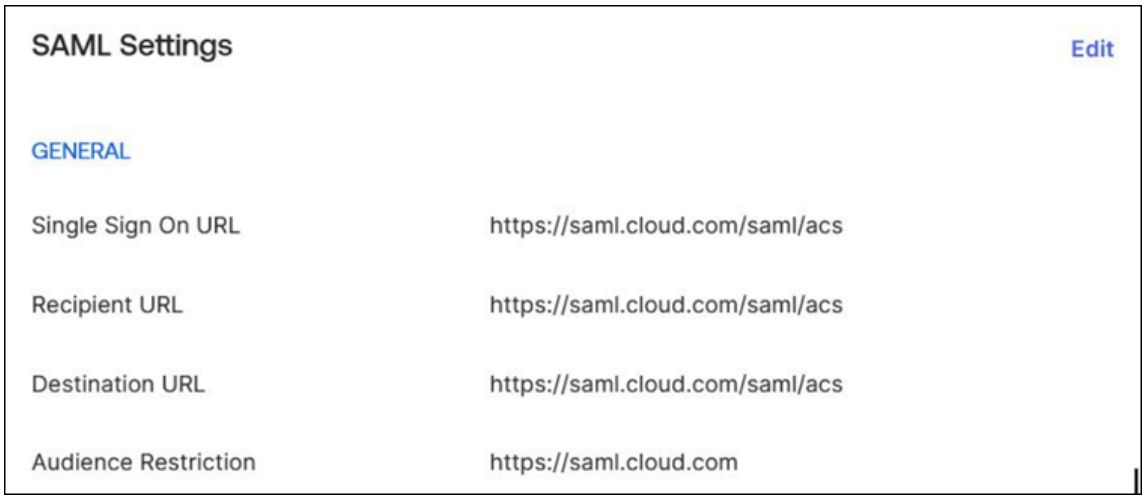
1. 在 Citrix Cloud 中，转到 **Workspace** 配置 **>** 访问并配置自定义域。有关更多信息，请参阅配置自定义域。
2. 在您的 SAML 提供商的管理控制台中，配置两个 SAML 应用程序。以相同方式配置这些应用程序，包括 SSO 和 SLO 请求的相同签名设置、绑定类型和注销设置。如果这些 SAML 应用程序中的配置不匹配，则在 Workspace URL 和 Workspace 自定义域之间切换时，您的登录和注销行为可能会有所不同。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

3. 在第一个 SAML 应用程序中，配置以下 SP 端点：

   - 实体 ID：`https://saml.cloud.com`
   - 声明使用者服务：`https://saml.cloud.com/saml/acs`
   - 注销：`https://saml.cloud.com/saml/logout/callback`

   以下示例显示了 Okta 管理控制台中的此端点配置：



4. 在第二个 SAML 应用程序中，配置以下 SP 端点。仅将您的 Workspace 自定义域用于声明使用者服务和注销端点。

   - 实体 ID：`https://saml.cloud.com`
   - 声明使用者服务：`https://workspaces.mycompany.com/saml/acs`
   - 注销：`https://workspaces.mycompany.com/saml/logout/callback`

   以下示例显示了 Okta 控制台中的此端点配置。请注意，受众限制包含实体 ID 值。

5. 下载两个 SAML 应用程序的 SAML 签名证书。您可以在稍后的步骤中将其上载到 Citrix Cloud。
6. 在 Citrix Cloud 管理控制台中，配置 SAML 连接：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

a) 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
b) 在身份验证选项卡上，找到 **SAML 2.0**，单击省略号按钮，然后选择连接。
c) 在配置 **SAML** 页面上，输入您在步骤 2 中创建的第一个 SAML 应用程序的详细信息。

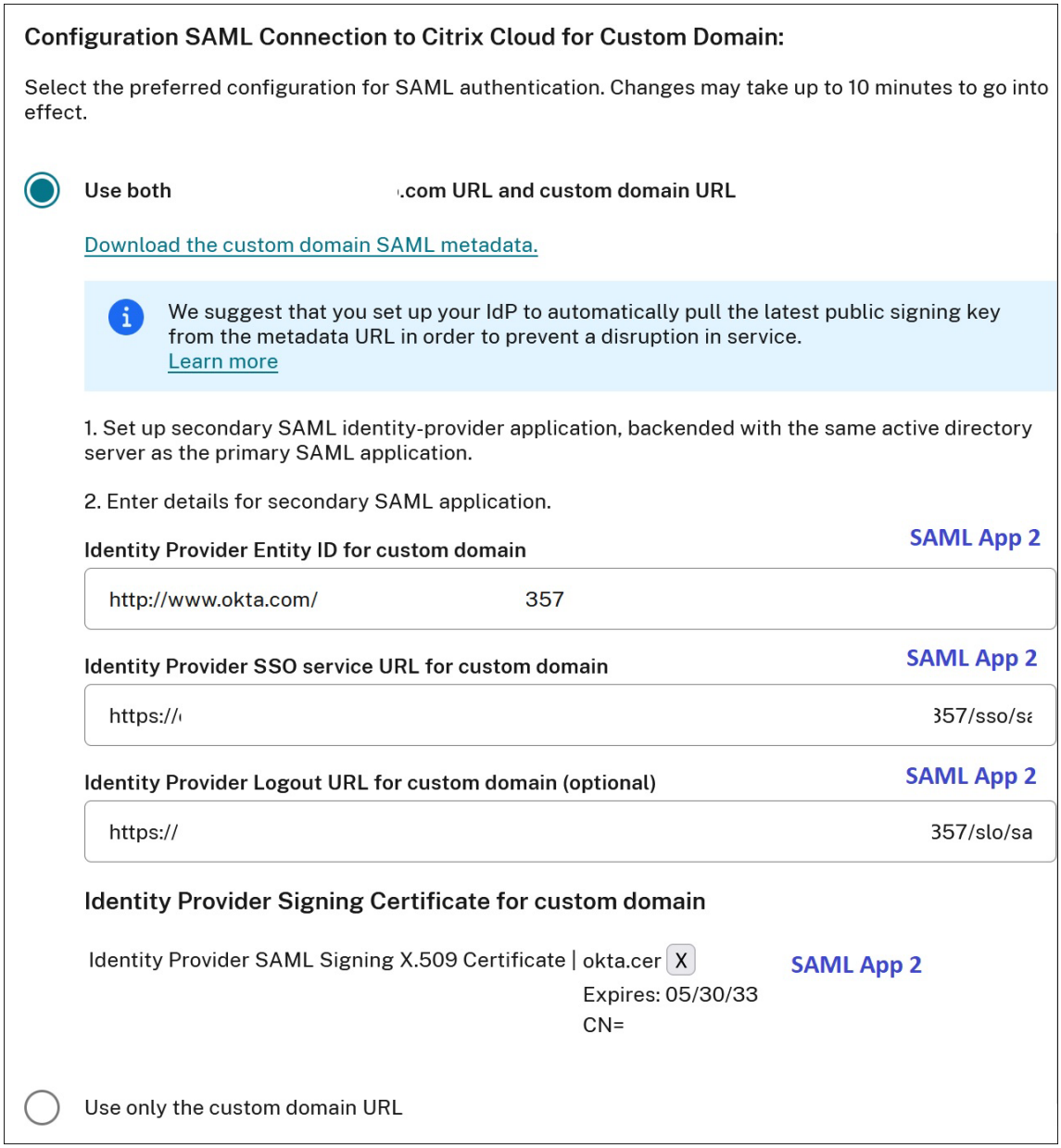
7. 将 Citrix Workspace 配置为使用新的 SAML 连接：

a) 在 Citrix Cloud 菜单中，选择 **Workspace** 配置。
b) 在身份验证选项卡上，选择 **SAML 2.0**。

8. 在访问选项卡的 自定义 **Workspace URL** 中，选择编辑。
9. 在“配置 **SAML**”页面上，选择“同时使用 **customer.cloud.com URL** 和自定义域 **URL**”。
10. 输入以下信息：

- 在自定义域的身份提供商实体 **ID** 中，输入您在步骤 2 中创建的第二个 SAML 应用程序中的实体 ID。
- 在自定义域的 **SSO** 服务 **URL** 中，输入第二个 SAML 应用程序的 SSO URL。
- 在自定义域的注销 **URL** 中，输入第二个 SAML 应用程序的 SLO URL。
- 在自定义域的身份提供商签名证书中，从第二个 SAML 应用程序上载 SAML 签名证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

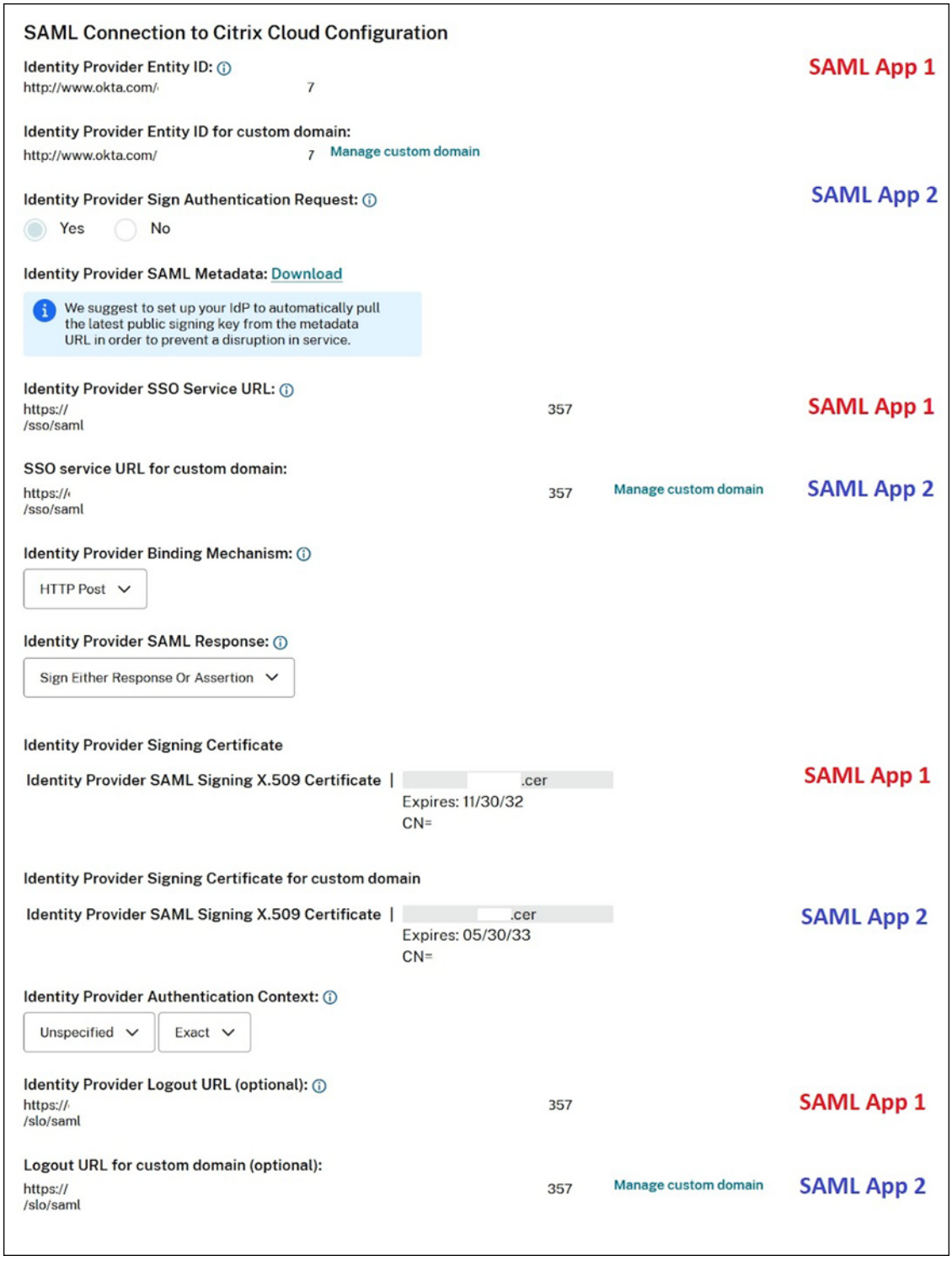


11. 选择“保存”以保存您的更改。

查看 **SAML** 连接的详细信息

配置完成后，转到身份和访问管理 **>** 身份验证。在 **SAML 2.0** 中，从省略号菜单中选择选择 **SAML** 提供商 **>** 查看。SAML 配置页面显示为实体 ID、SSO URL 和注销 URL 配置的成对的 SAML 端点。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



所有其他 SAML 配置设置适用于您创建的第一个和第二个 SAML 应用程序。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

验证登录 **Citrix Workspace**

要验证您配置的登录和注销行为，请执行以下测试：

- 使用您的 Workspace URL (`https://mycompany.cloud.com`) 和 SAML 提供程序登录 Citrix Workspace。
- 使用您的 Workspace 自定义域 (`https://workspace.mycompany.com`) 和 SAML 提供程序登录 Citrix Workspace。
- 使用您的唯一登录 URL (`https://citrix.cloud.com/go/mycompany`) 和您的 SAML 提供商登录 Citrix Cloud。

将 **Okta** 配置为 **SAML** 提供商以进行 **Workspace** 身份验证

March 11, 2024

Author:
Mark Dear

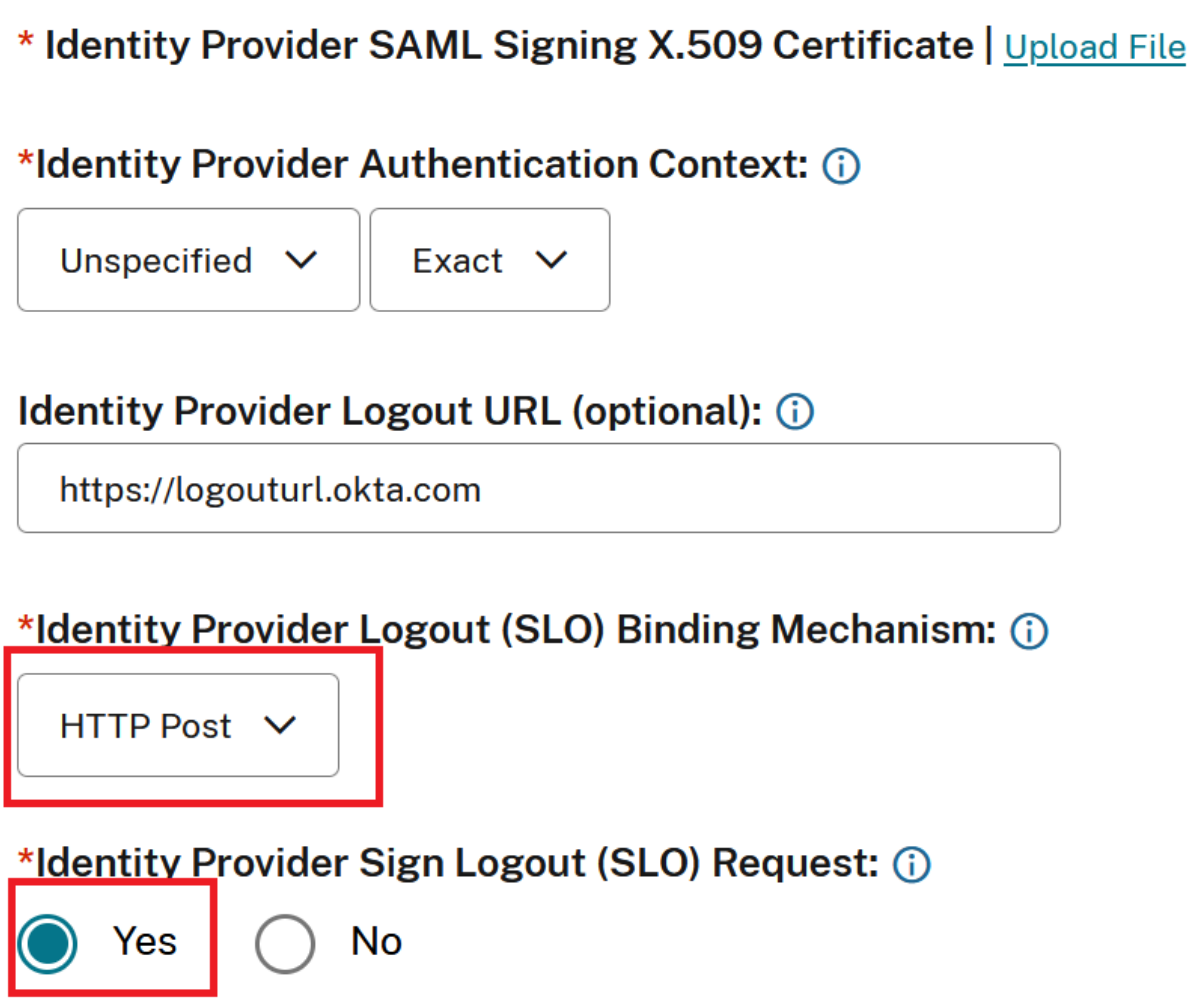
本文介绍了配置 Okta SAML 应用程序所需的步骤以及 Citrix Cloud 与您的 SAML 提供商之间的连接。其中一些步骤描述了您在 SAML 提供商的管理控制台中执行的操作。

必备条件

在完成本文中的任务之前，请确保满足以下必备条件：

- Citrix 支持已在 Citrix Cloud 中启用了 **SendNameIDPolicyInSAMLRequest** 功能。此功能可应要求启用。有关这些功能的详细信息，请参阅使用 Okta 的 SAML 所需的云功能。
- 您有一个使用下面其中一个 Okta 域的 Okta 组织：
  - okta.com
  - okta-eu.com
  - oktapreview.com
- 您已将 Active Directory (AD) 与 Okta 组织同步。
- 您的 Okta 组织已启用签名身份验证请求。
- 身份提供程序单点注销 **(SLO)** 是在 Citrix Cloud 和 Okta SAML 应用程序中配置的。配置 SLO 后，最终用户注销 Citrix Workspace 时，他们也会注销 Okta 和共享 Okta SAML 应用程序的所有其他服务提供商。
- 在 Citrix Cloud 中启用了身份提供程序登录注销 **(SLO)** 请求。
- 身份提供程序注销绑定 **(SLO)** 是 Citrix Cloud 中的 HTTPPost。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



使用 **Okta** 的 **SAML** 所需的云功能

在完成本文中的任务之前，必须联系 Citrix 支持部门以启用 **SendNameIDPolicyInSAMLRequest** 功能。此功能使 Citrix Cloud 能够在 SAML 请求中将 **NameID** 策略作为“未指定”提供给您的 SAML 提供程序。启用此功能仅适用于 Okta。

可以通过登录您的 Citrix 帐户并通过 Citrix 技术支持 Web 站点开立票据来请求这些功能。

要求

本文包括在 Okta 管理控制台中创建 SAML 应用程序的任务。此应用程序需要您的 Citrix Cloud 区域的 SAML 签名证书。

> 重要提示：
>
> 签名证书必须以 PEM 格式编码。Citrix Cloud 不接受其他编码格式的签名证书。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可以使用提取工具（例如位于 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract 的提取工具）从您所在地区的 Citrix Cloud SAML 元数据中提取此证书。Citrix 建议您事先获取 Citrix Cloud SAML 证书，以便在需要时提供该证书。

本部分中的步骤描述了如何使用提取工具获取签名证书，网址为 https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract。

要获取您所在地区的 Citrix Cloud 元数据，请执行以下操作：

1. 在您选择的提取工具中，输入您的 Citrix Cloud 区域的元数据 URL：
   - 对于欧盟、美国和亚太南部区域，请输入 `https://saml.cloud.com/saml/metadata`。
   - 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/metadata`。
   - 对于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/metadata`。
2. 单击加载。提取的证书显示在您输入的 URL 下方。
3. 单击下载下载 PEM 格式的证书。

与 **Okta AD** 代理同步帐户

要使用 Okta 作为 SAML 提供商，您必须先将本地 AD 与 Okta 集成。为此，您需要在域中安装 Okta AD 代理，然后将您的 AD 添加到您的 Okta 组织。有关部署 Okta AD 代理的指导，请参阅 Okta Web 站点上的 Active Directory 集成入门。

之后，将您的 AD 用户和组导入 Okta。导入时，请包括以下与您的 AD 帐户关联的值：

- 电子邮件
- SID
- UPN
- OID

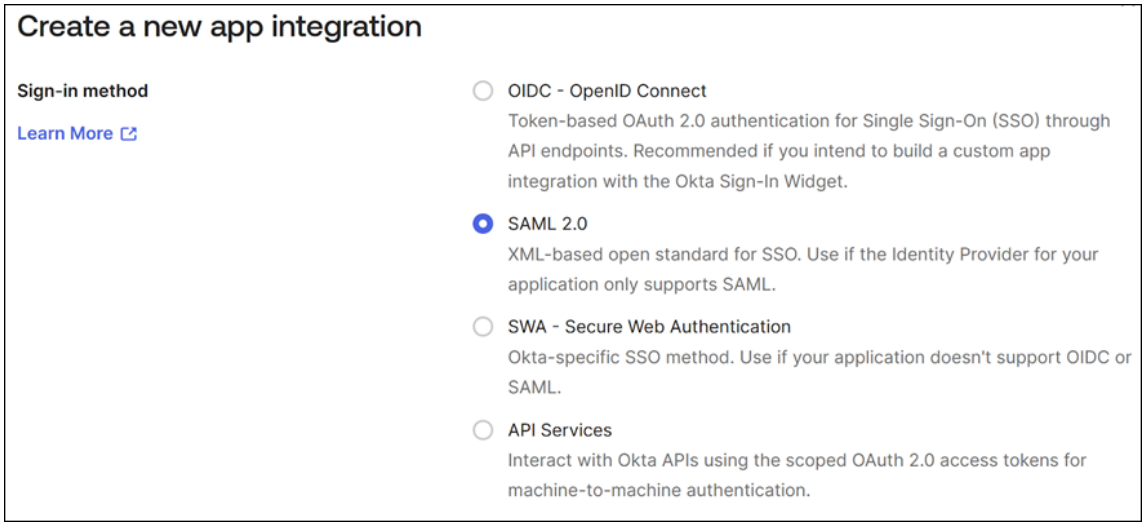
要将 AD 用户和组与 Okta 组织同步，请执行以下操作：

1. 安装和配置 Okta AD 代理。有关完整说明，请参阅 Okta 网站上的以下文章：
   - 安装 Okta Active Directory 代理
   - 配置 Active Directory 导入和帐户设置
   - 配置 Active Directory 置备设置
2. 通过执行手动导入或自动导入，将您的 AD 用户和组添加到 Okta。有关 Okta 导入方法和说明的详细信息，请参阅 Okta 网站上的 管理 Active Directory 用户和组 。

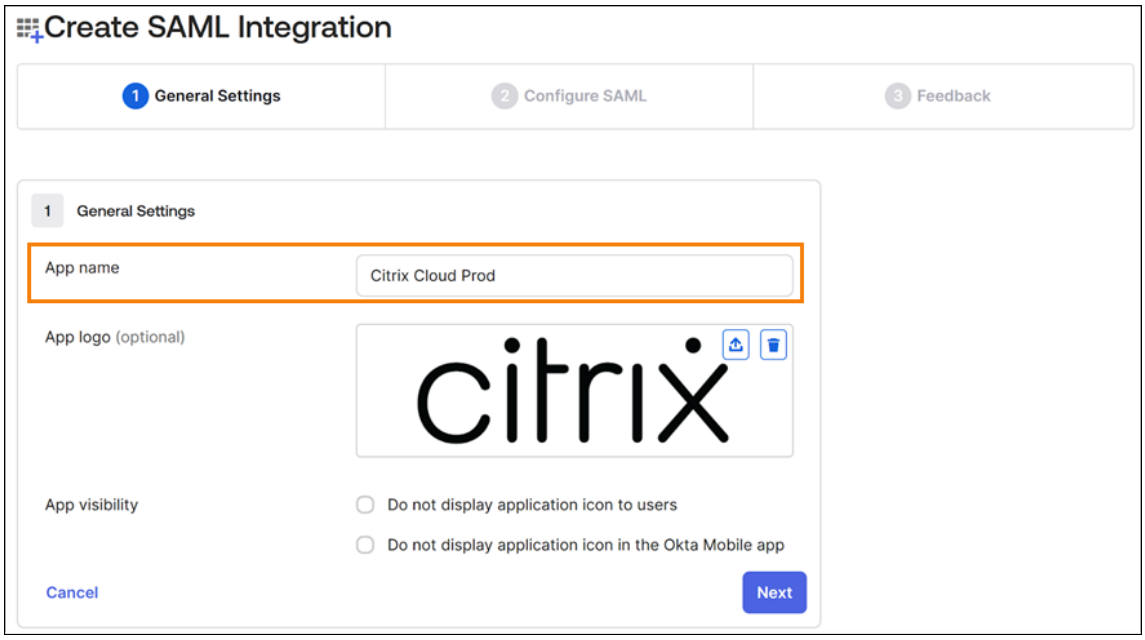
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置 **Okta SAML** 应用程序以进行 **Workspace** 身份验证

1. 使用具有添加和配置 SAML 应用程序权限的管理员帐户登录您的 Okta 组织。
2. 在管理员控制台中，选择应用程序 **>** 应用程序 **>** 创建应用程序集成，然后选择 **SAML 2.0**。选择下一步。



3. 在应用程序名称中，输入应用程序的友好名称。选择下一步。



4. 在 **SAML** 设置部分中，配置 Citrix Cloud 服务提供商 (SP) 连接：

   a) 在单点登录 **URL** 中，输入与您的 Citrix Cloud 客户的 Citrix Cloud 区域对应的 URL：

   - 如果您的客户 ID 位于欧盟、美国或亚太南部地区，请输入 `https://saml.cloud.com/saml/acs`。
   - 如果您的客户 ID 位于日本地区，请输入 `https://saml.citrixcloud.jp/saml/acs`。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 如果您的客户 ID 位于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us/saml/acs`。

b) 选择使用此 **URL** 作为收件人和目标 **URL**。

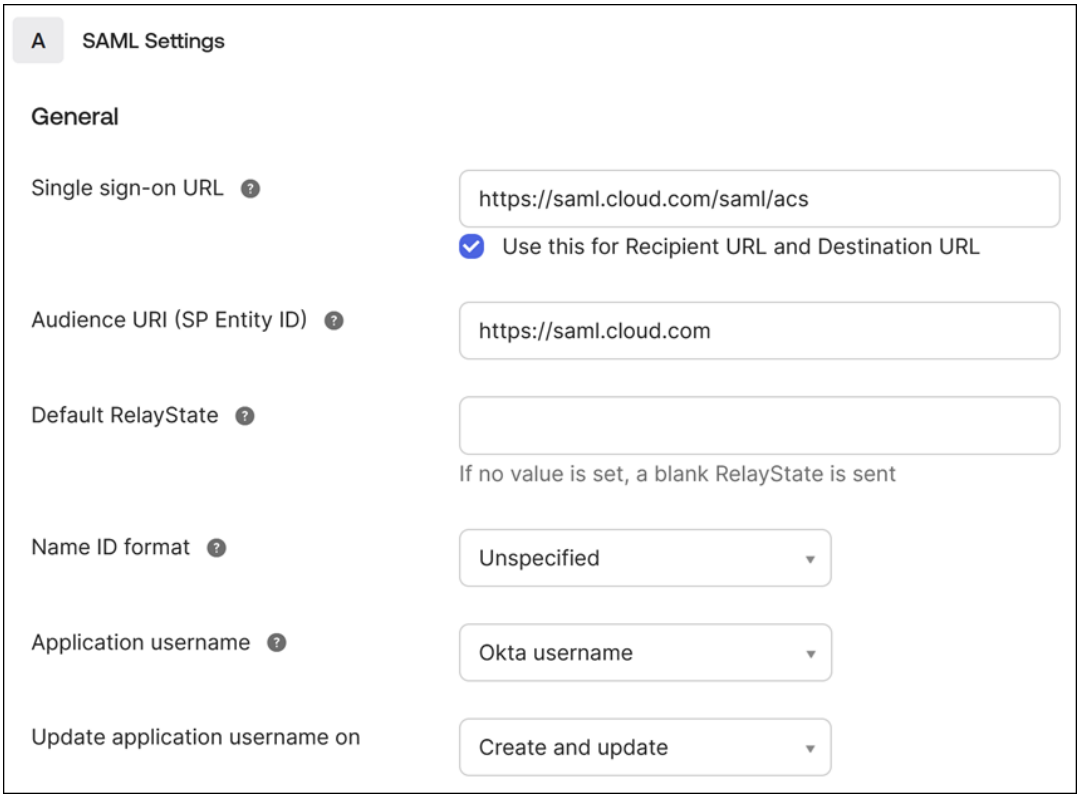
c) 在受众 **URI (SP** 实体 **ID)** 中，输入与您的 Citrix Cloud 客户的 Citrix Cloud 区域对应的 URL：

- 如果您的客户 ID 位于欧盟、美国或亚太南部地区，请输入 `https://saml.cloud.com`。
- 如果您的客户 ID 位于日本地区，请输入 `https://saml.citrixcloud.jp`。
- 如果您的客户 ID 位于 Citrix Cloud Government 区域，请输入 `https://saml.cloud.us`。

d) 在名称 **ID** 格式中，选择未指定。Citrix Cloud 在 SAML 请求中发送的 NameID 策略必须与 Okta SAML 应用程序中指定的 NameID 格式相匹配。如果这些项目不匹配，则启用签名身份验证请求会导致 Okta 出错。

e) 在应用程序用户名中，选择 **Okta** 用户名。

作为此配置的示例，下图说明了美国、欧盟和亚太南部地区的正确配置：



> 重要提示：
>
> 必须将名称 **ID** 设置配置为未指定。为此设置使用不同的值会导致 SAML 登录失败。

f) 单击显示高级设置并配置以下设置：

- 在响应中，选择已签名。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在断言签名中，选择已签名。
- 在签名算法中，选择 **RSA-SHA256**。
- 在断言加密中，选择未加密。

g) 在签名证书中，以 PEM 格式上载您的 Citrix Cloud 区域的 SAML 签名证书。有关获取 SAML 签名证书的说明，请参阅本文中的要求。

h) 在启用单点注销中，选择允许应用程序启动单点注销。

i) 在单点注销 **URL** 中，输入与您的 Citrix Cloud 区域对应的 URL：

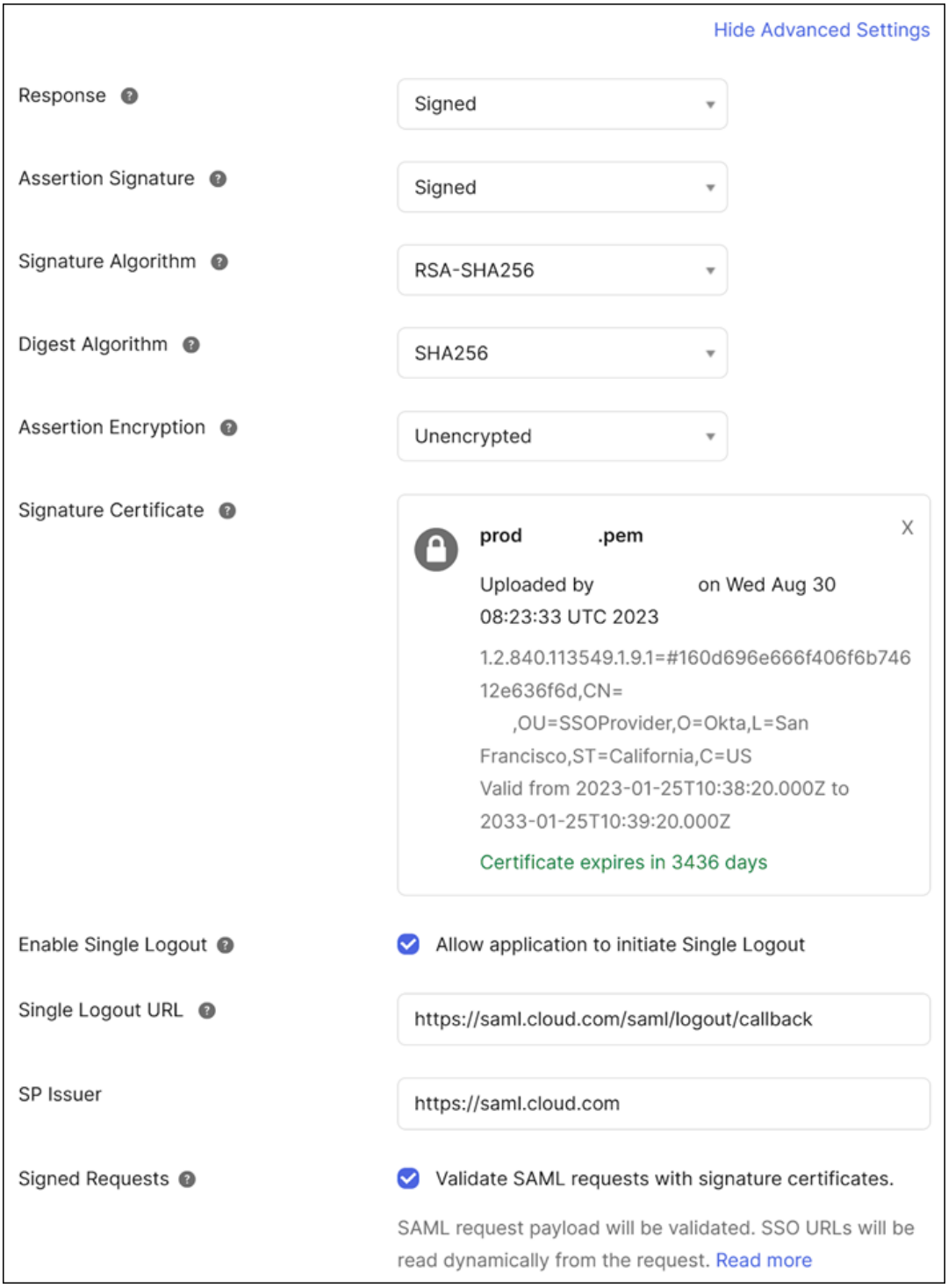
- 对于欧盟、美国和亚太南部区域，请输入 `https://saml.cloud.com/saml/logout/callback`。
- 对于日本区域，请输入 `https://saml.citrixcloud.jp/saml/saml/logout/callback`。
- 对于 Citrix Cloud Government，请输入 `https://saml.cloud.us/saml/logout/callback`。

j) 在 **SP** 发行者中，输入您之前在受众 **URI (SP** 实体 **ID)**（此任务的步骤 4c）中输入的值。

k) 在签名请求中，选择使用签名证书验证 **SAML** 请求。

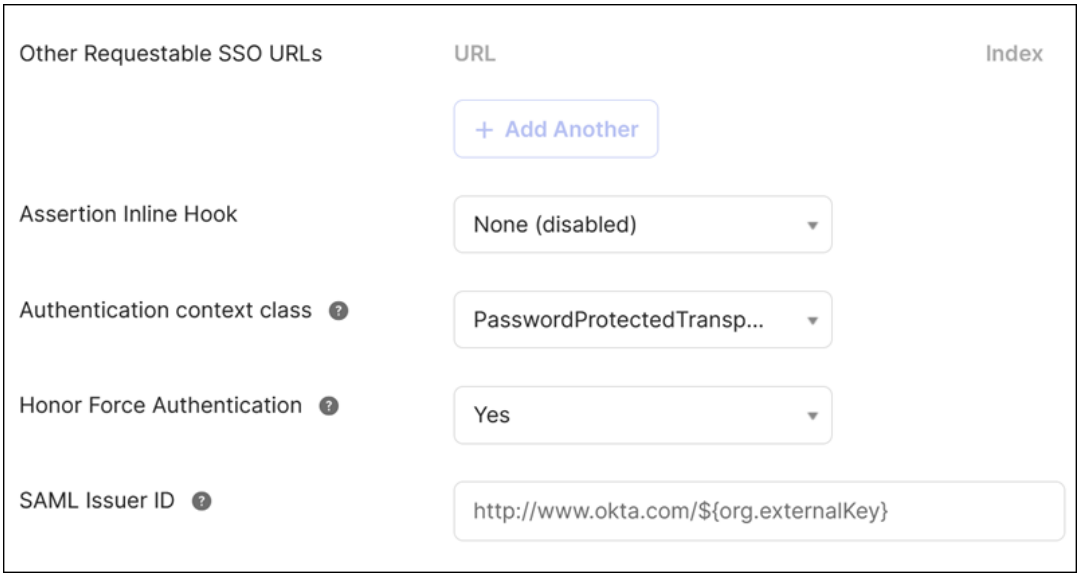
下图说明了美国、欧盟和亚太南部地区的正确配置：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



l) 对于所有剩余的高级设置，请接受默认值。

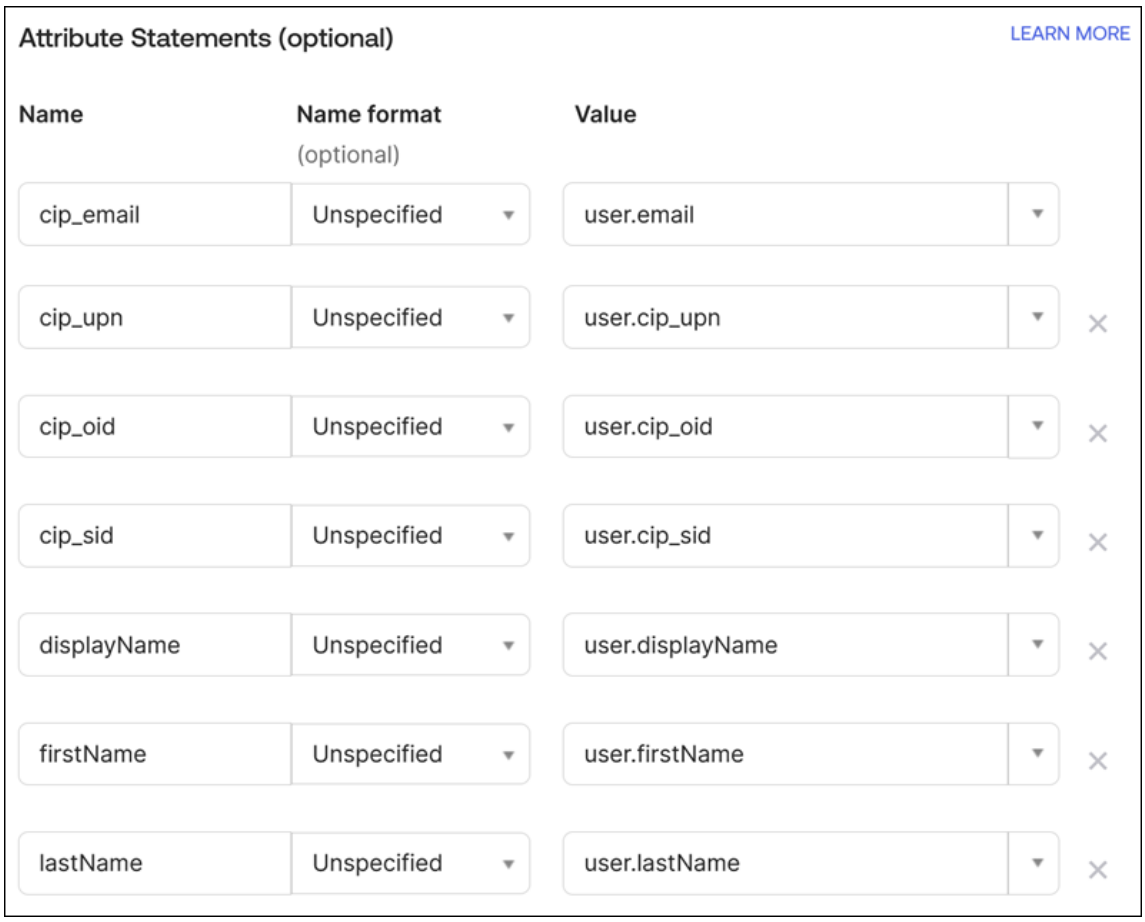
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



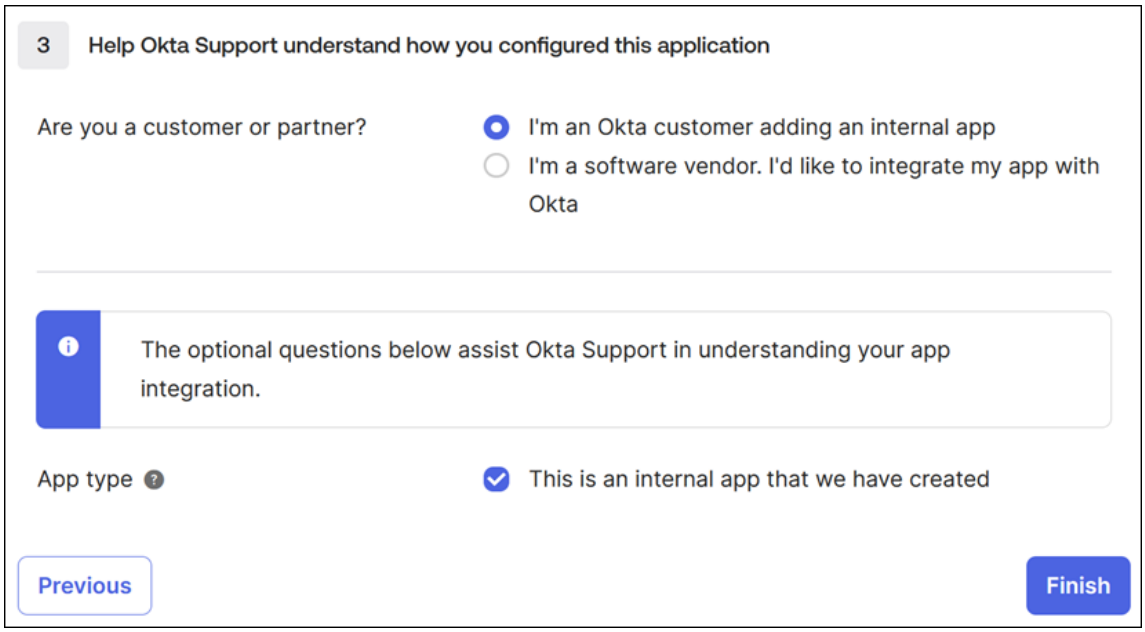
5. 在属性语句 **(**可选**)** 下，输入名称、名称格式和值的值，如下表所示：

名称	名称格式	值
cip_email	未指定	user.email
cip_upn	未指定	user.cip_upn
cip_oid	未指定	user.cip_oid
cip_sid	未指定	user.cip_sid
displayName	未指定	user.displayName
firstName	未指定	user.firstName
lastName	未指定	user.lastName

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



6. 选择下一步。此时将出现 Okta 配置语句。



7. 在您是客户还是合作伙伴**?** 中，选择我是添加内部应用程序的 **Okta** 客户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

8. 在应用程序类型中，选择这是我们创建的内部应用程序。
9. 选择完成保存您的配置。此时将显示您的 SAML 应用程序的配置文件页面，并显示登录选项卡的内容。

配置完成后，选择分配选项卡，然后将用户和组分配给 SAML 应用程序。

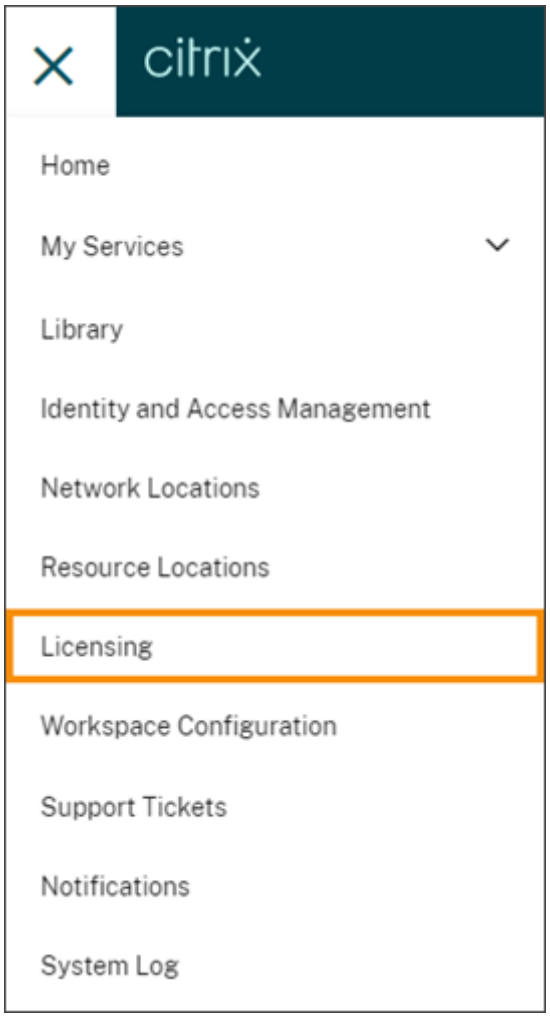
Citrix Cloud 的许可

November 30, 2023

Citrix Cloud 为某些云服务提供许可证和使用情况监视。此外，许可证和使用情况监控可用于在 Citrix Cloud 中注册 Citrix 许可证服务器的本地部署。

面向企业客户的许可

企业客户可以通过从 Citrix Cloud 菜单中选择“许可”来监视支持的云服务的许可分配和使用情况。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关云服务的企业许可证和使用情况监视的更多信息，请参阅监视云服务的许可证和活跃使用情况。

本地部署许可

在本地部署 Citrix Virtual Apps and Desktops 的企业客户可以使用 Citrix Cloud 随时了解用户/设备和并发许可模式的许可证和使用情况。通过向 Citrix Cloud 注册 Citrix 许可证服务器，客户可以使用 Citrix Cloud 中的 许可部署页面执行以下任务：

- 监视已注册许可证服务器的报告状态
- 查看使用用户/设备许可模式的部署的许可证分配和使用趋势。
- 查看使用并发许可模式的部署的许可证使用峰值趋势。

有关本地 Virtual Apps and Desktops 部署的许可证和使用情况监视的更多信息，请参阅监视本地部署的许可证和使用情况。

Citrix 服务提供商 **(CSP)** 的许可

Citrix 服务提供商可以使用以下工具来了解和报告产品许可证和使用情况：

- 许可证使用情况见解是 Citrix Cloud 中的一项免费服务，用于收集和汇总单租户和多租户客户的产品使用信息。有关详细信息，请参阅针对 Citrix 服务提供商的许可。
- Citrix Cloud 中的许可功能使 CSP 的客户能够监控其受支持的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）产品的许可证和使用情况。CSP 也可以在其客户的 Citrix Cloud 帐户下登录以查看和导出此信息。有关详细信息，请参阅以下文章：
  - Citrix DaaS 的客户许可证和使用情况监视
  - Citrix DaaS Standard for Azure 的客户许可证和使用情况监视

监视云服务的许可证和活跃使用情况

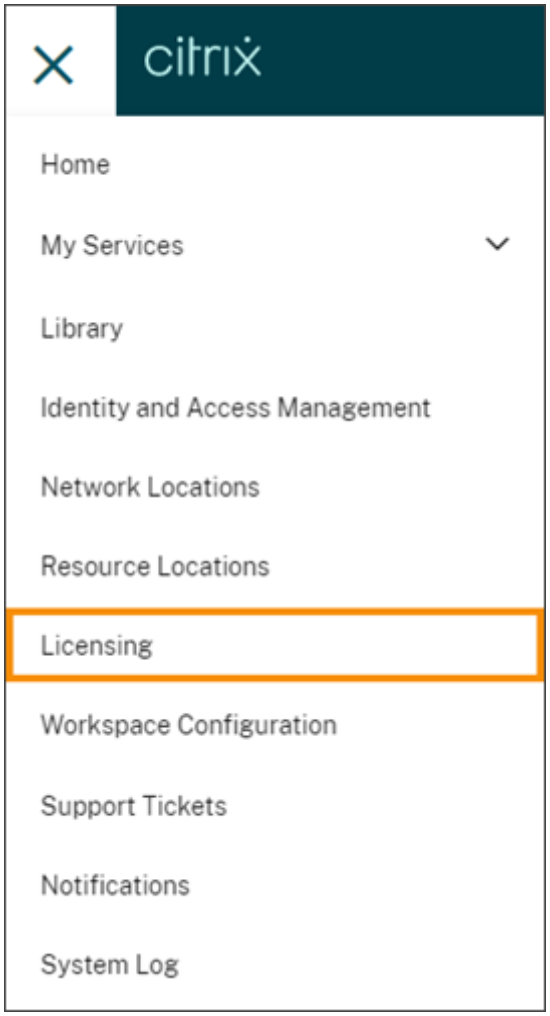
October 5, 2023

Citrix Cloud 中的许可使您能够掌握所购买的云服务的许可证消耗情况。使用摘要和详细报告，您可以：

- 一目了然地查看许可证的可用性和分配
- 查看适用云服务的每日和每月活跃使用量趋势
- 深入查看各个许可证分配的详细信息和使用趋势
- 将许可证使用数据导出为 CSV

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要查看云服务的许可数据，请从控制台菜单中选择 许可。



> 注意：
>
> 本文介绍所有受支持的 Citrix Cloud 服务通用的许可功能。许可的某些方面可能会有所不同，具体取决于服务（例如，许可证分配）。有关每项服务的许可证和使用情况的更多信息，请参阅以下文章：
>
> - 监视 Citrix DaaS（用户/设备）的许可证和活动使用情况
> - 监视 Citrix DaaS 和 Citrix DaaS Standard for Azure 的许可证和峰值使用情况（并发）
> - 监视 Citrix DaaS Standard for Azure 的许可证和活动使用情况 （仅限用户/设备）
> - 监控 Endpoint Management 服务的许可证和活动使用情况
> - 监控网关服务的带宽使用情况
> - 监视 Secure Private Access 的许可证和使用情况

支持的区域和云服务

许可仅适用于美国、欧盟和亚太南部地区的受支持服务。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

以下云服务支持许可：

- Citrix DaaS（用户/设备和并发许可模式）- 以前称为 Citrix Virtual Apps and Desktops 服务
- Citrix DaaS Standard for Azure（用户/设备许可模式）- 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard
- Endpoint Management
- 网关
- Secure Private Access（以前称为 Secure Workspace Access）

Citrix DaaS 的多类型许可

Citrix Cloud 中的许可支持 Citrix DaaS 的多类型许可。如果将用户/设备和并发许可模式引入到单个 Citrix Cloud 帐户中，Citrix Cloud 将在许可控制台页面中显示每种许可模式下的许可证使用情况。

Citrix 建议在查看许可页面之前，先在站点和交付组级别设置多类型许可。否则，可能不会显示正确的信息。有关说明，请参阅 Citrix DaaS 文档中的 多类型许可 。

如果成功使用 Web Studio 或 PowerShell 安装方法后，许可控制台页面未显示正确的多类型许可证使用情况，则可以使用以下选项：

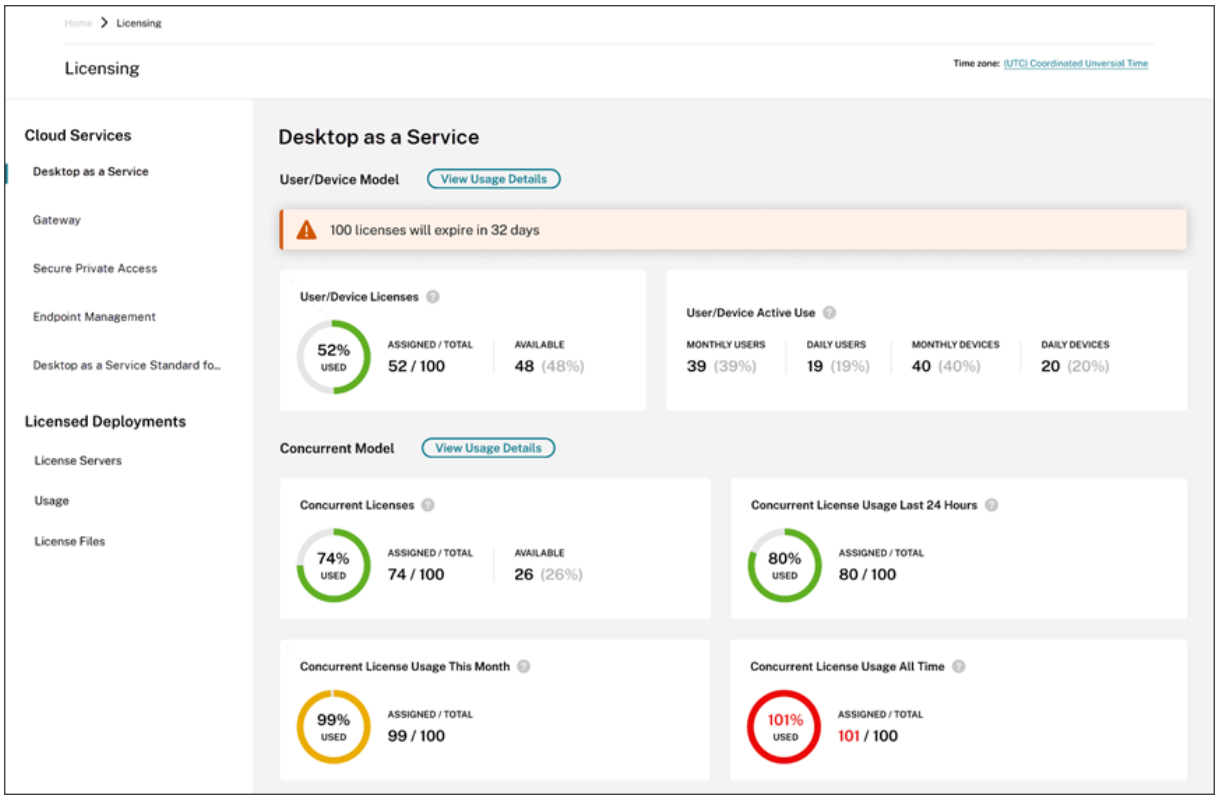
- 等待 30 天，然后 释放所有未使用的许可证。
- 请联系 Citrix 客户服务。

许可证分配

通常，用户在首次使用云服务时会获得许可。某些服务可能会根据其使用的许可模式以不同的方式分配许可证。有关如何为每项服务分配许可证的详细信息，请参阅本文顶部引用的许可文章。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

许可摘要和详细信息



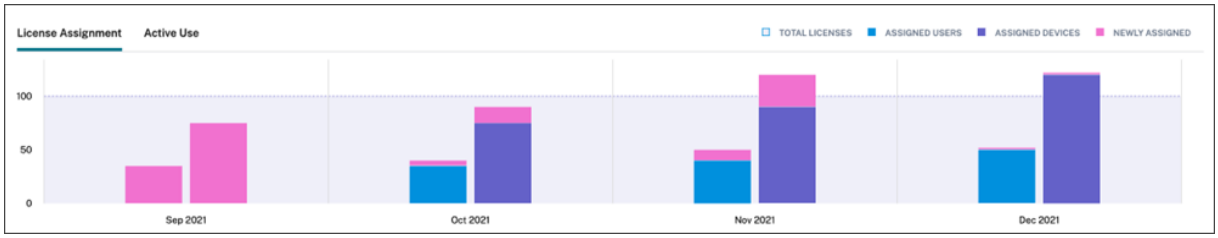
许可摘要提供了每项受支持服务的以下信息的概览：

- 分配的已购买许可证总数的百分比。当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。
- 分配的许可证与已购买的许可证的比率以及剩余的可用许可证数量。
- 云服务订阅到期之前的剩余时间。如果订阅在接下来的 90 天内到期，则会显示一条警告消息。

对于某些服务，此摘要可能包括其他信息，例如活跃使用情况。有关特定于服务的详细信息的更多信息，请参阅本文顶部引用的许可文章。

使用趋势和许可证活动

有关云服务许可证的详细视图，请单击 查看使用详情。然后，您可以查看云服务许可证的使用趋势和使用者的细分。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

此细分包括不同的信息，具体取决于云服务。有关特定于服务的使用趋势和许可证活动的更多信息，请参阅本文顶部引用的许可文章。

发放分配的许可证

通常，如果消费者连续 30 天未使用云服务，则分配的许可证有资格被释放。许可证发布后，剩余许可证的数量会增加，分配的许可证数量也会相应减少。

对于某些服务，许可证的发布可能会有所不同，具体取决于所使用的许可模式。有关发布特定服务许可证的更多信息，请参阅本文顶部引用的许可文章。

常见问题解答

- 如果分配的许可证超过购买的许可证，**Citrix** 是否会阻止使用云服务？不会，如果您过度使用云许可证金额，Citrix 不会阻止任何服务启动。许可证使用情况提供了用于了解您的云许可证使用情况的信息，因此 Citrix 希望您将监视许可证分配并保持在购买的许可金额之内。如果您认为自己会过度使用服务，Citrix 鼓励您联系销售代表，讨论您的许可要求。
- 正在捕获哪些许可信息？目前，仅捕获与用户登录相关的许可证信息。
- **Citrix DaaS** 是否支持多类型许可（例如，同时使用用户**/**设备和并发用户模型）？是。有关更多信息，请参阅本文中的 多类型许可 。
- **Citrix DaaS** 是否支持多版本许可？例如，我可以在同一 **Citrix Cloud** 帐户上同时使用高级版和高级版吗？不支持，此用例不受支持。Citrix DaaS 站点只能获得一个版本的许可。如果要在同一 Citrix Cloud 帐户上使用多个 Citrix DaaS 实例，则它们必须是同一版本。
- **Monitor** 报告（在 **Director** 中）与并发许可见解有什么区别？Monitor 报告和并发会话说明提供了与衡量正在使用的并发许可证不同的解释和指标。在大多数情况下，使用 Director 中的并发会话数来表示或预测使用中的峰值并发许可证会大大夸大所需的并发许可证数量。请勿使用 Director 中的监视器报告代替并发许可证使用情况的报告。报告工具的两个主要区别是：
  - 采样时间长度：许可有五分钟的采样周期。Citrix Cloud 每五分钟计算一次当前连接到该服务的唯一设备。将所有五分钟的采样周期进行汇总，以确定 24 小时、每月和合同期限内的峰值使用情况。Director 中的监视器报告最多可以显示两个小时的时间间隔，具体取决于报告的运行方式。
  - 唯一性：启动会话时，许可会寻找设备间的唯一性。监视器报告不考虑唯一的设备。
- * 在将用户迁移到云服务的新实例后（例如，我更改了组织的域名），为什么同一用户在用的许可证会被计算两次？ - Citrix Cloud 使用用户主体名称 (UPN) 来计算唯一用户数。如果用户在迁移之前和之后访问了云服务，Citrix Cloud 会为该用户捕获两个唯一的 UPN，每个都具有不同的域名。因此，Citrix Cloud 会对同一个用户进行两次计数。假设用户未使用旧域名访问服务，则可以在 30 天后释放旧的许可证分配。如果您过度使用云许可证金额，Citrix 不会阻止任何服务启动。
- * 为什么我看到同一个用户或设备有重复的许可证？ - 这是由适用于 HTML5 的 Workspace 应用程序和本地安装的 Workspace 应用程序设计的。通过 HTML5 的 Workspace 应用程序启动需要用户/设备许可证。同样，通过本地安装的 Workspace 应用程序启动会消耗用户/设备许可证。因此，如果用户通过适用于 HTML5 的

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Workspace 应用程序启动应用程序，然后通过本地安装的 Workspace 应用程序版本启动，Citrix Cloud 将显示该用户使用了两个许可证。此行为不会影响用户连接，但可能会导致许可控制台中的设备许可证使用报告过多。如果您过度使用云许可证金额，Citrix 不会阻止任何服务启动。

监视 **Citrix DaaS**（用户/设备）的许可证和活动使用情况

November 8, 2023

本文介绍如何使用 Citrix Cloud 中的许可控制台管理云服务许可证分配和监视活动使用情况。

如果您购买了 Citrix Azure 消费基金用于部署服务，请参阅 监视 Citrix DaaS 的 Citrix 托管 Azure 资源消耗情况，了解更多信息 。

许可证分配

当唯一用户或唯一设备首次启动应用程序或桌面时，Citrix Cloud 会分配许可证。

域名截断

如果您托管多个域并且用户在这些域中拥有相似的帐户（例如，johnsmith@company.com 和 johnsmith@mycompany.com），则可以允许 Citrix Cloud 忽略该帐户域，只考虑该帐户的用户名（例如 johnsmith）。此过程称为域名截断。默认情况下，域名截断处于禁用状态。

启用域名截断后，Citrix Cloud 对唯一用户的计算会发生变化。Citrix Cloud 没有将 johnsmith@company.com 和 johnsmith@mycompany.com 视为两个唯一用户，而只将 johnsmith 视为唯一用户。此计算更改会影响以下许可数据：

- 许可证分配
- 积极使用
- 一段时间内的许可证使用趋势
- 有资格发布的许可证

当您从许可控制台将数据导出到 CSV 文件时，许可数据的这些更改也会反映出来。

> 注意：
>
> 如果您托管多个具有相似帐户的域名，但用户名略有不同（例如，单个用户拥有帐户 johnsmith@company.com 和 jsmith@newcompany.com），则域名截断对 Citrix Cloud 的计算没有影响。Citrix Cloud 仍然将 johnsmith 和 jsmith 视为唯一用户，即使他们属于同一个人。

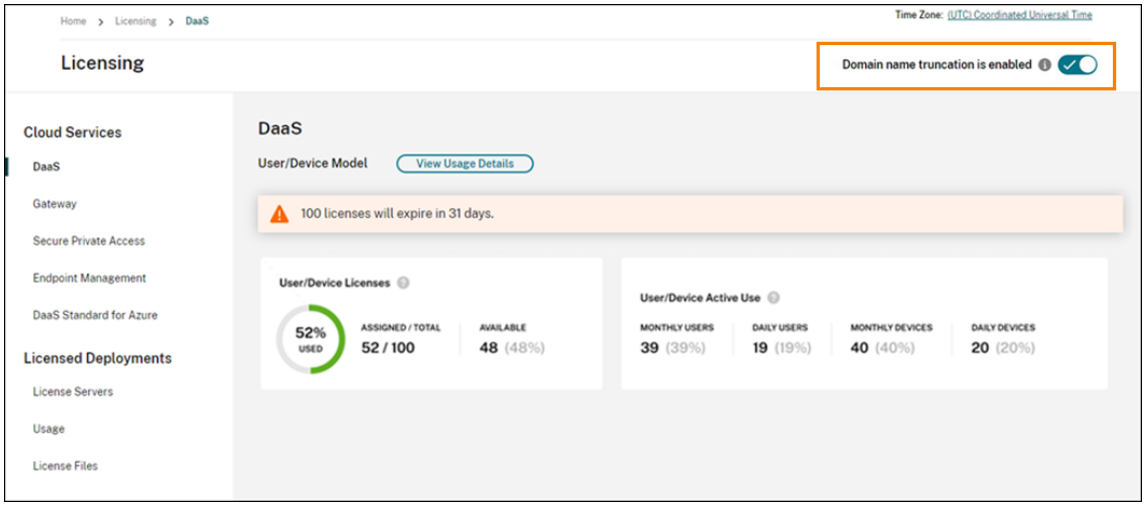
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

启用或禁用域名截断

默认情况下，域名截断处于禁用状态。从您启用或禁用该功能的那一刻起，域名截断就会影响您的用户/设备使用数据。例如，如果您在给定月份启用域名截断，Citrix Cloud 在该月记录的数据就会受到影响。但是，禁用该功能的前几个月的历史数据仍不受影响。同样，如果您在给定月份禁用域名截断，Citrix Cloud 在该月记录的数据也会受到影响。但是，启用该功能的月份的历史数据保持不变。

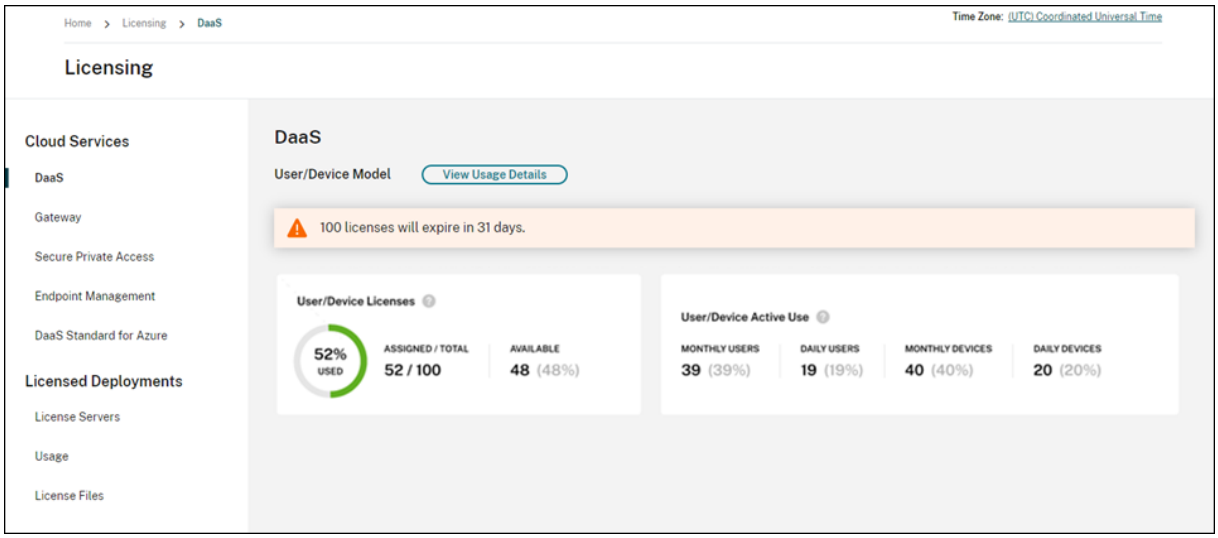
要启用或禁用域名截断，请执行以下操作：

1. 点击许可控制台右上角附近的切换开关。



2. 当系统提示您确认您的操作时，选择“是，我明白”。

许可摘要



许可摘要提供了以下信息的概览视图：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 已分配的已购买许可证占总许可证的百分比。当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。

  购买的许可证总数是已为使用用户/设备许可模式的 Citrix DaaS 版本购买的许可证的总和。

- 分配的许可证与已购买的许可证的比率以及剩余的可用许可证数量。
- 每月和每天的活跃使用情况统计信息：
  - 每月活跃使用量是指过去 30 天内使用过该服务的唯一身份用户或设备的数量。
  - 每日活跃使用量是指在过去 24 小时内使用过该服务的唯一用户或设备的数量。
- 云服务订阅到期之前的剩余时间。如果订阅在接下来的 90 天内到期，则会显示一条警告消息。

计算分配的许可证和有效使用情况

为了准确反映 Citrix DaaS 的用户/设备许可模式，Citrix Cloud 会计算使用该服务的唯一用户和唯一设备的数量。为了衡量分配的许可证，Citrix Cloud 使用这些计数中的较小值。为了衡量活跃使用情况，Citrix Cloud 使用每个计数作为给定时间段内活跃用户和活动设备的数量。

计算已分配许可证的示例

如果有 100 个唯一用户和 50 个唯一设备使用了该服务，Citrix Cloud 将使用较小的数字 (50) 来确定分配的许可证数量。已使用的许可证百分比和可用许可证的数量基于这 50 个分配的许可证。

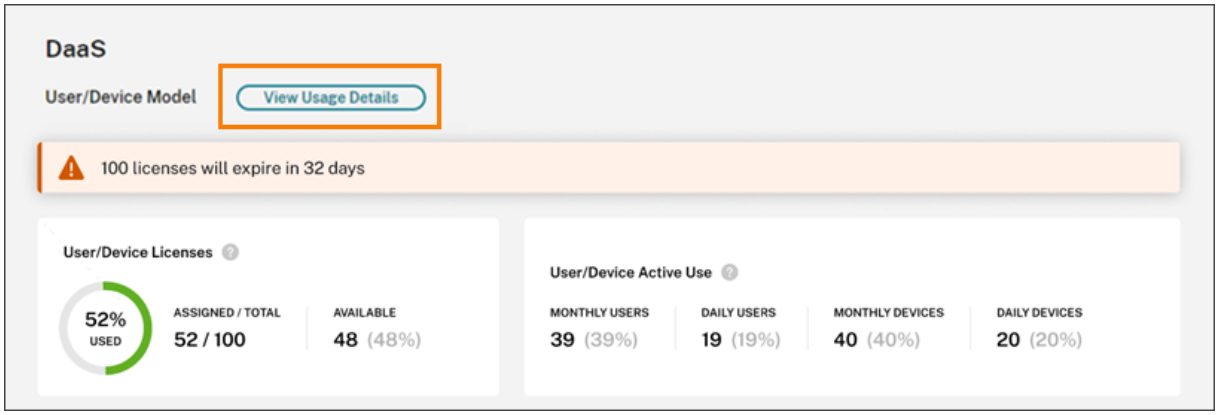
计算活跃使用量的示例

如果在过去 30 天内有 10 个唯一用户和 20 个唯一设备使用了该服务，则 Citrix Cloud 会确定每月活跃用户包括 10 个活跃用户和 20 个活动设备。同样，如果在过去 24 小时内计算了 30 个唯一用户和 15 个唯一设备，则 Citrix Cloud 会确定每日活跃用户包括 30 个活跃用户和 15 个活动设备。

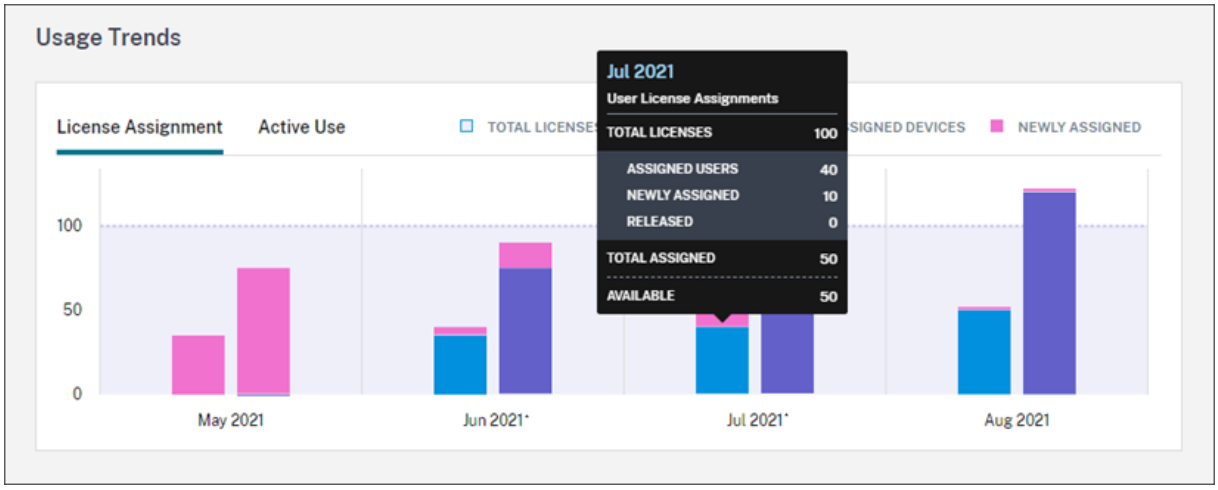
使用趋势

有关许可证的详细视图，请单击摘要最右侧的 查看使用详情。然后，您可以查看使用趋势以及正在使用云服务许可证的个人用户和设备的细分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



“使用趋势”部分将此细分显示为图表。

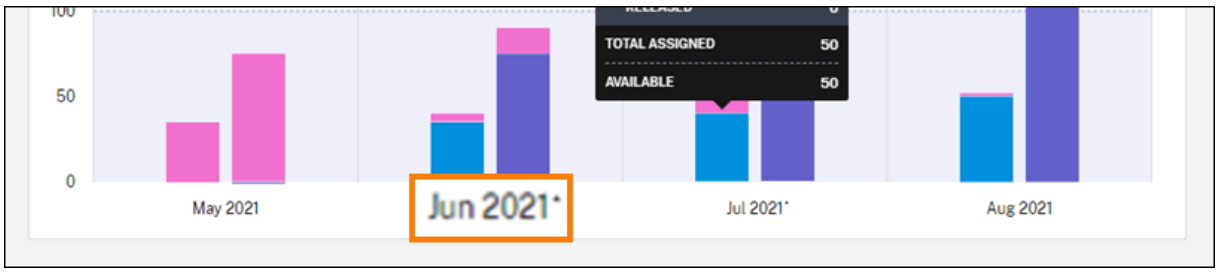


在 许可证分配 图表上，指向特定月份或日期的条形会显示以下信息：

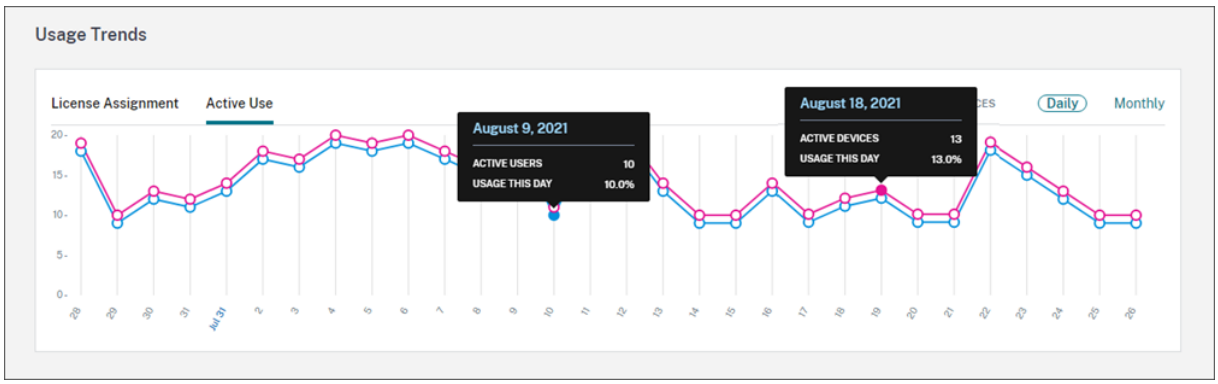
- 许可证总数：您在所有授权中为云服务购买的许可证总数。
- 分配的用户：截至当月分配给用户的许可证的累计数量。
- 分配的设备：截至当月分配给设备的许可证累计数量。如果这个数字在给定月份看起来特别高，这可能是应用程序或桌面通过网络浏览器启动的结果。要降低此数字，Citrix 建议使用本地安装的 Workspace 应用程序。
- 新分配的：每月分配的新许可证的数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。
- 已发布：每月发布的符合条件的许可证数量。例如，如果 20 个许可证有资格发布，而您在 7 月发布了其中 10 个，则显示的 7 月份已发布许可证数量为 10。

启用域截断的时间间隔用星号标记。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



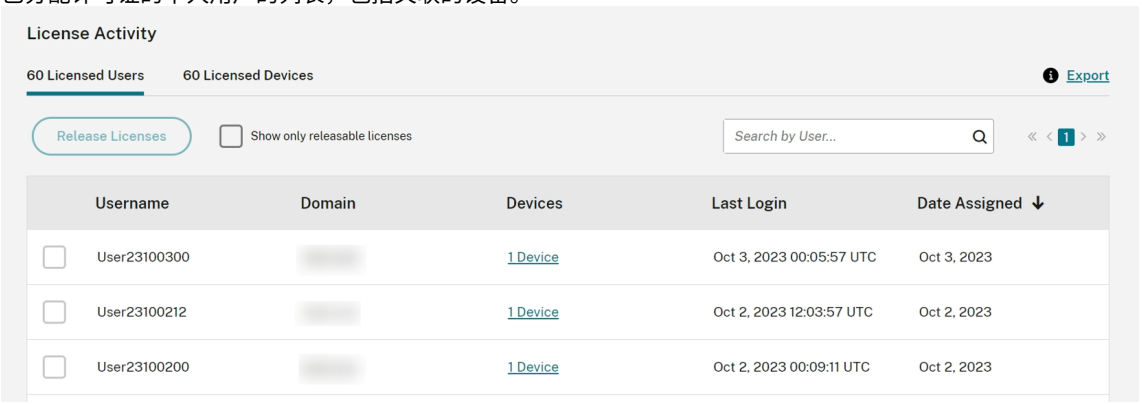
在活跃使用图表上，您可以分别查看上一个日历月和日历年的活跃用户和设备。指向图表上的特定间隔可显示活跃用户或设备的数量以及使用百分比。



许可证活动

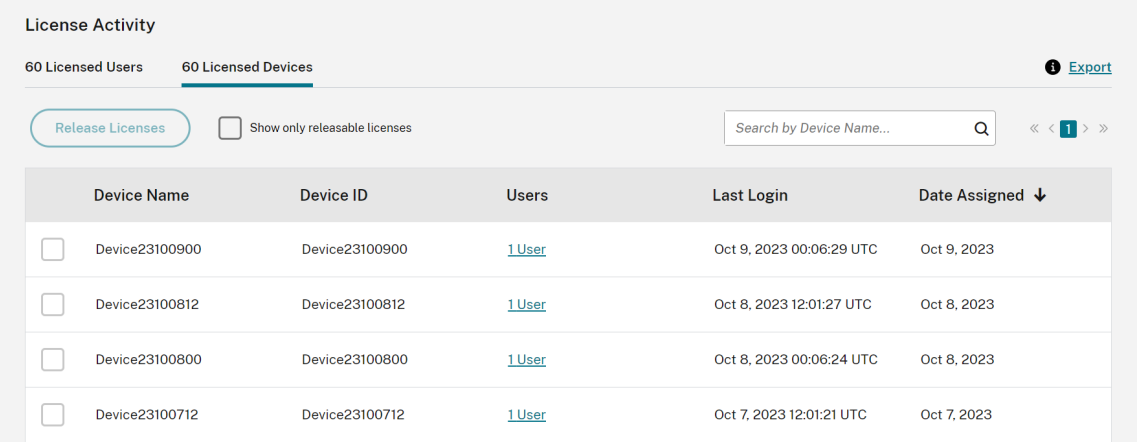
许可证活动部分显示以下信息：

- 已分配许可证的个人用户的列表，包括关联的设备。



- 已分配许可证的设备列表，包括关联用户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 向用户或设备分配许可证的日期。

您还可以筛选列表以仅显示符合发放条件的许可证。请参阅 本文中的释放分配的许可证 。

发放分配的许可证

分配许可证后，分配期限为 90 天，并建立与服务的连接。如果用户或设备已有 90 天没有启动应用程序或桌面，则这些许可证将被视为未使用的许可证，并在 90 天后由 Citrix Cloud 发放。此过程是自动化的，管理员无需执行任何操作。

分配期限（90 天）过后，仅允许管理员在以下情况下手动发放许可证：

- 该用户不再与公司相关联。
- 该用户的休假时间已延长。

只有当设备停止使用时，管理员才能发放设备的许可证。

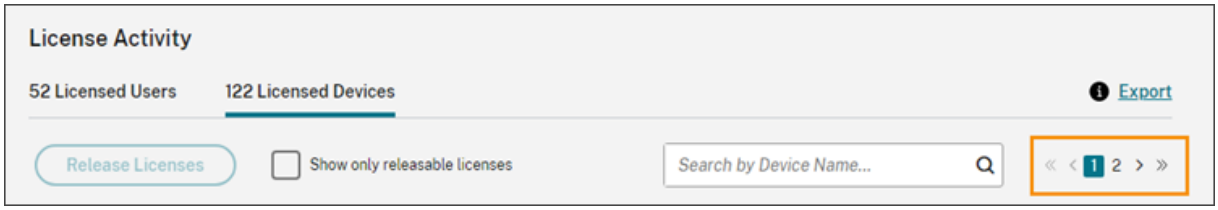
> 注意：
>
> - 建议遵循发放许可证的自动流程。但是，如果除上述原因外，管理员打算在 90 天期限之前发放许可证，这可能会违反 Citrix EULA。在执行此操作之前，请联系 Citrix。
> - 管理员可以通过用户界面手动发放单个许可证。或者，管理员可以选择使用云许可 API 发放许可证。有关详细信息，请参阅用于管理 Citrix Cloud 许可的 API。

查找可发布的许可证

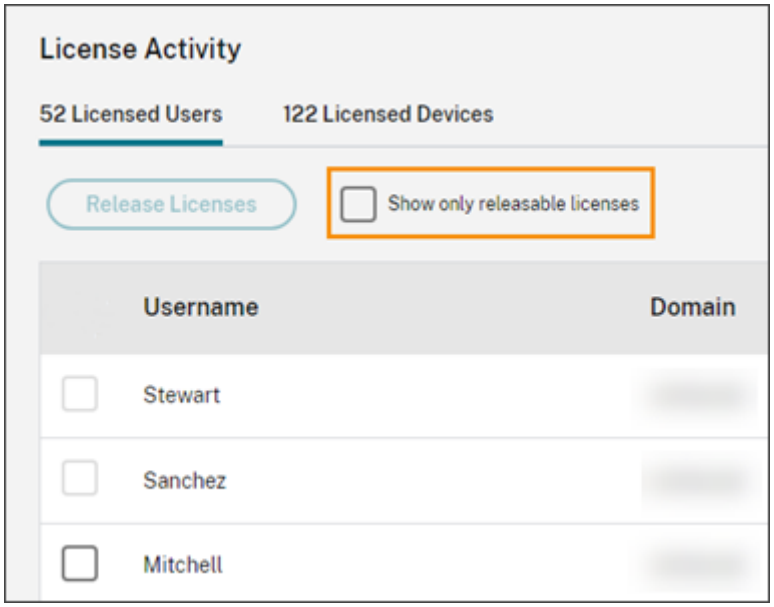
如果用户或设备已经 30 天没有启动应用程序或桌面，Citrix Cloud 会将许可证置于可发放状态。可发放的许可证显示在“许可使用的用户”或“许可使用的设备”列表中，带有深灰色复选框，可以将其选中。不可发放的许可证会显示一个浅灰色的复选框，表示无法选择该许可证。

出现在“许可证活动”部分的列表一次最多显示 100 个已分配的许可证。如果您拥有 100 个以上的许可证，请使用页面控件在列表中移动。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要快速找到可发布的许可证，请单击发放许可证按钮旁边的仅显示可发放的许可证。此操作隐藏了尚未允许发布的已分配许可证。



选择可发布的许可证

选中每个许可证旁边的深灰色复选框以选择要发放的许可证。当您从列表中选择许可证时，“发布许可证”按钮将变为活动状态。

您可以逐一选择所有可发放的许可证，然后单击发放许可证。

释放分配的许可证

1. 在许可证活动下，单击许可使用的用户或许可使用的设备选项卡。
2. 如果需要，请单击显示可发放的许可证以仅显示拥有允许发放的许可证的用户。
3. 选择要管理的用户或设备，然后单击发放许可证。
4. 查看您选择的用户或设备，然后单击发放许可证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

监视 **Citrix DaaS**（并发用户）的许可证和峰值使用情况

October 5, 2023

本文仅介绍管理 **Citrix DaaS** 的并发用户许可证的经验。

有关 Citrix DaaS 的用户/设备许可的信息，请参阅监视 Citrix DaaS（用户/设备）的许可证和活跃使用情况。

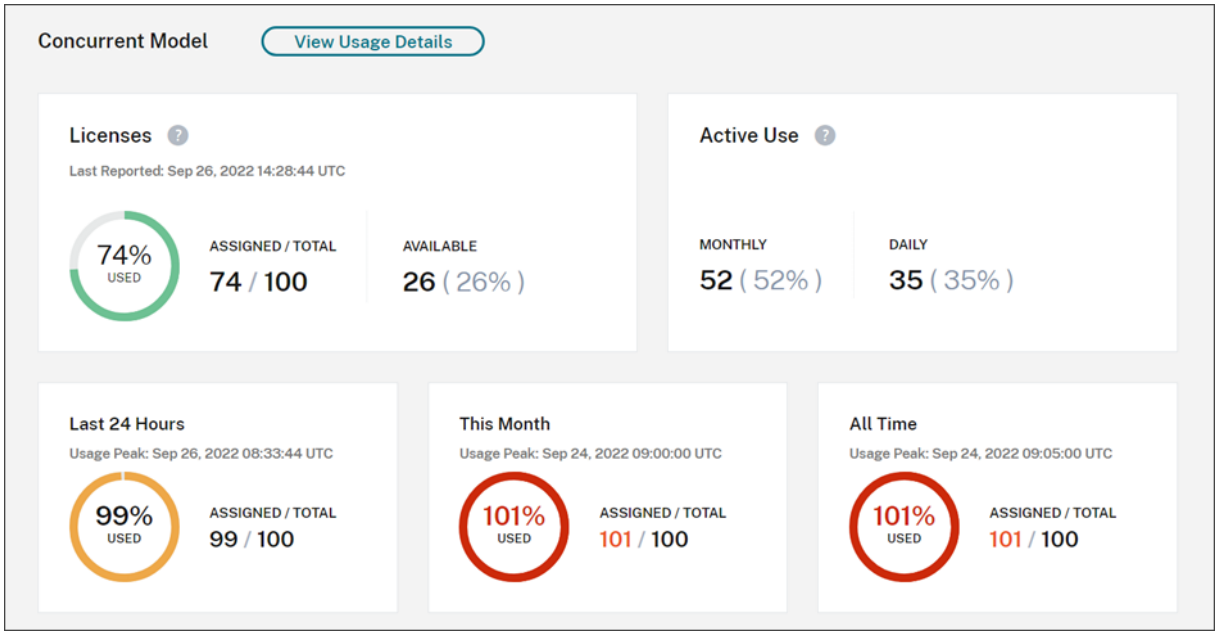
有关 Citrix DaaS Standard for Azure 的用户/设备和并发用户许可的信息，请参阅监视 Citrix DaaS Standard for Azure 的许可证和使用情况。

许可证分配

当用户在其设备上启动应用程序或桌面时，Citrix Cloud 会分配许可证。当用户注销或断开会话连接时，将不再分配许可证。由于许可证分配可能会根据在任何给定时间访问应用程序或桌面的设备数量而变化，因此 Citrix Cloud 每五分钟评估一次正在使用的许可证数量。

有关并发用户许可模式的更多信息，请参阅“许可使用产品”文档中的并发许可证。

许可摘要



许可摘要提供了以下信息的概览视图：

- Citrix Cloud 上次评估正在使用的许可证时，当前正在使用的已购买许可证总数的百分比。Citrix Cloud 根据与服务有活动连接的唯一设备每五分钟计算一次此百分比。购买的许可证总数是为使用并发用户许可模式的 Citrix DaaS 版本购买的许可证总数。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 当前分配的许可证与已购买许可证总数的比率以及剩余的可用许可证数量。该比率中显示的总数数字代表当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计。在计算使用中的峰值许可证时，Citrix Cloud 将检索在以下时间段内使用的最大许可证数：
  - 过去 **24** 小时：过去 24 个时段内一次使用的最大许可证数。
  - 本月：自当前日历月开始以来一次使用的许可证的最大数量。
  - 所有时间：自订阅开始以来一次使用的最大许可证数。

  这些使用高峰时段显示的总数表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且分配的许可证相应增加，则 总 数将发生变化，以反映该时间点新的拥有许可证数量。但是，如果没有相应的使用峰值，则总数 不会改变。
- 活跃使用情况统计。Citrix Cloud 显示以下时段内唯一连接的总数：
  - 每月：上一个日历月的连接总数。
  - 每天：过去 24 小时的连接总数。

    这些数字也以这些时期拥有的许可证总数的百分比表示。

计算使用中的峰值许可证

为了准确反映并发用户许可模式，Citrix Cloud 每五分钟计算一次同时访问该服务的唯一设备数量。如果计数大于显示的当前峰值使用率，Citrix Cloud 将显示新的峰值使用情况以及达到该峰值的日期和时间。如果计数小于当前峰值使用量，则当前峰值使用量不会改变。

> 重要：
>
> 如果您使用 Director 中的 Monitor 获取有关并发会话的信息，请注意，监视报告对并发会话的解释不同，并且不能准确反映正在使用的并发用户许可证的数量。有关监视报表和许可报告之间区别的更多信息，请参阅 常见问题解答。

计算每月活跃使用量

每个月初，Citrix Cloud 都会拍摄上一个日历月的快照。Citrix Cloud 显示该日历月内发生的唯一连接总数。

计算每日活跃使用量

每天的同一时间，Citrix Cloud 都会拍摄过去 24 小时的快照。Citrix Cloud 显示在该 24 小时内发生的唯一连接总数。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用趋势和许可证活动

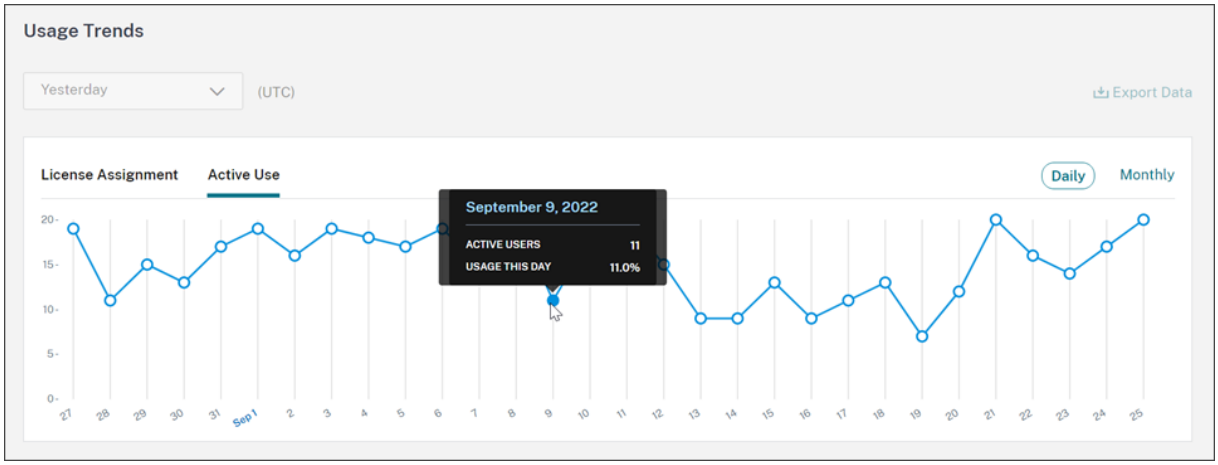
要查看许可证的历史视图，请单击 查看使用详情。

“使用趋势”部分向您显示以下信息：

- 许可证分配 显示包含以下信息的图表：
  - 许可证总数：您购买的并发用户许可证总数。
  - 使用中的峰值许可证：为您选择的日期范围分配的最大许可证数。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要向下钻取到每月或每小时的高峰使用量，请从下拉菜单中选择要查看的日历月或日。

  如果您选择的日期范围尚未完成，Citrix Cloud 将显示最新时间间隔的当前峰值使用情况。例如，如果您向下钻取以查看仍在进行中的日历日，则会显示截至当前时刻每小时的最大许可证数量。如果许可证的最大数量在接下来的五分钟计数间隔内增加，Citrix Cloud 将更新当前小时的峰值使用情况。
- 活跃使用显示包含以下信息的图表：
  - 每天：过去 30 天内每天的连接总数。
  - 每月：上一个日历年中每个月的连接总数。

指向“许可证分配”或“活跃使用”图表上的间隔即可显示该间隔的详细信息。



发放许可证

当用户注销或断开会话连接时，会自动发放并发用户许可证。您无需手动发放这些许可证。

监视 **Citrix DaaS Standard for Azure** 的许可证和使用情况

November 8, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本文介绍了管理用户/设备和并发用户许可模式的许可证分配的经验。

Citrix Azure 消费基金（仅限用户/设备）

如果您购买了 Citrix Azure 消费基金用于服务部署，请参阅监视面向 Citrix DaaS 的 Citrix 托管 Azure 资源消耗情况，以了解有关 Citrix 托管的资源消耗报告的更多信息。

许可证分配

用户/设备许可模式：当唯一用户或唯一设备首次启动桌面时，Citrix Cloud 会分配许可证。

并发用户许可模式：当用户在其设备上启动桌面时，Citrix Cloud 会分配许可证。当用户注销或断开会话连接时，将不再分配许可证。由于许可证分配可能会根据在任何给定时间访问桌面的设备数量而变化，因此 Citrix Cloud 每五分钟评估一次正在使用的许可证数量。

有关并发许可模式的更多信息，请参阅“许可使用产品”文档中的并发许可证。

计算使用中的峰值许可证

为了准确反映并发许可模式，Citrix Cloud 每五分钟计算一次同时访问该服务的唯一设备数量。如果计数大于显示的当前峰值使用率，Citrix Cloud 将显示新的峰值使用情况以及达到该峰值的日期和时间。如果计数小于当前峰值使用量，则当前峰值使用量不会改变。

域名截断

仅用户/设备许可模式支持此功能。

如果您托管多个域并且用户在这些域中拥有相似的帐户（例如，johnsmith@company.com 和 johnsmith@mycompany.com），则可以允许 Citrix Cloud 忽略该帐户域，只考虑该帐户的用户名（例如 johnsmith）。此过程称为域名截断。默认情况下，域名截断处于禁用状态。

启用域名截断后，Citrix Cloud 对唯一用户的计算会发生变化。Citrix Cloud 没有将 johnsmith@company.com 和 johnsmith@mycompany.com 视为两个唯一用户，而只将 johnsmith 视为唯一用户。此计算更改会影响以下许可数据：

- 许可证分配
- 积极使用
- 一段时间内的许可证使用趋势
- 有资格发布的许可证

当您从许可控制台将数据导出到 CSV 文件时，许可数据的这些更改也会反映出来。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

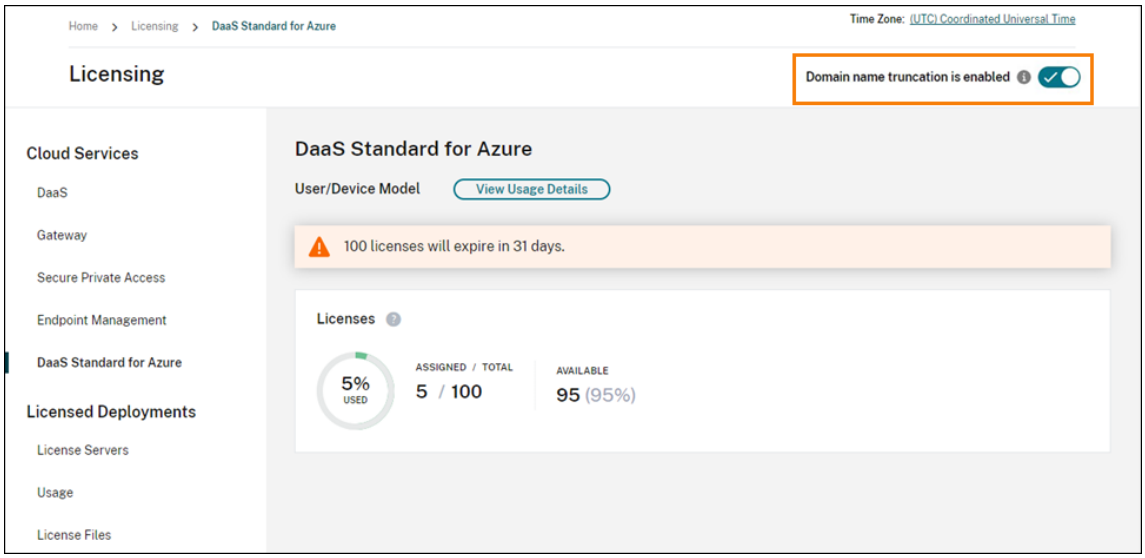
> 注意：
>
> 如果您托管多个具有相似帐户的域名，但用户名略有不同（例如，单个用户拥有帐户 johnsmith@company.com 和 jsmith@newcompany.com），则域名截断对 Citrix Cloud 的计算没有影响。Citrix Cloud 仍然将 johnsmith 和 jsmith 视为唯一用户，即使他们属于同一个人。

启用或禁用域名截断

默认情况下，域名截断处于禁用状态。从您启用或禁用该功能的那一刻起，域名截断就会影响您的用户/设备使用数据。例如，如果您在给定月份启用域名截断，Citrix Cloud 在该月记录的数据就会受到影响。但是，禁用该功能的前几个月的历史数据仍不受影响。同样，如果您在给定月份禁用域名截断，Citrix Cloud 在该月记录的数据也会受到影响。但是，启用该功能的月份的历史数据保持不变。

要启用或禁用域名截断，请执行以下操作：

1. 点击许可控制台右上角附近的切换开关。



2. 当系统提示您确认您的操作时，选择“是，我明白”。

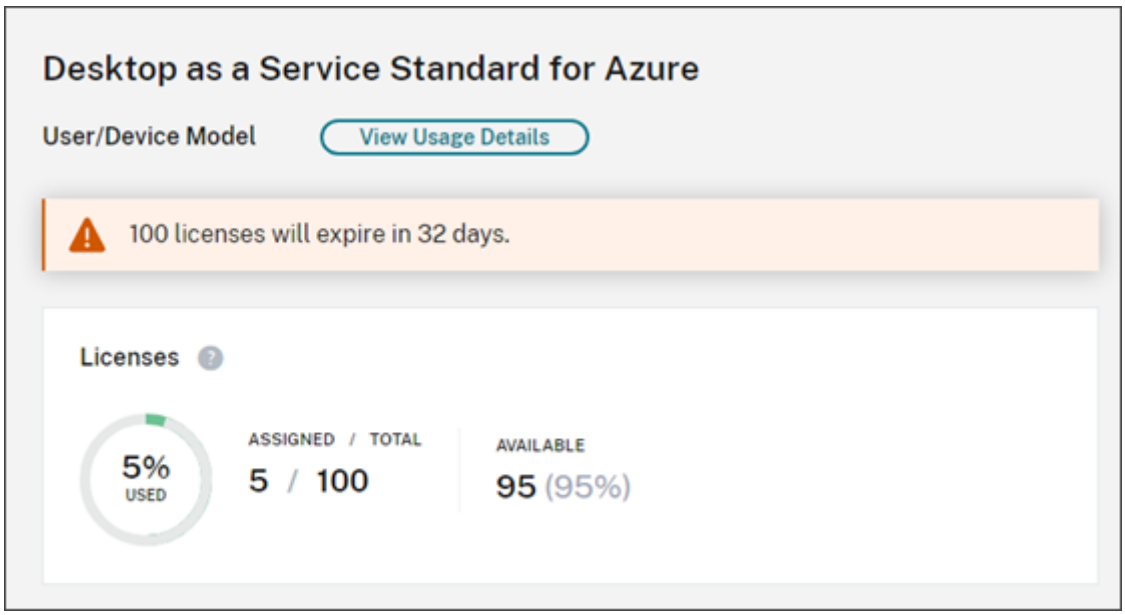
许可摘要

Citrix Cloud 显示用户/设备和并发用户许可模式下正在使用的许可证的摘要视图。

用户和设备摘要

对于用户/设备型号，许可摘要显示正在使用的许可证与您拥有的许可证总数的关系。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

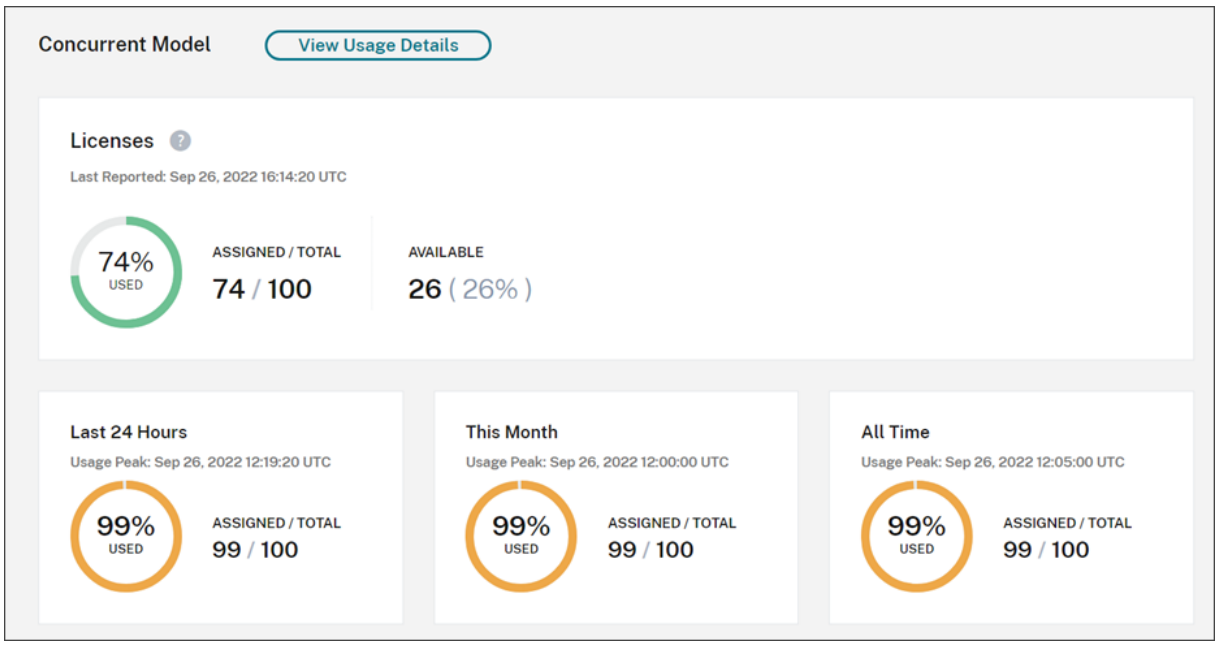


当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。

Citrix Cloud 还显示分配的许可证与购买的许可证的比率以及剩余的可用许可证数量。

并发用户摘要

对于并发模式，许可摘要提供了以下信息的一目了然的视图：



- Citrix Cloud 上次评估正在使用的许可证时，当前正在使用的已购买许可证总数的百分比。Citrix Cloud 根据与服务有活动连接的唯一设备每五分钟计算一次此百分比。购买的许可证总数是为使用并发许可模式的 Citrix DaaS Standard for Azure 购买的许可证的总和。

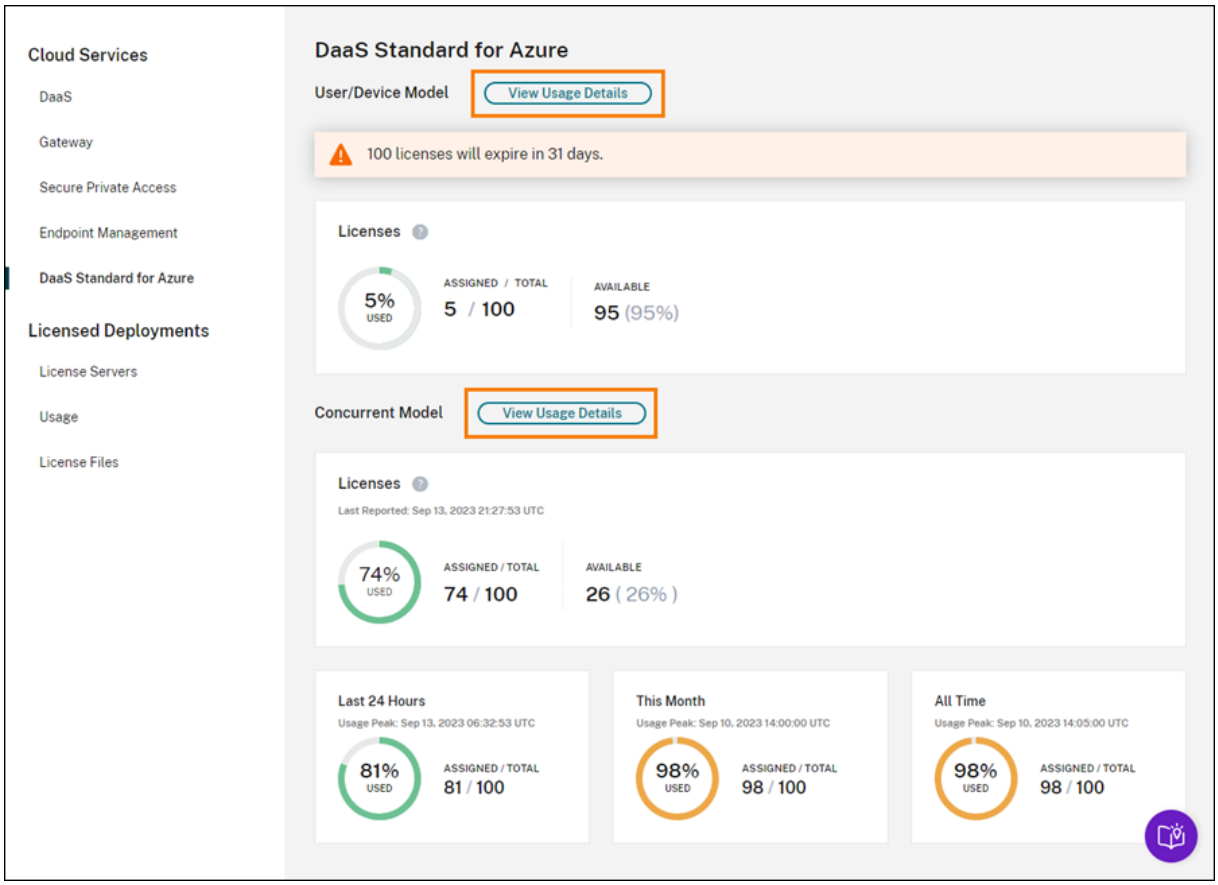
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 当前分配的许可证与已购买许可证总数的比率以及剩余的可用许可证数量。该比率中显示的总数数字代表当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计。在计算使用中的峰值许可证时，Citrix Cloud 将检索在以下时间段内使用的最大许可证数：
  - 过去 **24** 小时：过去 24 个时段内一次使用的最大许可证数。
  - 本月：自当前日历月开始以来一次使用的许可证的最大数量。
  - 所有时间：自订阅开始以来一次使用的最大许可证数。

  这些使用高峰时段显示的总数表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且分配的许可证相应增加，则 总 数将发生变化，以反映该时间点新的拥有许可证数量。但是，如果没有相应的使用峰值，则总数 不会改变。

使用趋势

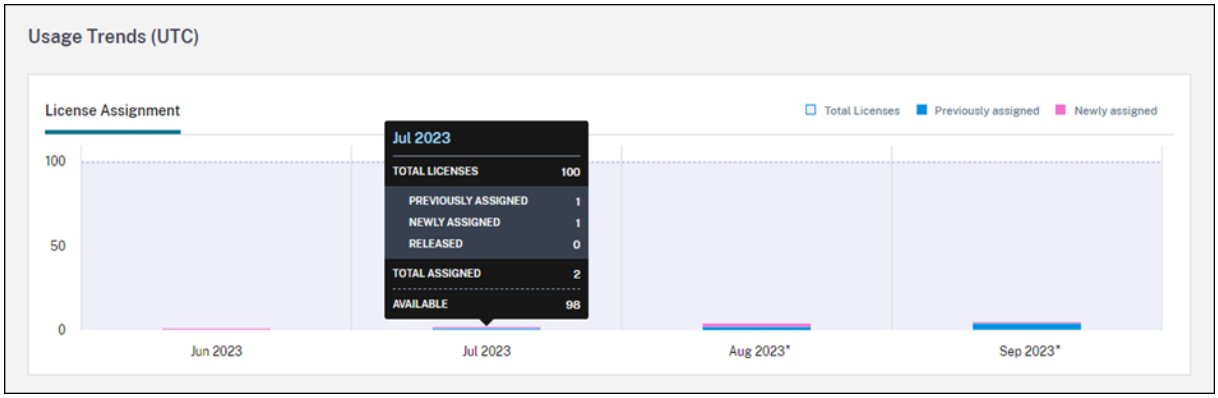
Citrix Cloud 显示用户/设备许可证或并发用户许可证的使用趋势明细。要查看此细目，请从许可摘要页面中选择查看使用情况详细信息。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用户和设备的趋势

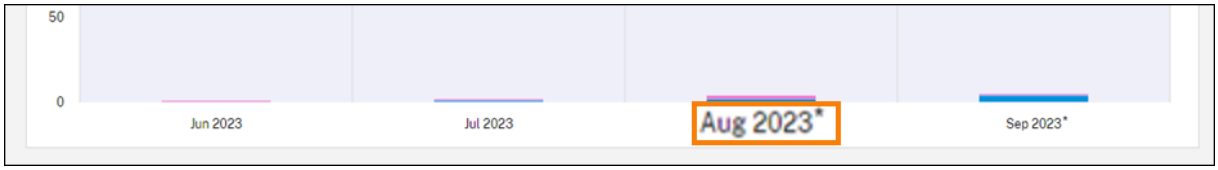
对于用户/设备许可证，“使用趋势”部分以图表形式向您显示已分配许可证的明细。



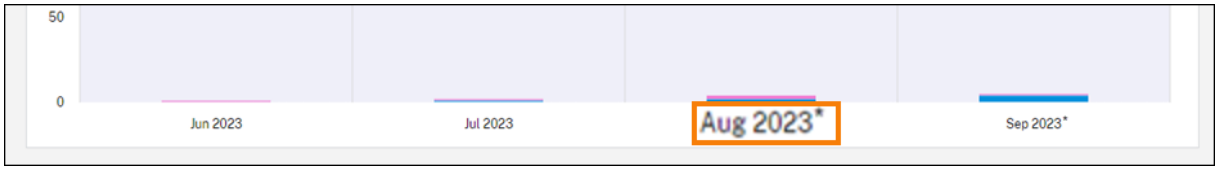
指向图表上的时间间隔会显示以下信息：

- 许可证总数：您在所有授权中为云服务购买的许可证总数。
- 以前分配的许可证数量：上个月分配的许可证数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。在 8 月份，此许可证被视为“先前已分配”。
- 新分配的：每月分配的新许可证的数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。

启用域截断的时间间隔用星号标记。



启用域截断的时间间隔用星号标记。



并发用户的趋势

对于并发用户许可证，“使用趋势”部分向您显示以下信息：

- 许可证总数：您购买的并发许可证总数。
- 使用中的峰值许可证：为您选择的日期范围分配的最大许可证数。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要向下钻取到每月或每小时的高峰使用量，请从下拉菜单中选择要查看的日历月或日。

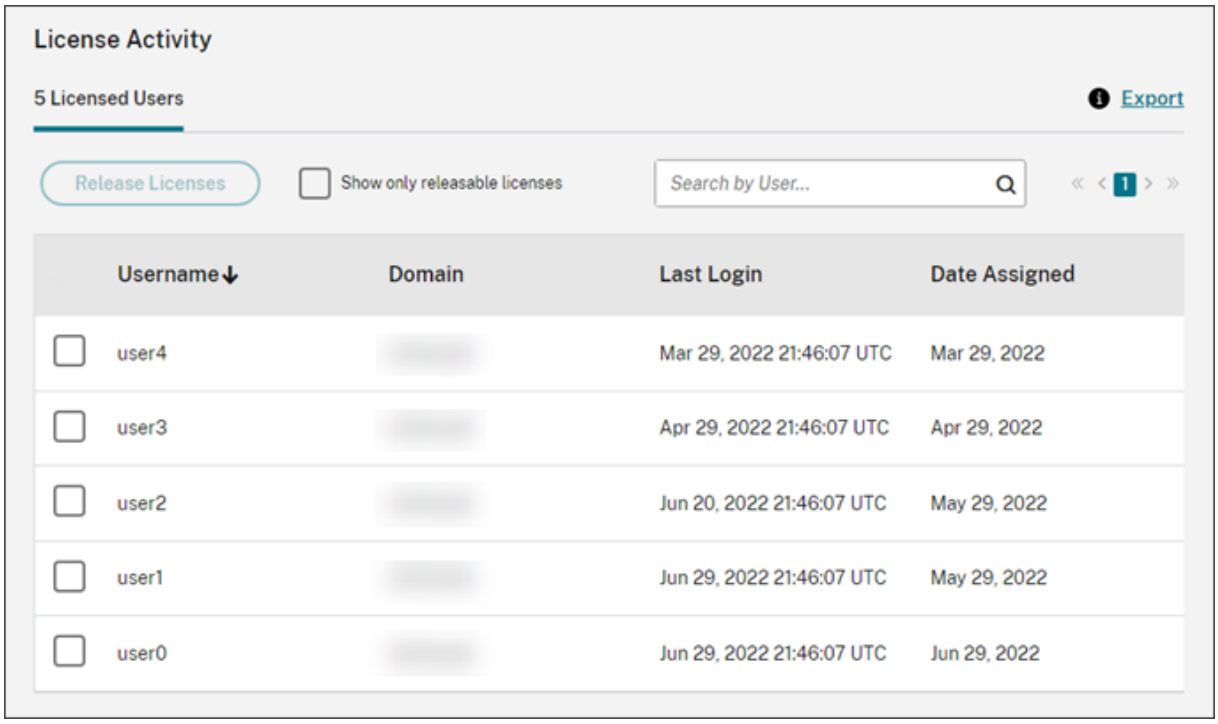
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您选择的日期范围尚未完成，Citrix Cloud 将显示最新时间间隔的当前峰值使用情况。例如，如果您向下钻取以查看仍在进行中的日历日，则会显示截至当前时刻每小时的最大许可证数量。如果许可证的最大数量在接下来的五分钟计数间隔内增加，Citrix Cloud 将更新当前小时的峰值使用情况。

指向图表上的时间间隔即可显示该时间间隔内使用的许可证总数和许可证峰值。

用户和设备的许可活动

对于用户/设备许可证，“许可证活动”部分显示已分配许可证的个人用户列表以及向用户分配许可证的日期。此部分不适用于并发许可证。



您还可以筛选列表以仅显示符合发放条件的许可证。请参阅本文中的“发放分配的许可证”。

发放用户/设备许可证

发放符合条件的用户/设备许可证因服务订阅类型而异。

- 年度服务订阅：如果您有按年订阅，则可以为过去 30 天内未启动应用程序或桌面的用户发放许可证。您可以批量或单独发放多个许可证。
- 月度服务订阅：如果您有月度订阅，则可以在每个月的第一天发放许可证，而不考虑闲置期限。

分配许可证后，分配期限为 90 天，并建立与服务的连接。如果用户或设备已有 90 天没有启动应用程序或桌面，则这些许可证将被视为未使用的许可证，并在 90 天后由 Citrix Cloud 发放。此过程是自动化的，管理员无需执行任何操作。

分配期限（90 天）过后，仅允许管理员在以下情况下手动发放许可证：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 该用户不再与公司相关联。
- 该用户的休假时间已延长。

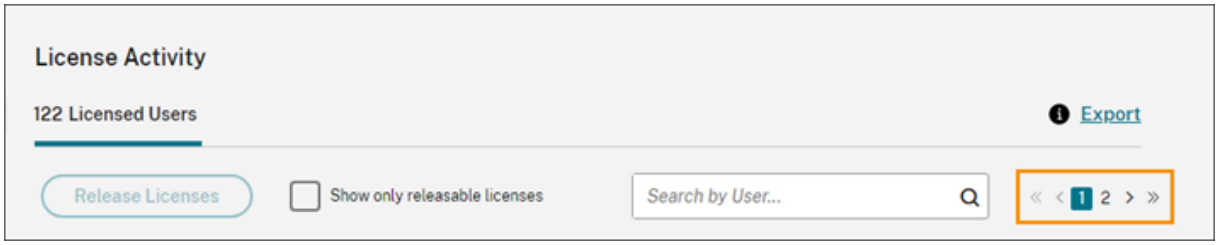
只有当设备停止使用时，管理员才能发放设备的许可证。

> 注意：
>
> - 建议遵循发放许可证的自动流程。但是，如果除上述原因外，管理员打算在 90 天期限之前发放许可证，这可能会违反 Citrix EULA。在执行此操作之前，请联系 Citrix。
> - 管理员可以通过用户界面手动发放单个许可证。或者，管理员可以选择使用云许可 API 发放许可证。有关详细信息，请参阅用于管理 Citrix Cloud 许可的 API。

查找符合条件的许可证

如果用户或设备已经 30 天没有启动应用程序或桌面，Citrix Cloud 会将许可证置于可发放状态。可发放的许可证显示在“许可使用的用户”或“许可使用的设备”列表中，带有深灰色复选框，可以将其选中。不可发放的许可证会显示一个浅灰色的复选框，表示无法选择该许可证。

出现在“许可证活动”部分的列表一次最多显示 100 个已分配的许可证。如果您拥有 100 个以上的许可证，请使用页面控件在列表中移动。



要快速找到符合条件的许可证，请选择发放许可证按钮旁边的仅显示可发放的许可证。此操作会隐藏尚未符合发放条件的已分配许可证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

选择符合条件的许可证

选中每个许可证旁边的深灰色复选框以选择要发放的许可证。当您选择许可证时，“发放许可证”按钮将变为活动状态。

您可以逐一选择所有可发放的许可证，然后单击发放许可证。

发放分配的许可证

1. 如果需要，请单击显示可发放的许可证以仅显示拥有允许发放的许可证的用户。
2. 选择要管理的用户，然后单击发放许可证。
3. 查看您选择的用户，然后单击发送许可证。

发放并发用户许可证

当用户注销或断开会话连接时，会自动发放并发用户许可证。您无需手动发放这些许可证。

监视 **Endpoint Management** 的许可证和活动使用情况

November 30, 2023

许可证分配

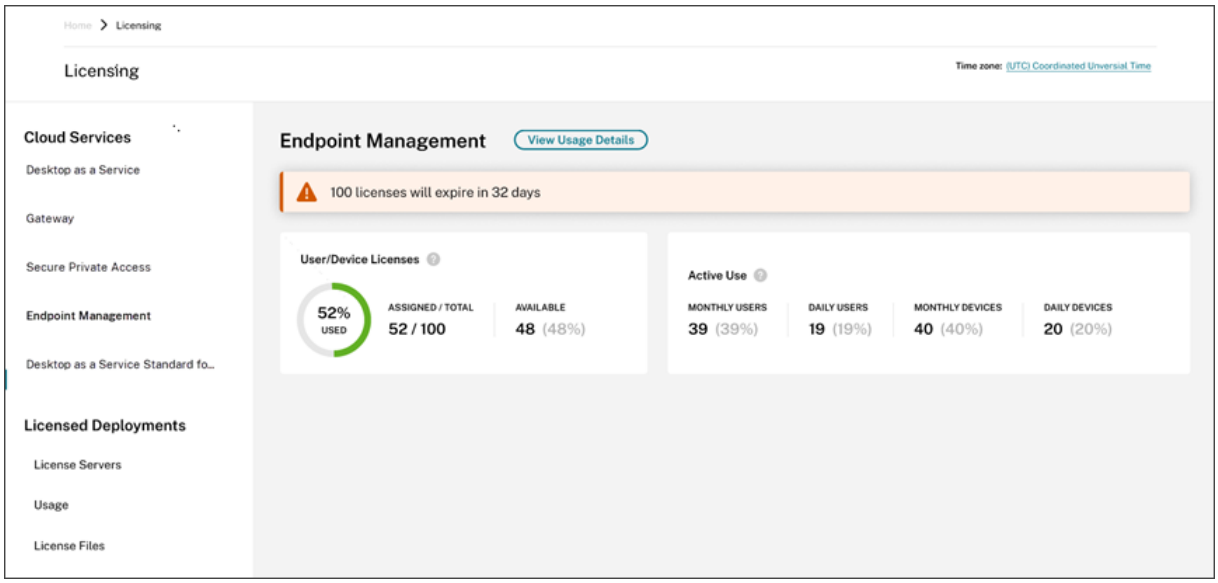
通常，用户在首次使用云服务时会获得许可。对于 Endpoint Management，用户注册设备时会分配许可证。注册设备后，设备会定期通过 Citrix Cloud 签入。然后，Citrix Cloud 使用此“签到脉冲”来计算每月使用量，并帮助管理员随时了解用户最近的服务使用情况。

首次使用发生在用户首次注册设备或设备首次出现“签到脉冲”时。

许可证是按用户分配的。因此，如果两个用户注册并使用同一设备，则会分配两个许可证。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

许可摘要和详细信息

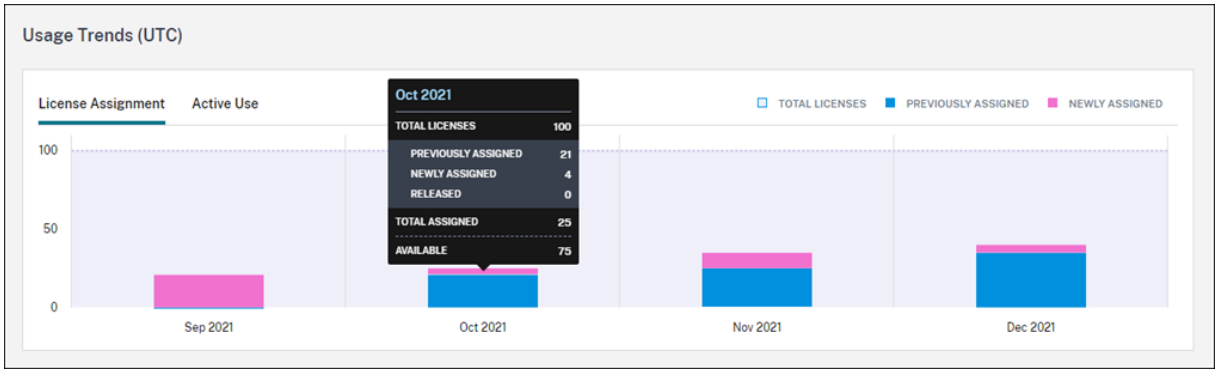


许可摘要提供了每项受支持服务的以下信息的概览：

- 分配的已购买许可证总数的百分比。当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。
- 分配的许可证与已购买的许可证的比率以及剩余的可用许可证数量。
- 每月和每天的活跃使用情况统计信息：
  - 每月活跃使用量是指在过去 30 天内使用过该服务的唯一身份用户的数量。
  - 每日活跃使用量是指在过去 24 小时内使用过该服务的唯一身份用户的数量。
- 云服务订阅到期之前的剩余时间。如果订阅在接下来的 90 天内到期，则会显示一条警告消息。

使用趋势

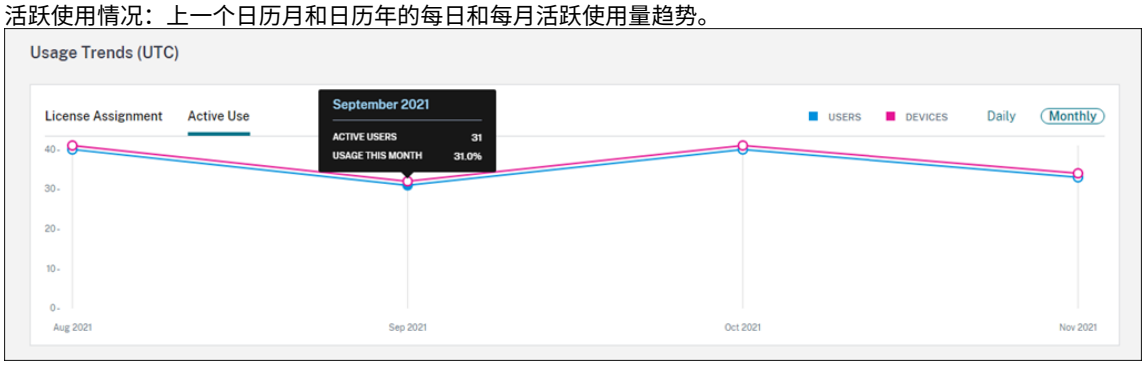
要查看许可证的详细视图，请单击 查看使用详情。然后，您可以查看使用趋势以及正在使用云服务许可证的个人用户和设备的细分。



此细分显示以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

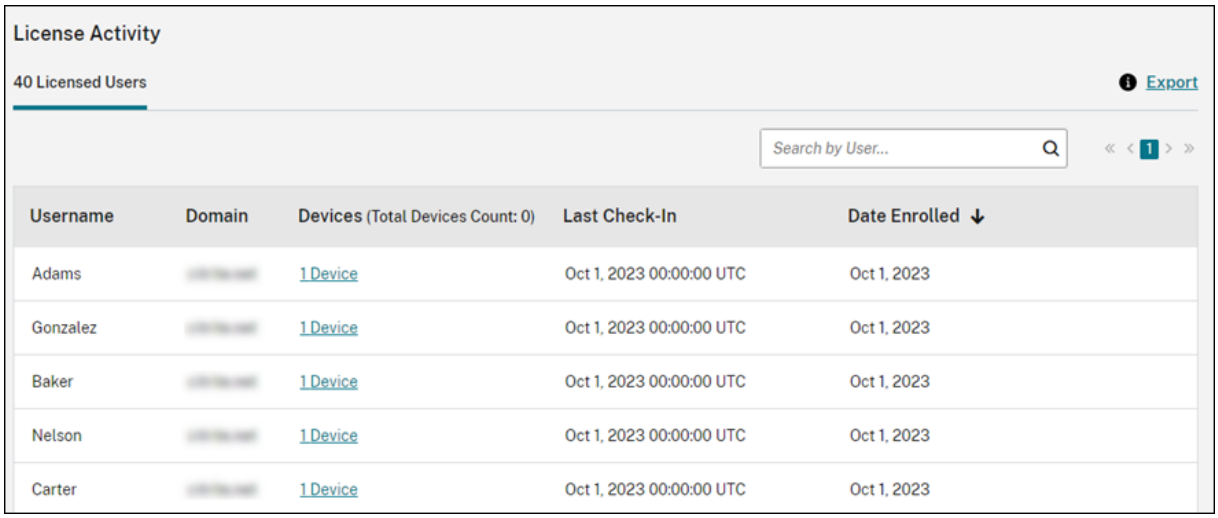
- 许可证总数：您在所有授权中为云服务购买的许可证总数。
- 之前已分配：每个月初已分配的云服务许可证。例如，如果在 7 月为用户分配了许可证，则该分配将计入 8 月的“先前分配的编号”中。
- 新分配的：每月分配的云服务许可证的数量。例如，在 7 月份首次访问云服务的用户将获得许可证。此许可证计入七月份的“新分配号码”中。
- 活跃使用情况：上一个日历月和日历年的每日和每月活跃使用量趋势。



许可证活动

“许可证活动”部分显示包含以下信息的列表：

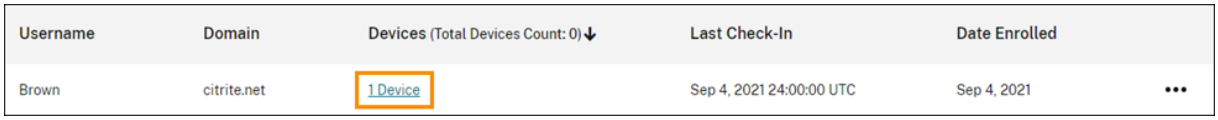
- 已分配许可证的个人消费者
- 分配许可证的日期
- 注册的设备数量和每位用户上次签到的日期



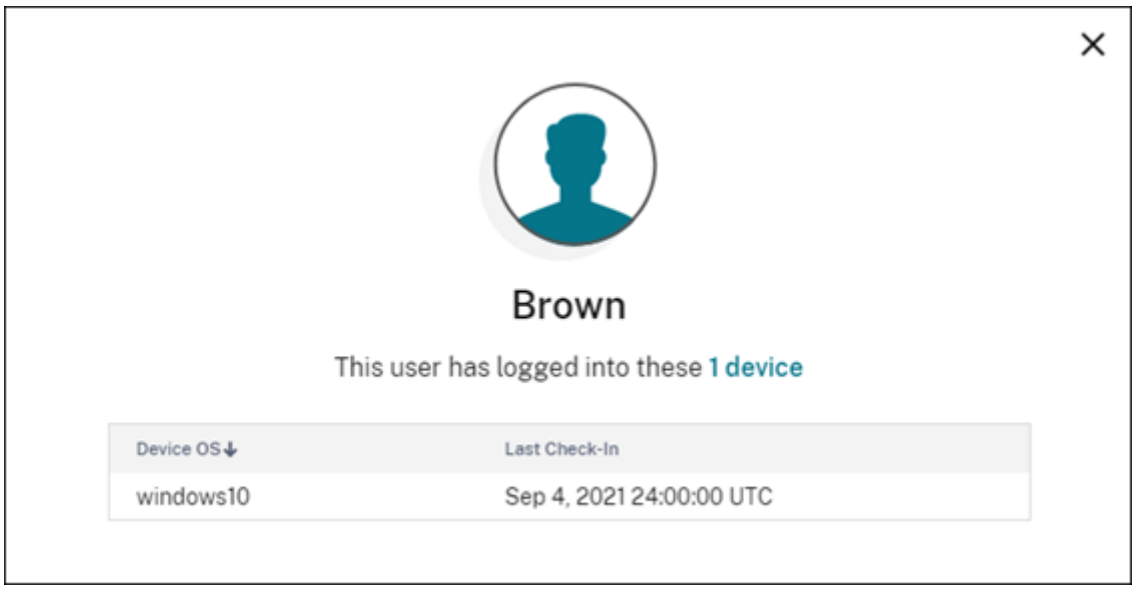
查看已注册的设备

要查看特定用户注册的设备数量，请单击“设备”列中的链接。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix Cloud 会显示用户已注册设备的列表以及每台设备上次签入的日期。



自动发放分配的许可证

Citrix Cloud 会自动向在过去 30 天内满足以下所有条件的用户发放许可证：

- 用户尚未注册新设备。
- 用户有一台尚未通过 Citrix Cloud 签入的现有设备。

无需采取其他措施即可发放符合条件的许可证。

发放符合条件的许可证后，用户可以通过注册设备获得另一个许可证。

监控网关服务的带宽使用情况

October 5, 2023

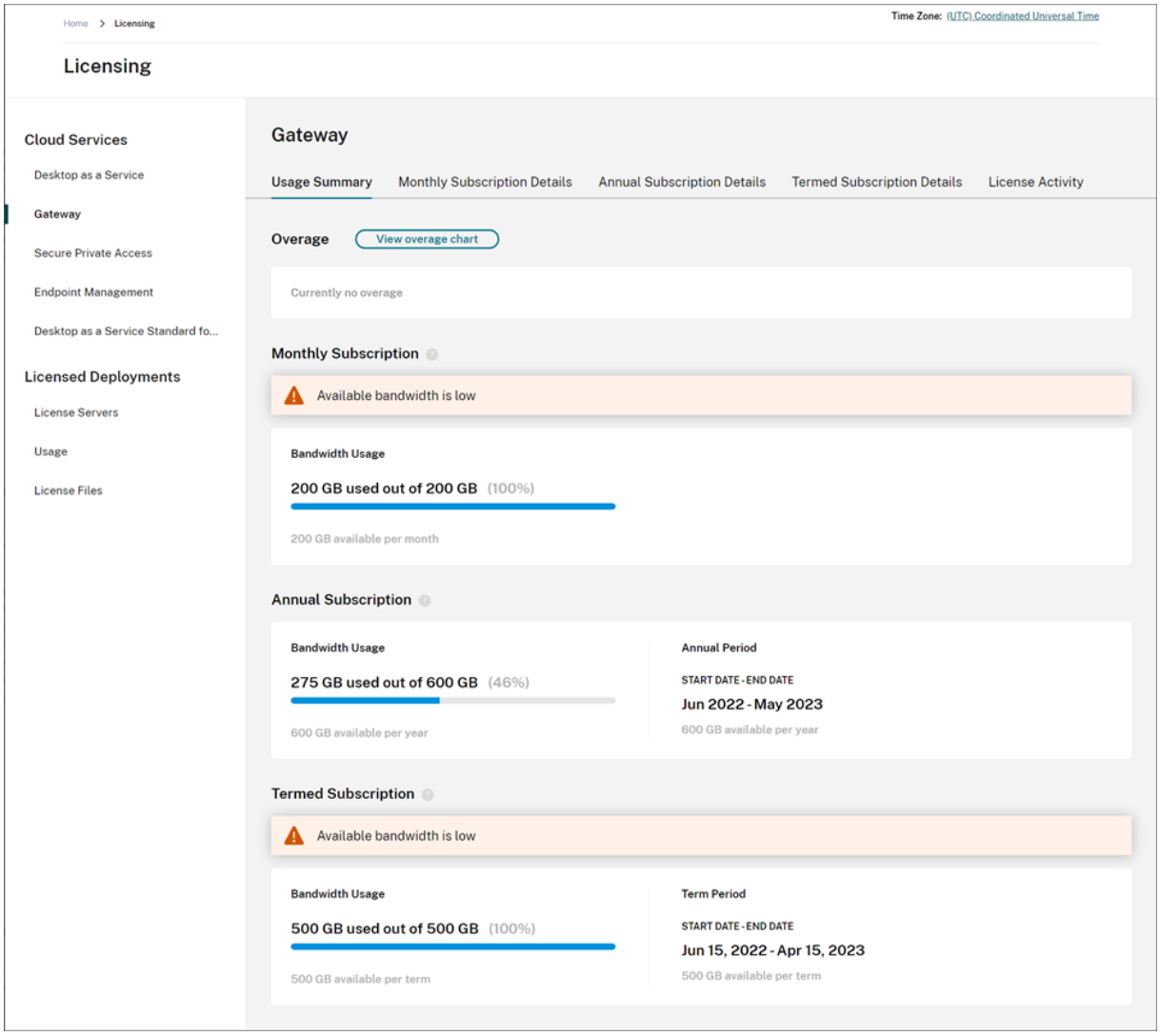
本文介绍了与 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 Citrix Workspace 一起使用时通过网关服务的带宽使用情况。Virtual Apps Essentials 服务中包含的网关服务的带宽消耗不会显示在 Citrix Cloud 管理控制台的许可页面上。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> Gateway 服务的许可可帮助您了解与使用虚拟应用程序和桌面相关的带宽使用情况。Citrix 不会在您的环境中强制分配带宽使用量。如果您过度使用带宽分配，Citrix 不会干扰生产工作负载或服务的运行。如果 Citrix 更改了网关服务和带宽使用策略的实施方式，Citrix 会在这些更改生效之前通知您。

用法摘要

使用情况摘要提供了每个网关服务订阅的带宽使用情况以及您的所有订阅（月度、年度和定期）的总超额概览。



Citrix Cloud 显示每种订阅类型的带宽总量和消耗的带宽量。

根据订阅类型，Citrix Cloud 还会显示订阅的计费周期：

- 每月订阅：Citrix Cloud 不显示当前计费周期。对于这些订阅，计费周期从每个月的第一天开始，到该月的最后一天结束。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 年度订阅：Citrix Cloud 显示计费周期的开始和结束日期。对于这些订阅，计费周期为一年。
- 定期订阅：Citrix Cloud 显示计费周期的开始和结束日期。对于这些订阅，计费周期是购买订阅的时间长度。例如，如果购买了为期三年的定期订阅，则计费周期的开始和结束日期对应于该三年时间间隔。

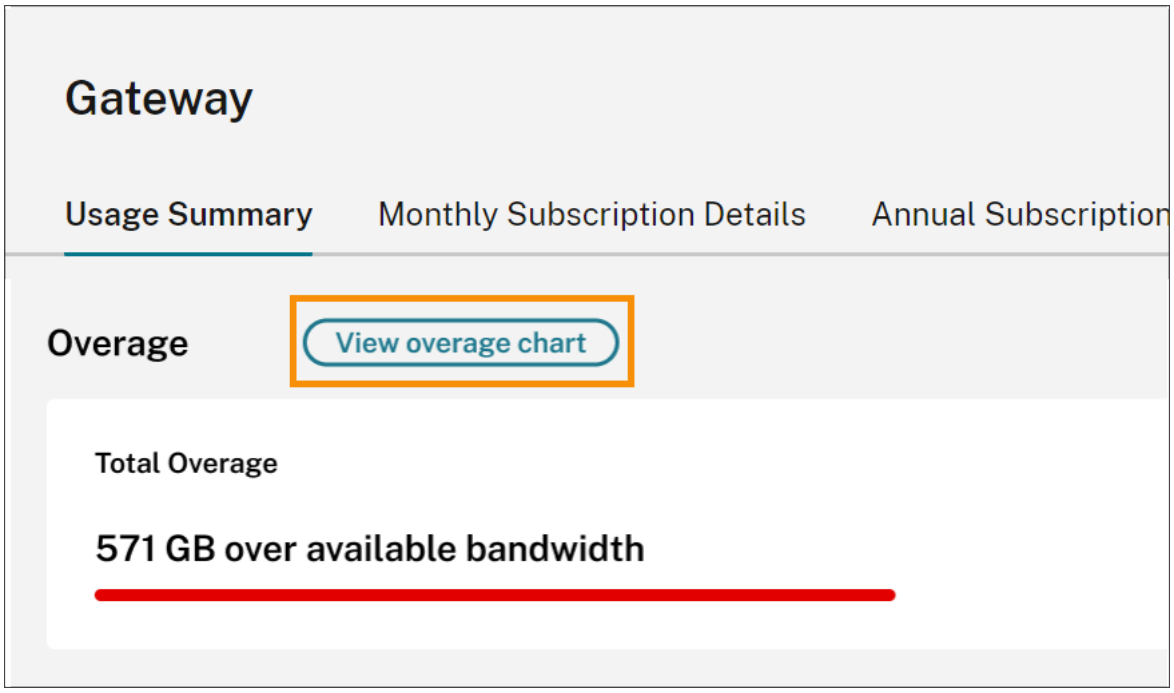
如果订阅在 90 天内过期，则会显示一条针对该订阅的警告消息。

超额

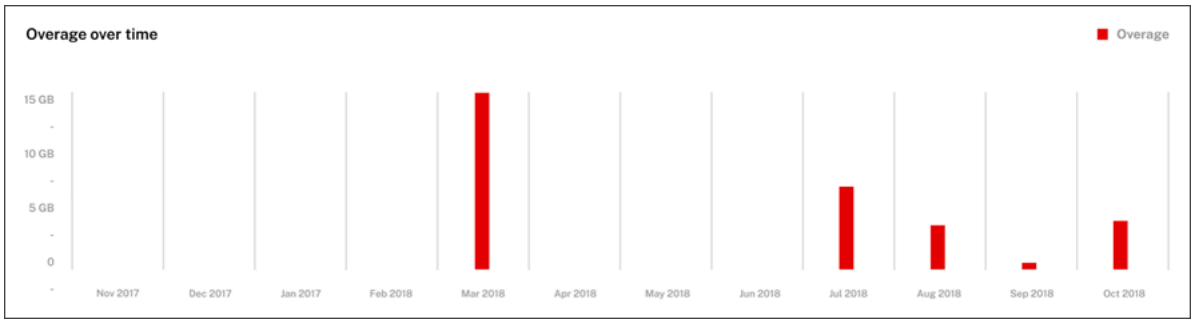
Citrix Cloud 每月计算所有订阅的超额。如果您消耗的带宽超过购买的带宽，Citrix Cloud 会将超额带宽显示为超额。

如果您有多个订阅，Citrix Cloud 会根据第一个具有最早结束日期的订阅来衡量您的带宽使用情况。如果您用尽了该订阅中的带宽配额，Citrix Cloud 会根据下一个最早的结束日期来衡量您的带宽使用情况。如果您用尽了所有订阅中的带宽配额，Citrix Cloud 会将超额使用量显示为超额。

“使用情况摘要”页面显示当月的总超额。要查看一段时间内的超额情况，请选择查看超额图表。



Citrix Cloud 显示过去 12 个月的总超额图表。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

当月的超额不会结转到下个月。下个月开始时，总超额将重置为零。

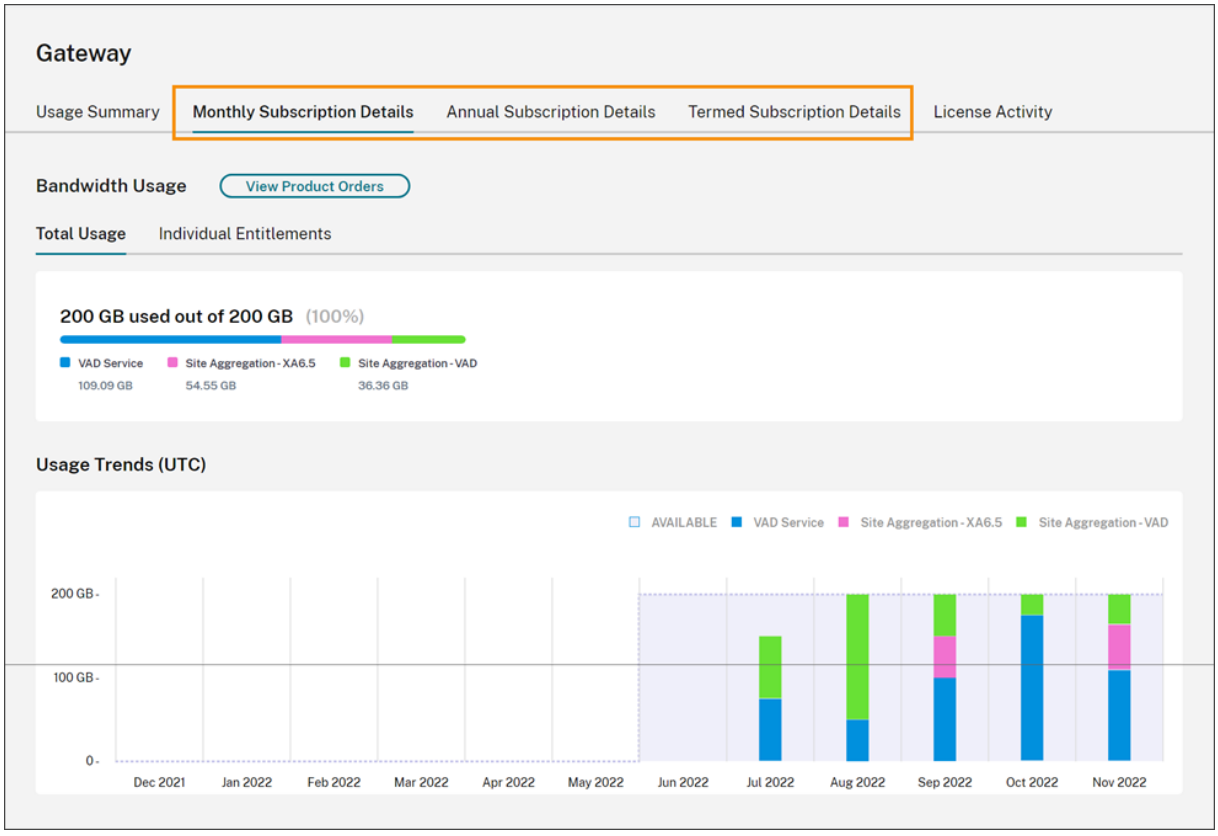
未使用的带宽

Citrix Cloud 会在下一个计费周期内自动重置订阅的带宽使用量。如果您在给定的订阅期内未使用全部带宽，Citrix Cloud 不会将任何未使用的带宽结转到下一个计费周期。

例如，如果您的月度订阅包含 150 GB 的总带宽，并且您在给定月份中使用了 100 GB 的带宽，Citrix Cloud 会将使用量重置为零，并在下个月初显示 150 GB 作为您的总带宽量。未使用的带宽不会添加到您的总带宽分配中。

使用情况详细信息

要详细查看您的订阅，请选择控制台顶部附近的月度、年度或定期订阅详细信息选项卡。



对于每种订阅类型，详细信息选项卡显示以下信息：

- 总使用量：从给定类型的所有订阅的可用总带宽中消耗的带宽量。对于月度订阅，将显示当月的总使用量。对于年度订阅和定期订阅，所有年度或定期订阅的总使用量是累积的。
- 个人权利：给定类型的每项订阅消耗的带宽总量。例如，如果您有多个年度订阅，则此选项卡将分别显示每个年度订阅的使用量明细。

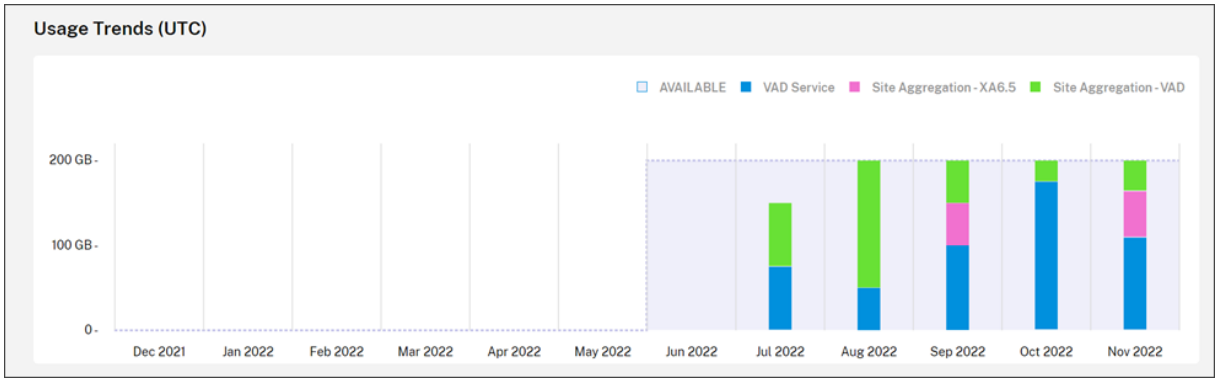
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

消耗的带宽量根据通过 Citrix DaaS（**VAD** 服务）或使用 Citrix Workspace 中的站点聚合通过本地 Virtual Apps and Desktops 部署进行的访问进行细分。

使用趋势

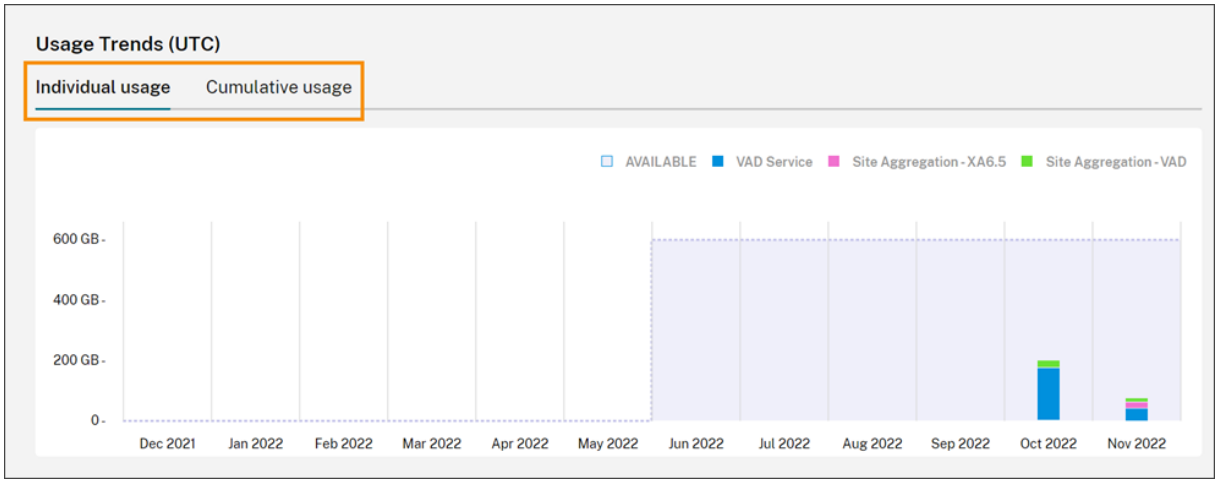
使用趋势部分显示了过去 12 个月的使用情况明细。

对于月度订阅，将显示使用该订阅的每个月的使用情况。



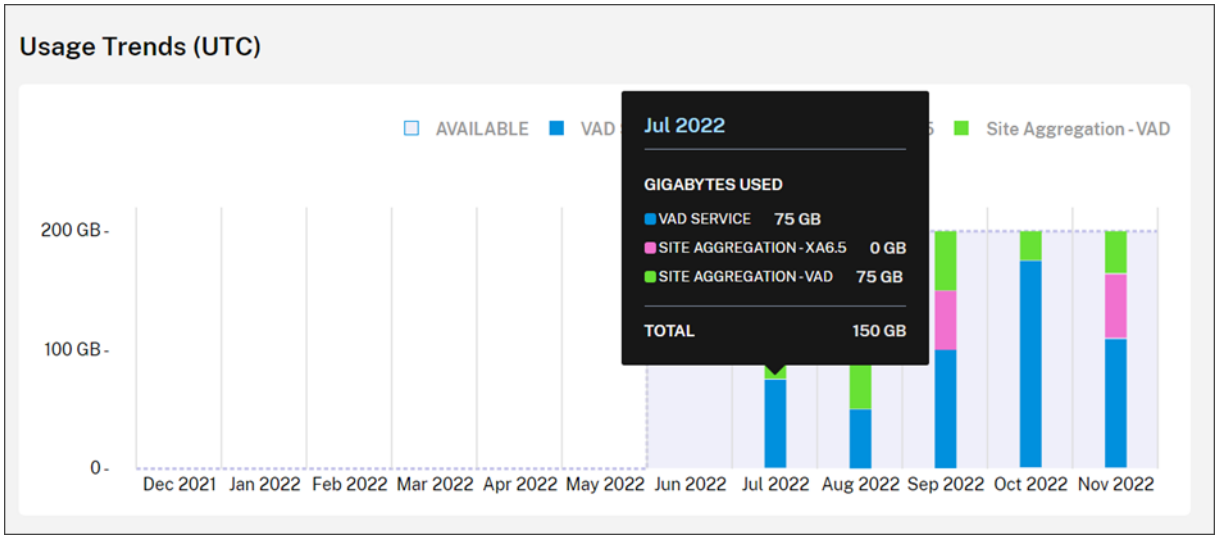
对于年度订阅和定期订阅，本部分包括以下视图：

- 个人使用量：当前计费周期内每个月的带宽使用量。
- 累积使用量：当前计费周期内每个月累积的带宽使用量。



对于所有订阅类型，指向“使用趋势”图表中的条形可显示该时间点的带宽使用情况，按访问量细分。

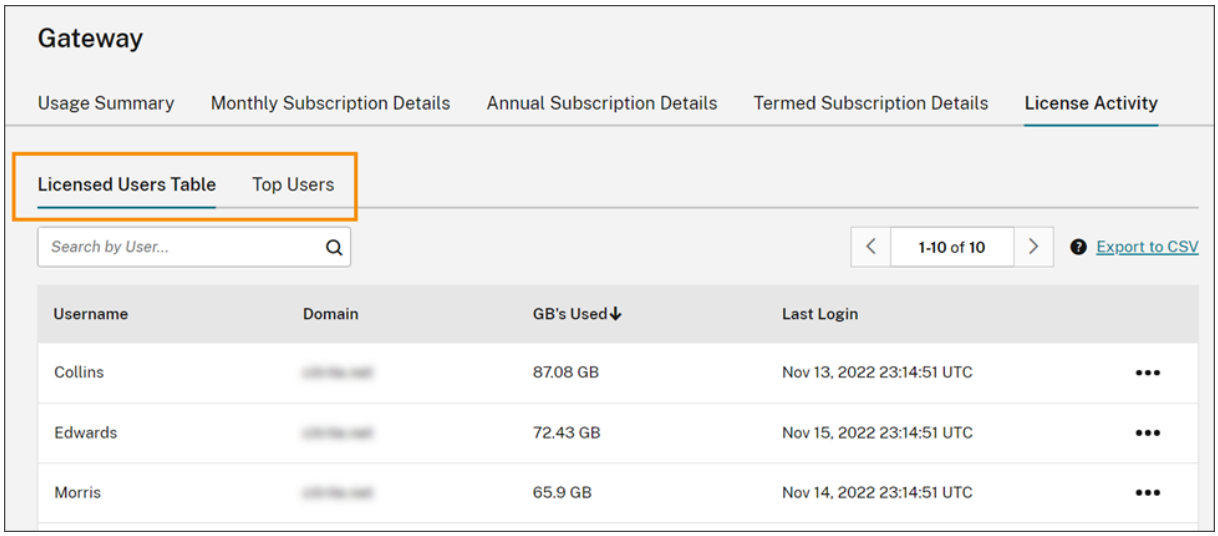
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



许可证活动

许可证活动部分提供以下信息的视图：

- 许可用户：显示已分配许可证的个人用户列表。此列表包括每个用户所属的域、过去 30 天内使用的带宽量以及用户上次使用需要使用带宽的服务的日期。
- 排名靠前的用户：根据带宽使用情况显示前 10 名用户的列表。此列表包括根据访问类型（Citrix DaaS 或通过站点聚合实现的本地 Virtual Apps and Desktops）在过去 30 天内每位用户的使用情况明细。

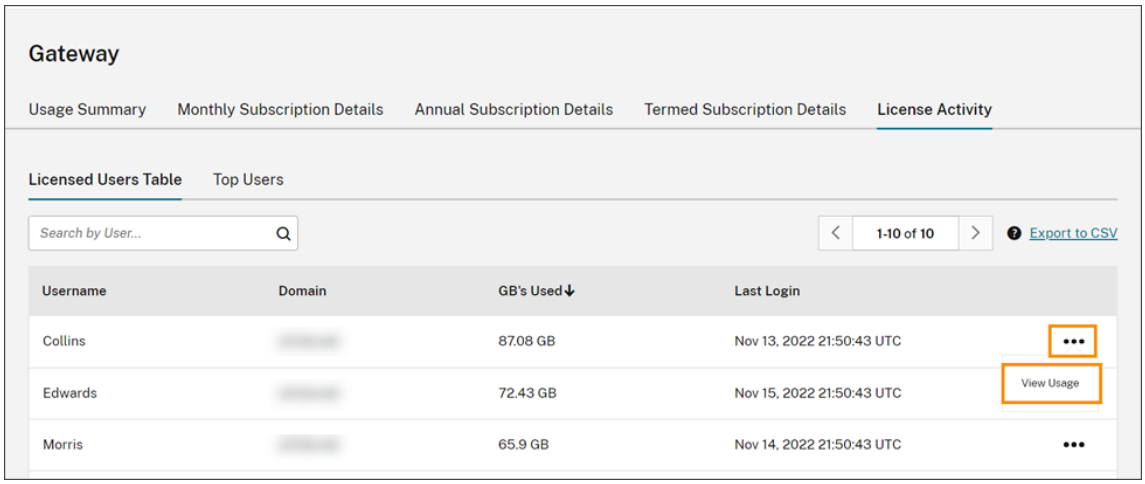


Citrix Cloud 会显示特定用户在过去 30 天内的带宽使用情况，即使他们不再使用许可证也是如此。当网关服务订阅到期时，Citrix Cloud 仍会显示单个用户在 30 天内消耗的带宽。

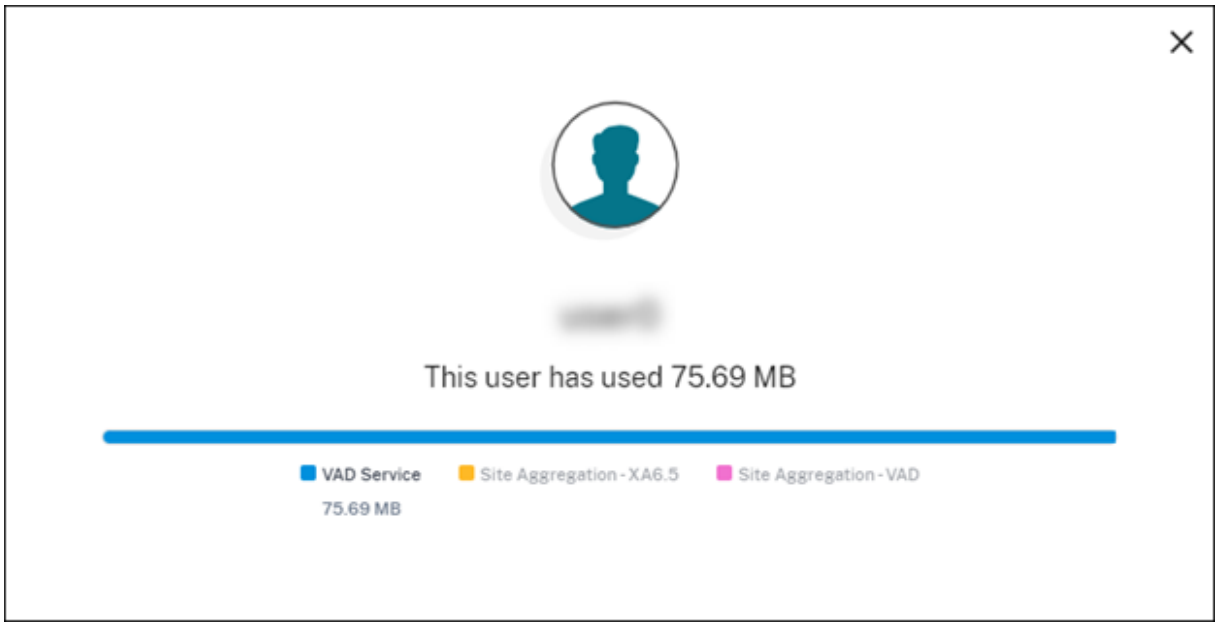
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

查看特定用户的使用情况详细信息

1. 选择许可用户表，然后在列表中找到要查看的用户。
2. 从页面最右侧的省略号菜单中选择查看使用情况。



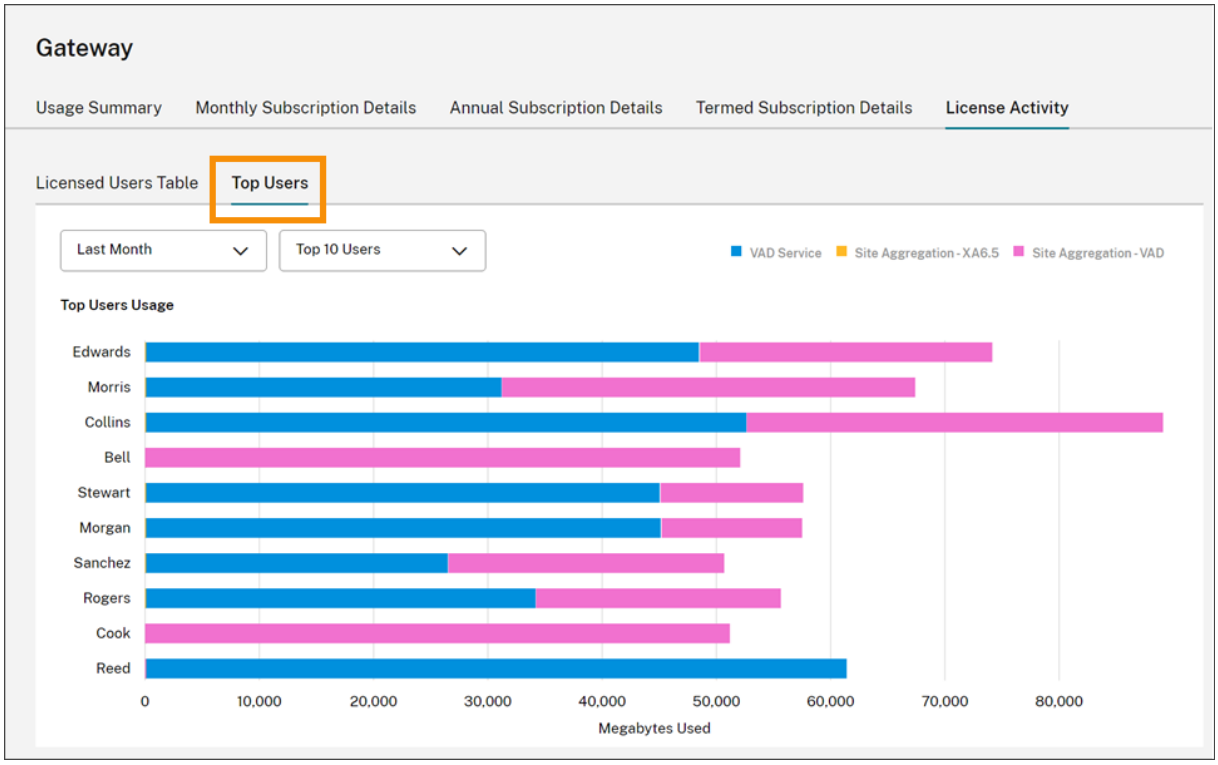
Citrix Cloud 显示按访问细分的用户带宽。



查看排名靠前的用户的使用情况详细信息

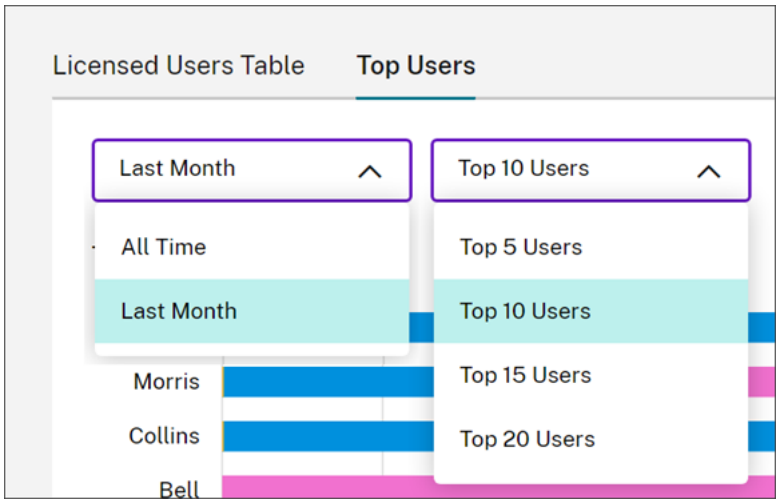
选择排名靠前的用户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



Citrix Cloud 显示按访问量细分的排名靠前的用户的带宽使用情况图表。

默认情况下，排名靠前的用户图表显示过去 30 天内使用带宽最多的前 10 位用户。您可以更改此视图以显示前 5 名、前 15 名或前 20 名用户。也可以将时长更改为所有时间，这会显示订阅生命周期内排名靠前的用户。要更改此视图，请从每个菜单中选择一个选项。



监视 **Secure Private Access** 的许可证和使用情况

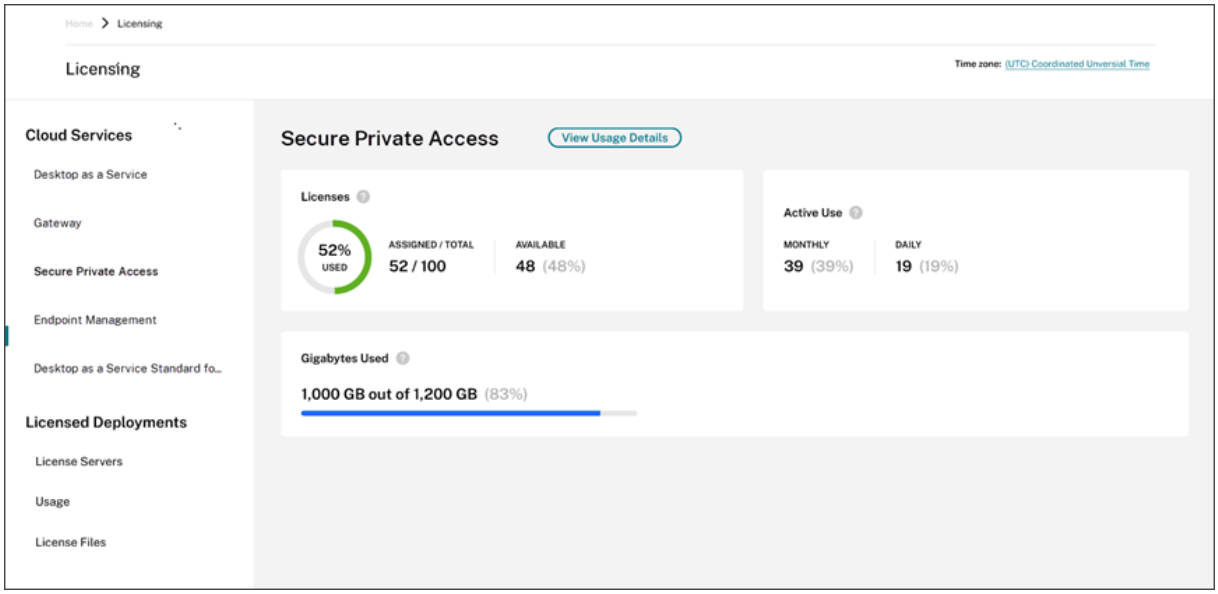
November 30, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

许可证分配

当唯一用户首次启动 Web 和 SaaS 应用程序或 TCP 和 UDP 应用程序时，将分配许可证。

许可摘要



许可摘要显示以下信息：

- 已分配占已购买许可证总数的百分比。
  - 当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则百分比变为红色。
- 分配的许可证与已购买的许可证的比率以及可供分配的许可证数量。
- 每月和每天的活跃使用情况统计信息：
  - 每月活跃使用量是指在过去 30 天内使用过该服务的唯一身份用户的数量。
  - 每日活跃使用量是指在过去 24 小时内使用过该服务的唯一身份用户的数量。
- 在所有订阅的带宽总量中消耗的带宽量。
- 云服务订阅到期之前的剩余时间。如果订阅将在接下来的 90 天内到期，则会显示一条警告消息。

使用的许可证和带宽

在 Secure Private Access Advanced 订阅中，每个用户每月可以获得 5 GB 的带宽（每位用户每年 60 GB）。在 Secure Private Access Standard 订阅中，每个用户每月可以获得 1 GB 的带宽（每位用户每年 12 GB）。此带宽在许可证数量和订阅期内共享。

例如，如果您在三年内购买 100 个许可证，则总带宽为 18000 GB（三年内每年购买 6000 GB）。此带宽在三年期限内分布于所有许可用户。如果您购买更多订阅，Citrix Cloud 将显示所有订阅的许可证总数和带宽。

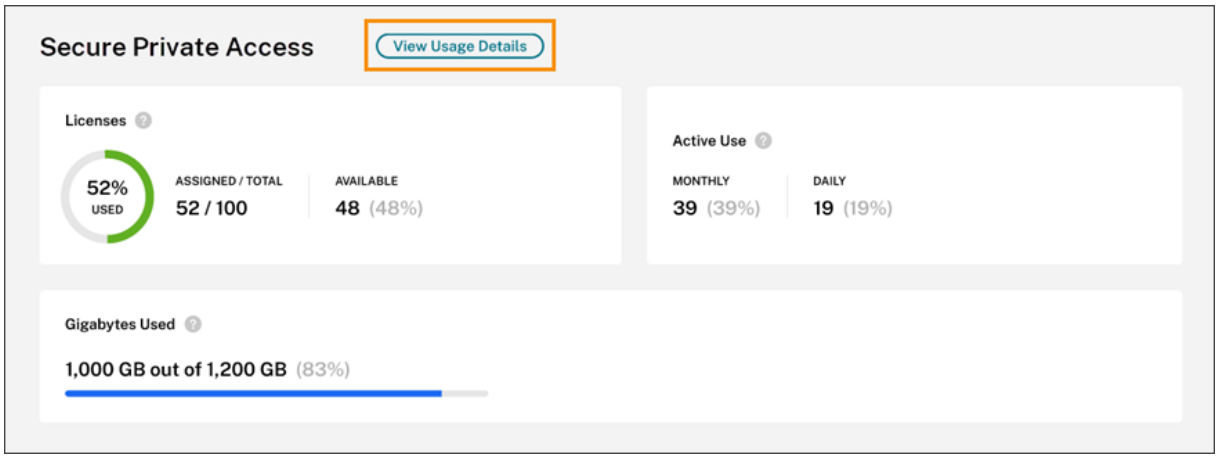
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您在订阅期内未使用全部带宽，Citrix Cloud 不会在续订时结转任何未使用的带宽。如果您使用的带宽超过购买的带宽，则订阅将过期，续订时可用带宽量将保持为零。

对于期限重叠的多个订阅，在每个订阅到期时，与每个订阅关联的带宽量将从许可中删除。例如，如果您购买了两个订阅，Citrix Cloud 将显示两个订阅的总许可证和总带宽。当第一个订阅到期时，Citrix Cloud 将仅显示与未过期订阅关联的带宽。

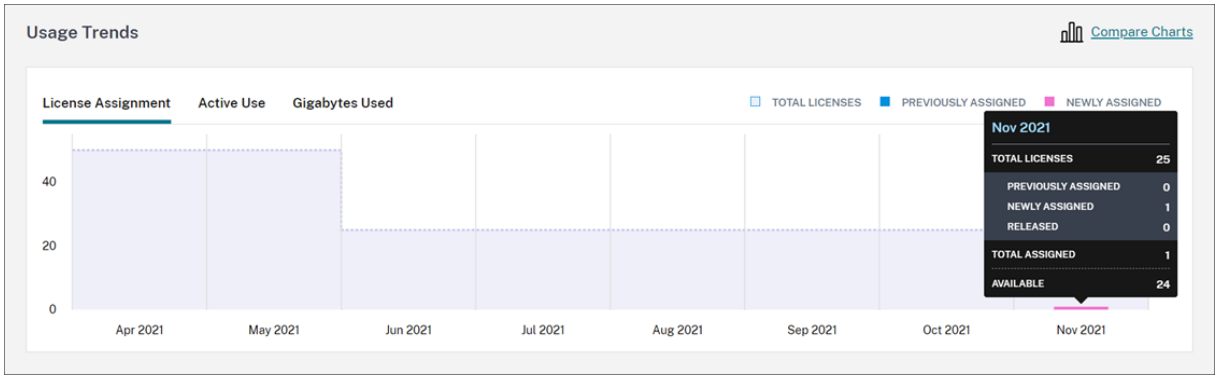
使用趋势

要详细了解您的带宽使用情况和许可证，请单击查看使用情况详细信息。



Citrix Cloud 根据用户可以访问的应用程序类型显示带宽消耗明细。

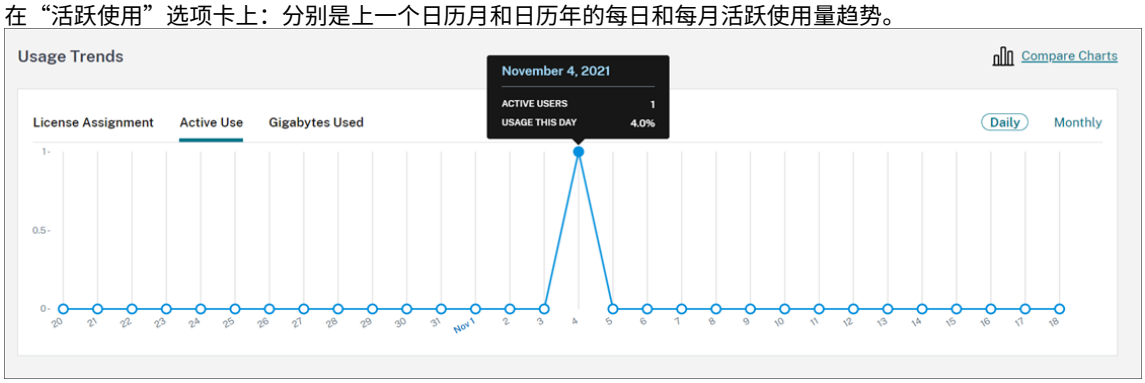
您还可以查看使用趋势以及使用云服务许可证和带宽的个人用户的明细。



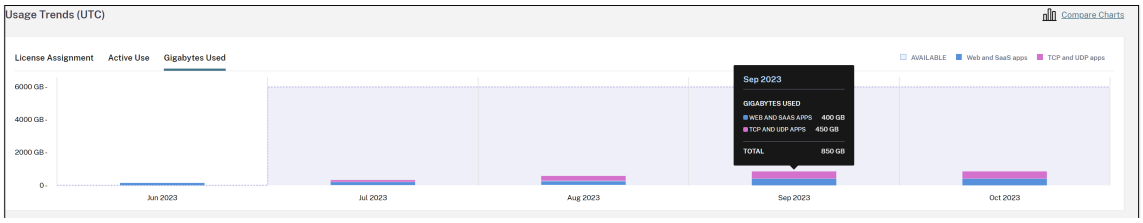
此细分在 使用趋势下，显示了以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 在“许可证分配”选项卡上：
  - 许可证总数：您在所有授权中为云服务购买的许可证总数。
  - 之前已分配：每个月初已分配的云服务许可证。例如，如果在 7 月为用户分配了许可证，则 Citrix Cloud 会将该分配计入八月份的先前分配编号中。
  - 新分配：每月分配的许可证数量。例如，当您在 7 月首次访问云服务并获得许可证时。Citrix Cloud 将该许可证计入七月份的新分配编号中。
- 在“活跃使用”选项卡上：分别是上一个日历月和日历年的每日和每月活跃使用量趋势。



- 在“已用千兆字节”选项卡上：总可用带宽中消耗的带宽量。它显示每个用户的使用情况和每个应用程序的信息，例如 Web 和 SaaS 应用程序以及 TCP 和 UDP 应用程序。



要比较许可证分配、有效使用和带宽使用趋势，请选择 比较图表。

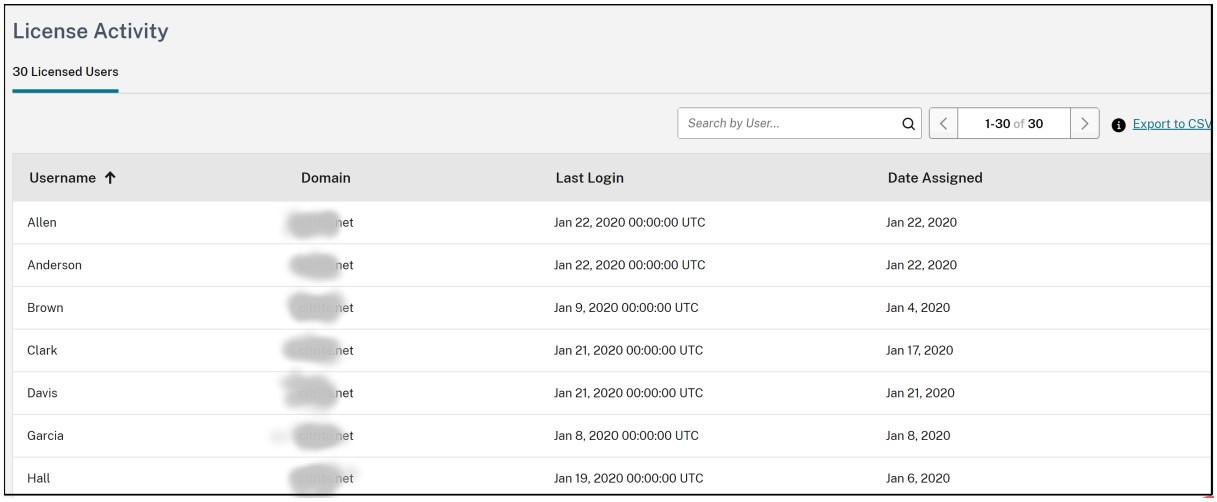
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> 当前订阅期限内的使用趋势是累积性的。续订订阅时，使用趋势将在新的订阅期开始时重置。

许可证活动

“许可证活动”部分还显示以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



- 已分配许可证的单个用户的列表。
- 用户所属的域。
- 用户上次使用服务的日期。
- 将许可证分配给用户的日期。

发放分配的许可证

如果您在过去 30 天内没有使用过该服务，Citrix Cloud 会自动发放许可。Citrix 管理员无需采取任何措施即可发布许可。

许可证发布后，剩余许可证的数量会增加，分配的许可证数量也会相应减少。许可证发布后，您可以通过登录和使用云服务获得另一个许可证。

监视 **Citrix DaaS** 的 **Citrix** 托管 **Azure**

October 5, 2023

当您购买 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的授权时，您还可以购买 Citrix Azure 消费基金，该基金允许您使用 Citrix 托管 Azure 订阅中的资源。您可以使用这些资源与本地 VDA 一起向用户交付应用程序和桌面。

购买 Citrix Azure 消费基金时，可以使用以下方法之一支付消费：

- 即用即付：对于您在给定月份使用的 Citrix 托管 Azure 资源，Citrix 将在下个月向您收费。Citrix Cloud 将您的使用量显示为超量。
- 预付消费：您可以按月或每年（期限）预付消费。对于超出预付费消耗量的任何使用量，Citrix Cloud 会将此使用量显示为超额。对于给定月份的任何超额，Citrix 将在下个月向您收费。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

每个消费单位的价值为 1.00 美元。Citrix Cloud 中的许可控制台可帮助您跟踪所使用的单元。

要估算消耗成本，请使用 Citrix 托管 Azure 使用量计算器。要估算 Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）的消耗和许可成本，请使用许可和消耗计算器。

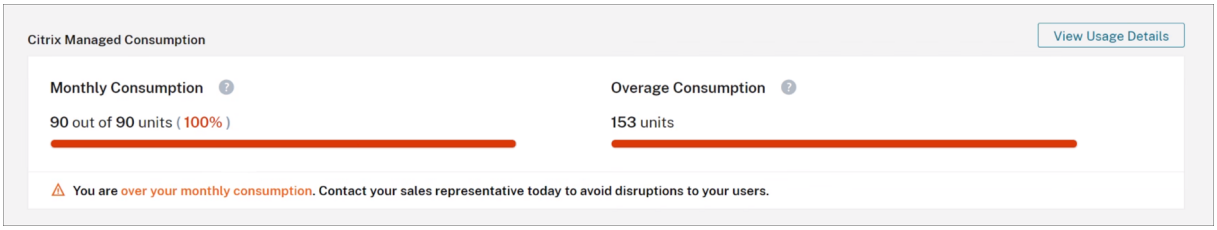
支持的产品

以下版本的 Citrix DaaS 可以使用消耗量监视：

- Citrix DaaS Advanced（以前称为 “Virtual Apps Advanced”）
- Citrix DaaS Premium（以前称为 Virtual Apps Premium）
- Citrix DaaS Advanced Plus（以前称为 Virtual Apps and Desktops 高级版）
- Citrix DaaS 高级版（以前称为 Virtual Apps and Desktops 高级版）
- Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Virtual Apps and Desktops Standard）

消耗摘要

Citrix 管理消费部分显示了您在消费基金中使用的单位的摘要。



每月消费量显示您购买的每月消费基金单位总数中您当月使用的消费单位数。每月消耗量每月重置。未使用的消费单位不会结转到下个月。

期限消费量显示您已购买的定期消费基金单位总数中已使用的消费单位数。与月度消费单位一样，未使用的定期消费单位不会结转到下一年。

超额消耗量 显示您已使用的超出 Azure 消耗基金单位数的消耗单位数。如果您使用 Citrix 托管 Azure 资源按使用量付费，则默认情况下，您的使用量将显示为超额使用。

如何衡量超额

如果您以即用即付的方式使用 Azure 消费基金，Citrix Cloud 会将您当月使用的消费单位数显示为超量。

如果您按月或按年预付消费，Citrix Cloud 将显示您在当月或当年使用的月度或定期消费单位数。如果消耗的单位数超过购买的数量，Citrix Cloud 会将多余的单位显示为超量单位。

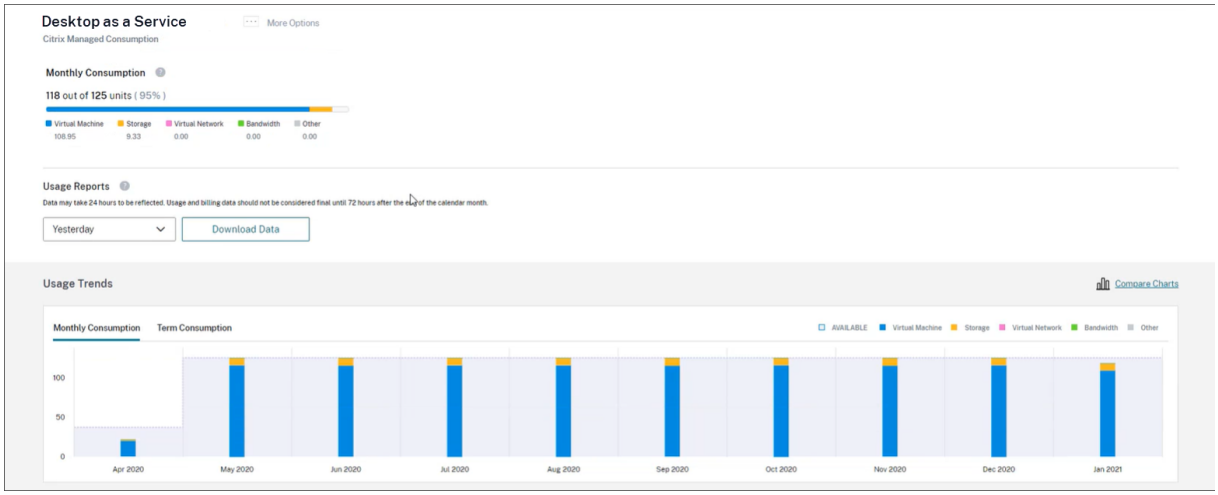
如果您按月和按年预付消费，Citrix Cloud 将首先根据您购买的月度单位来衡量您的消费。消耗这些单位后，Citrix Cloud 会根据您的年度单位来衡量您的消耗量。使用这些单位后，Citrix Cloud 会将您消耗的任何多余单位显示为超量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您购买了额外的消费单位，并且您的帐户存在超额，则新的消费单位不会应用于超额。新的消耗单位仅应用于购买这些单位后发生的用量。

消费详情

要查看消费单位的详细视图，请单击摘要最右侧的 查看使用详情。详细信息页面显示您的消费和使用趋势的细分。



使用情况报告

您可以将使用信息下载为指定时间间隔的 CSV 文件。单击“下载数据”生成 CSV 文件并将其下载到您的本地计算机。

在一天或一个月结束后，数据可能需要长达 72 小时才能反映所有使用情况。

CSV 文件包括以下部分：

- 报告摘要，显示报告日期范围之前和之后的可用消耗单位、总使用费用和待定超量。

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.			
Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	

Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 每日摘要，显示报告日期范围内每天的总使用费、剩余的月度资金和定期资金以及超额费用。

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

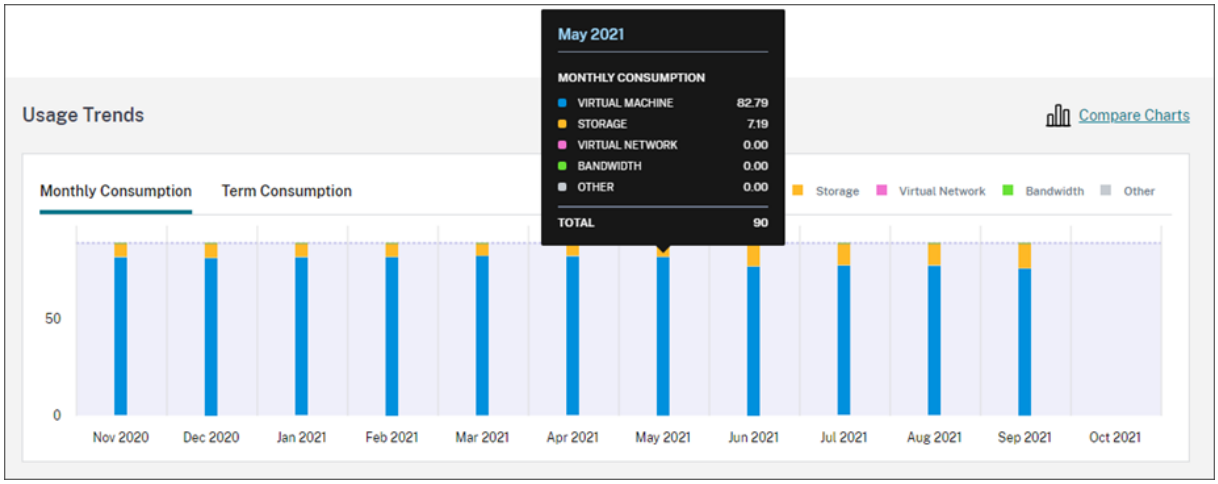
- 按报告日期范围内的每一天计量的 Azure VM、网络连接、Azure 存储和带宽使用量。

Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

使用趋势和消费活动

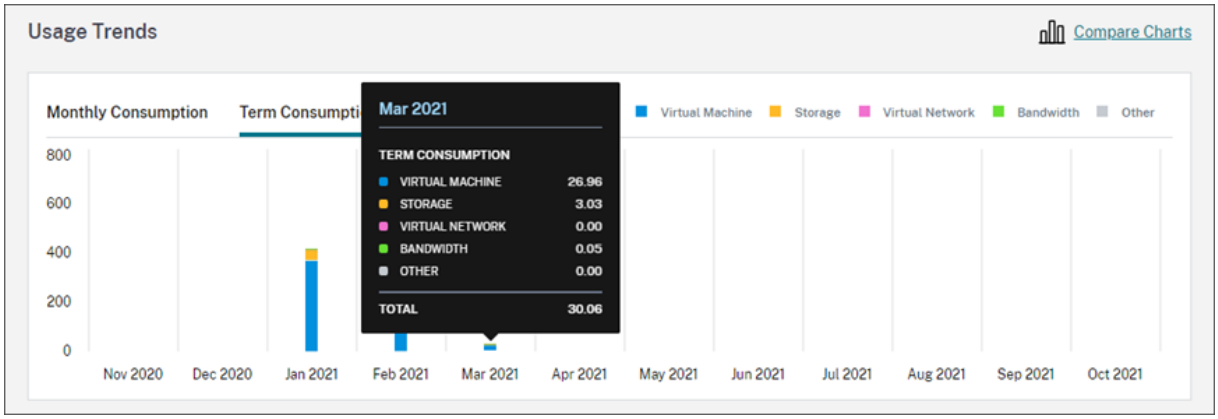
使用情况趋势 部分显示您使用过的 Citrix 托管 Azure 资源的图表。指向图表上的条形图可显示该月消耗的资源数量，包括虚拟机、存储、虚拟网络资源和带宽。

选择“每月消费”以查看过去 12 个月的每月消费。

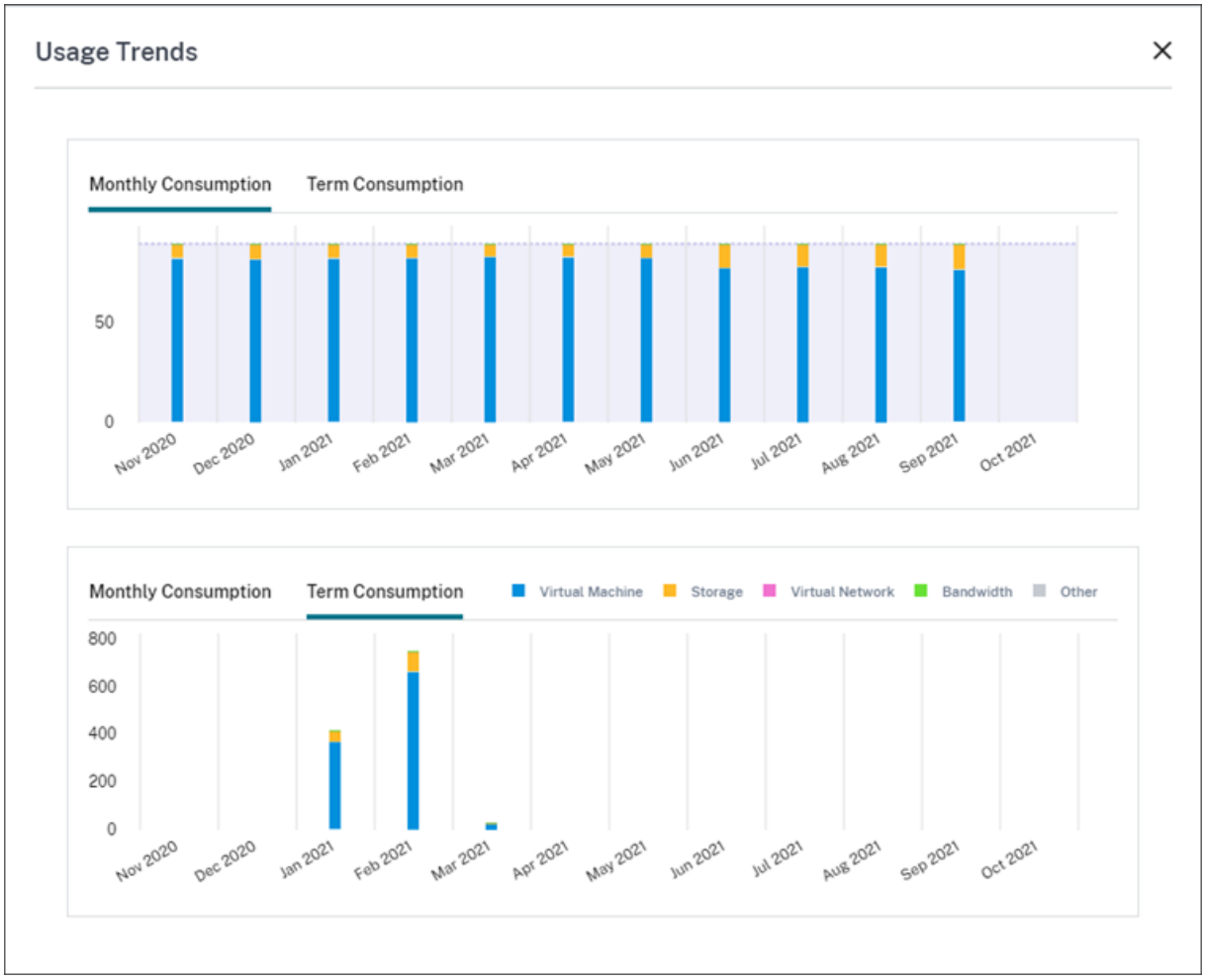


选择“学期消费”可查看上一年中每个月的学期消费。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

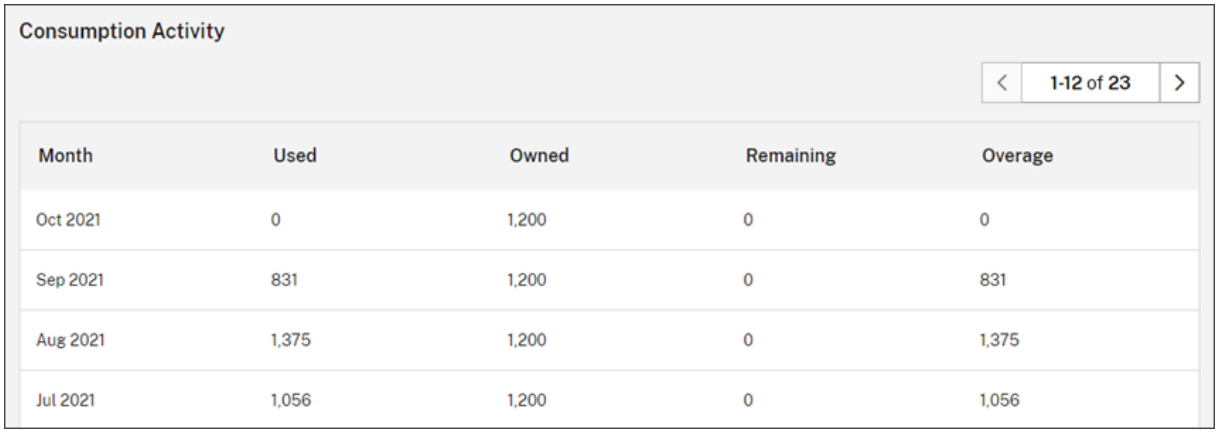


如果您同时购买了月和年度消费单位，请选择 图表最右侧的比较 图表，以在单个视图中查看每月和长期消费趋势。



消费活动 部分还显示每个月的消费单位列表。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.


Consumption Activity

1-12 of 23

Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

消费活动包括以下信息：

- 已 @@ 使用：每月使用的单位数。
- 已 @@ 拥有：每月购买的单位总数。
- 剩余：每月未使用的已购买商品数量。
- 超量：每月超出购买商品数量的已消耗商品数量。

发放分配的许可证

许可证分配何时有资格发放，取决于您购买的消费基金单位。

在以下情况下，您可以在 30 天后发放非活动许可证：

- 不要在服务部署中使用 Citrix 托管 Azure 订阅。
- 您购买了用于服务部署的年消耗单位。

在以下情况下，如果没有用户或设备启动应用程序或桌面，则可以在当月发放非活动许可证：

- 您购买了每月消费基金单位以用于服务部署。
- 您购买了月度和年度消费基金单位。

有关发放合格许可证的说明，请参阅以下文章：

- Citrix DaaS（用户/设备型号）：发放分配的许可证
- Citrix DaaS Standard for Azure：发放分配的许可证

监视本地部署的许可证和使用情况

October 5, 2023

Citrix Cloud 中的许可部署体验包括以下功能：

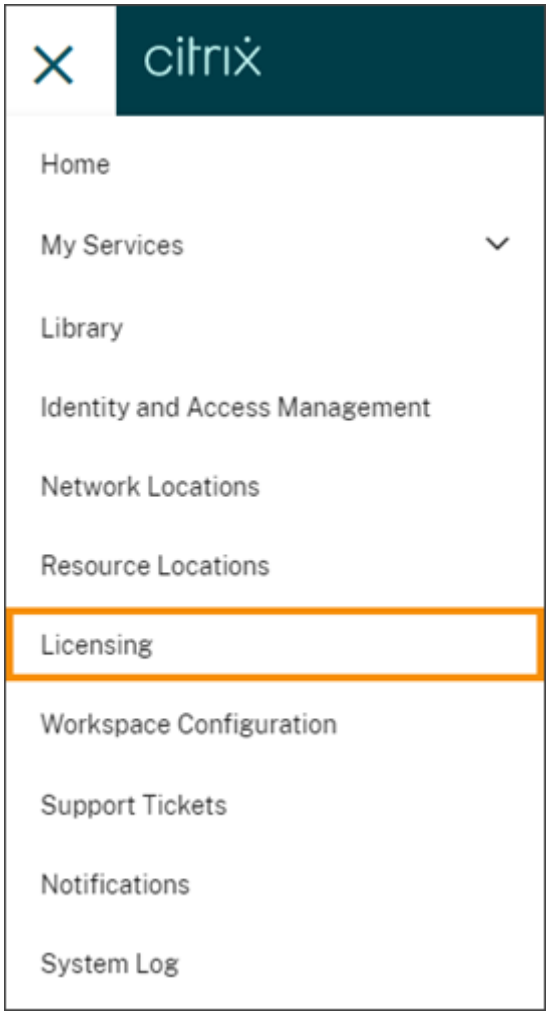
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 产品 注册：向 Citrix Cloud 注册现有 Citrix 许可证服务器，以获取有关部署的其他使用情况见解和报告。
- 许可证服务器状态：查看 Citrix 许可证服务器的状态，以了解哪些服务器成功报告使用情况以及上次向 Citrix Cloud 报告使用情况的时间。
- 使用情况见解：查看 Citrix 许可证服务器中已安装和使用的许可证数量，并深入了解历史许可证使用趋势。

支持的产品

Citrix 许可证服务器使用情况见解适用于并行和用户/设备许可模式下的所有虚拟应用程序和桌面版本。

要查看 Citrix 许可证服务器使用情况见解，请从控制台菜单中选择许可，然后选择许可的部署。



必备条件

要使用 Citrix 许可证服务器使用情况见解，请确保您具备以下项目：

- Citrix 许可证服务器版本 11.15.0.0 或更高版本

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- Citrix Cloud 帐户
- 从 Citrix 许可证服务器到 Citrix Cloud 的网络访问

连接要求

要在 Citrix Cloud 上成功注册许可证服务器，请确保以下地址可联系：

- https://citrix.cloud.com/ （用于访问管理员控制台以输入代码和查看许可证服务器状态）
- https://trust.citrixnetworkapi.net （用于检索代码）
- https://trust.citrixworkspacesapi.net/ （用于确认许可证服务器已注册）
- https://cis.citrix.com （用于数据上载）
- https://core-eastus-release-a.citrixworkspacesapi.net
- https://core.citrixworkspacesapi.net
- ocsp.digicert.com port 80
- crl3.digicert.com port 80
- crl4.digicert.com port 80
- ocsp.entrust.net port 80
- crl.entrust.net port 80

连接到 **Citrix Cloud**

要启用 Citrix 许可证服务器使用情况见解，请执行以下任务：

1. 使用 Licensing Manager 控制台为许可证服务器启用使用情况见解。有关更多信息，请参阅许可产品文档中的共享使用情况统计信息。
2. 查看本文的连接要求中描述的连接要求，并确保地址是可联系的。如果您将代理服务器与 Citrix 许可证服务器一起使用，请确保按照许可产品文档中的步骤 5 配置代理服务器中所述配置代理服务器。
3. 按照在 Citrix Cloud 注册本地产品中所述将许可证服务器注册到 Citrix Cloud。

查看本地产品许可证使用情况

Citrix 许可证服务器使用情况见解可让您了解整个 Citrix 资产的许可证使用情况。您可以访问使用情况报告，它可以帮助您：

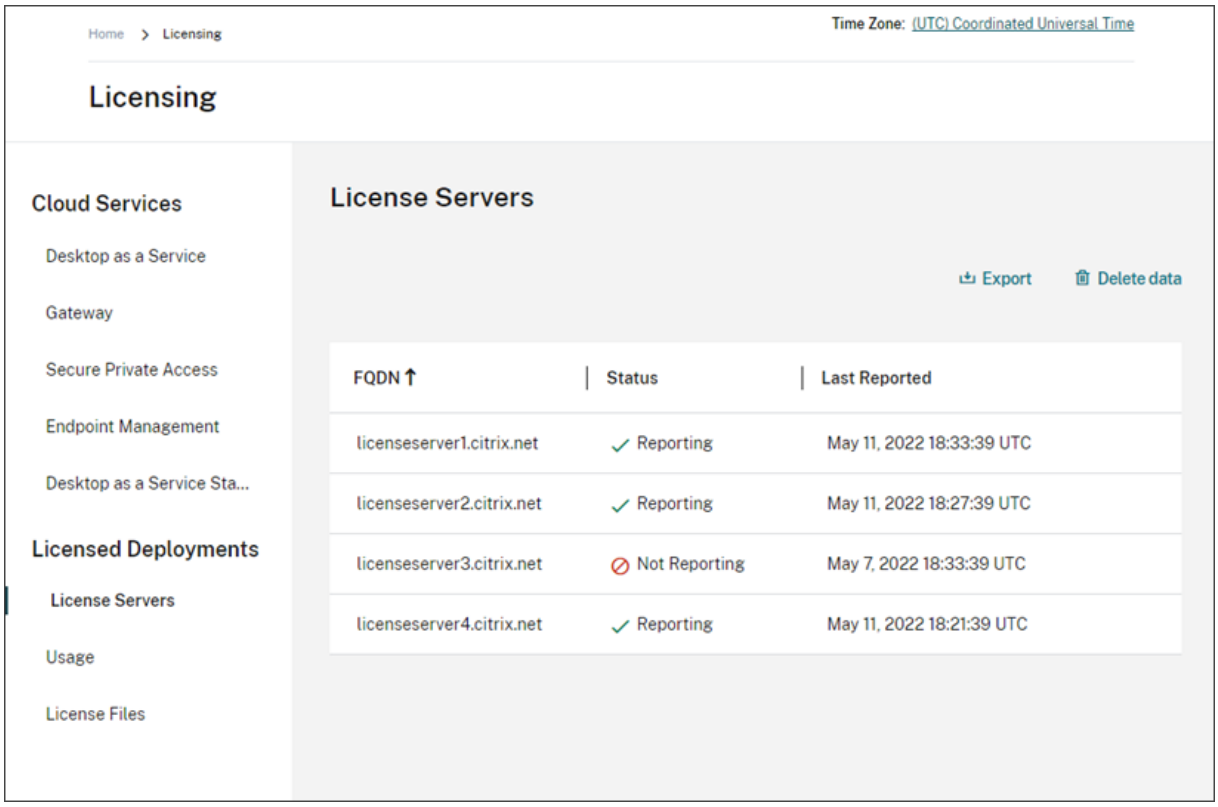
- 了解部署和注册的许可证服务器数量，以及它们是否向 Citrix Cloud 报告使用情况信息。
- 了解 Virtual Apps and Desktops 并发许可证和用户/设备许可证使用情况。
- 深入了解多个部署中的并发许可证和用户/设备许可证使用汇总情况。
- 了解许可证的历史使用情况和每月许可证使用趋势。
- 查看特定用户的上次登录时间。
- 比较安装的许可证数量与跨 Citrix 许可证服务器使用的许可证的数量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 监视许可证透支。
- 查看并发许可证和用户/设备许可证使用情况的细分。

查看许可证服务器状态

许可证服务器状态视图显示向 Citrix Cloud 报告使用情况的每个许可证服务器。



如果许可证服务器在过去三天内成功将使用情况上传到 Citrix Cloud，则会显示“报告”状态。如果许可证服务器先前报告了过去 30 天的使用情况，但在过去三天内未报告，则会显示“未报告”状态。过去 30 天内未报告使用情况的许可证服务器将从列表中删除。

许可证服务器状态对许可证使用情况视图的影响

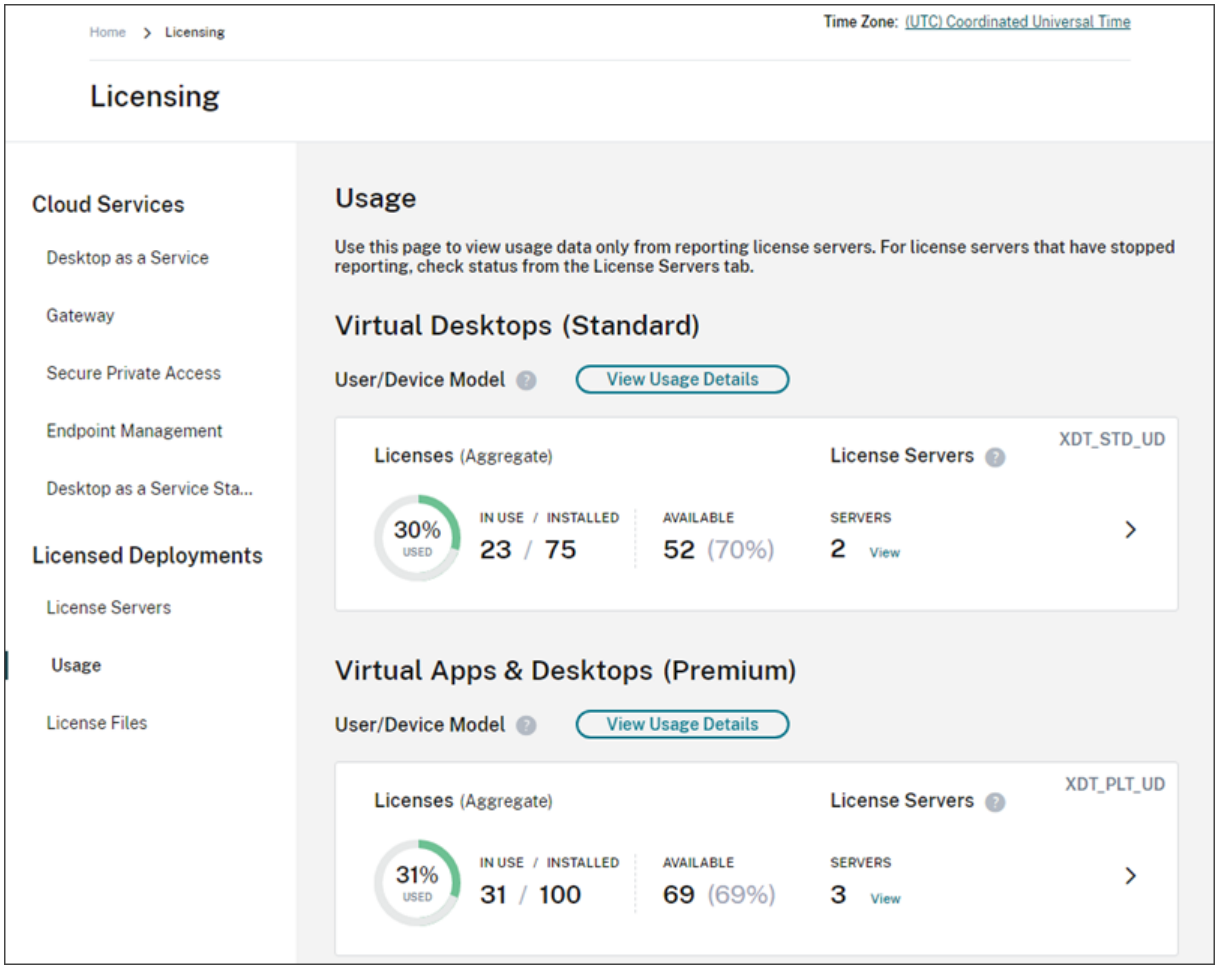
许可证服务器的报告状态和上次报告日期决定了特定许可证服务器的使用情况是否包含在使用情况分析视图和报告中。

- 当前已安装和正在使用的许可证完全基于报告许可证服务器的数据。如果许可证服务器列为“未报告”，则该许可证服务器的已安装和正在使用的许可证不会反映在使用情况见解体验中。
- 每个许可证服务器的上次报告日期决定了使用情况见解体验中许可证使用情况信息的最新情况。显示的许可证使用情况报告仅与每个许可证服务器的上次报告时间相同。
- Citrix 许可证服务器配置为获取使用情况见解，并在 Citrix Cloud 中注册，每天更新一次使用情况。如果需要，可以从许可证服务器上的 Citrix 许可证管理器管理控制台强制进行更新。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

许可证使用情况

“使用情况”选项卡提供整个 Citrix 部署中的许可证使用情况的综合视图。来自每个报告许可证服务器的许可信息合并到一个视图中。通过此视图，您可以轻松查看许多不同部署和许可证服务器的完整许可情况。



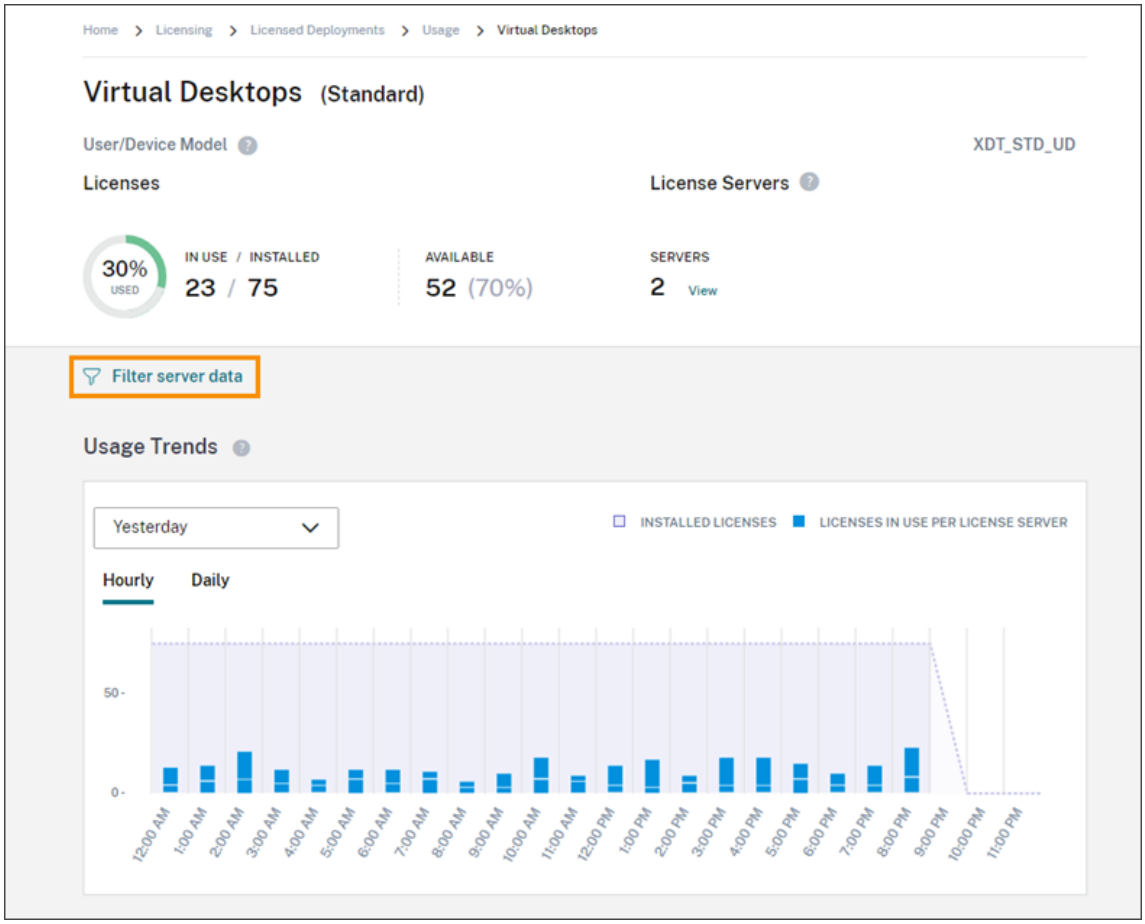
许可证使用根据产品版本和许可模式跨多个许可证服务器进行组织和汇总。对于在所有报告许可证服务器中找到的每个唯一许可证版本，都将显示许可证使用情况摘要卡。将为检测到的每个产品版本显示一张摘要卡。

每个许可证服务器的使用量

要查看每个许可证服务器的产品许可证使用情况，可以筛选服务器数据。

1. 在 使用情况页面中，选择要管理的产品的查看使用详情。
2. 单击筛选服务器数据，然后选择要查看其使用情况的许可证服务器。默认情况下，所有许可证服务器都处于选中状态。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



3. 选择应用。

应用筛选器后，Citrix Cloud 将仅显示所选服务器的使用趋势、许可证服务器细分和许可证活动。

并发许可模式的许可证使用峰值

并发许可证的报告体验围绕以下数据点进行组织：

- 已安装的许可证：每个许可证服务器上安装的许可证数量。
- 使用中的峰值许可证：在特定时间范围内使用的最大许可证数量。

在计算使用中的许可证峰值时，Citrix Cloud 会检索在以下时间段内使用的最大许可证数：

- 过去 7 天：过去七天内一次使用的最大许可证数。
- 本月：当前日历月中一次使用的许可证的最大数量。
- 所有时间：自许可证服务器向 Citrix Cloud 注册以来一次使用的最大许可证数。

> 重要：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 这些时间段的数据可能与许可证服务器上正在使用的许可证数量不匹配。许可证服务器只报告在任何给定时间使用的许可证数量。Citrix Cloud 接收这些单独的数据点并计算这些时间段的峰值。

解释许可证用法的注意事项

Citrix 许可支持多种使用场景，包括详细信息。监视使用情况时，请记住以下注意事项：

- 使用信息基于每个报告许可证服务器上安装的许可证。如果许可证服务器的可用许可证已用完，则可以在许可证服务器上分配和放置其他许可证，以增加可用许可证的数量。
- Citrix 许可证服务器使用情况见解视图中提供的信息仅包括注册和主动报告的 Citrix 许可证服务器收集和报告的信息。许可部署体验并不代表您实际拥有或购买的许可证总数，也可能与之不符。
- 可用许可证的百分比是根据正在使用的许可证数量相对于报告许可证服务器上安装的许可证数量计算得出的。

移除许可证服务器注册

从 Citrix Cloud 中完全删除许可证服务器注册包括以下任务：

1. 使用 Citrix Licensing Manager 控制台从 Citrix Cloud 中删除注册的许可证服务器。有关完整说明，请参阅删除许可证服务器的注册。
2. 移除之前收集的所有使用情况数据。
3. 确认 Citrix Cloud 不再在产品注册页面上显示许可证服务器。如果许可证服务器仍出现在列表中，请按照删除产品注册中的说明删除该服务器。

移除使用情况数据

从 Citrix Cloud 中删除已注册的许可证服务器时，仍会存储以前收集的使用情况数据。如果您不想再保留这些数据，可以将其删除。

> 重要：
>
> 删除使用情况数据是永久性的，无法撤消。如果您删除了使用情况数据，但未 删除许可证服务器的注册，Citrix Cloud 将继续收集使用情况数据。

1. 从 Citrix Cloud 菜单中，选择 许可。
2. 在许可证服务器选项卡上，选择删除数据。
3. 出现提示时，选中相应的复选框以确认您了解删除的影响。
4. 选择 删除服务器数据。

Citrix 服务提供商的许可

July 1, 2024

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 中的许可证使用情况见解服务是一项免费的云服务，可帮助 **Citrix** 服务提供商 **(CSP)** 了解和报告产品许可证和使用情况。只有 CSP 合作伙伴有权访问许可证使用情况见解。

> 注意：
>
> Citrix DaaS 以前称为 Citrix Virtual Apps and Desktops 服务。Citrix DaaS Standard for Azure 以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard。某些显示器可能包含以前的名称。

通过 License Usage Insights Service，可以执行以下操作：

- 自动从 Citrix 许可证服务器收集和汇总产品使用信息
- 自动汇总单租户和多租户客户的云许可使用和消费
- 轻松查看每月哪些用户正在访问您的 Virtual Apps and Desktops 部署
- 创建许可使用情况的客户细分
- 通过标识和跟踪免费用户的列表来优化许可证成本
- 查看和了解您与 Citrix 的历史业务
- 将 Virtual Apps and Desktops 和 Citrix DaaS 的许可使用情况、NetScaler VPX 分配数据以及 Citrix DaaS Standard for Azure 许可和使用数据导出到 CSV

其他信息

有关要求和设置说明，请参阅 许可证使用情况洞察入门。

要查看单租户客户和多租户合作伙伴的汇总使用情况，请参阅 Citrix 服务提供商的云服务许可证使用情况和报告。

要使用许可控制台查看客户对受支持服务的使用情况，请参阅以下文章：

- Citrix DaaS 的客户许可证和使用情况监视
- Citrix DaaS Standard for Azure 的客户许可证和使用情况监视

开始阅读许可证使用情况见解

July 1, 2024

受支持的 **Citrix** 产品

许可证使用情况见解服务提供以下 Citrix 产品的使用情况信息：

- Virtual Apps and Desktops（本地）产品使用情况
- Citrix DaaS Premium（前身为 Virtual Apps Premium 和 Virtual Apps and Desktops Premium 服务）
- Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Citrix Virtual Apps and Desktops Standard）
- NetScaler 控制台 VPX 分配

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要求

要捕获 Citrix 本地产品的许可证和使用情况信息，需要 Citrix 许可证服务器 11.16.3.0 或更高版本。仅支持基于 Windows 和基于 VPX 的许可证服务器。

Citrix 许可证服务器 11.16.3.0 及更高版本包含对 Citrix 服务提供商 (CSP) 合作伙伴非常重要的关键功能：

- 优化后的使用情况收集：许可证服务器包含用来优化许可行为和跟踪以更好地支持 CSP 的新功能。
- Call Home：许可证服务器包括用来自动为 CSP 合作伙伴执行产品使用情况收集的 Call Home 功能。这些功能是 CSP 合作伙伴独有的功能，仅在许可证服务器上检测到 CSP 许可证时激活。

步骤 **1**：更新 **Citrix** 许可证服务器

如果您运行的许可证服务器版本早于 11.16.3.0，则必须先升级许可证服务器，然后才能使用许可证使用情况见解。原位升级即简单又快速。请完成以下任务：

1. 下载最新的许可证服务器。有关最新版本的 Citrix 许可证服务器的详细信息，请参阅 Citrix 许可文档。
2. 升级 您当前的许可证服务器。
3. 对您的每个许可证服务器重复执行升级过程。

步骤 **2**：使用 **My Citrix** 凭据登录 **Citrix Cloud**

登录之前，您需要注册一个 Citrix Cloud 帐户。请按照 注册 Citrix Cloud 中描述的步骤进行操作。

创建帐户时，使用的 My Citrix 凭据应与您用来从 citrix.com 分配和下载 Citrix 许可证的凭据相同。Citrix Cloud 会通过与您的“我的 Citrix”凭据关联的地址向您发送一封电子邮件，以确认该帐户。

当您的 Citrix Cloud 帐户准备就绪后，请使用您的电子邮件地址和密码登录 https://citrix.cloud.com 。

第 **3** 步（可选）：通过许可证服务器匿名化用户名

默认情况下，与 Virtual Apps and Desktops 或 Citrix DaaS 许可证签出关联的用户名会安全地拨打电话给 Citrix 总部。

用户名已通过电话回家，因此 CSP 合作伙伴可以充分利用 License Usage Insights 功能和支持免费用户试用、测试和管理产品使用的 CSP 许可计划。

用户信息限制到单个 user@domain 条目；任何附加的个人身份数据都不会在挂断电话后自动返回到主界面。Citrix 不会共享此信息。

对上载用户名信息敏感的合作伙伴可以启用用户名匿名化。激活时，用户名匿名化会在上载之前使用安全且不可逆的算法将可读的用户名转换为唯一的字符串。

License Usage Insights 使用这些唯一标识符来跟踪产品使用情况，而不是实际的用户名。这种方法允许服务提供商利用月度见解，而不需要查看云服务用户界面中实际的用户名。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

配置用户名匿名功能

1. 在许可证服务器上，在文本编辑器中打开配置文件。配置文件通常位于 C:\Program Files\Citrix\Licensing\WebServicesFo
2. 在配置部分中，按如下所示添加 **UsageBasedBillingScramble** 设置：

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
<!--NeedCopy-->
```

3. 保存该文件。

步骤 **4**：使用 **License Usage Insights** 服务

在 Citrix Cloud 控制台中，找到许可证使用情况见解服务，然后单击 管理。有关该服务主要功能的概述，请参阅 管理产品使用情况、许可证服务器和通知。

其他详情

将 Citrix 许可证服务器与许可证使用情况见解配合使用时，请考虑以下事项：

- 新更新的许可证服务器最多可能需要 24 小时才能显示在“许可证使用情况见解”管理控制台中。
- 从许可证服务器上载使用情况数据时，将以安全的方式进行处理和存储，因此 License Usage Insights 可以在以后访问该数据。此过程可能需要长达 24 小时才能完成。
- 默认情况下，与 Virtual Apps and Desktops 或 Citrix DaaS 许可证签出关联的用户名会安全地拨打电话给 Citrix 总部。
- 用户名已通过电话回家，因此 CSP 合作伙伴可以充分利用 License Usage Insights 功能和支持免费用户试用、测试和管理产品使用的 CSP 许可计划。
- 用户信息限制到单个 user@domain 条目；任何附加的个人身份数据都不会在挂断电话后自动返回到主界面。Citrix 永不共享此信息。

帮助和支持

如果您需要有关许可证使用情况见解的帮助，请在“我的支持”门户上打开支持请求。要从 Citrix Cloud 访问我的支持，请执行以下操作：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1. 登录 Citrix Cloud。
2. 单击屏幕右上角附近的 帮助 图标。
3. 选择“打开票证”。
4. 选择“前往我的支持”，然后使用您的“My Citrix”凭据登录。
5. 填写并提交表单。

Citrix 技术支持的成员将跟进并 为您提供帮助。

常见问题解答

- 什么信息被打电话回家？我可以查看我的许可证服务器发送到 **Citrix** 的信息吗？可以，您可以查看打电话给 Citrix 总部的信息的副本。有关详细信息，请参阅 上载中包含的许可证服务器信息。
- 不是 **Citrix** 服务提供商的 **Citrix** 客户或合作伙伴是否可以使用许可证使用情况见解？不是。许可证使用情况见解仅适用于具有有效合作伙伴协议的 Citrix 服务提供商合作伙伴。
- 我能否在许可证服务器上禁用 “**Call Home** 总部”？不是。根据 Citrix 服务提供商许可协议，所有许可证服务器都必须拨打家庭产品使用电话。对在挂断电话后将用例自动返回到主界面敏感的合作伙伴可以使用用户名匿名功能。有关详细信息，请参阅 通过许可证服务器匿名化用户名。
- 是否会根据许可证使用情况见解中显示的产品使用情况向我收费？不是。许可证使用情况见解可帮助合作伙伴了解其产品使用情况，以便他们能够快速准确地向其 Citrix 分销商报告。我们将继续根据 CSP 合作伙伴向其 Citrix 分销商报告的产品使用情况对其进行收费。Citrix 分销商将继续拥有与 CSP 合作伙伴的结算关系。

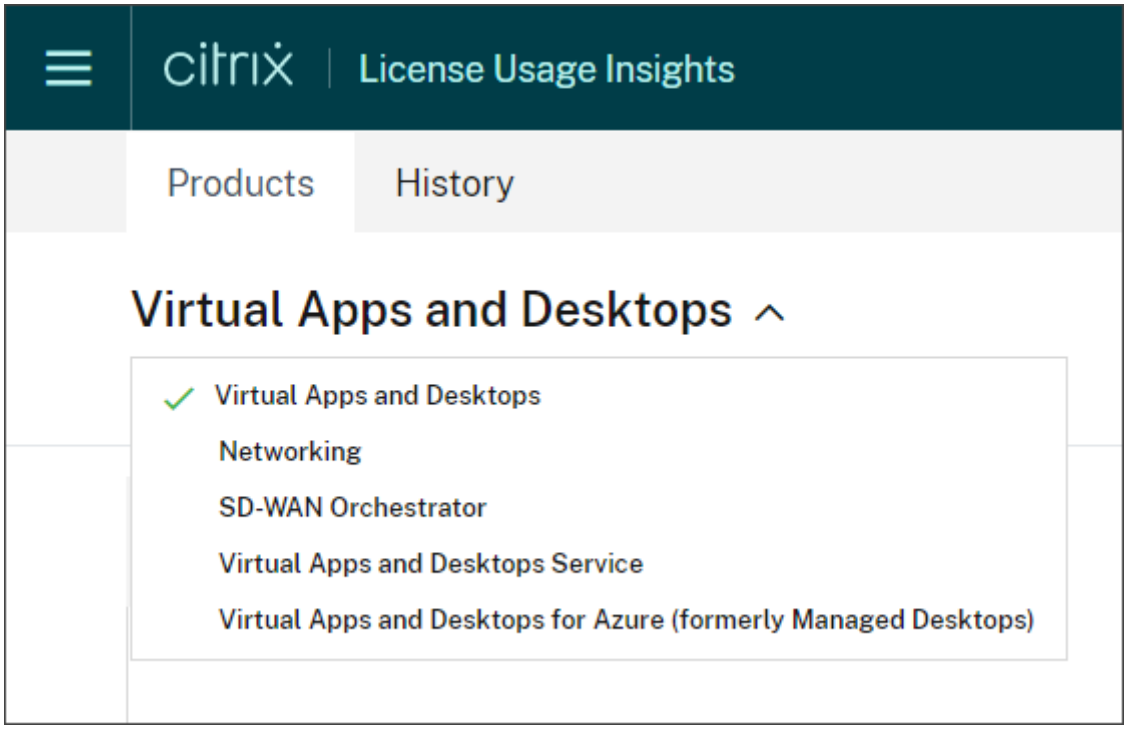
管理产品使用情况、许可证服务器和通知

July 1, 2024

产品选择

要查看其他产品的许可详细信息，请单击产品名称旁边的箭头，然后选择要查看的产品或服务。

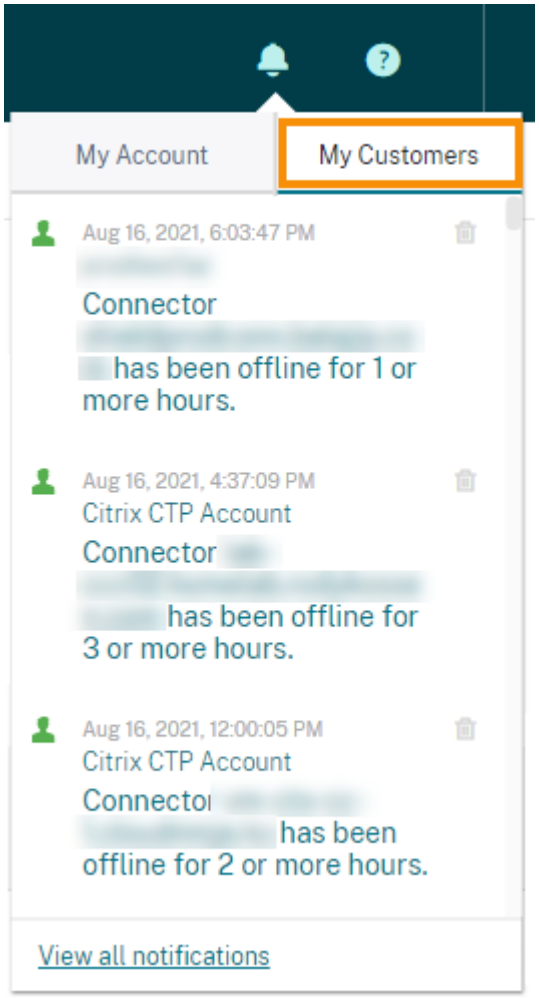
© 1999–2024 Cloud Software Group, Inc. All rights reserved.



客户通知

无需单独访问每个部署，即可监视多个客户的解决方案运行状况。Citrix Cloud 中的“Notifications”（通知）区域在您的控制板上汇聚多个客户的通知，以便您能够保证解决警报问题并且服务保持运行。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



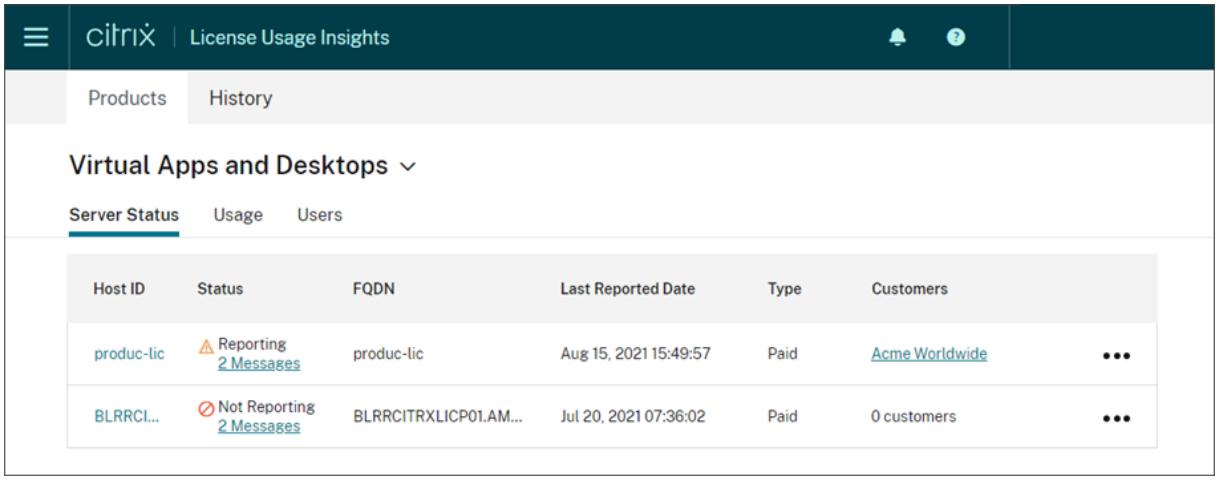
1. 在 Citrix Cloud 管理控制台中，单击 通知 图标，然后单击 我的客户。此时将显示最新通知的列表。
2. 要查看客户通知的完整列表，请单击 查看所有通知。

许可证服务器状态

必须更新并报告所有活动的许可证服务器，以遵从 Citrix Service Provider 许可证的指导原则。许可证服务器状态显示您拥有的许可证服务器，以及它们是否已更新以便与 License Usage Insights 一起使用。

此服务将显示使用 Citrix 后端办公系统中存储的许可证分配数据的活动许可证服务器列表。如果许可证服务器已更新并成功报告，License Usage Insights 将显示“报告”状态并包含最近上载的时间戳。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



上载中包含的许可证服务器信息

在许可证服务器上激活 Call Home 后，每天都会上载以下信息：

- 许可证服务器版本
- 许可证文件信息：
  - 服务器上安装的许可证文件
  - 许可证文件过期日期
  - 产品功能和版本授权信息
  - 许可证数量
- 许可证使用情况：
  - 当前日历月中使用的许可证
  - 与许可证签出相关联的用户名
  - 激活的产品功能和版本

查看许可证服务器上载

CSP 合作伙伴可以检查其许可证服务器上上次上载的负载，以充分理解许可证服务器向 Citrix 发送的所有详细信息。此负载的副本在许可证服务器上存储为.zip 文件。默认情况下，此位置为 C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip。

> 注意：
>
> 将删除除最后一个上载以外的成功上载。不成功的上载将继续保留在任务中，直至成功上载。出现该问题时，将删除除最后一个上载以外的所有上载。

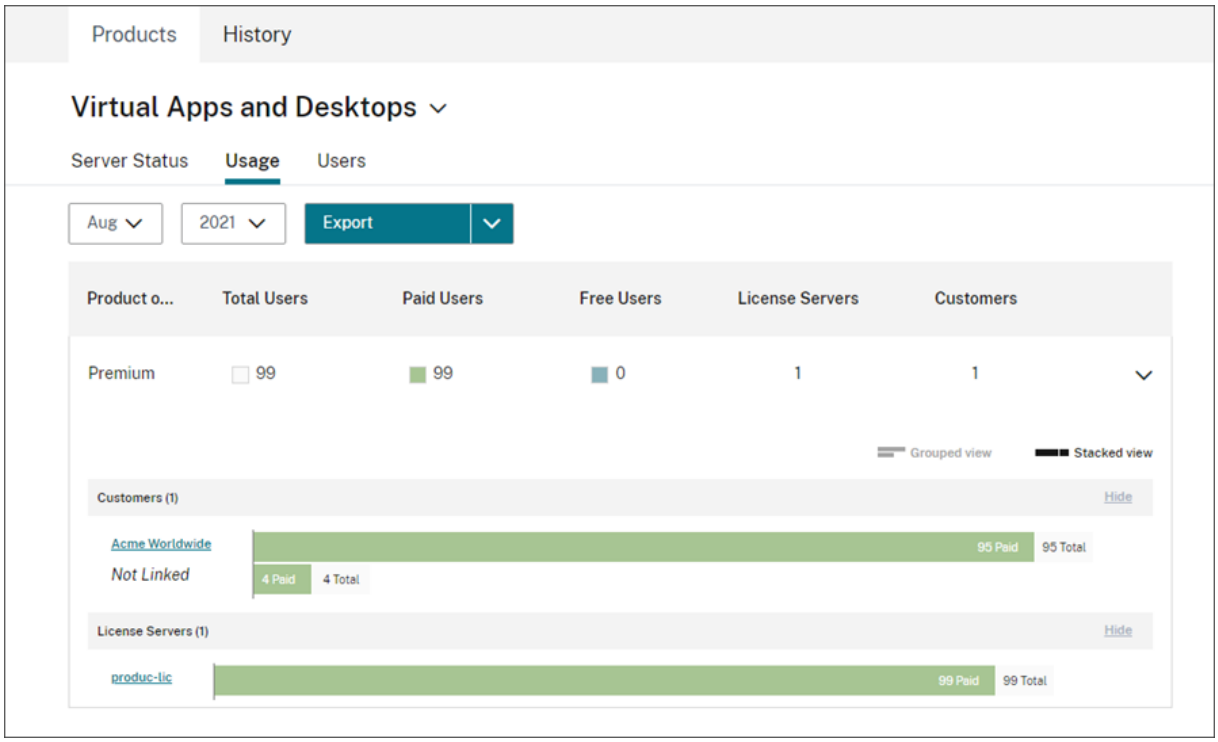
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用情况收集

使用情况收集有助于您通过自动化的数据收集和汇总来理解产品使用情况。不需要部署其他工具。

许可证使用情况见解会自动汇总所有 Citrix 许可证服务器的产品使用情况，以提供所有部署的完整使用情况视图。还可以通过将特定用户与其所属的客户或租户相关联来创建许可使用情况细分。

许可证服务器将收集和跟踪产品许可证使用情况，并使用安全的挂断电话后自动返回到主界面渠道将其报告回 Citrix。这一自动化方式向您提供恒定不变的更新后的使用数据的数据流，节省了时间并且有助于合作伙伴更好地理解其部署内部的使用趋势。



创建 **Virtual Apps and Desktops** 产品使用情况的客户细分

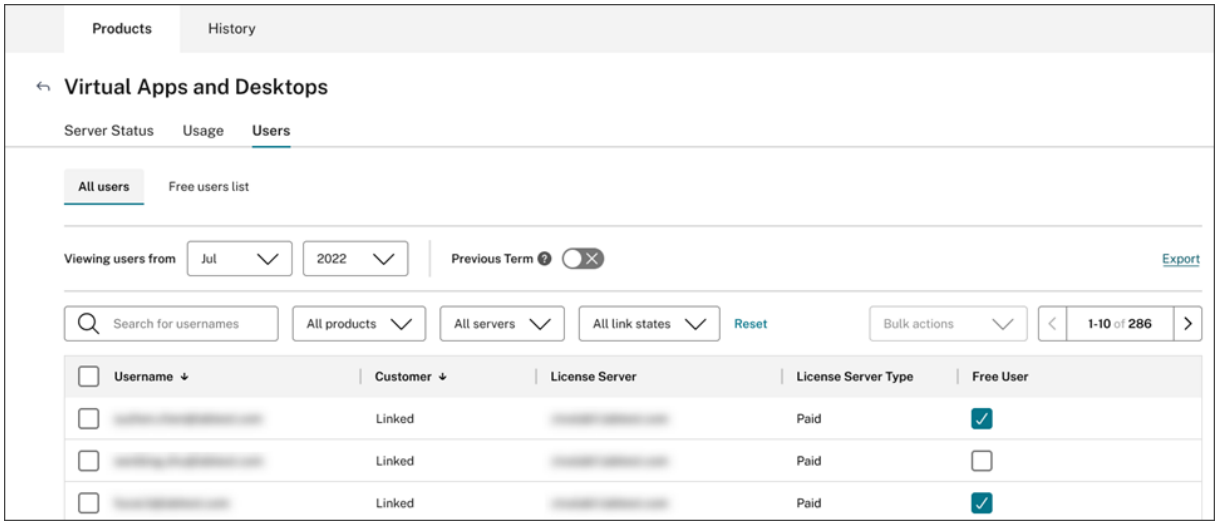
必须先将用户与其所属的客户或租户相关联，才能按客户细分许可使用情况。如果您未在自己的“Customers”（客户）控制板中定义任何客户，则可以添加新客户，也可以与现有 Citrix Cloud 客户建立连接。

1. 如果适用，将客户添加到客户控制面板：在 Citrix Cloud 管理控制台主页上，单击“客户”，单击“添加”或“邀请”，然后按照屏幕上的说明进行操作。
2. 单击菜单按钮，然后选择 我的服务 **>** 许可证使用情况见解。
3. 选择“**Virtual Apps and Des** ktops”产品后，单击“用户”。
4. 选择要关联的用户，然后单击“批量操作”**>**“管理客户链接”。
5. 在列表中，选择要将用户关联到的客户。
6. 单击保存。
7. 要查看每个客户的细分，请单击 使用 情况视图。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

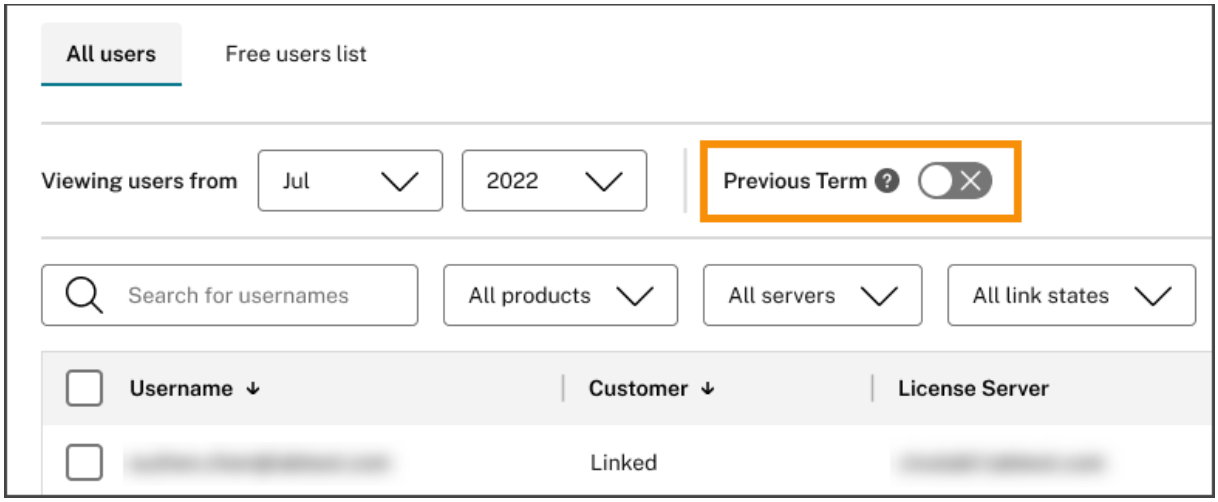
免费用户管理

License Usage Insights 提供跨部署的产品使用情况的全面视图，同时仍允许您充分利用支持试用、测试和管理用户的 Citrix 服务提供商许可证计划。



为确保在给定的计费周期内向付费用户收取适当的账单，您可以在该周期内将某些用户指定为免费用户。在当前计费周期的给定月份内，您可以随时选择免费用户，直到下个月的第 10 天。例如，在 3 月，您可以在 4 月 10 日之前随时选择免费用户。

在每个月的第一天和第十天之间，您还可以选择前一个计费周期的免费用户。在此期间，您可以启用“上一学期”设置，然后选择该计费周期的免费用户。在当月的第 10 天之后，Citrix Cloud 不再显示 上一学期 设置。



当您为付费用户计费时，您在给定月份中选择的免费用户会被考虑在内。当您将免费用户的状态更改为付费用户时，Citrix 会记录更改日期，并将该用户包括在发生更改的计费周期中。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

用户客户标记

此功能提供每位客户的许可证使用情况明细，包括支持管理和报告单租户和多租户许可证服务器架构。许可证使用情况洞察的对象是：

- 许可证服务器 - 列表上的“报告”或“未报告”许可证服务器。
- 用户 - 在 Call Home 使用数据中找到的单个用户名。
- NetScaler - 单个 NetScaler VPX 许可分配（VPX 列表上的 VPX）。

> 注意
>
> 用户客户标记功能与免费用户标记功能具有相同的行为，在该功能中，CSP 可以在下个月的 10 日之前更新当前计费周期的客户标记。

免费服务器标记

此功能使管理员能够根据其特定角色、位置或任何其他相关标准组织和识别服务器，而不必担心许可影响，从而灵活地管理 Citrix Cloud 环境中的资源。

> 注意
>
> CSP 只能修改本月的免费标签或客户标记，更改适用于当前月份和未来月份。

服务器客户标记

此功能可以更好地组织和管理 Citrix Cloud 环境中的资源，确保根据客户的特定需求对服务器进行标记。通过使用服务器客户标记，管理员可以轻松识别和跟踪与不同客户相关的资源，从而提高资源分配和管理的效率。

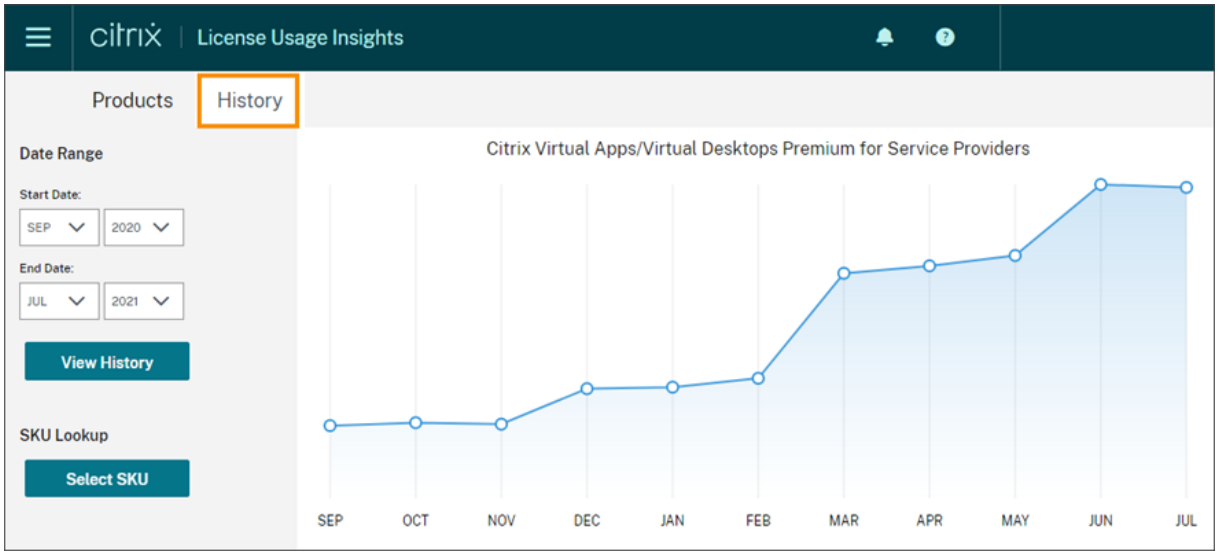
> 注意
>
> CSP 只能修改本月的免费标签或客户标记，更改适用于当前月份和未来月份。

历史趋势

可以查看您过去与 Citrix 的所有业务的完整历史记录。可以检查您上个月、去年或可配置的一段时间内报告的使用情况。

历史视图提供有价值的业务见解。作为 Citrix Service Provider 计划的成员，您可以快速地了解您与 Citrix 的业务发展趋势以及哪些产品在您的客户和订阅者中呈现最快速的增长。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



导出使用情况和分配数据

您可以从“许可证使用情况见解”中将以下类型的数据导出为 CSV 文件：

- 指定月份的 Virtual Apps and Desktops 产品使用情况和用户列表
- 当前 NetScaler VPX 的分配详细信息

1. 从产品列表中选择 **Virtual Apps and Desktops** 或网络。
2. 如果适用，请选择要导出的视图。例如，要导出 Virtual Apps and Desktops 使用情况详细信息，请单击 使用情况 视图。
3. 如果适用，请选择要导出的月份和年份。
4. 在屏幕右侧，单击“导出”。

使用 **API** 访问许可数据

Citrix 提供了多个 API，您可以使用它们在 Citrix Cloud 之外访问许可数据。要了解有关这些 API 的更多信息，请参阅 Citrix Developer 文档中的用于管理 Citrix Cloud 许可的 API。

要使用这些 API，必须先创建安全客户端并生成不记名令牌。要创建安全客户端，您必须在 Citrix Cloud 中拥有安全客户端权限。有关更多信息，请参阅 控制台权限。

有关使用 Citrix Cloud API 所需任务的更多信息，请参阅 Citrix Developer 文档中的 Citrix Cloud API 入门。

分销商对 **API** 的访问权限

您可以允许您的 Citrix 分销商通过 Citrix Cloud API 访问您的许可数据，而无需授予他们对您的 Citrix Cloud 帐户的完全管理员访问权限。您可以这样做，这样您的分销商就可以验证您的使用情况报告并确保账单准确无误。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

要向分销商提供对您的许可数据的访问权限，您可以创建一个自定义访问管理员，其权限仅限创建安全客户端和访问许可证使用情况见解服务。此帐户对 Citrix Cloud API 的访问权限有限，无法访问其他 Citrix Cloud 功能。创建帐户后，您可以与分销商共享帐户凭据，以便他们可以登录您的 Citrix Cloud 帐户并创建使用 Citrix Cloud API 所需的安全客户端。或者，您可以以自定义访问管理员身份登录，创建安全客户端，然后与分销商共享安全客户机详细信息。

要为您的分销商创建自定义访问帐户，请执行以下操作：

1. 专门为您的 Citrix 分销商创建一个新的管理员帐户。有关说明，请参阅 邀请个人管理员。
2. 在 设置访问权限中，选择 自定义访问 权限，然后选择以下权限：
    - 一般信息 **>** 安全客户端
    - 许可证使用情况洞察 **>** 许可证使用洞察：分销商访问权限

要创建安全客户端，请执行以下操作：

1. 使用新帐户的凭据登录 Citrix Cloud。
2. 按照 Citrix Cloud API 入门中所述创建新的安全客户端。
3. 记下 Citrix Cloud 生成的客户端 ID 和客户端密钥。这些详细信息是所有 Citrix Cloud API 的必填输入。

分销商可用的许可数据

本节介绍您的 Citrix 分销商可以使用您提供的安全客户端详细信息访问的许可数据和 API。使用以下链接了解有关每个 API 的更多详细信息。

CSP 报告虚拟应用程序和桌面许可证的每月和历史使用情况（许可证使用情况见解）：

- Virtual Apps and Desktops 当前使用情况
- Virtual Apps and Desktops 历史使用情况

CSP 报告单租户和多租户云许可证使用情况（许可证使用情况见解）：

- DaaS 的当前使用情况
- DaaS 的历史使用情况

CSP 的云许可证使用情况（许可）：

- DaaS 的当前使用情况
- DaaS 的历史使用情况

租户的云许可证使用情况（客户控制面板-> 查看许可）

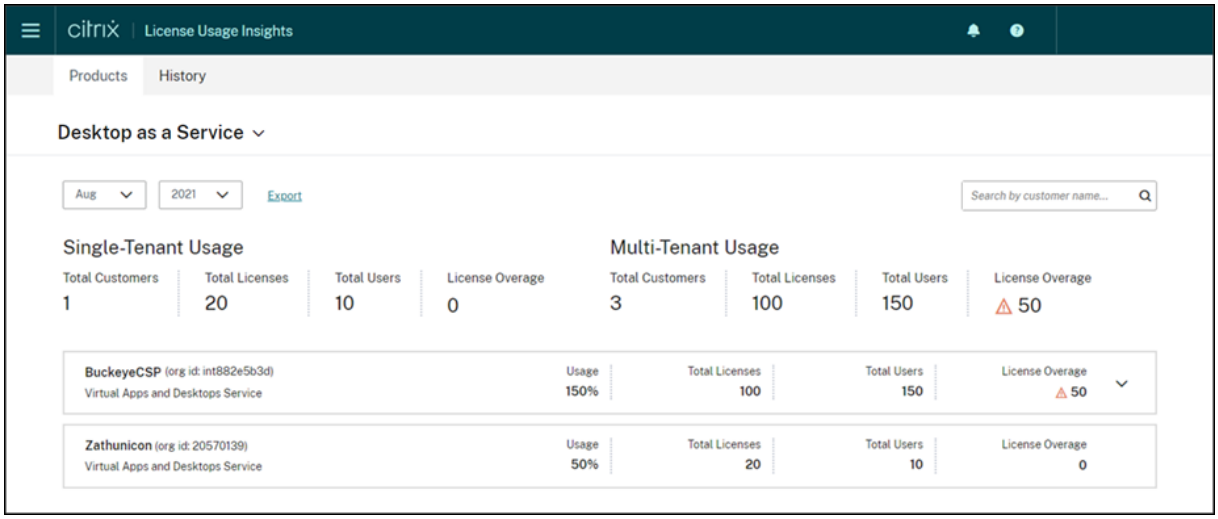
- DaaS CCU 当前使用情况
- DaaS CCU 的历史使用情况
- DaaS UD 当前使用情况
- DaaS UD 历史使用情况

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 服务提供商的云服务许可证使用情况和报告

October 5, 2023

License Usage Insights 会自动汇总云服务使用情况，以提供所有单租户客户和多租户合作伙伴的完整视图。您还可以将给定月份的这些详细信息导出到 CSV 文件以供进一步分析。



支持的服务

Citrix DaaS Premium（以前称为 Virtual Apps Premium 和 Virtual Apps and Desktops Premium）可以使用单租户许可证。

多租户许可证可用于以下服务：

- Citrix DaaS（以前称为 Virtual Apps and Desktops 服务）
- Citrix DaaS Standard for Azure（以前称为适用于 Azure 的 Virtual Apps and Desktops Standard）

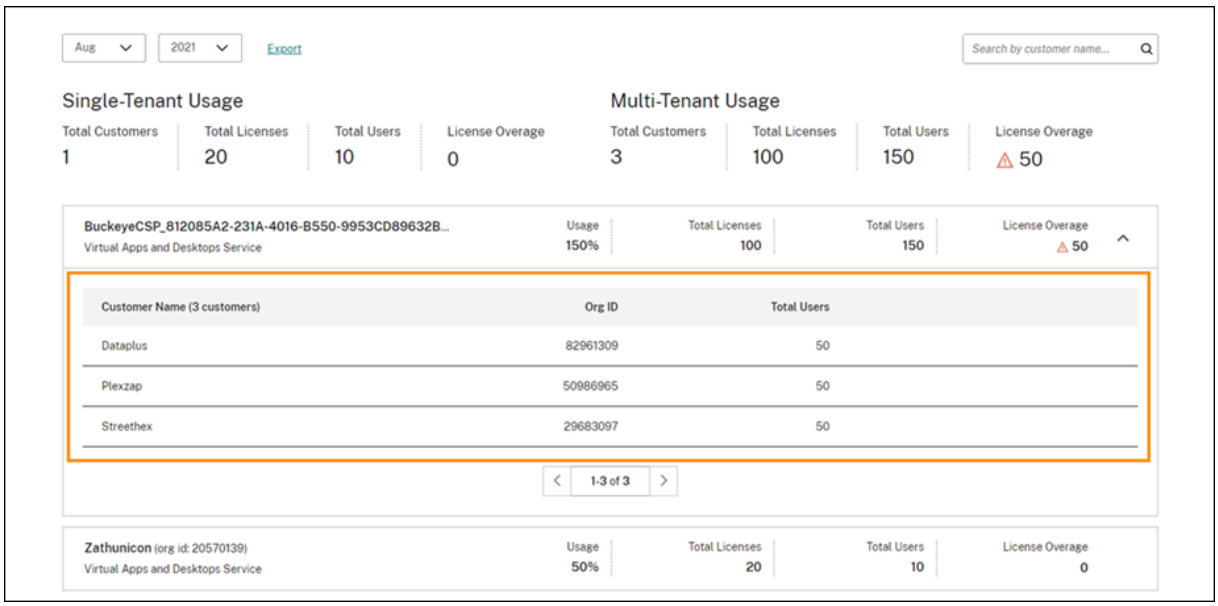
许可摘要

许可证使用情况见解为 Citrix Service Provider (CSP) 的单租户和多租户使用情况提供了以下明细：

- 按租户类型分组的概览摘要，包括客户总数以及所有客户购买的许可证、用户和超额分配许可证的总数。
- 每个客户或合作伙伴的使用情况摘要，包括使用中的许可证总数的百分比、已购买的许可证总数、用户数以及超额分配的许可证数量。

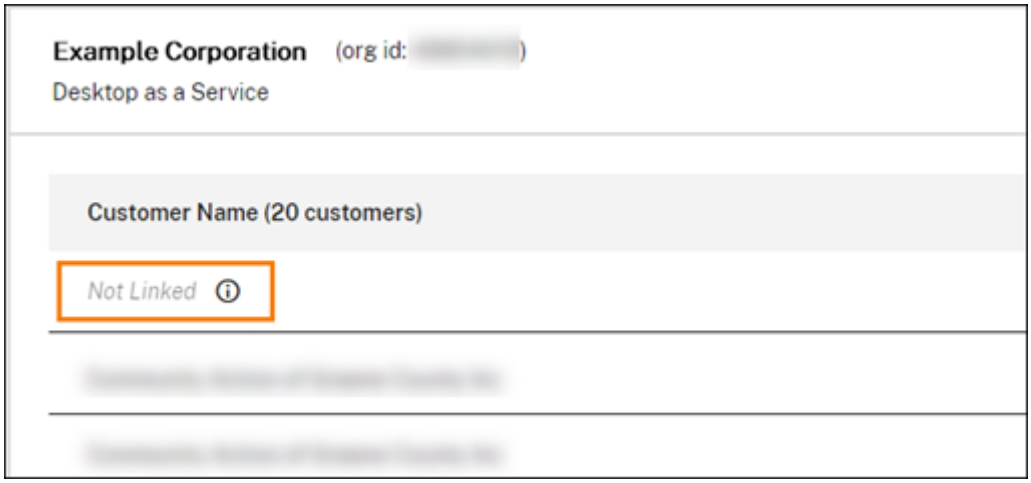
对于多租户服务，您可以展开使用情况摘要以查看与每个合作伙伴关联的客户、OrgID 和总用户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



租户客户未关联

在某些情况下，租户客户可能会被列为“未关联”。当该租户的用户通过 CSP 的工作区 URL 而不是租户工作区 URL 访问云服务时，就会出现这种状态。



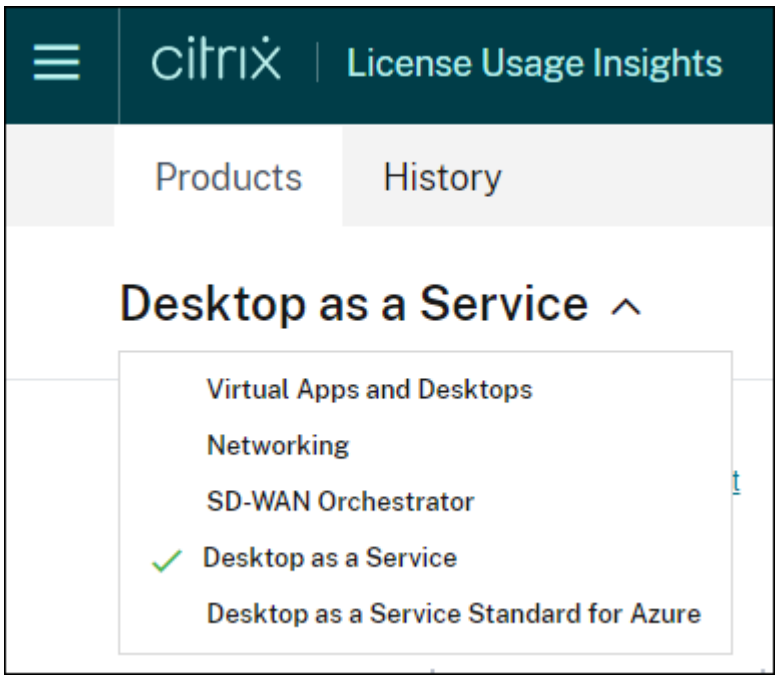
当租户用户通过租户工作区 URL 访问服务时，Citrix Cloud 会将该用户视为属于租户，“未链接”消息将被删除。

查看和导出每月使用量

您可以随时查看所有客户和合作伙伴前几个月的许可证使用情况。您也可以将此数据导出到 CSV 文件以供进一步分析。对于 Citrix DaaS Standard for Azure，您还可以导出每月消耗数据。

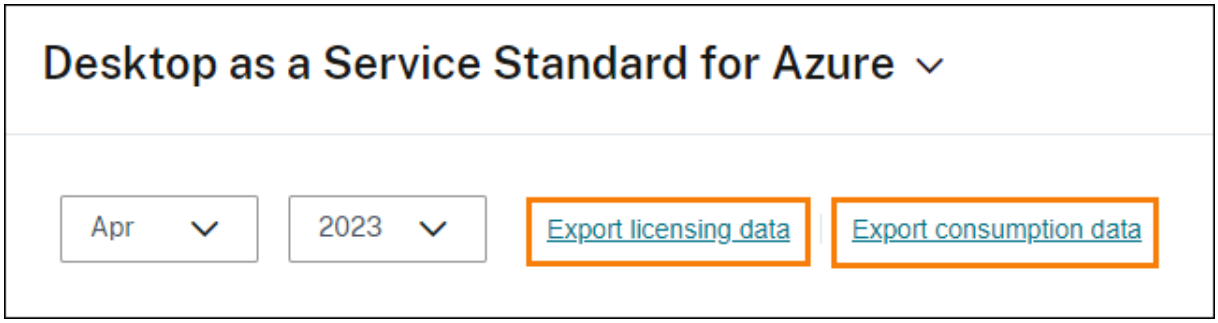
1. 从产品菜单中，选择要查看的云服务。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



对于 Citrix DaaS，选择要查看的月份和年份，然后选择 导出。

对于 Citrix DaaS Standard for Azure，选择要查看的月份和年份，然后选择 导出许可数据 或 导出使用数据。



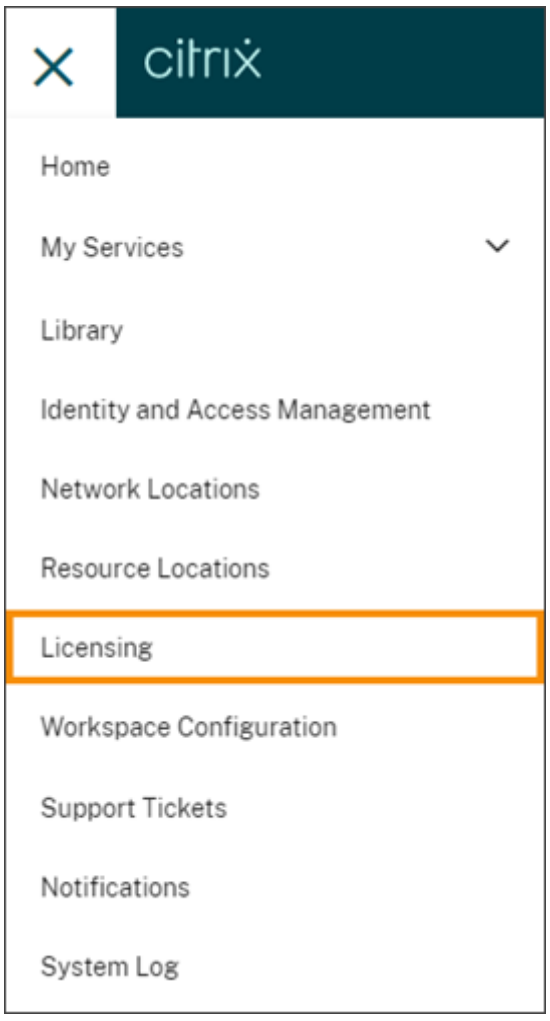
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix DaaS 的客户许可证和使用情况监视

October 5, 2023

Citrix Service Provider (CSP) 的客户可以在 Citrix Cloud 中轻松监视其用户的 Citrix DaaS 许可证。作为 CSP，您可以通过在 Citrix Cloud 中登录客户帐户来访问这些详细信息。要查看单租户和多租户客户的许可证使用情况汇总信息，请参阅 Citrix 服务提供商的云服务许可证使用情况和报告。

客户可以通过从 Citrix Cloud 菜单中选择 许可 来查看其许可数据。



许可证分配

用户/设备许可模式：当唯一客户用户在本月内首次启动应用程序或桌面时，Citrix Cloud 会分配许可证。

并发用户许可模式：当用户在其设备上启动应用程序或桌面时，Citrix Cloud 会分配许可证。当用户注销或断开会话连接时，将不再分配许可证。由于许可证分配可能会根据在任何给定时间访问应用程序或桌面的设备数量而变化，因此 Citrix Cloud 每五分钟评估一次正在使用的许可证数量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关并发许可模式的更多信息，请参阅“许可使用产品”文档中的并发许可证。

许可摘要

Citrix Cloud 显示用户/设备和并发用户许可模式下正在使用的许可证的摘要视图。

用户和设备摘要

对于用户/设备模式，许可摘要可让您一目了然地查看正在使用的许可证与您拥有的许可证总数的关系。

当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。

Citrix Cloud 还显示分配的许可证与购买的许可证的比率以及剩余的可用许可证数量。

并发用户摘要

对于并发用户模型，许可摘要提供了以下信息的一目了然的视图：

- Citrix Cloud 上次评估正在使用的许可证时，当前正在使用的已购买许可证总数的百分比。Citrix Cloud 根据与服务有活动连接的唯一设备每五分钟计算一次此百分比。购买的许可证总数是为使用并发许可模式的 Citrix DaaS 购买的许可证总数。
- 当前分配的许可证与已购买许可证总数的比率以及剩余的可用许可证数量。该比率中显示的总数数字代表当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计。在计算使用中的峰值许可证时，Citrix Cloud 将检索在以下时间段内使用的最大许可证数：
  - 过去 **24** 小时：过去 24 个时段内一次使用的最大许可证数。
  - 本月：自当前日历月开始以来一次使用的许可证的最大数量。
  - 所有时间：自订阅开始以来一次使用的最大许可证数。

  这些使用高峰时段显示的总数表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且分配的许可证相应增加，则 总 数将发生变化，以反映该时间点新的拥有许可证数量。但是，如果没有相应的使用峰值，则总数 不会改变。
- 活跃使用情况统计。Citrix Cloud 显示以下时段内唯一连接的总数：
  - 每月：上一个日历月的连接总数。
  - 每天：过去 24 小时的连接总数。这些数字也以这些时期拥有的许可证总数的百分比表示。

计算使用中的峰值许可证

为了准确反映并发许可模式，Citrix Cloud 每五分钟计算一次同时访问该服务的唯一设备数量。如果计数大于显示的当前峰值使用率，Citrix Cloud 将显示新的峰值使用情况以及达到该峰值的日期和时间。如果计数小于当前峰值使用量，则当前峰值使用量不会改变。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 重要：
>
> 如果您使用 Director 中的 Monitor 获取有关并发会话的信息，请注意，监视报告对并发会话的解释不同，并且不能准确反映正在使用的并发用户许可证的数量。有关监视报表和许可报告之间区别的更多信息，请参阅 常见问题解答。

计算每月活跃使用量

每个月初，Citrix Cloud 都会拍摄上一个日历月的快照。Citrix Cloud 显示该日历月内发生的唯一连接总数。

计算每日活跃使用量

每天的同一时间，Citrix Cloud 都会拍摄过去 24 小时的快照。Citrix Cloud 显示在该 24 小时内发生的唯一连接总数。

使用趋势

Citrix Cloud 显示用户/设备许可证或并发用户许可证的使用趋势明细。要查看此细目，请从许可摘要页面中选择查看使用情况详细信息。

用户和设备的趋势

对于用户/设备许可证，“使用趋势”部分以图表形式向您显示已分配许可证的明细。

指向图表上的时间间隔会显示以下信息：

- 许可证总数：您在所有授权中为云服务购买的许可证总数。
- 以前分配的许可证数量：上个月分配的许可证数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。在 8 月份，此许可证被视为“先前已分配”。
- 新分配的：每月分配的新许可证的数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。

并发用户的趋势

对于并发用户许可证，“使用趋势”部分向您显示以下信息：

- 许可证总数：您购买的并发许可证总数。
- 使用中的峰值许可证：为您选择的日期范围分配的最大许可证数。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要向下钻取到每月或每小时的高峰使用量，请从下拉菜单中选择要查看的日历月或日。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

如果您选择的日期范围尚未完成，Citrix Cloud 将显示最新时间间隔的当前峰值使用情况。例如，如果您向下钻取以查看仍在进行中的日历日，则会显示截至当前时刻每小时的最大许可证数量。如果许可证的最大数量在接下来的五分钟计数间隔内增加，Citrix Cloud 将更新当前小时的峰值使用情况。

- 活跃使用显示包含以下信息的图表：
  - 每天：过去 30 天内每天的连接总数。
  - 每月：上一个日历年中每个月的连接总数。

指向“许可证分配”或“活跃使用”图表上的间隔即可显示该间隔的详细信息。

许可用户

许可证活动 部分显示在当月内分配了许可证的个人客户用户的列表。此列表还显示每个用户所属的域、分配许可证的日期以及上次使用该服务的时间。

每月发放许可证

在每个月的第一天，上个月分配的许可证将自动发放。发生这种情况时，分配的许可证数量将重置为零，并清除许可客户用户的列表。当用户在新月内首次启动应用程序或桌面时，将重新分配许可。

查看月度许可证历史记录

在每个月的第一天，当分配的许可证数量重置为零时，许可证活动下方的上个月许可客户用户列表将被清除。但是，您可以随时访问前几个月的用户详细信息，并在需要时将其下载为 CSV 文件。

1. 在“许可证活动”部分中，选择该部分最右侧的“查看许可证历史记录”。
2. 选择要查看的月份。此时将显示所选月份的用户详细信息列表。
3. 要导出列表，请选择该部分最右侧的“导出到 **CSV**”，然后保存文件。

出口许可证详情

客户可以随时将获得许可的用户详细信息导出到 CSV 文件中，以供进一步分析。然后，客户可以根据需要使用 CSV 文件来分析许可证详细信息。

要导出当月的详细信息，请在“许可证活动”部分的最右侧选择“导出到 **CSV**”，然后保存文件。

要导出前几个月的详细信息，请生成选定月份的列表，如 查看每月许可证历史记录中所述。选择 导出为 **CSV** 并保存文件。

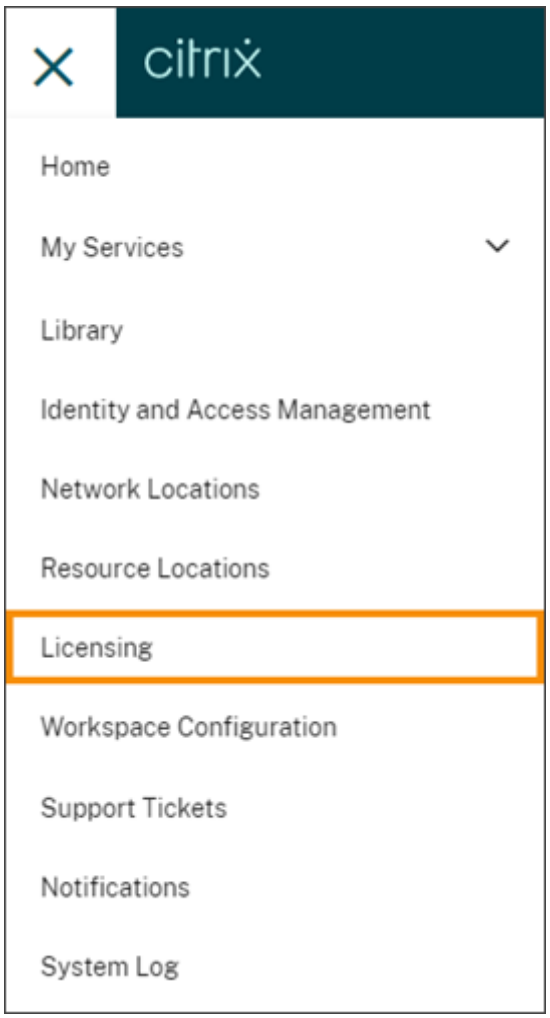
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix DaaS Standard for Azure 的客户许可证和使用情况监视

October 5, 2023

Citrix Service Provider (CSP) 的客户可以在 Citrix Cloud 中轻松监视其用户的 Citrix DaaS Standard for Azure 许可证。作为 CSP，您可以通过在 Citrix Cloud 中登录客户帐户来访问这些详细信息。要查看单租户和多租户客户的许可证使用情况汇总信息，请参阅 Citrix 服务提供商的云服务许可证使用情况和报告。

客户可以通过从 Citrix Cloud 菜单中选择 许可 来查看其许可数据。



许可证分配

用户/设备许可模式：当唯一用户或唯一设备首次启动桌面时，Citrix Cloud 会分配许可证。

并发用户许可模式：当用户在其设备上启动桌面时，Citrix Cloud 会分配许可证。当用户注销或断开会话连接时，将不再分配许可证。由于许可证分配可能会根据在任何给定时间访问桌面的设备数量而变化，因此 Citrix Cloud 每五分钟评估一次正在使用的许可证数量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

有关并发许可模式的更多信息，请参阅“许可使用产品”文档中的并发许可证。

许可摘要

Citrix Cloud 显示用户/设备和并发用户许可模式下正在使用的许可证的摘要视图。

用户和设备摘要

对于用户/设备模式，许可摘要可让您一目了然地查看正在使用的许可证与您拥有的许可证总数的关系。

当百分比接近 100% 时，百分比会从绿色变为黄色。如果百分比超过 100%，则该百分比变为红色。

Citrix Cloud 还显示分配的许可证与购买的许可证的比率以及剩余的可用许可证数量。

并发用户摘要

对于并发模式，许可摘要提供了以下信息的一目了然的视图：

- Citrix Cloud 上次评估正在使用的许可证时，当前正在使用的已购买许可证总数的百分比。Citrix Cloud 根据与服务有活动连接的唯一设备每五分钟计算一次此百分比。购买的许可证总数是为使用并发许可模式的 Citrix DaaS Standard for Azure 购买的许可证的总和。
- 当前分配的许可证与已购买许可证总数的比率以及剩余的可用许可证数量。该比率中显示的总数数字代表当前拥有的许可证总数（截至“上次报告”日期和时间）。
- 峰值使用情况统计。在计算使用中的峰值许可证时，Citrix Cloud 将检索在以下时间段内使用的最大许可证数：
  - 过去 **24** 小时：过去 24 个时段内一次使用的最大许可证数。
  - 本月：自当前日历月开始以来一次使用的许可证的最大数量。
  - 所有时间：自订阅开始以来一次使用的最大许可证数。

  这些使用高峰时段显示的总数表示当时拥有的许可证总数。如果拥有的许可证总数增加或减少，并且分配的许可证相应增加，则 总 数将发生变化，以反映该时间点新的拥有许可证数量。但是，如果没有相应的使用峰值，则总数 不会改变。

计算使用中的峰值许可证

为了准确反映并发许可模式，Citrix Cloud 每五分钟计算一次同时访问该服务的唯一设备数量。如果计数大于显示的当前峰值使用率，Citrix Cloud 将显示新的峰值使用情况以及达到该峰值的日期和时间。如果计数小于当前峰值使用量，则当前峰值使用量不会改变。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

使用趋势

Citrix Cloud 显示用户/设备许可证或并发用户许可证的使用趋势明细。要查看此细目，请从许可摘要页面中选择查看使用情况详细信息。

用户和设备的趋势

对于用户/设备许可证，“使用趋势”部分以图表形式向您显示已分配许可证的明细。

指向图表上的时间间隔会显示以下信息：

- 许可证总数：您在所有授权中为云服务购买的许可证总数。
- 以前分配的许可证数量：上个月分配的许可证数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。在 8 月份，此许可证被视为“先前已分配”。
- 新分配的：每月分配的新许可证的数量。例如，用户在 7 月份首次访问云服务并获得许可证。此许可证被视为 7 月份的“新分配”。

并发用户的趋势

对于并发用户许可证，“使用趋势”部分向您显示以下信息：

- 许可证总数：您购买的并发许可证总数。
- 使用中的峰值许可证：为您选择的日期范围分配的最大许可证数。默认情况下，Citrix Cloud 会显示当前日历年中每个月的峰值使用情况。要向下钻取到每月或每小时的高峰使用量，请从下拉菜单中选择要查看的日历月或日。

  如果您选择的日期范围尚未完成，Citrix Cloud 将显示最新时间间隔的当前峰值使用情况。例如，如果您向下钻取以查看仍在进行中的日历日，则会显示截至当前时刻每小时的最大许可证数量。如果许可证的最大数量在接下来的五分钟计数间隔内增加，Citrix Cloud 将更新当前小时的峰值使用情况。

指向图表上的时间间隔即可显示该时间间隔内使用的许可证总数和许可证峰值。

使用情况报告

您可以下载标准间隔或指定时间间隔的使用情况信息。
该信息包括以下各项的仪表使用情况：

- Azure VM
- 网络连接，例如 VNet 对等
- Azure 存储项目，例如托管磁盘、块 Blob 和页面 Blob

在一天/月结束后，数据可能需要长达 72 小时才能反映所有使用情况。

在“使用情况报告”下，选择间隔，然后选择“下载数据”以生成 CSV 文件并将其下载到本地计算机。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

许可用户

对于用户/设备许可证，“许可证活动”部分显示在当月内分配了许可证的个人客户用户的列表。此列表还显示每个用户所属的域、分配许可证的日期以及上次使用该服务的时间。本部分不适用于并发用户许可证。

每月发放许可证

在每个月的第一天，上个月分配的许可证将自动发放。发生这种情况时，分配的许可证数量将重置为零，并清除许可客户用户的列表。当用户在新月内首次启动应用程序或桌面时，将重新分配许可。

查看月度许可证历史记录

在每个月的第一天，当分配的许可证数量重置为零时，许可证活动下方的上个月许可客户用户列表将被清除。但是，您可以随时访问前几个月的用户详细信息，并在需要时将其下载为 CSV 文件。

1. 在“许可证活动”部分中，选择该部分最右侧的“查看许可证历史记录”。
2. 选择要查看的月份。此时将显示所选月份的用户详细信息列表。
3. 要导出列表，请选择该部分最右侧的“导出到 **CSV**”，然后保存文件。

出口许可证详情

您可以随时将单个客户的许可用户详细信息导出到 CSV 文件以供进一步分析。然后，您可以根据需要使用 CSV 文件来分析许可证详细信息。

要导出当月的详细信息，请在“许可证活动”部分的最右侧选择“导出到 **CSV**”，然后保存文件。

要导出前几个月的详细信息，请生成选定月份的列表，如 查看每月许可证历史记录中所述。选择 导出为 **CSV** 并保存文件。

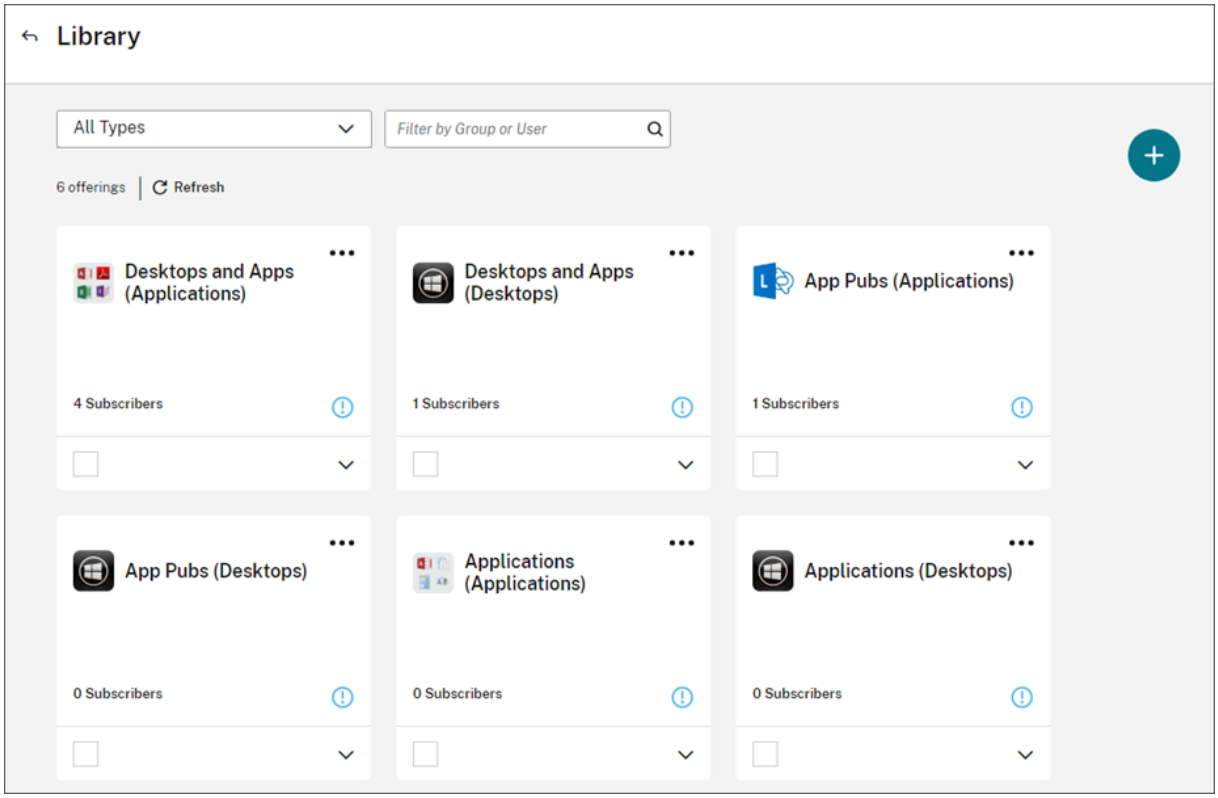
使用库向服务产品分配用户和组

April 26, 2024

> 注意：
>
> 对于由 *Citrix Cloud* 管理的交付组，现在可以直接在 Web Studio 控制台中管理用户分配。有关更多信息，请参阅 DaaS 文档。以前，这些交付组的管理仅限于资源库，但现在您可以在 Web Studio 控制台中使用相同的管理功能。此功能现已对所有客户上线。2024 年 6 月，云库中特定于 DaaS 的用例将完全弃用。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

您可以使用库将您在服务中配置的资源或其他项目分配给 Active Directory 用户和组。服务产品可能由通过 Citrix 服务创建的应用程序、桌面、数据共享和 Web 应用程序组成。库在单个视图中显示您的所有服务产品。



管理员访问权限

要访问资源库，管理员必须满足以下要求：

- 通过 Citrix 身份提供商或 Azure AD 进行身份验证。
- 以个人管理员身份登录，而不是以管理员组成员的身份登录。
- 拥有对 Citrix Cloud 的完全访问权限或选择资源库角色的自定义访问权限。

如果您在 Citrix Cloud 中有个人和组管理员帐户，则您对库的访问权限可能取决于您使用每个帐户登录时生效的权限。有关更多信息，请参阅拥有 Citrix、AD、Azure AD 和 Google Cloud 身份的管理员的结果权限。

在 **Citrix DaaS** 上使用 **StoreFront** 的注意事项

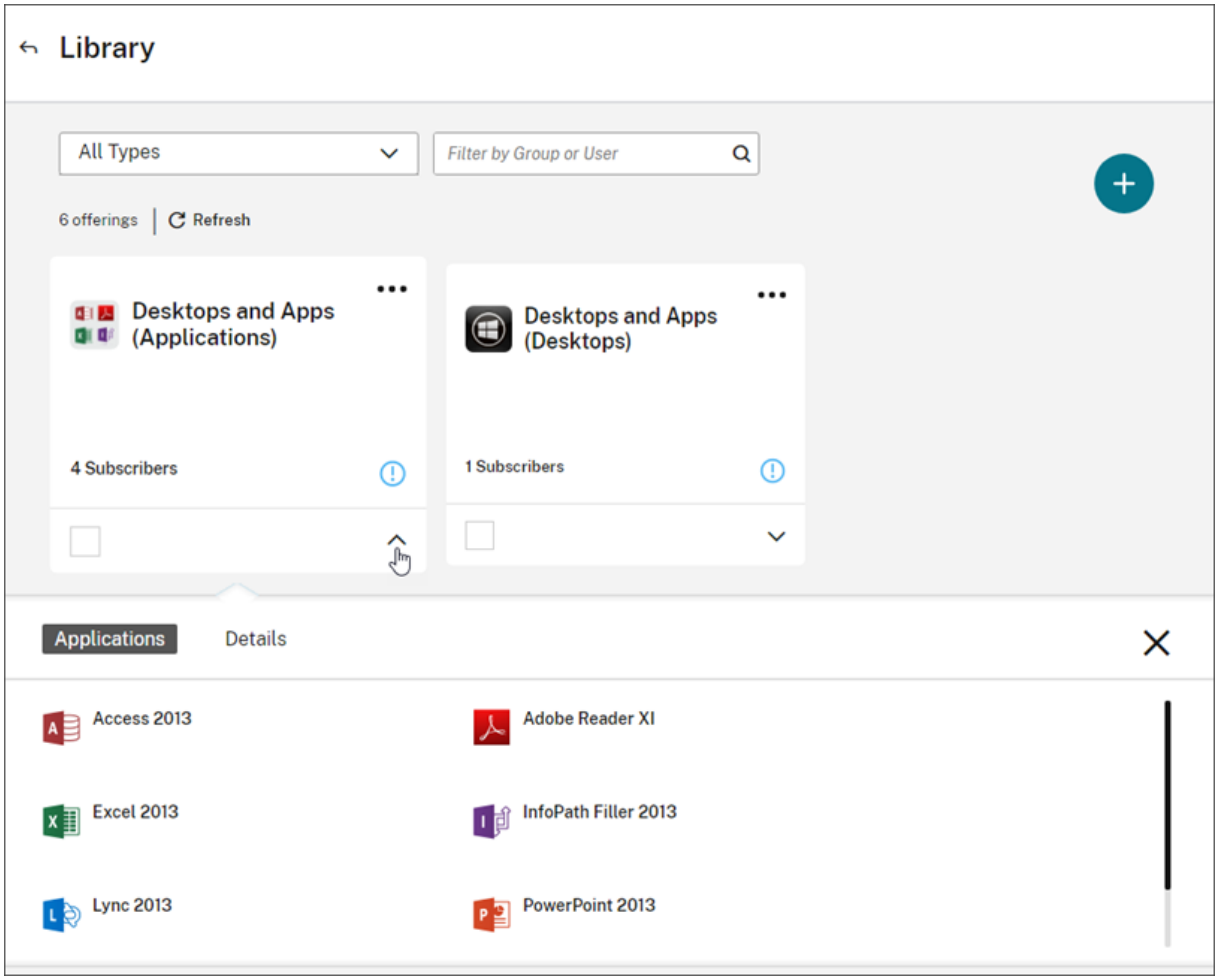
如果将本地 StoreFront 与 Citrix DaaS 结合使用，请勿在创建交付组时使用库来分配资源。相反，使用 Studio 将资源分配给用户。如果在这种情况下使用库，则可能不会向用户枚举资源。

在 Studio 中创建交付组时，请勿在 用户 页面上选择将 用户管理权留给 **Citrix Cloud**。而是选择其他选项（允许任何已通过身份验证的用户使用此交付组或限制以下用户使用此交付组）。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

查看服务产品详细信息

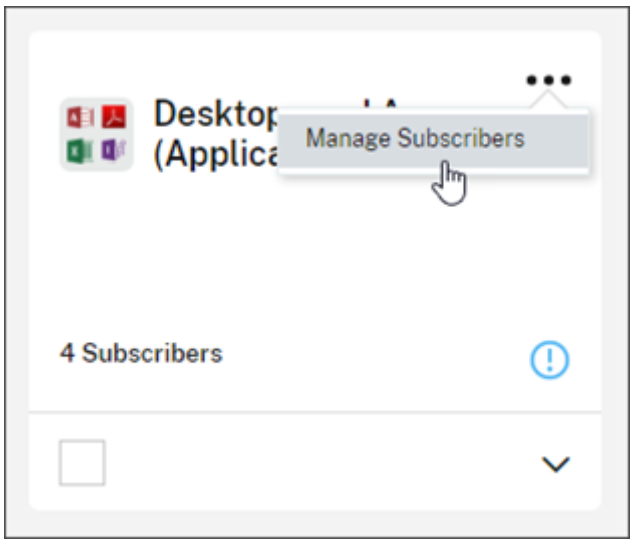
要查看应用程序、桌面、策略以及任何其他相关服务产品信息，请单击服务产品卡上的箭头。



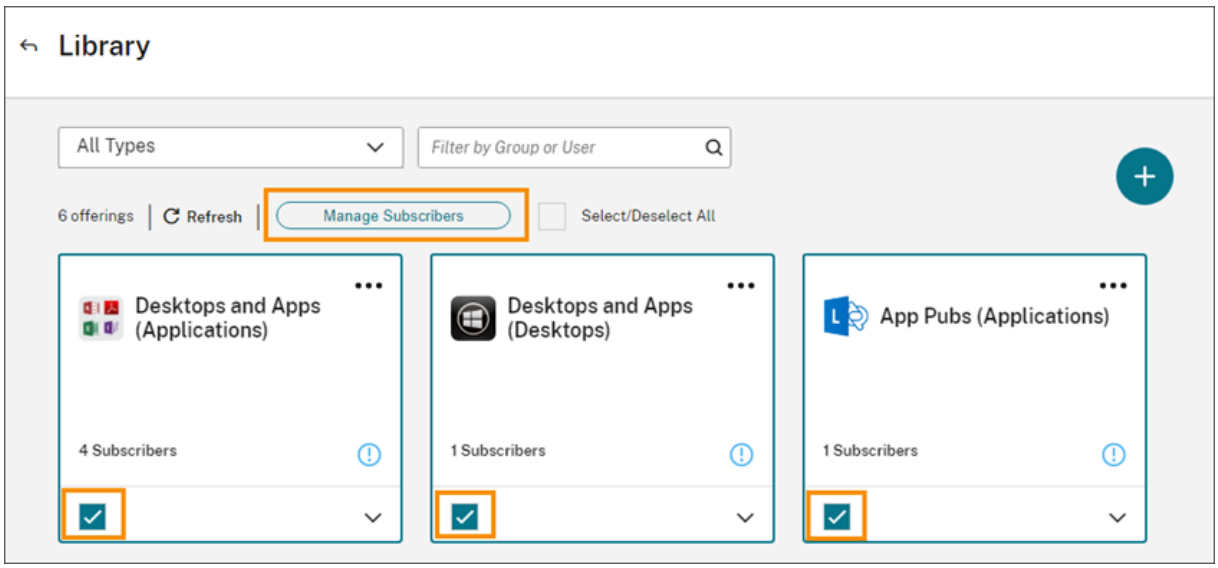
添加或删除订阅者

要管理单个既定课程的用户或组，请点击产品卡片菜单中的 管理订阅者。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

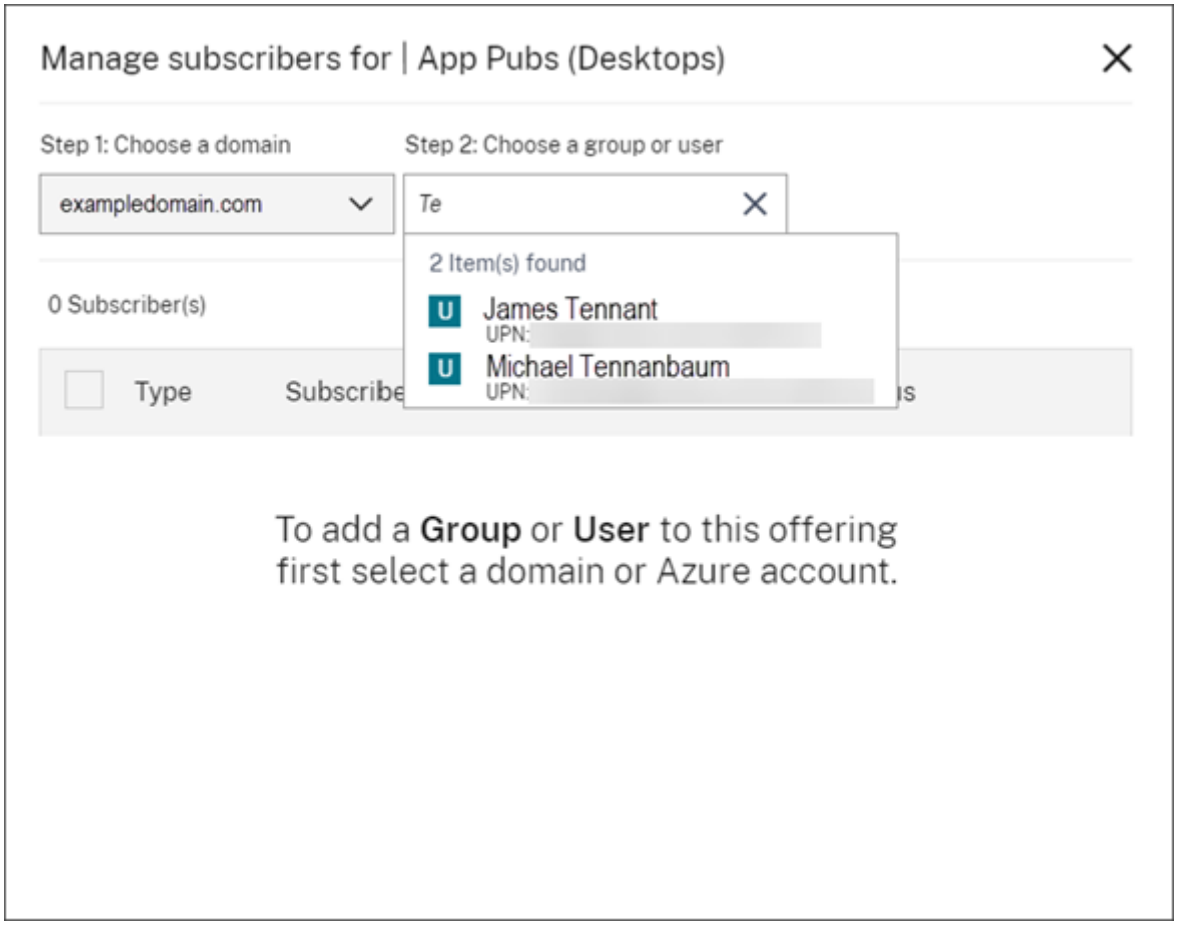


要管理多个产品的订阅者，请选中每个产品上的复选标记，然后单击 管理订阅者。



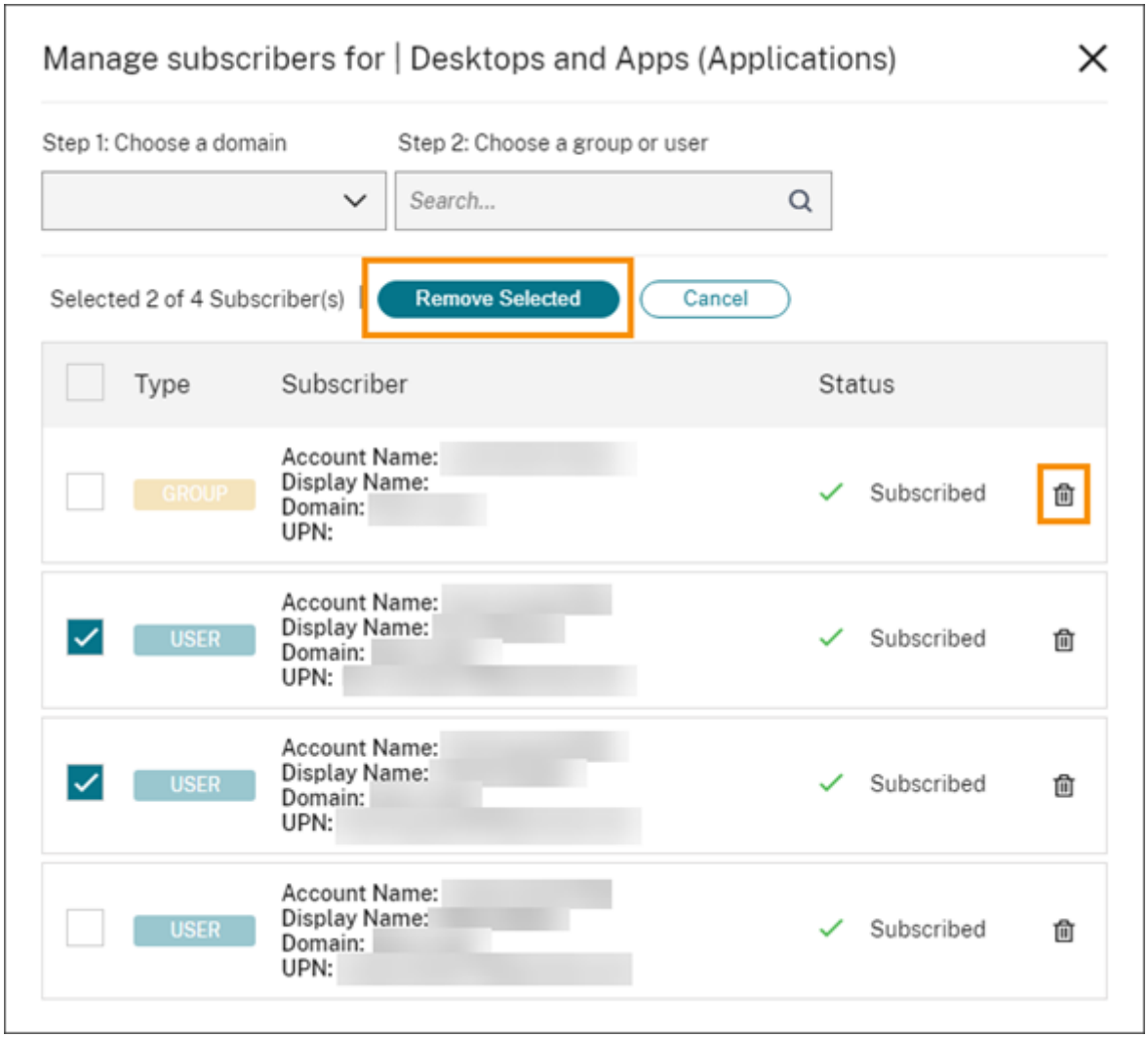
要向服务产品中添加订阅者，请选择一个域，然后选择要添加的用户或组。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要删除单个订阅者，请单击某个用户或组对应的垃圾桶图标。要删除多个订阅者，请选择用户或组，然后单击 移除选定项。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

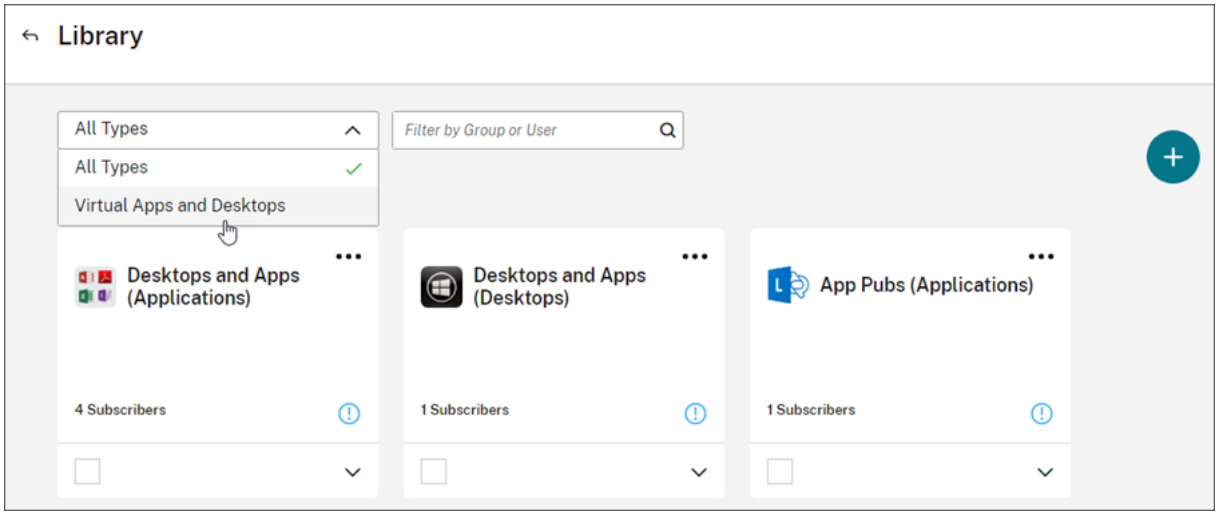


在服务产品中添加或删除订阅者后，服务产品卡将显示当前订阅者的数量。

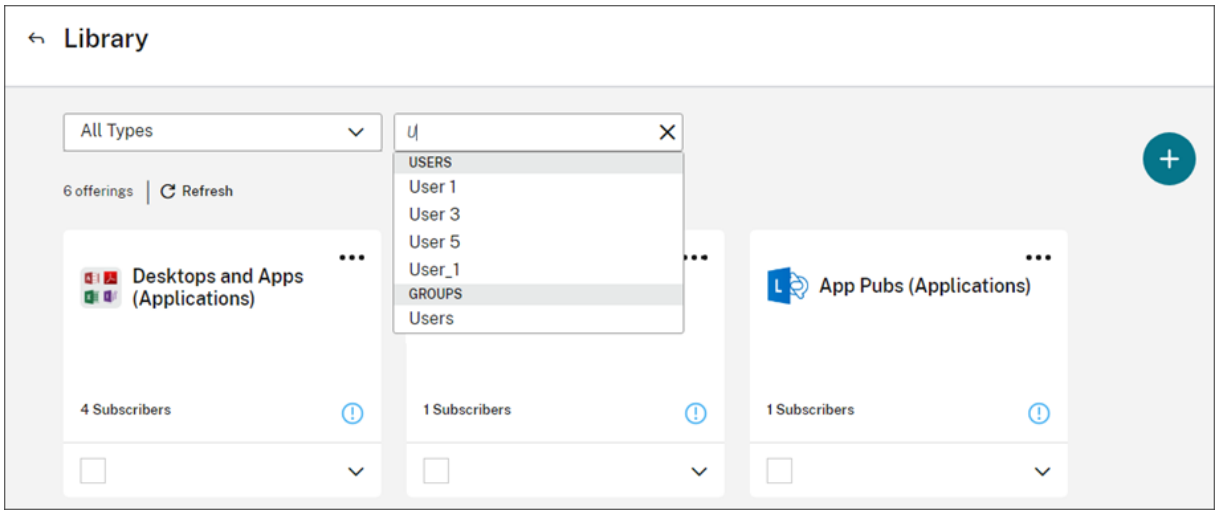
过滤服务产品

默认情况下，库将显示所有服务产品。要快速查看某项特定服务的服务产品，请选择该服务对应的过滤器。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



还可以在库中搜索当前订阅了某个服务产品的任何用户或组。Citrix Cloud 仅显示与您选择的用户或组有关的服务产品。要查看所有用户的所有服务产品，请单击 X 清除过滤器。



自定义登录页面

April 5, 2024

许多管理员访问云控制台来执行特定任务，例如在 Web Studio 控制台中管理应用或在 DaaS-监视中查看数据。但是，这些任务需要管理员每次登录时多次点击并浏览多个页面，这可能很耗时。这项新功能允许管理员设置或修改自定义登录页面，从而节省时间并提供增强的主机体验。

当前，可以将以下页面配置为自定义登录页面，预计将来还会添加更多页面：

- DaaS
- DaaS-Monitor

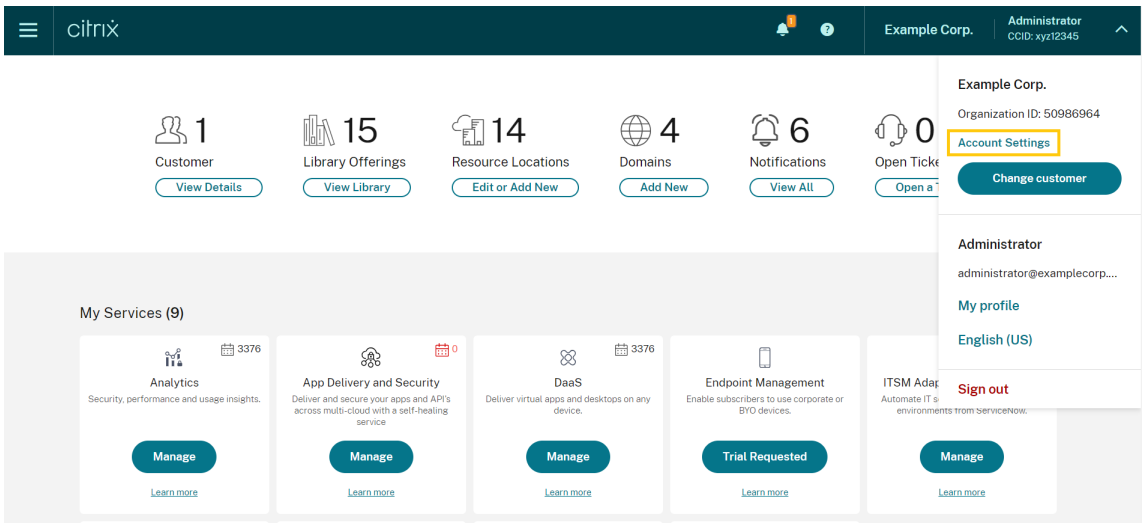
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- NetScaler 控制台
- CAS
- CAS 安全
- CAS 性能
- WEM
- 常规

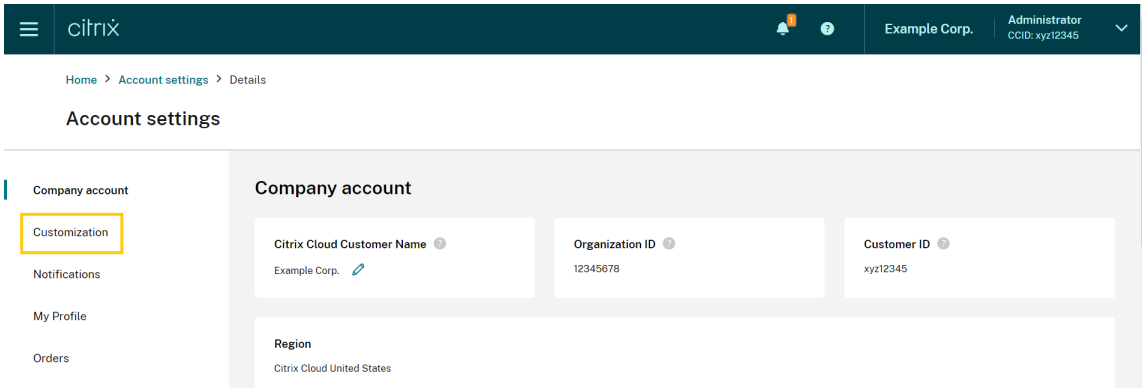
> 注意：
>
> 自定义登录页面设置是可选的，是针对每个帐户设置的。因此，每位管理员都可以在 Citrix Cloud 中自定义自己的体验。所有管理员（无论是自定义管理员还是完全管理员）都可以访问此功能。

配置自定义登录页面

1. 单击配置文件名称，然后选择帐户设置。

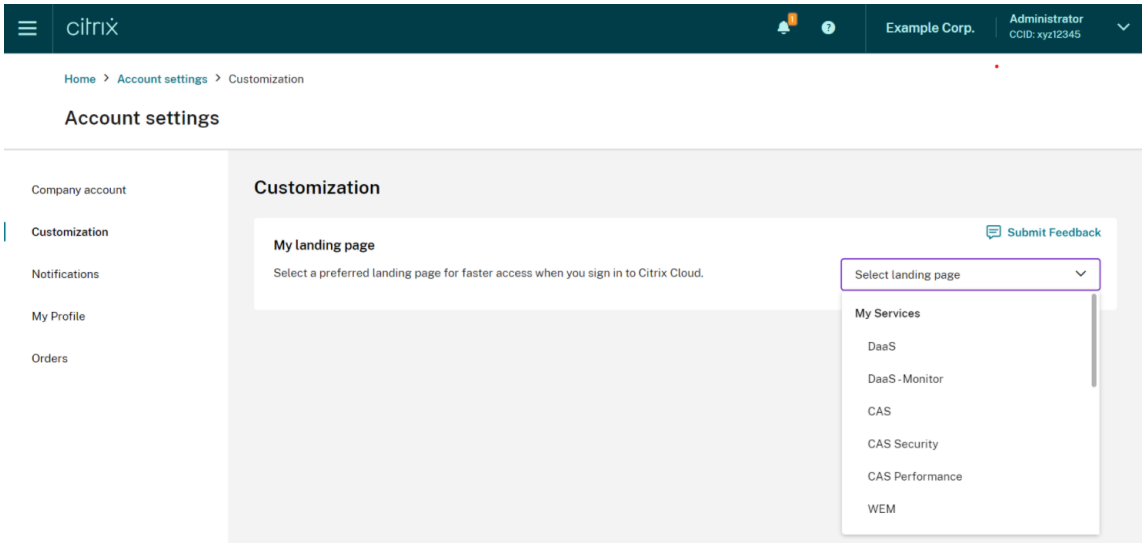


2. 单击“自定义”。



3. 选择您要配置为自定义登录页面的服务。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



4. 单击应用。

   您的自定义登录页面现已设置完毕。

> 注意：
>
> - 通过单击重置为默认值，您可以随时将自定义登录页面重置为默认 Cloud 主页。
> - 如果您在刚刚注销的同一页面上再次登录，它将带您进入上次查看的页面，而不是新的登录页面。

允许客户删除 **Citrix Cloud** 帐户并重新载入

April 26, 2024

Citrix Cloud 使客户能够安全删除其 Citrix Cloud 帐户，并在需要时无缝重新登录。

必备条件

- 如果您的帐户拥有有效的 DaaS 授权且您的 DaaS 环境已预配，请在继续操作之前联系 Citrix 技术支持以执行快速停用。有关如何检查您的 DaaS 环境是否已预配的详细信息，请参阅 Studio 控制台显示“启用 DaaS”以供首次使用一文。
- 删除与此帐户关联的所有 Cloud Connector 和 Connector Appliance。

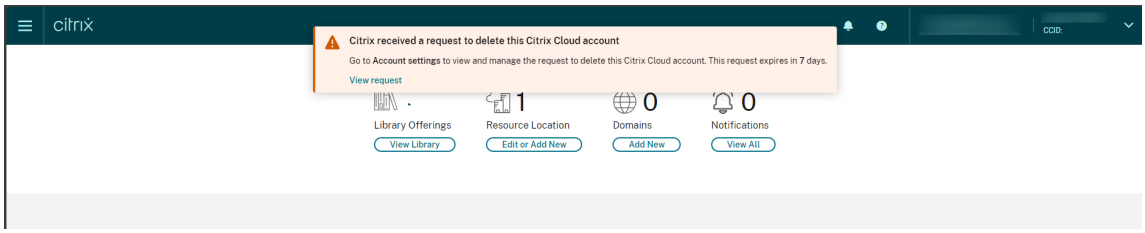
> 重要
>
> 在删除 Citrix Cloud 帐户之前，请注意以下几点：
>
> - 所有与客户相关的数据都将从 Citrix 数据库中删除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

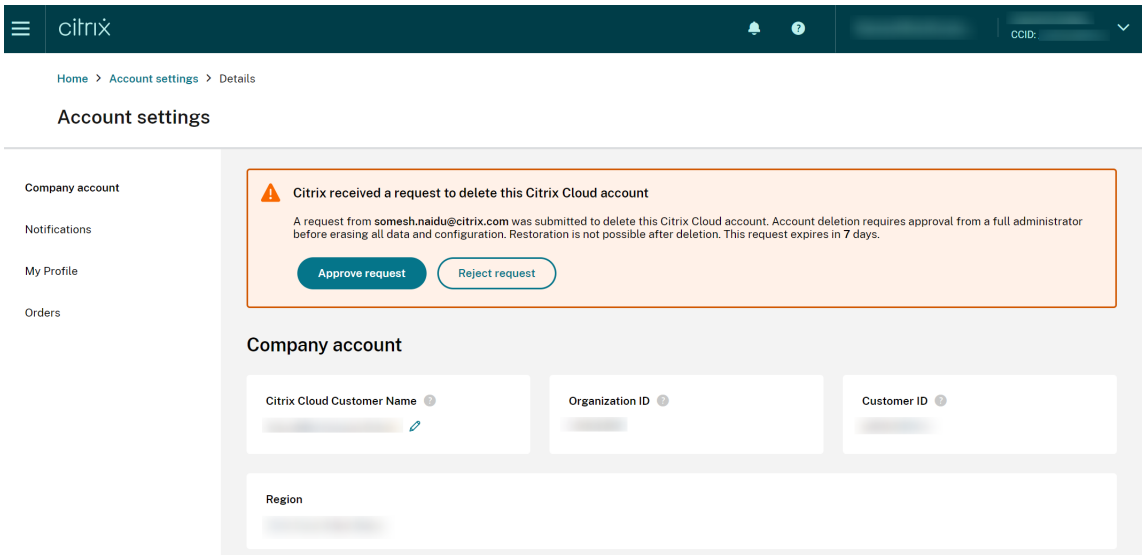
> - Citrix 在您的云环境中预配的所有与 Citrix Cloud 服务相关的资源（包括 Citrix 管理的 VM）都将被删除。有关特定 Citrix Cloud 服务中包含的 Citrix 托管组件的说明，请参阅 Citrix Cloud 服务。
> - 管理员和用户对 Citrix Cloud 和服务的访问被禁用。
> - 积极使用该服务的管理员或用户将遇到服务中断问题。
> - 此操作不可撤消。数据一旦被删除，就无法恢复。

步骤

1. 请联系 Citrix Customer Service 以提交删除请求。需要拥有 Citrix Cloud 帐户的完全权限管理员才能提交此请求。
2. 发起请求后，请登录到您的 Citrix Cloud 帐户。在该位置，您将看到 Citrix Cloud 帐户删除工作流程。

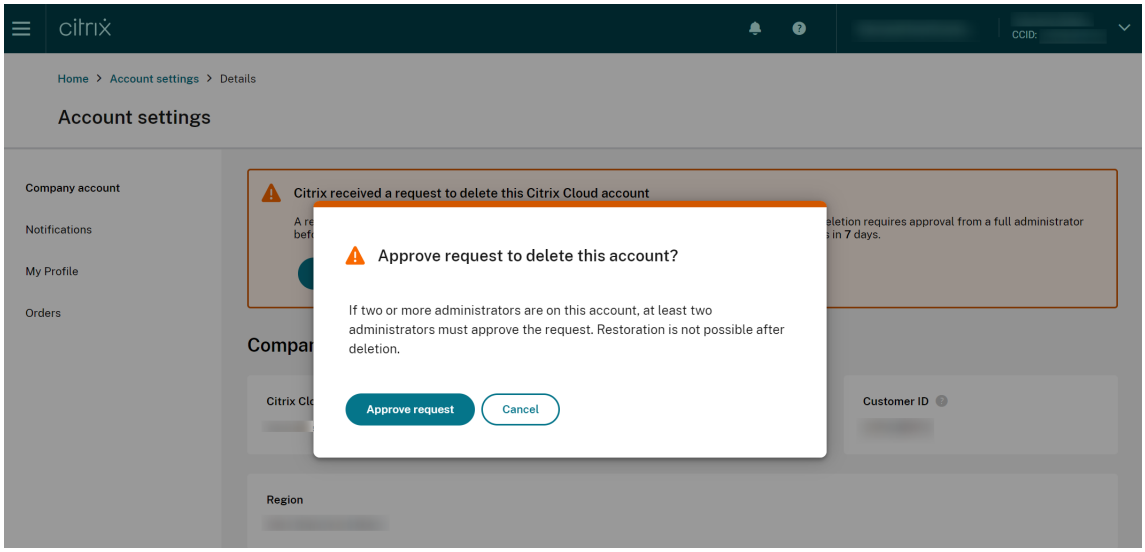


3. 请按照屏幕上的指导批准或拒绝此请求。



4. 要批准此删除请求，请登录该帐户，导航至“帐户设置”，然后在批准工作流程横幅上单击“批准请求”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要取消删除请求，请登录该帐户，导航到“帐户设置”，然后单击删除批准工作流程横幅上的“拒绝并删除请求”。

> 注意：
>
> - 如果此帐户有两个或更多管理员与其关联，则必须至少有两名管理员批准该请求。
> - 如果在 7 天内未收到所需的批准，该请求将过期。

通知

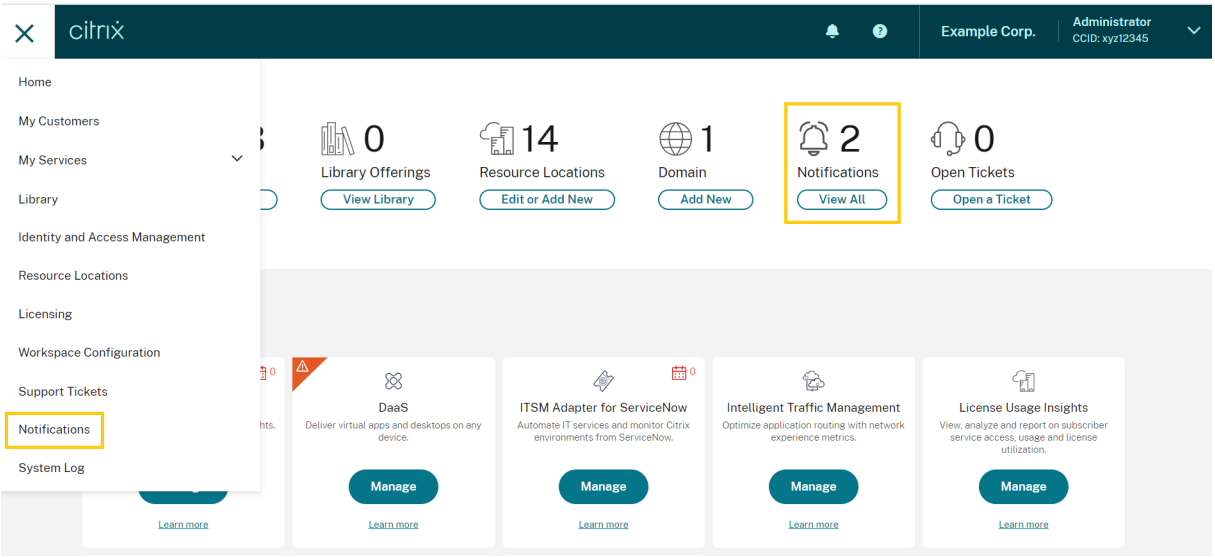
October 5, 2023

“Notifications”（通知）提供与管理员可能感兴趣的问题或事件有关的信息，例如新 Citrix Cloud 功能或资源位置中的计算机存在的问题。通知可以来自 Citrix Cloud 内部的任何服务。

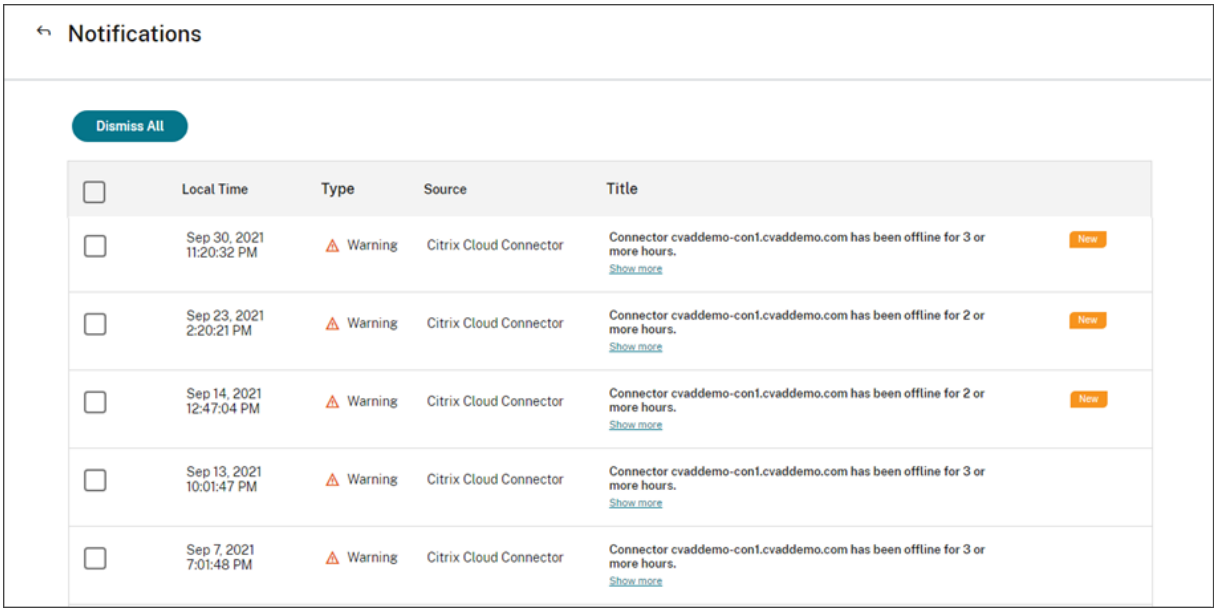
查看通知

通知的数量在靠近 Citrix Cloud 控制台页面顶部的位置显示。有关更多详细信息，请单击控制台中“通知”下的“查看全部”或从控制台菜单中选择“通知”。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



“通知”页面显示您收到的通知。最新通知位于列表顶部。



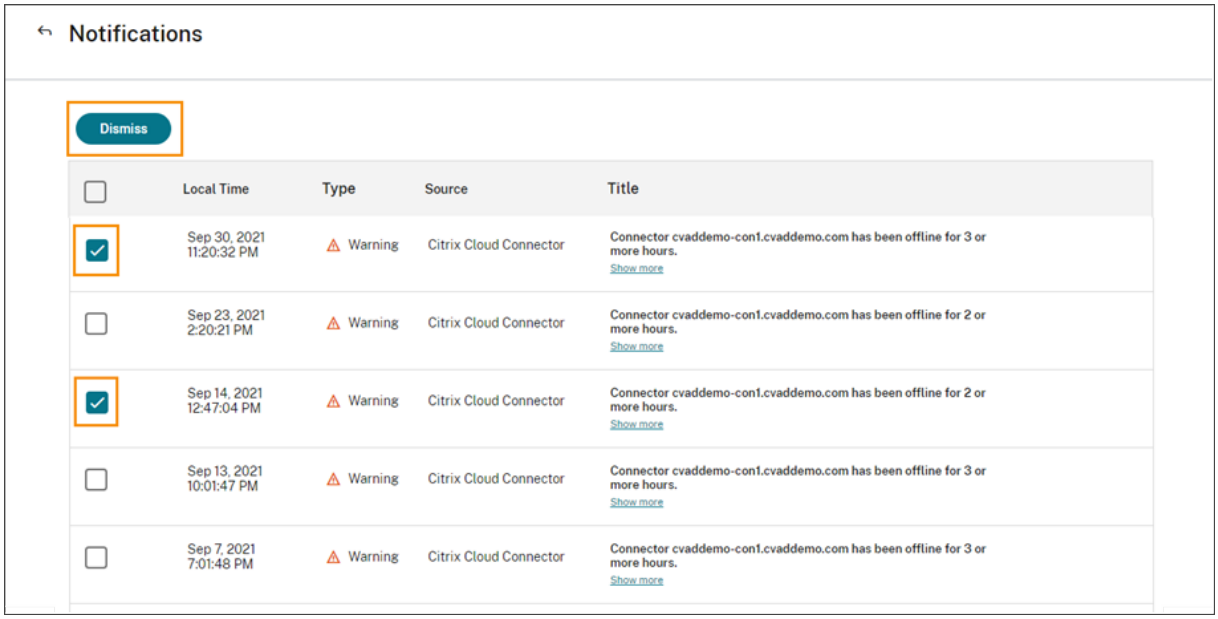
关闭通知

通知以每个管理员为单位进行管理。当您消除通知时，会在 Citrix Cloud 中以您自己的管理员身份消除通知。即使您消除了所有通知，其他管理员仍然可以查看和关闭他们自己的通知。

要消除收到的所有通知，请选择页面顶部附近的“全部消除”。

要消除单个通知，请选择每个通知，然后选择消除。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



接收电子邮件通知

您可以选择通过电子邮件接收通知，而不是登录以查看通知。默认情况下，电子邮件通知处于关闭状态。

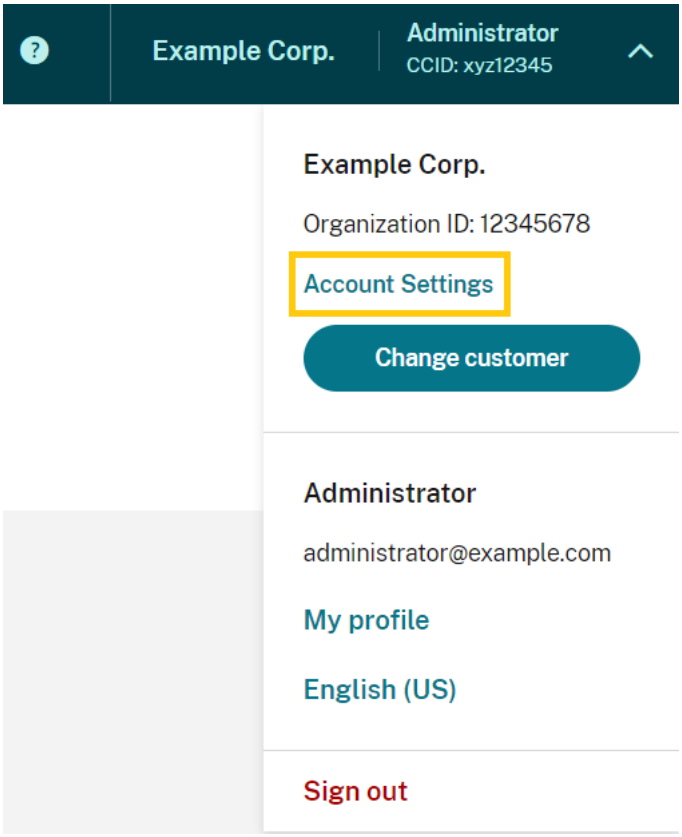
您还可以为没有管理员权限访问您的 Citrix Cloud 帐户的其他利益相关者（例如贵组织的安全和审计团队的成员）启用电子邮件通知。

启用电子邮件通知时，Citrix Cloud 会为每个通知发送一封电子邮件。通知会尽快发送。它们不会分组到一封电子邮件中，也不会进行批处理以便稍后发送。

为自己启用电子邮件通知

1. 在 Citrix Cloud 管理控制台中，选择帐户设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



2. 选择通知。
3. 打开“我的电子邮件通知”设置。
4. 在“管理我的通知设置”下，选择要接收的通知类型。默认情况下，所有通知类型都处于选中状态。
5. 单击“应用”保存您的设置。

为非管理员启用电子邮件通知

使用本节中的步骤将非管理员添加为电子邮件通知的联系人。如果您尝试将现有管理员添加为联系人，Citrix Cloud 会显示错误。

1. 在 Citrix Cloud 管理控制台中，单击 帐户设置。
2. 选择通知。
3. 在“联系人管理”下，选择“添加联系人”。
4. 输入联系人的姓名、电子邮件地址及其首选语言。
5. 在“管理通知设置”下，选择要发送的通知类型。
6. 选择 添加联系人 以保存联系人的信息。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

修改通知设置

作为管理员，您可以通过选中或清除“管理我的通知设置”下的复选框来更改收到的通知类型。更改您的通知不会影响其他管理员收到的通知。

您也可以修改非管理员收到的通知。

修改非管理员的通知

1. 在 Citrix Cloud 管理控制台中，单击 帐户设置。
2. 选择通知。
3. 在“联系人管理”下，找到要管理的联系人。
4. 指向联系人，然后选择铅笔图标。
5. 在“管理通知设置”下，选中或清除每种通知类型的复选框。

要修改联系人的电子邮件地址，必须先删除该联系人，然后使用新的电子邮件地址将其添加为新联系人。

禁用电子邮件通知

作为管理员，您可以随时通过关闭“我的电子邮件通知”设置来禁用自己的电子邮件通知。

非管理员可以通过单击每封通知电子邮件中显示的取消订阅链接来停止接收通知。已取消订阅的联系人在“联系人管理”部分的表格中具有“取消订阅”通知状态。

要禁用非管理员的通知，您可以执行以下操作之一：

- 清除“管理联系人的通知设置”中的所有复选框。
- 从“联系人管理”下的表格中删除联系人。

删除非管理员联系人

1. 在 Citrix Cloud 管理控制台中，单击 帐户设置。
2. 选择通知。
3. 在“联系人管理”下，找到要管理的联系人。
4. 指向联系人，然后选择垃圾桶图标。

Citrix Cloud 将联系人从表格中删除。

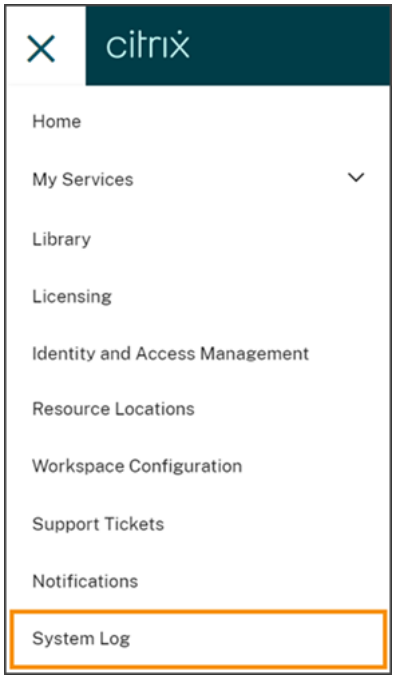
系统日志

October 5, 2023

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

系统日志显示 Citrix Cloud 中发生的事件的时间戳列表。您可以将这些更改导出为 CSV 文件，以满足组织的法规合规性要求或支持安全分析。

要查看系统日志，请从 Citrix Cloud 菜单中选择 系统日志。

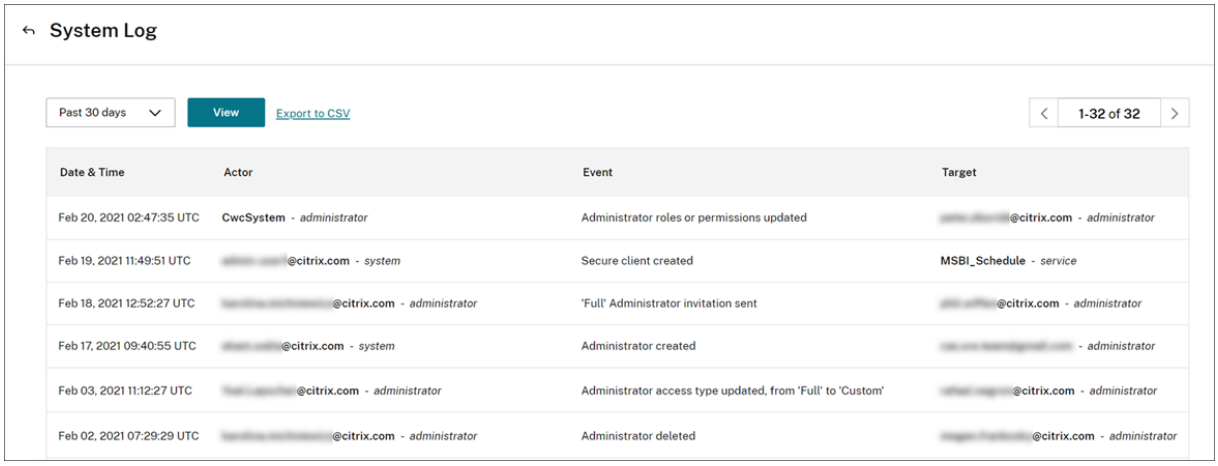


有关在系统日志中保留数据的更多信息，请参阅本文中的 数据保留 。

记录的事件

系统日志会捕获某些 Citrix Cloud 平台和云服务操作的事件。有关这些事件的完整列表和捕获数据的说明，请参阅 系统日志事件参考。

默认情况下，系统日志显示过去 30 天内发生的事件。最先显示最近的事件。

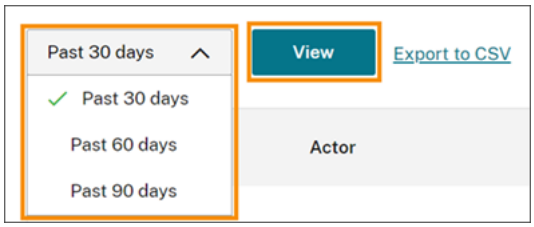


显示的列表包括以下信息：

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

- 事件发生的日期和时间 (UTC)。
- 发起事件的参与者，例如管理员或安全客户端。使用参与者 **CwcSystem** 的条目表示 Citrix Cloud 执行了该操作。
- 事件的简要描述，例如编辑管理员或创建新的安全客户端。
- 事件的目标。目标是由于事件而受到影响或更改的系统对象。例如，添加为管理员的用户。

要查看过去 30 天以上的事件，请通过选择要查看的时间段来筛选列表，然后选择 查看。您可以查看过去 90 天内发生的事件。

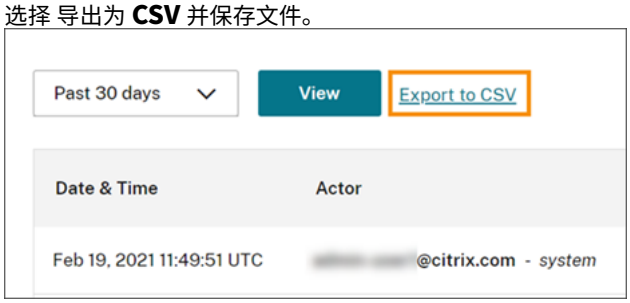


要检索在指定时间段内发生的较早事件，可以使用 SystemLog API。有关更多信息，请参阅本文中的 检索特定时间段内的事件 。

导出事件

您可以导出最近 90 天内发生的系统日志事件的 CSV 文件。下载的文件的名称遵循的格式 `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`。

1. 从 Citrix Cloud 菜单中，选择 系统日志。
2. 如果需要，筛选列表以显示要导出事件的时间段。
3. 选择 导出为 **CSV** 并保存文件。



CSV 文件包含以下信息：

- 每个事件的 UTC 时间戳
- 发起活动的参与者的详细信息，包括姓名和演员 ID。
- 事件详情，例如事件类型和事件文本
- 事件目标的详细信息，例如目标 ID、管理员名称或安全客户端。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

检索特定时间段的事件

如果您需要检索特定时间段内的事件，可以使用 SystemLog API。在使用 API 之前，您需要按照 Citrix Developer 文档网站上的 入门 中所述创建安全客户端。

有关使用 SystemLog API 的更多信息，请参阅 Citrix 开发人员文档网站上的 Citrix Cloud-SystemLog 。

转发系统日志事件

适用于 Splunk 的 Citrix 系统日志附加组件 使您能够将 Splunk 实例与 Citrix Cloud 连接起来。通过此连接，您可以将系统日志数据转发到 Splunk。有关更多信息，请参阅 GitHub 中 Citrix 存储库中的 附加组件文档 。

数据保留

Citrix 与您（客户）共同承担保留 Citrix Cloud 捕获的系统日志数据的责任。

在记录事件后，Citrix 会将系统日志记录保留 90 天。

您负责下载要保留的系统日志记录，以满足组织的合规性要求，并负责将这些记录存储在长期存储解决方案中。

系统日志事件参考

October 5, 2023

要查看 Citrix Cloud 帐户的所有系统日志事件数据，您可以：

- 下载过去 30 天、60 天或 90 天内发生的所有事件的 CSV 文件 。
- 使用 SystemLog API 检索特定时间段内的事件。

有关检索系统日志 事件 时捕获的数据的说明，请参阅本文中的事件数据说明。请参阅针对事件特定值（例如事件消息文本、事件类型以及是否在事件发生之前和之后记录对象字段数据）生成事件的云组件和服务。

生成事件的云组件和服务

系统日志记录以下 Citrix Cloud 实体、组件和服务的事件：

- Citrix Cloud 平台：与 Citrix Cloud 平台功能相关的事件，例如管理管理员、Workspace 订阅者的设备重置、Azure AD 租户以及管理域和网络位置。
- 连接器：与注册和更新 Citrix Cloud 连接器和连接器设备相关的事件。
- 许可：与注册本地许可证服务器、管理为云服务分配的许可证以及导出许可数据相关的事件。
- Secure Private Access 服务：与 Secure Private Access 服务配置相关的事件。
- Citrix Workspace：与 Workspace 配置设置相关的事件。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

事件数据描述

当您下载系统日志事件或使用 SystemLog API 检索它们时，会包含以下数据：

- **RecordID**：事件的唯一标识符。
- **UtcTimestamp**：事件发生的日期和 UTC 时间。
- **CustomerID**： Citrix Cloud 帐户的唯一组织标识符。
- **EventType**：记录的事件类型的标识符。事件类型使用格式进行记录 `OriginatingService`/`Actor`/`Action`。例如，用于创建管理员的事件类型为 `platform`/`administrator`/`create`。
- **TargetID**：受影响或更改的系统对象的 ID。
- **TargetDisplayName**：受影响或更改的系统对象的显示名称。例如，创建的管理员的姓名。
- **TargetEmail**：系统对象的电子邮件地址。例如，创建的管理员的电子邮件地址。
- **TargetUserID**：受影响或更改的系统对象的用户 ID。例如，创建管理员时，目标用户 ID 是创建的管理员的用户 ID。
- **TargetType**：事件的目标类别。
- **BeforeChanges** 和 **AfterChanges**：分别是事件发生前后的对象字段的内容。对于某些事件，这些对象字段包括：
  - CustomerID
  - 用户委托人
  - UserID
  - 管理员访问权限类型，例如“自定义”或“完全”
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **AgentID**：事件类别。
- **ActorID**：发起事件的系统对象的 ID。例如，对于创建管理员，这是邀请其他用户加入 Citrix Cloud 帐户的管理员的对象 ID。
- **ActorDisplayName**：发起事件的个人或实体的显示名称。例如，邀请其他用户加入 Citrix Cloud 帐户的管理员的姓名。
- **ActorType**：生成事件的服务。
- **EventMessage**：对所发生事件的简要描述。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix Cloud 平台的系统日志事件

July 12, 2023

本文介绍系统日志为 Citrix Cloud 平台捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

Azure AD 租户

活动消息	事件类型	目标类型	演员类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已连接 Azure AD 租户	platform/identityprovider/azuread/connect	服务	管理员		是	否
Azure AD 租户断开	platform/identityprovider/azuread/disconnect	服务	管理员		是	否
Azure AD 身份验证域名已更改	platform/identityprovider/azuread/authdomain/updatename	Customer	管理员		否	否
Azure AD 身份验证域名更改失败	platform/identityprovider/azuread/authdomain/updatenamefailed	Customer	管理员		否	否

Citrix Cloud 管理员和安全客户端

活动消息	事件类型	目标类型	演员类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
管理员已创建	platform/administrator/create	管理员	系统	否	是
已发送管理员邀请	platform/administrator/invite	管理员	管理员	否	是
管理员角色或权限已更新	platform/administrator/update	管理员	管理员	是	是
管理员已删除	platform/administrator/delete	管理员	管理员	否	是
已创建安全客户端	platform/clientadministrator/create	服务	系统	否	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	演员类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已删除安全客户端	platform/clientadministrator/delete	服务	管理员	是	否
管理员组已创建	platform/administratorgroup/create	管理员组		否	是
管理员组角色或权限已更新	platform/administratorgroup/update	管理员组		是	是
删除的管理员组	platform/administratorgroup/delete	管理员组	管理员	是	否

Active Directory 加令牌的设备重置

活动消息	事件类型	目标类型	演员类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
订阅者设备令牌重置已完成	platform/authentication/device/delete	订阅用户	管理员	否	是

域管理

活动消息	事件类型	目标类型	演员类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
删除的域	platform/domain/remove	服务	管理员	否	否

网络位置

事件消息	事件类型	目标 ID	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
网络位置已创建	sdwan/networklocation/create	创建的网络位置的 ID	添加网络位置的管理员的姓名	否	是
网络位置已更新	sdwan/networklocation/update	修改的网络位置的 ID	修改网络位置的管理员的姓名	是	是
网络位置已删除	sdwan/networklocation/delete	已删除的网络位置的 ID	删除网络位置的管理员的姓名	是	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

资源位置

活动消息	事件类型	目标 ID	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
资源位置已创建	平台/资源定位/创建	创建的资源位置的名称	创建资源位置的管理员的姓名	是	是
资源位置已更新	平台/资源位置/更新	已修改的资源位置的名称	修改资源位置的管理员的姓名	是	是
资源位置已删除	平台/资源定位/删除	已删除的资源位置的名称	删除资源位置的管理员的姓名	是	是

连接器的系统日志事件

August 31, 2022

本文介绍系统日志为云服务的 Citrix Cloud Connector 和连接器设备捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

连接器注册

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
连接器已注册	平台/edgeserver/creation	**Cloud Connector** 或 **Connector** 设备	注册连接器的管理员	是	是
连接器已删除	平台/edgeserver/deletion	**Cloud Connector** 或 **Connector** 设备	删除连接器的管理员	是	是

Connector 更新

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标 ID	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
资源位置维护时段已更新	平台/资源位置/维护窗口	已修改的资源位置的名称	更改配置的管理员	是	是
管理员触发的连接器升级	platform/edgeserver/upd 动升级	**Cloud Connector** 或 **Connector** 设备	启动更新的管理员	否	否
连接器升级已启动	平台/边缘服务器/升级已启动	**Cloud Connector** 或 **Connector** 设备	自动 或启动更新的管理员	是	否
连接器升级已完成	平台/边缘服务器/升级已完成	**Cloud Connector** 或 **Connector** 设备	自动 或启动更新的管理员	否	是

连接器公钥

活动消息	事件类型	目标 ID	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
公钥已添加到信任	平台/身份验证/createedgeserverkey		执行操作的管理员	否	否
公钥已从信任中移除	平台/身份验证/deleteedgeserverkey		执行操作的管理员	否	否

Citrix Cloud 中许可的系统日志事件

August 31, 2022

本文介绍系统日志为使用 Citrix Cloud 注册的本地 Citrix Licensing 捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

本地许可证服务器

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
本地许可证服务器已删除	lui/onpremlicenseservers/delete	许可证	删除许可证服务器的管理员	否	否
未能删除本地许可证服务器	lui/onpremlicenseservers/deletefailed	许可证	尝试删除许可证服务器的管理员	否	否

云服务许可

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
Citrix Cloud 服务许可证已发布	lui/cloud 许可证/发布	云许可证	发布云服务许可证的管理员	否	否
未能释放 Citrix Cloud 服务许可证	lui/cloud 许可证/发布失败	云许可证	尝试释放云服务许可证的管理员	否	否

针对 **Citrix** 服务提供商的许可证使用情况分析

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
合作伙伴本地用户列表数据已导出	lui/csp/userlistdata/export	许可	导出合作伙伴用户列表数据的管理员	否	否
无法导出合作伙伴本地用户列表数据	lui/csp/userlist 数据导出失败	许可	尝试导出合作伙伴用户列表数据的管理员	否	否

云服务和本地产品的许可证使用情况

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已导出许可证使用数据	lui/cloud 许可证/使用数据导出	云许可证或许可	导出许可证使用数据的管理员	否	否
无法导出许可证使用数据	lui/cloud 许可证/使用数据导出失败	云许可证或许可	尝试导出许可证使用数据的管理员	否	否

Secure Private Access 的系统日志事件

October 14, 2022

本文介绍了 System Log 为 Secure Private Access 服务捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

Web 和 SaaS 应用程序

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已创建 Web/SaaS 应用程序	swa/websaasppplicationcreate	web/saasapplication	否	是
Web/SaaS 应用程序已更新	swa/websaasppplicationupdate	web/saasapplication	是	是
Web/SaaS 应用程序已删除	swa/websaasppplicationdelete	web/saasapplication	是	否
Web/SaaS 应用程序创建失败	swa/websaasppplicationcreatefailed	web/saasapplication	否	否
Web/SaaS 应用程序更新失败	swa/websaasppplicationupdatefailed	web/saasapplication	是	是
Web/SaaS 应用程序删除失败	swa/websaasppplicationdeletefailed	web/saasapplication	是	是

用户和组订阅

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已添加用户/组订阅	swa/websaaspplicationsubscription/subscribe	websaaspplicationsubscribers	否	是
已移除用户/组订阅	swa/websaaspplicationsubscription/unsubscribe	websaaspplicationsubscribers	否	是
用户/组订阅失败	swa/websaaspplicationsubscription/subscribefailed	websaaspplicationsubscribers	否	否
用户/组取消订阅失败	swa/websaaspplicationsubscription/unsubscribefailed	websaaspplicationsubscribers	否	否

情境政策

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已创建上下文策略	swa/contextualpolicy/create	contextualpolicy	否	是
情境政策已更新	swa/contextualpolicy/update	contextualpolicy	是	是
上下文策略已删除	swa/contextualpolicy/delete	contextualpolicy	是	否
上下文策略创建失败	swa/contextualpolicy/createfailed	contextualpolicy	否	否
上下文策略更新失败	swa/contextualpolicy/updatefailed	contextualpolicy	否	否
上下文策略删除失败	swa/contextualpolicy/deletefailed	contextualpolicy	是	否

应用程序域

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
应用程序域已创建	swa/applicationdomain/create	applicationdomain	否	是
应用程序域已更新	swa/applicationdomain/update	applicationdomain	是	是
应用程序域已删除	swa/applicationdomain/delete	applicationdomain	是	否
创建应用程序域失败	swa/applicationdomain/createfailed	applicationdomain	否	否
应用程序域更新失败	swa/applicationdomain/updatefailed	applicationdomain	是	否
应用程序域删除失败	swa/applicationdomain/deletefailed	applicationdomain	是	否

浏览器扩展设置

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
浏览器扩展设置已更新	swa/browserextensionsettings/update	浏览器扩展设置	是	是
浏览器扩展设置更新失败	swa/browserextensionsettings/updatefailed	browserextensionsettings	是	否

网站 **URL** 列表和筛选器类别

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已启用 Web 站点筛选器列表和类别	swa/website/filterlists/websitefilterurlcategoryfeature/enabled/update	websitefilterurlcategoryfeature	是	是
已启用的网站过滤器列表和禁用的过滤器类别	swa/website/filterlists/websitefilterurlcategoryfeature/disabled/update	websitefilterurlcategoryfeature	是	是
禁用的网站过滤器列表和启用的过滤器类别	swa/website/filterlists/websitefilterurlcategoryfeature/enabled/update	websitefilterurlcategoryfeature	是	是
已禁用的网站筛选器列表和类别	swa/website/filterlists/websitefilterurlcategoryfeature/disabled/update	websitefilterurlcategoryfeature	是	是
无法启用网站筛选器列表和类别	swa/website/filterlists/websitefilterurlcategoryfeature/enabled/updatefailed	websitefilterurlcategoryfeature	是	failed
无法启用网站筛选器列表和禁用筛选器类别	swa/website/filterlists/websitefilterurlcategoryfeature/disabled/updatefailed	websitefilterurlcategoryfeature	是	failed
无法禁用网站筛选器列表和启用筛选器类别	swa/website/filterlists/websitefilterurlcategoryfeature/enabled/updatefailed	websitefilterurlcategoryfeature	是	failed
禁用网站筛选器列表和类别失败	swa/website/filterlists/websitefilterurlcategoryfeature/disabled/updatefailed	websitefilterurlcategoryfeature	是	failed
Web 站点 URL 列表已创建	swa/websiteurlfilteringlist/create	websiteurlfilteringlist	否	是
Web 站点 URL 列表已更新	swa/websiteurlfilteringlist/update	websiteurlfilteringlist	是	是
Web 站点 URL 列表已删除	swa/websiteurlfilteringlist/delete	websiteurlfilteringlist	是	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
网站 URL 列表创建失败	swa/websiteurlfilterweblist/createfailed	weblist	否	否
网站 URL 列表更新失败	swa/websiteurlfilterweblist/updatefailed	weblist	是	否
网站 URL 列表删除失败	swa/websiteurlfilterweblist/deletefailed	weblist	是	否
已创建网站 URL 过滤器类别	swa/websiteurlfiltercategory/created	category	否	是
网站 URL 过滤器类别已更新	swa/websiteurlfiltercategory/updated	category	是	是
已删除网站 URL 过滤器类别	swa/websiteurlfiltercategory/deleted	category	是	否
网站 URL 筛选器类别创建失败	swa/websiteurlfiltercategory/createfailed	category	否	否
网站 URL 过滤器类别更新失败	swa/websiteurlfiltercategory/updatefailed	category	是	否
网站 URL 筛选器类别删除失败	swa/websiteurlfiltercategory/deletefailed	category	是	否

网站筛选器类别预设

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
更新了网站过滤器类别预设	swa/websiteurlfiltercategory/updatedpreset	category	是	是
更新网站筛选器类别预设失败	swa/websiteurlfiltercategory/updatefailedpreset	category	是	是

阻止的网站 **URL** 列表和过滤器类别

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已创建阻止的网站 URL 列表	swa/websiteurlfilterweblist/blockedcreated	weblist	否	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已更新已阻止的网站 URL 列表	swa/websiteurlfilterwebsiteblockedlist/update	websiteblockedlist		是
已删除已阻止的网站 URL 列表	swa/websiteurlfilterwebsiteblockedlist/delete	websiteblockedlist		是
已阻止的网站 URL 列表创建失败	swa/websiteurlfilterwebsiteblockedlist/createfailed	websiteblockedlist		是
已阻止的网站 URL 列表更新失败	swa/websiteurlfilterwebsiteblockedlist/updatefailed	websiteblockedlist		是
删除阻止的网站 URL 列表失败	swa/websiteurlfilterwebsiteblockedlist/deletefailed	websiteblockedlist		是
已创建阻止的网站 URL 过滤器类别	swa/websiteurlfiltercategoryblockedlist/create	categoryblockedlist		是
已更新已阻止的网站 URL 过滤器类别	swa/websiteurlfiltercategoryblockedlist/update	categoryblockedlist		是
已删除阻止的网站 URL 过滤器类别	swa/websiteurlfiltercategoryblockedlist/delete	categoryblockedlist		是
已阻止的网站 URL 过滤器类别创建失败	swa/websiteurlfiltercategoryblockedlist/createfailed	categoryblockedlist		是
已阻止的网站 URL 筛选器类别更新失败	swa/websiteurlfiltercategoryblockedlist/updatefailed	categoryblockedlist		是
已阻止的网站 URL 筛选器类别删除失败	swa/websiteurlfiltercategoryblockedlist/deletefailed	categoryblockedlist		是

允许的网站 **URL** 列表和筛选器类别

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已创建允许的网站 URL 列表	swa/websiteurlfilterwebsiteallowedlist/create	websiteallowedlist		是
已更新允许的网站 URL 列表	swa/websiteurlfilterwebsiteallowedlist/update	websiteallowedlist		是
已删除允许的网站 URL 列表	swa/websiteurlfilterwebsiteallowedlist/delete	websiteallowedlist		是
允许的网站 URL 列表创建失败	swa/websiteurlfilterwebsiteallowedlist/createfailed	websiteallowedlist		是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	事件之前记录的当前对象字段	更新了事件后记录的对象字段
允许的网站 URL 列表更新失败	swa/websiteurlfilteringlist/allowed/updatefailed	websiteurlfilteringlist	No	是
允许的网站 URL 列表删除失败	swa/websiteurlfilteringlist/allowed/deletefailed	websiteurlfilteringlist	No	是
已创建允许的网站 URL 过滤器类别	swa/websiteurlfiltercategory/allowed/create	websiteurlfilteringlist	No	是
已更新允许的网站 URL 过滤器类别	swa/websiteurlfiltercategory/allowed/update	websiteurlfilteringlist	No	是
已删除允许的网站 URL 过滤器类别	swa/websiteurlfiltercategory/allowed/delete	websiteurlfilteringlist	No	是
允许的网站 URL 筛选器类别创建失败	swa/websiteurlfiltercategory/allowed/createfailed	websiteurlfilteringlist	No	是
允许的网站 URL 筛选器类别更新失败	swa/websiteurlfiltercategory/allowed/updatefailed	websiteurlfilteringlist	No	是
允许的网站 URL 筛选器类别删除失败	swa/websiteurlfiltercategory/allowed/deletefailed	websiteurlfilteringlist	No	是

已重定向到 **Remote Browser Isolation**（以前称为 **Secure Browser**）**Web** 站点 **URL** 列表和过滤器类别

活动消息	事件类型	目标类型	演员类型	代理 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已重定向至创建的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/create	websiteurlfilteringlist	No	Yes		
已重定向至更新的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/update	websiteurlfilteringlist	No	Yes		
已重定向至删除的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/delete	websiteurlfilteringlist	No	Yes		
无法重定向至创建的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/createfailed	websiteurlfilteringlist	No	Yes		
无法重定向至更新的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/updatedfailed	websiteurlfilteringlist	No	Yes		
无法重定向至删除的 Secure Browser Web 站点 URL 列表	swa/websiteurlfilteringlist/redirected/deletefailed	websiteurlfilteringlist	No	Yes		
已重定向至创建的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirected/create	websiteurlfilteringlist	No	Yes		
已重定向至更新的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirect-					

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

ed/update|websiteurlfilteringlist|No|Yes|
已重定向至删除的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirected/delete	websiteurlfilteringlist	No	Yes
无法重定向至创建的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirected/createfailed	websiteurlfilteringlist	No	Yes
无法重定向至更新的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirected/updatefailed	websiteurlfilteringlist	No	Yes
无法重定向至删除的 Secure Browser Web 站点 URL 过滤器类别	swa/websiteurlfiltercategory/redirected/deletefailed	websiteurlfilteringlist	No	Yes

Citrix Workspace 系统日志事件

August 31, 2022

本文介绍系统日志为 Citrix Workspace 捕获的事件数据。有关系统日志事件数据的更多信息，请参阅 系统日志事件参考。

要了解有关系统日志的更多信息，请参阅 系统日志。

Workspace URL

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
工作区 URL 已更新	wxp/url/update	订阅用户	更新 URL 的管理员	是	是
更新工作区 URL 失败	wxp/url/更新失败	订阅用户	尝试更新 URL 的管理员	是	是
工作区 URL 已启用	wxp/url/启用	订阅用户	启用工作区 URL 自定义的管理员	否	是
未能启用工作区 URL	wxp/url/enablefailed	订阅用户	尝试启用工作区 URL 自定义的管理员	否	是
工作区 URL 已禁用	wxp/url/禁用	订阅用户	禁用工作区 URL 自定义的管理员	否	是
禁用工作区 URL 失败	wxp/url/禁用失败	订阅用户	尝试禁用工作区 URL 自定义的管理员	否	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

工作区身份验证

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
工作区身份提供商已更新	wxp/身份提供商/更新	订阅用户	更新工作区身份验证方法的管理员	是	是
更新工作区身份提供者失败	wxp/身份提供商/更新失败	订阅用户	尝试更新工作区身份验证方法的管理员	是	是

Citrix 联合身份验证服务

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
工作空间联合身份验证服务 (FAS) 已启用	wxp/fas/启用	订阅用户	启用 FAS 的管理员	否	是
无法启用 Workspace 联合身份验证服务 (FAS)	wxp/fas/enablefailed	订阅用户	尝试启用 FAS 的管理员	否	是
工作空间联合身份验证服务 (FAS) 已禁用	wxp/fas/禁用	订阅用户	禁用 FAS 的管理员	否	是
无法禁用工作区联合身份验证服务 (FAS)	wxp/fas/禁用失败	订阅用户	尝试禁用 FAS 的管理员	否	是

收藏夹

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已启用工作区收藏夹	wxp/收藏夹/启用	订阅用户	启用收藏夹的管理员	否	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
未能启用工作区收藏夹	wxp/收藏夹/启用失败	订阅用户	尝试启用收藏夹的管理员	否	是
已禁用工作区收藏夹	wxp/收藏夹/禁用	订阅用户	禁用收藏夹的管理员	否	是
禁用工作区收藏夹失败	wxp/收藏夹/禁用失败	订阅用户	尝试禁用收藏夹的管理员	否	是

更改密码

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
工作区更改密码选项策略已更新	wxp/changepassword/选项/更新政策	订阅用户	在 Citrix Workspace 中更新密码更改策略的管理员	是	是
更新工作区更改密码选项策略失败	wxp/changepassword/选项/更新策略失败	订阅用户	尝试在 Citrix Workspace 中更新密码更改策略的管理员	是	是
工作区更改密码选项已启用	wxp/changepassword/options	订阅用户	在 Citrix Workspace 中启用更改密码设置的管理员	否	是
未能启用工作区更改密码选项	wxp/changepassword/选项/启用失败	订阅用户	尝试在 Citrix Workspace 中启用更改密码设置的管理员	否	是
工作区更改密码选项已禁用	wxp/changepassword/options	订阅用户	在 Citrix Workspace 中禁用更改密码设置的管理员	否	是
无法禁用工作区更改密码选项	wxp/changepassword/options/禁用失败	订阅用户	尝试在 Citrix Workspace 中禁用更改密码设置的管理员	否	是

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

长寿代币

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已更新工作区长期使用令牌配置	wxp/longlivetoken/更新	订阅用户	更新令牌配置的管理员	是	是
更新工作区长期存在令牌配置失败	wxp/longlivetoken/更新失败	订阅用户	尝试更新令牌配置的管理员	是	是

Web 不活动超时

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
工作区会话配置已更新	wxp/会话/更新	订阅用户	更新 Web 不活动超时设置的空闲时间的管理员	是	是
更新工作区会话配置失败	wxp/会话/更新失败	订阅用户	尝试更新 Web 不活动超时设置的空闲时间的管理员	是	是

功能推出

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
已分配的用户和组已更新，以获得智能工作区体验	wxp/iws/features/updateusersgroups	订阅用户	更新分配的用户和组以访问 Citrix Workspace 中的活动源通知的管理员	否	否

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

活动消息	事件类型	目标类型	操作者 ID	事件之前记录的当前对象字段	更新了事件后记录的对象字段
无法分配为智能工作区体验而更新的用户和组	wxp/iws/功能/更新用户组失败	订阅用户	尝试更新分配的用户和组以访问 Citrix Workspace 中的活动源通知的管理员	否	否
已启用智能工作区体验	wxp/iws/功能/启用	订阅用户	在 Citrix Workspace 中启用活动源通知的管理员	否	否
未能启用智能工作区体验	wxp/iws/功能/启用失败	订阅用户	尝试在 Citrix Workspace 中启用活动源通知的管理员	否	否
智能工作区体验已禁用	wxp/iws/功能/禁用	订阅用户	在 Citrix Workspace 中禁用活动源通知的管理员	否	否
未能禁用智能工作区体验	wxp/iws/features/禁用失败	订阅用户	尝试在 Citrix Workspace 中禁用活动源通知的管理员	否	否

SDK 和 API

July 1, 2024

Citrix Cloud 提供了几种 API，可用于检索信息并自动执行复杂而重复的任务，包括：

- 静默安装 Citrix Cloud Connector
- 创建和使用用于管理云许可证的报告
- 确定客户的权利状态
- 向 Citrix Cloud 管理员发送通知
- 检索系统日志事件
- 检索有关资源位置的详细信息以用于其他 API

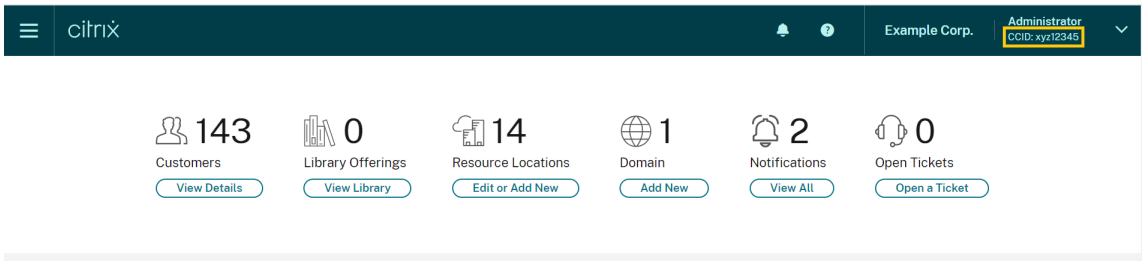
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

多种 Citrix Cloud 服务还提供软件开发工具包和 API，允许您检索信息、查询数据和执行管理任务。

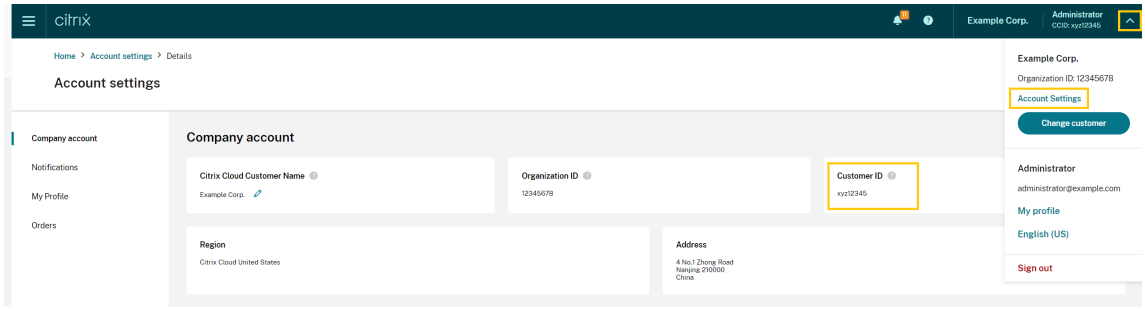
安全客户端

要使用 Citrix Cloud API，您需要创建一个代表您访问 Citrix Cloud 的安全客户端。要创建安全客户端，您需要提供 Citrix Cloud 帐户的客户 ID。您的客户 ID 位于管理控制台的以下位置：

- 控制台右上角，位于用户名下方。



- 您的 帐户设置 页面。



- **API** 访问 页面。

继承的权限

安全客户端与 Citrix Cloud 中的单个管理员和单个客户 ID 绑定。这意味着您的安全客户端将继承您在特定客户 ID 下所拥有的相同级别的权限。因此，如果您具有完全访问权限，则安全客户端也具有完全访问权限。如果稍后降低了权限级别，则已创建的安全客户端会自动继承降低的权限。

有关创建安全客户端的说明，请参阅 Citrix 开发人员文档中的 Citrix Cloud API 入门 。

云许可 **API**

企业客户可以使用云许可 API 执行管理任务，例如导出使用情况数据和释放分配的许可证。Citrix 合作伙伴可以使用这些 API 检索本地 Citrix Virtual Apps and Desktops 以及 Citrix DaaS 的摘要和历史数据。

有关更多信息，请参阅 Citrix Developer 文档中用于管理 Citrix Cloud 许可的 API。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

SystemLog API

SystemLog API 允许您检索 Citrix Cloud 帐户中在指定时间段内发生的事件。有关使用此 API 的更多信息，请参阅 Citrix Developer 文档中的 Citrix Cloud - SystemLog。

资源位置 API

资源位置 API 允许您检索有关资源位置的信息，以便与其他应用程序和脚本一起使用。例如，假设您要在 Citrix Cloud 帐户中的多个资源位置之一静默安装 Citrix Cloud Connector。您可以使用此 API 检索资源位置 ID 并将其传递给安装脚本。

有关使用此 API 的更多信息，请参阅 Citrix 开发人员文档中的 Citrix Cloud-资源位置 。

服务授权 API

服务授权 API 检索客户有权使用的服务、每项授权的剩余天数以及客户购买的授权数量。有关使用此 API 的更多信息，请参阅 Citrix 开发人员文档中的 Citrix Cloud-服务授权 。

通知 API

通知 API 允许您向其他 Citrix Cloud 管理员发送消息。收件人通过管理控制台中的 通知 页面接收您的消息。

其他服务的 SDK 和 API

有关可用于其他 Citrix Cloud 服务的软件开发工具包和 API 的更多信息，请参阅以下文章：

- 数字工作区：包括用于 Citrix DaaS 和 Citrix Workspace 等工作区服务的软件开发工具包和 API。
- App Delivery and Security：包括用于网络链接和应用程序交付服务（例如控制台、Intelligent Traffic Management 和 SD-WAN Orchestrator）的 SDK 和 API。

更多信息

要详细了解 Citrix Cloud API 和安全客户端如何帮助您执行复杂操作（例如迁移到云和使用推送令牌配置身份验证），请参阅以下 Tech Zone 文章：

- PoC 指南：使用推送令牌进行 Citrix Gateway 身份验证的 nFactor
- 部署指南：将 Citrix Virtual Apps and Desktops 服务从 VMware vSphere 迁移到 Microsoft Azure 上的 Citrix Virtual Apps and Desktops 服务
- PoC 指南：自动配置工具

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

面向合作伙伴的 **Citrix Cloud**

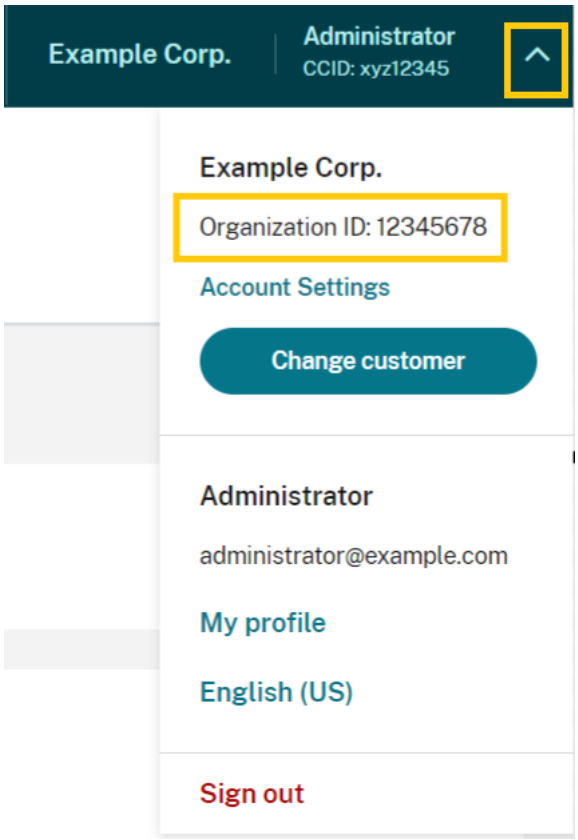
April 5, 2024

Citrix Cloud 包括专为客户和合作伙伴设计的服务、功能和体验。本部分内容概述了 Citrix 合作伙伴可用的功能，这些功能可以帮助合作伙伴针对 Citrix Cloud 服务和解决方案与客户协作。

合作伙伴标识

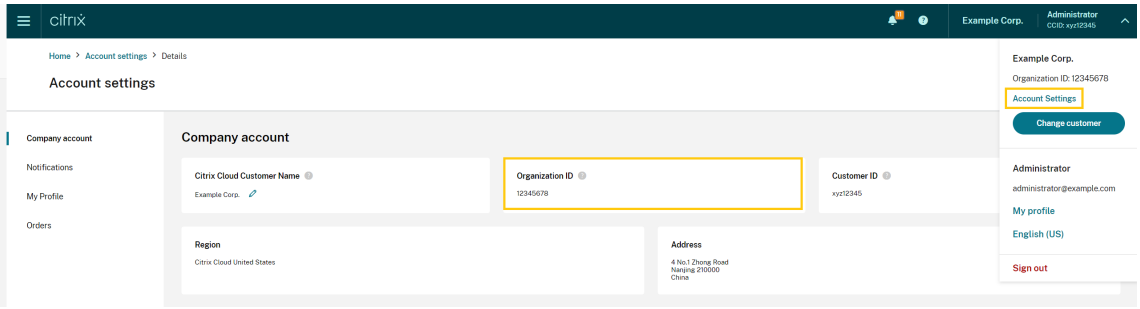
合作伙伴在 Citrix Cloud 中根据其 Citrix 组织 ID (ORGID) 进行标识。合作伙伴可以在 Citrix Cloud 管理控制台的以下位置查看与其 Citrix Cloud 帐户关联的 ORGID：

- 从客户菜单中。从控制台右上角单击您的客户名称。您的 ORGID 显示在菜单中您公司名称的下方。

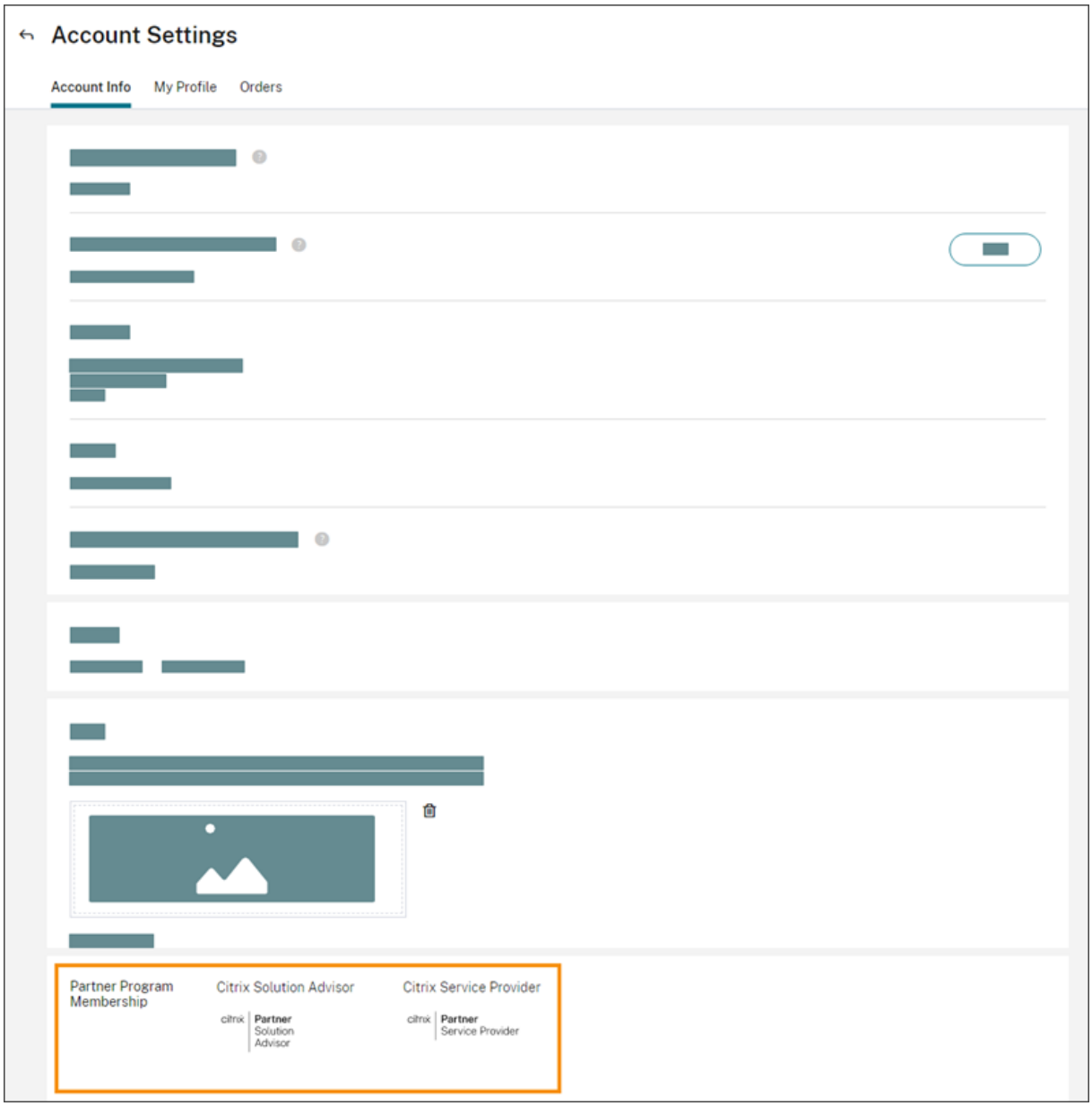


- 从帐户设置页面。从右上角的客户菜单中，选择 帐户设置。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



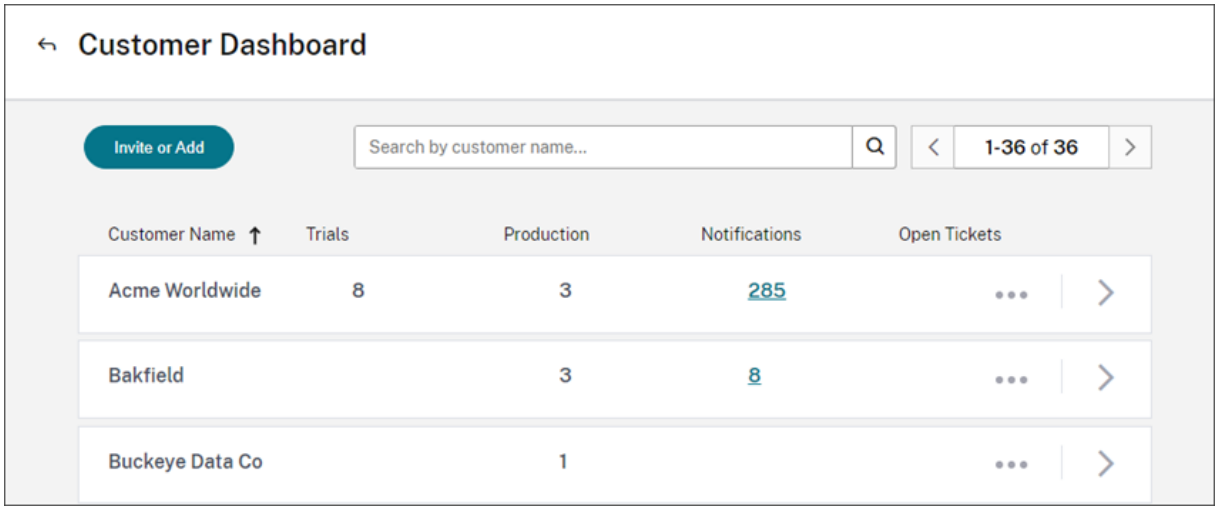
如果帐户上的 ORGID 是 Citrix 合作伙伴计划（例如 Citrix Solution Advisor 或 Citrix Service Provider）的活跃成员，则该计划徽章将表明 Citrix 合作伙伴拥有此帐户。然后，使用合作伙伴标识来管理对其他云服务或功能的访问。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

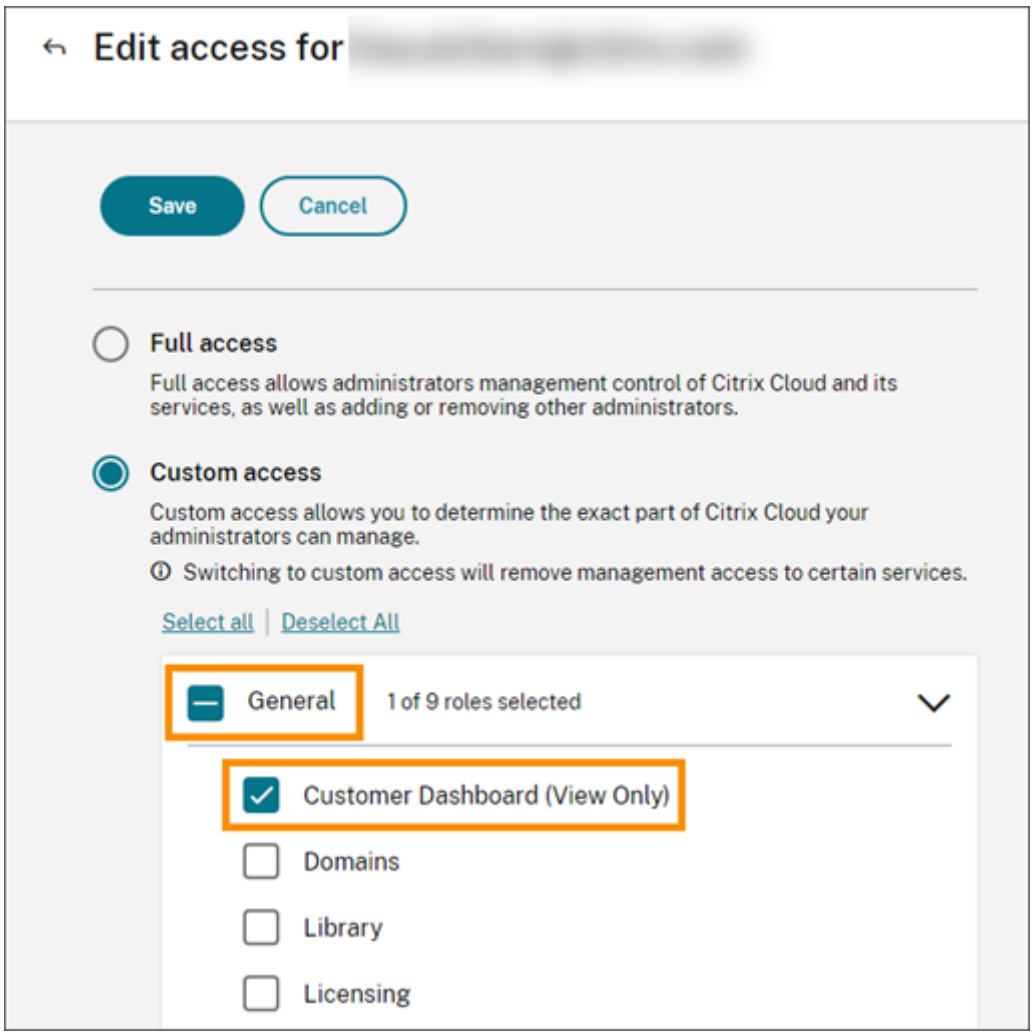
客户控制板

客户控制板专为合作伙伴设计，用来查看综合视图中的多个 Citrix Cloud 客户的状态。必须在合作伙伴与客户之间建立连接，才能使客户在控制板上显示。客户控制面板在带有合作伙伴徽章的 Citrix Cloud 帐户上可用。



默认情况下，完全访问权限管理员可以查看客户控制板。如果选择了客户控制板（仅限查看）权限，则自定义访问管理员可以查看控制面板。有关 Citrix Cloud 中管理员权限的更多信息，请参阅 修改管理员权限。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



合作伙伴与客户的联系

在 Citrix Cloud 解决方案上与客户合作的合作伙伴可以在其帐户之间建立可信链接。此帐户级别的关系使客户能够轻松与合作伙伴共享特定的信息。通过与合作伙伴建立联系，客户可以让合作伙伴了解有关其 Citrix Cloud 帐户及其与 Citrix 关系的信息。

建立合作伙伴连接将允许：

- 客户出现在合作伙伴的控制面板上
- 合作伙伴在客户的帐户设置中显示为活动连接
- 合作伙伴可以查看 Citrix Cloud 服务权利
- 合作伙伴可以了解 Citrix Cloud 授权的许可证使用情况和活跃使用情况

合作伙伴和客户建立联系后，合作伙伴管理员可以查看客户的基本帐户信息、客户下达的订单和权利信息，例如服务、许可证数量和到期日期。

合作伙伴与客户的联系不会过期。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

与多个合作伙伴或客户的联系

合作伙伴可以与多个客户建立联系。合作伙伴最多可以与 100 个客户帐户关联。如果合作伙伴需要管理 100 多个客户帐户，则他们必须使用不同的电子邮件地址创建一个单独的合作伙伴帐户来管理其他客户。或者，合作伙伴可以考虑删除他们不再需要管理的客户帐户。

客户可以与多个合作伙伴建立联系。客户与合作伙伴的连接数量没有限制。

连接通知

在以下情况下，Citrix Cloud 会向合作伙伴发送通知：

- 合作伙伴与客户建立联系
- 客户终止了与合作伙伴的连接

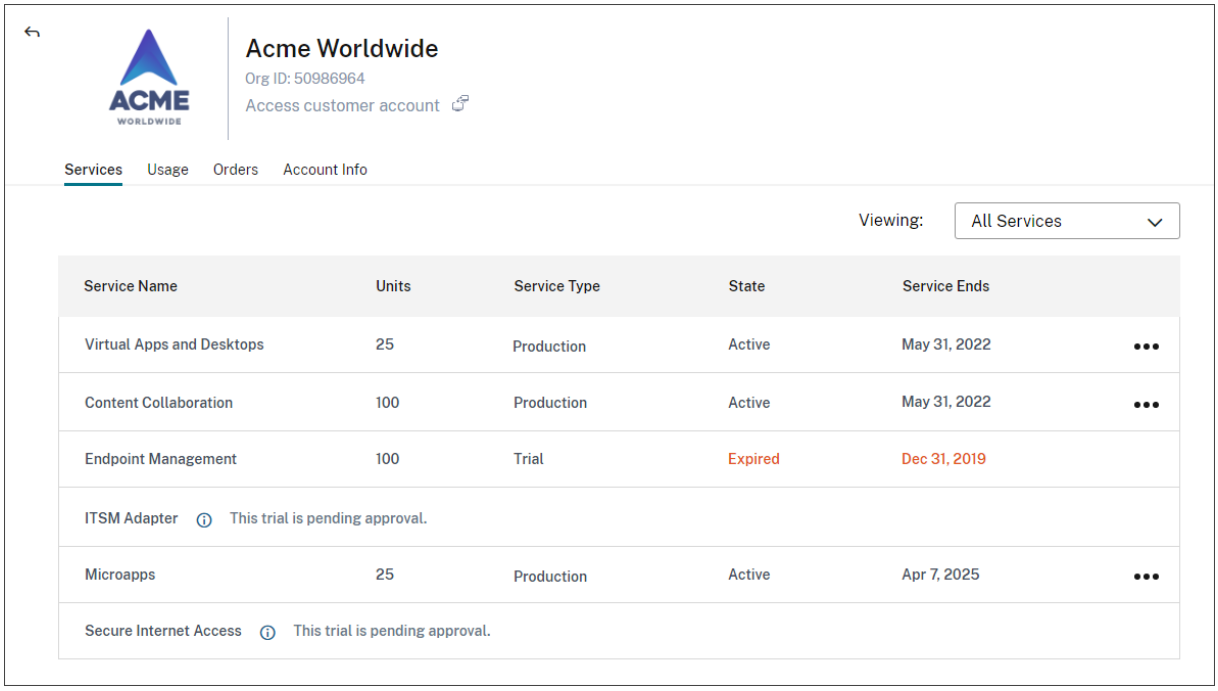
当合作伙伴终止与客户的连接时，Citrix Cloud 会向客户发送通知。

合作伙伴对服务权益的可见性

当与客户建立联系时，合作伙伴可以查看该客户的服务权利状态。此信息包括试用和非试用授权的状态。合作伙伴还可以查看以下信息：

- 活动的服务试用
- 挂起的服务试用请求
- 过期的服务试用
- 活动的服务授权（服务已购买，否则需要向客户授权或为其启用）
- 授权的许可证计数和过期日期

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



许可可见性仅限于查看许可证分配摘要和历史使用趋势。

与客户建立联系

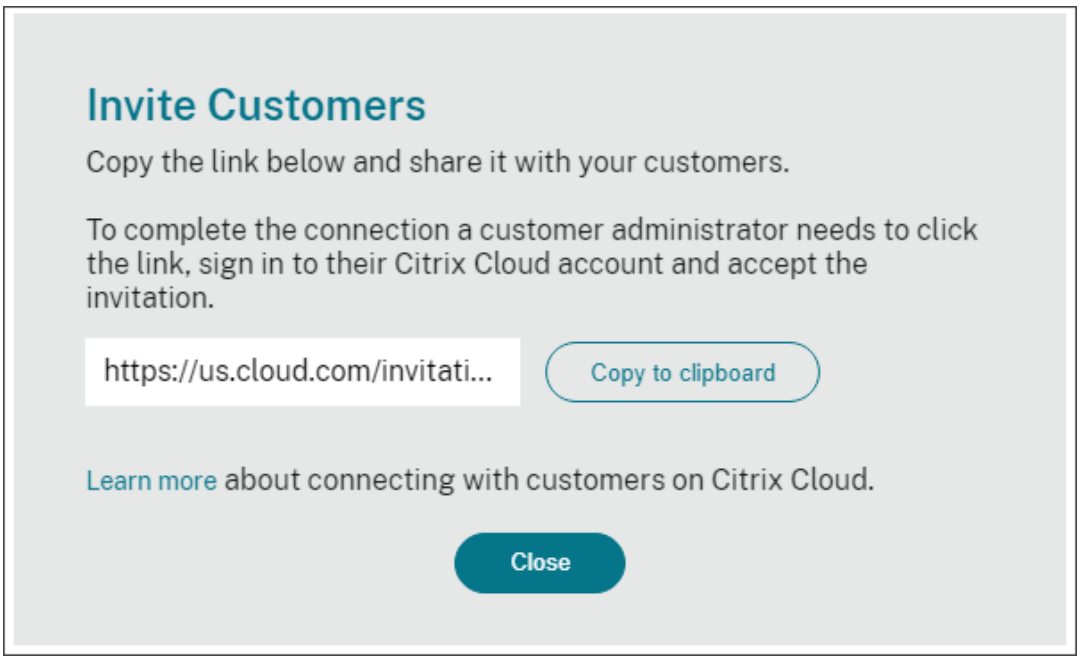
合作伙伴使用独特的邀请链接与客户建立联系。此链接已修复，无法更改或自定义。

合作伙伴可以无限次地使用其邀请链接来创建或重新创建连接。邀请链接不会过期。

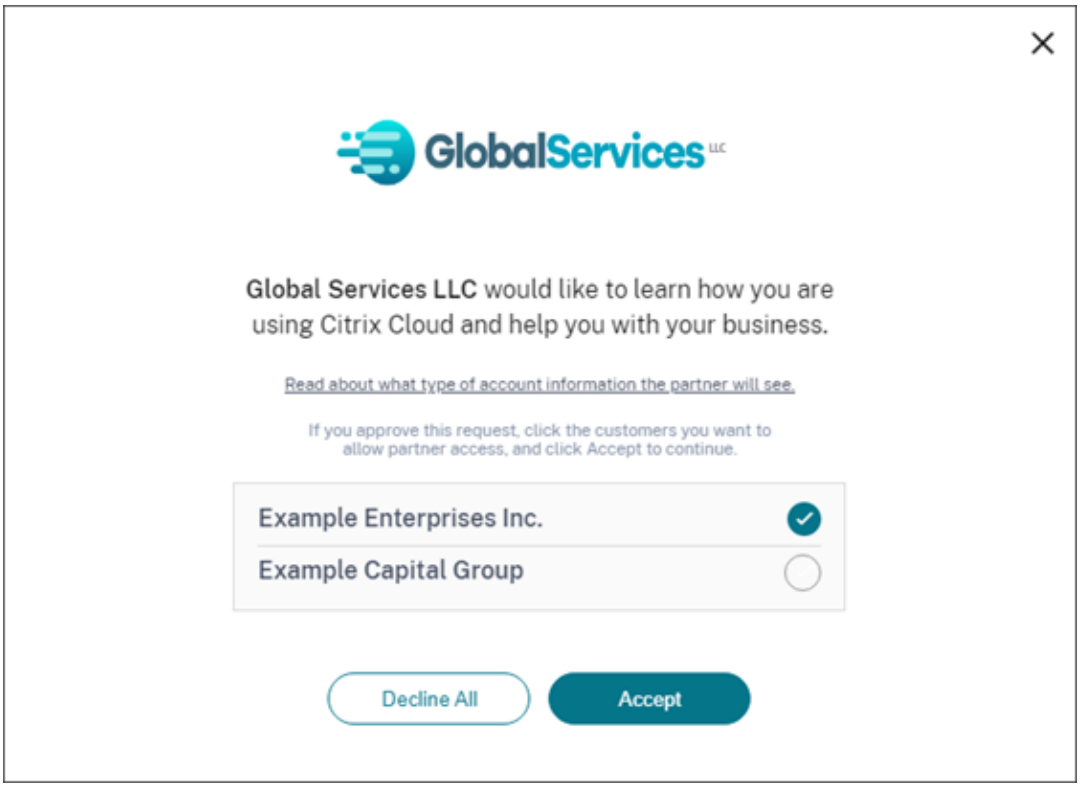
要创建连接，请执行以下操作：

1. 从 Citrix Cloud 菜单中，选择我的客户。
2. 在“Customer Dashboard”（客户控制板）中，选择 **Invite**（邀请）或 **Add**（添加）。
3. 要联系现有 Citrix Cloud 客户，请执行以下操作：
    a) 选择“邀请 **Citrix Cloud** 客户”，然后选择“继续”。
    b) 复制邀请链接并将其发送给客户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



要完成连接，客户点击邀请链接，登录 Citrix Cloud，然后接受邀请。



4. 要联系还没有 Citrix Cloud 帐户的新客户，请执行以下操作：

   a) 选择“添加客户”，然后选择“继续”。
   b) 输入客户的业务联系人详细信息，然后选择“完成”。Citrix Cloud 为客户创建了一个新帐户。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

之后，客户会收到一条通知，告知合作伙伴已作为管理员添加到新帐户。客户可以使用“忘记密码?”为新帐户设置密码 Citrix Cloud 登录页面上的链接。设置密码后，客户可以使用其企业电子邮件地址登录其帐户，并按照注册 Citrix Cloud 中所述完成登录流程。

移除合作伙伴或客户关系

合作伙伴或客户可以随时终止连接。

移除与客户的联系

要终止与客户的连接，合作伙伴要执行以下步骤：

1. 在控制台右上角的 Citrix Cloud 菜单中，选择“我的客户”。
2. 在客户控制面板中，找到您要管理的客户。
3. 单击客户的省略号菜单，然后选择删除客户连接。
4. 当系统提示您确认删除时，选择“删除”。

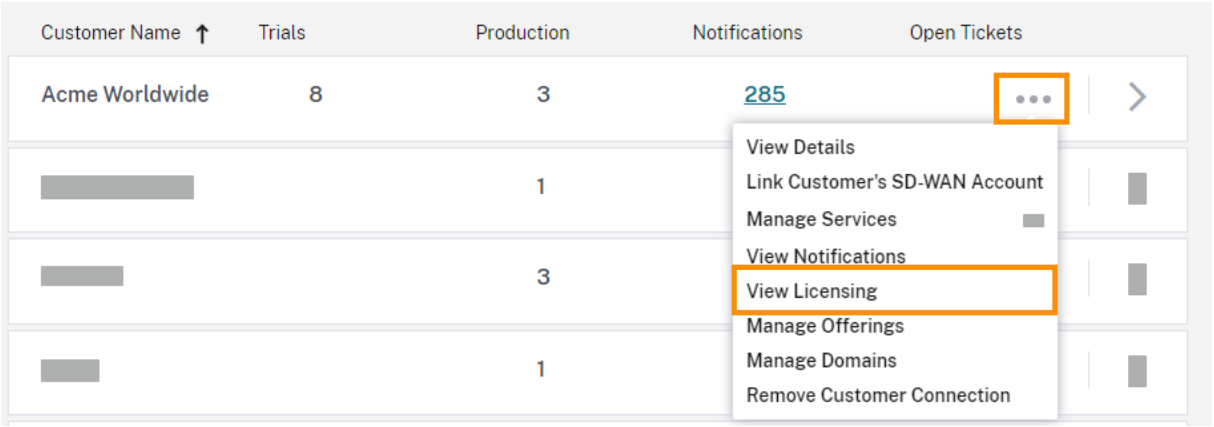
移除与合作伙伴的联系

要终止与合作伙伴的连接，客户需要执行以下步骤：

1. 从左上角的用户菜单中，选择帐户设置。
2. 在“公司帐户”页面中，找到“合作伙伴关系”部分。
3. 找到您要管理的合作伙伴，然后选择删除。
4. 当系统提示您确认删除时，选择确认。

许可趋势

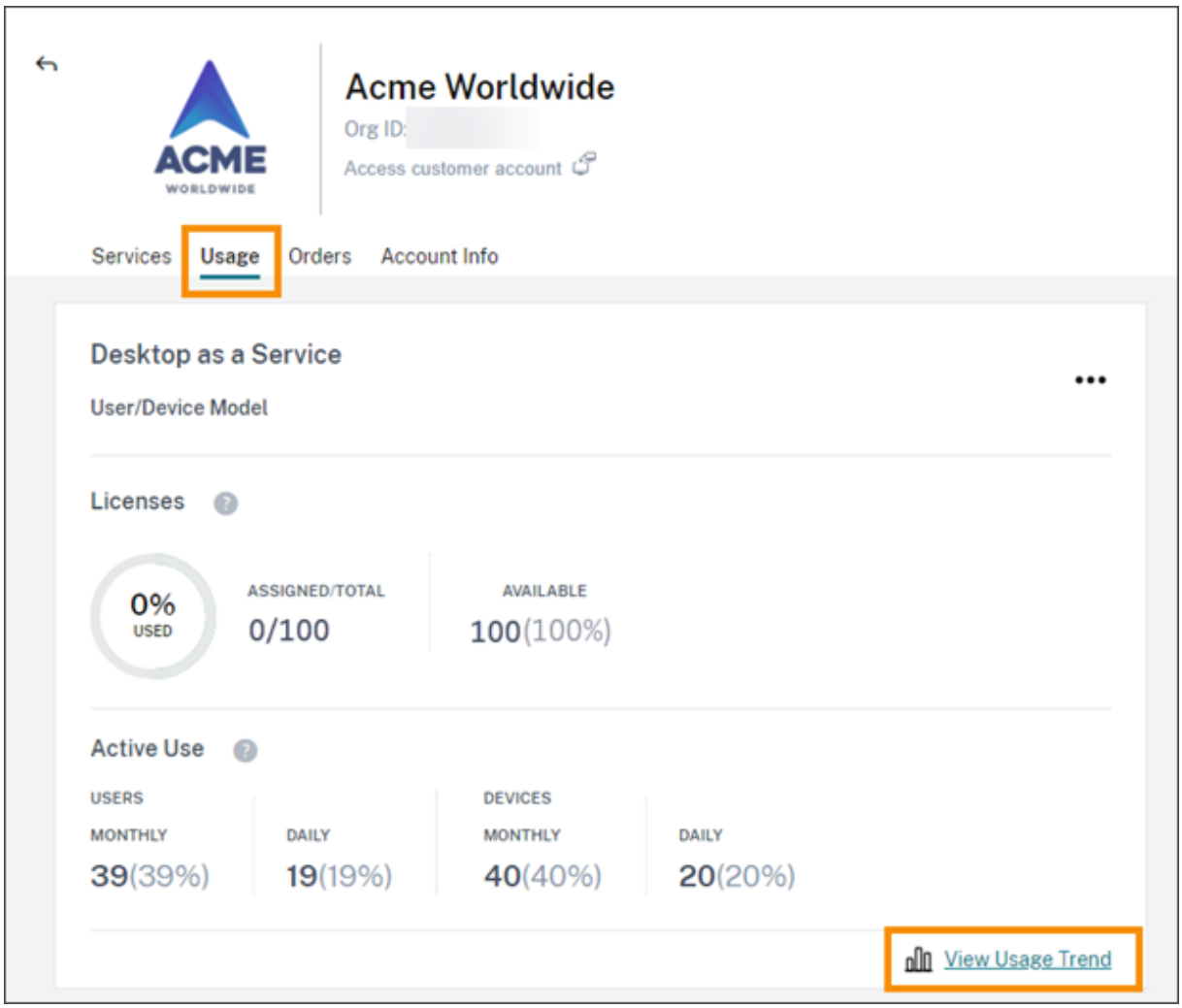
合作伙伴可以通过从客户控制板的省略号菜单中选择“查看许可”来查看客户的许可信息。



© 1999–2024 Cloud Software Group, Inc. All rights reserved.

> 注意：
>
> Citrix 合作伙伴只能查看许可摘要视图和历史活动使用趋势。他们无法查看为给定服务使用许可证的单个用户。

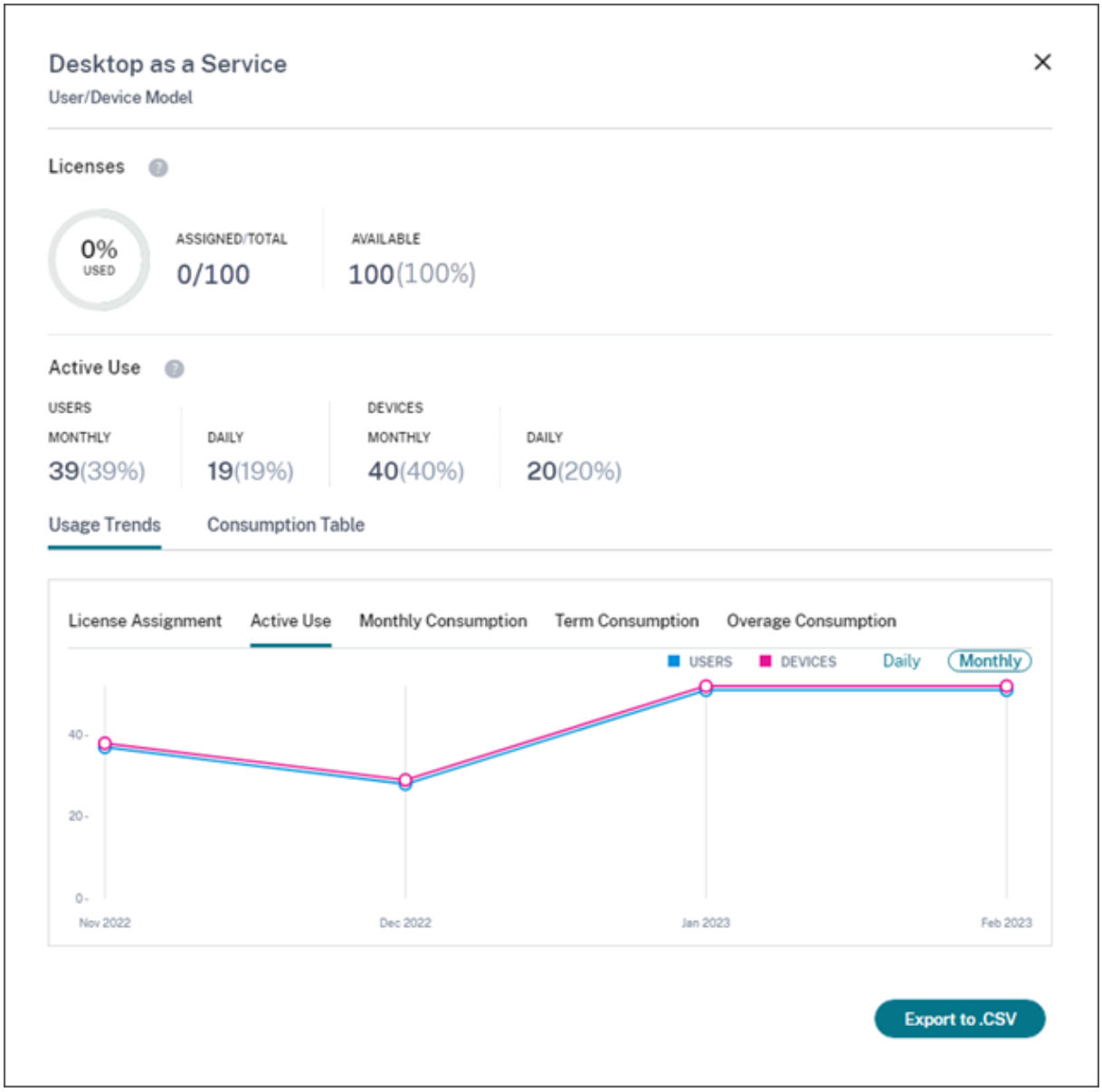
要查看客户对每项服务的许可摘要，请选择使用情况选项卡。有关更多使用信息，请选择要查看的服务授权的查看使用趋势。



根据服务的不同，使用趋势包括以下信息：

- 分配的许可证与购买的总许可证的比率
- 每月和每日活跃用户
- 许可证分配、活跃使用、每项权利的消耗量和超额的直观细分。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



如果需要，合作伙伴可以将此信息导出为.csv 文件。

带宽使用

对于 Citrix Gateway 服务，许可摘要包含以下信息：

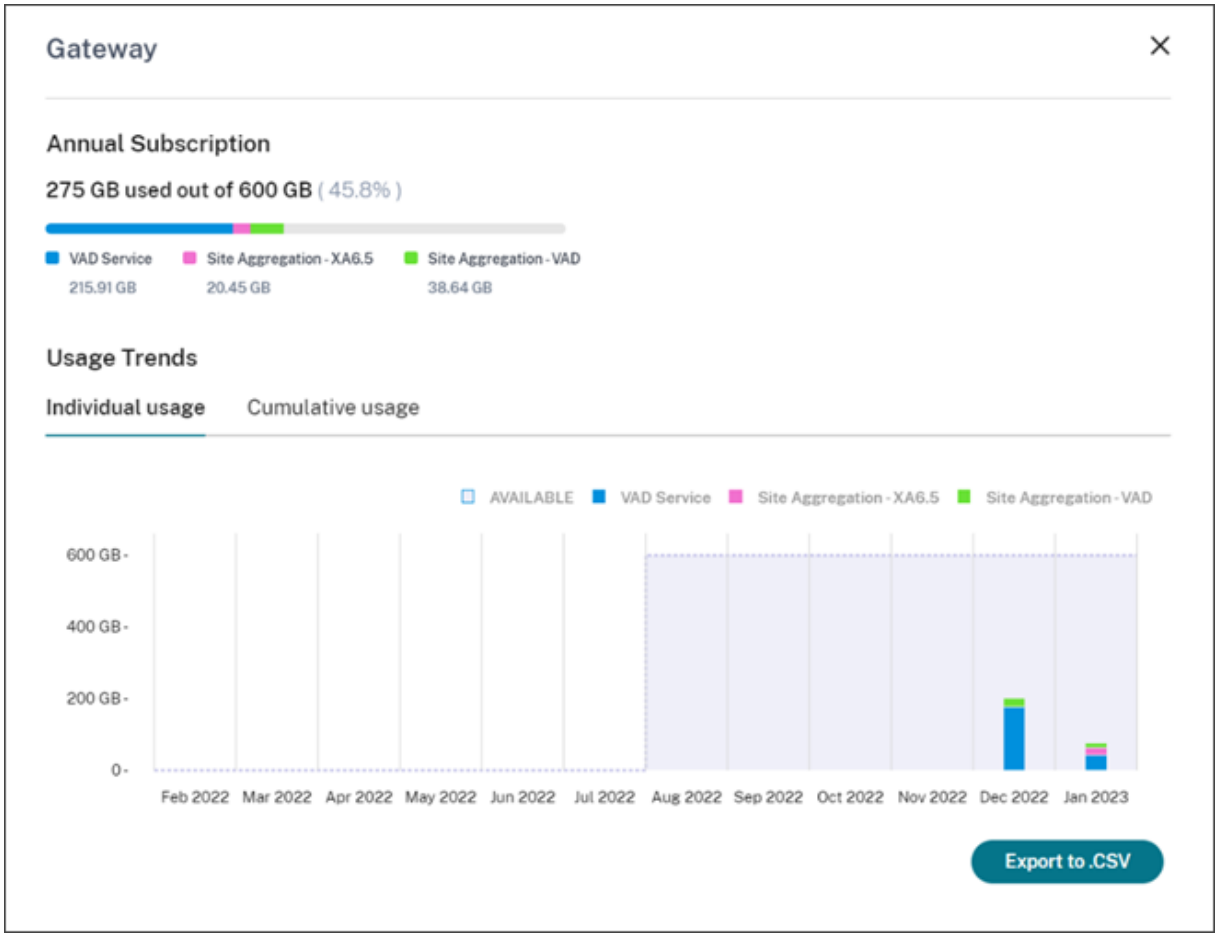
- 客户所有权利的总带宽使用量。
- 总带宽使用量按客户的每月、年度和定期权益细分。
- 当月的超额总量。有关如何计算超额的更多信息，请参阅超量。

选择页面最右侧的“查看使用趋势”以获得查看使用情况摘要的权限。选择“查看超额图表”以查看过去 12 个月的超额情况。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

根据权利的不同，使用趋势包括以下信息：

- Citrix DaaS（**VAD** 服务）和带有站点聚合的本地 Virtual Apps and Desktops 部署之间消耗的带宽量。
- 使用带宽的每个月的带宽使用情况的直观明细。（每月应享权利）
- 账单周期内每个月的个人带宽使用情况的直观明细。（年度和定期应享权利）
- 账单周期内每月累积的累计带宽使用量的直观明细。（年度和定期应享权利）



如果需要，合作伙伴可以将此信息导出为.csv 文件。

Citrix Service Provider 的客户许可和使用情况

Citrix Cloud 中的许可功能使 Citrix Service Provider (CSP) 的客户能够监视其受支持的 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops）产品的许可证和使用情况。CSP 也可以在其客户的 Citrix Cloud 帐户下登录以查看和导出此信息。有关详细信息，请参阅以下文章：

- Citrix DaaS 的客户许可证和使用情况监视
- Citrix DaaS Standard for Azure 的客户许可证和使用情况监视

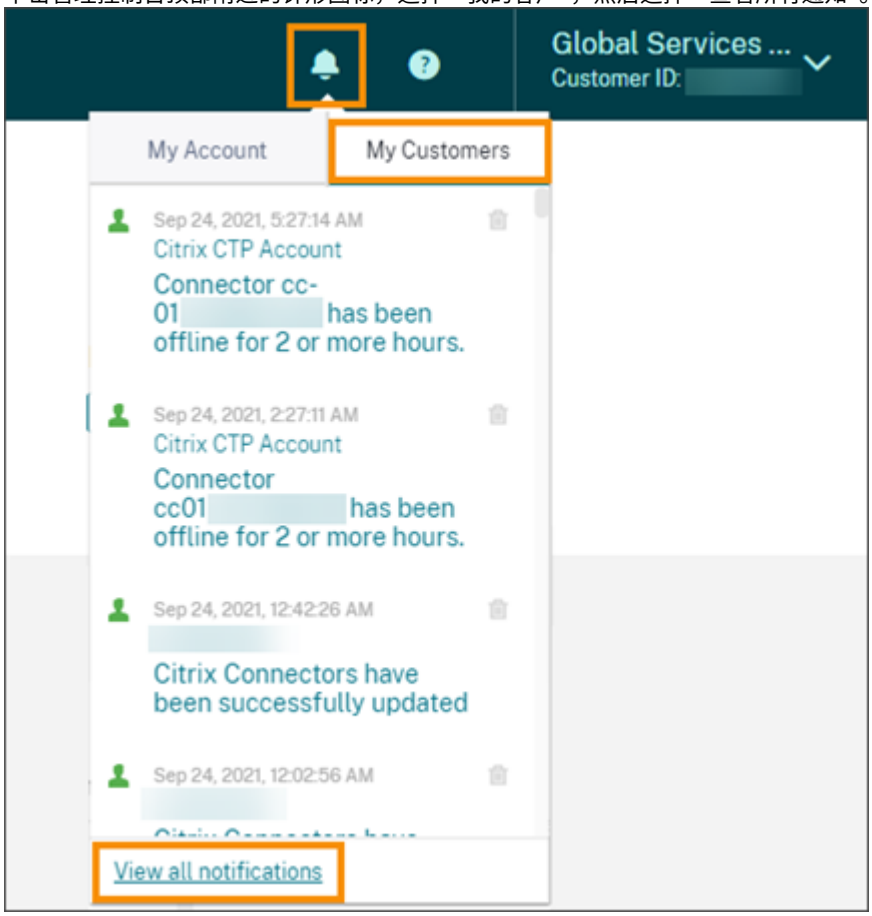
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

合作伙伴可见客户的通知和支持请求单

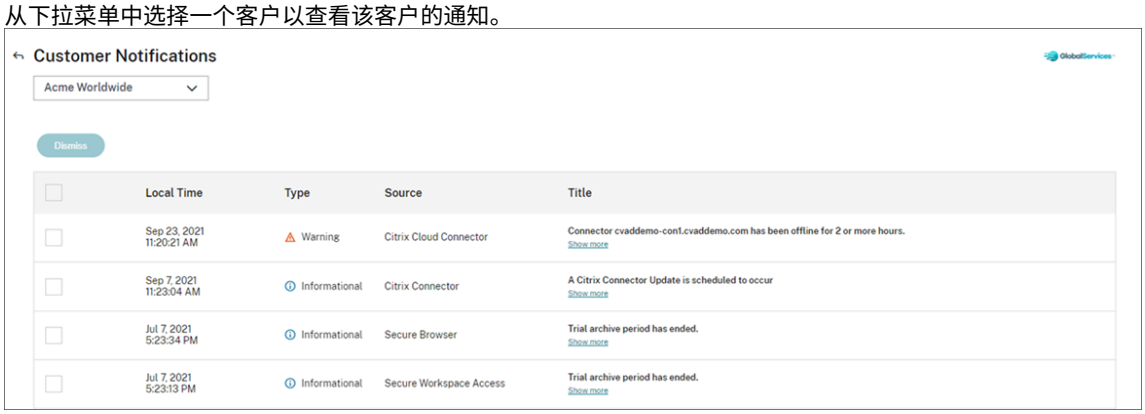
合作伙伴可以查看其关联客户的通知。合作伙伴还可以筛选特定于客户的通知并采取操作，例如取消通知。已解雇的通知不会显示给合作伙伴。但是，客户在登录 Citrix Cloud 后仍可以在其帐户中看到通知。

要查看客户通知，请执行以下操作：

1. 单击管理控制台顶部附近的钟形图标，选择“我的客户”，然后选择“查看所有通知”。

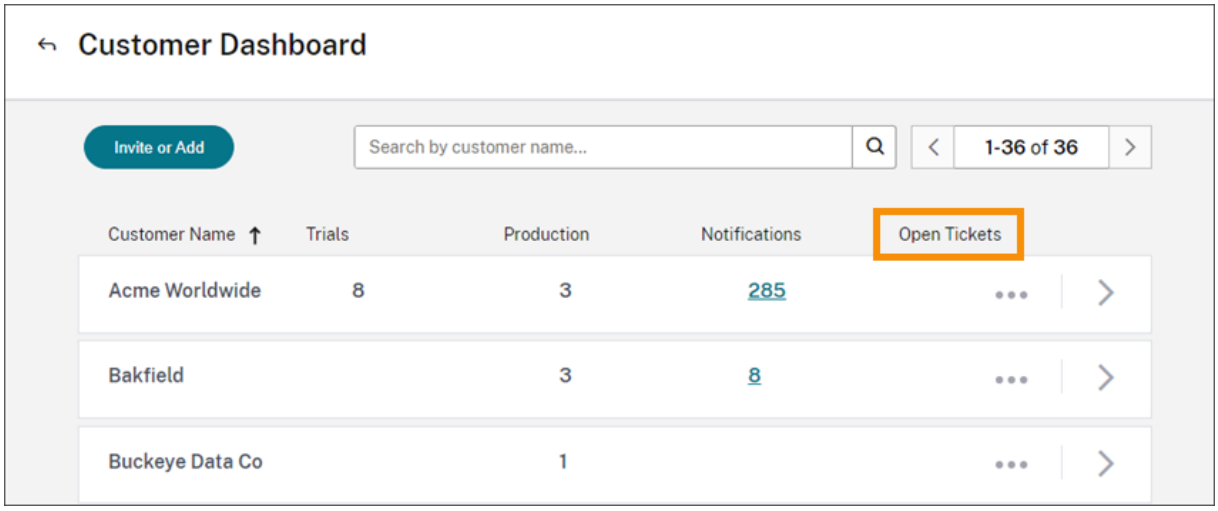


2. 从下拉菜单中选择一个客户以查看该客户的通知。



合作伙伴可以通过客户控制面板查看其客户的支持请求数量。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.



适用于 **Citrix Service Provider** 的联合域

联合域 _ 使客户用户能够使用附加到您的 *CSP* 资源位置的域中的凭据登录到工作区。这允许您使用自定义 *Workspace URL* 为客户用户提供专用工作区，例如 *_customer.cloud.com*。资源位置仍位于您的合作伙伴 Citrix Cloud 帐户中。您可以随客户可以使用您的 CSP Workspace URL（例如 csppartner.cloud.com）访问的共享工作区一起提供专用工作区。要使客户能够访问其专用工作区，可以将其添加到您管理的相应域中。配置工作区后，客户用户可以登录其工作区并访问您通过 Citrix DaaS 提供的应用程序和桌面。

当您将客户从联合域中移除时，该客户的用户将无法再使用合作伙伴域中的证书访问其工作区。

有关使用联合域交付应用程序和桌面的更多信息，请参阅适用于 Citrix Service Provider 的 Citrix DaaS。

Citrix Service Provider 的工作区外观选项

您可以使用自定义主题配置工作区颜色和徽标。要了解如何创建自定义主题，请参阅自定义工作区的外观。

> 注意
>
> 自定义主题是一项单租户功能。当前不支持服务提供商租户共享资源位置的 Citrix Service Provider、Cloud Connector 和 Active Directory 域（多租户）。完全支持拥有自己的专用资源位置、Cloud Connector 和专用 Active Directory 域（单租户）的 Citrix Service Provider 租户。

云服务

July 1, 2024

本文列出了通过 Citrix Cloud 提供的云服务以及每项服务的产品文档链接。有关这些服务及其所含产品的描述，请参阅 Citrix 服务的服务描述。

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

Citrix 服务

分析

- 安全分析
- 绩效分析
- 分析-使用情况

Citrix DaaS

Citrix DaaS Standard for Azure

Endpoint Management

网关

适用于 ServiceNow 的 ITSM 适配器

Remote Browser Isolation

Secure Private Access

Session Recording 服务

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

NetScaler 服务

控制台

App Delivery and Security

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall

© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).