自适应身份验证服务

Machine translated content

Disclaimer

Contents

发行说明

June 19, 2024

自适应身份验证发行说明是 NetScaler 发行说明的子集。自适应身份验证客户必须使用 NetScaler 发行说明来了解自适应身份验证服务中的增强功能、已修复的问题以及已知的问题。

> 注意：
>
> 本文档中的日期是指服务的最后一次升级日期。

16 Jan 2024

新增功能

- 自动升级自适应身份验证实例

自适应身份验证实例会自动升级到版本 14.1—12.35 及更高版本，以解决 CTX584986 中描述的安全漏洞。

2023 年 9 月 26 日

新增功能

- 自动升级自适应身份验证实例

自适应身份验证实例会自动升级到版本 14.1—8.50 及更高版本，以解决 CTX579459 中描述的安全漏洞。

2023 年 7 月 18 日

新增功能

- 自动升级自适应身份验证实例

自适应身份验证实例会自动升级到版本 13.1—49.101 及更高版本，以解决 CTX561482 中描述的安全漏洞。

2023 年 4 月 28 日

新增功能

- 通过负载平衡支持 **LDAP** 和 **LDAPS**

Citrix Adaptive Authentication 实例使用负载平衡虚拟服务器提供 LDAP 和 LDAPS 支持。有关更多详细信息，请参阅 LDAP 和 LDAPS 负载平衡配置示例。

[AAUTH-2067]

- 将后端 **AD** 或 **RADIUS** 服务器子网映射到资源位置

  管理员可以选择必须通过哪些连接器访问后端 AD 和 RADIUS 服务器。有关更多详细信息，请参阅 提供自适应身份验证。

已修复的问题

- NetScaler GUI 中缺少为自适应身份验证配置的智能访问策略和 OAuth 身份验证策略。

  [AAUTH-68]

已知问题

- 对于自适应身份验证实例，当您使用 LDAP 配置文件（NetScaler 管理界面）中的“测试连接”选项来检查连接时，即使无法访问 LDAP 服务器，它也会错误地显示为可访问。

  [AAUTH-2111]

配置自适应身份验证服务

June 19, 2024

配置自适应身份验证服务涉及以下高级步骤。

1. 提供自适应身份验证
2. 配置自适应身份验证策略
3. 为 Workspace 启用自适应身份验证

必备条件

- 为自适应身份验证实例预留 FQDN。例如 `aauth.xyz.com`，假定 `xyz.com` 是您的公司域。此 FQDN 在本文档中称为自适应身份验证服务 FQDN，在预配实例时使用。将 FQDN 与 IdP 虚拟服务器公有 IP 地址映射。此 IP 地址是在上载证书步骤中预配后获得的。
- 为 aauth.xyz.com 购买证书。证书必须包含 SAN 属性。否则证书不被接受。
- 自适应身份验证 UI 不支持上载证书捆绑包。要链接中间证书，请参阅 配置中间证书。

- 为本地 AD/RADIUS 连接选择连接类型。以下两个选项可用。如果您不希望数据中心连通性，请使用连接器连接类型。
  - **Citrix Cloud Connector** - 有关详细信息，请参阅 Citrix Cloud Connector。
  - **Azure vNet** 对等互连 - 有关详细信息，请参阅使用 Azure vNet 对等连接设置与本地身份验证服务器的连接。
- 配置网络时间协议 (NTP) 服务器以避免时间偏差。有关详细信息，请参阅 如何将系统时钟与网络上的服务器同步。

需要注意的事项

- Citrix 建议不要为任何自适应身份验证实例运行清除配置，也不要修改任何带有前缀 AA （例如 AAuthAuto-Config）的配置，包括证书。这会中断自适应身份验证管理，并影响用户访问。恢复的唯一方法是通过重新预配。
- 请勿在自适应身份验证实例上添加 SNIP 或任何其他路由。
- 如果客户 ID 不全为小写，则用户身份验证失败。您可以将您的 ID 全部转换为小写字母，然后使用 `set cloud parameter -customerID <all_lowercase_customerid>` 命令在 NetScaler 实例上进行设置。
- Citrix Workspace 或 Citrix Secure Private Access 服务所需的 nFactor 配置是客户应该直接在实例上创建的唯一配置。目前，NetScaler 中没有阻止管理员进行这些更改的检查或警告。
- 建议所有自定义配置都是在用户界面中进行的，而不是直接在自适应身份验证实例上进行的。这是因为在实例上所做的更改不会自动与用户界面同步，因此更改会丢失。
- 请勿将自适应身份验证实例升级为随机 RTM 构建。所有升级均由 Citrix Cloud 管理。
- 仅支持基于 Windows 的 Cloud Connector。此版本不支持 Connector Appliance。
- 如果您是 Citrix Cloud 的现有客户并且已经配置了 Azure AD（或其他身份验证方法），则要切换到自适应身份验证（例如，Device Posture 检查），则必须将自适应身份验证配置为身份验证方法，并在自适应身份验证实例中配置身份验证策略。有关详细信息，请参阅 将 Citrix Cloud 连接到 Azure AD。
- 对于 RADIUS 服务器部署，请将所有连接器私有 IP 地址添加为 RADIUS 服务器中的 RADIUS 客户端。
- 在当前版本中，不允许使用外部 ADM 代理，因此不支持 Citrix Analytics (CAS)。
- NetScaler Application Delivery Management 服务为您的自适应身份验证实例收集备份。要从 ADM 中提取备份，请载入 ADM 服务。有关详细信息，请参阅配置备份和还原。Citrix 不会从自适应身份验证服务显式获取备份。如有必要，客户必须从 Application Delivery Management 服务中获取其配置的备份。
- 如果在客户设置中配置了代理，则自适应身份验证实例无法建立通道。因此，建议您禁用自适应身份验证的代理配置。
- 如果您使用第三方身份验证服务，例如 SAML，如果未找到所有声明，则身份验证可能会失败。因此，建议客户在多因素身份验证配置中添加其他因素，例如 NOAUTH，以通过所有声明。
- 建议您在正常操作期间保持禁用调试日志级别，并且仅在需要时启用。如果始终启用调试日志级别，则会给管理 CPU 造成巨大负载。在高流量负载期间，这可能会导致系统崩溃。有关详细信息，请参阅 CTX222945。

如何配置自适应身份验证服务

访问自适应身份验证用户界面

您可以通过以下方法之一访问自适应身份验证用户界面。

- 手动键入 URL https://adaptive-authentication.cloud.com。
- 使用您的凭据登录并选择客户。

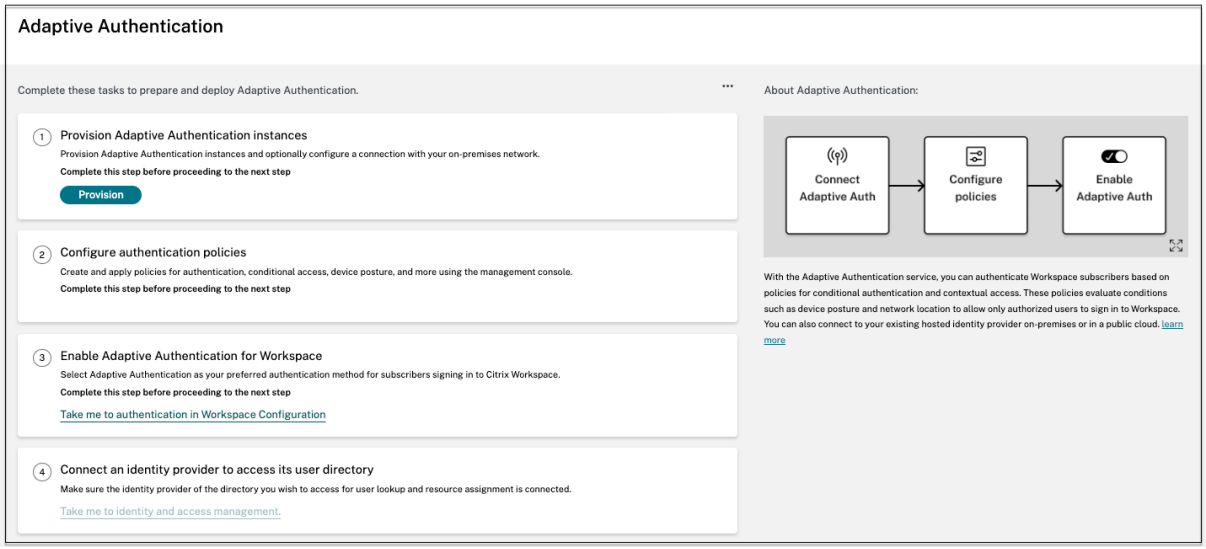
  成功通过身份验证后，您将被重定向到自适应身份验证用户界面。

或者

- 导航到 **Citrix Cloud >** 身份识别和访问管理。
- 在“身份验证”选项卡的“自适应身份验证”中，单击省略号菜单，然后选择管理。

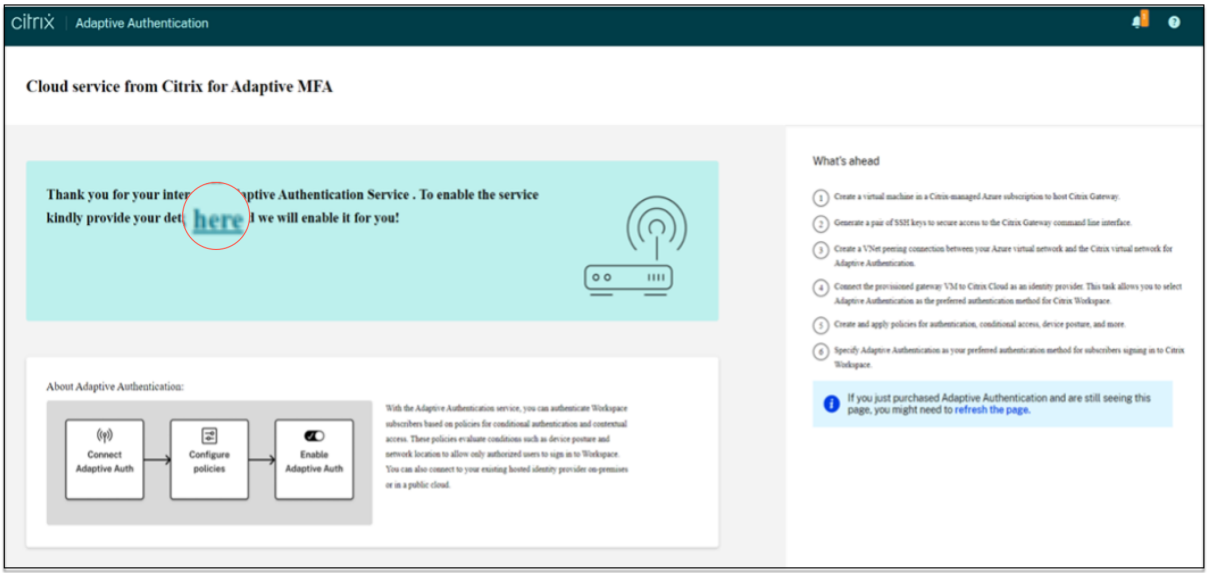
此时将显示自适应身份验证用户界面。

下图说明了配置自适应身份验证所涉及的步骤。



步骤 **1**：设置自适应身份验证

> 重要：
>
> 对自适应身份验证服务感兴趣的客户必须单击以下屏幕截图所示的链接，然后填写 Podio 表单。然后，Citrix 自适应身份验证团队可以配置自适应身份验证实例。



执行以下步骤来配置自适应身份验证实例：

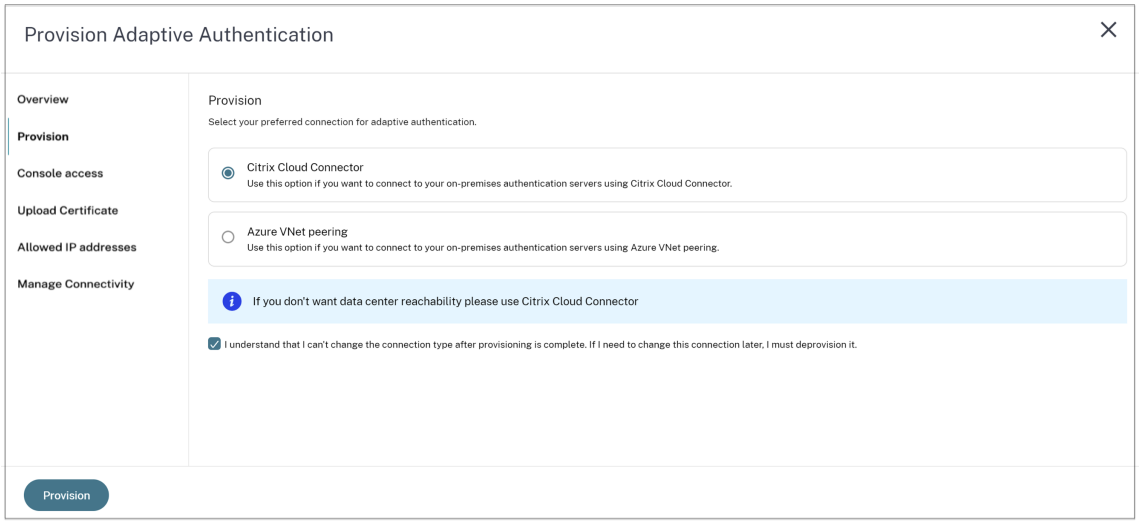
1. 在 自适应身份验证 UI 上，单击 设置。
2. 为自适应身份验证选择首选连接。

   - **Citrix Cloud Connector**：对于这种连接类型，您必须在本地网络中设置连接器。Citrix 建议您在环境中至少部署两个 Citrix Cloud Connector，以建立与 Azure 上托管的 Citrix Gateway 的连接。必须允许您的 Citrix Cloud Connector 访问为自适应身份验证实例保留的域/URL。例如，允许 https://aauth.xyz.com/*。

     有关 Citrix Cloud Connector 的详细信息，请参阅 Citrix Cloud Connector。

   - **Azure VNet** 对等 -必须使用 Azure 的 VNet 对等互连来设置服务器之间的连接。

     - 确保您有 Azure 订阅帐户来设置连接。
     - 正在进行对等互连的客户 VNet 必须已配置 Azure VPN 网关。有关详细信息，请参阅 https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal。



要将 **Citrix Cloud Connector** 添加为首选连接，请执行以下操作：

执行以下步骤。

- 选择 **Citrix Cloud Connector** 选项，然后选中“最终用户协议”复选框。
- 单击 设置。设置配置可能需要长达 30 分钟。

> 注意：
>
> 对于连接器连接类型，请确保在预配后可从连接器虚拟机访问自适应身份验证 FQDN。

要设置 **Azure VNet** 对等互连，请执行以下操作：

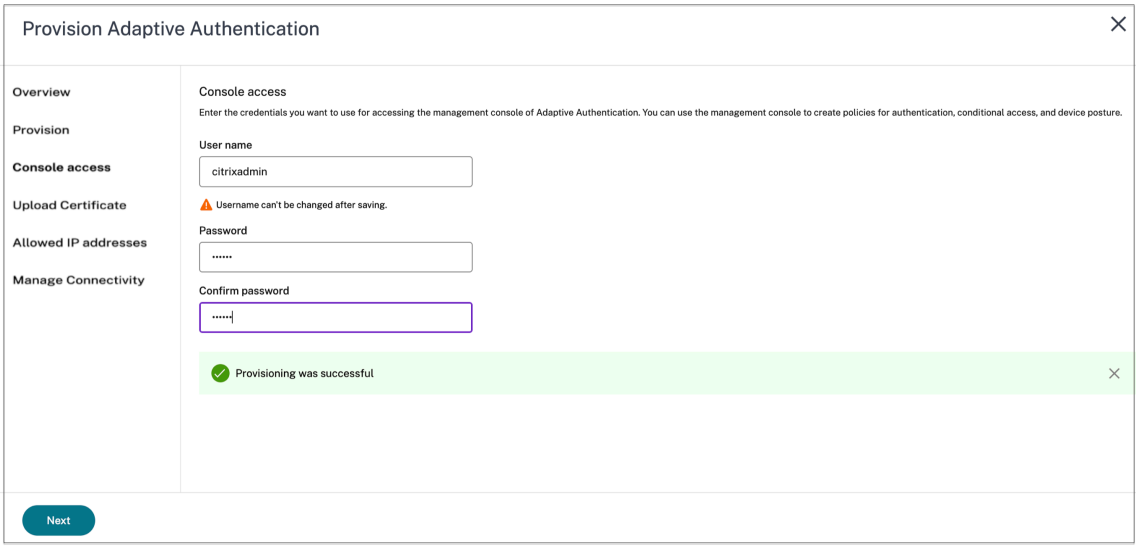
如果选择 **Azure VNet** 对等互连作为连接，则必须添加必须用于预配自适应身份验证实例的子网 CIDR 块。您还必须确保 CIDR 块不会与贵组织的其他网络范围重叠。

有关详细信息，请参阅 使用 Azure VNet 对等互连设置与本地身份验证服务器的连接。

3. 设置凭据以访问您为自适应身份验证启用的实例。您需要管理控制台访问权限才能创建身份验证、条件访问等策略。

   a) 在 控制台访问 屏幕中，输入用户名和密码。
   b) 单击下一步。

> 注意：
>
> 通过控制台访问屏幕创建的用户将获得具有 shell 访问权限的“超级用户”权限。



4. 添加自适应身份验证服务 FQDN 并上载证书密钥对。
   您必须为可公开访问的身份验证服务器输入您选择的自适应身份验证服务 FQDN。此 FQDN 必须是可公开解析的。

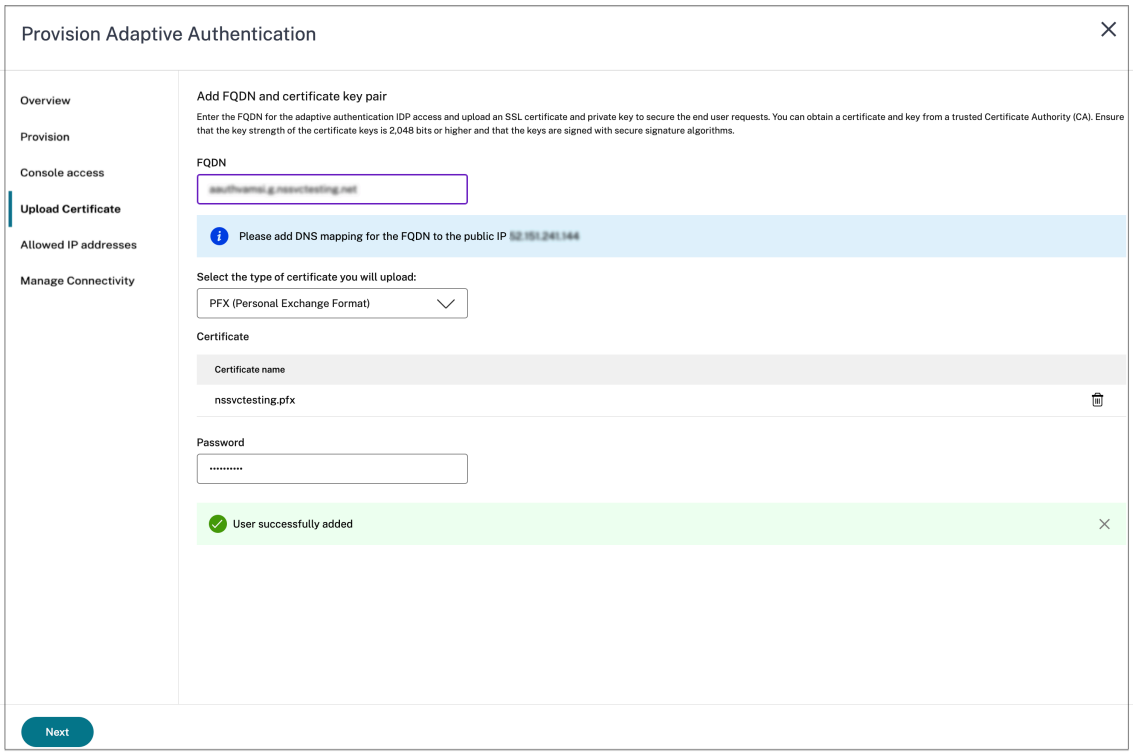
   a) 在 上载证书 屏幕中，输入您为自适应身份验证保留的 FQDN。

   b) 选择证书类型。

      - 自适应身份验证服务支持 PFX、PEM、DER 类型的证书，用于配置实例。
      - 只有类型为 PEM 的证书才支持证书捆绑包。对于其他捆绑包类型，Citrix 建议安装根证书和中间证书并将它们链接到服务器证书。

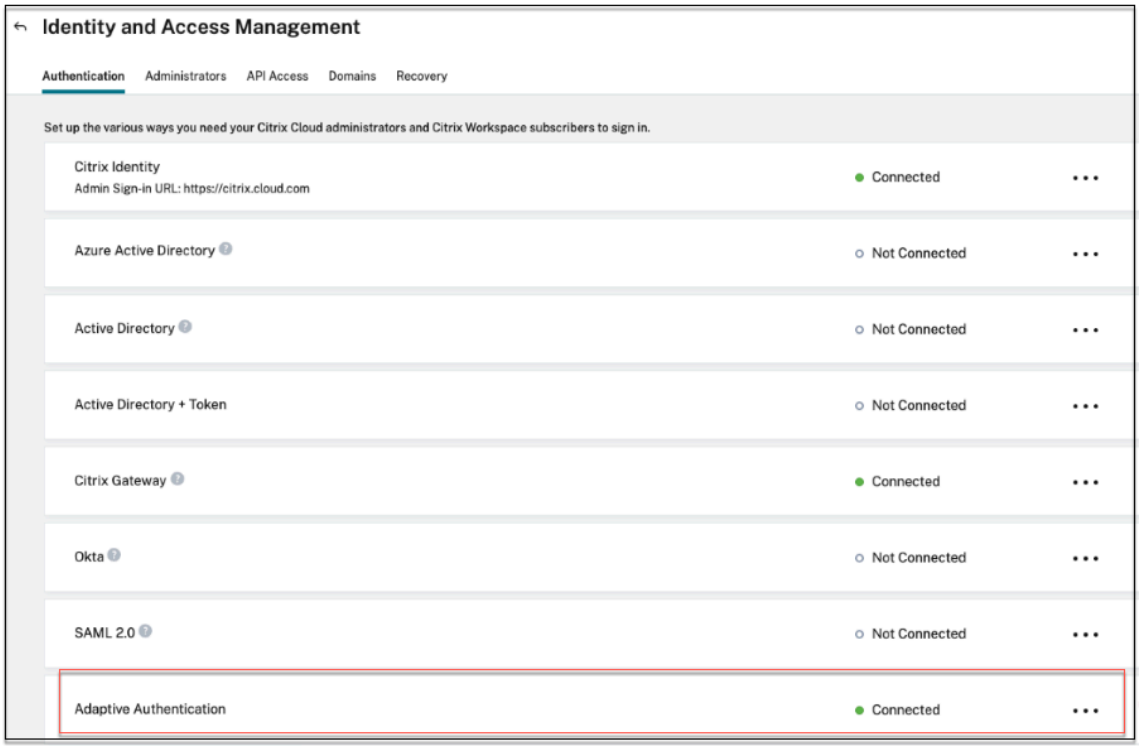
   c) 上载证书和密钥。

> 注意：
>
> - 在自适应身份验证实例上安装中间证书，并将其与服务器证书链接。
>
> ```
> 1. 登录自适应身份验证实例。 1. 导航到**流量管理 > SSL**。有关详细信息，请参阅 [配置中间证书](/en-us/citrix-gateway/current-release/install-citrix-gateway/certificate-management-on-citrix-gateway/configure-intermediate-certificate.html)。
> ```
>
> - 只接受公共证书。不接受由私有或未知 CA 签名的证书。
> - 只能使用自适应身份验证用户界面进行证书配置或证书更新。请勿直接在实例上更改它，因为这可能会导致不一致。



5. 上载证书和密钥。

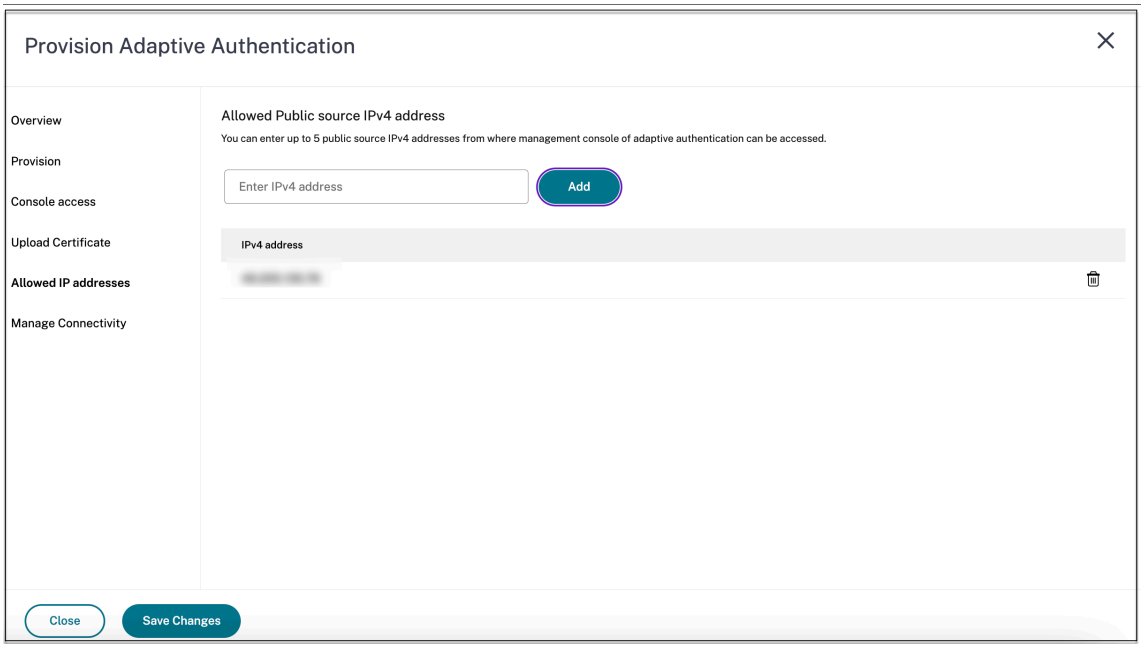
自适应身份验证实例现在已连接到身份和访问管理服务。自适应身份验证方法状态显示为已连接。



6. 设置一个 IP 地址，通过该地址可以访问自适应身份验证管理控制台。

a) 在 允许的 **IP** 地址 屏幕中，为每个实例输入一个公有 IP 地址作为管理 IP 地址。要限制对管理 IP 地址的访问，可以添加多个允许访问管理控制台的 IP 地址。

b) 要添加多个 IP 地址，必须单击“添加”，输入 IP 地址，然后单击“完成”。必须为每个 IP 地址执行此操作。如果不单击“完成”按钮，则 IP 地址不会添加到数据库中，而只会添加到用户界面中。



7. 如果您使用连接器连接类型，请指定一组资源位置（连接器），通过这些位置可以访问 AD 或 RADIUS 服务器。如果您使用的是 vNet 对等连接类型，则可以跳过此步骤。

   管理员可以选择必须通过哪些连接器访问后端 AD 和 RADIUS 服务器。要启用此功能，客户可以在其后端 AD/RADIUS 服务器子网之间设置映射，这样，如果身份验证流量属于特定子网，则该流量将定向到特定的资源位置。但是，如果资源位置未映射到子网，则管理员可以指定使用这些子网的通配符资源位置。

   以前，使用循环方法将本地 AD/RADIUS 的自适应身份验证流量定向到任何可用的资源位置。这给拥有多个资源地点的客户带来了问题。

   a) 在“自适应身份验证”用户界面上，单击“管理连接”。

   b) 输入子网详细信息并选择相应的资源位置。

      > 注意：
      >
      > 如果清除“为剩余子网使用任何可用资源位置”复选框，则只有定向到已配置子网的流量才会被传输。

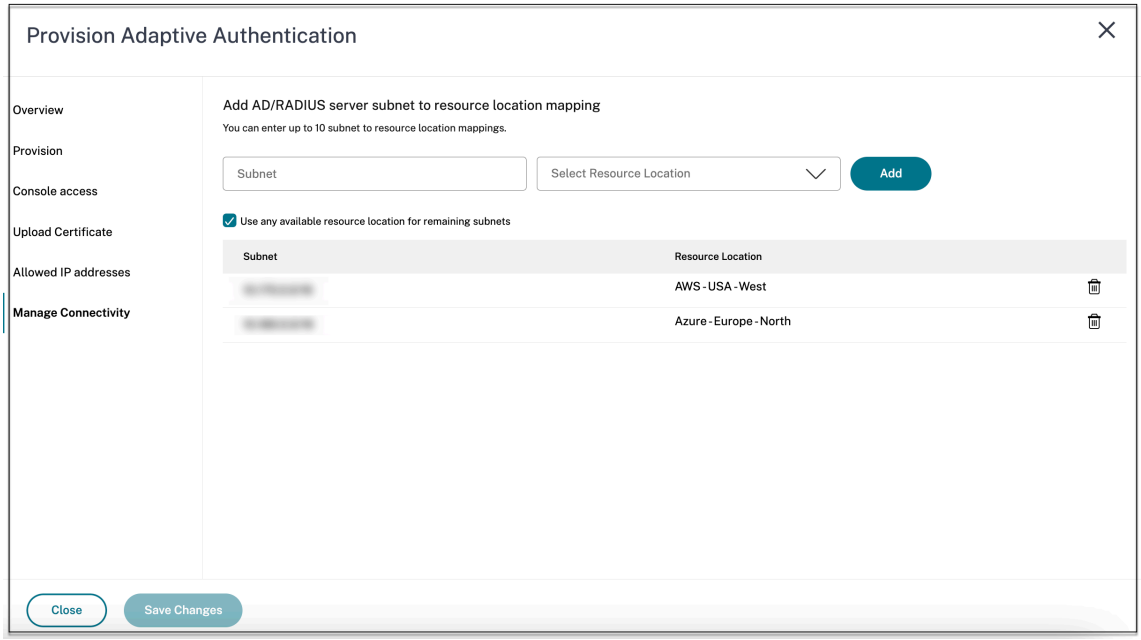
   c) 单击“添加”，然后单击“保存更改”。

> 注意：
>
> - 只允许使用 RFC1918 IP 地址子网。
> - 每个客户的子网资源位置映射数量限制为 10。

- 多个子网可以映射到单个资源位置。
- 同一个子网不允许重复条目。
- 要更新子网条目，请删除现有条目，然后更新。
- 如果您重命名或删除资源位置，请务必从“自适应身份验证”用户界面的“管理连接”屏幕中删除该条目。
- 使用以下 CLI 命令对资源位置映射所做的任何更改都会被用户界面（自适应身份验证预配 > 管理连接）推送的更改所覆盖。

```
- set cloudtunnel parameter -subnetResourceLocationMappings

- set policy expression aauth_allow_rfc1918_subnets
   <>
- set policy expression aauth_listen_policy_exp <>
```



预配自适应身份验证现已完成。

步骤 2：配置自适应身份验证策略

如何连接到您的自适应身份验证实例：

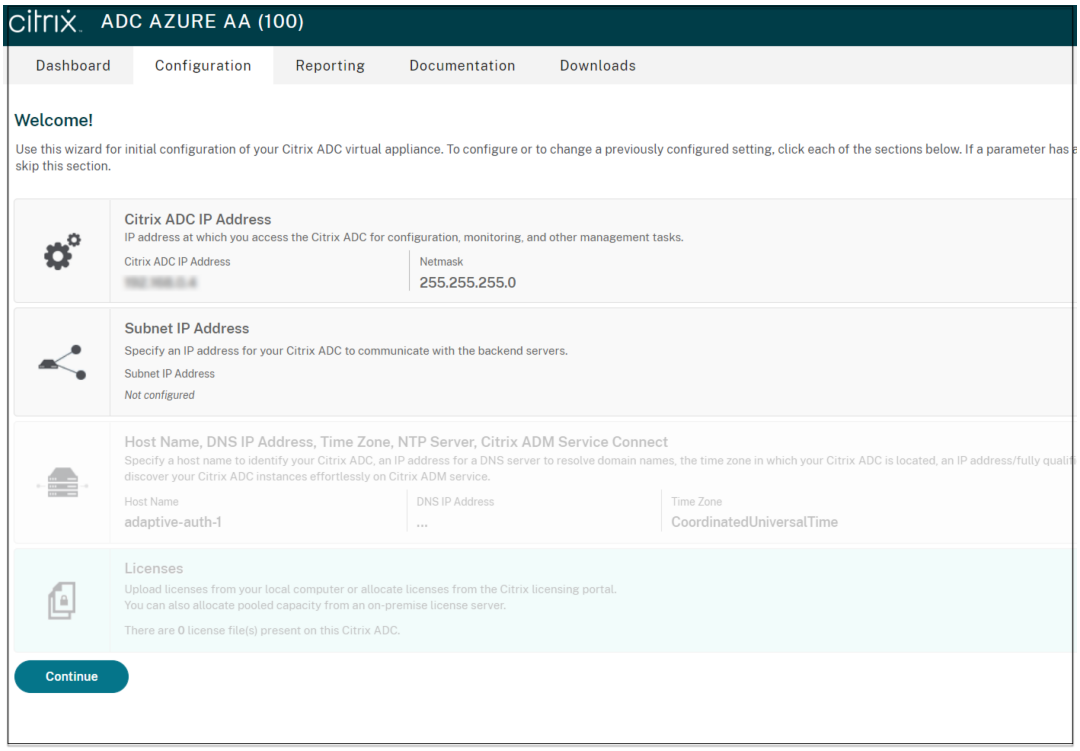
预配完成后，您可以直接访问自适应身份验证管理 IP 地址。您可以使用 FQDN 或您的主 IP 地址访问自适应身份验证管理控制台。

> 重要提示：
>
> - 在高可用性设置中，作为同步过程的一部分，证书也会同步。因此，请确保使用通配符证书。
> - 如果您需要每个节点的唯一证书，请将证书文件和密钥上载到任何未同步的文件夹（例如，在 nsconfig/SSL 目录中创建一个单独的文件夹 (nosync_cert)），然后在每个节点上唯一上载证书。

访问自适应身份验证管理控制台：

- 要使用 FQDN 访问自适应身份验证管理控制台，请参阅为 ADC 管理界面访问配置 SSL。
- 要使用您的主地址访问自适应身份验证，请执行以下操作：

1. 从 GUI 的“配置身份验证策略”部分复制主 IP 地址，然后在浏览器中访问该 IP 地址。
2. 使用您在配置时输入的凭据登录。
3. 单击继续。



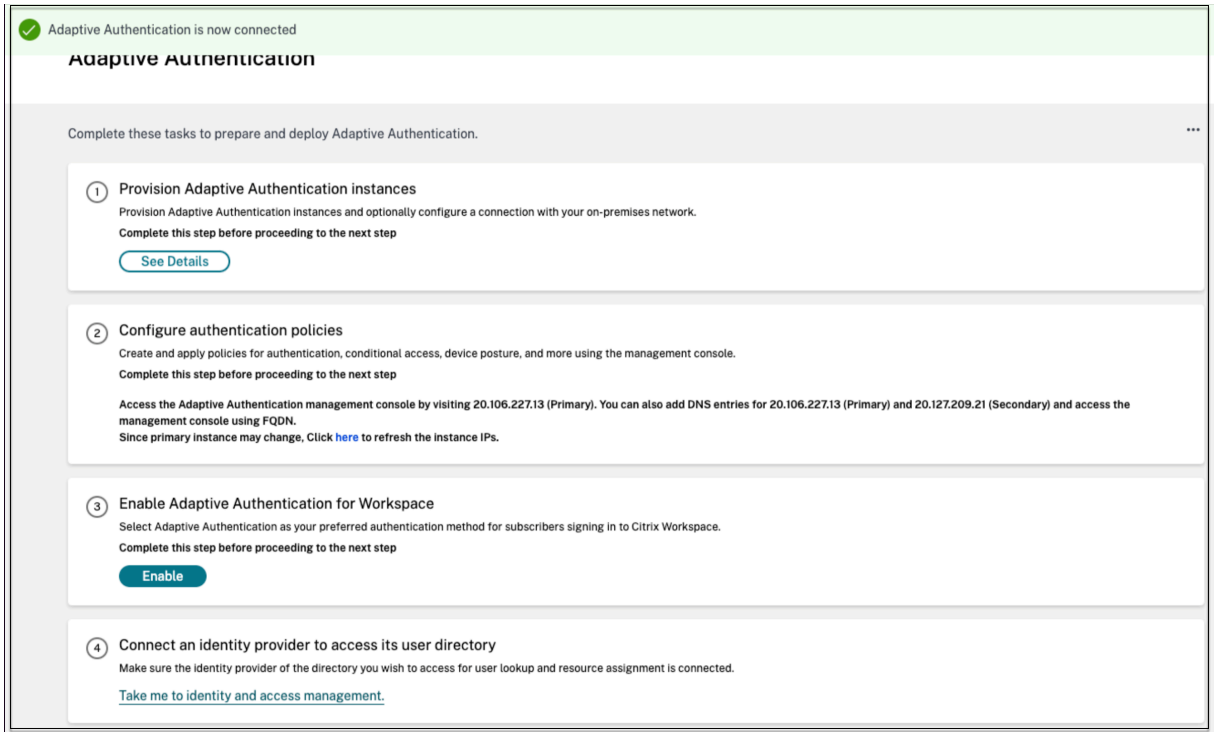
4. 导航到 **Configuration**（配置）**> Security**（安全）**> AAA - Application Traffic**（**AAA -** 应用程序流量）**> Virtual Servers**（虚拟服务器）。
5. 添加身份验证策略。有关各种使用案例，请参阅 身份验证配置示例。

> 注意：
>
> 使用 IP 地址访问自适应身份验证实例是不可信的，许多浏览器会发出警告来阻止访问。我们建议您使用 FQDN 访问自适应身份验证管理控制台，以避免任何安全屏障。您必须为自适应身份验证管理控制台保留 FQDN，并将其映射为主要和辅助管理 IP 地址。

> 例如，如果您的自适应身份验证实例 IP 为 192.0.2.0，辅助身份验证实例 IP 为 192.2.2.2，则；
>
> - primary.domain.com 可以映射到 192.0.2.0
> - secondary.domain.com 可以映射到 192.2.2.2

步骤 3：为 **Workspace** 启用自适应身份验证

预配完成后，您可以通过单击为 **Workspace** 启用自适应身份验证部分中的启用来启用 Workspace 的身份验证。



> 注意：
>
> 至此，自适应身份验证配置就完成了。当您访问 Workspace URL 时，必须重定向到自适应身份验证 FQDN。

相关参考文献

- 编辑 FQDN
- 安排自适应身份验证实例的升级
- 取消预配您的自适应身份验证实例
- 启用对网关的安全访问
- 使用 Azure VNet 对等互连设置与本地身份验证服务器的连接
- 自定义 Workspace URL 或虚名 URL
- 配置备份和还原
- 负载平衡的 LDAPS 配置示例

- 将身份验证方法迁移到自适应身份验证
- 身份验证配置示例

相关自适应身份验证配置

October 21, 2024

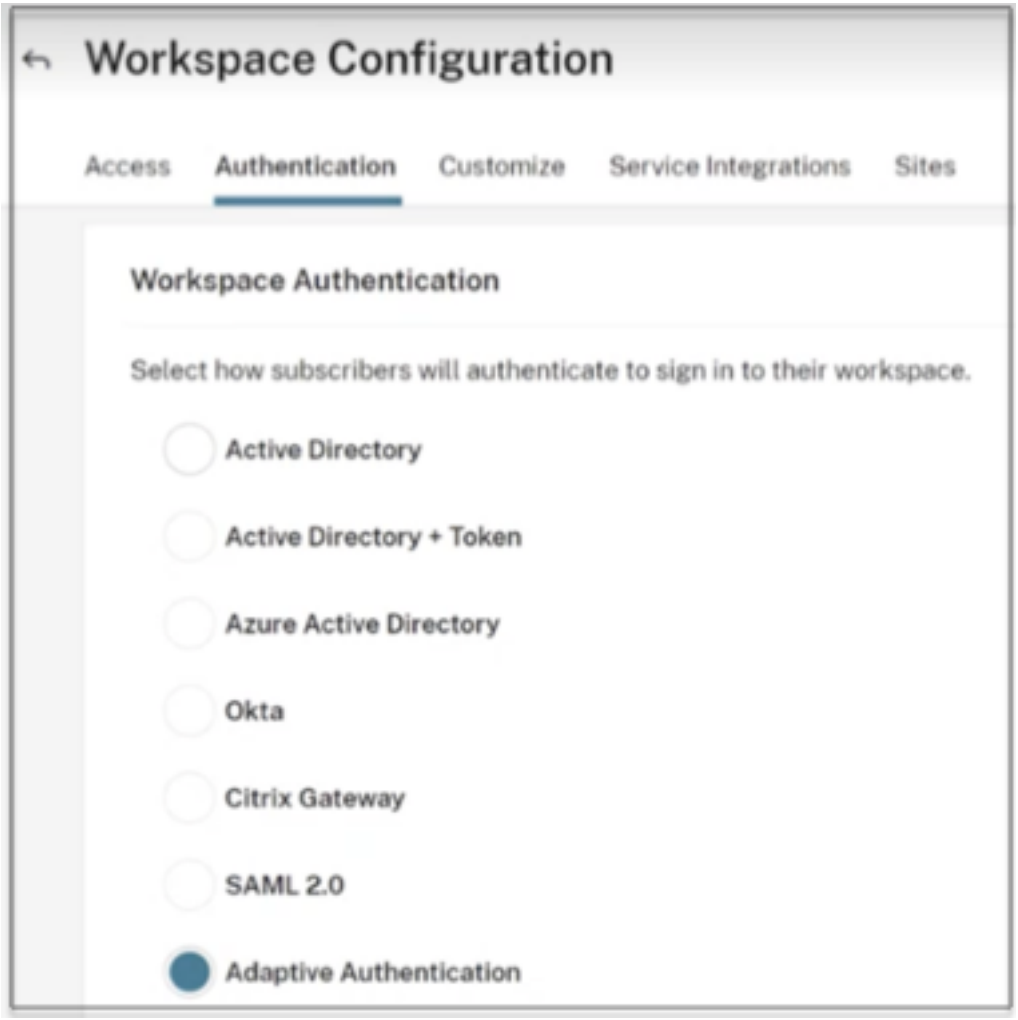
编辑 **FQDN**

如果出现以下情况，则无法编辑 FQDN 自适应身份验证 被选为 Workspace 配置中的身份验证方法。您必须切换到其他身份验证方法才能编辑 FQDN。但是，如有必要，您可以编辑证书。

> 重要提示：
>
> - 在修改 FQDN 之前，请确保将新 FQDN 映射到 IdP 虚拟服务器公有 IP 地址。
> - 连接到 **Citrix** 网关 使用 OAuth 策略必须将身份验证方法迁移到 自适应身份验证. 有关详细信息，请参阅 将身份验证方法迁移到自适应身份验证.

要编辑 FQDN，请执行以下操作：

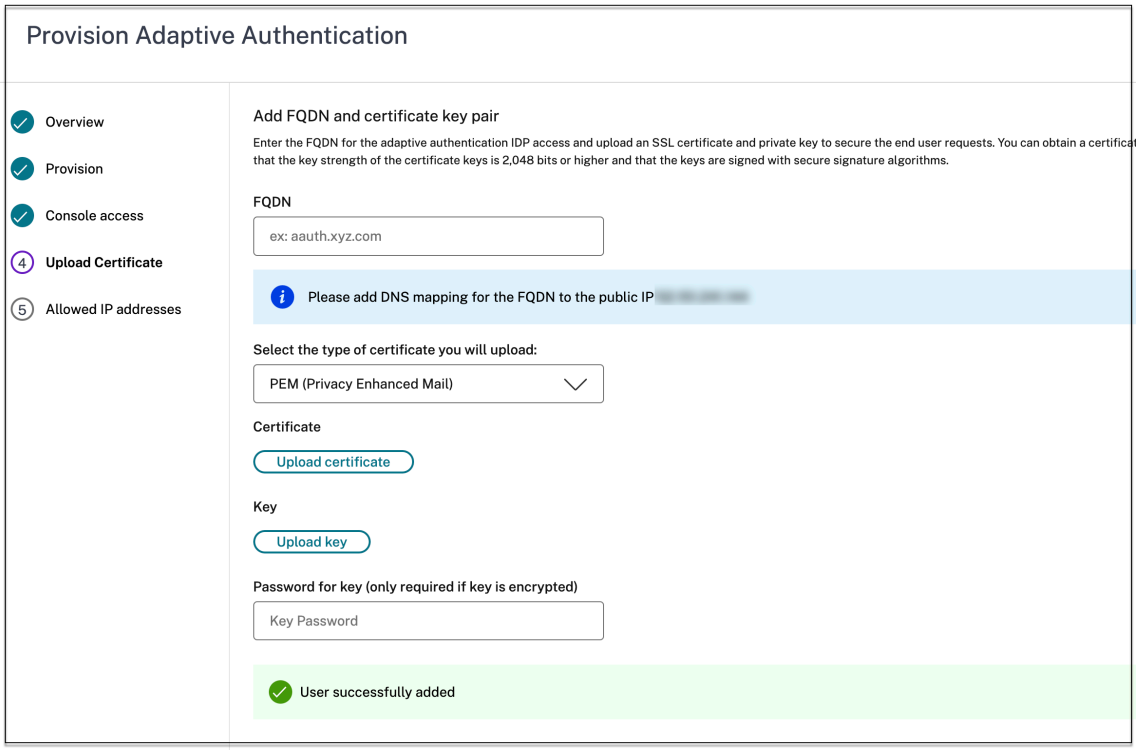
1. 切换到其他身份验证方法 自适应身份验证.



2. 选择 我了解对订阅者体验的影响，，然后单击 确认.

   单击 确认，则最终用户的工作区登录会受到影响，并且在再次启用自适应身份验证之前，自适应身份验证不会用于身份验证。因此，建议您在维护时段内修改 FQDN。

3. 在 上传证书 屏幕上，修改 FQDN。



4. 点击 保存更改.

> 重要提示：
>
> 如果编辑 FQDN，还必须再次上传证书。

1. 单击 Adaptive Authentication 方法，再次启用 Adaptive Authentication 方法 使（步骤 3）。

2. 单击 刷新。

自定义工作区 **URL** 或虚 **URL**

自定义工作区 URL 允许您使用所选的域访问 Citrix Workspace 应用商店。用户可以使用默认 Workspace URL 和/或自定义 Workspace URL 访问 Workspace。

要配置自定义工作区 URL 或虚 URL，必须执行以下操作：

1. 配置您的自定义域。有关详细信息，请参阅 配置自定义域.
2. 使用与当前或默认配置文件（AAuthAutoConfig_oauthIdpProf）相同的客户端 ID、密钥和受众配置新的 OAuthIDP 配置文件，但使用不同的重定向 URL。有关详细信息，请参阅 配置 OAuth 策略和配置文件.

示例：

当前概况：

```
-add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf
 -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https
://accounts-internal.cloud.com/core/login-cip"-audience zzzz -
sendPassword ON

add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol -
rule true -action AAuthAutoConfig_oauthIdpProf

bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol
 -priority 100 -gotoPriorityExpression NEXT
```

新配置文件：

```
add authentication OAuthIDPProfile AAuthAutoConfig_oauthIdpProf_Custom1
 -clientID xxxx -clientSecret yyyy -encrypted -encryptmethod
ENCMTHD_3 -kek -suffix 2023_07_09_20_09_30 -redirectURL "https://
custom_domain/core/login-cip"-audience zzzz -sendPassword ON

add authentication OAuthIdPPolicy AAuthAutoConfig_oauthIdpPol_Custom1
 -rule true -action AAuthAutoConfig_oauthIdpProf_Custom1

bind authentication vserver auth_vs -policy AAuthAutoConfig_oauthIdpPol_Cu
 -priority 101 -gotoPriorityExpression NEXT
```

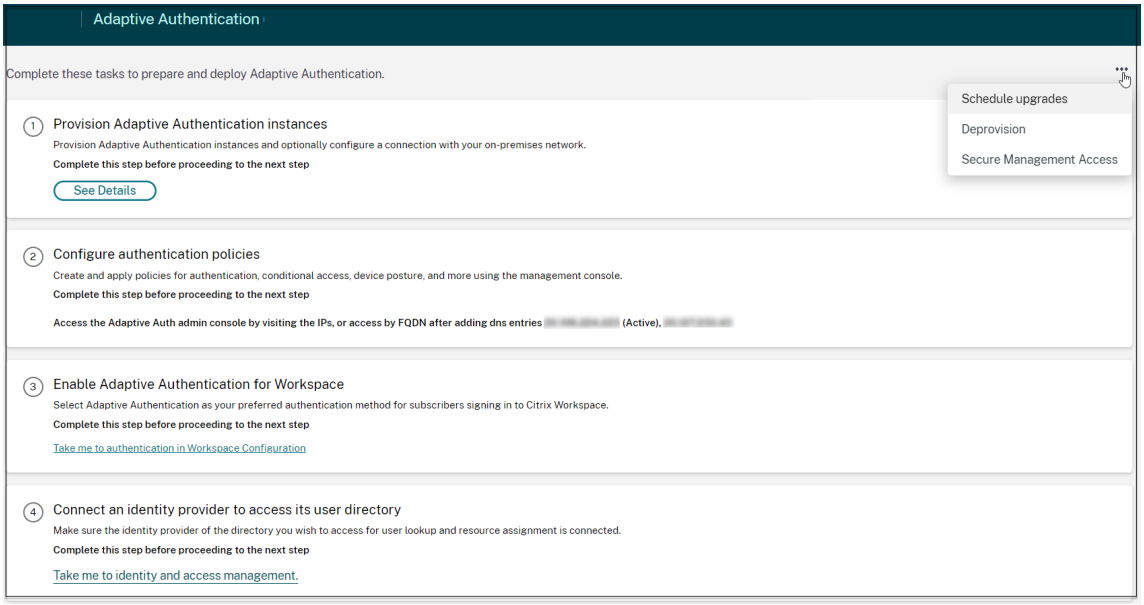
> 重要提示：
>
> - OAuth 策略和配置文件由 Adaptive Authentication 服务在预置阶段创建。因此，Citrix Cloud 管理员无权访问未加密的客户端密钥。您可以从 ns.conf 文件获取加密的密钥。要创建 OAuth 配置文件，您必须使用加密的密钥并仅使用 CLI 命令创建配置文件。
> - 您无法使用 NetScaler 用户界面创建 OAuth 配置文件。

计划自适应身份验证实例的升级

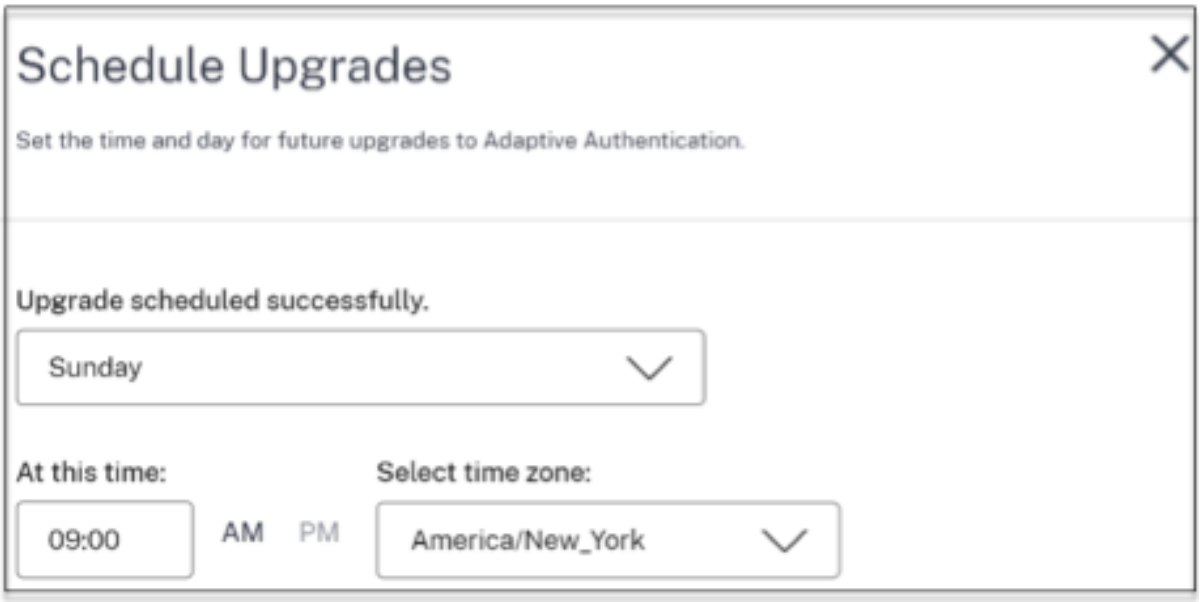
对于当前站点或部署，您可以选择用于升级的维护时段。

> 重要提示：
>
> 请勿将 Adaptive Authentication 实例升级到随机 RTM 版本。所有升级均由 Citrix Cloud 管理。

1. 在 自适应身份验证 UI 中，在 预置自适应身份验证实例 部分中，单击省略号按钮。



2. 点击 计划升级.
3. 选择升级的日期和时间。



取消预配 **Adaptive Authentication** 实例

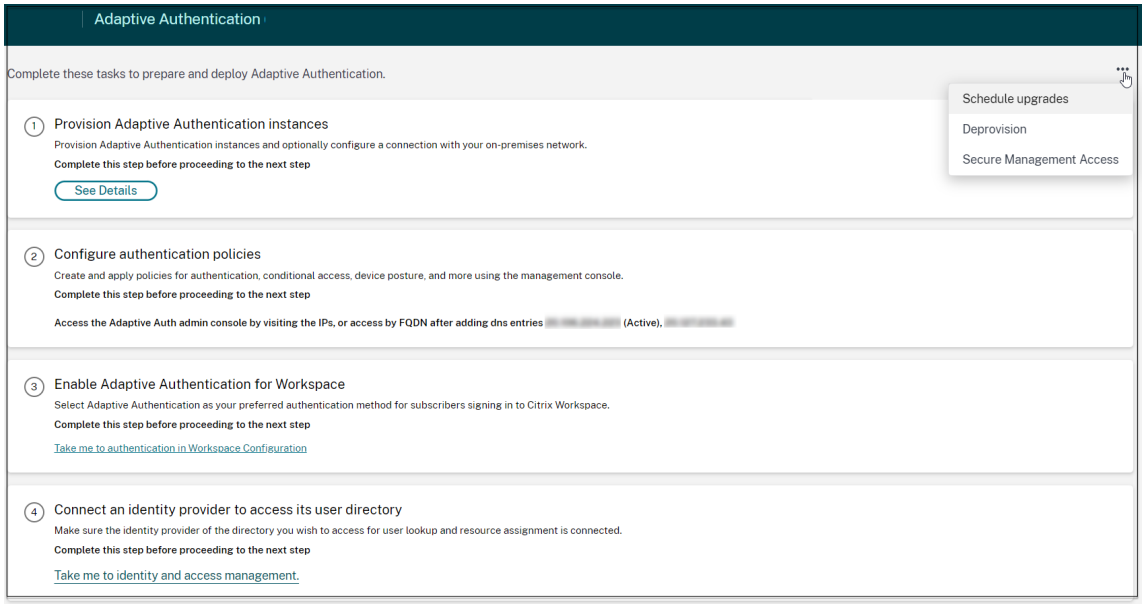
在以下情况下，客户可以根据 Citrix 支持的建议取消配置自适应身份验证实例。

- 自适应身份验证实例不可访问（尤其是在计划升级之后），但这种情况可能不会发生。
- 如果客户必须从 VNet 对等互连模式切换到连接器模式，或者相反。
- 如果客户在预置 VNet 对等模式时选择了错误的子网（子网与其数据中心或 Azure VNet 中的其他子网冲突）。

> 注意：
>
> 取消配置还会删除实例的配置备份。因此，您必须下载备份文件并保存，然后才能取消置备自适应身份验证实例。

执行以下操作以取消配置自适应身份验证实例：

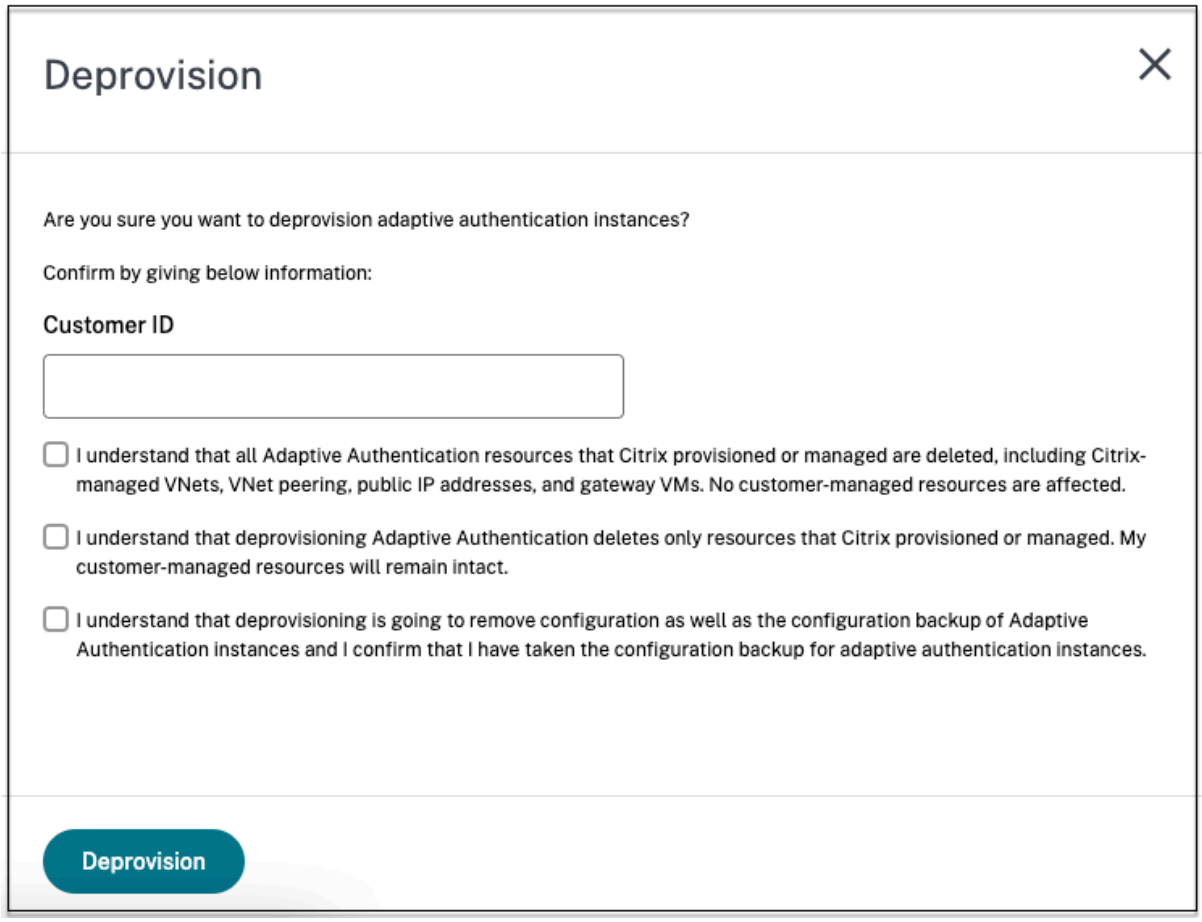
1. 在 自适应身份验证 UI 中，在 预置自适应身份验证实例 部分中，单击省略号按钮。



2. 点击 取消配置.

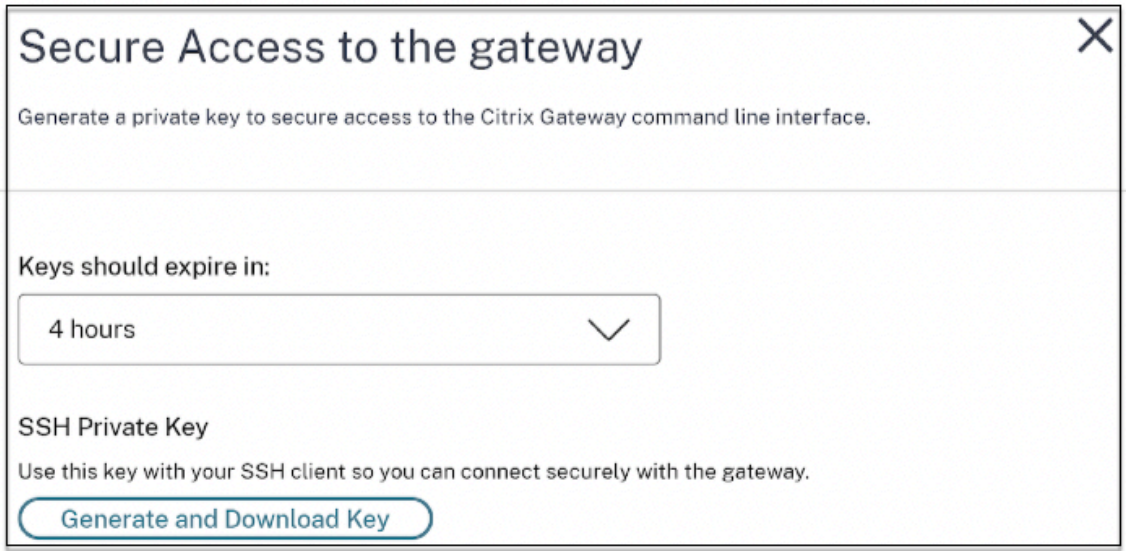
> 注意：
>
> 在取消配置之前，您必须断开连接 **Citrix** 网关 从 Workspace 配置。

1. 输入客户 ID 以取消配置自适应身份验证实例。



启用对网关的安全访问

1. 在 自适应身份验证 UI 中，在 预置自适应身份验证实例 部分中，单击省略号按钮。
2. 点击 安全管理访问.



3. 在 密钥应在，选择新 SSH 密钥的过期持续时间。
4. 点击 生成和下载密钥. 复制或下载 SSH 私钥供以后使用，因为在页面关闭后不会显示该密钥。此密钥可用于使用用户名 `authadmin` 认证.

   您可以单击 生成和下载密钥 以创建新的密钥对（如果较早的密钥对过期）。但是，只有一个密钥对可以处于活动状态。
5. 单击完成。

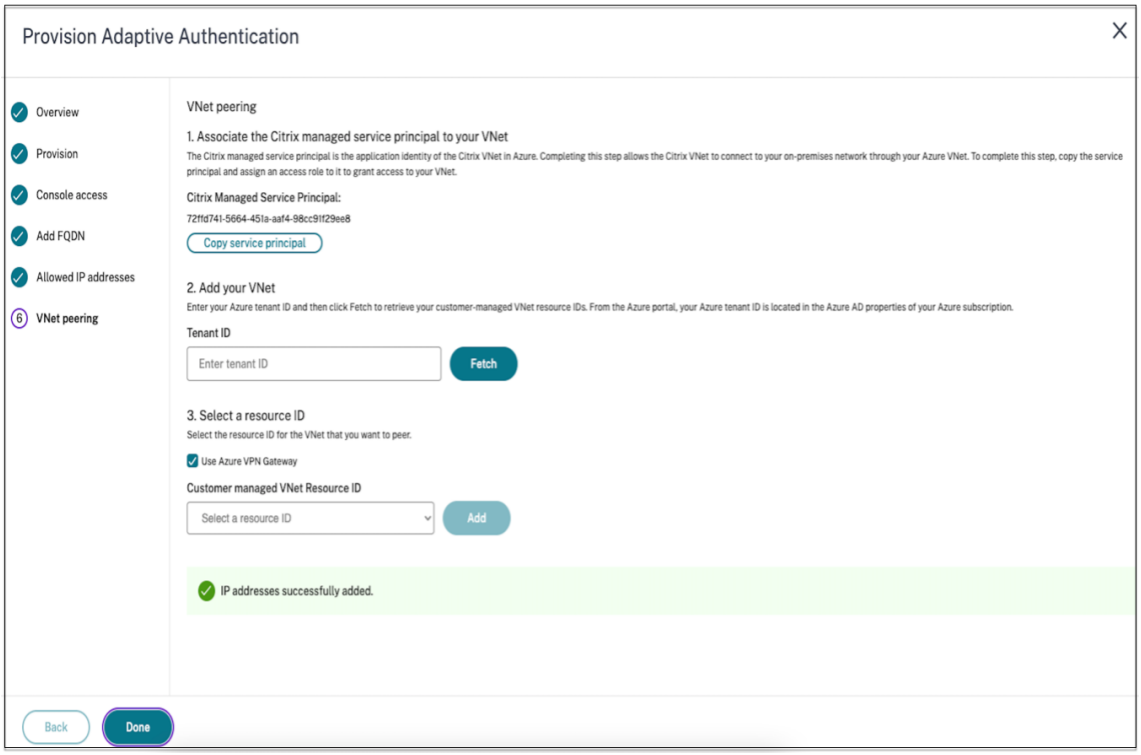
> 重要提示：
>
> - 如果您在 Windows 上使用 PuTTY 连接到自适应身份验证实例，则必须将下载的私钥转换为 PEM。有关详细信息，请访问 https://www.puttygen.com/convert-pem-to-ppk。
> - 建议使用以下命令从 MAC 或 Windows（版本 10）的 PowerShell/命令提示符通过终端连接到自适应身份验证实例。`ssh -i <path-to-private-key> authadmin@<ip address of ADC>`
> - 如果希望 AD 用户访问自适应身份验证 GUI，则必须将其作为新管理员添加到 LDAP 组。有关详细信息，请参阅https://support.citrix.com/article/CTX123782。对于所有其他配置，Citrix 建议您使用自适应身份验证 GUI，而不是 CLI 命令。

使用 **Azure VNet** 对等互连设置与本地身份验证服务器的连接

仅当已选择连接类型作为 Azure VNet 对等互连时，才必须设置此配置。

> 注意：
>
> 如果您使用的是 Okta、Azure AD、Ping 等第三方 IDP，则不需要执行此步骤。

1. 在 Connect 自适应身份验证 UI 上，单击 准备，然后单击 **Azure VNet** 对等互连.



这 **Citrix** 托管服务主体 字段包含 Citrix 为客户创建的 Azure 服务主体的应用程序 ID。需要此服务主体才能允许 Citrix 将 VNet 对等互连添加到您的订阅和租户中的 VNet。

若要允许此服务主体登录到客户租户，客户站点的管理员（租户的全局管理员）必须运行以下 PowerShell 命令，以将 SPN 添加到租户。也可以使用 CloudShell。`Connect-AzureAD New-AzureADServicePrincipal -AppId $App_ID` 哪里 `$App_ID` 是 Citrix 共享的 SPN 应用程序 ID。

> 注意：
>
> - 前面提到的命令输出必须用于角色分配的服务主体名称。
> - 要允许此服务主体添加 Azure VNet 对等互连，客户站点的管理员（不限于全局管理员）必须向必须链接到 Citrix 托管 VNet 的 VNet 添加“网络参与者”角色。
> - SPN 是用于关联 Azure 中的 Citrix 虚拟网络的唯一标识符。将 SPN 与 VNet 关联使 Citrix 虚拟网络能够通过 Azure 的 VNet 连接到客户的本地网络。

1. 创建 VNet 对等互连。

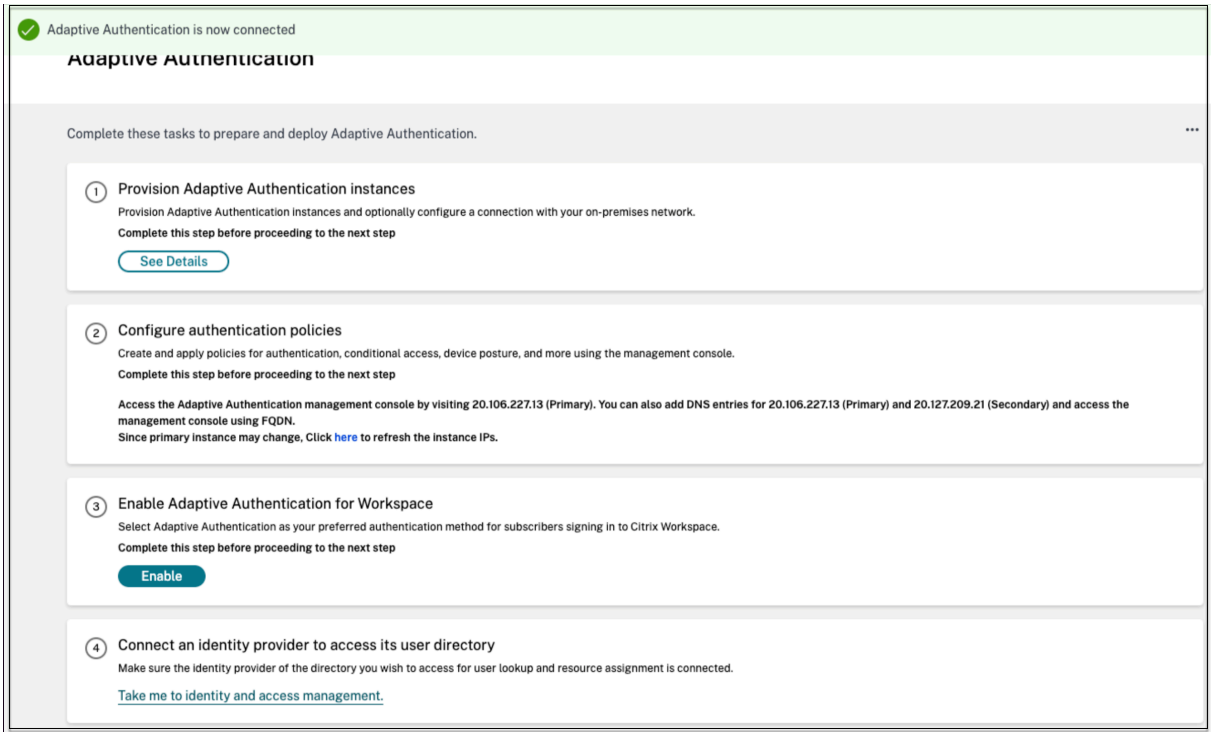
    - 输入运行前面步骤的租户 ID，然后单击 获取.

    这会使用为 SPN 添加网络参与者角色的候选 VNet 填充客户管理的 VNet 资源 ID。如果看不到 VNet，请确保正确运行前面的步骤或重复这些步骤。

> 注意：
>
> 有关如何查找租户 ID 的详细信息，请参阅 https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

1. 选择 使用 **Azure VPN** 网关 将本地网络连接到 Azure。
2. 在 客户管理的 **VNet** 资源 **ID**，选择为对等互连标识的 VNet，然后单击 加. VNet 将添加到表中，其状态最初为进行中. 对等互连成功完成后，Status （状态）将更改为 做.
3. 单击完成。
4. 继续配置，请参阅 步骤 1：配置自适应身份验证.

> 重要提示：
>
> - 要使流量在 Citrix 托管 VNet 和本地网络之间流动，可以在本地更改防火墙和路由规则，以将流量定向到 Citrix 托管 VNet。
> - 一次只能添加一个 VNet 对等体。目前不允许多个 VNet 对等互连。您可以根据需要删除 VNet 对等互连或创建一个 VNet 对等互连。



配置备份和恢复

Application Delivery Management 服务对自适应身份验证实例执行备份管理。有关详细信息，请参阅 备份和还原 NetScaler 实例.

1. 在“Application Delivery Management”图块上，单击“管理”。

2. 导航到 基础设施 > 实例 并访问备份。

> 注意：
>
> 如果您没有看到服务已载入，请载入 Application Delivery Management 服务。有关详细信息，请参阅 开始.

LDAP 和 LDAPS 负载均衡配置示例

Citrix 自适应身份验证实例使用负载平衡虚拟服务器提供 LDAP/LDAPS 支持。

> 注意：
>
> - 如果您没有对 LDAP/LDAPS 使用负载均衡，请避免为 LDAP 服务器创建服务或服务器，因为这可能会破坏自适应身份验证隧道。
> - 如果要对 LDAP 使用负载均衡，请创建一个服务组并将其绑定到负载均衡服务，而不是绑定到独立服务。
> - 使用负载平衡虚拟服务器进行身份验证时，请确保在 LDAP 操作中添加负载平衡虚拟服务器 IP 地址，而不是实际的 LDAP 服务器 IP 地址。
> - 默认情况下，TCP 监控器绑定到您创建的服务。在 Adaptive Authentication NetScaler 实例上，如果使用 TCP 监视器，则默认情况下，该服务将标记为 UP。
> - 对于监控，建议您使用自定义监控器。

必备条件

负载平衡虚拟服务器的私有 IP 地址（RFC1918 地址）。它可以是虚拟 IP 地址，因为此地址用于内部配置。

对 LDAP 服务器进行负载均衡

要对 LDAP 服务器进行负载均衡，请创建一个服务组并将其绑定到负载均衡虚拟服务器。不要创建用于负载平衡 LDAP 服务器的服务。

使用 **NetScaler CLI** 配置 **LDAP**：

您可以使用以下 CLI 命令作为配置 LDAP 的参考。

1. `add serviceGroup <serviceGroupName> <serviceType>`
2. `bind servicegroup <serviceGroupName> (<IP> | <serverName>)<port>`
3. `添加LB 虚拟服务器 <name> <serviceType> <ip> <port>` - 端口必须为 389。此端口用于内部通信，并且根据为服务组配置的端口，通过 SSL 连接到本地服务器。
4. `bind lb vserver <name> <serviceGroupName>`
5. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
6. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`

7. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

使用 **NetScaler GUI** 配置 **LDAP**：

1. 导航到 流量管理 **>** 负载均衡，然后单击 虚拟服务器.
2. 创建 TCP 类型和端口 389 的虚拟服务器。

   不要创建 SSL/SSL_TCP 类型的负载平衡虚拟服务器。
3. 导航到 流量管理 **>** 负载均衡，然后单击 服务组.
4. 创建 TCP 类型和端口 389 的服务组。
5. 将服务组绑定到您在步骤 1 中创建的虚拟服务器。

有关过程的详细信息，请参阅 设置基本负载均衡.

对 **LDAPS** 服务器进行负载均衡

对于负载平衡 LDAPS 服务器，您必须创建 TCP 类型的负载平衡虚拟服务器，以避免内部 SSL 加密或解密到自适应身份验证实例中。在这种情况下，负载平衡虚拟服务器处理 TLS 加密/解密。不要创建 SSL 类型的负载平衡虚拟服务器。

使用 **NetScaler CLI** 配置 **LDAPS**：

您可以使用以下 CLI 命令作为配置 LDAPS 的参考。

1. `添加LB 虚拟服务器 <name> <serviceType> <ip> <port>` - 端口必须为 636。
2. `bind lb vserver <name> <serviceGroupName>`
3. `add authentication ldapAction <name> { -serverIP } <ip_addr> | { -serverName <string> } } <lb vserver ip>`
4. `add authentication policy <ldap_policy_name> -rule <expression> -action <string>`
5. `bind authentication vserver auth_vs -policy <ldap_policy_name> -priority <ldap_policy_priority> -gotoPriorityExpression NEXT`

使用 **NetScaler GUI** 配置 **LDAPS**：

1. 导航到 流量管理 **>** 负载均衡，然后单击 虚拟服务器.
2. 创建 TCP 类型和端口 636 的虚拟服务器。

   不要创建 SSL/SSL_TCP 类型的负载平衡虚拟服务器。
3. 导航到 流量管理 **>** 负载均衡，然后单击 服务.
4. 创建 SSL_TCP 类型和端口 636 的服务。
5. 将服务绑定到您在步骤 1 中创建的虚拟服务器。

有关过程的详细信息，请参阅 设置基本负载均衡.

创建自定义监视器

使用 **NetScaler GUI** 创建自定义监视器：

1. 导航到 流量管理 **>** 负载平衡 **>** 监控器。
2. 创建 LDAP 类型的监视器。确保将监控器探测间隔设置为 15 秒，将响应超时设置为 10 秒。
3. 将此监控器绑定到您的服务。

有关更多详细信息，请参阅 自定义监视器.

配置以添加最多 **15** 个管理员 **IP** 地址

自适应身份验证服务允许您输入最多 15 个公有 IP 子网和单个 IP 地址来访问自适应身份验证管理控制台。

输入 IP 地址/子网时的注意事项：

- 确保公有 IP 子网的 CIDR 介于 /20 到 /32.B 之间。
- 确保条目之间没有重叠。

示例：

- 不接受 192.0.2.0/24 和 192.0.2.8，因为 192.0.2.8 位于 192.0.2.0/24 内。
- 不接受重叠子网：192.0.2.0/24 和 192.0.0.0/20，因为子网重叠。
- 输入网络子网值时，输入网络 IP 地址作为 IP 地址值。

  示例：

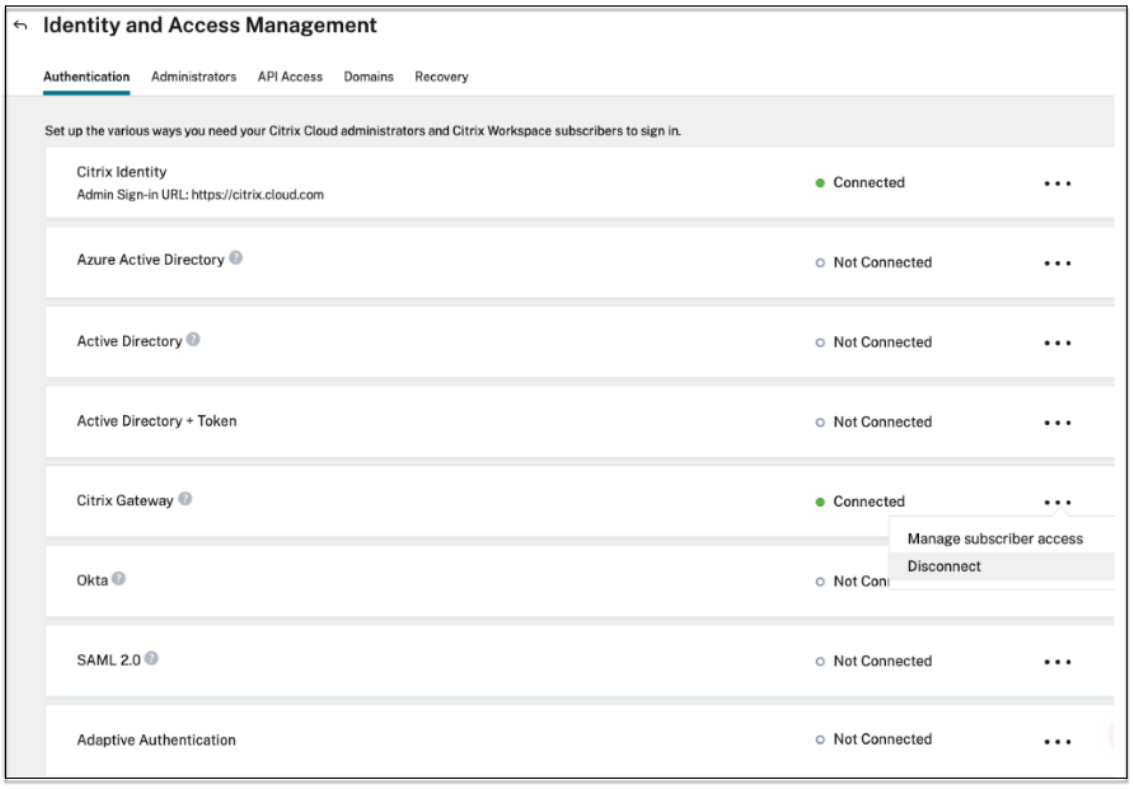
  - 192.0.2.2/24 不正确，请改用 191.0.2.0/24
  - 192.0.2.0/20 不正确，请改用 192.0.0.0/20

要启用此功能，请联系 Citrix 支持。

将身份验证方法迁移到自适应身份验证

已使用身份验证方法为 **Citrix** 网关 必须迁移 自适应身份验证，然后从 Adaptive Authentication 实例中删除 OAuth 配置。

1. 切换到 Citrix Gateway 以外的其他身份验证方法。
2. 在 **Citrix** 云 **>** 身份和访问管理中，单击与 Citrix Gateway 对应的省略号按钮，然后单击 断开.



3. 选择 我了解对订阅者体验的影响，然后单击 确认.

   单击 确认，则最终用户的工作区登录会受到影响，并且在再次启用自适应身份验证之前，自适应身份验证不会用于身份验证。

4. 在 Adaptive Authentication 实例管理控制台中，删除与 OAuth 相关的配置。

   通过使用 CLI：

   ```
   unbind authentication vs <authvsName> -policy <oauthIdpPolName>
   rm authentication oauthIdpPolicy <oauthIdpPolName>
   rm authentication oauthIdpProfile <oauthIdpProfName>
   ```

   通过使用 GUI：

   a) 导航到 **Security**（安全）**> AAA - Application Traffic**（**AAA -** 应用程序流量）**> Virtual Servers**（虚拟服务器）。
   b) 解绑 OAuth 策略。
   c) 导航到 安全 **> AAA -** 应用程序流量 **>** 政策 **>** 认证 **>** 高级策略 **> OAuth IDP**.
   d) 删除 OAuth 策略和配置文件。

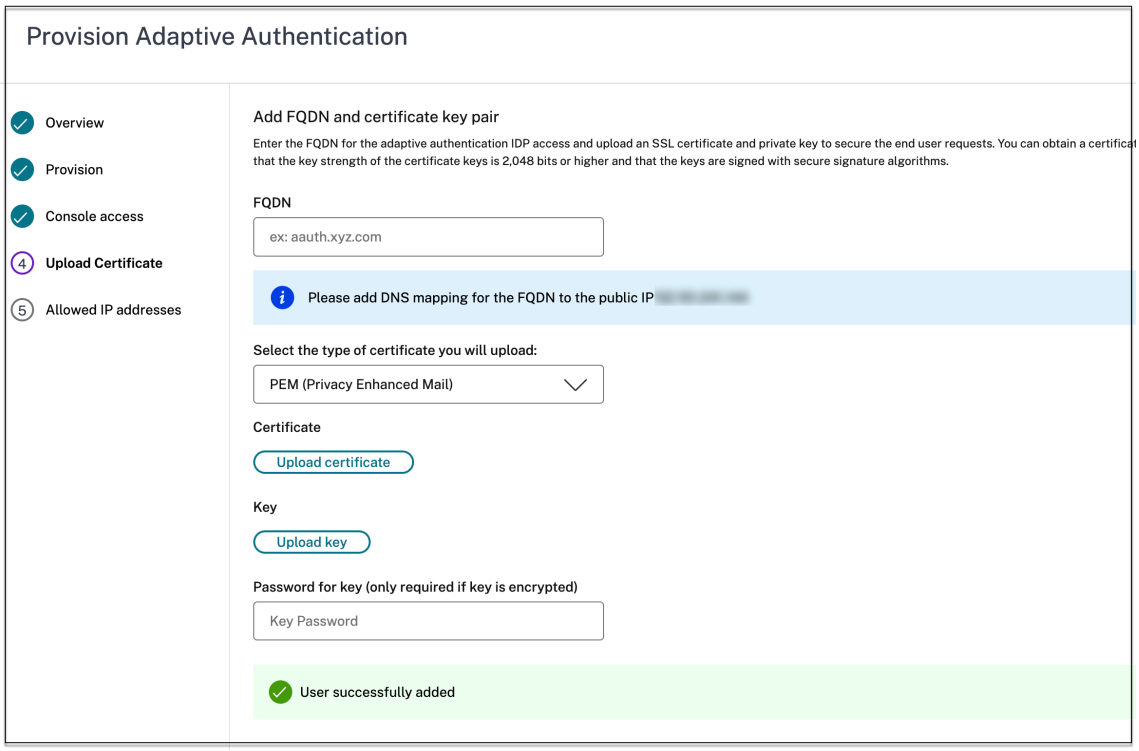
5. 导航到 **Citrix** 云 **>** 身份和访问管理. 在 Authentication 选项卡的 Adaptive Authentication 中，单击省略号菜单，然后选择 管理.

   OR 访问 https://adaptive-authentication.cloud.com

6. 点击 查看详情.

7. 在 上传证书 屏幕上，执行以下操作：

   - 添加自适应身份验证 FQDN。
   - 删除证书和密钥文件，然后重新上传。



> 重要提示：
>
> 如果直接编辑 FQDN 或证书密钥对，而不迁移到 自适应身份验证，则与 Identity and Access Management 的连接失败，并显示以下错误。您必须迁移到 Adaptive Authentication 方法才能修复这些错误。
>
> - ADC 命令失败并出现错误。策略已绑定到指定的优先级。
> - ADC 命令失败并出现错误。无法取消绑定未绑定的策略。

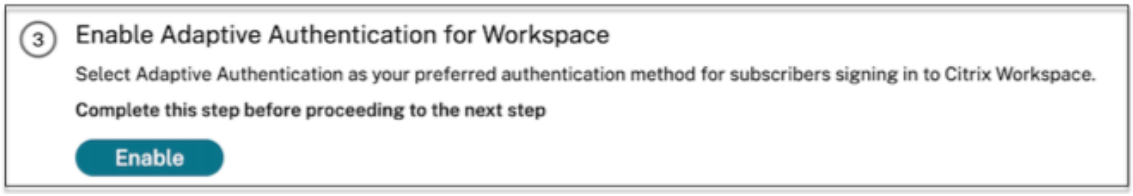
8. 点击 保存更改.

   此时，将显示 Identity and Access Management 自适应身份验证 如 连接 并且自适应身份验证实例已自动配置 OAuth 配置文件。

   您可以从 GUI 验证这一点。

   a) 访问您的自适应身份验证实例并使用您的凭证登录。
   b) 导航到 **Security**（安全）**> AAA - Application Traffic**（**AAA -** 应用程序流量）**> Virtual Servers**（虚拟服务器）。您必须看到 OAuth IdP 配置文件已创建。
   c) 导航到 **Citrix** 云 **>** 身份和访问管理. 自适应身份验证位于 连接 地位。

9. 单击 Adaptive Authentication 方法，再次启用 Adaptive Authentication 方法 使（步骤 3）。



此步骤在工作区配置中启用身份验证方法作为 Adaptive Authentication。

10. 单击后，单击步骤 3 上的工作区链接 使. 您必须看到身份验证方法已更改为 Adaptive Authentication。

> 注意：
>
> 新用户必须遵循相同的步骤，但删除 OAuth 相关配置的步骤除外。

身份验证配置示例

客户可以配置他们选择的身份验证策略并将其绑定到身份验证虚拟服务器。身份验证虚拟服务器不需要身份验证配置文件绑定。仅支持配置鉴权策略。以下是一些使用案例。

> 重要提示：
>
> 身份验证配置必须仅在主节点上完成。

使用条件身份验证的多重身份验证

- 使用双因素架构通过 LDAP 和 RADIUS 进行双因素身份验证（仅接受用户输入一次）
- 根据组织中用户的部门（员工、合作伙伴、供应商）的认证登录方法，使用下拉菜单选择部门
- 根据用户域的身份验证登录方法与下拉菜单
- 将电子邮件 ID（或用户名）输入配置为第一个因素，并在第一个因素中使用电子邮件 ID 进行基于组提取的条件访问，并为每个组提供不同的登录类型
- 对具有用户证书的用户使用证书身份验证，对非证书用户使用本机 OTP 注册进行多重身份验证
- 根据用户主机名输入提供不同的身份验证类型，具有条件身份验证
- 使用本机 OTP 身份验证进行双重身份验证
- Google Re-CAPTCHA

与多重身份验证的第三方集成

- 将 Azure AD 配置为 SAML IdP（将下一个因素配置为 LDAP 策略 - NO_AUTH 完成 OAuth 信任）
- 条件身份验证，首先将因素作为 SAML，然后根据 SAML 属性自定义登录到证书或 LDAP
- 第一个因素是 webauth 登录，然后是 LDAP

设备状态扫描（**EPA**）

- 设备状态检查，用于版本检查，然后为合规（RADIUS）和不合规用户（LDAP）自定义登录
- LDAP 身份验证，然后进行强制设备终端安全评估扫描
- AD 身份验证前后的设备状态检查 - EPA 前和后作为一个因素
- 作为 EPA 因素的设备证书

其他方案

- 添加带身份验证的 EULA
- 自定义 nFactor 策略标签、登录架构

实例的磁盘空间管理

June 19, 2024

自适应身份验证团队管理自适应身份验证实例的所有升级和维护。因此，建议您不要将自适应身份验证实例升级或降级为随机 RTM 版本。默认情况下，Citrix 管理自适应身份验证实例。

对于实例升级，VAR 目录中至少需要 7 GB 的空间。因此，自适应身份验证服务团队会在应用升级之前清除实例上的磁盘空间。建议您不要将任何敏感、专有或个人信息保存在以下目录中：

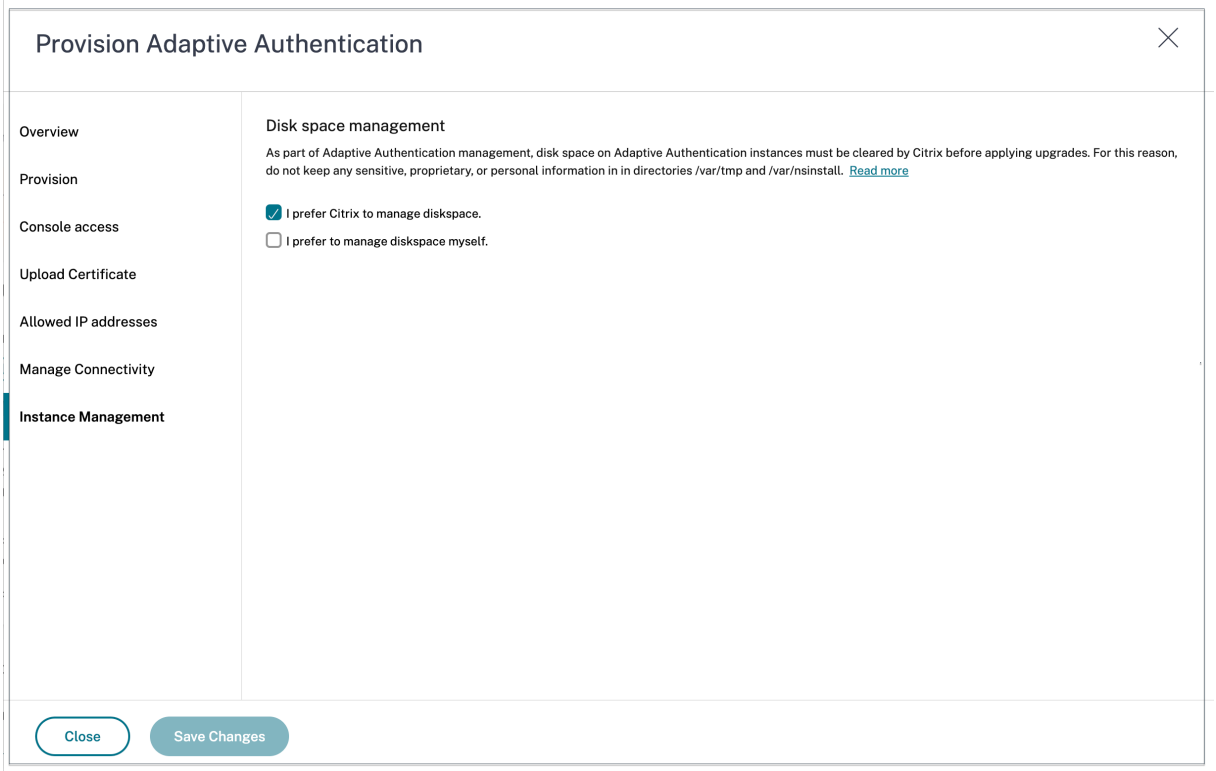
- /var/core
- /var/crash
- /var/tmp
- /var/nsinstall
- /var/nstrace
- /var/nslog

> 注意：
>
> - 升级期间首先清除 /var/nsinstall 目录，然后清除 /var/tmp 目录。如果仍未满足最低空间要求，则其他目录（/var/core、/var/crash、/var/nstracem 和 /var/nslog）也将被清除。
> - 客户负责管理和维护 NetScaler 磁盘空间和磁盘清理。

可以选择自己管理磁盘空间

尽管 Citrix 管理自适应身份验证实例，但默认情况下，您最好自己清理实例上的磁盘空间。您可以通过执行以下操作选择退出默认方法：

1. 在自适应身份验证导航窗格中，单击实例管理。
2. 选择“我更喜欢自己管理磁盘空间”，然后在确认消息对话框中单击确认。
3. 单击保存更改。



> 注意：
>
> 您也可以根据客户流量安排升级。然后，Citrix Cloud 团队会相应地升级您的实例。
>
> 有关安排升级的信息，请参阅安排自适应身份验证实例的升级。

解决自适应身份验证问题

June 19, 2024

根据配置中的不同阶段对问题进行分类：

- Provisioning
- 实例可访问性问题
- AD/Radius 连接和身份验证问题
- 身份验证问题
- EPA/设备姿势相关问题
- 与智能标签相关的问题

- 日志收集

您也可以使用自适应身份验证 CLI 对问题进行故障排除。要连接到 CLI，请执行以下操作：

- 在您的机器上下载 SSH 客户端，比如 putty/securecrt。
- 使用管理 IP（主）地址访问自适应身份验证实例。
- 使用您的凭据登录。

有关详细信息，请参阅 访问 NetScaler 设备。

启用自适应身份验证日志的记录

确保启用日志级别以捕获自适应身份验证日志。

使用 **CLI** 启用日志：

1. 登录到自适应身份验证实例 CLI。
2. 使用 PuTTY 输入管理证书。
3. 运行以下命令 `set audit syslogParams logLevel ALL`

使用 **GUI** 启用日志：

1. 使用浏览器登录自适应身份验证实例。
2. 导航到 配置 **>** 系统 **>** 审计。
3. 在“审核”页的“设置”下，单击“更改审核 **syslog** 设置”。
4. 在 日志级别中，选择 全部。

预配问题

- 无法访问自适应身份验证 **UI**

  检查您的客户 ID/租户是否启用了授权。

- 在配置页面停留超过 **45** 分钟

  收集错误的屏幕截图（如果有），然后联系 Citrix 支持部门寻求帮助。

- **VNet** 对等项已关闭

  - 检查 Azure 门户中是否存在与此对等对等对应的警报，并采取建议的操作。
  - 删除对等，然后从自适应身份验证 UI 中再次添加。

- 取消预配未完成

  联系 Citrix 支持部门以获得帮助。

实例可访问性问题

- 无法访问该实例的管理 **IP** 地址
  - 检查客户端用于访问的公有 IP 地址是否属于允许的源 IP 地址。
  - 验证是否有任何代理更改客户端源 IP 地址。
- 无法登录到实例

  确保管理员访问权限使用您在预配期间输入的凭据正常工作。
- 最终用户没有完全权限

  在添加用户时，请确保您已绑定了适当的访问命令策略。有关更多信息，请参阅 用户、用户组和命令策略。

AD 或 RADIUS 连接问题

Azure Vnet 对等连接类型存在问题：

- 检查是否可以从自适应身份验证实例访问客户管理的 Azure VNet。
- 检查从客户管理的 Azure VNet 到 AD 的连接/可访问性是否正常。
- 确保添加适当的路由，以便将流量从本地引导到 Azure VNet。

基于 **Windows** 的连接器：

- 所有日志都在 /var/log/ns.log 目录中可用，每个日志都带有 [NS_AAUTH_TUNNEL] 前缀。
- 日志中的 ConnectionID 可用于关联不同的事务。
- 确保将连接器虚拟机的专用 IP 地址添加为 RADIUS 服务器中的一个 RADIUS 客户端，因为该 IP 地址是连接器的源 IP 地址。

  对于每个身份验证请求，将在自适应身份验证实例（NS-AAAD 进程）和身份验证服务器之间建立通道。成功建立通道后，将进行身份验证。

  确保连接器虚拟机可以解析自适应身份验证 FQDN。
- 连接器已安装，但本地连接失败。

  验证是否正在建立 NSAUTH-TUNNEL。

  ```
  cat ns.log | grep -I “tunnel”
  ```

  如果身份验证请求的 ns.log 文件中没有打印以下示例日志，则可能在建立通道时出现问题，或者连接器端出现问题。

  ```
  1  LDAP:
  2  [NS_AAUTH_TUNNEL] Entering bitpump for
  ```



```
Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636 ,
    Connection2 => Src : 10.106.103.70:2271, Dst :
   10.106.103.80:443"
RADIUS:
[NS_AAUTH_UDP_TUNNEL] MUX channel established"
```

检查日志详细信息并采取相应的措施。

日志详情	更正措施
日志文件中 [NS_AAUTH_TUNNEL] 不包含带前缀的日志	运行 `show cloudtunnel vserver` 命令。此命令必须列出状态为“UP”的两个（TCP 和 UDP）云通道虚拟服务器。“
`[NS_AAUTH_TUNNEL] Waiting for outbound from connector` 对于此日志，如果未收到以下响应：`[NS-AAUTH-TUNNEL] Received connect command from connector and client connection lookupsucceeded"`	检查连接器计算机是否能够访问自适应身份验证 FQDN，或者检查连接器端防火墙是否有与自适应身份验证 FQDN 的出站连接
`[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0`和`[NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out"`	请联系 Citrix 支持人员。

连接器无响应：

- 确保可从连接器虚拟机访问自适应身份验证 FQDN。
- 确保已绑定中间证书并将其链接到自适应身份验证实例上的服务器证书。

LDAP/RADIUS 设置不正确：

如果您的 AD/RADIUS 服务器 IP 地址是公有 IP 地址，则必须在 NetScaler 中为表达式添加子网或 IP 地址。不要编辑现有范围。

- 要使用 CLI 添加子网或 IP 地址，请执行以下操作：

```
set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST
    .BETWEEN(10.0.0.0,10.255.255.255) || CLIENT.IP.DST.BETWEEN
    (172.16.0.0,172.31.255.255) || CLIENT.IP.DST.BETWEEN
    (192.168.0.0, 192.168.255.255) || CLIENT.IP.DST.BETWEEN
    (13.14.0.0, 13.14.255.255)||CLIENT.IP.DST.EQ(1.2.5.4))"
```

- 要使用 GUI 添加子网或 IP 地址，请执行以下操作：

1. 导航到 **Appexpert >** 表达式。
2. 添加表达式 **aauth_allow_rfc1918_subnets**。

如果通道已建立，但身份验证仍然失败，请使用以下步骤对问题进行故障排除。

LDAP:

- 验证绑定 DN 详细信息。
- 使用测试连通性确认错误。
- 使用 `aaad` 调试验证错误。
- 使用 CLI 登录到自适应身份验证实例。

```
shell
cd /tmp
cat aaad.debug
```

常见的 **LDAP** 错误：

- 服务器超时—连接器对 LDAP 查询没有响应。
- 其他 LDAP 错误，请参阅 https://support.citrix.com/article/CTX138663。

Radius:

- 连接器 IP 地址必须添加为 RADIUS 服务器配置中的 RADIUS 客户端源 IP 地址。

身份验证问题

- **OAuth** 的发布断言错误
  - 确保所有索赔均由 AD 提供。您需要 7 个索赔才能成功。
  - 验证 /var/log/ns.log 中的日志以找到 OAuth 失败的错误。

```
cat /var/log/ns.log
```

  - 验证 OAuth 配置文件参数。
- 断言后 **Azure AD** 身份验证停滞不前

  将 AD 身份验证作为身份验证设置为 off 的下一个因素。这是为了获得成功身份验证所需的所有声明。

与 **EPA** 相关的问题

- 插件已经存在，但用户收到下载插件的提示。

  可能的原因：版本不匹配或文件损坏

  - 运行开发人员工具并验证插件列表文件是否包含与 NetScaler 和客户端计算机相同的版本。
  - 确保 NetScaler 上的客户端版本与客户端计算机上的客户端版本相同。

    在 NetScaler 上更新客户端。

    在自适应身份验证实例上，导航到 **Citrix Gateway >** 全局设置 **>** 更新客户端库。

    Citrix 下载上的 EPA 插件库页面为您提供了详细信息。
  - 有时，即使版本已更新，也可以在 NetScaler 上缓存请求。

    `show cache object` 显示缓存的插件详细信息。您可以使用命令将其删除；

    `flush cache object -locator 0x00000023345600000007`

  有关 EPA 日志收集的详细信息，请参阅 https://support.citrix.com/article/CTX209148。

- 用户选择选项后，有没有办法恢复 **EPA** 设置（始终、是、否）。

  目前，EPA 设置还原是手动完成的。

  - 在客户端计算机上，导航到 C:\Users<user_name>\ AppData\ Local\ Citrix\ AGEE。
  - 打开 `config.js` 文件并将 trustAlways 设置为空 - `"trustAlways":null`

智能访问标签问题

- 配置智能访问后，应用程序不可用

  确保在自适应身份验证实例和 Citrix VDA 交付组上定义了标记。

  检查是否在所有大写字母的 Workspace 交付组中添加了标记。

  如果这样做不起作用，您可以收集 ns.log 并联系 Citrix 支持部门。

自适应身份验证实例的常规日志收集

- 技术支持包：有关详细信息，请参阅 如何从 SDX 和 VPX 设备收集技术支持包以进行洞察分析。
- 跟踪文件。有关详细信息，请参阅 如何在 NetScaler 上记录数据包跟踪。

请联系 Citrix 支持部门以获取指导。

使用自适应身份验证的智能访问

June 19, 2024

Citrix Cloud 客户可以使用自适应身份验证作为 Citrix Workspace 的 IdP，提供对 Citrix DaaS 资源（虚拟应用程序和桌面）或 Secure Private Access 服务的智能访问（自适应访问）。

智能访问功能允许自适应身份验证服务将有关用户的所有策略信息显示到 Citrix Workspace 或 Citrix DaaS。自适应身份验证服务可以提供 Device Posture (EPA)、网络位置（公司网络内部或外部、地理位置）、用户组等用户属性、一天中的时间或这些参数的组合作为策略信息的一部分。然后，Citrix DaaS 管理员可以使用此策略信息配置对虚拟应用程序和桌面的上下文访问。虚拟应用程序和桌面可以根据先前的参数（访问策略）进行枚举，也可以不枚举。也可以控制某些用户操作，例如剪贴板访问、打印机重定向、客户端驱动器或 USB 映射。

示例用例：

- 管理员可以将应用程序组配置为只能从特定的网络位置（例如公司网络）显示或访问。
- 管理员可以将应用程序组配置为只能从公司管理的设备上显示或访问。例如，EPA 扫描可以检查设备是企业托管设备还是自带设备。根据 EPA 扫描结果，可以为用户枚举相关的应用程序。

必备条件

- 必须为 Citrix Workspace 配置作为 IdP 的自适应身份验证。有关详细信息，请参阅 自适应身份验证服务。
- 使用 Citrix DaaS 的自适应身份验证服务已启动并且正在运行。
- 自适应访问功能已启用。有关详细信息，请参阅启用自适应访问。

了解智能访问的事件流程

1. 用户登录 Citrix Workspace。
2. 用户被重定向到配置为 IdP 的自适应身份验证服务。
3. 提示用户进行预身份验证 (EPA) 或身份验证。
4. 用户已成功通过身份验证。
5. 智能访问策略是根据配置进行评估的，标签与用户会话相关联。
6. 自适应身份验证服务将标签推送到 Citrix Graph 服务。用户被重定向到 Citrix Workspace 登录页面。
7. Citrix Workspace 会获取此用户会话的策略信息，匹配筛选器，并评估必须枚举的应用程序或桌面。
8. 管理员在 Citrix DaaS 上配置访问策略以限制用户的 ICA 访问权限。

在自适应身份验证实例上配置智能访问策略

在自适应身份验证实例上配置智能访问策略分为两个步骤：

1. 在自适应身份验证实例上使用智能访问标签定义智能访问策略。例如，请参见 步骤 *1*。
2. 在您的 DaaS/Secure Private Access 上定义相同的标签以访问资源。例如，请参见 步骤 *2*。

用例 **1**：配置智能访问策略，允许从 **Chrome** 浏览器登录的用户进行访问并阻止他们访问剪贴板

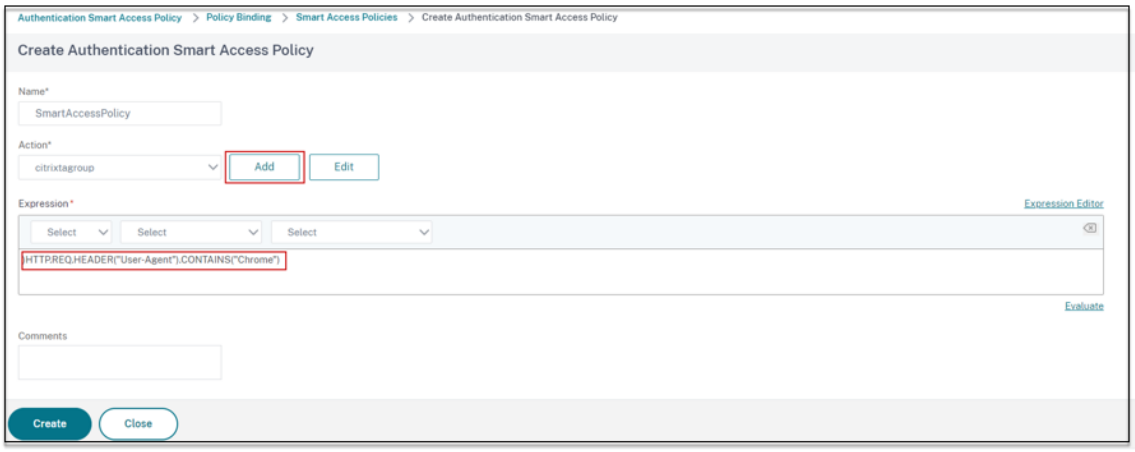
步骤 **1**：在自适应身份验证实例上使用智能标记配置智能访问策略

1. 登录自适应身份验证实例。
2. 导航到自适应身份验证虚拟服务器（安全 **>** **AAA -** 应用程序流量 **>** 虚拟服务器）。
3. 选择身份验证虚拟服务器，然后单击“编辑”。
4. 单击智能访问策略。
5. 根据您的要求定义策略的表达方式。

    a) 单击 **Add Binding**（添加绑定）。
    b) 在“选择策略”中，单击“添加”。
    c) 输入智能访问策略的名称。
    d) 定义表达式。

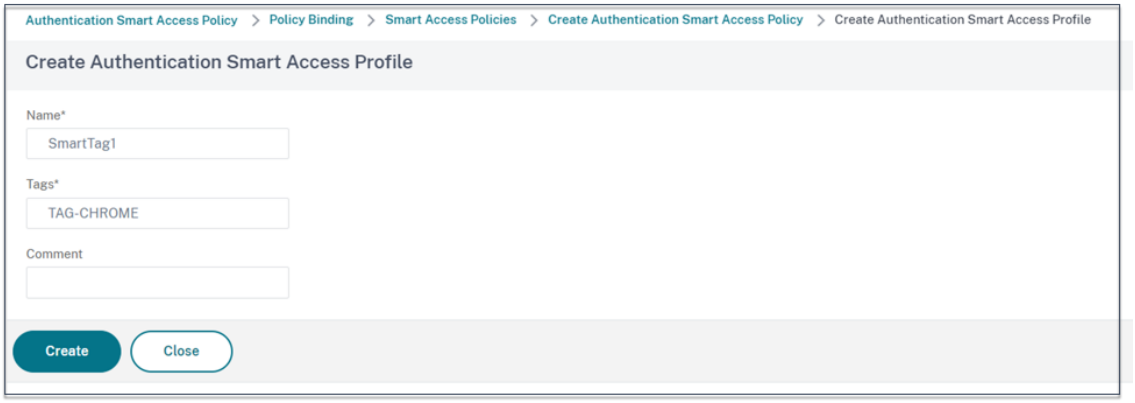
    对于允许用户从 Chrome 浏览器登录的访问权限的示例，请输入表达式 `HTTP.REQ.HEADER("User-Agent").CONTAINS("Chrome")`

    同样，您可以根据时间、用户登录、身份验证和授权组以及其他选项创建表达式。

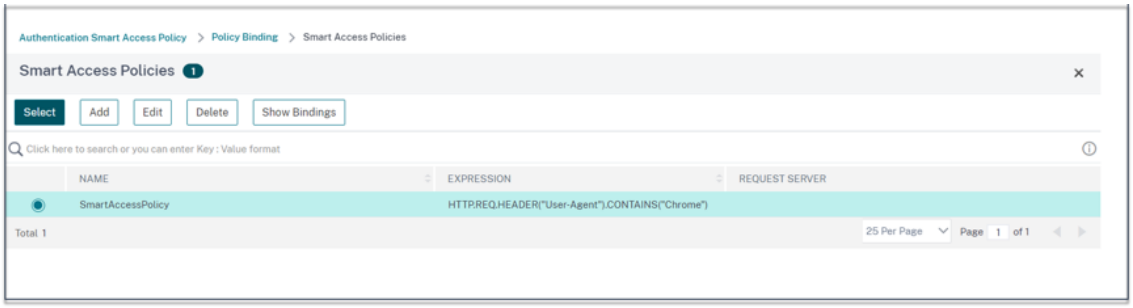


6. 现在，创建智能标签并将这些标签绑定到智能访问策略。

    a) 在“操作”中，单击“添加”。
    b) 在 名称中，键入智能访问配置文件的名称。
    c) 在 标签中，定义智能访问标签。例如，TAG-CHROME。



a) 单击创建。
b) 选择智能访问策略，然后单击“添加绑定”。
c) 将此智能访问标签绑定到之前创建的智能访问策略。



> 注意：
>
> 您也可以从“安全”**>**“**AAA-**应用程序流量”**>**“策略”**>**“身份验证”**>**“高级策略”**>**“智能访问”**>**“策略”中创建智能访问策略，然后将其绑定到身份验证虚拟服务器。

步骤 **2**：在 **DaaS Studio** 中定义智能访问标签

1. 添加带有“TAG-CHROME”智能标签的策略。有关详细信息，请参阅在 Citrix Studio 中定义标记。

用例 **2**：根据 **EPA** 结果配置智能访问策略，用于身份验证后

步骤 **1**：在自适应身份验证实例上使用智能标记配置智能访问策略　要根据端点分析等条件进行智能访问，请配置 nFactor 流程，定义 EPA 操作，然后添加默认组。

要将 EPA 配置为 nFactor 流中的因素，请参阅将 EPA 配置为因素。

逻辑流程

1. 用户访问 Workspace URL。

2. 用户被重定向到自适应身份验证以进行身份验证/EPA。
3. 终点分析在最终用户上完成，结果通过将用户添加到定义的默认组来存储。
4. 系统会提示用户进入下一个身份验证流程。
5. 对智能访问策略进行评估，并为用户分配智能访问标签。

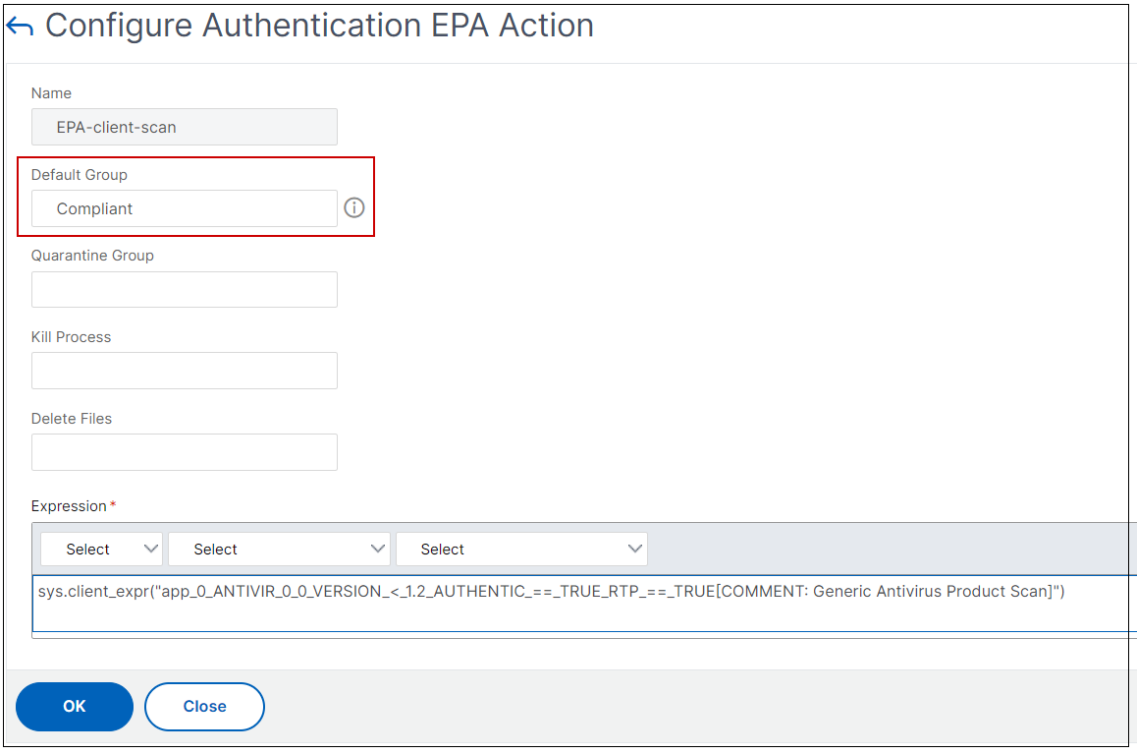
配置

从安装了防病毒软件的计算机上访问的用户必须标记为合规，并提供完全访问权限。但是，没有防病毒软件的用户计算机必须标记为不合规，并提供有限的访问权限。

1. 为 EPA 创建 nFactor 策略。有关详细信息，请参阅 将 EPA 配置为因素。

   在 nFactor 流程中，确保第一个是用户身份验证因素。

2. 选择 EPA 表达式以检查防病毒软件是否存在。
3. 在 EPA 操作中定义默认组。



   如果 EPA 成功运行，则会将用户添加到此默认组。

4. 现在，创建智能访问策略

   a) 登录自适应身份验证实例。

   b) 导航到自适应身份验证虚拟服务器（安全 **> AAA -** 应用程序流量 **>** 虚拟服务器）。

   c) 选择自适应身份验证虚拟服务器，然后单击“编辑”。

d) 单击智能访问策略。

e) 使用以下表达式创建两个智能访问策略。

- AAA.USER.IS_MEMBER_OF（“Compliant”）- 适用于用户 EPA 通行证条件
- !AAA.USER.IS_MEMBER_OF（“Compliant”）- 适用于用户 EPA 失败情况

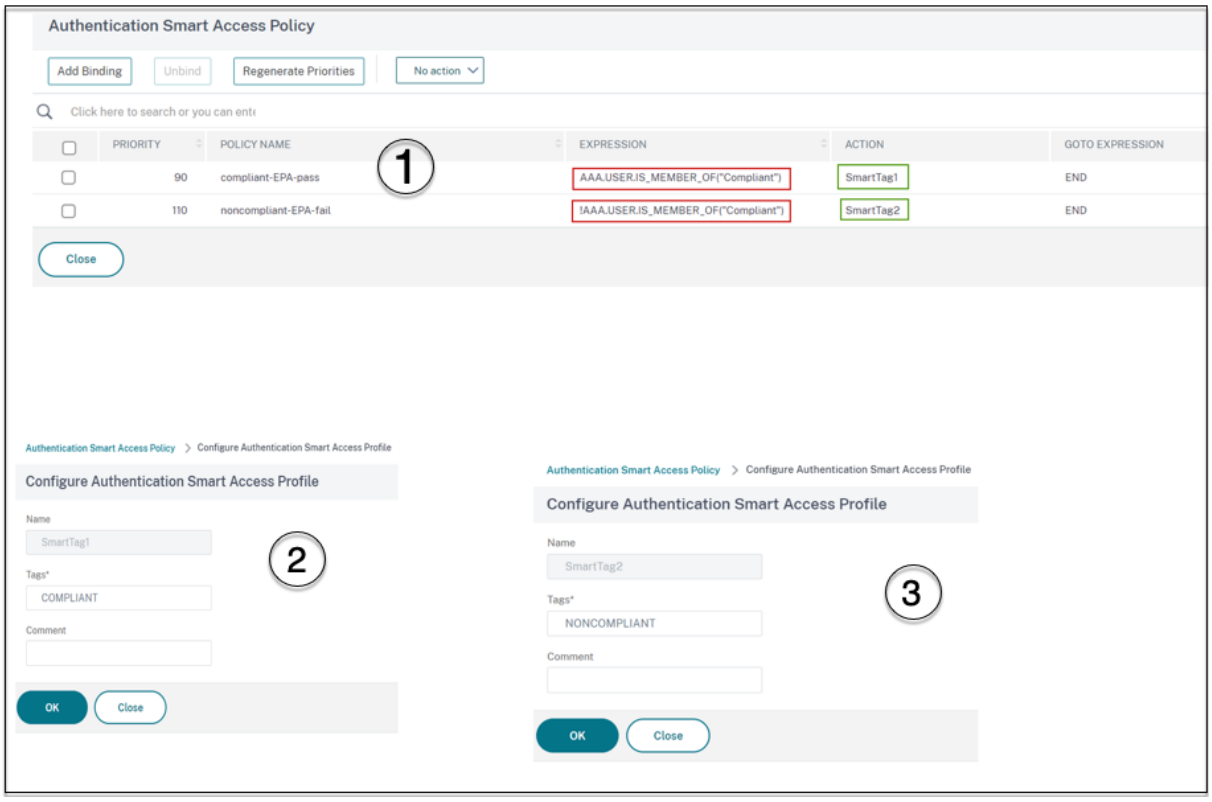
f) 为这两个策略定义智能访问标签。

示例：

- 带 AAA.USER.IS_MEMBER_OF （“Compliant”）的标记 COMPLIANT 的标记名称 SmartTag1
- 带 !AAA.USER.IS_MEMBER_OF （“Compliant”）的标记 NONCOMPLIANT 的标记名称 SmartTag2

智能访问条件为 EPA 的自适应身份验证实例配置现已完成。

您可以根据要求配置标签和表达式。



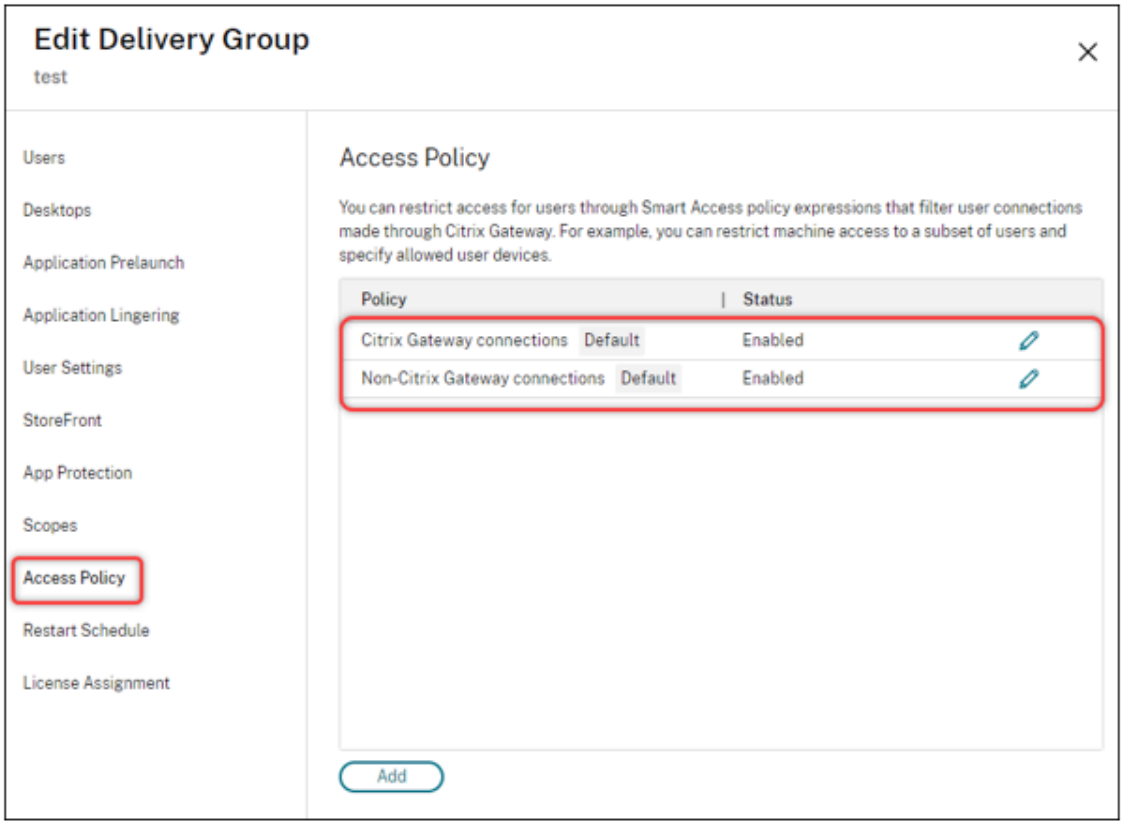
步骤 **2**：在 **DaaS Studio** 中配置智能访问标签　在相应的交付组中添加带有 “COMPLIANT” 和 “NONCOMPLIANT” 智能标签的策略。有关详细信息，请参阅在 Citrix Studio 中定义标记。

在 **DaaS** 工作室中定义标签

在交付组中定义标签以限制用户的应用程序枚举。

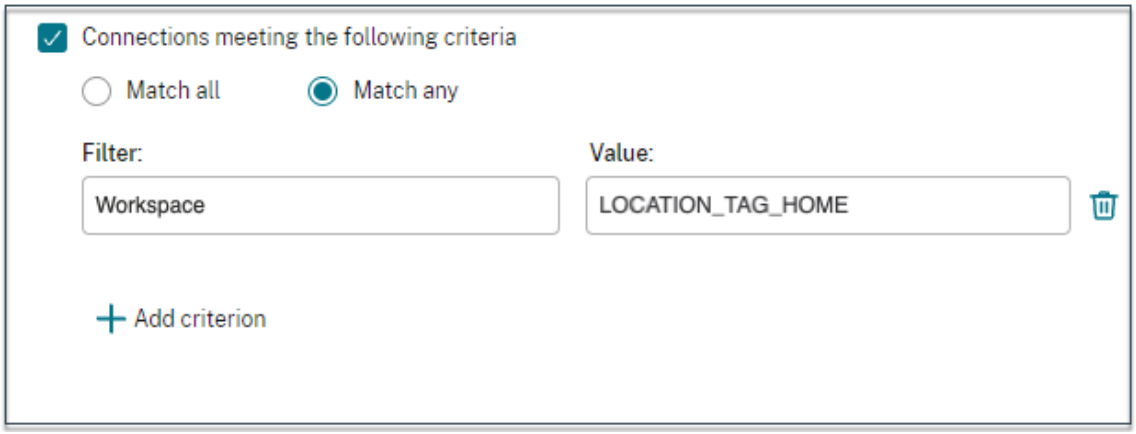
示例：BranchOffice 用户必须看到包含所有应用程序的 自适应访问交付组 中的应用程序。
而 WorkfromHome 用户必须看到来自 **WFH** 交付组的应用程序。

1. 登录 Citrix Cloud。
2. 选择“我的服务”**>** “**DaaS**”。
3. 单击管理。
4. 根据您的要求创建交付组。有关详细信息，请参阅创建交付组。
5. 选择已创建的交付组，然后单击编辑交付组。



6. 单击访问策略。
7. 对于在 Citrix Workspace 平台内使用自适应访问的客户，请执行以下步骤，将交付组的访问权限限制为仅限内部网络：

   a) 右键单击交付组并选择编辑。
   b) 在左侧窗格中选择访问策略。
   c) 单击“编辑”图标修改默认 Citrix Gateway 连接策略。
   d) 在“编辑策略”页面上，选择符合以下条件的连接，选择“匹配任意”，然后添加条件。



对于 WorkFromHome 用户，请在相应的 Delivery Controller 中输入以下值。

场：Workspace

过滤器：LOCATION_TAG_HOME

对于 BranchOffice 用户，在相应的 Delivery Controller 中输入以下值。

过滤器：Workspace

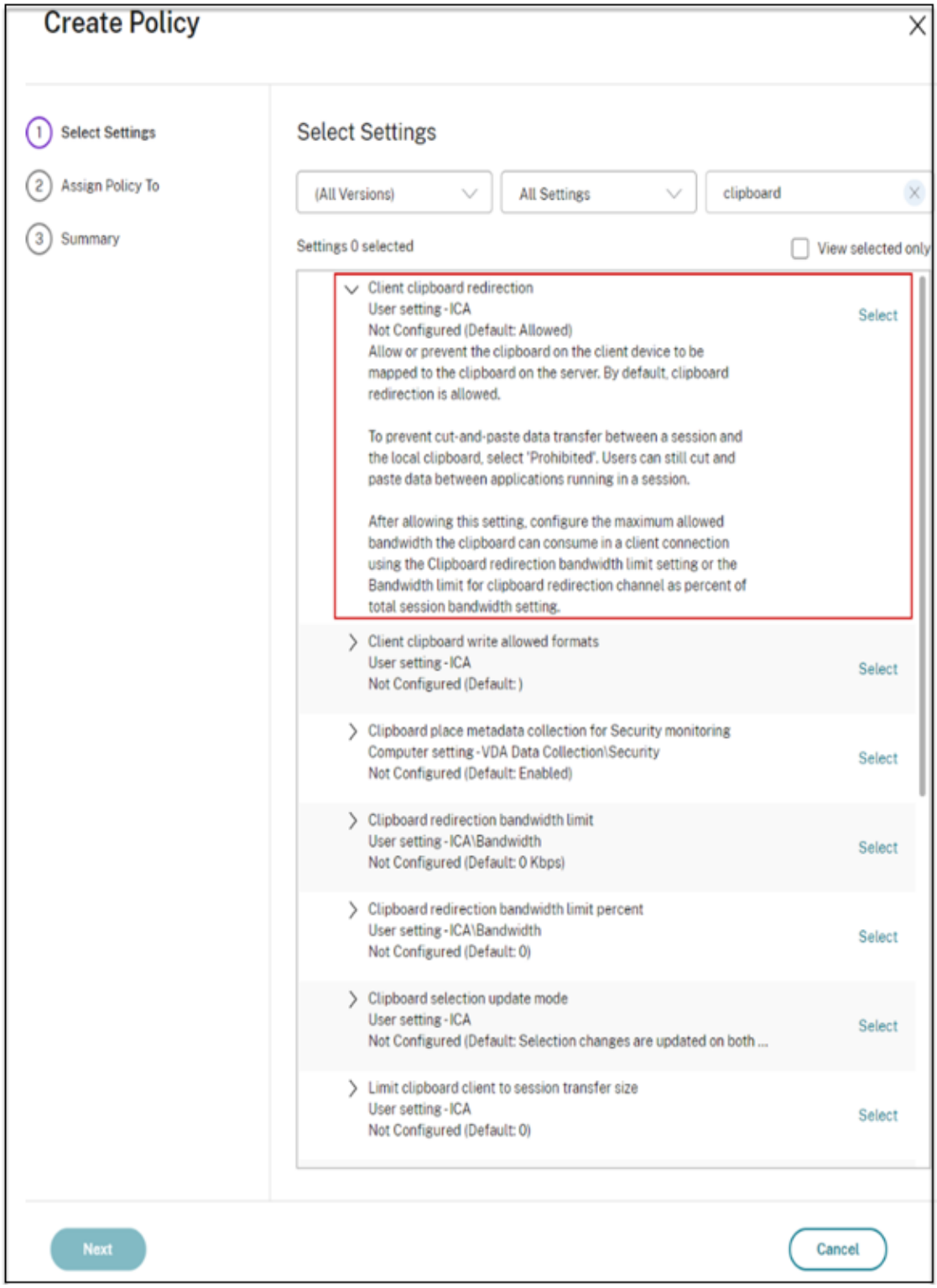
值：LOCATION_TAG_BRANCHOFFICE

现在，您可以使用这些标签来限制对应用程序的访问。

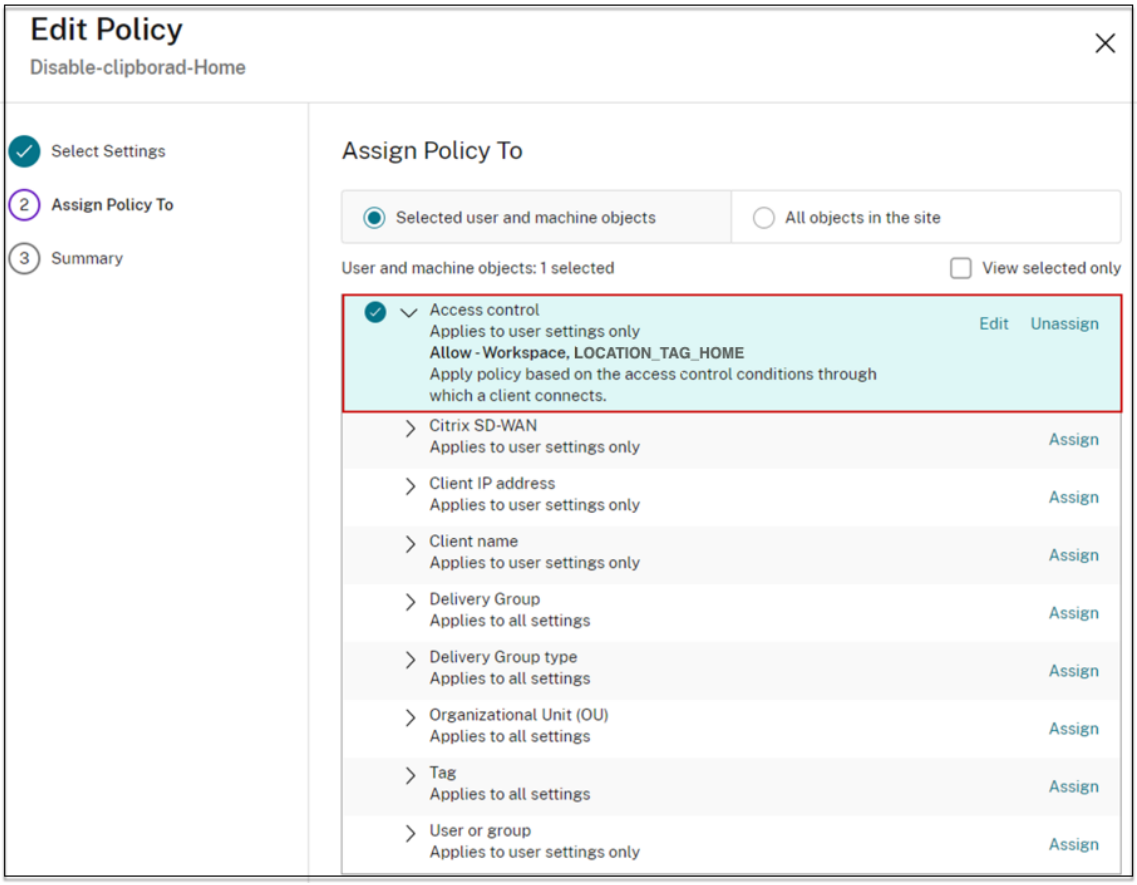
限制所提供应用程序的访问类型

示例：在家办公的用户不得拥有剪贴板权限。

1. 在 DaaS Studio 中，导航到 策略，然后点击 创建策略。
2. 在“创建策略”页面中，选择要允许或禁止访问的设置。
3. 单击“选择”。

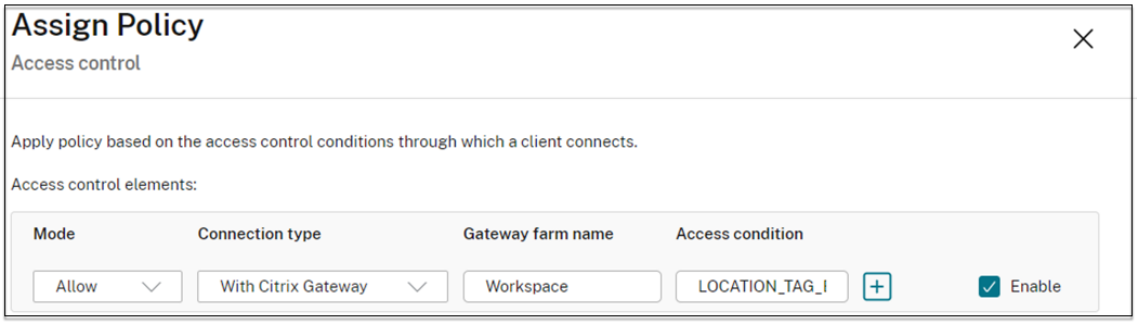


4. 在“编辑设置”页面中，单击“允许”或“禁止”，然后单击“保存”。
5. 单击下一步。
6. 在“将策略分配给”页面中，选择“访问控制”，然后单击“下一步”。

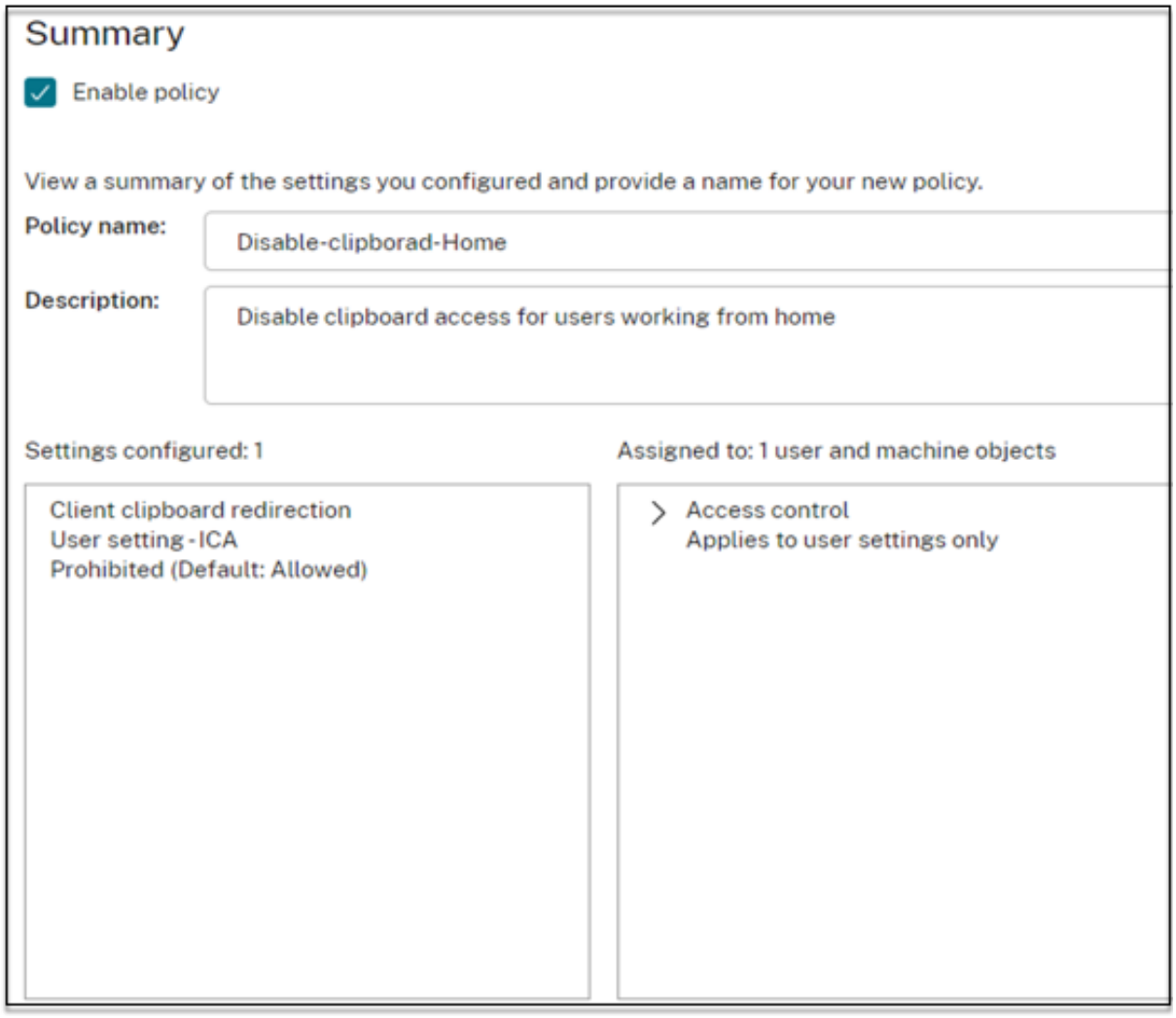


7. 使用以下详细信息定义策略：

   - 模式：-允许
   - 连接类型：-使用 Citrix Gateway
   - 场名称：- Workspace
   - 访问条件：LOCATION_TAG_HOME（全部为大写）



8. 单击“下一步”，然后输入策略的名称。
9. 单击完成。



现在，您已经准备好测试您的访问权限了。

对常见错误进行故障排除

- 问题：您会看到“无法完成您的请求”消息。

  解决方案

  1. 确保启用自适应访问。有关详细信息，请参阅启用自适应访问。
  2. 如果未启用该功能，请联系 Citrix 支持部门。

- 问题：未发布任何应用程序或桌面。

  如果智能标签未从自适应身份验证推送到工作区，或者未在 DaaS 或 Secure Private Access 处接收，则可能会出现此问题。

  解决方案：

- 检查智能访问策略是否受到影响。有关详细信息，请参阅https://support.citrix.com/article/CTX138840。
- 检查 Citrix 自适应身份验证实例是否能够连接到 `cas.citrix.com`。
- 有关智能标签的详细信息，请查看自适应身份验证实例。
  - 确保在 `set audit syslogParams` 命令中，所有实例上的 logLevel 参数都设置为 `ALL`。
  - 使用 putty 登录到自适应身份验证主实例。

    键入 shell

    ```
    cd /var/log

    cat ns.log | more or cat ns.log | grep -I “smartaccess”
    ```
- 如果这些都不能解决问题，请联系 Citrix 支持部门。

高可用性设置的配置更改

有时，在以下目录的高可用性设置中，可能会出现文件同步延迟。因此，在 Citrix ADM 注册期间创建的密钥无法按时读取。

- /var/mastools/conf/agent.conf
- /var/mastools/trust/.ssh/private.pem
- /var/mastools/trust/.ssh/public.pem

要解决文件同步问题，请执行以下步骤在辅助服务器上重新运行 `set cloud` 命令。

```
1  > shell cat /var/mastools/conf/agent.conf
2  <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3  <mps_agent>
4  <uuid>temp_str</uuid>
5  <url>fuji.agent.adm.cloud.com</url>
6  <customerid>customer_id</customerid>
7  <instanceid>instance_id</instanceid>
8  <servicename>MAS</servicename>
9  <download_service_url>download.citrixnetworkapistaging.net</
       download_service_url>
10 <abdp_url>fuji.agent.adm.cloud.com</abdp_url>
11 <msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
12 </mps_agent> Done
13 > set cloud param -CustomerID customer_id -InstanceID instance_id -
       Deployment Production
```


大小调整和性能指南

June 19, 2024

自适应身份验证让客户使用部署在其数据中心中的 Cloud Connector 或 Azure vNet 对等互连来访问其本地身份验证服务器（前提是已经从客户管理的 VNet 建立了数据中心可访问性）。本主题包含有关 Citrix Cloud Connector 和 Azure vNet 对等部署的性能数据以及 Citrix Cloud Connector 计算机的推荐规模和大小配置的信息。

用户身份验证率

大小为 2 个 vCPU 和 7 GB RAM 的连接器虚拟机每秒可以对 14 个用户进行身份验证。

默认情况下，连接器服务配置为在出现故障或崩溃时自动重新启动两次。在随后的故障或崩溃中，服务停止。此外，当前，如果身份验证速率提高到每秒 4 次身份验证以上，则连接器服务将失败。该速率可以通过将连接器服务配置为在出现任意数量的故障后重启来实现（**Citrix Netscaler Cloud Gateway >** 恢复 **>** 重启服务）。如果未配置此设置，则速率将降至每秒 4 次身份验证。

使用 **Citrix Cloud Connector** 时的流量延迟和用户身份验证速率

下表显示了使用 Citrix Cloud Connector 时的流量延迟和用户身份验证速率：

身份验证类型	身份验证延迟 (p95)（以毫秒为单位）	每秒的身份验证或用户登录速率
LDAP	5.99	14
RADIUS	3.17	14
LDAP+RADIUS	4.59	14
LDAPS	26.75	14
LDAPS+RADIUS	15.61	14

使用 **Azure vNet** 对等互连时的流量延迟和用户身份验证率

下表显示了使用 Azure vNet 对等互连时的流量延迟和用户身份验证速率：

身份验证类型	请求延迟 (p95)（以毫秒为单位）	每秒的身份验证或用户登录速率
LDAP	6.95	17.54
LDAPS	7.19	16.98

数据治理

June 19, 2024

本主题提供有关 Citrix 自适应身份验证服务和自适应身份验证实例收集、存储和保留日志的信息。定义中未定义的任何大写术语均具有 Citrix 最终用户服务协议中指定的含义。

- 自适应身份验证服务：管理员可以登录以部署和管理自适应身份验证实例的 Citrix Cloud 服务。
- 自适应身份验证实例：由自适应身份验证服务部署的 NetScaler 虚拟机，允许管理员管理用户身份验证。

数据驻留

自适应身份验证服务

Citrix 自适应身份验证服务客户内容数据位于 Azure 云服务东部区域。它们被复制到以下 Azure 区域以获得可用性和冗余：

- 美国西部
- 北欧

以下是服务配置和运行时日志的不同目标。

- Splunk 服务用于系统监视和调试日志，仅在美国和欧盟（欧盟）位置。
- NetScaler Application Delivery Management 服务，用于汇总的用户访问日志。有关详细信息，请参阅 NetScaler ADM 数据治理。
- 用于管理员审核日志的 Citrix Cloud 系统日志服务。有关详细信息，请参阅 Citrix Cloud 服务客户内容和日志处理以及地理注意事项。

自适应身份验证实例

NetScaler Application Delivery Management 服务，用于备份所有配置和特定于实例的工件。有关详细信息，请参阅 NetScaler ADM 数据治理。

数据收集

Citrix 自适应身份验证服务允许客户管理员通过自适应身份验证 UI 配置服务，并通过控制台配置配套的 Connector Appliance。收集以下客户内容：

- 自适应身份验证服务
  - IdP（身份提供商）终端节点的 FQDN（完全限定域名）和 IP 地址。

  - IP 地址/范围、端口和协议
  - 用于访问 IdP 身份验证虚拟服务器的证书
  - 管理端点的公有 IP 地址
  - 对于 Azure VNet 对等，是具有网络贡献者角色的服务主体。有关详细信息，请参阅 使用 Azure VNet 对等互连设置与本地身份验证服务器的连接。

- 应用程序权利的用户标识符
- Citrix Cloud Connector 相关详细信息。有关详细信息，请参阅 Citrix Cloud Connector。
  - IP 地址或 FQDN
  - 用户、设备和资源位置标识符
  - 内部代理配置

对于服务组件收集的运行时日志，关键信息包括以下内容：

- 客户端 IP 地址和端口
- 目标 FQDN/地址和端口
- 客户端用户代理
- 应用程序 URL 路径
- 应用程序访问时间和持续时间
- 请求字节数
- 响应字节数
- HTTP 事务 ID
- 部署模式（连接器或 Azure VNet 对等）
- Azure 资源
  - 资源组名称
  - VNet（IP 地址、CIDR）
  - 子网（IP 地址、CIDR）
  - 虚拟机名称

数据传输

Citrix 自适应身份验证服务将日志发送到受传输层安全保护的目标 (Splunk)。

数据控制

Citrix 自适应身份验证服务当前不为客户提供关闭发送日志或阻止全局复制客户内容的选项。

数据保留

根据 Citrix Cloud 数据保留策略，客户配置数据将在订阅到期 90 天（大约 3 个月）后从服务中清除。

日志目标维护其特定于服务的数据保留策略。

- 用于存储在 Citrix Application Delivery Management 中的事件。请参阅 Citrix ADM 数据治理。
- Splunk 日志会在 90 天（大约 3 个月）后存档并最终删除。
- 自适应身份验证实例将在订阅到期 30 天（大约四个半星期）后解除分配。

数据导出

对于几种类型的日志，有不同的数据导出选项。

- 管理员审核日志可从 Citrix Cloud 系统日志控制台访问。
- Splunk 日志不供客户使用。这些事件也可以从 Splunk 导出为 CSV 文件。

定义

- 客户内容是指上载到客户帐户以进行存储的任何数据，或在 Citrix 有权访问以执行服务的客户环境中的数据。
- 日志是指与服务相关的事件记录，包括衡量性能、稳定性、使用情况、安全性和支持的记录。
- 服务意味着前面概述的 Citrix Cloud 服务旨在促进客户使用案例。