在AppDynamics中配置单一登录并对其进行故障排除

目录

简介

本文档介绍如何在AppDynamics中配置单点登录(SSO)并排除问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 要配置单点登录，用户必须具有帐户所有者（默认）角色或具有管理、代理和入门向导权限的自定义角色。
- 对您的IdPaccount的管理员访问权限。
- AppDynamics的元数据或配置详细信息（例如，实体ID、ACS URL）。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- AppDynamics控制器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

单点登录(SSO)是一种身份验证机制，允许用户一次性登录并访问多个应用、系统或服务，而无需对每个应用进行再次身份验证。

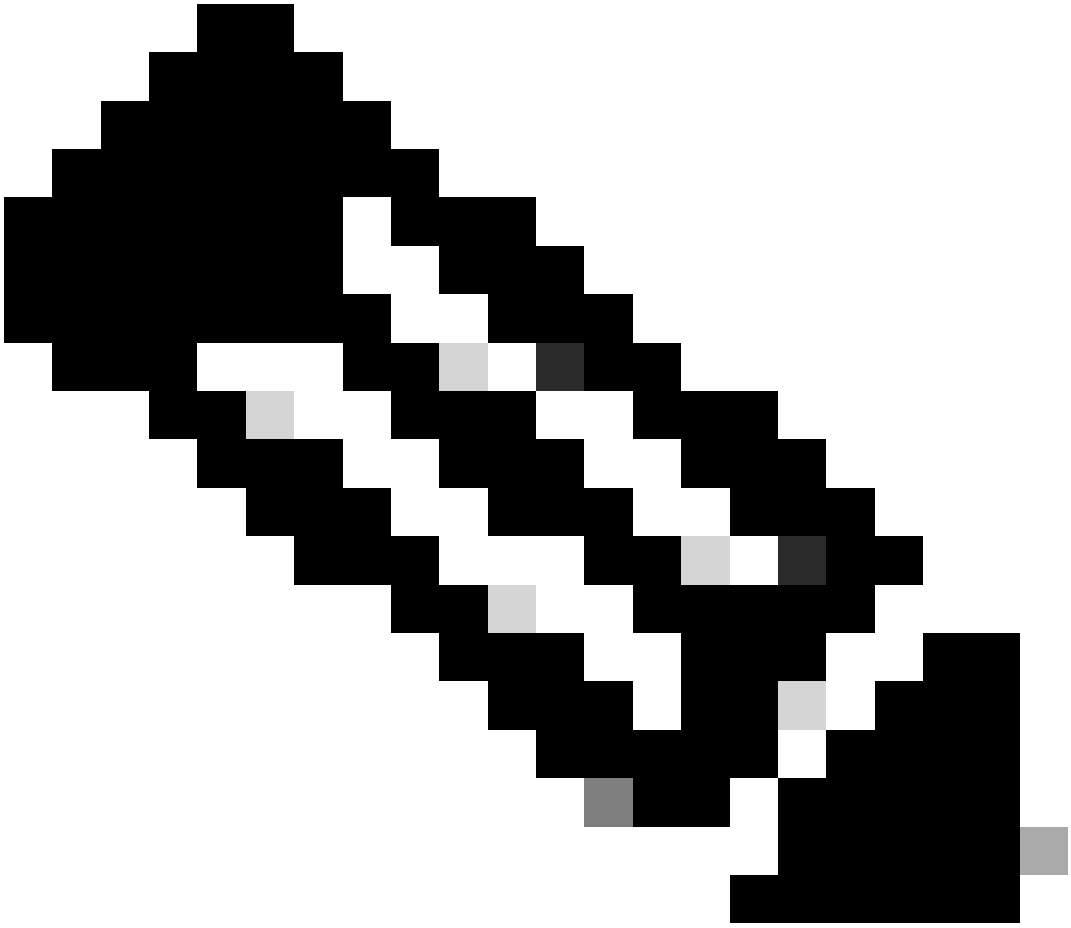
安全断言标记语言(SAML)是用于实现SSO的技术之一。它提供框架和协议，通过在身份提供程序(IdP)和服务提供程序(SP)之间安全地交换身份验证和授权数据来启用SSO。

SAML断言

- IdP和SP之间基于XML的消息交换。
- 它提供三种断言：
  - 身份验证断言：确认用户已通过身份验证。
  - 属性断言：共享用户属性，例如用户名或角色。
  - 授权决策声明：指示用户有权执行的操作。

SAML中的主要角色

- 身份提供程序(IdP)
  - 验证用户的身份。
  - 生成包含用户标识信息的SAML断言。
- 服务提供商(SP)
  - 用户想要访问的应用程序或系统。
  - 依赖IdP对用户进行身份验证。
  - 接受SAML断言以授予用户对其资源或应用的访问权限。
- 用户（承担者）
  - 发起请求或尝试从服务提供商访问资源的实际用户。
  - 与IdP（身份验证）和SP交互。



注意：AppDynamics支持IdP启动和SP启动的SSO。

SP启动的流：

- 用户通过键入应用（例如，AppDynamics）的URL或点击链接导航到服务提供商。
- SP检查现有会话。如果不存在会话，则SP会识别用户未通过身份验证，并启动SSO进程。
- SP生成SAML身份验证请求并将用户重定向到IdP进行身份验证。
    - 此请求包括：
        - 实体ID:服务提供商唯一标识符。
        - 断言消费者服务(ACS)URL:其中，IdP在身份验证后发送SAML断言。
        - 有关SP和安全详细信息的元数据（例如，签名的请求、加密要求）。
- 用户被重定向到IdP登录页面。
- IdP对用户进行身份验证（例如，通过用户名/密码或多重身份验证）。
- 身份验证成功后，IdP会生成SAML断言（安全令牌）。
- SAML断言通过使用HTTP POST绑定（大多数情况下）或HTTP重定向绑定通过用户浏览器发送回SP。
- SP验证SAML断言以确保：

    - 由受信任的IdP颁发。
    - 其地址为SP（通过SP实体ID）。
    - 它尚未过期或被篡改（使用IdP公钥进行验证）。

- 如果SAML断言有效，SP将为用户创建会话。
- 用户被授予对应用程序或资源的访问权限。

IdP发起的流：

- 用户导航到IdP登录门户并输入其凭证。
- IdP对用户进行身份验证（例如，使用用户名/密码组合、多重身份验证）。
- 身份验证后，IdP向用户显示他们可以访问的可用应用或服务(SP)的列表。
- 用户选择所需的SP（例如，AppDynamics）。
- IdP为选定SP生成SAML断言。

- IdP将用户重定向到SP声明使用者服务(ACS)URL，并随其发送SAML声明（使用HTTP POST绑定或HTTP重定向绑定）。
- SP接收SAML断言并验证它：
    - 确保由受信任的IdP发出断言。
    - 验证断言完整性和到期情况。
    - 确认用户身份和其他属性。

- 如果SAML断言有效，SP将为用户创建会话。
- 用户被授予对应用程序或资源的访问权限。

配置

AppDynamics控制器可以使用思科客户身份或外部SAML身份提供程序(IdP)对用户进行身份验证和授权。

支持的身份提供程序

AppDynamicscertificates为这些身份提供程序(IdP)提供支持：

- 奥克塔
- 奥内洛金
- Ping身份
- Azure AD
- IBM云身份
- 活动目录联合身份验证服务 (AD FS)

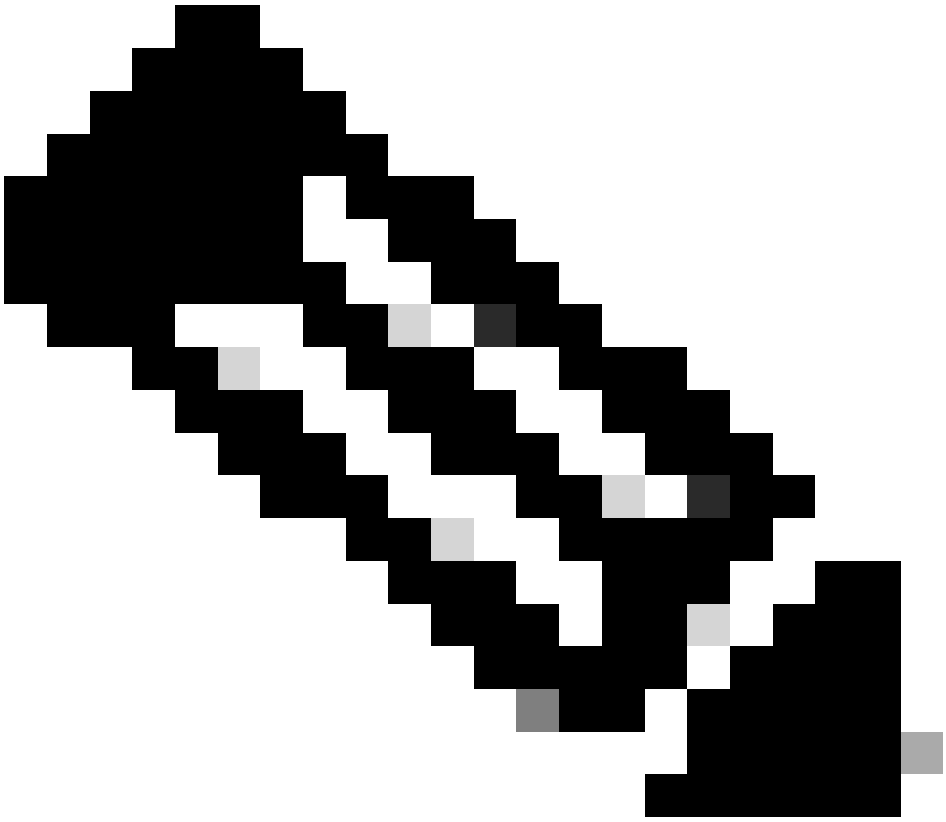
其他支持HTTP POST绑定的IdP也与AppDynamics SAML身份验证兼容。

在AppDynamics中配置SAML的步骤

步骤1.收集AppDynamics控制器详细信息

- 实体ID（SP实体ID）：AppDynamics的唯一标识符(例如，https://<controller-host>:<port>/controller)。
  - 语法: https://<controller_domain>/controller
  - 示例：https://<your_controller_domain>/controller

- 回复URL(Assertion Consumer Service， ACS URL)：服务提供商（例如，AppDynamics）上的终端，其中IdP在身份验证后发送SAML响应。
  - 语法:https://<controller_domain>/controller/saml-auth?accountName=<account_name>
  - 示例：https://your_controller_domain/controller/saml-auth?accountName=youraccountname



注意：对于内部控制器，默认帐户名称为customer1，除非您拥有具有不同帐户名称的多租户控制器。

- 单一注销URL（可选）：SP上用于处理SAML注销请求的终端(例如，https://<controller_domain>/controller)。

步骤2.在IdP中创建新应用程序并下载元数据

- 查找应用程序创建区域：通常在IdP管理控制台或控制面板中，通常标有应用程序、Web和移动应用、企业应用或信赖方等内容。

- 添加自定义或通用SAML应用程序：选择允许您配置自定义SAML应用程序或通用SAML服务提供商集成的选项。
- 提供应用详细信息：为应用提供名称，并可能上传用于标识的图标（可选）。
- 添加属性映射（用户名、displayName、电子邮件或角色）以将用户信息传递给AppDynamics。
- 下载IdP元数据文件，或者记下以下详细信息：
  - IdP登录网址
  - 注销URL
  - 属性名称
  - 证书

步骤3.在AppDynamics控制器中配置SAML身份验证

- 以帐户所有者角色或具有管理、代理和入门向导权限的角色身份登录控制器UI。
- 单击您的用户名（右上角）>管理>身份验证提供程序>选择SAML。

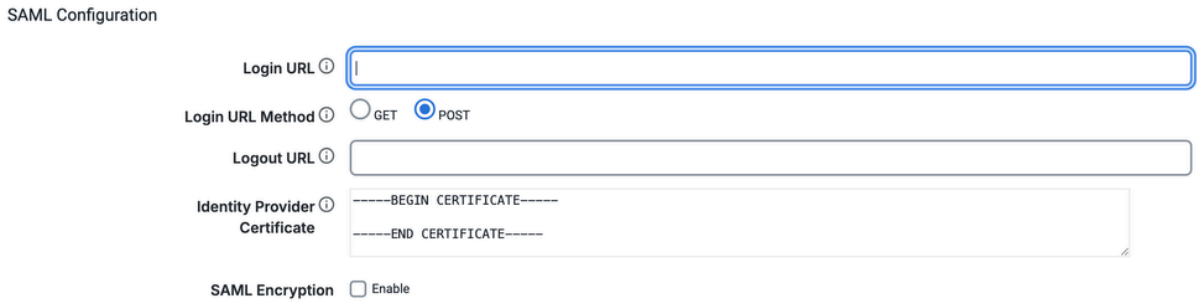
- 在SAML Configuration部分中，添加以下详细信息：

  - 登录URL:AppDynamics控制器在其中路由服务提供商(SP)启动的登录请求的IdP登录URL。

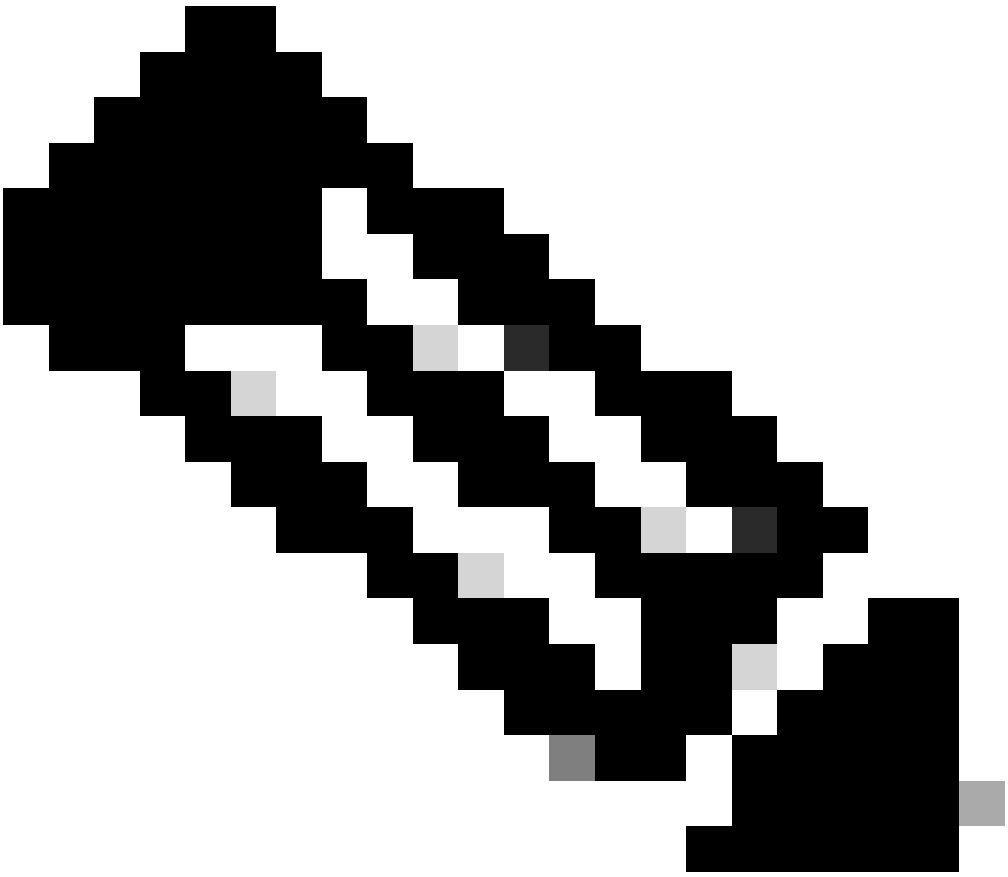
  - 注销URL（可选）:AppDynamics Controller在用户注销后重定向到的URL。如果未指定注销URL，则用户在注销时会看到AppDynamics登录屏幕。

  - 证书:IdP提供的X.509证书。在BEGIN CERTIFICATE和END CERTIFICATE分隔符之间粘贴证书。避免从源证书本身复制BEGIN CERTIFICATE和END CERTIFICATE分隔符。

  - SAML加密（可选）：可以通过加密从IdP到服务提供商的SAML响应来提高SAML身份验证的安全性。若要在AppDynamics中加密SAML响应，需要将身份提供程序(IdP)配置为加密SAML声明，然后将AppDynamics控制器配置为使用特定证书和私钥进行解密。

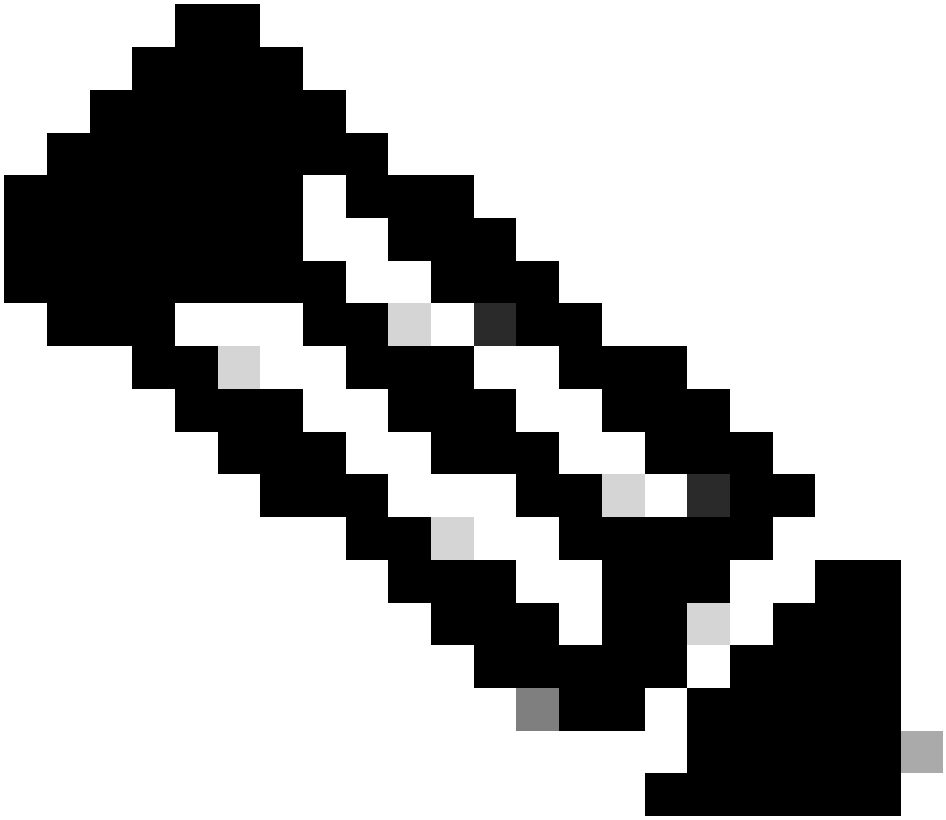


- 在SAML Attribute Mappings部分中，映射SAML属性(示例：用户名、DisplayName和电子邮件)。



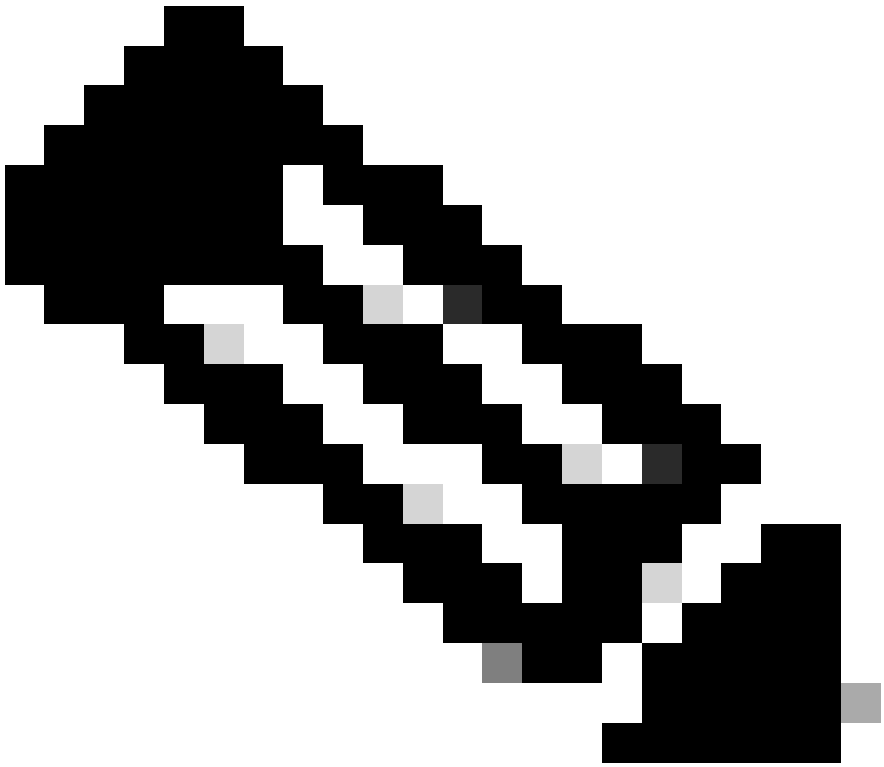
注意：AppDynamics显示SAML用户的用户名、电子邮件和显示名称。默认情况下，它使用SAML响应中的NameID属性创建用户名，该用户名也用作displayName。可以通过在SAML响应中包含用户名、电子邮件和显示名称属性来自定义此行为。在AppDynamics中配置IdP设置时，用户可以指定这些属性名称。在登录期间，AppDynamics检查是否配置了属性映射。如果映射已配置且SAML响应中存在匹配的属性，AppDynamics将使用这些属性值设置用户名、电子邮件和显示名称。

- 在SAML Group Mappings部分，添加这些详细信息。
  - SAML组属性名称：输入包含组信息的SAML属性的名称。这通常为组、组或角色、角色或组成员身份。
  - 组属性值(Group Attribute Value)：选择组属性的适当值格式。 常用选项包括多个嵌套组值或单个值，具体取决于IdP如何构建组信息。

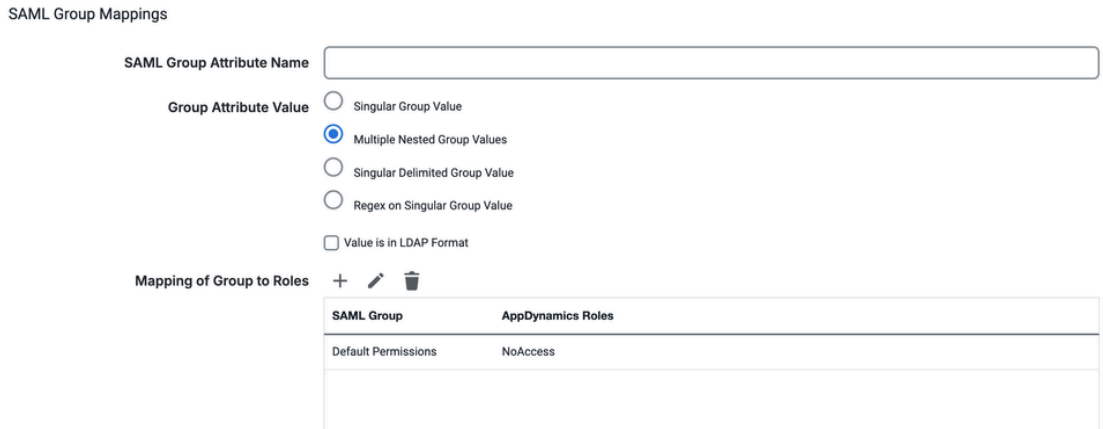


注意：如果组信息采用LDAP（轻量级目录访问协议）格式，请选择Value is in LDAP Format。

- 组到角色的映射：点击+按钮以添加新映射。
  - SAML组：输入要映射到AppDynamics角色的SAML组的名称（在IdP中定义）。
  - 角色：从可用列表中选择要分配给属于SAML组的用户的对应AppDynamics角色。
  - 默认权限：如果未配置SAML组映射，或者如果用户SAML断言不包括组信息，AppDynamics将回退到使用默认权限。



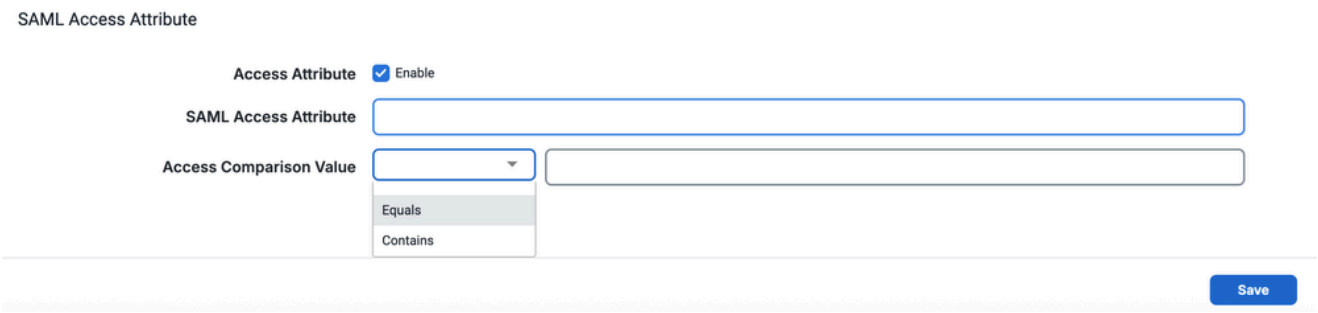
注意：建议为默认权限分配具有最低权限的角色。



- 在SAML Access Attribute部分，添加以下详细信息（可选）：
  - SAML访问属性：输入SAML响应中属性的名称。这将用于访问验证。
  - 访问比较值：有两个可用选项：
    1. 等于：仅当SAML响应中的属性值与配置中指定的值完全匹配时，才授予访问权限

。
2. 包含：如果SAML响应中的属性值包含配置中指定的值，则授予访问权限。
- 如果启用，其工作方式：
1. AppDynamics从SAML响应检索SAML Access Attribute字段中指定的属性。
2. 它将根据所选方法（Equal或Contains）将属性的值与用户定义的访问比较值进行比较。
3. 如果比较成功，则授予用户访问权限。
4. 如果比较失败，登录尝试将被拒绝。

- 单击Save（右下角）保存配置。



验证

- 打开浏览器并导航到AppDynamics Controller。系统将显示第三方IdP服务的“登录”对话框。
- 单击Log in with Single Sign-On。系统会将您重定向到IdP。
- 输入并提交您的凭据。
- 成功进行身份验证后，IdP会将您重定向到AppDynamics控制器。

常见问题和解决方案

400错误请求

- 问题：用户在尝试登录到AppDynamics Controller时遇到400 Bad Request错误。
- 示例错误：

```
HTTP status 400 - Bad Request
Message: Error while processing SAML Authentication Response - see server log for details
Description: The request sent by the client was syntactically incorrect.
```

- 常见根本原因：
  - 无效的SAML证书
  - SAML响应大于最大长度
  - 实体ID或ACS URL无效
- 解决方案：
  - 无效的SAML证书

- 确保身份提供程序(IdP)提供的证书有效且是最新的。
- 验证IdP证书的到期日期。如果已过期，请从IdP获取新证书。
- 如果在IdP端更新了证书，请确保在AppDynamics中上载并配置新证书。
- 在AppDynamics中更新证书的步骤：
  - 以帐户所有者角色或具有管理、代理、入门向导权限的角色身份登录到控制器UI。
  - 点击您的用户名（右上角）>管理>身份验证提供程序>选择SAML。
  - 在SAML Configuration部分中，找到certificate 字段，并用IdP提供的新证书替换旧证书。
  - 单击Save以更新SAML配置。

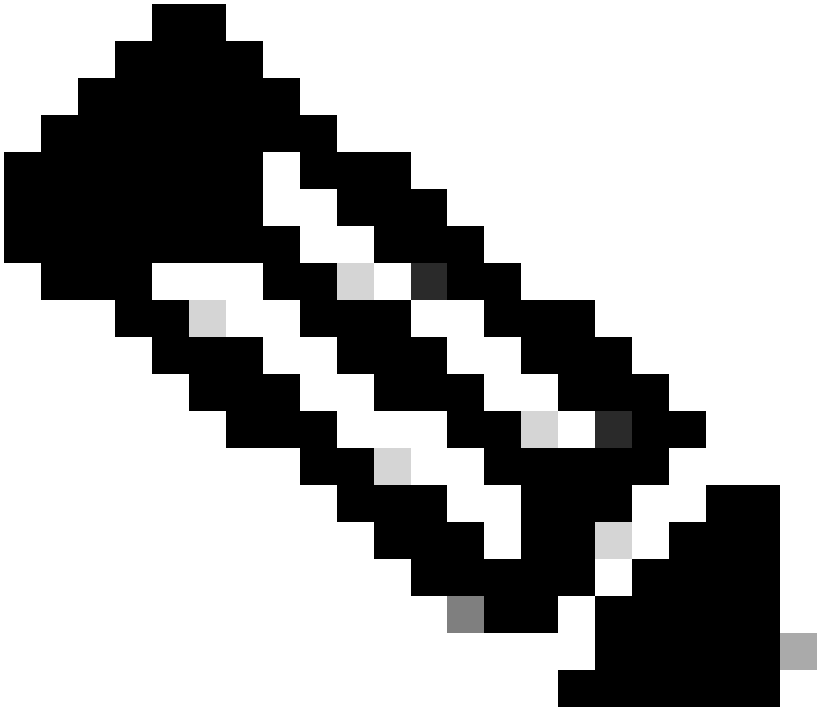
- SAML响应大于最大长度。
  - 从控制器版本23.11及以上版本开始，当控制器从GlassFish移至Jetty Server时，会出现此问题。在Jetty Server中，有一个名为 — Dorg.eclipse.jetty.server的属性。Request.maxFormContentSize位于……/appserver/jetty/start.d/start.ini文件。如果SAML响应大小超过为此属性设置的值，则控制器将拒绝负载并返回400错误请求 错误.
  - 大量SAML响应的原因：
    - 属性过多：SAML断言中包含的属性过多。
    - 签名或加密SAML响应：签名或加密会增加响应大小。
    - 其他用户或组数据：身份提供程序(IdP)具有额外的用户或组数据。

  - 有两种方法可以解决此问题。通过实施其中一种或两种解决方案，您可以解决问题并防止拒绝负载。
    1. 增加maxFormContentSize值
       - 对于内部控制器：更新……中的 — Dorg.eclipse.jetty.server.Request.maxFormContentSize属性。/appserver/jetty/start.d/start.ini文件更改为更大的值，然后重新启动控制器。
       - 对于SaaS控制器：提交支持票证，以便支持团队解决此问题。

    2. 优化SAML响应

       与您的身份提供程序(IdP)配合通过进行以下调整来减小SAML响应的大小：

       - 排除不必要的属性：通过IdP配置从SAML断言中删除未使用的或冗余属性。
       - 禁用加密（如果允许）：加密会增加SAML响应大小。如果连接已通过HTTPS受到保护，请考虑禁用加密以减小大小。
- 实体ID或ACS URL无效
  - 在Idp上：
    - 确认实体ID为https://your_controller_domain/controller。如果实体ID不同，请对其进行更新。
    - 确认ACS URL为https://your_controller_domain/controller/saml-auth?accountName=youraccountname。如果ACS URL不同，请相应地更新它。



注意：accountName必须与您的AppDynamics帐户名称匹配。（例如，customer1）

- 缺少用户权限
  - 问题：您已成功登录到控制器。但是，您未收到预期的角色和权限。
  - 配置和SAML响应示例：
    - 在SAML用户的Group属性中，名称为Groups，其值为AppD_Admin和AppD_Power_User。

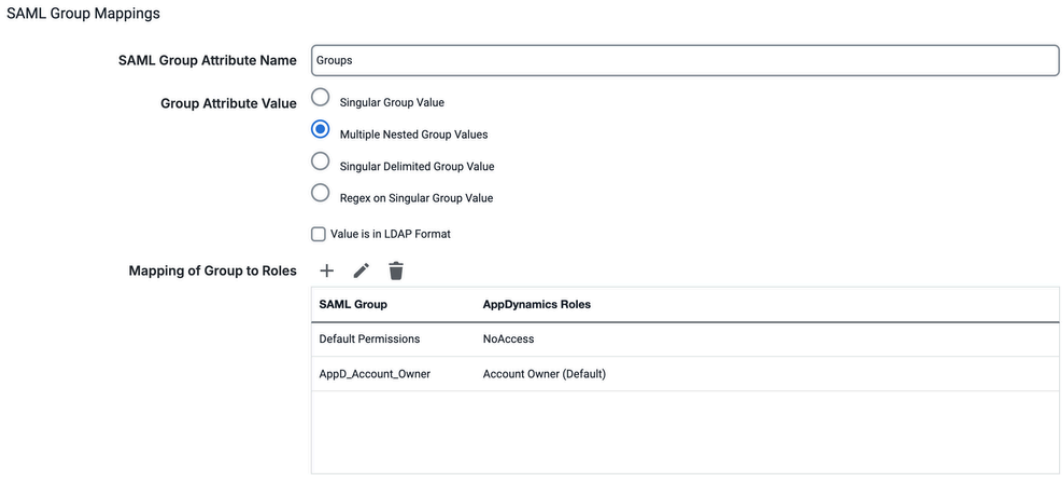
```
AppD_Admin
```

```
AppD_Power_User
```

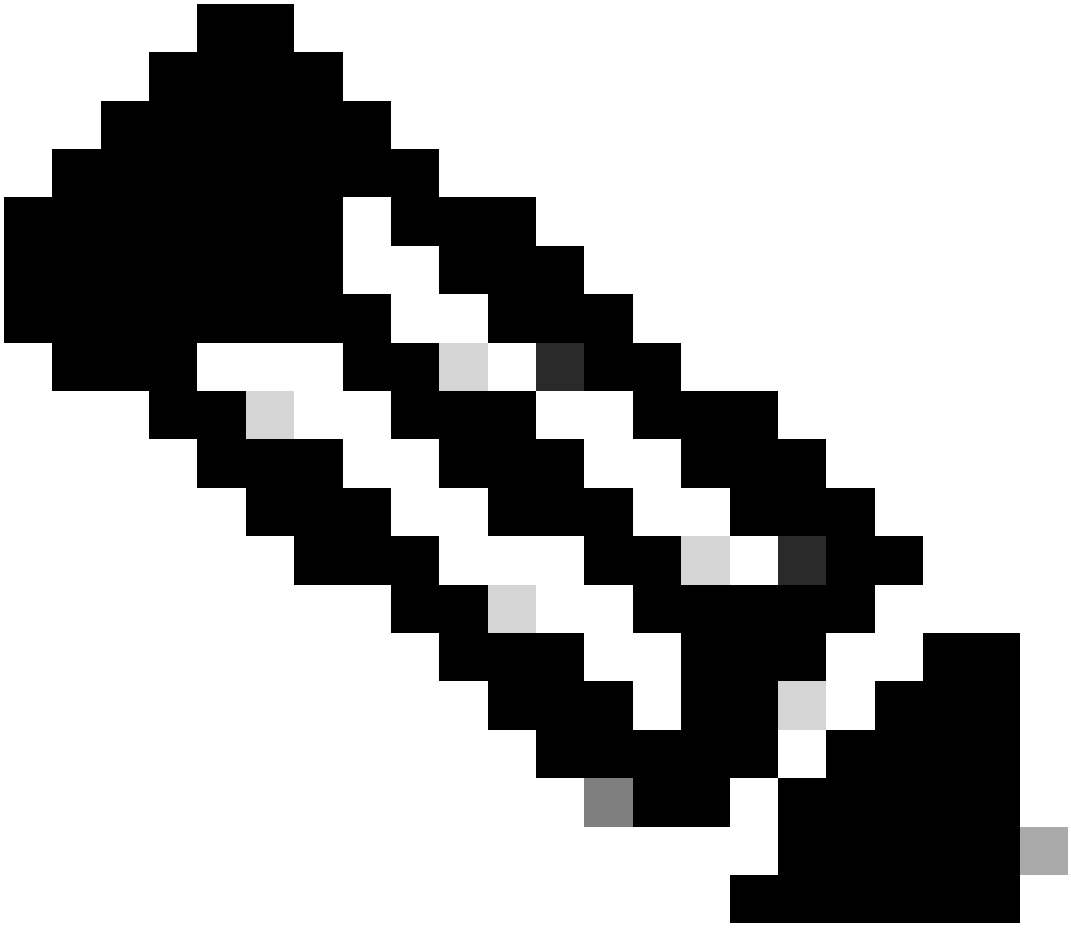
- 在AppDynamics的“SAML组映射”(SAML Group Mappings)部分下，配置了这些映射。
  - SAML组属性名称：组
  - 组属性值：多个嵌套组值
  - 映射到组角色：

SAML组	AppDynamics角色
AppD_Account_Owner	帐户所有者（默认）
默认权限	无法访问

No Access是没有权限的自定义角色。



- 常见问题和解决方案
  - 在SAML响应中找不到组属性。
    - 来自IdP的SAML响应缺少所需的组属性，或者SAML响应中的组的属性名称被设置为“角色”，但在AppDynamics中，它被配置为“组”。
    - 如果未提供组属性，系统会自动为用户分配与AppDynamics中的“默认权限”关联的角色。
    - 要解决此问题，请确保将IdP配置为在SAML响应中包含正确的组属性，并且组的属性名称与AppDynamics中的配置匹配。
  - AppDynamics中没有为SAML响应中提供的用户组配置相应的SAML组映射。
    - 在SAML响应中，“组”属性包含值AppD_Admin和AppD_Power_User。但是，在AppDynamics中，只有AppD_Account_Owner组存在组映射。
    - 由于AppD_Admin或AppD_Power_User没有对应的映射，因此没有为用户分配任何角色或权限。
    - 要解决此问题，请在AppDynamics中添加缺少的组映射（例如，AppD_Admin和AppD_Power_User），以确保正确的角色和权限分配。



注意：只有当AppDynamics中配置的SAML组属性名称与SAML响应中的组属性不同时，才会对SAML用户应用默认权限。

- SAML用户的邮件和/或名称缺失或不正确
  - 问题：当AppDynamics中的属性配置与SAML响应中的属性不匹配时，通常会发生这种情况。
  - SAML响应示例：SAML响应中的属性包括：User.email、User.fullName和Groups

FirstName LastName

AppD_Admin

AppD_Power_User

- AppDynamics中的SAML属性映射示例
  - 用户名属性：User.name
  - 显示名称属性：User.firstName或为空
  - 电子邮件属性：User.userPrincipal或空白

- 根本原因：在AppDynamics中配置的显示名称和电子邮件属性与SAML响应中提供的任何属性均不匹配。
  - 因此：

        - 电子邮件被设置为空白。
        - 显示名称默认为用户名。

    - 解决方案：确保AppDynamics中配置的“显示名称”和“电子邮件”属性与SAML响应中的相应属性匹配。
        - 例如:
            - 将“显示名称”属性更新为User.fullName。
            - 将Email属性更新为User.email。

- HTTP 404错误

- 问题：用户无法登录到控制器，并收到404 not found错误。
- 示例错误：在控制器日志中（仅适用于内部控制器），您会看到以下错误：

```
[#|2025-01-10T21:16:35.222+0000|SEVERE|glassfish 4.1|com.singularity.ee.controller.auth.saml.SAMLA
com.appdynamics.platform.services.auth.exception.SamlException: Requested url validation failed
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.validateRequest
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.getSamlAuthenti
```

- 根本原因：当控制器数据库中配置的控制器URL与用于登录的控制器URL或IdP上配置的URL不匹配时，通常会发生此错误
- 解决方案：
    - 对于内部控制器：
        - 运行此命令可更新控制器URL。（推荐）。

```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{


/controller" }' http://


/controller/rest/accounts/


/update-controller-url
```

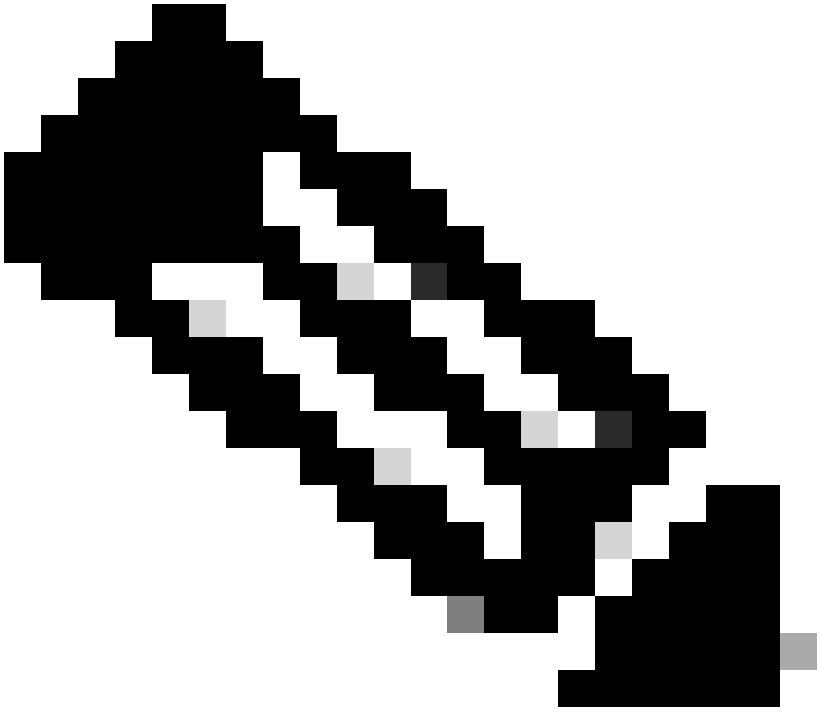
        - 或者，您可以在控制器数据库中运行这些命令以更新控制器URL。

```
UPDATE controller.account SET controller_url ='
```

```
' WHERE id=

;
UPDATE mds_auth.account SET controller_url='

' WHERE name='

';
```

- 运行此命令可获取<ACCOUNT_ID>。

```
Select id from controller.account where name = '

';
```



注意：如果仍然观察到相同问题，请运行curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll。

- 替换：
  - <NEW_CONTROLLER_URL>以及正在用于访问控制器的实际控制器URL。
  - <controller_domain>和您的控制器域。
  - <youraccountname>和您的帐户名称。

- 对于SaaS控制器：提交支持票证，以便支持团队解决此问题。

需要进一步的帮助

如果您遇到问题或遇到问题，请创建包含以下详细信息的支持通知单：

- 错误详细信息或屏幕截图：提供特定错误消息或问题的屏幕截图。
- SAML响应：收集SAML-Trace和HAR文件
- Controller Server.log（仅限内部版本）：如果适用，请从<controller-install-dir>/logs/server.log提供控制器服务器日志

相关信息

AppDynamics文档

适用于SaaS部署的SAML

加密SaaS部署的SAML响应

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。