在AppDynamics中配置單一登入並對其進行故障排除

目錄

簡介

本文檔介紹如何在AppDynamics中配置單一登入(SSO)並排除問題。

必要條件

需求

思科建議您瞭解以下主題：

- 要配置單一登入，使用者必須具有帳戶所有者（預設）角色或具有管理、代理和入門嚮導許可權的自定義角色。
- 對您的IdPaccount的管理員訪問許可權。
- AppDynamics中的後設資料或配置詳細資訊（例如，實體ID、ACS URL）。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AppDynamics控制器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

單點登入(SSO)是一種身份驗證機制，允許使用者一次性登入並訪問多個應用程式、系統或服務，而無需對每個應用程式進行再次身份驗證。

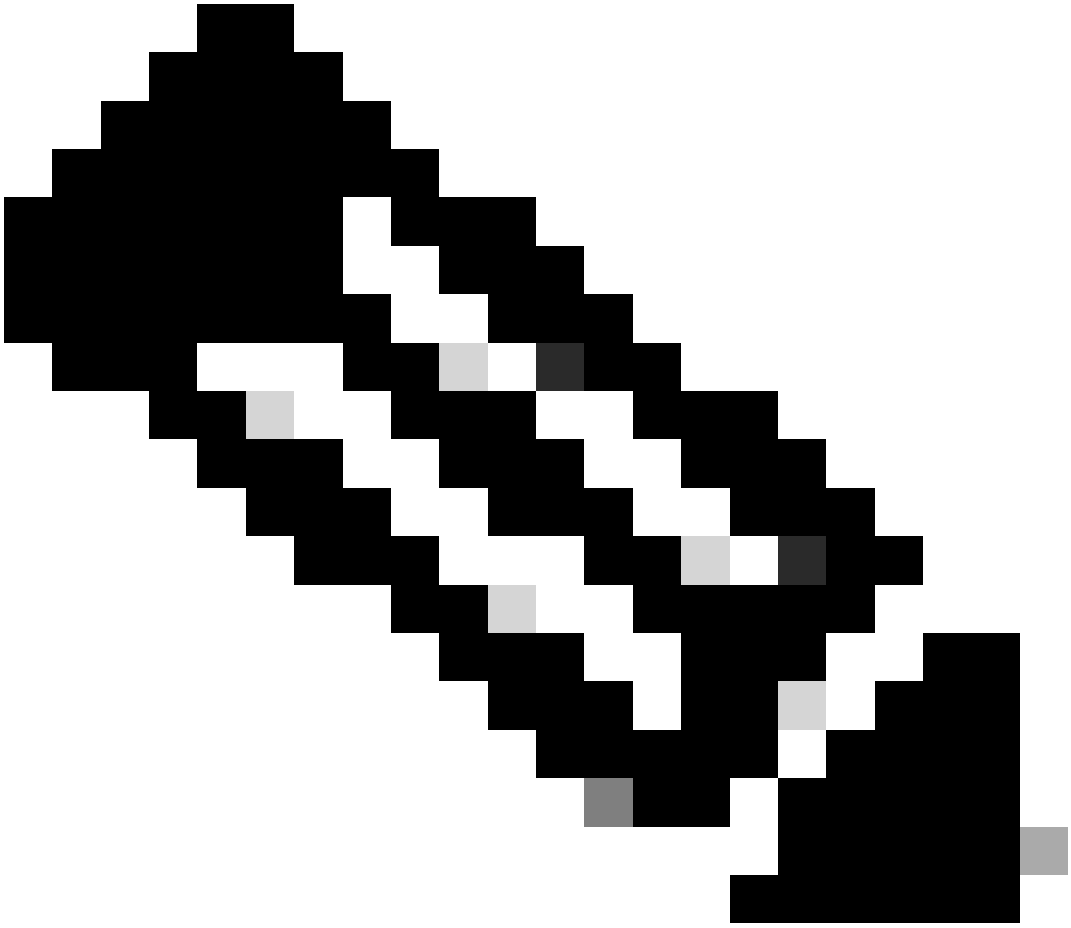
安全斷言標籤語言(SAML)是實現SSO的技術之一。它提供了框架和協定，通過在身份提供程式(IdP)和服務提供程式(SP)之間安全地交換身份驗證和授權資料來啟用SSO。

SAML斷言

- IdP和SP之間基於XML的報文交換。
- 它提供了三種斷言：
  - 身份驗證斷言：確認使用者已經過身份驗證。
  - 屬性斷言：共用使用者屬性，例如使用者名稱或角色。
  - 授權決策宣告：指示使用者有權執行的操作。

SAML中的關鍵角色

- 身份提供程式(IdP)
  - 驗證使用者的身份。
  - 生成包含使用者標識資訊的SAML斷言。
- 服務提供商(SP)
  - 使用者想要訪問的應用程式或系統。
  - 依賴IdP對使用者進行身份驗證。
  - 接受SAML斷言以授予使用者對其資源或應用程式的訪問許可權。
- 使用者（主體）
  - 發起請求或嘗試從服務提供商訪問資源的實際使用者。
  - 同時與IdP（身份驗證）和SP互動。



附註：AppDynamics支援IdP啟動和SP啟動的SSO。

SP啟動的流：

- 使用者通過鍵入應用程式（例如AppDynamics）的URL或按一下連結導航到Service Provider。
- SP將檢查現有會話。如果不存在任何會話，SP將識別使用者未通過身份驗證，並啟動SSO進程。
- SP生成SAML身份驗證請求，並將使用者重定向到IdP以進行身份驗證。
    - 此請求包括：
        - 實體ID:服務提供商唯一識別符號。
        - 斷言使用者服務(ACS)URL:其中IdP在身份驗證後傳送SAML斷言。
        - 有關SP和安全詳細資訊的後設資料（例如，簽名請求、加密要求）。
- 系統會將使用者重新導向到IdP登入頁面。
- IdP對使用者進行身份驗證（例如，通過使用者名稱/密碼或多重身份驗證）。
- 身份驗證成功後，IdP會生成SAML斷言（安全令牌）。
- 使用HTTP POST繫結（大多數情況下）或HTTP重定向繫結，通過使用者瀏覽器將SAML斷言

傳送回SP。
- SP驗證SAML斷言以確保：
  - 由受信任的IdP頒發。
  - 它通過SP實體ID傳送到SP。
  - 它尚未過期或被篡改（使用IdP公鑰進行驗證）。

- 如果SAML斷言有效，SP將為使用者建立會話。
- 授予使用者訪問應用程式或資源的許可權。

IdP啟動的流：

- 使用者導航到IdP登入門戶並輸入其憑據。
- IdP對使用者進行身份驗證（例如，使用使用者名稱/密碼組合、多重身份驗證）。
- 身份驗證後，IdP向使用者顯示他們可以訪問的可用應用程式或服務(SP)的清單。
- 使用者選擇所需的SP（例如，AppDynamics）。
- IdP為所選SP生成SAML斷言。

- IdP將使用者重定向到SP斷言使用者服務(ACS)URL，並隨其傳送SAML斷言（使用HTTP POST繫結或HTTP重定向繫結）。
- SP收到SAML斷言並驗證它：
  - 確保宣告由受信任的IdP發出。
  - 驗證斷言完整性和過期時間。
  - 確認使用者身份和其他屬性。

- 如果SAML斷言有效，SP將為使用者建立會話。
- 授予使用者訪問應用程式或資源的許可權。

設定

AppDynamics控制器可以使用思科客戶身份或外部SAML身份提供程式(IdP)對使用者進行身份驗證和授權。

支援的身份提供程式

AppDynamicscertificate支援這些身份提供程式(IdPs):

- 奧克塔
- 奧內洛金
- Ping身份
- Azure AD
- IBM雲端身分
- Active Directory聯合身份驗證服務(AD FS)

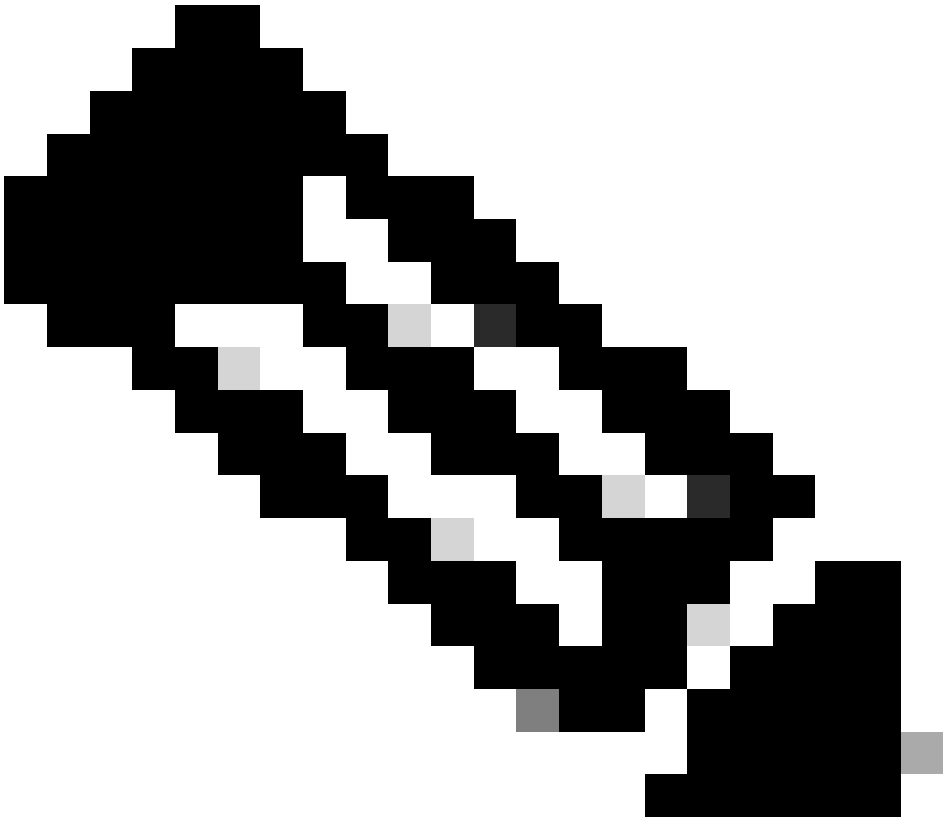
其他支援HTTP POST繫結的IdP也與AppDynamics SAML身份驗證相容。

在AppDynamics中配置SAML的步驟

步驟1.收集AppDynamics控制器詳細資訊

- 實體ID（SP實體ID）：AppDynamics的唯一識別符號(例如，https://<controller-host>:<port>/controller)。
  - 語法： https://<controller_domain>/controller
  - 範例：https://<your_controller_domain>/controller

- 回覆URL（斷言使用者服務、ACS URL）：服務提供程式（例如AppDynamics）上的終結點，其中IdP在身份驗證後傳送SAML響應。
  - 語法：https://<controller_domain>/controller/saml-auth?accountName=<account_name>
  - 示例： https://your_controller_domain/controller/saml-auth?accountName=youraccountname



附註：對於本地控制器，預設帳戶名稱為customer1，除非您有一個具有不同帳戶名稱的多租戶控制器。

- 單一註銷URL（可選）：SP上處理SAML註銷請求的終結點(例如，https://<controller_domain>/controller)。

步驟2.在IdP中建立新應用程式並下載後設資料

- 查詢應用程式建立區域：這通常在IdP管理控制檯或控制面板中，通常標有「應用程式」、「Web和移動應用程式」、「企業應用程式」或「信賴方」之類的內容。
- 新增自定義或通用SAML應用程式：選擇允許您配置自定義SAML應用程式或通用SAML服務提供商整合的選項。
- 提供應用程式詳細資訊：為應用程式指定一個名稱，並可能上傳一個標識圖示（可選）。
- 新增屬性對映（使用者名稱、displayName、電子郵件或角色）以將使用者資訊傳遞到AppDynamics。
- 下載IdP後設資料檔案，或者記下以下詳細資訊：
  - IdP登入網址
  - 註銷URL
  - 屬性名稱
  - 憑證

步驟3.在AppDynamics控制器中配置SAML身份驗證

- 以帳戶所有者角色或具有管理、代理和入門嚮導許可權的角色身份登入到Controller UI。
- 按一下User Name（右上角）> Administration > Authentication Provider > Select SAML。

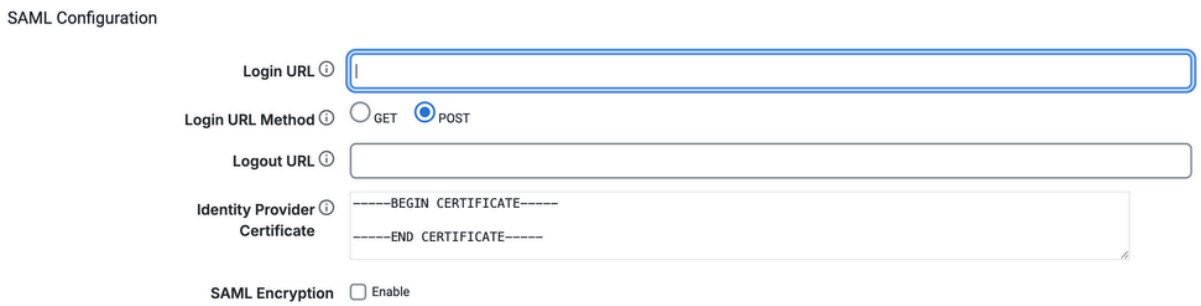
- 在SAML Configuration部分中，新增以下詳細資訊：

  - 登入URL:AppDynamics Controller在其中路由服務提供程式(SP)啟動的登入請求的IdP登入URL。

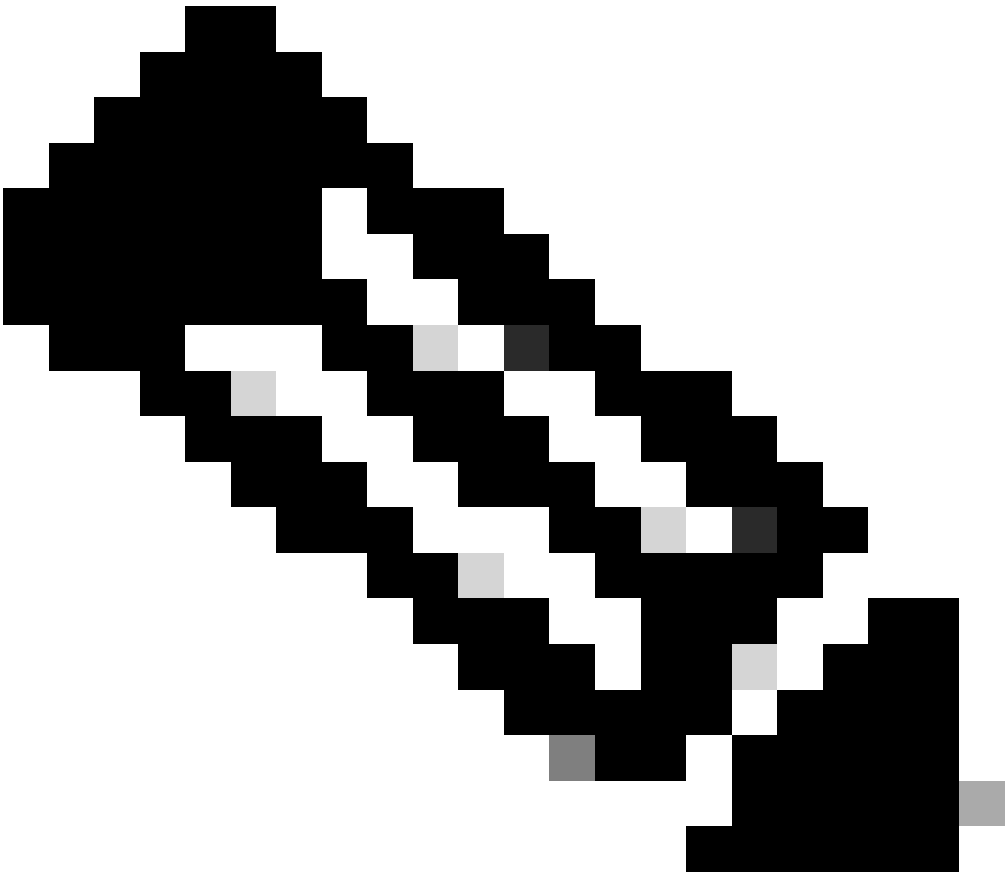
  - 註銷URL（可選）:AppDynamics Controller在使用者註銷後重定向的URL。如果未指定註銷URL，則使用者註銷時會看到AppDynamics登入螢幕。

  - 證書:來自IdP的X.509證書。在BEGIN CERTIFICATE和END CERTIFICATE分隔符之間貼上證書。避免從源證書本身複製BEGIN CERTIFICATE和END CERTIFICATE分隔符。

  - SAML加密（可選）：可以通過加密從IdP到服務提供商的SAML響應來提高SAML身份驗證的安全性。若要在AppDynamics中加密SAML響應，需要配置身份提供程式(IdP)以加密SAML斷言，然後配置AppDynamics控制器以使用特定證書和私鑰進行解密。

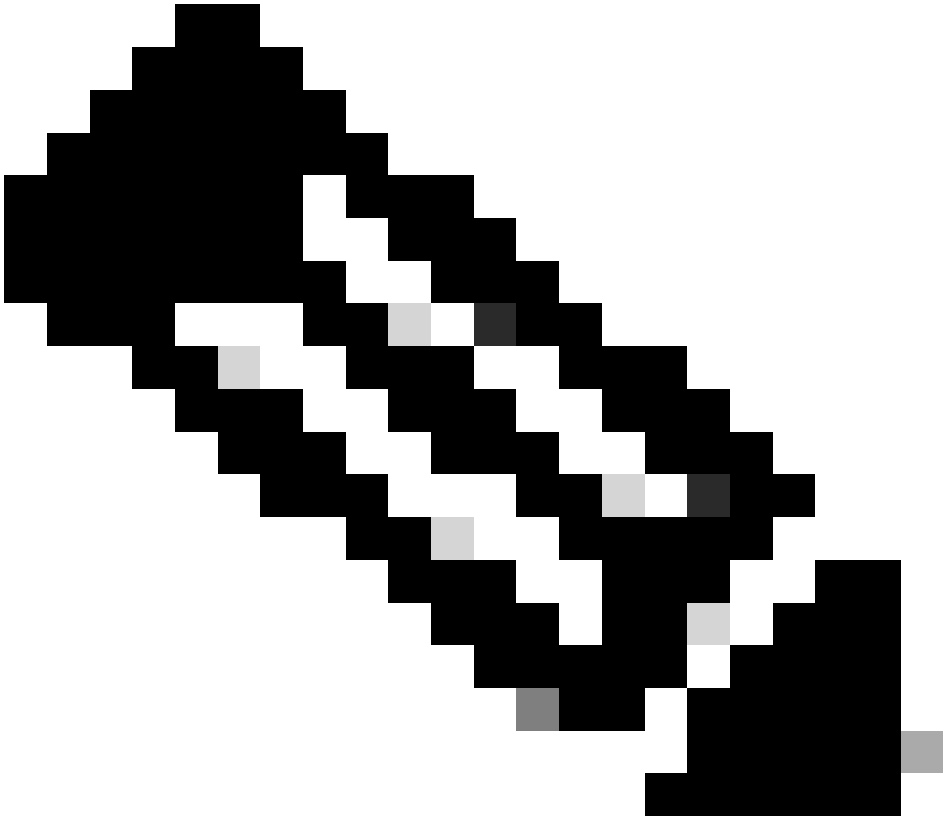


- 在「SAML屬性對映」部分中，對映SAML屬性(示例：使用者名稱、DisplayName和電子郵件)。



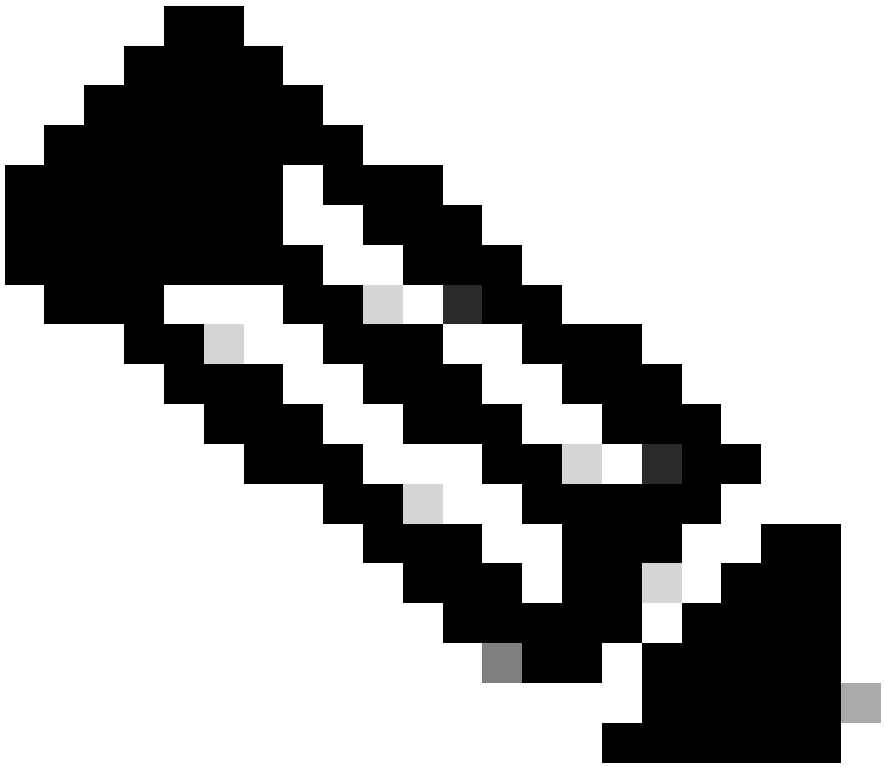
附註：AppDynamics顯示SAML使用者的使用者名稱、電子郵件和顯示名稱。預設情況下，它使用SAML響應中的NameID屬性來建立使用者名稱，該使用者名稱也用作displayName。可以通過在SAML響應中包括使用者名稱、電子郵件和顯示名稱屬性來自定義此行為。在AppDynamics中配置IdP設定時，使用者可以指定這些屬性名稱。在登入期間，AppDynamics將檢查是否配置了屬性對映。如果已配置對映且匹配屬性出現在SAML響應中，則AppDynamics使用這些屬性值設定使用者名稱、電子郵件和顯示名稱。

- 在「SAML組對映」部分中新增這些詳細資訊。
  - SAML組屬性名稱：輸入包含組資訊的SAML屬性的名稱。這通常為組、組或角色、角色或組成員身份。
  - 組屬性值：為組屬性選擇適當的值格式。 公共選項包括多個巢狀組值或單個值，具體取決於IdP如何構建組資訊。

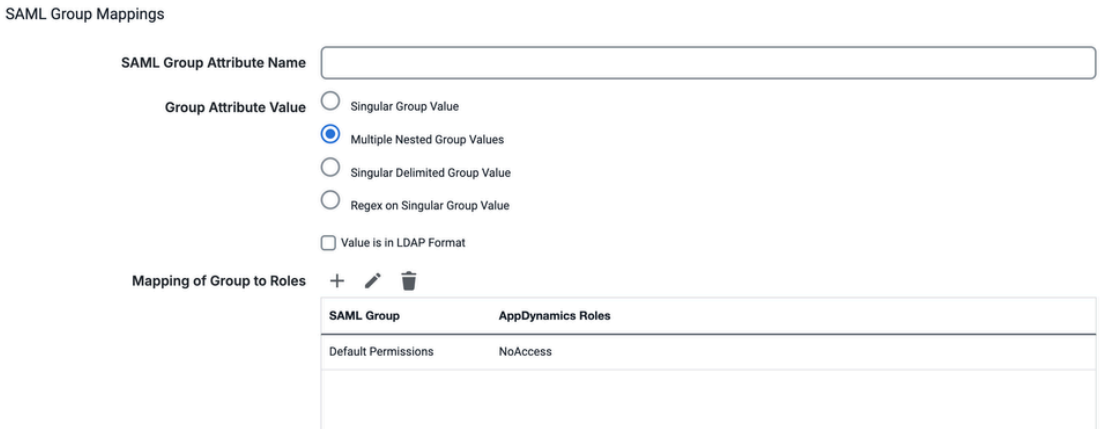


附註：如果組資訊採用LDAP（輕量目錄訪問協定）格式，則選擇Value is in LDAP Format。

- 將組對映到角色：按一下+按鈕以新增新對映。
  - SAML組：輸入要對映到AppDynamics角色的SAML組（在IdP中定義）的名稱。
  - 角色：從要分配給屬於SAML組的使用者的可用清單中選擇對應的AppDynamics角色。
  - 預設許可權：如果未配置SAML組對映或使用者SAML斷言未包含組資訊，則AppDynamics將回退到使用預設許可權。



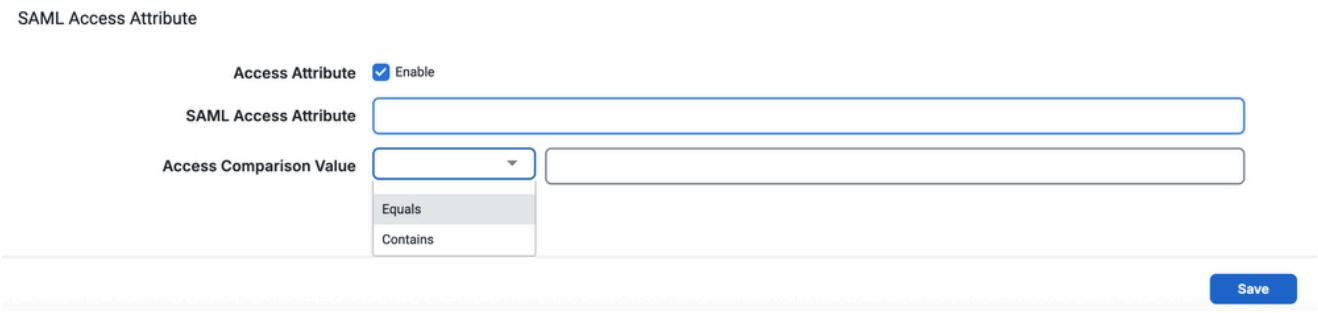
附註：建議為預設許可權分配具有最低許可權的角色。



- 在SAML Access Attribute部分，新增以下詳細資訊（可選）：
  - SAML訪問屬性：輸入SAML響應中屬性的名稱。這將用於訪問驗證。
  - 訪問比較值：有兩個可用選項：
    1. 等於：僅當SAML響應中的屬性值與配置中指定的值完全匹配時，才會授予訪問許

可權。
2. 包含：如果SAML響應中的屬性值包含配置中指定的值，則授予訪問許可權。
- 啟用後的工作方式：
1. AppDynamics從SAML響應檢索「SAML訪問屬性」欄位中指定的屬性。
2. 它將根據所選方法（相等或包含）比較屬性的值與使用者定義的訪問比較值。
3. 如果比較成功，則授予使用者訪問許可權。
4. 如果比較失敗，登入嘗試將被拒絕。

- 按一下「Save」（右下角）以儲存組態。



驗證

- 開啟瀏覽器並導航到AppDynamics Controller。系統將顯示第三方IdP服務的「登入」對話方塊。
- 按一下Log in with Single Sign-On。系統會將您重定向到IdP。
- 輸入並提交您的憑據。
- 成功進行身份驗證後，IdP會將您重定向到AppDynamics控制器。

常見問題和解決方案

400錯誤請求

- 問題：使用者在嘗試登入到AppDynamics Controller時遇到400錯誤請求錯誤。
- 示例錯誤：

```
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.
```

- 常見根本原因：
  - 無效的SAML證書
  - SAML響應大於最大長度
  - 實體ID或ACS URL無效
- 解決方案：
  - 無效的SAML證書

- 確保身份提供程式(IdP)提供的證書有效並且是最新的。
- 驗證IdP證書的到期日期。如果證書已過期，請從IdP獲取新證書。
- 如果在IdP端更新了證書，請確保在AppDynamics中上載並配置新證書。
- 在AppDynamics中更新證書的步驟：
  - 以帳戶所有者角色或具有管理、代理和入門嚮導許可權的角色身份登入到控制器UI。
  - 按一下您的使用者名稱（右上角）>管理>身份驗證提供程式>選擇SAML。
  - 在SAML Configuration部分中，找到certificate 欄位，然後將old certificate替換為IdP提供的新證書。
  - 按一下Save以更新SAML配置。

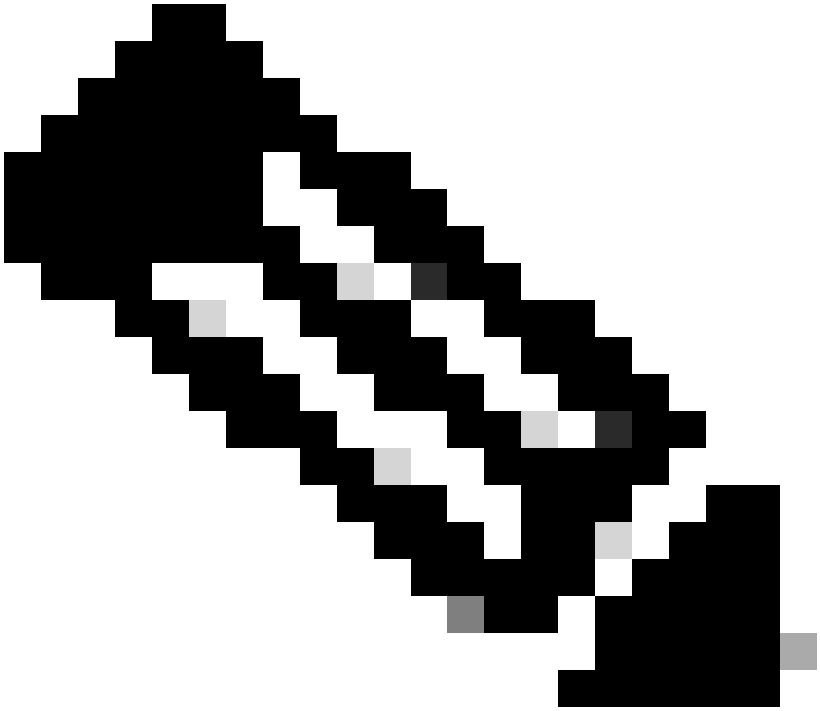
- SAML響應大於最大長度。
  - 從控制器版本23.11及更高版本開始，將控制器從GlassFish移動到Jetty Server時會出現此問題。在Jetty Server中，有一個名為 — Dorg.eclipse.jetty.server的屬性。Request.maxFormContentSize位於……/appserver/jetty/start.d/start.ini檔案。如果SAML響應大小超過為此屬性設定的值，則控制器將拒絕負載並返回400錯誤請求 錯誤。
  - 大型SAML響應的原因：
    - 屬性過多：SAML斷言中包含的屬性過多。
    - 簽名或加密的SAML響應：簽名或加密會增加響應大小。
    - 其他使用者或組資料：身份提供程式(IdP)具有額外的使用者或組資料。

  - 解決此問題的方法有兩種。通過實施其中一種或兩種解決方案，您可以解決問題並防止拒絕負載。
    1. 增加maxFormContentSize值
       - 對於內部控制器：更新中的 — Dorg.eclipse.jetty.server.Request.maxFormContentSize屬性 ……/appserver/jetty/start.d/start.ini檔案調至更大的值，然後重新啟動控制器。
       - 對於SaaS控制器：提交支援票證，以便支援團隊解決此問題。

    2. 最佳化SAML響應

       與您的身份提供方(IdP)合作，通過進行以下調整來減小SAML響應的大小：

       - 排除不必要的屬性：通過IdP配置從SAML斷言中刪除未使用或冗餘屬性。
       - 禁用加密（如果允許）：加密會增加SAML響應大小。如果已經通過HTTPS保護了連線，請考慮禁用加密以減小大小。
- 實體ID或ACS URL無效
  - 關於Idp:
    - 確認實體ID為https://your_controller_domain/controller。如果實體ID不同，請對其進行更新。
    - 確認ACS URL為https://your_controller_domain/controller/saml-auth?accountName=youraccountname。如果ACS URL不同，請相應地更新它。



附註：accountName必須與您的AppDynamics帳戶名稱匹配。（例如customer1）

- 缺少使用者許可權
  - 問題：您已成功登入到控制器。但是，您未收到所需的角色和許可權。
  - 配置和SAML響應示例：
    - 在SAML使用者的「組」屬性中，名稱為值為AppD_Admin和AppD_Power_User的「組」。

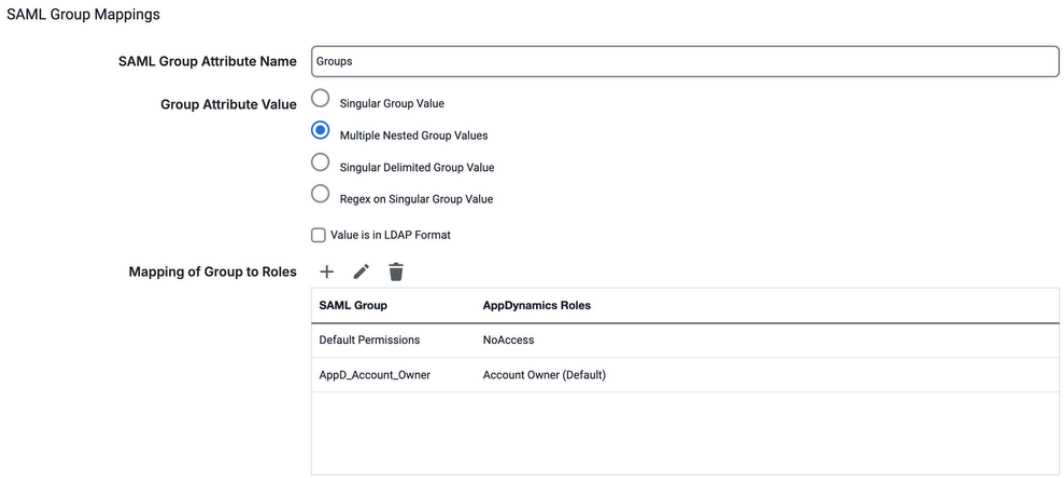
```
AppD_Admin
```

```
AppD_Power_User
```

- 在AppDynamics的「SAML組對映」部分中，配置了這些對映。
  - SAML組屬性名稱：組
  - 組屬性值：多個巢狀組值
  - 對映到組角色：

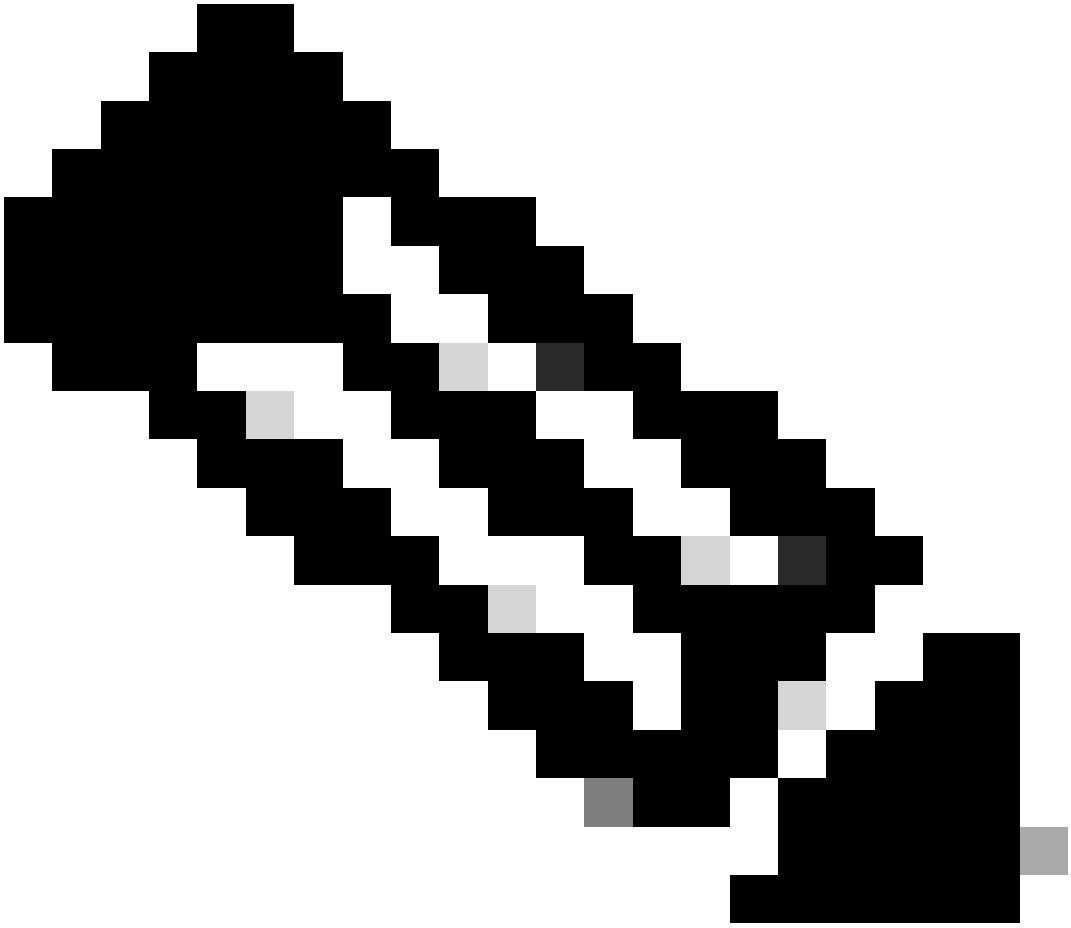
SAML組	AppDynamics角色
AppD_Account_Owner	帳戶所有者（預設）
預設許可權	無訪問許可權

No Access是沒有許可權的自定義角色。



- 常見問題和解決方案
  - 在SAML響應中找不到組屬性。
    - 來自IdP的SAML響應缺少必需的組屬性，或者在SAML響應中組的屬性名稱被設定為「角色」，而在AppDynamics中，它被配置為「組」。
    - 如果未提供組屬性，系統會自動為使用者分配與AppDynamics中的「預設許可權」關聯的角色。
    - 要解決此問題，請確保將IdP配置為在SAML響應中包括正確的組屬性，並且組的屬性名稱與AppDynamics中的配置匹配。

  - AppDynamics中未為SAML響應中提供的使用者組配置相應的SAML組對映。
    - 在SAML響應中，「組」屬性包含值AppD_Admin和AppD_Power_User。但是，在AppDynamics中，只有AppD_Account_Owner組的組對映存在。
    - 由於AppD_Admin或AppD_Power_User沒有對應的對映，因此沒有為使用者分配任何角色或許可權。
    - 要解決此問題，請在AppDynamics中新增缺少的組對映（例如AppD_Admin和AppD_Power_User），以確保正確的角色和許可權分配。



附註：只有當AppDynamics中配置的SAML組屬性名稱與SAML響應中的組屬性不同時，才會將預設許可權應用於SAML使用者。

- SAML使用者的電子郵件和/或名稱缺失或不正確
  - 問題：當AppDynamics中的屬性配置與SAML響應中的屬性不匹配時，通常會發生這種情況。
  - SAML響應示例：SAML響應中的屬性包括：User.email、User.fullName和Groups

```
FirstName LastName
```

```
AppD_Admin
```

```
AppD_Power_User
```

- AppDynamics中的SAML屬性對映示例
    - 使用者名稱屬性：User.name
    - 顯示名稱屬性：User.firstName或空白
    - 電子郵件屬性：User.userPrincipal或空白

- 根本原因：在AppDynamics中配置的顯示名稱和電子郵件屬性與SAML響應中提供的任何屬性都不匹配。
    - 因此：

        - 電子郵件設定為空白。
        - 顯示名稱預設為使用者名稱。

    - 解決方案：確保AppDynamics中配置的「顯示名稱」和「電子郵件」屬性與SAML響應中的相應屬性匹配。
        - 舉例來說：
            - 將「顯示名稱」屬性更新為User.fullName。
            - 將「電子郵件」屬性更新為User.email。

- HTTP 404錯誤

- 問題：使用者無法登入到控制器，並且出現404 not found錯誤。
- 示例錯誤：在控制器日誌中（僅適用於內部控制器），您會看到以下錯誤：

```
[#|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：當控制器資料庫中配置的控制器URL與用於登入的控制器URL或IdP上配置的URL不匹配時，通常會發生此錯誤
- 解決方案：
    - 對於內部控制器：
        - 運行此命令可更新控制器URL。（推薦）。

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

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

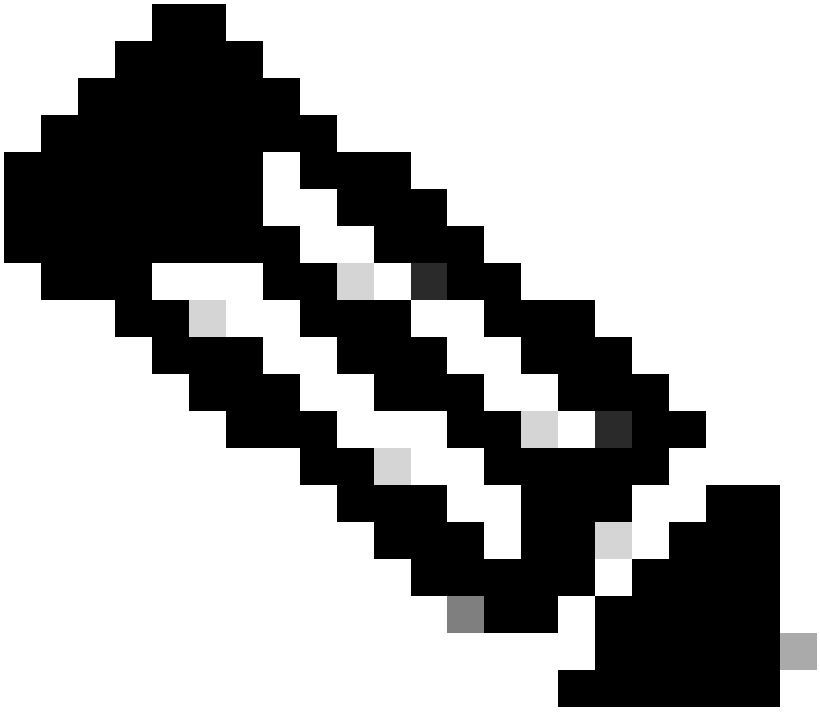
        - 或者，您也可以在控制器資料庫中運行這些命令以更新控制器URL。

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

```
' WHERE id=

;
UPDATE mds_auth.account SET controller_url='

' WHERE name='

';
```

- 運行此命令可獲取<ACCOUNT_ID>。

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

';
```



附註：如果仍然觀察到相同問題，請運行curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll。

- 替換：
  - <NEW_CONTROLLER_URL>，其中包含用於訪問控制器的實際控制器URL。
  - 控制器域中的<controller_domain>。
  - <youraccountname>和您的帳戶名。

- 對於SaaS控制器：提交支援票證，以便支援團隊解決此問題。

需要進一步協助

如果您遇到問題或遇到問題，請建立包含以下詳細信息的支援票證：

- 錯誤詳細資訊或螢幕快照：提供特定錯誤消息或問題的螢幕快照。
- SAML響應：收集SAML-Trace和HAR檔案
- Controller Server.log（僅限內部版本）：如果適用，請從<controller-install-dir>/logs/server.log提供控制器伺服器日誌

相關資訊

AppDynamics文檔

SAML for SaaS部署

加密SaaS部署的SAML響應

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。