Konfiguration und Problembehandlung bei einmaliger Anmeldung in AppDynamics

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie SSO (Single Sign On) in AppDynamics konfigurieren und Probleme beheben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Um die einmalige Anmeldung konfigurieren zu können, muss der Benutzer über die Rolle des Kontoinhabers (Standard) oder eine benutzerdefinierte Rolle mit der Berechtigung Administration, Agents, Getting Started Wizard (Assistenten für den Einstieg)verfügen.
- Administratorzugriff auf IhrIdPaccount.
- Die Metadaten oder Konfigurationsdetails aus AppDynamics (z. B. Entitäts-ID, ACS-URL).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AppDynamics-Controller

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Single Sign-On (SSO) ist ein Authentifizierungsmechanismus, mit dem sich Benutzer einmalig anmelden und auf mehrere Anwendungen, Systeme oder Services zugreifen können, ohne sich für jede Anwendung erneut authentifizieren zu müssen.

Die Security Assertion Markup Language (SAML) ist eine der Technologien zur Implementierung von SSO. Sie stellt das Framework und die Protokolle bereit, die SSO ermöglichen, indem Authentifizierungs- und Autorisierungsdaten sicher zwischen einem Identity Provider (IdP) und einem Service Provider (SP) ausgetauscht werden.

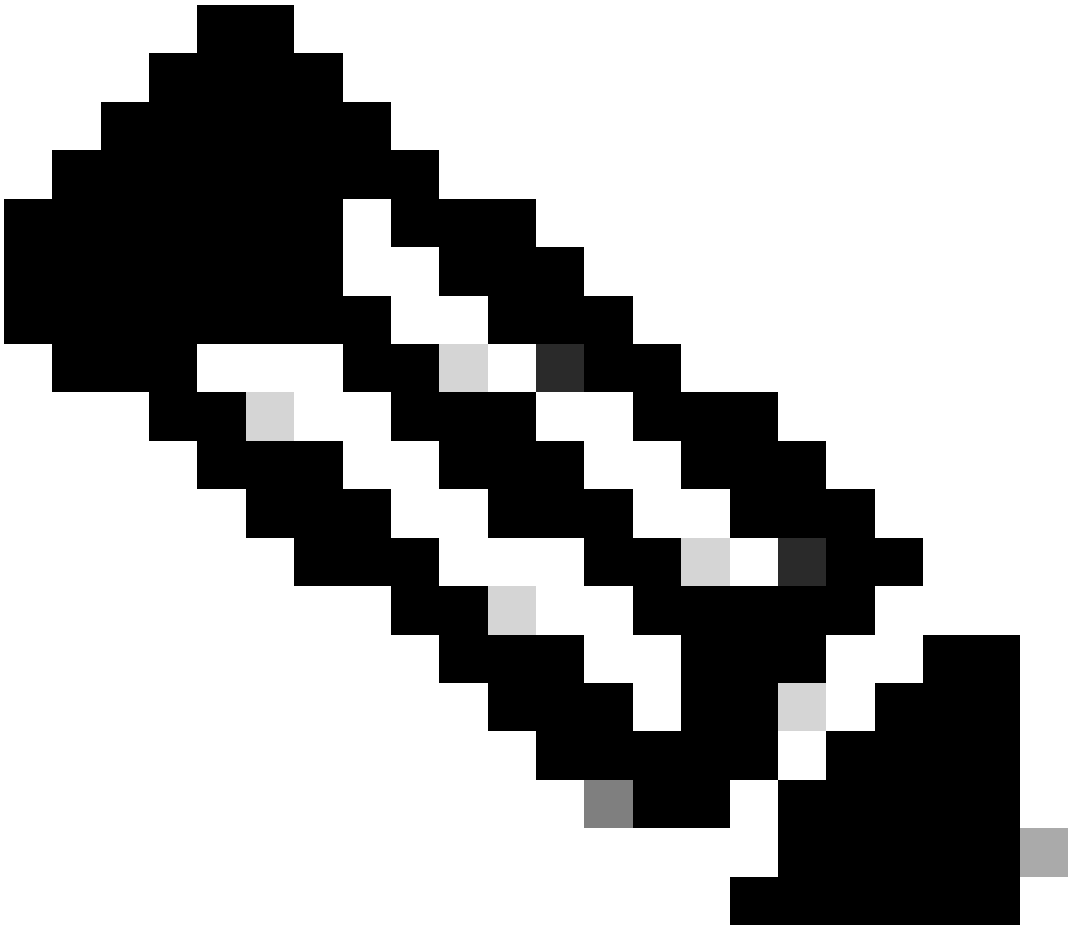
SAML-Assertion

- Der XML-basierte Nachrichtenaustausch zwischen IdP und SP.
- Es gibt drei Arten von Assertionen:
  - Authentifizierungsbestätigungen: Bestätigt die Authentifizierung des Benutzers.
  - Attribut-Assertionen: Gibt Benutzerattribute wie den Benutzernamen oder die Rollen frei.
  - Bestätigung der Autorisierungsentscheidung: Gibt an, wozu der Benutzer autorisiert ist.

Schlüsselrollen in SAML

- Identitätsanbieter (IdP)
  - Überprüft die Identität des Benutzers.
  - Generieren Sie die SAML Assertion, die Identifikationsinformationen des Benutzers enthält.
- Service Provider
  - Die Anwendung oder das System, auf die bzw. das der Benutzer zugreifen möchte.
  - Der Benutzer wird durch den IdP authentifiziert.
  - Akzeptiert die SAML-Assertion, um dem Benutzer Zugriff auf seine Ressourcen oder Anwendungen zu gewähren.
- Benutzer (Principal)
  - Der Benutzer, der die Anforderung initiiert oder versucht, vom Dienstanbieter auf eine Ressource zuzugreifen.

- Interaktion mit dem IdP (Authentifizierung) und dem SP.



Anmerkung: AppDynamics unterstützt sowohl vom IdP initiierte als auch vom SP initiierte SSO.

Vom SP initiierter Fluss:

- Der Benutzer navigiert zum Dienstanbieter, indem er die URL der Anwendung (z. B. AppDynamics) eingibt oder auf einen Link klickt.
- Der SP sucht nach einer vorhandenen Sitzung. Wenn keine Sitzung besteht, erkennt der SP, dass der Benutzer nicht authentifiziert ist, und initiiert den SSO-Prozess.
- Der SP generiert eine SAML-Authentifizierungsanforderung und leitet den Benutzer zur Authentifizierung an den IdP weiter.
    - Diese Anfrage umfasst:
        - Entitäts-ID: Eindeutige Kennung des Dienstanbieters.
        - Assertion Consumer Service (ACS)-URL: wobei IdP die SAML Assertion nach der Authentifizierung sendet.

    - Metadaten über den SP und Sicherheitsdetails (z. B. signierte Anforderung, Verschlüsselungsanforderungen).
- Der Benutzer wird zur IdP-Anmeldeseite weitergeleitet.
- Der IdP authentifiziert den Benutzer (z. B. über Benutzername/Kennwort oder Multi-Faktor-Authentifizierung).
- Nach erfolgreicher Authentifizierung generiert das IdP eine SAML Assertion (Sicherheitstoken).
- Die SAML Assertion wird über den Benutzerbrowser mit HTTP POST Binding (in den meisten Fällen) oder HTTP Redirect Binding zurück an den SP gesendet.
- Der SP validiert die SAML Assertion, um Folgendes sicherzustellen:
    - Sie wurde von der vertrauenswürdigen IDp ausgegeben.
    - Sie wird an den SP adressiert (über die SP Entity ID).
    - Sie ist nicht abgelaufen oder wurde manipuliert (mithilfe des öffentlichen IdP-Schlüssels validiert).

- Wenn die SAML Assertion gültig ist, erstellt der SP eine Sitzung für den Benutzer.
- Dem Benutzer wird der Zugriff auf die Anwendung oder Ressourcen gewährt.

Von IdP initiierter Fluss:

- Der Benutzer navigiert zum IdP-Anmeldeportal und gibt seine Anmeldeinformationen ein.
- Der IdP authentifiziert den Benutzer (z. B. mit einer Kombination aus Benutzername und Kennwort, mehrstufige Authentifizierung).
- Nach der Authentifizierung erhält der Benutzer durch die IdP eine Liste der verfügbaren Anwendungen oder Dienste (SPs), auf die er zugreifen kann.
- Der Benutzer wählt den gewünschten SP aus (z. B. AppDynamics).
- Der IdP generiert eine SAML Assertion für den ausgewählten SP.

- Der IdP leitet den Benutzer an die ACS-URL (SP Assertion Consumer Service) weiter und sendet die SAML Assertion mit (unter Verwendung von HTTP POST Binding oder HTTP Redirect Binding).
- Der SP erhält die SAML Assertion und validiert sie:
    - Stellt sicher, dass die Assertion von einer vertrauenswürdigen IDp ausgegeben wird.
    - Überprüft die Assertionsintegrität und den Ablauf.
    - Bestätigt die Benutzeridentität und andere Attribute.

- Wenn die SAML Assertion gültig ist, erstellt der SP eine Sitzung für den Benutzer.
- Dem Benutzer wird der Zugriff auf die Anwendung oder Ressourcen gewährt.

Konfigurieren

Der AppDynamics Controller kann die Cisco-Kundenidentität oder einen externen SAML-Identitätsanbieter (IdP) verwenden, um Benutzer zu authentifizieren und zu autorisieren.

Unterstützte Identitätsanbieter

AppDynamiczertifiziert die Unterstützung dieser Identitätsanbieter (IdPs):

- Okta
- Onelogin
- Ping-Identität
- Azure AD
- IBM Cloud-Identität
- Active Directory-Verbunddienst (AD FS)

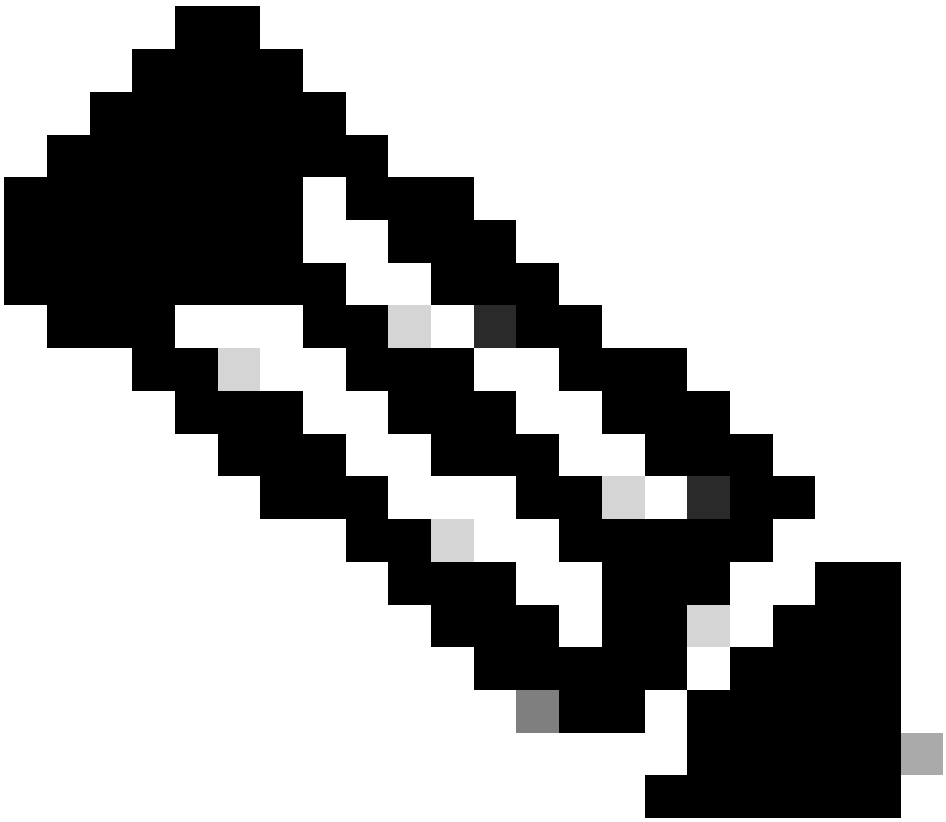
Andere IdPs, die HTTP POST-Bindungen unterstützen, sind ebenfalls mit der AppDynamics SAML-Authentifizierung kompatibel.

Schritte zum Konfigurieren von SAML in AppDynamics

Schritt 1. Erfassen der AppDynamics-Controller-Details

- Element-ID (SP-Element-ID): Eine eindeutige Kennung für AppDynamics (z. B. https://<Controller-Host>:<Port>/Controller).
  - Syntax: https://<Controller_Domain>/Controller
  - beispiel: https://<Ihr_Controller_Domäne>/Controller

- Antwort-URL (Assertion Consumer Service, ACS-URL): Der Endpunkt auf dem Dienstanbieter (z. B. AppDynamics), an den die IdP die SAML-Antwort nach der Authentifizierung sendet.
  - Syntax: https://<Controller_Domain>/controller/saml-auth?accountName=<Account_Name>
  - Beispiel: https://your_controller_domain/controller/saml-auth?accountName=youraccountname



Anmerkung: Im Fall eines Vor-Ort-Controllers lautet der Standardkontoname customer1, es sei denn, Sie haben einen Multi-Tenant-Controller mit einem anderen accountName.

- Single Logout URL (Optional): Der Endpunkt auf dem SP, der SAML-Abmeldeanforderungen verarbeitet (z. B. https://<controller_domain>/controller).

Schritt 2: Erstellen einer neuen Anwendung in IdP und Herunterladen der Metadaten

- Suchen Sie den Bereich für die Anwendungserstellung: Dieser Bereich befindet sich normalerweise in der IdP-Verwaltungskonsole oder im Dashboard und wird oft als Anwendungen, Web- und mobile Apps, Unternehmensanwendungen oder vertrauende Parteien bezeichnet.
- Hinzufügen einer benutzerdefinierten oder generischen SAML-Anwendung: Wählen Sie eine Option aus, mit der Sie eine benutzerdefinierte SAML-Anwendung oder eine generische SAML-Dienstanbieter-Integration konfigurieren können.
- Geben Sie Anwendungsdetails an: Geben Sie einen Namen für die Anwendung ein, und laden Sie möglicherweise ein Symbol zur Identifizierung hoch (optional).
- Fügen Sie Attributzuordnungen (Benutzername, displayName, E-Mail oder Rollen) hinzu, um Benutzerinformationen an AppDynamics zu übergeben.
- Laden Sie die IdP-Metadatendatei herunter, oder notieren Sie sich diese Details:

- IDp-Anmelde-URL
- Abmelde-URL
- Attributnamen
- Zertifikat

Schritt 3: Konfigurieren der SAML-Authentifizierung im AppDynamics-Controller

- Melden Sie sich bei der Benutzeroberfläche des Controllers als Kontoinhaberrolle oder als Rolle mit der Berechtigung Administration, Agents, Getting Started Wizard (Assistenten für den Einstieg)an.
- Klicken Sie auf Ihren Benutzernamen (obere rechte Ecke)> Administration > Authentication Provider > Select SAML.

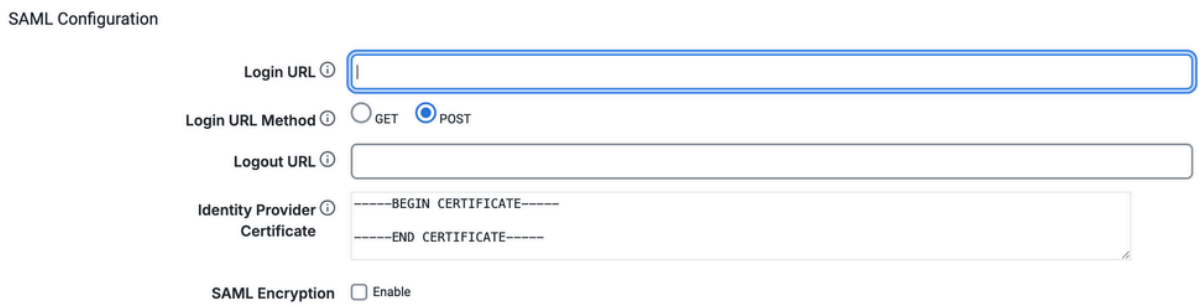
- Fügen Sie im Abschnitt "SAML Configuration" folgende Details hinzu:

  - Anmelde-URL: Die IDp-Anmelde-URL, über die der AppDynamics-Controller vom Dienstanbieter (SP) initiierte Anmeldeanforderungen weiterleitet.

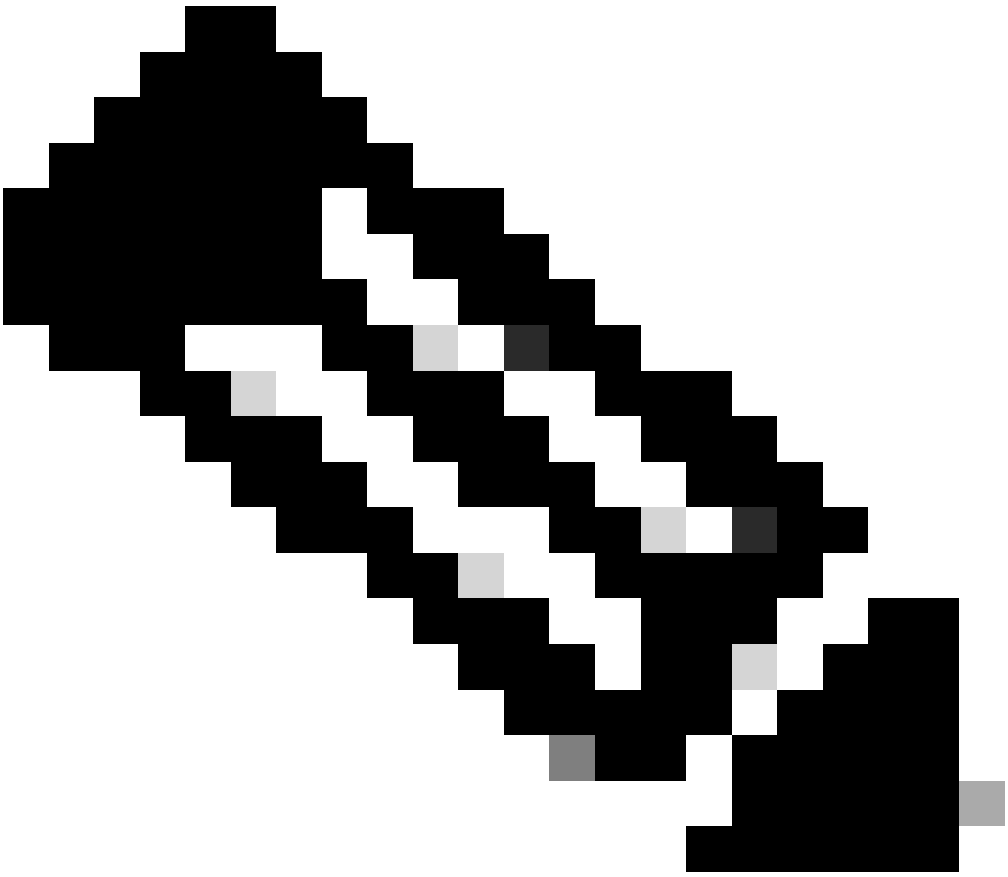
  - Abmelde-URL (optional): Die URL, an die der AppDynamics Controller Benutzer umleitet, nachdem sie sich abgemeldet haben. Wenn Sie keine Abmelde-URL angeben, erhalten Benutzer den AppDynamics-Anmeldebildschirm, wenn sie sich abmelden.

  - Zertifikat: Das X.509-Zertifikat von IdP. Fügen Sie das Zertifikat zwischen die Trennzeichen BEGIN CERTIFICATE und END CERTIFICATE ein. Vermeiden Sie das Duplizieren der Trennzeichen BEGIN CERTIFICATE und END CERTIFICATE aus dem Quellzertifikat.

  - SAML-Verschlüsselung (optional): Sie können die Sicherheit der SAML-Authentifizierung verbessern, indem Sie die SAML-Antwort von IdP an den Dienstanbieter verschlüsseln. Um SAML-Antworten in AppDynamics zu verschlüsseln, müssen Sie Ihren Identity Provider (IdP) so konfigurieren, dass er die SAML-Assertion verschlüsselt, und anschließend den AppDynamics Controller so konfigurieren, dass er ein bestimmtes Zertifikat und einen privaten Schlüssel für die Entschlüsselung verwendet.



- Ordnen Sie im Abschnitt "SAML Attribute Mappings" die SAML-Attribute zu (Beispiel: Benutzername, DisplayName, E-Mail) an die entsprechenden Felder in AppDynamics senden.

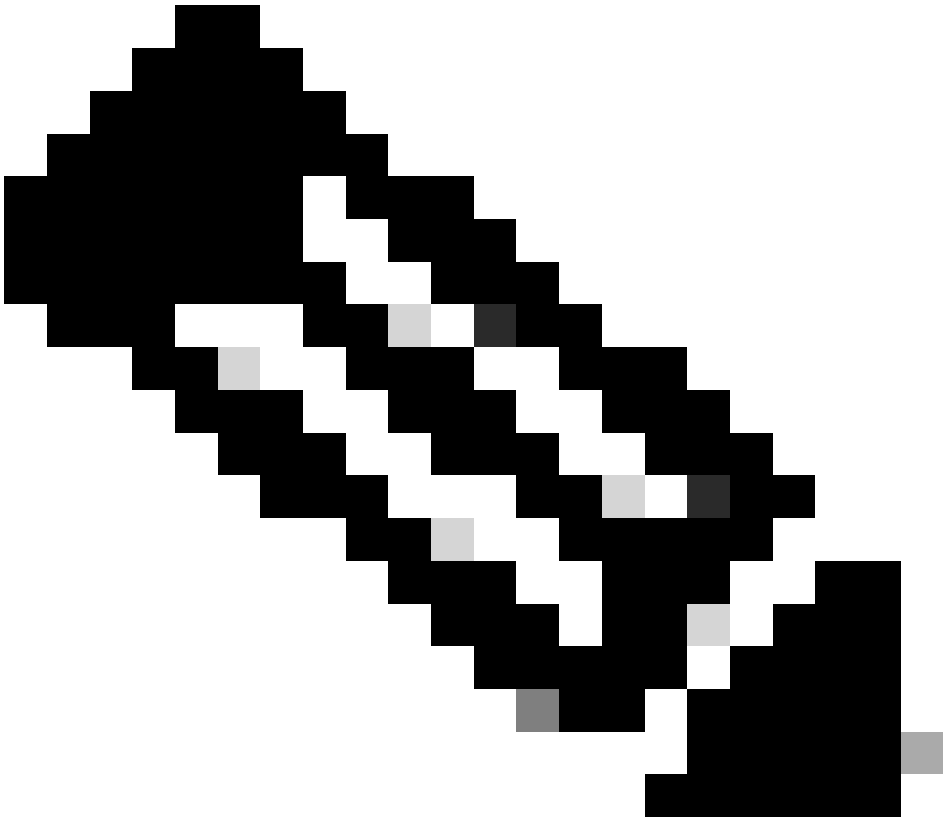


Anmerkung: AppDynamics zeigt den Benutzernamen, die E-Mail und den Anzeigenamen eines SAML-Benutzers an. Standardmäßig wird das NameID-Attribut aus der SAML-Antwort verwendet, um einen Benutzernamen zu erstellen, der auch als displayName verwendet wird. Dieses Verhalten kann angepasst werden, indem die Attribute "Benutzername", "E-Mail" und "Anzeigename" in die SAML-Antwort aufgenommen werden. Beim Konfigurieren der IdP-Einstellungen in AppDynamics kann der Benutzer diese Attributnamen angeben. Während der Anmeldung überprüft AppDynamics, ob die Attributzuordnung konfiguriert ist. Wenn Zuordnungen konfiguriert sind und übereinstimmende Attribute in der SAML-Antwort vorhanden sind, verwendet AppDynamics diese Attributwerte, um den Benutzernamen, die E-Mail-Adresse und den Anzeigenamen festzulegen.

- Fügen Sie im Abschnitt "SAML Group Mappings" (SAML-Gruppenzuordnungen) diese

Details hinzu.

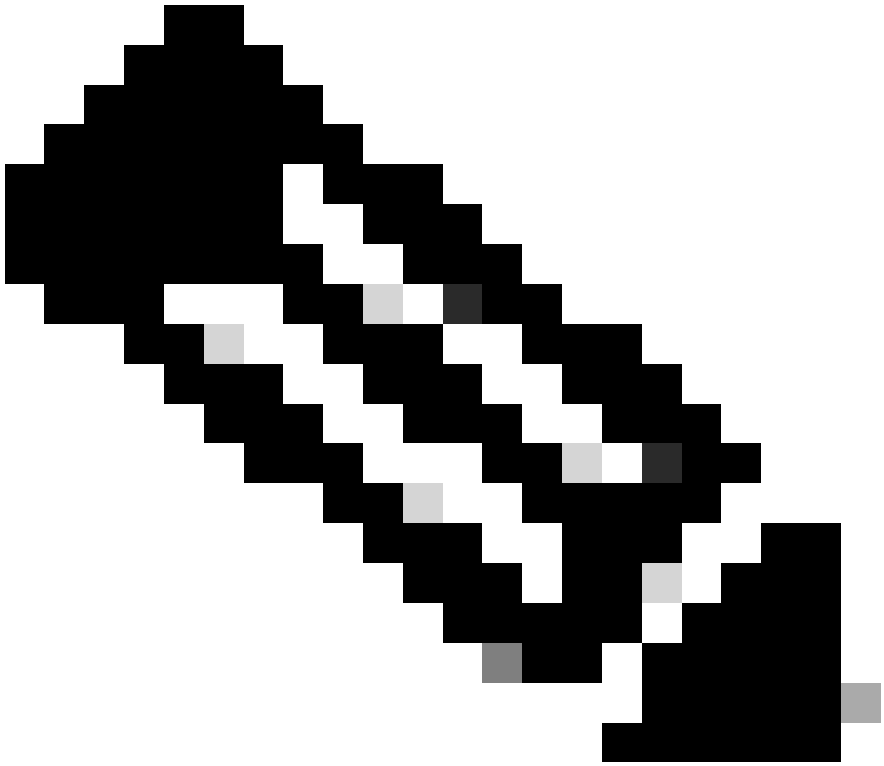
- SAML-Gruppenattribut-Name: Geben Sie den Namen des SAML-Attributs ein, das die Gruppeninformationen enthält. Dies sind in der Regel Gruppen oder Gruppen oder Rollen oder Rollen oder Rollen oder Gruppenmitgliedschaften.
- Gruppenattributwert: Wählen Sie das entsprechende Wertformat für das Gruppenattribut aus. Zu den allgemeinen Optionen gehören Multiple Nested Group Values (Mehrere verschachtelte Gruppenwerte) oder Single Value (Einzelwert), je nachdem, wie Ihre IdP die Gruppeninformationen strukturiert.



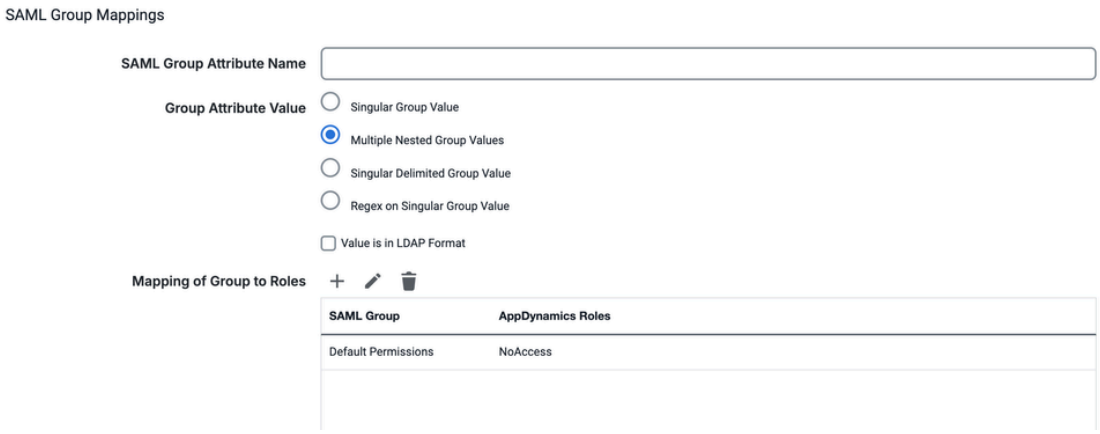
Anmerkung: Wählen Sie Value is in LDAP Format aus, wenn die Gruppeninformationen im LDAP-Format (Lightweight Directory Access Protocol) vorliegen.

- Zuordnung von Gruppen zu Rollen: Klicken Sie auf die +-Schaltfläche, um eine neue Zuordnung hinzuzufügen.
  - SAML Group (SAML-Gruppe): Geben Sie den Namen der SAML-Gruppe (wie in Ihrer IdP definiert) ein, die Sie einer AppDynamics-Rolle zuordnen möchten.
  - Rolle(n): Wählen Sie die entsprechende(n) AppDynamics-Rolle(n) aus der verfügbaren Liste aus, die Sie Benutzern zuweisen möchten, die zur SAML-Gruppe gehören.
  - Standardberechtigungen: Wenn die SAML-Gruppenzuordnung nicht konfiguriert

ist oder eine SAML-Assertion des Benutzers keine Gruppeninformationen enthält, greift AppDynamics auf die Verwendung von Standardberechtigungen zurück.



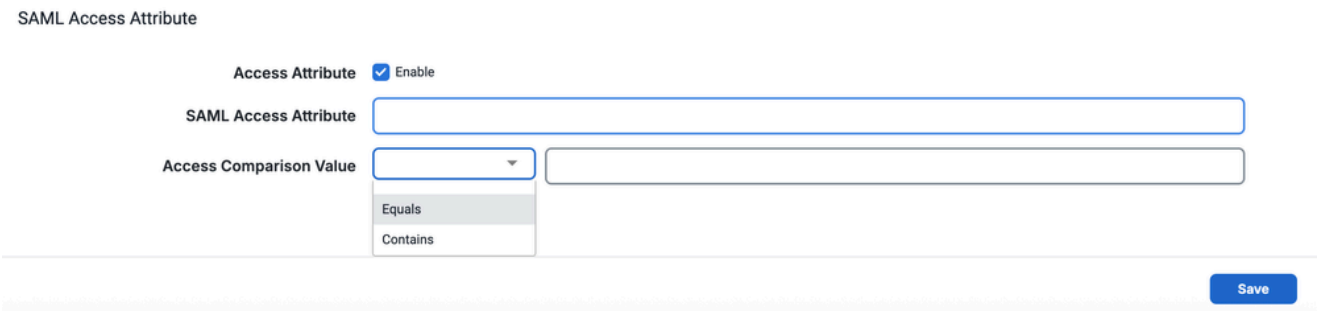
Anmerkung: Es wird empfohlen, Standardberechtigungen eine Rolle mit Mindestberechtigungen zuzuweisen.



- Fügen Sie im Abschnitt SAML Access Attribute folgende Details hinzu (optional):

- SAML-Zugriffsattribut: Geben Sie den Namen der Attribute aus der SAML-Antwort ein. Dies wird für die Zugriffsvalidierung verwendet.
- Wert des Zugriffsvergleichs: Es stehen zwei Optionen zur Verfügung:
    1. Gleich: Der Zugriff wird nur gewährt, wenn der Attributwert in der SAML-Antwort genau mit dem in der Konfiguration angegebenen Wert übereinstimmt.
    2. Enthält: Der Zugriff wird gewährt, wenn der Attributwert in der SAML-Antwort den in der Konfiguration angegebenen Wert enthält.
- Funktionsweise bei Aktivierung:
    1. AppDynamics ruft das im Feld SAML-Zugriffsattribut angegebene Attribut aus der SAML-Antwort ab.
    2. Es vergleicht den Wert des Attributs mit dem benutzerdefinierten Zugriffsvergleichswert, der auf der ausgewählten Methode (Equal oder Contains) basiert.
    3. Wenn der Vergleich erfolgreich ist, erhält der Benutzer Zugriff.
    4. Wenn der Vergleich fehlschlägt, wird die Anmeldung abgelehnt.

- Klicken Sie auf Speichern (untere rechte Ecke), um die Konfiguration zu speichern.



Überprüfung

- Öffnen Sie einen Browser, und navigieren Sie zu AppDynamics Controller. Der Anmeldedialog für Ihren IdP-Dienst eines Drittanbieters wird angezeigt.
- Klicken Sie auf Bei einmaliger Anmeldung anmelden. Das System leitet Sie zu Ihrem IdP um.
- Geben Sie Ihre Anmeldeinformationen ein, und übermitteln Sie sie.
- Nach erfolgreicher Authentifizierung werden Sie von IdP an Ihren AppDynamics-Controller umgeleitet.

Häufige Probleme und Lösung

400 Ungültige Anforderung

- Problem: Benutzer haben beim Versuch, sich bei AppDynamics Controller anzumelden, einen Fehler von 400 fehlerhaften Anforderungen festgestellt.
- Beispielfehler:

```
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.
```

- Häufige Ursachen:
  - Ungültiges SAML-Zertifikat
  - SAML-Antwort ist größer als die maximale Länge
  - Ungültige Element-ID oder ACS-URL
- Lösung:
  - Ungültiges SAML-Zertifikat
    - Stellen Sie sicher, dass das vom Identitätsanbieter (IdP) bereitgestellte Zertifikat gültig und aktuell ist.
    - Überprüfen Sie das Ablaufdatum des IdP-Zertifikats. Wenn es abgelaufen ist, holen Sie sich ein neues Zertifikat von der IdP.
    - Wenn das Zertifikat auf der IdP-Seite aktualisiert wurde, stellen Sie sicher, dass das neue Zertifikat in AppDynamics hochgeladen und konfiguriert wurde.
    - Schritte zum Aktualisieren des Zertifikats in AppDynamics:
      - Melden Sie sich bei der Benutzeroberfläche des Controllers als Kontoinhaberrolle oder als Rolle mit der Berechtigung Administration, Agents, Getting Started Wizard (Assistenten für den Einstieg) an.
      - Klicken Sie auf Ihren Benutzernamen (obere rechte Ecke)> Administration > Authentication Provider > Select SAML.
      - Suchen Sie im Abschnitt "SAML Configuration" das Feld Certificate, und ersetzen Sie das alte Zertifikat durch das neue, von der IdP bereitgestellte Zertifikat.
      - Klicken Sie auf Speichern, um die SAML-Konfiguration zu aktualisieren.
  - Die SAML-Antwort ist größer als die maximale Länge.
    - Dieses Problem tritt auf, wenn der Controller von GlassFish auf Jetty Server umgestellt wird, beginnend mit Controller Version 23.11 und höher. In Jetty Server gibt es eine Eigenschaft mit dem Namen -Dorg.eclipse.jetty.server. Request.maxFormContentSize befindet sich in der .../appserver/jetty/start.d/start.ini. Wenn die SAML-Antwortgröße den für diese Eigenschaft festgelegten Wert überschreitet, lehnt der Controller die Payload ab und gibt eine 400-mal fehlerhafte Anforderung zurück. fehler.
    - Ursachen für große SAML-Reaktionen:
      - Übermäßige Attribute: Zu viele Attribute in der SAML-Assertion.
      - Signierte oder verschlüsselte SAML-Antworten: Durch Signierung oder Verschlüsselung wird die Antwortgröße erhöht.
      - Zusätzliche Benutzer- oder Gruppendaten: Der Identitätsanbieter (IdP) verfügt über zusätzliche Benutzer- oder Gruppendaten.
    - Es gibt zwei Möglichkeiten, dieses Problem zu beheben. Durch Implementieren einer oder beider Lösungen können Sie das Problem beheben und verhindern, dass die Nutzlast abgelehnt wird.

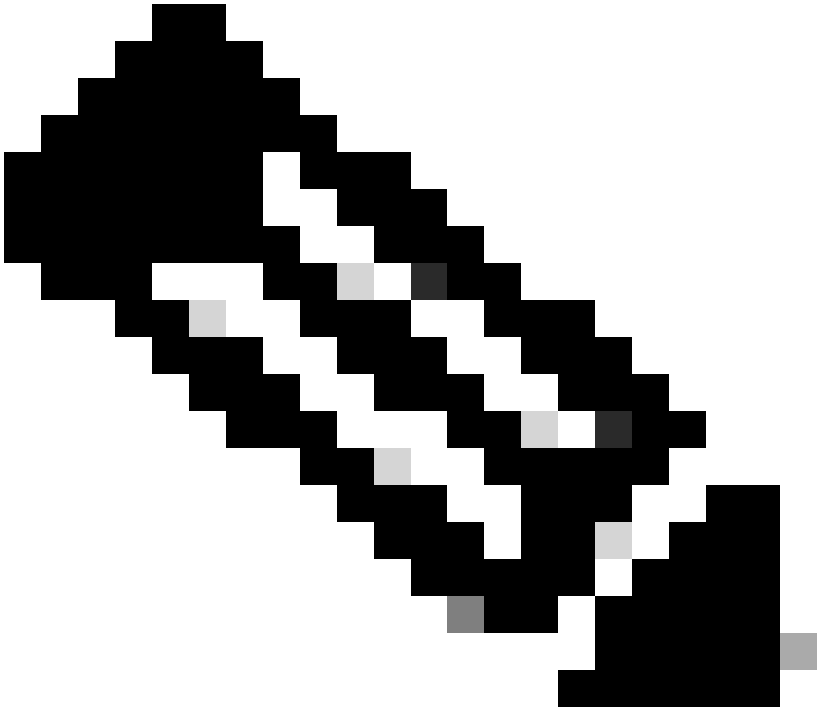
1. Erhöhen Sie den maxFormContentSize-Wert
    - Für Controller am Standort: Aktualisieren Sie die -Dorg.eclipse.jetty.server.Request.maxFormContentSize-Eigenschaft in der .../appserver/jetty/start.d/start.ini auf einen größeren Wert setzen und den Controller neu starten.
    - Für SaaS-Controller: Senden Sie ein Support-Ticket, um dieses Problem vom Support-Team beheben zu lassen.

2. Optimierung der SAML-Reaktion

    Arbeiten Sie mit Ihrem Identitätsanbieter (IdP) zusammen, um die Größe der SAML-Antwort zu reduzieren, indem Sie folgende Anpassungen vornehmen:

    - Unnötige Attribute ausschließen: Entfernen Sie nicht verwendete oder redundante Attribute aus der SAML Assertion über die IdP-Konfiguration.
    - Verschlüsselung deaktivieren (falls zulässig): Die Verschlüsselung erhöht die SAML-Antwortgröße. Wenn die Verbindung bereits über HTTPS gesichert ist, sollten Sie die Verschlüsselung deaktivieren, um die Größe zu reduzieren.

- Ungültige Element-ID oder ACS-URL
    - Über die IDP:
        - Bestätigen Sie, dass die Objektkennung https://your_controller_domain/controller lautet. Wenn sich die Objektkennung unterscheidet, aktualisieren Sie sie.
        - Bestätigen Sie, dass die ACS-URL https://your_controller_domain/controller/saml-auth?accountName=youraccountname lautet. Wenn die ACS-URL anders ist, aktualisieren Sie sie entsprechend.



Anmerkung: accountName muss mit Ihrem AppDynamics-Kontonamen übereinstimmen. (z. B. customer1)

- Fehlende Benutzerberechtigungen
  - Problem: Sie haben sich erfolgreich beim Controller angemeldet. Sie haben jedoch nicht die beabsichtigten Rollen und Berechtigungen erhalten.
  - Beispielkonfiguration und SAML-Antwort:
    - Im SAML-Benutzer das Group-Attribut lautet der Name Groups mit den Werten AppD_Admin & AppD_Power_User.

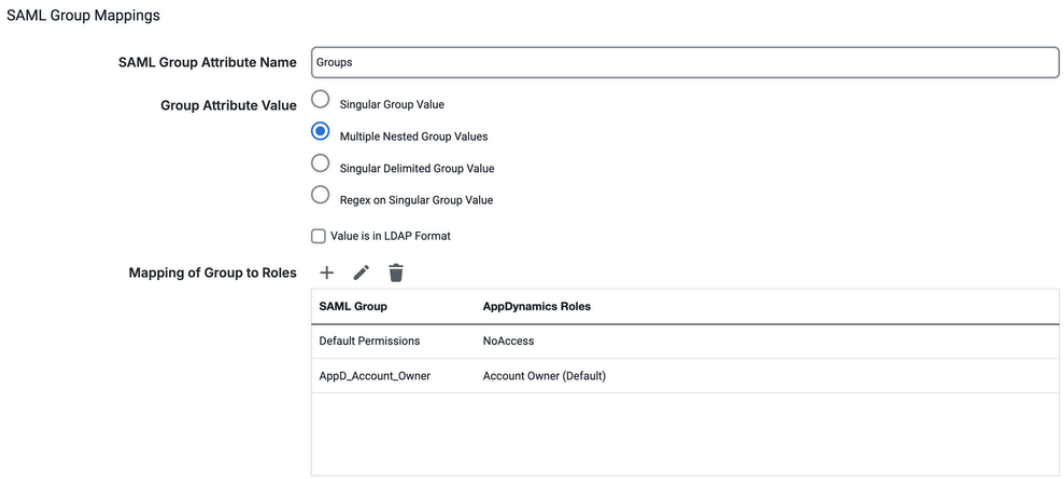
```
AppD_Admin
```

```
AppD_Power_User
```

- In AppDynamics werden diese im Abschnitt SAML-Gruppenzuordnungen konfiguriert.
  - Attributname der SAML-Gruppe: Gruppen
  - Gruppenattributwert: Mehrere verschachtelte Gruppenwerte
  - Zuordnung zu Gruppenrollen:

SAML-Gruppe	AppDynamics-Rollen
AppD_Account_Owner	Kontoinhaber (Standard)
Standardberechtigungen	Kein Zugriff

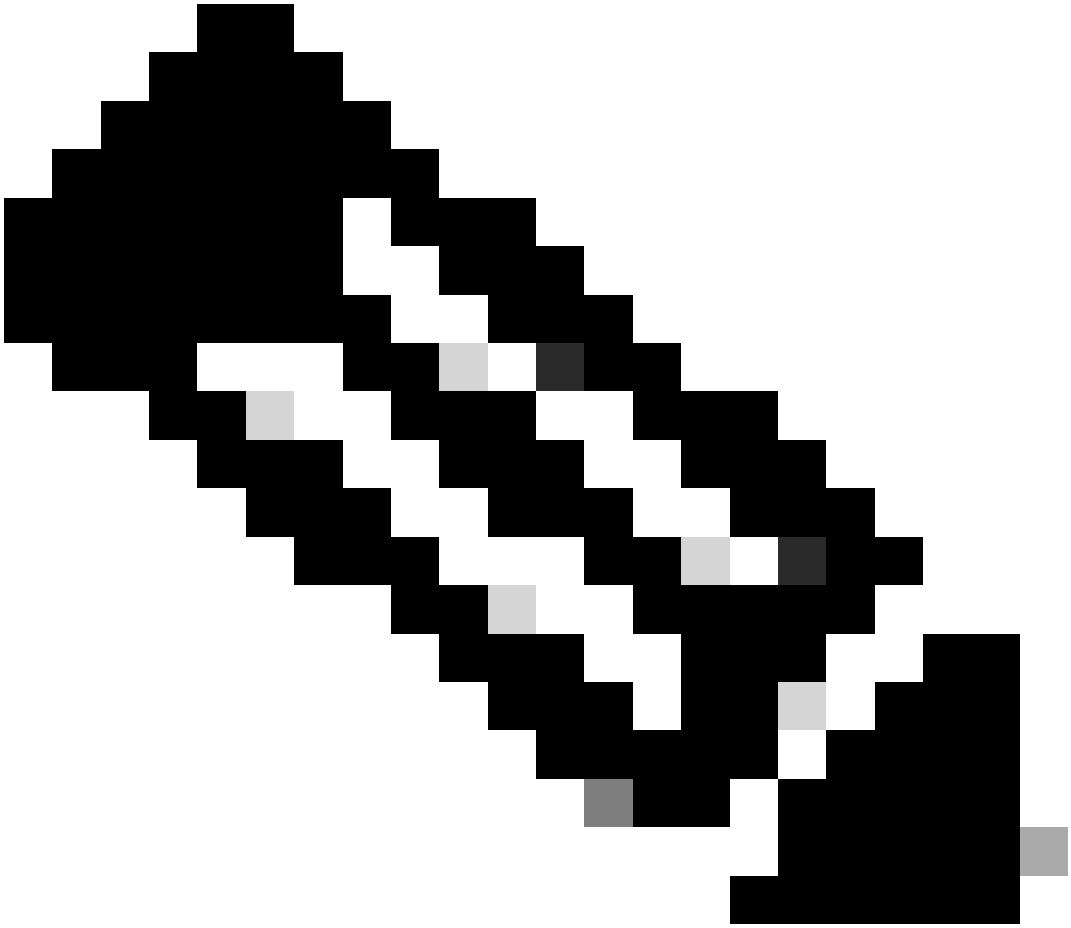
No Access ist eine benutzerdefinierte Rolle ohne Berechtigungen.



- Häufige Probleme und Lösungen
  - In der SAML-Antwort wurden keine Gruppenattribute gefunden.
    - In der SAML-Antwort von IdP fehlen die erforderlichen Gruppenattribute, oder der Attributname für Gruppen in der SAML-Antwort wird als Roles festgelegt, während er in AppDynamics als Groups konfiguriert ist.
    - Wenn keine Gruppenattribute angegeben werden, werden dem Benutzer automatisch die Rollen zugewiesen, die den Standardberechtigungen in AppDynamics zugeordnet sind.
    - Um dies zu beheben, stellen Sie sicher, dass IdP so konfiguriert ist, dass es die richtigen Gruppenattribute in die SAML-Antwort einbezieht, und dass der Attributname für Gruppen mit der Konfiguration in AppDynamics übereinstimmt.

  - In AppDynamics ist keine entsprechende SAML-Gruppenzuordnung für die in der SAML-Antwort angegebenen Benutzergruppen konfiguriert.
    - In der SAML-Antwort enthält das Groups-Attribut die Werte AppD_Admin

und AppD_Power_User. In AppDynamics sind Gruppenzuordnungen jedoch nur für die Gruppe AppD_Account_Owner vorhanden.
    - Da es keine entsprechende Zuordnung für AppD_Admin oder AppD_Power_User gibt, werden dem Benutzer keine Rollen oder Berechtigungen zugewiesen.
    - Fügen Sie zum Beheben dieses Problems die fehlenden Gruppenzuordnungen (z. B. AppD_Admin und AppD_Power_User) in AppDynamics hinzu, um die korrekte Rollen- und Berechtigungszuweisung sicherzustellen.



Anmerkung: Standardberechtigungen werden nur auf die SAML-Benutzer angewendet, wenn der in AppDynamics konfigurierte SAML-Gruppenattributname nicht mit den Gruppenattributen in der SAML-Antwort übereinstimmt.

- Fehlende oder falsche E-Mail und/oder Name für SAML-Benutzer

- Problem: Dies geschieht in der Regel, wenn die Attributkonfiguration in AppDynamics nicht mit den Attributen übereinstimmt, die in der SAML-Antwort eingehen.
- SAML-Beispielantwort: Attribute In der SAML-Antwort sind: User.email, User.fullName und Gruppen

```
example@domain.com
```

```
FirstName LastName
```

```
AppD_Admin
```

```
AppD_Power_User
```

- Beispiel für SAML-Attributzuordnungen in AppDynamics

        - Benutzername-Attribut: Benutzername
        - Anzeigenamenattribut: User.firstName oder leer
        - E-Mail-Attribut User.userPrincipal oder leer

    - Ursache: Die in AppDynamics konfigurierten Attribute "Anzeigename" und "E-Mail" stimmen mit keinem der in der SAML-Antwort angegebenen Attribute überein.
        - Das Ergebnis:
            - Die E-Mail ist leer.
            - Der Anzeigename wird standardmäßig als Benutzername angezeigt.

    - Lösung: Stellen Sie sicher, dass die in AppDynamics konfigurierten Attribute "Anzeigename" und "E-Mail" mit den entsprechenden Attributen in der SAML-Antwort übereinstimmen.
        - Beispiele:
            - Aktualisieren Sie das Display Name-Attribut auf User.fullName.
            - Aktualisieren Sie das E-Mail-Attribut auf User.email.

- HTTP 404-Fehler

- Problem: Der Benutzer kann sich nicht beim Controller anmelden, und es wird der Fehler 404 not found ausgegeben.
- Beispielfehler: In den Controller-Protokollen (nur für Vor-Ort-Controller) wird dieser Fehler angezeigt:

```
[#|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
```

- Root Cause (Ursache): Dieser Fehler tritt in der Regel dann auf, wenn die in der Controller-Datenbank konfigurierte Controller-URL nicht mit der Controller-URL übereinstimmt, die für die Anmeldung verwendet wird, oder mit der URL, die für die IdP konfiguriert wurde.
- Lösung:
    - Für Controller am Standort:
        - Führen Sie diesen Befehl aus, um die Controller-URL zu aktualisieren. (Empfohlen)

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

```
/controller" }' http://
```

```
 /controller/rest/accounts/
```

```
  /update-controller-url
```

- Alternativ können Sie diese Befehle auch in der Controller-Datenbank ausführen, um die Controller-URL zu aktualisieren.

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

```
' WHERE id=
```

```
 ;
UPDATE mds_auth.account SET controller_url='
```

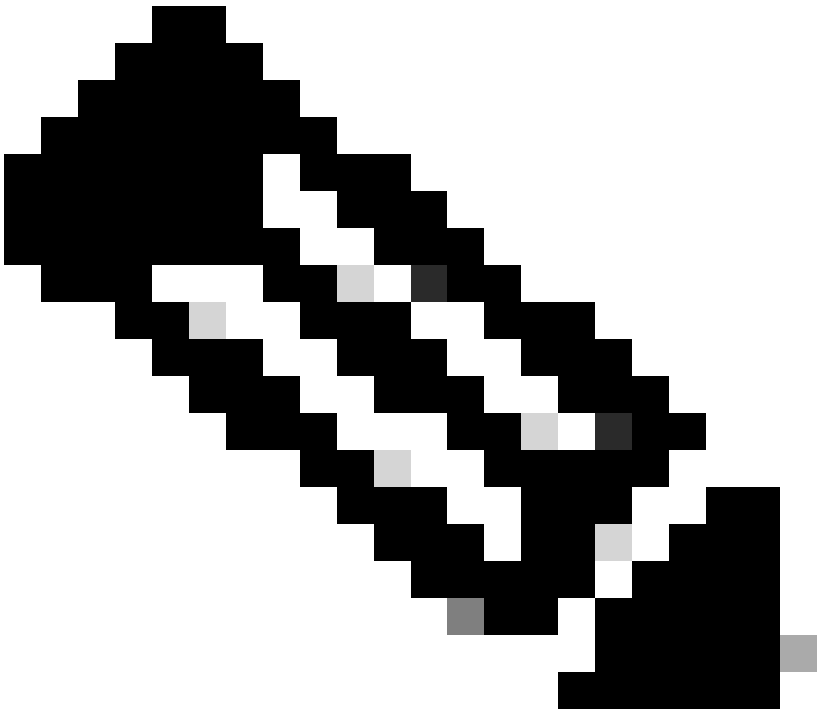
```
  ' WHERE name='
```

```
   ';
```

  - Führen Sie diesen Befehl aus, um <ACCOUNT_ID> abzurufen.

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

```
      ';
```



Anmerkung: Führen Sie curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll aus, wenn Sie das gleiche Problem weiterhin feststellen.

- Ersetzen:
  - <NEW_CONTROLLER_URL> mit der Controller-URL, die Sie für den Zugriff auf den Controller verwenden.
  - <controller_domain> mit Ihrer Controller-Domäne.
  - <IhrKontoname> mit Ihrem Kontonamen.

- Für SaaS-Controller: Senden Sie ein Support-Ticket, um dieses Problem vom Support-Team beheben zu lassen.

Weitere Unterstützung erforderlich

Wenn Sie Fragen haben oder Probleme auftreten, erstellen Sie ein Support-Ticket mit folgenden Informationen:

- Fehlerdetails oder Screenshot: Stellen Sie eine spezifische Fehlermeldung oder einen Screenshot des Problems bereit.

- SAML-Antwort: SAML-Trace- und HAR-Datei erfassen
- Controller Server.log (nur am Standort): Falls zutreffend, stellen Sie die Controller-Server-Protokolle unter <controller-install-dir>/logs/server.log bereit.

Zugehörige Informationen

AppDynamics-Dokumentation

SAML für SaaS-Bereitstellungen

Verschlüsseln von SAML-Antworten für SaaS-Bereitstellungen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.