Eenmalige aanmelding configureren en oplossen in AppDynamics

Inhoud

Inleiding

In dit document wordt beschreven hoe u Single Sign On (SSO) kunt configureren in AppDynamics en problemen kunt oplossen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Om Single Sign On te configureren, moet de gebruiker de functie Account Owner (standaard) hebben of een aangepaste rol met beheer, agents en toestemming van de wizard Aan de slag.
- Beheer toegang tot uw IDp-account.
- De metadata of configuratiegegevens van AppDynamics (bijvoorbeeld Entity ID, ACS URL).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- AppDynamics-controller

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Single Sign-On (SSO) is een verificatiemechanisme waarmee gebruikers zich één keer kunnen aanmelden en toegang krijgen tot meerdere toepassingen, systemen of services zonder dat ze zich voor elke toepassing opnieuw hoeven te authenticeren.

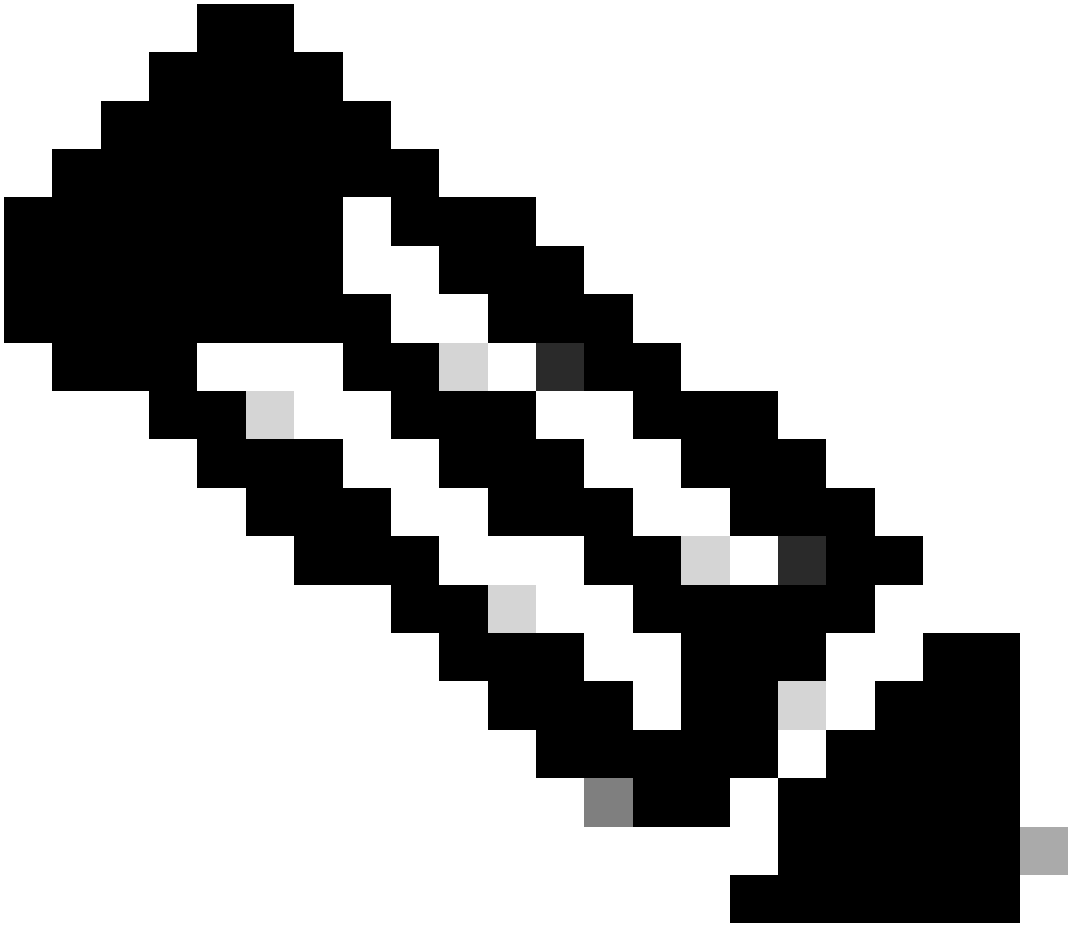
Security Assertion Markup Language (SAML) is een van de technologieën die worden gebruikt om SSO te implementeren. Het biedt het raamwerk en de protocollen die SSO mogelijk maken door authenticatie- en autorisatiegegevens veilig uit te wisselen tussen een Identity Provider (IdP) en een Service Provider (SP).

SAML-bewering

- De op XML gebaseerde berichten worden uitgewisseld tussen de IdP en SP.
- Er zijn drie soorten beweringen:
    - Verificatiebeweringen: Bevestigt dat de gebruiker is geverifieerd.
    - Attribuutbeweringen: deelt gebruikerskenmerken, zoals gebruikersnaam of rollen.
    - Autorisatiebesluit: Geeft aan wat de gebruiker mag doen.

Belangrijke rollen in SAML

- Identiteitsprovider (IDp)
    - Verifieer de identiteit van de gebruiker.
    - Genereer de SAML-bewering die identificatiegegevens van de gebruiker bevat.
- Serviceverlener (SP)
    - De applicatie of het systeem waartoe de gebruiker toegang wil.
    - Vertrouwt op de IdP om de gebruiker te verifiëren.
    - Accepteert de SAML-bewering om de gebruiker toegang te verlenen tot zijn bronnen of toepassingen.
- Gebruiker (opdrachtgever)
    - De daadwerkelijke gebruiker die het verzoek initieert of probeert toegang te krijgen tot een bron van de Serviceverlener.
    - Interactie met zowel de IdP (Authenticatie) als de SP.



Opmerking: AppDynamics ondersteunt zowel IdP-geïnitieerde als SP-geïnitieerde SSO.

SP-geïnitieerde stroom:

- De gebruiker navigeert naar de Serviceverlener door de URL van de toepassing te typen (bijvoorbeeld AppDynamics) of op een link te klikken.
- De SP controleert op een bestaande sessie. Als er geen sessie bestaat, herkent de SP dat de gebruiker niet is geverifieerd en start het SSO-proces.
- De SP genereert een SAML-verificatieverzoek en leidt de gebruiker door naar de IdP voor verificatie.
    - Dit verzoek omvat:
        - Entiteits-ID: unieke identificatiecode van de Serviceverlener.
        - Assertion Consumer Service (ACS) URL: waar de IdP de SAML Assertion verzendt na verificatie.
        - Metagegevens over de SP en beveiligingsdetails (bijvoorbeeld ondertekende aanvraag, coderingsvereisten).
- De gebruiker wordt doorgestuurd naar de IdP-aanmeldingspagina.

- De IdP authenticeert de gebruiker (bijvoorbeeld via gebruikersnaam/wachtwoord of multi-factor authenticatie).
- Na succesvolle authenticatie genereert de IdP een SAML Assertion (beveiligingstoken).
- De SAML Assertion wordt teruggestuurd naar de SP via de gebruikersbrowser met behulp van HTTP POST Binding (in de meeste gevallen) of HTTP Redirect Binding.
- De SP valideert de SAML-bewering om ervoor te zorgen:
    - Het werd uitgegeven door de vertrouwde IdP.
    - Het is gericht aan de SP (via de SP Entity ID).
    - Het is niet verlopen of gemanipuleerd (gevalideerd met de openbare IdP-sleutel).

- Als de SAML-bevestiging geldig is, maakt de SP een sessie voor de gebruiker.
- De gebruiker krijgt toegang tot de applicatie of bronnen.

IdP-geïnitieerde stroom:

- De gebruiker navigeert naar het IdP-inlogportaal en voert zijn referenties in.
- De IdP verifieert de gebruiker (bijvoorbeeld met een gebruikersnaam/wachtwoord combinatie, multi-factor authenticatie).
- Na verificatie geeft de IdP de gebruiker een lijst met beschikbare toepassingen of services (SP's) waartoe hij toegang heeft.
- De gebruiker selecteert de gewenste SP (bijvoorbeeld AppDynamics).
- De IdP genereert een SAML Assertion voor de geselecteerde SP.

- De IdP leidt de gebruiker door naar de SP Assertion Consumer Service (ACS) URL en stuurt de SAML Assertion mee (met behulp van HTTP POST Binding of HTTP Redirect Binding).
- De SP ontvangt de SAML-bewering en valideert deze:
    - Zorgt ervoor dat de bewering wordt uitgegeven door een vertrouwde IdP.
    - Controleert de integriteit en vervaldatum van de bewering.
    - Bevestigt de gebruikersidentiteit en andere kenmerken.

- Als de SAML-bevestiging geldig is, maakt de SP een sessie voor de gebruiker.
- De gebruiker krijgt toegang tot de applicatie of bronnen.

Configureren

De AppDynamics Controller kan de Cisco Customer Identity of een externe SAML Identity Provider (IdP) gebruiken om gebruikers te verifiëren en te autoriseren.

Ondersteunde identiteitsproviders

AppDynamics certificeert ondersteuning voor deze identity providers (IdP's):

- Okta
- onelogin
- Ping-identiteit
- Azure AD
- IBM Cloud Identity

- Active Directory Federation Service (AD FS)

Andere IdP's die HTTP POST-binding ondersteunen, zijn ook compatibel met AppDynamics SAML-verificatie.

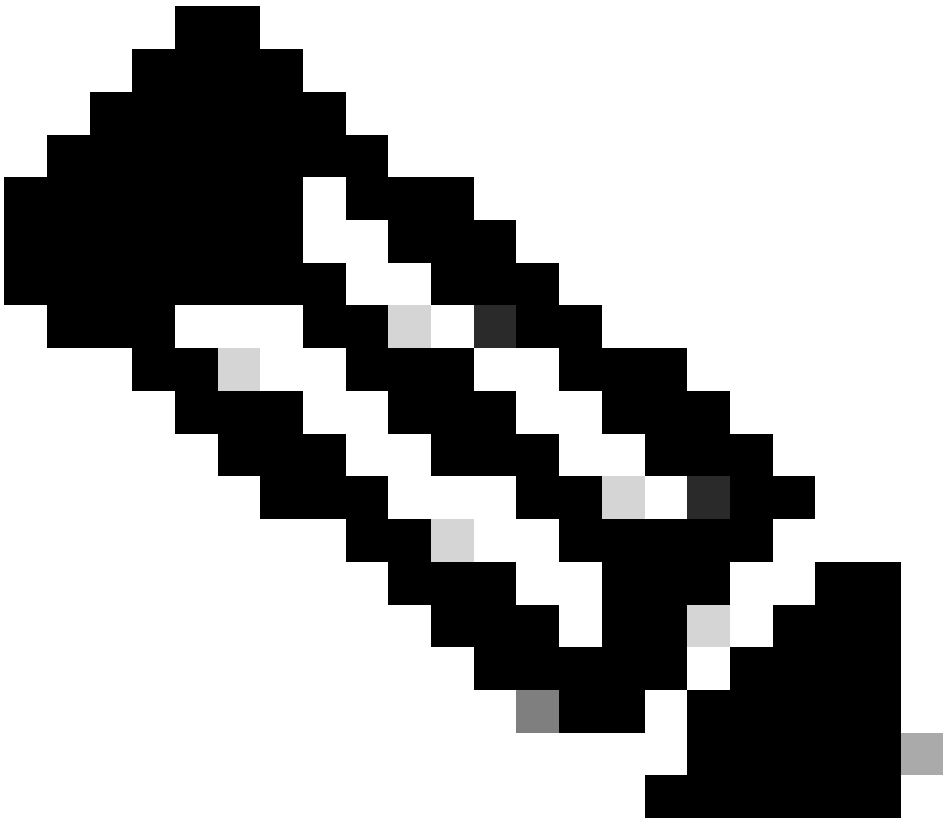
Stappen voor het configureren van SAML in AppDynamics

Stap 1. AppDynamics Controller Details verzamelen

- Entity ID (SP Entity ID): Een unieke ID voor de AppDynamics (bijvoorbeeld https://<controller-host>:<port>/controller).
  - Syntaxis: https://<controller_domain>/controller
  - Voorbeeld: https://<your_controller_domain>/controller

- Reply URL (Assertion Consumer Service, ACS URL): Het eindpunt op de Service Provider (bijvoorbeeld AppDynamics) waar de IdP het SAML-antwoord na verificatie verzendt.
  - Syntaxis: https://<controller_domain>/controller/saml-auth?accountName=<account_name>
  - Voorbeeld: https://your_controller_domain/controller/saml-auth?accountName=youraccountname

---



> Opmerking: In het geval van On-Prem-controller is de standaardaccountnaam klant1, tenzij u een multitenant-controller hebt met een andere accountnaam.

- Single Logout URL (Optioneel): Het eindpunt op de SP voor het verwerken van SAML-afmeldingsverzoeken (bijvoorbeeld https://<controller_domain>/controller).

Stap 2. Maak een nieuwe toepassing in IdP en download de metagegevens

- Lokaliseer het gebied voor het maken van toepassingen: Dit bevindt zich meestal in de IdP-beheerconsole of het dashboard, vaak aangeduid als iets als Toepassingen, Web- en mobiele apps, Bedrijfstoepassingen of Betrouwbare partijen.
- Een aangepaste of generieke SAML-toepassing toevoegen: Selecteer een optie waarmee u een aangepaste SAML-toepassing of een generieke SAML-serviceprovider-integratie kunt configureren.
- Geef de toepassing een naam en upload mogelijk een pictogram voor identificatie (optioneel).
- Voeg attribuuttoewijzingen toe (gebruikersnaam, displayName, e-mail of rollen) om gebruikersinformatie door te geven aan AppDynamics.
- Download het IdP-metagegevensbestand of noteer deze details als volgt:
  - Inlog-URL voor IDp
  - Afmeldings-URL
  - Namen van kenmerken
  - getuigschrift

Stap 3. SAML-verificatie configureren in AppDynamics-controller

- Meld u aan bij de gebruikersinterface voor de controller als een rol voor de eigenaar van een account of een rol met beheer, agents en toestemming voor de wizard Aan de slag.
- Klik op uw gebruikersnaam (rechterbovenhoek)> Beheer > Verificatieprovider > Selecteer SAML.

- Voeg in het gedeelte SAML Configuration de volgende details toe:

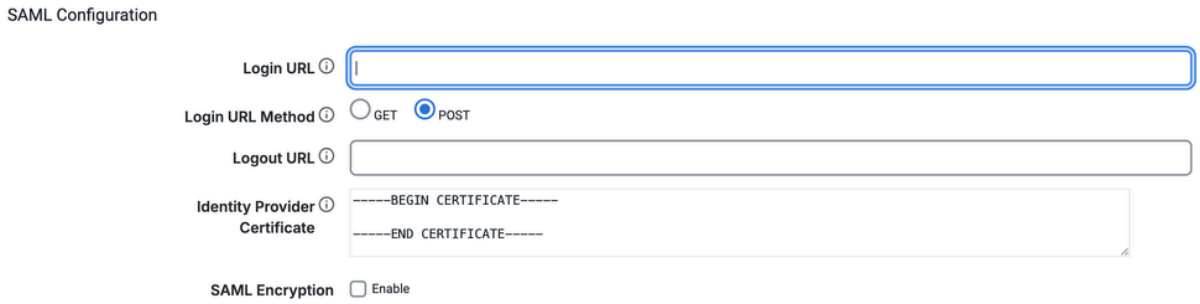
  - Inlog-URL: de IdP-inlog-URL waar AppDynamics Controller door Service Provider (SP) geïnitieerde inlogverzoeken routeert.

  - Afmeldings-URL (optioneel): de URL waar AppDynamics Controller gebruikers omleidt nadat ze zich hebben afgemeld. Als u geen afmeldings-URL opgeeft, krijgen gebruikers het aanmeldingsscherm van AppDynamics wanneer ze zich afmelden.

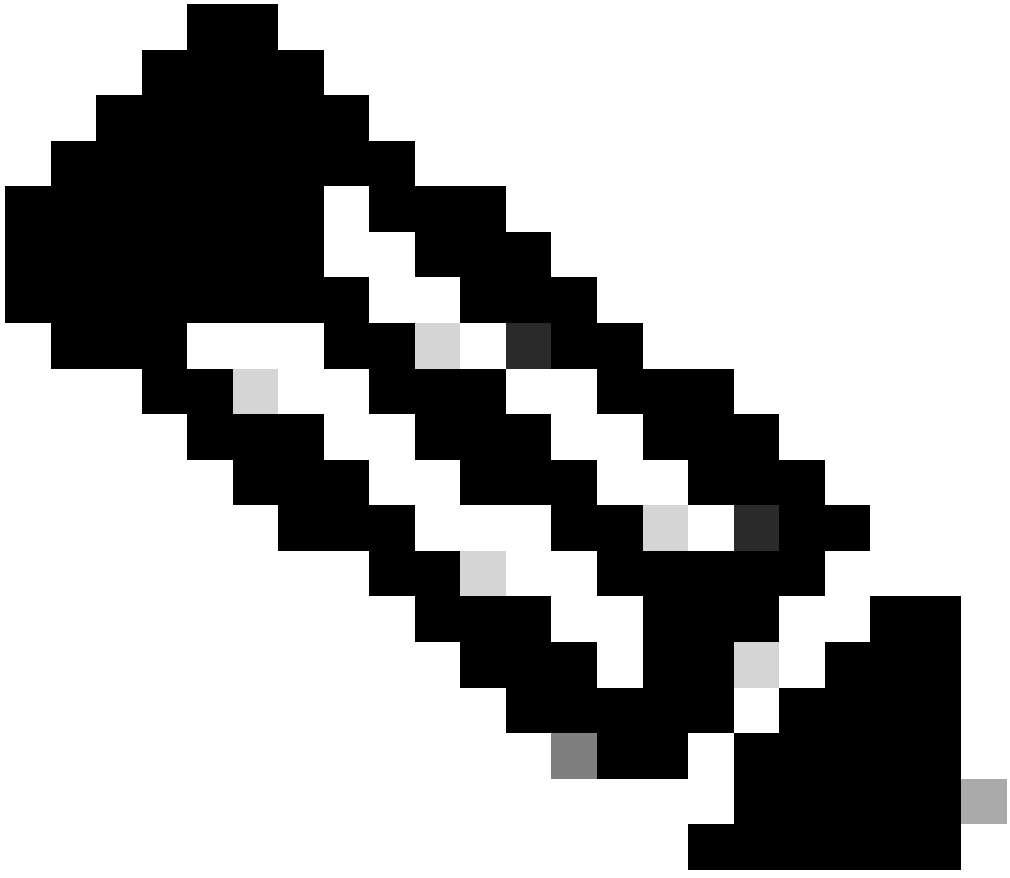
  - Certificaat: Het X.509 certificaat van IdP. Plak het certificaat tussen de scheidingstekens BEGIN-CERTIFICAAT en EIND-CERTIFICAAT. Vermijd duplicatie van begin- en eindcertificaatbegrenzers van het broncertificaat zelf.

  - SAML-codering (optioneel): u kunt de beveiliging van de SAML-verificatie verbeteren door de SAML-respons van de IdP naar de serviceprovider te coderen. Om SAML-antwoorden in AppDynamics te coderen, moet u uw Identity Provider (IdP)

configureren om de SAML-bevestiging te coderen en vervolgens de AppDynamics Controller configureren om een specifiek certificaat en een privésleutel te gebruiken voor decodering.



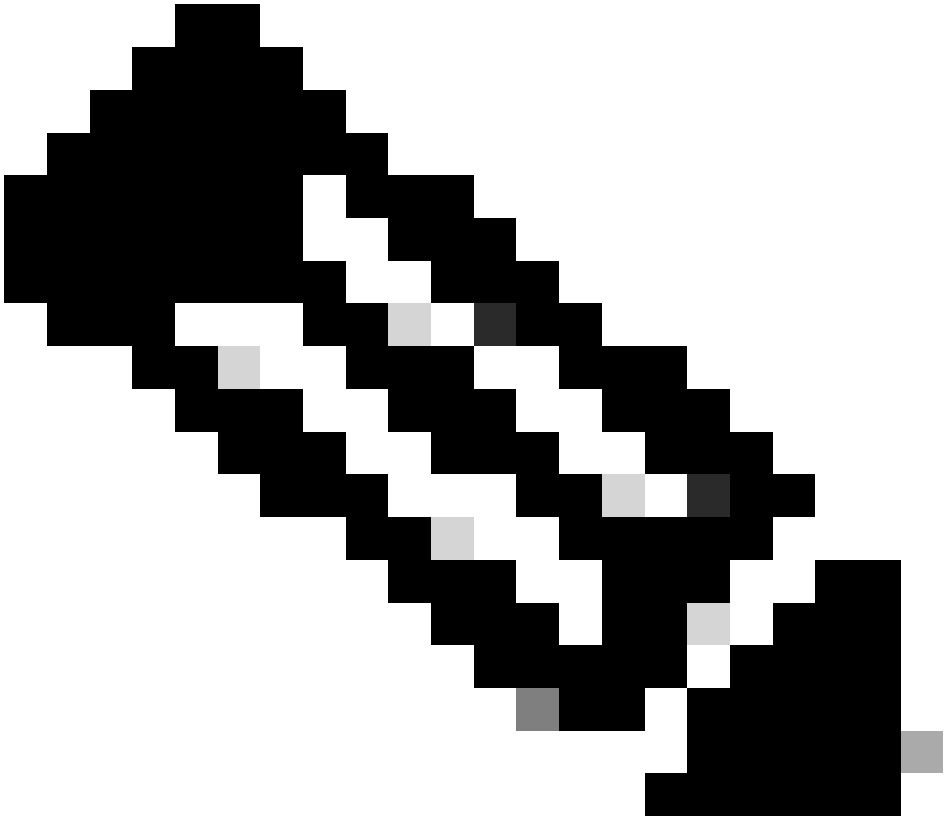
- In het gedeelte SAML Attribuuttoewijzingen koppelt u de SAML-kenmerken (bijvoorbeeld: Gebruikersnaam, DisplayName, E-mail) aan de bijbehorende velden in AppDynamics.



Opmerking: AppDynamics geeft de gebruikersnaam, e-mail en weergavenaam van een SAML-gebruiker weer. Standaard wordt het kenmerk NameID van het SAML-antwoord gebruikt om een gebruikersnaam te maken, die ook wordt gebruikt als de

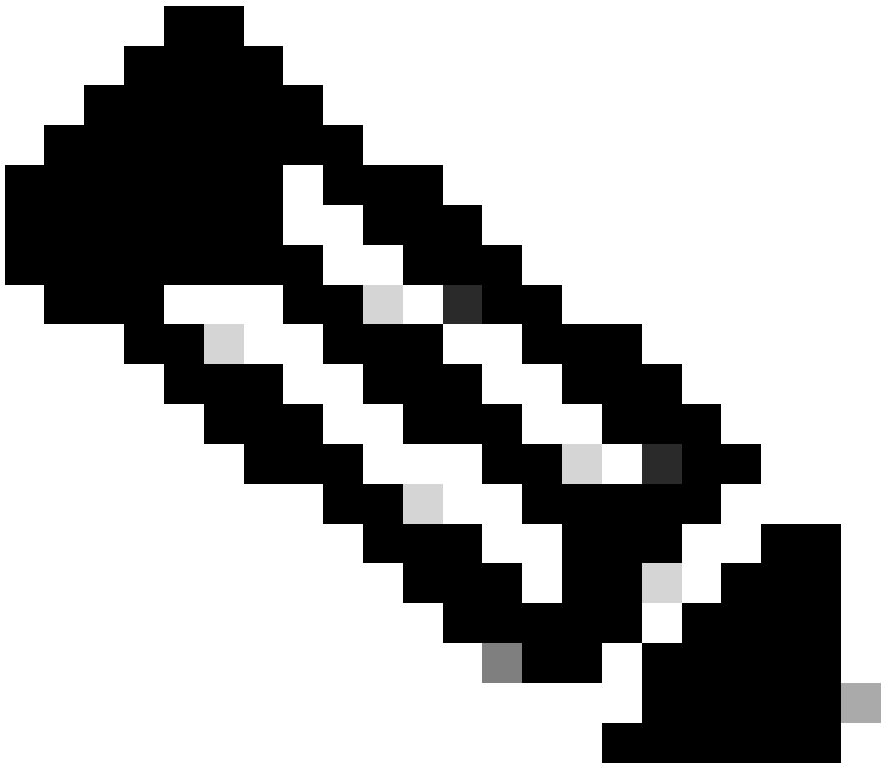
displayName. Dit gedrag kan worden aangepast door de kenmerken gebruikersnaam, e-mail en displaynaam op te nemen in de SAML-reactie. Tijdens het configureren van de IdP-instellingen in AppDynamics kan de gebruiker deze attribuutnamen opgeven. Tijdens het inloggen controleert AppDynamics of attribuuttoewijzing is geconfigureerd. Als toewijzingen zijn geconfigureerd en overeenkomende attributen aanwezig zijn in de SAML-respons, gebruikt AppDynamics deze attribuutwaarden om de gebruikersnaam, het e-mailadres en de displaynaam in te stellen.

- Voeg deze details toe in de sectie SAML Group Mappings.
  - SAML Group Attribuutnaam: Voer de naam in van het SAML-attribuut dat de groepsinformatie bevat. Dit zijn meestal Groepen, of groep of rollen, of Rollen of groepslidmaatschap.
  - Waarde groepsattribuut: Selecteer de juiste waardenindeling voor het groepsattribuut. Veelvoorkomende opties zijn Meerdere geneste groepswaarden of Enkele waarde, afhankelijk van hoe uw IdP de groepsinformatie structureert.

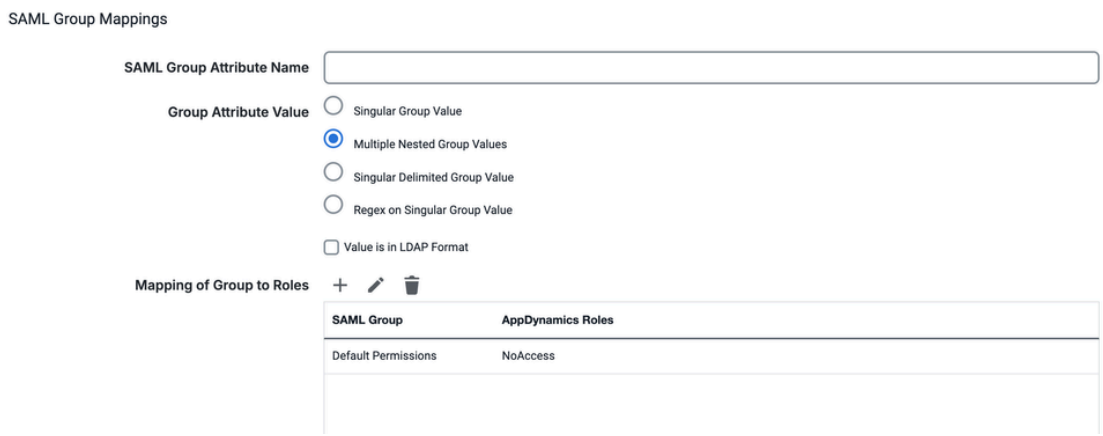


Opmerking: Selecteer de waarde in LDAP-indeling als de groepsgegevens in LDAP-indeling (Lightweight Directory Access Protocol) worden geleverd.

- Groepen toewijzen aan rollen: Klik op de + knop om een nieuwe toewijzing toe te voegen.
  - SAML-groep: Voer de naam in van de SAML-groep (zoals gedefinieerd in uw IdP) die u wilt toewijzen aan een AppDynamics-rol.
  - Rol(len): Selecteer de bijbehorende AppDynamics-rol(len) uit de beschikbare lijst die u wilt toewijzen aan gebruikers die behoren tot de SAML-groep.
  - Standaardmachtigingen: Als SAML-groepstoewijzing niet is geconfigureerd of als een SAML-bevestiging van een gebruiker geen groepsinformatie bevat, kan AppDynamics terugvallen op het gebruik van standaardmachtigingen.



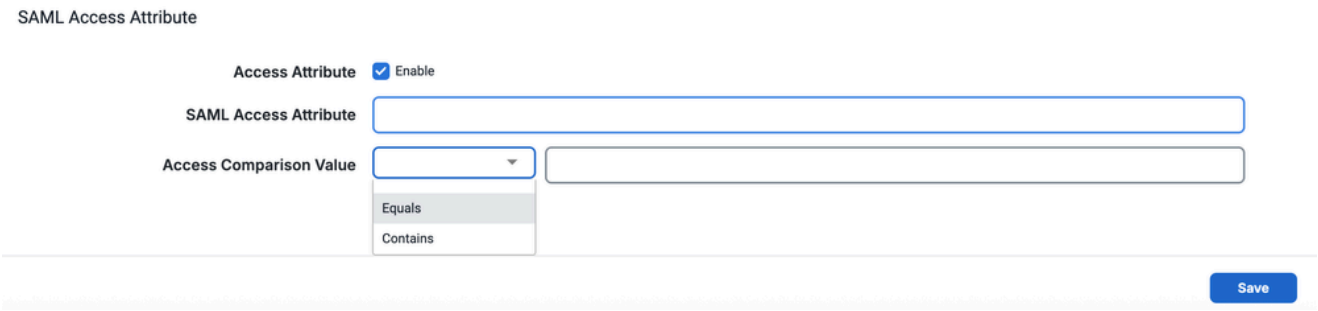
Opmerking: Het wordt aanbevolen om een rol met minimale rechten toe te wijzen aan Standaardmachtigingen.



- Voeg in het gedeelte SAML Access Attribute deze details toe (optioneel):
  - SAML Access Attribuut: Voer de naam in van de attributen uit de SAML reactie. Dit wordt gebruikt voor toegangsvalidatie.

- Toegangsvergelijkingswaarde: er zijn twee opties beschikbaar:
  1. Gelijk: Toegang wordt alleen verleend als de attribuutwaarde in de SAML-respons exact overeenkomt met de waarde die in de configuratie is opgegeven.
  2. Bevat: Toegang wordt verleend als de attribuutwaarde in de SAML-respons de waarde bevat die in de configuratie is opgegeven.
- Hoe werkt het als ingeschakeld:
  1. AppDynamics haalt het attribuut op dat is opgegeven in het veld SAML Access Attribuut uit de SAML-respons.
  2. Het vergelijkt de waarde van het attribuut met de door de gebruiker gedefinieerde waarde voor toegangsvergelijking op basis van de geselecteerde methode (Gelijk of Bevat).
  3. Als de vergelijking succesvol is, krijgt de gebruiker toegang.
  4. Als de vergelijking mislukt, wordt de inlogpoging geweigerd.

- Klik op Opslaan (rechtsonder) om de configuratie op te slaan.



Verifiëren

- Open een browser en navigeer naar AppDynamics Controller. Het dialoogvenster Inloggen voor uw 3rd-party IdP-service wordt weergegeven.
- Klik op Inloggen met eenmalige aanmelding. Het systeem leidt je door naar je IdP.
- Voer uw referenties in en verzend deze.
- Na een succesvolle authenticatie leidt The IdP je door naar je AppDynamics Controller.

Gemeenschappelijke problemen en oplossingen

400 slechte aanvraag

- Probleem: gebruikers krijgen te maken met een 400 Bad Request-fout wanneer ze proberen in te loggen op AppDynamics Controller.
- Voorbeeldfout:

```
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.
```

- Vaak voorkomende oorzaken:
    - Ongeldig SAML-certificaat
    - SAML-respons is groter dan de maximale lengte
    - Ongeldige entiteit-ID of ACS-URL
- Oplossing:
    - Ongeldig SAML-certificaat
        - Zorg ervoor dat het certificaat dat door de Identiteitsaanbieder (IdP) wordt verstrekt geldig en actueel is.
        - Controleer de vervaldatum van het IdP-certificaat. Als het is verlopen, verkrijg dan een nieuw certificaat van de IdP.
        - Als het certificaat aan de IdP-zijde is bijgewerkt, moet u ervoor zorgen dat het nieuwe certificaat wordt geüpload en geconfigureerd in AppDynamics.
        - Stappen om het certificaat bij te werken in AppDynamics:
            - Meld u aan bij de gebruikersinterface van de controller als een rol voor de accounteigenaar of als een rol met beheer, agents en toestemming voor de wizard Aan de slag.
            - Klik op uw gebruikersnaam (rechterbovenhoek)> Beheer > Verificatieprovider > Selecteer SAML.
            - Zoek in het gedeelte SAML-configuratie het veld Certificaat en vervang het oude certificaat door het nieuwe certificaat dat door de IdP wordt geleverd.
            - Klik op Opslaan om de SAML-configuratie bij te werken.

    - De SAML-respons is groter dan de maximale lengte.
        - Dit probleem doet zich voor wanneer de controller wordt verplaatst van GlassFish naar Jetty Server, te beginnen met Controller versie 10 .11 en hoger. In Jetty Server is er een eigenschap genaamd -Dorg.eclipse.jetty.server. Request.maxFormContentSize bevindt zich in het .../appserver/jetty/start.d/start.ini bestand. Als de SAML-reactiegrootte groter is dan de waarde die voor deze eigenschap is ingesteld, wijst de controller de payload af en retourneert hij een 400 Bad Request fout.
        - Oorzaken van grote SAML-reacties:
            - Excessieve attributen: te veel attributen die zijn opgenomen in de SAML-bewering.
            - Ondertekende of gecodeerde SAML-antwoorden: ondertekening of codering vergroot de responsgrootte.
            - Extra gebruikers- of groepsgegevens: de identiteitsprovider (IDp) heeft extra gebruikers- of groepsgegevens.

        - Er zijn twee manieren om dit probleem op te lossen. Door een of beide oplossingen te implementeren, kunt u het probleem oplossen en voorkomen dat de payload wordt afgewezen.
            1. De waarde maxFormContentSize verhogen
                - Voor On-Prem Controllers: Update de eigenschap -Dorg.eclipse.jetty.server.Request.maxFormContentSize in het .../appserver/jetty/start.d/start.ini-bestand naar een grotere waarde en

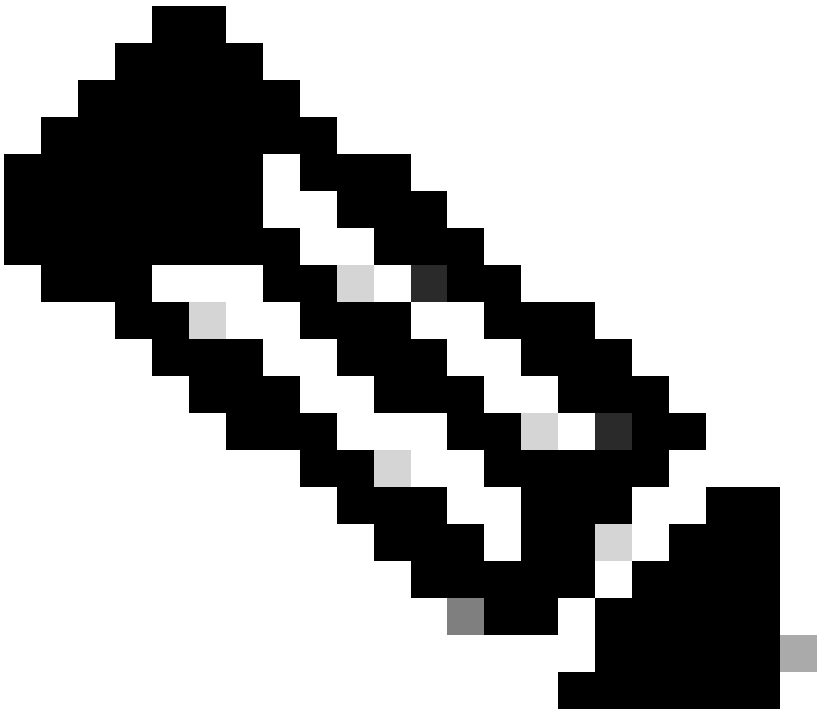
start de controller opnieuw op.
    - Voor SaaS-controllers: dien een supportticket in om dit probleem door het supportteam te laten oplossen.

2. De SAML-respons optimaliseren

   Werk samen met uw Identity Provider (IdP) om de omvang van de SAML-respons te verminderen door de volgende aanpassingen te maken:

   - Onnodige kenmerken uitsluiten: Verwijder ongebruikte of redundante kenmerken uit de SAML-bevestiging via de IdP-configuratie.
   - Encryptie uitschakelen (indien toegestaan): Encryptie vergroot de SAML-responsomvang. Als de verbinding al is beveiligd via HTTPS, overweeg dan om de codering uit te schakelen om de grootte te verkleinen.

- Ongeldige entiteit-ID of ACS-URL
  - Over het IDP:
    - Bevestig dat de Entiteit-ID https://your_controller_domain/controller is. Als de Entiteit-ID anders is, werk deze dan bij.
    - Bevestig dat de ACS-URL https://your_controller_domain/controller/saml-auth?accountName=youraccountname is. Als de ACS-URL anders is, werkt u deze dienovereenkomstig bij.



Opmerking: accountnaam moet overeenkomen met de naam van

---

uw AppDynamics-account. (bijvoorbeeld klant1)

- Ontbrekende gebruikersmachtigingen
  - Probleem: u bent met succes ingelogd bij de controller. U hebt echter niet de beoogde rollen en machtigingen ontvangen.
  - Voorbeeld configuratie en SAML-respons:
    - In de SAML-gebruiker is het attribuut Group de naam Groups met de waarden AppD_Admin & AppD_Power_User.

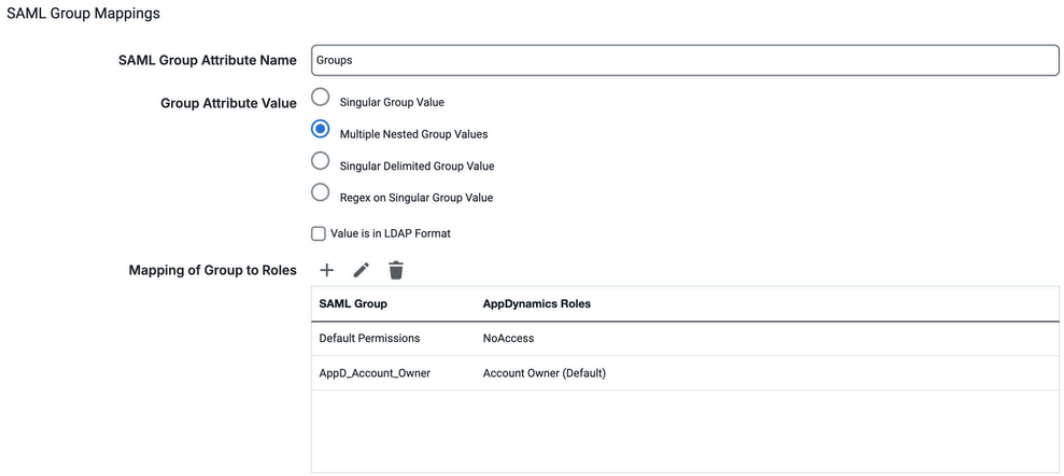
```
AppD_Admin
```

```
AppD_Power_User
```

    - In de AppDynamics, onder SAML Group Mappings sectie, worden deze geconfigureerd.
      - Naam SAML-groepsattribuut: Groepen
      - Waarde groepskenmerk: meerdere geneste groepswaarden
      - Toewijzen aan groepsrollen:

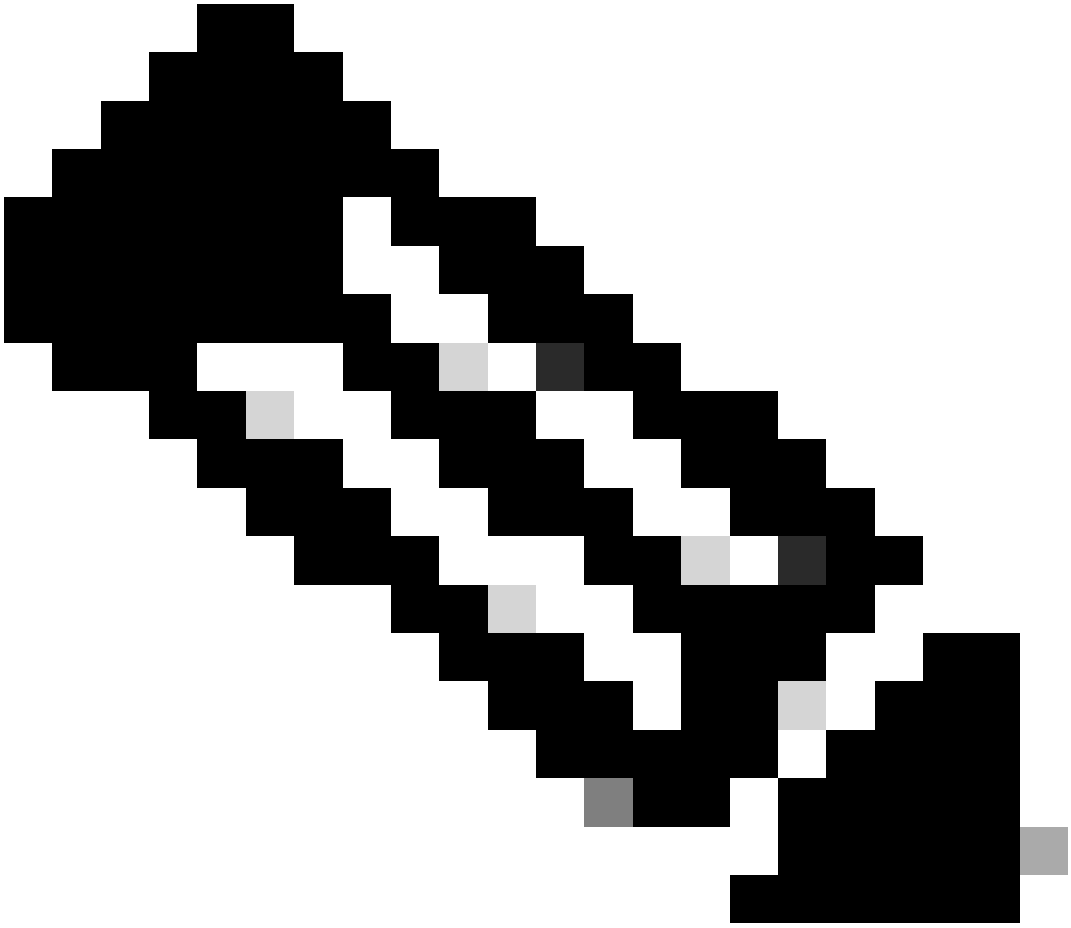
SAML-groep	AppDynamics-rollen
AppD_Account_Owner	Rekeninghouder (standaard)
Standaardmachtigingen	Geen toegang

No Access is een aangepaste rol zonder machtigingen.



- Gemeenschappelijke problemen en oplossingen
  - Geen groepskenmerken gevonden in SAML-respons.
    - Het SAML-antwoord van de IdP mist de vereiste groepsattributen of de attribuutnaam voor groepen in de SAML-reactie wordt ingesteld als Rollen terwijl het in AppDynamics wordt geconfigureerd als Groepen.
    - Als er geen groepskenmerken worden opgegeven, krijgt de gebruiker automatisch de rollen toegewezen die zijn gekoppeld aan Standaardmachtigingen in AppDynamics.
    - Om dit op te lossen, moet u ervoor zorgen dat de IdP is geconfigureerd om de juiste groepskenmerken in de SAML-respons op te nemen en dat de attribuutnaam voor groepen overeenkomt met de configuratie in AppDynamics.

  - Er is geen overeenkomstige SAML-groepstoewijzing geconfigureerd in AppDynamics voor de gebruikersgroepen die in de SAML-reactie worden verstrekt.
    - In het SAML-antwoord bevat het attribuut Groups de waarden AppD_Admin en AppD_Power_User. In AppDynamics bestaan groepstoewijzingen echter alleen voor de groep AppD_Account_Owner.
    - Aangezien er geen overeenkomstige toewijzing voor AppD_Admin of AppD_Power_User is, krijgt de gebruiker geen rollen of machtigingen toegewezen.
    - Om dit op te lossen, voegt u de ontbrekende groepstoewijzingen toe (bijvoorbeeld AppD_Admin en AppD_Power_User) in AppDynamics om de juiste rol en rechtstoewijzing te garanderen.



Opmerking: Standaardmachtigingen worden alleen toegepast op SAML-gebruikers wanneer de naam van het SAML-groepattribuut dat is geconfigureerd in AppDynamics, niet hetzelfde is als de kenmerken Groepen in het SAML-antwoord.

- Ontbrekende of onjuiste e-mail en/of naam voor SAML-gebruikers
    - Probleem: Dit gebeurt meestal wanneer de Attribuutconfiguratie in AppDynamics niet overeenkomt met de attributen die in de SAML-reactie komen.
    - Voorbeeld SAML-reactie: Attributen in de SAML-reactie zijn: User.email, User.fullName en Groups

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- Voorbeeld SAML Attribuuttoewijzingen in AppDynamics
  - Gebruikersnaam Attribuut: User.name
  - Display Name Attribuut: User.firstName of leeg
  - E-mailkenmerk: User.userPrincipal of leeg

- Hoofdoorzaak: de in AppDynamics geconfigureerde kenmerken Display Name en

Email komen niet overeen met een van de kenmerken die in de SAML-reactie worden gegeven.
    - Als gevolg hiervan:
        - De e-mail is ingesteld op leeg.
        - De weergavenaam is standaard gekoppeld aan de gebruikersnaam.

- Oplossing: zorg ervoor dat de in AppDynamics geconfigureerde Display Name en Email attributen overeenkomen met de bijbehorende attributen in de SAML respons.
    - Voorbeeld:
        - Werk het kenmerk Display Name bij naar User.fullName.
        - Werk het kenmerk E-mail bij naar User.email.

- HTTP 404-fout

- Probleem: de gebruiker kan zich niet aanmelden bij de controller en krijgt 404 niet gevonden fout.
- Voorbeeldfout: in controllerlogboeken (alleen voor On-Prem-controller) ziet u deze fout:

```
[#|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: Deze fout treedt meestal op wanneer de controller-URL die is geconfigureerd in de controller-database niet overeenkomt met de controller-URL die is gebruikt om in te loggen of de URL die is geconfigureerd op de IdP
- Oplossing:
    - Voor On-Prem-controllers:
        - Voer deze opdracht uit om de controller-URL bij te werken. (Aanbevolen).

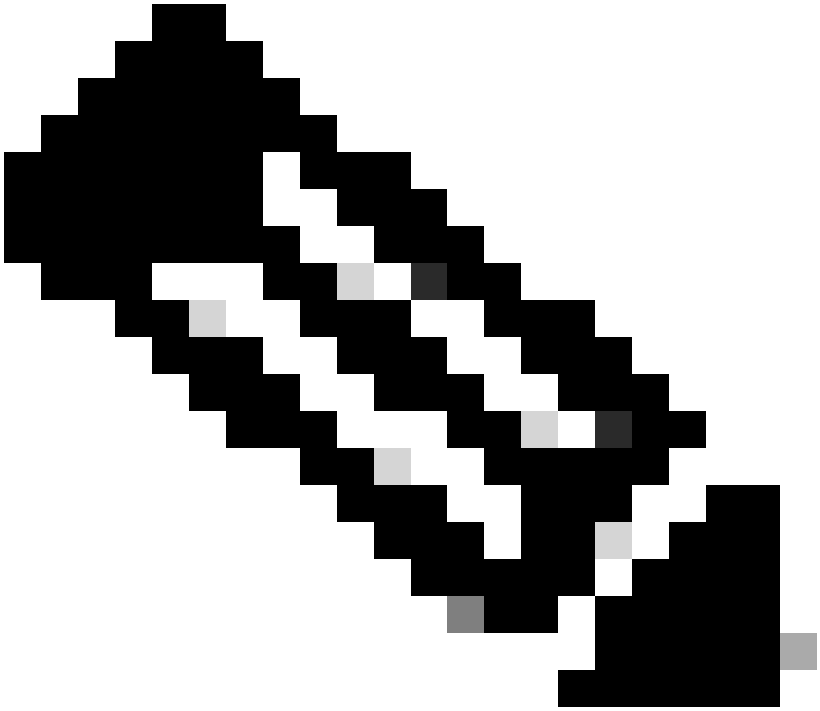
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- U kunt deze opdrachten ook uitvoeren in de controllerdatabase om de controller-URL bij te werken.

```
UPDATE controller.account SET controller_url ='

            ' WHERE id=

             ;
UPDATE mds_auth.account SET controller_url='

              ' WHERE name='

               ';
```

  - Voer deze opdracht uit om de <ACCOUNT_ID> op te halen.

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

                ';
```



Opmerking: Voer curl -X POST -u root@system https://<controller_domein>/controller/api/controllermds/syncAll uit als u nog steeds hetzelfde probleem waarneemt.

- Vervangen:
  - <NEW_CONTROLLER_URL> met de eigenlijke controller-URL die u gebruikt om toegang te krijgen tot de controller.
  - <controller_domain> met uw controllerdomein.
  - <Uw accountnaam> met uw accountnaam.

- Voor SaaS-controllers: dien een supportticket in om dit probleem door het supportteam te laten oplossen.

Verdere hulp nodig

Als u een vraag hebt of problemen ondervindt, maakt u een supportticket met deze gegevens:

- Foutdetails of schermafbeelding: geef een specifieke foutmelding of een schermafbeelding van het probleem op.
- SAML-respons: SAML-Trace- en HAR-bestand verzamelen
- Controller Server.log (alleen On-Prem): indien van toepassing, geef de controllerserverlogs op van <controller-install-dir>/logs/server.log

Gerelateerde informatie

AppDynamics-documentatie

SAML voor SaaS-implementaties

SAML-antwoorden voor SaaS-implementaties coderen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.