

AppDynamics API Client configureren en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Een API-client maken](#)

[Bestaande API-client bekijken](#)

[Bestaande API-client verwijderen](#)

[Toegangstoken genereren](#)

[Administrator UI \(langlevende tokens\)](#)

[OAuth API \(kortstondige tokens\)](#)

[Toegangstokens beheren](#)

[Toegangstoken opnieuw genereren](#)

[toegangstoken intrekken](#)

[Gebruik Access Token om Rest API te maken](#)

[Gemeenschappelijke problemen en oplossingen](#)

[401Niet geautoriseerd](#)

[Lege reactie.](#)

[Ongeldig type inhoud](#)

[Gerelateerde informatie](#)

[Meer hulp nodig?](#)

Inleiding

In dit document wordt beschreven hoe u een AppDynamics API-client maakt, tokens genereert en problemen oplost.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Als u een API-client wilt maken, moet een gebruiker de functie Account Owner (standaardrol) hebben of een aangepaste rol met de machtiging Beheer, Agenten en Wizard Aan de slag.

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.

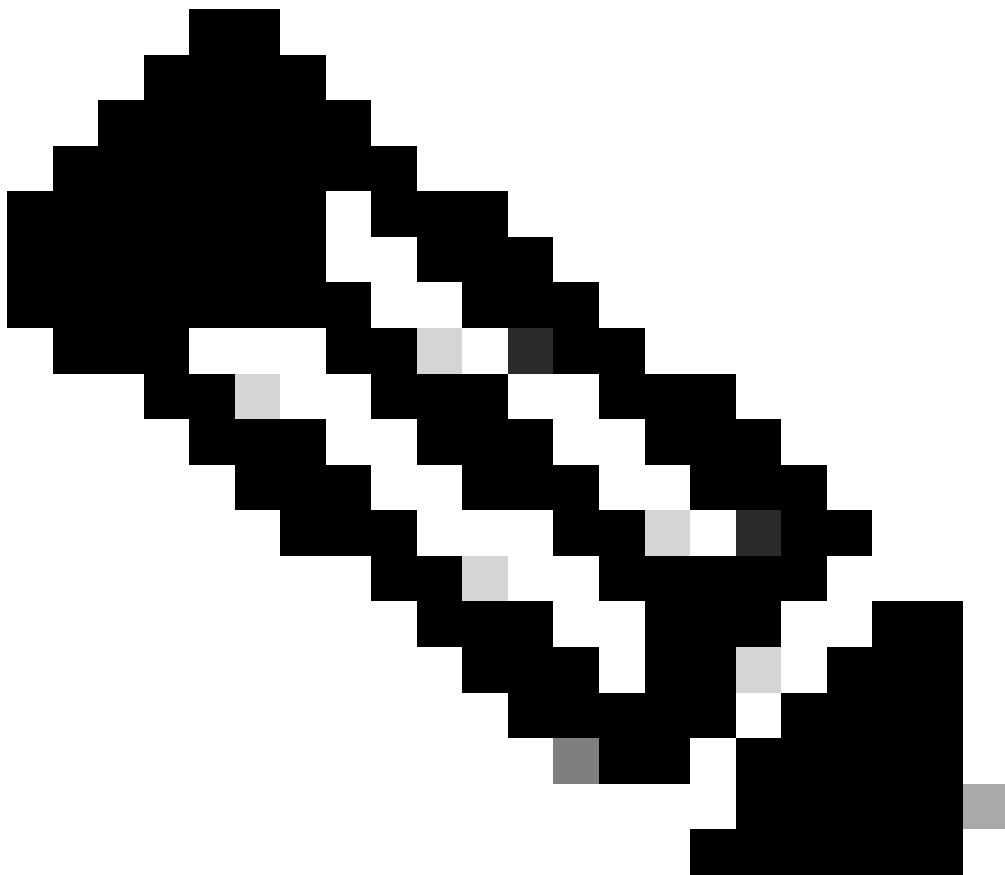
Achtergrondinformatie

Dit document beschrijft het proces voor het maken van API-clients om veilig toegang te krijgen tot de gegevens van de AppDynamics Controller met behulp van Representational State Transfer (REST) en Application Programming Interface (API)-oproepen. De API-clients maken gebruik van Open Authorization (OAuth) token-gebaseerde authenticatie. OAuth biedt services van derden toegang tot accountinformatie van een eindgebruiker zonder de gebruikersreferenties bloot te leggen. Het fungeert als tussenpersoon en biedt de service van derden een toegangstoken aan dat het delen van specifieke accountinformatie toestaat. Gebruikers kunnen het OAuth-token genereren na het instellen van de API-client. Bovendien behandelt dit document het oplossen van veelvoorkomende problemen bij het gebruik van API-clients.

Configureren

Een API-client maken

1. Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
2. Klik op Gebruikersnaam (rechtsboven) > Beheer.
3. Klik op het tabblad API-client.
4. Klik op + Aanmaken.
5. Voer de naam en beschrijving van de client in.
6. Klik op Geheim genereren om het clientgeheim in te vullen.



Opmerking: het clientgeheim wordt slechts eenmaal gegenereerd en weergegeven.
Kopieer en bewaar deze informatie veilig.

7. Stel de standaardvervaldatum van de token in.
8. Klik op + Toevoegen in rollen sectie om de rol toe te voegen.
9. Klik rechtsboven op Opslaan.

Bestaande API-client bekijken

1. Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
2. Klik op Gebruikersnaam (rechterbovenhoek) > Beheer.
3. Klik op het tabblad API-client om bestaande API-clients te bekijken.

Bestaande API-client verwijderen

1. Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een

- rol met de machtiging voor beheer, agents en de wizard Aan de slag.
2. Klik op uw gebruikersnaam (rechterbovenhoek) > Beheer > API-clients.
 3. Zoek de specifieke API-clients die u wilt verwijderen en selecteer ze.
 4. Klik op het pictogram Verwijderen of klik met de rechtermuisknop op de geselecteerde API-client(s) en selecteer API-client(s) verwijderen om de bestaande API-client(s) te verwijderen.
-



Waarschuwing: als u de API-client verwijdert, wordt de token ongeldig gemaakt.

Toegangstoken genereren

De Access Token kan worden gegenereerd via de Administrator UI of de OAuth API. De UI biedt tokens met een lange levensduur, terwijl de OAuth API tokens met een korte levensduur genereert, die regelmatig worden vernieuwd.

- Administrator UI (langlevende tokens)
 - Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of

een rol met de machtiging voor beheer, agents en de wizard Aan de slag.

- Klik op uw gebruikersnaam (rechterbovenhoek) > Beheer > API-clients.
- Selecteer de API-client waarvoor u het toegangstoken wilt genereren en klik op Tijdelijke toegangstoken genereren.
- De toegangstokens die worden gegenereerd vanuit de gebruikersinterface hebben een langere vervaltijd.

- OAuth API (kortstondige tokens)

- `U kunt REST API's gebruiken om een kortstondig Access Token te genereren.

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" "https://
```

```
/controller/api/oauth/access_token" -d 'grant_type=client_credentials&client_id=
```

```
@
```

```
&client_secret=
```

```
,
```

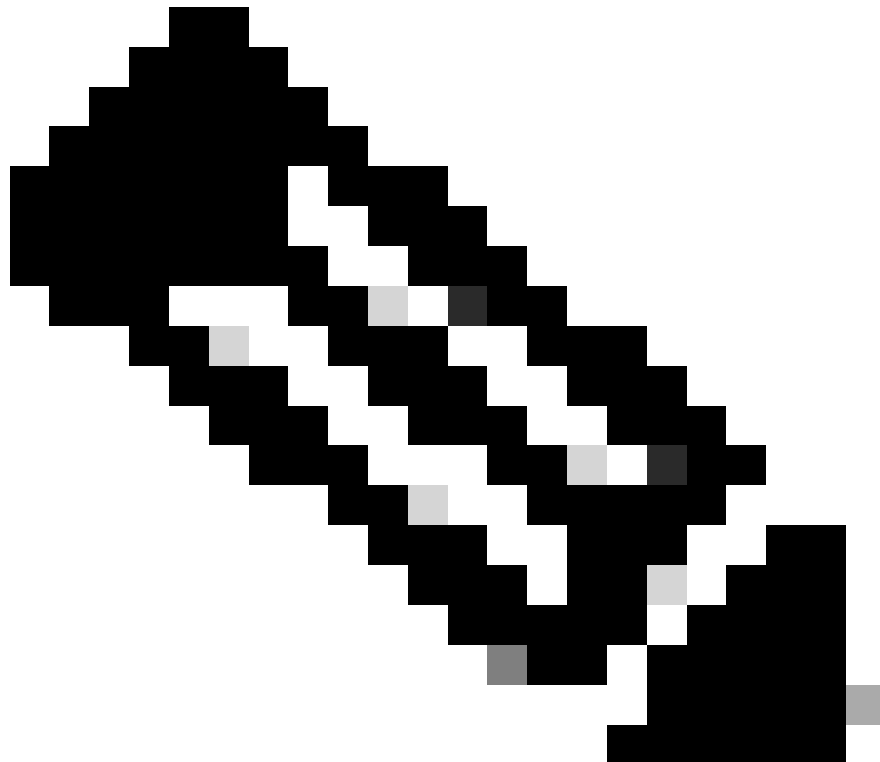
Vervangen:

- met de clientnaam die u hebt ingevoerd tijdens het maken van de API-client of zoals deze wordt gedeeld door uw beheerder.

- met de accountnaam.

-

met het clientgeheim dat u hebt gegenereerd tijdens het maken van de API-client of zoals gedeeld door uw beheerder.



Opmerking: On-demand token wordt niet bijgehouden op de gebruikersinterface.

Voorbeeldreactie:

```
{
  "access_token": "

  ",
  "expires_in": 300
}
```

Toegangstokens beheren

- Toegangstokens die zijn gegenereerd vanuit de REST API kunnen alleen worden ongeldig gemaakt door de bijbehorende API-client te verwijderen.

- Toegangstokens die zijn gegenereerd via de controller-gebruikersinterface kunnen worden ingetrokken of opnieuw worden gegenereerd.
 - Het opnieuw genereren van een toegangstoken maakt de vorige tokens niet ongeldig. De oudere tokens blijven actief tot de vervaldatum.
 - Er is geen manier om eerdere of momenteel geldige tokens op te halen. Alleen de huidige token kan worden ingetrokken.
- Toegangstoken opnieuw genereren
 - Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
 - Klik op uw gebruikersnaam (rechterbovenhoek) > Beheer > API-clients.
 - Selecteer de API-client waarvoor u het toegangstoken wilt regenereren en klik op Regenereren > Opslaan (rechterbovenhoek).
 - toegangstoken intrekken
 - Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
 - Klik op uw gebruikersnaam (rechterbovenhoek) > Beheer > API-clients.
 - Selecteer de API-client waarvoor u het toegangstoken wilt intrekken en klik op Intrekken > Opslaan (rechterbovenhoek).

Gebruik Access Token om Rest API te maken

- Van [Splunk AppDynamics API's](#) dBepaal het specifieke eindpunt waarmee u moet communiceren.
- Bouw het verzoek:
 - Methode: Selecteer de HTTP-methode (GET, POST, PUT, DELETE) op basis van de actie die u wilt uitvoeren.
 - Headers: Voeg de toegangstoken toe in de koptekst voor autorisatie.
 - Body (indien aanwezig): Voeg de hoofdtekst van het verzoek toe in de JavaScript Object Notation (JSON)-indeling.
- Voorbeeldaanvraag

```
curl --location --request GET 'https://
```

```
/controller/
```

```
' --header 'Authorization: Bearer
```

Vervangen:

- met de URL van de controller.
- Met het Rest Endpoint moet je communiceren.
- met het toegangstoken dat is gegenereerd met behulp van de clientnaam en het clientgeheim.

Gemeenschappelijke problemen en oplossingen

- 401 onbevoegd
 - Probleem: gebruikers krijgen te maken met een 401-fout bij het genereren van een toegangstoken.
 - Voorbeeldreactie:


```
HTTP Error 401 Unauthorized
```



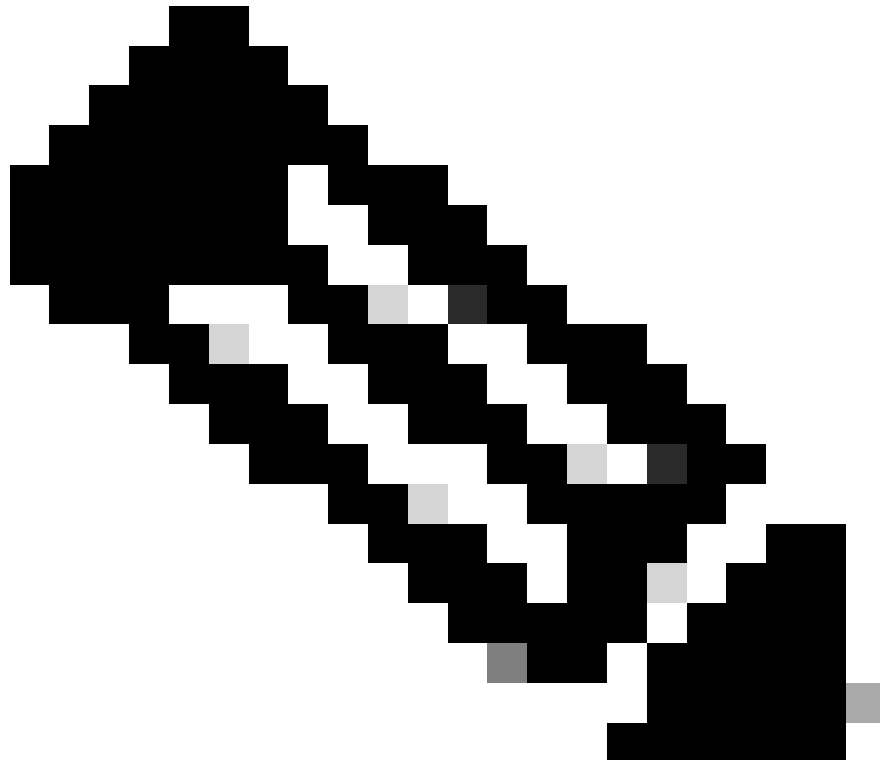
```
This request requires HTTP authentication
```
 - Hoofdoorzaak: het probleem ontstaat meestal als gevolg van het clientgeheim dat aan de clientnaam is gekoppeld, ongeldig is. Dit gebeurt vaak wanneer het cliëntgeheim wordt gegenereerd, maar niet wordt opgeslagen
 - Oplossing:
 - Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
 - Klik op Gebruikersnaam (rechterbovenhoek) > Beheer.
 - Klik op het tabblad API-client om bestaande API-clients te bekijken.
 - Selecteer de API-client waarvoor u de fout krijgt.

- Klik op Geheim genereren om een nieuw clientgeheim te genereren en klik op Opslaan (rechterbovenhoek)

- Lege reactie.

- Probleem: gebruikers krijgen te maken met een leeg antwoord wanneer ze een REST-eindpunt opvragen, zelfs nadat ze een toegangstoken succesvol hebben gegenereerd.
- Voorbeeldreactie:

- Root Cause: Het probleem ontstaat meestal als gevolg van onvoldoende rollen of machtigingen toegewezen aan de API-client. Zonder de benodigde rollen kan de API-client de verwachte gegevens van het eindpunt niet ophalen.
- Oplossing:
 - Meld u aan bij de controller-gebruikersinterface als een rol voor de accounteigenaar of een rol met de machtiging voor beheer, agents en de wizard Aan de slag.
 - Klik op Gebruikersnaam (rechterbovenhoek) > Beheer.
 - Klik op het tabblad API-client om bestaande API-clients te bekijken.
 - Selecteer de API-client waarvoor u de rol wilt toewijzen
 - Klik op + Toevoegen in rollen sectie om de rol toe te voegen.
 - Klik rechtsboven op Opslaan.



Opmerking: Zorg ervoor dat de API-client de juiste rollen heeft toegewezen. Rollen moeten worden afgestemd op de gegevenstoegangsvereisten van het REST-eindpunt.

- Ongeldig type inhoud

- Probleem: gebruiker krijgt een 500 Internal Server-fout wanneer hij probeert een toegangstoken te genereren.
- Voorbeeldfout:

HTTP ERROR 500 javax.servlet.ServletException: java.lang.Illeg

- Hoofdoorzaak: het probleem ontstaat als gevolg van het inhoudstype header. In de Controller versie 10.10 is het inhoudstype gewijzigd van `application/vnd.appd.cntrl+json; v=1` naar `application/x-www-form-urlencoded`
 - Oplossing:
 - Wijzig de koptekst voor het aanvraagtype en stel het inhoudstype in op `application/x-www-form-urlencoded`
- Voorbeeld:

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" "https://
```

```
/controller/api/oauth/access_token" -d 'grant_type=client_credentials&client_id=
```

```
@
```

```
&client_secret=
```

```
,
```

Gerelateerde informatie

[AppDynamics-documentatie](#)

[Splunk AppDynamics API's](#)

[API-clients](#)

[Toegangstokens beheren](#)

Meer 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.
- Gebruikte opdracht: Geef de exacte opdracht op die u hebt uitgevoerd toen het probleem zich voordeed.
- Controller Server.log (alleen On-Prem): indien van toepassing, geef de controllerserverlogs op van <controller-install-dir>/logs/server.log*

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.