# AppDynamics API-Client konfigurieren und Fehlerbehebung dafür durchführen

## Inhalt


- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
- Hintergrundinformationen
- Konfigurieren
  - Erstellen eines API-Clients
  - Vorhandenen API-Client anzeigen
  - Vorhandenen API-Client löschen
  - Zugriffstoken erstellen
    - Administrator-Benutzeroberfläche (langlebige Token)
    - OAuth-API (Short-alive-Token)
  - Manange-Zugriffstoken
    - Zugriffstoken neu generieren
    - Zugriffs-Token aufheben
  - Zugriffs-Token für REST-API verwenden
- Häufige Probleme und Lösung
  - 401Unautorisiert
  - Leere Antwort.
  - Ungültiger Inhaltstyp
- Zugehörige Informationen
- Benötigen Sie weitere Unterstützung?


## Einleitung

In diesem Dokument wird beschrieben, wie Sie einen AppDynamics API-Client erstellen, Token generieren und Probleme beheben.

## Voraussetzungen

### Anforderungen

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

- Um einen API-Client zu erstellen, muss der Benutzer über die Rolle des Kontoinhabers (Standard) oder eine benutzerdefinierte Rolle mit der Berechtigung Administration, Agents und Assistent für den Einstieg verfügen.

### 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.

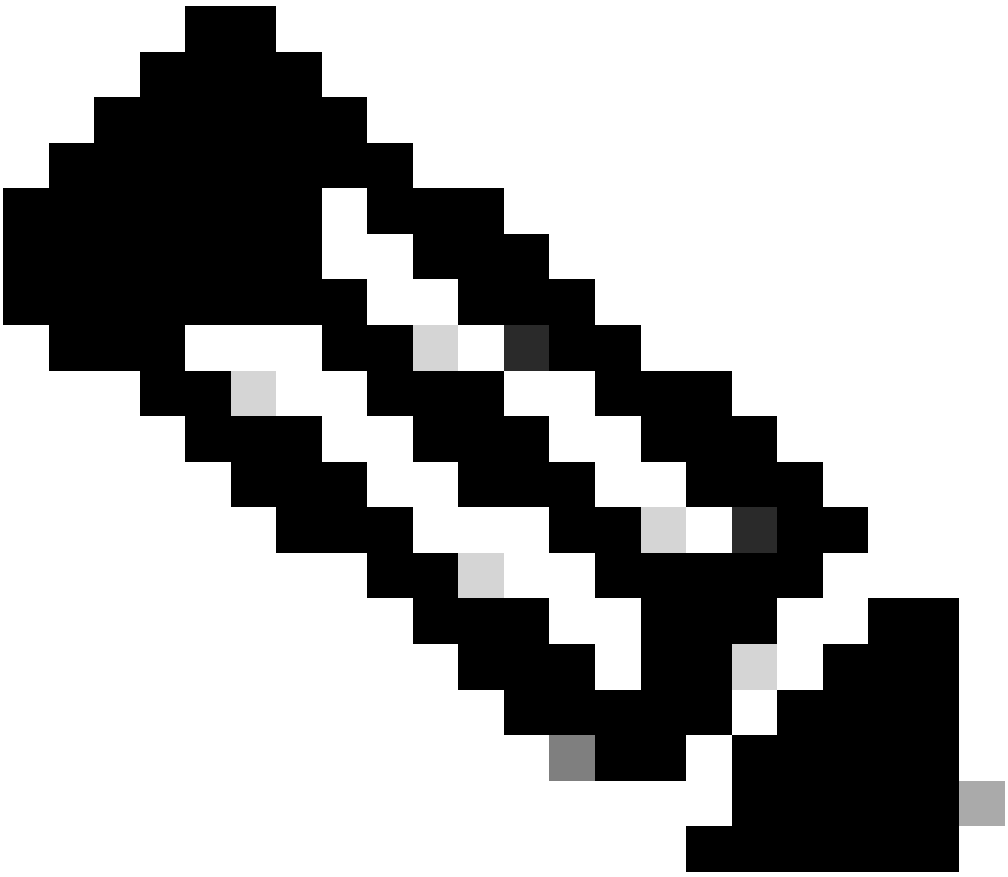
## Hintergrundinformationen

In diesem Dokument wird der Prozess zum Erstellen von API-Clients für den sicheren Zugriff auf die Daten vom AppDynamics-Controller mithilfe von REST- (Representational State Transfer) und API-Aufrufen (Application Programming Interface) beschrieben. Die API-Clients verwenden die OAuth-tokenbasierte Authentifizierung (Open Authorization). Mit OAuth können Dienste von Drittanbietern auf Kontoinformationen von Endbenutzern zugreifen, ohne die Anmeldeinformationen des Benutzers offenzulegen. Sie fungiert als Vermittler und stellt dem Drittanbieterdienst einen Zugriffstoken zur Verfügung, der die Freigabe bestimmter Kontoinformationen autorisiert. Benutzer können das OAuth-Token nach dem Einrichten des API-Clients generieren. Darüber hinaus wird in diesem Dokument die Behebung gängiger Probleme behandelt, die bei der Verwendung von API-Clients auftreten.

## Konfigurieren

### Erstellen eines API-Clients

1. 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.
2. Klicken Sie auf Benutzername (oben rechts) > Administration (Verwaltung).
3. Klicken Sie auf die Registerkarte API-Client.
4. Klicken Sie auf + Erstellen.
5. Geben Sie den Kundennamen und die Beschreibung ein.
6. Klicken Sie auf Geheimen Schlüssel generieren, um den geheimen Clientschlüssel auszufüllen.



Anmerkung: Der Client-Schlüssel wird nur einmal generiert und angezeigt. Diese Informationen kopieren und sicher speichern.

7. Legen Sie den Standard-Tokenablauf fest.
8. Klicken Sie auf + In Roles (Rollen hinzufügen), um die Rolle hinzuzufügen.
9. Klicken Sie oben rechts auf Speichern.

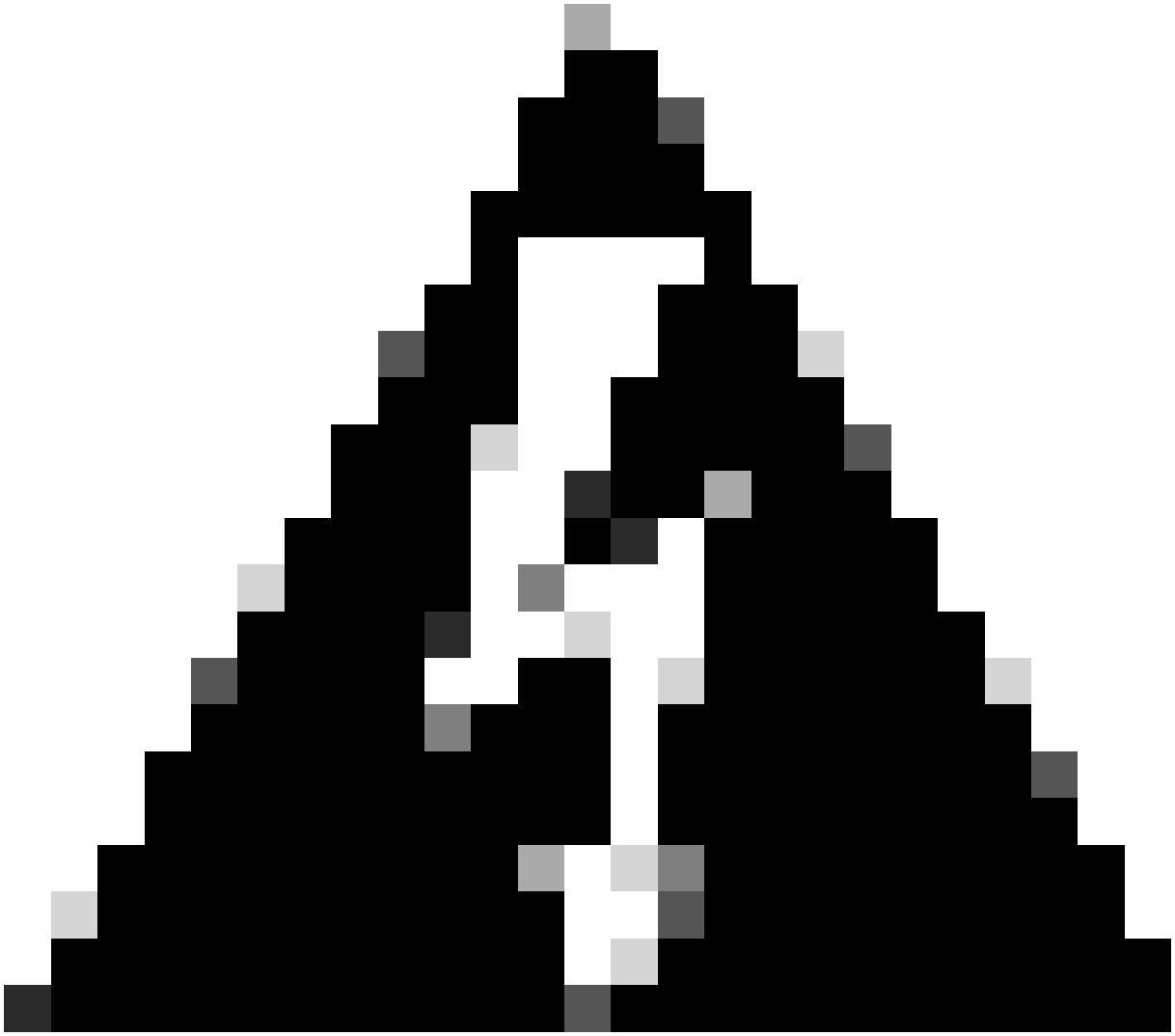
## Vorhandenen API-Client anzeigen

1. 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.
2. Klicken Sie auf Benutzername (obere rechte Ecke) > Administration (Verwaltung).
3. Klicken Sie auf die Registerkarte API-Client, um vorhandene API-Clients anzuzeigen.

## Vorhandenen API-Client löschen

1. 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.
2. Klicken Sie auf Ihren Benutzernamen (obere rechte Ecke) > Administration > API Clients.
3. Suchen Sie nach den API-Clients, die Sie löschen möchten, und wählen Sie sie aus.
4. Klicken Sie auf das Symbol Löschen oder klicken Sie mit der rechten Maustaste auf den/die ausgewählten API-Client(s) und wählen Sie API-Client(s löschen, um die vorhandenen API-Clients zu löschen.

---



Warnung: Durch das Löschen des API-Clients wird das Token ungültig.

---

## Zugriffstoken erstellen

Das Zugriffstoken kann über die Administratorbenutzeroberfläche oder die OAuth-API generiert werden. Die Benutzeroberfläche stellt langlebige Token bereit, während die OAuth-API kurzlebige, regelmäßig aktualisierte Token generiert.

- Administrator-Benutzeroberfläche (langlebige Token)
    - 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 > API Clients.
    - Wählen Sie den API-Client aus, für den Sie das Zugriffstoken generieren möchten, und klicken Sie auf Temporäres Zugriffstoken generieren.
    - Die über die Benutzeroberfläche generierten Zugriffstoken haben eine längere Ablaufzeit.

- OAuth-API (Short-alive-Token)
    - `Sie können REST-APIs verwenden, um ein kurzlebiges Zugriffstoken zu generieren.

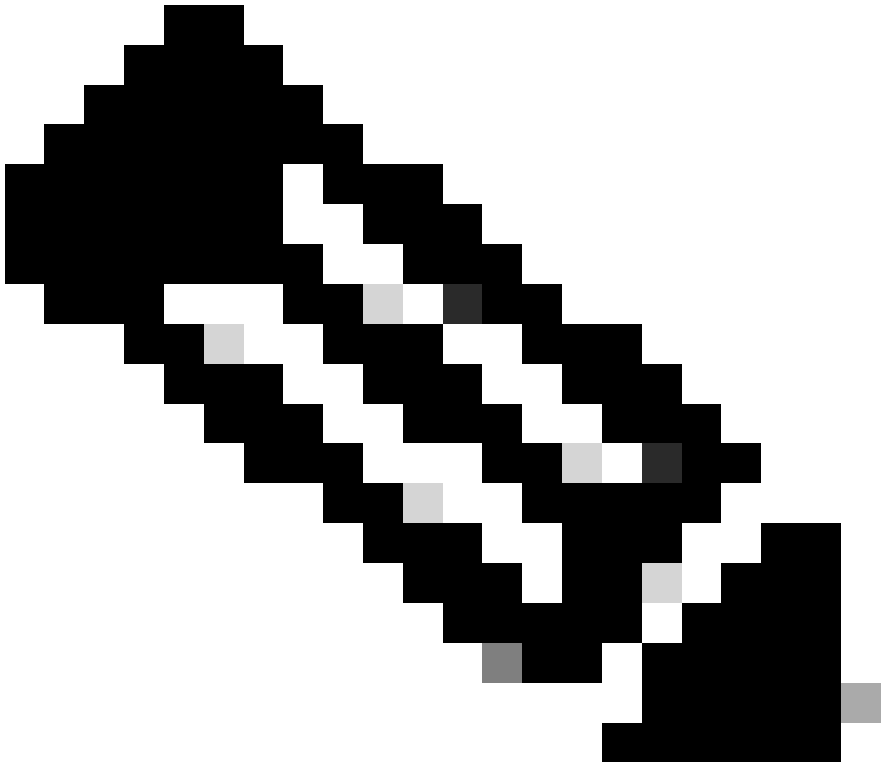
```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" "https://

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

             @

              &client_secret=

                '
```

Ersetzen:

- mit dem Client-Namen, den Sie bei der Erstellung des API-Clients eingegeben haben oder der von Ihrem Administrator freigegeben wurde.

- mit dem Kontonamen.
- mit dem Clientschlüssel, den Sie beim Erstellen des API-Clients generiert haben oder der von Ihrem Administrator freigegeben wurde.

---



Anmerkung: Ein On-Demand-Token wird auf der Benutzeroberfläche nicht nachverfolgt.

---

Beispielantwort:

```
{
"access_token": "


              ",
"expires_in": 300
}
```

## Manange-Zugriffstoken

- Zugriffstoken, die von der REST-API generiert werden, können nur durch Löschen des zugeordneten API-Clients ungültig gemacht werden.
- Zugriffstoken, die über die Benutzeroberfläche des Controllers generiert werden, können widerrufen oder neu generiert werden.
- Durch das Regenerieren eines Zugriffstokens werden die vorherigen Token nicht ungültig gemacht. Die älteren Token bleiben bis zu ihrem Ablauf aktiv.
- Es ist nicht möglich, vorherige oder aktuell gültige Token abzurufen. Daher kann nur das aktuelle Token widerrufen werden.

    - Zugriffstoken neu generieren

        - 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 > API Clients.
        - Wählen Sie den API-Client aus, für den Sie das Zugriffstoken neu generieren möchten, und klicken Sie auf Regenerieren > Speichern (oben rechts).

    - Zugriffs-Token aufheben

        - 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 > API Clients.
        - Wählen Sie den API-Client aus, für den Sie das Zugriffstoken widerrufen möchten, und klicken Sie auf Widerrufen > Speichern (oben rechts).

## Zugriffs-Token für REST-API verwenden

- Von Splunk AppDynamics APIs dBestimmen Sie den Endpunkt, mit dem Sie interagieren müssen.
- Konstruiert die Anforderung:
    - Methode: Wählen Sie die HTTP-Methode (GET, POST, PUT, DELETE) basierend auf der auszuführenden Aktion aus.
    - Headers: Fügen Sie das Zugriffstoken im Autorisierungs-Header hinzu.
    - Text (falls vorhanden): Fügen Sie den Anforderungstext im JavaScript Object Notation (JSON)-Format hinzu.

- Beispielanforderung

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

```
/controller/

' --header 'Authorization: Bearer

'
```

Ersetzen:

- mit der Controller-URL.
- mit dem Rest-Endpunkt, mit dem Sie interagieren müssen.
- mit dem Zugriffstoken, das unter Verwendung des Client-Namens und des Client-Schlüssels generiert wird.

# Häufige Probleme und Lösung

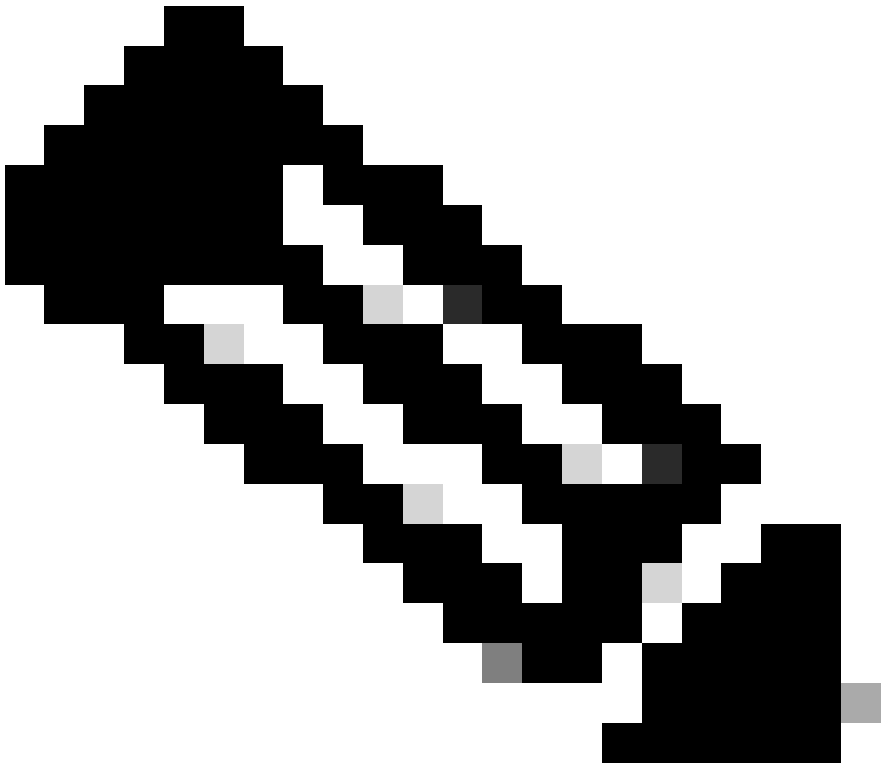
- 401 Nicht autorisiert
  - Problem: Beim Generieren eines Zugriffstokens tritt ein 401-Fehler auf, der nicht autorisiert ist.
  - Beispielantwort:

```
HTTP Error 401 Unauthorized

This request requires HTTP authentication
```

  - Ursache: Das Problem tritt in der Regel auf, weil der dem Client-Namen zugeordnete geheime Schlüssel ungültig ist. Dies geschieht häufig, wenn der geheime Schlüssel des Clients generiert, aber nicht gespeichert wird
  - Lösung:

    - 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 Benutzername (obere rechte Ecke) > Administration (Verwaltung).
    - Klicken Sie auf die Registerkarte API Client, um vorhandene API-Clients anzuzeigen.
    - Wählen Sie den API-Client aus, für den der Fehler ausgegeben wird.
    - Klicken Sie auf Geheimen Schlüssel generieren, um den neuen Schlüssel zu generieren, und klicken Sie auf Speichern (oben rechts).

- Leere Antwort.
    - Problem: Benutzer stoßen bei der Abfrage eines REST-Endpunkts auf eine leere Antwort, auch nachdem ein Zugriffstoken erfolgreich generiert wurde.
    - Beispielantwort:
    - Ursache: Das Problem tritt in der Regel auf, weil dem API-Client nicht genügend Rollen oder Berechtigungen zugewiesen wurden. Ohne die erforderlichen Rollen kann der API-Client die erwarteten Daten nicht vom Endpunkt abrufen.
    - Lösung:
        - 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 Benutzername (obere rechte Ecke) > Administration (Verwaltung).
        - Klicken Sie auf die Registerkarte API-Client, um vorhandene API-Clients anzuzeigen.
        - Wählen Sie den API-Client aus, dem Sie die Rolle zuweisen möchten.
        - Klicken Sie auf + In Roles (Rollen hinzufügen), um die Rolle hinzuzufügen.
        - Klicken Sie oben rechts auf Speichern.



Anmerkung: Stellen Sie sicher, dass dem API-Client die entsprechenden Rollen zugewiesen sind. Die Rollen müssen mit den Datenzugriffsanforderungen des REST-Endpunkts übereinstimmen.

---

- Ungültiger Inhaltstyp
  - Problem: Der Benutzer hat beim Versuch, ein Zugriffstoken zu generieren, einen 500-internen Serverfehler festgestellt.
  - Beispielfehler:

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

  - Ursache: Das Problem tritt aufgrund des Content-Typ-Headers auf. In der Controller-Version 24.10 wurde der Inhaltstyp von application/vnd.appd.cntrl+json;v=1 in application/x-www-form-urlencoded geändert.
  - Lösung:
    - Ändern Sie die Anforderung, und legen Sie den Content-Typ-Header auf application/x-www-form-urlencoded fest.
      Beispiel:

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

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

@

&client_secret=

'
```

---

## Zugehörige Informationen

AppDynamics-Dokumentation

Splunk-AppDynamics-APIs

API-Clients

Zugriffstoken verwalten

## Benötigen Sie weitere Unterstützung?

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

- Fehlerdetails oder Screenshot: Geben Sie eine spezielle Fehlermeldung oder einen Screenshot des Problems an.
- Verwendeter Befehl: Geben Sie den genauen Befehl an, den Sie ausgeführt haben, als das Problem auftrat.
- Controller Server.log (nur standortbasiert): Geben Sie ggf. die Controller-Serverprotokolle von <controller-install-dir>/logs/server.log* an.

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.