Configurer et dépanner le client AppDynamics API

Table des matières

Introduction

Ce document décrit comment créer un client AppDynamics API, générer des jetons et résoudre des problèmes.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pour créer un client API, un utilisateur doit avoir un rôle Propriétaire de compte (par défaut) ou un rôle personnalisé avec l'autorisation Administration, Agents, Assistant Mise en route.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur AppDynamics

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

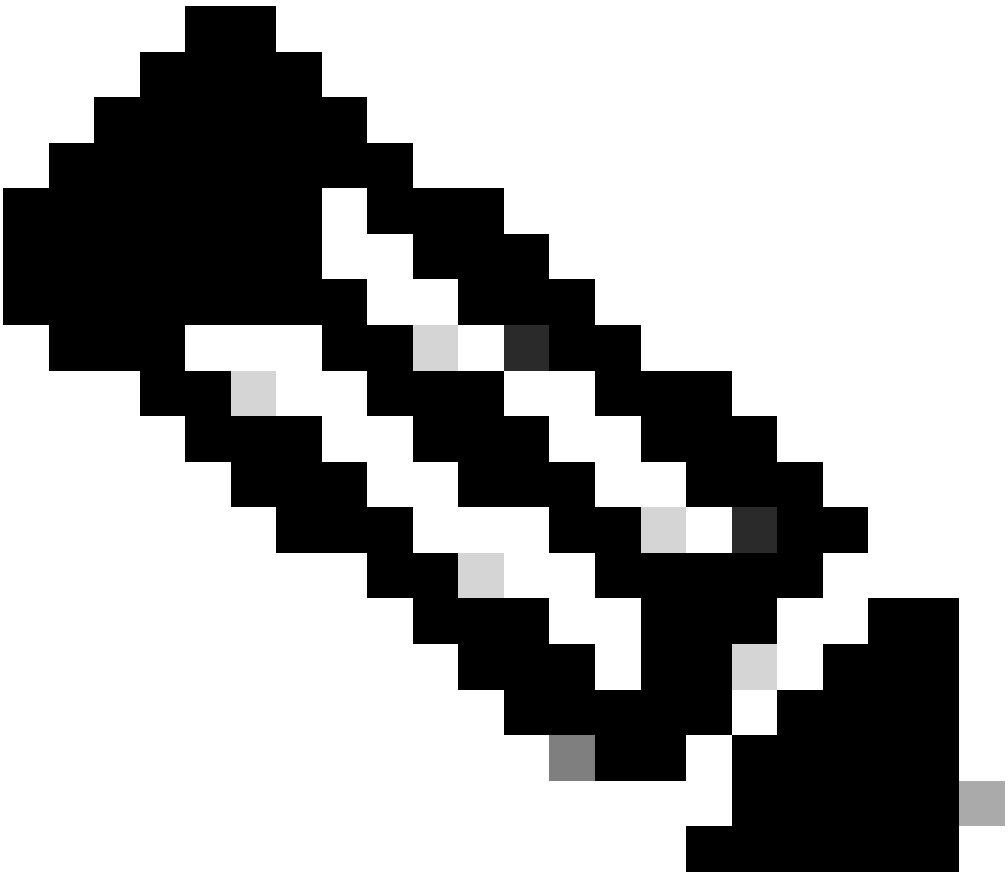
Informations générales

Ce document décrit le processus de création de clients API pour accéder en toute sécurité aux données à partir du contrôleur AppDynamics à l'aide des appels REST (Representational State Transfer) et API (Application Programming Interface). Les clients API utilisent l'authentification basée sur jeton Open Authorization (OAuth). OAuth permet aux services tiers d'accéder aux informations de compte d'un utilisateur final sans exposer les informations d'identification de l'utilisateur. Il agit en tant qu'intermédiaire, en fournissant au service tiers un jeton d'accès qui autorise le partage d'informations de compte spécifiques. Les utilisateurs peuvent générer le jeton OAuth après avoir configuré le client API. En outre, ce document couvre le dépannage des problèmes courants rencontrés lors de l'utilisation des clients API.

Configurer

Créer un client API

1. Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
2. Cliquez sur Nom d'utilisateur (en haut à droite) > Administration.
3. Cliquez sur l'onglet Client API.
4. Cliquez sur + Créer.
5. Saisissez le nom et la description du client.
6. Cliquez sur Generate Secret pour renseigner le champ Client Secret.



Remarque : Le secret client est généré et affiché une seule fois. Copiez et stockez ces informations en toute sécurité.

7. Définissez l'expiration du jeton par défaut.
8. Cliquez sur + Ajouter dans la section Rôles pour ajouter le rôle.
9. Cliquez sur Save en haut à droite.

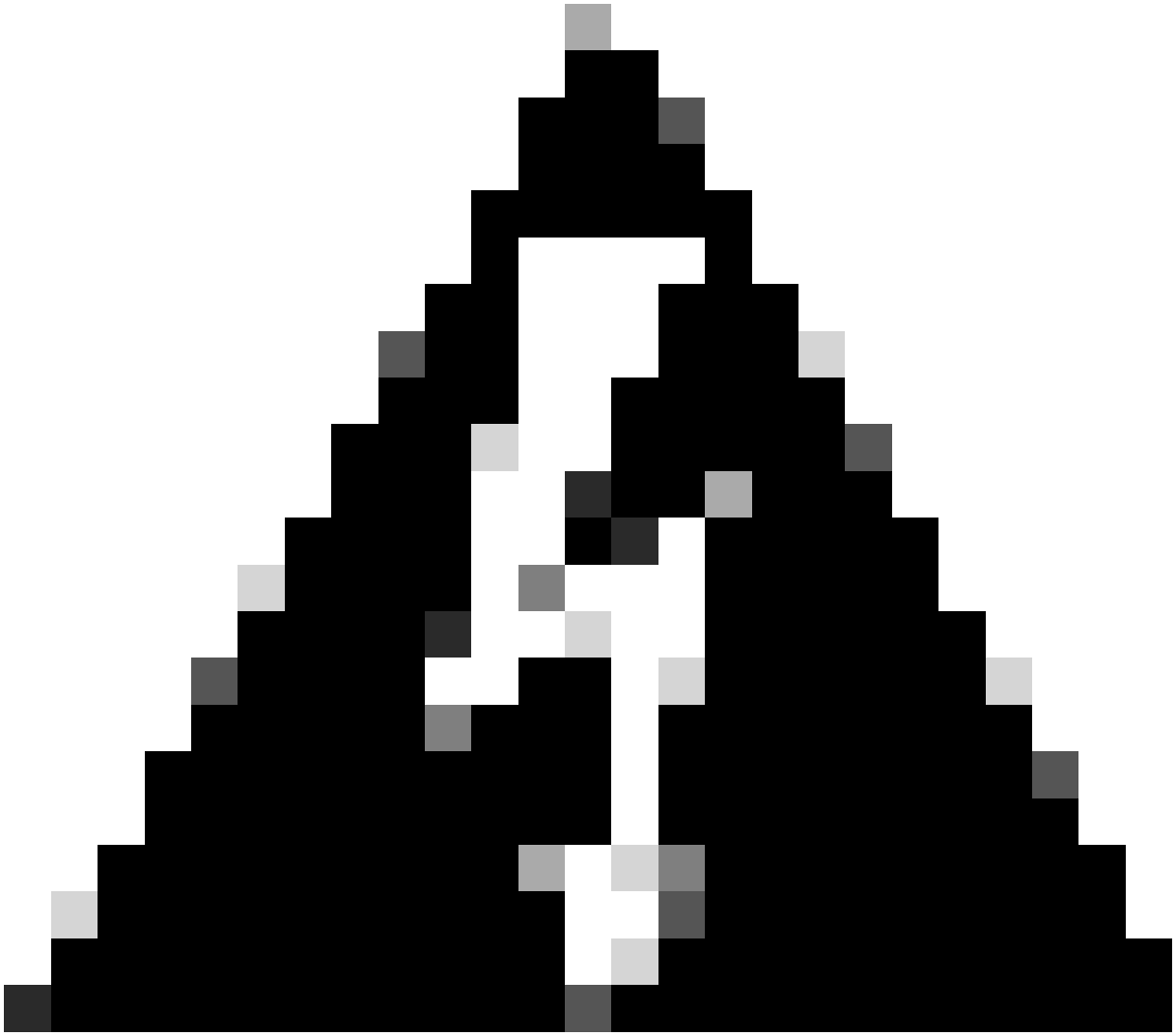
Afficher le client API existant

1. Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
2. Cliquez sur Nom d'utilisateur (coin supérieur droit) > Administration.
3. Cliquez sur l'onglet Client API pour afficher les clients API existants.

Supprimer le client API existant

1. Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de

compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
2. Cliquez sur votre nom d'utilisateur (en haut à droite) > Administration > API Clients.
3. Recherchez les clients API spécifiques que vous souhaitez supprimer et sélectionnez-les.
4. Cliquez sur l'icône Delete ou cliquez avec le bouton droit sur le ou les clients API sélectionnés et sélectionnez Delete API Client(s) pour supprimer le ou les clients API existants.



Avertissement : La suppression du client API invalide le jeton.

Générer un jeton d'accès

Le jeton d'accès peut être généré via l'interface utilisateur de l'administrateur ou l'API OAuth. L'interface utilisateur fournit des jetons à longue durée de vie, tandis que l'API OAuth génère des jetons à courte durée de vie régulièrement actualisés.

- Interface utilisateur de l'administrateur (jetons de longue durée)

- Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
- Cliquez sur votre nom d'utilisateur (en haut à droite) > Administration > API Clients.
- Sélectionnez le client API pour lequel vous voulez générer le jeton d'accès et cliquez sur Generate Temporary Access Token.
- Les jetons d'accès générés à partir de l'interface utilisateur ont un délai d'expiration plus long.

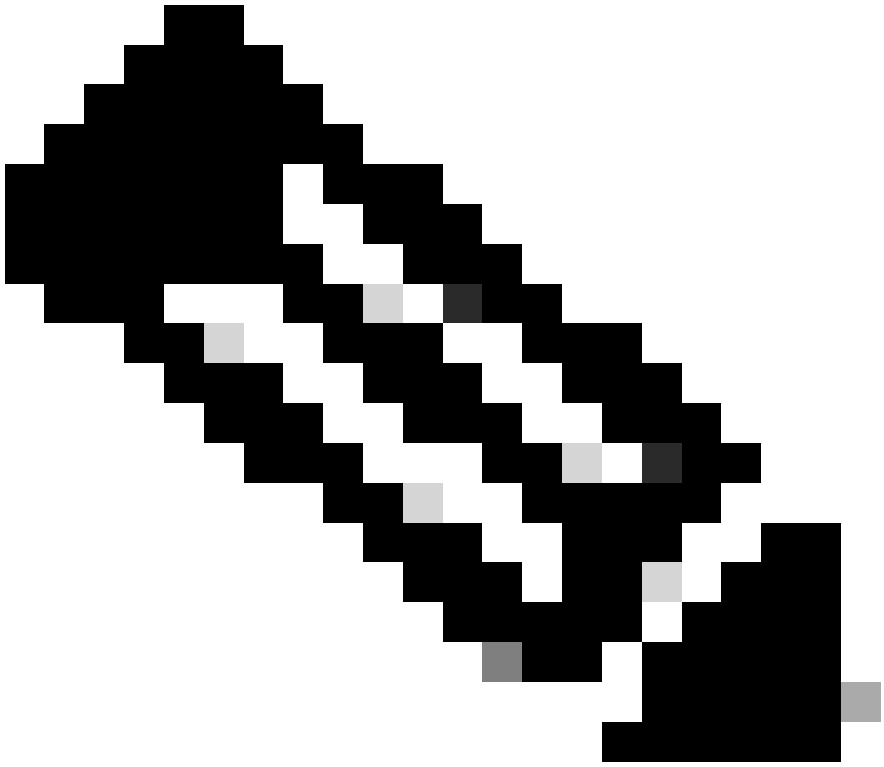
- API OAuth (jetons à durée de vie courte)
  - `Vous pouvez utiliser des API REST pour générer un jeton d'accès de courte durée.

```
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=

                '
```

Remplacer :

- avec le nom de client que vous avez entré lors de la création du client API ou tel que partagé par votre administrateur.
- avec le nom du compte.

avec le secret client que vous avez généré lors de la création du client API ou tel que partagé par votre administrateur.



Remarque : Le jeton à la demande n'est pas suivi sur l'interface utilisateur.

Exemple de réponse :

```
{
"access_token": "


              ",
"expires_in": 300
}
```

Gérer les jetons d'accès

- Les jetons d'accès générés à partir de l'API REST ne peuvent être invalidés qu'en supprimant le client API associé.

- Les jetons d'accès générés via l'interface utilisateur du contrôleur peuvent être révoqués ou régénérés.
- La régénération d'un jeton d'accès n'invalide pas les jetons précédents. Les anciens jetons restent actifs jusqu'à leur expiration.
- Il n'existe aucun moyen de récupérer des jetons valides précédents ou actuels. Par conséquent, seul le jeton actuel peut être révoqué.

    - Régénérer le jeton d'accès

        - Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
        - Cliquez sur votre nom d'utilisateur (en haut à droite) > Administration > API Clients.
        - Sélectionnez le client API pour lequel vous voulez régénérer le jeton d'accès, cliquez sur Regenerate > Save (coin supérieur droit).

    - Revoke Access Token

        - Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
        - Cliquez sur votre nom d'utilisateur (coin supérieur droit) > Administration > API Clients.
        - Sélectionnez le client API pour lequel vous voulez révoquer le jeton d'accès, cliquez sur Revoke > Save (coin supérieur droit).

Utiliser le jeton d'accès pour créer l'API Rest

- À partir des API AppDynamics Splunk dDéterminez le terminal spécifique avec lequel vous devez interagir.
- Construire la requête :
    - Méthode : Sélectionnez la méthode HTTP (GET, POST, PUT, DELETE) en fonction de l'action que vous souhaitez effectuer.
    - En-têtes : ajoutez le jeton d'accès dans l'en-tête d'autorisation.
    - Corps (le cas échéant) : Ajoutez le corps de la demande au format JSON (JavaScript Object Notation).

- Exemple de demande

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

        /controller/
```

```
' --header 'Authorization: Bearer

'
```

Remplacer :

- avec l'URL du contrôleur.
- avec le terminal de repos avec lequel vous devez interagir.
- avec le jeton d'accès généré à l'aide du nom et du secret du client.

Problèmes courants et solution

- 401 Non Autorisé
  - Problème : Les utilisateurs rencontrent une erreur 401 Unauthorized lors de la tentative de génération d'un jeton d'accès.
  - Exemple de réponse :

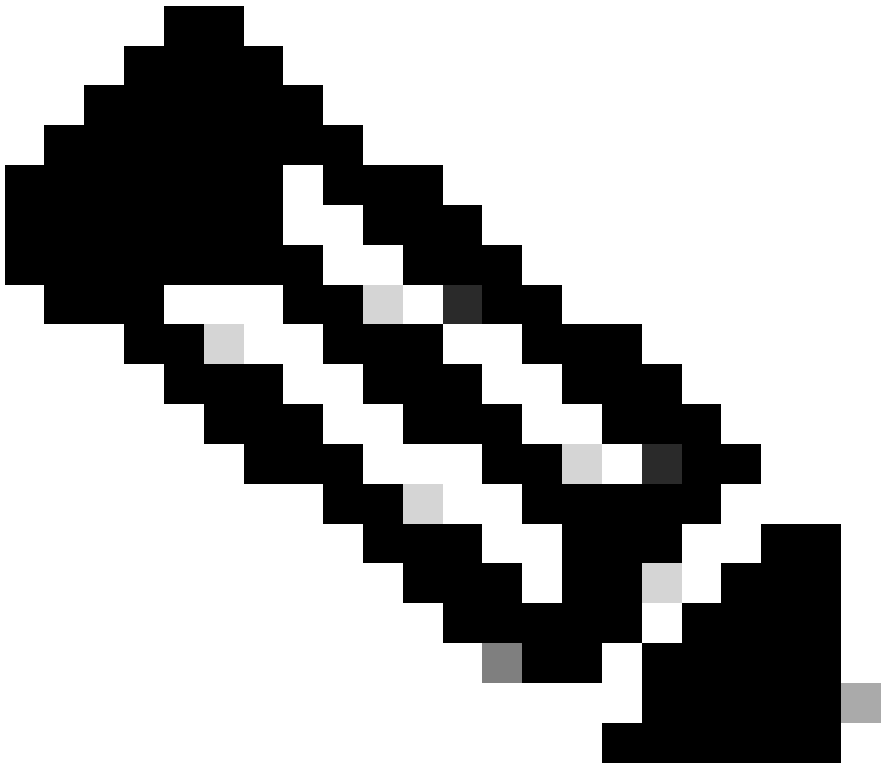
```
HTTP Error 401 Unauthorized

This request requires HTTP authentication
```

  - Cause première : le problème se produit généralement en raison de la non-validité du secret client associé au nom du client. Cela se produit souvent lorsque le secret client est généré mais pas enregistré
  - Solution :
    - Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
    - Cliquez sur Nom d'utilisateur (coin supérieur droit) > Administration.
    - Cliquez sur l'onglet Client API pour afficher les clients API existants.

    - Sélectionnez le client API pour lequel vous obtenez l'erreur.
    - Cliquez sur Generate Secret pour générer une nouvelle clé secrète client et cliquez sur Save (en haut à droite)

- Réponse vide.
    - Problème : Les utilisateurs obtiennent une réponse vide lorsqu'ils demandent un point de terminaison REST, même après avoir généré un jeton d'accès.
    - Exemple de réponse :

    - Cause première : Le problème se pose généralement en raison d'un nombre insuffisant de rôles ou d'autorisations attribués au client API. Sans les rôles nécessaires, le client API ne peut pas récupérer les données attendues à partir du point de terminaison.
    - Solution :
        - Connectez-vous à l'interface utilisateur du contrôleur en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
        - Cliquez sur Nom d'utilisateur (coin supérieur droit) > Administration.
        - Cliquez sur l'onglet Client API pour afficher les clients Api existants.
        - Sélectionnez le client API auquel vous souhaitez attribuer le rôle
        - Cliquez sur + Ajouter dans la section Rôles pour ajouter le rôle.
        - Cliquez sur Save en haut à droite.



Remarque : Assurez-vous que les rôles appropriés sont attribués au client API. Les rôles doivent correspondre aux exigences d'accès aux données du terminal REST.

- Type de contenu non valide
  - Problème : L'utilisateur rencontre une erreur 500 Internal Server lors de la tentative de génération d'un jeton d'accès.
  - Exemple d'erreur :

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

  - Cause première : Le problème se pose en raison de l'en-tête du type de contenu. Dans la version 24.10 du contrôleur, le type de contenu est passé de application/vnd.appd.cntrl+json;v=1 à application/x-www-form-urlencoded
  - Solution :
    - Modifiez la requête et définissez l'en-tête du type de contenu sur application/x-www-form-urlencoded
      Exemple :

```
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=

'
```

Informations connexes

[Documentation AppDynamics]

[API AppDynamics Splunk]

[Clients de l’API]

[Gérer les jetons d'accès]

Besoin d'aide supplémentaire ?

Si vous avez une question ou rencontrez des problèmes, créez un [ticket d'assistance] avec les informations suivantes :

- Détails de l'erreur ou Capture d'écran : Fournissez un message d'erreur spécifique ou une capture d'écran du problème.
- Commande utilisée : Spécifiez la commande exacte que vous étiez en train d'exécuter lorsque le problème s'est produit.
- Controller Server.log (sur site uniquement) : Le cas échéant, fournissez les journaux du serveur contrôleur depuis <controller-install-dir>/logs/server.log*

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.