Configurazione e risoluzione dei problemi del client API AppDynamics

Sommario

Introduzione

In questo documento viene descritto come creare un client API AppDynamics, generare token e risolvere i problemi.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Per creare il client API, un utente deve disporre del ruolo Proprietario account (predefinito) o di un ruolo personalizzato con l'autorizzazione Amministrazione, Agenti, Riquadro attività iniziale.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- AppDynamics Controller

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

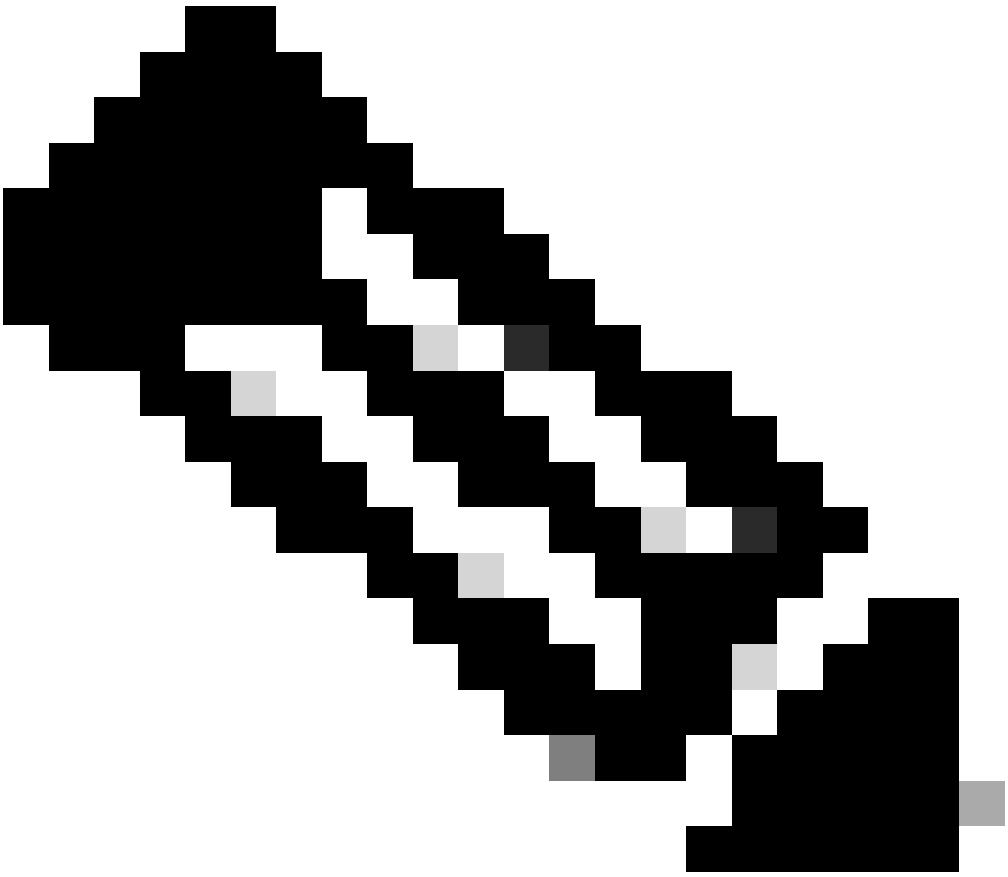
Premesse

In questo documento viene descritto il processo di creazione di client API per l'accesso protetto ai dati da AppDynamics Controller tramite chiamate REST (Representative State Transfer) e API (Application Programming Interface). I client API utilizzano l'autenticazione basata su token OAuth (Open Authorization). OAuth consente ai servizi di terze parti di accedere alle informazioni di un account utente finale senza esporre le credenziali dell'utente. Agisce da intermediario, fornendo al servizio di terze parti un token di accesso che autorizza la condivisione di informazioni specifiche sull'account. Gli utenti possono generare il token OAuth dopo aver configurato il client API. Inoltre, questo documento descrive la risoluzione dei problemi più comuni incontrati durante l'uso dei client API.

Configurazione

Crea un client API

1. Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
2. Fare clic su Nome utente (in alto a destra) > Amministrazione.
3. Fare clic su API Client Tab.
4. Fate clic su + Crea (Create).
5. Immettere il nome del client e la descrizione.
6. Fare clic su Genera segreto per popolare il segreto client.



Nota: Il segreto client viene generato e visualizzato una sola volta. Copiare e memorizzare queste informazioni in modo sicuro.

7. Impostare la scadenza predefinita del token.

8. Fare clic su + Aggiungi in sezione Ruoli per aggiungere il ruolo.
9. Fare clic su Save (Salva) in alto a destra.

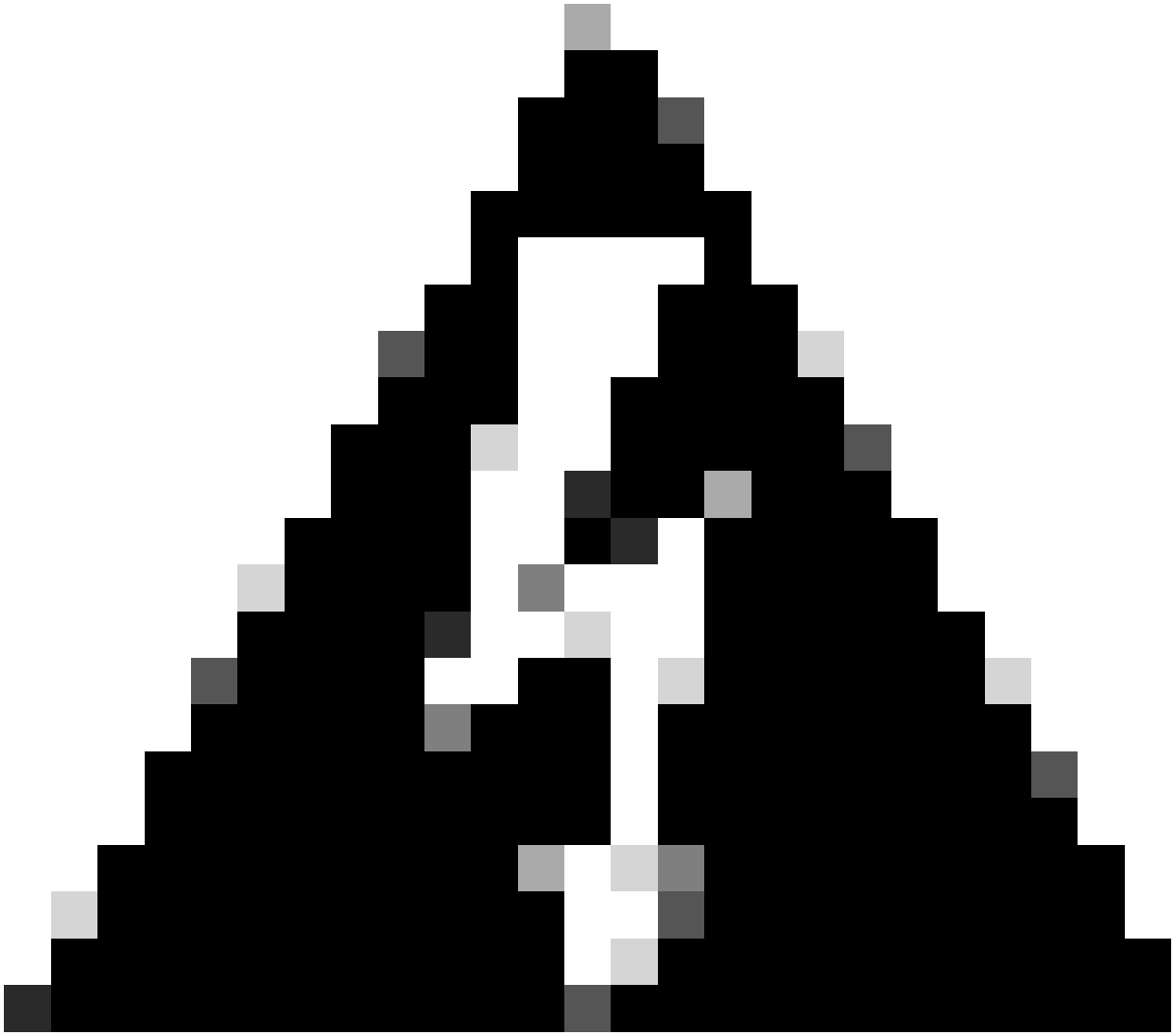
Visualizza client API esistente

1. Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
2. Fare clic su Nome utente (angolo superiore destro) > Amministrazione.
3. Fare clic sulla scheda Client API per visualizzare i client API esistenti.

Elimina client API esistente

1. Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con

l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
2. Fare clic su Nome utente (angolo superiore destro) > Amministrazione > Client API.
3. Individuare i client API specifici da eliminare e selezionarli.
4. Fare clic sull'icona Delete o fare clic con il pulsante destro del mouse sui client API selezionati e selezionare Delete API Client(s) per eliminare i client API esistenti.



Avviso: L'eliminazione del client API invalida il token.

Genera token di accesso

Il token di accesso può essere generato tramite l'interfaccia utente dell'amministratore o l'API OAuth. L'interfaccia utente fornisce token di lunga durata, mentre l'API OAuth genera token di breve durata e regolarmente aggiornati.

- Interfaccia utente amministratore (token di lunga durata)
    - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o

con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
- Fare clic su Nome utente (angolo superiore destro) > Amministrazione > Client API.
- Selezionare il client API per il quale si desidera generare il token di accesso e fare clic su Genera token di accesso temporaneo.
- I token di accesso generati dall'interfaccia utente hanno una scadenza più lunga.

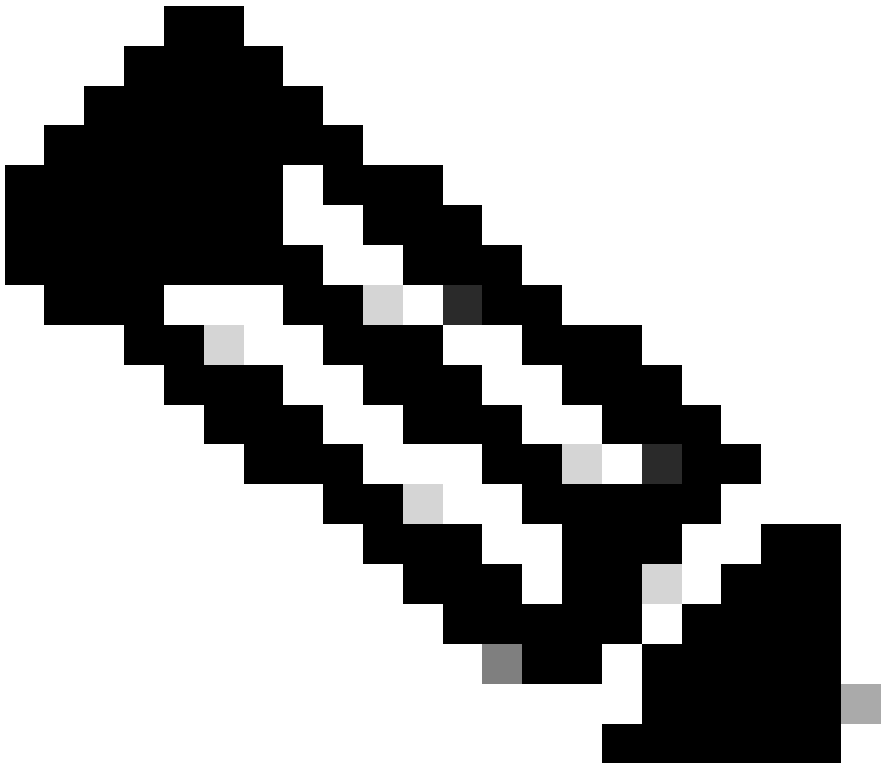
- API OAuth (token di breve durata)
  - `È possibile utilizzare le API REST per generare un token di accesso di breve durata.

```
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=

                '
```

Sostituisci:

- con il Nome client immesso durante la creazione del client API o come condiviso dall'amministratore.
- con il Nome account.
- con il segreto client generato durante la creazione del client API o come

condiviso dall'amministratore.



Nota: Token su richiesta non rilevato nell'interfaccia utente.

Esempio di risposta:

```
{
"access_token": "


              ",
"expires_in": 300
}
```

Gestisci token di accesso

- I token di accesso generati dall'API REST possono essere invalidati solo eliminando il client API associato.
- I token di accesso generati tramite l'interfaccia utente del controller possono essere revocati o rigenerati.

- La rigenerazione di un token di accesso non invalida i token precedenti. I token meno recenti rimangono attivi fino alla scadenza.
- Non è possibile recuperare i token precedenti o attualmente validi. Pertanto, solo il token corrente può essere revocato.

    - Rigenera token di accesso

        - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
        - Fare clic su Nome utente (angolo superiore destro) > Amministrazione > Client API.
        - Selezionare il client API per il quale si desidera rigenerare il token di accesso, fare clic su Rigenera > Salva (angolo in alto a destra).

    - Revoca token di accesso

        - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
        - Fare clic sul nome utente (angolo superiore destro) > Amministrazione > Client API.
        - Selezionare il client API per il quale si desidera revocare il token di accesso, fare clic su Revoca > Salva (angolo in alto a destra).

Usa token di accesso per rendere l'API Rest

- Da API Splunk AppDynamics dDeterminare l'endpoint specifico con cui interagire.
- Creare la richiesta:
    - Metodo: Selezionare il metodo HTTP (GET, POST, PUT, DELETE) in base all'azione che si desidera eseguire.
    - Intestazioni: aggiungere il token di accesso nell'intestazione Authorization.
    - Corpo (se presente): Aggiungere il corpo della richiesta in formato JSON (JavaScript Object Notation).

- Richiesta di esempio

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

        /controller/

         ' --header 'Authorization: Bearer

          '
```

Sostituisci:

- con l'URL del controller.
- con l'endpoint restante con cui è necessario interagire.
- con il token di accesso generato utilizzando il nome e il segreto del client.

Problemi comuni e soluzioni

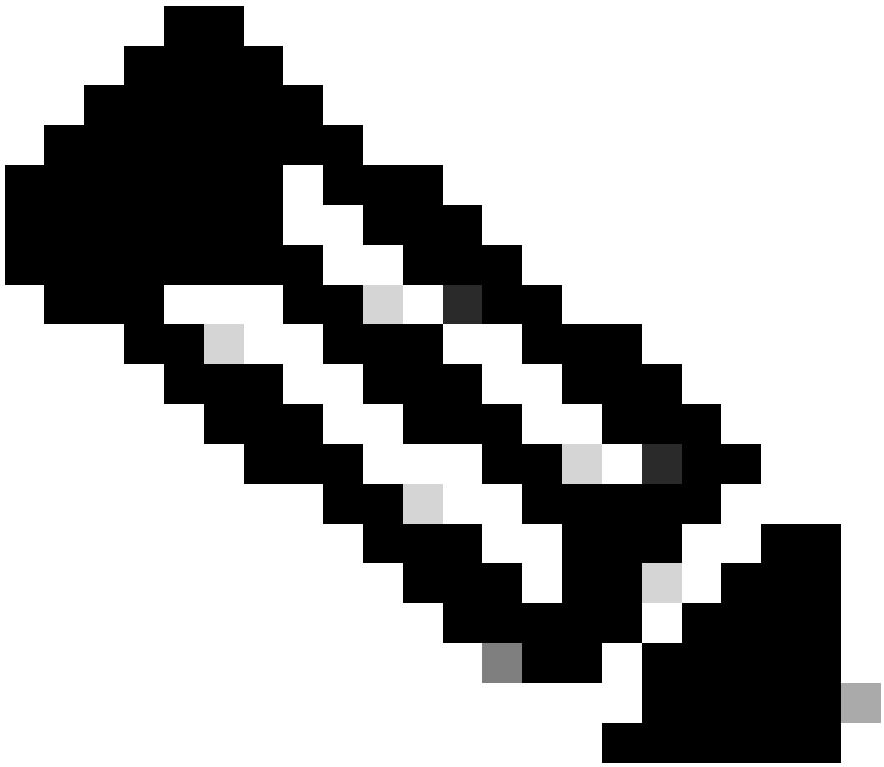
- 401 Non autorizzato
  - Problema: Errore 401 non autorizzato durante il tentativo di generare un token di accesso.
  - Risposta di esempio:

```
HTTP Error 401 Unauthorized

This request requires HTTP authentication
```

  - Causa principale: in genere il problema si verifica perché il segreto client associato al nome del client non è valido. Questo accade spesso quando il segreto client viene generato ma non salvato
  - Soluzione:
    - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
    - Fare clic su Nome utente (angolo superiore destro) > Amministrazione.
    - Fare clic sulla scheda Client API per visualizzare i client API esistenti.
    - Selezionare il client API per il quale si sta ricevendo l'errore.
    - Fare clic su Generate Secret per generare un nuovo segreto client e fare clic su Save (angolo in alto a destra).

- Risposta vuota.
    - Problema: Gli utenti ricevono una risposta vuota quando eseguono una query su un endpoint REST, anche dopo la generazione corretta di un token di accesso.
    - Risposta di esempio:

    - Causa principale: Il problema si verifica in genere a causa di ruoli o autorizzazioni insufficienti assegnati al client API. Senza i ruoli necessari, il client API non può recuperare i dati previsti dall'endpoint.
    - Soluzione:
        - Accedere all'interfaccia utente del controller come ruolo del proprietario dell'account o con l'autorizzazione Amministrazione, Agenti, Guida introduttiva.
        - Fare clic su Nome utente (angolo superiore destro) > Amministrazione.
        - Fare clic sulla scheda Client API per visualizzare i client API esistenti.
        - Selezionare il client API per il quale si desidera assegnare il ruolo
        - Fare clic su + Aggiungi in sezione Ruoli per aggiungere il ruolo.
        - Fare clic su Save (Salva) in alto a destra.



Nota: Accertarsi che al client API siano assegnati i ruoli appropriati. I ruoli devono essere allineati ai requisiti di accesso ai dati dell'endpoint REST.

- Tipo di contenuto non valido
  - Problema: Errore interno del server 500 durante il tentativo di generare un token di accesso.
  - Errore di esempio:

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

  - Causa principale: Il problema è dovuto all'intestazione del tipo di contenuto. Nel controller versione 24.10 il tipo di contenuto è stato modificato da application/vnd.appd.cntrl+json;v=1 a application/x-www-form-urlencoded
  - Soluzione:
    - Modificare la richiesta e impostare l'intestazione del tipo di contenuto su application/x-www-form-urlencoded
      Esempio:

```
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=

'
```

Informazioni correlate

[Documentazione di AppDynamics]

[API AppDynamics Splunk]

[Client API]

[Gestisci token di accesso]

Ulteriori informazioni

In caso di domande o problemi, creare una richiesta di [assistenza] con i seguenti dettagli:

- Dettagli errore o schermata: Fornire un messaggio di errore specifico o uno screenshot del problema.
- Comando utilizzato: Specificare il comando esatto che si stava eseguendo quando si è verificato il problema.
- Controller Server.log (solo in locale): Se pertinente, fornire i registri del server controller da <controller-install-dir>/logs/server.log*

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).