Configurar y solucionar problemas de AppDynamics API Client

Contenido

Introducción

Este documento describe cómo crear un cliente API de AppDynamics, generar tokens y solucionar problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Para crear un cliente de API, un usuario debe tener una función de propietario de cuenta (predeterminado) o una función personalizada con permisos de administración, agentes y asistente de inicio.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Controlador AppDynamics

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

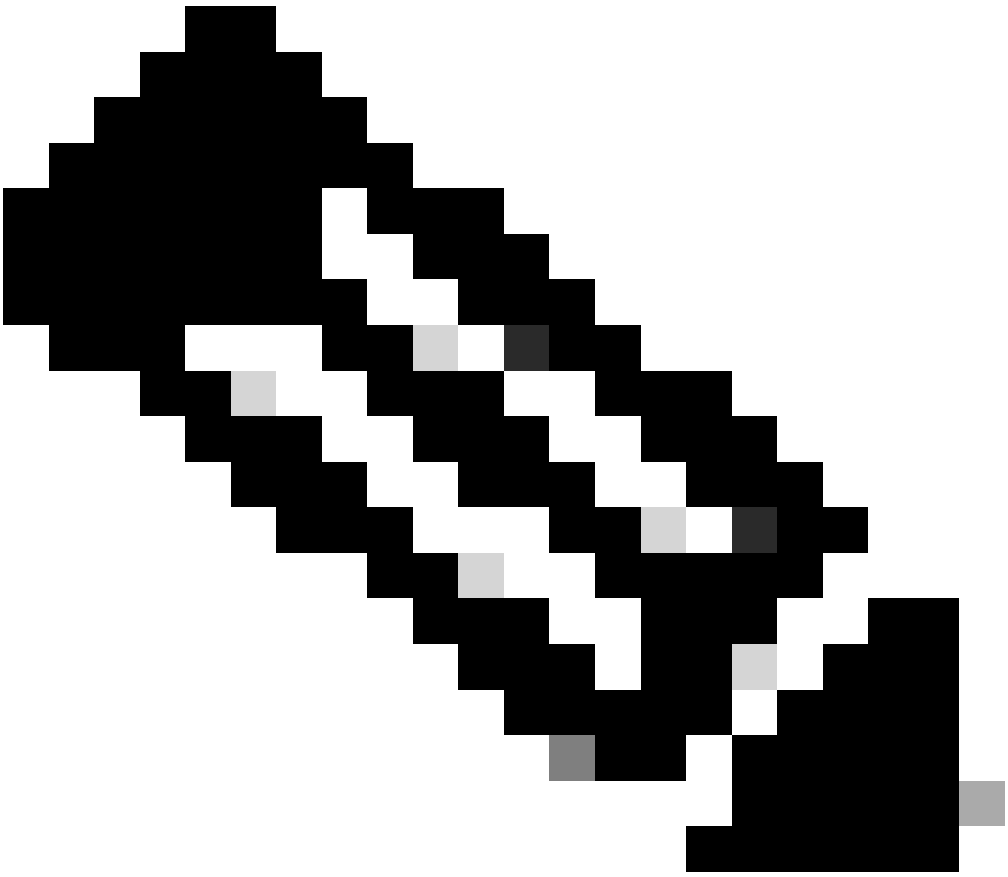
Antecedentes

Este documento describe el proceso para crear clientes de API para acceder de forma segura a los datos desde AppDynamics Controller mediante llamadas de transferencia de estado representacional (REST) y de interfaz de programación de aplicaciones (API). Los clientes de API utilizan la autenticación basada en tokens de autorización abierta (OAuth). OAuth permite que los servicios de terceros accedan a la información de una cuenta de usuario final sin exponer las credenciales del usuario. Actúa como intermediario, proporcionando al servicio de terceros un token de acceso que autoriza el uso compartido de información de cuenta específica. Los usuarios pueden generar el token de OAuth después de configurar el cliente de API. Además, este documento cubre la resolución de problemas comunes encontrados mientras se utilizan los clientes de API.

Configurar

Crear un cliente API

1. Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
2. Haga clic en Nombre de usuario (parte superior derecha) > Administración.
3. Haga clic en la ficha Cliente API.
4. Haga clic en + Crear.
5. Ingrese el Nombre del Cliente y la Descripción.
6. Haga clic en Generate Secret para rellenar el secreto de cliente.



Nota: El secreto de cliente se genera y se muestra sólo una vez. Copie y almacene de forma segura esta información.

7. Establezca el valor predeterminado de Vencimiento del token.
8. Haga clic en la sección + Agregar en roles para agregar el rol.
9. Haga clic en Guardar en la parte superior derecha.

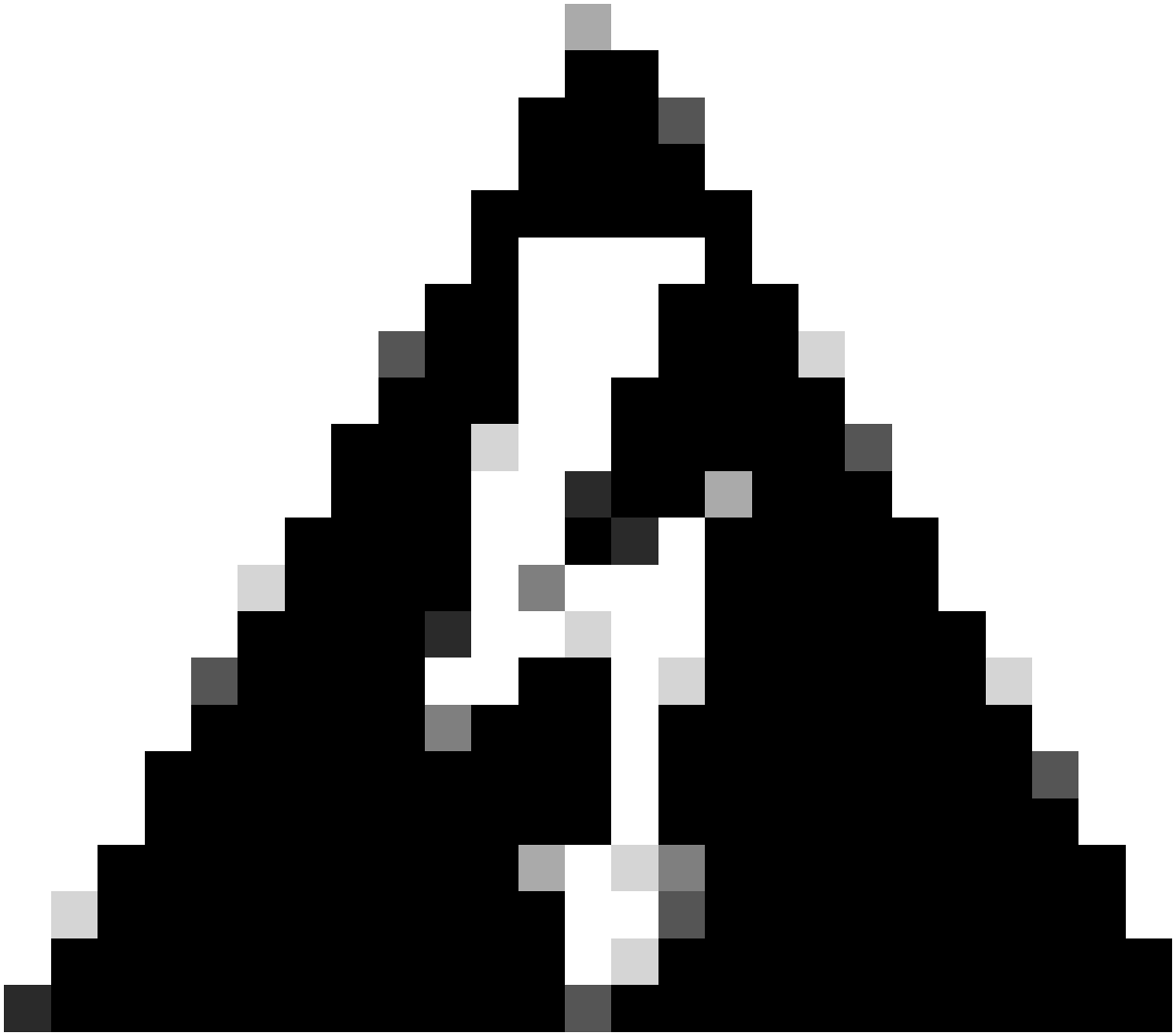
Ver cliente de API existente

1. Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
2. Haga clic en Nombre de usuario (esquina superior derecha) > Administración.
3. Haga clic en API Client Tab para ver los clientes API existentes.

Eliminar cliente de API existente

1. Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o

un rol con permisos de administración, agentes o asistente de introducción.
2. Haga clic en su Nombre de usuario (esquina superior derecha) > Administración > Clientes de API.
3. Busque los clientes de API específicos que desea eliminar y selecciónelos.
4. Haga clic en el icono Delete o Haga clic con el botón derecho en los clientes API seleccionados y seleccione Delete API Client(s) para eliminar los clientes API existentes.



Advertencia: La eliminación del cliente API invalida el token.

Generar token de acceso

El token de acceso se puede generar a través de la interfaz de usuario del administrador o la API OAuth. La interfaz de usuario proporciona tokens de larga duración, mientras que la API de OAuth genera tokens de corta duración que se actualizan con regularidad.

- IU de administrador (tokens de larga duración)

- Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
- Haga clic en su Nombre de usuario (esquina superior derecha) > Administración > Clientes de API.
- Seleccione el cliente API para el que desea generar el token de acceso y haga clic en Generar token de acceso temporal.
- Los tokens de acceso generados desde la interfaz de usuario tienen un tiempo de vencimiento más largo.

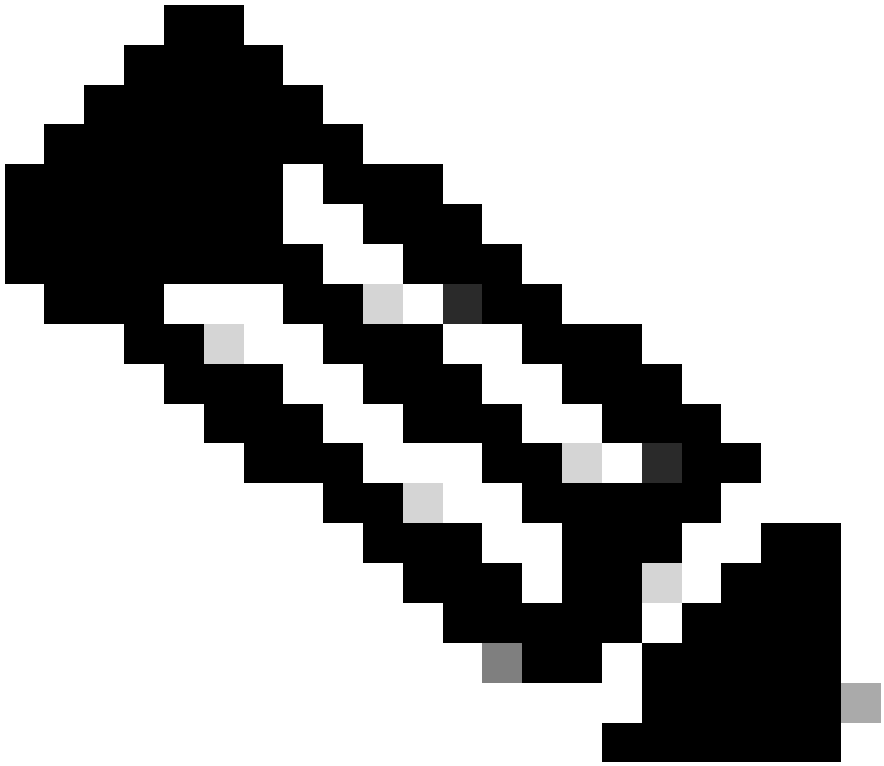
- API de OAuth (tokens de corta duración)
  - `Puede utilizar las API REST para generar un token de acceso de corta duración.

```
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=

                '
```

Sustituir:

- con el nombre de cliente que introdujo al crear el cliente de API o según lo compartido por el administrador.
- con el nombre de cuenta.

con el secreto de cliente que generó al crear el cliente de API o según lo compartido por el administrador.



Nota: No se realiza un seguimiento del token a petición en la interfaz de usuario.

Ejemplo de respuesta:

```
{
"access_token": "


              ",
"expires_in": 300
}
```

Administrar tokens de acceso

- Los tokens de acceso generados a partir de la API REST solo se pueden invalidar

eliminando el cliente de API asociado.
- Los tokens de acceso generados a través de la interfaz de usuario del controlador se pueden revocar o regenerar.
- La regeneración de un token de acceso no invalida los tokens anteriores. Los tokens más antiguos permanecen activos hasta su vencimiento.
- No hay forma de recuperar tokens anteriores o válidos actualmente. Por lo tanto, sólo se puede revocar el token actual.

    - Regenere el token de acceso

        - Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
        - Haga clic en su Nombre de usuario (esquina superior derecha) > Administración > Clientes de API.
        - Seleccione el cliente API para el que desea regenerar el token de acceso, haga clic en Regenerar > Guardar (esquina superior derecha).

    - Revocar token de acceso

        - Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
        - Haga clic en su Nombre de usuario (esquina superior derecha) > Administración > Clientes API.
        - Seleccione el cliente API para el que desea revocar el token de acceso, haga clic en Revocar > Guardar (esquina superior derecha).

Utilice el token de acceso para crear la API Rest

- Desde las API de Splunk AppDynamics dDetermine el terminal específico con el que necesita interactuar.
- Construir la solicitud:
    - Método: Seleccione el método HTTP (GET, POST, PUT, DELETE) en función de la acción que desee realizar.
    - Encabezados: agregue el token de acceso en el encabezado de autorización.
    - Cuerpo (si lo hubiera): Agregue el cuerpo de la solicitud en formato JavaScript Object Notation (JSON).

- Solicitud de ejemplo

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

        /controller/
```

```
' --header 'Authorization: Bearer

'
```

Sustituir:

- con la URL del controlador.
- con el terminal de resto con el que necesita interactuar.
- con el token de acceso generado mediante el nombre de cliente y el secreto de cliente.

Problemas comunes y solución

- 401 No autorizado
  - Problema: Los usuarios encuentran un error 401 Unauthorized al intentar generar un token de acceso.
  - Respuesta de ejemplo:

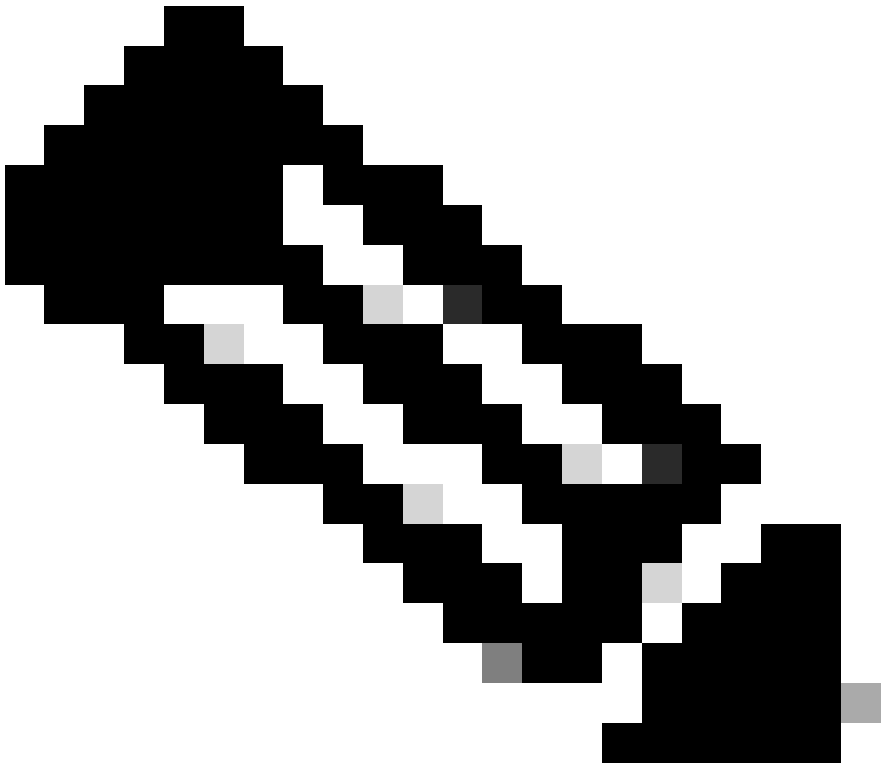
```
HTTP Error 401 Unauthorized

This request requires HTTP authentication
```

  - Causa raíz: el problema suele producirse debido a que el secreto de cliente asociado al nombre de cliente no es válido. Esto sucede a menudo cuando se genera el secreto del cliente pero no se guarda
  - Solución:
    - Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.

    - Haga clic en Nombre de usuario (esquina superior derecha) > Administración.
    - Haga clic en API Client Tab para ver los clientes API existentes.
    - Seleccione el cliente de API para el que aparece el error.
    - Haga clic en Generate Secret para generar un nuevo secreto de cliente y haga clic en Save (esquina superior derecha)

- Respuesta vacía.
    - Problema: Los usuarios encuentran una respuesta vacía cuando consultan un extremo REST, incluso después de generar un token de acceso correctamente.
    - Respuesta de ejemplo:

    - Causa raíz: El problema suele surgir debido a que no se han asignado funciones o permisos suficientes al cliente de API. Sin las funciones necesarias, el cliente de la API no puede recuperar los datos esperados del extremo.
    - Solución:
        - Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes o asistente de introducción.
        - Haga clic en Nombre de usuario (esquina superior derecha) > Administración.
        - Haga clic en API Client Tab para ver los clientes Api existentes.
        - Seleccione el cliente de API al que desea asignar el rol
        - Haga clic en la sección + Agregar en roles para agregar el rol.
        - Haga clic en Guardar en la parte superior derecha.



Nota: Asegúrese de que el cliente de API tenga asignadas las funciones adecuadas. Las funciones deben ajustarse a los requisitos de acceso a datos del extremo REST.

- Tipo de contenido no válido
  - Problema: El usuario encuentra un error 500 Internal Server cuando intenta generar un token de acceso.
  - Error de ejemplo:

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

  - Causa raíz: El problema surge debido al encabezado del tipo de contenido. En la versión 24.10 del controlador, el tipo de contenido se cambió de application/vnd.appd.cntrl+json;v=1 a application/x-www-form-urlencoded
  - Solución:
    - Modifique la solicitud y establezca el encabezado del tipo de contenido en application/x-www-form-urlencoded
      Ejemplo:

```
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=

'
```

Información Relacionada

Documentación de AppDynamics

API de Splunk AppDynamics

Clientes de API

Administrar tokens de acceso

¿Necesita más asistencia?

Si tiene alguna pregunta o experimenta algún problema, cree un ticket de soporte con estos datos:

- Detalles del error o captura de pantalla: Proporcione un mensaje de error específico o una captura de pantalla del problema.
- Comando utilizado: Especifique el comando exacto que estaba ejecutando cuando se produjo el problema.
- Controller Server.log (sólo en las instalaciones): Si corresponde, proporcione los registros del servidor del controlador desde <controller-install-dir>/logs/server.log*

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).