Configurar y solucionar problemas de inicio de sesión único en AppDynamics

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Configurar

- Proveedores de identidad admitidos
- Pasos para configurar SAML en AppDynamics
  - Paso 1. Recopilar detalles de AppDynamics Controller
  - Paso 2. Crear una nueva Aplicación en IdP y Descargar los Metadatos
  - Paso 3. Configure la autenticación SAML en AppDynamics Controller

Verificación

Problemas comunes y solución

- 400 Solicitud incorrecta
- Permisos de usuario que faltan
- Falta el correo electrónico o nombre incorrecto para los usuarios de SAML
- Error de HTTP 404

Necesita más ayuda

Información Relacionada

Introducción

Este documento describe cómo configurar el inicio de sesión único (SSO) en AppDynamics y solucionar problemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Para configurar el inicio de sesión único, el usuario debe tener una función de propietario de cuenta (predeterminada)o una función personalizada con permisos de administración, agentes y asistente de inicio de sesión.
- Acceso de administrador a sucuenta de ID.
- Los metadatos o los detalles de configuración de AppDynamics (por ejemplo, ID de entidad, URL de ACS).

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

Single Sign-On (SSO) es un mecanismo de autenticación que permite a los usuarios iniciar sesión una vez y obtener acceso a varias aplicaciones, sistemas o servicios sin necesidad de volver a autenticarse para cada uno.

El lenguaje de marcado de aserción de seguridad (SAML) es una de las tecnologías utilizadas para implementar SSO. Proporciona el marco y los protocolos que permiten el inicio de sesión único mediante el intercambio seguro de datos de autenticación y autorización entre un proveedor de identidad (IdP) y un proveedor de servicios (SP).

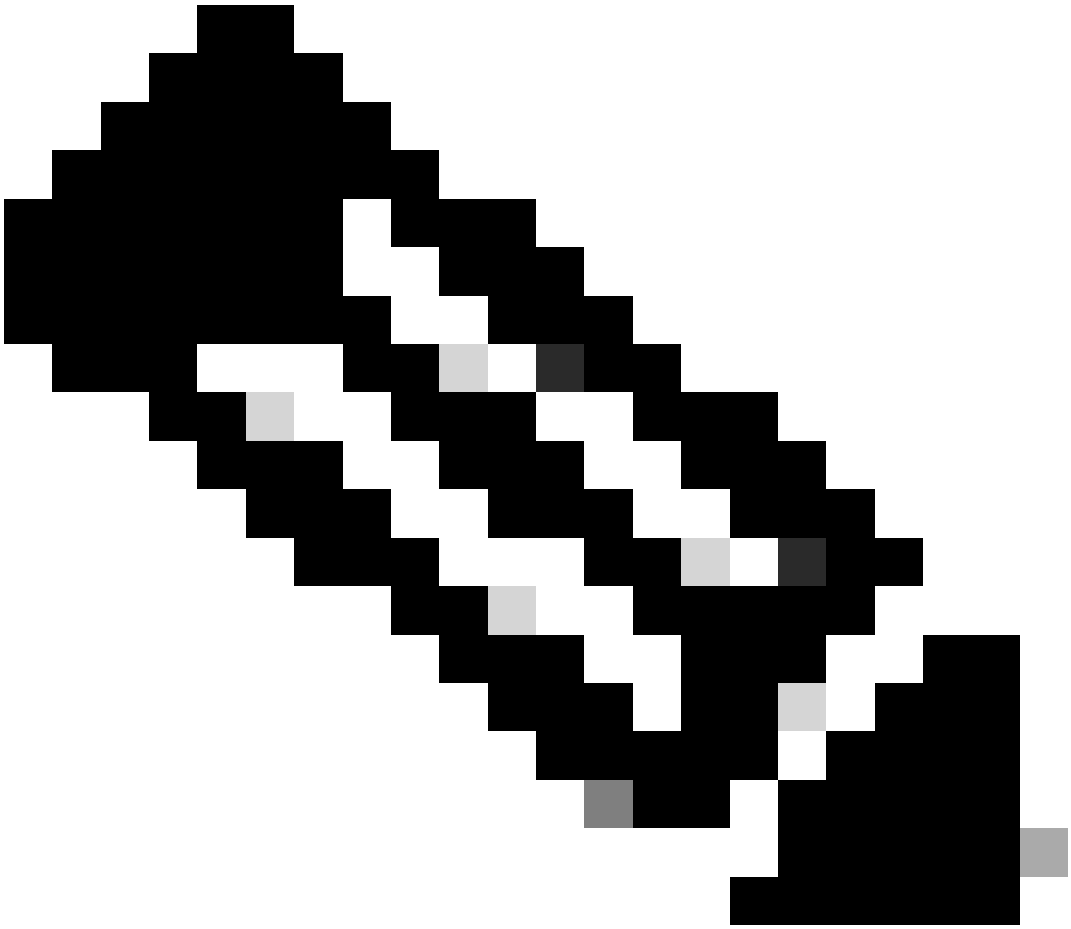
Afirmación SAML

- El intercambio de mensajes basado en XML entre el IdP y el SP.
- Proporciona tres tipos de aserciones:
    - Aserciones de autenticación: Confirma que el usuario se ha autenticado.
    - Aserciones de atributos: Comparte los atributos de usuario, como el nombre de usuario o las funciones.
    - Afirmaciones de decisión de autorización: Indica qué está autorizado a hacer el usuario.

Funciones clave en SAML

- Proveedor de identidad (IdP)
    - Verifica la identidad del usuario.
    - Generar la afirmación SAML que contiene la información de identificación del usuario.
- Proveedor de servicios (SP)
    - Aplicación o sistema al que el usuario desea acceder.
    - Se basa en el IdP para autenticar al usuario.
    - Acepta la afirmación SAML para conceder al usuario acceso a sus recursos o aplicación.
- Usuario (principal)
    - Usuario real que inicia la solicitud o intenta obtener acceso a un recurso desde el proveedor de servicios.

- Interactúa tanto con el IdP (Autenticación) como con el SP.



Nota: AppDynamics admite SSO iniciado por IdP e iniciado por SP.

Flujo iniciado por SP:

- El usuario se desplaza al proveedor de servicios escribiendo la dirección URL de la aplicación (por ejemplo, AppDynamics) o haciendo clic en un vínculo.
- El SP busca una sesión existente. Si no existe ninguna sesión, el SP reconoce que el usuario no está autenticado e inicia el proceso SSO.
- El SP genera una Solicitud de autenticación SAML y redirige al usuario al IdP para la autenticación.
    - Esta solicitud incluye:
        - ID de entidad: Identificador único del proveedor de servicios.
        - URL de servicio de consumidor de afirmación (ACS): donde el IdP envía la Afirmación SAML después de la autenticación.
        - Metadatos sobre el SP y detalles de seguridad (por ejemplo, solicitud firmada,

requisitos de cifrado).
- El usuario es redirigido a la página de login de IdP.
- El IdP autentica al usuario (por ejemplo, vía nombre de usuario/contraseña o autenticación multifactor).
- Después de una autenticación exitosa, el IdP genera una Afirmación SAML (token de seguridad).
- La afirmación SAML se envía de vuelta al SP a través del navegador de usuario utilizando HTTP POST Binding (en la mayoría de los casos) o HTTP Redirect Binding.
- El SP valida la afirmación SAML para garantizar:
    - Fue emitido por el idP confiable.
    - Se dirige al proveedor de servicios (a través de la ID de entidad del proveedor de servicios).
    - No ha caducado ni ha sido manipulado (validado mediante la clave pública IdP).
- Si la afirmación SAML es válida, el SP crea una sesión para el usuario.
- Se concede al usuario acceso a la aplicación o a los recursos.

Flujo iniciado por IdP:

- El usuario navega al portal de registro de IdP e ingresa sus credenciales.
- El IdP autentica al usuario (por ejemplo, con una combinación de nombre de usuario/contraseña, autenticación multifactor).
- Después de la autenticación, el IdP presenta al usuario una lista de aplicaciones o servicios (SP) disponibles a los que puede acceder.
- El usuario selecciona el SP deseado (por ejemplo, AppDynamics).
- El IdP genera una Aserción SAML para el SP seleccionado.
- El IdP redirige al usuario a la URL de SP Assertion Consumer Service (ACS) y envía la Aserción SAML junto con ella (mediante HTTP POST Binding o HTTP Redirect Binding).
- El SP recibe la afirmación SAML y la valida:
    - Asegura que la afirmación es emitida por un IdP confiable.
    - Verifica la integridad y caducidad de la aserción.
    - Confirma la identidad del usuario y otros atributos.
- Si la afirmación SAML es válida, el SP crea una sesión para el usuario.
- Se concede al usuario acceso a la aplicación o a los recursos.

Configurar

El controlador de AppDynamics puede utilizar la identidad del cliente de Cisco o un proveedor de identidad SAML (IdP) externo para autenticar y autorizar a los usuarios.

Proveedores de identidad admitidos

AppDynamics certifica el soporte para estos proveedores de identidad (IdPs):

- Okta

- Onelogin
- Identidad de ping
- Azure AD
- Identidad de nube de IBM
- Servicio de federación de Active Directory (AD FS)

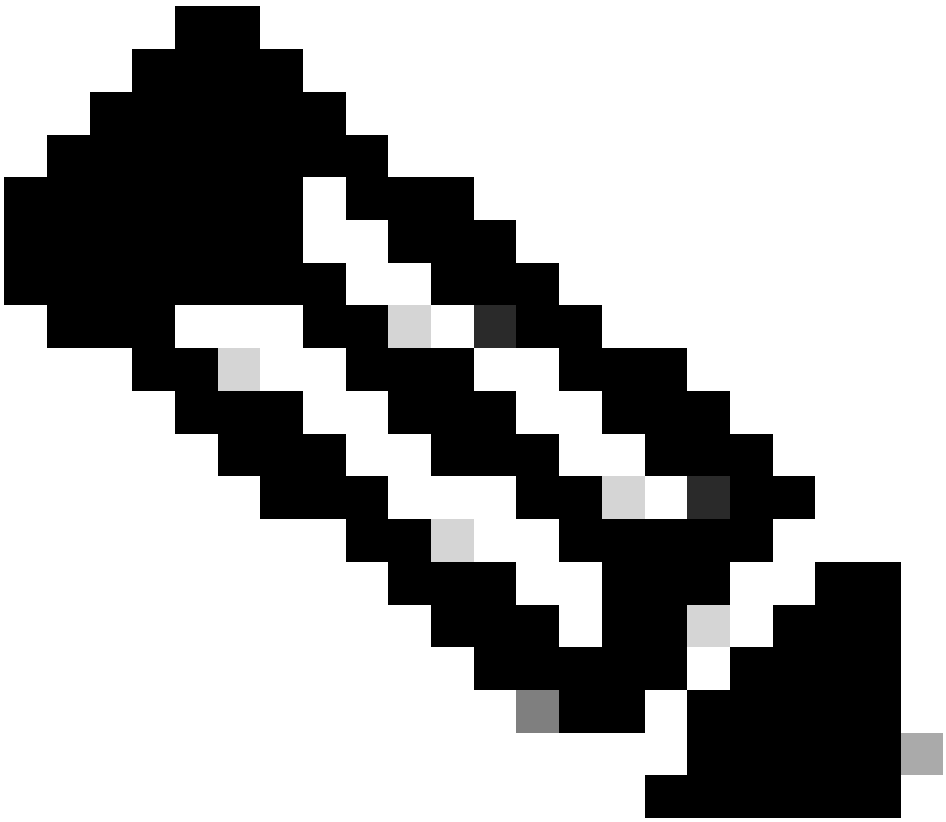
Otros IdPs que admiten el enlace HTTP POST también son compatibles con la autenticación SAML de AppDynamics.

Pasos para configurar SAML en AppDynamics

Paso 1. Recopilar detalles de AppDynamics Controller

- Id. de entidad (Id. de entidad SP): identificador único de AppDynamics (por ejemplo, https://<controller-host>:<port>/controller).
    - Sintaxis: https://<controller_domain>/controller
    - ejemplo: https://<your_controller_domain>/controller

- URL de respuesta (Assertion Consumer Service, ACS URL): el punto final en el proveedor de servicios (por ejemplo, AppDynamics) donde el IdP envía la respuesta SAML después de la autenticación.
    - Sintaxis: https://<controller_domain>/controller/saml-auth?accountName=<account_name>
    - ejemplo: https://your_controller_domain/controller/saml-auth?accountName=youraccountname



Nota: En el caso del controlador local, el nombre de cuenta predeterminado es customer1, a menos que tenga un controlador de varios arrendatarios con un accountName diferente.

- URL de cierre de sesión único (opcional): el terminal del SP para gestionar las solicitudes de cierre de sesión de SAML (por ejemplo, https://<controller_domain>/controller).

Paso 2. Crear una nueva Aplicación en IdP y Descargar los Metadatos

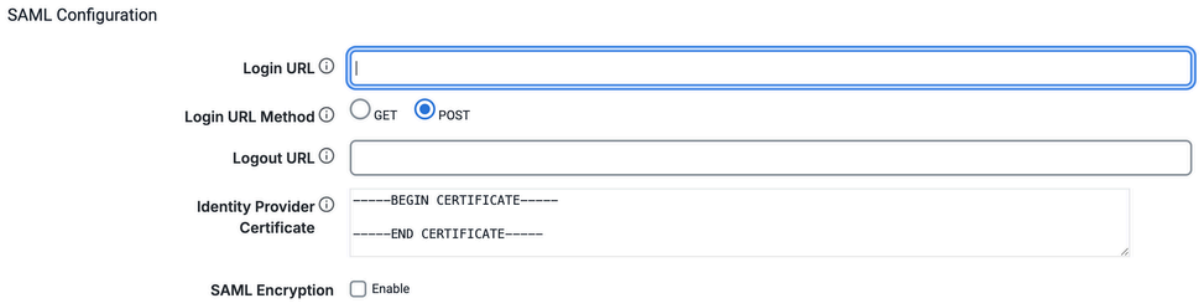
- Localice el área de creación de la aplicación: normalmente se encuentra dentro de la consola administrativa o el panel de IdP, a menudo con etiquetas como Aplicaciones, Aplicaciones Web y Móviles, Aplicaciones Empresariales o Usuarios que Confían.
- Agregar una aplicación SAML personalizada o genérica: seleccione una opción que le permita configurar una aplicación SAML personalizada o una integración de proveedor de servicios SAML genérico.
- Proporcionar detalles de la aplicación: asigne un nombre a la aplicación y cargue potencialmente un icono para su identificación (opcional).
- Agregue asignaciones de atributos (nombre de usuario, displayName, correo electrónico o roles) para pasar información de usuario a AppDynamics.
- Descargue el archivo de metadatos IdP o, alternativamente, anote estos detalles:
    - URL de inicio de sesión IdP

- URL de desconexión
- Nombres de atributos
- Certificado

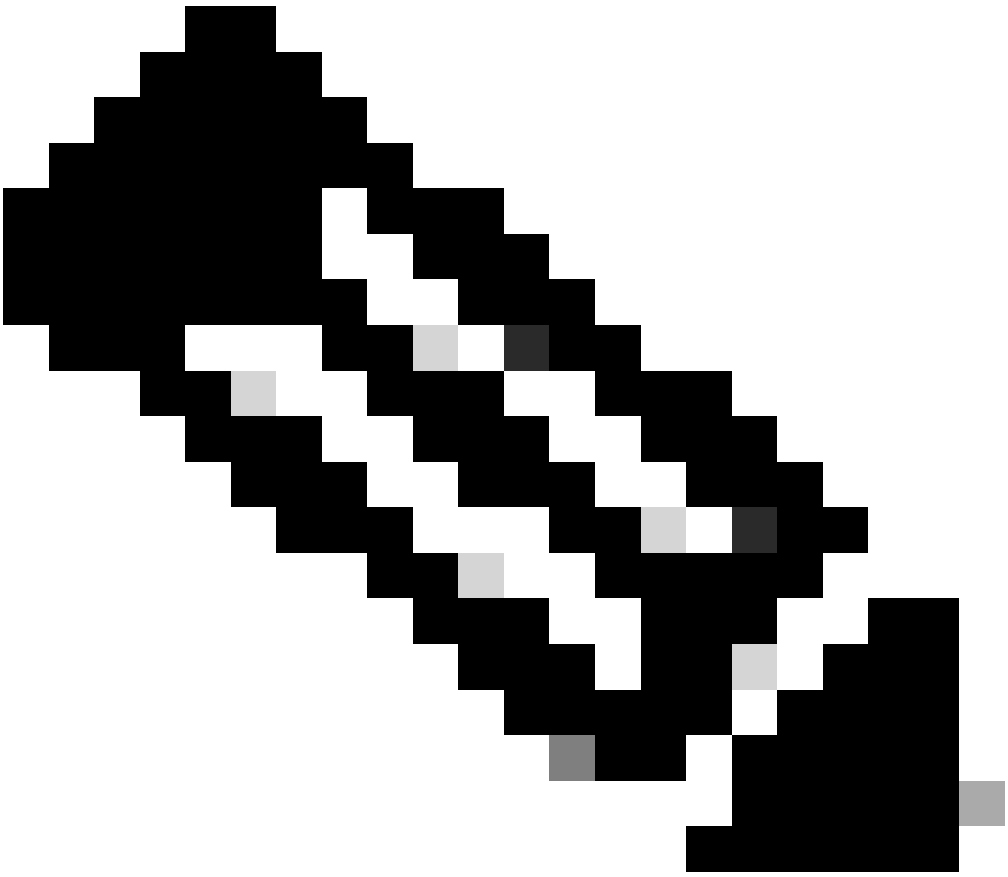
Paso 3. Configure la autenticación SAML en AppDynamics Controller

- Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes y asistente de introducción.
- Haga clic en su Nombre de usuario(esquina superior derecha)> Administración > Proveedor de autenticación > Seleccionar SAML.

- En la sección Configuración de SAML, agregue estos detalles:
  - URL de inicio de sesión: La URL de inicio de sesión IdP donde AppDynamics Controller enruta las solicitudes de inicio de sesión iniciadas por el proveedor de servicios (SP).
  - URL de cierre de sesión (opcional): La dirección URL donde AppDynamics Controller redirige a los usuarios después de cerrar sesión. Si no especifica una URL de cierre de sesión, los usuarios obtienen la pantalla de inicio de sesión de AppDynamics cuando cierran la sesión.
  - Certificado: El certificado X.509 de IdP. Pegue el certificado entre los delimitadores BEGIN CERTIFICATE y END CERTIFICATE. Evite duplicar los delimitadores BEGIN CERTIFICATE y END CERTIFICATE desde el propio certificado de origen.
  - Cifrado SAML (opcional): puede mejorar la seguridad de la autenticación SAML cifrando la respuesta SAML desde el IdP al proveedor de servicios. Para cifrar las respuestas SAML en AppDynamics, debe configurar el proveedor de identidad (IdP) para cifrar la afirmación SAML y, a continuación, configurar AppDynamics Controller para utilizar un certificado y una clave privada específicos para el descifrado.



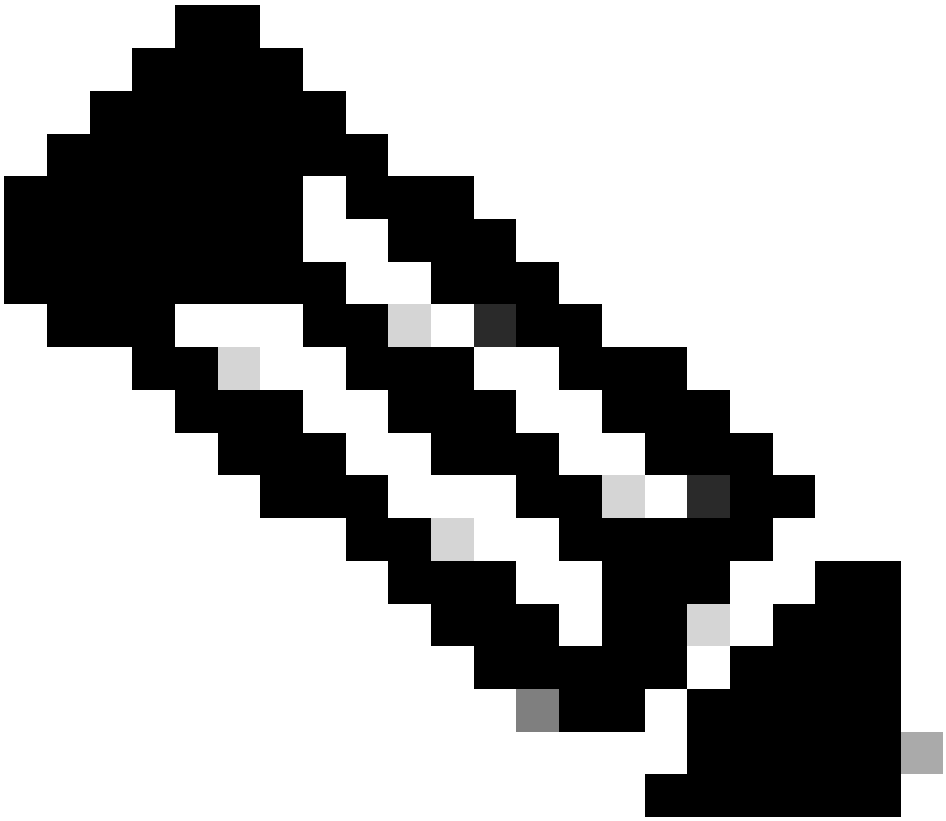
- En la sección Asignaciones de atributos SAML, asigne los atributos SAML (ejemplo: Nombre de usuario, DisplayName, Correo electrónico) a sus campos correspondientes en AppDynamics.



Nota: AppDynamics muestra el nombre de usuario, el correo electrónico y el nombre para mostrar de un usuario SAML. De forma predeterminada, utiliza el atributo NameID de la respuesta SAML para crear un nombre de usuario, que también se utiliza como displayName. Este comportamiento se puede personalizar incluyendo los atributos username, email y displayname en la respuesta SAML. Al configurar los valores de IdP en AppDynamics, el usuario puede especificar estos nombres de atributo. Durante el inicio de sesión, AppDynamics comprueba si se ha configurado la asignación de atributos. Si se configuran las asignaciones y los atributos coincidentes están presentes en la respuesta SAML, AppDynamics utiliza esos valores de atributo para establecer el nombre de usuario, el correo electrónico y el nombre de visualización.

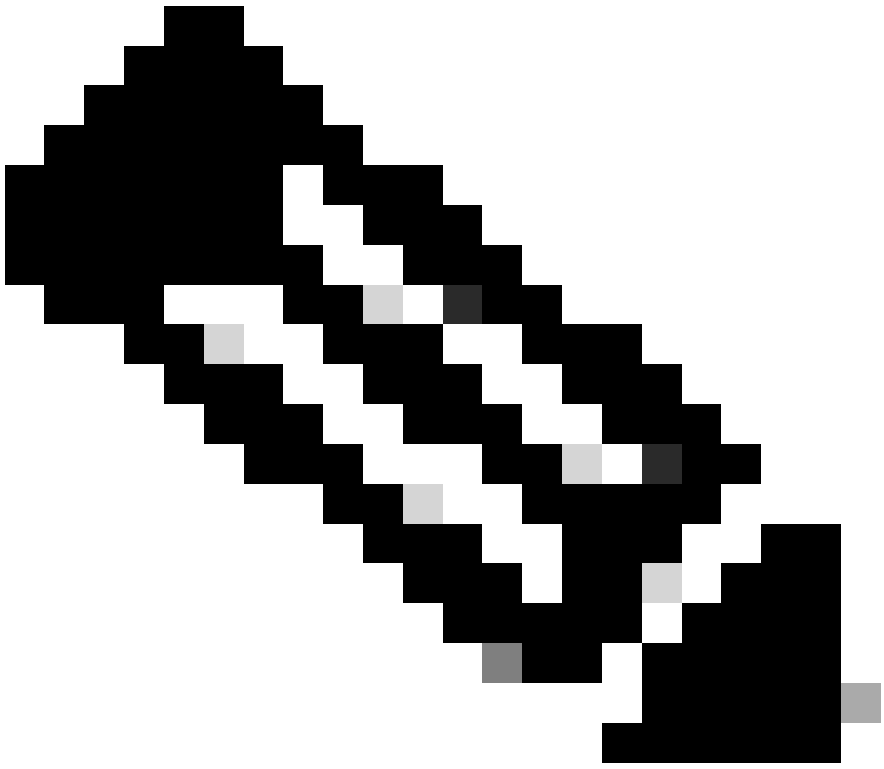
- En la sección Asignaciones de grupos SAML, agregue estos detalles.

- Nombre de Atributo de Grupo SAML: Introduzca el nombre del atributo SAML que contiene la información de grupo. Normalmente es Grupos, o grupo o roles, o Roles o pertenencia a grupo.
- Valor de Atributo de Grupo: Seleccione el formato de valor adecuado para el atributo de grupo. Las opciones comunes incluyen Valores de Grupos Múltiples Anidados o Valor Único dependiendo de cómo su IdP estructure la información del grupo.

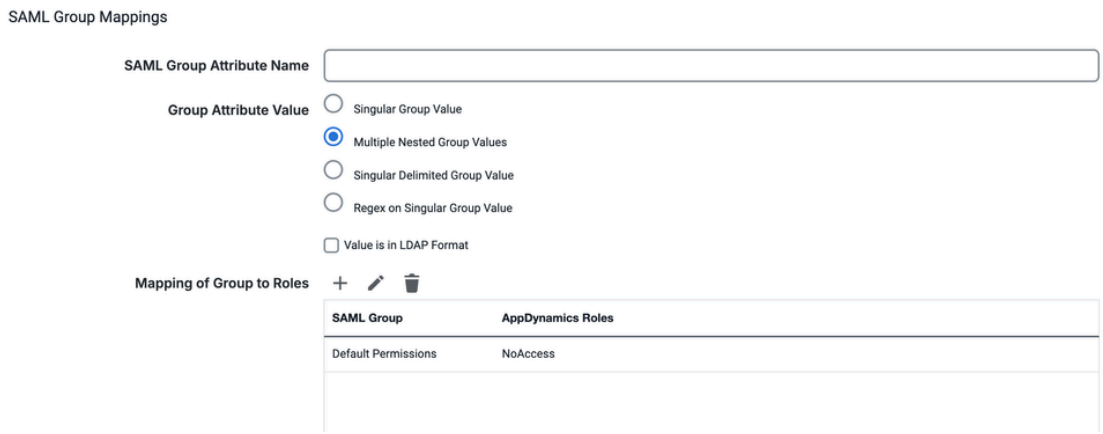


Nota: Seleccione El valor está en formato LDAP si la información de grupo viene en formato LDAP (protocolo ligero de acceso a directorios).

- Asignación de un grupo a roles: haga clic en el botón + para agregar una nueva asignación.
  - Grupo SAML: introduzca el nombre del grupo SAML (como se define en su IdP) que desea asignar a un rol de AppDynamics.
  - Rol(s): seleccione los roles de AppDynamics correspondientes de la lista disponible que desea asignar a los usuarios que pertenecen al grupo SAML.
  - Permisos predeterminados: si la asignación de grupo SAML no está configurada o si una afirmación SAML de usuario no incluye información de grupo, AppDynamics recurre al uso de permisos predeterminados.



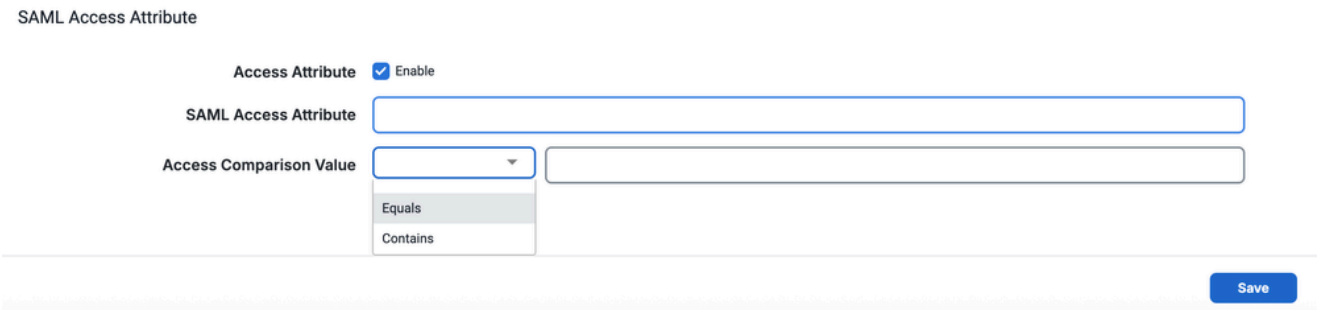
Nota: Se recomienda asignar una función con permisos mínimos a Permisos predeterminados.



- En la sección Atributo de Acceso SAML, agregue estos detalles (Opcional):
  - Atributo de acceso SAML: Introduzca el nombre de los atributos de la respuesta SAML. Se va a utilizar para la validación de acceso.

- Valor de comparación de acceso: hay dos opciones disponibles:
  1. Igual: El acceso se concede sólo si el valor del atributo en la respuesta SAML coincide exactamente con el valor especificado en la configuración.
  2. Contiene: Se concede acceso si el valor del atributo en la respuesta SAML contiene el valor especificado en la configuración.
- Cómo funciona si está habilitado:
  1. AppDynamics recupera el atributo especificado en el campo Atributo de acceso SAML de la respuesta SAML.
  2. Compara el valor del atributo con el valor de comparación de acceso definido por el usuario basándose en el método seleccionado (Igual o Contiene).
  3. Si la comparación se realiza correctamente, se concede acceso al usuario.
  4. Si la comparación falla, se deniega el intento de inicio de sesión.

- Haga clic en Guardar (esquina inferior derecha) para guardar la configuración.



Verificación

- Abra un explorador y navegue hasta AppDynamics Controller. Aparecerá el cuadro de diálogo Iniciar sesión del servicio IdP de terceros.
- Haga clic en Iniciar sesión con inicio de sesión único. El sistema le redirige a su IdP.
- Introduzca y envíe sus credenciales.
- Después de la autenticación exitosa, el IdP lo redirige a su AppDynamics Controller.

Problemas comunes y solución

400 Solicitud incorrecta

- Problema: los usuarios encuentran un error 400 Bad Request al intentar iniciar sesión en AppDynamics Controller.
- Error de ejemplo:

```
HTTP status 400 - Bad Request
Message: Error while processing SAML Authentication Response - see server log for details
Description: The request sent by the client was syntactically incorrect.
```

- Causas principales comunes:
    - Certificado SAML no válido
    - La respuesta de SAML es mayor que la longitud máxima
    - ID de entidad o URL ACS no válidos
- Solución:
    - Certificado SAML no válido
        - Asegúrese de que el certificado proporcionado por el proveedor de identidad (IdP) es válido y está actualizado.
        - Verifique la fecha de vencimiento del certificado IdP. Si ha caducado, obtenga un nuevo certificado del IdP.
        - Si el certificado se ha actualizado en el lado IdP, asegúrese de que el nuevo certificado se carga y configura en AppDynamics.
        - Pasos para actualizar el certificado en AppDynamics:
            - Inicie sesión en la interfaz de usuario del controlador como un rol de propietario de cuenta o un rol con permisos de administración, agentes y asistente de introducción.
            - Haga clic en su Nombre de usuario(esquina superior derecha)**>** Administración **>** Proveedor de autenticación **>** Seleccionar SAML.
            - En la sección Configuración SAML, localice el campo certificate y reemplace el viejo certificate con el nuevo proporcionado por el IdP.
            - Haga clic en Guardar para actualizar la configuración SAML.

    - La respuesta de SAML es mayor que la longitud máxima.
        - Este problema surge cuando el controlador se mueve de GlassFish a Jetty Server, a partir de la versión 23.11 del controlador y posteriores. En Jetty Server, hay una propiedad denominada -Dorg.eclipse.jetty.server. Request.maxFormContentSize ubicado en la ...archivo /appserver/jetty/start.d/start.ini. Si el tamaño de la respuesta SAML excede el valor establecido para esta propiedad, el controlador rechaza la carga y devuelve una solicitud 400 incorrecta error
        - Causas de respuestas SAML grandes:
            - Atributos excesivos: Demasiados atributos incluidos en la afirmación SAML.
            - Respuestas SAML firmadas o cifradas: La firma o el cifrado aumentan el tamaño de la respuesta.
            - Datos adicionales de usuario o grupo: El proveedor de identidad (IdP) tiene datos de usuario o grupo adicionales.

        - Hay dos formas de resolver este problema. Si implementa una o ambas soluciones, puede resolver el problema y evitar que se rechace la carga.
            1. Aumentar el valor maxFormContentSize
                - Para controladores in situ: Actualice la propiedad -Dorg.eclipse.jetty.server.Request.maxFormContentSize en el .../appserver/jetty/start.d/start.ini a un valor mayor y reinicie el controlador.
                - Para controladores SaaS: Presente una incidencia de soporte técnico

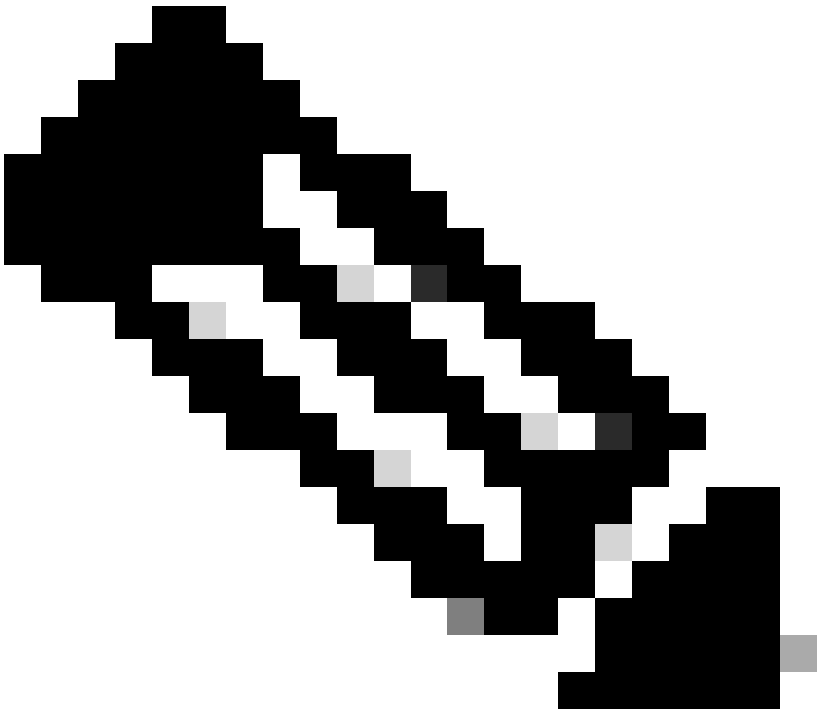
para que el equipo de soporte técnico resuelva este problema.

2. Optimización de la respuesta SAML

   Trabaje con su proveedor de identidad (IdP) para reducir el tamaño de la respuesta SAML realizando estos ajustes:

   - Excluir atributos innecesarios: Elimine los atributos no utilizados o redundantes de la afirmación SAML a través de la configuración IdP.
   - Desactivar cifrado (si está permitido): El cifrado aumenta el tamaño de la respuesta SAML. Si la conexión ya está protegida mediante HTTPS, considere la posibilidad de deshabilitar el cifrado para reducir el tamaño.

- ID de entidad o URL ACS no válidos
  - En el Idp:
    - Confirme que el ID de entidad sea https://your_controller_domain/controller. Si el ID de entidad es diferente, actualícelo.
    - Confirme que la URL de ACS sea https://your_controller_domain/controller/saml-auth?accountName=youraccountname. Si la URL de ACS es diferente, actualícela en consecuencia.



Nota: accountName debe coincidir con el nombre de cuenta de AppDynamics. (por ejemplo, customer1)

- Permisos de usuario que faltan
    - Problema: ha iniciado sesión correctamente en el controlador. Sin embargo, no recibió los roles y permisos deseados.
    - Ejemplo de configuración y respuesta SAML:
        - En el usuario SAML del atributo Group, el nombre es Groups con valores AppD_Admin & AppD_Power_User.

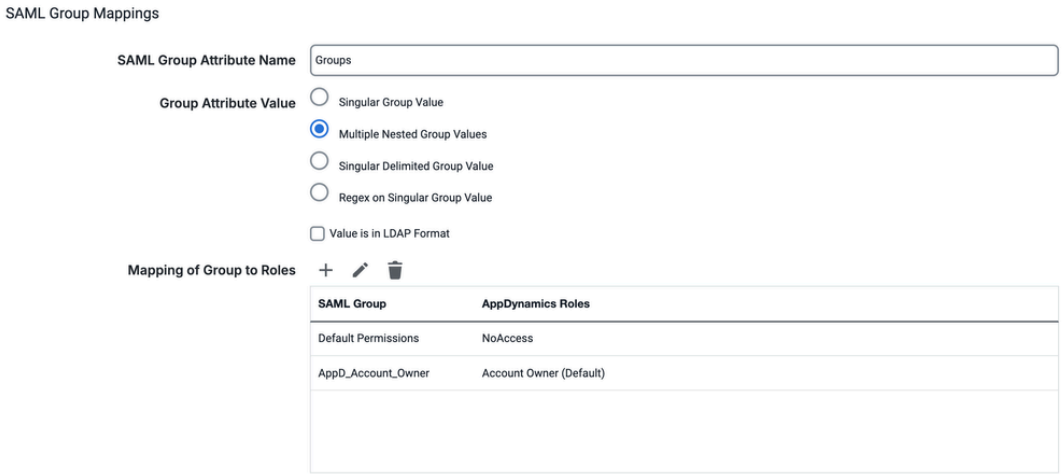
```
AppD_Admin
```

```
AppD_Power_User
```

        - En AppDynamics, en la sección Asignaciones de grupos SAML, se configuran.
            - Nombre de atributo de grupo SAML: Grupos
            - Valor de atributo de grupo: Varios valores de grupos anidados
            - Asignación a funciones de grupo:

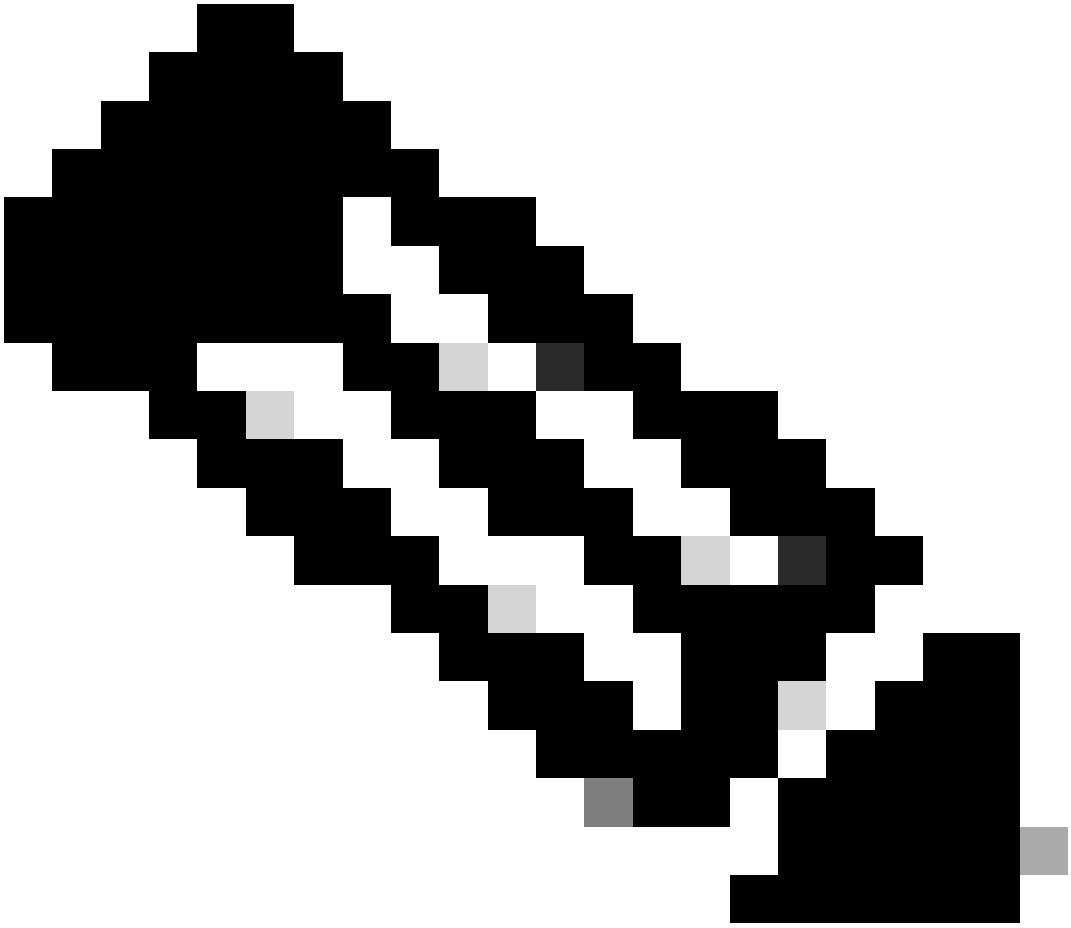
Grupo SAML	Funciones de AppDynamics
AppD_Account_Owner	Propietario de cuenta (predeterminado)
Permisos predeterminados	Sin acceso

            Sin acceso es una función personalizada sin permisos.



- Problemas comunes y solución
  - No se han encontrado atributos de grupo en la respuesta SAML.
    - A la respuesta SAML del IdP le faltan los atributos de grupo requeridos o el nombre de atributo para los grupos en la respuesta SAML se establece como Roles mientras que en AppDynamics, se configura como Grupos.
    - Cuando no se proporcionan atributos de grupo, al usuario se le asignan automáticamente las funciones asociadas con los permisos predeterminados en AppDynamics.
    - Para resolver esto, asegúrese de que el IdP esté configurado para incluir los atributos de grupo correctos en la respuesta SAML y que el nombre de atributo para los grupos coincida con la configuración en AppDynamics.

  - No hay ninguna asignación de grupo SAML correspondiente configurada en AppDynamics para los grupos de usuarios proporcionados en la respuesta SAML.
    - En la respuesta SAML, el atributo Groups contiene los valores AppD_Admin y AppD_Power_User. Sin embargo, en AppDynamics, las asignaciones de grupo sólo existen para el grupo AppD_Account_Owner.
    - Como no hay ninguna asignación correspondiente para AppD_Admin o AppD_Power_User, al usuario no se le asignan roles ni permisos.
    - Para resolver esto, agregue las asignaciones de grupo que faltan (por ejemplo, AppD_Admin y AppD_Power_User) en AppDynamics para garantizar una asignación de permisos y funciones adecuada.



Nota: Los permisos predeterminados solo se aplican a los usuarios SAML cuando el nombre de atributo de grupo SAML configurado en AppDynamics no es el mismo que los atributos Groups en la respuesta SAML.

- Falta el correo electrónico o nombre incorrecto para los usuarios de SAML
  - Problema: Esto suele suceder cuando la configuración de Attribute en AppDynamics no coincide con los atributos que vienen en la respuesta SAML.
  - Ejemplo de respuesta SAML: Atributos En la respuesta SAML son: User.email, User.fullName y Groups

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- Ejemplo de asignaciones de atributos SAML en AppDynamics
    - Atributo de nombre de usuario: Nombre de usuario
    - Atributo de nombre para mostrar: User.firstName o en blanco
    - Atributo de correo electrónico: User.userPrincipal o vacío

- Causa raíz: los atributos Display Name y Email configurados en AppDynamics no

coinciden con ninguno de los atributos proporcionados en la respuesta SAML.
    - Como resultado:
        - El correo electrónico está en blanco.
        - El nombre para mostrar toma de forma predeterminada el nombre de usuario.

- Solución: Asegúrese de que los atributos Display Name y Email configurados en AppDynamics coincidan con los atributos correspondientes en la respuesta SAML.
    - Por ejemplo:
        - Actualice el atributo Display Name a User.fullName.
        - Actualice el atributo Email a User.email.

- Error de HTTP 404

- Problema: el usuario no puede iniciar sesión en el controlador y se produce el error 404 not found.
- Error de ejemplo: En Registros del controlador (sólo para el controlador en las instalaciones), verá este error:

```
[#|2025-01-10T21:16:35.222+0000|SEVERE|glassfish 4.1|com.singularity.ee.controller.auth.saml.SAMLA
com.appdynamics.platform.services.auth.exception.SamlException: Requested url validation failed
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.validateRequest
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.getSamlAuthenti
```

- Causa raíz: este error suele producirse cuando la dirección URL del controlador configurada en la base de datos del controlador no coincide con la dirección URL del controlador utilizada para iniciar sesión o la dirección URL configurada en el IdP
- Solución:
    - Para controladores in situ:
        - Ejecute este comando para actualizar la URL del controlador. (Recomendado).

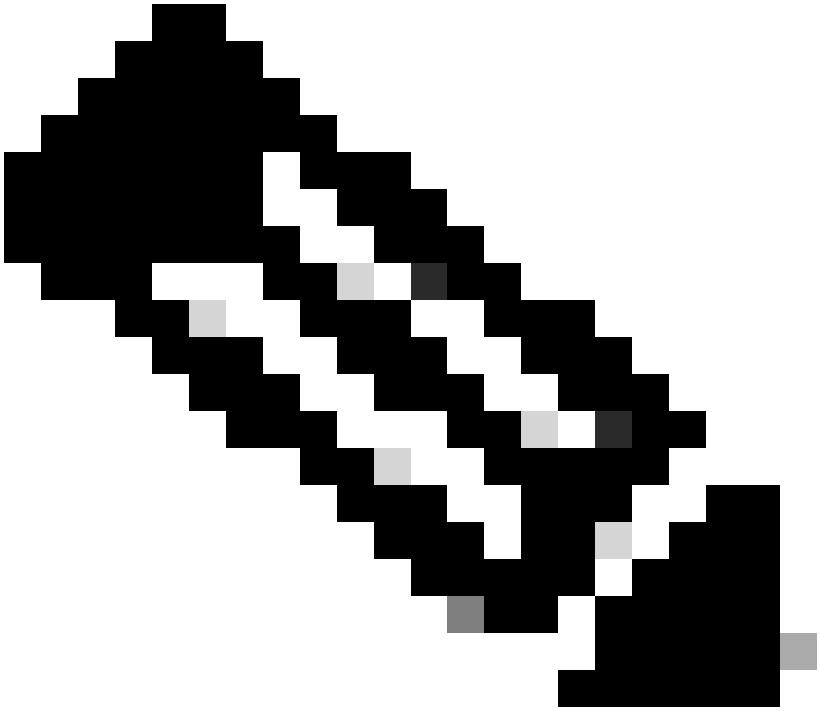
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- Como alternativa, puede ejecutar estos comandos en la base de datos del controlador para actualizar la URL del controlador.

```
UPDATE controller.account SET controller_url ='

             ' WHERE id=

              ;
UPDATE mds_auth.account SET controller_url='

               ' WHERE name='

                ';
```

  - Ejecute este comando para obtener el <ACCOUNT_ID>.

```
Select id from controller.account where name = '

                  ';
```



Nota: Ejecute curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll si aún observa el mismo problema.

- Sustituir:
  - <NEW_CONTROLLER_URL> con la URL del controlador real que está utilizando para acceder al controlador.
  - <controller_domain> con su dominio de controlador.
  - <youraccount name> con su nombre de cuenta.

- Para controladores SaaS: Presente una incidencia de soporte técnico para que el equipo de soporte técnico resuelva este problema.

Necesita más ayuda

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.
- Respuesta SAML: Recopile el archivo SAML-Trace y HAR
- Controller Server.log (solo en las instalaciones): si procede, proporcione los registros del servidor del controlador desde <controller-install-dir>/logs/server.log

Información Relacionada

Documentación de AppDynamics

SAML para implementaciones de SaaS

Cifrar respuestas SAML para implementaciones SaaS

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).