Solución de problemas de ISE 3.1 GUI Inicio de sesión con SAML SSO

Contenido

Introducción

Este documento describe la mayoría de los problemas que se han observado en ISE 3.1 con el inicio de sesión en la GUI de SAML. Mediante el uso del estándar SAML 2.0, el inicio de sesión de administrador basado en SAML agrega la capacidad de inicio de sesión único (SSO) a ISE. Puede utilizar cualquier proveedor de identidad (IdP) como Azure, Okta, PingOne, DUO Gateway o cualquier IdP que implemente SAML 2.0.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

1. Cisco ISE 3.1 o superior
2. Entender los conceptos básicos de las configuraciones SSO de SAML

Consulte la guía de administración de ISE 3.1 para la configuración de SAML e ISE Admin Login Flow a través de SAML con Azure AD para obtener más detalles sobre la configuración y el flujo.

> **Nota:** Debe estar familiarizado con el servicio Identity Provider y asegurarse de que está en funcionamiento.

Componentes Utilizados

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

- ISE versión 3.1

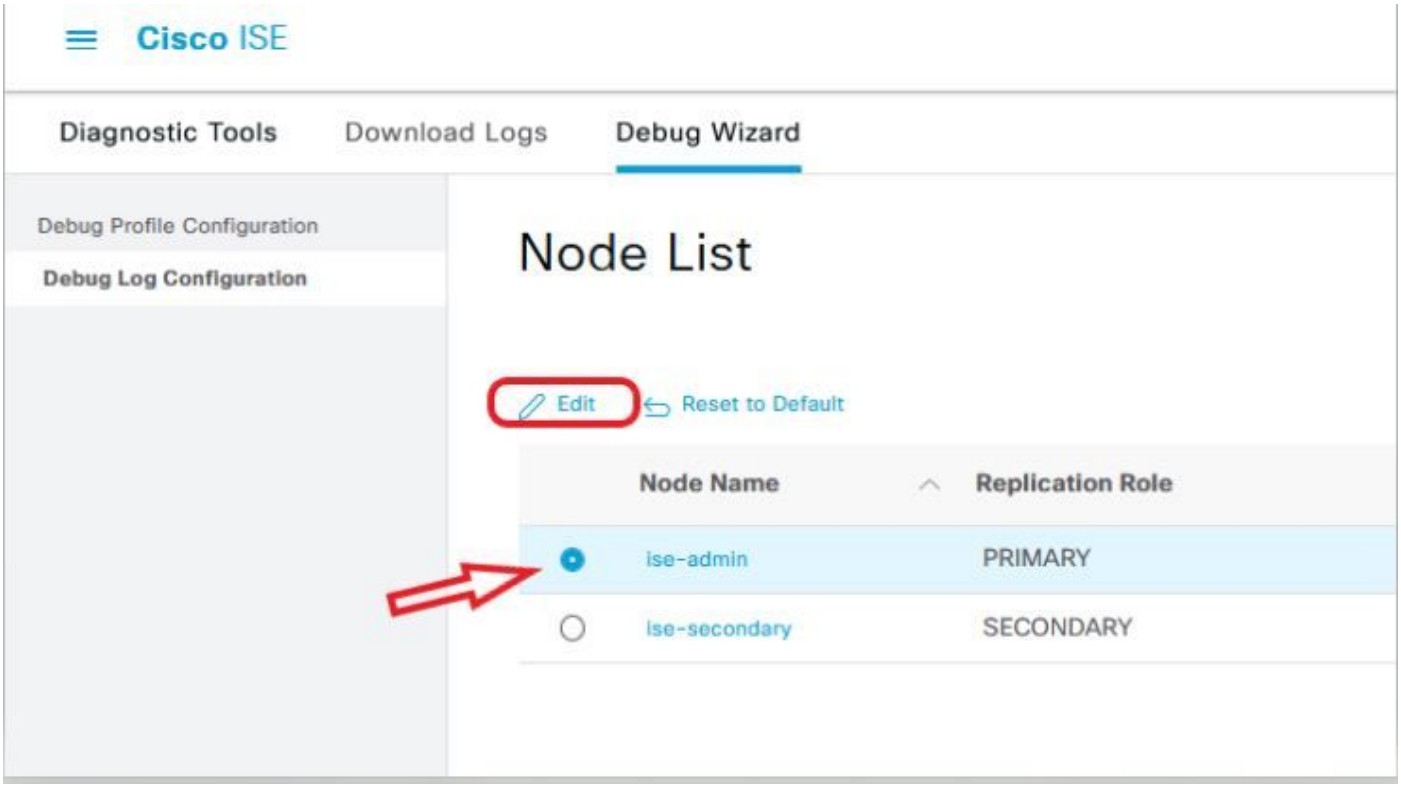
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red

en vivo, asegúrese de entender el posible impacto de cualquier comando.

Habilite las depuraciones

Para iniciar la solución de problemas, primero debe habilitar las depuraciones como se describe a continuación.

Vaya a **Operaciones > Solución de problemas > Asistente de depuración > Configuración del registro de depuración. Seleccione el nodo de administración principal y haga clic en Editar**, como se muestra en la siguiente imagen.



- Establezca los siguientes componentes en el nivel **DEBUG**.

Nombre del componente	Nivel de registro	Nombre de archivo de registro
portal	DEPURAR	guest.log
opensaml	DEPURAR	ise-psc.log
pequeño	DEPURAR	ise-psc.log

> **Nota:** Cuando haya terminado de resolver problemas, recuerde restablecer los debugs seleccionando el nodo y haga clic en "Restablecer a predeterminado".

Descargar los registros

Una vez reproducido el problema, debe obtener los archivos de registro necesarios.

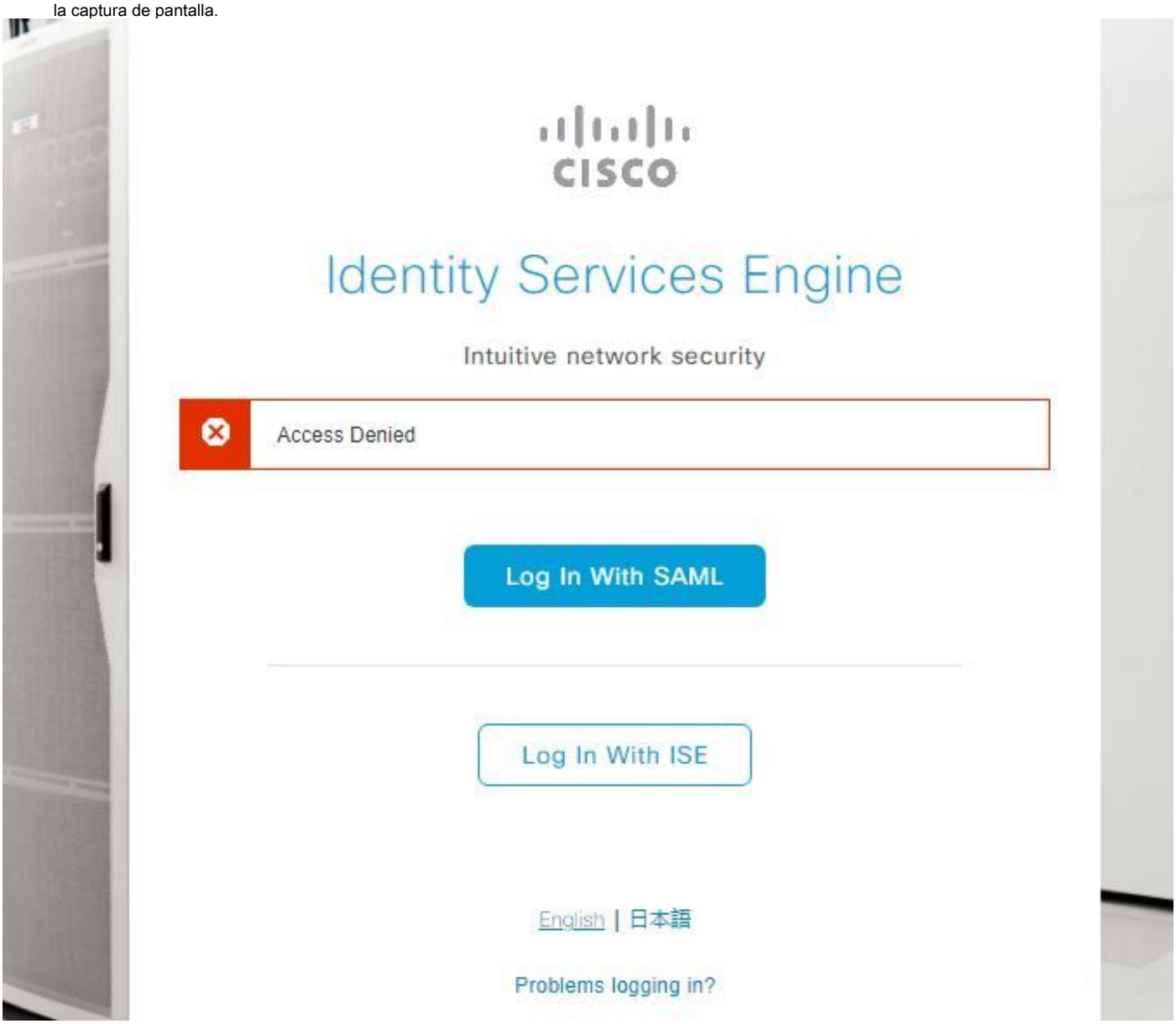
Paso 1. Navegue hasta Operaciones > Solución de problemas > Registros de descarga. Seleccione el nodo de administración principal en 'Lista de nodos de dispositivos' > Registros de depuración

Paso 2. Localizar y expandir carpetas principales de invitado e ise-psc

Paso 3. Descargar guest.log y ise-psc.log archivos.

Problema 1a: Access Denied

- Después de haber configurado su inicio de sesión de administrador basado en SAML,
  - Seleccione Iniciar sesión con SAML.
  - La redirección a la página de inicio de sesión de IdP funciona como se esperaba
  - La autenticación es correcta por respuesta SAML/IdP
  - El idP envía el atributo de grupo y puede ver el mismo ID de grupo/objeto configurado en ISE.
  - A continuación, cuando ISE intenta analizar sus políticas, lanza una excepción que provoca un mensaje de "Acceso denegado", como se muestra en la captura de pantalla.



Inicia sesión en ise-psc.log

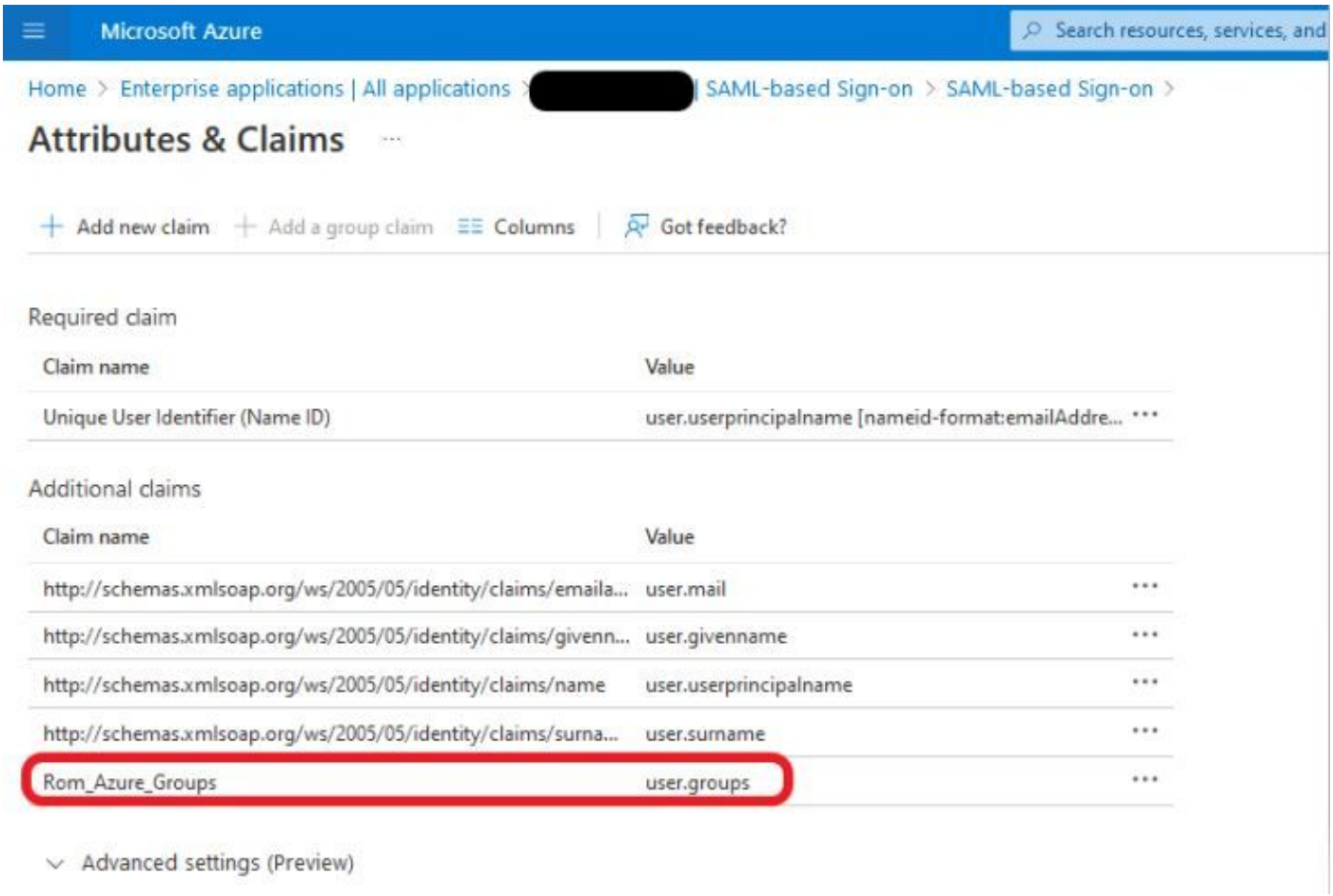
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true SAML Status Message:null SAML
email: SAML Exception:nullUserRole : NONE 2021-09-27 17:16:18,218 DEBUG [https-jsse-nio-
10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser
- about to call authenticateSAMLUser messageCode:null subject: ise.test 2021-09-27 17:16:18,225
DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAMLFacadeImpl -::::-
Authenticate SAML User - result:PASSED 2021-09-27 17:16:18,390 INFO [admin-http-pool5][]
ise.rbac.evaluator.impl.MenuPermissionEvaluatorImpl -::::- **********Rbac Log
Summary for user samlUser********** 2021-09-27 17:16:18,392 INFO [admin-http-
pool5][] com.cisco.ise.util.RBACUtil -::::- Populating cache for external to internal group
linkage. 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][]
```

```
cpm.admin.infra.utils.PermissionEvaluationUtil -::::- Exception in login action
java.lang.NullPointerException 2021-09-27 17:16:18,402 INFO [admin-http-pool5][]
cpm.admin.infra.action.LoginAction -::::- In Login Action user has Menu Permission: false 2021-
09-27 17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginAction -::::- In Login
action, user has no menu permission 2021-09-27 17:16:18,402 ERROR [admin-http-pool5][]
cpm.admin.infra.action.LoginAction -::::- Can't save locale. loginSuccess: false 2021-09-27
17:16:18,402 INFO [admin-http-pool5][] cpm.admin.infra.action.LoginActionResultHandler -::::-
Redirected to: /admin/login.jsp?mid=access_denied
```

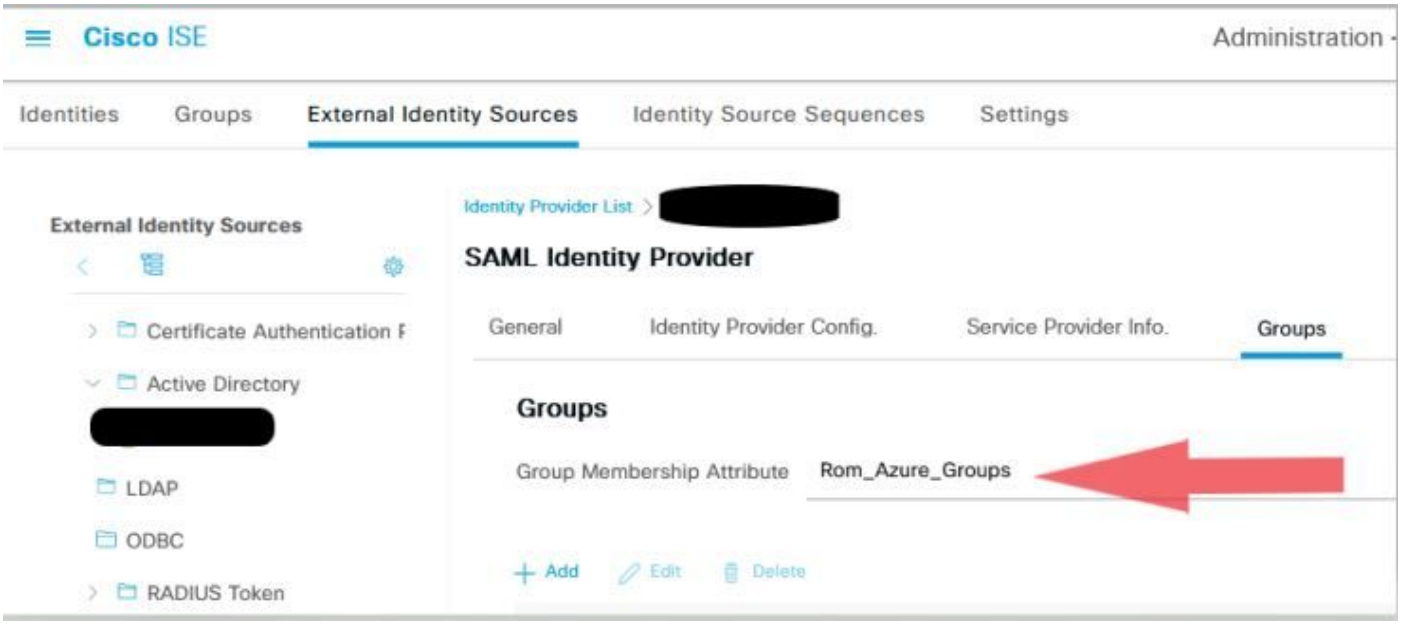
Causa/Solución

Asegúrese de que el nombre de notificación de grupo en las configuraciones de IdP sea el mismo que el configurado en ISE.

La siguiente captura de pantalla fue tomada del lado de Azure.



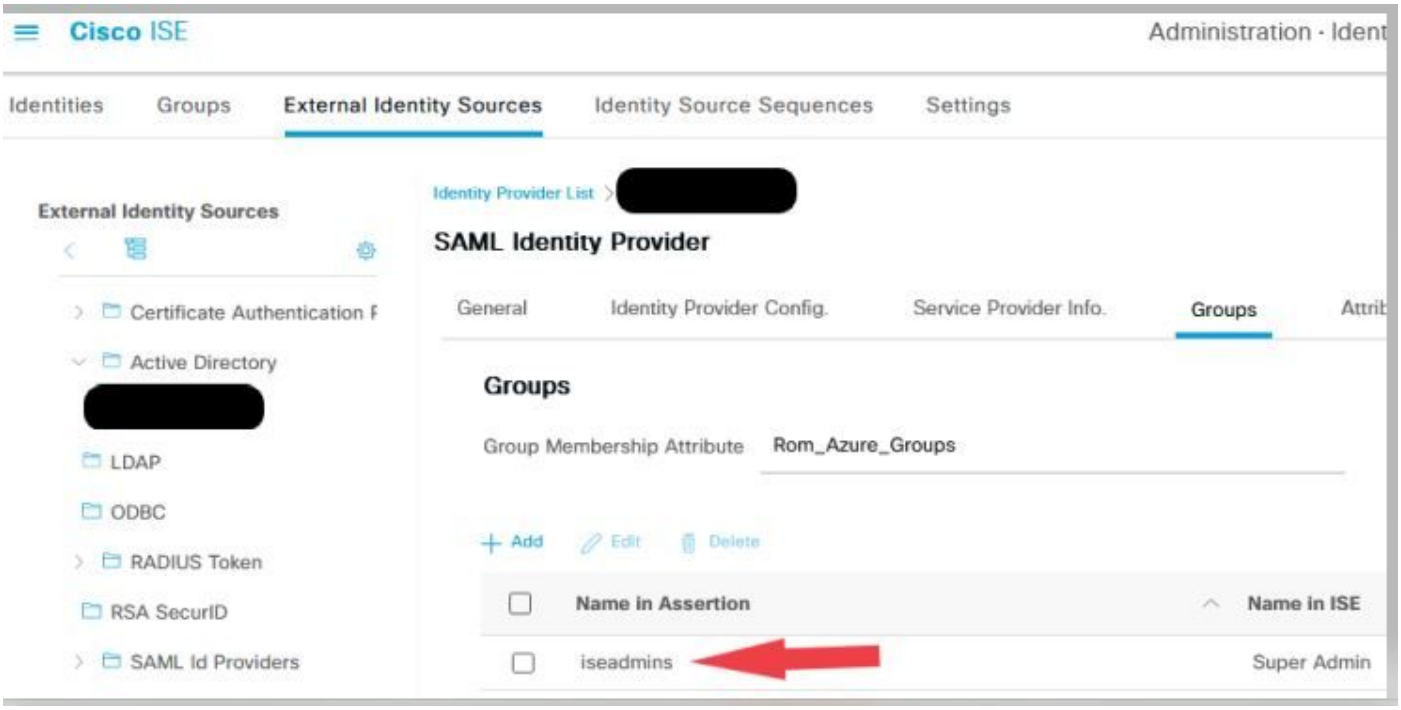
Captura de pantalla de ISE Side.



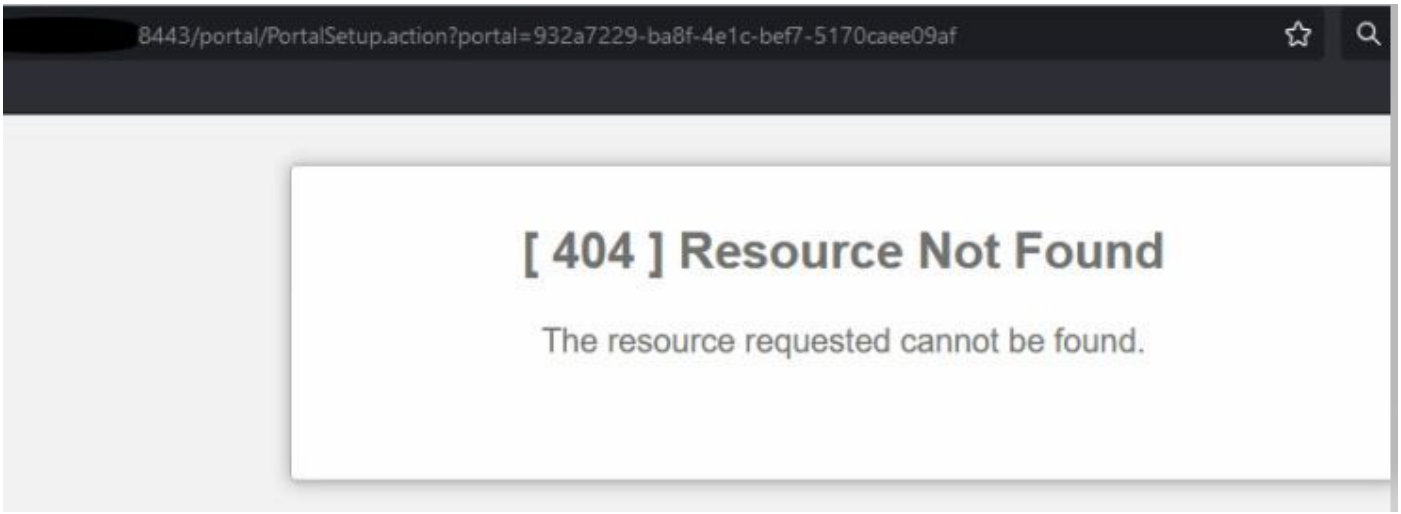
Problema 1b: Varios grupos en respuesta SAML (acceso denegado)

Si la solución anterior no resuelve el problema, asegúrese de que el usuario no es miembro de más de un grupo. Si este es el caso, debe haber encontrado el ID de bug de Cisco CSCwa17470 donde ISE solo coincide con el primer valor (nombre de grupo / ID) en la lista de respuesta SAML. Este bug se resuelve en 3.1 P3

De acuerdo con la respuesta de IdP proporcionada anteriormente, la asignación de ISE para el grupo **iseadmins** debe configurarse para que el inicio de sesión se realice correctamente.



Problema 2: 404 Recurso no encontrado



Aparece un error en **guest.log**

```
2021-10-21 13:38:49,308 ERROR  [https-jsse-nio-10.200.50.44-8443-exec-3][]
cpm.guestaccess.flowmanager.step.StepExecutor -::-
Can not find the matched transition step on Step=id: 51d3f147-5261-4eb7-a1c9-ce47ec8ec093,
tranEnum=PROCEED_SSO.
```

Causa/Solución

Este problema se observa después de crear el primer almacén de ID solamente.

Para resolver este problema, pruebe con el siguiente en el mismo orden:

Paso 1. Crear un nuevo IdP SAML en su ISE (No elimine el actual por el momento).

Paso 2. Vaya a la página de acceso de administrador y asigne su acceso de administrador a este nuevo IdP.

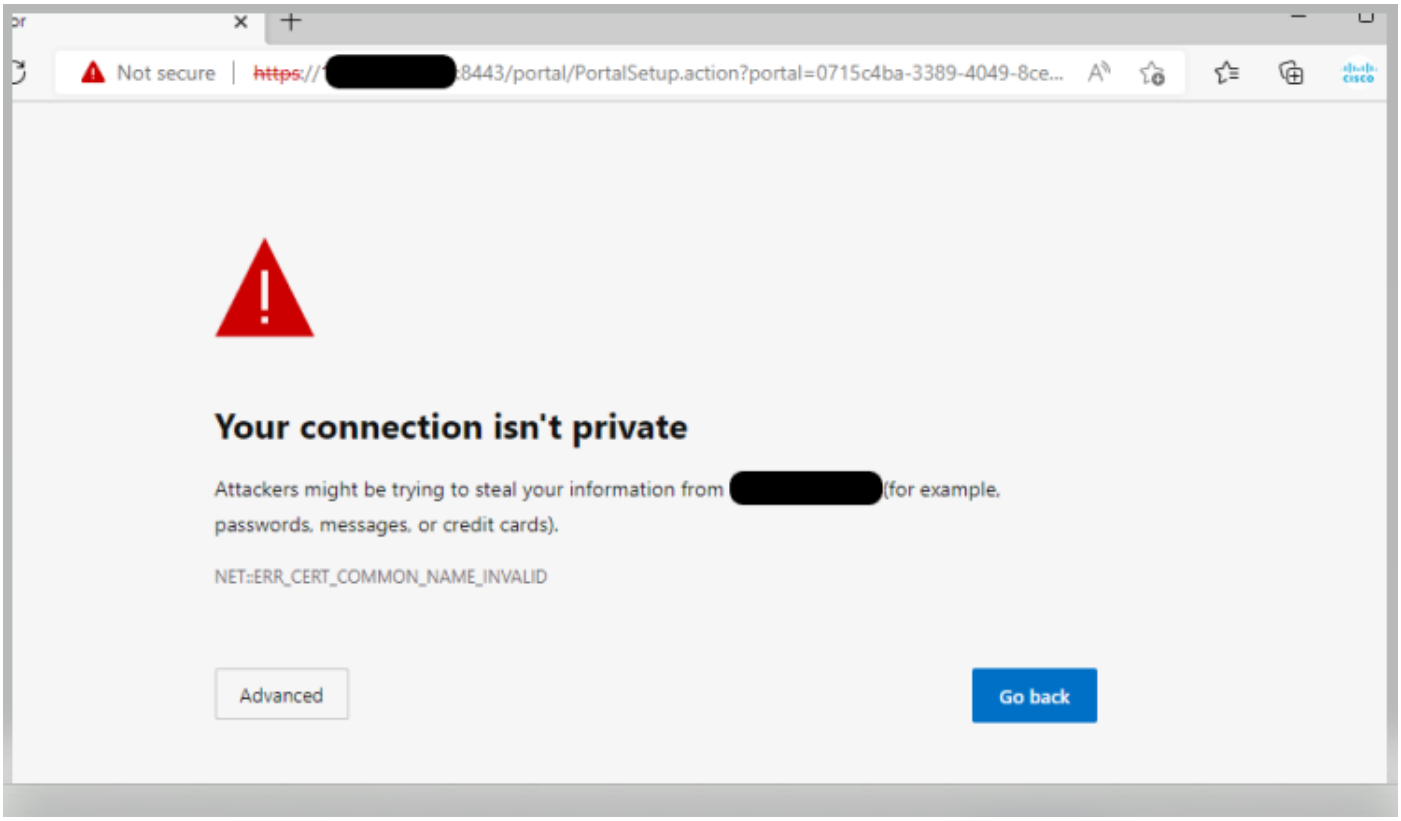
Paso 3. Suprima el IdP antiguo en la página Proveedores de Identidad Externos.

Paso 4. Importe los metadatos del IdP actual en el nuevo IdP creado en el paso 1 y realice las asignaciones de grupo necesarias.

Paso 5. Ahora intente iniciar sesión en SAML; va a funcionar.

Problema 3: Advertencia de certificado

En una implementación de varios nodos, al hacer clic en "Iniciar sesión con SAML", puede ver una advertencia de certificado no fiable en el navegador



Causa/Solución

En algunos casos, pPAN le redirige a la IP de PSNs activa, no a FQDN. Esto provoca una advertencia de certificado en algunas implementaciones PKI, si no hay ninguna dirección IP en el campo SAN.

La solución alternativa es agregar IP en el campo SAN del certificado.

Id. de error de Cisco CSCvz89415. Esto se resuelve en 3.1p1

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).