Dépannage de la connexion à l'interface utilisateur graphique ISE 3.1 avec SAML SSO

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Activer les débogages
- Télécharger les journaux
  - Problème 1a - « Accès refusé »
    - Motif
    - Solution
  - Problème 1b - Plusieurs groupes dans la réponse SAML ("Accès refusé")
  - Problème 2 - « Ressource 404 introuvable »
    - Motif
    - Solution
  - Problème 3 - Avertissement de certificat
    - Motif
    - Solution

Introduction

Ce document décrit la plupart des problèmes qui ont été observés dans ISE 3.1 avec la connexion SAML GUI.

Conditions préalables

Grâce à l'utilisation de la norme SAML 2.0, la connexion d'administrateur basée sur SAML ajoute la fonctionnalité SSO (Single Sign-on) à ISE. Vous pouvez utiliser n'importe quel fournisseur d'identité (IdP) tel qu'Azure, Okta, PingOne, DUO Gateway ou n'importe quel fournisseur d'identité qui implémente SAML 2.0.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

1. Cisco ISE 3.1 ou version ultérieure
2. Comprendre les bases des configurations SSO SAML.

Référez-vous au guide d'administration d'ISE 3.1 pour la configuration SAML et au flux de connexion d'administration d'ISE via SAML avec Azure AD pour plus de détails sur la configuration et le flux.

Remarque : Vous devez vous familiariser avec votre service de fournisseur d'identité et vous assurer qu'il est opérationnel.

Composants utilisés

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

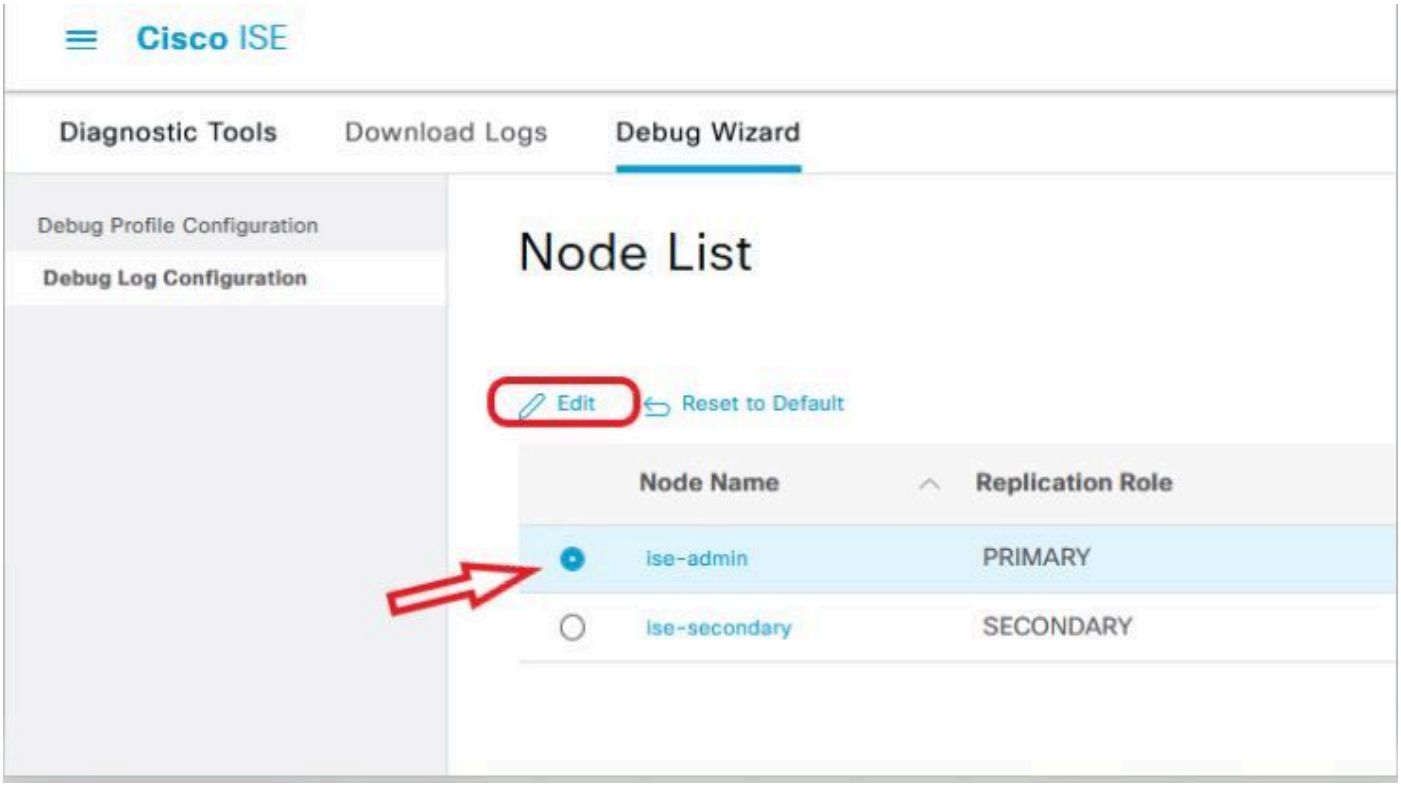
- ISE version 3.1

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Activer les débogages

Pour commencer le dépannage, vous devez d'abord activer les débogages comme décrit ci-dessous.

Accédez à Operations > Troubleshoot > Debug Wizard > Debug Log Configuration. Sélectionnez le noeud d'administration principale et cliquez sur Edit comme indiqué dans l'image suivante.



- Définissez le niveau DEBUG pour les composants suivants.

Nom du composant	Niveau de consignation	Nom du fichier journal
portail	DÉBOGUER	guest.log
ouvert	DÉBOGUER	ise-psc.log
petit	DÉBOGUER	ise-psc.log

Remarque : Lorsque vous avez terminé le dépannage, n'oubliez pas de réinitialiser les débogages en sélectionnant le noeud et cliquez sur Reset to Default.

Télécharger les journaux

Une fois le problème reproduit, vous devez obtenir les fichiers journaux nécessaires.

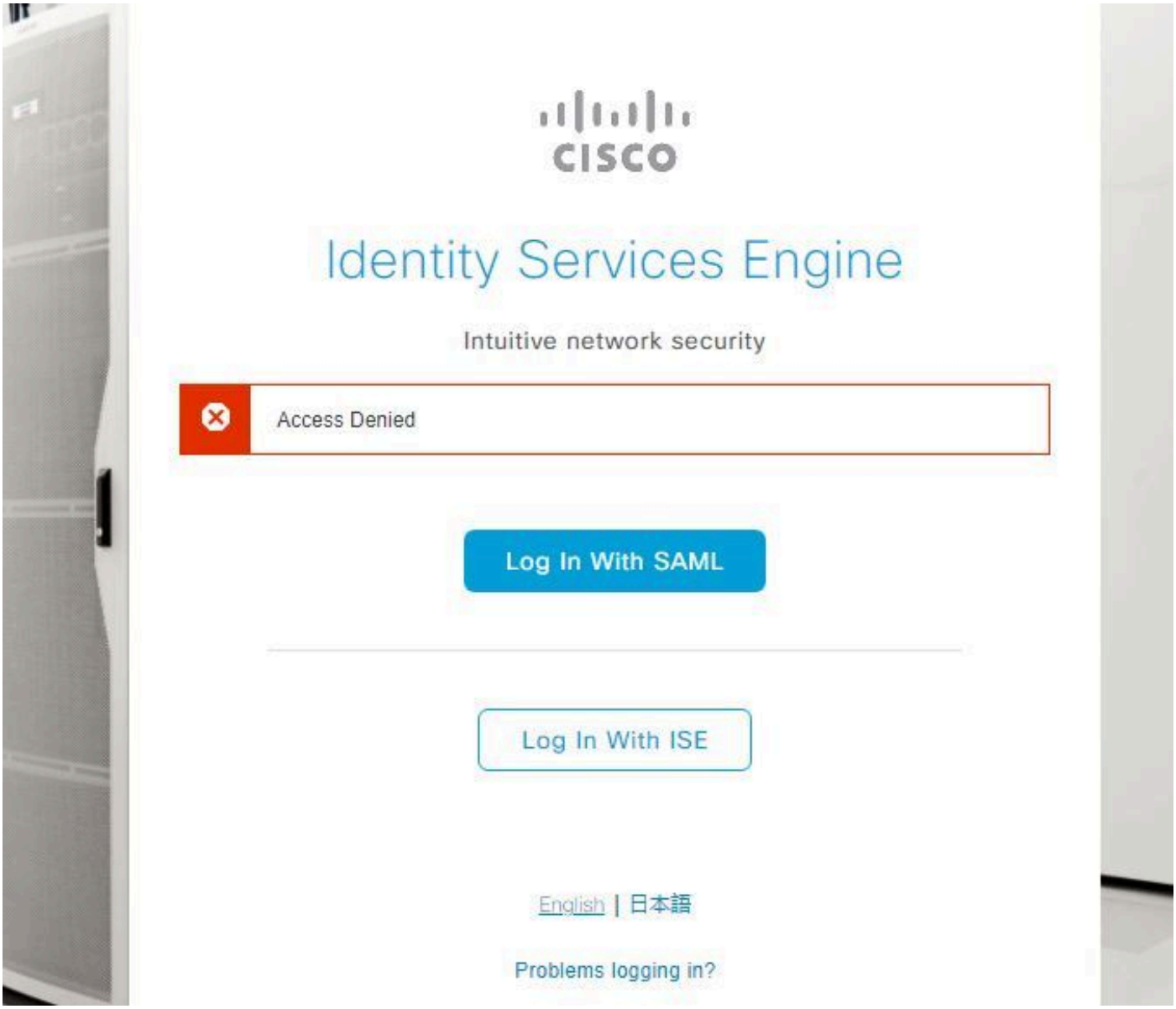
Étape 1. Accédez à Operations > Troubleshoot > Download logs. Sélectionnez le noeud d'administration principal sous Liste de noeuds du matériel > Journaux de débogage.

Étape 2. Localisation et développement des dossiers parent invité et ise-psc

Étape 3 : téléchargement des fichiers guest.log et ise-psc.log

Problème 1a - « Accès refusé »

- Après avoir configuré votre connexion d'administrateur SAML.
- Sélectionnez Se connecter avec SAML.
- La redirection vers la page de connexion IdP fonctionne comme prévu.
- L'authentification est réussie par réponse SAML/IdP.
- IdP envoie un attribut de groupe et vous pouvez voir le même ID de groupe/d'objet configuré dans ISE.
- Ensuite, alors qu'ISE tente d'analyser ses stratégies, il génère une exception qui entraîne un message « Accès refusé », comme indiqué dans la capture d'écran.



Journaux dans 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.SAML
```

```
                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.SAML
2021-09-27 17:16:18,225 DEBUG  [https-jsse-nio-10.200.50.44-8443-exec-2][] cpm.saml.framework.impl.SAML
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
2021-09-27 17:16:18,402 ERROR  [admin-http-pool5][] cpm.admin.infra.utils.PermissionEvaluationUtil -:::

java.lang.NullPointerException

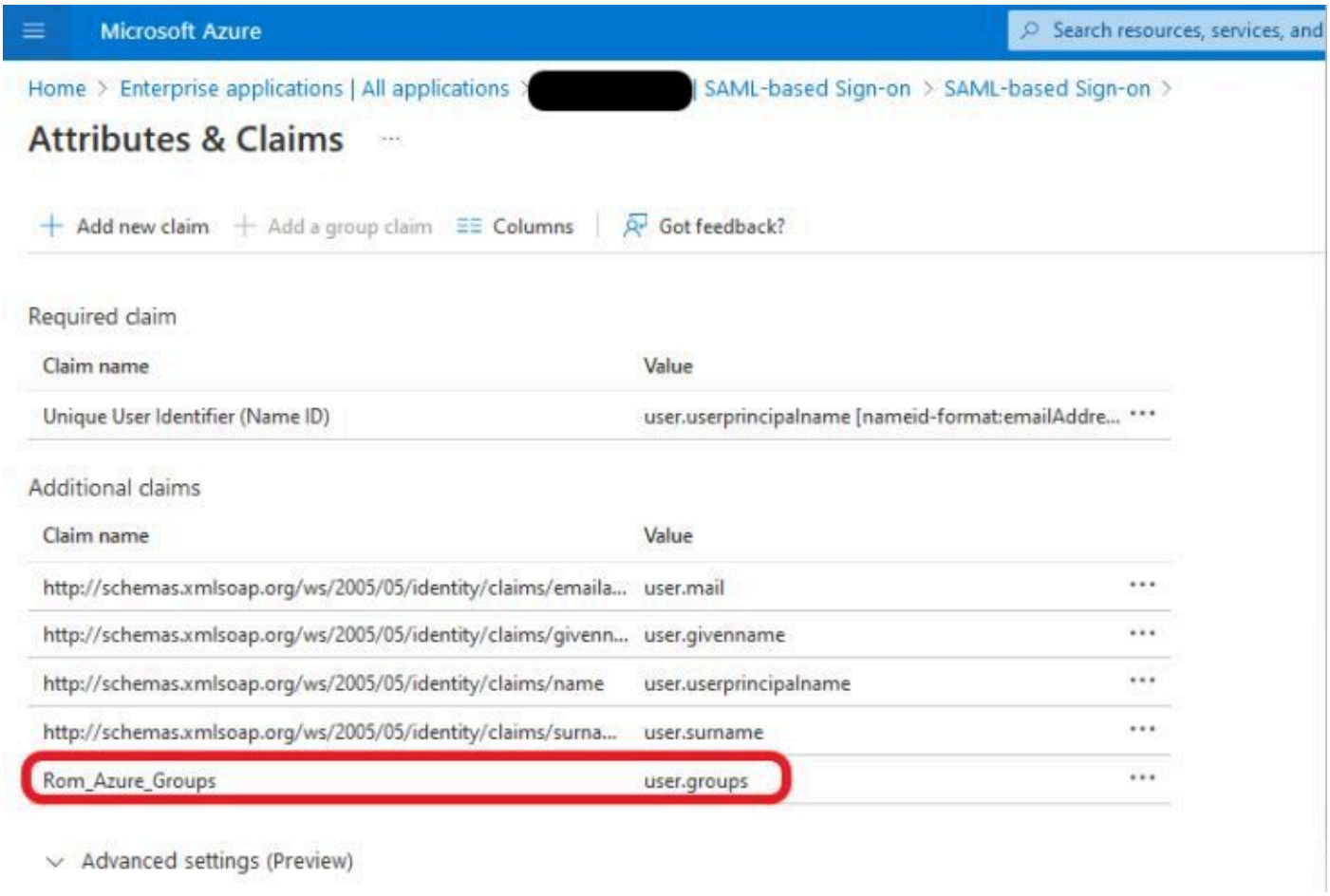
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- In Login
2021-09-27 17:16:18,402 ERROR  [admin-http-pool5][] cpm.admin.infra.action.LoginAction -:::::- Can't sav
2021-09-27 17:16:18,402 INFO   [admin-http-pool5][] cpm.admin.infra.action.LoginActionResultHandler -::
```

Motif

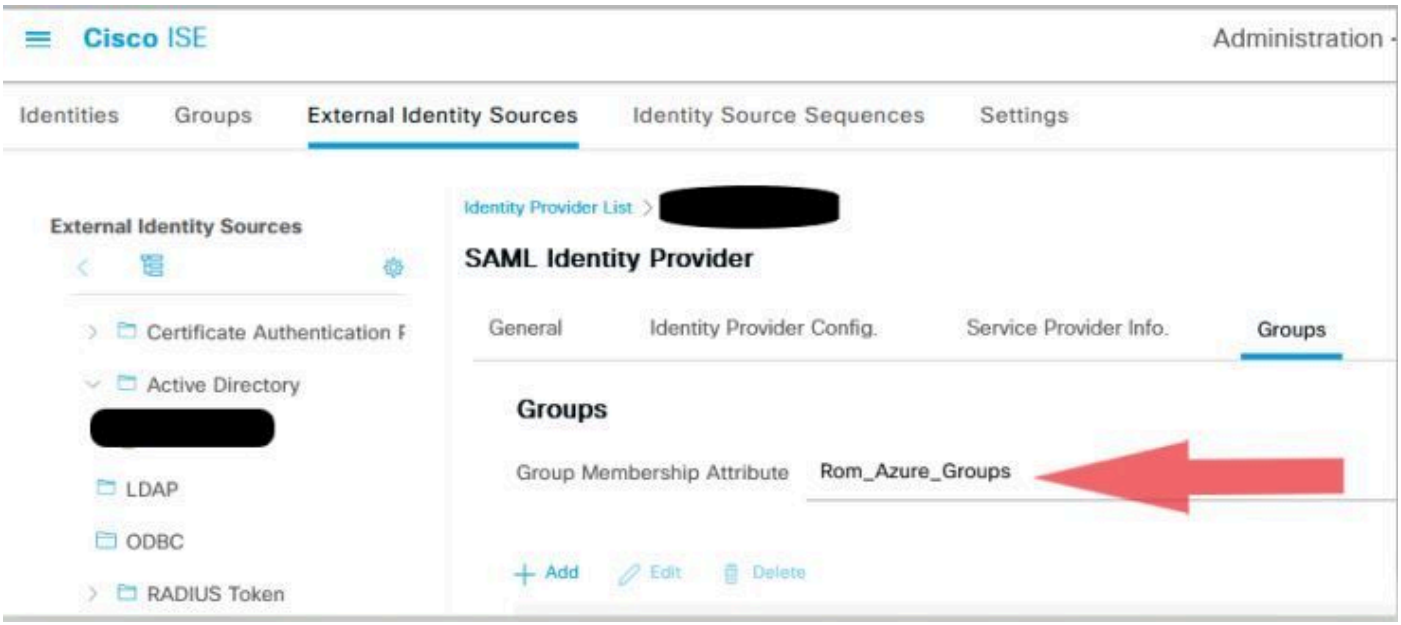
Assurez-vous que le nom de la revendication de groupe dans les configurations IdP est identique à celui configuré dans ISE.

Solution

La capture d'écran suivante a été prise du côté Azure :



Capture d'écran côté ISE :



Problème 1b - Plusieurs groupes dans la réponse SAML ("Accès refusé")

Si le correctif précédent ne résout pas le problème, assurez-vous que l'utilisateur n'est pas

membre de plusieurs groupes. Si c'est le cas, vous devez avoir rencontré le bogue Cisco ID CSCwa17470 où ISE correspond seulement à la première valeur (nom de groupe / ID) dans la liste de la réponse SAML. Ce bogue est résolu dans 3.1 P3.

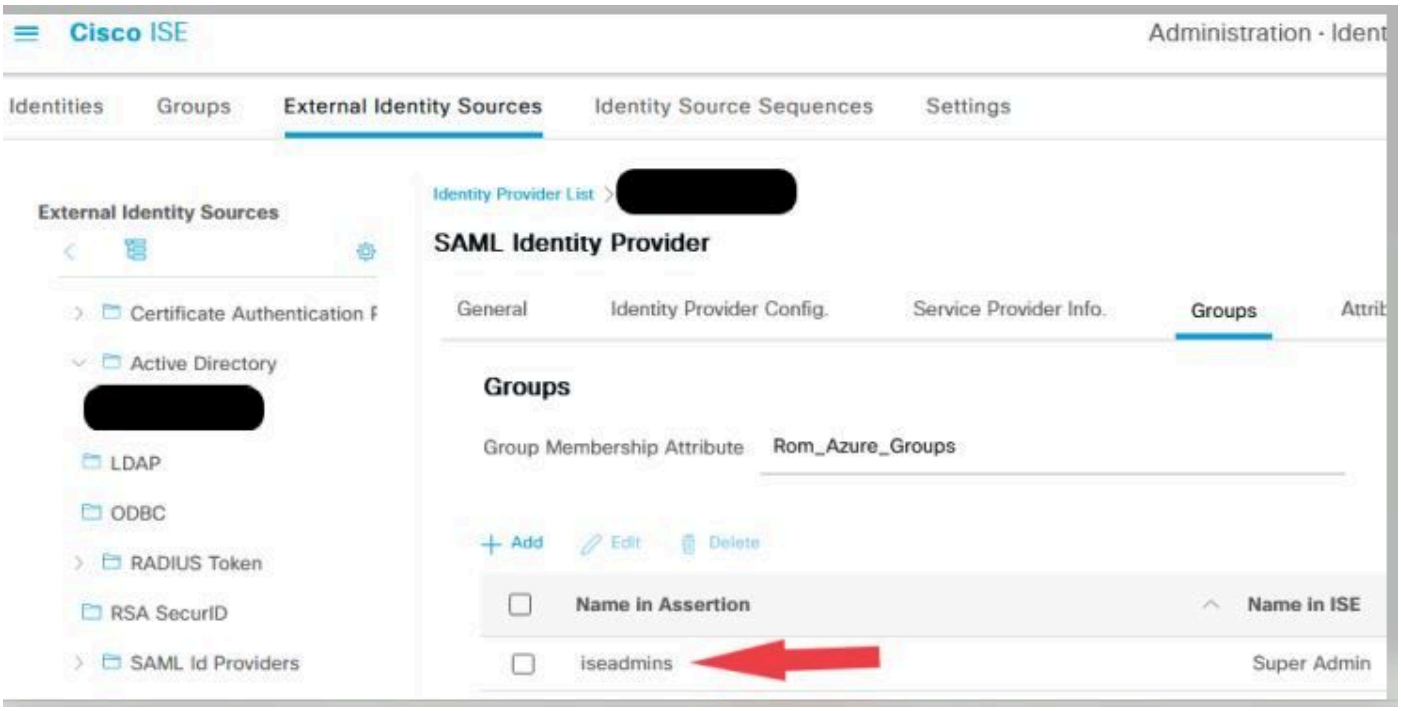
```
iseadmins
```

```
Sysadmins
```

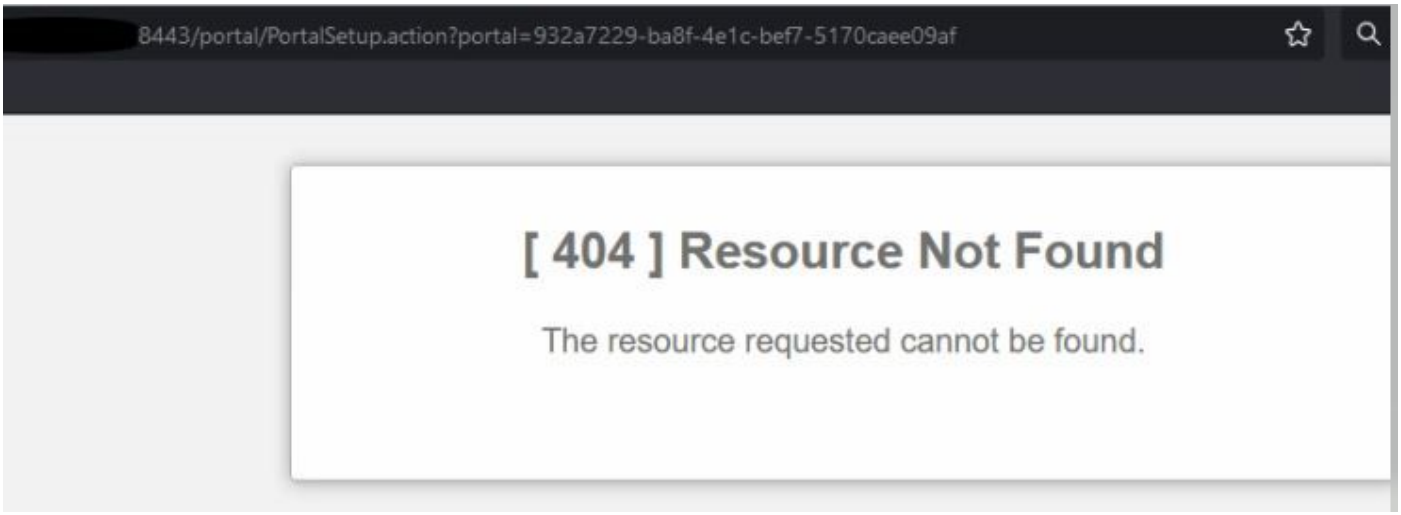
```
domain admins
```

```
change-esc
```

Selon la réponse IdP donnée précédemment, le mappage ISE du groupe iseadmins doit être configuré pour que la connexion réussisse.



Problème 2 - « Ressource 404 introuvable »



Vous voyez une erreur dans guest.log :

<#root>

```
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=PROC
```

Motif

Ce problème est observé après la création du premier magasin d'ID uniquement.

Solution

Pour résoudre ce problème, essayez la suivante dans le même ordre :

Étape 1 : création d'un nouveau fournisseur d'identité SAML dans votre ISE (ne supprimez pas encore le fournisseur actuel)

Étape 2. Accédez à la page d'accès admin et attribuez votre accès admin à ce nouveau fournisseur d'identité.

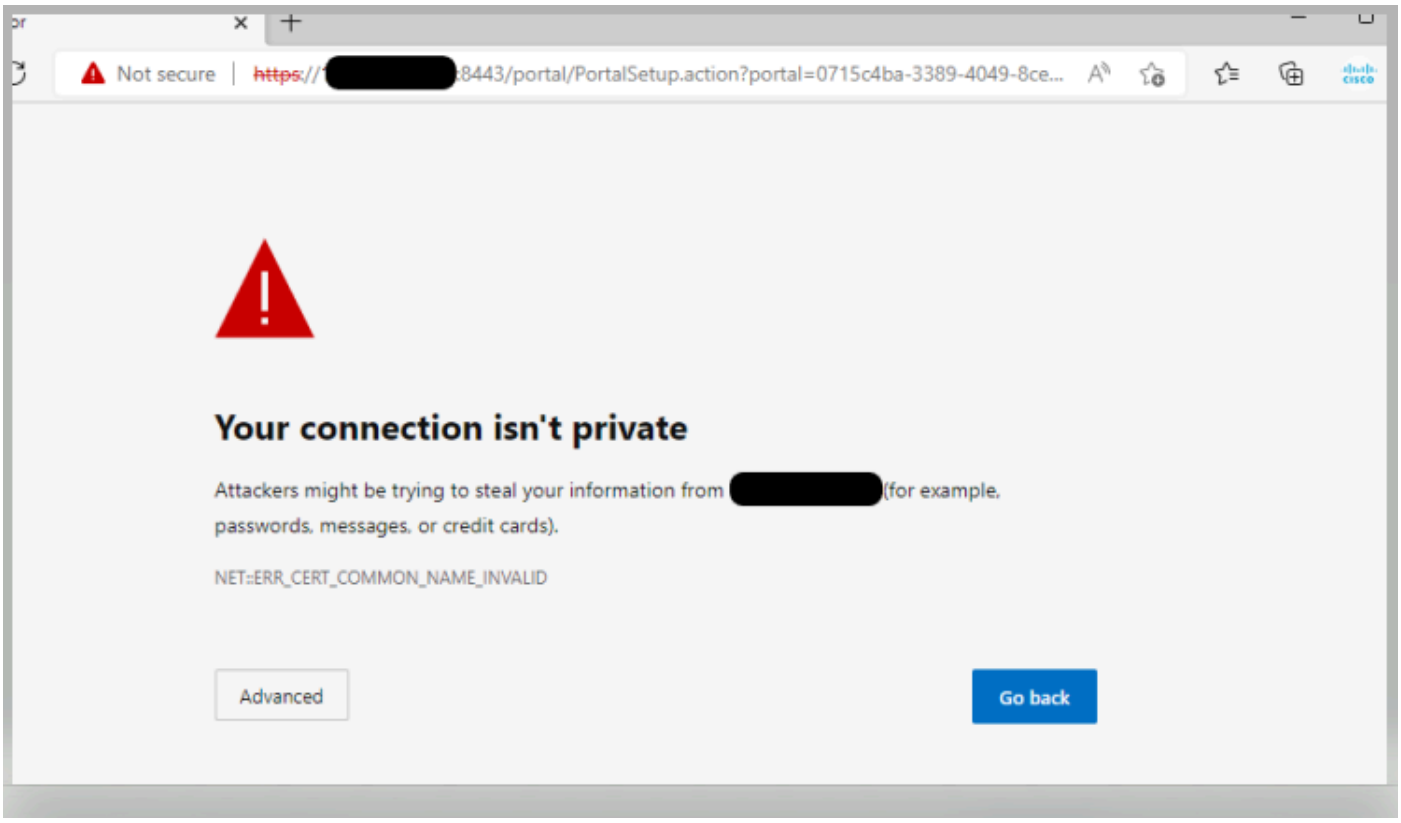
Étape 3 : suppression de l'ancien fournisseur d'identités dans la page Fournisseurs d'identités externes

Étape 4. Importez les métadonnées IdP actuelles dans le nouvel IdP créé à l'étape 1 et effectuez les mappages de groupe nécessaires.

Étape 5. Essayez à présent de vous connecter à SAML et assurez-vous qu'il fonctionne.

Problème 3 - Avertissement de certificat

Dans un déploiement à plusieurs noeuds, lorsque vous cliquez sur Se connecter avec SAML, vous pouvez voir l'avertissement de certificat non approuvé dans le navigateur :



Motif

Dans certains cas, pPAN vous redirige vers l'adresse IP des PSN actifs, et non vers le nom de domaine complet. Cela entraîne un avertissement de certificat dans certains déploiements PKI, s'il n'y a pas d'adresse IP dans le champ SAN.

Solution

La solution de contournement consiste à ajouter IP dans le champ SAN du certificat.

ID de bogue Cisco CSCvz89415. Ceci est résolu dans 3.1p1.

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.