Risoluzione dei problemi relativi all'interfaccia utente grafica di ISE 3.1 Accesso con SAML SSO

Sommario

Introduzione

Questo documento descrive la maggior parte dei problemi osservati in ISE 3.1 con l'accesso tramite GUI SAML. Usando lo standard SAML 2.0, l'accesso tramite amministratore basato su SAML aggiunge la funzionalità Single Sign-On (SSO) ad ISE. È possibile utilizzare qualsiasi provider di identità (IdP), ad esempio Azure, Okta, PingOne, DUO Gateway o qualsiasi IdP che implementa SAML 2.0.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

1. Cisco ISE 3.1 o superiore
2. Informazioni di base sulle impostazioni di SAML SSO

Per ulteriori dettagli sulla configurazione e sul flusso di accesso a ISE Admin tramite SAML con Azure AD, consultare la guida per l'amministratore di ISE 3.1 per la configurazione SAML e il flusso di accesso ad ISE.

> **Nota:** È necessario avere familiarità con il servizio Identity Provider e assicurarsi che sia attivo e in esecuzione.

Componenti usati

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

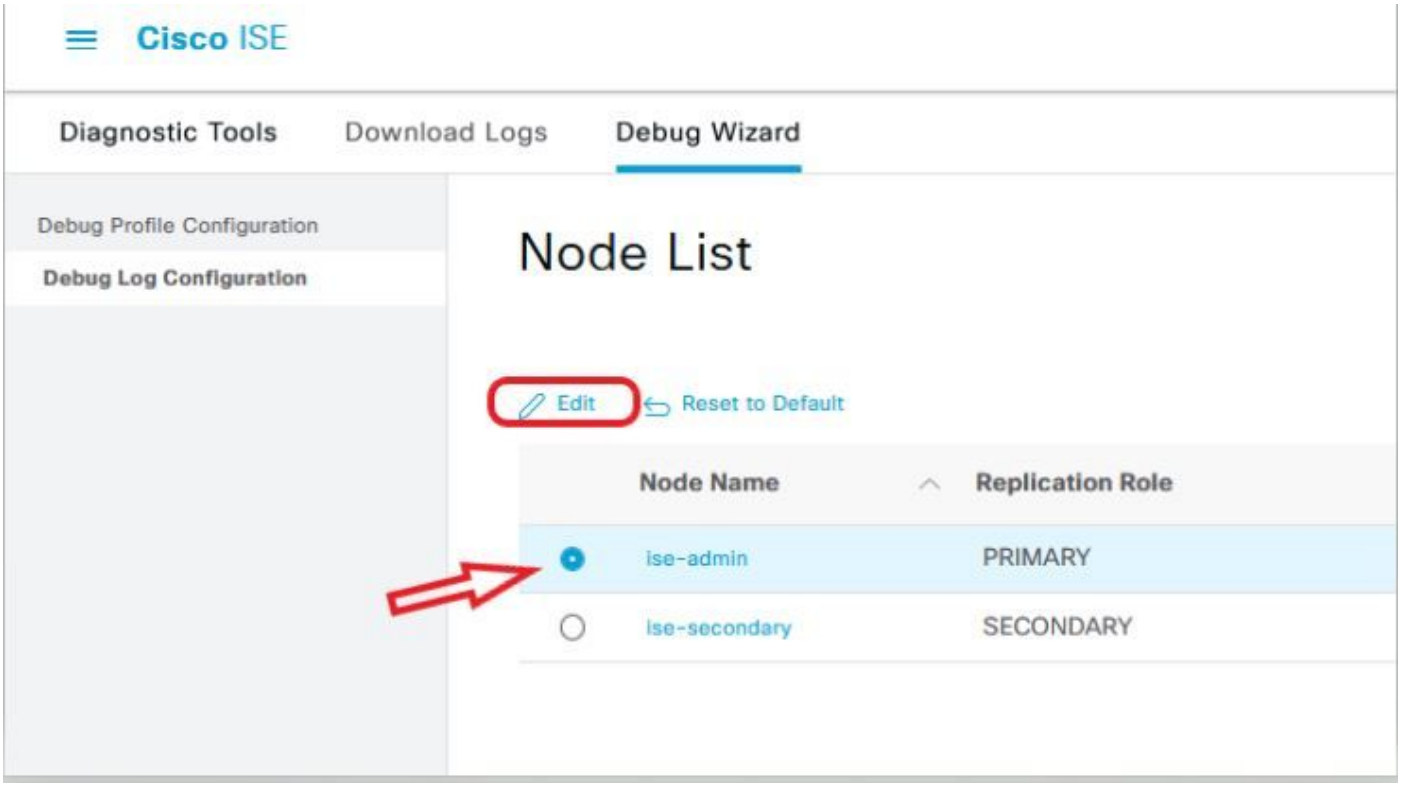
- ISE versione 3.1

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.

Abilita debug

Per avviare la risoluzione dei problemi, è necessario abilitare i debug come descritto di seguito.

Passare a **Operazioni > Risoluzione dei problemi > Debug guidato > Configurazione log di debug.** Selezionare il nodo Amministrazione primaria e fare clic su **Modifica** come mostrato nell'immagine successiva.



- Impostare i componenti successivi al livello **DEBUG**.

Nome componente	Livello log	Nome file di log
portale	DEBUG	guest.log
opensaml	DEBUG	ise-psc.log
saml	DEBUG	ise-psc.log

Nota: Al termine della risoluzione dei problemi, ricordarsi di ripristinare i debug selezionando il nodo e fare clic su "Ripristina valori predefiniti".

Scarica i log

Una volta riprodotto il problema, è necessario ottenere i file di registro necessari.

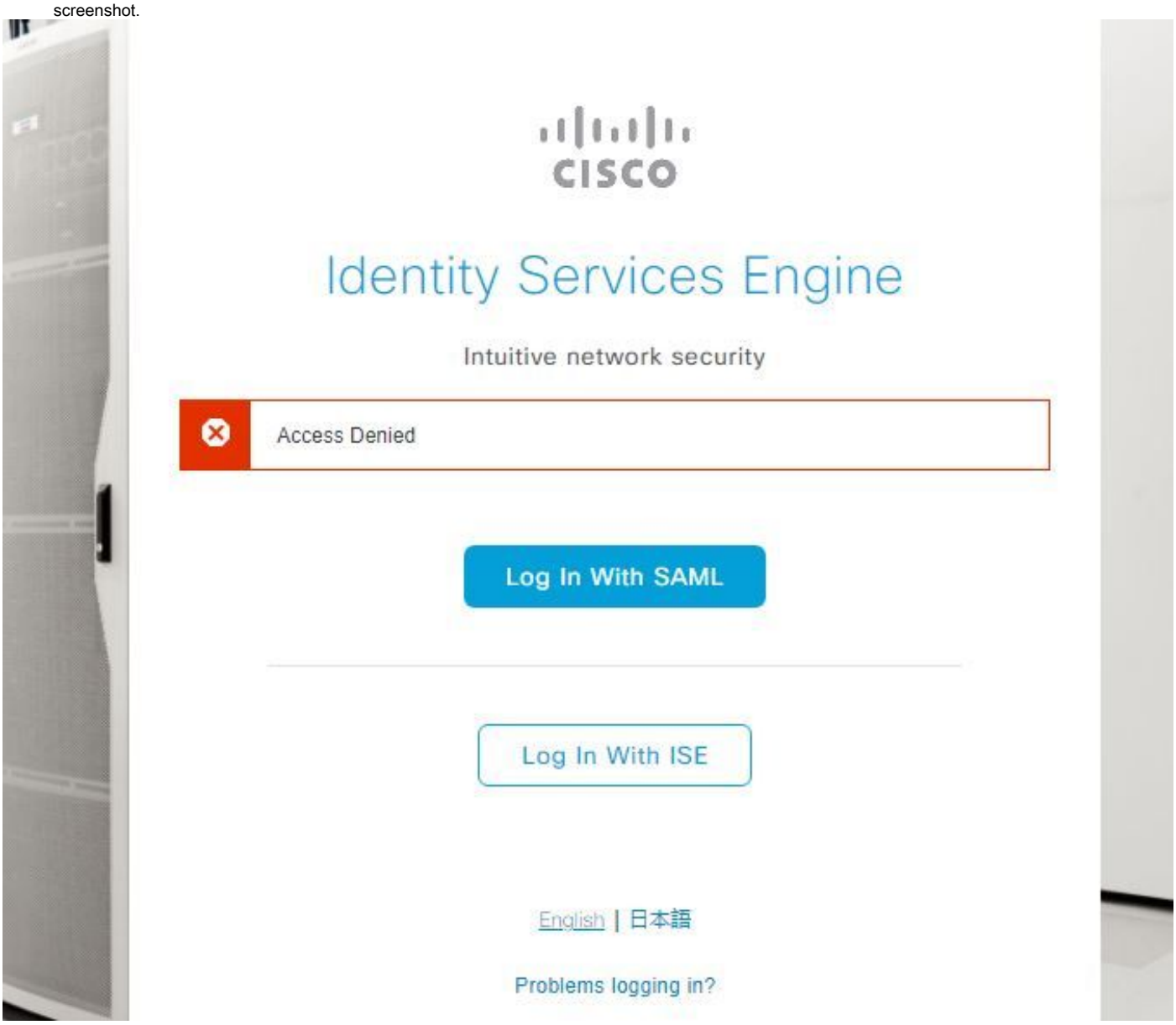
Passaggio 1. Passare a Operazioni > Risoluzione dei problemi > Scarica log. Selezionare il nodo di amministrazione principale in 'Elenco nodi accessorio' > Registri di debug

Passaggio 2. Individuare ed espandere le cartelle guest e ise-psc padre

Passaggio 3. Download guest.log e ise-psc.log file.

Problema 1a: Accesso negato

- Dopo aver configurato il login dell'amministratore basato su SAML,
- Selezionare Log in With SAML (Accedi con SAML).
- Il reindirizzamento alla pagina di accesso IdP funziona come previsto
- Autenticazione riuscita per risposta SAML/IdP
- IdP invia l'attributo gruppo ed è possibile vedere lo stesso ID gruppo/oggetto configurato in ISE.
- Quindi, mentre ISE cerca di analizzare le sue policy, genera un'eccezione che causa un messaggio di "Accesso negato", come mostrato nello screenshot.



Effettua il login in ise-psc.log

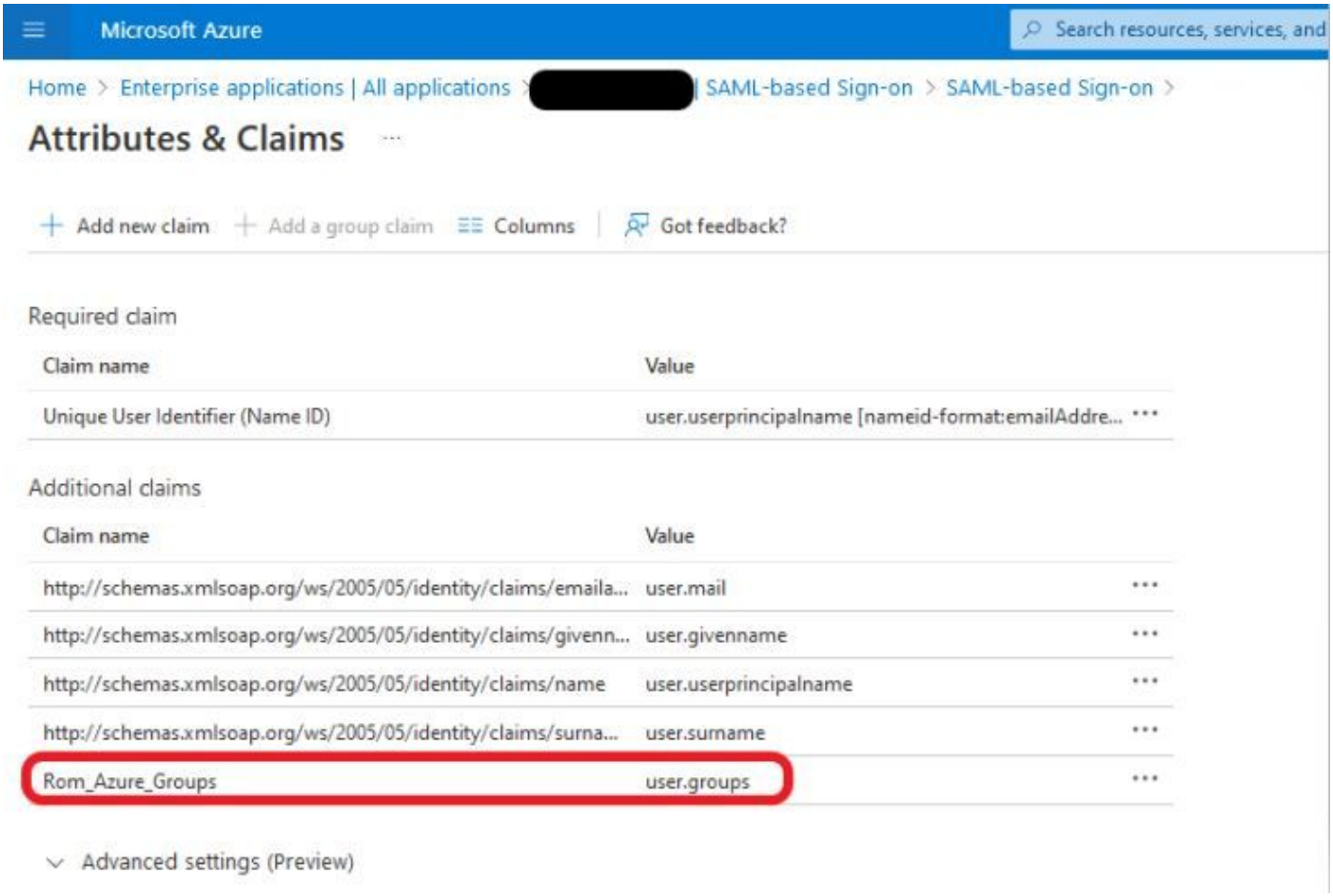
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true 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
```

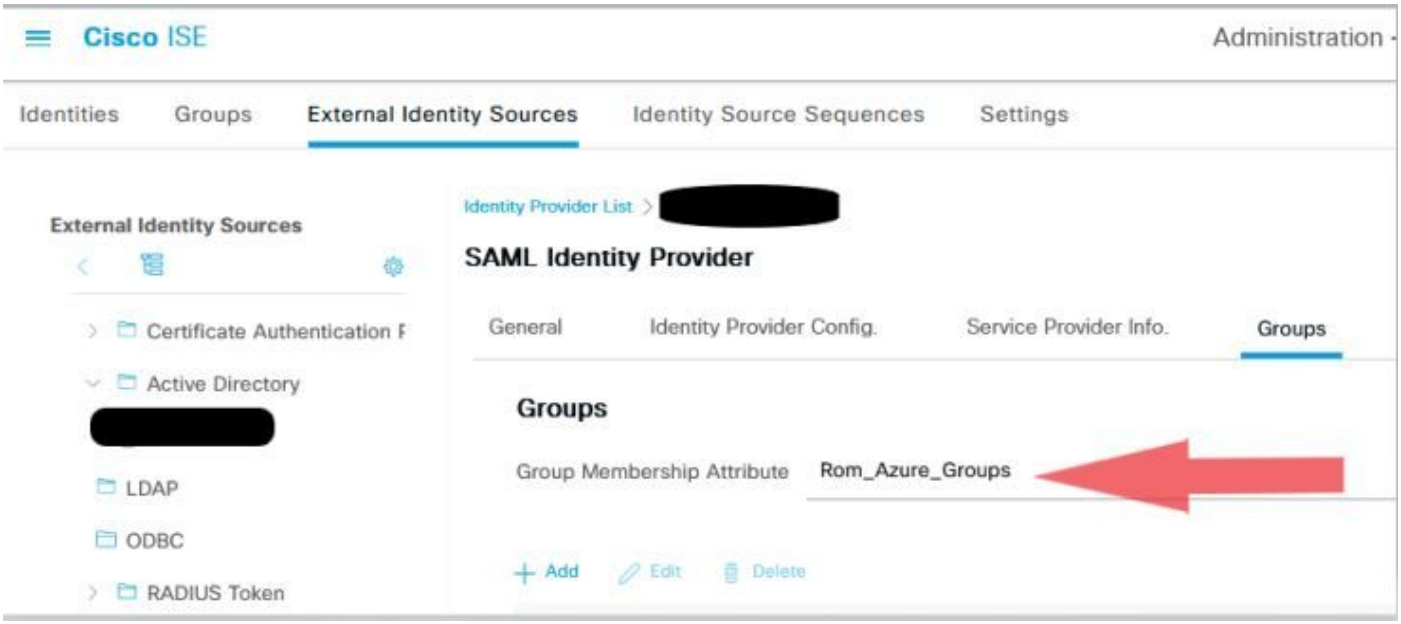
Causa/soluzione

Verificare che il nome dell'attestazione basata su gruppo nelle configurazioni IdP sia uguale a quello configurato in ISE.

Lo screenshot successivo è stato acquisito dal lato di Azure.



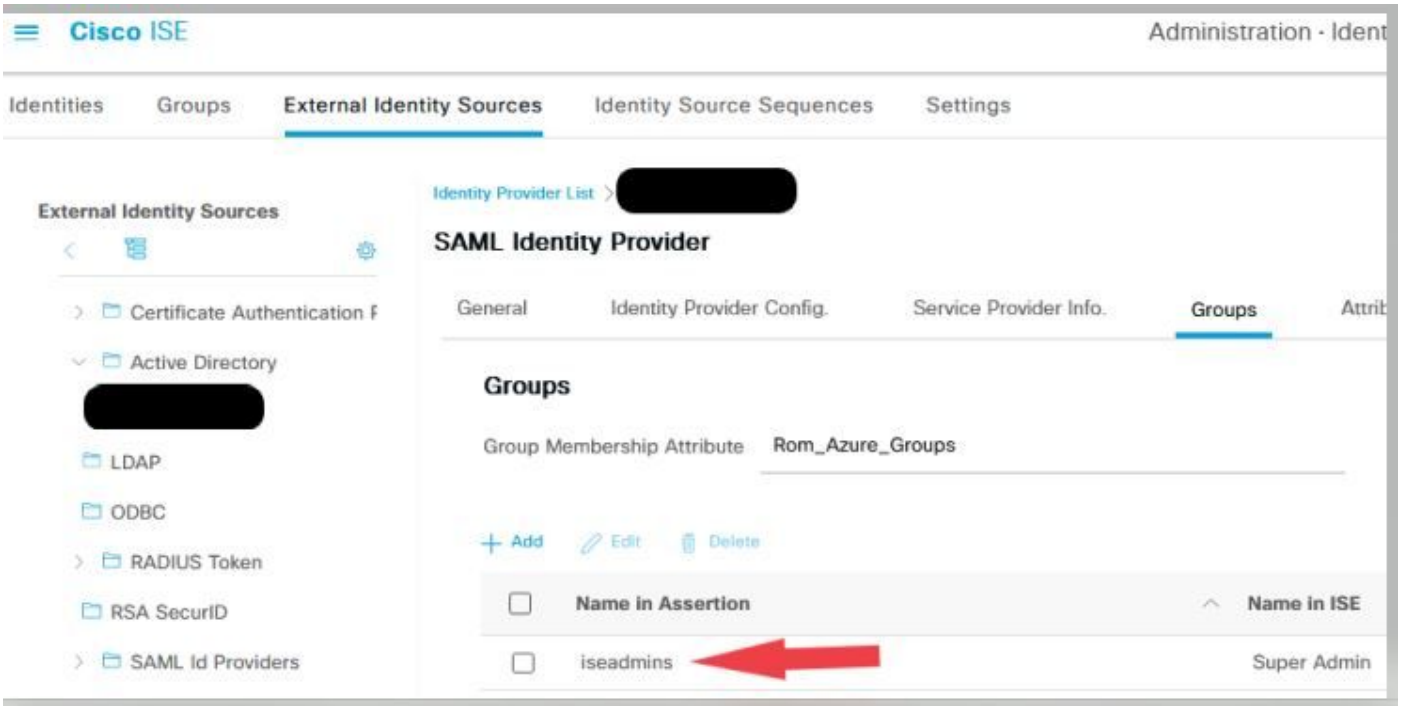
Screenshot da ISE Side



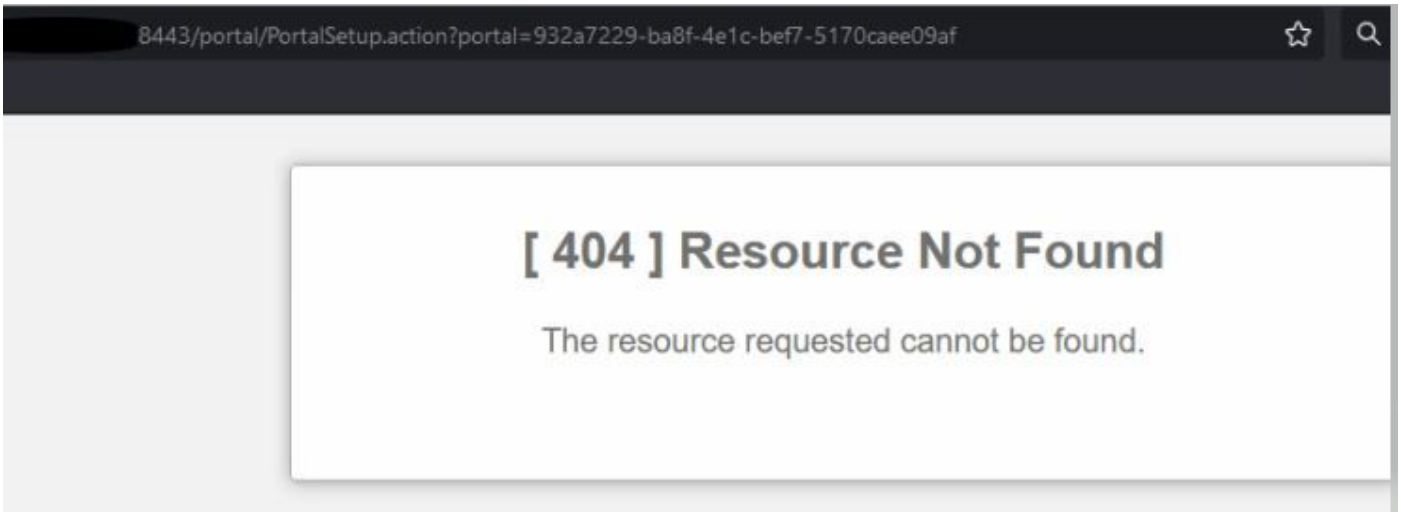
Problema 1b: Più gruppi nella risposta SAML (accesso negato)

Se la correzione precedente non risolve il problema, verificare che l'utente non sia membro di più gruppi. In questo caso, è necessario che l'ID bug Cisco CSCwa17470 sia stato trovato dove ISE corrisponde solo al primo valore (nome gruppo / ID) dell'elenco nella risposta SAML. Il bug è stato risolto nella versione 3.1 P3

In base alla risposta del provider di identità fornita in precedenza, il mapping ISE per il gruppo **iseadmins** deve essere configurato per il corretto accesso.



Problema 2: Risorsa 404 non trovata



Errore in **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/soluzione

Questo problema si verifica dopo la creazione del solo primo archivio ID.

Per risolvere il problema, provare con il comando successivo nello stesso ordine:

Passaggio 1. Crea un nuovo SAML IdP nell'ISE (non rimuovere ancora quello corrente).

Passaggio 2. Andare alla pagina di accesso come amministratore e assegnare all'amministratore l'accesso a questo nuovo IdP.

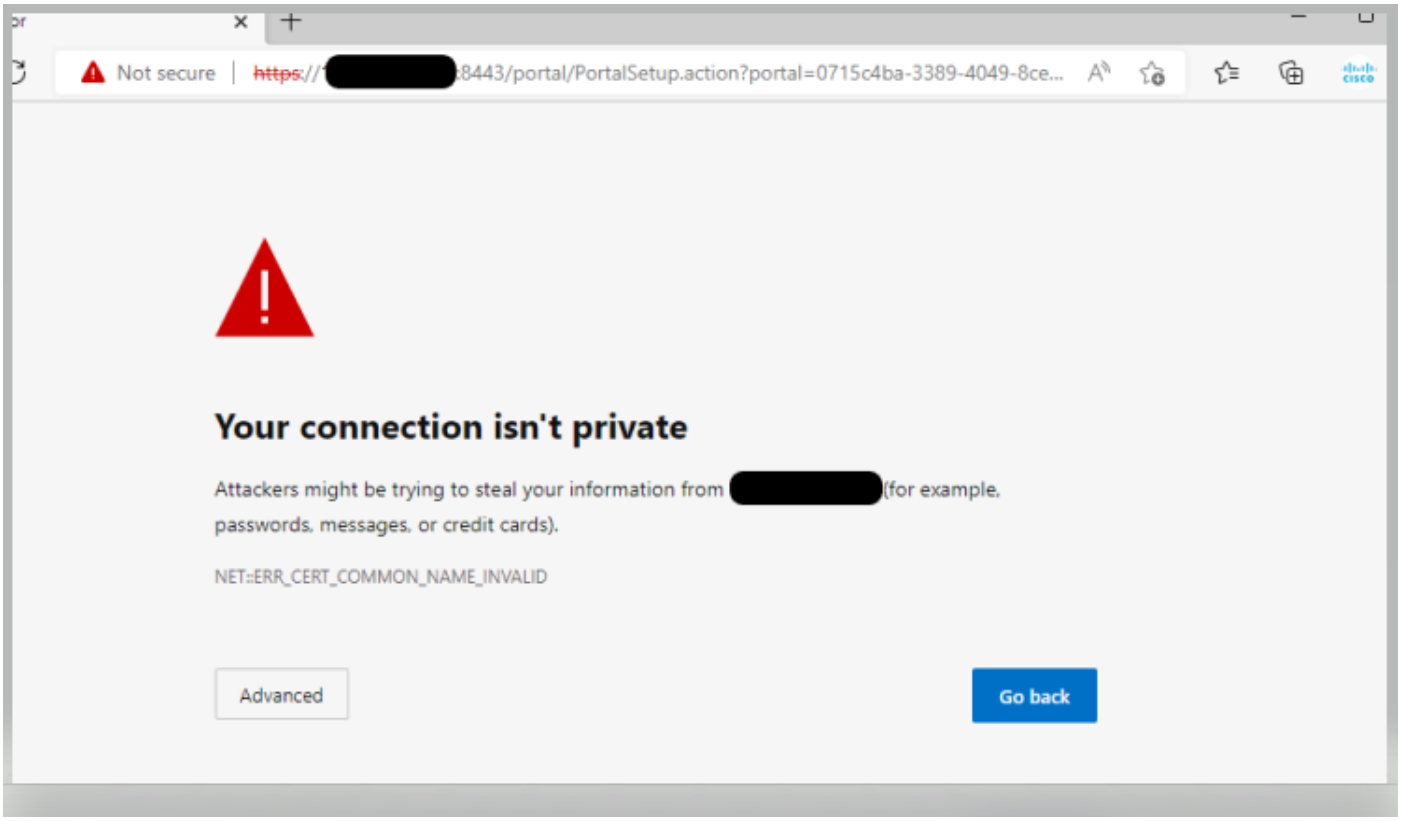
Passaggio 3. Eliminare l'IdP precedente nella pagina Provider di identità esterni.

Passaggio 4. Importare i metadati IdP correnti nel nuovo IdP creato nel passaggio 1 ed eseguire i mapping di gruppo necessari.

Passaggio 5. Provare ad accedere a SAML. funzionerà.

Problema 3: Avviso certificato

In una distribuzione a più nodi, quando si fa clic su "Log In with SAML" (Accedi con SAML), nel browser viene visualizzato un avviso di certificato non attendibile



Causa/soluzione

In alcuni casi, pPAN reindirizza l'utente all'IP dei nomi di dominio primario (PSN) attivi, non al nome di dominio completo (FQDN). In alcune distribuzioni di PKI ciò provoca la visualizzazione di un avviso di certificato se nel campo SAN non è presente alcun indirizzo IP.

Per risolvere il problema, aggiungere l'indirizzo IP nel campo SAN del certificato.

ID bug Cisco CSCvz89415. La causa è da ricercare nella versione 3.1p1

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).