أستكشاف أخطاء تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل ISE 3.1 وإصلاحها باستخدام SAML SSO

المحتويات

المقدمة

يصف هذا المستند معظم المشاكل التي تم مواجهتها في ISE 3.1 مع تسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل SAML. من خلال استخدام معيار SAML 2.0، يمكن إعداد مزود هوية تسجيل الدخول الأحادي (SSO) إلى ISE. يمكن استخدام أي موفر هوية (IDp) مثل Azure أو OKTA أو PingOne أو Duo أو أي مزود P يطبق SAML 2.0.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

1. Cisco ISE 3.1 أو أعلى
2. فهم أساسيات SAML SSO Setups

ارجع إلى دليل مسؤول ISE 3.1 لتكوين SAML وتدفق تسجيل دخول مسؤول ISE عبر SAML مع Azure AD للحصول على مزيد من التفاصيل حول التكوين والتدفق.

> **ملاحظة:** يجب أن تكون على دراية بخدمة مزود الهوية، وتأكد من أنها تعمل بكفاءة.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- ISE الإصدار 3.1

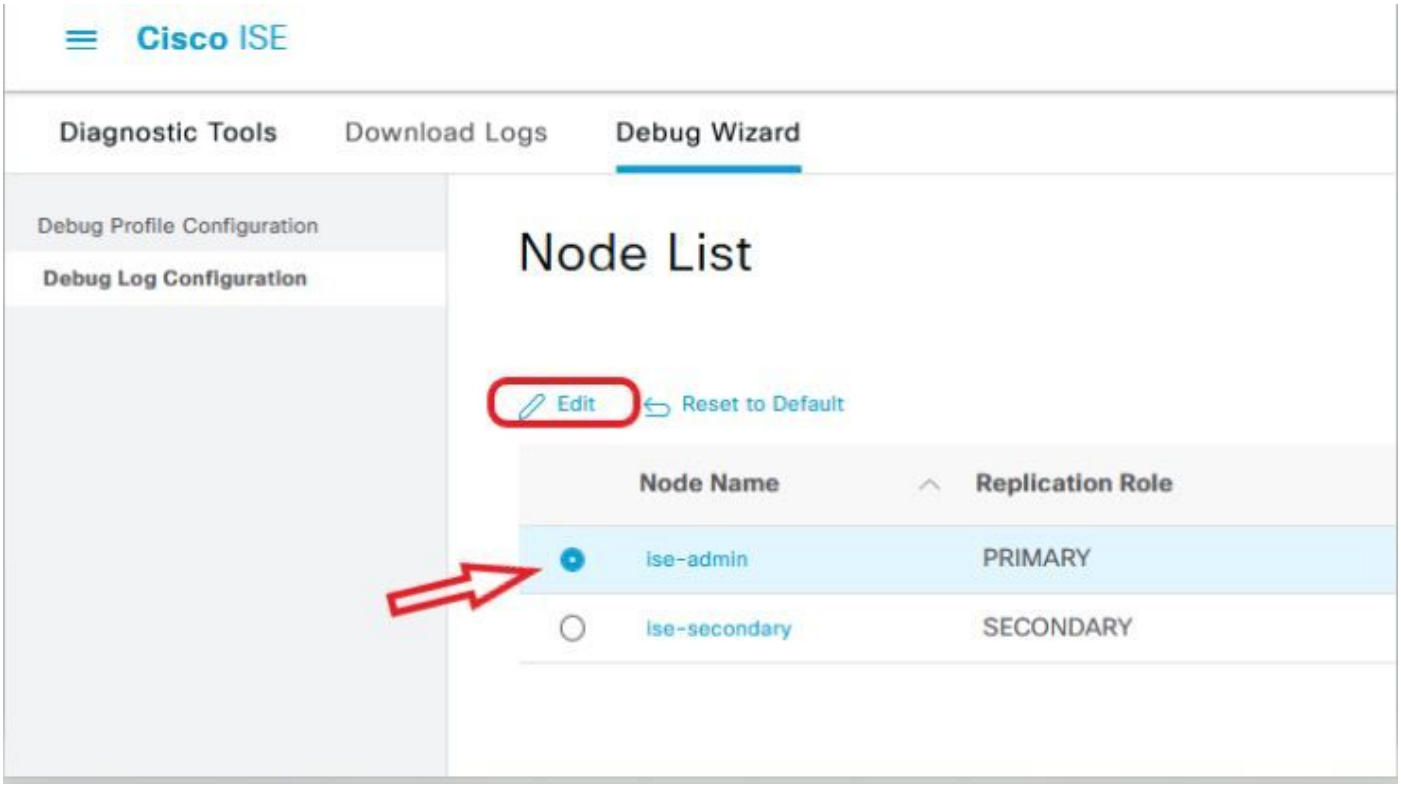
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تمكين تصحيح الأخطاء

لبدء أستكشاف الأخطاء وإصلاحها، يجب أولا تمكين عمليات تصحيح الأخطاء كما هو موضح أدناه.

انتقل إلى **العمليات > أستكشاف الأخطاء وإصلاحها > معالج تصحيح الأخطاء > تكوين سجل الأخطاء**. حدد عقدة الإدارة الأساسية وانقر على تحرير كما هو موضح في الصورة التالية.



- قم بتعيين المكونات التالية على مستوى **تصحيح الأخطاء**.

اسم المكون	مستوى التسجيل	اسم ملف السجل
بوابة	تصحيح الأخطاء	guest.log
أوبن سامل	تصحيح الأخطاء	ise-psc.log
سامل	تصحيح الأخطاء	ise-psc.log

ملاحظة: عند الانتهاء من أستكشاف الأخطاء وإصلاحها، تذكر إعادة تعيين تصحيح الأخطاء عن طريق تحديد العقدة وانقر فوق "إعادة التعيين إلى الافتراضي".

تنزيل السجلات

بمجرد أن يتم نسخ المشكلة، يجب عليك الحصول على ملفات السجل الضرورية.

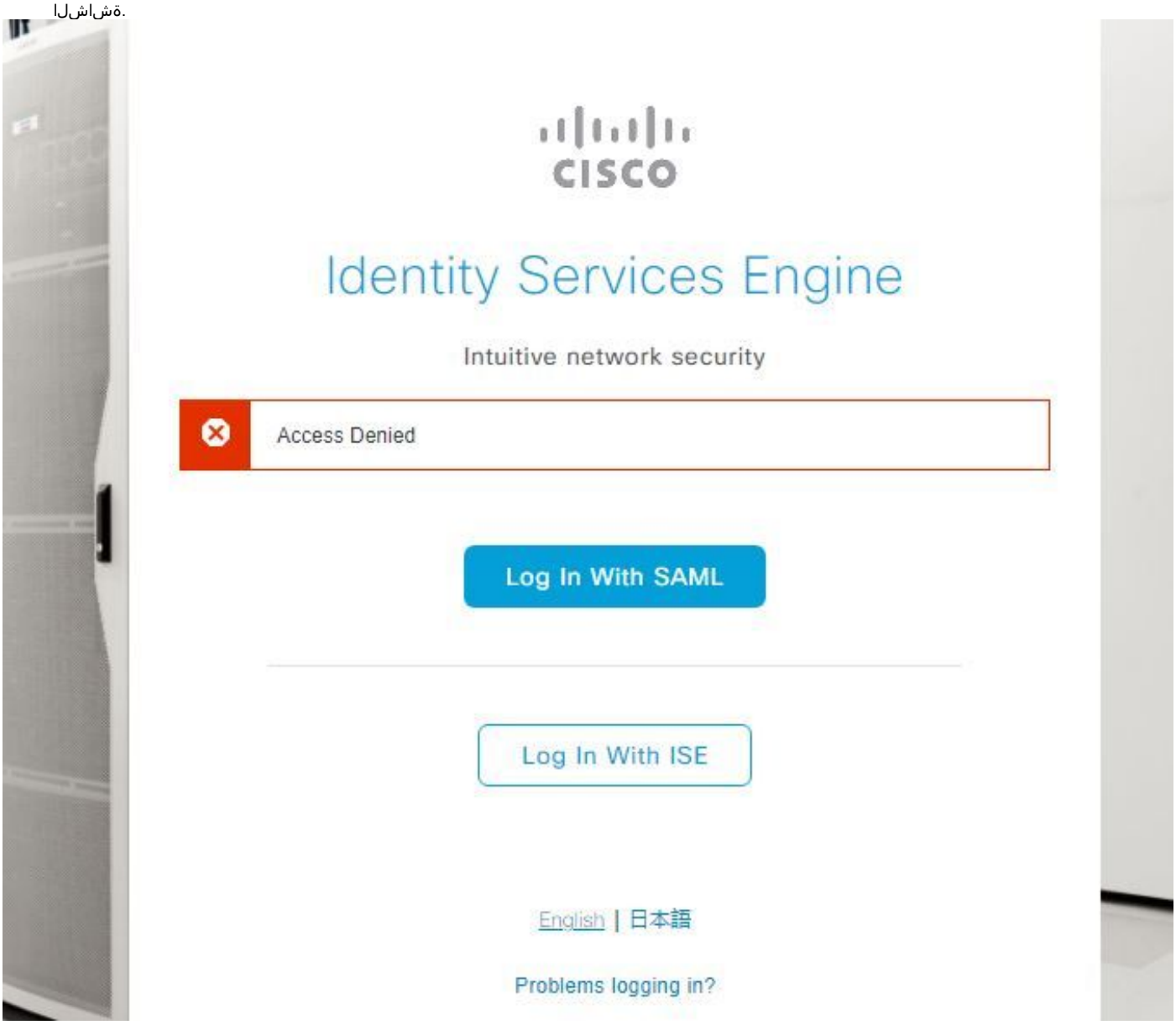
الخطوة 1. انتقل إلى العمليات > أستكشاف الأخطاء وإصلاحها > سجلات التنزيل. حدد عقدة المسؤول الأساسية ضمن 'قائمة عقد الجهاز' > سجلات تصحيح الأخطاء

الخطوة 2. حدد مكان ومدد المجلدات الأصل للضيف و ISE-PSC

الخطوة 3. تنزيل guest.log و ise-psc.log ملفات.

المشكلة 1a: تم رفض الوصول

- بعد تكوين تسجيل دخول المسؤول المستند إلى SAML،
- حدد تسجيل الدخول باستخدام SAML.
- إعادة التوجيه إلى عمل صفحة تسجيل الدخول إلى IdP كما هو متوقع
- تعد المصادقة ناجحة لكل استجابة SAML/IdP
- سمة مجموعة الرسال IDp ويمكن رؤية نفس معرف المجموعة/الكائن المكون في ISE.
- ثم، بينما يحاول ISE تحليل سياساته، فإنه يقوم برمي استثناء يتسبب في ظهور رسالة "رفض الوصول"، كما هو موضح في لقطة الشاشة.



سجل الدخول في ise-psc.log

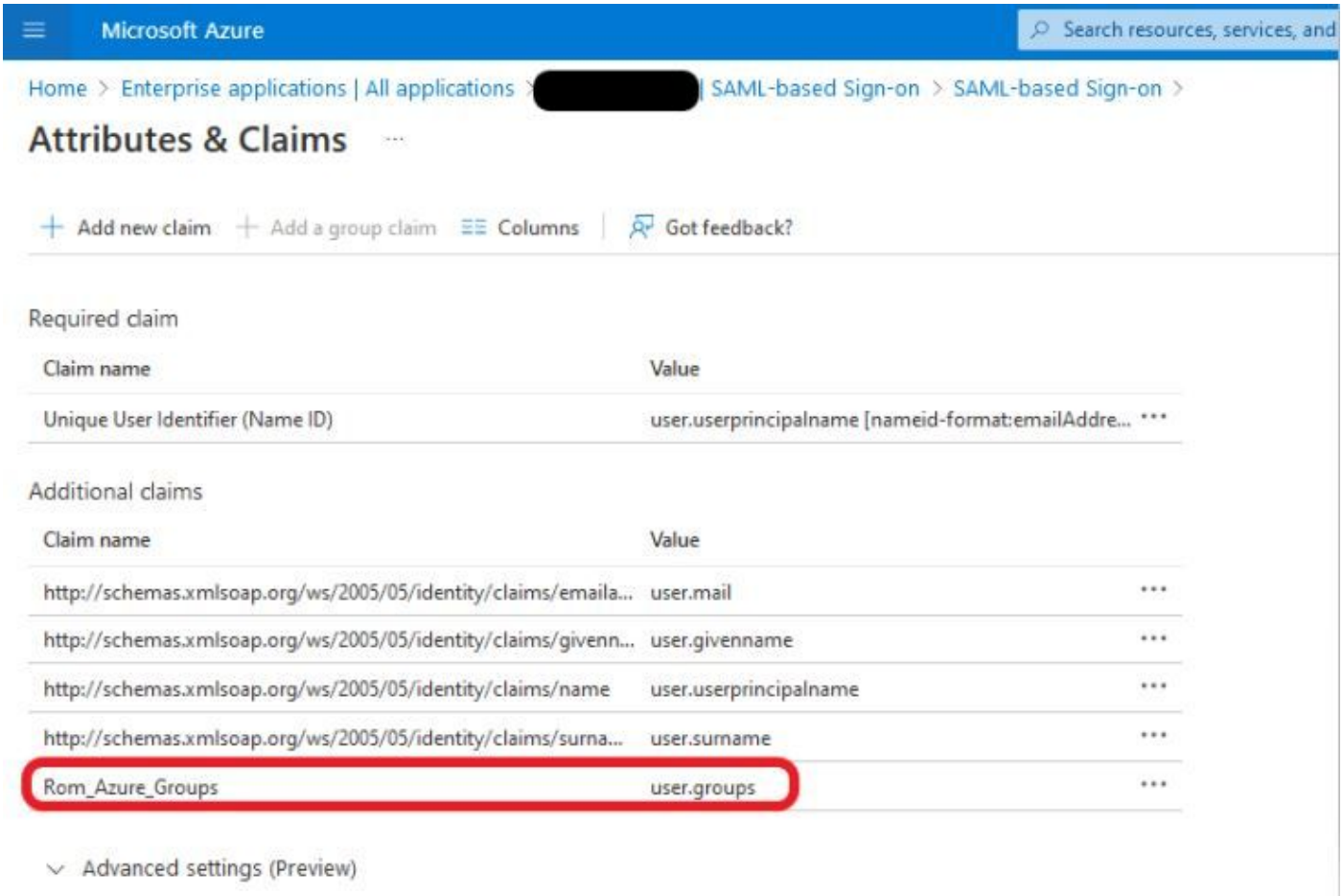
```
2021-09-27 17:16:18,211 DEBUG [https-jsse-nio-10.200.50.44-8443-exec-2][]
cpm.saml.framework.impl.SAMLFacadeImpl -::::- AuthenticatePortalUser - Session:null IDPResponse:
IdP ID: TSDLAB_DAG Subject: ise.test Group: null SAML Status
Code:urn:oasis:names:tc:SAML:2.0:status:Success SAML Success:true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

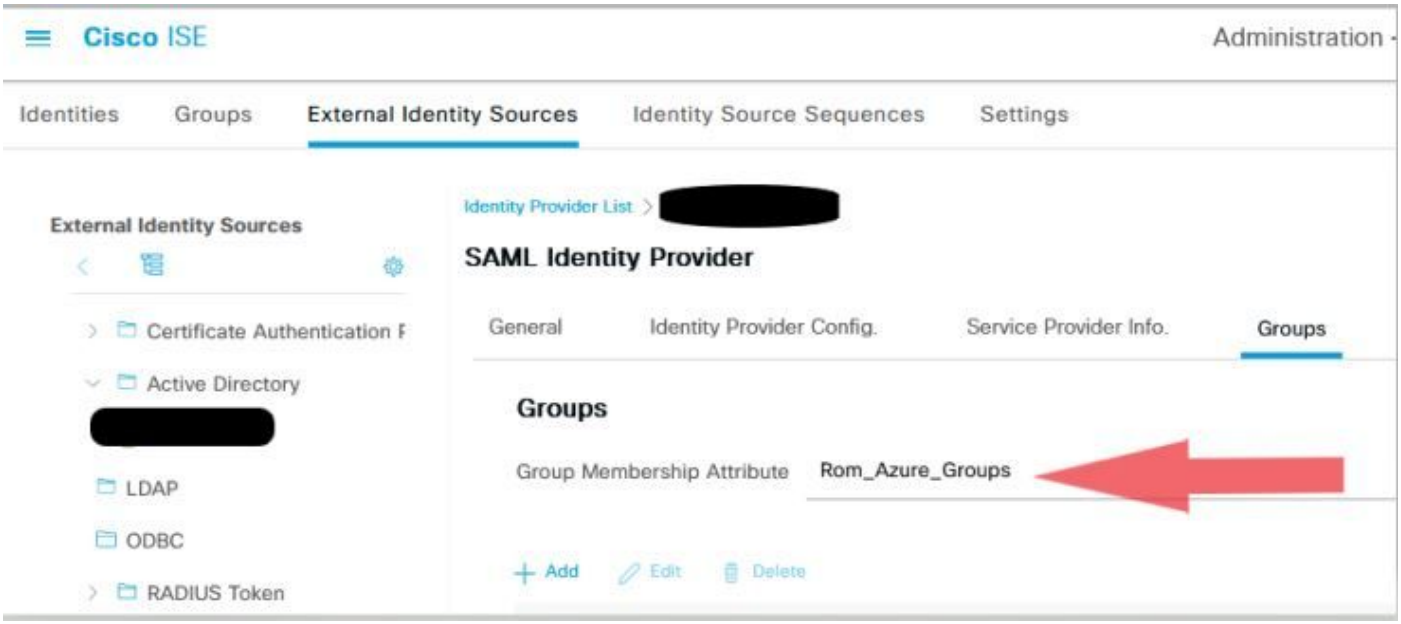
السبب/الحل

تأكد من أن اسم مطالبة المجموعة في تكوينات IdP هو نفسه الذي تم تكوينه في ISE.

تم التقاط لقطة الشاشة التالية من جانب Azure.



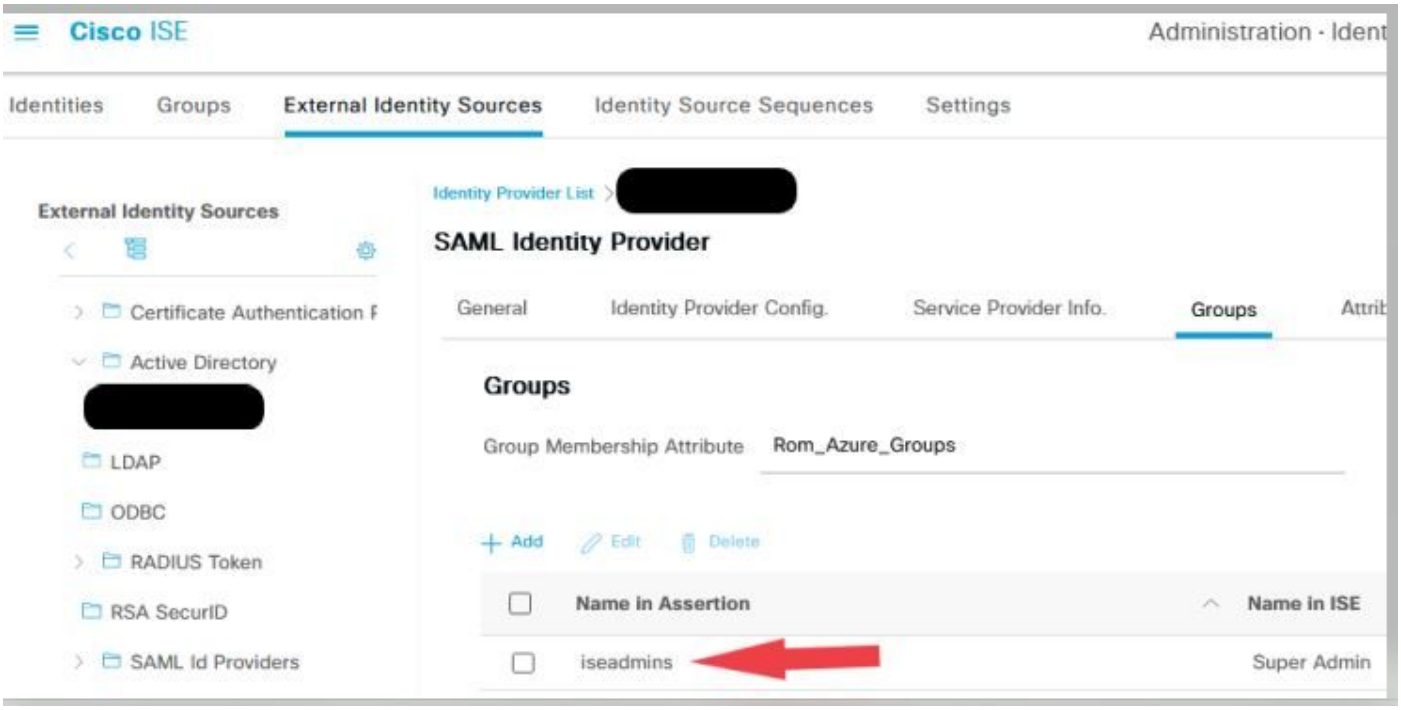
لقطة شاشة من ISE Side.



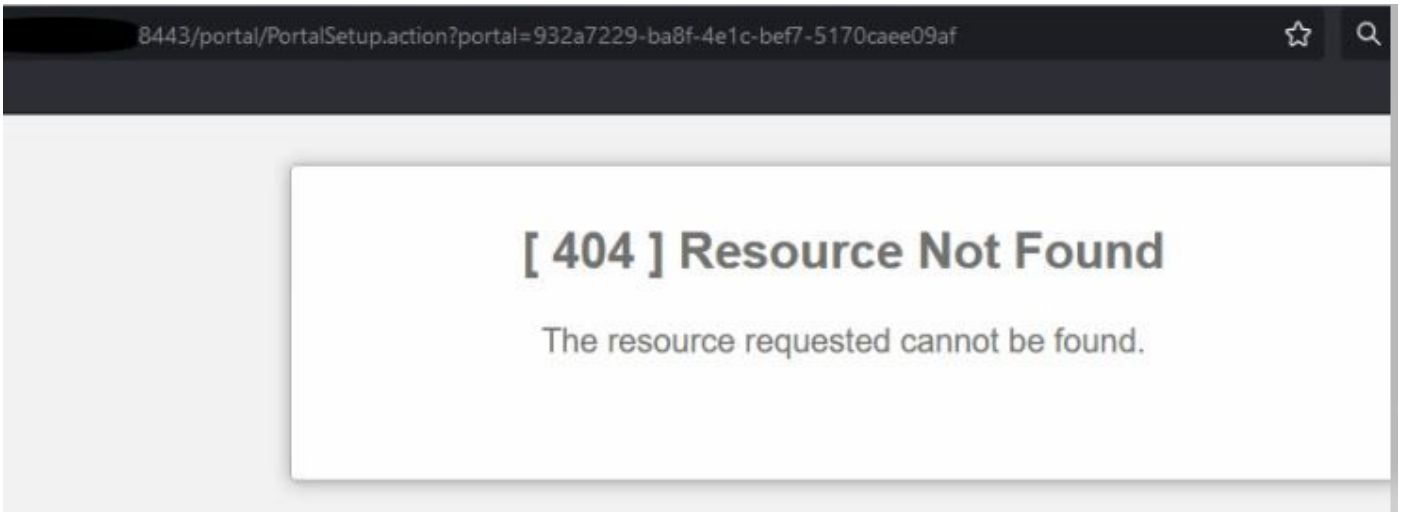
المشكلة 1b: مجموعات متعددة في إستجابة SAML (تم رفض الوصول)

إذا لم يحل الإصلاح السابق المشكلة، فتأكد من أن المستخدم ليس عضوا في أكثر من مجموعة واحدة. إذا كانت هذه هي الحالة، فيجب أن تكون قد واجهت معرف تصحيح الأخطاء من Cisco CSCwa17470 حيث تطابق ISE القيمة الأولى (اسم المجموعة / معرف) فقط في القائمة من إستجابة SAML. تم حل هذا الخطأ في 3.1 P3

وفقا لاستجابة IdP التي تم تقديمها مسبقا، يجب تكوين **تعيين ISE** لمجموعة **iAdmins** حتى يمكن تسجيل الدخول بنجاح.



المشكلة 2: لم يتم العثور على مورد 404



يظهر خطأ في **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.
```

السبب/الحل

تتم ملاحظة هذه المشكلة بعد إنشاء مخزن المعرف الأول فقط.

لحل هذه المشكلة، جرب التالي بنفس الترتيب:

الخطوة 1. قم بإنشاء معرف SAML جديد في ISE (لا تقم بإزالة المعرف الحالي بعد.).

الخطوة 2. انتقل إلى صفحة الوصول إلى المسؤول وقم بتعيين وصول المسؤول إلى IdP الجديد هذا.

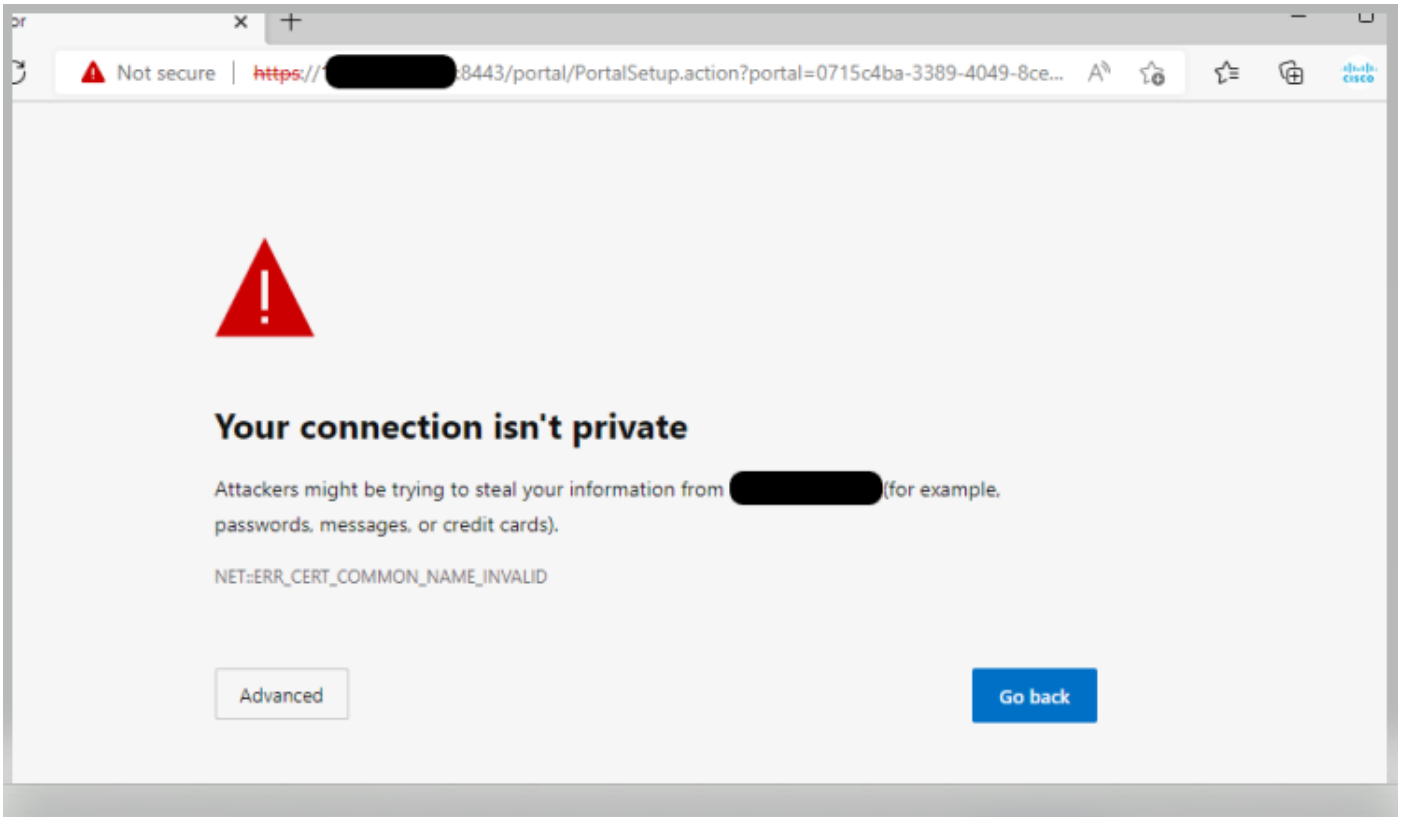
الخطوة 3. احذف المعرف القديم في صفحة موفري الهوية الخارجية.

الخطوة 4. قم باستيراد بيانات تعريف IdP الحالية إلى معرف جديد تم إنشاؤه في الخطوة 1 وقم بإجراء أي تعيينات ضرورية للمجموعة.

الخطوة 5. الآن حاول تسجيل الدخول إلى SAML، وسينجح ذلك.

المشكلة 3: تحذير الشهادة

في النشر متعدد العقد، عندما تنقر على "تسجيل الدخول باستخدام SAML"، يمكنك أن ترى تحذير الشهادة غير الموثوق بها في المستعرض



السبب/الحل

في بعض الحالات، تقوم pPAN بإعادة توجيهك إلى PSNs النشطة IP، وليس FQDN. وهذا يؤدي إلى تحذير الشهادة في بعض نشر PKI، إذا لم يكن هناك عنوان IP في حقل SAN.

ال workaround أن يضيف ip في ال SAN مجال من الترخيص.

معرف تصحيح الأخطاء من Cisco CSCvz89415. تم حل هذه في 3.1p1

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).