ISE و 2way trust ad configuration

المحتويات

المقدمة

يصف هذا المستند تعريف "الثقة المزدوجة الإتجاه" على ISE ومثال تكوين بسيط: كيفية مصادقة مستخدم غير موجود في الإعلان المتصل ب ISE ولكنه موجود في إعلان آخر.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن لديك معرفة أساسية ب :

- دمج ISE 2.x و Active Directory .
- مصادقة الهوية الخارجية على ISE.

المكونات المستخدمة

- ISE 2.x .
- دليلين نشطين.

التكوين

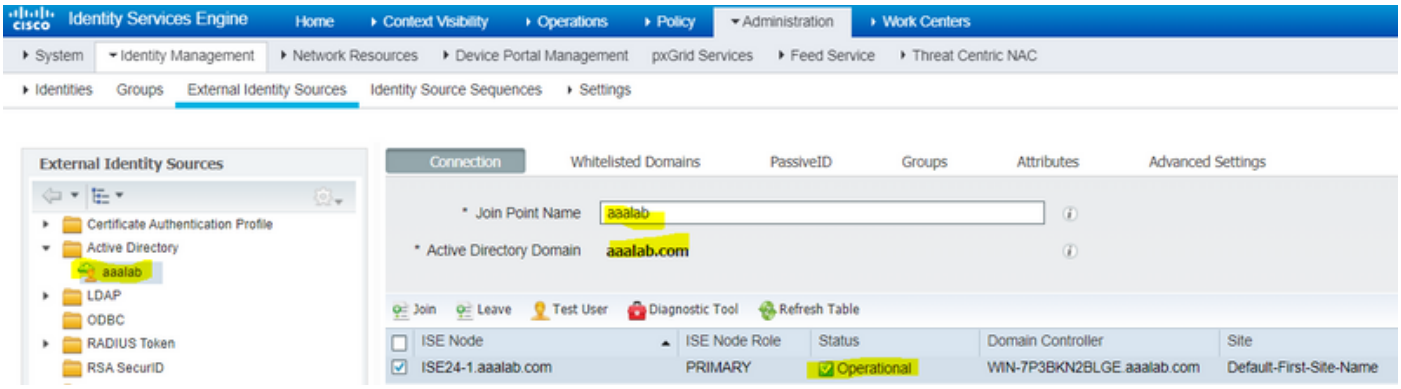
من أجل توسيع مجالك، وتضمين مستخدمين آخرين في مجال مختلف عن المجال الذي تم ضمه بالفعل إلى ISE، لديك طريقتان لتحقيق ذلك :

1. يمكنك إضافة المجال يدويا وبشكل فريد على ISE. عند ذلك، سيكون لديك دليلين نشيطين متفرجين.
2. انضم إلى إعلان ISE واحد، ثم قم بتكوين **الثقة المزدوجة الإتجاه** بين هذا الإعلان والإعلان الثاني، دون إضافته إلى ISE. هذا في الأساس هو تكوين ثقة بطريقتين، وهو خيار يتم تكوينه بين دليلين أو أكثر من الدلائل النشطة. سيقوم ISE تلقائيا باكتشاف هذه المجالات الموثوق بها باستخدام موصل AD وإضافتها إلى "المجالات البيضاء" ومعاملتها كإعلانات منفصلة يتم الانضمام إليها إلى ISE. هذه هي الطريقة التي يمكنك من خلالها مصادقة مستخدم في AD "zatar.jo"، والذي لم يتم انضمامه إلى

ISE.

تصف الخطوات التالية إجراء التكوين على كل من ISE و AD:

الخطوة 1. تأكد من انضمام ISE إلى AD، في هذا المثال، لديك المجال aalab :

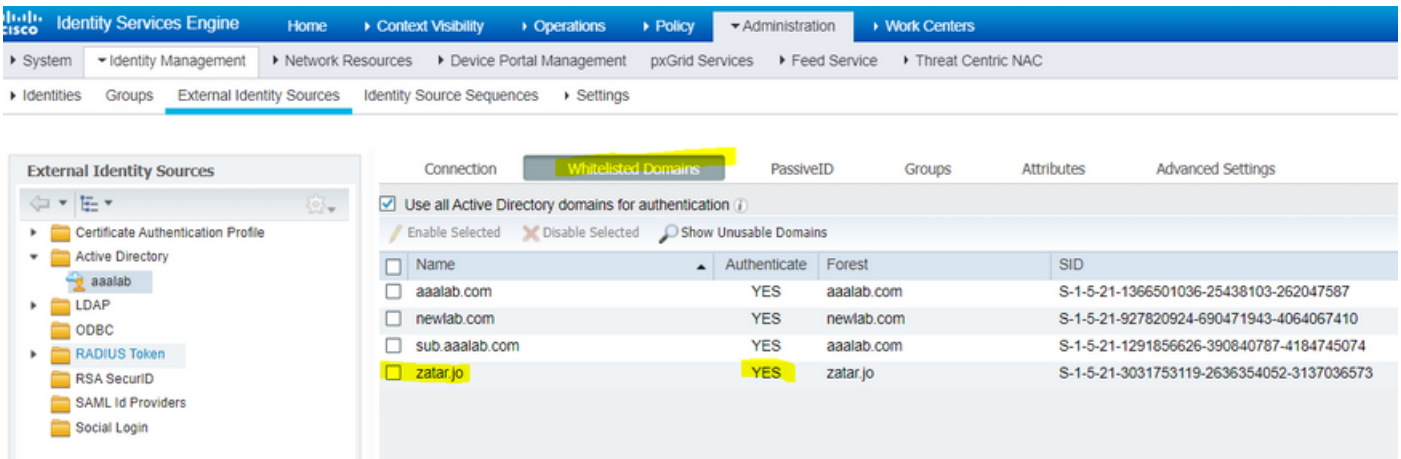


الخطوة 2. تأكد من تمكين الثقة المزدوجة الإتجاه بين كل من الدلائل النشطة، كما هو موضح أدناه :

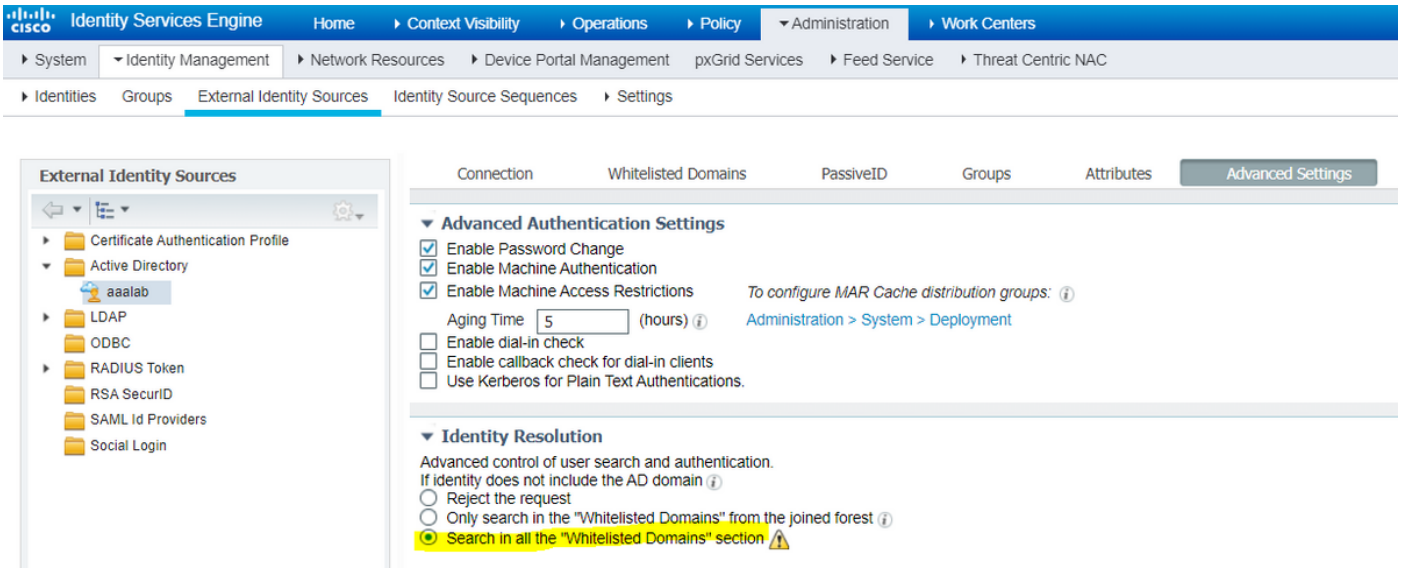
1. افتح مجالات Active Directory وأداة الأمان الإضافية.
2. في الجزء الأيسر، انقر بزر الماوس الأيمن فوق المجال الذي تريد إضافة ثقة له، ثم حدد "خصائص".
3. انقر فوق علامة التبويب Trust.
4. انقر فوق الزر ثقة جديدة.
5. بعد فتح معالج الثقة الجديدة، انقر فوق التالي.
6. اكتب اسم DNS لمجال AD وانقر فوق التالي.
7. بافتراض أن مجال AD قابل للحل عبر DNS، ستسأل الشاشة التالية عن إتجاه الثقة. حدد ثنائي الإتجاه وانقر التالي.
8. لخصائص الثقة الصادرة، حدد كل المورد التي سيتم مصادقتها وانقر فوق التالي.
9. أدخل كلمة مرور الثقة وأعد كتابتها وانقر فوق التالي.
10. طقطقت بعد ذلك مرتين.

ملاحظة: تكوين AD خارج نطاق دعم Cisco، يمكن إشراك دعم Microsoft في حالة حدوث أي مشاكل.

بمجرد تكوين هذا، يمكن لمثال AD (aalab) الاتصال ب AD الجديد (zatar.jo) ويجب أن يظهر في علامة التبويب "المجالات البيضاء"، كما هو موضح أدناه. إذا لم يتم عرضه، فعندئذ يكون تكوين الثقة باتجاهين غير صحيح :



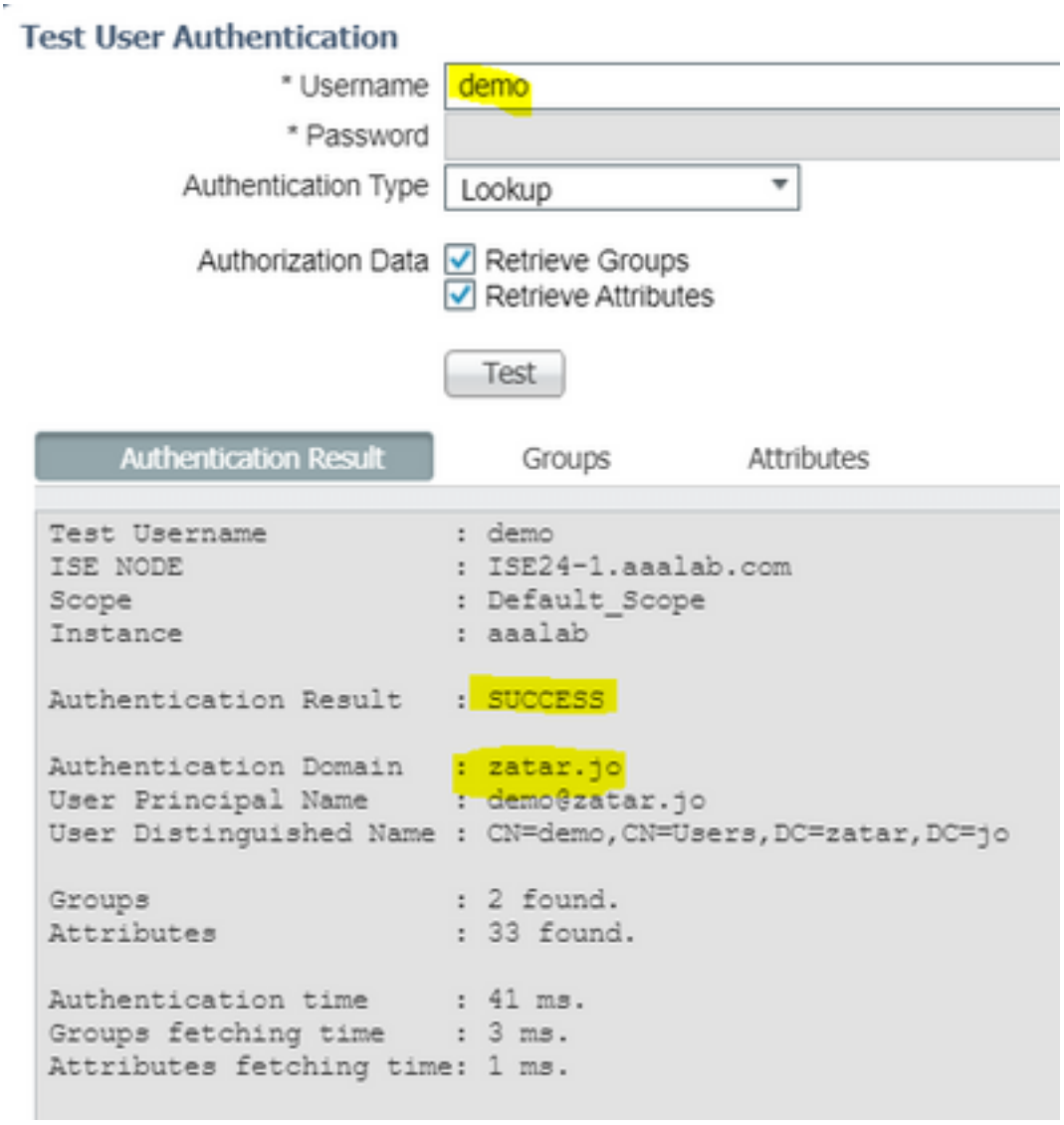
الخطوة 3. تأكد من تمكين **بحث** الخيار **في كل قسم "المجالات البيضاء"**، كما هو موضح أدناه. سيسمح بالبحث في كل المجالات ذات الصلة بما في ذلك المجالات الموثوق بها ذات الاتجاهين. إذا تم تمكين **البحث فقط في "المجالات البيضاء" من الغابة المترابطة**، سيتم البحث فقط في مجالات "التابع" للمجال الرئيسي. { مثال مجال الطفل: sub.aaalab.com في لقطة الشاشة أعلاه }.



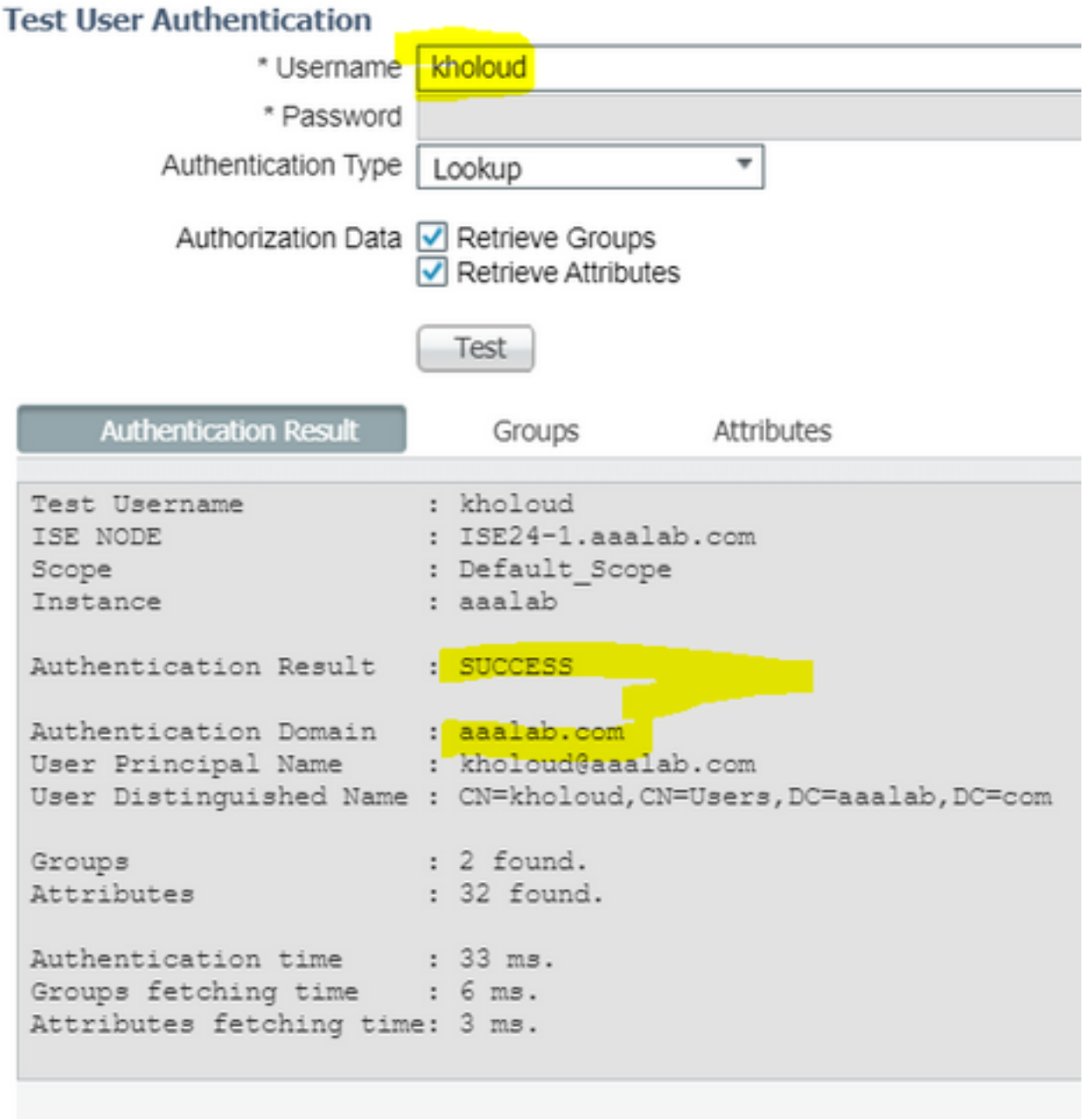
الآن، يمكن أن يقوم ISE بالبحث عن المستخدم في aaalab.com و zatar.com.

التحقق من الصحة

تحقق من أنه يعمل عبر خيار "إختبار المستخدم"، أستخدم المستخدم الموجود في مجال "zatar.jo" (في هذا المثال، المستخدم "demo" موجود فقط في مجال "zatar.jo"، وهو ليس في "aaalab.com"، تكون نتيجة الاختبار أدناه) :



عملا بأن المستخدمين في aaalab.com، يعملون أيضا، مستخدم kholoud في aaalab.com :



استكشاف الأخطاء وإصلاحها

هناك إجراءان رئيسيان لاستكشاف أخطاء معظم وثائق الإعلانات/الثقة المزدوجة الإتجاه وإصلاحها، حتى معظم مصادقات الهوية الخارجية :

1. تجميع سجلات ISE (حزمة الدعم) مع تمكين تصحيح الأخطاء. في مجلدات محددة في مجموعة الدعم هذه، يمكننا العثور على جميع تفاصيل أي محاولة مصادقة على AD.

2. تجميع مجموعات الحزم بين ISE و AD.

الخطوة 1. تجميع سجلات ISE:

أ. قم بتمكين تصحيح الأخطاء وتعيين تصحيح الأخطاء التالية على "تتبع":

- خدمة Active Directory (ad_agent.log)
- Identity-store-AD (ad_agent.log)
- Runtime-AAA (prrt-server.log)

- nsf (ise-psc.log)
- nsf-session (ise-psc.log)

ب. إعادة إنتاج المشكلة، الاتصال بمستخدم إشكالي.

ج. جمع مجموعة دعم.

سيناريو العمل "سجلات":

ملاحظة: سيتم العثور على تفاصيل محاولات المصادقة في الملف ad_agent.log

من ملف ad_agent.log :

التحقق من اتصال الثقة بزارات وثنائي الإتجاه:

```
2020-01-16 12:26:21,210 VERBOSE,140568698918656,LsaDmEnginepDiscoverTrustsForDomain: Adding
trust info zatar.jo (Other Forest, Two way) in forest
zatar.jo,LsaDmEnginepDiscoverTrustsForDomain(),lsass/server/auth-providers/ad-open-
provider/lsadmengine.c:472
2020-01-16 12:26:21,210 DEBUG ,140568698918656,New domain zatar.jo will be added to the trusted
domain list.,LsaDmAddTrustedDomain(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1997
```

البحث عن المستخدم "نسخة تجريبية" في المجال الرئيسي aalab :

```
2020-01-16 12:29:08,579 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
aaalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
```

(الحالة أن المستخدم التجريبي موجود في مجال Zatar، وهو ذلك سيوقع ISE بفحصه في مجال newlab.com. مثل "عاصي" المجالات التوبيخ المجالات أخرى في عالمة التوبيخ المجالات أخرى في مجال Aalab أو الأول، ثم في مجال UPN الحقة استخدام مباشرة، يجب إ Zatar.jo وفحص الرئيسي، المجال في الغش لتجنب لدخول به المستخدم تسجيل بـ يجب أن يوقع المستخدم وبالتالي البحث، مكان الـ ISE عرف حيث بـ التنسيق : demo.zatar.jo).

يتم الآن البحث عن المستخدم "العرض التوضيحي" في zatar.jo.

```
2020-01-16 12:29:08,604 DEBUG ,140568690480896,AdIdentityResolver::search: do
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=demo)) search in forest
zatar.jo,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:738
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpLdapOpen: gc=1,
domain=zatar.jo,LsaDmpLdapOpen(),lsass/server/auth-providers/ad-open-provider/lsadm.c:4102
2020-01-16 12:29:08,604 DEBUG ,140568690480896,LsaDmpIsDomainOffline: checking status of domain
zatar.jo,LsaDmpIsDomainOffline(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3158
```

المستخدم "نسخة تجريبية" موجودة في مجال Zatar :

```
18037: pszResolvedIdentity = "demo@zatar.jo"
Line 18039: pszResolvedDN = "CN=demo,CN=Users,DC=zatar,DC=jo"
Line 18044: pszResolvedSAM = "demo"
Line 18045: pszResolvedExplicitUPN = "demo@zatar.jo"
Line 18056: "1579177748579 24325 "demo" AD-Log-Id=1579177581/40,
```

```
Line 18095: pszBase = "CN=demo,CN=Users,DC=zatar,DC=jo"
```

الخطوة 2. تجميع عمليات المصادقة:

أ. يتم تشفير الحزم المتبادلة بين ISE و AD/LDAP، حتى تكون قابلة للقراءة إذا قمنا بتجميع عمليات المصادقة دون فك تشفيرها أولا.

ISE AD ( ):

1. ISE : " -> Active Directory -> ->
2. ISE .
3. 'Name' : Troubleshooting.EncryptionOffPeriod.
4. ''

< >

:

30

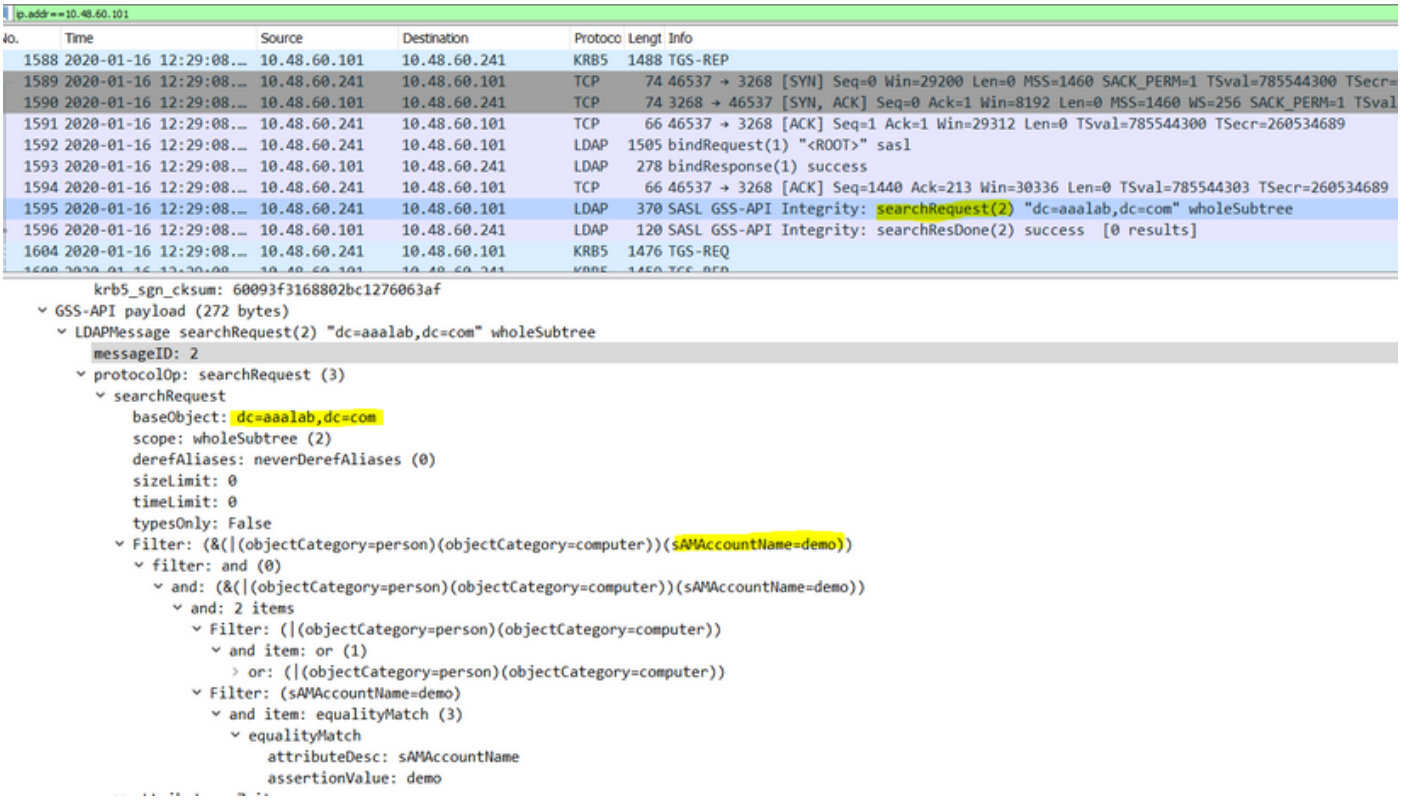
5. . .
6. ' '
7. ' Active Directory.
8. 10 .

ب. بدء المصادقة على ISE.

ج - إستنساخ المسألة.

د. ثم قم بإيقاف المصادقة وتنزيله

<u>سيناريو العمل "السجلات":</u>



التحقق من الصحة

هنا بعض الأمثلة على مواقف العمل ومواقف عدم العمل التي قد تواجهها وعلى السجلات التي تنتجها.

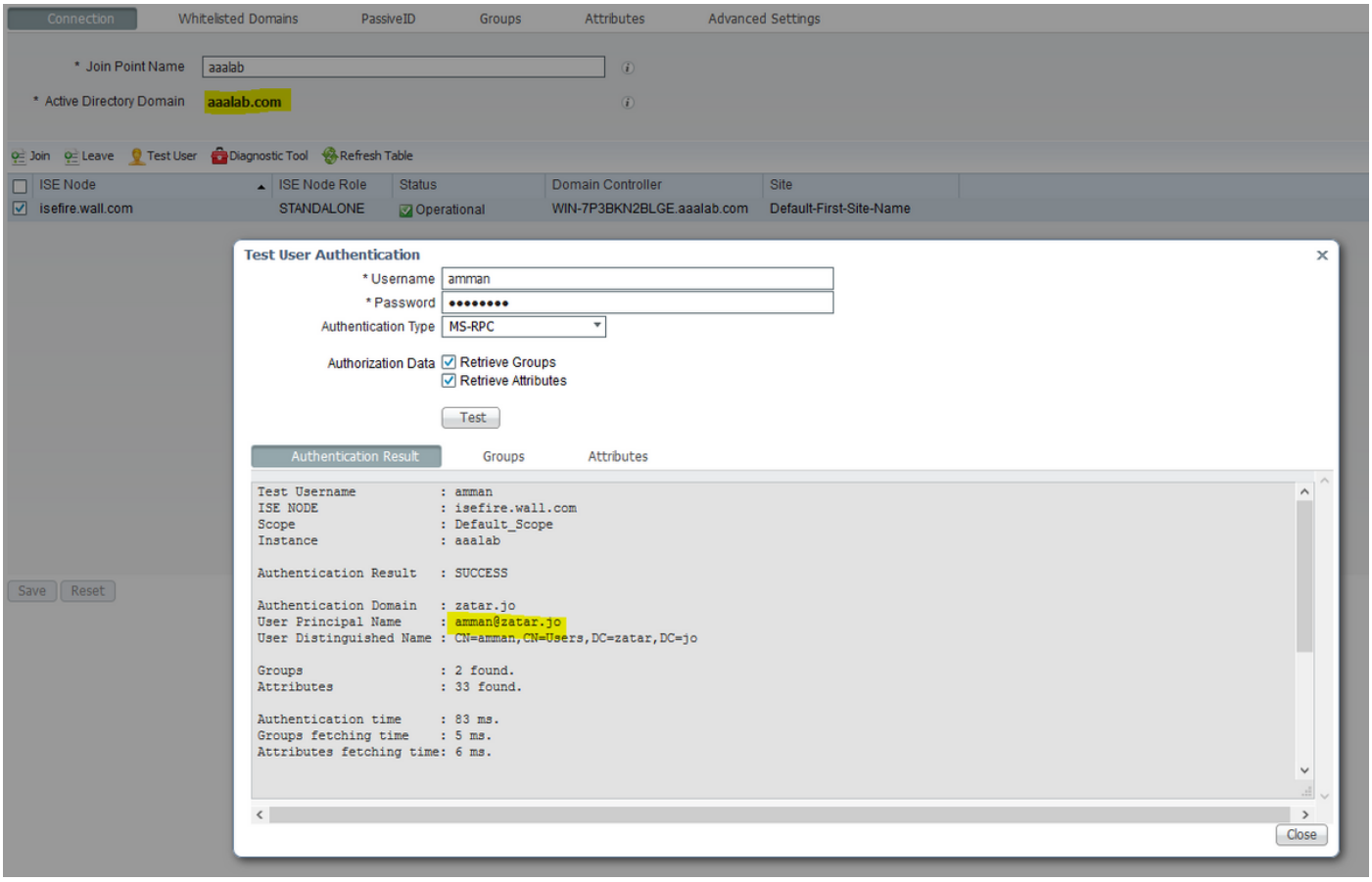
1. المصادقة المستندة إلى مجموعات AD "zatar.jo":

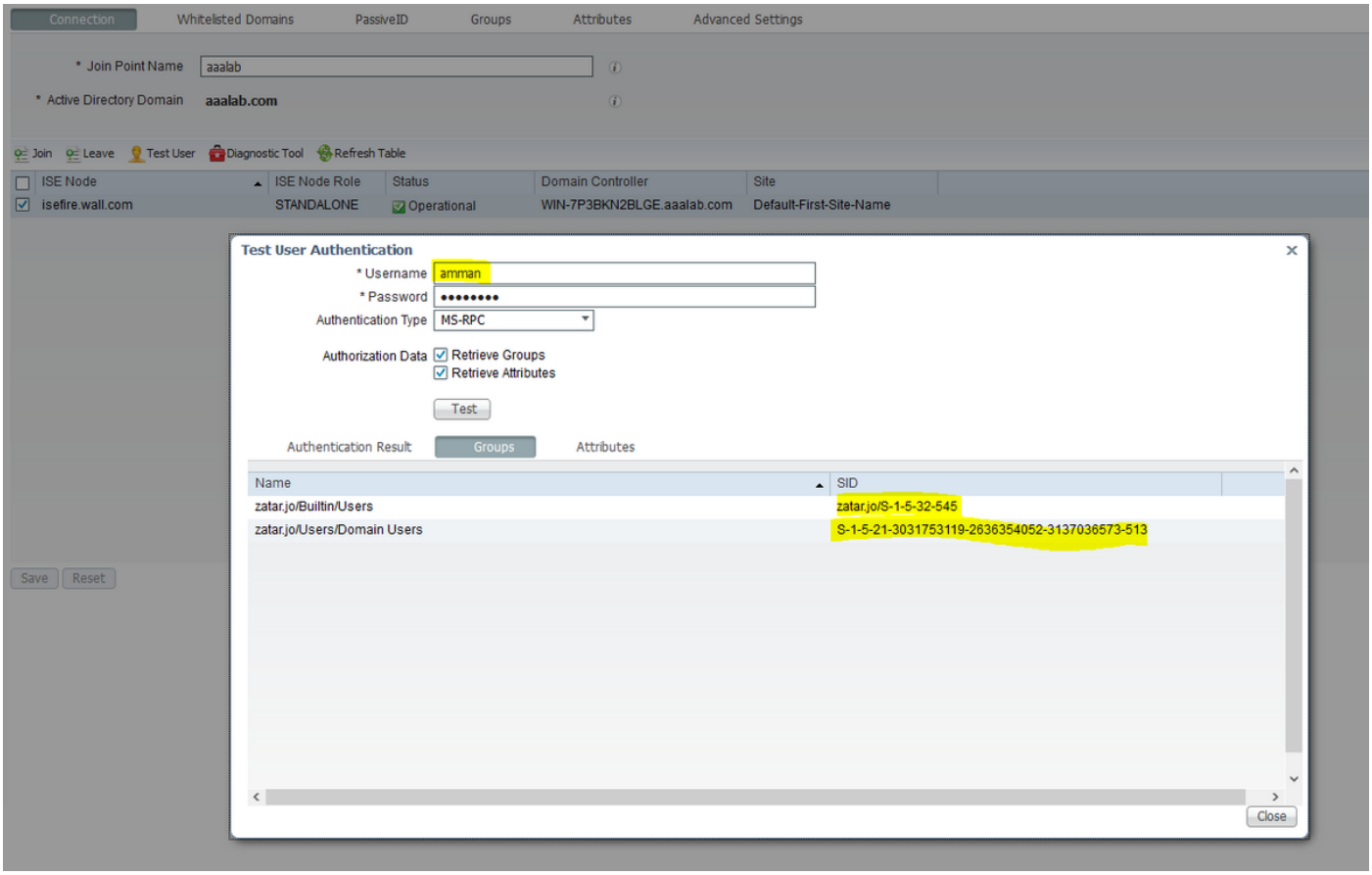
إذا لم يتم إعادة تعيين المجموعة من علامة التبويب المجموعة، فستحصل على رسالة السجلات هذه:

```
2020-01-22 10:41:01,526 DEBUG ,140390418061056,Do not know about domain for object SID 'S-1-5-21-3031753119-2636354052-3137036573-513',LsaDmpMustFindDomainByObjectSid(),lsass/server/auth-providers/ad-open-provider/lsadm.c:1574
```

نحتاج إلى إستيراد المجموعات في zatar.jo من علامة التبويب "مجموعات".

التحقق من إستيراد مجموعة AD من علامة التبويب AD:





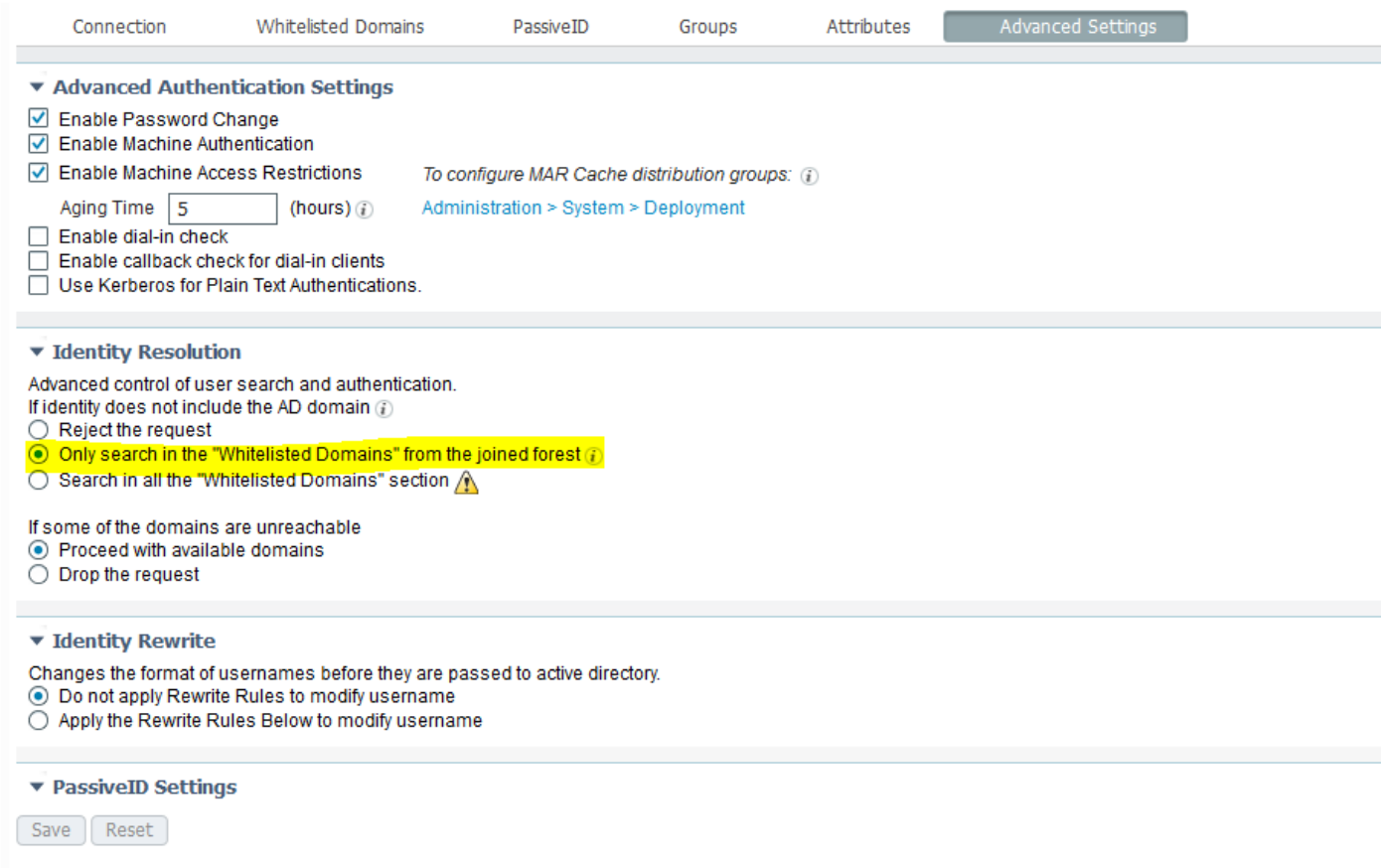
سيناريو العمل من السجلات AD_AGENT.log:

```
2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [zatar.jo/S-1-5-
32-545],AD_GetTokenGroups(),lsass/server/auth-providers/ad-open-provider/provider-main.c:9669
2020-01-22 10:41:01,516 DEBUG ,140390418061056,AD_GetTokenGroups: SID selected: [S-1-5-21-
```

```
3031753119-2636354052-3137036573-513],AD_GetTokenGroups(),lsass/server/auth-providers/ad-open-provider/provider-main.c:9669


pTokenGroupsList =
{
dwStringsCount = 2
ppszStrings =
{
"zatar.jo/S-1-5-32-545"
"S-1-5-21-3031753119-2636354052-3137036573-513"
}
}
```

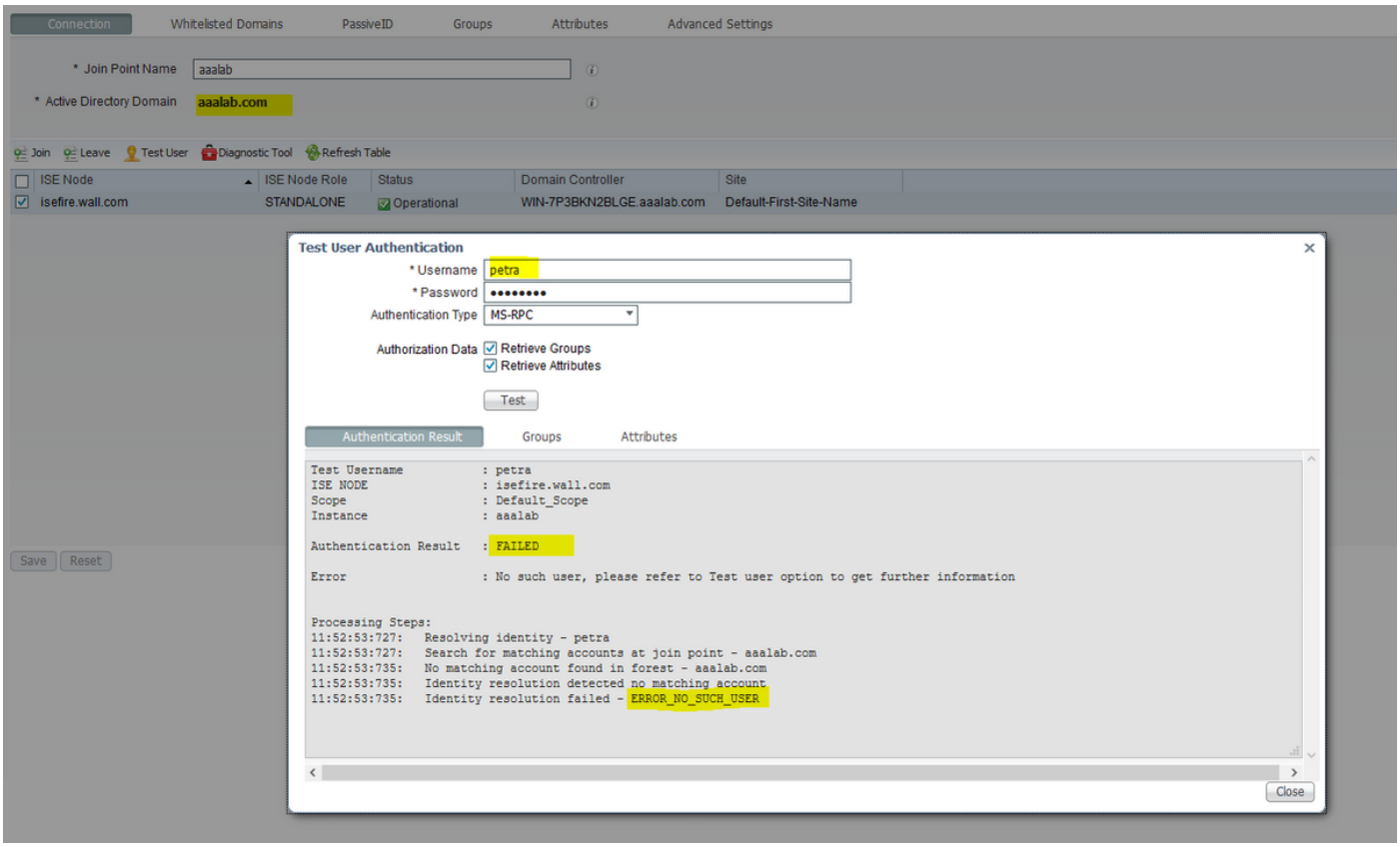
2. إذا تم التحقق من الخيار المتقدم "البحث فقط في "المجالات البيضاء" من الغابة المشتركة":



عندما تختار الخيار "بحث فقط في "المجالات البيضاء" من الغابة المشتركة"، قام ISE بوضع علامة عليها دون اتصال:

```
2020-01-22 13:53:31,000 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain newlab.com,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3423
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain newlab.com is usable and is marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3498
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: examine domain zatar.jo,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3423
2020-01-22 13:53:31,001 DEBUG ,140629434660608,LsaDmpFilterOfflineCallback: domain zatar.jo is not marked offline (DC or GC).,LsaDmpFilterOfflineCallback(),lsass/server/auth-providers/ad-open-provider/lsadm.c:3454
```

المستخدم "Petra" موجود في موقع Zatar.jo وسيفشل في المصادقة، كما هو موضح أدناه:



في السجلات:

لم يتمكن ISE من الوصول إلى مجالات أخرى، بسبب الخيار المتقدم "البحث فقط في "المجالات البيضاء" من الغابة المرتبطة":

```
2020-01-22 13:52:53,735 DEBUG ,140629511296768,AdIdentityResolver::search: already did
(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=petra)) search in forest
aaalab.com,searchIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:735
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains:
newlab.com,examineDomains(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::examineDomains:
zatar.jo,examineDomains(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:601
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AdIdentityResolver::finalizeResult: result:
40008 (symbol: LW_ERROR_NO_SUCH_USER),finalizeResult(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver_impl.cpp:491
2020-01-22 13:52:53,735 VERBOSE,140629511296768,AD_ResolveIdentity: identity=[petra], flags=0,
dwError=40008,AD_ResolveIdentity(),lsass/server/auth-providers/ad-open-
provider/ad_identity_resolver.cpp:131
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra],
flags=0, dwError=40008,LsaSrvResolveIdentity(),lsass/server/api/api2.c:2877
2020-01-22 13:52:53,735 VERBOSE,140629511296768,Error code: 40008 (symbol:
LW_ERROR_NO_SUCH_USER),LsaSrvResolveIdentity(),lsass/server/api/api2.c:2890
2020-01-22 13:52:53,735 VERBOSE,140629511296768,LsaSrvResolveIdentity: identity=[petra],
flags=0, dwError=40008, resolved identity list returned =
NO,LsaSrvIpcResolveIdentity(),lsass/server/api/ipc_dispatch.c:2738
```

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).