فهم Identity Service Engine (ISE) و Active Directory (AD)

المحتويات

المقدمة

يوضح هذا المستند كيفية اتصال Identity Service Engine (ISE) و Active Directory (AD)، والبروتوكولات المستخدمة، وعوامل تصفية AD، والتدفقات.

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة أساسية بـ :

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

المكونات المستخدمة

- ISE 2.x .
- خادم Windows (Active Directory) .

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.

بروتوكولات AD

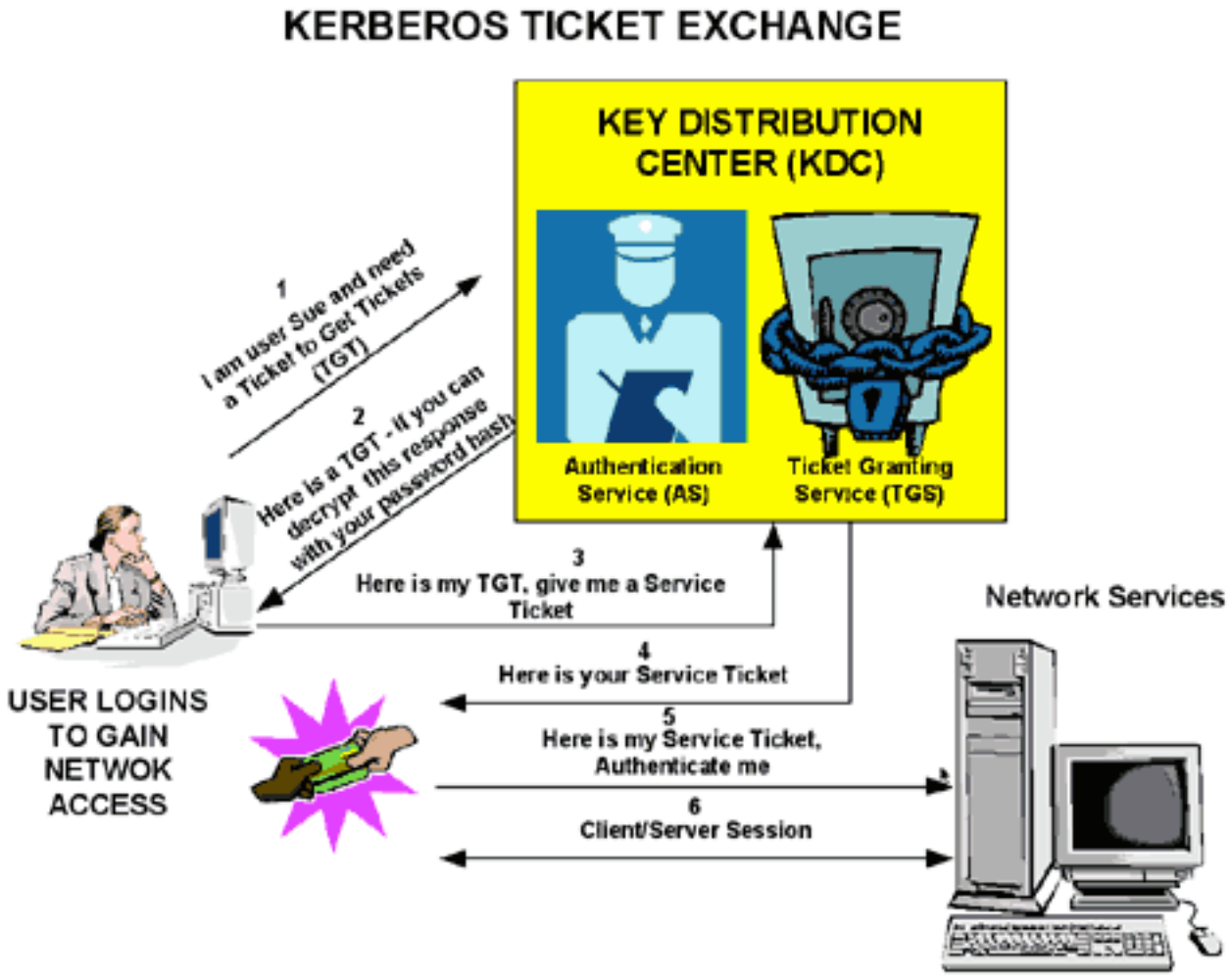
بروتوكول Kerberos

تتألف رؤوس Kerberos الثلاثة من مركز توزيع المفاتيح (KDC) ومستخدم العميل والخادم الذي يجب الوصول إليه.

يتم تثبيت KDC كجزء من وحدة التحكم بالمجال (DC) وتؤدي وظيفتين للخدمات: خدمة المصادقة (AS) وخدمة منح التذاكر (TGS).

يتم تضمين ثلاث عمليات تبادل عندما يقوم العميل بالوصول في البداية إلى مورد خادم:

1. كبديل.
2. تبادل TGS.
3. تبادل العميل/الخادم (CS).



- وحدة التحكم بالمجال = KDC (AS + TGS).
- مصادقة إلى AS (مدخل SSO) باستخدام كلمة المرور الخاصة بك.
- الحصول على تذكرة منح (TGT) (ملف تعريف إرتباط جلسة).
- طلب تسجيل الدخول إلى خدمة (SRV01).
- يقوم SRV01 بإعادة توجيهك إلى KDC.
- إظهار TGT إلى KDC - (أنا مصدق عليه بالفعل)
- تقدم لك شركة KDC TGS ل SRV01.

- قم بإعادة التوجيه إلى SRV01.
- إظهار تذكرة الخدمة إلى SRV01.
- يقوم SRV01 بالتحقق من تذكرة الخدمة أو الوثوق بها.
- بطاقة الخدمة تحتوي على جميع المعلومات الخاصة بي.
- يقوم SRV01 بتسجيل دخولي.

عند تسجيل الدخول في البداية إلى شبكة، يجب على المستخدمين التفاوض بشأن الوصول وتوفير اسم تسجيل الدخول وكلمة المرور للتحقق منه بواسطة جزء AS من KDC داخل مجالهم.

لدى KDC إمكانية الوصول إلى معلومات حساب مستخدم Active Directory. وبمجرد مصادقته، يتم منح المستخدم تذكرة منح (TGT) صالحة للمجال المحلي.

يبلغ عمر TGT الافتراضي 10 ساعات ويتم تجديده خلال جلسة عمل تسجيل دخول المستخدم بدون الحاجة إلى إعادة إدخال كلمة المرور الخاصة به.

يتم تخزين TGT مؤقتا على الجهاز المحلي في مساحة ذاكرة متطايرة ويتم إستخدامه لطلب جلسات العمل مع الخدمات عبر الشبكة.

يقدم المستخدم TGT إلى جزء TGS من KDC عند الحاجة إلى الوصول إلى خدمة الخادم.

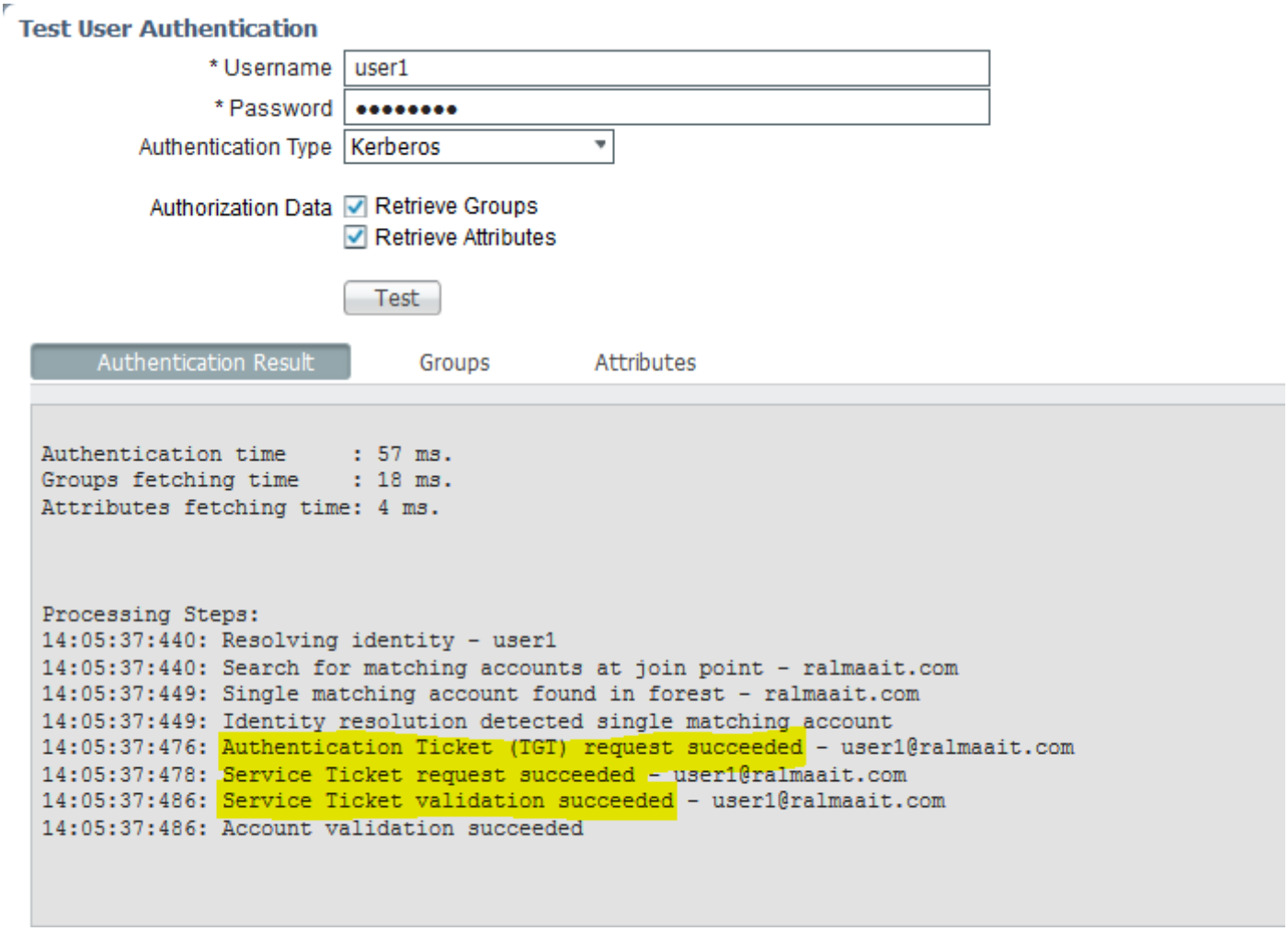
يقوم TGS الموجود على KDC بمصادقة TGT للمستخدم وإنشاء تذكرة ومفتاح جلسة عمل لكل من العميل والخادم البعيد. يتم بعد ذلك تخزين هذه المعلومات (بطاقة الخدمة) مؤقتا محليا على جهاز العميل.

يتلقى TGS العميل TGT ويقرأه بمفتاحه الخاص. إذا وافق TGS على طلب العميل، يتم إنشاء تذكرة خدمة لكل من العميل والخادم الهدف.

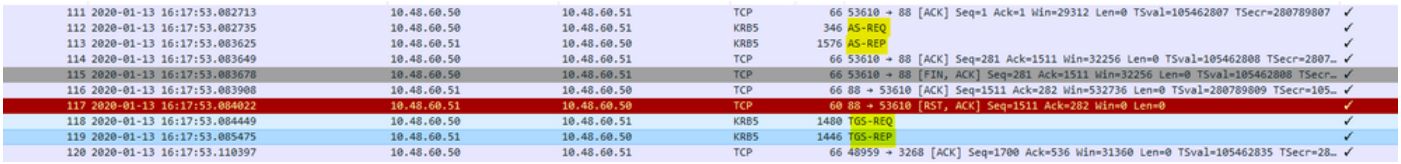
يقرأ العميل نصيبه مع مفتاح جلسة TGS الذي تم إسترداده مسبقا من رد AS.

يقوم العميل بتقديم جزء الخادم الخاص برد TGS على الخادم الهدف في عملية تبادل العميل/الخادم التالية.

مثال:



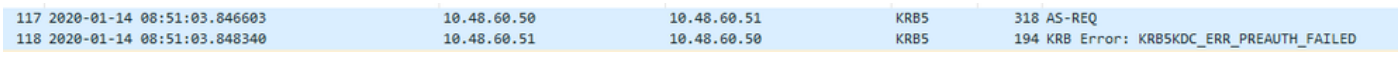
التقاط الحزمة من ISE لمستخدم تتم مصادقته:



تحتوي AS-REQ على اسم المستخدم. إذا كانت كلمة المرور صحيحة، فإن خدمة AS توفر TGT مشفرا باستخدام كلمة مرور المستخدم. وبعد ذلك يتم توفير TGT لخدمة TGT للحصول على تذكرة جلسة عمل.

تكون المصادقة ناجحة عند إستلام تذكرة جلسة عمل..

هذا مثال حيث كلمة المرور المقدمة من العميل خاطئة:



إذا كانت كلمة المرور غير صحيحة، يفشل طلب AS ولا يتم تلقي TGT:

```
Processing Steps:
13:19:55:837:   Resolving Identity - User1
13:19:55:837:   Search For Matching Accounts At Join Point - Ralmaait.com
13:19:55:843:   Single Matching Account Found In Forest - Ralmaait.com
13:19:55:843:   Identity Resolution Detected Single Matching Account
13:19:55:856:   Authentication Ticket (TGT) Request Failed - User1@ralmaait.com,ERROR_PASSWORD_MISMATCH
```

قم بتسجيل الدخول إلى ملف ad_agent.log عندما تكون كلمة المرور غير صحيحة:

2020-01-14 13:36:05،442 تصحيح الأخطاء، 140574072981248،krb5: طلب مرسل (276 بايت) إلى RALMAAIT.COM،LwKrb5TraceCallback()،lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05،444 DEBUG، 140574072981248،krb5: تم تلقي خطأ من KDC: -1765328360/Preauthentication failed، LwKrb5TraceCallback()،lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05،444 تصحيح الأخطاء، 140574072981248،krb5: أنواع إدخالات إعادة المحاولة السابقة: 16، 14، 19، 2،LwKrb5TraceCallback()،lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05،444 تحذير، 140574072981248،[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] رمز الخطأ KRB5: -1765328360 (رسالة: فشل المصادقة المسبقة)، LwTranslateKrb5Error()،lwadvapi/threaded/lwkrb5.c:892

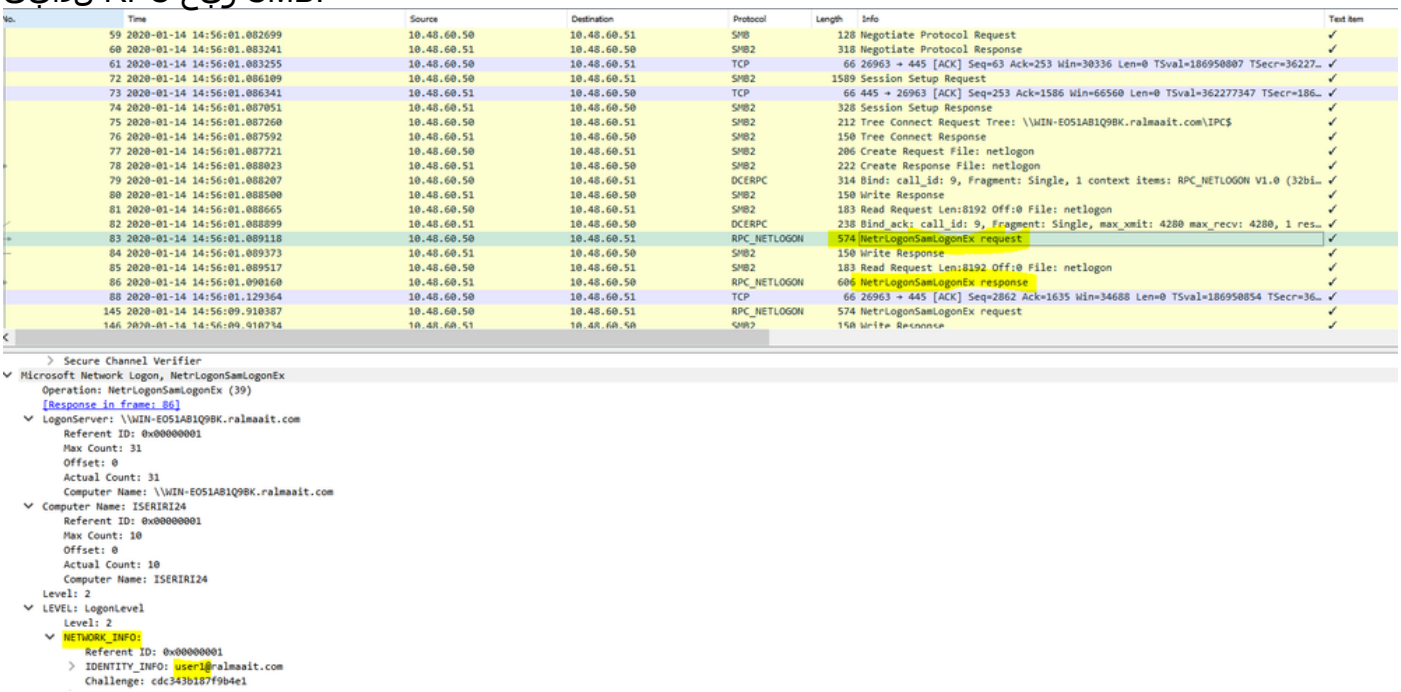
2020-01-14 13:36:05،444 تصحيح الأخطاء، 140574072981248،[LwKrb5InitializeUserLoginCredentials()] رمز الخطأ: 40022 (الرمز: LW_ERROR_PASSWORD_MISMATCH)،LwKrb5InitializeUserLoginCredentials()،lwadvapi/threaded/lwkrb5.c:1453

بروتوكول MS-RPC

يستخدم ISE MS-RPC عبر SMB، وتوفر SMB المصادقة والا تتطلب جلسة منفصلة للعثور على موقع خدمة RPC معينة. وهو يستخدم آلية تسمى "ممر البيانات المسمى" للاتصال بين العميل والخادم.

- إنشاء اتصال جلسة عمل SMB.
- نقل رسائل RPC عبر SMB/CIFS.TCP منفذ 445 كنقل
- تحدد جلسة عمل SMB المنفذ الذي تقوم خدمة RPC معينة بتشغيله وتعالج مصادقة المستخدم.
- الاتصال ب IPC$ للمشاركة المخفية للاتصال بين العمليات.
- فتح ممر بيانات مسمى مناسب لمورد/وظيفة RPC المطلوبة.

تبادل RPC عبر SMB.



يعرض الأمر **negotiate protocol request/response** تفاوض السطر على لهجة الشركات الصغيرة والمتوسطة. يعرض الأمر **session setup request/response** يجري المصادقة.

اتصال طلب اتصال الشجرة والاستجابة بالمورد المطلوب. أنت متصل بمشاركة خاصة IPC$.

وتوفر هذه المشاركة في الاتصال بين العمليات وسائل الاتصال بين الأجهزة المضيفة MSRPC. وكذلك كوسيلة نقل لوظائف

في الحزمة 77 وهو **Create Request File** واسم الملف وهو اسم الخدمة المتصلة (خدمة Netlogon في هذا المثال).

في الحزم 83 و86، يكون طلب NetrlogonSamLogonEX وهو المكان الذي تقوم فيه بإرسال اسم المستخدم لمصادقة العميل على ISE إلى AD في الحقل network_info.

تقوم حزمة إستجابة NetrlogonSamLogonEX بالرد مع النتائج.

بعض قيم العلامات لاستجابة NetrlogonSamLogonEX:
0xc00006a status_wrong_password
0x000000 وهو status_success
0x0000103 وهو status_pending

دمج ISE مع خدمة Active Directory (AD)

يستخدم ISE بروتوكول LDAP و KRB و MSRBC للاتصال بالإعلان أثناء عملية الانضمام/المغادرة والمصادقة.

توفر الأقسام التالية البروتوكولات وتنسيق البحث والآليات المستخدمة للاتصال بـ DC هذا. مقابل DC ومصادقة المستخدم في AD في حدد

وفي حالة عدم اتصال وحدة التحكم بالمجال (DC) لأي سبب من الأسباب، يفشل ISE في الوصول إلى وحدة التحكم بالمجال (DC) التالية المتاحة والتي تأثر عملية المصادقة.

خادم الكتالوج العمومي (GC) هو وحدة تحكم بالمجال تقوم بتخزين نسخ من كافة كائنات Active Directory في الغابة.

وهو يخزن نسخة كاملة من كل الكائنات في دليل مجال ونسخة جزئية من كل الكائنات من كل مجالات الغابات الأخرى.

وبالتالي، يتيح الكتالوج العمومي للمستخدمين والتطبيقات العثور على كائنات في أي مجال من مجالات الغابة الحالية مع البحث عن سمات مضمنة في GC.

يحتوي الكتالوج العمومي على مجموعة أساسية (غير كاملة) من السمات لكل كائن غابة في كل مجال (مجموعة سمات جزئية، PAT).

يتلقى GC بيانات من كل أقسام دليل المجال في الغابة. يتم نسخها باستخدام الخدمة القياسية للنسخ المتماثل باستخدام AD.

انضمام ISE إلى AD

المتطلبات الأساسية لتكامل Active Directory و ISE

1. تحقق أنت من أن لديك امتيازات مسؤول مجال أو مسؤول المجال في ISE.
2. استخدم إعدادات خادم بروتوكول وقت الشبكة (NTP) لمزامنة الوقت بين خادم Cisco ISE و Active Directory. الحد الأقصى للفرق في الوقت المسموح به بين ISE و AD هو 5 دقائق
3. يجب أن يكون DNS الذي تم تكوينه على ISE قادرا على الرد على استعلامات SRV الخاصة ب DCs و GCs و KDCs مع معلومات الموقع الإضافية أو بدونها.
4. تأكد من أن خوادم DNS يمكنها الرد على استعلامات DNS الأمامية والعكسية لأي مجال DNS محتمل ل Active Directory.
5. يجب أن يكون ل AD خادم كتالوج عمومي واحد على الأقل قيد التشغيل ويمكن الوصول إليه بواسطة Cisco، في المجال الذي تنضم إليه Cisco.

الانضمام إلى مجال AD

يطبق ISE اكتشاف المجال للحصول على معلومات حول المجال الانضمام في ثلاث مراحل:

1. تم استعلام المجالات المنضم إليها—اكتشاف المجالات من غاباتها والمجالات الموثوق بها خارجيا للمجال المنضم.
2. يستعلم عن المجالات الجذرية في غاباته - يؤسس الثقة مع الغابة.
3. استعلامات المجالات الجذرية في الغابات الموثوق بها—يكتشف المجالات من الغابات الموثوق بها.

وبالإضافة إلى ذلك، يكتشف Cisco ISE أسماء مجالات DNS (لاحقات UPN)، ولاحقات UPN البديلة، وأسماء مجال NTLM.

يطبق موقع ISE اكتشاف DC للحصول على جميع المعلومات حول وحدات DC و GCs المتوفرة.

1. تبدأ عملية الانضمام ببيانات اعتماد الإدخال الخاصة بالمسؤول المتميز على AD الموجودة في المجال نفسه. إذا كان موجودا في مجال أو مجال فرعي مختلف، فيجب الملاحظة في اسم المستخدم في تدوين UPN (username@domain).
2. يرسل موقع ISE استعلام DNS لجميع سجلات DCs و GCs و KDCs. إذا لم يحتوي رد DNS على أي واحد منها في إجابته، فيفشل التكامل مع خطأ المرتبط DNS.
3. يستخدم ISE إختبار اتصال CLDAP لاكتشاف جميع DCs و GCs من خلال طلبات CLDAP المرسلة إلى DCs والتي تتوافق مع أولوياتها في سجل SRV. يتم إستخدام إستجابة وحدة التحكم بالمجال (DC) الأولى ومن ثم يتم توصيل ISE بهذه وحدة التحكم بالمجال DC.

أحد العوامل المستخدمة لحساب أولوية التيار المباشر هو الوقت الذي يستغرقه التيار المباشر للاستجابة لاجتماعات CLDAP؛ فالاستجابة الأسرع تحظى بأولوية أعلى.

> **ملاحظة:** CLDAP هي الآلية التي يستخدمها ISE لإنشاء اتصال مع وحدات التحكم بالمجال DC والحفاظ عليه. يقيس وقت الاستجابة حتى أول رد ل DC. لم يفشل إذا لم تجد إجابة من التيار المستمر. حذر إذا كان وقت الاستجابة أكبر من 2.5 ثانية. يتم مسح كافة وحدات التحكم بالمجال DC في الموقع (في حالة عدم وجود موقع، فإنه يتم مسح كافة وحدات التحكم بالمجال DC في المجال). تحتوي إستجابة CLDAP على موقع DC وموقع العميل (الموقع الذي تم تعيين جهاز ISE إليه).

4. ثم يستقبل ISE TGT مع بيانات اعتماد "الانضمام إلى المستخدم".
5. قم بإنشاء اسم حساب جهاز ISE باستخدام MSRPC. (SAM و SPN)
6. بحث AD بواسطة SPN إذا كان حساب جهاز ISE موجودا بالفعل. إذا لم يكن جهاز ISE موجودا، يقوم ISE بإنشاء جهاز جديد.
7. فتح حساب الجهاز، وتعيين كلمة مرور حساب جهاز ISE، والتحقق من إمكانية الوصول إلى حساب جهاز ISE.
8. قم بتعيين سمات حساب جهاز ISE (SPN و dnsHostname وما شابه).
9. احصل على TGT باستخدام بيانات اعتماد جهاز ISE باستخدام KRB5 واكتشف جميع المجالات الموثوق بها.
10. وعند اكتمال الانضمام، تقوم عقدة ISE بتحديث مجموعات AD و SIDS المقترنة بها وتبدأ عملية تحديث SID تلقائيا. تحقق من إمكانية إكمال هذه العملية على جانب AD.

ترك مجال AD

عندما يغادر ISE، يجب أن يأخذ العالن بعين الاعتبار:

1. أستخدم مستخدم مسؤول AD كامل لإجراء عمليات المغادرة. وهذا يتحقق من إزالة حساب جهاز ISE من قاعدة بيانات Active Directory.
2. إذا تم ترك AD بدون بيانات اعتماد، فلن يتم إزالة حساب ISE من AD ويجب حذفه يدويا.
3. عند إعادة ضبط تكوين ISE من واجهة سطر الأوامر (CLI) أو إستعادة التكوين بعد النسخ الاحتياطي أو الترقية، فإنه يقوم بتنفيذ عملية خروج وقطع اتصال عقدة ISE من مجال Active Directory. (إذا تم الانضمام). ومع ذلك، لم تتم إزالة حساب عقدة ISE من مجال Active Directory.
4. يوصى بإجراء عملية خروج من مدخل المسؤول مع بيانات اعتماد Active Directory لأنه يزيل أيضا حساب العقدة من مجال Active Directory. كما يوصى بذلك عند تغيير اسم مضيف ISE.

تجاوز فشل التاير المستمر

عند اتصال وحدة التحكم بالمجال DC ب ISE يصبح غير متصل أو يتعذر الوصول إليه لأي سبب، يتم تشغيل تجاوز فشل وحدة التحكم بالمجال DC تلقائيا على ISE. يمكن تشغيل تجاوز فشل التاير المستمر بواسطة الشروط التالية:

1. يكتشف موصل AD أن DC المحدد حاليا أصبح غير متوفر أثناء محاولة اتصال Cldap أو LDAP أو RPC أو Kerberos. في مثل هذه الحالات، يبدأ موصل AD تحديد DC ويفشل في الوصول إلى DC المحدد حديثا.
2. تم تشغيل وحدة التحكم بالمجال (DC) والاستجابة لاختبار اتصال CLDAP، ولكن وحدة RPC، وكانت تتعذر على موصل AD الاتصال به لسبب ما (مثال: تم رفض منفذ RPC، ولم يتم إيقاف تشغيل وحدة التحكم بالمجال DC في حالة "النسخ المتماثل المعطل"، ولكن وحدة التحكم بالمجال DC بشكل صحيح).

في مثل هذه الحالات، يقوم موصل AD بتهيئة تحديد DC بقائمة محظورة (يتم وضع DC المحدد. لم يتم تخزين وحدة التحكم بالمجال DC ويحاول الاتصال ب DC "سيئ" في القائمة المحظورة) بالمجال (DC) المحددة في القائمة المحظورة لمدة تصل إلى 60 دقيقة.

يجب أن يقوم موصل AD بإكمال تجاوز الفشل خلال فترة زمنية معقولة (أو الفشل إذا لم يكن ذلك ممكنا). ولهذا السبب، يحاول موصل AD تجربة عدد محدود من محاولات DC أثناء تجاوز الفشل.

يقوم ISE بحظر محاولات التحكم بالمجال AD إذا كان هناك خطأ غير قابل للاسترداد في الشبكة

أو الخادم لمنع ISE من إستخدام DC تالف. ال تتم إضافة DC إلى القائمة المحظورة إذا لم يستجيب إلى إختبارات اتصال CLDAP. تعمل خدمة ISE على تقليل أولوية وحدة التحكم بالمجال (DC) التي ال تستجيب.

اتصال ISE-AD من خالل LDAP

يبحث ISE عن آلة أو مستخدم في AD بإحدى تنسيقات البحث هذه. إذا كان البحث عن جهاز، فإن ISE يضيف "$" في نهاية اسم الجهاز. هذه قائمة بأنواع الهوية التي تستخدم لتعريف مستخدم في AD:

- اسم SAM: اسم المستخدم أو اسم الجهاز بدون أي عالمة مجال، هذا هو اسم تسجيل دخول المستخدم في AD. **مثال: ساجدة أو ساجدة$**
- cn: هو اسم عرض المستخدم على AD، يجب ألا يكون هو نفسه SAM. **مثال: ساجدة أحمد.**
- اسم المستخدم الأساسي (UPN): هو مزيج من اسم SAM واسم المجال (SAM_NAME@domian). **مثال: sajeda@cisco.com أو sajeda$@cisco.com**
- UPN البديل: عبارة عن الحقات UPN إضافية / بديلة تم تكوينها في AD بخالف اسم المجال. تتم إضافة هذا التكوين بشكل عام في AD (لم يتم تكوينه لكل مستخدم) ومن غير الضروري أن يكون الحقة اسم مجال حقيقي.
يمكن أن يكون لكل إعالن الحقة UPN متعددة(@alt1.com،@alt2.com،...، وما إلى ذلك). مثال: Main UPN (sajeda@cisco.com)، Alternative UPN:sajeda@domain1 ، sajeda@domain2

- اسم NetBIOS الثابت مسبقا: هو اسم المجال\اسم المستخدم لاسم الجهاز. **مثال: cisco\sajeda أو cisco\machine$**
- المضيف/البادئة مع الجهاز غير المؤهل: يستخدم هذا لمصادقة الجهاز عند إستخدام اسم الجهاز فقط، وهو اسم المضيف/الجهاز فقط. **مثال: المضيف/الجهاز**
- المضيف/ البادئة مع الجهاز المؤهل بالكامل: يتم إستخدام هذا الأمر لمصادقة الجهاز عند إستخدام FQDN للجهاز، وعادة في حالة مصادقة الشهادة، يكون المضيف/FQDN الخاص بالجهاز. **مثال: host/machine.cisco.com**
- اسم SPN: االسم الذي يقوم العميل من خالله بتعريف مثيل خدمة بشكل فريد، (أمثلة: HTTP و LDAP و SSH) المستخدم للجهاز فقط.

مصادقة المستخدم مقابل تدفق AD:

1. حل الهوية وتحديد نوع الهوية - SAM و UPN و SPN. إذا استلم ISE الهوية كاسم مستخدم فقط، فإنه يبحث عن حساب SAM مرتبط في AD. إذا استلم ISE الهوية على هيئة username@domain، فإنه يبحث عن UPN أو بريد مطابق في AD. في كال السيناريوين يستخدم ISE عوامل تصفية إضافية للجهاز أو اسم المستخدم.
2. مجال البحث أو الغابة (يعتمد على نوع الهوية)
3. الحتفاظ بمعلومات حول جميع الحسابات المقترنة (JP و DN و UPN و Domain)
4. في حالة عدم العثور على أي حساب مقترن، تكون ردود AD مع المستخدم غير معروفة.
5. إجراء مصادقة MS-RPC (أو Kerberos) لكل حساب مقترن
6. في حالة تطابق حساب واحد فقط مع هوية الإدخال وكلمة المرور، تكون المصادقة ناجحة
7. وإذا تطابقت حسابات متعددة مع الهوية الواردة، فإن ISE يستخدم كلمة المرور لحل الغموض بحيث تتم مصادقة الحساب مع كلمة المرور المقترنة وتزيد الحسابات الأخرى

من عداد كلمة المرور غير الصحيح بمقدار 1.

8. إذا لم يتطابق أي حساب مع الهوية وكلمة المرور الواردين، فعندئذ ترد AD بكلمة مرور غير صحيحة.

محرك خدمات كشف الهوية (ISE) عوامل تصفية البحث

تستخدم عوامل التصفية لتعريف الكيان الذي يريد الاتصال ب AD. تبحث ISE دائما عن هذا الكيان في مجموعات المستخدمين والآلات.

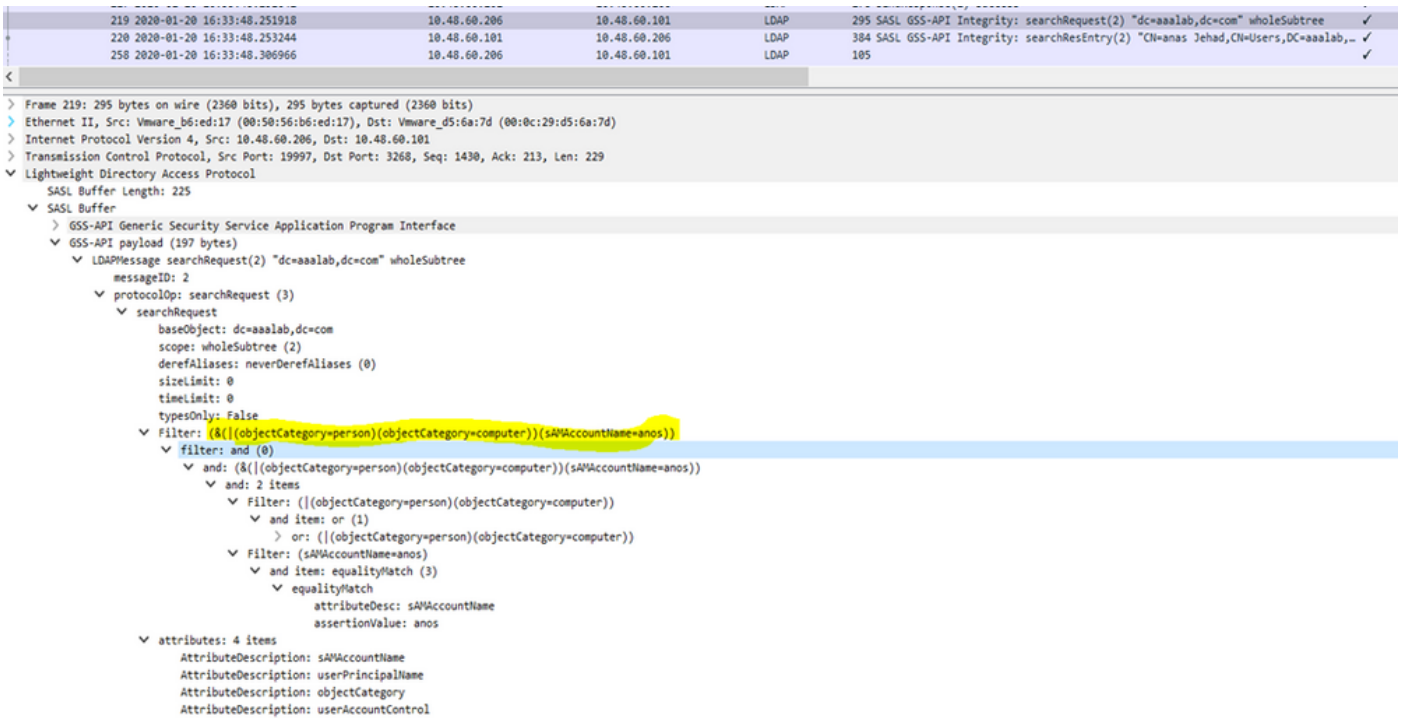
أمثلة على عوامل تصفية البحث:

1. **SAM Search:** إذا كان ISE يتلقى هوية كاسم مستخدم فقط دون أي علامة مجال، فإن ISE يعامل اسم المستخدم هذا كSAM ويبحث في AD لجميع مستخدمي الأجهزة أو الأجهزة التي لها تلك الهوية كاسم SAM.

إذا لم يكن اسم SAM فريدا، فإن ISE يستخدم كلمة المرور للتمييز بين المستخدمين وكان ISE مكون لاستخدام بروتوكول غير معرف كلمة مرور مثل EAP-TLS.

لا توجد معايير أخرى لتحديد موقع المستخدم المناسب، لذلك يفشل ISE في المصادقة مع حدوث خطأ "هوية غامضة".

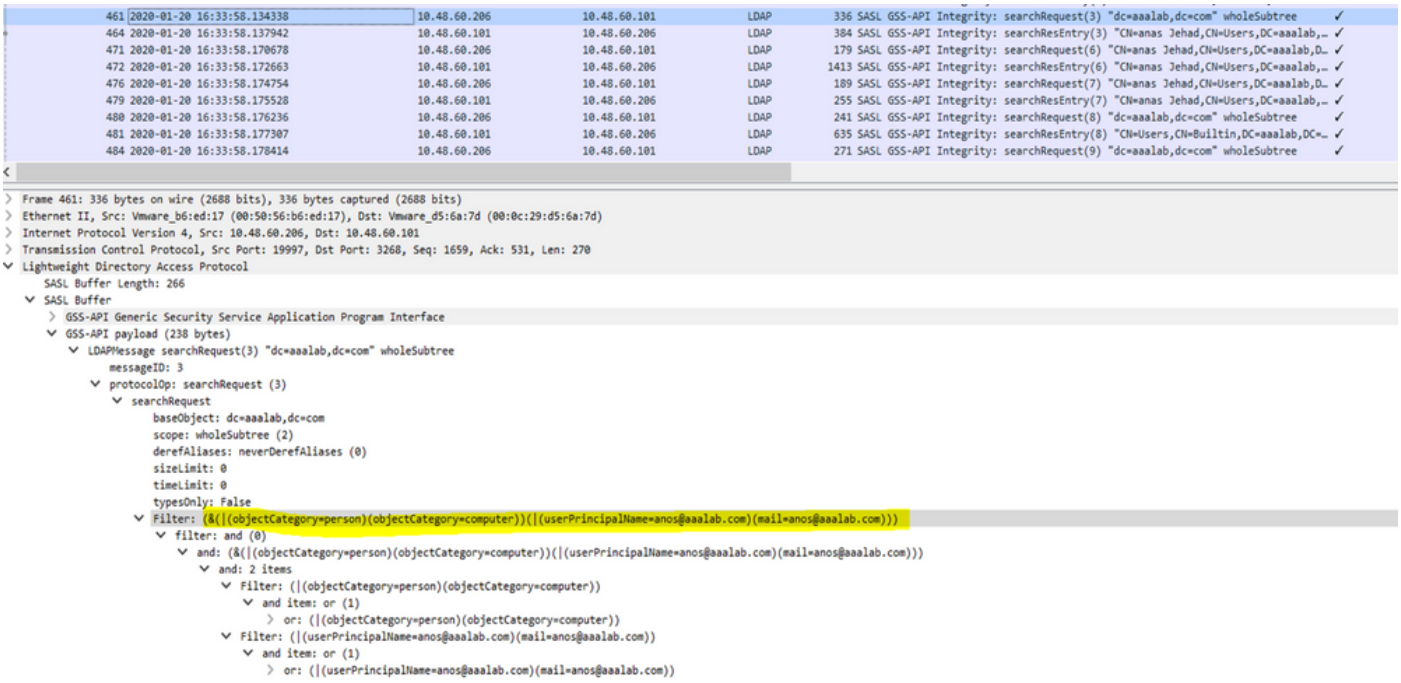
ومع ذلك، إذا كانت شهادة المستخدم موجودة في Active Directory، يستخدم Cisco ISE مقارنة ثنائية لحل الهوية.



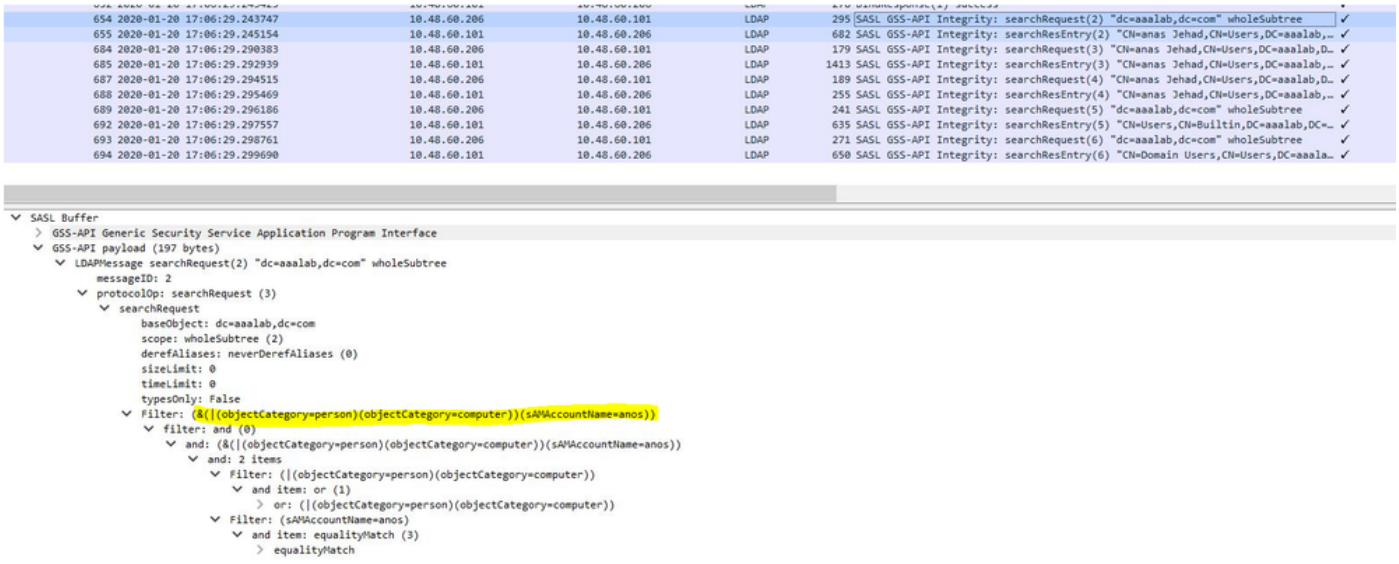
2. **بحث عبر UPN أو Mail:** إذا كان ISE يتلقى هوية على هيئة username@domain، يبحث ISE في كل كتالوجات عمومية في الغابة بحثا عن تطابق مع هوية UPN تلك أو هوية البريد الإلكتروني UPN أو البريد "identity=match".

إذا كان هناك تطابق فريد، يستمر Cisco ISE مع تدفق AAA.

إذا كانت هناك نقاط ربط متعددة لها نفس UPN وكلمة مرور أو نفس UPN والبريد، فإن Cisco ISE يفشل في المصادقة مع حدوث خطأ "معرف ملتبس".



3. **بحث NetBIOS:** إذا تلقت ISE هوية باستخدام بادئة مجال NetBIOS (ex:Cisco\Sajedah)، فعندئذ تقوم ISE بالبحث في الغابات عن مجال NetBIOS. وبمجرد العثور عليها، تبحث عن اسم SAM المتوفر (ساجدة في المثال الذي نمثله)

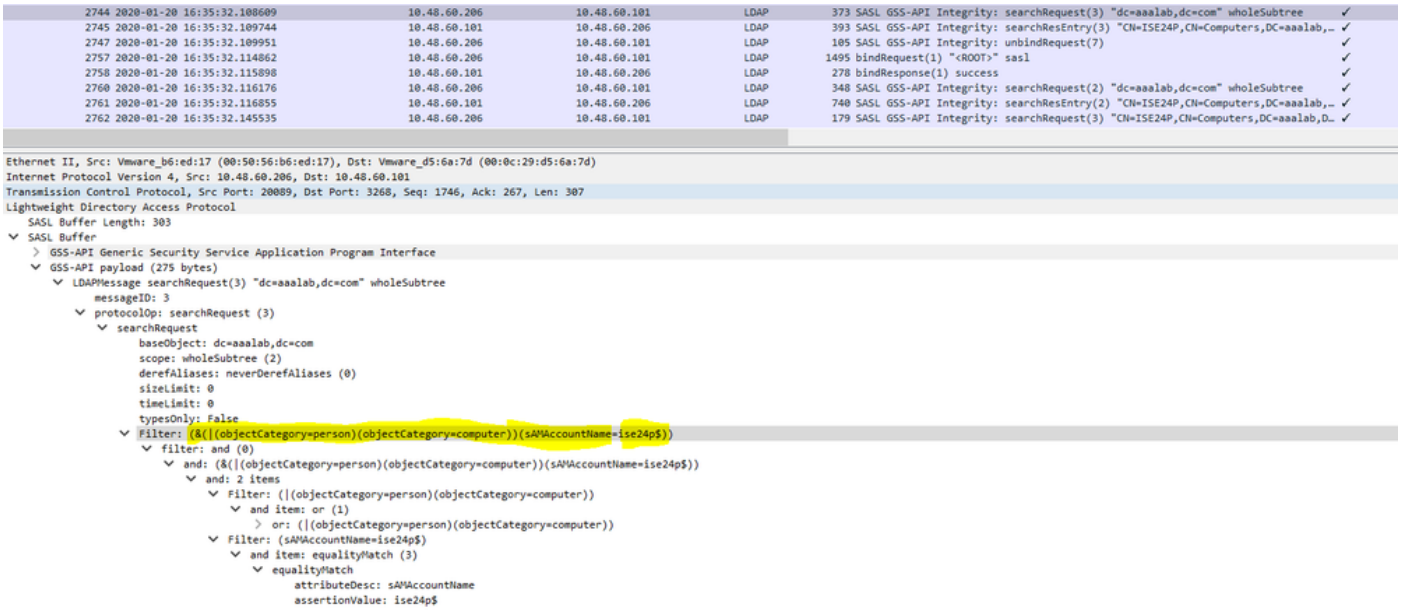


4. **بحث عن قاعدة الجهاز:** إذا كان ISE يتلقى مصادقة جهاز، بهوية مضيف/بادئة، يقوم ISE بالبحث في الغابة عن سمة servicePrincipalName متطابقة.

إذا تم تحديد لاحقة مجال مؤهلة بالكامل في الهوية، على سبيل المثال host/machine.domain.com، فإن Cisco ISE يبحث في الغابة حيث يوجد هذا المجال.

إذا كانت الهوية في شكل مضيف/جهاز، يقوم Cisco ISE بالبحث في جميع الغابات عن اسم الخدمة الأساسي.

إذا كان هناك أكثر من تطابق واحد، يفشل Cisco ISE في المصادقة باستخدام خطأ "معرف ملتبس".



ملاحظة: تظهر نفس المرشحات في ملفات ISE Ad-Agent.log

ملاحظة: ISE 2.2 تصحيح 4 و السابق و 2.3 تصحيح 1 و المستخدمين المحددين مسبقا مع الخصائص SAM أو CN أو كالهما. Cisco ISE، الإصدار 2.2 تصحيح 5 وأعلى، و 2.3 تصحيح 2 وأعلى، أستخدم سمة sAMAccountName فقط كسمة افتراضية.

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).