Identity Service Engine (ISE) und Active Directory (AD)

Inhalt

Einleitung

In diesem Dokument wird die Kommunikation zwischen Identity Service Engine (ISE) und Active Directory (AD), verwendeten Protokollen, AD-Filtern und Datenflüssen beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt grundlegende Kenntnisse in folgenden Bereichen:

- ISE 2.x- und Active Directory-Integration .
- Externe Identitätsauthentifizierung auf der ISE.

Verwendete Komponenten

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

AD-Protokolle

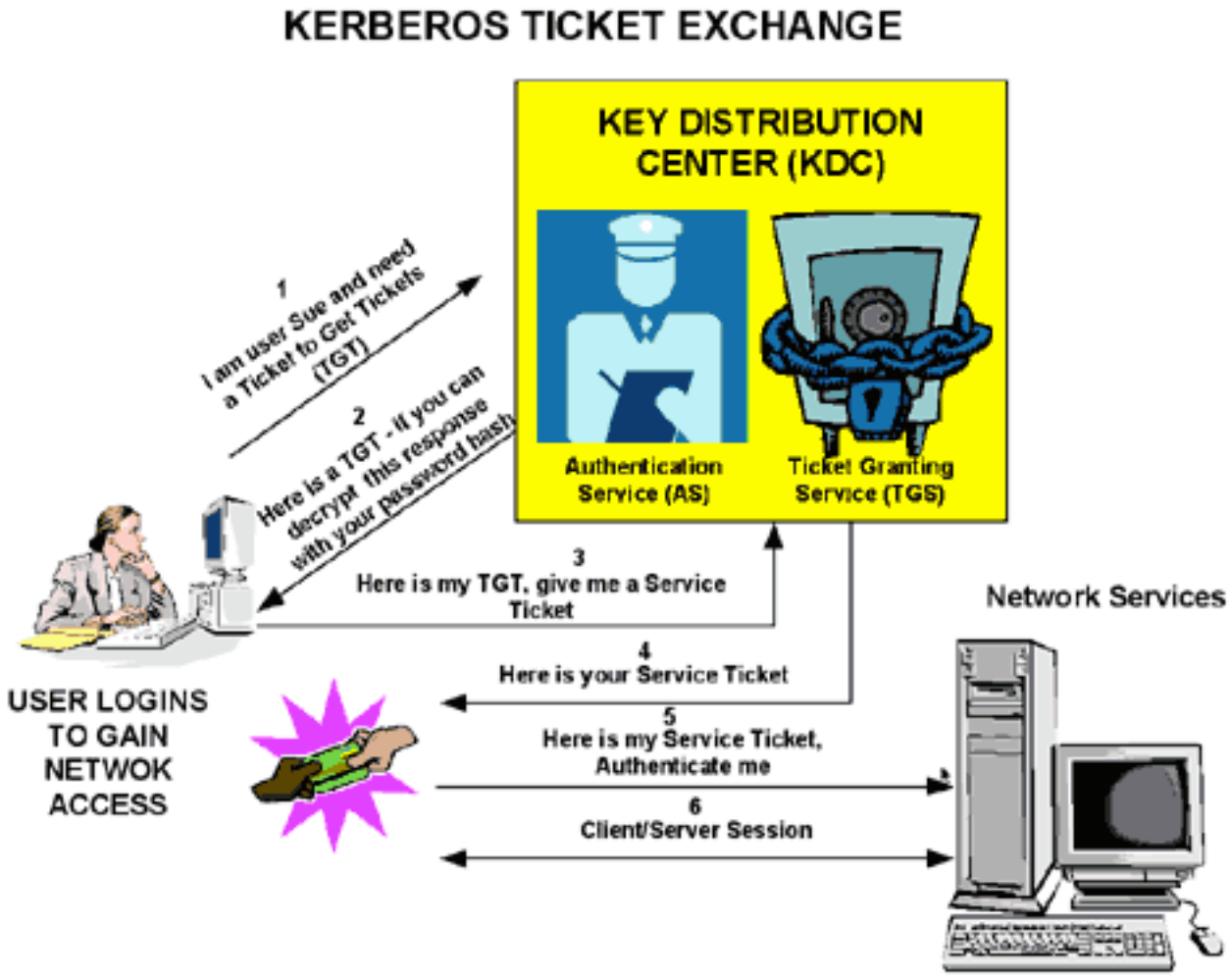
Kerberos-Protokoll

Die drei Kerberos-Chefs umfassen das Key Distribution Center (KDC), den Client-Benutzer und den Server für den Zugriff.

Der KDC wird als Teil des Domänencontrollers installiert und führt zwei Dienstfunktionen aus: Der Authentifizierungsdienst (AS) und der Ticket-Granting-Dienst (TGS).

Beim ersten Zugriff des Clients auf eine Serverressource sind drei Austauschvorgänge erforderlich:

1. AS-Austausch.
2. TGS-Austausch.
3. Client/Server (CS) Exchange



- Domänencontroller = KDC (AS + TGS).
- Melden Sie sich bei AS (dem SSO-Portal) mit Ihrem Kennwort an.
- Holen Sie sich ein Ticket Granting Ticket (TGT) (ein Session-Cookie).
- Anfordern der Anmeldung bei einem Service (SRV01)
- SRV01 leitet Sie zu KDC um.
- TGT dem KDC anzeigen - (Ich bin bereits authentifiziert)

- KDC bietet Ihnen TGS für SRV01.
- Umleitung zu SRV01.
- Service-Ticket zum SRV01 anzeigen.
- SRV01 überprüft/vertraut Service Ticket.
- Das Service-Ticket enthält alle meine Informationen.
- SRV01 meldet mich an.

Bei der erstmaligen Anmeldung an einem Netzwerk müssen die Benutzer den Zugriff aushandeln und einen Anmeldenamen und ein Kennwort angeben, um von der AS-Komponente eines KDC in ihrer Domäne überprüft zu werden.

Der KDC hat Zugriff auf Active Directory-Benutzerkontoinformationen. Nach der Authentifizierung erhält der Benutzer ein Ticket Granting Ticket (TGT), das für die lokale Domäne gültig ist.

Das TGT hat eine standardmäßige Lebensdauer von 10 Stunden und wird während der Benutzeranmeldesitzung verlängert, ohne dass der Benutzer sein Kennwort erneut eingeben muss.

Das TGT wird auf dem lokalen System im flüchtigen Speicherplatz zwischengespeichert und zum Anfordern von Sitzungen mit Diensten im gesamten Netzwerk verwendet.

Der Benutzer zeigt das TGT dem TGS-Teil des KDC an, wenn der Zugriff auf einen Serverdienst erforderlich ist.

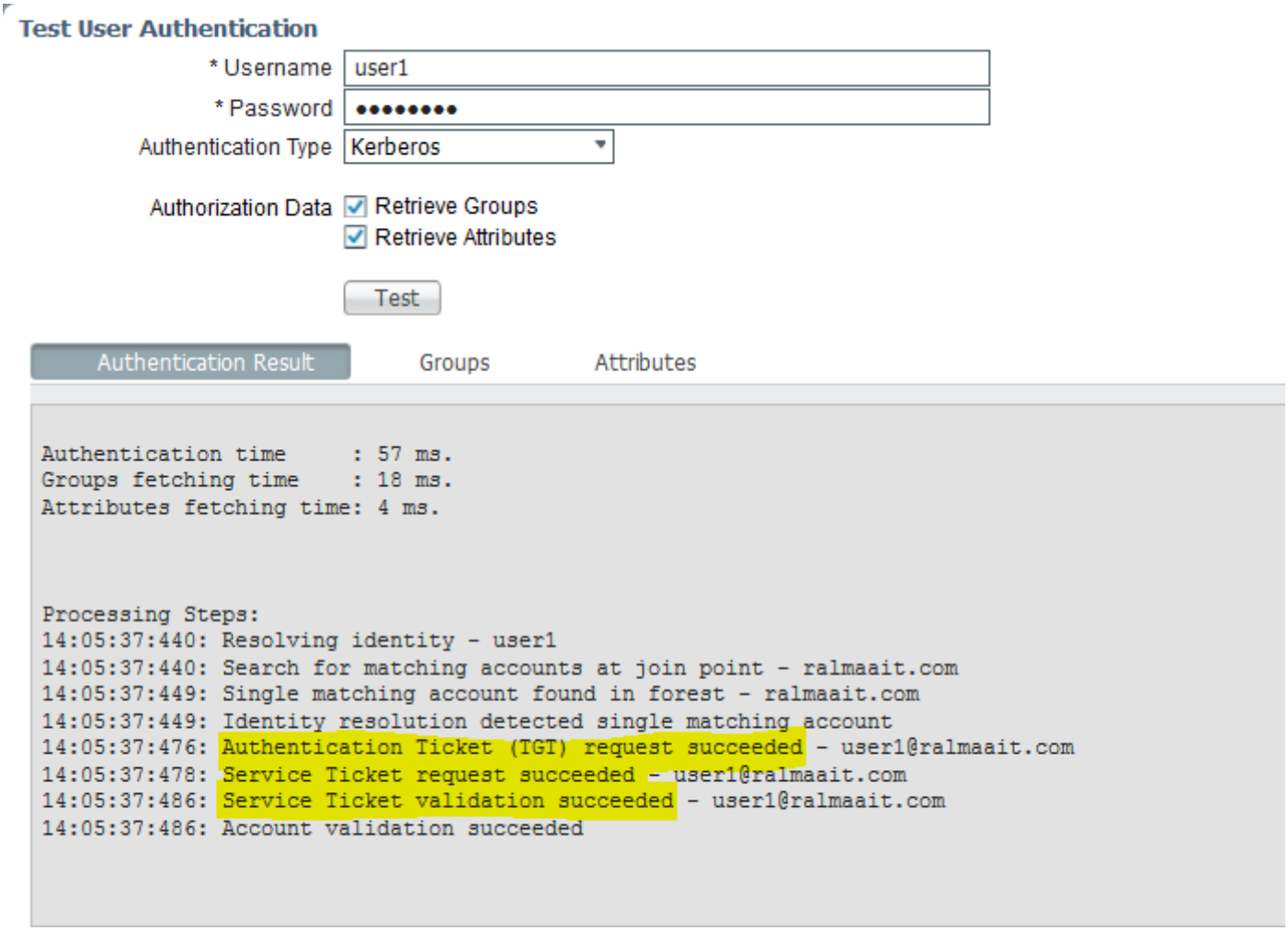
Das TGS auf dem KDC authentifiziert den Benutzer-TGT und erstellt ein Ticket und einen Sitzungsschlüssel für den Client und den Remote-Server. Diese Informationen (das Service-Ticket) werden dann lokal auf dem Client-Rechner zwischengespeichert.

Der TGS empfängt den Client TGT und liest ihn mit seinem eigenen Schlüssel. Wenn das TGS die Client-Anforderung genehmigt, wird sowohl für den Client als auch für den Zielserver ein Service-Ticket generiert.

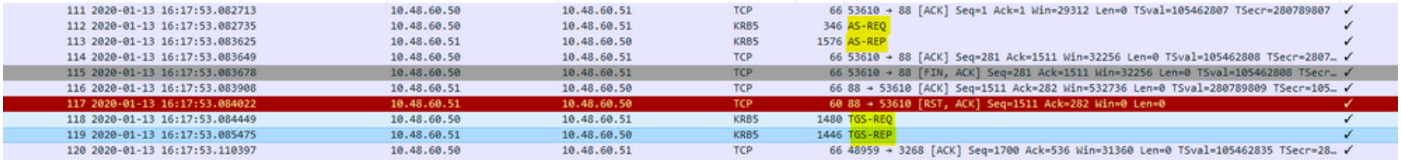
Der Client liest seinen Teil mit dem TGS-Sitzungsschlüssel, der zuvor aus der AS-Antwort abgerufen wurde.

Der Client zeigt den Serverteil der TGS-Antwort dem Zielserver im nächsten Client/Server-Austausch an.

Beispiel:



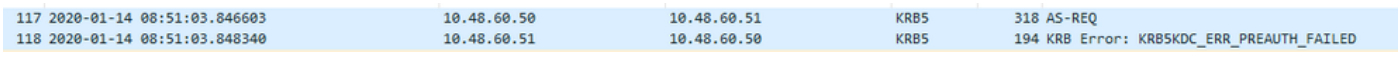
Paketerfassung von der ISE für einen authentifizierten Benutzer:



Die AS-REQ enthält den Benutzernamen. Wenn das Kennwort richtig ist, stellt der AS-Dienst ein mit dem Benutzerkennwort verschlüsseltes TGT bereit. Das TGT wird dann an den TGT-Dienst weitergeleitet, um ein Sitzungsticket zu erhalten.

Die Authentifizierung ist erfolgreich, wenn ein Sitzungsticket empfangen wird.

Dies ist ein Beispiel, bei dem das vom Client angegebene Kennwort falsch ist:



Wenn das Kennwort falsch ist, schlägt die AS-Anforderung fehl, und es wird kein TGT empfangen:

```
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
```

Meldet sich bei falschem Kennwort in der Datei ad_agent.log an:

2020-01-14 13:36:05,442 DEBUG ,140574072981248,krb5: Anfrage (276 Byte) an RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325 gesendet

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Fehler von KDC empfangen: -1765328360/Vorauthentifizierung fehlgeschlagen,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 DEBUG ,140574072981248,krb5: Eingabetypen für Vorauth wiederholen: 16, 14, 19, 2,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WARNUNG,140574072981248,[LwKrb5GetTgtImpl ../../lwadvapi/threaded/krbtgt.c:329] KRB5 Fehlercode: -1765328360 (Nachricht: Preauthentication fehlgeschlagen),LwTranslateKrb5Error(),lwadvapi/threaded/lwkrb5.c:892

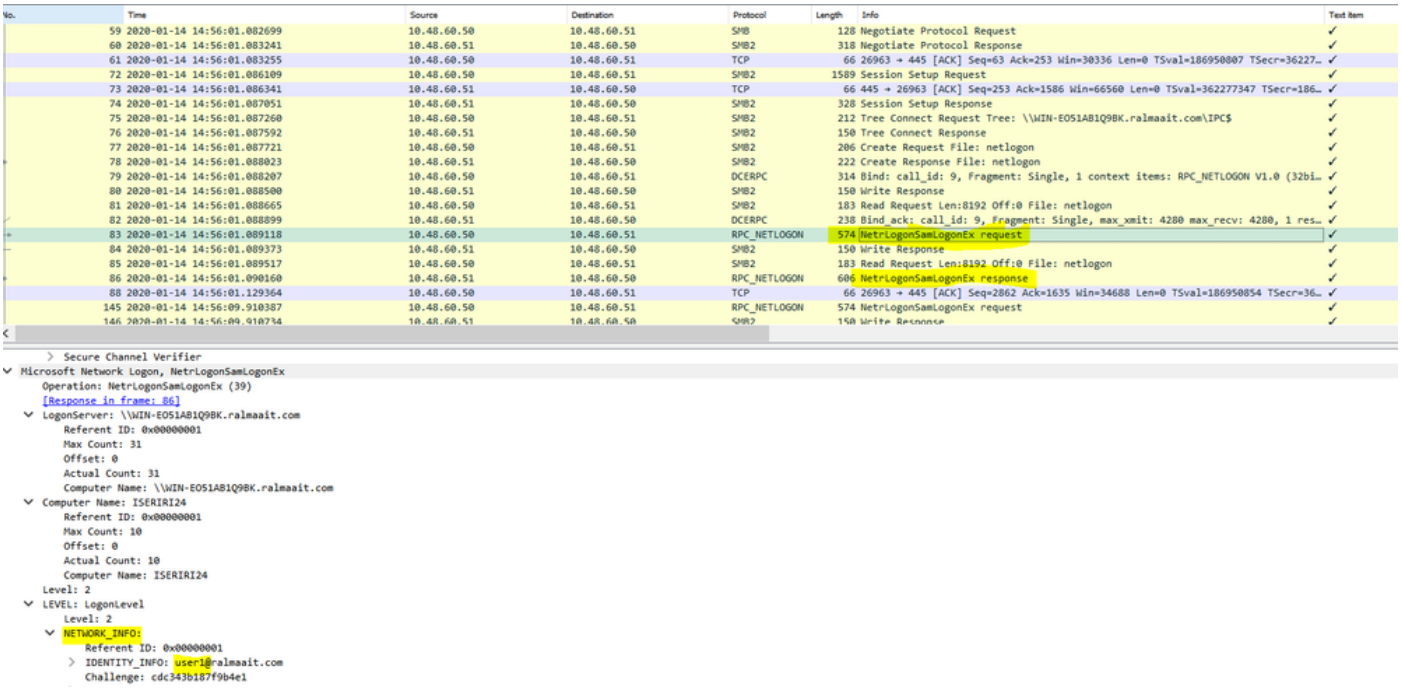
2020-01-14 13:36:05,444 DEBUG ,140574072981248,[LwKrb5InitializeUserLoginCredentials()] Fehlercode: 40022 (Symbol: LW_ERROR_PASSWORD_MISMATCH),LwKrb5InitializeUserLoginCredentials(),lwadvapi/threaded/lwkrb5.c:1453

MS-RPC-Protokoll

ISE verwendet MS-RPC über SMB, SMB stellt die Authentifizierung bereit und benötigt keine separate Sitzung, um den Standort eines bestimmten RPC-Services zu ermitteln. Es verwendet einen Mechanismus namens "Named Pipe", um zwischen dem Client und dem Server zu kommunizieren.

- Erstellen Sie eine SMB-Sitzungsverbindung.
- Transport von RPC-Nachrichten über SMB/CIFS.TCP Port 445 als Transportmedium
- Die SMB-Sitzung identifiziert, welcher Port von einem bestimmten RPC-Dienst ausgeführt wird, und verarbeitet die Benutzerauthentifizierung.
- Stellen Sie eine Verbindung zu versteckter Freigabe IPC$ für die Kommunikation zwischen Prozessen her.
- Öffnen Sie eine entsprechende Named Pipe für die gewünschte RPC-Ressource/Funktion.

Transaktion des RPC-Austauschs über SMB.



Die Fehlermeldung **negotiate protocol request/response** Zeile handelt den Dialekt von SMB aus. Die Fehlermeldung **session setup request/response** führt die Authentifizierung durch.

Strukturverbindungsanforderung und -antwort stellen eine Verbindung mit der angeforderten Ressource her. Sie sind mit einer speziellen Freigabe IPC$ verbunden.

Diese prozessübergreifende Kommunikationsfreigabe stellt die Kommunikationsmittel zwischen Hosts und auch als Transport für MSRPC-Funktionen bereit.

Bei Paket 77 ist **Create Request File** und der Dateiname ist der Name des verbundenen Dienstes (in diesem Beispiel der Netzwerkanmeldedienst).

Bei den Paketen 83 und 86 ist die NetLogonSamLogonEX-Anforderung, bei der Sie den Benutzernamen für die Client-Authentifizierung auf der ISE an das AD im Feld Network_INFO senden.

Das NetLogonSamLogonEX-Antwortpaket antwortet mit den Ergebnissen.

Einige Flags-Werte für die NetlogonSamLogonEX-Antwort:
0xc000006a ist STATUS_WRONG_PASSWORD
0x00000000 ist STATUS_SUCCESS
0x00000103 ist STATUS_PENDING

ISE-Integration mit Active Directory (AD)

Die ISE verwendet LDAP, KRB und MSRBC, um während des Join/Leave- und Authentifizierungsprozesses mit AD zu kommunizieren.

Die nächsten Abschnitte enthalten die Protokolle, das Suchformat und die Mechanismen, die für die Verbindung mit einem bestimmten AD-Rechenzentrum und die Benutzerauthentifizierung für diesen Rechenzentrum verwendet werden.

Falls das Rechenzentrum aus irgendeinem Grund offline geht, wird ein Failover von der ISE zum nächsten verfügbaren Rechenzentrum durchgeführt, und der Authentifizierungsprozess wird nicht beeinträchtigt.

Ein Global Catalog-Server (GC) ist ein Domänencontroller, auf dem Kopien aller Active Directory-Objekte in der Gesamtstruktur gespeichert werden.

Es speichert eine vollständige Kopie aller Objekte im Verzeichnis Ihrer Domäne und eine teilweise Kopie aller Objekte aller anderen Gesamtstrukturdomänen.

Der globale Katalog ermöglicht es Benutzern und Anwendungen, Objekte in einer beliebigen Domäne der aktuellen Gesamtstruktur zu finden, wobei nach Attributen gesucht wird, die in GC enthalten sind.

Der globale Katalog enthält einen grundlegenden (aber unvollständigen) Attributsatz für jedes Gesamtstrukturobjekt in jeder Domäne (Partial Attribute Set, PAT).

Der GC empfängt Daten von allen Domänenverzeichnispartitionen in der Gesamtstruktur. Sie werden mit dem standardmäßigen AD-Replikationsdienst kopiert.

Der ISE zur AD beitreten

Voraussetzungen für die Integration von Active Directory und ISE

1. Vergewissern Sie sich, dass Sie über die Berechtigungen eines Super-Administrators oder eines System-Administrators in der ISE verfügen.
2. Verwenden Sie die NTP-Servereinstellungen (Network Time Protocol), um die Zeit zwischen dem Cisco Server und Active Directory zu synchronisieren. Die maximal zulässige Zeitdifferenz zwischen ISE und AD beträgt 5 Minuten.
3. Der auf der ISE konfigurierte DNS muss SRV-Abfragen für DCs, GCs und KDCs mit oder ohne zusätzliche Standortinformationen beantworten können.
4. Stellen Sie sicher, dass alle DNS-Server DNS-Abfragen für eine beliebige Active Directory-DNS-Domäne beantworten und rückgängig machen können.
5. AD muss über mindestens einen globalen Katalogserver verfügen, der von Cisco in der Domäne, der Sie Cisco beitreten, betrieben wird und auf den Cisco zugreifen kann.

AD-Domäne beitreten

Die ISE wendet die Domänenerkennung an, um Informationen über die verbundene Domäne in drei Phasen zu erhalten:

1. Abfragen verbundener Domänen - Erkennt Domänen aus der Gesamtstruktur und Domänen, die der verbundenen Domäne extern vertraut sind.
2. Abfragen von Stammdomänen in der Gesamtstruktur - Erstellt eine Vertrauensstellung mit der Gesamtstruktur.
3. Abfragen von Stammdomänen in vertrauenswürdigen Gesamtstrukturen - Erkennt Domänen

aus den vertrauenswürdigen Gesamtstrukturen.

Darüber hinaus erkennt die Cisco ISE DNS-Domänennamen (UPN-Suffixe), alternative UPN-Suffixe und NTLM-Domänennamen.

Die ISE wendet eine DC-Erkennung an, um alle Informationen über die verfügbaren DCs und GCs abzurufen.

1. Der Join-Prozess beginnt mit den Anmeldeinformationen des Super Admin auf AD, die in der Domäne selbst vorhanden sind. Wenn der Benutzername in einer anderen Domäne oder Subdomäne vorhanden ist, muss er in der UPN-Schreibweise (username@domain) angegeben werden.
2. Die ISE sendet eine DNS-Abfrage für alle DCs-, GCs- und KDCs-Datensätze. Wenn die DNS-Antwort keine Antwort enthielt, schlägt die Integration mit einem DNS-bezogenen Fehler fehl.
3. Die ISE verwendet den CLDAP-Ping, um alle DCs und GCs durch gesendete CLDAP-Anfragen an die DCs zu erkennen, die ihren Prioritäten im SRV-Datensatz entsprechen. Die erste DC-Antwort wird verwendet, und die ISE wird dann mit diesem DC verbunden.

Ein Faktor, der zur Berechnung der DC-Priorität verwendet wird, ist die Zeit, die das DC benötigt, um auf CLDAP-Pings zu reagieren. Eine schnellere Antwort erhält eine höhere Priorität.

> **Anmerkung:** CLDAP ist der Mechanismus, den die ISE verwendet, um Verbindungen zu den Rechenzentren herzustellen und aufrechtzuerhalten. Es misst die Reaktionszeit bis zur ersten Gleichstromantwort. Es schlägt fehl, wenn Sie keine Antwort von DC sehen. Warnen, wenn die Antwortzeit länger als 2,5 Sekunden ist. CLDAP pingt alle Rechenzentren am Standort (falls kein Standort vorhanden ist, werden alle Rechenzentren in der Domäne angepingt). Die CLDAP-Antwort enthält den DC-Standort und den Client-Standort (den Standort, dem der ISE-Computer zugewiesen ist).

4. Die ISE empfängt dann TGT mit Anmeldeinformationen für "join user".
5. Generieren Sie den ISE-Systemkontonamen mit dem MSRPC. (SAM und SPN)
6. AD nach SPN durchsuchen, wenn das ISE-Computerkonto bereits vorhanden ist. Wenn der ISE-Rechner nicht vorhanden ist, erstellt die ISE einen neuen.
7. Öffnen Sie das Computerkonto, legen Sie das Kennwort für das ISE-Computerkonto fest, und stellen Sie sicher, dass auf das ISE-Computerkonto zugegriffen werden kann.
8. Legen Sie ISE-Systemkontoattribute (SPN, dnsHostname usw.) fest.
9. Rufen Sie TGT mit ISE-Systemanmeldeinformationen mit KRB5 ab, und suchen Sie nach allen vertrauenswürdigen Domänen.
10. Wenn der Join abgeschlossen ist, aktualisiert der ISE-Knoten seine AD-Gruppen und die zugehörigen SIDS und startet automatisch den SID-Update-Prozess. Stellen Sie sicher, dass dieser Vorgang auf der AD-Seite abgeschlossen werden kann.

AD-Domäne verlassen

Wenn die ISE ausläuft, muss die AD Folgendes berücksichtigen:

1. Verwenden Sie einen vollständigen AD-Administrator-Benutzer, um den Verlassungsprozess durchzuführen. Dadurch wird überprüft, ob das ISE-Computerkonto aus der Active Directory-Datenbank entfernt wird.

2. Wenn das AD ohne Anmeldeinformationen zurückgelassen wurde, wird das ISE-Konto nicht aus dem AD entfernt und muss manuell gelöscht werden.
3. Wenn Sie die ISE-Konfiguration aus der CLI zurücksetzen oder die Konfiguration nach einem Backup oder Upgrade wiederherstellen, führt dies einen Vorgang aus und trennt den ISE-Knoten von der Active Directory-Domäne. (falls beigetreten). Das ISE-Knotenkonto wird jedoch nicht aus der Active Directory-Domäne entfernt.
4. Es wird empfohlen, einen Vorgang zum Verlassen des Admin-Portals mit den Active Directory-Anmeldeinformationen auszuführen, da dadurch auch das Node-Konto aus der Active Directory-Domäne entfernt wird. Dies wird auch empfohlen, wenn Sie den ISE-Hostnamen ändern.

DC-Failover

Wenn das mit der ISE verbundene Rechenzentrum offline ist oder aus irgendeinem Grund nicht erreichbar ist, wird auf der ISE automatisch ein Failover ausgelöst. Der RZ-Failover kann durch folgende Umstände ausgelöst werden:

1. Der AD-Connector erkennt, dass der aktuell ausgewählte Domänencontroller während eines CLDAP-, LDAP-, RPC- oder Kerberos-Kommunikationsversuchs nicht verfügbar war. In diesen Fällen initiiert der AD-Anschluss die DC-Auswahl und führt einen Failover zum neu ausgewählten DC durch.
2. DC ist eingeschaltet und reagiert auf CLDAP-Ping, aber AD Connector kann aus irgendeinem Grund nicht mit ihm kommunizieren (Beispiele: Der RPC-Port ist blockiert, das Rechenzentrum befindet sich im Zustand "unterbrochene Replikation", das Rechenzentrum wurde nicht ordnungsgemäß außer Betrieb genommen.)

In solchen Fällen initiiert der AD-Connector die DC-Auswahl mit einer gesperrten Liste ("böser" DC wird in der gesperrten Liste platziert) und versucht, mit dem ausgewählten DC zu kommunizieren. Der in der Liste gesperrter DCs ausgewählte DC wird nicht zwischengespeichert.

Der AD-Connector muss das Failover innerhalb eines angemessenen Zeitraums abschließen (oder ausfallen, wenn dies nicht möglich ist). Aus diesem Grund versucht der AD-Connector, während des Failovers eine begrenzte Anzahl von Rechenzentren zu verwenden.

Die ISE blockiert AD-Domänencontroller, wenn ein nicht behebbarer Netzwerk- oder Serverfehler vorliegt, um zu verhindern, dass die ISE einen fehlerhaften Rechenzentrum verwendet. Der Domänencontroller wird der Liste der gesperrten Geräte nicht hinzugefügt, wenn er nicht auf CLDAP-Pings antwortet. Die ISE verringert nur die Priorität des Rechenzentrums, das nicht reagiert.

ISE-AD-Kommunikation über LDAP

ISE sucht mit einem der folgenden Suchformate nach einem Computer oder Benutzer in AD. Wenn die Suche nach einem Computer durchgeführt wurde, fügt die ISE "$" am Ende des Computernamens hinzu. Dies ist eine Liste von Identitätstypen, die zum Identifizieren eines Benutzers in AD verwendet wird:

- SAM-Name: Benutzername oder Computername ohne Domänen-Markup. Dies ist der Benutzername in AD. **Beispiel: Sajeda oder Sajeda$**

- KN: der Anzeigename des Benutzers in AD ist, darf er nicht mit dem SAM identisch sein.

Beispiel: sajeda Ahmed.

- Benutzerprinzipalname (UPN): ist eine Kombination aus dem SAM-Namen und dem Domänennamen (SAM_NAME@domian). **Beispiel: sajeda@cisco.com oder sajeda$@cisco.com**

- Alternative UPN: ist eine zusätzliche / alternative UPN-Suffixe, die im AD konfiguriert sind, mit Ausnahme des Domänennamens. Diese Konfiguration wird global im AD hinzugefügt (nicht pro Benutzer konfiguriert), und es ist nicht erforderlich, ein echtes Domänennamen-Suffix zu sein.

Jedes AD kann mehrere UPN-Suffix (@alt1.com,@alt2.com,... usw.) haben. **Beispiel: Haupt-UPN (sajeda@cisco.com), Alternative UPN :sajeda@domain1 , sajeda@domain2**

- NetBIOS-Präfixname: ist der Domänenname\Benutzername des Systemnamens. **Beispiel: CISCO\sajeda oder CISCO\machine$**

- Host/Präfix mit nicht qualifiziertem Computer: Dies wird für die Authentifizierung des Computers verwendet, wenn nur der Computername verwendet wird. Es handelt sich nur um den Host-/Computernamen. **Beispiel: Host/Maschine**

- Host/Präfix mit voll qualifiziertem Rechner: Dies wird für die Authentifizierung des Computers verwendet, wenn der Computer-FQDN verwendet wird. In der Regel handelt es sich bei der Zertifikatauthentifizierung um den Host/FQDN des Computers. **Beispiel: host/machine.cisco.com**

- SPN-Name: Der Name, mit dem ein Client eine Instanz eines Dienstes eindeutig identifiziert (Beispiele: HTTP, LDAP, SSH), der nur für Computer verwendet wird.

Benutzerauthentifizierung für AD-Fluss:

1. Identitätstyp auflösen und Identitätstyp ermitteln - SAM, UPN, SPN. Wenn ISE die Identität nur als Benutzernamen empfängt, sucht sie im AD nach einem zugeordneten SAM-Konto. Wenn die ISE die Identität als username@domain erhält, sucht sie im AD nach einer übereinstimmenden UPN oder E-Mail. In beiden Szenarien verwendet die ISE zusätzliche Filter für den Computer- oder Benutzernamen.
2. Domäne oder Gesamtstruktur durchsuchen (abhängig vom Identitätstyp)
3. Behalten Sie Informationen zu allen verbundenen Konten (JP, DN, UPN, Domain) bei.
4. Wenn kein verbundenes Konto gefunden wird, sind die AD-Antworten für den Benutzer unbekannt.
5. MS-RPC- (oder Kerberos-) Authentifizierung für jedes verbundene Konto durchführen
6. Wenn nur ein einziges Konto mit der eingegebenen Identität und dem eingegebenen Kennwort übereinstimmt, ist die Authentifizierung erfolgreich.
7. Wenn mehrere Konten mit der eingehenden Identität übereinstimmen, verwendet die ISE das Kennwort, um die Mehrdeutigkeit zu beheben, sodass das Konto mit dem zugehörigen Kennwort authentifiziert wird und die anderen Konten den falschen Kennwortzähler um 1 erhöhen.
8. Wenn kein Konto mit der eingehenden Identität und dem Kennwort übereinstimmt, antwortet AD mit falschem Kennwort.

ISE Suchfilter

Filter werden verwendet, um eine Entität zu identifizieren, die mit AD kommunizieren möchte. Die ISE sucht immer nach dieser Entität in den Benutzer- und Computergruppen.

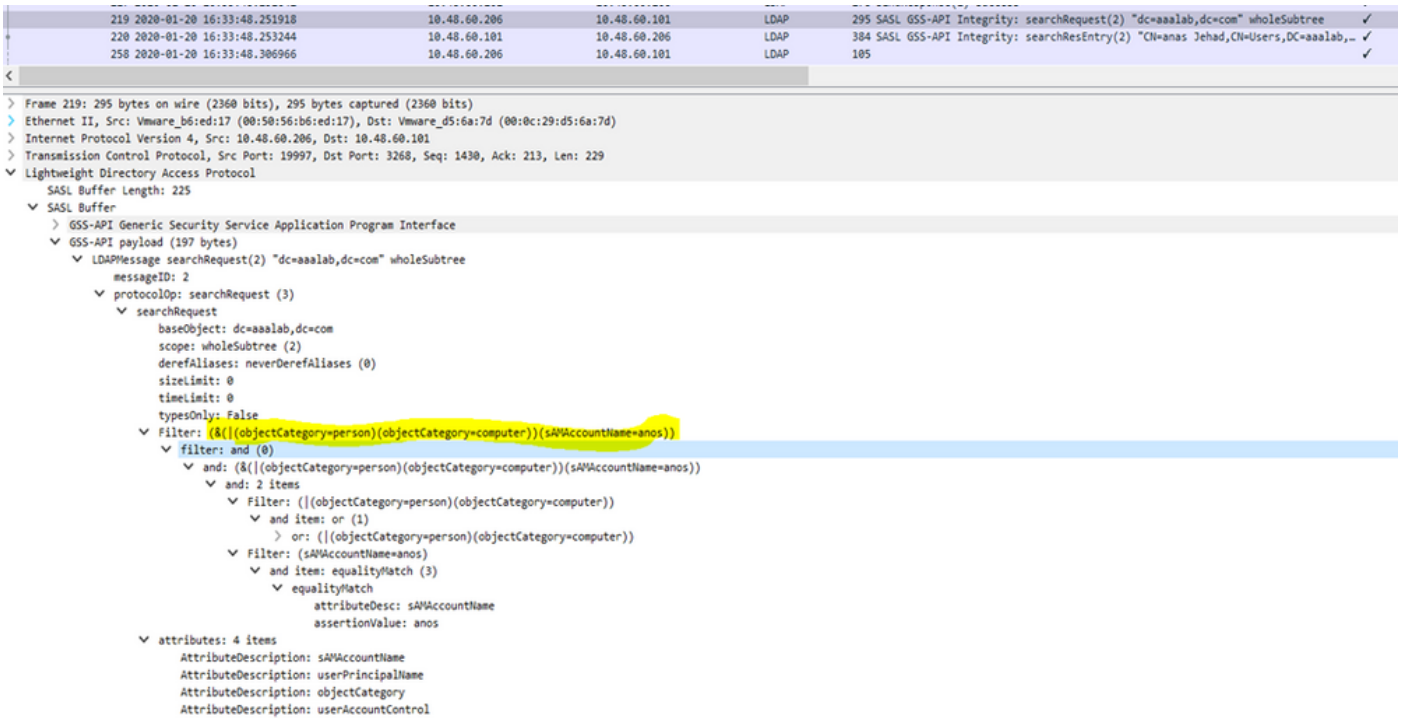
Beispiele für Suchfilter:

1. **SAM-Suche:** Wenn die ISE eine Identität als Benutzernamen nur ohne Domänenmarkup empfängt, behandelt die ISE diesen Benutzernamen als SAM und sucht in AD nach allen Computerbenutzern oder Computern, die diese Identität als SAM-Namen haben.

Wenn der SAM-Name nicht eindeutig ist, verwendet die ISE das Kennwort zur Unterscheidung zwischen Benutzern, und die ISE ist für die Verwendung eines kennwortlosen Protokolls wie EAP-TLS konfiguriert.

Es gibt keine anderen Kriterien für die Suche nach dem richtigen Benutzer, daher schlägt die ISE bei der Authentifizierung mit einem Fehler "Uneindeutige Identität" fehl.

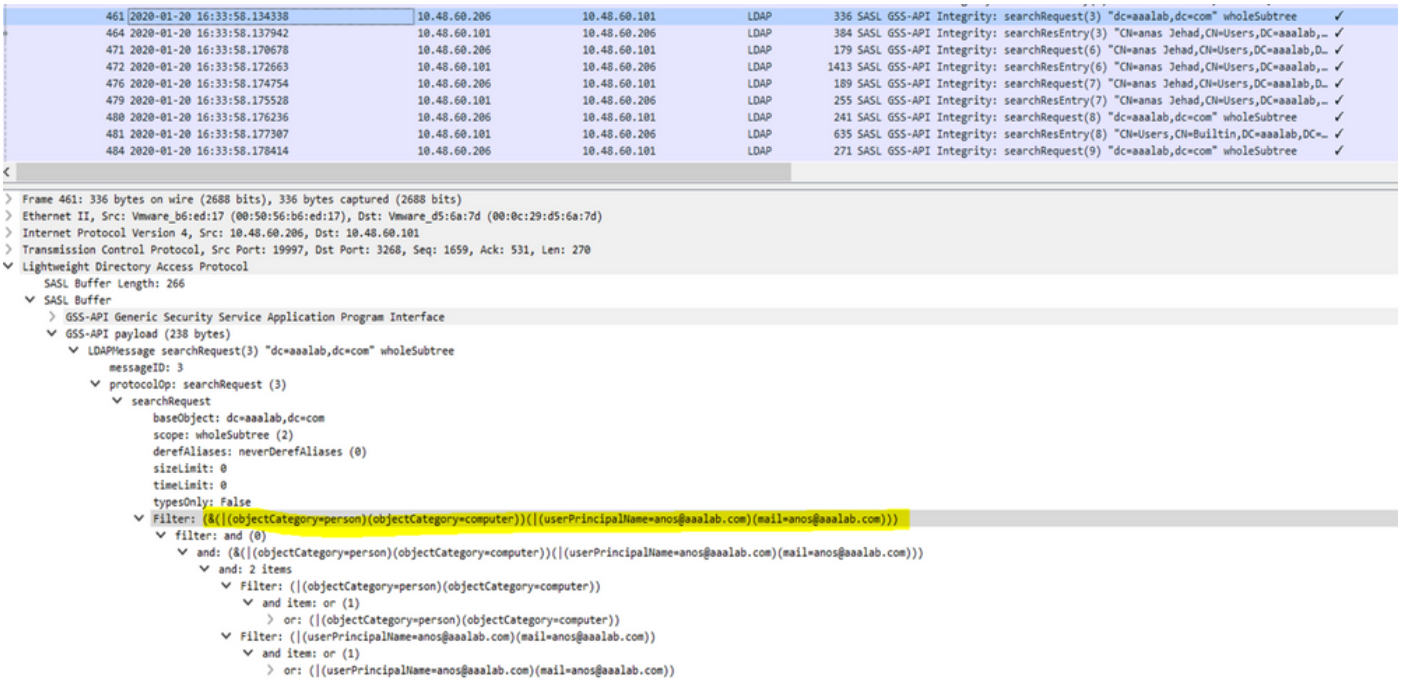
Wenn das Benutzerzertifikat jedoch in Active Directory vorhanden ist, verwendet die Cisco ISE einen Binärvergleich, um die Identität aufzulösen.



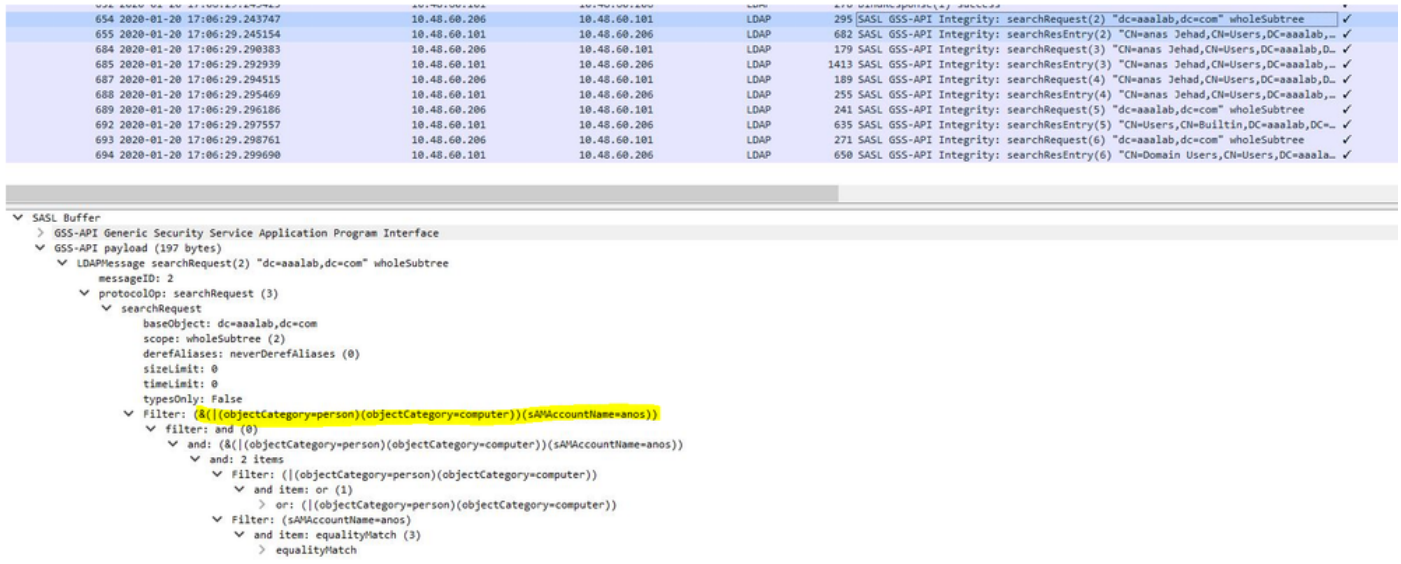
2. **UPN- oder MAIL-Suche:** Wenn die ISE eine Identität als username@domain erhält, durchsucht die ISE alle globalen Kataloge der Gesamtstruktur nach einer Übereinstimmung mit der UPN-Identität oder der Mail-Identität "identity=matching UPN or email".

Wenn eine eindeutige Übereinstimmung besteht, fährt die Cisco ISE mit dem AAA-Fluss fort.

Wenn mehrere Verbindungspunkte mit demselben UPN und einem Kennwort oder demselben UPN und derselben Mail vorhanden sind, schlägt die Authentifizierung der Cisco ISE mit dem Fehler "Uneindeutige Identität" fehl.



3. **NetBIOS-Suche:** Wenn die ISE eine Identität mit einem NetBIOS-Domänenpräfix (z. B. CISCO\sajedah) erhält, sucht die ISE in den Gesamtstrukturen nach der NetBIOS-Domäne. Nach der Suche wird der angegebene SAM-Name gesucht (in unserem Beispiel sajeda).

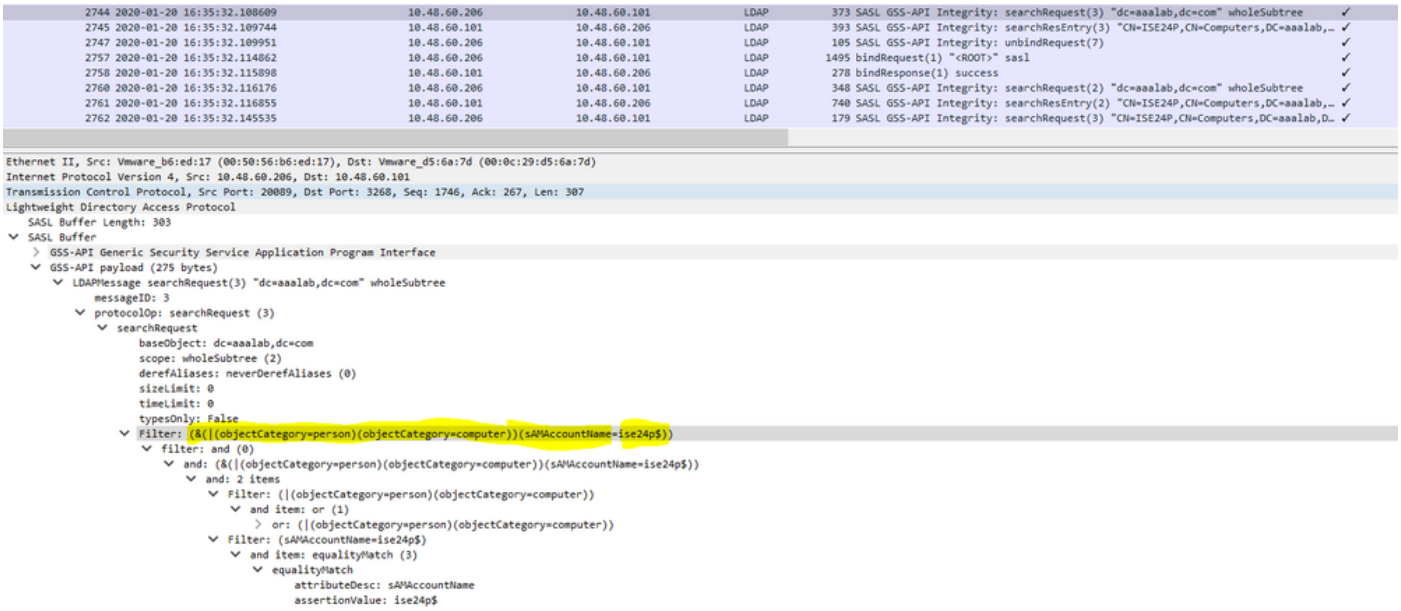


4. **Suche auf Computerbasis:** Wenn ISE eine Computerauthentifizierung mit einer Host-/Präfix-Identität empfängt, durchsucht ISE die Gesamtstruktur nach einem übereinstimmenden servicePrincipalName-Attribut.

Wenn in der Identität ein vollqualifiziertes Domänensuffix angegeben wurde, z. B. host/machine.domain.com, durchsucht die Cisco ISE die Gesamtstruktur, in der die Domäne vorhanden ist.

Wenn die Identität die Form eines Hosts oder Computers hat, durchsucht die Cisco ISE alle Gesamtstrukturen nach dem Namen des Dienstprinzips.

Bei mehreren Übereinstimmungen schlägt die Cisco ISE bei der Authentifizierung mit dem Fehler "Ambiguous Identity" (mehrdeutige Identität) fehl.



Anmerkung: Dieselben Filter werden in den Dateien "ISE ad-agent.log"

Anmerkung: ISE 2.2 Patch 4 und vor und 2.3 Patch 1 und vor identifizierten Benutzern mit den Attributen SAM, CN oder beiden. Für die Cisco ISE, Version 2.2, Patch 5 und höher, und Version 2.3, Patch 2 und höher, wird nur das Attribut "sAMAccountName" als Standardattribut verwendet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.