

# Identity Service Engine (ISE) en Active Directory (AD) begrijpen

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[AD-protocollen](#)

[Kerberos-protocol](#)

[MS-RPC-protocol](#)

[ISE-integratie met Active Directory \(AD\)](#)

[Doe mee aan ISE naar AD](#)

[Lid worden van het AD-domein](#)

[AD-domein verlaten](#)

[DC-failover](#)

[ISE-AD-communicatie via LDAP](#)

[Gebruikersverificatie bij AD-flow:](#)

[ISE-zoekfilters](#)

## Inleiding

Dit document beschrijft hoe Identity Service Engine (ISE) en Active Directory (AD) communiceren, gebruikte protocollen, AD-filters en stromen.

## Voorwaarden

### Vereisten

Cisco adviseert een basiskennis van:

- ISE 2.x en Active Directory-integratie.
- Externe identiteitsverificatie op ISE.

### Gebruikte componenten

- ISE 2.x.
- Windows Server (actieve map) .

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# AD-protocollen

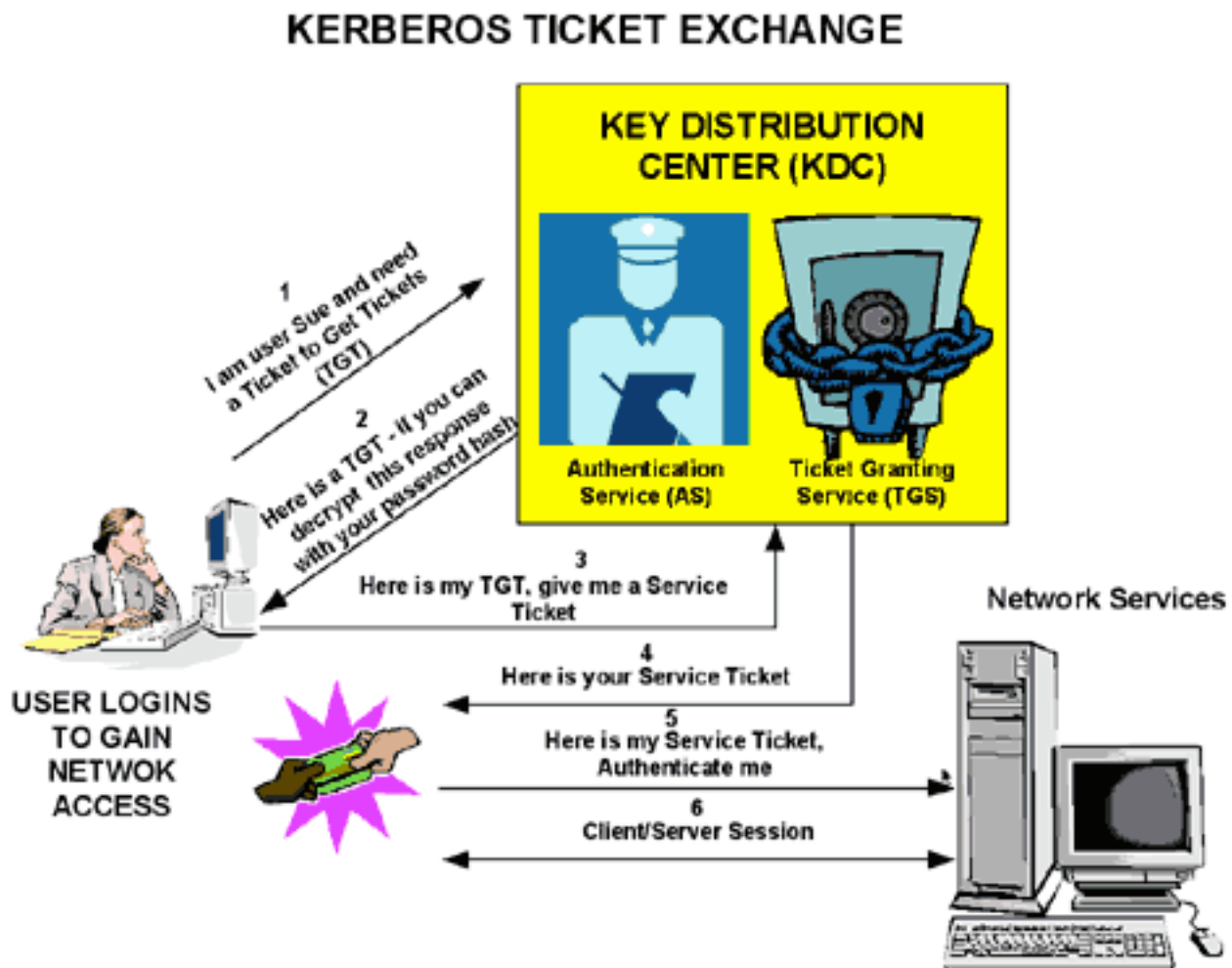
## Kerberos-protocol

De drie koppen van Kerberos bestaan uit het Key Distribution Center (KDC), de clientgebruiker en de server die toegang moet krijgen.

De KDC wordt geïnstalleerd als deel van de Domain Controller (DC) en voert twee servicefuncties uit: de verificatiedienst (AS) en de ticketservice (TGS).

Drie uitwisselingen zijn betrokken wanneer de client in eerste instantie toegang heeft tot een serverbron:

1. AS Exchange.
2. TGS Exchange.
3. Client/Server (UCS) Exchange.



- Domain Controller = KDC (AS + TGS).
- Verifiëren naar AS (het SSO-portal) met uw wachtwoord.
- Ontvang een Ticket Granting Ticket (TGT) (een sessiecookie).
- Meld u aan bij een service (SRV01).
- SRV01 verwijst u naar KDC.
- TGT naar KDC tonen - (ik ben al geverifieerd)

- KDC geeft je TGS voor SRV01.
- Omleiden naar SRV01.
- Toon service ticket naar SRV01.
- SRV01 verifieert/vertrouwt op serviceticket.
- Service ticket heeft al mijn informatie.
- SRV01 logt me in.

Wanneer gebruikers zich voor het eerst aanmelden bij een netwerk, moeten ze onderhandelen over toegang en een inlognaam en wachtwoord opgeven om te worden geverifieerd door het AS-gedeelte van een KDC binnen hun domein.

De KDC heeft toegang tot de informatie van de Active Directory-gebruikersaccount. Na authenticatie krijgt de gebruiker een Ticket Granting Ticket (TGT) dat geldig is voor het lokale domein.

De TGT heeft een standaardlevensduur van 10 uur en wordt tijdens de gebruikersaanmelding vernieuwd zonder dat de gebruiker zijn wachtwoord opnieuw moet invoeren.

De TGT wordt op de lokale machine in vluchtige geheugenruimte gecachet en wordt gebruikt om sessies aan te vragen met diensten door het hele netwerk.

De gebruiker legt de TGT voor aan het TGS-gedeelte van de KDC wanneer toegang tot een serverservice nodig is.

De TGS op de KDC verifieert de gebruiker TGT en maakt een ticket en sessiesleutel voor zowel de client als de externe server. Deze informatie (de service ticket) wordt vervolgens lokaal gecachet op de client machine.

De TGS ontvangt de client TGT en leest deze met een eigen sleutel. Als de TGS het cliëntverzoek goedkeurt, wordt een dienstkaartje geproduceerd voor zowel de cliënt als de doelserver.

De client leest zijn deel met de TGS-sessiesleutel die eerder uit het AS-antwoord is opgehaald.

De client presenteert het servergedeelte van het TGS-antwoord aan de doelserver in de volgende client/server-uitwisseling.

Voorbeeld:

## Test User Authentication

\* Username

\* Password

Authentication Type

Authorization Data  Retrieve Groups  
 Retrieve Attributes

Authentication Result	Groups	Attributes
<pre>Authentication time      : 57 ms. Groups fetching time     : 18 ms. Attributes fetching time : 4 ms.  Processing Steps: 14:05:37:440: Resolving identity - user1 14:05:37:440: Search for matching accounts at join point - ralmaait.com 14:05:37:449: Single matching account found in forest - ralmaait.com 14:05:37:449: Identity resolution detected single matching account 14:05:37:476: Authentication Ticket (TGT) request succeeded - user1@ralmaait.com 14:05:37:478: Service Ticket request succeeded - user1@ralmaait.com 14:05:37:486: Service Ticket validation succeeded - user1@ralmaait.com 14:05:37:486: Account validation succeeded</pre>		

Packet-opnamen van ISE voor een geverifieerde gebruiker:

Time	Source IP	Destination IP	Protocol	Details
111 2020-01-13 16:17:53.082713	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=105462807 TSecr=280789807 ✓
112 2020-01-13 16:17:53.082735	10.48.60.50	10.48.60.51	KRB5	346 AS-REQ ✓
113 2020-01-13 16:17:53.083625	10.48.60.51	10.48.60.50	KRB5	1576 AS-REP ✓
114 2020-01-13 16:17:53.083649	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=2807... ✓
115 2020-01-13 16:17:53.083678	10.48.60.50	10.48.60.51	TCP	66 53610 → 88 [FIN, ACK] Seq=281 Ack=1511 Win=32256 Len=0 TSval=105462808 TSecr=... ✓
116 2020-01-13 16:17:53.083908	10.48.60.51	10.48.60.50	TCP	66 88 → 53610 [ACK] Seq=1511 Ack=282 Win=532726 Len=0 TSval=280789809 TSecr=105... ✓
117 2020-01-13 16:17:53.084022	10.48.60.51	10.48.60.50	TCP	60 88 → 53610 [RST, ACK] Seq=1511 Ack=282 Win=0 Len=0 ✓
118 2020-01-13 16:17:53.084449	10.48.60.50	10.48.60.51	KRB5	1480 TGS-REQ ✓
119 2020-01-13 16:17:53.085475	10.48.60.51	10.48.60.50	KRB5	1446 TGS-REP ✓
120 2020-01-13 16:17:53.110397	10.48.60.50	10.48.60.51	TCP	66 48959 → 3268 [ACK] Seq=1700 Ack=536 Win=31360 Len=0 TSval=105462835 TSecr=28... ✓

De AS-REQ bevat de gebruikersnaam. Als het wachtwoord juist is, biedt de AS-service een TGT die met het gebruikerswachtwoord is versleuteld. De TGT wordt vervolgens aan de TGT-dienst geleverd om een sessieticket te krijgen.

Verificatie is succesvol wanneer een sessieticket is ontvangen.

Dit is een voorbeeld waarbij het wachtwoord gegeven door client onjuist is:

Time	Source IP	Destination IP	Protocol	Details
117 2020-01-14 08:51:03.846603	10.48.60.50	10.48.60.51	KRB5	318 AS-REQ
118 2020-01-14 08:51:03.848340	10.48.60.51	10.48.60.50	KRB5	194 KRB Error: KRB5KDC_ERR_PREAUTH_FAILED

Als het wachtwoord niet goed is, wordt de AS-aanvraag mislukt en wordt geen TGT ontvangen:

Time	Source IP	Destination IP	Protocol	Details
<pre>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</pre>				

Logt het bestand ad\_agent.log in als het wachtwoord onjuist is:

2020-01-14 13:36:05,442 DEBUG,140574072981248,krb5: Verzend verzoek (276 bytes) naar RALMAAIT.COM,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,44 DEBUG,140574072981248,krb5: Ontvangen fout van KDC: -1765328360/Verificatie vooraf mislukt,LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,44 DEBUG,140574072981248,krb5: Probeer nogmaals invoertypen: 16, 14, 19, 2, LwKrb5TraceCallback(),lwadvapi/threaded/lwkrb5.c:1325

2020-01-14 13:36:05,444 WAARSCHUWING,140574072981248,[LwKrb5GetTgtImpl ../lwadvapi/threaded/krbtgt.c:329] KRB5 Foutcode: -1765328360 (Bericht: Verificatie vooraf mislukt), LwTranslateKrb5Error(), lwadvapi/threaded/lwkrb5.c:892

2020-01-14 13:36:05,444 DEBUG,140574072981248,[wKrb5InitializeUserLoginCredentials()] Foutcode: 40022 (symbol: LW\_ERROR\_PASSWORD\_MISMATCH),LWKrb5InitializeUserLoginCredentials(),lwadvapi/thread ed/lwkrb5.c:1453

## MS-RPC-protocol

ISE maakt gebruik van MS-RPC via SMB, SMB biedt de verificatie en vereist geen afzonderlijke sessie om te vinden waar een bepaalde RPC-service zich bevindt. Het maakt gebruik van een mechanisme genaamd "met name pipe" om te communiceren tussen de client en server.

- Maak een SMB-sessieverbinding.
- Transport RPC-berichten via SMB/CIFS.TCP port 445 als een transport
- SMB-sessie identificeert welke poort een bepaalde RPC-service draait en de gebruikersverificatie verwerkt.
- Maak verbinding met verborgen delen IPC\$ voor communicatie tussen processen.
- Open een geschikte benoemde pijp voor de gewenste RPC-bron/functie.

Transformeer de RPC exchange via SMB.

No.	Time	Source	Destination	Protocol	Length	Info	Text Item
59	2020-01-14 14:56:01.082699	10.48.60.50	10.48.60.51	SMB	128	Negotiate Protocol Request	✓
60	2020-01-14 14:56:01.083241	10.48.60.51	10.48.60.50	SMB2	318	Negotiate Protocol Response	✓
61	2020-01-14 14:56:01.083255	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=63 Ack=253 Win=30336 Len=0 TSval=186950807 TSecr=36227...	✓
72	2020-01-14 14:56:01.086109	10.48.60.50	10.48.60.51	SMB2	1589	Session Setup Request	✓
73	2020-01-14 14:56:01.086341	10.48.60.51	10.48.60.50	TCP	66	445 → 26963 [ACK] Seq=253 Ack=1586 Win=66560 Len=0 TSval=362277347 TSecr=186...	✓
74	2020-01-14 14:56:01.087051	10.48.60.51	10.48.60.50	SMB2	328	Session Setup Response	✓
75	2020-01-14 14:56:01.087268	10.48.60.50	10.48.60.51	SMB2	212	Tree Connect Request Tree: \\WIN-E051AB1Q9BK.ralmaait.com\IPC\$	✓
76	2020-01-14 14:56:01.087592	10.48.60.51	10.48.60.50	SMB2	150	Tree Connect Response	✓
77	2020-01-14 14:56:01.087721	10.48.60.50	10.48.60.51	SMB2	206	Create Request File: netlogon	✓
78	2020-01-14 14:56:01.088023	10.48.60.51	10.48.60.50	SMB2	222	Create Response File: netlogon	✓
79	2020-01-14 14:56:01.088207	10.48.60.50	10.48.60.51	DCERPC	314	Bind: call_id: 9, Fragment: Single, 1 context items: RPC_NETLOGON V1.0 (32bi...	✓
80	2020-01-14 14:56:01.088500	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
81	2020-01-14 14:56:01.088665	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
82	2020-01-14 14:56:01.088899	10.48.60.51	10.48.60.50	DCERPC	230	Bind ack: call_id: 9, Fragment: Single, max_xmit: 4280 max_rcv: 4280, 1 res...	✓
83	2020-01-14 14:56:01.089118	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
84	2020-01-14 14:56:01.089373	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓
85	2020-01-14 14:56:01.089517	10.48.60.50	10.48.60.51	SMB2	183	Read Request Len:8192 Off:0 File: netlogon	✓
86	2020-01-14 14:56:01.090160	10.48.60.51	10.48.60.50	RPC_NETLOGON	608	NetLogonSamLogonEx response	✓
88	2020-01-14 14:56:01.129364	10.48.60.50	10.48.60.51	TCP	66	26963 → 445 [ACK] Seq=2862 Ack=1635 Win=34688 Len=0 TSval=186950854 TSecr=36...	✓
145	2020-01-14 14:56:09.910387	10.48.60.50	10.48.60.51	RPC_NETLOGON	574	NetLogonSamLogonEx request	✓
146	2020-01-14 14:56:09.910714	10.48.60.51	10.48.60.50	SMB2	150	Write Response	✓

```
> Secure Channel Verifier
Microsoft Network Logon, NetLogonSamLogonEx
Operation: NetLogonSamLogonEx (39)
[Response in frame: 86]
  LogonServer: \\WIN-E051AB1Q9BK.ralmaait.com
    Referent ID: 0x00000001
    Max Count: 31
    Offset: 0
    Actual Count: 31
    Computer Name: \\WIN-E051AB1Q9BK.ralmaait.com
  Computer Name: ISERIRI24
    Referent ID: 0x00000001
    Max Count: 10
    Offset: 0
    Actual Count: 10
    Computer Name: ISERIRI24
  Level: 2
  LEVEL: LogonLevel
  Level: 2
  NETWORK_INFO:
    Referent ID: 0x00000001
    IDENTITY_INFO: user@ralmaait.com
    Challenge: cdc343b187f9b4e1
```

Het **negotiate protocol request/response** De lijn onderhandelt het dialect van SMB. Het **session setup request/response** voert de verificatie uit.

Tree Connect-verzoek en -antwoord maken verbinding met de gevraagde bron. U bent verbonden met een speciaal gedeelde IPC\$.

Dit interprocescommunicatie-aandeel biedt de communicatiemiddelen tussen hosts en ook als transport voor MSRPC-functies.

Bij pakket 77 **Create Request File** en de bestandsnaam is de naam van de aangesloten service (de netwerkservice in dit voorbeeld).

Bij de pakketten 83 en 86, is het NetlogonSamLogonEX verzoek waar u de gebruikersnaam voor de cliëntauthenticatie op ISE naar de advertentie bij het gebied Network\_INFO verzendt.

Het NetlogonSamLogonEX reactiepakket antwoordt met de resultaten.

Sommige vlaggenwaarden voor de reactie van NetlogonSamLogonEX:

0xc000006a is STATUS\_FOUT\_WACHTWOORD

0x00000000 is STATUS\_SUCCES

0x00000103 is STATUS\_PENDING

## ISE-integratie met Active Directory (AD)

ISE gebruikt LDAP, KRB en MSRBC om te communiceren met AD tijdens het toetreden/verlaten en authenticatieproces.

De volgende secties verstrekken de protocollen, het onderzoeksformaat, en de mechanismen die worden gebruikt om met een specifieke DC op AD en gebruikersauthenticatie tegen dat DC te verbinden.

In het geval dat de DC om welke reden dan ook offline wordt, gaat ISE over naar de volgende beschikbare DC en wordt het authenticatieproces niet beïnvloed.

Een Global Catalog Server (GC) is een domeincontroller die kopieën van alle Active Directory-objecten in het bos opslaat.

Het slaat een volledige kopie van alle objecten op in de map van uw domein en een gedeeltelijke kopie van alle objecten van alle andere bosdomeinen.

De Global Catalog stelt gebruikers en applicaties in staat om objecten te vinden in elk domein van het huidige bos met een zoektocht naar attributen opgenomen in GC.

De Global Catalog bevat een basis (maar onvolledige) reeks attributen voor elk bosobject in elk domein (Partial Attribute Set, PAT).

De GC ontvangt gegevens van alle domeindirectory partities in het bos. Ze worden gekopieerd met de standaard AD replicatieservice.

## Doe mee aan ISE naar AD

### Voorwaarden voor Active Directory en ISE-integratie

1. Controleer of u de rechten van een Super Admin of System Admin in ISE hebt.
2. Gebruik de NTP-serverinstellingen (Network Time Protocol) om de tijd tussen de Cisco-server en Active Directory te synchroniseren. Het maximaal toegestane tijdsverschil tussen ISE en AD bedraagt 5 minuten
3. De geconfigureerde DNS op ISE moet in staat zijn SRV-vragen voor DC's, GC's en KDC's te beantwoorden met of zonder aanvullende siteinformatie.
4. Zorg ervoor dat alle DNS-servers voorwaartse en omgekeerde DNS-vragen kunnen beantwoorden voor elk mogelijk Active Directory DNS-domein.
5. AD moet minimaal één wereldwijde catalogusserver operationeel en toegankelijk zijn voor Cisco, in het domein waartoe u zich bij Cisco aansluit.

### Lid worden van het AD-domein

ISE past Domain Discovery toe om informatie te verkrijgen over het Joed-domein in drie fasen:

1. Queries sloot zich aan bij domeinen - ontdekt domeinen uit het bos en domeinen die extern worden vertrouwd op het aangesloten domein.
2. Vraagt worteldomeinen in zijn bos-Vestigt vertrouwen met het bos.
3. Vraagt worteldomeinen in vertrouwde bossen-ontdekt domeinen van de vertrouwde bossen.

Daarnaast detecteert Cisco ISE DNS-domeinnamen (UPN-achtervoegsels), alternatieve UPN-achtervoegsels en NTLM-domeinnamen.

ISE past een DC-detectie toe om alle informatie over de beschikbare DC's en GC's te krijgen.

1. Het proces wordt gestart met de invoerreferenties van super admin op AD die in het domein zelf bestaan. Als het in een ander domein of subdomein bestaat, moet de gebruikersnaam worden genoteerd in een UPN-notatie (username@domain).
2. ISE stuurt een DNS-query voor alle DC's, GC's en KDC's-records. Als het DNS-antwoord niet een van hen in zijn antwoord had dan mislukt de integratie met DNS-gerelateerde fout.
3. ISE gebruikt de CLDAP ping om alle DC's en GC's te ontdekken via verzonden CLDAP-verzoeken aan de DC's die overeenkomen met hun prioriteiten in de SRV-record. De eerste DC-respons wordt gebruikt en ISE wordt vervolgens aangesloten op die DC.

Een factor die wordt gebruikt om de DC-prioriteit te berekenen is de tijd die de DC neemt om te reageren op CLDAP pings; een snellere reactie krijgt een hogere prioriteit.

**Opmerking:** CLDAP is het mechanisme dat ISE gebruikt om connectiviteit met de DC's vast te stellen en te handhaven. Het meet de reactietijd tot het eerste DC antwoord. Het mislukt als je geen antwoord van DC ziet. Waarschuwen als de responstijd groter is dan 2,5 seconden. CLDAP pingt alle DC's in de site (als er geen site is, alle DC's in het domein). De CLDAP-respons bevat DC-site en clientsite (de site waaraan ISE-machine is toegewezen).

4. ISE ontvangt dan TGT met 'word lid van gebruiker' referenties.
5. Genereert de naam van de ISE-machinerekening met MSRPC. (SAM en SPN)
6. Zoek AD op SPN als ISE machine account al bestaat. Als de machine van ISE niet bestaat,

leidt ISE tot nieuwe.

7. Open Machine-account, stel het wachtwoord van de ISE-machine-account in en controleer of de ISE-machine-account toegankelijk is.
8. Stel ISE-machineaccounteigenschappen in (SPN, dnsHostname en dergelijke).
9. Krijg TGT met ISE machine referenties met KRB5 en ontdek alle vertrouwde domeinen.
10. Wanneer de koppeling is voltooid, werkt de ISE-knooppunt de AD-groepen en de bijbehorende SIDS bij en start automatisch het SID-updateproces. Controleer of dit proces bij AD kan worden voltooid.

## AD-domein verlaten

Wanneer ISE vertrekt, moet de AD rekening houden met:

1. Gebruik een volledige AD admin gebruiker om de verlofprocessen uit te voeren. Hiermee wordt gecontroleerd of de ISE-machinerekening uit de Active Directory-database is verwijderd.
2. Als de AD zonder referenties werd achtergelaten, dan wordt de ISE-account niet verwijderd uit de AD en moet deze handmatig worden verwijderd.
3. Wanneer u de ISE-configuratie van de CLI opnieuw instelt of de configuratie na een back-up of upgrade terugzet, wordt een verlofbewerking uitgevoerd en wordt de ISE-knooppunt losgekoppeld van het Active Directory-domein. (bij aansluiting). De ISE-knooppunt wordt echter niet verwijderd uit het Active Directory-domein.
4. Het wordt aanbevolen om een verlofhandeling uit te voeren vanuit het Admin portal met de Active Directory-referenties, omdat het ook de node-account verwijdert uit het Active Directory-domein. Dit wordt ook aanbevolen wanneer u de ISE hostnaam wijzigt.

## DC-failover

Wanneer de DC verbonden met ISE offline of onbereikbaar wordt om welke reden dan ook, wordt DC failover automatisch geactiveerd op ISE. DC failover kan worden geactiveerd door de volgende omstandigheden:

1. De AD-connector detecteert dat de momenteel geselecteerde DC niet beschikbaar is gekomen tijdens een of andere communicatiepoging van CLDAP, LDAP, RPC of Kerberos. In dergelijke gevallen start de AD-connector de DC-selectie op en wordt deze overgeslagen naar de nieuw geselecteerde DC.
2. DC is omhoog en reageert op CLDAP ping, maar AD Connector kan niet met het communiceren om de een of andere reden (voorbeelden: RPC-poort is geblokkeerd, DC bevindt zich in status 'verbroken replicatie', DC is niet correct buiten bedrijf gesteld).

In dergelijke gevallen start de AD-connector DC-selectie met een geblokkeerde lijst ("slechte" DC wordt in de geblokkeerde lijst geplaatst) en probeert hij te communiceren met de geselecteerde DC. DC die in de geblokkeerde lijst is geselecteerd, wordt niet gecached.

De AD-connector moet de failover binnen een redelijke tijd voltooien (of falen als dit niet mogelijk is). Om deze reden probeert de AD-connector een beperkt aantal DC's tijdens failover.

ISE blokkeert AD Domain Controllers als er een onherstelbare netwerk- of serverfout is om te voorkomen dat ISE een slechte DC gebruikt. DC wordt niet toegevoegd aan de geblokkeerde lijst als deze niet reageert op CLDAP pings. ISE verlaagt alleen de prioriteit van de DC die niet



reageert.

## ISE-AD-communicatie via LDAP

ISE zoekt naar machine of gebruiker in AD met een van deze zoekformaten. Als u naar een machine zocht, voegt ISE "\$" toe aan het einde van de naam van de machine. Dit is een lijst van identiteitstypen die wordt gebruikt om een gebruiker in AD te identificeren:

- Naam SAM: Gebruikersnaam of machinenaam zonder domeinopmaak, dit is de Gebruikersloginnaam in AD. **Voorbeeld: sajeda of sajeda\$**
- GN: is de naam van de gebruikersweergave op AD, deze mag niet gelijk zijn aan de SAM. **Voorbeeld: Sajeda Ahmed.**
- Hoofdnaam gebruiker (UPN): is een combinatie van de SAM-naam en de domeinnaam (SAM\_NAME@domain). **Voorbeeld: [sajeda@cisco.com](mailto:sajeda@cisco.com) of sajeda\$cisco.com**
- Alternatief UPN: is een extra / alternatieve UPN-achtervoegsels die in de AD zijn geconfigureerd behalve de domeinnaam. Deze configuratie wordt globaal toegevoegd in de advertentie (niet per gebruiker geconfigureerd) en het is niet nodig om een echte domeinnaam achtervoegsel te zijn.

Elke AD kan meerdere UPN-achtervoegsels hebben (@alt1.com,@alt2.com,..., etc). **Voorbeeld: belangrijkste UPN ([sajeda@cisco.com](mailto:sajeda@cisco.com)), alternatief UPN:sajeda@domain1 , sajeda@domain2**

- NetBIOS voorgefixeerde naam: is de domeinnaam\gebruikersnaam van de machine. **Voorbeeld: CISCO\SAJEDA of CISCO\MACHINE\$**
- Host/prefix met ongeschikte machine: Dit wordt gebruikt voor machineverificatie wanneer alleen de machinenaam wordt gebruikt, dit is alleen de host-/machinenaam. **Voorbeeld: host/machine**
- Host/prefix met volledig gekwalificeerde machine: dit wordt gebruikt voor machinechtheidscontrole wanneer de machine FQDN wordt gebruikt, gewoonlijk in het geval van certificaatauthenticatie, is het host/FQDN van de machine. **Voorbeeld: host/machine.cisco.com**
- SPN-naam: De naam waardoor een client een uniek geval van een service identificeert (voorbeelden: HTTP, LDAP, SSH), alleen gebruikt voor Machine.

## Gebruikersverificatie bij AD-flow:

1. Identiteit oplossen en identiteitstype bepalen - SAM, UPN, SPN. Als ISE de identiteit alleen als gebruikersnaam ontvangt, zoekt het naar een gekoppeld SAM-account in de AD. Als ISE de identiteit ontvangt als username@domain, dan zoekt het naar een overeenkomende UPN of mail in de AD. in beide scenario's gebruikt ISE extra filters voor machine of gebruikersnaam.
2. Zoeken naar domein of bos (afhankelijk van identiteitstype)
3. Informatie over alle gekoppelde accounts behouden (JP, DN, UPN, domein)
4. Als er geen gekoppelde account wordt gevonden, is de AD-antwoorden met de gebruiker

onbekend.

5. Voer MS-RPC (of Kerberos) verificatie uit voor elke gekoppelde account
6. Als slechts één account overeenkomt met de invoeridentiteit en het wachtwoord, dan is de verificatie geslaagd
7. Als meerdere accounts overeenkomen met de inkomende identiteit, gebruikt ISE het wachtwoord om de ambiguïteit op te lossen, zodat de account met een gekoppeld wachtwoord wordt geverifieerd en de andere accounts de onjuiste wachtwoordteller met 1 verhogen.
8. Als er geen account met de inkomende identiteit en het wachtwoord overeenkomt, antwoordt AD met het verkeerde wachtwoord.

## ISE Zoekfilters

Filters worden gebruikt om een entiteit te identificeren die met AD wil communiceren. ISE zoekt altijd naar die entiteit in de gebruikers- en machinegroepen.

Voorbeelden van zoekfilters:

1. **Zoeken op SAM:** Als ISE een identiteit als gebruikersnaam ontvangt zonder enige domeinmarkering, dan behandelt ISE deze gebruikersnaam als een SAM en zoekt in AD naar alle machinegebruikers of machines die die identiteit als een SAM naam hebben.

Als de SAM-naam niet uniek is, gebruikt ISE het wachtwoord om onderscheid te maken tussen gebruikers en wordt ISE geconfigureerd om een wachtwoordloos protocol te gebruiken zoals EAP-TLS.

Er zijn geen andere criteria om de juiste gebruiker te vinden, dus ISE mislukt de authenticatie met een "Ambiguous Identity" fout.

Als het gebruikerscertificaat echter in Active Directory aanwezig is, gebruikt Cisco ISE binaire vergelijking om de identiteit op te lossen.

```
> Frame 219: 295 bytes on wire (2360 bits), 295 bytes captured (2360 bits)
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1430, Ack: 213, Len: 229
v Lightweight Directory Access Protocol
  SASL Buffer Length: 225
  v SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
    v GSS-API payload (197 bytes)
      v LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
        messageID: 2
        v protocolOp: searchRequest (3)
          v searchRequest
            baseObject: dc=aaalab,dc=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            v filter: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
              v filter: and (0)
                v and: (&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
                  v and: 2 items
                    v Filter: (|(objectCategory=person)(objectCategory=computer))
                      v and item: or (1)
                        > or: (|(objectCategory=person)(objectCategory=computer))
                    v Filter: (sAMAccountName=anos)
                      v and item: equalityMatch (3)
                        v equalityMatch
                          attributeDesc: sAMAccountName
                          assertionValue: anos
              v attributes: 4 items
                AttributeDescription: sAMAccountName
                AttributeDescription: userPrincipalName
                AttributeDescription: objectCategory
                AttributeDescription: userAccountControl
```

## 2. Zoeken op UPN of MAIL: Als ISE een identiteit als username@domain ontvangt, zoekt ISE elk bosplatform naar een overeenkomst met die UPN-identiteit of Mail-identiteit "identified UPN of email".

Als er een unieke overeenkomst is, gaat Cisco ISE over op de AAA-stroom.

Als er meerdere samengevoegde punten zijn met hetzelfde UPN en een wachtwoord of dezelfde UPN en Mail, mislukt Cisco ISE de verificatie met een fout in "Ambiguous Identity".

```

461 2020-01-20 16:33:58.134338 10.48.60.206 10.48.60.101 LDAP 336 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree ✓
464 2020-01-20 16:33:58.137942 10.48.60.101 10.48.60.206 LDAP 384 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
471 2020-01-20 16:33:58.170678 10.48.60.206 10.48.60.101 LDAP 179 SASL GSS-API Integrity: searchRequest(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
472 2020-01-20 16:33:58.172663 10.48.60.101 10.48.60.206 LDAP 1413 SASL GSS-API Integrity: searchResEntry(6) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
476 2020-01-20 16:33:58.174754 10.48.60.206 10.48.60.101 LDAP 189 SASL GSS-API Integrity: searchRequest(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
479 2020-01-20 16:33:58.175528 10.48.60.101 10.48.60.206 LDAP 255 SASL GSS-API Integrity: searchResEntry(7) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
480 2020-01-20 16:33:58.176236 10.48.60.206 10.48.60.101 LDAP 241 SASL GSS-API Integrity: searchRequest(8) "dc=aaalab,dc=com" wholeSubtree ✓
481 2020-01-20 16:33:58.177307 10.48.60.101 10.48.60.206 LDAP 635 SASL GSS-API Integrity: searchResEntry(8) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
484 2020-01-20 16:33:58.178414 10.48.60.206 10.48.60.101 LDAP 271 SASL GSS-API Integrity: searchRequest(9) "dc=aaalab,dc=com" wholeSubtree ✓

> Frame 461: 336 bytes on wire (2688 bits), 336 bytes captured (2688 bits)
> Ethernet II, Src: Vmware_b6:ed:17 (00:50:56:b6:ed:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
> Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
> Transmission Control Protocol, Src Port: 19997, Dst Port: 3268, Seq: 1659, Ack: 531, Len: 270
> Lightweight Directory Access Protocol
  SASL Buffer Length: 266
  SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
    > GSS-API payload (238 bytes)
      LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
        messageID: 3
        protocolOp: searchRequest(3)
          searchRequest
            baseObject: dc=aaalab,dc=com
            scope: wholeSubtree (2)
            derefAliases: neverDerefAliases (0)
            sizeLimit: 0
            timeLimit: 0
            typesOnly: False
            Filter: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
            filter: and (0)
              and: (&((objectCategory=person)(objectCategory=computer))((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com)))
                and: 2 items
                  Filter: ((objectCategory=person)(objectCategory=computer))
                    and item: or (1)
                      or: ((objectCategory=person)(objectCategory=computer))
                  Filter: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))
                    and item: or (1)
                      or: ((userPrincipalName=anos@aaalab.com)(mail=anos@aaalab.com))

```

## 3. NetBIOS-zoekopdracht: Als ISE een identiteit ontvangt met een NetBIOS-prefix (bijvoorbeeld Cisco\sajedah), zoekt ISE in de bossen naar het NetBIOS-domein. Eenmaal gevonden zoekt het de meegeleverde SAM naam (sajeda in ons voorbeeld)

```

654 2020-01-20 17:06:29.243747 10.48.60.206 10.48.60.101 LDAP 295 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree ✓
655 2020-01-20 17:06:29.245154 10.48.60.101 10.48.60.206 LDAP 682 SASL GSS-API Integrity: searchResEntry(2) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
684 2020-01-20 17:06:29.290383 10.48.60.206 10.48.60.101 LDAP 179 SASL GSS-API Integrity: searchRequest(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
685 2020-01-20 17:06:29.292939 10.48.60.101 10.48.60.206 LDAP 1413 SASL GSS-API Integrity: searchResEntry(3) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
687 2020-01-20 17:06:29.294515 10.48.60.206 10.48.60.101 LDAP 189 SASL GSS-API Integrity: searchRequest(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
688 2020-01-20 17:06:29.295469 10.48.60.101 10.48.60.206 LDAP 255 SASL GSS-API Integrity: searchResEntry(4) "CN=anas Jehad,CN=Users,DC=aaalab,DC=..." ✓
689 2020-01-20 17:06:29.296186 10.48.60.206 10.48.60.101 LDAP 241 SASL GSS-API Integrity: searchRequest(5) "dc=aaalab,dc=com" wholeSubtree ✓
692 2020-01-20 17:06:29.297557 10.48.60.101 10.48.60.206 LDAP 635 SASL GSS-API Integrity: searchResEntry(5) "CN=Users,CN=Builtin,DC=aaalab,DC=..." ✓
693 2020-01-20 17:06:29.298761 10.48.60.206 10.48.60.101 LDAP 271 SASL GSS-API Integrity: searchRequest(6) "dc=aaalab,dc=com" wholeSubtree ✓
694 2020-01-20 17:06:29.299690 10.48.60.101 10.48.60.206 LDAP 690 SASL GSS-API Integrity: searchResEntry(6) "CN=Domain Users,CN=Users,DC=aaalab,DC=..." ✓

> SASL Buffer
  > GSS-API Generic Security Service Application Program Interface
  > GSS-API payload (197 bytes)
    LDAPMessage searchRequest(2) "dc=aaalab,dc=com" wholeSubtree
      messageID: 2
      protocolOp: searchRequest(3)
        searchRequest
          baseObject: dc=aaalab,dc=com
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
          Filter: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
          filter: and (0)
            and: (&((objectCategory=person)(objectCategory=computer))(sAMAccountName=anos))
              and: 2 items
                Filter: ((objectCategory=person)(objectCategory=computer))
                  and item: or (1)
                    or: ((objectCategory=person)(objectCategory=computer))
                Filter: (sAMAccountName=anos)
                  and item: equalityMatch (3)
                    equalityMatch

```

## 4. Zoeken op basis machine: Als ISE een machine-authenticatie ontvangt, met een host/prefix-identiteit, dan zoekt ISE in het bos naar een bijpassende servicePrincipalName-kenmerk.

Als een volledig-gekwificeerd domeinachtervoegsel in de identiteit werd gespecificeerd, bijvoorbeeld host/machine.domain.com, zoekt Cisco ISE in het bos waar dat domein bestaat.

Als de identiteit de vorm heeft van een host/machine, zoekt Cisco ISE alle bossen naar de naam van het onderhoudspersoneel.

Als er meer dan één overeenkomst is, faalt Cisco ISE-verificatie met een fout in "dubbelzinnige identiteit".

2744	2020-01-20	16:35:32.108699	10.48.60.206	10.48.60.101	LDAP	373 SASL GSS-API Integrity: searchRequest(3) "dc=aaalab,dc=com" wholeSubtree	✓
2745	2020-01-20	16:35:32.109744	10.48.60.101	10.48.60.206	LDAP	393 SASL GSS-API Integrity: searchResEntry(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com"	✓
2747	2020-01-20	16:35:32.109951	10.48.60.206	10.48.60.101	LDAP	185 SASL GSS-API Integrity: unbindRequest(7)	✓
2757	2020-01-20	16:35:32.114862	10.48.60.206	10.48.60.101	LDAP	1495 bindRequest(1) "<ROOT>" sasl	✓
2758	2020-01-20	16:35:32.115898	10.48.60.101	10.48.60.206	LDAP	278 bindResponse(1) success	✓
2760	2020-01-20	16:35:32.116176	10.48.60.206	10.48.60.101	LDAP	348 SASL GSS-API Integrity: searchRequest(2) "dc=aaalab,dc=com" wholeSubtree	✓
2761	2020-01-20	16:35:32.116855	10.48.60.101	10.48.60.206	LDAP	740 SASL GSS-API Integrity: searchResEntry(2) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com"	✓
2762	2020-01-20	16:35:32.145535	10.48.60.206	10.48.60.101	LDAP	179 SASL GSS-API Integrity: searchRequest(3) "CN=ISE24P,CN=Computers,DC=aaalab,DC=aaalab,DC=com"	✓

```
Ethernet II, Src: Vmware_b6:red:17 (00:50:56:b6:red:17), Dst: Vmware_d5:6a:7d (00:0c:29:d5:6a:7d)
Internet Protocol Version 4, Src: 10.48.60.206, Dst: 10.48.60.101
Transmission Control Protocol, Src Port: 28889, Dst Port: 3268, Seq: 1746, Ack: 267, Len: 307
Lightweight Directory Access Protocol
  SASL Buffer Length: 303
  SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
    > GSS-API payload (275 bytes)
    > LDAPMessage searchRequest(3) "dc=aaalab,dc=com" wholeSubtree
      messageID: 3
      > protocolOp: searchRequest (3)
        > searchRequest
          baseObject: dc=aaalab,dc=com
          scope: wholeSubtree (2)
          derefAliases: neverDerefAliases (0)
          sizeLimit: 0
          timeLimit: 0
          typesOnly: False
          > Filter: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=ise24p$)
            > filter: and (0)
              > and: (&(|(objectCategory=person)(objectCategory=computer)))(sAMAccountName=ise24p$)
                > and: 2 items
                  > Filter: (|(objectCategory=person)(objectCategory=computer))
                    > and item: or (1)
                      > or: (|(objectCategory=person)(objectCategory=computer))
                        > Filter: (sAMAccountName=ise24p$)
                          > and item: equalityMatch (3)
                            > equalityMatch
                              attributeDesc: sAMAccountName
                              assertionValue: ise24p$
```

**Opmerking:** Dezelfde filters zijn te zien in ISE ad-agent.log-bestanden

**Opmerking:** ISE 2.2 patch 4 en Prior en 2.3 patch 1 en eerdere geïdentificeerde gebruikers met de kenmerken SAM, CN, of beide. Cisco ISE, release 2.2 Patch 5 en hoger, en 2.3 Patch 2 en hoger, gebruiken alleen het kenmerk AccountName als het standaardkenmerk.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.