Geïntegreerde AD voor ISE GUI en CLI-aanmelding

Inhoud

Inleiding

Dit document beschrijft de configuratie van Microsoft AD als externe identiteitsopslag voor administratieve toegang tot de Cisco ISE-beheerGUI en CLI.

Voorwaarden

Cisco raadt kennis van deze onderwerpen aan:

- Configuratie van Cisco ISE versie 3.0
- Microsoft AD

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.0
- Windows Server 2016

Dit document beschrijft de configuratie van Microsoft **Active Directory (AD)** als extern identiteitsarchief voor administratieve toegang tot Cisco **Identity Services Engine (ISE)** beheer-GUI en CLI.

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.

Configureren

Gebruik deze sectie om het gebruik van Microsoft AD als extern identiteitsarchief voor administratieve toegang tot de Cisco ISE-beheerGUI te configureren.

Deze poorten worden gebruikt tussen ISE-knooppunt en AD voor deze communicatie:

Service	Port	Protocol	Notes
DNS	53	UDP and TCP	
LDAP	389	UDP and TCP	
Kerberos	88	UDP and TCP	
Kerberos	464	UDP and TCP	Used by kadmin for setting and changing a password
LDAP Global Catalog	3268	TCP	If the `id_provider = ad` option is being used
NTP	123	UDP	Optional

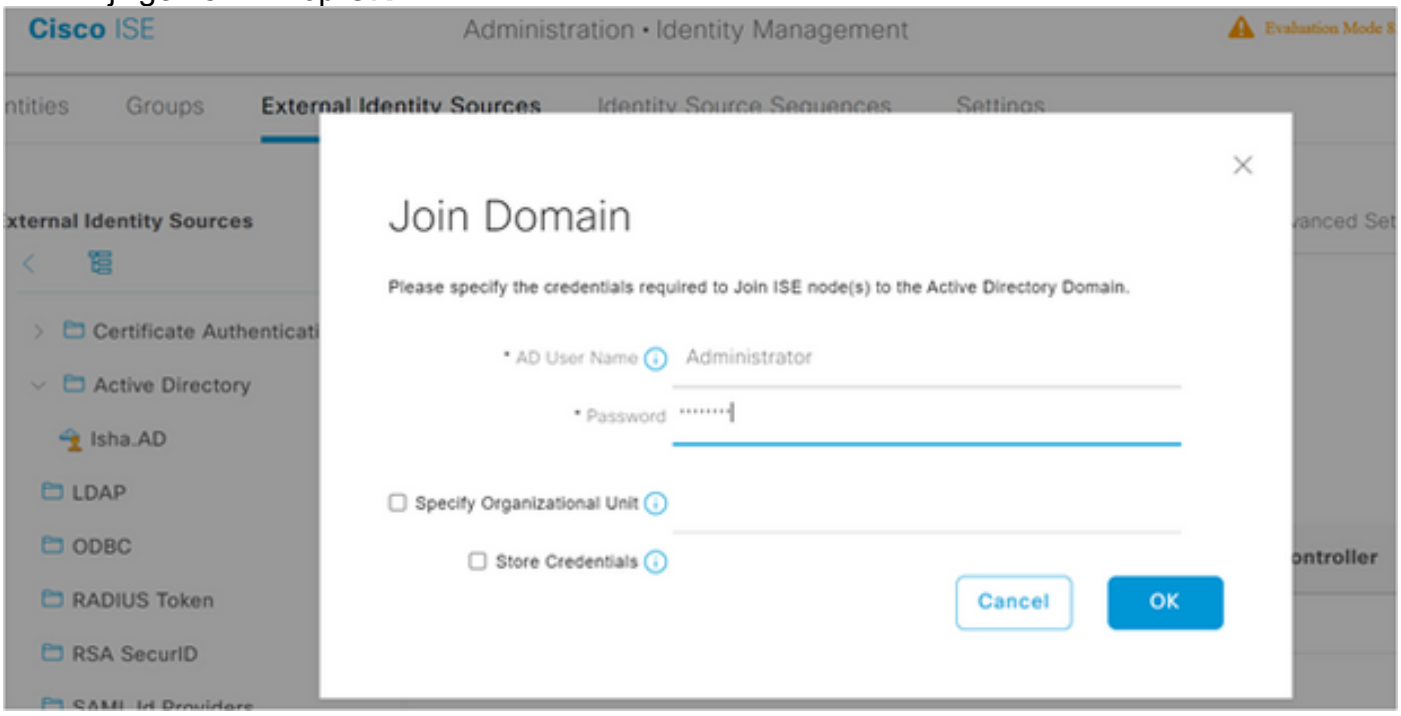
Opmerking: zorg ervoor dat de AD-account alle vereiste rechten heeft.

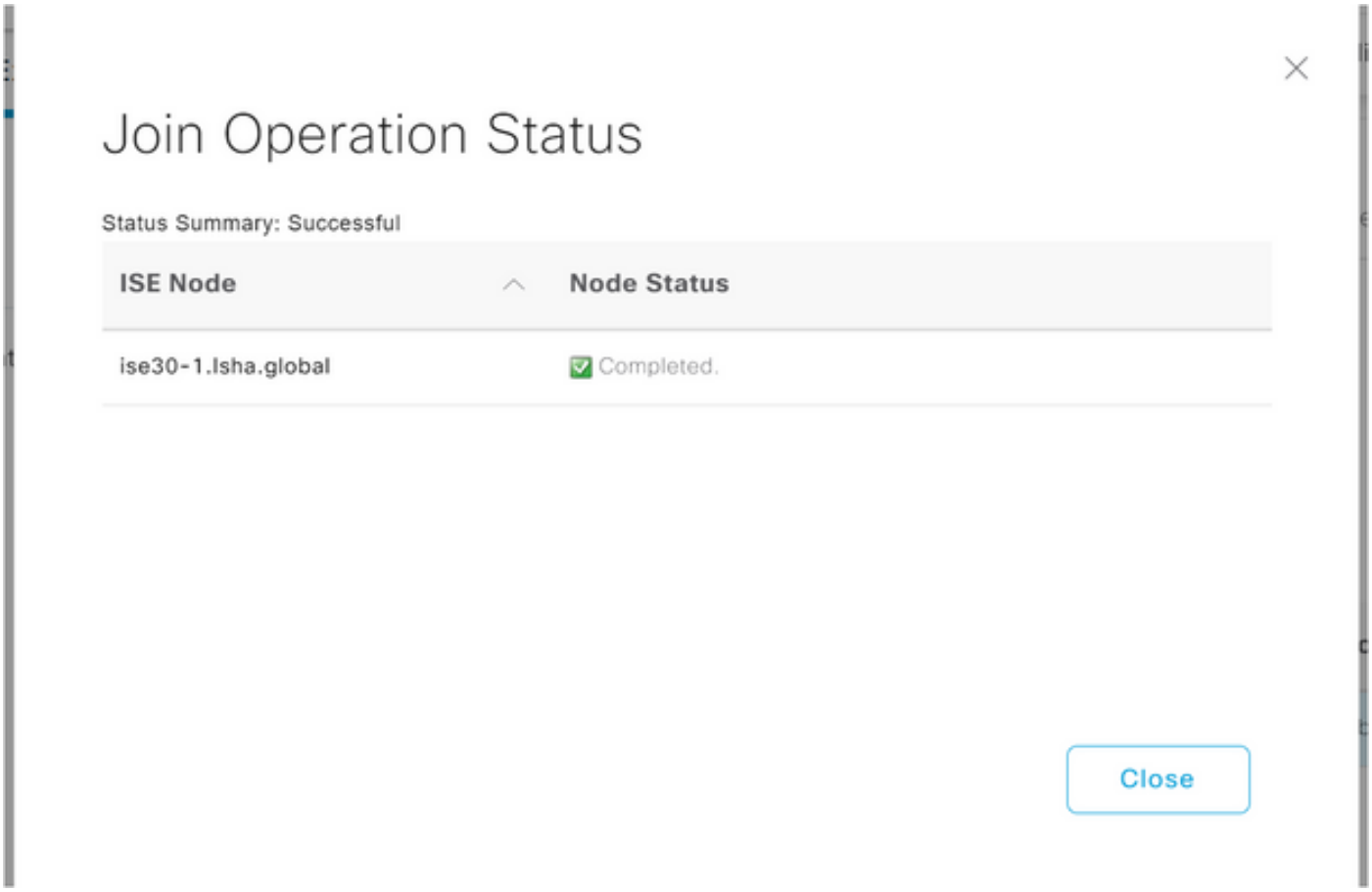
Active Directory Account Permissions Required for Performing Various Operations

Join Operations	Leave Operations	Cisco ISE Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: • Search Active Directory (to see if a Cisco ISE machine account already exists) • Create Cisco ISE machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname) It is not mandatory to be a domain administrator to perform a join operation.	For the account that is used to perform the leave operation, the following permissions are required: • Search Active Directory (to see if a Cisco ISE machine account already exists) • Remove Cisco ISE machine account from domain If you perform a force leave (leave without the password), it will not remove the machine account from the domain.	For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required: • Ability to change own password • Read the user/machine objects corresponding to users/machines being authenticated • Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) • Ability to read tokenGroups attribute You can precreate the machine account in Active Directory, and if the SAM name matches the Cisco ISE appliance hostname, it should be located during the join operation and re-used. If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.

Meld u aan bij ISE-to-AD

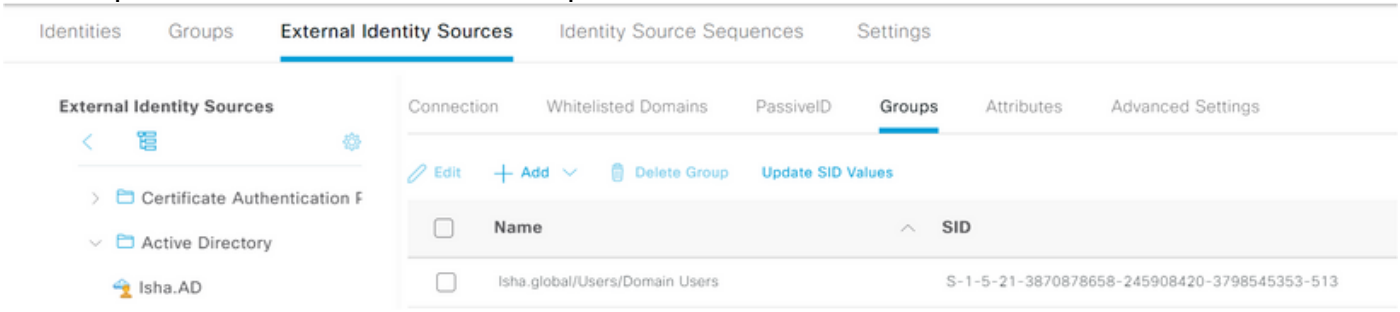
1. Naar navigeren **Administration > Identity Management > External Identity Sources > Active Directory** .
2. Voer de nieuwe naam van het toetredingspunt en het AD-domein in.
3. Voer de referenties in van de AD-account waarmee u computerobjecten kunt toevoegen en wijzigen en klik op **OK**.





Directory-groepen selecteren

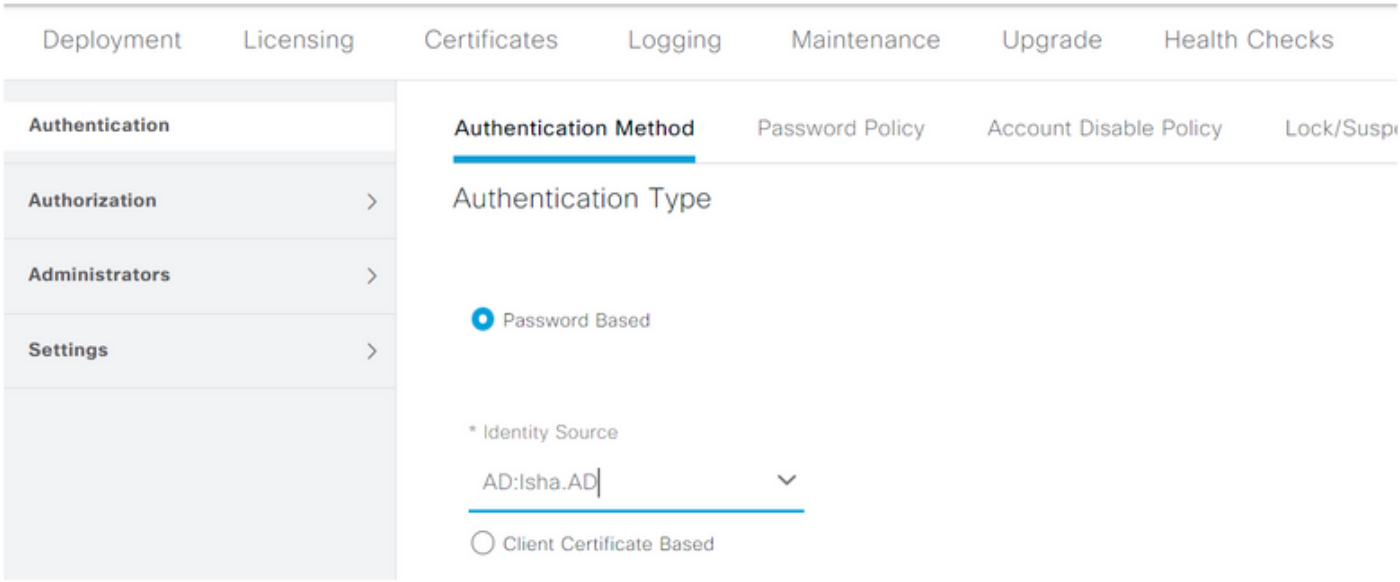
1. Naar navigeren **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. Importeer ten minste één AD Group waartoe uw beheerder behoort.



Administratieve toegang voor AD inschakelen

Voltooi deze stappen om wachtwoordgebaseerde verificatie voor AD in te schakelen:

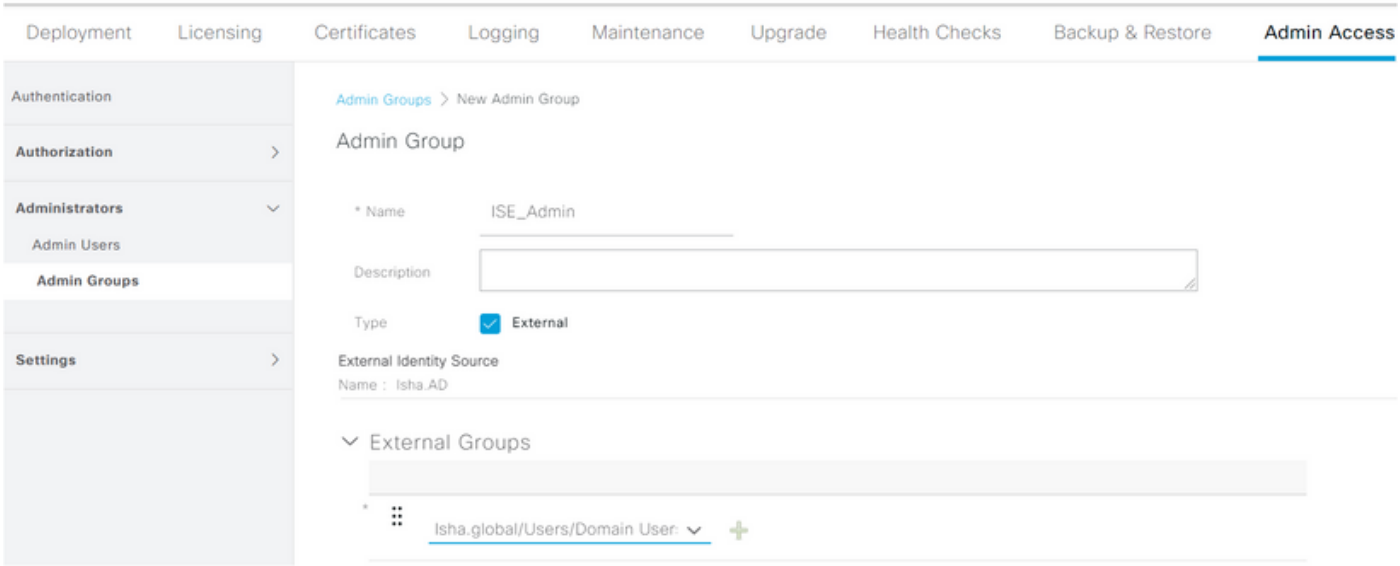
1. Naar navigeren **Administration > System > Admin Access > Authentication** .
2. Van de **Authentication Method** tabblad kiest u de **Password Based** optie.
3. Selecteer **AD** in het veld **Identity Source** (Functie).
4. Klik **Save Changes** .



De beheergroep configureren voor toewijzing van AD-groepen

Een Cisco ISE-lijnkaart definiëren **Admin Group** en in kaart te brengen aan een AD-groep. Dit maakt het mogelijk om de **Role Based Access Control (RBAC)** toestemmingen voor de beheerder op basis van groepslidmaatschap in AD.

1. Naar navigeren **Administration > System > Admin Access > Administrators > Admin Groups** .
2. Klik **Add** in de kop van de tabel om de nieuwe **Admin Group** configuratievenster.
3. Voer de naam in voor de nieuwe Admin-groep.
4. In het **Type** veld controleert u het **External** vink het vakje aan.
5. Van de **External Groups** Kies de AD-groep waaraan u deze Admin-groep wilt toewijzen, zoals gedefinieerd in de **Select Directory Groups** doorsnede.
6. Klik **Save Changes** .

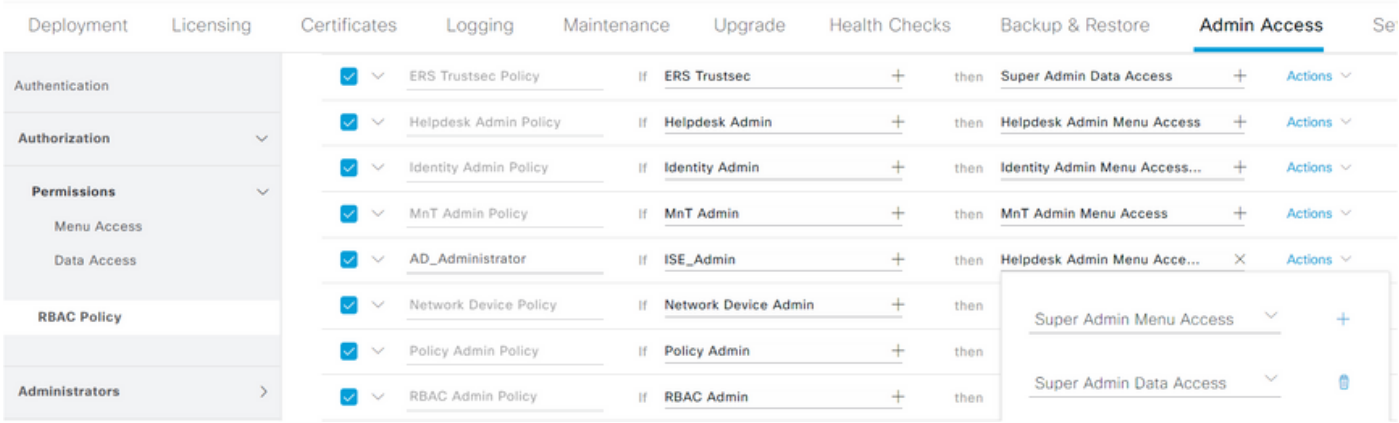


RBAC-toegangsrechten instellen voor de Admin-groep

Voltooi deze stappen om RBAC-rechten toe te wijzen aan de Admin-groepen die in de vorige sectie zijn gemaakt:

1. Naar navigeren **Administration > System > Admin Access > Authorization > Policy** .

2. Van de **Actions** vervolgkeuzelijst aan de rechterkant, kies **Insert New Policy** een nieuw beleid toevoegen.
3. Maak een nieuwe regel met de naam **AD_Administrator** , wijst u deze toe aan de Admin Group die is gedefinieerd in de **Enable Administrative Access** voor AD sectie, en toewijzen het toestemmingen. **Opmerking**: in dit voorbeeld wordt de Admin Group **Super Admin** toegewezen, wat overeenkomt met de standaard admin-account.
4. Klik **Save Changes** . De bevestiging van de opgeslagen wijzigingen wordt weergegeven in de rechterbenedenhoek van de GUI.

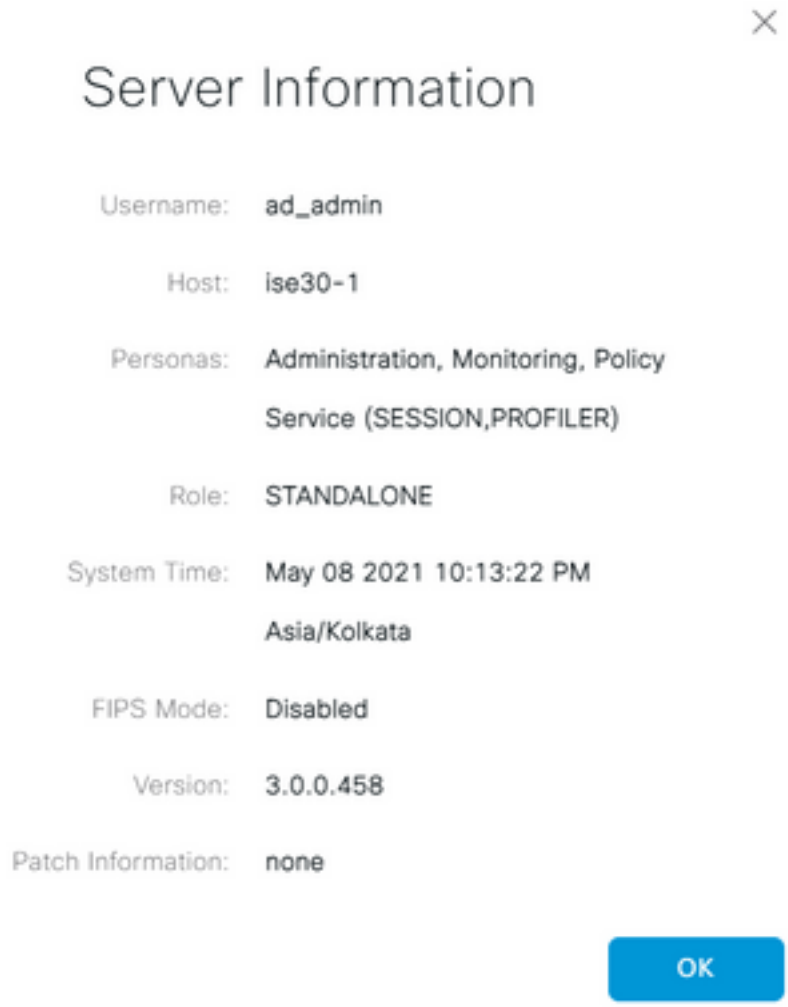


ISE GUI-toegang met AD-referenties

Voltooi de volgende stappen om toegang te krijgen tot de ISE GUI met AD-referenties:

1. Uitloggen op de administratieve GUI.
2. Selecteer **AD** in het veld **Identity Source** (Functie).
3. Voer de gebruikersnaam en het wachtwoord in uit de AD-database en log in.

Opmerking: ISE-standaardwaarden voor de interne gebruikersopslag als AD onbereikbaar is of de gebruikte accountreferenties niet in AD bestaan. Dit vergemakkelijkt snel inloggen als u de interne winkel gebruikt terwijl AD is geconfigureerd voor beheertoegang.



ISE-CLI-toegang met AD-referenties

Verificatie met een externe identiteitsbron is veiliger dan met de interne database. RBAC voor **CLI Administrators** ondersteunt een extern identiteitsarchief.

> **Opmerking**: ISE versie 2.6 en hoger ondersteunt verificatie van CLI-beheerders door externe identiteitsbronnen, zoals AD.

Beheer één bron voor wachtwoorden zonder dat u meerdere wachtwoordbeleidsregels hoeft te beheren en interne gebruikers binnen ISE dient te beheren, wat resulteert in minder tijd en moeite.

Voorwaarden

U moet de Admin-gebruiker gedefinieerd hebben en deze toegevoegd hebben aan een beheerdersgroep. De beheerder moet een **Super Admin** .

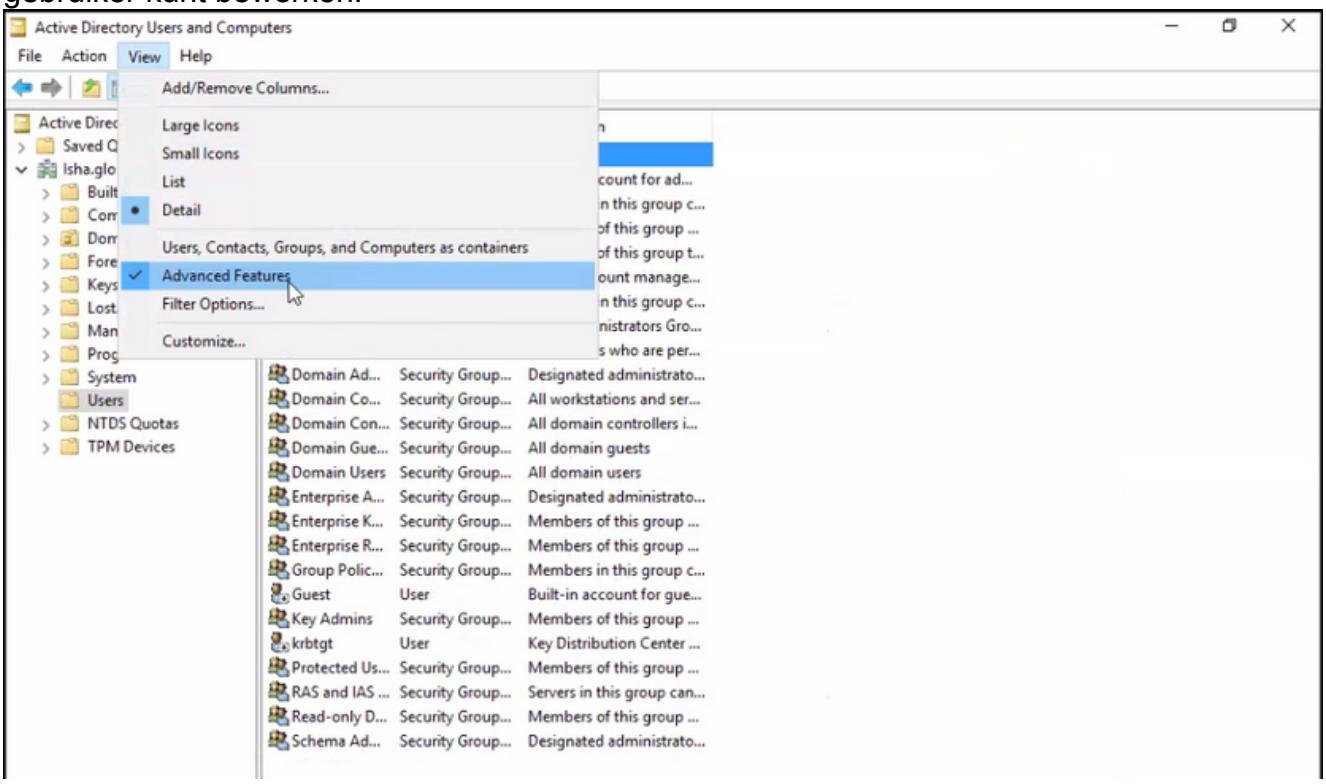
Define the User's Attributes in the AD User Directory

Op de Windows-server die wordt uitgevoerd **Active Directory** Wijzig de kenmerken voor elke gebruiker die u als CLI-beheerder wilt configureren.

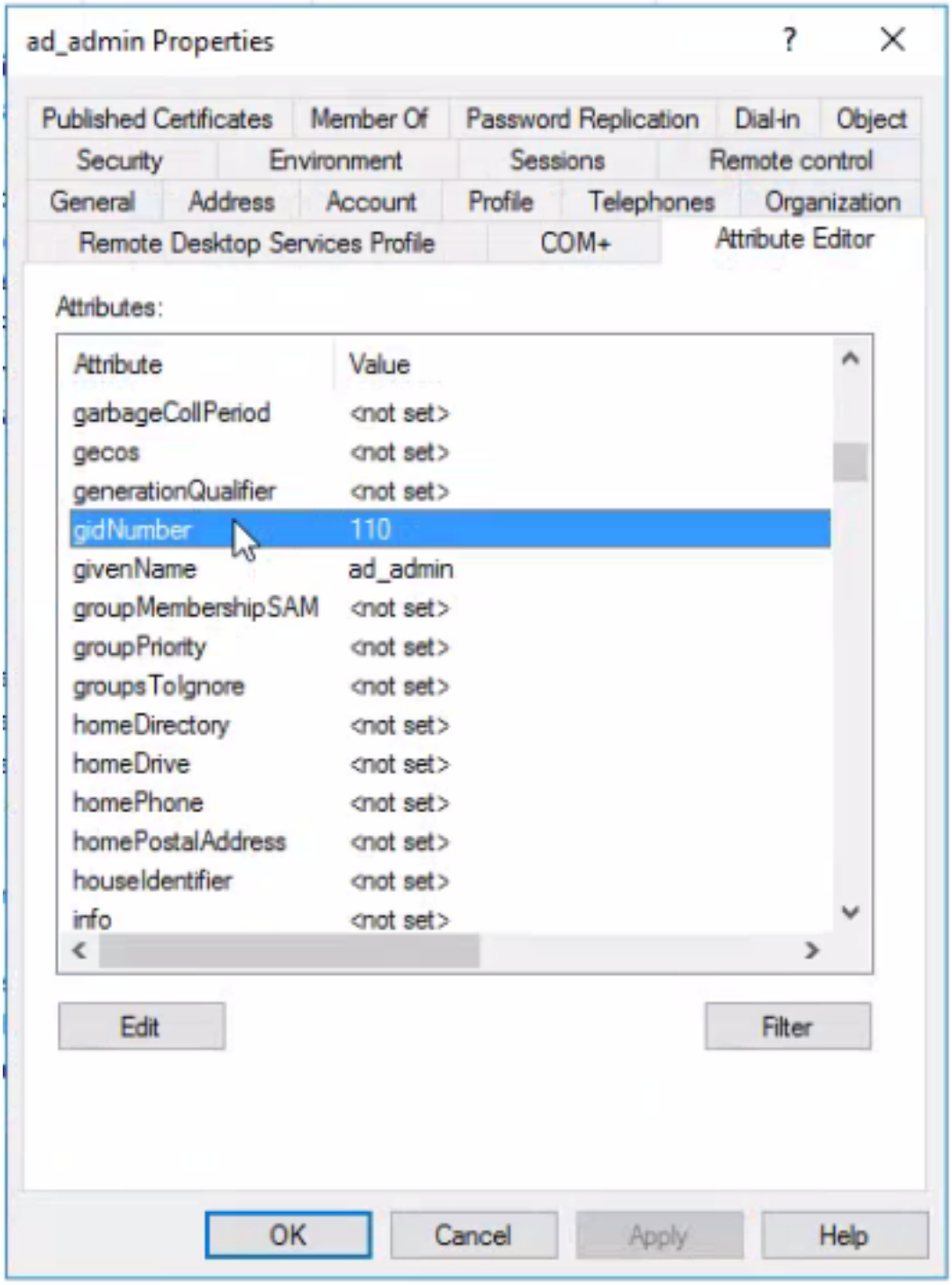
1. Open de **Server Manager Window** en naar **Server Manager > Roles > Active Directory Domain Services > Active**

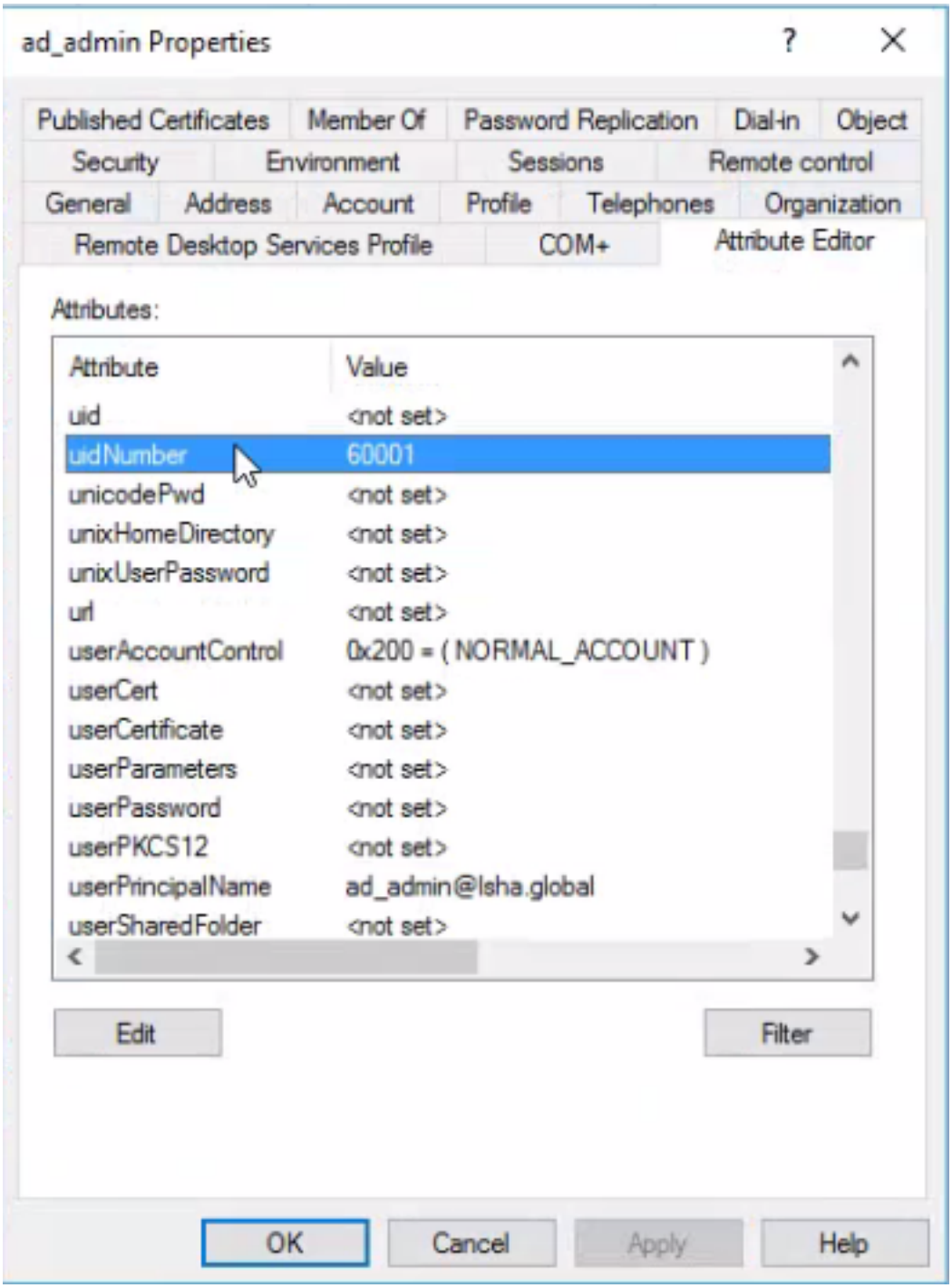
Directory Users and Computers > [ad.adserver]

2. Inschakelen **Advanced Features** onder het menu Beeld zodat u de eigenschappen van een gebruiker kunt bewerken.



3. Navigeer naar de AD-groep die de Admin-gebruiker bevat en zoek die gebruiker.
4. Dubbelklik op de gebruiker om het menu te openen **Properties** venster en kies de **Attribute Editor** .
5. Klik op een kenmerk en voer **gid** om het kenmerk te vinden **gidNumber** . Als u de **gidNumber** kenmerk klikt u op het **Filter** knop en uitvink. Alleen eigenschappen met waarden tonen.
6. Dubbelklik op de naam van het kenmerk om elk kenmerk te bewerken. Voor elke gebruiker: toewijzen **uidNumber** groter dan 60000, en zorg ervoor dat het nummer uniek is.toewijzen **gidNumber** als 110 of 111.GidNumber 110 duidt een beheerder aan, terwijl 111 een alleen-lezen gebruiker aanduidt.Wijzig de **uidNumber** na toewijzing.Als u de **gidNumber** , wacht minstens vijf minuten voordat u een SSH-verbinding maakt.


ad_admin Properties
Published Certificates
Member Of
Password Replication
Dial-in
Object
Security
Environment
Sessions
Remote control
General
Address
Account
Profile
Telephones
Organization
Remote Desktop Services Profile
COM+
Attribute Editor
Attributes:
Attribute
Value
garbageCollPeriod <not set>
gecos <not set>
generationQualifier <not set>
gidNumber 110
givenName ad_admin
groupMembershipSAM <not set>
groupPriority <not set>
groupsToIgnore <not set>
homeDirectory <not set>
homeDrive <not set>
homePhone <not set>
homePostalAddress <not set>
houseIdentifier <not set>
info <not set>
Edit
Filter
OK
Cancel
Apply
Help



Lid worden van de beheerder CLI-gebruiker naar het AD-domein

Verbinding maken met de Cisco ISE-CLI, voer de **identity-store** opdracht geven en de beheerder toewijzen aan het ID-archief.

Als u bijvoorbeeld de CLI-beheerder wilt toewijzen aan de Active Directory die in ISE is gedefinieerd als isha.global, voert u deze opdracht uit:

identity-store active-directory domain-name

Wanneer de koppeling is voltooid, maakt u verbinding met de Cisco ISE-CLI en logt u in als de beheerder-CLI-gebruiker om uw configuratie te verifiëren.

Als het domein dat u gebruikt in deze opdracht eerder was aangesloten bij de ISE-knooppunt, sluit u zich dan opnieuw aan bij het domein in de beheerdersconsole.

1. Klik in de Cisco ISE GUI op de **Menu** pictogram en navigeer naar **Administration > Identity Management > External Identity Sources .**
2. Kies in het linker deelvenster **Active Directory** en kies uw AD-naam.
3. In het rechter deelvenster wordt mogelijk de status van uw AD-verbinding gelezen **Operational** . Er zijn fouten als u de verbinding met Test Gebruiker met of MS-RPC of Kerberos test.
4. Controleer of u nog steeds kunt inloggen op de Cisco ISE-CLI als de Admin CLI-gebruiker.

ISE CLI

1. Log in op de ISE-CLI:
```
ise30-1/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise30-1/admin(config)#
```

2. Sluit je aan bij het domein: **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

   Als het domein **isha.global** is al aangesloten via UI, dan moet u opnieuw toetreden tot het domein **isha.global** van UI na deze configuratie. Totdat de herkoppeling gebeurt, worden verificaties uitgevoerd op **isha.global** faalt.

   Do you want to proceed? Y/N :Y
   Password for Administrator:

   Lid geworden van de domein sha.global succesvol**Opmerkingen:**

   - Als het domein al is aangesloten via GUI, sluit u zich dan opnieuw aan bij het knooppunt van GUI, anders blijven de verificaties tegen AD mislukken.
   - Alle knooppunten moeten individueel via CLI worden aangesloten.**Verifiëren**Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.**Problemen oplossen****Problemen samenvoegen**Problemen tijdens het samenvoegen en de bijbehorende logs kunnen worden weergegeven onder "/var/log/message file".Opdracht: **show logging system messages****Werkscenario**2021-07-19T21:15:01.457723+05:30 ise30-1 dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realmd' unit='realmd.service'
2021-07-19T21:15:01.462981+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...
2021-07-19T21:15:01.500846+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realmd'
2021-07-19T21:15:01.501045+05:30 ise30-1 systemd: Started Realm and Domain Configuration.
2021-07-19T21:15:01.541478+05:30 ise30-1 realmd: * Resolving: _ldap._tcp.isha.global
2021-07-19T21:15:01.544480+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.115
2021-07-19T21:15:01.546254+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.236
2021-07-19T21:15:01.546777+05:30 ise30-1 realmd: * Successfully discovered: Isha.global
2021-07-19T21:15:09.282364+05:30 ise30-1 realmd: * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/
2021-07-19T21:15:09.282708+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.MU0M60 -U Administrator ads join Isha.global
2021-07-19T21:15:12.701071+05:30 ise30-1 realmd: Enter Administrator's password:DNS update failed: NT_STATUS_INVALID_PARAMETER
2021-07-19T21:15:12.705753+05:30 ise30-1 realmd:
2021-07-19T21:15:12.706142+05:30 ise30-1 realmd: Use short domain name -- ISHA
2021-07-19T21:15:12.706580+05:30 ise30-1 realmd: Joined 'ISE30-1' to dns domain 'Isha.global'
2021-07-19T21:15:12.708781+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.MU0M60 -U Administrator ads keytab create

2021-07-19T21:15:13.786749+05:30 ise30-1 realmd: Enter Administrator's password:
2021-07-19T21:15:13.859916+05:30 ise30-1 realmd: * /usr/bin/systemctl enable sssd.service
2021-07-19T21:15:13.870511+05:30 ise30-1 systemd: Reloading.
2021-07-19T21:15:13.870724+05:30 ise30-1 realmd: Created symlink from /etc/systemd/system/multi-user.target.wants/sssd.service to /usr/lib/systemd/system/sssd.service.
2021-07-19T21:15:13.943407+05:30 ise30-1 realmd: * /usr/bin/systemctl restart sssd.service
2021-07-19T21:15:13.956987+05:30 ise30-1 systemd: Starting System Security Services Daemon...
2021-07-19T21:15:14.240764+05:30 ise30-1 sssd: Starting up
2021-07-19T21:15:14.458345+05:30 ise30-1 sssd[be[Isha.global]]: Starting up
2021-07-19T21:15:15.180211+05:30 ise30-1 sssd[nss]: Starting up
2021-07-19T21:15:15.208949+05:30 ise30-1 sssd[pam]: Starting up
2021-07-19T21:15:15.316360+05:30 ise30-1 systemd: Started System Security Services Daemon.
2021-07-19T21:15:15.317846+05:30 ise30-1 realmd: * /usr/bin/sh -c /usr/sbin/authconfig --update --enablesssd --enablesssdauth --enablemkhomedir --nostart && /usr/bin/systemctl enable oddjobd.service && /usr/bin/systemctl start oddjobd.service
2021-07-19T21:15:15.596220+05:30 ise30-1 systemd: Reloading.
2021-07-19T21:15:15.691786+05:30 ise30-1 systemd: Reloading.

2021-07-19T21:15:15.750889+05:30 ise30-1 realmd: * Successfully enrolled machine in realm**Niet-werkend scenarioDoe mee aan een mislukking vanwege een onjuist wachtwoord:**2021-07-19T21:12:45.487538+05:30 ise30-1 dbus[9675]: [system] Activating via systemd: service name='org.freedesktop.realmd' unit='realmd.service'
2021-07-19T21:12:45.496066+05:30 ise30-1 systemd: Starting Realm and Domain Configuration...
2021-07-19T21:12:45.531667+05:30 ise30-1 dbus[9675]: [system] Successfully activated service 'org.freedesktop.realmd'
2021-07-19T21:12:45.531950+05:30 ise30-1 systemd: Started Realm and Domain Configuration.
2021-07-19T21:12:45.567816+05:30 ise30-1 realmd: * Resolving: _ldap._tcp.isha.global
2021-07-19T21:12:45.571092+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.115
2021-07-19T21:12:45.572854+05:30 ise30-1 realmd: * Performing LDAP DSE lookup on: 10.127.197.236
2021-07-19T21:12:45.573376+05:30 ise30-1 realmd: * Successfully discovered: Isha.global
2021-07-19T21:12:52.273667+05:30 ise30-1 realmd: * Required files: /usr/sbin/oddjobd, /usr/libexec/oddjob/mkhomedir, /usr/sbin/sssd, /usr/bin/net
2021-07-19T21:12:52.274730+05:30 ise30-1 realmd: * LANG=C LOGNAME=root /usr/bin/net -s /var/cache/realmd/realmd-smb-conf.R0SM60 -U Administrator ads join Isha.global
2021-07-19T21:12:52.369726+05:30 ise30-1 realmd: Enter Administrator's password:
2021-07-19T21:12:52.370190+05:30 ise30-1 realmd: Failed to join domain: failed to lookup DC info for domain 'Isha.global' over rpc: The attempted logon is invalid. This is either due to a bad username or authentication information.
2021-07-19T21:12:52.372180+05:30 ise30-1 realmd: ! Joining the domain Isha.global failed**Aanmeldingsproblemen**Problemen tijdens het inloggen en de bijbehorende logbestanden zijn te zien onder **/var/log/secure** .Opdracht: show logging system secure **Succesvolle authenticatie:**2021-07-19T21:25:10.435849+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:auth): unknown option: no_magic_root
2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): received for user ad_admin: 12 (Authentication token is no longer valid; new one required)
2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:account): unknown option: reset
2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam_succeed_if(sshd:account): 'uid' resolves to '60001'
2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad_admin from 10.227.243.67 port 61613 ssh2
2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:setcred): unknown option: no_magic_root
2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): reading settings from '/etc/security/limits.conf'
2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf'
2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): process_limit: processing soft nproc 4096 for DEFAULT
2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam_unix(sshd:session): session opened for user ad_admin by (uid=0)

2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam_tally2(sshd:setcred): unknown option: no_magic_root

Verificatiefout vanwege onjuist wachtwoord:

2021-07-19T21:25:10.435849+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:auth): unknown option: no_magic_root
2021-07-19T21:25:10.438694+05:30 ise30-1 sshd[119435]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365110+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:25:11.365156+05:30 ise30-1 sshd[119435]: pam_sss(sshd:auth): received for user ad_admin: 12 (Authentication token is no longer valid; new one required)
2021-07-19T21:25:11.368231+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:account): unknown option: reset
2021-07-19T21:25:11.370223+05:30 ise30-1 sshd[119435]: pam_succeed_if(sshd:account): 'uid' resolves to '60001'
2021-07-19T21:25:11.370337+05:30 ise30-1 sshd[119435]: Accepted password for ad_admin from 10.227.243.67 port 61613 ssh2
2021-07-19T21:25:11.371478+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:setcred): unknown option: no_magic_root
2021-07-19T21:25:11.781374+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): reading settings from '/etc/security/limits.conf'
2021-07-19T21:25:11.781445+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): reading settings from '/etc/security/limits.d/20-nproc.conf'
2021-07-19T21:25:11.781462+05:30 ise30-1 sshd[119435]: pam_limits(sshd:session): process_limit: processing soft nproc 4096 for DEFAULT
2021-07-19T21:25:11.781592+05:30 ise30-1 sshd[119435]: pam_unix(sshd:session): session opened for user ad_admin by (uid=0)
2021-07-19T21:25:11.784725+05:30 ise30-1 sshd[121474]: pam_tally2(sshd:setcred): unknown option: no_magic_root
2021-07-19T21:25:56.737559+05:30 ise30-1 sshd[119435]: pam_unix(sshd:session): session closed for user ad_admin
2021-07-19T21:25:56.738341+05:30 ise30-1 sshd[119435]: pam_tally2(sshd:setcred): unknown option: no_magic_root
2021-07-19T21:26:21.375211+05:30 ise30-1 sshd[122957]: pam_tally2(sshd:auth): unknown option: no_magic_root
2021-07-19T21:26:21.376387+05:30 ise30-1 sshd[122957]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:26:21.434442+05:30 ise30-1 sshd[122957]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=ad_admin
2021-07-19T21:26:21.434461+05:30 ise30-1 sshd[122957]: pam_sss(sshd:auth): received for user ad_admin: 17 (Failure setting user credentials)
2021-07-19T21:26:21.434480+05:30 ise30-1 sshd[122957]: pam_nologin(sshd:auth): unknown option: debug
2021-07-19T21:26:22.742663+05:30 ise30-1 sshd[122957]: Failed password for ad_admin from 10.227.243.67 port 61675 ssh2

Verificatiefout vanwege ongeldige gebruiker:

2021-07-19T21:28:08.756228+05:30 ise30-1 sshd[125725]: Invalid user Masked(xxxxx) from 10.227.243.67 port 61691
2021-07-19T21:28:08.757646+05:30 ise30-1 sshd[125725]: input_userauth_request: invalid user Masked(xxxxx) [preauth]
2021-07-19T21:28:15.628387+05:30 ise30-1 sshd[125725]: pam_tally2(sshd:auth): unknown option: no_magic_root
2021-07-19T21:28:15.628658+05:30 ise30-1 sshd[125725]: pam_tally2(sshd:auth): pam_get_uid; no such user
2021-07-19T21:28:15.628899+05:30 ise30-1 sshd[125725]: pam_unix(sshd:auth): check pass; user unknown
2021-07-19T21:28:15.629142+05:30 ise30-1 sshd[125725]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67
2021-07-19T21:28:15.631975+05:30 ise30-1 sshd[125725]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.227.243.67 user=isha
2021-07-19T21:28:15.631987+05:30 ise30-1 sshd[125725]: pam_sss(sshd:auth): received for user isha: 10 (User not known to the underlying authentication module)
2021-07-19T21:28:15.631993+05:30 ise30-1 sshd[125725]: pam_nologin(sshd:auth): unknown option: debug
2021-07-19T21:28:17.256541+05:30 ise30-1 sshd[125725]: Failed password for invalid user Masked(xxxxx) from 10.227.243.67 port 61691 ssh2

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.