Integrazione di AD per l'interfaccia grafica ISE e accesso tramite CLI

Sommario

Introduzione

Questo documento descrive la configurazione di Microsoft AD come archivio identità esterno per l'accesso amministrativo alla GUI e alla CLI di Cisco ISE Management.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Cisco ISE versione 3.0
- Microsoft AD

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE versione 3.0
- Windows Server 2016

Questo documento descrive la configurazione di Microsoft **Active Directory (AD)** come archivio identità esterno per l'accesso amministrativo a Cisco **Identity Services Engine (ISE)** GUI e CLI di gestione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Utilizzare questa sezione per configurare l'uso di Microsoft AD come archivio identità esterno per l'accesso amministrativo all'interfaccia utente grafica di gestione di Cisco ISE.

Queste porte vengono usate tra il nodo ISE e AD per questa comunicazione:

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

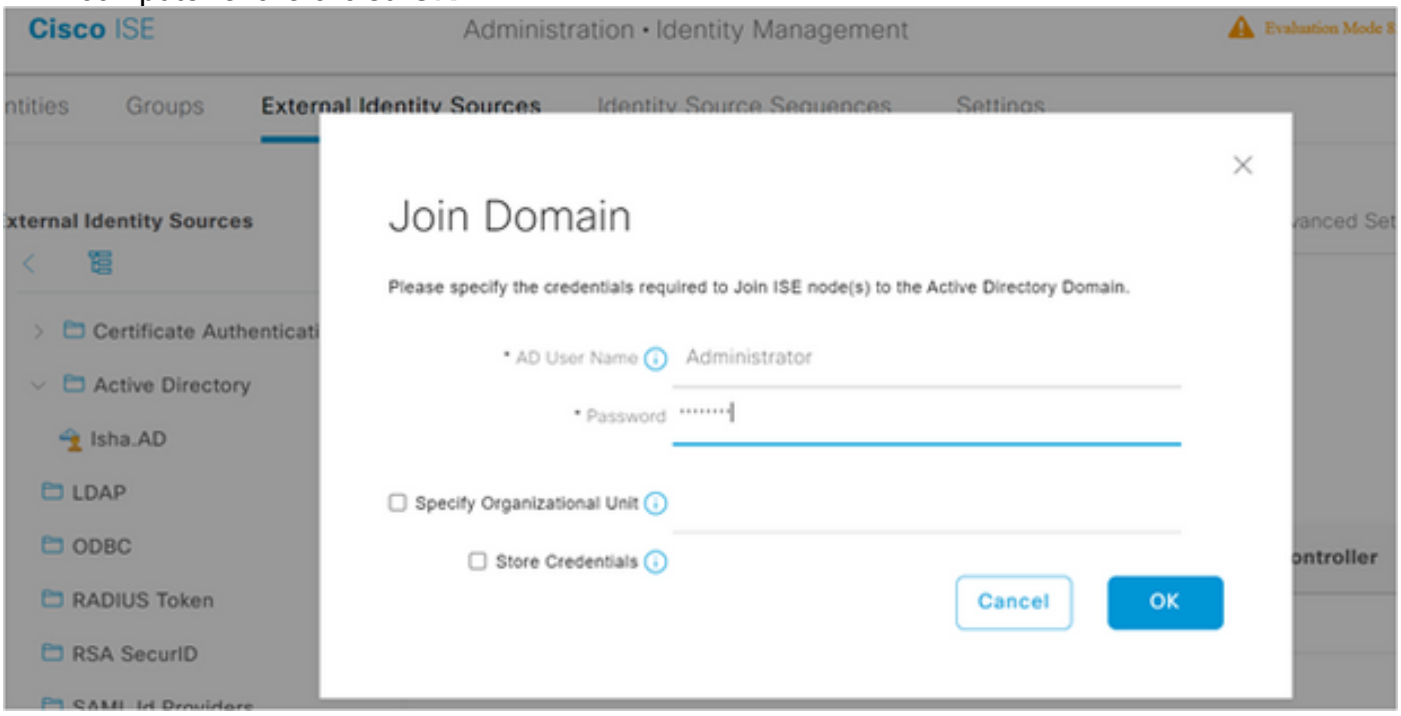
Nota: verificare che l'account AD disponga di tutti i privilegi necessari.

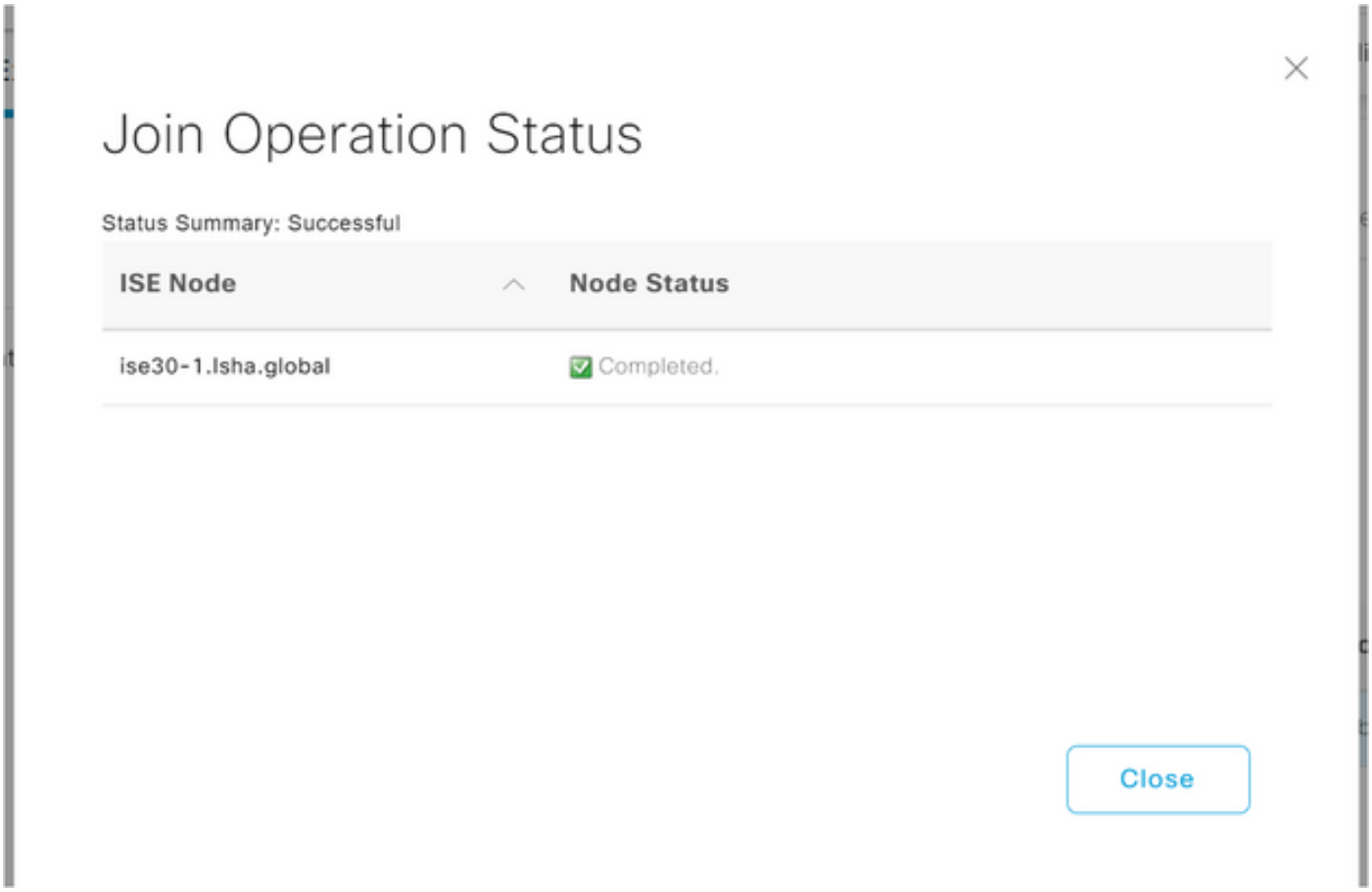
Active Directory Account Permissions Required for Performing Various Operations

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.

Iscriviti ad ISE 2008

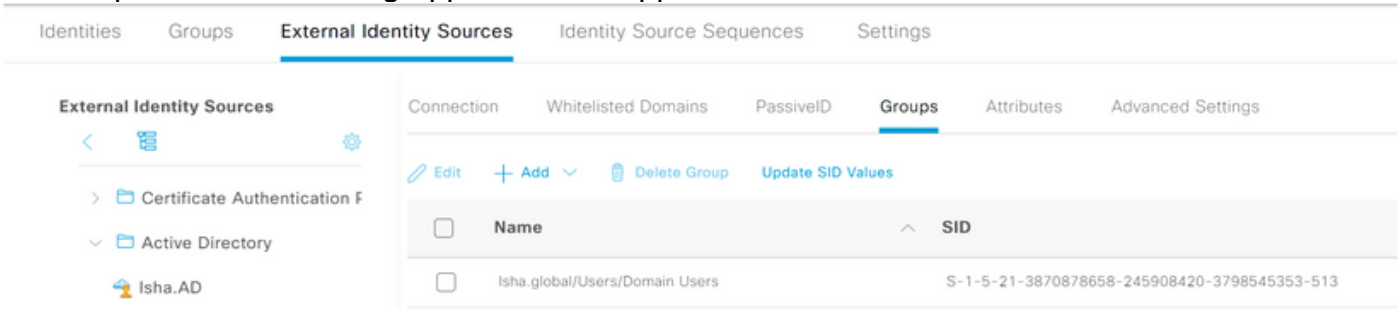
1. Passa a **Administration > Identity Management > External Identity Sources > Active Directory** .
2. Immettere il nuovo nome del punto di join e il dominio Active Directory.
3. Immettere le credenziali dell'account AD che consente di aggiungere e modificare gli oggetti computer e fare clic su **OK**.





Seleziona gruppi di directory

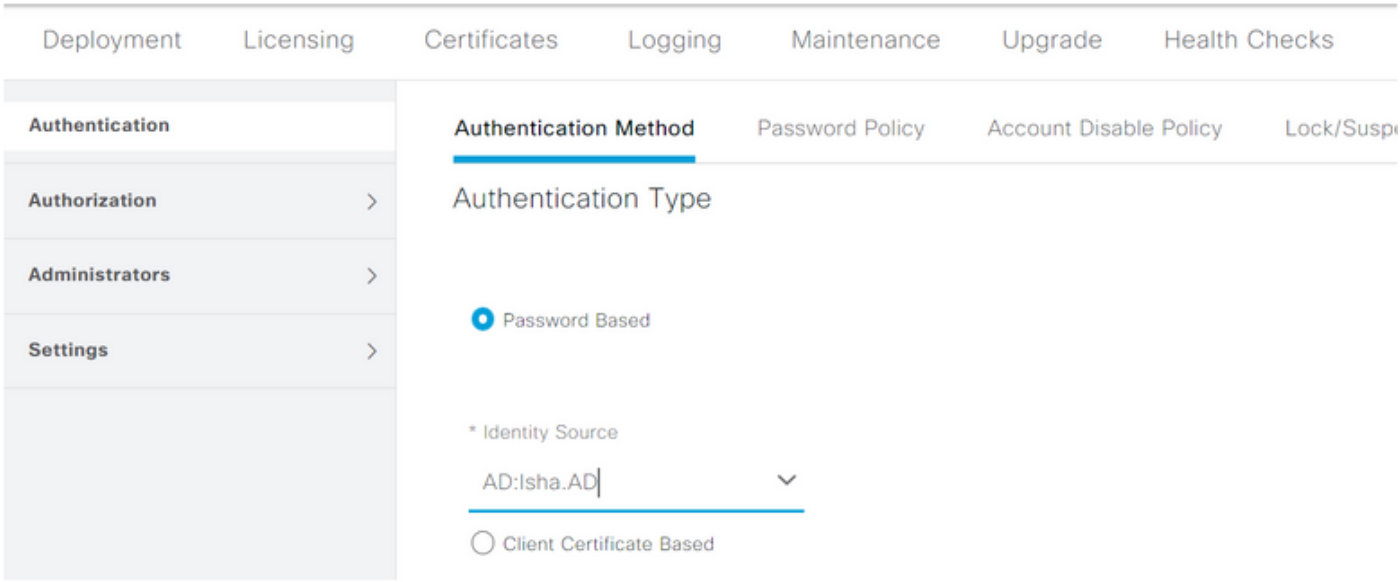
1. Passa a **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. Importare almeno un gruppo AD a cui appartiene l'amministratore.



Abilita accesso amministrativo per AD

Completare questa procedura per abilitare l'autenticazione basata su password per AD:

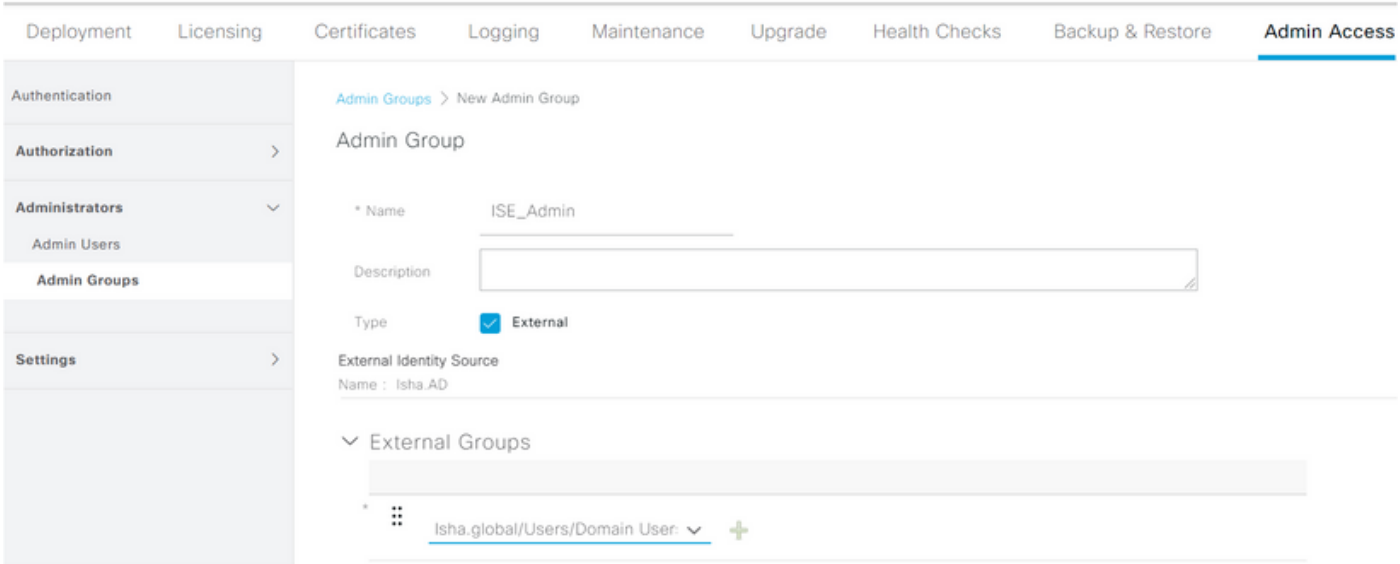
1. Passa a **Administration > System > Admin Access > Authentication** .
2. Dal **Authentication Method** , scegliere la scheda **Password Based** opzione.
3. Scegliere **AD** dal menu **Identity Source** elenco a discesa.
4. Clic **Save Changes** .



Configurare il mapping tra il gruppo di amministratori e il gruppo AD

Definisci un Cisco ISE **Admin Group** e mapparlo a un gruppo AD. In questo modo è possibile determinare **Role Based Access Control (RBAC)** autorizzazioni per l'amministratore in base all'appartenenza ai gruppi in Active Directory.

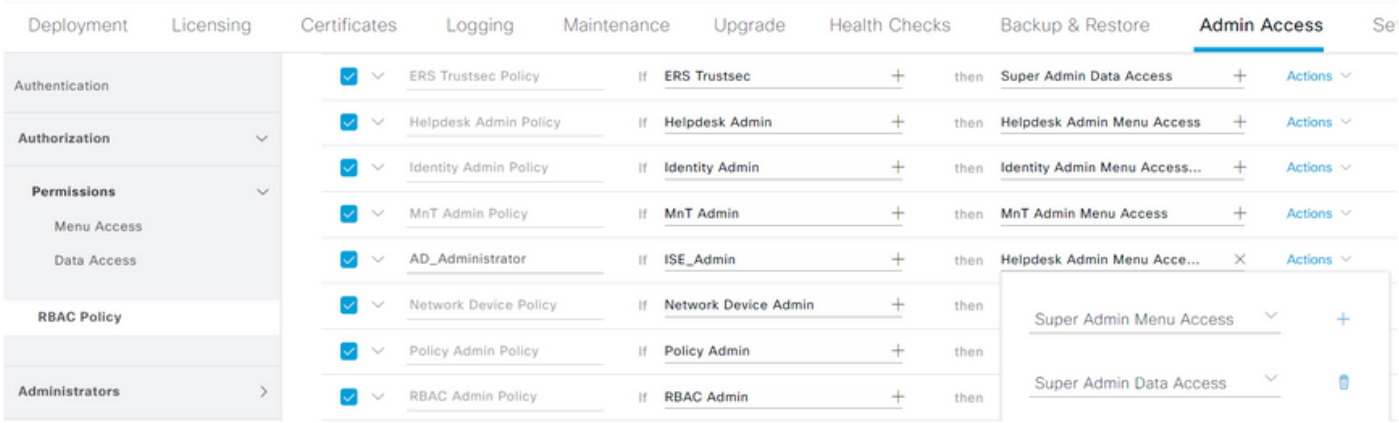
1. Passa a **Administration > System > Admin Access > Administrators > Admin Groups** .
2. Clic **Add** nell'intestazione della tabella per visualizzare il nuovo **Admin Group** riquadro di configurazione.
3. Immettere il nome del nuovo gruppo Amministratore.
4. Nella scheda **Type** , selezionare il **External** .
5. Dal **External Groups** dall'elenco a discesa, scegliere il gruppo AD a cui si desidera mappare questo gruppo di amministratori, come definito **Select Directory Groups** sezione.
6. Clic **Save Changes** .



Impostare le autorizzazioni RBAC per il gruppo Admin

Completare questi passaggi per assegnare le autorizzazioni RBAC ai gruppi amministrativi creati nella sezione precedente:

1. Passa a **Administration > System > Admin Access > Authorization > Policy** .
2. Dal **Actions** a destra, scegliere **Insert New Policy** per aggiungere un nuovo criterio.
3. Creare una nuova regola denominata **AD_Administrator** , eseguirne il mapping con il gruppo Admin definito nel **Enable Administrative Access** per la sezione AD e assegnarle le autorizzazioni. **Nota**: in questo esempio viene assegnato il gruppo amministrativo denominato **Super Admin**, che equivale all'account amministratore standard.
4. Clic **Save Changes** . La conferma delle modifiche salvate viene visualizzata nell'angolo inferiore destro dell'interfaccia utente.

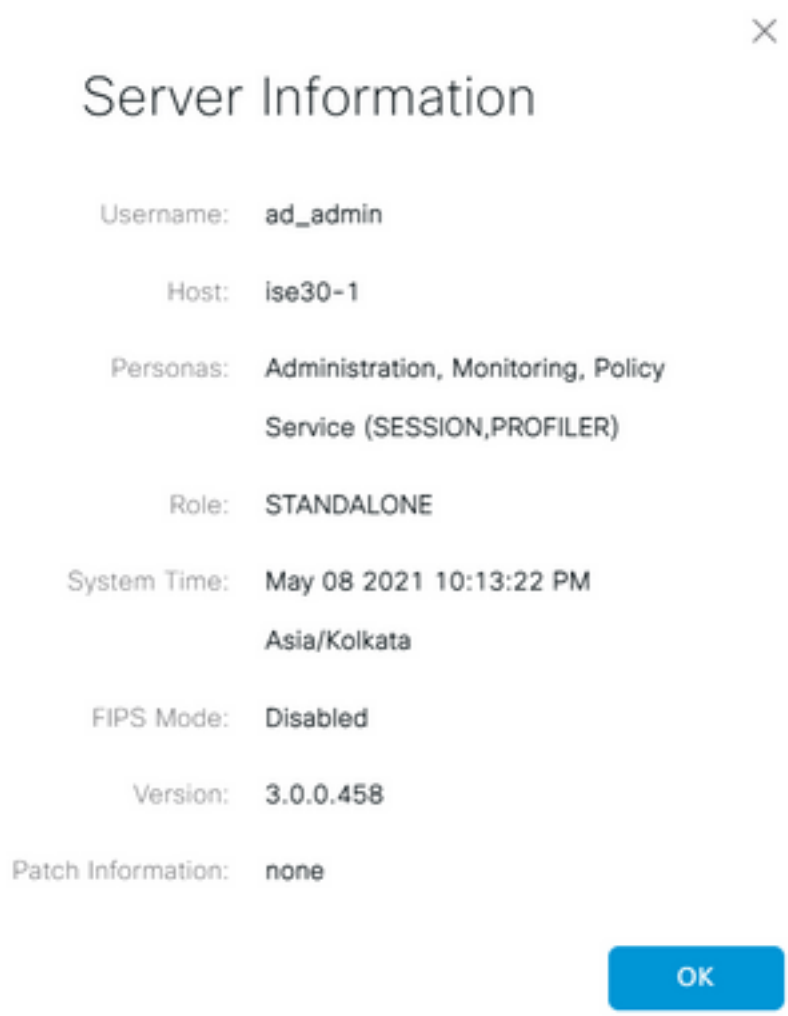


Accesso GUI ISE con credenziali AD

Per accedere alla GUI di ISE con le credenziali di AD, completare la procedura seguente:

1. Uscire dalla GUI amministrativa.
2. Scegliere **AD** dal menu **Identity Source** elenco a discesa.
3. Immettere il nome utente e la password dal database di Active Directory ed eseguire l'accesso.

   Nota: per impostazione predefinita, ISE utilizza l'archivio utenti interno nel caso in cui AD non sia raggiungibile o le credenziali dell'account utilizzate non esistano in AD. Ciò semplifica l'accesso rapido se si utilizza l'archivio interno mentre AD è configurato per l'accesso amministrativo.



Accesso CLI ISE con credenziali AD

L'autenticazione con un'origine identità esterna è più sicura rispetto a quella con il database interno. RBAC per **CLI Administrators** supporta un archivio identità esterno.

Nota: ISE versione 2.6 e successive supportano l'autenticazione degli amministratori CLI da origini identità esterne, ad esempio AD.

Gestione di un'unica origine per le password senza la necessità di gestire più policy sulle password e di amministrare gli utenti interni all'interno di ISE, con una conseguente riduzione di tempi e sforzi.

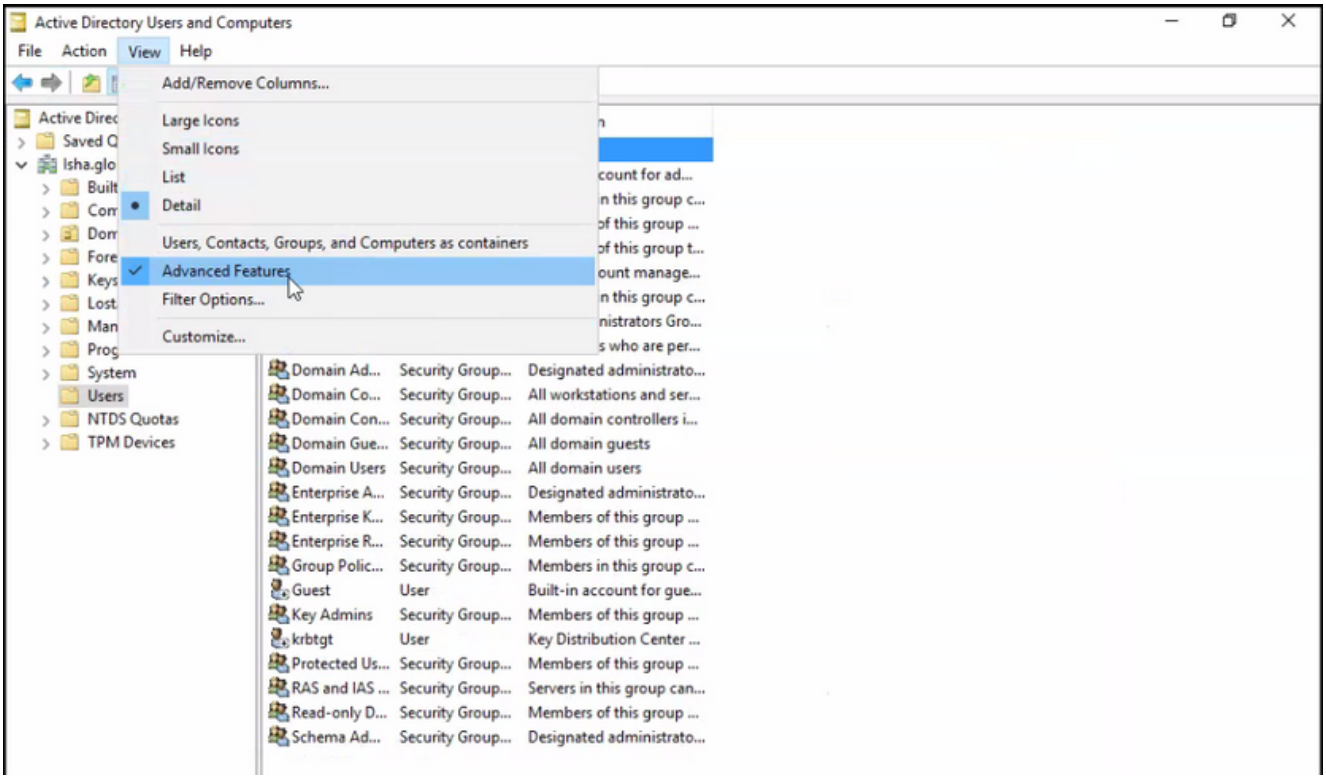
Prerequisiti

Ènecessario aver definito l'utente Admin e averlo aggiunto a un gruppo Administrator. L'amministratore deve essere un **Super Admin** .

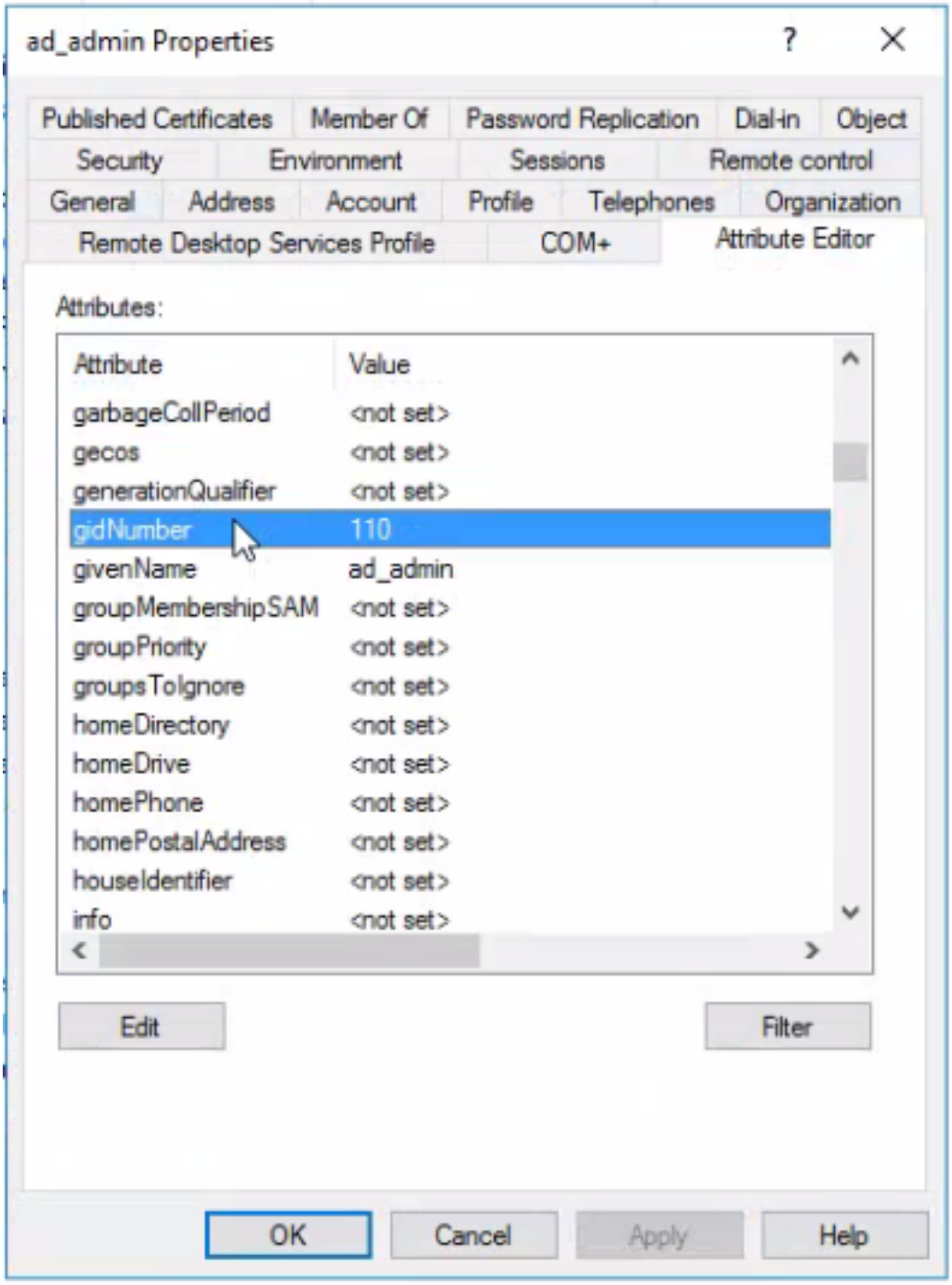
Define the User's Attributes in the AD User Directory

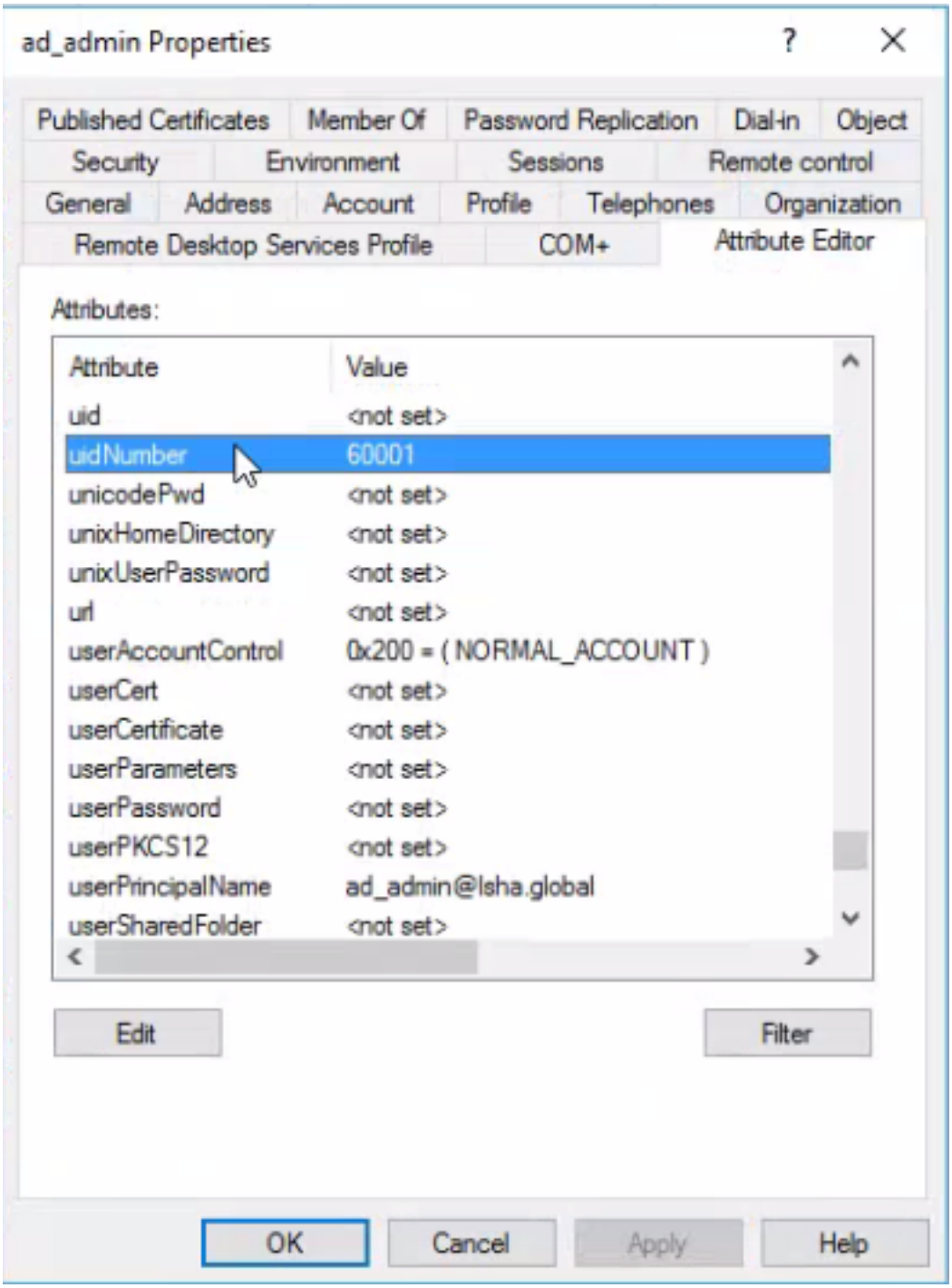
Sul server Windows in esecuzione **Active Directory** modificare gli attributi per ogni utente che si intende configurare come amministratore CLI.

1. Aprire il **Server Manager Window** e passare a **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]**
2. Abilita **Advanced Features** nel menu Visualizza, in modo da poter modificare gli attributi di un utente.



3. Passare al gruppo AD che contiene l'utente Amministratore e individuare tale utente.
4. Fare doppio clic sull'utente per aprire **Properties** e scegliere il pulsante **Attribute Editor** .
5. Fare clic su un attributo e immettere: **gid** per individuare l'attributo **gidNumber** . Se non si trova la **gidNumber** , fare clic sull'attributo **Filter** e deselezionare. Mostra solo gli attributi con valori.
6. Fare doppio clic sul nome dell'attributo per modificarlo. Per ogni utente: Assegna **uidNumber** maggiore di 60000 e assicurarsi che il numero sia univoco.Assegna **gidNumber** come 110 o 111.GidNumber 110 indica un utente amministratore, mentre 111 indica un utente di sola lettura.Non modificare **uidNumber** dopo l'assegnazione.Se si modifica il **gidNumber** , attendere almeno cinque minuti prima di stabilire una connessione SSH.


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



Aggiunta dell'utente CLI di amministrazione al dominio AD

Collegarsi alla CLI di Cisco ISE, eseguire la **identity-store** e assegnare l'utente Admin all'archivio ID.

Ad esempio, per mappare l'utente amministratore CLI ad Active Directory definito in ISE come isha.global, eseguire questo comando:

identity-store active-directory domain-name

Una volta completato il join, connettersi alla CLI di Cisco ISE e accedere come utente Admin CLI per verificare la configurazione.

Se il dominio usato in questo comando è stato aggiunto in precedenza al nodo ISE, aggiungere nuovamente il dominio nella console Administrators.

1. Nell'interfaccia utente di Cisco ISE, fare clic sul pulsante **Menu** e passare a **Administration >**

Identity Management > External Identity Sources .

2. Nel riquadro di sinistra, scegliere **Active Directory** e scegliere il nome dell'annuncio.
3. Nel riquadro di destra, lo stato della connessione AD potrebbe essere **Operational** . Se si esegue il test della connessione con Test User con MS-RPC o Kerberos, si verificano errori.
4. Verificare di poter ancora accedere alla CLI di Cisco ISE come utente Admin CLI.

ISE CLI

1. Accedere alla CLI di ISE:
```
ise30-1/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise30-1/admin(config)#
```

2. Aggiungere il nodo al dominio: **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

   Se il dominio **isha.global** è già stato aggiunto tramite l'interfaccia utente, quindi è necessario aggiungere di nuovo il dominio **isha.global** dall'interfaccia utente dopo questa configurazione.

   Fino a quando non si verifica il rejoin, le autenticazioni a **isha.global** non riesce.

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

   Aggiunta al dominio isha.global completata**Note:**

   - Se il dominio è già stato aggiunto tramite GUI, aggiungere di nuovo il nodo dalla GUI; in caso contrario, le autenticazioni di AD continuano a fallire.

   - Tutti i nodi devono essere uniti singolarmente tramite la CLI.**Verifica**Attualmente non è disponibile una procedura di verifica per questa configurazione.**Risoluzione dei problemi****Problemi di join**I problemi durante l'operazione di unione e i relativi registri possono essere visualizzati in "/var/log/messages file".Comando: **show logging system messages****Scenario di lavoro**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**Scenario non lavorativoErrore di accesso a causa di password errata:**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**Problemi di accesso**I problemi durante l'accesso e i log relativi possono essere visualizzati in **/var/log/secure**.Comando: show logging system secure **Autenticazione riuscita:**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

Errore di autenticazione a causa di una password errata: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

Errore di autenticazione a causa di un utente non valido:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).