整合AD用於ISE GUI和CLI登入

目錄

簡介

本文檔描述將Microsoft AD配置為外部身份庫，以便對Cisco ISE管理GUI和CLI進行管理訪問。

必要條件

思科建議瞭解以下主題：

- 思科ISE版本3.0的配置
- Microsoft廣告

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本3.0
- Windows Server 2016

本文檔介紹Microsoft的配置 **Active Directory (AD)** 作為外部身份庫，用於對Cisco **Identity Services Engine (ISE)** 管理GUI和CLI。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

使用此部分可以配置使用Microsoft AD作為外部身份庫對思科ISE管理GUI進行管理訪問。

ISE節點和AD之間使用以下埠進行通訊：

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

注意：確保AD帳戶具有所有必需的許可權。

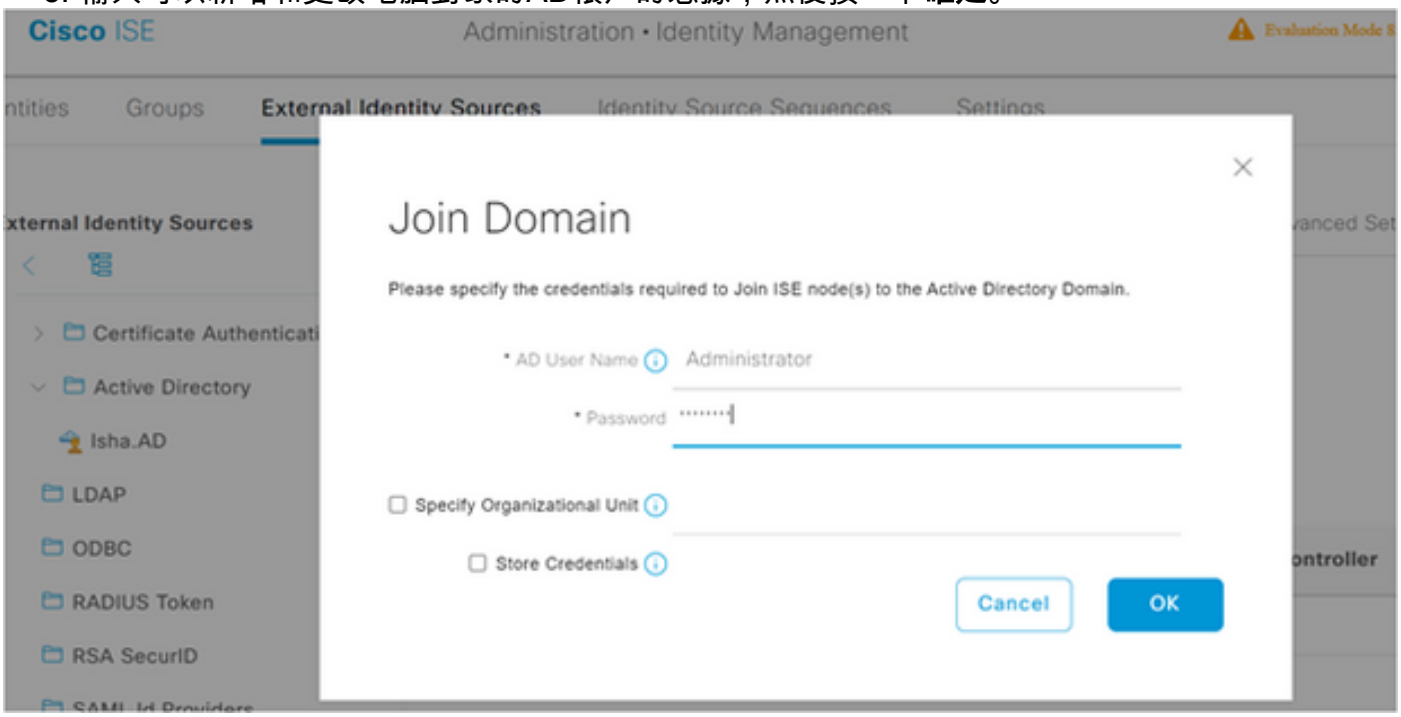
Active Directory Account Permissions Required for Performing Various Operations

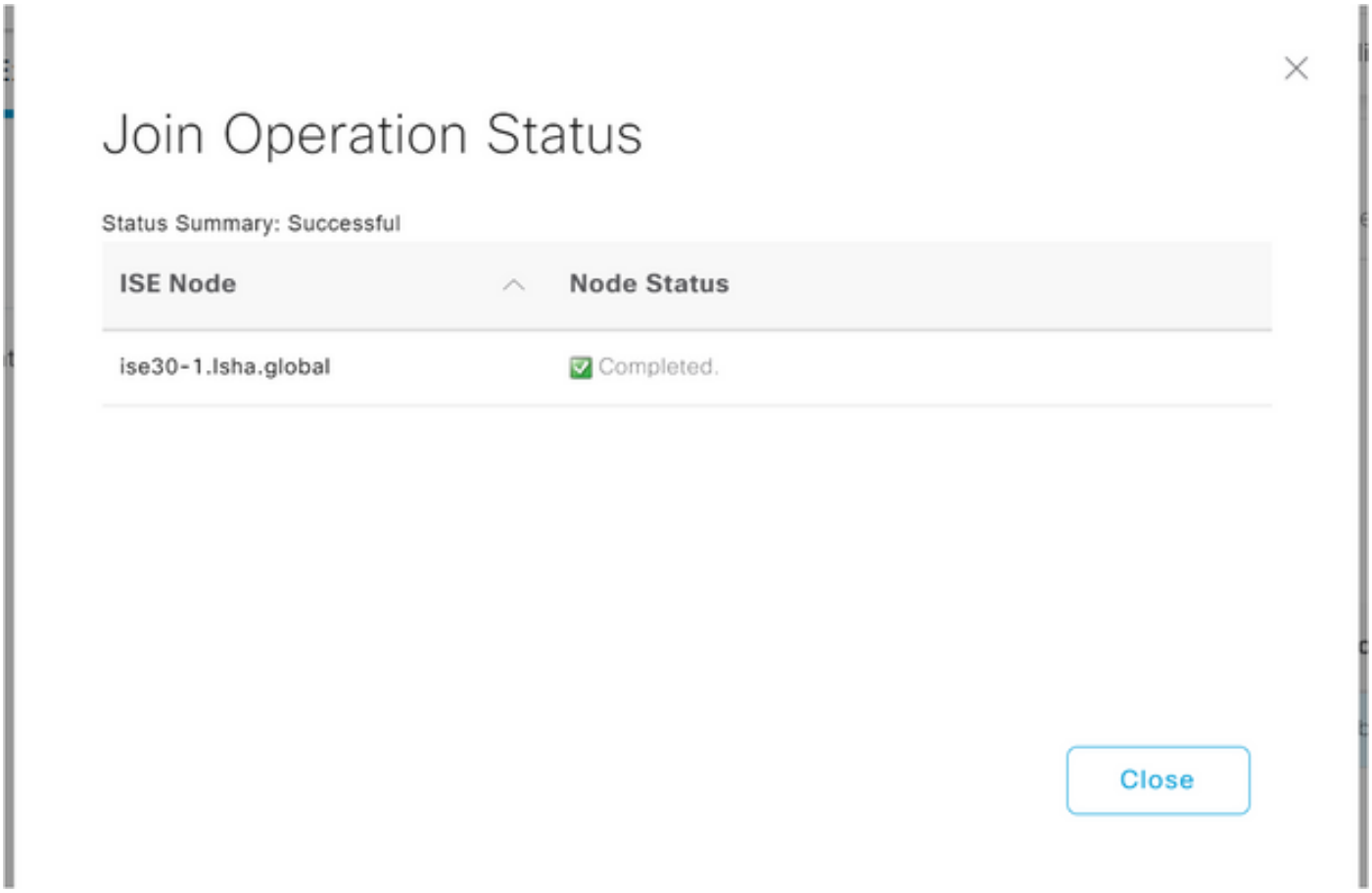
Join Operations	Leave Operations	Cisco ISE Machine Accounts
For the account that is used to perform the join operation, the following permissions are required: • Search Active Directory (to see if a Cisco ISE machine account already exists) • Create Cisco ISE machine account to domain (if the machine 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.

將ISE加入AD

1. 導航至 **Administration > Identity Management > External Identity Sources > Active Directory** .
2. 輸入新的加入點名稱和AD域。

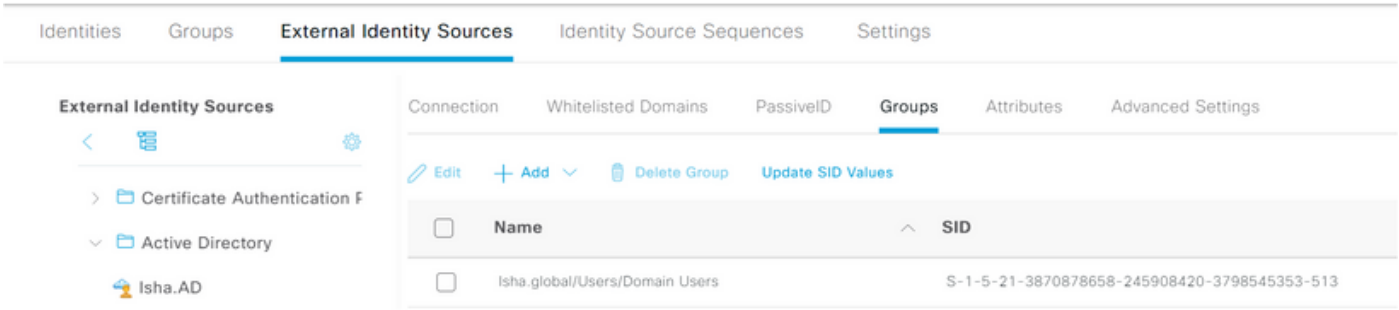
3. 輸入可以新增和更改電腦對象的AD帳戶的憑據，然後按一下**確定**。





選擇目錄組

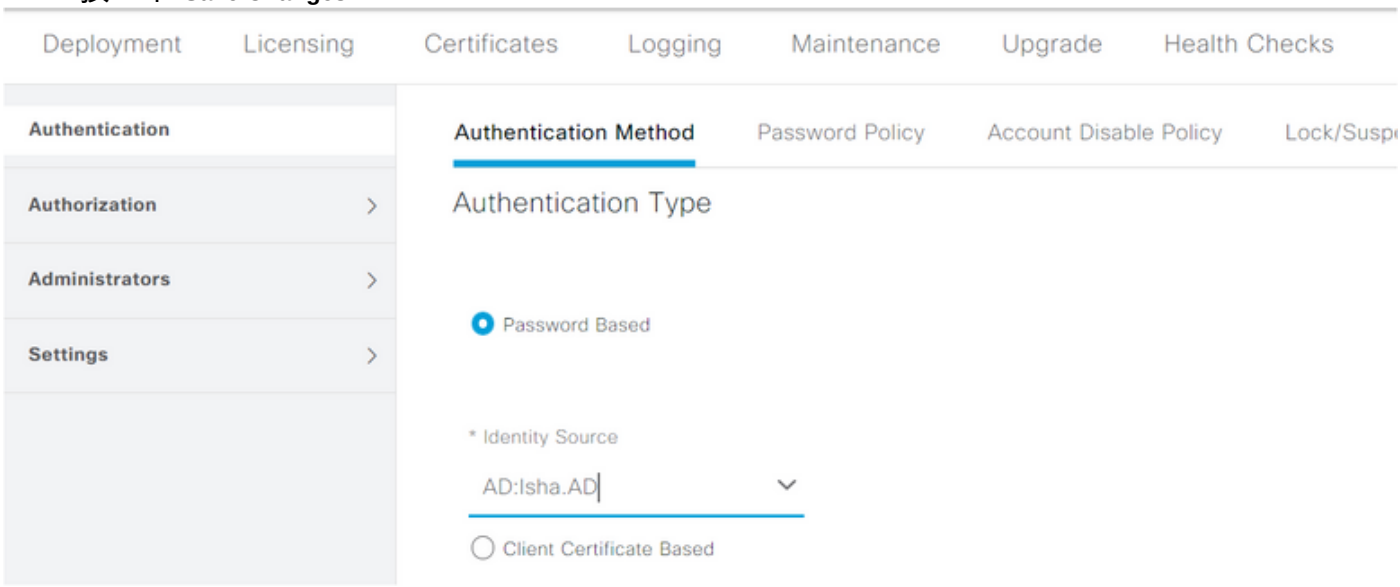
1. 導航至 **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. 至少匯入管理員所屬的一個AD組。



啟用AD的管理訪問

完成以下步驟，以便為AD啟用基於密碼的身份驗證：

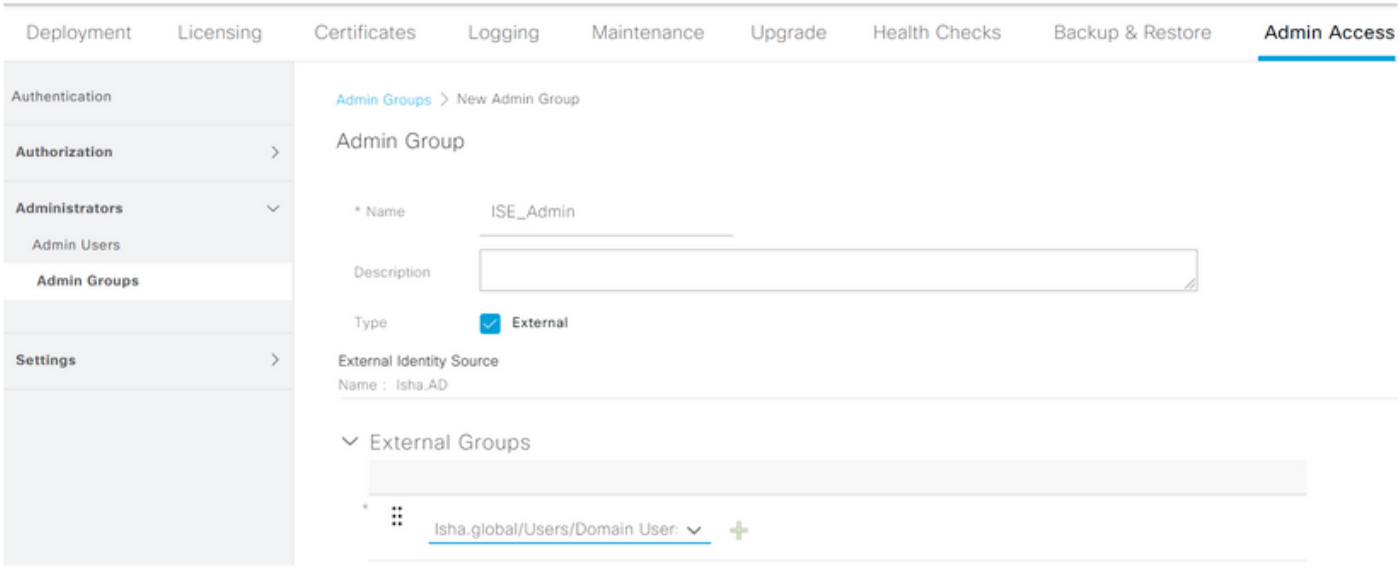
1. 導航至 **Administration > System > Admin Access > Authentication** .
2. 從 **Authentication Method** 頁籤中，選擇 **Password Based** 選項。
3. 從中選擇AD。 **Identity Source** 下拉選單。
4. 按一下 **Save Changes** .



配置管理組到AD組的對映

定義思科ISE **Admin Group** 並將其對映到AD組。這樣授權就可以確定 **Role Based Access Control (RBAC)** 管理員的許可權基於AD中的組成員身份。

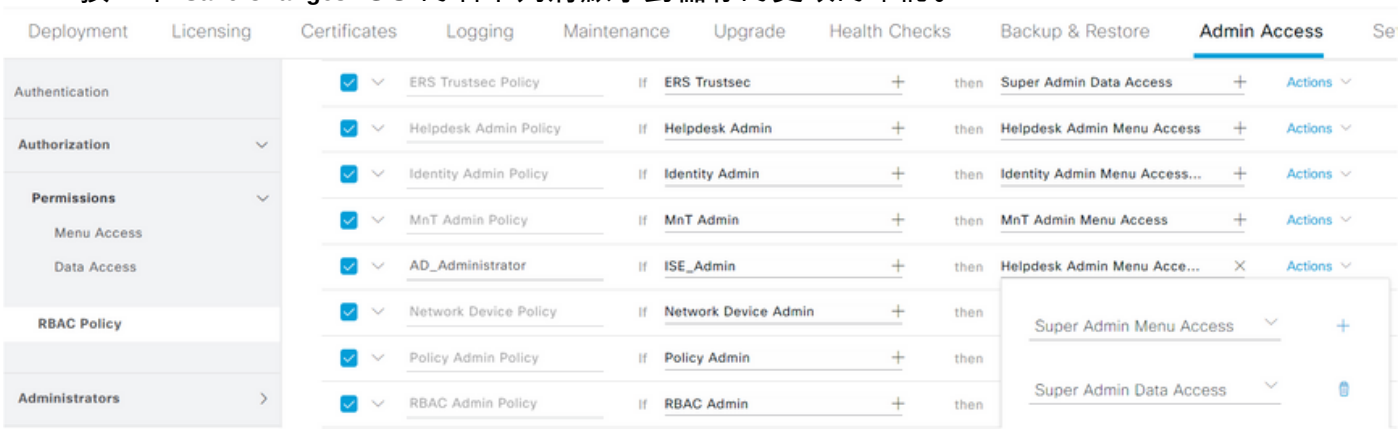
1. 導航至 **Administration > System > Admin Access > Administrators > Admin Groups** .
2. 按一下 **Add** 在表頭中檢視新的 **Admin Group** 配置窗格。
3. 輸入新管理員組的名稱。
4. 在 **Type** 欄位，請檢查 **External** 覈取方塊。
5. 從 **External Groups** 下拉選單中，選擇希望此管理員組對映到的AD組，如在 **Select Directory Groups** 部分。
6. 按一下 **Save Changes** .



設定管理員組的RBAC許可權

完成以下步驟，將RBAC許可權分配給在上一節中建立的管理員組：

1. 導航至 **Administration > System > Admin Access > Authorization > Policy .**
2. 從 **Actions** 下拉選單，選擇 **Insert New Policy** 新增新策略。
3. 新建規則名為 **AD_Administrator** ，將其與中定義的管理員組進行對映 **Enable Administrative Access** ，並為其分配許可權。 **注意**：在本示例中，分配了名為**Super Admin的**管理員組，該組等效於標準管理員帳戶。
4. 按一下 **Save Changes** .GUI的右下角將顯示對儲存的更改的確認。

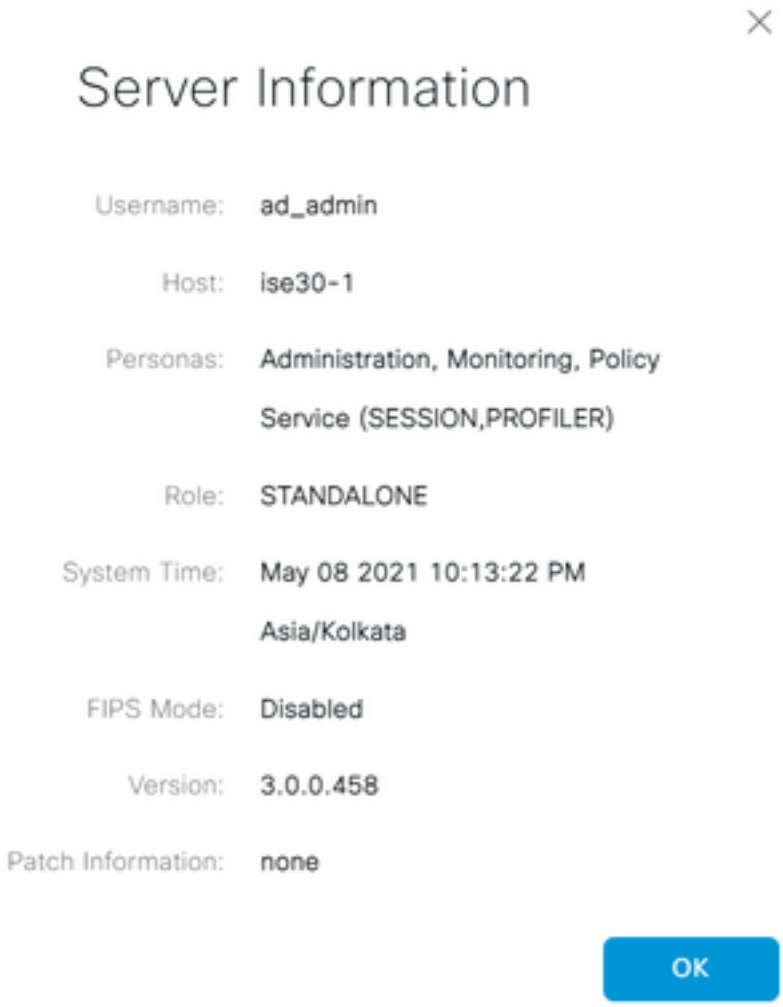


使用AD憑證的ISE GUI訪問

完成以下步驟，以便使用AD憑證訪問ISE GUI:

1. 從管理GUI註銷。
2. 從中選擇**AD**。 **Identity Source** 下拉選單。
3. 從AD資料庫輸入使用者名稱和密碼並登入。

註：如果AD無法訪問，或者使用的帳戶憑證在AD中不存在，則ISE預設為內部使用者儲存。如果在為AD配置管理訪問時使用內部儲存，這將有助於快速登入。



使用AD憑證的ISE CLI訪問

使用外部身份源進行身份驗證比使用內部資料庫進行身份驗證更安全。RBAC **CLI Administrators** 支援外部身份庫。

注意:ISE版本2.6及更高版本支援通過外部身份源（如AD）對CLI管理員進行身份驗證。

管理單個密碼源，無需管理多個密碼策略並管理ISE中的內部使用者，從而減少時間和工作量。

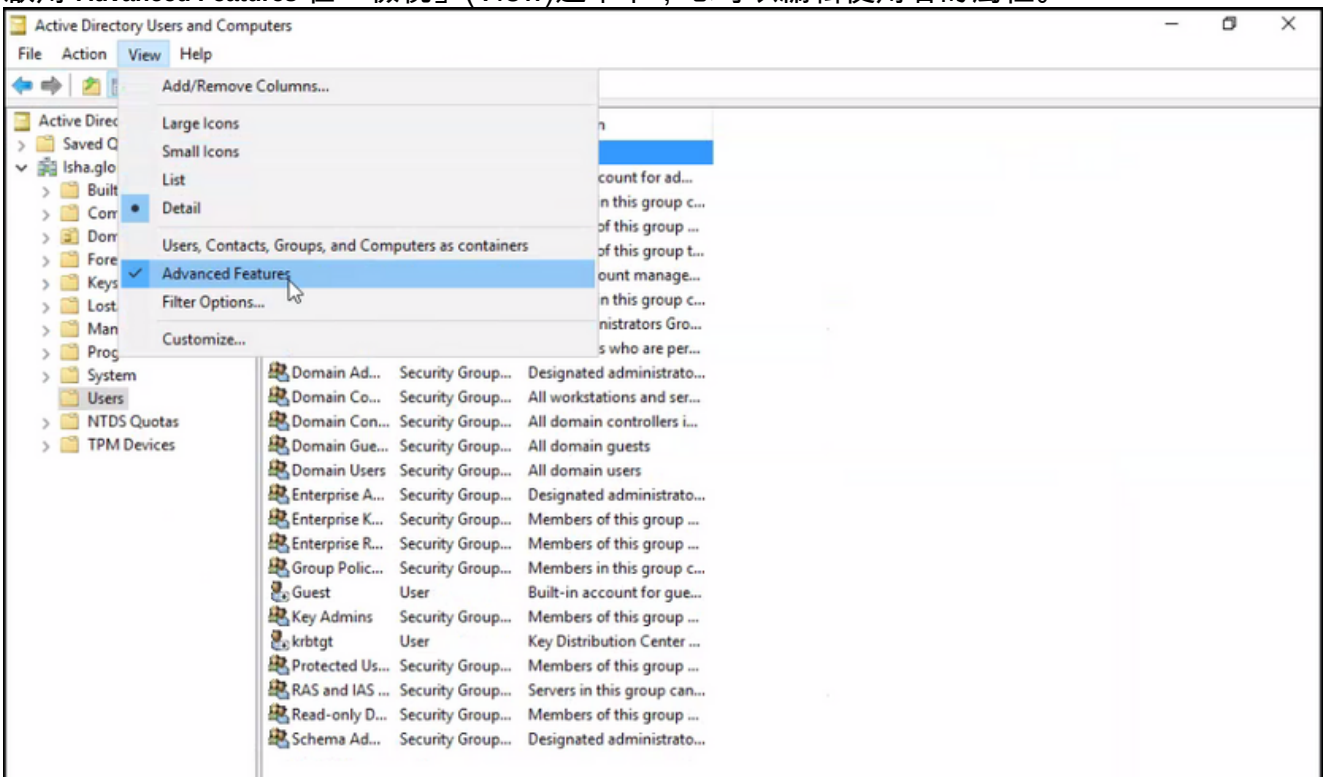
必要條件

您必須已定義Admin使用者，並將其新增到Administrator組中。管理員必須是 **Super Admin** .

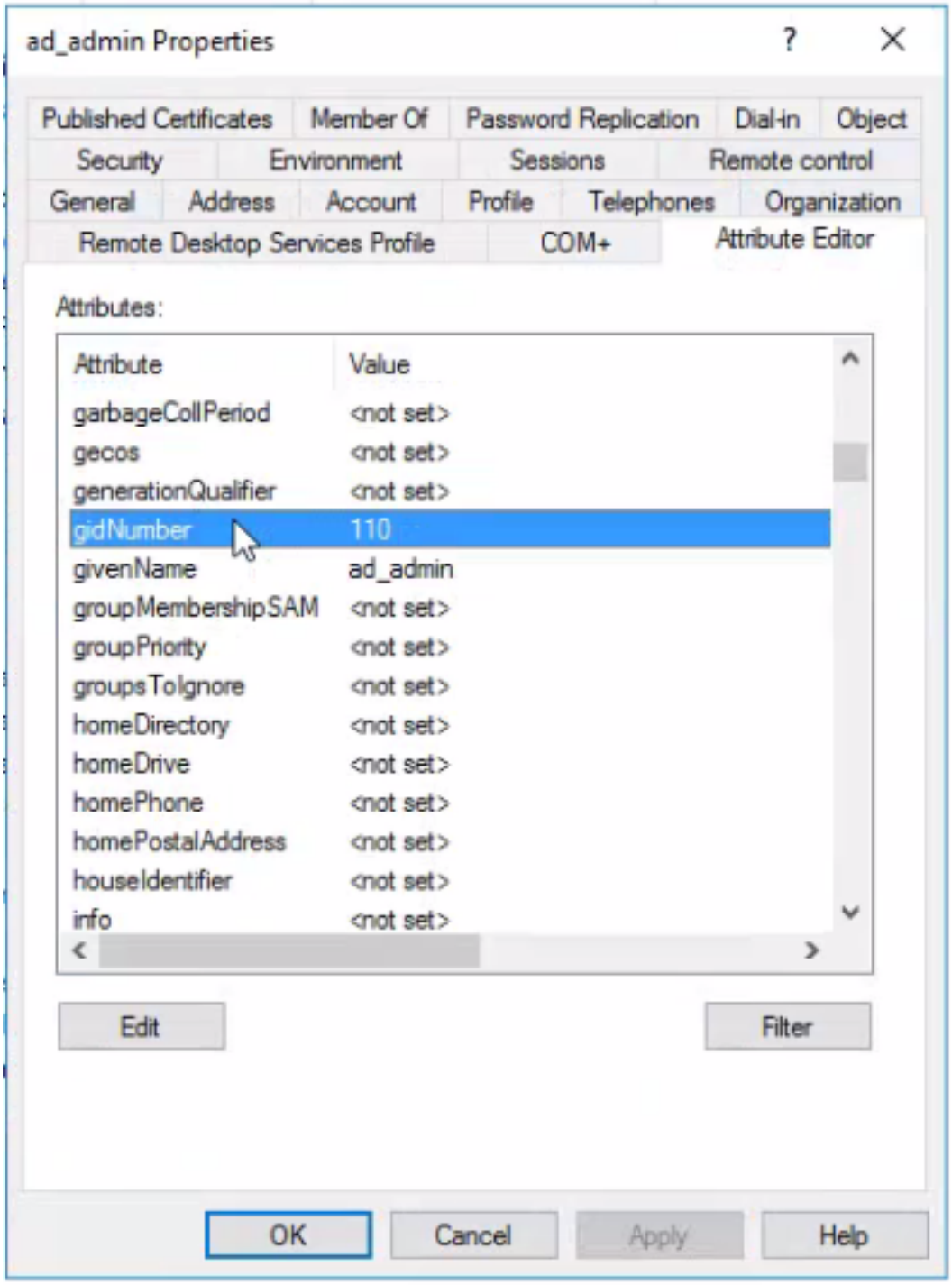
Define the User's Attributes in the AD User Directory

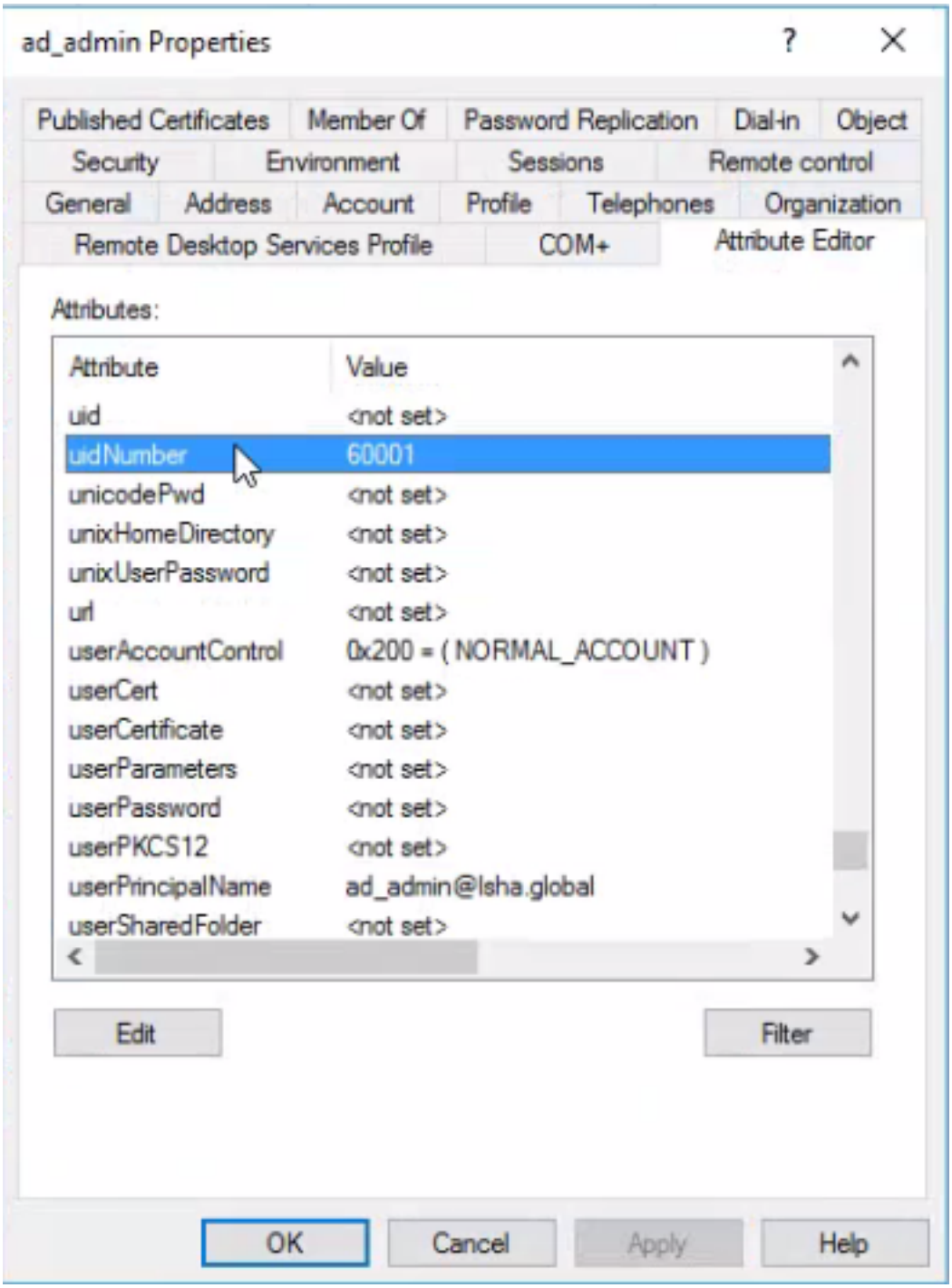
在運行的Windows伺服器上 **Active Directory** 中，修改您計畫配置為CLI管理員的每個使用者的屬性。

1. 開啟 **Server Manager Window** ，然後導航至 **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]**
2. 啟用 **Advanced Features** 在「檢視」(View)選單下，您可以編輯使用者的屬性。



3. 導航到包含Admin使用者的AD組，然後查詢該使用者。
4. 按兩下使用者以開啟 **Properties** 視窗並選擇 **Attribute Editor** .
5. 按一下任何屬性並輸入 **gid** 查詢屬性 **gidNumber** .如果您未找到 **gidNumber** 屬性，按一下 **Filter** 按鈕並取消選中。 僅顯示具有值的屬性。
6. 按兩下屬性名稱以編輯每個屬性。對於每個使用者： 分配 **uidNumber** 大於60000，並確保編號唯一。分配 **gidNumber** 110或111。GidNumber 110表示管理員使用者，而111表示只讀使用者。請勿更改 **uidNumber** 任務之後。如果您修改 **gidNumber** ，請至少等待5分鐘，然後建立SSH連線。


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



將管理員CLI使用者加入AD域

連線到Cisco ISE CLI，運行 **identity-store** 命令，並將Admin使用者分配給ID儲存。

例如，要將CLI管理員使用者對映到ISE中定義為isha.global的Active Directory，請運行以下命令：

identity-store active-directory domain-name

當加入完成時，連線到Cisco ISE CLI並以管理CLI使用者身份登入，以驗證您的配置。

如果您在此命令中使用的域先前已加入ISE節點，則重新加入管理員控制檯中的域。

1. 在Cisco ISE GUI中，按一下 **Menu** 圖示並導航至 **Administration > Identity Management > External Identity Sources** .
2. 在左側窗格中，選擇 **Active Directory** 然後選擇您的廣告名稱。
3. 在右側窗格中，AD連線的狀態可能為 **Operational** .如果使用MS-RPC或Kerberos使用測試使用

者測試連線，則會出現錯誤。
4. 確認您仍可以作為管理員CLI使用者登入思科ISE CLI。

ISE CLI

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

2. 將節點加入域： **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

   如果域 **isha.global** 已通過UI加入，則必須重新加入域 **isha.global** 在此配置之後從UI進行刪除。在重新加入之前，驗證到 **isha.global** 失敗。

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

   已成功加入域isha.global**附註**：

   — 如果域已通過GUI加入，則從GUI重新加入節點，否則針對AD的身份驗證將繼續失敗。

   — 所有節點必須通過CLI單獨加入。**驗證**目前沒有適用於此組態的驗證程序。**疑難排解**

   加入問題在「/var/log/messages file」下可以看到加入操作期間出現的問題以及與此相關的日誌。指令: **show logging system messages工作場景**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**非工作場景由於密碼不正確而導致加入失敗：**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**登入問題**登入期間出現的問題以及與此相關的日誌可在 **/var/log/secure** .指令: show logging system secure **身份驗證成功：**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

由於密碼不正確導致身份驗證失敗：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**由於使用者無效而導致身份驗證失敗：**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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。