# 集成AD，用于ISE GUI和CLI登录

## 目录



## 简介

本文档介绍将Microsoft AD配置为外部身份库以管理访问思科ISE管理GUI和CLI。

## 先决条件

建议掌握下列主题的相关知识：

- 思科ISE版本3.0的配置
- Microsoft广告

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE版本3.0
- Windows Server 2016

本文档介绍Microsoft的配置 **Active Directory (AD)** 作为外部身份库，用于对Cisco **Identity Services Engine (ISE)** 管理GUI和CLI。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

使用此部分可以配置使用Microsoft AD作为外部身份库对思科ISE管理GUI进行管理访问。

ISE节点和AD之间使用以下端口进行此通信：

| 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**：确保AD帐户具有所有所需的权限。

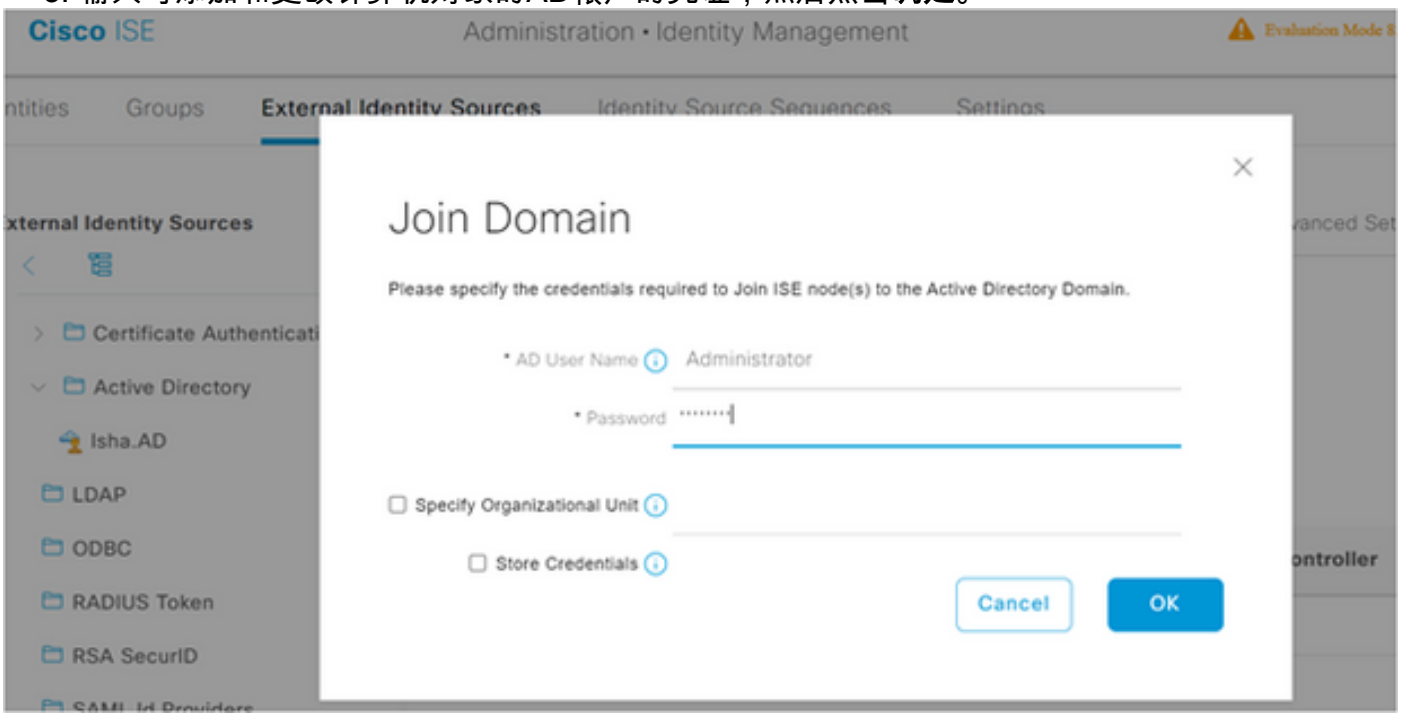
**Active Directory Account Permissions Required for Performing Various Operations**

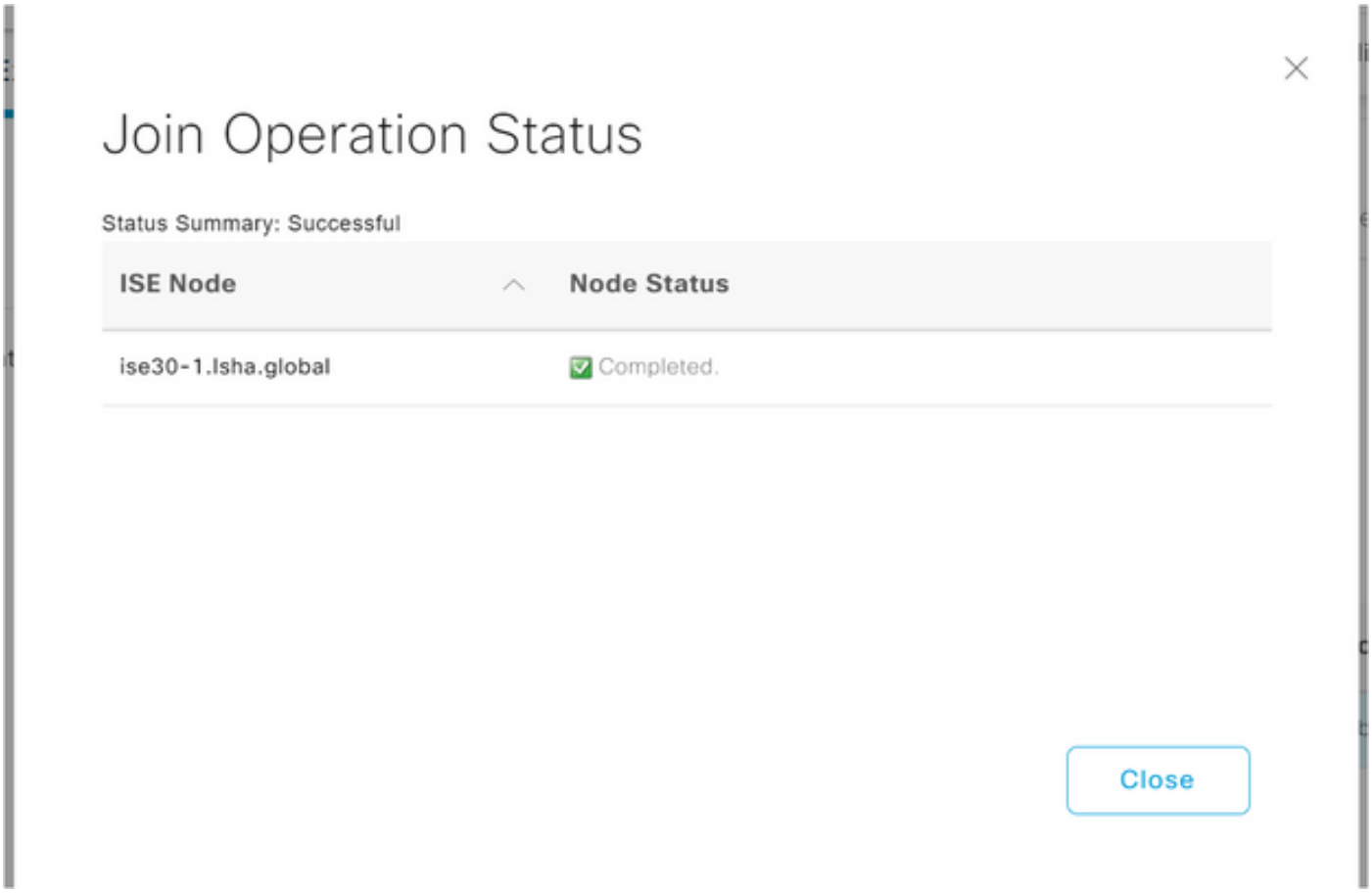
| Join Operations | Leave Operations | Cisco ISE Machine Accounts |
|---|---|---|
| For the account that is used to perform the join operation, the following permissions are required:<br>• Search Active Directory (to see if a Cisco ISE machine account already exists)<br>• Create Cisco ISE machine account to domain (if the machine account does not already exist)<br>• Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)<br>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:<br>• Search Active Directory (to see if a Cisco ISE machine account already exists)<br>• Remove Cisco ISE machine account from domain<br>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:<br>• Ability to change own password<br>• Read the user/machine objects corresponding to users/machines being authenticated<br>• Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.)<br>• Ability to read tokenGroups attribute<br>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.<br>If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join. |

## 将ISE加入AD

1. 导航至 **Administration > Identity Management > External Identity Sources > Active Directory** .
2. 输入新的加入点名称和AD域。

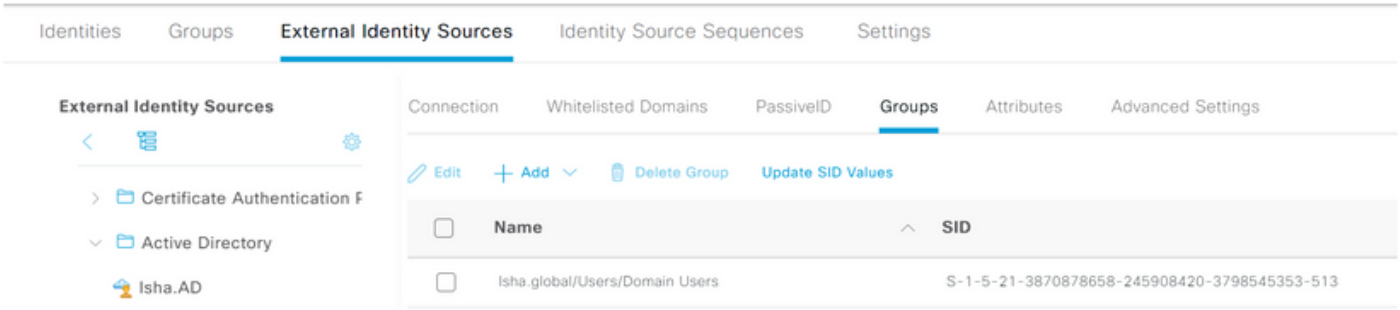
3. 输入可添加和更改计算机对象的AD帐户的凭证，然后点击**确定**。




## 选择目录组

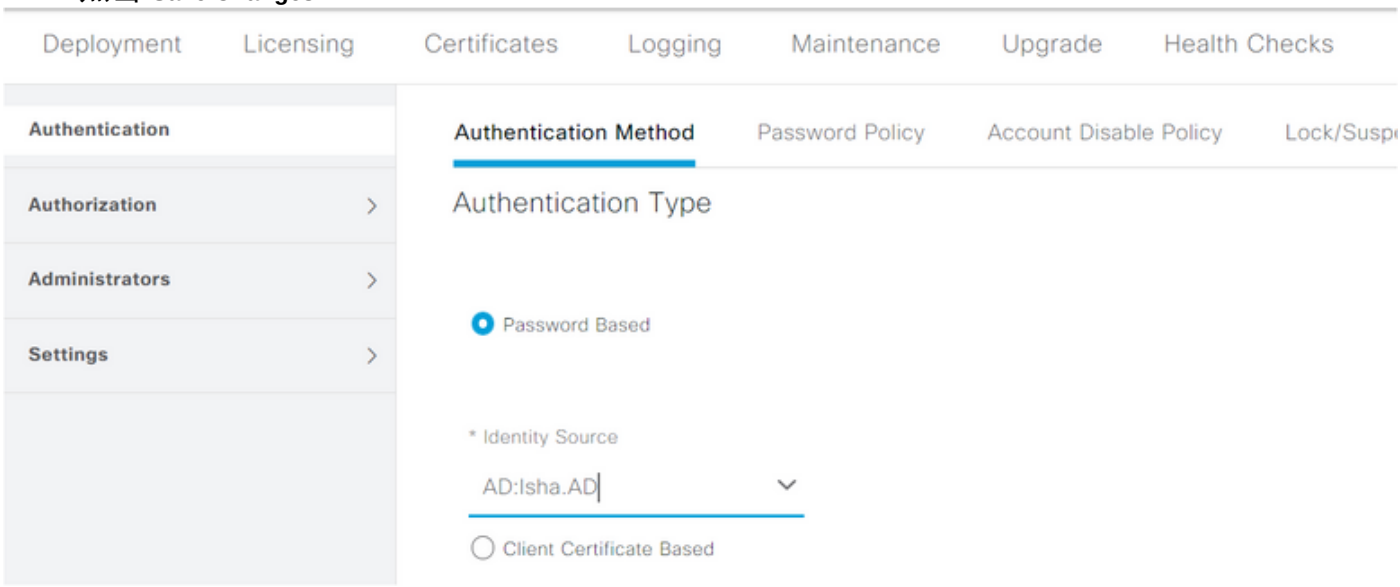
1. 导航至 **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. 导入至少一个管理员所属的AD组。




## 启用AD管理访问

要为AD启用基于密码的身份验证，请完成以下步骤：

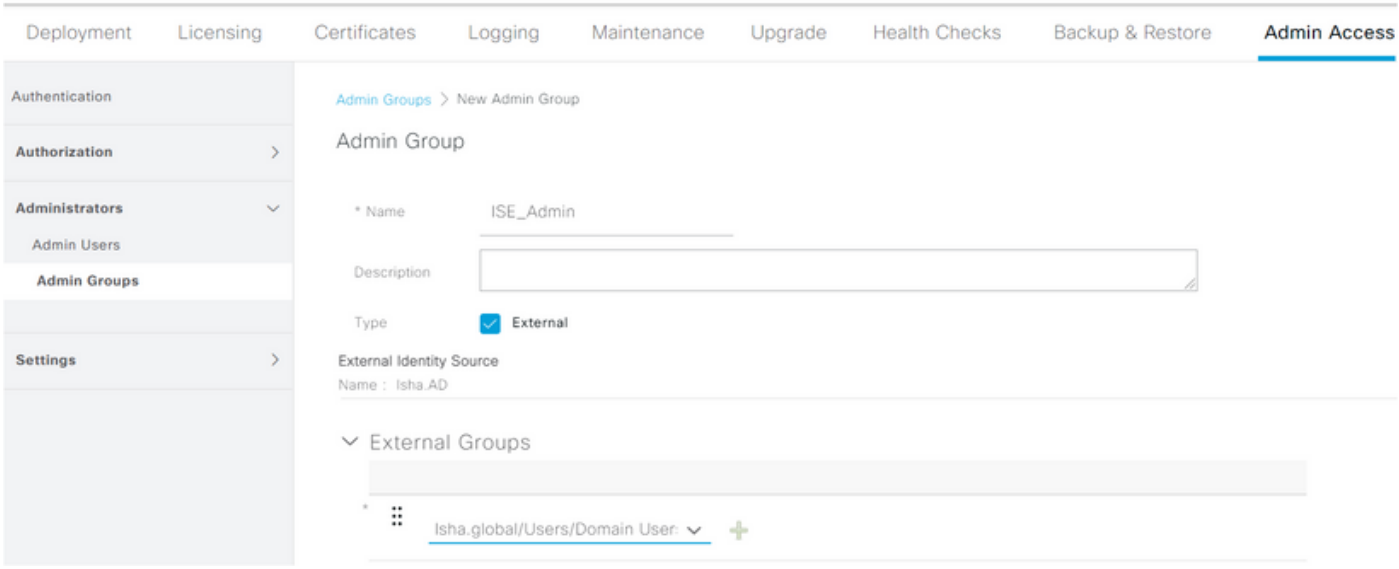
1. 导航至 **Administration > System > Admin Access > Authentication** .
2. 从 **Authentication Method** 选项卡中，选择 **Password Based** 选项.
3. 从AD中选择 **Identity Source** 下拉列表。
4. 点击 **Save Changes** .




## 配置管理员组到AD组的映射

定义Cisco ISE **Admin Group** 并将其映射到AD组。这允许授权确定 **Role Based Access Control (RBAC)** 管理员的权限取决于AD中的组成员身份。

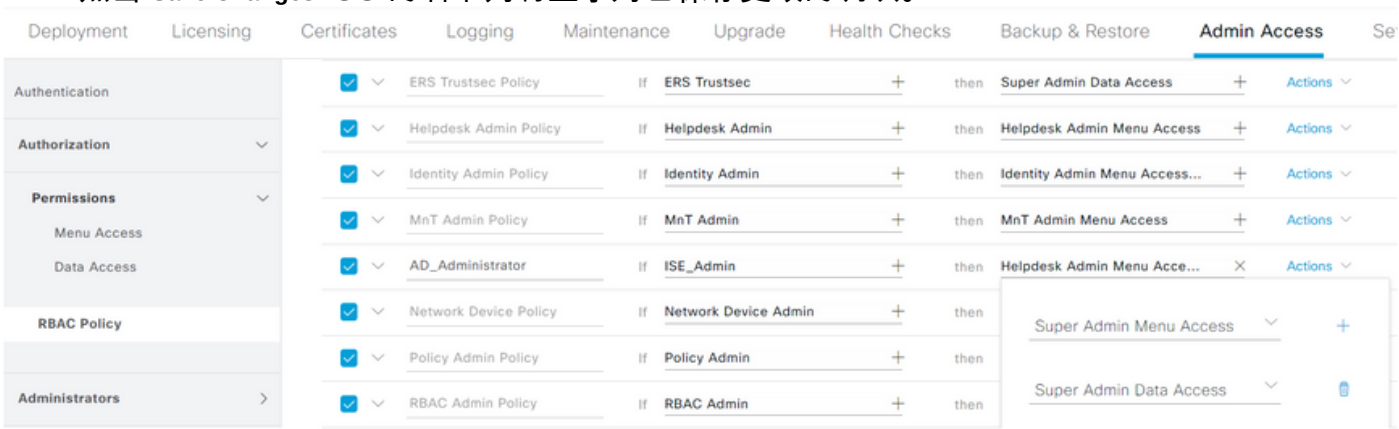
1. 导航至 **Administration > System > Admin Access > Administrators > Admin Groups** .
2. 点击 **Add** 在表头中查看新的 **Admin Group** 配置窗格。
3. 输入新管理员组的名称。
4. 如果 **Type** 字段，请查看 **External** 复选框。
5. 从 **External Groups** 下拉列表中，选择希望此管理员组映射到的AD组，如在 **Select Directory Groups** 部分。
6. 点击 **Save Changes** .




## 设置管理员组的RBAC权限

要将RBAC权限分配到上一节中创建的管理员组，请完成以下步骤：

1. 导航至 **Administration > System > Admin Access > Authorization > Policy** .
2. 从 **Actions** 下拉列表，选择 **Insert New Policy** 添加新策略。
3. 创建一个名为 **AD_Administrator** ，将其与在中定义的管理员组进行映射 **Enable Administrative Access** ，并为其分配权限。 **注意**：在本示例中，分配了名为**Super Admin的**管理组，该组相当于标准管理帐户。
4. 点击 **Save Changes** .GUI的右下角将显示对已保存更改的确认。

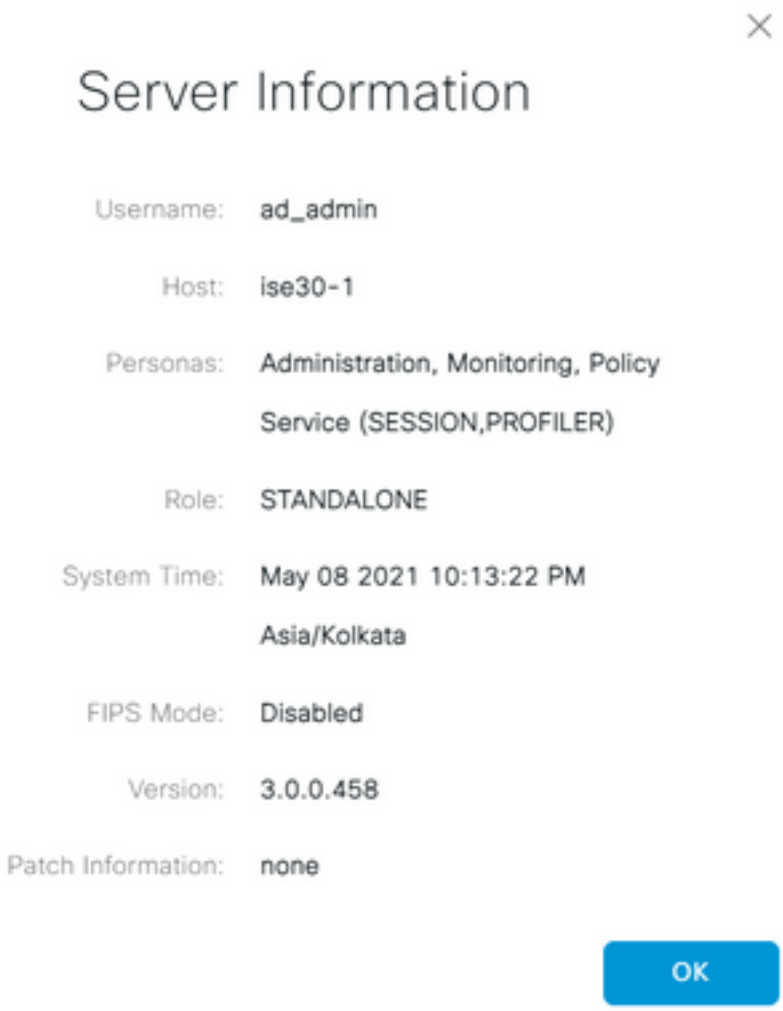



## 使用AD凭证的ISE GUI访问

完成以下步骤，以使用AD凭证访问ISE GUI:

1. 从管理GUI注销。
2. 从**AD**中选择 **Identity Source** 下拉列表。
3. 从AD数据库输入用户名和密码并登录。

**注**：如果AD无法访问，或者使用的帐户凭证在AD中不存在，则ISE默认为内部用户存储。当AD配置为管理访问时，如果您使用内部存储，这有助于快速登录。


## 使用AD凭证的ISE CLI访问

使用外部身份源进行身份验证比使用内部数据库进行身份验证更安全。的RBAC **CLI Administrators** 支持外部身份库。

**注意**:ISE版本2.6及更高版本支持通过外部身份源（如AD）对CLI管理员进行身份验证。

管理单个密码源，无需管理多个密码策略并管理ISE中的内部用户，从而减少时间和工作量。

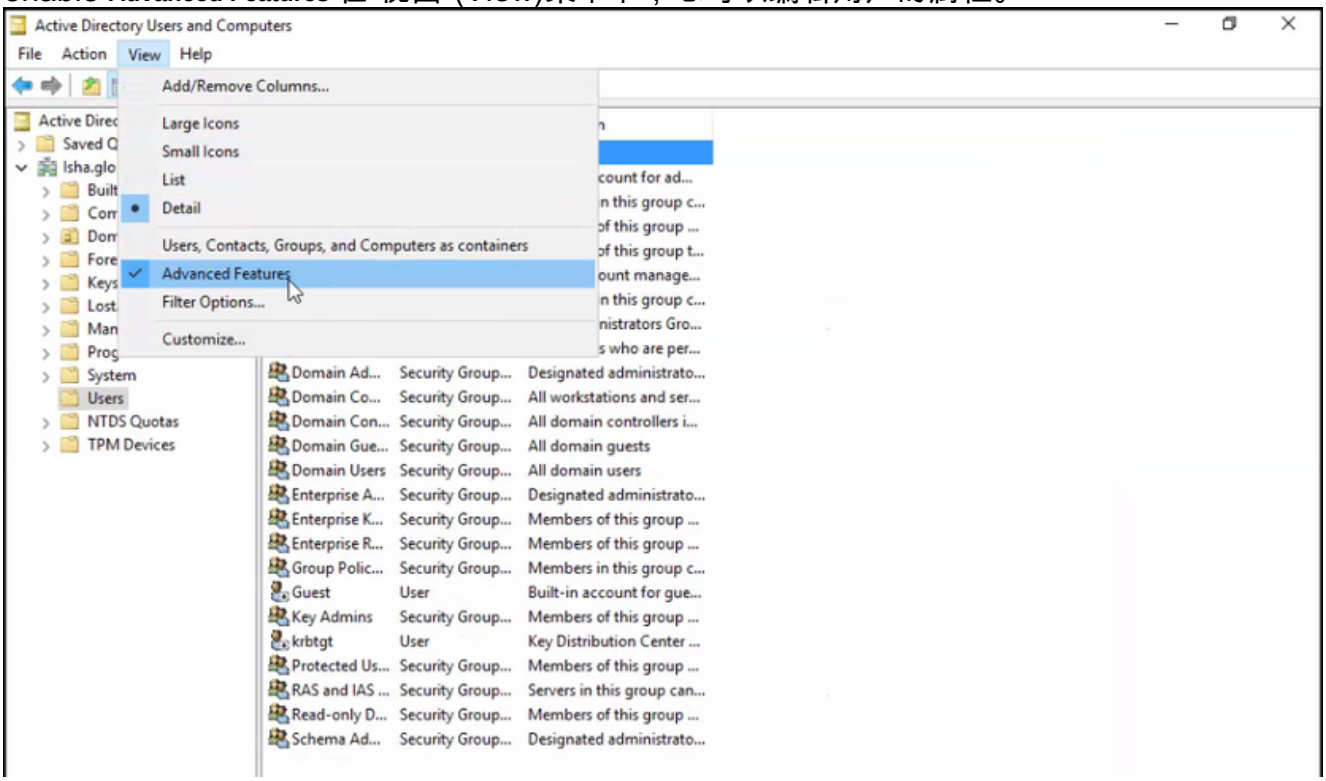
**先决条件**

您必须已经定义管理员用户，并将他们添加到管理员组。管理员必须是 **Super Admin** .

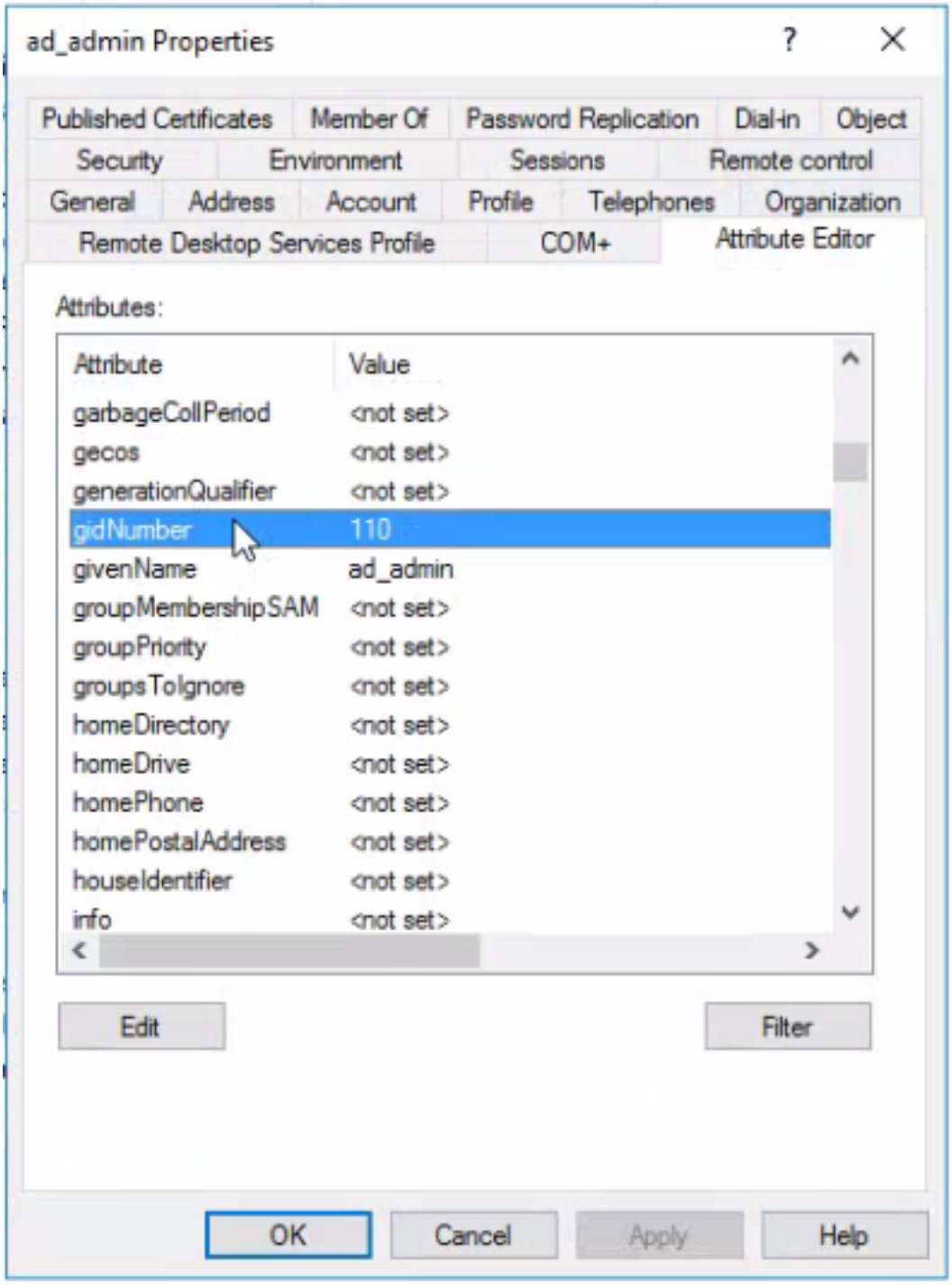
**Define the User's Attributes in the AD User Directory**

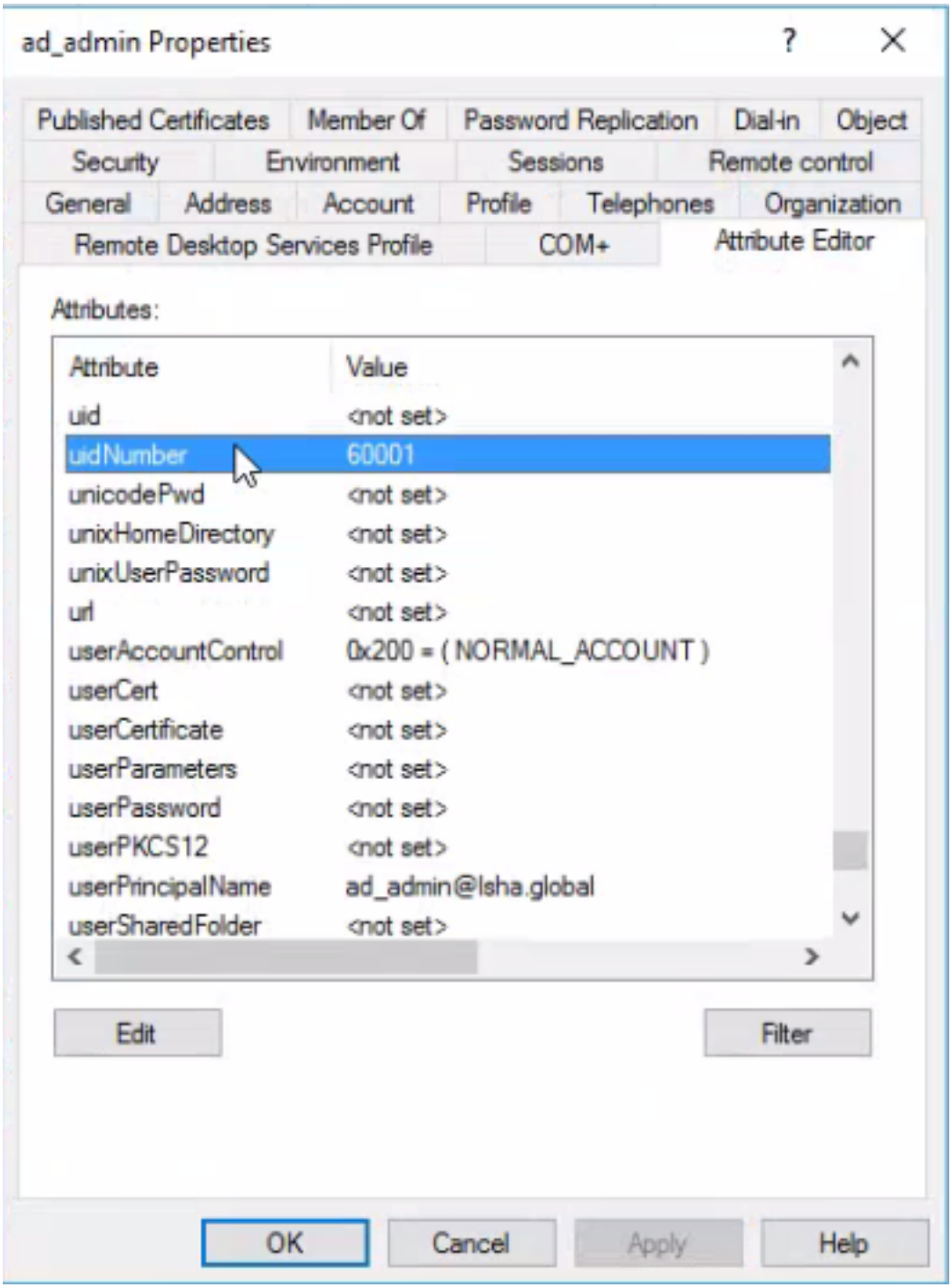
在运行的Windows服务器上 **Active Directory** 修改计划配置为CLI管理员的每个用户的属性。

1. 打开 **Server Manager Window** ，并导航至 **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ ad.adserver ]**
2. enable **Advanced Features** 在"视图"(View)菜单下，您可以编辑用户的属性。




3. 导航到包含管理员用户的AD组并查找该用户。
4. 双击用户以打开 **Properties** 窗口并选择 **Attribute Editor** .
5. 点击任何属性并输入 **gid** 查找属性 **gidNumber** .如果您未找到 **gidNumber** 属性，点击 **Filter** 按钮并取消选中。 仅显示具有值的属性。
6. 双击属性名称以编辑每个属性。对于每个用户： 分配 **uidNumber** 大于60000，请确保编号唯一。分配 **gidNumber** as 110或111。GidNumber 110表示管理员用户，111表示只读用户。请勿更改 **uidNumber** 作业后。如果修改 **gidNumber** ，请至少等待5分钟，然后建立SSH连接。


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




**将管理员CLI用户加入AD域**

连接到Cisco ISE CLI，运行 **identity-store** 命令，并将Admin用户分配给ID存储。

例如，要将CLI管理员用户映射到ISE中定义为isha.global的Active Directory，请运行以下命令：

**identity-store active-directory domain-name**

加入完成后，连接到Cisco ISE CLI并以管理员CLI用户身份登录，以验证您的配置。

如果在此命令中使用的域之前已加入ISE节点，则重新加入管理员控制台中的域。

1. 在Cisco ISE GUI中，点击 **Menu** 图标并导航至 **Administration > Identity Management > External Identity Sources** .
2. 在左侧窗格中，选择 **Active Directory** 并选择您的AD名称。
3. 在右侧窗格中，您的AD连接的状态可能为 **Operational** .如果使用MS-RPC或Kerberos测试与测

试用户的连接，则会出错。
4. 验证您仍可以作为管理员CLI用户登录思科ISE CLI。

## ISE CLI

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

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

   如果域 **isha.global** 已通过UI加入，则必须重新加入域 **isha.global** 配置后，从UI。在重新加入之前，身份验证到 **isha.global** 失败。

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

   已成功加入域isha.global**注意：**

   — 如果域已通过GUI加入，则从GUI重新加入节点，否则，针对AD的身份验证继续失败。

   — 所有节点必须通过CLI单独加入。**验证**当前没有可用于此配置的验证过程。**故障排除加入问题**在“/var/log/messages file”下可以看到加入操作期间出现的问题以及与此相关的日志。命令: **show logging system messages工作场景**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**非工作场景由于密码不正确而导致加入失败：**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**登录问题**登录期间出现的问题以及与此相关的日志可在 **/var/log/secure** .命令: show logging system secure **成功的身份验证：**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

**由于密码不正确导致身份验证失败：**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**由于用户无效而导致身份验证失败：**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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。