ISE GUIおよびCLIログイン用のADの統合

内容

概要

このドキュメントでは、Cisco ISE管理GUIおよびCLIへの管理アクセス用の外部IDストアとしてのMicrosoft ADの設定について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco ISEバージョン3.0の設定
- Microsoft AD

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.0
- Windows Server 2016

このドキュメントでは、Microsoftの設定について説明します **Active Directory (AD)** 外部IDストアとして提供され、シスコへの管理アクセスを可能にする **Identity Services Engine (ISE)** 管理GUIおよびCLI。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく

ださい。

設定

このセクションでは、Cisco ISE管理GUIへの管理アクセス用の外部IDストアとしてMicrosoft ADを使用するように設定します。

この通信では、ISEノードとADの間で次のポートが使用されます。

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

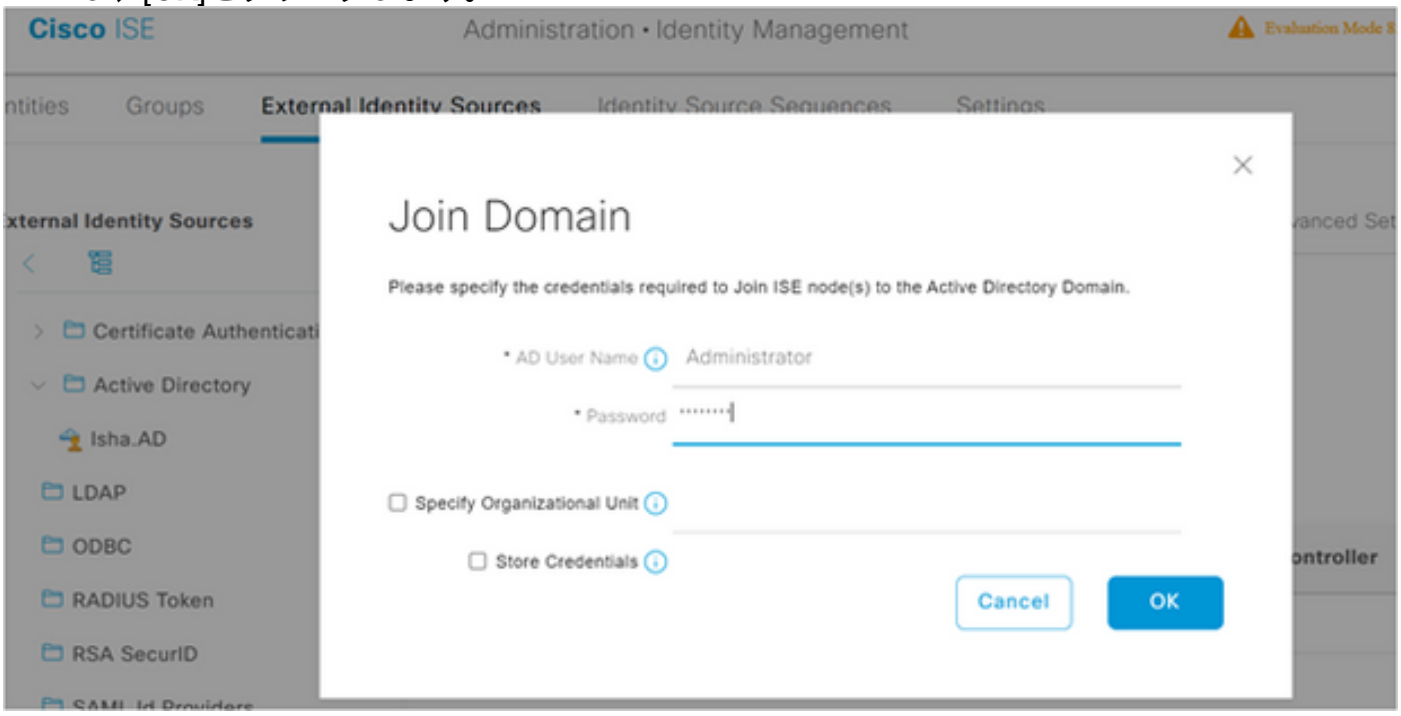
注：ADアカウントに必要なすべての権限があることを確認します。

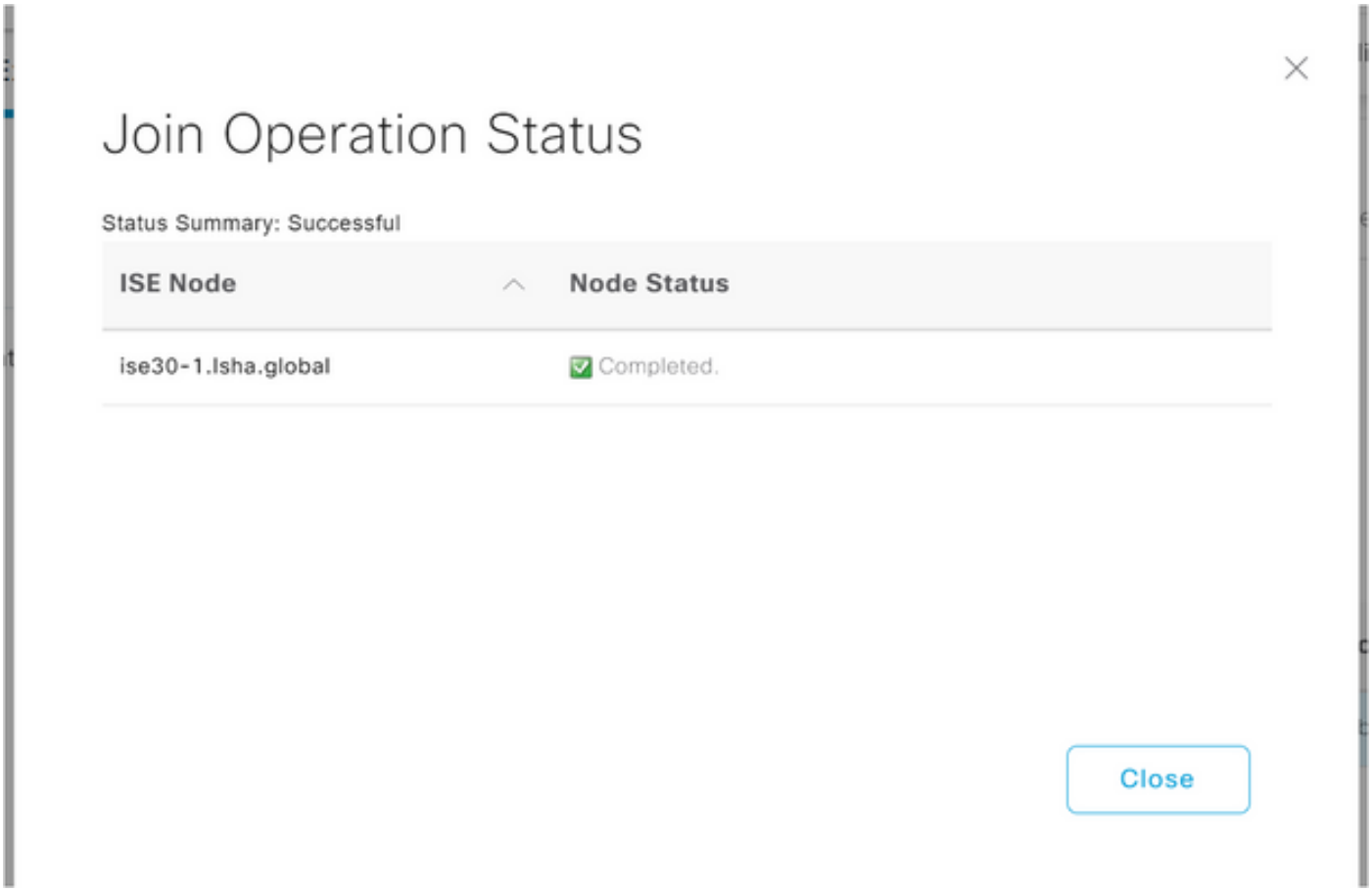
Active Directory Account Permissions Required for Performing Various Operations

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.

AD への ISE の結合

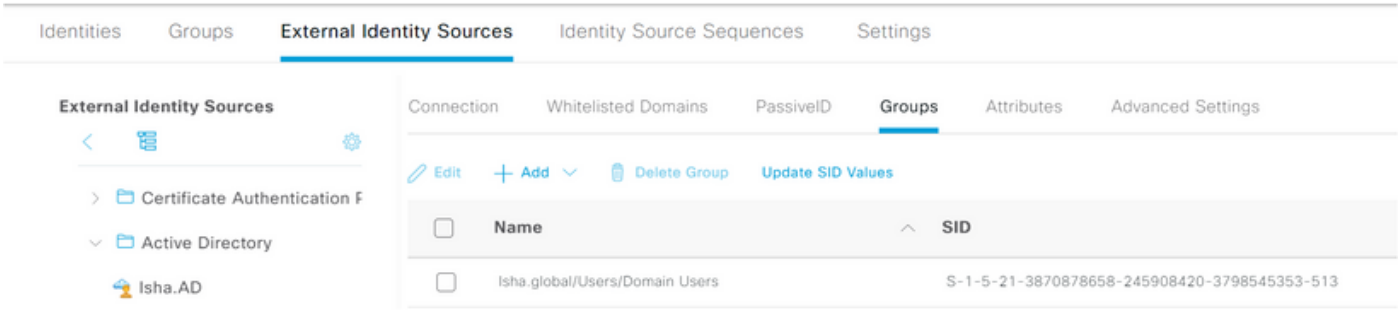
1. 移動先 **Administration > Identity Management > External Identity Sources > Active Directory** .
2. 新しい参加ポイント名とADドメインを入力します。
3. コンピュータオブジェクトを追加および変更できるADアカウントのクレデンシャルを入力し、[OK]をクリックします。





ディレクトリ グループの選択

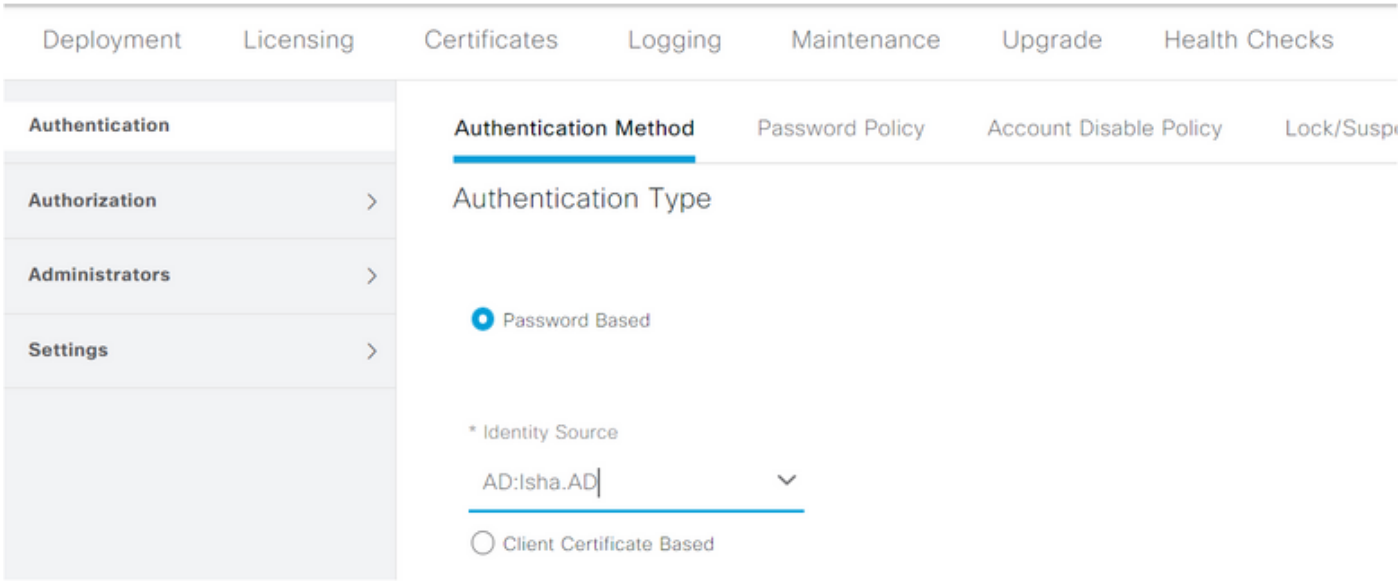
1. 移動先 **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. 管理者が属する 1 つ以上の AD グループをインポートします。



AD 用管理アクセスの有効化

AD のパスワード ベースの認証を有効にするには、次の手順を実行してください。

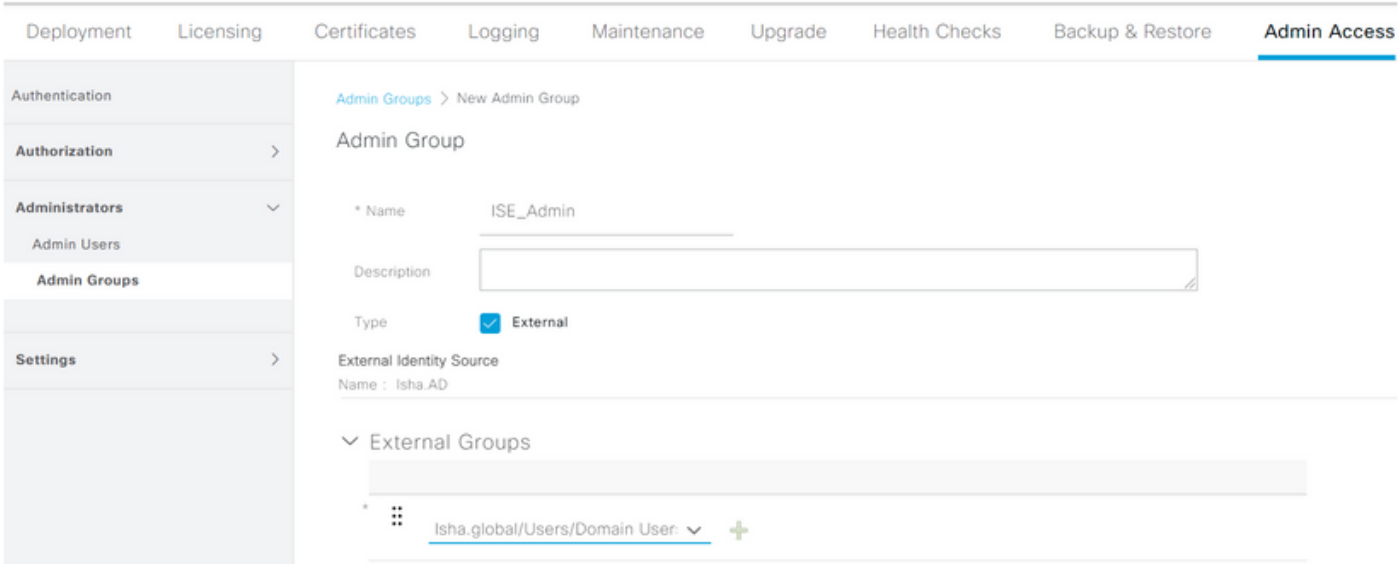
1. 移動先 **Administration > System > Admin Access > Authentication** .
2. **Authentication Method** タブを選択し、 **Password Based** オプション.
3. [Add] を選択します。 **Identity Source** 選択します。
4. クリック **Save Changes** .



管理グループから AD グループへのマッピングの設定

Cisco ISEの定義 **Admin Group** ADグループにマッピングします。これにより、認証でIPアドレスが **Role Based Access Control (RBAC)** adのグループメンバーシップに基づく管理者の権限。

1. 移動先 **Administration > System > Admin Access > Administrators > Admin Groups** .
2. クリック **Add** テーブルのヘッダーに表示されます。 **Admin Group** Configurationペイン。
3. 新しい管理グループの名前を入力します。
4. 内 **Type** フィールドをチェックし、 **External** チェックボックスをオンにします。
5. **External Groups** ドロップダウンリストから、この管理グループをマッピングするADグループを選択します。ADグループの定義は、 **Select Directory Groups** 。
6. クリック **Save Changes** .

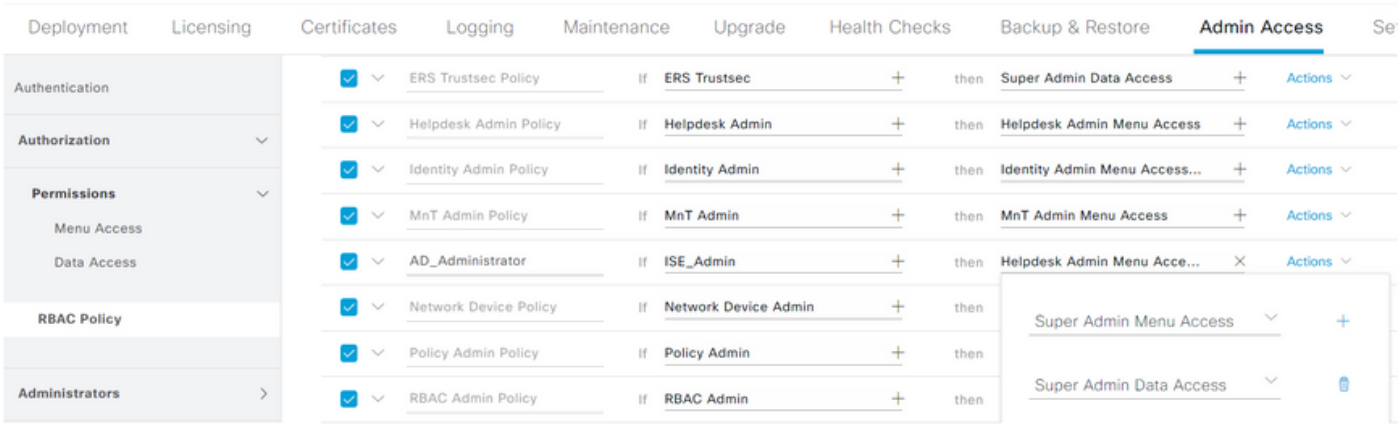


管理グループの RBAC アクセス許可の設定

前のセクションで作成した管理グループに RBAC の権限を割り当てるには、次の手順を実行してください。

1. 移動先 **Administration > System > Admin Access > Authorization > Policy** .
2. **Actions** 右側のドロップダウンリストから、 **Insert New Policy** 新しいポリシーを追加します。

3. という名前の新しいルールの作成 **AD_Administrator** で定義されているAdmin Groupにマッピングします。 **Enable Administrative Access** ADセクションにアクセス権を割り当てます。 **注**：この例では、**Super Admin**という名前のAdmin Groupが割り当てられています。これは標準のadminアカウントに相当します。
4. クリック **Save Changes** .保存された変更の確認は、GUIの右下隅に表示されます。

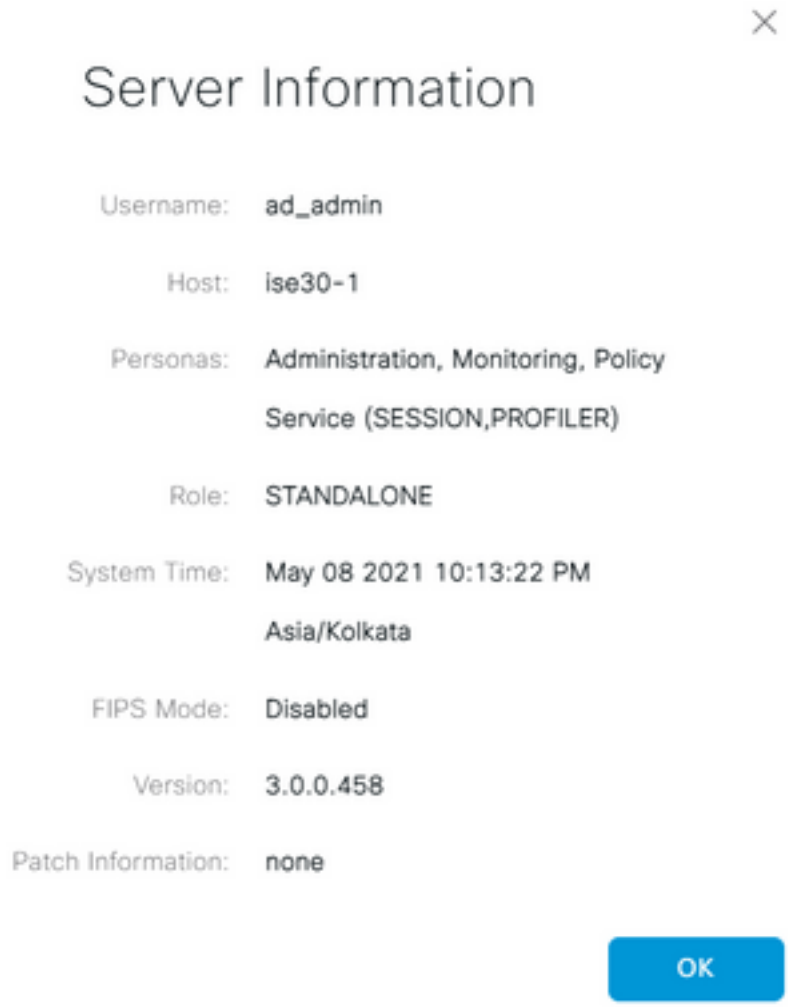


ADクレデンシャルを使用したISE GUIアクセス

ADクレデンシャルを使用してISE GUIにアクセスするには、次の手順を実行します。

1. 管理 GUI からログアウトします。
2. [Add] を選択します。 **Identity Source** 選択します。
3. ADデータベースからユーザ名とパスワードを入力し、ログインします。

注:ADに到達できない場合、または使用されているアカウントのクレデンシャルがADに存在しない場合、ISEはデフォルトで内部ユーザストアに設定されます。これにより、AD が管理アクセス用に設定されているときには、内部ストアを使用すると、クイック ログインが促進されます。



ADクレデンシャルを使用したISE CLIアクセス

外部アイデンティティソースを使用した認証は、内部データベースを使用した認証よりも安全です。RBAC **CLI Administrators** は、外部IDストアをサポートしています。

> **注**：ISEバージョン2.6以降では、ADなどの外部アイデンティティソースによるCLI管理者の認証がサポートされています。

複数のパスワードポリシーを管理したり、ISE内で内部ユーザを管理したりする必要がなく、単一のパスワードソースを管理できるため、時間と労力を削減できます。

前提条件

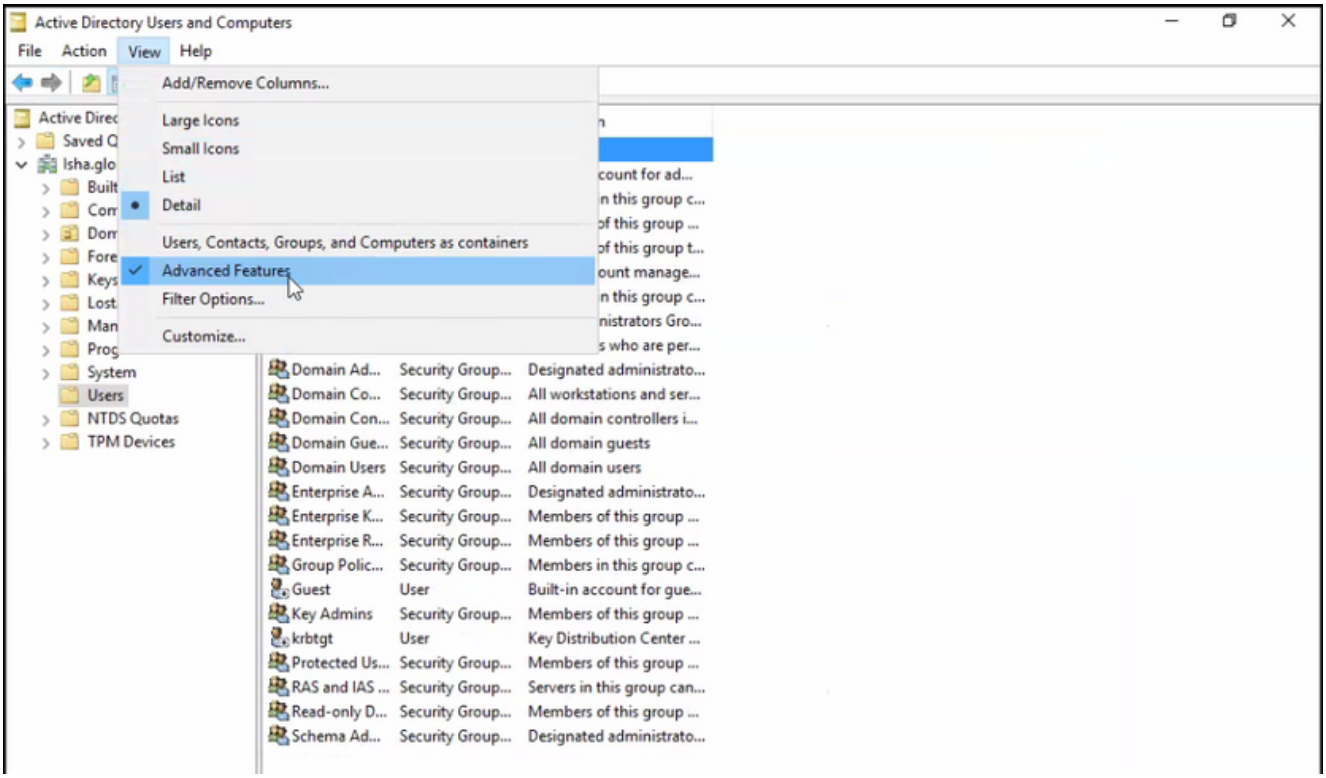
管理者ユーザを定義し、管理者グループに追加しておく必要があります。Adminは **Super Admin** .

Define the User's Attributes in the AD User Directory

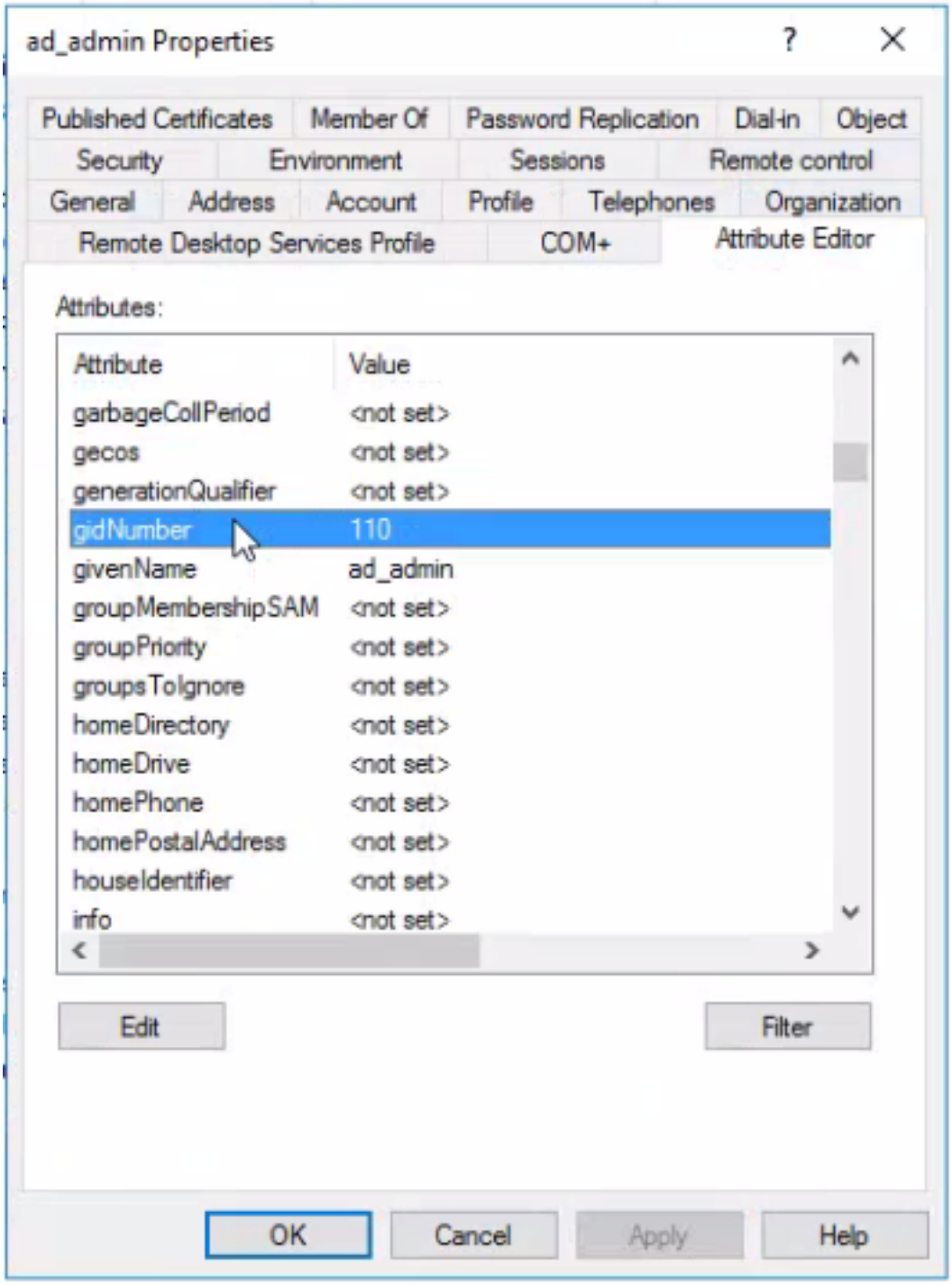
を実行するWindowsサーバ **Active Directory** を選択し、CLI管理者として設定する予定の各ユーザの属性を変更します。

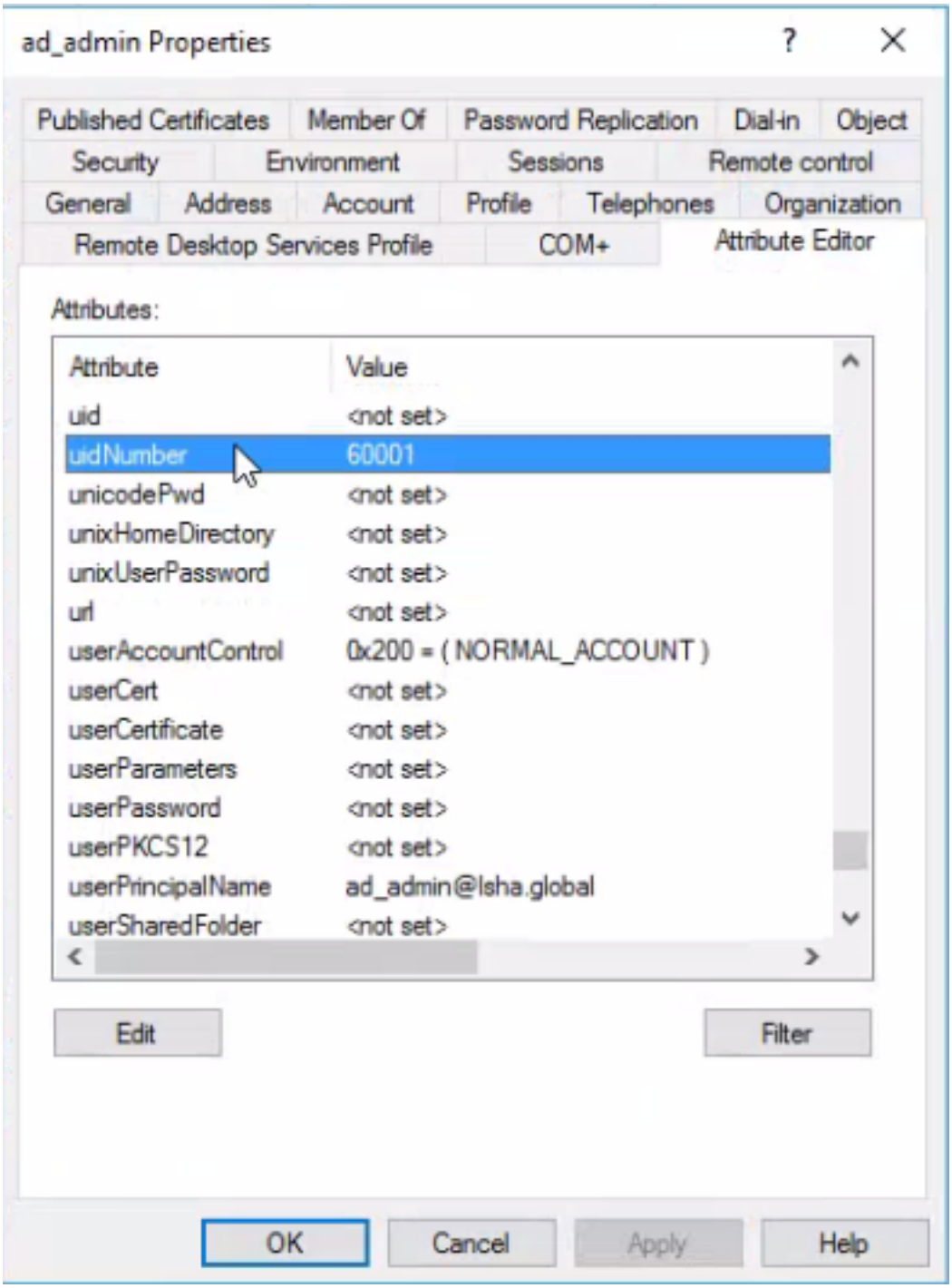
1. を開きます。 **Server Manager Window** をクリックし、 **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]**

2. Enable **Advanced Features** ユーザの属性を編集できるように、[View]メニューの下に表示されます。



3. Adminユーザを含むADグループに移動し、そのユーザを見つけます。
4. ユーザをダブルクリックして、 **Properties** ウィンドウを開き、 **Attribute Editor** .
5. 任意の属性をクリックし、次のように入力します。 **gid** 属性を検索するには **gidNumber** .Cisco Unified Communications Managerが見つからない場合、 **gidNumber** 属性を選択し、 **Filter** ボタンをクリックし、チェックマークを外します。 値を持つ属性のみを表示します。
6. 属性名をダブルクリックして、各属性を編集します。ユーザごとに次の手順を実行します。 Assign **uidNumber** 60000より大きい値を指定し、一意の番号であることを確認します。 Assign **gidNumber** 110または111として設定します。GidNumber 110はadminユーザを表し、111は読み取り専用ユーザを表します。変更しないでください。 **uidNumber** 割り当て後。この設定を変更すると、 **gidNumber** SSH接続を確立する前に、少なくとも5分間待ちます。


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



Admin CLIユーザのADドメインへの参加

Cisco ISE CLIに接続し、 **identity-store** コマンドを実行し、IDストアにAdminユーザを割り当てます。

たとえば、CLI管理ユーザをISEでisha.globalとして定義されているActive Directoryにマッピングするには、次のコマンドを実行します。

identity-store active-directory domain-name

参加が完了したら、Cisco ISE CLIに接続し、Admin CLIユーザとしてログインして設定を確認します。

このコマンドで使用するドメインが以前にISEノードに参加していた場合は、管理者コンソールでドメインに再度参加します。

1. Cisco ISE GUIで、 **Menu** アイコンをクリックし、 **Administration > Identity Management > External Identity Sources** .
2. 左側のペインで、 **Active Directory** AD名を選択します。
3. 右側のペインで、AD接続のステータスが次のように表示されます **Operational** .MS-RPCまたはKerberosを使用してテストユーザを使用して接続をテストすると、エラーが発生します。
4. Admin CLIユーザとしてCisco ISE CLIにログインできることを確認します。

ISE CLI

1. ISE CLIにログインします。

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

2. ノードをドメインに参加させます。 **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

   ドメインが **isha.global** はUIを介してすでに参加しているため、ドメインに再度参加する必要があります **isha.global** この設定後にUIから読み込みます。再参加が発生するまで、認証は **isha.global** 失敗します。

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

   ドメインisha.globalに正常に参加しました**注：**

   – ドメインがすでにGUI経由で参加している場合は、GUIからノードに再参加します。そうでない場合は、ADに対する認証が失敗し続けます。

   - CLIを使用してすべてのノードを個別に結合する必要があります。**確認**現在、この設定に使用できる確認手順はありません。**トラブルシュート参加の問題**参加操作中の問題と、これに関連するログは「/var/log/messages file」の下に表示されます。コマンド：

   show logging system messages正常動作シナリオ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**動作しないシナリオ**

パスワードが正しくないため、参加に失敗しました：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**ログインの問題**ログ

インの問題と、これに関連するログは、次のURLで確認できます。 **/var/log/secure** .コマンド

： show logging system secure **正常な認証：**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

パスワードの誤りによる認証の失敗：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**無効なユーザによる認証エラー：**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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。