Intégration d'AD pour interface utilisateur ISE et connexion CLI

Table des matières

Introduction

Ce document décrit la configuration de Microsoft AD en tant que magasin d'identités externe pour l'accès administratif à l'interface utilisateur graphique et à l'interface de ligne de commande de gestion Cisco ISE.

Conditions préalables

Cisco recommande de connaître les sujets suivants :

- Configuration de Cisco ISE version 3.0
- Microsoft AD

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ISE version 3.0
- Windows Server 2016

Ce document décrit la configuration de Microsoft **Active Directory (AD)** en tant que magasin d'identités externe pour l'accès administratif à Cisco **Identity Services Engine (ISE)** GUI et CLI de gestion.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Utilisez cette section afin de configurer l'utilisation de Microsoft AD comme magasin d'identités externe pour l'accès administratif à l'interface utilisateur graphique de gestion Cisco ISE.

Ces ports sont utilisés entre le noeud ISE et AD pour cette communication :

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

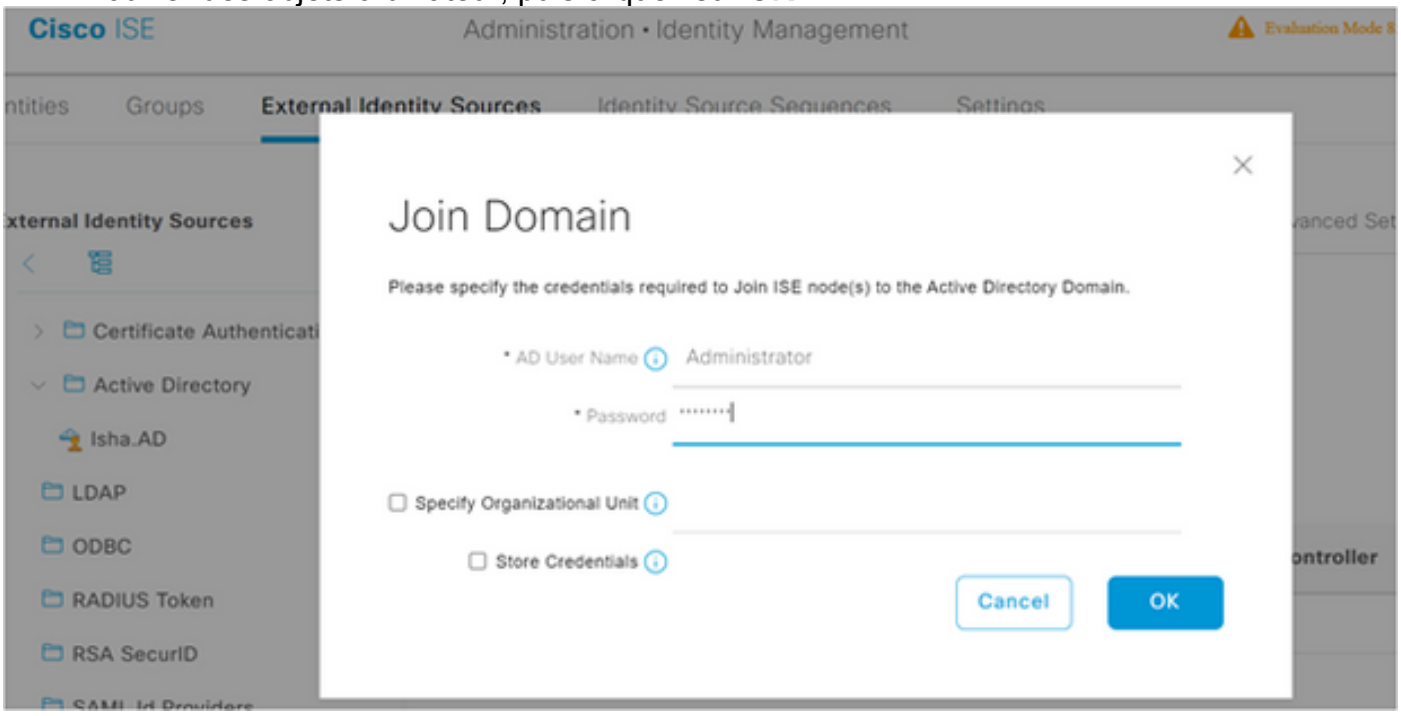
Remarque : assurez-vous que le compte AD dispose de tous les privilèges requis.

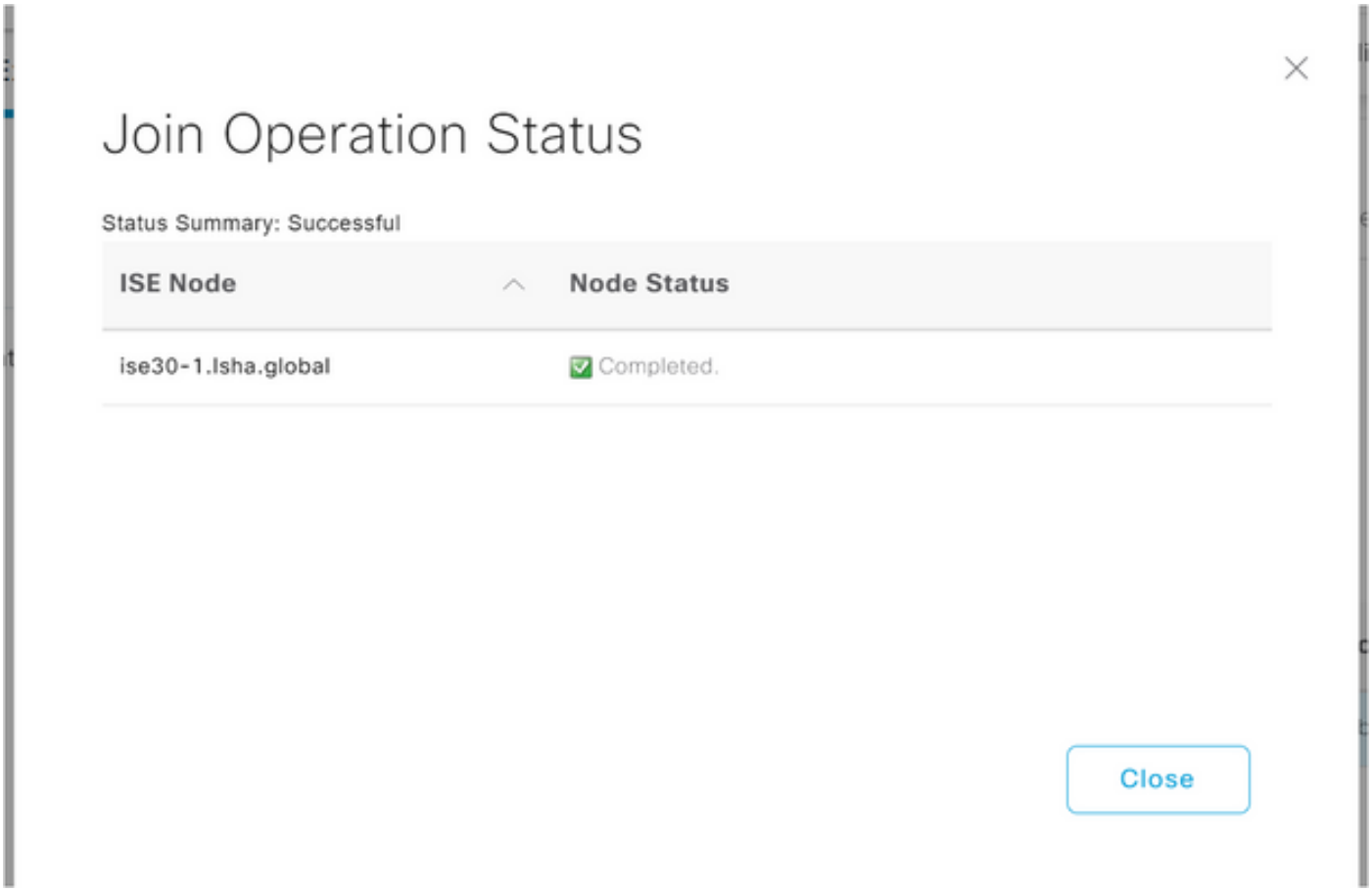
Active Directory Account Permissions Required for Performing Various Operations

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.

Rejoindre ISE à AD

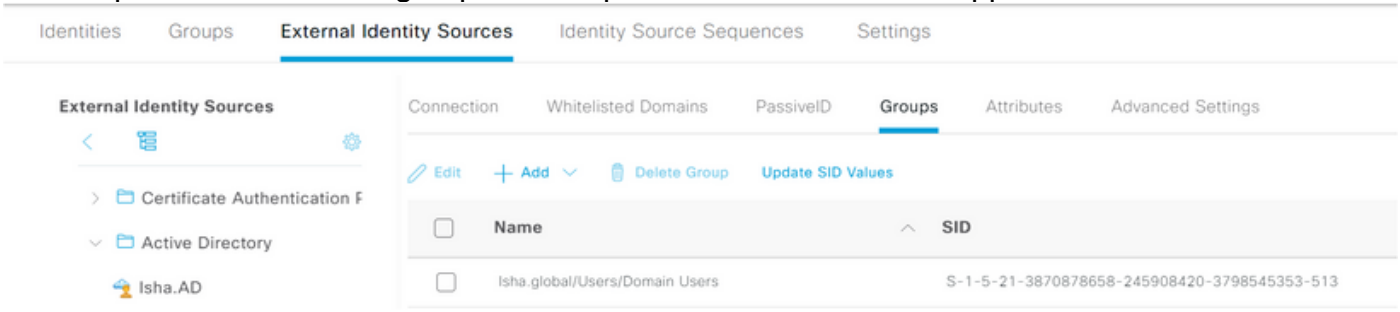
1. Naviguez jusqu'à **Administration > Identity Management > External Identity Sources > Active Directory** .
2. Entrez le nouveau nom du point de jointure et le domaine Active Directory.
3. Entrez les informations d'identification du compte Active Directory qui peuvent ajouter et modifier des objets ordinateur, puis cliquez sur **OK**.





Sélectionner des groupes de répertoires

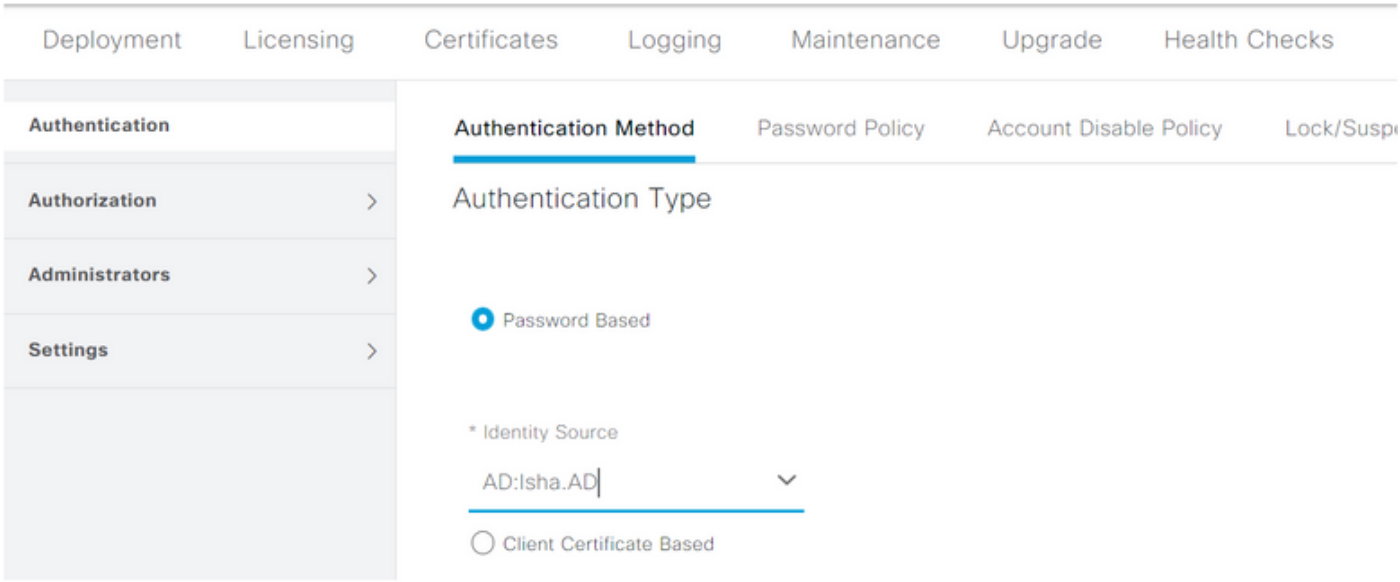
1. Naviguez jusqu'à **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. Importez au moins un groupe AD auquel votre administrateur appartient.



Activer l'accès administratif pour AD

Complétez ces étapes afin d'activer l'authentification par mot de passe pour AD :

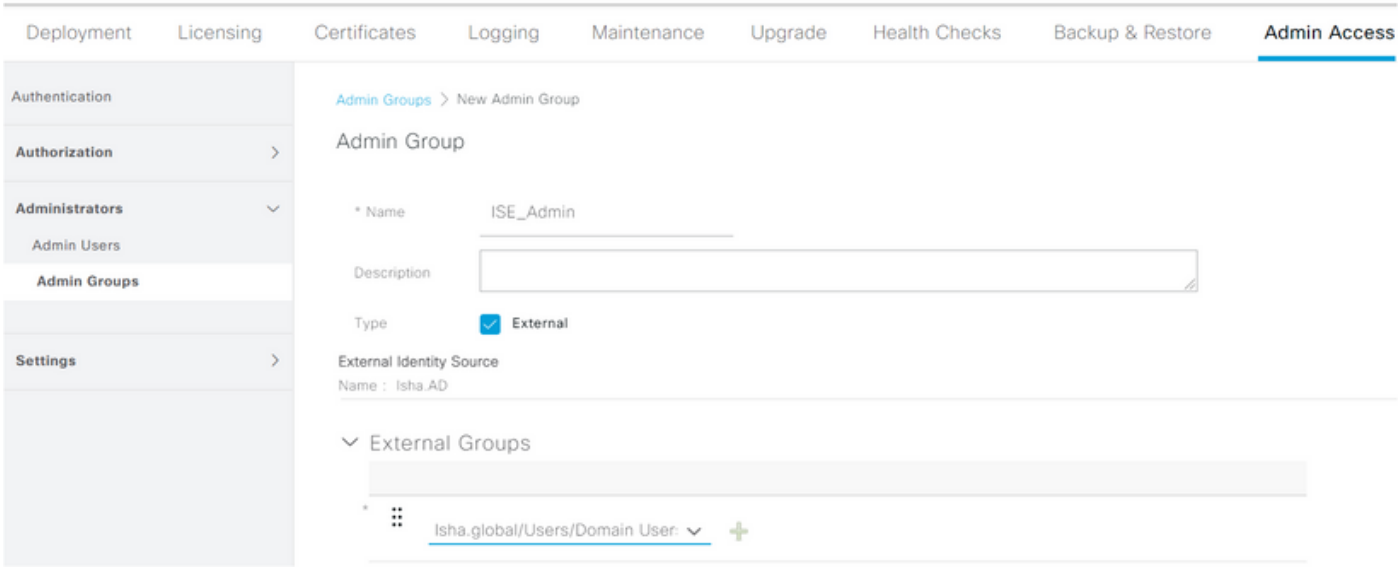
1. Naviguez jusqu'à **Administration > System > Admin Access > Authentication** .
2. A partir des versions **Authentication Method** , sélectionnez l'option **Password Based** de l'assistant.
3. Sélectionnez **AD** dans la liste **Identity Source** liste déroulante.
4. Cliquer **Save Changes** .



Configurer le mappage du groupe Admin au groupe AD

Définir un Cisco ISE **Admin Group** et mappez-le à un groupe AD. Cela permet d'obtenir l'autorisation de **Role Based Access Control (RBAC)** autorisations de l'administrateur en fonction de l'appartenance à un groupe dans Active Directory.

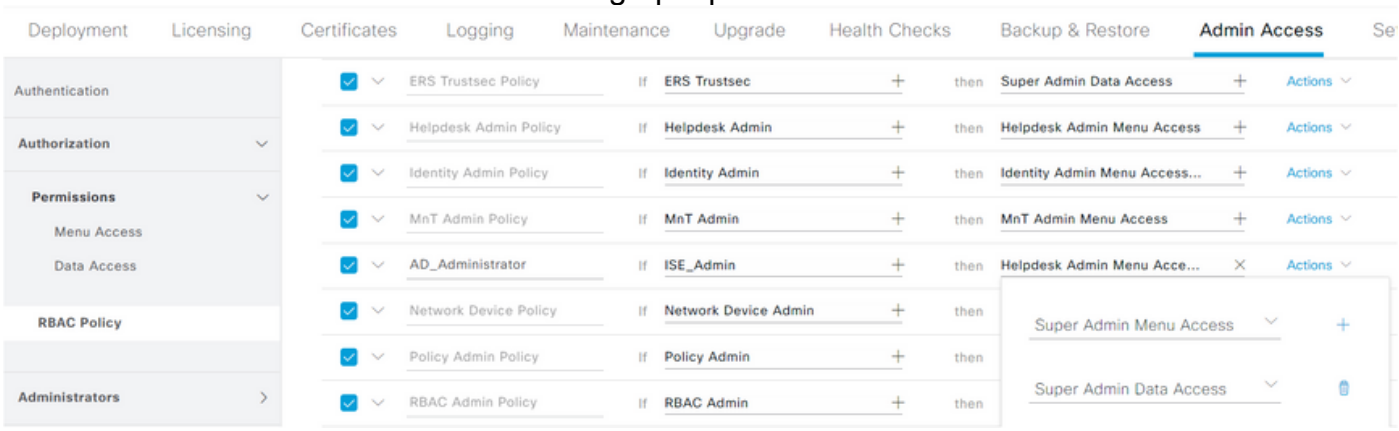
1. Naviguez jusqu'à **Administration > System > Admin Access > Administrators > Admin Groups** .
2. Cliquer **Add** dans l'en-tête du tableau afin d'afficher le nouveau **Admin Group** volet de configuration.
3. Entrez le nom du nouveau groupe Admin.
4. Dans la **Type** , cochez la case **External** de l'Aide.
5. A partir des versions **External Groups** , choisissez le groupe Active Directory auquel vous souhaitez que ce groupe d'administrateurs soit mappé, comme défini dans la **Select Directory Groups** de l'Aide.
6. Cliquer **Save Changes** .



Définir les autorisations RBAC pour le groupe Admin

Complétez ces étapes afin d'attribuer des autorisations RBAC aux groupes d'administration créés dans la section précédente :

1. Naviguez jusqu'à **Administration > System > Admin Access > Authorization > Policy** .
2. A partir des versions **Actions** dans la liste déroulante de droite, sélectionnez **Insert New Policy** pour ajouter une nouvelle stratégie.
3. Créer une nouvelle règle appelée **AD_Administrator** , mappez-le avec le groupe d'administration défini dans le **Enable Administrative Access** pour la section AD, et lui attribuer des autorisations.
   Remarque : dans cet exemple, le groupe Admin appelé **Super Admin** est attribué, ce qui équivaut au compte d'administrateur standard.
4. Cliquer **Save Changes** . La confirmation des modifications enregistrées s'affiche dans l'angle inférieur droit de l'interface utilisateur graphique.

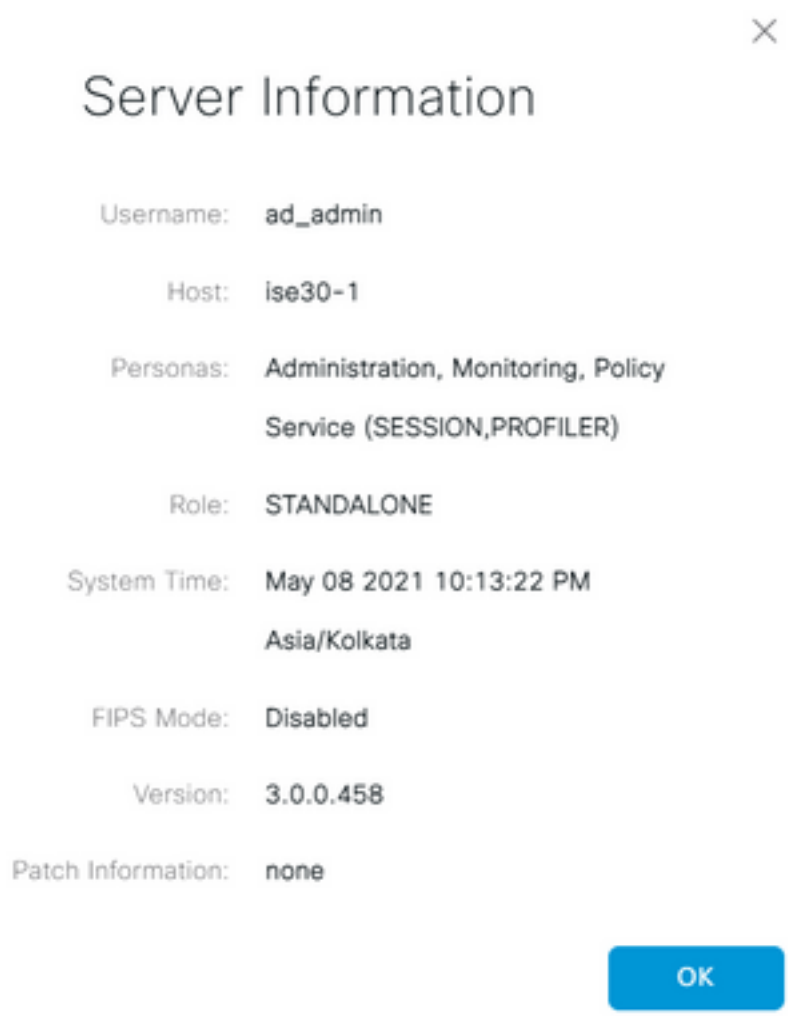


Accès à l'interface utilisateur ISE avec identifiants AD

Complétez ces étapes afin d'accéder à l'interface utilisateur graphique ISE avec les informations d'identification AD :

1. Déconnectez-vous de la GUI d'administration.
2. Sélectionnez **AD** dans la liste **Identity Source** liste déroulante.
3. Entrez le nom d'utilisateur et le mot de passe de la base de données AD et connectez-vous.

   Remarque : ISE utilise par défaut le magasin d'utilisateurs interne dans le cas où AD est inaccessible, ou les informations d'identification de compte utilisées n'existent pas dans AD. Cela facilite la connexion rapide si vous utilisez le magasin interne alors qu'AD est configuré pour l'accès administratif.



Accès ISE CLI avec identifiants AD

L'authentification avec une source d'identité externe est plus sécurisée qu'avec la base de données interne. RBAC pour **CLI Administrators** prend en charge un magasin d'identités externe.

Remarque : ISE version 2.6 et ultérieure prend en charge l'authentification des administrateurs CLI par des sources d'identité externes, telles qu'AD.

Gérez une source unique de mots de passe sans devoir gérer plusieurs politiques de mots de passe et administrer les utilisateurs internes au sein d'ISE, ce qui réduit le temps et les efforts.

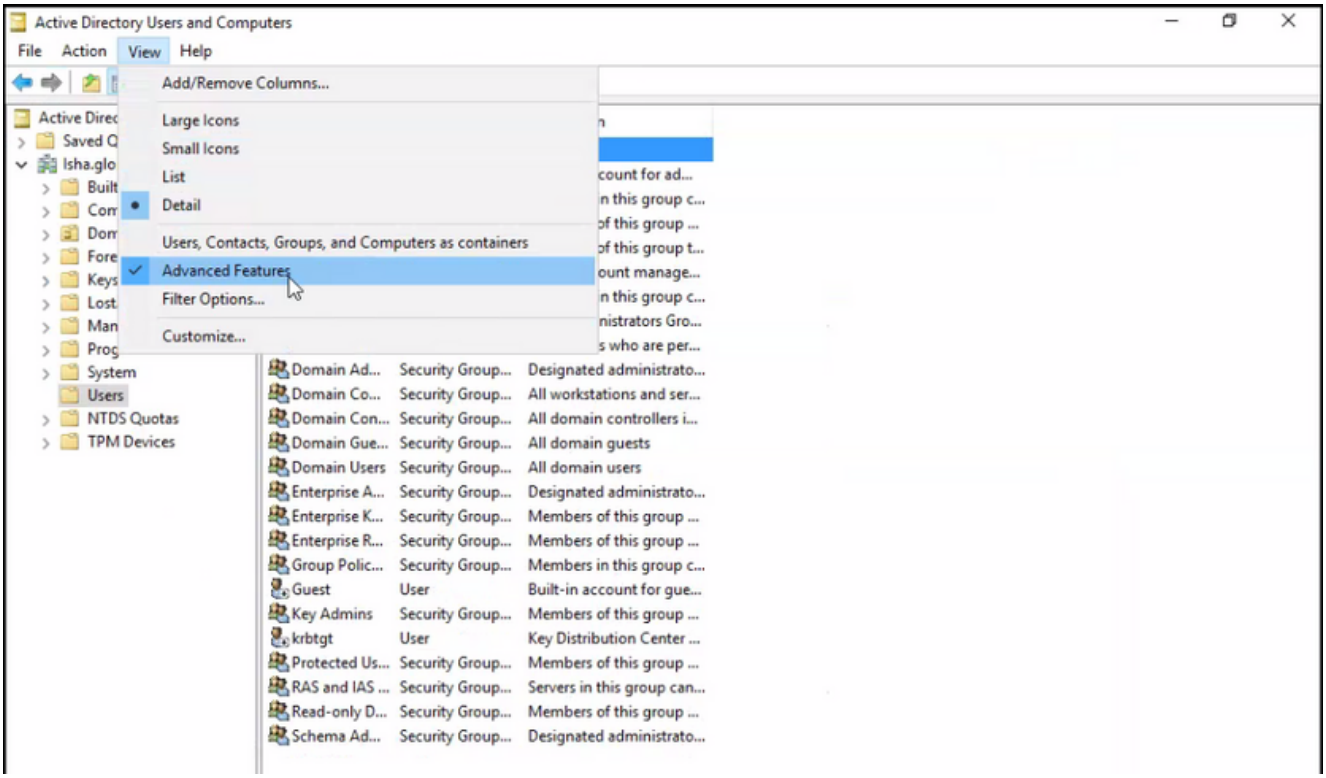
Conditions préalables

Vous devez avoir défini l'utilisateur Admin et l'avoir ajouté à un groupe Administrateur. L'administrateur doit être un **Super Admin** .

Define the User's Attributes in the AD User Directory

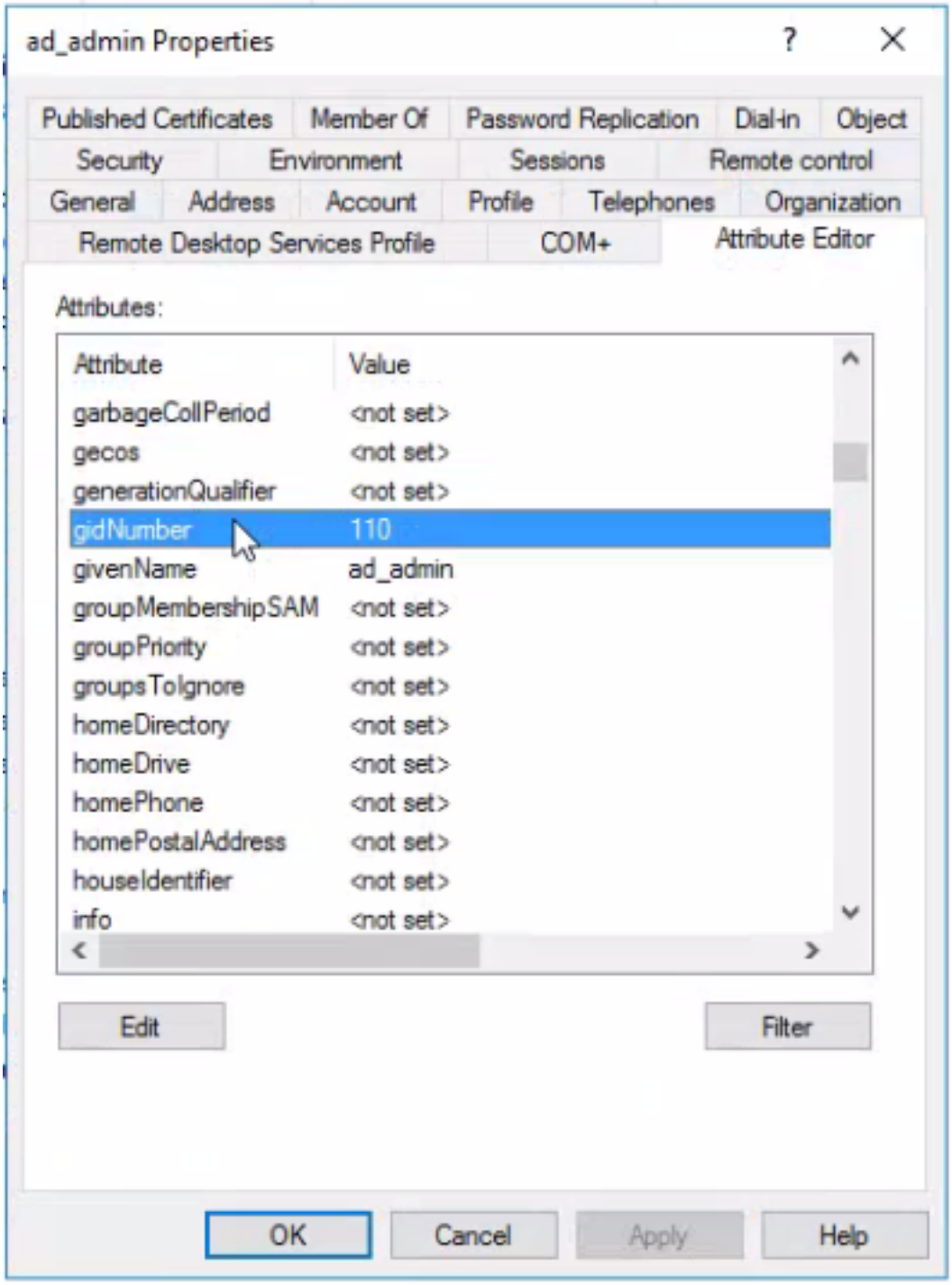
Sur le serveur Windows qui exécute **Active Directory** , modifiez les attributs de chaque utilisateur que vous prévoyez de configurer en tant qu'administrateur CLI.

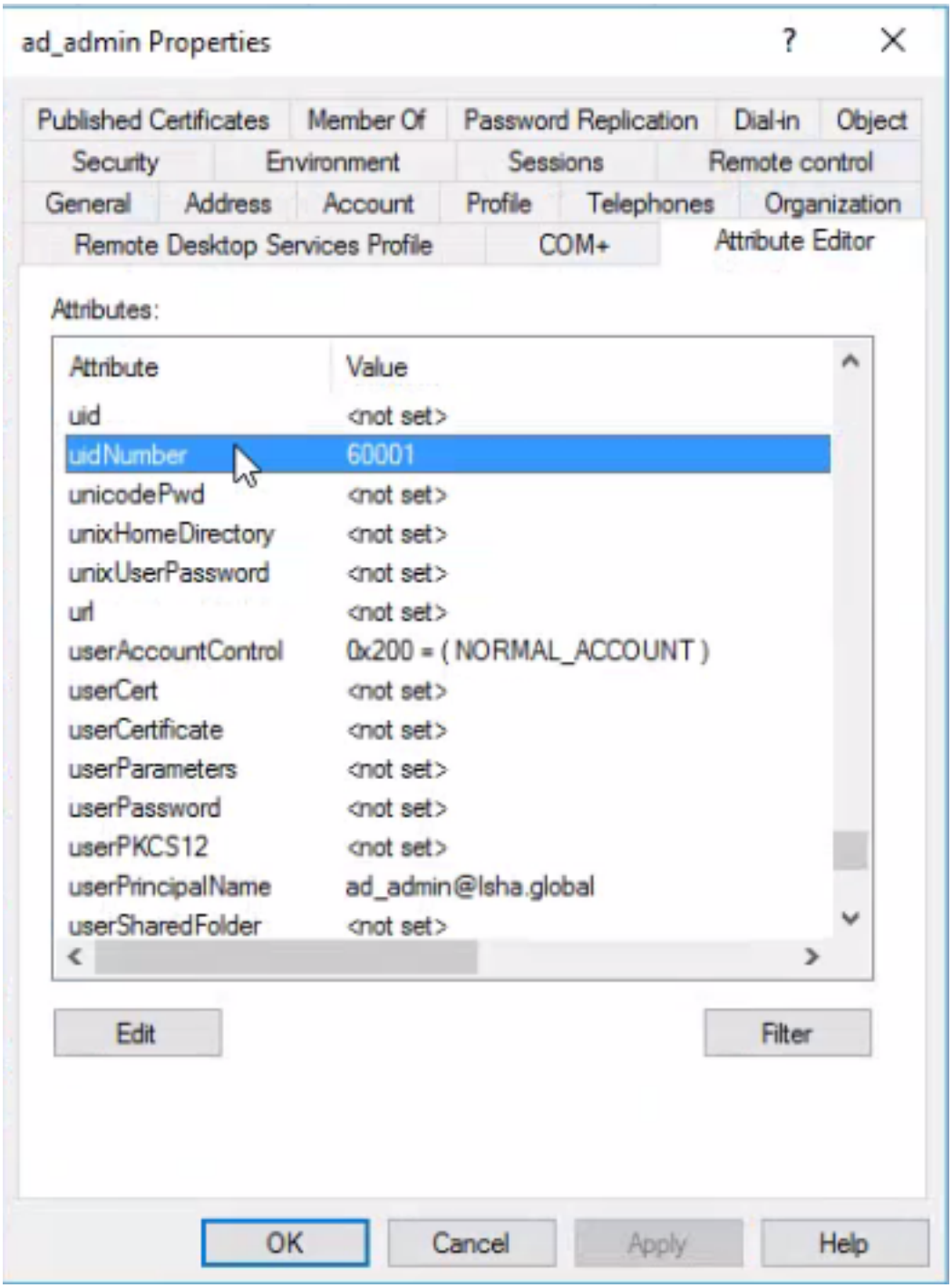
1. Ouvrez le **Server Manager Window** et accédez à **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]**
2. Activer **Advanced Features** dans le menu Affichage afin de pouvoir modifier les attributs d'un utilisateur.



3. Accédez au groupe AD qui contient l'utilisateur Admin et recherchez cet utilisateur.
4. Double-cliquez sur l'utilisateur pour ouvrir le **Properties** et choisissez la commande **Attribute Editor** .
5. Cliquez sur un attribut et saisissez **gid** pour localiser l'attribut **gidNumber** . Si vous ne trouvez pas le **gidNumber** , cliquez sur l'onglet **Filter** et décochez. Afficher uniquement les attributs qui ont des valeurs.
6. Double-cliquez sur le nom de l'attribut pour modifier chaque attribut. Pour chaque utilisateur : Attribuer **uidNumber** supérieur à 60000 et assurez-vous que le numéro est unique.Attribuer **gidNumber** comme 110 ou 111.GidNumber 110 indique un utilisateur admin, tandis que 111 indique un utilisateur en lecture seule.Ne modifiez pas le **uidNumber** après l'affectation.Si vous

modifiez le **gidNumber** , attendez au moins cinq minutes avant d'établir une connexion SSH.





Joindre l'utilisateur de l'interface de ligne de commande Admin au domaine AD

Connectez-vous à l'interface de ligne de commande Cisco ISE, exécutez **identity-store** et attribuez l'utilisateur Admin au magasin d'ID.

Par exemple, pour mapper l'utilisateur admin de l'interface de ligne de commande à Active Directory défini dans ISE comme isha.global, exécutez la commande suivante :

identity-store active-directory domain-name

Une fois la connexion terminée, connectez-vous à l'interface de ligne de commande Cisco ISE et connectez-vous en tant qu'utilisateur de l'interface de ligne de commande Admin pour vérifier votre configuration.

Si le domaine que vous utilisez dans cette commande a déjà été joint au noeud ISE, rejoignez à nouveau le domaine dans la console Administrateurs.

1. Dans l'interface utilisateur graphique de Cisco ISE, cliquez sur **Menu** et accédez à **Administration > Identity Management > External Identity Sources .**
2. Dans le volet de gauche, sélectionnez **Active Directory** et choisissez votre nom AD.
3. Dans le volet de droite, l'état de votre connexion Active Directory indique peut-être **Operational** . Des erreurs se produisent si vous testez la connexion avec l'utilisateur test avec MS-RPC ou Kerberos.
4. Vérifiez que vous pouvez toujours vous connecter à l'interface de ligne de commande Cisco ISE en tant qu'utilisateur de l'interface de ligne de commande Admin.

ISE CLI

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

2. Joignez le noeud au domaine : **ise30-1/admin(config)# identity-store active-directory domain-name isha.global user Administrator**

   Si le domaine **isha.global** est déjà joint via l'interface utilisateur, alors vous devez rejoindre le domaine **isha.global** de l'interface utilisateur après cette configuration. Jusqu'à la réunion, les authentifications **isha.global** échoue.

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

   Connexion réussie au domaine isha.global**Remarques :**

   - Si le domaine est déjà joint via l'interface utilisateur graphique, rejoignez le noeud à partir de l'interface utilisateur graphique. Dans le cas contraire, les authentifications par rapport à AD continuent d'échouer.

   - Tous les noeuds doivent être joints individuellement via l'interface de ligne de commande.**Vérifier**Aucune procédure de vérification n'est disponible pour cette configuration.**Dépannage****Problèmes de jointure**Les problèmes lors de l'opération de jointure et les journaux associés peuvent être vus sous "/var/log/messages file".commande :

   show logging system messages**Scénario de travail**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## Scénario de non-fonctionnementÉchec de la connexion en raison d'un mot de passe incorrect :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## Problèmes de connexionLes problèmes rencontrés lors de la connexion et les journaux associés sont visibles sous **/var/log/secure** .commande : show logging system secure **Authentification réussie :**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

Échec d'authentification dû à un mot de passe incorrect :

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

Échec d'authentification dû à un utilisateur non valide :

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.