Integración de AD para la GUI de ISE y el inicio de sesión de CLI

Contenido

[Introducción](#)
[Prerequisites](#)
[Componentes Utilizados](#)
[Configurar](#)
[Incorporación de ISE a AD](#)
[Seleccionar grupos de directorios](#)
[Habilitar acceso administrativo para AD](#)
[Configuración del grupo de administradores para la asignación de grupos de AD](#)
[Establecer permisos RBAC para el grupo de administradores](#)
[Acceso a la GUI de ISE con credenciales de AD](#)
[Acceso a ISE CLI con credenciales de AD](#)
[CLI DE ISE](#)
[Verificación](#)
[Troubleshoot](#)
[Unir problemas](#)
[Problemas de conexión](#)

Introducción

Este documento describe la configuración de Microsoft AD como almacén de identidad externo para el acceso administrativo a la GUI y CLI de administración de Cisco ISE.

Prerequisites

Cisco recomienda conocer estos temas:

- Configuración de Cisco ISE versión 3.0
- AD de Microsoft

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco ISE versión 3.0
- Windows Server 2016

Este documento describe la configuración de Microsoft **Active Directory (AD)** como almacén de identidades externo para el acceso administrativo a Cisco **Identity Services Engine (ISE)** GUI y CLI de gestión.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Utilice esta sección para configurar el uso de Microsoft AD como almacén de identidad externo para el acceso administrativo a la GUI de administración de Cisco ISE.

Estos puertos se utilizan entre el nodo ISE y AD para esta comunicación:

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

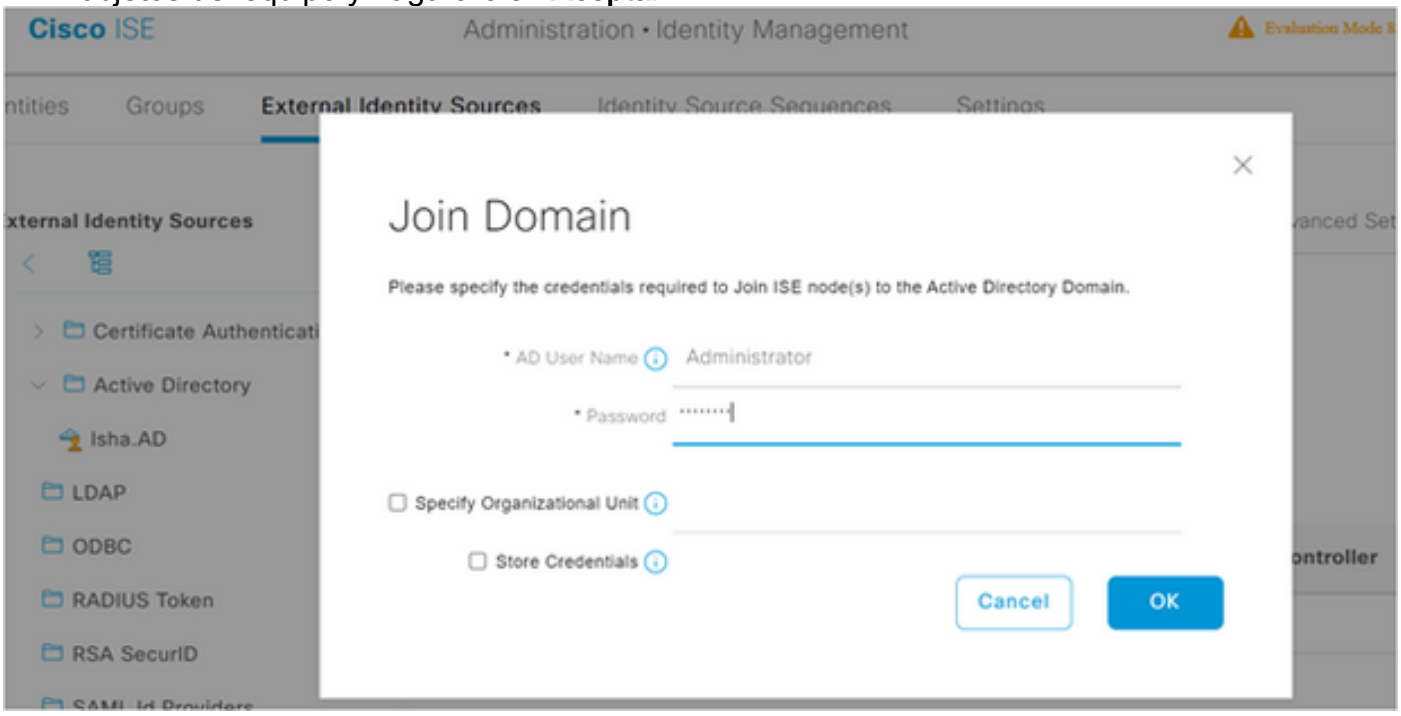
Nota: asegúrese de que la cuenta de AD tenga todos los privilegios necesarios.

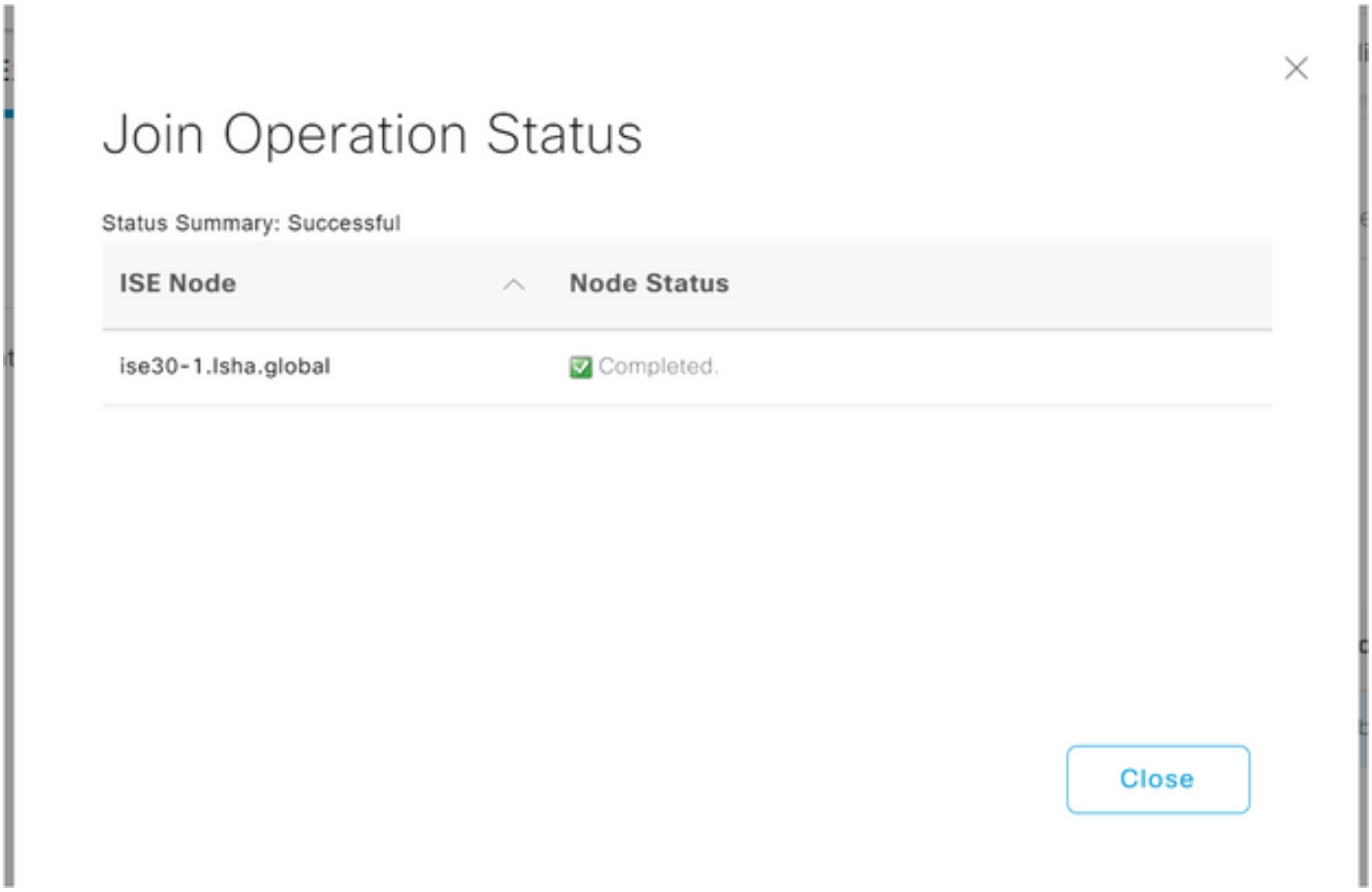
Active Directory Account Permissions Required for Performing Various Operations

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.

Incorporación de ISE a AD

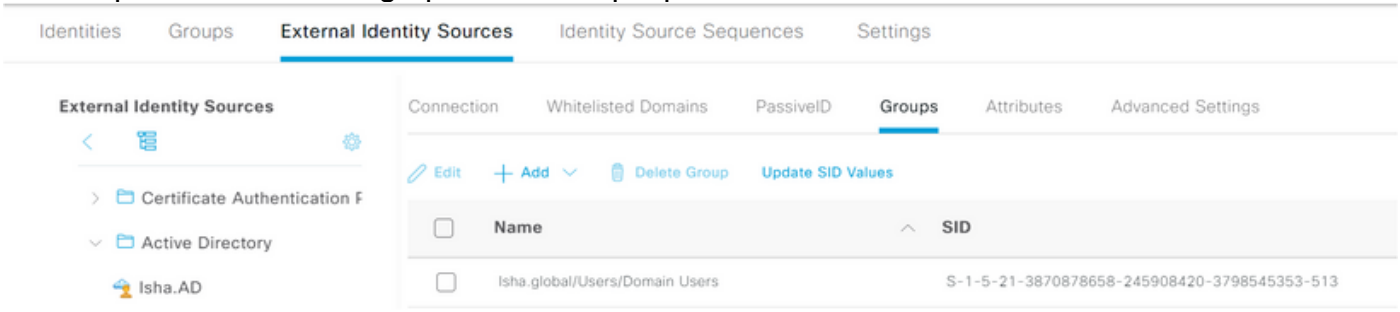
1. Desplácese hasta **Administration > Identity Management > External Identity Sources > Active Directory** .
2. Introduzca el nuevo nombre del punto de unión y el dominio de AD.
3. Escriba las credenciales de la cuenta de AD que puede agregar y realizar cambios en los objetos del equipo y haga clic en **Aceptar**.





Seleccionar grupos de directorios

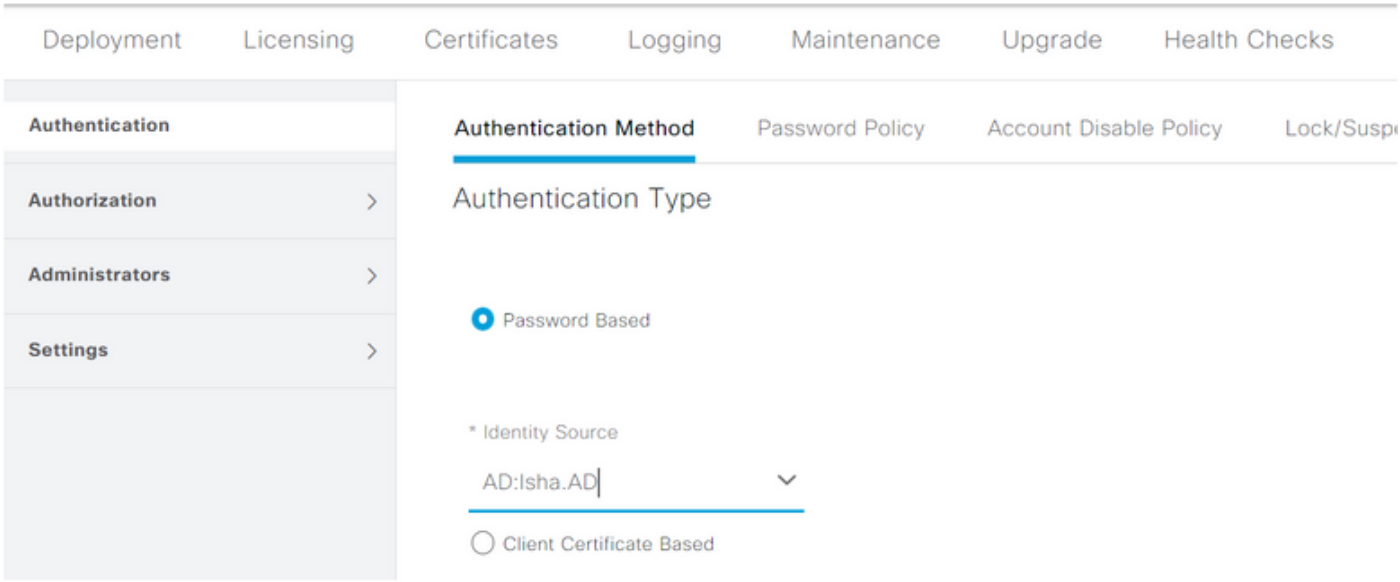
1. Desplácese hasta **Administration > Identity Management > External Identity Sources > Active Directory > Groups > Add > Select groups form Directory** .
2. Importe al menos un grupo de AD al que pertenezca el administrador.



Habilitar acceso administrativo para AD

Complete estos pasos para habilitar la autenticación basada en contraseña para AD:

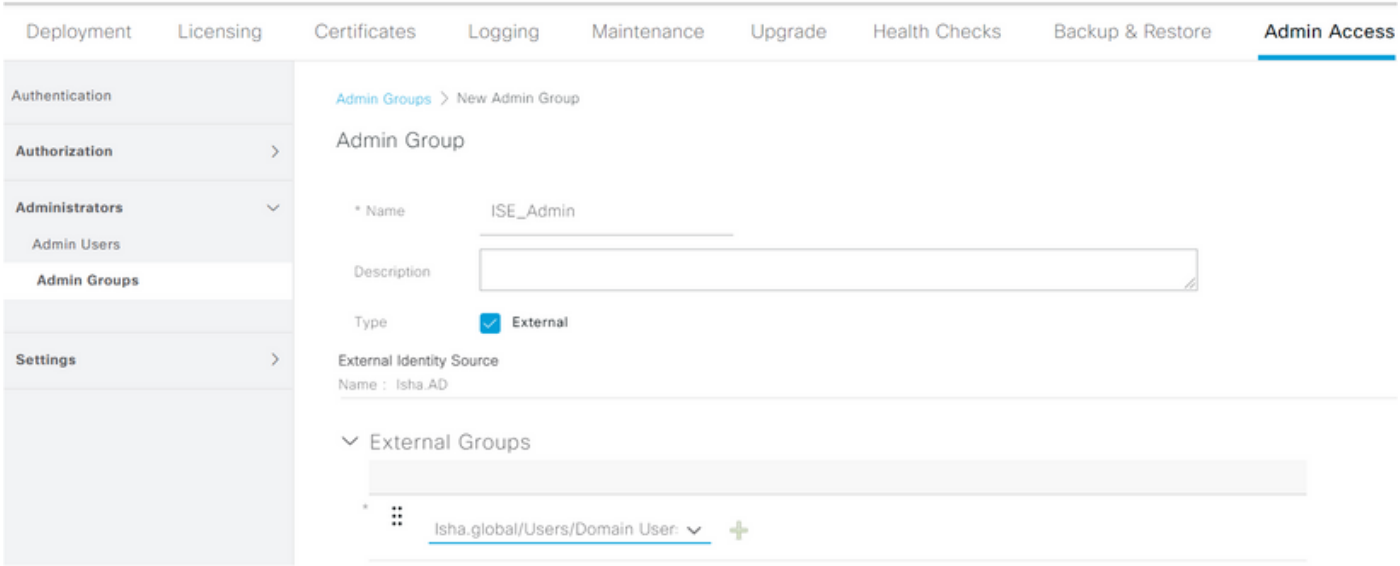
1. Desplácese hasta **Administration > System > Admin Access > Authentication** .
2. Desde **Authentication Method** , seleccione la ficha **Password Based** opción.
3. Elija **AD** en el **Identity Source** lista desplegable.
4. Haga clic en **Save Changes** .



Configuración del grupo de administradores para la asignación de grupos de AD

Definición de un ISE de Cisco **Admin Group** y asígnelo a un grupo de AD. Esto permite la autorización para determinar el **Role Based Access Control (RBAC)** permisos para el administrador según la pertenencia a grupos en AD.

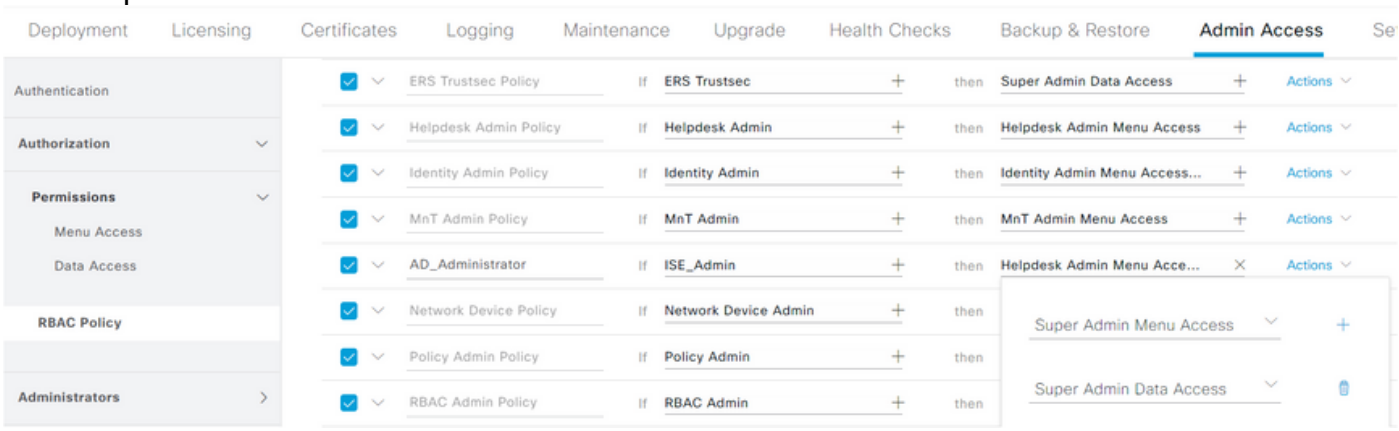
1. Desplácese hasta **Administration > System > Admin Access > Administrators > Admin Groups** .
2. Haga clic en **Add** en el encabezado de la tabla para ver el nuevo **Admin Group** panel de configuración.
3. Introduzca el nombre del nuevo grupo de administradores.
4. En el **Type** , compruebe el **External** casilla de verificación.
5. Desde **External Groups** , seleccione el grupo de AD al que desea que se asigne este grupo de administradores, como se define en la **Select Directory Groups** sección.
6. Haga clic en **Save Changes** .



Establecer permisos RBAC para el grupo de administradores

Complete estos pasos para asignar permisos RBAC a los grupos de administradores creados en la sección anterior:

1. Desplácese hasta **Administration > System > Admin Access > Authorization > Policy** .
2. Desde **Actions** lista desplegable de la derecha, seleccione **Insert New Policy** para agregar una nueva directiva.
3. Cree una nueva regla denominada **AD_Administrator** , asígnelo al grupo de administradores definido en el **Enable Administrative Access** para la sección AD y asígnele permisos. **Nota**: En este ejemplo, se asigna el grupo de administradores llamado **Super Admin**, que es equivalente a la cuenta de administración estándar.
4. Haga clic en **Save Changes** . La confirmación de los cambios guardados se muestra en la esquina inferior derecha de la GUI.

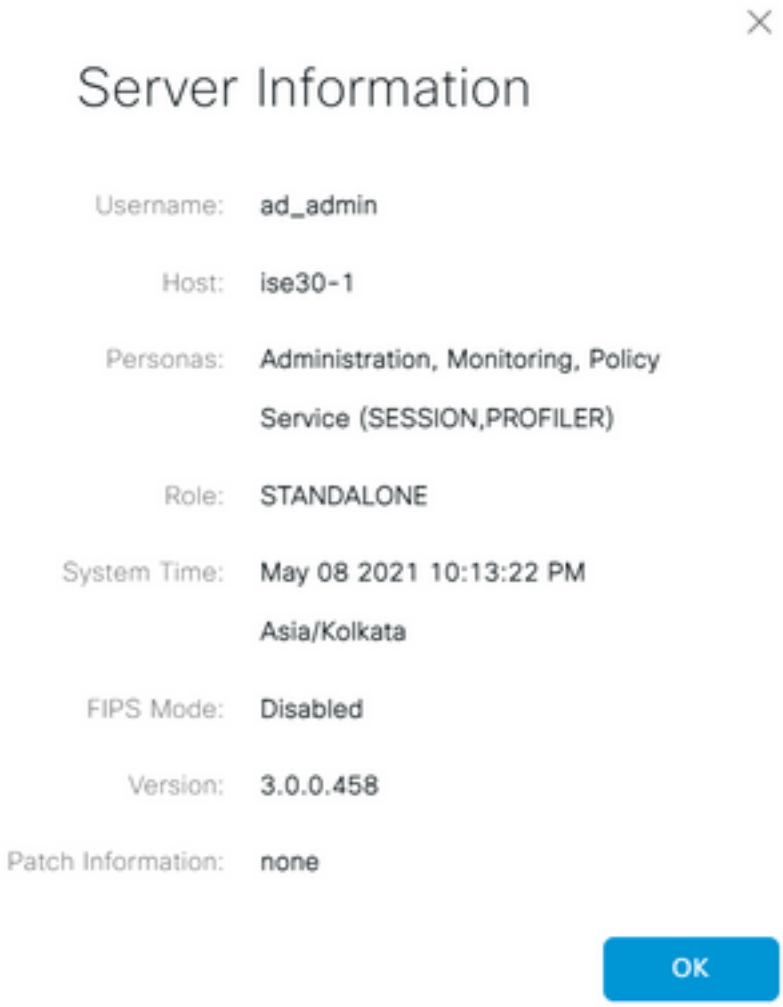


Acceso a la GUI de ISE con credenciales de AD

Complete estos pasos para acceder a la GUI de ISE con credenciales de AD:

1. Cierre la sesión de la GUI administrativa.
2. Elija **AD** en el **Identity Source** lista desplegable.
3. Introduzca el nombre de usuario y la contraseña de la base de datos de AD e inicie sesión.

Nota: ISE usa de forma predeterminada el almacén de usuarios interno en caso de que AD no esté disponible o de que las credenciales de cuenta utilizadas no existan en AD. Esto facilita el inicio de sesión rápido si utiliza el almacén interno mientras AD está configurado para el acceso administrativo.



Acceso a ISE CLI con credenciales de AD

La autenticación con un origen de identidad externo es más segura que con la base de datos interna. RBAC para **CLI Administrators** admite un almacén de identidades externo.

Nota: ISE versión 2.6 y posteriores admiten la autenticación de los administradores de CLI por parte de fuentes de identidad externas, como AD.

Gestione un único origen de contraseñas sin necesidad de gestionar varias políticas de contraseñas ni de administrar usuarios internos en ISE, lo que se traduce en menos tiempo y esfuerzo.

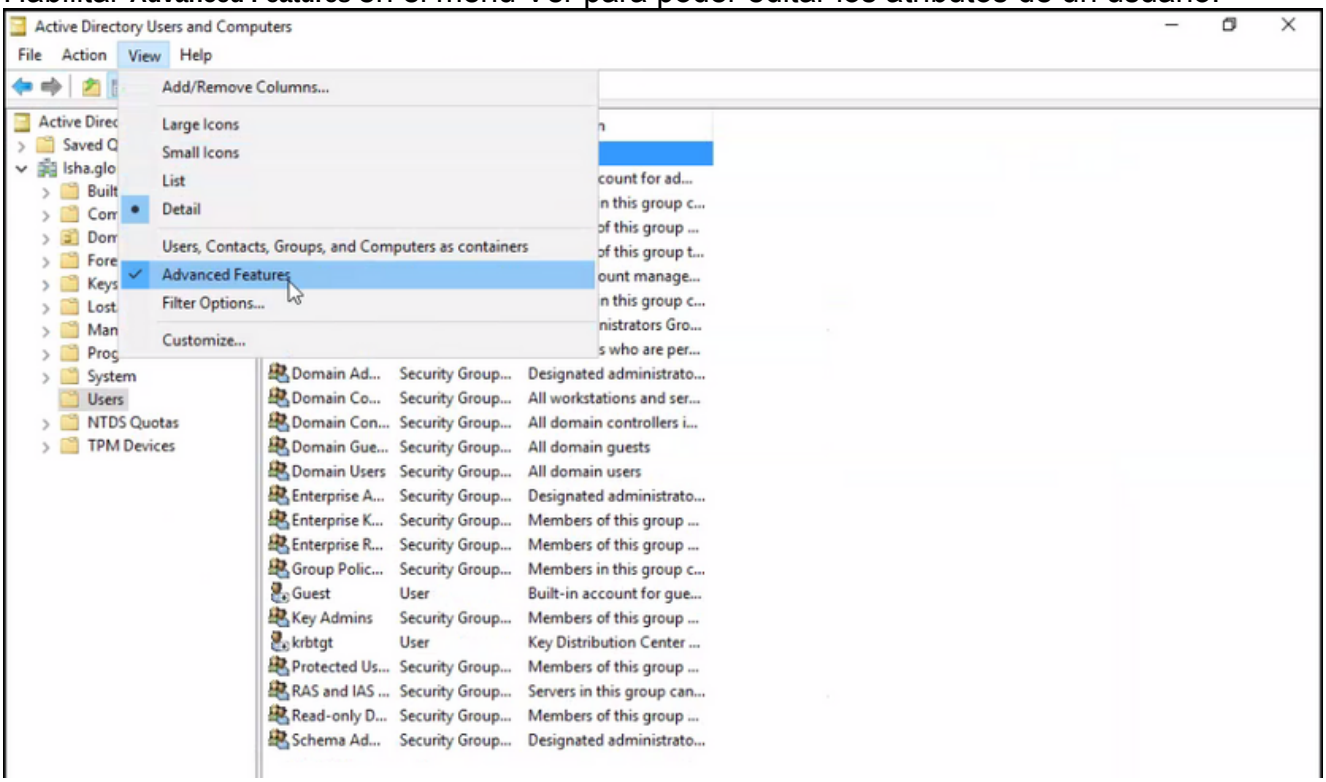
Prerequisites

Debe haber definido el usuario administrador y haberlo agregado a un grupo de administradores. El administrador debe ser un **Super Admin** .

Define the User's Attributes in the AD User Directory

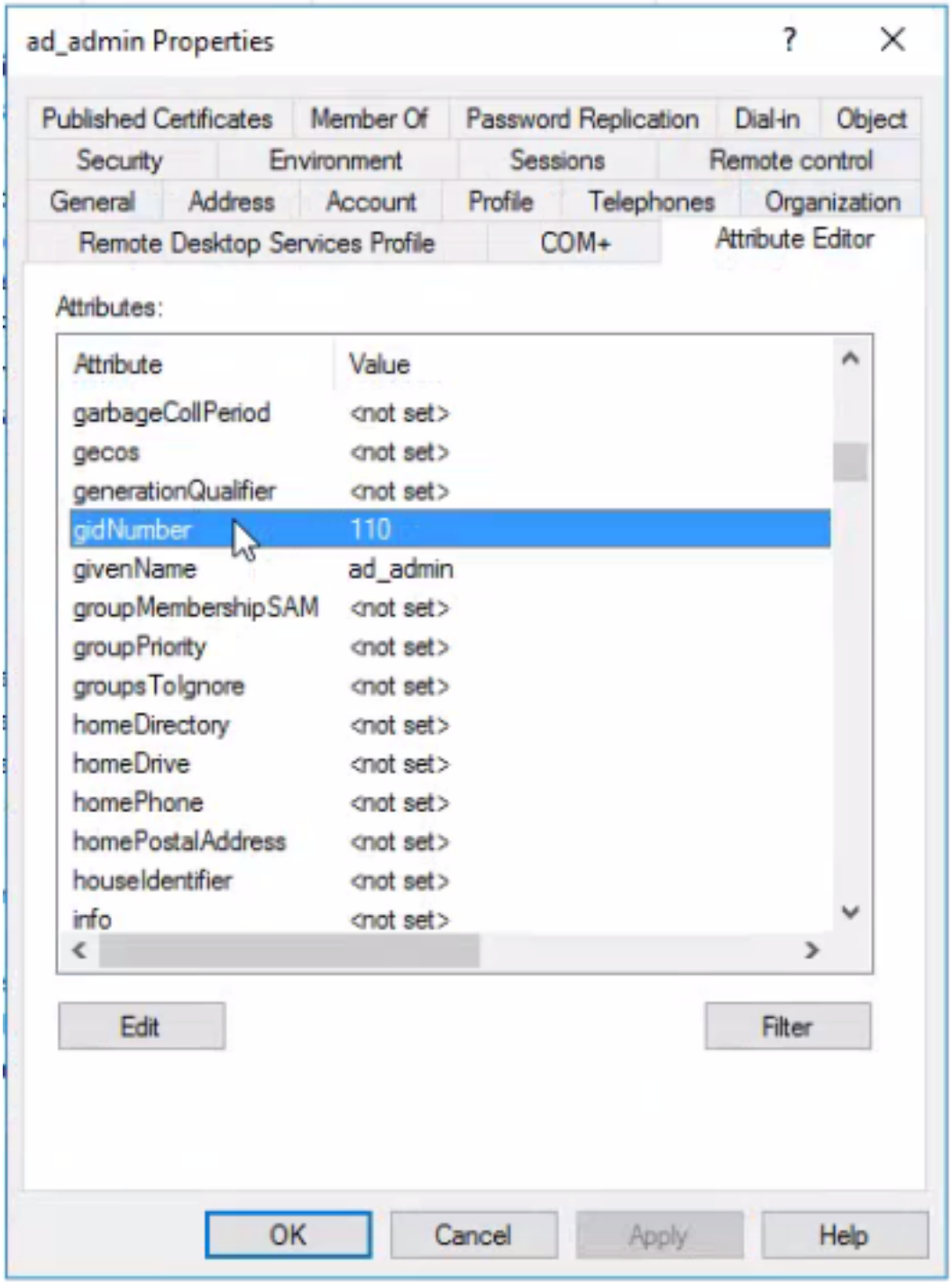
En el servidor de Windows que se ejecuta **Active Directory** , modifique los atributos de cada usuario que planee configurar como administrador de CLI.

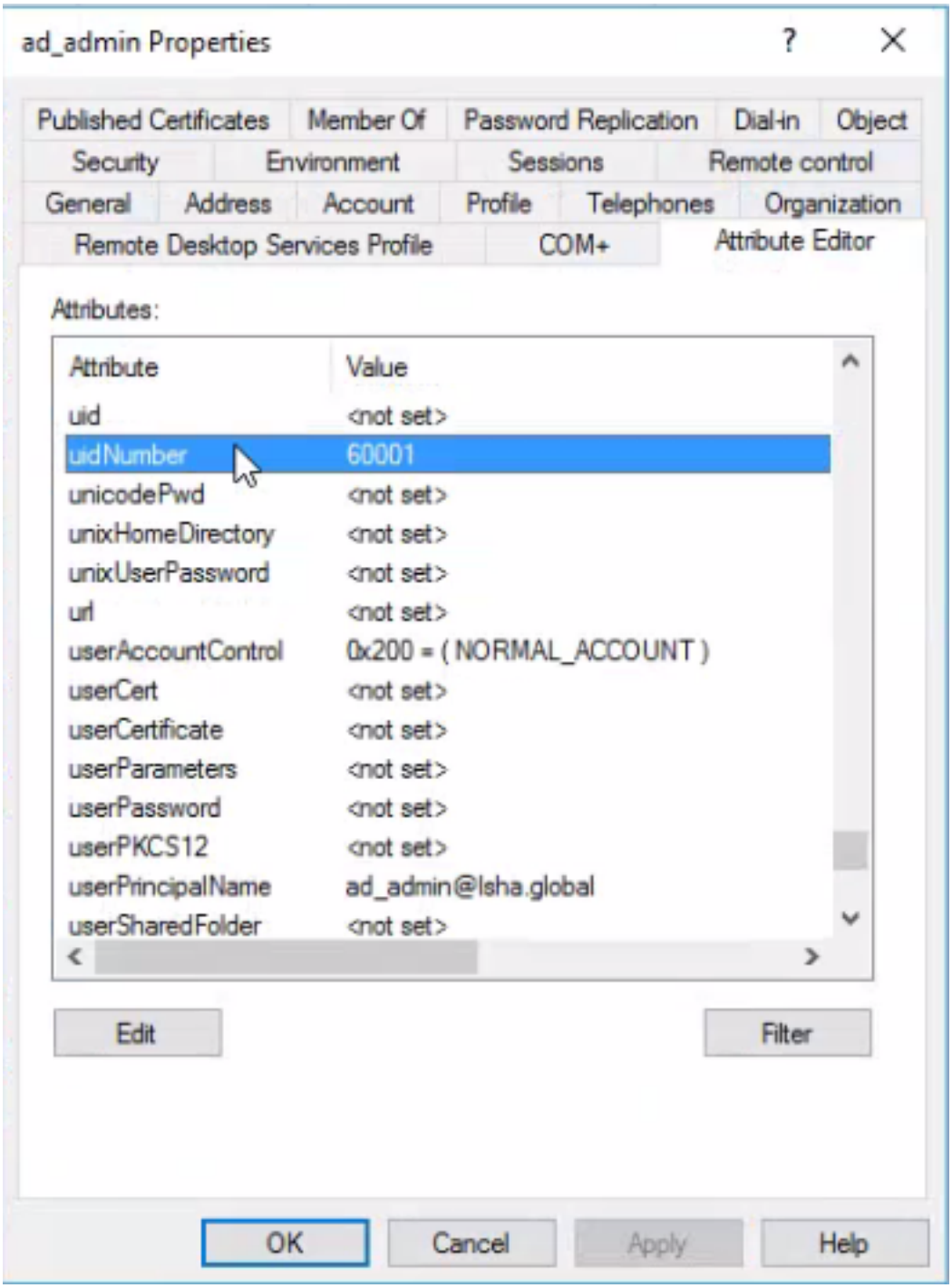
1. Abra el **Server Manager Window** y desplácese hasta **Server Manager > Roles > Active Directory Domain Services > Active Directory Users and Computers > [ad.adserver]**
2. Habilitar **Advanced Features** en el menú Ver para poder editar los atributos de un usuario.



3. Desplácese hasta el grupo de AD que contiene el usuario administrador y busque ese usuario.
4. Haga doble clic en el usuario para abrir el **Properties** y seleccione la **Attribute Editor** .
5. Haga clic en cualquier atributo e introduzca **gid** para localizar el atributo **gidNumber** . Si no encuentra el **gidNumber** haga clic en el **Filter** y desmarque. Mostrar sólo los atributos que tienen valores.
6. Haga doble clic en el nombre del atributo para editar cada atributo. Para cada usuario: Asignar **uidNumber** mayor que 60000 y asegúrese de que el número es único.Asignar **gidNumber** como 110 o 111.GidNumber 110 indica un usuario administrador, mientras que 111 indica un usuario de solo lectura.No cambie el **uidNumber** después de la asignación.Si

modifica el **gidNumber** , espere al menos cinco minutos antes de establecer una conexión SSH.





Unirse al usuario CLI de administración en el dominio AD

Conéctese a la CLI de Cisco ISE, ejecute el **identity-store** y asigne el usuario administrador al almacén de ID.

Por ejemplo, para asignar el usuario administrador de CLI al Active Directory definido en ISE como isha.global, ejecute este comando:

identity-store active-directory domain-name

Una vez completada la unión, conéctese a la CLI de Cisco ISE e inicie sesión como el usuario de la CLI de administración para verificar la configuración.

Si el dominio que utiliza en este comando se unió previamente al nodo ISE, vuelva a unirse al dominio en la consola de administradores.

1. En la GUI de Cisco ISE, haga clic en el botón **Menu** y desplácese hasta **Administration > Identity Management > External Identity Sources** .
2. En el panel izquierdo, seleccione **Active Directory** y elija el nombre de AD.
3. En el panel de la derecha, es posible que el estado de la conexión de AD sea **Operational** . Hay errores si prueba la conexión con el usuario de prueba con MS-RPC o Kerberos.
4. Compruebe que aún puede iniciar sesión en la CLI de Cisco ISE como usuario de la CLI de administración.

CLI DE ISE

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

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

   Si el dominio **isha.global** ya se ha unido a través de la interfaz de usuario, entonces debe volver a unirse al dominio **isha.global** de la interfaz de usuario después de esta configuración. Hasta que se produzca la reincorporación, las autenticaciones **isha.global** falla.

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

   Se ha unido al dominio isha.global correctamente**Notas:**

   - Si el dominio ya está unido a través de la GUI, vuelva a unirse al nodo desde la GUI; de lo contrario, las autenticaciones contra AD seguirán fallando.

   - Todos los nodos se deben unir de forma individual mediante CLI.**Verificación**Actualmente, no hay un procedimiento de verificación disponible para esta configuración.**Troubleshoot****Unir problemas**Los problemas durante la operación de unión y los registros relacionados con esto se pueden ver en "/var/log/messages file".Comando: **show logging system messages****Escenario de trabajo**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**Escenario no laborableError en la conexión debido a una contraseña incorrecta:**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**Problemas de conexión**Los problemas durante el inicio de sesión y los registros relacionados con esto se pueden ver en **/var/log/secure** .Comando: show logging system secure **Autenticación correcta:**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

Error de autenticación debido a una contraseña incorrecta:

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

Error de autenticación debido a un usuario no válido:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).