Solución de problemas de acceso remoto en un fabric ACI

Introducción

Este documento describe cómo verificar, resolver y resolver problemas de acceso remoto en un fabric de Cisco Application Centric Infrastructure (ACI). Abarca el acceso Secure Shell (SSH) y el protocolo de transferencia de hipertexto (HTTPS) a los APIC y los switches de fabric, la autenticación, autorización y administración de cuentas (AAA) remotas con Terminal Access Controller Access-Control System Plus (TACACS+), el servicio de usuario de acceso telefónico de autenticación remota (RADIUS), el protocolo ligero de acceso a directorios (LDAP) y la autorización de control de acceso basado en roles (RBAC). Para cada área se incluye un árbol de decisiones de clasificación y escenarios detallados de resolución de problemas.

Antecedentes

El material de este documento se sintetizó a partir de la guía Troubleshooting ACI Management and Core Services — Pod Policies, la Guía de Configuración Básica de Cisco APIC, Release 6.1(x) — Management capítulo, y la Guía de Configuración de Seguridad de Cisco APIC — Access, Authentication, and Accounting capítulo.

Overview

El acceso remoto a un fabric de ACI implica tres capas distintas, cada una de las cuales debe funcionar para que un ingeniero inicie sesión y funcione correctamente:

1. Transporte: la ruta de red de administración (OOB o en banda) y el servicio de protocolo (SSH o HTTPS) deben ser accesibles y estar habilitados.
2. Autenticación: las credenciales del usuario deben validarse, ya sea localmente en el APIC o en un servidor AAA remoto (TACACS+, RADIUS o LDAP).
3. Autorización: al usuario autenticado se le deben asignar los roles RBAC y los dominios de seguridad correctos para ver y modificar los objetos ACI deseados.

Un fallo en cualquier capa produce síntomas diferentes. Una falla de transporte impide la conexión por completo. Un error de autenticación devuelve un error de credenciales. Un fallo de autorización permite el inicio de sesión, pero restringe la visibilidad o produce errores "403

Forbidden" (Prohibido) en la API.

Política de acceso a la gestión

La directiva de acceso a la administración (**commPol**) es el objeto central que controla qué protocolos de acceso remoto están habilitados en el fabric. Se encuentra en Fabric > Fabric Policies > Policies > Pod > Management Access > default. La directiva contiene objetos secundarios que configuran:

- SSH (**commSsh**): estado administrativo, puerto, cifrados, algoritmos de intercambio de claves (KEX), códigos de autenticación de mensajes (MAC) y algoritmos de clave de host.
- HTTPS (**commHttps**): estado administrativo, puerto, versión de protocolo de seguridad de la capa de transporte (TLS), velocidad de aceleración y autenticación de certificado de cliente.
- Telnet (**commTelnet**): estado administrativo y puerto. Telnet está deshabilitado de forma predeterminada y Cisco recomienda que permanezca deshabilitado.

Gestión OOB y en banda

Los nodos ACI admiten dos rutas de acceso a la gestión:

- Fuera de banda (OOB): utiliza el puerto de gestión dedicado en el APIC o el switch. Las direcciones de administración OOB se asignan desde un grupo bajo el arrendatario mgmt y se asignan a nodos a través de **mgmtRsOoBStNode**. En el APIC, los contratos OOB se aplican mediante **iptables** reglas. Si se aplica un contrato OOB, solo el tráfico permitido explícitamente por el contrato puede alcanzar la interfaz de gestión APIC.
- En banda (INB): utiliza el plano de datos del fabric para el tráfico de gestión. La administración en banda requiere una asignación de dirección de dominio de puente (BD), subred, grupo de terminales (EPG), contrato y administración de nodos. Las direcciones IP en banda no son accesibles desde fuera del fabric sin un routing adicional o una configuración de políticas.

Nota: Las IP de gestión de OOB de APIC se configuran durante la configuración inicial y el APIC obtiene conectividad IP antes de que se descubra completamente el fabric. OOB es la ruta de gestión principal y siempre está disponible si la red de gestión física está conectada.

Arquitectura AAA

ACI utiliza un modelo AAA de tres niveles:

1. Dominio de inicio de sesión (**aaaLoginDomain**): agrupa los proveedores AAA bajo un rango con nombre. Los usuarios especifican el dominio de inicio de sesión en la pantalla de inicio de sesión (por ejemplo, `apic:TACACS-Domain` o a través del menú desplegable de la interfaz de usuario). Siempre existe un dominio de inicio de sesión de reserva especial y se asigna a la autenticación local.
2. Grupo de proveedores (**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**, **aaaLdapProviderGroup**): hace referencia a uno o más servidores AAA y define el orden en el que se prueban.
3. Proveedor (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**): define la IP del servidor, el puerto, el secreto compartido (o DN de enlace para LDAP), el tiempo de espera, los reintentos, el EPG de administración y las credenciales de supervisión.

El rango de autenticación predeterminado (**aaaDefaultAuth**) determina qué dominio de inicio de sesión se utiliza cuando el usuario no especifica uno al iniciar sesión. El rango de autenticación de la consola controla la autenticación para las sesiones de la consola.

Nota: Si cambia el rango de autenticación predeterminado a un servidor AAA remoto mientras ese servidor está inalcanzable, se bloqueará el acceso al fabric. Pruebe siempre la conectividad del servidor AAA antes de cambiar el rango. El dominio de inicio de sesión de reserva (`apic:fallback\\admin`) se puede utilizar para omitir el rango predeterminado y autenticarse localmente.

Archivos de registro AAA de clave

Los eventos de autenticación AAA se registran en varios archivos tanto en el APIC como en los switches de fabric. Estos registros son la herramienta principal para validar los resultados de autenticación, identificar el rango y el grupo de proveedores que se está utilizando, y diagnosticar errores de asignación de roles.

Archivo de registro	Ubicación (APIC)	Ubicación (switches)	D
nginx.bin.log (APIC) nginx.log (switches)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	Registro A Contiene autentica solicitud c selección búsqueda comunica LDAP/TA análisis d asignació rol, y resu denegaci nombre d

Archivo de registro	Ubicación (APIC)	Ubicación (switches)	D
			entre las pero el fo contenido
access.log	/var/log/dme/log/access.log	/var/log/dme/log/access.log	Registro HTTP de línea por En el API llamadas aaaRefres estado H correcto, denegado switches, solicitude internas y aaaRefres
pam.module.log	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	registro d Muestra e autentica sesiones autentica e ID de u asignado esta es la rápida de usuario fu rechazad

Nota: El registro AAA principal tiene un nombre de archivo diferente en cada plataforma. En el APIC está **nginx.bin.log** en /var/log/dme/log/. En los switches de columna y hoja, se encuentra **nginx.log** en /var/sysmgr/tmp_logs/dme_logs/. El formato de contenido de registro y los mensajes AAA son los mismos en ambas plataformas.

Las entradas AAA en el registro nginx siguen este formato:

```
PID||TIMESTAMP||aaa||SEVERITY||CONTEXT||MESSAGE||SOURCE_FILE||LINE
```

Filtrar entradas de registro relacionadas con AAA para el flujo de autenticación de un usuario específico:

<#root>

```
! On the APIC:
apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'username' | tail -20


! On a leaf or spine switch:
leaf101#

grep '||aaa||' /var/sysmgr/tmp_logs/dme_logs/nginx.log | grep -i 'username' | tail -20
```

O vea todas las solicitudes de autenticación y resultados recientes:

<#root>

```
! On the APIC:
apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'PAM authenticate\|was denied\|Unauthorized\|DEN


! On a leaf or spine switch:
leaf101#

grep '||aaa||' /var/sysmgr/tmp_logs/dme_logs/nginx.log | grep -i 'PAM authenticate\|was denied\|Unauthor
```

Un flujo de autenticación exitoso típico muestra estos mensajes clave en orden:

1. `Solicitud de autenticación de PAM recibida de nginx para el nombre de usuario: <user>`: se recibió la solicitud de inicio de sesión.
2. `DefaultAuthMo especifica el rango <N>. Grupo de proveedores <name> !` — el rango fue seleccionado (0=fallback/local, 2=TACACS+, 3=LDAP).
3. Mensajes específicos del proveedor (enlace LDAP, búsqueda del proveedor TACACS+ o solicitud RADIUS).
4. `Se encontró UserDomain <domain> en el nombre de usuario remoto: <user>`: la asignación de dominio de la respuesta AAA.
5. `Nombre de usuario encontrado admin con privilegios de escritura admin en UserDomain all (el usuario es un usuario admin)`: se ha superado la comprobación de rol.

Registros de autenticación fallidos:

- `El usuario <user> fue denegado durante la autenticación AAA`

- `Error <user> de usuario no autorizado: Autenticación de servidor AAA DENEGADA`

Nota: El registro nginx gira con frecuencia y las entradas más antiguas se comprimen con un sufijo numérico. En el APIC, los registros girados se encuentran en el mismo directorio (por ejemplo, **nginx.bin.log.22815.gz**). En los switches, los registros rotados se almacenan en **/var/log/dme/oldlog/dme/nginx.log.*.gz** (con enlaces simbólicos en `/var/sysmgr/tmp_logs/dme_logs/`). Para buscar registros girados:

<#root>

```
! On the APIC:
apic1#

zegrep '||aaa||' /var/log/dme/log/nginx.bin.log.*.gz | grep 'PAM authenticate'


! On a leaf or spine switch:
leaf101#

zegrep '||aaa||' /var/sysmgr/tmp_logs/dme_logs/nginx.log.*.gz | grep 'PAM authenticate'
```

Modelo RBAC

ACI RBAC controla lo que un usuario autenticado puede ver y hacer. El modelo tiene tres componentes:

- Dominio de seguridad (**aaaDomain**): un limitador de alcance que se asigna a objetos de ACI (arrendatarios, políticas de acceso, políticas de fabric). Los dominios integrados all, common y mgmt siempre están presentes. Los dominios personalizados restringen la visibilidad de un usuario a arrendatarios o áreas de políticas específicas.
- Rol (**aaaRole**): define un conjunto de privilegios. Los roles predefinidos incluyen admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops y new-svc-admin.
- Privilegio: cada rol otorga acceso de lectura o escritura (lo que implica lectura) a un área funcional específica.

A una cuenta de usuario se le asignan uno o más pares de roles y dominios de seguridad. Para los usuarios remotos autenticados a través de TACACS+, RADIUS o LDAP, la asignación de roles se entrega a través de atributos específicos del proveedor en la respuesta AAA (por ejemplo, el **cisco-av-pair** atributo).

Árbol de decisión de selección

Utilice este árbol de decisiones cuando un usuario informe de que no puede acceder al fabric de ACI de forma remota:

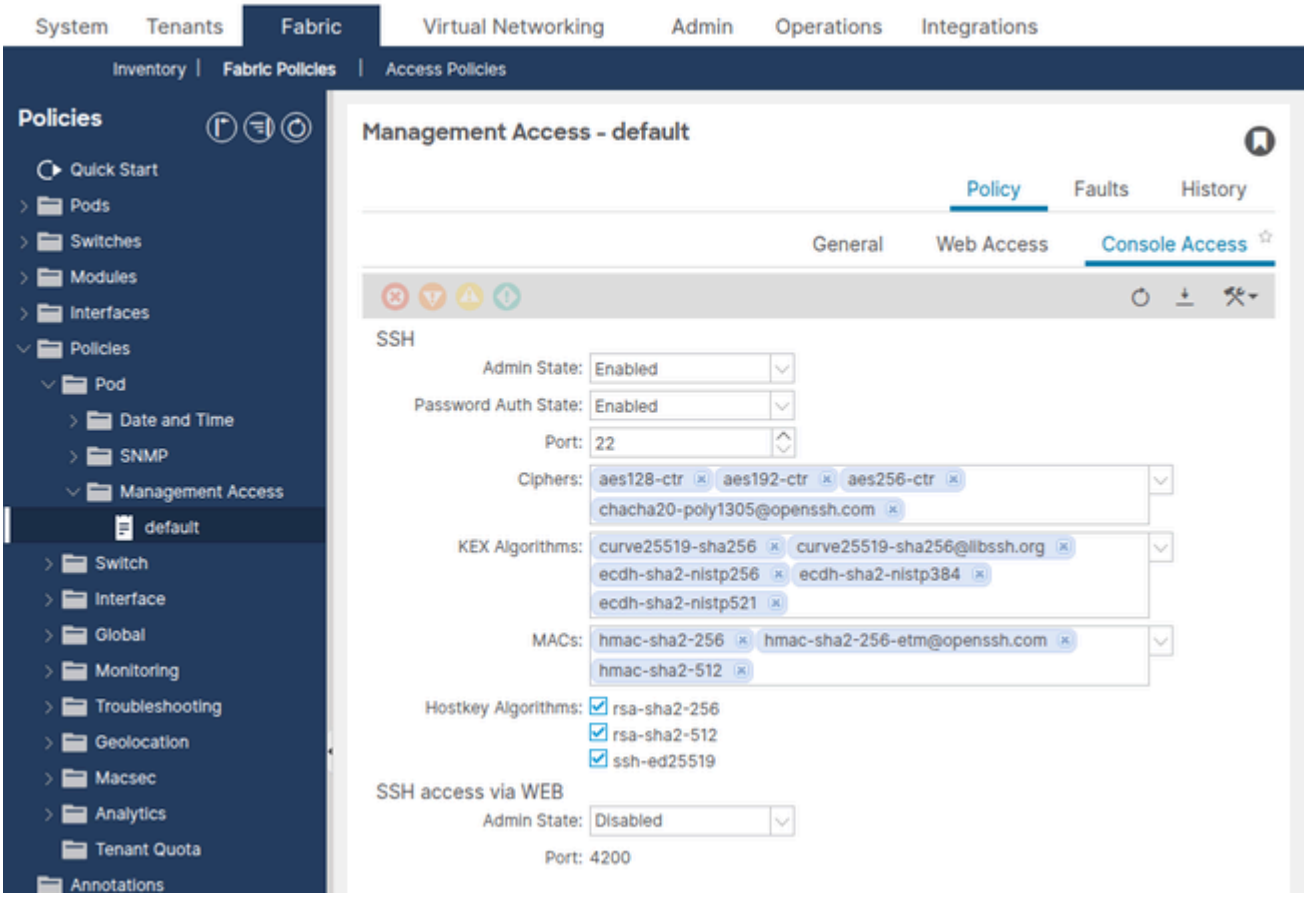
1. ¿Puede hacer ping al APIC o a la IP de administración de switches?
    - No → Solucionar problemas de la ruta de red de administración. Consulte la sección "Resolución de problemas de OOB y administración en banda".
    - Sí → Continuar.
2. ¿Puede establecer una conexión SSH o HTTPS (se abre la conexión en absoluto)?
    - No → El servicio de protocolo se puede inhabilitar, el puerto se puede filtrar o puede haber una discordancia de cifrado. Consulte las secciones "Solucionar problemas de acceso SSH" o "Solucionar problemas de acceso HTTPS".
    - Sí → Continuar.
3. ¿Aparece la pantalla de inicio de sesión (HTTPS) o se completa el protocolo de enlace SSH y se solicitan las credenciales?
    - No hay → error de intercambio de claves SSH o de intercambio de señales TLS. Consulte la sección "Resolución de Problemas de Acceso SSH" para ver las discrepancias de cifrado y KEX.
    - Sí → Continuar.
4. ¿Las credenciales fallan con "Authentication Failed" o similar?
    - Sí → Problema de autenticación. Consulte las secciones "Troubleshooting AAA Authentication" (Resolución de problemas de autenticación AAA) (TACACS+, RADIUS o LDAP, en función del dominio de inicio de sesión en uso).
    - No → Continuar.
5. ¿El usuario inicia sesión pero no puede ver los objetos esperados o recibe errores de "403 Forbidden"?
    - Sí → Problema de autorización o RBAC. Consulte la sección "Resolución de problemas de RBAC y privilegios de usuario".
    - No → Access funciona. Verifique el problema específico que está experimentando el usuario.

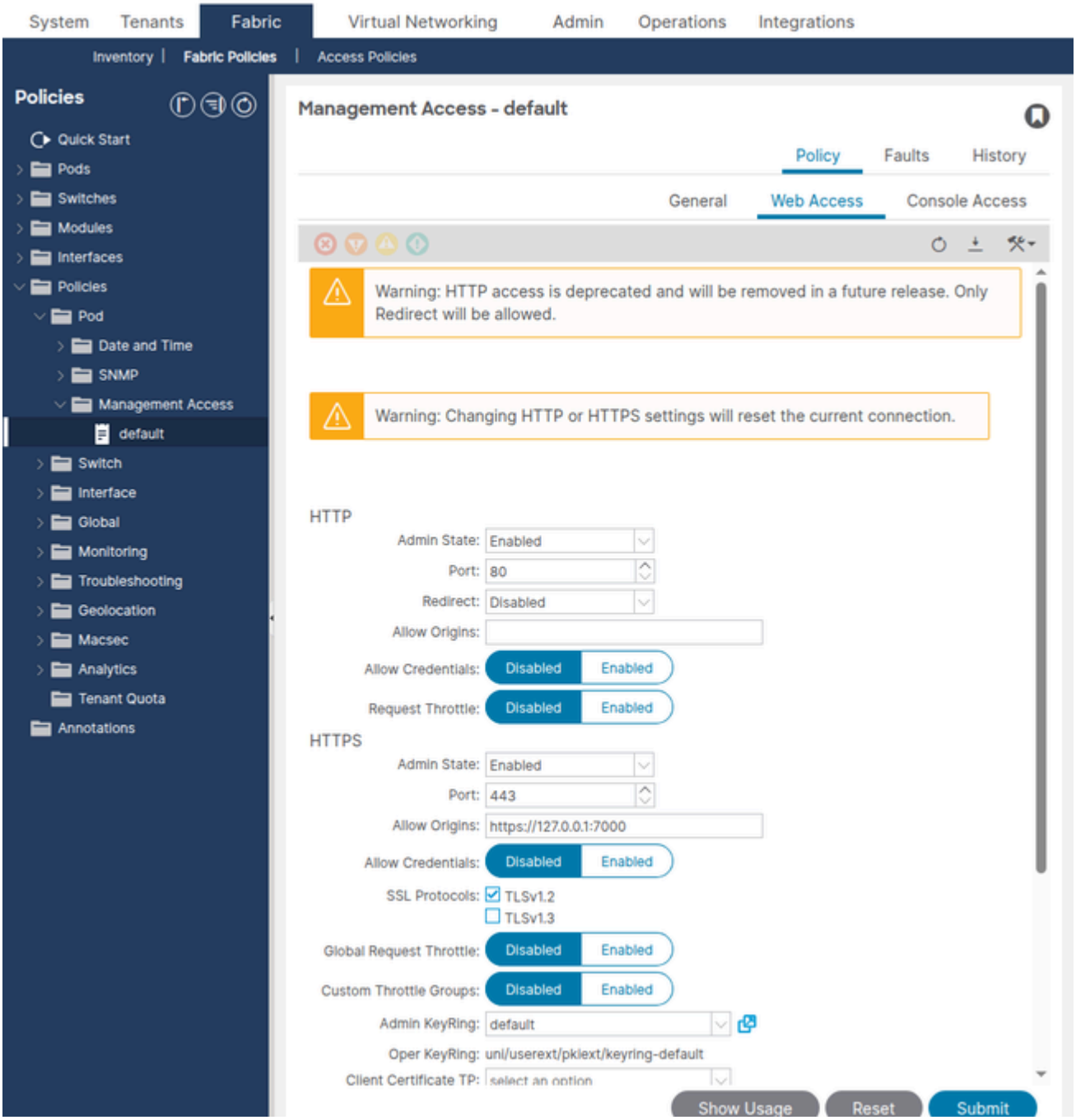
Verifique la configuración

Antes de resolver problemas de estado operativo, verifique que la cadena de configuración esté completa. La configuración incorrecta es la causa principal más común de los problemas de acceso remoto.

Verificar la política de acceso a la gestión (SSH y HTTPS)

Vaya a Fabric > Fabric Policies > Policies > Pod > Management Access > default.


System
Tenants
Fabric
Virtual Networking
Admin
Operations
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Pods
Switches
Modules
Interfaces
Policies
Pod
Date and Time
SNMP
Management Access
default
Switch
Interface
Global
Monitoring
Troubleshooting
Geolocation
Macsec
Analytics
Tenant Quota
Annotations
Management Access - default
Policy
Faults
History
General
Web Access
Console Access
SSH
Admin State: Enabled
Password Auth State: Enabled
Port: 22
Ciphers: aes128-ctr aes192-ctr aes256-ctr chacha20-poly1305@openssh.com
KEX Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
MACs: hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512
Hostkey Algorithms: rsa-sha2-256 rsa-sha2-512 ssh-ed25519
SSH access via WEB
Admin State: Disabled
Port: 4200



Confirme los siguientes parámetros de SSH:

- Estado de administración: debe estar habilitado.
- Puerto: valor predeterminado 22. Si se cambia, el cliente SSH debe utilizar el puerto personalizado.
- Autenticación de contraseña: habilitada (a menos que se pretenda la autenticación sólo de certificados).
- Cifrados SSH: deben incluir al menos un cifrado soportado por el cliente SSH.
- Algoritmos KEX: deben incluir al menos un algoritmo soportado por el cliente SSH.
- SSH MACs: debe incluir al menos un MAC soportado por el cliente SSH.

Consulte el objeto administrado de SSH a través de la API:

<#root>

```
apic1#
```

moquery -c commSsh

```
dn              : uni/fabric/comm-default/ssh
adminSt         : enabled                       <--- must be enabled
port            : 22
passwordAuth    : enabled
sshCiphers      : aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305@openssh.com
kexAlgos        : curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,
sshMacs         : hmac-sha2-256,hmac-sha2-256-etm@openssh.com,hmac-sha2-512
hostkeyAlgos    : rsa-sha2-256,rsa-sha2-512,ssh-ed25519
```

Confirme la siguiente configuración de HTTPS:

- Estado de administración: debe estar habilitado.
- Puerto: 443 predeterminado.
- Protocolos SSL: TLSv1.2 (predeterminado). Los clientes más antiguos pueden requerir que se agregue TLSv1.1 de forma explícita.
- Estado del acelerador: si está activado, la velocidad del acelerador limita las solicitudes por segundo por usuario. Un valor muy bajo puede causar errores de tiempo de espera de API.

<#root>

```
apic1#
```

moquery -c commHttps

```
dn              : uni/fabric/comm-default/https
adminSt         : enabled                       <--- must be enabled
port            : 443
sslProtocols    : TLSv1.2
throttleSt      : enabled
throttleRate    : 2
```

Problemas comunes de configuración incorrecta

- Los cifrados SSH se restringen de forma demasiado agresiva: en la versión ACI 5.2(1) y posteriores, los cifrados SSH predeterminados se endurecieron. Los clientes SSH más antiguos (por ejemplo, las versiones de PuTTY anteriores a 0.75, o las versiones de OpenSSH que sólo ofrecen **diffie-hellman-group14-sha1**) pueden fallar en el intercambio de claves. El cliente SSH muestra "no se ha encontrado ninguna clave coincidente" o "no se ha encontrado ningún método de intercambio de claves coincidente".
- Autenticación de contraseña desactivada: si **passwordAuth** se establece en desactivada, sólo se

permite la autenticación basada en clave SSH. Los usuarios que se conecten con contraseñas verán "Permiso denegado (clave pública)".
- Puerto SSH personalizado sin reconocimiento de cliente: si el puerto SSH se cambió de 2, el cliente SSH debe especificar el nuevo puerto (por ejemplo, **ssh -p 2222 admin@10.1.1.1**).

Verificar direcciones de administración OOB

Vaya a Arrendatarios > Administración > Direcciones de administración de nodos.

Confirme que cada APIC y nodo de switch tenga una dirección IP de administración OOB asignada con una gateway válida. Los nodos sin direcciones de administración no serán accesibles a través de la red de administración.

Consulte las asignaciones de nodos estáticos OOB a través de la API:

<#root>

```
apic1#

moquery -c mgmtRsOoBStNode

# Example output for one node:
dn      : uni/tn-mgmt/mgmtp-default/oob-default/rsooBStNode-[topology/pod-1/node-201]
addr    : 10.1.1.104/27               <--- OOB IP assigned
gw      : 10.1.1.97                   <--- gateway for the OOB subnet
tDn     : topology/pod-1/node-201     <--- target node
```

Problemas comunes de configuración incorrecta

- Falta la asignación de dirección OOB: un switch no tiene una entrada en **mgmtRsOoBStNode**. El nodo no tendrá una IP de administración y no responderá a SSH o HTTPS en la interfaz OOB.
- Gateway incorrecto: la dirección del gateway no coincide con el gateway real en la red de administración OOB. El nodo puede recibir paquetes pero no puede enviar tráfico de retorno.
- Incoherencia de máscara de subred: la máscara de subred OOB no coincide con la red de administración física. Esto puede hacer que el nodo crea que la estación de administración está en una subred diferente y enrute el tráfico a través de una gateway que no existe o que es incorrecta.

Verificar contratos OOB

Navegue hasta Arrendatarios > Administración > Contratos.

Si se aplica un contrato OOB al EPG de gestión OOB, solo el tráfico permitido explícitamente por dicho contrato alcanzará la interfaz de gestión APIC. En el APIC, los contratos OOB se aplican mediante **iptables** reglas.

Consulte los contratos proporcionados por OOB EPG:

<#root>

apic1#

moquery -c mgmtRsOoBProv -x 'query-target-filter=wcard(mgmtRsOoBProv.dn,"oob-default")'

Si la consulta devuelve resultados, se aplican los contratos. Verifique que los sujetos del contrato y los filtros permitan los protocolos requeridos:

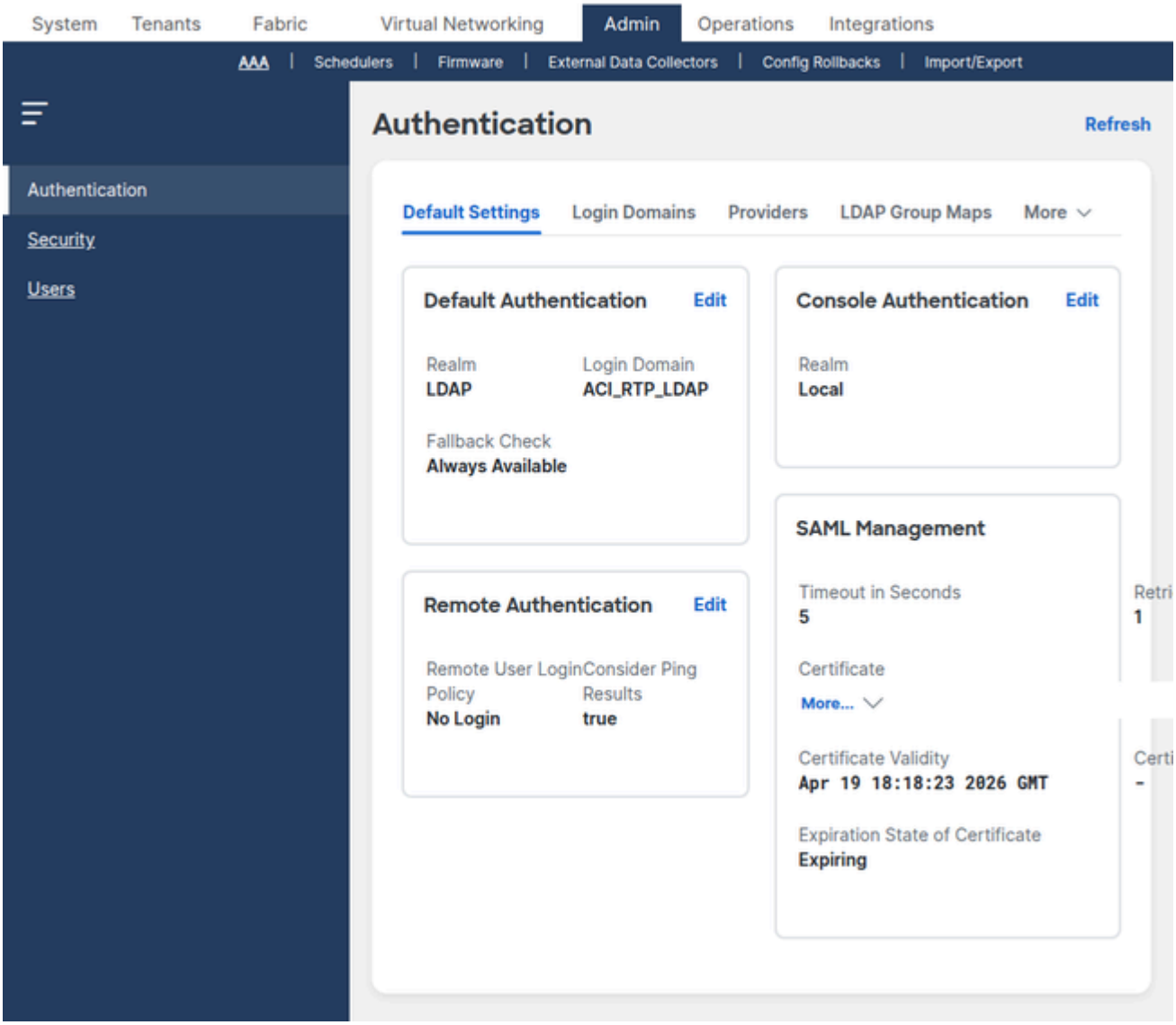
- SSH: puerto TCP 22 (o puerto personalizado)
- HTTPS: puerto TCP 443 (o puerto personalizado)
- ICMP: para verificación de ping

Problemas comunes de configuración incorrecta

- El contrato OOB no incluye SSH o HTTPS: el ingeniero puede hacer ping al APIC pero no puede conectarse a través de SSH o HTTPS. Las **iptables** reglas del APIC descartan el tráfico en silencio.
- Restricción de IP de origen en el filtro de contrato OOB: el filtro de contrato limita el acceso a subredes de origen específicas. Los ingenieros fuera de esa subred no pueden conectarse.

Verificar configuración AAA

Vaya a Admin > AAA > Authentication > AAA.



Confirme lo siguiente:

- Rango de autenticación predeterminado: identifica qué dominio de inicio de sesión se utiliza cuando el usuario no especifica ninguno. Si se establece en un dominio de inicio de sesión AAA remoto, el servidor correspondiente debe ser accesible.
- Rango de autenticación de la consola: controla el acceso a la consola. Si se establece en local, el inicio de sesión de la consola siempre utiliza credenciales locales (recomendado).

Verificar dominios de inicio de sesión

Vaya a Admin > AAA > Authentication > Login Domains.

<#root>

```
apic1#
```

```
moquery -c aaaLoginDomain

# Example output:
dn    : uni/userext/logindomain-TACACS-Domain
name  : TACACS-Domain

dn    : uni/userext/logindomain-LOCAL
name  : LOCAL

dn    : uni/userext/logindomain-fallback
name  : fallback
descr : Special login domain to allow fallback to local authentication
```

Verifique que el dominio de inicio de sesión utilizado para la autenticación esté presente y que haga referencia al grupo de proveedores correcto.

Verificar proveedores TACACS+

Vaya a Admin > AAA > Authentication > TACACS+ > TACACS+ Providers.

<#root>

```
apic1#

moquery -c aaaTacacsPlusProvider

dn              : uni/userext/tacacsext/tacacsplusprovider-10.1.1.50
name            : 10.1.1.50
authProtocol    : pap
port            : 49                          <--- default TACACS+ port
monitorServer   : disabled
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Verificar proveedores RADIUS

Vaya a Admin > AAA > Authentication > RADIUS > RADIUS Providers.

<#root>

```
apic1#

moquery -c aaaRadiusProvider

dn              : uni/userext/radiusext/radiusprovider-10.1.1.51
name            : 10.1.1.51
authPort        : 1812                        <--- default RADIUS auth port
```

```
authProtocol    : pap
retries         : 1
timeout         : 5
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Verificar proveedores LDAP

Vaya a Admin > AAA > Authentication > LDAP > LDAP Providers.

<#root>

```
apic1#

moquery -c aaaLdapProvider

dn              : uni/userext/ldapext/ldapprovider-10.1.1.52
name            : 10.1.1.52
port            : 389                          <--- 389 for LDAP, 636 for LDAPS
enableSSL       : no
rootdn          : CN=binduser,CN=Users,DC=example,DC=com
basedn          : CN=Users,DC=example,DC=com
filter          : sAMAccountName=$userid
attribute       : memberOf                     <--- attribute used for group map
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Errores de configuración AAA comunes

- Discordancia de secreto compartido: la clave configurada en el ACI TACACS+ o el proveedor RADIUS no coincide con la clave del servidor. La autenticación falla silenciosamente.
- EPG de administración incorrecto: el EPG del proveedor **epgDn** está vacío o apunta al EPG incorrecto (por ejemplo, en banda cuando el servidor está en la red OOB). El APIC no puede alcanzar el servidor.
- El dominio de inicio de sesión no coincide: el dominio de inicio de sesión está configurado como LDAP pero el usuario espera autenticación TACACS+. Los dominios de inicio de sesión deben hacer referencia al tipo de grupo de proveedores correcto.
- DN de enlace LDAP incorrecto: **rootdn** (DN de enlace) o **basedn** son incorrectos. La autenticación LDAP falla con un error de enlace incluso cuando las credenciales del usuario son correctas.
- El filtro LDAP no coincide con el esquema de directorio; para Active Directory, utilice **sAMAccountName=$userid**. Para OpenLDAP, utilice **cn=$userid** o **uid=$userid**.

Verificar configuración de RBAC

Navegue hasta Admin > AAA > Users para ver las cuentas de usuario local y sus asignaciones de dominio y rol de seguridad.

Consulte dominios de seguridad a través de la API:

<#root>

```
apic1#

moquery -c aaaDomain

# Built-in domains:
dn      : uni/userext/domain-all
name    : all                           <--- full fabric access

dn      : uni/userext/domain-common
name    : common                        <--- access to tenant common

dn      : uni/userext/domain-mgmt
name    : mgmt                          <--- access to tenant mgmt
```

Un usuario asignado al dominio all con el rol admin tiene acceso completo de lectura y escritura a todo el fabric. Un usuario asignado a un dominio de seguridad personalizado con el rol tenant-admin solo puede administrar arrendatarios asociados a ese dominio.

Configuraciones erróneas comunes de RBAC

- Usuario creado sin un dominio de seguridad: el usuario puede iniciar sesión pero no ve arrendatarios y recibe "403 Forbidden" en llamadas API. Se debe asignar al menos un dominio de seguridad.
- Función de sólo lectura asignada cuando se necesita acceso de escritura: el usuario puede ver objetos pero no puede enviar cambios. Verifique que el privilegio de rol esté establecido en writePriv.
- Falta la asignación de rol de usuario remoto en el servidor AAA: el servidor TACACS+ o RADIUS no devuelve el **cisco-av-pair** atributo que contiene **shell:domains=all/admin/**. El usuario se autentica correctamente pero no tiene funciones y no puede ver nada en el fabric.

Solución de problemas de administración OOB y en banda

Si el APIC o la IP de administración del switch no es accesible en la red, resuelva el problema de la trayectoria de administración antes de investigar SSH, HTTPS o AAA.

Situación: No se puede hacer ping a la IP OOB APIC

Problema: La estación de administración no puede hacer ping a la dirección IP de administración OOB de APIC.

Pasos de verificación:

1. Verifique que el puerto de administración APIC esté conectado físicamente y que el link esté activo.
2. Verifique que la estación de administración esté en el mismo segmento L2 o que tenga una ruta a la subred OOB.
3. Verifique que la dirección IP de administración OOB esté asignada correctamente:
   <#root>

   ```
   apic1#

   ifconfig oobmgmt

   oobmgmt: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
           inet 10.1.1.1  netmask 255.255.255.224  broadcast 10.1.1.31
   ```

4. Verifique que el gateway predeterminado sea accesible:
   <#root>

   ```
   apic1#

   netstat -rn | grep oobmgmt

   0.0.0.0         10.1.1.97       0.0.0.0         UG    0      0        0 oobmgmt
   10.1.1.96       0.0.0.0         255.255.255.224  U     0      0        0 oobmgmt
   ```

5. Si se aplica un contrato OOB, verifique que permite los protocolos requeridos. Consulte los contratos proporcionados por OOB EPG como se muestra en la sección "Verificación de Contratos OOB". Los contratos OOB se aplican como **iptables** reglas en el APIC. Puede ver las reglas guardadas desde el shell APIC:
   <#root>

   ```
   apic1#

   cat /etc/sysconfig/iptables | grep -A 20 "filter"
   ```

   Si la política INPUT es DROP y no existe una regla ACCEPT para el protocolo requerido, el contrato OOB está filtrando el tráfico.

   > Nota: El **iptables -L -n** comando para ver las reglas del núcleo en vivo requiere acceso a la raíz y no está disponible para las sesiones SSH de administración regulares.

Causa raíz: Falta la dirección de administración OOB o está mal configurada, el gateway es incorrecto o el tráfico de filtrado de contratos OOB es incorrecto.

Solución: Corrija la asignación de la dirección OOB, verifique la ruta de la red física o actualice el contrato OOB para permitir los protocolos requeridos.

Situación: No se puede alcanzar una IP de administración de switch

Problema: La estación de administración puede alcanzar el APIC pero no puede alcanzar un switch mediante OOB.

Pasos de verificación:

1. Verifique que el switch tenga una dirección OOB asignada:
   <#root>

```
apic1#

moquery -c mgmtRsOoBStNode -x 'query-target-filter=eq(mgmtRsOoBStNode.tDn,"topology/pod-1/node-101

dn      : uni/tn-mgmt/mgmtp-default/oob-default/rsooBStNode-[topology/pod-1/node-101]
addr    : 10.1.1.101/27
gw      : 10.1.1.97
```

2. Verifique que la interfaz de administración del switch tenga la IP asignada:
   <#root>

```
leaf101#

ifconfig eth0

eth0      Link encap:Ethernet  HWaddr 20:db:ea:14:42:54
          inet addr:10.1.1.101  Bcast:10.1.1.127  Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500
```

3. Verifique la ruta predeterminada de VRF de administración:
   <#root>

```
leaf101#

ip route show

default via 10.1.1.97 dev eth0
10.1.1.96/27 dev eth0 proto kernel scope link src 10.1.1.101
```

Causa raíz: Falta la asignación de la dirección OOB, el gateway es incorrecto o el puerto físico de administración del switch está inactivo.

Solución: Asigne la dirección OOB en Arrendatarios > Administración > Direcciones de administración de nodos. Verifique que el link de administración física esté activo.

Troubleshooting de Acceso SSH

Esta sección cubre escenarios donde la IP de administración es alcanzable (ping exitoso) pero la sesión SSH no puede establecer o autenticar.

Situación: Conexión SSH rechazada

Problema: El cliente SSH informa de "Conexión rechazada" cuando se conecta al APIC o al switch.

Pasos de verificación:

1. Verifique que SSH esté habilitado en la política de acceso a la administración:
   <#root>

   ```
   apic1#

   moquery -c commSsh -x 'query-target-filter=eq(commSsh.adminSt,"enabled")'

   dn        : uni/fabric/comm-default/ssh
   adminSt   : enabled
   port      : 22
   ```

   Si **adminSt** está inhabilitado, se rechazan las conexiones SSH.

2. Verifique que se esté utilizando el puerto correcto. Si el puerto SSH fue cambiado de 22:
   <#root>

   ```
   $

   ssh -p

    custom-port

   admin@10.1.1.1
   ```

3. Verifique que el contrato OOB permita TCP en el puerto SSH. Consulte la sección "Verificación de los contratos OOB".

Causa raíz: SSH desactivado en la política de acceso a la gestión, el puerto personalizado desconocido para el cliente o el filtrado de contratos OOB.

Solución: Habilite SSH en la política de acceso a la administración o utilice el puerto correcto.

Situación: Error de intercambio de claves SSH (discrepancia de cifrado o KEX)

Problema: El cliente SSH falla con "no se encontró código que coincida", "no se encontró método de intercambio de claves que coincida" o "no se encontró MAC que coincida".

Pasos de verificación:

1. Verifique el resultado detallado del cliente SSH para identificar qué algoritmos ofrece el cliente:
   <#root>

   ```
   $

   ssh -vv admin@10.1.1.1

   debug2: KEX algorithms: curve25519-sha256,diffie-hellman-group14-sha256,diffie-hellman-group14-sha
   debug2: host key algorithms: ssh-ed25519,rsa-sha2-512,rsa-sha2-256
   debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr
   debug2: MACs ctos: hmac-sha2-256,hmac-sha1
   ```

2. Compare los algoritmos ofrecidos por el cliente con los algoritmos configurados por APIC:
   <#root>

   ```
   apic1#

   moquery -c commSsh

   sshCiphers   : aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305@openssh.com
   kexAlgos     : curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp38
   sshMacs      : hmac-sha2-256,hmac-sha2-256-etm@openssh.com,hmac-sha2-512
   hostkeyAlgos : rsa-sha2-256,rsa-sha2-512,ssh-ed25519
   ```

3. Identifique la intersección. Si no hay un algoritmo común en ninguna categoría, el protocolo de enlace falla.

Nota: En la versión ACI 5.2(1) y posteriores, se reforzaron los cifrados SSH predeterminados y los algoritmos KEX. Los algoritmos heredados como **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**, **aes128-cbc**, y **hmac-sha1** ya no se ofrecen de forma predeterminada. Si ha actualizado recientemente, verifique que los clientes SSH de su entorno admitan los nuevos valores predeterminados.

Causa raíz: No hay cifrado, algoritmo KEX o MAC común entre el cliente SSH y el APIC después de una actualización de ACI o endurecimiento de cifrado.

Solución: Actualice el cliente SSH para soportar algoritmos modernos, o vuelva a agregar el algoritmo heredado requerido a la política de acceso a la administración. La reincorporación de algoritmos heredados conlleva riesgos de seguridad y no se recomienda a largo plazo.

Situación: SSH se conecta pero la autenticación falla para los usuarios locales

Problema: El protocolo de enlace SSH se ha establecido correctamente (aparece el mensaje de contraseña), pero la contraseña se rechaza para un usuario local.

Pasos de verificación:

1. Verifique que el usuario exista localmente:
   <#root>

   ```
   apic1#

   moquery -c aaaUser -x 'query-target-filter=eq(aaaUser.name,"admin")'

   dn        : uni/userext/user-admin
   name      : admin
   accountStatus : active                <--- must be active, not inactive or locked
   ```

2. Compruebe si la cuenta está bloqueada debido a un número excesivo de intentos fallidos de inicio de sesión:
   <#root>

   ```
   apic1#

   moquery -c aaaUserEp

   dn                  : uni/userext
   pwdStrengthCheck    : no
   ```

   Verifique la política de bloqueo del dominio de inicio de sesión en Admin > AAA > Security Management > Lockout Policy.

3. Compruebe que el usuario está iniciando sesión con el dominio de inicio de sesión correcto. Si el rango de autenticación predeterminado se establece en un dominio de inicio de sesión AAA remoto, el usuario debe anteponer **apic:LOCAL\\username** o **apic:fallback\\username** para forzar la autenticación local.
4. Valide el resultado de la autenticación en los registros. Active **nginx.bin.log** el APIC para el evento de inicio de sesión:
   <#root>

   ```
   apic1#

   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'admin' | tail -20
   ```

Busque el rango y el grupo de proveedores asignados al intento de inicio de sesión:

```
! Working – Successful local authentication via the fallback domain (Realm 0 = fallback/local):
||aaa||INFO||Received PAM authenticate request from nginx for Username:  apic#fallback\\admin
||aaa||INFO||auth-domain realm = local, LocalUser admin
||aaa||DBG4||Decoded username string to Domain: fallback Username: admin Realm 0, PG
||aaa||DBG4||Found password for local Username: apic#fallback\\admin
||aaa||DBG4||Calling UpdateLastLogin method for user: apic#fallback\\admin

! Not Working – Login was sent to the LDAP realm because the Default Authentication Realm is set t
! The admin user does not exist in the LDAP directory, so the LDAP search returns empty and the lo
||aaa||INFO||Received PAM authenticate request from nginx for Username:  apic#LDAP-Domain\\admin
||aaa||DBG4||Decoded username string to Domain: LDAP-Domain Username: admin Realm 3, PG LDAP-Domai
||aaa||DBG4||Adding LdapProvider ldap-server.example.com to the list, order 1
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com,
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com,
||aaa||INFO||User apic#LDAP-Domain\\admin was denied during AAA authentication
||aaa||DBG4||Setting error LDAP/AD Server Authentication DENIED
||aaa||ERROR||Unauthorized Username: admin error: LDAP/AD Server Authentication DENIED
```

Si el rango no es 0 (reserva/local), el login fue enviado a un servidor AAA remoto en lugar de a la base de datos local. El usuario debe anteponer **apic:fallback\\username** o **apic:LOCAL\\username** para forzar la autenticación local.

Causa raíz: Se está enviando una contraseña incorrecta, una cuenta bloqueada o un intento de inicio de sesión a un servidor AAA remoto en lugar de a la base de datos local.

Solución: Restablezca la contraseña, desbloquee la cuenta o utilice el prefijo de dominio de inicio de sesión correcto.

Solucionar problemas de acceso HTTPS

En esta sección se tratan situaciones en las que la interfaz de usuario web de APIC o la interfaz de programación de aplicaciones (API) de transferencia de estado representacional (REST) no es accesible a través de HTTPS.

Situación: Límite de tiempo de conexión HTTPS

Problema: El navegador muestra "ERR_CONNECTION_TIMED_OUT" o la llamada API se bloquea al conectarse al APIC en el puerto 443.

Pasos de verificación:

1. Verifique que HTTPS esté habilitado:
   <#root>

   ```
   apic1#

   moquery -c commHttps -x 'query-target-filter=eq(commHttps.adminSt,"enabled")'

   dn        : uni/fabric/comm-default/https
   adminSt   : enabled
   port      : 443
   ```

2. Verifique que el contrato OOB permite TCP 443. Consulte la sección "Verificación de Contratos OOB".
3. Pruebe desde el propio APIC para confirmar que el proceso HTTPS está escuchando:
   <#root>

   ```
   apic1#

   ss -tlnp | grep 443

   LISTEN  0  128  *:443  *:*  users:(("nginx",pid=12345,fd=6))
   ```

Causa raíz: HTTPS deshabilitado, el filtrado de contratos OOB TCP 443 o el proceso nginx en el APIC se ha bloqueado.

Solución: Habilite HTTPS en la política de acceso a la gestión, actualice el contrato OOB o reinicie el servicio web en el APIC.

Situación: El navegador muestra el error de intercambio de señales TLS

Problema: El navegador muestra "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" o un error de TLS similar.

Pasos de verificación:

1. Verifique la versión del protocolo TLS configurada en el APIC:
   <#root>

   ```
   apic1#

   moquery -c commHttps

   sslProtocols : TLSv1.2
   ```

2. Compruebe que el explorador es compatible con TLSv1.2. Los exploradores muy antiguos (por ejemplo, Internet Explorer 10 y versiones anteriores) no son compatibles con TLSv1.2 de forma predeterminada.

Causa raíz: El APIC solo ofrece TLSv1.2 (el valor predeterminado) y el navegador o el cliente de API solo admite versiones de TLS más antiguas.

Solución: Actualice el explorador o el cliente. Si debe admitir clientes más antiguos temporalmente, agregue TLSv1.1 a la directiva de acceso a la administración, pero esto supone un riesgo para la seguridad.

Situación: Límite del acelerador API

Problema: Las llamadas de API REST fallan intermitentemente con errores de HTTP 503 o la interfaz de usuario web se ralentiza durante una automatización intensa.

Pasos de verificación:

<#root>

```
apic1#

moquery -c commHttps

throttleSt   : enabled
throttleRate : 2                        <--- requests per second per user
```

Si la velocidad del acelerador es muy baja y los scripts de automatización envían muchas solicitudes por segundo, el APIC rechaza las solicitudes en exceso.

Causa raíz: La velocidad del acelerador por usuario es demasiado baja para la carga de trabajo de automatización.

Solución: Aumente la velocidad del acelerador según la política de acceso a la gestión u optimice los scripts de automatización para reducir la frecuencia de las solicitudes. Como alternativa, desactive la limitación si el fabric no está compartido.

Troubleshooting AAA — TACACS+

Esta sección cubre los fallos de autenticación de TACACS+. El APIC se comunica con el servidor TACACS+ a través del puerto TCP 49.

Verificación operativa

Los switches ACI no admiten el **test aaa** comando disponible en NX-OS independiente. Para verificar el funcionamiento de TACACS+, utilice el APIC para comprobar el estado del proveedor, los fallos y el historial de sesiones de inicio de sesión.

Verifique si hay fallas activas en el proveedor TACACS+:

```
<#root>

apic1#

moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"tacacsplusprovider")'
```

Si no se devuelve ningún error, el APIC considera que el proveedor es accesible. Si hay errores, el resultado incluye códigos de error como F1773 (proveedor inalcanzable) o F1774 (error de autenticación).

Verifique la configuración del proveedor TACACS+:

```
<#root>

apic1#

moquery -c aaaTacacsPlusProvider

dn              : uni/userext/tacacsext/tacacsplusprovider-10.1.1.50
name            : 10.1.1.50
authProtocol    : pap
port            : 49
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default
```

Verifique el alcance básico de la red desde el APIC al servidor TACACS+:

```
<#root>

apic1#

ping 10.1.1.50

PING 10.1.1.50 (10.1.1.50): 56 data bytes
64 bytes from 10.1.1.50: icmp_seq=0 ttl=64 time=0.5 ms
```

Intente iniciar sesión en el APIC con el dominio de inicio de sesión TACACS+ y compruebe el

resultado de la sesión:

<#root>

apic1#

moquery -c aaaSessionLR -x 'order-by=aaaSessionLR.created|desc' -x page-size=5

Mire el **descr** campo para determinar si la falla se debió al rechazo de la autenticación o a un problema de conectividad.

Valide el flujo de autenticación TACACS+ en los registros APIC. Filtro para el nombre de usuario en cuestión:

<#root>

apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i '*username*' | tail -20

Los inicios de sesión de TACACS+ siguen el mismo flujo de **nginx.bin.log** autenticación que LDAP (consulte la sección Verificación operativa de LDAP para ver ejemplos completos de registros reales). Las diferencias clave para TACACS+ son:

- `DefaultAuthMo especifica el rango 2`: el rango 2 indica TACACS+ (frente al rango 3 para LDAP).
- `Agregar TacACSProvider <IP> a la lista` — identifica el servidor TACACS+ con el que se está contactando (frente a `LdapProvider` para LDAP).
- `TACACS+ Cisco-avpair (shell:domains=all/admin/)`: el par AV es devuelto directamente por el servidor TACACS+ (en lugar de ser convertido desde un mapa de grupo LDAP).

Un inicio de sesión exitoso de TACACS+ muestra la misma progresión: Solicitud PAM → selección de rango → búsqueda de proveedor → análisis de pares AV → inyección de usuario → UserDomain y asignación de rol → `privilegios de escritura de administrador`.

Un inicio de sesión fallido de TACACS+ termina con `Usuario <nombre de usuario> fue denegado durante la autenticación AAA` y error `Unauthorized ...: Autenticación de servidor AAA DENEGADA`, el mismo patrón que una denegación LDAP.

Situación: Error de autenticación de TACACS+

Problema: El login falla con "Authentication Failed" cuando el usuario selecciona un dominio de login TACACS+.

Pasos de verificación:

1. Verifique si hay fallas activas en el proveedor TACACS+:
   <#root>

   ```
   apic1#
   ```

   ```
   moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"tacacsplusprovider")'
   ```

   El error F1773 indica un problema de conectividad. El error F1774 indica un rechazo de autenticación.

2. Verifique el alcance de la red desde el APIC al servidor TACACS+:
   <#root>

   ```
   apic1#
   ```

   ```
   ping 10.1.1.50
   ```

   ```
   PING 10.1.1.50 (10.1.1.50): 56 data bytes
   64 bytes from 10.1.1.50: icmp_seq=0 ttl=64 time=0.5 ms
   ```

3. Si el ping se realiza correctamente pero la autenticación falla, verifique las coincidencias secretas compartidas tanto en la configuración del proveedor APIC como en la configuración del servidor TACACS+.
4. Verifique las sesiones de inicio de sesión más recientes para ver los detalles de la falla:
   <#root>

   ```
   apic1#
   ```

   ```
   moquery -c aaaSessionLR -x 'order-by=aaaSessionLR.created|desc' -x page-size=5
   ```

5. Verifique los registros del servidor TACACS+ para el intento de autenticación. Un intento correcto registrado en el servidor pero rechazado indica un problema de configuración del usuario en el servidor (por ejemplo, falta coincidencia de contraseña o falta cuenta de usuario).
6. Verifique el APIC **nginx.bin.log** para obtener el flujo de autenticación completo. Filtre por el nombre de usuario en lugar de palabras clave específicas para que no se pierdan los mensajes intermedios:
   <#root>

   ```
   apic1#
   ```

   ```
   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'tacuser1' | tail -20
   ```

Compare el resultado con los ejemplos de funcionamiento y de no funcionamiento de la sección Verificación operativa anterior. Indicadores clave:

- `fue denegado` o `DENEGADO`: se alcanzó el servidor TACACS+ pero se rechazaron las credenciales. Compruebe que el usuario existe en el servidor y que la contraseña coincide.
- No hay mensajes específicos del proveedor después de `Agregar TacacsProvider`: el servidor está inaccesible o con tiempo de espera agotado. Verifique la disponibilidad de la red y el EPG de administración.
- `La inyección de usuario remoto... se completó` seguida de líneas de comprobación de funciones: la autenticación se realizó correctamente, pero el problema puede estar relacionado con la asignación de funciones (consulte la sección de pares AV a continuación).

TACACS+ cisco-av-pair para RBAC

Para los usuarios remotos autenticados a través de TACACS+, el servidor debe devolver el **cisco-av-pair** atributo en la respuesta de autorización. Este atributo asigna al usuario a los roles y dominios de seguridad de ACI.

Formato:

`shell:domains=`*`domain/role/`*

Examples:

- Administración completa: **shell:domains=all/admin/**
- Sólo lectura para todos: **shell:domains=all/read-all/**
- Administrador de arrendatarios para un dominio específico: **shell:domains=TenantA/tenant-admin/**
- Varios dominios: **shell:domains=all/admin/,TenantA/tenant-admin/**

Si falta este atributo o está mal formado, el usuario se autentica correctamente pero no tiene funciones y no puede ver ningún objeto en la interfaz de usuario de APIC.

Nota: El acceso SSH a los switches de columna y hoja requiere el rol admin con el privilegio write en el dominio de seguridad all. El par AV mínimo para el acceso SSH del switch es **shell:domains=all/admin/**. Los usuarios con funciones no administrativas (por ejemplo, `read-all`, `tenant-admin`, `aaa`) o usuarios asignados a un dominio de seguridad distinto de `all` pueden

---

iniciar sesión en el APIC pero se les deniega el acceso SSH a los switches. El registro de APIC muestra que `se deniegan los inicios de sesión no administrativos en el switch` para estos usuarios.

Valide el par AV recibido mediante la comprobación **nginx.bin.log**. Filtre por el nombre de usuario para ver el flujo de inyección de roles completo:

<#root>

apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i '*username*' | tail -20

Para TACACS+, el par AV se registra como `TACACS+ Cisco-avpair (shell:domains=...)`. Una inyección exitosa muestra `Injection of remote user <username> was completed` seguido de `Found UserDomain` y `admin write privilege` lines (vea la sección LDAP Operational Verification para obtener ejemplos completos de este flujo con salida de registro real).

Si el formato de par AV no es válido, el registro muestra `Injection of remote user <username> data FAILED - error message is Invalid shell:domains string`. Si el usuario se autentica con un rol no administrador, se deniega el SSH a los switches y se deniegan los inicios de sesión `no administrativos en el switch`.

Causa raíz: Discordancia de secreto compartido, servidor inaccesible desde la red de administración, usuario no existente en el servidor TACACS+ o el EPG de administración en el proveedor es incorrecto.

Solución: Corrija el secreto compartido, corrija la disponibilidad o cree el usuario en el servidor TACACS+.

Validar registros de autenticación de switch de hoja

En los switches de columna y hoja, los eventos de inicio de sesión SSH se registran en **pam.module.log** y **nginx.log**. El **pam.module.log** muestra el resultado de la autenticación de PAM (aceptar o rechazar). El **nginx.log** contiene el flujo AAA completo —selección de rango, búsqueda de proveedor, comunicación LDAP/TACACS+/RADIUS, análisis de pares AV y asignación de roles— idéntico al **nginx.bin.log** del APIC. Estos registros se aplican a todos los tipos de AAA remotos (TACACS+, RADIUS, LDAP).

Verifique **pam.module.log** el resultado de la autenticación:

<#root>

```
leaf101#
```

cat /var/sysmgr/tmp_logs/pam.module.log | tail -30

Funcionando — autenticación remota exitosa en el switch:

```
||pam||INFO||Received pamauth request for jsmith
||pam||INFO||User: jsmith, rhost: 10.1.1.50, tty: ssh
||pam||INFO||Connecting to default PAM socket path /var/run/mgmt/socket/pam
||pam||INFO||Securitymgr is ALIVE
||pam||INFO||Connection successful - attempting to authenticate user jsmith client ssh
||pam||INFO||Sent authentication credentials (total pkt len 58)
||pam||INFO||Received authentication response from PAM server
||pam||INFO||User jsmith from 10.1.1.50 authenticated by securitymgrAG with UNIX user id 16004
||pam||INFO||pam_putenv username=jsmith
||pam||INFO||pam_putenv remote=1
||pam||INFO||pam_putenv unix_user_id=16004
||pam||INFO||pam_putenv groupuid=15374
||pam||INFO||returning success
```

El **remote=1** indicador confirma que el usuario fue autenticado por un servidor AAA remoto.

No funciona: el usuario fue rechazado. SecurityMgrAG deniega al usuario y el switch intenta realizar una búsqueda de usuario local como reserva final:

```
||pam||INFO||Received pamauth request for baduser
||pam||INFO||User: baduser, rhost: 10.1.1.50, tty: ssh
||pam||INFO||Connection successful - attempting to authenticate user baduser client ssh
||pam||INFO||ERROR: securitymgrAG rejected user baduser from 10.1.1.50
||pam||INFO||You entered user baduser ...attempting to match against local users
||pam||INFO||Username baduser is not a special local auth user
```

Si no aparece ninguna entrada de PAM para el usuario, es probable que la conexión SSH se haya rechazado antes de alcanzar la fase de PAM (por ejemplo, debido a una discordancia de cifrado o a que el usuario ha cancelado la conexión).

Para obtener una vista más detallada del flujo de autenticación en el switch, verifique **nginx.log**. Este registro contiene la cadena de decisión AAA completa, con el mismo formato y mensajes que **nginx.bin.log** en el APIC:

<#root>

```
leaf101#
```

```
grep '||aaa||' /var/sysmgr/tmp_logs/dme_logs/nginx.log | grep -i 'username' | tail -20
```

En funcionamiento — autenticación LDAP correcta en un switch (comparar con los ejemplos de LDAP APIC en la sección Verificación operativa de LDAP — los mensajes son los mismos):

```
||aaa||INFO||Received PAM authenticate request from nginx for Username:  jsmith
||aaa||DBG4||Decoded username string to Domain:  Username: jsmith Realm 3, PG LDAP-Domain
||aaa||DBG4||Username: jsmith does not exist locally
||aaa||DBG4||Initialized LdapAuthenticationBroker for lookup of jsmith (address 10.1.1.100, hostname ss
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com, filte
||aaa||INFO||LDAP Record DN : CN=jsmith,CN=Users,DC=example,DC=com
||aaa||DBG4||Bind to UserDN CN=jsmith,CN=Users,DC=example,DC=com using user password successful
||aaa||INFO||User AAA authentication was successful
||aaa||DBG4||Injection of remote user jsmith was completed
||aaa||DBG4||Checking all UserDomains under remote Username: jsmith
||aaa||DBG4||Found UserDomain all under remote Username: jsmith
||aaa||DBG4||Found Username: admin with admin write privileges under UserDomain all - user is an admin
```

El switch **nginx.log** es particularmente útil cuando **pam.module.log** muestra un rechazo pero no explica por qué. El archivo nginx.log revela el rango AAA, el proveedor y la razón de falla específica (por ejemplo, la búsqueda LDAP devolvió vacío, el tiempo de espera TACACS+ o la inyección de par AV falló).

Troubleshooting AAA - RADIUS

Esta sección trata sobre fallas de autenticación RADIUS. El APIC se comunica con el servidor RADIUS a través del puerto UDP 1812 (autenticación) y opcionalmente el puerto UDP 1813 (contabilidad).

Verificación operativa

Los switches ACI no admiten el **test aaa** comando disponible en NX-OS independiente. Utilice los métodos siguientes para verificar el funcionamiento de RADIUS.

Verifique la configuración del servidor RADIUS y las estadísticas de alcance desde un switch hoja:

<#root>

```
leaf101#
```

```
show radius-server


timeout value:5
retransmission count:3
deadtime value:0
source interface:any available
total number of servers:1

following RADIUS servers are configured:
        10.1.1.51:
                available for authentication on port: 1812
                Radius shared secret:********
                timeout:5
                retries:1
```

Situación: Error de autenticación RADIUS

Problema: El login falla cuando un usuario selecciona un dominio de login RADIUS.

Pasos de verificación:

1. Verifique las estadísticas del servidor RADIUS de un switch para detectar señales de tiempos de espera o fallas:
   <#root>

   ```
   leaf101#

   show radius-server statistics 10.1.1.51

   Authentication Statistics
       failed transactions: 0
       sucessfull transactions: 5
       requests sent: 5
       requests timed out: 0
   ```

   Un conteo alto en solicitudes con tiempo de espera agotado indica que el servidor RADIUS es inalcanzable o que el secreto compartido no coincide (RADIUS descarta silenciosamente los paquetes en la discordancia del secreto compartido).

2. Verifique el alcance de la red al servidor RADIUS:
   <#root>

   ```
   apic1#

   ping 10.1.1.51

   PING 10.1.1.51 (10.1.1.51): 56 data bytes
   64 bytes from 10.1.1.51: icmp_seq=0 ttl=64 time=0.5 ms
   ```

3. Verifique las coincidencias secretas compartidas entre el APIC y el servidor RADIUS. A

diferencia de TACACS+, que utiliza TCP e informa de fallos de conexión, RADIUS utiliza UDP y descarta paquetes de forma silenciosa cuando el secreto compartido no coincide. El único síntoma es un tiempo de espera.

4. Verifique los registros del servidor RADIUS. FreeRADIUS en modo de depuración (**radiusd -X**) muestra cada solicitud e indica si fue aceptada, rechazada o si tenía una discordancia secreta compartida.
5. Verifique el APIC **nginx.bin.log** para el flujo de autenticación RADIUS. Filtrar por nombre de usuario:
   <#root>

   apic1#

   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i '*username*' | tail -20

   Los inicios de sesión RADIUS siguen el mismo flujo de **nginx.bin.log** autenticación que LDAP y TACACS+ (consulte la sección Verificación operativa de LDAP para ver ejemplos completos de registros reales). Las diferencias clave para RADIUS son:

   - `Agregar RadiusProvider <IP> a la lista`: identifica el servidor RADIUS (frente a `TacacsProvider` o `LdapProvider`).
   - El número de rango para RADIUS varía según la configuración.

   Un inicio de sesión exitoso de RADIUS termina con `Inyección de usuario remoto ... fue completado` y `privilegios de escritura de administrador`.

   Un login fallido de RADIUS termina con `fue denegado durante la autenticación AAA` y `DENIED`.

   Si no aparece ningún mensaje específico de RADIUS después de la línea `Adding RadiusProvider`, el servidor ha agotado el tiempo de espera. A diferencia de TACACS+, que utiliza TCP e informa de fallos de conexión, RADIUS utiliza UDP y descarta paquetes de forma silenciosa cuando el secreto compartido no coincide. El único síntoma es un tiempo de espera seguido de una negación.

6. Verifique si hay fallas activas en el proveedor RADIUS:
   <#root>

   apic1#

   moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"radiusprovider")'

RADIUS cisco-av-pair para RBAC

RADIUS utiliza el mismo **cisco-av-pair** atributo que TACACS+ para la asignación de roles RBAC. El servidor RADIUS debe devolver este atributo en la respuesta Access-Accept:

<#root>

```
# FreeRADIUS users file entry:
labadmin  Cleartext-Password := "password"
```

```
Cisco-AVPair = "shell:domains=all/admin/"
```

En FreeRADIUS, esto se configura en el **users** archivo o backend LDAP. Para ISE, se configura en el perfil de autorización como un atributo avanzado.

Causa raíz: Discordancia de secreto compartido (más común con RADIUS: provoca tiempos de espera silenciosos), servidor inalcanzable, puerto de autenticación incorrecto o cuenta de usuario faltante en el servidor RADIUS.

Solución: Corrija el secreto compartido, verifique la disponibilidad de UDP 1812 o configure el usuario en el servidor RADIUS.

Troubleshooting AAA — LDAP

Esta sección cubre los errores de autenticación LDAP. El APIC se conecta al servidor LDAP a través del puerto TCP 389 (LDAP) o el puerto TCP 636 (LDAP con SSL).

Verificación operativa

Los switches ACI no admiten el **test aaa** comando disponible en NX-OS independiente. Para verificar el funcionamiento de LDAP, verifique los fallos del proveedor y la configuración desde el APIC.

Verifique si hay fallas activas en el proveedor LDAP:

<#root>

```
apic1#
```

```
moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"ldapprovider")'
```

El error F1777 indica un problema de conectividad. El error F1778 indica una falla de autenticación o de enlace. Si no se devuelve ningún error, el APIC considera que el proveedor es accesible.

Verifique el alcance básico de la red al servidor LDAP:

<#root>

```
apic1#

ping 10.1.1.52

PING 10.1.1.52 (10.1.1.52): 56 data bytes
64 bytes from 10.1.1.52: icmp_seq=0 ttl=64 time=0.5 ms
```

Para LDAP, verifique también la conectividad TCP con el puerto 389 (o 636 para LDAP). Si el APIC puede hacer ping al servidor pero persisten los fallos de LDAP, el problema suele ser un DN de enlace incorrecto, una contraseña incorrecta o un firewall que bloquea el puerto LDAP.

Valide el flujo de autenticación LDAP en los registros de APIC. Filtrar por nombre de usuario:

<#root>

```
apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'jsmith' | tail -20
```

En funcionamiento: un inicio de sesión LDAP correcto muestra el flujo completo de búsqueda, vinculación y asignación de roles:

```
||aaa||INFO||Received PAM authenticate request from nginx for Username:  jsmith
||aaa||DBG4||DefaultAuthMo specifies realm 3. Provider Group LDAP-Domain !
||aaa||DBG4||Decoded username string to Domain:  Username: jsmith Realm 3, PG LDAP-Domain
||aaa||DBG4||Username: jsmith does not exist locally
||aaa||DBG4||Initialized LdapAuthenticationBroker for lookup of jsmith (address 10.1.1.50, hostname ssh
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com, filte
||aaa||INFO||LDAP Record DN : CN=jsmith,CN=Users,DC=example,DC=com
||aaa||DBG4||Bind to UserDN CN=jsmith,CN=Users,DC=example,DC=com using user password successful
||aaa||DBG4||    Adding WriteRole: admin
||aaa||DBG4||Converted to CiscoAVPair string shell:domains = all/admin/
||aaa||DBG4||Injection of remote user jsmith was completed
||aaa||DBG4||Checking all UserDomains under remote Username: jsmith
||aaa||DBG4||Found UserDomain all under remote Username: jsmith
||aaa||DBG4||Found Username: admin with admin write privileges under UserDomain all - user is an admin
```

No funciona — usuario no encontrado en el directorio LDAP (la búsqueda devuelve un conjunto vacío):

```
||aaa||INFO||Received PAM authenticate request from nginx for Username:  baduser
||aaa||DBG4||Decoded username string to Domain:  Username: baduser Realm 3, PG LDAP-Domain
||aaa||DBG4||Username: baduser does not exist locally
||aaa||DBG4||Initialized LdapAuthenticationBroker for lookup of baduser (address 10.1.1.50, hostname RE
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com, filte
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com, filte
||aaa||INFO||User baduser was denied during AAA authentication
||aaa||ERROR||Unauthorized Username: baduser error: LDAP/AD Server Authentication DENIED
```

Situación: Error de autenticación LDAP

Problema: El inicio de sesión falla cuando un usuario selecciona un dominio de inicio de sesión LDAP.

Pasos de verificación:

1. Verifique la disponibilidad del servidor LDAP desde el APIC:
   <#root>

   ```
   apic1#
   ```

   ping 10.1.1.52

   ```
   PING 10.1.1.52 (10.1.1.52): 56 data bytes
   64 bytes from 10.1.1.52: icmp_seq=0 ttl=64 time=0.5 ms
   ```

2. Verifique si hay fallas activas del proveedor LDAP:
   <#root>

   ```
   apic1#
   ```

   moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"ldapprovider")'

3. Verifique la configuración del proveedor LDAP:
   <#root>

   ```
   apic1#
   ```

   moquery -c aaaLdapProvider -x 'query-target-filter=eq(aaaLdapProvider.name,"10.1.1.52")'

   ```
   rootdn    : CN=binduser,CN=Users,DC=example,DC=com    <--- bind DN
   basedn    : CN=Users,DC=example,DC=com                 <--- search base
   filter    : sAMAccountName=$userid                      <--- search filter
   attribute : memberOf                                    <--- group mapping attribute
   enableSSL : no                                          <--- LDAP vs LDAPS
   port      : 389
   ```

4. Verifique que el usuario exista en el directorio LDAP bajo el DN base configurado y que coincida con el filtro. Para Active Directory, el **sAMAccountName** atributo del usuario debe coincidir con el nombre de usuario introducido al iniciar sesión. Para OpenLDAP, el atributo **cn**

o debe coincidir con el **uid** atributo.

5. Si utiliza LDAPS (puerto 636), verifique la cadena de certificados SSL. Si **SSLValidationLevel** se establece en strict, el APIC rechazará la conexión si el certificado del servidor no es confiable o ha caducado.
6. Verifique el APIC **nginx.bin.log** para el flujo de autenticación LDAP completo. Filtre por el nombre de usuario para que no se pierdan los mensajes intermedios:
   <#root>

   apic1#

   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'jsmith' | tail -20

   Compare el resultado con los ejemplos de funcionamiento y de no funcionamiento de la sección Verificación operativa anterior. Se pueden encontrar patrones de falla adicionales específicos de LDAP mediante una búsqueda amplia en el registro:

   <#root>

   apic1#

   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'LDAP\|ldap' | tail -20

   Patrones comunes de no funcionamiento (comparar con los ejemplos de verificación operativa anteriores para el flujo completo):

```
! Not Working – User not found (wrong baseDn, wrong filter, or user does not exist).
! Real example – "baduser" does not exist in the LDAP directory:
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com,
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com,
||aaa||INFO||User baduser was denied during AAA authentication
||aaa||ERROR||Unauthorized Username: baduser error: LDAP/AD Server Authentication DENIED
```

   Otros patrones de falla de LDAP a buscar:

   - La búsqueda de LDAP ha agotado el tiempo de espera (servidor inalcanzable, lento o firewall que bloquea el puerto 389/636) — `error al` buscar `Ldap Search: código de retorno para ldap_search_ext_s: -5: Tiempo agotado`
   - Error de enlace (la contraseña de enlace o raíz es incorrecta o el servidor rechazó la conexión): `error al` buscar `Ldap Search: código de retorno para ldap_search_ext_s: -1: No se puede establecer contacto con el servidor LDAP`
   - Se ha encontrado un usuario pero la contraseña es incorrecta (se produce un error en el enlace con la contraseña de usuario): el registro muestra la línea `LDAP Record DN` pero va seguido de un mensaje denegado sin `enlace a UserDN... con éxito`.

Mapa de grupo LDAP para RBAC

LDAP utiliza mapas de grupo en lugar del **cisco-av-pair** atributo. El **attribute** campo del proveedor LDAP especifica qué atributo LDAP contiene la información del grupo. Para Active Directory, suele ser **memberOf.**

El APIC compara el DN de grupo devuelto con las Reglas de Mapa de Grupo LDAP (**aaaLdapGroupMapRule**) configuradas para asignar el dominio de seguridad y el rol apropiados. Si no coincide ninguna regla de asignación de grupo, el usuario se autentica pero no tiene funciones.

Alternativamente, puede configurar el **attribute** para **CiscoAVPair** y almacenar el **shell:domains=all/admin/** valor directamente en los atributos LDAP del usuario, que sigue el mismo formato que TACACS+ y RADIUS.

Causa raíz: DN de enlace o contraseña incorrectos, el DN base no contiene el usuario, el filtro de búsqueda no coincide con el esquema de directorio, el error de validación del certificado LDAPS o las reglas de asignación de grupo que faltan.

Solución: Corrija la configuración del proveedor (DN de enlace, DN base, filtro, configuración de SSL). Para problemas de RBAC, verifique que las reglas de mapa de grupo coincidan con los grupos LDAP a los que pertenece el usuario.

Troubleshooting de RBAC y Privilegios de Usuario

En esta sección se tratan situaciones en las que el usuario se autentica correctamente pero no tiene el nivel de acceso esperado.

Situación: El Usuario Ha Iniciado Sesión Pero No Ve Ningún Arrendatario

Problema: Un usuario remoto inicia sesión mediante TACACS+, RADIUS o LDAP. El inicio de sesión se ha realizado correctamente, pero el usuario no ve ningún arrendatario en la interfaz de usuario y las llamadas a la API devuelven resultados vacíos o "403 Forbidden".

Pasos de verificación:

1. Compruebe la sesión del usuario para ver qué funciones se asignaron al iniciar sesión:
   <#root>

   ```
   apic1#
   ```

```
moquery -c aaaSessionLR -x 'query-target-filter=wcard(aaaSessionLR.descr,"jsmith")' -x 'order-by=a

dn          : subj-[uni/userext/remoteuser-jsmith]/sess-123456789
descr       : [user jsmith] From-10.1.1.100-client-type-https-Success
```

El **descr** campo muestra el resultado del inicio de sesión. Si el usuario se autenticó correctamente pero no tiene roles RBAC, el servidor AAA no devolvió una coincidencia válida **cisco-av-pair** o de mapa de grupo LDAP.

2. Compruebe el APIC **nginx.bin.log** para ver el par AV y la asignación de roles durante el inicio de sesión. Filtrar por nombre de usuario:
<#root>

```
apic1#

grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'jsmith' | tail -20
```

Busque la inserción de roles y los mensajes de asignación de dominio:

Trabajando — Par AV convertido desde el mapa de grupo LDAP, el usuario obtiene el rol de administrador:

```
||aaa||DBG4||    Adding WriteRole: admin
||aaa||DBG4||Converted to CiscoAVPair string shell:domains = all/admin/
||aaa||DBG4||Injection of remote user jsmith was completed
||aaa||DBG4||Checking all UserDomains under remote Username: jsmith
||aaa||DBG4||Found UserDomain all under remote Username: jsmith
||aaa||DBG4||Found Username: admin with admin write privileges under UserDomain all - user is an a
```

No funciona: si no aparece una línea **Cisco-avpair** o **Converted to CiscoAVPair** en el flujo, el servidor AAA no devolvió el atributo y no coincidió ninguna regla de mapa de grupo LDAP. Busque **Checking all UserDomains Found UserDomain** sin líneas a continuación: el usuario se autenticó pero no tiene asignaciones de funciones. Si aparece un **Injection ... data FAILED** mensaje, el formato de cadena de par AV no es válido.

3. Verifique que el servidor AAA devuelve el **cisco-av-pair** atributo (para TACACS+ o RADIUS) o la pertenencia al grupo LDAP correcta (para LDAP). Verifique la configuración del servidor AAA:
    - TACACS+: Compruebe que el perfil de usuario incluye **cisco-av-pair** con el formato **shell:domains=all/admin/.**
    - RADIUS: Verifique que el perfil de usuario vuelva **Cisco-AVPair = "shell:domains=all/admin/"** en Access-Accept.
    - LDAP: Verifique que el usuario sea miembro de un grupo LDAP que coincida con una regla de mapa de grupo LDAP configurada (**aaaLdapGroupMapRule**).
4. Si el atributo está presente pero el usuario aún no tiene acceso, verifique que el nombre de

dominio de seguridad en el atributo coincida con un dominio de seguridad existente en el APIC:
<#root>

```
apic1#
moquery -c aaaDomain
```

Si el **cisco-av-pair** hace referencia a un dominio que no existe (por ejemplo, **shell:domains=NonExistentDomain/admin/**), la asignación de función falla de forma silenciosa.

Causa raíz: El servidor AAA no devuelve los atributos de asignación RBAC, el formato del atributo es incorrecto o el dominio de seguridad al que se hace referencia en el atributo no existe en el APIC.

Solución: Configure el servidor AAA para que devuelva la asignación de grupo **cisco-av-pair** o correcta. Verifique que el dominio de seguridad exista en el APIC.

Situación: El usuario puede ver pero no modificar la configuración

Problema: Un usuario puede iniciar sesión y examinar objetos, pero recibe un error cuando intenta enviar los cambios.

Pasos de verificación:

1. Compruebe las asignaciones de funciones del usuario:
<#root>

```
apic1#
moquery -c aaaUserRole -x 'query-target-filter=wcard(aaaUserRole.dn,"user-jsmith")'

dn        : uni/userext/user-jsmith/userdomain-all/role-read-all
name      : read-all
privType  : readPriv                  <--- read only, no write privilege
```

2. Si el usuario necesita acceso de escritura, la función debe conceder **writePriv**. Los roles comunes con privilegios de escritura incluyen admin, tenant-admin, access-admin y fabric-admin.
3. Valide la asignación de roles en los registros de APIC. Filtrar por nombre de usuario:
<#root>

```
apic1#
grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'jsmith' | tail -20
```

Busque los mensajes de asignación de roles cerca del final del flujo de autenticación:

Trabajando: el usuario tiene el rol de escritura de administrador (desde un inicio de sesión LDAP real):

```
||aaa||DBG4||Checking all UserDomains under remote Username: jsmith
||aaa||DBG4||Found UserDomain all under remote Username: jsmith
||aaa||DBG4||Found Username: admin with admin write privileges under UserDomain all - user is an a
```

No funciona: si el registro muestra `UserRole no administrador` con `privilegios de lectura` en lugar de `privilegios de escritura de administrador`, el usuario tiene un rol de sólo lectura y no puede modificar la configuración. Busque líneas como:

```
||aaa||DBG4||Found non-admin UserRole read-all (read privileges) under UserDomain all
```

Si el registro muestra solamente `privilegios de lectura` y ningún `privilegio de escritura`, actualice el rol del usuario o el par AV en el servidor AAA.

Causa raíz: El usuario tiene una función de sólo lectura (por ejemplo, read-all u ops) en lugar de una función con capacidad de escritura.

Solución: Actualice la asignación de rol del usuario en el APIC (para usuarios locales) o actualice el **cisco-av-pair** en el servidor AAA (para usuarios remotos) para incluir un rol con privilegios de escritura.

Situación: El Usuario Puede Acceder A Algunos Arrendatarios, Pero No A Otros

Problema: Un usuario puede ver y administrar un arrendatario pero no puede ver a otros arrendatarios, aunque necesiten acceso.

Pasos de verificación:

1. Compruebe la asignación de dominio de seguridad del usuario:
   <#root>

   ```
   apic1#
   moquery -c aaaUserDomain -x 'query-target-filter=wcard(aaaUserDomain.dn,"user-jsmith")'
   ```

```
dn    : uni/userext/user-jsmith/userdomain-TenantA
name  : TenantA                       <--- only has access to TenantA
```

2. Los dominios de seguridad se asignan a los arrendatarios. Si el usuario necesita acceder al arrendatario B, también se le debe asignar al dominio de seguridad asociado con el arrendatario B o al dominio all.
3. Para los usuarios remotos, confirme que el par AV o el mapa de grupo LDAP asigna los dominios correctos. Verifique el APIC **nginx.bin.log** para la asignación de dominio al iniciar sesión. Filtrar por nombre de usuario:
   <#root>

   apic1#

   grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'jsmith' | tail -20

   Trabajando: el usuario tiene el dominio all (visibilidad completa), desde un inicio de sesión LDAP real:

```
||aaa||DBG4||Converted to CiscoAVPair string shell:domains = all/admin/
||aaa||DBG4||Injection of remote user jsmith was completed
||aaa||DBG4||Found UserDomain all under remote Username: jsmith
||aaa||DBG4||Found Username: admin with admin write privileges under UserDomain all - user is an a
```

   No funciona: si el usuario sólo tiene un dominio de arrendatario, en los mensajes sólo aparecerá ese dominio en lugar de todos los **Found UserDomain**mensajes. Por ejemplo, `Found UserDomain TenantA` significa que el usuario sólo puede ver TenantA. El usuario necesita dominios adicionales agregados al par AV en el servidor AAA, o el dominio all para el acceso completo.

Causa raíz: El usuario está asignado a un dominio de seguridad restringido que solo cubre a arrendatarios específicos.

Solución: Agregue los dominios de seguridad necesarios a la configuración del usuario o utilice el dominio all para obtener acceso completo.

Recuperación de contraseña y acceso de emergencia

Si todas las cuentas de administrador están bloqueadas o el servidor AAA remoto es inalcanzable y el rango predeterminado ha sido cambiado, utilice uno de estos métodos de recuperación:

Dominio de inicio de sesión alternativo

ACI proporciona un dominio de inicio de sesión de reserva integrado que siempre utiliza la autenticación local, independientemente del rango de autenticación predeterminado. Para utilizarlo:

- SSH: Inicie sesión como **apic:fallback\\admin** (o **apic#fallback\\admin** dependiendo de la versión).
- GUI: En el menú desplegable Dominio de la pantalla de inicio de sesión, seleccione reserva y utilice las credenciales locales.

Acceso a consola

Si el rango de autenticación de la consola se establece en local (valor predeterminado), siempre puede iniciar sesión a través del puerto de la consola APIC con credenciales locales. Si se desconoce la contraseña del administrador local, se puede restablecer mediante Cisco Integrated Management Controller (CIMC) (para APIC físicos) o la consola de hipervisor (para APIC virtuales).

Nota: Si el rango de autenticación de la consola se ha cambiado a un servidor AAA remoto y ese servidor es inalcanzable, el acceso a la consola también fallará. Este es un escenario de bloqueo común. Mantenga siempre el rango de autenticación de la consola establecido en local.

Referencia de fallos comunes

Los siguientes fallos de ACI suelen estar asociados a problemas de AAA y acceso remoto:

- F1773 — Problema de conectividad del proveedor TACACS+. El APIC no puede alcanzar el servidor TACACS+.
- F1774: falla de autenticación de TACACS+. Se puede acceder al servidor, pero se rechazó el intento de autenticación.
- F1775: problema de conectividad del proveedor RADIUS.
- F1776: falla de autenticación RADIUS.
- F1777 — Problema de conectividad del proveedor LDAP.
- F1778 — Falla de autenticación LDAP.
- F0532: subred de administración no configurada para un nodo.

Consulta de fallos AAA activos:

<#root>

```
apic1#
```

```
moquery -c faultInst -x 'query-target-filter=or(wcard(faultInst.dn,"tacacsplusprovider"),wcard(faultInst
```

Referencias

- Solución de problemas de administración de ACI y servicios principales: políticas de POD
- Guía de configuración básica de Cisco APIC, versión 6.1(x) — Gestión
- Guía de configuración de seguridad de Cisco APIC: acceso, autenticación y cuentas

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).