Solucionar problemas de acesso remoto em uma estrutura da ACI

Introdução

Este documento descreve como verificar, solucionar problemas e resolver problemas de acesso remoto em uma estrutura da Cisco Application Centric Infrastructure (ACI). Ele abrange acesso Secure Shell (SSH) e Hypertext Transfer Protocol Secure (HTTPS) a APICs e switches de estrutura, autenticação remota, autorização e relatório (AAA) com Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS) e Lightweight Diretory Access Protocol (LDAP) e autorização Role-Based Access Control (RBAC). Uma árvore de decisão de triagem e cenários detalhados de solução de problemas estão incluídos para cada área.

Informações de Apoio

O material deste documento foi sintetizado a partir do guia Troubleshoot ACI Management and Core Services — Pod Policies, do capítulo Cisco APIC Basic Configuration, Release 6.1(x) — Management e do capítulo Cisco APIC Security Configuration Guide — Access, Authentication, and Accounting.

Overview

O acesso remoto a uma estrutura da ACI envolve três camadas distintas, cada uma das quais deve estar funcionando para que um engenheiro possa fazer login e operar com êxito:

1. Transporte — o caminho da rede de gerenciamento (OOB ou in-band) e o serviço de protocolo (SSH ou HTTPS) devem estar acessíveis e ativados.
2. Autenticação — as credenciais do usuário devem ser validadas, localmente no APIC ou em um servidor AAA remoto (TACACS+, RADIUS ou LDAP).
3. Autorização — o usuário autenticado deve receber as funções e os domínios de segurança corretos do RBAC para visualizar e modificar os objetos da ACI desejados.

Uma falha em qualquer camada produz sintomas diferentes. Uma falha de transporte impede totalmente a conexão. Uma falha de autenticação retorna um erro de credenciais. Uma falha de autorização permite o login, mas restringe a visibilidade ou produz erros "403 Forbidden" na API.

Política de acesso de gerenciamento

A Política de Acesso de Gerenciamento (**commPol**) é o objeto central que controla quais protocolos de acesso remoto estão ativados na malha. Ele está localizado em Fabric > Fabric Policies > Policies > Pod > Management Access > default. A política contém objetos filho que configuram:

- SSH (**commSsh**) — estado administrativo, porta, cifras, algoritmos de troca de chaves (KEX), códigos de autenticação de mensagens (MACs) e algoritmos de chave de host.
- HTTPS (**commHttps**) — estado administrativo, porta, versão do protocolo Transport Layer Security (TLS), taxa de aceleração e autenticação de certificado de cliente.
- Telnet (**commTelnet**) — estado administrativo e porta. O Telnet é desativado por padrão e a Cisco recomenda que permaneça desativado.

Gerenciamento OOB e In-Band

Os nós da ACI suportam dois caminhos de acesso de gerenciamento:

- Out-of-Band (OOB) — usa a porta de gerenciamento dedicada no APIC ou no switch. Os endereços de gerenciamento OOB são alocados de um pool sob o locatário mgmt e atribuídos aos nós via **mgmtRsOoBStNode**. No APIC, os contratos OOB são aplicados por meio de **iptables** regras. Se um contrato OOB for aplicado, somente o tráfego explicitamente permitido pelo contrato poderá acessar a interface de gerenciamento do APIC.
- In-Band (INB) — usa o plano de dados da estrutura para o tráfego de gerenciamento. O gerenciamento em banda exige um domínio de ponte (BD - Bridge Domain), sub-rede, grupo de endpoint (EPG - Endpoint Group), contrato e atribuição de endereço de gerenciamento de nó. Os endereços IP em banda não podem ser acessados de fora da malha sem configuração adicional de roteamento ou política.

Note: Os IPs de gerenciamento OOB do APIC são configurados durante a configuração inicial e o APIC obtém conectividade IP antes que a malha seja totalmente descoberta. O OOB é o caminho de gerenciamento primário e está sempre disponível se a rede de gerenciamento físico estiver conectada.

Arquitetura AAA

A ACI usa um modelo AAA de três níveis:

1. Login Domain (**aaaLoginDomain**) — agrupa provedores AAA sob um domínio nomeado. Os usuários especificam o domínio de login na tela de login (por exemplo, `apic:TACACS-Domain` ou através do menu suspenso na interface do usuário). Sempre existe um domínio de login

especial de fallback e mapeia para autenticação local.
2. Provider Group (**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**, **aaaLdapProviderGroup**) — faz referência a um ou mais servidores AAA e define a ordem na qual eles são tentados.
3. Provedor (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**) — define o IP do servidor, a porta, o segredo compartilhado (ou DN de vinculação para LDAP), o tempo limite, as novas tentativas, o EPG de gerenciamento e as credenciais de monitoramento.

O Default Authentication Realm (**aaaDefaultAuth**) determina qual domínio de login será usado quando o usuário não especificar um no login. O território de autenticação de console controla a autenticação das sessões de console.

Note: Alterar o Default Authentication Realm para um servidor AAA remoto enquanto esse servidor estiver inacessível o bloqueará fora da estrutura. Sempre teste a conectividade do servidor AAA antes de alterar o território. O domínio de login de fallback (`apic:fallback\\admin`) pode ser usado para ignorar o território padrão e autenticar localmente.

Arquivos de log de AAA principais

Os eventos de autenticação AAA são registrados em vários arquivos no APIC e nos switches de malha. Esses logs são a ferramenta principal para validar resultados de autenticação, identificar o realm e o grupo de provedores que estão sendo usados e diagnosticar falhas de atribuição de função.

Arquivo de log	Local (APIC)	Local (switches)	D
nginx.bin.log (APIC) nginx.log (switches)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	Log AAA Contém c autentica Solicitaçã de territór provedor, LDAP/TA análise d atribuiçã função e sucesso nome do entre as o formato mesmo.
access.log	`/var/log/dme/log/access.log`	`/var/log/dme/log/access.log`	Log de s NGINX. U

Arquivo de log	Local (APIC)	Local (switches)	D
			solicitaçã APIC, mo `aaaRefres` códigos d (200 = su negado). mostra so DME inte `aaaRefres`
pam.module.log	`/var/log/dme/log/pam.module.log`	`/var/log/dme/log/pam.module.log`	Log do m Mostra o autentica sessões S autentica e ID de u atribuída. essa é a rápida de usuário fo rejeitado.

Note: O log AAA primário tem um nome de arquivo diferente em cada plataforma. No APIC, ele está **nginx.bin.log** em `/var/log/dme/log/`. Nos switches leaf e spine, ele está **nginx.log** em `/var/sysmgr/tmp_logs/dme_logs/`. O formato de conteúdo de log e as mensagens AAA são os mesmos em ambas as plataformas.

As entradas AAA no registro nginx seguem este formato:

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

Filtrar entradas de log relacionadas a AAA para o fluxo de autenticação de um usuário 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
```

Ou visualize todas as solicitações e resultados de autenticação recentes:

<#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
```

Um fluxo de autenticação bem-sucedido típico mostra estas mensagens-chave na ordem:

1. `Solicitação de autenticação do PAM recebida do Nginx para o Nome de Usuário: <user>` — a solicitação de login foi recebida.
2. `DefaultAuthMo especifica o território <N>. Grupo de Provedores <nome> !` — o território foi selecionado (0=fallback/local, 2=TACACS+, 3=LDAP).
3. Mensagens específicas do provedor (ligação LDAP, pesquisa do provedor TACACS+ ou solicitação RADIUS).
4. `UserDomain <domínio> encontrado sob o nome de usuário remoto: <user>` — a atribuição de domínio da resposta AAA.
5. `Nome de usuário encontrado: admin com privilégios de gravação admin em UserDomain all - o usuário é um usuário admin` — a verificação de função foi aprovada.

Logs de autenticação com falha:

- `O usuário <user> foi negado durante a autenticação AAA`
- `Erro de usuário não autorizado <user>: Autenticação de servidor AAA NEGADA`

Note: O log nginx gira com frequência e as entradas mais antigas são compactadas por gzip com um sufixo numérico. No APIC, os registros girados estão no mesmo diretório (por exemplo, **nginx.bin.log.22815.gz**). Nos switches, os registros girados são armazenados em **/var/log/dme/oldlog/dme/nginx.log.*.gz** (com links simbólicos em `/var/sysmgr/tmp_logs/dme_logs/`). Para pesquisar logs 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

O ACI RBAC controla o que um usuário autenticado pode ver e fazer. O modelo tem três componentes:

- Security Domain (**aaaDomain**) — um limitador de escopo que mapeia para objetos da ACI (usuários, políticas de acesso, políticas de malha). Os domínios internos all, common e mgmt estão sempre presentes. Os domínios personalizados restringem a visibilidade de um usuário a espaços ou áreas de política específicos.
- Função (**aaaRole**) — define um conjunto de privilégios. As funções pré-criadas incluem admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops e nw-svc-admin.
- Privilégio — cada função concede acesso de leitura ou gravação (o que implica leitura) a uma área funcional específica.

Uma conta de usuário recebe um ou mais pares de domínio e função de segurança. Para usuários remotos autenticados via TACACS+, RADIUS ou LDAP, o mapeamento de função é fornecido através de atributos específicos do fornecedor na resposta AAA (por exemplo, o **cisco-av-pair** atributo).

Árvore decisória de triagem

Use esta árvore decisória quando um usuário informar que não pode acessar a estrutura da ACI remotamente:

1. Você pode fazer ping no APIC ou no IP de gerenciamento do switch?
    - Sem → Solucione problemas no caminho da rede de gerenciamento. Consulte a seção "Solução de problemas de OOB e gerenciamento dentro da banda".
    - Sim → Continuar.

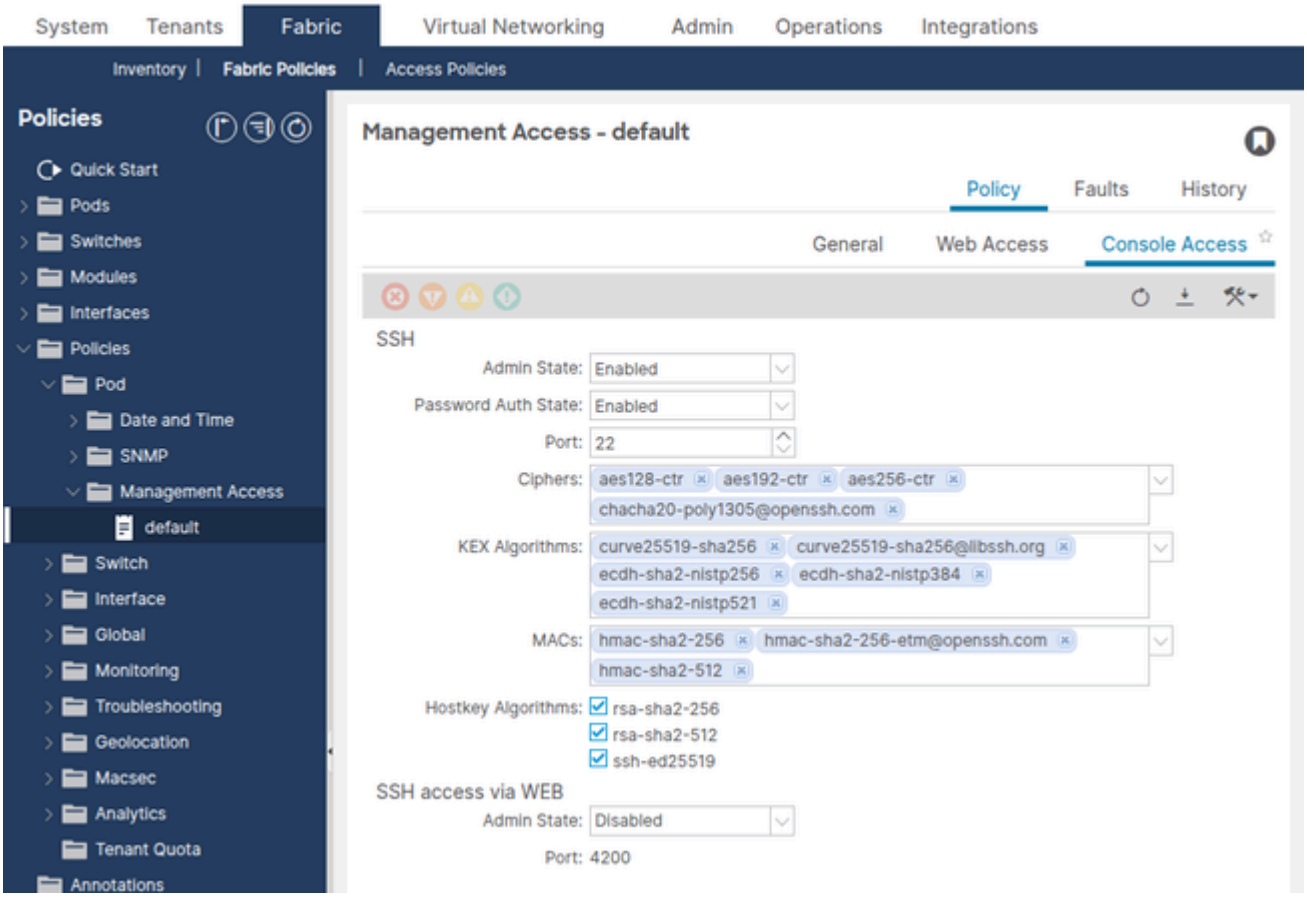
2. Você consegue estabelecer uma conexão SSH ou HTTPS (a conexão é aberta)?
    - Não → O serviço de protocolo pode ser desativado, a porta pode ser filtrada ou uma incompatibilidade de codificação pode estar presente. Consulte as seções "Solucionar problemas de acesso SSH" ou "Solucionar problemas de acesso HTTPS".
    - Sim → Continuar.
3. A tela de login é exibida (HTTPS) ou o handshake SSH é concluído e solicita as credenciais?
    - Nenhuma troca de chave SSH → ou falha de handshake TLS. Consulte a seção "Solução de problemas de acesso SSH" para obter informações sobre incompatibilidades de codificação e KEX.
    - Sim → Continuar.
4. As credenciais falham com "Authentication Failed" ou similar?
    - Sim → problema de autenticação. Consulte as seções "Troubleshoot AAA Authentication" (TACACS+, RADIUS ou LDAP, dependendo do domínio de login em uso).
    - Não → Continuar.
5. O usuário faz login, mas não consegue ver os objetos esperados, ou recebe erros "403 Forbidden"?
    - Sim → problema de autorização ou RBAC. Consulte a seção "Solucionar problemas de RBAC e privilégios de usuário".
    - Nenhum acesso → está funcionando. Verifique o problema específico que o usuário está tendo.

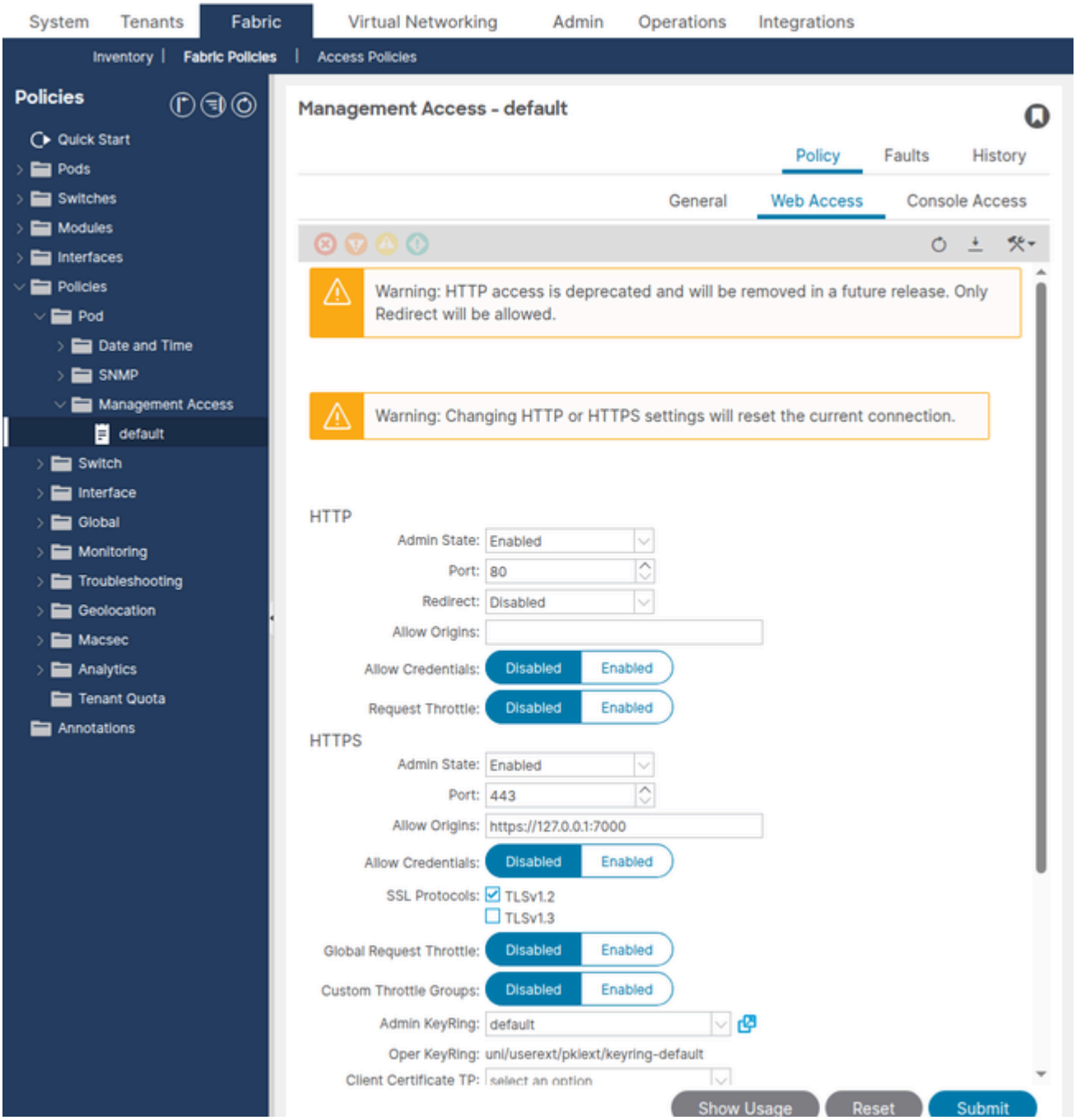
Verifique a configuração

Antes de solucionar problemas do estado operacional, verifique se a cadeia de configuração está completa. A configuração incorreta é a causa raiz mais comum de problemas de acesso remoto.

Verificar a Política de Acesso de Gerenciamento (SSH e HTTPS)

Navegue até 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 as seguintes configurações de SSH:

- Estado do administrador — deve ser habilitado.
- Porta — padrão 22. Se alterado, o cliente SSH deve usar a porta personalizada.
- Autenticação de Senha — habilitada (a menos que a autenticação somente de certificado seja intencional).
- Cifras SSH — devem incluir pelo menos uma cifra suportada pelo cliente SSH.
- Algoritmos KEX — devem incluir pelo menos um algoritmo suportado pelo cliente SSH.
- MACs SSH — devem incluir pelo menos um MAC suportado pelo cliente SSH.

Consulte o objeto gerenciado SSH através da 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 as seguintes configurações HTTPS:

- Estado do administrador — deve ser habilitado.
- Porta — padrão 443.
- Protocolos SSL — TLSv1.2 (padrão). Os clientes mais antigos podem exigir que o TLSv1.1 seja adicionado explicitamente.
- Estado de Aceleração — se ativado, a Taxa de Aceleração limita as solicitações por segundo por usuário. Um valor muito baixo pode causar erros de tempo limite 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
```

Erros comuns de configuração

- As cifras SSH eram muito agressivas — na versão 5.2(1) e posteriores da ACI, as cifras SSH padrão eram endurecidas. Clientes SSH mais antigos (por exemplo, versões PuTTY anteriores a 0.75 ou versões OpenSSH que oferecem apenas **diffie-hellman-group14-sha1**) podem falhar na troca de chaves. O cliente SSH exibe "nenhuma codificação correspondente encontrada" ou "nenhum método de troca de chave correspondente encontrado".
- Autenticação de senha desabilitada — se **passwordAuth** estiver definido como desabilitado, somente a autenticação baseada em chave SSH será permitida. Os usuários que se conectarem com senhas verão "Permissão negada (chave pública)".

- Porta SSH personalizada sem reconhecimento do cliente — se a porta SSH foi alterada de 22, o cliente SSH deve especificar a nova porta (por exemplo, **ssh -p 2222 admin@10.1.1.1**).

Verificar Endereços de Gerenciamento OOB

Navegue até Locatários > gerenciamento > Endereços de gerenciamento de nó.

Confirme se cada APIC e nó do switch tem um endereço IP de gerenciamento OOB atribuído com um gateway válido. Nós sem endereços de gerenciamento não poderão ser acessados pela rede de gerenciamento.

Consulte as atribuições de nó estático OOB por meio da 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
```

Erros comuns de configuração

- Atribuição de endereço OOB ausente — um switch não tem uma entrada em **mgmtRsOoBStNode**. O nó não terá um IP de gerenciamento e não responderá a SSH ou HTTPS na interface OOB.
- Gateway incorreto — o endereço do gateway não corresponde ao gateway real na rede de gerenciamento OOB. O nó pode receber pacotes, mas não pode enviar tráfego de retorno.
- Incompatibilidade de máscara de sub-rede — a máscara de sub-rede OOB não corresponde à rede de gerenciamento física. Isso pode fazer com que o nó acredite que a estação de gerenciamento está em uma sub-rede diferente e roteie o tráfego através de um gateway que não existe ou está incorreto.

Verificar contratos OOB

Navegue até Locatários > Gerenciamento > Contratos.

Se um contrato OOB for aplicado ao EPG de gerenciamento OOB, somente o tráfego explicitamente permitido por esse contrato alcançará a interface de gerenciamento do APIC. No APIC, os contratos OOB são executados por meio de **iptables** regras.

Consulte os contratos fornecidos pelo OOB EPG:

<#root>

apic1#

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

Se a consulta retornar resultados, os contratos serão aplicados. Verifique se os assuntos e filtros do contrato permitem os protocolos necessários:

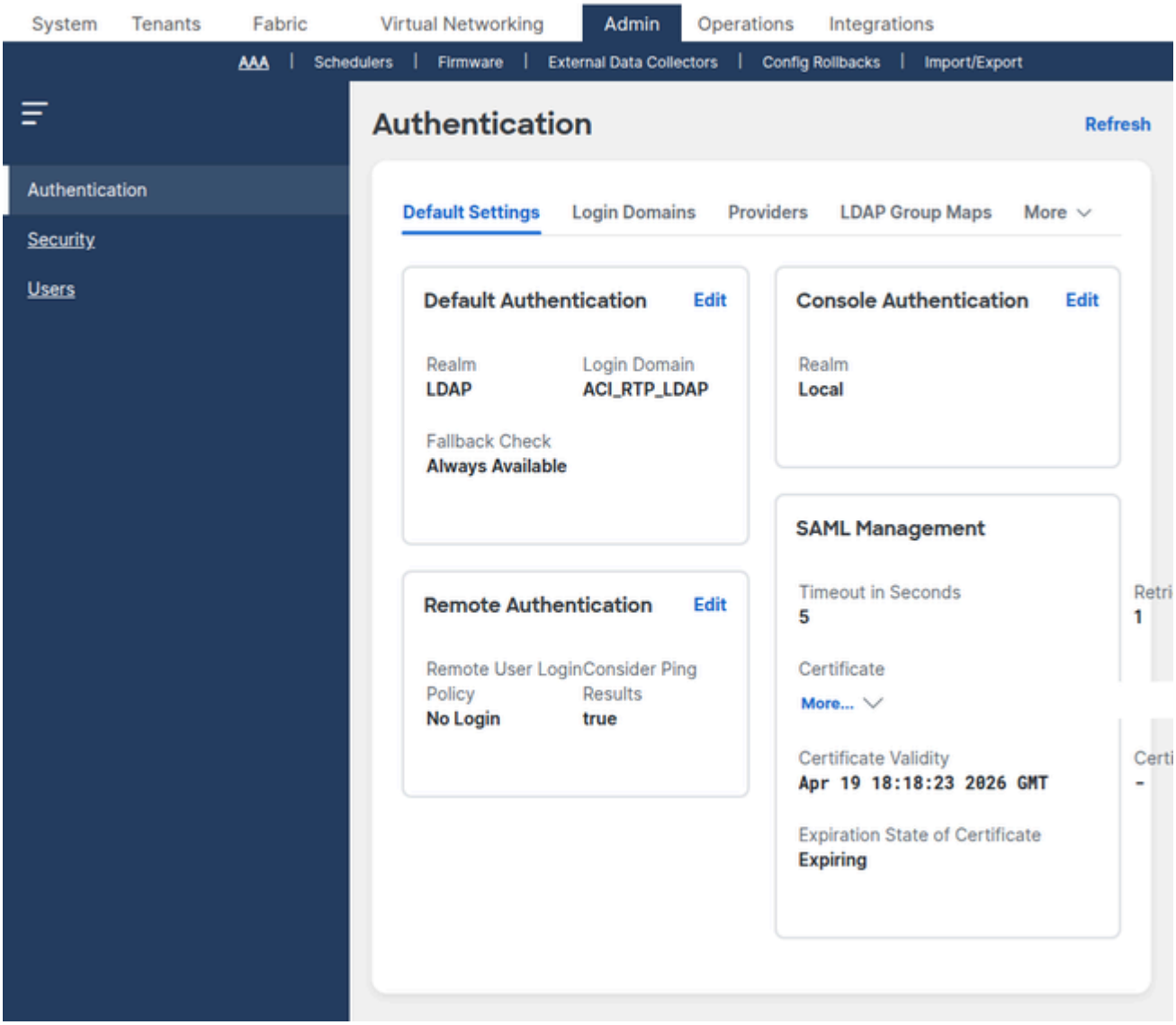
- SSH — porta TCP 22 (ou porta personalizada)
- HTTPS — porta TCP 443 (ou porta personalizada)
- ICMP — para verificação de ping

Erros comuns de configuração

- O contrato OOB não inclui SSH ou HTTPS — o engenheiro pode fazer ping no APIC, mas não pode se conectar via SSH ou HTTPS. As **iptables** regras no APIC silenciosamente descartam o tráfego.
- Restrição de IP de origem no filtro de contrato OOB — o filtro de contrato limita o acesso a sub-redes de origem específicas. Engenheiros fora dessa sub-rede não podem se conectar.

Verifique a configuração de AAA

Navegue até Admin > AAA > Authentication > AAA.



Confirme o seguinte:

- Default Authentication Realm — identifica qual domínio de login será usado quando o usuário não especificar um. Se definido para um domínio de login AAA remoto, o servidor correspondente deve estar acessível.
- Console Authentication Realm — controla o acesso ao console. Se definido como local, o login do console sempre usará credenciais locais (recomendado).

Verificar domínios de login

Navegue até 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 se o domínio de logon usado para autenticação está presente e se ele faz referência ao grupo de provedores correto.

Verificar provedores TACACS+

Navegue até 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 provedores RADIUS

Navegue até 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 provedores LDAP

Navegue até 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
```

Erros comuns de configuração de AAA

- Incompatibilidade de segredo compartilhado — a chave configurada no provedor ACI TACACS+ ou RADIUS não corresponde à chave no servidor. A autenticação falha silenciosamente.
- EPG de gerenciamento incorreto — o **epgDn** do provedor está vazio ou aponta para o EPG incorreto (por exemplo, in-band quando o servidor está na rede OOB). O APIC não pode acessar o servidor.
- Incompatibilidade de realm do domínio de login — o domínio de login é configurado como LDAP, mas o usuário espera a autenticação TACACS+. Os domínios de logon devem fazer referência ao tipo correto de grupo de provedores.
- DN de vinculação LDAP incorreto — o **rootdn** (DN de vinculação) ou **basedn** estão errados. A autenticação LDAP falha com um erro de ligação mesmo quando as credenciais do usuário estão corretas.
- O filtro LDAP não corresponde ao esquema do diretório — para o Ative Diretory, use **sAMAccountName=$userid**. Para OpenLDAP, use **cn=$userid** ou **uid=$userid**.

Verificar a Configuração do RBAC

Navegue para Admin > AAA > Users para visualizar as contas de usuário locais e seus domínios de segurança e atribuições de função.

Consultar domínios de segurança por meio da 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
```

Um usuário atribuído ao domínio all com a função admin tem acesso de leitura-gravação completo à malha inteira. Um usuário atribuído a um domínio de segurança personalizado com a função tenant-admin só pode gerenciar espaços associados a esse domínio.

Configurações incorretas comuns de RBAC

- Usuário criado sem um domínio de segurança — o usuário pode fazer login, mas não vê espaços e recebe "403 Proibido" em chamadas de API. Pelo menos um domínio de segurança deve ser atribuído.
- Função somente leitura atribuída quando o acesso de gravação é necessário — o usuário pode exibir objetos, mas não pode enviar alterações. Verifique se o privilégio da função está definido como writePriv.
- Mapeamento de função de usuário remoto ausente no servidor AAA — o servidor TACACS+ ou RADIUS não retorna o atributo que **cisco-av-pair** contém **shell:domains=all/admin/**. O usuário se autentica com êxito, mas não tem funções e não consegue ver nada na malha.

Solucionar problemas de OOB e gerenciamento dentro da banda

Se o APIC ou o IP de gerenciamento do switch não estiver acessível na rede, identifique e solucione os problemas do caminho de gerenciamento antes de investigar SSH, HTTPS ou AAA.

Cenário: Não é possível fazer ping no IP OOB do APIC

Problema: A estação de gerenciamento não pode fazer ping no endereço IP de gerenciamento OOB do APIC.

Etapas de verificação:

1. Verifique se a porta de gerenciamento do APIC está fisicamente conectada e se o link está ativo.
2. Verifique se a estação de gerenciamento está no mesmo segmento L2 ou tem uma rota para a sub-rede OOB.
3. Verifique se o IP de gerenciamento OOB está atribuído corretamente:
   <#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 se o gateway padrão está acessível:
   <#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. Se um contrato OOB for aplicado, verifique se ele permite os protocolos necessários. Consulte os contratos fornecidos pelo OOB EPG conforme mostrado na seção "Verificar contratos OOB". Os contratos OOB são aplicados como **iptables** regras no APIC. Você pode visualizar as regras salvas no shell do APIC:
   <#root>

   ```
   apic1#

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

   Se a política INPUT for DROP e não houver nenhuma regra ACCEPT para o protocolo necessário, o contrato OOB está filtrando o tráfego.

   > Note: O **iptables -L -n** comando para visualizar as regras do kernel ao vivo requer acesso à raiz e não está disponível para sessões SSH de administração regulares.

Causa raiz: Endereço de gerenciamento OOB ausente ou configurado incorretamente, gateway incorreto ou tráfego de filtragem de contrato OOB.

Solução: Corrija a atribuição de endereço OOB, verifique o caminho da rede física ou atualize o contrato OOB para permitir os protocolos necessários.

Cenário: Não É Possível Acessar um IP de Gerenciamento do Switch

Problema: A estação de gerenciamento pode acessar o APIC, mas não pode acessar um switch via OOB.

Etapas de verificação:

1. Verifique se o switch tem um endereço OOB atribuído:
   <#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 se a interface de gerenciamento do switch tem o IP atribuído:
   <#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 a rota padrão de VRF de gerenciamento:
   <#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 raiz: Atribuição de endereço OOB ausente, gateway incorreto ou a porta física de gerenciamento do switch está inativa.

Solução: Atribua o endereço OOB em Tenants > mgmt > Node Management Addresses. Verifique se o link de gerenciamento físico está ativo.

Solucionar problemas de acesso SSH

Esta seção aborda cenários onde o IP de gerenciamento é alcançável (ping bem-sucedido), mas a sessão SSH não estabelece ou autentica.

Cenário: Conexão SSH recusada

Problema: O cliente SSH relata "Conexão recusada" ao se conectar ao APIC ou switch.

Etapas de verificação:

1. Verifique se o SSH está habilitado na Política de acesso de gerenciamento:
   <#root>

   ```
   apic1#

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

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

   Se o **adminSt** estiver desabilitado, as conexões SSH serão rejeitadas.

2. Verifique se a porta correta está sendo usada. Se a porta SSH foi alterada de 22:
   <#root>

   ```
   $

   ssh -p

    custom-port

   admin@10.1.1.1
   ```

3. Verifique se o contrato OOB permite o TCP na porta SSH. Consulte a seção "Verificar contratos OOB".

Causa raiz: SSH desabilitado na política de acesso de gerenciamento, porta personalizada desconhecida para o cliente ou filtragem de contrato OOB.

Solução: Habilite o SSH na política de acesso de gerenciamento ou use a porta correta.

Cenário: Falha na troca de chave SSH (incompatibilidade de codificação ou KEX)

Problema: O cliente SSH falha com "nenhuma codificação correspondente encontrada", "nenhum método de troca de chave correspondente encontrado" ou "nenhum MAC correspondente encontrado".

Etapas de verificação:

1. Verifique a saída detalhada do cliente SSH para identificar quais algoritmos o cliente oferece:
   <#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 os algoritmos oferecidos pelo cliente com os algoritmos configurados no 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. Identificar a interseção. Se não houver algoritmo comum em nenhuma categoria, o handshake falha.

Note: Na versão 5.2(1) e posteriores da ACI, as cifras SSH e os algoritmos KEX padrão foram reforçados. Algoritmos antigos como **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**, **aes128-cbc**, e **hmac-sha1** não são mais oferecidos por padrão. Se você fez upgrade recentemente, verifique se os clientes SSH em seu ambiente suportam os novos padrões.

Causa raiz: Sem cifra comum, algoritmo KEX ou MAC entre o cliente SSH e o APIC após uma atualização de ACI ou endurecimento de cifra.

Solução: Atualize o cliente SSH para suportar algoritmos modernos ou adicione novamente o algoritmo herdado necessário à Política de Acesso de Gerenciamento. A readição de algoritmos herdados apresenta riscos à segurança e não é recomendada a longo prazo.

Cenário: O SSH se conecta, mas a autenticação falha para usuários locais

Problema: O handshake SSH é bem-sucedido (o prompt de senha é exibido), mas a senha é rejeitada para um usuário local.

Etapas de verificação:

1. Verifique se o usuário existe 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. Verifique se a conta está bloqueada devido ao excesso de tentativas de login com falha:
   <#root>

   ```
   apic1#

   moquery -c aaaUserEp

   dn                 : uni/userext
   pwdStrengthCheck   : no
   ```

   Verifique a política de bloqueio de domínio de login em Admin > AAA > Gerenciamento de segurança > Política de bloqueio.

3. Verifique se o usuário está fazendo login com o domínio de login correto. Se o Default Authentication Realm for definido como um domínio de login AAA remoto, o usuário deverá preceder **apic:LOCAL\\username** ou **apic:fallback\\username** forçar a autenticação local.
4. Valide o resultado da autenticação nos logs. Verifique **nginx.bin.log** o evento de login no APIC:
   <#root>

   ```
   apic1#

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

   Procure o realm e o grupo de provedores designados para a tentativa de login:

```
! 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
```

Se o território não for 0 (fallback/local), o login foi enviado para um servidor AAA remoto em vez do banco de dados local. O usuário deve preceder **apic:fallback\\username** ou **apic:LOCAL\\username** para forçar a autenticação local.

Causa raiz: Senha incorreta, conta bloqueada ou tentativa de logon sendo enviada para um servidor AAA remoto em vez do banco de dados local.

Solução: Redefina a senha, desbloqueie a conta ou use o prefixo de domínio de login correto.

Solucionar problemas de acesso HTTPS

Esta seção aborda cenários em que a interface de usuário da Web do APIC ou a interface de programação de aplicativo (API) de transferência de estado representacional (REST) não pode ser alcançada em HTTPS.

Cenário: Tempo Limite da Conexão HTTPS

Problema: O navegador mostra "ERR_CONNECTION_TIMED_OUT" ou a chamada de API trava quando se conecta ao APIC na porta 443.

Etapas de verificação:

1. Verifique se HTTPS está 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 se o contrato OOB permite TCP 443. Consulte a seção "Verificar contratos OOB".
3. Teste do próprio APIC para confirmar se o processo HTTPS está escutando:
   <#root>

```
apic1#

ss -tlnp | grep 443

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

Causa raiz: HTTPS desabilitado, filtragem de contrato OOB TCP 443 ou travamento do processo nginx no APIC.

Solução: Ative o HTTPS na política de acesso de gerenciamento, atualize o contrato OOB ou reinicie o serviço da Web no APIC.

Cenário: O navegador mostra o erro de handshake TLS

Problema: O navegador exibe "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" ou um erro TLS semelhante.

Etapas de verificação:

1. Verifique a versão do protocolo TLS configurada no APIC:
   <#root>

```
apic1#

moquery -c commHttps

sslProtocols : TLSv1.2
```

2. Verifique se o navegador oferece suporte a TLSv1.2. Navegadores muito antigos (por exemplo, Internet Explorer 10 e mais antigos) não oferecem suporte a TLSv1.2 por padrão.

Causa raiz: O APIC oferece apenas TLSv1.2 (o padrão) e o navegador ou cliente API oferece suporte apenas a versões TLS mais antigas.

Solução: Atualize o navegador ou o cliente. Se você precisar oferecer suporte a clientes mais antigos temporariamente, adicione TLSv1.1 à Política de acesso de gerenciamento, mas isso apresenta riscos à segurança.

Cenário: Limitação de API

Problema: As chamadas da API REST falham intermitentemente com erros HTTP 503 ou a interface do usuário da Web fica lenta durante a automação pesada.

Etapas de verificação:

<#root>

```
apic1#

moquery -c commHttps

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

Se a taxa de aceleração for muito baixa e os scripts de automação enviarem muitas solicitações por segundo, o APIC rejeitará solicitações em excesso.

Causa raiz: A taxa de aceleração por usuário é muito baixa para a carga de trabalho de automação.

Solução: Aumente a taxa de aceleração na Política de acesso de gerenciamento ou otimize os scripts de automação para reduzir a frequência das solicitações. Como alternativa, desabilite a limitação se a estrutura não for compartilhada.

Identificar e Solucionar Problemas de AAA — TACACS+

Esta seção aborda as falhas de autenticação do TACACS+. O APIC se comunica com o servidor TACACS+ pela porta TCP 49.

Verificação operacional

Os switches da ACI não suportam o **test aaa** comando disponível no NX-OS autônomo. Para verificar a operação TACACS+, use o APIC para verificar o status do provedor, falhas e histórico

de sessão de login.

Verifique se há falhas ativas no provedor TACACS+:

<#root>

apic1#

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

Se nenhuma falha for retornada, o APIC considerará o provedor alcançável. Se houver falhas, a saída incluirá códigos de falhas como F1773 (provedor inalcançável) ou F1774 (falha de autenticação).

Verifique a configuração do provedor 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 a acessibilidade básica da rede do APIC para o 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
```

Tente fazer login no APIC com o domínio de login TACACS+ e verifique o resultado da sessão:

<#root>

```
apic1#

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

Examine o campo para determinar se a falha se deve à rejeição da autenticação ou a um problema de conectividade **descr**.

Valide o fluxo de autenticação TACACS+ nos logs do APIC. Filtro para o nome de usuário em questão:

```
<#root>

apic1#

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

nginx.bin.log Os logons TACACS+ seguem o mesmo fluxo de autenticação que o LDAP (consulte a seção Verificação operacional LDAP para obter exemplos reais completos de log). As principais diferenças para TACACS+ são:

- `DefaultAuthMo especifica o território 2` — o território 2 indica TACACS+ (versus território 3 para LDAP).
- `Adicionar TacacsProvider <IP> à lista` — identifica o servidor TACACS+ que está sendo contatado (em comparação com `LdapProvider` para LDAP).
- `TACACS+ Cisco-avpair (shell:domains=all/admin/)` — o par AV é retornado diretamente pelo servidor TACACS+ (em vez de ser convertido de um mapa de grupo LDAP).

Um login bem-sucedido do TACACS+ mostra a mesma progressão: O PAM solicita → seleção de realm → pesquisa de provedor → par de AV analisando → injeção de usuário → UserDomain e atribuição de função → `privilégios de gravação de administrador`.

Um login TACACS+ com falha termina com `User <username> foi negado durante autenticação AAA` e `Unauthorized ... erro: Autenticação de servidor AAA NEGADA`, o mesmo padrão de uma negação LDAP.

Cenário: Falha na autenticação TACACS+

Problema: O login falha com "Authentication Failed" quando o usuário seleciona um domínio de login TACACS+.

Etapas de verificação:

1. Verifique se há falhas ativas no provedor TACACS+:
   <#root>

   ```
   apic1#

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

   A falha F1773 indica um problema de conectividade. A falha F1774 indica uma rejeição de autenticação.

2. Verifique a acessibilidade da rede do APIC para o 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. Se o ping for bem-sucedido, mas a autenticação falhar, verifique se o segredo compartilhado corresponde na configuração do provedor APIC e na configuração do servidor TACACS+.
4. Verifique as sessões de login mais recentes para ver os detalhes da falha:
   <#root>

   ```
   apic1#

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

5. Verifique os registros do servidor TACACS+ para a tentativa de autenticação. Uma tentativa bem-sucedida registrada no servidor, mas rejeitada, indica um problema de configuração do usuário no lado do servidor (por exemplo, incompatibilidade de senha ou conta de usuário ausente).
6. Verifique o APIC **nginx.bin.log** para obter o fluxo de autenticação completo. Filtrar por nome de usuário em vez de palavras-chave específicas para que as mensagens intermediárias não sejam perdidas:
   <#root>

   ```
   apic1#

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

   Compare a saída com os exemplos de funcionamento e não funcionamento na seção Verificação operacional acima. Principais indicadores:

   - `foi negado` ou `NEGADO` — o servidor TACACS+ foi alcançado, mas rejeitou as

credenciais. Verifique se o usuário existe no servidor e se a senha corresponde.
- Nenhuma mensagem específica do provedor depois de `Adicionar TacacsProvider` — o servidor está inacessível ou o tempo expirou. Verifique o alcance da rede e o EPG de gerenciamento.
- `A injeção de usuário remoto ... foi concluída` seguida por linhas de verificação de função — a autenticação foi bem-sucedida, mas o problema pode estar na atribuição de função (consulte a seção par AV abaixo).

TACACS+ cisco-av-pair para RBAC

Para usuários remotos autenticados via TACACS+, o servidor deve retornar o **cisco-av-pair** atributo na resposta de autorização. Esse atributo mapeia o usuário para os domínios e funções de segurança da ACI.

Formato:

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

Examples:

- Administrador completo: **shell:domains=all/admin/**
- Somente leitura para todos: **shell:domains=all/read-all/**
- Administração de locatários para um domínio específico: **shell:domains=TenantA/tenant-admin/**
- Vários domínios: **shell:domains=all/admin/,TenantA/tenant-admin/**

Se esse atributo estiver ausente ou malformado, o usuário será autenticado com êxito, mas não terá funções e não poderá ver nenhum objeto na interface do usuário do APIC.

Note: O acesso SSH aos switches leaf e spine requer a função admin com o privilégio write no domínio de segurança all. O par AV mínimo para o acesso SSH do switch é **shell:domains=all/admin/**. Os usuários com funções não administrativas (por exemplo, `read-all`, `tenant-admin`, `aaa`) ou usuários atribuídos a um domínio de segurança diferente de `all` podem fazer login no APIC, mas o acesso SSH aos switches é negado. O log do APIC mostra `logons não administrativos no switch que foram negados` para esses usuários.

Valide o par AV recebido verificando **nginx.bin.log**. Filtre pelo nome de usuário para ver o fluxo de injeção de função completo:

<#root>

```
apic1#

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

Para TACACS+, o par AV é registrado como `TACACS+ Cisco-avpair (shell:domains=...)`. Uma injeção bem-sucedida mostra `Injeção de usuário remoto <username> concluída` seguida por `Found UserDomain` e `admin write privilege` linhas (consulte a seção Verificação operacional LDAP para obter exemplos completos desse fluxo com saída de log real).

Se o formato do par AV for inválido, o log mostrará `Injeção de dados do usuário remoto <username> FALHA - a mensagem de erro é Sequência de caracteres shell:domains inválida`. Se o usuário autenticar com uma função não-admin, SSH para switches é negado com `logons não-admin no switch são negados`.

Causa raiz: Incompatibilidade de segredo compartilhado, servidor inacessível da rede de gerenciamento, usuário não existe no servidor TACACS+ ou o EPG de gerenciamento no provedor está incorreto.

Solução: Corrija o segredo compartilhado, corrija a acessibilidade ou crie o usuário no servidor TACACS+.

Validar Logs de Autenticação do Switch Leaf

Nos switches leaf e spine, os eventos de login do SSH são registrados no **pam.module.log** e no **nginx.log**. O **pam.module.log** mostra o resultado da autenticação do PAM (aceitar ou rejeitar). O **nginx.log** contém o fluxo AAA completo — seleção de território, pesquisa de provedor, comunicação LDAP/TACACS+/RADIUS, análise de par AV e atribuição de função — idêntico **nginx.bin.log** ao APIC. Esses registros se aplicam a todos os tipos de AAA remotos (TACACS+, RADIUS, LDAP).

Verifique **pam.module.log** o resultado da autenticação:

```
<#root>

leaf101#

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

Em funcionamento — autenticação remota bem-sucedida no 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
```

remote=1 O sinalizador confirma que o usuário foi autenticado por um servidor AAA remoto.

Não funciona — o usuário foi rejeitado. O securitymgrAG nega ao usuário e o switch tenta uma pesquisa de usuário local como um fallback 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
```

Se nenhuma entrada do PAM aparecer para o usuário, a conexão SSH provavelmente foi rejeitada antes de atingir o estágio PAM (por exemplo, devido a uma incompatibilidade de cifras ou ao cancelamento da conexão pelo usuário).

Para obter uma visão mais detalhada do fluxo de autenticação no switch, verifique **nginx.log**. Esse registro contém toda a cadeia de decisão AAA — o mesmo formato e mensagens que **nginx.bin.log** no APIC:

<#root>

```
leaf101#
```

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

Em funcionamento — autenticação LDAP bem-sucedida em um switch (compare com os exemplos LDAP do APIC na seção Verificação operacional do LDAP — as mensagens são as mesmas):

```
||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
```

O switch **nginx.log** é particularmente útil quando **pam.module.log** mostra uma rejeição, mas não explica por quê. O nginx.log revela o domínio AAA, o provedor e o motivo específico da falha (por exemplo, a pesquisa LDAP retornou vazio, o tempo limite TACACS+ ou a injeção do par AV falhou).

Identificar e Solucionar Problemas de AAA - RADIUS

Esta seção aborda falhas de autenticação RADIUS. O APIC se comunica com o servidor RADIUS pela porta UDP 1812 (autenticação) e, opcionalmente, pela porta UDP 1813 (contabilidade).

Verificação operacional

Os switches da ACI não suportam o **test aaa** comando disponível no NX-OS autônomo. Use os seguintes métodos para verificar a operação do RADIUS.

Verifique a configuração do servidor RADIUS e as estatísticas de acessibilidade de um switch leaf:

<#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
```

Cenário: Falha na autenticação RADIUS

Problema: O logon falha quando um usuário seleciona um domínio de logon RADIUS.

Etapas de verificação:

1. Verifique as estatísticas de servidor RADIUS de um switch para sinais de timeouts ou falhas:
   <#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
   ```

   Uma contagem alta nas solicitações com tempo limite esgotado indica que o servidor RADIUS está inacessível ou o segredo compartilhado é incompatível (o RADIUS descarta silenciosamente os pacotes na incompatibilidade de segredo compartilhado).

2. Verifique a acessibilidade da rede ao 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 se o segredo compartilhado corresponde entre o APIC e o servidor RADIUS. Diferentemente do TACACS+, que usa TCP e relata falhas de conexão, o RADIUS usa UDP e silenciosamente descarta pacotes quando o segredo compartilhado não corresponde. O único sintoma é um tempo limite.
4. Verifique os registros do servidor RADIUS. FreeRADIUS no modo de depuração (**radiusd -X**) mostra cada solicitação e indica se ela foi aceita, rejeitada ou se teve uma incompatibilidade de segredo compartilhado.
5. Verifique o APIC **nginx.bin.log** quanto ao fluxo de autenticação do RADIUS. Filtrar pelo nome de usuário:
   <#root>

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

nginx.bin.log Os logons RADIUS seguem o mesmo fluxo de autenticação que o LDAP e o TACACS+ (consulte a seção Verificação operacional LDAP para obter exemplos reais completos de log). As principais diferenças do RADIUS são:

- `Adicionando RadiusProvider <IP> à lista` — identifica o servidor RADIUS (vs. `TacacsProvider` ou `LdapProvider`).
- O número de território do RADIUS varia de acordo com a configuração.

Um login RADIUS bem-sucedido termina com `Injeção de usuário remoto... concluída` e `privilégios de gravação de administrador`.

Um login RADIUS com falha termina com `foi negado durante a autenticação AAA` e `NEGADO`.

Se nenhuma mensagem específica de RADIUS for exibida após a linha `Adding RadiusProvider`, o servidor atingiu o tempo limite. Diferentemente do TACACS+, que usa TCP e relata falhas de conexão, o RADIUS usa UDP e silenciosamente descarta pacotes quando o segredo compartilhado não corresponde. O único sintoma é um tempo limite seguido de negação.

6. Verifique se há falhas ativas no provedor RADIUS:
<#root>

```
apic1#
moquery -c faultInst -x 'query-target-filter=wcard(faultInst.dn,"radiusprovider")'
```

RADIUS cisco-av-pair para RBAC

O RADIUS usa o mesmo **cisco-av-pair** atributo que o TACACS+ para mapeamento de função RBAC. O servidor RADIUS deve retornar este atributo na resposta Access-Accept:

<#root>

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

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

No FreeRADIUS, isso é configurado no arquivo ou back-end LDAP **users**. Para o ISE, ele é

configurado no perfil de autorização como um atributo avançado.

Causa raiz: Incompatibilidade de segredo compartilhado (mais comum com RADIUS — causa timeouts silenciosos), servidor inalcançável, porta de autenticação incorreta ou conta de usuário ausente no servidor RADIUS.

Solução: Corrija o segredo compartilhado, verifique a acessibilidade do UDP 1812 ou configure o usuário no servidor RADIUS.

Identificar e Solucionar Problemas de AAA — LDAP

Esta seção aborda falhas de autenticação LDAP. O APIC se conecta ao servidor LDAP pela porta TCP 389 (LDAP) ou pela porta TCP 636 (LDAPS com SSL).

Verificação operacional

Os switches da ACI não suportam o **test aaa** comando disponível no NX-OS autônomo. Para verificar a operação LDAP, verifique as falhas do provedor e a configuração do APIC.

Verifique se há falhas ativas no provedor LDAP:

<#root>

apic1#

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

A falha F1777 indica um problema de conectividade. Falha F1778 indica uma falha de autenticação ou de ligação. Se nenhuma falha for retornada, o APIC considerará o provedor alcançável.

Verifique a acessibilidade básica da rede para o 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 também a conectividade TCP com a porta 389 (ou 636 para LDAPS). Se o APIC puder fazer ping no servidor, mas as falhas de LDAP persistirem, o problema é normalmente um DN de vinculação incorreto, uma senha incorreta ou um firewall que esteja bloqueando a porta LDAP.

Valide o fluxo de autenticação LDAP nos logs do APIC. Filtrar pelo nome de usuário:

<#root>

```
apic1#

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

Trabalhando — Um login LDAP bem-sucedido mostra o fluxo completo de pesquisa, associação e atribuição de função:

```
||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
```

Não funciona — usuário não encontrado no diretório LDAP (pesquisa retorna conjunto vazio):

```
||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
```

Cenário: Falha na autenticação LDAP

Problema: O login falha quando um usuário seleciona um domínio de login LDAP.

Etapas de verificação:

1. Verifique a acessibilidade do servidor LDAP a partir do 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. Verificar falhas do provedor LDAP ativo:
   <#root>

   ```
   apic1#
   ```

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

3. Verifique a configuração do provedor 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 se o usuário existe no diretório LDAP sob o DN base configurado e corresponde ao filtro. Para o Ative Diretory, o atributo do usuário deve corresponder ao nome de usuário **sAMAccountName** inserido no logon. Para OpenLDAP, o atributo **cn** ou **uid** deve corresponder.
5. Se estiver usando LDAPS (porta 636), verifique a cadeia de certificados SSL. Se **SSLValidationLevel** for definido como strict, o APIC rejeitará a conexão se o certificado do servidor não for confiável ou tiver expirado.
6. Verifique o APIC **nginx.bin.log** para obter o fluxo de autenticação LDAP completo. Filtrar pelo nome de usuário para que as mensagens intermediárias não sejam perdidas:
   <#root>

   ```
   apic1#
   ```

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

Compare a saída com os exemplos de funcionamento e não funcionamento na seção Verificação operacional acima. Padrões de falha adicionais específicos do LDAP podem ser encontrados pesquisando amplamente o log:

<#root>

apic1#

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

Padrões comuns de não funcionamento (compare com os exemplos de Verificação Operacional acima para o fluxo 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
```

Outros padrões de falha LDAP a serem procurados:

- Tempo limite da pesquisa LDAP (servidor inacessível, lento ou firewall bloqueando a porta 389/636) — falha ao procurar `Pesquisa Ldap: código de retorno para ldap_search_ext_s: -5 : Tempo limite atingido`
- Falha na associação (rootdn ou senha de associação incorreta, ou o servidor recusou a conexão) — falha ao procurar `Pesquisa Ldap: código de retorno para ldap_search_ext_s: -1 : Não é possível contatar o servidor LDAP`
- Usuário encontrado, mas a senha está incorreta (falha ao vincular com a senha do usuário) — o log mostra a linha `LDAP Record DN`, mas é seguido por uma mensagem negada sem linha `Bind to UserDN ... successful`.

Mapa de grupo LDAP para RBAC

O LDAP usa mapas de grupo em vez do **cisco-av-pair** atributo. O campo do provedor LDAP **attribute** especifica qual atributo LDAP contém as informações do grupo. Para o Ative Diretory, isso é normalmente **memberOf**.

O APIC faz a correspondência do DN do grupo retornado com as Regras de mapa de grupo LDAP (**aaaLdapGroupMapRule**) configuradas para atribuir o domínio e a função de segurança apropriados. Se nenhuma regra de mapa de grupo corresponder, o usuário autenticará, mas não

terá funções.

Como alternativa, você pode definir o **attribute** para **CiscoAVPair** e armazenar o **shell:domains=all/admin/** valor diretamente nos atributos LDAP do usuário, que seguem o mesmo formato que TACACS+ e RADIUS.

Causa raiz: DN ou senha de associação incorreta, DN base não contém o usuário, filtro de pesquisa não corresponde ao esquema de diretório, falha de validação de certificado LDAPS ou regras de mapa de grupo ausentes.

Solução: Corrija a configuração do provedor (vincular DN, DN base, filtro, configurações de SSL). Para problemas de RBAC, verifique se as regras de mapa de grupo correspondem aos grupos LDAP aos quais o usuário pertence.

Identificar e Solucionar Problemas de RBAC e Privilégios de Usuário

Esta seção aborda os cenários em que o usuário autentica com êxito, mas não tem o nível de acesso esperado.

Cenário: O Usuário Fez Logon, Mas Não Vê Locatários

Problema: Um usuário remoto faz login via TACACS+, RADIUS ou LDAP. O login é bem-sucedido, mas o usuário não vê nenhum espaço na interface do usuário e as chamadas de API retornam resultados vazios ou "403 Proibido".

Etapas de verificação:

1. Verifique a sessão do usuário para ver quais funções foram atribuídas no login:
   <#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
   ```

   O campo **descr** mostra o resultado do logon. Se o usuário foi autenticado com êxito, mas não tem funções RBAC, o servidor AAA não retornou uma correspondência de mapa de grupo válida **cisco-av-pair** ou LDAP.

2. Verifique o APIC **nginx.bin.log** para ver o par AV e a atribuição de função durante o login. Filtrar pelo nome de usuário:
<#root>

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

Procure as mensagens de injeção de função e atribuição de domínio:

Em funcionamento — Par AV convertido do mapa de grupo LDAP, o usuário obtém a função 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
```

Not Working — se uma linha **Cisco-avpair** ou **Converted to CiscoAVPair** não aparecer no fluxo, o servidor AAA não retornou o atributo e nenhuma regra de mapa de grupo LDAP correspondeu. Procure **Checking all UserDomains** sem nenhuma **Found UserDomain** linha seguindo-o — o usuário foi autenticado, mas não tem nenhuma atribuição de função. Se uma **Injection ... data FAILED** mensagem for exibida, o formato da cadeia de caracteres do par AV é inválido.

3. Verifique se o servidor AAA está retornando o atributo **cisco-av-pair** (para TACACS+ ou RADIUS) ou a associação de grupo LDAP correta (para LDAP). Verifique a configuração do servidor AAA:
    - TACACS+: Verifique se o perfil de usuário inclui **cisco-av-pair** o com o formato **shell:domains=all/admin/.**
    - RADIUS: Verifique se o perfil do usuário retorna **Cisco-AVPair = "shell:domains=all/admin/"** no Access-Accept.
    - LDAP: Verifique se o usuário é membro de um grupo LDAP que corresponda a uma regra de mapa de grupo (**aaaLdapGroupMapRule**) LDAP configurada.
4. Se o atributo estiver presente, mas o usuário ainda não tiver acesso, verifique se o nome do domínio de segurança no atributo corresponde a um domínio de segurança existente no APIC:
<#root>

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

Se o faz **cisco-av-pair** referência a um domínio que não existe (por exemplo, **shell:domains=NonExistentDomain/admin/**

), a atribuição de função falha silenciosamente.

Causa raiz: O servidor AAA não retorna os atributos de mapeamento RBAC, o formato do atributo está incorreto ou o domínio de segurança referenciado no atributo não existe no APIC.

Solução: Configure o servidor AAA para retornar o mapeamento correto **cisco-av-pair** ou de grupo. Verifique se o domínio de segurança existe no APIC.

Cenário: O Usuário Pode Exibir, Mas Não Pode Modificar A Configuração

Problema: Um usuário pode fazer logon e procurar objetos, mas recebe um erro quando tenta enviar alterações.

Etapas de verificação:

1. Verifique as atribuições de função do usuário:
   <#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. Se o usuário precisar de acesso de gravação, a atribuição deverá conceder **writePriv**. As funções comuns com privilégios de gravação incluem admin, tenant-admin, access-admin e fabric-admin.
3. Valide a atribuição de função nos logs do APIC. Filtrar pelo nome de usuário:
   <#root>

   ```
   apic1#

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

   Procure as mensagens de atribuição de função próximas ao final do fluxo de autenticação:

   Em funcionamento — o usuário tem a função de gravação de administrador (de um login 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
   ```

Não funciona — se o log mostrar `UserRole não-admin` com `privilégios de leitura` em vez de privilégios de gravação admin, o usuário terá uma função somente leitura e não poderá modificar a configuração. Procurar linhas como:

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

Se o registro mostrar apenas `privilégios de leitura` e nenhum `privilégio de gravação`, atualize a função do usuário ou o par AV no servidor AAA.

Causa raiz: O usuário tem uma função somente leitura (por exemplo, read-all ou ops) em vez de uma função com capacidade de gravação.

Solução: Atualize a atribuição de função do usuário no APIC (para usuários locais) ou atualize o **cisco-av-pair** no servidor AAA (para usuários remotos) para incluir uma função com privilégios de gravação.

Cenário: O Usuário Pode Acessar Alguns Locatários, Mas Não Outros

Problema: Um usuário pode ver e gerenciar um espaço, mas não pode ver outros espaços, mesmo que precise de acesso.

Etapas de verificação:

1. Verifique a atribuição de domínio de segurança do usuário:
   <#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. Os domínios de segurança são mapeados para usuários. Se o usuário precisar acessar o EspaçoB, ele também deverá ser atribuído ao domínio de segurança associado ao EspaçoB ou atribuído ao domínio all.
3. Para usuários remotos, confirme se o par AV ou o mapa de grupo LDAP atribui os domínios corretos. Verifique o APIC **nginx.bin.log** para a atribuição de domínio no login. Filtrar pelo nome de usuário:
   <#root>

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

Em funcionamento — o usuário tem o domínio de todos (visibilidade total), a partir de um login 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
```

Não está funcionando — se o usuário tiver apenas um único domínio de espaço, somente esse domínio aparecerá nas **Found UserDomain** mensagens em vez de todos. Por exemplo, `Encontrado UserDomain TenantA` significa que o usuário só pode ver o TenantA. O usuário precisa de domínios adicionais adicionados ao par de AV no servidor AAA ou ao domínio all para acesso completo.

Causa raiz: O usuário é atribuído a um domínio de segurança restrito que cobre apenas espaços específicos.

Solução: Adicione os domínios de segurança necessários à configuração do usuário ou use o domínio all para obter acesso total.

Recuperação de senha e acesso de emergência

Se todas as contas de administrador estiverem bloqueadas ou o servidor AAA remoto estiver inacessível e o território padrão tiver sido alterado, use um destes métodos de recuperação:

Domínio de logon de fallback

A ACI fornece um domínio de login de fallback integrado que sempre usa autenticação local, independentemente do território de autenticação padrão. Para usá-lo:

- SSH: Faça login como **apic:fallback\\admin** (ou **apic#fallback\\admin** , dependendo da versão).
- GUI: No menu suspenso Domínio na tela de login, selecione fallback e use as credenciais locais.

Acesso ao console

Se o território de autenticação de console estiver definido como local (o padrão), você sempre poderá fazer login através da porta de console do APIC com credenciais locais. Se a senha do administrador local for desconhecida, a senha poderá ser redefinida por meio do Cisco Integrated Management Controller (CIMC) (para APICs físicos) ou do console do hipervisor (para APICs virtuais).

Note: Se o território de autenticação de console tiver sido alterado para um servidor AAA remoto e esse servidor estiver inacessível, o acesso de console também falhará. Este é um cenário de bloqueio comum. Sempre mantenha o território de autenticação de console definido como local.

Referência a falhas comuns

As seguintes falhas da ACI são geralmente associadas ao acesso remoto e a problemas de AAA:

- F1773 — Problema de conectividade do provedor TACACS+. O APIC não pode acessar o servidor TACACS+.
- F1774 — Falha de autenticação TACACS+. O servidor está acessível, mas rejeitou a tentativa de autenticação.
- F1775 — Problema de conectividade do provedor RADIUS.
- F1776 — Falha de autenticação RADIUS.
- F1777 — Problema de conectividade do provedor LDAP.
- F1778 — Falha de autenticação LDAP.
- F0532 — Sub-rede de gerenciamento não configurada para um nó.

Consultar falhas AAA ativas:

<#root>

```
apic1#

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

Referências

- Solução de problemas de gerenciamento da ACI e Core Services — Políticas de Pod

- Guia de configuração básica do Cisco APIC, versão 6.1(x) — Gerenciamento
- Guia de configuração de segurança do Cisco APIC — acesso, autenticação e tarifação

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.