Problemen met externe toegang in een ACI-structuur oplossen

Inleiding

In dit document wordt beschreven hoe problemen met externe toegang in een Cisco Application Centric Infrastructure (ACI)-fabric kunnen worden geverifieerd, opgelost en opgelost. Het omvat Secure Shell (SSH) en Hypertext Transfer Protocol Secure (HTTPS) toegang tot APIC's en fabric-switches, externe verificatie, autorisatie en boekhouding (AAA) met toegangscontrolesysteem voor terminaltoegang Access-Control System Plus (TACACS+), externe verificatie Dial-In User Service (RADIUS) en Lightweight Directory Access Protocol (LDAP) en rolgebaseerde toegangscontrole (RBAC) autorisatie. Voor elk gebied zijn een beslissingsboom voor triage en gedetailleerde scenario's voor probleemoplossing opgenomen.

Achtergrondinformatie

Het materiaal uit dit document is samengesteld uit het hoofdstuk Problemen oplossen met ACI-beheer en kernservices — Pod Policies guide, de Cisco APIC Basic Configuration Guide, versie 6.1(x) — Management en de Cisco APIC Security Configuration Guide — Access, Authentication en Accounting.

Overzicht

Toegang op afstand tot een ACI-fabric omvat drie verschillende lagen, die elk moeten werken voor een ingenieur om succesvol in te loggen en te werken:

1. Transport — het beheernetwerkpad (OOB of in-band) en de protocolservice (SSH of HTTPS) moeten bereikbaar en ingeschakeld zijn.
2. Authenticatie — de gebruikersreferenties moeten worden gevalideerd, lokaal op de APIC of op een externe AAA-server (TACACS+, RADIUS of LDAP).
3. Autorisatie — de geverifieerde gebruiker moet de juiste RBAC-rollen en beveiligingsdomeinen toegewezen krijgen om de beoogde ACI-objecten te kunnen bekijken en wijzigen.

Een storing in elke laag veroorzaakt verschillende symptomen. Een transportstoring verhindert de verbinding volledig. Een verificatiefout retourneert een inloggegevens fout. Een autorisatiefout

maakt inloggen mogelijk, maar beperkt de zichtbaarheid of veroorzaakt "403 Verboden" fouten in de API.

Toegangsbeleid voor beheer

Het toegangsbeleid voor beheer (**commPol**Management Access Policy) is het centrale object dat bepaalt welke protocollen voor externe toegang op de fabric zijn ingeschakeld. Het bevindt zich onder Fabric > Fabric Policies > Policies > Pod > Management Access > default. Het beleid bevat onderliggende objecten die het volgende configureren:

- SSH (**commSsh**) — administratieve status, poort, codering, Key Exchange (KEX)-algoritmen, Message Authentication Codes (MAC's) en algoritmen voor hostsleutels.
- HTTPS (**commHttps**) — beheerdersstatus, poort, TLS-protocolversie (Transport Layer Security), throttle rate en verificatie van clientcertificaten.
- Telnet (**commTelnet**) — administratieve staat en haven. Telnet is standaard uitgeschakeld en Cisco raadt aan dat het uitgeschakeld blijft.

OOB en In-Band Management

ACI-nodes ondersteunen twee beheertoegangspaden:

- Out-of-Band (OOB) — gebruikt de speciale beheerpoort op de APIC of switch. OOB-beheeradressen worden toegewezen vanuit een pool onder de beheerderstenant en toegewezen aan knooppunten via **mgmtRsOoBStNode**beheerdersbeheer. Op de APIC worden OOB-contracten afgedwongen door middel van **iptables** regels. Als een OOB-contract wordt toegepast, kan alleen verkeer dat expliciet is toegestaan door het contract de APIC-beheerinterface bereiken.
- In-Band (INB) — gebruikt het fabric-gegevensvlak voor verkeersbeheer. Voor In-band-beheer is een toewijzing van adressen voor Bridge Domain (BD), subnet, Endpoint Group (EPG), contract- en knooppuntbeheer vereist. In-band IP-adressen zijn niet bereikbaar van buiten de verbinding zonder extra routering of beleidsconfiguratie.

 Opmerking: APIC OOB-beheer-IP's worden geconfigureerd tijdens de eerste configuratie en de APIC verkrijgt IP-connectiviteit voordat de verbinding volledig is ontdekt. OOB is het primaire beheerpad en is altijd beschikbaar als het fysieke beheernetwerk is verbonden.

AAA-architectuur

ACI maakt gebruik van een drieledig AAA-model:

1. Login Domain (**aaaLoginDomain**) - groepeert AAA-providers onder een benoemde realm. Gebruikers geven het aanmeldingsdomein op in het aanmeldingsscherm (bijvoorbeeld `apic:TACACS-Domain` of via de vervolgkeuzelijst in de gebruikersinterface). Er bestaat altijd een speciaal fallback-aanmeldingsdomein dat wordt toegewezen aan lokale verificatie.
2. Provider Group (**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**,, **aaaLdapProviderGroup**) — verwijst naar een of meer AAA-servers en definieert de volgorde waarin ze worden geprobeerd.
3. Provider (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**) — definieert het IP-adres van de server, de poort, het gedeelde geheim (of het bind-DN voor LDAP), de time-out, nieuwe pogingen, EPG-beheer en controlereferenties.

Het standaarddomein voor verificatie (**aaaDefaultAuth**Default Authentication Realm) bepaalt welk aanmeldingsdomein wordt gebruikt wanneer de gebruiker er geen opgeeft bij het aanmelden. De Console Authentication Realm regelt de verificatie voor consolesessies.

Opmerking: als u het standaardverificatieniveau wijzigt in een externe AAA-server terwijl die server onbereikbaar is, wordt u uit de verbinding gesloten. Test altijd de connectiviteit van de AAA-server voordat u het domein wijzigt. Het fallback-aanmeldingsdomein (`apic:fallback\\admin`) kan worden gebruikt om het standaarddomein te omzeilen en lokaal te verifiëren.

Belangrijkste AAA-logbestanden

AAA-verificatiegebeurtenissen worden in verschillende bestanden aangemeld op zowel de APIC- als fabric-switches. Deze logboeken zijn het primaire hulpmiddel voor het valideren van authenticatieresultaten, het identificeren van het rijk en de providergroep die wordt gebruikt en het diagnosticeren van roltoewijzingsfouten.

logbestand	Locatie (APIC)	Locatie (Switches)	Be
nginx.bin.log (APIC) nginx.log (switches)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	Primair A volledige PAM-aan selectie, provider, LDAP/TA communi van AV-p roltoewijz van succe De besta verschilt maar de i hetzelfde

logbestand	Locatie (APIC)	Locatie (Switches)	Be
access.log	/var/log/dme/log/access.log	/var/log/dme/log/access.log	NGINX H verzoeklo per API-v APIC, toc aaaRefres HTTP sta succes, 4 Op switch interne D verzoeke oproepen
pam.module.log	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	Logboek Toont het verificatie SSH-sess geverifiee bron-IP e UNIX-geb switches manier or of een ge geverifiee

Opmerking: het primaire AAA-log heeft een andere bestandsnaam op elk platform. Op de APIC is het **nginx.bin.log** at/var/log/dme/log/. Op blad- en ruggengraat switches is het **nginx.log** at/var/sysmgr/tmp_logs/dme_logs/. De indeling van de loginhoud en AAA-berichten zijn op beide platforms hetzelfde.

AAA-items in het nginx-log volgen deze indeling:

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

Filter AAA-gerelateerde logboekvermeldingen voor de verificatiestroom van een specifieke gebruiker:

<#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
```

Of bekijk alle recente authenticatieverzoeken en -resultaten:

<#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
```

Een typische succesvolle verificatiestroom toont deze belangrijke berichten in volgorde:

1. `Ontvangen PAM-authenticatieverzoek van nginx voor Gebruikersnaam: <user>` — het aanmeldingsverzoek is ontvangen.
2. `DefaultAuthMo geeft realm <N> op. Providergroep <naam>!` — het gebied werd geselecteerd (0=fallback/lokaal, 2=TACACS+, 3=LDAP).
3. Provider-specifieke berichten (LDAP-binding, TACACS+-provider zoeken of RADIUS-verzoek).
4. `Gevonden UserDomain <domain> onder externe gebruikersnaam: <user>` — de domeintoewijzing van het AAA-antwoord.
5. `Gevonden gebruikersnaam: admin met schrijfbevoegdheden voor admin onder UserDomain - alle gebruiker is een admin-gebruiker` - de rolcontrole is geslaagd.

Een mislukt verificatielogboek:

- `Gebruiker <gebruiker> is geweigerd tijdens AAA-verificatie`
- `Fout van niet-geautoriseerde gebruiker <user>: verificatie AAA-server GEWEIGERD`

Opmerking: Het nginx-log roteert vaak en oudere items zijn gzip gecomprimeerd met een numeriek achtervoegsel. Op de APIC bevinden de geroteerde logs zich in dezelfde directory (bijvoorbeeld **nginx.bin.log.22815.gz**CMS). Op switches worden de geroteerde logs opgeslagen op

---

/var/log/dme/oldlog/dme/nginx.log.*.gz (met symlinks in `/var/sysmgr/tmp_logs/dme_logs/`). U kunt als volgt zoeken in geroteerde logs:

<#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'
```

RBAC-model

ACI RBAC bepaalt wat een geverifieerde gebruiker kan zien en doen. Het model bestaat uit drie onderdelen:

- Beveiligingsdomein (**aaaDomain**) — een bereikbeperking die wordt toegewezen aan ACI-objecten (huurders, toegangsbeleid, structuurbeleid). De ingebouwde domeinen alle, gemeenschappelijke, en beheer zijn altijd aanwezig. Aangepaste domeinen beperken de zichtbaarheid van een gebruiker tot specifieke huurders of beleidsgebieden.
- Rol (**aaaRole**) — definieert een reeks bevoegdheden. Vooraf gebouwde rollen omvatten admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops en nw-svc-admin.
- Privilege — elke rol geeft lees- of schrijftoegang (wat lees impliceert) tot een specifiek functioneel gebied.

Aan een gebruikersaccount worden een of meer beveiligingsdomein- en rolparen toegewezen. Voor externe gebruikers die zijn geverifieerd via TACACS+, RADIUS of LDAP, wordt de roltoewijzing geleverd via leverancierspecifieke kenmerken in de AAA-respons (bijvoorbeeld het **cisco-av-pair** kenmerk).

triage-beslisboom

Gebruik deze beslisboom wanneer een gebruiker meldt dat hij geen toegang heeft tot de ACI-structuur op afstand:

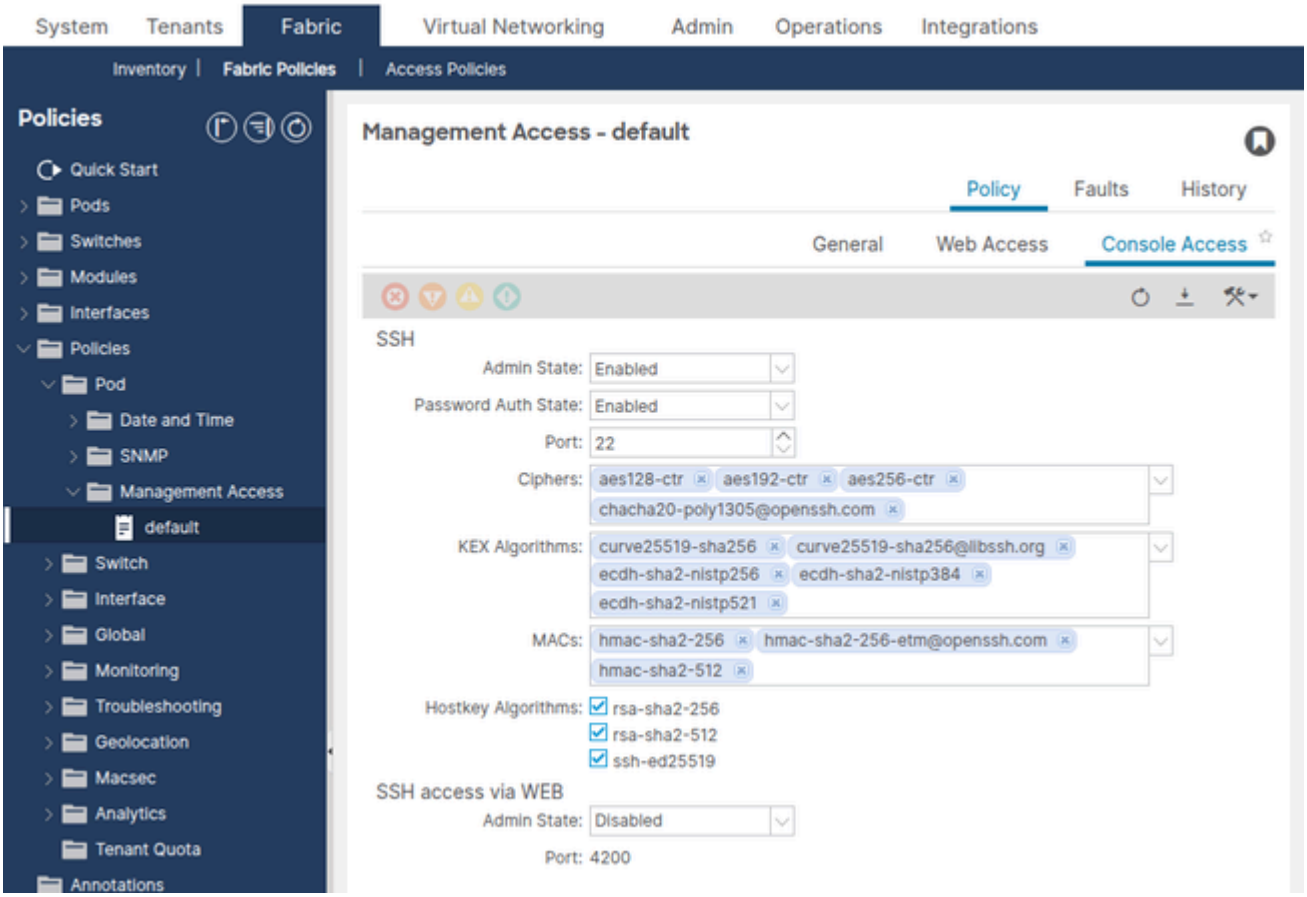
1. Kun je de APIC of switch management IP pingen?
    - Nee → Problemen met het beheernetwerkpad oplossen. Raadpleeg de sectie "Problemen oplossen met OOB en In-Band Management".
    - Ja → Doorgaan.
2. Kunt u een SSH- of HTTPS-verbinding tot stand brengen (wordt de verbinding überhaupt geopend)?
    - Nee → De protocolservice kan worden uitgeschakeld, de poort kan worden gefilterd of er kan een coderingsfout optreden. Raadpleeg de secties "Problemen oplossen met SSH-toegang" of "Problemen oplossen met HTTPS-toegang".
    - Ja → Doorgaan.
3. Wordt het aanmeldingsscherm weergegeven (HTTPS) of wordt de SSH-handshake voltooid en wordt gevraagd om referenties?
    - Geen → SSH-sleuteluitwisseling of TLS-handshake-fout. Raadpleeg de sectie "Problemen oplossen met SSH-toegang" voor mismatches tussen cijfers en KEX.
    - Ja → Doorgaan.
4. Zijn referenties mislukt met "Verificatie mislukt" of vergelijkbaar?
    - Ja → Verificatieprobleem. Raadpleeg de secties "Problemen met AAA-verificatie oplossen" (TACACS+, RADIUS of LDAP, afhankelijk van het aanmeldingsdomein dat wordt gebruikt).
    - Nee → Doorgaan.
5. Meld de gebruiker zich aan, maar kan hij verwachte objecten niet zien, of krijgt hij "403 Verboden"-fouten?
    - Ja → Vergunningverlening of RBAC-kwestie. Raadpleeg de sectie "Problemen met RBAC en gebruikersrechten oplossen".
    - Nee → Toegang werkt. Controleer het specifieke probleem dat de gebruiker ondervindt.

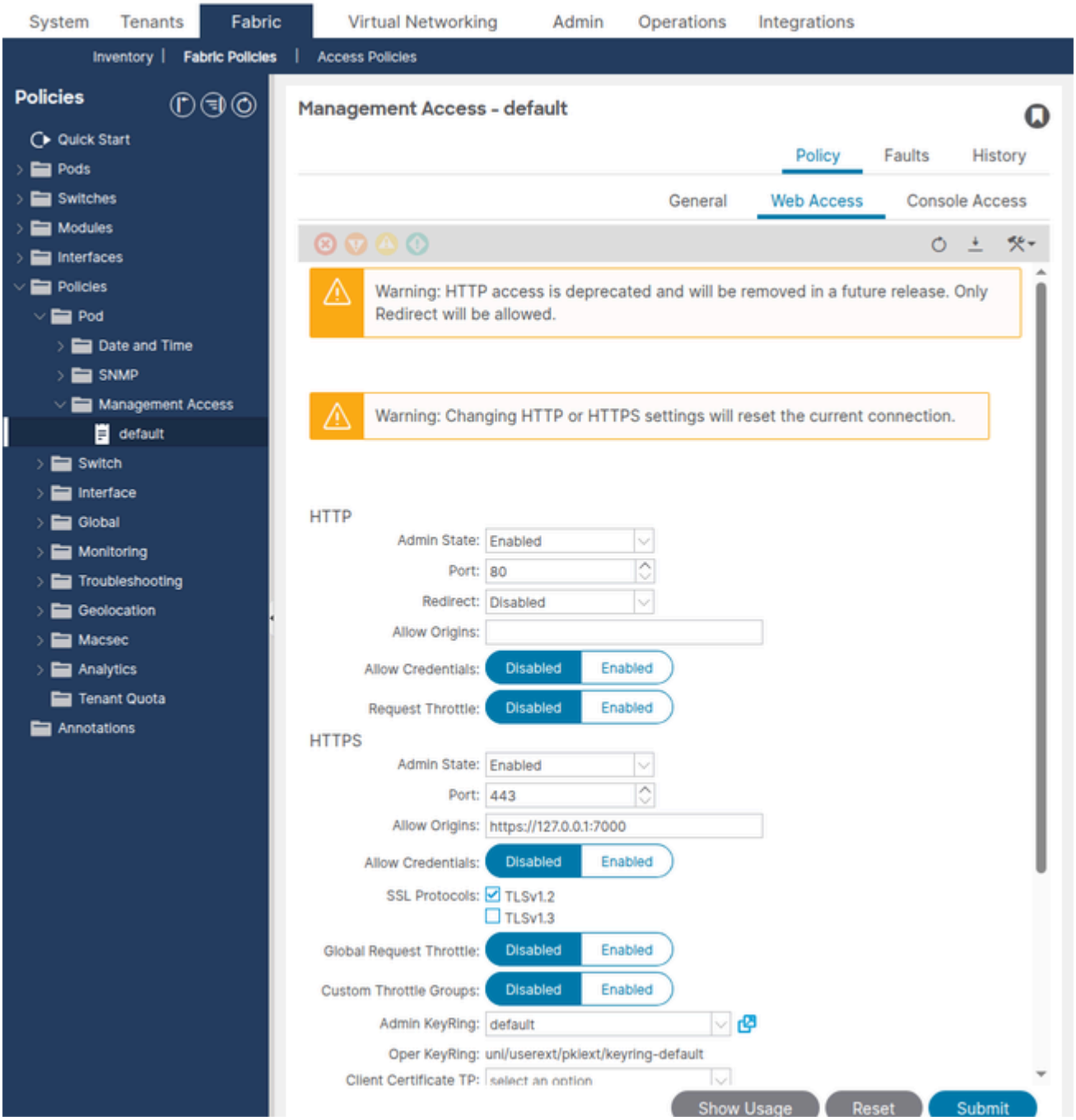
De configuratie verifiëren

Voordat u problemen met de operationele status oplost, controleert u of de configuratieketen is voltooid. Misconfiguratie is de meest voorkomende hoofdoorzaak van problemen met externe toegang.

Controleer het toegangsbeleid voor beheer (SSH en HTTPS)

Navigeer naar 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



Bevestig de volgende SSH-instellingen:

- Beheerdersstatus — moet zijn ingeschakeld.
- Poort — standaard 22. Indien gewijzigd, moet de SSH-client de aangepaste poort gebruiken.
- Wachtwoordverificatie — ingeschakeld (tenzij alleen certificaatverificatie is bedoeld).
- SSH-coderingen — moeten ten minste één codering bevatten die door de SSH-client wordt ondersteund.
- KEX-algoritmen — moeten ten minste één algoritme bevatten dat wordt ondersteund door de SSH-client.
- SSH-MAC's — moeten ten minste één MAC bevatten die door de SSH-client wordt ondersteund.

Het door SSH beheerde object opvragen via de 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
```

Bevestig de volgende HTTPS-instellingen:

- Beheerdersstatus — moet zijn ingeschakeld.
- Poort — standaard 443.
- SSL-protocollen — TLSv1.2 (standaard). Oudere clients kunnen eisen dat TLSv1.1 expliciet wordt toegevoegd.
- Throttle State — indien ingeschakeld, beperkt de Throttle Rate verzoeken per seconde per gebruiker. Een zeer lage waarde kan fouten in de time-out van de API veroorzaken.

<#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
```

Veelvoorkomende misconfiguraties

- SSH-coderingen werden te agressief beperkt - in ACI-release 5.2(1) en later werden de standaard SSH-coderingen gehard. Oudere SSH-clients (bijvoorbeeld PuTTY-versies vóór 0,75 of OpenSSH-versies die alleen **diffie-hellman-group14-sha1**ondersteuning bieden) kunnen de sleuteluitwisseling mislukken. De SSH-client geeft "geen overeenkomende codering

gevonden" of "geen overeenkomende methode voor sleuteluitwisseling gevonden" weer.
- Wachtwoordverificatie uitgeschakeld — als **passwordAuth** is ingesteld op Uitgeschakeld, is alleen op SSH-sleutel gebaseerde verificatie toegestaan. Gebruikers die verbinding maken met wachtwoorden zien "Toestemming geweigerd (public key)".
- Aangepaste SSH-poort zonder clientbewustzijn — als de SSH-poort is gewijzigd van 22, moet de SSH-client de nieuwe poort opgeven (bijvoorbeeld **ssh -p 2222 admin@10.1.1.1**).

OOB-beheeradressen controleren

Navigeer naar Huurders > Beheer > Adressen voor knooppuntbeheer.

Bevestig dat aan elk APIC- en switch-knooppunt een IP-adres voor OOB-beheer is toegewezen met een geldige gateway. Nodes zonder beheeradressen zijn niet bereikbaar via het beheernetwerk.

De toewijzingen van de statische OOB-knooppunten via de API opvragen:

<#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
```

Veelvoorkomende misconfiguraties

- Ontbrekende OOB-adrestoewijzing - een switch heeft geen vermelding onder **mgmtRsOoBStNode**. De node heeft geen IP-beheer en reageert niet op SSH of HTTPS op de OOB-interface.
- Onjuiste gateway — het gateway-adres komt niet overeen met de werkelijke gateway op het OOB-beheernetwerk. De node kan pakketten ontvangen, maar kan geen retourverkeer verzenden.
- Mismatch van subnetmasker — het OOB-subnetmasker komt niet overeen met het fysieke beheernetwerk. Dit kan ertoe leiden dat de node gelooft dat het beheerstation zich op een ander subnet bevindt en dat het verkeer door een gateway wordt geleid die niet bestaat of onjuist is.

OOB-contracten verifiëren

Navigeer naar Huurders > beheer > Contracten.

Als een OOB-contract wordt toegepast op de OOB-beheer-EPG, zal alleen verkeer dat expliciet is toegestaan door dat contract de APIC-beheerinterface bereiken. Op de APIC worden OOB-contracten afgedwongen via **iptables** regels.

Vraag de OOB EPG verstrekte contracten:

<#root>

```
apic1#

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

Als de query resultaten oplevert, worden contracten toegepast. Controleer de contractonderwerpen en filters die de vereiste protocollen toestaan:

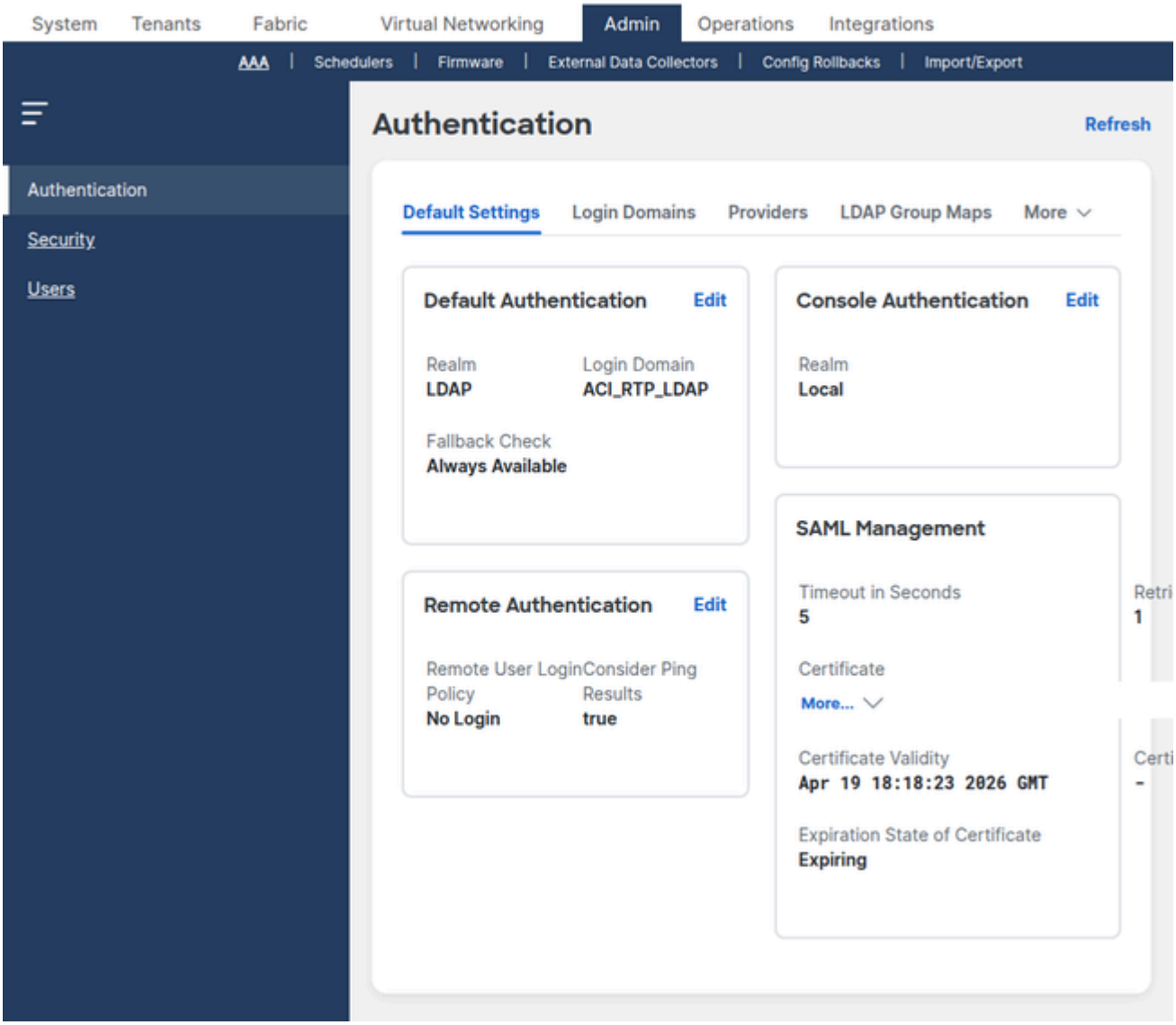
- SSH — TCP-poort 22 (of aangepaste poort)
- HTTPS — TCP-poort 443 (of aangepaste poort)
- ICMP — voor ping-verificatie

Veelvoorkomende misconfiguraties

- Het OOB-contract bevat geen SSH of HTTPS — de technicus kan de APIC pingen, maar kan geen verbinding maken via SSH of HTTPS. De **iptables** regels op de APIC laten het verkeer stilletjes vallen.
- IP-bronbeperking in het OOB-contractfilter — het contractfilter beperkt de toegang tot specifieke bronsubnetten. Ingenieurs buiten dat subnet kunnen geen verbinding maken.

AAA-configuratie controleren

Navigeer naar Beheer > AAA > Authenticatie > AAA.



Bevestig het volgende:

- Standaardverificatieruimte — identificeert welk aanmeldingsdomein wordt gebruikt wanneer de gebruiker er geen opgeeft. Indien ingesteld op een extern AAA-aanmeldingsdomein, moet de corresponderende server bereikbaar zijn.
- Console Authentication Realm — regelt de toegang tot de console. Als deze optie is ingesteld op lokaal, wordt bij het aanmelden voor de console altijd gebruikgemaakt van lokale referenties (aanbevolen).

Aanmeldingsdomeinen verifiëren

Navigeer naar Beheer > AAA > Authenticatie > Aanmeldingsdomeinen.

<#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
```

Controleer of het aanmeldingsdomein dat wordt gebruikt voor verificatie aanwezig is en of het verwijst naar de juiste providergroep.

Controleer TACACS+-providers

Navigeer naar Beheer > AAA > Authenticatie > 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
```

RADIUS-providers verifiëren

Navigeer naar Beheer > AAA > Authenticatie > 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
```

LDAP-providers verifiëren

Navigeer naar Beheer > AAA > Verificatie > 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
```

Veel voorkomende AAA-misconfiguraties

- Gedeelde geheime mismatch — de sleutel die is geconfigureerd op de ACI TACACS+- of RADIUS-provider komt niet overeen met de sleutel op de server. Authenticatie mislukt stilletjes.
- Verkeerd EPG-beheer — de EPG van de provider **epgDn** is leeg of wijst naar de verkeerde EPG (bijvoorbeeld in-band wanneer de server zich op het OOB-netwerk bevindt). De APIC kan de server niet bereiken.
- Login domain realm mismatch — het aanmeldingsdomein is geconfigureerd als LDAP, maar de gebruiker verwacht TACACS+-verificatie. Aanmeldingsdomeinen moeten verwijzen naar het juiste type providergroep.
- LDAP binden DN onjuist - de **rootdn** binding (DN) of **basedn** zijn verkeerd. LDAP-verificatie mislukt met een bindfout, zelfs als de gebruikersreferenties juist zijn.
- Het LDAP-filter komt niet overeen met het directoryschema — gebruik **sAMAccountName=$userid**hiervoor Active Directory. Voor OpenLDAP gebruikt u **cn=$userid** of **uid=$userid**gebruikt u.

Controleer de RBAC-configuratie

Navigeer naar Beheer > AAA > Gebruikers om lokale gebruikersaccounts en hun beveiligingsdomein en roltoewijzingen te bekijken.

Beveiligingsdomeinen opvragen via de 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
```

Een gebruiker die is toegewezen aan een domein met alle functies van rolbeheer heeft volledige lees-schrijf toegang tot de gehele fabric. Een gebruiker die is toegewezen aan een aangepast beveiligingsdomein met rol tenant-admin kan alleen huurders beheren die aan dat domein zijn gekoppeld.

Algemene RBAC-misconfiguraties

- Gebruiker gemaakt zonder beveiligingsdomein - de gebruiker kan inloggen maar ziet geen huurders en ontvangt "403 Verboden" op API-oproepen. Ten minste één beveiligingsdomein moet worden toegewezen.
- Alleen-lezen rol toegewezen wanneer schrijftoegang nodig is - de gebruiker kan objecten bekijken maar kan geen wijzigingen indienen. Controleer of het rolprivilege is ingesteld op writePriv.
- Toewijzing van gebruikersrollen op afstand ontbreekt op de AAA-server — de TACACS+- of RADIUS-server retourneert niet het **cisco-av-pair** kenmerk met **shell:domains=all/admin/**daarin. De gebruiker verifieert met succes, maar heeft geen rollen en kan niets zien in de structuur.

Problemen met OOB en In-Band Management oplossen

Als de APIC of switch management IP niet bereikbaar is op het netwerk, moet u het beheerpad oplossen voordat u SSH, HTTPS of AAA onderzoekt.

Scenario: kan de APIC OOB IP niet pingen

Probleem: het beheerstation kan het IP-adres van het APIC OOB-beheer niet pingen.

Verificatiestappen:

1. Controleer of de APIC-beheerpoort fysiek is aangesloten en of de koppeling actief is.
2. Controleer of het beheerstation zich in hetzelfde L2-segment bevindt of een route heeft naar het OOB-subnet.
3. Controleer of de OOB-beheer-IP correct is toegewezen:
   <#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. Controleer of de standaardgateway bereikbaar is:
   <#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. Als een OOB-contract wordt toegepast, controleer dan of het de vereiste protocollen toestaat. Vraag de OOB EPG verstrekte contracten zoals weergegeven in de sectie "OOB-contracten verifiëren". OOB-contracten worden afgedwongen als **iptables** regels voor de APIC. U kunt de opgeslagen regels bekijken vanuit de APIC-shell:
   <#root>

   ```
   apic1#

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

   Als het INPUT-beleid DROP is en er geen Accept-regel is voor het vereiste protocol, filtert het OOB-contract het verkeer.

   > Opmerking: De **iptables -L -n** opdracht om live kernel-regels te bekijken vereist root-toegang en is niet beschikbaar voor reguliere SSH-beheersessies.

Hoofdoorzaak: ontbrekend of verkeerd geconfigureerd OOB-beheeradres, onjuiste gateway of

OOB-contractfilterverkeer.

Oplossing: corrigeer de toewijzing van het OOB-adres, controleer het fysieke netwerkpad of werk het OOB-contract bij om de vereiste protocollen toe te staan.

Scenario: kan IP-adres voor Switch-beheer niet bereiken

Probleem: het beheerstation kan de APIC bereiken, maar kan geen switch bereiken via OOB.

Verificatiestappen:

1. Controleer of aan de switch een OOB-adres is toegewezen:
   <#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. Controleer of aan de beheerinterface van de switch het IP-adres is toegewezen:
   <#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. Verifieer de standaard VRF-beheerroute:
   <#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
   ```

Hoofdoorzaak: toewijzing van het OOB-adres ontbreekt, gateway niet correct is of de fysieke poort voor het beheer van de switch niet beschikbaar is.

Oplossing: het OOB-adres toewijzen onder Huurders **>** beheer **>** Adressen voor knooppuntbeheer.

Controleer of de koppeling voor fysiek beheer is ingeschakeld.

Problemen met SSH-toegang oplossen

In dit gedeelte worden scenario's beschreven waarbij het IP-beheer bereikbaar is (ping slaagt), maar de SSH-sessie niet tot stand kan worden gebracht of kan worden geverifieerd.

Scenario: SSH-verbinding geweigerd

Probleem: De SSH-client meldt "Verbinding geweigerd" bij het verbinden met de APIC of switch.

Verificatiestappen:

1. Controleer of SSH is ingeschakeld in het toegangsbeleid voor beheer:
   <#root>

   ```
   apic1#
   moquery -c commSsh -x 'query-target-filter=eq(commSsh.adminSt,"enabled")'

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

   Als **adminSt** SSH is uitgeschakeld, worden SSH-verbindingen geweigerd.

2. Controleer of de juiste poort wordt gebruikt. Als de SSH-poort is gewijzigd van 22:
   <#root>

   ```
   $
   ssh -p
    custom-port
   admin@10.1.1.1
   ```

3. Controleer of het OOB-contract TCP toestaat op de SSH-poort. Raadpleeg de sectie "OOB-contracten verifiëren".

Hoofdoorzaak: SSH is uitgeschakeld in het toegangsbeleid voor beheer, aangepaste poort die niet bekend is bij de client of OOB-contractfiltering.

Oplossing: SSH inschakelen in het toegangsbeleid voor beheer of de juiste poort gebruiken.

Scenario: SSH-sleuteluitwisselingsfout (codering of KEX-mismatch)

Probleem: de SSH-client mislukt met "geen overeenkomende codering gevonden", "geen overeenkomende methode voor sleuteluitwisseling gevonden" of "geen overeenkomende MAC gevonden".

Verificatiestappen:

1. Controleer de uitvoeruitvoer van de SSH-client om te bepalen welke algoritmen de client aanbiedt:
<#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. Vergelijk de door de klant aangeboden algoritmen met de APIC-geconfigureerde algoritmen:
<#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. Identificeer het kruispunt. Als er geen gemeenschappelijk algoritme in een categorie, de handshake mislukt.

Opmerking: In ACI versie 5.2(1) en later werden de standaard SSH-coderingen en KEX-algoritmen gehard. Legacy-algoritmen zoals **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**, **aes128-cbc**en **hmac-sha1** worden niet langer standaard aangeboden. Als u onlangs een upgrade hebt uitgevoerd, controleert u of de SSH-clients in uw omgeving de nieuwe standaardinstellingen ondersteunen.

Root Cause: Geen gemeenschappelijk cijfer, KEX-algoritme of MAC tussen de SSH-client en de APIC na een ACI-upgrade of versleuteling.

Oplossing: de SSH-client bijwerken om moderne algoritmen te ondersteunen of het vereiste algoritme opnieuw toevoegen aan het toegangsbeleid voor beheer. Het opnieuw toevoegen van

oude algoritmen brengt beveiligingsrisico's met zich mee en wordt niet aanbevolen voor de lange termijn.

Scenario: SSH maakt verbinding, maar verificatie mislukt voor lokale gebruikers

Probleem: SSH-handshake is geslaagd (wachtwoordprompt wordt weergegeven), maar het wachtwoord wordt geweigerd voor een lokale gebruiker.

Verificatiestappen:

1. Controleer of de gebruiker lokaal bestaat:
   <#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. Controleer of de account is vergrendeld vanwege overmatige mislukte inlogpogingen:
   <#root>

   ```
   apic1#
   ```

   ```
   moquery -c aaaUserEp
   ```

   ```
   dn                 : uni/userext
   pwdStrengthCheck   : no
   ```

   Controleer het vergrendelingsbeleid voor het aanmeldingsdomein onder Beheer > AAA > Beveiligingsbeheer > Vergrendelingsbeleid.

3. Controleer of de gebruiker zich aanmeldt met het juiste aanmeldingsdomein. Als het standaardverificatieniveau is ingesteld op een extern AAA-aanmeldingsdomein, moet de gebruiker zich aanmelden **apic:LOCAL\\username** of **apic:fallback\\username** de lokale verificatie forceren.
4. De verificatieresultaten in de logs valideren. Controleer **nginx.bin.log** de APIC voor de inloggebeurtenis:
   <#root>

   ```
   apic1#
   ```

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

   Zoek naar het domein en de providergroep die is toegewezen aan de aanmeldingspoging:

```
! 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
```

Als het domein niet 0 is (fallback/lokaal), is de aanmelding verzonden naar een externe AAA-server in plaats van de lokale database. De gebruiker moet zich **apic:fallback\\username** voorbereiden of **apic:LOCAL\\username** de lokale authenticatie afdwingen.

Hoofdoorzaak: Onjuist wachtwoord, vergrendelde account of de aanmeldingspoging wordt verzonden naar een externe AAA-server in plaats van de lokale database.

Oplossing: Reset het wachtwoord, ontgrendel de account of gebruik het juiste voorvoegsel voor het aanmeldingsdomein.

Problemen met HTTPS-toegang oplossen

Deze sectie behandelt scenario's waarbij de APIC web UI of Representational State Transfer (REST) Application Programming Interface (API) onbereikbaar is via HTTPS.

Scenario: HTTPS-verbindingstijden uit

Probleem: de browser toont "ERR_CONNECTION_TIMED_OUT" of de API-aanroep hangt bij het verbinden met de APIC op poort 443.

Verificatiestappen:

1. Controleren of HTTPS is ingeschakeld:
   <#root>

```
apic1#

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

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

2. Controleer of het OOB-contract TCP 443 toestaat. Raadpleeg de sectie "OOB-contracten verifiëren".
3. Test vanuit de APIC zelf om te bevestigen dat het HTTPS-proces luistert:
   <#root>

```
apic1#

ss -tlnp | grep 443

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

Hoofdoorzaak: HTTPS uitgeschakeld, OOB-contractfiltering TCP 443 of het nginx-proces op de APIC is gecrasht.

Oplossing: HTTPS inschakelen in het toegangsbeleid voor beheer, het OOB-contract bijwerken of de webservice op de APIC opnieuw starten.

Scenario: Browser toont TLS-handshake-fout

Probleem: De browser geeft "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" of een soortgelijke TLS-fout weer.

Verificatiestappen:

1. Controleer de versie van het TLS-protocol die is geconfigureerd op de APIC:
   <#root>

```
apic1#

moquery -c commHttps

sslProtocols : TLSv1.2
```

2. Controleer of de browser TLSv1.2 ondersteunt. Zeer oude browsers (bijvoorbeeld Internet Explorer 10 en ouder) ondersteunen standaard geen TLSv1.2.

Hoofdoorzaak: De APIC biedt alleen TLSv1.2 (de standaard) en de browser of API-client ondersteunt alleen oudere TLS-versies.

Oplossing: de browser of client bijwerken. Als u oudere clients tijdelijk moet ondersteunen, voegt u TLSv1.1 toe aan het toegangsbeleid voor beheer, maar dit brengt beveiligingsrisico's met zich mee.

Scenario: API Throttle Limiting

Probleem: REST API-oproepen mislukken met tussenpozen met HTTP 503-fouten of de web-gebruikersinterface wordt traag tijdens zware automatisering.

Verificatiestappen:

```
<#root>

apic1#

moquery -c commHttps

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

Als de gasklepsnelheid erg laag is en automatiseringsscripts veel verzoeken per seconde verzenden, wijst de APIC overtollige verzoeken af.

Hoofdoorzaak: de gasklepsnelheid per gebruiker is te laag voor de automatiseringswerklast.

Oplossing: Verhoog de gasklepsnelheid onder het toegangsbeleid voor beheer of optimaliseer de automatiseringsscripts om de aanvraagfrequentie te verminderen. U kunt ook throttling uitschakelen als de verbinding niet wordt gedeeld.

Problemen met AAA oplossen — TACACS+

In dit gedeelte wordt ingegaan op TACACS+-verificatiefouten. De APIC communiceert met de TACACS+-server via TCP-poort 49.

operationele verificatie

ACI-switches ondersteunen de **test aaa** opdracht die beschikbaar is op standalone NX-OS niet. Om de werking van TACACS+ te verifiëren, gebruikt u de APIC om de status van de provider, fouten en de geschiedenis van de aanmeldingssessie te controleren.

Controleer op actieve fouten bij de TACACS+-provider:

```
<#root>

apic1#

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

Als er geen fouten worden geretourneerd, beschouwt de APIC de provider als bereikbaar. Als er fouten aanwezig zijn, bevat de uitvoer foutcodes zoals F1773 (provider onbereikbaar) of F1774 (verificatiefout).

Controleer de configuratie van de TACACS+-provider:

```
<#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
```

Verifieer de bereikbaarheid van het basisnetwerk van de APIC naar de TACACS+-server:

```
<#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
```

Probeer in te loggen op de APIC met het TACACS+-aanmeldingsdomein en controleer het sessieresultaat:

```
<#root>

apic1#
```

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

Kijk in het **descr** veld om te bepalen of de fout te wijten was aan authenticatieafwijzing of een connectiviteitsprobleem.

De TACACS+-verificatiestroom valideren in de APIC-logs. Filter voor de betreffende gebruikersnaam:

<#root>

apic1#

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

TACACS+-aanmeldingen volgen dezelfde **nginx.bin.log** verificatiestroom als LDAP (zie de sectie LDAP Operational Verification voor volledige voorbeelden van echte logbestanden). De belangrijkste verschillen voor TACACS+ zijn:

- `DefaultAuthMo specificeert realm 2` — realm 2 geeft TACACS+ aan (vs. realm 3 voor LDAP).
- `TacacsProvider <IP> toevoegen aan de lijst` — identificeert de TACACS+-server waarmee contact wordt opgenomen (vs. `LdapProvider` voor LDAP).
- `TACACS+ Cisco-avpair (shell: domains=all/admin/admin)` — het AV-paar wordt rechtstreeks teruggegeven door de TACACS+-server (in plaats van te worden geconverteerd van een LDAP-groepskaart).

Een succesvolle TACACS+ login toont dezelfde progressie: PAM request → realm selection → provider lookup → AV pair parsing → user injection → UserDomain and role assignment → `admin write privileges`.

Een mislukte TACACS+-aanmelding eindigt met `Gebruiker <gebruikersnaam> werd geweigerd tijdens AAA-verificatie` en `Onbevoegde ... fout: AAA Server-verificatie GEWEIGERD`, hetzelfde patroon als een LDAP-weigering.

Scenario: TACACS+-verificatie mislukt

Probleem: aanmelden mislukt met "Verificatie mislukt" wanneer de gebruiker een TACACS+-aanmeldingsdomein selecteert.

Verificatiestappen:

1. Controleer op actieve fouten bij de TACACS+-provider:
   <#root>

   ```
   apic1#

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

   Fout F1773 duidt op een connectiviteitsprobleem. Fout F1774 duidt op een afwijzing van de verificatie.

2. Controleer de netwerkbereikbaarheid van de APIC naar de TACACS+-server:
   <#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. Als de ping slaagt maar de verificatie mislukt, controleert u de gedeelde geheime overeenkomsten op zowel de APIC-providerconfiguratie als de TACACS+-serverconfiguratie.
4. Controleer de meest recente aanmeldingssessies om de details van de fout te bekijken:
   <#root>

   ```
   apic1#

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

5. Controleer de logboeken van de TACACS+-server voor de verificatiepoging. Een succesvolle poging die op de server is aangemeld maar is afgewezen, duidt op een probleem met de gebruikersconfiguratie aan de serverzijde (bijvoorbeeld een fout in het wachtwoord of een ontbrekende gebruikersaccount).
6. Controleer de APIC `nginx.bin.log` voor de volledige verificatiestroom. Filter op de gebruikersnaam in plaats van specifieke zoekwoorden, zodat tussenliggende berichten niet worden gemist:
   <#root>

   ```
   apic1#

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

   Vergelijk de output met de werkende en niet-werkende voorbeelden in de sectie Operationele verificatie hierboven. Kernindicatoren:

   - `werd geweigerd` of `geweigerd` — de TACACS+-server werd bereikt, maar de referenties werden afgewezen. Controleer of de gebruiker op de server aanwezig is en of het wachtwoord overeenkomt.

- Geen providerspecifieke berichten na het `toevoegen van TacacsProvider` - de server is onbereikbaar of is niet getimed. Controleer de bereikbaarheid van het netwerk en het EPG-beheer.
- `Injectie van externe gebruiker ... werd voltooid` gevolgd door rolcontrolelijnen - authenticatie is gelukt, maar het probleem kan worden opgelost met roltoewijzing (zie de sectie AV-paar hieronder).

TACACS+ cisco-av-pair voor RBAC

Voor externe gebruikers die via TACACS+ zijn geverifieerd, moet de server het **cisco-av-pair** attribuut in de autorisatierespons retourneren. Dit attribuut wijst de gebruiker toe aan ACI-beveiligingsdomeinen en -rollen.

Formaat:

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

Voorbeelden:

- Volledig beheer: **shell:domains=all/admin/**
- Alleen-lezen voor iedereen: **shell:domains=all/read-all/**
- Huurder-beheerder voor een specifiek domein: **shell:domains=TenantA/tenant-admin/**
- Meerdere domeinen: **shell:domains=all/admin/,TenantA/tenant-admin/**

Als dit kenmerk ontbreekt of verkeerd is gevormd, wordt de gebruiker met succes geverifieerd, maar heeft geen rollen en kan geen objecten in de APIC-gebruikersinterface zien.

Opmerking: voor SSH-toegang tot switches met bladeren en ruggegraat is de beheerdersrol met schrijfbevoegdheid in het all security-domein vereist. Het minimum AV-paar voor switch SSH-toegang is **shell:domains=all/admin/**beperkt. Gebruikers met niet-beheerdersrollen (bijvoorbeeld `read-all`, `tenant-admin`, `aaa`) of gebruikers die zijn toegewezen aan een ander beveiligingsdomein dan alle kunnen zich aanmelden bij de APIC, maar krijgen geen toegang tot SSH-switches. Het APIC-logboek laat zien dat `niet-admin-aanmeldingen op switch` voor deze gebruikers `worden geweigerd`.

Valideer het AV-paar dat is ontvangen door te **nginx.bin.log**controleren. Filter op de gebruikersnaam om de volledige rol-injectiestroom te zien:

<#root>

```
apic1#

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

Voor TACACS+ wordt het AV-paar geregistreerd als `TACACS+ Cisco-avpair (shell: domains=...)`. Een succesvolle injectie toont dat `de injectie van de externe gebruiker <gebruikersnaam> is voltooid` gevolgd door `Found UserDomain` en `admin write privileges` lijnen (zie de LDAP Operational Verification sectie voor volledige voorbeelden van deze stroom met echte log output).

Als de AV-paarindeling ongeldig is, wordt in het logboek `Injection of remote user <username> data FAILED` weergegeven `- foutbericht is Invalid shell:domains string`. Als de gebruiker zich verifieert met een niet-beheerdersrol, wordt SSH aan switches geweigerd met `niet-beheerdersaanmeldingen op switch .`

Hoofdoorzaak: gedeelde geheime mismatch, server onbereikbaar vanaf het beheernetwerk, gebruiker bestaat niet op de TACACS+-server of de beheer-EPG op de provider is onjuist.

Oplossing: Corrigeer het gedeelde geheim, los bereikbaarheid op of maak de gebruiker aan op de TACACS+-server.

Verificatielogs van Leaf Switch valideren

Op blad- en ruggengraat switches worden SSH-inloggebeurtenissen zowel **pam.module.log** als **nginx.log**geregistreerd. Het **pam.module.log** resultaat van de PAM-verificatie wordt weergegeven (accepteren of weigeren). De **nginx.log** volledige AAA-stroom bevat de volledige AAA-stroom - realm selectie, provider lookup, LDAP / TACACS + / RADIUS-communicatie, AV-paarparsing en roltoewijzing - identiek aan **nginx.bin.log** op de APIC. Deze logs zijn van toepassing op alle externe AAA-typen (TACACS+, RADIUS, LDAP).

Controleer **pam.module.log** op het verificatieresultaat:

<#root>

```
leaf101#

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

Werken — verificatie op afstand op de 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
```

De vlag **remote=1** bevestigt dat de gebruiker is geverifieerd door een externe AAA-server.

Werkt niet — de gebruiker is afgewezen. De securityGrAG ontkent de gebruiker en de switch probeert een lokale gebruiker op te zoeken als een laatste terugvalmogelijkheid:

```
||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
```

Als er helemaal geen PAM-items verschijnen voor de gebruiker, is de SSH-verbinding waarschijnlijk afgewezen voordat de PAM-fase werd bereikt (bijvoorbeeld vanwege een coderingsmismatch of de gebruiker die de verbinding annuleert).

Voor een meer gedetailleerde weergave van de verificatiestroom op de switch, **nginx.log**controleert u. Dit logboek bevat de volledige AAA-beslissingsketen — hetzelfde formaat en dezelfde berichten als **nginx.bin.log** op de APIC:

<#root>

```
leaf101#
```

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

Werken — geslaagde LDAP-verificatie op een switch (vergelijk de APIC LDAP-voorbeelden in de sectie LDAP Operational Verification — de berichten zijn hetzelfde):

```
||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
```

De switch **nginx.log** is vooral handig wanneer **pam.module.log** een afwijzing wordt weergegeven, maar niet wordt uitgelegd waarom. De nginx.log onthult het AAA-domein, de provider en de specifieke storingsreden (bijvoorbeeld LDAP-zoekopdracht leeg geretourneerd, TACACS + time-out of AV-paarinjectie mislukt).

Problemen met AAA oplossen — RADIUS

Dit gedeelte behandelt RADIUS-verificatiefouten. De APIC communiceert met de RADIUS-server via UDP-poort 1812 (verificatie) en optioneel UDP-poort 1813 (boekhouding).

operationele verificatie

ACI-switches ondersteunen de **test aaa** opdracht die beschikbaar is op standalone NX-OS niet. Gebruik de volgende methoden om de werking van RADIUS te controleren.

Verifieer de RADIUS-serverconfiguratie en bereikbaarheidsstatistieken van een leaf-switch:

<#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
```

Scenario: RADIUS-verificatie mislukt

Probleem: aanmelden mislukt wanneer een gebruiker een RADIUS-aanmeldingsdomein selecteert.

Verificatiestappen:

1. Controleer RADIUS-serverstatistieken van een switch op tekenen van time-outs of storingen:

   <#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
   ```

   Een hoog aantal onder verzoeken met time-out geeft aan dat de RADIUS-server onbereikbaar is of dat het gedeelde geheim niet overeenkomt (RADIUS laat stilletjes pakketten vallen op gedeelde geheime mismatch).

2. De netwerkbereikbaarheid van de RADIUS-server controleren:
   <#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. Controleer de gedeelde geheime overeenkomsten tussen de APIC- en de RADIUS-server. In tegenstelling tot TACACS+, dat TCP gebruikt en verbindingsfouten rapporteert, gebruikt RADIUS UDP en laat het stilletjes pakketten vallen wanneer het gedeelde geheim niet overeenkomt. Het enige symptoom is een time-out.
4. Controleer de RADIUS-serverlogs. FreeRADIUS in debug mode (**radiusd -X**) toont elk verzoek en geeft aan of het werd geaccepteerd, afgewezen of een gedeelde geheime mismatch had.
5. Controleer de APIC **nginx.bin.log** voor de RADIUS-verificatiestroom. Filter op de gebruikersnaam:
   <#root>

   ```
   apic1#
   ```

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

RADIUS-aanmeldingen volgen dezelfde **nginx.bin.log** verificatiestroom als LDAP en TACACS+ (zie de sectie LDAP Operational Verification voor volledige voorbeelden van echte logbestanden). De belangrijkste verschillen voor RADIUS zijn:

- `Als u RadiusProvider <IP> aan de lijst toevoegt`, wordt de RADIUS-server geïdentificeerd (tegenover `TacacsProvider` of `LdapProvider`).
- Realm number voor RADIUS verschilt per configuratie.

Een succesvolle RADIUS-aanmelding eindigt met `Injectie van externe gebruiker ... is voltooid` en `beheerdersschrijfbevoegdheden`.

Een mislukte RADIUS-aanmelding eindigt met `werd geweigerd tijdens AAA-verificatie` en `GEWEIGERD`.

Als er geen RADIUS-specifieke berichten worden weergegeven na de regel `Adding RadiusProvider`, wordt de server getimed. In tegenstelling tot TACACS+, dat TCP gebruikt en verbindingsfouten rapporteert, gebruikt RADIUS UDP en laat het stilletjes pakketten vallen wanneer het gedeelde geheim niet overeenkomt. Het enige symptoom is een time-out gevolgd door ontkenning.

6. Controleer op actieve fouten bij de RADIUS-provider:
<#root>

apic1#

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

RADIUS cisco-av-pair voor RBAC

RADIUS gebruikt hetzelfde **cisco-av-pair** attribuut als TACACS+ voor RBAC-roltoewijzing. De RADIUS-server moet dit attribuut teruggeven in het Access-Accept-antwoord:

<#root>

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

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

In FreeRADIUS wordt dit geconfigureerd in het **users** bestand of de LDAP-backend. Voor ISE wordt

het onder het Autorisatieprofiel geconfigureerd als een geavanceerd attribuut.

Hoofdoorzaak: Gedeelde geheime mismatch (meest voorkomend bij RADIUS - veroorzaakt stille time-outs), server onbereikbaar, onjuiste auth-poort of ontbrekend gebruikersaccount op de RADIUS-server.

Oplossing: Corrigeer het gedeelde geheim, controleer de bereikbaarheid van UDP 1812 of configureer de gebruiker op de RADIUS-server.

Problemen met AAA oplossen — LDAP

Dit gedeelte behandelt LDAP-verificatiefouten. De APIC maakt verbinding met de LDAP-server via TCP-poort 389 (LDAP) of TCP-poort 636 (LDAPS met SSL).

operationele verificatie

ACI-switches ondersteunen de **test aaa** opdracht die beschikbaar is op standalone NX-OS niet. Om de werking van de LDAP te controleren, controleert u de fouten en configuratie van de provider in de APIC.

Controleer op actieve fouten bij de LDAP-provider:

<#root>

apic1#

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

Fout F1777 duidt op een connectiviteitsprobleem. Fout F1778 duidt op een verificatie- of bindfout. Als er geen fouten worden geretourneerd, beschouwt de APIC de provider als bereikbaar.

Verifieer de bereikbaarheid van het basisnetwerk voor de LDAP-server:

<#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
```

Controleer voor LDAP ook de TCP-connectiviteit met poort 389 (of 636 voor LDAPS). Als de APIC de server kan pingen, maar LDAP-fouten blijven bestaan, is het probleem meestal een onjuist bindend DN, een verkeerd wachtwoord of een firewall die de LDAP-poort blokkeert.

De LDAP-verificatiestroom valideren in de APIC-logs. Filter op de gebruikersnaam:

<#root>

```
apic1#
```

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

Werken — Een succesvolle LDAP-aanmelding toont de volledige toewijzingsstroom voor zoeken, binden en rollen:

```
||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
```

Niet-werkend — gebruiker niet gevonden in de LDAP-directory (zoekopdracht retourneert lege set):

```
||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
```

Scenario: LDAP-verificatie mislukt

Probleem: aanmelden mislukt wanneer een gebruiker een LDAP-aanmeldingsdomein selecteert.

Verificatiestappen:

1. Controleer de bereikbaarheid van de LDAP-server vanuit de 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. Controleren op fouten van actieve LDAP-provider:
   <#root>

   ```
   apic1#

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

3. Controleer de configuratie van de LDAP-provider:
   <#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. Controleer of de gebruiker in de LDAP-directory onder de geconfigureerde basis-DN staat en overeenkomt met het filter. Voor Active Directory moet het **sAMAccountName** kenmerk van de gebruiker overeenkomen met de gebruikersnaam die is ingevoerd bij de aanmelding. Voor OpenLDAP moet het **cn** of **uid** attribuut overeenkomen.
5. Als u LDAPS (poort 636) gebruikt, controleert u de SSL-certificaatketen. Als **SSLValidationLevel** is ingesteld op strict, zal de APIC de verbinding weigeren als het servercertificaat niet wordt vertrouwd of is verlopen.
6. Controleer de APIC **nginx.bin.log** voor de volledige LDAP-verificatiestroom. Filter op de gebruikersnaam zodat tussenliggende berichten niet worden gemist:
   <#root>

   ```
   apic1#

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

Vergelijk de output met de werkende en niet-werkende voorbeelden in de sectie Operationele verificatie hierboven. Extra LDAP-specifieke faalpatronen zijn te vinden door het logboek in grote lijnen te doorzoeken:

<#root>

apic1#

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

Gemeenschappelijke niet-werkende patronen (vergelijk met de bovenstaande operationele verificatievoorbeelden voor de volledige stroom):

```
! 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
```

Andere LDAP-faalpatronen om te zoeken naar:

- Time-out LDAP-zoekopdracht (server onbereikbaar, traag of firewall blokkerende poort 389/636) — zoeken naar `Ldap Zoeken mislukt: retourcode voor ldap_search_ext_s: -5: Time-out`
- Binden is mislukt (wachtwoord voor rootdn of binding is onjuist of de server heeft de verbinding geweigerd) — zoeken naar `Ldap Search is mislukt: retourcode voor ldap_search_ext_s: -1: Kan geen contact opnemen met LDAP-server`
- Gebruiker gevonden maar wachtwoord is fout (binding met gebruikerswachtwoord mislukt) — het logboek toont de `LDAP Record DN-`regel, maar wordt gevolgd door een geweigerd bericht zonder `binding aan UserDN ... succesvolle` regel.

LDAP Group Map voor RBAC

LDAP gebruikt groepskaarten in plaats van het **cisco-av-pair** attribuut. Het veld van de LDAP-provider **attribute** geeft aan welk LDAP-kenmerk de groepsgegevens bevat. Voor Active Directory is dit doorgaans **memberOf**ongebruikelijk.

De APIC koppelt het geretourneerde groep-DN aan de geconfigureerde LDAP Group Map Rules (**aaaLdapGroupMapRule**LDAP Group Map Rules) om het juiste beveiligingsdomein en de juiste rol toe te wijzen. Als er geen groepskaartregel overeenkomt, wordt de gebruiker geverifieerd, maar heeft

deze geen rollen.

U kunt de **attribute** waarde ook instellen op **CiscoAVPair shell:domains=all/admin/** en direct opslaan in de LDAP-kenmerken van de gebruiker, die hetzelfde formaat hebben als TACACS+ en RADIUS.

Oorzaak van hoofdmap: Onjuist bindend DN of wachtwoord, basis-DN bevat de gebruiker niet, zoekfilter komt niet overeen met het directoryschema, LDAPS-certificaatvalidatiefout of ontbrekende regels voor groepskaarten.

Oplossing: Corrigeer de configuratie van de provider (verbind DN, basis DN, filter, SSL-instellingen). Controleer voor RBAC-problemen of de regels voor groepskaarten overeenkomen met de LDAP-groepen waartoe de gebruiker behoort.

Problemen met RBAC en gebruikersrechten oplossen

Dit gedeelte behandelt scenario's waarbij de gebruiker met succes authenticeert, maar niet het verwachte toegangsniveau heeft.

Scenario: Gebruiker ingelogd maar ziet geen huurders

Probleem: een externe gebruiker meldt zich aan via TACACS+, RADIUS of LDAP. De login slaagt, maar de gebruiker ziet geen huurders in de gebruikersinterface en API-oproepen retourneren lege resultaten of "403 Verboden".

Verificatiestappen:

1. Controleer de sessie van de gebruiker om te zien welke rollen zijn toegewezen bij aanmelding:
   <#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
   ```

   Het **descr** veld toont het aanmeldingsresultaat. Als de gebruiker zich succesvol heeft geverifieerd maar geen RBAC-rollen heeft, heeft de AAA-server geen geldige **cisco-av-pair** of LDAP-groepstoewijzing geretourneerd.

2. Controleer de APIC **nginx.bin.log** om het AV-paar en de roltoewijzing te zien tijdens de aanmelding. Filter op de gebruikersnaam:
<#root>

```
apic1#
```

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

Zoek naar de berichten voor rolinjectie en domeintoewijzing:

Werken — AV-paar geconverteerd van LDAP-groepskaart, gebruiker krijgt beheerdersrol:

```
||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
```

Niet werken — als een **Cisco-avpair** of een **Converted to CiscoAVPair** regel niet in de stroom wordt weergegeven, heeft de AAA-server het kenmerk niet geretourneerd en is er geen LDAP-groepkaartregel gekoppeld. Zoek naar **Checking all UserDomains** zonder **Found UserDomain** regels erna - de gebruiker is geverifieerd maar heeft geen roltoewijzingen. Als er een **Injection ... data FAILED** bericht verschijnt, is de tekenreeksindeling van het AV-paar ongeldig.

3. Controleer of de AAA-server het **cisco-av-pair** kenmerk (voor TACACS+ of RADIUS) of het juiste LDAP-groepslidmaatschap (voor LDAP) retourneert. Controleer de configuratie van de AAA-server:
    - TACACS+: Controleer het gebruikersprofiel dat wordt opgenomen **cisco-av-pair** met de **shell:domains=all/admin/**indeling.
    - RADIUS: Controleer of het gebruikersprofiel terugkeert **Cisco-AVPair = "shell:domains=all/admin/"** in Access-Accept.
    - LDAP: Controleer of de gebruiker lid is van een LDAP-groep die overeenkomt met een geconfigureerde LDAP Group Map Rule (**aaaLdapGroupMapRule**LDAP).
4. Als het attribuut aanwezig is, maar de gebruiker nog steeds geen toegang heeft, controleert u of de domeinnaam voor de beveiliging in het attribuut overeenkomt met een bestaand beveiligingsdomein op de APIC:
<#root>

```
apic1#
```

```
moquery -c aaaDomain
```

Als de verwijzing **cisco-av-pair** verwijst naar een domein dat niet bestaat (bijvoorbeeld **shell:domains=NonExistentDomain/admin/**), mislukt de roltoewijzing stilletjes.

Hoofdoorzaak: de AAA-server retourneert de toewijzingskenmerken van de RBAC niet, de attribuutindeling is onjuist of het beveiligingsdomein waarnaar in het kenmerk wordt verwezen, bestaat niet op de APIC.

Oplossing: Configureer de AAA-server om de juiste **cisco-av-pair** toewijzing of groepstoewijzing te retourneren. Controleer of het beveiligingsdomein bestaat op de APIC.

Scenario: de gebruiker kan de configuratie wel bekijken, maar niet wijzigen

Probleem: een gebruiker kan zich aanmelden en door objecten bladeren, maar krijgt een fout wanneer hij probeert wijzigingen in te dienen.

Verificatiestappen:

1. Controleer de roltoewijzingen van de gebruiker:
   <#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. Als de gebruiker schrijftoegang nodig heeft, moet de rol **writePriv**verlenen. Veel voorkomende rollen met schrijfbevoegdheden zijn admin, tenant-admin, access-admin en fabric-admin.
3. De roltoewijzing valideren in de APIC-logs. Filter op de gebruikersnaam:
   <#root>

   ```
   apic1#

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

   Zoek naar de berichten voor roltoewijzing aan het einde van de verificatiestroom:

   Werken — gebruiker heeft de rol van beheerder schrijven (van een echte LDAP-login):

   ```
   ||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
   ```

   Niet werken — als het logboek `niet-admin UserRole` toont met `leesbevoegdheden` in plaats van `schrijfbevoegdheden voor beheerders`, heeft de gebruiker een alleen-lezen rol en kan de

configuratie niet wijzigen. Zoek naar lijnen zoals:

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

Als in het log alleen `leesbevoegdheden` en geen `schrijfbevoegdheden worden` weergegeven, werkt u de rol of het AV-paar van de gebruiker op de AAA-server bij.

Hoofdoorzaak: de gebruiker heeft een alleen-lezen rol (bijvoorbeeld alles-lezen of ops) in plaats van een schrijfbare rol.

Oplossing: Werk de roltoewijzing van de gebruiker op de APIC bij (voor lokale gebruikers) of werk de functies op de AAA-server bij (voor externe gebruikers) om een rol met schrijfbevoegdheden op te nemen. **cisco-av-pair.**

Scenario: Gebruiker heeft toegang tot sommige huurders, maar niet tot andere

Probleem: een gebruiker kan één tenant zien en beheren, maar kan andere huurders niet zien, ook al hebben ze toegang nodig.

Verificatiestappen:

1. Controleer de toewijzing van het beveiligingsdomein van de gebruiker:
   <#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. Beveiligingsdomeinen worden toegewezen aan huurders. Als de gebruiker toegang nodig heeft tot TenantB, moet deze ook worden toegewezen aan het beveiligingsdomein dat is gekoppeld aan TenantB of aan het volledige domein.
3. Bevestig voor externe gebruikers dat het AV-paar of de LDAP-groepskaart de juiste domeinen toewijst. Controleer de APIC **nginx.bin.log** voor de domeintoewijzing bij aanmelding. Filter op de gebruikersnaam:
   <#root>

   ```
   apic1#

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

Werken — de gebruiker heeft alle domeinen (volledige zichtbaarheid), via een echte LDAP-login:

```
||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
```

Niet werken — als de gebruiker slechts één tenant-domein heeft, wordt alleen dat domein weergegeven in de **Found UserDomain** berichten in plaats van alle. Bijvoorbeeld, `Gevonden UserDomain TenantA` betekent dat de gebruiker alleen kan zien TenantA. De gebruiker heeft extra domeinen nodig die zijn toegevoegd aan het AV-paar op de AAA-server of het All Domain voor volledige toegang.

Hoofdoorzaak: de gebruiker wordt toegewezen aan een beperkt beveiligingsdomein dat alleen betrekking heeft op specifieke huurders.

Oplossing: voeg de vereiste beveiligingsdomeinen toe aan de configuratie van de gebruiker of gebruik het all domain voor volledige toegang.

Wachtwoordherstel en noodtoegang

Als alle beheerdersaccounts zijn vergrendeld of als de externe AAA-server onbereikbaar is en het standaarddomein is gewijzigd, gebruikt u een van de volgende herstelmethoden:

Fallback-aanmeldingsdomein

ACI biedt een ingebouwd fallback-aanmeldingsdomein dat altijd lokale verificatie gebruikt, ongeacht het standaardverificatieniveau. Om het te gebruiken:

- SSH: Log in als **apic:fallback\\admin** (of **apic#fallback\\admin** afhankelijk van de versie).
- GUI: Selecteer in de vervolgkeuzelijst Domein op het aanmeldingsscherm de optie Fallback en gebruik lokale referenties.

Consoletoegang

Als het Console Authentication Realm is ingesteld op lokaal (standaard), kunt u altijd inloggen via de APIC-consolepoort met lokale referenties. Als het wachtwoord van de lokale beheerder niet

bekend is, kan het wachtwoord opnieuw worden ingesteld via de Cisco Integrated Management Controller (CIMC) (voor fysieke APIC's) of de hypervisorconsole (voor virtuele APIC's).

Opmerking: als het consoleverificatierealum is gewijzigd in een externe AAA-server en deze server niet bereikbaar is, wordt ook de consoletoegang geblokkeerd. Dit is een algemeen uitsluitingsscenario. Zorg ervoor dat het Console Authentication Realm altijd is ingesteld op lokaal.

Common Faults-verwijzing

De volgende ACI-fouten worden vaak geassocieerd met externe toegang en AAA-problemen:

- F1773 — Probleem met connectiviteit van TACACS+-provider. De APIC kan de TACACS+-server niet bereiken.
- F1774 — Tacacs+-verificatiefout. De server is bereikbaar, maar de verificatiepoging is afgewezen.
- F1775 — Probleem met connectiviteit van RADIUS-provider.
- F1776 — RADIUS-verificatiefout.
- F1777 — Probleem met connectiviteit van LDAP-provider.
- F1778 — LDAP-verificatiefout.
- F0532 — Beheersubnet niet geconfigureerd voor een node.

Actieve AAA-fouten opvragen:

<#root>

```
apic1#

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

Referenties

- Problemen met ACI-beheer en kernservices oplossen — POD-beleid
- Cisco APIC Basic Configuration Guide, versie 6.1(x) — Beheer
- Cisco APIC Security Configuration Guide — Toegang, verificatie en boekhouding

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.