Fehlerbehebung bei Remote-Zugriffsproblemen in einer ACI-Fabric

Einleitung

In diesem Dokument wird beschrieben, wie Probleme mit dem Remote-Zugriff in einer Cisco Application Centric Infrastructure (ACI)-Fabric überprüft, behoben und behoben werden können. Es umfasst Secure Shell (SSH)- und Hypertext Transfer Protocol Secure (HTTPS)-Zugriff auf APICs und Fabric Switches, Remote Authentication, Authorization and Accounting (AAA) mit Terminal Access Controller Access-Control System Plus (TACACS+), Remote Authentication Dial-In User Service (RADIUS) und Lightweight Directory Access Protocol (LDAP) sowie rollenbasierte Zugriffskontrolle (RBAC). Für jeden Bereich stehen ein Entscheidungsablauf und detaillierte Fehlerbehebungsszenarien zur Verfügung.

Hintergrundinformationen

Das Material aus diesem Dokument wurde aus dem Leitfaden zur Fehlerbehebung für ACI-Management und Core-Services - Pod-Richtlinien, dem Cisco APIC Basic-Konfigurationsleitfaden, dem Kapitel 6.1(x) - Management und dem Kapitel Cisco APIC Security Configuration Guide - Access, Authentication, and Accounting (Zugriff, Authentifizierung und Abrechnung) zusammengesetzt.

Überblick

Der Remote-Zugriff auf eine ACI-Fabric umfasst drei verschiedene Ebenen, die jeweils von einem Techniker ausgeführt werden müssen, damit er sich erfolgreich anmelden und betreiben kann:

1. Transport - Der Managementnetzwerkpfad (OOB oder In-Band) und der Protokolldienst (SSH oder HTTPS) müssen erreichbar und aktiviert sein.
2. Authentifizierung - Die Anmeldeinformationen des Benutzers müssen entweder lokal auf dem APIC oder auf einem AAA-Remote-Server (TACACS+, RADIUS oder LDAP) validiert werden.
3. Autorisierung: Dem authentifizierten Benutzer müssen die richtigen RBAC-Rollen und Sicherheitsdomänen zugewiesen werden, um die beabsichtigten ACI-Objekte anzeigen und ändern zu können.

Ein Ausfall auf einer Ebene verursacht verschiedene Symptome. Ein Transportfehler verhindert die Verbindung vollständig. Bei einem Authentifizierungsfehler wird ein Fehler mit den Anmeldeinformationen zurückgegeben. Ein Autorisierungsfehler ermöglicht die Anmeldung, schränkt jedoch die Transparenz ein oder erzeugt "403 Forbidden"-Fehler in der API.

Management-Zugriffsrichtlinie

Die Management Access Policy (**commPol**) ist das zentrale Objekt, das steuert, welche Remote-Zugriffsprotokolle in der Fabric aktiviert sind. Sie finden sie unter Fabric > Fabric Policies > Policies > Pod > Management Access > default. Die Richtlinie enthält untergeordnete Objekte, die Folgendes konfigurieren:

- SSH (**commSsh**): Verwaltungsstatus, Port, Chiffren, KEX-Algorithmen (Key Exchange), MACs (Message Authentication Codes) und Host-Schlüsselalgorithmen.
- HTTPS (**commHttps**): Verwaltungsstatus, Port, TLS-Protokollversion (Transport Layer Security), Drosselungsrate und Client-Zertifikatauthentifizierung.
- Telnet (**commTelnet**) - Verwaltungsstatus und Port Telnet ist standardmäßig deaktiviert, und Cisco empfiehlt, es zu deaktivieren.

OOB- und In-Band-Management

ACI-Knoten unterstützen zwei Management-Zugriffspfade:

- Out-of-Band (OOB): Verwendet den dedizierten Management-Port des APIC oder Switches. OOB-Managementadressen werden aus einem Pool unter dem mgmt-Tenant zugewiesen und über **mgmtRsOoBStNode**den Knoten zugewiesen. Auf dem APIC werden OOB-Verträge durch **iptables** Regeln durchgesetzt. Wenn ein OOB-Vertrag angewendet wird, kann nur der laut Vertrag zulässige Datenverkehr die APIC-Management-Schnittstelle erreichen.
- In-Band (INB) - Nutzt die Fabric-Datenebene für den Management-Datenverkehr. Für die In-Band-Verwaltung ist eine Adresszuweisung für Bridge-Domäne (BD), Subnetz, Endpunktgruppe (EPG), Vertrag und Knotenverwaltung erforderlich. In-Band-IP-Adressen können nicht von außerhalb der Fabric erreicht werden, ohne dass zusätzliches Routing oder eine Richtlinienkonfiguration erforderlich sind.

Anmerkung: Die OOB-Management-IPs des APIC werden bei der Ersteinrichtung konfiguriert, und der APIC erhält die IP-Verbindung, bevor die Fabric vollständig erkannt wird. OOB ist der primäre Management-Pfad und immer verfügbar, wenn das physische Management-Netzwerk verbunden ist.

AAA-Architektur

Die ACI verwendet ein dreistufiges AAA-Modell:

1. Login Domain (**aaaLoginDomain**) (Anmeldungsdomäne): Gruppiert AAA-Anbieter unter einem benannten Bereich. Benutzer geben die Anmelde-Domäne im Anmeldebildschirm an (z. B. `apic:TACACS-Domain` oder über das Dropdown-Menü in der Benutzeroberfläche). Eine spezielle Fallback-Anmeldungsdomäne ist immer vorhanden und wird der lokalen Authentifizierung zugeordnet.
2. Anbietergruppe (**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**, **aaaLdapProviderGroup**): Bezieht sich auf einen oder mehrere AAA-Server und legt die Reihenfolge fest, in der versucht wird, diese Server zu verwenden.
3. Provider (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**): Definiert die Server-IP, den Port, den gemeinsamen geheimen Schlüssel (oder die DN-Anbindung für LDAP), die Zeitüberschreitung, Wiederholungsversuche, die Verwaltungs-EPG und die Anmeldeinformationen für die Überwachung.

Der Standard-Authentifizierungsbereich (**aaaDefaultAuth**) bestimmt, welche Anmelde-Domäne verwendet wird, wenn der Benutzer bei der Anmeldung keine Domäne angibt. Der Konsolenauthentifizierungsbereich steuert die Authentifizierung für Konsolensitzungen.

Anmerkung: Wenn Sie den Standard-Authentifizierungsbereich in einen Remote-AAA-Server ändern, während der Server nicht erreichbar ist, werden Sie aus der Fabric ausgeschlossen. Testen Sie immer die AAA-Serverkonnektivität, bevor Sie den Bereich ändern. Die Fallback-Anmeldedomäne (`apic:fallback\\admin`) kann verwendet werden, um den Standardbereich zu umgehen und sich lokal zu authentifizieren.

Wichtige AAA-Protokolldateien

AAA-Authentifizierungsereignisse werden in mehreren Dateien auf dem APIC und auf den Fabric-Switches protokolliert. Diese Protokolle sind das primäre Tool für die Validierung von Authentifizierungsergebnissen, die Identifizierung des Bereichs und der Anbietergruppe, die verwendet werden, und die Diagnose von Fehlern bei der Rollenzuweisung.

Protokolldatei	Standort (APIC)	Standort (Switches)	Be
nginx.bin.log (APIC) nginx.log (Switches)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	Primäres Beinhalte vollständi Authentifi PAM-Anfr Bereichsa Anbieters /TACACS Kommuni Parsing,

Protokolldatei	Standort (APIC)	Standort (Switches)	Be
			Rollenzuv Erfolgs- o Ablehnun Dateinam sich zwis Plattform Content-F gleiche.
access.log	/var/log/dme/log/access.log	/var/log/dme/log/access.log	NGINX H Anforderu Eine Leitu Anfrage. APIC aaa aaaRefres HTTP-Sta (200 = Er abgelehn Switches API-Anfo aaaRefres
pam.module.log	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	PAM-Mod das Authentifi für SSH-S authentifiz Quell-IP u UNIX-Ber Switches schnellste bestätige Benutzer oder abge

Anmerkung: Das primäre AAA-Protokoll hat auf jeder Plattform einen anderen Dateinamen. Auf dem APIC: **nginx.bin.log** /var/log/dme/log. Auf Leaf- und Spine-Switches ist dies **nginx.log** /var/sysmgr/tmp_logs/dme_logs/. Das Format des Protokollinhalts und die AAA-Meldungen sind auf beiden Plattformen identisch.

AAA-Einträge im nginx-Protokoll haben folgendes Format:

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

AAA-bezogene Protokolleinträge für den Authentifizierungsablauf eines bestimmten Benutzers filtern:

<#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
```

Oder zeigen Sie alle aktuellen Authentifizierungsanforderungen und -ergebnisse an:

<#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
```

Ein typischer erfolgreicher Authentifizierungsablauf zeigt die folgenden Schlüsselnachrichten der Reihe nach an:

1. `PAM-Authentifizierungsanforderung von nginx für Benutzername empfangen: <Benutzer>` — die Anmeldeanfrage wurde empfangen.
2. `DefaultAuthMo gibt den Bereich <N> an. Provider Group <Name> !` — der Bereich wurde ausgewählt (0=fallback/local, 2=TACACS+, 3=LDAP).
3. Anbieterspezifische Nachrichten (LDAP-Anbindung, TACACS+-Anbietersuche oder RADIUS-Anforderung).
4. `UserDomain <Domäne> unter Remote-Benutzername gefunden: <user>` - die Domänenzuweisung aus der AAA-Antwort.
5. `Gefundener Benutzername: admin mit admin-Schreibberechtigungen unter UserDomain all - Benutzer ist ein admin-Benutzer` - die Rollenüberprüfung wurde bestanden.

Fehlgeschlagene Authentifizierungsprotokolle:

- `Benutzer <user> wurde bei der AAA-Authentifizierung abgelehnt`
- `Fehler bei nicht autorisiertem Benutzer <user>: AAA-Serverauthentifizierung ABGELEHNT`

Anmerkung: Das nginx-Protokoll rotiert häufig und ältere Einträge werden mit einem numerischen Suffix gzip komprimiert. Auf dem APIC befinden sich die rotierten Protokolle im gleichen Verzeichnis (z. B. **nginx.bin.log.22815.gz**). Auf Switches werden die rotierten Protokolle unter gespeichert **/var/log/dme/oldlog/dme/nginx.log.*.gz** (mit Symlinks in `/var/sysmgr/tmp_logs/dme_logs/`). So durchsuchen Sie gedrehte Protokolle:

<#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-Modell

ACI RBAC steuert, was authentifizierte Benutzer sehen und tun können. Das Modell besteht aus drei Komponenten:

- Sicherheitsdomäne (**aaaDomain**): Eine Bereichsbeschränkung, die ACI-Objekten (Tenants, Zugriffsrichtlinien, Fabric-Richtlinien) zugeordnet ist. Die integrierten Domänen all, common und mgmt sind immer vorhanden. Benutzerdefinierte Domänen schränken die Transparenz eines Benutzers auf bestimmte Tenants oder Richtlinienbereiche ein.
- Rolle (**aaaRole**): Definiert eine Reihe von Berechtigungen. Zu den vordefinierten Rollen gehören admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops und nw-svc-admin.
- Berechtigung - Jede Rolle gewährt entweder Lese- oder Schreibzugriff (was Lese- und Schreibzugriff bedeutet) auf einen bestimmten Funktionsbereich.

Einem Benutzerkonto wird ein oder mehrere Sicherheitsdomänen- und Rollenpaare zugewiesen. Bei Remote-Benutzern, die über TACACS+, RADIUS oder LDAP authentifiziert wurden, erfolgt die Rollenzuordnung über anbieterspezifische Attribute in der AAA-Antwort (z. B. das **cisco-av-pair**

Attribut).

Entscheidungsablauf der Triage

Verwenden Sie diesen Entscheidungsbaum, wenn ein Benutzer berichtet, dass er nicht per Fernzugriff auf die ACI-Fabric zugreifen kann:

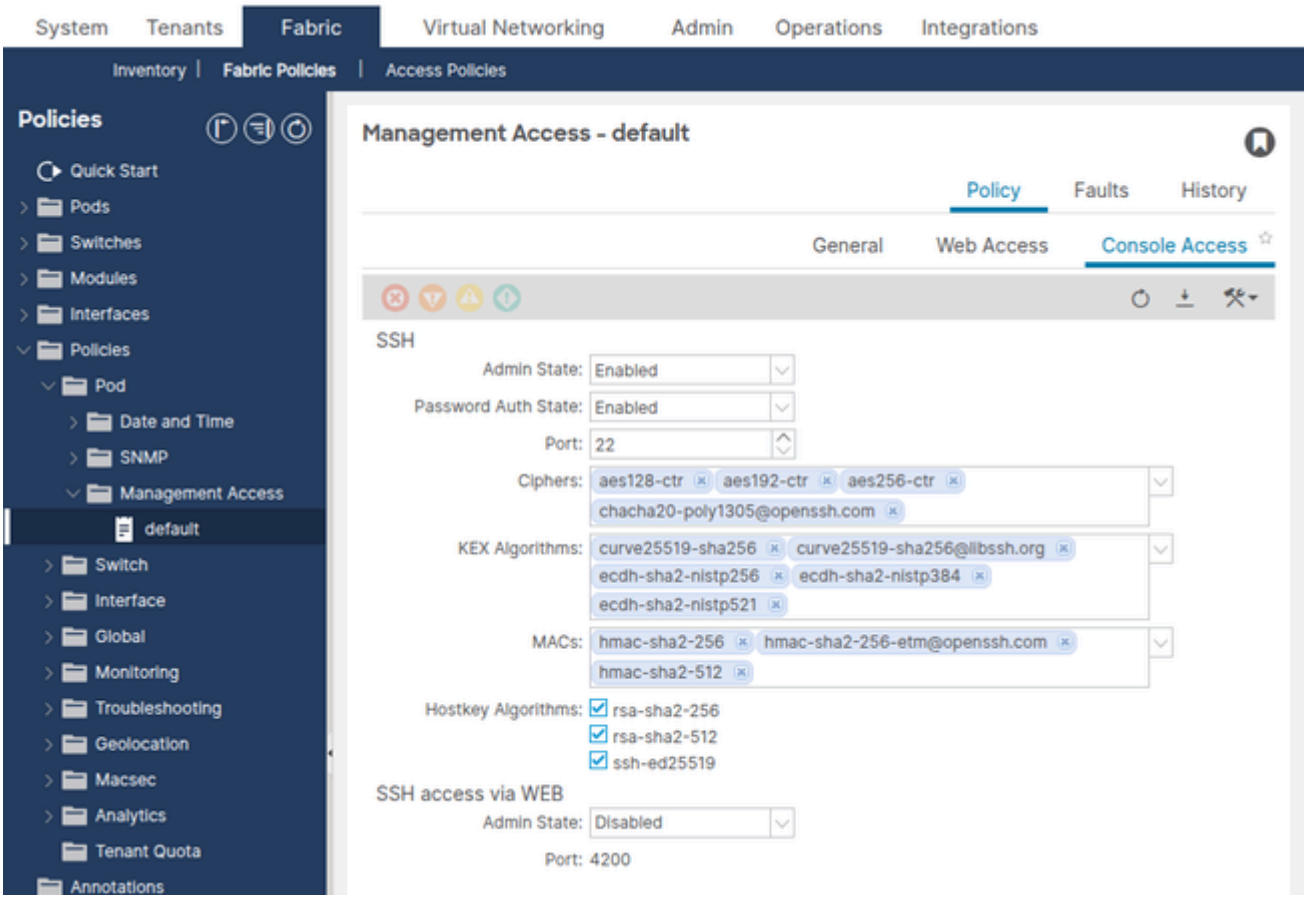
1. Können Sie den APIC oder die Management-IP-Adresse des Switches pingen?
    - Nein → Fehlerbehebung beim Management-Netzwerkpfad. Weitere Informationen finden Sie im Abschnitt "Fehlerbehebung bei OOB und In-Band-Management".
    - Ja → Weiter.
2. Können Sie eine SSH- oder HTTPS-Verbindung herstellen (öffnet sich die Verbindung überhaupt)?
    - Nein → Der Protokolldienst kann deaktiviert, der Port kann gefiltert werden, oder es kann eine Cipher-Fehlanpassung vorliegen. Lesen Sie die Abschnitte "Fehlerbehebung bei SSH-Zugriff" oder "Fehlerbehebung bei HTTPS-Zugriff".
    - Ja → Weiter.
3. Wird der Anmeldebildschirm angezeigt (HTTPS), oder ist der SSH-Handshake abgeschlossen, und werden die Anmeldeinformationen angefordert?
    - Kein → SSH-Schlüsselaustausch oder TLS-Handshake-Fehler. Informationen zu Cipher- und KEX-Diskrepanzen finden Sie im Abschnitt "Fehlerbehebung bei SSH-Zugriff".
    - Ja → Weiter.
4. Schlägen die Anmeldedaten bei "Authentifizierung fehlgeschlagen" oder ähnlichem fehl?
    - Ja → Authentifizierungsproblem. Lesen Sie die Abschnitte "Fehlerbehebung bei AAA-Authentifizierung" (TACACS+, RADIUS oder LDAP, je nach verwendeter Anmeldedomäne).
    - Nein → Weiter.
5. Meldet sich der Benutzer an, kann aber die erwarteten Objekte nicht sehen, oder erhält er die Fehlermeldung "403 Forbidden"?
    - Ja → Autorisierung oder RBAC-Problem. Weitere Informationen finden Sie im Abschnitt "Fehlerbehebung bei RBAC und Benutzerberechtigungen".
    - Nein → Der Zugriff funktioniert. Überprüfen Sie das spezifische Problem des Benutzers.

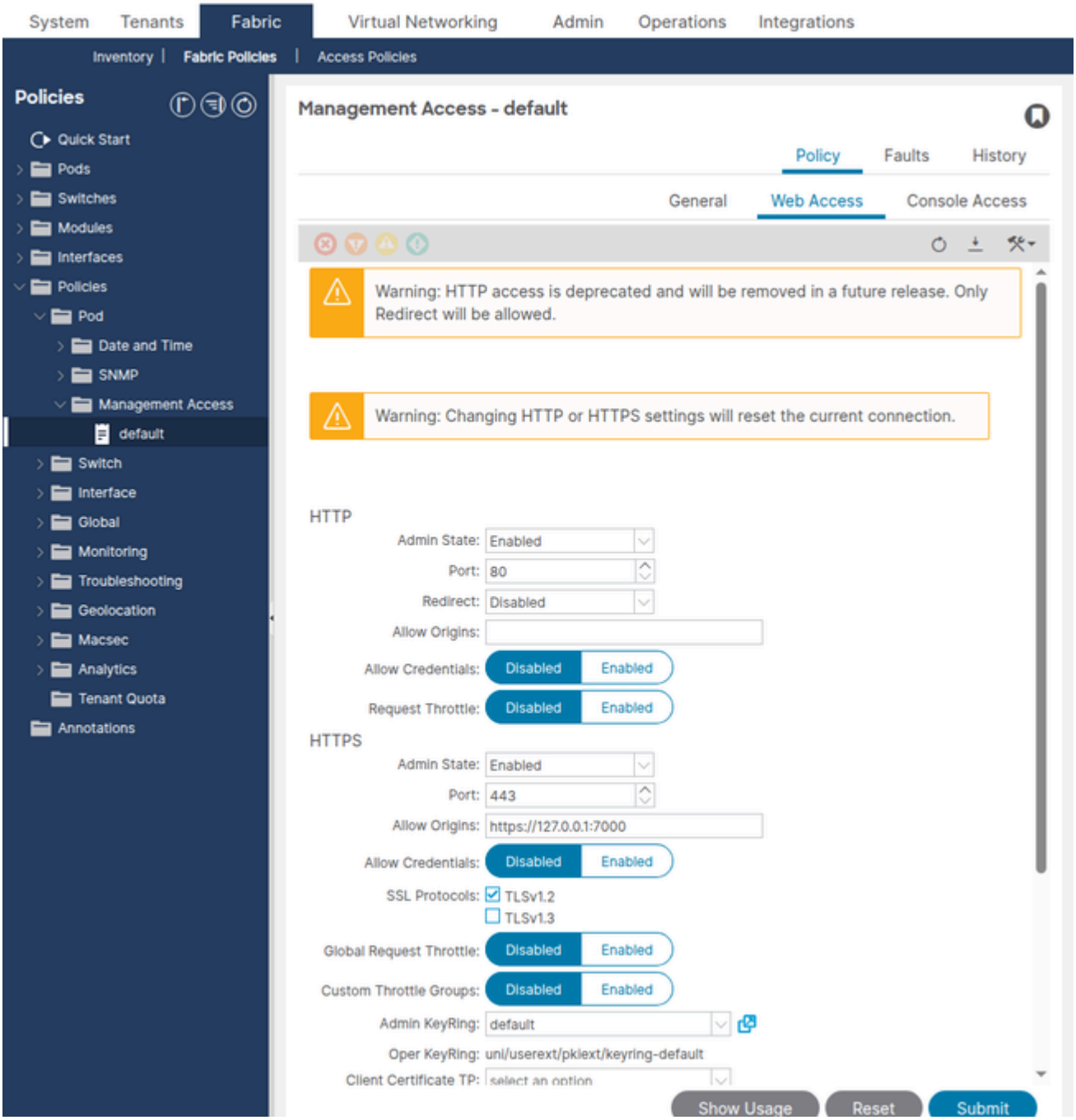
Konfiguration überprüfen

Bevor Sie die Fehlerbehebung für den Betriebszustand durchführen, stellen Sie sicher, dass die Konfigurationskette abgeschlossen ist. Fehlkonfigurationen sind die häufigste Ursache für Probleme beim Remote-Zugriff.

Überprüfen der Management-Zugriffsrichtlinie (SSH und HTTPS)

Navigieren Sie zu Fabric > Fabric Policies > Policies > Pod > Management Access > default.





Bestätigen Sie die folgenden SSH-Einstellungen:

- Admin State (Admin-Status) - muss aktiviert sein.
- Port — Standard 22. Falls geändert, muss der SSH-Client den benutzerdefinierten Port verwenden.
- Passwortauthentifizierung — aktiviert (sofern keine reine Zertifikatsauthentifizierung vorgesehen ist).
- SSH-Chiffren — müssen mindestens eine vom SSH-Client unterstützte Chiffre enthalten.
- KEX-Algorithmen: Sie müssen mindestens einen vom SSH-Client unterstützten Algorithmus enthalten.
- SSH-MACs: Diese müssen mindestens eine vom SSH-Client unterstützte MAC enthalten.

Abfragen des verwalteten SSH-Objekts über die 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
```

Bestätigen Sie die folgenden HTTPS-Einstellungen:

- Admin State (Admin-Status) - muss aktiviert sein.
- Port: Standard 443.
- SSL-Protokolle - TLSv1.2 (Standard). Für ältere Clients kann TLSv1.1 explizit hinzugefügt werden.
- Drosselungszustand - Wenn aktiviert, begrenzt die Drosselungsrate Anforderungen pro Sekunde pro Benutzer. Ein sehr niedriger Wert kann zu API-Timeout-Fehlern führen.

<#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
```

Häufige Fehlkonfigurationen

- SSH-Verschlüsselungen sind zu stark eingeschränkt - in ACI Version 5.2(1) und höher wurden die Standard-SSH-Verschlüsselungen gehärtet. Ältere SSH-Clients (z. B. PuTTY-Versionen vor 0,75 oder OpenSSH-Versionen, die nur angeboten **diffie-hellman-group14-sha1**werden) können den Schlüsselaustausch nicht erfolgreich durchführen. Der SSH-Client

zeigt "Keine übereinstimmende Verschlüsselung gefunden" oder "Keine übereinstimmende Schlüsselaustauschmethode gefunden" an.
- Kennwortauthentifizierung deaktiviert - Wenn **passwordAuth** die Option deaktiviert ist, ist nur die schlüsselbasierte SSH-Authentifizierung zulässig. Benutzer, die sich mit Passwörtern verbinden, sehen "Berechtigung verweigert (publickey)".
- Benutzerdefinierter SSH-Port ohne Client-Erkennung - Wenn der SSH-Port von 22 geändert wurde, muss der SSH-Client den neuen Port angeben (z. B. **ssh -p 2222 admin@10.1.1.1**).

Überprüfen der OOB-Managementadressen

Navigieren Sie zu Tenants > mgmt > Node Management Addresses.

Vergewissern Sie sich, dass jedem APIC- und Switch-Knoten eine OOB-Management-IP-Adresse mit einem gültigen Gateway zugewiesen wurde. Knoten ohne Verwaltungsadressen sind über das Verwaltungsnetzwerk nicht erreichbar.

Fragen Sie die statischen OOB-Knotenzuweisungen über die API ab:

<#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
```

Häufige Fehlkonfigurationen

- Fehlende OOB-Adresszuweisung - Ein Switch hat keinen Eintrag unter **mgmtRsOoBStNode**. Der Knoten verfügt über keine Management-IP-Adresse und antwortet nicht auf SSH oder HTTPS an der OOB-Schnittstelle.
- Falsches Gateway - die Gateway-Adresse stimmt nicht mit dem tatsächlichen Gateway im OOB-Managementnetzwerk überein. Der Knoten kann Pakete empfangen, aber keinen zurückkehrenden Datenverkehr senden.
- Subnetzmaske stimmt nicht überein - die OOB-Subnetzmaske stimmt nicht mit dem physischen Managementnetzwerk überein. Dies kann dazu führen, dass der Knoten glaubt, die Management-Station befinde sich in einem anderen Subnetz, und den Datenverkehr über ein nicht vorhandenes oder falsches Gateway weiterleitet.

OOB-Verträge überprüfen

Navigieren Sie zu Tenants > mgmt > Contracts.

Wenn ein OOB-Vertrag auf die OOB-Management-EPG angewendet wird, erreicht nur der gemäß diesem Vertrag zulässige Datenverkehr die APIC-Management-Schnittstelle. Auf dem APIC werden OOB-Verträge mithilfe von **iptables** Regeln durchgesetzt.

Fragen Sie die von der OOB-EPG bereitgestellten Verträge ab:

<#root>

apic1#

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

Wenn die Abfrage Ergebnisse zurückgibt, werden Verträge angewendet. Überprüfen Sie, ob die Vertragsgegenstände und Filter die erforderlichen Protokolle zulassen:

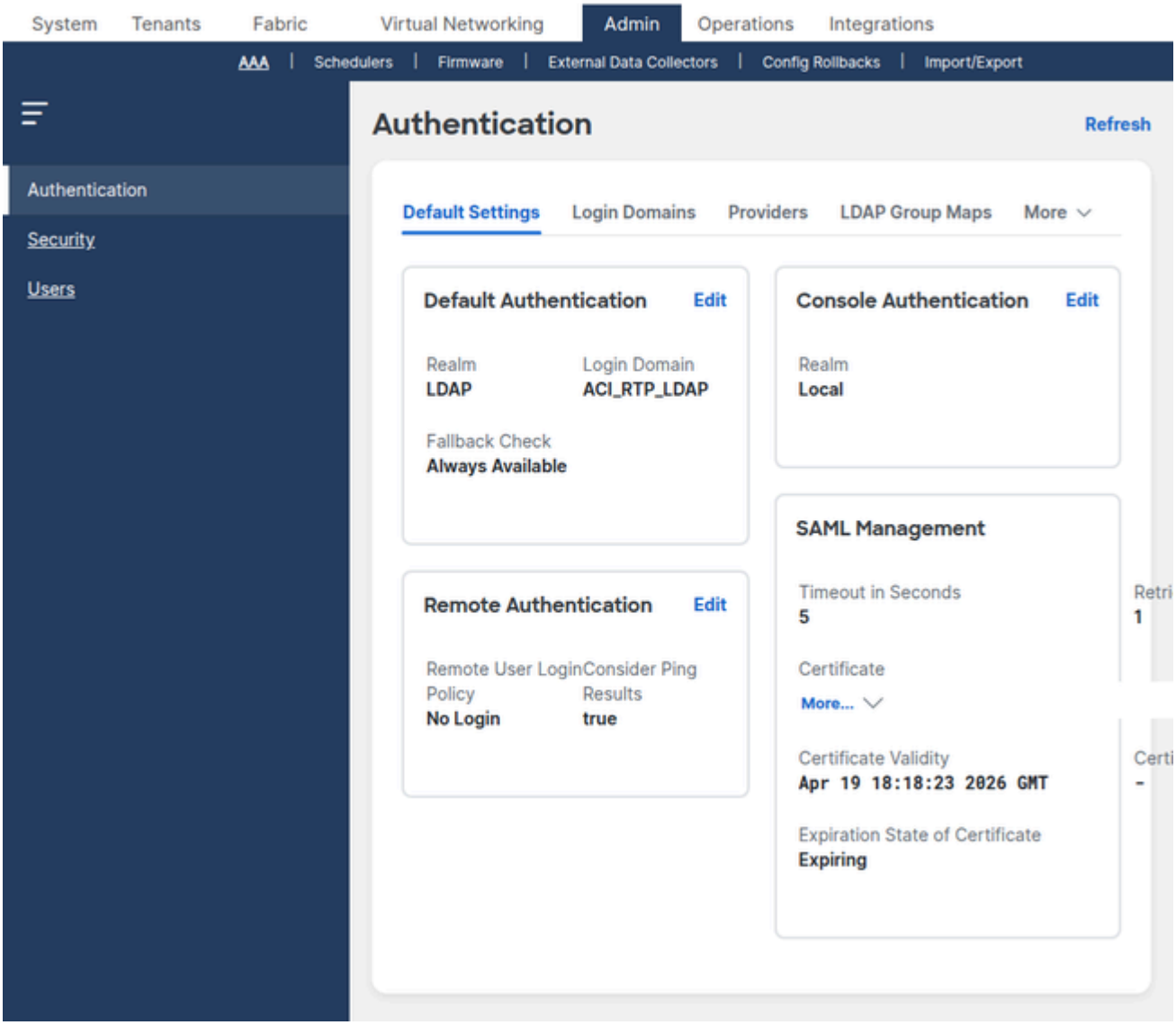
- SSH - TCP-Port 22 (oder benutzerdefinierter Port)
- HTTPS - TCP-Port 443 (oder benutzerdefinierter Port)
- ICMP - zur Ping-Verifizierung

Häufige Fehlkonfigurationen

- Der OOB-Vertrag enthält kein SSH oder HTTPS - der Techniker kann den APIC pingen, aber keine Verbindung über SSH oder HTTPS herstellen. In den **iptables** Regeln des APIC wird der Datenverkehr unbeaufsichtigt fallen gelassen.
- Quell-IP-Einschränkung im OOB-Vertragsfilter - Der Vertragsfilter beschränkt den Zugriff auf bestimmte Quell-Subnetze. Techniker außerhalb dieses Subnetzes können keine Verbindung herstellen.

Überprüfen der AAA-Konfiguration

Navigieren Sie zu Admin > AAA > Authentication > AAA.



Bestätigen Sie Folgendes:

- Standard-Authentifizierungsbereich: Gibt an, welche Anmeldungsdomäne verwendet wird, wenn der Benutzer keine Domäne angibt. Wenn eine Remote-AAA-Anmeldungsdomäne festgelegt ist, muss der entsprechende Server erreichbar sein.
- Konsolen-Authentifizierungsbereich — steuert den Konsolenzugriff. Bei lokaler Einstellung werden bei der Konsolenanmeldung immer lokale Anmeldeinformationen verwendet (empfohlen).

Anmeldedomänen überprüfen

Navigieren Sie zu Admin > AAA > Authentication > Login Domains (Admin > AAA > Authentifizierung > Anmeldedomänen).

<#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
```

Stellen Sie sicher, dass die für die Authentifizierung verwendete Anmeldedomäne vorhanden ist und auf die richtige Anbietergruppe verweist.

Überprüfung von TACACS+-Anbietern

Navigieren Sie zu 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
```

RADIUS-Anbieter überprüfen

Navigieren Sie zu 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
```

LDAP-Anbieter überprüfen

Navigieren Sie zu 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
```

Häufige AAA-Fehlkonfigurationen

- Diskrepanz beim gemeinsamen geheimen Schlüssel - der für den ACI TACACS+- oder RADIUS-Anbieter konfigurierte Schlüssel stimmt nicht mit dem Schlüssel auf dem Server überein. Die Authentifizierung schlägt automatisch fehl.
- Falsche Verwaltungs-EPG - die des Anbieters **epgDn** ist leer oder verweist auf die falsche EPG (z. B. In-Band, wenn sich der Server im OOB-Netzwerk befindet). Der APIC kann den Server nicht erreichen.
- Nicht übereinstimmende Anmeldedomänenbereiche — die Anmeldedomäne ist als LDAP konfiguriert, der Benutzer erwartet jedoch TACACS+-Authentifizierung. Anmeldedomänen müssen auf den richtigen Anbietergruppentyp verweisen.
- Die LDAP-DN-Anbindung ist falsch - die **rootdn** (DN-Anbindung) ist falsch oder **basedn** falsch. Die LDAP-Authentifizierung schlägt fehl, und es tritt ein Fehler bei der Anbindung auf, selbst wenn die Anmeldeinformationen des Benutzers korrekt sind.
- Der LDAP-Filter stimmt nicht mit dem Verzeichnisschema überein - für Active Directory verwenden Sie **sAMAccountName=$userid**. Für OpenLDAP verwenden Sie **cn=$userid** oder **uid=$userid**.

RBAC-Konfiguration überprüfen

Navigieren Sie zu Admin > AAA > Users, um die lokalen Benutzerkonten sowie deren Sicherheitsdomäne und Rollenzuweisungen anzuzeigen.

Abfragen von Sicherheitsdomänen über die 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
```

Ein Benutzer, der der Domäne all mit der Rolle admin zugewiesen ist, hat vollen Lese- und Schreibzugriff auf die gesamte Fabric. Ein Benutzer, der einer benutzerdefinierten Sicherheitsdomäne mit der Rolle tenant-admin zugewiesen ist, kann nur Tenants verwalten, die dieser Domäne zugeordnet sind.

Häufige RBAC-Fehler

- Benutzer ohne Sicherheitsdomäne erstellt: Der Benutzer kann sich anmelden, sieht aber keine Tenants und erhält "403 Forbidden" für API-Anrufe. Es muss mindestens eine Sicherheitsdomäne zugewiesen sein.
- Schreibgeschützte Rolle zugewiesen, wenn Schreibzugriff erforderlich ist — der Benutzer kann Objekte anzeigen, aber keine Änderungen senden. Überprüfen Sie, ob die Rollenberechtigung auf writePriv festgelegt ist.
- Auf dem AAA-Server fehlt die Remote-Benutzerrollenzuordnung - der TACACS+- oder RADIUS-Server gibt das **cisco-av-pair** Attribut, das **shell:domains=all/admin/**enthält, nicht zurück. Der Benutzer wird erfolgreich authentifiziert, hat jedoch keine Rollen und kann in der Fabric nichts sehen.

Fehlerbehebung bei OOB- und In-Band-Management

Wenn die Management-IP-Adresse des APIC oder Switches im Netzwerk nicht erreichbar ist, beheben Sie den Fehler im Management-Pfad, bevor Sie SSH, HTTPS oder AAA untersuchen.

Szenario: Ping der APIC OOB-IP-Adresse nicht möglich

Problem: Die Management-Station kann keinen Ping an die IP-Adresse des APIC OOB-Managements senden.

Verifizierungsschritte:

1. Überprüfen Sie, ob der APIC-Management-Port physisch angeschlossen und die Verbindung aktiv ist.
2. Überprüfen Sie, ob sich die Managementstation im gleichen L2-Segment befindet oder eine Route zum OOB-Subnetz aufweist.
3. Überprüfen Sie, ob die OOB-Management-IP richtig zugewiesen wurde:
   <#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. Überprüfen Sie, ob das Standard-Gateway erreichbar ist:
   <#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. Wenn ein OOB-Vertrag angewendet wird, stellen Sie sicher, dass er die erforderlichen Protokolle zulässt. Fragen Sie die von der OOB-EPG bereitgestellten Verträge ab, wie im Abschnitt "OOB-Verträge verifizieren" dargestellt. OOB-Verträge werden als **iptables** Regeln für den APIC durchgesetzt. Sie können die gespeicherten Regeln aus der APIC-Shell anzeigen:
   <#root>

   ```
   apic1#

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

   Wenn die INPUT-Richtlinie DROP lautet und es für das erforderliche Protokoll keine ACCEPT-Regel gibt, filtert der OOB-Vertrag den Datenverkehr.

> Anmerkung: Der **iptables -L -n** Befehl zum Anzeigen von Live-Kernel-Regeln erfordert Root-Zugriff und ist für reguläre Admin-SSH-Sitzungen nicht verfügbar.

Ursache: Fehlende oder falsch konfigurierte OOB-Managementadresse, falsches Gateway oder OOB-Vertragsfilterungsverkehr.

Lösung: Korrigieren Sie die OOB-Adresszuweisung, überprüfen Sie den physischen Netzwerkpfad, oder aktualisieren Sie den OOB-Vertrag, um die erforderlichen Protokolle zuzulassen.

Szenario: Keine Switch-Management-IP-Adresse erreichbar

Problem: Die Management-Station kann den APIC erreichen, aber keinen Switch über OOB.

Verifizierungsschritte:

1. Überprüfen Sie, ob dem Switch eine OOB-Adresse zugewiesen ist:
   <#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. Überprüfen Sie, ob der Switch-Management-Schnittstelle die zugewiesene IP-Adresse zugeordnet ist:
   <#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. Überprüfen Sie die Standard-VRF-Management-Route:
   <#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
```

Ursache: Fehlende OOB-Adressenzuweisung, falsches Gateway oder ausgefallener physischer Switch-Management-Port.

Lösung: Weisen Sie die OOB-Adresse unter Tenants > mgmt > Node Management Addresses (Tenants > mgmt > Node-Management-Adressen) zu. Überprüfen Sie, ob die physische Management-Verbindung aktiv ist.

Fehlerbehebung bei SSH-Zugriff

In diesem Abschnitt werden Szenarien beschrieben, in denen die Management-IP-Adresse erreichbar ist (Ping erfolgreich), die SSH-Sitzung jedoch nicht eingerichtet oder authentifiziert werden kann.

Szenario: SSH-Verbindung verweigert

Problem: Der SSH-Client meldet beim Herstellen einer Verbindung mit dem APIC oder Switch "Verbindung verweigert".

Verifizierungsschritte:

1. Überprüfen Sie, ob SSH in der Management-Zugriffsrichtlinie aktiviert ist:
   <#root>

   ```
   apic1#

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

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

   Wenn **adminSt**deaktiviert ist, werden SSH-Verbindungen abgelehnt.

2. Überprüfen Sie, ob der richtige Port verwendet wird. Wenn der SSH-Port von 22 geändert wurde:
   <#root>

   ```
   $

   ssh -p

    custom-port
   ```

```
admin@10.1.1.1
```

3. Überprüfen Sie, ob der OOB-Vertrag TCP auf dem SSH-Port zulässt. Weitere Informationen finden Sie im Abschnitt "Prüfen von OOB-Verträgen".

Ursache: SSH wurde in der Management-Zugriffsrichtlinie deaktiviert, benutzerdefinierter Port vom Client nicht bekannt oder OOB-Vertragsfilterung.

Lösung: Aktivieren Sie SSH in der Management-Zugriffsrichtlinie, oder verwenden Sie den richtigen Port.

Szenario: Fehler beim Austausch des SSH-Schlüssels (Cipher oder KEX stimmen nicht überein)

Problem: Der SSH-Client schlägt fehl: "Keine übereinstimmende Chiffre gefunden", "Keine übereinstimmende Schlüsselaustauschmethode gefunden" oder "Keine übereinstimmende MAC gefunden".

Verifizierungsschritte:

1. Überprüfen Sie die ausführliche Ausgabe des SSH-Clients, um festzustellen, welche Algorithmen der Client anbietet:
<#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. Vergleichen Sie die vom Client bereitgestellten Algorithmen mit den vom APIC konfigurierten Algorithmen:
<#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. Identifizieren Sie die Kreuzung. Wenn es in keiner Kategorie einen gemeinsamen

Algorithmus gibt, schlägt der Handshake fehl.

Anmerkung: In der ACI-Version 5.2(1) und höher wurden die SSH-Standardchiffren und die KEX-Algorithmen gehärtet. Alte Algorithmen wie **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**, **aes128-cbc**und **hmac-sha1** werden nicht mehr standardmäßig angeboten. Wenn Sie kürzlich ein Upgrade durchgeführt haben, stellen Sie sicher, dass die SSH-Clients in Ihrer Umgebung die neuen Standardeinstellungen unterstützen.

Ursache: Nach einem ACI-Upgrade oder einer Cipher-Härtung gibt es zwischen dem SSH-Client und dem APIC keine einheitliche Chiffre, keinen einheitlichen KEX-Algorithmus oder keine einheitliche MAC-Adresse.

Lösung: Aktualisieren Sie entweder den SSH-Client, um moderne Algorithmen zu unterstützen, oder fügen Sie den erforderlichen Legacy-Algorithmus erneut der Management Access Policy hinzu. Das erneute Hinzufügen älterer Algorithmen ist mit Sicherheitsrisiken verbunden und wird langfristig nicht empfohlen.

Szenario: SSH stellt Verbindung her, aber Authentifizierung schlägt für lokale Benutzer fehl

Problem: SSH-Handshake war erfolgreich (Kennworteingabeaufforderung wird angezeigt), aber das Kennwort wurde für einen lokalen Benutzer abgelehnt.

Verifizierungsschritte:

1. Überprüfen Sie, ob der Benutzer lokal vorhanden ist:
   <#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. Überprüfen Sie, ob das Konto aufgrund übermäßiger fehlgeschlagener Anmeldeversuche gesperrt ist:
   <#root>

```
apic1#

moquery -c aaaUserEp

dn                : uni/userext
pwdStrengthCheck  : no
```

Überprüfen Sie die Richtlinien für das Sperren der Anmeldedomäne unter Admin > AAA > Security Management > Lockout Policy.

3. Vergewissern Sie sich, dass sich der Benutzer mit der richtigen Anmeldedomäne anmeldet. Wenn der Standard-Authentifizierungsbereich auf eine AAA-Anmeldedomäne festgelegt ist, muss der Benutzer vor **apic:LOCAL\\username** oder **apic:fallback\\username** stehen, um die lokale Authentifizierung zu erzwingen.
4. Validieren Sie das Authentifizierungsergebnis in den Protokollen. Überprüfen Sie **nginx.bin.log** den APIC auf das Anmeldeereignis:
<#root>

```
apic1#

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

Suchen Sie nach dem Bereich und der Anbietergruppe, die dem Anmeldeversuch zugewiesen sind:

```
! 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
```

Wenn der Bereich nicht 0 (fallback/local) ist, wurde die Anmeldung an einen Remote-AAA-Server anstatt an die lokale Datenbank gesendet. Der Benutzer muss vorangestellt **apic:fallback\\username** oder **apic:LOCAL\\username** sein, um die lokale Authentifizierung zu erzwingen.

Ursache: Falsches Kennwort, gesperrtes Konto oder der Anmeldeversuch wird an einen Remote-AAA-Server anstatt an die lokale Datenbank gesendet.

Lösung: Setzen Sie das Kennwort zurück, entsperren Sie das Konto, oder verwenden Sie das richtige Präfix für die Anmelde-Domäne.

Fehlerbehebung für HTTPS-Zugriff

In diesem Abschnitt werden Szenarien beschrieben, in denen die APIC-Webbenutzeroberfläche oder die REST-API (Representational State Transfer) über HTTPS nicht erreichbar ist.

Szenario: Zeitüberschreitung bei HTTPS-Verbindung

Problem: Der Browser zeigt "ERR_CONNECTION_TIMED_OUT" an, oder der API-Aufruf hängt, wenn eine Verbindung mit dem APIC an Port 443 hergestellt wird.

Verifizierungsschritte:

1. Überprüfen Sie, ob HTTPS aktiviert ist:
   <#root>

   ```
   apic1#
   ```

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

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

2. Überprüfen Sie, ob der OOB-Vertrag TCP 443 zulässt. Weitere Informationen finden Sie im Abschnitt "OOB-Verträge verifizieren".
3. Test vom APIC selbst, um zu bestätigen, dass der HTTPS-Prozess auf Verbindungen wartet:
   <#root>

   ```
   apic1#
   ```

   ```
   ss -tlnp | grep 443
   ```

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

Ursache: HTTPS deaktiviert, OOB-Vertragsfilterung TCP 443, oder der Nginx-Prozess auf dem APIC ist abgestürzt.

Lösung: Aktivieren Sie HTTPS in der Management-Zugriffsrichtlinie, aktualisieren Sie den OOB-Vertrag, oder starten Sie den Webdienst auf dem APIC neu.

Szenario: Browser zeigt TLS-Handshake-Fehler an

Problem: Der Browser zeigt "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" oder einen ähnlichen TLS-Fehler an.

Verifizierungsschritte:

1. Überprüfen Sie die auf dem APIC konfigurierte TLS-Protokollversion:
   <#root>

   ```
   apic1#

   moquery -c commHttps

   sslProtocols : TLSv1.2
   ```

2. Stellen Sie sicher, dass der Browser TLSv1.2 unterstützt. Sehr alte Browser (z. B. Internet Explorer 10 und älter) unterstützen TLSv1.2 standardmäßig nicht.

Ursache: Der APIC bietet nur TLSv1.2 (Standard) und der Browser bzw. API-Client unterstützt nur ältere TLS-Versionen.

Lösung: Aktualisieren Sie den Browser oder Client. Wenn Sie ältere Clients vorübergehend unterstützen müssen, fügen Sie TLSv1.1 zur Management-Zugriffsrichtlinie hinzu. Dies bringt jedoch Sicherheitsrisiken mit sich.

Szenario: API-Drosselungsbegrenzung

Problem: REST-API-Aufrufe schlagen zeitweilig mit HTTP 503-Fehlern fehl, oder die Web-Benutzeroberfläche wird bei starker Automatisierung langsam.

Verifizierungsschritte:

<#root>

```
apic1#

moquery -c commHttps

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

Wenn die Drosselungsrate sehr niedrig ist und Automatisierungsskripts viele Anfragen pro Sekunde senden, lehnt der APIC überzählige Anfragen ab.

Ursache: Die Drosselungsrate pro Benutzer ist für den Automatisierungs-Workload zu niedrig.

Lösung: Erhöhen Sie die Drosselungsrate gemäß der Management Access Policy, oder optimieren Sie die Automatisierungsskripts, um die Anfragefrequenz zu reduzieren. Alternativ können Sie die Drosselung deaktivieren, wenn die Fabric nicht freigegeben ist.

Fehlerbehebung: AAA - TACACS+

In diesem Abschnitt werden Fehler bei der TACACS+-Authentifizierung beschrieben. Der APIC kommuniziert über den TCP-Port 49 mit dem TACACS+-Server.

Betriebliche Überprüfung

ACI-Switches unterstützen den **test aaa** auf Standalone NX-OS verfügbaren Befehl nicht. Verwenden Sie zur Überprüfung des TACACS+-Betriebs den APIC, um den Anbieterstatus, Fehler und den Verlauf der Anmeldesitzung zu überprüfen.

Überprüfen Sie den TACACS+-Anbieter auf aktive Fehler:

<#root>

```
apic1#

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

Wenn keine Fehler zurückgegeben werden, hält der APIC den Provider für erreichbar. Bei Fehlern enthält die Ausgabe Fehlercodes wie F1773 (Provider unreachable) oder F1774 (Authentication Failure).

Überprüfen Sie die TACACS+-Anbieterkonfiguration:

<#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
```

Überprüfen der grundlegenden Netzwerkerreichbarkeit vom APIC zum 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
```

Melden Sie sich mit der TACACS+-Anmeldedomäne beim APIC an, und überprüfen Sie das Sitzungsergebnis:

<#root>

```
apic1#

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

Überprüfen Sie anhand des **descr** Felds, ob der Fehler auf eine abgewiesene Authentifizierung oder ein Verbindungsproblem zurückzuführen ist.

Validierung des TACACS+-Authentifizierungsflusses in den APIC-Protokollen Filter für den fraglichen Benutzernamen:

<#root>

```
apic1#

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

TACACS+-Anmeldungen folgen demselben **nginx.bin.log** Authentifizierungsablauf wie LDAP (vollständige Beispiele für echte Protokolldateien finden Sie im Abschnitt LDAP Operational Verification). Die wichtigsten Unterschiede bei TACACS+ sind:

- `DefaultAuthMo gibt den Bereich 2 an` - Bereich 2 gibt TACACS+ an (im Gegensatz zu Bereich 3 für LDAP).

- `Hinzufügen von TACACSProvider <IP> zur Liste` - Identifiziert den TACACS+-Server, der kontaktiert wird (im Gegensatz zu LDAP`-Provider` für LDAP).
- `TACACS+ Cisco-avpair (shell:domains=all/admin/)` — das AV-Paar wird direkt vom TACACS+-Server zurückgegeben (im Gegensatz zur Konvertierung aus einer LDAP-Gruppenzuordnung).

Eine erfolgreiche TACACS+-Anmeldung zeigt dieselbe Entwicklung: PAM-Anfrage → Bereichsauswahl → Anbietersuche → AV-Paar-Parsing → User-Injection → UserDomain und Rollenzuweisung → `Admin-Schreibrechte`.

Eine fehlgeschlagene TACACS+-Anmeldung endet mit `Benutzer <Benutzername> wurde bei der AAA-Authentifizierung verweigert` und `Fehler: Unauthorized ... AAA-Serverauthentifizierung ABGELEHNT`, dasselbe Muster wie bei einer LDAP-Absage.

Szenario: Fehler bei TACACS+-Authentifizierung

Problem: Die Anmeldung schlägt fehl mit "Authentifizierung fehlgeschlagen", wenn der Benutzer eine TACACS+-Anmeldedomäne auswählt.

Verifizierungsschritte:

1. Überprüfen Sie den TACACS+-Anbieter auf aktive Fehler:
   <#root>

   ```
   apic1#
   ```

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

   Der Fehler F1773 weist auf ein Verbindungsproblem hin. Der Fehler F1774 weist auf eine Zurückweisung der Authentifizierung hin.

2. Überprüfung der Netzwerkerreichbarkeit vom APIC zum 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. Wenn der Ping-Test erfolgreich ist, die Authentifizierung jedoch fehlschlägt, überprüfen Sie die Übereinstimmung des gemeinsamen geheimen Schlüssels sowohl in der APIC-Anbieterkonfiguration als auch in der TACACS+-Serverkonfiguration.
4. Sehen Sie sich die letzten Anmeldesitzungen an, um Details zum Fehler anzuzeigen:

<#root>

apic1#

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

5. Überprüfen Sie die TACACS+-Serverprotokolle auf den Authentifizierungsversuch. Ein erfolgreicher Versuch, der am Server angemeldet, aber abgelehnt wurde, weist auf ein serverseitiges Problem mit der Benutzerkonfiguration hin (z. B. Passwortungleichheit oder fehlendes Benutzerkonto).
6. Überprüfen Sie den APIC auf **nginx.bin.log** den vollständigen Authentifizierungsablauf. Filtern Sie nach Benutzernamen und nicht nach bestimmten Schlüsselwörtern, damit keine Zwischenmeldungen verpasst werden:
<#root>

apic1#

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

Vergleichen Sie die Ergebnisse mit den funktionierenden und nicht funktionierenden Beispielen im Abschnitt "Betriebsverifizierung" oben. Schlüsselindikatoren:

- `wurde abgelehnt` oder `ABGELEHNT` - der TACACS+-Server wurde erreicht, aber die Anmeldedaten wurden abgelehnt. Überprüfen Sie, ob der Benutzer auf dem Server vorhanden ist und ob das Kennwort übereinstimmt.
- Keine anbieterspezifischen Meldungen nach dem `Hinzufügen von TACACSprovider` — der Server ist nicht erreichbar oder abgelaufen. Überprüfen der Netzwerkerreichbarkeit und der Verwaltungs-EPG
- `Das Einschleusen des Remote-Benutzers ... wurde abgeschlossen`, gefolgt von Rollenprüfungszeilen — Authentifizierung war erfolgreich, aber das Problem kann bei der Rollenzuweisung auftreten (siehe Abschnitt zu AV-Paaren unten).

TACACS+ cisco-av-pair für RBAC

Bei Remote-Benutzern, die über TACACS+ authentifiziert wurden, muss der Server das **cisco-av-pair** Attribut in der Autorisierungsantwort zurückgeben. Dieses Attribut ordnet den Benutzer den ACI-Sicherheitsdomänen und -rollen zu.

Format:

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

Beispiele:

- Vollständiger Administrator: **shell:domains=all/admin/**
- Schreibgeschützt für alle: **shell:domains=all/read-all/**
- Tenant-Administrator für eine bestimmte Domäne: **shell:domains=TenantA/tenant-admin/**
- Mehrere Domänen: **shell:domains=all/admin/,TenantA/tenant-admin/**

Wenn dieses Attribut fehlt oder falsch formatiert ist, wird der Benutzer erfolgreich authentifiziert, hat jedoch keine Rollen und kann keine Objekte in der APIC-Benutzeroberfläche sehen.

Anmerkung: Für den SSH-Zugriff auf Leaf- und Spine-Switches ist die Admin-Rolle mit Schreibberechtigung in der gesamten Sicherheitsdomäne erforderlich. Das minimale AV-Paar für den Switch-SSH-Zugriff ist **shell:domains=all/admin/**. Benutzer ohne Administratorrolle (z. B. `Read-all`, `Tenant-admin`, `aaa`) oder Benutzer, die einer anderen Sicherheitsdomäne als allen zugewiesen sind, können sich beim APIC anmelden, erhalten jedoch keinen SSH-Zugriff auf Switches. Das APIC-Protokoll zeigt an, dass `Nicht-Admin-Anmeldungen auf dem Switch` für diese Benutzer `abgelehnt wurden`.

Validieren Sie das empfangene AV-Paar durch Überprüfung **nginx.bin.log**. Filtern Sie nach dem Benutzernamen, um den vollständigen Fluss der Rolleninjektion anzuzeigen:

<#root>

`apic1#`

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

Für TACACS+ wird das AV-Paar als `TACACS+ Cisco-avpair (shell:domains=...) protokolliert`. Eine erfolgreiche Injection zeigt, dass `die Injection des Remote-Benutzers <Benutzername> abgeschlossen wurde`, gefolgt von den Zeilen `Found UserDomain (Benutzerdomäne gefunden)` und `Admin Write Privilegien (`vollständige Beispiele dieses Datenflusses mit echter Protokollausgabe finden Sie im Abschnitt LDAP Operational Verification).

Wenn das AV-Paarformat ungültig ist, wird im Protokoll die Meldung `Injection of remote user <username> data FAILED (Einschleusen von Remote-Benutzer <username>) angezeigt. Die Fehlermeldung lautet Invalid shell:domains string (Ungültige Shell:domains-Zeichenfolge)`. Wenn sich der Benutzer mit einer Nicht-Admin-Rolle authentifiziert, wird die SSH-Verbindung zu den Switches verweigert, wenn `sich der Benutzer nicht beim Switch anmeldet`.

Ursache: Diskrepanz beim gemeinsamen geheimen Schlüssel, vom Verwaltungsnetzwerk nicht erreichbarer Server, kein Benutzer auf dem TACACS+-Server vorhanden, oder die Verwaltungs-EPG des Anbieters ist falsch.

Lösung: Korrigieren Sie den gemeinsamen geheimen Schlüssel, beheben Sie die Erreichbarkeit, oder erstellen Sie den Benutzer auf dem TACACS+-Server.

Leaf-Switch-Authentifizierungsprotokolle überprüfen

Bei Leaf- und Spine-Switches werden SSH-Anmeldeereignisse sowohl in als auch **pam.module.log** in **nginx.log**protokolliert. Das **pam.module.log** zeigt das PAM-Authentifizierungsergebnis an (Akzeptieren oder Ablehnen). Der **nginx.log** enthält den vollständigen AAA-Fluss (Bereichsauswahl, Anbietersuche, LDAP/TACACS+/RADIUS-Kommunikation, AV-Paarparsing und Rollenzuweisung), der mit **nginx.bin.log** dem des APIC identisch ist. Diese Protokolle gelten für alle Remote-AAA-Typen (TACACS+, RADIUS, LDAP).

Überprüfen Sie **pam.module.log** das Authentifizierungsergebnis:

<#root>

```
leaf101#

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

Funktionierend - erfolgreiche Remote-Authentifizierung auf dem 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
```

Das **remote=1** Flag bestätigt, dass der Benutzer von einem Remote-AAA-Server authentifiziert wurde.

Funktioniert nicht - der Benutzer wurde abgelehnt. Die securitymgrAG verweigert den Benutzer, und der Switch versucht eine lokale Benutzersuche als letzten Fallback:

```
||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
```

Wenn für den Benutzer überhaupt keine PAM-Einträge angezeigt werden, wurde die SSH-Verbindung wahrscheinlich vor Erreichen der PAM-Stufe abgelehnt (z. B. aufgrund einer nicht übereinstimmenden Verschlüsselung oder weil der Benutzer die Verbindung abgebrochen hat).

Eine detailliertere Ansicht des Authentifizierungsflusses auf dem Switch finden Sie unter **nginx.log**. Dieses Protokoll enthält die gesamte AAA-Entscheidungskette - dasselbe Format und dieselben Meldungen wie **nginx.bin.log** auf dem APIC:

<#root>

```
leaf101#
```

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

Funktionierend - erfolgreiche LDAP-Authentifizierung an einem Switch (vergleichen Sie mit den APIC-LDAP-Beispielen im Abschnitt "LDAP Operational Verification" - die Meldungen sind identisch):

```
||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
```

Der Schalter **nginx.log** ist insbesondere dann nützlich, wenn er eine Ablehnung **pam.module.log** zeigt, aber nicht erklärt, warum. Die Datei "nginx.log" zeigt den AAA-Bereich, -Anbieter und den spezifischen Fehlergrund (z. B. leere LDAP-Suche, TACACS+-Zeitüberschreitung oder Fehler beim Einschleusen von AV-Paaren).

Fehlerbehebung: AAA - RADIUS

In diesem Abschnitt werden Fehler bei der RADIUS-Authentifizierung behandelt. Der APIC kommuniziert mit dem RADIUS-Server über den UDP-Port 1812 (Authentifizierung) und optional über den UDP-Port 1813 (Accounting).

Betriebliche Überprüfung

ACI-Switches unterstützen den **test aaa** auf Standalone NX-OS verfügbaren Befehl nicht. Verwenden Sie die folgenden Methoden, um den RADIUS-Betrieb zu überprüfen.

Überprüfen Sie die RADIUS-Serverkonfiguration und die Erreichbarkeitsstatistiken von einem 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
```

Szenario: RADIUS-Authentifizierung fehlgeschlagen

Problem: Die Anmeldung schlägt fehl, wenn ein Benutzer eine RADIUS-Anmeldedomäne auswählt.

Verifizierungsschritte:

1. RADIUS-Serverstatistiken von einem Switch auf Anzeichen von Zeitüberschreitungen oder Fehlern überprüfen:

<#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
```

Eine hohe Anzahl bei Anfragen mit Zeitüberschreitung zeigt an, dass der RADIUS-Server nicht erreichbar ist oder der gemeinsame geheime Schlüssel nicht übereinstimmt (bei nicht übereinstimmenden gemeinsamen geheimen Paketen verwirft RADIUS unbeaufsichtigt Pakete).

2. Überprüfen Sie die Netzwerkerreichbarkeit zum RADIUS-Server:
<#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. Überprüfen Sie die Übereinstimmung des gemeinsamen geheimen Schlüssels zwischen dem APIC und dem RADIUS-Server. Im Gegensatz zu TACACS+, das TCP verwendet und Verbindungsfehler meldet, verwendet RADIUS UDP und verwirft unbeaufsichtigt Pakete, wenn der gemeinsame geheime Schlüssel nicht übereinstimmt. Das einzige Symptom ist ein Timeout.
4. Überprüfen der RADIUS-Serverprotokolle FreeRADIUS im Debug-Modus (**radiusd -X**) zeigt jede Anforderung an und gibt an, ob sie akzeptiert wurde, abgelehnt wurde oder ob eine Diskrepanz zwischen "shared secret" und "shared secret" vorliegt.
5. Überprüfen Sie den APIC auf **nginx.bin.log** den RADIUS-Authentifizierungsablauf. Nach Benutzername filtern:
<#root>

```
apic1#

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

RADIUS-Anmeldungen folgen demselben **nginx.bin.log** Authentifizierungsablauf wie LDAP und TACACS+ (vollständige Beispiele für echte Protokolle finden Sie im Abschnitt LDAP Operational Verification). Die wichtigsten Unterschiede für RADIUS sind:

- `Durch Hinzufügen von RadiusProvider <IP> zur Liste` wird der RADIUS-Server identifiziert (im Gegensatz zu `TACACSProvider` oder `LDAPProvider`).
- Die Bereichsnummer für RADIUS variiert je nach Konfiguration.

Eine erfolgreiche RADIUS-Anmeldung endet mit `der Einschleusung des Remote-Benutzers ... wurde abgeschlossen` und `Administratorrechte wurden erteilt`.

Eine fehlgeschlagene RADIUS-Anmeldung endet mit `wurde während der AAA-Authentifizierung abgelehnt` und `ABGELEHNT`.

Wenn nach der Zeile `Adding RadiusProvider` keine RADIUS-spezifischen Meldungen angezeigt werden, ist die Zeitüberschreitung beim Server aufgetreten. Im Gegensatz zu TACACS+, das TCP verwendet und Verbindungsfehler meldet, verwendet RADIUS UDP und verwirft unbeaufsichtigt Pakete, wenn der gemeinsame geheime Schlüssel nicht übereinstimmt. Das einzige Symptom ist eine Zeitüberschreitung gefolgt von einer Verweigerung.

6. Auf aktive Fehler des RADIUS-Anbieters prüfen:
<#root>

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

RADIUS cisco-av-pair für RBAC

RADIUS verwendet dasselbe **cisco-av-pair** Attribut wie TACACS+ für die RBAC-Rollenzuordnung. Der RADIUS-Server muss dieses Attribut in der Access-Accept-Antwort zurückgeben:

<#root>

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

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

In FreeRADIUS wird dies in der **users** Datei oder im LDAP-Backend konfiguriert. Für die ISE wird sie im Autorisierungsprofil als erweitertes Attribut konfiguriert.

Ursache: Diskrepanz beim gemeinsamen geheimen Schlüssel (am häufigsten bei RADIUS - verursacht stille Zeitüberschreitungen), nicht erreichbarer Server, falscher Authentifizierungsport oder fehlendes Benutzerkonto auf dem RADIUS-Server.

Lösung: Korrigieren Sie den gemeinsamen geheimen Schlüssel, überprüfen Sie die UDP 1812-Erreichbarkeit, oder konfigurieren Sie den Benutzer auf dem RADIUS-Server.

Fehlerbehebung: AAA - LDAP

In diesem Abschnitt werden Fehler bei der LDAP-Authentifizierung behandelt. Der APIC stellt über den TCP-Port 389 (LDAP) oder den TCP-Port 636 (LDAPS mit SSL) eine Verbindung zum LDAP-Server her.

Betriebliche Überprüfung

ACI-Switches unterstützen den **test aaa** auf Standalone NX-OS verfügbaren Befehl nicht. Um den LDAP-Betrieb zu überprüfen, überprüfen Sie die Provider-Fehler und die Konfiguration über den APIC.

Auf aktive Fehler des LDAP-Anbieters überprüfen:

<#root>

```
apic1#

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

Der Fehler F1777 weist auf ein Verbindungsproblem hin. Der Fehler F1778 weist auf einen Authentifizierungs- oder Bindungsfehler hin. Wenn keine Fehler zurückgegeben werden, hält der APIC den Provider für erreichbar.

Überprüfung der grundlegenden Netzwerkerreichbarkeit zum 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
```

Überprüfen Sie für LDAP auch die TCP-Verbindung mit Port 389 (oder 636 für LDAPS). Wenn der APIC den Server pingen kann, LDAP-Fehler jedoch weiterhin bestehen, liegt das Problem in der Regel in einer falschen Bindungs-DN, einem falschen Kennwort oder einer Firewall, die den LDAP-Port blockiert.

Validieren Sie den LDAP-Authentifizierungsablauf in den APIC-Protokollen. Nach Benutzername filtern:

<#root>

apic1#

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

Funktionierend - Eine erfolgreiche LDAP-Anmeldung zeigt den vollständigen Such-, Binde- und Rollenzuweisungs-Workflow an:

```
||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
```

Funktioniert nicht - Benutzer wurde nicht im LDAP-Verzeichnis gefunden (Suchergebnis ist eine leere Zeichenfolge):

```
||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
```

Szenario: LDAP-Authentifizierung fehlgeschlagen

Problem: Die Anmeldung schlägt fehl, wenn ein Benutzer eine LDAP-Anmeldedomäne auswählt.

Verifizierungsschritte:

1. Überprüfung der Erreichbarkeit des LDAP-Servers vom 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. Auf aktive LDAP-Anbieterfehler prüfen:
   <#root>

   ```
   apic1#

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

3. Überprüfen Sie die LDAP-Anbieterkonfiguration:
   <#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. Überprüfen Sie, ob der Benutzer im LDAP-Verzeichnis unter der konfigurierten Basis-DN vorhanden ist und mit dem Filter übereinstimmt. Bei Active Directory muss das **sAMAccountName** Benutzerattribut mit dem bei der Anmeldung eingegebenen Benutzernamen übereinstimmen. Bei OpenLDAP muss das **cn** oder das **uid** Attribut übereinstimmen.
5. Wenn Sie LDAPS (Port 636) verwenden, überprüfen Sie die SSL-Zertifikatkette. Wenn **SSLValidationLevel** der Wert strict festgelegt ist, lehnt der APIC die Verbindung ab, wenn das Serverzertifikat nicht vertrauenswürdig ist oder abgelaufen ist.
6. Überprüfen Sie den APIC auf **nginx.bin.log** den vollständigen LDAP-Authentifizierungsablauf. Filtern Sie nach dem Benutzernamen, damit Zwischenmeldungen nicht verpasst werden:
   <#root>

   ```
   apic1#

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

   Vergleichen Sie die Ergebnisse mit den funktionierenden und nicht funktionierenden Beispielen im Abschnitt "Betriebsverifizierung" oben. Zusätzliche LDAP-spezifische Fehlermuster können durch eine umfassende Suche im Protokoll gefunden werden:

<#root>

apic1#

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

Häufige Muster bei nicht funktionierendem Betrieb (Vergleich mit den oben genannten Beispielen für die betriebliche Überprüfung für den vollständigen Fluss):

```
! 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-Fehlermuster, nach denen gesucht werden soll:

- Timeout bei LDAP-Suche (Server nicht erreichbar, langsam oder Firewall blockierender Port 389/636) — Suche nach LDAP-`Suche fehlgeschlagen: Rückgabecode für ldap_search_ext_s: -5: Zeitüberschreitung`
- Bind fehlgeschlagen (root- oder bind-Passwort falsch, oder der Server hat die Verbindung verweigert) — Suche nach `LDAP fehlgeschlagen: Rückgabecode für ldap_search_ext_s: -1: Verbindung zum LDAP-Server nicht möglich`
- Benutzer gefunden, aber Kennwort ist falsch (Bindung mit Benutzerkennwort fehlgeschlagen) - Das Protokoll zeigt die `LDAP-Datensatz-DN`-Leitung an, gefolgt von einer abgelehnten Nachricht ohne "`Bind to UserDN ... successful`"-Leitung.

LDAP-Gruppenzuordnung für RBAC

LDAP verwendet Gruppenzuordnungen anstelle des **cisco-av-pair** Attributs. Das Feld des LDAP-Anbieters **attribute** gibt an, welches LDAP-Attribut die Gruppeninformationen enthält. Für Active Directory ist dies normalerweise **memberOf**.

Der APIC vergleicht die zurückgegebene Gruppen-DN mit den konfigurierten LDAP-Gruppenzuordnungsregeln (**aaaLdapGroupMapRule**), um die entsprechende Sicherheitsdomäne und -rolle zuzuweisen. Wenn keine Gruppenzuordnungsregel übereinstimmt, wird der Benutzer authentifiziert, verfügt jedoch über keine Rollen.

Alternativ können Sie festlegen, **attribute** dass der Wert direkt in den LDAP-Attributen des Benutzers gespeichert **CiscoAVPair shell:domains=all/admin/** und gespeichert wird. Diese Attribute haben dasselbe Format wie TACACS+ und RADIUS.

Ursache: Falscher Bindungs-DN oder falsches Kennwort, der Basis-DN enthält den Benutzer nicht, der Suchfilter stimmt nicht mit dem Verzeichnisschema überein, die LDAP-Zertifikatvalidierung ist fehlgeschlagen, oder es fehlen Regeln für die Gruppenzuordnung.

Lösung: Korrigieren Sie die Anbieterkonfiguration (Bind-DN, Basis-DN, Filter, SSL-Einstellungen). Überprüfen Sie bei RBAC-Problemen, ob die Gruppenzuordnungsregeln mit den LDAP-Gruppen übereinstimmen, zu denen der Benutzer gehört.

Fehlerbehebung bei RBAC und Benutzerberechtigungen

In diesem Abschnitt werden Szenarien behandelt, in denen sich der Benutzer erfolgreich authentifiziert, aber nicht über die erwartete Zugriffsstufe verfügt.

Szenario: Benutzer angemeldet, aber keine Tenants erkannt

Problem: Ein Remote-Benutzer meldet sich über TACACS+, RADIUS oder LDAP an. Die Anmeldung ist erfolgreich, aber der Benutzer sieht keine Tenants in der Benutzeroberfläche und API-Aufrufe geben leere Ergebnisse oder "403 Forbidden" zurück.

Verifizierungsschritte:

1. Überprüfen Sie die Benutzersitzung, um festzustellen, welche Rollen bei der Anmeldung zugewiesen wurden:
   <#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
   ```

   Das **descr** Feld zeigt das Anmeldeergebnis an. Wenn der Benutzer erfolgreich authentifiziert wurde, aber keine RBAC-Rollen hat, hat der AAA-Server keine gültige **cisco-av-pair** oder LDAP-Gruppenzuordnung zurückgegeben.

2. Überprüfen Sie den APIC, **nginx.bin.log** um das AV-Paar und die Rollenzuweisung während der Anmeldung anzuzeigen. Nach Benutzername filtern:
   <#root>

   ```
   apic1#

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

Suchen Sie nach Nachrichten für die Rolleninjektion und Domänenzuweisung:

Funktioniert - AV-Paar aus LDAP-Gruppenzuordnung konvertiert, Benutzer erhält Admin-Rolle:

```
||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
```

Funktioniert nicht - Wenn eine **Cisco-avpair** oder **Converted to CiscoAVPair** eine Zeile nicht im Fluss angezeigt wird, hat der AAA-Server das Attribut nicht zurückgegeben, und es wurde keine LDAP-Gruppenzuordnungsregel zugeordnet. Suchen Sie nach **Checking all UserDomains** , ohne dass **Found UserDomain** Zeilen folgen: Der Benutzer wurde authentifiziert, hat aber keine Rollenzuweisungen. Wenn eine **Injection ... data FAILED** Meldung angezeigt wird, ist das AV-Zeichenfolgenformat ungültig.

3. Überprüfen Sie, ob der AAA-Server das **cisco-av-pair** Attribut (für TACACS+ oder RADIUS) oder die richtige LDAP-Gruppenmitgliedschaft (für LDAP) zurückgibt. Überprüfen Sie die AAA-Serverkonfiguration:
    - TACACS+: Überprüfen Sie, ob das Benutzerprofil **cisco-av-pair** das Format **shell:domains=all/admin/**aufweist.
    - RADIUS: Vergewissern Sie sich, dass das Benutzerprofil **Cisco-AVPair = "shell:domains=all/admin/"** im Feld Access-Accept (Akzeptieren) zurückgegeben wird.
    - LSAP: Überprüfen Sie, ob der Benutzer Mitglied einer LDAP-Gruppe ist, die mit einer konfigurierten LDAP-Gruppenzuordnungsregel (**aaaLdapGroupMapRule**) übereinstimmt.
4. Wenn das Attribut vorhanden ist, der Benutzer jedoch immer noch keinen Zugriff hat, überprüfen Sie, ob der Name der Sicherheitsdomäne im Attribut mit einer vorhandenen Sicherheitsdomäne im APIC übereinstimmt:
<#root>

```
apic1#

moquery -c aaaDomain
```

Wenn der **cisco-av-pair** auf eine nicht existierende Domäne verweist (z. B. **shell:domains=NonExistentDomain/admin/**), schlägt die Rollenzuweisung im Hintergrund fehl.

Ursache: Der AAA-Server gibt die RBAC-Zuordnungsattribute nicht zurück, das Attributformat ist falsch, oder die Sicherheitsdomäne, auf die im Attribut verwiesen wird, ist auf dem APIC nicht vorhanden.

Lösung: Konfigurieren Sie den AAA-Server so, dass die richtige Zuordnung **cisco-av-pair** oder Gruppenzuordnung zurückgegeben wird. Überprüfen Sie, ob die Sicherheitsdomäne auf dem APIC vorhanden ist.

Szenario: Benutzer kann Konfiguration anzeigen, aber nicht ändern

Problem: Ein Benutzer kann sich anmelden und Objekte durchsuchen, erhält jedoch einen Fehler, wenn er versucht, Änderungen zu übermitteln.

Verifizierungsschritte:

1. Überprüfen Sie die Rollenzuweisungen des Benutzers:
   <#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. Wenn der Benutzer Schreibzugriff benötigt, muss die Rolle gewähren **writePriv**. Allgemeine Rollen mit Schreibberechtigungen sind admin, tenant-admin, access-admin und fabric-admin.
3. Validierung der Rollenzuweisung in den APIC-Protokollen Nach Benutzername filtern:
   <#root>

   ```
   apic1#

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

   Suchen Sie nach den Nachrichten für die Rollenzuweisung am Ende des Authentifizierungsflusses:

   Funktionierend - Der Benutzer hat die Admin-Schreibrolle (von einer echten LDAP-Anmeldung):

   ```
   ||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 (Nicht funktionsfähig): Wenn das Protokoll `keine Admin UserRole` mit `Leseberechtigungen` anstelle von `Admin Write-Berechtigungen` anzeigt, hat der Benutzer eine

schreibgeschützte Rolle und kann die Konfiguration nicht ändern. Suchen Sie nach Posten wie:

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

Wenn das Protokoll nur `Lese-` und keine `Schreibrechte` anzeigt, aktualisieren Sie die Benutzerrolle oder das AV-Paar auf dem AAA-Server.

Ursache: Der Benutzer hat eine schreibgeschützte Rolle (z. B. Read-all oder ops) anstelle einer schreibfähigen Rolle.

Lösung: Aktualisieren Sie die Rollenzuweisung des Benutzers auf dem APIC (für lokale Benutzer) oder aktualisieren Sie die Rolle **cisco-av-pair** auf dem AAA-Server (für Remote-Benutzer), um eine Rolle mit Schreibberechtigungen einzubeziehen.

Szenario: Benutzer können auf einige Tenants zugreifen, andere jedoch nicht.

Problem: Ein Benutzer kann einen Tenant sehen und verwalten, andere Tenants jedoch nicht, obwohl er Zugriff benötigt.

Verifizierungsschritte:

1. Überprüfen Sie die Sicherheitsdomänenzuweisung des Benutzers:
   <#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. Sicherheitsdomänen werden Tenants zugeordnet. Wenn der Benutzer Zugriff auf TenantB benötigt, muss er auch der Sicherheitsdomäne zugewiesen sein, die TenantB zugeordnet ist, oder er muss der Domäne all zugewiesen sein.
3. Bestätigen Sie für Remote-Benutzer, dass das AV-Paar oder die LDAP-Gruppenzuordnung die richtigen Domänen zuweist. Überprüfen Sie den APIC **nginx.bin.log** bei der Anmeldung auf die Domänenzuweisung. Nach Benutzername filtern:
   <#root>

   ```
   apic1#
   ```

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

Funktionierend: Der Benutzer verfügt über die gesamte Domäne (vollständige Transparenz) von einem echten LDAP-Anmeldenamen:

```
||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
```

Funktioniert nicht - Wenn der Benutzer nur über eine Tenant-Domäne verfügt, wird in den **Found UserDomain** Nachrichten statt "all" nur diese Domäne angezeigt. Beispielsweise bedeutet `Found UserDomain TenantA`, dass der Benutzer nur TenantA sehen kann. Der Benutzer benötigt zusätzliche Domänen, die dem AV-Paar auf dem AAA-Server hinzugefügt werden, oder alle Domänen für den vollständigen Zugriff.

Ursache: Der Benutzer wird einer eingeschränkten Sicherheitsdomäne zugewiesen, die nur bestimmte Tenants abdeckt.

Lösung: Fügen Sie der Konfiguration des Benutzers die erforderlichen Sicherheitsdomänen hinzu, oder verwenden Sie die Domäne all für den vollständigen Zugriff.

Kennwortwiederherstellung und Notfallzugriff

Wenn alle Admin-Konten gesperrt sind oder der Remote-AAA-Server nicht erreichbar ist und der Standardbereich geändert wurde, verwenden Sie eine der folgenden Wiederherstellungsmethoden:

Fallback-Anmeldedomäne

Die ACI bietet eine integrierte Fallback-Anmelde-Domäne, die unabhängig vom Standard-Authentifizierungsbereich immer die lokale Authentifizierung verwendet. So verwenden Sie es:

- SSH: Melden Sie sich an als **apic:fallback\\admin** (oder **apic#fallback\\admin** abhängig von der Version).
- GUI: Wählen Sie im Dropdown-Menü Domain (Domäne) auf dem Anmeldebildschirm die Option Fallback aus, und verwenden Sie die lokalen Anmeldeinformationen.

Konsolenzugriff

Wenn der Authentifizierungsbereich der Konsole auf "lokal" (Standard) eingestellt ist, können Sie sich immer über den APIC-Konsolen-Port mit lokalen Anmeldeinformationen anmelden. Wenn das lokale Admin-Kennwort unbekannt ist, kann es über den Cisco Integrated Management Controller (CIMC) (für physische APICs) oder die Hypervisor-Konsole (für virtuelle APICs) zurückgesetzt werden.

Anmerkung: Wenn der Authentifizierungsbereich der Konsole in einen Remote-AAA-Server geändert wurde und dieser Server nicht erreichbar ist, schlägt der Konsolenzugriff ebenfalls fehl. Dies ist ein übliches Lockout-Szenario. Behalten Sie die Konsolenauthentifizierungsrealms immer lokal bei.

Referenz zu häufigen Fehlern

Die folgenden ACI-Fehler werden häufig mit Problemen beim Remote-Zugriff und bei AAA in Verbindung gebracht:

- F1773 - Verbindungsproblem mit TACACS+-Anbietern. Der APIC kann den TACACS+-Server nicht erreichen.
- F1774 - Fehler bei der TACACS+-Authentifizierung. Der Server ist erreichbar, aber der Authentifizierungsversuch wurde abgelehnt.
- F1775 - Verbindungsproblem bei RADIUS-Anbietern.
- F1776 - RADIUS-Authentifizierungsfehler.
- F1777 - Verbindungsproblem mit LDAP-Anbietern.
- F1778 - LDAP-Authentifizierungsfehler.
- F0532 - Management-Subnetz nicht für einen Knoten konfiguriert.

Abfrage aktiver AAA-Fehler:

<#root>

```
apic1#

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

Referenzen

- Fehlerbehebung bei ACI Management und Core Services - Pod-Richtlinien
- Cisco APIC Basic Konfigurationsleitfaden, Version 6.1(x) - Verwaltung
- Cisco APIC Security Konfigurationsleitfaden - Zugriff, Authentifizierung und Abrechnung

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.