排除ACI交换矩阵中的远程访问问题

简介

本文档介绍如何验证、排除和解决思科以应用为中心的基础设施(ACI)交换矩阵中的远程访问问题。它涵盖对APIC和交换矩阵交换机的安全外壳(SSH)和超文本传输协议安全(HTTPS)访问、使用终端访问控制器访问控制系统Plus(TACACS+)的远程身份验证、授权和记帐(AAA)、远程身份验证拨入用户服务(RADIUS)、轻量目录访问协议(LDAP)和基于角色的访问控制(RBAC)授权。每个区域都包含分类决策树和详细的故障排除场景。

背景信息

本文档中的材料综合了ACI管理和核心服务故障排除 — Pod策略指南、Cisco APIC基本配置指南 6.1(x)版本 — 管理一章和Cisco APIC安全配置指南 — 访问、身份验证和记帐一章。

概述

对ACI交换矩阵的远程访问包括三个不同的层，每个层都必须让工程师成功登录并运行：

1. 传输 — 必须能够访问并启用管理网络路径（OOB或带内）和协议服务（SSH或HTTPS）。
2. 身份验证 — 必须验证用户的凭证，无论是在APIC上本地验证，还是针对远程AAA服务器（TACACS+、RADIUS或LDAP）验证。
3. 授权 — 必须为通过身份验证的用户分配正确的RBAC角色和安全域，以便查看和修改预期的ACI对象。

任何层的故障都会产生不同的症状。传输故障会完全阻止连接。身份验证失败将返回凭证错误。授权失败允许登录，但会限制可视性或在API中产生“403禁止”错误。

管理访问策略

管理访问策略(commPol)是控制交换矩阵上启用了哪些远程访问协议的中心对象。它位于Fabric > Fabric Policies > Policies > Pod > Management Access > default下。策略包含配置以下内容的子对象：

- SSH(commSsh) — 管理状态、端口、密码、密钥交换(KEX)算法、消息身份验证代码(MAC)和主

机密钥算法。
- HTTPS()-**commHttps**管理状态、端口、传输层安全(TLS)协议版本、限制速率和客户端证书身份验证。
- Telnet(**commTelnet**) — 管理状态和端口。默认情况下，Telnet处于禁用状态，Cisco建议保持禁用状态。

OOB和带内管理

ACI节点支持两种管理访问路径：

- 带外(OOB) — 使用APIC或交换机上的专用管理端口。OOB管理地址从mgmt租户下的池分配，并通过分配到节**mgmtRsOoBStNode**点。在APIC上，OOB合同通过规则实**iptables**施。如果应用OOB合同，则只有合同明确允许的流量才能到达APIC管理接口。
- 带内(INB) — 使用交换矩阵数据平面管理流量。带内管理需要网桥域(BD)、子网、终端组(EPG)、合同和节点管理地址分配。如果没有额外的路由或策略配置，则无法从交换矩阵外部访问带内IP地址。

注意：APIC OOB管理IP在初始设置期间配置，并且APIC在完全发现交换矩阵之前获得IP连接。OOB是主要管理路径，如果物理管理网络已连接，则始终可用。

AAA架构

ACI使用三层AAA模型：

1. Login Domain()-**aaaLoginDomain**在命名领域下对AAA提供程序进行分组。用户在登录屏幕指定登录域(例如，`apic:TACACS-Domain`或通过UI中的下拉列表)。特殊的回退登录域始终存在，并且映射到本地身份验证。
2. 提供商组**aaaTacacsPlusProviderGroup**(**aaaRadiusProviderGroup**,,**aaaLdapProviderGroup**) — 引用一个或多个AAA服务器并定义它们的尝试顺序。
3. 提供程**aaaTacacsPlusProvider**序(**aaaRadiusProvider**, **aaaLdapProvider**) — 定义服务器IP、端口、共享密钥（或绑定DN for LDAP）、超时、重试、管理EPG和监控凭证。

Default Authentication Realm(**aaaDefaultAuth**)确定在用户登录时未指定登录域时使用哪个登录域。控制台身份验证领域控制控制台会话的身份验证。

注意：当无法访问远程AAA服务器时，将默认身份验证领域更改为远程AAA服务器会将您锁定在交换矩阵之外。更改领域之前，请始终测试AAA服务器连接。fallback登录域(`apic:fallback\\admin`)可用于绕过默认领域并在本地进行身份验证。

关键AAA日志文件

AAA身份验证事件记录在APIC和交换矩阵交换机上的多个文件中。这些日志是验证身份验证结果、标识正在使用的领域和提供程序组以及诊断角色分配失败的主要工具。

日志文件	位置(APIC)	位置（交换机）	
nginx.bin.log(APIC) nginx.log(交换机)	/var/log/dme/log/nginx.bin.log	/var/sysmgr/tmp_logs/dme_logs/nginx.log	主AAA 份验证 域选择 LDAP 信、A 配，以 不同平 内容格
access.log	/var/log/dme/log/access.log	/var/log/dme/log/access.log	NGINX 个API ，显示 （200 ）的aa 用。 在 DME A aaaRef
pam.module.log	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	PAM模 话的身 份验证 的UNI ，这是 份验证

注意：主AAA日志在每个平台上具有不同的文件名。在APIC上，它**nginx.bin.log**位于/var/log/dme/log/。在枝叶和主干交换机**nginx.log**上，它位于/var/sysmgr/tmp_logs/dme_logs/。两个平台上的日志内容格式和AAA消息相同。

nginx日志中的AAA条目遵循以下格式：

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

过滤特定用户的身份验证流的AAA相关日志条目：

<#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
```

或查看所有最近的身份验证请求和结果：

<#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
```

典型的成功身份验证流程按顺序显示以下关键消息：

1. 收到来自nginx的PAM身份验证请求，请求用户名：<user> — 已收到登录请求。
2. DefaultAuthMo指定领域<N>。提供程序组<名称>！— 已选择领域（0=回退/本地，2=TACACS+,3=LDAP）。
3. 提供程序特定消息（LDAP绑定、TACACS+提供程序查找或RADIUS请求）。
4. 在远程用户名下找到UserDomain <domain>:<user> — 从AAA响应分配的域。
5. 找到的用户名：admin with admin write privileges under UserDomain all - user is an admin user — 已通过角色检查。

失败的身份验证日志：

- 用户<user>在AAA身份验证期间被拒绝
- Unauthorized user <user>错误：AAA服务器身份验证被拒绝

注意：nginx日志频繁旋转，较早的条目使用数字后缀进行gzip压缩。在APIC上，轮换日志位

于同一目录中(例如**nginx.bin.log.22815.gz**)。 在交换机上，旋转日志存**/var/log/dme/oldlog/dme/nginx.log.*.gz**储在(/var/sysmgr/tmp_logs/dme_logs/中有符号链接)。 要搜索循环日志，请执行以下操作：

<#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模型

ACI RBAC控制经过身份验证的用户可以查看和执行的操作。该模型有三个组成部分：

- 安全域(**aaaDomain**) — 映射到ACI对象（租户、访问策略、交换矩阵策略）的范围限制器。 内置域all、common和mgmt始终存在。自定义域将用户的可见性限制为特定租户或策略区域。
- 角色(**aaaRole**) — 定义一组权限。预构建角色包括admin、aaa、tenant-admin、tenant-ext-admin、read-all、access-admin、fabric-admin、ops和nw-svc-admin。
- 权限 — 每个角色都授予对特定功能区域的读取或写入（意味着读取）访问权限。

为用户帐户分配一个或多个安全域和角色对。对于通过TACACS+、RADIUS或LDAP进行身份验证的远程用户，角色映射通过AAA响应中的供应商特定属性（例如，属性）**cisco-av-pair**提供。

分类决策树

当用户报告无法远程访问ACI交换矩阵时，请使用此诊断树：

1. 您能否ping通APIC或交换机管理IP?
   - No →排除管理网络路径故障。请参考“排除OOB和带内管理故障”部分。
   - 是→继续。
2. 是否可以建立SSH或HTTPS连接（该连接是否完全打开）？
   - 无→协议服务可以禁用，端口可以过滤，或可能存在密码不匹配。请参考“排除SSH访问故障”或“排除HTTPS访问故障”部分。

- 是→继续。

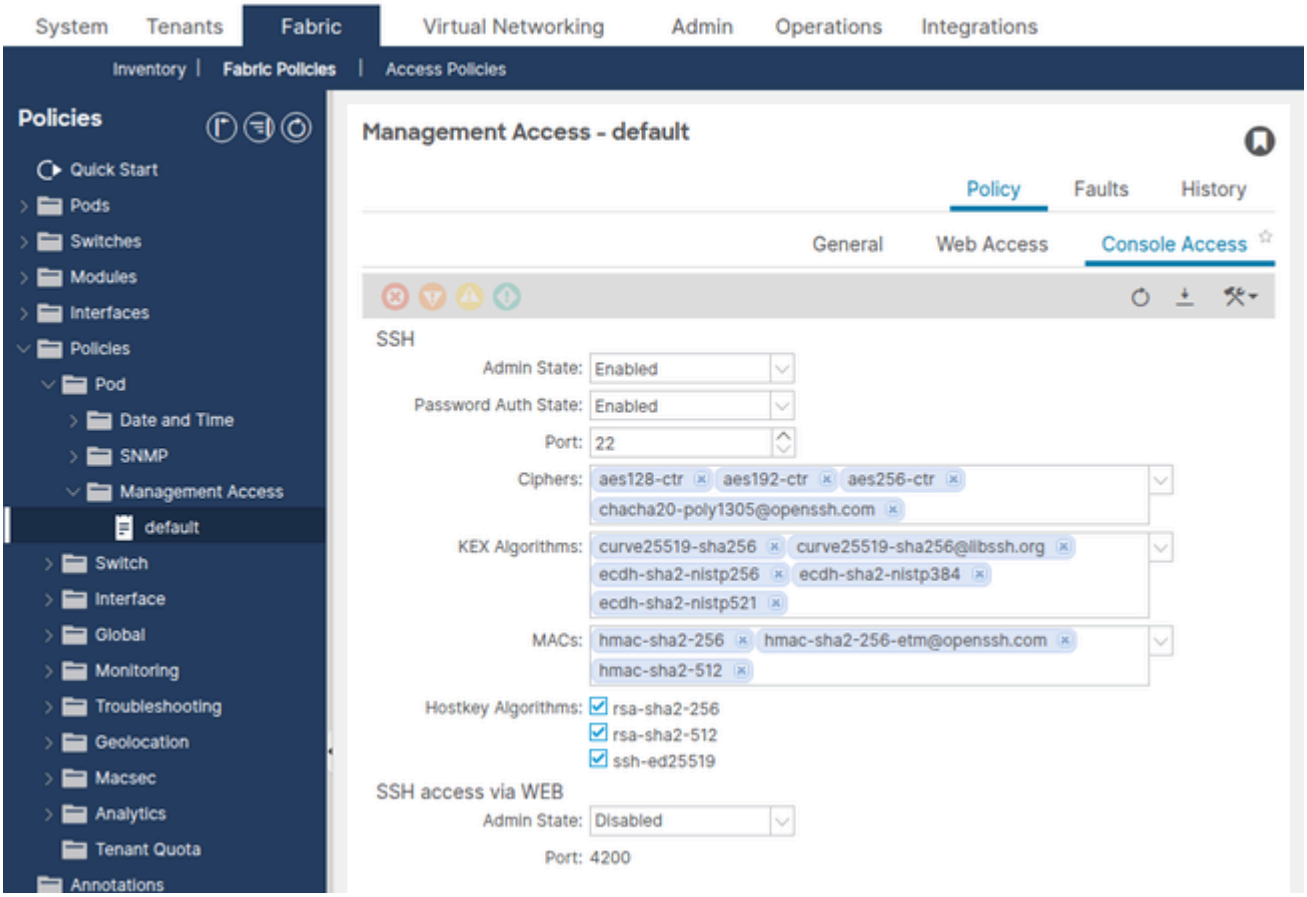
3. 登录屏幕是否显示(HTTPS)，或者SSH握手是否完成并提示输入凭证？
   - 没有→SSH密钥交换或TLS握手失败。有关密码和KEX不匹配的信息，请参阅“排除SSH访问故障”部分。
   - 是→继续。
4. 凭证是否因“身份验证失败”或类似原因而失败？
   - 是，→份验证问题。请参考“排除AAA身份验证故障”部分（TACACS+、RADIUS或LDAP，具体取决于使用的登录域）。
   - 不→继续。
5. 用户是否登录但看不到预期对象，或收到“403已禁止”错误？
   - 是→权或RBAC问题。请参考“排除RBAC和用户权限故障”部分。
   - 无→访问有效。验证用户遇到的特定问题。

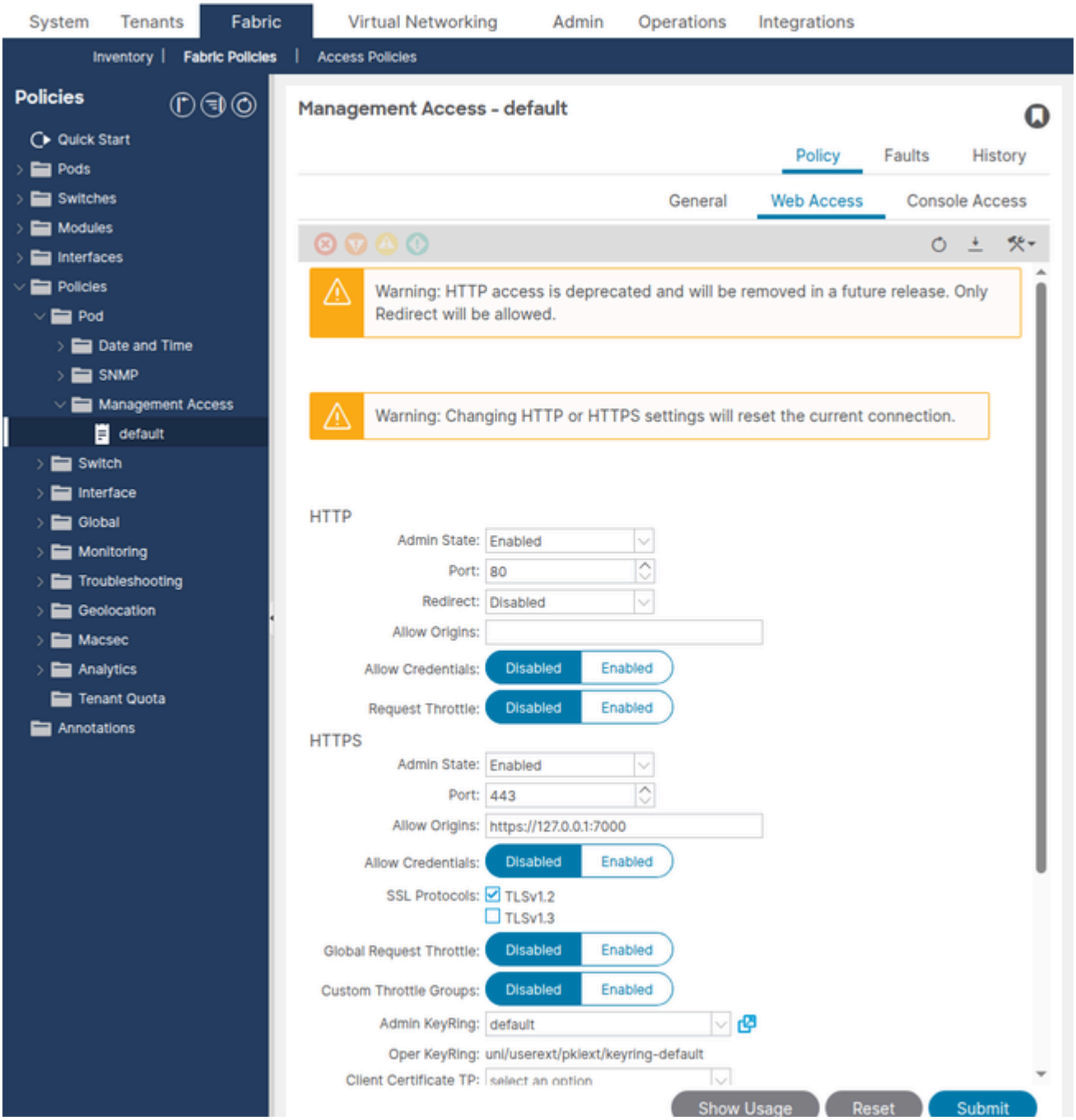
验证配置

在对运行状态进行故障排除之前，请验证配置链是否完整。配置错误是远程访问问题最常见的根本原因。

验证管理访问策略（SSH和HTTPS）

导航到交换矩阵>交换矩阵策略>策略> Pod >管理访问>默认。


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



确认以下SSH设置：

- 管理状态 — 必须启用。
- Port — 默认22。如果更改，SSH客户端必须使用自定义端口。
- Password Authentication — 启用（除非需要仅证书身份验证）。
- SSH密码 — 必须包括SSH客户端支持的至少一个密码。
- KEX Algorithms — 必须至少包括SSH客户端支持的一种算法。
- SSH MACs — 必须至少包含一个SSH客户端支持的MAC。

通过API查询SSH托管对象：

<#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
```

确认以下HTTPS设置：

- 管理状态 — 必须启用。
- 端口 — 默认443。
- SSL协议- TLSv1.2（默认）。 较旧的客户端可能需要显式添加TLSv1.1。
- 限制状态 — 如果启用，限制速率将限制每个用户的每秒请求数。值非常低可能会导致API超时错误。

<#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
```

常见错误配置

- SSH密码限制过于严重 — 在ACI版本5.2(1)及更高版本中，默认的SSH密码被强化。较旧的SSH客户端（例如，0.75之前的PuTTY版本或仅提供的OpenSSH版本）**diffie-hellman-group14-sha1**可能会使密钥交换失败。SSH客户端显示“未找到匹配的密码”或“未找到匹配的密钥交换方法”。
- 禁用密码身份验证**passwordAuth**如果设置为禁用，则仅允许基于SSH密钥的身份验证。使用密码连接的用户将看到“Permission denied(publickey)”。
- 无客户端感知的自定义SSH端口 — 如果SSH端口从22更改，则SSH客户端必须指定新端口(例如**ssh -p 2222 admin@10.1.1.1**)。

检验OOB管理地址

导航到租户>管理>节点管理地址。

确认每个APIC和交换机节点都分配有一个带有效网关的OOB管理IP地址。没有管理地址的节点将无法通过管理网络访问。

通过API查询OOB静态节点分配：

<#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
```

常见错误配置

- 缺少OOB地址分配 — 交换机下没有条**mgmtRsOoBStNode**目。节点没有管理IP，并且不会响应OOB接口上的SSH或HTTPS。
- 网关不正确 — 网关地址与OOB管理网络上的实际网关不匹配。节点可以接收数据包，但无法发送返回流量。
- 子网掩码不匹配 — OOB子网掩码与物理管理网络不匹配。这会导致节点认为管理站位于不同的子网上，并通过不存在或不正确的网关路由流量。

验证OOB合同

导航到租户>管理>合同。

如果OOB合同应用到OOB管理EPG，则只有该合同明确允许的流量才会到达APIC管理接口。在APIC上，OOB合同通过规则实**iptables**施。

查询OOB EPG提供的合同：

<#root>

```
apic1#
```

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

如果查询返回结果，则应用合同。验证合同主题和过滤器是否允许所需的协议：

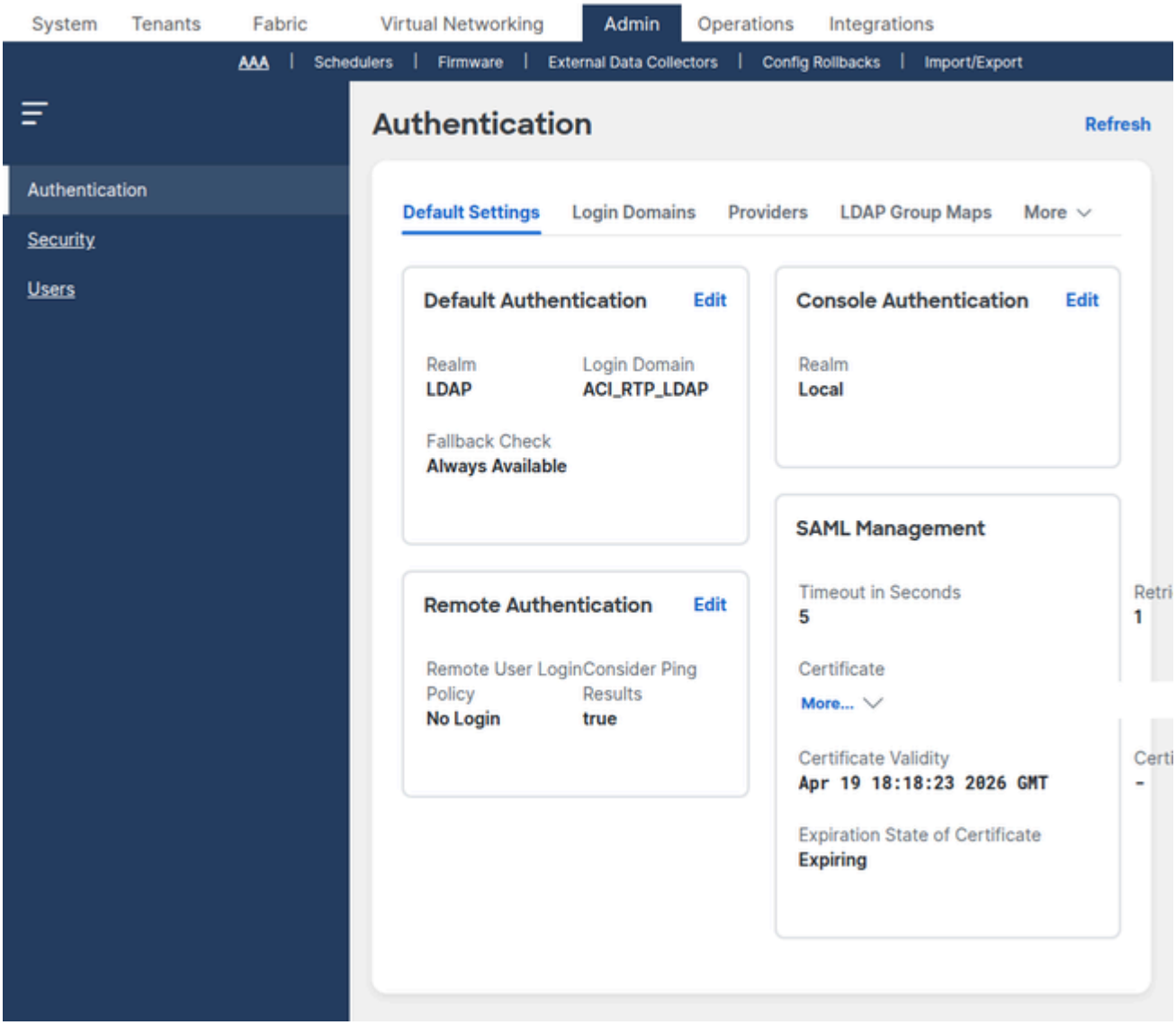
- SSH - TCP端口22（或自定义端口）
- HTTPS - TCP端口443（或自定义端口）
- ICMP — 用于ping验证

常见错误配置

- OOB合同不包括SSH或HTTPS -工程师可以ping通APIC，但无法通过SSH或HTTPS进行连接。APIC上iptables的规则以静默方式丢弃流量。
- OOB合同过滤器中的源IP限制 — 合同过滤器限制对特定源子网的访问。该子网外的工程师无法连接。

验证AAA配置

导航到Admin > AAA > Authentication > AAA。



确认以下内容：

- Default Authentication Realm — 标识用户未指定登录域时使用哪个登录域。如果设置为远程AAA登录域，必须可访问相应的服务器。
- 控制台身份验证领域(Console Authentication Realm) — 控制控制台访问。如果设置为local，则控制台登录始终使用本地凭证（推荐）。

验证登录域

导航到Admin > AAA > Authentication > Login Domains。

<#root>

```
apic1#
```

moquery -c aaaLoginDomain

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

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

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

验证用于身份验证的登录域是否存在，并且它引用了正确的提供程序组。

验证TACACS+提供程序

导航到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
```

验证RADIUS提供程序

导航到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
```

验证LDAP提供程序

导航到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
```

常见AAA配置错误

- 共享密钥不匹配 — ACI TACACS+或RADIUS提供程序上配置的密钥与服务器上的密钥不匹配。身份验证以静默方式失败。
- 管理EPG错误 — 提供商的EPG为空或指向错误的EPG(例如，当服务器位于OOB网络时，处于带内**epgDn**)。 APIC无法到达服务器。
- 登录域领域不匹配 — 登录域配置为LDAP，但用户需要TACACS+身份验证。登录域必须引用正确的提供程序组类型。
- LDAP绑定DN不正确**rootdn** — （绑定DN）或**basedn**错误。LDAP身份验证失败，出现绑定错误，即使用户凭据正确也是如此。
- LDAP过滤器与目录架构不匹配 — 对于Active Directory，请使用**sAMAccountName=$userid**。对于OpenLDAP，使**cn=$userid**用或**uid=$userid**。

验证RBAC配置

导航到Admin > AAA > Users以查看本地用户帐户及其安全域和角色分配。

通过API查询安全域：

<#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
```

分配给domain all并具有admin角色的用户对整个交换矩阵具有完全读写访问权限。分配至角色为tenant-admin的自定义安全域的用户只能管理与该域关联的租户。

常见RBAC配置错误

- 创建没有安全域的用户 — 用户可以登录，但看不到租户，并且在API调用中收到“403 Forbidden”。必须至少分配一个安全域。
- 在需要写入访问权限时分配的只读角色 — 用户可以查看对象，但不能提交更改。验证角色权限是否设置为writePriv。
- AAA服务器中缺少远程用户角色映射 — TACACS+或RADIUS服务器不返回包含**cisco-av-pair**的属性**shell:domains=all/admin/**。用户身份验证成功，但没有任何角色，并且在交换矩阵中看不到任何内容。

排除OOB和带内管理故障

如果网络中无法访问APIC或交换机管理IP，请在调查SSH、HTTPS或AAA之前先对管理路径进行故障排除。

场景:无法Ping APIC OOB IP

问题：管理站无法ping APIC OOB管理IP地址。

验证步骤:

1. 验证APIC管理端口是否物理连接且链路是否打开。
2. 检验管理站是否在同一个L2网段上，或者是否有到OOB子网的路由。
3. 验证是否已正确分配OOB管理IP:
   <#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. 验证默认网关是否可访问：
   <#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. 如果应用了OOB合同，请验证它是否允许所需的协议。按照“验证OOB合同”部分所示，查询OOB EPG提供的合同。OOB合同作为APIC$_{iptables}$上的规则实施。您可以从APIC外壳查看保存的规则：
   <#root>

```
apic1#

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

   如果INPUT策略为DROP，并且所需协议没有ACCEPT规则，则OOB合同将过滤流量。

> 注意：查看$_{iptables\ -L\ -n}$实时内核规则的命令需要根访问权限，并且不适用于常规管理SSH会话。

根本原因：OOB管理地址缺失或配置错误、网关不正确或OOB合同过滤流量。

解决方案：更正OOB地址分配，验证物理网络路径，或者更新OOB合同以允许所需的协议。

场景:无法访问交换机管理IP

问题：管理站可以到达APIC，但无法通过OOB到达交换机。

验证步骤:

1. 验证交换机是否已分配OOB地址：
   <#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. 验证交换机管理接口是否已分配了IP:
   <#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. 验证管理VRF默认路由：
   <#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
```

根本原因：缺少OOB地址分配、网关不正确或交换机管理物理端口关闭。

解决方案：在Tenants > mgmt > Node Management Addresses下分配OOB地址。检验物理管理链路是否打开。

排除SSH访问故障

本节介绍可访问管理IP（ping成功）但SSH会话无法建立或进行身份验证的场景。

场景:SSH连接被拒绝

问题：SSH客户端在连接到APIC或交换机时报告“连接被拒绝”。

验证步骤:

1. 验证管理访问策略中是否启用了SSH:
   <#root>

```
apic1#
```

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

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

如果**adminSt**为disabled，则会拒绝SSH连接。

2. 检验是否使用了正确的端口。如果SSH端口从22:
   <#root>

   $

   ssh -p

   custom-port

   admin@10.1.1.1

3. 检验OOB合同是否允许SSH端口上的TCP。请参阅“验证OOB合同”部分。

根本原因：在管理访问策略中禁用SSH，客户端不知道自定义端口，或OOB合同过滤。

解决方案：在管理访问策略中启用SSH或使用正确的端口。

场景:SSH密钥交换故障（密码或KEX不匹配）

问题：SSH客户端失败并显示“未找到匹配的密码”、“未找到匹配的密钥交换方法”或“未找到匹配的MAC”。

验证步骤:

1. 检查SSH客户端详细输出，以确定客户端提供哪些算法：
   <#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. 比较客户端提供的算法与APIC配置的算法：
   <#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. 确定交叉点。如果任何类别中没有通用算法，握手将会失败。

注意：在ACI版本5.2(1)及更高版本中，默认的SSH密码和KEX算法得到了强化。默认情况下不**diffie-hellman-group1-sha1**再**diffie-hellman-group14-sha1**提**aes128-cbc**供、**hmac-sha1**和等传统算法。如果最近进行了升级，请验证环境中的SSH客户端是否支持新的默认值。

根本原因：在ACI升级或密码强化后，SSH客户端和APIC之间没有通用密码、KEX算法或MAC。

解决方案：更新SSH客户端以支持现代算法，或者将所需的传统算法重新添加到管理访问策略。重新添加传统算法会带来安全风险，不建议长期使用。

场景:SSH连接，但本地用户的身份验证失败

问题：SSH握手成功（出现密码提示），但本地用户的密码被拒绝。

验证步骤:

1. 验证用户是否本地存在：
   <#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. 检查帐户是否由于登录尝试失败次数过多而被锁定：
   <#root>

```
apic1#

moquery -c aaaUserEp

dn                : uni/userext
pwdStrengthCheck  : no
```

   在Admin > AAA > Security Management > Lockout Policy下检查登录域锁定策略。

3. 验证用户是否使用正确的登录域登录。如果Default Authentication Realm设置为远程AAA登录域，则用户必须预置或**apic:LOCAL\\username**以**apic:fallback\\username**强制进行本地身份验证。
4. 验证日志中的身份验证结果。在**nginx.bin.log**APIC上检查登录事件：
   <#root>

   apic1#

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

   查找分配给登录尝试的领域和提供程序组：

```
! 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
```

   如果领域不是0（回退/本地），则登录被发送到远程AAA服务器而不是本地数据库。用户必须预置**apic:fallback\\username**或**apic:LOCAL\\username**才能强制进行本地身份验证。

根本原因：密码不正确、帐户被锁定，或者正在将登录尝试发送到远程AAA服务器而不是本地数据库。

解决方案：重置密码、解锁帐户或使用正确的登录域前缀。

排除HTTPS访问故障

本节介绍无法通过HTTPS访问APIC Web UI或具象状态传输(REST)应用编程接口(API)的场景。

场景:HTTPS连接超时

问题：浏览器显示“ERR_CONNECTION_TIMED_OUT”或API调用在连接到端口443上的APIC时挂起。

验证步骤:

1. 验证是否已启用HTTPS:
   <#root>

   ```
   apic1#

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

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

2. 验证OOB合同允许TCP 443。请参阅“验证OOB合同”部分。
3. 从APIC自身进行测试，以确认HTTPS进程正在侦听：
   <#root>

   ```
   apic1#

   ss -tlnp | grep 443

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

根本原因：HTTPS已禁用、OOB合同过滤TCP 443或APIC上的nginx进程已崩溃。

解决方案：在管理访问策略中启用HTTPS、更新OOB合同或重新启动APIC上的Web服务。

场景:浏览器显示TLS握手错误

问题：浏览器显示“ERR_SSL_VERSION_OR_CIPHER_MISMATCH”或类似的TLS错误。

验证步骤:

1. 检查APIC上配置的TLS协议版本：
   <#root>

   ```
   apic1#

   moquery -c commHttps

   sslProtocols : TLSv1.2
   ```

2. 验证浏览器是否支持TLSv1.2。非常旧的浏览器（例如，Internet Explorer 10及更早版本）默

认不支持TLSv1.2。

根本原因：APIC仅提供TLSv1.2（默认值），而浏览器或API客户端仅支持较旧的TLS版本。

解决方案：更新浏览器或客户端。如果必须临时支持较旧的客户端，请将TLSv1.1添加到管理访问策略，但这会导致安全风险。

场景:API限制限制

问题：REST API调用间歇性失败，出现HTTP 503错误，或者Web UI在繁重的自动化过程中变得迟缓。

验证步骤:

<#root>

```
apic1#

moquery -c commHttps

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

如果限制速率非常低且自动化脚本每秒发送许多请求，则APIC将拒绝超额请求。

根本原因：对于自动化工作负载，每用户限制速率过低。

解决方案：在管理访问策略下增加限制速率，或优化自动化脚本以降低请求频率。或者，如果未共享交换矩阵，请禁用限制。

排除AAA故障 — TACACS+

本节介绍TACACS+身份验证失败。APIC通过TCP端口49与TACACS+服务器通信。

操作验证

ACI交换机不支持在独test aaa立NX-OS上可用的命令。要验证TACACS+操作，请使用APIC检查提供程序状态、故障和登录会话历史记录。

检查TACACS+提供程序上的活动故障：

```
<#root>

apic1#

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

如果未返回错误，APIC会认为提供商可访问。如果存在故障，输出包括故障代码，例如F1773（提供程序无法访问）或F1774（身份验证失败）。

验证TACACS+提供程序配置：

```
<#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
```

验证从APIC到TACACS+服务器的基本网络连通性：

```
<#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
```

尝试使用TACACS+登录域登录APIC并检查会话结果：

```
<#root>

apic1#

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

查看字段**descr**以确定故障是由于身份验证拒绝还是连接问题引起的。

验证APIC日志中的TACACS+身份验证流程。过滤有关用户名：

<#root>

apic1#

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

TACACS+登录遵循与LDAP相同**nginx.bin.log**的身份验证流程（请参阅LDAP操作验证部分以了解完整的实际日志示例）。 TACACS+的主要区别包括：

- DefaultAuthMo指定领域2 — 领域2表示TACACS+（与LDAP的领域3相比）。
- 将TacacsProvider <IP>添加到列表 — 标识所联系的TACACS+服务器(与LDAP的LdapProvider相比)。
- TACACS+ Cisco-avpair(shell:domains=all/admin/)- AV对直接由TACACS+服务器返回（与从LDAP组映射转换时相比）。

成功的TACACS+登录显示相同的进度：PAM请求→域选择→提供→查找AV对解析→户注入→UserDomain和角色分配→管理员写入权限。

failed TACACS+登录以User <username> is denied during AAA authentication和Unauthorized ... 错误结束：AAA Server Authentication DENIED，与LDAP拒绝的模式相同。

场景:TACACS+身份验证失败

问题：当用户选择TACACS+登录域时，登录失败并显示“Authentication Failed”。

验证步骤:

1. 检查TACACS+提供程序上的活动故障：
   <#root>

   apic1#

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

   故障F1773指示连接问题。故障F1774表示身份验证被拒绝。

2. 验证从APIC到TACACS+服务器的网络连通性：
   <#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. 如果ping成功，但身份验证失败，请验证APIC提供程序配置和TACACS+服务器配置上的共享密钥是否匹配。
4. 检查最近的登录会话以查看故障详细信息：
   <#root>

   apic1#

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

5. 检查TACACS+服务器日志以尝试进行身份验证。在服务器上成功登录但被拒绝的尝试表示在服务器端存在用户配置问题（例如，密码不匹配或缺少用户帐户）。
6. 检查APIC的**nginx.bin.log**完整身份验证流程。按用户名而不是特定关键字进行过滤，这样中间消息不会丢失：
   <#root>

   apic1#

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

   将上面的操作验证部分中的输出与正常运行示例和非正常运行示例相比较。主要指标：

   - 被拒绝或DENIED — 已到达TACACS+服务器，但拒绝了凭证。验证服务器上是否存在该用户，并且密码是否匹配。
   - 添加TacacsProvider后没有特定于提供程序的消息 — 服务器无法访问或超时。检验网络连通性和管理EPG。
   - 已完成远程用户注入，然后是角色检查行 — 身份验证成功，但可能是与角色分配有关的问题（请参阅下面的AV对部分）。

TACACS+ cisco-av-pair，用于RBAC

对于通过TACACS+进行身份验证的远程用户，服务器必须在授**cisco-av-pair**权响应中返回属性。此属性将用户映射到ACI安全域和角色。

Format:

shell:domains=*domain/role/*

示例：

- 完全管理员： **shell:domains=all/admin/**
- 全部为只读： **shell:domains=all/read-all/**
- 特定域的租户管理员： **shell:domains=TenantA/tenant-admin/**
- 多个域： **shell:domains=all/admin/,TenantA/tenant-admin/**

如果此属性缺失或格式不正确，则用户成功进行身份验证，但没有角色，并且在APIC UI中看不到任何对象。

注意：对枝叶和主干交换机的SSH访问需要具有write权限的admin角色在all security域中。交换机SSH访问的最低AV对为**shell:domains=all/admin/**1。具有非管理员角色(例如，read-all、tenant-admin、aaa)的用户或分配到all以外的安全域的用户可以登录到APIC，但被拒绝对交换机的SSH访问。APIC日志显示这些用户拒绝交换机上的非管理员登录。

通过检查验证收到的AV对**nginx.bin.log**。按用户名过滤，以查看完整角色注入流程：

<#root>

apic1#

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

对于TACACS+,AV对记录为TACACS+ Cisco-avpair(shell:domains=...)。成功注入显示已完成远程用户<username>的注入，然后是Found UserDomain和admin write privileges行(请参阅LDAP操作验证(LDAP Operational Verification)部分，以获取具有实际日志输出的此流的完整示例)。

如果AV对格式无效，日志显示Injection of remote user <username> data FAILED – 错误消息为Invalid shell:domains string。如果用户使用非管理员角色进行身份验证，则到交换机的SSH会被拒绝，而交换机上的非管理员登录会被拒绝。

根本原因：共享密钥不匹配、服务器无法从管理网络访问、TACACS+服务器上不存在用户，或者提供商上的管理EPG不正确。

解决方案：更正共享密钥、修复可达性，或在TACACS+服务器上创建用户。

验证枝叶交换机身份验证日志

在枝叶和主干交换机上，SSH登录事件同时在和中**pam.module.log**记**nginx.log**录。显示**pam.module.log**PAM身份验证结果（接受或拒绝）。 包含**nginx.log**与APIC上相同的完整AAA流(领域选择、提供程序查找、LDAP/TACACS+/RADIUS通信、AV对分析和角色分配**nginx.bin.log**)。这些日志适用于所有远程AAA类型(TACACS+、RADIUS、LDAP)。

检查**pam.module.log**身份验证结果：

<#root>

```
leaf101#

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

工作 — 交换机上的远程身份验证成功：

```
||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
```

该标**remote=1**记确认用户已通过远程AAA服务器的身份验证。

未工作 — 用户被拒绝。securitymgrAG拒绝用户，并且交换机尝试查找本地用户作为最终回退：

```
||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
```

如果用户根本未显示PAM条目，则在到达PAM阶段之前（例如，由于密码不匹配或用户取消连接），SSH连接可能已被拒绝。

有关交换机上的身份验证流的更详细视图，请检nginx.log查。此日志包含完整的AAA决策链 — 格式和消息与APICnginx.bin.log上相同：

<#root>

leaf101#

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

工作 — 交换机上的LDAP身份验证成功（与“LDAP操作验证”部分中的APIC LDAP示例相比较 — 消息相同）：

```
||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
```

当显示nginx.log拒绝但不解释pam.module.log原因时，该开关特别有用。nginx.log显示AAA领域、提供程序和特定故障原因（例如，LDAP搜索返回为空、TACACS+超时或AV对注入失败）。

排除AAA故障 — RADIUS

本节介绍RADIUS身份验证失败。APIC通过UDP端口1812（身份验证）和UDP端口1813（记帐）与RADIUS服务器通信。

操作验证

ACI交换机不支持在独test aaa立NX-OS上可用的命令。使用以下方法验证RADIUS操作。

验证来自枝叶交换机的RADIUS服务器配置和可达性统计信息：

<#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
```

场景:RADIUS身份验证失败

问题：当用户选择RADIUS登录域时，登录失败。

验证步骤:

1. 检查交换机的RADIUS服务器统计信息是否有超时或故障迹象：
   <#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
   ```

   requests timed out下的高计数表示RADIUS服务器不可达或共享密钥不匹配（RADIUS在共享密钥不匹配时以静默方式丢弃数据包）。

2. 验证与RADIUS服务器的网络可达性：
   <#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. 验证APIC和RADIUS服务器之间的共享密钥匹配。与使用TCP并报告连接故障的TACACS+不

同，RADIUS使用UDP，并在共享密钥不匹配时以静默方式丢弃数据包。唯一的症状是超时。

4. 检查RADIUS服务器日志。在调试模式(**radiusd -X**)下的FreeRADIUS显示每个请求，并指示其是否被接受、拒绝或共享密钥不匹配。
5. 检查APIC**nginx.bin.log**以获取RADIUS身份验证流程。按用户名过滤：
   <#root>

   apic1#

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

   RADIUS登录遵循与LDAP**nginx.bin.log**和TACACS+相同的身份验证流程（请参阅LDAP操作验证部分了解完整的实际日志示例）。 RADIUS的主要区别是：

   - 将RadiusProvider <IP>添加到列表 — 标识RADIUS服务器(与TacacsProvider或LdapProvider)。
   - RADIUS的领域编号因配置而异。

   成功的RADIUS登录以远程用户的注入结束……已完成，并具有管理员写入权限。

   在AAA身份验证和DENIED期间，拒绝了失败的RADIUS登录以。

   如果添加RadiusProvider行后未显示特定于RADIUS的消息，则服务器超时。与使用TCP并报告连接故障的TACACS+不同，RADIUS使用UDP，并在共享密钥不匹配时以静默方式丢弃数据包。唯一的症状是超时和拒绝。

6. 检查RADIUS提供程序上的活动故障：
   <#root>

   apic1#

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

用于RBAC的RADIUS cisco-av-pair

RADIUS使用与TACACS+**cisco-av-pair**相同的属性进行RBAC角色映射。RADIUS服务器必须在Access-Accept响应中返回此属性：

<#root>

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

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

在FreeRADIUS中，该文件或LDAP**users**后端配置。对于ISE，在授权配置文件下将其配置为高级属性。

根本原因：共享密钥不匹配（最常用于RADIUS — 导致静默超时）、服务器无法访问、身份验证端口不正确或RADIUS服务器上缺少用户帐户。

解决方案：更正共享密钥，验证UDP 1812可达性，或在RADIUS服务器上配置用户。

排除AAA故障 — LDAP

本节介绍LDAP身份验证失败。APIC通过TCP端口389(LDAP)或TCP端口636（使用SSL的LDAPS）连接到LDAP服务器。

操作验证

ACI交换机不支持在独**test aaa**立NX-OS上可用的命令。要验证LDAP操作，请从APIC检查提供程序故障和配置。

检查LDAP提供程序上的活动故障：

<#root>

apic1#

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

故障F1777指示连接问题。故障F1778表示身份验证或绑定失败。如果未返回错误，APIC会认为提供商可访问。

验证到LDAP服务器的基本网络连通性：

<#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
```

对于LDAP，还要验证到端口389的TCP连接（对于LDAPS，则为636）。 如果APIC可以ping服务器，但LDAP故障仍然存在，则问题通常是不正确的绑定DN、错误的密码或防火墙阻止LDAP端口。

验证APIC日志中的LDAP身份验证流程。按用户名过滤：

<#root>

apic1#

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

工作 — 成功的LDAP登录显示完整的搜索、绑定和角色分配流程：

```
||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
```

未工作 — 在LDAP目录中找不到用户（搜索返回空集）：

```
||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
```

场景:LDAP身份验证失败

问题：当用户选择LDAP登录域时，登录失败。

验证步骤:

1. 从APIC验证LDAP服务器可达性：
   <#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. 检查活动的LDAP提供程序故障：
   <#root>

   ```
   apic1#

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

3. 验证LDAP提供程序配置：
   <#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. 验证用户是否存在于已配置基本DN下的LDAP目录中，并与过滤器匹配。对于Active Directory，用户的属性必须**sAMAccountName**与登录时输入的用户名匹配。对于OpenLDAP，或属**cn**性**uid**必须匹配。
5. 如果使用LDAPS（端口636），请验证SSL证书链。如果**SSLValidationLevel**设置为strict，如果服务器证书不受信任或已过期，APIC将拒绝连接。
6. 检查APIC以**nginx.bin.log**了解完整的LDAP身份验证流程。按用户名过滤，这样中间消息不会丢失：
   <#root>

   ```
   apic1#

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

   将上面的操作验证部分中的输出与正常运行示例和非正常运行示例相比较。通过广泛搜索日志可以找到其他特定于LDAP的故障模式：

   <#root>

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

常见的非工作模式（与以上完整流程的操作验证示例进行比较）：

```
! 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
```

要查找的其他LDAP故障模式：

- LDAP搜索超时(服务器无法访问、速度缓慢或防火墙阻止端口389/636) — 查找Ldap搜索失败：ldap_search_ext_s的返回代码：-5：超时
- 绑定失败（根或绑定密码不正确，或者服务器拒绝连接） — 查找Ldap搜索失败：ldap_search_ext_s的返回代码：-1：无法联系LDAP服务器
- 找到用户，但密码错误（与用户密码绑定失败） — 日志显示LDAP记录DN行，但后跟拒绝消息，且没有Bind to UserDN ...成功行数。

RBAC的LDAP组映射

LDAP使用组映射而非属**cisco-av-pair**性。LDAP提供程序的字**attribute**段指定包含组信息的LDAP属性。对于Active Directory，这通常是**memberOf**的。

APIC将返回的组DN与配置的LDAP组映射规则(**aaaLdapGroupMapRule**)进行匹配，以便分配适当的安全域和角色。如果没有匹配的组映射规则，则用户进行身份验证，但没有角色。

或者，可以将设置为**attribute,CiscoAVPair**并将值直接存储在用户的LDAP属性**shell:domains=all/admin/**中，该属性采用与TACACS+和RADIUS相同的格式。

根本原因：绑定DN或密码不正确、基本DN不包含用户、搜索筛选器与目录架构不匹配、LDAPS证书验证失败或缺少组映射规则。

解决方案：更正提供商配置（绑定DN、基本DN、过滤器、SSL设置）。 对于RBAC问题，请验证组映射规则是否与用户所属的LDAP组匹配。

排除RBAC和用户权限故障

本部分介绍用户成功进行身份验证但不具备预期访问级别的情况。

场景:用户已登录，但看不到租户

问题：远程用户通过TACACS+、RADIUS或LDAP登录。登录成功，但用户在UI中看不到租户，并且API调用返回空结果或“403 Forbidden”。

验证步骤:

1. 检查用户会话，查看登录时分配了哪些角色：
   <#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
   ```

   该字**descr**段显示登录结果。如果用户身份验证成功，但没有RBAC角色，则AAA服务器未返回有效或**cisco-av-pair**LDAP组映射匹配。

2. 检查APIC以**nginx.bin.log**查看登录期间的AV对和角色分配。按用户名过滤：
   <#root>

   ```
   apic1#

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

   查找角色注入和域分配消息：

   工作 — 从LDAP组映射转换的AV对，用户获得管理员角色：

   ```
   ||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
   ```

   不工作 — 如果流**Cisco-avpairConverted to CiscoAVPair**中未显示或行，则AAA服务器未返回该属性，并且未匹配LDAP组映射规则。查找**Checking all UserDomains**后面没**Found UserDomain**有行 — 用户已通过身份验证但没有角色分配。如果出现**Injection ... data FAILED**消息，则AV对字符串格式无效。

3. 验证AAA服务器正在返cisco-av-pair回属性（对于TACACS+或RADIUS）或正确的LDAP组成员身份（对于LDAP）。 检查AAA服务器配置：
   - TACACS+:验证用户配置文件包cisco-av-pair含的格式为shell:domains=all/admin/否。
   - RADIUS:验证Access-Accept中返回Cisco-AVPair = "shell:domains=all/admin/"的用户配置文件。
   - LDAP:验证用户是否是与已配置的LDAP组映射规则()匹配的LDAP组的成员aaaLdapGroupMapRule。
4. 如果属性存在，但用户仍然没有访问权限，请验证属性中的安全域名是否与APIC上的现有安全域匹配：
   <#root>

   ```
   apic1#

   moquery -c aaaDomain
   ```

   如果引cisco-av-pair用不存在的域（例如），则角色分shell:domains=NonExistentDomain/admin/配将以静默方式失败。

根本原因：AAA服务器不返回RBAC映射属性，属性格式不正确，或者APIC上不存在属性中引用的安全域。

解决方案：配置AAA服务器以返回正确的cisco-av-pair或组映射。验证APIC上是否存在安全域。

场景:用户可以查看但不能修改配置

问题：用户可以登录和浏览对象，但在用户尝试提交更改时收到错误。

验证步骤:

1. 检查用户的角色分配：
   <#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. 如果用户需要写入权限，则角色必须授writePriv予。具有写入权限的常见角色包括admin、tenant-admin、access-admin和fabric-admin。
3. 验证APIC日志中的角色分配。按用户名过滤：
   <#root>

   ```
   apic1#
   ```

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

在身份验证流程结束时查找角色分配消息：

工作 — 用户具有管理员写入角色（通过实际LDAP登录）：

```
||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
```

不工作 — 如果日志显示具有读取权限而不是admin write权限的非admin UserRole，则用户具有只读角色且无法修改配置。查找以下行：

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

如果日志仅显示read privileges而没有write privileges，请更新AAA服务器上的用户角色或AV对。

根本原因：用户具有只读角色(例如，read-all或ops)，而不是可写角色。

解决方案：在APIC上更新用户的角色分配（适用于本地用户）或在AAA服务器上更新**cisco-av-pair**（适用于远程用户），以包括具有写入权限的角色。

场景:用户可以访问某些租户，但不能访问其他租户

问题：用户可以查看和管理一个租户，但无法查看其他租户，即使这些租户需要访问权限。

验证步骤:

1. 检查用户的安全域分配：
   <#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. 安全域映射到租户。如果用户需要访问TenantB，还必须将其分配给与TenantB关联的安全域，或将其分配到所有域。
3. 对于远程用户，请确认AV对或LDAP组映射分配正确的域。登录时**nginx.bin.log**检查APIC的域分配。按用户名过滤：
   <#root>

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

   工作 — 用户从实际LDAP登录拥有所有域（完全可视性）：

   ```
   ||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
   ```

   不工作 — 如果用户只有单个租户域，则消息中只会显示该域**Found UserDomain**，而不是所有域。例如，`Found UserDomain TenantA`表示用户只能看到TenantA。用户需要向AAA服务器上的AV对添加额外的域，或者需要为all域进行完全访问。

根本原因：用户被分配到只包含特定租户的受限安全域。

解决方案：将所需的安全域添加到用户的配置中，或者使用all域进行完全访问。

密码恢复和紧急访问

如果所有管理员帐户被锁定或远程AAA服务器不可访问且默认领域已更改，请使用以下恢复方法之一：

回退登录域

ACI提供始终使用本地身份验证的内置回退登录域，而不考虑默认身份验证领域。要使用它，请执行以下操作：

- SSH：登录身份**apic:fallback\\admin**(或根**apic#fallback\\admin**据版本而定)。
- GUI:在登录屏幕的Domain（域）下拉列表中，选择fallback并使用本地凭证。

控制台访问

如果Console Authentication Realm设置为local（默认值），则始终可以使用本地凭证通过APIC控制台端口登录。如果本地管理员密码未知，可以通过思科集成管理控制器(CIMC)（用于物理APIC）或虚拟机监控程序控制台（用于虚拟APIC）重置密码。

注意：如果控制台身份验证领域已更改为远程AAA服务器，并且该服务器无法访问，则控制台访问也将失败。这是一个常见的锁定场景。始终将控制台身份验证领域设置为local。

常见故障参考

以下ACI故障通常与远程访问和AAA问题相关：

- F1773 - TACACS+提供程序连接问题。APIC无法到达TACACS+服务器。
- F1774 — TACACS+身份验证失败。服务器可访问，但拒绝身份验证尝试。
- F1775 — RADIUS提供程序连接问题。
- F1776 — RADIUS身份验证失败。
- F1777 — LDAP提供程序连接问题。
- F1778 — LDAP身份验证失败。
- F0532 -没有为节点配置管理子网。

查询活动AAA故障：

<#root>

apic1#

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

参考

- 排除ACI管理和核心服务故障 — Pod策略
- 思科APIC基本配置指南，版本6.1(x) — 管理
- 思科APIC安全配置指南 — 访问、身份验证和记帐

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。