ACI 패브릭에서 원격 액세스 문제 해결

소개

이 문서에서는 Cisco ACI(Application Centric Infrastructure) 패브릭에서 원격 액세스 문제를 확인, 트러블슈팅, 해결하는 방법에 대해 설명합니다. APIC 및 패브릭 스위치에 대한 SSH(Secure Shell) 및 HTTPS(Hypertext Transfer Protocol Secure) 액세스, TACACS+(Terminal Access Controller Access-Control System Plus), RADIUS(Remote Authentication Dial-In User Service), LDAP(Lightweight Directory Access Protocol) 및 RBAC(Role-Based Access Control) 권한 부여를 통한 원격 AAA(Authentication, Authorization and Accounting) 등을 다룹니다. 각 영역에 대한 분류 결정 트리와 자세한 문제 해결 시나리오가 포함되어 있습니다.

배경 정보

이 문서의 자료는 Troubleshoot ACI Management and Core Services — Pod Policies 가이드, Cisco APIC Basic Configuration Guide, Release 6.1(x) — Management 장 및 Cisco APIC Security Configuration Guide — Access, Authentication, and Accounting 장에서 종합했습니다.

개요

ACI 패브릭에 대한 원격 액세스에는 세 개의 서로 다른 레이어가 포함되며, 각 레이어는 엔지니어가 성공적으로 로그인하고 운영하기 위해 작동해야 합니다.

1. 전송 — 관리 네트워크 경로(OOB 또는 대역 내) 및 프로토콜 서비스(SSH 또는 HTTPS)에 연결하고 활성화해야 합니다.
2. 인증 — 사용자의 자격 증명을 APIC에서 로컬로 또는 원격 AAA 서버(TACACS+, RADIUS 또는 LDAP)에 대해 검증해야 합니다.
3. 권한 부여 — 인증된 사용자에게 올바른 RBAC 역할 및 보안 도메인을 할당해야 원하는 ACI 객체를 보고 수정할 수 있습니다.

어느 층에서든 장애가 발생하면 다른 증상이 나타납니다. 전송 실패로 인해 연결이 완전히 차단됩니다. 인증 실패는 자격 증명 오류를 반환합니다. 권한 부여 실패는 로그인을 허용하지만 가시성을 제한하거나 API에서 "403 금지" 오류를 생성합니다.

관리 액세스 정책

관리 액세스 정책(**commPol**)은 패브릭에서 활성화되는 원격 액세스 프로토콜을 제어하는 중앙 객체입니다. Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > Management Access(관리 액세스) > default(기본값)에 있습니다. 정책에는 다음을 구성하는 하위 객체가 포함되어 있습니다.

- SSH(**commSsh**) — 관리 상태, 포트, 암호, KEX(Key Exchange) 알고리즘, MAC(Message Authentication Code), 호스트 키 알고리즘
- HTTPS(**commHttps**) — 관리 상태, 포트, TLS(Transport Layer Security) 프로토콜 버전, 전송률 및 클라이언트 인증서 인증
- 텔넷(**commTelnet**) - 관리 상태 및 포트. 텔넷은 기본적으로 비활성화되어 있으며, Cisco에서는 비활성화되어 있는 상태를 유지할 것을 권장합니다.

OOB 및 대역 내 관리

ACI 노드는 두 가지 관리 액세스 경로를 지원합니다.

- OOB(Out-of-Band) - APIC 또는 스위치의 전용 관리 포트를 사용합니다. OOB 관리 주소는 관리 테넌트 아래의 풀에서 할당되며 를 통해 노드에 **mgmtRsOoBStNode**할당됩니다. APIC에서 OOB 계약은 규칙을 통해 **iptables** 시행됩니다. OOB 계약이 적용되는 경우 계약에 의해 명시적으로 허용된 트래픽만 APIC 관리 인터페이스에 도달할 수 있습니다.
- INB(In-Band) - 관리 트래픽에 패브릭 데이터 플레인을 사용합니다. 대역 내 관리에는 BD(Bridge Domain), 서브넷, EPG(Endpoint Group), 계약 및 노드 관리 주소 할당이 필요합니다. 추가 라우팅 또는 정책 컨피그레이션 없이 패브릭 외부에서 인밴드 IP 주소에 연결할 수 없습니다.

참고: APIC OOB 관리 IP는 초기 설정 중에 구성되며 APIC는 패브릭이 완전히 검색되기 전에 IP 연결을 가져옵니다. OOB는 기본 관리 경로이며 물리적 관리 네트워크가 연결된 경우 항상 사용할 수 있습니다.

AAA 아키텍처

ACI는 3계층 AAA 모델을 사용합니다.

1. 로그인 도메인(**aaaLoginDomain**) - 명명된 영역 아래에 AAA 제공자를 그룹화합니다. 사용자는 로그인 화면에서 로그인 도메인을 지정합니다(예: `apic:TACACS-Domain` 또는 UI의 드롭다운을 통해). 특수 대체 로그인 도메인은 항상 존재하며 로컬 인증에 매핑됩니다.
2. 제공 기관 그룹(**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**, **aaaLdapProviderGroup**) - 하나 이상의 AAA 서버를 참조하고 시도할 순서를 정의합니다.
3. Provider (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**) — 서버 IP, 포트, 공유 암호(또는 LDAP용 바인딩 DN), 시간 초과, 재시도, 관리 EPG 및 모니터링 자격 증명을 정의합니다.

사용자가 로그인 시 **aaaDefaultAuth** 로그인 도메인을 지정하지 않을 때 사용되는 로그인 도메인은 Default Authentication Realm(기본 인증 영역)에 따라 결정됩니다. Console Authentication Realm(콘솔 인증 영역)은 콘솔 세션에 대한 인증을 제어합니다.

> 참고: 원격 AAA 서버에 연결할 수 없는 상태에서 기본 인증 영역을 변경하면 패브릭에서 잠깁니다. 영역을 변경하기 전에 항상 AAA 서버 연결을 테스트합니다. 폴백 로그인 도메인(`apic:fallback\\admin`)을 사용하여 기본 영역을 우회하고 로컬에서 인증할 수 있습니다.

키 AAA 로그 파일

AAA 인증 이벤트는 APIC 및 패브릭 스위치 모두에서 여러 파일에 기록됩니다. 이러한 로그는 인증 결과를 검증하고, 사용 중인 영역 및 제공자 그룹을 식별하고, 역할 할당 실패를 진단하기 위한 기본 툴입니다.

로그 파일	위치(APIC)	위치(스위치)	
nginx.bin.log(APIC) nginx.log(스위치)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	기본 A 흐름을 요청, 조회, LDAP 통신, 메인 및 또는 7 은 플랫 컨텐츠 .
access.log	`/var/log/dme/log/access.log`	`/var/log/dme/log/access.log`	NGINX API 요 APIC에 드(200 됨)와 `aaaRef` 니다. DME A aaaRe 니다.
pam.module.log	`/var/log/dme/log/pam.module.log`	`/var/log/dme/log/pam.module.log`	PAM 모 에 대한 합니다 스 IP 용자 I 자가 인

로그 파일	위치(APIC)	위치(스위치)	
			거부도 장 빠른

참고: 기본 AAA 로그의 파일 이름은 플랫폼마다 다릅니다. APIC의 경우 **nginx.bin.log**/var/log/dme/log/입니다. 리프 및 스파인 스위치에서는 **nginx.log**/var/sysmgr/tmp_logs/dme_logs/에 있습니다. 로그 콘텐츠 형식과 AAA 메시지는 두 플랫폼에서 동일합니다.

nginx 로그의 AAA 항목은 다음 형식을 따릅니다.

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

특정 사용자의 인증 흐름에 대해 AAA 관련 로그 항목을 필터링합니다.

<#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
```

또는 모든 최근 인증 요청 및 결과를 볼 수 있습니다.

<#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
```

일반적인 성공적인 인증 흐름은 다음과 같은 주요 메시지를 순서대로 보여줍니다.

1. nginx에서 사용자 이름에 대한 PAM 인증 요청을 받았습니다. <user> — 로그인 요청을 받았습니다.
2. DefaultAuthMo는 <N> 영역을 지정합니다. 제공 기관 그룹 <name> ! — 영역이 선택되었습니다 (0=fallback/local, 2=TACACS+, 3=LDAP).
3. 공급자별 메시지(LDAP 바인딩, TACACS+ 공급자 조회 또는 RADIUS 요청).
4. 원격 사용자 이름 아래에서 UserDomain <domain>을 찾았습니다. <user> — AAA 응답의 도메인 할당입니다.
5. 사용자 이름 찾음: admin 쓰기 권한이 있는 admin이 UserDomain all - user is an admin user — 역할 확인에 성공했습니다.

실패한 인증 로그:

- 사용자 <user>가 AAA 인증 중에 거부되었습니다.
- 권한이 없는 사용자 <user> 오류: AAA 서버 인증 거부됨

참고: nginx 로그는 자주 회전하며 이전 항목은 숫자 접미사로 gzip 압축됩니다. APIC에서 회전된 로그는 동일한 디렉토리(예: **nginx.bin.log.22815.gz**)에 있습니다. 스위치에서 회전된 로그는 (symlinks in **/var/log/dme/oldlog/dme/nginx.log.*.gz** /var/sysmgr/tmp_logs/dme_logs/)에 저장됩니다. 순환된 로그를 검색하려면

<#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 모델

ACI RBAC는 인증된 사용자가 보고 수행할 수 있는 작업을 제어합니다. 이 모델에는 세 가지 구성 요소가 있습니다.

- 보안 도메인(**aaaDomain**) — ACI 객체(테넌트, 액세스 정책, 패브릭 정책)에 매핑되는 범위 제한 기입니다. 내장형 도메인 모두, 공통, 관리는 항상 존재합니다. 사용자 지정 도메인은 특정 테

넌트 또는 정책 영역에 대한 사용자의 가시성을 제한합니다.
- 역할(**aaaRole**) — 권한 집합을 정의합니다. 사전 구축된 역할에는 admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops 및 nw-svc-admin이 포함됩니다.
- 권한 — 각 역할은 특정 기능 영역에 대한 읽기 또는 쓰기(읽기를 의미) 액세스를 부여합니다.

사용자 계정에는 하나 이상의 보안 도메인 및 역할 쌍이 할당됩니다. TACACS+, RADIUS 또는 LDAP를 통해 인증된 원격 사용자의 경우 역할 매핑은 AAA 응답의 벤더별 특성(예: 특성)을 통해 **cisco-av-pair** 전달됩니다.

분류 결정 트리

사용자가 ACI 패브릭에 원격으로 액세스할 수 없다고 보고할 경우 이 진단트리를 사용합니다.

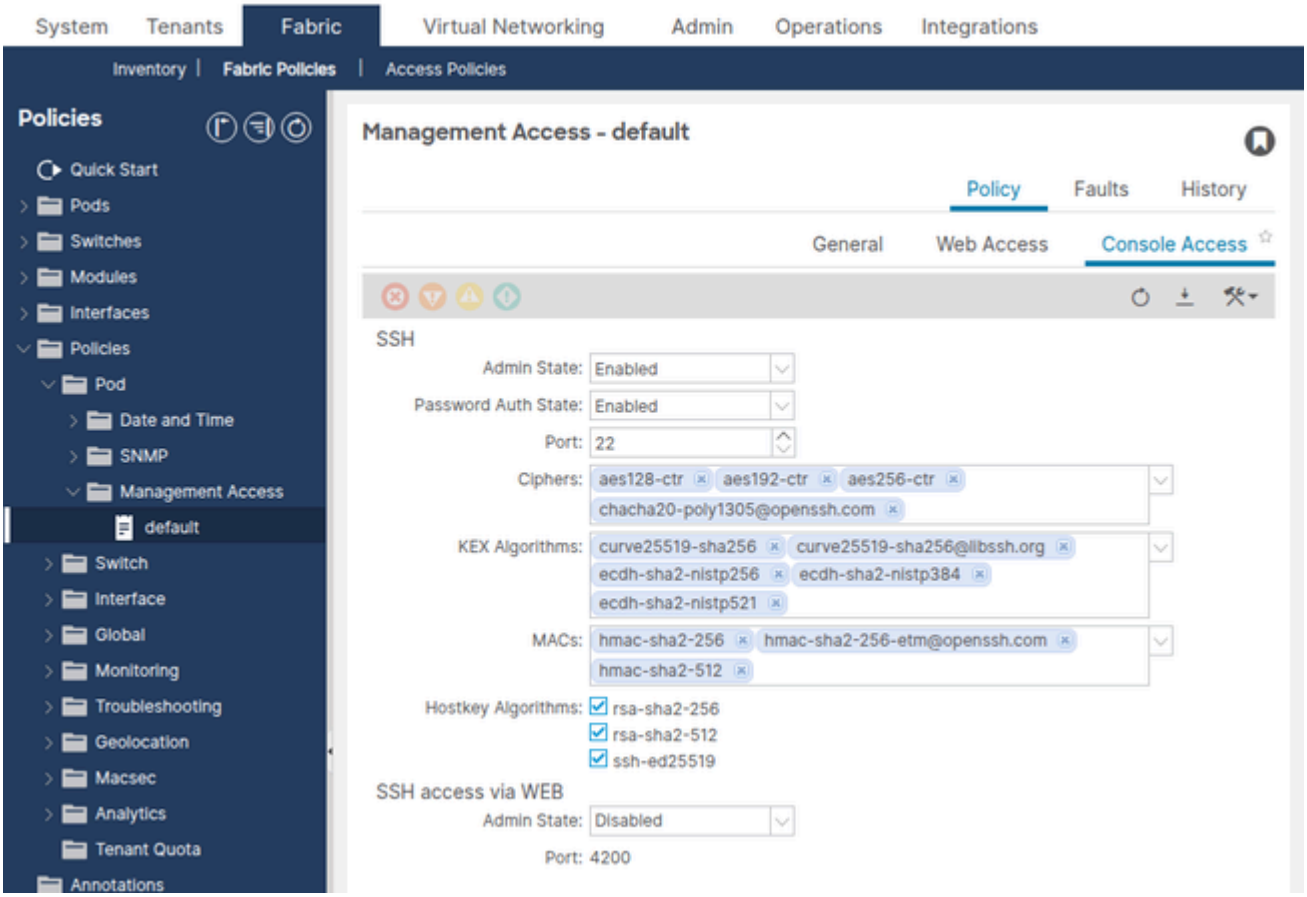
1. APIC 또는 스위치 관리 IP를 ping할 수 있습니까?
   - No → 관리 네트워크 경로를 트러블슈팅합니다. "OOB 및 대역 내 관리 문제 해결" 섹션을 참조하십시오.
   - 예→ 계속합니다.
2. SSH 또는 HTTPS 연결을 설정할 수 있습니까(연결이 전혀 열리는지 여부)?
   - → 프로토콜 서비스를 비활성화하거나, 포트를 필터링하거나, 암호 불일치가 있을 수 있습니다. "SSH 액세스 문제 해결" 또는 "HTTPS 액세스 문제 해결" 섹션을 참조하십시오.
   - 예→ 계속합니다.
3. 로그인 화면이 표시됩니까(HTTPS)? 아니면 SSH 핸드셰이크가 완료되어 자격 증명을 입력하라는 프롬프트가 표시됩니까?
   - → SSH 키 교환 또는 TLS 핸드셰이크 오류가 없습니다. 암호 및 KEX 불일치에 대해서는 "SSH 액세스 문제 해결" 섹션을 참조하십시오.
   - 예→ 계속합니다.
4. 자격 증명이 "Authentication Failed(인증 실패)" 또는 이와 유사한 상태로 실패합니까?
   - 예 → 인증 문제. "Troubleshoot AAA Authentication(AAA 인증 트러블슈팅)" 섹션(사용 중인 로그인 도메인에 따라 TACACS+, RADIUS 또는 LDAP)을 참조하십시오.
   - 계속하지 →.
5. 사용자가 로그인하지만 예상 객체를 볼 수 없거나 "403 Forbidden" 오류를 수신합니까?
   - 예 → 또는 RBAC 문제. "RBAC 및 사용자 권한 문제 해결" 섹션을 참조하십시오.
   - → 액세스 없음. 사용자가 겪고 있는 특정 문제를 확인합니다.

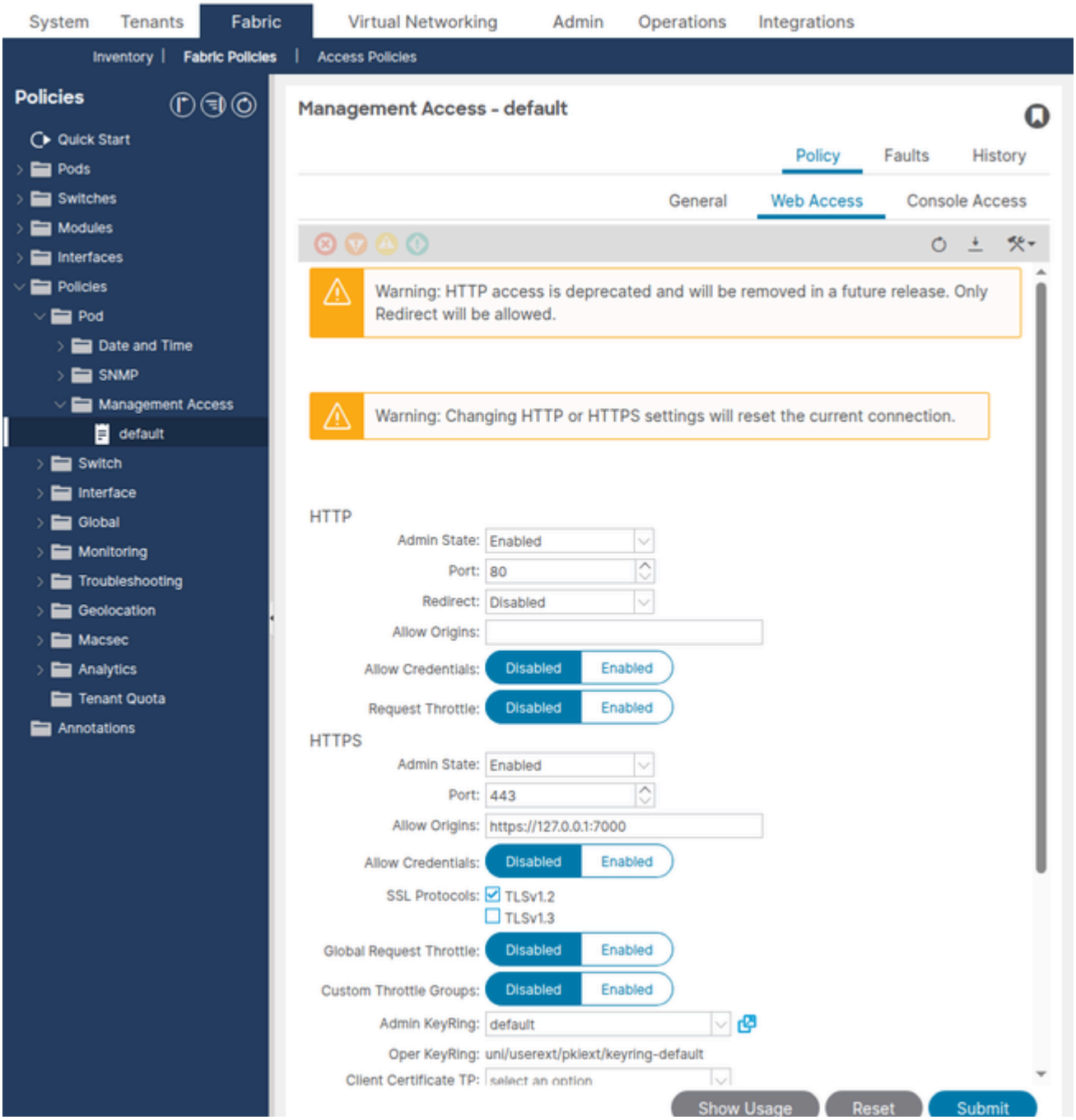
컨피그레이션 확인

작동 상태를 트러블슈팅하기 전에 컨피그레이션 체인이 완료되었는지 확인합니다. 컨피그레이션 오류는 원격 액세스 문제의 가장 일반적인 근본 원인입니다.

관리 액세스 정책(SSH 및 HTTPS) 확인

Fabric(패브릭) > Fabric Policies(패브릭 정책) > Policies(정책) > Pod(포드) > Management Access(관리 액세스) > default(기본값)로 이동합니다.





다음 SSH 설정을 확인합니다.

- Admin State(관리 상태) — 를 활성화해야 합니다.
- 포트 — 기본값 22. 변경된 경우 SSH 클라이언트는 사용자 지정 포트를 사용해야 합니다.
- 비밀번호 인증 — 활성화됨(인증서 전용 인증이 필요한 경우 제외).
- SSH 암호 — SSH 클라이언트에서 지원하는 암호를 하나 이상 포함해야 합니다.
- KEX 알고리즘 — SSH 클라이언트에서 지원하는 알고리즘을 하나 이상 포함해야 합니다.
- SSH MAC — SSH 클라이언트에서 지원하는 MAC을 하나 이상 포함해야 합니다.

API를 통해 SSH 관리 개체를 쿼리합니다.

<#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
```

다음 HTTPS 설정을 확인합니다.

- Admin State(관리 상태) — 를 활성화해야 합니다.
- 포트 — 기본값 443.
- SSL 프로토콜 — TLSv1.2(기본값). 이전 클라이언트는 TLSv1.1을 명시적으로 추가해야 할 수 있습니다.
- Throttle State(스로틀 상태) - 활성화된 경우, Throttle Rate(스로틀 속도)는 사용자당 초당 요청을 제한합니다. 값이 매우 낮으면 API 시간 초과 오류가 발생할 수 있습니다.

<#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
```

일반적인 컨피그레이션 오류

- SSH 암호가 너무 공격적으로 제한되었습니다. ACI 릴리스 5.2(1) 이상에서는 기본 SSH 암호가 강화되었습니다. 이전 SSH 클라이언트(예: 0.75 이전의 PuTTY 버전 또는 제공만 하는 OpenSSH 버전)는 키 **diffie-hellman-group14-sha1**교환에 실패할 수 있습니다. SSH 클라이언트는 "일치하는 암호를 찾을 수 없음" 또는 "일치하는 키 교환 메서드를 찾을 수 없음"을 표시합니다 .
- 비밀번호 인증 사용 안 함 — **passwordAuth** 이를 사용 안 함으로 설정하면 SSH 키 기반 인증만 허용됩니다. 암호로 연결하는 사용자에게 "Permission denied (publickey)(사용 권한 거부 (publickey))"가 표시됩니다.
- 클라이언트 인식 없는 사용자 지정 SSH 포트 — SSH 포트가 22에서 변경된 경우 SSH 클라

이언트는 새 포트(예: **ssh -p 2222 admin@10.1.1.1**)를 지정해야 합니다.

OOB 관리 주소 확인

Tenants(테넌트) > mgmt(관리) > Node Management Addresses(노드 관리 주소)로 이동합니다.

모든 APIC 및 스위치 노드에 유효한 게이트웨이와 함께 할당된 OOB 관리 IP 주소가 있는지 확인합니다. 관리 주소가 없는 노드는 관리 네트워크를 통해 연결할 수 없습니다.

API를 통해 OOB 고정 노드 할당을 쿼리합니다.

<#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
```

일반적인 컨피그레이션 오류

- OOB 주소 할당 누락 — 스위치에 항목이 **mgmtRsOoBStNode**없습니다. 노드에는 관리 IP가 없으며 OOB 인터페이스의 SSH 또는 HTTPS에 응답하지 않습니다.
- 잘못된 게이트웨이 — 게이트웨이 주소가 OOB 관리 네트워크의 실제 게이트웨이와 일치하지 않습니다. 노드는 패킷을 받을 수 있지만 반환 트래픽을 전송할 수 없습니다.
- 서브넷 마스크 불일치 — OOB 서브넷 마스크가 물리적 관리 네트워크와 일치하지 않습니다. 이로 인해 노드는 관리 스테이션이 다른 서브넷에 있다고 생각하고 존재하지 않거나 잘못된 게이트웨이를 통해 트래픽을 라우팅할 수 있습니다.

OOB 계약 확인

Tenants(테넌트) > mgmt(관리) > Contracts(계약)로 이동합니다.

OOB 계약이 OOB 관리 EPG에 적용되는 경우 해당 계약에 의해 명시적으로 허용된 트래픽만 APIC 관리 인터페이스에 도달합니다. APIC에서 OOB 계약은 규칙을 통해 **iptables** 시행됩니다.

OOB EPG 제공 계약을 쿼리합니다.

<#root>

apic1#

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

질의가 결과를 반환하면 계약이 적용됩니다. 계약 주체 및 필터가 필요한 프로토콜을 허용하는지 확인합니다.

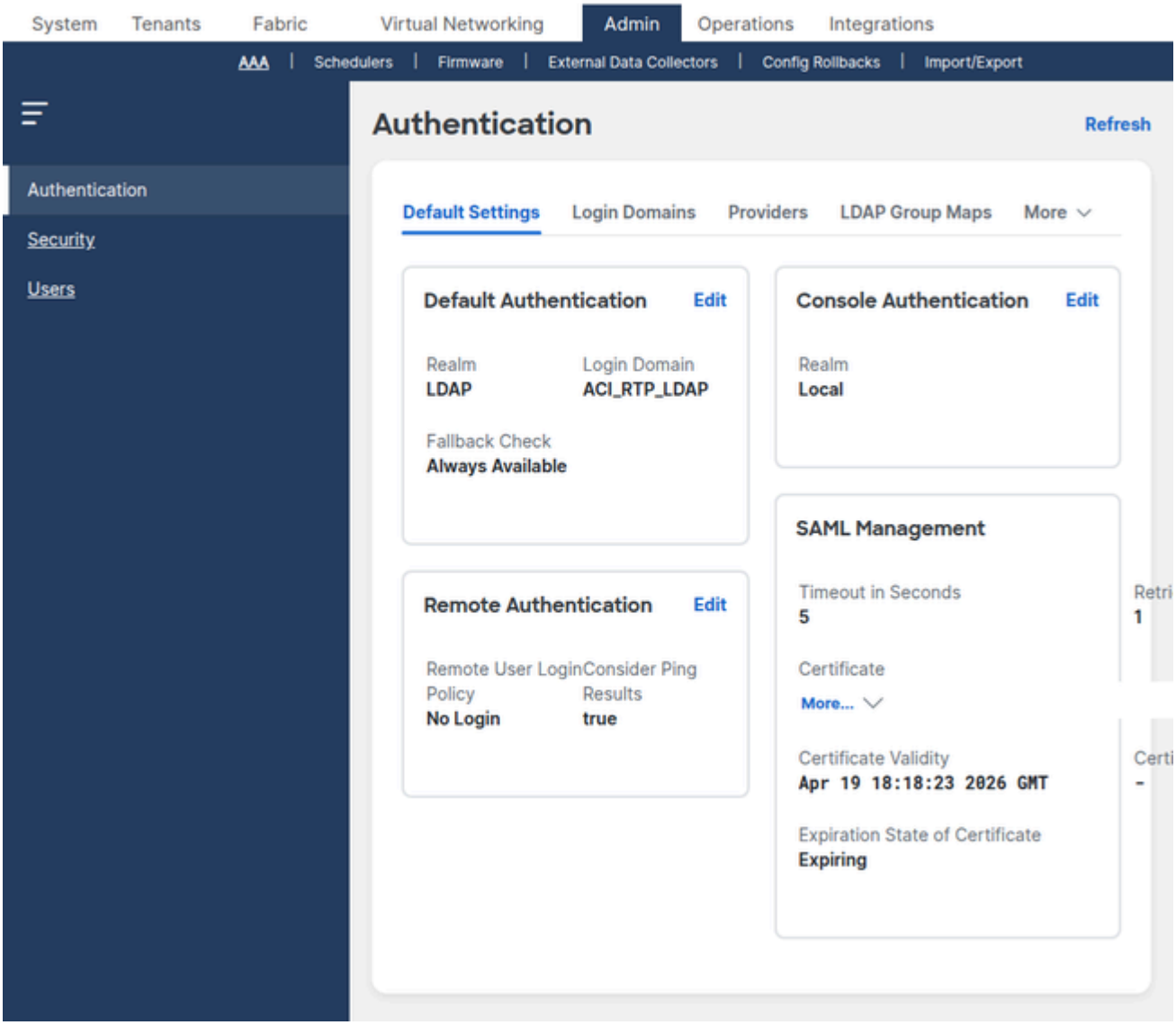
- SSH — TCP 포트 22(또는 사용자 지정 포트)
- HTTPS — TCP 포트 443(또는 사용자 지정 포트)
- ICMP - ping 확인용

일반적인 컨피그레이션 오류

- OOB 계약에는 SSH 또는 HTTPS가 포함되지 않습니다. 엔지니어는 APIC에 ping을 수행할 수 있지만 SSH 또는 HTTPS를 통해 연결할 수는 없습니다. APIC$_{\text{iptables}}$의 규칙은 자동으로 트래픽을 삭제합니다.
- OOB 계약 필터의 소스 IP 제한 — 계약 필터는 특정 소스 서브넷에 대한 액세스를 제한합니다. 서브넷을 벗어난 엔지니어는 연결할 수 없습니다.

AAA 컨피그레이션 확인

Admin(관리) > AAA > Authentication(인증) > AAA로 이동합니다.



다음을 확인합니다.

- Default Authentication Realm — 사용자가 로그인 도메인을 지정하지 않을 때 어떤 로그인 도메인이 사용되는지 식별합니다. 원격 AAA 로그인 도메인으로 설정된 경우 해당 서버에 연결할 수 있어야 합니다.
- 콘솔 인증 영역 — 콘솔 액세스를 제어합니다. 로컬로 설정된 경우 콘솔 로그인은 항상 로컬 자격 증명을 사용합니다(권장).

로그인 도메인 확인

Admin(관리) > AAA > Authentication(인증) > Login Domains(로그인 도메인)로 이동합니다.

<#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
```

인증에 사용되는 로그인 도메인이 있으며 올바른 제공자 그룹을 참조하는지 확인합니다.

TACACS+ 제공자 확인

Admin(관리) > AAA > Authentication(인증) > TACACS+ > TACACS+ Providers(TACACS+ 제공자)로 이동합니다.

<#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 제공자 확인

Admin(관리) > AAA > Authentication(인증) > RADIUS > RADIUS Providers(RADIUS 제공자)로 이동합니다.

<#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 제공자 확인

Admin(관리) > AAA > Authentication(인증) > LDAP > LDAP Providers(LDAP 제공자)로 이동합니다.

<#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
```

일반적인 AAA 컨피그레이션 오류

- 공유 암호 불일치 — ACI TACACS+ 또는 RADIUS 제공자에 구성된 키가 서버의 키와 일치하지 않습니다. 인증이 자동으로 실패합니다.
- 잘못된 관리 EPG — 제공자의 **epgDn** EPG가 비어 있거나 잘못된 EPG를 가리킵니다(예: 서버가 OOB 네트워크에 있는 경우 대역 내). APIC에서 서버에 연결할 수 없습니다.
- 로그인 도메인 영역 불일치 - 로그인 도메인이 LDAP로 구성되었지만 사용자는 TACACS+ 인증을 요구합니다. 로그인 도메인은 올바른 제공 기관 그룹 유형을 참조해야 합니다.
- LDAP bind DN incorrect — **rootdn** (bind DN) 또는 **basedn** 잘못되었습니다. 사용자 자격 증명이 올바르더라도 바인드 오류와 함께 LDAP 인증이 실패합니다.
- LDAP 필터가 디렉토리 스키마와 일치하지 않습니다. Active Directory의 경우 를 **sAMAccountName=$userid**사용합니다. OpenLDAP의 경우 또는**cn=$userid**를 사용합니다**uid=$userid.**

RBAC 구성 확인

로컬 사용자 계정과 해당 보안 도메인 및 역할 할당을 보려면 Admin(관리) > AAA > Users(사용자)로 이동합니다.

API를 통해 보안 도메인을 쿼리합니다.

<#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
```

admin 역할이 있는 모든 도메인에 할당된 사용자는 전체 패브릭에 대한 전체 읽기/쓰기 액세스 권한을 갖습니다. 테넌트-admin 역할의 사용자 지정 보안 도메인에 할당된 사용자는 해당 도메인과 연결된 테넌트만 관리할 수 있습니다.

일반적인 RBAC 구성 오류

- 보안 도메인 없이 생성된 사용자 - 로그인할 수 있지만 테넌트를 볼 수 없으며 API 호출에 대해 "403 금지"를 수신합니다. 하나 이상의 보안 도메인을 할당해야 합니다.
- 쓰기 액세스가 필요할 때 할당된 읽기 전용 역할 - 사용자는 객체를 볼 수 있지만 변경 사항을 제출할 수는 없습니다. 역할 권한이 writePriv로 설정되어 있는지 확인합니다.
- AAA 서버에서 원격 사용자 역할 매핑 누락 — TACACS+ 또는 RADIUS 서버는 포함 특성을 **cisco-av-pair** 반환하지 **shell:domains=all/admin/**않습니다. 사용자는 성공적으로 인증되지만 역할이 없으므로 패브릭에서 아무 것도 볼 수 없습니다.

OOB 및 대역 내 관리 문제 해결

네트워크에서 APIC 또는 스위치 관리 IP에 연결할 수 없는 경우 SSH, HTTPS 또는 AAA를 조사하기 전에 관리 경로의 문제를 해결하십시오.

시나리오: APIC OOB IP를 Ping할 수 없습니다.

문제/장애: 관리 스테이션에서 APIC OOB 관리 IP 주소를 ping할 수 없습니다.

확인 단계:

1. APIC 관리 포트가 물리적으로 연결되어 있고 링크가 작동하고 있는지 확인합니다.
2. 관리 스테이션이 동일한 L2 세그먼트에 있거나 OOB 서브넷에 대한 경로가 있는지 확인합니다.
3. OOB 관리 IP가 올바르게 할당되었는지 확인합니다.
   <#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. 기본 게이트웨이에 연결할 수 있는지 확인합니다.
   <#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. OOB 계약이 적용되는 경우 필요한 프로토콜을 허용하는지 확인합니다. "OOB 계약 확인" 섹션에 표시된 대로 OOB EPG 제공 계약을 질의합니다. OOB 계약은 APIC$_{\text{iptables}}$에 대한 규칙으로 시행됩니다. APIC 셸에서 저장된 규칙을 볼 수 있습니다.
   <#root>

   ```
   apic1#

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

   INPUT 정책이 DROP이고 필요한 프로토콜에 대한 ACCEPT 규칙이 없는 경우 OOB 계약은 트래픽을 필터링하는 것입니다.

   > 참고: 라이브 **iptables -L -n** 커널 규칙을 보기 위한 명령은 루트 액세스가 필요하며 일반 관리 SSH 세션에서는 사용할 수 없습니다.

근본 원인: 누락되거나 잘못 구성된 OOB 관리 주소, 잘못된 게이트웨이 또는 OOB 계약 필터링 트래픽입니다.

해결책: OOB 주소 할당을 수정하거나, 물리적 네트워크 경로를 확인하거나, 필요한 프로토콜을 허용하도록 OOB 계약을 업데이트합니다.

시나리오: 스위치 관리 IP에 연결할 수 없음

문제/장애: 관리 스테이션은 APIC에 연결할 수 있지만 OOB를 통해 스위치에 연결할 수는 없습니다
.

확인 단계:

1. 스위치에 OOB 주소가 할당되었는지 확인합니다.
   <#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. 스위치 관리 인터페이스에 할당된 IP가 있는지 확인합니다.
   <#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. 관리 VRF 기본 경로를 확인합니다.
   <#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
   ```

근본 원인: OOB 주소 할당이 없거나, 게이트웨이가 잘못되었거나, 스위치 관리 물리적 포트가 다운되었습니다.

해결책: Tenants(테넌트) > mgmt(관리) > Node Management Addresses(노드 관리 주소)에서 OOB 주소를 할당합니다. 물리적 관리 링크가 작동 중인지 확인합니다.

SSH 액세스 문제 해결

이 섹션에서는 관리 IP에 연결 가능하지만(ping 성공) SSH 세션이 설정 또는 인증에 실패한 시나리오를 다룹니다.

시나리오: SSH 연결 거부됨

문제/장애: SSH 클라이언트는 APIC 또는 스위치에 연결할 때 "연결 거부됨"을 보고합니다.

확인 단계:

1. SSH가 관리 액세스 정책에서 활성화되었는지 확인합니다.
   <#root>

   ```
   apic1#

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

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

   이 **adminSt** 비활성화된 경우 SSH 연결이 거부됩니다.

2. 올바른 포트가 사용되고 있는지 확인합니다. SSH 포트가 22에서 변경된 경우:
   <#root>

   ```
   $

   ssh -p

    custom-port

   admin@10.1.1.1
   ```

3. OOB 계약이 SSH 포트에서 TCP를 허용하는지 확인합니다. "OOB 계약 확인" 섹션을 참조하십시오.

근본 원인: SSH가 관리 액세스 정책에서 비활성화되었거나, 클라이언트에 알려지지 않은 사용자 지정 포트 또는 OOB 계약 필터링입니다.

해결책: 관리 액세스 정책에서 SSH를 활성화하거나 올바른 포트를 사용합니다.

시나리오: SSH 키 교환 실패(암호 또는 KEX 불일치)

문제/장애: SSH 클라이언트가 "일치하는 암호를 찾을 수 없음", "일치하는 키 교환 메서드를 찾을 수 없음" 또는 "일치하는 MAC을 찾을 수 없음"과 함께 실패합니다.

확인 단계:

1. 클라이언트가 제공하는 알고리즘을 식별하려면 SSH 클라이언트 세부 정보 출력을 확인합니다.
<#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. 클라이언트 제공 알고리즘을 APIC에서 구성한 알고리즘과 비교합니다.
<#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. 교차를 식별합니다. 어떤 카테고리에도 공통된 알고리즘이 없으면 핸드셰이크가 실패합니다.

참고: ACI 릴리스 5.2(1) 이상에서는 기본 SSH 암호 및 KEX 알고리즘이 강화되었습니다. ,, **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**및 **aes128-cbc**과 같은 레거시 알고리즘**hmac-sha1**은 더 이상 기본적으로 제공되지 않습니다. 최근에 업그레이드한 경우 해당 환경의 SSH 클라이언트가 새 기본값을 지원하는지 확인합니다.

근본 원인: ACI 업그레이드 또는 암호 강화 후 SSH 클라이언트와 APIC 간에 공통 암호, KEX 알고리즘 또는 MAC이 없습니다.

해결책: 최신 알고리즘을 지원하기 위해 SSH 클라이언트를 업데이트하거나, 필요한 레거시 알고리즘을 관리 액세스 정책에 다시 추가합니다. 레거시 알고리즘을 다시 추가하면 보안 위험이 따르므로 장기적으로는 권장되지 않습니다.

시나리오: SSH가 연결되지만 로컬 사용자에 대한 인증이 실패함

문제/장애: SSH 핸드셰이크가 성공하지만(비밀번호 프롬프트가 표시됨) 로컬 사용자에 대해 비밀번호가 거부됩니다.

확인 단계:

1. 사용자가 로컬에 존재하는지 확인합니다.
   <#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. 과도한 로그인 시도 실패로 인해 계정이 잠겼는지 확인합니다.
   <#root>

```
apic1#

moquery -c aaaUserEp

dn                  : uni/userext
pwdStrengthCheck    : no
```

   Admin(관리) > AAA > Security Management(보안 관리) > Lockout Policy(잠금 정책)에서 로그인 도메인 잠금 정책을 선택합니다.

3. 사용자가 올바른 로그인 도메인으로 로그인하고 있는지 확인합니다. Default Authentication Realm(기본 인증 영역)이 원격 AAA 로그인 도메인으로 설정된 경우, 사용자는 로컬 인증 **apic:LOCAL\\username**을 **apic:fallback\\username** 강제하기 위해 또는 앞에 와야 합니다.
4. 로그에서 인증 결과를 확인합니다. APIC**nginx.bin.log**에서 로그인 이벤트를 확인합니다.
   <#root>

```
apic1#

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

   로그인 시도에 할당된 영역 및 공급자 그룹을 찾습니다.

```
! 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
```

영역이 0이 아니면(대체/로컬) 로컬 데이터베이스 대신 원격 AAA 서버로 로그인이 전송되었습니다. 사용자가 로컬 인증**apic:fallback\\username**을 **apic:LOCAL\\username** 강제 실행하려면 앞에 또는 를 추가해야 합니다.

근본 원인: 잘못된 암호, 잠긴 계정 또는 로그인 시도가 로컬 데이터베이스가 아닌 원격 AAA 서버로 전송되고 있습니다.

해결책: 비밀번호를 재설정하거나, 계정을 잠금 해제하거나, 올바른 로그인 도메인 접두사를 사용합니다.

HTTPS 액세스 문제 해결

이 섹션에서는 APIC 웹 UI 또는 REST(Representational State Transfer) API(Application Programming Interface)가 HTTPS를 통해 연결할 수 없는 시나리오를 다룹니다.

시나리오: HTTPS 연결 시간 초과

문제/장애: 브라우저에 "ERR_CONNECTION_TIMED_OUT"이 표시되거나 포트 443의 APIC에 연결할 때 API 호출이 중단됩니다.

확인 단계:

1. HTTPS가 활성화되었는지 확인합니다.
   <#root>

   ```
   apic1#
   ```

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

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

2. OOB 계약이 TCP 443을 허용하는지 확인합니다. "OOB 계약 확인" 섹션을 참조하십시오.
3. APIC 자체에서 테스트하여 HTTPS 프로세스가 수신 대기하고 있는지 확인합니다.
   <#root>

   ```
   apic1#
   ```

   ss -tlnp | grep 443

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

근본 원인: HTTPS가 비활성화되었거나, OOB 계약 필터링 TCP 443 또는 APIC의 nginx 프로세스가 crash했습니다.

해결책: 관리 액세스 정책에서 HTTPS를 활성화하거나, OOB 계약을 업데이트하거나, APIC에서 웹 서비스를 다시 시작합니다.

시나리오: 브라우저에 TLS 핸드셰이크 오류 표시

문제/장애: 브라우저에 "ERR_SSL_VERSION_OR_CIPHER_MISMATCH" 또는 유사한 TLS 오류가 표시됩니다.

확인 단계:

1. APIC에 구성된 TLS 프로토콜 버전을 확인합니다.
   <#root>

   ```
   apic1#

   moquery -c commHttps

   sslProtocols : TLSv1.2
   ```

2. 브라우저에서 TLSv1.2를 지원하는지 확인합니다. 매우 오래된 브라우저(예: Internet Explorer 10 이상)는 기본적으로 TLSv1.2를 지원하지 않습니다.

근본 원인: APIC는 TLSv1.2(기본값)만 제공하고 브라우저 또는 API 클라이언트는 이전 TLS 버전만 지원합니다.

해결책: 브라우저 또는 클라이언트를 업데이트합니다. 일시적으로 이전 클라이언트를 지원해야 하는 경우 TLSv1.1을 관리 액세스 정책에 추가하지만 이로 인해 보안 위험이 발생합니다.

시나리오: API 제한

문제/장애: REST API 호출이 간헐적으로 실패하고 HTTP 503 오류가 발생하거나 과중한 자동화 과정에서 웹 UI가 느려집니다.

확인 단계:

<#root>

```
apic1#

moquery -c commHttps

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

스로틀 속도가 매우 낮고 자동화 스크립트가 초당 많은 요청을 전송하면 APIC는 초과 요청을 거부합니다.

근본 원인: 사용자 단위 조절 속도가 자동화 워크로드에 비해 너무 낮습니다.

해결책: 관리 액세스 정책에서 스로틀 속도를 높이거나, 요청 빈도를 줄이기 위해 자동화 스크립트를 최적화하십시오. 또는 패브릭이 공유되지 않는 경우 제한을 비활성화합니다.

AAA 트러블슈팅 - TACACS+

이 섹션에서는 TACACS+ 인증 실패에 대해 설명합니다. APIC는 TCP 포트 49를 통해 TACACS+ 서버와 통신합니다.

운영 확인

ACI 스위치는 독립형 NX-OS에서 **test aaa** 사용 가능한 명령을 지원하지 않습니다. TACACS+ 작업을 확인하려면 APIC를 사용하여 제공자 상태, 결함 및 로그인 세션 기록을 확인합니다.

TACACS+ 공급자에서 활성 결함을 확인합니다.

```
<#root>

apic1#

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

어떤 fault도 반환되지 않으면 APIC에서 제공 기관에 도달 가능한 것으로 간주합니다. 결함이 있는 경우, 출력에 F1773(제공자에 연결할 수 없음) 또는 F1774(인증 실패)와 같은 결함 코드가 포함됩니다.

TACACS+ 제공자 컨피그레이션을 확인합니다.

<#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
```

APIC에서 TACACS+ 서버로의 기본 네트워크 연결성을 확인합니다.

<#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
```

TACACS+ 로그인 도메인을 사용하여 APIC에 로그인을 시도하고 세션 결과를 확인합니다.

<#root>

apic1#

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

인증 거부 **descr** 또는 연결 문제로 인해 실패했는지 확인하려면 필드를 확인합니다.

APIC 로그에서 TACACS+ 인증 흐름을 검증합니다. 문제의 사용자 이름에 대한 필터:

<#root>

apic1#

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

TACACS+ 로그인은 LDAP와 동일한 **nginx.bin.log** 인증 흐름을 따릅니다(전체 실제 로그 예는 LDAP

Operational Verification 섹션 참조). TACACS+의 주요 차이점은 다음과 같습니다.

- DefaultAuthMo는 영역 2를 지정합니다. 영역 2는 TACACS+(LDAP의 경우 영역 3)를 나타냅니다.
- 목록에 TacacsProvider <IP> 추가 — 연결할 TACACS+ 서버(LDAP용 LdapProvider와 비교)를 식별합니다.
- TACACS+ Cisco-avpair(shell:domains=all/admin/) — AV 쌍은 TACACS+ 서버에서 직접 반환되고 LDAP 그룹 맵에서 변환됩니다.

TACACS+ 로그인에 성공한 경우에도 동일한 진행이 표시됩니다. PAM 요청→ 영역 선택 → 공급자 조회 → AV 쌍 구문 분석 → 사용자 삽입 → UserDomain 및 역할 할당→ 관리자 쓰기 권한입니다.

TACACS+ 로그인에 실패한 경우는 <username> 사용자가 AAA 인증 중에 거부되었으며 무단으로 인해 종료됩니다. 오류: AAA Server Authentication Denied(AAA 서버 인증 거부됨), LDAP 거부와 동일한 패턴.

시나리오: TACACS+ 인증 실패

문제/장애: 사용자가 TACACS+ 로그인 도메인을 선택하면 "Authentication Failed(인증 실패)"로 로그인이 실패합니다.

확인 단계:

1. TACACS+ 공급자에서 활성 결함을 확인합니다.
   <#root>

   ```
   apic1#
   ```

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

   결함 F1773은 연결 문제를 나타냅니다. 결함 F1774는 인증 거부를 나타냅니다.

2. APIC에서 TACACS+ 서버로의 네트워크 연결성을 확인합니다.
   <#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. ping은 성공하지만 인증이 실패할 경우 APIC 제공자 컨피그레이션 및 TACACS+ 서버 컨피그레이션에서 공유 암호 일치를 확인합니다.
4. 가장 최근 로그인 세션을 확인하여 실패 세부 정보를 확인합니다.
   <#root>

```
apic1#
moquery -c aaaSessionLR -x 'order-by=aaaSessionLR.created|desc' -x page-size=5
```

5. 인증 시도에 대한 TACACS+ 서버 로그를 확인합니다. 서버에 로그인했지만 거부된 시도는 서버 측의 사용자 컨피그레이션 문제를 나타냅니다(예: 비밀번호 불일치 또는 사용자 계정 누락).
6. APIC에서 전체 인증 **nginx.bin.log** 흐름을 확인합니다. 중간 메시지가 누락되지 않도록 특정 키워드가 아닌 사용자 이름으로 필터링합니다.
   <#root>

```
apic1#
grep '||aaa||' /var/log/dme/log/nginx.bin.log | grep -i 'tacuser1' | tail -20
```

위의 Operational Verification(운영 확인) 섹션에서 작동 및 비작동 예와 출력을 비교합니다. 주요 지표:

- was denied 또는 DENIED — TACACS+ 서버에 도달했지만 자격 증명을 거부했습니다. 사용자가 서버에 있으며 비밀번호가 일치하는지 확인합니다.
- TacacsProvider를 추가한 후 공급자별 메시지 없음 - 서버에 연결할 수 없거나 시간이 초과되었습니다. 네트워크 연결성 및 관리 EPG를 확인합니다.
- 원격 사용자 삽입 ...이 완료되고 역할 확인 줄이 이어졌습니다. 인증에 성공했지만 역할 할당으로 인해 문제가 발생할 수 있습니다(아래 AV 쌍 섹션 참조).

RBAC용 TACACS+ cisco-av-pair

TACACS+를 통해 인증된 원격 사용자의 경우 서버는 권한 부여 응답에서 **cisco-av-pair** 특성을 반환해야 합니다. 이 특성은 사용자를 ACI 보안 도메인 및 역할에 매핑합니다.

형식:

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

예:

- 전체 관리자: **shell:domains=all/admin/**
- 모두 읽기 전용: **shell:domains=all/read-all/**
- 특정 도메인에 대한 테넌트 관리자: **shell:domains=TenantA/tenant-admin/**
- 여러 도메인: **shell:domains=all/admin/,TenantA/tenant-admin/**

이 특성이 없거나 잘못된 경우 사용자는 성공적으로 인증되지만 역할이 없으며 APIC UI에서 어떤 객체도 볼 수 없습니다.

참고: 리프 및 스파인 스위치에 대한 SSH 액세스에는 모든 보안 도메인에서 쓰기 권한이 있는 관리자 역할이 필요합니다. 스위치 SSH 액세스를 위한 최소 AV 쌍은 **shell:domains=all/admin/**입니다. 비관리자 역할(예: `read-all`, `tenant-admin`, `aaa`)을 가진 사용자 또는 all이 아닌 보안 도메인에 할당된 사용자는 APIC에 로그인할 수 있지만 스위치에 대한 SSH 액세스는 거부됩니다. APIC 로그에는 스위치의 비관리자 로그인이 이러한 사용자에 대해 거부된 것으로 표시됩니다.

를 확인하여 수신한 AV 쌍을 확인합니다**nginx.bin.log**. 전체 역할 주입 흐름을 보려면 사용자 이름으로 필터링합니다.

<#root>

apic1#

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

TACACS+의 경우 AV 쌍이 TACACS+ `Cisco-avpair(shell:domains=...)`로 기록됩니다. 성공적으로 삽입하면 원격 사용자 <username>의 주입이 완료된 다음 `Found UserDomain` 및 관리자 쓰기 권한 행이 표시됩니다(실제 로그 출력을 사용하는 이 흐름의 전체 예는 LDAP Operational Verification 섹션 참조).

AV 쌍 형식이 잘못된 경우 로그에 원격 사용자 <username> 데이터 주입 실패 - 오류 메시지가 잘못된 셸:도메인 문자열입니다. 사용자가 비관리자 역할로 인증하면 스위치에 대한 SSH가 거부되고 스위치에 대한 비관리자 로그인이 거부됩니다.

근본 원인: 공유 암호가 일치하지 않거나, 관리 네트워크에서 서버에 연결할 수 없거나, 사용자가 TACACS+ 서버에 없거나, 공급자의 관리 EPG가 잘못되었습니다.

해결책: 공유 암호를 수정하거나, 연결 가능성을 수정하거나, TACACS+ 서버에서 사용자를 생성합니다.

리프 스위치 인증 로그 검증

리프 및 스파인 스위치에서 SSH 로그인 이벤트는 및 모두에 **pam.module.log** 로그인됩니다**nginx.log**. 는 PAM 인증 결과(accept 또는 reject)를 **pam.module.log** 표시합니다. 에는 **nginx.log** APIC에서와 동일한 전체 AAA 플로우(영역 선택, 제공자 조회, LDAP/TACACS+/RADIUS 통신, AV 쌍 구문 분석, 역할 할당)**nginx.bin.log**가 포함되어 있습니다. 이러한 로그는 모든 원격 AAA 유형(TACACS+, RADIUS, LDAP)에 적용됩니다.

인증 결과**pam.module.log**를 확인합니다.

<#root>

leaf101#

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

작동 — 스위치에서 성공적인 원격 인증:

```
||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
```

이 **remote=1** 플래그는 사용자가 원격 AAA 서버에 의해 인증되었음을 확인합니다.

Not Working — 사용자가 거부되었습니다. securitymgrAG는 사용자를 거부하고 스위치는 최종 대안으로서 로컬 사용자 조회를 시도합니다.

```
||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
```

사용자에 대해 PAM 항목이 전혀 나타나지 않으면 PAM 단계에 도달하기 전에(예: 암호 불일치 또는 사용자가 연결을 취소하여) SSH 연결이 거부되었을 가능성이 있습니다.

스위치의 인증 흐름에 대한 자세한 내용을 보려면 를 **nginx.log**선택합니다. 이 로그에는 APIC에서와 동일한 형식 및 메시지인 전체 AAA 결정 체인이 포함되어 **nginx.bin.log** 있습니다.

<#root>

```
leaf101#
```

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

작동 — 스위치에서 성공적인 LDAP 인증(LDAP Operational Verification 섹션의 APIC LDAP 예와 비교 - 메시지는 동일함):

```
||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
```

이 스위치**nginx.log**는 거부 표시를 **pam.module.log** 하지만 그 이유를 설명하지 않을 때 특히 유용합니다. nginx.log는 AAA 영역, 제공자 및 특정 실패 이유를 표시합니다(예: LDAP 검색에서 빈 값이 반환됨, TACACS+ 시간 초과 또는 AV 쌍 주입이 실패함).

AAA 트러블슈팅 - RADIUS

이 섹션에서는 RADIUS 인증 실패에 대해 설명합니다. APIC는 UDP 포트 1812(인증) 및 선택적으로 UDP 포트 1813(어카운팅)을 통해 RADIUS 서버와 통신합니다.

운영 확인

ACI 스위치는 독립형 NX-OS에서 **test aaa** 사용 가능한 명령을 지원하지 않습니다. 다음 방법을 사용하여 RADIUS 작업을 확인합니다.

리프 스위치에서 RADIUS 서버 컨피그레이션 및 연결 가능성 통계를 확인합니다.

<#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
```

시나리오: RADIUS 인증 실패

문제/장애: 사용자가 RADIUS 로그인 도메인을 선택하면 로그인이 실패합니다.

확인 단계:

1. 스위치의 RADIUS 서버 통계에서 시간 초과 또는 장애 징후를 확인합니다.
   <#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
   ```

   요청 시간 초과에 대한 높은 카운트는 RADIUS 서버에 연결할 수 없거나 공유 암호가 일치하지 않음을 나타냅니다(RADIUS는 공유 암호 불일치에서 패킷을 자동으로 삭제함).

2. RADIUS 서버에 대한 네트워크 연결성을 확인합니다.
   <#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. APIC와 RADIUS 서버 간의 공유 암호 일치를 확인합니다. TCP를 사용하고 연결 실패를 보고하는 TACACS+와 달리 RADIUS는 UDP를 사용하며 공유 암호가 일치하지 않을 때 패킷을 자동으로 삭제합니다. 유일한 증상은 시간 초과입니다.
4. RADIUS 서버 로그를 확인 합니다. 디버그 모드(**radiusd -X**)의 FreeRADIUS는 각 요청을 표시하며, 수락되었는지, 거부되었는지 또는 공유 암호가 일치하지 않았는지 여부를 나타냅니다.

5. APIC에서 RADIUS 인증 **nginx.bin.log** 플로우를 확인합니다. 사용자 이름으로 필터링:
   <#root>

   apic1#

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

   RADIUS 로그인은 LDAP 및 TACACS+와 동일한 **nginx.bin.log** 인증 흐름을 따릅니다(전체 실제 로그 예는 LDAP Operational Verification 섹션 참조). RADIUS의 주요 차이점은 다음과 같습니다.

   - 목록에 RadiusProvider <IP> 추가 — RADIUS 서버(TacacsProvider 또는 LdapProvider와 비교)를 식별합니다.
   - RADIUS의 영역 번호는 컨피그레이션에 따라 다릅니다.

   RADIUS 로그인이 성공하면 원격 사용자 주입이 완료되고 관리자 쓰기 권한이 부여됩니다.

   실패한 RADIUS 로그인은 AAA 인증 중에 denied 및 DENIED로 종료됩니다.

   Adding RadiusProvider(RadiusProvider 추가) 줄 뒤에 RADIUS별 메시지가 나타나지 않으면 서버 시간이 초과됩니다. TCP를 사용하고 연결 실패를 보고하는 TACACS+와 달리 RADIUS는 UDP를 사용하며 공유 암호가 일치하지 않을 때 패킷을 자동으로 삭제합니다. 유일한 증상은 시간 초과와 거부 입니다.

6. RADIUS 공급자에서 활성 결함을 확인 합니다.
   <#root>

   apic1#

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

RBAC용 RADIUS cisco av 쌍

RADIUS는 RBAC 역할 매핑**cisco-av-pair**에 대해 TACACS+와 동일한 특성을 사용합니다. RADIUS 서버는 Access-Accept 응답에서 이 특성을 반환해야 합니다.

<#root>

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

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

FreeRADIUS에서는 파일 또는 LDAP 백엔드에 **users** 구성됩니다. ISE의 경우 Authorization Profile(권한 부여 프로파일)에서 Advanced Attribute(고급 특성)로 구성됩니다.

근본 원인: 공유 암호 불일치(RADIUS에서 가장 많이 발생 - 무음 시간 초과), 서버에 연결할 수 없음, 잘못된 인증 포트 또는 RADIUS 서버에 사용자 계정이 없습니다.

해결책: 공유 암호를 수정하고 UDP 1812 연결 가능성을 확인하거나 RADIUS 서버에서 사용자를 구성합니다.

AAA 트러블슈팅 - LDAP

이 섹션에서는 LDAP 인증 실패에 대해 설명합니다. APIC는 TCP 포트 389(LDAP) 또는 TCP 포트 636(LDAP with SSL)을 통해 LDAP 서버에 연결합니다.

운영 확인

ACI 스위치는 독립형 NX-OS에서 **test aaa** 사용 가능한 명령을 지원하지 않습니다. LDAP 작업을 확인하려면 APIC에서 사업자 결함 및 컨피그레이션을 확인합니다.

LDAP 제공자에서 활성 결함을 확인합니다.

```
<#root>

apic1#

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

결함 F1777은 연결 문제를 나타냅니다. 결함 F1778은 인증 또는 바인딩 실패를 나타냅니다. 어떤 fault도 반환되지 않으면 APIC에서 제공 기관에 도달 가능한 것으로 간주합니다.

LDAP 서버에 대한 기본 네트워크 연결 확인:

```
<#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
```

LDAP의 경우 포트 389(또는 LDAPS의 경우 636)에 대한 TCP 연결도 확인합니다. APIC에서 서버를 ping할 수 있지만 LDAP 장애가 지속되면 일반적으로 잘못된 바인드 DN, 잘못된 비밀번호 또는 LDAP 포트를 차단하는 방화벽이 문제가 됩니다.

APIC 로그에서 LDAP 인증 흐름을 검증합니다. 사용자 이름으로 필터링:

<#root>

apic1#

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

작업 중 — LDAP 로그인이 성공하면 전체 검색, 바인딩 및 역할 할당 플로우가 표시됩니다.

```
||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
```

Not Working — LDAP 디렉토리에서 사용자를 찾을 수 없습니다(검색 결과 빈 세트가 반환됨).

```
||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
```

시나리오: LDAP 인증 실패

문제/장애: 사용자가 LDAP 로그인 도메인을 선택하면 로그인이 실패합니다.

확인 단계:

1. APIC에서 LDAP 서버 연결성을 확인합니다.
   <#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. 활성 LDAP 제공자 결함을 확인합니다.
   <#root>

   ```
   apic1#

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

3. LDAP 제공자 컨피그레이션을 확인합니다.
   <#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. 사용자가 구성된 기본 DN 아래의 LDAP 디렉터리에 있으며 필터와 일치하는지 확인합니다. Active Directory의 경우 사용자 특성이 로그인 시 입력한 사용자 이름과 일치해야 **sAMAccountName** 합니다. OpenLDAP의 경우 또는 **cn** 특성이 **uid** 일치해야 합니다.
5. LDAPS(포트 636)를 사용하는 경우 SSL 인증서 체인을 확인합니다. strict**SSLValidationLevel**로 설정된 경우 서버 인증서가 신뢰되지 않거나 만료된 경우 APIC에서 연결을 거부합니다.
6. 전체 LDAP 인증 **nginx.bin.log** 흐름에 대해 APIC를 선택합니다. 중간 메시지가 누락되지 않도록 사용자 이름으로 필터링합니다.
   <#root>

   ```
   apic1#

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

   위의 Operational Verification(운영 확인) 섹션에서 작동 및 비작동 예와 출력을 비교합니다. 로그를 광범위하게 검색하여 추가 LDAP 관련 실패 패턴을 찾을 수 있습니다.

<#root>

apic1#

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

일반적인 비작동 패턴(전체 흐름에 대한 위의 작동 확인 예와 비교):

```
! 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
```

기타 LDAP 실패 패턴:

- LDAP 검색 시간 초과(서버 연결 불가, 저속 또는 방화벽 차단 포트 389/636) — LDAP 검색 실패: ldap_search_ext_s에 대한 반환 코드: -5: 시간 초과됨
- 바인딩 실패(rootdn 또는 바인드 비밀번호가 잘못되었거나 서버에서 연결을 거부함) - Ldap 검색 실패: ldap_search_ext_s에 대한 반환 코드: -1: LDAP 서버에 연결할 수 없음
- 사용자를 찾았지만 암호가 잘못되었습니다(사용자 암호로 바인딩 실패) - 로그에 LDAP 레코드 DN 회선이 표시되지만 UserDN에 바인딩되지 않은 거부된 메시지가 표시됩니다.

RBAC에 대한 LDAP 그룹 맵

LDAP는 특성 대신 그룹 맵을 **cisco-av-pair** 사용합니다. LDAP 제공자의 필드는 **attribute** 그룹 정보를 포함하는 LDAP 특성을 지정합니다. Active Directory의 경우 일반적으로 **memberOf**입니다.

APIC는 반환된 그룹 DN을 구성된 LDAP 그룹 맵 규칙(**aaaLdapGroupMapRule**)과 일치시켜 적절한 보안 도메인 및 역할을 할당합니다. 일치하는 그룹 맵 규칙이 없는 경우 사용자는 인증하지만 역할이 없습니다.

또는 를 로 **attribute** 설정하고 **CiscoAVPair** TACACS+ 및 **shell:domains=all/admin/** RADIUS와 동일한 형식을 따르는 사용자의 LDAP 특성에 값을 직접 저장할 수 있습니다.

근본 원인: 바인드 DN 또는 암호가 올바르지 않거나, 기본 DN에 사용자가 포함되어 있지 않거나, 검색 필터가 디렉터리 스키마와 일치하지 않거나, LDAPS 인증서 유효성 검사에 실패했거나, 그룹 맵 규칙이 없습니다.

해결책: 공급자 컨피그레이션(바인드 DN, 기본 DN, 필터, SSL 설정)을 수정합니다. RBAC 문제의

경우 그룹 맵 규칙이 사용자가 속한 LDAP 그룹과 일치하는지 확인합니다.

RBAC 및 사용자 권한 문제 해결

이 섹션에서는 사용자가 성공적으로 인증했지만 예상 액세스 수준이 없는 경우에 대해 설명합니다.

시나리오: 사용자가 로그인했지만 테넌트가 표시되지 않음

문제/장애: 원격 사용자는 TACACS+, RADIUS 또는 LDAP를 통해 로그인합니다. 로그인이 성공하지만 UI 및 API 호출에서 테넌트가 비어 있는 결과 또는 "403 Forbidden"을 반환하지 않는 것을 사용자에게 확인합니다.

확인 단계:

1. 로그인 시 어떤 역할이 할당되었는지 보려면 사용자 세션을 확인합니다.
   <#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
   ```

   필드에 **descr** 로그인 결과가 표시됩니다. 사용자가 성공적으로 인증되었지만 RBAC 역할이 없는 경우 AAA 서버가 유효한 또는 LDAP 그룹 **cisco-av-pair** 맵 일치를 반환하지 않았습니다.

2. 로그인 중에 AV 쌍 및 역할 할당을 보려면 APIC를 **nginx.bin.log** 선택합니다. 사용자 이름으로 필터링:
   <#root>

   ```
   apic1#

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

   역할 주입 및 도메인 할당 메시지를 찾습니다.

   작업 중 — LDAP 그룹 맵에서 변환된 AV 쌍으로, 사용자가 관리자 역할을 가져옵니다.

   ```
   ||aaa||DBG4||    Adding WriteRole: admin
   ||aaa||DBG4||Converted to CiscoAVPair string shell:domains = all/admin/
   ||aaa||DBG4||Injection of remote user jsmith was completed
   ||aaa||DBG4||Checking all UserDomains under remote Username: jsmith
   ```

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

Not Working — **Cisco-avpair** 또는 **Converted to CiscoAVPair** 줄이 흐름에 나타나지 않으면 AAA 서버가 특성을 반환하지 않고 일치하는 LDAP 그룹 맵 규칙이 없습니다. 뒤에 줄**Checking all UserDomains**이 **Found UserDomain** 없는 사용자를 찾습니다. 사용자가 인증되었지만 역할이 할당되지 않았습니다. 메시지가 **Injection ... data FAILED** 나타나면 AV 쌍 문자열 형식이 잘못되었습니다.

3. AAA 서버가 (TACACS+ 또는 **cisco-av-pair** RADIUS의 경우) 특성을 반환하는지 또는 (LDAP의 경우) 올바른 LDAP 그룹 멤버십을 반환하는지 확인합니다. AAA 서버 컨피그레이션을 확인합니다.
   - TACACS+: 사용자 프로필이 형식**cisco-av-pair**과 함께 포함되는지 확인합니다 **shell:domains=all/admin/.**
   - RADIUS: Access-Accept(액세스 수락)**Cisco-AVPair = "shell:domains=all/admin/"**에서 사용자 프로파일이 반환되는지 확인합니다.
   - LDAP: 사용자가 구성된 LDAP 그룹 맵 규칙(**aaaLdapGroupMapRule**)과 일치하는 LDAP 그룹의 구성원인지 확인합니다.
4. 특성이 있지만 사용자에게 아직 액세스 권한이 없는 경우, 특성의 보안 도메인 이름이 APIC의 기존 보안 도메인과 일치하는지 확인합니다.
   <#root>

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

   에서 **cisco-av-pair** 존재하지 않는 도메인을 참조하는 경우(예: **shell:domains=NonExistentDomain/admin/**) 역할 할당이 자동으로 실패합니다.

근본 원인: AAA 서버가 RBAC 매핑 특성을 반환하지 않거나, 특성 형식이 잘못되었거나, 특성에서 참조하는 보안 도메인이 APIC에 없습니다.

해결책: 올바른 또는 그룹 매핑을 반환하도록 AAA **cisco-av-pair** 서버를 구성합니다. APIC에 보안 도메인이 있는지 확인합니다.

시나리오: 사용자는 구성을 볼 수는 있지만 수정할 수는 없습니다.

문제/장애: 사용자가 로그인하여 객체를 찾아볼 수 있지만 변경 사항을 제출하려고 하면 오류가 발생합니다.

확인 단계:

1. 사용자의 역할 할당을 확인합니다.

```
<#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. 사용자에게 쓰기 액세스 권한이 필요한 경우 역할이 부여해야 **writePriv**합니다. 쓰기 권한이 있는 일반적인 역할에는 admin, tenant-admin, access-admin 및 fabric-admin이 있습니다.
3. APIC 로그에서 역할 할당을 확인합니다. 사용자 이름으로 필터링:

```
<#root>

apic1#

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

인증 흐름의 끝에 있는 역할 할당 메시지를 찾습니다.

작업 중 - 사용자에게 관리자 쓰기 역할이 있음(실제 LDAP 로그인에서):

```
||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 — 로그에 관리자가 아닌 UserRole과 관리자 쓰기 권한 대신 읽기 권한이 있는 경우 사용자는 읽기 전용 역할을 가지며 컨피그레이션을 수정할 수 없습니다. 다음과 같은 행을 찾습니다.

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

로그에 읽기 권한만 표시되고 쓰기 권한은 표시되지 않는 경우, AAA 서버에서 사용자의 역할 또는 AV 쌍을 업데이트합니다.

근본 원인: 사용자에게 쓰기 가능한 역할 대신 읽기 전용 역할(예: 읽기 전용 또는 ops)이 있습니다.

해결책: 쓰기 권한이 있는 역할을 포함하려면 APIC(로컬 사용자의 경우)에서 사용자의 역할 할당을 업데이트하거나 AAA 서버(원격 사용자의 **cisco-av-pair** 경우)에서 를 업데이트합니다.

시나리오: 사용자는 일부 테넌트에 액세스할 수 있지만 다른 테넌트는 액세스할 수 없음

문제/장애: 사용자는 한 테넌트를 보고 관리할 수 있지만 다른 테넌트는 볼 수 없습니다. 액세스 권한이 필요한 경우에도 마찬가지입니다.

확인 단계:

1. 사용자의 보안 도메인 할당을 확인합니다.
   <#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. 보안 도메인은 테넌트에 매핑됩니다. 사용자가 TenantB에 액세스해야 하는 경우 TenantB와 연결된 보안 도메인에도 할당하거나 모든 도메인에 할당해야 합니다.
3. 원격 사용자의 경우 AV 쌍 또는 LDAP 그룹 맵이 올바른 도메인을 할당하는지 확인합니다. 로그인 시 도메인 **nginx.bin.log** 할당에 대한 APIC를 확인합니다. 사용자 이름으로 필터링:
   <#root>

   ```
   apic1#

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

   작업 중 - 사용자가 실제 LDAP 로그인에서 모든 도메인(전체 가시성)을 갖습니다.

   ```
   ||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
   ```

   Not Working — 사용자에게 단일 테넌트 도메인만 있는 경우 메시지에 모두 대신 해당 **Found UserDomain** 도메인만 표시됩니다. 예를 들어, `Found UserDomain TenantA`는 사용자가 TenantA만 볼 수 있음을 의미합니다. 사용자는 AAA 서버의 AV 쌍에 추가 도메인이 필요하거나 전체 액세스를 위해 모든 도메인이 필요합니다.

근본 원인: 사용자는 특정 테넌트만 포함하는 제한된 보안 도메인에 할당됩니다.

해결책: 사용자 구성에 필요한 보안 도메인을 추가하거나 전체 액세스에 모든 도메인을 사용합니다
.

비밀번호 복구 및 긴급 액세스

모든 관리자 계정이 잠겼거나 원격 AAA 서버에 연결할 수 없고 기본 영역이 변경된 경우 다음 복구 방법 중 하나를 사용합니다.

대체 로그인 도메인

ACI는 Default Authentication Realm(기본 인증 영역)과 상관없이 항상 로컬 인증을 사용하는 내장형 폴백 로그인 도메인을 제공합니다. 사용 방법:

- SSH: (또는 **apic:fallback\\admin** 버전에 **apic#fallback\\admin** 따라) 로 로그인합니다.
- GUI: 로그인 화면의 Domain(도메인) 드롭다운에서 fallback(대체)을 선택하고 로컬 자격 증명을 사용합니다.

콘솔 액세스

Console Authentication Realm(콘솔 인증 영역)이 local(기본값)로 설정된 경우 항상 로컬 자격 증명을 사용하여 APIC 콘솔 포트를 통해 로그인할 수 있습니다. 로컬 관리자 비밀번호를 알 수 없는 경우 CIMC(Cisco Integrated Management Controller)(물리적 APIC의 경우) 또는 하이퍼바이저 콘솔(가상 APIC의 경우)을 통해 비밀번호를 재설정할 수 있습니다.

✎ 참고: 콘솔 인증 영역이 원격 AAA 서버로 변경되었고 해당 서버에 연결할 수 없는 경우 콘솔 액세스도 실패합니다. 이는 일반적인 잠금 시나리오입니다. 항상 Console Authentication Realm(콘솔 인증 영역)을 local(로컬)로 설정합니다.

일반 결함 참조

다음 ACI 결함은 일반적으로 원격 액세스 및 AAA 문제와 관련이 있습니다.

- F1773 - TACACS+ 제공자 연결 문제 APIC에서 TACACS+ 서버에 연결할 수 없습니다.
- F1774 — TACACS+ 인증 실패 서버에 연결할 수 있지만 인증 시도를 거부했습니다.
- F1775 — RADIUS 공급자 연결 문제
- F1776 — RADIUS 인증 실패
- F1777 - LDAP 공급자 연결 문제
- F1778 — LDAP 인증 실패
- F0532 - 노드에 대해 관리 서브넷이 구성되지 않았습니다.

활성 AAA 오류 쿼리:

<#root>

```
apic1#

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

참조

- ACI 관리 및 코어 서비스 문제 해결 — 포드 정책
- Cisco APIC 기본 컨피그레이션 가이드, 릴리스 6.1(x) — 관리
- Cisco APIC 보안 컨피그레이션 가이드 — 액세스, 인증 및 어카운팅

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.