ACIファブリックのリモートアクセス問題のトラブルシューティング

はじめに

このドキュメントでは、シスコアプリケーションセントリックインフラストラクチャ(ACI)ファブリックのリモートアクセスの問題を確認、トラブルシューティング、および解決する方法について説明します。APICおよびファブリックスイッチへのセキュアシェル(SSH)およびHypertext Transfer Protocol Secure(HTTPS)アクセス、Terminal Access Controller Access-Control System Plus(TACACS+)によるリモート認証、許可、アカウンティング(AAA)、Remote Authentication Dial-In User Service(RADIUS)、Lightweight Directory Access Protocol(LDAP)、およびロールベースアクセスコントロール(RBAC)許可について説明します。各エリアのトリアージの決定ツリーと詳細なトラブルシューティングシナリオが含まれています。

バックグラウンド情報

このドキュメントの内容は、『ACIの管理およびコアサービスのトラブルシューティング：ポッドポリシー』、『Cisco APIC基本設定ガイド、リリース6.1(x)：管理』の章、および『Cisco APICセキュリティ設定ガイド：アクセス、認証、アカウンティング』の章から合成されたものです。

概要

ACIファブリックへのリモートアクセスには、3つの個別のレイヤが必要です。エンジニアがログインして正常に動作するためには、各レイヤが動作している必要があります。

1. トランスポート：管理ネットワークパス（OOBまたはインバンド）およびプロトコルサービス（SSHまたはHTTPS）が到達可能で有効になっている必要があります。
2. 認証：ユーザのクレデンシャルは、APICでローカルに、またはリモートAAAサーバ（TACACS+、RADIUS、またはLDAP）に対して検証する必要があります。
3. 許可：目的のACIオブジェクトを表示および変更するには、認証されたユーザに正しいRBACの役割とセキュリティドメインを割り当てる必要があります。

どの層で障害が発生しても、異なる症状が現れます。トランスポート障害が発生すると、接続が完全に妨げられます。認証が失敗すると、クレデンシャルエラーが返されます。認証に失敗すると、ログインは可能になりますが、表示が制限されるか、APIで「403 Forbidden」エラーが発生

します。

管理アクセスポリシー

管理アクセスポリシー(commPol)は、ファブリックで有効にするリモートアクセスプロトコルを制御する中央オブジェクトです。これは、Fabric > Fabric Policies > Policies > Pod > Management Access > defaultの順に選択すると表示されます。ポリシーには、次を設定する子オブジェクトが含まれます。

- SSH(commSsh)：管理状態、ポート、暗号、キーエクスチェンジ(KEX)アルゴリズム、メッセージ認証コード(MAC)、およびホストキーアルゴリズム。
- HTTPS(commHttps)：管理状態、ポート、Transport Layer Security(TLS)プロトコルバージョン、スロットル率、クライアント証明書認証。
- Telnet(commTelnet)：管理状態およびポート。Telnetはデフォルトで無効になっているため、無効のままにしておくことを推奨します。

OOBおよびインバンド管理

ACIノードは、次の2つの管理アクセスパスをサポートします。

- アウトオブバンド(OOB):APICまたはスイッチの専用管理ポートを使用します。OOB管理アドレスは、mgmtテナントの下のプールから割り当てられ、mgmtRsOoBStNodeを介してノードに割り当てられます。APICでは、OOB契約はiptablesルールによって適用されます。OOB契約が適用されると、契約によって明示的に許可されたトラフィックだけがAPIC管理インターフェイスに到達できます。
- インバンド(INB)：管理トラフィックにファブリックデータプレーンを使用します。インバンド管理には、ブリッジドメイン(BD)、サブネット、エンドポイントグループ(EPG)、コントラクト、およびノード管理アドレスの割り当てが必要です。インバンドIPアドレスは、追加のルーティングまたはポリシー設定を行わないと、ファブリックの外部から到達できません。

注:APIC OOB管理IPは初期設定時に設定され、APICはファブリックが完全に検出される前にIP接続を取得します。OOBはプライマリ管理パスであり、物理管理ネットワークが接続されている場合は常に使用できます。

AAAアーキテクチャ

ACIは3階層のAAAモデルを使用します。

1. Login Domain(aaaLoginDomain):AAAプロバイダーを名前付きレルムでグループ化します。ユーザはログイン画面でログインドメインを指定します(たとえば、apic:TACACS-Domain、またはUIのドロップダウンから)。 特殊なフォールバックログインドメインは常に存在し、ローカル認証にマッピングされます。
2. Provider Group(**aaaTacacsPlusProviderGroup、 aaaRadiusProviderGroup、 aaaLdapProviderGroup**):1つ以上のAAAサーバを参照し、それらのサーバが試行される順序を定義します。
3. Provider(aaaTacacsPlusProvider、**aaaRadiusProvider、 aaaLdapProvider**)：サーバのIP、ポート、共有秘密（LDAPの場合はバインドDN）、タイムアウト、再試行、管理EPG、およびモニタリング認証情報を定義します。

Default Authentication Realm(**aaaDefaultAuth**)は、ユーザがログイン時にログインドメインを指定しなかった場合に使用されるログインドメインを決定します。コンソール認証レルムは、コンソールセッションの認証を制御します。

注：サーバに到達できないときにデフォルトの認証レルムをリモートAAAサーバに変更すると、ファブリックからロックアウトされます。レルムを変更する前に、必ずAAAサーバの接続をテストしてください。fallbackログインドメイン(apic:fallback\\admin)を使用すると、デフォルトのレルムをバイパスして、ローカルで認証できます。

主なAAAログファイル

AAA認証イベントは、APICとファブリックスイッチの両方で複数のファイルに記録されます。これらのログは、認証結果の検証、使用されるレルムとプロバイダーグループの特定、ロール割り当ての失敗の診断を行うための主要なツールです。

ログファイル	ロケーション(APIC)	ロケーション（スイッチ）	
nginx.bin.log(APIC) nginx.log（スイッチ）	/var/log/dme/log/nginx.bin.log	/var/sysmgr/tmp_logs/dme_logs/nginx.log	プライ な認証 レルム 検索、 LDAP 信、A とロー または ます。 トフォ ますが 同じて
アクセス。ログ	/var/log/dme/log/access.log	/var/log/dme/log/access.log	NGIN API要 は、aa aaaRef

ログファイル	ロケーション(APIC)	ロケーション（スイッチ）	
			HTTP（200）で表チでは とaaa します
pam.module.logを開きます。	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	PAM SSH （認証 IP、お UNIX す。 ユーザ された 速な方

注：プライマリAAAログのファイル名はプラットフォームごとに異なります。APICでは、**nginx.bin.log**(/var/log/dme/log/)です。リーフ/スパインスイッチでは、**/var/sysmgr/tmp_logs/dme_logs/**にあるnginx.logです。ログのコンテンツ形式とAAAメッセージは、両方のプラットフォームで同じです。

nginxログのAAAエントリは次の形式に従います。

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

特定のユーザの認証フローのAAA関連のログエントリをフィルタリングします。

<#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
```

または、最近の認証要求と結果をすべて表示します。

<#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
```

一般的な正常な認証フローは、次のキーメッセージを順番に示しています。

1. Received PAM authenticate request from nginx for Username: <user>：ログイン要求を受信しました。
2. DefaultAuthMoはrealm <N>を指定します。プロバイダーグループ<名前>！– レルムが選択されました（0=フォールバック/ローカル、2=TACACS+、3=LDAP）。
3. プロバイダー固有のメッセージ（LDAPバインド、TACACS+プロバイダー検索、またはRADIUS要求）。
4. Found UserDomain <domain> under remote Username: <user>:AAA応答からのドメイン割り当て。
5. Found Username: admin with admin write privileges under UserDomain all - user is an admin user：ロールチェックに合格しました。

失敗した認証ログ：

- AAA認証中にユーザ<user>が拒否された
- Unauthorized user <user> error: AAA Server Authentication DENIED

注: nginxログは頻繁にローテーションされ、古いエントリは数値のサフィックスでgzip圧縮されます。APICでは、ローテーションされたログは同じディレクトリにあります(例：**nginx.bin.log.22815.gz**)。 スイッチでは、ローテーションされたログは**/var/log/dme/oldlog/dme/nginx.log.*.gz**に保存されます(シンボリックリンクは/var/sysmgr/tmp_logs/dme_logs/にあります)。 回転したログを検索するには、次の手順に従います。

<#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モデル

ACI RBACは、認証されたユーザが表示および実行できる内容を制御します。このモデルには、次の3つのコンポーネントがあります。

- セキュリティドメイン(**aaaDomain**):ACIオブジェクト（テナント、アクセスポリシー、ファブリックポリシー）にマッピングされるスコープリミッタ。 組み込みドメインのall、common、およびmgmtは常に存在します。カスタムドメインは、ユーザの可視性を特定のテナントまたはポリシーエリアに制限します。
- Role(aaaRole)：権限のセットを定義します。構築済みのロールには、admin、aaa、tenant-admin、tenant-ext-admin、read-all、access-admin、fabric-admin、ops、およびnw-svc-adminがあります。
- 特権：各ロールは、特定の機能領域への読み取り（読み取りを暗黙的に示す）または書き込み（読み取りを暗黙的に示す）アクセスを許可します。

ユーザーアカウントには、1つ以上のセキュリティドメインと役割のペアが割り当てられます。TACACS+、RADIUS、またはLDAPで認証されたリモートユーザの場合、ロールマッピングは、AAA応答のベンダー固有属性(**cisco-av-pair**属性など)によって提供されます。

トリアージ決定ツリー

このDecision Treeは、ACIファブリックにリモートからアクセスできないとユーザが報告した場合に使用します。

1. APICまたはスイッチの管理IPにpingを実行できますか。
   - No →管理ネットワークパスのトラブルシューティングを行います。「OOBおよびインバンド管理のトラブルシューティング」のセクションを参照してください。
   - はい→続行します。
2. SSHまたはHTTPS接続を確立できますか（接続は開いていますか）。
   - No →プロトコルサービスを無効にすることも、ポートをフィルタ処理することも、暗号の不一致を示すこともできます。「SSHアクセスのトラブルシューティング」また

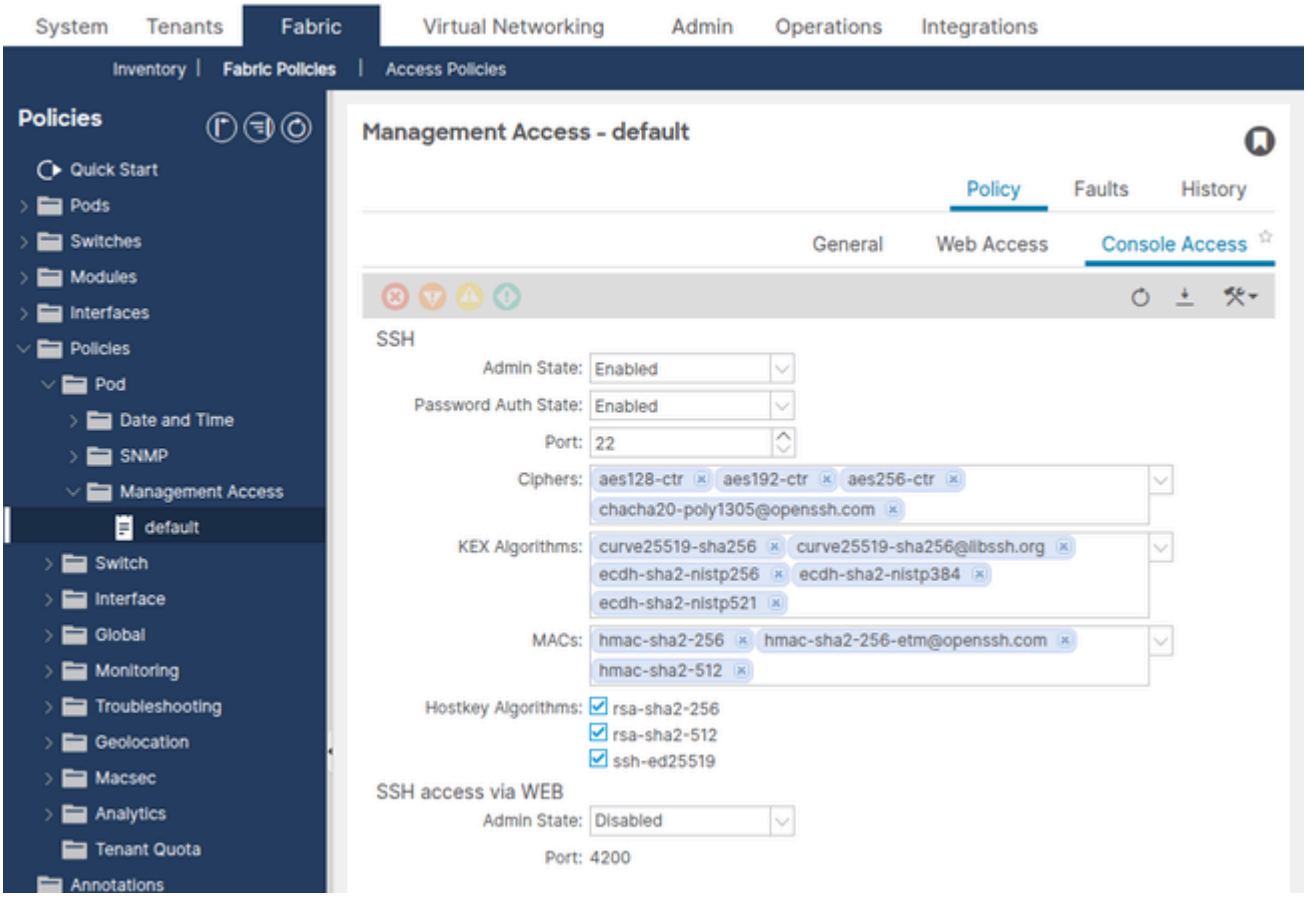
は「HTTPSアクセスのトラブルシューティング」のセクションを参照してください。
    - はい→続行します。
3. ログイン画面が表示されますか(HTTPS)、またはSSHハンドシェイクが完了してクレデンシャルの入力を求められますか。
    - → SSHキー交換またはTLSハンドシェイクの失敗はありません。暗号とKEXの不一致については、「SSHアクセスのトラブルシューティング」のセクションを参照してください。
    - はい→続行します。
4. クレデンシャルが「Authentication Failed」または同様のメッセージで失敗しますか。
    - はい→認証の問題です。「AAA認証のトラブルシューティング」のセクション（使用している口グインドメインに応じてTACACS+、RADIUS、またはLDAP）を参照してください。
    - 続行→ません。
5. ユーザが口グインしても、予期されたオブジェクトが表示されないか、または「403 Forbidden」エラーが表示されるか。
    - はい→認証またはRBACの問題です。「RBACとユーザ権限のトラブルシューティング」のセクションを参照してください。
    - → Accessが機能していない。ユーザに発生している特定の問題を確認します。

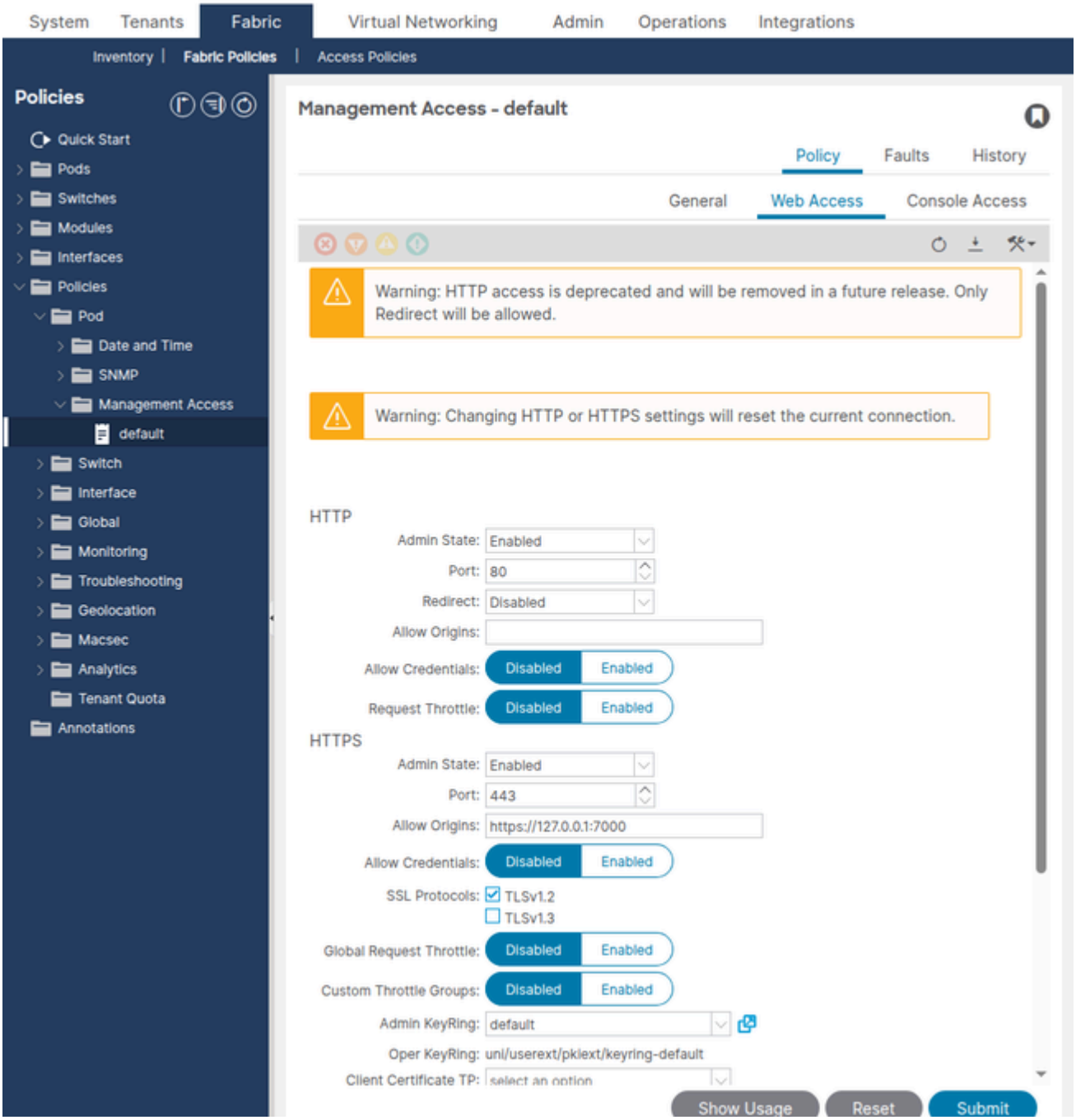
設定の確認

動作状態のトラブルシューティングを行う前に、設定チェーンが完了していることを確認します。設定ミスは、リモートアクセスの問題の最も一般的な根本原因です。

管理アクセスポリシー（SSHおよびHTTPS）の確認

Fabric > Fabric Policies > Policies > Pod > Management Access > defaultの順に移動します。


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



次のSSH設定を確認します。

- Admin State:enabledである必要があります。
- Port：デフォルトは22。変更した場合、SSHクライアントはカスタムポートを使用する必要があります。
- Password Authentication:enabled（証明書のみの認証を意図していない場合）。
- SSH暗号:SSHクライアントでサポートされる暗号を少なくとも1つ含む必要があります。
- KEXアルゴリズム:SSHクライアントでサポートされるアルゴリズムを少なくとも1つ含む必要があります。
- SSH MAC:SSHクライアントでサポートされるMACを少なくとも1つ含む必要があります。

APIを使用してSSH管理対象オブジェクトを照会します。

<#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
```

次のHTTPS設定を確認します。

- Admin State:enabledである必要があります。
- Port：デフォルトは443。
- SSLプロトコル:TLSv1.2（デフォルト）。 古いクライアントでは、TLSv1.1を明示的に追加する必要があります。
- Throttle State：有効にすると、Throttle Rateにより、ユーザごとの1秒あたりの要求が制限されます。非常に低い値を設定すると、APIタイムアウトエラーが発生する可能性があります。

<#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
```

よくある設定上の間違い

- SSH暗号の制限が厳しすぎる:ACIリリース5.2(1)以降では、デフォルトのSSH暗号が強化されています。古いSSHクライアント(0.75より前のPuTTYバージョンや、**diffie-hellman-group14-sha1**のみを提供するOpenSSHバージョンなど)では、キー交換が失敗する可能性があります。SSHクライアントで「no matching cipher found」または「no matching key exchange method found」が表示されます。
- Password authentication disabled:passwordAuthがdisabledに設定されている場合は、

SSHキーベースの認証だけが許可されます。パスワードを使用して接続するユーザには、「Permission denied (publickey)」と表示されます。
- クライアント認識なしのカスタムSSHポート:SSHポートが22から変更された場合、SSHクライアントは新しいポートを指定する必要があります(たとえば、**ssh -p 2222 admin@10.1.1.1**)。

OOB管理アドレスの確認

Tenants > mgmt > Node Management Addressesの順に移動します。

すべてのAPICとスイッチノードに、有効なゲートウェイが割り当てられたOOB管理IPアドレスがあることを確認します。管理アドレスを持たないノードには、管理ネットワークを介して到達できません。

APIを介してOOB静的ノード割り当てを照会します。

<#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
```

よくある設定上の間違い

- OOBアドレス割り当ての欠落：スイッチは**mgmtRsOoBStNode**の下にエントリを持っていません。ノードには管理IPがなく、OOBインターフェイス上のSSHまたはHTTPSに応答しません。
- ゲートウェイが正しくない – ゲートウェイアドレスが、OOB管理ネットワーク上の実際のゲートウェイと一致しない。ノードはパケットを受信できますが、リターントラフィックを送信できません。
- サブネットマスクの不一致 — OOBサブネットマスクが物理管理ネットワークと一致しません。これにより、ノードは管理ステーションが別のサブネット上にあると認識し、存在しないゲートウェイまたは正しくないゲートウェイを介してトラフィックをルーティングする可能性があります。

OOB契約の確認

Tenants > mgmt > Contractsの順に移動します。

OOB契約がOOB管理EPGに適用されると、その契約によって明示的に許可されたトラフィックだけがAPIC管理インターフェイスに到達します。APICでは、OOB契約はiptablesルールによって適用されます。

OOB EPGが提供したコントラクトを照会します。

<#root>

apic1#

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

クエリの結果が返されると、契約が適用されます。コントラクト対象およびフィルタで必要なプロトコルが許可されていることを確認します。

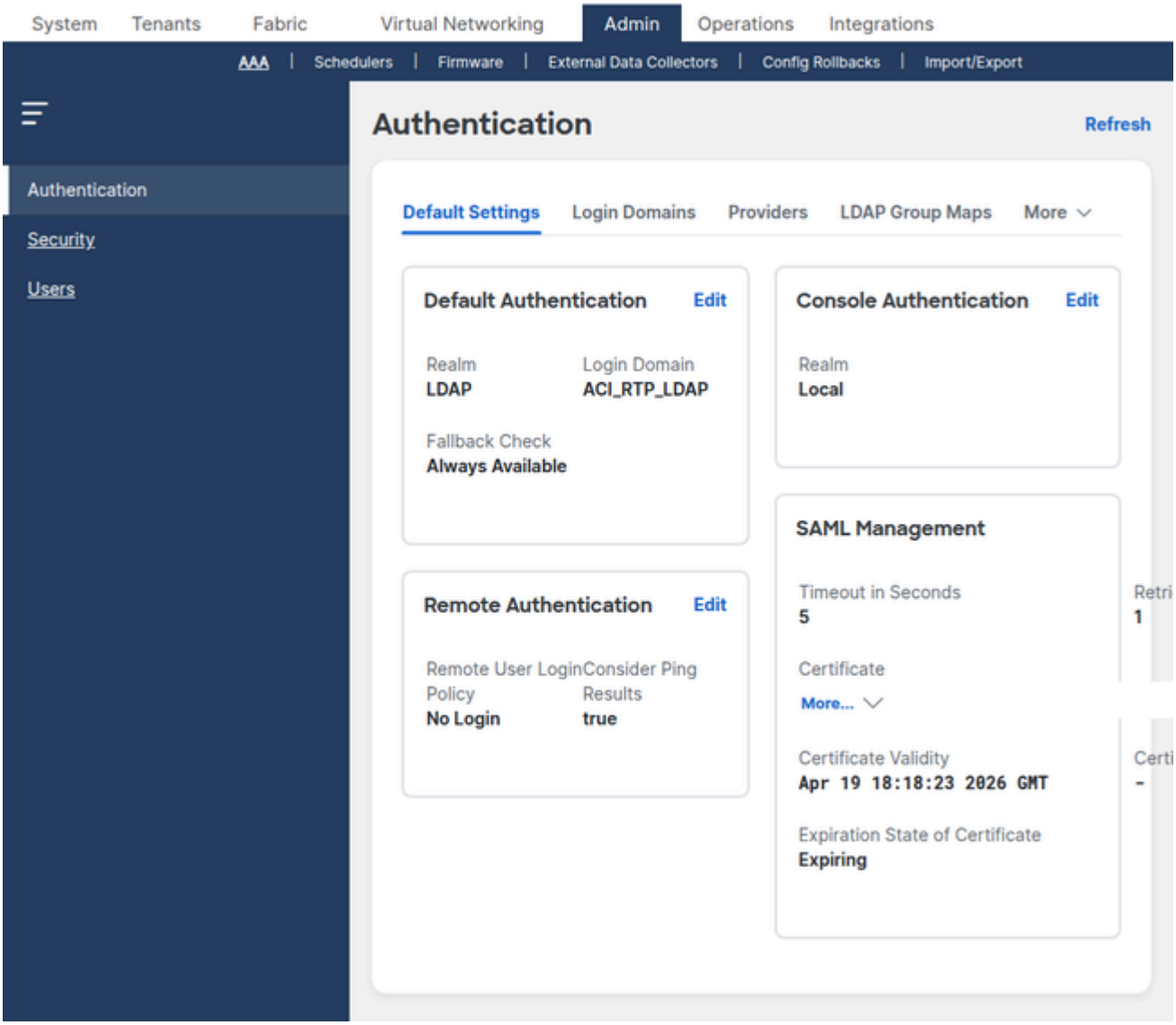
- SSH:TCPポート22（またはカスタムポート）
- HTTPS:TCPポート443（またはカスタムポート）
- ICMP:ping検証用

よくある設定上の間違い

- OOB契約にSSHまたはHTTPSが含まれていない：エンジニアはAPICにpingできますが、SSHまたはHTTPS経由で接続できません。APICのiptablesルールでは、通知せずにトラフィックがドロップされます。
- OOBコントラクトフィルタでの送信元IP制限：コントラクトフィルタは、特定の送信元サブネットへのアクセスを制限します。そのサブネット外のエンジニアは接続できません。

AAA設定の確認

Admin > AAA > Authentication > AAAの順に移動します。



次の内容を確認します。

- Default Authentication Realm：ユーザがログインドメインを指定しなかった場合に使用されるログインドメインを指定します。リモートAAAログインドメインに設定する場合、対応するサーバに到達できる必要があります。
- コンソール認証レルム：コンソールアクセスを制御します。localに設定すると、コンソールログインは常にローカルクレデンシャルを使用します（推奨）。

ログインドメインの確認

Admin > AAA > Authentication > Login Domainsの順に移動します。

<#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
```

認証に使用されるログインドメインが存在し、正しいプロバイダーグループを参照していることを確認します。

TACACS+プロバイダーの確認

Admin > AAA > Authentication > TACACS+ > TACACS+ Providersの順に選択します。

```
<#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プロバイダーの確認

Admin > AAA > Authentication > RADIUS > RADIUS Providersの順に移動します。

```
<#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プロバイダーの確認

Admin > AAA > Authentication > LDAP > LDAP Providersの順に移動します。

<#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
```

一般的なAAAの設定ミス

- Shared secret mismatch:ACI TACACS+またはRADIUSプロバイダーに設定されているキーが、サーバのキーと一致しません。認証は通知なしで失敗します。
- 誤った管理EPG：プロバイダーの**epgDn**が空であるか、誤ったEPGを指しています（たとえば、サーバがOOBネットワーク上にある場合のインバンド）。 APICがサーバに到達できません。
- Login domain realm mismatch：ログインドメインはLDAPとして設定されていますが、ユーザはTACACS+認証を想定しています。ログインドメインは正しいプロバイダーグループタイプを参照する必要があります。
- LDAPバインドDNが正しくない — **rootdn**（バインドDN）または**basedn**が間違っています。ユーザクレデンシャルが正しくても、LDAP認証はバインドエラーで失敗します。
- LDAPフィルタがディレクトリスキーマと一致しません。Active Directoryの場合は、**sAMAccountName=$userid**を使用します。OpenLDAPの場合は、**cn=$userid**または**uid=$userid**を使用します。

RBAC設定の確認

Admin > AAA > Usersの順に移動し、ローカルユーザアカウントとそのセキュリティドメインおよびロールの割り当てを表示します。

APIを使用してセキュリティ・ドメインをクエリーする：

<#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
```

ドメインallに割り当てられ、ロールadminを持つユーザには、ファブリック全体に対する完全な読み取り/書き込みアクセス権があります。ロールtenant-adminを持つカスタムセキュリティドメインに割り当てられたユーザは、そのドメインに関連付けられているテナントのみを管理できます。

一般的なRBACの設定ミス

- セキュリティドメインなしで作成されたユーザ：ユーザはログインできますが、テナントが表示されず、APIコールで「403 Forbidden」を受信します。少なくとも1つのセキュリティドメインを割り当てる必要があります。
- 書き込みアクセスが必要なときに割り当てられる読み取り専用ロール：ユーザはオブジェクトを表示できますが、変更を送信できません。ロール権限がwritePrivに設定されていることを確認します。
- AAAサーバにリモートユーザロールマッピングがない — TACACS+またはRADIUSサーバが、**shell:domains=all/admin/**を含む**cisco-av-pair**属性を返しません。ユーザは正常に認証されますが、ロールがなく、ファブリック内に何も表示されません。

OOBおよびインバンド管理のトラブルシューティング

APICまたはスイッチの管理IPがネットワーク上で到達不能な場合は、SSH、HTTPS、またはAAAを調査する前に、管理パスのトラブルシューティングを行ってください。

シナリオ：APIC OOB IPにpingできない

問題：管理ステーションがAPIC OOB管理IPアドレスにpingを実行できない。

確認手順:

1. APIC管理ポートが物理的に接続され、リンクがアップしていることを確認します。
2. 管理ステーションが同じL2セグメント上にあるか、OOBサブネットへのルートがあることを確認します。
3. OOB管理IPが正しく割り当てられていることを確認します。
   <#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. デフォルトゲートウェイに到達できることを確認します。
   <#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契約が適用されている場合は、必要なプロトコルが許可されていることを確認します。「OOBコントラクトの確認」セクションに示すように、OOB EPGが提供するコントラクトを照会します。OOBコントラクトは、APIC上の**iptables**ルールとして適用されます。APICシェルから保存済みのルールを表示できます。
   <#root>

   ```
   apic1#

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

   INPUTポリシーがDROPで、必要なプロトコルのACCEPTルールがない場合、OOBコントラクトはトラフィックをフィルタリングしています。

   > 注：ライブカーネルルールを表示する**iptables -L -n**コマンドはルートアクセスを必要とし、通常の管理者SSHセッションでは使用できません。

根本原因： OOB管理アドレスが欠落しているか正しく設定されていない、ゲートウェイが正しく

ない、またはOOB契約がトラフィックをフィルタリングしている。

解決策：OOBアドレス割り当てを修正するか、物理ネットワークパスを確認するか、OOB契約を更新して必要なプロトコルを許可します。

シナリオ：スイッチ管理IPに到達できない

問題：管理ステーションはAPICに到達できますが、OOB経由でスイッチに到達できません。

確認手順:

1. スイッチにOOBアドレスが割り当てられていることを確認します。
   <#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. スイッチ管理インターフェイスにIPが割り当てられていることを確認します。
   <#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. 管理VRFデフォルトルートを確認します。
   <#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： OOBアドレスが割り当てられていないか、ゲートウェイが正しくないか、スイッチ管理の物理ポートがダウンしています。

解決策：Tenants > mgmt > Node Management AddressesでOOBアドレスを割り当てます。物理

管理リンクがアップしていることを確認します。

SSHアクセスのトラブルシューティング

このセクションでは、管理IPに到達できるが（pingは成功する）、SSHセッションが確立または認証に失敗するシナリオについて説明します。

シナリオ：SSH接続が拒否される

問題： APICまたはスイッチに接続する際に、SSHクライアントが「Connection refused」と報告する。

確認手順:

1. 管理アクセスポリシーでSSHが有効になっていることを確認します。
   <#root>

   ```
   apic1#

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

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

   adminStがdisabledの場合、SSH接続は拒否されます。
2. 正しいポートが使用されていることを確認します。SSHポートを22から変更した場合：
   <#root>

   ```
   $

   ssh -p

    custom-port

   admin@10.1.1.1
   ```

3. OOBコントラクトがSSHポートでTCPを許可していることを確認します。「OOB契約の確認」のセクションを参照してください。

根本原因：管理アクセスポリシーでSSHが無効になっているか、クライアントに認識されないカスタムポートがあるか、OOB契約フィルタリングです。

解決策：管理アクセスポリシーでSSHを有効にするか、正しいポートを使用します。

シナリオ：SSHキー交換の失敗（暗号またはKEXの不一致）

問題： SSHクライアントが「一致する暗号が見つかりません」、「一致するキー交換方式が見つかりません」、または「一致するMACが見つかりません」で失敗します。

確認手順:

1. SSHクライアントの詳細出力を確認して、クライアントが提供するアルゴリズムを特定します。
   <#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. クライアントが提供するアルゴリズムとAPICが設定されたアルゴリズムを比較します。
   <#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. 交点を指定します。どのカテゴリにも共通のアルゴリズムがない場合、ハンドシェイクは失敗します。

注:ACIリリース5.2(1)以降では、デフォルトのSSH暗号およびKEXアルゴリズムが強化されました。**diffie-hellman-group1-sha1、 diffie-hellman-group14-sha1、 aes128-cbc、 hmac-sha1**などのレガシーアルゴリズムは、デフォルトで提供されなくなりました。最近アップグレードした場合は、環境内のSSHクライアントが新しいデフォルトをサポートしていることを確認します。

根本原因：ACIアップグレード後または暗号の堅牢化後に、SSHクライアントとAPIC間に共通の暗号、KEXアルゴリズム、またはMACが存在しない。

解決策：最新のアルゴリズムをサポートするようにSSHクライアントを更新するか、必要なレガ

シーアルゴリズムを管理アクセスポリシーに再追加します。従来のアルゴリズムを再度追加すると、セキュリティ上のリスクが生じるため、長期的な使用はお勧めしません。

シナリオ：SSHは接続するが、ローカルユーザの認証が失敗する

問題： SSHハンドシェイクは成功しますが（パスワードプロンプトが表示されます）、ローカルユーザのパスワードは拒否されます。

確認手順:

1. ユーザがローカルに存在することを確認します。
   <#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. ログイン試行の失敗回数が多すぎることが原因でアカウントがロックされているかどうかを確認します。
   <#root>

   ```
   apic1#

   moquery -c aaaUserEp

   dn                 : uni/userext
   pwdStrengthCheck   : no
   ```

   Admin > AAA > Security Management > Lockout Policyの順に選択して、ログインドメインロックアウトポリシーを確認します。

3. ユーザが正しいログインドメインでログインしていることを確認します。デフォルトの認証レルムがリモートのAAAログインドメインに設定されている場合、ユーザはローカル認証を強制するために**apic:LOCAL\\username**または**apic:fallback\\username**を先頭に追加する必要があります。
4. ログで認証結果を検証します。APICの**nginx.bin.log**でログインイベントを確認します。
   <#root>

   ```
   apic1#

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

   ログイン試行に割り当てられているレルムとプロバイダーグループを探します。

```
! 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
```

レルムが0（フォールバック/ローカル）でない場合、ログインはローカルデータベースではなくリモートAAAサーバに送信されます。ユーザがローカル認証を強制するためには、**apic:fallback\\username**または**apic:LOCAL\\username**を先頭に付加する必要があります。

根本原因：パスワードが正しくない、アカウントがロックされている、またはログインの試行がローカルデータベースではなくリモートAAAサーバに送信されている。

解決方法：パスワードをリセットするか、アカウントのロックを解除するか、正しいログインドメインプレフィックスを使用してください。

HTTPSアクセスのトラブルシューティング

このセクションでは、APIC Web UIまたはRepresentational State Transfer(REST)のアプリケーションプログラミングインターフェイス(API)にHTTPSで到達できないシナリオについて説明します。

シナリオ：HTTPS接続がタイムアウトする

問題：ブラウザに「ERR_CONNECTION_TIMED_OUT」と表示されるか、またはポート443でAPICに接続する際にAPIコールがハングします。

確認手順:

1. HTTPSが有効になっていることを確認します。

<#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コントラクトがTCP 443を許可していることを確認します。「OOB契約の確認」のセクションを参照してください。
3. APIC自体からテストして、HTTPSプロセスがリッスンしていることを確認します。
<#root>

apic1#

ss -tlnp | grep 443

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

根本原因：HTTPSが無効になっているか、TCP 443をフィルタするOOB契約があるか、またはAPICのnginxプロセスがクラッシュしました。

解決策：管理アクセスポリシーでHTTPSを有効にするか、OOB契約を更新するか、APICでWebサービスを再起動します。

シナリオ：ブラウザにTLSハンドシェイクエラーが表示される

問題：ブラウザに「ERR_SSL_VERSION_OR_CIPHER_MISMATCH」または同様のTLSエラーが表示されます。

確認手順:

1. APICで設定されているTLSプロトコルバージョンを確認します。
<#root>

apic1#

moquery -c commHttps

sslProtocols : TLSv1.2

2. ブラウザがTLSv1.2をサポートしていることを確認します。非常に古いブラウザ（Internet Explorer 10以前など）は、デフォルトではTLSv1.2をサポートしていません。

根本原因： APICはTLSv1.2（デフォルト）のみを提供し、ブラウザまたはAPIクライアントは古いTLSバージョンのみをサポートします。

解決策：ブラウザまたはクライアントを更新します。古いクライアントを一時的にサポートする必要がある場合は、管理アクセスポリシーにTLSv1.1を追加します。ただし、これによりセキュリティ上のリスクが生じます。

シナリオ：APIスロットル制限

問題：HTTP 503エラーでREST APIのコールが断続的に失敗するか、ヘビーオートメーション中にWeb UIの反応が遅くなる。

確認手順:

<#root>

```
apic1#

moquery -c commHttps

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

スロットル率が非常に低く、自動化スクリプトが1秒間に多くの要求を送信する場合、APICは過剰な要求を拒否します。

根本的な原因：ユーザーごとのスロットル率が自動化ワークロードに対して低すぎます。

解決策：管理アクセスポリシーのスロットル率を上げるか、自動化スクリプトを最適化して要求頻度を減らします。または、ファブリックが共有されていない場合はスロットリングを無効にします。

AAAのトラブルシューティング：TACACS+

このセクションでは、TACACS+認証の失敗について説明します。APICはTCPポート49経由でTACACS+サーバと通信します。

動作検証

ACIスイッチは、スタンドアロンNX-OSで使用できる**test aaa**コマンドをサポートしていません。TACACS+の動作を確認するには、APICを使用してプロバイダーのステータス、障害、ログインセッション履歴を確認します。

TACACS+プロバイダーのアクティブな障害を確認します。

```
<#root>

apic1#

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

障害が返されない場合、APICはプロバイダーが到達可能であると見なします。障害が存在する場合、出力にはF1773（プロバイダーが到達不能）やF1774（認証の失敗）などの障害コードが含まれます。

TACACS+プロバイダーの設定を確認します。

```
<#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
```

APICからTACACS+サーバへの基本的なネットワーク到達可能性を確認します。

```
<#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+ログインドメインを使用してAPICへのログインを試行し、セッションの結果を確認し

ます。

<#root>

apic1#

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

descrフィールドを見て、障害の原因が認証の拒否にあるのか、または接続の問題にあるのかを判断します。

APICログでTACACS+認証フローを検証します。問題のユーザ名のフィルタ：

<#root>

apic1#

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

TACACS+のログインは、LDAPと同じ**nginx.bin.log**認証フローに従います（完全な実際のログの例については、「LDAPの動作検証」セクションを参照してください）。 TACACS+の主な違いは次のとおりです。

- DefaultAuthMoがレルム2を指定：レルム2はTACACS+を示します（LDAPではレルム3）。
- Adding TacacsProvider <IP> to the list：接続するTACACS+サーバを識別します(vs. LdapProvider for LDAP)。
- TACACS+ Cisco-avpair(shell:domains=all/admin/):AVペアは（LDAPグループマップから変換されるのではなく）TACACS+サーバから直接返されます。

成功した TACACS+ログインは、次のように同じ手順で行われます。PAM要求→レルム選択→プロバイダールックアップ→ AVペア解析→ユーザインジェクション→ UserDomainおよびロール割り当て→admin write権限。

失敗した TACACS+ログインは、「User <username> was denied during AAA authentication」および「Unauthorized ... error: AAA Server Authentication DENIED」で終わります。これはLDAP拒否と同じパターンです。

シナリオ：TACACS+認証の失敗

問題：ユーザがTACACS+ログインドメインを選択すると、「Authentication Failed」でログインが失敗する。

確認手順:

1. TACACS+プロバイダーのアクティブな障害を確認します。
   <#root>

   ```
   apic1#

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

   障害F1773は、接続の問題を示しています。障害F1774は、認証拒否を示しています。

2. APICからTACACS+サーバへのネットワーク到達可能性を確認します。
   <#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. pingは成功するが認証が失敗する場合は、APICプロバイダーの設定とTACACS+サーバの設定の両方で共有秘密が一致することを確認します。
4. 失敗の詳細を確認するには、最新のログインセッションを確認します。
   <#root>

   ```
   apic1#

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

5. TACACS+サーバのログで認証の試行を確認します。サーバにログオンしたが拒否された場合は、サーバ側のユーザ設定の問題（パスワードの不一致やユーザアカウントの欠落など）を示しています。
6. APIC **nginx.bin.log**で完全な認証フローを確認します。中間メッセージが失われないように、特定のキーワードではなくユーザ名でフィルタリングします。
   <#root>

   ```
   apic1#

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

   出力を、上記の「動作検証」セクションの動作している例と動作していない例と比較します。主要指標：

   - `was denied` or `DENIED`:TACACS+サーバに到達したが、クレデンシャルが拒否された。ユ

ーザがサーバに存在し、パスワードが一致することを確認します。

- TacacsProviderの追加後にプロバイダー固有のメッセージが表示されない：サーバが到達不能またはタイムアウトしている。ネットワーク到達可能性と管理EPGを確認します。
- リモートユーザのインジェクトが完了し、その後、ロールチェック行が表示される – 認証は成功しましたが、ロール割り当てに問題がある可能性があります（次のAVペアセクションを参照）。

RBAC用TACACS+ cisco-av-pair

TACACS+で認証されたリモートユーザの場合、サーバは認証応答で**cisco-av-pair**属性を返す必要があります。この属性は、ユーザをACIセキュリティドメインとロールにマッピングします。

形式:

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

例:

- 完全な管理者：**shell:domains=all/admin/**
- すべて読み取り専用： **shell:domains=all/read-all/**
- 特定のドメインのテナント管理者：**shell:domains=TenantA/tenant-admin/**
- 複数のドメイン：**shell:domains=all/admin/,TenantA/tenant-admin/**

この属性が存在しないか、形式が正しくない場合、ユーザは正常に認証されますが、ロールがなく、APIC UIでオブジェクトを表示できません。

注：リーフスイッチおよびスパインスイッチへのSSHアクセスには、allセキュリティドメインにwrite権限を持つadminロールが必要です。スイッチSSHアクセスに最小限必要なAVペアは、**shell:domains=all/admin/**です。管理者ロール以外のロール(read-all、tenant-admin、aaaなど)を持つユーザ、またはall以外のセキュリティドメインに割り当てられたユーザは、APICにログインできますが、スイッチへのSSHアクセスは拒否されます。APICログは、これらのユーザについてスイッチ上の非管理者ログインが拒否されていることを示します。

---

nginx.bin.logを確認して、受信したAVペアを検証します。完全なロール注入フローを確認するには、ユーザ名でフィルタリングします。

```
<#root>

apic1#
```

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

TACACS+の場合、AVペアはTACACS+ Cisco-avpair(shell:domains=...)として記録されます。 正常にインジェクトされると、「Injection of remote user <username> was completed」の後に「Found UserDomain」と「admin write privileges」の行が続くことが示されます（実際のログ出力を含むこのフローの完全な例については、「LDAP Operational Verification」の項を参照してください）。

AVペアの形式が無効な場合、ログには「Injection of remote user <username> data FAILED - error message is Invalid shell:domains string」と表示されます。ユーザが非管理者ロールで認証されると、スイッチへのSSHは拒否され、スイッチへの非管理者ログインは拒否されます。

根本原因：共有秘密が一致しない、管理ネットワークからサーバに到達できない、TACACS+サーバにユーザが存在しない、またはプロバイダーの管理EPGが正しくない。

解決策：共有秘密を修正し、到達可能性を修正するか、TACACS+サーバでユーザを作成します。

リーフスイッチ認証ログの検証

リーフスイッチおよびスパインスイッチでは、SSHログインイベントは**pam.module.log**と**nginx.log**の両方に記録されます。**pam.module.log**にはPAMの認証結果（許可または拒否）が表示されます。**nginx.log**には、完全なAAAフロー（レルム選択、プロバイダー検索、LDAP/TACACS+/RADIUS通信、AVペア解析、ロール割り当て）が含まれています。これらはAPICの**nginx.bin.log**と同じです。これらのログは、すべてのリモートAAAタイプ(TACACS+、RADIUS、LDAP)に適用されます。

pam.module.logで認証結果を確認します。

<#root>

leaf101#

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

Working:switch：でのリモート認証の成功

```
||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
```

remote=1フラグは、ユーザがリモートAAAサーバによって認証されたことを確認します。

Not Working：ユーザは拒否されました。securitymgrAGはユーザを拒否し、スイッチは最終的なフォールバックとしてローカルユーザルックアップを試行します。

```
||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
```

ユーザのPAMエントリがまったく表示されない場合は、SSH接続がPAM段階に達する前に拒否された可能性が高くなります（暗号の不一致やユーザによる接続のキャンセルなど）。

スイッチ上の認証フローの詳細を表示するには、**nginx.log**を確認します。このログには、完全なAAAデシジョンチェーン(APICの**nginx.bin.log**と同じ形式とメッセージ)が含まれています。

<#root>

leaf101#

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

Working：スイッチ上で成功したLDAP認証（「LDAP動作検証」セクションのAPIC LDAPの例と比較。メッセージは同じです）。

```
||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
```

スイッチ**nginx.log**は、**pam.module.log**に拒否が示されるものの、その理由が説明されていない場合に特に役立ちます。nginx.logは、AAAレルム、プロバイダー、および特定のエラーの原因（たとえば、LDAP検索で空が返された、TACACS+タイムアウトが返された、またはAVペアインジェクションが失敗した）を明らかにします。

AAAのトラブルシューティング：RADIUS

このセクションでは、RADIUS認証の失敗について説明します。APICは、UDPポート1812（認証）とオプションのUDPポート1813（アカウンティング）を介してRADIUSサーバと通信します。

動作検証

ACIスイッチは、スタンドアロンNX-OSで使用できる**test aaa**コマンドをサポートしていません。RADIUSの動作を確認するには、次の方法を使用します。

リーフスイッチからのRADIUSサーバの設定と到達可能性の統計情報を確認します。

<#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
```

シナリオ：RADIUS認証に失敗した

問題：ユーザがRADIUSログインドメインを選択すると、ログインが失敗する。

確認手順:

1. スイッチからのRADIUSサーバの統計情報で、タイムアウトまたは障害の兆候がないか確認します。
   <#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のカウントが高い場合は、RADIUSサーバに到達できないか、共有秘密鍵に不一致があることを示しています（RADIUSでは、共有秘密鍵が一致しない場合は、通知なくパケットが廃棄されます）。

2. RADIUSサーバへのネットワーク到達可能性を確認します。
   <#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. APICとRADIUSサーバ間で共有秘密が一致することを確認します。TCPを使用して接続障害を報告するTACACS+とは異なり、RADIUSではUDPが使用され、共有秘密鍵が一致しない場合は通知なしでパケットが廃棄されます。唯一の症状はタイムアウトです。
4. RADIUSサーバのログを確認します。デバッグモードのFreeRADIUS(**radiusd -X**)は、各要求を表示し、要求が受け入れられたか、拒否されたか、または共有秘密の不一致があったかどうかを示します。
5. APIC **nginx.bin.log**でRADIUS認証フローを確認します。ユーザ名でフィルタリングします。
   <#root>

   ```
   apic1#

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

   RADIUSログインは、LDAPおよびTACACS+と同じ**nginx.bin.log**認証フローに従います（完全な実際のログの例については、「LDAP動作検証」セクションを参照してください）。
   RADIUSの主な違いは次のとおりです。

- `Adding RadiusProvider <IP> to the list`:RADIUSサーバを示します(`TacacsProvider`や`LdapProvider`と対比)。
- RADIUSのレルム番号は設定によって異なります。

成功した RADIUSログインは、「`Injection of remote user ... was completed`」および「`admin write privileges`」で終了します。

failed RADIUSログインは、was denied during AAA authenticationおよびDENIEDで終了します。

`Adding RadiusProvider`行の後にRADIUS固有のメッセージが表示されない場合、サーバはタイムアウトしました。TCPを使用して接続障害を報告するTACACS+とは異なり、RADIUSではUDPが使用され、共有秘密鍵が一致しない場合は通知なしでパケットが廃棄されます。唯一の症状は、タイムアウトの後に拒否が続くことです。

6. RADIUSプロバイダーのアクティブな障害を確認します。
   <#root>

   apic1#

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

RBAC用RADIUS cisco-av-pair

RADIUSでは、RBACのロールマッピングに、TACACS+と同じ**cisco-av-pair**属性を使用します。RADIUSサーバは、Access-Accept応答で次の属性を返す必要があります。

<#root>

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

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

FreeRADIUSでは、これは**users**ファイルまたはLDAPバックエンドで設定されます。ISEでは、認可プロファイルで拡張属性として設定されます。

根本原因：共有秘密鍵の不一致 (RADIUSで最も一般的な不一致により、サイレントタイムアウトが発生します) 、サーバに到達できない、認証ポートが正しくない、またはRADIUSサーバでユーザアカウントが欠落している。

解決策：共有秘密を修正し、UDP 1812の到達可能性を確認するか、RADIUSサーバでユーザを設

定します。

AAAのトラブルシューティング：LDAP

このセクションでは、LDAP認証の失敗について説明します。APICは、TCPポート389(LDAP)またはTCPポート636（SSLを使用するLDAPS）を介してLDAPサーバに接続します。

動作検証

ACIスイッチは、スタンドアロンNX-OSで使用できる**test aaa**コマンドをサポートしていません。LDAPの動作を確認するには、APICからプロバイダーの障害と設定を確認します。

LDAPプロバイダーのアクティブな障害を確認します。

```
<#root>

apic1#

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

障害F1777は、接続の問題を示しています。障害F1778は、認証またはバインドの失敗を示しています。障害が返されない場合、APICはプロバイダーが到達可能であると見なします。

LDAPサーバへの基本的なネットワーク到達可能性を確認します。

```
<#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
```

LDAPの場合は、ポート389（LDAPSの場合は636）へのTCP接続も確認します。 APICがサーバにpingできてもLDAP障害が続く場合、通常はバインドDNが正しくないか、パスワードが間違っているか、ファイアウォールがLDAPポートをブロックしていることが問題です。

APICログでLDAP認証フローを検証します。ユーザ名でフィルタリングします。

<#root>

apic1#

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

Working:LDAPログインに成功すると、検索、バインド、およびロール割り当てのフロー全体が表示されます。

```
||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ディレクトリでユーザが見つかりません（検索で空のセットが返されます）。

```
||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
```

シナリオ：LDAP認証の失敗

問題：ユーザがLDAPログインドメインを選択すると、ログインが失敗する。

確認手順:

1. APICからのLDAPサーバの到達可能性を確認します。

<#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. アクティブなLDAPプロバイダーの障害を確認します。
<#root>

```
apic1#

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

3. LDAPプロバイダーの設定を確認します。
<#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. 設定されたベースDNの下のLDAPディレクトリにユーザが存在し、フィルタと一致することを確認します。Active Directoryでは、ユーザの**sAMAccountName**属性はログイン時に入力したユーザ名と一致している必要があります。OpenLDAPの場合、**cn**または**uid**属性は一致する必要があります。
5. LDAPS（ポート636）を使用している場合は、SSL証明書チェーンを確認します。**SSLValidationLevel**がstrictに設定されている場合、サーバ証明書が信頼されないか、期限切れになると、APICは接続を拒否します。
6. APIC **nginx.bin.log**で完全なLDAP認証フローを確認します。中間メッセージが失われないように、ユーザ名でフィルタリングします。
<#root>

```
apic1#

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

出力を、上記の「動作検証」セクションの動作している例と動作していない例と比較します。その他のLDAP固有の障害パターンは、ログを幅広く検索することで確認できます。

<#root>

```
apic1#
```

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

一般的な動作しないパターン（完全なフローについては、上記の動作検証例と比較してください）：

```
! 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
```

その他のLDAP障害パターン：

- LDAP検索がタイムアウトしました（サーバに到達できない、低速、またはファイアウォールがポート389/636をブロックしている）。「`Ldap Search failed: return code for ldap_search_ext_s: -5: Timed out`
- バインドに失敗しました（rootdnまたはバインドパスワードが間違っているか、サーバが接続を拒否しました）。— `Ldap Search failed: return code for ldap_search_ext_s: -1: Can't contact LDAP server`
- User found but password is wrong(bind with user password fails)：ログには`LDAP Record DN`行が表示されますが、その後に「`Bind to UserDN ... successful`」という拒否されたメッセージが続きます。

RBAC用のLDAPグループマップ

LDAPでは、**cisco-av-pair**属性の代わりにグループマップが使用されます。LDAPプロバイダーの属性フィールドは、グループ情報を含むLDAP属性を指定します。Active Directoryの場合、これは通常**memberOf**です。

APICは、返されたグループDNを設定済みのLDAPグループマップルール(**aaaLdapGroupMapRule**)と照合して、適切なセキュリティドメインとロールを割り当てます。一致するグループマップルールがない場合、ユーザは認証されますが、ロールはありません。

または、属性を**CiscoAVPair**に設定し、**shell:domains=all/admin/**の値をユーザのLDAP属性に直接保存します。この属性の形式はTACACS+およびRADIUSと同じです。

根本原因：バインドDNまたはパスワードが正しくない、ベースDNにユーザが含まれていない、検索フィルタがディレクトリスキーマに一致しない、LDAPS証明書の検証が失敗している、またはグループマップルールがない。

解決策：プロバイダーの設定（バインドDN、ベースDN、フィルタ、SSL設定）を修正します。RBACの問題に関しては、グループマップルールがユーザが属するLDAPグループと一致することを確認します。

RBACとユーザ権限のトラブルシューティング

このセクションでは、ユーザが正常に認証されるものの、期待されるアクセスレベルが設定されていないシナリオについて説明します。

シナリオ：ユーザはログインしたが、テナントが表示されない

問題：リモートユーザがTACACS+、RADIUS、またはLDAP経由でログインしている。ログインは成功するが、ユーザのUIにテナントが表示されず、APIコールは空の結果または「403 Forbidden」を返す。

確認手順:

1. ユーザのセッションを確認し、ログイン時にどのロールが割り当てられたかを確認します。

   <#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
   ```

   descrフィールドには、ログイン結果が表示されます。ユーザの認証に成功したが、RBACの役割がない場合、AAAサーバは有効な**cisco-av-pair**またはLDAPグループマップ一致を返しませんでした。

2. APIC **nginx.bin.log**を確認して、ログイン時のAVペアとロール割り当てを確認します。ユーザ名でフィルタリングします。
   <#root>

   ```
   apic1#

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

   ロールインジェクションとドメイン割り当てのメッセージを探します。

   Working:LDAPグループマップから変換されたAVペア、ユーザは管理者ロールを取得：

```
||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またはConverted to CiscoAVPairの行がフローに表示されない場合、AAAサーバは属性を返さず、一致するLDAPグループマップルールはありません。「**Checking all UserDomains**」の行の後に「**Found UserDomain**」の行がないかどうかを確認します。ユーザは認証されましたが、ロールの割り当てはありません。**Injection ... data FAILED**メッセージが表示された場合、AV pair文字列の形式が無効です。

3. AAAサーバが、**cisco-av-pair**属性（TACACS+またはRADIUS）または正しいLDAPグループメンバーシップ(LDAP)を返していることを確認します。 AAAサーバの設定をチェックします。
   - TACACS+：ユーザプロファイルに**cisco-av-pair**が含まれており、**shell:domains=all/admin/**の形式であることを確認します。
   - RADIUS：ユーザプロファイルがAccess-Acceptで**Cisco-AVPair = "shell:domains=all/admin/"**を返すことを確認します。
   - LDAP：ユーザが、設定済みのLDAPグループマップルール(**aaaLdapGroupMapRule**)に一致するLDAPグループのメンバーであることを確認します。
4. 属性は存在するがユーザがまだアクセスできない場合は、属性のセキュリティドメイン名がAPICの既存のセキュリティドメインと一致することを確認します。
   <#root>

   ```
   apic1#

   moquery -c aaaDomain
   ```

cisco-av-pairが存在しないドメイン(**shell:domains=NonExistentDomain/admin/**など)を参照する場合、ロールの割り当ては警告なしで失敗します。

根本原因： AAAサーバがRBACマッピング属性を返さない、属性の形式が正しくない、または属性で参照されているセキュリティドメインがAPICに存在しない。

解決策：正しい**cisco-av-pair**またはグループマッピングを返すようにAAAサーバを設定します。APICにセキュリティドメインが存在することを確認します。

シナリオ：ユーザは設定を表示できるが、変更できない

問題：ユーザはログインしてオブジェクトを参照できますが、変更を送信しようとするとエラー

が発生します。

確認手順:

1. ユーザのロール割り当てを確認します。
   <#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. ユーザが書き込みアクセスを必要とする場合、ロールは**writePriv**を許可する必要があります。書き込み権限を持つ一般的なロールには、admin、tenant-admin、access-admin、およびfabric-adminがあります。
3. APICログでロール割り当てを検証します。ユーザ名でフィルタリングします。
   <#root>

   ```
   apic1#

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

   認証フローの最後の近くにあるロール割り当てメッセージを探します。

   Working：ユーザには（実際のLDAPログインからの）admin書き込みロールがあります。

   ```
   ||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：ログに`admin write権限`ではなく`read権限`を持つ`non-admin UserRole`と記録されている場合、そのユーザは読み取り専用ロールを持ち、設定を変更できません。次のような行を探します。

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

   ログに`読み取り権限`だけが示され、`書き込み権限`が示されていない場合は、AAAサーバ上のユーザのロールまたはAVペアを更新します。

根本原因：ユーザに、書き込み可能なロールではなく、読み取り専用のロール(例：read-all、

ops)が割り当てられている。

解決策：APIC上のユーザのロール割り当て（ローカルユーザの場合）を更新するか、AAAサーバ上の**cisco-av-pair**（リモートユーザの場合）を更新して、書き込み権限を持つロールを含めます。

シナリオ：ユーザは一部のテナントにはアクセスできるが、他のテナントにはアクセスできない

問題：ユーザは1つのテナントを表示および管理できますが、他のテナントはアクセスが必要であるにもかかわらず表示できません。

確認手順:

1. ユーザのセキュリティドメイン割り当てを確認します。
   <#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. セキュリティドメインはテナントにマッピングされます。ユーザがテナントBにアクセスする必要がある場合は、テナントBに関連付けられたセキュリティドメインか、すべてのドメインにこれらのユーザを割り当てる必要もあります。
3. リモートユーザの場合は、AVペアまたはLDAPグループマップによって正しいドメインが割り当てられていることを確認します。ログイン時にAPIC **nginx.bin.log**でドメイン割り当てを確認します。ユーザ名でフィルタリングします。
   <#root>

   ```
   apic1#

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

   Working：ユーザは実際のLDAPログインからallドメイン（完全な可視性）を持っています。

   ```
   ||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：ユーザに単一のテナントドメインしかない場合、そのドメインだけが**all**メッセージではなく**Found UserDomain**メッセージに表示されます。たとえば、`Found UserDomain TenantA`は、ユーザがテナントAのみを表示できることを意味します。ユーザはAAAサーバのAVペアに追加ドメインを追加するか、フルアクセス用のallドメインを追加する必要があります。

根本原因：ユーザは、特定のテナントのみを対象とする制限付きセキュリティドメインに割り当てられています。

解決策：必要なセキュリティドメインをユーザの設定に追加するか、フルアクセスにallドメインを使用します。

パスワード回復と緊急アクセス

すべての管理者アカウントがロックアウトされているか、リモートAAAサーバに到達できず、デフォルトレルムが変更されている場合は、次のいずれかの回復方法を使用します。

フォールバックログインドメイン

ACIは、デフォルトの認証レルムに関係なく、常にローカル認証を使用する組み込みのフォールバックログインドメインを提供します。使用するには：

- SSH:**apic:fallback\\admin**(バージョンによっては**apic#fallback\\admin**)として ログインします。
- GUI：ログイン画面のDomainドロップダウンで、fallbackを選択し、ローカルクレデンシャルを使用します。

コンソールアクセス

コンソール認証レルムがlocal（デフォルト）に設定されている場合、ローカルクレデンシャルを使用してAPICコンソールポートからいつでもログインできます。ローカル管理者パスワードが不明な場合は、Cisco Integrated Management Controller(CIMC)（物理APICの場合）またはハイパーバイザコンソール（仮想APICの場合）を使用してパスワードをリセットできます。

注：コンソール認証レルムがリモートAAAサーバに変更され、そのサーバに到達できない場合、コンソールアクセスも失敗します。これは一般的なロックアウトのシナリオです。コンソール認証レルムは常にローカルに設定してください。

一般的な障害のリファレンス

次のACI障害は、一般的にリモートアクセスとAAAの問題に関連しています。

- F1773:TACACS+プロバイダーの接続の問題。APICがTACACS+サーバに到達できません。
- F1774:TACACS+認証の失敗。サーバは到達可能ですが、認証の試行が拒否されました。
- F1775:RADIUSプロバイダーの接続の問題。
- F1776:RADIUS認証が失敗しました。
- F1777:LDAPプロバイダーの接続の問題です。
- F1778:LDAP認証が失敗しました。
- F0532：ノードに管理サブネットが設定されていません。

アクティブなAAA障害の照会：

<#root>

apic1#

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

参照資料

- ACI管理およびコアサービスのトラブルシューティング：ポッドポリシー
- Cisco APIC基本設定ガイド、リリース6.1(x)：管理
- Cisco APICセキュリティ設定ガイド：アクセス、認証、アカウンティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。