Dépannage des problèmes d'accès à distance dans un fabric ACI

Introduction

Ce document décrit comment vérifier, dépanner et résoudre les problèmes d'accès à distance dans un fabric Cisco ACI (Application Centric Infrastructure). Il couvre l'accès sécurisé SSH (Secure Shell) et HTTPS (Hypertext Transfer Protocol Secure) aux APIC et aux commutateurs de fabric, l'authentification, l'autorisation et la comptabilité à distance (AAA) avec TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial-In User Service), LDAP (Lightweight Directory Access Protocol) et l'autorisation RBAC (Role-Based Access Control). Un arbre de décision de triage et des scénarios de dépannage détaillés sont inclus pour chaque zone.

Informations générales

Le contenu de ce document a été synthétisé à partir du guide Troubleshoot ACI Management and Core Services — Pod Policies, du guide Cisco APIC Basic Configuration Guide, du chapitre Release 6.1(x) — Management et du chapitre Cisco APIC Security Configuration Guide — Access, Authentication, and Accounting.

Aperçu

L'accès à distance à un fabric ACI implique trois couches distinctes, chacune devant fonctionner pour qu'un ingénieur puisse se connecter et fonctionner :

1. Transport : le chemin du réseau de gestion (OOB ou intrabande) et le service de protocole (SSH ou HTTPS) doivent être accessibles et activés.
2. Authentification : les informations d'identification de l'utilisateur doivent être validées, soit localement sur le contrôleur APIC, soit sur un serveur AAA distant (TACACS+, RADIUS ou LDAP).
3. Autorisation — L'utilisateur authentifié doit se voir attribuer les rôles RBAC et les domaines de sécurité appropriés afin d'afficher et de modifier les objets ACI prévus.

Une défaillance au niveau de n'importe quelle couche produit des symptômes différents. Une panne de transport empêche entièrement la connexion. Un échec d'authentification renvoie une

erreur d'informations d'identification. Un échec d'autorisation permet la connexion mais restreint la visibilité ou produit des erreurs « 403 Interdit » dans l'API.

Politique d'accès de gestion

La stratégie d'accès à la gestion (**commPol**MAP) est l'objet central qui contrôle quels protocoles d'accès à distance sont activés sur le fabric. Il se trouve sous Fabric > Fabric Policies > Policies > Pod > Management Access > default. La stratégie contient des objets enfants qui configurent :

- SSH (**commSsh**) : état administratif, port, chiffrements, algorithmes d'échange de clés (KEX), codes d'authentification de message (MAC) et algorithmes de clé hôte.
- HTTPS (**commHttps**) : état administratif, port, version du protocole TLS (Transport Layer Security), taux d'accélération et authentification du certificat client.
- Telnet (**commTelnet**) : état administratif et port. Telnet est désactivé par défaut et Cisco recommande de le rester.

OOB et gestion intrabande

Les noeuds ACI prennent en charge deux chemins d'accès de gestion :

- Out-of-Band (OOB) : utilise le port de gestion dédié sur l'APIC ou le commutateur. Les adresses de gestion OOB sont attribuées à partir d'un pool sous le locataire de gestion et attribuées aux noeuds via **mgmtRsOoBStNode**. Dans le cas du CPPA, les contrats d'OOB sont mis en oeuvre par des **iptables** règles. Si un contrat OOB est appliqué, seul le trafic explicitement autorisé par le contrat peut atteindre l'interface de gestion APIC.
- Intrabande (INB) : utilise le plan de données de fabric pour le trafic de gestion. La gestion intrabande nécessite l'attribution d'une adresse de gestion de domaine de pont (BD), de sous-réseau, de groupe de terminaux (EPG), de contrat et de noeud. Les adresses IP intrabande ne sont pas accessibles depuis l'extérieur du fabric sans configuration supplémentaire du routage ou de la stratégie.

Remarque : Les adresses IP de gestion OOB du contrôleur APIC sont configurées lors de la configuration initiale et le contrôleur APIC obtient la connectivité IP avant que le fabric ne soit entièrement découvert. OOB est le chemin de gestion principal et est toujours disponible si le réseau de gestion physique est connecté.

Architecture AAA

L'ACI utilise un modèle AAA à trois niveaux :

1. Login Domain (**aaaLoginDomain**) : regroupe les fournisseurs AAA sous un domaine nommé. Les utilisateurs spécifient le domaine de connexion à l'écran de connexion (par exemple, `apic:TACACS-Domain` ou via la liste déroulante dans l'interface utilisateur). Un domaine de connexion de secours spécial existe toujours et correspond à l'authentification locale.
2. Provider Group (**aaaTacacsPlusProviderGroup**, **aaaRadiusProviderGroup**, **aaaLdapProviderGroup**) : référence un ou plusieurs serveurs AAA et définit l'ordre dans lequel ils sont essayés.
3. Provider (**aaaTacacsPlusProvider**, **aaaRadiusProvider**, **aaaLdapProvider**) : définit l'adresse IP du serveur, le port, le secret partagé (ou le DN de liaison pour LDAP), le délai d'attente, les tentatives, l'EPG de gestion et les informations d'identification de surveillance.

Le domaine d'authentification par défaut (**aaaDefaultAuth**) détermine quel domaine de connexion est utilisé lorsque l'utilisateur n'en spécifie aucun à la connexion. Le domaine d'authentification de console contrôle l'authentification pour les sessions de console.

Remarque : Le fait de remplacer le domaine d'authentification par défaut par un serveur AAA distant alors que ce serveur est inaccessible vous verrouille hors du fabric. Testez toujours la connectivité du serveur AAA avant de modifier le domaine. Le domaine de connexion de secours (`apic:fallback\\admin`) peut être utilisé afin de contourner le domaine par défaut et de s'authentifier localement.

Fichiers journaux AAA clés

Les événements d'authentification AAA sont consignés dans plusieurs fichiers à la fois sur le contrôleur APIC et sur les commutateurs de fabric. Ces journaux constituent le principal outil de validation des résultats de l'authentification, d'identification du domaine et du groupe de fournisseurs utilisés et de diagnostic des échecs d'attribution de rôles.

Fichier journal	Emplacement (APIC)	Emplacement (commutateurs)	D
nginx.bin.log (APIC) nginx.log (commutateurs)	`/var/log/dme/log/nginx.bin.log`	`/var/sysmgr/tmp_logs/dme_logs/nginx.log`	Journal A Contient d'authent Requête de domai fournisse communi LDAP/TA analyse d d'antivirus domaine résultat d refus. Le diffère se formes, m

Fichier journal	Emplacement (APIC)	Emplacement (commutateurs)	D
			contenu e
access.log	/var/log/dme/log/access.log	/var/log/dme/log/access.log	Journal d HTTP NG par requê contrôleu les appels aaaRefres d'état HT réussite, Sur les co affiche les d'API DM appels aa
pam.module.log	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log	Journal d Affiche le l'authentif sessions authentifi l'ID utilisa attribué. S commuta moyen le confirmer a été auth

Remarque : Le journal AAA principal a un nom de fichier différent sur chaque plate-forme. Sur l'APIC, il est **nginx.bin.log** à /var/log/dme/log/. Sur les commutateurs Leaf et Spine, il est **nginx.log** à /var/sysmgr/tmp_logs/dme_logs/. Le format du contenu du journal et les messages AAA sont identiques sur les deux plates-formes.

Les entrées AAA dans le journal nginx suivent le format suivant :

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

Filtrer les entrées de journal liées à AAA pour un flux d'authentification d'utilisateur spécifique :

<#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
```

Vous pouvez également afficher toutes les demandes d'authentification récentes et leurs résultats :

<#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
```

Un flux d'authentification réussi type affiche ces messages clés dans l'ordre suivant :

1. `Demande d'authentification PAM reçue de nginx pour Nom d'utilisateur : <user>` — la demande de connexion a été reçue.
2. `DefaultAuthMo spécifie le domaine <N>. Groupe de fournisseurs <nom> !` — le domaine a été sélectionné (0=fallback/local, 2=TACACS+, 3=LDAP).
3. Messages spécifiques au fournisseur (liaison LDAP, recherche de fournisseur TACACS+ ou requête RADIUS).
4. `UserDomain <domaine> trouvé sous le nom d'utilisateur distant : <user>` : attribution de domaine à partir de la réponse AAA.
5. `Nom d'utilisateur trouvé : admin avec des privilèges d'écriture admin sous UserDomain all - l'utilisateur est un utilisateur admin` - la vérification du rôle a réussi.

Journaux d'authentification ayant échoué :

- `L'utilisateur <user> a été refusé lors de l'authentification AAA`
- `Erreur utilisateur non autorisé <user> : Authentification du serveur AAA REFUSÉE`

Remarque : Le journal nginx tourne fréquemment et les entrées plus anciennes sont compressées gzip avec un suffixe numérique. Sur le contrôleur APIC, les journaux pivotés se trouvent dans le même répertoire (par exemple, **nginx.bin.log.22815.gz**). Sur les commutateurs, les journaux pivotés sont stockés à **/var/log/dme/oldlog/dme/nginx.log.*.gz** (avec des liens symboliques dans `/var/sysmgr/tmp_logs/dme_logs/`). Pour rechercher des journaux pivotés :

<#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'
```

Modèle RBAC

L'ACI RBAC contrôle ce qu'un utilisateur authentifié peut voir et faire. Le modèle comporte trois composants :

- Domaine de sécurité (**aaaDomain**) : limiteur d'étendue mappé aux objets ACI (locataires, politiques d'accès, politiques de fabric). Les domaines intégrés all, common et mgmt sont toujours présents. Les domaines personnalisés limitent la visibilité d'un utilisateur à des locataires ou des domaines de stratégie spécifiques.
- Role (**aaaRole**) : définit un ensemble de privilèges. Les rôles prédéfinis sont les suivants : admin, aaa, tenant-admin, tenant-ext-admin, read-all, access-admin, fabric-admin, ops et nw-svc-admin.
- Privilège - chaque rôle accorde un accès en lecture ou en écriture (ce qui implique un accès en lecture) à une zone fonctionnelle spécifique.

Un ou plusieurs domaines de sécurité et paires de rôles sont affectés à un compte utilisateur. Pour les utilisateurs distants authentifiés via TACACS+, RADIUS ou LDAP, le mappage de rôle est fourni via des attributs spécifiques au fournisseur dans la réponse AAA (par exemple, l'**cisco-av-pair**attribut).

Arbre de décision de triage

Utilisez cet arbre de décision lorsqu'un utilisateur signale qu'il ne peut pas accéder à distance au fabric ACI :

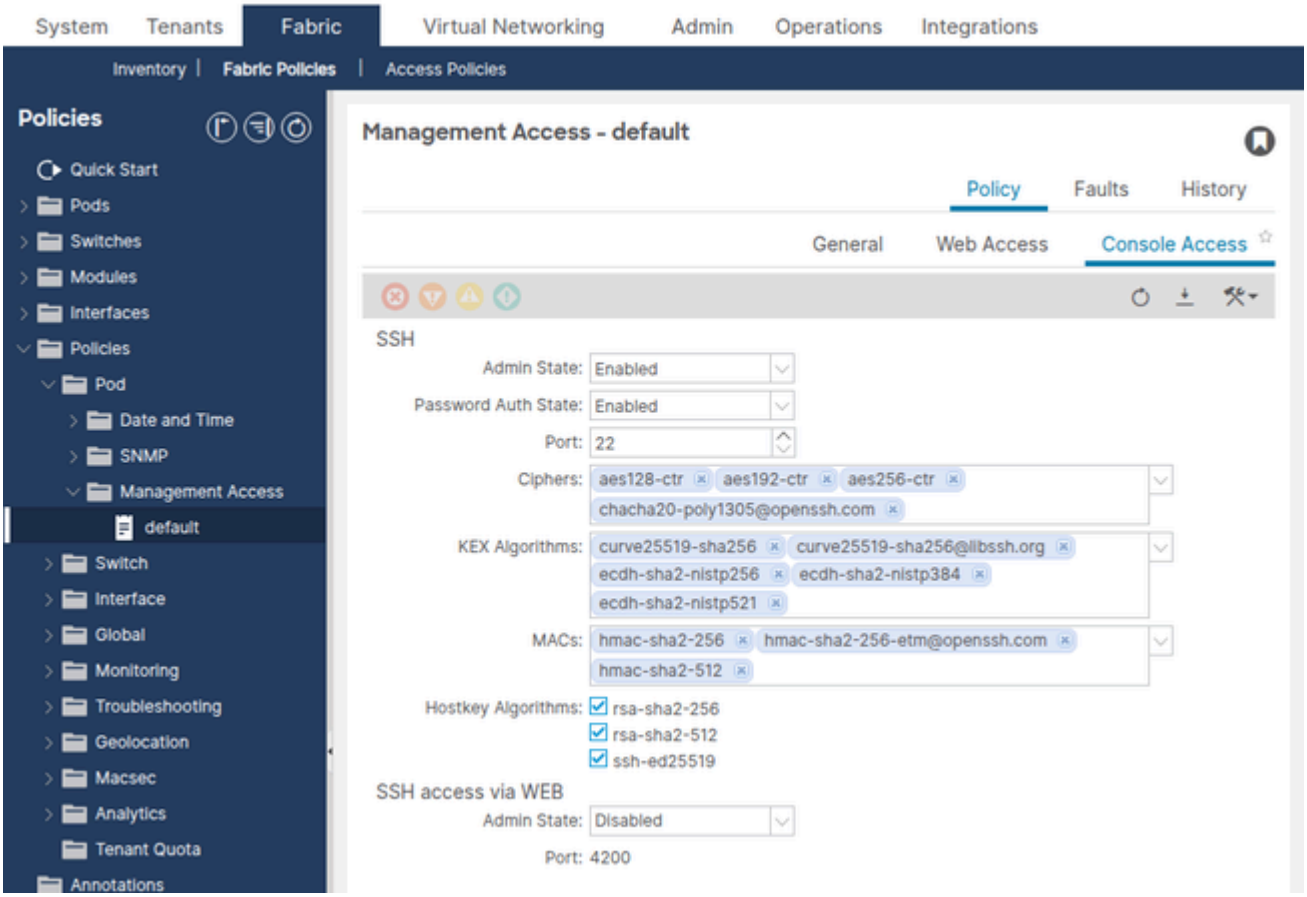
1. Pouvez-vous envoyer une requête ping à l’APIC ou à l’IP de gestion du commutateur ?
    - Non → Dépanner le chemin réseau de gestion. Veuillez vous reporter à la section « Dépannage de l'OOB et de la gestion intrabande ».
    - Oui → Continuer.
2. Pouvez-vous établir une connexion SSH ou HTTPS (la connexion est-elle ouverte du tout) ?
    - Non → Le service de protocole peut être désactivé, le port peut être filtré ou une non-concordance de chiffrement peut être présente. Reportez-vous aux sections « Dépannage de l'accès SSH » ou « Dépannage de l'accès HTTPS ».
    - Oui → Continuer.
3. L'écran de connexion s'affiche-t-il (HTTPS) ou la connexion SSH est-elle terminée et invite-t-elle à fournir des informations d'identification ?
    - Aucun → échec d'échange de clé SSH ou de connexion TLS. Veuillez consulter la section « Dépannage de l'accès SSH » pour les incohérences de chiffrement et de KEX.
    - Oui → Continuer.
4. Les informations d'identification échouent-elles avec « Authentication Failed » ou similaire ?
    - Oui → Problème d'authentification. Reportez-vous aux sections « Dépannage de l'authentification AAA » (TACACS+, RADIUS ou LDAP selon le domaine de connexion utilisé).
    - Non → Continuer.
5. L'utilisateur se connecte-t-il mais ne peut pas voir les objets attendus ou reçoit-il des erreurs « 403 Interdit » ?
    - Oui → Autorisation ou problème RBAC. Reportez-vous à la section « Dépannage du RBAC et des privilèges utilisateur ».
    - Non → L'accès fonctionne. Vérifiez le problème spécifique rencontré par l'utilisateur.

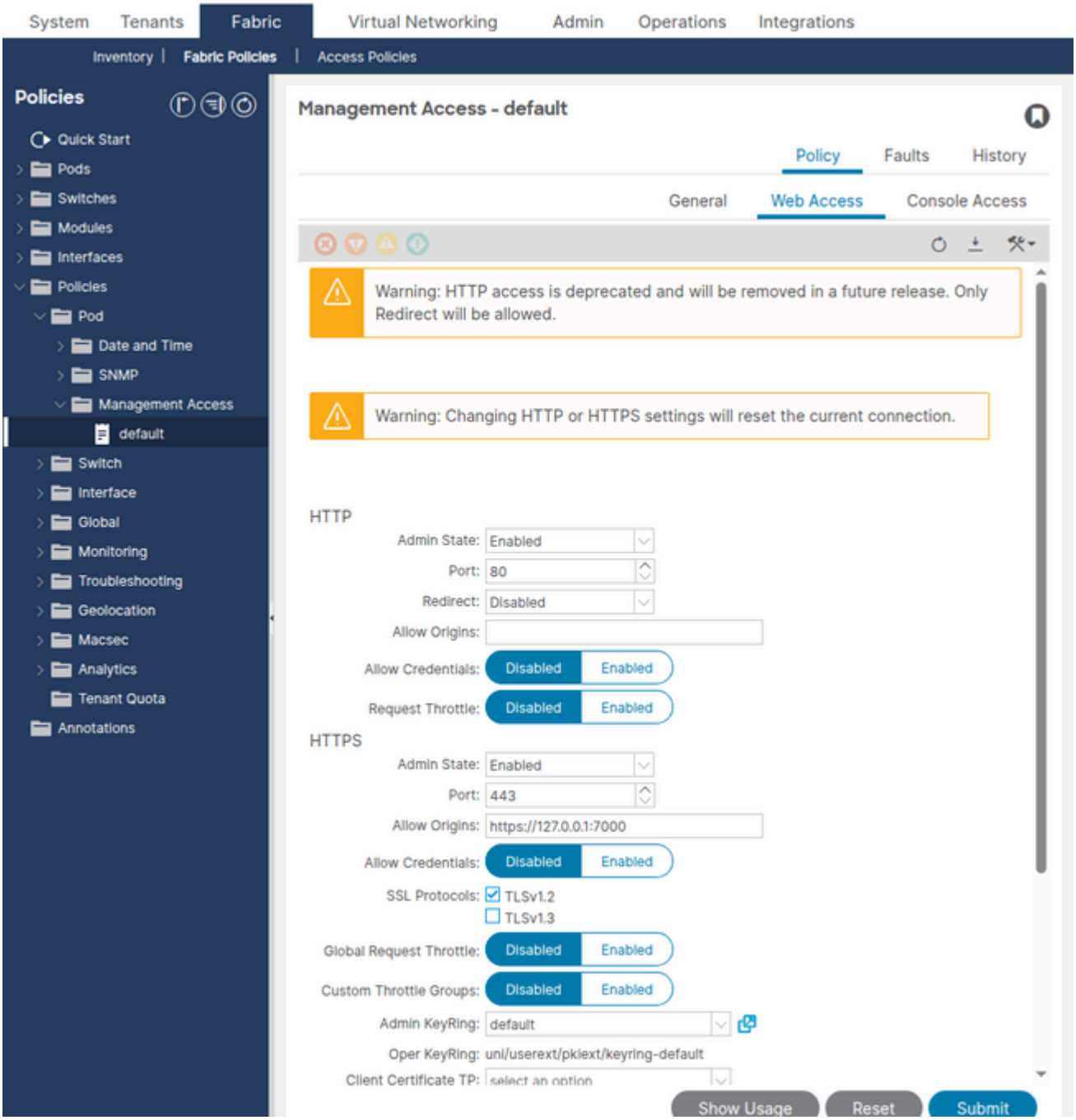
Vérifier la configuration

Avant de dépanner l'état opérationnel, vérifiez que la chaîne de configuration est terminée. La mauvaise configuration est la cause principale des problèmes d'accès à distance.

Vérification de la stratégie d'accès à la gestion (SSH et HTTPS)

Accédez à Fabric > Fabric Policies > Policies > Pod > Management Access > default.


System
Tenants
Fabric
Virtual Networking
Admin
Operations
Integrations
Inventory
Fabric Policies
Access Policies
Policies
Quick Start
Pods
Switches
Modules
Interfaces
Policies
Pod
Date and Time
SNMP
Management Access
default
Switch
Interface
Global
Monitoring
Troubleshooting
Geolocation
Macsec
Analytics
Tenant Quota
Annotations
Management Access - default
Policy
Faults
History
General
Web Access
Console Access
SSH
Admin State: Enabled
Password Auth State: Enabled
Port: 22
Ciphers: aes128-ctr aes192-ctr aes256-ctr chacha20-poly1305@openssh.com
KEX Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521
MACs: hmac-sha2-256 hmac-sha2-256-etm@openssh.com hmac-sha2-512
Hostkey Algorithms: rsa-sha2-256 rsa-sha2-512 ssh-ed25519
SSH access via WEB
Admin State: Disabled
Port: 4200



Confirmez les paramètres SSH suivants :

- Admin State : doit être activé.
- Port : valeur par défaut 22. Si elle est modifiée, le client SSH doit utiliser le port personnalisé.
- Authentification par mot de passe : activée (sauf si l'authentification par certificat uniquement est prévue).
- Chiffres SSH : doit inclure au moins un chiffre pris en charge par le client SSH.
- Algorithmes KEX — Doit inclure au moins un algorithme pris en charge par le client SSH.
- SSH MACs : doit inclure au moins un MAC pris en charge par le client SSH.

Interrogez l'objet géré SSH via l'API :

<#root>

apic1#

moquery -c commSsh

```
dn              : uni/fabric/comm-default/ssh
adminSt         : enabled                       <--- must be enabled
port            : 22
passwordAuth    : enabled
sshCiphers      : aes128-ctr,aes192-ctr,aes256-ctr,chacha20-poly1305@openssh.com
kexAlgos        : curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,
sshMacs         : hmac-sha2-256,hmac-sha2-256-etm@openssh.com,hmac-sha2-512
hostkeyAlgos    : rsa-sha2-256,rsa-sha2-512,ssh-ed25519
```

Confirmez les paramètres HTTPS suivants :

- Admin State : doit être activé.
- Port : 443 par défaut.
- Protocoles SSL — TLSv1.2 (par défaut). Les clients plus anciens peuvent nécessiter l'ajout explicite de TLSv1.1.
- Throttle State : si cette option est activée, le taux de limitation limite les demandes par seconde par utilisateur. Une valeur très faible peut entraîner des erreurs de délai d'attente API.

<#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
```

Mauvaises configurations courantes

- Chiffres SSH limités de manière trop agressive - dans ACI version 5.2(1) et ultérieures, les chiffrements SSH par défaut ont été renforcés. Les clients SSH plus anciens (par exemple, les versions PuTTY antérieures à 0.75, ou les versions OpenSSH qui offrent uniquement **diffie-hellman-group14-sha1**) peuvent échouer l'échange de clés. Le client SSH affiche « aucun chiffre correspondant trouvé » ou « aucune méthode d'échange de clés correspondante trouvée ».

- Password authentication disabled : si **passwordAuth** est défini sur disabled, seule l'authentification SSH basée sur les clés est autorisée. Les utilisateurs qui se connectent avec des mots de passe verront « Autorisation refusée (clé publique) ».
- Port SSH personnalisé sans reconnaissance du client — si le port SSH est passé de 22, le client SSH doit spécifier le nouveau port (par exemple, **ssh -p 2222 admin@10.1.1.1**).

Vérifier les adresses de gestion OOB

Accédez à Tenants > mgmt > Node Management Addresses.

Vérifiez que chaque APIC et noeud de commutateur possède une adresse IP de gestion OOB attribuée avec une passerelle valide. Les noeuds sans adresse de gestion ne sont pas accessibles sur le réseau de gestion.

Interrogez les affectations de noeuds statiques OOB via l'API :

<#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
```

Mauvaises configurations courantes

- Attribution d'adresse OOB manquante — un commutateur n'a pas d'entrée sous **mgmtRsOoBStNode**. Le noeud n'aura pas d'adresse IP de gestion et ne répondra pas à SSH ou HTTPS sur l'interface OOB.
- Passerelle incorrecte : l'adresse de la passerelle ne correspond pas à la passerelle réelle sur le réseau de gestion OOB. Le noeud peut recevoir des paquets mais ne peut pas envoyer de trafic de retour.
- Non-concordance du masque de sous-réseau — le masque de sous-réseau OOB ne correspond pas au réseau de gestion physique. Cela peut amener le noeud à croire que la station de gestion se trouve sur un sous-réseau différent et à acheminer le trafic via une passerelle qui n'existe pas ou qui est incorrecte.

Vérifier les contrats OOB

Accédez à Locataires > Gestion > Contrats.

Si un contrat OOB est appliqué à l'EPG de gestion OOB, seul le trafic explicitement autorisé par ce contrat atteindra l'interface de gestion APIC. Dans le cadre du PAC, les contrats OOB sont appliqués par le biais de **iptables** règles.

Recherchez les contrats fournis par OOB EPG :

<#root>

apic1#

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

Si la requête renvoie des résultats, les contrats sont appliqués. Vérifiez que les objets et les filtres du contrat autorisent les protocoles requis :

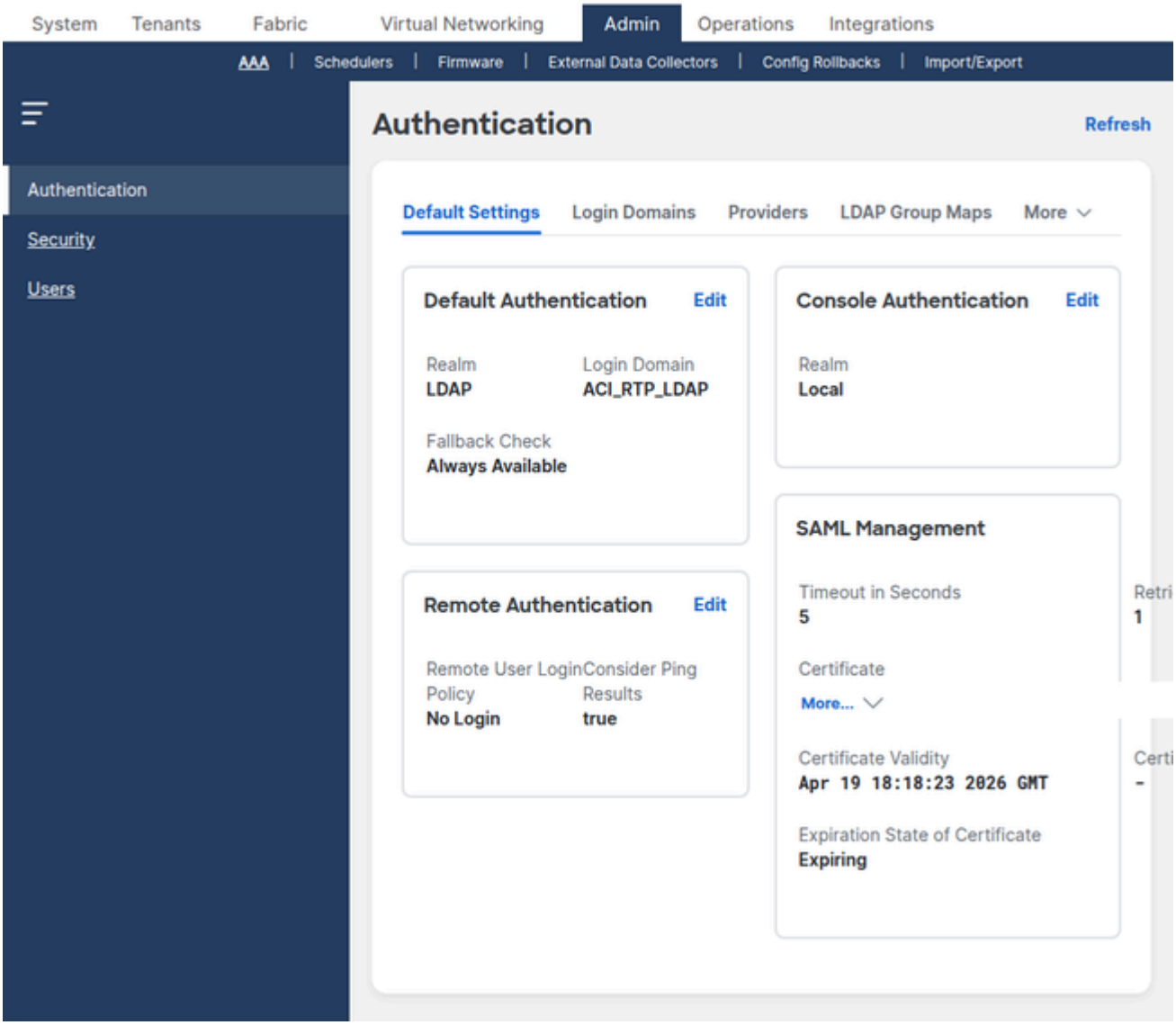
- SSH : port TCP 22 (ou port personnalisé)
- HTTPS : port TCP 443 (ou port personnalisé)
- ICMP — pour la vérification de la requête ping

Mauvaises configurations courantes

- Le contrat OOB n'inclut pas SSH ou HTTPS — l'ingénieur peut envoyer une requête ping à l'APIC mais ne peut pas se connecter via SSH ou HTTPS. Les **iptables** règles du contrôleur APIC suppriment silencieusement le trafic.
- Restriction IP source dans le filtre de contrat OOB : le filtre de contrat limite l'accès à des sous-réseaux source spécifiques. Les ingénieurs en dehors de ce sous-réseau ne peuvent pas se connecter.

Vérification de la configuration AAA

Accédez à Admin > AAA > Authentication > AAA.



Confirmez ce qui suit :

- Default Authentication Realm : identifie le domaine de connexion utilisé lorsque l'utilisateur n'en spécifie aucun. S'il est défini sur un domaine de connexion AAA distant, le serveur correspondant doit être accessible.
- Console Authentication Realm — contrôle l'accès à la console. Si cette option est définie sur local, la connexion à la console utilise toujours des informations d'identification locales (recommandé).

Vérifier les domaines de connexion

Accédez à Admin > AAA > Authentication > Login Domains.

<#root>

```
apic1#
```

```
moquery -c aaaLoginDomain

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

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

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

Vérifiez que le domaine de connexion utilisé pour l'authentification est présent et qu'il fait référence au groupe de fournisseurs approprié.

Vérification des fournisseurs TACACS+

Accédez à Admin > AAA > Authentication > TACACS+ > TACACS+ Providers.

<#root>

```
apic1#

moquery -c aaaTacacsPlusProvider

dn              : uni/userext/tacacsext/tacacsplusprovider-10.1.1.50
name            : 10.1.1.50
authProtocol    : pap
port            : 49                          <--- default TACACS+ port
monitorServer   : disabled
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Vérification des fournisseurs RADIUS

Accédez à Admin > AAA > Authentication > RADIUS > RADIUS Providers.

<#root>

```
apic1#

moquery -c aaaRadiusProvider

dn              : uni/userext/radiusext/radiusprovider-10.1.1.51
name            : 10.1.1.51
authPort        : 1812                        <--- default RADIUS auth port
```

```
authProtocol    : pap
retries         : 1
timeout         : 5
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Vérifier les fournisseurs LDAP

Accédez à Admin > AAA > Authentication > LDAP > LDAP Providers.

<#root>

```
apic1#

moquery -c aaaLdapProvider

dn              : uni/userext/ldapext/ldapprovider-10.1.1.52
name            : 10.1.1.52
port            : 389                          <--- 389 for LDAP, 636 for LDAPS
enableSSL       : no
rootdn          : CN=binduser,CN=Users,DC=example,DC=com
basedn          : CN=Users,DC=example,DC=com
filter          : sAMAccountName=$userid
attribute       : memberOf                     <--- attribute used for group map
epgDn           : uni/tn-mgmt/mgmtp-default/oob-default    <--- management EPG
```

Mauvaises configurations AAA courantes

- Non-concordance du secret partagé — la clé configurée sur le fournisseur ACI TACACS+ ou RADIUS ne correspond pas à la clé sur le serveur. L'authentification échoue silencieusement.
- EPG de gestion incorrect - le EPG du fournisseur **epgDn** est vide ou pointe vers le mauvais EPG (par exemple, intrabande lorsque le serveur se trouve sur le réseau OOB). Le contrôleur APIC ne peut pas atteindre le serveur.
- Non-concordance du domaine de connexion — le domaine de connexion est configuré comme LDAP mais l'utilisateur attend une authentification TACACS+. Les domaines de connexion doivent faire référence au type de groupe de fournisseurs correct.
- DN de liaison LDAP incorrect — le **rootdn** (DN de liaison) ou **basedn** sont erronés. L'authentification LDAP échoue avec une erreur de liaison même si les informations d'identification de l'utilisateur sont correctes.
- Le filtre LDAP ne correspond pas au schéma d'annuaire : pour Active Directory, utilisez **sAMAccountName=$userid**. Pour OpenLDAP, utilisez **cn=$userid** ou **uid=$userid**.

Vérification de la configuration RBAC

Accédez à Admin > AAA > Users afin d'afficher les comptes d'utilisateurs locaux et leurs affectations de domaine et de rôle de sécurité.

Interroger les domaines de sécurité via l'API :

<#root>

```
apic1#

moquery -c aaaDomain

# Built-in domains:
dn      : uni/userext/domain-all
name    : all                           <--- full fabric access

dn      : uni/userext/domain-common
name    : common                        <--- access to tenant common

dn      : uni/userext/domain-mgmt
name    : mgmt                          <--- access to tenant mgmt
```

Un utilisateur affecté au domaine tous avec le rôle admin dispose d'un accès complet en lecture-écriture à l'ensemble du fabric. Un utilisateur affecté à un domaine de sécurité personnalisé avec le rôle tenant-admin ne peut gérer que les locataires associés à ce domaine.

Mauvaises configurations RBAC courantes

- Utilisateur créé sans domaine de sécurité - l'utilisateur peut se connecter mais ne voit aucun locataire et reçoit « 403 Interdit » sur les appels d'API. Au moins un domaine de sécurité doit être attribué.
- Rôle en lecture seule attribué lorsque l'accès en écriture est nécessaire — l'utilisateur peut afficher des objets mais ne peut pas envoyer de modifications. Vérifiez que le privilège de rôle est défini sur writePriv.
- Mappage de rôle d'utilisateur distant manquant sur le serveur AAA — le serveur TACACS+ ou RADIUS ne renvoie pas l'**cisco-av-pair**attribut contenant **shell:domains=all/admin/**. L'utilisateur s'authentifie correctement, mais il n'a aucun rôle et ne peut rien voir dans le fabric.

Dépannage de l'OOB et de la gestion intrabande

Si l'adresse IP de gestion du contrôleur APIC ou du commutateur n'est pas accessible sur le réseau, dépannez le chemin de gestion avant d'étudier SSH, HTTPS ou AAA.

Scénario: Impossible d'envoyer une requête ping à APIC OOB IP

Problème : La station de gestion ne peut pas envoyer de requête ping à l'adresse IP de gestion OOB APIC.

Étapes de vérification :

1. Vérifiez que le port de gestion APIC est physiquement connecté et que la liaison est active.
2. Vérifiez que la station de gestion se trouve sur le même segment L2 ou dispose d'une route vers le sous-réseau OOB.
3. Vérifiez que l'adresse IP de gestion OOB est correctement attribuée :
   <#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. Vérifiez que la passerelle par défaut est accessible :
   <#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. Si un contrat OOB est appliqué, vérifiez qu'il autorise les protocoles requis. Recherchez les contrats fournis par OOB EPG, comme indiqué dans la section « Vérifier les contrats OOB ». Les contrats OOB sont appliqués en tant que **iptables** règles sur le PAC. Vous pouvez afficher les règles enregistrées à partir du shell APIC :
   <#root>

   ```
   apic1#

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

   Si la stratégie INPUT est DROP et qu'il n'y a pas de règle ACCEPT pour le protocole requis, le contrat OOB filtre le trafic.

   Remarque : La **iptables -L -n** commande permettant d'afficher les règles du noyau en direct nécessite un accès racine et n'est pas disponible pour les sessions SSH d'administration normales.

Cause première : Adresse de gestion OOB manquante ou mal configurée, passerelle incorrecte ou trafic de filtrage de contrat OOB.

Solution : Corrigez l'attribution de l'adresse OOB, vérifiez le chemin d'accès au réseau physique ou mettez à jour le contrat OOB pour autoriser les protocoles requis.

Scénario: Impossible d'atteindre une adresse IP de gestion de commutateur

Problème : La station de gestion peut atteindre le contrôleur APIC, mais pas un commutateur via OOB.

Étapes de vérification :

1. Vérifiez qu'une adresse OOB est attribuée au commutateur :
   <#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. Vérifiez que l'interface de gestion du commutateur dispose de l'adresse IP attribuée :
   <#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. Vérifiez la route par défaut du VRF de gestion :
   <#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
   ```

Cause première : Attribution d'adresse OOB manquante, passerelle incorrecte ou le port physique de gestion du commutateur est en panne.

Solution : Attribuez l'adresse OOB sous Tenants > mgmt > Node Management Addresses. Vérifiez que la liaison de gestion physique est active.

Dépannage de l'accès SSH

Cette section couvre les scénarios où l'IP de gestion est accessible (la requête ping réussit) mais où la session SSH ne parvient pas à établir ou à authentifier.

Scénario: Connexion SSH refusée

Problème : Le client SSH signale « Connexion refusée » lors de la connexion à l'APIC ou au commutateur.

Étapes de vérification :

1. Vérifiez que SSH est activé dans la stratégie d'accès à la gestion :
   <#root>

   ```
   apic1#

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

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

   Si **adminSt** est désactivé, les connexions SSH sont rejetées.

2. Vérifiez que le port approprié est utilisé. Si le port SSH est passé de 22 :
   <#root>

   ```
   $

   ssh -p

    custom-port

   admin@10.1.1.1
   ```

3. Vérifiez que le contrat OOB autorise TCP sur le port SSH. Veuillez consulter la section « Vérifier les contrats OOB ».

Cause première : SSH désactivé dans la stratégie d'accès à la gestion, port personnalisé inconnu du client ou filtrage de contrat OOB.

Solution : Activez SSH dans la stratégie d'accès de gestion ou utilisez le port approprié.

Scénario: Échec de l'échange de clés SSH (non-concordance de chiffrement ou KEX)

Problème : Le client SSH échoue avec « aucun chiffre correspondant trouvé », « aucune méthode d'échange de clé correspondante trouvée » ou « aucun MAC correspondant trouvé ».

Étapes de vérification :

1. Vérifiez le résultat détaillé du client SSH afin d'identifier quels algorithmes le client offre :
   <#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. Comparez les algorithmes proposés par le client aux algorithmes configurés par le contrôleur APIC :
   <#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. Identifiez l'intersection. S'il n'existe aucun algorithme commun dans une catégorie, la connexion échoue.

Remarque : Dans les versions 5.2(1) et ultérieures de l'ACI, les algorithmes de chiffrement SSH et KEX par défaut ont été renforcés. Les algorithmes hérités tels que **diffie-hellman-group1-sha1**, **diffie-hellman-group14-sha1**, **aes128-cbc**, et **hmac-sha1** ne sont plus proposés par défaut. Si vous avez récemment effectué une mise à niveau, vérifiez que les clients SSH de votre environnement prennent en charge les nouveaux paramètres par défaut.

Cause première : Aucun chiffrement commun, algorithme KEX ou MAC entre le client SSH et l'APIC après une mise à niveau ACI ou un renforcement du chiffrement.

Solution : Mettez à jour le client SSH afin de prendre en charge les algorithmes modernes ou ajoutez à nouveau l'algorithme hérité requis à la stratégie d'accès à la gestion. Le réajout d'algorithmes hérités présente un risque pour la sécurité et n'est pas recommandé à long terme.

Scénario: SSH se connecte mais l'authentification échoue pour les utilisateurs locaux

Problème : La connexion SSH réussit (une invite de mot de passe s'affiche) mais le mot de passe est rejeté pour un utilisateur local.

Étapes de vérification :

1. Vérifiez que l'utilisateur existe localement :
   <#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. Vérifiez si le compte est verrouillé en raison d'un nombre excessif d'échecs de connexion :
   <#root>

   ```
   apic1#

   moquery -c aaaUserEp

   dn                  : uni/userext
   pwdStrengthCheck    : no
   ```

   Vérifiez la stratégie de verrouillage du domaine de connexion sous Admin > AAA > Security Management > Lockout Policy.

3. Vérifiez que l'utilisateur se connecte avec le domaine de connexion approprié. Si le domaine d'authentification par défaut est défini sur un domaine de connexion AAA distant, l'utilisateur doit ajouter un préfixe **apic:LOCAL\\username** ou un **apic:fallback\\username** afin de forcer l'authentification locale.
4. Validez le résultat de l'authentification dans les journaux. Vérifiez **nginx.bin.log** l'événement de connexion sur le contrôleur APIC :
   <#root>

   ```
   apic1#

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

Recherchez le domaine et le groupe de fournisseurs affectés à la tentative de connexion :

```
! 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
```

Si le domaine n'est pas 0 (secours/local), la connexion a été envoyée à un serveur AAA distant au lieu de la base de données locale. L'utilisateur doit faire précéder **apic:fallback\\username** ou **apic:LOCAL\\username** pour forcer l'authentification locale.

Cause première : Mot de passe incorrect, compte verrouillé ou tentative de connexion envoyée à un serveur AAA distant au lieu de la base de données locale.

Solution : Réinitialisez le mot de passe, déverrouillez le compte ou utilisez le préfixe de domaine de connexion correct.

Dépannage de l'accès HTTPS

Cette section couvre les scénarios dans lesquels l'interface utilisateur Web APIC ou l'interface de programmation d'application (API) REST (Representational State Transfer) est inaccessible via HTTPS.

Scénario: Délais de connexion HTTPS expirés

Problème : Le navigateur affiche « ERR_CONNECTION_TIMED_OUT » ou l'appel API se bloque lors de la connexion au contrôleur APIC sur le port 443.

Étapes de vérification :

1. Vérifiez que HTTPS est activé :
   <#root>

   ```
   apic1#

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

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

2. Vérifiez que le contrat OOB autorise le protocole TCP 443. Consultez la section « Vérifier les contrats OOB ».
3. Testez le contrôleur APIC lui-même pour confirmer que le processus HTTPS écoute :
   <#root>

   ```
   apic1#

   ss -tlnp | grep 443

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

Cause première : HTTPS désactivé, TCP 443 de filtrage de contrat OOB ou le processus nginx sur l'APIC a planté.

Solution : Activez HTTPS dans la stratégie d'accès à la gestion, mettez à jour le contrat OOB ou redémarrez le service Web sur le contrôleur APIC.

Scénario: Le navigateur affiche une erreur TLS Handshake

Problème : Le navigateur affiche « ERR_SSL_VERSION_OR_CIPHER_MISMATCH » ou une erreur TLS similaire.

Étapes de vérification :

1. Vérifiez la version du protocole TLS configurée sur le contrôleur APIC :
   <#root>

   ```
   apic1#

   moquery -c commHttps

   sslProtocols : TLSv1.2
   ```

2. Vérifiez que le navigateur prend en charge TLSv1.2. Les très anciens navigateurs (par exemple, Internet Explorer 10 et versions antérieures) ne prennent pas en charge TLSv1.2 par défaut.

Cause première : Le contrôleur APIC offre uniquement TLSv1.2 (par défaut) et le navigateur ou le client API prend uniquement en charge les versions TLS plus anciennes.

Solution : Mettez à jour le navigateur ou le client. Si vous devez prendre temporairement en charge des clients plus anciens, ajoutez TLSv1.1 à la stratégie d'accès à la gestion, mais cela présente un risque pour la sécurité.

Scénario: Limitation de limitation API

Problème : Les appels de l'API REST échouent par intermittence avec des erreurs HTTP 503 ou l'interface utilisateur Web devient lente pendant une automatisation importante.

Étapes de vérification :

<#root>

```
apic1#

moquery -c commHttps

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

Si le taux de régulation est très faible et que les scripts d'automatisation envoient de nombreuses requêtes par seconde, le contrôleur APIC rejette les requêtes excédentaires.

Cause première : Le taux d'accélération par utilisateur est trop faible pour la charge de travail d'automatisation.

Solution : Augmentez le taux d'étranglement sous la politique d'accès à la gestion ou optimisez les scripts d'automatisation afin de réduire la fréquence des demandes. Vous pouvez également désactiver la limitation si le fabric n'est pas partagé.

Dépannage de AAA — TACACS+

Cette section traite des échecs d'authentification TACACS+. Le contrôleur APIC communique avec le serveur TACACS+ via le port TCP 49.

Vérification opérationnelle

Les commutateurs ACI ne prennent pas en charge la **test aaa** commande disponible sur NX-OS autonome. Pour vérifier le fonctionnement de TACACS+, utilisez le contrôleur APIC pour vérifier l'état du fournisseur, les défaillances et l'historique des sessions de connexion.

Recherchez les défaillances actives sur le fournisseur TACACS+ :

<#root>

apic1#

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

Si aucune erreur n'est renvoyée, le contrôleur APIC considère que le fournisseur est accessible. Si des erreurs sont présentes, le résultat inclut des codes d'erreur tels que F1773 (fournisseur inaccessible) ou F1774 (échec d'authentification).

Vérifiez la configuration du fournisseur TACACS+ :

<#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
```

Vérifiez l'accessibilité du réseau de base du contrôleur APIC au serveur TACACS+ :

<#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
```

Tentez une connexion au contrôleur APIC avec le domaine de connexion TACACS+ et vérifiez le résultat de la session :

<#root>

apic1#

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

Examinez ce champ pour **descr** déterminer si l'échec est dû au rejet de l'authentification ou à un problème de connectivité.

Validez le flux d'authentification TACACS+ dans les journaux APIC. Filtrer pour le nom d'utilisateur en question :

<#root>

apic1#

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

Les connexions TACACS+ suivent le même flux d'**nginx.bin.log**authentification que LDAP (voir la section Vérification opérationnelle LDAP pour des exemples complets de journaux réels). Les principales différences de TACACS+ sont les suivantes :

- `DefaultAuthMo spécifie le domaine 2` — Le domaine 2 indique TACACS+ (par rapport au domaine 3 pour LDAP).
- `Ajout de TacacsProvider <IP> à la liste` — identifie le serveur TACACS+ contacté (par rapport à `LdapProvider` pour LDAP).
- `TACACS+ Cisco-avpair (shell : domains=all/admin/)` — la paire AV est retournée directement par le serveur TACACS+ (au lieu d'être convertie à partir d'une carte de groupe LDAP).

Une connexion TACACS+ réussie affiche la même progression : Demande PAM → Sélection du domaine → Recherche du fournisseur → Analyse des paires AV → Injection de l'utilisateur → Attribution du domaine et du rôle à l'utilisateur → `Privilèges d'écriture administrateur`.

Une connexion TACACS+ ayant échoué se termine avec l'`utilisateur <username> a été refusée`

`lors de l'authentification AAA` et l'erreur `Unauthorized ... : AAA Server Authentication DENIED`, le même modèle qu'un refus LDAP.

Scénario: Échec de l'authentification TACACS+

Problème : La connexion échoue avec « Authentication Failed » lorsque l'utilisateur sélectionne un domaine de connexion TACACS+.

Étapes de vérification :

1. Recherchez les défaillances actives sur le fournisseur TACACS+ :
   <#root>

   ```
   apic1#
   ```

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

   Le défaut F1773 indique un problème de connectivité. Le défaut F1774 indique un refus d'authentification.

2. Vérifiez l'accessibilité du réseau du contrôleur APIC au serveur TACACS+ :
   <#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. Si la requête ping aboutit mais que l'authentification échoue, vérifiez que le secret partagé correspond à la fois à la configuration du fournisseur APIC et à la configuration du serveur TACACS+.
4. Vérifiez les dernières sessions de connexion pour voir les détails de l'échec :
   <#root>

   ```
   apic1#
   ```

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

5. Recherchez la tentative d'authentification dans les journaux du serveur TACACS+. Une tentative réussie de connexion au serveur mais rejetée indique un problème de configuration utilisateur côté serveur (par exemple, une non-concordance de mot de passe ou un compte utilisateur manquant).
6. Vérifiez le flux d'authentification complet sur le contrôleur APIC **nginx.bin.log**. Filtrez par nom d'utilisateur plutôt que par mots-clés spécifiques afin que les messages intermédiaires ne

soient pas manqués :
<#root>

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

Comparez les résultats avec les exemples de fonctionnement et de non-fonctionnement dans la section Vérification opérationnelle ci-dessus. Indicateurs clés :

- `a été refusé` ou `REFUSÉ` — le serveur TACACS+ a été atteint mais a rejeté les informations d'identification. Vérifiez que l'utilisateur existe sur le serveur et que le mot de passe correspond.
- Aucun message spécifique au fournisseur après l'`ajout de TacacsProvider` — le serveur est inaccessible ou a expiré. Vérifiez l'accessibilité du réseau et l'EPG de gestion.
- `L'injection de l'utilisateur distant ... a été effectuée` suivie de lignes de vérification du rôle — l'authentification a réussi, mais le problème peut être lié à l'attribution du rôle (voir la section Paire AV ci-dessous).

Paire Cisco-AV TACACS+ pour RBAC

Pour les utilisateurs distants authentifiés via TACACS+, le serveur doit renvoyer l'**cisco-av-pair**attribut dans la réponse d'autorisation. Cet attribut mappe l'utilisateur aux domaines et rôles de sécurité de l'ACI.

Format :

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

Exemples:

- Administrateur complet : **shell:domains=all/admin/**
- Lecture seule pour tous : **shell:domains=all/read-all/**
- Administrateur du locataire pour un domaine spécifique : **shell:domains=TenantA/tenant-admin/**
- Domaines multiples : **shell:domains=all/admin/,TenantA/tenant-admin/**

Si cet attribut est manquant ou mal formé, l'utilisateur s'authentifie avec succès mais n'a aucun rôle et ne peut pas voir d'objets dans l'interface utilisateur APIC.

Remarque : L'accès SSH aux commutateurs Leaf et Spine nécessite le rôle admin avec le

privilège d'écriture dans le domaine de sécurité all. La paire AV minimale pour l'accès SSH du commutateur est **shell:domains=all/admin/**. Les utilisateurs avec des rôles non-admin (par exemple, `read-all`, `tenant-admin`, `aaa`) ou les utilisateurs assignés à un domaine de sécurité autre que all peuvent se connecter à l'APIC mais se voient refuser l'accès SSH aux commutateurs. Le journal APIC indique que les `connexions non admin sur le commutateur sont refusées` pour ces utilisateurs.

Validez la paire AV reçue en vérifiant **nginx.bin.log**. Filtrez par le nom d'utilisateur afin de voir le flux d'injection de rôle complet :

<#root>

apic1#

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

Pour TACACS+, la paire AV est enregistrée comme `TACACS+ Cisco-avpair (shell : domains=...)`. Une injection réussie montre que l'`injection de l'utilisateur distant <username> a été effectuée` suivie de `Found UserDomain` et de lignes de `privilèges d'écriture admin` (voir la section Vérification opérationnelle LDAP pour des exemples complets de ce flux avec une sortie de journal réelle).

Si le format de la paire AV n'est pas valide, le journal indique `ÉCHEC de l'injection des données <username> de l'utilisateur distant - le message d'erreur est Chaîne shell : domains non valide`. Si l'utilisateur s'authentifie avec un rôle non-admin, SSH aux commutateurs est refusé avec des `connexions non-admin sur le commutateur sont refusées`.

Cause première : Non-concordance du secret partagé, serveur inaccessible à partir du réseau de gestion, l'utilisateur n'existe pas sur le serveur TACACS+ ou l'EPG de gestion sur le fournisseur est incorrect.

Solution : Corrigez le secret partagé, corrigez l'accessibilité ou créez l'utilisateur sur le serveur TACACS+.

Valider les journaux d'authentification du commutateur Leaf

Sur les commutateurs Leaf et Spine, les événements de connexion SSH sont connectés à la fois à **pam.module.log** et à **nginx.log**. La **pam.module.log** affiche le résultat de l'authentification PAM (acceptation ou rejet). Le **nginx.log** contient le flux AAA complet (sélection de domaine, recherche de fournisseur, communication LDAP/TACACS+/RADIUS, analyse des paires AV et affectation de rôle) identique à celui du contrôleur APIC (**nginx.bin.log**sur le contrôleur APIC). Ces journaux s'appliquent à tous les

types AAA distants (TACACS+, RADIUS, LDAP).

Vérifiez **pam.module.log** le résultat de l'authentification :

<#root>

```
leaf101#

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

Fonctionnement — Authentification à distance réussie sur le commutateur :

```
||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
```

L'**remote=1**indicateur confirme que l'utilisateur a été authentifié par un serveur AAA distant.

Non opérationnel — l'utilisateur a été rejeté. La commande securitymgrAG refuse l'utilisateur et le commutateur tente une recherche d'utilisateur local comme dernier secours :

```
||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
```

Si aucune entrée PAM n'apparaît pour l'utilisateur, la connexion SSH a probablement été rejetée avant d'atteindre l'étape PAM (par exemple, en raison d'une non-concordance de chiffrement ou de l'annulation de la connexion par l'utilisateur).

Pour obtenir une vue plus détaillée du flux d'authentification sur le commutateur, cochez la case **nginx.log**. Ce journal contient la chaîne de décision AAA complète, au même format et avec les mêmes messages que **nginx.bin.log** sur le contrôleur APIC :

<#root>

leaf101#

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

Fonctionnement — Authentification LDAP réussie sur un commutateur (comparez avec les exemples LDAP APIC dans la section Vérification opérationnelle LDAP — les messages sont les mêmes) :

```
||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
```

Le commutateur **nginx.log** est particulièrement utile lorsqu'il **pam.module.log** affiche un rejet, mais n'explique pas pourquoi. Le fichier nginx.log indique le domaine AAA, le fournisseur et la raison de l'échec spécifique (par exemple, la recherche LDAP a renvoyé une valeur vide, le délai d'attente TACACS+ ou l'injection de paires AV a échoué).

Dépannage de AAA — RADIUS

Cette section traite des échecs d'authentification RADIUS. Le contrôleur APIC communique avec le serveur RADIUS via le port UDP 1812 (authentification) et éventuellement le port UDP 1813 (comptabilité).

Vérification opérationnelle

Les commutateurs ACI ne prennent pas en charge la **test aaa** commande disponible sur NX-OS

autonome. Utilisez les méthodes suivantes pour vérifier le fonctionnement de RADIUS.

Vérifiez la configuration du serveur RADIUS et les statistiques d'accessibilité à partir d'un commutateur Leaf :

<#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
```

Scénario: Échec de l'authentification RADIUS

Problème : La connexion échoue lorsqu'un utilisateur sélectionne un domaine de connexion RADIUS.

Étapes de vérification :

1. Vérifiez les statistiques du serveur RADIUS à partir d'un commutateur pour les signes de dépassement de délai ou d'échec :
   <#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
   ```

   Un nombre élevé sous demandes expirées indique que le serveur RADIUS est inaccessible ou que le secret partagé ne correspond pas (RADIUS abandonne silencieusement les

paquets en cas de conflit de secret partagé).

2. Vérifiez l'accessibilité du réseau au serveur RADIUS :
   <#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. Vérifiez que le secret partagé correspond entre le contrôleur APIC et le serveur RADIUS. Contrairement à TACACS+ qui utilise TCP et signale les échecs de connexion, RADIUS utilise UDP et supprime silencieusement les paquets lorsque le secret partagé ne correspond pas. Le seul symptôme est un dépassement de délai.
4. Vérifiez les journaux du serveur RADIUS. FreeRADIUS en mode de débogage (**radiusd -X**) affiche chaque requête et indique si elle a été acceptée, rejetée ou si elle ne correspondait pas à un secret partagé.
5. Recherchez le flux d'authentification RADIUS dans le contrôleur APIC **nginx.bin.log**. Filtrer par nom d'utilisateur :
   <#root>

   ```
   apic1#

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

   Les connexions RADIUS suivent le même flux d'**nginx.bin.log**authentification que LDAP et TACACS+ (voir la section Vérification opérationnelle LDAP pour des exemples complets de journaux réels). Les principales différences pour RADIUS sont les suivantes :

   - `Ajout de RadiusProvider <IP> à la liste` — identifie le serveur RADIUS (par rapport à `TacacsProvider` ou `LdapProvider`).
   - Le numéro de domaine pour RADIUS varie selon la configuration.

   Une connexion RADIUS réussie se termine par l'`injection de l'utilisateur distant... a été terminée` et les `privilèges d'écriture admin`.

   Une connexion RADIUS ayant échoué se termine par `a été refusée pendant l'authentification AAA` et `REFUSÉE`.

   Si aucun message spécifique à RADIUS n'apparaît après la ligne `Adding RadiusProvider`, le serveur a expiré. Contrairement à TACACS+ qui utilise TCP et signale les échecs de connexion, RADIUS utilise UDP et supprime silencieusement les paquets lorsque le secret partagé ne correspond pas. Le seul symptôme est un dépassement de délai suivi d'un déni.

6. Recherchez les erreurs actives sur le fournisseur RADIUS :
   <#root>

   ```
   apic1#
   ```

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

RADIUS cisco-av-pair pour RBAC

RADIUS utilise le même **cisco-av-pair** attribut que TACACS+ pour le mappage de rôle RBAC. Le serveur RADIUS doit renvoyer cet attribut dans la réponse Access-Accept :

<#root>

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

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

Dans FreeRADIUS, cette option est configurée dans le serveur principal LDAP ou dans le fichier de configuration **users**. Pour ISE, il est configuré sous le profil d'autorisation en tant qu'attribut avancé.

Cause première : Non-concordance du secret partagé (la plus courante avec RADIUS — cause des délais d'attente silencieux), serveur inaccessible, port d'authentification incorrect ou compte utilisateur manquant sur le serveur RADIUS.

Solution : Corrigez le secret partagé, vérifiez l'accessibilité du protocole UDP 1812 ou configurez l'utilisateur sur le serveur RADIUS.

Dépannage de AAA — LDAP

Cette section traite des échecs d'authentification LDAP. Le contrôleur APIC se connecte au serveur LDAP via le port TCP 389 (LDAP) ou le port TCP 636 (LDAP avec SSL).

Vérification opérationnelle

Les commutateurs ACI ne prennent pas en charge la **test aaa** commande disponible sur NX-OS autonome. Pour vérifier le fonctionnement du protocole LDAP, vérifiez les défaillances du fournisseur et la configuration du contrôleur APIC.

Recherchez les erreurs actives sur le fournisseur LDAP :

<#root>

apic1#

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

Le défaut F1777 indique un problème de connectivité. Le défaut F1778 indique un échec d'authentification ou de liaison. Si aucune erreur n'est renvoyée, le contrôleur APIC considère que le fournisseur est accessible.

Vérifiez l'accessibilité de base du réseau au serveur LDAP :

<#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
```

Pour LDAP, vérifiez également la connectivité TCP au port 389 (ou 636 pour LDAP). Si le contrôleur APIC peut envoyer une requête ping au serveur, mais que les erreurs LDAP persistent, le problème est généralement un DN de liaison incorrect, un mot de passe incorrect ou un pare-feu bloquant le port LDAP.

Validez le flux d'authentification LDAP dans les journaux APIC. Filtrer par nom d'utilisateur :

<#root>

apic1#

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

En cours — Une connexion LDAP réussie affiche le flux complet de recherche, de liaison et d'affectation de rôle :

```
||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
```

Non opérationnel — utilisateur introuvable dans l'annuaire LDAP (la recherche renvoie un jeu vide) :

```
||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
```

Scénario: Échec de l'authentification LDAP

Problème : La connexion échoue lorsqu'un utilisateur sélectionne un domaine de connexion LDAP.

Étapes de vérification :

1. Vérifiez l'accessibilité du serveur LDAP à partir du contrôleur APIC :
   <#root>

   ```
   apic1#
   ```

   ping 10.1.1.52

   ```
   PING 10.1.1.52 (10.1.1.52): 56 data bytes
   64 bytes from 10.1.1.52: icmp_seq=0 ttl=64 time=0.5 ms
   ```

2. Vérifier les défaillances du fournisseur LDAP actif :
   <#root>

   ```
   apic1#
   ```

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

3. Vérifiez la configuration du fournisseur LDAP :
   <#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. Vérifiez que l'utilisateur existe dans l'annuaire LDAP sous le DN de base configuré et qu'il correspond au filtre. Pour Active Directory, l'**sAMAccountName**attribut de l'utilisateur doit correspondre au nom d'utilisateur saisi lors de la connexion. Pour OpenLDAP, l'**cn**attribut ou **uid** doit correspondre.
5. Si vous utilisez LDAPS (port 636), vérifiez la chaîne de certificats SSL. Si **SSLValidationLevel** est défini sur strict, le contrôleur APIC rejettera la connexion si le certificat du serveur n'est pas approuvé ou a expiré.
6. Recherchez le flux d'authentification LDAP complet dans le contrôleur APIC **nginx.bin.log**. Filtrez par le nom d'utilisateur afin que les messages intermédiaires ne soient pas manqués :

   <#root>

```
apic1#

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

   Comparez les résultats avec les exemples de fonctionnement et de non-fonctionnement dans la section Vérification opérationnelle ci-dessus. D'autres modèles d'échec spécifiques à LDAP peuvent être trouvés en recherchant le journal en général :

   <#root>

```
apic1#

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

   Modèles courants de non-fonctionnement (comparer avec les exemples de vérification opérationnelle ci-dessus pour le flux complet) :

```
! 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
```

Autres modèles d'échec LDAP à rechercher :

- Délai de recherche LDAP dépassé (serveur inaccessible, lent ou pare-feu bloquant le port 389/636) - `échec` de la recherche `LDAP : code de retour pour ldap_search_ext_s : -5: Délai dépassé`
- Échec de la liaison (mot de passe racine ou de liaison incorrect, ou serveur a refusé la connexion) — `échec` de la `recherche LDAP : code de retour pour ldap_search_ext_s : -1: Impossible de contacter le serveur LDAP`
- Utilisateur trouvé mais mot de passe incorrect (échec de la liaison avec le mot de passe utilisateur) : le journal affiche la ligne `LDAP Record DN` mais est suivi d'un message refusé sans ligne `Bind to UserDN ... successful`.

Carte de groupe LDAP pour RBAC

LDAP utilise des mappages de groupe au lieu de l'**cisco-av-pair**attribut. Le champ du fournisseur **attribute** LDAP indique l'attribut LDAP qui contient les informations de groupe. Pour Active Directory, il s'agit généralement de **memberOf**.

Le contrôleur APIC compare le DN du groupe renvoyé aux règles de mappage de groupe LDAP (**aaaLdapGroupMapRule**) configurées afin d'attribuer le domaine de sécurité et le rôle appropriés. Si aucune règle de mappage de groupe ne correspond, l'utilisateur s'authentifie mais n'a aucun rôle.

Vous pouvez également définir le **attribute** sur **CiscoAVPair** et stocker la **shell:domains=all/admin/** valeur directement dans les attributs LDAP de l'utilisateur, qui suivent le même format que TACACS+ et RADIUS.

Cause première : DN ou mot de passe de liaison incorrect, le DN de base ne contient pas l'utilisateur, le filtre de recherche ne correspond pas au schéma de répertoire, l'échec de la validation du certificat LDAPS ou les règles de mappage de groupe manquantes.

Solution : Corrigez la configuration du fournisseur (DN de liaison, DN de base, filtre, paramètres SSL). Pour les problèmes RBAC, vérifiez que les règles de mappage de groupe correspondent aux groupes LDAP auxquels l'utilisateur appartient.

Dépannage du RBAC et des privilèges utilisateur

Cette section couvre les scénarios dans lesquels l'utilisateur réussit à s'authentifier mais ne

dispose pas du niveau d'accès attendu.

Scénario: Utilisateur Connecté Mais Ne Voit Aucun Locataire

Problème : Un utilisateur distant se connecte via TACACS+, RADIUS ou LDAP. La connexion réussit, mais l'utilisateur ne voit aucun locataire dans l'interface utilisateur et les appels d'API renvoient des résultats vides ou « 403 Interdit ».

Étapes de vérification :

1. Vérifiez la session de l'utilisateur pour voir quels rôles ont été attribués à la connexion :
   <#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
   ```

   Le **descr** champ affiche le résultat de la connexion. Si l'utilisateur s'est authentifié avec succès mais n'a pas de rôle RBAC, le serveur AAA n'a pas renvoyé de correspondance valide **cisco-av-pair** ou de correspondance de groupe LDAP.

2. Vérifiez le contrôleur APIC **nginx.bin.log** pour voir la paire AV et l'attribution de rôle lors de la connexion. Filtrer par nom d'utilisateur :
   <#root>

   ```
   apic1#

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

   Recherchez les messages d'injection de rôle et d'attribution de domaine :

   En cours — Paire AV convertie à partir du mappage de groupe LDAP, l'utilisateur obtient le rôle admin :

   ```
   ||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
   ```

Non opérationnel : si une ligne **Cisco-avpair** ou **Converted to CiscoAVPair** n'apparaît pas dans le flux, le serveur AAA n'a pas renvoyé l'attribut et aucune règle de mappage de groupe LDAP ne correspond. Recherchez **Checking all UserDomains** si aucune ligne **Found UserDomain** ne le suit : l'utilisateur a été authentifié mais n'a pas de rôle attribué. Si un **Injection ... data FAILED** message apparaît, le format de la chaîne de la paire AV n'est pas valide.

3. Vérifiez que le serveur AAA renvoie l'**cisco-av-pair**attribut (pour TACACS+ ou RADIUS) ou l'appartenance au groupe LDAP correcte (pour LDAP). Vérifiez la configuration du serveur AAA :
    - TACACS+: Vérifiez que le profil utilisateur inclut **cisco-av-pair** avec le format **shell:domains=all/admin/.**
    - RADIUS: Vérifiez que le profil utilisateur est renvoyé **Cisco-AVPair = "shell:domains=all/admin/"** dans Access-Accept.
    - LDAP : Vérifiez que l'utilisateur est membre d'un groupe LDAP qui correspond à une règle de mappage de groupe LDAP (**aaaLdapGroupMapRule**) configurée.
4. Si l'attribut est présent mais que l'utilisateur n'a toujours pas accès, vérifiez que le nom du domaine de sécurité dans l'attribut correspond à un domaine de sécurité existant sur le contrôleur APIC :
    <#root>

    ```
    apic1#

    moquery -c aaaDomain
    ```

    Si le **cisco-av-pair** fait référence à un domaine qui n'existe pas (par exemple, **shell:domains=NonExistentDomain/admin/**), l'attribution du rôle échoue en silence.

Cause première : Le serveur AAA ne renvoie pas les attributs de mappage RBAC, le format d'attribut est incorrect ou le domaine de sécurité référencé dans l'attribut n'existe pas sur le contrôleur APIC.

Solution : Configurez le serveur AAA pour renvoyer le mappage correct **cisco-av-pair** ou le mappage de groupe. Vérifiez que le domaine de sécurité existe sur le contrôleur APIC.

Scénario: L'Utilisateur Peut Afficher Mais Ne Peut Pas Modifier La Configuration

Problème : Un utilisateur peut se connecter et parcourir les objets, mais il reçoit une erreur lorsqu'il tente d'envoyer des modifications.

Étapes de vérification :

1. Vérifiez les attributions de rôle de l'utilisateur :
    <#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. Si l'utilisateur a besoin d'un accès en écriture, le rôle doit accorder **writePriv**. Les rôles communs avec des privilèges d'écriture incluent admin, tenant-admin, access-admin et fabric-admin.
3. Validez l'affectation de rôle dans les journaux APIC. Filtrer par nom d'utilisateur : <#root>

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

Recherchez les messages d'attribution de rôle vers la fin du flux d'authentification :

En cours — l'utilisateur a le rôle d'écriture admin (à partir d'une connexion LDAP réelle) :

```
||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 — si le journal affiche `non-admin UserRole` avec des `privilèges de lecture` au lieu de `privilèges d'écriture admin`, l'utilisateur a un rôle en lecture seule et ne peut pas modifier la configuration. Recherchez des lignes comme :

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

Si le journal affiche uniquement les `privilèges de lecture` et aucun privilège d'`écriture`, mettez à jour le rôle de l'utilisateur ou la paire AV sur le serveur AAA.

Cause première : L'utilisateur dispose d'un rôle en lecture seule (par exemple, lecture totale ou opérations) au lieu d'un rôle capable d'écrire.

Solution : Mettez à jour l'affectation de rôle de l'utilisateur sur le contrôleur APIC (pour les utilisateurs locaux) ou mettez à jour le **cisco-av-pair** sur le serveur AAA (pour les utilisateurs distants) afin d'inclure un rôle avec des privilèges d'écriture.

Scénario: L'Utilisateur Peut Accéder À Certains Locataires Mais Pas À D'Autres

Problème : Un utilisateur peut voir et gérer un service partagé mais ne peut pas voir d'autres services partagés, même s'ils ont besoin d'un accès.

Étapes de vérification :

1. Vérifiez l'attribution du domaine de sécurité de l'utilisateur :
   <#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. Les domaines de sécurité correspondent aux locataires. Si l'utilisateur a besoin d'un accès à TenantB, il doit également être affecté au domaine de sécurité associé à TenantB ou au domaine all.
3. Pour les utilisateurs distants, vérifiez que la paire AV ou le mappage de groupe LDAP attribue les domaines appropriés. Vérifiez le contrôleur APIC **nginx.bin.log** pour l'attribution de domaine à la connexion. Filtrer par nom d'utilisateur :
   <#root>

   ```
   apic1#

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

   Fonctionnement — l'utilisateur dispose du domaine all (visibilité totale), à partir d'une véritable connexion LDAP :

   ```
   ||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
   ```

   Non opérationnel : si l'utilisateur n'a qu'un seul domaine de service partagé, seul ce domaine apparaît dans les **Found UserDomain** messages au lieu de tous. Par exemple, `Found UserDomain TenantA` signifie que l'utilisateur peut uniquement voir TenantA. L'utilisateur a besoin de domaines supplémentaires ajoutés à la paire AV sur le serveur AAA, ou le domaine all pour un accès complet.

Cause première : L'utilisateur est affecté à un domaine de sécurité restreint qui couvre

uniquement des locataires spécifiques.

Solution : Ajoutez les domaines de sécurité requis à la configuration de l'utilisateur ou utilisez le domaine all pour un accès complet.

Récupération de mot de passe et accès d'urgence

Si tous les comptes d'administration sont verrouillés ou si le serveur AAA distant est inaccessible et que le domaine par défaut a été modifié, utilisez l'une des méthodes de récupération suivantes :

Domaine de connexion de secours

L'ACI fournit un domaine de connexion de secours intégré qui utilise toujours l'authentification locale, quel que soit le domaine d'authentification par défaut. Pour l'utiliser :

- SSH : Connectez-vous en tant que **apic:fallback\\admin** (ou, **apic#fallback\\admin** selon la version).
- IUG: Dans la liste déroulante Domain de l'écran de connexion, sélectionnez fallback et utilisez les informations d'identification locales.

Accès console

Si le domaine d'authentification de la console est défini sur local (valeur par défaut), vous pouvez toujours vous connecter via le port de console APIC avec des informations d'identification locales. Si le mot de passe de l'administrateur local est inconnu, il peut être réinitialisé via le contrôleur de gestion intégré Cisco (CIMC) (pour les APIC physiques) ou la console de l'hyperviseur (pour les APIC virtuels).

Remarque : Si le domaine d'authentification de la console a été remplacé par un serveur AAA distant et que ce serveur est inaccessible, l'accès à la console échoue également. Il s'agit d'un scénario de verrouillage courant. Conservez toujours le domaine d'authentification de la console défini sur local.

Référence des erreurs courantes

Les défaillances suivantes de l'ACI sont généralement associées à des problèmes d'accès à distance et AAA :

- F1773 : problème de connectivité du fournisseur TACACS+. Le contrôleur APIC ne peut pas atteindre le serveur TACACS+.
- F1774 — Échec de l'authentification TACACS+. Le serveur est accessible mais a rejeté la tentative d'authentification.
- F1775 — Problème de connectivité du fournisseur RADIUS.
- F1776 — Échec de l'authentification RADIUS.
- F1777 — Problème de connectivité du fournisseur LDAP.
- F1778 — Échec de l'authentification LDAP.
- F0532 — Sous-réseau de gestion non configuré pour un noeud.

Interroger les erreurs AAA actives :

<#root>

```
apic1#

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

Références

- Dépannage de la gestion ACI et des services principaux — Politiques de pod
- Cisco APIC Basic Configuration Guide, version 6.1(x) — Gestion
- Guide de configuration de la sécurité Cisco APIC - Accès, authentification et comptabilité

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.