أستكشاف أخطاء الوصول عن بعد وإصلاحها في بنية قائمة التحكم في الوصول (ACI)

المقدمة

يوضح هذا المستند كيفية التحقق من مشاكل الوصول عن بعد واستكشاف أخطائها وإصلاحها في بنية Cisco Application Centric Infrastructure (ACI). وهو يغطي الوصول إلى واجهات الآمن عبر بروتوكولات طبقة الأمان (SSH) ونقل النص التشعبي الآمن (HTTPS) والمحولات البنية، والمصادقة عن بعد، والتخويل والمحاسبة (AAA) وبرمجة التطبيقات (APIC) الطرفية باستخدام نظام التحكم في الوصول إلى وحدة تحكم الوصول إلى المحطة الطرفية لدليل (TACACS+)، وخدمة مستخدم طلب الاتصال عن بعد (RADIUS)، وبروتوكول الوصول إلى الدليل خفيف الوزن (LDAP)، تفويض التحكم في الوصول المستند إلى الأدوار (RBAC). يتم تضمين شجرة قرارات فرز وسيناريوهات مفصلة لاستكشاف المشكلات وحلها لكل منطقة.

معلومات أساسية

تم توليف المواد الواردة من هذا المستند من دليل أستكشاف أخطاء إدارة قائمة التحكم في الوصول (ACI) وإصلاحها — دليل سياسات البنية الأساسية، دليل التكوين POD، دليل الإدارة، ودليل البرمجة الأساسي لواجهة برمجة التطبيقات (APIC) من Cisco، الإصدار 6.1(x) — فصل الوصول والمصادقة والمحاسبة وتكوين أمان واجهة برمجة التطبيقات (APIC) من Cisco — فصل.

نظرة عامة

يتضمن الوصول عن بعد إلى بنية قائمة التحكم في الوصول (ACI) ثلاث طبقات مختلفة، يجب أن يعمل كل منها للمهندس لتسجيل الدخول والتشغيل بنجاح:

1. النقل — يجب أن يكون مسار شبكة الإدارة (OOB أو داخل النطاق الترددي) وخدمة البروتوكول (SSH أو HTTPS) قابلين للوصول والتمكين.
2. المصادقة — يجب التحقق من بيانات اعتماد المستخدم، إما محليا على APIC أو مقابل خادم AAA بعيد (TACACS+ أو RADIUS أو LDAP).
3. التفويض — يجب أن يتم تعيين أدوار RBAC الصحيحة ومجالات الأمان للمستخدم الذي تمت مصادقته لعرض كائنات ACI المقصودة وتعديلها.

والفشل في أي طبقة ينتج أعراضا مختلفة. يؤدي فشل النقل إلى منع الاتصال بالكامل.

يرجع فشل المصادقة خطأ بيانات اعتماد. يسمح فشل التخويل بتسجيل الدخول ولكنه يقيد إمكانية الرؤية وأ ينتج عن أخطاء "403 ممنوع" في واجهة برمجة التطبيقات.

سياسة الوصول إلى الإدارة

Management Access Policy (commPol) هو الكائن المركزي الذي يتحكم في أي بروتوكولات الوصول عن بعد يتم تمكينها على البنية. يوجد أسفل البنية > سياسات البنية > السياسات > Pod > الوصول إلى الإدارة > الافتراضي. يحتوي النهج على كائنات تابعة يتم تكوينها:

- SSH (commSsh) — خوارزميات الحالة الإدارية والمنفذ والشفرات وتبادل المفاتيح (KEX) وخوارزميات مفاتيح المضيف وأكواد مصادقة الرسائل (MACs).
- HTTPS (commHttps) — الحالة الإدارية، المنفذ، إصدار بروتوكول أمان طبقة النقل (TLS)، مدعل الكبح، ومصادقة شهادة العميل.
- Telnet (commTelnet) — الدولة والمنفذ الإداريان. أعجزت Telnet افتراضيا وهو يوصي cisco بظل معأق.

إدارة خارج النطاق الترددي وداخل النطاق

تدعم عقد واجهة التحكم في الوصول (ACI) مساريين للوصول إلى الإدارة:

- خارج النطاق (OOB) — يستخدم منفذ الإدارة المخصص على APIC أو المحول. يتم تخصيص عناوين الإدارة خارج النطاق (OOB) من تجمع تحت مستأجر الإدارة وتخصيصها للعقد عبر mgmtRsOoBStNode. في APIC، يتم فرض عقود OOB من خلال iptables قواعد. إذا تم تطبيق عقد خارج النطاق (OOB)، يمكن لحركة مرور البيانات المسموح بها بشكل صريح بواسطة العقد فقط الوصول إلى واجهة إدارة APIC.
- داخل النطاق (INB) — يستخدم مستوى بيانات البنية لحركة مرور الإدارة. تتطلب طاق ومجموعة نطاق الإدارة داخل النطاق تعييني عنوان إدارة العقد والشبكة الفرعية (BD) الإدارة داخل النطاق من خارج البنية دون الوصول إلى عناوين IP داخل النطاق من خارج البنية. لا يمكن والعقد (EPG) النهائية توجيه إضافي أو تكوين نهج.

ملاحظة: يتم تكوين عناوين IP الخاصة بإدارة APIC OOB أثناء الإعداد الأولي ويحصل وهو مسار الإدارة الأساسي وهو OOB. لم التشاف البنية بالكامل قبل اتصال IP على APIC متوفر دائما إذا كانت شبكة الإدارة المادية متصلة.

بنية AAA

يستخدم ACI نموذج AAA من ثلاث طبقات:

1. يحدد. مسمى نطاق ضمن AAA مزودي مجموعات — (**aaaLoginDomain**) الدخول تسجيل مجال
   المستخدمون مجال تسجيل الدخول في شاشة تسجيل الدخول (على سبيل المثال،
   apic:TACACS-Domain أو عبر القائمة المنسدلة في واجهة المستخدم). يوجد دائما مجال
   إحتياطي خاص لتسجيل الدخول وخرائط للمصادقة المحلية.
2. تشير — (**aaaTacacsPlusProviderGroup**، **aaaRadiusProviderGroup**، **aaaLdapProviderGroup**) الموفر مجموعة
   إلى خادم AAA واحد أو أكثر وتعرف الترتيب الذي تتم تجربته به.
3. يحدد الخادم IP أو المنفذ وأ — (**aaaTacacsPlusProvider**، **aaaRadiusProvider**، **aaaLdapProvider**) الموفر
   وأ EPG إدارة وأ المحاولة وأ إعادة المهلة وأ عمليات (LDAP ل Bind DN وأ) المشترك السر
   مراقبة بيانات الاعتماد.

يحدد نطاق المصادقة الافتراضي (**aaaDefaultAuth**) أي مجال تسجيل الدخول يتم إستخدامه عندما
ال يحدد المستخدم مجال تسجيل دخول. يتحكم نطاق مصادقة وحدة التحكم في مصادقة
جلسات عمل وحدة التحكم.

ملاحظة: سيؤدي تغيير نطاق المصادقة الافتراضي إلى خادم AAA بعيد أثناء عدم
إمكانية الوصول إلى الخادم إلى منع كل من الوصول إلى البنية. اختبر اتصال خادم
AAA الإحتياطي قبل تغيير النطاق. يمكن إستخدام مجال تسجيل الدخول الافتراضي والمصادقة محليا
(apic:backback\\admin) من أجل تجاوز النطاق الافتراضي.

ملفات سجل المصادقة والتفويض والمحاسبة (AAA) الأساسية

يتم تسجيل أحداث مصادقة AAA في العديد من الملفات على كل من وحدات APIC و fabric.
هذه السجلات هي الأداة الأساسية للتحقق من نتائج المصادقة وتحديد النطاق ومجموعة
الموفر التي يتم إستخدامها وتشخيص حالات فشل تعيين الدور.

الوصف	الموقع (الوحدات)	الموقع (APIC)
سجل AAA الأساسي. يحتوي على تدفق طلب المصادقة الكامل: PAM، تحديد النطاق، اتصال LDAP/TACACS+/RADIUS، بحث الموفر، تعيين AV، تحليل زوج الدور، ونتيجة المجال والرفض أو النجاح. يختلف اسم الملف بين منصات الأنظمة الأساسية ولكن تنسيق المحتوى هو نفسه.	/var/sysmgr/tmp_logs/dme_logs/nginx.log	/var/log/dme/log/nginx.bin.log
سجل طلب NGINX HTTP. يسجل سطر واحد لكل طلب واجهة برمجة تطبيقات.	/var/log/dme/log/access.log	/var/log/dme/log/access.log

الوصف	الموقع (المحولات)	الموقع (APIC)
في APIC، رهظي aaaLogin وaaaRefresh عم ةملاكم HTTP (200 = رمز ةلاح، 401 = ضفر). في تاملاكملا، رهظت تابلط وأ ةجمرب تاقيبطت ةيلخادلا DME تاملاكملاو aaaRefresh.		
سجل PAM ةدحو ةيطمنلا. ةجيتن ضرعي لمع تاسلجل ةقداصملا SSH: يذلا مدختسملا IP و تمت ةقداصم هتقداصم فرعمو ردصملا مدختسم UNIX نيعملا. في تالوحملا، هذه يه ةقيرطلا عرسألا دكأتلل دق مدختسملا ناك اذإ ام تمت ةقداصم هتقداصم وأ هضفر.	/var/log/dme/log/pam.module.log	/var/log/dme/log/pam.module.log

ملاحظة: يحتوي سجل المصادقة والتفويض والمحاسبة (AAA) الأساسي على اسم ملف ماظن لك ىلع فلتخم يساسأ. على APIC يكون في **nginx.bin.log**/var/log/dme/log/. على المحولات الطرفية والخلفية يكون في **nginx.log**/var/sysmgr/tmp_log/dme_log/. قيسنت ىوتحم السجل ورسائل AAA هي نفسها على كلا النظامين الأساسيين.

تتبع إدخالات AAA في سجل NGINX هذا التنسيق:

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

تصفية إدخالات السجل المتعلقة ب AAA لتدفق مصادقة مستخدم معين:

<#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
```

أو عرض كافة طلبات المصادقة والنتائج الأخيرة:

<#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
```

يبدي تدفق المصادقة النموذجي الناجح هذه الرسائل الأساسية بالترتيب:

1. الدخول.تسجيل طلب يتلقى تم — <user> :اسم المستخدم NGINX من PAM مصادقة طلب يتلقى تم
2. النطاق.تحديد تم — ! <name> المورفع مجموعة .<N> المجال DefaultAuthMo يحدد
   (0=إحتياطي/محلي، 2=TACACS+، 3=ldap).
3. (RADIUS أو طلب +TACACS مورفع بحث أو LDAP طبر) بالمزود خاصة رسائل
4. تعيين المجال من — <user> :اسم المستخدم البعيد تحت <domain> UserDomain على العثور تم
   AAA استجابة.
5. UserDomain all ضمن لمسؤول كتابة امتيازات لديه مسؤول :اسم المستخدم الذي تم العثور عليه
   الدور.من التحقق تمرير تم — لمسؤول مستخدم مستخدم مستخدم

سجل مصادقة فاشل:

- AAA مصادقة أثناء <user> المستخدم رفض تم
- AAA خادم مصادقة رفض تم :به مصرح غير مستخدم <user> خطأ

ملاحظة: يتم تدوير سجل NGINX بشكل متكرر ويتم ضغط الإدخالات الأقدم باستخدام اللاحقة الرقمية. في APIC، السجلات التي تم تدويرها موجودة في نفس الدليل (على سبيل المثال، **nginx.bin.log.22815.gz**). في المحولات، يتم تخزين السجلات المدارة في **/var/log/dme/oldlog/dme/nginx.log.*.gz** (مع الارتباطات المماثلة في /var/sysmgr/tmp_log/dme_log/). للبحث في السجلات المدارة:

<#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'
```

نموذج RBAC

تتحكم ACI RBAC في ما يمكن للمستخدم الذي تمت مصادقة بياناته أن يراه ويفعله. يحتوي النموذج على ثلاثة مكونات:

- مجال الأمان (**aaaDomain**) — محدد النطاق الذي يقوم بالتعيين إلى كائنات ACI (المستأجرين، سياسات الوصول، سياسات البنية). المجالات المضمنة جميعها، الشائعة، و mgmt موجودة دائما. تقيد المجالات المخصصة إمكانية رؤية المستخدم على مستأجرين أو مناطق نهج معينة.
- الدور (**aaaRole**) — يحدد مجموعة من الامتيازات. تتضمن الأدوار التي تم إنشاؤها مسبقا fabric-admin، و access-admin، و read-all، و tenant-ext-admin، و المستأجر-admin، و aaa، والمسؤول، و nw-svc-admin، و ops، و admin.
- امتياز — كل دور يمنح إما قراءة وأ كتابة (مما يعني قراءة) الوصول إلى منطقة وظيفية معينة.

تم تعيين حساب مستخدم واحد أو أكثر من أزواج أدوار ومجال أمان. بالنسبة للمستخدمين البعيدين الذين تمت مصادقتهم عبر بروتوكول TACACS+ أو RADIUS أو LDAP، يتم تسليم تعيين الدور عبر السمات الخاصة بالمورد في إستجابة المصادقة والتفويض والمحاسبة (AAA) (على سبيل المثال، **cisco-av-pair** السمة).

شجرة قرارات الفرز

أستخدم شجرة القرارات هذه عندما يبلغ المستخدم عن عدم قدرته على الوصول إلى بنية واجهة التحكم في الوصول (ACI) عن بعد:

1. هل يمكنك إختبار اتصال APIC أو IP لإدارة المحول؟
   - نعم ← متابعة.
   - لا ← أستكشاف أخطاء مسار شبكة الإدارة وإصلاحها. يرجى الرجوع إلى قسم "أستكشاف أخطاء النشر خارج النطاق (OOB) وإدارتها داخل النطاق وإصلاحها".
2. هل يمكنك إنشاء اتصال SSH أو HTTPS (هل الاتصال مفتوح على الإطلاق)؟

- عدم وجود تكوين المنفذ، أو تكوين البروتوكول، أو تكوين مدخل التعطيل ← لا يمكن الوصول إلى SSH. تشفير. تحقق من الأقسام "استكشاف أخطاء الوصول إلى SSH وإصلاحها" أو "استكشاف أخطاء الوصول إلى HTTPS وإصلاحها".
- متابعة. ← نعم

3. هل تظهر شاشة تسجيل الدخول (HTTPS) أو هل اكتملت مصافحة SSH وتطلب بيانات الاعتماد؟
- فشل في تبادل مفتاح SSH أو مصافحة TLS. يرجى الإشارة إلى قسم ← لا يوجد تشفير KEX. "استكشاف أخطاء الوصول إلى SSH وإصلاحها"
- متابعة. ← نعم

4. هل فشلت بيانات الاعتماد مع "فشل المصادقة" أو ما شابه؟
- استكشاف أخطاء المصادقة في مشكلة ← نعم. الرجاء الإشارة إلى أقسام "استكشاف أخطاء المصادقة AAA وإصلاحها" (TACACS+ أو RADIUS أو LDAP ووفقا لمجال تسجيل الدخول قيد الاستخدام).
- متابعة. ← لا

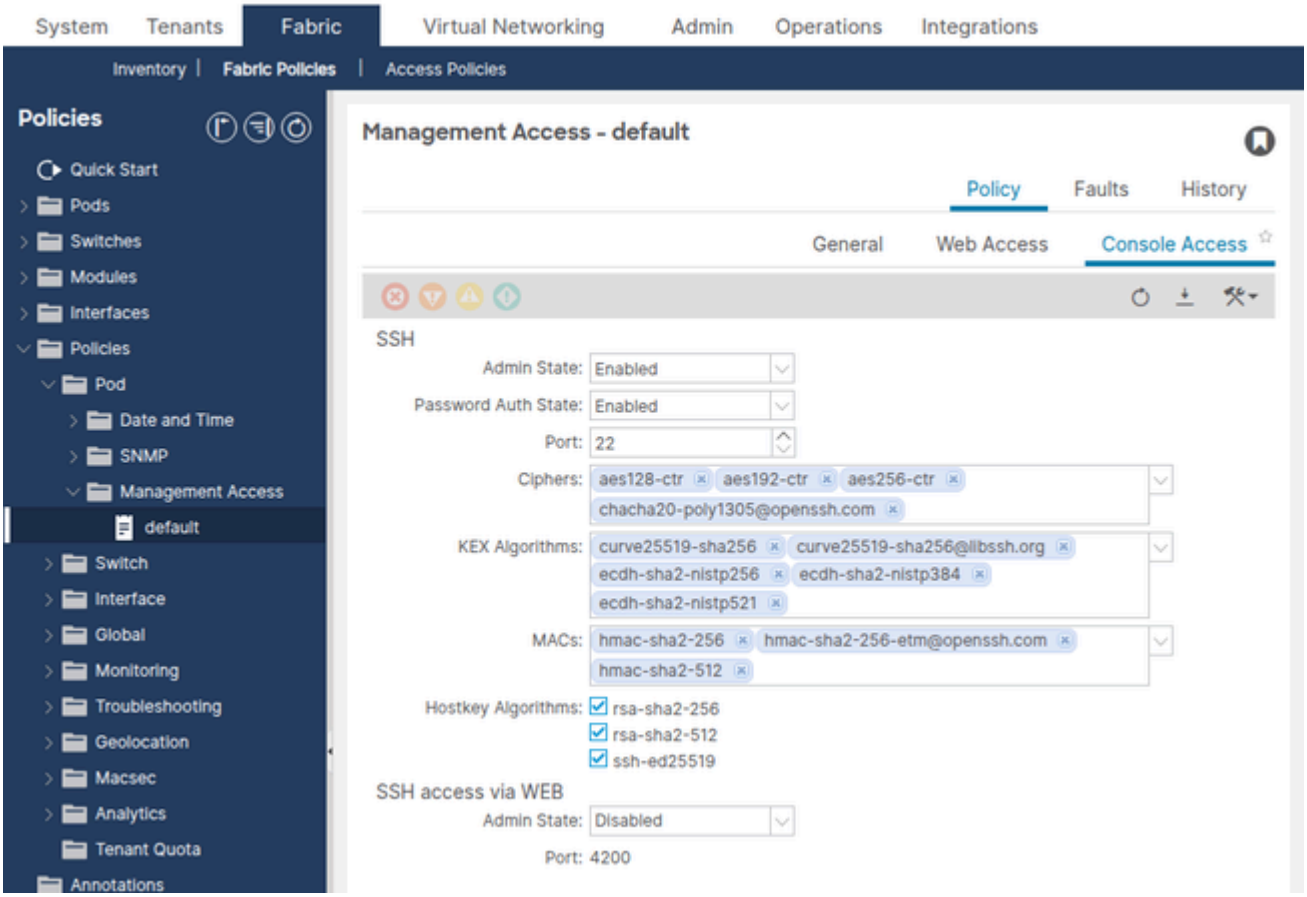
5. هل يقوم المستخدم بتسجيل الدخول ولكن لا يمكنه رؤية الكائنات المتوقعة، أو يستلم ممنوع "403"؟
- أخطاء RBAC ← نعم. يرجى الرجوع إلى قسم "استكشاف أخطاء RBAC وإصلاح التخويل أو إصدار المستخدم وامتيازات المستخدم".
- ← لا يعمل أي وصول. تحقق من المشكلة المحددة التي يواجهها المستخدم.

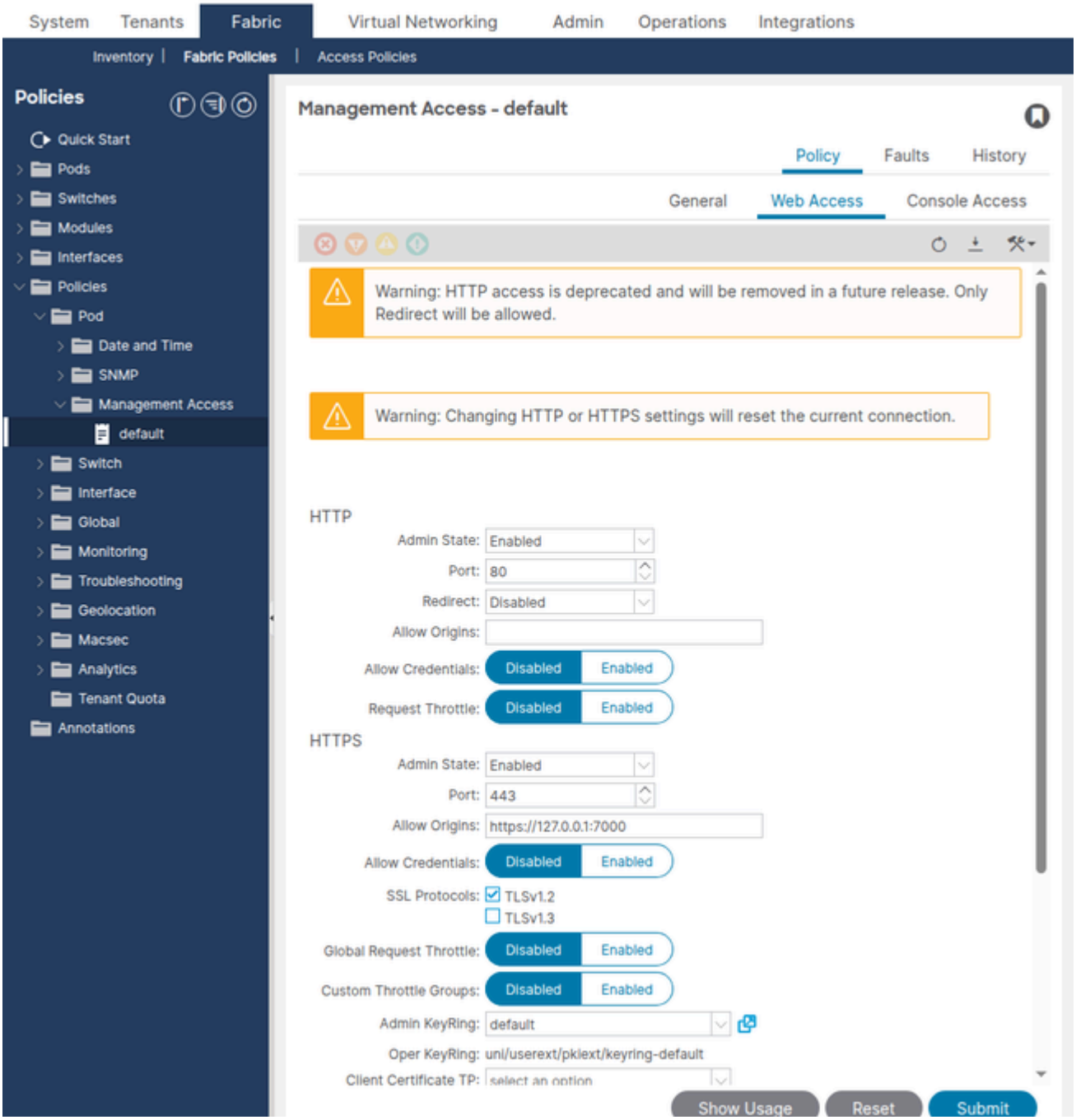
التحقق من التكوين

قبل استكشاف أخطاء حالة التشغيل وإصلاحها، تحقق من اكتمال سلسلة التكوين. يعد التكوين الخاطئ هو السبب الجذري الأكثر شيوعا لمشاكل الوصول عن بعد.

التحقق من سياسة الوصول إلى الإدارة (SSH و HTTPS)

انتقل إلى البنية > سياسات البنية > السياسات > Pod > الوصول إلى الإدارة > الافتراضي.


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



تأكيد إعدادات SSH التالية:

- حالة المسؤول — يجب تمكينها.
- المنفذ — الافتراضي 22. إذا تم التغيير، يجب أن يستخدم عميل SSH المنفذ المخصص.
- مصادقة كلمة المرور — ممكنة (ما لم تكن المصادقة على الشهادة فقط معدة).
- يجب أن تتضمن شفرة SSH — على الأقل شفرة واحدة يدعمها عميل SSH.
- خوارزميات KEX — يجب أن تتضمن على الأقل خوارزمية واحدة يدعمها عميل SSH.
- عناوين MAC عبر بروتوكول SSH — يجب أن تتضمن على الأقل أحد عناوين MAC المدعومة من قبل عميل SSH.

الاستعلام عن الكائن المدار بواسطة SSH عبر واجهة برمجة التطبيقات:

<#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
```

تأكيد إعدادات HTTPS التالية:

- حالة المسؤول — يجب تمكينها.
- المنفذ — 443.
- بروتوكولات SSL — TLSv1.2 (الافتراضي). قد يتطلب العملاء الأقدم إضافة TLSv1.1 بشكل صريح.
- حالة الكبح — في حالة التمكين، يحد معدل الكبح عدد الطلبات في الثانية لكل مستخدم. قد تتسبب القيمة المنخفضة جدا في حدوث أخطاء في مهلة واجهة برمجة التطبيقات.

<#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
```

أخطاء تكوين شائعة

- تم تقييد شفرة SSH بشكل مفرط — في الإصدار 5.2(1) من وحدة التحكم في الوصول (ACI) والإصدارات الأحدث، تم تقوية شفرة SSH الافتراضية. يمكن للعملاء SSH الأقدم (على سبيل المثال، إصدارات PuTTY قبل 0.75، أو إصدارات OpenSSH التي توفر فقط **diffie-hellman-group14-sha1**) فشل تبادل المفاتيح. يعرض عميل SSH "لم يتم العثور على أسلوب تبادل مفاتيح مطابق" أو "لم يتم العثور على تشفير مطابق".
- يتم تعطيل مصادقة كلمة المرور — إذا تم تعيين **passwordAuth** على تعطيل، يتم

السماح بالمصادقة المستندة إلى مفتاح SSH فقط. سيرى المستخدمون الذين يتصلون بكلمات المرور "تم رفض الإذن (publicKey)".
- يحدد أن يجب، 22 من SSH منفذ تغيير تم إذا — العميل وعي دون مخصص SSH منفذ عميل SSH المنفذ الجديد (على سبيل المثال، **ssh -p 2222 admin@10.1.1.1**).

التحقق من عناوين إدارة OOB

انتقل إلى المستأجرين > الإدارة > عناوين إدارة العقد.

تأكد من أن كل عقدة APIC والمحول تحتوي على عنوان IP لإدارة OOB مع بوابة صالحة. لن يمكن الوصول إلى العقد التي لا تحتوي على عناوين إدارة عبر شبكة الإدارة.

الاستعلام عن تعيينات العقدة الثابتة OOB عبر واجهة برمجة التطبيقات (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
```

أخطاء تكوين شائعة

- لن **mgmtRsOoBStNode.** لفسأ لاخدإ ىلع لوحملا يوتحي لا — دوقفم OOB ناونع نييعت إلى SSH أو HTTPS على الواجهة ولن تستجيب لبروتوكول IP للإدارة على العقدة يحتوي خارج النطاق (OOB).
- إدارة غير صحيحة — البوابة الفعلية على شبكة إدارة الإجراء. يمكن للعقدة تلقي الحزم ولكن لا يمكنها إرسال حركة مرور OOB.
- عدم تطابق قناع الشبكة الفرعية — لا يتطابق قناع الشبكة الفرعية مع OOB على شبكة الإدارة المادية. قد يتسبب ذلك في اعتقاد العقدة بأن محطة الإدارة موجودة على شبكة فرعية مختلفة وحركة مرور المسار عبر بوابة غير موجودة أو غير صحيحة.

التحقق من عقود خارج النطاق الترددي

انتقل إلى المستأجرين > الإدارة > العقود.

إذا تم تطبيق عقد OOB على EPG الخاص بالإدارة OOB، فإن حركة المرور المسموح بها بشكل صريح بواسطة هذه العقد هي فقط التي ستصل إلى واجهة إدارة APIC. في APIC، يتم فرض عقود OOB من خلال iptables قواعد.

الاستعلام عن العقود التي قدمها EPG OOB:

```
<#root>

apic1#

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

في حالة إرجاع الاستعلام للنتائج، يتم تطبيق العقود. التحقق من أن مواضيع العقد وعوامل التصفية تسمح بالبروتوكولات المطلوبة:

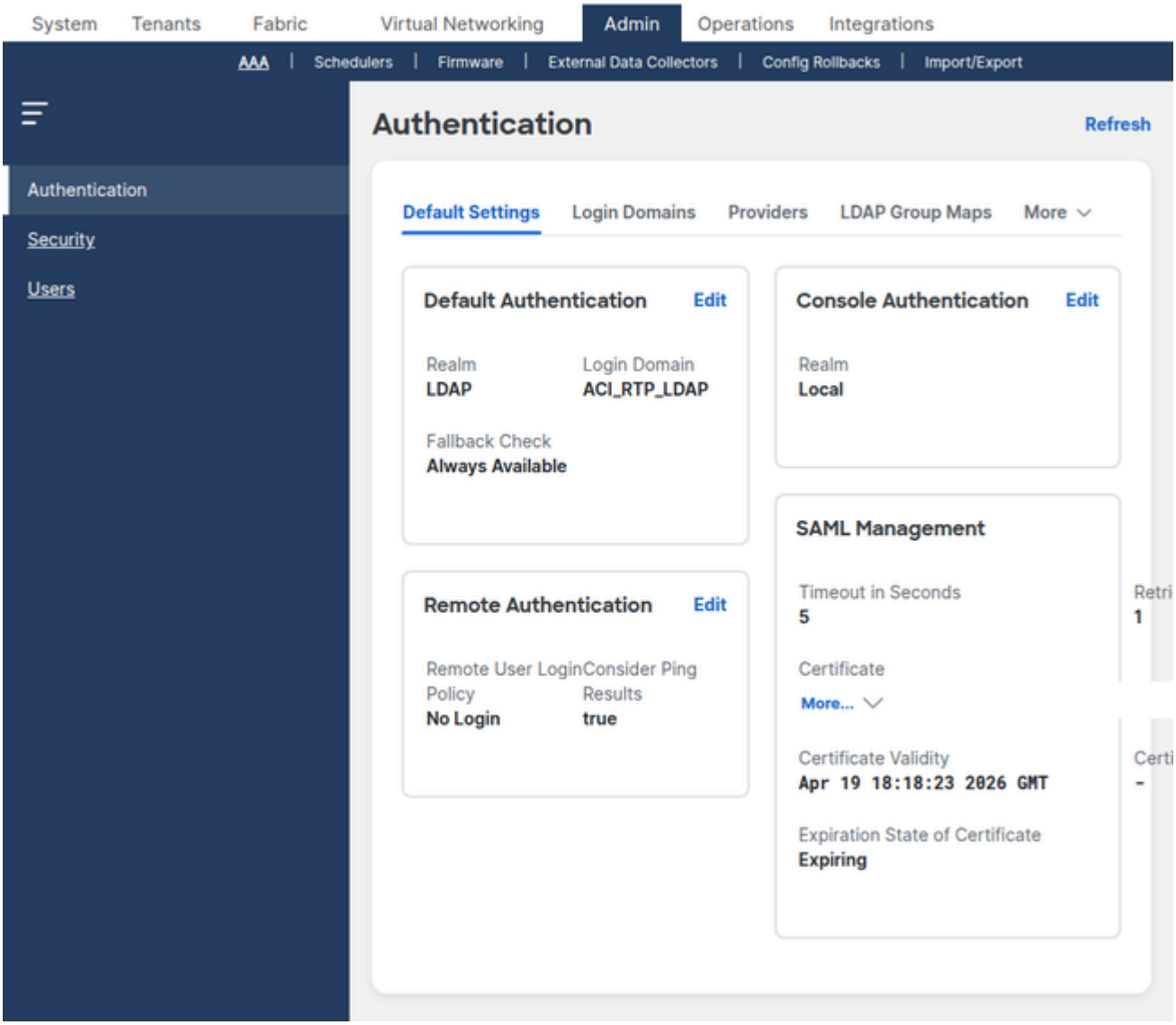
- SSH — منفذ TCP 22 (أو منفذ مخصص)
- HTTPS — منفذ TCP رقم 443 (أو منفذ مخصص)
- ICMP — للتحقق من إختبار الاتصال

أخطاء تكوين شائعة

- APIC يتضمن عقد OOB بروتوكول SSH أو HTTPS — يمكن للمهندس إختبار اتصال HTTPS. تسقط قواعد iptables APIC حركة المرور عبر SSH أو HTTPS ولكن لا يمكنه الاتصال بصمت.
- تقييد IP المصدر في عامل تصفية عقد خارج النطاق — يحد عامل تصفية العقد من الوصول إلى شبكات فرعية مصدر معينة. لا يمكن للمهندسين خارج هذه الشبكة الفرعية الاتصال.

التحقق من تكوين AAA

انتقل إلى admin > AAA > المصادقة > AAA.



تأكيد ما يلي:

- نطاق المصادقة الافتراضي — يحدد أي مجال تسجيل الدخول يتم إستخدامه عندما لا يحدد المستخدم مجال تسجيل دخول. إذا تم تعيينها على مجال تسجيل دخول AAA بعيد، فيجب أن يكون الخادم المتوافق قابلا للوصول.
- نطاق مصادقة وحدة التحكم — للتحكم في الوصول إلى وحدة التحكم. في حالة التعيين إلى محلي، يستخدم تسجيل الدخول إلى وحدة التحكم بيانات الاعتماد المحلية دائما (مستحسن).

التحقق من مجالات تسجيل الدخول

انتقل إلى Admin > AAA > المصادقة > مجالات تسجيل الدخول.

```
<#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
```

تحقق من وجود مجال تسجيل الدخول المستخدم للمصادقة ومن أنه يشير إلى مجموعة الموفر الصحيحة.

التحقق من موفري TACACS+

انتقل إلى admin > AAA > المصادقة > TACACS+ > موفري TACACS+.

```
<#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
```

التحقق من موفري RADIUS

انتقل إلى Admin > AAA > المصادقة > RADIUS > موفرو RADIUS.

```
<#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
```

التحقق من موفري LDAP

انتقل إلى Admin > AAA > المصادقة > LDAP > موفري LDAP.

<#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
```

أخطاء تكوين AAA الشائعة

- ACI TACACS+ على تكوينه تم الذي المفتاح تطابق الـ — مشترك سري تطابق عدم مع RADIUS أو موفر المفتاح الموجود على الخادم. تفشل المصادقة دون توقف.
- على سبيل المثال (EPG غير صحيح EPG إلى يشير أو فارغًا موفر يكون **epgDn** — خاطئة إدارة EPG APIC يتعذر على OOB). شبكة على الخادم يكون عندما يتردد قاطن النطاق داخل المثال، إلى الوصول إلى الخادم.
- ولكن LDAP ك تسجيل الدخول يتم تكوين مجال تسجيل الدخول غير متطابق — مجال تسجيل الدخول إلى نوع المجالات تسجيل الدخول يجب أن تشير إلى TACACS+ مصادقة يتوقع المستخدم موفر الصحيح.
- مع LDAP مصادقة تفشل. خطأ **basedn** أو (bind DN) **rootdn** الـ — غير صحيح LDAP ربط DN صحيح مستخدم المستخدم اعتمادات بيانات تكون عندما حتى ربط أخطاء تحدث.
- مستخدم، Active Directory ل — الدليل مخطط مع LDAP تصفية عامل تطابق ال **sAMAccountName=$userid**. ل OpenLDAP، استخدم **cn=$userid** أو **uid=$userid**.

التحقق من تكوين RBAC

انتقل إلى Admin > AAA > Users لعرض حسابات المستخدمين المحليين والمجال الأمان الخاص

بمه تاناييعتو راودألا.

استعمال مجالات الأمان عبر واجهة برمجة التطبيقات:

<#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
```

يتمتع المستخدم المعين للمجال all with role admin بحق الوصول الكامل للقراءة والكتابة إلى البنية بأكملها. يمكن لمستخدم تم تعيينه إلى مجال أمان مخصص له دور Tenant-admin إدارة المستأجرين المقترنين بذلك المجال فقط.

الشائعة RBAC التكوينات الخاطئة

- المستخدم الذي تم إنشاؤه بدون مجال أمان — يمكن للمستخدم تسجيل الدخول ولكن لا يرى أي مستأجرين ويستلم "403 ممنوع" على كائنات API. يجب تعيين مجال أمان واحد على الأقل.
- تم تعيين دور للقراءة فقط عند الحاجة إلى الوصول للكتابة — يمكن للمستخدم عرض الكائنات ولكن لا يمكنه إرسال التغييرات. تحقق من تعيين امتياز الدور إلى writePriv.
- RADIUS أو +TACACS مفقود من خادم AAA — يرجع خادم المستخدم البعيد دون تعيين **cisco-av-pair** السمة التي تحتوي على **shell:domains=all/admin/**. تتم مصادقة المستخدم بنجاح ولكن ليس له أدوار ولا يمكنه رؤية أي شيء في البنية.

استكشاف أخطاء تسجيل الدخول خارج النطاق وإدارة النطاق وإصلاحها

إذا لم يكن APIC أو IP الخاص بإدارة المحول يمكن الوصول إليه على الشبكة، فعليك التحقق من HTTPS أو SSH قبل استكشاف أخطاء مسار الإدارة وإصلاحها أو AAA.

السيناريو: يتعذر إختبار اتصال APIC OOB IP

المشكلة: يتعذر على محطة الإدارة إختبار اتصال عنوان IP الخاص بإدارة APIC OOB.

خطوات التحقق:

1. تحقق من أن منفذ إدارة APIC متصل ماديا وأن الارتباط قيد التشغيل.
2. تحقق من أن محطة الإدارة موجودة على نفس مقطع L2 أو أنها تحتوي على مسار إلى الشبكة الفرعية OOB.
3. تحقق من تعيين IP الخاص بإدارة OOB بشكل صحيح:

<#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. تحقق من التقصير لخدم reachable:

<#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. البروتوكولات المطلوبة، تحقق من أنه يسمح بالبروتوكولات المطلوبة. إذا تم تطبيق عقد خارج "التحقق من العقود في قسم "التحقق من العقود كما هو موضح في قسم العقود الذي يقدم EPG OOB من الاستعلام عن النطاق". يتم فرض عقود OOB كقواعد **iptables** على APIC. يمكنك عرض القواعد المحفوظة من طبقة APIC:

<#root>

```
apic1#

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

في العقد، فإن البروتوكول المطلوب هو قاعدة ACCEPT والتوجد قاعدة DROP هو الإدخال إذا كان هناك حركة المرور بتصفية موقع (OOB) النطاق خارج.

ملاحظة: يتطلب الأمر **iptables -L -n** لعرض قواعد kernel المباشر الوصول إلى الجذر وهو غير متوفر لجلسات عمل SSH للمستخدمين العادية.

السبب الجذري: عنوان إدارة OOB مفقود أو غير مكون بشكل صحيح أو عبارة غير صحيحة أو

حركة مرور تصفية عقد OOB.

الحل: قم بتصحيح تعيين عنوان خارج النطاق (OOB) أو التحقق من مسار الشبكة الفعلي أو تحديث عقد خارج النطاق (OOB) للسماح بالبروتوكولات المطلوبة.

السيناريو: لا يمكن الوصول إلى IP الإدارة للمحول

المشكلة: يمكن الوصول إلى APIC ولكن لا يمكنها الوصول إلى محول عبر الوصول لإدارة OOB.

خطوات التحقق:

1. تحقق من أن المحول يحتوي على عنوان OOB تم تعيينه: <#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. تحقق من أن واجهة إدارة المحول تحتوي على عنوان IP المعين: <#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. تحقق من مسار VRF للإدارة: <#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
```

السبب الجذري: تعيين عنوان OOB مفقود، عبارة غير صحيحة، أو المنفذ المادي للإدارة معطل.

الحل: قم بتعيين عنوان OOB تحت المستأجرين > الإدارة > عناوين إدارة العقد. تحقق من أن إرتباط الإدارة الفعلية قيد التشغيل.

أستكشاف أخطاء وصول SSH وإصلاحها

يغطي هذا القسم السيناريوهات التي يمكن فيها الوصول إلى عنوان IP الخاص بالإدارة مصادقة. (يتجح إختبار الاتصال) ولكن فشل جلسة SSH في إنشاء أو

السيناريو: تم رفض اتصال SSH

المشكلة: يبلغ عميل SSH عن "رفض الاتصال" عند الاتصال ب APIC أو المحول.

خطوات التحقق:

1. تحقق من تمكين بروتوكول SSH في نهج الوصول إلى الإدارة:
<#root>

apic1#

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

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

إذا تم **adminSt** تعطيل إتصالات SSH، فسيتم رفض إتصالات SSH.

2. تحقق من إستخدام المنفذ الصحيح. إذا تم تغيير منفذ SSH من 22:
<#root>

$

ssh -p

custom-port

admin@10.1.1.1

3. تحقق من أن عقد OOB يسمح ب TCP على منفذ SSH. يرجى الرجوع إلى قسم "التحقق من العقود خارج النطاق".

السبب الجذري: تم تعطيل SSH في نهج الوصول إلى الإدارة أو المنفذ المخصص غير المعروف للعميل أو تصفية العقد خارج النطاق (OOB).

الحل: قم بتمكين SSH في سياسة الوصول إلى الإدارة أو استخدم المنفذ الصحيح.

السيناريو: فشل تبادل مفتاح SSH (عدم تطابق KEX أو تشفير)

المشكلة: فشل عميل SSH مع "لم يتم العثور على تشفير مطابق"، أو "لم يتم العثور على طريقة تبادل مفاتيح مطابقة"، أو "لم يتم العثور على MAC مطابق".

خطوات التحقق:

1. تحقق من إخراج المطبعة الاحتياطية لعميل SSH لتحديد الخوارزميات التي يقدمها العميل:
<#root>

```
$

ssh -vv admin@10.1.1.1

debug2: KEX algorithms: curve25519-sha256,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1
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. قارن بين الخوارزميات التي يقدمها العميل والخوارزميات التي يتم تكوينها بواسطة 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-nistp384,ecdl
sshMacs      : hmac-sha2-256,hmac-sha2-256-etm@openssh.com,hmac-sha2-512
hostkeyAlgos : rsa-sha2-256,rsa-sha2-512,ssh-ed25519
```

3. تعرف على التقاطع. في حالة عدم وجود خوارزمية شائعة في أي فئة، تفشل المصافحة.

ملاحظة: في الإصدار 5.2(1) من واجهة التحكم في الوصول (ACI) والإصدارات الأحدث، تم تحسين شفرة SSH وخوارزميات KEX الافتراضية. الخوارزميات القديمة، مثل **diffie-hellman-group1-sha1** ،**diffie-hellman-group14-sha1** ،**aes128-cbc** و**hmac-sha1** لم تعد تقدم بشكل افتراضي. إذا قمت بالترقية مؤخرا، فتحقق من عدم اعتماد عملاء SSH في بيئتك للإعدادات الافتراضية الجديدة.

السبب الجذري: لا يوجد تشفير مشترك أو خوارزمية KEX أو MAC بين عميل SSH و APIC بعد ترقية ACI أو تقوية التشفير.

ةميدقلا ةيمزراوخلا ةفاضإ ةداعإ وأ ،ةثيدحلا تايمزراوخلا معدل SSH ليمع ثيدحتب مق :لحلا
ىلع ارطخ لكشت ةميدقلا تايمزراوخلا ةفاضإ ةداعإ نإ .ةرادإلا ىلإ لوصولا جهن ىلإ ةبولطملا
.ديعبلا ىدملا ىلع اهب ىصوي الو نامألا

نييلحملا نيمدختسملل ةقداصملا لشفت نكلو SSH لصتي :ويرانيسلا

ةملك ضفر متي نكلو (رورملا ةملك ةبلاطم رهظت) SSH لاصتا ديكأت حجني :ةلكشملا
.يلحملا مدختسملل رورملا

:ققحتلا تاوطخ

1. ايلحم مدختسملا دوجو نم ققحت:
<#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. ةدئازلا ةلشافلا لوخدلا ليجست تالواحم ببسب باسحلا نيمأت نم ققحتلا:
<#root>

```
apic1#

moquery -c aaaUserEp

dn                    : uni/userext
pwdStrengthCheck    : no
```

< نامألا ةرادإ < Admin > AAA تحت لوخدلا ليجست لاجم نيمأت ةسايس نم ققحت
.نيمأتلا ةسايس

3. مت اذإ .حيحصلا لوخدلا ليجست لاجم مادختساب مدختسملا لوخد ليجست نم ققحت
ىلع بجيف ،ديعب AAA لوخد ليجست لاجم ىلع يضارتفالا ةقداصملا قاطن نييعت
ةيلحملا ةقداصملا ضرف لجأ نم **apic:fallback\\username** وأ **apic:LOCAL\\username** دادعإلا مدختسملا.

4. ثدحل APIC نم **nginx.bin.log** ققحت .تالجسلا يف ةقداصملا ةجيتن ةحص نم ققحتلا
:لوخدلا ليجست
<#root>

```
apic1#

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

:لوخدلا ليجست ةلواحمل اهنييعت مت يتلا رفوملا ةعومجمو قاطنلا نع ثحبا

```
! 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 to LDA
! The admin user does not exist in the LDAP directory, so the LDAP search returns empty and the login i
||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-Domain
              ||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, filte
||aaa||INFO||LDAP search to server ldap-server.example.com for baseDn CN=Users,DC=example,DC=com, filte
             ||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
```

إذا لم يكن النطاق 0 (إحتياطي/محلي)، فسيتم إرسال تسجيل الدخول إلى خادم AAA بعيد بدلا من قاعدة البيانات المحلية. يجب أن يقوم المستخدم بالإعداد لفرض المصادقة المحلية. **apic:fallback\\username** و **apic:LOCAL\\username**.

السبب الجذري: يتم إرسال كلمة مرور غير صحيحة أو حساب مؤمن أو محاولة تسجيل الدخول بعيد بدلا من قاعدة البيانات المحلية إلى خادم AAA.

الحل: قم بإعادة تعيين كلمة المرور أو إلغاء تأمين الحساب أو أستخدم باديء مجال تسجيل الدخول الصحيحة.

أستكشاف أخطاء وصول HTTPS وإصلاحها

يغطي هذا القسم السيناريوهات التي يتعذر فيها الوصول إلى واجهة برمجة تطبيقات نقل الحالة التمثيلية (REST) الخاصة ب APIC على ويب أو واجهة برمجة تطبيقات نقل الحالة (REST) عبر HTTPS.

السيناريو: انتهت مهلة اتصال HTTPS

المشكلة: يعرض المستعرض "err_connection_timed_out" أو توقف إستدعاء API عند الاتصال ب APIC على المنفذ 443.

خطوات التحقق:

1. تحقق من تمكين HTTPS:

<#root>

```
apic1#

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

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

2.دوقعلا نم ققحتلا" مسقلا ىلإ ةراشإلا ءاجرلا .TCP 443 ب حمسي OOB دقع نأ نم ققحت ةيمحملا ريغ (OOB)".
3. :ءامتسالا وه HTTPS ةيلمع ديكأتل هسفن APIC نم رابتخإ

<#root>

```
apic1#

ss -tlnp | grep 443

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

السبب الجذري: HTTPS لطعم، OOB دقع ييفصي TCP 443، وأ لا nginx ةيلمع ىلع لا APIC تمطحت.

الحل: مق نيكمتب HTTPS يف جهن الوصول ىلإ الإدارة وأ ثيدحت دقع OOB وأ ةداعإ ليغشت ةمدخ بيو ىلع APIC.

السيناريو: ضرعي المستعرض أطخ ةحفاصم TLS

المشكلة: ضرعي المستعرض "err_ssl_version_or_cipher_mismatch" وأ أطخ TLS الثامم.

خطوات التحقق:

1. :ىلع APIC هنيوكت مت يذلا TLS لوكوتورب رادصإ نم ققحت

<#root>

```
apic1#

moquery -c commHttps

sslProtocols : TLSv1.2
```

2.ليبس ىلع) ادج ةميدقلا تاضرعتسملا معدت ال .TLSv1.2 ل ضرعتسملا معد نم ققحت المثال، Internet Explorer 10 هلبق امو) TLSv1.2 يضارتفا لكشب.

السبب الجذري: ضرعت APIC TLSv1.2 (يضارتفالا) طقف ويدعم المستعرض وأ ليمع API

إصدارات TLS القديمة فقط.

الحل: قم بتحديث المستعرض أو العميل. إذا كان يجب عليك دعم العملاء الأقدم وقوات، فقم بإضافة TLSv1.1 إلى نهج الوصول للإدارة، ولكن هذا يقدم مخاطر أمنية.

السيناريو: تقييد تقييد تقييد تقييد تقييد واجهة برمجة التطبيقات

المشكلة: فشل مكالمات REST API بشكل متقطع مع أخطاء HTTP 503 أو تصبح واجهة مستخدم الويب بطيئة أثناء التشغيل التلقائي المكثف.

خطوات التحقق:

```
<#root>

apic1#

moquery -c commHttps

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

إذا كان معدل الكبح منخفض جدا وكانت البرامج النصية للأتمتة ترسل العديد من الطلبات في الثانية، فإن APIC يرفض الطلبات الزائدة.

السبب الجذري: معدل الكبح لكل مستخدم منخفض جدا لأعباء عمل التشغيل التلقائي.

الحل: قم بزيادة معدل الكبح بموجب نهج الوصول للإدارة، أو قم بتحسين برامج التشغيل التلقائي النصية من أجل تقليل تكرار الطلب. بدلا من ذلك، قم بتعطيل التحكم في حالة عدم مشاركة البنية.

أستكشاف أخطاء المصادقة والتفويض والمحاسبة (AAA) وإصلاحها — TACACS+

يغطي هذا القسم حالات فشل مصادقة TACACS+. تتصل APIC بخادم TACACS+ عبر منفذ TCP رقم 49.

التحقق العملي

ةيلمع نم ققحتلل .لقتسملا NX-OS ىلع رفوتملا **test aaa** رمألا ACI تالوحم معدت ال
ءاطخألاو رفوملا ةلاح نم ققحتلل (APIC) تاقيبطتلا ةجمرب ةهجاو مدختسأ ،TACACS+
.لوخدلا ليجست تالواحمو

:TACACS+ رفوم يف ةطشن ءاطخأ دوجو نم ققحت

<#root>

```
apic1#

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

ءاطخألا تناك اذإ .هيلإ لوصولل الباق رفوملا ربتعي APIC نإف ،ءاطخأ ةيأ عاجرإ متي مل اذإ
F1774 وأ (رفوملا ىلإ لوصولا رذعتي) F1773 لثم لاطعألا داوكأ نمضتي جارخإلا نإف ،ةدوجوم
.(ةقداصملا لشف)

:TACACS+ رفوم نيوكت نم ققحت

<#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
```

:TACACS+ مداخ ىلإ APIC نم ةيساسألا ةكبشلا ىلإ لوصولا ةيناكمإ نم ققحت

<#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
```

لواح ليجست لوخدلا ىلإ APIC مادختساب لاجم ليجست لوخدلا ىلإ TACACS+ ددحو ةجيتن

:لمعلا ةسلج

<#root>

```
apic1#

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

يف ةلكشم وأ ةقداصملا ضفر ببسب لشفلا ناك اذإ ام ديدحتل لقحلا **descr** يف ثحبا .لاصتالا

مدختسملا مسا ةيفصت .APIC تالجس يف +TACACS ةقداصم قفدت ةحص نم ققحت :ينعملا

<#root>

```
apic1#

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

عجار) LDAP لثم ةقداصملا **nginx.bin.log** قفدت سفن +TACACS لوخد ليجست تايلمع عبتت يلي اميف .(يقيقحلا لجسلل ةلماك ةلثمأ ىلع لوصحلل LDAP ليغشت نم ققحتلا مسق :ةيسيئرلا قورفلا ل +TACACS

- .(LDAP ل 3 قاطنلا لباقم) +TACACS ىلإ ريشي 2 لاجملا — 2 قاطنلا `DefaultAuthMo` ددحي
- هب لاصتالا متي يذلا +TACACS مداخ ددحي — ةمئاقلا ىلإ `TacacsProvider <ip>` ةفاضإ (مباقم `LdapProvider` ل LDAP).
- مداخ ةطساوب ةرشابم AV جوز عاجرإ متي — `TACACS+ Cisco-avpair (shell:domains=all/admin/)` +TACACS (لباقم متي هليوحت نم ةطيرخ ةعومجم LDAP).

→ ثحب رفوملا → PAM → بلط قاطن ديدحت :مدقتلا سفن حجان +TACACS لوخد ليجست رهظي .لوؤسملا ةباتك تازايتما ← رودلا نييعتو UserDomain ← مدختسملا ← AV جوز ليلحت

هب حرصملا ريغو AAA ةقداصم ءانثأ مدختسملا `<username>` ب لشافلا +TACACS لوخد ليجست يهتني .LDAP ضفر طمن سفن وهو ،AAA مداخ ةقداصم ضفر مت :أطخلا ...

+TACACS ةقداصم تلشف :ويرانيسلا

ليجست لاجم مدختسملا ددحي امدنع "ةقداصملا لشف" عم لوخدلا ليجست لشفي :ةلكشملا

دخول TACACS+.

خطوات التحقق:

1. تحقق من وجود أخطاء نشطة في مورد TACACS+:
<#root>

apic1#

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

أشير الخطأ F1774 إلى رفض المصادقة. أشير الخطأ F1773 إلى وجود مشكلة في الاتصال.

2. تحقق من إمكانية الوصول إلى الشبكة من APIC إلى خادم 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. إذا نجح إختبار الاتصال ولكن فشلت المصادقة، فتحقق من التطابقات السرية المشتركة على كل من تكوين مورد APIC وتكوين خادم TACACS+.
4. تحقق من أحدث جلسات عمل تسجيل الدخول للاطلاع على تفاصيل الفشل:
<#root>

apic1#

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

5. تحقق من سجلات خادم TACACS+ لإجراء محاولة المصادقة. تشير محاولة ناجحة تم تسجيلها على الخادم ولكن تم رفضها إلى وجود مشكلة في تكوين المستخدم على جانب الخادم (على سبيل المثال، عدم تطابق كلمة المرور أو فقدان حساب المستخدم).
6. تحقق من APIC **nginx.bin.log** للحصول على تدفق المصادقة الكامل. التصفية حسب اسم المستخدم بدلا من كلمات أساسية محددة حتى لا يتم فقد الرسائل الوسيطة:
<#root>

apic1#

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

قارن الناتج بالنماذج العملية وغير العاملة في قسم التحقق التشغيلي أعلاه.
المؤشرات الرئيسية:

- تم الوصول إلى خادم TACACS+ ولكنه رفض بيانات الاعتماد. — تم رفضه أو تم رفضه

تحقق من وجود المستخدم على الخادم ومن تطابق كلمة المرور.

- يتعذر الوصول إلى الخادم — TacacsProvider لا توجد رسائل خاصة بالمزود بعد إضافة TacacsProvider. تحقق من قابلية الوصول إلى الشبكة و EPG للإدارة. أو انتهت مهلته.
- نجحت المصادقة — متبوعة بخطوط فحص الدور تم إكمال عملية حقن المستخدم البعيد ولكن يمكن أن تكون المشكلة مع تعيين الدور (راجع قسم زوج AV أدناه).

RBAC ل Cisco من AV-زوج TACACS+

بالنسبة للمستخدمين البعيدين الذين تمت مصادقتهم عبر TACACS+، يجب على الخادم إرجاع **cisco-av-pair** السمة في استجابة التخويل. تقوم هذه السمة بتعيين المستخدم إلى مجالات أمان ACI وأدواره.

التنسيق:

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

الأمثلة:

- المسؤول الكامل: **shell:domains=all/admin/**
- للقراءة فقط للجميع: **shell:domains=all/read-all/**
- مسؤول المستأجر لمجال محدد: **shell:domains=TenantA/tenant-admin/**
- مجالات متعددة: **shell:domains=all/admin/,TenantA/tenant-admin/**

إذا كانت هذه السمة مفقودة أو غير مكونة بشكل صحيح، تتم مصادقة المستخدم بنجاح، ولكن ليس له أي أدوار ولا يمكنه رؤية أي كائنات في واجهة مستخدم APIC.

ملاحظة: يتطلب وصول SSH إلى المحولات والوحدة الرئيسية دور المسؤول مع امتيازات الكتابة في مجال all security. الحد الأدنى لزوج الصوت/الفيديو للوصول إلى SSH للمحول هو **shell:domains=all/admin/**. يمكن للمستخدمين الذين لديهم أدوار غير إدارية (على سبيل المثال، read-all، tenant-admin، aaa) أو المستخدمين الذين تم تعيينهم في مجال أمان بخلاف all تسجيل الدخول إلى واجهة برمجة التطبيقات (APIC) ولكن يتم رفض وصول SSH إلى المحولات. يظهر سجل APIC على المسؤول غير الدخول تسجيل رفض المحول لهؤلاء المستخدمين.

تحقق من صحة زوج AV الذي تم استلامه عن طريق التحقق **nginx.bin.log**. اسم بحث التصفية المستخدم لعرض تدفق حقن الدور بالكامل:

<#root>

apic1#

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

رهظت TACACS+ Cisco-avpair (shell:domain=..). ك AV جوز ليجست متي ،TACACS+ ىلإ ةبسنلاب Admin و Found UserDomain اعوبتم هلامكإ مت <username> ديعبلا مدختسملا نقح نأ ةحجان نقح ةيلمع اذه نم ةلماك ةلثمأ ىلع لوصحلل LDAP ليغشت نم ققحتلا مسق عجار) write privileges lines يقيقح لجس جارخإ عم قفدتلا).

مدختسملل <username> تانايب نقح ةيلمع لجسلا ضرعيسف ،حلاص ريغ AV جوز قيسنت ناك اذإ ةقداصملاب مدختسملا ماق اذإ .ةحلاص ريغ shell:domain string يه أطخلا ةلاسر - تلشف يتلا ديعبلا لوحملا ىلع لوؤسم ريغ لوخد ليجست عم تالوحملا ىلإ SSH ضفر متي ،لوؤسم ريغ رود مادختساب.

السبب الجذري: مدع قباطت يرس كرتشم وأ مداخ رذعتي لوصولا هيلإ نم ةكبش وأ ةرادإلا نأ وأ TACACS+ مداخ ىلع دوجوم ريغ مدختسملا EPG الخاص بالإدارة على الموفر غير صحيح.

الحل: مق حيحصتب رسلا كرتشملا وأ حالصإ ةيناكمإ لوصولا وأ ءاشنإ مدختسملا ىلع مداخ TACACS+.

ققحتلا نم ةحص تالجس ةقداصم لوحم قرولا

نم لك يف SSH لوخد ليجست ثادحأ ليجست متي ،يسيئرلا دومعلاو ةقرولا تالوحم يف **pam.module.log** و **nginx.log**. ضرعت **pam.module.log** ةجيتن ةقداصم PAM (ضفر وأ لوبق). يوتحي **nginx.log** على تدفق AAA الكامل — تحديد النطاق، بحث الموفر، اتصال LDAP/TACACS+/RADIUS، ليلحت جوز AV، ويعتين الدور — قباطم **nginx.bin.log** امل وه دوجوم يف APIC. قبطنت هذه على سجلات جميع أنواع AAA البعيدة (TACACS+، RADIUS، LDAP).

ققحتلا **pam.module.log** نم ةجيتن ةقداصملا:

<#root>

leaf101#

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

لوحملا ىلع ةحجان دعب نع ةقداصم — لمعلا:

```
||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 groupid=15374
||pam||INFO||returning success
```

remote=1 دكؤت ةمالعلا نأ مدختسملا تمت دق ةقداصم نم لبق مداخ AAA ديعب.

يلحم لواحي حاتفملاو لمعتسملا securityMgrAG لا ركني .مدختسملا ضفر مت — لمعي لا يئاهن يطايتحإك ثحب لمعتسم:

```
||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
```

دق SSH لاصتا نوكي نأ لمتحملا نمف ،قالطإلا ىلع مدختسملل PAM تالاخدإ ةيأ رهظت مل اذإ ريفشتلا قباطت مدع ببسب ،لاثملا ليبس ىلع) PAM ةلحرم ىلإ لوصولا لبق هضفر مت لاصتالا ءاغلإب مدختسملا مايق وأ).

اذه يوتحي .**nginx.log** ققحت ،لوحملا ىلع ةقداصملا قفدتل اليصفت رثكأ ضرع ىلع لوصحلل **nginx.bin.log** ةدوجوملا لئاسرلاو قيسنتلا سفن — ةلماكلا AAA تارارق ةلسلس ىلع لجسلا يف APIC:

<#root>

```
leaf101#

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

ققحتلا مسق يف APIC LDAP ةلثمأب ةنراقم) ام لوحم ىلع ةحجانلا LDAP ةقداصم — لمعلا نم ليغشت LDAP — لئاسرلا يه اهسفن):

```
||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
```

.ببسلا حرشي ال هنكلو ضفر راهظإ **pam.module.log** دنع صاخ لكشب اديفم **nginx.log** لوحملا نوكي LDAP ثحب عجرأ ،لاثملا ليبس ىلع) ددحمو دوزملاو AAA لشف ببس نع nginx.log فشكي AV). جوز نقح لشف وأ ،+TACACS ةلهم ،ةغراف ةميق

RADIUS — اهحالصإو AAA ءاطخأ فاشكتسأ

UDP ذفنم ربع RADIUS مداخب APIC لصتت .RADIUS ةقداصم لشف تالاح مسقلا اذه يطغي .ايرايتخإ (ةبساحملا) 1813 UDP ذفنمو (ةقداصملا) 1812

التحقق العملي

ةيلاتلا قرطلا مدختسأ. لقتسملا NX-OS ىلع رفوتملا **test aaa** رمألا ACI تالوحم معدت ال .RADIUS ةيلمع نم ققحتلل

:يفرط لوحم نم هيلإ لوصولا ةيناكمإو RADIUS مداخ نيوكت تايئاصحإ نم ققحت

<#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
```

السيناريو: فشل مصادقة RADIUS

المشكلة: يفشل تسجيل الدخول عندما يحدد المستخدم مجال تسجيل الدخول إلى RADIUS.

خطوات التحقق:

1. أو المهلة انتهاءات العالمات على التعرف للمحول من RADIUS خادم تايئاصحإ نم قحقت الفشل:
<#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
```

غير قابل RADIUS خادم أن إلى انتهاء المهلة تحت الكبير العدد يشير إلى الطلبات التي انتهت مهلتها إلى أن خادم RADIUS غير قابل للوصول أو أن السر المشترك غير متطابق (يوقم RADIUS بإسقاط الحزم بصمت على السر المشترك غير مطابق).

2. تحقق من إمكانية الوصول إلى الشبكة إلى خادم 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. تحقق من التطابقات السرية المشتركة بين APIC وخادم RADIUS. وعلى عكس TACACS+ الذي يستخدم بروتوكول TCP ويبلغ عن حالات فشل الاتصال، يستخدم RADIUS بروتوكول UDP ويقوم بإسقاط الحزم بصمت عندما يكون السر المشترك غير متطابق. العرض الوحيد هو المهلة.
4. (radiusd -X) الأخطاء تصحيح وضع في FreeRADIUS يعرض .RADIUS خادم سجلات من تحقق سري طلب كل ويشير إلى ما إذا كان قد تم قبوله أو رفضه لديه عدم تطابق سر مشترك.
5. تحقق من nginx.bin.log APIC لتدفق مصادقة RADIUS. التصفية حسب اسم المستخدم:
<#root>

```
apic1#

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

لثم ةقداصملا قفدت **nginx.bin.log** سفن RADIUS ىلإ لوخدلا ليجست تايلمع عبتت LDAP و TACACS+ ‏(راجع قسم التحقق من تشغيل LDAP للحصول على أمثلة كاملة على السجل الحقيقي). فيما يلي الفروق الأساسية ل RADIUS:

- وأ `TacacsProvider` لباقم) RADIUS مداخ ددحي — `ةمئاقلا ىلإ <IP> RadiusProvider ةفاضإ` `LdapProvider`).
- .نيوكتلا بسح RADIUS ل قاطنلا مقر فلتخي

`تازايتملا` لامكإ `مت دقو ... ديعبلا مدختسملا نقحب` RADIUS ىلإ حاجنلا لوخدلا ليجست يهتني `.لوؤسملل ةباتكلا`

`.ضفرو AAA ةقداصم ءانثأ ضفر عم` لشافلا RADIUS لوخد ليجست يهتني

مداخلا ةلهم نوكت `،RadiusProvider ةفاضإ` رطس دعب RADIUS ب ةصاخ لئاسر يأ رهظت مل اذإ لشف تالاح نع غلبيو TCP لوكوتورب مدختسي يذلا TACACS+ سكع ىلعو .ةيهتنم نوكي امدنع تمصب مزحلا طاقسإب موقيو UDP لوكوتورب RADIUS مدختسي ،لاصتالا .راكنإلا اهعبتي يتلا ةلهملا وه ديحولا ضرعلاو .قباطتم ريغ كرتشملا رسلا

6. :RADIUS رفوم يف ةطشن ءاطخأ دوجو نم ققحتلا

<#root>

```
apic1#

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

جوز RADIUS Cisco-AV ل RBAC

مداخ عجري نأ بجي .RBAC رود نييعتل TACACS+ ةمس **cisco-av-pair** سفن RADIUS مدختسي :لوصولا لوبق ةباجتسإ يف ةمسلا هذه RADIUS

<#root>

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


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

في FreeRADIUS، متي اذه نيوكت يف فلملا وأ **users** ةيفلخلا LDAP. ةبسنلاب ىلإ ISE، متي .ةمدقتم ةمسك ليوختلا فيرعت فلم نمض اهنيوكت

تالاح يف ببستي — RADIUS عم اعويش رثكألا) كرتشم يرس قباطت مدع :يرذجلا ببسلا وأ ،حيحص ريغ ةقداصم ذفنم وأ ،مداخلا ىلإ لوصولا رذعتي وأ ،(ةتماصلا ةلهملا ءاهتنا .RADIUS مداخ ىلع مدختسملا باسح دقتفي

الحل: صحح ال تححص ال يشراك رس، دقق udp 1812 reachability، وأ شكلت المستعمل على ال RADIUS لداني.

LDAP — وإصلاحها AAA استكشاف أخطاء

389 منفذ TCP عبر LDAP بخادم APIC يتصل .LDAP مصادقة فشل حالات القسم هذا يغطي (LDAP) أو منفذ TCP 636 (LDAPs مع SSL).

التحقق العملي

ال تعدم حوالت ACI الأمر **test aaa** المتوفر على NX-OS المستقل. للتحقق من عملية LDAP، تحقق من أخطاء المورد والتكوين من APIC.

التحقق من وجود أخطاء نشطة في موفر LDAP:

<#root>

```
apic1#

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

يشير العطل F1777 إلى وجود مشكلة في الاتصال. يشير الخطأ F1778 إلى المصادقة أو إليه. فإن APIC يعتبر المورد القابل للوصول إليه. إذا لم يتم إرجاع أية أخطاء، فشل الربط.

التحقق من إمكانية الوصول إلى الشبكة الأساسية لخادم 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
```

بالنسبة ل LDAP، تحقق أيضا من اتصال TCP بالمنفذ 389 (أو 636 ل LDAPs). إذا كان بإمكان APIC اختبار الاتصال بالخادم مع استمرار أخطاء LDAP، فإن المشكلة تكون عادة DN ربط غير صحيح أو كلمة مرور خاطئة أو جدار حماية يمنع منفذ LDAP.

تحقق من صحة تدفق مصادقة LDAP في سجلات APIC. التصفية حسب اسم المستخدم:

```
<#root>

apic1#

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

العمل — يظهر تسجيل دخول LDAP بنجاح تدفق البحث الكامل والربط وتعيين الأدوار:

```
||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
```

لا يعمل — لم يتم العثور على المستخدم في دليل LDAP (يقوم البحث بإرجاع مجموعة فارغة):

```
||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
```

السيناريو: فشلت مصادقة LDAP

المشكلة: يفشل تسجيل الدخول عندما يحدد المستخدم مجال تسجيل دخول LDAP.

خطوات التحقق:

1. التحقق من إمكانية الوصول إلى خادم LDAP من 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. التحقق من وجود أخطاء نشطة في موفر LDAP:
<#root>

```
apic1#

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

3. التحقق من تكوين موفر 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. تحقق من وجود المستخدم في دليل LDAP ضمن DN الأساسي الذي تم تكوينه. بالنسبة لـ Active Directory، يجب أن تتطابق سمة **sAMAccountName** مع اسم المستخدم الذي تم إدخاله عند تسجيل الدخول. بالنسبة لـ OpenLDAP، يجب أن تكون السمة **uid** أو **cn** مطابقة.
5. إذا تم تمكين SSL، فتحقق من سلسلة الشهادات (منفذ 636) إذا كنت تستخدم LDAPs، فسترفض APIC الاتصال إذا لم تكن شهادة الخادم موثوقًا بها أو انتهت صلاحيتها. تحقق من **SSLValidationLevel** وتعيينها على مستوى مقبول.
6. تحقق من **nginx.bin.log** من APIC للحصول على تدفق مصادقة LDAP الكامل. يتم فقد الرسائل الوسيطة ما لم يتم تحديد اسم المستخدم:
<#root>

```
apic1#

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

قارن الناتج بالنماذج العملية وغير العاملة في قسم التحقق التشغيلي أعلاه.
يمكن العثور على أنماط فشل إضافية خاصة ب LDAP من خلال البحث في السجل بشكل عام:

<#root>

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

هالعأ ةدراولا تايلمعلا نم ققحتلا ةلثمأب نراق) ةلماعلا ريغ ةعئاشلا طامنألا لمالكا قفدتلل):

```
! 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, 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
```

أنماط فشل LDAP الأخرى للبحث عنها:

- لوصولل لباقلا ريغ ذفنملا وأ ةيامحلا رادج رظح ذفنم) LDAP ثحب ةلهم تهتنا (389/636 وأ ءيطب وأ مداخلا إلى — لشف البحث عن LDAP: رمز الإرجاع ل `ldap_search_ext_s: -5:` انتهت المهلة
- (لاصتالا مداخلا ضفر وأ ،ةحيحص ريغ طبر رورم ةملك وأ ردصم مسا) طبرلا لشف LDAP مداخب لاصتالا رذعتي `ldap_search_ext_s: -1:` ل عاجرإلا زمر :LDAP نع ثحبلا لشف —
- ةملك لشف عم طبرلا) ةحيحص ريغ رورملا ةملك نكلو مدختسملا ىلع روثعلا مت ةلاسر ەعبتي نكلو LDAP Record DN رطس لجسلا رهظي — (مدختسملا رورم رطس ..UserDN ب طبر نودب ةضوفرم حجان.

ةعومجم ةطيرخ LDAP ل RBAC

ةمس **attribute** LDAP رفوم لقح ددحي .ةمسلا **cisco-av-pair** نم الدب ةعومجملا طئارخ LDAP مدختسي ةداع اذه نوكي ،Active Directory ةمدخل ةبسنلاب .ةعومجملا تامولعم ىلع يوتحت يتلا LDAP **memberOf.**

مت يتلا LDAP ةعومجم ةطيرخ دعاوق لباقم اهعاجرإ مت يتلا ةعومجملا DN عم APIC قباطتي قباطت مدع ةلاح يف .نيبسانملا رودلاو نامألا لاجم نييعتل (**aaaLdapGroupMapRule**) اهنيوكت .راودأ هيدل سيل نكلو ةقداصمب مدختسملا موقي ،ةعومجم نييعت ةدعاق.

ةرشابم /**shell:domains=all/admin** نيزختو **CiscoAVPair** ىلإ ةميقلا **attribute** طبض كنكمي ،كلذ نم الدب تامس يف LDAP الخاصة ةصاخلا مدختسملاب ،يتلاو عبتت سفن قيسنت TACACS+ و RADIUS.

السبب الجذري: DN وأ ةملك رورم طبرلا ريغ ةحيحص ،الو يوتحي DN الأساسي على ةحص نم ققحتلا لشف وأ ،ليلدلا ططخم عم ثحبلا ةيفصت لماع قباطتي الو ،مدختسملا ةداهش LDAP، وأ دعاوق نييعت ةعومجملا ةدوقفملا.

الحل: قم بتصحيح تكوين الموفر (ربط DN و DN الأساسي و عامل التصفية و SSL).
بالنسبة لمشاكل RBAC، تحقق من مطابقة قواعد خريطة المجموعة لمجموعات LDAP التي ينتمي إليها المستخدم.

أستكشاف أخطاء RBAC وامتيازات المستخدم وإصلاحها

يغطي هذا القسم السيناريوهات التي يقوم فيها المستخدم بالمصادقة بنجاح ولكنه لا يملك مستوى الوصول المتوقع.

السيناريو: المستخدم الذي قام بتسجيل الدخول ولكنه لا يرى أي مستأجرين

المشكلة: يقوم المستخدم البعيد بتسجيل الدخول عبر بروتوكول TACACS+ أو RADIUS أو LDAP. ينجح تسجيل الدخول، ولكن المستخدم لا يرى أي مستأجرين في مكالمات واجهة برمجة التطبيقات يعيدون نتائج فارغة أو "403 ممنوع" أو واجهة المستخدم.

خطوات التحقق:

1. تحقق من جلسة عمل المستخدم لمعرفة الأدوار التي تم تعيينها عند تسجيل الدخول:
<#root>

apic1#

```
moquery -c aaaSessionLR -x 'query-target-filter=wcard(aaaSessionLR.descr,"jsmith")' -x 'order-by=aaaSess
```

```
                dn          : subj-[uni/userext/remoteuser-jsmith]/sess-123456789
             descr       : [user jsmith] From-10.1.1.100-client-type-https-Success
```

يعرض الحقل descr نتيجة تسجيل الدخول. إذا تمت مصادقة المستخدم بنجاح ولكن cisco-av-pair صالح لمجموعة LDAP خريطة تطابق يرجع لم AAA خادم فإن ،RBAC أدوار لديه ليس وأ LDAP.

2. تحقق من APIC nginx.bin.log للاطلاع على زوج AV وتعيين الدور أثناء تسجيل الدخول.
التصفية حسب اسم المستخدم:
<#root>

apic1#

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

ابحث عن رسائل حقن الدور وتعيين المجال:

العمل — زوج AV محول من خريطة مجموعة LDAP، يحصل المستخدم على دور المسؤول:

```
||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
```

AAA مداخ نإف ،قفدتلا يف **Converted to CiscoAVPair** وأ **Cisco-avpair** رطس رهظي مل اذإ — لمعي ال **Checking all UserDomains** اهنع ثحبا .LDAP ةعومجم ةطيرخ ةدعاق قباطتت ملو ةمسلا عجري مل هيدل سيل نكلو مدختسملا ةقداصم تمت — اهعباتت دونب **Found UserDomain** نودب ريغ AV جوز ةلسلس قيسنت نإف ،ةلاسرلا **Injection ... data FAILED** ترهظ اذإ .راودأ تانييعت حيحص.

3. ةعومجم ةيوضع وأ (RADIUS وأ TACACS+ ل) ةمسلل **cisco-av-pair** AAA مداخ ءاجرإ نم ققحت LDAP الصحيحة (ل LDAP). ققحت نم نيوكت مداخ AAA:
   - TACACS+: ققحت نم نيمضت فلم فيرعت المستخدم **cisco-av-pair** قيسنتلاب **shell:domains=all/admin/.**
   - RADIUS: ققحت نم تاعجترم فلم فيرعت المستخدم **Cisco-AVPair = "shell:domains=all/admin/"** يف Access-Accept.
   - LDAP: ققحت نم أن المستخدم عضو يف ةعومجم LDAP التي قباطت ةدعاق ةطيرخ ةعومجم LDAP (**aaaLdapGroupMapRule**) التي مت اهنيوكت.
4. ةقباطم نم ققحت ،لوصولا قح كلمي ال مدختسملا لازي ال نكلو ةدوجوم ةمسلا تناك اذإ APIC: ىلع دوجوم نامأ لاجمل ةمسلا يف نامألا لاجم مسا
<#root>

```
apic1#

moquery -c aaaDomain
```

إذا كانت المراجع **cisco-av-pair** ريشت إلى لاجم ريغ دوجوم (ىلع ليبس المثال، **shell:domains=NonExistentDomain/admin/**)، نإف نييعت رودلا لشفي تمصب.

السبب الجذري: ال يرجع مداخ AAA تامس نييعت RBAC، وأ نوكي قيسنت السمة ريغ حيحص، وأ نأ ريشت السمة إلى لاجم نامأ ريغ دوجوم ىلع APIC.

الحل: مق بتكوين مداخ AAA إلرجاع نييعت المجموعة **cisco-av-pair** وأ الصحيح. ققحت نم دوجو لاجم نامألا ىلع APIC.

السيناريو: يمكن للمستخدم عرض التكوين ولكن ال يمكنه تعديله

المشكلة: يمكن للمستخدم تسجيل الدخول وتصفح الكائنات ولكنه يستلم أخطاء عند محاولة إرسال التغييرات.

خطوات التحقق:

1. تحقق من تعيينات دور المستخدم:
<#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. تتضمن الأدوار التي تمنح writePriv، الكتابة والوصول إلى حاجب المستخدم إذا كان المستخدم ذات امتيازات الكتابة admin وtenant-admin وaccess-admin وfabric-admin.
3. اسم المستخدم: تحقق من صحة تعيين الدور في سجلات APIC. التفصيلية حسب
<#root>

```
apic1#

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

المصادقة تفيد من نهاية بالقرب من الدور تعيين رسائل عن ابحث:

للعمل — دور المستخدم للكتابة للمسؤول (من تسجيل دخول LDAP حقيقي):

```
||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
```

امتيازات بدلا من القراءة بامتيازات المسؤول غير UserRole يظهر السجل كان إذا — لم يعمل الكتابة للمسؤول، فإن المستخدم لديه دور للقراءة فقط ولا يمكنه تعديل التكوين.
ابحث عن سطر مثل:

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

إذا كان السجل يظهر امتيازات القراءة فقط وبدون امتيازات الكتابة، قم بتحديث دور المستخدم أو زوج التوصل/الفيديو على خادم AAA.

السبب الجذري: للمستخدم دور للقراءة فقط (على سبيل المثال، read-all أو ops) بدلا من دور يمكنه الكتابة.

الحل: قم بتحديث تعيين دور المستخدم على APIC (للمستخدمين المحليين) أو قم

بتحديث خادم AAA cisco-av-pair (للمستخدمين البعيدين) لتضمين دور له امتيازات الكتابة.

السيناريو: يستطيع المستخدم الوصول إلى بعض المستأجرين دون الآخرين

المشكلة: يستطيع المستخدم رؤية مستأجر واحد وإدارته ولكنه لا يستطيع رؤية مستأجر آخر، حتى ولو كانوا بحاجة إلى الوصول.

خطوات التحقق:

1. تحقق من تعيين مجال أمان المستخدم:
```
apic1# <#root>

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. تعيين مجالات الأمان إلى المستأجرين. إذا كان المستخدم بحاجة إلى الوصول إلى TenantB، فيجب أيضا تعيينه إلى مجال الأمان المقترن ب TenantB، أو تعيينه إلى مجال all.
3. بالنسبة للمستخدمين عن بعد، قم بتأكيد زوج AV أو خريطة مجموعة LDAP التي تقوم بتعيين المجالات الصحيحة. تحقق من APIC nginx.bin.log لتعيين المجال عند تسجيل الدخول. التصفية حسب اسم المستخدم:
```
apic1# <#root>

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

العمل — يتلقى المستخدم المجال بأكمله (إمكانية الرؤية الكاملة)، من تسجيل دخول LDAP الحقيقي:

```
||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 admin
```

لا يعمل — إذا كان لدى المستخدم مجال مستأجر واحد فقط، يظهر هذا المجال فقط في Found UserDomain TenantA، على سبيل المثال. تحتاج المستخدم إلى مجالات إضافية تمت إضافتها إلى زوج AV على خادم AAA، أو مجال all للوصول الكامل.

السبب الجذري: يتم تعيين المستخدم إلى مجال أمان مقيد يغطي مستأجرين محددين فقط.

الحل: قم بإضافة مجالات الأمان المطلوبة إلى تكوين المستخدم، أو أستخدم مجال all للوصول الكامل.

إسترداد كلمة المرور والوصول إلى الطوارئ

إذا تم تأمين جميع حسابات المسؤولين أو كان خادم AAA البعيد غير قابل للوصول وتم تغيير النطاق الافتراضي، فاستخدم أحد أساليب الاسترداد التالية:

مجال تسجيل الدخول الاحتياطي

توفر واجهة التحكم في الوصول (ACI) مجال تسجيل دخول إحتياطي مضمن يستخدم المصادقة المحلية دائما، بغض النظر عن نطاق المصادقة الافتراضي. لاستعماله:

- برتوكول النقل الآمن (SSH): قم بتسجيل الدخول باسم **apic:fallback\\admin** (أو **apic#fallback\\admin** حسب الإصدار).
- GUI: في القائمة المنسدلة المجال على شاشة تسجيل الدخول، حدد إحتياطي واستخدم بيانات الاعتماد المحلية.

الوصول إلى وحدة التحكم

إذا تم تعيين نطاق مصادقة وحدة التحكم على محلي (الافتراضي)، يمكنك دائما تسجيل الدخول عبر منفذ وحدة تحكم APIC باستخدام بيانات الاعتماد المحلية. إذا كانت كلمة مرور المسؤول المحلي غير معروفة، يمكن إعادة ضبط كلمة المرور من خلال وحدة التحكم في الإدارة المتكاملة (CIMC) من Cisco (لواجهات برمجة التطبيقات المادية) أو وحدة تحكم برنامج hypervisor (لواجهات برمجة التطبيقات الظاهرية).

ملاحظة: إذا تم تغيير نطاق مصادقة وحدة التحكم إلى خادم AAA بعيد ويتعذر الوصول إلى هذا الخادم، فسيفشل أيضا الوصول إلى وحدة التحكم. هذا هو سيناريو الإغلاق الشائع. الاحتفاظ دائما بمجال مصادقة وحدة التحكم الذي تم تعيينه على محلي.

مرجع الأخطاء الشائعة

عادة ما تكون أخطاء قائمة التحكم في الوصول (ACI) التالية مرتبطة بالوصول عن بعد ومشكلات AAA:

- F1773 — مشكلة في اتصال موفر TACACS+. يتعذر على APIC الوصول إلى خادم TACACS+.
- F1774 — فشل مصادقة TACACS+. يمكن الوصول إلى الخادم ولكنه رفض محاولة المصادقة.
- F1775 — مشكلة في اتصال موفر RADIUS.
- F1776 — فشل مصادقة RADIUS.
- F1777 — مشكلة في اتصال موفر LDAP.
- F1778 — فشل مصادقة LDAP.
- F0532 — لم يتم تكوين الشبكة الفرعية للإدارة لعقدة.

الاستعلام عن أخطاء AAA النشطة:

<#root>

apic1#

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

المراجع

- — اهالصإو ةيساسألا تامدخلاو (ACI) لوصولا يف مكحتلا ةمئاق ةرادإ عاطخأ فاشكتسأ PODسايسات
- ةرادإلا — (x)6.1 رادصإلا ،Cisco APIC ل يساسألا نيوكتلا ليلد
- ةبقارملاو ةقداصملاو لوصولا — Cisco نم تاقيبطتلا ةمجرب ةهجاو نامأ نيوكت ليلد

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).