

Firepower Xsible Operating System (FXOS) 2.2: ماساب اراصتخا فورعمل (ماظن دعب نع ةرادال ل لك يهلا ضي وفت/ة ق داصم RADIUS مادختساب

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [تهيئة هيكل FXOS](#)
- [تكوين خادم ISE](#)
- [التحقق من الصحة](#)
- [التحقق من هيكل FXOS](#)
- [التحقق من ISE 2.0](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة RADIUS والتحويل لهيكل نظام التشغيل القابل للتشغيل (FXOS) عبر محرك خدمات الهوية (ISE).

يتضمن هيكل FXOS أدوار المستخدم التالية:

- المسؤول - وصول كامل للقراءة والكتابة إلى النظام بالكامل. يتم تعيين هذا الدور بشكل افتراضي لحساب المسؤول الافتراضي ولا يمكن تغييره.
 - للقراءة فقط - وصول للقراءة فقط إلى تكوين النظام بدون امتيازات لتعديل حالة النظام.
 - العمليات - الوصول للقراءة والكتابة إلى تكوين NTP، والتكوين الذكي ل Call Home للترخيص الذكي، وسجلات النظام، بما في ذلك خوادم syslog والأعطال. قراءة الوصول إلى باقي النظام.
 - الوصول إلى المصادقة والتفويض والمحاسبة (AAA) - وصول للقراءة والكتابة إلى المستخدمين والأدوار وتكوين المصادقة والتفويض والمحاسبة (AAA). قراءة الوصول إلى باقي النظام.
- يمكن ملاحظة ذلك عبر واجهة سطر الأوامر (CLI) على النحو التالي:

دور العرض # *FPR4120-TAC-A /security

الدور:

اسم الدور Priv

— —
aaa aaa

مسؤول

عمليات العمليات

للقراءة فقط

تمت المساهمة من قبل توني ريميريز، خوسيه سوتو، مهندسي TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة نظام التشغيل (FXOS) (Firepower Xsible)
- معرفة تكوين ISE

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان Cisco Firepower 4120، الإصدار 2.2

- Virtual Cisco Identity Services Engine 2.2.0.470

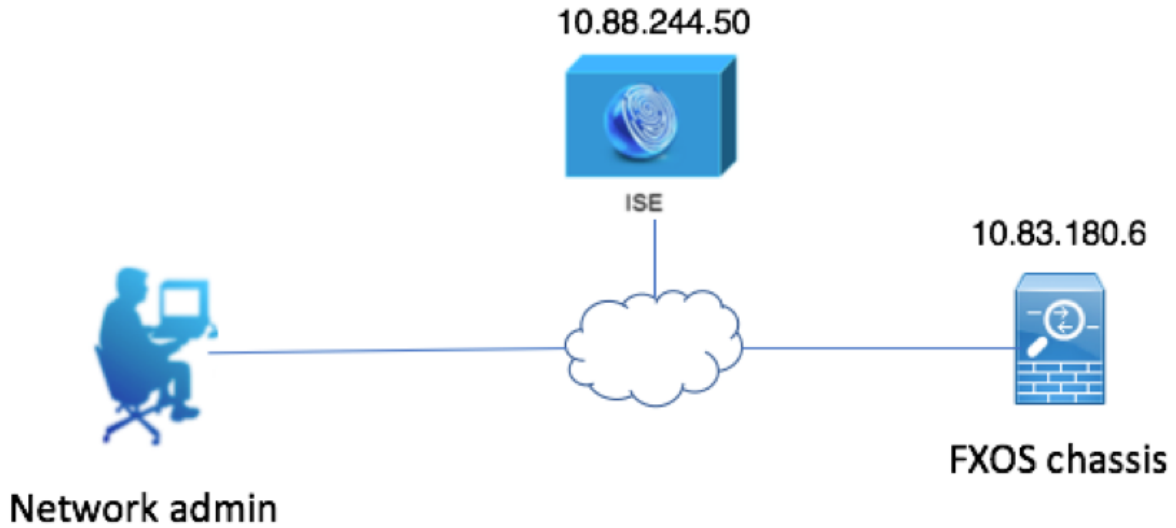
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الهدف من التكوين هو:

- مصادقة المستخدمين الذين يقومون بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) المستندة إلى الويب و SSH باستخدام ISE
- السماح للمستخدمين بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) المستندة إلى الويب و SSH القائمة على FXOS وفقاً لدور المستخدم الخاص بهم من خلال ISE.
- التحقق من التشغيل السليم للمصادقة والتفويض على FXOS باستخدام ISE

الرسم التخطيطي للشبكة



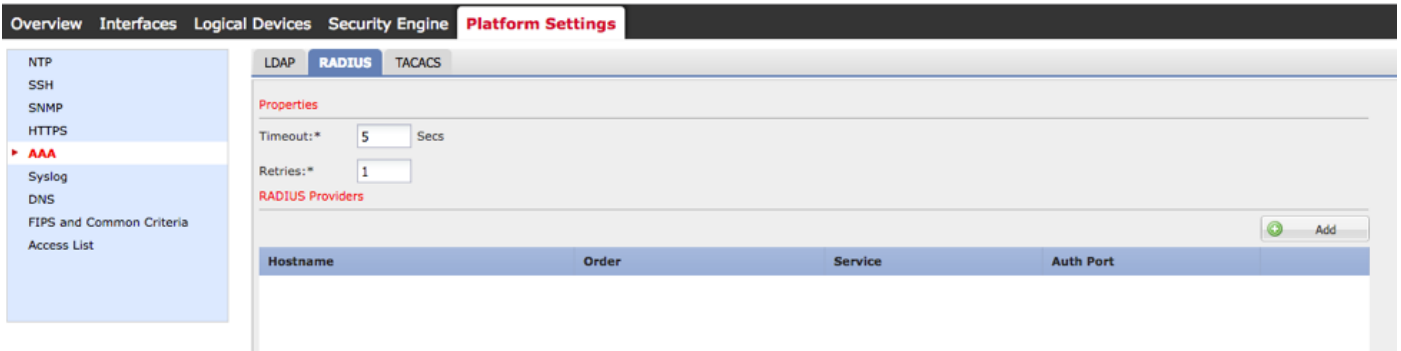
التكوينات

تهيئة هيكل FXOS

إنشاء موفر RADIUS باستخدام Chassis Manager

الخطوة 1. انتقل إلى إعدادات النظام الأساسي < AAA.

الخطوة 2. انقر فوق علامة التبويب RADIUS.



الخطوة 3. لكل موفر RADIUS تريد إضافته (حتى 16 موفرا).

3.1 في منطقة موفري RADIUS، انقر فوق إضافة.

3.2 بمجرد فتح شاشة إضافة مزود RADIUS، قم بإدخال القيم المطلوبة.

3.3 انقر فوق موافق لإغلاق مربع الحوار إضافة موفر RADIUS.

Edit 10.88.244.50

Hostname/FQDN(or IP Address):* 10.88.244.50

Order:* 1

Key: Set: Yes

Confirm Key:

Authorization Port:* 1812

Timeout:* 5 Secs

Retries:* 1

OK Cancel

الخطوة 4. طقطقة حفظ.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
▶ **AAA**
Syslog
DNS
FIPS and Common Criteria
Access List

LDAP **RADIUS** TACACS

Properties

Timeout:* 5 Secs

Retries:* 1

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.50	1	authorization	1812

Save Cancel

الخطوة 5. انتقل إلى النظام < إدارة المستخدم > إعدادات.

الخطوة 6. تحت المصادقة الافتراضية أختار RADIUS.

Overview Interfaces Logical Devices Security Engine Platform Settings

System Tools Help frosadmin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: RADIUS *Local is fallback authentication method

Console Authentication: Local

Remote User Settings

Remote User Role Policy: Assign Default Role No-Login

إنشاء موفر RADIUS باستخدام CLI (واجهة سطر الأوامر)

الخطوة 1. لتمكين مصادقة RADIUS، قم بتشغيل الأوامر التالية.

#FPR4120-TAC-A أمان النطاق

FPR4120-TAC-A /security # scope default-auth

FPR4120-TAC-A /security/default-auth # set مجال

الخطوة 2. أستخدم الأمر **show detail** لعرض النتائج.

FPR4120-TAC-A /security/default-auth تفاصيل العرض

المصادقة الافتراضية:

مجال الإدارة: **RADIUS**

النطاق التشغيلي: **RADIUS**

فترة تحديث جلسة ويب (بالثواني): 600

مهلة جلسة العمل (بالثواني) للويب و ssh و telnet جلسات: 600

مهلة جلسة العمل المطلقة (بالثواني) للويب و SSH و telnet جلسات: 3600

مهلة جلسة عمل وحدة التحكم التسلسلية (بالثواني): 600

مهلة الجلسة المطلقة لوحدة التحكم التسلسلية (بالثواني): 3600

مجموعة خوادم مصادقة المسؤول:

مجموعة خوادم المصادقة التشغيلية:

إستخدام العامل الثاني: لا

الخطوة 3. لتكوين معلمات خادم RADIUS، قم بتشغيل الأوامر التالية.

#FPR4120-TAC-A أمان النطاق

FPR4120-TAC-A /security # radius

FPR4120-TAC-A /security/radius # الخادم 10.88.244.50 يدخل

FPR4120-TAC-A /security/radius/server # مجموعة ISE Server "DESCR"

FPR4120-TAC-A /security/radius/server # مفتاح المجموعة

أدخل المفتاح: *****

تأكيد المفتاح: *****

الخطوة 4. أستخدم الأمر **show detail** لعرض النتائج.

FPR4120-TAC-A /security/radius/server # تفاصيل العرض

خادم RADIUS:

اسم المضيف أو FQDN أو عنوان IP: 10.88.244.50

إدارة الحقوق:

الطلب: 1

منفذ المصادقة: 1812

المفتاح: ***

المهلة: 5

تكوين خادم ISE

إضافة كمورد شبكة

الخطوة 1. انتقل إلى إدارة < موارد الشبكة > أجهزة الشبكة.

الخطوة 2. طقطة يضيف

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded, showing 'Network Resources' and 'Device Portal Management'. The 'Network Resources' menu is further expanded to show 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' page is active, displaying a table with columns for Name, IP/Mask, Profile Name, Location, Type, and Description. The table is currently empty, with the text 'No data available' displayed below it. The left sidebar shows 'Network devices', 'Default Device', and 'Device Security Settings'.

الخطوة 3. أدخل القيم المطلوبة (الاسم وعنوان IP ونوع الجهاز وتمكين RADIUS وإضافة المفتاح)، انقر فوق إرسال.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings

DTLS Required

Shared Secret

CoA Port

Issuer CA of ISE Certificates for CoA

إنشاء مجموعات الهوية والمستخدمين

- الخطوة 1. انتقل إلى إدارة < إدارة الهوية < مجموعات < مجموعات هوية المستخدم.
- الخطوة 2. انقر فوق إضافة (Add).

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

Endpoint Identity Groups

User Identity Groups

User Identity Groups

Edit Add Delete Import Export

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

الخطوة 3. أدخل قيمة الاسم وانقر فوق إرسال.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC. The sub-menu is: Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups > New User Identity Group'. It features a form with a 'Name' field containing 'FXOS ADMIN' and an empty 'Description' field. There are 'Submit' and 'Cancel' buttons at the bottom.

الخطوة 4. كرر الخطوة 3 لجميع أدوار المستخدم المطلوبة.

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC. The sub-menu is: Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups'. It features a toolbar with 'Edit', '+ Add', 'X Delete', 'Import', and 'Export'. Below the toolbar is a table with columns 'Name' and 'Description'. The table contains the following rows:

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Employee	Default Employee User Group
FXOS AAA	
FXOS ADMIN	
FXOS OPER	
FXOS Read Only	
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group

الخطوة 5. انتقل إلى إدارة < إدارة الهوية < هوية < مستخدمون.

الخطوة 6. انقر فوق إضافة (Add).

The screenshot shows the Cisco ISE Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main menu includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat Centric NAC. The sub-menu is: Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The left sidebar shows 'Users' with a search bar and a tree view containing 'Latest Manual Network Scan Results'. The main content area is titled 'Network Access Users'. It features a toolbar with 'Edit', '+ Add', 'Change Status', 'Import', 'Export', 'Delete', and 'Duplicate'. Below the toolbar is a table with columns: Status, Name, Description, First Name, Last Name, Email Address, User Identity Groups, and Admin. The table is empty, displaying 'No data available'.

الخطوة 7. أدخل القيم المطلوبة (الاسم ومجموعة المستخدمين وكلمة المرور).

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

Name: fxosadmin

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

Enable Password:

User Information

First Name:

Last Name:

Account Options

Description:

Change password on next login:

Account Disable Policy

Disable account if date exceeds: 2018-03-01 (yyyy-mm-dd)

User Groups

FXOS ADMIN

الخطوة 8. كرر الخطوة 6 لجميع المستخدمين المطلوبين.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

Edit Add Change Status Import Export Delete Duplicate

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	fxosaaa					FXOS AAA	
<input type="checkbox"/> Enabled	fxosadmin					FXOS ADMIN	
<input type="checkbox"/> Enabled	fxosoper					FXOS OPER	
<input type="checkbox"/> Enabled	fxosro					FXOS Read Only	

إنشاء ملف تعريف التحويل لكل دور مستخدم

الخطوة 1. انتقل إلى السياسة < عناصر السياسة < النتائج < التفويض < ملفات تخصيص التفويض.

Standard Authorization Profiles
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Name	Profile	Description
Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensu
Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA port
NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisionir
Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
DenyAccess		Default Profile with access type as Access-Reject
PermitAccess		Default Profile with access type as Access-Accept

الخطوة 2. قم بتعبئة كل السمات لملف تعريف التحويل.

2.1. قم بتكوين اسم ملف التعريف.

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile: Cisco

2.2. في إعدادات السمات المتقدمة، قم بتكوين زوج Cisco-AV التالي

"cisco-av-pair=shell:roles="admin"

Advanced Attributes Settings

Cisco:cisco-av-pair = shell:roles="admin"

2.3. انقر فوق حفظ.

Save Reset

الخطوة 3. كرر الخطوة 2 لأدوار المستخدم المتبقية باستخدام أزواج Cisco-AV التالية

"cisco-av-pair=shell:roles="aaa"

"cisco-av-pair=shell:roles="operations"

"cisco-av-pair=shell:roles="read-only"

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="aaa" - +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="operations" - +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="read-only" - +

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionarys > Conditions > Results

Authentication

Authorization

Authorization Profiles

Downloadable ACLs

Profiling

Posture

Client Provisioning

Standard Authorization Profiles

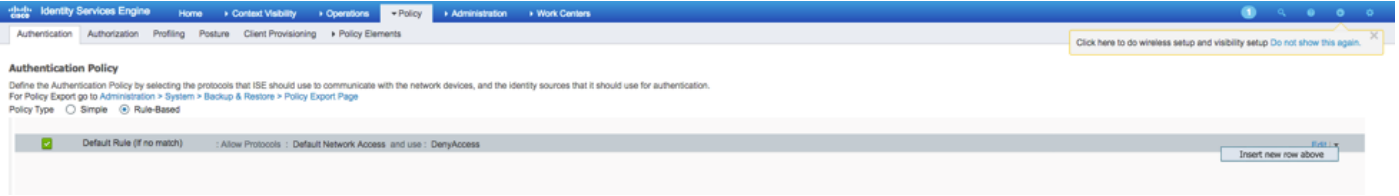
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Edit + Add Duplicate Delete

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco
<input type="checkbox"/>	Cisco_IP_Phones	Cisco
<input type="checkbox"/>	Cisco_WebAuth	Cisco
<input type="checkbox"/>	FXOS-AAA-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ADMIN-PROFILE	Cisco
<input type="checkbox"/>	FXOS-OPER-PROFILE	Cisco
<input type="checkbox"/>	FXOS-ReadOnly-PROFILE	Cisco

إنشاء سياسة المصادقة

الخطوة 1. انتقل إلى سياسة < مصادقة > وانقر فوق السهم المجاور للتحريك حيث تريد إنشاء القاعدة.



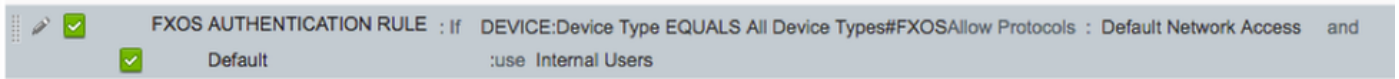
الخطوة 2. الإعداد بسيط، ويمكن تنفيذه بدقة أكبر، ولكن لهذا المثال سنستخدم نوع الجهاز:

الاسم: قاعدة مصادقة FXOS

إذا حددت سمة/قيمة جديدة: الجهاز: نوع الجهاز يساوي جميع أنواع الأجهزة #FXOS#

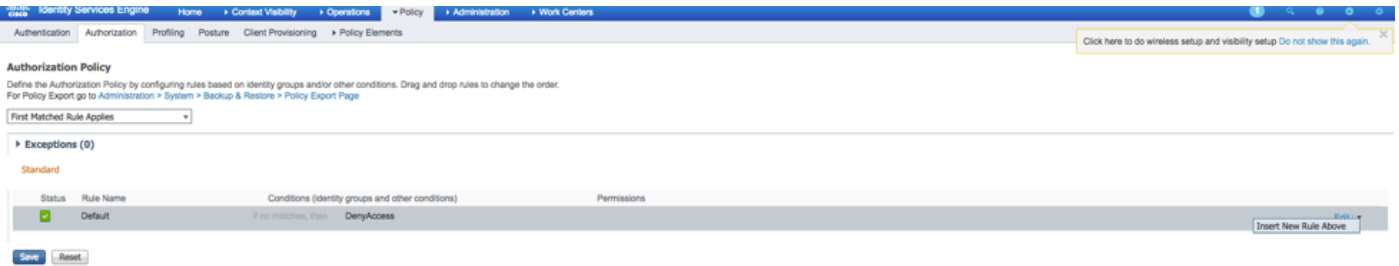
السماح بالبروتوكولات: الوصول الافتراضي إلى الشبكة

الاستخدام: المستخدمون الداخليون



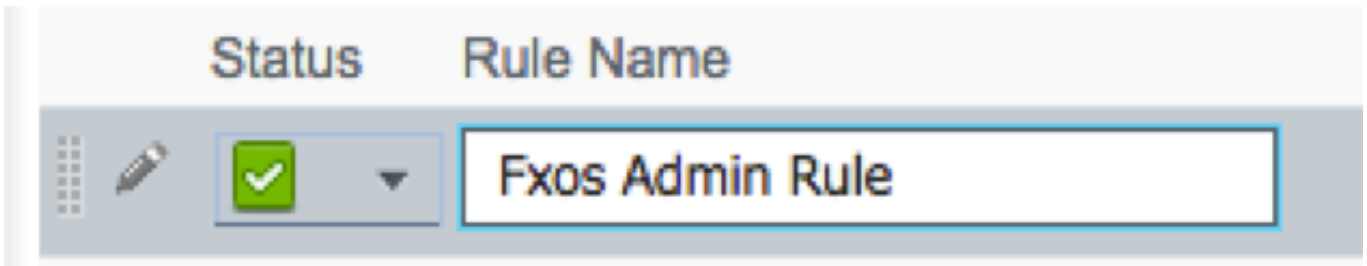
إنشاء نهج التحويل

الخطوة 1. انتقل إلى نهج < تحويل > وانقر فوق شبكة الأسهم لتحريك المكان الذي تريد إنشاء القاعدة فيه.

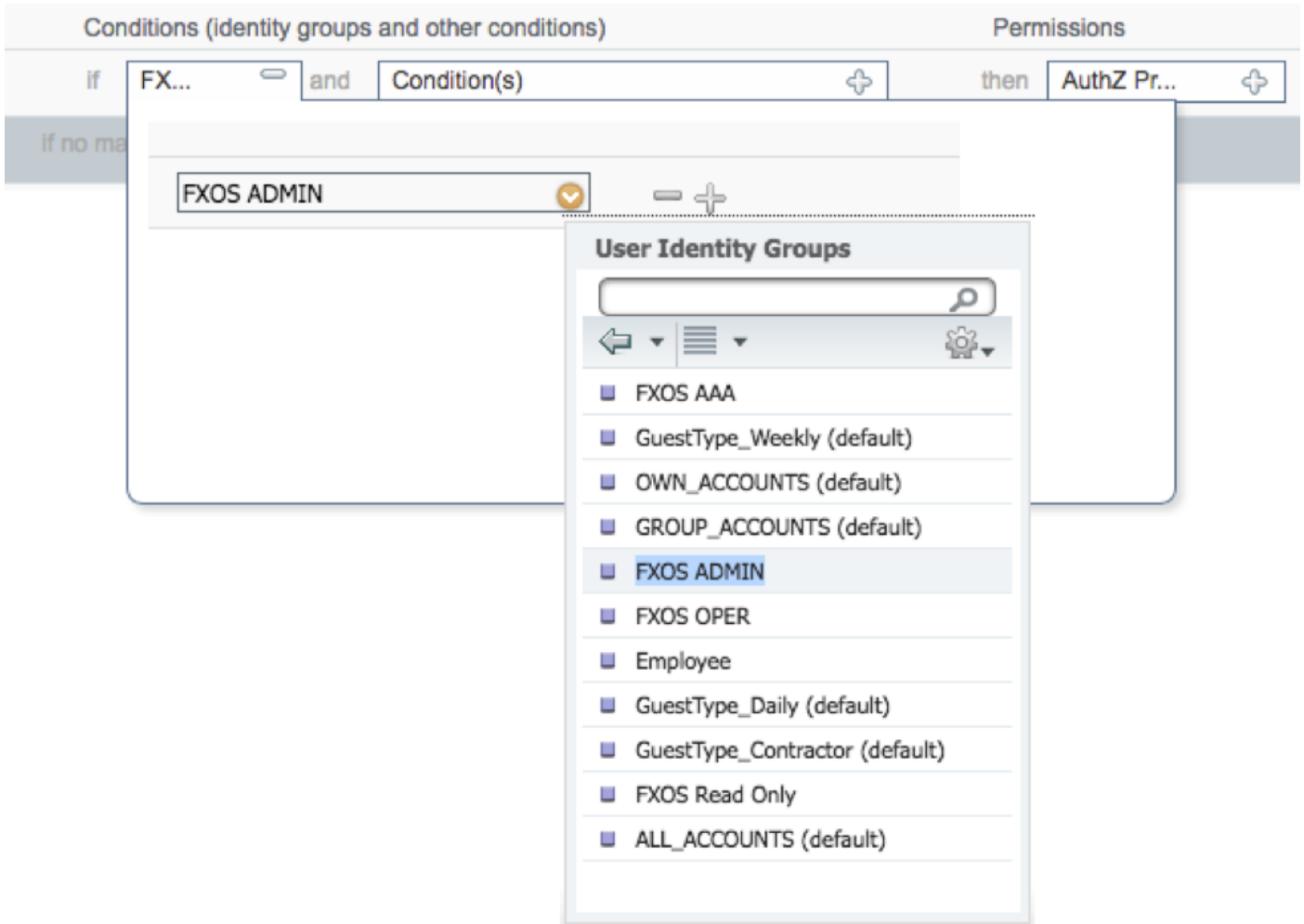


الخطوة 2. أدخل قيم قاعدة التحويل مع المعلومات المطلوبة.

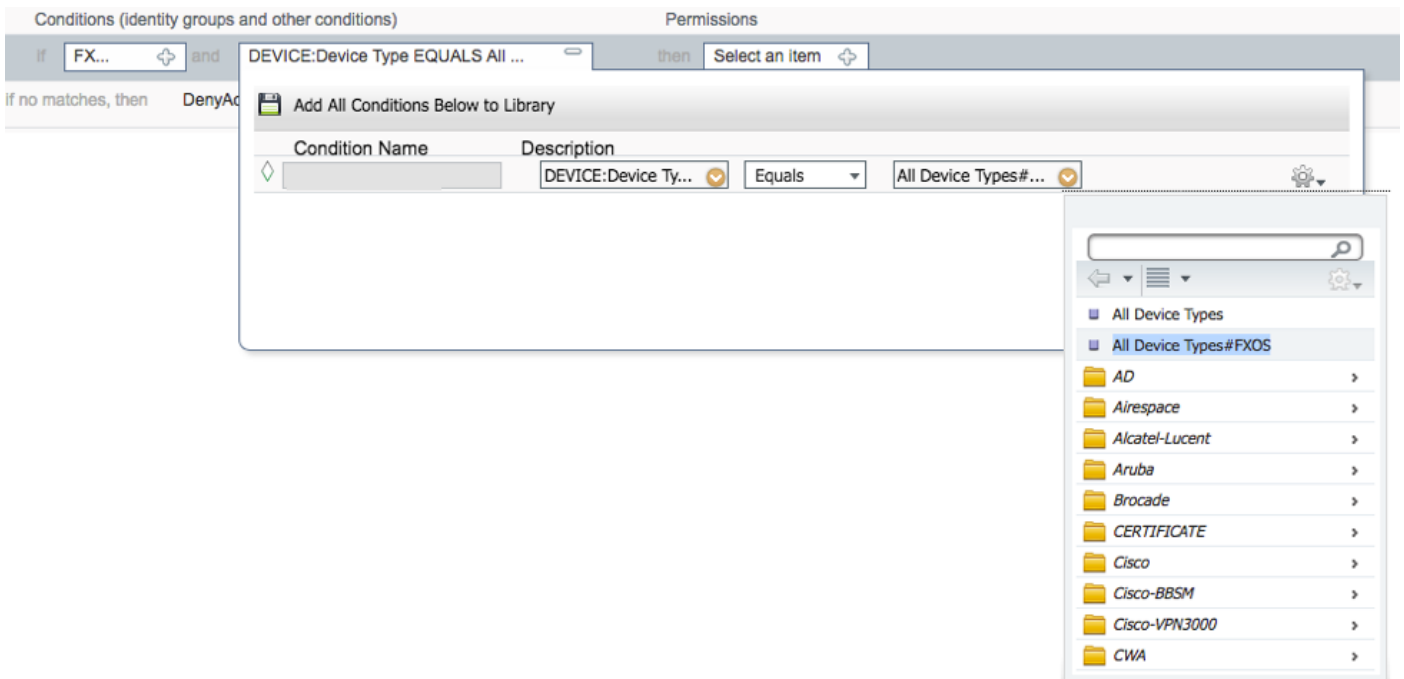
2.1. اسم القاعدة: قاعدة > fxos > USER ROLE.



2.2. إذا: مجموعات هوية المستخدم < تحديد > دور المستخدم.<



2.3. و: إنشاء شرط جديد < الجهاز: نوع الجهاز يساوي جميع أنواع الأجهزة #FXOS.



2.4. الأذونات: قياسي < إختيار ملف تعريف دور المستخدم

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

Standard

- Blackhole_Wireless_Access
- Cisco_IP_Phones
- Cisco_WebAuth
- DenyAccess
- FXOS-AAA-PROFILE
- FXOS-ADMIN-PROFILE**
- FXOS-OPER-PROFILE
- FXOS-ReadOnly-PROFILE
- NSP_Onboard
- Non_Cisco_IP_Phones
- PermitAccess

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE

الخطوة 3. كرر الخطوة 2 لجميع أدوار المستخدمين.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Fxos Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ADMIN-PROFILE
✓	Fxos AAA Rule	if FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-AAA-PROFILE
✓	Fxos Oper Rule	if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-OPER-PROFILE
✓	Fxos Read only Rule	if FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then FXOS-ReadOnly-PROFILE
✓	Default	if no matches, then DenyAccess	

الخطوة 4. انقر فوق حفظ في أسفل الصفحة.

Save

Reset

التحقق من الصحة

يمكنك الآن إختبار كل مستخدم والتحقق من دور المستخدم المعين.

التحقق من هيكل FXOS

1. Telnet أو SSH إلى هيكل FXOS وتسجيل الدخول باستخدام أي من المستخدمين الذين تم إنشاؤها على ISE.

اسم المستخدم: fxosadmin

كلمة المرور:

أمان النطاق #FPR4120-TAC-A #أمان النطاق

FPR4120-TAC-A /security # إظهار تفاصيل المستخدم عن بعد

المستخدم البعيد fxosaaa:

الوصف:

أدوار المستخدم:

الاسم: AAA

الاسم: للقراءة فقط

المستخدم البعيد fxOsadmin:

الوصف:

أدوار المستخدم:

الاسم: المسؤول

الاسم: للقراءة فقط

المستخدم البعيد fxosoper:

الوصف:

أدوار المستخدم:

الاسم: العمليات

الاسم: للقراءة فقط

المستخدم البعيد fxosro:

الوصف:

أدوار المستخدم:

الاسم: للقراءة فقط

حسب اسم المستخدم الذي تم إدخاله، لن تعرض واجهة سطر الأوامر (CLI) الخاصة بهيكل FXOS إلا الأوامر المصرح بها لدور المستخدم المعين.

دور مستخدم المسؤول.

؟ # FPR4120-TAC-A /security

نصح

مسح جلسات المستخدم لجلسات عمل المستخدم

إنشاء كائنات تتم إدارتها

حذف حذف كائنات مدارة

تعطيل الخدمات

تمكين الخدمات

إدخال كائن مدار

النطاق يغير الوضع الحالي

تعيين قيم الخاصة

إظهار معلومات النظام

إنهاء جلسات عمل CIMC النشطة

FPR4120-TAC-A#connect fxos

FPR4120-TAC-A (fxos)# debug aaa-requests

?(fpr4120-TAC-A (fxos

دور مستخدم للقراءة فقط.

؟ # FPR4120-TAC-A /security

النطاق يغير الوضع الحالي

تعيين قيم الخاصة

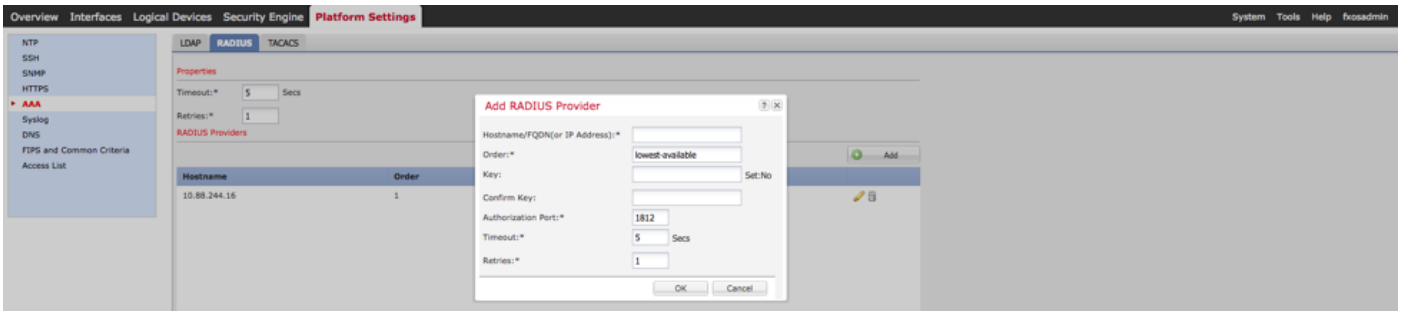
إظهار معلومات النظام

FPR4120-TAC-A#connect fxos

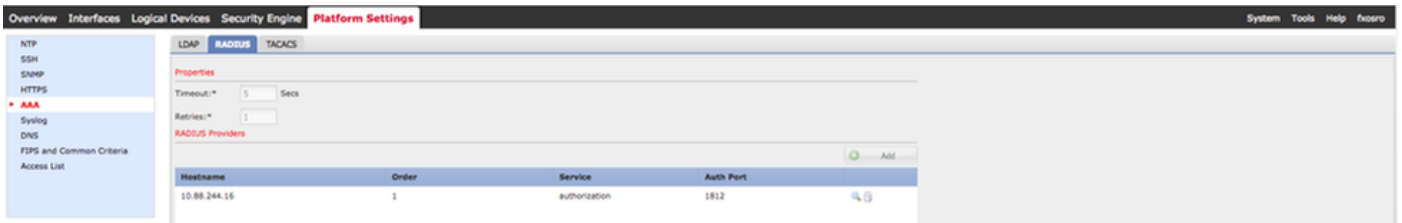
FPR4120-TAC-A (fxos)# debug aaa-requests

٪ الإذن المرفوض للدور

2. تصفح إلى عنوان IP الخاص بهيكل FXOS ودخول باستخدام أي من المستخدمين الذين تم إنشاؤها على ISE.
دور مستخدم المسؤول.



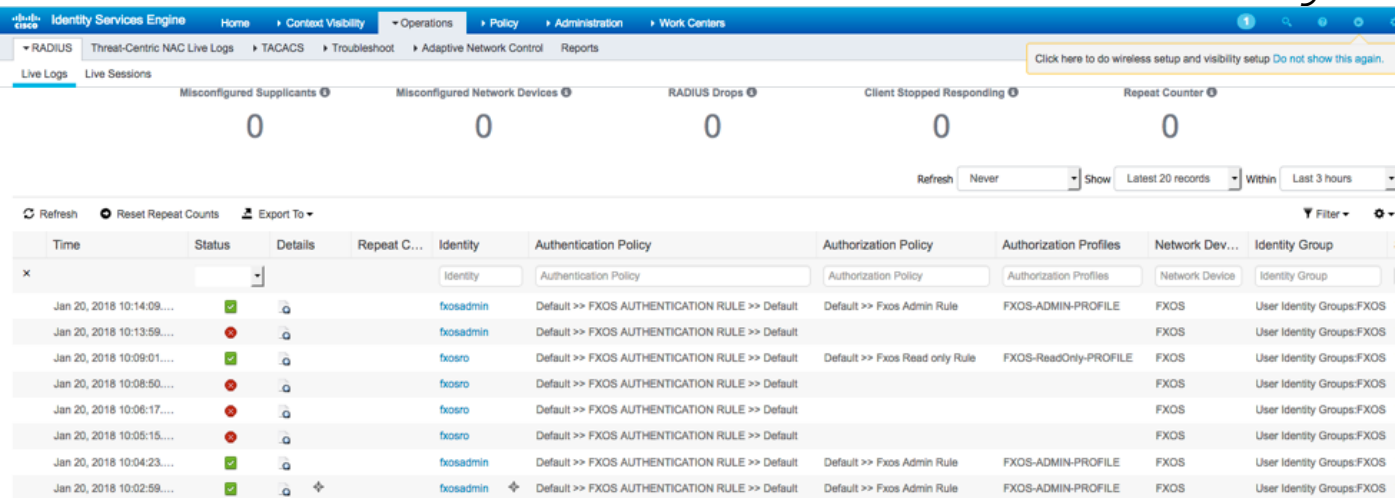
دور مستخدم للقراءة فقط.



ملاحظة: لاحظ أن الزر ADD مصقول.

التحقق من ISE 2.0

1. انتقل إلى العمليات < RADIUS > السجلات المباشرة. يجب أن تكون قادرا على رؤية المحاولات الناجحة والفاشلة.



استكشاف الأخطاء وإصلاحها

من أجل تصحيح أخطاء مصادقة AAA والتفويض عنها، قم بتشغيل الأوامر التالية في واجهة سطر الأوامر (CLI) لـ FXOS.

```
FPR4120-TAC-A#connect fxos
```

```
FPR4120-TAC-A (fxos)# debug aaa-requests
```

```
FPR4120-TAC-A (fxos)#debug aaa الحدث
```

```
أخطاء تصحيح الأخطاء (FPR4120-TAC-A (fxos)#
```

```
FPR4120-TAC-A (fxos)# term mon
```

بعد محاولة المصادقة الناجحة، سترى الإخراج التالي.

```
2018 يناير 20 17:18:02.410275 aaa: aaa_req_process للجلسة رقم 0
```

```
2018 يناير 20 17:18:02.410297 aaa: aaa_req_process طلب AAA عام من التطبيق: تسجيل الدخول إلى التطبيق_subtype: الافتراضي
```

```
2018 يناير 20 17:18:02.410310 aaa: try_next_aaa_method
```

```
2018 يناير 20 17:18:02.410330 aaa: إجمالي الطرق التي تم تكوينها هو 1، الفهرس الحالي الذي يجب تجربته هو 0
```

```
2018 يناير 20 17:18:02.410344aaa: handle_req_using_method
```

```
2018 يناير 20 17:18:02.410356 aaa: aaa_method_server_group
```

```
2018 يناير 20 17:18:02.410367 aaa: aaa_sg_method_handler group = radius
```

```
2018 يناير 20 17:18:02.410379 aaa: استخدام sg_protocol الذي تم تمريره إلى هذه الدالة
```

```
2018 يناير 20 17:18:02.410393 aaa: إرسال الطلب إلى خدمة RADIUS
```

```
2018 يناير 20 17:18:02.412944 aaa: mts_send_msg_to_prot_daemon طول الحمولة = 374
```

```
2018 كانون الثاني/يناير 20: 17:18:02.412973 aaa: الجلسة: 0x8dfd68c مضافة إلى جدول الجلسة 1
```

```
2018 يناير 20 17:18:02.412987 aaa: تم تكوين مجموعة الطرق بنجاح
```

```
2018 يناير 20 17:18:02.656425 aaa: aaa_process_fd_set
```

```
2018 يناير 20 17:18:02.656447 aaa: aaa_process_fd_set: mtscallback على aaa_q
```

```
2018 يناير 20 17:18:02.656470 aaa: mts_message_response_handler: إستجابة MTS
```

```
2018 يناير 20 17:18:02.656483 aaa: prot_daemon_reponse_handler
```

```
2018 يناير 20: 17:18:02.656497 aaa: جلسة: 0x8dfd68c تمت إزالتها من جدول جلسة العمل 0
```

2018 يناير 20:17:18:02.656512 aaa: is_aaa_resp_status_success status = 1

2018 يناير 17:18:02.656525 aaa: is_aaa_resp_status_success true

2018 يناير 17:18:02.656538 aaa: aaa_send_client_response للمصادقة. <session-العلامات=21.
aaa_resp<-العلامات=0.

2018 يناير 20:17:18:02.656550 aaa: aaa_req_flag_normal

2018 يناير 20:17:18:02.656577 aaa: mts_send_response ناجح

2018 يناير 20:17:18:02.700520 aaa: aaa_process_fd_set تصحيح الأخطاء على aaa_accounting_q

2018 يناير 17:18:02.700688 aaa: كود التشغيل القديم: accounting_interim_update

2018 يناير 20:17:18:02.700702 aaa: aaa_create_local_acct_req: user=, session_id=, log=added
user fxosro

2018 يناير 17:18:02.700725 aaa: aaa_req_process للمحاسبة، الجلسة رقم 0

2018 يناير 20:17:18:02.700738 aaa: مرجع طلب MTS هو NULL. طلب محلي

2018 يناير 17:18:02.700749 aaa: إعداد AAA_REQ_RESPONSE_NOT_NEEDED

2018 يناير 20:17:18:02.700762 aaa: aaa_req_process طلب AAA عام من التطبيق: الافتراضي
apple_subtype: الافتراضي

2018 يناير 17:18:02.700774 aaa: try_next_aaa_method

2018 يناير 17:18:02.700798 aaa: لا توجد طرق تم تكوينها للإعدادات الافتراضية

2018 يناير 20:17:18:02.700810 aaa: لا يتوفر تكوين لهذا الطلب

2018 يناير 17:18:02.700997 aaa: aaa_send_client_response for accounting. session->flags=254.
aaa_resp->flags=0.

2018 يناير 17:18:02.701010 aaa: سيتم إرسال الرد على طلب المحاسبة الخاص بالمكتبة القديمة بنجاح

2018 يناير 17:18:02.701021 aaa: الاستجابة غير ضرورية لهذا الطلب

2018 يناير 17:18:02.701033 aaa: aaa_req_flag_local_resp

2018 يناير 17:18:02.701044 aaa: aaa_cleanup_session

2018 يناير 20:17:18:02.701055 aaa: يجب تحرير aaa_req.

2018 يناير 20:17:18:02.701067 aaa: نجح أسلوب التراجع المحلي

2018 يناير 17:18:02.706922 aaa: aaa_process_fd_set

2018 يناير 20:17:18:02.706937 aaa: aaa_process_fd_set: mtscallback على aaa_accounting_q

2018 يناير 17:18:02.706959 aaa: الرمز التشغيلي القديم: accounting_interim_update

aaa: aaa_create_local_acct_req: user=, session_id=, log=added 20:17:18:02.706972 يناير 2018
user:fxosro to role:read-only

بعد محاولة مصادقة فاشلة، سترى الإخراج التالي.

aaa: aaa_process_fd_set 17:15:18.102130 20 يناير 2018

aaa_q على aaa: aaa_process_fd_set: mtscallback 20:17:15:18.102149 يناير 2018

aaa: aaa_process_fd_set 17:15:18.102267 20 يناير 2018

aaa_q على aaa: aaa_process_fd_set: mtscallback 20:17:15:18.102281 يناير 2018

aaa: aaa_process_fd_set 17:15:18.102363 20 يناير 2018

aaa_q على aaa: aaa_process_fd_set: mtscallback 20:17:15:18.102377 يناير 2018

aaa: aaa_process_fd_set 17:15:18.102456 20 يناير 2018

aaa_q على aaa: aaa_process_fd_set: mtscallback 20:17:15:18.102468 يناير 2018

aaa: mts_aaa_req_process 17:15:18.102489 20 يناير 2018

aaa: aaa_req_process 17:15:18.102503 20 يناير 2018 للجلسة رقم 0

2018 يناير 20: 17:15:18.102526: aaa: aaa_req_process طلب AAA عام من التطبيق: تسجيل الدخول إلى التطبيق_subtype: الافتراضي

aaa: try_next_aaa_method 17:15:18.102540 20 يناير 2018

2018 يناير 20 17:15:18.102562: aaa: إجمالي الطرق التي تم تكوينها هو 1، الفهرس الحالي الذي يجب تجربته هو 0

aaa: handle_req_using_method 17:15:18.102575 20 يناير 2018

aaa: aaa_method_server_group 17:15:18.102586 20 يناير 2018

aaa: aaa_sg_method_handler group = radius 17:15:18.102598 20 يناير 2018

2018 يناير 20 17:15:18.102610: aaa: استخدام sg_protocol الذي تم تمريره إلى هذه الدالة

2018 يناير 20 17:15:18.102625: aaa: إرسال الطلب إلى خدمة RADIUS

2018 يناير 20: 17:15:18.102658: aaa: mts_send_msg_to_prot_daemon طول الحمولة = 371

2018 كانون الثاني/يناير 20: 17:15:18.102684: aaa: الجلسة: 0x8dfd68c مضافة إلى جدول الجلسة 1

2018 يناير 20:17:15:18.102698: aaa: تم تكوين مجموعة الطرق بنجاح

aaa: aaa_process_fd_set 17:15:18.273682 20 يناير 2018

aaa_q على aaa: aaa_process_fd_set: mtscallback 17:15:18.273724 20 يناير 2018

2018 يناير 20 17:15:18.273753 aaa: mts_message_response_handler :إستجابة MTS

2018 يناير 20 17:15:18.273768 aaa: prot_daemon_reponse_handler

2018 يناير 20 تمت إزالة aaa: aaa 17:15:18.273783 :الجلسة: 0x8dfd68c من جدول الجلسة 0

2018 يناير 20:17:15:18.273801 aaa: is_aaa_resp_status_success status = 2

2018 يناير 20 17:15:18.273815 aaa: is_aaa_resp_status_success true

2018 يناير 20 17:15:18.273829 aaa: aaa_send_client_response للمصادقة. <session-العلامات=21.
<aaa_resp-العلامات=0.

2018 يناير 20 17:15:18.273843 aaa: aaa_req_flag_normal

2018 يناير 20:17:15:18.273877 aaa: mts_send_response ناجح

2018 يناير 20 17:15:18.273902 aaa: aaa_cleanup_session

2018 يناير 20:17:15:18.273916 aaa: mts_drop من الطلب msg

2018 يناير 20:17:15:18.273935 aaa: يجب تحرير aaa_req.

2018 يناير 20 17:15:18.280416 aaa: aaa_process_fd_set

2018 يناير 20:17:15:18.280443 aaa: aaa_process_fd_set: mtscallback على aaa_q

2018 يناير 20:17:15:18.280454 aaa: aaa_enable_info_config: GET_REQ لرسالة خطأ تسجيل الدخول إلى
المصادقة والتفويض والمحاسبة (AAA)

2018 يناير 20 17:15:18.280460 aaa: إستعادة قيمة الإرجاع لعملية التكوين:عنصر أمان غير معروف

معلومات ذات صلة

سيطلب أمر ethanalyzer على FX-OS CLI بكلمة مرور عند تمكين مصادقة TACACS/RADIUS. يحدث هذا السلوك بسبب خطأ.

معرف الخطأ: [CSCvg87518](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ا م ا د ا د و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا