

Firepower Xsible Operating System (FXOS) 2.2: مساب اراصتخا فورعمل (ماظن نع ةرادإلا لجأ نم ضي وفتلاو لك يهلا ةقداصم ACS لبق نم RADIUS مادختساب دعب

المحتويات

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

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة RADIUS والتفويض لهيكل نظام التشغيل القابل للتشغيل (FXOS) عبر خادم التحكم في الوصول (ACS).

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 ACS

المكونات المستخدمة

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

- جهاز الأمان Cisco Firepower 4120، الإصدار 2.2
- Cisco Access Control Server، الإصدار 5.8.0.32

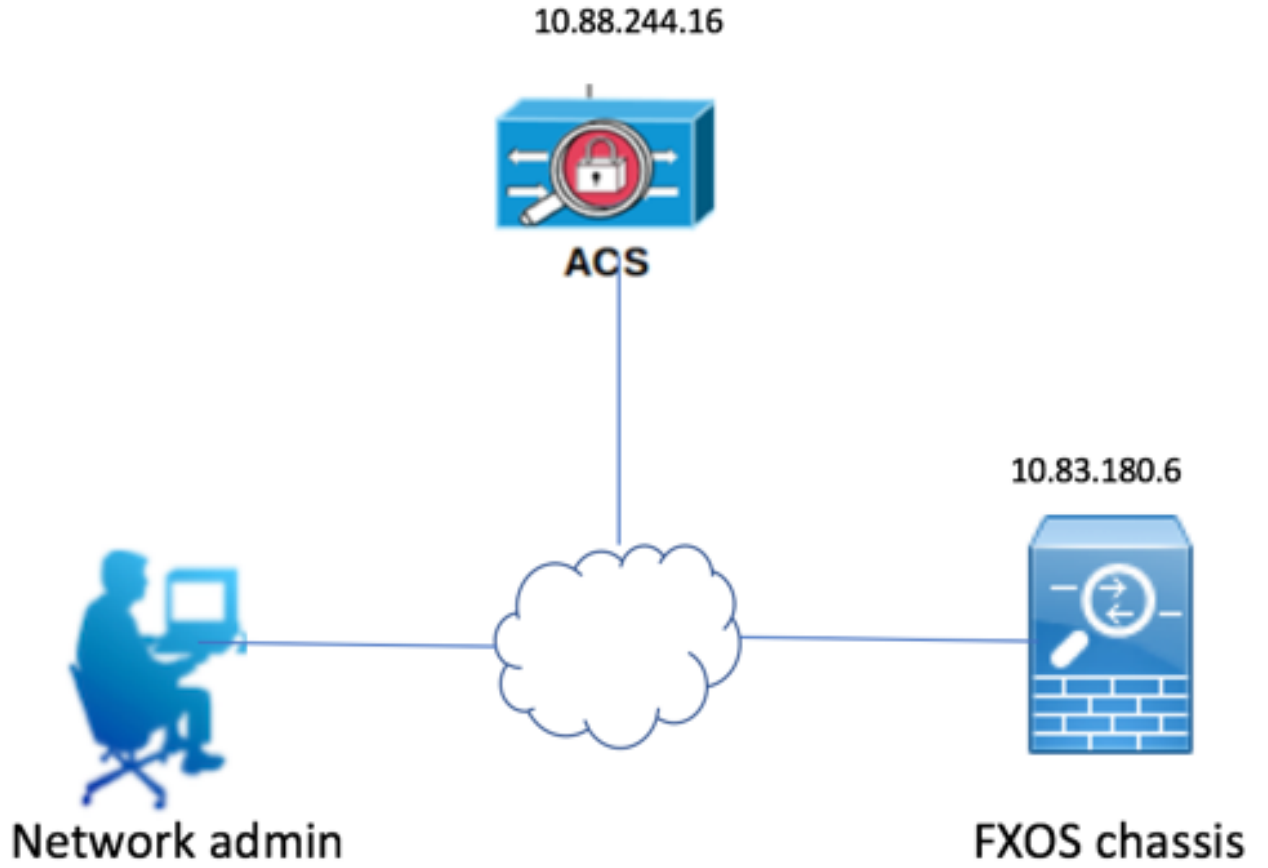
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الهدف من التكوين هو:

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

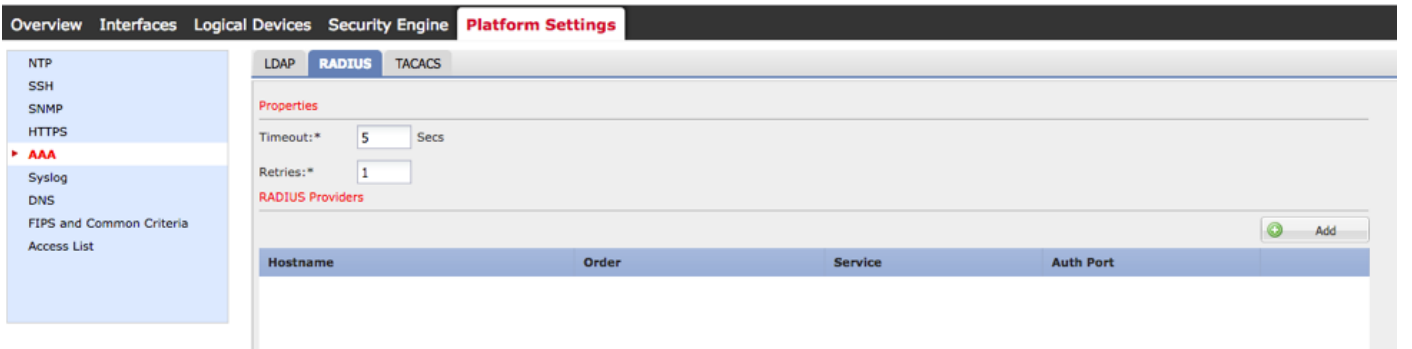
الرسم التخطيطي للشبكة



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. في شاشة إضافة مزود RADIUS، قم بإدخال القيم المطلوبة.

3.3. انقر فوق موافق لإغلاق مربع الحوار إضافة موفر RADIUS.

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

الخطوة 4. طقطقة حفظ.

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

LDAP **RADIUS** TACACS

Properties

Timeout:* Secs

Retries:*

RADIUS Providers

Hostname	Order	Service	Auth Port
10.88.244.16	1	authorization	1812

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 frossadmin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: *Local is fallback authentication method

Console Authentication:

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 10.88.244.16 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: 10.88.244.16

إدارة الحقوق:

الطلب: 1

منفذ المصادقة: 1812

المفتاح: ***

المهلة: 5

تكوين خادم ACS

إضافة FXOS كمورد شبكة

الخطوة 1. انتقل إلى موارد الشبكة < أجهزة الشبكة وعملاء AAA.

الخطوة 2. انقر فوق إنشاء.

My Workspace

Network Resources

- Network Device Groups
 - Location
 - Device Type
 - Network Devices and AAA Clients**
 - Default Network Device
 - External Proxy Servers
 - OCSP Services
- Users and Identity Stores
- Policy Elements
- Access Policies
- Monitoring and Reports
- System Administration

Network Resources > Network Devices and AAA Clients

Network Devices

Filter: Match if: Go

<input type="checkbox"/>	Name	IP Address	Description	NDG:Location	NDG:Device Type
<input type="checkbox"/>	APIC1P1	10.88.247.4/32		All Locations	All Device Types
<input type="checkbox"/>	APIC1P22	10.48.22.69/32		All Locations	All Device Types
<input type="checkbox"/>	ASA	10.88.244.12/32		All Locations	All Device Types
<input type="checkbox"/>	ASA_10.88.244.60	10.88.244.60/32	ASA_10.88.244.60	All Locations	All Device Types
<input type="checkbox"/>	Firesight	10.88.244.11/32		All Locations	All Device Types
<input type="checkbox"/>	FMC 6.1	10.88.244.51/32		All Locations	All Device Types
<input type="checkbox"/>	FXQS	10.83.180.6/32		All Locations	All Device Types

Create Duplicate Edit Delete | File Operations Export

الخطوة 3. أدخل القيم المطلوبة (الاسم وعنوان بروتوكول الإنترنت ونوع الجهاز وتمكين RADIUS وإضافة المفتاح).

Name:

Description:

Network Device Groups

Location

Device Type

IP Address

Single IP Address IP Subnets IP Range(s)

IP:

Authentication Options

▼ TACACS+

Shared Secret:

Single Connect Device

Legacy TACACS+ Single Connect Support

TACACS+ Draft Compliant Single Connect Support

▼ RADIUS

Shared Secret:

CoA port:

Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format ASCII HEXADECIMAL

 = Required fields

الخطوة 4. انقر على إرسال.

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه 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 ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا