

(FXOS) ليغشت لل لباق لا ليغشت لا ماطن لكيه لا ضيوف ت/ة ق داصم :Firepower 2.2 TACACS+ مادخت ساب دع ب نع ة رادال

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 TACACS+ والتفويض لهيكل نظام التشغيل القابل للتشغيل ((FXOS Firepower 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 ريميرز، 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
- ترخيص إدارة أجهزة TACACS+ مطلوب داخل 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 TACACS+

الخطوة 1. انتقل إلى إعدادات النظام الأساسي < AAA.

الخطوة 2. انقر فوق علامة التبويب TACACS.



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

3.1 في منطقة موفري TACACS، انقر فوق إضافة.

3.2 بمجرد فتح مربع الحوار "إضافة موفر TACACS"، أدخل القيم المطلوبة.

3.3 انقر فوق موافق لإغلاق مربع الحوار إضافة موفر TACACS.

Add TACACS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Port:*

Timeout:* Secs

الخطوة 4. طقطقة حفظ.

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

LDAP RADIUS **TACACS**

Properties

Timeout:* Secs

TACACS Providers

Hostname	Order	Port
10.88.244.50	1	49

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

الخطوة 6. تحت المصادقة الافتراضية أختار TACACS.

Overview Interfaces Logical Devices Security Engine Platform Settings

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 TACACS+ باستخدام CLI (واجهة سطر الأوامر)

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

أمان النطاق #FPR4120-TAC-A

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

FPR4120-TAC-A /security/default-auth # set domain tacacs

الخطوة 2. أستخدم الأمر **show detail** للتحقق من التكوين.

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

المصادقة الافتراضية:

مجال الإدارة: **TACACS**

النطاق التشغيلي: **TACACS**

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. تقوم معلمات خادم TACACS بتشغيل الأوامر التالية.

#FPR4120-TAC-A أمان النطاق

FPR4120-TAC-A /security # scope tacacs

10.88.244.50 # FPR4120-TAC-A /security/tacacs أدخل الخادم

"ACS # FPR4120-TAC-A /security/tacacs/server مجموعة إدارة خادم"

*FPR4120-TAC-A /security/tacacs/server # مفتاح المجموعة

أدخل المفتاح: *****

تأكيد المفتاح: *****

الخطوة 4. أستخدم الأمر **show detail** للتحقق من التكوين.

*FPR4120-TAC-A /security/tacacs/server # تفاصيل العرض

خادم TACACS: +

اسم المضيف أو FQDN أو عنوان IP: 10.88.244.50

إدارة الحقوق:

الطلب: 1

المنفذ: 49

المفتاح: ***

المهلة: 5

تكوين خادم ISE

إضافة كمورد شبكة

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

الخطوة 2. انقر فوق إضافة (Add).

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 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Service', and 'Threat Centric NAC'. 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 TACACS+ 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 > FXOS

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

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, and 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 a '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, and 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, and 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 Shell لكل دور مستخدم

الخطوة 1. انتقل إلى مراكز العمل < إدارة الأجهزة < عناصر السياسة < النتائج < ملفات تعريف TACACS وانقر +إضافة.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected Rows/Page 4 / 1 Go 4 Total Rows

Refresh Add Duplicate Trash Edit Filter

Name	Type	Description
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR
Deny All Shell Profile	Shell	Deny All Shell Profile
Default Shell Profile	Shell	Default Shell Profile

الخطوة 2. أدخل القيم المطلوبة لملف تعريف TACACS
2.1. أدخل الاسم.

TACACS Profiles > New

TACACS Profile

Name

Description

Task Attribute View

Raw View

2.2. في علامة التبويب عرض أولي، قم بتكوين زوج Cisco-AV التالي.

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

TACACS Profile

Name FXOS_Admin_Profile

Description

Task Attribute View

Raw View

Profile Attributes

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

Cancel

Submit

2.3. انقر فوق إرسال.

TACACS Profile

Name

Description

Task Attribute View Raw View

Common Tasks

Common Task Type

<input type="checkbox"/> Default Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Maximum Privilege	<input type="text"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List	<input type="text"/>	
<input type="checkbox"/> Auto Command	<input type="text"/>	
<input type="checkbox"/> No Escape	<input type="text"/>	(Select true or false)
<input type="checkbox"/> Timeout	<input type="text"/>	Minutes (0-9999)
<input type="checkbox"/> Idle Time	<input type="text"/>	Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="admin"	<input type="checkbox"/>

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

Custom Attributes

+ Add Trash Edit

Type	Name	Value	
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles="aaa"	<input type="checkbox"/>

Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="operations"	 

Custom Attributes

<input type="checkbox"/>	Type	Name	Value	
<input type="checkbox"/>	MANDATORY	cisco-av-pair	shell:roles="read-only"	 

TACACS Profiles

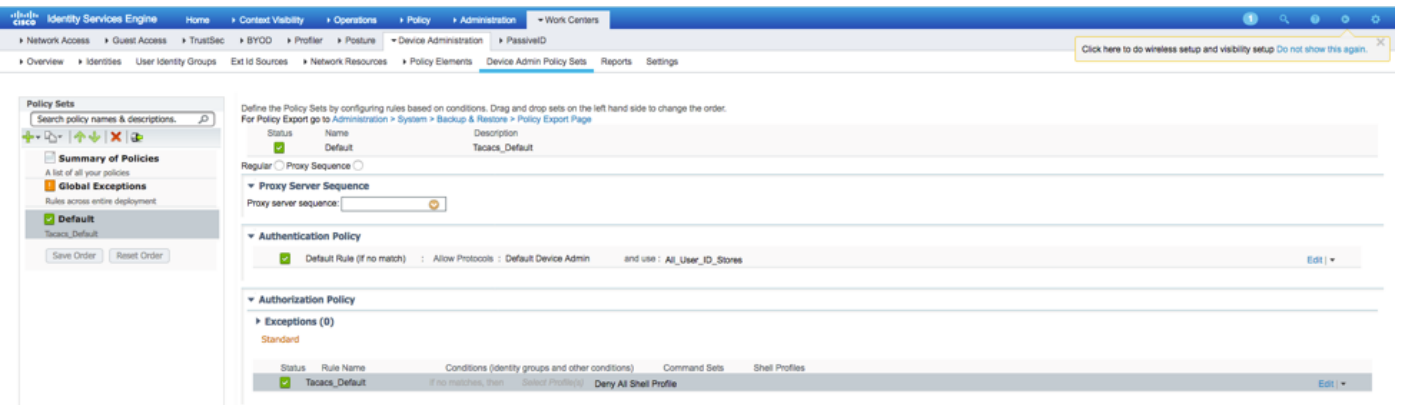
0 Selected

Rows/Page 8 / 1 / 1 Go 8 Total Rows

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	FXOS_Admin_Profile	Shell	
<input type="checkbox"/>	FXOS_AAA_Shell	Shell	
<input type="checkbox"/>	FXOS_Operations_Shell	Shell	
<input type="checkbox"/>	FXOS_ReadOnly_Shell	Shell	

إنشاء سياسة تفويض TACACS

الخطوة 1. انتقل إلى مراكز العمل < إدارة الأجهزة > مجموعات نهج إدارة الأجهزة.



The screenshot displays the Cisco ISE Policy Sets configuration interface. The 'Tactics_Default' policy set is selected. The 'Authentication Policy' section is expanded, showing the 'Default Rule (if no match)' set to 'Allow Protocols: Default Device Admin' and 'and use: All_User_ID_Stores'. The 'Authorization Policy' section is also expanded, showing the 'Default Rule' set to 'Deny All Shell Profile'.

الخطوة 2. تأكد من أن نهج المصادقة يشير إلى قاعدة بيانات المستخدمين الداخليين أو مخزن الهوية المطلوب.

Authentication Policy



Default Rule (If no match) : Allow Protocols : Default Device Admin and use : All_User_ID_Stores

الخطوة 3. انقر فوق السهم في نهاية نهج التحويل الافتراضي وانقر فوق إدراج قاعدة أعلاه.

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then Select Profile(s) Deny All Shell Profile		

Insert New Rule Above

الخطوة 4. أدخل قيم القاعدة مع المعلمات المطلوبة:

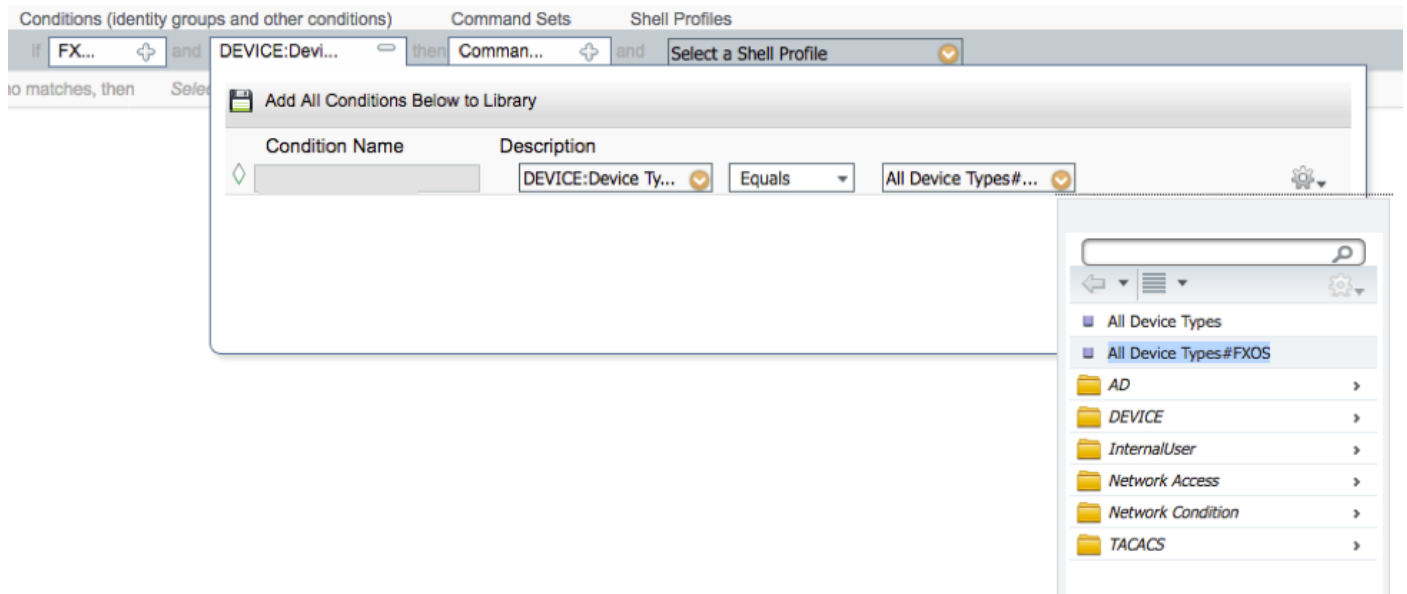
4.1. اسم القاعدة: قاعدة مسؤول FXOS.

4-2 الشروط.

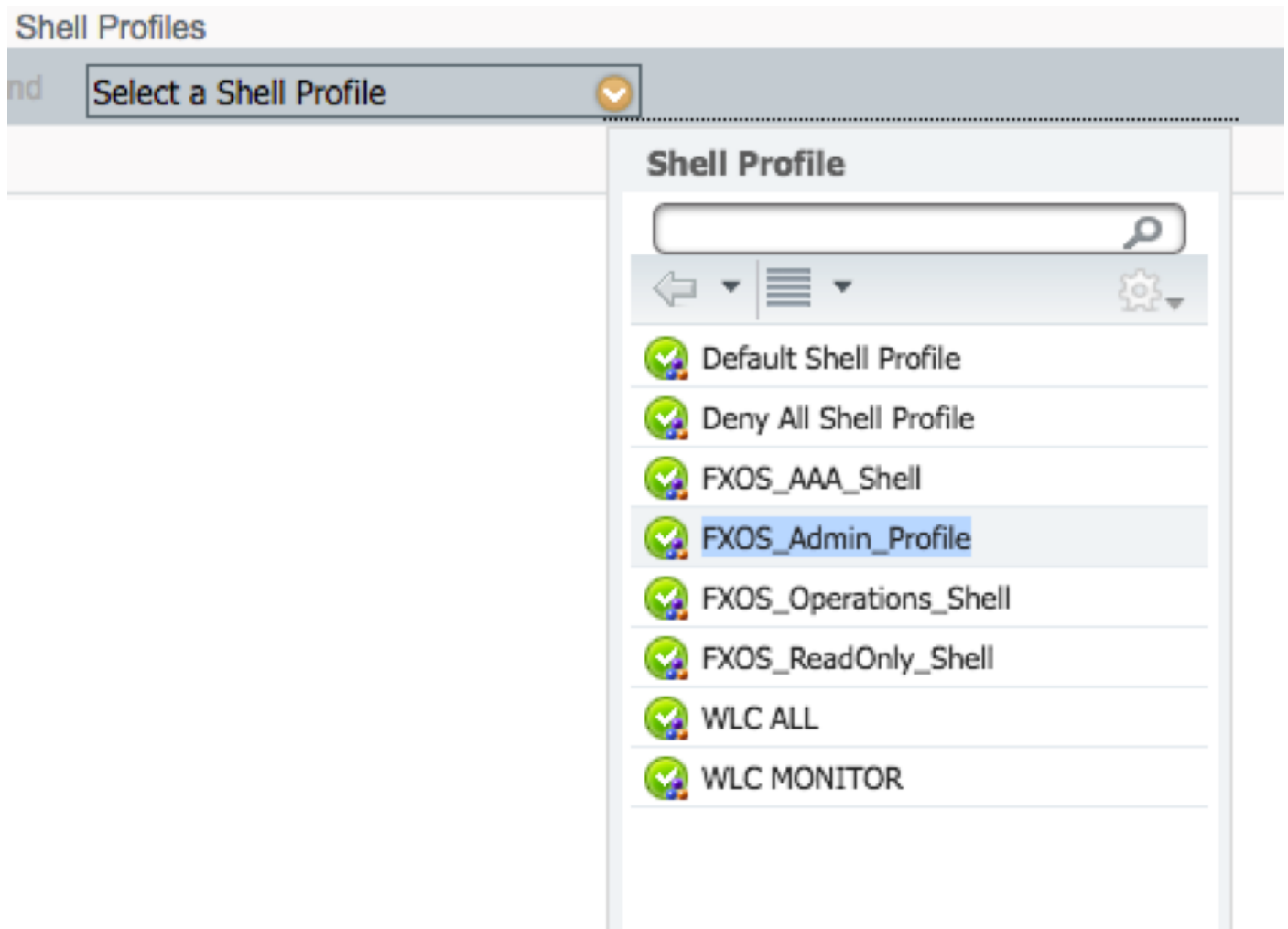
إذا: مجموعة هوية المستخدم هي مسؤول FXOS

The screenshot shows the configuration interface for an authorization policy. The 'Conditions' field is set to 'Any'. A dropdown menu for 'User Identity Groups' is open, showing a list of groups including 'FXOS ADMIN' which is highlighted. The 'Command Sets' field is empty, and the 'Shell Profiles' field is set to 'Select a Shell Profile'. 'Save' and 'Reset' buttons are visible at the bottom left.

والجهاز: نوع الجهاز يساوي كل أنواع الأجهزة #FXOS



Shell: FXOS_ADMIN_PROFILE ملف تعريف



الخطوة 5. طقطقة تم.

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	FXOS Admin Rule	FX... AND DEVICE:Devi...	Select an item	FXOS_Admin_Profile
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s)	Deny All Shell Profile

Save Reset

الخطوة 6. كرر الخطوة 3 و 4 لأدوار المستخدم المتبقية وعند الانتهاء انقر فوق حفظ.

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	FXOS Admin Rule	if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS	then Select an item	FXOS_Admin_Profile
<input checked="" type="checkbox"/>	FXOS AAA Rule	if FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS	then Select Profile(s)	FXOS_AAA_Shell
<input checked="" type="checkbox"/>	FXOS Operations Rule	if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS	then Select Profile(s)	FXOS_Operations_Shell
<input checked="" type="checkbox"/>	FXOS Read Only Rule	if FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS	then Select Profile(s)	FXOS_ReadOnly_Shell
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	Select Profile(s)	Deny All Shell Profile

Save Reset

التحقق من الصحة

يمكنك الآن إختبار كل مستخدم والتحقق من دور المستخدم المعين.

التحقق من هيكل FXOS

1. يدخل Telnet أو SSH إلى هيكل FXOS ويدخل باستخدام أي من المستخدمين الذين تم إنشاؤه 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 fxOadmin:

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

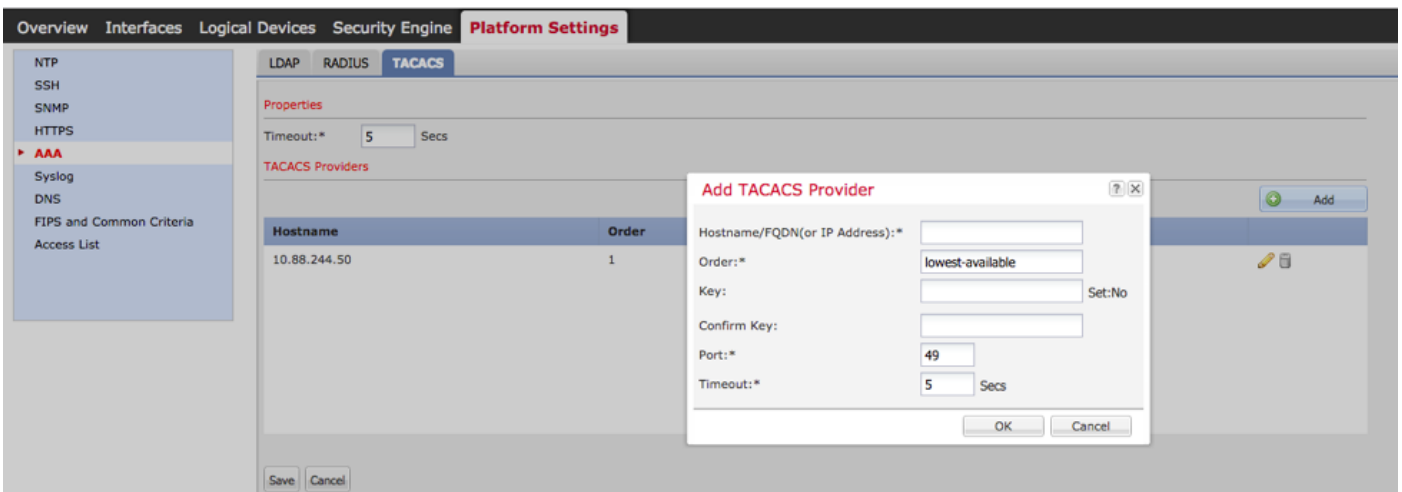
FPR4120-TAC-A#connect fxos

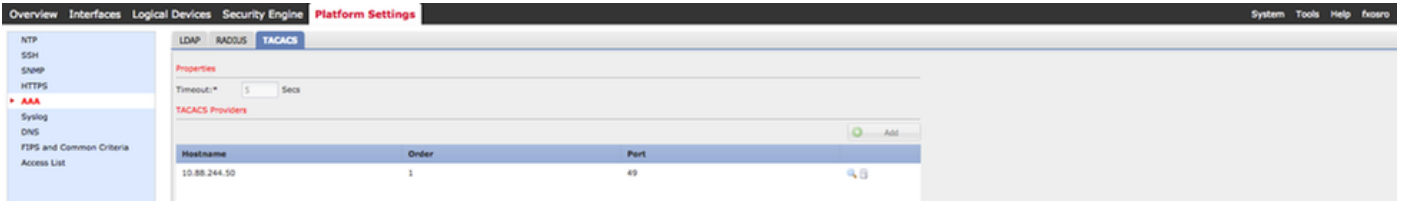
FPR4120-TAC-A (fxos)# debug aaa-requests

٪ الإذن المرفوض للدور

2. استعرض عنوان IP الخاص بهيكل FXOS وقم بتسجيل الدخول باستخدام أي من المستخدمين الذين تم إنشاؤه على ISE.

دور مستخدم المسؤول.

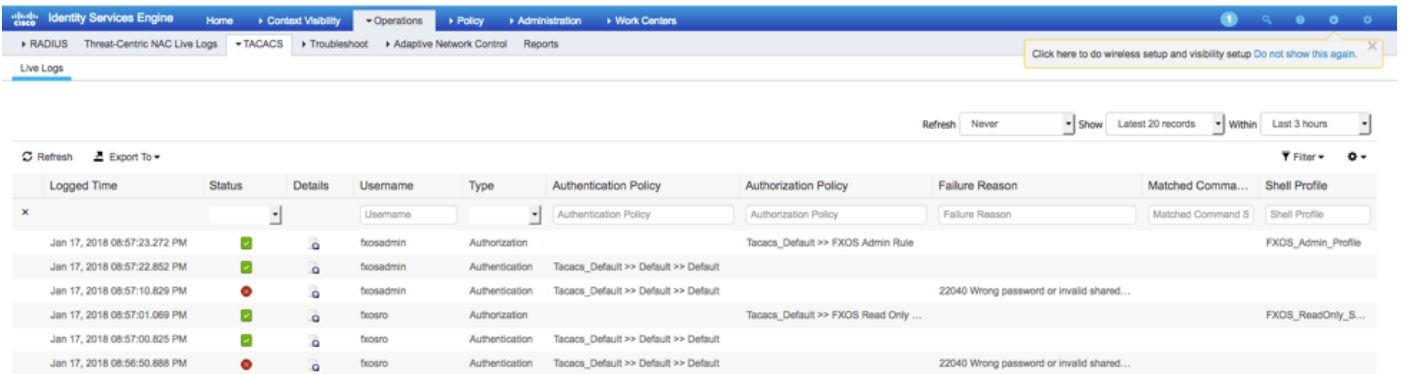




ملاحظة: لاحظ أن الزر ADD مصقول.

التحقق من ISE 2.0

1. انتقل إلى العمليات < TACACS LiveLog. يجب أن تكون قادراً 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
```

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

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

بعد محاولة المصادقة الناجحة، سترى الإخراج التالي.

```
2018 يناير 17 15:46:40.305247 aaa: aaa_req_process 15:46:40.305247
```

```
2018 يناير 17: 15:46:40.305262 aaa: aaa_req_process 15:46:40.305262 طلب AAA عام من التطبيق: تسجيل الدخول إلى التطبيق subtype الافتراضي
```

```
2018 يناير 17:46:40.305271 aaa: try_next_aaa_method 17:46:40.305271
```

```
2018 يناير 17:46:40.305285 aaa: إجمالي الأساليب التي تم تكوينها هو 1، الفهرس الحالي الذي يجب تجربته هو 0
```

2018 يناير 17:46:40.305294 aaa: handle_req_using_method

2018 يناير 17:46:40.305301 aaa: aaa_method_server_group

2018 يناير 17:46:40.305308 aaa: aaa_sg_method_handler group = tacacs

2018 يناير 17:46:40.305315 aaa: استخدام sg_protocol الذي يتم تمريره إلى هذه الدالة

2018 يناير 17:46:40.305324 aaa: إرسال طلب إلى خدمة TACACS

2018 يناير 17:46:40.305384 aaa: تم تكوين مجموعة الطرق بنجاح

2018 يناير 17:46:40.554631 aaa: aaa_process_fd_set

2018 يناير 17:46:40.55229 aaa: aaa_process_fd_set: mtscallback على aaa_q

2018 يناير 17:46:40.55817 aaa: mts_message_response_handler: إستجابة MTS

2018 يناير 17:46:40.556387 aaa: prot_daemon_reponse_handler

2018 كانون الثاني 17:46:40.557042 AAA: الجلسة: 0x8dfd68c تمت إزالتها من جدول الجلسة 0

2018 يناير 17:46:40.557059 aaa: is_aaa_resp_status_success status = 1

2018 يناير 17:46:40.557066 aaa: is_aaa_resp_status_success true

2018 يناير 17:46:40.557075 aaa: aaa_send_client_response session=<العلامات=21.0=aaa_resp->المصادقة.

2018 يناير 17:46:40.557083 aaa: aaa_req_flag_normal

2018 يناير 17:46:40.557106 aaa: mts_send_response ناجح

2018 يناير 17:46:40.557364 aaa: aaa_req_process للتحويل. جلسة العمل رقم 0

2018 يناير 17:46:40.557378 aaa: aaa_req_process الذي تم استدعاؤه مع سياق من التطبيق: تسجيل الدخول
app_subtype: default authen_type:2, authen_method: 0

2018 يناير 17:46:40.557386 aaa: aaa_send_req_using_context

2018 يناير 17:46:40.557394 (aaa: aaa_sg_method_handler group = (null

2018 يناير 17:46:40.557401 aaa: استخدام sg_protocol الذي تم تمريره إلى هذه الدالة

2018 يناير 17:46:40.557408 aaa: مستند إلى السياق أو موجه AAA req (الاستثناء: ليس طلب ترحيل). لن يتم الحصول على نسخة من طلب AAA

2018 يناير 17:46:40.557415 aaa: إرسال طلب إلى خدمة TACACS

2018 يناير 17:46:40.801732 aaa: aaa_send_client_response session=<العلامات=9=aaa_resp->التحويل.

2018 يناير 17:46:40.801740 aaa: aaa_req_flag_normal

2018 يناير 17:46:40.801761 aaa: mts_send_response ناجح

2018 يناير 17:46:40.848932 aaa: accounting_interim_update: كود التشغيل القديم:

2018 يناير 17:46:40.848943 aaa: aaa_create_local_acct_req: user=، session_id=، log=added
role:admin إلى user:fxosadmin

2018 يناير 15:46:40.848963 aaa: aaa_req_process 0 للجلسة رقم

2018 يناير 17:46:40.848972 aaa: مرجع طلب MTS هو NULL. طلب محلي

2018 يناير 17:46:40.848982 aaa: إعداد AAA_REQ_RESPONSE_NOT_NEEDED

2018 يناير 17:46:40.848992 aaa: aaa_req_process طلب AAA عام من التطبيق: الافتراضي
apple_subtype: الافتراضي

2018 يناير 17:46:40.84902 aaa: try_next_aaa_method

2018 يناير 17:46:40.849022 aaa: لا توجد طرق تم تكوينها للإعدادات الافتراضية

2018 يناير 17:46:40.849032 aaa: لا يتوفر تكوين لهذا الطلب

2018 يناير 17:46:40.849043 aaa: try_backback_method

2018 يناير 17:46:40.849053 aaa: handle_req_using_method

2018 يناير 17:46:40.849063 aaa: محلي_method_handler

2018 يناير 17:46:40.849073 aaa: aaa_local_accounting_msg

2018 يناير 17:46:40.849085 aaa: تحديث::إضافة مستخدم:fxosadmin إلى الدور:admin

بعد محاولة مصادقة فاشلة، سترى الإخراج التالي.

2018 يناير 15:46:17.836271 aaa: aaa_req_process 0 للجلسة رقم

2018 يناير 17:46:17.836616 aaa: aaa_req_process طلب AAA عام من التطبيق: تسجيل الدخول إلى
التطبيق_subtype: الافتراضي

2018 يناير 17:46:17.837063 aaa: try_next_aaa_method

2018 يناير 17:46:17.837416 aaa: إجمالي الأساليب التي تم تكوينها هو 1، الفهرس الحالي الذي يجب تجربته هو
0

2018 يناير 17:46:17.837766 aaa: handle_req_using_method

2018 يناير 17:46:17.838103 aaa: aaa_method_server_group

2018 يناير 17:46:17.838477 aaa: aaa_sg_method_handler group = tacacs

2018 يناير 17:46:17.83826 aaa: استخدام sg_protocol الذي تم تمريره إلى هذه الدالة

2018 يناير 17:46:17.839167 aaa: إرسال طلب إلى خدمة TACACS

2018 يناير 17:46:17.840225 aaa: تم تكوين مجموعة الطرق بنجاح

2018 يناير 17:46:18.043710 aaa: is_aaa_resp_status_success status = 2

2018 يناير 15:46:18.044048 aaa: is_aaa_resp_status_success true

2018 يناير 17:46:18.044395 aaa: aaa_send_client_response للمصادقة. <العلامات=21.
aaa_resp <العلامات=0.

2018 يناير 17:46:18.044733 aaa: aaa_req_flag_normal

2018 يناير 17:46:18.045096 aaa: mts_send_response ناجح

2018 يناير 17:46:18.045677 aaa: aaa_cleanup_session

2018 يناير 17:46:18.045689 aaa: mts_drop من الطلب msg

2018 يناير 17:46:18.045699 aaa: يجب تحرير aaa_req.

2018 يناير 17:46:18.045715 aaa: aaa_process_fd_set

2018 يناير 17:46:18.045722 aaa: aaa_process_fd_set: mtscallback على aaa_q

2018 يناير 17:46:18.045732 aaa: aaa_enable_info_config: GET_REQ لرسالة خطأ تسجيل الدخول إلى
المصادقة والتفويض والمحاسبة (AAA)

2018 يناير 17:46:18.045738 aaa: إستعادة قيمة الإرجاع لعملية التكوين:عنصر أمان غير معروف

معلومات ذات صلة

سيطالب 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 نم ةومجم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انء مچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئى. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه
ىل إامئاد ةوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزلچنل دن تسمل