

Firepower可擴展作業系統(FXOS)2.2:使用RADIUS通過ACS進行遠端管理的機箱身份驗證和授權

目錄

- [簡介](#)
- [必要條件](#)
- [需求](#)
- [採用元件](#)
- [設定](#)
- [網路圖表](#)
- [組態](#)
- [配置FXOS機箱](#)
- [配置ACS伺服器](#)
- [驗證](#)
- [FXOS機箱驗證](#)
- [ACS驗證](#)
- [疑難排解](#)
- [相關資訊](#)

簡介

本檔案介紹如何透過存取控制伺服器(ACS)設定Firepower可擴充作業系統(FXOS)機箱的RADIUS驗證和授權。

FXOS機箱包括以下使用者角色：

- Administrator — 對整個系統的完全讀寫訪問許可權。預設情況下為預設管理員帳戶分配此角色，並且無法更改。
- 只讀 — 對系統配置的可讀訪問許可權，無修改系統狀態的許可權。
- 操作 — 對NTP配置、智慧許可的Smart Call Home配置以及系統日誌（包括系統日誌伺服器和故障）的可讀訪問許可權。對系統其餘部分的可讀訪問許可權。
- AAA — 對使用者、角色和AAA配置的可讀訪問。對系統其餘部分的可讀訪問許可權。

通過CLI可以看到，如下所示：

```
fr4120-TAC-A /security* # show role
```

角色：

```
角色名稱Priv
```

```
-----
```

```
aaa aaa
```

admin

運營運營

唯讀唯讀

作者：Tony Ramirez、Jose Soto、Cisco TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower可擴展作業系統(FXOS)知識
- ACS配置知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Firepower 4120安全裝置版本2.2
- 虛擬思科存取控制伺服器版本5.8.0.32

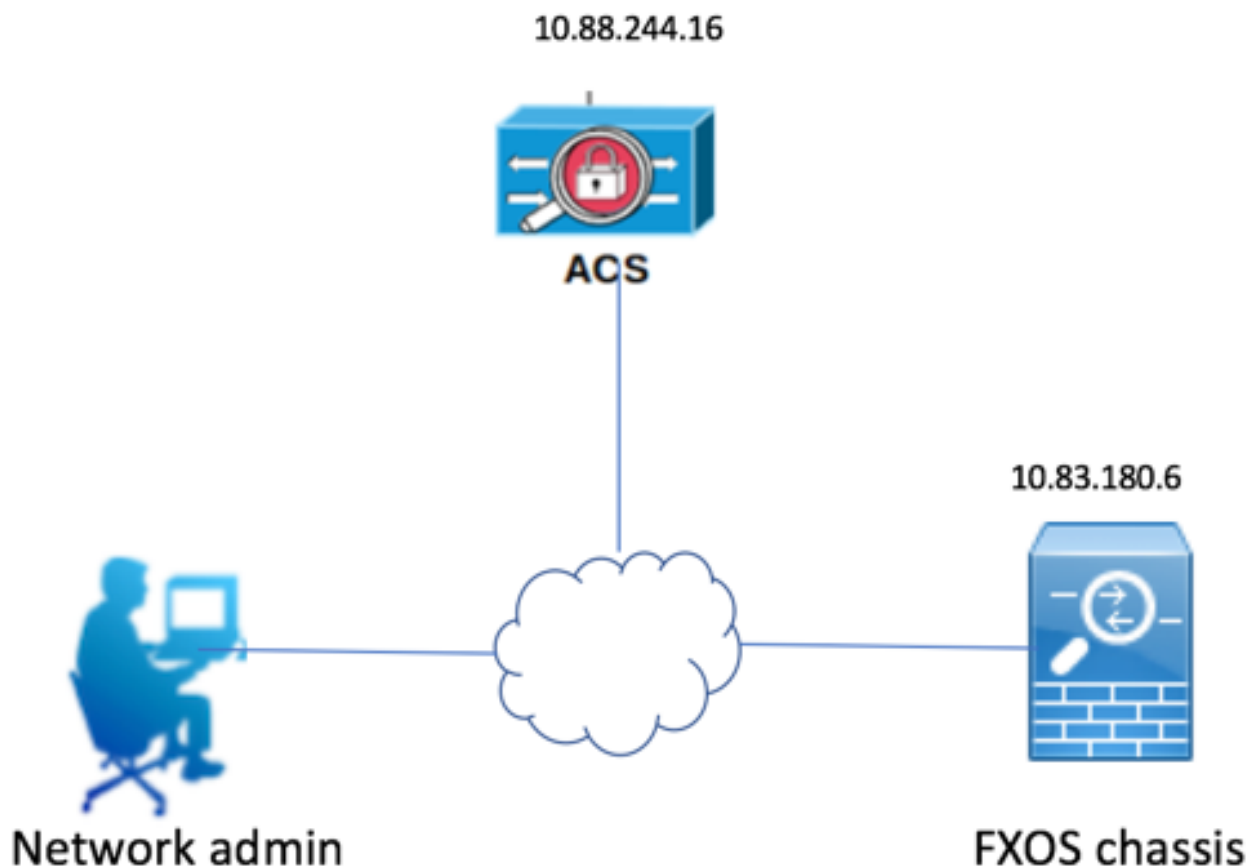
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

此組態的目的是：

- 通過ACS驗證登入到FXOS基於Web的GUI和SSH的使用者。
- 通過ACS，根據使用者各自的使用者角色授權使用者登入FXOS的基於Web的GUI和SSH。
- 通過ACS驗證FXOS上的身份驗證和授權操作是否正確。

網路圖表



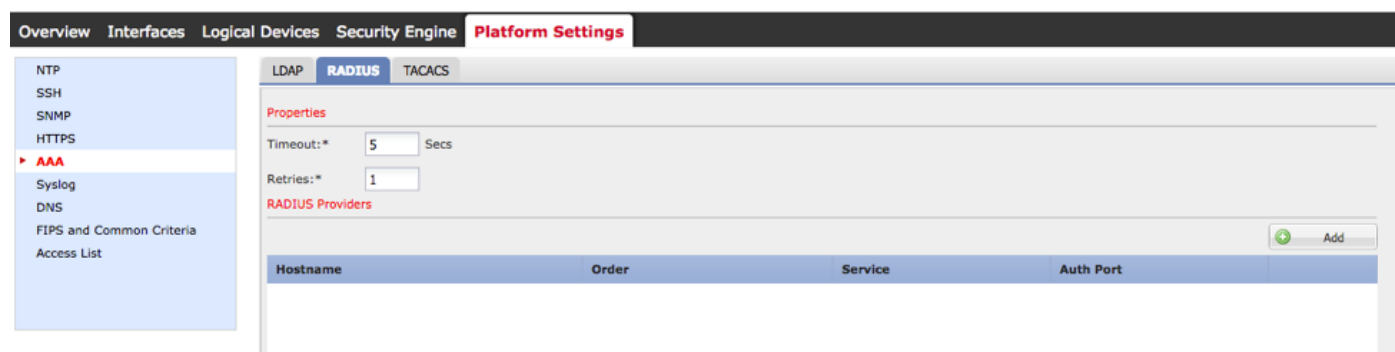
組態

配置FXOS機箱

使用機箱管理器建立RADIUS提供程式

步驟1.導覽至Platform Settings > AAA。

步驟2.按一下RADIUS索引標籤。



步驟3.對於要新增的每個RADIUS提供程式 (最多16個提供程式) 。

3.1.在RADIUS提供程式區域中，按一下Add。

3.2.在「新增RADIUS提供程式」對話方塊中，輸入所需的值。

3.3.按一下**確定**關閉「新增RADIUS提供程式」對話方塊。

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

步驟4.按一下「Save」。

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

步驟5.導覽至System > User Management > Settings。

步驟6.在Default Authentication下選擇RADIUS。

Overview Interfaces Logical Devices Security Engine Platform Settings

System Tools Help fssadmin

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

使用CLI建立RADIUS提供程式

步驟1. 若要啟用RADIUS驗證，請運行以下命令。

```
fpr4120-TAC-A#作用域安全性
```

```
fpr4120-TAC-A /security # scope default-auth
```

```
fpr4120-TAC-A /security/default-auth # set realm radius
```

步驟2. 使用**show detail**命令顯示結果。

```
fpr4120-TAC-A /security/default-auth # show detail
```

預設身份驗證：

管理領域：**Radius**

操作領域：**Radius**

Web會話刷新期間 (秒)：600

Web、ssh、telnet會話的會話超時 (秒)：600

Web、ssh、telnet會話的絕對會話超時 (秒)：3600

串列控制檯會話超時 (秒)：600

串列控制檯絕對會話超時 (秒)：3600

管理員身份驗證伺服器組：

操作身份驗證伺服器組：

使用第二個因素：否

步驟3. 要配置RADIUS伺服器引數，請運行以下命令。

```
fpr4120-TAC-A#作用域安全性
```

```
fpr4120-TAC-A /security # scope radius
```

```
fpr4120-TAC-A /security/radius # enter server 10.88.244.16
```

```
fpr4120-TAC-A /security/radius/server # set descr "ISE Server"
```

```
fpr4120-TAC-A /security/radius/server* # set key
```

輸入金鑰：*****

確認金鑰：*****

步驟4. 使用**show detail**命令顯示結果。

```
fpr4120-TAC-A /security/radius/server* # show detail
```

RADIUS伺服器：

主機名、FQDN或IP地址：10.88.244.16

描述：

訂購：1

身份驗證埠：1812

主要:****

逾時:5

配置ACS伺服器

將FXOS新增為網路資源

步驟1.導覽至Network Resources > Network Devices and AAA Clients。

步驟2.按一下「Create」。

Network Resources > Network Devices and AAA Clients

Network Devices

Filter: Match if:

<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

|

步驟3.輸入所需的值 (名稱、IP地址、裝置型別和啟用RADIUS並新增金鑰)。

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

步驟4.按一下「Submit」。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。