

Firepower eXtensible Operating System (FXOS)

2.2: Autenticazione e autorizzazione dello chassis per la gestione remota con ACS tramite RADIUS

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione dello chassis FXOS](#)

[Configurazione del server ACS](#)

[Verifica](#)

[Verifica dello chassis FXOS](#)

[Verifica ACS](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare l'autenticazione e l'autorizzazione RADIUS per lo chassis Firepower eXtensible Operating System (FXOS) tramite Access Control Server (ACS).

Lo chassis FXOS include i seguenti ruoli utente:

- Amministratore: accesso completo in lettura e scrittura all'intero sistema. All'account amministratore predefinito viene assegnato questo ruolo per impostazione predefinita e non può essere modificato.
- Sola lettura - Accesso in sola lettura alla configurazione del sistema senza privilegi per la modifica dello stato del sistema.
- Operazioni: accesso in lettura e scrittura alla configurazione NTP, alla configurazione di Smart Call Home per Smart Licensing e ai registri di sistema, inclusi i server syslog e i relativi errori. Accesso in lettura al resto del sistema.
- AAA: accesso in lettura e scrittura a utenti, ruoli e configurazione AAA. Accesso in lettura al resto del sistema.

Dalla CLI, questa condizione può essere vista come segue:

```
fpr4120-TAC-A /security* # show role
```

Ruolo:

Priv nome ruolo

—

aaa aaa

admin admin

operazioni

sola lettura

Contributo di Tony Ramirez, Jose Soto, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Firepower eXtensible Operating System (FXOS)
- Conoscenza della configurazione di ACS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Firepower 4120 Security Appliance versione 2.2
- Virtual Cisco Access Control Server versione 5.8.0.32

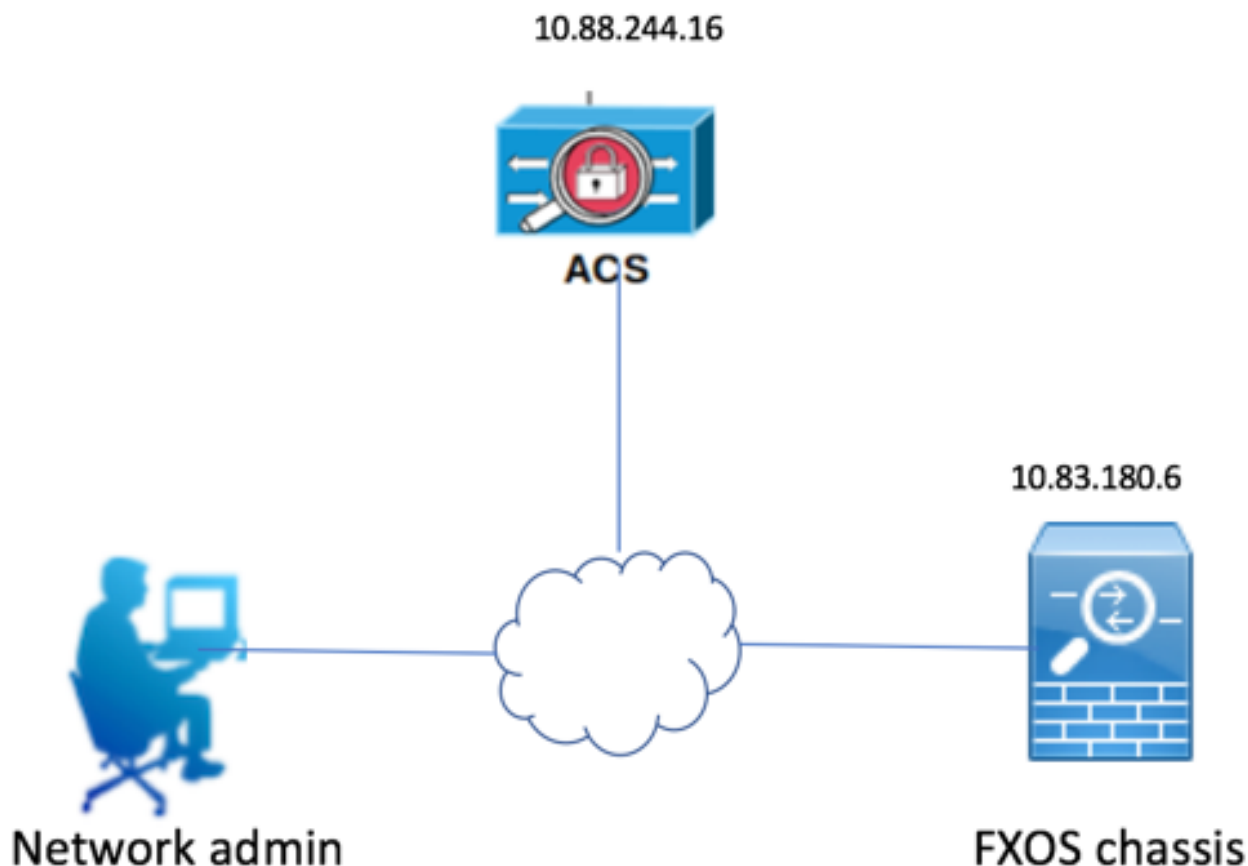
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

L'obiettivo della configurazione è:

- Autenticare gli utenti che accedono alla GUI e SSH basate sul Web di FXOS tramite ACS.
- Autorizzare gli utenti ad accedere alla GUI basata sul Web di FXOS e al protocollo SSH in base al rispettivo ruolo utente tramite ACS.
- Verificare il corretto funzionamento dell'autenticazione e dell'autorizzazione su FXOS tramite ACS.

Esempio di rete



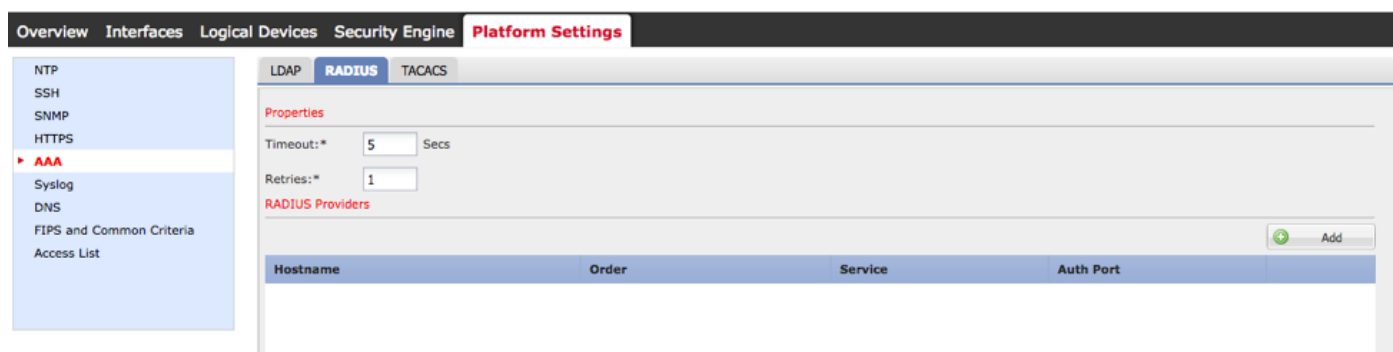
Configurazioni

Configurazione dello chassis FXOS

Creazione di un provider RADIUS mediante Chassis Manager

Passaggio 1. Passare a **Impostazioni piattaforma > AAA**.

Passaggio 2. Fare clic sulla scheda **RADIUS**.



Passaggio 3. Per ogni provider RADIUS che si desidera aggiungere (fino a 16 provider).

- 3.1. Nell'area Provider RADIUS, fare clic su **Aggiungi**.
- 3.2. Nella finestra di dialogo Aggiungi provider RADIUS, immettere i valori richiesti.
- 3.3. Fare clic su **OK** per chiudere la finestra di dialogo Aggiungi provider RADIUS.

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

Passaggio 4. Fare clic su **Salva**.

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

Passaggio 5. Passare a **Sistema > Gestione utente > Impostazioni**.

Passaggio 6. In Autenticazione predefinita scegliere **RADIUS**.

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

Creazione di un provider RADIUS tramite CLI

Passaggio 1. Per abilitare l'autenticazione RADIUS, eseguire i comandi seguenti.

```
fpr4120-TAC-A# ambito sicurezza
```

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

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

Passaggio 2. Utilizzare il comando **show detail** per visualizzare i risultati.

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

Autenticazione predefinita:

Area di autenticazione amministrativa: **Raggio**

Area operativa: **Raggio**

Periodo di aggiornamento sessione Web (sec): 600

Timeout sessione (in sec) per sessioni Web, ssh e telnet: 600

Timeout sessione assoluta (in secondi) per sessioni Web, ssh e telnet: 3600

Timeout sessione console seriale (sec): 600

Timeout sessione assoluta console seriale (sec): 3600

Gruppo server Autenticazione amministratore:

Gruppo server di autenticazione operativo:

Utilizzo del secondo fattore: No

Passaggio 3. Per configurare i parametri del server RADIUS, eseguire i comandi seguenti.

```
fpr4120-TAC-A# ambito sicurezza
```

```
fpr4120-TAC-A /security # raggio ambito
```

```
fpr4120-TAC-A /security/radius # ingresso nel server 10.88.244.16
```

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

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

Immettere la chiave: *****

Confermare la chiave: *****

Passaggio 4. Per visualizzare i risultati, utilizzare il comando **show detail**.

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

Server RADIUS:

Nome host, FQDN o indirizzo IP: 10.88.244.16

Descr.:

Ordine: 1

Auth Port (Porta autenticazione): 1812

Chiave: ****

Timeout: 5

Configurazione del server ACS

Aggiunta di FXOS come risorsa di rete

Passaggio 1. Passare a **Risorse di rete > Dispositivi di rete e client AAA.**

Passaggio 2. Fare clic su **Crea.**

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

Passaggio 3. Immettere i valori richiesti (Nome, Indirizzo IP, Tipo di dispositivo, Abilita RADIUS e aggiungere la chiave).

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

Passaggio 4. Fare clic su **Sottometti**.

