

Sistema operacional Firepower eXtensible (FXOS) 2.2: Autenticação e autorização do chassi para gerenciamento remoto com ACS usando RADIUS

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurando o chassi FXOS](#)

[Configurando o servidor ACS](#)

[Verificar](#)

[Verificação do chassi FXOS](#)

[Verificação ACS](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a Autenticação e a Autorização RADIUS para o chassi do Sistema Operacional Extensível Firepower (FXOS) através do Access Control Server (ACS).

O chassi FXOS inclui as seguintes funções de usuário:

- Administrador - Acesso completo de leitura e gravação a todo o sistema. A conta admin padrão recebe essa função por padrão e não pode ser alterada.
- Somente leitura - Acesso somente leitura à configuração do sistema sem privilégios para modificar o estado do sistema.
- Operações - Acesso de leitura e gravação à configuração do NTP, configuração do Smart Call Home para Smart Licensing e registros do sistema, incluindo servidores de syslog e falhas. Leia o acesso ao restante do sistema.
- AAA - acesso de leitura e gravação a usuários, funções e configuração de AAA. Leia o acesso ao restante do sistema.

Através da CLI, isso pode ser visto da seguinte maneira:

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

Função:

Nome da função Priv

—

aaa aaa

admin admin

operações operacionais

somente leitura

Contribuído por Tony Ramirez, José Soto, engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do Firepower eXtensible Operating System (FXOS)
- Conhecimento da configuração do ACS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

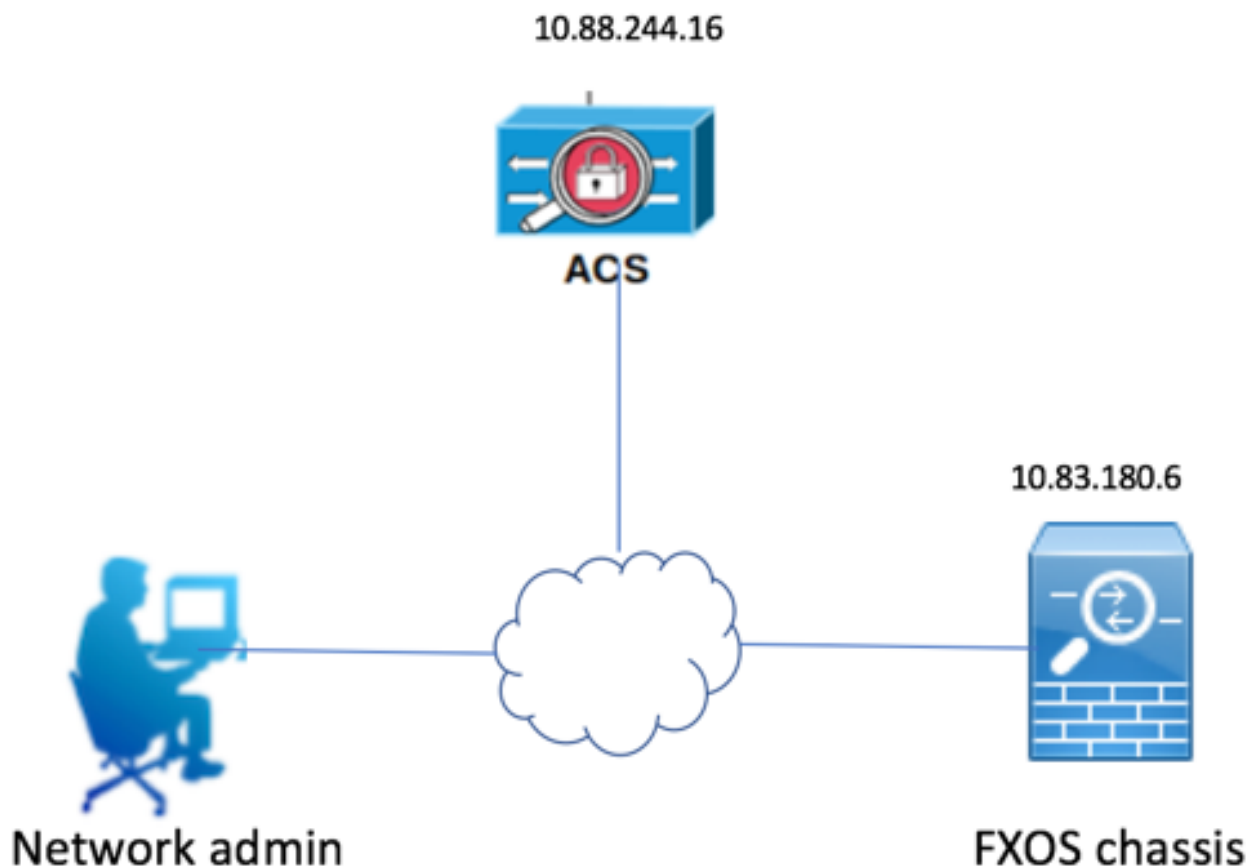
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurar

O objetivo da configuração é:

- Autentique os usuários que fazem login na GUI baseada na Web e no SSH do FXOS por meio do ACS.
- Autorize os usuários a fazer login na GUI baseada na Web e no SSH do FXOS de acordo com sua respectiva função de usuário por meio do ACS.
- Verifique o funcionamento correto da autenticação e autorização no FXOS por meio do ACS.

Diagrama de Rede



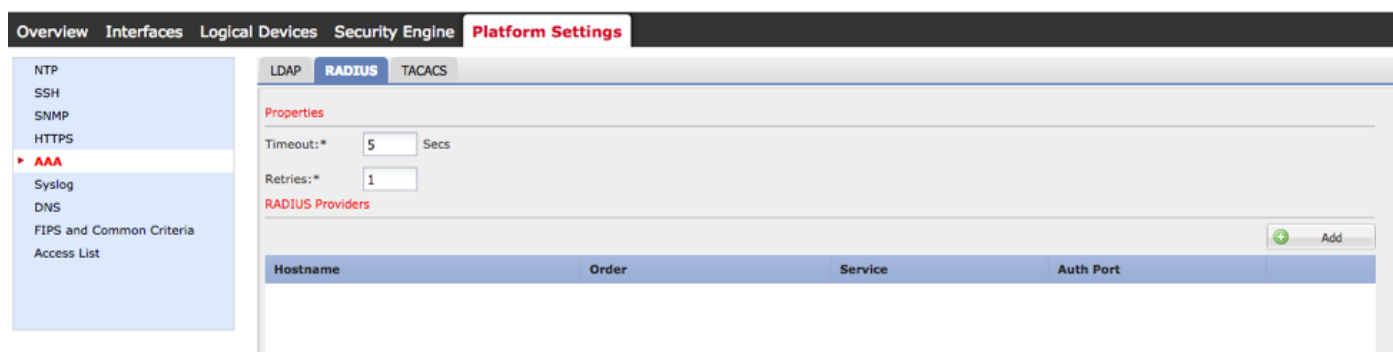
Configurações

Configurando o chassi FXOS

Criando um provedor RADIUS usando o gerenciador de chassi

Etapa 1. Navegue até Configurações da plataforma > AAA.

Etapa 2. Clique na guia RADIUS.



Etapa 3. Para cada provedor RADIUS que você deseja adicionar (até 16 provedores).

3.1. Na área RADIUS Providers, clique em **Add**.

3.2. Na caixa de diálogo Adicionar provedor RADIUS, insira os valores necessários.

3.3. Clique em **OK** para fechar a caixa de diálogo Adicionar provedor RADIUS.

Add RADIUS Provider

Hostname/FQDN(or IP Address):*

Order:*

Key: Set: No

Confirm Key:

Authorization Port:*

Timeout:* Secs

Retries:*

Etapa 4. Click **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

Etapa 5. Navegue até **System > User Management > Settings**.

Etapa 6. Em Autenticação padrão, escolha **RADIUS**.

Overview Interfaces Logical Devices Security Engine Platform Settings **System** Tools Help fossadmin

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

Criando um provedor RADIUS usando CLI

Etapa 1. Para habilitar a autenticação RADIUS, execute os seguintes comandos.

```
segurança de escopo fpr4120-TAC-A#
```

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

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

Etapa 2. Use o comando **show detail** para exibir os resultados.

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

Autenticação padrão:

Domínio administrativo: **Radius**

Domínio operacional: **Radius**

Período de atualização da sessão da Web (em segundos): 600

Tempo limite da sessão (em segundos) para sessões web, ssh, telnet: 600

Tempo limite da sessão absoluta (em segundos) para sessões web, ssh, telnet: 3600

Tempo limite da sessão do console serial (em segundos): 600

Tempo limite da sessão absoluta do console serial (em segundos): 3600

Grupo de servidores de Autenticação do Administrador:

Grupo de servidores de Autenticação Operacional:

Uso do segundo fator: No

Etapa 3. Para configurar os parâmetros do servidor RADIUS, execute os seguintes comandos.

```
segurança de escopo fpr4120-TAC-A#
```

```
raio de escopo fpr4120-TAC-A /security #
```

```
fpr4120-TAC-A /security/radius # entre no servidor 10.88.244.16
```

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

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

Digite a chave: *****

Confirme a chave: *****

Etapa 4. Use o comando **show detail** para exibir os resultados.

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

Servidor RADIUS:

Nome do host, FQDN ou endereço IP: 10.88.244.16

Descr:

Pedido: 1

Porta Aut.: 1812

Chave: ****

tempo limite: 5

Configurando o servidor ACS

Adicionando o FXOS como um recurso de rede

Etapa 1. Navegue até **Network Resources > Network Devices and AAA Clients**.

Etapa 2. Clique em **Criar**.

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

Etapa 3. Insira os valores necessários (Nome, Endereço IP, Tipo de dispositivo e Habilitar RADIUS e adicione a CHAVE).

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

Etapa 4. Clique em Submit.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.