

Firepower 拡張可能なオペレーティング システム (FXOS) 2.2: RADIUS を使用して ISE の遠隔管理のためのシャーシ認証/許可

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[FXOS シャーシの設定](#)

[ISE サーバの設定](#)

[確認](#)

[FXOS Chasis 確認](#)

[ISE 2.0 の検証](#)

[トラブルシューティング](#)

[関連情報](#)

概要

この資料に Identity Services Engine (ISE) で Firepower 拡張可能なオペレーティング システム (FXOS) シャーシのための RADIUS 認証および許可を設定する方法を記述されています。

FXOS シャーシは次のユーザの役割が含まれています:

- 管理者-システム全体に読み書きアクセスを完了して下さい。 デフォルト管理者アカウントこのロールはデフォルトで割り当てられ、変更することができません。
- 読み取り専用-システム 状態を変更する特権無しのシステム構成への読み取り専用アクセス。
- オペレーション-スマートな認可のための NTP 設定、Smart Call Home 設定、および syslog サーバおよびエラーを含むシステムログへの読み書きアクセス。 システムの他への読み取りアクセス。
- AAA : ユーザ、ロールおよび AAA 設定への読み書きアクセス。 システムの他への読み取りアクセス。

CLI によってこれは次の通り見られる場合があります:

```
fpr4120-TAC-A /security * #ロールを示して下さい
```

ロール:

```
ロール名 Priv
```

```
----- ----
```

AAA AAA

admin admin

オペレーション オペレーション

読み取り専用読み取り専用

、ホセ Soto トニー Remirez によって貢献される、Cisco TAC エンジニア。

前提条件

要件

次の項目に関する知識が推奨されます。

- Firepower 拡張可能なオペレーティング システム (FXOS) のナレッジ
- ISE 設定のナレッジ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Firepower 4120 セキュリティ アプライアンス バージョン 2.2
- バーチャル Cisco Identity Services Engine 2.2.0.470

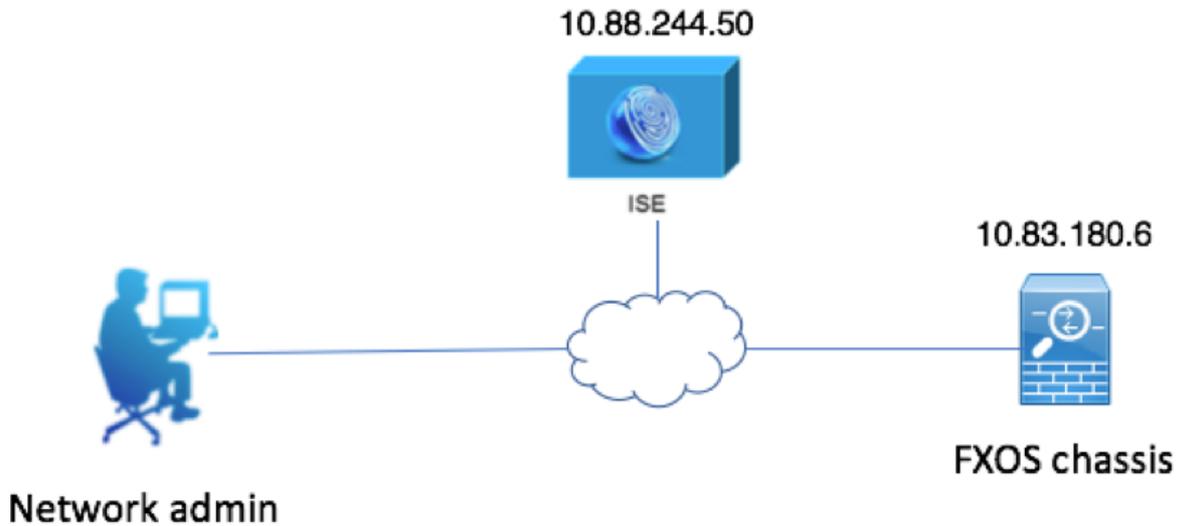
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

設定の目標はにあります:

- ISE によって FXOS の Webベース GUI および SSH にログインしているユーザを認証して下さい
- ISE によってそれぞれユーザの役割に従って FXOS の Webベース GUI および SSH にログインしているユーザを許可して下さい。
- ISE によって FXOS の認証 および 権限の正しい動作を確認して下さい

ネットワーク図



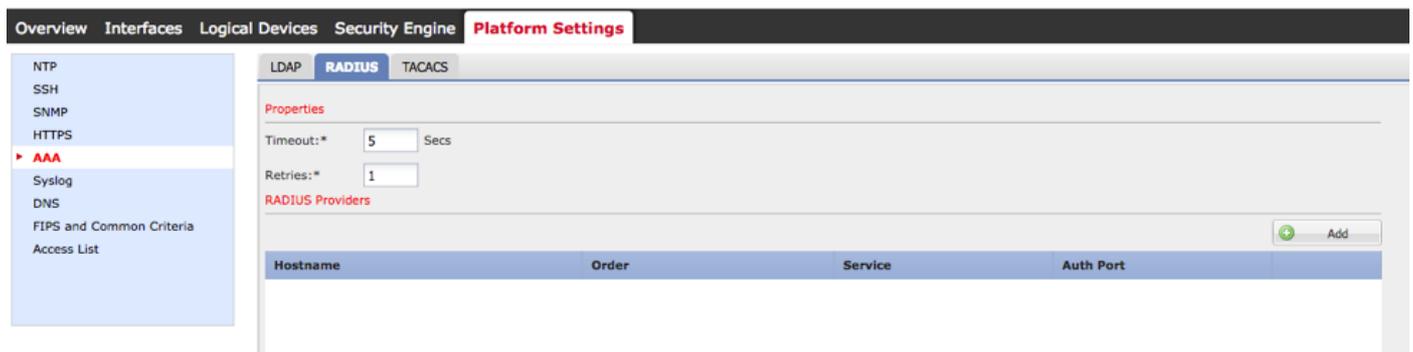
設定

FXOS シャーシの設定

シャーシ マネージャを使用する RADIUS プロバイダの作成

ステップ 1.プラットフォーム設定 > AAA へのナビゲート。

ステップ 2. RADIUS タブをクリックして下さい。



ステップ 3 追加したいと思う各 RADIUS プロバイダに関しては (16 人までのプロバイダ)。

3.1. RADIUS プロバイダ エリアで、『Add』 をクリックして下さい。

3.2. 追加 RADIUS プロバイダ ダイアログボックスが開いたら、必要な値を入力して下さい。

3.3. 追加 RADIUS プロバイダ ダイアログボックスを閉じるために『OK』 をクリックして下さい。

Edit 10.88.244.50

Hostname/FQDN(or IP Address):* 10.88.244.50

Order:* 1

Key: Set: Yes

Confirm Key:

Authorization Port:* 1812

Timeout:* 5 Secs

Retries:* 1

OK Cancel

ステップ 4. 『SAVE』 をクリックして下さい。

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

NTP
SSH
SNMP
HTTPS
▶ AAA
Syslog
DNS
FIPS and Common Criteria
Access List

LDAP **RADIUS** TACACS

Properties

Timeout:* 5 Secs

Retries:* 1

RADIUS Providers

| Hostname | Order | Service | Auth Port |
|--------------|-------|---------------|-----------|
| 10.88.244.50 | 1 | authorization | 1812 |

Save Cancel

ステップ 5. システム > ユーザー管理 > 設定へのナビゲート。

ステップ 6 デフォルトの認証の下で 『RADIUS』 を選択して下さい。

Overview Interfaces Logical Devices Security Engine Platform Settings

System Tools Help frosadmin

Configuration Licensing Updates **User Management**

Local Users **Settings**

Default Authentication: RADIUS *Local is fallback authentication method

Console Authentication: Local

Remote User Settings

Remote User Role Policy: Assign Default Role No-Login

CLI を使用する RADIUS プロバイダの作成

ステップ 1. RADIUS認証を有効にするために、次のコマンドを実行して下さい。

```
fpr4120-TAC-A# スコープ セキュリティ
```

```
fpr4120-TAC-A /security #スコープ デフォルトauth
```

```
fpr4120-TAC-A /security/default-auth は#レルム半径を設定しました
```

呼び出します。結果を表示する提示 detail コマンドを使用して下さい。

```
fpr4120-TAC-A /security/default-auth は#詳細を示します
```

デフォルトの認証:

Admin レルム: Radius

操作上レルム: Radius

Web セッション リフレッシュ期間 (秒): 600

Web のためのセッション タイムアウト (秒)、ssh、Telnetセッション: 600

Web のための絶対セッション タイムアウト (秒)、ssh、Telnetセッション: 3600

シリアルコンソール セッション タイムアウト (秒): 600

シリアルコンソール絶対セッション タイムアウト (秒): 3600

Admin 認証サーバ グループ:

操作上認証サーバ グループ:

第 2 ファクタの使用: なし

ステップ 3. RADIUSサーバ パラメータを設定するために次のコマンドを実行して下さい。

```
fpr4120-TAC-A# スコープ セキュリティ
```

```
fpr4120-TAC-A /security #スコープ半径
```

```
fpr4120-TAC-A /security/radius は#サーバ 10.88.244.50 を入力します
```

```
fpr4120-TAC-A /security/radius/server は#設定しました descr 「ISE サーバ」を
```

```
fpr4120-TAC-A /security/radius/server * # Set 鍵
```

キーを入力して下さい: *****

キーを確認して下さい: *****

ステップ 4 結果を表示する提示 detail コマンドを使用して下さい。

```
fpr4120-TAC-A /security/radius/server * #詳細を示して下さい
```

RADIUSサーバ:

ホスト名、FQDN または IP アドレス: 10.88.244.50

descr :

発注 : 1

Auth ポート: 1812

凡例 : ****

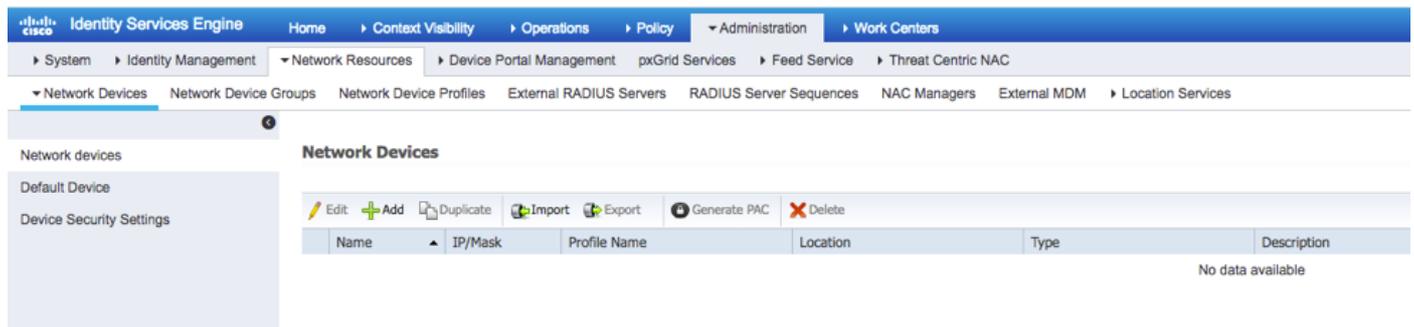
タイムアウト : 5

ISE サーバの設定

ネットワークリソースとして FXOS の追加

ステップ 1. Administration > ネットワークリソース > ネットワークデバイスへのナビゲート。

ステップ 2. 『Add』 をクリックして下さい



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Administration, the 'Network Resources' section is expanded, showing 'Network Devices' as the selected option. The 'Network Devices' page displays 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. Action buttons for Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete are visible above the table.

ステップ 3. 必要な値を (名前、IP アドレス、デバイスの種類およびイネーブル RADIUS は KEY を追加します) 入力し、 『SUBMIT』 をクリックして下さい。

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 > New Network Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol **RADIUS**

* Shared Secret

CoA Port

RADIUS DTLS Settings ⓘ

DTLS Required ⓘ

Shared Secret ⓘ

CoA Port

Issuer CA of ISE Certificates for CoA ⓘ

識別グループおよびユーザの作成

ステップ 1. Administration > アイデンティティ管理 > Groups > ユーザ識別グループにナビゲートして下さい。

ステップ 2. 『Add』 をクリックして下さい。

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

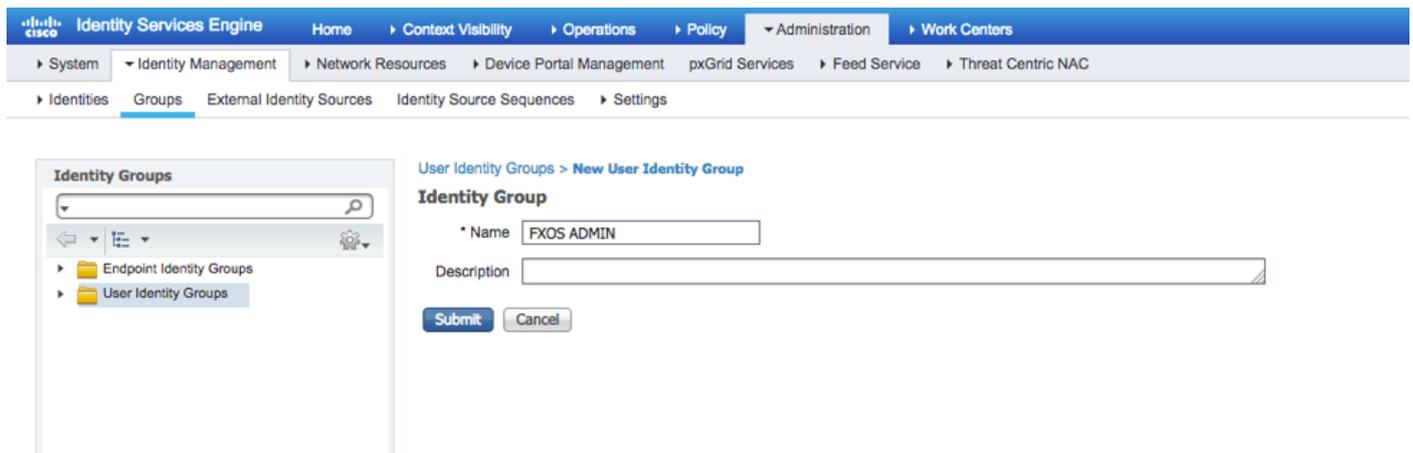
Endpoint Identity Groups

User Identity Groups

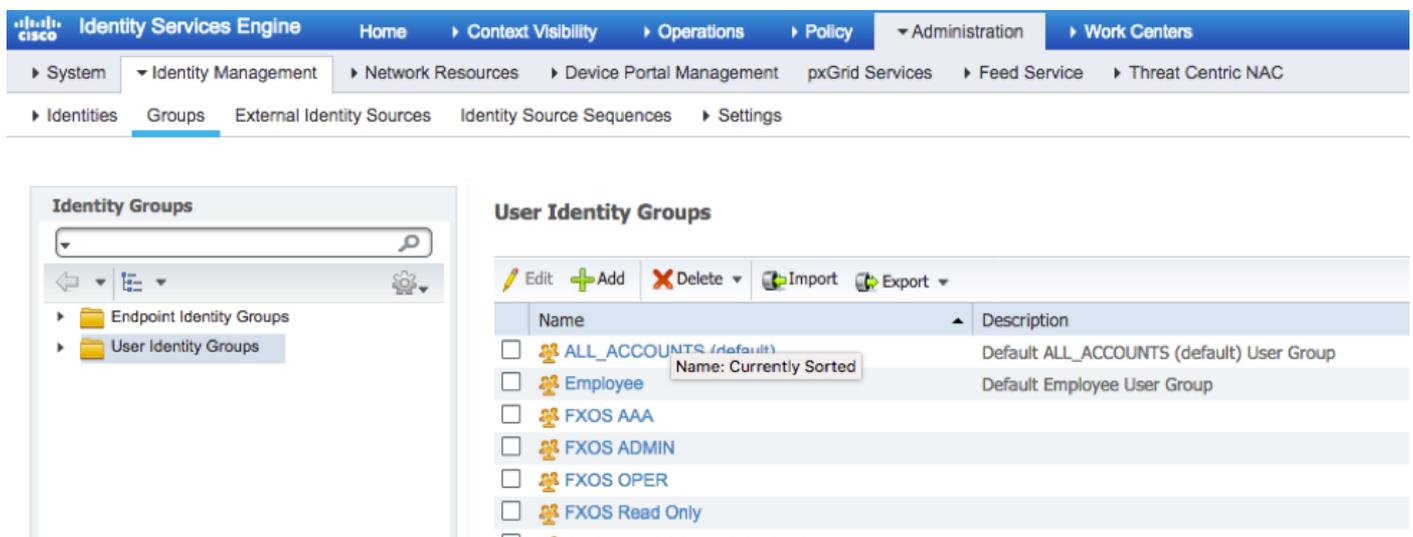
User Identity Groups

| 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 |

ステップ 3. 名前の値を入力し、『SUBMIT』をクリックして下さい。

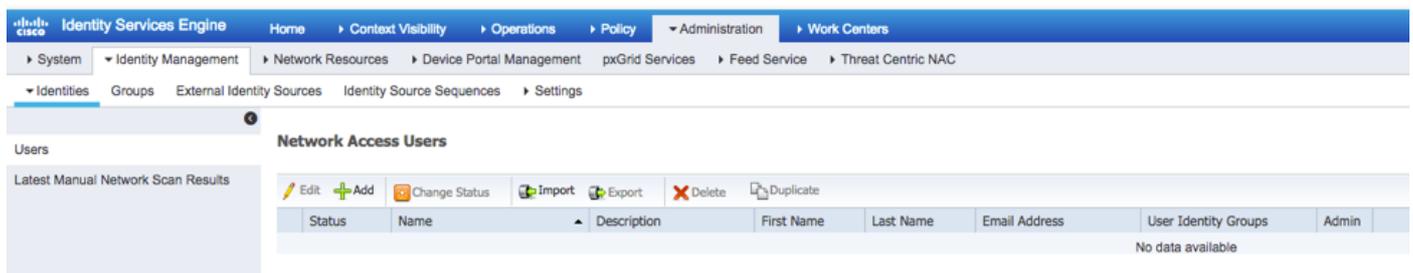


ステップ 4. すべての必須ユーザの役割のためのステップ 3 を繰り返して下さい。



ステップ 5. Administration > アイデンティティ管理 > 識別 > Users にナビゲートして下さい。

ステップ 6. 『Add』をクリックして下さい。



ステップ 7. 必要な値 (名前、ユーザグループ、パスワード) を入力して下さい。

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:

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: (yyyy-mm-dd)

User Groups

+

ステップ 8.必要なすべてのユーザ向けのステップ 6 を繰り返して下さい。

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 | |

各ユーザの役割のための許可プロファイルの作成

ステップ 1.ポリシー > ポリシー要素へのナビゲートは >> 許可 > 許可プロファイル生じます。

Standard Authorization Profiles
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

| Name | Profile | Description |
|--|---------|--|
| <input type="checkbox"/> Blackhole_Wireless_Access | Cisco | Default profile used to blacklist wireless devices. Ensu |
| <input type="checkbox"/> Cisco_IP_Phones | Cisco | Default profile used for Cisco Phones. |
| <input type="checkbox"/> Cisco_WebAuth | Cisco | Default Profile used to redirect users to the CWA port |
| <input type="checkbox"/> NSP_Onboard | Cisco | Onboard the device with Native Supplicant Provisionir |
| <input type="checkbox"/> Non_Cisco_IP_Phones | Cisco | Default Profile used for Non Cisco Phones. |
| <input type="checkbox"/> DenyAccess | | Default Profile with access type as Access-Reject |
| <input type="checkbox"/> PermitAccess | | Default Profile with access type as Access-Accept |

ステップ 2.許可プロファイルのためのすべての属性を一杯にして下さい。

2.1. Profile Name を設定して下さい。

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile: Cisco

2.2. 高度属性設定で次の CISCO-AV-PAIR を設定して下さい

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

Advanced Attributes Settings

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

2.3. [Save] をクリックします。

Save **Reset**

ステップ 3.次の Cisco AVペアを使用して残りのユーザの役割のためのステップ 2 を繰り返して

下さい

cisco-av-pair=shell: roles= " AAA」

cisco-av-pair=shell: roles= "オペレーション」

cisco-av-pair=shell: 」読み取り専用 roles= "

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="aaa" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="operations" +

▼ **Advanced Attributes Settings**

Cisco:cisco-av-pair = shell:roles="read-only" +

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Authentication Authorization Profiling Posture Client Provisioning > Policy Elements

Dictionaryes > Conditions > Results

Standard Authorization Profiles

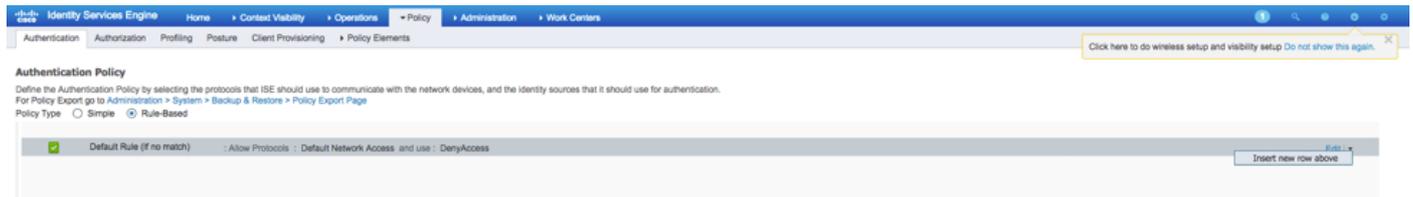
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Edit + Add Duplicate Delete

| <input type="checkbox"/> | Name | Profile |
|--------------------------|---------------------------|---------|
| <input type="checkbox"/> | Blackhole_Wireless_Access | Cisco |
| <input type="checkbox"/> | Cisco_IP_Phones | Cisco |
| <input type="checkbox"/> | Cisco_WebAuth | Cisco |
| <input type="checkbox"/> | FXOS-AAA-PROFILE | Cisco |
| <input type="checkbox"/> | FXOS-ADMIN-PROFILE | Cisco |
| <input type="checkbox"/> | FXOS-OPER-PROFILE | Cisco |
| <input type="checkbox"/> | FXOS-ReadOnly-PROFILE | Cisco |

認証ポリシーの作成

ステップ 1.ポリシー > 認証へのナビゲートは > およびルールをどこに作成したいと思うか矢印をの隣で編集しをクリックします。



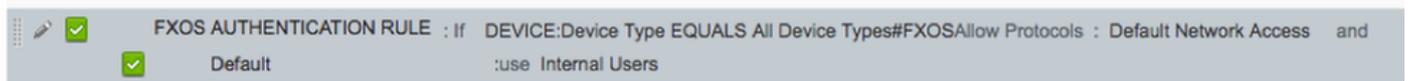
呼び出します。設定は簡単です;それはされた粒状である場合もありますが、この例のためにデバイスの種類を使用します:

[Name] : FXOS 認証ルール

IF は属性/値を『New』を選択します: デバイス: デバイスの種類はすべての装置タイプ #FXOS に匹敵します

割り当てプロトコル: デフォルトネットワーク アクセス

使用: 内部ユーザ



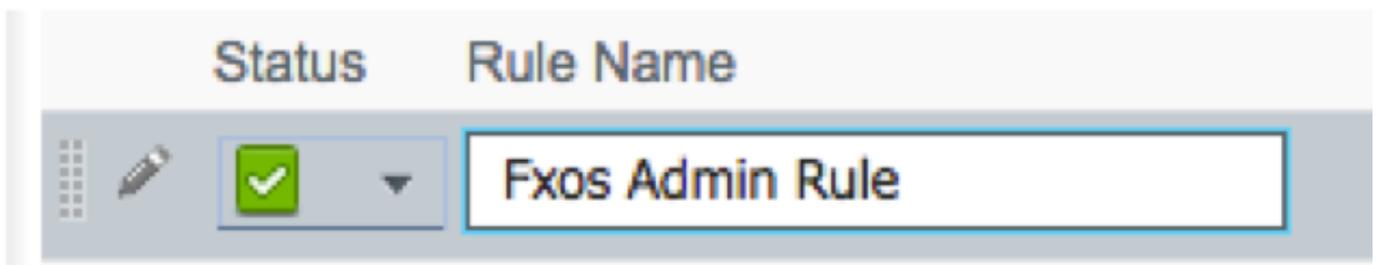
承認ポリシーの作成

ステップ 1.ポリシー > 許可へのナビゲートは > およびルールをどこに作成したいと思うか編集するために矢印ネットをクリックします。

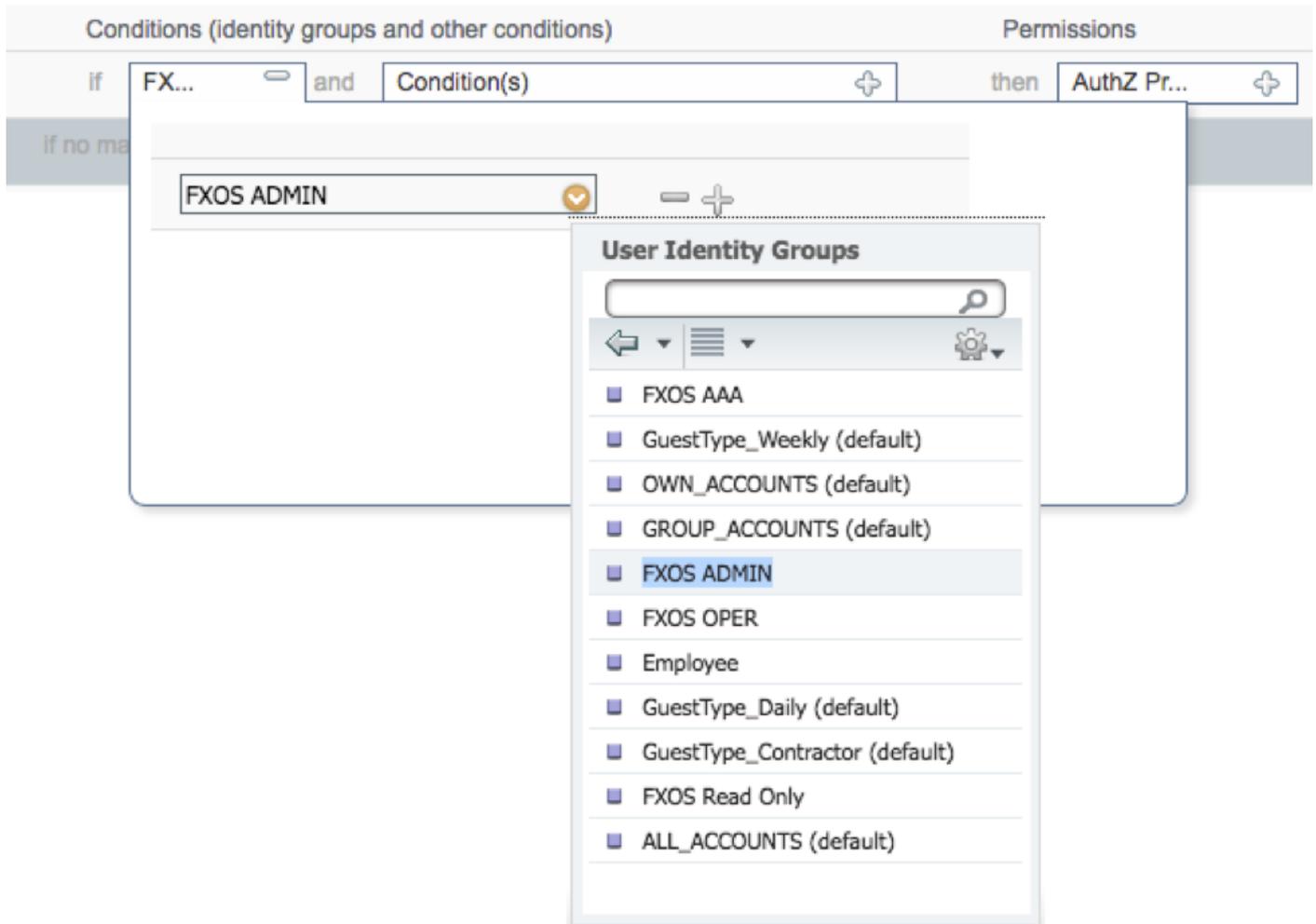


ステップ 2.必須パラメータの承認規則の値を入力して下さい。

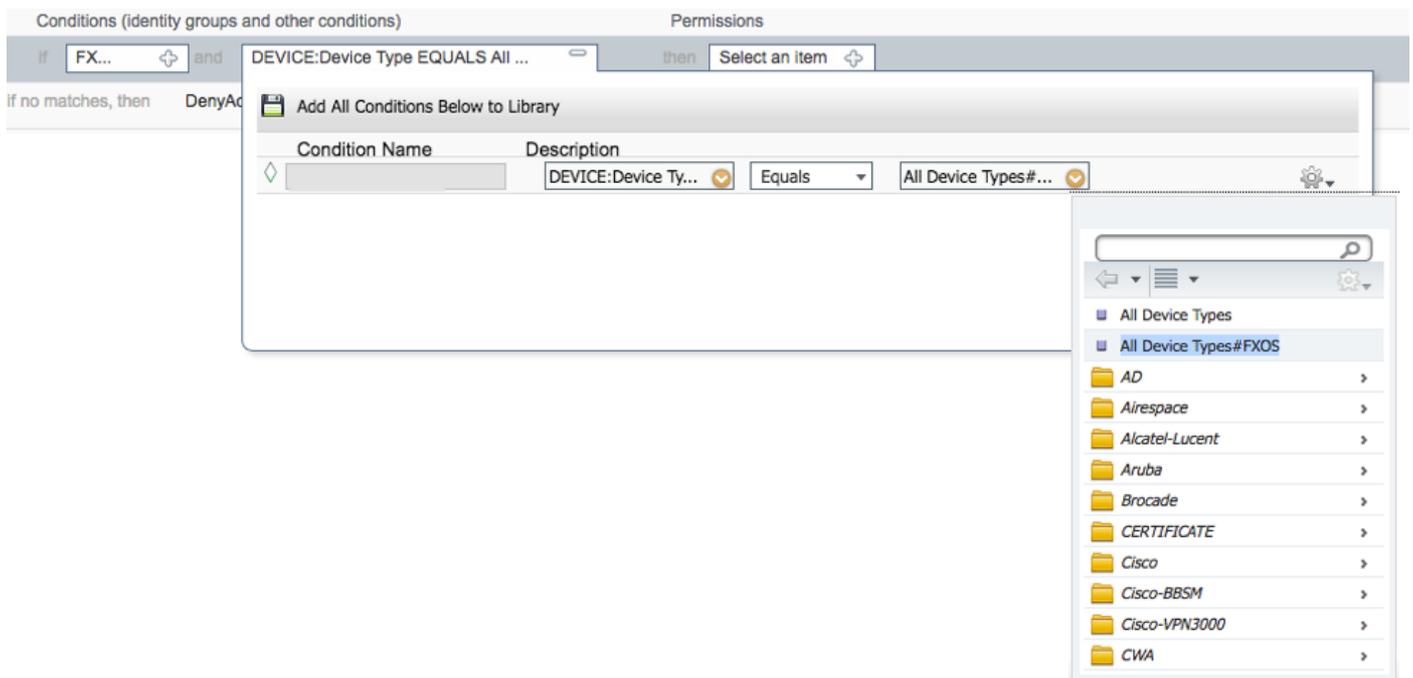
2.1. [Rule Name] : Fxos <USER ROLE> ルール。



2.2. 条件 ユーザ識別グループ > 選定された <USER ROLE>。



2.3. および: 新しい状態 > デバイスを作成して下さい: デバイスの種類は**すべての装置タイプ #FXOS**に匹敵します。



2.4. [Permissions] : 規格は > プロファイル ユーザの役割の選択します

Permissions

then FXOS-A...

FXOS-ADMIN-PROFILE

Standard

- Blackhole_Wireless_Access
- Cisco_IP_Phones
- Cisco_WebAuth
- DenyAccess
- FXOS-AAA-PROFILE
- FXOS-ADMIN-PROFILE**
- FXOS-OPER-PROFILE
- FXOS-ReadOnly-PROFILE
- NSP_Onboard
- Non_Cisco_IP_Phones
- PermitAccess

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|-------------------------------------|-----------------|--|-------------------------|
| <input checked="" type="checkbox"/> | Fxos Admin Rule | if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ADMIN-PROFILE |

ステップ 3.すべてのユーザの役割のためのステップ 2 を繰り返して下さい。

| Status | Rule Name | Conditions (identity groups and other conditions) | Permissions |
|-------------------------------------|---------------------|--|----------------------------|
| <input checked="" type="checkbox"/> | Fxos Admin Rule | if FXOS ADMIN AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ADMIN-PROFILE |
| <input checked="" type="checkbox"/> | Fxos AAA Rule | if FXOS AAA AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-AAA-PROFILE |
| <input checked="" type="checkbox"/> | Fxos Oper Rule | if FXOS OPER AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-OPER-PROFILE |
| <input checked="" type="checkbox"/> | Fxos Read only Rule | if FXOS Read Only AND DEVICE:Device Type EQUALS All Device Types#FXOS | then FXOS-ReadOnly-PROFILE |
| <input checked="" type="checkbox"/> | Default | if no matches, then DenyAccess | |

ステップ 4.ページの一番下に『SAVE』 をクリックして下さい。

Save

Reset

確認

今各ユーザをテストし、割り当てられたユーザの役割を確認することができます。

FXOS Chasis 確認

1. FXOS シャーシへの Telnet か SSH および ISE の作成されたユーザの何れかを使用するログオン。

ユーザ名 : fxosadmin

パスワード :

fpr4120-TAC-A# スコープ セキュリティ

fpr4120-TAC-A /security は#リモートユーザ 詳細を示します

リモートユーザ fxosaaa:

説明 :

ユーザの役割:

[Name] : AAA

[Name] : 読み取り専用

リモートユーザ fxosadmin:

説明 :

ユーザの役割:

[Name] : admin

[Name] : 読み取り専用

リモートユーザ fxosoper:

説明 :

ユーザの役割:

[Name] : 操作

[Name] : 読み取り専用

リモートユーザ fxosro:

説明 :

ユーザの役割:

[Name] : 読み取り専用

FXOS シャーシ cli 入力されたユーザ名によっては割り当てられたユーザの役割のために承認されたコマンドだけを表示します。

管理者ユーザ ロール。

fpr4120-TAC-A /security #か。

確認します確認して下さい

オフ ユーザ セッションはユーザセッションを解決します

作成します管理対象オブジェクトを作成して下さい

削除管理対象オブジェクトを削除して下さい

ディセーブル無効サービス

イネーブル有効サービス

入力します管理対象オブジェクトを入力して下さい

スコープは現在のモードを変更します

セットのプロパティ値を設定して下さい

Show system information を示して下さい

アクティブ cimc セッションを終了して下さい

fpr4120-TAC-A# は fxos を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

fpr4120-TAC-A (fxos) #

読み取り専用ユーザの役割。

fpr4120-TAC-A /security #か。

スコープは現在のモードを変更します

セットのプロパティ値を設定して下さい

Show system information を示して下さい

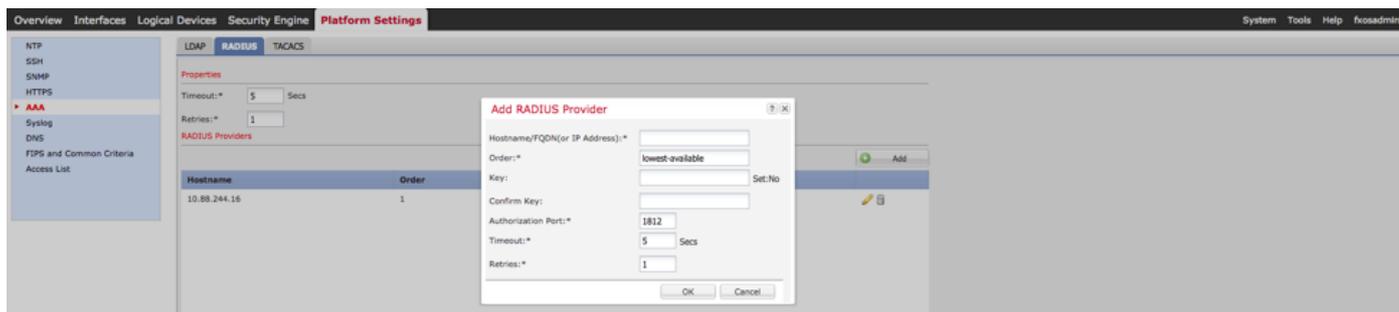
fpr4120-TAC-A# は fxos を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

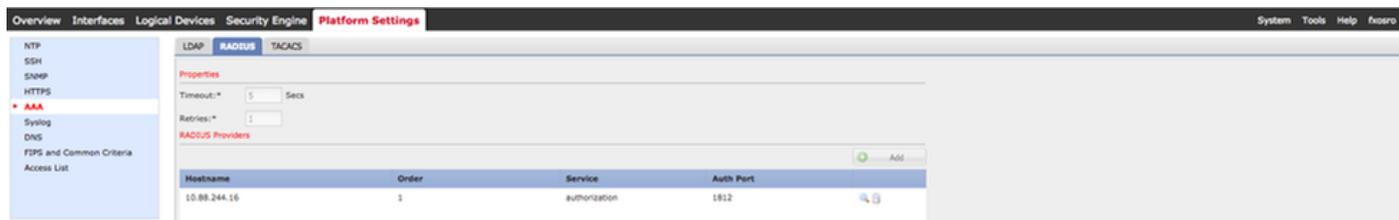
権限%のロールのために否定される

2. ISE の作成されたユーザの何れかを使用して FXOS シャーシ IP アドレスおよびログオンに参照して下さい。

管理者ユーザ ロール。



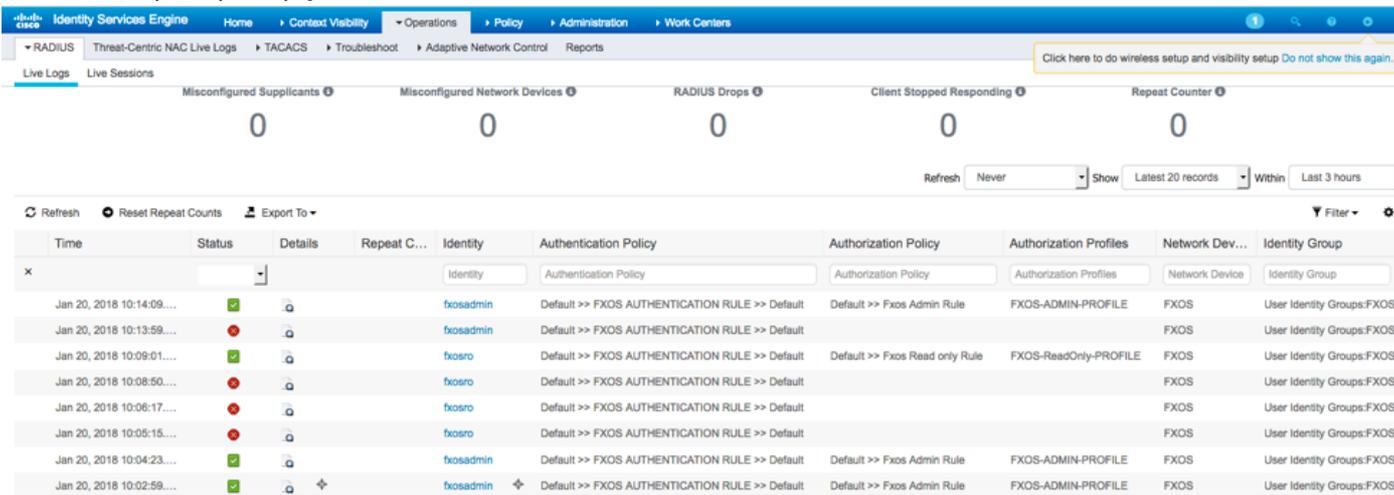
読み取り専用ユーザの役割。



注: Add ボタンが選択不可能になることに注意して下さい。

ISE 2.0 の検証

1. オペレーション > RADIUS へのナビゲート > ライブ ログ。成功したおよび試行失敗を見られますはずです。



トラブルシューティング

debug aaa authentication および許可は FXOS cli の次のコマンドを実行します。

fpr4120-TAC-A# は **fxos** を接続します

fpr4120-TAC-A (fxos) #デバッグ AAA AAA 要求

fpr4120-TAC-A (fxos) #デバッグ AAA イベント

fpr4120-TAC-A (fxos) #デバッグ AAA エラー

fpr4120-TAC-A (fxos) # term mon

認証の成功試みが、次の出力を見た後。

20 年 1 月 2018 日 17:18:02.410275 AAA: 認証のための aaa_req_process。 セッション 0 無し

20 年 1 月 2018 日 17:18:02.410297 AAA: aaa_req_process: appln からの一般 AAA 要求: ログオン
appln_subtype: デフォルト

20 年 1 月 2018 日 17:18:02.410310 AAA: try_next_aaa_method

20 年 1 月 2018 日 17:18:02.410330 AAA: 設定される総方式は 1、試みられるべき現在のインデックスです 0 です

20 年 1 月 2018 日 17:18:02.410344 AAA: handle_req_using_method

20 年 1 月 2018 日 17:18:02.410356 AAA: AAA_METHOD_SERVER_GROUP

20 年 1 月 2018 日 17:18:02.410367 AAA: aaa_sg_method_handler グループ = 半径

20 年 1 月 2018 日 17:18:02.410379 AAA: この機能に通じる sg_protocol の使用

20 年 1 月 2018 日 17:18:02.410393 AAA: RADIUSサービスへ要求を送信 すること

20 年 1 月 2018 日 17:18:02.412944 AAA: mts_send_msg_to_prot_daemon: ペイロード長 = 374

20 年 1 月 2018 日 17:18:02.412973 AAA: セッション: セッション表 1 に追加される 0x8dfd68c

20 年 1 月 2018 日 17:18:02.412987 AAA: 成功する設定された方式グループ

20 年 1 月 2018 日 17:18:02.656425 AAA: aaa_process_fd_set

20 年 1 月 2018 日 17:18:02.656447 AAA: aaa_process_fd_set: aaa_q の mtscallback

20 年 1 月 2018 日 17:18:02.656470 AAA: mts_message_response_handler: mts 応答

20 年 1 月 2018 日 17:18:02.656483 AAA: prot_daemon_reponse_handler

20 年 1 月 2018 日 17:18:02.656497 AAA: セッション: セッション表 0 から取除かれる 0x8dfd68c

20年1月2018日 17:18:02.656512 AAA: is_aaa_resp_status_success ステータス = 1

20年1月2018日 17:18:02.656525 AAA: is_aaa_resp_status_success は TRUE です

20年1月2018日 17:18:02.656538 AAA: 認証のための aaa_send_client_response。 session->flags=21. aaa_resp->flags=0.

20年1月2018日 17:18:02.656550 AAA: AAA_REQ_FLAG_NORMAL

20年1月2018日 17:18:02.656577 AAA: 正常な mts_send_response

20年1月2018日 17:18:02.700520 AAA: aaa_process_fd_set: aaa_accounting_q の mtscallback

20年1月2018日 17:18:02.700688 AAA: 古いオペレーション コード:
accounting_interim_update

20年1月2018日 17:18:02.700702 AAA: aaa_create_local_acct_req: user=、 session_id=、
log=added ユーザ fxosro

20年1月2018日 17:18:02.700725 AAA: 説明のための aaa_req_process。 セッション 0 無し

20年1月2018日 17:18:02.700738 AAA: MTS 要求参照は NULL です。 ローカル要求

20年1月2018日 17:18:02.700749 AAA: AAA_REQ_RESPONSE_NOT_NEEDED の設定

20年1月2018日 17:18:02.700762 AAA: aaa_req_process: appln からの一般 AAA 要求: デフォルト
appln_subtype: デフォルト

20年1月2018日 17:18:02.700774 AAA: try_next_aaa_method

20年1月2018日 17:18:02.700798 AAA: デフォルト デフォルトのために設定される方式無し

20年1月2018日 17:18:02.700810 AAA: これのために利用可能な設定無し要求

20年1月2018日 17:18:02.700997 AAA: 説明のための aaa_send_client_response。 session->flags=254. aaa_resp->flags=0.

20年1月2018日 17:18:02.701010 AAA: 古いライブラリの説明要求のための応答は成功として
返されます

20年1月2018日 17:18:02.701021 AAA: この要求のために必要とされない応答

20年1月2018日 17:18:02.701033 AAA: AAA_REQ_FLAG_LOCAL_RESP

20年1月2018日 17:18:02.701044 AAA: aaa_cleanup_session

20年1月2018日 17:18:02.701055 AAA: aaa_req は解放する必要があります。

20年1月2018日 17:18:02.701067 AAA: 成功するフォールバック方式ローカル

20年1月2018日 17:18:02.706922 AAA: aaa_process_fd_set

20年1月2018日 17:18:02.706937 AAA: aaa_process_fd_set: aaa_accounting_q の mtscallback

20年1月2018日17:18:02.706959 AAA: 古いオペレーションコード:
accounting_interim_update

20年1月2018日17:18:02.706972 AAA: aaa_create_local_acct_req: user=、session_id=、
log=added ユーザ: コールへの fxosro: 読み取り専用

失敗した認証試みが、次の出力を見た後。

20年1月2018日17:15:18.102130 AAA: aaa_process_fd_set

20年1月2018日17:15:18.102149 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日17:15:18.102267 AAA: aaa_process_fd_set

20年1月2018日17:15:18.102281 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日17:15:18.102363 AAA: aaa_process_fd_set

20年1月2018日17:15:18.102377 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日17:15:18.102456 AAA: aaa_process_fd_set

20年1月2018日17:15:18.102468 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日17:15:18.102489 AAA: mts_aaa_req_process

20年1月2018日17:15:18.102503 AAA: 認証のための aaa_req_process。セッション 0 無し

20年1月2018日17:15:18.102526 AAA: aaa_req_process: appln からの一般 AAA 要求: ログオン
appln_subtype: デフォルト

20年1月2018日17:15:18.102540 AAA: try_next_aaa_method

20年1月2018日17:15:18.102562 AAA: 設定される総方式は 1、試みられるべき現在のインデックスです 0 です

20年1月2018日17:15:18.102575 AAA: handle_req_using_method

20年1月2018日17:15:18.102586 AAA: AAA_METHOD_SERVER_GROUP

20年1月2018日17:15:18.102598 AAA: aaa_sg_method_handler グループ = 半径

20年1月2018日17:15:18.102610 AAA: この機能に通じる sg_protocol の使用

20年1月2018日17:15:18.102625 AAA: RADIUSサービスへ要求を送信 すること

20年1月2018日17:15:18.102658 AAA: mts_send_msg_to_prot_daemon: ペイロード長 = 371

20年1月2018日17:15:18.102684 AAA: セッション: セッション表 1 に追加される 0x8dfd68c

20年1月2018日17:15:18.102698 AAA: 成功する設定された方式グループ

20年1月2018日17:15:18.273682 AAA: aaa_process_fd_set

20年1月2018日 17:15:18.273724 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日 17:15:18.273753 AAA: mts_message_response_handler: mts 応答

20年1月2018日 17:15:18.273768 AAA: prot_daemon_reponse_handler

20年1月2018日 17:15:18.273783 AAA: セッション: セッション表 0 から取除かれる 0x8dfd68c

20年1月2018日 17:15:18.273801 AAA: is_aaa_resp_status_success ステータス = 2

20年1月2018日 17:15:18.273815 AAA: is_aaa_resp_status_success は TRUE です

20年1月2018日 17:15:18.273829 AAA: 認証のための aaa_send_client_response。 session->flags=21. aaa_resp->flags=0.

20年1月2018日 17:15:18.273843 AAA: AAA_REQ_FLAG_NORMAL

20年1月2018日 17:15:18.273877 AAA: 正常な mts_send_response

20年1月2018日 17:15:18.273902 AAA: aaa_cleanup_session

20年1月2018日 17:15:18.273916 AAA: 要求メッセージの mts_drop

20年1月2018日 17:15:18.273935 AAA: aaa_req は解放する必要があります。

20年1月2018日 17:15:18.280416 AAA: aaa_process_fd_set

20年1月2018日 17:15:18.280443 AAA: aaa_process_fd_set: aaa_q の mtscallback

20年1月2018日 17:15:18.280454 AAA: aaa_enable_info_config: AAA Login エラーメッセージのための GET_REQ

20年1月2018日 17:15:18.280460 AAA: 設定 オペレーションの戻り値を取得される: 未知セキュリティ項目

関連情報

FX-OS cli の Ethalyzer コマンドはパスワードのパスワードのために TACACS/RADIUS 認証がイネーブルになっているときプロンプト表示します。この動作はバグによって引き起こされます。

バグID: [CSCvg87518](#)