

ISEサーバを使用したCIMCでのTACACS+認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[権限関連付けのTACACS+サーバ側設定](#)

[ISEの設定要件](#)

[CIMCでのTACACS+の設定](#)

[確認](#)

[CIMCのCLIからの設定の確認](#)

[トラブルシューティング](#)

[ISEのトラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Integrated Management Controller(CIMC)でのTerminal Access Controller Access-Control System Plus(TACACS+)認証の設定について説明します。

TACACS+は、一般に中央サーバでネットワークデバイスを認証するために使用されます。リリースバージョン4.1(3b)以降、Cisco IMCはTACACS+認証をサポートしています。CIMCでのTACACS+サポートにより、デバイスにアクセスできる複数のユーザアカウントを管理する手間が軽減されます。この機能は、ユーザのクレデンシャルを定期的に変更し、ユーザアカウントをリモートで管理するのに役立ちます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco インテグレートド マネージメント コントローラ (CIMC)
- Terminal Access Controller Access-Control System Plus(TACACS+)

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いています。

- UCSC-C220-M4S
- CIMCバージョン : 4.1(3b)

- Cisco Identity Services Engine(ISE)バージョン3.0.0.458

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

権限関連付けのTACACS+サーバ側設定

ユーザの特権レベルは、そのユーザに対して設定されたcisco-av-pair値に基づいて計算されます。cisco-av-pairはTACACS+サーバ上に作成する必要があり、ユーザはデフォルトのTACACS+属性を使用できません。次に示す3つの構文は、cisco-av-pair属性でサポートされます

管理権限の場合：

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

ユーザー特権の場合：

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

読み取り専用権限の場合：

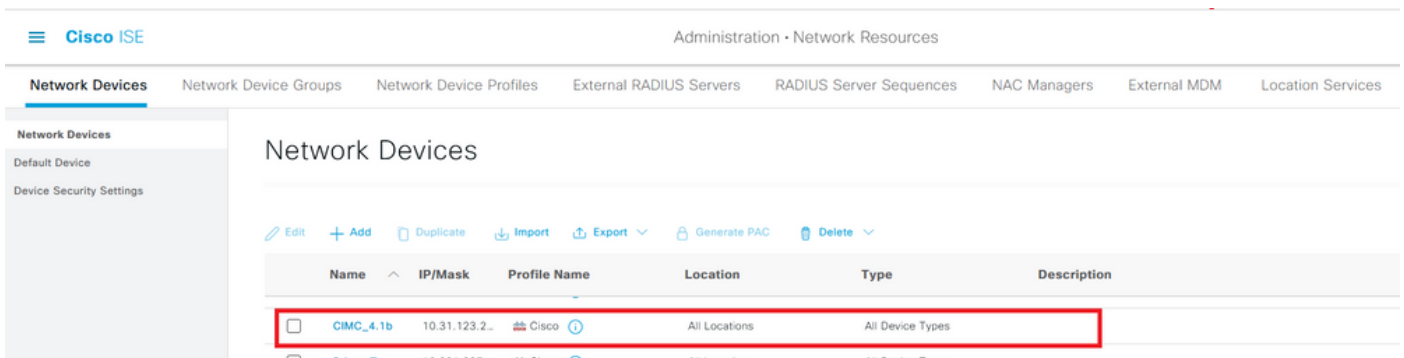
```
cisco-av-pair=shell:roles="read-only"
```

他のデバイスをサポートするには、他のロールを追加する必要がある場合は、カンマを区切り文字として追加できません。たとえば、UCSMはaaaをサポートしているため、shell:roles="admin,aaa"を設定できて、CIMCはこの形式を受け入れます。

注：TACACS+サーバでcisco-av-pairが設定されていない場合、そのサーバを持つユーザには読み取り専用権限が与えられます。

ISEの設定要件

サーバの管理IPをISEネットワークデバイスで許可する必要があります。



The screenshot shows the Cisco ISE Administration interface. The main content area is titled "Network Devices" and contains a table with the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> CIMC_4.1b	10.31.123.2	Cisco	All Locations	All Device Types	
<input type="checkbox"/> Prima Test	10.201.223	Cisco	All Locations	All Device Types	

CIMCに入力する共有秘密パスワード。

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server

Network Devices

Default Device

Device Security Settings

Network Devices List > CIMC_4.1b

Network Devices

* Name CIMC_4.1b

Description

IP Address * IP: 10.31.123.27 / 32

* Device Profile Cisco

Model Name

Software Version

* Network Device Group

Location All Locations Set To Default

IPSEC No Set To Default

Device Type All Device Types Set To Default

TEST TEST Set To Default

 RADIUS Authentication Settings TACACS Authentication Settings

Shared Secret

Cisc0123

Hide

Retire

管理者権限を持つcisco-av-pair属性を持つシェルプロファイル。

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

Conditions >
Network Conditions >
Results >
Allowed Protocols
TACACS Command Sets
TACACS Profiles

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

+ Add Trash Edit

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

CIMCでのTACACS+の設定

ステップ1:[Admin] > [User Management] > [TACACS+]に移動します。

ステップ2 : チェックボックスをオンにしてTACACS+を有効にします

ステップ3 : テーブルで指定した6行のいずれかで新しいサーバを追加できます。次の図に示すように、行をクリックするか、行を選択し、表の上にある編集ボタンをクリックします。

TACACS+ Properties

Enabled: 1 ←

Fallback only on no connectivity:

Timeout (for each server): (5 - 30 Seconds)

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key
<input type="radio"/> 1			
<input type="radio"/> 2			
<input type="radio"/> 3			
<input type="radio"/> 4			
<input type="radio"/> 5			
<input type="radio"/> 6			

注：ユーザがTACACS+フォールバックをno connectivityオプションで有効にしている場合、CIMCは最初の認証優先順位を常にTACACS+に設定する必要があることを強制します。そうしないと、フォールバック設定が無関係になる可能性があります。

ステップ4:IPアドレスまたはホスト名、ポート、サーバキー/共有秘密を入力し、設定を保存します。

Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key	Confirm Server Key
1	<input type="text" value="10.31.126.220"/>	<input type="text" value="49"/>	<input type="text" value="*****"/>	<input type="text" value="*****"/>
2				
3				
4				
5				
6				

Save | Cancel

Cisco IMCは最大6台のTACACS+リモートサーバをサポートします。ユーザが正常に認証されると、ユーザ名に(TACACS+)が追加されます。

0
 tacacs_user (TACACS+)@10.24.92.202 - C220-WZP22460WCD

Refresh | ? i

これは、セッション管理にも表示されます

Sessions

Selected 0 / Total 1 ⚙

Terminate Session				
	Session ID	User Name	IP Address	Session Type
<input type="checkbox"/>	81	tacacs_user (TACACS+)	10.24.92.202	webgui

確認

- CIMCには最大6台のTACACS+サーバを設定できます。
- サーバに関連付けられる秘密キーの長さは最大64文字です。
- タイムアウトは5 ~ 30秒の間で設定できます (LDAPに従って最大180秒と評価されます)。
- TACACS+サーバがサービス名を使用してcisco-av-pairを作成する必要がある場合は、サービス名としてLog inを使用する必要があります。
- 設定を変更するRedfishのサポートはありません。

CIMCのCLIからの設定の確認

- TACACS+が有効になっているかどうかを確認します。

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- サーバごとの設定の詳細を確認します。

```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: *****
Server Port: 49
```

トラブルシューティング

- CIMCからTACACS+サーバのIPに到達でき、ポートが正しく設定されていることを確認します。
- TACACS+サーバでcisco-av-pairが正しく設定されていることを確認します。
- TACACS+サーバ (IPおよびポート) が到達可能かどうかを確認します。
- 秘密キーまたはクレデンシャルが、TACACS+サーバで設定されている秘密キーと一致していることを確認します。
- TACACS+を使用してログインできるが、読み取り専用の権限しか持たない場合は、cisco-av-pairがTACACS+サーバで正しい構文を持っているかどうかを確認します。

ISEのトラブルシューティング

- 認証試行の1つに対するTacacs Liveログを確認します。状態は合格である必要があります。

Overview

Request Type	Authorization
Status	Pass
Session Key	ise30baaamex/408819883/155352
Message Text	Device-Administration: Session Authorization succeeded
Username	tacacs_user
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Shell Profile	Test_Shell
Matched Command Set	
Command From Device	

- 応答に正しいcisco-av-pair属性が設定されていることを確認します。

Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

関連情報

- [TACACS+認証Cisco UCS-C](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)
- [ISE 2.0 の設定 : AD グループ メンバーシップに基づく IOS TACACS+ 認証およびコマンド認可の設定例](#)