

Configurazione dell'autenticazione TACACS+ su CIMC con ISE Server

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Configurazione lato server TACACS+ per l'associazione dei privilegi](#)

[Requisiti di configurazione ISE](#)

[Configurazione TACACS+ su CIMC](#)

[Verifica](#)

[Verifica della configurazione dalla CLI in CIMC](#)

[Risoluzione dei problemi](#)

[Risoluzione dei problemi ISE](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la configurazione dell'autenticazione Access-Control System Plus (TACACS+) di Terminal Access Controller su Cisco Integrated Management Controller (CIMC).

TACACS+ viene comunemente utilizzato per autenticare i dispositivi di rete con un server centrale. Dalla versione 4.1(3b), Cisco IMC supporta l'autenticazione TACACS+. Il supporto TACACS+ su CIMC semplifica la gestione di più account utente che hanno accesso al dispositivo. Questa funzionalità consente di modificare periodicamente le credenziali dell'utente e di gestire gli account utente in remoto.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Integrated Management Controller (CIMC)
- Access-Control System Plus di Terminal Access Controller (TACACS+)

Componenti usati

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

- UCS-C220-M4S

- Versione CIMC: 4.1, paragrafo 3 ter
- Cisco Identity Services Engine (ISE) versione 3.0.0.458

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

Configurazione lato server TACACS+ per l'associazione dei privilegi

Il livello di privilegio dell'utente viene calcolato in base al valore **cisco-av-pair** configurato per tale utente. È necessario creare una **coppia cisco-av** sul server TACACS+ e gli utenti non possono usare alcun attributo TACACS+ predefinito. Per l'attributo **cisco-av-pair** sono supportate le tre sintassi seguenti

Per il privilegio **admin**:

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

Per il privilegio **utente**:

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

Per il privilegio di **sola lettura**:

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

Per supportare altri dispositivi, se è necessario aggiungere altri ruoli, è possibile aggiungerli con una virgola come separatore. Ad esempio, UCSM supporta **aaa**, quindi è possibile configurare **shell:roles="admin,aaa"** e CIMC accetta questo formato.

Nota: se **cisco-av-pair** non è configurato sul server TACACS+, un utente con quel server ha un privilegio di **sola lettura**.

Requisiti di configurazione ISE

L'IP di gestione del server deve essere consentito sui dispositivi di rete ISE.

The screenshot shows the Cisco ISE Administration interface. The main content area is titled 'Network Devices' and contains a table with the following columns: Name, IP/Mask, Profile Name, Location, Type, and Description. The first row in the table is highlighted with a red border and contains the following data:

Name	IP/Mask	Profile Name	Location	Type	Description
CIMC_4.1b	10.31.123.2...	Cisco	All Locations	All Device Types	

Password segreta condivisa da immettere in CIMC.

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](#)

Shell Profile con attributo **cisco-av-pair** con autorizzazioni di amministratore.

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*

Configurazione TACACS+ su CIMC

Passaggio 1. Selezionare **Admin > User Management > TACACS+**

Passaggio 2. Selezionare la casella di controllo per abilitare **TACACS+**

Passaggio 3. È possibile aggiungere un nuovo server in una delle 6 righe specificate nella tabella. Fate clic sulla riga o selezionatela e fate clic sul pulsante **Modifica** sopra la tabella, come mostrato nell'immagine.

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 checked="" type="radio"/> 1			
<input type="radio"/> 2			
<input type="radio"/> 3			
<input type="radio"/> 4			
<input type="radio"/> 5			
<input type="radio"/> 6			

Nota: Nel caso in cui un utente abbia abilitato il fallback di TACACS+ su nessuna opzione di connettività, CIMC applica che la priorità della prima autenticazione deve sempre essere impostata su TACACS+ altrimenti la configurazione del fallback potrebbe diventare irrilevante.

Passaggio 4. Inserire l'indirizzo IP o il nome host, la porta e la chiave del server/il segreto condiviso e **salvare** la configurazione.

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				

Save | Cancel

3 ↑

Cisco IMC supporta fino a sei server remoti TACACS+. Una volta completata l'autenticazione, al nome utente viene aggiunto (TACACS+).

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

Refresh | ? | i

Questa condizione viene visualizzata anche in Gestione sessioni

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	

Verifica

- È possibile configurare un massimo di 6 server TACACS+ sul CIMC.
- La lunghezza massima della chiave segreta associata al server è 64 caratteri.
- Il timeout può essere configurato tra 5 e 30 secondi (il che corrisponde al massimo a 180 secondi per essere in linea con LDAP).
- Se un server TACACS+ deve usare il nome del servizio per creare **cisco-av-pair**, gli utenti devono usare **Log in** come nome del servizio.
- Nessun supporto per lo scorfano per modificare le configurazioni.

Verifica della configurazione dalla CLI in CIMC

- Verificare se TACACS+ è abilitato.

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

- Verificare i dettagli di configurazione per server.

```
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
```

Risoluzione dei problemi

- Verificare che TACACS+ Server IP sia raggiungibile dal CIMC e che la porta sia configurata correttamente.
- Verificare che la **coppia cisco-av** sia configurata correttamente sul server TACACS+.
- Verificare che il server TACACS+ sia raggiungibile (IP e porta).
- Verificare che la chiave segreta o le credenziali corrispondano a quelle configurate sul server TACACS+.
- Se è possibile accedere con TACACS+ ma si hanno solo autorizzazioni di **sola lettura**, verificare se **cisco-av-pair** ha la sintassi corretta sul server TACACS+.

Risoluzione dei problemi ISE

- Verificare i registri Tacacs Live per uno dei tentativi di autenticazione. Lo stato deve essere **Superato**.

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	

- Verificare che per la risposta sia configurato l'attributo **cisco-av-pair** corretto.

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" ; }

Informazioni correlate

- [Autenticazione TACACS+ Cisco UCS-C](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)
- [Configurare ISE 2.0: Autenticazione e autorizzazione dei comandi IOS TACACS+ in base all'appartenenza al gruppo AD](#)