

Configuración de la Autenticación TACACS+ en CIMC con el Servidor ISE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuración del lado del servidor TACACS+ para asociación de privilegios](#)

[Requisitos de configuración de ISE](#)

[Configuración TACACS+ en CIMC](#)

[Verificación](#)

[Verificar la configuración desde CLI en CIMC](#)

[Troubleshoot](#)

[Solución de problemas de ISE](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de la autenticación de Sistema de control de acceso del controlador de acceso de terminal Plus (TACACS+) en Cisco Integrated Management Controller (CIMC).

TACACS+ se utiliza habitualmente para autenticar dispositivos de red con un servidor central. Desde la versión 4.1(3b), Cisco IMC admite la autenticación TACACS+. La compatibilidad con TACACS+ en CIMC facilita el esfuerzo de administrar varias cuentas de usuario que tienen acceso al dispositivo. Esta función es de ayuda para cambiar periódicamente las credenciales del usuario y gestionar las cuentas de usuario de forma remota.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controlador de gestión integrada de Cisco (CIMC)
- Terminal Access Controller Access-Control System Plus (TACACS+)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- UCSC-C220-M4S
- Versión de CIMC: 4.1(3 ter)
- Cisco Identity Services Engine (ISE) versión 3.0.0.458

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Configuración del lado del servidor TACACS+ para asociación de privilegios

El nivel de privilegio del usuario se calcula en función del valor de par **cisco-av** configurado para ese usuario. Se debe crear un **par** cisco-av en el servidor TACACS+ para y los usuarios no pueden utilizar ningún atributo TACACS+ predeterminado. Las tres sintaxis como se muestra a continuación son compatibles con el atributo **cisco-av-pair**

Para el privilegio **de administración**:

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

Para el privilegio **de usuario**:

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

Para el privilegio **de sólo lectura**:

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

Para admitir otros dispositivos, si es necesario agregar otras funciones, se pueden agregar con una coma como separador. Por ejemplo, UCSM admite **aaa**, por lo que **shell:roles="admin,aaa"** se puede configurar y CIMC acepta este formato.

Nota: Si **cisco-av-pair** no está configurado en el servidor TACACS+, entonces un usuario con ese servidor tiene un **privilegio de sólo lectura**.

Requisitos de configuración de ISE

Se debe permitir la IP de administración del servidor en los dispositivos de red ISE.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE' and 'Administration - Network Resources'. Below this, there are several tabs: 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' tab is selected, and the main content area displays a table of network devices. The table has columns for Name, IP/Mask, Profile Name, Location, Type, and Description. A red box highlights the first row, which contains the following data: Name: CIMC_4.1b, IP/Mask: 10.31.123.2, Profile Name: Cisco, Location: All Locations, Type: All Device Types, and Description: (empty).

Name	IP/Mask	Profile Name	Location	Type	Description
CIMC_4.1b	10.31.123.2	Cisco	All Locations	All Device Types	
Cisco Test	10.201.222	Cisco	All Locations	All Device Types	

La contraseña secreta compartida se ingresará en CIMC.

Network Devices

- Default Device
- Device Security Settings

Network Devices List > CIMC_4.1b

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

TEST

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Perfil de Shell con el atributo **cisco-av-pair** con permisos de administrador.

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 (Minutos (0-9999))
- Idle Time (Minutos (0-9999))

Custom Attributes

+ Add Trash Edit

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

Configuración TACACS+ en CIMC

Paso 1. Vaya a **Admin > User Management > TACACS+**

Paso 2. Active la casilla de verificación para activar **TACACS+**

Paso 3. Se puede agregar un nuevo servidor en cualquiera de las 6 filas especificadas en la tabla. Haga clic en la fila o seleccione la fila y haga clic en el botón **editar** de la parte superior de la tabla, como se muestra en esta imagen.

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: En el caso de que un usuario haya habilitado el repliegue de TACACS+ en ninguna opción de conectividad, CIMC aplica que la primera prioridad de autenticación siempre se debe establecer en TACACS+; de lo contrario, la configuración de repliegue podría volverse irrelevante.

Paso 4. Rellene la dirección IP o el nombre de host, el puerto y la clave de servidor/segredo compartido y **guarde** la configuración.

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 admite hasta seis servidores remotos TACACS+. Una vez que un usuario se ha autenticado correctamente, el nombre de usuario se agrega con (TACACS+).



Refresh | ? | i

Esto también se muestra en la Administración de sesiones

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	

Verificación

- Se puede configurar un máximo de 6 servidores TACACS+ en el CIMC.
- La clave secreta asociada al servidor puede tener una longitud máxima de 64 caracteres.
- El tiempo de espera se puede configurar entre 5 y 30 segundos (que se evalúa como máximo en 180 segundos para estar en línea con LDAP).
- Si un servidor TACACS+ necesita utilizar el nombre de servicio para crear el **par cisco-av**, los usuarios deben utilizar **Iniciar sesión** como nombre de servicio.
- No hay soporte de pelirroja para modificar las configuraciones.

Verificar la configuración desde CLI en CIMC

- Verifique si TACACS+ está habilitado.

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

- Verifique los detalles de la configuración por servidor.

```
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
```

Troubleshoot

- Asegúrese de que la IP del servidor TACACS+ esté accesible desde el CIMC y que el puerto esté configurado correctamente.
- Asegúrese de que el **par cisco-av** esté configurado correctamente en el servidor TACACS+.
- Compruebe si el servidor TACACS+ es accesible (IP y puerto).
- Asegúrese de que la clave secreta o las credenciales coincidan con las configuradas en el servidor TACACS+.
- Si puede iniciar sesión con TACACS+ pero sólo tiene permisos **de sólo lectura**, verifique si **cisco-av-pair** tiene la sintaxis correcta en el servidor TACACS+.

Solución de problemas de ISE

- Verifique los registros Tacacs Live para uno de los intentos de autenticación. El estado debe ser **Pass**.

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	

- Verifique que la respuesta tenga el atributo **cisco-av-pair** correcto configurado.

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" ; }

Información Relacionada

- [Autenticación TACACS+ Cisco UCS-C](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)
- [Configuración de ISE 2.0: Autorización de Autenticación y Comando TACACS+ de IOS basada en la pertenencia al grupo AD](#)