Configurar a autenticação TACACS+ no CIMC com servidor ISE

Contents

Introduction

Este documento descreve a configuração da autenticação do Terminal Access Controller Access Control System Plus (TACACS+) no Cisco Integrated Management Controller (CIMC).

O TACACS+ é comumente usado para autenticar dispositivos de rede com um servidor central. Desde a versão 4.1(3b), o Cisco IMC suporta autenticação TACACS+. O suporte TACACS+ no CIMC facilita o esforço de gerenciar várias contas de usuário que têm acesso ao dispositivo. Este recurso ajuda a alterar periodicamente as credenciais do usuário e a gerenciar contas de usuário remotamente.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

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

- UCSC-C220-M4S
- Versão do CIMC: 4.1(3 ter)

- Cisco Identity Services Engine (ISE) versão 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

TACACS+ Configuração do lado do servidor para associação de privilégios

O nível de privilégio do usuário é calculado com base no valor do par **cisco-av** configurado para esse usuário. Um **par de porta cisco** precisa ser criado no servidor TACACS+ para e os usuários não podem usar nenhum atributo TACACS+ padrão. As três sintaxes mostradas abaixo são suportadas para o atributo **cisco-av-pair**

Para privilégio **de administrador**:

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

Para privilégio **de usuário**:

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

Para privilégio **somente leitura**:

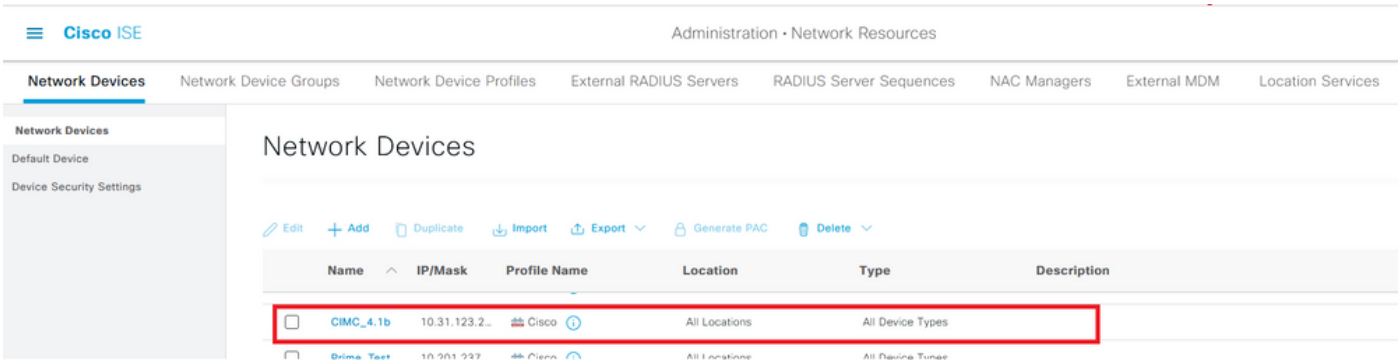
```
cisco-av-pair=shell:roles="read-only"
```

Para suportar outros dispositivos, se outras funções precisarem ser adicionadas, elas poderão ser adicionadas com uma vírgula como separador. Por exemplo, o UCSM suporta **aaa**, portanto, **shell:role="admin,aaa"** pode ser configurado e o CIMC aceita este formato.

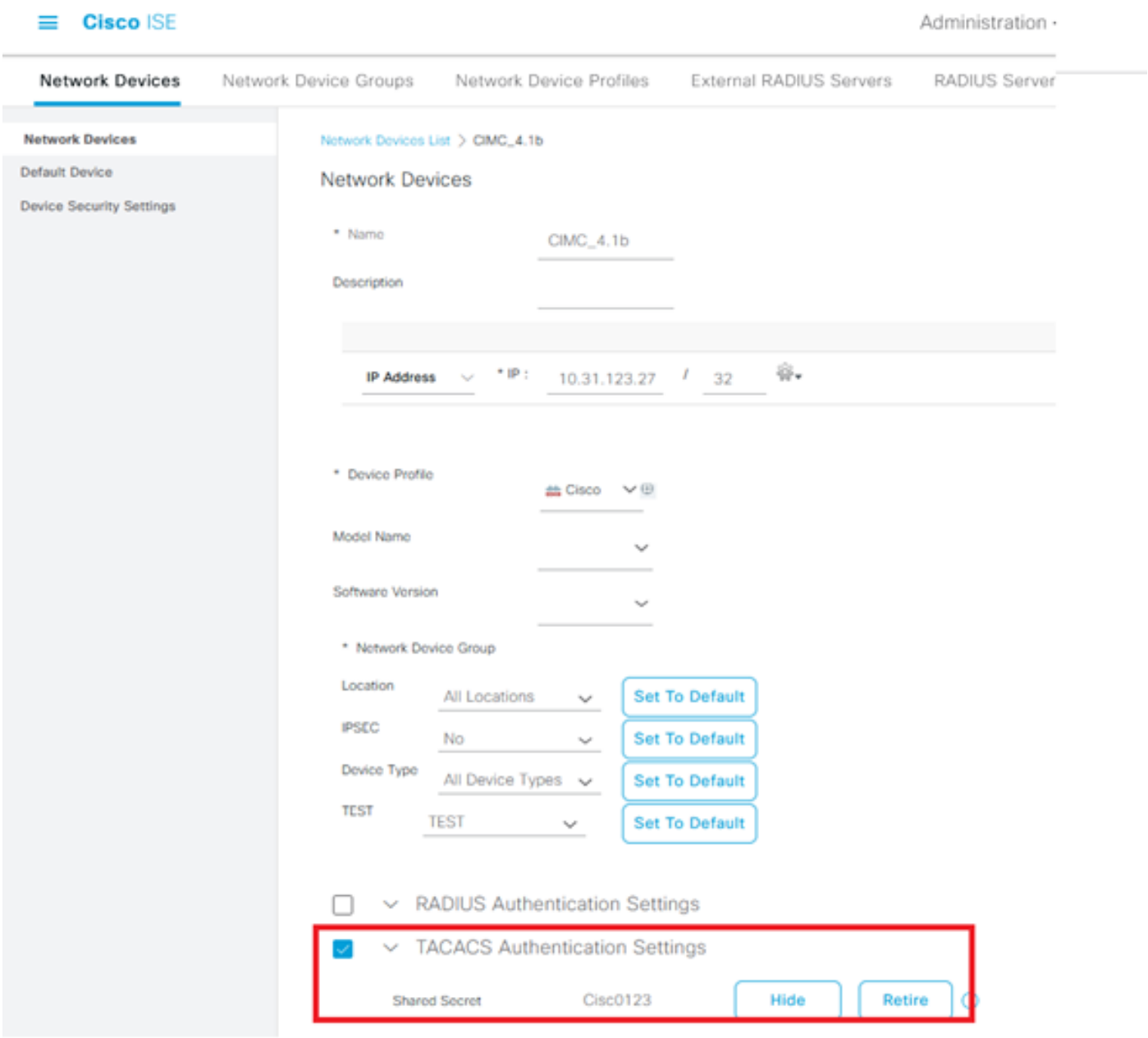
> **Note**: Se **cisco-av-pair** não estiver configurado no servidor TACACS+, um usuário com esse servidor terá um privilégio **somente leitura**.

Requisitos de configuração do ISE

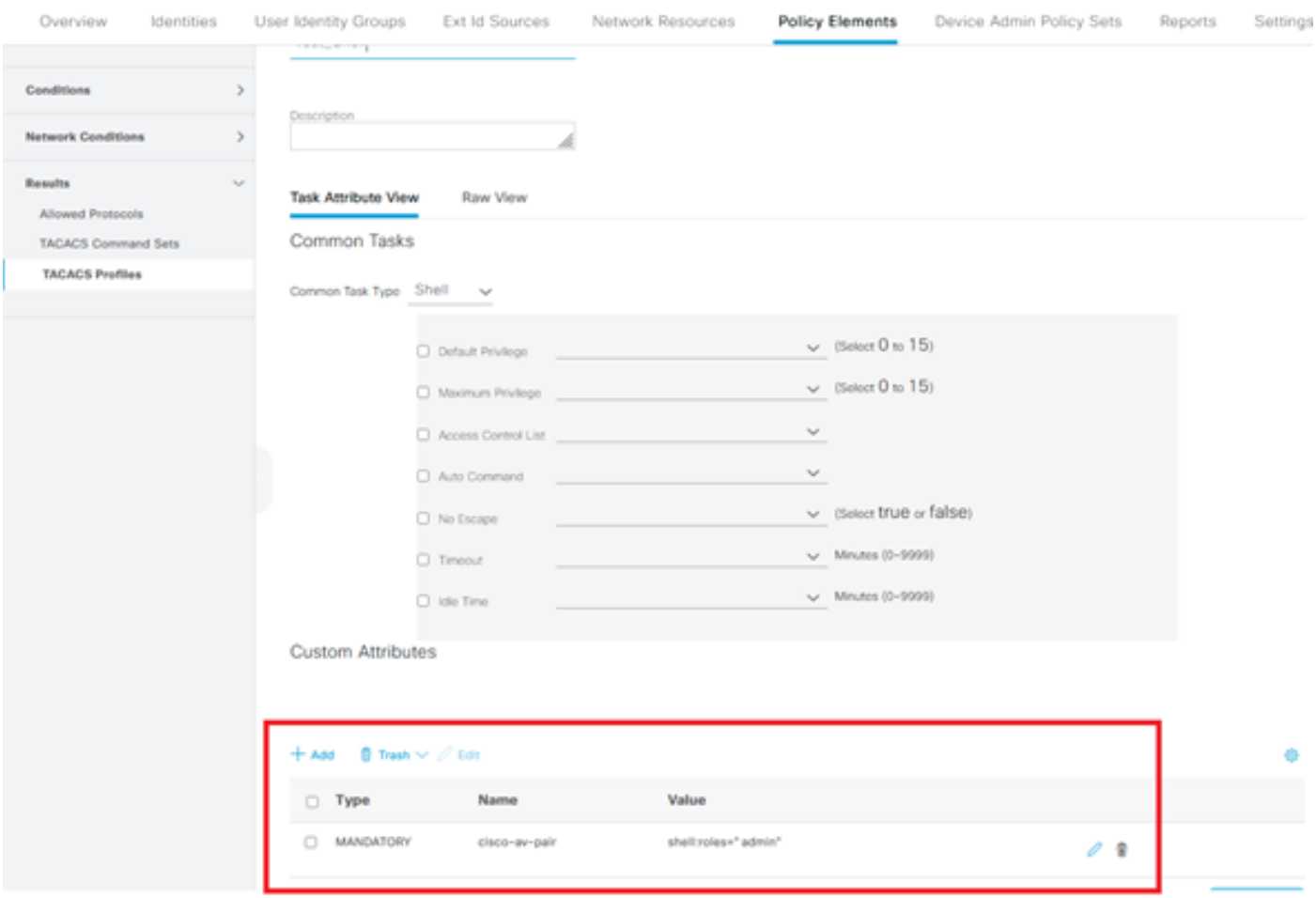
O IP de gerenciamento do servidor deve ser permitido nos dispositivos de rede ISE.



Senha secreta compartilhada a ser inserida no CIMC.



Perfil Shell com atributo **cisco-av-pair** com permissões de administrador.

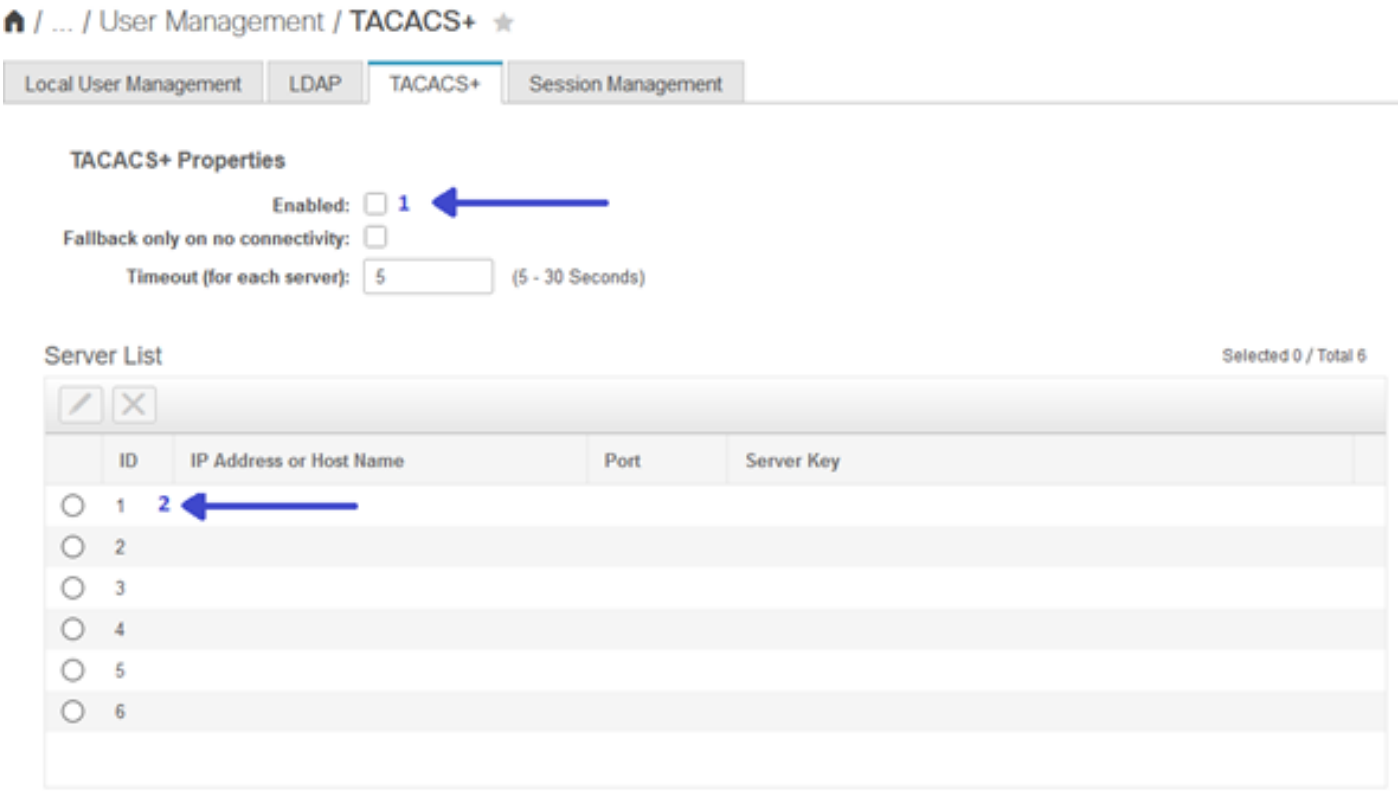


Configuração TACACS+ no CIMC

Etapa 1. Navegue até **Admin > User Management > TACACS+**

Etapa 2. Marque a caixa de seleção para habilitar o **TACACS+**

Etapa 3. Um novo servidor pode ser adicionado em qualquer uma das 6 linhas especificadas na tabela. Clique na linha ou selecione a linha e clique no botão **editar** na parte superior da tabela, como mostrado nesta imagem.

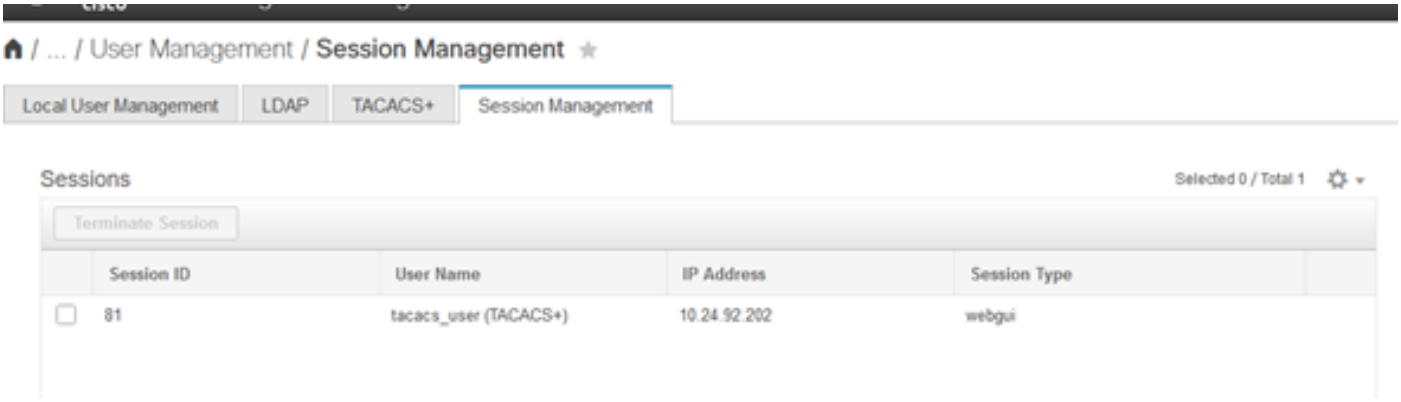


Note: Caso um usuário tenha ativado o recuo TACACS+ em nenhuma opção de conectividade, o CIMC garante que a primeira precedência de autenticação deve sempre ser definida como TACACS+, caso contrário, a configuração de fallback pode se tornar irrelevante.

Etapa 4. Preencha o endereço IP ou o nome do host, a porta e a chave do servidor/segredo compartilhado e **salve** a configuração.

O Cisco IMC suporta até seis servidores remotos TACACS+. Quando um usuário é autenticado com êxito, o nome de usuário é anexado ao (TACACS+).

Isso também é exibido no Session Management



Verificar

- Um máximo de 6 servidores TACACS+ podem ser configurados no CIMC.
- A chave secreta associada ao servidor pode ter no máximo 64 caracteres.
- O tempo limite pode ser configurado entre 5 e 30 segundos (o que é avaliado como o máximo como 180 segundos para estar em linha com o LDAP).
- Se um servidor TACACS+ precisar usar o nome do serviço para criar o **par cisco-av**, os usuários precisarão usar **Login** como o nome do serviço.
- Não há suporte para redfish para modificar as configurações.

Verificar a configuração da CLI no CIMC

- Verifique se TACACS+ está ativado.

```
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 os detalhes da configuração por servidor.

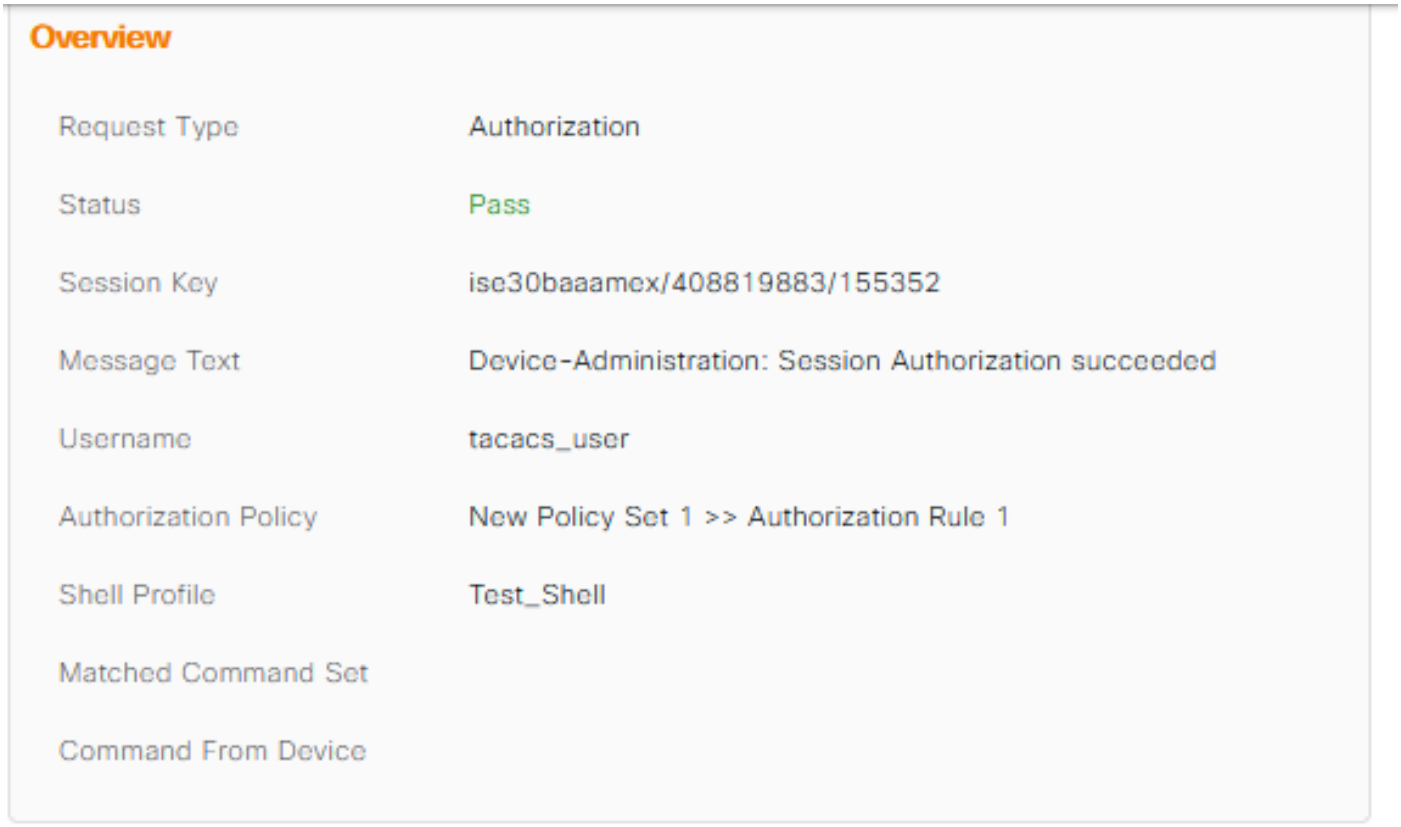
```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: ******
Server Port: 49
```

Troubleshoot

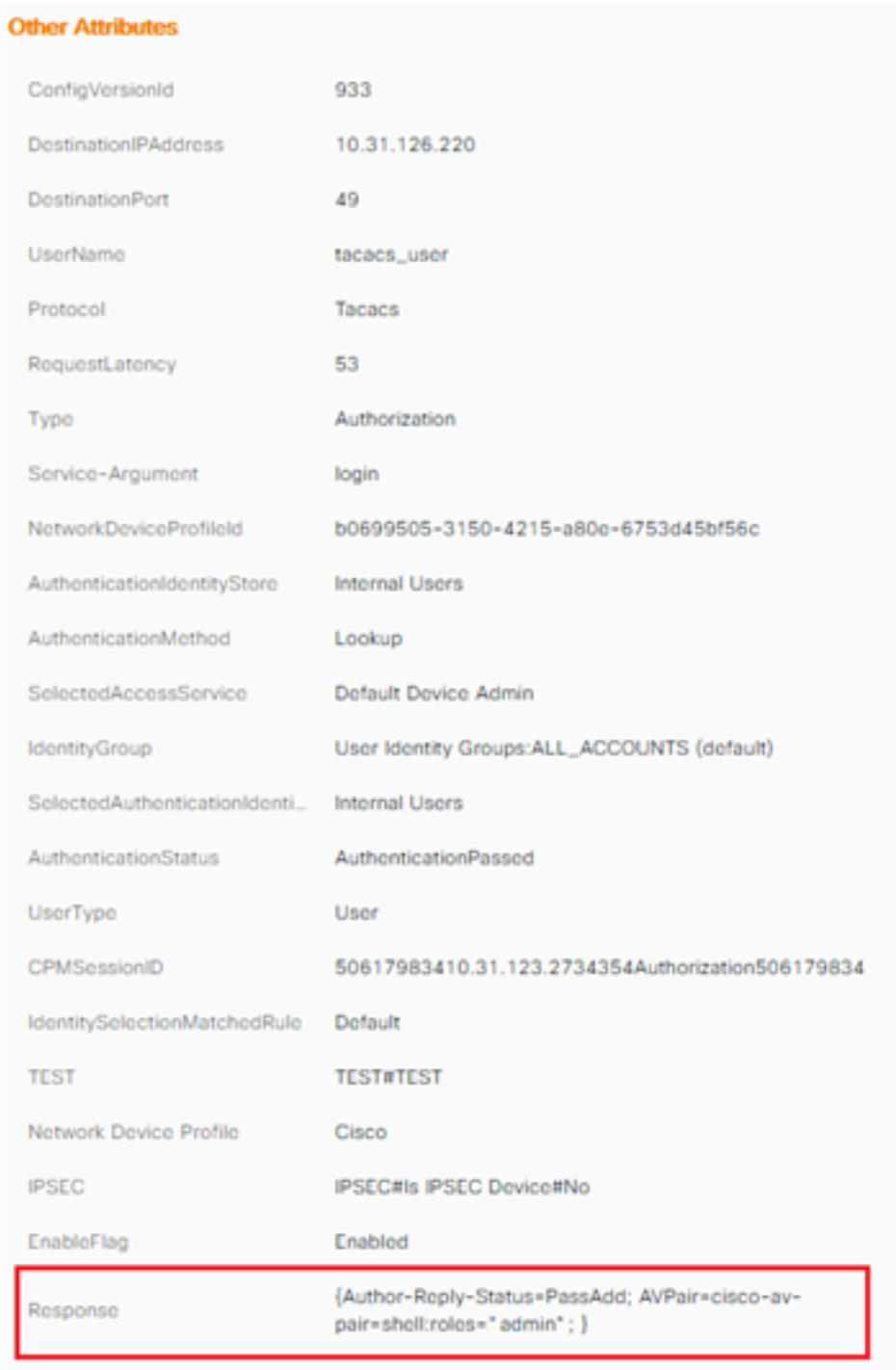
- Verifique se o IP do servidor TACACS+ pode ser alcançado do CIMC e se a porta está configurada corretamente.
- Certifique-se de que o **cisco-av-pair** esteja configurado corretamente no servidor TACACS+.
- Verifique se o servidor TACACS+ está acessível (IP e porta).
- Verifique se a chave ou credenciais secretas correspondem às configuradas no servidor TACACS+.
- Se você puder fazer login com o TACACS+, mas só tiver permissões **somente leitura**, verifique se o par cisco-av tem a sintaxe correta no servidor TACACS+.

Solução de problemas do ISE

- Verifique se há uma das tentativas de autenticação nos registros ao vivo do Tacacs. O status deve ser **Pass**.



- Verifique se a resposta tem o atributo **cisco-av-pair** correto 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" ; }

Informações Relacionadas

- Autenticação TACACS+ Cisco UCS-C
- Suporte Técnico e Documentação - Cisco Systems
- Configurar o ISE 2.0: Autenticação IOS TACACS+ e autorização de comando com base na associação do grupo AD