

Configurar e pesquise defeitos servidores de TACACS externos no ISE

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o ISE](#)

[Configurar o ACS](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve a característica para utilizar o server externo TACACS+ em um desenvolvimento usando o serviço Engine(ISE) da identidade como um proxy.

Pré-requisitos

Requisitos

- Compreensão básica da administração do dispositivo no ISE.
- Este documento é baseado na versão 2.0 do motor do serviço da identidade, aplicável em toda a versão do verison do motor do serviço da identidade mais altamente de 2.0.

Componentes Utilizados

Note: Toda a referência ao ACS neste documento pode ser interpretted para ser uma referência a qualquer server externo TACACS+. Contudo, a configuração no ACS e a configuração em todo o outro servidor de TACACS podem variar.

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

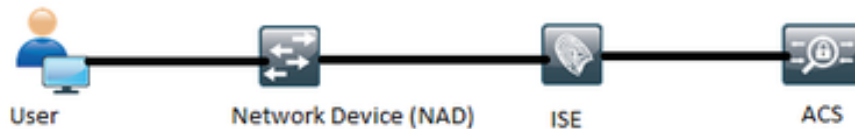
- Motor 2.0 do serviço da identidade
- Sistema de controle de acesso (ACS) 5.7

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, certifique-se de que você compreende o impacto potencial de toda a alteração de configuração.

Configurar

Esta seção ajuda a configurar o ISE aos pedidos do proxy TACACS+ ao ACS.

Diagrama de Rede



Configurar o ISE

1. Os servidores de TACACS externos do múltiplo podem ser configurados no ISE e podem ser usados para autenticar os usuários. A fim configurar o server externo TACACS+ no ISE, navegue aos **centros de trabalho > à administração do dispositivo > aos recursos de rede > aos servidores internos TACACS**. O clique **adiciona** e preenche os detalhes dos detalhes do servidor interno.

A captura de tela mostra a interface de administração do Cisco Identity Services Engine (ISE). O caminho de navegação é: TrustSec > Device Administration > Network Resources > TACACS External Servers > External_Server. O formulário de configuração para o servidor 'External_Server' contém os seguintes campos:

- Name:** External_Server
- Description:** External TACACS Server
- Host IP:** 10.127.196.237
- Connection Port:** 49 (1-65,535)
- Timeout:** 20 Seconds (1-999)
- Shared Secret:** ***** (com botão 'Show Secret')
- Use Single Connect:**

Botões 'Cancel' e 'Save' estão visíveis na base do formulário.

O segredo compartilhado fornecido nesta seção deve ser o mesmo segredo usado no ACS.

2. A fim utilizar o servidor de TACACS externo configurado, deve ser adicionado em uma sequência do servidor de TACACS a ser usada nos grupos da política. Eu peço para configurar a sequência do servidor de TACACS, navego aos **centros de trabalho > à administração do dispositivo > aos recursos de rede > à sequência do servidor de TACACS**. Clique **adicionam**, preenchem os detalhes e escolhem os server que são precisados de ser

usados nessa sequência.

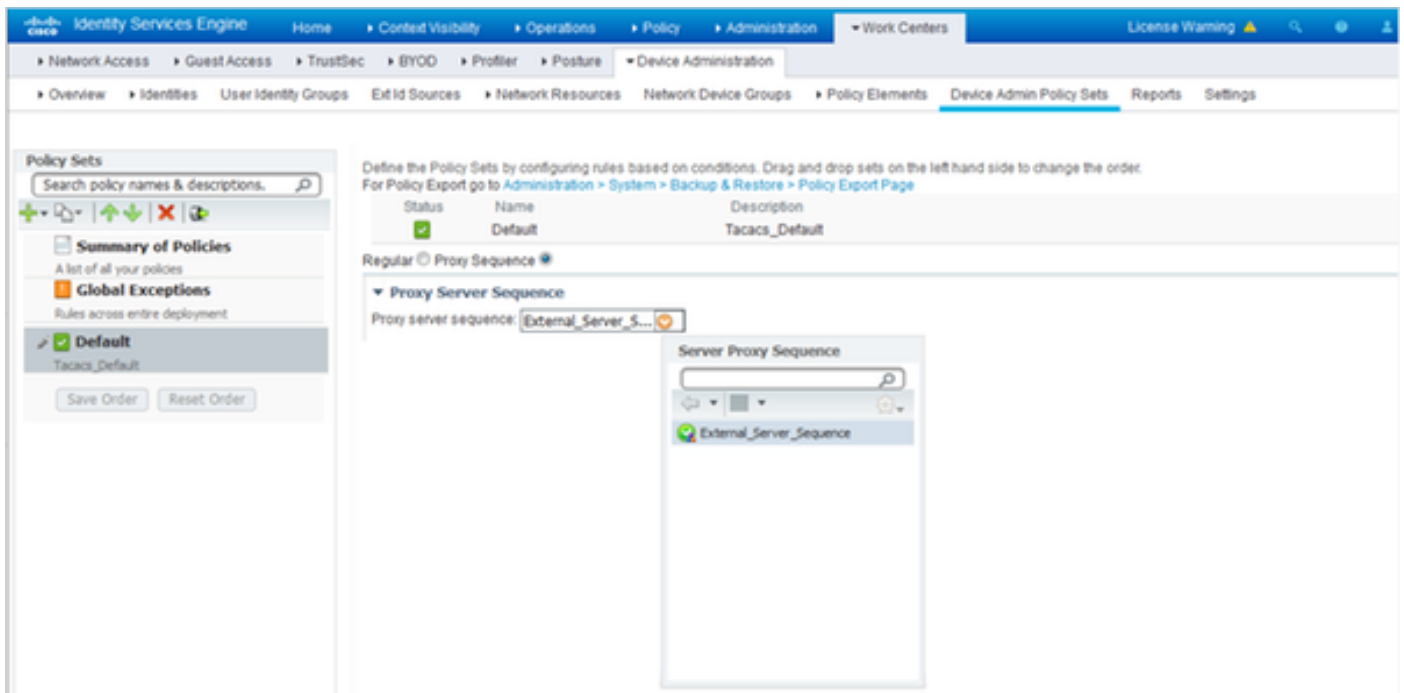
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main heading is "Server Sequence". The "Name" field is set to "External_Server_Sequence" and the "Description" is "Sequence for External Servers". Below this is a "Server List" section with the instruction: "The TACACS Proxy Servers selected will be tried in order:". It features two panes: "Available" (empty) and "Chosen" (containing "External_Server"). There are "Choose all" and "Clear all" buttons at the bottom of the panes. Below the server list, there is a "Logging Control" section with a radio button selected for "Accounting requests should be handled" and checkboxes for "Local Accounting" and "Remote Accounting". The "Username Stripping" section has checkboxes for "Prefix Strip" (with a value of "1") and "Suffix Strip" (with a value of "@"). At the bottom right are "Cancel" and "Submit" buttons.

Além do que a sequência do server, duas outras opções foram fornecidas. Controle de registro e descascamento username.

O controle de registro dá a uma opção ao log os pedidos da contabilidade localmente no ISE ou registra os pedidos da contabilidade ao servidor interno que segura a autenticação também.

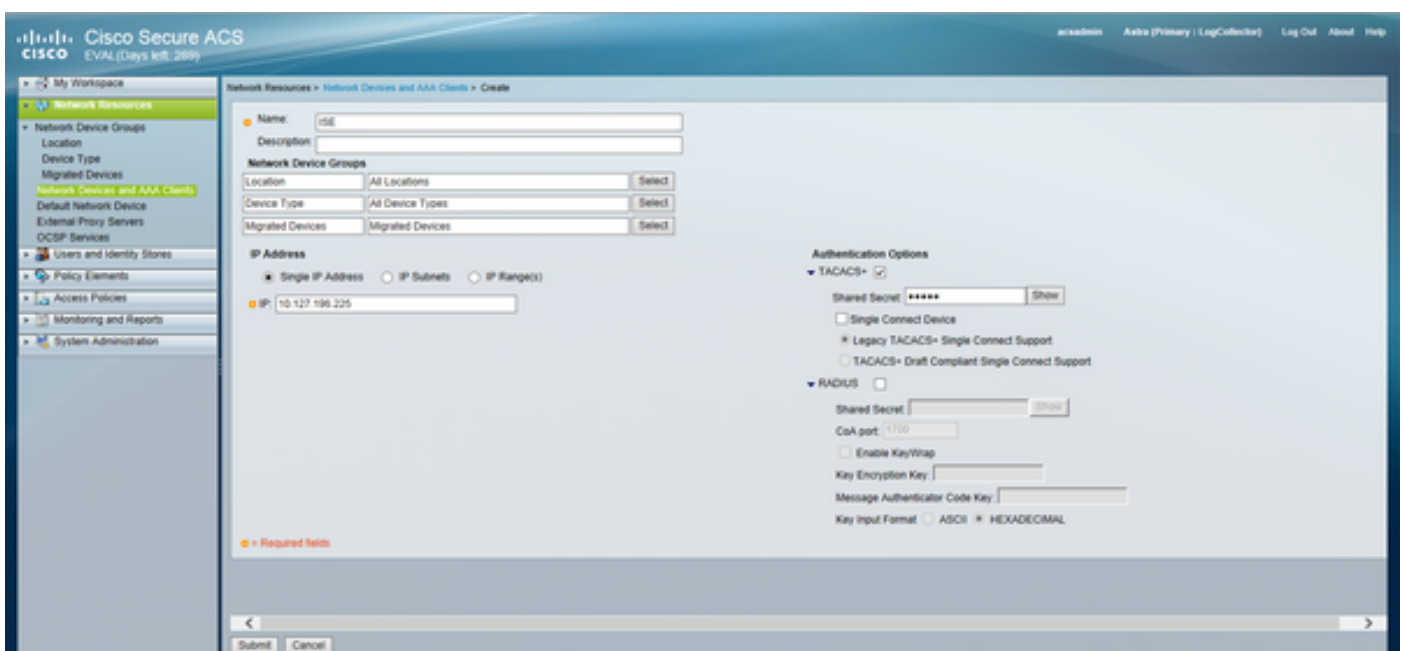
O descascamento username é usado para descascar o prefixo ou o sufixo specifying um delimitador antes de enviar o pedido a um servidor de TACACS externo.

3. Para utilizar a sequência externo do servidor de TACACS configurada, os grupos da política devem ser configurados para usar a sequência criada. A fim configurar os grupos da política para usar a sequência do servidor interno, navegue aos **centros de trabalho > aos grupos > ao [select the policy set] da política Admin da administração do dispositivo > do dispositivo**. Firme o botão de rádio que diz a **sequência do proxy**. Escolha a sequência do servidor interno criada.

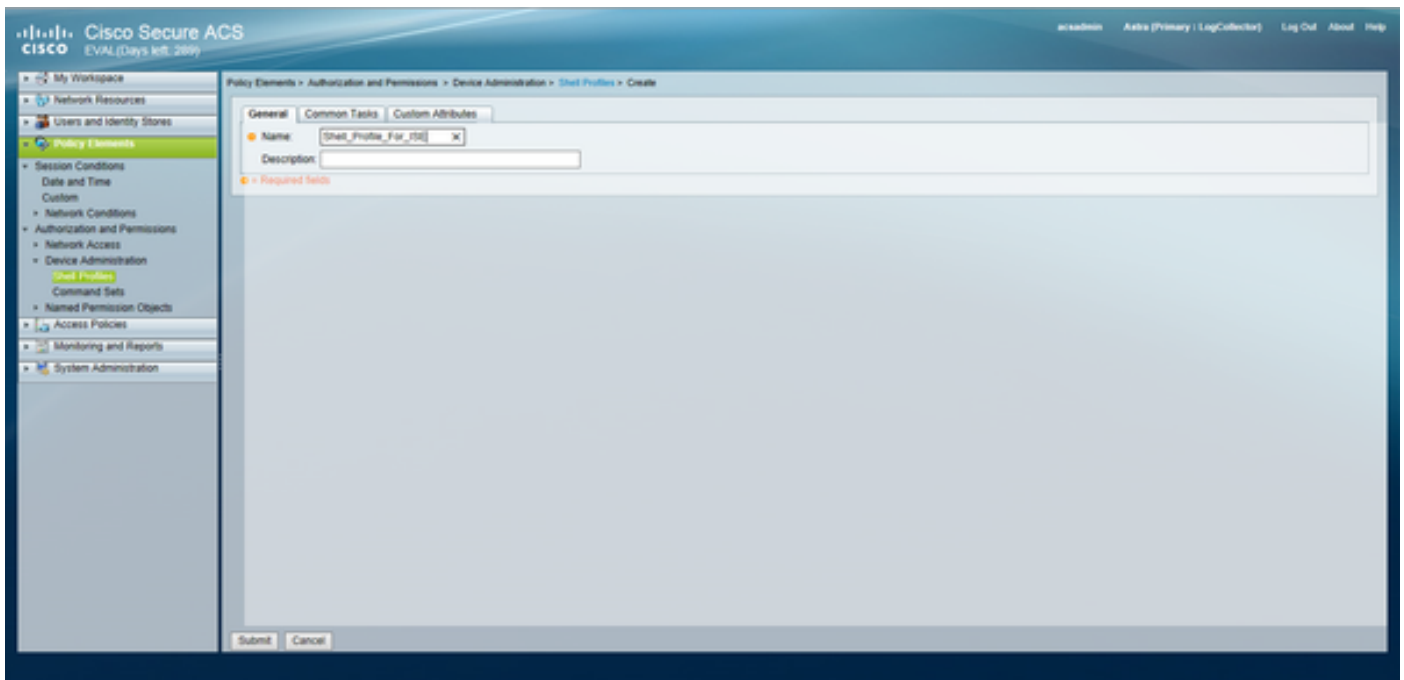


Configurar o ACS


Para o ACS, o ISE é apenas um outro dispositivo de rede que esteja enviando um pedido TACACS. A fim configurar o ISE como um dispositivo de rede no ACS, navegue aos **recursos de rede > aos dispositivos de rede e aos clientes de AAA**. O clique cria e preenche os detalhes do server ISE usando o mesmo segredo compartilhado que configurado no ISE.




Configurar os parâmetros da administração do dispositivo no ACS que são, nos perfis do shell e nos conjuntos de comandos. A fim configurar perfis do shell, navegue aos **elementos da política > à autorização e às permissões > à administração > ao shell do dispositivo perfis**. O clique cria e configura o nome, as tarefas comuns e os atributos feitos sob encomenda conforme a exigência.



Os conjuntos de comandos do conofigure, navegam aos **elementos da política > à autorização e às permissões > à administração do dispositivo > aos conjuntos de comandos**. O clique cria e preenche os detalhes conforme a exigência.

General
Name: Status: 

 The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Protocol:

Results
Service:

Configurar o serviço do acesso selecionado na regra de seleção do serviço conforme a exigência. A fim configurar o acesso preste serviços de manutenção a regras, navegam ao **dispositivo do >Default das políticas de acesso > dos serviços do acesso Admin > identidade** onde a loja da identidade que precisa de ser usada pode ser selecionada para a autenticação. As regras da autorização podem ser configuradas navegando ao **dispositivo do >Default das políticas de acesso > dos serviços do acesso Admin > autorização**.

Note: A configuração das políticas da autorização e dos perfles do shell para dispositivos específicos pode variar e aquela é fora do âmbito deste documento.

Verificar

Use esta seção para confirmar que a configuração trabalha corretamente.

A verificação pode ser feita no ISE e no ACS. Todo o erro na configuração do ISE ou do ACS conduzirá a uma falha de autenticação. O ACS é o servidor primário que segurará a autenticação e os pedidos de autorização, ISE carrega a responsabilidade a e do servidor ACS e atua como

um proxy para os pedidos. Desde que o pacote atravessa através de ambos os server, a verificação da autenticação ou do pedido de autorização pode ser feita em ambos os server.

Os dispositivos de rede são configurados com o ISE como o servidor de TACACS e não o ACS. Daqui o pedido alcança o ISE primeiramente e baseado nas regras configuradas, o ISE decide se o pedido precisa de ser enviado a um servidor interno. Isto pode ser verificado no TACACS vivo entra o ISE.

A fim ver o vivo entra o ISE, navegam às **operações > ao TACACS > logs vivos**. Os relatórios vivos podem ser considerados nesta página e os detalhes de um pedido particular podem ser verificados clicando o ícone da lupa que refere-se esse pedido específico que é do interesse.

Steps

```
13020  Get TACACS+ default network device setting
13013  Received TACACS+ Authentication START Request
15049  Evaluating Policy Group
15008  Evaluating Service Selection Policy
15048  Queried PIP - Network Access.Protocol
15006  Matched Default Rule
13064  TACACS proxy received incoming request for forwarding.
13065  TACACS proxy received valid incoming authentication request.
13063  Start forwarding request to remote TACACS server.
13074  Finished to process TACACS Proxy request.
13020  Get TACACS+ default network device setting
13014  Received TACACS+ Authentication CONTINUE Request
13064  TACACS proxy received incoming request for forwarding.
13065  TACACS proxy received valid incoming authentication request.
13071  Continue flow (seq_no > 1).
13063  Start forwarding request to remote TACACS server.
13074  Finished to process TACACS Proxy request.
```

A fim ver os relatórios da autenticação no ACS, navegue à **monitoração e aos relatórios > à monitoração do lançamento e relate o visor > a monitoração e os relatórios > os relatórios > o protocolo de AAA > a autenticação TACACS**. Como o ISE, os detalhes de um pedido particular podem ser verificados clicando o ícone da lupa que refere-se esse pedido específico que é do

interesse



Troubleshooting

Esta seção fornece a informação que você pode se usar para pesquisar defeitos sua configuração

1. Se os detalhes do relatório no ISE mostram a Mensagem de Erro mostrado na figura, a seguir indica um segredo compartilhado inválido configurado no ISE ou no dispositivo de Netowrk (NAD).

Message Text

TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. Se não há nenhum relatório da autenticação para um pedido no ISE mas o acesso está sendo negado ao utilizador final a um dispositivo de rede, este indica geralmente diversas coisas.

- O pedido próprio não fez nenhum alcance o server ISE.
- Se a personalidade da administração do dispositivo é desabilitada no ISE, a seguir todo o pedido TACACS+ ao ISE estará deixado cair silenciosamente. Nenhum log que indica o mesmos será mostrado nos relatórios ou nos logs vivos. Para verificar isto, navegue à **administração > ao sistema > ao desenvolvimento > ao [select the node]**. O clique **edita** e observa “**para permitir a caixa de verificação do serviço Admin do dispositivo**” sob a aba **geral dos ajustes** segundo as indicações da figura. Que a caixa de seleção precisa de ser verificada para ver se há a administração do dispositivo para trabalhar no ISE.

Personas

Administration Role **PRIMARY**

Monitoring Role PRIMARY Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service Use Interface GigabitEthernet 0

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

- Se uma licença da administração do dispositivo não está atual do expirado, a seguir todos os pedidos TACACS+ estão deixados cair silenciosamente. Nenhum log é mostrado no GUI para o mesmos. Navegue à **administração > ao sistema > licenciando** para verificar a licença da administração do dispositivo.

Licenses How do I register/modify or lookup my licenses?

| License File | Quantity | Term | Expiration Date |
|----------------|-----------|---------|-----------------------------------|
| EVALUATION Lic | | | |
| Base | 100 | 90 days | ⚠ 22-Jan-2017 (43 days remaining) |
| Plus | 100 | 90 days | ⚠ 22-Jan-2017 (43 days remaining) |
| Apex | 100 | 90 days | ⚠ 22-Jan-2017 (43 days remaining) |
| Wired | 100 | 90 days | ⚠ 22-Jan-2017 (43 days remaining) |
| Device Admin | Uncounted | 90 days | ⚠ 22-Jan-2017 (43 days remaining) |

- Se o dispositivo de rede não é configurado ou se um IP errado do dispositivo de rede está configurado no ISE, a seguir o ISE deixará cair silenciosamente o pacote. Nenhuma resposta é enviada para trás ao cliente e nenhum log é mostrado no GUI. Esta é uma mudança do comportamento no ISE para o TACACS+ quando comparada àquele do ACS que informa que o pedido veio dentro de um dispositivo de rede ou de um cliente de AAA do unkown.
- O pedido alcançou o ACS mas a resposta não veio para trás ao ISE. Esta encenação pode ser verificada dos relatórios no ACS segundo as indicações da figura. Geralmente isto é devido a um segredo compartilhado inválido no ACS configurado para o ISE ou no ISE configurado para o ACS.




- A resposta não será enviada mesmo se o ISE não é configurado ou o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface de gerenciamento do ISE não é configurado no ACS na configuração de dispositivo de rede. Em tal secario, a mensagem na figura pode ser observada no ACS.



- Se um relatório da autenticação bem sucedida está considerado no ACS mas nenhum relatório é considerado no ISE e o usuário está sendo rejeitado, a seguir poderia muito jorrar seja uma edição na rede. Isto pode ser verificado por uma captura de pacote de informação no ISE com filtros necessários. Para recolher uma captura de pacote de informação no ISE, navegue às **operações > pesquisam defeitos > ferramentas de diagnóstico > ferramentas gerais > descarga TCP**.

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status  Stopped

Host Name

Network Interface

Promiscuous Mode On Off

Filter

Example: 'ip host helios and not iceberg'

Format

Dump File Last created on Fri Dec 09 20:51:18 IST 2016
File size: 9,606 bytes
Format: Raw Packet Data
Host Name: tornado
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

3. Se os relatórios podem ser considerados no ISE mas não no ACS, poderia um ou outro meio que o pedido não alcançou o ACS devido a um misconfiguration dos grupos da política no ISE que pode ser pesquisado defeitos baseou no relatório detalhado no ISE ou devido a uma questão de rede que possa ser identificada por uma captura de pacote de informação no ACS.
4. Se os relatórios são considerados no ISE e o ACS mas usuário estão sendo negados ainda o acesso, a seguir é mais frequentemente uma edição na configuração das políticas de acesso no ACS que pode ser pesquisado defeitos baseou no relatório detalhado no ACS. Também, o tráfego de retorno do ISE ao dispositivo de Network deve ser permitido.