

Servidores TACACS externos de la configuración y del Troubleshooting en el ISE

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración ISE](#)

[Configuración ACS](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe la característica para utilizar el servidor del externo TACACS+ en un despliegue usando el servicio Engine(ISE) de la identidad como proxy.

Prerrequisitos

Requisitos

- Comprensión básica Device Administration (Administración del dispositivo) encendido del ISE.
- Este documento se basa en la versión 2.0 del motor del servicio de la identidad, aplicable en cualquier versión del verison del motor del servicio de la identidad más arriba de 2.0.

Componentes Utilizados

Nota: Cualquier referencia al ACS en este documento se puede interpreted para ser una referencia a cualquier servidor del externo TACACS+. Sin embargo, la configuración en el ACS y la configuración en cualquier otro servidor TACACS pueden variar.

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

- Motor 2.0 del servicio de la identidad
- Sistema de control de acceso (ACS) 5.7

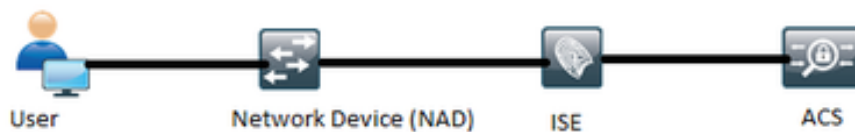
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese que usted entiende el impacto potencial de cualquier cambio de configuración.

Configurar

Esta sección ayuda a configurar el ISE a las peticiones del proxy TACACS+ al ACS.

Diagrama de la red



Configuración ISE

1. Los servidores TACACS externos múltiples pueden ser configurados en el ISE y pueden ser utilizados para autenticar a los usuarios. Para configurar el servidor externo TACACS+ en el ISE, navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > los recursos de red > los servidores externos TACACS**. El teclado agrega y completa a los detalles de los detalles del servidor externo.

La imagen muestra la interfaz de configuración de ISE en un navegador. El título de la página es 'Identity Services Engine'. El menú de navegación superior incluye 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration' y 'Work Centers'. El menú de navegación lateral incluye 'TrustSec', 'Device Administration', 'Overview', 'Identities', 'User Identity Groups', 'Network Resources', 'Network Device Groups', 'Policy Conditions', 'Policy Results', 'Device Admin Policy Sets', 'Reports' y 'Settings'. El contenido principal muestra la configuración de un 'TACACS External Servers > External_Server'. Los campos de configuración son:

- 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: ***** (con un botón 'Show Secret')
- Use Single Connect:

En la parte inferior derecha hay botones 'Cancel' y 'Save'.

El secreto compartido proporcionado en esta sección debe ser el mismo secreto usado en el ACS.

2. Para utilizar al servidor TACACS externo configurado, debe ser agregado en una secuencia del servidor TACACS que se utilizará en los conjuntos de la directiva. Ordeno para

configurar la secuencia del servidor TACACS, navego a los **centros de trabajo > Device Administration (Administración del dispositivo) > los recursos de red > secuencia del servidor TACACS**. Haga clic **agregar**, completan los detalles y eligen los servidores que son necesarios ser utilizados en esa secuencia.

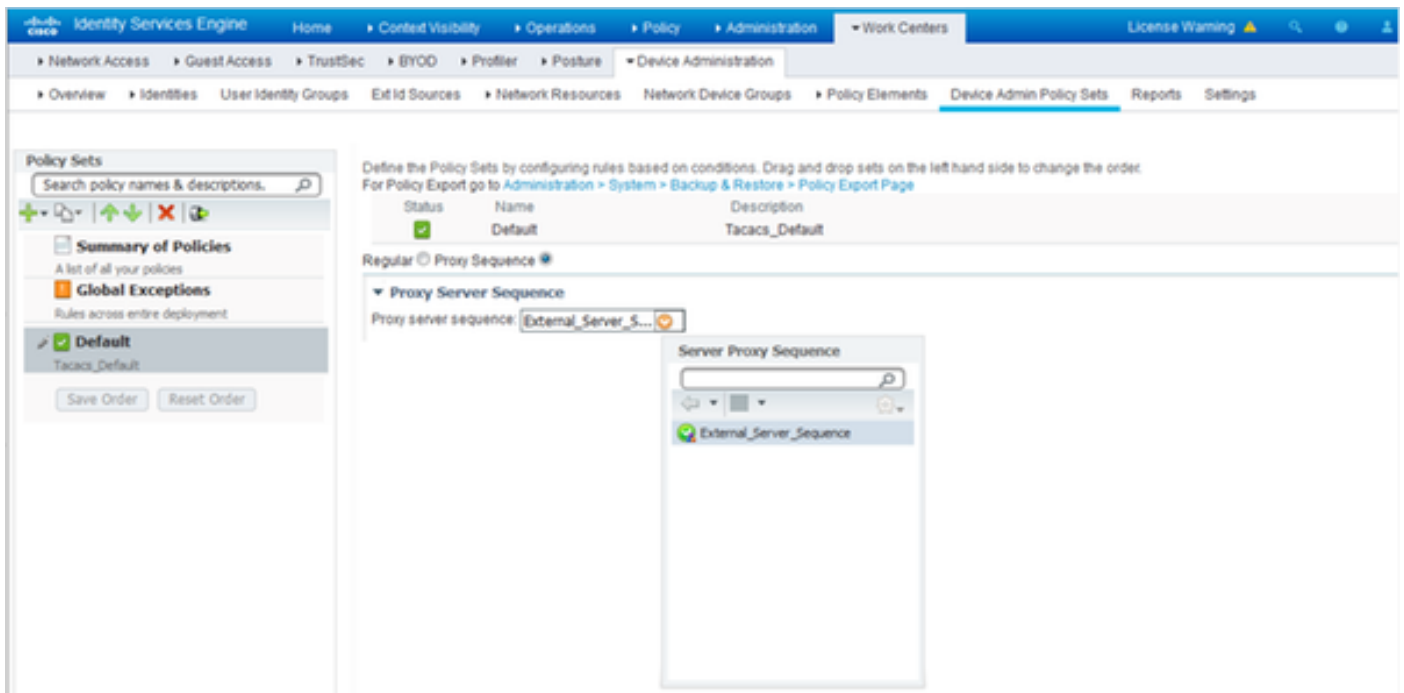
The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a TACACS Server Sequence. The page title is "Server Sequence" and the name is "External_Server_Sequence". The description is "Sequence for External Servers". The server list section shows two columns: "Available" and "Chosen". The "Chosen" column contains "External_Server". Below the server list, there are options for "Logging Control" (Local Accounting and Remote Accounting) and "Username Stripping" (Prefix Strip and Suffix Strip). The page includes "Cancel" and "Submit" buttons.

Además de la secuencia del servidor, se han proporcionado dos otras opciones. Control y el eliminar de registración del nombre de usuario.

El control de registración da a opción al registro las peticiones de las estadísticas localmente en el ISE o registra las peticiones de las estadísticas al servidor externo que maneja la autenticación también.

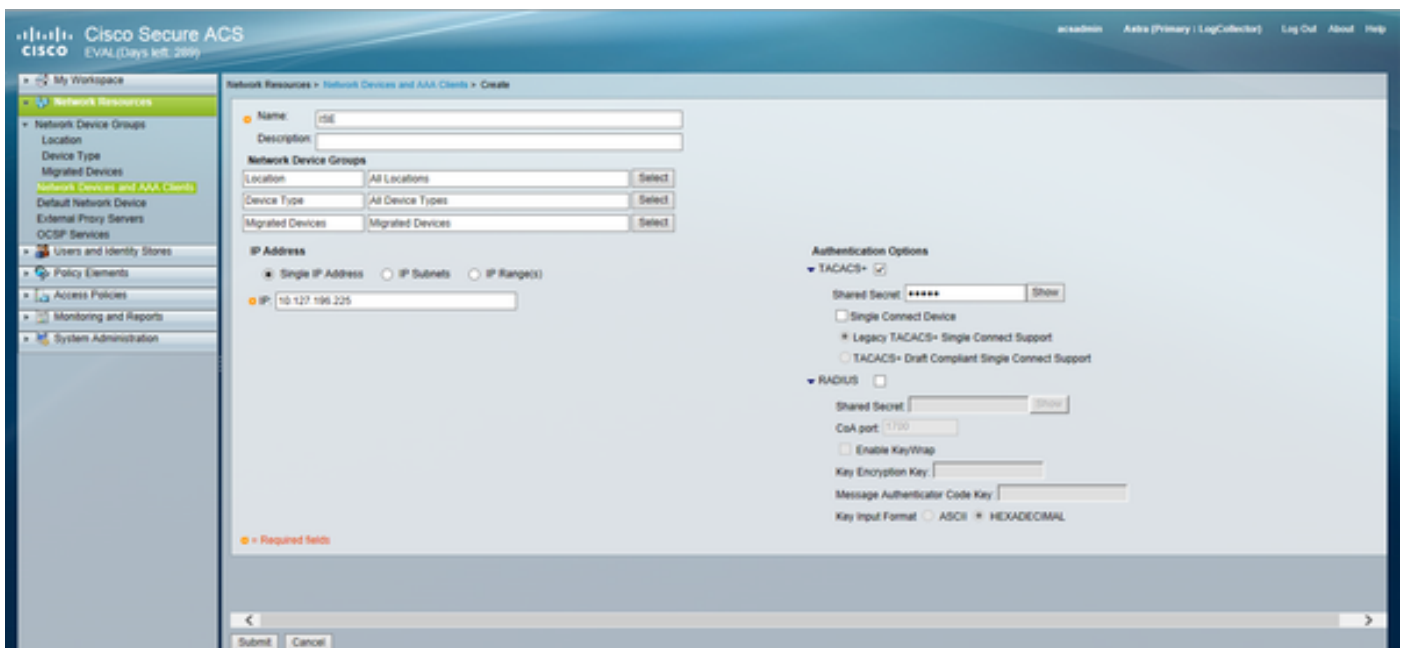
El eliminar del nombre de usuario es utilizado para eliminar el prefijo o el sufijo sepcifying un delimitador antes de remitir la petición a un servidor TACACS externo.

3. Para utilizar la secuencia externa del servidor TACACS configurada, los conjuntos de la directiva se deben configurar para utilizar la secuencia creada. Para configurar los conjuntos de la directiva para utilizar la secuencia del servidor externo, navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > los conjuntos > [select the policy set] de la directiva Admin del dispositivo**. Conecte el botón de radio que dice la **secuencia del proxy**. Elija la secuencia del servidor externo creada.

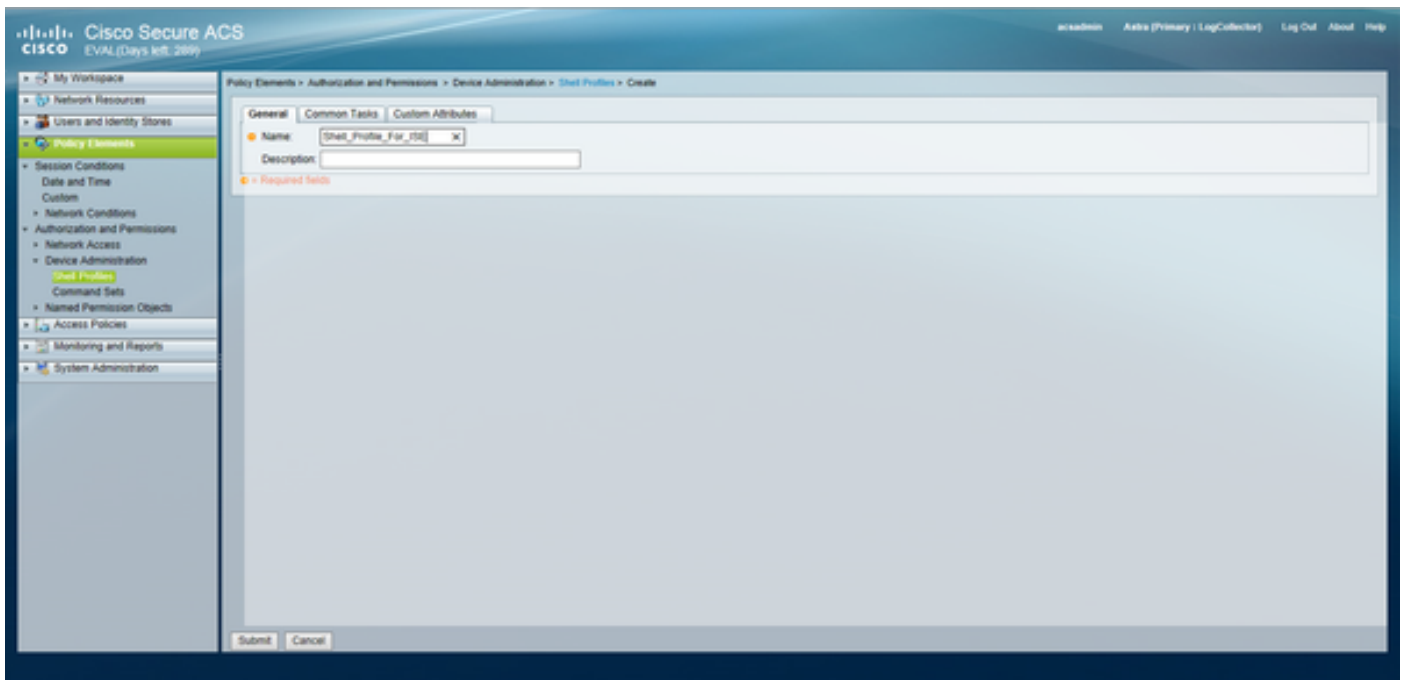


Configure el ACS


Para el ACS, el ISE es apenas otro dispositivo de red que enviará una petición TACACS. Para configurar el ISE como dispositivo de red en el ACS, navegue a los **recursos de red > a los dispositivos de red y a los clientes AAA**. El teclado **crea** y completa los detalles del servidor ISE usando el mismo secreto compartido según lo configurado en el ISE.




Configure Device Administration (Administración del dispositivo) los parámetros en el ACS que son, los perfiles del shell y los comandos establece. Para configurar los perfiles del shell, navegue a los **elementos de la directiva > a la autorización y a los permisos > Device Administration (Administración del dispositivo) > los perfiles del shell**. El teclado **crea** y configura el nombre, las tareas del campo común y los atributos personalizados según el requisito.



Para los comandos establece del conofigure, navegan a los **elementos de la directiva > a la autorización y a los permisos > Device Administration (Administración del dispositivo) > los comandos establece**. El tecleo crea y completa los detalles según el requisito.

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:

Configure el servicio del acceso seleccionado en la regla de selección del servicio según el requisito. Para configurar el acceso mantenga las reglas, navegan al **dispositivo del >Default de las políticas de acceso > de los servicios del acceso Admin > identidad** donde el almacén de la identidad que necesita ser utilizado se puede seleccionar para la autenticación. Las reglas de la autorización pueden ser configuradas navegando al **dispositivo del >Default de las políticas de acceso > de los servicios del acceso Admin > autorización**.

Nota: La configuración de las directivas de la autorización y de los perfiles del shell para los dispositivos específicos puede variar y ésta está fuera del ámbito de este documento.

Verificación

Utilice esta sección para confirmar que la configuración trabaja correctamente.

La verificación se puede hacer en el ISE y el ACS. Cualquier error en la configuración del ISE o del ACS dará lugar a una falla de autenticación. El ACS es el servidor primario que manejará la autenticación y los pedidos de autorización, ISE lleva la responsabilidad a y desde el servidor

ACS y actúa como proxy para las peticiones. Puesto que el paquete atraviesa a través ambos los servidores, la verificación de la autenticación o del pedido de autorización se puede hacer en ambos los servidores.

Los dispositivos de red se configuran con el ISE como el servidor TACACS y no el ACS. Por lo tanto la petición alcanza el ISE primero y basado sobre las reglas configuradas, el ISE decide a si la petición necesita ser remitida a un servidor externo. Esto se puede verificar en el TACACS vivo abre una sesión el ISE.

Para ver el vivo abre una sesión el ISE, navegan a las **operaciones > al TACACS > los registros vivos**. Los informes vivos se pueden considerar en esta página y los detalles de una petición determinada pueden ser marcados haciendo clic el icono de la lupa referente a esa petición específica que esté de interés.

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.

Para ver los informes de la autenticación sobre el ACS, navegue a **monitorear y a los informes > a la supervisión del lanzamiento y señale que el Visualizador > la supervisión y los informes >**

señala >AAA el protocolo > la autenticación de TACACS. Como el ISE, los detalles de una petición determinada pueden ser marcados haciendo clic el icono de la lupa referente a esa petición específica que esté de interés



Steps
Message
Received TACACS+ Authentication START Request
Evaluating Service Selection Policy
Matched rule
Selected Access Service - Default Device Admin
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration.
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request
Using previously selected Access Service
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
Authentication Passed
Evaluating Group Mapping Policy
Evaluating Exception Authorization Policy
No rule was matched
Evaluating Authorization Policy
Matched Default Rule
Returned TACACS+ Authentication Reply

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración

1. Si los detalles del informe sobre el ISE muestran el mensaje de error mostrado en la figura, después indica un secreto compartido inválido configurado en el ISE o el dispositivo de Netowrk (NAD).

Message Text

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

2. Si no hay informe de la autenticación para una petición en el ISE pero el acceso se está negando al usuario final a un dispositivo de red, éste indica generalmente varias cosas.

- La petición sí mismo no hizo ningún alcance el servidor ISE.
- Si Device Administration (Administración del dispositivo) el personaje se inhabilita en el ISE, después cualquier petición TACACS+ al ISE será caída silenciosamente. No se mostrará ningunos registros que indican lo mismo en los informes o los registros vivos. Para verificar esto, navegue a la **administración > al sistema > al despliegue > al [select the node]**. El tecleo **edita** y nota “la casilla de verificación del **servicio Admin del dispositivo del permiso**” bajo lengüeta de las **opciones generales** tal y como se muestra en de la figura. Que el checkbox necesita ser marcado para saber si hay Device Administration (Administración del dispositivo) para trabajar en el 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

- Si Device Administration (Administración del dispositivo) una licencia no está presente de expirado, después todas las peticiones TACACS+ se caen silenciosamente. No se muestra ningunos registros en el GUI para lo mismo. Navegue a la **administración > al sistema > autorizando** para marcar Device Administration (Administración del dispositivo) la licencia.

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)

- Si el dispositivo de red no se configura o si un IP incorrecto del dispositivo de red se configura en el ISE, después el ISE caerá silenciosamente el paquete. No se devuelve ninguna respuesta al cliente y no se muestra ningunos registros en el GUI. Éste es un cambio del comportamiento en el ISE para el TACACS+ cuando está comparada al del ACS que informa que la petición vino adentro de un dispositivo de red o de un cliente AAA del unknown.
- La petición alcanzó el ACS pero la respuesta no volvió al ISE. Este escenario se puede marcar de los informes sobre el ACS tal y como se muestra en de la figura. Esto está generalmente debido a un secreto compartido inválido en el ACS configurado para el ISE o en el ISE configurado para el ACS.

Steps

Message

Received TACACS+ Authentication START Request

Invalid TACACS+ request packet - possibly mismatched Shared Secrets

- La respuesta no será enviada incluso si el ISE no se configura o la dirección IP de la interfaz de administración del ISE no se configura en el ACS en la configuración del dispositivo de red. En tal secario, el mensaje en la figura se puede observar en el ACS.

Steps


Message

Received TACACS+ packet from unknown Network Device or AAA Client

- Si un informe de la autenticación satisfactoria se considera en el ACS pero no se considera ningunos informes en el ISE y están rechazando al usuario, después podría muy bien ser un problema en la red. Esto se puede verificar por una captura de paquetes en el ISE con los filtros necesarios. Para recoger a una captura de paquetes en el ISE, navegue a las **operaciones > al Troubleshooting > a las herramientas de diagnóstico > las herramientas generales > volcado 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. Si los informes se pueden considerar en el ISE pero no en el ACS, podría cualquier medio que la petición no ha alcanzado el ACS debido a un misconfiguration de los conjuntos de la directiva en el ISE que se puede localizar averías basó en el informe detallado sobre el ISE o debido a un problema de red que se pueda identificar por una captura de paquetes en el ACS.
4. Si los informes se consideran en el ISE y el ACS pero usuario todavía se están negando el acceso, después es más a menudo un problema en la configuración de las políticas de acceso en el ACS que se puede localizar averías basó sobre el informe detallado en el ACS. También, el tráfico de retorno del ISE al dispositivo de Network debe ser permitido.