ISE 2.0: ASA CLI autenticación de TACACS+ y ejemplo de configuración del comando authorization

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Configurar
Diagrama de la red
Configuraciones
Configuración ISE para la autenticación y autorización
Agregue el dispositivo de red
Configurar los grupos de la Identificación del usuario
Configurar a los usuarios
Servicio Admin del dispositivo del permiso
Configurar los conjuntos del comando tacacs
Configurar el perfil TACACS
Configurar la directiva de la autorización TACACS
Configure el Firewall de Cisco ASA para la autenticación y autorización
Verificación
Verificación del Firewall de Cisco ASA
Verificación ISE 2.0
Troubleshooting
Información Relacionada
Discusiones relacionadas de la comunidad del soporte de Cisco

Introducción

Este documento describe cómo configurar autenticación de TACACS+ y comando authorization en el dispositivo de seguridad adaptante de Cisco (ASA) con el motor del servicio de la identidad (ISE) 2.0 y posterior. El ISE utiliza el almacén local de la identidad para salvar los recursos tales como usuarios, grupos, y puntos finales.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- El Firewall ASA es completamente - operativo

- Conectividad entre el ASA y el ISE
- Se ata con correa el servidor ISE

Componentes Utilizados

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

- Motor 2.0 del servicio de la identidad de Cisco
- Software Release 9.5(1) de Cisco ASA

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

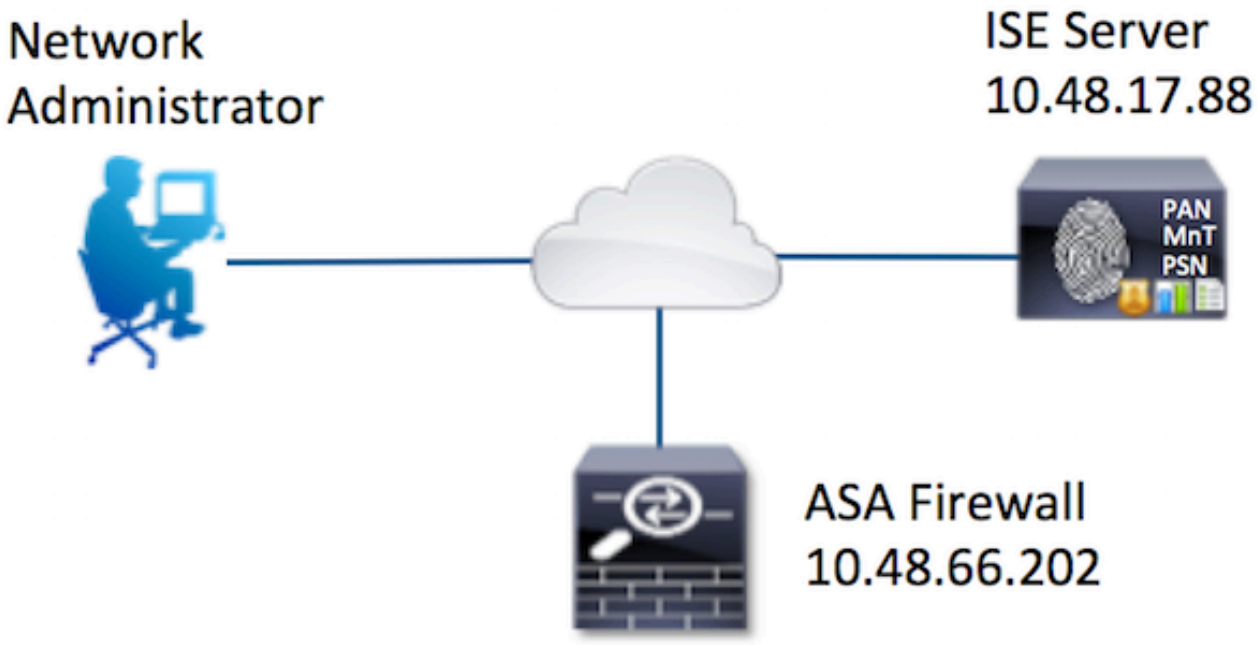
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configurar

El objetivo de la configuración está a:

- Autentique al usuario del ssh vía el almacén interno de la identidad
- Autorice al usuario del ssh así que será colocado en el modo EXEC privilegiado después del login
- Marque y envíe cada comando ejecutado al ISE para la verificación

Diagrama de la red



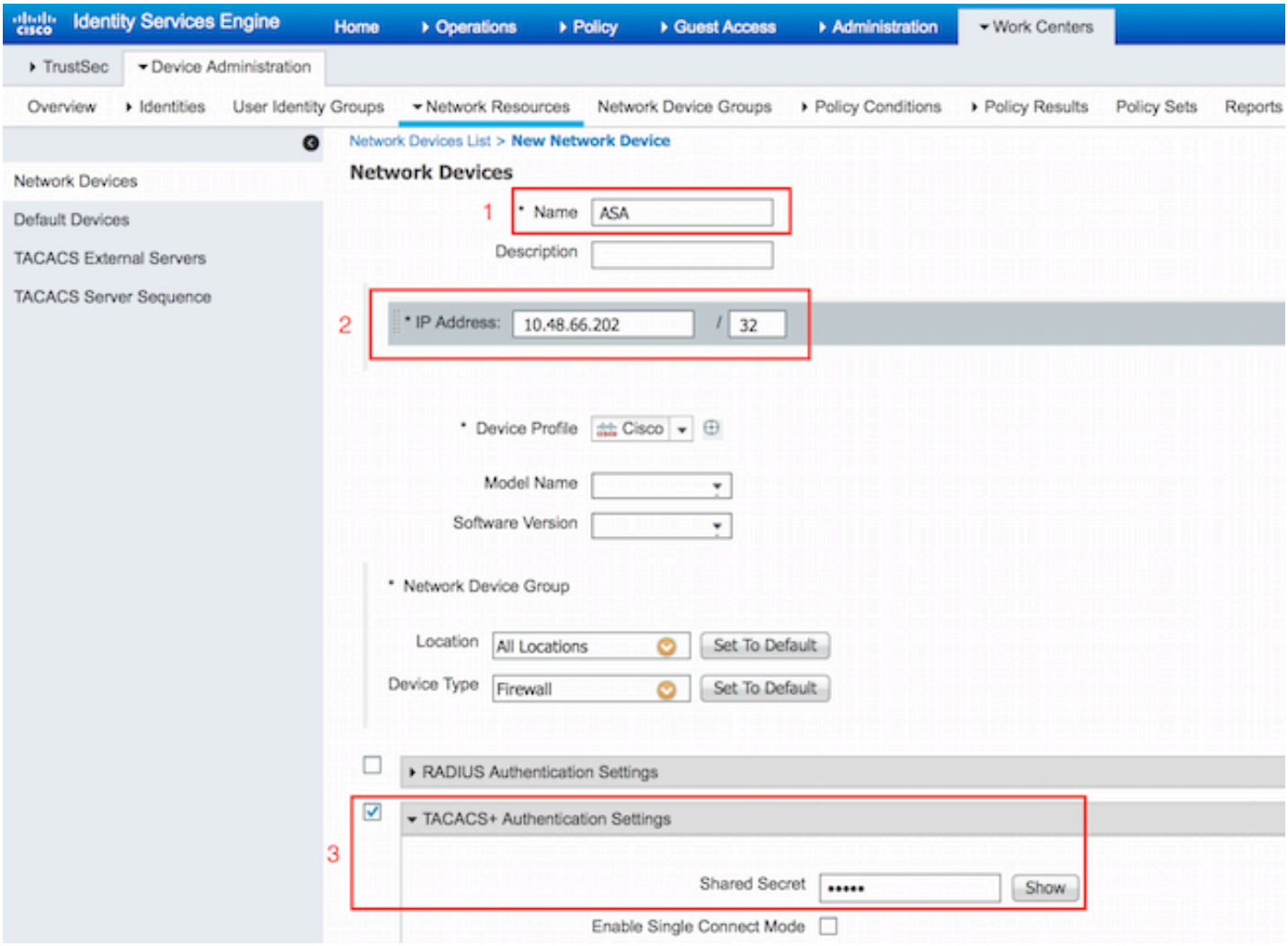
Configuraciones

Configuración ISE para la autenticación y autorización

Crean a dos usuarios. El administrador de usuarios es un grupo local de la identidad de **Admins de la red de la** parte de en el ISE. Este usuario tiene privilegios completos CLI. **El usuario del** usuario es un grupo local de la identidad del **equipo del mantenimiento de red de la** parte de en el ISE. Se permite a este usuario hacer solamente los comandos show y el ping.

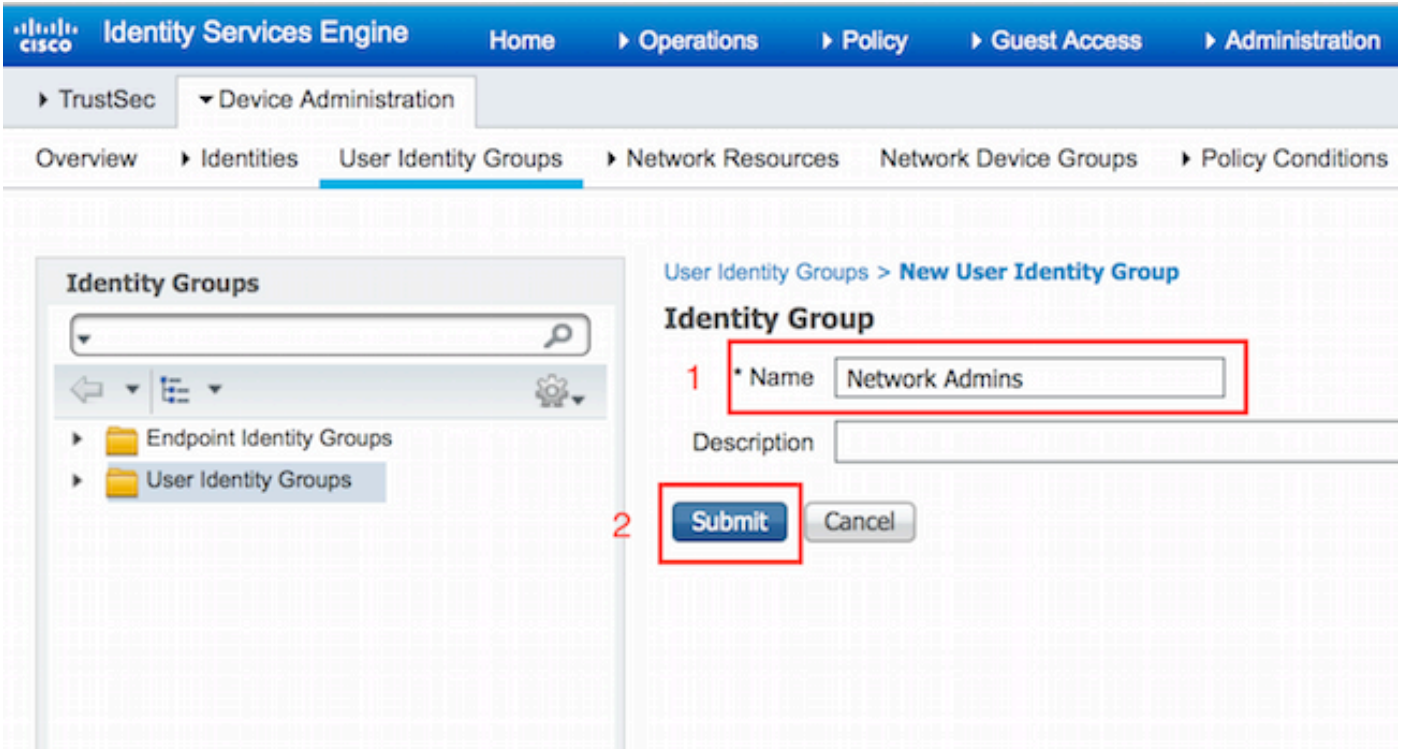
Agregue el dispositivo de red

Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > los recursos de red > los dispositivos de red.** Haga clic en Add (Agregar). Proporcione el nombre, dirección IP, seleccione **autenticación de TACACS+ la casilla de verificación Settings (Configuración)** y proporcione la **clave secreta compartida**. Opcionalmente el tipo de dispositivo/la ubicación puede ser especificado.



Configurar los grupos de la Identificación del usuario

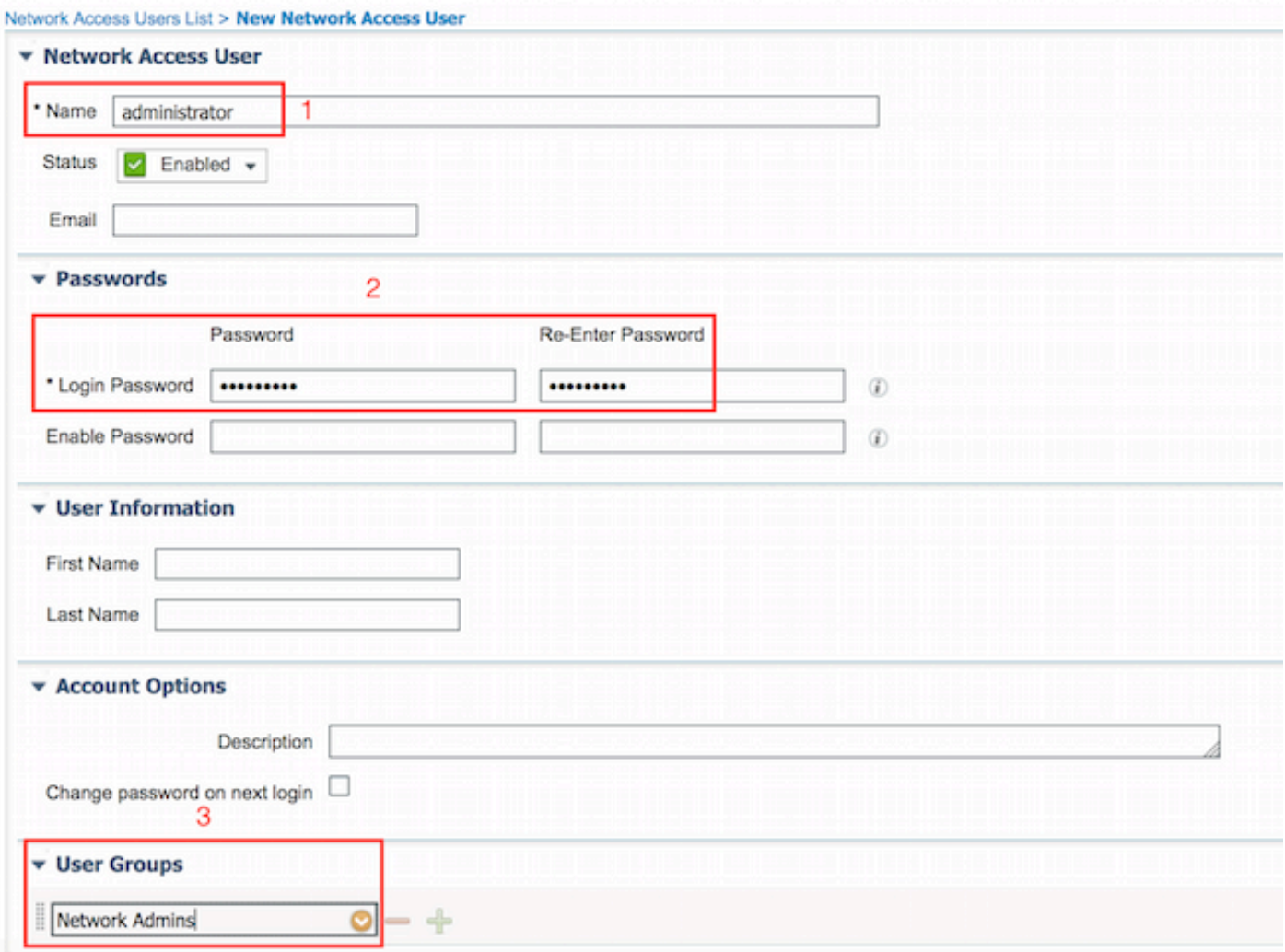
Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > los grupos de la Identificación del usuario.** Haga clic en Add (Agregar). Proporcione el nombre y el tecleo **somete.**



Relance el mismo paso para configurar el grupo de la Identificación del usuario del **equipo del mantenimiento de red**.

Configurar a los usuarios

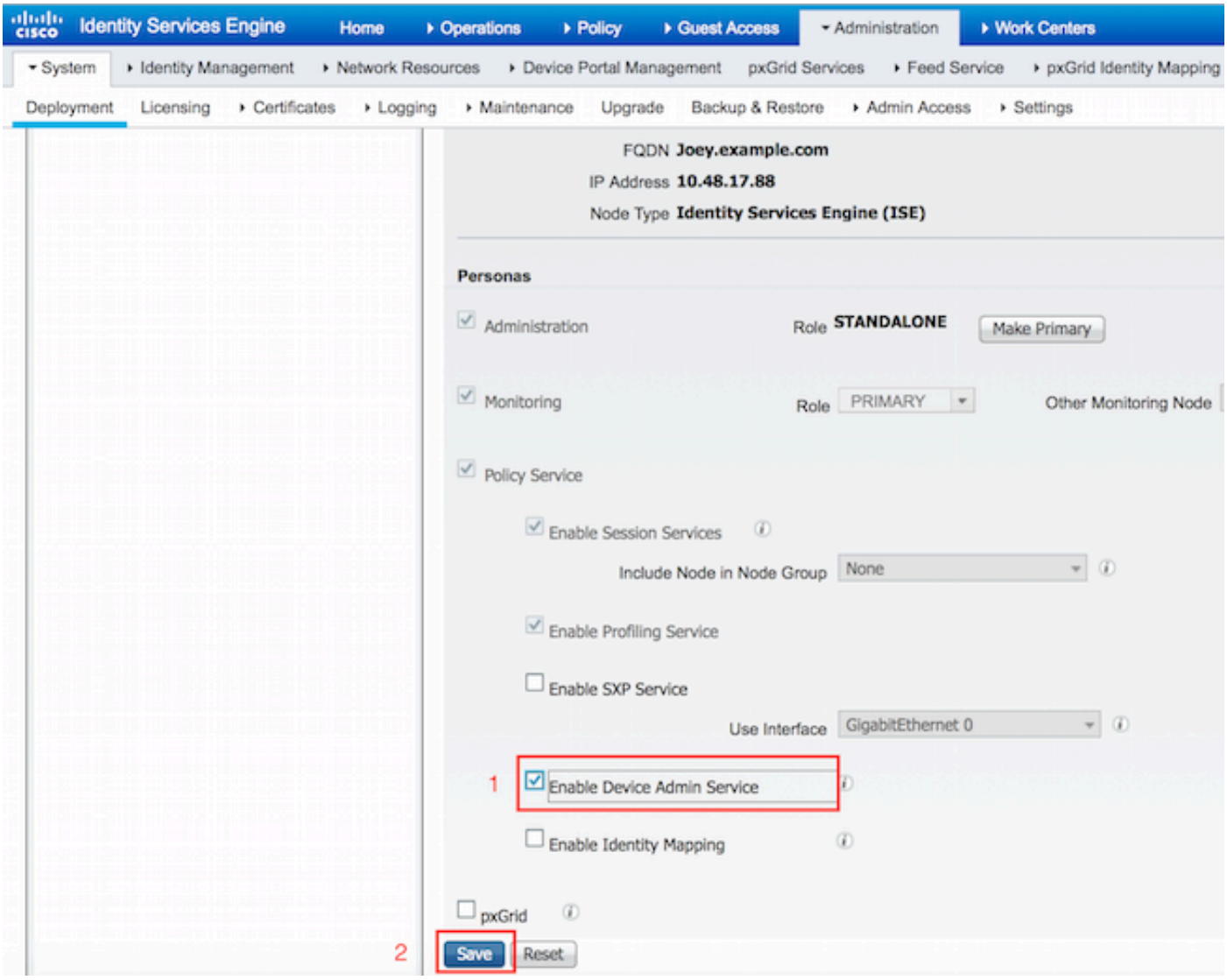
Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > las identidades > Users.** Haga clic en Add (Agregar). Proporcione el nombre, la contraseña de inicio de sesión especifica al grupo de usuarios y el tecleo **somete**.



Relance los pasos para configurar al **usuario del** usuario y para asignar el grupo de la Identificación del usuario del **equipo del mantenimiento de red**.

Habilite el servicio Admin del dispositivo

Navegue a la **administración > al sistema > al despliegue.** Select requirió el nodo. Seleccione el checkbox del **servicio Admin del dispositivo del permiso** y haga clic la **salvaguardia.**

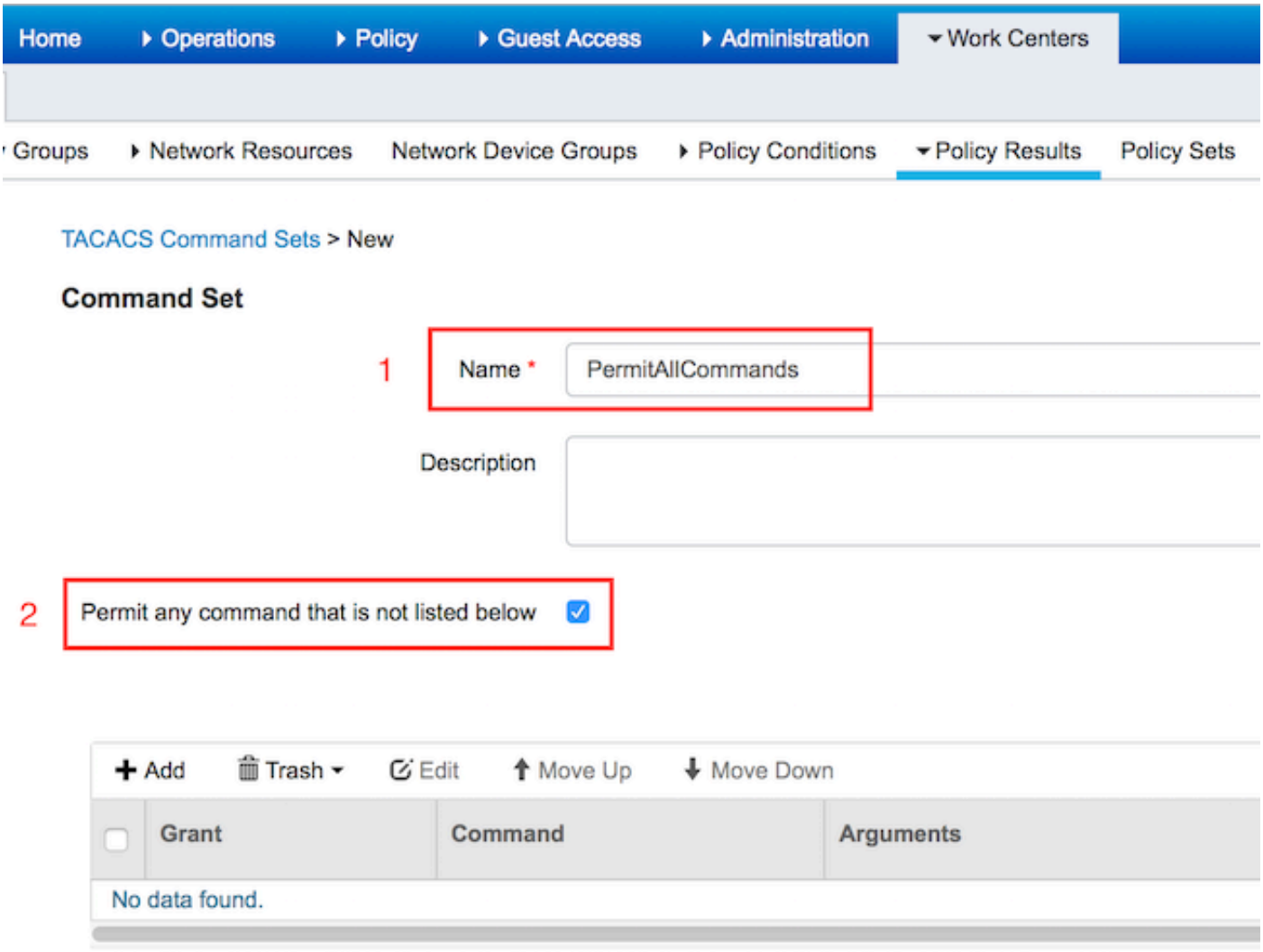


Note: Para el TACACS usted necesita hacer la licencia separada instalar.

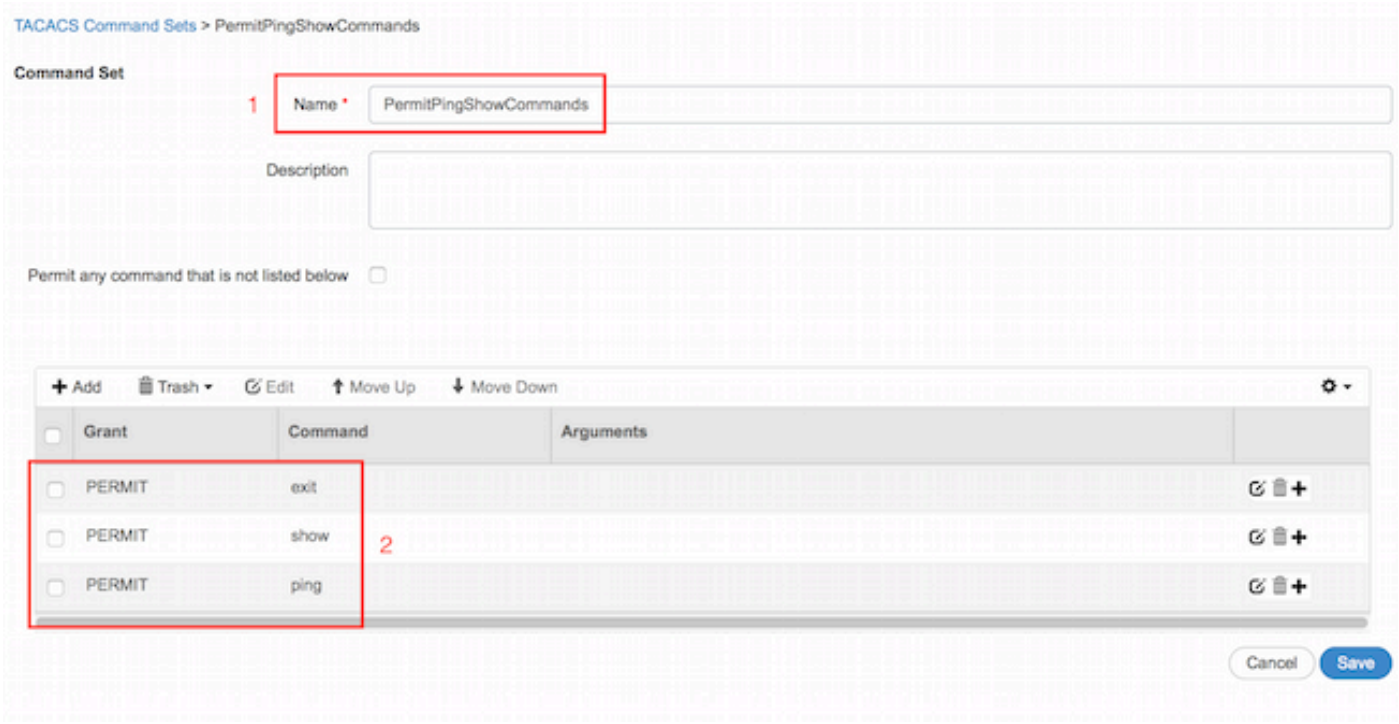
Configurar los conjuntos del comando tacacs

Configuran a dos comandos estableces. Primer **PermitAllCommands** para el **usuario administrador** que permiten los comandos all en el dispositivo. En segundo lugar **PermitPingShowCommands** para el usuario del **usuario** que permiten solamente la demostración y los comandos ping.

1. Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > directiva resulta > los conjuntos del comando tacacs.** Haga clic en Add (Agregar). Proporcione el nombre **PermitAllCommands, el comando permit any** selecto **que no es** checkbox **abajo mencionado** y el tecleo **somete.**

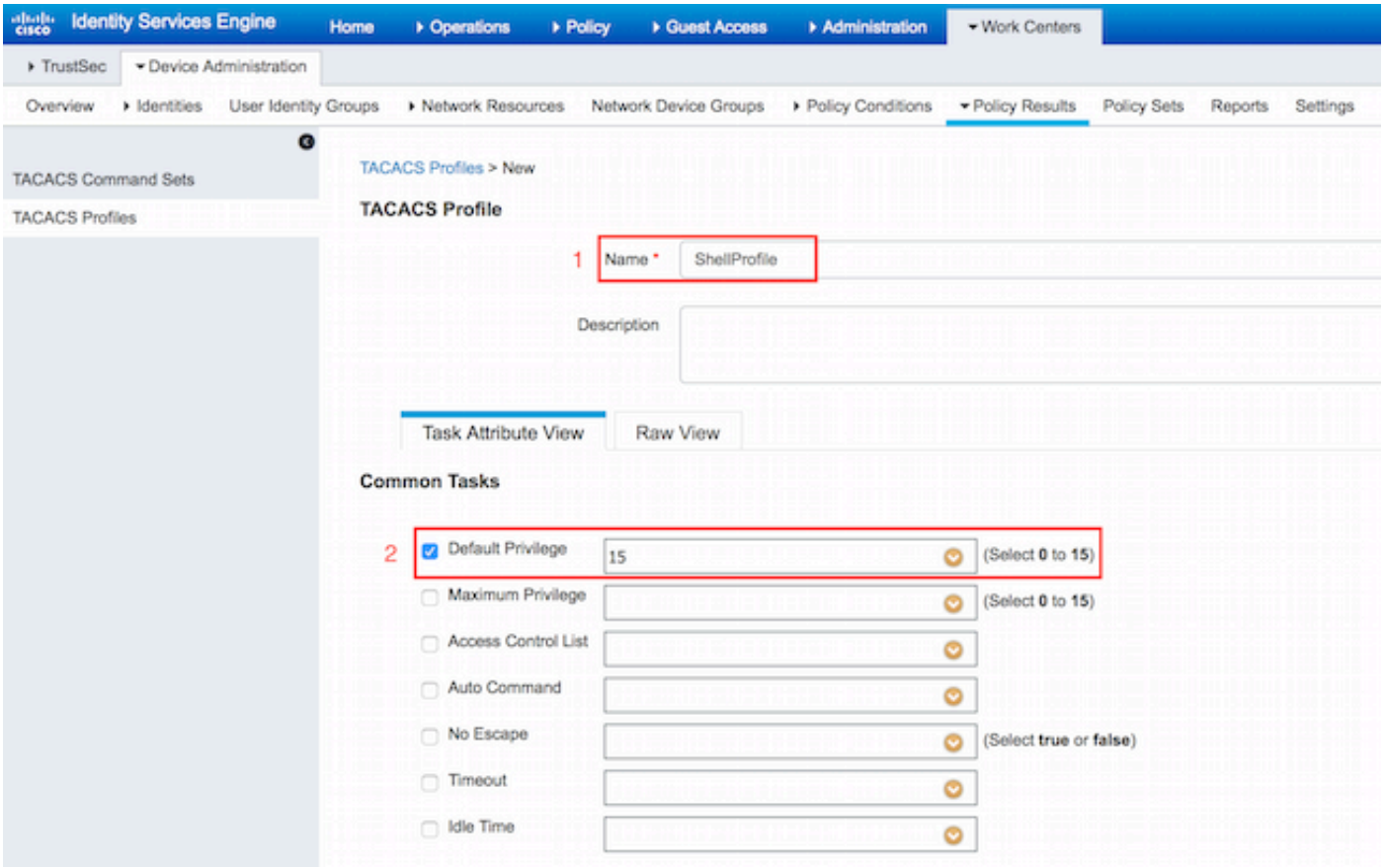


2. Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > directiva resulta > los conjuntos del comando tacacs.** Haga clic en Add (Agregar). Proporcione el nombre **PermitPingShowCommands,** tecleo **agregan** y permiten la **demostración, el ping** y los **comandos exit**. Por abandono si los argumentos se dejan en blanco, todos los argumentos son incluidos. Haga clic en Submit (Enviar).



Configurar el perfil TACACS

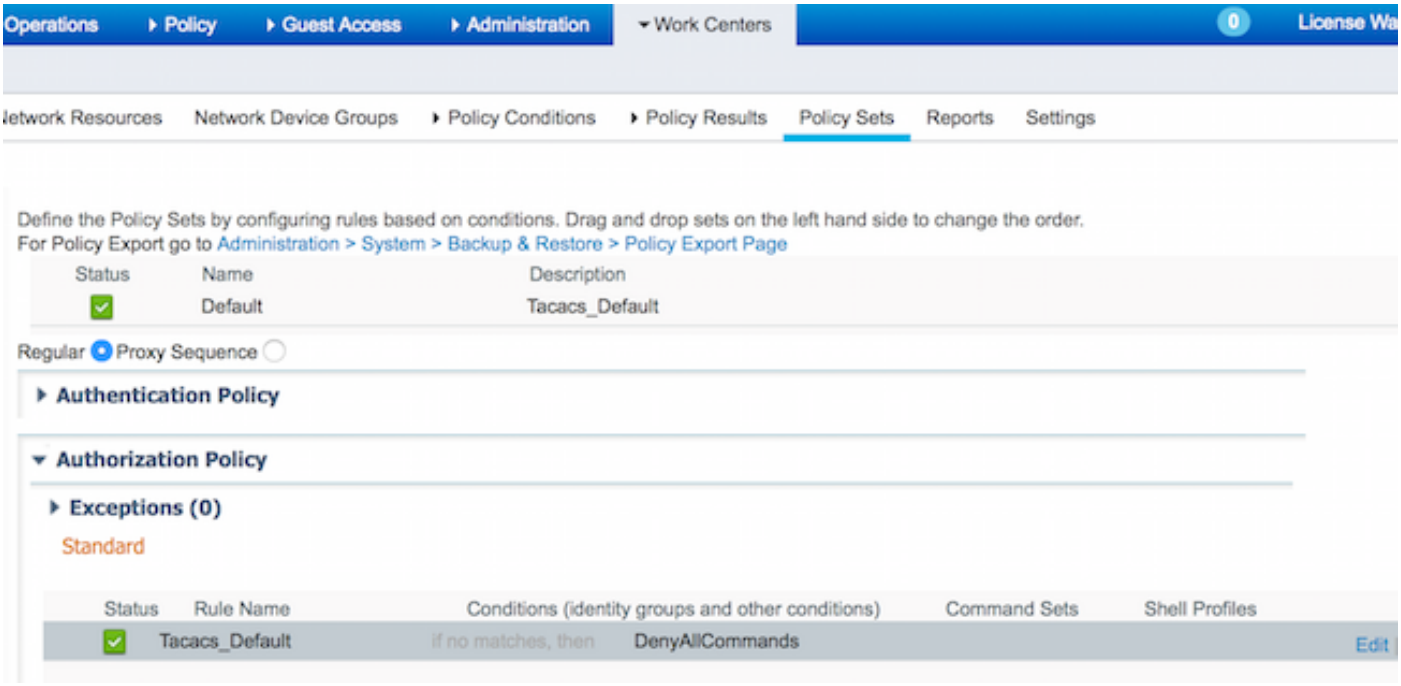
El solo perfil TACACS será configurado. La aplicación real del comando será hecha vía los comandos estableces. Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > directiva resulta > los perfiles TACACS.** Haga clic en Add (Agregar). Proporcione el nombre **ShellProfile,** seleccione el checkbox del **privilegio predeterminado** y ingrese el valor de 15. Haga clic en Submit (Enviar).



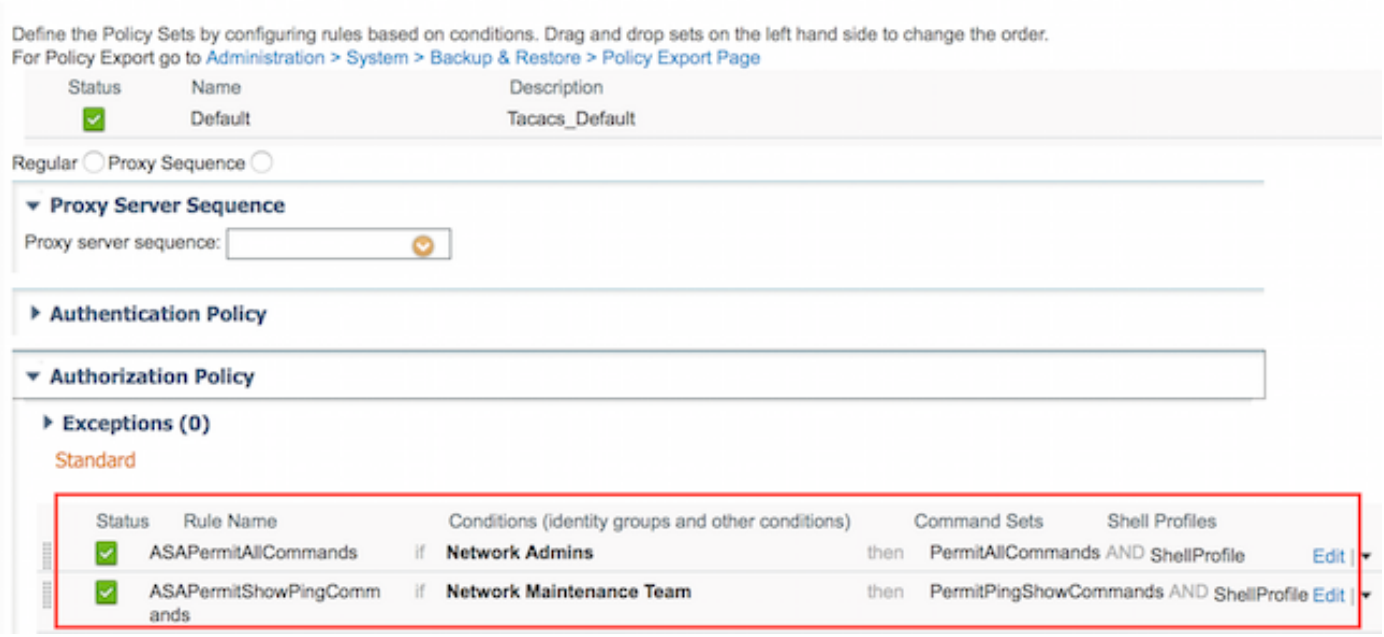
Configurar la directiva de la autorización TACACS

La política de autenticación por abandono señala a All_User_ID_Stores, que incluye el almacén local también, así que se deja sin cambios.

Navegue a los **centros de trabajo > Device Administration (Administración del dispositivo) > los conjuntos de la directiva > directiva del valor por defecto > de la autorización > editan > nueva regla del separador de millares arriba.**



El rulesare de dos autorizaciones configurado, primera regla asigna el perfil **ShellProfile** TACACS y el comando set **PermitAllCommands** basado en la membresía del grupo de la Identificación del usuario de **Admins de la red**. La segunda regla asigna el perfil **ShellProfile** TACACS y el comando set **PermitPingShowCommands** basado en la membresía del grupo de la Identificación del usuario del **equipo del mantenimiento de red**.



Configure el Firewall de Cisco ASA para la autenticación y autorización

1. Cree a un usuario local con el privilegio completo para el retraso con el **comando username**

como se muestra aquí

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. Defina al servidor TACACS ISE, especifique la interfaz, el IP Address del protocolo, y la clave de los **tacacs**.

```
ciscoasa(config)# username cisco password cisco privilege 15
```

> **Note**: La clave del servidor debe hacer juego el define en el servidor ISE anterior.

3. Pruebe el accesibilidad del servidor TACACS con el **comando aaa de la** prueba como se muestra.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

La salida del comando anterior muestra que el servidor TACACS es accesible y han autenticado al usuario con éxito.

4. Configure la autenticación para el ssh, la autorización de EXEC y las autorizaciones de comando como se muestra abajo. Con el auto-**permiso del servidor de autenticación del exec de autorización aaa** le colocarán en el modo EXEC privilegiado automáticamente.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

> **Note**: Con los comandos arriba, la autenticación se hace en el ISE, usuario se coloca directamente en el modo del privilegio y el comando authorization ocurre.

5. Permita shh en la interfaz del mgmt.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds)
INFO: Authentication Successful
```

Verificación

Verificación del Firewall de Cisco ASA

1. Ssh al Firewall ASA como **administrador** que pertenece al grupo de total acceso de la Identificación del usuario. El grupo de **Admins de la red** se asocia a **ShellProfile** y al comando set de **PermitAllCommands** en el ISE. Intente funcionar con el comando any de asegurar el acceso total.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
```

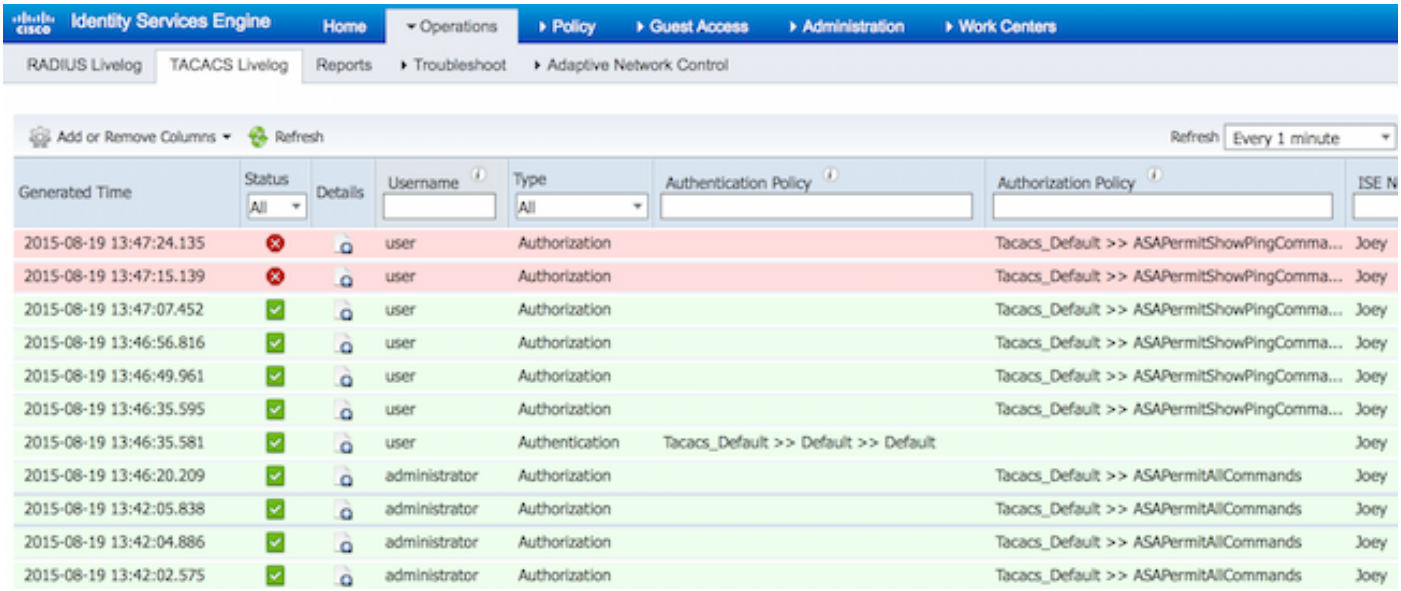
```
ciscoasa#
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
ciscoasa#
```

2. Ssh al Firewall ASA como **usuario** que pertenece al grupo limitado de la Identificación del usuario del acceso. Asocian al grupo del **mantenimiento de red a ShellProfile** y al comando set de **PermitPingShowCommands** en el ISE. Intente funcionar con el comando any de asegurarse de que solamente la demostración y los comandos ping pueden ser publicados.

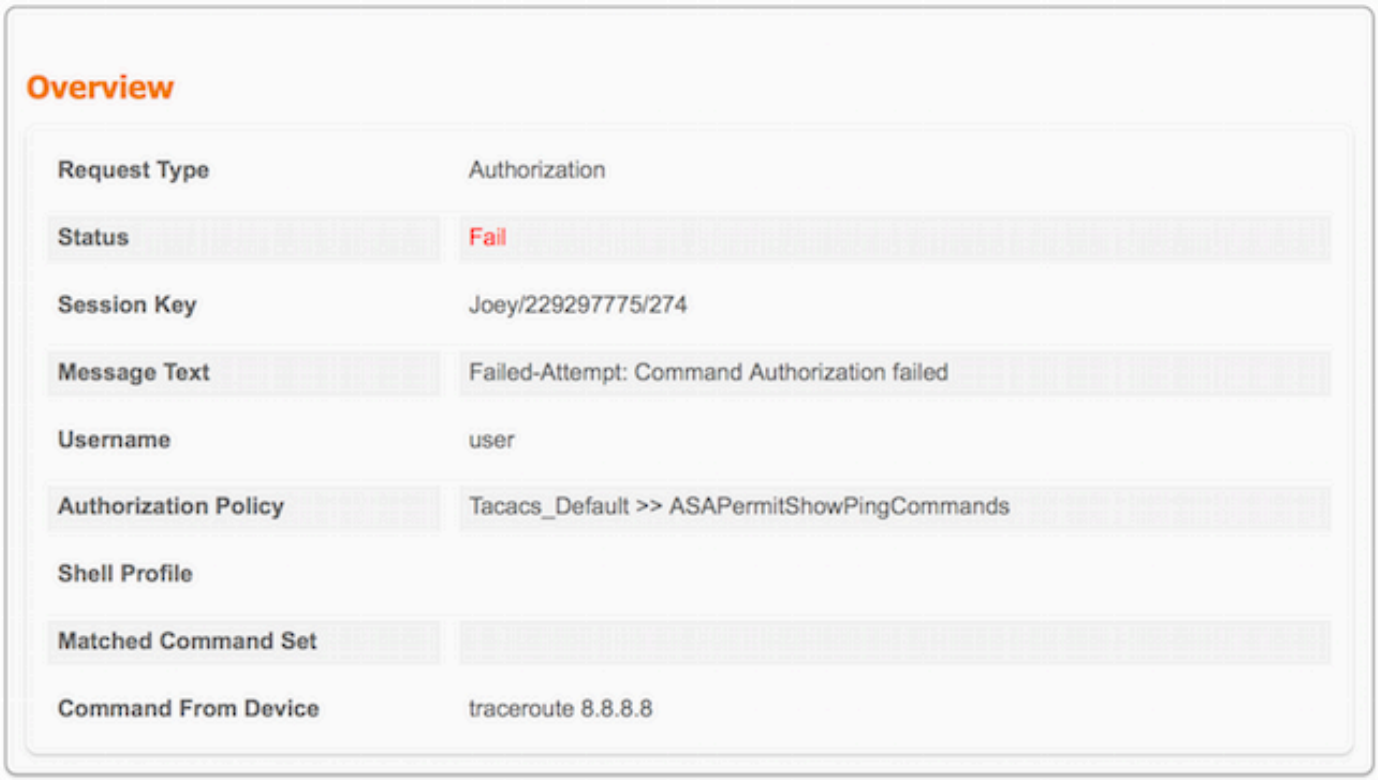
```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
administrator@10.48.66.202's password:
Type help or '?' for a list of available commands.
ciscoasa#
ciscoasa# show version | include Software
Cisco Adaptive Security Appliance Software Version 9.5(1)
ciscoasa# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

Verificación ISE 2.0

1. Navegue a las **operaciones > a TACACS Livelog.** Asegúrese de que las tentativas hechas arriba estén consideradas.



2. Haga clic en los detalles de uno de los informes rojos, anterior ejecutada comando fallada puede ser visto.



Troubleshooting

Error: Intento fallido: Comando authorization fallado

Marque los atributos de SelectedCommandSet para verificar que los conjuntos del comando expected fueron seleccionados por la directiva de la autorización

Información Relacionada

Soporte Técnico y Documentación - Cisco Systems

Release Note ISE 2.0

Guía de instalación del hardware ISE 2.0

Guía de actualización ISE 2.0

ACS a la guía de la herramienta de la migración ISE

Guía de la integración de Active Directory ISE 2.0

Guía del administrador del motor ISE 2.0